OMRON

耐環境型リモートターミナル

NXR-Sシリーズ

CIP Safety対応
簡易ロジックセーフティI/Oターミナル

ユーザーズマニュアル

形NXR-SXD1204-CST
形NXR-SXD1204B-CST

セーフティI/Oターミナル



SBCD-386B

おことわり

- 本マニュアルの内容の一部または全部を無断で複写、複製、転載することを禁じます。
- 本マニュアルの内容に関しては、改良のため予告なしに仕様などを変更することがあります。
  あらかじめご了承ください。
- 本マニュアルの内容に関しては、万全を期しておりますが、万一ご不審な点や誤りなど、お気づきのことがありましたら、お手数ですが、弊社支店または営業所までご連絡ください。
  その際、巻末記載の Man.No.（マニュアル No.）も併せてお知らせください。

商標

- Sysmac は、オムロン株式会社 FA 機器製品の日本およびその他の国における商標または登録商標です。
- Smartclickは、オムロン株式会社の日本およびその他の国における商標または登録商標です。
- Microsoft、Windows、Excel、Visual Basic、Microsoft Edge は、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
- EtherCAT®は、Beckhoff Automation GmbH（ドイツ）よりライセンスを受けた特許取得済み技術であり登録商標です。
- Safety over EtherCAT®は、Beckhoff Automation GmbH（ドイツ）よりライセンスを受けた特許取得済み技術であり登録商標です。
- ODVA、CIP、CompoNet、DeviceNet、EtherNet/IP 、CIP Safetyは ODVA の商標です。
- ODVA、CIP Safetyロゴは ODVA の商標です。
- SD、SDHC ロゴは、SD-3C,LLC の商標です。

その他、本文中に掲載している会社名および製品名は、それぞれ各社の商標または登録商標です。

著作権

- スクリーンショットはマイクロソフトの許諾を得て使用しています。
- 本製品にはサードパーティ製のソフトウェアが組み込まれています。このソフトウェアに関連するライセンスと著作権については、http://www.fa.omron.co.jp/nj_info_j/ および http://www.fa.omron.co.jp/nx_info_j/ をご覧ください。

はじめに

このたびは、耐環境型リモートターミナル NXR-S シリーズ CIP Safety 対応 簡易ロジックセーフティ I/O ターミナル（以下、セーフティ I/O ターミナルと呼びます）をお買い上げいただきまして、ありがとうございます。
本マニュアルは、セーフティ I/O ターミナルを使用するうえで、必要な情報を記載しています。お使いになる前に本マニュアルをよく読んで、機能や性能などを十分ご理解いただき、システムの構築にご活用ください。
また、お読みになったあとも本マニュアルは大切に保管して、いつも手元に置いてお使いください。

対象となる読者の方々

本マニュアルは、電気の知識（電気工事士あるいは同等の知識）を有する、次の方を対象に記述しています。
- FA 機器の導入を担当される方
- FA システムを設計される方
- FA 機器を設置、接続される方
- FA 現場を管理される方

また、プログラミング言語に関して、国際標準規格 IEC 61131-3 もしくは国内標準規格 JIS B 3503 に規定される内容をご理解いただいている方を対象に記述しています。

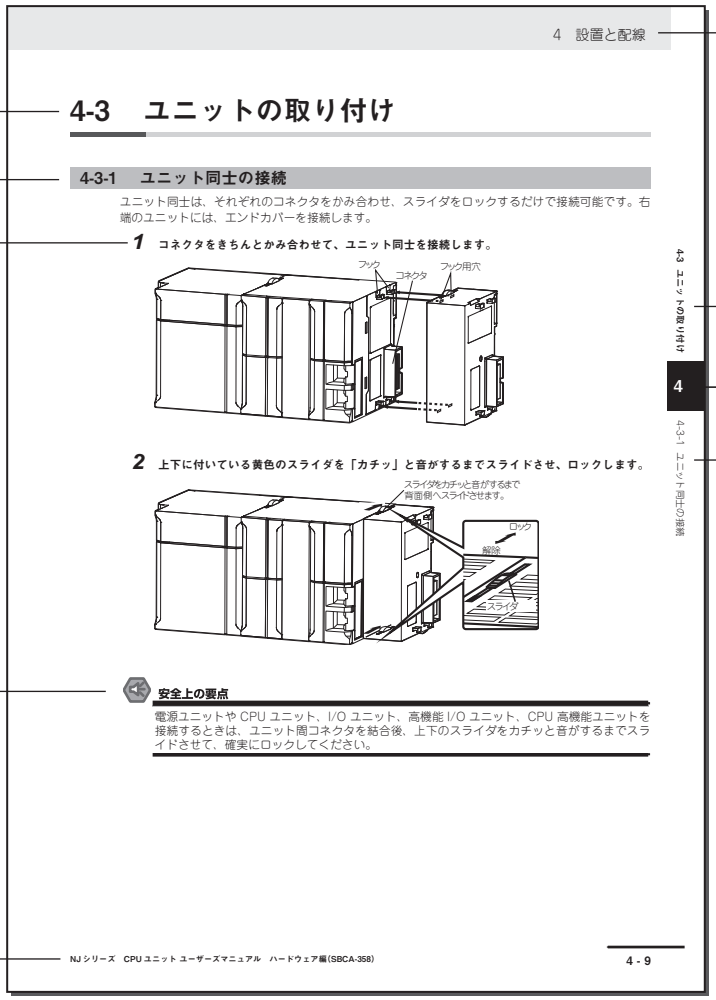
対象となる製品

本マニュアルは以下の製品を対象にしています。
- 耐環境型リモートターミナル NXR-S シリーズ CIP Safety 対応 簡易ロジックセーフティ I/O ターミナル
  形 NXR-SXD1204-CST
  形 NXR-SXD1204B-CST

マニュアルの読み方

ページ構成

このマニュアルの各ページの構成は次のとおりです。



節タイトル

項タイトル

操作手順
操作手順を示します。

注記、補足、参照先
注記、補足、参照先などの各項目を、アイコンによって示しています。

マニュアル名称

章タイトル

節タイトル

項タイトル
現在のページの章／節／項タイトルをそれぞれ示します。

章番号
現在のページの章番号を示します。

このページは、説明用の見本です。実際の内容とは異なります。

アイコン

このマニュアルで使われているアイコンには、次のような意味があります。

安全上の要点

製品を安全に使用するために実施または回避すべきことを示します。

使用上の注意

製品の動作不能、誤動作、または性能・機能への悪影響を予防するために実施または回避すべきことを示します。

参考

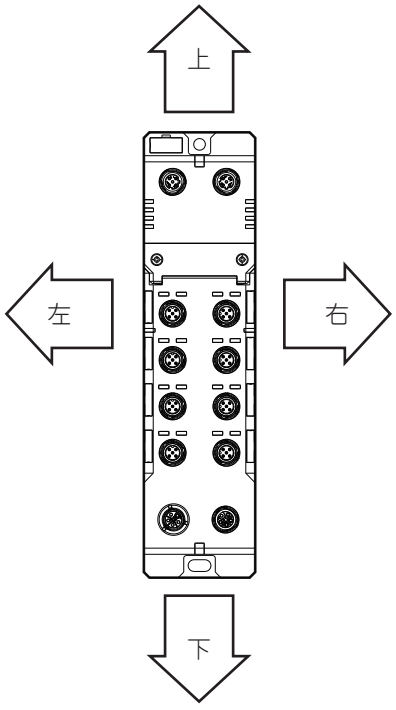
必要に応じて読んでいただきたい項目です。
知っておくと便利な情報や、使用する上で参考となる内容について説明しています。

バージョン関連情報

コントローラやサポートソフトの、バージョンによる性能や機能の違いについて説明しています。

表記についての留意事項

- このユーザーズマニュアルでは、サポートソフトから実機にデータを転送することを“ダウンロード”、実機からデータをサポートソフトに転送することを“アップロード”と記述しています。
- このマニュアルでは、以下の図を正面として、ユニットの向きについて次のように表現しています。



目次構成

1 特長とシステム構成

2 仕様と使用手順

3 各部の名称と機能

4 電源供給の設計

5 取り付けと配線

6 セーフティI/Oターミナルの動作

7 セーフティI/Oターミナルの設定

8 セーフティI/Oターミナルの機能

9 安全応答性能

10 セキュリティガイドライン

11 異常発生時の処置

12 保守点検

A 付録

I 索引

目次

はじめに 1
対象となる読者の方々 1
対象となる製品 1

マニュアルの読み方 2
ページ構成 2
アイコン 3
表記についての留意事項 3

目次構成 5

ご承諾事項 13

安全上の注意 16
安全に使用していただくための表示と意味 16
図記号の説明 16
警告 17
注意 22

安全上の要点 24

使用上の注意 27

法規と規格 28
海外でのご使用 28
EU 指令／規則への適合 28
EN ISO 13849-1 の適合 29
UL,CSA 規格への適合 29
船級規格への適合 30
KC 認証への適合 30

ユニットバージョン 31
ユニットバージョンとは 31

関連マニュアル 33

用語説明 35

マニュアル改訂履歴 37

第 1 章　特長とシステム構成

1-1　セーフティ I/O ターミナルの概要 1-2

1-2　セーフティ I/O ターミナルの特長 1-3

1-3　システム構成 1-4
1-3-1　セーフティコントロールシステム 1-4
1-3-2　ネットワークトポロジ 1-13
1-3-3　カスケード接続 1-14

1-4　サポートソフト 1-16

第 2 章　仕様と使用手順

2-1　仕様 2-2
2-1-1　一般仕様 2-2
2-1-2　通信仕様 2-3
2-1-3　安全仕様 2-4
2-1-4　ユニット仕様 2-6

2-2　使用手順 2-8
2-2-1　STEP1 システム設計 2-8
2-2-2　STEP2 ソフト設計 2-8
2-2-3　STEP3 ハード設計 2-9
2-2-4　STEP4 安全応答性能の計算と検証 2-9
2-2-5　STEP5 ソフトウェア設定とプログラミング 2-10
2-2-6　STEP6 取り付けと配線 2-10
2-2-7　STEP7 動作確認 2-11
2-2-8　STEP8 運転と保守点検 2-11

第 3 章　各部の名称と機能

3-1　各部の名称 3-2

3-2　表示部 3-5
3-2-1　ステータス LED 3-5
3-2-2　I/O LED 3-7
3-2-3　ユニット特定表示 LED 3-9

3-3　ロータリスイッチ 3-10

3-4　コネクタ 3-11
3-4-1　EtherNet/IP 通信コネクタ 3-11
3-4-2　電源コネクタ 3-11
3-4-3　I/O コネクタ 3-12

第 4 章　電源供給の設計

4-1　電源の種類と電源供給システム 4-2
4-1-1　電源の種類と用途 4-2
4-1-2　電源供給システム 4-2

4-2　電源供給の設計方法 4-6
4-2-1　電源供給の設計手順 4-6
4-2-2　直接供給での設計方法 4-6
4-2-3　渡り配線による供給での設計方法 4-12

4-3　電源や保護機器の選定 4-19
4-3-1　外部供給電源の選定 4-19
4-3-2　保護機器の選定 4-19

第 5 章　取り付けと配線

5-1　ユニットの取り付け 5-2
5-1-1　取り付け時の注意事項 5-2
5-1-2　取り付け方向 5-2
5-1-3　取り付け方法 5-2

5-2　EtherNet/IP ネットワークの配線 5-4
5-2-1　敷設時の注意事項 5-4
5-2-2　通信ケーブルの接続 5-4

5-3　電源の配線 5-11
5-3-1　敷設時の注意事項 5-11

5-3-2 使用する電源ケーブルと締め付け工具・締め付けトルク 5-11
5-3-3 外部供給電源への電源ケーブルの接続 5-12
5-3-4 電源ケーブルの接続 5-13

5-4 I/O ケーブルの配線 5-17
5-4-1 敷設時の注意事項 5-17
5-4-2 I/O ケーブルの接続 5-17
5-4-3 配線例 5-22

5-5 接続関連機器 5-26
5-5-1 Ethernet ケーブル 5-26
5-5-2 電源コネクタ接続用ケーブル 5-28
5-5-3 I/O コネクタ接続用ケーブル 5-31
5-5-4 コネクタ用防水カバー 5-34

5-6 オプション品 5-35
5-6-1 マーカ 5-35

第 6 章 セーフティ I/O ターミナルの動作

6-1 動作の概要 6-2

6-2 CIP Safety 通信 6-4

6-3 EtherNet/IP 通信 6-6
6-3-1 タグデータリンク通信 6-6
6-3-2 Explicit メッセージ通信 6-6

6-4 セーフティ入力機能 6-8
6-4-1 接続可能なデバイス 6-8
6-4-2 テスト出力機能 6-10
6-4-3 テストパルス評価機能 6-10
6-4-4 デュアルチャネル評価機能 6-11
6-4-5 セーフティ入力端子の診断機能で検出可能な異常 6-12
6-4-6 入力フィルタ機能 6-12
6-4-7 入力エラーラッチ時間 6-14

6-5 セーフティ出力機能 6-16
6-5-1 接続可能なデバイス 6-16
6-5-2 テストパルス評価機能 6-16
6-5-3 デュアルチャネル評価機能 6-17
6-5-4 セーフティ出力端子の診断機能で検出可能な異常 6-18
6-5-5 出力エラーラッチ時間 6-18
6-5-6 EDM フィードバック 6-19
6-5-7 出力遅延 6-19

6-6 ロジック機能 6-20
6-6-1 ロジック演算 6-20

6-7 安全アプリケーション 6-23
6-7-1 安全アプリケーションの目的 6-23
6-7-2 安全アプリケーションの種類 6-23
6-7-3 固定アプリケーションの詳細 6-27

6-8 動作モード 6-47
6-8-1 動作モードの種類 6-47
6-8-2 各動作モードで実行可能な機能 6-48
6-8-3 各動作モードで実行可能な Web UI 機能 6-49
6-8-4 動作モードの変更と電源投入時モード 6-49

第 7 章 セーフティ I/O ターミナルの設定

7-1 設定の手順 7-3
7-1-1 セーフティコントローラが制御する構成（Type 1 Safety Open によるコンフィグレーション）の設定手順 7-3
7-1-2 セーフティコントローラが制御する構成（Web UI によるコンフィグレーション）の設定手順 7-6

7-1-3 プリセットされた安全アプリケーションでセーフティ I/O ターミナルが制御する構成の設定手順 7-9
7-1-4 ユーザが設計した安全アプリケーションでセーフティ I/O ターミナルが制御する構成（集中管理型）の設定手順 7-11
7-1-5 ユーザが設計した安全アプリケーションでセーフティ I/O ターミナルが制御する構成（分散管理型）の設定手順 7-13

7-2 Web UI の概要 7-16
7-2-1 Web UI の各種仕様 7-16
7-2-2 Web UI の操作権限 7-16
7-2-3 Web UI の画面構成 7-16
7-2-4 メインメニュー一覧 7-17
7-2-5 Web UI の起動手順 7-19
7-2-6 ログイン 7-21
7-2-7 ログアウト 7-23
7-2-8 初回ログイン時の注意事項 7-23

7-3 CIP Safety 通信の設定 7-25
7-3-1 CIP Safety 通信のコネクション設定 7-25
7-3-2 セーフティ I/O ターミナルの設定のエクスポートとインポート 7-34

7-4 EtherNet/IP 通信の設定 7-36
7-4-1 タグデータリンク通信の設定 7-36
7-4-2 LLDP 機能 7-40

7-5 セーフティ入力機能の設定 7-42
7-5-1 セーフティ入力機能の設定手順 7-42
7-5-2 スタンダード出力機能の設定手順 7-44

7-6 セーフティ出力機能の設定 7-47
7-6-1 セーフティ出力機能の設定手順 7-47

7-7 ロジック機能の設定 7-50
7-7-1 ロジック設定手順 7-50
7-7-2 パラメーター覧表示 7-55
7-7-3 考慮すべき入力デバイスの異常動作の例 7-56

7-8 セーフティ署名の設定 7-60

7-9 安全アプリケーションファイルの作成 7-62
7-9-1 セーフティ I/O ターミナルの登録 7-62
7-9-2 安全アプリケーションの設定 7-63
7-9-3 セーフティ入出力機能の設定 7-66
7-9-4 ロジック機能の設定 7-66
7-9-5 安全アプリケーションファイルのエクスポート 7-66

7-10 IP アドレスの設定 7-69
7-10-1 IP アドレスの構成 7-69
7-10-2 ロータリスイッチによる IP アドレスの設定方法の選択 7-71
7-10-3 Sysmac Studio による設定 7-72
7-10-4 Web UI による設定 7-74

7-11 TUNID の設定 7-76
7-11-1 TUNID の目的 7-76
7-11-2 TUNID の設定手順 7-76

7-12 安全アプリケーションの選択 7-81

7-13 再起動 7-82
7-13-1 再起動の目的 7-82
7-13-2 再起動の使用手順 7-82

7-14 コンフィグレーション 7-84
7-14-1 セーフティコントローラのコンフィグレーション 7-84
7-14-2 セーフティ I/O ターミナルのコンフィグレーション 7-84

7-15 時計情報自動調整機能の設定 7-87
7-15-1 時計情報自動調整機能の目的 7-87
7-15-2 時計情報自動調整機能の使用手順 7-87
7-15-3 時計情報自動調整機能の詳細 7-90

7-16 動作モードの変更 7-91

7-16-1 動作モード変更の使用手順 7-91

7-17 コンフィグレーションロック 7-95
7-17-1 コンフィグレーションロックの目的 7-95
7-17-2 コンフィグレーションロックの使用手順 7-95
7-17-3 コンフィグレーションロックの詳細 7-99

7-18 セーフティパスワードの設定 7-100
7-18-1 セーフティパスワードの目的 7-100
7-18-2 セーフティパスワード設定の使用手順 7-100
7-18-3 セーフティパスワードの詳細 7-102

7-19 バックアップ 7-104
7-19-1 バックアップの目的 7-104
7-19-2 バックアップの使用手順 7-104
7-19-3 バックアップの詳細 7-107

第 8 章 セーフティ I/O ターミナルの機能

8-1 機能一覧 8-3

8-2 メモリオールクリア機能 8-4
8-2-1 メモリオールクリア機能の目的 8-4
8-2-2 メモリオールクリア機能の使用手順 8-4
8-2-3 メモリオールクリア機能の詳細 8-7

8-3 HTTPS 通信機能 8-8
8-3-1 HTTPS 通信機能の目的 8-8
8-3-2 HTTPS 通信機能の使用手順 8-8
8-3-3 HTTPS 通信機能の詳細 8-9

8-4 Device Level Ring(DLR)機能 8-10
8-4-1 DLR 機能の目的 8-10
8-4-2 DLR 機能の使用手順 8-10
8-4-3 DLR 機能の詳細 8-10

8-5 渡り配線出力用電源遮断機能 8-11
8-5-1 渡り配線出力用電源遮断機能の目的 8-11
8-5-2 渡り配線出力用電源遮断機能の使用手順 8-11

8-6 I/O 配線チェック機能 8-13
8-6-1 I/O 配線チェック機能の目的 8-13
8-6-2 I/O 配線チェック機能の動作 8-13
8-6-3 I/O 配線チェック機能の I/O 構成設定 8-13
8-6-4 I/O 配線チェック機能の使用手順 8-14

8-7 汎用 CIP コマンド送信機能 8-15
8-7-1 汎用 CIP コマンド送信機能の目的 8-15
8-7-2 汎用 CIP コマンド送信機能の使用手順 8-15

8-8 ユニット特定機能 8-16
8-8-1 ユニット特定機能の目的 8-16
8-8-2 ユニット特定機能の使用手順 8-16
8-8-3 ユニット特定機能の詳細 8-18

8-9 IP アドレス表示機能 8-19
8-9-1 IP アドレス表示機能の目的 8-19
8-9-2 IP アドレス表示機能の使用手順 8-19
8-9-3 IP アドレス表示機能の詳細 8-19

8-10 電源モニタ機能 8-22
8-10-1 電源モニタ機能の目的 8-22
8-10-2 電源モニタ機能の使用手順 8-22
8-10-3 電源モニタ機能の詳細 8-24

8-11 I/O モニタ機能 8-27
8-11-1 I/O モニタ機能の目的 8-27
8-11-2 I/O モニタ機能の使用手順 8-27

8-12 接点動作回数モニタ機能 8-29
8-12-1 接点動作回数モニタ機能の目的 8-29
8-12-2 セーフティ入力端子における使用手順 8-29
8-12-3 セーフティ出力端子における使用手順 8-29

8-13 通信ケーブル診断機能 8-31
8-13-1 通信ケーブル診断機能の目的 8-31
8-13-2 通信ケーブル診断機能の使用手順 8-31
8-13-3 通信ケーブル診断機能の詳細 8-33

8-14 ファームウェアアップデート機能 8-34
8-14-1 ファームウェアアップデート機能の目的 8-34
8-14-2 ファームウェアアップデート機能の使用手順 8-34
8-14-3 ファームウェアアップデート機能の詳細 8-35

第 9 章 安全応答性能

9-1 セーフティ I/O ターミナルの安全応答性能 9-2
9-1-1 安全応答性能の計算方法 9-2
9-1-2 安全応答性能の検証 9-5

第 10 章 セキュリティガイドライン

10-1 セーフティ I/O ターミナルによる多層防御 10-2
10-1-1 セーフティ I/O ターミナルの使用環境 10-2
10-1-2 セーフティ I/O ターミナルを活用した技術層のセキュリティ対策 10-3

10-2 資産を守るセーフティ I/O ターミナルのセキュリティ機能 10-5
10-2-1 通信回線上のデータを保護する 10-5
10-2-2 セーフティ I/O ターミナルへの外部からの攻撃を遮断する 10-7
10-2-3 セーフティ I/O ターミナルの不正操作を防止する 10-9
10-2-4 セーフティ I/O ターミナルの資産の改ざんを防止する 10-10
10-2-5 安全アプリケーションファイル、バックアップファイルを保護する 10-11
10-2-6 否認を防止する 10-12

10-3 セキュリティパッチを適用する 10-13
10-3-1 セーフティ I/O ターミナルをアップデートする 10-13
10-3-2 Sysmac Studio をアップデートする 10-13
10-3-3 パソコンの OS をアップデートする 10-13

10-4 装置を安全に廃棄する 10-14
10-4-1 セーフティ I/O ターミナル内の資産を消去する 10-14

第 11 章 異常発生時の処置

11-1 異常の確認 11-2
11-1-1 異常の通知方法と確認する情報 11-2
11-1-2 異常の確認手順 11-2
11-1-3 動作状態モニタ機能 11-3

11-2 イベントによる異常の確認と対処方法 11-6
11-2-1 イベントログ機能 11-6
11-2-2 Sysmac Studio によるイベントの確認 11-6
11-2-3 Web UI によるイベントの確認方法 11-9
11-2-4 イベントの内容と対処方法 11-12

第 12 章 保守点検

12-1 清掃と点検 12-2
12-1-1 清掃方法 12-2

12-1-2　点検方法 12-2

12-2　ユニットの交換 12-4
12-2-1　ユニット交換時の注意事項 12-4
12-2-2　バックアップ機能を使ったユニット交換 12-4
12-2-3　バックアップ機能を使わないユニット交換 12-5

付録

A-1　外形寸法 A-2

A-2　セーフティ I/O アセンブリデータ A-4
A-2-1　セーフティ入力アセンブリデータ A-4
A-2-2　セーフティ出力アセンブリデータ A-5
A-2-3　コンフィグレーションアセンブリデータ A-7

A-3　I/O アセンブリのポートと対応するセーフティ I/O アセンブリデータの要素 A-13

A-4　サポートする CIP オブジェクト A-15
A-4-1　Identity オブジェクト（クラス ID：01Hex） A-16
A-4-2　Assembly オブジェクト（クラス ID：04Hex） A-18
A-4-3　Unit Manager オブジェクト（クラス ID：380Hex） A-21
A-4-4　Event History Log オブジェクト（クラス ID：34BHex） A-25
A-4-5　Error Event オブジェクト（クラス ID：34CHex） A-28
A-4-6　Safety Discrete Input Point (SDIP)オブジェクト（クラス ID：3DHex） A-31
A-4-7　Safety Discrete Ouput Point (SDOP)オブジェクト（クラス ID：3BHex） A-33
A-4-8　Device Level Ring (DLR)オブジェクト（クラス ID：47Hex） A-35
A-4-9　QoS オブジェクト（クラス ID：48Hex） A-37
A-4-10　TCP/IP Interface オブジェクト（クラス ID：F5Hex） A-39
A-4-11　Ethernet Link オブジェクト（クラス ID：F6Hex） A-43
A-4-12　LLDP Management オブジェクト（クラス ID：109Hex） A-48
A-4-13　LLDP Data Table オブジェクト（クラス ID：10AHex） A-50
A-4-14　Logic Process オブジェクト（クラス ID：309Hex） A-55

A-5　適合宣言書 A-57

索引

ご承諾事項

「当社商品」について特別の合意がない場合には、お客様のご購入先にかかわらず、本ご承諾事項記載の条件を適用いたします。

定義

本ご承諾事項中の用語の定義は次のとおりです。

- 「当社商品」:「当社」の FA システム機器、汎用制御機器、センシング機器、電子・機構部品
- 「カタログ等」:「当社商品」に関する、ベスト制御機器オムロン、電子・機構部品総合カタログ、その他のカタログ、仕様書、取扱説明書、マニュアル等であって電磁的方法で提供されるものも含みます。
- 「利用条件等」:「カタログ等」に記載の、「当社商品」の利用条件、定格、性能、動作環境、取り扱い方法、利用上の注意、禁止事項その他
- 「お客様用途」:「当社商品」のお客様におけるご利用方法であって、お客様が製造する部品、電子基板、機器、設備またはシステム等への「当社商品」の組み込み、または利用を含みます。
- 「適合性等」:「お客様用途」での「当社商品」の(a)適合性、(b)動作、(c)第三者の知的財産の非侵害、(d)法令の遵守および(e)各種規格の遵守

記載事項のご注意

「カタログ等」の記載内容については次の点をご理解ください。

- 定格値および性能値は、単独試験における各条件のもとで得られた値であり、各定格値および性能値の複合条件のもとで得られる値を保証するものではありません。
- 参考データはご参考として提供するもので、その範囲で常に正常に動作することを保証するものではありません。
- 利用事例はご参考ですので、「当社」は「適合性等」について保証いたしかねます。
- 「当社」は、改善や当社都合等により、「当社商品」の生産を中止し、または「当社商品」の仕様を変更することがあります。

ご利用にあたってのご注意

ご採用およびご利用に際しては次の点をご理解ください。

- 定格・性能ほか「利用条件等」を遵守しご利用ください。
- お客様ご自身にて「適合性等」をご確認いただき、「当社商品」のご利用の可否をご判断ください。「当社」は「適合性等」を一切保証いたしかねます。
- 「当社商品」がお客様のシステム全体の中で意図した用途に対して、適切に配電・設置されていることをお客様ご自身で、必ず事前に確認してください。
- 「当社商品」をご使用の際には、(i)定格および性能に対し余裕のある「当社商品」のご利用、冗長設計などの安全設計、(ii)「当社商品」が故障しても、「お客様用途」の危険を最小にする安全設計、(iii)利用者に危険を知らせるための、安全対策のシステム全体としての構築、(iv)「当社商品」および「お客様用途」の定期的な保守、の各事項を実施してください。
- 「当社」は DDoS 攻撃（分散型 DoS 攻撃）、コンピュータウイルスその他の技術的な有害プログラム、不正アクセスにより、「当社商品」、インストールされたソフトウェア、またはすべてのコンピュータ機器、コンピュ

ータプログラム、ネットワーク、データベースが感染したとしても、そのことにより直接または間接的に生じた損失、損害その他の費用について一切責任を負わないものとします。
お客様ご自身にて、①アンチウイルス保護、②データ入出力、③紛失データの復元、④「当社商品」またはインストールされたソフトウェアに対するコンピュータウイルス感染防止、⑤「当社商品」に対する不正アクセス防止についての十分な措置を講じてください。

- 「当社商品」は、一般工業製品向けの汎用品として設計製造されています。従いまして、次に掲げる用途での使用は意図しておらず、お客様が「当社商品」をこれらの用途に使用される際には、「当社」は「当社商品」に対して一切保証をいたしません。ただし、次に掲げる用途であっても「当社」の意図した特別な商品用途の場合や特別の合意がある場合は除きます。
  a）高い安全性が必要とされる用途（例：原子力制御設備、燃焼設備、航空・宇宙設備、鉄道設備、昇降設備、娯楽設備、医用機器、安全装置、その他生命・身体に危険が及びうる用途）
  b）高い信頼性が必要な用途（例：ガス・水道・電気等の供給システム、24 時間連続運転システム、決済システムほか権利・財産を取扱う用途など）
  c）厳しい条件または環境での用途（例：屋外に設置する設備、化学的汚染を被る設備、電磁的妨害を被る設備、振動・衝撃を受ける設備など）
  d）「カタログ等」に記載のない条件や環境での用途
- 上記の(a)から(d)に記載されている他、「本カタログ等記載の商品」は自動車（二輪車含む。以下同じ）向けではありません。自動車に搭載する用途には利用しないで下さい。自動車搭載用商品については当社営業担当者にご相談ください。

保証条件

「当社商品」の保証条件は次のとおりです。

- 保証期間　ご購入後 1 年間といたします。
  （ただし「カタログ等」に別途記載がある場合を除きます。）
- 保証内容　故障した「当社商品」について、以下のいずれかを「当社」の任意の判断で実施します。
  a）当社保守サービス拠点における故障した「当社商品」の無償修理
  （ただし、電子・機構部品については、修理対応は行いません。）
  b）故障した「当社商品」と同数の代替品の無償提供
- 保証対象外　故障の原因が次のいずれかに該当する場合は、保証いたしません。
  a）「当社商品」本来の使い方以外のご利用
  b）「利用条件等」から外れたご利用
  c）本ご承諾事項「ご利用にあたってのご注意」に反するご利用
  d）「当社」以外による改造、修理による場合
  e）「当社」以外の者によるソフトウェアプログラムによる場合
  f）「当社」からの出荷時の科学・技術の水準では予見できなかった原因
  g）上記のほか「当社」または「当社商品」以外の原因（天災等の不可抗力を含む）

責任の制限

本ご承諾事項に記載の保証が、「当社商品」に関する保証のすべてです。
「当社商品」に関連して生じた損害について、「当社」および「当社商品」の販売店は責任を負いません。

輸出管理

「当社商品」または技術資料を、輸出または非居住者に提供する場合は、安全保障貿易管理に関する日本および関係各国の法令・規制を遵守ください。お客様が法令・規則に違反する場合には、「当社商品」または技術資料をご提供できない場合があります。

安全上の注意

安全に使用していただくための表示と意味

このユーザーズマニュアルでは、耐環境型リモートターミナル NXR-S シリーズ CIP Safety 対応 簡易ロジックセーフティ I/O ターミナルを安全に使用していただくために、注意事項を次のような表示と図記号で示しています。
ここで示した注意事項は、安全に関する重大な内容を記載しています。必ず守ってください。
表示と意味は次のとおりです。

⚠ 警 告	正しい取り扱いをしなければ、この危険のために、軽傷・中程度の傷害を負ったり万一の場合には重傷や死亡に至ったりするおそれがあります。また、同様に重大な物的損害をもたらすおそれがあります。
⚠ 注 意	正しい取り扱いをしなければ、この危険のために、時に軽傷・中程度の傷害を負ったり、あるいは物的損害を受けたりするおそれがあります。

図記号の説明

	○に斜線の記号は、禁止を意味しています。 具体的な内容は、○の中と文章で示します。 左図の場合は、「分解禁止」を表します。
	△ 記号は、注意（警告を含む）を意味しています。 具体的な内容は、△ の中と文章で示します。 左図の場合は、「感電注意」を表します。
	△ 記号は、注意（警告を含む）を意味しています。 具体的な内容は、△ の中と文章で示します。 左図の場合は、「一般的な注意」を表します。
	● 記号は、強制を意味しています。 具体的な内容は、● の中と文章で示します。 左図の場合は、「一般的な強制事項」を表します。

警告

⚠ 警告

通電中

通電中は、端子部に触れないでください。
感電のおそれがあります。



本製品を分解しないでください。
特に通電中や通電 OFF 直後は、電圧の高い部分があり、感電のおそれがあります。また、内部の鋭利な部品でけがをする可能性があります。



フェールセーフ対策

CPU ユニットおよび各ユニット／スレーブの故障や外部要因による異常が発生した場合でも、システム全体が安全側に働くように、外部で安全対策を施してください。
異常動作により、重大な事故につながるおそれがあります。



非常停止回路、インタロック回路、リミット回路など、安全保護に関する回路は、必ず外部の制御回路で構成してください。



出力リレーの溶着や焼損、出力トランジスタの破壊などによって、出力が ON または OFF になったままになることがあります。このとき、システムが安全側に動作するように、外部で対策を施してください。



CPU ユニットは、以下のときに、基本出力ユニットの全出力を OFF にし、リモート I/O 上のスレーブはスレーブ側の動作に従います。

- 電源部異常が発生したとき
- 電源接続不正が発生したとき
- CPU 異常（WDT 異常）または CPU リセットが発生したとき
- 全停止フォールトレベルのコントローラ異常が発生したとき
- 電源投入から運転モードに移行するまでの起動中

これらのとき、システムが安全側に動作するよう、外部で対策を施してください。



信号線の断線、瞬時停電による異常信号などに備えて、ご使用者側でフェールセーフ対策を施してください。
異常動作により重大な事故につながるおそれがあります。



電圧／電流入力

ユニット／スレーブに入力する電圧／電流は定められた範囲で入力してください。
範囲外の電圧／電流を使用すると故障や火災の原因となります。



電源設計時

このマニュアルに示すとおり、正しく電源の設計や配線を行ってください。範囲外の電圧／電流の入力や誤配線は、故障や火災の原因となります。



CIP Safety 通信

セーフティ I/O ターミナルを設備・装置への設置およびネットワーク接続する前に、メモリオールクリアを実行してセーフティ I/O ターミナル本体に保存されている以前の設定データを削除してください。 人身傷害による死亡が万一の場合起こる恐れがあります。	
セーフティ I/O ターミナルをネットワークに接続する前に、適切な IP アドレスと通信速度の設定を行ってください。 人身傷害による死亡が万一の場合起こる恐れがあります。	
すべてのセーフティチェーンについて、算出したリアクションタイムが要求仕様を満たしていることを確認してください。 安全機能が損なわれ、人身傷害による死亡が万一の場合起こる恐れがあります。	
オープンタイプを「オープンのみ」に設定する場合は、オリジネータおよびターゲットが正しくコンフィグレーションされていることを確認した上でご使用ください。 安全機能が損なわれ、人身傷害による死亡が万一の場合起こる恐れがあります。	
セーフティ I/O ターミナルのデバッグの時に、オリジネータデバイスでプログラムした動作に対して、ユニットおよび外部接続機器が正しく動作することを確認してください。 安全機能が損なわれ、人身傷害による死亡が万一の場合起こる恐れがあります。	
システムの稼動前にユーザテストを実施して、すべてのデバイスのコンフィグレーションデータと、その動作が正しいことを確認してください。 人身傷害による死亡が万一の場合起こる恐れがあります。	
セーフティネットワーク内に異なる SIL の安全機器を混在させる場合、その影響を十分に検討し、システム全体として必要な安全レベルを確保できることを確認してください。 人身傷害による死亡が万一の場合起こる恐れがあります。	
各安全ネットワークまたは安全サブネットに対して割り当てる SNN は、システム全体で一意となるよう必ず設定してください。 安全機能が損なわれ、人身傷害による死亡が万一の場合起こる恐れがあります。	
セーフティ I/O ターミナルに対するコンフィグレーションデータが正しくダウンロードされたことを Web UI の表示内容に基づいて確認してください。 人身傷害による死亡が万一の場合起こる恐れがあります。	
Type1 Safety Open によってコンフィグレーションする場合、オーナーシップ（CFUNID）の割り当てが正しく設定されていることを、最終検証プロセスの一環として必ず確認してください。 人身傷害による死亡が万一の場合起こる恐れがあります。	
オリジネータに設定した接続データおよび／またはターゲットのコンフィグレーションデータは、必ずターゲットにダウンロードし、テストおよび検証を実施してください。 テストおよび検証が完了した後にのみ、ターゲット上の SCID を確認してください。 人身傷害による死亡が万一の場合起こる恐れがあります。	
セーフティ I/O ターミナルに転送された SCID およびコンフィグレーションデータを、設定時に設定ツール上で表示・確認した SCID およびコンフィグレーションデータと必ず比較してください。 人身傷害による死亡が万一の場合起こる恐れがあります。	
セーフティ I/O ターミナルを交換する場合は、交換用のデバイスが正しく設定されていることを必ず確認し、交換後は必ずユーザー自身がデバイスの動作を検証してください。 人身傷害による死亡が万一の場合起こる恐れがあります。	
セーフティ I/O ターミナルをロックする前に、必ず当該デバイスの動作を完全にテストしてください。 人身傷害による死亡が万一の場合起こる恐れがあります。	

接地時

+24V 側接地は絶対に行わないでください。安全出力の地絡により安全機能が損なわれる恐れがあります。
人身傷害による死亡が万一の場合起こる恐れがあります。

システム構築時

システム構築を実施するにあたり下記事項を遵守の上、その機能が十分発揮されるように安全関連部のシステム構築を行ってください。
安全機能が損なわれ、人身傷害による死亡が万一の場合起こる恐れがあります。

リスクアセスメントの実施

お客様の装置・設備に最適な安全機器類の選択を行うために、設計開発段階において十分なリスクアセスメントを実施し、お客様の装置・設備に潜在する危険要因を特定してください。
関連国際規格例

- ISO 12100「設計の一般原則－リスクアセスメント及びリスク低減」

安全方策

安全機器類を使用してお客様の設備・装置の安全関連部のシステム構築を行う際には、下記を代表例とする一連の国際規格類および/ または関連業界規格類を十分に理解し、適合するように設計してください。
関連国際規格例

- ISO 12100「設計の一般原則－リスクアセスメント及びリスク低減」
- IEC 60204-1「機械用電気機器 第一部：一般要求事項」
- ISO 13849-1, -2「制御システムの安全関連部」
- ISO 14119「ガードに連動するインタロック装置－設計と選択の一般原則」
- IEC/TS 62046「機械類の安全性－人を検出する保護設備の使用基準」
- IEC 62061「安全関連の電気・電子・プログラマブル電子制御システムの機能安全」
- IEC 61508「電気・電子・プログラマブル電子安全関連系の機能安全」

安全機器類の役割

安全機器類は関連法規および規格に適合しておりますが、これらの機能・機構は安全関連部のシステム構築の中で発揮されるように設計されています。そのため、安全機器類がもつ機能・機構が十分に発揮可能なシステム構築を行ってください。
関連国際規格例

- ISO 14119「ガードに連動するインタロック装置－設計と選択の一般原則」
- ISO 13857「上肢および下肢の安全距離」

安全機器類の設置

安全関連部のシステム構築および設置は、適切な教育訓練を受けた技術者により実施してください。使用前に、期待された機能どおりに設置されていることを試運転などで検証してください。
関連国際規格例

- ISO 12100「設計の一般原則－リスクアセスメント及びリスク低減」
- IEC 60204-1「機械用電気機器 第一部：一般要求事項」
- ISO 13849-1, -2「制御システムの安全関連部」
- ISO 14119「ガードに連動するインタロック装置－設計と選択の一般原則」
- IEC 62061「安全関連の電気・電子・プログラマブル電子制御システムの機能安全」
- IEC 61508「電気・電子・プログラマブル電子安全関連系の機能安全」

法令の遵守

安全機器類は関連法規および規格に適合しておりますが、ご使用に際してはお客様の装置・設備に適用される各国関連法規および規格を遵守の上ご使用ください。

使用上の注意事項の遵守

適切に選択された安全機器類の具体的な使用方法に関しては、「取扱説明書」および「ユーザーズマニュアル」に記載されている「仕様」および「注意事項」を遵守してご使用ください。
記載事項から逸脱した使用方法は安全関連部の期待された機能を発揮せず、お客様の設備・装置の予期せぬ故障及び故障に伴う災害発生の要因となります。

装置・設備の移転・譲渡

お客様の設備・装置を移転および譲渡する際は、安全機器類の取扱説明書を必ず保存・付属し、移転先及び譲渡先にて取扱・保守上の支障を来たさないようにしてください。

関連国際規格例

- ISO 12100「設計の一般原則－リスクアセスメント及びリスク低減」
- IEC 60204-1「機械用電気機器 第一部：一般要求事項」
- ISO 13849-1, -2「制御システムの安全関連部」
- IEC 62061「安全関連の電気・電子・プログラマブル電子制御システムの機能安全」
- IEC 61508「電気・電子・プログラマブル電子安全関連系の機能安全」



セーフティ I/O ターミナル使用時

LED は信頼できる表示ではなく、正確な情報を提供することが保証されていません。試運転やトラブルシューティングの際の一般的な診断にのみ使用してください。LED を運転時の表示として使用しないでください。
人身傷害による死亡が万一の場合起こる恐れがあります。



Explicit メッセージ、公開変数などの非安全信号を安全信号として使用しないでください。
安全機能が損なわれ、人身傷害による死亡が万一の場合起こる恐れがあります。



ユニットのテスト出力を安全出力として使用しないでください。
安全機能が損なわれ、人身傷害による死亡が万一の場合起こる恐れがあります。



グローバルアドレス経由でイントラネット環境を利用する場合、SCADA、HMI などの不正な端末や不正なサーバに接続すると、なりすまし、改ざんなどネットワークセキュリティの問題になる可能性があります。お客様ご自身で、端末へのアクセスの制限、セキュア機能を搭載した端末の使用、設置エリアの施錠などの十分な措置を講じてください。



ユニットに接続する安全機能に関わる機器、部品については要求される安全性のレベル、安全カテゴリに応じ、適切な規格適合品を使用してください。
安全機能が損なわれ、重度の人身障害が万一の場合起こるおそれがあります。



システムの稼動前にユーザテストを実施してすべての安全機器がただしく動作することを確認してください。 セーフティ署名はユーザテスト完了によって、検証されたことになります。
安全機能が損なわれ、重度の人身障害が万一の場合起こるおそれがあります。



ユニットを交換した際は、ユニットの形式、ユニットとコネクタの装着位置、およびユニットのコンフィグレーションとその動作が正しいことを確認してください。



渡り配線出力遮断機能は非安全機能です。安全出力として使用しないでください。
安全機能が損なわれ、人身傷害による死亡が万一の場合起こる恐れがあります。



ユニットの安全アプリケーション機能を使用する場合は、ロータリスイッチの設定が正しいことを確認し、必ず実機にて動作確認を行ってから装置を運転してください。
安全機能が損なわれ、人身傷害による死亡が万一の場合起こる恐れがあります。



Sysmac Studio 等のツールからユニット構成情報、パラメータ等の各種データ、設定値を転送するときは、転送先の安全を確認してから行ってください。コントローラの動作モードにかかわらず、装置や機械が想定外の動作をするおそれがあります。



コンフィグレーションが意図せず変更されることを防止するため、妥当性確認が完了した後、コンフィグレーションロックを行ってください。



シングルチャネル出力でセーフティチェーンを構築する際は安全カテゴリ 2 PLc までしか構築できません。シングルチャネル入力、出力を使用する場合は、安全カテゴリ、PL の制約、エラー検出などのシステムに対する要求が発生します。要求・制約に従ってシステムを構築してください。



下記の機能を実行する際は、必ずシステム周辺の安全を確認してから行ってください。
- 当該ユニットの動作モード変更
- セーフティ I/O の接点のセット／リセット
- セーフティ I/O の接点の強制値リフレッシュ
- セーフティ I/O のデータの現在値変更

出力が動作し、重度の人身障害が万一の場合起こるおそれがあります。



ユニットのリストアを行う際は、リストアされたプログラムのセーフティ署名が正しいことを確認してください。安全機能が損なわれ、重度の人身傷害が万一の場合起こるおそれがあります。



妥当性確認が完了した後、コンフィグレーションロックを行ってください。コンフィグレーションロック解除中に安全アプリケーション用ロータリスイッチを変更し、電源を再起動すると異なるセーフティコンフィグレーションで起動します。安全機能が損なわれ、重度の人身傷害が万一の場合起こるおそれがあります。



運用前および運用時

人身傷害による死亡が万一の場合起こる恐れがあります。
お客様にて装置全体を対象としたリスクアセスメントを実施してください。リスクアセスメントにより、電源投入後の自動運転状態遷移が危険な状態を生じないことを確認してください。
電源投入時モードが Executing の場合、本製品は電源投入後又は Type1 Safety Open によるコンフィグレーション後、自動的に運転状態(Executing)になります。電源投入時モードが Executing になる条件は以下です。
- 固定アプリケーションを使用する場合
- アドオンアプリケーション又はユーザ定義アプリケーションのロジックを設計する時に、電源投入時モードを Executing に設定した場合



人身傷害による死亡が万一の場合起こる恐れがあります。
ユーザー定義アプリケーションとアドオンアプリケーションは、お客様の装置の SIL（Safety Integrity Level：安全度水準)の要求事項に基づいて設計、テスト、検証を実行してください。
これらアプリケーションの設計に Sysmac Studio を使用します。Sysmac Studio の使用方法は、本マニュアル及び『Sysmac Studio Version 1 オペレーションマニュアル（SBCA-470)』を参照してください。



人身傷害による死亡が万一の場合起こる恐れがあります。
本製品の連続運転を最低 8 時間以上確保してください。
本製品では、一部のハードウェア自己診断に最大 8 時間かかります。連続運転が 8 時間未満の場合、特定の機能・領域の診断だけが実行されず、当該領域で発生した故障が検出できない可能性があります。



セキュリティ対策

アンチウイルス保護
制御システムに接続するパソコンへの最新の商用品質のウイルス対策ソフトの導入および保守を行ってください。



不正アクセスの防止
当社商品に対して、以下の不正アクセス防止対策を行ってください。
- 権限保有者だけを制御システムや装置へアクセス可能とする物理的統制の導入
- 制御システムや装置のネットワーク接続を最小限に抑えることによる、信頼できないデバイスからのアクセス防止
- ファイアウォールの導入による IT ネットワークからの分離（未使用通信ポートの遮断、通信ホストの制限）
- 制御システムや装置へのリモートアクセスが必要な場合における、仮想プライベートネットワーク(VPN)の使用
- 制御システムや装置へのリモートアクセスにおける多要素認証の導入
- 強固なパスワードの採用と頻繁な変更
- 制御システムや装置で USB メモリなど外部ストレージデバイスを使用する場合の事前ウイルススキャン



データ入出力の保護
制御システムや装置への入出力データの意図せぬ改変に備えた、バックアップや範囲チェックなどの妥当性の確認を行ってください。
- データの範囲チェック
- データの改ざんや異常に備えた、バックアップによる妥当性確認、リストアの準備
- データの改ざんや異常を想定した、緊急停止や縮退運転などの安全設計



紛失データの復元
データ紛失対策として、定期的な設定データのバックアップと保守を行ってください。



グローバルアドレス経由でイントラネット環境を利用する場合、SCADA、HMI などの不正な端末や不正なサーバに接続すると、なりすまし、改ざんなどネットワークセキュリティの問題になる可能性があります。お客様ご自身で、端末へのアクセスの制限、セキュア機能を搭載した端末を使用、設置エリアの施錠などの十分な措置を講じてください。



イントラネットを構築する場合、ケーブル断線や不正ネットワーク機器の影響により通信障害が発生する可能性があります。設置エリアの施錠などの方法によって、ネットワーク機器への物理アクセスを制限するなど、十分な措置を講じてください。



SD メモリカード機能を搭載した機器を使用する場合は、リムーバブルメディアの抜き取り、不正アンマウントなどにより、第三者がリムーバブルメディアの中身のファイルやデータを不正取得、改ざん、差し替えなどを行うセキュリティリスクがあります。お客様ご自身で、設置エリアの施錠、入室管理などの方法によって、コントローラへの物理アクセスを制限したり、リムーバブルメディアの適切な管理対策を行ったりするなどの十分な措置を講じてください。



注意

⚠ 注意

IP アドレス取得時

DHCP サーバから IP アドレスを取得する場合、DHCP サーバ側の設定を以下にしてください。以下の設定になっていない場合、制御対象が想定外の動作をするおそれがあります。
- IP アドレス割付方法: 静的割付
- リース期間: 無限



通電中、電源 OFF 時

通電中や電源を切った直後は、装置に触れないでください。やけどのおそれがあります。



安全上の要点

輸送時

- ユニットを輸送するときは、専用のこん包箱を使用してください。
  また、輸送中に過度な振動や衝撃が加わらないように注意してください。
- 製品を落下させたり、異常な振動や衝撃を与えたりしないでください。
  製品の故障、誤動作の可能性があります。

設置時

- 接地された金属に触れるなどして、人体の静電気を放電させてから製品に触れてください。
- 製品の取り付けねじやスイッチ用カバーのねじは、このマニュアルで指定したトルクで締め付けてください。

装着時

- 端子台、通信ケーブルなどロック機構のあるものは、必ずロックしていることを確認してから使用してください。

配線時

- ケーブル、コネクタおよび防水カバーは、このマニュアルで指定したものを使用してください。
- ケーブルや防水カバーのねじは、このマニュアルで指定したトルクで締め付けてください。
- スイッチなどの設定や配線に間違いがないかを十分に確認してから通電してください。配線をする際は、正しい配線部品、配線工具を使用してください。
- ケーブルを無理に曲げたり、引っ張ったりしないでください。
- ケーブルにものを載せたり、踏んだりしないでください。
- 複数のシステムにて使用する場合、干渉による動作の不安定を防ぐために、各ケーブルどうしは束ねずに必ず 5mm 以上離してください。
- 通信ケーブルの配線時には、以下の注意事項を守ってください。
  a）通信ケーブルは、動力線や高圧線から離してください。
  b）通信ケーブルは、必ずダクト内に配線してください。
  c）通信ケーブルは、このマニュアルで指定した推奨ケーブルを使用してください。
  d）通信ケーブルのシールド線は、両端ともコネクタフードに接続してください。

電源設計時

- 本マニュアルで指定した電源電圧で使用してください。
- 電源最大電流はユニット／入力用電源と出力用電源の合計で 9A です。電源最大電流を超えて使用しないでください。電源最大電流を超えて使用すると、電源ケーブルに過剰な電流が流れることで、発火するおそれがあります。
- ユニット／入力用電源と出力用電源は、以下のとき突入電流が流れることがあります。

a）電源投入時

b）外部接続機器への電源供給開始時

c）外部接続機器の ON/OFF 動作時

また、I/O ケーブルの短絡時、保護がかかるまでの間、過電流が流れることがあります。これらの電流を考慮し、十分に余裕を持った容量の電源を選定してください。突入電流により電源が立ち上がらなくなったり、電源が落ちたりすることがあります。

EtherNet/IP 通信

- EtherNet/IP は通信距離および接続台数／接続方法を仕様の範囲内で使用してください。
- 電源投入直後、EtherNet/IP の通信が確立していない場合があります。CPU ユニットのシステム定義変数またはステータスを用いて通信が確立したことを確認してから、制御に使用するようにプログラミングしてください。

本運転時

- 作成したユーザプログラムおよび各種データや設定値は、十分な動作確認を行ったあと、本運転に移行してください。
- 電源事情が悪い場所では、定格の電圧や周波数の電源を供給できるようにして使用してください。

電源 OFF 時

- ユニットの外部供給電源および通信する相手機器の電源を OFF にして、通信ケーブルを配線してください。
- 次のことを行うときは、ユニットの外部供給電源を OFF にしてください。
  a）接続機器を含む装置の組み立て
  b）ロータリスイッチの設定
  c）ケーブルの接続、配線
  d）端子台やコネクタの取り付け、取り外し

操作時

- 次の操作は設備に影響がないかを確認したうえで行ってください。
  a）CPU ユニットの動作モードの変更（電源投入時の動作モード設定含む）
  b）ユーザプログラム、設定の変更
  c）設定値／現在値の変更
  d）強制値リフレッシュ
- 運転を停止している状態（「プログラム」モード）においても、CPU ユニットは、I/O リフレッシュを行っています。したがって、以下のいずれかの操作によって、本製品に割り付けられた出力リレーエリアのデータ、または高機能 I/O ユニット／CPU 高機能ユニットに割り付けられた各リレーエリアのデータを変更する場合、十分に安全を確認してから行ってください。本製品または高機能 I/O ユニット／CPU 高機能ユニットに接続された負荷が思いがけない動作をするおそれがあります。
  a）周辺ツール（パソコンツール）による、I/O メモリの CPU ユニットへの転送操作
  b）周辺ツールによる、現在値変更操作

c）周辺ツールによる、強制セット／リセット操作
d）メモリカードまたは EM ファイルメモリからの、I/O メモリファイルの CPU ユニットへの転送操作
e）ネットワーク上の他の PLC または上位コンピュータからの、I/O メモリの転送操作

保守時

- 清掃時にシンナー類は使用しないでください。市販のアルコール類を使用してください。
- 高圧洗浄はしないでください。

廃棄時

- 本体の廃棄については、地方自治体により規制を受ける場合があります。それぞれの自治体規制に従って廃棄してください。
- 情報漏えい防止のため、ユーザデータをすべて消去してから廃棄してください。

使用上の注意

保管時、装着時、配線時

- 次のような環境に設置や保管しないでください。運転停止、誤動作する可能性があります。
  a）日光が直接あたる場所
  b）周囲温度や相対湿度が仕様値の範囲を超える場所
  c）温度変化が急激で結露するような場所
  d）腐食性ガス、可燃性ガスのある場所
  e）ちり、ほこり、塩分、鉄粉が多い場所
  f）酸、油、薬品などのひまつがかかる場所
  g）本体に直接振動や衝撃が伝わる場所
  h）動力線が近くを通る場所
- 次のような場所で使用する際は、遮へい対策を十分に行ってください。
  a）静電気などによるノイズが発生する場所
  b）強い電界や磁界が生じる場所
  c）放射線を被ばくするおそれのある場所
  d）電源線が近くを通る場所
- このマニュアルに示すとおり、正しく配線してください。
- スイッチ用カバー取り付け時はパッキンにねじれがないことを確認してください。また、ケース、パッキンに異物付着がないことを確認してください。
- 常時水没させての使用はしないでください。

電源設計時

ユニット／入力用電源を供給する電源と、出力用電源を供給する電源は、別々の電源から供給してください。同一の電源から供給すると、出力機器の負荷変動による誤動作の原因となることがあります。

EtherNet/IP 通信

運転中に EtherNet/IP の通信ケーブルを抜かないでください。出力が不安定になります。

通信ケーブル診断実行時

通信ケーブル診断実行中のポートは通信が遮断され、本ポートを経由するすべてのコネクション（タグデータリンク）やメッセージ通信が一時的に停止します。通信ケーブル診断はシステムに影響ないことを確認したうえで、実施してください。

セキュリティ対策

セキュリティのために、ユニットおよびプロジェクトファイルへのセーフティパスワードの設定を推奨します。セーフティパスワードは漏洩しないよう、厳重に管理してください。特にインターネット回線を通じてセーフティパスワードの受け渡しを行うときは、公開鍵暗号方式を用いるなどして、傍受されないようにしてください。

法規と規格

NXR-S シリーズセーフティ I/O ターミナルは、以下の規格の認証を取得しています。

認証機関	規格
TÜV ラインランド	• EN 61508 parts 1-3 • EN ISO 13849-1 • EN ISO 13849-2 • EN IEC 61131-2 • IEC 61326-3-1 • EN 60529 • EN 61131-6
UL	• NRAQ/NRAQ7 • UL 61010-1、および UL 61010-2-201 • CSA C22.2 No.61010-1、および CSA C22.2 No.61010-2-201 • FSPC （IEC 61508 parts 1-3 および ISO 13849-1）
ODVA	• CIP Safety on EtherNet/IP • EtherNet/IP

NXR-S シリーズセーフティ I/O ターミナルを使用することにより、以下を満足するセーフティコントロールシステムを構築することができます。

- IEC 61508（電気・電子・プログラマブル電子安全関連系の機能安全）の SIL（Safety Integrity Level：安全度水準）3 の要求事項
- EN ISO 13849-1 の PLe (Performance Level e)/ 安全カテゴリ 4 までの要求事項

また、セーフティ I/O ターミナルは、RCM、UKCA、および KC（韓国電波法）の適合登録をしています。

海外でのご使用

本製品のうち、外国為替および外国貿易管理法に定める輸出許可、承認対象貨物（または技術）に該当するものを輸出（または非居住者に提供）する場合は、同法に基づく輸出許可、承認（または役務取引許可）が必要です。

EU 指令／規則への適合

適合指令

- EMC 指令 2014/30/EU
- 機械指令 2006/42/EC

適合の考え方

● EMC 指令 2014/30/EU

オムロンの商品は、各種機械、製造装置に組み込まれ使用される電気機器であるため、組み込んだ機械や装置がより容易に EMC 規格に適合できるように、商品自身の関連する EMC 規格(*1)の適合を図っています。しかし、お客様の機械や装置はさまざまであり、かつ EMC の性能は EU 指令適合商品を組み込んだ機器や制御盤の構成、配線状態、配置状態などにより変化しますので、お客様の使用状態での適合性は確認できま

せん。したがって、機械や装置全体での最終的な EMC 適合性の確認を、お客様自身で実施していただくようにお願いします。

***1.** EMC（Electro-Magnetic Compatibility：電磁環境両立性） 関連規格のうち、EMS（Electro-Magnetic Susceptibility：電磁感受性） に関しては EN 61131-2、EMI（Electro-Magnetic Interference：電磁妨害） に関しては EN 61131-2。また、Radiated emission は 10m 法によります。

● 機械指令 2006/42/EC

機械指令では機械の安全性に用いるセーフティコンポーネントに対して必要な安全性が確保されていることを求めています。
適用規格は EN ISO 13849-1 です。

● EU 指令への適合

NXR-S シリーズは、EU 指令に適合しています。しかし、お客様の機械や装置を EU 指令に適合させるにあたり、以下の注意が必要です。

- NXR-S シリーズにユニット／入力用電源、出力用電源として接続する DC 電源は、SELV 仕様の電源を使用してください。
  オムロン製 S8VK-S シリーズの電源を推奨します。この推奨電源にて EMC 規格の適合性を確認しています。
- NXR-S シリーズの EU 指令適合商品は、EMI に関して共通エミッション規格に適合していますが、特に Radiated emission（10m 法）に関しては、使用する制御盤の構成、接続される他の機器との関係、配線等により変化することがあります。
  したがって、EU 指令適合品である NXR-S シリーズを使用する場合でも、お客様にて機械や装置全体で EU 指令適合性を確認および対応をしていただく必要があります。
- NXR-S シリーズにユニット／入力用電源、出力用電源として接続する DC 電源は、出力保持時間が 10ms 以上の電源を使用してください。
- この商品は「class A」（工業環境商品）です。住宅環境で利用しますと、電波妨害の原因となる可能性があります。その場合には電波妨害に対する適切な対策が必要となります。
- 電源ケーブルおよび I/O ケーブルの長さ 30m 以下で、適合性を確認しています。

EN ISO 13849-1 の適合

EN ISO 13849-1 では、セーフティコントロールシステム構築時の安全関連ソフトウェアを作成する、ソフトウェア設計のライフサイクルの全ての活動（例：基本ソフトウェア設計、安全回路システム設計、ソフトウェアアップグレード）においてシステムの障害を回避するために、ソフトウェアを見やすく、理解しやすく、試験しやすく、かつ保守しやすくするための工程管理を運用することが要求されています。
つまり、設備・装置などのソフトウェア設計・開発に対しても工程管理を運用することが要求されています。
規格の適合はお客様自身で実施していただくようお願いします。

お客様の装置の安全性能を検証するために必要な機械安全信頼性データは、
http://www.ia.omron.com/support/sistemalibrary/index_jp.html を参照してください。

UL,CSA 規格への適合

NXR-S シリーズには、UL 規格や CSA 規格に適合している形式があります。
UL 規格や CSA 規格に適合している形式を使用して、お客様の機械や装置に規格を適用する場合は、製品に付属する「INSTRUCTION SHEET」を参照してください。「INSTRUCTION SHEET」に、規格を適用するための使用条件が説明されています。

船級規格への適合

本製品は、各種船級規格に適合していません。

KC 認証への適合

本製品を韓国で使用する場合には、以下の注意事項を守ってください。

사 용 자 안 내 문
이 기기는 업무용 환경에서 사용할 목적으로 적합성평가를 받은 기기로서 가정용 환경에서 사용하는 경우 전파간섭의 우려가 있습니다.

この機器は業務用環境で使用する目的で適合性評価を受けた機器のため、家庭用環境で使用する場合、電波干渉のおそれがあります。

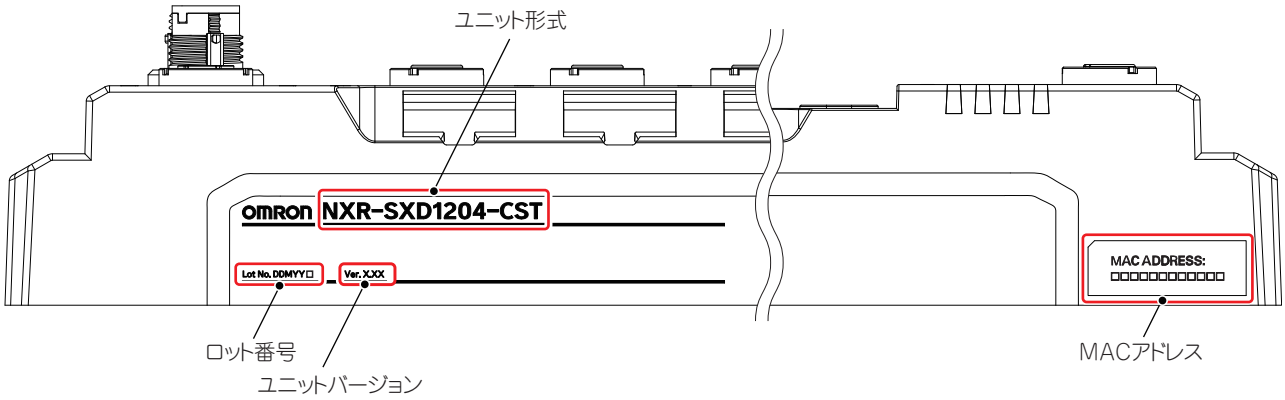
ユニットバージョン

ユニットバージョンとは

ユニットバージョンとは、NXR-S シリーズの各ユニットの改変番号のことです。同一形式のユニットでも、ユニットバージョンが異なると、搭載機能にいくらかの違いがあります。

製品での表記

製品の側面の仕様表記部にて、「ユニットバージョン」が確認できます。



仕様表記部には以下の情報が記載されています。

名称	機能
ユニット形式	本ユニットの形式を示します。
ユニットバージョン	本ユニットのユニットバージョンを示します。
ロット番号	本ユニットのロット番号を示します。 DDMYY：ロット番号、□：当社使用 M は月を表し、X は 10 月、Y は 11 月、Z は 12 月を意味します。
MAC アドレス	本ユニットの EtherNet/IP ポートの MAC アドレスを示します。

Web UI での表示

Web UI の生産情報表示機能を使用しても、ユニットバージョンを確認できます。以下は、Web UI の「生産情報表示機能」と「生産情報画面」です。

● 生産情報表示機能の詳細

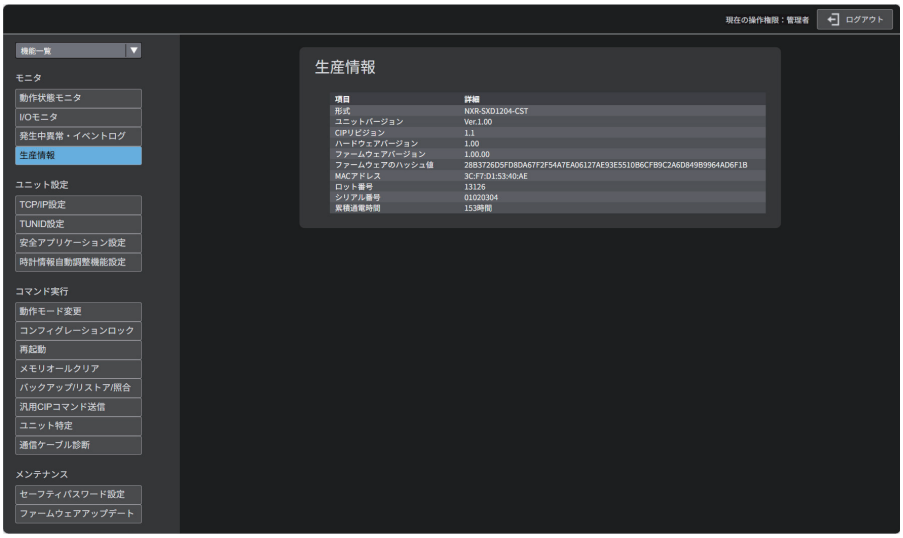
生産情報表示機能では、セーフティ I/O ターミナルの以下の情報が表示されます。

- 形式
- ユニットバージョン
- CIP リビジョン
- ハードウェアバージョン
- ファームウェアバージョン

- ファームウェアのハッシュ値
- MAC アドレス
- ロット番号
- シリアル番号
- 累積通電時間

● 生産情報画面

生産情報画面は、ユニットバージョンなど当該ユニットの生産情報を表示する画面です。



関連マニュアル

関連するマニュアルは下表のとおりです。併せてご覧ください。

マニュアル名称	Man.No.	形式	用途	内容
耐環境型リモートターミナル NXR-S シリーズ CIP Safety 対応 簡易ロジックセーフティ I/O ターミナル ユーザーズマニュアル（本書）	SBCD-386	形 NXR-SXD1204-CST 形 NXR-SXD1204B-CST	耐環境型リモートターミナル NXR-S シリーズ CIP Safety 対応 簡易ロジックセーフティ I/O ターミナルの使用方法を知りたいとき。	耐環境型リモートターミナル NXR-S シリーズ CIP Safety 対応 簡易ロジックセーフティ I/O ターミナルのハードウェアや設定方法、機能について説明しています。
NX シリーズ セーフティコントロールユニット／通信コントロールユニット ユーザーズマニュアル	SGFM-723	形 NX-SL5□□□ 形 NX-SI□□□□ 形 NX-SO□□□□ 形 NX-CSG□□□	NX シリーズ セーフティコントロールユニット／通信コントロールユニットの使用方法について知りたいとき。	NX シリーズ セーフティコントロールユニット／通信コントロールユニットのハードウェアや設定方法、機能について説明します。
NX シリーズ 通信コントロールユニット ユーザーズマニュアル 内蔵機能編	SGFM-724	形 NX-CSG□□□	NX シリーズ 通信コントロールユニットの内蔵機能について知りたいとき。	NX シリーズ 通信コントロールユニットのソフトウェア設定方法や通信機能について説明します。
NX シリーズ セーフティコントロールユニット ユーザーズマニュアル	SGFM-710	形 NX-SL□□□□ 形 NX-SI□□□□ 形 NX-SO□□□□	NX シリーズ セーフティコントロールユニットの使用方法について知りたいとき。	NX シリーズ セーフティコントロールユニットのハードウェアや設定方法、機能について説明します。
NX シリーズ セーフティコントロールユニット コマンドリファレンスマニュアル	SGFM-711	形 NX-SL□□□□	セーフティ CPU ユニット用の命令仕様の詳細について知りたいとき。	セーフティ CPU ユニット用の命令の詳細を説明します。
NJ/NX シリーズ CPU ユニット 内蔵 EtherNet/IP™ポート ユーザーズマニュアル	SBCD-377	形 NX701-□□□□ 形 NX502-□□□□ 形 NX102-□□□□ 形 NX1P2-□□□□ 形 NJ501-□□□□ 形 NJ301-□□□□ 形 NJ101-□□□□	NJ/NX シリーズ CPU ユニットの内蔵 EtherNet/IP ポートを使用するとき。	内蔵 EtherNet/IP ポートに関して説明します。 基本設定、タグデータリンク、その他の機能について記述しています。
NY シリーズ IPC マシンコントローラ 産業用パネル型 PC ／産業用 ボックス型 PC ユーザーズマニュアル 内蔵 EtherNet/IP™ポート編	SBCD-369	形 NY532-□□□□ 形 NY512-□□□□	NY シリーズ産業用 PC の内蔵 EtherNet/IP ポートを使用するとき。	内蔵 EtherNet/IP ポートに関して説明します。 基本設定、タグデータリンク、その他の機能について記述しています。
Sysmac Studio Version 1 オペレーションマニュアル	SBCA-470	形 SYSMAC-SE2□□□	Sysmac Studio の操作方法、機能について知りたいとき。	Sysmac Studio の操作方法について説明します。

マニュアル名称	Man.No.	形式	用途	内容
FA システム セキュリティガイドライン	SBCA-140	-	FA システム全般にかかわるセキュリティの考え方について知りたいとき。	オムロンの FA 製品のセキュリティの取り組みとご利用いただくお客様にて実施していただきたいセキュリティ対策について説明します。
NJ/NX コントローラ セキュリティガイドライン	SBCA-142	形 NX701-□□□□ 形 NX502-□□□□ 形 NX102-□□□□ 形 NX1P2-□□□□ 形 NJ501-□□□□ 形 NJ301-□□□□ 形 NJ101-□□□□	NJ/NX シリーズ CPU ユニットを用いたセキュリティ対策ついて知りたいとき。	NJ/NX シリーズ CPU ユニットを用いて実施できるセキュリティ対策について説明します。
耐環境型 IP67・パワーサプライ ユーザーズマニュアル	SGTC-706	形 S8NR-S□□ □24	耐環境型 IP67・パワーサプライの使用方法について知りたいとき。	耐環境型 IP67・パワーサプライの機能、性能、使用方法について記述しています。

用語説明

用語	説明
CIP Safety オリジネータ	CIP Safety における通信上の役割のひとつです。CIP Safety オリジネータは CIP Safety ターゲットに対して CIP Safety コネクションの管理を行います。CIP Safety オリジネータはデバイス単位ではなく、コネクション単位で存在します。
CIP Safety コネクション	セーフティプロセスデータ通信のプロトコルが CIP Safety であるセーフティ I/O コネクションを指します。通信上の役割により、CIP Safety オリジネータコネクションと CIP Safety ターゲットコネクションがあります。
CIP Safety ターゲット	CIP Safety における通信上の役割のひとつです。CIP Safety ターゲットは CIP Safety オリジネータからの CIP Safety コネクションの開設要求に応じます。CIP Safety ターゲットはデバイス単位ではなく、コネクション単位で存在します。
Device Level Ring (DLR)	EtherNet/IP 規格で定義された、シングル・フォルト・トレラント・リダンダンシーを提供するデータリンク層プロトコル
TUNID	CIP Safety 通信で、セーフティシステム上のすべてのネットワークから、デバイスを一意に特定するための ID です。6 バイトのセーフティネットワーク番号 (SNN) と 4 バイトのノード ID を組み合わせた、合計 10 バイトの値です。
アセンブリ	デバイスの内部にもっているデータを外部からアクセスするためひとつに集めたものです。
アドオンアプリケーション	本ユニットに対し、Web UI を使用してロータリスイッチの番号に割り付ける、ロジックを持つ安全アプリケーションです。
安全アプリケーション	安全アプリケーションとは、安全制御を実現するためのアプリケーションのことです。本書では、本ユニット内で動作するものに限定して「安全アプリケーション」と呼びます。 本書で扱う安全アプリケーションには、固定アプリケーション、アドオンアプリケーション、ユーザ定義アプリケーション、リモート I/O モード用アプリケーションの 4 種類があります。
簡易ロジックモード	簡易ロジック演算機能を使用して動作するモードです。
簡易ロジックモード用アプリケーション	簡易ロジックモードで使用されるアプリケーションです。I/O 構成設定およびロジック設定が定義されています。 固定アプリケーション、アドオンアプリケーション、ユーザ定義アプリケーションの 3 種類があります。
固定アプリケーション	本ユニットにあらかじめ内蔵されている安全アプリケーションです。
コネクション	デバイス間で通信を行うための、論理的な通信路です。
コンフィグレーション	デバイスおよびネットワークに対して行う設定です。
シングルチャネル	冗長性をもたせず、入力または出力を 1 つ（1 点）で使用することです。
スタンダード	セーフティコントロールで使用するために特別な安全方策を施した機器、機能、データなどと区別するために、一般制御用途で使用されるものを、このマニュアルでは、「スタンダード」と呼びます。
スタンダードコントロール	一般制御用途の機器、機能、データ等を使用した制御を指します。セーフティコントロールと区別するための呼称です。
セーフティ CPU ユニット	セーフティコントロール用の CPU ユニットです。NX ユニットの一種です。
セーフティ I/O ターミナル	セーフティコントロールに使用する I/O ターミナルです。
セーフティ機能	機械からの危険に対し、セーフティ状態を実現するために、セーフティコントロールシステムによって実行される機能です。
セーフティコントロール	特別な安全方策を施した機器、機能、データを使用した制御を指します。
セーフティコントロールユニット	セーフティコントロールに使用する NX ユニット群の総称です。
セーフティ出力機器	セーフティコントロールで使用するために特別な安全方策を施した出力機器。 安全リレーなどの総称です。
セーフティ出力機能	セーフティ出力データの値、およびセーフティ出力端子の出力信号が正常か異常かを評価する機能です。 セーフティ特有の評価機能として、テストパルス評価機能、デュアルチャネル評価機能などがあります。 評価結果が異常時にはセーフティ出力端子の出力信号を OFF とします。
セーフティ状態	人に危害がおよぶリスクが許容できるレベルまで低減されている時の、機器または装置の状態です。
セーフティ入力機器	セーフティコントロールで使用するために特別な安全方策を施した入力機器。 非常停止スイッチ、セーフティドアスイッチなどの総称です。
セーフティ入力機能	セーフティ入力端子に取り込まれた信号が正常か異常かを評価する機能です。 セーフティ特有の評価機能として、テストパルス評価機能、デュアルチャネル評価機能などがあります。 評価結果が異常時にはセーフティ入力データをインアクティブ（OFF）とします。

用語	説明
セーフティネットワークコントローラ	NX シリーズ通信コントロールユニットにセーフティコントロールユニットを装着したビルディングブロック型のセーフティコントローラの総称です。
セーフティネットワーク番号 (SNN)	CIP Safety 通信で、セーフティネットワークを一意に特定するための固有の番号です。
セーフティプログラム	セーフティコントローラのユーザプログラムを指します。 スタンダードコントローラのユーザプログラムと区別するための呼称です。
セーフティリアクションタイム	セーフティに関連した入力(非常停止スイッチの押下やライトカーテンの遮断、安全扉の開放など)や機器の故障が発生してから、システムがセーフティ状態に遷移するまでの最悪ケースの応答時間です。
妥当性確認	安全性確認テストにて、セーフティシステムとしての要求仕様を満足することを確認することです。セーフティアプリケーションデータにその確認情報を付加す行為を指す場合もあります。
通信コントロールユニット	セーフティ CPU ユニットと CIP Safety on EtherNet/IP デバイスが、ネットワーク上で CIP Safety 通信するためのインタフェースユニットの総称です。
テストパルスによる評価機能	接続されている外部機器の故障または配線異常を検出するために、テストパルスを出力することでセーフティ入力またはセーフティ出力を評価する機能です。
デュアルチャネル	冗長性をもたせるため、入力または出力を 2 つ（2 点）で使用することです。
デュアルチャネル評価機能	セーフティ入力端子またはセーフティ出力端子を二重化して使用し、その 2 入力または出力の整合性をチェックすることでセーフティ入力またはセーフティ出力を評価する機能です。
動作モード	本ユニットの動作の各状態のことです。動作モードに応じて、使用できる機能が異なります。
ノード ID	CIP Safety 通信で、セーフティネットワーク番号 (SNN) が同じネットワーク上のデバイスを一意に特定するための ID です。 セーフティ CPU ユニットは NX バス上で唯一の CIP Safety デバイスであり、ノード ID は「1」固定です。EtherNet/IP 上の CIP Safety デバイスの場合、ノード ID は IP アドレスになります。
ユーザ定義アプリケーション	本ユニットに対し、Type1 Safety Open でのコンフィグレーションを使用してダウンロードする、ロジックを持つ安全アプリケーションです。 ユーザ定義アプリケーションはユーザ自身が Sysmac Studio で作成します。
ユーザプログラム	ユーザが作成するプログラム全体を指します。スタンダードコントローラのスタンダードコントロール用のプログラムおよびセーフティ CPU ユニットのセーフティプログラムを指します。
リモート I/O モード	簡易ロジック演算機能を使用せず、シンプルなリモート I/O として動作するモードです。
リモート I/O モード用アプリケーション	リモート I/O モードで使用されるアプリケーションです。I/O 構成設定だけを定義する、ロジックは含みません。 本ユニットに対し、Type1 Safety Open、または Web UI を使用して設定されます。
リングスーパーバイザ	リングスーパバイザは、リングの完全性を実証する責任があります。障害から回復するためにリングを再設定し、リングの診断情報を収集します。

マニュアル改訂履歴

マニュアル改訂記号は、表表紙・裏表紙に記載されている Man.No.の後尾に付記されます。



改訂記号	改訂年月	改訂理由・改訂ページ
A	2026 年 7 月	初版
B	2026 年 7 月	電源コネクタ接続用ケーブルの追加に伴う改定

1

特長とシステム構成

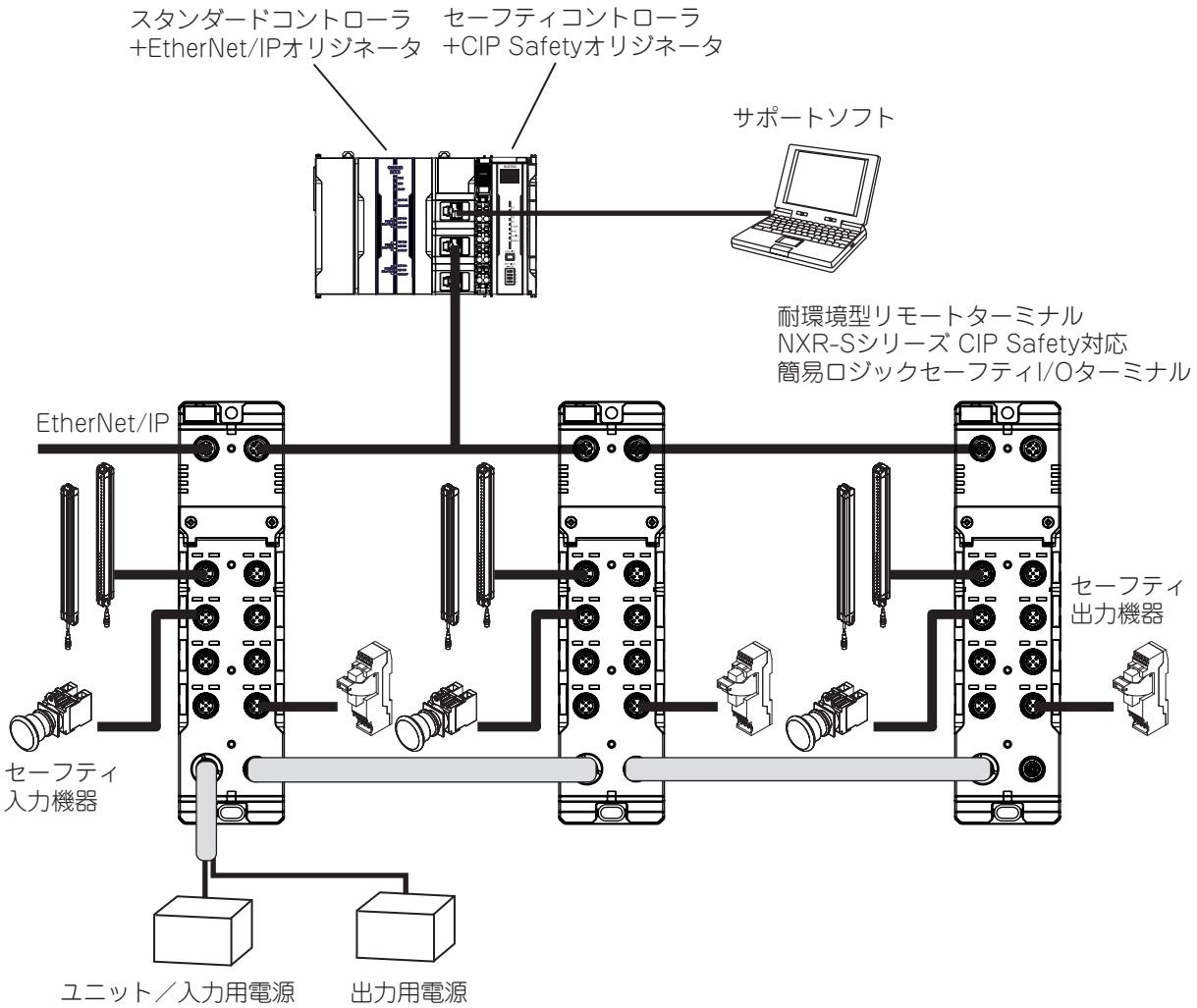
この章では、耐環境型リモートターミナル NXR-S シリーズ CIP Safety 対応 簡易ロジックセーフティ I/O ターミナルの特長とシステム構成について説明しています。

1-1　セーフティ I/O ターミナルの概要 1-2
1-2　セーフティ I/O ターミナルの特長 1-3
1-3　システム構成 1-4
1-3-1　セーフティコントロールシステム 1-4
1-3-2　ネットワークトポロジ 1-13
1-3-3　カスケード接続 1-14
1-4　サポートソフト 1-16

1-1 セーフティ I/O ターミナルの概要

耐環境型リモートターミナル NXR-S シリーズ CIP Safety 対応 簡易ロジックセーフティ I/O ターミナルは、CIP Safety ターゲット機能および IP67 準拠の高い耐環境性能を備えたセーフティ I/O デバイスです。また、簡易なロジック機能によりセーフティ出力機器を制御できます。
基本的な機能として、以下の機能をサポートしています。

- CIP Safety ターゲットとして、CIP Safety オリジネータとセーフティ通信を行う。
- EtherNet/IP ターゲットとして、EtherNet/IP オリジネータとデータ交換する。
- 非常停止用押ボタンスイッチやセーフティライトカーテンなどのセーフティデバイスとの入出力処理を行う。



1-2 セーフティ I/O ターミナルの特長

耐環境型リモートターミナル NXR-S シリーズ CIP Safety 対応 簡易ロジックセーフティ I/O ターミナルの特長を説明します。

簡易なロジック機能

セーフティ I/O ターミナルは、セーフティ出力機器を制御するためのロジック機能を搭載しています。
そのため、簡単な制御をプログラムレスで実現し、セーフティ I/O ターミナル単独で高速応答の安全制御が可能です。

IP67 準拠の耐環境性能

セーフティ I/O ターミナルは、IP67 準拠の高い耐環境性能を備えています。そのため、水がかかったり粉じんが多かったりする環境でも、制御盤の外に設置することが可能です。

各種ケーブルの簡単配線

セーフティ I/O ターミナルは、電源ケーブル、通信ケーブルを含むすべてのポートがコネクタ接続であるため、端子台接続に比べて簡単に配線できます。さらに、すべてのポートにスマートクリックコネクタを搭載しており、ワンタッチで簡単接続が可能です。

簡単なユニット交換

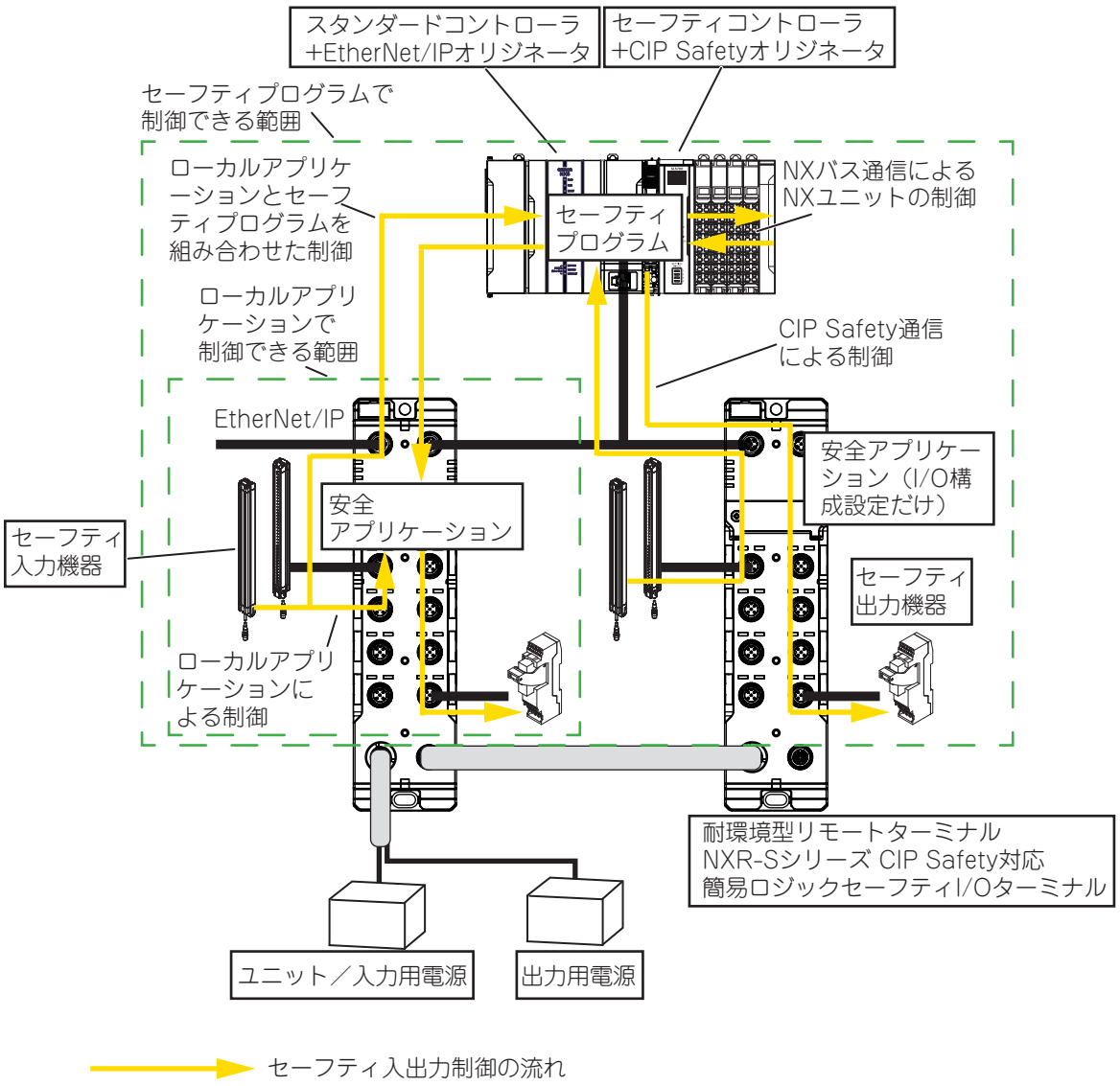
セーフティ I/O ターミナルは、Web UI を搭載しています。
Web UI を使用することで、セーフティ I/O ターミナルの I/O モニタ、トラブルシュート、およびユニット交換時に必要なバックアップ、リストアなどの作業が、専用のサポートソフトを使わずに実行できます。

1-3 システム構成

セーフティ I/O ターミナルを使用する際のシステム構成を、セーフティコントロールシステムと呼びます。ここでは、セーフティコントロールシステム、セーフティ I/O ターミナルを同一の EtherNet/IP ネットワークに接続する際のネットワークトポロジ、およびセーフティ I/O ターミナルのセーフティ入力ポートとセーフティ出力ポートを接続するカスケード接続について説明します。

1-3-1 セーフティコントロールシステム

セーフティ I/O ターミナルを用いたセーフティコントロールシステムの構成を以下に示します。



各構成機器の説明を下表に示します。

構成機器	説明
耐環境型リモートターミナル NXR-S シリーズ CIP Safety 対応 簡易ロジックセーフティ I/O ターミナル形 NXR-SXD□□□□-CST	本製品 CIP Safety オリジネータと、セーフティデータの交換を行う機器。CIP Safety オリジネータから受け取ったデータをセーフティ出力機器へ出力したり、セーフティ入力機器からの入力信号を CIP Safety オリジネータへ送信したりする。 また、簡易なロジック機能により、セーフティ出力機器を調節制御することもできる。
スタンダードコントローラ + EtherNet/IP オリジネータ	セーフティ I/O ターミナルの標準制御を行う。また EtherNet/IP 通信を行い、セーフティ I/O ターミナルの動作状況をモニタリングするのに使用する。 オムロン製品では、形 NX502 CPU ユニット、形 NX102 CPU ユニット。 また、オムロン製品の EtherNet/IP オリジネータとしては、形 NX-CSG320 がある。
セーフティコントローラ+ CIP Safety オリジネータ	セーフティ I/O ターミナルと CIP Safety 通信を行い、セーフティプログラムでセーフティ機能の制御を行う。 オムロン製品では、形 NX-SL5□□□。
セーフティプログラム	セーフティコントローラで動作する安全制御用のユーザプログラムのこと。 NX バス通信、CIP Safety 通信などの通信により、セーフティコントロールシステム全体を制御する。
ローカルアプリケーション	セーフティコントローラではなく、リモート機器上で実行されるアプリケーションのこと。 本製品ではこれを安全アプリケーションと呼び、安全入出力診断機能やロジック機能によって実現される。 セーフティ I/O ターミナルの安全アプリケーションは、I/O 構成設定だけを含むものと、ロジック設定と I/O 構成設定の両方を含むものの 2 種類に分類される。 I/O 構成設定だけを持つ安全アプリケーションは、セーフティ I/O ターミナルをシンプルなリモート I/O として使用するためのものであり、安全制御はセーフティコントローラのセーフティプログラムによって実行される。 一方、ロジック設定と I/O 構成設定の両方を持つ安全アプリケーションでは、セーフティコントローラを介さずに、セーフティ I/O ターミナル内でのローカル制御が可能であるため、高速な応答が求められる用途に適している。またセーフティコントローラから送信されるセーフティ出力データと安全アプリケーションのロジック設定を組み合わせて制御を行うことも可能である。
ユニット／入力用電源	セーフティ I/O ターミナルの動作やセーフティ入力機器とのインタフェースで使用する電源。電源コネクタ IN に外部供給電源を接続して供給する。
出力用電源	セーフティ出力機器とのインタフェースで使用する電源。電源コネクタ IN に外部供給電源を接続して供給する。
セーフティ入力機器	セーフティコントロールで使用するために特別な安全方策を施した入力機器。 非常停止スイッチ、セーフティドアスイッチなどの総称。
セーフティ出力機器	セーフティコントロールで使用するために特別な安全方策を施した出力機器。 安全リレーなどの総称。

セーフティコントロールシステムを細分化すると、使用するアプリケーションやプログラムによって、以下の 4 種類があります。特徴に応じて使い分けてください。

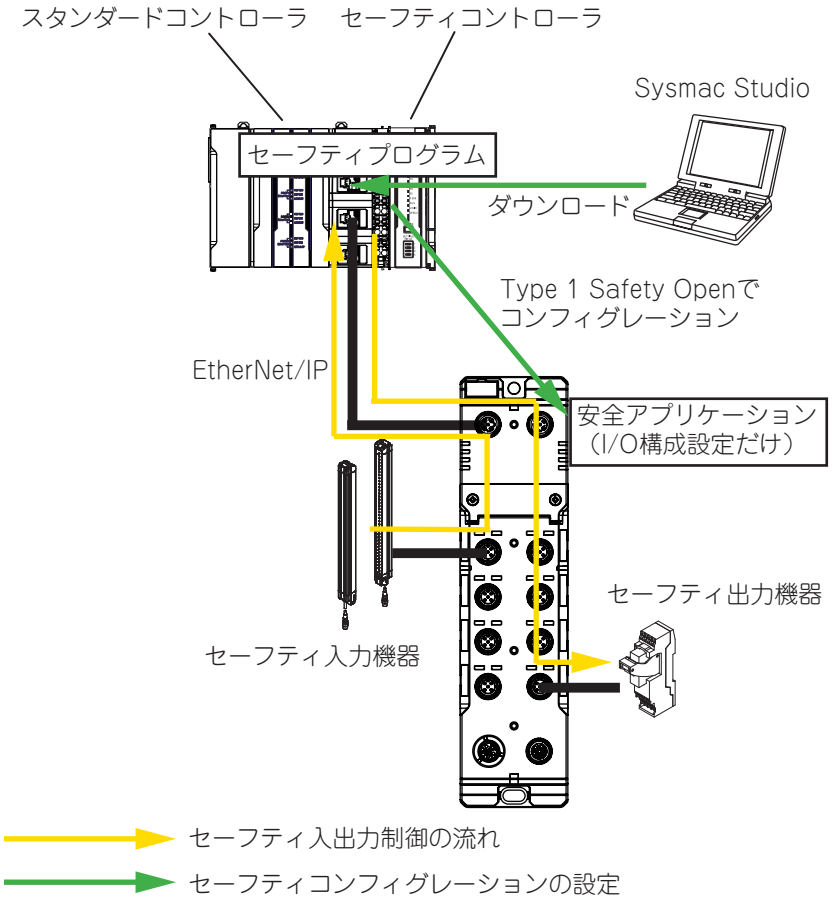
セーフティコントロールシステムの構成	使用する安全アプリケーション	特徴	安全アプリケーションの設定と変更方法	選択基準
セーフティコントローラが制御する構成	リモート I/O モード用アプリケーション	• セーフティコントローラが、ネットワークを介してセーフティ出力機器を制御する。 • ネットワーク通信により複雑で大規模なシステムが構築可能。 • 応答時間が長くなる場合がある。	• I/O 構成設定だけの安全アプリケーションを設計し、セーフティコントローラにダウンロードする。この場合、セーフティコントローラは、ダウンロードされた安全アプリケーションに基づいて、セーフティ I/O ターミナルをコンフィグレーションする（Type 1 Safety Open によるコンフィグレーション）。 • 代替として、ユーザが設計した I/O 構成設定だけの安全アプリケーションをセーフティ I/O ターミナルにダウンロードする（Web UI によるコンフィグレーション）。	• セーフティ I/O ターミナルのロジック機能では実現が難しい、複雑で大規模なシステムを構築したい。 • セーフティコントローラでセーフティプログラムを使用する。
プリセットされた安全アプリケーションで、セーフティ I/O ターミナルが制御する構成	固定アプリケーション	• セーフティ I/O ターミナルが、セーフティ出力機器を制御する。 • 簡易なロジックによる小規模制御のシステム。 • 高速な応答が可能。	• セーフティ I/O ターミナルにプリセットされた安全アプリケーション（固定アプリケーション）を使用する。	• 固定アプリケーションの中に、そのまま使用できるアプリケーションがある。

セーフティコントロールシステムの構成	使用する安全アプリケーション	特徴	安全アプリケーションの設定と変更方法	選択基準
ユーザが設計した安全アプリケーションで、セーフティ I/O ターミナルが制御する構成（集中管理型）	ユーザ定義アプリケーション	• セーフティ I/O ターミナルが、セーフティ出力機器を制御する。 • ユーザがロジックを設計するので、プリセットされた安全アプリケーションよりも自由度の高い制御が可能。以下のようなシステムが構築できる。 a）セーフティプログラムによるネットワークを介した制御と、安全アプリケーションによるローカルで高速応答の制御を組み合わせた制御。 b）ユーザが設計した安全アプリケーションによるローカル制御。 c）セーフティ I/O ターミナルをカスケード接続して制御点数を拡大した制御。	• ロジック設定と I/O 構成設定を含む安全アプリケーション（ユーザ定義アプリケーション）を設計し、セーフティコントローラにダウンロードする。 • セーフティコントローラは、ダウンロードされた安全アプリケーションに基づいて、セーフティ I/O ターミナルをコンフィグレーションする（Type 1 Safety Open によるコンフィグレーション）。	• 簡単な処理のため、セーフティ I/O ターミナルのロジック機能で実現可能なアプリケーションである。 • 固定アプリケーションの中に、そのまま使用できるものがない。 • 複数のセーフティ I/O ターミナルに同じ処理をさせるため、セーフティコントローラ側で安全アプリケーションを管理したい。
ユーザが設計した安全アプリケーションで、セーフティ I/O ターミナルが制御する構成（分散管理型）	アドオンアプリケーション		• ロジック設定と I/O 構成設定を含む安全アプリケーション（アドオンアプリケーション）を設計し、セーフティ I/O ターミナルにダウンロードする（Web UI によるコンフィグレーション）。 • アドオンアプリケーションは、セーフティ I/O ターミナルに最大 5 種類まで保存でき、その中から使用する安全アプリケーションを選択する。	• 簡単な処理のため、セーフティ I/O ターミナルのロジック機能で実現可能なアプリケーションである。 • 固定アプリケーションの中に、そのまま使用できるものがない。 • セーフティ I/O ターミナルを単体で使用するため、セーフティ I/O ターミナル側で安全アプリケーションを管理したい。

以下に、それぞれのセーフティコントロールシステムの構成例と動作の詳細を示します。

セーフティコントローラが制御する構成（Type 1 Safety Open によるコンフィグレーション）

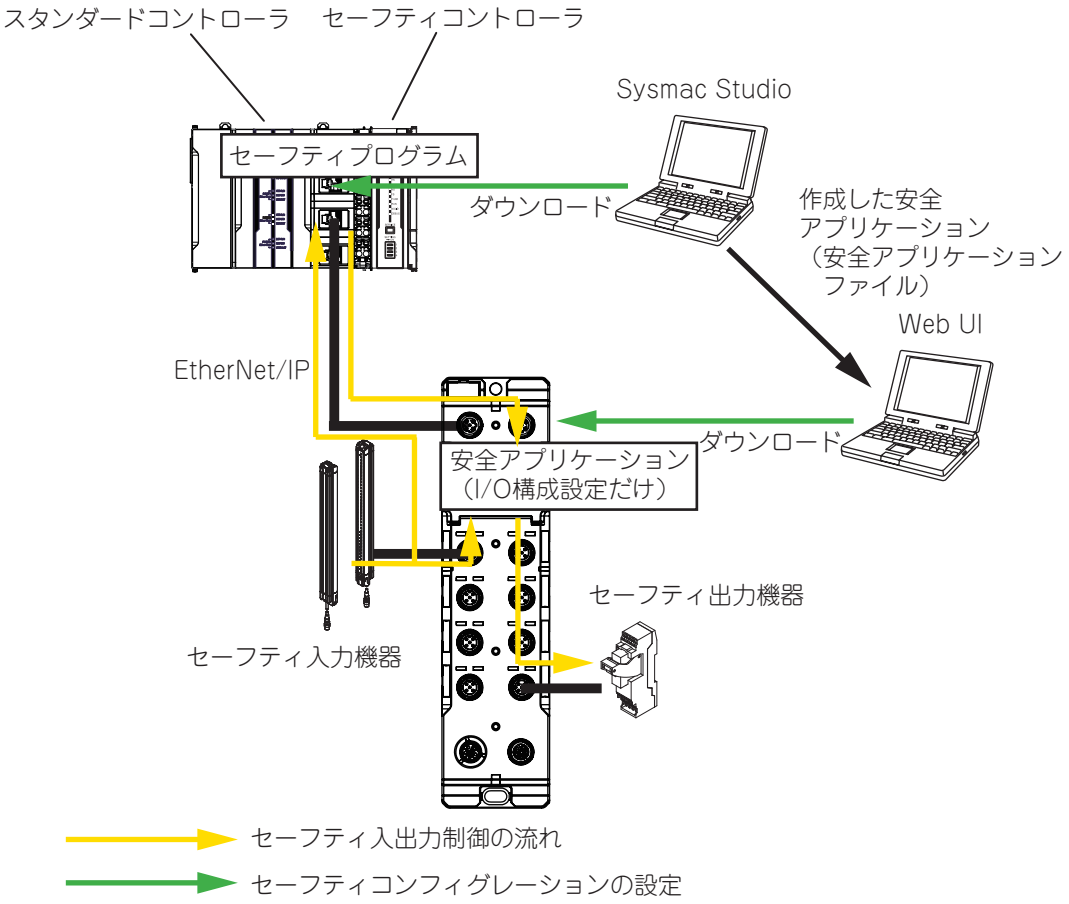
セーフティコントローラが制御する構成（Type 1 Safety Open によるコンフィグレーション）の図を以下に示します。



- セーフティコントローラのセーフティプログラムで制御します。
- セーフティ I/O ターミナルには I/O 構成設定だけの安全アプリケーションを使用します。ロジック機能は使用しません。
- 安全アプリケーションはセーフティプログラムとともにセーフティコントローラ内に保持され、コネクション開設時にセーフティ I/O ターミナルに転送されます。
- セーフティ I/O ターミナルのロータリスイッチの SETTING SW1、SW2 の、両方を「0」に設定します。

セーフティコントローラが制御する構成（Web UI によるコンフィグレーション）

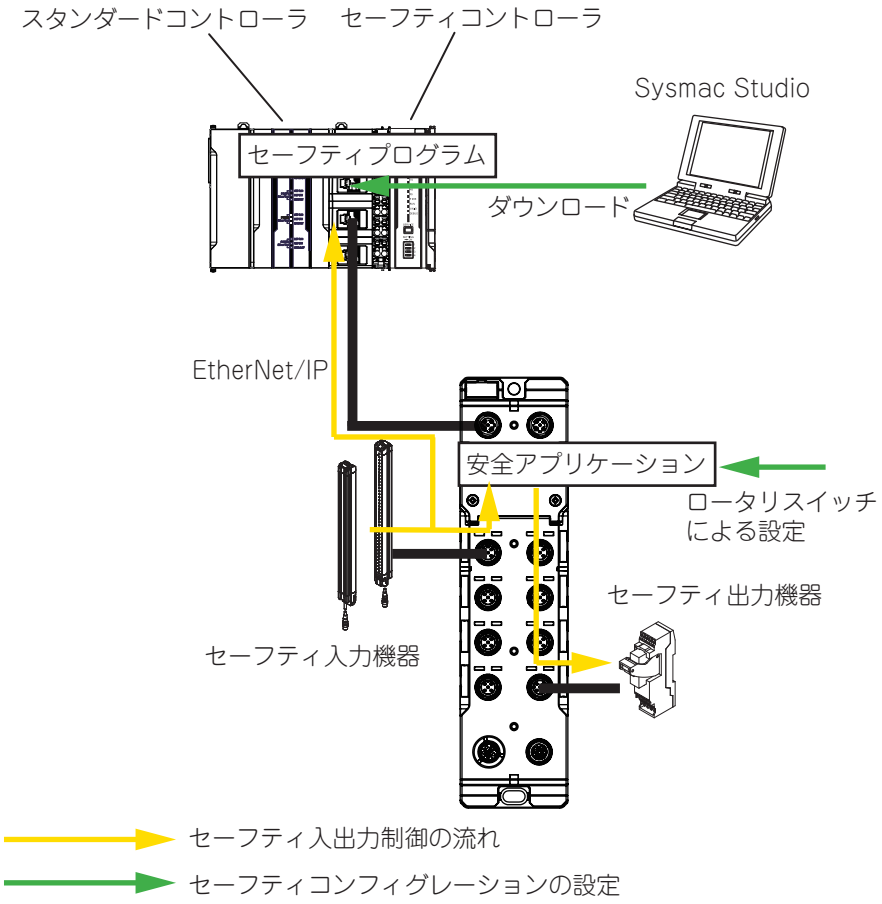
セーフティコントローラが制御する構成（Web UI によるコンフィグレーション）の図を以下に示します。



- セーフティコントローラのセーフティプログラムで制御します。
- セーフティコントローラは、セーフティ I/O ターミナルに対して Type 2a Safety Open でコネクションを開設します。
- セーフティ I/O ターミナルには I/O 構成設定だけの安全アプリケーションを使用します。ロジック機能は使用しません。
- セーフティプログラムは、セーフティコントローラ内に保持されます。安全アプリケーションは Sysmac Studio で作成し、Web UI を使用してセーフティ I/O ターミナルにダウンロードします。
- セーフティ I/O ターミナルのロータリスイッチの SETTING SW1、SW2 の、両方を「0」に設定します。

プリセットされた安全アプリケーションでセーフティ I/O ターミナルが制御する構成

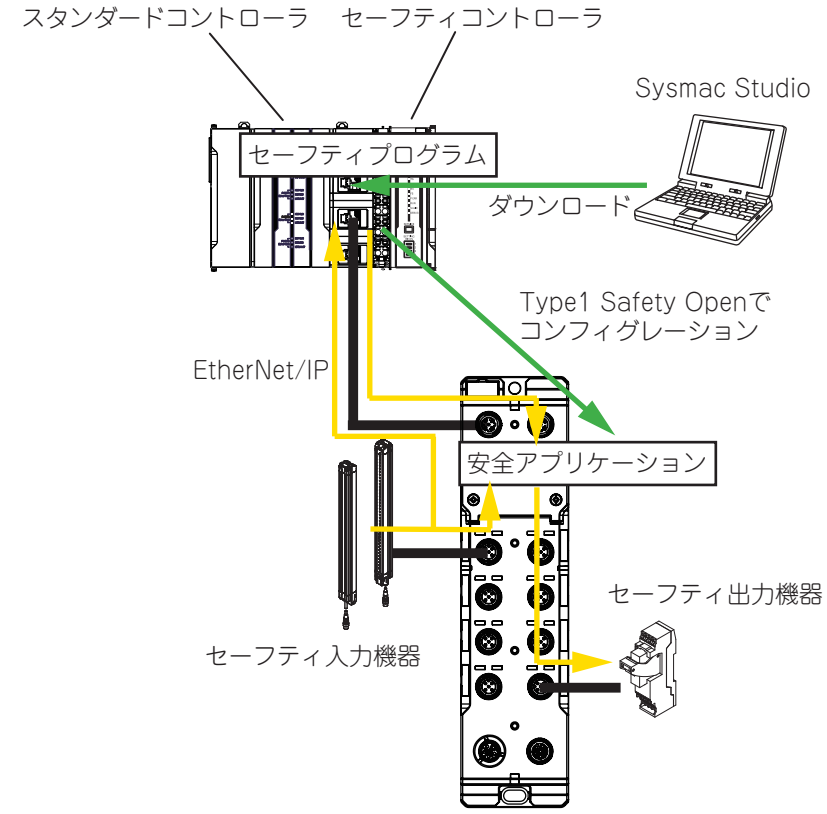
プリセットされた安全アプリケーションでセーフティ I/O ターミナルが制御する構成の図を以下に示します。



- セーフティ I/O ターミナルにプリセットされた安全アプリケーションを使用します。安全アプリケーションにはロジック設定と I/O 構成設定が含まれます。
- セーフティコントローラのセーフティプログラムで、セーフティ I/O ターミナルの入出力データのモニタを行うことも可能です。
- 安全アプリケーションは、セーフティ I/O ターミナル内に保持されています。
- セーフティ I/O ターミナルのロータリスイッチの SETTING SW1、SW2 の、両方を使用する安全アプリケーション（固定アプリケーション）の番号「1-3」に設定します。

ユーザが設計した安全アプリケーションでセーフティ I/O ターミナルが制御する構成（集中管理型）

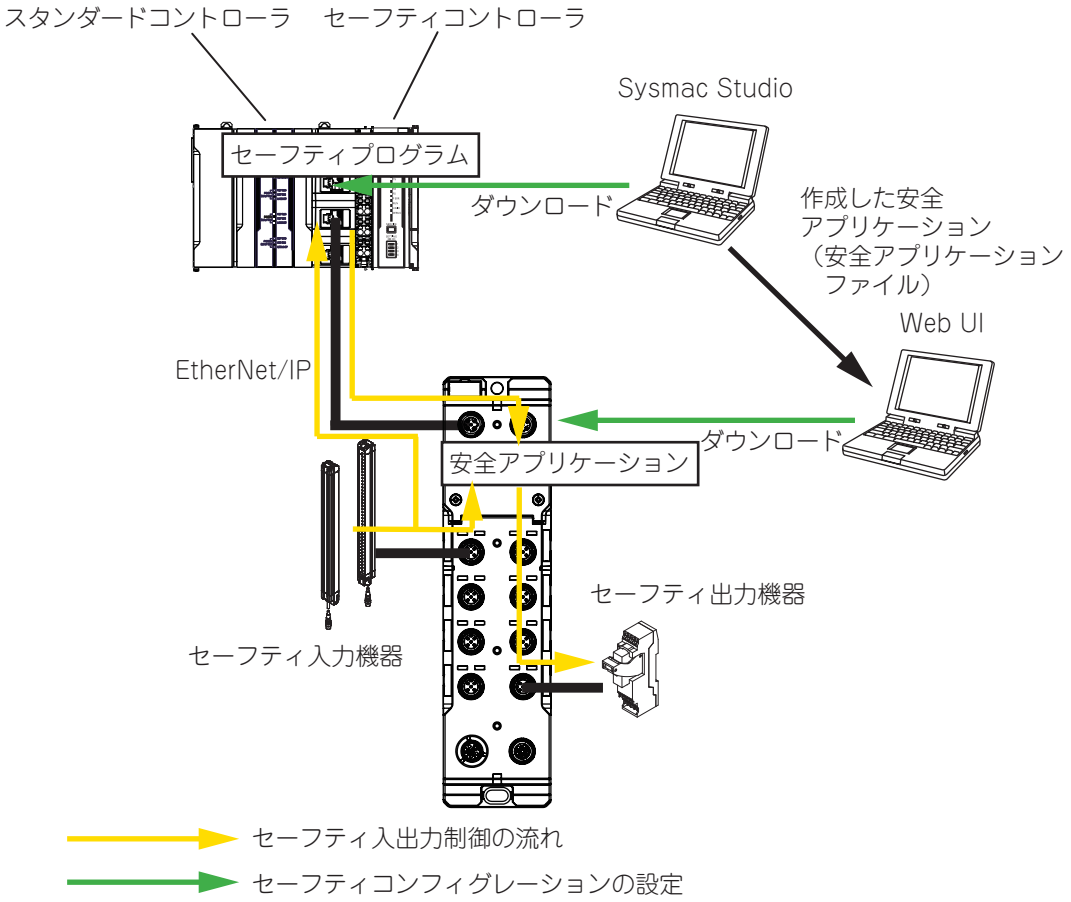
ユーザが設計した安全アプリケーションでセーフティ I/O ターミナルが制御する構成（集中管理型）の図を以下に示します。



- セーフティ I/O ターミナルの安全アプリケーションを使用して制御します。安全アプリケーションにはロジック設定と I/O 構成設定が含まれます。
- セーフティコントローラのセーフティプログラムと組み合わせた制御も可能です。
- 安全アプリケーションはセーフティプログラムとともにセーフティコントローラ内に保持され、コネクション開設時にセーフティ I/O ターミナルに転送されます。
- セーフティ I/O ターミナルのロータリスイッチの SETTING SW1、SW2 の、両方を「F」（ユーザ定義アプリケーション）に設定します。

ユーザが設計した安全アプリケーションでセーフティ I/O ターミナルが制御する構成（分散管理型）

ユーザが設計した安全アプリケーションでセーフティ I/O ターミナルが制御する構成（分散管理型）の図を以下に示します。



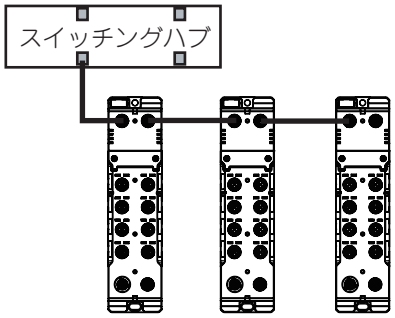
- セーフティコントローラは、セーフティ I/O ターミナルに対して Type 2a Safety Open でコネクションを開設します。
- セーフティ I/O ターミナルの安全アプリケーションを使用して制御します。安全アプリケーションにはロジック設定と I/O 構成設定が含まれます。
- セーフティコントローラのセーフティプログラムと組み合わせた制御も可能です。
- セーフティプログラムは、セーフティコントローラ内に保持されます。安全アプリケーションは Sysmac Studio で作成し、Web UI を使用してセーフティ I/O ターミナルにダウンロードします。
- セーフティ I/O ターミナルのロータリスイッチの SETTING SW1、SW2 の、両方を使用する安全アプリケーション（アドオンアプリケーション）の番号「9-D」に設定します。

1-3-2 ネットワークトポロジ

セーフティ I/O ターミナルでは、ユニットに通信ポートが 2 個あるため、EtherNet/IP ネットワークのライン型、スター型、ツリー型、およびリング型の各種トポロジが構築できます。

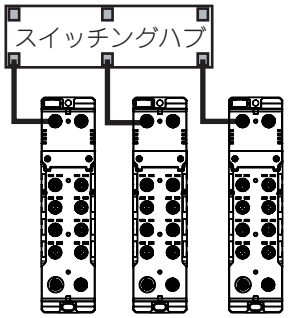
● ライン型

ライン型は、セーフティ I/O ターミナルどうしを接続して構築するトポロジです。



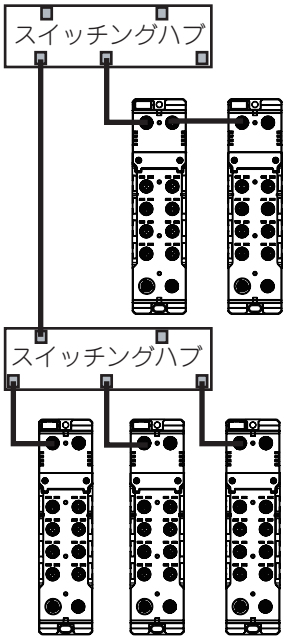
● スター型

スター型は、スイッチングハブに複数のセーフティ I/O ターミナルを接続して構築するトポロジです。



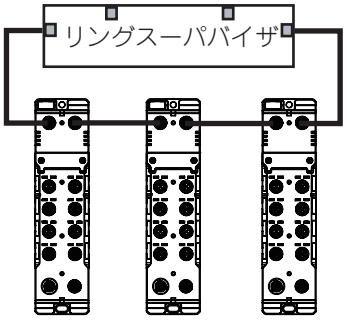
● ツリー型

ツリー型は、スター型とライン型を組み合わせて構築するトポロジです。



● **リング型**

リング型は、リングスーパバイザとセーフティ I/O ターミナルを組み合わせて構築するリング形状のトポロジです。リング型は、Device Level Ring(DLR)機能を使用するため、通信ケーブルが 1 か所断線しても正常な通信を維持できる特長があります。DLR 機能についての詳細は、「8-4 Device Level Ring(DLR)機能 (P.8-10)」を参照してください。



1-3-3 カスケード接続

形 NXR-SXD1204-CST の場合、複数のユニットのセーフティ入力ポートとセーフティ出力ポートをカスケード接続することが可能です。
この構成には、以下のメリットがあります。

- CIP Safety 通信の通信時間の影響を受けないため、複雑なロジックが実現できる。
- セーフティ入力端子、およびセーフティ出力端子の数を増やすことができる。

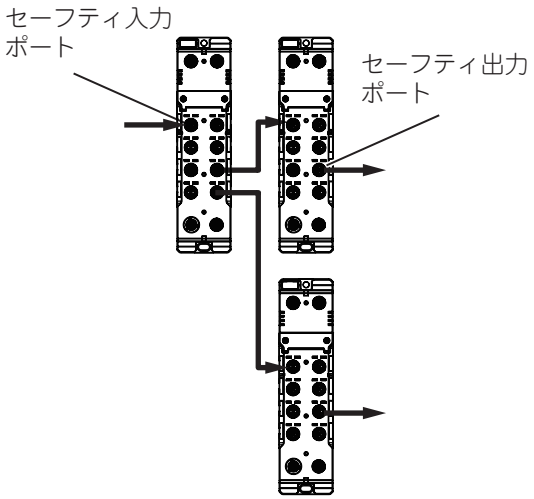
セーフティ入力機能とセーフティ出力機能の I/O 構成設定はデュアルチャネルにしてください。

使用上の注意

カスケード接続を行う場合は、安全応答性能を確認してください。安全応答性能の詳細は、「第 9 章 安全応答性能 (P.9-1)」を参照してください。

下図のように、1 段のカスケード接続をサポートしており、最大 3 台の接続が可能です。

カスケード接続では、すべてのユニットで CIP Safety オリジネータとの CIP Safety 通信が可能です。



1-4 サポートソフト

セーフティ I/O ターミナルで使用可能なサポートソフトを、以下に示します。

設定対象	形式	サポートソフト
セーフティ I/O ターミナル	• 形 NXR-SXD1204-CST • 形 NXR-SXD1204B-CST	• Sysmac Studio　Ver.1.67 以降

使用上の注意

Sysmac Studio による設定は、NJ/NX シリーズ CPU ユニット、NY シリーズ産業用パネル PC／産業用ボックス PC、または通信コントロールユニット 形 NX-CSG320 を介して行ってください。その際の接続方法は、Ethernet 直接接続、または Ethernet HUB 接続を使用します。

2

仕様と使用手順

この章では、セーフティ I/O ターミナルの仕様と使用手順について説明しています。

2-1 仕様 2-2
2-1-1 一般仕様 2-2
2-1-2 通信仕様 2-3
2-1-3 安全仕様 2-4
2-1-4 ユニット仕様 2-6
2-2 使用手順 2-8
2-2-1 STEP1 システム設計 2-8
2-2-2 STEP2 ソフト設計 2-8
2-2-3 STEP3 ハード設計 2-9
2-2-4 STEP4 安全応答性能の計算と検証 2-9
2-2-5 STEP5 ソフトウェア設定とプログラミング 2-10
2-2-6 STEP6 取り付けと配線 2-10
2-2-7 STEP7 動作確認 2-11
2-2-8 STEP8 運転と保守点検 2-11

2-1 仕様

ここでは、セーフティ I/O ターミナルについて、以下の仕様を説明します。

- 一般仕様
- 通信仕様
- ユニット仕様
- 安全仕様

2-1-1 一般仕様

セーフティ I/O ターミナルの一般仕様は、以下のとおりです。

項目		仕様
保護構造		IP67
使用環境	**使用周囲温度**	-10～+55°C
	使用周囲湿度	25～85%（結露のないこと）
	使用周囲雰囲気	腐食性ガスのないこと
	保存温度	-25～+65°C
	保存湿度	25～85%（結露のないこと）
	使用標高	2000m 以下
	汚染度	汚染度 3 以下: IEC 61010-2-201 に該当
	耐ノイズ性	IEC 61131-2 (Zone B) および EN 61131-2 (Zone B)に準拠 IEC 61326-3-1 および EN 61326-3-1 に準拠
	オーバーボルテージカテゴリ	カテゴリⅡ: IEC 61010-2-201 に該当
	EMC イミュニティレベル	ゾーン B
	耐振動	IEC 60068-2-6 に準拠 5～8.4Hz 振幅 3.5mm、8.4～150Hz 10m/s^2 X、Y、Z 各方向 100 分 その他 10～60Hz 振幅 0.35mm、60～150Hz 50m/s^2 X、Y、Z 各方向 80 分
	耐衝撃	IEC 60068-2-27 に準拠 150m/s^2　3 軸 6 方向各 3 回
	耐電圧	AC600V（絶縁されている回路間）
	絶縁抵抗	20MΩ 以上（絶縁されている回路間）

項目		仕様
規格適合	TÜV ラインランド	• EN 61508 parts 1-3 • EN ISO 13849-1 • EN ISO 13849-2 • EN IEC 61131-2 • IEC 61326-3-1 • EN 60529 • EN 61131-6
	UL	• NRAQ/NRAQ7 • UL 61010-1、および UL 61010-2-201 • CSA C22.2 No.61010-1、および CSA C22.2 No.61010-2-201 • FSPC （IEC 61508 parts 1-3 および ISO 13849-1）
	ODVA	• CIP Safety on EtherNet/IP • EtherNet/IP
	その他	• EU: EN61131-2, RCM • UKCA • KC: 韓国電波法登録 • 機械指令

（注）最新の適合規格については、当社ホームページ（www.fa.omron.co.jp または www.ia.omron.com）、または当社営業担当者に確認してください。

2-1-2 通信仕様

セーフティ I/O ターミナルの通信仕様は、以下のとおりです。

項目		仕様
物理仕様	ポート	レイヤ 2 スイッチポート
	物理層	10BASE-T/100BASE-TX Auto Negotiation／固定設定
	媒体アクセス方式	CSMA/CD
	変調方式	ベースバンド
	トポロジ	ライン型、スター型、ツリー型、リング型
	伝送速度	100Mbps(100BASE-TX)
	伝送媒体	カテゴリ 5 以上ツイストペアケーブル（推奨ケーブル: アルミテープと編組の二重遮へいシールドケーブル）
	伝送距離	100m 以内（ノードとノード間、ハブとノード間）
	ライン接続可能台数	50 台
CIP Safety	CIP Safety ターゲット	可能
	最大コネクション数	5(Input 2/Output 3) Input コネクションは Multicast 通信を使うことで同じデータを最大 8 台までの CIP Safety オリジネータと共用できる。
	パケットインターバル	5 - 500ms
	最大データサイズ	Input: 9 バイト Output: 3 バイト

項目		仕様
EtherNet/IP 通信	**EtherNet/IP ターゲット**	可能(Exclusive Owner、 Input Only、 Listen Only)
	最大コネクション数	2(Input 2/Output 0) Input コネクションは Multicast 通信を使うことで同じデータを EtherNet/IP オリジネータと共用できる。
	パケットインターバル	5 - 10000ms
	最大データサイズ	Input: 9 バイト
	DLR	リングノードに対応
	EtherNet/IP コンフォーマンステスト	CT21 準拠
CIP メッセージ通信	**プロトコル**	Class3/UCMM
	最大コネクション数(Class3)	5
	データサイズ	504 バイト
HTTPS 通信	**TLS バージョン**	TLS 1.2 に対応 TLS 1.0、TLS 1.1、SSL には非対応
	認証方式	サーバ認証(X.509)、およびセーフティパスワードによるセッション認証

各外部インタフェースで使用するポート番号、通信路暗号化機能の有無、デフォルトでの有効／無効、および有効無効切り替えの可否は、以下のとおりです。

外部インタフェース		ポート番号	通信路暗号化	デフォルトでの有効／無効	有効無効切り替えの可否
Ethernet ポート	**CIP Safety**	UDP/2222	なし	有効	不可
	HTTPS	TCP/443	あり	有効	不可
	SNTP	UDP/123	なし	無効	Sysmac Studio、Web UI、および CIP メッセージにより可
	DHCP	UDP/68	なし	無効	Sysmac Studio、Web UI、および CIP メッセージにより可
	EtherNet/IP	UDP/2222	なし	有効	不可
	CIP メッセージ	TCP/44818、UDP/44818	なし	有効	不可
ロータリスイッチ		対象外	対象外	有効	不可

2-1-3 安全仕様

セーフティ I/O ターミナルの安全仕様は、以下のとおりです。

項目	仕様			
	セーフティ入力		セーフティ出力	
	デュアルチャネル	シングルチャネル	デュアルチャネル	シングルチャネル
PL	Up to PL e	Up to PL d***1**	Up to PL e	Up to PL c***2**
Category	Up to Cat.4	Up to Cat.2***1**	Up to Cat.4	Up to Cat.2***2**
$MTTF_D$	1428 年	100 年	1431 年	100 年
Mission Time	20 年	20 年	20 年	20 年
DCavg	98.61%	98.60%	98.60%	98.60%
SIL	Up to SIL 3	Up to SIL 2	Up to SIL 3	Up to SIL 1
PFH	4.6×10^{-10} 1/h	4.6×10^{-10} 1/h	4.6×10^{-10} 1/h	4.6×10^{-10} 1/h

***1.** シングルチャネルのセーフティ入力で Cat.2/PLd を達成するために、セーフティコントロールシステムには、以下を満たすセーフティ出力機能を持たせてください。
- 故障発生時に、セーフティコントロールシステムが安全状態に移行できる。
- 故障発生時に、故障原因がクリアされるまでセーフティコントロールシステムが安全状態を維持できる。

***2.** シングルチャネルのセーフティ出力で Cat.2/PLc を達成するために、CIP Safety 通信、または EtherNet/IP 通信を使用して、セーフティ I/O ターミナルの出力端子を監視し、セーフティコントロールシステムとして、セーフティ出力の故障を検出してください。
セーフティ出力の故障を検出したら、表示灯や表示器などでユーザに異常発生を通知してください。
出力端子ステータス監視の対象は、Input アセンブリの、以下の 4 種類のビットのいずれかとします。

アセンブリ	監視対象ビット	ビット名
Safety Input 1	出力端子ステータス（集約）	Combined Safety Output Status
Safety Input 2	出力端子ステータス（集約）	Combined Safety Output Status
Safety Input 3	出力端子ステータス（集約）	Combined Safety Output Status
	出力端子ステータス（個別）	Safety Output0 Status ～ Safety Output3 Status

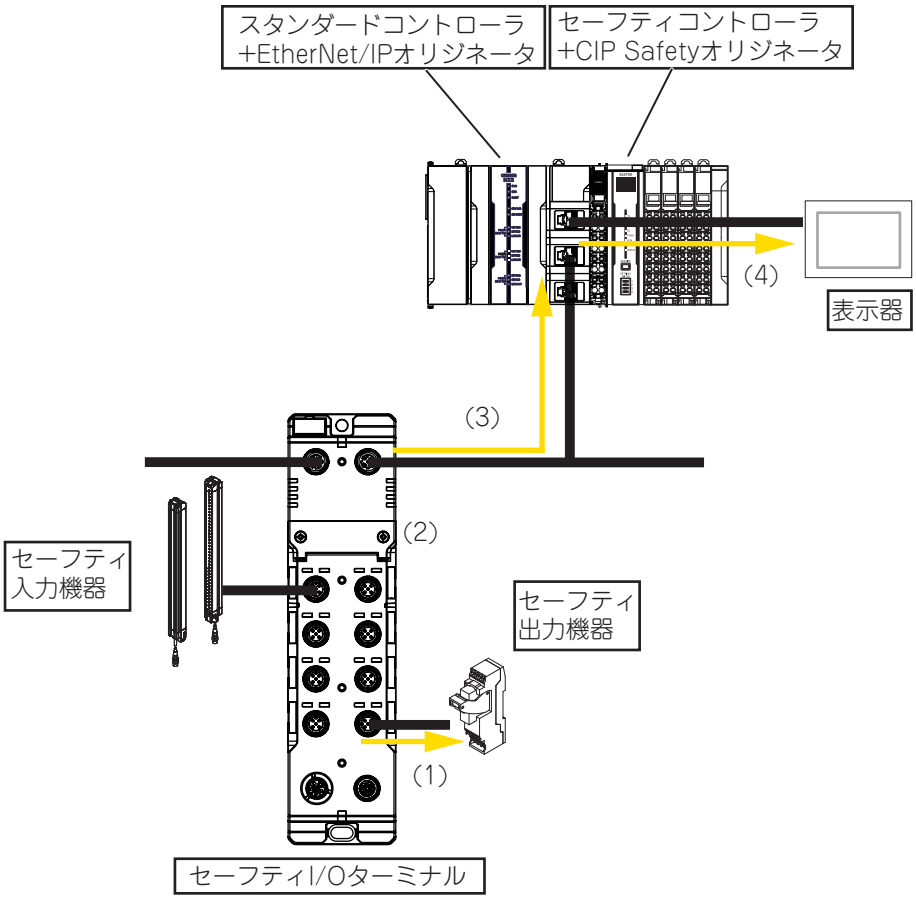
セーフティ出力端子で異常が発生してから、ユーザに異常発生を通知するまでの手順は、以下のとおりです。

(1) セーフティ出力端子で異常が発生する。

(2) セーフティ I/O ターミナルが、セーフティ出力端子の異常を検出し、異常が発生したセーフティ出力端子を Inactive にする。さらに、対象の出力端子ステータスのビットを FALSE にする。

(3) セーフティコントローラまたはスタンダードコントローラが、セーフティ I/O ターミナルの出力端子ステータスが FALSE になったことを検出する。

(4) セーフティコントローラまたはスタンダードコントローラが、表示灯や表示器などでユーザに異常発生を通知する。



さらにセーフティコントロールシステムを安全状態に移行させる場合は、通知された異常内容に基づいて、セーフティ I/O ターミナル以外の遮断装置を使用してセーフティ出力機器の電源を遮断してください。セーフティ出力機器の電源を遮断するまでの時間は、（セーフティ I/O ターミナルが異常の発生を通知するまでの時間：265ms）、（ネットワーク応答時間）、および（セーフティ I/O ターミナル以外の遮断装置の応答時間）の合計として算出してください。
監視対象ビットが出力端子ステータス（集約）の場合は、セーフティ I/O ターミナルが制御しているすべてのセーフティ出力機器の電源を遮断してください。監視対象ビットが出力端子ステータス（個別）の場合は、異常が発生したセーフティ出力機器の電源を遮断してください。

2-1-4 ユニット仕様

セーフティ I/O ターミナルのユニット仕様は、以下のとおりです。

項目		仕様	
		形 NXR-SXD1204-CST	形 NXR-SXD1204B-CST
ユニット名称		耐環境型リモートターミナル NXR-S シリーズ CIP Safety 対応 簡易ロジック セーフティ I/O ターミナル	
外形寸法		60(W)×240(H)×34.2(D)[mm] (60(W)×240(H)×46.65(D)[mm]：コネクタを含む場合)	
取り付け方法		M5 ねじでの取り付け	
取り付け強度		100N	
取り付け方向と制限		取り付け方向: 6 方向 制限: なし	
コネクタ種類		• EtherNet/IP 通信コネクタ: M12（D-coding、メス） • 電源コネクタ: M12（L-coding、メス）、M12（L-coding、オス） • I/O コネクタ: M12（A-coding、メス）	
コネクタ強度		30N すべてのコネクタが対象	
ねじの締め付けトルク		• EtherNet/IP 通信コネクタと I/O コネクタ（M12 ねじ）: 0.5～0.6N·m*1 • 電源コネクタ（M12 ねじ）: 0.39～0.49N·m*1 • ユニット取り付け（M5 ねじ）: 1.47～1.96N·m • ロータリスイッチ用カバー（M3 ねじ）: 0.4～0.6N·m	
質量		710g	700g
ユニット／入力用電源電圧		DC24V（DC19.2～28.8V）	
出力用電源電圧		DC24V（DC19.2～28.8V）	
絶縁方式		デジタルアイソレータ絶縁	
ユニット内部の絶縁		ユニット／入力用電源、出力用電源間を絶縁	
絶縁抵抗		絶縁されている回路間 20MΩ 以上 （DC100V にて）	
電源最大電流		9A	
消費電流		• ユニット／入力用電源: 220mA • 出力用電源: 40mA	
セーフティ I/O 端子数	セーフティ入力端子数	12	
	テスト出力端子数	12	
	セーフティ出力端子数	4	
I/O ポート数	セーフティ入力ポート	5pin × 6 ポート	5pin × 4 ポート
	セーフティ出力ポート	4pin × 2 ポート	0
	セーフティ入出力ポート	0	8pin × 2 ポート
I/O ポートごとの端子数	セーフティ入力ポート	• セーフティ入力 : 2 • テスト出力 : 2 • ユニット／入力用電源ー : 1	
	セーフティ出力ポート	• セーフティ出力 : 2 • 出力用電源ー : 2	ー

項目		仕様	
		形 NXR-SXD1204-CST	形 NXR-SXD1204B-CST
	セーフティ入出力ポート	ー	• セーフティ入力 : 2 • テスト出力 : 2 • セーフティ出力 : 2 • ユニット／入力用電源ー : 1 • 出力用電源ー : 1
セーフティ入力電流		4.5mA TYP.	
セーフティ入力 ON 電圧		DC11V 以上	
セーフティ入力 OFF 電圧／OFF 電流		DC5V 以下／1mA 以下	
テスト出力タイプ		ソース出力（PNP 対応）	
テスト出力定格電流		0.7A／点	
テスト出力 ON 残電圧		1.2V 以下（ユニット／入力用電源+と各出力端子）	
テスト出力漏れ電流		0.1mA 以下	
セーフティ出力 内部 I/O コモン線処理		PNP （ソース出力）	
セーフティ出力 最大負荷電流		2.0A／点、 9.0A／ユニット	0.7A／点、 9.0A／ユニット
セーフティ出力 ON 残電圧		1.2V 以下（出力用電源+と各出力端子間）	
セーフティ出力 OFF 残電圧		2V 以下（出力用電源-と各出力端子間）	
安全アプリケーション機能	ロジックなし	リモート I/O モード用アプリケーション	
	ロジックあり	固定アプリケーション、ユーザ定義アプリケーション、アドオンアプリケーション	

***1.** ねじ式コネクタの場合の値です。スマートクリックコネクタの場合は、トルク管理は不要です。コネクタを奥まで差し込み、約 1/8 回転させてください。

2-2 使用手順

ここでは、セーフティ I/O ターミナルの使用手順を説明します。

2-2-1 STEP1 システム設計

手順	内容	参照
STEP1-1 リスクアセスメント実施による安全方策の決定	• 危険源を同定し、リスクのアセスメント（見積もり、評価）を実施する。 • リスクを低減させるための方策を検討し、決定する。	−
↓		
STEP1-2 セーフティ機器の選定	セーフティ I/O ターミナルを使用するかどうかを決定する。 また、使用する形式を決定する。	「2-1 仕様 (P.2-2)」
↓		
STEP1-3 ネットワーク機器の選定	通信トポロジなどの通信仕様を確認し、Ethernet ネットワーク構成を決定する。	「1-3 システム構成 (P.1-4)」
	セーフティ I/O ターミナルの仕様に適合したスイッチングハブ、ツイストペアケーブル、および通信コネクタを選定する。	「5-5 接続関連機器 (P.5-26)」
↓		
STEP1-4 セーフティコントローラとセーフティ I/O ターミナル間のインタフェース設計	セーフティコントローラとセーフティ I/O ターミナル間のインタフェースを設計する。	「7-3 CIP Safety 通信の設定 (P.7-25)」
↓		
STEP1-5 スタンダードコントローラとセーフティ I/O ターミナル間のインタフェース設計	スタンダードコントローラとセーフティ I/O ターミナル間のインタフェースを設計する。	「7-4 EtherNet/IP 通信の設定 (P.7-36)」
↓		
STEP1-6 装置のセキュリティ設計	セキュリティガイドラインに従って、装置や設備のセキュリティ設定を行う。	「第 10 章 セキュリティガイドライン (P.10-1)」

2-2-2 STEP2 ソフト設計

手順	内容	参照
STEP2-1 入出力機器と処理の設計	セーフティ I/O ターミナルの以下の項目を設計する。 • 接続するセーフティ入出力機器 • 接続するスタンダード入出力機器	「第 6 章 セーフティ I/O ターミナルの動作 (P.6-1)」
↓		

手順	内容	参照
STEP2-2 プログラムの設計	**セーフティコントローラが制御する構成の場合** セーフティコントローラのセーフティプログラムを設計する。	『NX シリーズ セーフティコントロールユニット／通信コントロールユニット ユーザーズマニュアル(SGFM-723)』
	プリセットされた安全アプリケーションで、セーフティ I/O ターミナルが制御する構成の場合 • 安全アプリケーションとして、固定アプリケーションを使用する。 • 固定アプリケーションの中から、使用するアプリケーションを決定する。	「固定アプリケーション (P.6-24)」
	ユーザが設計した安全アプリケーションで、セーフティ I/O ターミナルが制御する構成（集中管理型）の場合 • 安全アプリケーションとして、ユーザ定義アプリケーションを使用する。 • ユーザ定義アプリケーションのロジックを設計する。	「ユーザ定義アプリケーション (P.6-25)」
	ユーザが設計した安全アプリケーションで、セーフティ I/O ターミナルが制御する構成（分散管理型）の場合 • 安全アプリケーションとして、ユーザが設計したアドオンアプリケーションを使用する。 • アドオンアプリケーションのロジックを設計する。	「アドオンアプリケーション (P.6-25)」

2-2-3 STEP3 ハード設計

手順	内容	参照
STEP3 通信、電源、外部接続入出力機器の配線の決定	セーフティ I/O ターミナルへの電源供給方法を決定する。	「第 4 章 電源供給の設計 (P.4-1)」
	• セーフティ I/O ターミナルの仕様に適合した通信ケーブルを選定する。 • セーフティ I/O ターミナルに供給される電源電圧、最大電流を計算し、電源ケーブルを選定する。 • セーフティ入出力機器間の I/O ケーブルを選定する。	「5-5 接続関連機器 (P.5-26)」

2-2-4 STEP4 安全応答性能の計算と検証

手順	内容	参照
STEP4-1 セーフティ通信性能の計算	STEP1-4、STEP1-5 で決定した CIP Safety コネクション、およびタグデータリンクコネクションに基づいて、EPI、通信負荷、およびセーフティコントローラのセーフティタスク周期を検証する。	「第 9 章 安全応答性能 (P.9-1)」 『NX シリーズ セーフティコントロールユニット／通信コントロールユニット ユーザーズマニュアル(SGFM-723)』の「セーフティリアクションタイムの計算」
↓		
STEP4-2 セーフティリアクションタイムの算出	セーフティ入出力機器、セーフティ I/O ターミナルの入出力応答時間、および CIP Safety コネクションの応答時間に基づいて、セーフティリアクションタイムを計算する。	「第 6 章 セーフティ I/O ターミナルの動作 (P.6-1)」 「第 9 章 安全応答性能 (P.9-1)」
↓		

手順	内容	参照
STEP4-3 安全距離の算出と要求仕様満足の検証	セーフティリアクションタイムから安全距離を算出する。安全距離が要求仕様を満足しているか確認し、要求仕様を満足していない場合は、システム設計から検討する。	−

2-2-5 STEP5 ソフトウェア設定とプログラミング

手順	内容	参照
STEP5-1 セーフティネットワークコントローラシステムの作成	セーフティ I/O ターミナルを配置する。	『NX シリーズ セーフティコントロールユニット／通信コントロールユニット ユーザーズマニュアル(SGFM-723)』の「CPU ラックの構成・設定」
STEP5-2 通信設定、プログラミング、およびセーフティ入出力端子への接続機器の割り付け	**セーフティコントローラが制御する構成の場合** 右記を参照	「7-1-1 セーフティコントローラが制御する構成（Type 1 Safety Open によるコンフィグレーション）の設定手順 (P.7-3)」
	プリセットされた安全アプリケーションで、セーフティ I/O ターミナルが制御する構成の場合 右記を参照	「7-1-3 プリセットされた安全アプリケーションでセーフティ I/O ターミナルが制御する構成の設定手順 (P.7-9)」
	ユーザが設計した安全アプリケーションで、セーフティ I/O ターミナルが制御する構成（集中管理型）の場合 右記を参照	「7-1-4 ユーザが設計した安全アプリケーションでセーフティ I/O ターミナルが制御する構成（集中管理型）の設定手順 (P.7-11)」
	ユーザが設計した安全アプリケーションで、セーフティ I/O ターミナルが制御する構成（分散管理型）の場合 右記を参照	「7-1-5 ユーザが設計した安全アプリケーションでセーフティ I/O ターミナルが制御する構成（分散管理型）の設定手順 (P.7-13)」

2-2-6 STEP6 取り付けと配線

手順	内容	参照
STEP6-1 取り付け	セーフティ I/O ターミナルの取り付け穴をねじ止めする。	「5-1 ユニットの取り付け (P.5-2)」
	ロータリスイッチで IP アドレスの設定方法を選択する。	「7-10 IP アドレスの設定 (P.7-69)」
	ロータリスイッチで安全アプリケーションを選択する。	「3-3 ロータリスイッチ (P.3-10)」
STEP6-2 電源および I/O の配線	セーフティ I/O ターミナルに電源や I/O ケーブルを配線する。	「5-3 電源の配線 (P.5-11)」 「5-4 I/O ケーブルの配線 (P.5-17)」
	I/O ケーブルの配線チェックを行う。	「8-6 I/O 配線チェック機能 (P.8-13)」
STEP6-3 Ethernet ケーブルの配線	セーフティ I/O ターミナルに通信ケーブルを配線する。	「5-2 EtherNet/IP ネットワークの配線 (P.5-4)」

手順	内容	参照
	通信ケーブルの配線チェックを行う。	「8-13 通信ケーブル診断機能 (P.8-31)」

2-2-7 STEP7 動作確認

手順	内容	参照
STEP7 動作確認	**セーフティコントローラが制御する構成の場合** 右記を参照	「7-1-1 セーフティコントローラが制御する構成（Type 1 Safety Open によるコンフィグレーション）の設定手順 (P.7-3)」
	プリセットされた安全アプリケーションで、セーフティ I/O ターミナルが制御する構成の場合 右記を参照	「7-1-3 プリセットされた安全アプリケーションでセーフティ I/O ターミナルが制御する構成の設定手順 (P.7-9)」
	ユーザが設計した安全アプリケーションで、セーフティ I/O ターミナルが制御する構成（集中管理型）の場合 右記を参照	「7-1-4 ユーザが設計した安全アプリケーションでセーフティ I/O ターミナルが制御する構成（集中管理型）の設定手順 (P.7-11)」
	ユーザが設計した安全アプリケーションで、セーフティ I/O ターミナルが制御する構成（分散管理型）の場合 右記を参照	「7-1-5 ユーザが設計した安全アプリケーションでセーフティ I/O ターミナルが制御する構成（分散管理型）の設定手順 (P.7-13)」

2-2-8 STEP8 運転と保守点検

手順	内容	参照
STEP8-1 運転	電源投入時モード設定や動作モード変更によって、動作モードが「Executing」に遷移することを確認する。	「7-16 動作モードの変更 (P.7-91)」
↓		
STEP8-2 異常発生時のトラブルシュート	異常が発生した場合は、LED 表示やモニタ機能を使用して、異常を確認および原因を特定した後、異常を取り除く。	「第 11 章 異常発生時の処置 (P.11-1)」
	セーフティ I/O ターミナルの電源モニタ機能を実行する。	「8-10 電源モニタ機能 (P.8-22)」
	セーフティ I/O ターミナルのユニット特定機能を実行する。	「8-8 ユニット特定機能 (P.8-16)」
	セーフティ I/O ターミナルの IP アドレス表示機能を実行する。	「8-9 IP アドレス表示機能 (P.8-19)」
	セーフティ I/O ターミナルの通信ケーブル診断機能を実行する。	「8-13 通信ケーブル診断機能 (P.8-31)」
↓		
STEP8-3 点検および交換	セーフティ I/O ターミナルが故障した場合、交換する。	「第 12 章 保守点検 (P.12-1)」
	セーフティ I/O ターミナルを交換した場合、ファームウェアをアップデートする。	「8-14 ファームウェアアップデート機能 (P.8-34)」

3

各部の名称と機能

この章では、セーフティ I/O ターミナルの各部の名称と機能について説明しています。

3-1　各部の名称 3-2

3-2　表示部 3-5
3-2-1　ステータス LED 3-5
3-2-2　I/O LED 3-7
3-2-3　ユニット特定表示 LED 3-9

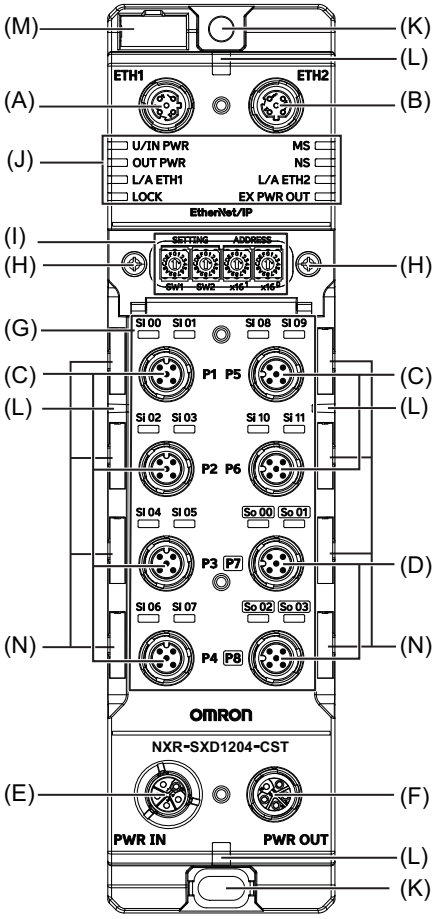
3-3　ロータリスイッチ 3-10

3-4　コネクタ 3-11
3-4-1　EtherNet/IP 通信コネクタ 3-11
3-4-2　電源コネクタ 3-11
3-4-3　I/O コネクタ 3-12

3-1 各部の名称

セーフティ I/O ターミナルの各部の名称を説明します。

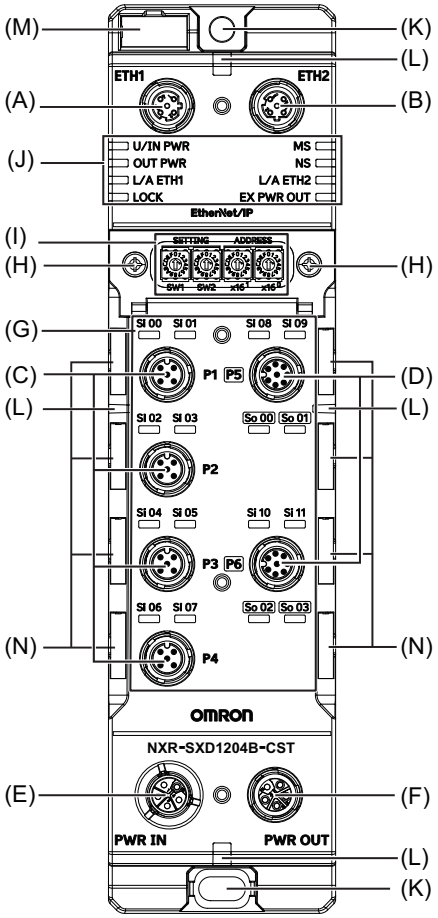
● 形 NXR-SXD1204-CST



記号	名称	機能
(A)	EtherNet/IP 通信コネクタ 1	EtherNet/IP ポート 1 のコネクタです。 M12 コネクタ（D-coding、メス、スマートクリック対応）です。 通信ケーブルを接続します。
(B)	EtherNet/IP 通信コネクタ 2	EtherNet/IP ポート 2 のコネクタです。 M12 コネクタ（D-coding、メス、スマートクリック対応）です。 通信ケーブルを接続します。
(C)	I/O コネクタ（セーフティ入力ポート用）	セーフティ入力機器を接続するためのコネクタです。 I/O コネクタの横に取り外し可能なマーカを取り付けます。 M12 コネクタ（A-coding、メス、5pin、スマートクリック対応）です。 I/O ケーブル（5 芯）を接続します。
(D)	I/O コネクタ（セーフティ出力ポート用）	セーフティ出力機器を接続するためのコネクタです。 I/O コネクタの横に取り外し可能なマーカを取り付けます。 M12 コネクタ（A-coding、メス、5pin、スマートクリック対応）です。 I/O ケーブル（5 芯）を接続します。
(E)	電源コネクタ IN	ユニット／入力用電源と出力用電源を供給するためのコネクタです。 M12 コネクタ（L-coding、オス、スマートクリック対応）です。 外部供給電源と接続するための電源ケーブルを接続します。

記号	名称	機能
(F)	電源コネクタ OUT	自ノードから他のノードに、ユニット／入力用電源と出力用電源を供給するためのコネクタです。電源供給方法で、渡り配線による供給をする場合に使用します。 M12 コネクタ（L-coding、メス、スマートクリック対応）です。
(G)	I/O LED	各ポートの端子ごとに、セーフティ入力／セーフティ出力の状態を表示します。
(H)	カバー固定穴	ロータリスイッチ用カバーを固定するための穴です。2 箇所あります。上記は、穴をねじ止めした状態を示しています。
(I)	ロータリスイッチ	安全アプリケーションの選択と IP アドレス設定で使用するスイッチです。
(J)	ステータス LED	セーフティ I/O ターミナルの現在の動作状態を表示します。
(K)	ユニット取付穴	ユニットを取り付けるための穴です。2 箇所あります。M5 ねじで取り付けます。
(L)	ユニット特定表示 LED	ユニット特定機能を使用する際、表示して知らせます。
(M)	ユニット識別マーカ	セーフティ I/O ターミナルを識別するマーカです。色は白色です。
(N)	I/O 識別マーカ	I/O 端子を識別するマーカです。色は白色です。

● 形 NXR-SXD1204B-CST



記号	名称	機能
(A)	EtherNet/IP 通信コネクタ 1	EtherNet/IP ポート 1 のコネクタです。 M12 コネクタ（D-coding、メス、スマートクリック対応）です。 通信ケーブルを接続します。
(B)	EtherNet/IP 通信コネクタ 2	EtherNet/IP ポート 2 のコネクタです。 M12 コネクタ（D-coding、メス、スマートクリック対応）です。 通信ケーブルを接続します。

記号	名称	機能
(C)	I/O コネクタ (セーフティ入力ポート用)	セーフティ入力機器を接続するためのコネクタです。 I/O コネクタの横に取り外し可能なマーカを取り付けます。 M12 コネクタ（A-coding、メス、5pin、スマートクリック対応）です。 I/O ケーブル（5 芯）を接続します。
(D)	I/O コネクタ (セーフティ入出力ポート用)	セーフティ入力機器、およびセーフティ出力機器を接続するためのコネクタです。 I/O コネクタの横に取り外し可能なマーカを取り付けます。 M12 コネクタ（A-coding、メス、8pin、スマートクリック対応）です。 I/O ケーブル（8 芯）を接続します。
(E)	電源コネクタ IN	ユニット／入力用電源と出力用電源を供給するためのコネクタです。 M12 コネクタ（L-coding、オス、スマートクリック対応）です。 外部供給電源と接続するための電源ケーブルを接続します。
(F)	電源コネクタ OUT	自ノードから他のノードに、ユニット／入力用電源と出力用電源を供給するためのコネクタです。電源供給方法で、渡り配線による供給をする場合に使用します。 M12 コネクタ（L-coding、メス、スマートクリック対応）です。
(G)	I/O LED	各ポートの端子ごとに、セーフティ入力／セーフティ出力の状態を表示します。
(H)	カバー固定穴	ロータリスイッチ用カバーを固定するための穴です。2 箇所あります。上記は、穴をねじ止めした状態を示しています。
(I)	ロータリスイッチ	安全アプリケーションの選択と IP アドレス設定で使用するスイッチです。
(J)	ステータス LED	セーフティ I/O ターミナルの現在の動作状態を表示します。
(K)	ユニット取付穴	ユニットを取り付けるための穴です。2 箇所あります。M5 ねじで取り付けます。
(L)	ユニット特定表示 LED	ユニット特定機能を使用する際、表示して知らせます。
(M)	ユニット識別マーカ	セーフティ I/O ターミナルを識別するマーカです。色は白色です。
(N)	I/O 識別マーカ	I/O 端子を識別するマーカです。色は白色です。

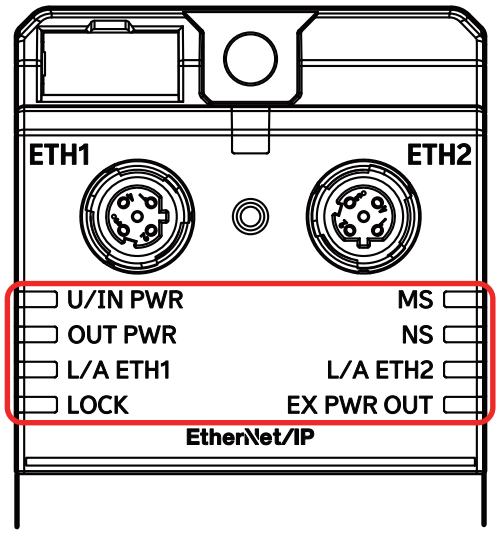
3-2 表示部

セーフティ I/O ターミナルには、以下の表示部があります。これらの LED を説明します。

- ステータス LED
- I/OLED
- ユニット特定表示 LED

3-2-1 ステータス LED

セーフティ I/O ターミナルの現在の動作状態を表示します。



U/IN PWR LED

ユニット／入力用電源の状態を表示します。

色	状態		説明
緑		点灯	ユニット／入力用電源が供給されている
−		消灯	ユニット／入力用電源が供給されていない

OUT PWR LED

出力用電源の状態を表示します。

色	状態		説明
緑		点灯	出力用電源が供給されている
−		消灯	出力用電源が供給されていない

MS LED

モジュールステータス LED です。ユニットの動作状態を表示します。

色	状態		説明
緑		点灯	正常運転状態 (Executing)
		点滅	正常運転待ち状態 (Idle)
赤		点灯	致命的な異常が発生 (Critical Fault)
		点滅	運転停止異常 (Abort) *1
緑／赤		点滅	初期処理中 (Self-Testing)、TUNID 設定待ち状態 (Waiting for TUNID)、またはコンフィグレーション待ち状態 (Configuring)
－		消灯	IP アドレス表示機能実行中 (IP Address Display)、I/O 配線チェック機能実行中 (I/O Wiring Checking)、または電源 OFF

***1.** 異常の詳細は、「11-2 イベントによる異常の確認と対処方法 (P.11-6)」を参照してください。

NS LED

ネットワークステータス LED です。セーフティ I/O ターミナルの通信状態を表示します。

色	状態		説明
緑		点灯	CIP Safety / EtherNet/IP / CIP メッセージ通信のうち、いずれかのコネクションが確立している状態
		点滅	CIP Safety / EtherNet/IP / CIP メッセージ通信のいずれのコネクションも確立していない状態
赤		点灯	ネットワークに影響がある致命的な異常が発生 例）IP アドレス重複
		点滅	CIP Safety / EtherNet/IP 通信のうち、いずれか 1 つのコネクションでタイムアウト異常が発生*1
－		消灯	IP アドレス未設定、または電源 OFF

***1.** 異常の詳細は、「11-2 イベントによる異常の確認と対処方法 (P.11-6)」を参照ください。

L/A ETH1 LED

EtherNet/IP ポート 1 リンク／アクティビティ LED です。EtherNet/IP ポート 1 のリンク状態と通信状態を表示します。

色	状態		説明
緑		点灯	リンク確立済み
		点滅	リンク確立し、通信中

色	状態		説明
－	□	消灯	リンク確立なし

L/A ETH2 LED

EtherNet/IP ポート 2 リンク／アクティビティ LED です。EtherNet/IP ポート 2 のリンク状態と通信状態を表示します。

色	状態		説明
緑		点灯	リンク確立済み
		点滅	リンク確立し、通信中
－	□	消灯	リンク確立なし

LOCK LED

セーフティ I/O ターミナルの設定データのユーザ認証状態を表します。ユーザはアプリケーション動作確認チェック後、コンフィグレーションロック状態にし、使用することを推奨します。

色	状態		説明
黄		点灯	コンフィグレーションロック済
		点滅	コンフィグレーションロック解除、かつロック可
－	□	消灯	コンフィグレーションロック解除、かつロック不可

EX PWR OUT LED

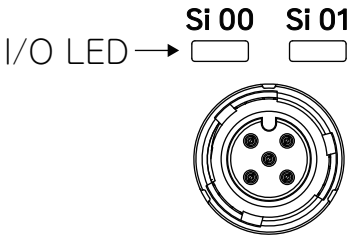
渡り配線の出力用電源の状態を表示します。

色	状態		説明
緑		点灯	渡り配線の出力用電源が供給されている
－	□	消灯	渡り配線の出力用電源が供給されていない

3-2-2 I/O LED

I/O LED はセーフティ入力端子およびセーフティ出力端子の状態を示します。

例）セーフティ入力 LED



セーフティ入力 LED

セーフティ入力端子の状態を表す LED です。

色	状態		説明
黄		点灯	セーフティ入力端子が ON（正常動作中）
赤		点灯	次のいずれかの異常を検出した • セーフティ入力端子外部接続機器異常 • セーフティ入力端子内部回路異常 • セーフティ入力端子デュアルチャネル監視異常
		点滅	• デュアルチャネルの相手側のセーフティ入力端子に異常が発生
−		消灯	セーフティ入力端子が OFF（正常動作中）

セーフティ出力 LED

セーフティ出力端子の状態を表す LED です。

色	状態		説明
黄		点灯	セーフティ出力端子が ON（正常動作中）
赤		点灯	次のいずれかの異常を検出した • セーフティ出力端子地絡異常 • セーフティ出力端子出力 ON 固着異常 • セーフティ出力端子内部回路異常 • デュアルチャネル出力間のデータ異常*1 • EDM 異常*1
		点滅	• 関連する他のセーフティ出力端子に異常が発生
−		消灯	セーフティ出力端子が OFF（正常動作中）

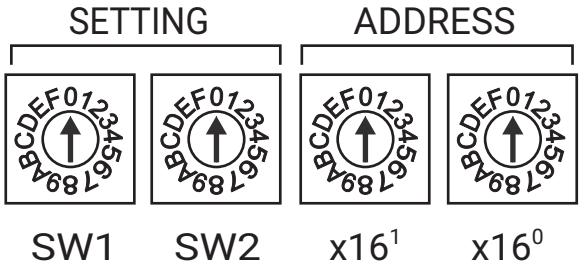
***1.** セーフティ出力端子がデュアルチャネル設定されている場合、EDM 異常またはデュアルチャネル出力間のデータ異常のとき、両チャネルのセーフティ出力 LED が赤点灯となります。シングルチャネル設定されている場合、EDM 異常は該当チャネルのセーフティ出力 LED のみ赤点灯します。

3-2-3 ユニット特定表示 LED

ユニット特定機能とファームウェアアップデート機能で使用します。
詳しくは、「8-8 ユニット特定機能 (P.8-16)」、「8-14 ファームウェアアップデート機能 (P.8-34)」を参照してください。

3-3 ロータリスイッチ

ロータリスイッチで、アプリケーション設定と IP アドレスの設定を行います。



概要は、以下のとおりです。

ロータリスイッチ名	説明
SETTING*1	安全アプリケーション*2、IP アドレス表示機能*3、および I/O 配線チェック機能*4 の中から選択します。 SW1 と SW2 をいずれも以下の値に設定してください。 •「0」：リモート I/O モードで動作します。 •「1」～「3」：固定アプリケーションで動作します。 •「4」～「7」：Reserved •「8」：IP アドレス表示機能で動作します。 •「9」～「D」：アドオンアプリケーションで動作します。 •「E」：I/O 配線チェック機能で動作します。 •「F」：ユーザ定義アプリケーションで動作します。
ADDRESS*1	2 個のスイッチで 16 進数の 2 桁を表現します。 設定範囲は 00～FFHex で、工場出荷時設定は 00Hex です。 IP アドレスの設定方法については、「7-10-2 ロータリスイッチによる IP アドレスの設定方法の選択 (P.7-71)」を参照してください。

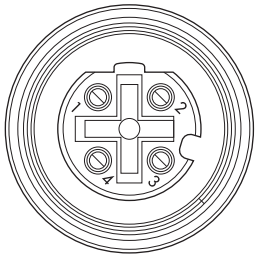
***1.** ロータリスイッチの設定を反映するには、電源を OFF/ON、もしくは再起動が必要です。
***2.** 安全アプリケーションの詳細については「6-7 安全アプリケーション (P.6-23)」を参照してください。
***3.** IP アドレス表示機能については「8-9 IP アドレス表示機能 (P.8-19)」を参照してください。
***4.** I/O 配線チェック機能については「8-6 I/O 配線チェック機能 (P.8-13)」を参照してください。

3-4 コネクタ

セーフティ I/O ターミナルには、以下のコネクタがあります。
- EtherNet/IP 通信コネクタ
- 電源コネクタ
- I/O コネクタ

3-4-1 EtherNet/IP 通信コネクタ

EtherNet/IP 通信を行うためのコネクタです。本書では“通信コネクタ”とも呼びます。

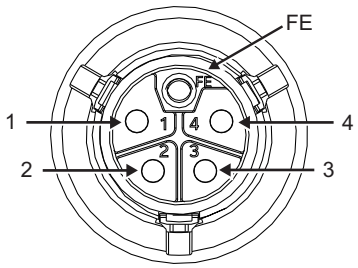


電気的特性、コネクタ機構、および端子配列は以下のとおりです。
- 電気的特性
  IEEE802.3 規格に準拠
- コネクタ機構
  M12 コネクタ（D-coding、メス、シールド対応）×2 個
- 端子配列

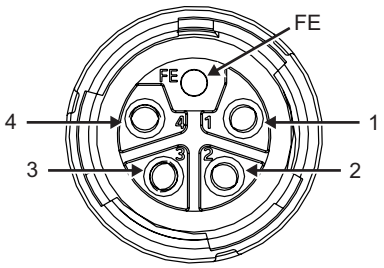
ピン番号	信号名	説明
1	TD+	送信用データ+
2	RD+	受信用データ+
3	TD-	送信用データ-
4	RD-	受信用データ-

3-4-2 電源コネクタ

セーフティ I/O ターミナルに電源を供給するためのコネクタです。



電源コネクタIN（PWR IN）



電源コネクタOUT（PWR OUT）

● 電源コネクタ IN

ユニット／入力用電源と出力用電源を供給するためのコネクタです。外部供給電源の電源ケーブルを接続します。

● 電源コネクタ OUT

自ノードから他のノードへ出力用電源を供給するためのコネクタです。渡り配線による電源共有を行う場合に使用します。

● コネクタ機構および端子配列

コネクタ機構、および端子配列は以下のとおりです。

a. コネクタ機構
電源コネクタ IN: M12 コネクタ（L-coding、オス、スマートクリック対応）
電源コネクタ OUT: M12 コネクタ（L-coding、メス、スマートクリック対応）

b. 端子配列
電源コネクタ IN、電源コネクタ OUT 共通です。

ピン番号	信号名	説明
1	U/IN P+	ユニット／入力用電源+
2	OUT P-	出力用電源-
3	U/IN P-	ユニット／入力用電源-
4	OUT P+	出力用電源+
FE (Functional Earth)	FG	フレームグラウンド

安全上の要点

電源最大電流はユニット／入力用電源と出力用電源の合計で 9A です。電源最大電流を超えて使用しないでください。電源最大電流を超えて使用すると、電源ケーブルに過剰な電流が流れることで、発火するおそれがあります。

使用上の注意

ユニット／入力用電源を供給する電源と、出力用電源を供給する電源は、別々の電源から供給してください。同一の電源から供給すると、出力機器の負荷変動による誤動作の原因となることがあります。

3-4-3 I/O コネクタ

セーフティ入力機器、セーフティ出力機器を接続するためのコネクタです。
I/O コネクタは接続する機器により、以下のように分けられます。
また本書では、１コネクタ単位で“ポート”と呼びます。

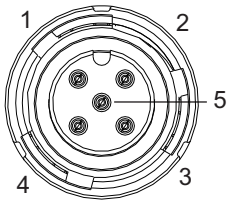
- セーフティ入力ポート
- セーフティ出力ポート
- セーフティ入出力ポート

セーフティ入力ポート

I/O コネクタのうち、セーフティ入力端子やテスト出力端子をもつコネクタをセーフティ入力ポートと呼びます。
セーフティ入力ポートの数と場所は形式で異なります。

- 形 NXR-SXD1204-CST の場合：ポート P1～P6
- 形 NXR-SXD1204B-CST の場合：ポート P1～P4

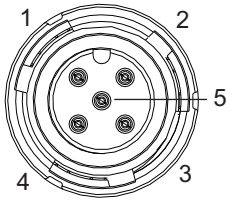
セーフティ入力ポートのピン配置を以下に示します。



ピン番号	信号名	説明	ポート					
			P1	P2	P3	P4	P5	P6
1	T (n)	テスト出力端子 (n)	T00	T02	T04	T06	T08	T10
2	Si (n)	セーフティ入力端子 (n)	Si00	Si02	Si04	Si06	Si08	Si10
3	U/IN P-	ユニット/入力電源 -	GND					
4	Si (n+1)	セーフティ入力端子 (n+1)	Si01	Si03	Si05	Si07	Si09	Si11
5	T (n+1)	テスト出力端子 (n+1)	T01	T03	T05	T07	T09	T11

セーフティ出力ポート

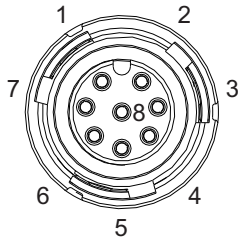
I/O コネクタのうち、セーフティ出力端子をもつコネクタをセーフティ出力ポートと呼びます。
セーフティ出力ポートは、形 NXR-SXD1204-CST だけにあります。
セーフティ出力ポートは、ポート P7～P8 です。
セーフティ出力ポートのピン配置を以下に示します。



ピン番号	信号名	説明	ポート	
			P7	P8
1	NC	NC	NC	
2	So (n)	セーフティ出力端子 (n)	So00	So02
3	OUT P-	出力用電源 -	OUT GND	
4	So (n+1)	セーフティ出力端子 (n+1)	So01	So03
5	OUT P-	出力用電源 -	OUT GND	

セーフティ入出力ポート

I/O コネクタのうち、セーフティ入力端子とセーフティ出力端子をもつコネクタをセーフティ入出力ポートと呼びます。
セーフティ入出力ポートは、形 NXR-SXD1204B-CST だけにあります。
セーフティ入出力ポートは、ポート P5～P6 です。
セーフティ入出力ポートのピン配置を以下に示します。



ピン番号	信号名	説明	ポート	
			P5	P6
1	T (n)	テスト出力端子 (n)	T08	T10
2	Si (n)	セーフティ入力端子 (n)	Si08	Si10
3	U/IN P-	ユニット/入力電源 -	GND	
4	Si (n+1)	セーフティ入力端子 (n+1)	Si09	Si11
5	T (n+1)	テスト出力端子 (n+1)	T09	T11
6	So (n)	セーフティ出力端子 (n)	So00	So02
7	So (n+1)	セーフティ出力端子 (n+1)	So01	So03
8	OUT P-	出力用電源 -	OUT GND	

4

電源供給の設計

この章では、セーフティ I/O ターミナルの電源供給の設計について説明しています。

4-1　電源の種類と電源供給システム 4-2
4-1-1　電源の種類と用途 4-2
4-1-2　電源供給システム 4-2
4-2　電源供給の設計方法 4-6
4-2-1　電源供給の設計手順 4-6
4-2-2　直接供給での設計方法 4-6
4-2-3　渡り配線による供給での設計方法 4-12
4-3　電源や保護機器の選定 4-19
4-3-1　外部供給電源の選定 4-19
4-3-2　保護機器の選定 4-19

4-1 電源の種類と電源供給システム

セーフティ I/O ターミナルの電源の種類と用途、および電源供給システムを説明します。

4-1-1 電源の種類と用途

セーフティ I/O ターミナルの電源の種類と用途を説明します。

電源の種類

セーフティ I/O ターミナルに供給する電源には、以下の 2 種類があります。

- ユニット／入力用電源
- 出力用電源

電源の用途

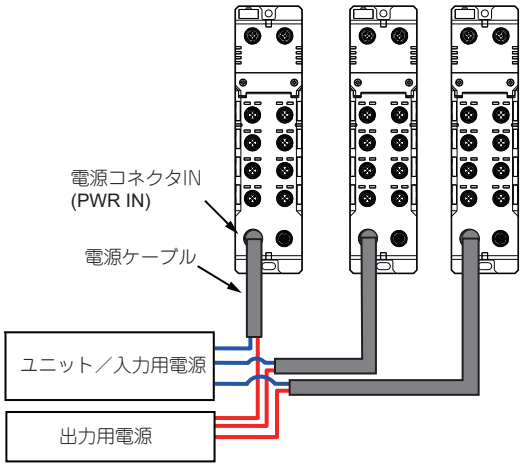
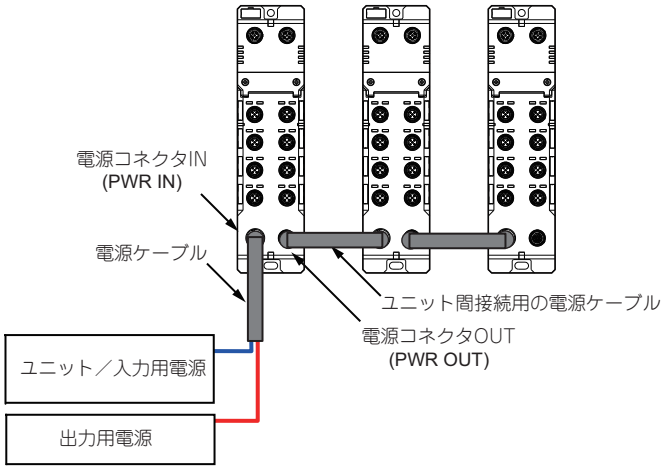
各電源の用途は以下のとおりです。

種類	用途
ユニット／入力用電源	セーフティ I/O ターミナルの動作やセーフティ入力機器とのインタフェースで使用します。 以下に示します。 • セーフティ I/O ターミナルの内部回路、セーフティ入力回路、テスト出力回路の動作 • メカ接点タイプのセーフティ入力機器へのテストパルス出力 • 半導体出力タイプのセーフティ入力機器への電源供給
出力用電源	セーフティ出力機器とのインタフェースで使用します。 以下に示します。 • セーフティ I/O ターミナルの出力回路の動作 • PNP 出力が接続可能なセーフティ出力機器への負荷電流

いずれの電源も電圧・電流モニタおよび過電圧・過電流保護を行います。

4-1-2 電源供給システム

セーフティ I/O ターミナルへの電源の供給方法は以下の二つがあります。

方法	説明	特長
直接供給	各セーフティ I/O ターミナルの電源コネクタ PWR IN に、外部供給電源を接続する方法です。*1  	渡り配線のケーブルでの電圧降下がありません。
渡り配線による供給*2	1 台のセーフティ I/O ターミナルの電源コネクタ PWR IN に、外部供給電源を接続します。そのユニットの電源コネクタ PWR OUT と他のセーフティ I/O ターミナルの電源コネクタ PWR IN を電源ケーブルで接続します。以降のユニット間を電源ケーブルで渡り配線して供給する方法です。*1  	渡り配線のため、システム全体で使用する電源ケーブルの長さを短くすることができます。 この電源配線時、渡り配線出力用電源遮断機能の使用が可能となります。詳しくは「8-5 渡り配線出力用電源遮断機能 (P.8-11)」を参照してください。

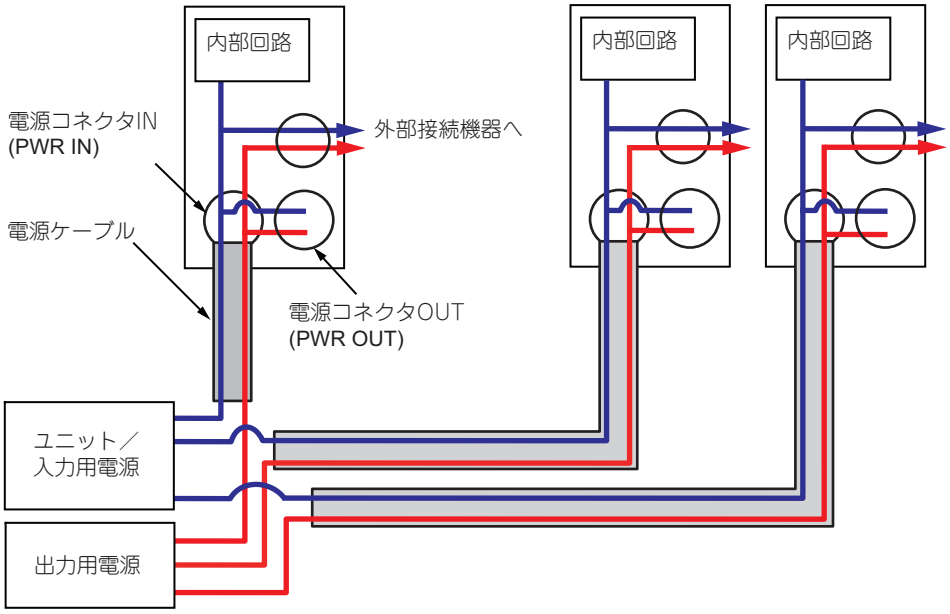
***1.** オムロン製の耐環境型 IP67・パワーサプライ（形 S8NR-S シリーズ）を使用する場合、ユニット／入力用電源の GND と、出力用電源の GND が電源ユニット内で接続されます。そのためセーフティ I/O ターミナル内の絶縁が担保されません。絶縁が必要な場合は、ユニット／入力用電源と出力用電源を分離してください。

***2.** セーフティ I/O ターミナルにユニット／入力用電源が供給されている時のみ、PWR OUT から出力用電源が供給されます。ユニット／入力用電源が OFF の時や、過電圧などが原因でユニット／入力用電源が遮断された時、PWR OUT からの出力用電源の供給も遮断されます。

以下に、システム構成図の詳細を示します。

● 直接供給のシステム構成

以下に例を示します。各セーフティ I/O ターミナルの電源コネクタ PWR IN に、外部供給電源を接続して供給します。

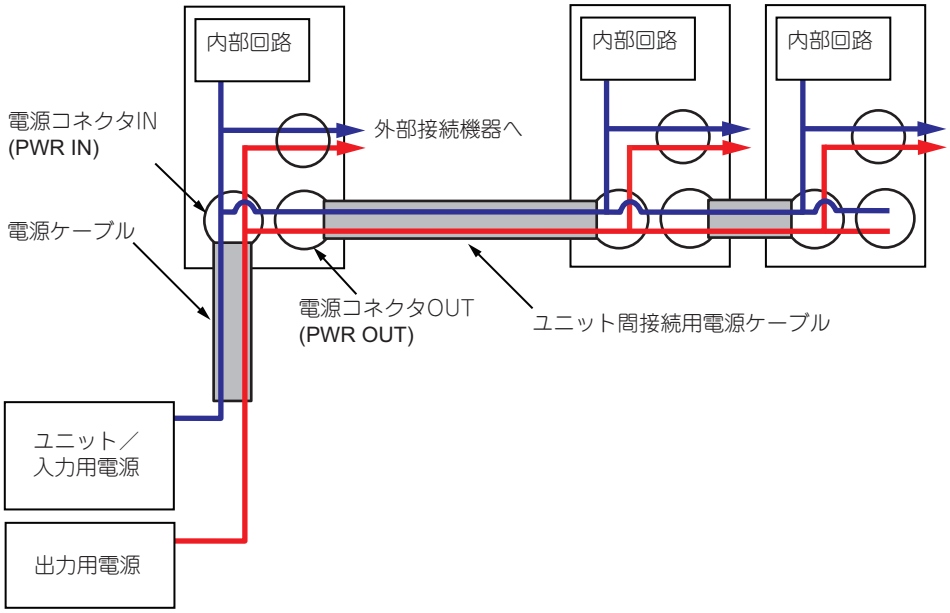


使用上の注意

- ユニット／入力用電源を供給する電源と、出力用電源を供給する電源は、別々の電源から供給してください。同一の電源から供給すると、出力機器の負荷変動による誤動作の原因となることがあります。

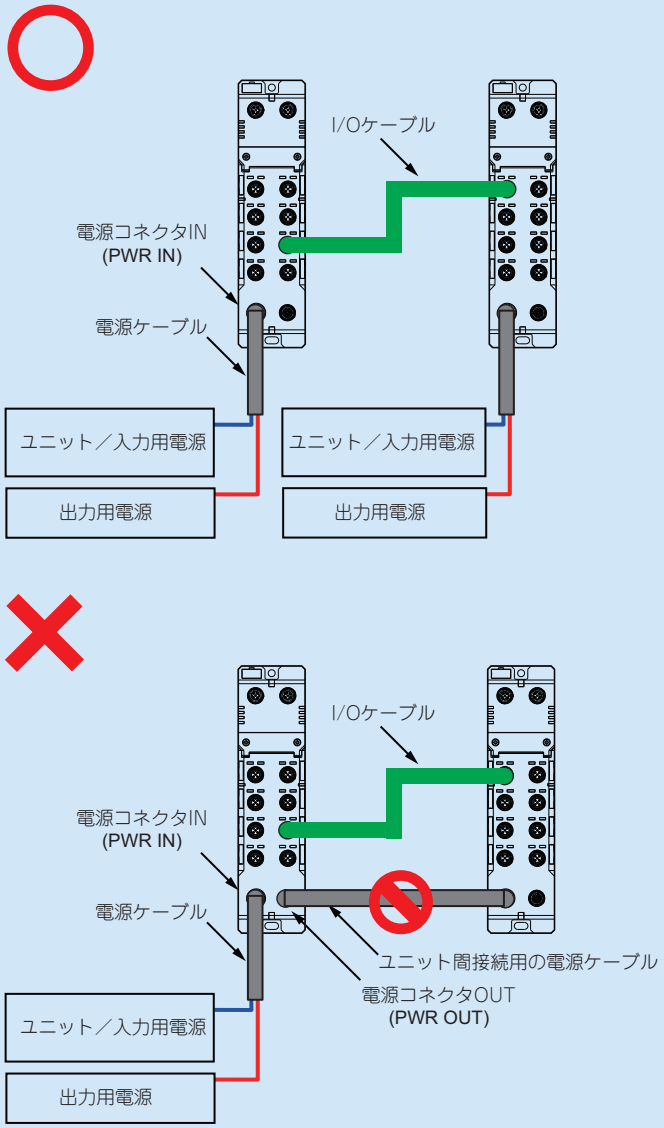
● 渡り配線による供給のシステム構成

最初のセーフティ I/O ターミナルの電源コネクタ PWR IN に、外部供給電源を接続します。そのユニットの電源コネクタ PWR OUT と他のセーフティ I/O ターミナルの電源コネクタ PWR IN を電源ケーブルで接続します。以降のユニット間を電源ケーブルで渡り配線していきます。



使用上の注意

- ユニット／入力用電源を供給する電源と、出力用電源を供給する電源は、別々の電源から供給してください。同一の電源から供給すると、出力機器の負荷変動による誤動作の原因となることがあります。
- ユニット間でセーフティ I/O ポートを接続する場合、渡り配線による電源供給を行わないでください。電源間の GND が I/O ケーブルで接続されるため、絶縁されません。



4-2 電源供給の設計方法

セーフティ I/O ターミナルの電源供給の設計方法について、説明します。

⚠ 警告

このマニュアルに示すとおり、正しく電源の設計や配線を行ってください。範囲外の電圧／電流の入力や誤配線は、故障や火災の原因となります。

4-2-1 電源供給の設計手順

セーフティ I/O ターミナルの電源供給の全体の設計手順を以下に示します。

手順	説明	参照
1.供給方法の決定	電源の供給方法を決定します。 供給方法は、以下の二つがあります。 • 直接供給 • 渡り配線による供給	「4-1-2 電源供給システム (P.4-2)」
↓		
2.電源供給の設計	供給方法ごとに、以下の設計を行い、設計条件を満足することを確認します。 • ユニット／入力用電源供給の設計 • 出力用電源供給の設計	• 直接供給の場合 「4-2-2 直接供給での設計方法 (P.4-6)」 • 渡り配線による供給の場合 「4-2-3 渡り配線による供給での設計方法 (P.4-12)」
↓		
3.外部供給電源と保護機器の選定	手順 2 で算出した消費電流から、電源容量を算出して、外部供給電源を選定します。また、外部回路の短絡や過電流に備えるための保護機器（ブレーカやヒューズなど）を選定します。	「4-3 電源や保護機器の選定 (P.4-19)」

4-2-2 直接供給での設計方法

電源の供給方法が直接供給の場合の、電源供給の設計方法を説明します。

直接供給での設計手順

以下の設計条件(a)～(c)を満足することを確認します。確認方法については、参照先の説明を参照してください。

設計条件	確認方法の参照先
(a)ユニット／入力用電源と出力用電源の総消費電流の合計が、セーフティ I/O ターミナルの電源最大電流の範囲内であること。*1	「直接供給での総消費電流の計算方法 (P.4-7)」

設計条件	確認方法の参照先
(b)ユニット／入力用電源電圧が降下しても、セーフティ I/O ターミナルの入力回路仕様および外部接続機器の電圧仕様を満たすこと。*2	「直接供給での電圧降下の計算 (P.4-10)」
(c)出力用電源電圧が降下しても、セーフティ I/O ターミナルの出力回路仕様および外部接続機器の電圧仕様を満たすこと。*3	

***1.** 電源最大電流は 9A です。9A を超えないようにします。
***2.** たとえば、セーフティ I/O ターミナルでは、ユニット／入力用電源電圧が、DC19.2～28.8V 内であることを確認します。
***3.** たとえば、セーフティ I/O ターミナルでは、出力用電源電圧が、DC19.2～28.8V 内であることを確認します。

直接供給での総消費電流の計算方法

直接供給とは、セーフティ I/O ターミナルごとに電源を供給する方法です。そのため、ユニットごとに各電源の総消費電流を計算します。各電源の総消費電流の合計が、セーフティ I/O ターミナルの電源最大電流を下回るように設計します。

セーフティ I/O ターミナルが消費するユニット／入力用電源または出力用電源の総消費電流の計算方法を以下に示します。

● ユニット／入力用電源の総消費電流

＝（ユニット／入力用電源の消費電流）
　＋（接続するセーフティ入力機器で消費する電流）
　＋（テスト出力で消費する電流）

計算式の各項目を以下に説明します。

項目	説明
ユニット／入力用電源の消費電流	セーフティ I/O ターミナルで消費する電流です。「2-1-4 ユニット仕様 (P.2-6)」の「消費電流値」のうち、「ユニット／入力用電源」の値を適用します。
接続するセーフティ入力機器で消費する電流	以下の計算式で計算します。 （セーフティ入力機器の電源の消費電流）＋（セーフティ入力電流×使用入力点数）
テスト出力で消費する電流*1	以下の計算式で計算します。 （テスト出力の負荷電流×使用出力点数）

***1.** 半導体出力機器を接続する場合、テスト出力の出力電流は 0.7A／点 必要になります。

● 出力用電源の総消費電流

＝（出力用電源の消費電流）
　＋（接続するセーフティ出力機器で消費する電流）

計算式の各項目を以下に説明します。

項目	説明
出力用電源の消費電流	セーフティ I/O ターミナルで消費する電流です。「2-1-4 ユニット仕様 (P.2-6)」の「消費電流値」のうち、「出力用電源」の値を適用します。
接続するセーフティ出力機器で消費する電流 *1	以下の計算式で計算します。 （セーフティ出力の負荷電流×使用出力点数）

***1.** 形 NXR-SXD1204-CST の場合、セーフティ出力の最大負荷電流 2A／点を超えないようにしてください。形 NXR-SXD1204B-CST の場合、セーフティ出力の最大負荷電流 0.7A／点を超えないようにしてください。

直接供給での総消費電流の計算例

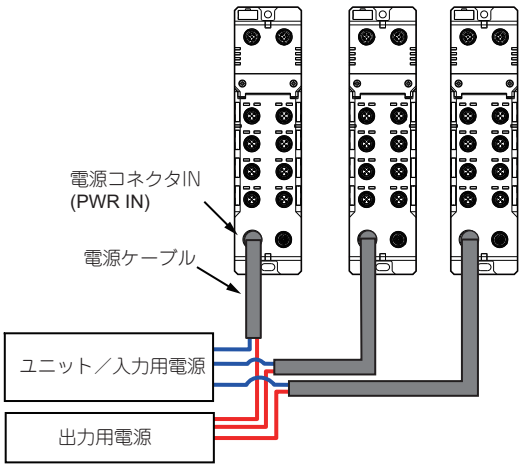
ある構成と使用条件を例に、ユニット／入力用電源と出力用電源の総消費電流の計算方法を以下に示します。

使用上の注意

ここでは計算例を示しています。お客様の装置・設備は、さまざまであるため、お客様の使用状態にあわせた計算をしてください。

● 構成例

セーフティ I/O ターミナルを左から SXD1、SXD2、SXD3 とします。



● 外部接続機器の使用条件

セーフティ I/O ターミナルごとに、以下の使用条件とします。SXD2 と SXD3 は同じ条件としています。

セーフティ I/O ターミナルの条件				外部接続機器の条件	
ユニット名	セーフティ I/O ポート			品名	仕様
	ポート名	信号名	端子番号		
SXD1	セーフティ入力ポート 1	セーフティ入力	Si00 /01	セーフティ入力機器	• セーフティ入力機器の消費電流: 50mA • セーフティ入力電流: 4.5mA/点 • テスト出力の負荷電流: 200mA/点
		テスト出力	T00 /01		
	セーフティ入力ポート 2	セーフティ入力	Si02 /03	セーフティ入力機器	• セーフティ入力機器の消費電流: 50mA • セーフティ入力電流: 4.5mA/点 • テスト出力の負荷電流: 200mA/点
		テスト出力	T02 /03		
	セーフティ入力ポート 3～6	セーフティ入力	Si04～11	未使用	－
		テスト出力	T04～11	未使用	－
	セーフティ出力ポート 1	セーフティ出力	So00 /01	セーフティ出力機器	• セーフティ出力機器の消費電流: 50mA • セーフティ出力の負荷電流: 500mA/点
	セーフティ出力ポート 2	セーフティ出力	So02 /03	未使用	－

セーフティ I/O ターミナルの条件				外部接続機器の条件	
ユニット名	セーフティ I/O ポート			品名	仕様
	ポート名	信号名	端子番号		
SXD2 と SXD3	セーフティ入力ポート 1	セーフティ入力	Si00 /01	セーフティ入力機器	• セーフティ入力機器の消費電流: 50mA • セーフティ入力電流: 4.5mA/点 • テスト出力の負荷電流: 200mA/点
		テスト出力	T00 /01		
	セーフティ入力ポート 2～6	セーフティ入力	Si02～11	未使用	−
		テスト出力	T02～11	未使用	−
	セーフティ出力ポート 1	セーフティ出力	So00 /01	セーフティ出力機器	• セーフティ出力機器の消費電流: 50mA • セーフティ出力の負荷電流: 500mA/点
	セーフティ出力ポート 2	セーフティ出力	So02 /03	未使用	−

● 総消費電流の計算

セーフティ I/O ターミナルごとに、ユニット／入力用電源と出力用電源の総消費電流の各計算項目は以下となります。

ユニット名	電源の種類	総消費電流の計算項目	計算結果
SXD1	ユニット／入力用電源	ユニット／入力用電源の消費電流	セーフティ I/O ターミナルの仕様から 220mA です。
		接続するセーフティ入力機器で消費する電流	セーフティ入力ポート 1 と 2 が対象です。 （セーフティ入力機器の電源の消費電流）＋（セーフティ入力電流×使用入力点数） =(50mA+50mA)+（4.5mA×4 点） =118mA
		テスト出力で消費する電流	セーフティ入力ポート 1 と 2 が対象です。 （テスト出力の負荷電流×使用出力点数） =200mA×4 点 =800mA
	出力用電源	出力用電源の消費電流	セーフティ I/O ターミナルの仕様から 40mA です。
		接続するセーフティ出力機器で消費する電流	セーフティ出力ポート 1 が対象です。 （セーフティ出力の負荷電流×使用出力点数） =500mA×2 点 =1000mA
SXD2 と SXD3	ユニット／入力用電源	ユニット／入力用電源の消費電流	セーフティ I/O ターミナルの仕様から 220mA です。
		接続するセーフティ入力機器で消費する電流	セーフティ入力ポート 1 が対象です。 （セーフティ入力機器の電源の消費電流）＋（セーフティ入力電流×使用入力点数） =50mA+（4.5mA×2 点） =59mA
		テスト出力で消費する電流	セーフティ入力ポート 1 が対象です。 （テスト出力の負荷電流×使用出力点数） =200mA×2 点 =400mA
	出力用電源	出力用電源の消費電流	セーフティ I/O ターミナルの仕様から 40mA です。
		接続するセーフティ出力機器で消費する電流	セーフティ出力ポート 1 が対象です。 （セーフティ出力の負荷電流×使用出力点数） =500mA×2 点 =1000mA

以上から、セーフティ I/O ターミナルごとの総消費電流の合計は以下となります。

a. SXD1 の総消費電流の合計
（SXD1 のユニット／入力用電源の総消費電流）＋（SXD1 の出力用電源の総消費電流）
=(220mA+118mA+800mA)+(40mA+1000mA)
=(1138mA)+(1040mA)
≒(1.14A)+(1.04A)
=2.18A

b. SXD2 の総消費電流の合計
（SXD2 のユニット／入力用電源の総消費電流）＋（SXD2 の出力用電源の総消費電流）
=(220mA+59mA+400mA)+(40mA+1000mA)
=(679mA)+(1040mA)
≒(0.68A)+(1.04A)
=1.72A

c. SXD3 の総消費電流の合計
SXD2 と同じです。
（SXD3 のユニット／入力用電源の総消費電流）＋（SXD3 の出力用電源の総消費電流）
≒1.72A

ユニットごとの総消費電流の合計は、いずれもセーフティ I/O ターミナルの電源最大電流 9A を下回るため、この例では、問題ありません。

直接供給での電圧降下の計算

電源ケーブルで電圧降下が発生します。
オムロン製の M12 L コード電源ケーブル（形 XS5F-L521-□12-F、形 XS5W-L521-□12-F）を使用した場合の電圧降下は、下表となります。

ユニット／入力用電源もしくは出力用電源の消費電流(A)	電源ケーブル長における電圧降下(V)			
	1m	3m	5m	10m
9	0.80	2.40	4.00	8.00
8	0.71	2.13	3.56	7.11
6	0.53	1.60	2.67	5.33
4	0.36	1.07	1.78	3.56
3	0.27	0.80	1.33	2.67
2	0.18	0.53	0.89	1.78
1	0.09	0.27	0.44	0.89

ユニット／入力用電源と出力用電源の電圧が降下しても、セーフティ I/O ターミナルや外部接続機器の電圧仕様を満足するように設計してください。

使用上の注意

ここでは計算例を示しています。お客様の装置・設備は、さまざまであるため、お客様の使用状態にあわせた計算をしてください。

● 電圧降下の計算例

以下の条件における、電圧降下の計算方法の例を説明します。

項目	条件
構成	前述の「直接供給での総消費電流の計算例 (P.4-8)」と同じとします。 そのため、ユニットごとの各電源における総消費電流の合計は以下となります。 • SXD1: 2.18A ユニット／入力用電源の総消費電流 : 1.14A 出力用電源の総消費電流 : 1.04A • SXD2: 1.72A ユニット／入力用電源の総消費電流 : 0.68A 出力用電源の総消費電流 : 1.04A • SXD3: 1.72A ユニット／入力用電源の総消費電流 : 0.68A 出力用電源の総消費電流 : 1.04A
外部接続機器の使用条件	
電源ケーブル長	• SXD1 に接続する電源ケーブル: 1m • SXD2 に接続する電源ケーブル: 3m • SXD3 に接続する電源ケーブル: 5m
外部供給電源の電源端子の電圧	• ユニット／入力用電源: DC24.0V • 出力用電源: DC24.0V

電源ケーブルでの電圧降下の表から、ユニットごとの各電源の電圧降下は、以下となります。

ユニット名	電圧降下	
	ユニット／入力用電源	出力用電源
SXD1	0.18V（ケーブル長 1m、消費電流 1.14A から、2A を適用）	0.18V（ケーブル長 1m、消費電流 1.04A から、2A を適用）
SXD2	0.27V（ケーブル長 3m、消費電流 0.68A から、1A を適用）	0.53V（ケーブル長 3m、消費電流 1.04A から、2A を適用）
SXD3	0.44V（ケーブル長 5m、消費電流 0.68A から、1A を適用）	0.89V（ケーブル長 5m、消費電流 1.04A から、2A を適用）

以上から、各ユニットに入力される各電源の電圧値を計算すると以下となります。

a. SXD1 に入力される各電源の電圧値
ユニット／入力用電源の電圧値
=24.0V-電源ケーブルの電圧降下
=24.0V-0.18V
=23.82V
出力用電源の電圧値
=24.0V-電源ケーブルの電圧降下
=24.0V-0.18V
=23.89V

b. SXD2 に入力される各電源の電圧値
ユニット／入力用電源の電圧値
=24.0V-電源ケーブルの電圧降下
=24.0V-0.27V
=23.73V
出力用電源の電圧値
=24.0V-電源ケーブルの電圧降下
=24.0V-0.53V

=23.47V

c. SXD3 に入力される各電源の電圧値
ユニット／入力用電源の電圧値
=24.0V-電源ケーブルの電圧降下
=24.0V-0.44V
=23.56V
出力用電源の電圧値
=24.0V-電源ケーブルの電圧降下
=24.0V-0.89V
=23.11V

いずれもセーフティ I/O ターミナルの各電源電圧仕様内（DC19.2～28.8V）であるため、問題ありません。接続するセーフティ入力機器やセーフティ出力機器の電圧仕様を満足していることも確認してください。この例では省略しています。
電圧仕様を満たさない場合は、電源ケーブル長や接続する外部機器を見直してください。

4-2-3 渡り配線による供給での設計方法

電源の供給方法が渡り配線による供給の場合の、電源供給の設計方法を説明します。

渡り配線による供給での設計手順

以下の設計条件(a)～(c)を満足することを確認します。確認方法については、参照先の説明を参照してください。

設計条件	確認方法の参照先
(a)ユニット／入力用電源と出力用電源の総消費電流の合計が、セーフティ I/O ターミナルの電源最大電流の範囲内であること。*1	「渡り配線による供給での総消費電流の計算方法 (P.4-12)」
(b)ユニット／入力用電源電圧が降下しても、セーフティ I/O ターミナルの入力回路仕様および外部接続機器の電圧仕様を満たすこと。*2	「渡り配線による供給での電圧降下の計算 (P.4-15)」
(c)出力用電源電圧が降下しても、セーフティ I/O ターミナルの出力回路仕様および外部接続機器の電圧仕様を満たすこと。*3	

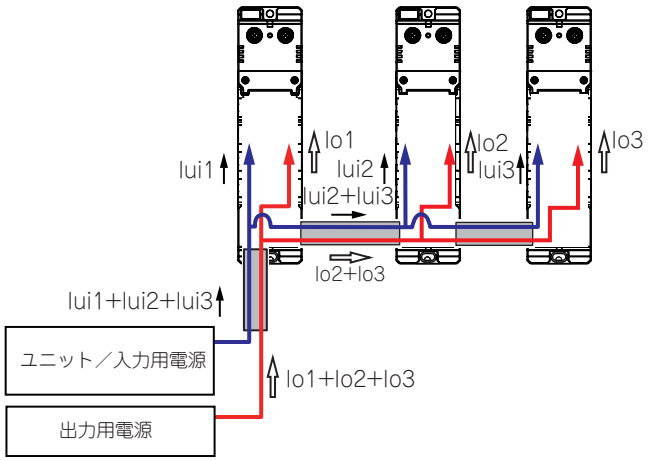
***1.** 電源最大電流は 9A です。9A を超えないようにします。
***2.** たとえば、セーフティ I/O ターミナルでは、ユニット／入力用電源電圧が、DC19.2～28.8V 内であることを確認します。
***3.** たとえば、セーフティ I/O ターミナルでは、出力用電源電圧が、DC19.2～28.8V 内であることを確認します。

渡り配線による供給での総消費電流の計算方法

渡り配線による供給の場合、直接供給の場合と異なり、外部供給電源を接続するセーフティ I/O ターミナルに、供給対象となる他のセーフティ I/O ターミナルの消費電流が全て流れることになります。すなわち、各ユニットの消費電流の合計が、セーフティ I/O ターミナルの電源最大電流を下回るように設計します。

以下に具体例を示します。この例では、次の式が満足していることを確認します。
セーフティ I/O ターミナルを左から SXD1、SXD2、SXD3 とします。

(Iui1+Iui2+Iui3+Io1+Io2+Io3)＜（SXD1 の電源最大電流*1）

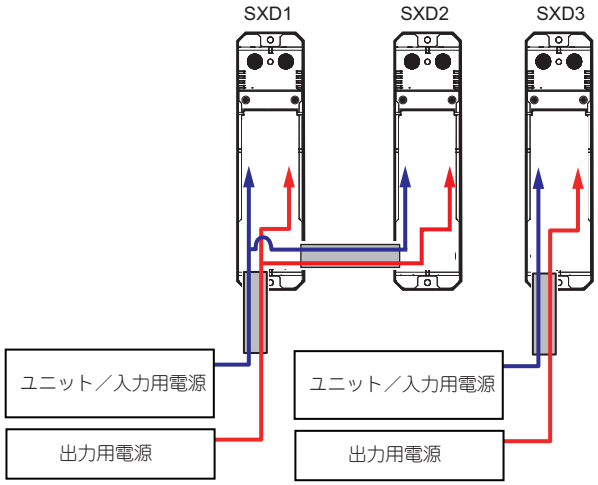


Iui1: SXD1 のユニット／入力用電源の総消費電流
Iui2: SXD2 のユニット／入力用電源の総消費電流
Iui3: SXD3 のユニット／入力用電源の総消費電流
Io1: SXD1 の出力用電源の総消費電流
Io2: SXD2 の出力用電源の総消費電流
Io3: SXD3 の出力用電源の総消費電流

***1.** SXD1 の電源最大電流を超えていなければ、SXD2 と SXD3 でも超えていないことになります。

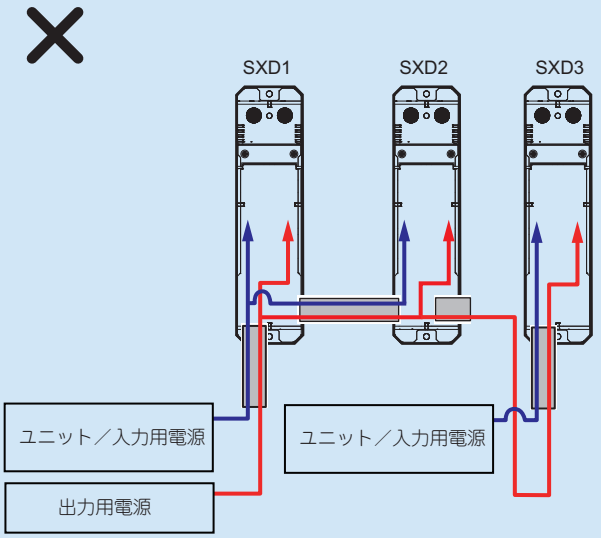
各ユニットのユニット／入力用電源または出力用電源の総消費電流の計算方法は、直接供給で説明している内容と同じです。「直接供給での総消費電流の計算方法 (P.4-7)」を参照してください。
計算し、条件を満たさない場合は、外部供給電源を追加して、条件を満足するようにしてください。

例: 外部供給電源を追加したシステム



使用上の注意

ユニット／入力用電源または出力用電源のいずれか一つだけを追加することはできません。



渡り配線による供給での総消費電流の計算例

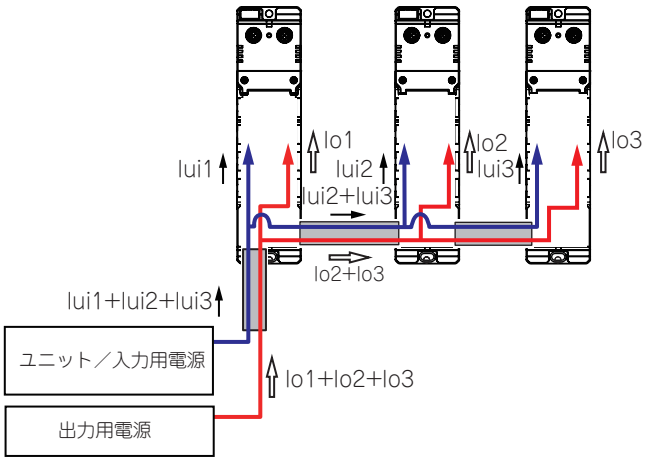
ある構成と使用条件を例に、渡り配線による供給での総消費電流の計算方法を以下に示します。

使用上の注意

ここでは計算例を示しています。お客様の装置・設備は、さまざまであるため、お客様の使用状態にあわせた計算をしてください。

● 構成例

セーフティ I/O ターミナルを左から SXD1、SXD2、SXD3 とします。



● 外部接続機器の使用条件

「直接供給での総消費電流の計算例 (P.4-8)」と同じ条件とします。

● 総消費電流の計算

「直接供給での総消費電流の計算例 (P.4-8)」のとおり、各ユニットの総消費電流は以下となります。

(1)SXD1 の総消費電流の合計
（SXD1 のユニット／入力用電源の総消費電流）＋（SXD1 の出力用電源の総消費電流）
(Iui1+Io1)
=(220mA+118mA+800mA)+(40mA+1000mA)
=(1138mA)+(1040mA)
≒(1.14A)+(1.04A)
=2.18A

(2)SXD2 の総消費電流の合計
（SXD2 のユニット／入力用電源の総消費電流）＋（SXD2 の出力用電源の総消費電流）
(Iui2+Io2)
=(220mA+59mA+400mA)+(40mA+1000mA)
=(679mA)+(1040mA)
≒(0.68A)+(1.04A)
=1.72A

(3)SXD3 の総消費電流の合計
SXD2 と同じです。
（SXD3 のユニット／入力用電源の総消費電流）＋（SXD3 の出力用電源の総消費電流）
(Iui3+Io3)
≒1.72A

外部供給電源が供給する各ユニットの総消費電流の合計は以下となります。
(Iui1+Iui2+Iui3+Io1+Io2+Io3)
=(2.18A+1.72A+1.72A)
=5.62A

計算結果がセーフティ I/O ターミナルの電源最大電流 9A を下回るため、この例では、問題ありません。

渡り配線による供給での電圧降下の計算

渡り配線による供給では、以下の要素によって、電圧降下が発生します。
- セーフティ I/O ターミナルの内部回路
- 電源ケーブル

渡り配線による供給では、セーフティ I/O ターミナル内に他のユニットの消費電流が流れるため、ユニットの内部回路による電圧降下が発生します。
オムロン製の M12 L コード電源ケーブル（形 XS5F-L521-□12-F、形 XS5W-L521-□12-F）を使用した場合、セーフティ I/O ターミナルの内部回路と電源ケーブルでの電圧降下は、ユニット／入力用電源と出力用電源で、下表となります。

ユニット／入力用電源の消費電流(A)	ユニットの内部回路での電圧降下(V)	電源ケーブル長における電圧降下(V)			
		1m	3m	5m	10m
9	0.40	0.80	2.40	4.00	8.00
8	0.36	0.71	2.13	3.56	7.11
6	0.27	0.53	1.60	2.67	5.33
4	0.18	0.36	1.07	1.78	3.56

ユニット／入力用電源の消費電流(A)	ユニットの内部回路での電圧降下(V)	電源ケーブル長における電圧降下(V)			
		1m	3m	5m	10m
3	0.13	0.27	0.80	1.33	2.67
2	0.09	0.18	0.53	0.89	1.78
1	0.04	0.09	0.27	0.44	0.89

出力用電源の消費電流(A)	ユニットの内部回路での電圧降下(V)	電源ケーブル長における電圧降下(V)			
		1m	3m	5m	10m
9	0.50	0.80	2.40	4.00	8.00
8	0.44	0.71	2.13	3.56	7.11
6	0.33	0.53	1.60	2.67	5.33
4	0.22	0.36	1.07	1.78	3.56
3	0.17	0.27	0.80	1.33	2.67
2	0.11	0.18	0.53	0.89	1.78
1	0.06	0.09	0.27	0.44	0.89

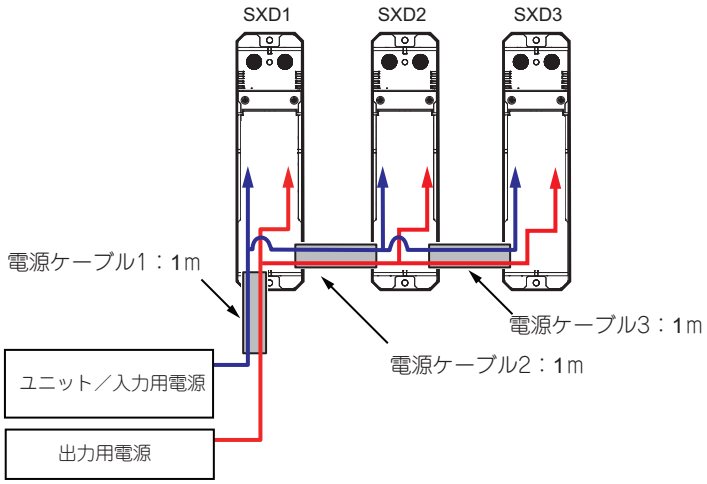
ユニット／入力用電源と出力用電源の電圧が降下しても、セーフティ I/O ターミナルや外部接続機器の電圧仕様を満足するように設計してください。

使用上の注意

ここでは計算例を示しています。お客様の装置・設備は、さまざまであるため、お客様の使用状態にあわせた計算をしてください。

● 電圧降下の計算例

以下の条件における、電圧降下の計算方法の例を説明します。

項目	条件
構成	前述の「渡り配線による供給での総消費電流の計算例 (P.4-14)」と同じとします。
外部接続機器の使用条件	
電源ケーブル長	以下とします。 
外部供給電源の電源端子の電圧	• ユニット入力用電源: DC24.0V • 出力用電源: DC24.0V

セーフティ I/O ターミナルの内部回路と電源ケーブルでの電圧降下の表から、ユニットごとの各電源の電圧降下は、以下となります。

ユニット名	ユニットの内部回路での電圧降下	電源ケーブルの電圧降下	備考
SXD1	−	• 電源ケーブル 1 の電圧降下: 0.53V	外部供給電源が供給する各ユニットの消費電流の合計 5.62A から、6A 時の電圧降下を適用します。
SXD2	SXD1 内部回路での電圧降下 • ユニット／入力用電源 : 0.18V • 出力用電源 : 0.22V	• 電源ケーブル 1 の電圧降下: 0.53V • 電源ケーブル 2 の電圧降下: 0.36V	電源ケーブル 1 での電圧降下は、SXD1 の値を適用します。 電源ケーブル 2 と SXD1 内部回路での電圧降下は、以下の電流値を適用します。 （外部供給電源が供給する各ユニットの消費電流の合計）-（SXD1 の総消費電流の合計）=5.62A-2.18A=3.44A よって 4A の値を適用します。
SXD3	SXD1 内部回路での電圧降下 • ユニット／入力用電源 : 0.18V • 出力用電源 : 0.22V SXD2 内部での電圧降下 • ユニット／入力用電源 : 0.09V • 出力用電源 : 0.11V	• 電源ケーブル 1 の電圧降下: 0.53V • 電源ケーブル 2 の電圧降下: 0.36V • 電源ケーブル 3 の電圧降下: 0.18V	電源ケーブル 1 と電源ケーブル 2 での電圧降下および SXD1 内部回路での電圧降下は、SXD1 と SXD2 の値を適用します。 電源ケーブル 3 と SXD2 内部回路での電圧降下は、以下の電流値を適用します。 （外部供給電源が供給する各ユニットの消費電流の合計）-（SXD1 と SXD2 の総消費電流の合計） =5.62A-2.18A-1.72A=1.72A よって 2A の値を適用します。

以上から、各ユニットに入力される各電源の電圧値を計算すると以下となります。

a. SXD1 に入力される各電源の電圧値
ユニット／入力用電源の電圧値
=24.0V-電源ケーブル 1 の電圧降下
=24.0V-0.53V
=23.47V
出力用電源の電圧値
=24.0V-電源ケーブル 1 の電圧降下
=24.0V-0.53V
=23.47V

b. SXD2 に入力される各電源の電圧値
ユニット／入力用電源の電圧値
=24.0V-（電源ケーブル 1 の電圧降下+SXD1 内部回路での電圧降下+電源ケーブル 2 の電圧降下）
=24.0V-(0.53V+0.18V+0.36V)
=22.93V
出力用電源の電圧値
=24.0V-（電源ケーブル 1 の電圧降下+SXD1 内部回路での電圧降下+電源ケーブル 2 の電圧降下）
=24.0V-(0.53V+0.22V+0.36V)
=22.89V

c. SXD3 に入力される各電源の電圧値
ユニット／入力用電源の電圧値
=24.0V-（電源ケーブル 1 の電圧降下+SXD1 内部回路での電圧降下+電源ケーブル 2 の電圧降下
+SXD2 内部回路での電圧降下+電源ケーブル 3 での電圧降下）
=24.0V-(0.53V+0.18V+0.36V+0.09V+0.18V)

=22.66V
出力用電源の電圧値
=24.0V-（電源ケーブル 1 の電圧降下+SXD1 内部回路での電圧降下+電源ケーブル 2 の電圧降下+SXD2 内部回路での電圧降下+電源ケーブル 3 での電圧降下）
=24.0V-(0.53V+0.22V+0.36V+0.11V+0.18V)
=22.6V

いずれもセーフティ I/O ターミナルの各電源電圧仕様内（DC19.2～28.8V）であるため、問題ありません。接続するセーフティ入力機器やセーフティ出力機器の電圧仕様を満足していることも確認してください。この例では省略しています。
電圧仕様を満たさない場合は、電源ケーブル長や接続する外部機器を見直してください。

4-3 電源や保護機器の選定

セーフティ I/O ターミナルの外部供給電源であるユニット／入力用電源と出力用電源、および保護機器の選定について説明します。

4-3-1 外部供給電源の選定

外部供給電源の推奨電源と電源容量の選定について説明します。

使用する電源

セーフティ I/O ターミナルの外部供給電源のユニット／入力用電源と出力用電源には、以下の条件を満たす SELV 電源、またはオムロン製の耐環境型 IP67・パワーサプライ（形 S8NR-S シリーズ）を使用してください。

- 過電流保護機能を持つ
- 入出力間が二重または強化絶縁されている
- 出力電圧が DC24V（DC19.2～28.8V）である

推奨電源: 形 S8VK-S シリーズ（オムロン製）、形 S8NR-S シリーズ（オムロン製）

電源容量

「4-2 電源供給の設計方法 (P.4-6)」で説明した計算方法に従って、ユニット／入力用電源と出力用電源の各総消費電流を計算し、各電源の電源容量を算出してください。

安全上の要点

ユニット／入力用電源と出力用電源は、以下のとき突入電流が流れることがあります。

a. 電源投入時

b. 外部接続機器への電源供給開始時

c. 外部接続機器の ON/OFF 動作時

また、I/O ケーブルの短絡時、保護がかかるまでの間、過電流が流れることがあります。これらの電流を考慮し、十分に余裕を持った容量の電源を選定してください。突入電流により電源が立ち上がらなくなったり、電源が落ちたりすることがあります。

4-3-2 保護機器の選定

外部回路の短絡や過電流に備えるための保護機器（ブレーカやヒューズなど）の選定について説明します。
過電流とは、短絡や機器の故障など、以下の定格を超えて使用している状態で流れる電流です。

- ユニット／入力用電源と出力用電源共通：電源最大電流
- ユニット／入力用電源：テスト出力端子への定格電流
- 出力用電源：セーフティ出力機器への最大負荷電流

上記、定格値については、「2-1-4 ユニット仕様 (P.2-6)」を参照してください。

保護機器の選定方法

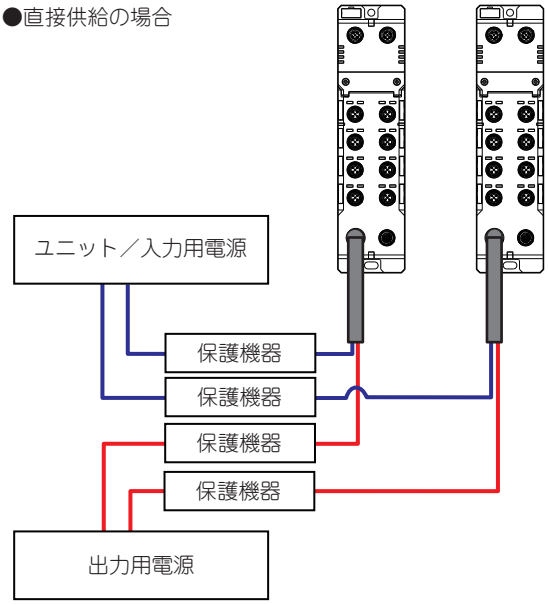
保護機器は以下を考慮して選定してください。

- 保護機器の仕様（遮断や溶断、検知特性、定常電流値など）
- 電源投入時の突入電流
- 外部接続機器への電源供給開始時の突入電流
- 外部接続機器の ON/OFF 動作による突入電流

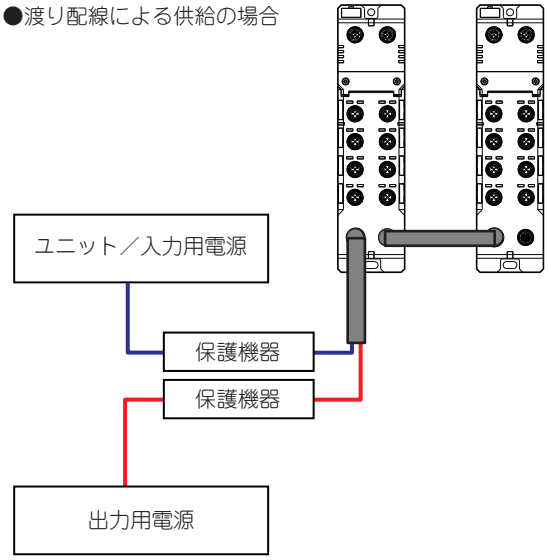
保護機器の取付箇所

保護機器は、ユニット／入力用電源と出力用電源ごとに下図のように取り付けてください。

●直接供給の場合



●渡り配線による供給の場合



5

取り付けと配線

この章では、セーフティ I/O ターミナルの取り付けと配線方法について説明しています。

5-1　ユニットの取り付け 5-2
5-1-1　取り付け時の注意事項 5-2
5-1-2　取り付け方向 5-2
5-1-3　取り付け方法 5-2

5-2　EtherNet/IP ネットワークの配線 5-4
5-2-1　敷設時の注意事項 5-4
5-2-2　通信ケーブルの接続 5-4

5-3　電源の配線 5-11
5-3-1　敷設時の注意事項 5-11
5-3-2　使用する電源ケーブルと締め付け工具・締め付けトルク 5-11
5-3-3　外部供給電源への電源ケーブルの接続 5-12
5-3-4　電源ケーブルの接続 5-13

5-4　I/O ケーブルの配線 5-17
5-4-1　敷設時の注意事項 5-17
5-4-2　I/O ケーブルの接続 5-17
5-4-3　配線例 5-22

5-5　接続関連機器 5-26
5-5-1　Ethernet ケーブル 5-26
5-5-2　電源コネクタ接続用ケーブル 5-28
5-5-3　I/O コネクタ接続用ケーブル 5-31
5-5-4　コネクタ用防水カバー 5-34

5-6　オプション品 5-35
5-6-1　マーカ 5-35

5-1 ユニットの取り付け

セーフティ I/O ターミナルの取り付けについて説明します。

5-1-1 取り付け時の注意事項

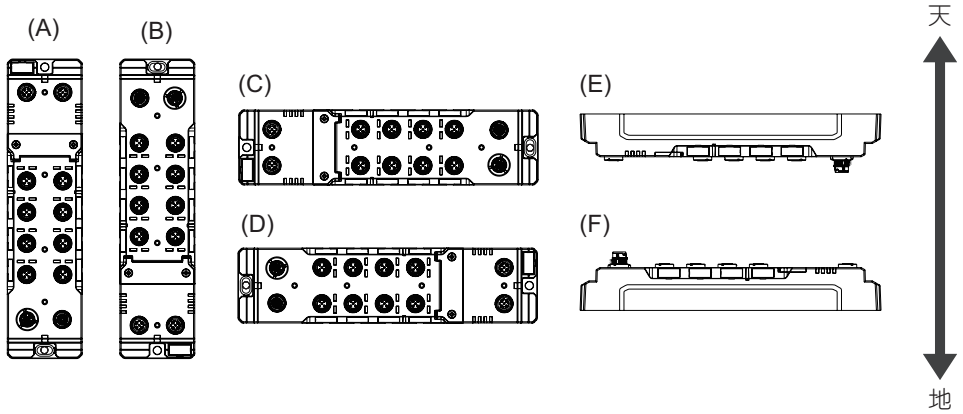
セーフティ I/O ターミナルの信頼性を高め、その機能を十分発揮するために、以下を考慮して設置してください。

次のような場所は避けて設置してください。
- 日光が直接当たる場所
- 周囲温度や相対湿度がユニットの仕様を超える場所
- 温度変化が急激で結露するような場所
- 腐食性ガス、可燃性ガスのある場所
- ちり、ほこり、塩分、鉄粉が多い場所
- 酸、油、薬品などのひまつがかかる場所
- 本体に直接振動や衝撃が伝わる場所
- 動力線が近くを通る場所

次のような場所で使用する際は、遮へい対策を十分に行ってください。
- 静電気などによるノイズが発生する場所
- 強い電界や磁界が生じる場所
- 放射線を被ばくするおそれのある場所
- 電源線が近くを通る場所

5-1-2 取り付け方向

セーフティ I/O ターミナルは以下の 6 方向で取り付けできます。

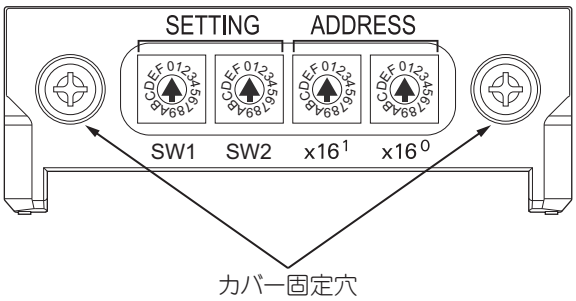


5-1-3 取り付け方法

セーフティ I/O ターミナルの以下の取り付け方法について説明します。
- ロータリスイッチ用カバーの取り付け
- ユニット本体の取り付け

ロータリスイッチ用カバーの取り付け

ロータリスイッチ用カバーを固定するために、2 箇所のカバー固定穴をねじ止めしてください。



M3 ねじを使用し、以下のトルクで締め付けてください。以下の締め付けトルクでねじが締め付けられているときに、保護構造 IP67 を保つことができます。

締め付け箇所	ねじのサイズ	締め付けトルク
ロータリスイッチ用カバーの固定穴	M3	0.4～0.6N·m

使用上の注意

- ねじに油分を付着させないようにしてください。油分が付着すると、ねじ破損の原因となります。
- ねじの締め付けは適正なドライバで行ってください。適正でないドライバでの締め付けはねじ破損の原因となります。

参考

工場出荷時は、カバーが固定されています。

ユニット本体の取り付け

セーフティ I/O ターミナルの 2 箇所のユニット取付穴をねじ止めしてください。
取付穴はユニットの上下にあります。取り付け寸法についての詳細は、「A-1 外形寸法 (P.A-2)」を参照してください。
M5 ねじを使用し、以下のトルクで締め付けてください。

締め付け箇所	ねじのサイズ	締め付けトルク
ユニット取付穴	M5	1.47～1.96N·m

使用上の注意

- 正しく固定してください。固定が不十分な場合、振動の影響を受け、故障の原因となる場合があります。
- ねじに油分を付着させないようにしてください。油分が付着すると、ねじ破損の原因となります。
- ねじの締め付けは適正なドライバで行ってください。適正でないドライバでの締め付けはねじ破損の原因となります。

5-2 EtherNet/IP ネットワークの配線

セーフティ I/O ターミナルの EtherNet/IP ネットワークの敷設方法について説明します。

5-2-1 敷設時の注意事項

セーフティ I/O ターミナルの EtherNet/IP ネットワーク敷設時の基本的な注意事項は、以下のとおりです。

ネットワーク敷設時の注意事項

- EtherNet/IP ネットワーク敷設工事を行うときは、十分な安全対策を講じたうえ、規格に従った敷設を行ってください。(「JIS X5252」または「電気設備技術基準」参照)
  敷設工事は、安全対策および規格に詳しい専門業者に依頼されることをおすすめします。
- EtherNet/IP ネットワーク機器は、ノイズを発生する機器の近くに敷設しないでください。やむを得ずノイズの多い環境に敷設する場合は、各機器を金属ケースに収納するなどのノイズ対策を必ず施してください。

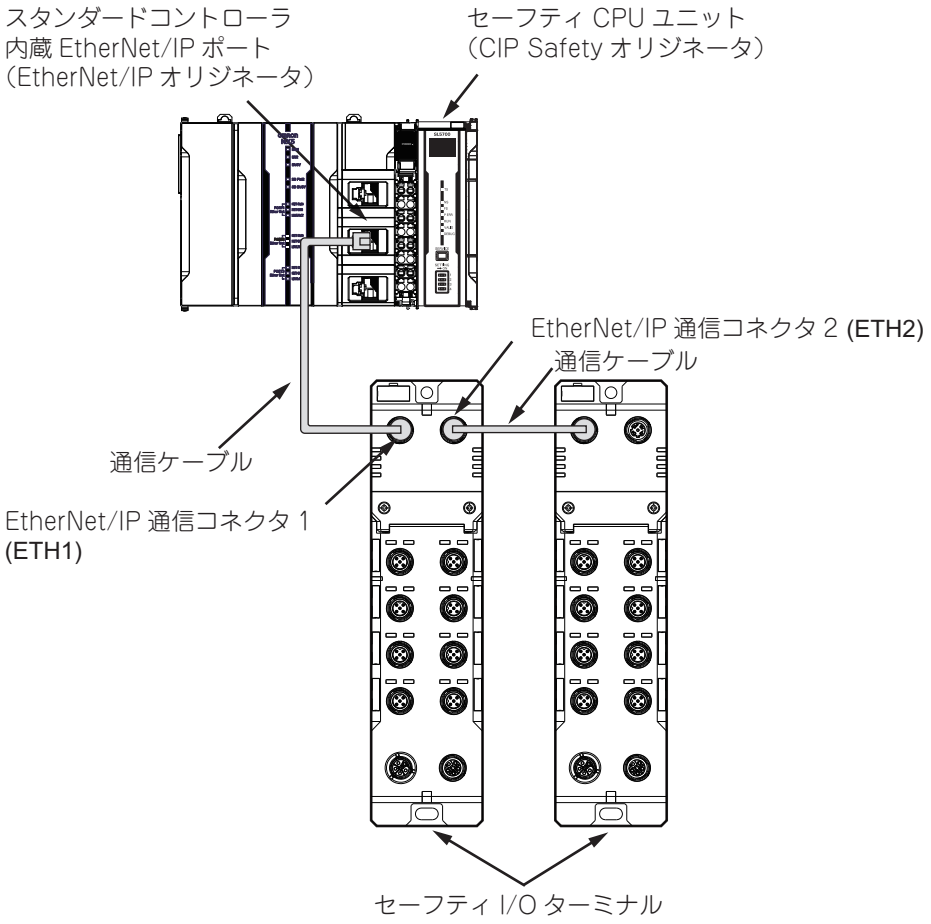
通信ケーブル敷設時の注意事項

- セーフティ I/O ターミナルの保護構造 IP67 を保つために、使用する通信コネクタには、「5-5-1 Ethernet ケーブル (P.5-26)」で紹介している通信ケーブルを使用してください。
- セーフティ I/O ターミナルの保護構造 IP67 を保つために、未使用の通信コネクタには、「5-5-4 コネクタ用防水カバー (P.5-34)」で紹介している防水カバーを使用してください。
- ねじ式コネクタを用いる場合、正しい配線工具を用いて規定のトルク値で締め付けてください。
- RJ45 モジュラコネクタの通信コネクタを持つ機器に接続するときは、通信ケーブルのコネクタをロックするまで確実に差し込んでください。
- 使用する通信ケーブルについて、下記の事項を確認してください。
  断線がないか
  ショートしていないか
  コネクタの接続に問題がないか
- 通信ケーブルは、高圧電線と区別して敷設、配線してください。
- ノイズを発生する機器の近くには敷設しないでください。
- 高温多湿の環境には敷設しないでください。
- ほこりやオイルミストなどのない場所で使用してください。
- 通信ケーブルの曲げ半径には制限があります。曲げ半径については、使用する通信ケーブルの仕様を確認してください。
- ケーブルのシールドと両端のコネクタフードが接続されていない通信ケーブルを使用すると耐ノイズ性能が低下する場合があります。通信ケーブルは、接続関連機器で紹介している Ethernet ケーブルを使用してください。これらの通信ケーブルは、ケーブルのシールドと両端のコネクタフードが接続されています。

5-2-2 通信ケーブルの接続

EtherNet/IP ネットワークは、接続形態を選ばず自由な結線が可能です。
下図はライン形トポロジの接続例です。

EtherNet/IP オリジネータ側からの通信ケーブルを最初のセーフティ I/O ターミナルの通信コネクタに接続します。次に、最初のユニットのもうひとつの通信コネクタから、別の通信ケーブルを 2 番目のセーフティ I/O ターミナルの通信コネクタに接続します。



なお、通信コネクタの ETH1 および ETH2 の区別は不要です。スター接続でひとつのコネクタだけ使用する場合は、ETH1 および ETH2 のどちらでも接続できます。

スマートクリックコネクタによる接続手順

ここでは、スマートクリックコネクタタイプのケーブルによる接続手順および取り外し手順について説明します。

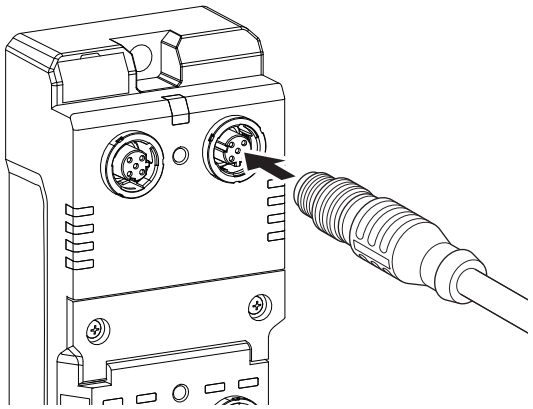
● 通信ケーブル

通信ケーブルには、「5-5-1 Ethernet ケーブル (P.5-26)」で紹介する Ethernet ケーブルを使用します。

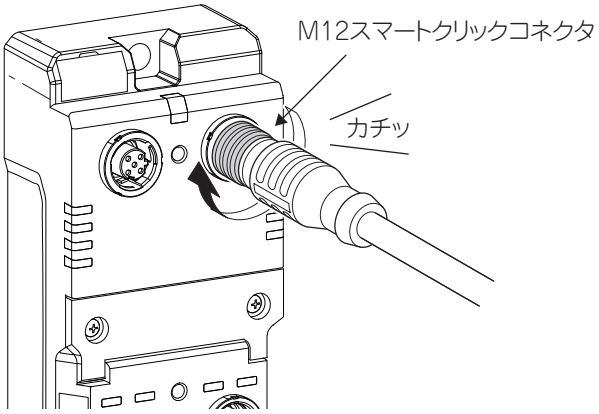
● 接続手順（スマートクリックコネクタ）

通信ケーブルの接続手順は以下のとおりです。通信ケーブルを接続する前に、セーフティ I/O ターミナルのユニット／入力用電源、出力用電源、および通信する相手機器の電源を OFF にしておいてください。

1 **通信コネクタの向きに注意して、Ethernet ケーブルの M12 プラグ側（オス）を、セーフティ I/O ターミナルの通信コネクタ（メス）に押し込みます。**



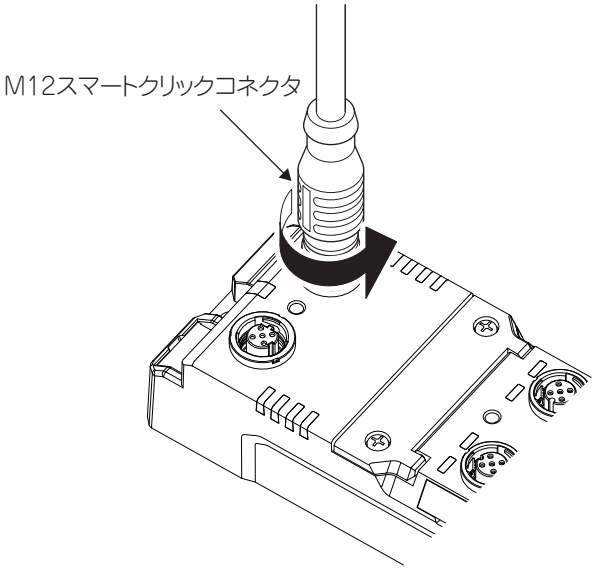
2 Ethernet ケーブルの M12 スマートクリックコネクタを奥まで差し込み、下図に示す方向に約 1/8 回転させます。



● 取り外し手順（スマートクリックコネクタ）

通信ケーブルの取り外し手順は以下のとおりです。通信ケーブルを取り外す前に、セーフティ I/O ターミナルのユニット／入力用電源、出力用電源、および通信する相手機器の電源を OFF にしておいてください。

1 Ethernet ケーブルの M12 スマートクリックコネクタを、下図に示す方向に約 1/8 回転させてケーブルを取り外します。



ねじ式コネクタによる接続手順

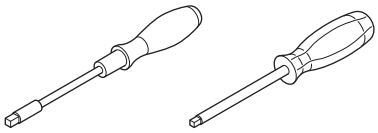
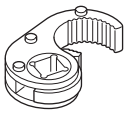
ここでは、ねじ式コネクタタイプのケーブルによる接続手順および取り外し手順について説明します。

● 通信ケーブル

通信ケーブルには、「5-5-1 Ethernet ケーブル (P.5-26)」で紹介する Ethernet ケーブルを使用します。

● 締め付け工具

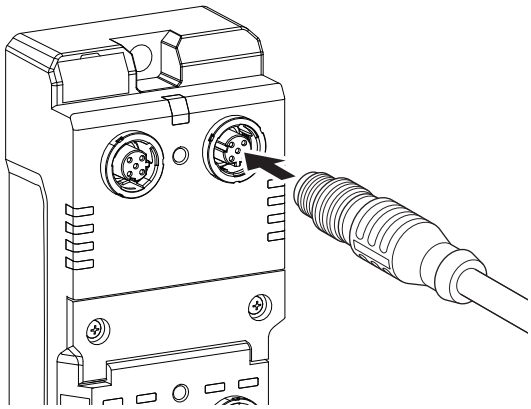
Ethernet ケーブルの M12 ねじ式コネクタを規定のトルク値で締め付けるときに、以下の工具を使用します。

品名／外観	メーカ	形式
• M12 トルクレンチ 本体、トルク値変更工具  • M12 アタッチメント 	ワイドミュラー	Screwty-M12-DM

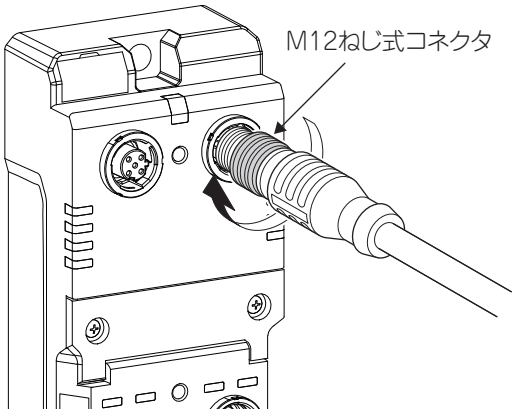
● 接続手順（ねじ式コネクタ）

通信ケーブルの接続手順は以下のとおりです。通信ケーブルを接続する前に、セーフティ I/O ターミナルのユニット／入力用電源、出力用電源、および通信する相手機器の電源を OFF にしておいてください。

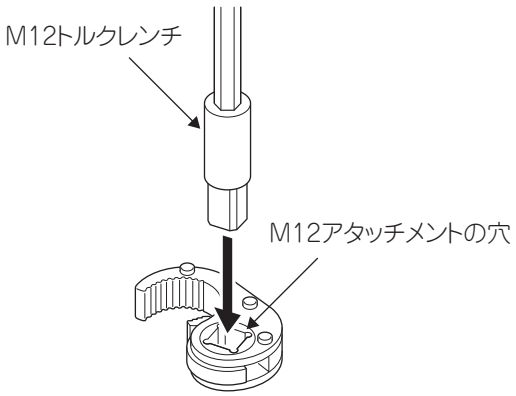
1 通信コネクタの向きに注意して、Ethernet ケーブルの M12 プラグ側（オス）を、セーフティ I/O ターミナルの通信コネクタ（メス）に押し込みます。



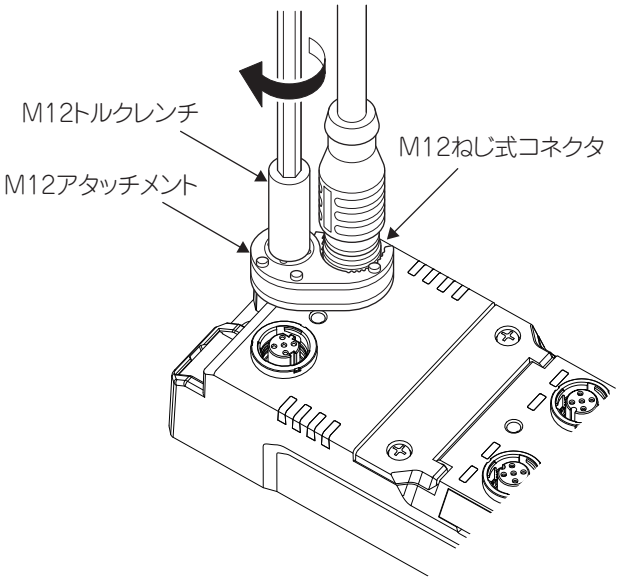
2 **Ethernet ケーブルの M12 ねじ式コネクタを下図に示す方向に回して締めます。規定のトルクで締め付ける前に締めておきます。**



3 **M12 アタッチメントの締め付け用穴に、規定のトルク値に設定した M12 トルクレンチを差し込みます。締め付け時の M12 アタッチメントの向きは、下図の向きで差し込みます。**
規定のトルク値は、「締め付けトルク (P.5-10)」を参照してください。



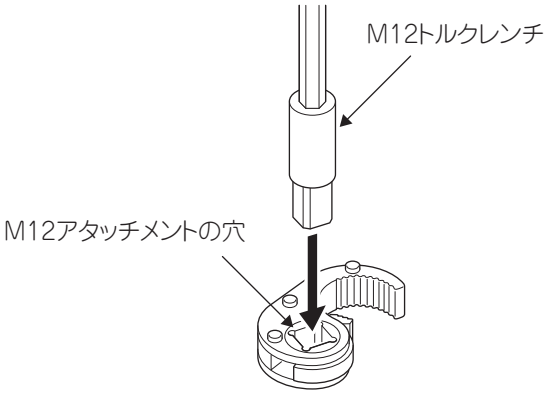
4 **M12 アタッチメントを Ethernet ケーブルの M12 ねじ式コネクタに装着します。装着後、M12 トルクレンチを下図に示す方向に回して、M12 ねじ式コネクタを規定のトルクで締め付けます。**



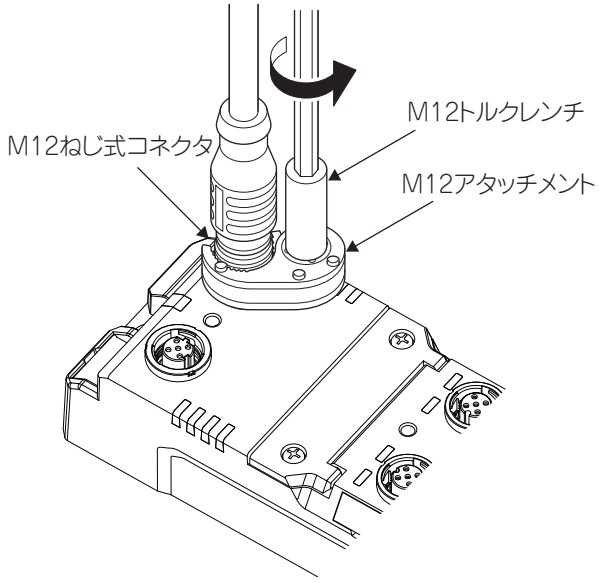
● **取り外し手順（ねじ式コネクタ）**

通信ケーブルの取り外し手順は以下のとおりです。通信ケーブルを取り外す前に、セーフティ I/O ターミナルのユニット／入力用電源、出力用電源、および通信する相手機器の電源を OFF にしておいてください。

1 **M12 アタッチメントの締め付け用穴に、M12 トルクレンチを差し込みます。取り外し時の M12 アタッチメントの向きは、接続時の向きと上下を逆さまにします。**



2 **M12 アタッチメントを Ethernet ケーブルの M12 ねじ式コネクタに装着します。装着後、M12 トルクレンチを下図に示す方向に回して、M12 ねじ式コネクタを緩めます。**



3 **Ethernet ケーブルの M12 ねじ式コネクタを取り付けと反対の向きに回して、ケーブルを取り外します。**

締め付けトルク

Ethernet ケーブルの M12 ねじ式コネクタは、以下のトルクで締め付けてください。
適切なトルクでねじ式コネクタが締められているときに、保護構造 IP67 を保つことができます。

締め付け箇所	ねじのサイズ	締め付けトルク
EtherNet/IP 通信コネクタ	M12	0.5～0.6N·m*1

***1.** スマートクリックコネクタタイプの場合、トルク管理不要です。コネクタを奥まで差し込み約 1/8 回転させてください。

防水カバー

未使用の EtherNet/IP 通信コネクタには、「5-5-4 コネクタ用防水カバー (P.5-34)」で紹介する防水カバーを取り付けてください。

5-3 電源の配線

セーフティ I/O ターミナルのユニット／入力用電源および出力用電源の配線について説明します。

⚠ 警告

- ユニットおよびスレーブに入力する電圧や電流は定められた範囲で入力してください。範囲外の電圧や電流を使用すると故障や火災の原因となります。
- このマニュアルに示すとおり、正しく電源の設計や配線を行ってください。範囲外の電圧／電流の入力や誤配線は、故障や火災の原因となります。

5-3-1 敷設時の注意事項

セーフティ I/O ターミナルの各電源の敷設時の注意事項は、以下のとおりです。

- セーフティ I/O ターミナルの保護構造 IP67 を保つために、電源コネクタには、「5-5-2 電源コネクタ接続用ケーブル (P.5-28)」で紹介しているねじ式コネクタタイプの電源ケーブルを使用してください。
- セーフティ I/O ターミナルの保護構造 IP67 を保つために、未使用の電源コネクタには、「5-5-4 コネクタ用防水カバー (P.5-34)」で紹介している防水カバーを使用してください。
- 高温多湿の環境には敷設しないでください。
- ほこりやオイルミストなどのない場所で使用してください。
- 電源ケーブルの曲げ半径には制限があります。曲げ半径については、使用する電源ケーブルの仕様を確認してください。

5-3-2 使用する電源ケーブルと締め付け工具・締め付けトルク

ここでは、セーフティ I/O ターミナルで使用する電源ケーブルと締め付け工具・締め付けトルクについて説明します。

● 電源ケーブル

電源ケーブルには、「5-5-2 電源コネクタ接続用ケーブル (P.5-28)」で紹介する電源コネクタ接続用ケーブルを使用します。

● 締め付け工具

ねじ式コネクタタイプの電源ケーブルを使用する場合、各メーカが推奨する締め付け工具を使用してください。
スマートクリックコネクタタイプの電源ケーブルの場合、締め付け工具は不要です。

● 締め付けトルク

ねじ式コネクタタイプの電源ケーブルを使用する場合、以下のトルクで締め付けてください。適切なトルクでねじ式コネクタが締められているとき、保護構造 IP67 を保つことができます。

締め付け箇所	ねじのサイズ	締め付けトルク
電源コネクタ	M12	0.39～0.49N·m*1

***1.** スマートクリックコネクタタイプの場合、トルク管理不要です。コネクタを奥まで差し込み約 1/8 回転させてください。

5-3-3 外部供給電源への電源ケーブルの接続

外部供給電源には、「5-5-2 電源コネクタ接続用ケーブル (P.5-28)」で紹介する電源ケーブルを使用します。ここでは、オムロン製の M12 L コード電源ケーブル（形 XS5F-L521-□12-F、形 XS5W-L521-□12-F）を使用した場合の接続方法について説明します。

形 XS5W-L521-□12-F が両側コネクタケーブル、形 XS5F-L521-□12-F がバラ線ケーブルです。

電源ケーブルの M12 ソケット側（メス側）はセーフティ I/O ターミナルの電源コネクタ IN に、もう一方を電源ユニットへ接続します。

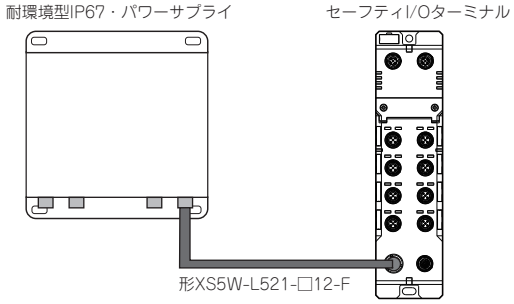
耐環境型 IP67・パワーサプライ（形 S8NR-S シリーズ）との接続

耐環境型 IP67・パワーサプライ（形 S8NR-S シリーズ）を使用する場合、両側コネクタの電源ケーブル（形 XS5W-L521-□12-F）を使用します。

以下は、形 XS5W-L521-□12-F の外観です。



以下となるように、M12 プラグ側（オス側）を耐環境型 IP67・パワーサプライへ接続してください。



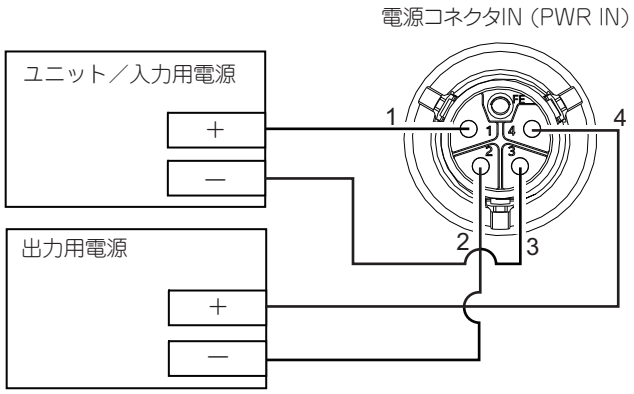
汎用電源ユニットとの接続

汎用の電源ユニットを使用する場合、バラ線の電源ケーブル（形 XS5F-L521-□12-F）を使用します。

以下は、形 XS5F-L521-□12-F の外観です。



以下の配線となるように、外部供給電源に電源ケーブルのバラ線側を接続してください。

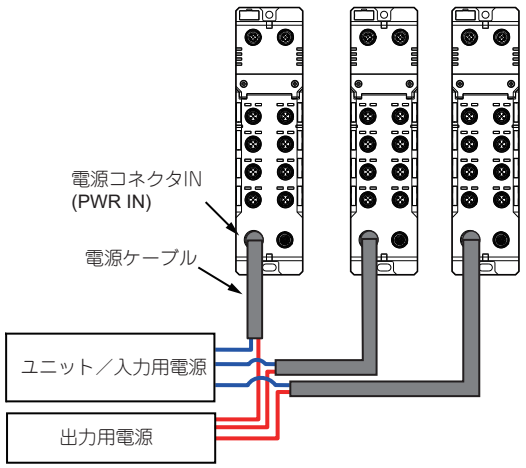


電源コネクタ IN の端子配列		外部供給電源の配線	電源ケーブルバラ線の色
ピン番号	信号名		
1	U/IN P+	ユニット／入力用電源+側を接続します。	茶
2	OUT P-	出力用電源-側を接続します。	白
3	U/IN P-	ユニット／入力用電源-側を接続します。	青
4	OUT P+	出力用電源+側を接続します。	黒
FE (Functional Earth)	FG	フレームグラウンド	灰

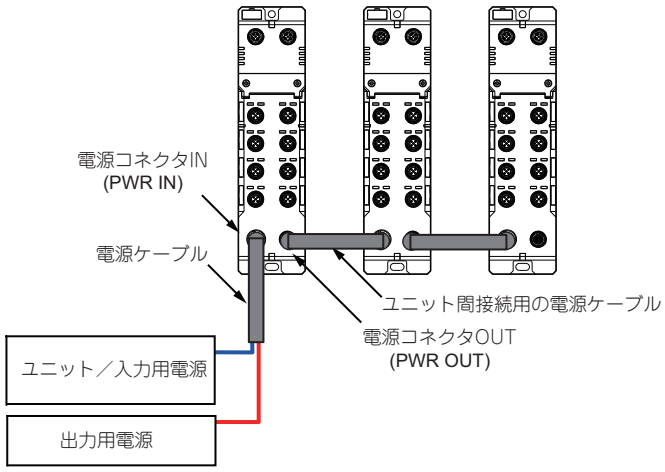
5-3-4 電源ケーブルの接続

セーフティ I/O ターミナルへの外部供給電源の供給方法は、以下の 2 種類があります。

- 直接供給



- 渡り配線による供給



直接供給の場合、セーフティ I/O ターミナルの電源コネクタ OUT を使用しません。
渡り配線の場合、セーフティ I/O ターミナルの電源コネクタ OUT を使用します。ただし、電源供給する最後のユニットの電源コネクタ OUT は使用しません。

電源供給方法の詳細は、「4-1-2 電源供給システム (P.4-2)」を参照してください。

安全上の要点

電源最大電流はユニット／入力用電源と出力用電源の合計で 9A です。電源最大電流を超えて使用しないでください。
電源最大電流を超えて使用すると、電源ケーブルに過剰な電流が流れることで、発火するおそれがあります。

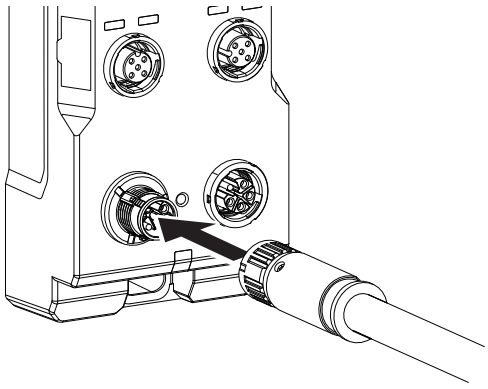
使用上の注意

ユニット／入力用電源を供給する電源と、出力用電源を供給する電源は、別々の電源から供給してください。同一の電源から供給すると、出力機器の負荷変動による誤動作の原因となることがあります。

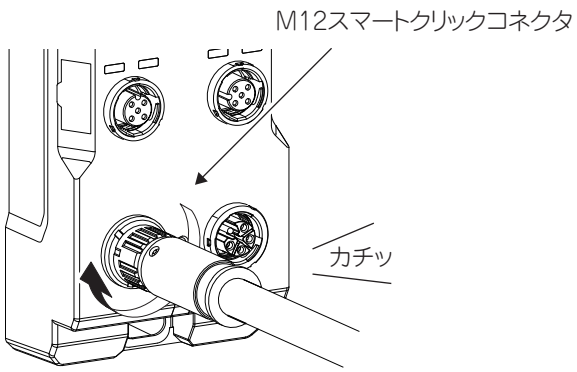
接続手順

ここでは、オムロン製の M12 L コード電源ケーブル（形 XS5F-L521-□12-F、形 XS5W-L521-□12-F）を使用した場合の接続手順について説明します。
電源ケーブルの接続手順は以下のとおりです。電源ケーブルを接続する前に、ユニット／入力用電源および出力用電源を OFF にしておいてください。

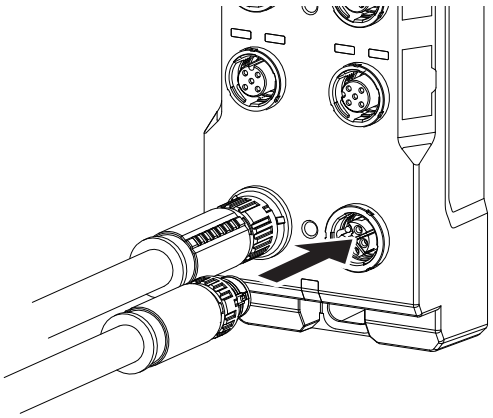
1 電源コネクタの向きに注意して、電源ケーブルの M12 ソケット側（メス）を、セーフティ I/O ターミナルの電源コネクタ IN（オス）に押し込みます。



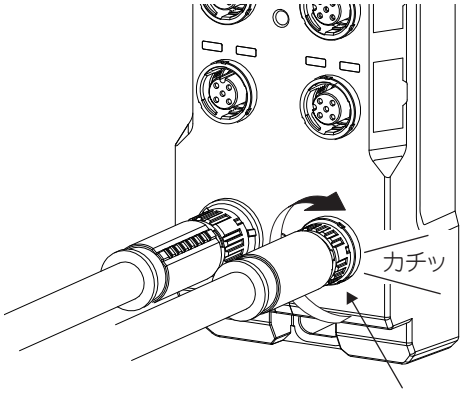
2 **電源ケーブルの M12 スマートクリックコネクタを奥まで差し込み、下図に示す方向に約 1/8 回転させます。**



3 **渡り配線による供給を行う場合は、電源コネクタの向きに注意して、電源ケーブルの M12 ソケット側（オス）を、セーフティ I/O ターミナルの電源コネクタ OUT（メス）に押し込みます。**



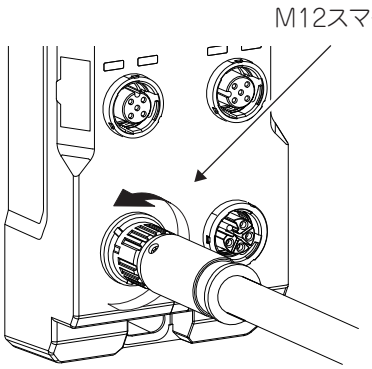
4 **電源ケーブルの M12 スマートクリックコネクタを奥まで差し込み、下図に示す方向に約 1/8 回転させます。**



取り外し手順

ここでは、オムロン製の M12 L コード電源ケーブル（形 XS5F-L521-□12-F、形 XS5W-L521-□12-F）を使用した場合の取り外し手順について説明します。
電源ケーブルの取り外し手順は以下のとおりです。電源ケーブルを取り外す前に、ユニット／入力用電源および出力用電源を OFF にしておいてください。

1 **電源ケーブルの M12 スマートクリックコネクタを、下図に示す方向に約 1/8 回転させてケーブルを取り外します。**



2 **渡り配線による供給を行う場合も同様の手順で取り外します。**

防水カバー

未使用の電源コネクタには、「5-5-4 コネクタ用防水カバー (P.5-34)」で紹介する防水カバーを取り付けてください。

5-4 I/O ケーブルの配線

セーフティ I/O ターミナルに外部機器を接続するための I/O ケーブルの配線方法について説明します。

5-4-1 敷設時の注意事項

セーフティ I/O ターミナルの I/O ケーブルの敷設時の注意事項は、以下のとおりです。

- セーフティ I/O ターミナルの保護構造 IP67 を保つために、I/O コネクタには、「スマートクリックコネクタタイプ (P.5-31)」や「ねじ式コネクタタイプ (P.5-33)」で紹介している I/O ケーブルを使用してください。
- セーフティ I/O ターミナルの保護構造 IP67 を保つために、未使用の I/O コネクタには、「5-5-4 コネクタ用防水カバー (P.5-34)」で紹介している防水カバーを使用してください。
- ねじ式コネクタを用いる場合、正しい配線工具を用いて規定のトルク値で締め付けてください。
- 高温多湿の環境には敷設しないでください。
- ほこりやオイルミストなどのない場所で使用してください。
- I/O ケーブルの曲げ半径には制限があります。曲げ半径については、使用する I/O ケーブルの仕様を確認してください。

5-4-2 I/O ケーブルの接続

I/O ケーブルの接続手順、取り外し手順、締め付けトルク、および防水カバーについて説明します。

スマートクリックコネクタによる接続手順

ここでは I/O ケーブルについて、スマートクリックコネクタタイプのケーブルによる接続手順および取り外し手順について説明します。

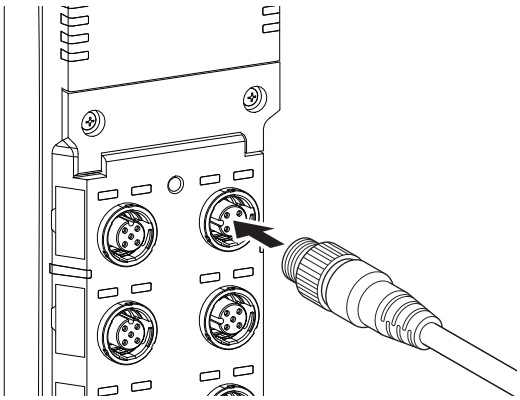
● I/O ケーブル

I/O ケーブルには、「スマートクリックコネクタタイプ (P.5-31)」で紹介する I/O コネクタ接続用ケーブルを使用します。

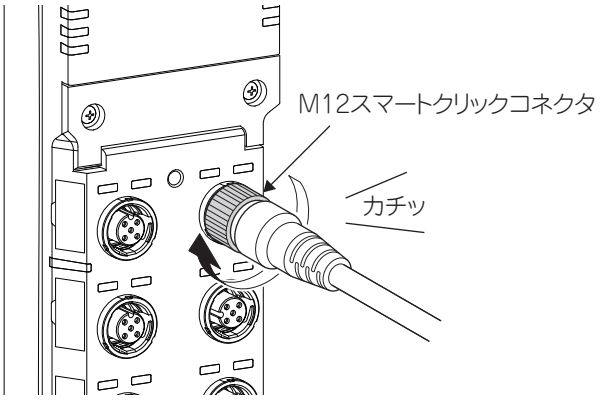
● 接続手順（スマートクリックコネクタ）

I/O ケーブルの接続手順は以下のとおりです。I/O ケーブルを接続する前に、セーフティ I/O ターミナルのユニット／入力用電源および出力用電源を OFF にしておいてください。

1 **I/O コネクタの向きに注意して、I/O ケーブルの M12 プラグ側（オス）を、セーフティ I/O ターミナルの I/O コネクタ（メス）に押し込みます。**



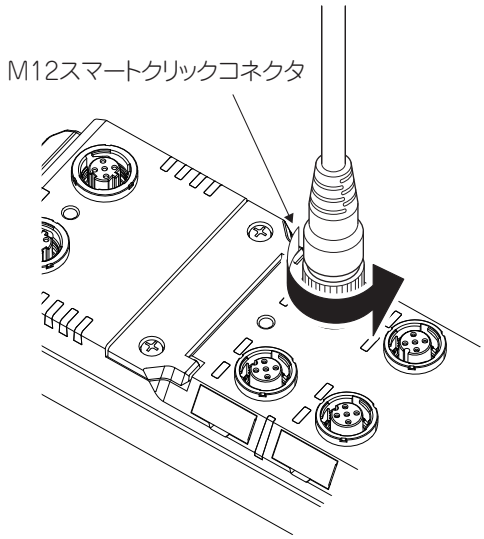
2 **I/O ケーブルの M12 スマートクリックコネクタを奥まで差し込み、下図に示す方向に約 1/8 回転させます。**



● 取り外し手順（スマートクリックコネクタ）

I/O ケーブルの取り外し手順は以下のとおりです。I/O ケーブルを取り外す前に、セーフティ I/O ターミナルのユニット／入力用電源および出力用電源を OFF にしておいてください。

1 **I/O ケーブルの M12 スマートクリックコネクタを、下図に示す方向に約 1/8 回転させてケーブルを取り外します。**



ねじ式コネクタによる接続手順

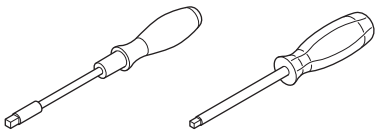
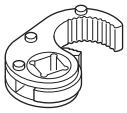
ここでは I/O ケーブルについて、ねじ式コネクタタイプのケーブルによる接続手順および取り外し手順について説明します。

● I/O ケーブル

I/O ケーブルには、「ねじ式コネクタタイプ (P.5-33)」で紹介する I/O コネクタ接続用ケーブルを使用します。

● 締め付け工具

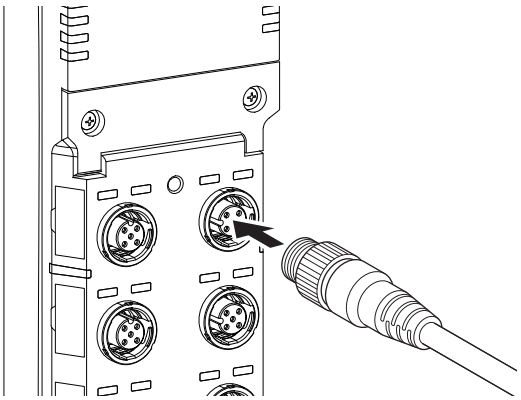
I/O ケーブルの M12 ねじ式コネクタを規定のトルク値で締め付けるときに、以下に示す工具を使用します。

品名／外観	メーカ	形式
• M12 トルクレンチ 本体、トルク値変更工具  • M12 アタッチメント 	ワイドミュラー	Screwty-M12-DM

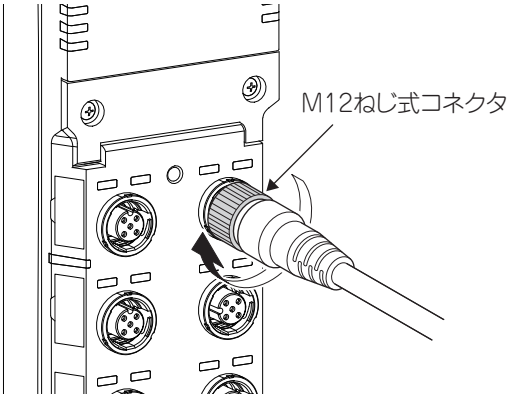
● 接続手順（ねじ式コネクタ）

I/O ケーブルの接続手順は以下のとおりです。I/O ケーブルを接続する前に、セーフティ I/O ターミナルのユニット／入力用電源および出力用電源を OFF にしておいてください。

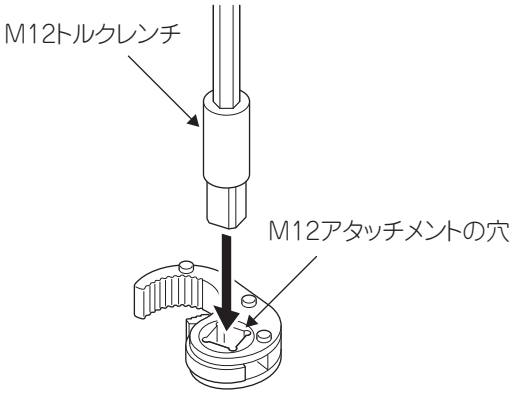
1 I/O コネクタの向きに注意して、I/O ケーブルの M12 プラグ側（オス）を、セーフティ I/O ターミナルの I/O コネクタ（メス）に押し込みます。



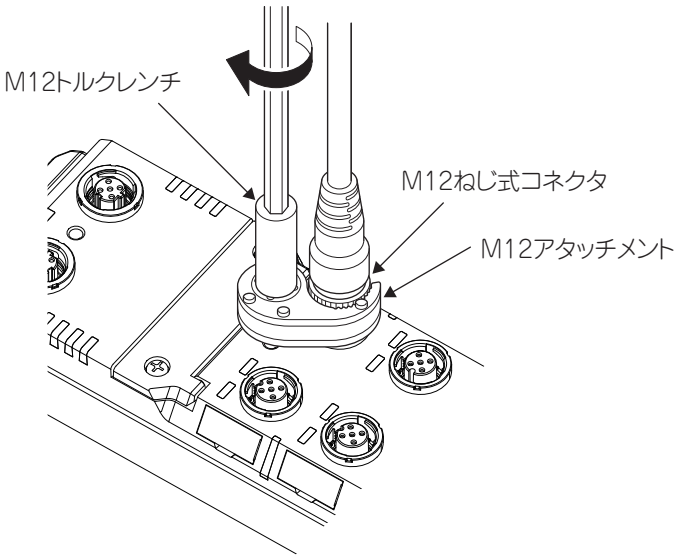
2 I/O ケーブルの M12 ねじ式コネクタを下図に示す方向に回して締めます。規定のトルクで締め付ける前に締めておきます。



3 **M12 アタッチメントの締め付け用穴に、規定のトルク値に設定した M12 トルクレンチを差し込みます。締め付け時の M12 アタッチメントの向きは、下図の向きで差し込みます。**
規定のトルク値は、「締め付けトルク (P.5-21)」を参照してください。



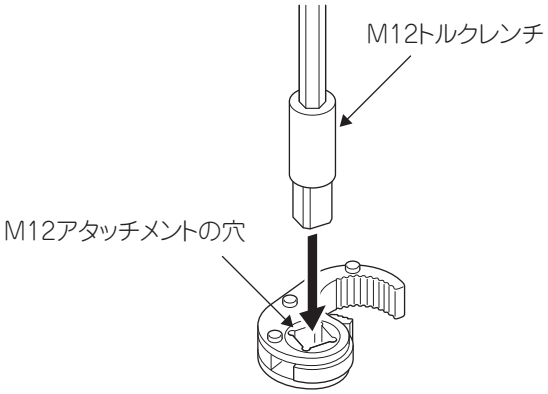
4 **M12 アタッチメントを I/O ケーブルの M12 ねじ式コネクタに装着します。装着後、M12 トルクレンチを下図に示す方向に回して、M12 ねじ式コネクタを規定のトルクで締め付けます。**



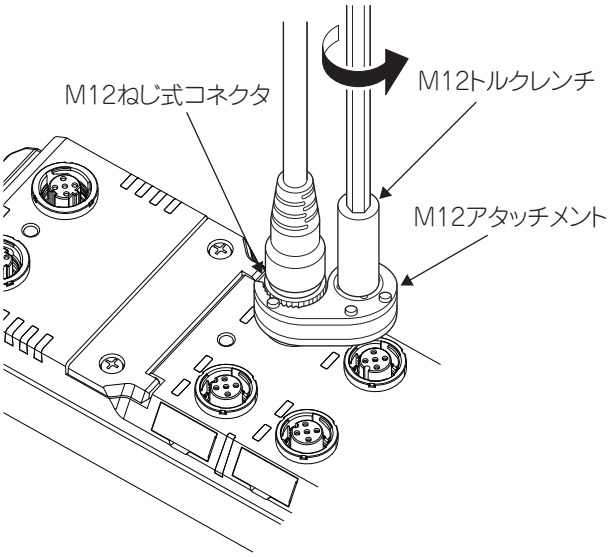
● 取り外し手順（ねじ式コネクタ）

I/O ケーブルの取り外し手順は以下のとおりです。I/O ケーブルを取り外す前に、セーフティ I/O ターミナルのユニット／入力用電源および出力用電源を OFF にしておいてください。

1 **M12 アタッチメントの締め付け用穴に、M12 トルクレンチを差し込みます。取り外し時の M12 アタッチメントの向きは、接続時の向きと上下を逆さまにします。**



2 **M12 アタッチメントを I/O ケーブルの M12 ねじ式コネクタに装着します。装着後、M12 トルクレンチを下図に示す方向に回して、M12 ねじ式コネクタを緩めます。**



3 **I/O ケーブルの M12 ねじ式コネクタを取り付けと反対の向きに回して、ケーブルを取り外します。**

締め付けトルク

I/O ケーブルの M12 ねじ式コネクタは、以下のトルクで締め付けてください。
適切なトルクでねじ式コネクタが締められているときに、保護構造 IP67 を保つことができます。

締め付け箇所	ねじのサイズ	締め付けトルク
I/O コネクタ	M12	0.5～0.6N·m*1

***1.** スマートクリックコネクタタイプの場合、トルク管理不要です。コネクタを奥まで差し込み約 1/8 回転させてください。

防水カバー

未使用の I/O コネクタには、「5-5-4 コネクタ用防水カバー (P.5-34)」で紹介する防水カバーを取り付けてください。

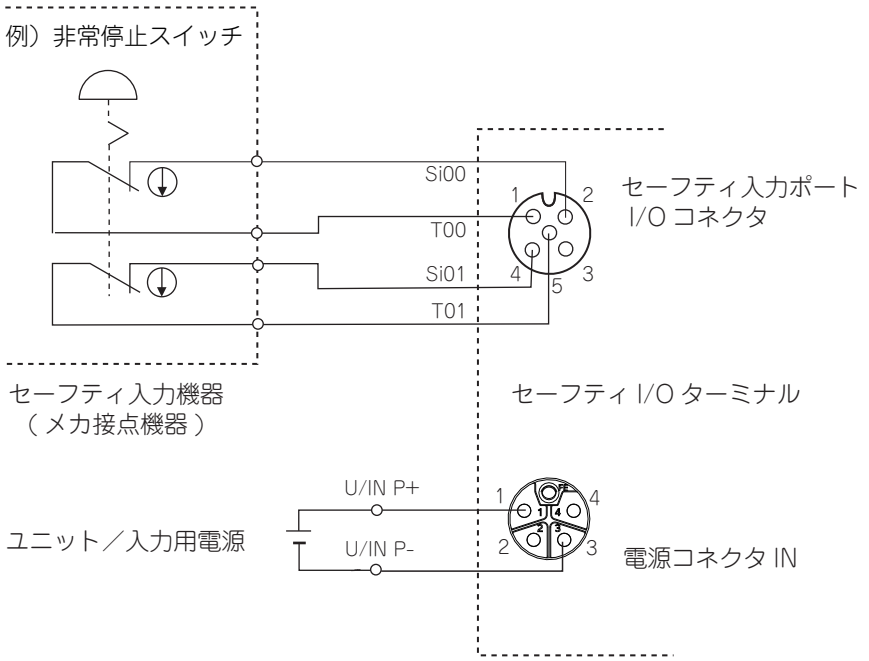
5-4-3 配線例

セーフティ I/O ターミナルの I/O コネクタと外部接続機器との配線例を以下に示します。

- セーフティ入力機器（メカ接点機器）の場合
- セーフティ入力機器（半導体出力機器）の場合
- セーフティ入力機器（セーフティライトカーテン）の場合
- セーフティ出力機器の場合
- DC 遮断 BOX（形 S8R-BB シリーズ）の場合
- ユニット間で I/O ケーブルを接続する場合

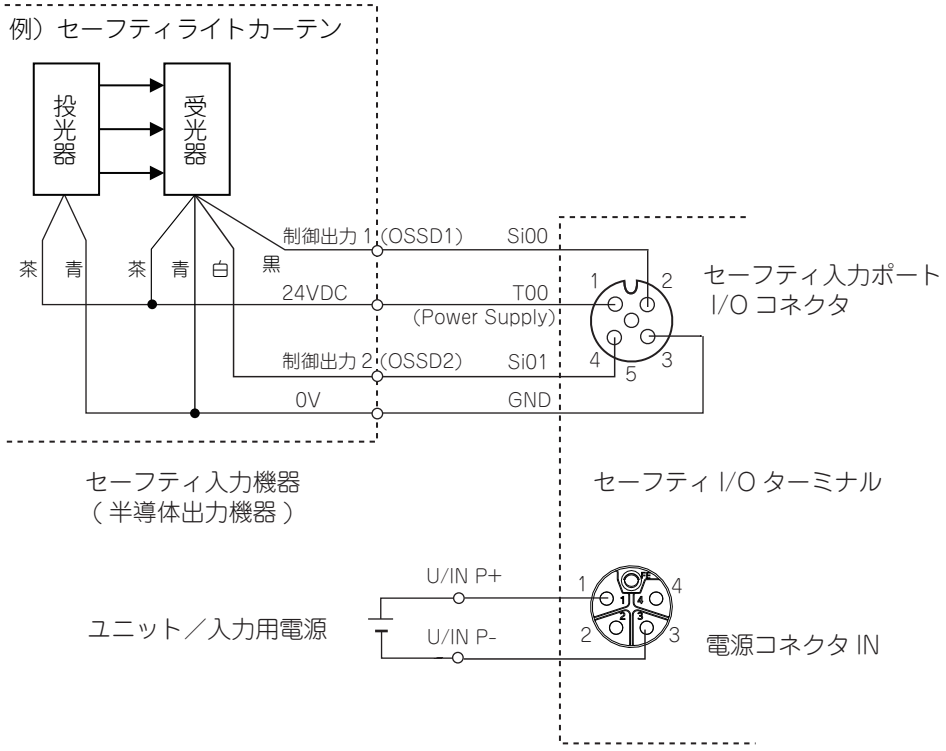
セーフティ入力機器（メカ接点機器）の場合

非常停止スイッチやセーフティリミットスイッチなどのメカ接点のセーフティ入力機器とセーフティ I/O ターミナルとの配線例を以下に示します。



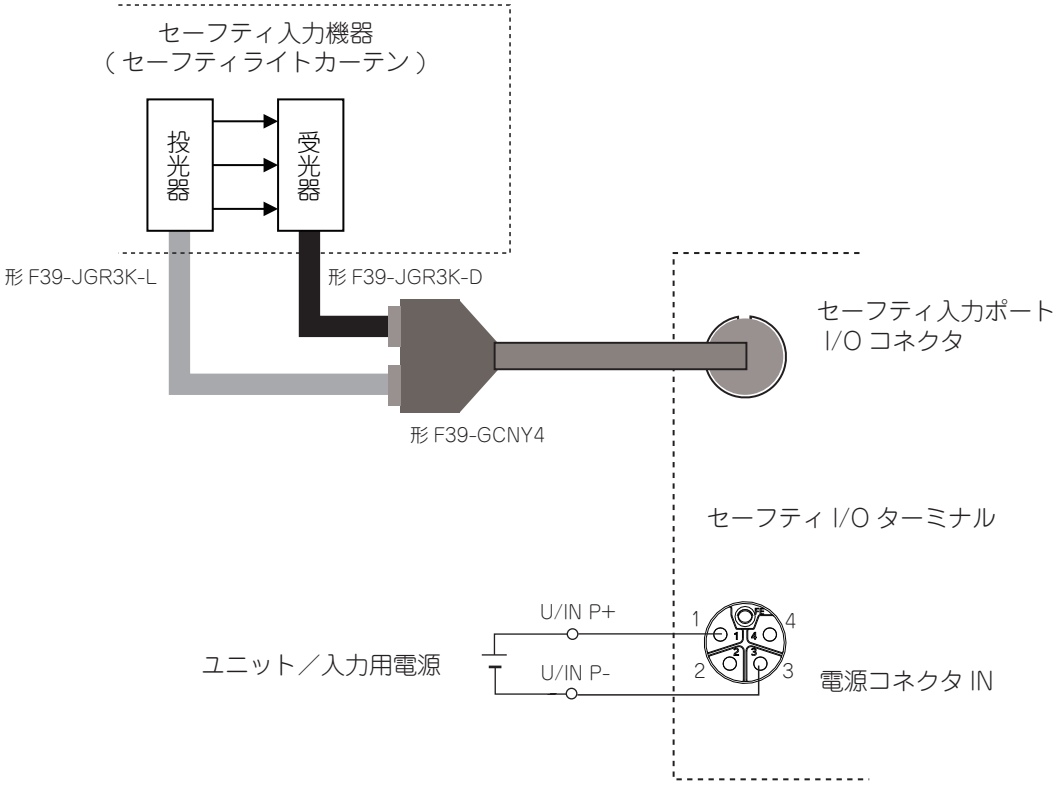
セーフティ入力機器（半導体出力機器）の場合

ライトカーテンなどの半導体出力のセーフティ入力機器とセーフティ I/O ターミナルとの配線例を以下に示します。



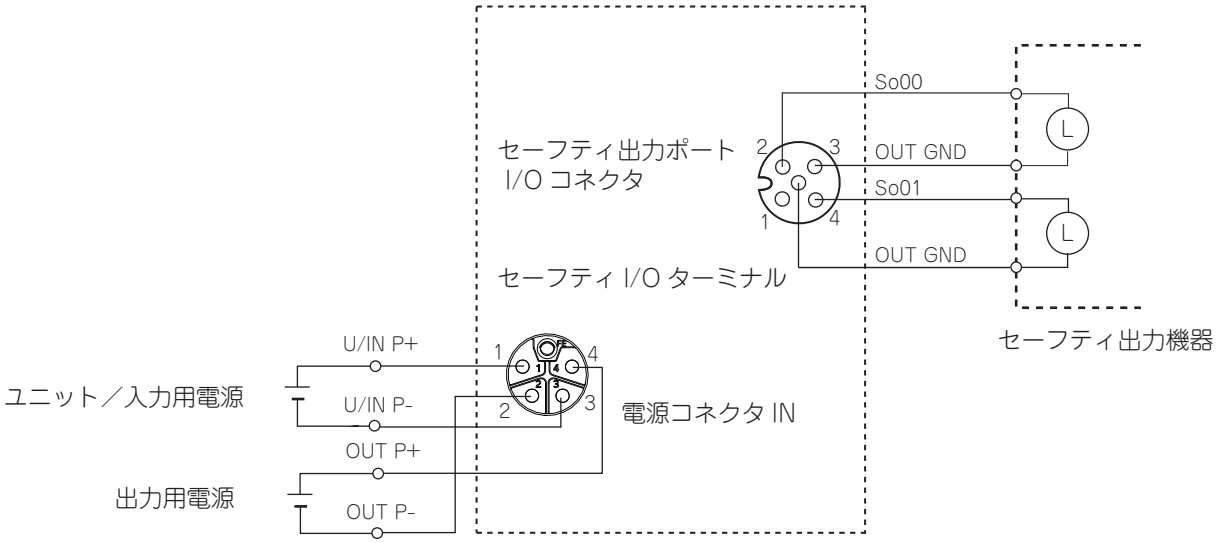
セーフティ入力機器（セーフティライトカーテン）の場合

ライトカーテンとの接続に形 F39-GCNY4 を使用した場合の配線例を以下に示します。



セーフティ出力機器の場合

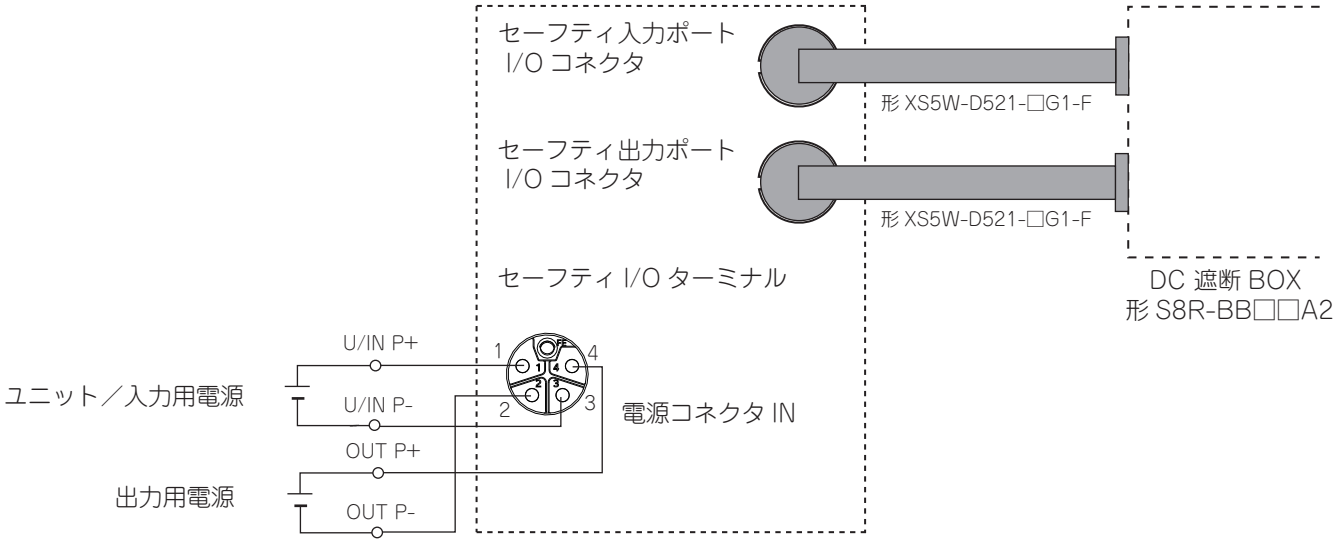
セーフティリレーなどのセーフティ出力機器とセーフティ I/O ターミナルとの配線例を以下に示します。
出力は PNP 出力です。



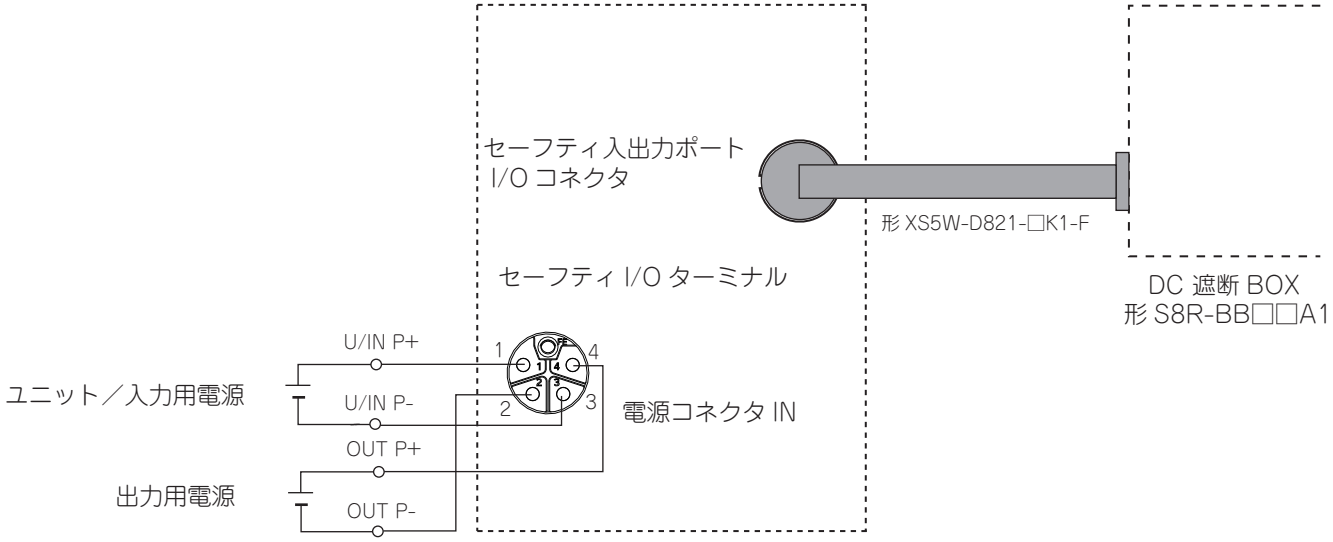
DC 遮断 BOX（形 S8R-BB シリーズ）の場合

DC 遮断 BOX（形 S8R-BB シリーズ）とセーフティ I/O ターミナルとの配線例は以下のとおりです。通信ケーブルを接続する前に、セーフティ I/O ターミナルのユニット／入力用電源、出力用電源、および通信する相手機器の電源を OFF にしておいてください。

● 形 NXR-SXD1204-CST の場合

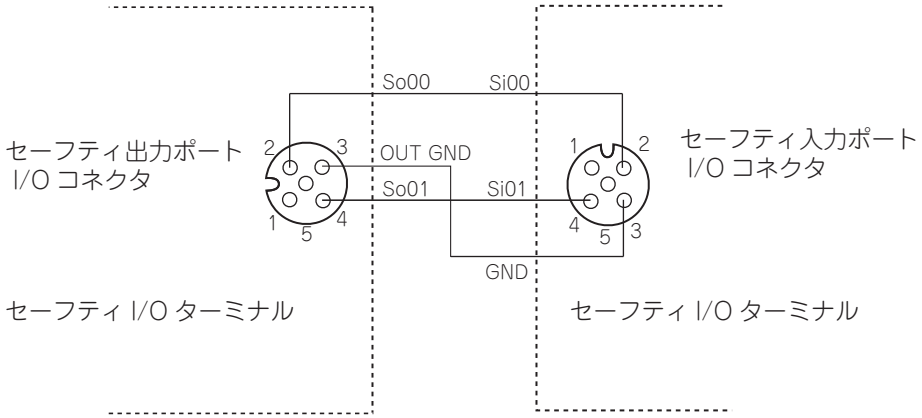


● 形 NXR-SXD1204B-CST の場合



ユニット間で I/O ケーブルを接続する場合

ユニット間でセーフティ I/O ポートを接続する場合の配線例を以下に示します。



使用上の注意

- ユニット間で I/O ケーブルを接続する場合、ピン番号 5 を接続しないでください。セーフティ入力ポートの［テスト出力］とセーフティ出力ポートの［出力用電源 -］が短絡しテスト出力端子過電流異常が発生します。
- ユニット間で 5 極仕様の I/O ケーブルを接続する場合、セーフティ入力端子設定でテスト出力モードを［Not Used］に設定してください。

5-5 接続関連機器

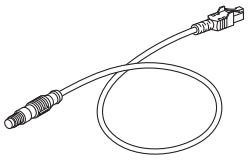
ここでは、セーフティ I/O ターミナルの配線に対する接続関連機器を紹介します。

5-5-1 Ethernet ケーブル

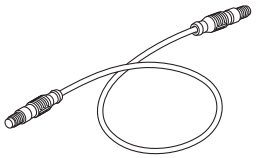
ここではセーフティ I/O ターミナルで使用する Ethernet ケーブルについて紹介します。
コネクタには以下があります。

- スマートクリックコネクタ
- ねじ式コネクタ

● セーフティ I/O ターミナルと RJ45 コネクタタイプの EtherNet/IP ターゲットとの接続用

品名／外観	メーカ	仕様	ケーブル芯線数	コネクタ種類	ケーブル引出方向	ケーブル長	形式
産業用イーサネットコネクタケーブル 	オムロン株式会社	M12 プラグ（D-coding、オス）－RJ45	4芯	スマートクリックコネクタ	ストレート／ストレート	0.5m	形 XS5W-T421-BMC-SS
						1m	形 XS5W-T421-CMC-SS
						2m	形 XS5W-T421-DMC-SS
						3m	形 XS5W-T421-EMC-SS
						5m	形 XS5W-T421-GMC-SS
						10m	形 XS5W-T421-JMC-SS
				ねじ式コネクタ		0.5m	形 XS2W-T421-BMC-SS
						1m	形 XS2W-T421-CMC-SS
						2m	形 XS2W-T421-DMC-SS
						3m	形 XS2W-T421-EMC-SS
						5m	形 XS2W-T421-GMC-SS
						10m	形 XS2W-T421-JMC-SS

● セーフティ I/O ターミナルどうしの接続用

品名／外観	メーカ	仕様	ケーブル芯線数	コネクタ種類	ケーブル引出方向	ケーブル長	形式
産業用イーサネットコネクタケーブル 	オムロン株式会社	M12 プラグ（D-coding、オス）－M12 プラグ（D-coding、オス）	4芯	スマートクリックコネクタ	ストレート／ストレート	0.5m	形 XS5W-T421-BM2-SS
						1m	形 XS5W-T421-CM2-SS
						2m	形 XS5W-T421-DM2-SS
						3m	形 XS5W-T421-EM2-SS
						5m	形 XS5W-T421-GM2-SS
						10m	形 XS5W-T421-JM2-SS
				ねじ式コネクタ		0.5m	形 XS2W-T421-BM2-SS
						1m	形 XS2W-T421-CM2-SS
						2m	形 XS2W-T421-DM2-SS
						3m	形 XS2W-T421-EM2-SS
						5m	形 XS2W-T421-GM2-SS
						10m	形 XS2W-T421-JM2-SS

5-5-2 電源コネクタ接続用ケーブル

ここではセーフティ I/O ターミナルで使用する電源コネクタ接続用ケーブルについて紹介します。
コネクタには以下があります。

- ねじ式コネクタ
- スマートクリックコネクタ

● ねじ式コネクタタイプ

ねじ式コネクタタイプの電源コネクタ接続用ケーブルについて紹介します。

品名／外観	メーカ	仕様	ケーブル芯線数	コネクタ種類	ケーブル引出方向	ケーブル長	形式
M12 L コード電源ケーブル(M12 ストレートメス-バラ線)	オムロン株式会社	M12 ソケット(L-coding、メス)ーバラ線	5芯	ねじ式コネクタ	ストレート	2m	形 XS2FP-L521-0200
						5m	形 XS2FP-L521-0500
						10m	形 XS2FP-L521-1000
	Murrelektronik GmbH	M12 ソケット(L-coding、メス)ーバラ線	5芯	ねじ式コネクタ	ストレート	2m	7000-P4221-P040200
						5m	7000-P4221-P040500
						10m	7000-P4221-P041000
M12 L コード電源ケーブル(M12 ストレートオス-M12 ストレートメス)	オムロン株式会社	M12 プラグ(L-coding、オス)ーM12 ソケット(L-coding、メス)	5芯	ねじ式コネクタ	ストレート／ストレート	2m	形 XS2WP-L521-0200
						5m	形 XS2WP-L521-0500
						10m	形 XS2WP-L521-1000
	Murrelektronik GmbH	M12 プラグ(L-coding、オス)ーM12 ソケット(L-coding、メス)	5芯	ねじ式コネクタ	ストレート／ストレート	2m	7000-P4241-P040200
						5m	7000-P4241-P040500
						10m	7000-P4241-P041000

● スマートクリックコネクタタイプ

スマートクリックコネクタタイプの電源コネクタ接続用ケーブルについて紹介します。形 XS5F-L521-□12-F、形 XS5W-L521-□12-F の保護構造は IP65 です。

品名／外観	メーカ	仕様	ケーブル芯線数	コネクタ種類	ケーブル引出方向	ケーブル長	形式
M12 L コード電源ケーブル(M12 ストレートメス-バラ線) 	オムロン株式会社	M12 ソケット(L-coding、メス)−バラ線	5芯	スマートクリックコネクタ	ストレート	0.5m	形 XS5F-L521-B12-F
						1m	形 XS5F-L521-C12-F
						2m	形 XS5F-L521-D12-F
						3m	形 XS5F-L521-E12-F
						5m	形 XS5F-L521-G12-F
						10m	形 XS5F-L521-J12-F
						15m	形 XS5F-L521-K12-F
						20m	形 XS5F-L521-L12-F

品名／外観	メーカ	仕様	ケーブル芯線数	コネクタ種類	ケーブル引出方向	ケーブル長	形式
M12 L コード電源ケーブル(M12 ストレートオス-M12 ストレートメス) 	オムロン株式会社	M12 プラグ(L-coding、オス)ーM12 ソケット(L-coding、メス)	5芯	スマートクリックコネクタ	ストレート／ストレート	0.5m	形 XS5W-L521-B12-F
						1m	形 XS5W-L521-C12-F
						2m	形 XS5W-L521-D12-F
						3m	形 XS5W-L521-E12-F
						5m	形 XS5W-L521-G12-F
						10m	形 XS5W-L521-J12-F
						15m	形 XS5W-L521-K12-F
						20m	形 XS5W-L521-L12-F

5-5-3 I/O コネクタ接続用ケーブル

ここではセーフティ I/O ターミナルで使用する I/O コネクタ接続用ケーブルについて紹介します。

直接接続または延長接続用ケーブル

M12 プラグのデバイスと直接接続するときに使用するケーブルです。また、M12 プラグのデバイスや外部機器からの延長接続でも使用します。
コネクタには以下があります。

- スマートクリックコネクタ
- ねじ式コネクタ

● スマートクリックコネクタタイプ

ここでは、スマートクリックコネクタタイプの I/O コネクタ接続用ケーブルについて紹介します。

品名／外観	メーカ	仕様	ケーブル芯線数	コネクタ種類	ケーブル引出方向	ケーブル長	形式
XS5W ケーブル付コネクタ (M12 ソケット/M12 プラグ) 	オムロン株式会社	M12 ソケット(A-coding、メス)-M12 プラグ(A-coding、オス)、DC 用	5 芯	スマートクリックコネクタ	ストレート／ストレート	0.5m	形 XS5W-D521-BG1-F
						1m	形 XS5W-D521-CG1-F
						2m	形 XS5W-D521-DG1-F
						3m	形 XS5W-D521-EG1-F
						5m	形 XS5W-D521-GG1-F
						10m	形 XS5W-D521-JG1-F
						15m	形 XS5W-D521-KG1-F
						20m	形 XS5W-D521-LG1-F
XS5H ケーブル付コネクタ (M12 プラグ/バラ線) 	オムロン株式会社	M12 プラグ(A-coding、オス)ーバラ線	5 芯	スマートクリックコネクタ	ストレート	0.5m	形 XS5H-D521-BG0-F
						1m	形 XS5H-D521-CG0-F
						2m	形 XS5H-D521-DG0-F
						3m	形 XS5H-D521-EG0-F
						5m	形 XS5H-D521-GG0-F
セーフティライトカーテン用 Y 字形ジョイントプラグ／ソケット 両側コネクタ（セーフティ I/O ターミナル用） 	オムロン株式会社	M12 プラグ(A-coding、オス)-M12 ソケット(A-coding、メス、5 芯)/M12 ソケット(A-coding、メス、8 芯)	5 芯ー5 芯/8 芯	スマートクリックコネクタ	ストレート／ストレート	0.5m	形 F39-GCNY4

品名／外観	メーカ	仕様	ケーブル芯線数	コネクタ種類	ケーブル引出方向	ケーブル長	形式
形 NXR-SXD1204B-CST 用 XS5W ケーブル付きコネクタ（M12 ソケット/M12 プラグ） 	オムロン株式会社	M12 ソケット(A-coding、メス)-M12 プラグ(A-coding、オス)	8 芯	スマートクリックコネクタ	ストレート／ストレート	0.5m	形 XS5W-D821-BK1-F
						1m	形 XS5W-D821-CK1-F
						2m	形 XS5W-D821-DK1-F
						3m	形 XS5W-D821-EK1-F
						5m	形 XS5W-D821-GK1-F
						10m	形 XS5W-D821-JK1-F
						15m	形 XS5W-D821-KK1-F
						20m	形 XS5W-D821-LK1-F
形 NXR-SXD1204B-CST 用 XS5H ケーブル付きコネクタ（M12 プラグ/バラ線） 	オムロン株式会社	M12 プラグ(A-coding、オス)ーバラ線	8 芯	スマートクリックコネクタ	ストレート	0.5m	形 XS5H-D821-BK0-F
						1m	形 XS5H-D821-CK0-F
						2m	形 XS5H-D821-DK0-F
						3m	形 XS5H-D821-EK0-F
						5m	形 XS5H-D821-GK0-F

● ねじ式コネクタタイプ

ここでは、ねじ式コネクタタイプの I/O コネクタ接続用ケーブルについて紹介します。

品名／外観	メーカ	仕様	ケーブル芯線数	コネクタ種類	ケーブル引出方向	ケーブル長	形式
XS2W ケーブル付コネクタ (M12 ソケット/M12 プラグ) 	オムロン株式会社	M12 ソケット(A-coding、メス)-M12 プラグ(A-coding、オス)、DC 用	5 芯	ねじ式コネクタ	ストレート／ストレート	2m	形 XS2W-D521-DG1-A
						5m	形 XS2W-D521-GG1-A
			8 芯			2m	形 XS2W-D821-DH1-C
						5m	形 XS2W-D821-GH1-C
XS2H ケーブル付コネクタ (M12 プラグ/バラ線) 	オムロン株式会社	M12 プラグ(A-coding、オス)ーバラ線	5 芯	ねじ式コネクタ	ストレート	0.3m	形 XS2H-D521-AG0-A
						0.5m	形 XS2H-D521-BG0-A
						1m	形 XS2H-D521-CG0-A
						2m	形 XS2H-D521-DG0-A
						5m	形 XS2H-D521-GG0-A
			8 芯			0.3m	形 XS2H-D821-AH0-C
						1m	形 XS2H-D821-CH0-C

5-5-4 コネクタ用防水カバー

未使用の M12 コネクタの防水カバーです。
この防水カバーを用いると、保護構造 IP67 を保つことができます。
防水カバーには以下があります。

品名／外観	メーカ	仕様	コネクタ種類	形式
M12 用防水カバー 	オムロン株式会社	• M12 A-coding • M12 D-coding • M12 L-coding	スマートクリックコネクタ	形 XS5Z-12

5-6 オプション品

ここでは、セーフティ I/O ターミナルのオプション品を紹介します。

5-6-1 マーカ

ユニット識別マーカと I/O 識別マーカには以下の他社製のマーカを取り付けることができます。
プリンタでマーカに印字することも可能です。

品名／外観	メーカ	仕様	形式
マーカ 	Phoenix Contact	白色 17.5mm × 7.5mm	0825495

6

セーフティ I/O ターミナルの動作

この章ではセーフティ I/O ターミナルの各種動作について説明します。

6-1 動作の概要 6-2

6-2 CIP Safety 通信 6-4

6-3 EtherNet/IP 通信 6-6
6-3-1 タグデータリンク通信 6-6
6-3-2 Explicit メッセージ通信 6-6

6-4 セーフティ入力機能 6-8
6-4-1 接続可能なデバイス 6-8
6-4-2 テスト出力機能 6-10
6-4-3 テストパルス評価機能 6-10
6-4-4 デュアルチャネル評価機能 6-11
6-4-5 セーフティ入力端子の診断機能で検出可能な異常 6-12
6-4-6 入力フィルタ機能 6-12
6-4-7 入力エラーラッチ時間 6-14

6-5 セーフティ出力機能 6-16
6-5-1 接続可能なデバイス 6-16
6-5-2 テストパルス評価機能 6-16
6-5-3 デュアルチャネル評価機能 6-17
6-5-4 セーフティ出力端子の診断機能で検出可能な異常 6-18
6-5-5 出力エラーラッチ時間 6-18
6-5-6 EDM フィードバック 6-19
6-5-7 出力遅延 6-19

6-6 ロジック機能 6-20
6-6-1 ロジック演算 6-20

6-7 安全アプリケーション 6-23
6-7-1 安全アプリケーションの目的 6-23
6-7-2 安全アプリケーションの種類 6-23
6-7-3 固定アプリケーションの詳細 6-27

6-8 動作モード 6-47
6-8-1 動作モードの種類 6-47
6-8-2 各動作モードで実行可能な機能 6-48
6-8-3 各動作モードで実行可能な Web UI 機能 6-49
6-8-4 動作モードの変更と電源投入時モード 6-49

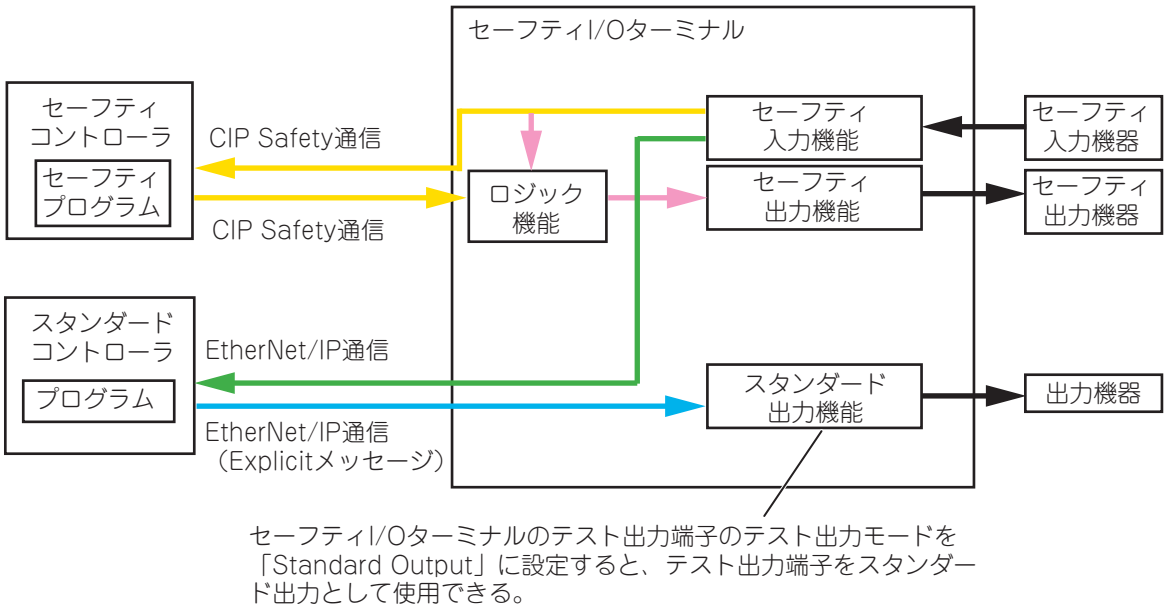
6-1 動作の概要

セーフティ I/O ターミナルの主な動作は、以下の機能の組み合わせによって実行されます。

機能	内容
CIP Safety 通信	セーフティコントローラ（CIP Safety オリジネータ）とセーフティ I/O ターミナル（CIP Safety ターゲット）間で行われる通信
EtherNet/IP 通信	スタンダードコントローラ（EtherNet/IP オリジネータ）とセーフティ I/O ターミナル（EtherNet/IP ターゲット）間で行われる通信
セーフティ入力機能	セーフティ I/O ターミナルが、セーフティ入力機器からセーフティ入力データを取得する。
セーフティ出力機能	セーフティ I/O ターミナルが、セーフティ出力機器にセーフティ出力データを出力する。
ロジック機能	セーフティ I/O ターミナル内で、セーフティ入力データに対して実行される処理。処理結果はセーフティ出力データとして、セーフティ出力機能に渡される。

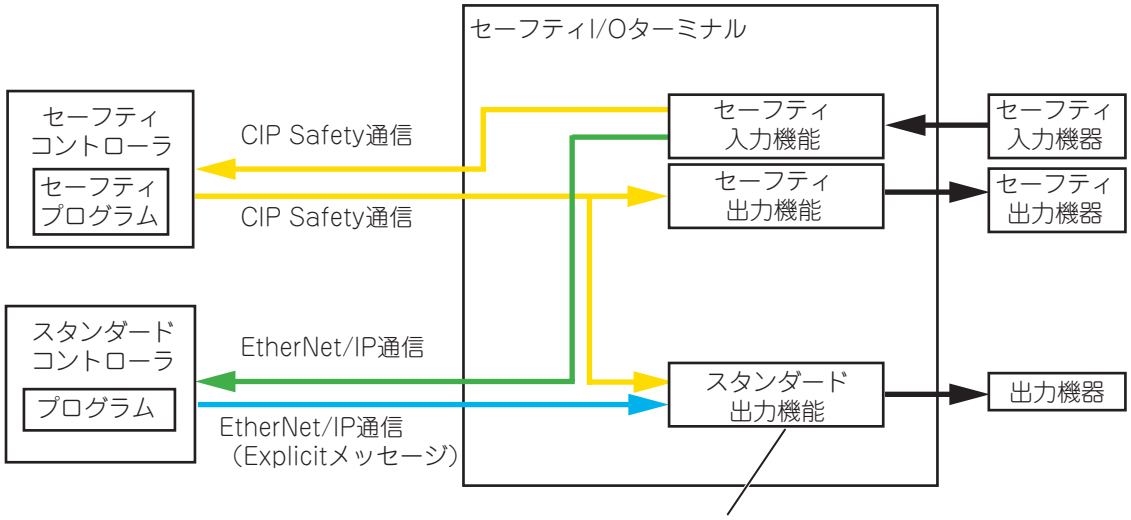
これらの機能およびセーフティ I/O ターミナルの周辺装置との関係を示します。

- セーフティ I/O ターミナル内のロジック機能が、セーフティ入力機能から取得したセーフティ入力データをロジック設定に従って処理し、その結果をセーフティ出力機能に渡す。
- また、セーフティコントローラから送信されるセーフティ出力データを、ロジック機能に組み合わせることも可能。
- さらに、セーフティ入力機能から取得したセーフティ入力データをスタンダードコントローラで処理し、その結果をスタンダード出力機能に渡すことも可能。



ロジック機能を使用しない場合は、下図のようになります。

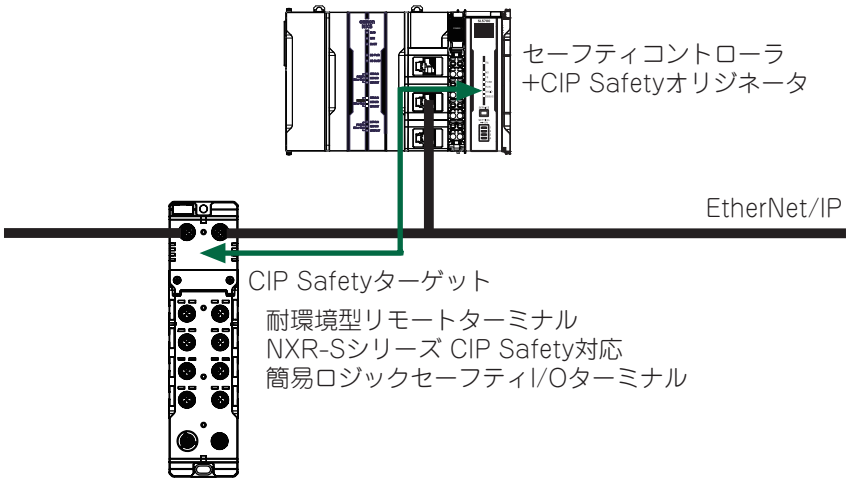
- セーフティコントローラが、セーフティ入力機能から取得したデータを処理し、その結果をセーフティ出力機能に渡す。
- また、セーフティコントローラから送信されたセーフティ出力データを、スタンダード出力機能に渡すことも可能。
- さらに、セーフティ入力機能から取得したセーフティ入力データをスタンダードコントローラで処理し、その結果をスタンダード出力機能に渡すことも可能。



セーフティI/Oターミナルのテスト出力端子のテスト出力モードを「Standard Output」に設定すると、テスト出力端子をスタンダード出力として使用できる。

6-2 CIP Safety 通信

CIP Safety 通信とは、EtherNet/IP ネットワーク上の CIP Safety デバイス間で CIP Safety on EtherNet/IP 通信を用いた通信です。
CIP Safety コネクションの開設を要求する側を CIP Safety オリジネータといい、要求される側を CIP Safety ターゲットといいます。セーフティ I/O ターミナルは、CIP Safety ターゲット機能だけをサポートしています。



CIP Safety コネクションが確立すると、CIP Safety オリジネータと CIP Safety ターゲットの間でサイクリックにセーフティ I/O データを交換します。
これにより、セーフティ I/O ターミナルのセーフティ入力の状態を上位のセーフティコントローラに送信したり、セーフティコントローラからのセーフティ出力データを受信したりすることが可能です。

CIP Safety コネクションの設定パラメータ

CIP Safety コネクションでは、次の設定パラメータがあります。

● オープンタイプ

オープンタイプは、CIP Safety コネクションの開設要求方式を示す設定です。
CIP Safety オリジネータがセーフティ I/O ターミナルに対して CIP Safety コネクションの開設を要求する際に、この［オープンタイプ］を指定できます。
オープンタイプの種類には、以下のものがあります。

オープンタイプ	内容
ターゲットデバイスをコンフィグレーション（Type 1）	コネクション確立時にセーフティ I/O ターミナルのコンフィグレーションを行います。
セーフティ署名をチェック（Type 2a）	コネクション確立時にセーフティ I/O ターミナルのコンフィグレーションが正しいことをセーフティ署名によりチェックします。セーフティ署名は、セーフティコンフィグレーション CRC とセーフティコンフィグレーションタイムスタンプで構成されます。
オープンのみ（Type 2b）	コネクション確立時にセーフティ I/O ターミナルのコンフィグレーションチェックを行いません。

⚠ 警告

オープンタイプを［オープンのみ］に設定する場合は、オリジネータ／ターゲットが正しいコンフィグレーションを持っていることを確認した上で使用してください。
安全機能が損なわれ、重度の人身傷害が万一の場合起こるおそれがあります。

● コネクションタイプ

CIP Safety のコネクション設定では、コネクションタイプとしてマルチキャスト（Multi-cast connection）またはシングルキャスト（Point to Point connection）を選択できます。
マルチキャストは、1 パケットで 1 つの入力アセンブリを複数のオリジネータデバイスに送信することが可能です。
一方、シングルキャストは、1 つの入力アセンブリを、各オリジネータデバイスに対して個別に送信します。このため、1 つの入力アセンブリを複数のオリジネータデバイスに送信する場合、マルチキャストを使用したほうが、通信負荷を減らすことができます。
なお、マルチキャストを使用し 1 パケットで 1 つの入力アセンブリを複数のオリジネータデバイスに送信する場合は、これを受信する各コネクションのコネクションタイプがマルチキャスト（Multi-cast connection）で、コネクション I/O タイプ、データパケットインターバル（EPI）、タイムアウト値のすべてが同一の場合に限ります。

使用上の注意

マルチキャストを使用する場合、ネットワーク上のすべてのノードがこれを受信する場合を除き、マルチキャストフィルタ機能を持つスイッチングハブを使用してください。
マルチキャストフィルタ機能を持たないスイッチングハブを使用した場合、マルチキャストパケットがネットワーク全体にブロードキャスト（一斉同報）されるため、無駄なパケットがこれを必要としないノードにも送信され、そのノードの通信負荷を増加させる原因となります。

● データパケットインターバル（EPI）

データパケットインターバル（EPI: Expected Packet Interval）とは、CIP Safety 通信における Ethernet 回線上の入出力データ更新周期です。EtherNet/IP では、ノード数に依存せず、コネクションごとに設定した EPI で回線上のデータ交換が行われます。
内蔵 EtherNet/IP ポートではコネクションごとに、EPI を設定できます。

使用上の注意

通信デバイスの性能は、製品仕様ごとに、ある程度の限界が定められています。このため、データパケットインターバル（EPI）を無制限に設定することはできません。
詳細は、『NX シリーズ セーフティコントロールユニット／通信コントロールユニット ユーザーズマニュアル (SGFM-723)』を参照して、適正なデータパケットインターバル（EPI）を設定してください。

● I/O アセンブリ

I/O アセンブリは、オリジネータとターゲットの間でサイクリックに交換する I/O データの単位です。
セーフティ I/O ターミナルは、いくつかの I/O アセンブリを定義し用意しています。定義された I/O アセンブリの中から選択し、コネクション 1 本につき 1 つの I/O アセンブリを設定します。
セーフティ I/O ターミナルと CIP Safety オリジネータ間で設定可能な I/O アセンブリは以下のとおりです。

- Input コネクション: 25C Hex(2 バイト)、3C0 Hex(5 バイト)、3C1 Hex(9 バイト)
- Output コネクション: なし

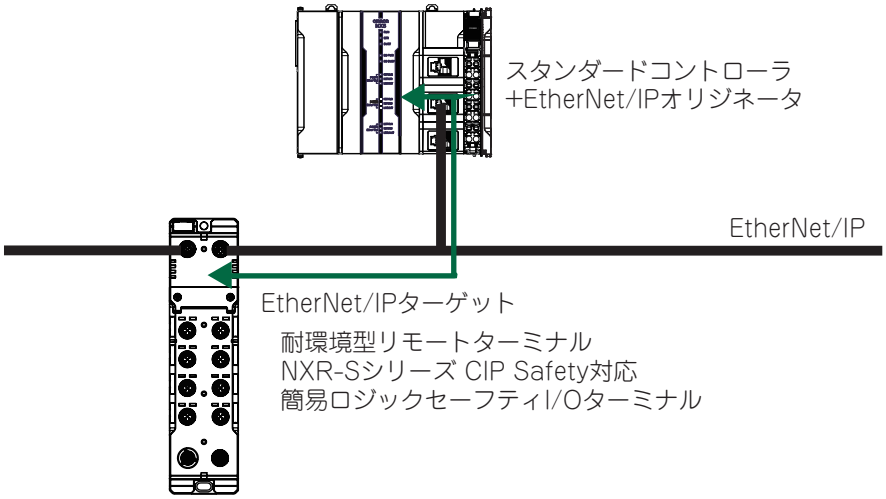
I/O アセンブリデータの詳細は、「A-2 セーフティ I/O アセンブリデータ (P.A-4)」を参照してください。

6-3 EtherNet/IP 通信

EtherNet/IP 通信は、EtherNet/IP ネットワーク上で、デバイス間でデータをやり取りをするための通信です。
通信方式としてタグデータリンク通信と Explicit メッセージ通信があります。

6-3-1 タグデータリンク通信

タグデータリンク通信とは、EtherNet/IP ネットワーク上のデバイス間でサイクリックに I/O データを交換する通信です。
タグデータリンク通信では、一方のノードがコネクションと呼ばれる通信回線の開設を要求（オープン）し、相手のノードとの間で I/O データを交換します。
タグデータリンク通信のコネクション開設を要求する側を EtherNet/IP オリジネータ、要求される側を EtherNet/IP ターゲットといいます。セーフティ I/O ターミナルは EtherNet/IP ターゲットの機能だけをサポートしています。



I/O データの交換対象となる単位をタグと呼び、オリジネータとターゲットの間でサイクリックにデータ交換を行います。
セーフティ I/O ターミナルはいくつかの I/O アセンブリを定義し用意しています。
I/O アセンブリデータの設定などタグデータリンク通信する設定方法は、「タグデータリンク通信の設定手順 (P.7-36)」を参照してください。

6-3-2 Explicit メッセージ通信

Explicit メッセージ通信とは、EtherNet/IP ネットワーク上で、要求／応答形式により機器の設定や状態をやり取りする CIP 通信です。
Explicit メッセージクライアントからの要求に対し、Explicit メッセージサーバが応答することで通信が行われます。
セーフティ I/O ターミナルは、Explicit メッセージサーバ機能だけををサポートしています。

Explicit メッセージサーバ機能

Explicit メッセージサーバ機能により、Explicit メッセージクライアントからの Explicit メッセージでセーフティ I/O ターミナルの CIP オブジェクトへアクセスでき、以下が可能となります。
- セーフティ I/O ターミナルのイベントログの取得やイベントログクリアなどのトラブルシュート

- セーフティ I/O ターミナルのデバイスパラメータ設定や IP アドレス設定などの通信パラメータ設定

また、Explicit メッセージクライアント機能を持つデバイスがタグデータリンク（Implicit メッセージ）通信をサポートしていない場合、代替手段として Explicit メッセージでセーフティ I/O ターミナルの I/O 制御が可能です。
セーフティ I/O ターミナルがサポートする CIP オブジェクトの詳細は、「A-4 サポートする CIP オブジェクト (P.A-15)」を参照してください。
セーフティ I/O ターミナルの CIP オブジェクトへの Explicit メッセージによるアクセス方法は、使用しているコントローラのマニュアルを参照してください。

6-4 セーフティ入力機能

セーフティ I/O ターミナルにおけるセーフティ入力機能について説明します。

6-4-1 接続可能なデバイス

セーフティ I/O ターミナルはセーフティ入力端子にて、接続する外部機器の診断などを行います。
セーフティ入力端子に接続できるセーフティ入力機器、スタンダード入力機器を以下に示します。

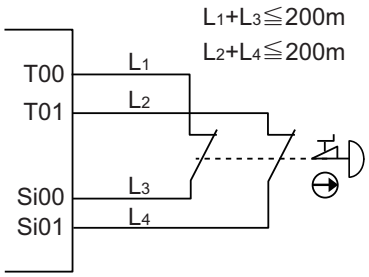
入力機器種別	チャネルモード			テスト出力端子
	デュアルチャネル（同値入力）	デュアルチャネル（反転入力）	シングルチャネル	テスト出力モード (Test Output Mode)
セーフティ入力機器（メカ接点機器）	• 非常停止用押ボタンスイッチ（2NC 接点） • セーフティ・ドアスイッチ（2NC 接点） • セーフティ・リミットスイッチ（2NC 接点） • セーフティ・キーセレクタスイッチ（2NC 接点） • イネーブルスイッチ（2NC 接点） • デュアルチャネル同値入力用メカ接点（2NC 接点）	• セーフティ・ドアスイッチ（1NC/1NO 接点） • セーフティ・リミットスイッチ（1NC/1NO 接点） • ２ハンドスイッチ（1NO/1NC 接点） • セーフティ・キーセレクタスイッチ（1NC/1NO 接点） • デュアルチャネル反転入力用メカ接点（1NC/1NO 接点）	• 非常停止用押ボタンスイッチ（1NC 接点） • セーフティ・ドアスイッチ（1NC 接点） • セーフティ・リミットスイッチ（1NC 接点） • セーフティ・キーセレクタスイッチ（1NC 接点） • EDM フィードバック（1NC 接点） • シングルチャネル用メカ接点（1NC 接点）	Test Output
セーフティ入力機器（半導体出力機器）	• セーフティライトカーテン • セーフティレーザースキャナ • 高コードドアスイッチ • 高コードドアスイッチ（ゲート用） • 高コードドアスイッチ（電磁ロック付き） • デュアルチャネル同値入力用半導体出力	• デュアルチャネル反転入力用半導体出力	• シングルチャネル用半導体出力	• Power Supply • Standard Output • Not Used
スタンダード入力機器	該当なし	該当なし	• リセットスイッチ（テストパルスあり）（1NO 接点）	Test Output
	該当なし	該当なし	• リセットスイッチ（テストパルスなし）（1NO 接点）	Power Supply

セーフティ入力機器は、大きく分けて 2 種類あります。
1 つはメカ接点機器であり、もう 1 つは半導体出力機器です。

● メカ接点機器

非常停止スイッチやセーフティリミットスイッチなどの接点出力の機器をセーフティ入力に接続します。
セーフティ入力（Si）とテスト出力（T）を組み合わせて使用します。

接続例として、デュアルチャネル入力で使用する場合を示します。



セーフティ入力とテスト出力の組み合わせは、同じ番号の場合だけが使用可能です。上記例では、“Si00”と“T00”、“Si01”と“T01”の組み合わせとなります。
この場合、“T00”と“T01”のテスト出力モード（Test Output Mode）の設定は［Test Output］となります。

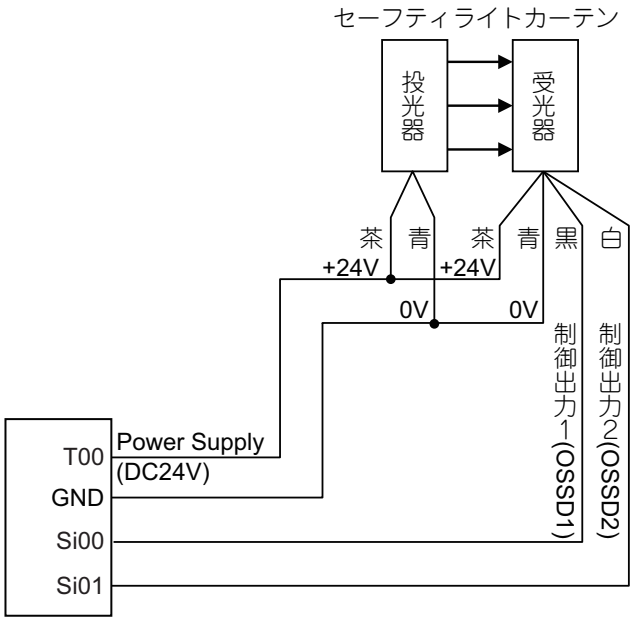
使用上の注意

テスト出力 1 点に接続されるケーブルの総配線長は 200m 以下としてください。

● 半導体出力機器

ライトカーテンなどの半導体出力の機器をセーフティ入力（Si）に接続します。

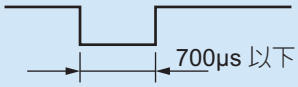
接続例として、デュアルチャネル入力で使用する場合を示します。



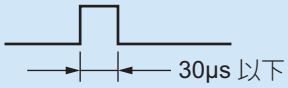
セーフティ入力の“Si00”と“Si01”にライトカーテンの出力を接続し、テスト出力 “T00”は、ライトカーテンへの供給電源として使用しています。
この場合、“T00”のテスト出力モード（Test Output Mode）の設定は［Power Supply］となります。

使用上の注意

- ライトカーテンへの電源をテスト出力端子から供給します。テスト出力から供給可能な出力電流は最大 0.7A／点です。
- セーフティライトカーテンなどの半導体出力機器には、配線異常を検出するためにパルスを出力するタイプがあります。セーフティ入力端子に半導体出力機器を接続する場合は、下記の点に注意してください。
  a）半導体出力の ON 時の OFF パルス幅が 700μs 以下であること。



  b）半導体出力 OFF 時の ON パルス幅が 30μs 以下であること。



6-4-2 テスト出力機能

テスト出力端子は、テストパルス評価時（メカ接点機器）のテスト出力や半導体出力機器への電源供給など、セーフティ入力の補助として動作します。
テスト出力機能（テスト出力端子の機能）について、以下の通りです。

テストパルス有無	テスト出力モード (Test Output Mode)	概要
テストパルスあり（メカ接点機器）	[Test Output]	テスト出力端子から一定間隔のテストパルス付き DC 24V を出力します。 テストパルス評価機能については「6-4-3 テストパルス評価機能 (P.6-10)」を参照してください。
テストパルスなし（メカ接点機器）	[Power Supply]	テスト出力端子から DC 24V を出力します。
テストパルスなし（半導体出力機器）	[Power Supply]	テスト出力端子から DC 24V を出力します。 半導体出力機器の電源として使用します。
	[Standard Output]	テスト出力端子を使用して、コントローラからのスタンダード出力が可能となります。*1 非安全のデジタル信号出力端子として使用します。例えば、表示灯や PLC の入力に接続して、モニタ出力などに使用します。 設定方法は、「7-5-2 スタンダード出力機能の設定手順 (P.7-44)」を参照してください。

***1.** コントローラからのスタンダード出力機能は、安全機能ではありません。

またテスト出力端子には、過電流を検知する機能があります。過電流を検知した場合、イベントログに記録を残します。詳しくは「11-2-4 イベントの内容と対処方法 (P.11-12)」を参照してください。

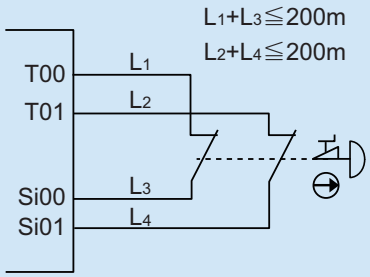
6-4-3 テストパルス評価機能

テストパルスあり（メカ接点機器）の場合、テスト出力端子から一定間隔のテストパルス付き DC 24V を出力し、接続されている外部機器の故障や配線異常を検出できます。

テストパルス有無	テスト出力モード (Test Output Mode)	概要
テストパルスあり （メカ接点機器）	[Test Output]	メカ接点を経由しセーフティ入力端子にテスト出力信号（テストパルス）を入力します。 入力信号線の電源ライン（＋側）への接触、ほかの入力信号線との短絡が検出できます。

使用上の注意

セーフティ入力端子とテスト出力端子の組み合わせは、同じ番号の場合だけが使用可能です。
以下の例では、“Si00”と“T00”、“Si01”と“T01”の組み合わせとなります。



6-4-4 デュアルチャネル評価機能

セーフティ入力端子はデュアルチャネル（二重化）で使用することができます。デュアルチャネル評価機能とは、2 入力間のデータの不整合時間を評価する機能です。
不整合時間とは、一方の入力値の変化から他方が変化するまでの時間のことです。
［デュアルチャネル監視時間］で設定した時間を超えて他方の入力に変化がない場合、異常と判断します。

デュアルチャネル評価機能の設定

入力機器にデュアルチャネルモードのデバイスを選び、［デュアルチャネル監視時間］を設定します。

以下に、設定を示します。

設定データ名	概要	設定範囲
チャネルモード	入力機器にデュアルチャネルモードのデバイスを選びます。	以下から選択します。 • デュアルチャネル同値入力 • デュアルチャネル反転入力 チャネルモードとデバイスの詳細については、「6-4-1 接続可能なデバイス (P.6-8)」を参照してください。
デュアルチャネル監視時間	2 入力間のデータの不整合時間*1 を監視します。この値を超えて不整合の場合、異常とします。	10 から 64000(ms)で設定します。 5(ms)単位です。 工場出荷時設定は、500(ms)です。

***1.** 不整合時間とは、一方の入力値の変化から他方が変化するまでの時間のことです。

設定方法については、「7-5-1 セーフティ入力機能の設定手順 (P.7-42)」を参照してください。

セーフティ入力端子の入力信号とセーフティ入力データとの関係

セーフティ入力信号とセーフティ入力データの関係は以下となります。

チャネルモード	セーフティ入力端子の入力信号		セーフティ入力データ		状態の意味
	Si (n)	Si (n+1)	Si (n)	Si (n+1)	
デュアルチャネル同値入力	0	0	0	0*1	インアクティブ（OFF）
	0	1	0	0*1	2 入力間データずれ
	1	0	0	0*1	2 入力間データずれ
	1	1	1	0*1	アクティブ（ON）
デュアルチャネル反転入力	0	0	0	0*1	2 入力間データずれ
	0	1	0	0*1	インアクティブ（OFF）
	1	0	1	0*1	アクティブ（ON）
	1	1	0	0*1	2 入力間データずれ

***1.** デュアルチャネル設定された端子の場合、偶数端子番号のセーフティ入力データをセーフティコントローラのセーフティプログラムで使用します。

6-4-5 セーフティ入力端子の診断機能で検出可能な異常

セーフティ入力端子の異常は、パラメータの設定内容により、検出できる異常が異なります。
以下にパラメータ設定ごとの検出可能な異常を示します。

パラメータ設定		異常の検出			
チャネルモード	テストパルス	電源ライン（＋側）への接続	地絡*1	断線	入力配線間の短絡
シングルチャネル	テストパルスなし（半導体出力機器）	検出不可	検出不可	検出不可	—
	テストパルスあり（メカ接点機器）	検出可	入力 ON 時に検出可	検出不可	—
デュアルチャネル（同値入力）	テストパルスなし（半導体出力機器）	検出不可*2	入力 ON 時に検出可	検出不可*3	検出不可*2
	テストパルスあり（メカ接点機器）	検出可	入力 ON 時に検出可	検出不可*3	検出可
デュアルチャネル（反転入力）	テストパルスなし（半導体出力機器）	ON から OFF 時、または OFF から ON 時に検出可	ON から OFF 時、または OFF から ON 時に検出可	ON から OFF 時、または OFF から ON 時に検出可	検出可
	テストパルスあり（メカ接点機器）	検出可	ON から OFF 時、または OFF から ON 時に検出可	ON から OFF 時、または OFF から ON 時に検出可	検出可

***1.** 地絡の検出には、外部電源の 0V 接地が必要です。
***2.** ライトカーテンやレーザースキャナがもつ OSSD 診断機能によって検出可能です。
***3.** 入力 ON 時に片方の信号線が断線した場合のみ検出可能です。

6-4-6 入力フィルタ機能

セーフティ入力端子に接続された外部機器のチャタリングやノイズによる誤動作を防止する機能です。
［ON→OFF 遅延時間］、または［OFF→ON 遅延時間］を設定し、外部機器のチャタリングやノイズをフィルタリングします。

以下に、設定を示します。

設定データ名	概要	設定範囲
［ON→OFF 遅延時間］	入力データが ON から OFF になる遅延時間です。	0 から 1600(ms)で設定します。 5(ms)単位です。 工場出荷時設定は、0(ms)です。
［OFF→ON 遅延時間］	入力データが OFF から ON になる遅延時間です。	0 から 1600(ms)で設定します。 5(ms)単位です。 工場出荷時設定は、0(ms)です。

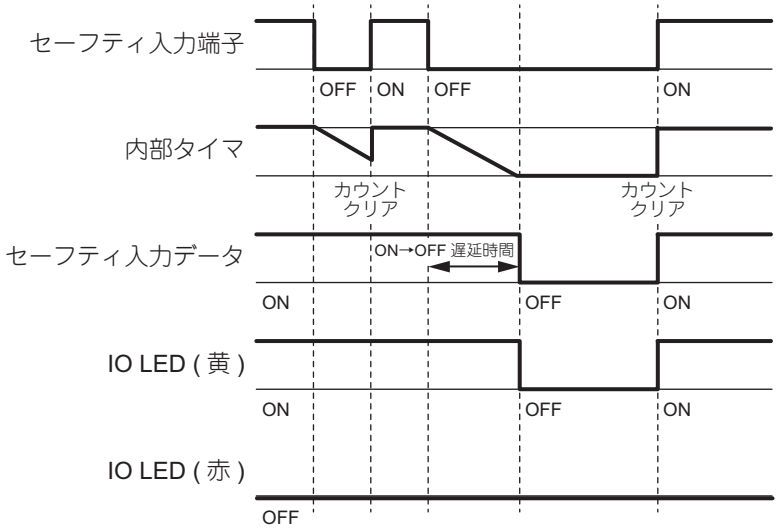
設定方法については、「7-5-1 セーフティ入力機能の設定手順 (P.7-42)」を参照してください。

使用上の注意

遅延時間の設定が大きいほどチャタリングやノイズへの耐性が上がりますが、入力信号に対する応答が遅くなります。

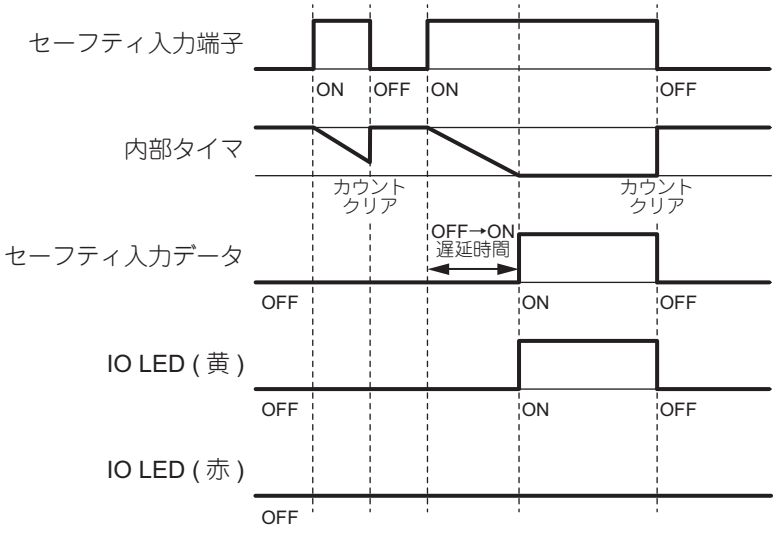
OFF 遅延時間設定時の動作

［ON→OFF 遅延時間］で設定した時間よりも短い OFF パルスがフィルタリングできます。



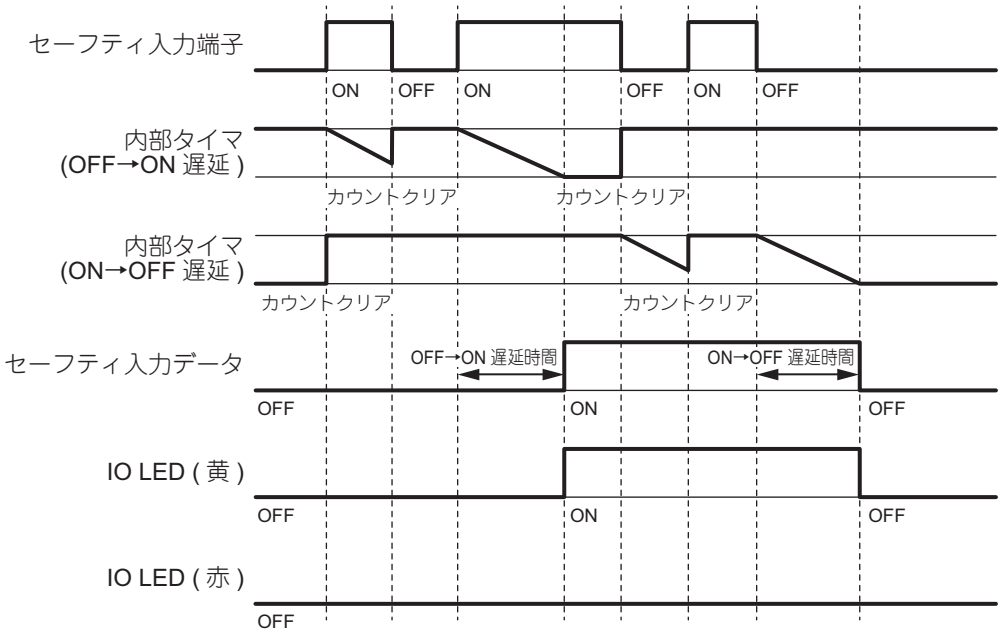
ON 遅延時間設定時の動作

［OFF→ON 遅延時間］で設定した時間よりも短い ON パルスがフィルタリングできます。



ON 遅延時間と OFF 遅延時間両方設定時の動作

［OFF→ON 遅延時間］で設定した時間よりも短い ON パルス、および［ON→OFF 遅延時間］で設定した時間よりも短い OFF パルスがフィルタリングできます。



6-4-7 入力エラーラッチ時間

入力エラーラッチ時間は全ての入力端子に適用されるパラメータです。
入力端子でエラーが発生した場合にエラー状態をラッチする時間を設定します。
断続的に発生するエラーをセーフティ I/O ターミナルが検出できるように、最小のラッチ時間を設定します。
エラーラッチ時間は、セーフティ I/O ターミナルとオリジネータデバイス間のネットワー応答時間を考慮して、エラーを検出できる最適な数値を設定してください。

以下に、設定を示します。

設定データ名	概要	設定範囲
入力エラーラッチ時間	エラー発生から解除までの最低時間を設定します。*1	0 から 65530(ms)で設定します。 10(ms)単位です。 0(ms)の場合、エラーラッチしません。 工場出荷時設定は、1000(ms)です。

***1.** エラー要因を除去し該当セーフティ入力をインアクティブ（OFF）にするとエラー解除します。

6-5 セーフティ出力機能

セーフティ I/O ターミナルにおけるセーフティ出力機能について説明します。

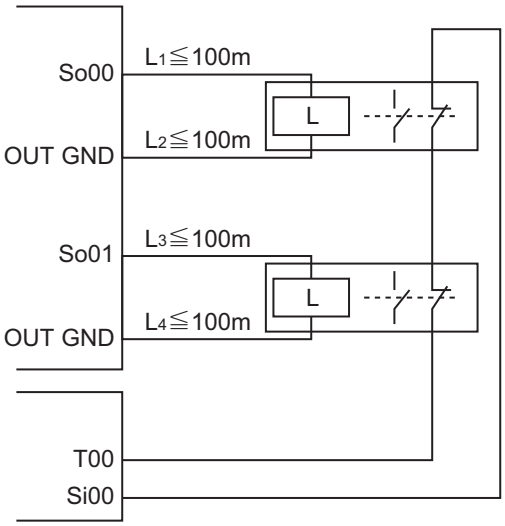
6-5-1 接続可能なデバイス

セーフティ I/O ターミナルはセーフティ出力端子にて、接続する外部機器の診断などを行います。
セーフティ出力端子に接続できるセーフティ出力機器を以下に示します。

チャネルモード		出力端子の設定
デュアルチャネル	シングルチャネル	テストパルス
• セーフティリレー（デュアルチャネル） • デュアルチャネル同値出力（テストパルスあり）	• セーフティリレー（シングルチャネル） • シングルチャネル（テストパルスあり）	テストパルスあり
• デュアルチャネル同値出力（テストパルスなし）	• シングルチャネル（テストパルスなし）	テストパルスなし

セーフティ出力機器には、セーフティリレー、コンタクタ、ソレノイドバルブなどの機器があります。
出力は PNP 出力です。

接続例として、セーフティリレーまたはコンタクタで使用する場合を示します。



使用上の注意

セーフティ出力端子からセーフティ出力機器までの配線長（L1, L2, L3, L4）は、それぞれ 100m 以下としてください。

6-5-2 テストパルス評価機能

セーフティ出力端子から一定間隔のテストパルスを出力し、出力端子の配線異常を検出する機能です。
以下に、設定を示します。

設定データ名	概要	設定範囲
テストパルス	セーフティ出力機器にテストパルスありのデバイスを選びます。	以下から選択します。 • セーフティリレー（デュアルチャネル） • デュアルチャネル同値出力（テストパルスあり） • セーフティリレー（シングルチャネル） • シングルチャネル（テストパルスあり）

使用上の注意

テストパルス評価機能を使用する場合、セーフティ出力 ON のとき、出力回路診断のために OFF パルス信号（パルス幅: 500(μs)）が出力されます。
この OFF パルスによって誤動作しないように、接続する制御機器の入力応答時間に注意してください。

参考

セーフティリレーはデュアルチャネル／シングルチャネルとも、［テストパルスあり］のデバイスになります。

6-5-3 デュアルチャネル評価機能

セーフティ出力端子はデュアルチャネル（二重化）で使用することができます。デュアルチャネル評価機能とは、2 出力間の信号の不一致を評価する機能です。
２つの出力端子のうち、片方で異常が検出されると、２つの出力ともに遮断(OFF)します。

デュアルチャネル評価機能の設定

出力機器にデュアルチャネルモードのデバイスを選ぶことで設定をします。

以下に、設定を示します。

設定データ名	概要	設定範囲
チャネルモード	出力機器にデュアルチャネルモードのデバイスを選びます。	以下から選択します。 • セーフティリレー（デュアルチャネル） • デュアルチャネル同値出力（テストパルスあり） • デュアルチャネル同値出力（テストパルスなし） チャネルモードとデバイスの詳細については、「6-5-1 接続可能なデバイス (P.6-16)」を参照してください。

設定方法については、「7-6-1 セーフティ出力機能の設定手順 (P.7-47)」を参照してください。

セーフティ出力データとセーフティ出力端子の出力信号の関係

デュアルチャネルモードのデバイスの場合、セーフティ出力データとセーフティ出力信号の関係は以下となります。

チャネルモード	セーフティ出力データ		セーフティ出力端子の出力信号		状態の意味
	So (n)	So (n+1)	So (n)	So (n+1)	
• セーフティリレー（デュアルチャネル） • デュアルチャネル同値出力（テストパルスあり） • デュアルチャネル同値出力（テストパルスなし）	0	0	0（OFF）	0（OFF）	インアクティブ（OFF）
	0	1	0（OFF）	0（OFF）	インアクティブ（OFF）*1
	1	0	0（OFF）	0（OFF）	インアクティブ（OFF）*1
	1	1	1（ON）	1（ON）	アクティブ（ON）

***1.** デュアルチャネル出力間のデータ異常の発生によりインアクティブとなります。

6-5-4 セーフティ出力端子の診断機能で検出可能な異常

セーフティ出力端子の異常は、パラメータの設定内容により、検出できる異常が異なります。
以下に検出可能な異常を示します。

パラメータ設定		異常の検出						
出力端子の設定	概要	電源ライン（＋側）への接続		地絡*1		出力配線間の短絡*2		
		出力 ON 時	出力 OFF 時	出力 ON 時	出力 OFF 時	出力 ON どうし短絡	出力 OFF どうし短絡	出力が異なる時の短絡
テストパルスなし	出力 ON 時にテストパルスを出力しません。	検出不可	検出可	検出可	検出不可	検出不可	検出不可	検出可
テストパルスあり	出力 ON 時にテストパルスを出力します。	検出可	検出可	検出可	検出不可	検出可	検出不可	検出可

***1.** 地絡の検出には、外部電源の 0V 接地が必要です。
***2.** 出力配線間の短絡の検出は、デュアルチャネルモードでのみ有効です。

6-5-5 出力エラーラッチ時間

出力エラーラッチ時間は全ての出力端子に適用されるパラメータです。
出力端子でエラーが発生した場合にエラー状態をラッチする時間を設定します。
断続的に発生するエラーをセーフティ I/O ターミナルが検出できるように、最小のラッチ時間を設定します。
エラーラッチ時間は、セーフティ I/O ターミナルとオリジネータデバイス間のネットワーク応答時間を考慮して、エラーを検出できる最適な数値を設定してください。

以下に、設定を示します。

設定データ名	概要	設定範囲
出力エラーラッチ時間	エラー発生から解除までの最低時間を設定します。*1	0 から 65530(ms) で設定します。 10(ms)単位です。 0(ms)の場合、エラーラッチしません。 工場出荷時設定は、1000(ms) です。

***1.** エラー要因を除去し該当セーフティ出力をインアクティブ（OFF）にするとエラー解除します。

6-5-6 EDM フィードバック

安全アプリケーションがユーザ定義アプリケーションの場合、EDM フィードバック設定を表示します。

以下に、設定を示します。

設定データ名	概要	設定範囲
EDM フィードバック	セーフティ入力機器で［EDM フィードバック］を登録している端子の中から選択します。	以下から選択します。 • 0: 未使用 • 1: Si00～12: Si11 工場出荷時設定は、0（未使用）です。

6-5-7 出力遅延

安全アプリケーションがユーザ定義アプリケーションの場合、セーフティ出力端子に接続された外部機器への出力遅延時間を設定できます。モータやロボットアーム等が完全に止まるまでの時間を考慮し出力を遅らせることで急停止による機械損傷を防いだり、外部機器が復帰した後に動作が安定してからセーフティ出力を ON させたりする等に使用する機能です。

以下に、設定を示します。

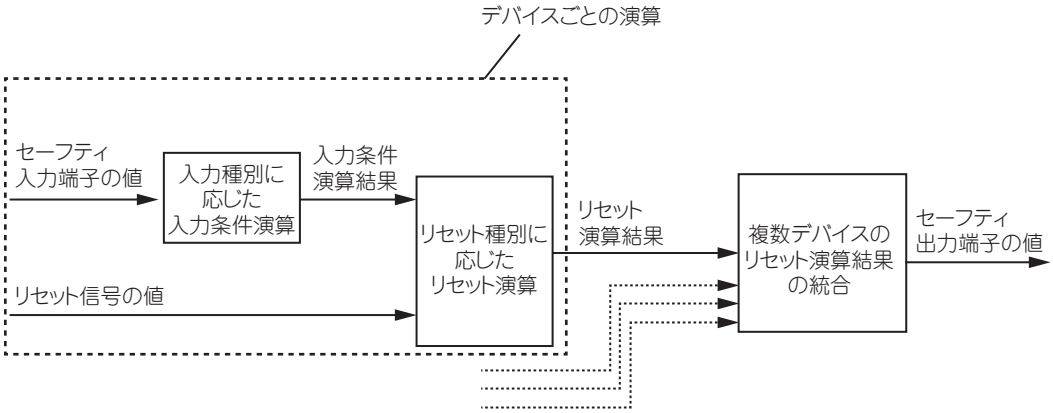
設定データ名	概要	設定範囲
［ON→OFF 遅延時間］	出力データが ON から OFF になる遅延時間です。モータやロボットアーム等が完全に止まるまでの時間を考慮し出力を遅らせることで、急停止による機械損傷を防ぐために使用します。	設定値×100(ms)の値、出力を遅延します。 0 から 1500 で設定します。 工場出荷時設定は、0(ms)です。
［OFF→ON 遅延時間］	出力データが OFF から ON になる遅延時間です。外部機器が復帰した後に動作が安定してからセーフティ出力を ON するために使用します。	

6-6 ロジック機能

ロジック機能は、セーフティ I/O ターミナル内で、セーフティ入力データに対して実行される処理のことです。処理結果はセーフティ出力データとして、セーフティ出力に渡されます。
ここでは、ロジック演算のしくみについて説明します。

6-6-1 ロジック演算

ロジック設定では、各デバイスに対して「入力種別」、「リセット種別」、「セーフティ出力端子 So00-So03 への出力値」の 3 種類のパラメータを設定する必要があります。
ロジック演算は、まずデバイスごとにセーフティ入力端子 SiXX の値に対して「入力種別」に応じた入力条件演算、「リセット種別」に応じたリセット演算が実行されます。次に複数デバイスのリセット演算結果の統合が実行され、最終的にセーフティ出力端子 SoXX の値が決まります。ロジック設定は、これらの処理の内容を意識して行う必要があります。



入力種別に応じた入力条件演算

入力条件演算では、「入力種別」の設定に応じて、2 種類のデバイスからの入力値を統合して入力条件演算結果を求めることができます。これにより、たとえば 2 対のセーフティライトカーテンの両方が遮光された場合にだけ装置を停止させるといった処理が可能になります。
「入力種別」の設定には、[2 Input(OR)]、[2 Input(AND)]、および設定なしの 3 種類があります。各設定と入力条件演算結果の関係を以下に示します。

入力種別	入力条件演算結果
2 Input(OR)	2 種類のデバイスからの入力値の OR 演算結果
2 Input(AND)	2 種類のデバイスからの入力値の AND 演算結果
設定なし	2 種類のデバイスからの入力値を統合しない。1 種類のデバイスからの入力値を、そのまま入力条件演算結果とする。

リセット種別に応じたリセット演算

各デバイスに対する出力値は、いったん FALSE になるとリセットするまでは TRUE に戻りません。「リセット種別」とは、各デバイスに対する出力値をリセットする方法のことで、[Manual(SiXX)] と [Auto] の 2 種類があります。各設定とリセット条件の関係を以下に示します。

リセット種別	リセット条件
Manual(SiXX)	セーフティ入力端子 SiXX の値をリセット信号とする。リセットが実行された場合に当該デバイスの出力値がリセットされる。

リセット種別	リセット条件
Auto	リセット信号を使用しない。当該デバイスの入力条件演算結果が TRUE になった時点で出力値がリセットされる。

表中のリセット信号とは、当該デバイスの出力をリセットするための Low-High-Low のパルス信号のことです。リセット信号は、自動登録および登録後の設定変更が可能です。それぞれの手順は、「7-7-1 ロジック設定手順 (P.7-50)」を参照してください。

デバイスごとに、入力条件演算結果とリセット条件が成立しているかどうかをもとにリセット演算が実行されます。入力条件演算結果、リセット条件成立／不成立とリセット演算結果の関係を以下に示します。

入力条件演算結果	リセット条件	リセット条件演算結果
TRUE	成立	TRUE
	不成立	現在値を維持する。
FALSE	成立	FALSE
	不成立	FALSE

使用上の注意

リセット種別に Auto を使用する場合、再起動またはリセットにより予期せぬ起動や危険な機械の動きが発生せず、人に危害を及ぼすおそれがないことを十分に確認してください。確認できない場合は、リセット種別に Auto を使用しないでください。

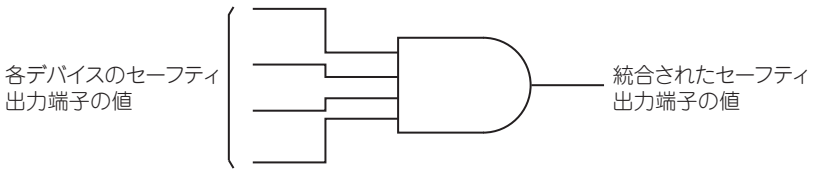
セーフティ出力端子 So00-So03 への出力値設定

「セーフティ出力端子 So00-So03 への出力値」の設定とは、各デバイスのリセット演算結果をセーフティ出力端子に割り付ける設定のことです。デバイスごとに設定値［0］または［1］を、セーフティ出力端子 So00-So03 に割り付けます。設定値の意味は以下のとおりです。

設定値	意味
0	リセット演算結果を、当該セーフティ出力端子に反映する。
1	リセット演算結果を、当該セーフティ出力端子に反映しない。

複数デバイスの出力演算結果の統合

複数のデバイスが接続されている場合、セーフティ出力端子の値は各デバイスのセーフティ出力端子の値を AND 演算で統合したものになります。つまり、複数デバイスのうち、セーフティ出力端子の値が FALSE になるものがひとつでもあれば、セーフティ出力端子の値は FALSE になります。



設定例

以下に、ロジック設定の設定例を示します。

入力	デバイス	入力種別	リセット種別	So00	So02
Si00	非常停止用押ボタンスイッチ（デュアルチャネル同値入力	−	Manual(Si10)	0	0
Si02	セーフティライトカーテン	2 Input(OR)	Manual(Si11)	1	0

入力	デバイス	入力種別	リセット種別	So00	So02
Si04	セーフティライトカーテン				
Si06	セーフティ・ドアスイッチ（デュアルチャネル同値入力）	−	Auto	0	1
Ro1-01	Remote Output 1 - 01	2 Input(OR)	Manual(Si10)	0	0
Ro2-01	Remote Output 2 - 01				

この設定の場合、So00 の値は以下のいずれかの条件がひとつでも発生すると FALSE になります。
- 非常停止用押ボタンスイッチが押される。
- セーフティ・ドアスイッチが設置されたドアが開く。
- リモート出力 Remote Output 1 - 01 と Remote Output 2 - 01 の両方の値が FALSE になる。

また、So02 の値は以下のいずれかの条件がひとつでも発生すると FALSE になります。
- 非常停止用押ボタンスイッチが押される。
- 2 対のセーフティライトカーテンの両方が遮光される。
- リモート出力 Remote Output 1 - 01 と Remote Output 2 - 01 の両方の値が FALSE になる。

So00 または So02 の値が FALSE になった場合、以下の条件が成立するとリセットされ、値が TRUE に戻ります。

So00 または So02 の値が FALSE になった要因	So00 または So02 の値がリセットされる条件
非常停止用押ボタンスイッチが押された。	Si10 のリセット条件が成立する。
2 対のセーフティライトカーテンの両方が遮光された。	Si11 のリセット条件が成立する。
セーフティ・ドアスイッチが設置されたドアが開いた。	セーフティ・ドアスイッチが設置されたドアが閉まる。
リモート出力 Remote Output 1 - 01 と Remote Output 2 - 01 の両方の値が FALSE になった。	Si10 のリセット条件が成立する。

6-7 安全アプリケーション

ここでは、安全アプリケーションの目的、種類、およびセーフティ I/O ターミナルにプリセットされている固定アプリケーションの詳細について説明します。

6-7-1 安全アプリケーションの目的

安全アプリケーションのロジック機能を使用すると、セーフティコントローラを介さずにローカルで制御を行うことで、高速な応答を実現することができます。
さらに必要に応じてセーフティコントローラから送信されたセーフティ出力データを内部ロジックに組み合わせることで、制御の柔軟性を高めることもできます。

6-7-2 安全アプリケーションの種類

安全アプリケーションには、リモート I/O モード用アプリケーション、固定アプリケーション、ユーザ定義アプリケーション、アドオンアプリケーションの 4 種類があります。
それぞれの概要、アプリケーションの内容、選択基準、対応するセーフティコントロールシステムを以下に示します。

安全アプリケーション	概要	選択基準	セーフティコントロールシステム
リモート I/O モード用アプリケーション	ロジック機能を使用せず、I/O 端子設定だけの安全アプリケーション。 ロジック機能を使用しないので、セーフティコントローラが制御する。	• セーフティ I/O ターミナルのロジック機能では実現が難しい、複雑で大規模なシステムを構築したい。	「セーフティコントローラが制御する構成（Type 1 Safety Open によるコンフィグレーション）（P.1-8)」 「セーフティコントローラが制御する構成（Web UI によるコンフィグレーション）（P.1-9)」
固定アプリケーション	ロジック機能と I/O 構成設定を持つ安全アプリケーション。セーフティ I/O ターミナルにプリセットされており、仕様をカスタマイズすることはできない。 セーフティ I/O ターミナルが制御する。	• 固定アプリケーションの中に、そのまま使用できるアプリケーションがある。	「プリセットされた安全アプリケーションでセーフティ I/O ターミナルが制御する構成 (P.1-10)」

安全アプリケーション	概要	選択基準	セーフティコントロールシステム
ユーザ定義アプリケーション	ロジック機能と I/O 構成設定を持つ安全アプリケーション。ユーザがそれぞれの設定をカスタマイズできる。 セーフティ I/O ターミナルが制御する。	• 簡単な処理のため、セーフティ I/O ターミナルのロジック機能で実現可能なアプリケーションである。 • 固定アプリケーションの中に、そのまま使用できるものがない。 • 複数のセーフティ I/O ターミナルに同じ処理をさせるため、セーフティコントローラ側で安全アプリケーションを管理したい。	「ユーザが設計した安全アプリケーションでセーフティ I/O ターミナルが制御する構成（集中管理型）（P.1-11)」
アドオンアプリケーション		• 簡単な処理のため、セーフティ I/O ターミナルのロジック機能で実現可能なアプリケーションである。 • 固定アプリケーションの中に、そのまま使用できるものがない。 • セーフティ I/O ターミナルを単体で使用するため、セーフティ I/O ターミナル側で安全アプリケーションを管理したい。	「ユーザが設計した安全アプリケーションでセーフティ I/O ターミナルが制御する構成（分散管理型）（P.1-12)」

リモート I/O モード用アプリケーション

リモート I/O モード用アプリケーションは、ユーザが Sysmac Studio を使用して I/O 構成設定だけを定義するアプリケーションです。ロジック設定は行いません。セーフティコントローラのセーフティプログラムと組み合わせて使用します。セーフティ I/O ターミナルのロジック機能では実現が難しい複雑で大規模なシステムを構築するのに向いています。
リモート I/O モード用アプリケーションをセーフティ I/O ターミナルにコンフィグレーションする方法には、以下の 2 種類があります。

- セーフティコントローラからの Type 1 Safety Open による方法
- Web UI によるコンフィグレーションによる方法

固定アプリケーション

固定アプリケーションは、あらかじめセーフティ I/O ターミナルに内蔵されている安全アプリケーションです。仕様をカスタマイズすることはできません。
固定アプリケーションには、以下の 3 種類があります。いずれも非常停止用押ボタンスイッチやセーフティライトカーテンなどを使用して、危険な事象が発生する前に駆動部やロボットを停止させるアプリケーションです。実現したいアプリケーションに合致するものがある場合に使用してください。各アプリケーションの詳細は、下表の参照先に記載されています。

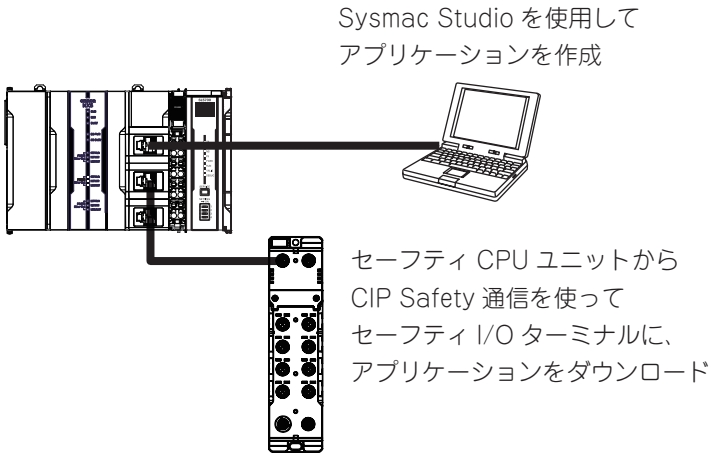
ロータリスイッチ SETTING SW1,SW2 の番号	名称	使用用途	参照先
1	部分停止+全体停止アプリケーション	セーフティライトカーテンによる部分停止と、非常停止用押ボタンスイッチによる全体停止のアプリケーション。外部機器モニタリング（EDM）なし。	「No.1 部分停止+全体停止アプリケーション (P.6-27)」

ロータリスイッチ SETTING SW1,SW2 の番号	名称	使用用途	参照先
2	部分停止+全体停止アプリケーション（EDM あり）	セーフティライトカーテンによる部分停止と、非常停止用押ボタンスイッチによる全体停止のアプリケーション。外部機器モニタリング（EDM）あり。	「No.2 部分停止+全体停止アプリケーション（EDM あり）（P.6-34)」
3	作業者とロボットのオートスイッチングアプリケーション	作業者とロボットのオートスイッチングと、非常停止用押ボタンスイッチとガードによる全体停止のアプリケーション	「No.3 作業者とロボットのオートスイッチングアプリケーション (P.6-38)」

固定アプリケーションは、ロータリスイッチの番号にあらかじめ割り付けられています。ロータリスイッチを設定することで任意の固定アプリケーションを起動できます。

ユーザ定義アプリケーション

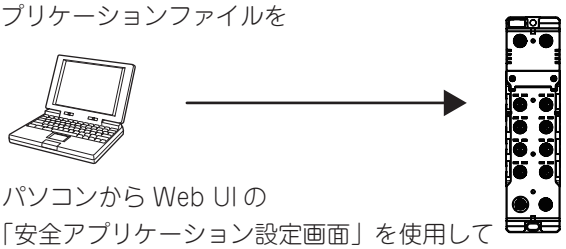
ユーザ定義アプリケーションは、ユーザが Sysmac Studio を使用して独自に作成するアプリケーションです。セーフティ CPU ユニットから CIP Safety 通信を使って、セーフティ I/O ターミナルにアプリケーションをダウンロードして使用します。
ユーザ定義アプリケーションは、CIP Safety 通信でオープンタイプ「Type1 Safety Open」のコネクションを設定することにより、セーフティ I/O ターミナルにコンフィグレーションされます。



アドオンアプリケーション

アドオンアプリケーションは、あらかじめセーフティ I/O ターミナルに内蔵されておらず、必要に応じてセーフティ I/O ターミナルに安全アプリケーションファイルをダウンロードして使用する安全アプリケーションです。
ユーザが Sysmac Studio を使用して独自のロジック設定、I/O 構成設定を行い、安全アプリケーションファイルを作成します。
その安全アプリケーションファイルを Web UI の「安全アプリケーション設定画面」を使用してセーフティ I/O ターミナルにダウンロードします。

Sysmac Studio を使用して
安全アプリケーションファイルを
作成



パソコンから Web UI の
「安全アプリケーション設定画面」を使用して
セーフティ I/O ターミナルに安全アプリケーションファイルをダウンロード

6-7-3 固定アプリケーションの詳細

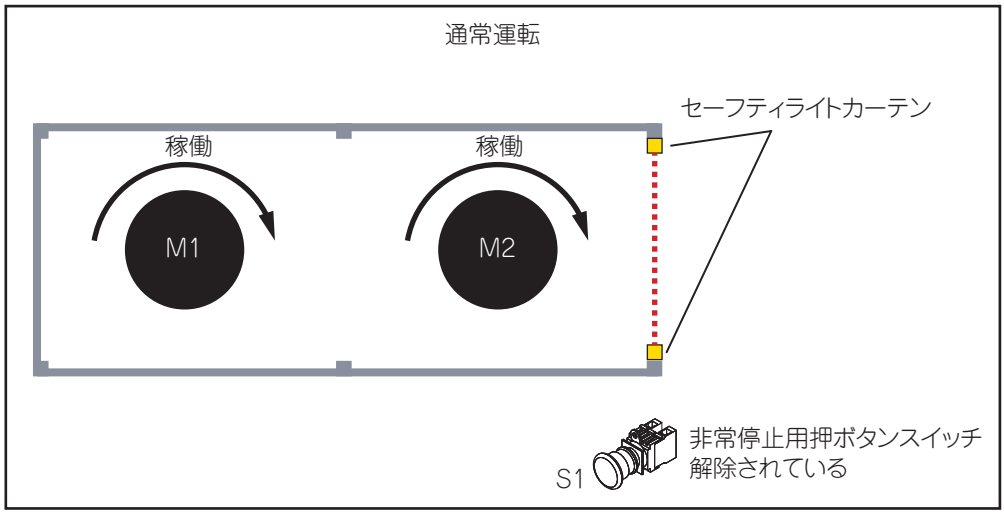
各固定アプリケーションのロジックや I/O 構成設定について説明します。

No.1 部分停止+全体停止アプリケーション

「部分停止+全体停止アプリケーション」は、セーフティライトカーテンによる部分停止と非常停止用押ボタンスイッチによる全体停止のアプリケーションです。外部機器モニタリング(EDM)は、使用しません。2 台の駆動装置を両方とも停止させる全体停止と、そのうちの 1 台だけを停止させる部分停止を使い分けます。

● アプリケーションの概要

生産現場で、2 台の駆動装置 M1、M2 が稼働しています。
駆動装置が設置されている空間は三方が壁で囲まれていますが、一方は人が作業するために開けられており、セーフティライトカーテンが設置されています。
異常が発生した場合、人が非常停止用押ボタンスイッチを押すと 2 台の駆動装置が停止します。
セーフティライトカーテンが遮光された場合は、セーフティライトカーテンに近い方の駆動装置 M2 だけが部分停止し、駆動装置 M1 は稼働を継続します。



安全カテゴリ／PL／SIL	仕様
安全カテゴリ	Up to Cat.3*1
PL	Up to PLe
SIL	Up to SIL3

***1.** 接続を想定しているセーフティサーボドライバの安全カテゴリが Cat.3 であるため、本アプリケーションの安全カテゴリも Cat.3 になります。

● 動作

各デバイスからの入力信号による動作仕様は、以下のとおりです。

非常停止用押ボタンスイッチ S1 が押された場合

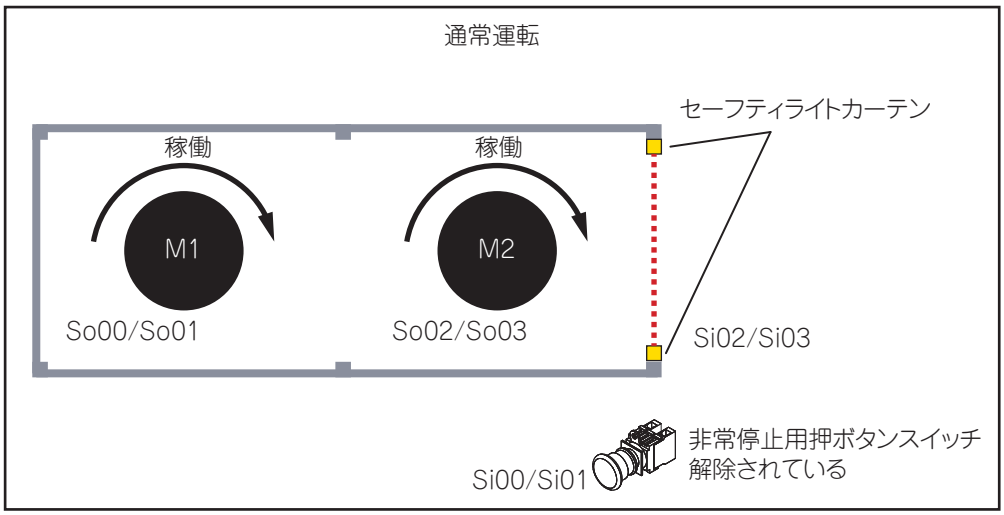
- 非常停止用押ボタンスイッチ S1 が押されると、駆動装置 M1、M2 への電源供給が即時に遮断される。
- 非常停止用押ボタンスイッチ S1 が解除され、リセットスイッチ S2 が押されるまで、駆動装置 M 1、M2 への電源供給遮断状態が保持される。

セーフティライトカーテンが遮光された場合（非常停止用押ボタンスイッチ S1 は押されていない）

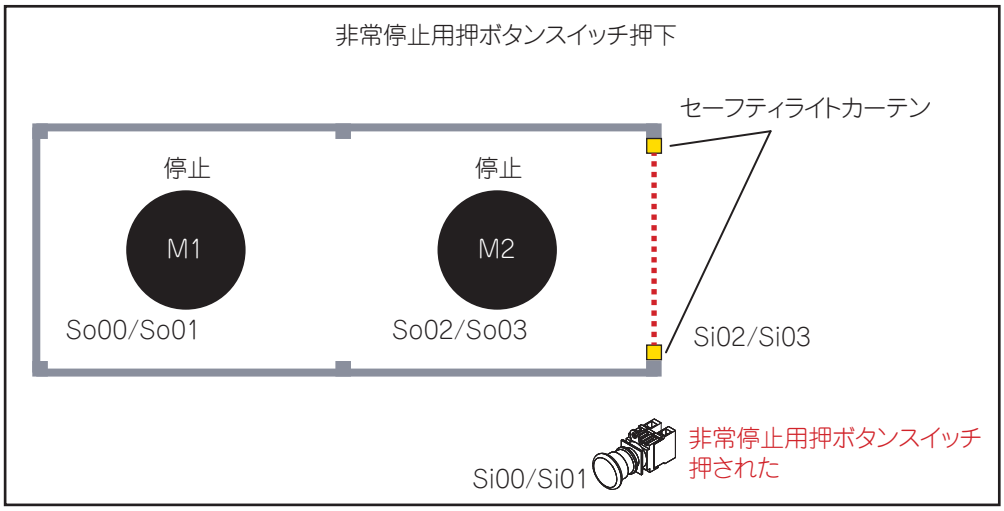
- セーフティライトカーテンが遮光されると、駆動装置 M2 への電源供給が即時に遮断される。駆動装置 M1 への電源供給は継続される。
- セーフティライトカーテンが入光され、リセットスイッチ S2 が押されるまで、駆動装置 M2 への電源供給遮断状態が保持される。

各場面での動作を、図で説明します。

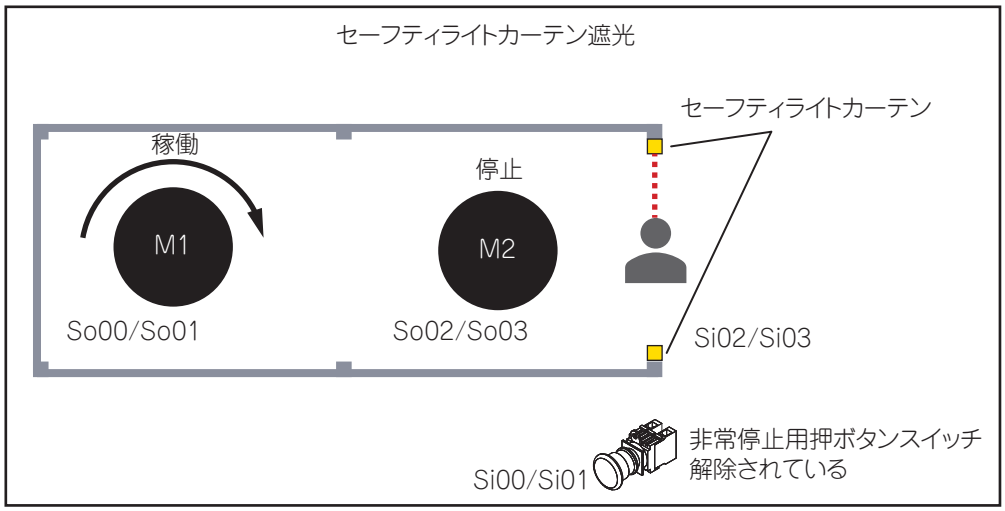
通常運転では、2 台の駆動装置 M1、M2 が稼働しています。



非常停止用押ボタンスイッチ S1 を押すと、駆動装置 M1、M2 が 2 台とも停止します。

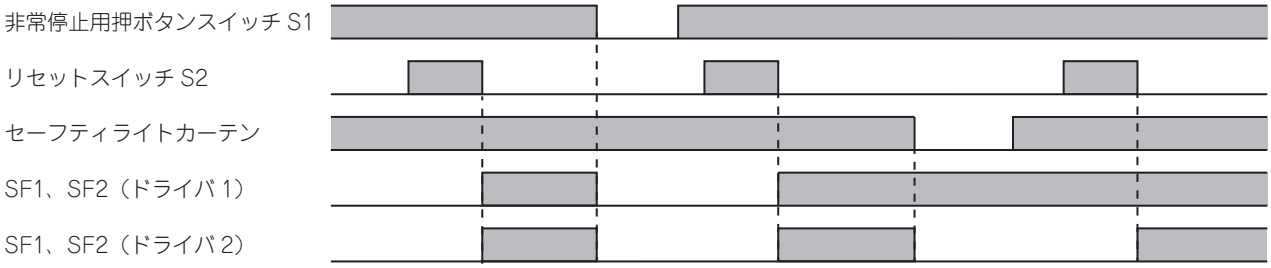


セーフティライトカーテンが遮光されると駆動装置 M2 だけが停止します。



● 動作チャート

動作チャートを以下に示します。



● I/O 構成設定

I/O 構成設定の内容は、以下のとおりです。

入力

Input	Device	Test Output Mode	ON→OFF 遅延時間	OFF→ON 遅延時間	デュアルチャネル監視時間
Si00/T00	非常停止用押ボタンスイッチ(デュアルチャネル同値入力)	Test Output	0ms	0ms	500ms
Si01/T01		Test Output	0ms	0ms	
Si02/T02	セーフティライトカーテン	Power Supply	0ms	0ms	500ms
Si03/T03		Standard Output	0ms	0ms	
Si04/T04	−	Not Used	−	−	−
Si05/T05	−	Not Used	−	−	−
Si06/T06	リセットスイッチ	Test Output	0ms	0ms	−
Si07/T07	−	Standard Output	−	−	−
Si08/T08	−	Not Used	−	−	−
Si09/T09	−	Not Used	−	−	−
Si10/T10	−	Not Used	−	−	−
Si11/T11	−	Not Used	−	−	−

入力エラーラッチ信号：1000ms

出力

Output	Device	EDM フィードバック設定	ON→OFF 遅延時間	OFF→ON 遅延時間
So00/ So01	デュアルチャネル同値出力（テストパルスあり）	未使用	0 × 100ms	0 × 100ms
So02/ So03	デュアルチャネル同値出力（テストパルスあり）	未使用	0 × 100ms	0 × 100ms

出力エラーラッチ信号：1000ms

ロジック

入力	デバイス	入力種別	リセット種別	So00/ So01	So02/ So03
Si00/Si01	非常停止用押ボタンスイッチ（デュアルチャネル同値入力）	−	Manual(Si06)	0	0
Si02/Si03	セーフティライトカーテン	−	Manual(Si06)	1	0

リセット信号	最小 ON パルス幅[ms]	最大 ON パルス幅[ms]
Si06	350	2000

電源投入時モード：Executing

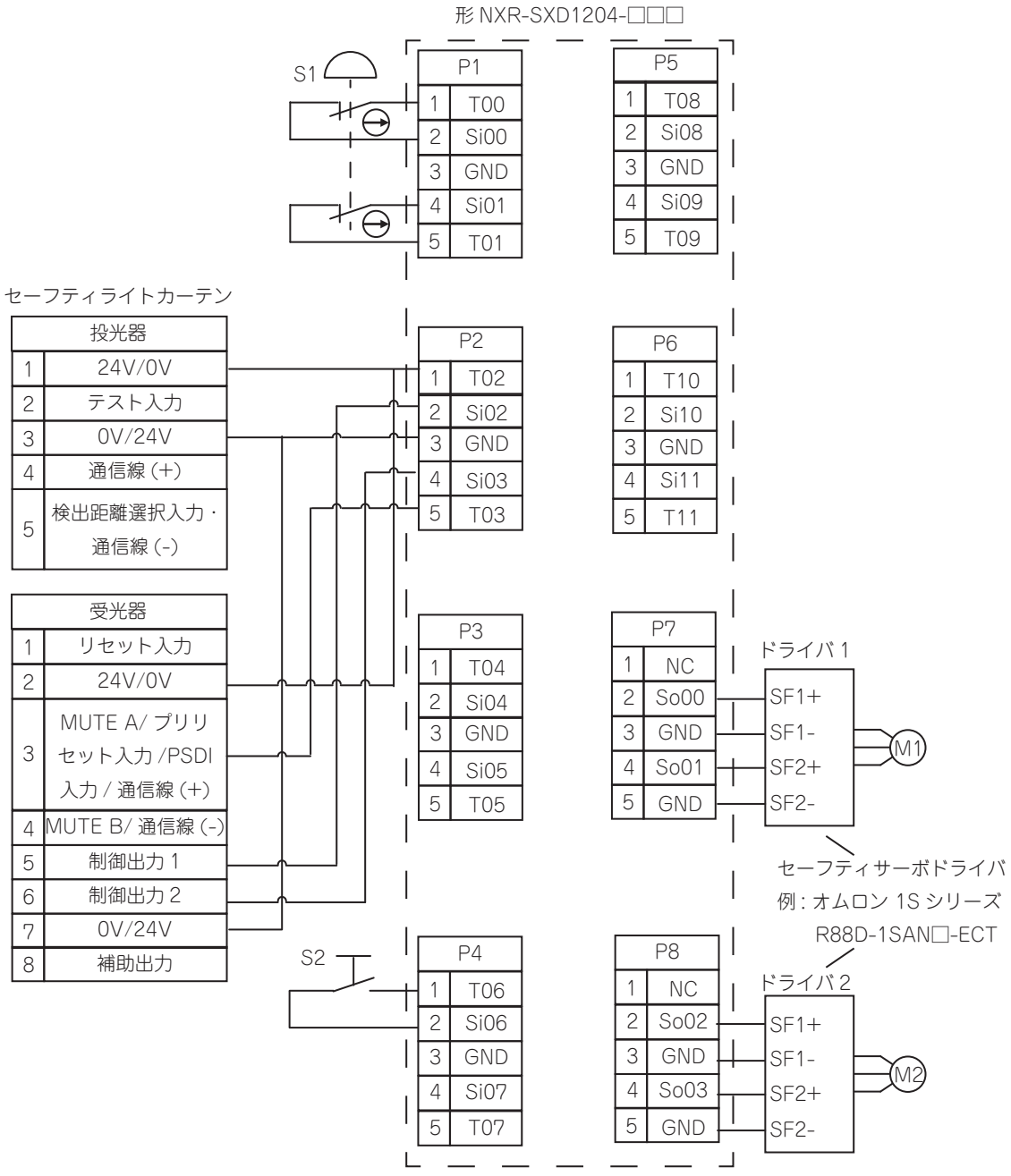
署名

セーフティコンフィグレーション CRC（SCCRC）：519F5023
セーフティコンフィグレーションタイムスタンプ(SCTS)：4D0C00000000

● 結線図

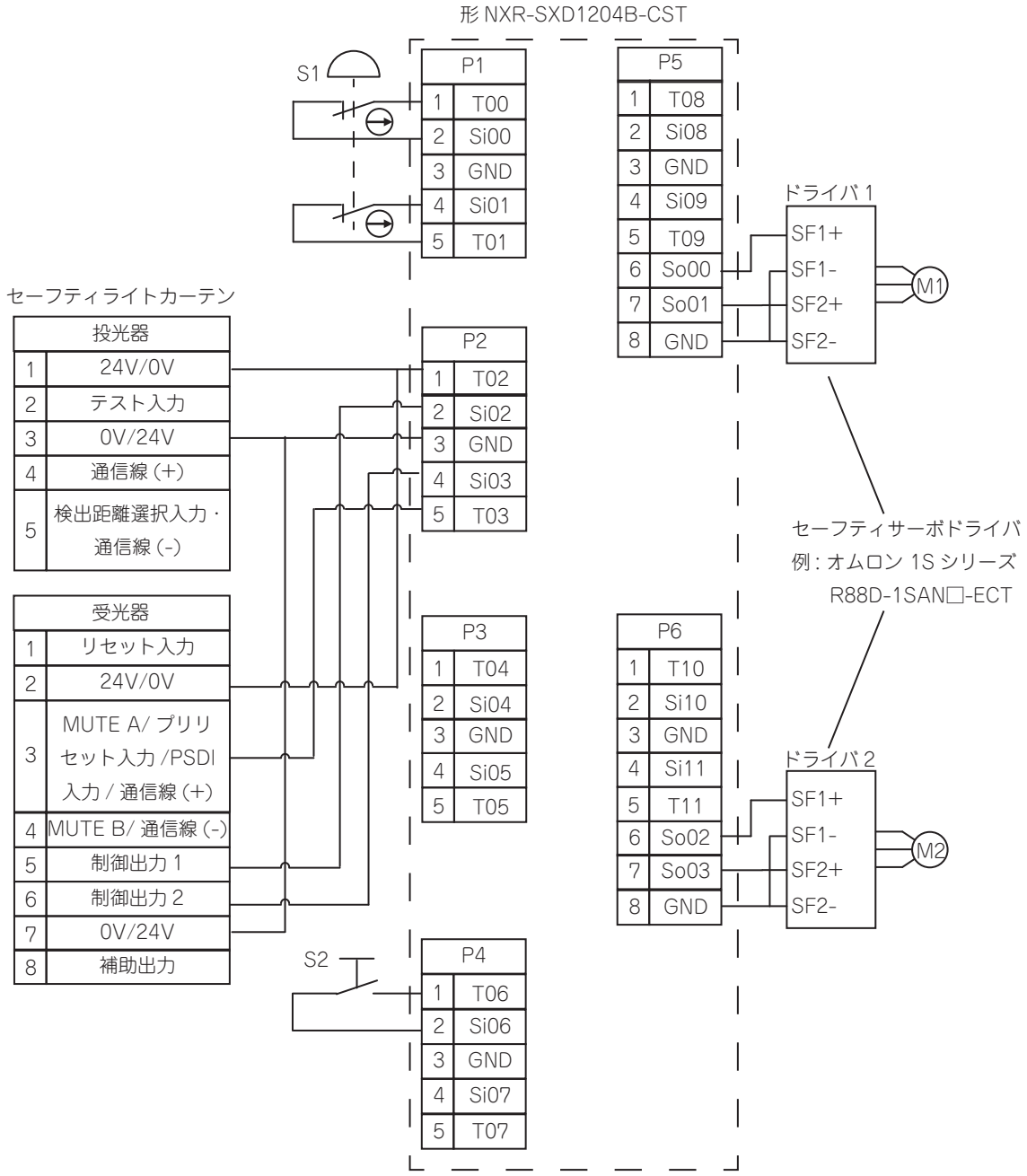
形 NXR-SXD1204-□□□の結線図を以下に示します。

S1 : 非常停止用押ボタンスイッチ
S2 : リセットスイッチ
SF1、SF2 : セーフティサーボドライバの STO 機能のセーフティ入力
M1、M2 : 駆動装置



形 NXR-SXD1204B-CST の結線図を以下に示します。

S1 : 非常停止用押ボタンスイッチ
S2 : リセットスイッチ
SF1、SF2 : セーフティサーボドライバの STO 機能のセーフティ入力
M1、M2 : 駆動装置



● 注意事項

使用上の注意

- セーフティライトカーテンと非常停止用押ボタンスイッチは、システムの安全要求レベルに応じて選定してください。
- セーフティサーボドライバは、EDM を使用せずにシステムの安全要求レベルを実現できる機器を選定してください。
- サーボドライバのセーフティ入力回路の故障を検出するため、機能テストを 6 か月ごとに実施してください。
- システム全体の規格の適合については、お客様の責任において対応してください。
- 電気的およびメカ的な故障を検出するために、二重化された半導体出力接点と、二重化されたメカ式出力機器を組み合わせて使用してください。

No.2 部分停止+全体停止アプリケーション（EDM あり）

「部分停止+全体停止アプリケーション（EDM あり）」は、セーフティライトカーテンによる部分停止と非常停止用押ボタンスイッチによる全体停止のアプリケーションです。「部分停止+全体停止アプリケーション」に、外部機器モニタリング(EDM)を追加したものです。

● アプリケーションの概要

アプリケーションの内容は、「部分停止+全体停止アプリケーション」と同じです。

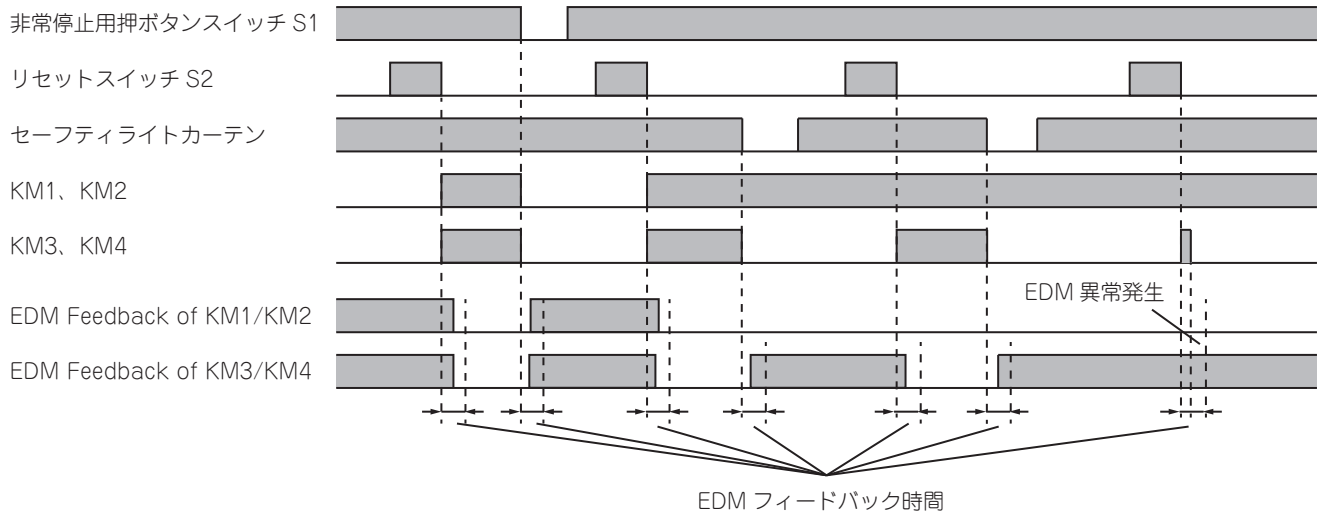
安全カテゴリ／PL／SIL	仕様
安全カテゴリ	Up to Cat.4
PL	Up to PLe
SIL	Up to SIL3

● 動作

動作は、「部分停止+全体停止アプリケーション」と同じです。

● 動作チャート

動作チャートを以下に示します。



● I/O 構成設定

I/O 構成設定の内容は、以下のとおりです。

入力

Input	Device	Test Output Mode	ON→OFF 遅延時間	OFF→ON 遅延時間	デュアルチャネル監視時間
Si00/T00	非常停止用押ボタンスイッチ（デュアルチャネル同値入力）	Test Output	0ms	0ms	500ms
Si01/T01		Test Output	0ms	0ms	
Si02/T02	セーフティライトカーテン	Power Supply	0ms	0ms	500ms
Si03/T03		Standard Output	0ms	0ms	
Si04/T04	−	Not Used	−	−	−
Si05/T05	−	Not Used	−	−	−
Si06/T06	リセットスイッチ	Test Output	0ms	0ms	−
Si07/T07	−	Not Used	−	−	−
Si08/T08	EDM フィードバック	Test Output	0ms	0ms	−
Si09/T09	−	Not Used	−	−	−
Si10/T10	EDM フィードバック	Test Output	0ms	0ms	−
Si11/T11	−	Not Used	−	−	−

入力エラーラッチ信号：1000ms

出力

Output	Device	EDM フィードバック設定	ON→OFF 遅延時間	OFF→ON 遅延時間
So00/ So01	デュアルチャネル同値出力（テストパルスあり）	Si08	0 × 100ms	0 × 100ms
So02/ So03	デュアルチャネル同値出力（テストパルスあり）	Si10	0 × 100ms	0 × 100ms

出力エラーラッチ信号：1000ms

ロジック

入力	デバイス	入力種別	リセット種別	So00/ So01	So02/ So03
Si00/Si01	非常停止用押ボタンスイッチ（デュアルチャネル同値入力）	−	Manual(Si06)	0	0
Si02/Si03	セーフティライトカーテン	−	Manual(Si06)	1	0

リセット信号	最小 ON パルス幅[ms]	最大 ON パルス幅[ms]
Si06	350	2000

電源投入時モード：Executing

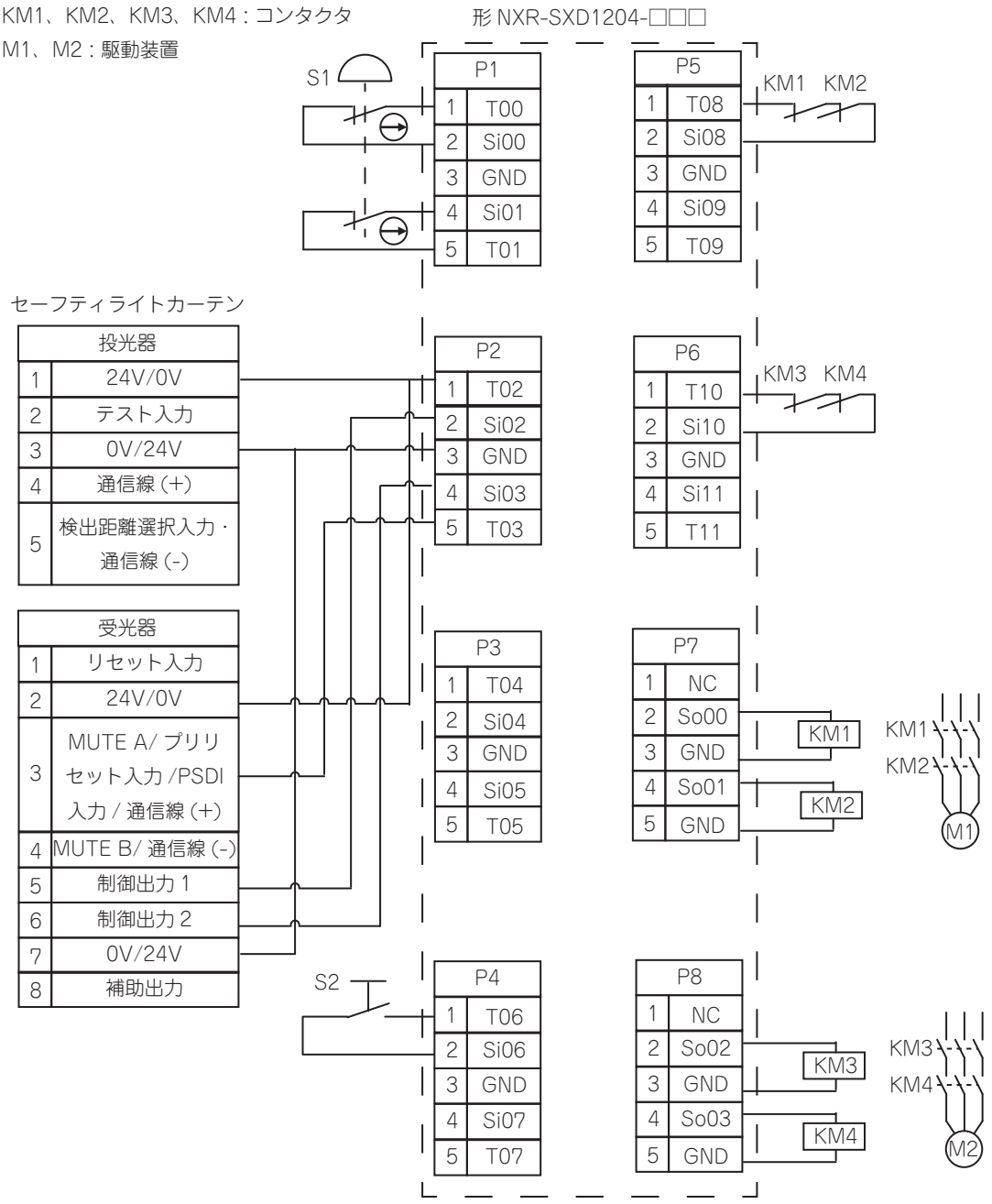
署名

セーフティコンフィグレーション CRC（SCCRC）：C54E34C8
セーフティコンフィグレーションタイムスタンプ(SCTS)：4D0C00000000

● 結線図

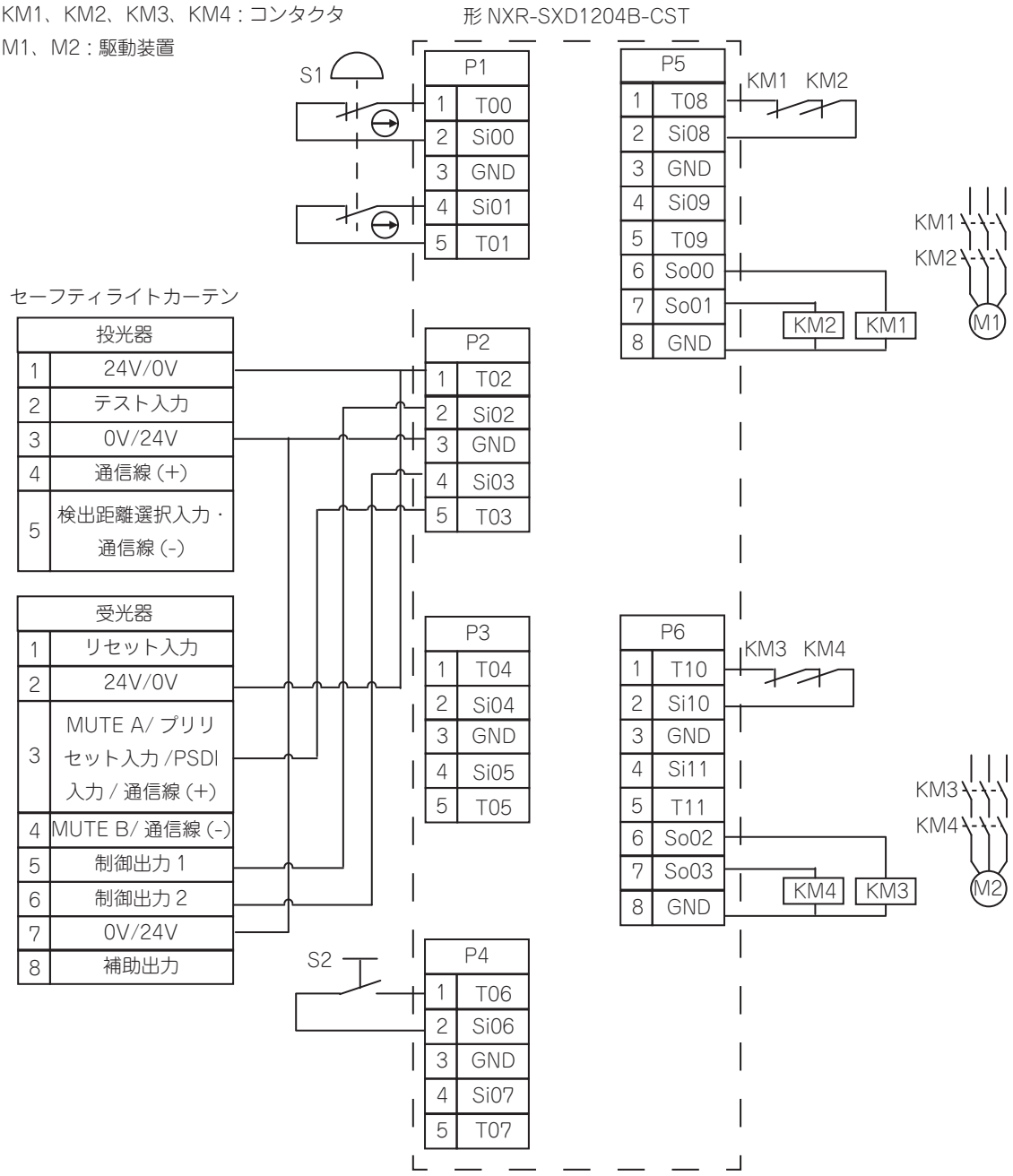
形 NXR-SXD1204-□□□の結線図を以下に示します。

S1：非常停止用押ボタンスイッチ
S2：リセットスイッチ
KM1、KM2、KM3、KM4：コンタクタ
M1、M2：駆動装置



形 NXR-SXD1204B-CST の結線図を以下に示します。

S1：非常停止用押ボタンスイッチ
S2：リセットスイッチ
KM1、KM2、KM3、KM4：コンタクタ
M1、M2：駆動装置



● 注意事項

使用上の注意

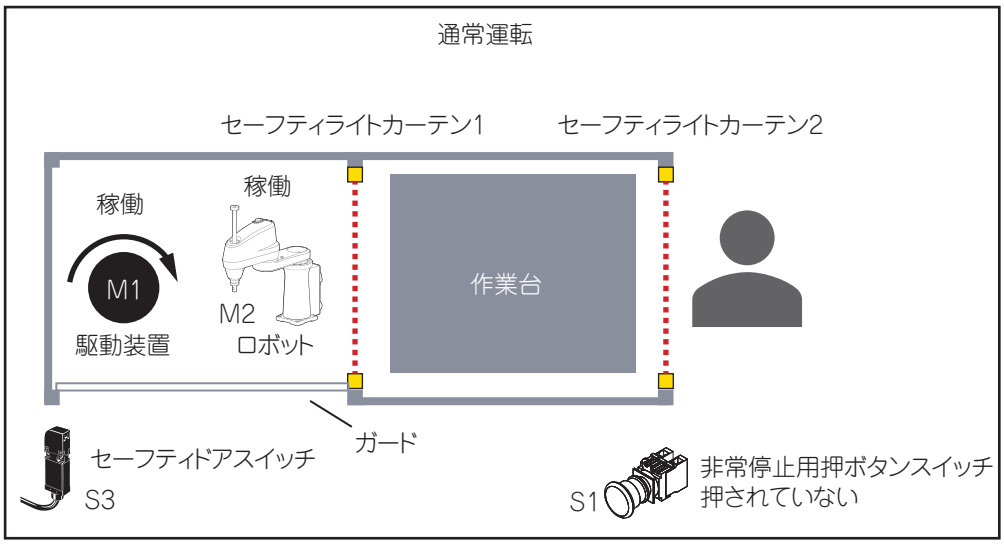
- セーフティライトカーテンと非常停止用押ボタンスイッチは、システムの安全要求レベルに応じて選定してください。
- コンタクタ接点の溶着故障を検出するため、機能テストを 1 か月ごとに実施してください。
- システム全体の規格の適合については、お客様の責任において対応してください。
- 電気的およびメカ的な故障を検出するために、二重化された半導体出力接点と、二重化されたメカ式出力機器を組み合わせて使用してください。

No.3 作業者とロボットのオートスイッチングアプリケーション

「作業者とロボットのオートスイッチングアプリケーション」は、作業者とロボットのオートスイッチングと、非常停止用押ボタンとガードによる全体停止のアプリケーションです。作業者とロボットが接触しないように、必要に応じてロボットを停止させます。

● アプリケーションの概要

生産現場で、1 台の駆動装置と 1 台のロボットが稼働しています。
ロボットの横には作業台があります。ロボットが作業台に製品を置くと、人が反対側からその製品を受け取ります。
作業台の両側にはセーフティライトカーテンが設置されています。ロボットと人の両方が作業台にアクセスすると危険なので、2 対のセーフティライトカーテンが両方とも遮光されるとロボットが停止します。その際、ロボットの奥にある駆動装置は停止しません。
駆動装置とロボットが設置されている空間には、メンテナンスのためのガードがありセーフティドアスイッチが設置されています。人がドアを開けると駆動装置とロボットの両方が全停止します。
異常が発生した場合、人が非常停止用押ボタンスイッチを押します。その場合も駆動装置とロボットの両方が全停止します。



安全カテゴリ／PL／SIL	仕様
安全カテゴリ	Up to Cat.3
PL	Up to PLe
SIL	Up to SIL3

● 動作

各デバイスからの入力信号による動作仕様は、以下のとおりです。

非常停止用押ボタンスイッチ S1 が押された場合

- 非常停止用押ボタンスイッチ S1 が押されると、駆動装置 M1 およびロボット M2 への電源供給が即時に遮断される。
- ガードが閉じられていて、セーフティライトカーテン 1 またはセーフティライトカーテン 2 が入光され、かつ非常停止用押ボタンスイッチ S1 が解除され、リセットスイッチ S2 が押されるまで、ロボット M2 への電源供給遮断状態が保持される。
- ガードが閉じられていて、かつ非常停止用押ボタンスイッチ S1 が解除され、リセットスイッチ S2 が押されるまで、駆動装置 M1 への電源供給遮断状態が保持される。

ガードが開いた場合（非常停止用押ボタンスイッチ S1 は押されていない）

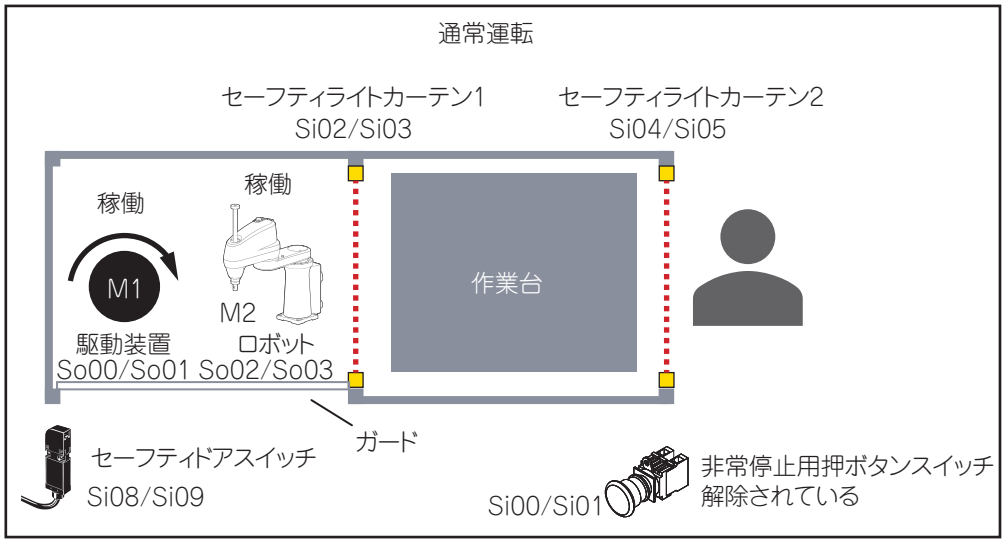
- ガードが開かれたことがセーフティドアスイッチ S3 で検出され、駆動装置 M1 およびロボット M2 への電源供給が即時に遮断される。
- ガードが閉じられ、セーフティライトカーテン 1 またはセーフティライトカーテン 2 が入光され、リセットスイッチ S2 が押されるまで、ロボット M2 への電源供給遮断状態が保持される。
- ガードが閉じられ、リセットスイッチ S2 が押されるまで、駆動装置 M1 への電源供給遮断状態が保持される。

セーフティライトカーテンが遮光された場合（非常停止用押ボタンスイッチ S1 は押されていない、かつガードは閉じられている）

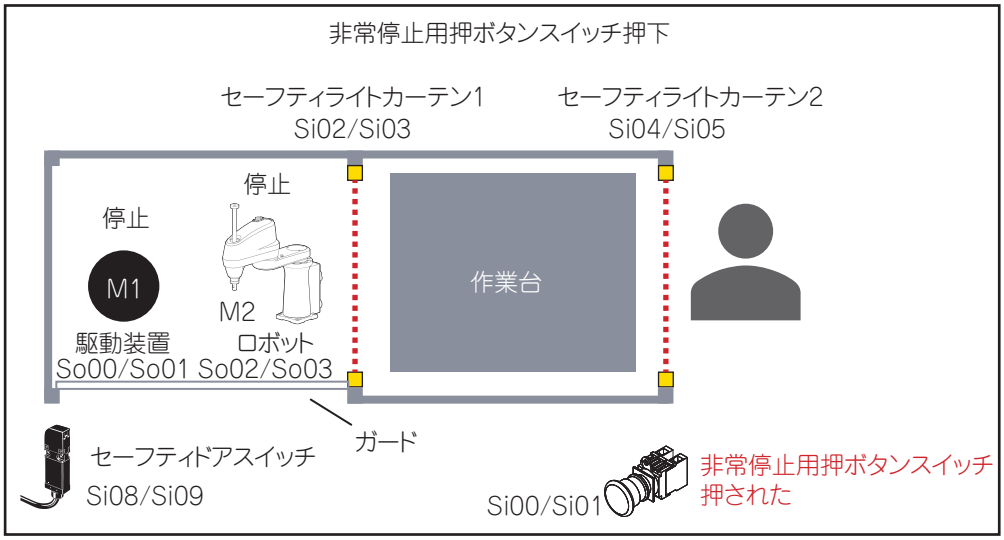
- セーフティライトカーテン 1 とセーフティライトカーテン 2 の両方が遮光されると、ロボット M2 への電源供給が即時に遮断される。駆動装置 M1 への電源供給は継続される。
- セーフティライトカーテン 1 またはセーフティライトカーテン 2 が入光されるまで、ロボット M2 への電源供給遮断状態が保持される。

各場面での動作を、図で説明します。

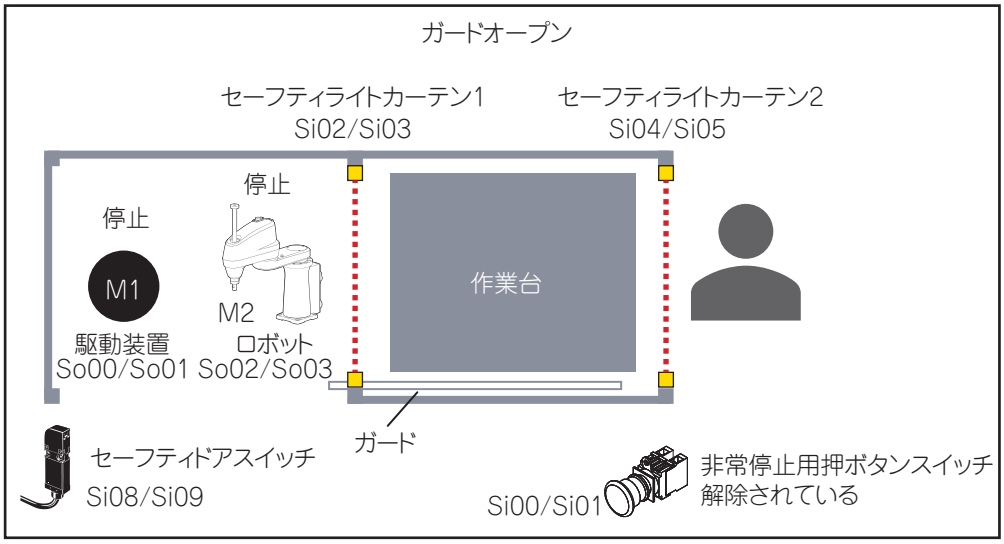
通常運転では、1 台の駆動装置 M1 と 1 台のロボット M2 が稼働しています。



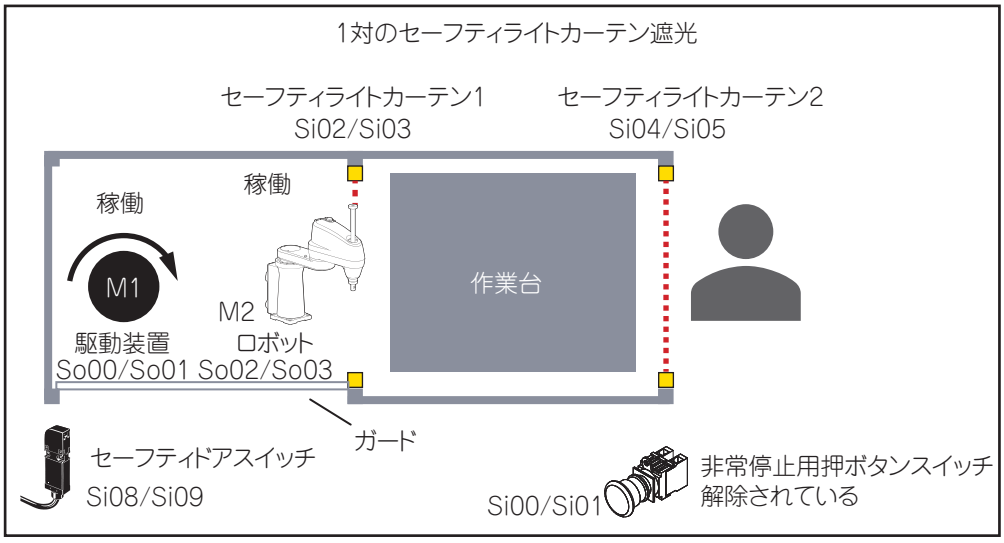
非常停止用押ボタンスイッチ S1 を押すと、駆動装置 M1 もロボット M2 も停止します。

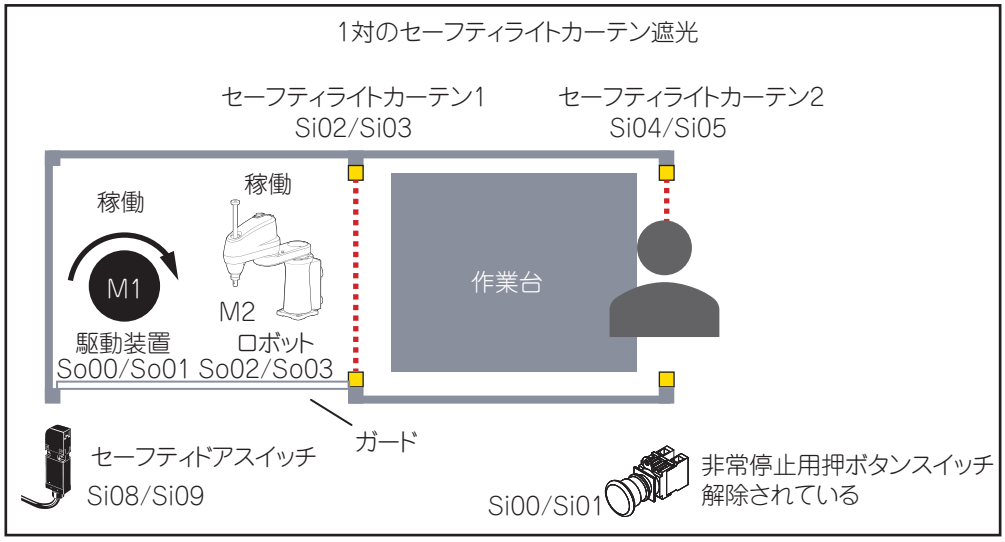


ガードが開いた場合、駆動装置 M1 とロボット M2 の両方が停止します。

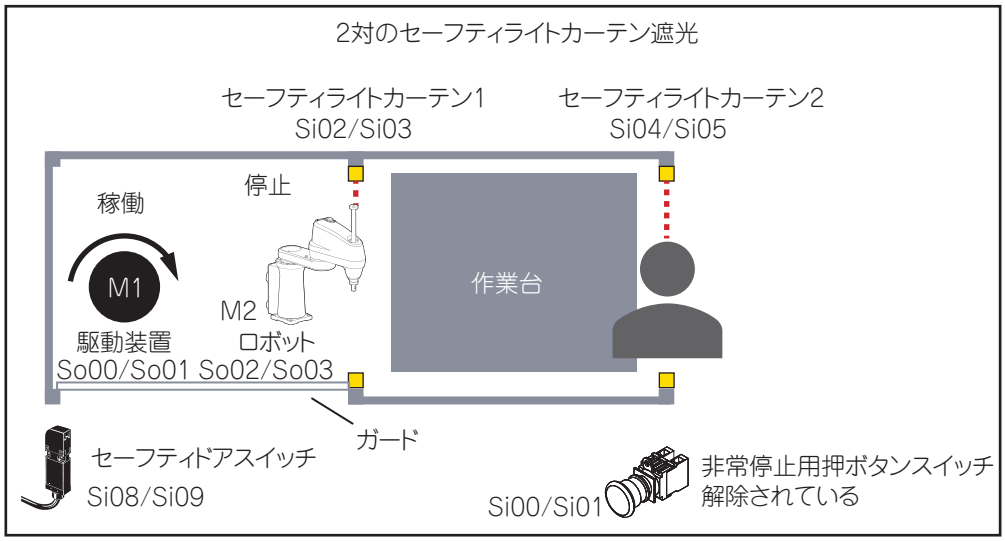


2 対のセーフティライトカーテンのうち 1 対が遮光されても、駆動装置 M1 もロボット M2 も稼働を続けます。



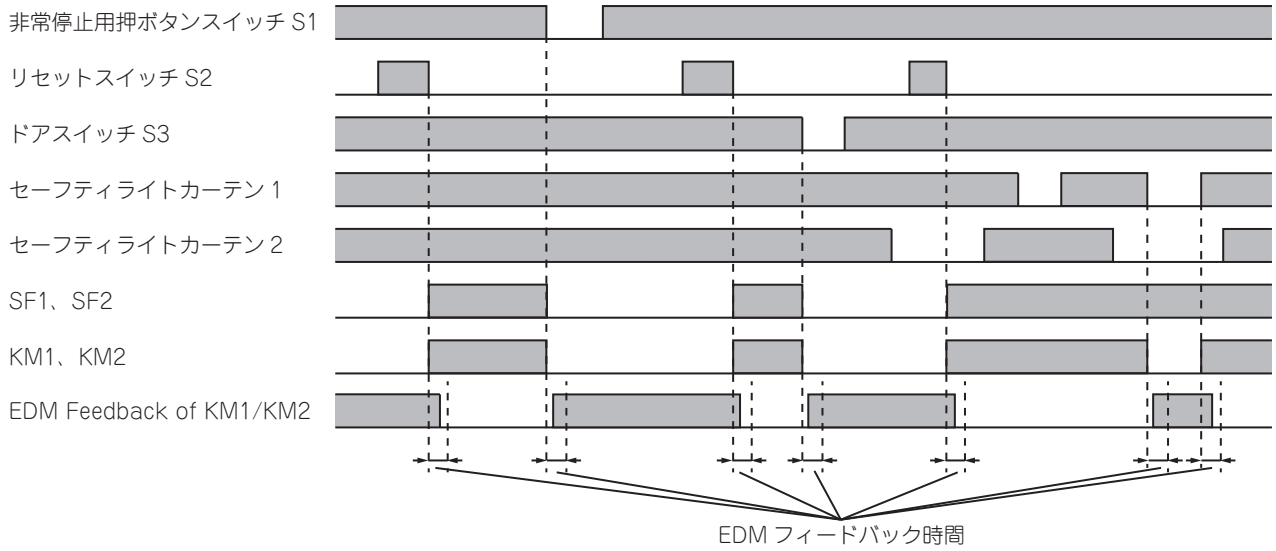


2 対のセーフティライトカーテンの両方が遮光されると、作業者とロボット M2 の接触の危険があるため、ロボット M2 が停止します。駆動装置 M1 は稼働を続けます。



● 動作チャート

動作チャートを以下に示します。



● I/O 構成設定

I/O 構成設定の内容は、以下のとおりです。

入力

Input	Device	Test Output Mode	ON→OFF 遅延時間	OFF→ON 遅延時間	デュアルチャネル監視時間
Si00/T00	非常停止用押ボタンスイッチ（デュアルチャネル同値入力）	Test Output	0ms	0ms	500ms
Si01/T01		Test Output	0ms	0ms	
Si02/T02	セーフティライトカーテン	Power Supply	0ms	0ms	500ms
Si03/T03		Standard Output	0ms	0ms	
Si04/T04	セーフティライトカーテン	Power Supply	0ms	0ms	500ms
Si05/T05		Standard Output	0ms	0ms	
Si06/T06	リセットスイッチ	Test Output	0ms	0ms	—
Si07/T07	—	Standard Output	—	—	—
Si08/T08	セーフティ・ドアスイッチ（デュアルチャネル同値入力）	Test Output	0ms	0ms	500ms
Si09/T09		Test Output	0ms	0ms	
Si10/T10	EDM フィードバック	Test Output	0ms	0ms	—
Si11/T11	—	Not Used	—	—	—

入力エラーラッチ信号：1000ms

出力

Output	Device	EDM フィードバック設定	ON→OFF 遅延時間	OFF→ON 遅延時間
So00/So01	デュアルチャネル同値出力（テストパルスあり）	未使用	0 × 100ms	0 × 100ms
So02/So03	デュアルチャネル同値出力（テストパルスあり）	Si10	0 × 100ms	0 × 100ms

出力エラーラッチ信号：1000ms

ロジック

入力	デバイス	入力種別	リセット種別	So00/ So01	So02/ So03
Si00/Si01	非常停止用押ボタンスイッチ（デュアルチャネル同値入力）	−	Manual(Si06)	0	0
Si08/Si09	セーフティ・ドアスイッチ（デュアルチャネル同値入力）	−	Manual(Si06)	0	0
Si02/Si03	セーフティライトカーテン	2 Input(OR)	Auto	1	0
Si04/Si05	セーフティライトカーテン				

リセット信号	最小 ON パルス幅[ms]	最大 ON パルス幅[ms]
Si06	350	2000

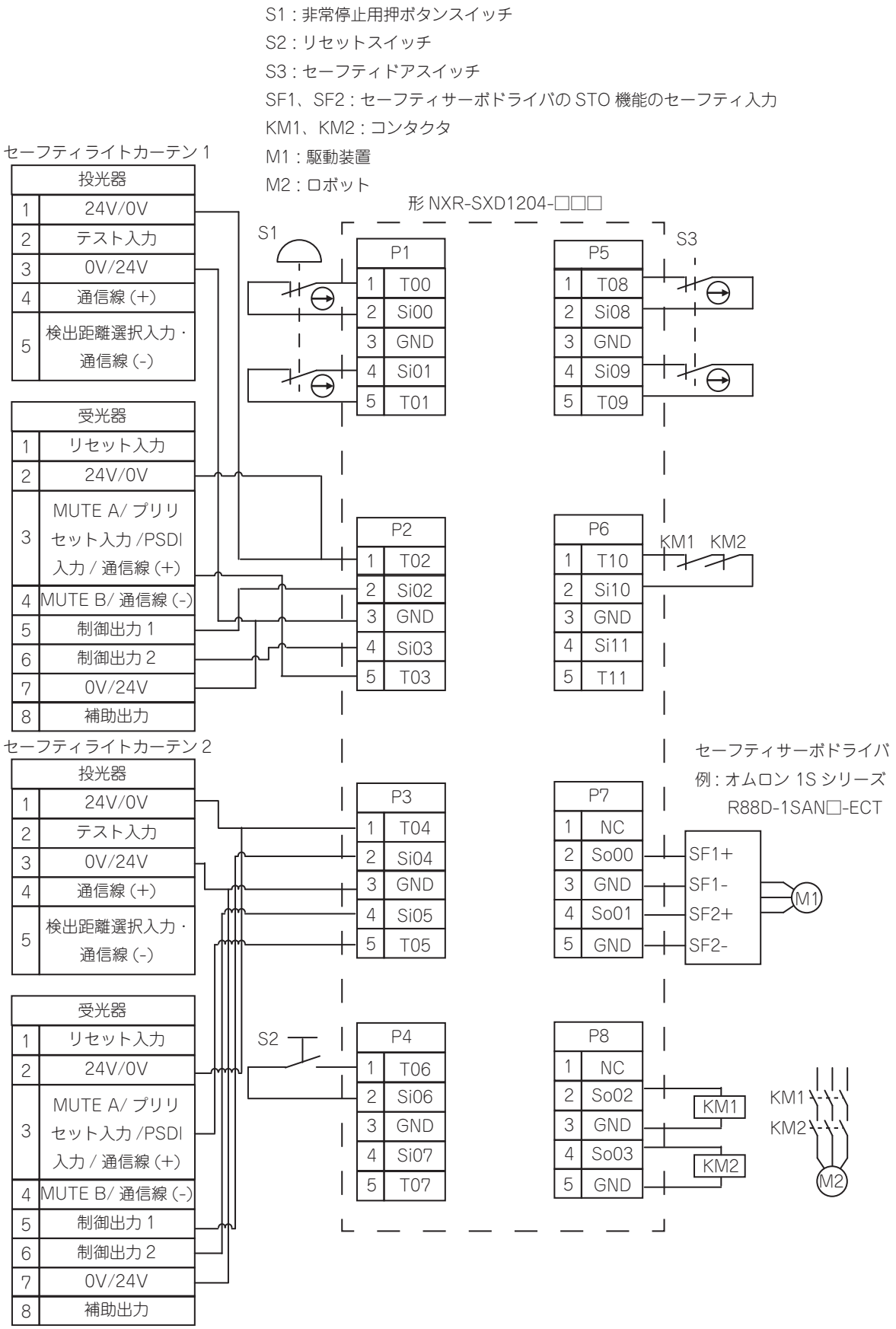
電源投入時モード：Executing

署名

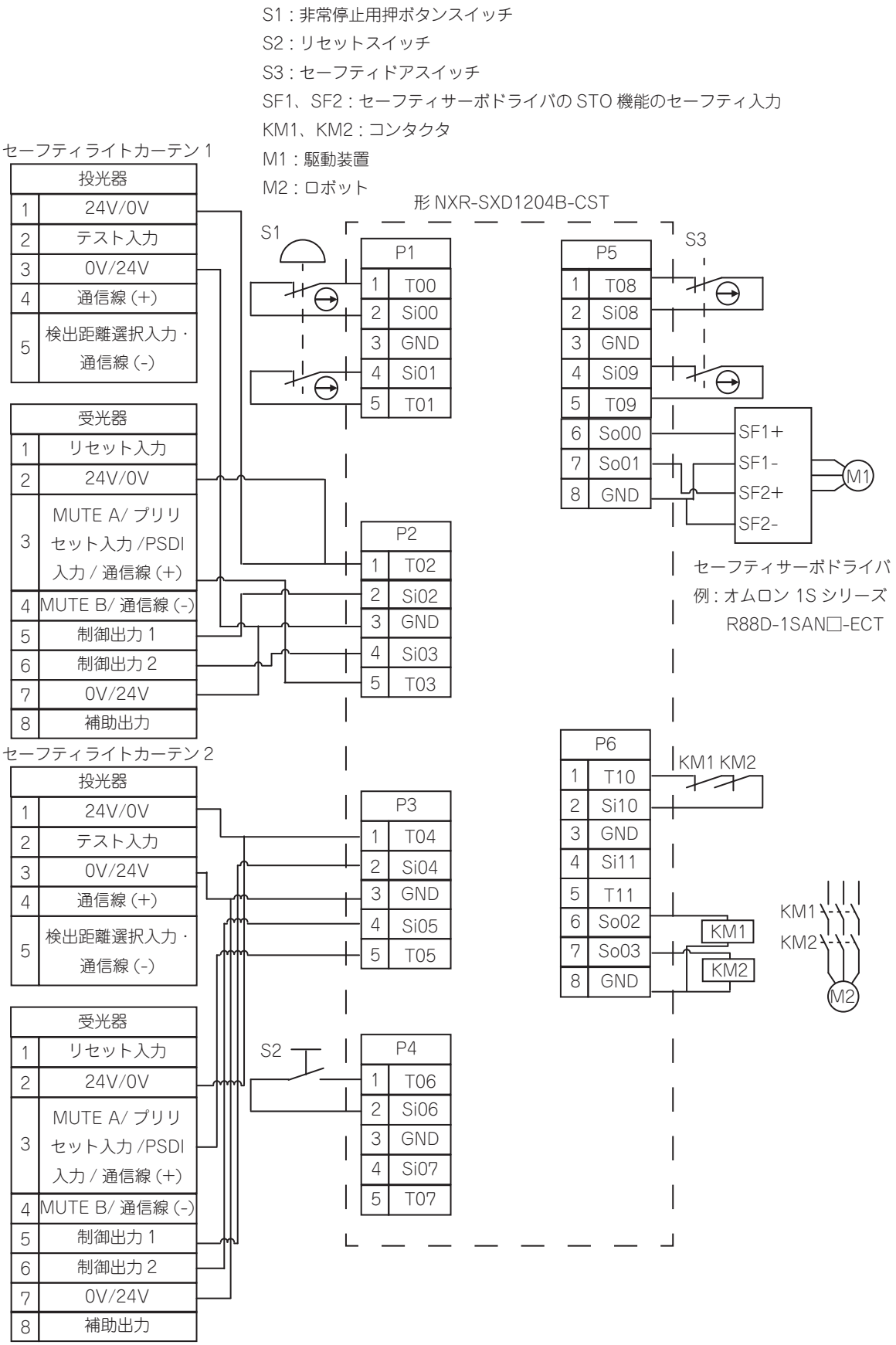
セーフティコンフィグレーション CRC（SCCRC）: F63EF4B6
セーフティコンフィグレーションタイムスタンプ(SCTS) : 4D0C00000000

● 結線図

形 NXR-SXD1204-□□□の結線図を以下に示します。



形 NXR-SXD1204B-CST の結線図を以下に示します。



● 注意事項

使用上の注意

- 接続機器は、システムの安全要求レベルに応じて選定してください。
- セーフティサーボドライバは、EDM を使用せずにシステムの安全要求レベルを実現できる機器を選定してください。
- コンタクタ接点の溶着故障を検出するため、機能テストを 1 か月ごとに実施してください。
- サーボドライバのセーフティ入力回路の故障を検出するため、機能テストを 6 か月ごとに実施してください。
- システム全体の規格の適合については、お客様の責任において対応してください。
- 電気的およびメカ的な故障を検出するために、二重化された半導体出力接点と、二重化されたメカ式出力機器を組み合わせて使用してください。
- ガードと共同するインタロック装置の、無効化の可能性を最小にするための追加方策については、ISO14119:2013 を参照してください。

6-8 動作モード

セーフティ I/O ターミナルの動作モードについて説明します。

6-8-1 動作モードの種類

セーフティ I/O ターミナルには、以下の動作モードがあります。
動作モードは、MS LED や Web UI の動作状態モニタで確認することができます。

動作モード	Web UI での表示	MS LED の状態	リモート I/O モードの場合の動作	簡易ロジックモードの場合の動作
運転状態 (Executing)	Executing	緑点灯	セーフティ I/O ターミナルが運転中の状態 すべての機能が動作しており、通常運転が行われている。 この状態における主なセーフティ機能の状態は、以下のとおり。 • ロジック機能：無効 • CIP Safety 通信：コネクション確立中 • セーフティ入力：有効 • セーフティ出力：有効 運転待ち状態(Idle)において CIP Safety コネクションが開設されると、本状態に遷移する。	セーフティ I/O ターミナルが運転中の状態 すべての機能が動作しており、通常運転が行われている。 この状態における主なセーフティ機能の状態は、以下のとおり。 • ロジック機能：実行 • CIP Safety 通信：通信可能 • セーフティ入力：有効 • セーフティ出力：有効 運転待ち状態(Idle)において動作モード変更機能により運転状態が指示されると、本状態に遷移する。
運転待ち状態 (Idle)	Idle	緑点滅	安全コンフィグレーションが完了しており、運転状態(Executing)への移行を待っている状態 この状態における主なセーフティ機能の状態は、以下のとおり。 • ロジック機能：無効 • CIP Safety 通信：コネクション確立待ち • セーフティ入力：有効 • セーフティ出力：クリア 運転状態(Executing)において CIP Safety コネクションがすべて切断されると、本状態に遷移する。	安全コンフィグレーションが完了しており、運転状態(Executing)への移行を待っている状態 この状態における主なセーフティ機能の状態は、以下のとおり。 • ロジック機能：停止 • CIP Safety 通信：通信可能 • セーフティ入力：有効 • セーフティ出力：クリア 運転状態(Executing)において動作モード変更機能により運転待ち状態が指示されると、本状態に遷移する。
TUNID 設定待ち状態 (Waiting for TUNID)	Waiting for TUNID	緑赤点滅	TUNID が設定されていない状態 この状態で IP アドレスのソフトウェア設定を実行することができる。	
コンフィグレーション待ち状態 (Configuring)	Configuring	緑赤点滅	TUNID 設定が完了しており、安全コンフィグレーションが実施されていない状態	
運転停止異常 (Abort)	Abort	赤点滅	回復可能な異常が発生している状態	
致命的な異常 (Critical Fault)	Critical Fault	赤点灯	致命的な異常が発生している状態 すべての機能を停止して、安全状態に移行する。	
初期処理中 (Self-Testing)	Self-Testing	緑赤点滅	セーフティ機能を保証するために必要な自己診断を実行中の状態	−

動作モード	Web UI での表示	MS LED の状態	リモート I/O モードの場合の動作	簡易ロジックモードの場合の動作
IP アドレス表示（IP Address Display）	Web UI アクセス不可	消灯	IP アドレス表示機能を実行中の状態	−
I/O 配線チェック）（I/O Wiring Checking）	読み出し不可 Web UI アクセス不可	消灯	I/O 配線チェック機能を実行中の状態	−

6-8-2 各動作モードで実行可能な機能

各動作モードにおける機能の実行可否は、以下のとおりです。

機能	通常の動作モード							特殊モード	
	初期処理中 (Self-Testing)	TUNID 設定待ち状態 (Waiting for TUNID)	コンフィグレーション待ち状態 (Configuring)	運転待ち状態 (Idle)	運転状態 (Executing)	運転停止異常 (Abort)	致命的な異常 (Critical Fault)	IP アドレス表示 (IP Address Display)	I/O 配線チェック）(I/O Wiring Checking)
CIP Safety 通信	不可	不可	不可	可	可	不可	不可	不可	不可
EtherNet/IP 通信	不可	不可	不可	可	可	不可	不可	不可	不可
CIP メッセージ通信	不可	可	可	可	可	可	不可	不可	不可
Web UI からのアクセス	不可	可	可	可	可	可	不可	不可	不可
セーフティ入力機能	不可	不可	不可	可	可	可	不可	不可	可*1
テスト出力機能	不可	不可	不可	可	可	可	不可	不可	可*1
セーフティ出力機能	不可	不可	不可	不可	可	可	不可	不可	可*1
IP アドレス設定機能	不可	可	不可	不可	不可	不可	不可	不可	不可
渡り配線出力用電源遮断機能	不可	可	可	可	可	可	不可	不可	不可
簡易ロジック機能	不可	不可	不可	不可	可*2	不可	不可	不可	可*1
I/O 配線チェック機能	不可	不可	不可	不可	不可	不可	不可	不可	可
IP アドレス表示機能	不可	不可	不可	不可	不可	不可	不可	可	不可
バックアップ機能のバックアップ	不可	不可	不可	可	可	不可	不可	不可	不可
バックアップ機能の照合	不可	可	可	可	可	可	不可	不可	不可
バックアップ機能のリストア	不可	可	可	可*3	可*3	可	不可	不可	不可
ファームウェアアップデート機能	不可	可	可	可*3	可*3	可	不可	不可	不可
セーフティパスワード変更	不可	可	可	可	可	可	不可	不可	不可
動作モード変更機能	不可	不可	不可	可	可	不可	不可	不可	不可
コンフィグレーションロック機能	不可	不可	不可	可	可	可*4	不可	不可	不可
再起動機能	不可	可	可	可*3	可*3	可	不可	不可	不可
メモリオールクリア機能	不可	可	可	可*3	可*3	可	不可	不可	不可

***1.** I/O 配線チェック専用設定で動作します。
***2.** リモート I/O モードでは、簡易ロジック演算機能は動作しません。
***3.** CIP Safety 通信のコネクション確立中は、実行できません。
***4.** コンフィグレーションロックの解除だけ可能です。

6-8-3 各動作モードで実行可能な Web UI 機能

各動作モードにおける Web UI 機能の実行可否は、以下のとおりです。

画面	機能	動作モード				
		TUNID 設定待ち状態 (Waiting for TUNID)	コンフィグレーション待ち状態 (Configuring)	運転待ち状態 (Idle)	運転状態 (Executing)	運転停止異常 (Abort)
動作状態モニタ画面	動作状態モニタ	可	可	可	可	可
I/O モニタ画面	I/O モニタ	可	可	可	可	可
発生中異常・イベントログ画面	発生中異常表示	可	可	可	可	可
	イベントログ表示、ファイル出力	可	可	可	可	可
	イベントログクリア	可	可	可	可	可
生産情報画面	生産情報表示	可	可	可	可	可
TCP/IP 設定画面	TCP/IP 設定書き込み	可	不可	不可	不可	不可
	TCP/IP 設定読み出し	可	可	可	可	可
TUNID 設定画面	TUNID 書き込み	可	不可	不可	不可	不可
	TUNID 読み出し	可	可	可	可	可
安全アプリケーション設定画面	安全アプリケーション設定表示	可	可	可	可	可
	安全アプリケーション設定書き込み、削除	可	可	可	可	可
時計情報自動調整機能設定画面	時計情報自動調整機能設定書き込み	可	可	可	可	可
	時計情報自動調整機能設定読み出し	可	可	可	可	可
動作モード変更画面	動作モード変更	不可	不可	可	可	不可
コンフィグレーションロック画面	コンフィグレーションロック	不可	不可	可	可	不可
	コンフィグレーションロック解除	不可	不可	可	可	可
再起動画面	再起動	可	可	可*1	可*1	可
メモリオールクリア画面	メモリオールクリア	可	可	可*1	可*1	可
バックアップ	バックアップ	不可	不可	可	可	不可
	照合	可	可	可	可	可
	リストア	可	可	可*1	可*1	可
汎用 CIP コマンド送信画面	汎用 CIP コマンド送信	可	可	可	可	可
ユニット特定画面	ユニット特定	可	可	可	可	可
通信ケーブル診断画面	通信ケーブル診断	可	可	可	可	可
セーフティパスワード設定画面	セーフティパスワード設定	可	可	可	可	可
ファームウェアアップデート画面	ファームウェアアップデート	可	可	可*1	可*1	可

***1.** CIP Safety 通信のコネクション確立中は、実行できません。

6-8-4 動作モードの変更と電源投入時モード

使用する安全アプリケーションが、固定アプリケーション、ユーザ定義アプリケーション、またはアドオンアプリケーションの場合、ロジック機能の実行／停止を切り替えるためには、動作モードを変更する必要があります。

Sysmac Studio または Web UI を使用した動作モードの変更手順については、「7-16 動作モードの変更 (P.7-91)」を参照してください。
また、安全アプリケーションの設定で、電源投入時の動作モードを指定することができます。
電源投入時モードによる動作の違いは、以下のとおりです。

電源投入時モード	動作
Executing	• 電源投入時に「運転状態」になり、ロジック機能が自動的に実行される。 • 固定アプリケーションの電源投入時モードは、「Executing」に設定されているため、TUNID が設定された状態で電源を再投入すると、「運転状態」で起動する。 • ユーザ定義アプリケーションで Type 1 Safety Oen でコンフィグレーションされた直後も、「運転状態」に遷移する。
Idle	• 電源投入時に「運転待ち状態」となり、ロジック機能は停止した状態で起動する。

7

セーフティ I/O ターミナルの設定

この章ではセーフティ I/O ターミナルの各種設定について説明します。

7-1 設定の手順 7-3
7-1-1 セーフティコントローラが制御する構成（Type 1 Safety Open によるコンフィグレーション）の設定手順 7-3
7-1-2 セーフティコントローラが制御する構成（Web UI によるコンフィグレーション）の設定手順 7-6
7-1-3 プリセットされた安全アプリケーションでセーフティ I/O ターミナルが制御する構成の設定手順 7-9
7-1-4 ユーザが設計した安全アプリケーションでセーフティ I/O ターミナルが制御する構成（集中管理型）の設定手順 7-11
7-1-5 ユーザが設計した安全アプリケーションでセーフティ I/O ターミナルが制御する構成（分散管理型）の設定手順 7-13

7-2 Web UI の概要 7-16
7-2-1 Web UI の各種仕様 7-16
7-2-2 Web UI の操作権限 7-16
7-2-3 Web UI の画面構成 7-16
7-2-4 メインメニュー一覧 7-17
7-2-5 Web UI の起動手順 7-19
7-2-6 ログイン 7-21
7-2-7 ログアウト 7-23
7-2-8 初回ログイン時の注意事項 7-23

7-3 CIP Safety 通信の設定 7-25
7-3-1 CIP Safety 通信のコネクション設定 7-25
7-3-2 セーフティ I/O ターミナルの設定のエクスポートとインポート 7-34

7-4 EtherNet/IP 通信の設定 7-36
7-4-1 タグデータリンク通信の設定 7-36
7-4-2 LLDP 機能 7-40

7-5 セーフティ入力機能の設定 7-42
7-5-1 セーフティ入力機能の設定手順 7-42
7-5-2 スタンダード出力機能の設定手順 7-44

7-6 セーフティ出力機能の設定 7-47
7-6-1 セーフティ出力機能の設定手順 7-47

7-7 ロジック機能の設定 7-50
7-7-1 ロジック設定手順 7-50
7-7-2 パラメーター覧表示 7-55
7-7-3 考慮すべき入力デバイスの異常動作の例 7-56

7-8 セーフティ署名の設定 7-60

7-9　安全アプリケーションファイルの作成 7-62
7-9-1　セーフティ I/O ターミナルの登録 7-62
7-9-2　安全アプリケーションの設定 7-63
7-9-3　セーフティ入出力機能の設定 7-66
7-9-4　ロジック機能の設定 7-66
7-9-5　安全アプリケーションファイルのエクスポート 7-66

7-10　IP アドレスの設定 7-69
7-10-1　IP アドレスの構成 7-69
7-10-2　ロータリスイッチによる IP アドレスの設定方法の選択 7-71
7-10-3　Sysmac Studio による設定 7-72
7-10-4　Web UI による設定 7-74

7-11　TUNID の設定 7-76
7-11-1　TUNID の目的 7-76
7-11-2　TUNID の設定手順 7-76

7-12　安全アプリケーションの選択 7-81

7-13　再起動 7-82
7-13-1　再起動の目的 7-82
7-13-2　再起動の使用手順 7-82

7-14　コンフィグレーション 7-84
7-14-1　セーフティコントローラのコンフィグレーション 7-84
7-14-2　セーフティ I/O ターミナルのコンフィグレーション 7-84

7-15　時計情報自動調整機能の設定 7-87
7-15-1　時計情報自動調整機能の目的 7-87
7-15-2　時計情報自動調整機能の使用手順 7-87
7-15-3　時計情報自動調整機能の詳細 7-90

7-16　動作モードの変更 7-91
7-16-1　動作モード変更の使用手順 7-91

7-17　コンフィグレーションロック 7-95
7-17-1　コンフィグレーションロックの目的 7-95
7-17-2　コンフィグレーションロックの使用手順 7-95
7-17-3　コンフィグレーションロックの詳細 7-99

7-18　セーフティパスワードの設定 7-100
7-18-1　セーフティパスワードの目的 7-100
7-18-2　セーフティパスワード設定の使用手順 7-100
7-18-3　セーフティパスワードの詳細 7-102

7-19　バックアップ 7-104
7-19-1　バックアップの目的 7-104
7-19-2　バックアップの使用手順 7-104
7-19-3　バックアップの詳細 7-107

7-1 設定の手順

セーフティ I/O ターミナルの設定の手順は、セーフティコントロールシステムによって異なります。
セーフティコントロールシステムの構成の詳細は、「1-3-1 セーフティコントロールシステム (P.1-4)」を参照してください。

使用上の注意

Sysmac Studio でセーフティ I/O ターミナルの設定を変更した場合は、同期転送を実行して Sysmac Studio の設定内容をセーフティ I/O ターミナルに反映してください。Sysmac Studio の同期機能の詳細は、『Sysmac Studio Version 1 オペレーションマニュアル（SBCA-470)』を参照してください。

7-1-1 セーフティコントローラが制御する構成（Type 1 Safety Open によるコンフィグレーション）の設定手順

セーフティコントローラが制御する構成 (Type 1 Safety Open によるコンフィグレーション) の設定手順を示します。
取り付けと配線前の手順は、以下のとおりです。

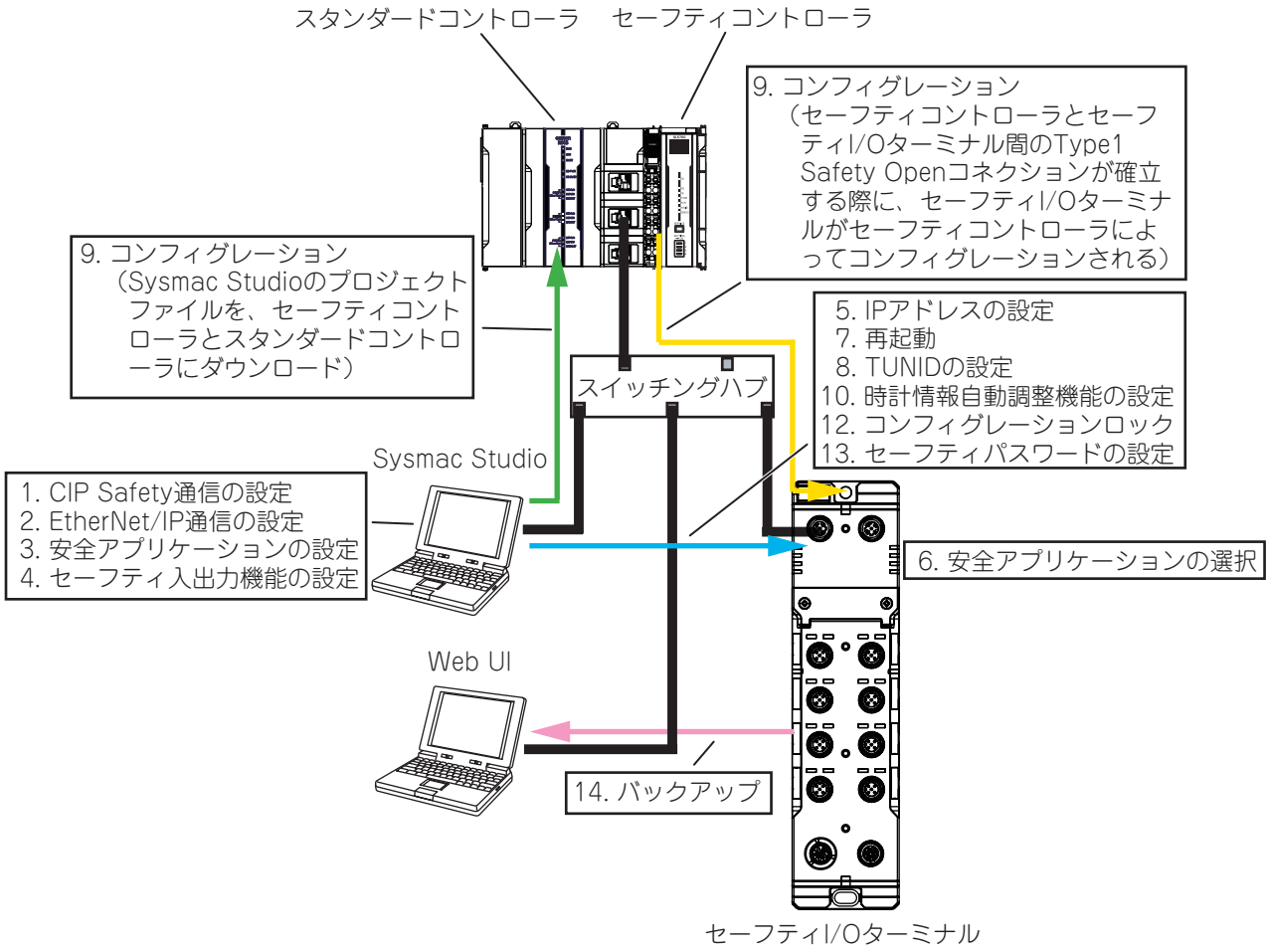
手順	設定項目	使用するサポートソフト	内容	参照先
1	CIP Safety 通信の設定	Sysmac Studio	Sysmac Studio のプロジェクトファイルで、セーフティコントローラとセーフティ I/O ターミナル間の CIP Safety 通信の設定を行う。 オープンタイプは、［ターゲットデバイスをコンフィグレーション(Type1)］を選択する。	「7-3 CIP Safety 通信の設定 (P.7-25)」
2	EtherNet/IP 通信の設定	Sysmac Studio	Sysmac Studio のプロジェクトファイルで、スタンダードコントローラとセーフティ I/O ターミナル間の EtherNet/IP 通信（タグデータリンク）の設定を行う。	「7-4 EtherNet/IP 通信の設定 (P.7-36)」
3	安全アプリケーションの設定	Sysmac Studio	Sysmac Studio のプロジェクトファイルで、安全アプリケーションの設定を行う。 00: リモート I/O モードを選択する。	「7-9-2 安全アプリケーションの設定 (P.7-63)」
4	セーフティ入出力機能の設定	Sysmac Studio	Sysmac Studio のプロジェクトファイルで、セーフティ I/O ターミナルの I/O 構成の設定を行う。	「7-5 セーフティ入力機能の設定 (P.7-42)」 「7-6 セーフティ出力機能の設定 (P.7-47)」

取り付けと配線後の手順は、以下のとおりです。

手順	設定項目	使用するサポートソフト	内容	参照先
5	IP アドレスの設定	Sysmac Studio*1	セーフティ I/O ターミナルの IP アドレスの設定を行う。	「7-10 IP アドレスの設定 (P.7-69)」
6	安全アプリケーションの選択	－	セーフティ I/O ターミナルのロータリスイッチの SETTING SW1、SW2 の、両方を「0」に設定する。	「7-12 安全アプリケーションの選択 (P.7-81)」
7	再起動	Sysmac Studio*1	セーフティ I/O ターミナルを再起動する。	「7-13 再起動 (P.7-82)」
8	TUNID の設定	Sysmac Studio*1	セーフティ I/O ターミナルの TUNID の設定を行う。	「7-11 TUNID の設定 (P.7-76)」

手順	設定項目	使用するサポートソフト	内容	参照先
9	コンフィグレーション	Sysmac Studio	Sysmac Studio のプロジェクトファイルをダウンロードして、セーフティコントローラ、スタンダードコントローラをコンフィグレーションする。 セーフティ I/O ターミナルは、セーフティコントローラとセーフティ I/O ターミナル間の Type1 Safety Open コネクションが確立する際に、セーフティコントローラによってコンフィグレーションされる。	「7-14 コンフィグレーション (P.7-84)」
10	時計情報自動調整機能の設定	Sysmac Studio*1	セーフティ I/O ターミナルの時計情報自動調整機能の設定を行う。	「7-15 時計情報自動調整機能の設定 (P.7-87)」
11	動作確認	−	I/O 配線チェック、およびプログラムの動作確認を行い、セーフティ I/O ターミナルが意図した動作をしていることを確認する。	−
12	コンフィグレーションロック	Sysmac Studio*1	セーフティコントロールシステムの妥当性確認を実施し、設定値が正しいことを確認する。 確認後に、コンフィグレーションロックを実行する。 コンフィグレーションロック実行後は、コンフィグレーションロックを解除するまでセーフティ I/O ターミナルの設定値を変更できない。	「7-17 コンフィグレーションロック (P.7-95)」
13	セーフティパスワードの設定	Sysmac Studio*1	セーフティ I/O ターミナルのセーフティパスワードの設定を行う。	「7-18 セーフティパスワードの設定 (P.7-100)」
14	バックアップ	Web UI	セーフティ I/O ターミナルのバックアップファイルを作成する。	「7-19 バックアップ (P.7-104)」

***1.** Web UI を使用して設定することも可能です。


スタンダードコントローラ
セーフティコントローラ
9. コンフィグレーション
（セーフティコントローラとセーフティI/Oターミナル間のType1 Safety Openコネクションが確立する際に、セーフティI/Oターミナルがセーフティコントローラによってコンフィグレーションされる）
9. コンフィグレーション
（Sysmac Studioのプロジェクトファイルを、セーフティコントローラとスタンダードコントローラにダウンロード）
5. IPアドレスの設定
7. 再起動
8. TUNIDの設定
10. 時計情報自動調整機能の設定
12. コンフィグレーションロック
13. セーフティパスワードの設定
スイッチングハブ
Sysmac Studio
1. CIP Safety通信の設定
2. EtherNet/IP通信の設定
3. 安全アプリケーションの設定
4. セーフティ入出力機能の設定
6. 安全アプリケーションの選択
Web UI
14. バックアップ
セーフティI/Oターミナル

7-1-2 セーフティコントローラが制御する構成（Web UI によるコンフィグレーション）の設定手順

セーフティコントローラが制御する構成（Web UI によるコンフィグレーション）の設定手順を示します。
取り付けと配線前の手順は、以下のとおりです。

手順	設定項目		使用するサポートソフト	内容	参照先
1	リモート I/O モード用の安全アプリケーション作成*1	安全アプリケーションファイルの作成	Sysmac Studio	安全アプリケーションファイルのエクスポート用のプロジェクトファイルを作成する。 このプロジェクトファイルで、安全アプリケーションファイルのエクスポートを実行する。 この安全アプリケーションファイルは、I/O 構成設定だけを定義する。	「7-9 安全アプリケーションファイルの作成 (P.7-62)」
2	セーフティコントローラのセーフティプログラム用の、プロジェクトファイル作成*1	CIP Safety 通信の設定	Sysmac Studio	Sysmac Studio のプロジェクトファイルで、セーフティコントローラとセーフティ I/O ターミナル間の CIP Safety 通信の設定を行う。 オープンタイプは、[セーフティ署名をチェック (Type2a)] を選択する。	「7-3 CIP Safety 通信の設定 (P.7-25)」
3		EtherNet/IP 通信の設定	Sysmac Studio	Sysmac Studio のプロジェクトファイルで、スタンダードコントローラとセーフティ I/O ターミナル間の EtherNet/IP 通信（タグデータリンク）の設定を行う。	「7-4 EtherNet/IP 通信の設定 (P.7-36)」
4		安全アプリケーションの設定	Sysmac Studio	Sysmac Studio のプロジェクトファイルで、安全アプリケーションの設定を行う。 00: リモート I/O モードを選択する。	「7-9-2 安全アプリケーションの設定 (P.7-63)」
5		セーフティ署名の設定	Sysmac Studio	Sysmac Studio のプロジェクトファイルで、セーフティ署名の設定を行う。 「7-9-5 安全アプリケーションファイルのエクスポート (P.7-66)」で記録した SCCRC と SCTS を入力する。	「7-8 セーフティ署名の設定 (P.7-60)」

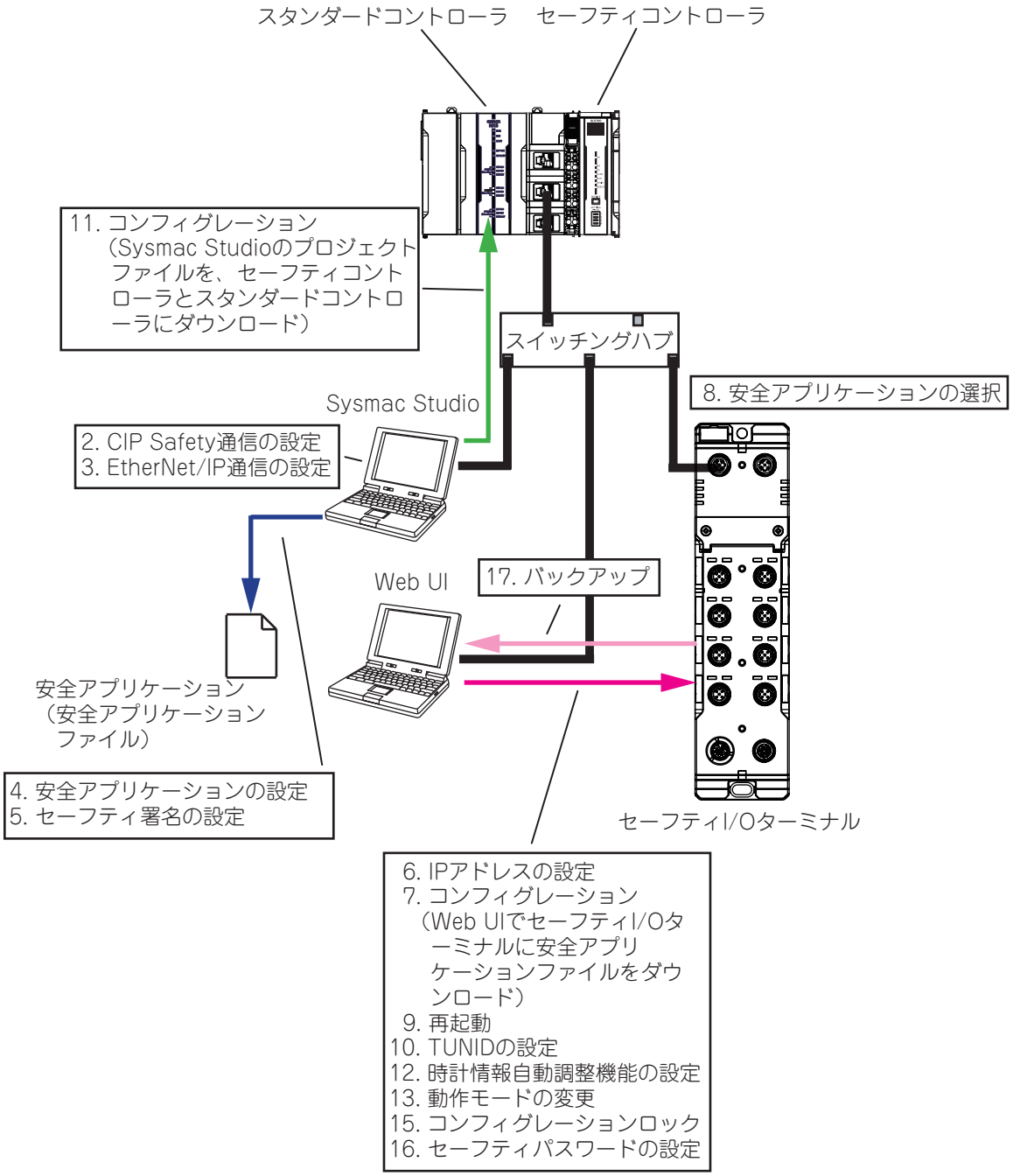
***1.** 安全アプリケーションファイルのエクスポート用のプロジェクトファイルと、セーフティコントローラのセーフティプログラム用のプロジェクトファイルは、別に作成してください。

取り付けと配線後の手順は、以下のとおりです。
セーフティコントローラの設定には、セーフティプログラム用のプロジェクトファイルを使用してください。

手順	設定項目	使用するサポートソフト	内容	参照先
6	IP アドレスの設定	Web UI*1	セーフティ I/O ターミナルの IP アドレスの設定を行う。	「7-10 IP アドレスの設定 (P.7-69)」
7	コンフィグレーション（セーフティ I/O ターミナル側）	Web UI	Web UI を使用してセーフティ I/O ターミナルに安全アプリケーションファイルをダウンロードすることよって、セーフティ I/O ターミナルをコンフィグレーションする。 リモート I/O モード用の安全アプリケーションファイルを使用する。アドオンアプリケーション用の安全アプリケーションファイルは使用できない。	「7-14-2 セーフティ I/O ターミナルのコンフィグレーション (P.7-84)」
8	安全アプリケーションの選択	−	セーフティ I/O ターミナルのロータリスイッチの SETTING SW1、SW2 の、両方を「0」に設定する。	「7-12 安全アプリケーションの選択 (P.7-81)」
9	再起動	Web UI*1	セーフティ I/O ターミナルを再起動する。	「7-13 再起動 (P.7-82)」
10	TUNID の設定	Web UI*1	セーフティ I/O ターミナルの TUNID の設定を行う。	「7-11 TUNID の設定 (P.7-76)」

手順	設定項目	使用するサポートソフト	内容	参照先
11	コンフィグレーション（セーフティコントローラ、スタンダードコントローラ側）	Sysmac Studio	Sysmac Studio のプロジェクトファイルをダウンロードして、セーフティコントローラ、スタンダードコントローラをコンフィグレーションする。	「7-14-1 セーフティコントローラのコンフィグレーション (P.7-84)」
12	時計情報自動調整機能の設定	Web UI*1	セーフティ I/O ターミナルの時計情報自動調整機能の設定を行う。	「7-15 時計情報自動調整機能の設定 (P.7-87)」
13	動作モードの変更*2	Web UI*1	セーフティ I/O ターミナルの動作モードを、「Executing」に変更する。	「7-16 動作モードの変更 (P.7-91)」
14	動作確認	－	I/O 配線チェック、およびプログラムの動作確認を行い、セーフティ I/O ターミナルが意図した動作をしていることを確認する。	－
15	コンフィグレーションロック	Web UI*1	セーフティコントロールシステムの妥当性確認を実施し、設定値が正しいことを確認する。 確認後に、コンフィグレーションロックを実行する。 コンフィグレーションロック実行後は、コンフィグレーションロックを解除するまでセーフティ I/O ターミナルの設定値を変更できない。	「7-17 コンフィグレーションロック (P.7-95)」
16	セーフティパスワードの設定	Web UI*1	セーフティ I/O ターミナルのセーフティパスワードの設定を行う。	「7-18 セーフティパスワードの設定 (P.7-100)」
17	バックアップ	Web UI	セーフティ I/O ターミナルのバックアップファイルを作成する。	「7-19 バックアップ (P.7-104)」

***1.** Sysmac Studio を使用して設定することも可能です。
***2.** 手順 4 のロジック機能の設定で、電源投入時モードを「Idle」に設定した場合だけ、この設定が必要です。電源投入時モードを「Executing」に設定した場合、この設定は不要です。


スタンダードコントローラ
セーフティコントローラ
11. コンフィグレーション
（Sysmac Studioのプロジェクト
ファイルを、セーフティコント
ローラとスタンダードコントロ
ーラにダウンロード）
スイッチングハブ
8. 安全アプリケーションの選択
Sysmac Studio
2. CIP Safety通信の設定
3. EtherNet/IP通信の設定
Web UI
17. バックアップ
安全アプリケーション
（安全アプリケーション
ファイル）
4. 安全アプリケーションの設定
5. セーフティ署名の設定
セーフティI/Oターミナル
6. IPアドレスの設定
7. コンフィグレーション
（Web UIでセーフティI/Oタ
ーミナルに安全アプリ
ケーションファイルをダウ
ンロード）
9. 再起動
10. TUNIDの設定
12. 時計情報自動調整機能の設定
13. 動作モードの変更
15. コンフィグレーションロック
16. セーフティパスワードの設定

7-1-3 プリセットされた安全アプリケーションでセーフティ I/O ターミナルが制御する構成の設定手順

プリセットされた安全アプリケーションでセーフティ I/O ターミナルが制御する構成の設定手順を示します。
取り付けと配線前の手順は、以下のとおりです。

手順	設定項目	使用するサポートソフト	内容	参照先
1	CIP Safety 通信の設定*1	Sysmac Studio	Sysmac Studio のプロジェクトファイルで、セーフティコントローラとセーフティ I/O ターミナル間の CIP Safety 通信の設定を行う。 オープンタイプは、［セーフティ署名をチェック (Type2a)］を選択する。	「7-3 CIP Safety 通信の設定 (P.7-25)」
2	EtherNet/IP 通信の設定*2	Sysmac Studio	Sysmac Studio のプロジェクトファイルで、スタンダードコントローラとセーフティ I/O ターミナル間の EtherNet/IP 通信（タグデータリンク）の設定を行う。	「7-4 EtherNet/IP 通信の設定 (P.7-36)」
3	安全アプリケーションの設定*1	Sysmac Studio	Sysmac Studio のプロジェクトファイルで、安全アプリケーションの設定を行う。 使用する固定アプリケーションを選択する。	「7-9-2 安全アプリケーションの設定 (P.7-63)」

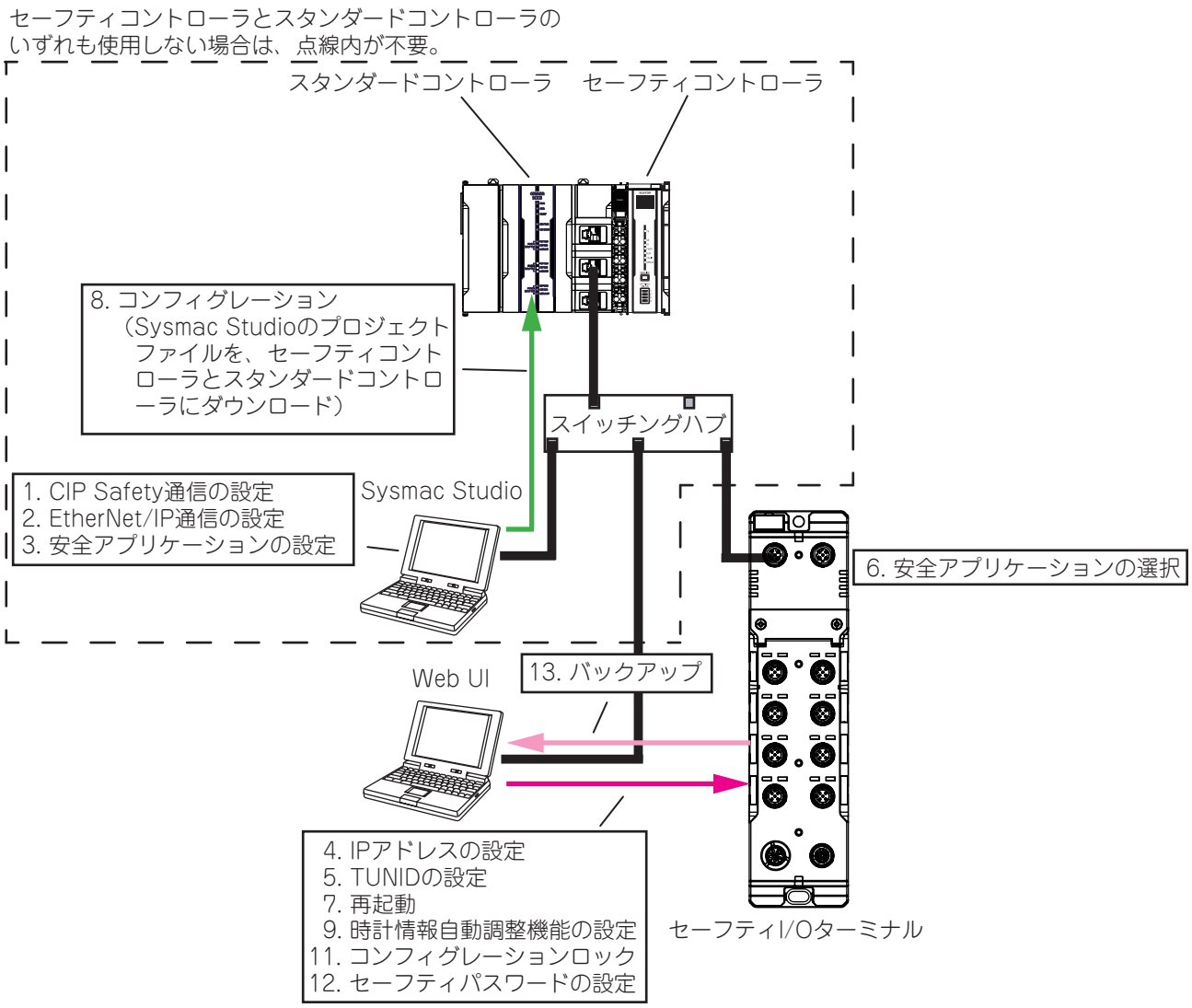
***1.** セーフティコントローラを使用しない場合、この設定は不要です。
***2.** スタンダードコントローラを使用しない場合、この設定は不要です。

取り付けと配線後の手順は、以下のとおりです。

手順	設定項目	使用するサポートソフト	内容	参照先
4	IP アドレスの設定*1	Web UI*2	セーフティ I/O ターミナルの IP アドレスの設定を行う。	「7-10 IP アドレスの設定 (P.7-69)」
5	TUNID の設定	Web UI*2	セーフティ I/O ターミナルの TUNID の設定を行う。	「7-11 TUNID の設定 (P.7-76)」
6	安全アプリケーションの選択	－	セーフティ I/O ターミナルのロータリスイッチの SETTING SW1、SW2 を、両方とも使用する安全アプリケーション（固定アプリケーション）の番号「1-3」のいずれかに設定する。	「7-12 安全アプリケーションの選択 (P.7-81)」
7	再起動	Web UI*2	セーフティ I/O ターミナルを再起動する。	「7-13 再起動 (P.7-82)」
8	コンフィグレーション*3	Sysmac Studio	Sysmac Studio のプロジェクトファイルをダウンロードして、セーフティコントローラ、スタンダードコントローラをコンフィグレーションする。 セーフティ I/O ターミナルのコンフィグレーションは不要。	「7-14-1 セーフティコントローラのコンフィグレーション (P.7-84)」
9	時計情報自動調整機能の設定	Web UI*2	セーフティ I/O ターミナルの時計情報自動調整機能の設定を行う。	「7-15 時計情報自動調整機能の設定 (P.7-87)」
10	動作確認	－	I/O 配線チェック、およびプログラムの動作確認を行い、セーフティ I/O ターミナルが意図した動作をしていることを確認する。	－
11	コンフィグレーションロック	Web UI*2	セーフティコントロールシステムの妥当性確認を実施し、設定値が正しいことを確認する。 確認後に、コンフィグレーションロックを実行する。 コンフィグレーションロック実行後は、コンフィグレーションロックを解除するまでセーフティ I/O ターミナルの設定値を変更できない。	「7-17 コンフィグレーションロック (P.7-95)」
12	セーフティパスワードの設定	Web UI*2	セーフティ I/O ターミナルのセーフティパスワードの設定を行う。	「7-18 セーフティパスワードの設定 (P.7-100)」

手順	設定項目	使用するサポートソフト	内容	参照先
13	バックアップ	Web UI	セーフティ I/O ターミナルのバックアップファイルを作成する。	「7-19 バックアップ (P.7-104)」

***1.** セーフティコントローラとスタンダードコントローラのいずれも使用しない場合、この設定は不要です。その場合、セーフティ I/O ターミナルは、工場出荷時の IP アドレスで動作します。
***2.** Sysmac Studio を使用して設定することも可能です。
***3.** セーフティコントローラとスタンダードコントローラのいずれも使用しない場合、この設定は不要です。



7-1-4 ユーザが設計した安全アプリケーションでセーフティ I/O ターミナルが制御する構成（集中管理型）の設定手順

ユーザが設計した安全アプリケーションでセーフティ I/O ターミナルが制御する構成（集中管理型）の設定手順を示します。
取り付けと配線前の手順は、以下のとおりです。

手順	設定項目	使用するサポートソフト	内容	参照先
1	CIP Safety 通信の設定	Sysmac Studio	Sysmac Studio のプロジェクトファイルで、セーフティコントローラとセーフティ I/O ターミナル間の CIP Safety 通信の設定を行う。 オープンタイプは、［ターゲットデバイスをコンフィグレーション(Type1)］を選択する。	「7-3 CIP Safety 通信の設定 (P.7-25)」
2	EtherNet/IP 通信の設定*1	Sysmac Studio	Sysmac Studio のプロジェクトファイルで、スタンダードコントローラとセーフティ I/O ターミナル間の EtherNet/IP 通信（タグデータリンク）の設定を行う。	「7-4 EtherNet/IP 通信の設定 (P.7-36)」
3	安全アプリケーションの設定	Sysmac Studio	Sysmac Studio のプロジェクトファイルで、安全アプリケーションの設定を行う。 15: ユーザ定義を選択する。	「7-9-2 安全アプリケーションの設定 (P.7-63)」
4	セーフティ入出力機能の設定	Sysmac Studio	Sysmac Studio のプロジェクトファイルで、セーフティ I/O ターミナルの I/O 構成の設定を行う。	「7-5 セーフティ入力機能の設定 (P.7-42)」 「7-6 セーフティ出力機能の設定 (P.7-47)」
5	ロジック機能の設定	Sysmac Studio	Sysmac Studio のプロジェクトファイルで、セーフティ I/O ターミナルのロジックと電源投入時モードの設定を行う。	「7-7 ロジック機能の設定 (P.7-50)」

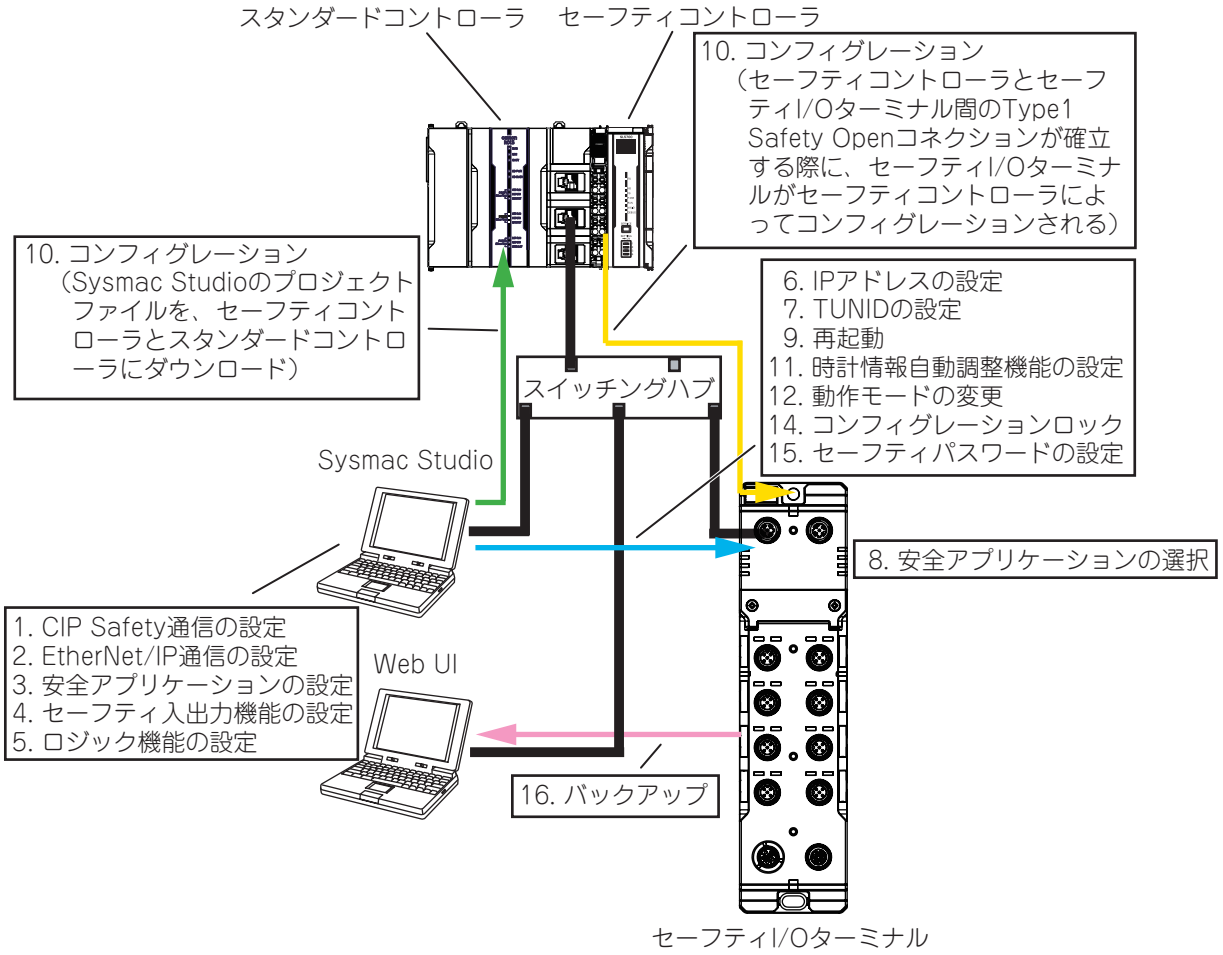
***1.** スタンダードコントローラを使用しない場合、この設定は不要です。

取り付けと配線後の手順は、以下のとおりです。

手順	設定項目	使用するサポートソフト	内容	参照先
6	IP アドレスの設定	Sysmac Studio*1	セーフティ I/O ターミナルの IP アドレスの設定を行う。	「7-10 IP アドレスの設定 (P.7-69)」
7	TUNID の設定	Sysmac Studio*1	セーフティ I/O ターミナルの TUNID の設定を行う。	「7-11 TUNID の設定 (P.7-76)」
8	安全アプリケーションの選択	－	セーフティ I/O ターミナルのロータリスイッチの SETTING SW1、SW2 を、両方とも「F」に設定する。	「7-12 安全アプリケーションの選択 (P.7-81)」
9	再起動	Sysmac Studio*1	セーフティ I/O ターミナルを再起動する。	「7-13 再起動 (P.7-82)」
10	コンフィグレーション	Sysmac Studio	Sysmac Studio のプロジェクトファイルをダウンロードして、セーフティコントローラ、スタンダードコントローラをコンフィグレーションする。 セーフティ I/O ターミナルは、セーフティコントローラとセーフティ I/O ターミナル間の Type1 Safety Open コネクションが確立する際に、セーフティコントローラによってコンフィグレーションされる。	「7-14-1 セーフティコントローラのコンフィグレーション (P.7-84)」
11	時計情報自動調整機能の設定	Sysmac Studio*1	セーフティ I/O ターミナルの時計情報自動調整機能の設定を行う。	「7-15 時計情報自動調整機能の設定 (P.7-87)」
12	動作モードの変更 *2	Sysmac Studio*1	セーフティ I/O ターミナルの動作モードを、「Executing」に変更する。	「7-16 動作モードの変更 (P.7-91)」

手順	設定項目	使用するサポートソフト	内容	参照先
13	動作確認	−	I/O 配線チェック、およびプログラムの動作確認を行い、セーフティ I/O ターミナルが意図した動作をしていることを確認する。	−
14	コンフィグレーションロック	Sysmac Studio*1	セーフティコントロールシステムの妥当性確認を実施し、設定値が正しいことを確認する。 確認後に、コンフィグレーションロックを実行する。 コンフィグレーションロック実行後は、コンフィグレーションロックを解除するまでセーフティ I/O ターミナルの設定値を変更できない。	「7-17 コンフィグレーションロック (P.7-95)」
15	セーフティパスワードの設定	Sysmac Studio*1	セーフティ I/O ターミナルのセーフティパスワードの設定を行う。	「7-18 セーフティパスワードの設定 (P.7-100)」
16	バックアップ	Web UI	セーフティ I/O ターミナルのバックアップファイルを作成する。	「7-19 バックアップ (P.7-104)」

***1.** Web UI を使用して設定することも可能です。
***2.** 手順 4 のロジック機能の設定で、電源投入時モードを「Idle」に設定した場合だけ、この設定が必要です。電源投入時モードを「Executing」に設定した場合、この設定は不要です。



7-1-5 ユーザが設計した安全アプリケーションでセーフティ I/O ターミナルが制御する構成（分散管理型）の設定手順

ユーザが設計した安全アプリケーションでセーフティ I/O ターミナルが制御する構成（分散管理型）の設定手順を示します。
取り付けと配線前の手順は、以下のとおりです。

手順	設定項目		使用するサポートソフト	内容	参照先
1	アドオンアプリケーション用の安全アプリケーションファイル作成*1	安全アプリケーションファイルのエクスポート	Sysmac Studio	安全アプリケーションファイルのエクスポート用のプロジェクトファイルを作成する。 このプロジェクトファイルで、安全アプリケーションのエクスポートを実行する。 この安全アプリケーションファイルは、ロジック設定と I/O 構成設定を定義する。	「7-9 安全アプリケーションファイルの作成 (P.7-62)」
2	セーフティコントローラのセーフティプログラム用の、プロジェクトファイル作成*1	CIP Safety 通信の設定*2	Sysmac Studio	Sysmac Studio のプロジェクトファイルで、セーフティコントローラとセーフティ I/O ターミナル間の CIP Safety 通信の設定を行う。 オープンタイプは、[セーフティ署名をチェック (Type2a)] を選択する。	「7-3 CIP Safety 通信の設定 (P.7-25)」
3		EtherNet/IP 通信の設定*3	Sysmac Studio	Sysmac Studio のプロジェクトファイルで、スタンダードコントローラとセーフティ I/O ターミナル間の EtherNet/IP 通信（タグデータリンク）の設定を行う。	「7-4 EtherNet/IP 通信の設定 (P.7-36)」
4		安全アプリケーションの設定*2	Sysmac Studio	Sysmac Studio のプロジェクトファイルで、安全アプリケーションの設定を行う。 使用するアドオンアプリケーションを選択する。	「7-9-2 安全アプリケーションの設定 (P.7-63)」
5		セーフティ署名の設定*2	Sysmac Studio	Sysmac Studio のプロジェクトファイルで、セーフティ署名の設定を行う。 「安全アプリケーションファイルのエクスポート」で記録した SCCRC と SCTS を入力する。	「7-8 セーフティ署名の設定 (P.7-60)」

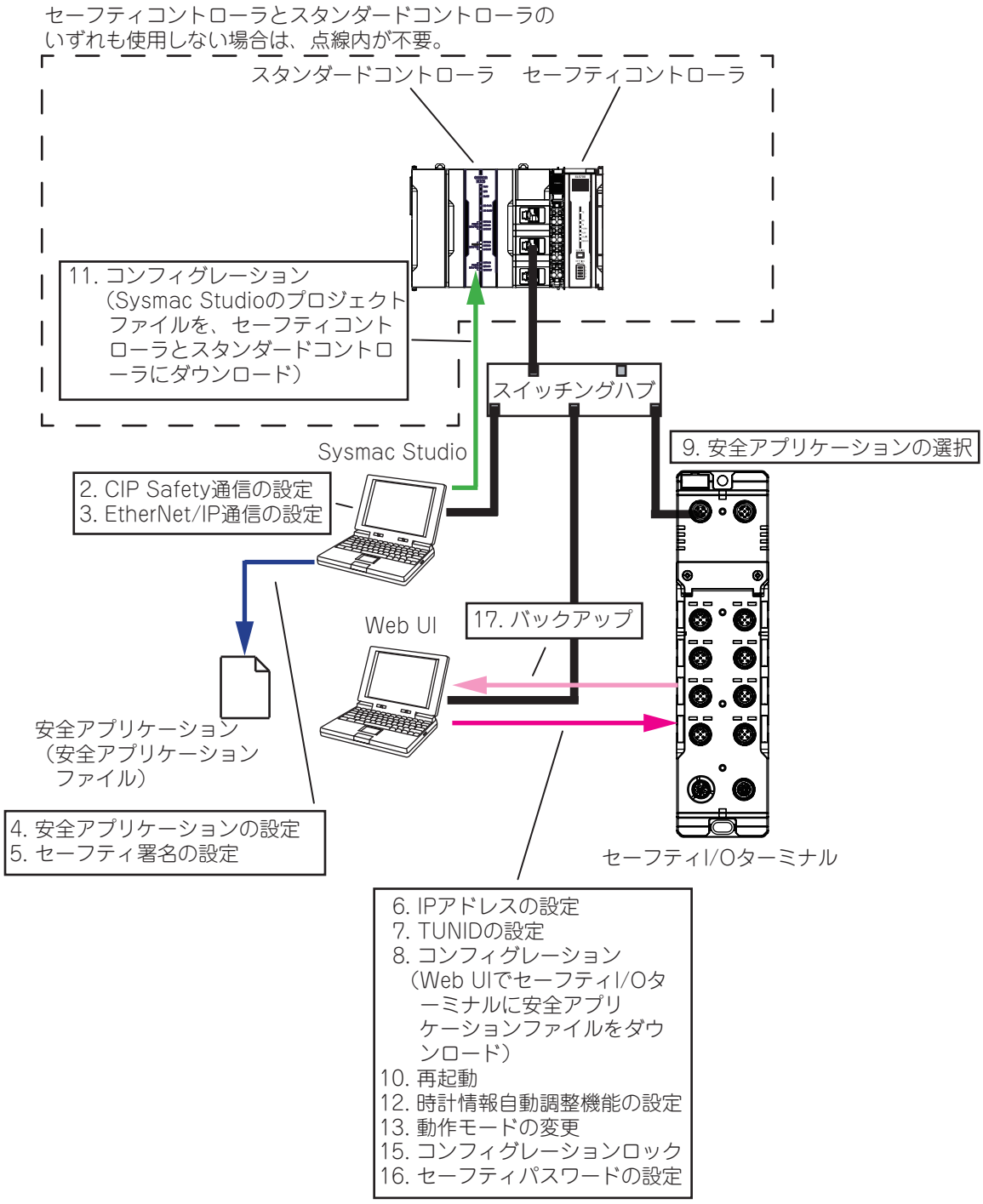
***1.** 安全アプリケーションファイルのエクスポート用のプロジェクトファイルと、セーフティコントローラのセーフティプログラム用のプロジェクトファイルは、別に作成してください。
***2.** セーフティコントローラを使用しない場合、この設定は不要です。
***3.** スタンダードコントローラを使用しない場合、この設定は不要です。

取り付けと配線後の手順は、以下のとおりです。
セーフティコントローラの設定には、セーフティプログラム用のプロジェクトファイルを使用してください。

手順	設定項目	使用するサポートソフト	内容	参照先
6	IP アドレスの設定*1	Web UI*2	セーフティ I/O ターミナルの IP アドレスの設定を行う。	「7-10 IP アドレスの設定 (P.7-69)」
7	TUNID の設定	Web UI*2	セーフティ I/O ターミナルの TUNID の設定を行う。	「7-11 TUNID の設定 (P.7-76)」
8	コンフィグレーション（セーフティ I/O ターミナル側）	Web UI	Web UI を使用してセーフティ I/O ターミナルに安全アプリケーションファイルをダウンロードすることよって、セーフティ I/O ターミナルをコンフィグレーションする。 アドオンアプリケーション用の安全アプリケーションファイルを使用する。リモート I/O モード用の安全アプリケーションファイルは使用できない。	「7-14-2 セーフティ I/O ターミナルのコンフィグレーション (P.7-84)」

手順	設定項目	使用するサポートソフト	内容	参照先
9	安全アプリケーションの選択	－	セーフティ I/O ターミナルのロータリスイッチの SETTING SW1、SW2 を、両方とも使用する安全アプリケーション（アドオンアプリケーション）の番号「9-D」に設定する。	「7-12 安全アプリケーションの選択 (P.7-81)」
10	再起動	Web UI*2	セーフティ I/O ターミナルを再起動する。	「7-13 再起動 (P.7-82)」
11	コンフィグレーション（セーフティコントローラ、スタンダードコントローラ側）*3	Sysmac Studio	Sysmac Studio のプロジェクトファイルをダウンロードして、セーフティコントローラ、スタンダードコントローラをコンフィグレーションする。	「7-14-1 セーフティコントローラのコンフィグレーション (P.7-84)」
12	時計情報自動調整機能の設定	Web UI*2	の時計情報自動調整機能の設定を行う。	「7-15 時計情報自動調整機能の設定 (P.7-87)」
13	動作モードの変更*4	Web UI*2	の動作モードを、「Executing」に変更する。	「7-16 動作モードの変更 (P.7-91)」
14	動作確認	－	I/O 配線チェック、およびプログラムの動作確認を行い、セーフティ I/O ターミナルが意図した動作をしていることを確認する。	－
15	コンフィグレーションロック	Web UI*2	セーフティコントロールシステムの妥当性確認を実施し、設定値が正しいことを確認する。 確認後に、コンフィグレーションロックを実行する。 コンフィグレーションロック実行後は、コンフィグレーションロックを解除するまでセーフティ I/O ターミナルの設定値を変更できない。	「7-17 コンフィグレーションロック (P.7-95)」
16	セーフティパスワードの設定	Web UI*2	セーフティ I/O ターミナルのセーフティパスワードの設定を行う。	「7-18 セーフティパスワードの設定 (P.7-100)」
17	バックアップ	Web UI	セーフティ I/O ターミナルのバックアップファイルを作成する。	「7-19 バックアップ (P.7-104)」

***1.** セーフティコントローラとスタンダードコントローラのいずれも使用しない場合、この設定は不要です。その場合、セーフティ I/O ターミナルは、工場出荷時の IP アドレスで動作します。
***2.** Sysmac Studio を使用して設定することも可能です。
***3.** セーフティコントローラとスタンダードコントローラのいずれも使用しない場合、この設定は不要です。
***4.** 手順 4 のロジック機能の設定で、電源投入時モードを「Idle」に設定した場合だけ、この設定が必要です。電源投入時モードを「Executing」に設定した場合、この設定は不要です。


セーフティコントローラとスタンダードコントローラの
いずれも使用しない場合は、点線内が不要。
スタンダードコントローラ
セーフティコントローラ
11. コンフィグレーション
（Sysmac Studioのプロジェクト
ファイルを、セーフティコント
ローラとスタンダードコントロ
ーラにダウンロード）
スイッチングハブ
Sysmac Studio
9. 安全アプリケーションの選択
2. CIP Safety通信の設定
3. EtherNet/IP通信の設定
Web UI
17. バックアップ
安全アプリケーション
（安全アプリケーション
ファイル）
4. 安全アプリケーションの設定
5. セーフティ署名の設定
セーフティI/Oターミナル
6. IPアドレスの設定
7. TUNIDの設定
8. コンフィグレーション
（Web UIでセーフティI/Oタ
ーミナルに安全アプリ
ケーションファイルをダウ
ンロード）
10. 再起動
12. 時計情報自動調整機能の設定
13. 動作モードの変更
15. コンフィグレーションロック
16. セーフティパスワードの設定

7-2 Web UI の概要

設定に使用する Web UI の、全体的な内容および各画面に共通の内容を説明します。

7-2-1 Web UI の各種仕様

Web UI の各種仕様を、以下に示します。

項目	仕様
同時にログインできるユーザ数	観察者、管理者を合わせて 1
自局ポート番号	443
対応言語	日本語(ja)、英語(en-US)
対応文字コード	UTF-8
権限	管理者、観察者
対応プロトコル	HTTPS
対応ブラウザ	パソコン版 Edge、パソコン版 Chrome
セッションタイムアウト時間	アクセスがない状態で 10 分
TLS バージョン	TLS 1.2 に対応 TLS 1.0、TLS 1.1、SSL には非対応

7-2-2 Web UI の操作権限

Web UI には、「管理者」と「観察者」の 2 種類の操作権限があります。
「管理者」と「観察者」の、それぞれができることおよびセーフティパスワード認証の要否を以下に示します。
セーフティパスワードとは、セーフティ I/O ターミナルのセーフティ関連の設定を行うのに必要なパスワードです。セーフティパスワードの設定も、Web UI を使用して実行できます。

操作権限	できること	セーフティパスワード認証
管理者	各種情報の読み出し、設定、変更、および各種コマンドの実行	必要
観察者	各種情報の読み出し	不要

Web UI の各種画面と「観察者」、および「管理者」の使用可否の関係は、「7-2-4 メインメニュー一覧 (P.7-17)」を参照してください。
操作権限を変更する場合は、Web UI をいったんログアウトして新しい操作権限で再ログインしてください。

7-2-3 Web UI の画面構成

Web UI の画面構成を以下に示します。



記号	名称	内容
(A)	共通メニュー	操作メニューの選択に関係なく、すべてのメインメニューに共通して設定するメニュー ［現在の操作権限］欄には、ログインしている操作者の権限が表示される。 ［ログアウト］ボタンを押すと、ログアウト画面が表示され、ログアウトできる。
(B)	操作メニュー	メインメニューを選択するメニュー
(C)	メインメニュー	選択した操作メニューの具体的内容を設定するメニュー

メインメニュー上部に、［自動更新］のチェックボックスと［手動更新］のボタンがある画面があります。これは、画面を更新するタイミングを設定するものです。それぞれの意味は、以下のとおりです。

項目	内容
自動更新	チェックが入っていると、画面が 1 秒間隔で自動更新される。 デフォルト：チェックあり
手動更新	クリックしたときに、画面が更新される。 ［自動更新］にチェックが入っていない場合だけ有効。

7-2-4 メインメニュー一覧

メインメニューには、以下のように機能一覧とユニット交換があります。
機能一覧とユニット交換の切り替えは、操作メニューの一番上のプルダウンメニューで行います。

メニュー	内容
機能一覧	セーフティ I/O ターミナルの各種設定およびモニタリングで使用する。
ユニット交換	ユニット交換時に使用する。 機能一覧のうち、ユニット交換時に必要な機能だけを集めたもの。

機能一覧



機能一覧には、以下のものがあります。それぞれの概要、観察者の使用可否、および参照先を示します。

メインメニューのグループ	メインメニューの画面名称	概要	観察者の使用可否	参照先
モニタ	動作状態モニタ	当該ユニットのユニットステータスや電源ステータスなどを表示する。	可	「11-1-3 動作状態モニタ機能 (P.11-3)」
	I/O モニタ	当該ユニットの各 I/O 端子の値を表示する。	可	「8-11 I/O モニタ機能 (P.8-27)」
	発生中異常・イベントログ	当該ユニットの発生中異常およびイベントログを表示する。また、イベントログの保存やクリアもできる。	可	「11-2 イベントによる異常の確認と対処方法 (P.11-6)」
	生産情報	ユニットバージョンなど当該ユニットの生産情報を表示する。	可	「生産情報画面 (P.32)」
ユニット設定	TCP/IP 設定	当該ユニットの IP アドレス、サブネットマスク、デフォルトデートウェイ、および LINK 設定を行う。	不可	「7-10 IP アドレスの設定 (P.7-69)」
	TUNID 設定	当該ユニットの TUNID を設定する。	不可	「7-11 TUNID の設定 (P.7-76)」
	安全アプリケーション設定	当該ユニットで動作する安全アプリケーションを、ロータリスイッチの番号に割り付けたり削除したりする。	不可	「7-14 コンフィグレーション (P.7-84)」
	時計情報自動調整機能設定	当該ユニットの時刻を合わせる。	不可	「7-15 時計情報自動調整機能の設定 (P.7-87)」
コマンド実行	動作モード変更	動作モードを「Idle」、または「Executing」に設定する。	不可	「7-16 動作モードの変更 (P.7-91)」
	コンフィグレーションロック	コンフィグレーションロックおよびロック解除を実行する。	不可	「7-17 コンフィグレーションロック (P.7-95)」
	再起動	当該ユニットを再起動する。	不可	「7-13 再起動 (P.7-82)」
	メモリオールクリア	当該ユニットの設定データをすべて工場出荷時に戻す。	不可	「8-2 メモリオールクリア機能 (P.8-4)」
	バックアップ／リストア／照合	当該ユニットの設定データをバックアップ、リストア、照合する。	不可	「7-19 バックアップ (P.7-104)」

メインメニューのグループ	メインメニューの画面名称	概要	観察者の使用可否	参照先
	汎用 CIP コマンド送信	専用ツールなしで当該ユニットに CIP メッセージコマンドを発行し、実行結果を表示する。	不可	「8-7 汎用 CIP コマンド送信機能 (P.8-15)」
	ユニット特定	当該ユニットのユニット特定表示 LED を点灯させる。	不可	「8-8 ユニット特定機能 (P.8-16)」
	通信ケーブル診断	通信ケーブルの断線や短絡の有無を確認する。	不可	「8-13 通信ケーブル診断機能 (P.8-31)」
メンテナンス	セーフティパスワード設定	当該ユニットの Web UI のセーフティパスワードを設定する。	不可	「7-18 セーフティパスワードの設定 (P.7-100)」
	ファームウェアアップデート	当該ユニットのファームウェアを更新する。	不可	「8-14 ファームウェアアップデート機能 (P.8-34)」

ユニット交換



ユニット交換には、以下のものがあります。それぞれの概要、観察者の使用可否、および参照先は、機能一覧と同じです。

メインメニューのグループ	メインメニューの画面名称	参照先
モニタ	生産情報	「生産情報画面 (P.32)」
	動作状態モニタ	「11-1-3 動作状態モニタ機能 (P.11-3)」
バックアップファイルがある場合	リストア*1	「7-19 バックアップ (P.7-104)」
バックアップファイルがない場合	メモリオールクリア	「8-2 メモリオールクリア機能 (P.8-4)」
	TCP/IP 設定	「7-10 IP アドレスの設定 (P.7-69)」
	TUNID 設定	「7-11 TUNID の設定 (P.7-76)」
	コンフィグレーションロック	「7-17 コンフィグレーションロック (P.7-95)」

***1.** 機能一覧のバックアップ／リストア／照合画面から、リストア機能だけを抽出したものです。

7-2-5 Web UI の起動手順

Web UI を起動する方法には、以下の 2 種類があります。

- パソコンの Web ブラウザに、セーフティ I/O ターミナルの IP アドレスを入力する方法

- パソコンの Web ブラウザに、セーフティ I/O ターミナルの IP アドレスを割り当てたドメイン名を入力する方法

IP アドレスを入力する方法

パソコンの Web ブラウザに、セーフティ I/O ターミナルの IP アドレスを入力する方法の手順を説明します。

1 **セーフティ I/O ターミナルの EtherNet/IP ポートとパソコンの Ethernet ポートを、Ethernet ケーブルで接続します。**

2 **パソコンで Web ブラウザを起動します。**

3 **Web ブラウザに、セーフティ I/O ターミナルの IP アドレスを入力します。たとえば、セーフティ I/O ターミナルの IP アドレスが 192.168.250.1 の場合、「https://192.168.250.1/」と入力します。**
Web UI が起動し Web ブラウザに以下のログイン画面が表示されます。



使用上の注意

パソコンの Web ブラウザに、セーフティ I/O ターミナルの IP アドレスを入力する方法を使用する場合、次のようなセキュリティリスクがあります。ネットワーク上でパソコンとセーフティ I/O ターミナルの間に不正デバイスが介入した場合、不正デバイスによってセーフティパスワードなどの情報が漏えいする可能性があります。したがって、以下のようなセキュリティ対策が必要です。

- ファイアウォールなどを使用して、生産エリア外からセーフティ I/O ターミナルにアクセスできないようにする。
- 入退室管理などの方法で、生産エリア内に不正な第三者が侵入できないようにする。
- パソコンとセーフティ I/O ターミナルを直接接続するなどの方法で、パソコンとセーフティ I/O ターミナルの間に、不正デバイスが介入できないようにする。

ドメイン名を入力する方法

パソコンの Web ブラウザに、セーフティ I/O ターミナルの IP アドレスを割り当てたドメイン名を入力する方法の手順を説明します。この方法は、通信データの暗号化およびサーバ証明書による認証を行うため、IP アドレスを入力する方法に比べてセキュリティリスクが低減されます。
ドメイン名を入力する方法を使用するためには、あらかじめパソコンに HTTPS 通信機能を使用するための設定を行っておく必要があります。HTTPS 通信機能の詳細は、「8-3 HTTPS 通信機能 (P.8-8)」を参照してく

ださい。HTTPS 通信機能を使用するための設定は、パソコンごとに一度行うだけです。ここでは、すでに HTTPS 通信機能を使用する設定が行われているパソコンを使用しているとして、Web UI の起動手順を説明します。

1 **セーフティ I/O ターミナルの EtherNet/IP ポートとパソコンの Ethernet ポートを、Ethernet ケーブルで接続します。**

2 **パソコンで Web ブラウザを起動します。**

3 **Web ブラウザに、セーフティ I/O ターミナルの IP アドレスに割り当てたドメイン名を入力します。たとえば、ドメイン名が「device1.NXR-SXD.local」の場合、以下のように入力します。「https://device1.NXR-SXD.local」**
Web UI が起動し Web ブラウザに以下のログイン画面が表示されます。



使用上の注意

パソコンの Web ブラウザに、セーフティ I/O ターミナルの IP アドレスを割り当てたドメイン名を入力する方法を使用する場合、つぎの点に注意してください。ドメインネームサーバの設定を変更せず、セーフティ I/O ターミナルの IP アドレスを変更した場合、IP アドレスを割り当てたドメイン名を入力すると意図しないデバイスにアクセスしてしまう可能性があります。セーフティ I/O ターミナルの IP アドレスを変更する際は、ドメインネームサーバの設定も合わせて変更してください。また、Web UI のログイン画面に表示される MAC アドレスが、意図したセーフティ I/O ターミナルの MAC アドレスと一致していることを確認してください。

7-2-6 ログイン

セーフティパスワードを入力して権限認証を行い、Web UI にログインします。



工場出荷時には、セーフティパスワードは設定されていません。

セーフティパスワードを 5 回間違えると、10 分間ログインできなくなります。セーフティパスワードを間違えた回数は、ログインに成功する、電源を再投入する、または 10 分経過するのいずれかでリセットされます。

ログイン後 10 分以上操作しなかった場合、管理者の権限を持たない第三者による不正使用を防ぐため、セーフティパスワードの再入力が要求されます。

ログイン後、ログアウトせずに Web ブラウザを終了させた場合、ログイン状態が 10 分間維持されます。したがって、同じユーザが同じパソコンから Web ブラウザを起動すると、ログイン操作なしに Web UI を使用できます。その間、他のユーザはログインできません。

ログイン後、ログアウトせずにセーフティ I/O ターミナルの電源を OFF した場合、ログイン状態は破棄されます。したがって、同じユーザが同じパソコンから Web ブラウザを起動しても、再度 Web UI へのログインが必要です。

［セーフティパスワード］欄は、セーフティパスワードの表示／非表示を切り替えられます。

使用上の注意

- ログイン画面に表示される MAC アドレスが、意図したユニットの MAC アドレスであることを確認してから使用してください。ユニットの MAC アドレスは、ユニット本体側面に書かれています。
- 第三者による不正使用を防止するため、Web UI による操作を中断しパソコンから離れる際にセーフティ I/O ターミナルからログアウトしてください。Web UI の動作状態モニタ画面、I/O モニタ画面、発生中異常・イベントログ画面で［自動更新］を選択すると、10 分以上操作しなくてもセーフティパスワードの再入力が要求されません。

ログインの使用手順

ログインの使用手順は、以下のとおりです。

1 **［IP アドレス］欄に当該ユニットの IP アドレス、［MAC アドレス］欄に当該ユニットの MAC アドレスが表示されていることを確認します。**

2 **［操作権限］で［管理者］、または［観察者］を選択します。**

3 **［Language settings］で［English］、または［日本語］を選択します。**
Web UI で表示される言語が決定します。

4 **管理者の場合、セーフティパスワードを入力して、[ログイン] ボタンを押します。観察者の場合は、セーフティパスワードの入力は不要です。**
当該ユニットへの初回のログイン時、かつ管理者の場合は、ログインした後に初期セーフティパスワード変更画面が表示されます。それ以外の場合は、ログイン後に動作状態モニタ画面が表示されます。

7-2-7 ログアウト

Web UI からログアウトします。
共通メニューの［ログアウト］ボタンを押すと、ログアウト画面が表示されます。



ログアウトの使用手順

ログアウト画面で、Web UI からログアウトします。設定の手順は、以下のとおりです。

1 **[ログアウト] ボタンを押します。**
ログアウトが実行され、ログイン画面が表示されます。

7-2-8 初回ログイン時の注意事項

初回ログイン時には、初期セーフティパスワード変更画面が表示されます。セキュリティ性向上のため、必ずセーフティパスワードを変更してください。

初期セーフティパスワード変更

初期セーフティパスワード変更画面は、初回ログイン時にセーフティパスワードを初期セーフティパスワードから変更する画面です。初回ログイン時に、ログイン画面の直後に表示されます。新しいセーフティパスワードを設定する、または［初期セーフティパスワードのまま使用］を選択すると、次回のログイン時からは表示されません。
セーフティパスワード認証機能の詳細は、「7-18 セーフティパスワードの設定 (P.7-100)」を参照してください。



● 初期セーフティパスワード変更の使用手順

初期セーフティパスワード変更画面で、セーフティパスワードを初期セーフティパスワードから変更します。使用手順は、以下のとおりです。

1 **[新しいセーフティパスワードを設定]、または［初期セーフティパスワードのまま使用］のどちらかにチェックを入れます。**
［初期セーフティパスワードのまま使用］にチェックを入れると、セーフティパスワードは変更されません。しかし、セキュリティ性を向上させるため、セーフティパスワードを変更することをお勧めします。

2 **［新しいセーフティパスワードを設定］にチェックを入れた場合、［新しいセーフティパスワード］、および［新しいセーフティパスワード（確認用）］に新しいセーフティパスワードを入力します。**
セーフティパスワードは、セキュリティ性を向上させるため 8 文字以上にしてください。
ただし、他の機器と同じパスワードにしたいなど特別な事情がある場合には、［1 から 7 文字のセーフティパスワードを入力］にチェックを入れると、1 から 7 文字のセーフティパスワードが設定できます。

3 **［設定］ボタンを押します。**
セーフティパスワードが設定され、以下のメッセージが表示されます。



4 **［OK］ボタンを押します。**
ログイン画面が表示されます。



5 **新しいセーフティパスワードを入力して、［ログイン］ボタンを押します。**
動作状態モニタ画面が表示されます。

7-3 CIP Safety 通信の設定

ここでは、CIP Safety オリジネータと CIP Safety ターゲットのセーフティ I/O ターミナルで CIP Safety 通信するためのコネクションの設定方法について説明します。

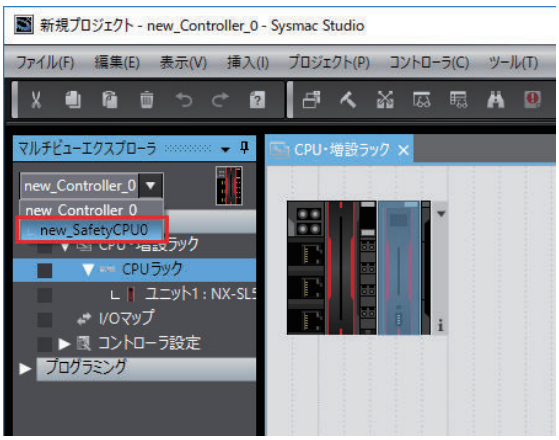
7-3-1 CIP Safety 通信のコネクション設定

セーフティ I/O ターミナルの CIP Safety コネクション設定方法を説明します。

コネクションの登録手順

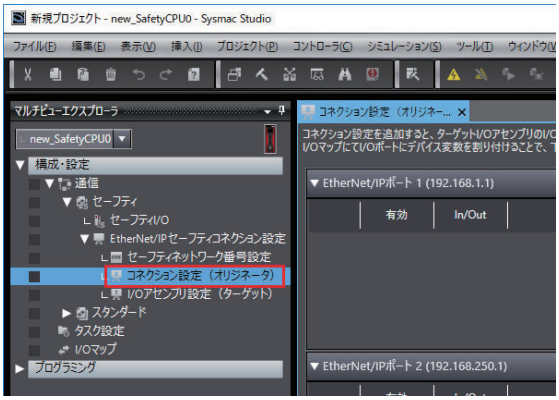
セーフティネットワークコントローラを CIP Safety オリジネータの一例として、Sysmac Studio 上でのセーフティ I/O ターミナルの CIP Safety コネクションの登録手順を説明します。

1 **マルチビューエクスプローラのコントローラ選択ボックスから、対象となるセーフティ CPU ユニットを選択します。**



2 **マルチビューエクスプローラの［構成・設定］－［通信］－［セーフティ］－［EtherNet/IP セーフティコネクション設定］－［コネクション設定（オリジネータ）］をダブルクリック、または右クリックして［編集］を選択します。**

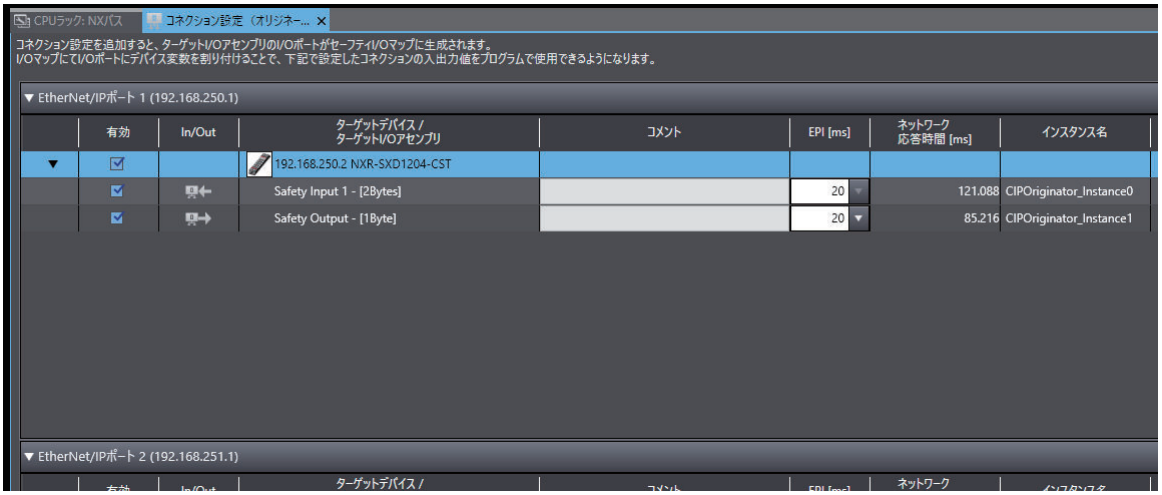
エディットウィンドウには、コネクション設定（オリジネータ）編集画面が表示されます。



3 **ツールボックスから［Safety I/O and Logic Device］グループを選択し、［NXR-SXD1204-CST］または［NXR-SXD1204B-CST］を選択します。**



4 **ツールボックスで選択したセーフティ I/O ターミナルをドラッグし、コネクション設定（オリジネータ）編集画面へドロップ、または選択したセーフティ I/O ターミナルをダブルクリックします。**



5 **必要に応じて、セーフティ I/O ターミナルの IP アドレスを設定します。**
追加されたコネクションの IP アドレスはセーフティネットワークコントローラに設定された EtherNet/IP ポートの IP アドレスから自動的に割り当てられます。ネットワークの構成に応じて、IP アドレスの編集を行ってください。
IP アドレスを編集する方法は、「コネクションの IP アドレス設定手順 (P.7-26)」を参照してください。

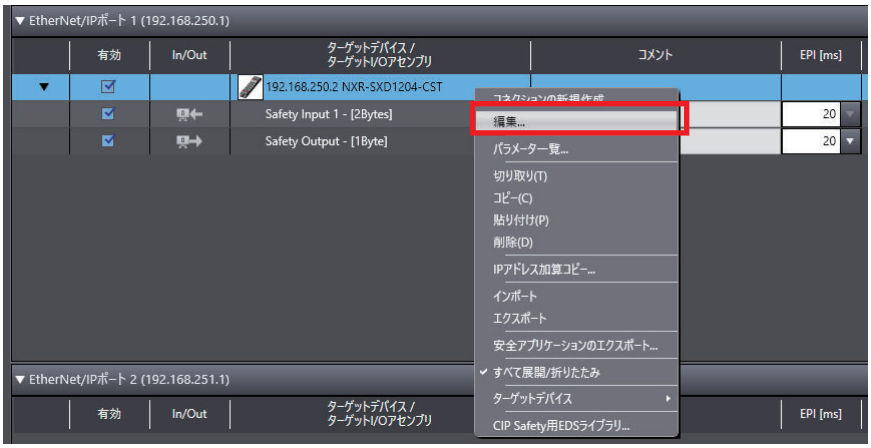
6 **必要に応じて、I/O アセンブリを変更します。**
初期状態では、形 NXR-SXD1204-CST は［Safety Input 1］と［Safety Output］が登録されます。形 NXR-SXD1204B-CST も同様です。
I/O アセンブリを変更する方法は、「コネクションの追加登録手順 (P.7-27)」を参照してください。

7 **登録したコネクションのパラメータを編集します。**
コネクションのパラメータを編集する方法は、「コネクションのパラメータ編集手順 (P.7-30)」を参照してください。

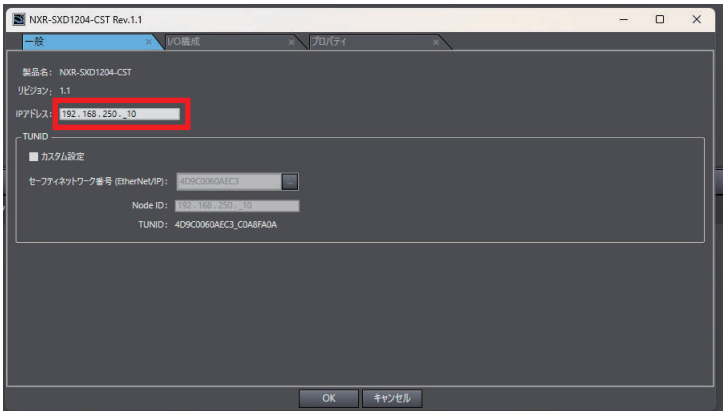
コネクションの IP アドレス設定手順

コネクション設定の IP アドレスに、セーフティ I/O ターミナルの IP アドレスを設定する手順を説明します。

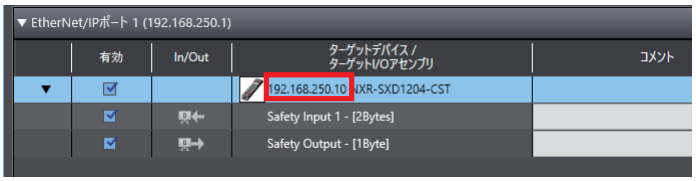
1 **コネクション設定（オリジネータ）編集画面でセーフティ I/O ターミナルを選択し、右クリックして［編集］を選択します。**



2 **IP アドレス欄に IP アドレスを入力し、［OK］ボタンをクリックします。**



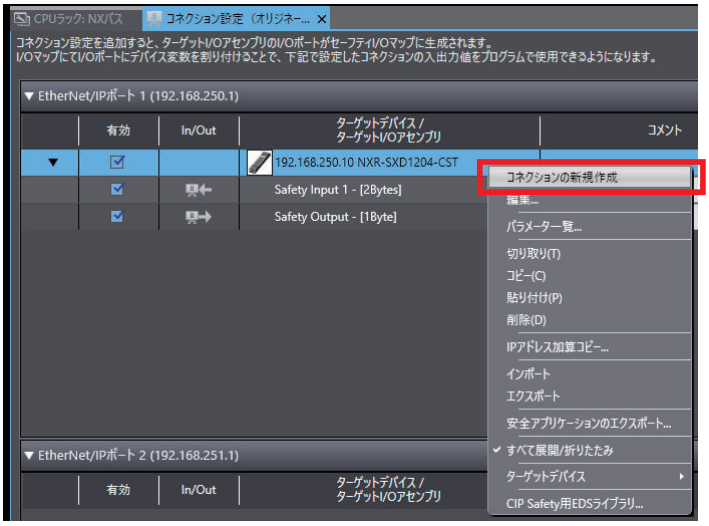
入力した IP アドレスがコネクション設定（オリジネータ）編集画面に反映されます。



コネクションの追加登録手順

セーフティ I/O ターミナルとのコネクションを追加で登録する手順を以下に示します。

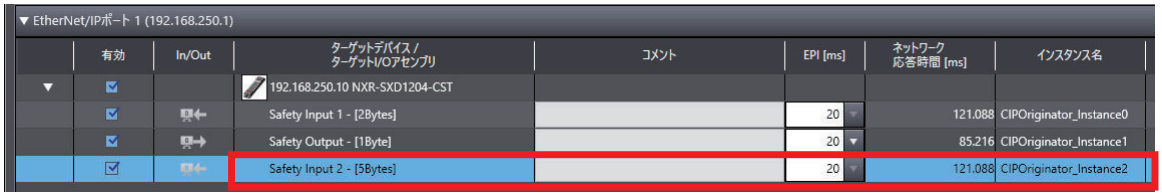
1 **コネクション設定（オリジネータ）編集画面でセーフティ I/O ターミナルを選択し、右クリックして［コネクションの新規作成 ］を選択します。**



2 [I/O アセンブリ] のプルダウンリストから追加したい項目を選択し、[OK] ボタンをクリックします。



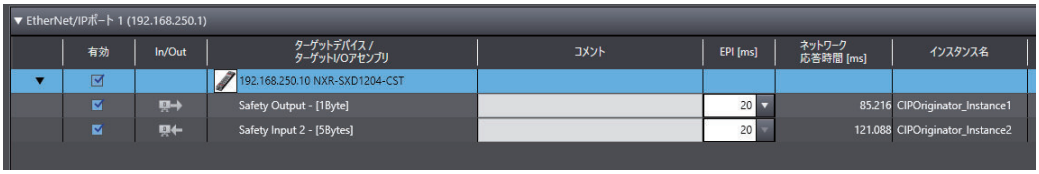
追加した I/O アセンブリがコネクション設定（オリジネータ）編集画面に表示されます。



3 使用しない I/O アセンブリを選択し、右クリックして [削除] を選択します。



IN:
OUT:



設定した I/O アセンブリは、自動で I/O マップにも反映されます。



● I/O アセンブリの種類と制約事項

以下に、セーフティ I/O ターミナルの登録可能な Input アセンブリと Output アセンブリの種類と制約事項を記載します。

- Input アセンブリ
  Input アセンブリは、セーフティ I/O ターミナルからセーフティコントローラ方向への送信データです。

アセンブリ	データサイズ	備考
Safety Input 1	2byte	セーフティ入力端子の値＋セーフティ入力端子のステータス情報（集約）＋セーフティ出力端子のステータス情報（集約）＋出力用電源エラーフラグ＋コネクションのステータス情報
Safety Input 2	5byte	セーフティ入力端子の値 + セーフティ入力端子のステータス情報 +セーフティ入力端子のステータス情報（集約）＋セーフティ出力端子のステータス情報（集約）+ 出力用電源エラーフラグ + コネクションのステータス情報+ 安全アプリケーションの番号
Safety Input 3	9byte	セーフティ入力端子の値 + セーフティ入力端子のステータス情報 + セーフティ出力端子のステータス情報 + セーフティ出力端子に実際に出力されている値 + テスト出力端子のステータス情報 + テスト出力端子の値 + セーフティ入力端子のステータス情報（集約）＋セーフティ出力端子のステータス情報（集約）+ 出力用電源エラーフラグ + コネクションのステータス情報+ 安全アプリケーションの番号

- Output アセンブリ
  Output アセンブリは、セーフティコントローラからセーフティ I/O ターミナル方向への送信データです。

アセンブリ	データサイズ	備考
Safety Output	1byte	セーフティ出力端子への ON/OFF
Safety Output + Standard Output	3byte	セーフティ出力端子への ON/OFF +テスト出力端子へのスタンダード出力の ON/OFF
Safety Remote Output 1 + Standard Output	3byte	リモート出力 Ro 1 の ON/OFF +テスト出力端子へのスタンダード出力の ON/OFF
Safety Remote Output 2	1byte	リモート出力 Ro 2 の ON/OFF
Safety Remote Output 3	1byte	リモート出力 Ro 3 の ON/OFF

安全アプリケーションの使用有無によって、設定可能な Output アセンブリが異なります。また、Output アセンブリの組み合わせは以下のとおりです。

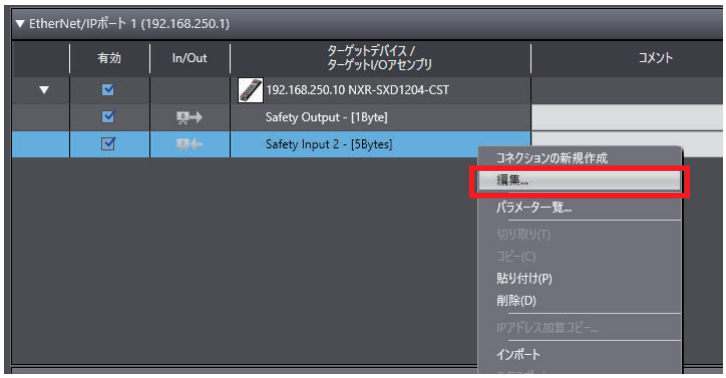
安全アプリケーションの Sysmac Studio の設定値およびロータリスイッチ設定	Output アセンブリの組み合わせ
安全アプリケーションを未使用 （安全アプリケーションの設定値が「00: リモート I/O モード」、およびロータリスイッチの SW1=SW2=0 の場合）	以下の 2 種類のアセンブリを使用できます。 • Safety Output • Safety Output + Standard Output ただし、2 つのアセンブリのコネクションを同時に開設することはできません。
安全アプリケーションを使用 （安全アプリケーションの設定値が「00: リモート I/O モード」以外、およびロータリスイッチの SW1=SW2=1～3、9～13、15 の場合）	以下の 3 種類のアセンブリを使用できます。 • Safety Remote Output 1 + Standard Output • Safety Remote Output 2 • Safety Remote Output 3

I/O アセンブリの詳細については、「A-3 I/O アセンブリのポートと対応するセーフティ I/O アセンブリデータの要素 (P.A-13)」を参照してください。

コネクションのパラメータ編集手順

CIP Safety コネクションのパラメータを編集する手順を以下に示します

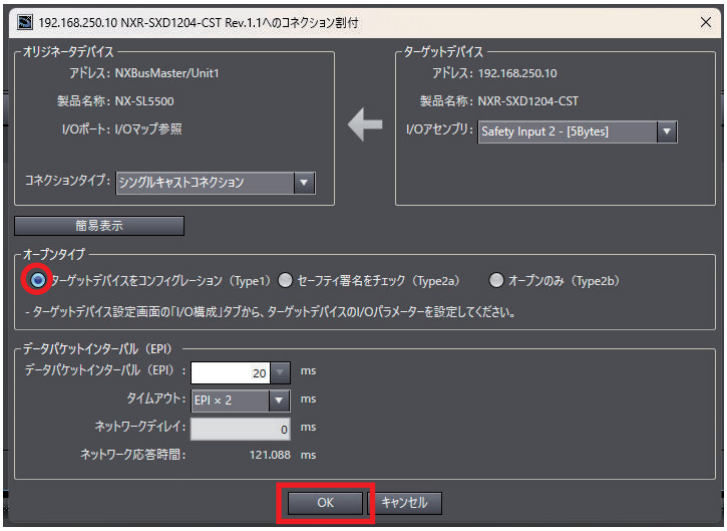
1 **コネクション設定（オリジネータ）編集画面でセーフティ I/O ターミナルのコネクションを選択し、右クリックして［編集］を選択します。**



2 **［詳細表示］を選択します。**



3 **［オープンタイプ］の設定で［ターゲットデバイスをコンフィグレーション］を選択し、［OK］ボタンをクリックします。**



項目	内容
I/O アセンブリ	I/O アセンブリは、CIP Safety オリジネータと CIP Safety ターゲットの間でサイクリックに交換する I/O データの単位です。 セーフティ I/O ターミナルは、いくつかの I/O アセンブリを定義し用意しています。定義された I/O アセンブリの中から選択し、CIP Safety コネクション 1 本につき 1 つの I/O アセンブリを登録します。 CIP Safety コネクションが開設可能な、ターゲットデバイスの I/O アセンブリがリスト表示されます。
コネクションタイプ	入力コネクション（ターゲットデバイスから受信）の場合は、［シングルキャスト］か［マルチキャスト］を選択します。 初期値は［シングルキャスト］です。
オープンタイプ	コネクション開設の種類を選択します。 • ターゲットデバイスをコンフィグレーション(Type1) コネクション確立後、ターゲットデバイスのコンフィグレーションを行います。 • セーフティ署名をチェック(Type2a) コネクション確立時にターゲットデバイスのコンフィグレーションが正しいことをセーフティ署名によりチェックします。セーフティ署名は、セーフティコンフィグレーション CRC とセーフティコンフィグレーションタイムスタンプで構成されます。 • オープンのみ(Type2b) コネクション確立時にターゲットデバイスのコンフィグレーションチェックを行いません。 初期値は［ターゲットデバイスをコンフィグレーション(Type1)］です。
データパケットインターバル(EPI)	オリジネータとターゲットとの間でセーフティプロセスデータ通信を行う間隔を設定します。 初期値は 20(ms)です。設定範囲は「2-1-2 通信仕様 (P.2-3)」を参照してください。
タイムアウト	通信エラーを判定するまでのタイムアウト時間を EPI の倍数で指定します。 初期値は EPIx2(ms)（1 回のタイムアウトを許容）です。倍数の設定範囲は 1～4 です。
ネットワークディレイ	ネットワーク上の伝搬遅延時間を設定します。 初期値は 0(ms)です。
ネットワーク応答時間	コネクション応答性能の値が ms 単位で表示されます。セーフティリアクションタイムの計算に使用します。

⚠ 警告

オープンタイプを［オープンのみ］に設定する場合は、オリジネータ／ターゲットが正しいコンフィグレーションを持っていることを確認した上で使用してください。
安全機能が損なわれ、重度の人身傷害が万一の場合起こるおそれがあります。

参考

登録したコネクション数に対する EPI の最小値の目安です。なお、Input のコネクションタイプがマルチキャストの場合は、オリジネータを 8 台接続する想定です。

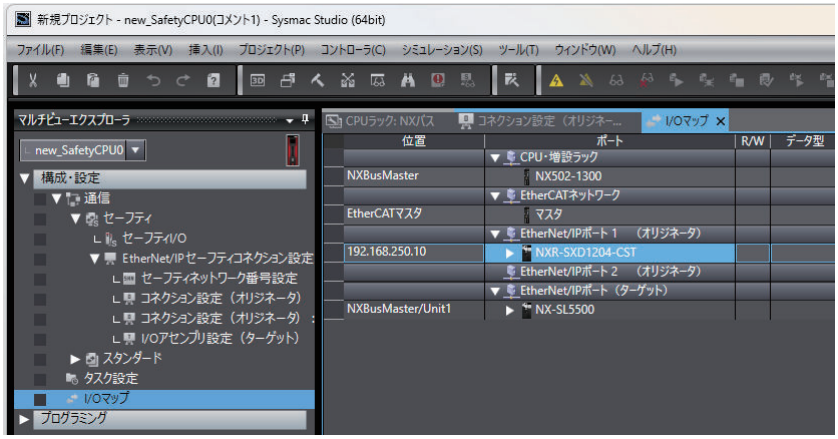
コネクション数	EPI の最小値
1 本（Input 1 本または Output 1 本）	5ms
5 本（Input 2 本および Output 3 本）	20ms

4 **設定が完了したら、[OK] ボタンをクリックします。**

デバイス変数の登録手順

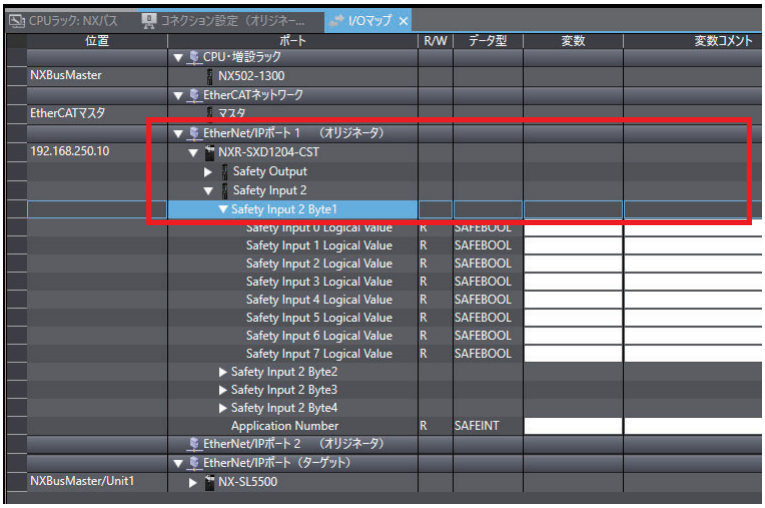
デバイス変数とはデバイス（スレーブ／ユニット／セーフティ I/O ターミナル）内のデータにアクセスする変数です。
セーフティ CPU ユニットは、“I/O ポート”と呼ばれる論理的なインタフェースを介して、外部のデバイスと信号交換を行います。
デバイスの入出力の値をセーフティ CPU ユニットのセーフティプログラム上で使用するために、デバイスの I/O ポートに対してデバイス変数を登録する手順を説明します。
セーフティ I/O ターミナルに形 NXR-SXD1204-CST を使用した例です。

1 **マルチビューエクスプローラの [構成・設定] – [I/O マップ] を選択します。**



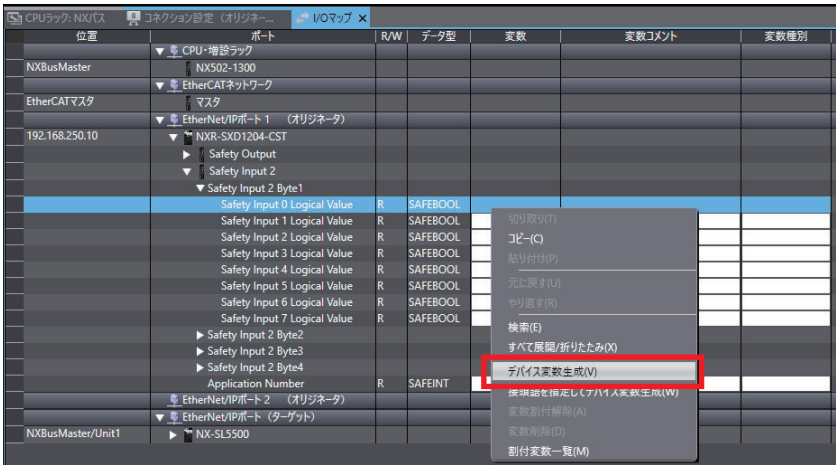
エディットウィンドウには、I/O マップ編集画面が表示されます。

2 **I/O マップ編集画面で [EtherNet/IP ポート 1（オリジネータ）] – [NXR-SXD1204-CST] – [Safety Input 2] – [Safety Input 2 Byte1] を展開します。**

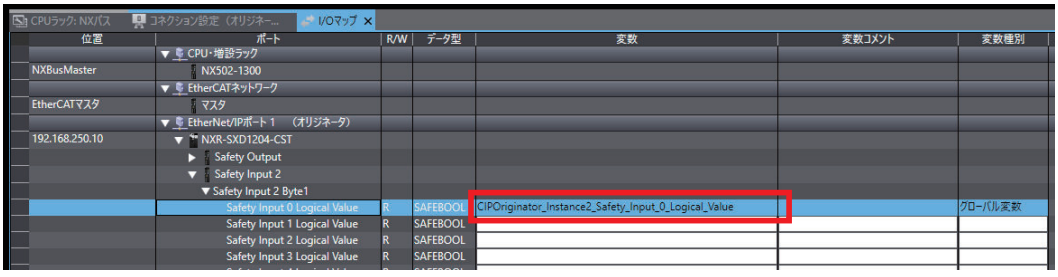


3 **I/O ポートを選択し、［変数］の列に直接変数名を入力します。または、セーフティ I/O ターミナル名もしくは I/O ポート（複数選択可）を選択し、右クリックして［デバイス変数生成］を選択します。**

［デバイス変数生成］を選択した場合、デバイス変数名は自動的にデバイス名＋ポート名称となります。



デバイス変数が登録されます。



ここで入力、あるいは自動生成したデバイス変数は、グローバル変数テーブルに登録されます。

参考

あらかじめ変数を登録している場合は、I/O ポートに割り付ける変数をプルダウンリストから選択してください。

7-3-2 セーフティ I/O ターミナルの設定のエクスポートとインポート

セーフティ I/O ターミナルの設定を 1 つのファイル（拡張子.tds）としてエクスポート／インポートし、再利用することができます。

対象データは、以下のとおりです。
- CPU ユニットとのコネクション設定
- Sysmac Studio で設定したセーフティ I/O ターミナルの IP アドレス
- セーフティ I/O ターミナルの入出力機能の設定

参考

Web UI によるバックアップ、照合、リストアは、「7-19 バックアップ (P.7-104)」を参照してください。

設定のエクスポート手順

セーフティ I/O ターミナルの設定をエクスポートする場合の手順は以下となります。

1 コネクション設定（オリジネータ）編集画面でセーフティ I/O ターミナルを選択し、右クリックして［エクスポート］を選択します。



［エクスポート］ダイアログボックスが表示されます。

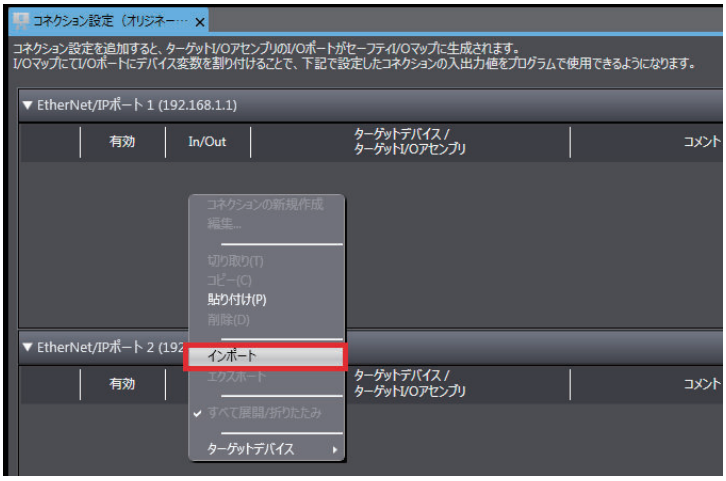
2 保存先を選択し、任意のファイル名をつけて［保存］ボタンをクリックします。

指定した保存先に拡張子 .tds のセーフティ I/O ターミナル設定ファイルが保存されます。
デフォルトのファイル名は、IP アドレス␣ターゲットデバイス名.tds となります。

設定のインポート手順

セーフティ I/O ターミナルの設定をインポートする場合の手順は以下となります。

1 コネクション設定（オリジネータ）編集画面でセーフティ I/O ターミナルを選択し、右クリックして［インポート］を選択します。



［インポート］ダイアログボックスが表示されます。

2 **任意の拡張子.tds のセーフティ I/O ターミナル設定ファイルを選択して、［開く］ボタンをクリックします。**

使用上の注意

ターゲットデバイス設定ファイルのインポートでは、CRC によるデータの整合性チェックは行われません。
お客様の責任において、インポート後に設定が正しいことを検証し、十分に動作確認を行った後、本運転に移行してください。

7-4 EtherNet/IP 通信の設定

ここでは、EtherNet/IP オリジネータと EtherNet/IP ターゲットのセーフティ I/O ターミナルでタグデータリンク通信するためのコネクションの設定方法、および LLDP 機能の設定方法について説明します。

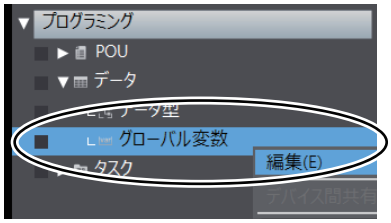
7-4-1 タグデータリンク通信の設定

セーフティ I/O ターミナルとオリジネータ間でタグデータリンク通信するためのコネクションを設定します。

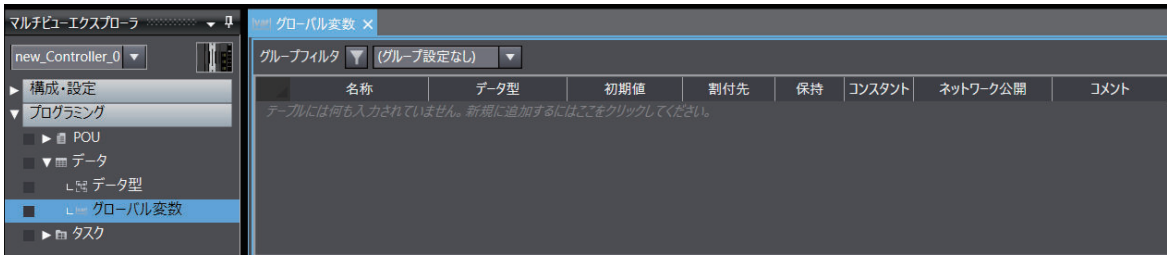
タグデータリンク通信の設定手順

ここでは、Sysmac Studio を用いてセーフティ I/O ターミナルのタグデータリンク通信を設定する手順について説明します。
下記の手順は、オリジネータにはスタンダードコントローラの内蔵 EtherNet/IP ポートを使用し、タグデータリンクの I/O アセンブリデータに Input Data (Assembly 960 - 3C0Hex), Size 5 bytes を設定する例です。

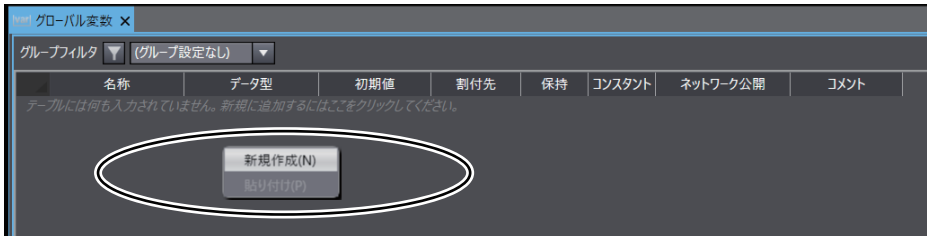
1 **マルチビューエクスプローラでスタンダードコントローラの［プログラミング］－［データ］－［グローバル変数］をダブルクリックします。**
または、［プログラミング］－［データ］－［グローバル変数］を右クリックして、メニューから［編集］を選択します。



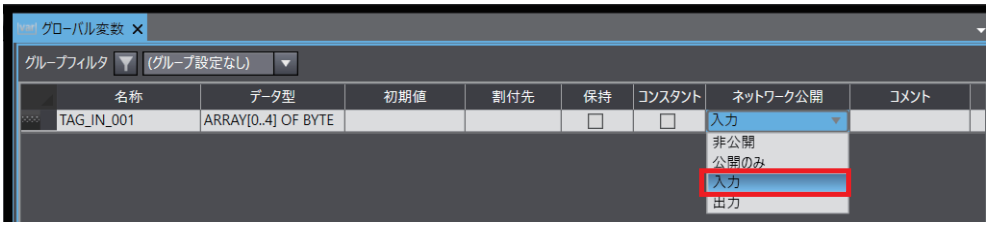
グローバル変数の登録テーブルが表示されます。



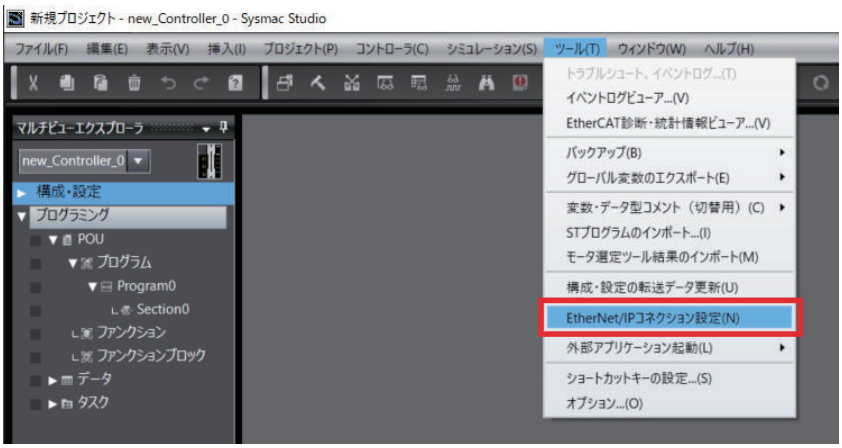
2 **グローバル変数テーブル内で［Insert］キーを押すか、または右クリックしてメニューから［新規作成］を選択します。**



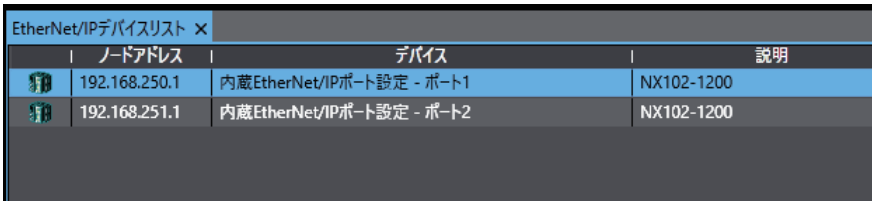
3 グローバル変数に 5byte 分の変数を登録し、［ネットワーク公開］を［入力］に設定します。



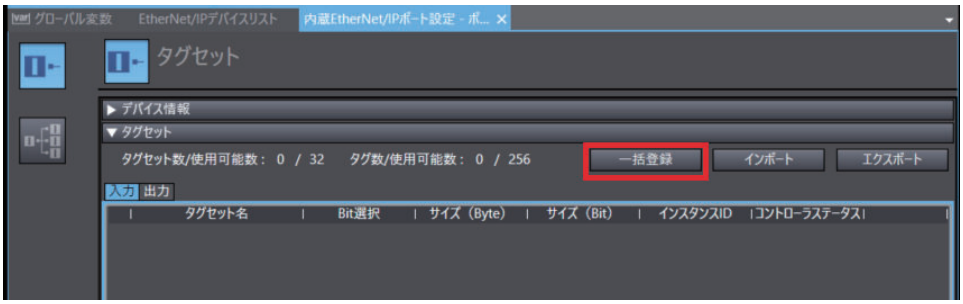
4 マルチビューエクスプローラで標準 PLC（初期表示 new_Controller_0）を選択し、画面上部のメニューバーから、［ツール］－［EtherNet/IP コネクション設定］を選択します。



5 タグデータリンクを設定したいネットワークをダブルクリック、または、右クリックして［編集］を選択します。



6 ［入力］タブが選択されていることを確認し、［一括登録］をクリックします。



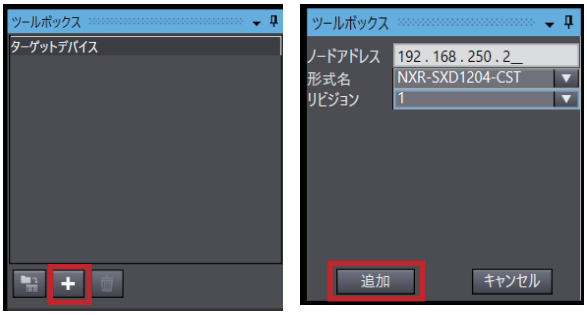
7 手順 3 で登録した変数が表示されていることを確認し、［登録］をクリックします。



タグセットが登録されます。

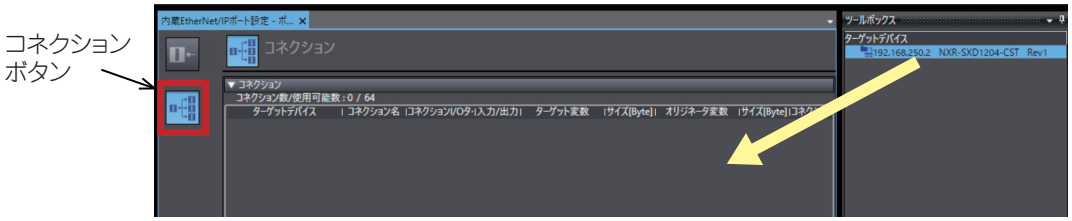


8 **ターゲットデバイス欄の［+］ボタンをクリックし、ターゲットの IP アドレス、形式名、リビジョンを入力し、［追加］ボタンをクリックします。**

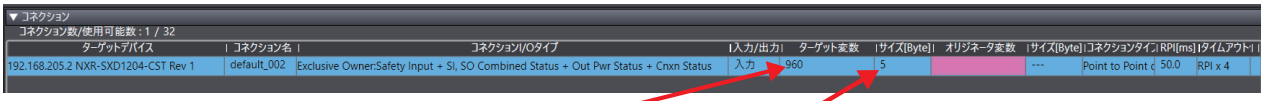


形式名がプルダウンリストにない場合は、その形式の EDS ファイルをインストールしてください。インストール方法は、下記の参考の「EDS ファイルのインストール手順」を参照してください。

9 **［コネクション］ボタンをクリックするとコネクション設定画面が開きます。先ほど追加したターゲットの情報が、ターゲットデバイス欄に表示されるので、コネクションウィンドウへドラッグ&ドロップします。**



10 **コネクションウィンドウにターゲットデバイスが追加されるので、ターゲット変数を入力します。**



Input Data (Assembly 960 - 3C0Hex), Size 5 bytes

byte	bit							
	7	6	5	4	3	2	1	0
0	Safety Input7	Safety Input6	Safety Input5	Safety Input4	Safety Input3	Safety Input2	Safety Input1	Safety Input0
1	Safety Input3 Status	Safety Input2 Status	Safety Input1 Status	Safety Input0 Status	Safety Input11	Safety Input10	Safety Input9	Safety Input8
2	Safety Input11 Status	Safety Input10 Status	Safety Input9 Status	Safety Input8 Status	Safety Input7 Status	Safety Input6 Status	Safety Input5 Status	Safety Input4 Status
3	Safety Input Status	Safety Output Status	Output Power Status	Cnxn. Status (ON)	予約	予約	予約	予約
4	Application Number							

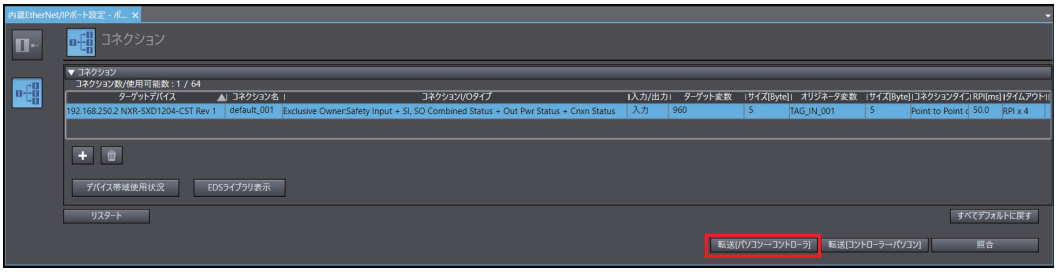
ターゲット変数とサイズは、「A-2 セーフティ I/O アセンブリデータ (P.A-4)」の表に記載している Assembly と Size の値を入力してください。
［コネクション I/O タイプ］、［コネクションタイプ］、［RPI］、［タイムアウト値］については、必要に応じて設定してください。

11 同様に、オリジネータ変数を入力します。

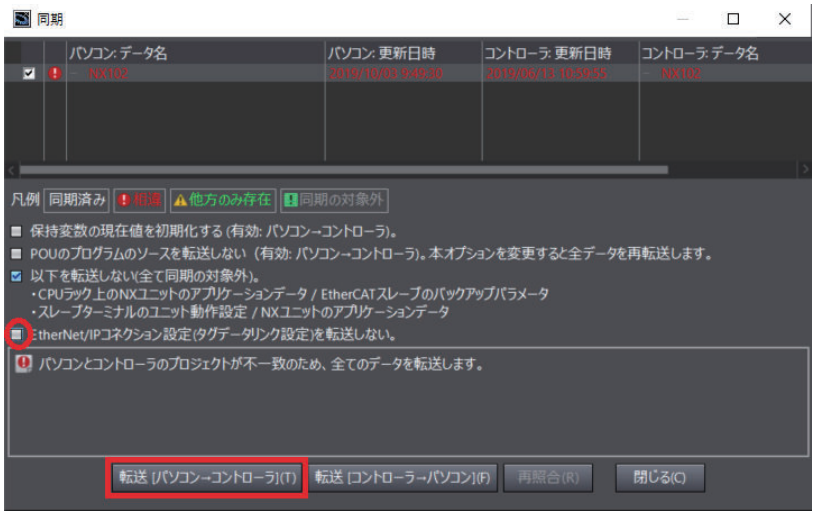
オリジネータ変数は、手順 7 で設定したタグセット名をプルダウンリストより選択してください。

12 オンラインにして、タグセットおよびコネクション設定をデバイスに書き込みます。

- タグデータリンク設定だけを転送する場合
  コネクション設定画面で、転送［パソコン→コントローラ］をクリックします。



- プログラムを含むすべてを同期する場合
  メニューの［コントローラ］から［同期］を選択し、同期ウィンドウを表示します。
  ［EtherNet/IP コネクション設定（タグデータリンク設定）を転送しない］のチェックを外し、転送［パソコン→コントローラ］をクリックします。



7-4-2 LLDP 機能

LLDP(Link Layer Discovery Protocol)機能は、ネットワーク上でセーフティ I/O ターミナルと物理的に通信可能な範囲に接続されている別のネットワーク機器との間で情報交換する機能です。

LLDP 機能の目的

LLDP 機能の目的は、隣接するネットワーク機器の情報を収集することにより、ネットワークの構成変更や異常の原因の特定を迅速に行えるようにすることです。
たとえば、本機能を使用することによって、ネットワークにどんな機器が接続しているかやそれらの機器で現在どんな機能が有効になっているかを検知することができます。それにより、通信異常の原因が、ネットワーク機器の設定誤りであることがわかるなどの効果があります。

LLDP 機能の使用手順

LLDP 機能の有効／無効設定は、Explicit メッセージ通信を使用して行います。
LLDP 機能に関する CIP オブジェクトは、「LLDP Management オブジェクト」と「LLDP Data Table オブジェクト」です。それぞれの詳細は、「A-4-12 LLDP Management オブジェクト（クラス ID：109Hex）(P.A-48)」、および「A-4-13 LLDP Data Table オブジェクト（クラス ID：10AHex）(P.A-50)」を参照してください。
CIP オブジェクトへの Explicit メッセージによるアクセス方法は、「Explicit メッセージサーバ機能 (P.6-6)」を参照してください。

LLDP 機能の詳細

LLDP 機能を使用して取得できるネットワーク機器の情報には、以下のものがあります。

- MAC アドレス
- インタフェースラベル
- 取得した情報が有効である時間
- サポートしている機能
- マネジメントアドレス

- CIP Identity
- Ethernet Preemption 機能の状態
- 情報が最後に更新されたときの時間情報

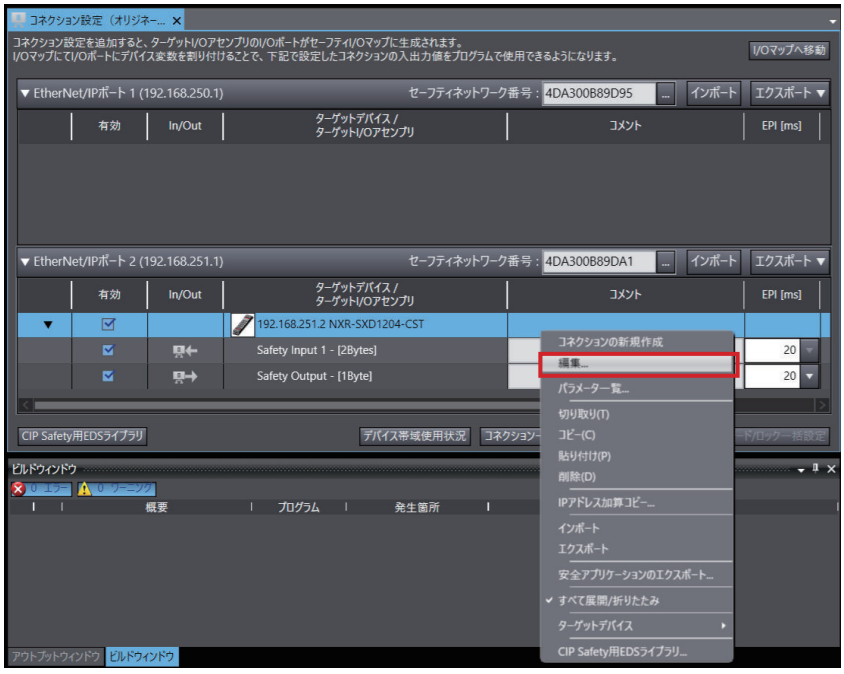
7-5 セーフティ入力機能の設定

セーフティ入力機能の設定を行うには、接続する機器に合わせてパラメータを設定していきます。
ここでは、Sysmac Studio での設定を例に説明します。

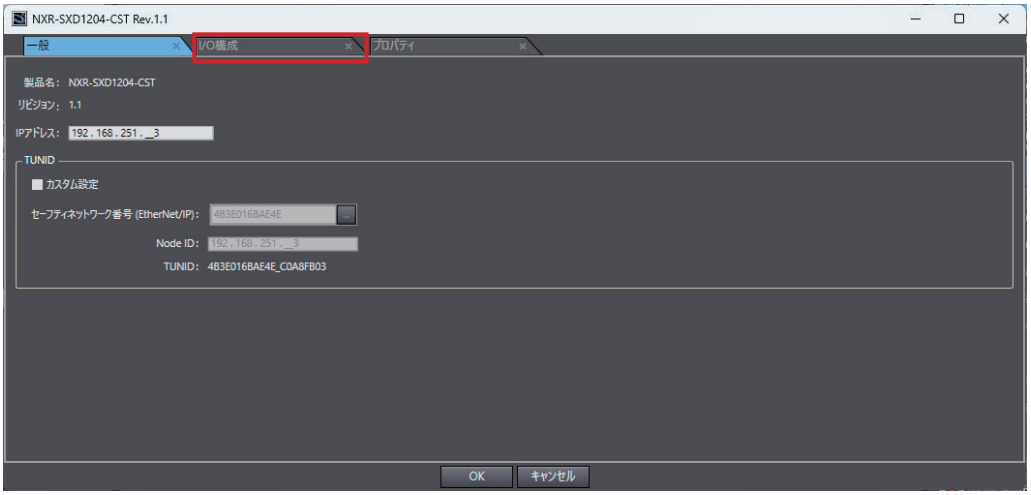
7-5-1 セーフティ入力機能の設定手順

セーフティ I/O ターミナルに入力機器を割り付けることにより、セーフティ I/O ターミナルのセーフティ入力機能の設定を行います。
さらに接続した入力機器の信号を取り込むためには、セーフティ I/O ターミナルの各入力端子に対して、I/O 構成設定を行う必要があります。
Sysmac Studio では、この設定はコネクション設定（オリジネータ）編集画面の中にあるため、コネクション設定（オリジネータ）編集画面から説明します。
なお CIP Safety コネクション設定の詳細については、「7-3-1 CIP Safety 通信のコネクション設定 (P.7-25)」を参照してください。
またセーフティ入力機能の詳細については、「6-4 セーフティ入力機能 (P.6-8)」を参照してください。
コネクション設定（オリジネータ）編集画面に登録されたデバイスに対して、I/O 構成設定を行う手順を以下に示します。

1 コネクション設定（オリジネータ）編集画面でセーフティ I/O ターミナルを選択し、ダブルクリック、または右クリックして［編集］を選択します。

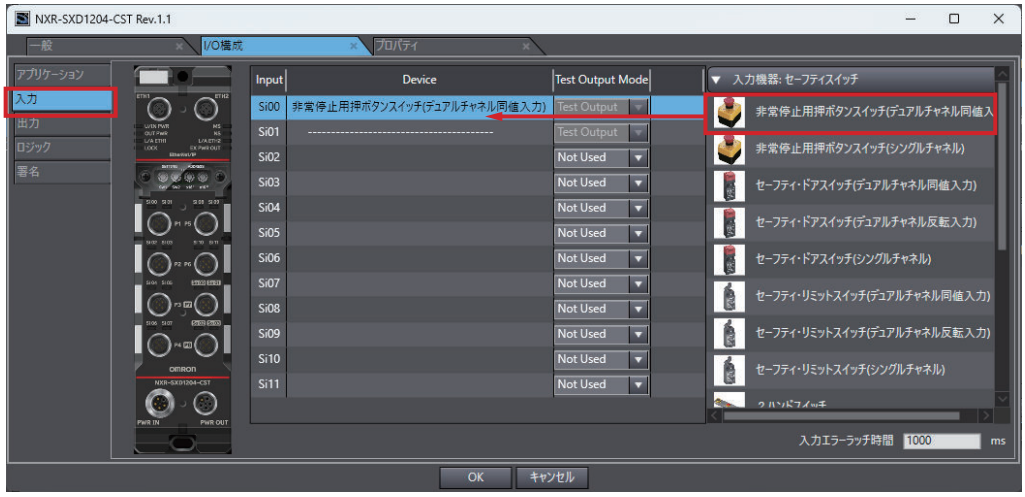


2 ［I/O 構成］タブを選択します。



3 **I/O 構成画面から入力機器の登録を行います。安全アプリケーションがリモート I/O モード、ユーザ定義アプリケーションの場合のみ、入力機器の登録ができます。**

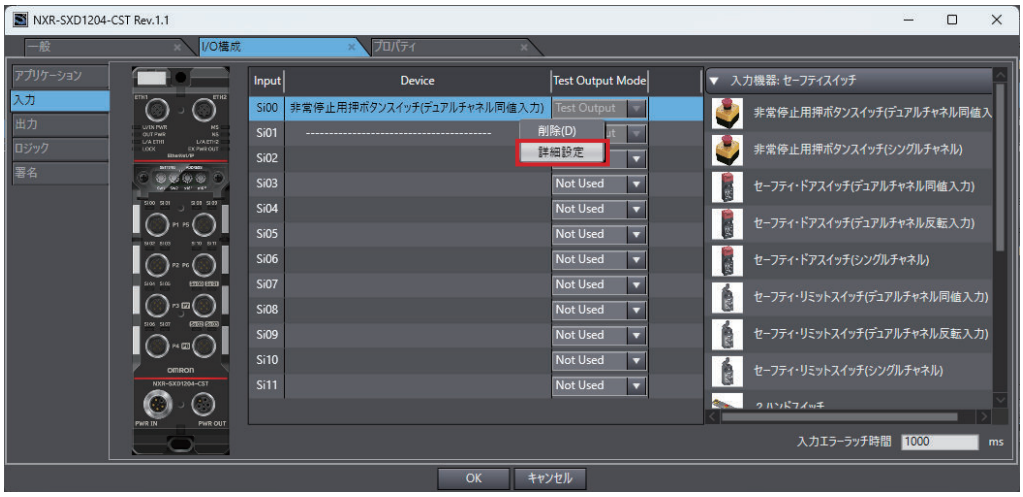
左側の［入力］タブを選択し入力機器の登録画面を表示します。右側のツールボックスを展開し、任意のデバイスを指定した端子へドラッグ&ドロップすることにより、入力機器を登録します。



4 **必要により、画面右下にある［入力エラーラッチ時間］を設定します。**

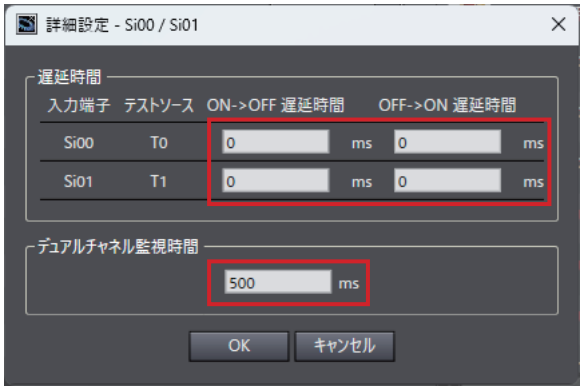


5 **登録した入力機器を選択し、ダブルクリック、もしくは登録した入力機器のコンテキストメニューから［詳細設定］を選択することで、［詳細設定］画面を表示します。**



6 **必要により以下の項目を設定します。**

- ［ON→OFF 遅延時間］
- ［OFF→ON 遅延時間］
- デュアルチャネル監視時間（デュアルチャネルの入力機器のみ）



7 **設定が完了したら、［OK］ボタンをクリックします。**

7-5-2 スタンダード出力機能の設定手順

セーフティ入力機器が半導体出力機器の場合、テスト出力端子のテスト出力モード（Test Output Mode）の設定に［Standard Output］も選択できます。
テスト出力端子を使用して、コントローラからのスタンダード出力が可能となります。
非安全のデジタル信号出力端子として使用します。例えば、表示灯や PLC の入力に接続して、モニタ出力などに使用します。
スタンダード出力機能には、Sysmac Studio を使用する方法、および Explicit メッセージ通信を使用する方法があります。

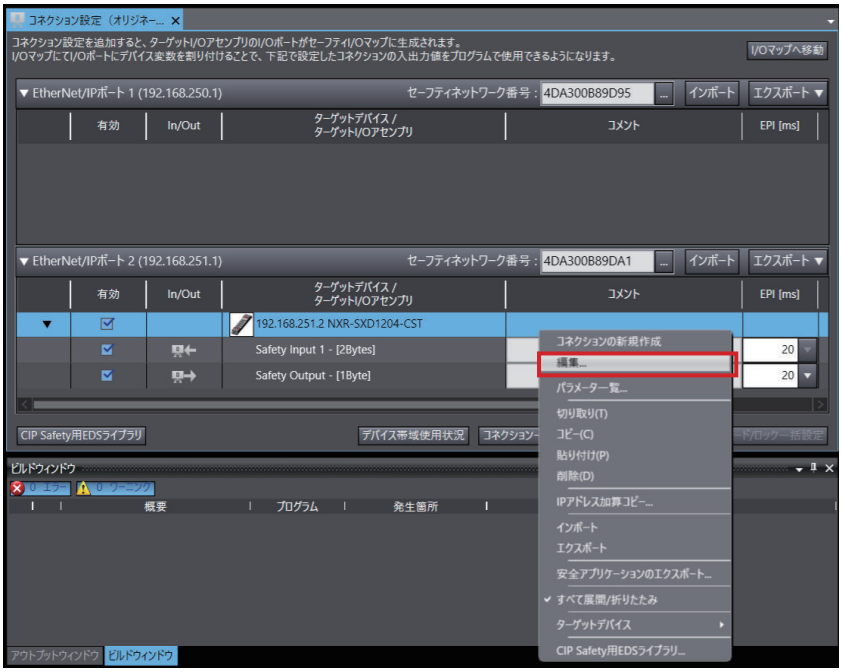
参考

本機能は、安全機能ではありません。

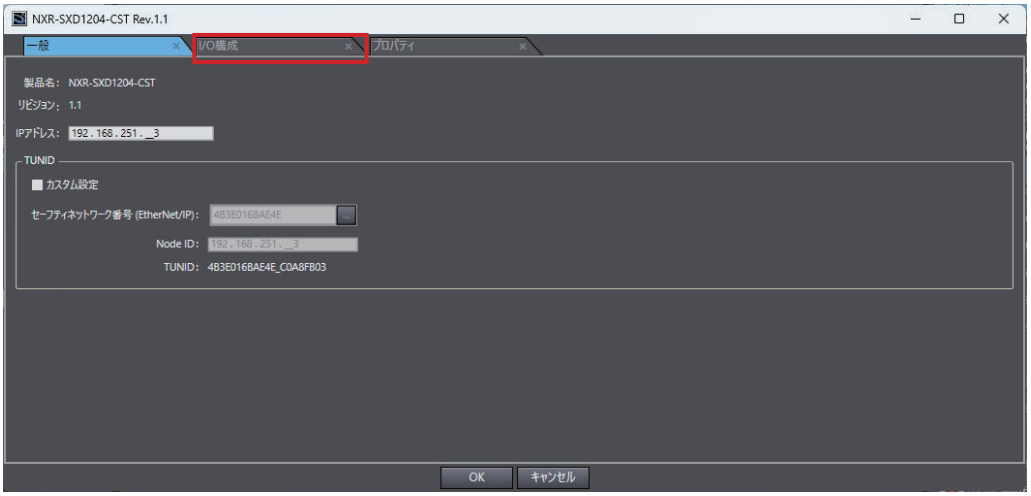
Sysmac Studio での設定手順

Sysmac Studio での手順は、以下のとおりです。
Sysmac Studio では、この設定はコネクション設定（オリジネータ）編集画面の中にあるため、コネクション設定（オリジネータ）編集画面から説明します。
なお CIP Safety コネクション設定の詳細については、「7-3-1 CIP Safety 通信のコネクション設定 (P.7-25)」を参照してください。
またセーフティ入力機能の詳細については、「6-4 セーフティ入力機能 (P.6-8)」を参照してください。
コネクション設定（オリジネータ）編集画面に登録されたデバイスに対して、I/O 構成設定を行う手順を以下に示します。

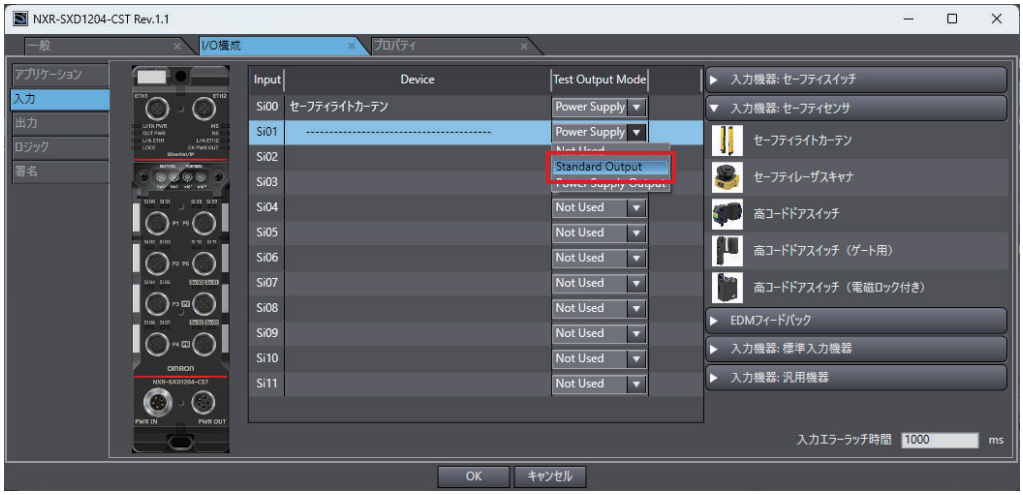
1 **コネクション設定（オリジネータ）編集画面でセーフティ I/O ターミナルを選択し、ダブルクリック、または右クリックして［編集］を選択します。**



2 **［I/O 構成］タブを選択します。**



3 **入力機器が半導体出力機器の端子に対し、[Test Output Mode] の設定で [Standard Output] を選択します。安全アプリケーションがリモート I/O モード、ユーザ定義アプリケーションの場合のみ、設定が可能です。**



4 **設定が完了したら、[OK] ボタンをクリックします。**

Explicit メッセージ通信での設定手順

テスト出力モードの使用方法を［Standard Output］に設定します。また、テスト出力端子の出力値を設定します。
送信コマンドは、以下のとおりです。

実施内容	送信コマンドの項目	送信コマンドの値
テスト出力端子の出力値を設定*1	サービスコード	10Hex(Set_Attribute_Single)
	クラス ID	09Hex(Discrete Output Point (DOP) オブジェクト)
	インスタンス ID	01Hex-0CHex (テスト出力端子ごとのインスタンスを指定する)
	アトリビュート ID	3(Value)
	サービスデータ	TRUE : テスト出力端子 ON FALSE : テスト出力端子 OFF

***1.** 値の書き込みができるのは、テスト出力モード（Test Output Mode）が［Standard Output］の場合だけです。それ以外の場合、テスト出力端子の出力値は TRUE 固定です。

CIP オブジェクトへの Explicit メッセージによるアクセス方法は、「Explicit メッセージサーバ機能 (P.6-6)」を参照してください。

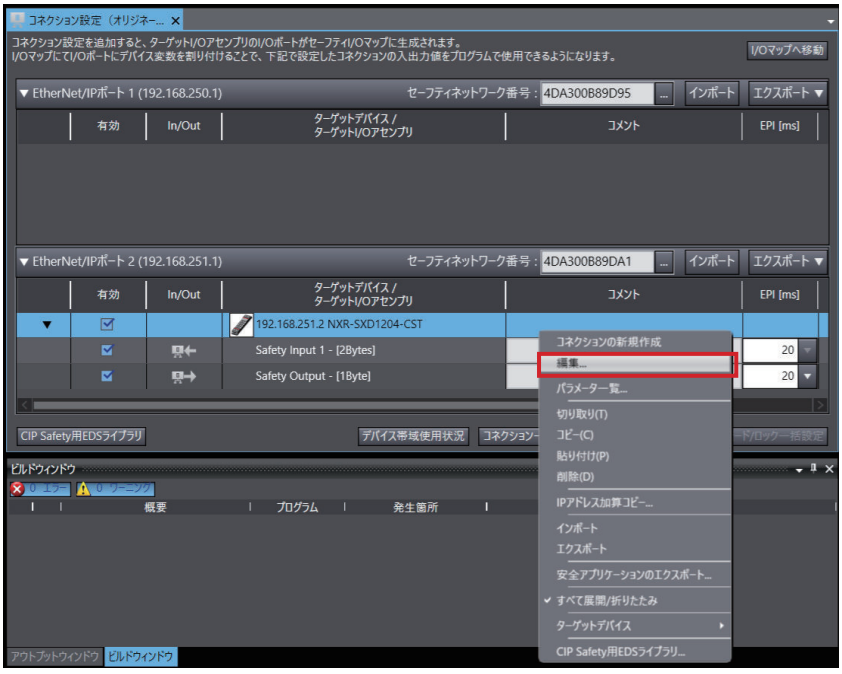
7-6 セーフティ出力機能の設定

セーフティ出力機能の設定を行うには、接続する機器に合わせてパラメータを設定していきます。
ここでは、Sysmac Studio での設定を例に説明します。

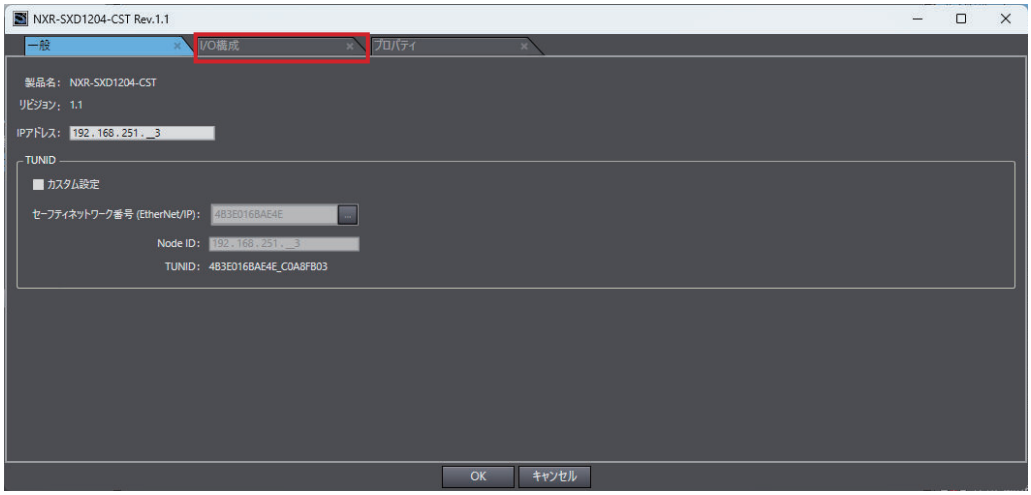
7-6-1 セーフティ出力機能の設定手順

セーフティ I/O ターミナルに出力機器を割り付けることにより、セーフティ I/O ターミナルのセーフティ出力機能の設定を行います。
さらに接続した出力機器へ信号を出力するためには、セーフティ I/O ターミナルの各出力端子に対して、I/O 構成設定を行う必要があります。
Sysmac Studio では、この設定はコネクション設定（オリジネータ）編集画面の中にあるため、コネクション設定（オリジネータ）編集画面から説明します。
なお CIP Safety コネクション設定の詳細については、「7-3-1 CIP Safety 通信のコネクション設定 (P.7-25)」を参照してください。
またセーフティ出力機能の詳細については、「6-5 セーフティ出力機能 (P.6-16)」を参照してください。
コネクション設定（オリジネータ）編集画面に登録されたデバイスに対して、I/O 構成設定を行う手順を以下に示します。

1 コネクション設定（オリジネータ）編集画面でセーフティ I/O ターミナルを選択し、ダブルクリック、または右クリックして［編集］を選択します。

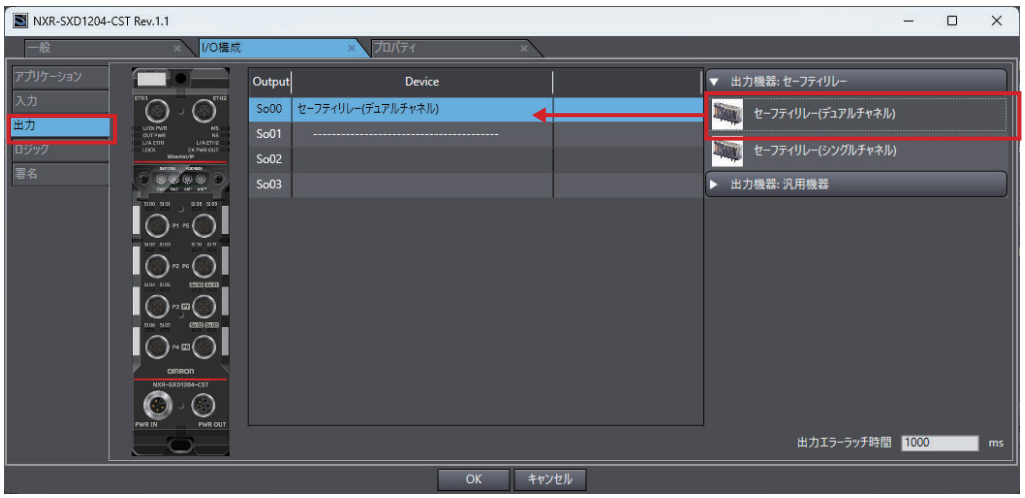


2 ［I/O 構成］タブを選択します。



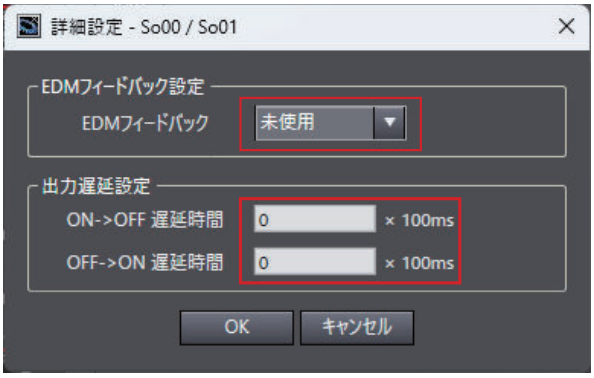
3 **I/O 構成画面から出力機器の登録を行います。安全アプリケーションがリモート I/O モード、ユーザ定義アプリケーションの場合のみ、出力機器の登録ができます。**

左側の［出力］タブを選択し出力機器の登録画面を表示します。右側のツールボックスを展開し、任意のデバイスを指定した端子へドラッグ&ドロップすることにより、出力機器を登録します。

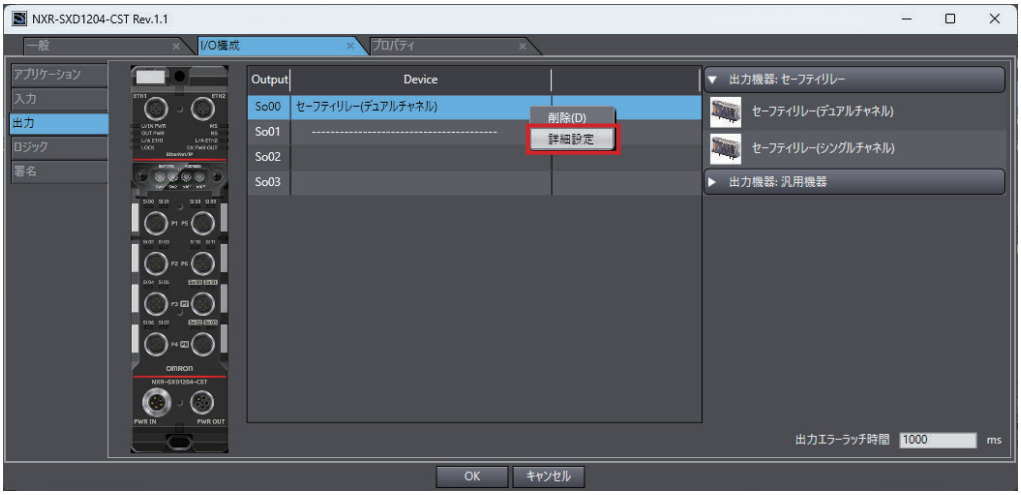


4 **安全アプリケーションがユーザ定義アプリケーションの場合、ドラッグ & ドロップすると［詳細設定］画面が表示され、以下の項目の設定ができます。**

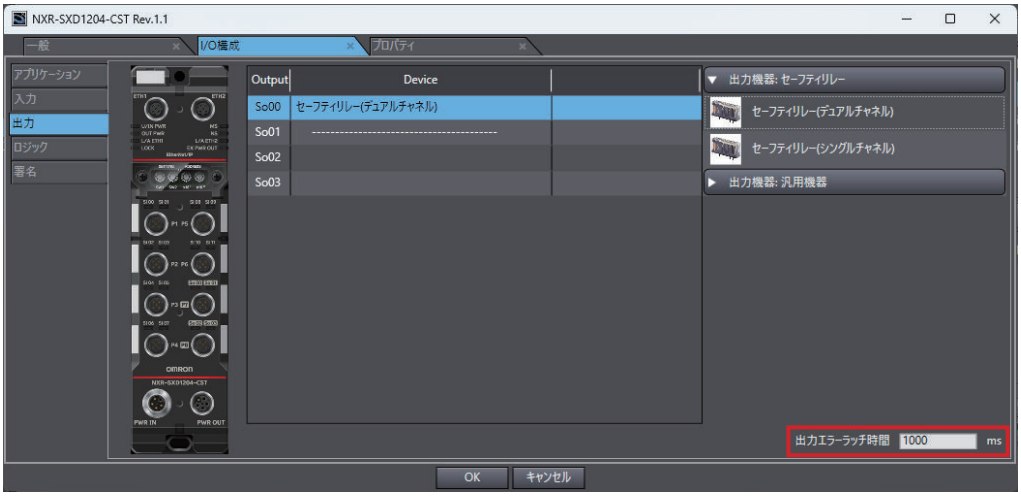
- EDM フィードバック（セーフティ入力機器で［EDM フィードバック］を登録している端子のみ表示します）
- ［ON→OFF 遅延時間］
- ［OFF→ON 遅延時間］



5 安全アプリケーションがユーザ定義アプリケーションの場合、登録した出力機器を選択し、ダブルクリック、もしくは登録した出力機器のコンテキストメニューから［詳細設定］を選択することで、［詳細設定］画面の表示も可能です。



6 必要により、画面右下にある［出力エラーラッチ時間］を設定します。



7 設定が完了したら、［OK］ボタンをクリックします。

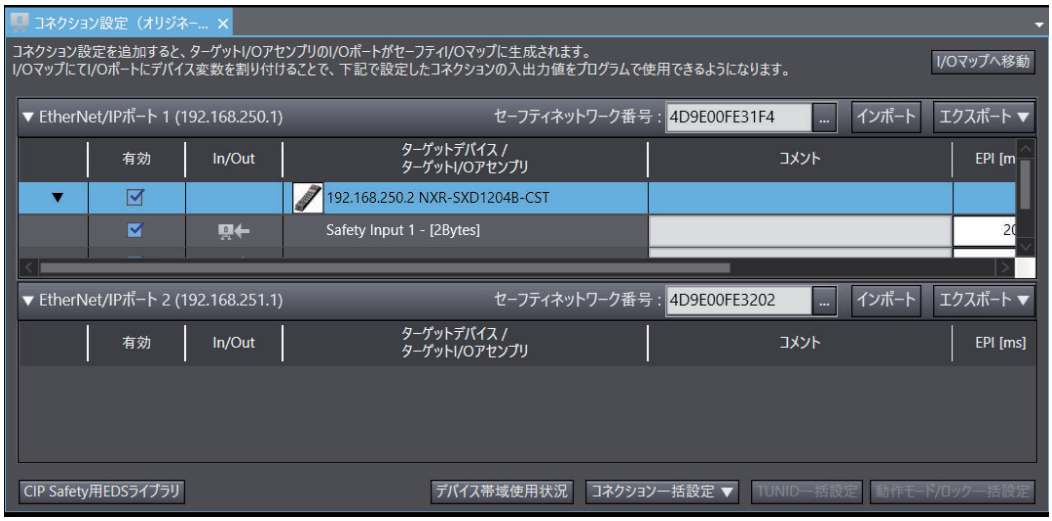
7-7 ロジック機能の設定

ユーザ定義アプリケーション、アドオンアプリケーションでは、ユーザが独自のロジックを設計することができます。ロジック設定には、Sysmac Studio を使用します。

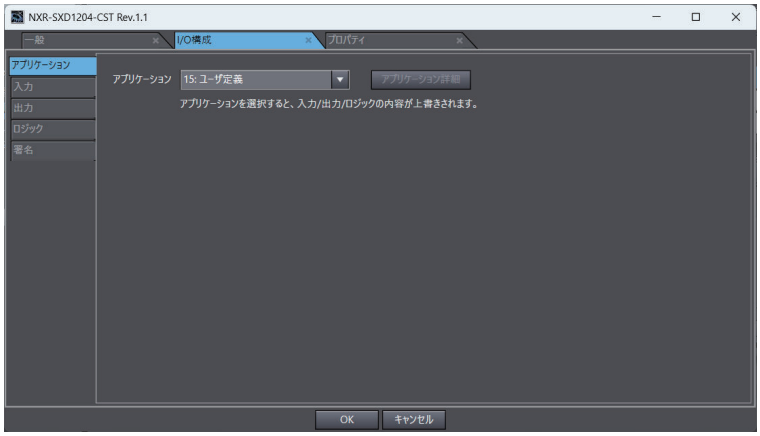
7-7-1 ロジック設定手順

ロジック設定は、セーフティ I/O ターミナルに接続する各ターゲットデバイスおよびターゲット I/O アセンブリの、EtherNet/IP セーフティコネクション設定を行った後に実行します。ここでは、セーフティ入力のデバイス設定はすでに実施済みであるとして説明します。
セーフティ入力のデバイス設定手順の詳細は、「7-5-1 セーフティ入力機能の設定手順 (P.7-42)」を参照してください。
ロジック設定手順は、以下のとおりです。

1 **Sysmac Studio で、セーフティ CPU ユニットの［構成・設定］-［通信］-［セーフティ］-［EtherNet/IP セーフティコネクション設定］ -［コネクション設定（オリジネータ)］を選択します。**
［コネクション設定（オリジネータ)］画面が表示されます。

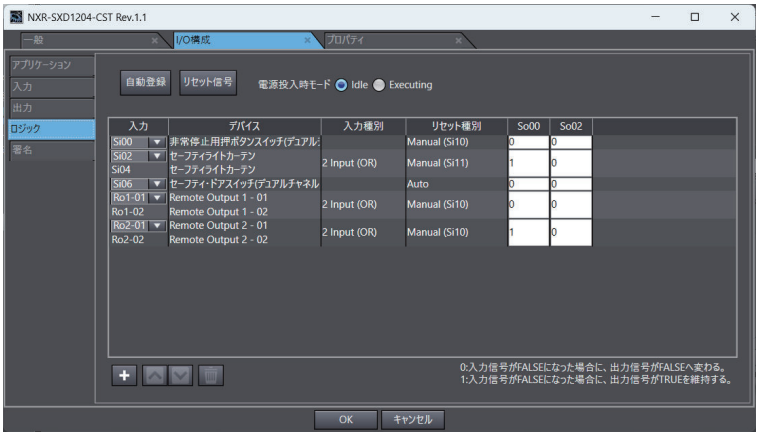


2 **［I/O 構成］タブの［アプリケーション］タブを選択し、アプリケーションを［15: ユーザ定義］に設定します。**



3 **［I/O 構成］タブの［ロジック］タブを選択します。**

以下のロジック設定画面が表示されます。



4 **[自動登録] ボタンを押します。**

デバイスの行が追加されます。また、各行のリセット種別、入力種別、および入力信号の設定が自動で登録されます。自動登録の規則は、以下のとおりです。

項目	自動登録の規則
デバイス	[入力] タブに設定されたデバイスのうち、リセットスイッチと EDM フィードバック以外のものが追加される。
リセット種別	[入力] タブにリセットスイッチが設定されている場合：リセットスイッチが設定されている最小の入力端子番号の Manual リセット [入力] タブにリセットスイッチが設定されていない場合：Auto
入力種別	すべて設定なし
So00-So03	[出力] タブの設定に従って、ロジック設定画面に列が作成される。 値はすべて 0

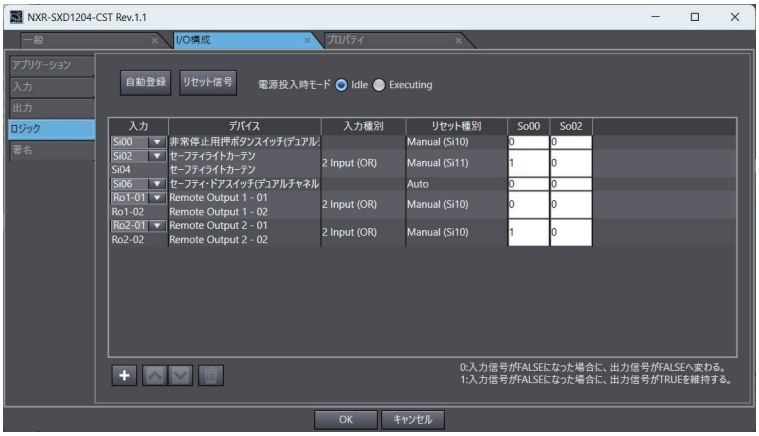
また、リセット信号には、[入力] タブに設定されているリセットスイッチの入力端子番号が、自動登録されます。

5 **この後、リセット信号設定の変更、ロジック設定の変更、リモート出力の設定を行います。**

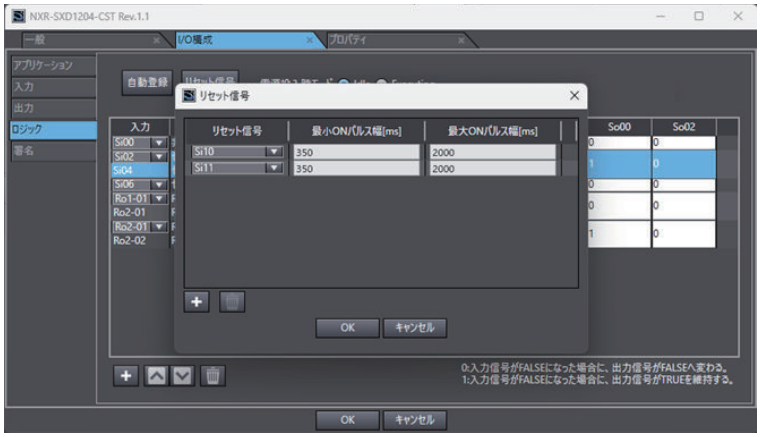
リセット信号設定の変更

必要に応じて、自動登録したリセット信号設定を変更します。

1 **[I/O 構成] タブ、および [ロジック] タブで、[リセット信号] ボタンを押します。**



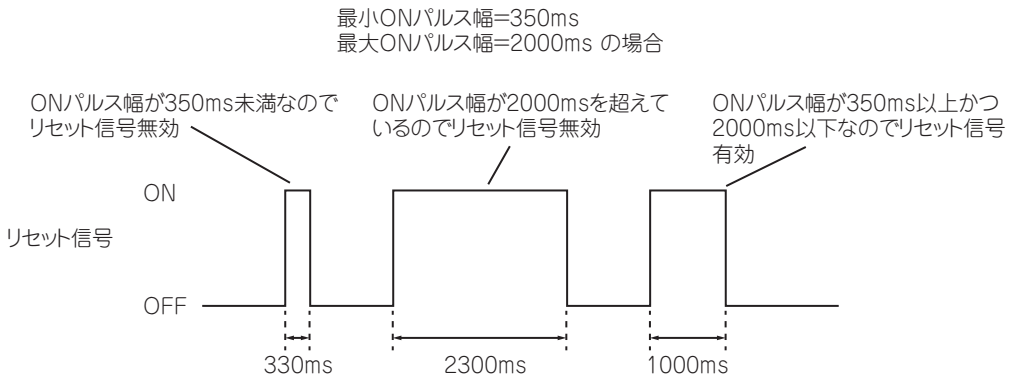
［リセット信号］画面が表示されます。



2 **セーフティ入力端子 Si00 から Si11 のいずれか、またはリモート出力 Ro1-01、Ro1-02、Ro2-01、Ro2-02、Ro3-01、Ro3-02 のいずれかをリセット信号に設定します。**

3 **リセット信号の最小 ON パルス幅と最大 ON パルス幅を設定します。**
リセット信号が ON である時間が、最小 ON パルス幅以上かつ最大 ON パルス幅以下である場合、ロジックのリセットが実行されます。各設定項目の初期値と設定可能範囲は、以下のとおりです。

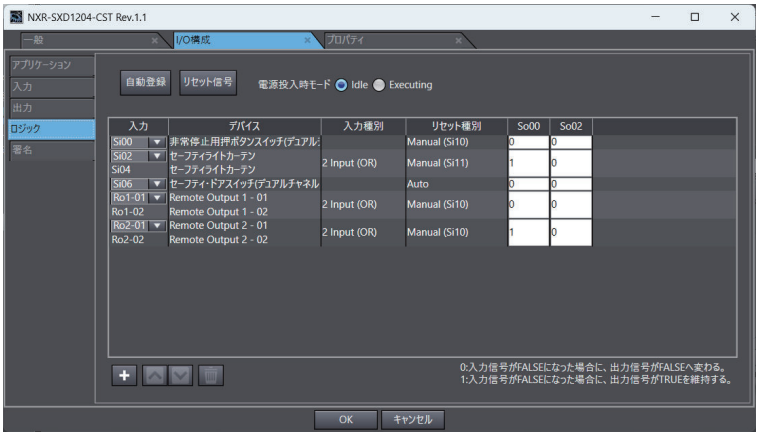
設定項目	初期値[ms]	設定可能範囲[ms]
最小 ON パルス幅	350	100 - 1000 50ms 刻み
最大 ON パルス幅	2000	1000 - 30000 50ms 刻み



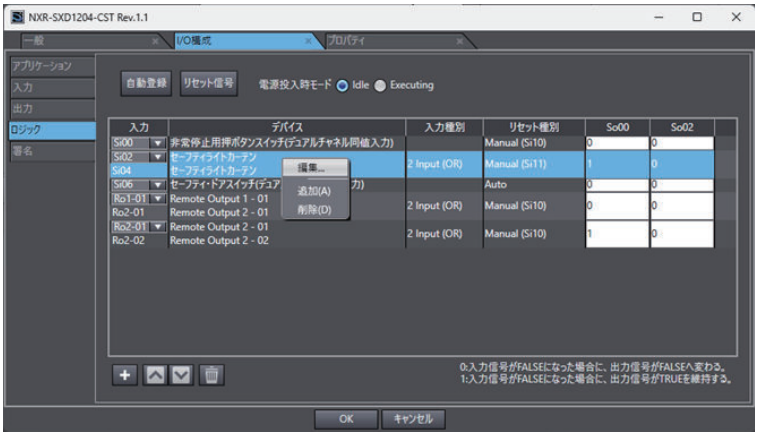
ロジック設定の変更

必要に応じて、各デバイスのロジック設定を変更します。

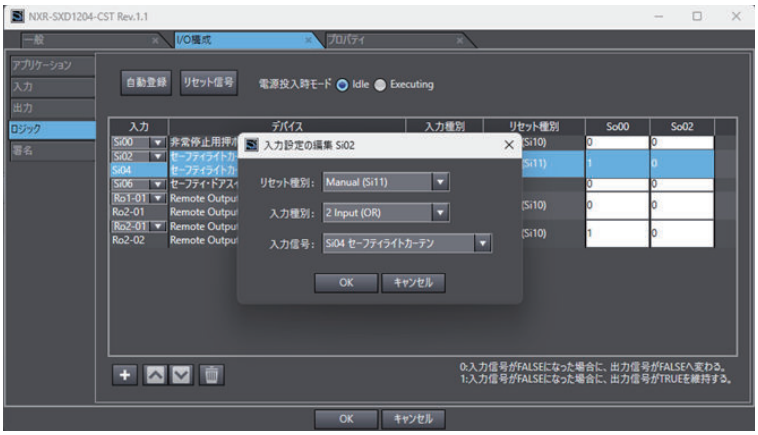
1 **［I/O 構成］タブ、および［ロジック］タブで、設定を変更したいデバイスの行にカーソルを移動し、右クリックします。**



以下のようなサブメニューが表示されます。



2 **[編集] を選択します。**
以下の編集画面が表示されます。



3 **[リセット種別]、[入力種別]、および [入力信号] を設定します。**

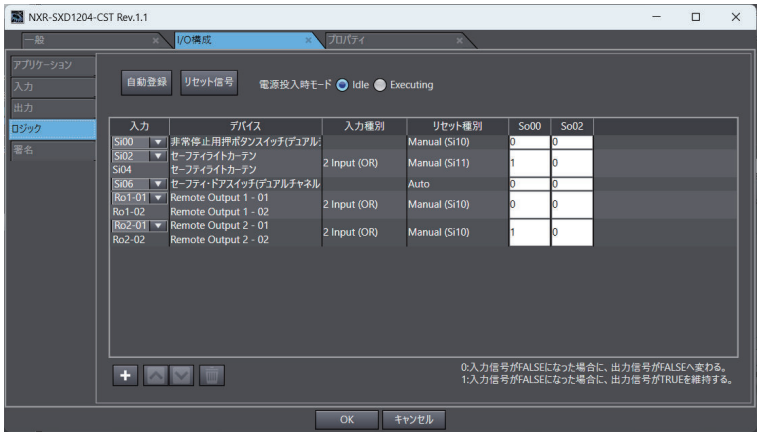
4 **セーフティ出力端子 So00-So03 の欄には、設定値 [0] または [1] を直接入力します。**

5 **行追加する場合は、サブメニューで [追加] を選択します。行削除する場合は、[削除] を選択します。**

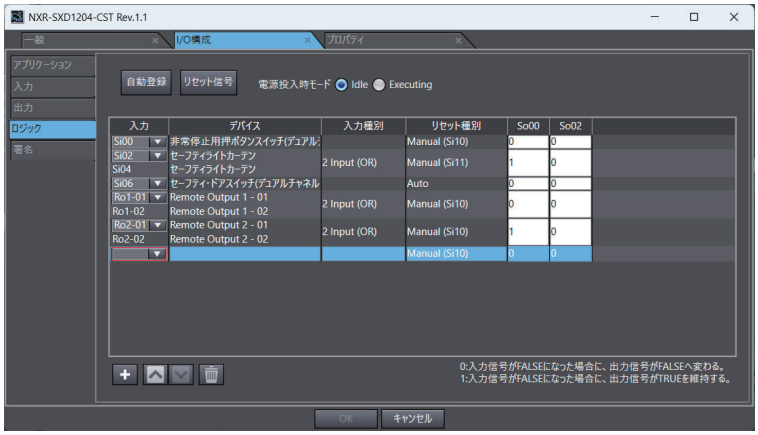
リモート出力の設定

必要に応じて、リモート出力の追加および設定を行います。

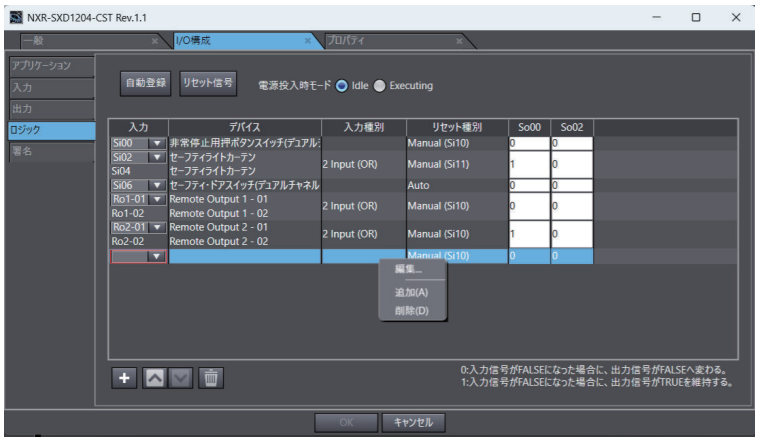
1 **［I/O 構成］タブ、および［ロジック］タブで、［+］ボタンを押します。**



新しい行が追加されます。

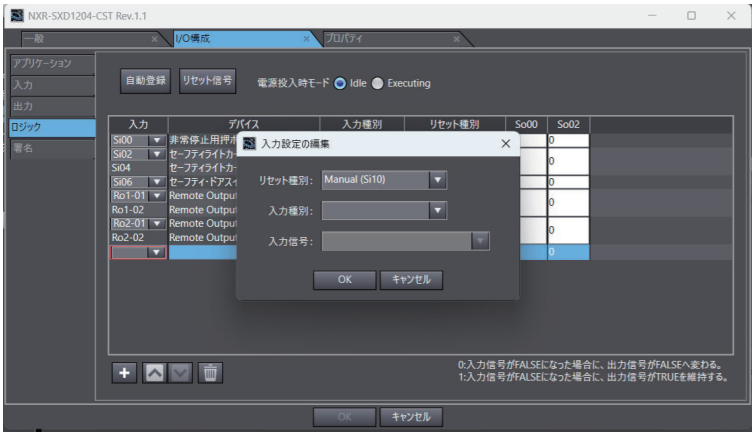


2 **追加した行にカーソルを移動し、右クリックします。**
以下のようなサブメニューが表示されます。



3 **［編集］を選択します。**

以下の編集画面が表示されます。

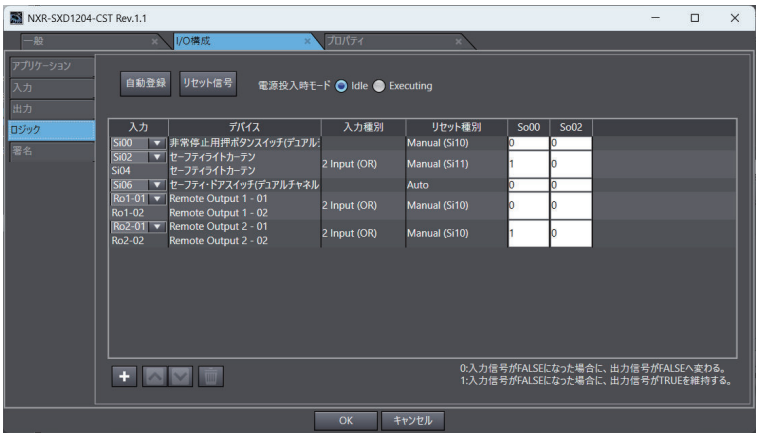


4 **[リセット種別]、[入力種別]、および [入力信号] を設定します。[入力信号] には、[Ro1-01]、[Ro1-02]、[Ro2-01]、[Ro2-02]、[Ro3-01]、[Ro3-02] のいずれかを設定します。**

電源投入時モードの設定

電源投入時の動作モードを設定します。電源投入時の動作モードを［Executing］にすると、電源投入後すぐに安全アプリケーションが動作します。

1 **[I/O 構成] タブ、および [ロジック] タブで、[電源投入時モード] を [Idle] または [Executing] に設定します。**



2 **[OK] ボタンを押します。**

使用上の注意

電源投入時モードを［Idle］にした場合、電源投入時に安全アプリケーションが動作しないため、セーフティ出力が OFF になります。安全アプリケーションを実行するには、セーフティ I/O ターミナルに対して動作モード変更を行い、動作モードを［Executing］にしてください。

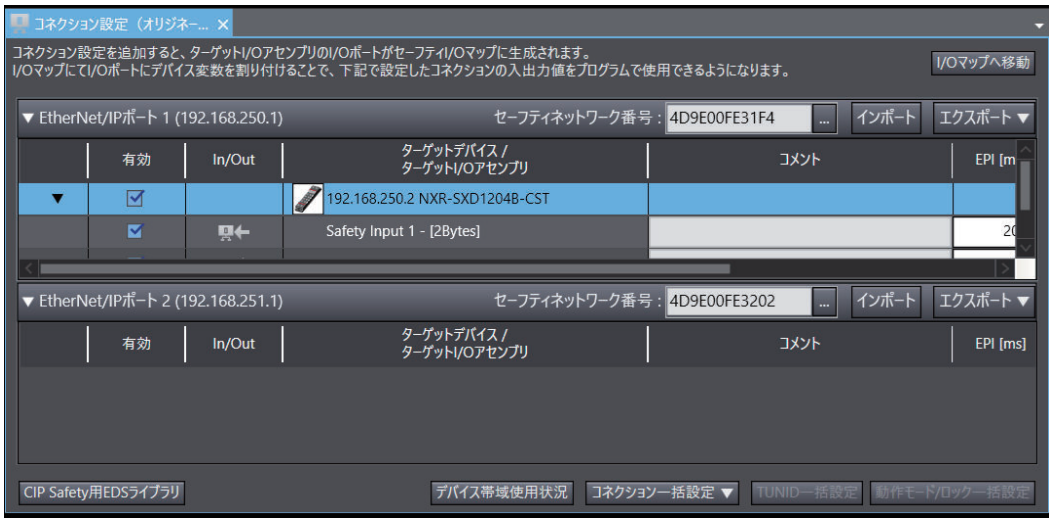
7-7-2 パラメーター覧表示

設定したパラメータの一覧を表示します。各パラメータが意図どおりに設定されていることを確認します。

表示される項目は、以下のとおりです。

項目	内容
パラメータ名	設定パラメータの名称
設定値	設定されている値
設定値（列挙値）	設定値の意味
説明	パラメータ名の意味

1 **Sysmac Studio で、セーフティ CPU ユニットの［構成・設定］-［通信］-［セーフティ］-［EtherNet/IP セーフティコネクション設定］-［コネクション設定（オリジネータ）］を選択します。**
［コネクション設定（オリジネータ）］画面が表示されます。



2 **セーフティ I/O ターミナルをダブルクリック、または右クリックして［パラメーター覧］を選択します。**
パラメーター一覧が表示されます。

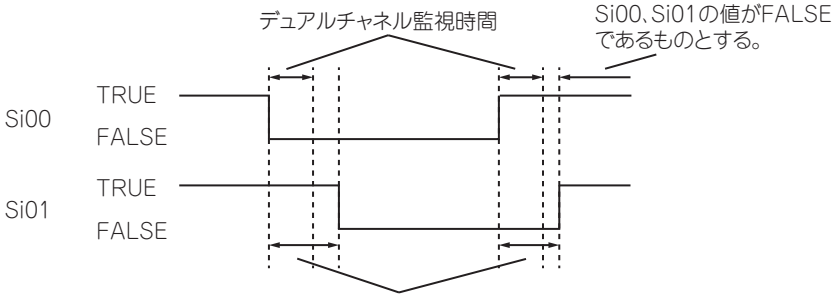


7-7-3 考慮すべき入力デバイスの異常動作の例

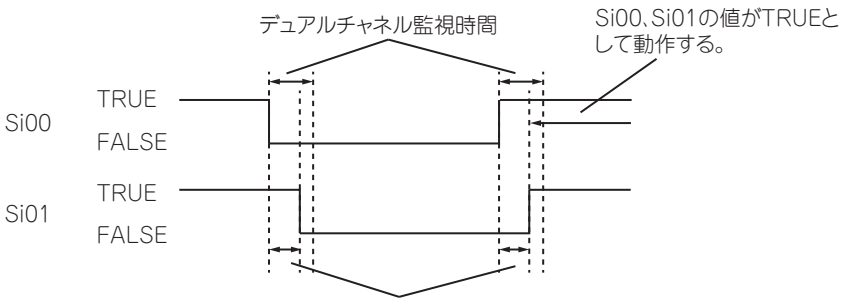
ロジック機能を設定する際、装置を常に安全に動作させるために入力デバイスが予期せぬ異常動作を起こす可能性があることを考慮すべきです。ここでは、入力デバイスの異常動作の例をいくつか示します。

セーフティ入力端子デュアルチャネル監視異常

デュアルチャネル入力デバイスの 2 入力のうち、一方の値が変化してからもう一方の値が変化するまでの時間があらかじめ設定したデュアルチャネル監視時間を超える場合、入力値の変化を正常に検知できないため、「セーフティ入力端子デュアルチャネル監視異常 (65230000Hex)」のイベントが発生します。「セーフティ入力端子デュアルチャネル監視異常(65230000Hex)」のイベントが発生すると、セーフティ入力データの値が FALSE であるものとして動作します。
デュアルチャネル監視時間の詳細は、「6-4-4 デュアルチャネル評価機能 (P.6-11)」を参照してください。
イベントの詳細は、「11-2-4 イベントの内容と対処方法 (P.11-12)」を参照してください。



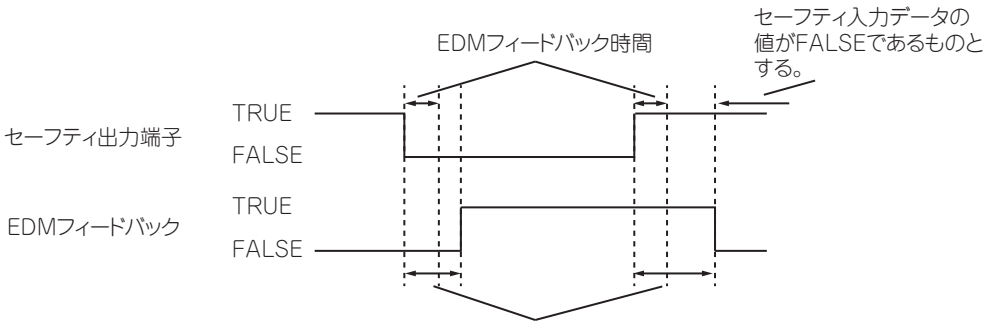
Si00が変化してからSi01が変化するまでの時間が、デュアルチャネル監視時間を超えているので、Si00、Si01の値がTRUEになった後もSi00、Si01の値がFALSEであるものとして動作する。



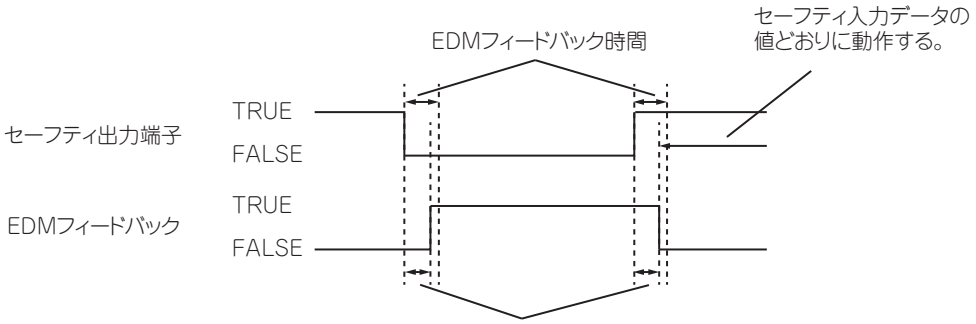
Si00が変化してからSi01が変化するまでの時間が、デュアルチャネル監視時間以内なので、Si00、Si01の値どおりに動作する。

EDM 異常

EDM フィードバックの設定をしている場合、セーフティ出力端子の値が変化してから EDM フィードバックの値が変化するまでの時間が EDM フィードバック時間を超えると「EDM 異常 (652B0000Hex)」のイベントが発生します。「EDM 異常 (652B0000Hex)」のイベントが発生すると、セーフティ入力データの値が FALSE であるものとして動作します。
EDM フィードバックの詳細は、「6-5 セーフティ出力機能 (P.6-16)」を参照してください。また、イベントの詳細は、「11-2-4 イベントの内容と対処方法 (P.11-12)」を参照してください。



セーフティ出力端子の値が変化してからEDMフィードバックの値が
変化するまでの時間が、EDMフィードバック時間を超えているので、
セーフティ入力データの値がFALSEであるものとして動作する。



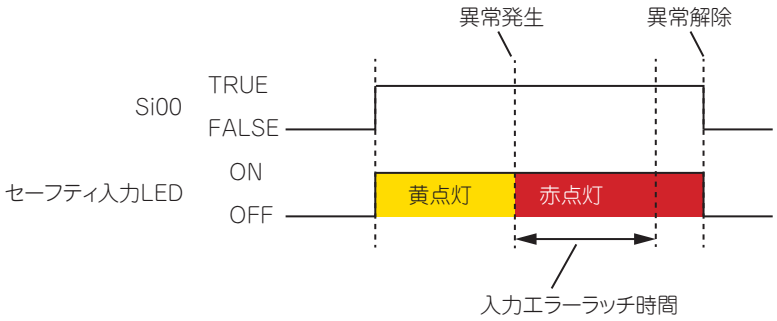
セーフティ出力端子の値が変化してからEDMフィードバックの値が
変化するまでの時間が、EDMフィードバック時間以内なので、
セーフティ入力データの値どおりに動作する。

セーフティ入力端子外部接続機器異常

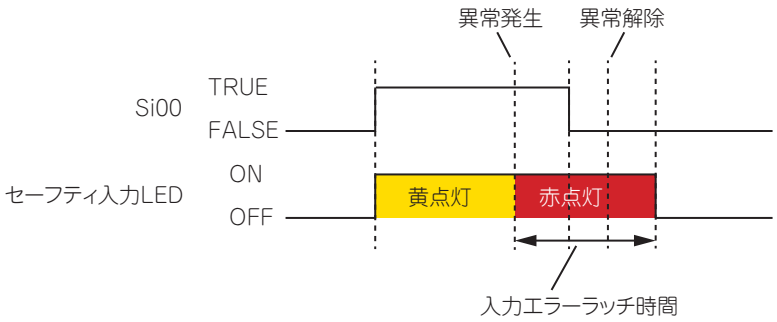
テストパルス評価機能を使用している場合、入力信号線と電源（＋側）との接触、入力信号線間の短絡、および外部接続機器の故障などが発生すると、「セーフティ入力端子外部接続機器異常（65220000Hex)」のイベントが発生します。「セーフティ入力端子外部接続機器異常（65220000Hex)」のイベントが発生すると、セーフティ入力データの値が FALSE であるものとして動作します。
テストパルス評価機能の詳細は、「6-4-3 テストパルス評価機能 (P.6-10)」を参照してください。
イベントの詳細は、「11-2-4 イベントの内容と対処方法 (P.11-12)」を参照してください。

継続時間が入力エラーラッチ時間未満の異常

入力エラーラッチ時間を設定している場合、異常発生から異常解除までの時間が入力エラーラッチ時間未満であったとしても、入力エラーラッチ時間の間は異常処理を継続します。
たとえば、セーフティ入力 LED は、異常が解除された後も入力エラーラッチ時間が終了するまで赤点灯を継続します。
入力エラーラッチ時間の詳細は、「6-4-7 入力エラーラッチ時間 (P.6-14)」を参照してください。



異常発生から異常解除までの時間が入力エラーラッチ時間を超えているので、
異常解除後ただちにセーフティ入力LEDが消灯する。

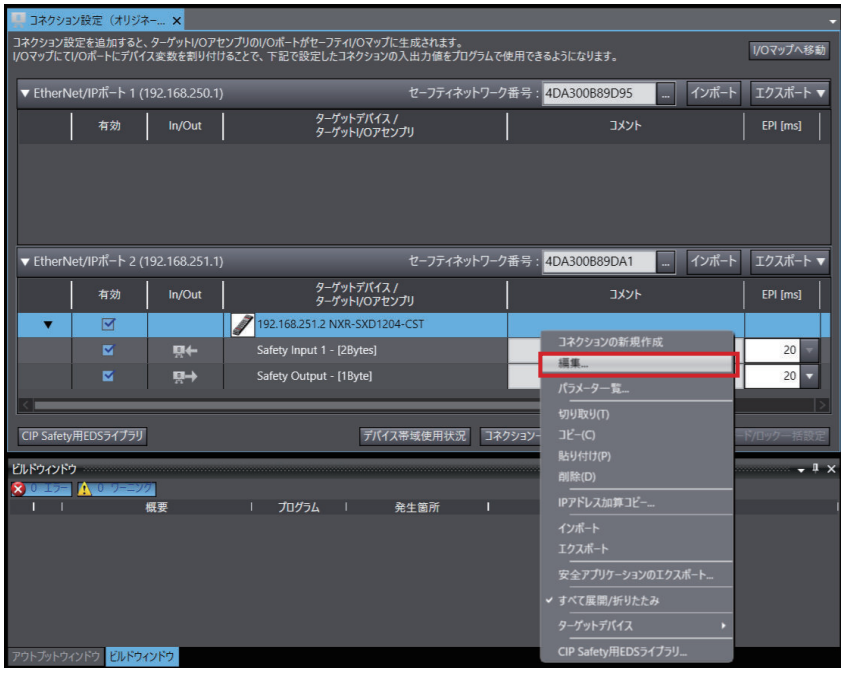


異常が解除されても、入力エラーラッチ時間が終了するまで
セーフティ入力LEDは赤点灯を継続する。

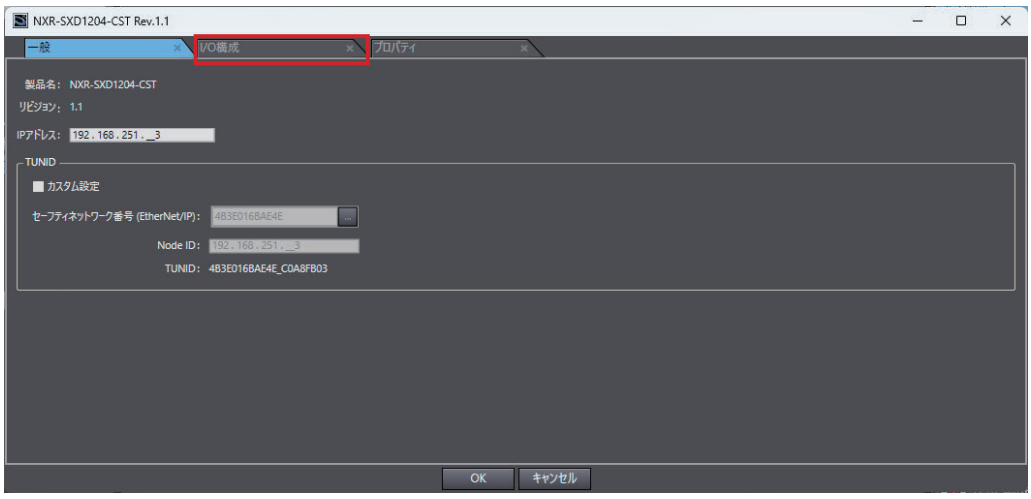
7-8 セーフティ署名の設定

セーフティ I/O ターミナルでセーフティ署名の設定を行います。
Sysmac Studio では、この設定はコネクション設定（オリジネータ）編集画面の中にあるため、コネクション設定（オリジネータ）編集画面から説明します。
なお CIP Safety コネクション設定の詳細については、「7-3-1 CIP Safety 通信のコネクション設定 (P.7-25)」を参照してください。
コネクション設定（オリジネータ）編集画面に登録されたデバイスに対して、使用する安全アプリケーションの設定を行う手順を以下に示します。

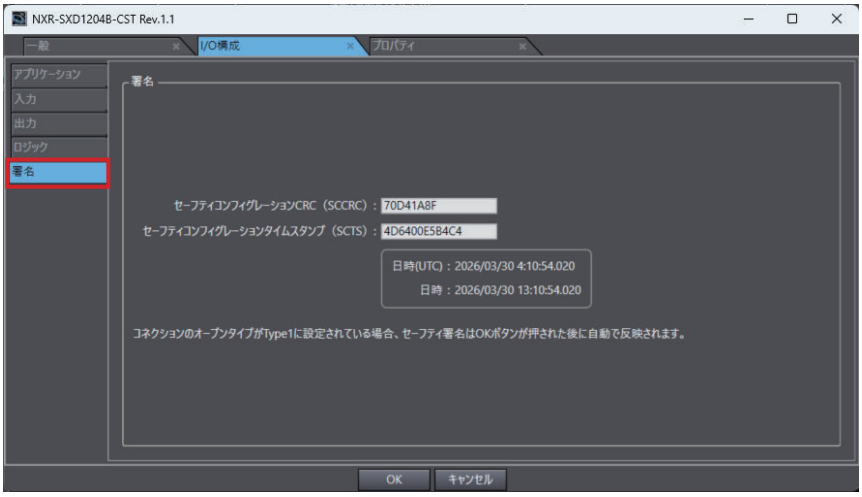
1 **コネクション設定（オリジネータ）編集画面でセーフティ I/O ターミナルを選択し、ダブルクリック、または右クリックして［編集］を選択します。**



2 **［I/O 構成］タブを選択します。**



3 **［署名］タブを選択します。**



4 **セーフティコンフィグレーション CRC（SCCRC)とセーフティコンフィグレーションタイムスタンプ(SCTS)を設定し、［OK］ボタンをクリックします。**

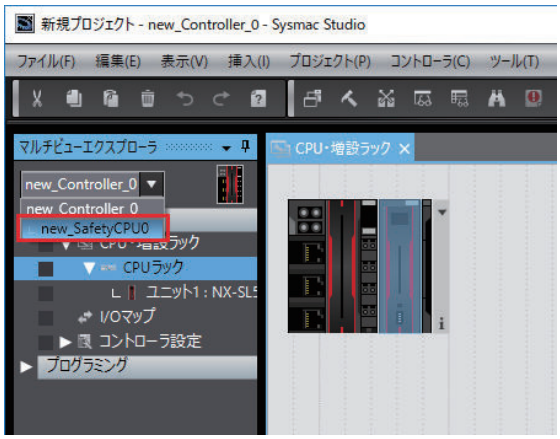
7-9 安全アプリケーションファイルの作成

安全アプリケーションファイルを作成し、エクスポートする手順を説明します。
セーフティコントロールシステムが、「セーフティコントローラが制御する構成（Web UI によるコンフィグレーション）」の場合は、リモート I/O モード用の安全アプリケーションファイルを作成してエクスポートします。この安全アプリケーションファイルは、I/O 構成設定だけを定義します。
セーフティコントロールシステムが、「ユーザが設計した安全アプリケーションで、セーフティ I/O ターミナルが制御する構成（分散管理型）」の場合は、アドオンアプリケーション用の安全アプリケーションファイルを作成してエクスポートします。この安全アプリケーションファイルは、ロジック設定と I/O 構成設定を定義します。

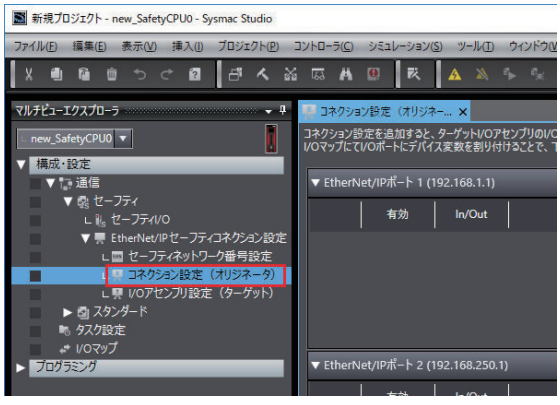
7-9-1 セーフティ I/O ターミナルの登録

安全アプリケーションファイルをエクスポートするために、セーフティ I/O ターミナルを登録します。

1 **マルチビューエクスプローラのコントローラ選択ボックスから、対象となるセーフティ CPU ユニットを選択します。**



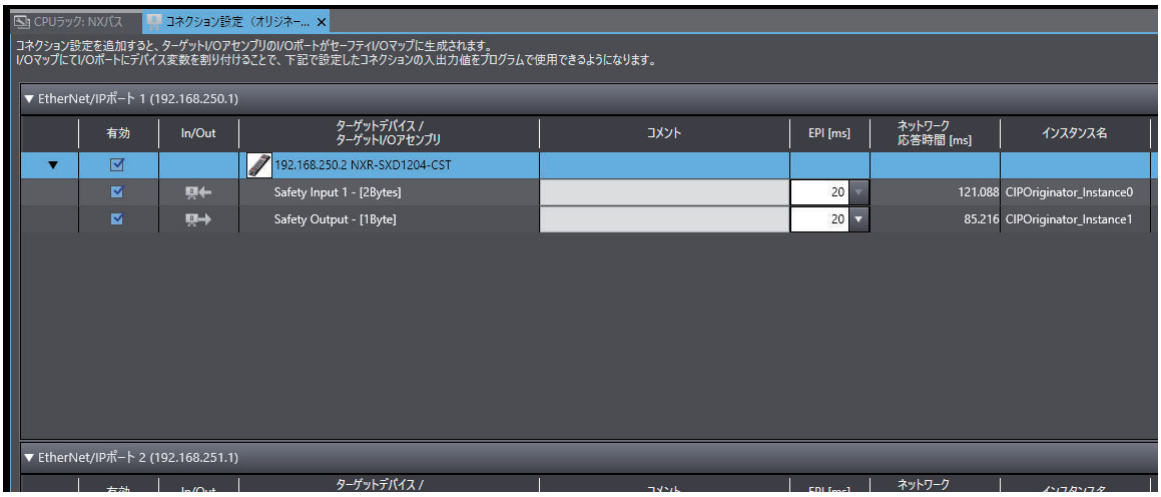
2 **マルチビューエクスプローラの［構成・設定］－［通信］－［セーフティ］－［EtherNet/IP セーフティコネクション設定］－［コネクション設定（オリジネータ）］をダブルクリック、または右クリックして［編集］を選択します。**
エディットウィンドウには、コネクション設定（オリジネータ）編集画面が表示されます。



3 **ツールボックスから［Safety I/O and Logic Device］グループを選択し、［NXR-SXD1204-CST］または［NXR-SXD1204B-CST］を選択します。**



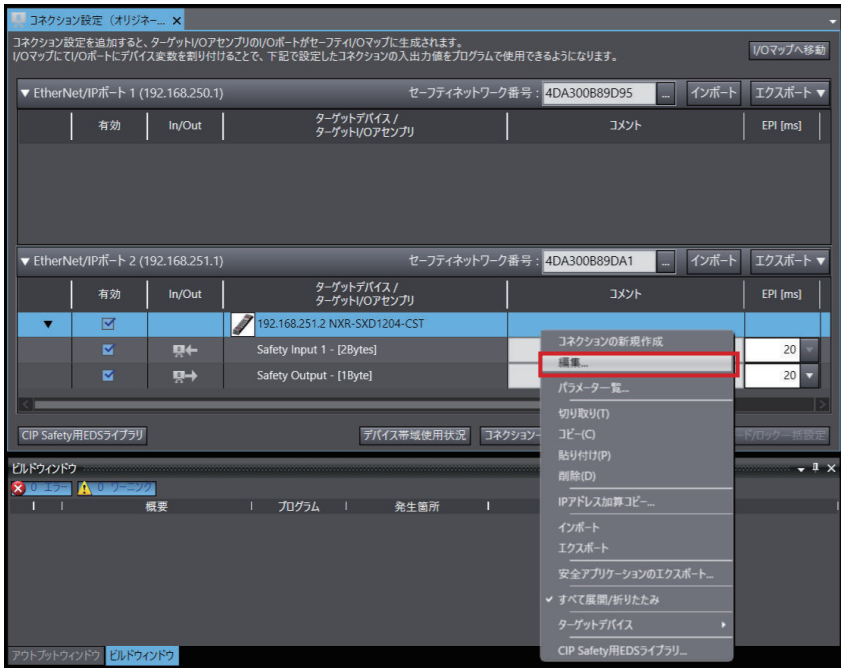
4 **ツールボックスで選択したセーフティ I/O ターミナルをドラッグします。**



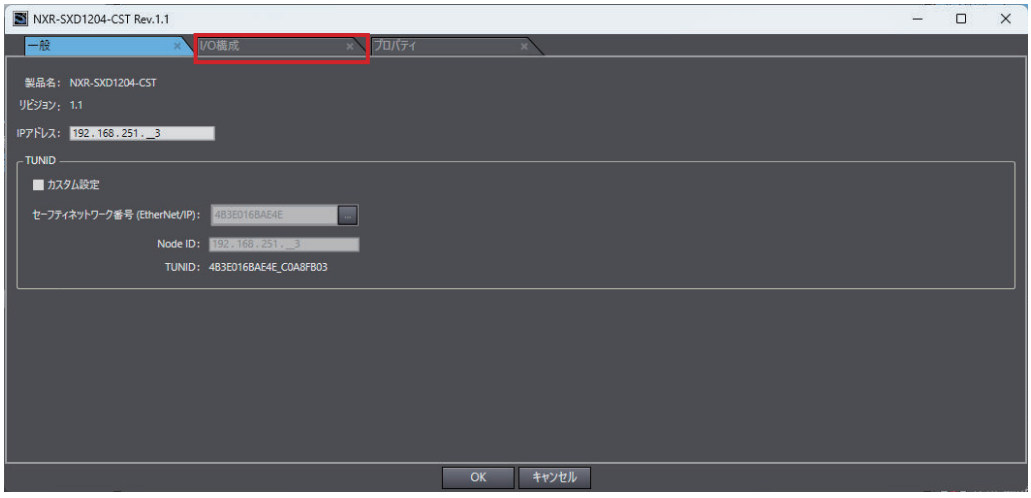
7-9-2 安全アプリケーションの設定

セーフティ I/O ターミナルで使用する安全アプリケーションの設定を行います。

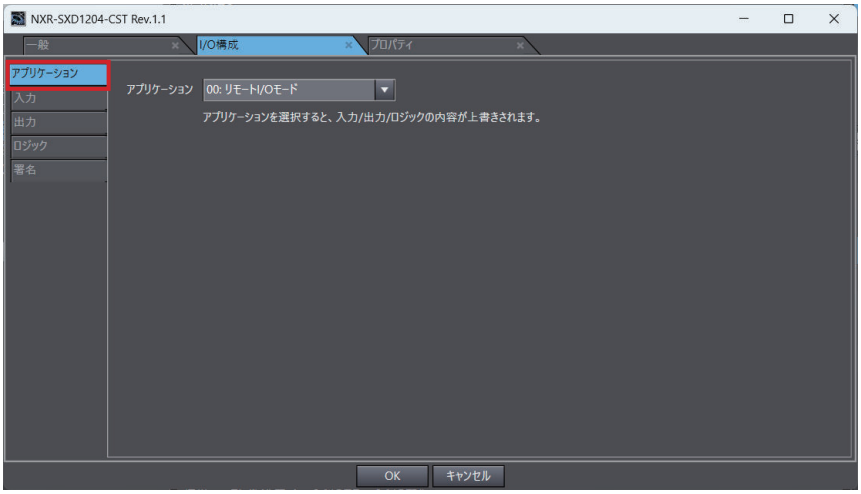
1 **コネクション設定（オリジネータ）編集画面でセーフティ I/O ターミナルを選択し、ダブルクリック、または右クリックして［編集］を選択します。**



2 ［I/O 構成］タブを選択します。



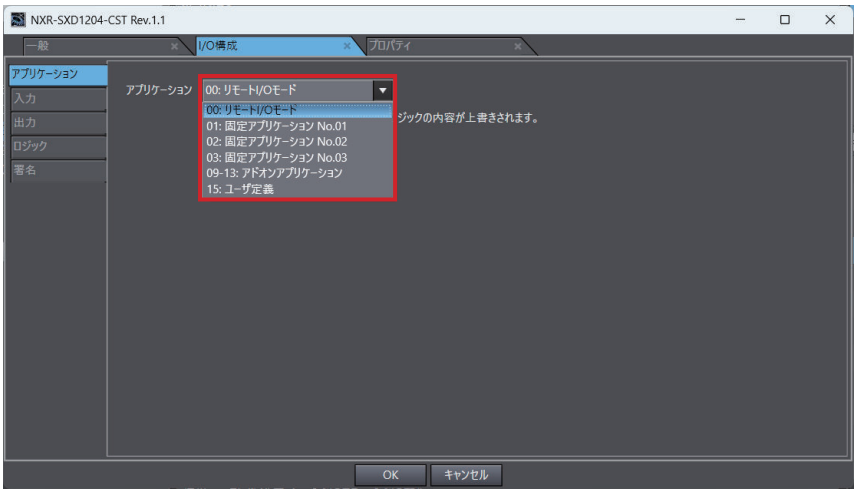
3 ［アプリケーション］タブを選択します。



4 **使用する安全アプリケーションを選択します。**

セーフティコントロールシステムと安全アプリケーションは、以下のように対応しています。

セーフティコントロールシステム	安全アプリケーション
「セーフティコントローラが制御する構成（Type 1 Safety Open によるコンフィグレーション）（P.1-8)」 「セーフティコントローラが制御する構成（Web UI によるコンフィグレーション）（P.1-9)」	00: リモート I/O モード
「プリセットされた安全アプリケーションでセーフティ I/O ターミナルが制御する構成 (P.1-10)」	01: 固定アプリケーション No.01 02: 固定アプリケーション No.02 03: 固定アプリケーション No.03
「ユーザが設計した安全アプリケーションでセーフティ I/O ターミナルが制御する構成（集中管理型）（P.1-11)」	15: ユーザ定義
「ユーザが設計した安全アプリケーションでセーフティ I/O ターミナルが制御する構成（分散管理型）（P.1-12)」	09-13: アドオンアプリケーション



5 **設定が完了したら、[OK] ボタンをクリックします。**

7-9-3 セーフティ入出力機能の設定

Sysmac Studio のプロジェクトファイルで、セーフティ I/O ターミナルの I/O 構成の設定をします。詳細は、「7-5 セーフティ入力機能の設定 (P.7-42)」、「7-6 セーフティ出力機能の設定 (P.7-47)」を参照してください。

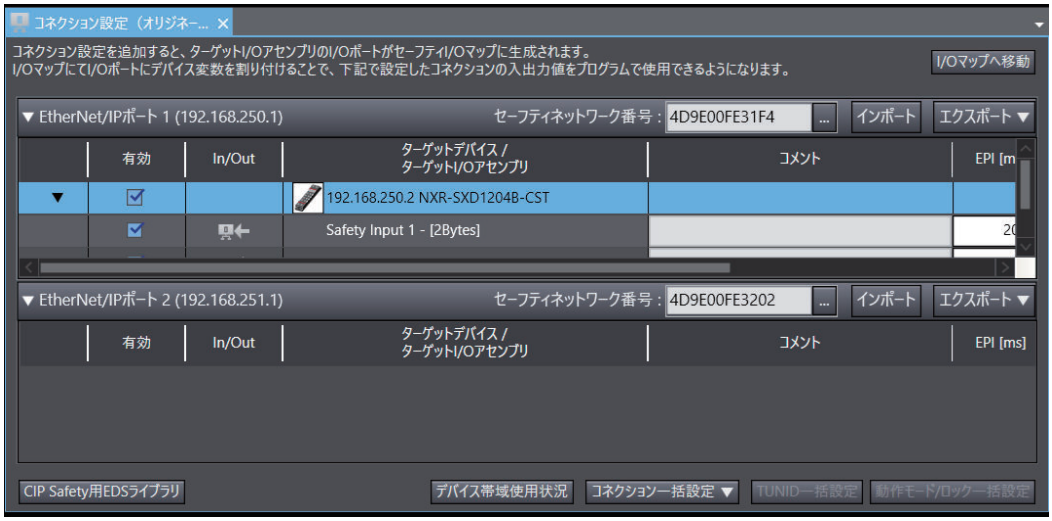
7-9-4 ロジック機能の設定

Sysmac Studio のプロジェクトファイルで、セーフティ I/O ターミナルのロジックと電源投入時モードの設定をします。この手順は、セーフティコントロールシステムが、「ユーザが設計した安全アプリケーションでセーフティ I/O ターミナルが制御する構成（分散管理型）」の場合だけに必要です。詳細は、「7-7 ロジック機能の設定 (P.7-50)」を参照してください。

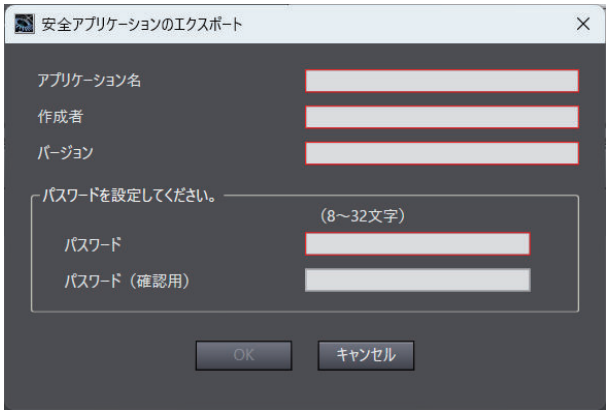
7-9-5 安全アプリケーションファイルのエクスポート

安全アプリケーションファイルのエクスポートの手順は、以下のとおりです。

1 **Sysmac Studio で、セーフティ CPU ユニットの［構成・設定］-［通信］-［セーフティ］-［EtherNet/IP セーフティコネクション設定］-［コネクション設定（オリジネータ）］を選択します。**
［コネクション設定（オリジネータ）］画面が表示されます。



2 **セーフティ I/O ターミナルを右クリックして［安全アプリケーションのエクスポート］を選択します。**
セーフティ I/O ターミナルの［安全アプリケーションのエクスポート］画面が表示されます。



3 **アプリケーション名、作成者、バージョン、安全アプリケーションファイルパスワード、および安全アプリケーションファイルパスワード（確認用）を入力して、［OK］ボタンを押します。**
各設定項目の文字制限は以下のとおりです。

設定項目	文字制限
アプリケーション名	半角英数字 32 文字以下
作成者	半角英数字 32 文字以下
バージョン	半角英数字 32 文字以下
安全アプリケーションファイルパスワード	半角英数字で 8 文字以上 32 文字以下
安全アプリケーションファイルパスワード（確認用）	

安全アプリケーションファイルパスワードは、安全アプリケーションを使用するために安全アプリケーションファイルごとに設定するパスワードです。セーフティパスワードとは異なります。

4 **エクスポートするファイルの保存先を指定して保存します。**
エクスポート完了の画面が表示されます。



5 **セーフティ署名を確認して［OK］ボタンを押します。**
エクスポートが実行され、安全アプリケーションファイルが保存されます。

使用上の注意

入力したアプリケーション名、作成者、バージョン、安全アプリケーションファイルパスワード、およびセーフティ署名（SCCRC と SCTS）は記録しておいてください。安全アプリケーションファイルで安全アプリケーションの設定をする際に使用します。

安全アプリケーションファイルパスワードの仕様

安全アプリケーションファイルパスワードに使用できる文字列の条件は、以下のとおりです。

項目	内容
文字数	8 文字以上 32 文字以下
使用できる文字	A-Z、a-z、0-9、! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { ¦ } ~ 半角スペース

使用上の注意

- セキュリティリスクを下げるため、設定する安全アプリケーションファイルパスワードには、アルファベット、記号、数字のすべてを使用してください。
- 安全アプリケーションファイルパスワードは、表示することも初期化することもできません。忘れないように管理してください。

属性情報の仕様

ユーザが作成するアドオンアプリケーションの属性情報は、以下のとおりです。

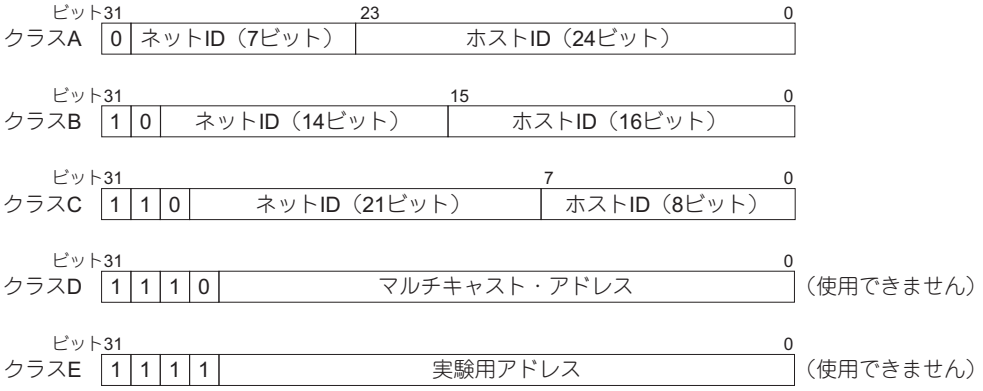
項目	使用できる文字	文字数
アプリケーション名	半角英数字	1 文字以上 32 文字以下
作成者	半角英数字	1 文字以上 32 文字以下
バージョン	半角英数字	1 文字以上 32 文字以下

7-10 IP アドレスの設定

ここでは、IP アドレスの構成や IP アドレスの設定方法について説明します。

7-10-1 IP アドレスの構成

IP アドレスは 32 ビットのバイナリデータで、ネット ID とホスト ID から構成されています。
ネット ID とは Ethernet ネットワークを識別するためのアドレスで、ホスト ID とはホスト（ノード）を識別するためのアドレスです。
IP アドレスは、ネットワークの規模に応じてアドレス体系が選択できるように、クラス A～クラス C の 3 つのクラスに分かれています。クラス D とクラス E は使用できません。



クラスにより、識別できるネットワーク数とホスト数が異なります。

クラス	ネットワーク数	ホスト数
クラス A	小	2^{24}-2 以下（16777214 以下）
クラス B	中	2^{16}-2 以下（65534 以下）
クラス C	大	2^{8}-2 以下（254 以下）

IP アドレスは、32 ビットのバイナリデータを 8 ビットずつの 4 つの組に分け、それぞれをドットで区切った 4 つの 10 進数で表記します。
（例）10000010　00111010　00010001　00100000　→　130.58.17.32

IP アドレスの割り当て

IP アドレスは、ネットワーク内または複数のネットワーク間で重複がないようにノードに割り当てる必要があります。

CIDR 機能

CIDR とは Classless Inter-Domain Routing の略で、クラスを使わない IP アドレスの割り当てを行う機能です。
クラスを使用した IP アドレスでは、ネット ID 部とホスト ID 部が決められたブロック単位で区切られるので、IP アドレス空間（ホスト数）が効率良く割り当てられないデメリットがあります。
CIDR ではクラスを使わないため、ネット ID 部とホスト ID 部を任意の IP アドレス空間で区切ることができ、IP アドレス空間（ホスト数）を効率良く使用することができます。

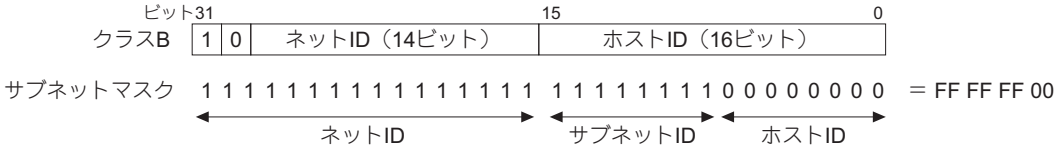
例えば、クラス C（192.168.･･･）を使用しても CIDR によるネットマスク設定をすることで、254 ノードを超える水平分散ネットワークを構築することが可能になります。

サブネットマスク範囲
192.0.0.0～255.255.255.252

サブネットマスク

1 つのネットワークに数多くのノードを接続すると、ネットワークの運用や管理が大変になります。このような場合、1 つのネットワークを複数のサブネットワークに分けてシステムを構築すると便利です。
内部的には複数のネットワークとして運用しますが、外部からは 1 つのネットワークとして見えるようになります。
このような運用を行うためには、IP アドレスのホスト ID 部をサブネット ID 部とホスト ID 部の 2 つに分けて使用します。
このサブネット ID 部を識別するための情報がサブネットマスクです。
サブネットマスクは、ネット ID 部とサブネット ID 部を“1”に、ホスト ID 部を“0”にビットマスクしたものです。

（例）クラス B の IP アドレスで 8 ビットをサブネット ID として使用する場合のサブネットマスクは、以下になります。



サブネットマスクは、そのサブネットワーク上のすべてのノードで共通の値を設定してください。EtherNet/IP 内蔵ポートは、CIDR(Classless Inter-Domain Routing)に対応しているため、サブネットマスクには 192.0.0.0～255.255.255.252 までの値が設定可能です。

参考

サブネットワークを使用しない場合は、IP アドレスのホスト ID 部をすべて“0”でマスクします。
IP アドレスのクラス A～クラス C によって、以下のサブネットマスク値を設定してください。

クラス	サブネットマスク値
クラス A	255.0.0.0
クラス B	255.255.0.0
クラス C	255.255.255.0

ネットワークアドレス

サブネットマスクを利用し、各ネットワークを識別するための情報にネットワークアドレスがあります。
ネットワークアドレスによって、ある複数ノードが同一ネットワークに属するかどうかが分かります。
ネットワークアドレスは、ノードの IP アドレスとサブネットマスクの論理積で算出されます。

次にネットワークアドレスの算出例を示します。
ノード 1 の IP アドレスに“192.168.250.20”、ノード 2 の IP アドレスに“192.168.245.30”、サブネットマスクに“255.255.240.0”と設定すると、それぞれのノードのネットワークアドレスは下記の表のとおりです。
• ノード 1 のネットワークアドレスの算出は、以下になります。

項目	10 進数表記	2 進数表記
IP アドレス	192.168.250.20	11000000.10101000.11111010.00010100
サブネットマスク	255.255.240.0	11111111.11111111.11110000.00000000
ネットワークアドレス	192.168.240.0	11000000.10101000.11110000.00000000

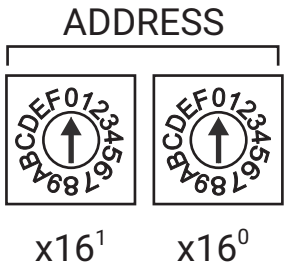
- ノード 2 のネットワークアドレスの算出は、以下になります。

項目	10 進数表記	2 進数表記
IP アドレス	192.168.245.30	11000000.10101000.11110101.00011110
サブネットマスク	255.255.240.0	11111111.11111111.11110000.00000000
ネットワークアドレス	192.168.240.0	11000000.10101000.11110000.00000000

上記より、ノード 1 とノード 2 のネットワークアドレスが同じため、同一ネットワークに属することが分かります。

7-10-2 ロータリスイッチによる IP アドレスの設定方法の選択

セーフティ I/O ターミナルのロータリスイッチで、IP アドレスの設定方法の選択し、IP アドレス自体を設定できます。
ADDRESS のロータリスイッチを使用します。



下記のようにロータリスイッチの設定値で、ソフトウェア設定、ハードウェア設定のいずれかを選択します。選択した方法で IP アドレスを設定します。

設定名	設定値 (Hex)	IP アドレスの設定方法
ソフトウェア設定	00	Sysmac Studio または Web UI で、以下の方法から選択して設定できます。 • 固定 IP アドレスの設定 • DHCP サーバから取得 工場出荷時は、192.168.250.1 になっています。 Sysmac Studio による設定方法は「7-10-3 Sysmac Studio による設定 (P.7-72)」を参照してください。Web UI による設定方法は、「7-10-4 Web UI による設定 (P.7-74)」を参照してください。
ハードウェア設定*2	01～FE	192.168.250.□*1
	FF	DHCP サーバから IP アドレスを取得します。

***1.** “□”には、ロータリスイッチの設定値が入ります。
***2.** ロータリスイッチを設定後、再起動すると設定内容が反映されます。

使用上の注意

DHCP サーバから取得して IP アドレスを設定する場合、DHCP サーバから IP アドレスの取得に成功しても、電源を OFF または再起動すると取得した IP アドレスはクリアされます。よって、以降も DHCP サーバが必要になります。

参考

推奨する DHCP サーバは、DHCP Server 3.06 以降になります。

7-10-3 Sysmac Studio による設定

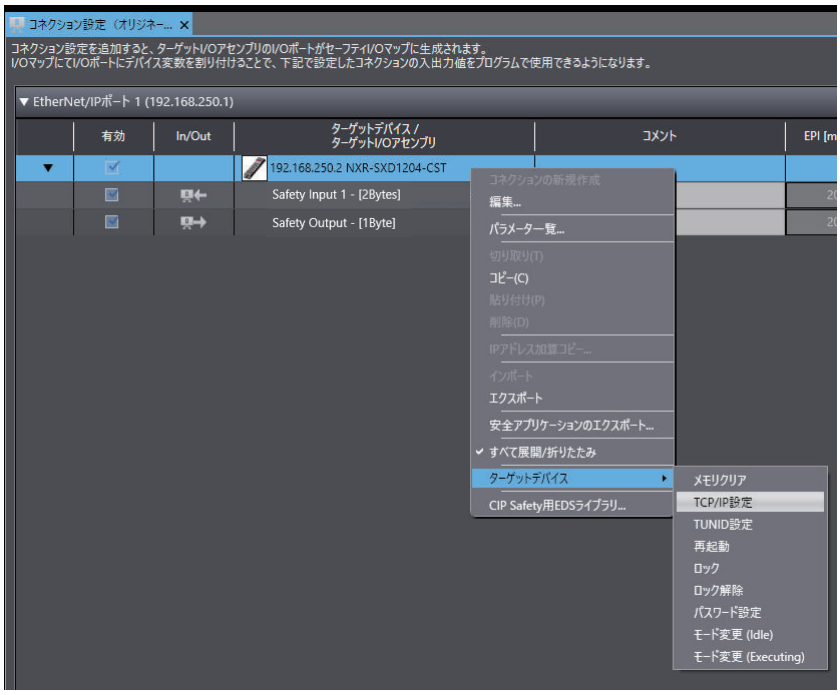
Sysmac Studio の TCP/IP 設定画面で、当該ユニットの IP アドレス設定と LINK 設定を行います。

使用上の注意

本 TCP/IP 設定で、以下の機能をセーフティ I/O ターミナルはサポートしていません。
- ［IP アドレス］の［BOOTP サーバーから取得］
- ［DNS］

1 **ロータリスイッチの ADDRESS の設定値を“00”に設定し、起動します。**
初回起動時は、192.168.250.1 となります。

2 **コネクション設定（オリジネータ）の設定画面で、セーフティ I/O ターミナルを右クリックして表示されるメニューから、［ターゲットデバイス］–［TCP/IP 設定］をクリックします。**



参考

CIP Safety ターゲットデバイス操作画面からも実行可能です。

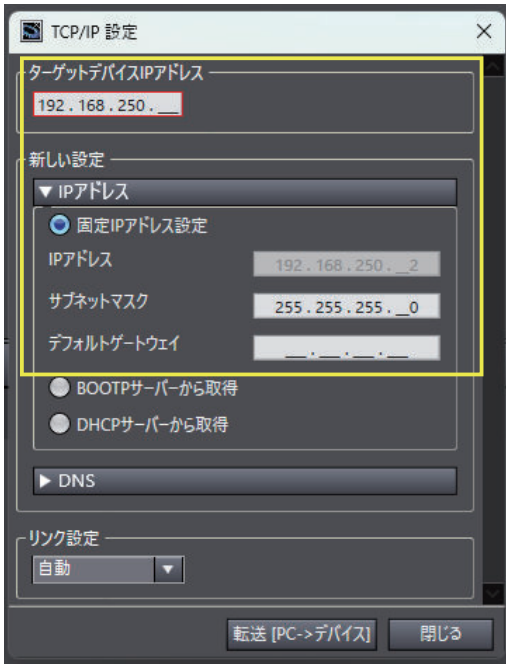
1）マルチビューエクスプローラでセーフティ PLC（初期表示 new_SafetyCPU_0）を選択し、画面上部のメニューバーから、［ツール］-［CIP Safety ターゲットデバイス操作設定］を選択します。

2）［IP アドレス］にセーフティ I/O ターミナルに現在設定されている IP アドレスを入力し、［TCP/IP 設定］ボタンをクリックします。

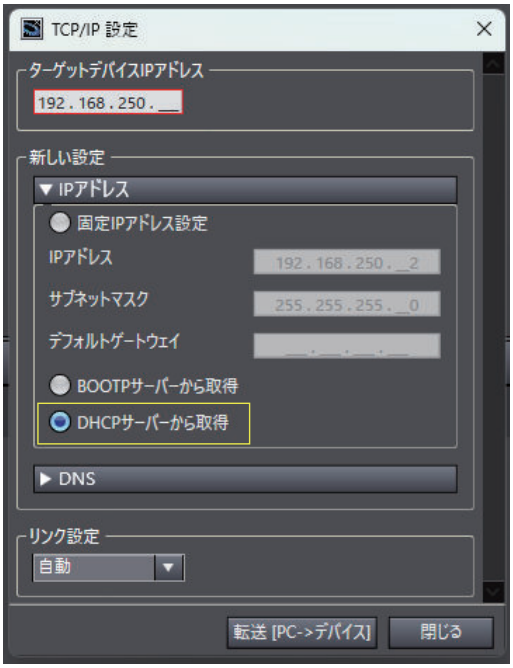


3 **固定 IP アドレスまたは DHCP サーバーから取得のいずれかの方法で IP アドレスを設定します。**

a）固定 IP アドレスの場合、［固定 IP アドレス設定］にチェックを入れて［IP アドレス］の設定を行います。



b）DHCP サーバーから取得の場合、［DHCP サーバーから取得］にチェックします。



4 **[リンク設定] を設定します。**

選択肢は、以下のとおりです。

- Auto
- 10Mbps Half Duplex
- 10Mbps Full Duplex
- 100Mbps Half Duplex
- 100Mbps Full Duplex

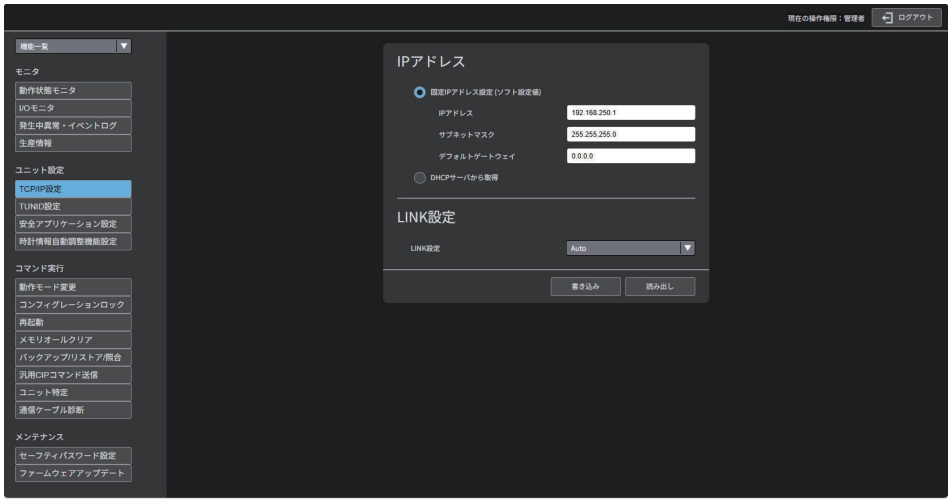
5 **[転送[PC->デバイス]] ボタンをクリックします。**

設定値がセーフティ I/O ターミナルに転送されます。

6 **転送した設定値を有効にするためには、電源再投入または再起動を実行します。**

7-10-4 Web UI による設定

Web UI の TCP/IP 設定画面で、当該ユニットの IP アドレス設定と LINK 設定を行います。
この画面は、管理者の権限を持つユーザだけが設定できます。



設定の手順は、以下のとおりです。

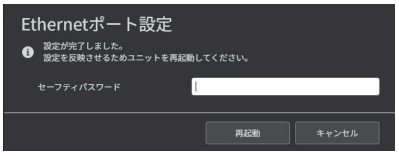
1 **IP アドレスの決定方法を、[固定 IP アドレス設定]、および［DHCP サーバから取得］の中から選択します。**

2 **[固定 IP アドレス設定］を選択した場合、[IP アドレス]、[サブネットマスク]、および［デフォルトゲートウェイ］を入力します。**
［読み出し］ボタンを押すと、現在の IP アドレス、サブネットマスク、およびデフォルトゲートウェイを確認することができます。

3 **[LINK 設定］を設定します。**
選択肢は、以下のとおりです。
- Auto
- 100Mbps Half Duplex
- 100Mbps Full Duplex

［読み出し］ボタンを押すと、現在の LINK 設定を確認することができます。

4 **［書き込み］ボタンを押します。**
設定した内容が当該ユニットに転送されます。転送に成功すると、以下のメッセージが表示されます。



5 **ロータリスイッチの ADDRESS の設定値を“00”に設定してください。**

6 **セーフティパスワードを入力して、[再起動］ボタンを押します。**
セーフティ I/O ターミナルが再起動され、IP アドレス設定と LINK 設定が反映されます。

7-11 TUNID の設定

ここでは、セーフティ I/O ターミナルの TUNID 設定の手順について説明します。

7-11-1 TUNID の目的

TUNID は、CIP Safety 通信において特定のセーフティ接続を識別するために使用されます。
6 バイトのセーフティネットワーク番号(SNN)と 4 バイトのノード ID を組み合わせた、合計 10 バイトの値です。
セーフティネットワーク番号は複数のセーフティネットワークを識別する番号で、ノード ID は EtherNet/IP ネットワーク内の各デバイスを識別する番号です。

7-11-2 TUNID の設定手順

TUNID の設定には、Sysmac Studio を使用する方法、および Web UI を使用する方法があります。

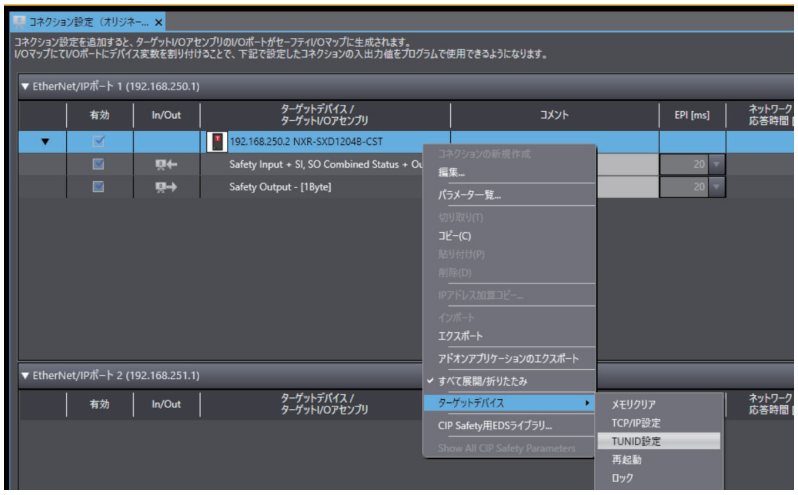
Sysmac Studio による設定

TUNID をユニットを個別設定する方法と一括設定する方法があります。

- **TUNID 設定（個別設定）**

1 **セーフティ CPU ユニットにオンライン接続します。**

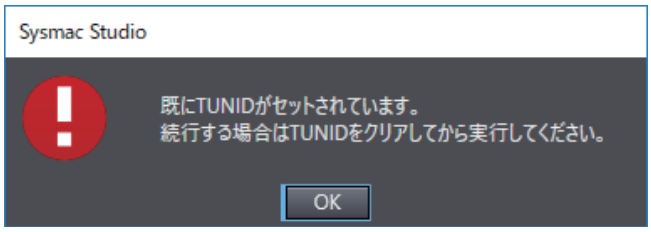
2 **コネクション設定（オリジネータ）編集画面でセーフティ I/O ターミナルを選択し、右クリックして［ターゲットデバイス］–［TUNID 設定］を選択します。**



3 **TUNID 設定に成功したら、［OK］ボタンをクリックします。**



TUNID が既にセットされている場合は、以下の画面が表示されます。



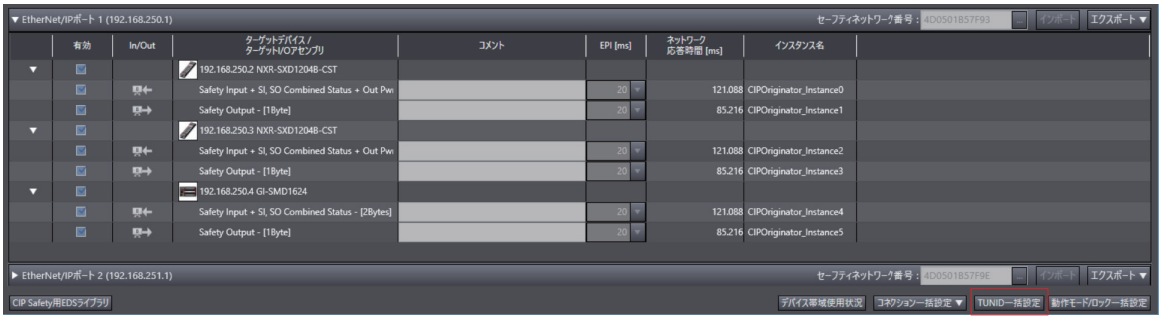
新たに TUNID を設定する場合は、メモリオールクリア機能を使用して、セーフティ I/O ターミナルから TUNID を削除してください。
メモリオールクリア機能の詳細は、「8-2 メモリオールクリア機能 (P.8-4)」を参照してください。

● TUNID 設定（一括設定）

コネクション設定（オリジネータ）編集画面に登録したターゲットに対して、一括で TUNID 設定をすることができます。

1 セーフティ CPU ユニットにオンライン接続します。

2 コネクション設定（オリジネータ）編集画面の右下部にある［TUNID 一括設定］ボタンをクリックします。

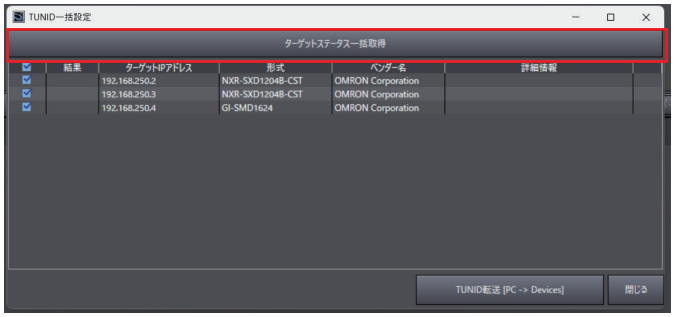


TUNID 一括設定画面が表示されます。



3 **［ターゲットステータス一括取得］ボタンをクリックします。**

一覧表示されたターゲットからステータスを取得し、ターゲットが現在 TUNID 設定可能な状態か否かを判定します。



参考

チェックボックスのチェックを外すことでステータス取得対象から除外することができます。

4 **取得されたステータスを確認します。**

TUNID 設定不可のステータスである場合、チェックボックスのチェックが外れます。

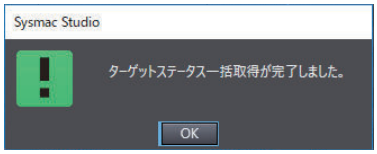


また、詳細列には以下のようなステータス取得結果が表示されます。

- TUNID 設定が可能な場合
  設定可: Waiting for TUNID
- TUNID 設定が不可能な場合
  設定不可: そのデバイスのステータスを表示します。
  ステータス情報は CIP Safety の仕様で定義されたものとなります。
- デバイスと通信できなかった場合
  ターゲットとの通信に失敗しました。

［ターゲットとの通信に失敗しました。］と表示された場合、通信ケーブルの接続状態、ターゲットの IP アドレス設定などを見直してください。
また、設定不可と表示された場合、状況に応じてメモリオールクリア機能を使用してターゲットのステータスを変更してください。

ステータス取得が完了すると、以下のように表示されます。



5 **［TUNID 転送[PC->Devices]］ボタンをクリックします。**

TUNID 一括設定を開始します。



参考

この時にチェックボックスの選択状態を編集する事も可能です。

6 **TUNID 一括設定の結果を確認します。**



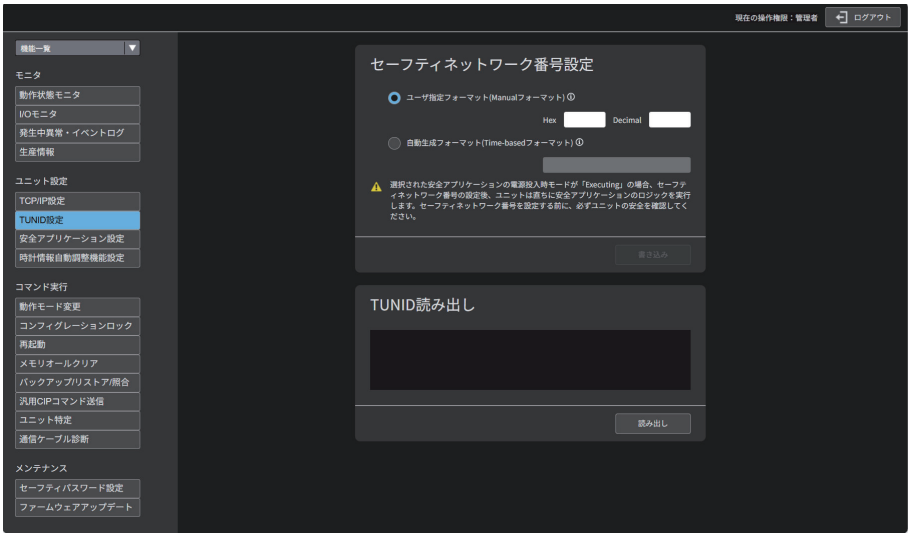
［結果］列には TUNID 設定結果が表示されます。

［結果］列	内容
成功	TUNID の設定が正しく実行されました。
失敗	TUNID の設定が正しく実行できていません。

通信環境を見直すか、既に TUNID が設定されている場合は、メモリオールクリア機能で TUNID をクリア実施後に再度 TUNID 設定を実施してください。

Web UI による設定

Web UI の TUNID 設定画面で、セーフティネットワーク番号を確定させることで、当該ユニットの TUNID が設定を行います。
この画面は、管理者の権限を持つユーザだけが設定できます。



設定の手順は、以下のとおりです。

1 **セーフティネットワーク番号の決定方法を、[ユーザ指定フォーマット（Manual フォーマット)]、[自動生成フォーマット（Time-based フォーマット)] の中から選択します。**
各決定方法の意味と仕様は、以下のとおりです。いずれの方法でも、セーフティ I/O ターミナルが接続されているネットワークのセーフティネットワーク番号を設定してください。

セーフティネットワーク番号決定方法	意味	仕様
ユーザ指定フォーマット（Manual フォーマット）	ユーザが他のシステムと重複しないセーフティネットワーク番号を独自に決めて入力する。	[Hex] 桁数は 4、入力可能文字は 0-9 および大文字の A-F [Decimal] 桁数は 4、入力可能文字は 0-9
自動生成フォーマット（Time-based フォーマット）	ユーザが事前に CIP Safety オリジネータのセーフティネットワークコンフィグレーションツールで自動生成したセーフティネットワーク番号を入力する。	桁数は 4、入力可能文字は 0-9 および大文字の A-F

2 **選択したセーフティネットワーク番号の決定方法に応じて、セーフティネットワーク番号を入力します。**
[読み出し] ボタンを押すと、現在の TUNID、セーフティネットワーク番号、およびノード ID を確認することができます。

3 **[書き込み] ボタンを押します。**
設定した内容が当該ユニットに転送されます。転送に成功すると、以下のメッセージが表示されます。



4 **[OK] ボタンを押します。**

7-12 安全アプリケーションの選択

安全アプリケーションの選択は、ロータリスイッチの SETTING SW1、SW2 で行います。

安全アプリケーションの種類	ロータリスイッチの SETTING SW 1 、SW2
リモート I/O モード用アプリケーション	両方とも「0」
固定アプリケーション	両方とも、使用する固定アプリケーションの番号「1-3」
ユーザ定義アプリケーション	両方とも「F」
アドオンアプリケーション	両方とも、使用するアドオンアプリケーションの番号「9-D」

7-13 再起動

セーフティ I/O ターミナルを再起動させます。

7-13-1 再起動の目的

再起動の目的は、IP アドレスなどの設定や変更を有効にすることです。

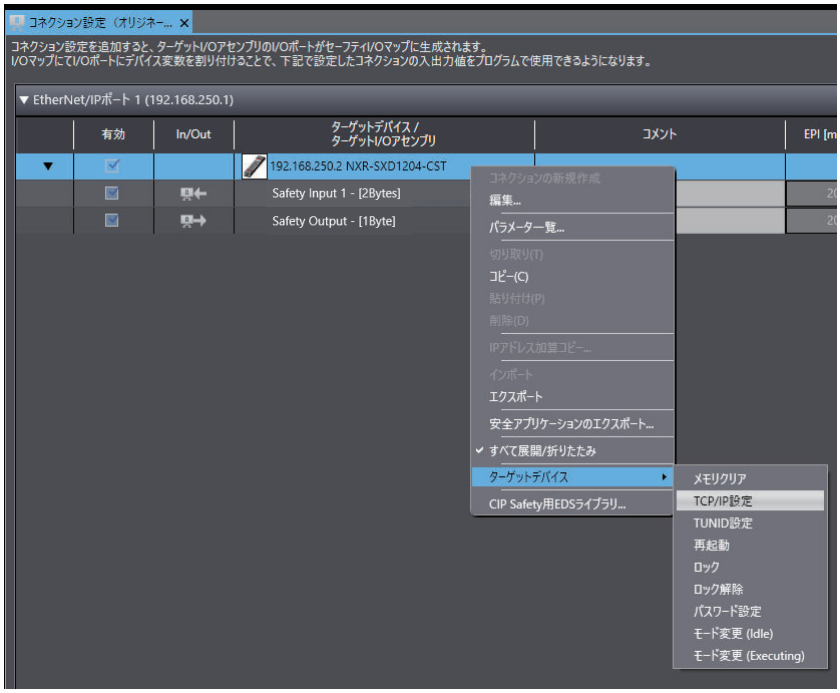
7-13-2 再起動の使用手順

再起動には、Sysmac Studio を使用する方法、および Web UI を使用する方法があります。

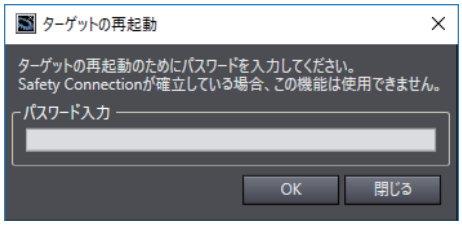
Sysmac Studio での使用手順

Sysmac Studio での手順は、以下のとおりです。

1 **コネクション設定（オリジネータ）の設定画面で、セーフティ I/O ターミナルを右クリックして表示されるメニューから、[ターゲットデバイス] をクリックします。**



2 **[再起動] をクリックします。**
以下の画面が表示されます。



3 **セーフティパスワードを入力して、[OK] ボタンを押します。**
再起動が実行されます。

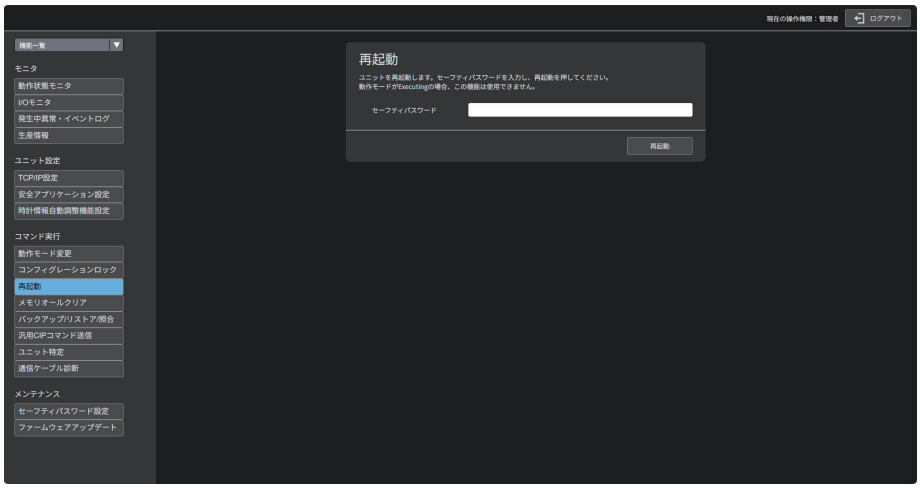
参考

CIP Safety ターゲットデバイス操作画面からも実行可能です。
1）マルチビューエクスプローラでセーフティ PLC（初期表示 new_SafetyCPU_0）を選択し、画面上部のメニューバーから、[ツール] - [CIP Safety ターゲットデバイス操作設定] を選択します。
2）[IP アドレス] にセーフティ I/O ターミナルの IP アドレスを入力します。



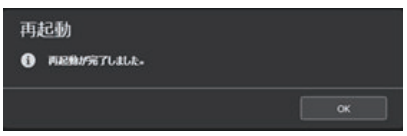
Web UI での使用手順

Web UI の再起動画面で、セーフティ I/O ターミナルを再起動します。
この画面は、管理者の権限を持つユーザだけが設定できます。



設定の手順は、以下のとおりです。

1 **セーフティパスワードを入力して、[再起動] ボタンを押します。**
再起動が実行され、以下の画面が表示されます。



2 **[OK] ボタンを押します。**
Web UI からログアウトし、ログイン画面が表示されます。

7-14 コンフィグレーション

セーフティコントローラとセーフティ I/O ターミナルをコンフィグレーションする手順を説明します。
セーフティコントローラのコンフィグレーションについての詳細は、『NX シリーズ セーフティコントロールユニット／通信コントロールユニット ユーザーズマニュアル(SGFM-723)』を参照してください。
セーフティ I/O ターミナルは安全アプリケーションファイルを使用し、Web UI の安全アプリケーション設定画面でコンフィグレーションします。

7-14-1 セーフティコントローラのコンフィグレーション

セーフティコントローラのコンフィグレーションを行います。

1 **Sysmac Studio で作成したリモート I/O モード用アプリケーションを、セーフティコントローラに転送します。**
セーフティ I/O ターミナルのオープンタイプが「type1 Safety open」の場合、セーフティコントローラとセーフティ I/O ターミナル間の Type1Safety Open コネクションが確立する際に、セーフティ I/O ターミナルはセーフティコントローラによってコンフィグレーションされます。

7-14-2 セーフティ I/O ターミナルのコンフィグレーション

安全アプリケーションファイルで、安全アプリケーションを設定する手順を説明します。安全アプリケーションは、ロータリスイッチの番号に割り付けて使用します。安全アプリケーションファイルを誤ってセーフティ I/O ターミナルにダウンロードした場合は安全アプリケーションをロータリスイッチの番号から削除してください。

ロータリスイッチで選択した安全アプリケーションのコンフィグレーション

ロータリスイッチで選択した安全アプリケーションをコンフィグレーションする手順は、以下のとおりです。

1 **Sysmac Studio で作成した安全アプリケーションファイルを準備します。**

2 **パソコンをセーフティ I/O ターミナルの EtherNet/IP ポートに接続して、Web UI にログインします。**

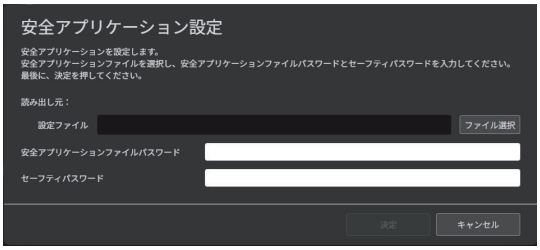
3 **Web UI の安全アプリケーション設定画面を表示します。この画面は、管理者の権限を持つユーザだけが設定できます。**



使用上の注意

リモート I/O モード用アプリケーションの安全アプリケーションファイルは、アドオンアプリケーションとしてコンフィグレーションできません。また、アドオンアプリケーションの安全アプリケーションファイルは、リモート I/O モード用アプリケーションとしてコンフィグレーションできません。

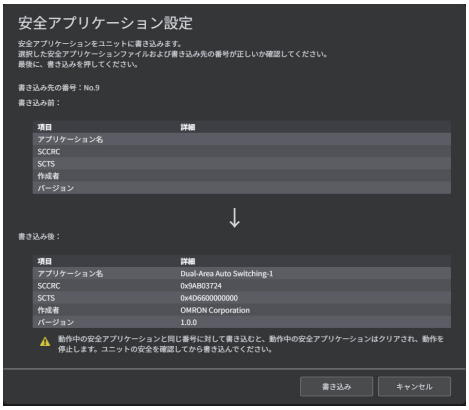
4 **アドオンアプリケーションを割り付けるロータリスイッチの番号の［設定］ボタンを押します。**
以下のメッセージが表示されます。



5 **［ファイル選択］ボタンを押して、パソコン内の安全アプリケーションファイルを選択します。**
［設定ファイル］欄に、選択した安全アプリケーションファイルが表示されます。

6 **安全アプリケーションファイルパスワードとセーフティパスワードを入力します。**

7 **［決定］ボタンを押します。**
以下のメッセージが表示されます。



使用上の注意

安全アプリケーション設定画面に表示される SCCRC と SCTS が、意図どおりであることを確認してください。

8 **読み出し元および書き込み先の表示内容を確認して［書き込み］ボタンを押します。**
設定がセーフティ I/O ターミナルに反映され、以下のメッセージが表示されます。



9 **アドオンアプリケーションを動作させる場合は、電源を OFF、ロータリスイッチの設定、電源 ON を実行します。**

ロータリスイッチの番号からの削除

アドオンアプリケーションをロータリスイッチの番号から削除する手順は、以下のとおりです。

1 **Web UI の安全アプリケーション設定画面で、アドオンアプリケーションを削除するロータリスイッチの番号の［削除］ボタンを押します。**
以下のメッセージが表示されます。



2 **削除元の表示内容を確認し、セーフティパスワードを入力して［削除］ボタンを押します。**
アドオンアプリケーションがロータリスイッチの番号から削除され、以下のメッセージが表示されます。



7-15 時計情報自動調整機能の設定

時計情報自動調整機能は、当該ユニットの時刻を合わせるための機能です。

7-15-1 時計情報自動調整機能の目的

時計情報自動調整機能の目的は、イベントログに正しい日時が記録されるようにすることです。
本機能は、セーフティ I/O ターミナルの時計情報を自動で調整するものです。正確な時刻が記録されることで、異常発生のタイミングを正確に把握でき、迅速な対応や原因分析に役立ちます。

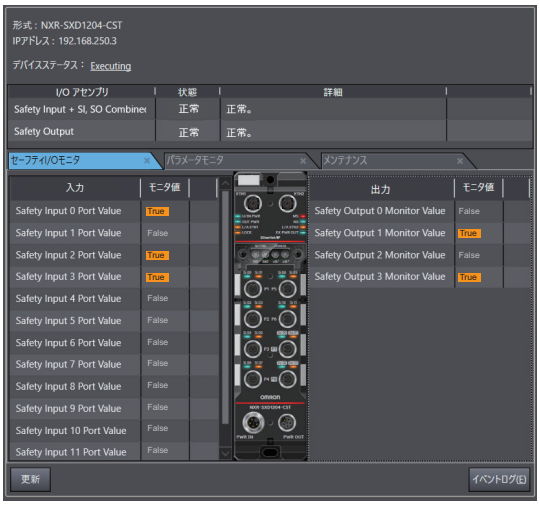
7-15-2 時計情報自動調整機能の使用手順

時計情報自動調整機能には、Sysmac Studio を使用する方法、Web UI を使用する方法、および Explicit メッセージ通信を使用する方法があります。

Sysmac Studio での使用手順

Sysmac Studio での手順は、以下のとおりです。

1 **Sysmac Studio の CIP Safety モニタ画面で、セーフティ I/O ターミナルを選択します。**
以下の画面が表示されます。



2 **［メンテナンス］タブを選択します。**
以下の画面が表示されます。



3 **[SNTP 設定] のラジオボタンで [有効] を選択します。**

4 **[SNTP 設定] の [IP アドレス] に、NTP サーバまたは SNTP サーバの IP アドレスを設定します。**

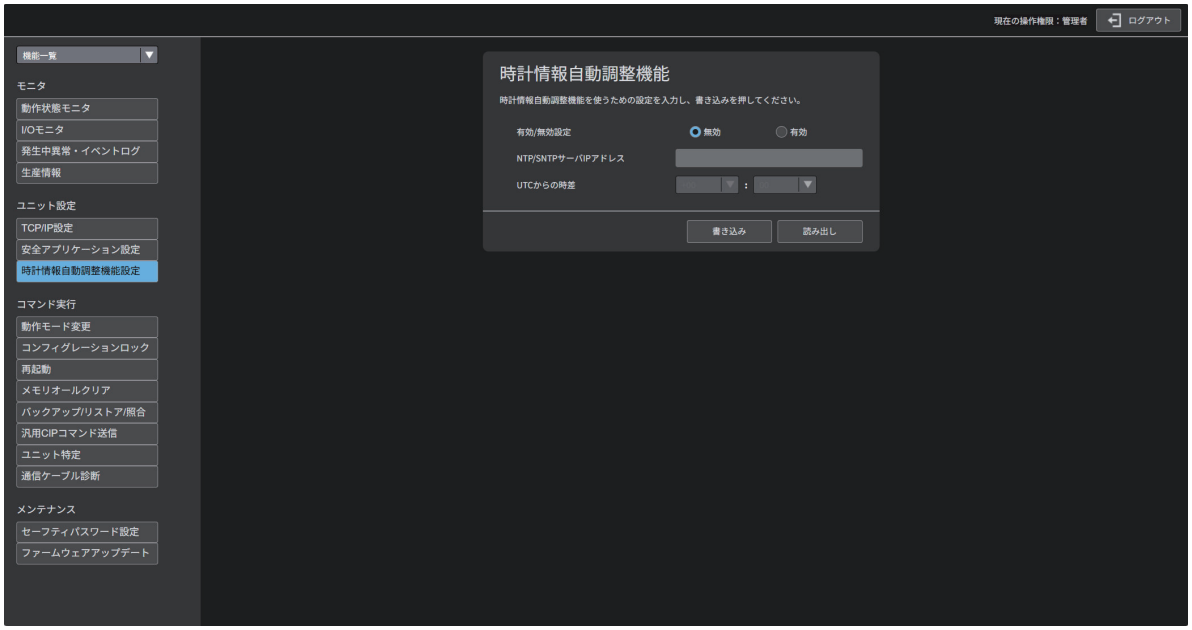
5 **[タイムゾーン] で、設定するタイムゾーンを選択します。**

6 **[設定] をクリックします。**

7 **ユニットをリスタートします。**
ユニットに内蔵されている時計に、NTP サーバまたは SNTP サーバから取得した日時が設定されます。

Web UI での使用手順

Web UI の時計情報自動調整機能設定画面で、セーフティ I/O ターミナルの時刻合わせをします。
この画面は、管理者の権限を持つユーザだけが設定できます。

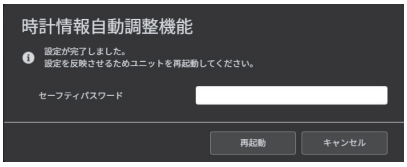


設定の手順は、以下のとおりです。

1 **［有効／無効設定］を［有効］に設定します。**

2 **［NTP/SNTP サーバ IP アドレス］に、NTP/SNTP サーバの IP アドレスを入力します。［UTC からの時差］に、UTC（協定世界時）からの時差を設定します。**

3 **［書き込み］ボタンを押します。**
設定した内容が当該ユニットに転送されます。転送に成功すると、以下のメッセージが表示されます。



4 **セーフティパスワードを入力して、［再起動］ボタンを押します。**
セーフティ I/O ターミナルが再起動され、時刻設定が反映されます。

Explicit メッセージ通信での使用手順

NTP/SNTP サーバの IP アドレス設定およびタイムゾーン設定のための送信コマンドは、以下のとおりです。

実施内容	送信コマンドの項目	送信コマンドの値
SNTP サーバの IP アドレス設定	サービスコード	10Hex(Set_Attribute_Single)
	クラス ID	380Hex(Unit Manager オブジェクト)
	インスタンス ID	01Hex（インスタンス指定）
	アトリビュート ID	12(SNTP Server IP Address)
	サービスデータ	SNTP サーバの IP アドレス
現在時刻を修正するための分単位のオフセット	サービスコード	10Hex(Set_Attribute_Single)
	クラス ID	380Hex（Unit Manager オブジェクト）
	インスタンス ID	01Hex（インスタンス指定）
	アトリビュート ID	102(Time Zone Offset - Minutes)
	サービスデータ	-720～840

CIP オブジェクトへの Explicit メッセージによるアクセス方法は、「Explicit メッセージサーバ機能 (P.6-6)」を参照してください。

7-15-3 時計情報自動調整機能の詳細

ユニットの時刻情報は、電源断によりクリアされます。
時計情報の自動調整は定期的に行われますが、調整タイミングを任意に設定することはできません。
サマータイムには対応していません。

NTP サーバまたは SNTP サーバとの接続に失敗した場合、「NTP サーバ接続失敗」(84040000Hex)のイベントが発生します。詳細は、「11-2-4 イベントの内容と対処方法 (P.11-12)」を参照してください。

使用上の注意

- 時計情報自動調整機能を使用していない場合、ユニット内部の時計は電源投入時に 1972 年 1 月 1 日午前 0 時 0 分 0 秒に設定され、そこから計時されます。
- セキュリティリスクを下げるために、時計情報自動調整機能を必ず実行してください。

7-16 動作モードの変更

セーフティ I/O ターミナルの動作モードを、「Idle」、または「Executing」に変更します。
動作モードの詳細は、「6-8 動作モード (P.6-47)」を参照してください。

7-16-1 動作モード変更の使用手順

動作モード変更には、Sysmac Studio を使用する方法と Web UI を使用する方法があります。

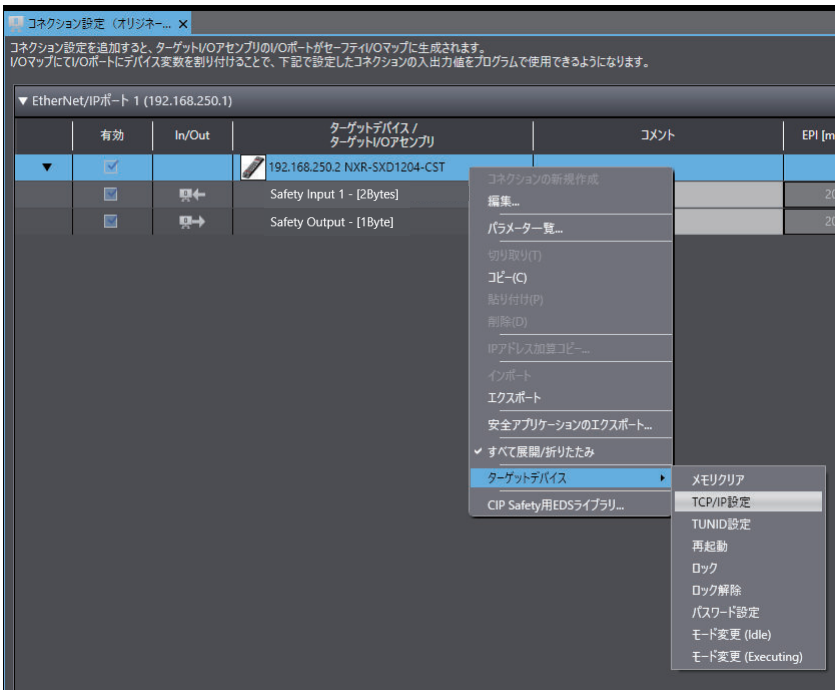
Sysmac Studio での使用手順

Sysmac Studio では、ユニット個別に動作モードを変更する方法と、CIP Safety コネクション設定画面に登録されている複数ユニットの動作モードを一括で変更する方法があります。

● ユニット個別での変更

ユニット個別での変更の使用手順は、以下のとおりです。

1 **コネクション設定（オリジネータ）の設定画面で、セーフティ I/O ターミナルを右クリックして表示されるメニューから、［ターゲットデバイス］をクリックします。**



2 **［モード変更(Idle)］または［モード変更(Executing)］をクリックします。**

3 **セーフティパスワード入力画面が表示されるので、セーフティパスワードを入力します。**



4 **［OK］ボタンを押します。**
動作モードが変更されます。

参考

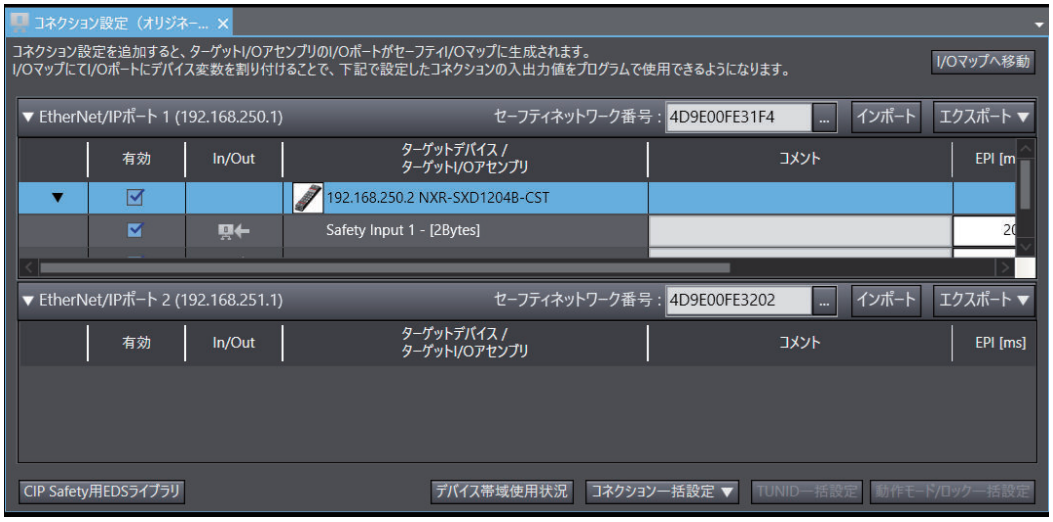
CIP Safety ターゲットデバイス操作画面からも実行可能です。
1）マルチビューエクスプローラでセーフティ PLC（初期表示 new_SafetyCPU_0）を選択し、画面上部のメニューバーから、［ツール］-［CIP Safety ターゲットデバイス操作設定］を選択します。
2）［IP アドレス］にセーフティ I/O ターミナルの IP アドレスを入力します。



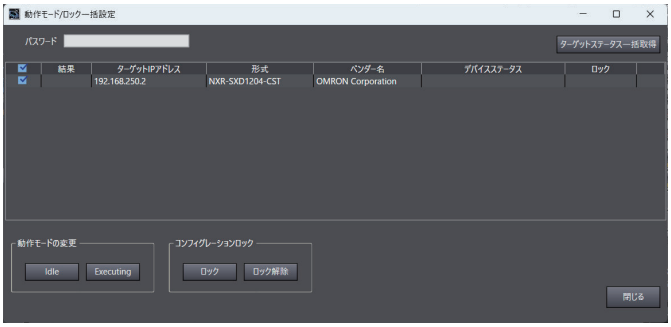
● 複数ユニット一括での変更

複数ユニット一括での変更の使用手順は、以下のとおりです。

1 **Sysmac Studio で、コネクション設定（オリジネータ）の設定画面を表示します。**

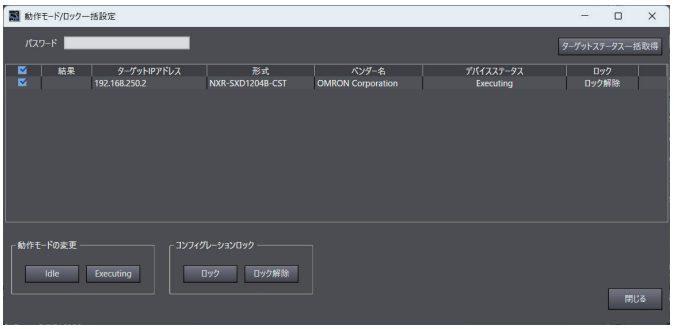


2 **［動作モード／ロック一括設定］ボタンを押します。**
以下の画面が表示されます。



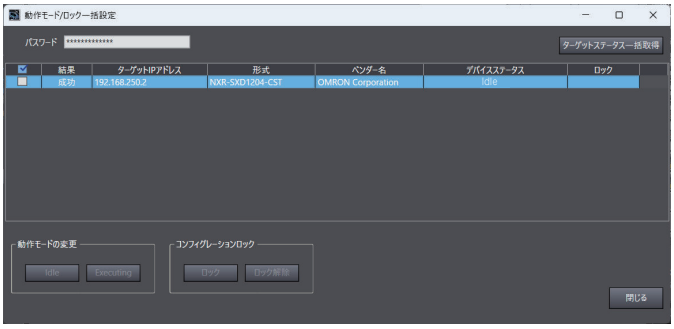
3 **［ターゲットステータス一括取得］ボタンを押します。**

以下のように、［デバイスステータス］欄に、各ターゲットのデバイスステータスが表示されます。「デバイスステータス」は、「動作モード」と同じ意味です。



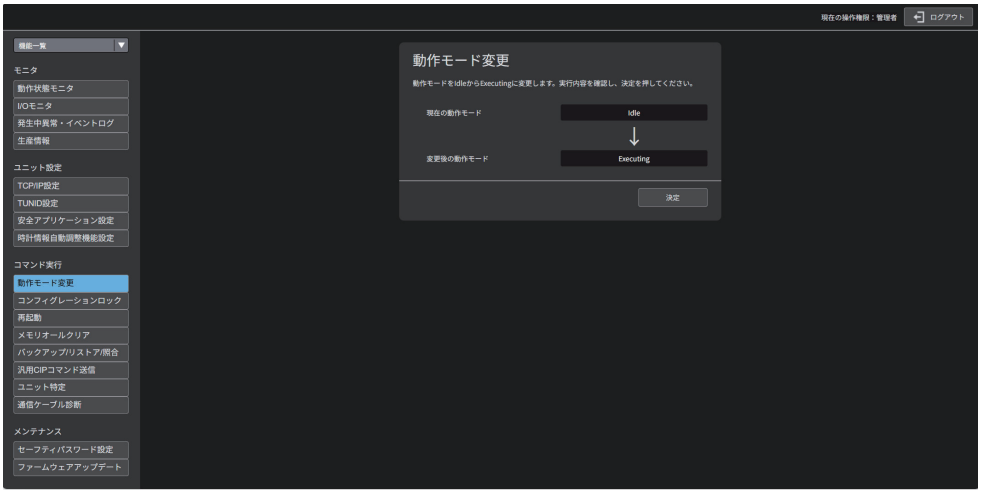
4 **セーフティパスワードを入力し、［動作モードの変更］の［Idle］ボタン、または［Executing］ボタンを押します。**

複数のユニットの動作モードが一括に変更されます。以下のように、［結果］欄に各ターゲットの動作モード変更が成功したか失敗したかが表示されます。



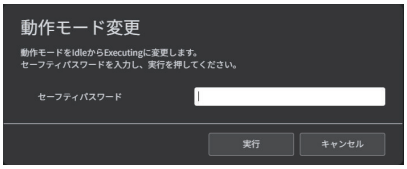
Web UI での使用手順

Web UI の動作モード変更画面で、セーフティ I/O ターミナルの動作モードを変更します。
この画面は、管理者の権限を持つユーザだけが設定できます。



設定の手順は、以下のとおりです。

1 **［現在の動作モード］欄に現在の動作モード、［変更後の動作モード］欄に変更後の動作モードが表示されます。［決定］ボタンを押します。**
以下のメッセージが表示されます。



2 **セーフティパスワードを入力して、［実行］ボタンを押します。**
動作モードが変更され、以下のメッセージが表示されます。



3 **［OK］ボタンを押します。**

7-17 コンフィグレーションロック

コンフィグレーションロックは、セーフティ I/O ターミナルのコンフィグレーションをロックおよびロック解除をする機能です。
CIP Safety コネクション設定画面に登録されている複数のセーフティ I/O ターミナルのコンフィグレーションロックを一括して実行することも可能です。

7-17-1 コンフィグレーションロックの目的

コンフィグレーションロックの目的は、セーフティ I/O ターミナルのセーフティ関連の設定データや実行する安全アプリケーションが意図せずに変更されることを防止することです。コンフィグレーションロックを実行することによって、セーフティパスワードを入力しなければすべての設定データが変更できなくなります。

7-17-2 コンフィグレーションロックの使用手順

コンフィグレーションロックには、Sysmac Studio を使用する方法、および Web UI を使用する方法があります。

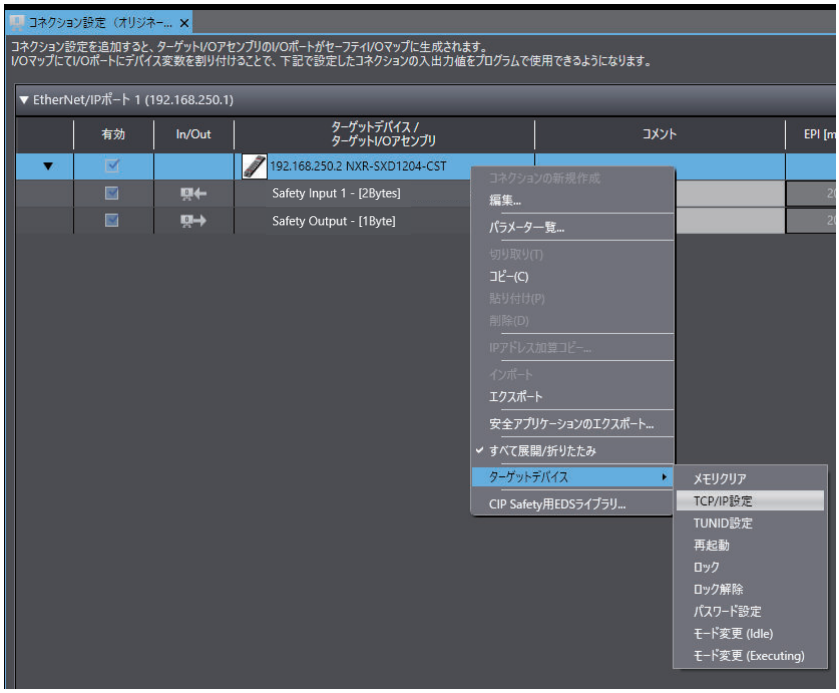
Sysmac Studio での使用手順

Sysmac Studio では、ユニット個別にコンフィグレーションロックおよびロック解除を実行する方法と、CIP Safety コネクション設定画面に登録されている複数ユニットのコンフィグレーションロックおよびロック解除を一括で実行する方法があります。

- **ユニット個別での設定**

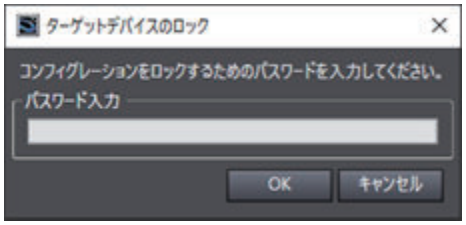
  ユニット個別でのコンフィグレーションロックおよびロック解除の使用手順は、以下のとおりです。

  1 コネクション設定（オリジネータ）の設定画面で、セーフティ I/O ターミナルを右クリックして表示されるメニューから、［ターゲットデバイス］をクリックします。



2 **［ロック］または［ロック解除］をクリックします。**

3 **セーフティパスワード入力画面が表示されるので、セーフティパスワードを入力します。**



4 **［OK］をクリックします。**
コンフィグレーションロックまたはロック解除が実行されます。

参考

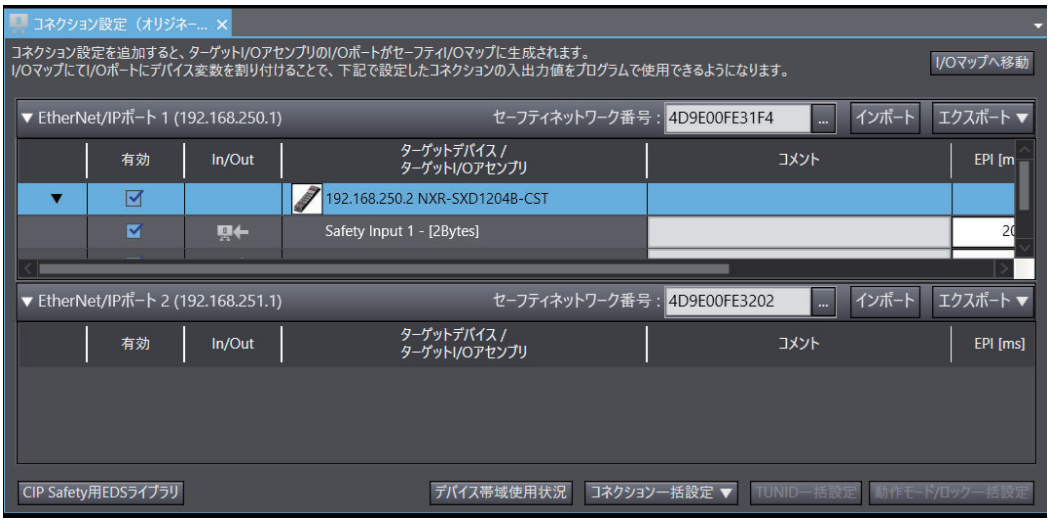
CIP Safety ターゲットデバイス操作画面からも実行可能です。
1）マルチビューエクスプローラでセーフティ PLC（初期表示 new_SafetyCPU_0）を選択し、画面上部のメニューバーから、［ツール］-［CIP Safety ターゲットデバイス操作設定］を選択します。
2）［IP アドレス］にセーフティ I/O ターミナルの IP アドレスを入力します。



● 複数ユニット一括での設定

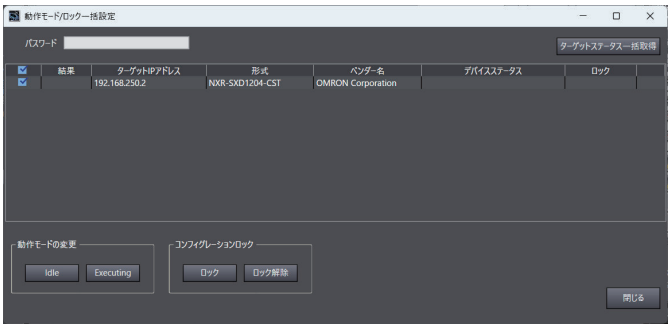
複数ユニット一括での設定の使用手順は、以下のとおりです。

1 **Sysmac Studio で、コネクション設定（オリジネータ）の設定画面を表示します。**



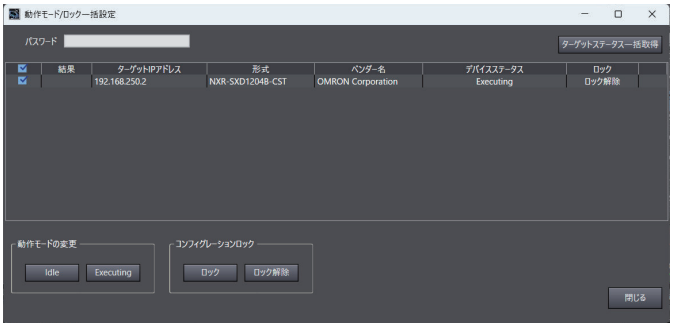
2 **［動作モード／ロック一括設定］ボタンを押します。**

以下の画面が表示されます。



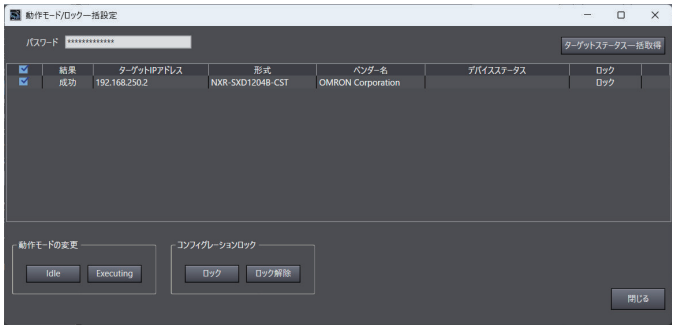
3 **［ターゲットステータス一括取得］ボタンを押します。**

以下のように、［ロック］欄に、各ターゲットのコンフィグレーションロックの状態が表示されます。



4 **セーフティパスワードを入力し、［コンフィグレーションロック］の［ロック］ボタン、または［ロック解除］ボタンを押します。**

複数のユニットのコンフィグレーションロックまたはロック解除が一括で実行されます。以下のように、［結果］欄に各ターゲットのコンフィグレーションロックまたはロック解除が成功したか失敗したかが表示されます。



Web UI での使用手順

Web UI のコンフィグレーションロック画面で、セーフティ I/O ターミナルのコンフィグレーションロックをしたり解除したりします。
この画面は、管理者の権限を持つユーザだけが設定できます。



設定の手順は、以下のとおりです。

1 **［現在の状態］欄に現在のコンフィグレーションロックの状態、［変更後の状態］欄に変更後のコンフィグレーションロックの状態が表示されます。［決定］ボタンを押します。**
以下のメッセージが表示されます。



2 **セーフティパスワードを入力して、［実行］ボタンを押します。**
コンフィグレーションロックまたはロック解除が実行され、以下のようなメッセージが表示されます。



3 **［OK］ボタンを押します。**

7-17-3 コンフィグレーションロックの詳細

ロック状態にあるかどうかは、本体表示部の LOCK LED で確認することができます。ロック状態であれば LOCK LED が点灯し、ロック解除状態であれば LOCK LED が点滅または消灯します。LOCK LED の詳細は、「LOCK LED (P.3-7)」を参照してください。

コンフィグレーションロックの対象データ

コンフィグレーションロックの対象データは、以下のとおりです。ロック状態の場合、これらのデータを変更することはできません。

項目	内容
CIP Safety 通信設定	TUNID を含む CIP Safety 通信設定全般
安全アプリケーション設定	アドオンアプリケーションとユーザ定義アプリケーションの設定、リモート I/O モード用アプリケーションの I/O 構成設定 固定アプリケーションの設定はロック状態によらず変更できない。
非安全機能の設定データ	EtherNet/IP 通信設定、TCP/IP 設定、LINK 設定、Ethernet ポート有効／無効設定、LLDP 機能設定、渡り配線出力用電源遮断機能有効／無効設定、SNTP 設定

コンフィグレーションロックを実行した後、ロータリスイッチを異なる値に変更して電源を ON した場合、「コンフィグレーションロック後のロータリスイッチ設定変更」のイベントが発生し、当該ユニットは動作を停止します。

コンフィグレーションロックの対象機能

コンフィグレーションロックの対象機能は、以下のとおりです。ロック状態の場合、これらの機能を実行することはできません。

- I/O 配線チェック機能
- バックアップ機能のリストア
- メモリオールクリア機能

逆に、以下の機能を実行中は、コンフィグレーションロックを実行できません。

- I/O 配線チェック機能

7-18 セーフティパスワードの設定

セーフティパスワードは、セーフティ I/O ターミナル本体への不正アクセス防止およびセーフティ I/O ターミナル本体に保存された資産の保護のためのパスワードです。

7-18-1 セーフティパスワードの目的

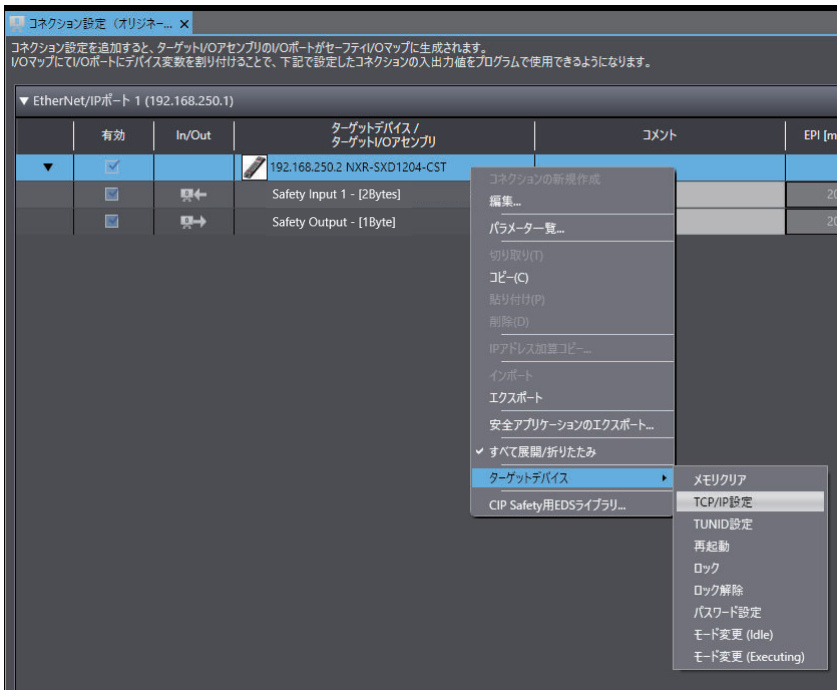
セーフティパスワードの目的は、ユーザの権限に応じた操作だけを使用可能にすることで、セーフティ I/O ターミナルの資産の改ざんや漏えいを防止することです。
そのため、セーフティパスワードを含むユーザのアカウント情報は、適切に管理することが必要です。

7-18-2 セーフティパスワード設定の使用手順

セーフティパスワード設定には、Web UI を使用する方法があります。
また、Sysmac Studio でもセーフティパスワードを変更することは可能です。

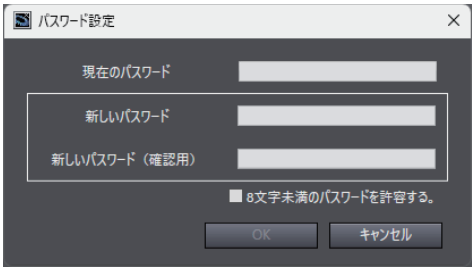
Sysmac Studio でのセーフティパスワード変更手順

1 **コネクション設定（オリジネータ）の設定画面で、セーフティ I/O ターミナルを右クリックして表示されるメニューから、［ターゲットデバイス］をクリックします。**



2 **［パスワード設定］をクリックします。**

3 **パスワード設定画面が表示されるので、現在のセーフティパスワードと新しいセーフティパスワードを入力します。**



4 **［OK］をクリックします。**
新しいセーフティパスワードが設定されます。

参考

CIP Safety ターゲットデバイス操作画面からも実行可能です。
1）マルチビューエクスプローラでセーフティ PLC（初期表示 new_SafetyCPU_0）を選択し、画面上部のメニューバーから、［ツール］-［CIP Safety ターゲットデバイス操作設定］を選択します。
2）［IP アドレス］にセーフティ I/O ターミナルの IP アドレスを入力します。



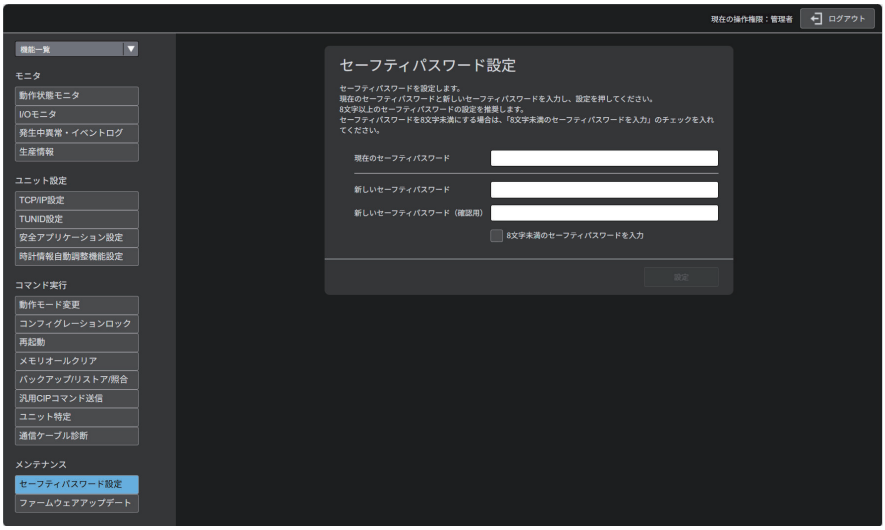
Web UI での使用手順

Web UI でのセーフティパスワード関係の使用手順は、以下を参照してください。

機能	参照先
セーフティパスワード認証	「7-2-6 ログイン (P.7-21)」
セーフティパスワード設定	「Web UI でのセーフティパスワード設定手順 (P.7-101)」
初期セーフティパスワード変更	「初期セーフティパスワード変更 (P.7-23)」

Web UI でのセーフティパスワード設定手順

Web UI のセーフティパスワード設定画面で、セーフティパスワードを設定します。
この画面は、管理者の権限を持つユーザだけが設定できます。



設定の手順は、以下のとおりです。

1 **［現在のセーフティパスワード］に現在のセーフティパスワードを入力します。［新しいセーフティパスワード］、および［新しいセーフティパスワード（確認用）］に新しいセーフティパスワードを入力します。**

セーフティパスワードは、セキュリティ性を向上させるため 8 文字以上にしてください。
ただし、他の機器と同じパスワードにしたいなど特別な事情がある場合には、［8 文字未満のセーフティパスワードを入力］にチェックを入れると、8 文字未満のセーフティパスワードが設定できます。

2 **［設定］ボタンを押します。**

セーフティパスワードが設定され、以下のメッセージが表示されます。



3 **［OK］ボタンを押します。**

Web UI からログアウトし、ログイン画面が表示されます。

7-18-3 セーフティパスワードの詳細

セーフティパスワードの各種仕様を説明します。

セーフティパスワードの入力が要求される操作

Sysmac Studio では、以下の操作の際にセーフティパスワードの入力が要求されます。セーフティパスワードを入力しないと、これらの操作を実行できません。

- セーフティパスワードの変更
- コンフィグレーションロック設定、およびコンフィグレーションロック解除
- 再起動
- 動作モード変更
- メモリオールクリア

Web UI では、ユーザの権限を Web UI が画面に表示する各種情報を閲覧する観察者と、Web UI が提供する各種設定を行う管理者に分けています。
Web UI の各種画面と、観察者および管理者の使用可否の関係は、「7-2-4 メインメニュー一覧 (P.7-17)」を参照してください。

セーフティパスワードの仕様

セーフティパスワードに使用できる文字列の条件は、以下のとおりです。

項目	内容
文字数	8 文字以上 32 文字以下
使用できる文字	A-Z、a-z、0-9、! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { ¦ } ~ 半角スペース

工場出荷時には、セーフティパスワードは設定されていません。

使用上の注意

セキュリティリスクを下げるため、セーフティパスワードは必ず設定してください。また設定するセーフティパスワードは、アルファベット、記号、数字の複数の文字種を使用して複雑にしてください。

その他の仕様

Web UI にログイン後 10 分以上操作しなかった場合、編集権限を持たない第三者による不正使用を防止するため、セーフティパスワードの再入力が要求されます。

ブルートフォース攻撃対策のため、Web UI でセーフティパスワードを 5 回間違えると、10 分間ログインできなくなります。セーフティパスワードを間違えた回数は、ログインに成功する、電源を再投入する、または 10 分経過するのいずれかでリセットされます。

使用上の注意

- セーフティパスワードは、表示することができません。また、メモリオールクリアによってセーフティパスワードを初期化をする場合は、セーフティパスワードを入力する必要があります。
- 第三者による不正使用を防止するため、Web UI による操作を中断しパソコンから離れる際にセーフティ I/O ターミナルからログアウトしてください。Web UI の動作状態モニタ画面、I/O モニタ画面、発生中異常・イベントログ画面で［自動更新］を選択すると、10 分以上操作しなくてもセーフティパスワードの再入力が要求されません。

7-19 バックアップ

バックアップには、バックアップ、リストア、および照合の三つの機能があります。

- **バックアップ**

  当該ユニットの設定データをまとめてバックアップファイルとして、パソコンに保存します。セキュリティ対策のため、バックアップファイルにはバックアップファイルパスワードを設定します。

- **リストア**

  パソコン内のバックアップファイルの内容を、当該ユニットに展開します。

- **照合**

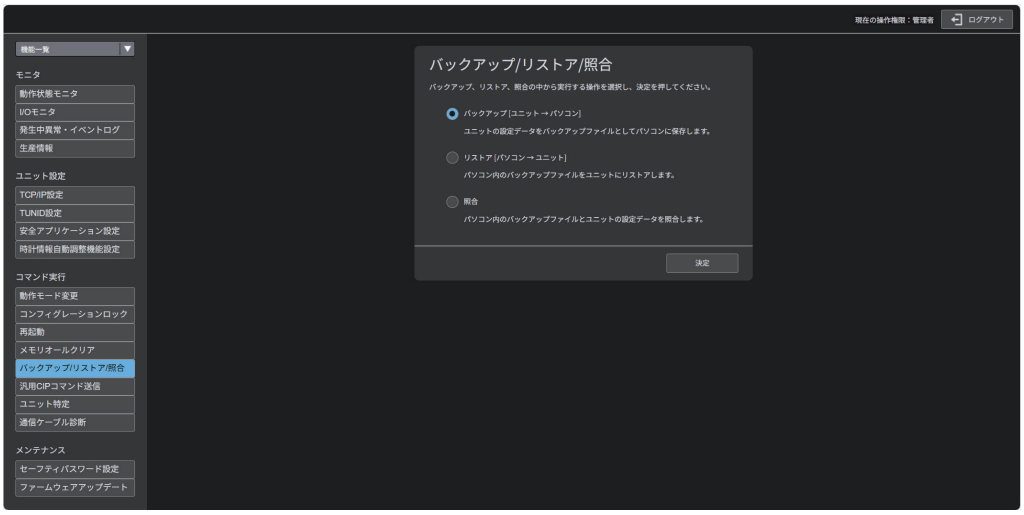
  当該ユニットの設定データと、パソコン内のバックアップファイルの内容を照合して、内容が同じかどうかを検証します。

7-19-1 バックアップの目的

バックアップの目的は、セーフティ I/O ターミナルの設定データを一括してバックアップ、リストア、および照合することで、セーフティ I/O ターミナルの交換時のパラメータ設定時間を短縮することです。
バックアップを定期的および設定変更時に実施し、セーフティ I/O ターミナルの設定内容とバックアップファイルの内容を常に一致させてください。

7-19-2 バックアップの使用手順

Web UI のバックアップ／リストア／照合画面で、バックアップ／リストア／照合を行います。
この画面は、管理者の権限を持つユーザだけが設定できます。



それぞれの手順を示します。

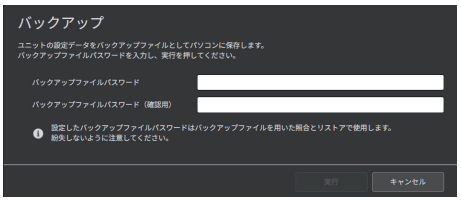
使用上の注意

バックアップを実行するためには、コンフィグレーションロック機能を使用してセーフティ I/O ターミナルをロック状態にしておく必要があります。また、リストアを実行するためには、セーフティ I/O ターミナルをロック解除状態にしておく必要があります。コンフィグレーションロック機能の詳細は、「7-17 コンフィグレーションロック (P.7-95)」を参照してください。

バックアップ

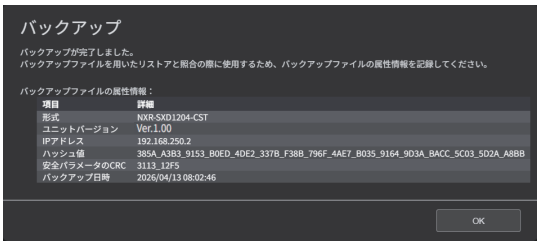
バックアップの手順は、以下のとおりです。

1 **[バックアップ[ユニット→パソコン]] を選択して、[決定] ボタンを押します。**
以下の画面が表示されます。



2 **[バックアップファイルパスワード]、および [バックアップファイルパスワード（確認用）] にバックアップファイルパスワードを入力します。**
バックアップファイルパスワードは、バックアップファイル作成、リストア、および照合のためのパスワードです。セーフティパスワードとは異なります。

3 **[実行] ボタンを押します。**
パソコンのダウンロードフォルダに、バックアップファイルが格納バックアップが格納されます。ファイル名は、「ユニット形式_IP アドレス_日付.dat」です。
以下のメッセージが表示されます。



表示されたバックアップファイルの属性情報は、リストアの際に必要です。記録しておいてください。

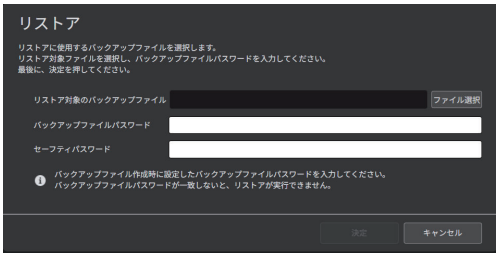
4 **[OK] ボタンを押します。**

リストア

リストアの手順は、以下のとおりです。

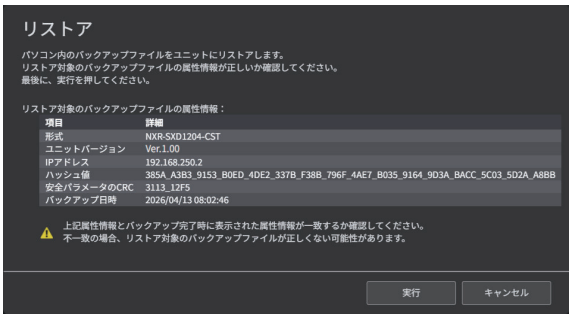
1 **リストア先となる、工場出荷状態またはメモリオールクリア済みのセーフティ I/O ターミナル、バックアップファイル、およびバックアップファイルを作成した際に記録したバックアップファイルの属性情報を準備します。**

2 **Web UI のバックアップ／リストア／照合画面で [リストア[パソコン→ユニット]] を選択して、[決定] ボタンを押します。**
以下の画面が表示されます。



3 **［選択］ボタンを押して、パソコン内のリストア対象のバックアップファイルを選択します。**
［リストア対象のバックアップファイル］欄に、選択したバックアップファイルが表示されます。

4 **バックアップファイルパスワードとセーフティパスワードを入力して［決定］ボタンを押します。**
以下のメッセージが表示されます。



5 **［リストア対象のバックアップファイルの属性情報］欄に表示された属性情報が、バックアップファイル作成時に表示された属性情報と一致するか確認し、［実行］ボタンを押します。一致していなければ、指定したバックアップファイルが破損している可能性があるので［キャンセル］ボタンを押します。**
［実行］ボタンを押した場合はリストアが実行され、以下のメッセージが表示されます。



6 **セーフティパスワードを入力して、［再起動］ボタンを押します。**
セーフティ I/O ターミナルが再起動され、リストアした内容が反映されます。以下のメッセージが表示されます。



7 **［リストア結果］欄に表示された属性情報が、バックアップファイル作成時に表示された属性情報と一致するか確認して、［実行］ボタンを押します。一致していなければ、リストアが失敗している可能性があるので［キャンセル］ボタンを押します。**

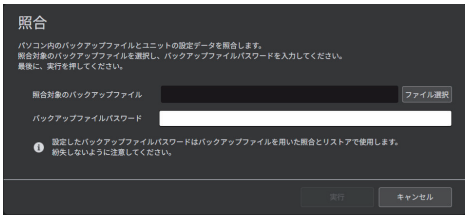
8 **電源を再投入する、または Web UI の再起動画面を使用して、セーフティ I/O ターミナルを再起動します。**

リストアが完了してセーフティ I/O ターミナルが再起動します。手順 7 で［キャンセル］ボタンを押した場合は、自動的にメモリオールクリアが実行されます。
再起動後の動作モードは、リストアされたバックアップデータの電源投入時モード設定に従います。コンフィグレーションロックは、ロック状態になります。

照合

照合の手順は、以下のとおりです。

1 **［照合］を選択して、［決定］ボタンを押します。**
以下の画面が表示されます。



2 **［ファイル選択］ボタンを押して、パソコン内の照合対象のバックアップファイルを選択します。**
［照合対象のバックアップファイル］欄に、選択したバックアップファイルが表示されます。

3 **［バックアップファイルパスワード］に、バックアップファイルを作成した際のバックアップファイルパスワードを入力します。**
バックアップファイルパスワードは、バックアップファイル作成、リストア、および照合のためのパスワードです。セーフティパスワードとは異なります。

4 **［実行］ボタンを押します。**
バックアップファイルパスワードが一致すると、照合が実行され照合結果が表示されます。



5 **［OK］ボタンを押します。**

7-19-3 バックアップの詳細

バックアップの各種仕様を説明します。

バックアップ対象データ

バックアップ、リストア、および照合の対象データは、以下のとおりです。

項目	内容
CIP Safety 通信設定	SNN、TUNID を含む CIP Safety 通信設定全般
安全アプリケーション設定	アドオンアプリケーションとユーザ定義アプリケーションの設定、リモート I/O モード用アプリケーションの I/O 構成設定 固定アプリケーションの設定は含まない。
コンフィグレーションロックの状態	コンフィグレーションロック中であることの情報、およびコンフィグレーションロック時に記憶された各種設定値
生産情報	ユニット形式、ユニットバージョン
非安全機能の設定データ	EtherNet/IP 通信設定、TCP/IP 設定*1、LINK 設定、Ethernet ポート有効／無効設定、LLDP 機能設定、渡り配線出力用電源遮断機能有効／無効設定、SNTP 設定

***1.** IP アドレス設定方法が DHCP の場合、DHCP サーバから取得した IP アドレスはバックアップ、リストア、および照合の対象外です。

バックアップファイルのファイル名

バックアップファイルのデフォルトのファイル名は、「ユニット形式_IP アドレス_日付.dat」です。自由にファイル名を変更することが可能です。

バックアップファイルパスワードの仕様

バックアップファイルパスワードに使用できる文字列の条件は、以下のとおりです。

項目	内容
文字数	8 文字以上 32 文字以下
使用できる文字	A-Z、a-z、0-9、! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { ¦ } ~ 半角スペース

使用上の注意

- セキュリティリスクを下げるため、バックアップファイルパスワードには、アルファベット、記号、数字のすべてを使用してください。
- バックアップファイルパスワードは、表示することも初期化することもできません。忘れないように管理してください。

8

セーフティ I/O ターミナルの機能

この章では、セーフティ I/O ターミナルの各種機能について説明しています。

8-1 機能一覧 8-3

8-2 メモリオールクリア機能 8-4
8-2-1 メモリオールクリア機能の目的 8-4
8-2-2 メモリオールクリア機能の使用手順 8-4
8-2-3 メモリオールクリア機能の詳細 8-7

8-3 HTTPS 通信機能 8-8
8-3-1 HTTPS 通信機能の目的 8-8
8-3-2 HTTPS 通信機能の使用手順 8-8
8-3-3 HTTPS 通信機能の詳細 8-9

8-4 Device Level Ring(DLR)機能 8-10
8-4-1 DLR 機能の目的 8-10
8-4-2 DLR 機能の使用手順 8-10
8-4-3 DLR 機能の詳細 8-10

8-5 渡り配線出力用電源遮断機能 8-11
8-5-1 渡り配線出力用電源遮断機能の目的 8-11
8-5-2 渡り配線出力用電源遮断機能の使用手順 8-11

8-6 I/O 配線チェック機能 8-13
8-6-1 I/O 配線チェック機能の目的 8-13
8-6-2 I/O 配線チェック機能の動作 8-13
8-6-3 I/O 配線チェック機能の I/O 構成設定 8-13
8-6-4 I/O 配線チェック機能の使用手順 8-14

8-7 汎用 CIP コマンド送信機能 8-15
8-7-1 汎用 CIP コマンド送信機能の目的 8-15
8-7-2 汎用 CIP コマンド送信機能の使用手順 8-15

8-8 ユニット特定機能 8-16
8-8-1 ユニット特定機能の目的 8-16
8-8-2 ユニット特定機能の使用手順 8-16
8-8-3 ユニット特定機能の詳細 8-18

8-9 IP アドレス表示機能 8-19
8-9-1 IP アドレス表示機能の目的 8-19
8-9-2 IP アドレス表示機能の使用手順 8-19
8-9-3 IP アドレス表示機能の詳細 8-19

8-10 電源モニタ機能 8-22
8-10-1 電源モニタ機能の目的 8-22
8-10-2 電源モニタ機能の使用手順 8-22

8-10-3　電源モニタ機能の詳細 8-24

8-11　I/O モニタ機能 8-27
8-11-1　I/O モニタ機能の目的 8-27
8-11-2　I/O モニタ機能の使用手順 8-27

8-12　接点動作回数モニタ機能 8-29
8-12-1　接点動作回数モニタ機能の目的 8-29
8-12-2　セーフティ入力端子における使用手順 8-29
8-12-3　セーフティ出力端子における使用手順 8-29

8-13　通信ケーブル診断機能 8-31
8-13-1　通信ケーブル診断機能の目的 8-31
8-13-2　通信ケーブル診断機能の使用手順 8-31
8-13-3　通信ケーブル診断機能の詳細 8-33

8-14　ファームウェアアップデート機能 8-34
8-14-1　ファームウェアアップデート機能の目的 8-34
8-14-2　ファームウェアアップデート機能の使用手順 8-34
8-14-3　ファームウェアアップデート機能の詳細 8-35

8-1 機能一覧

セーフティ I/O ターミナルの各種機能には、以下のものがあります。

機能名	目的	概要	参照先
メモリオールクリア機能	当該ユニットの設定データの情報漏えいを防止する。	当該ユニットの設定データをすべて工場出荷時に戻す。	「8-2 メモリオールクリア機能 (P.8-4)」
HTTPS 通信機能	通信データの情報漏えいを防止する。	Web UI を使用する際に、パソコンと当該ユニット間で暗号化通信を行う。	「8-3 HTTPS 通信機能 (P.8-8)」
Device Level Ring(DLR)機能	通信ケーブルが 1 か所断線しても正常な通信を維持できるようにする。	通信ケーブルをリング状に接続する。	「8-4 Device Level Ring(DLR)機能 (P.8-10)」
渡り配線出力用電源遮断機能	電源の使用量を低減させる。	出力用電源を複数のユニットに渡り配線で接続している場合に、そのユニット以降の出力用電源の供給を遮断する。	「8-5 渡り配線出力用電源遮断機能 (P.8-11)」
I/O 配線チェック機能	セーフティ入出力端子への配線の確認を確実かつ簡単に行えるようにする。	セーフティ入出力端子への配線が正しく行われていることを確認する。	「8-6 I/O 配線チェック機能 (P.8-13)」
汎用 CIP コマンド送信機能	専用ツールや SNCT なしで、当該ユニットが持つ CIP オブジェクトの機能を実行する。	CIP メッセージコマンドを発行する。	「8-7 汎用 CIP コマンド送信機能 (P.8-15)」
ユニット特定機能	操作中のユニットを特定できるようにする。	当該ユニットのユニット特定表示 LED を点灯させる。	「8-8 ユニット特定機能 (P.8-16)」
IP アドレス表示機能	所在はわかっているけれど IP アドレスがわからなくなってしまったユニットの IP アドレスを確認する。	IP アドレスの値を I/O LED 使用して表示する。	「8-9 IP アドレス表示機能 (P.8-19)」
電源モニタ機能	電源電圧値や電源電流値が正常範囲内にない場合に、適切な処置を行えるようにする。	電源電圧値や電源電流値を確認する。	「8-10 電源モニタ機能 (P.8-22)」
I/O モニタ機能	当該ユニットの動作確認や異常の原因特定にかかる時間を短縮する。	当該ユニットの各 I/O 端子の値を表示する。	「8-11 I/O モニタ機能 (P.8-27)」
接点動作回数モニタ機能	当該ユニットのメンテナンス時期を確認する。	当該ユニットのセーフティ入力端子、およびセーフティ出力端子の ON/OFF 回数をモニタリングする。	「8-12 接点動作回数モニタ機能 (P.8-29)」
通信ケーブル診断機能	通信異常の原因究明の効率を向上させる。	通信ケーブルの断線や短絡の有無を確認する。	「8-13 通信ケーブル診断機能 (P.8-31)」
ファームウェアアップデート機能	発覚した当該ユニットのセキュリティ上の脆弱性を改善する。	当該ユニットのファームウェアを更新する。	「8-14 ファームウェアアップデート機能 (P.8-34)」

8-2 メモリオールクリア機能

メモリオールクリア機能は、セーフティ I/O ターミナルの設定データをすべて工場出荷時に戻す機能です。
ただし、以下の情報はメモリオールクリアの対象からはずすことができます。

- IP アドレス
- TUNID
- セーフティパスワード
- イベントログ
- ロータリスイッチ設定 No.9～D のアドオンアプリケーション

使用上の注意

セーフティ I/O ターミナルを廃棄する際には、情報漏えいを防止するために必ず Web UI でメモリオールクリア機能を実行してください。Sysmac Studio によるメモリオールクリアでは、イベントログとロータリスイッチ設定 No.9～D のアドオンアプリケーションがクリアできません。もし、故障などの原因でメモリオールクリア機能が実行できない場合は、当社営業担当者にご相談ください。

8-2-1 メモリオールクリア機能の目的

メモリオールクリア機能の目的は、セーフティ I/O ターミナルの段取り替えの際に設定をいったん工場出荷時に戻したり、セーフティ I/O ターミナルの廃棄の際に設定データをすべてクリアしたりすることです。

8-2-2 メモリオールクリア機能の使用手順

メモリオールクリア機能には、Sysmac Studio を使用する方法、および Web UI を使用する方法があります。

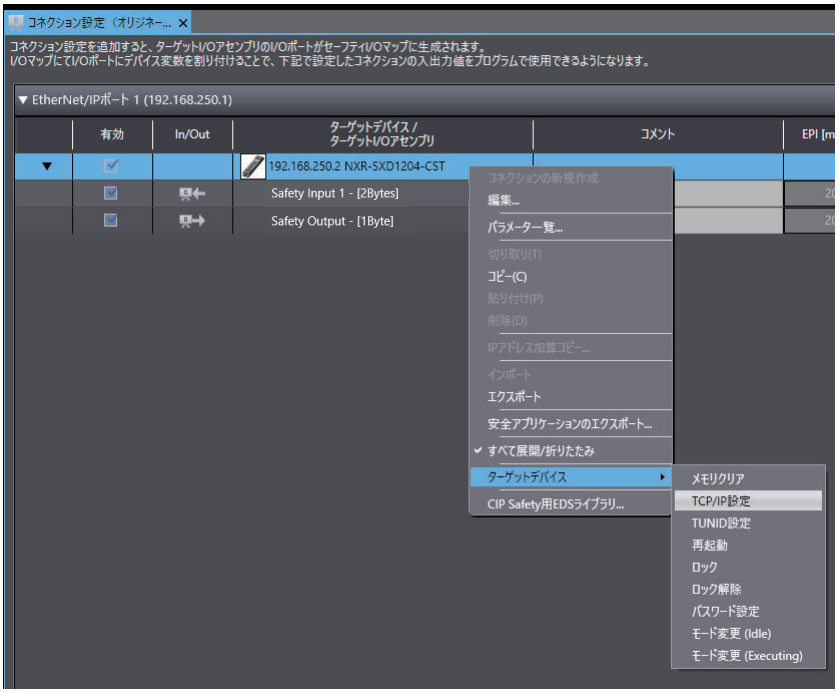
使用上の注意

メモリオールクリア機能を実行するためには、コンフィグレーションロック機能を使用してセーフティ I/O ターミナルをロック解除状態にしておく必要があります。コンフィグレーションロック機能の詳細は、「7-17 コンフィグレーションロック (P.7-95)」を参照してください。

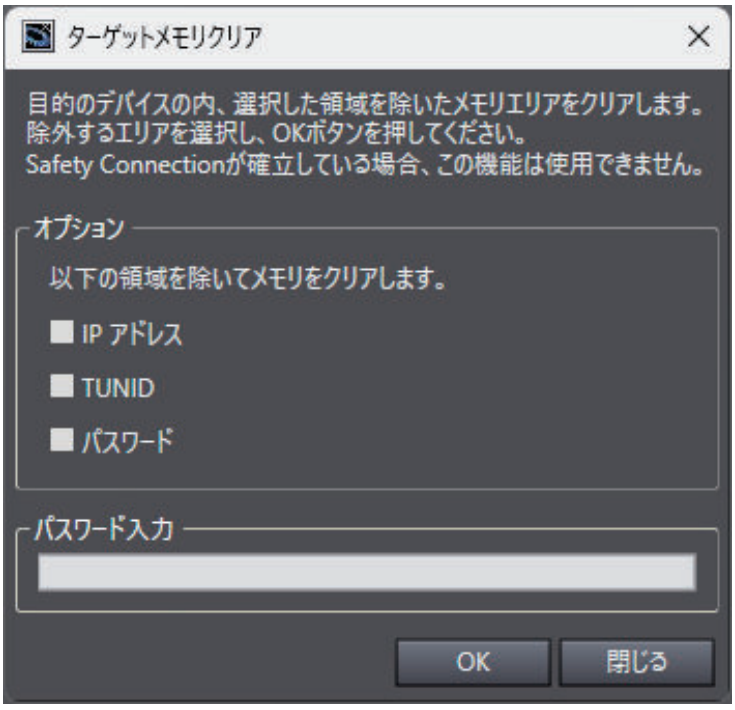
Sysmac Studio での使用手順

Sysmac Studio での手順は、以下のとおりです。

1 コネクション設定（オリジネータ）の設定画面で、セーフティ I/O ターミナルを右クリックして表示されるメニューから、[ターゲットデバイス] をクリックします。



2 **［メモリクリア］をクリックします。**
以下のターゲットメモリクリア画面が表示されます。



3 **［IP アドレス］、［TUNID］、および［パスワード］の中で、クリアしたくない項目にチェックを入れ、［パスワード入力］欄にセーフティパスワードを入力して、［OK］ボタンを押します。**
メモリオールクリアが実行されます。

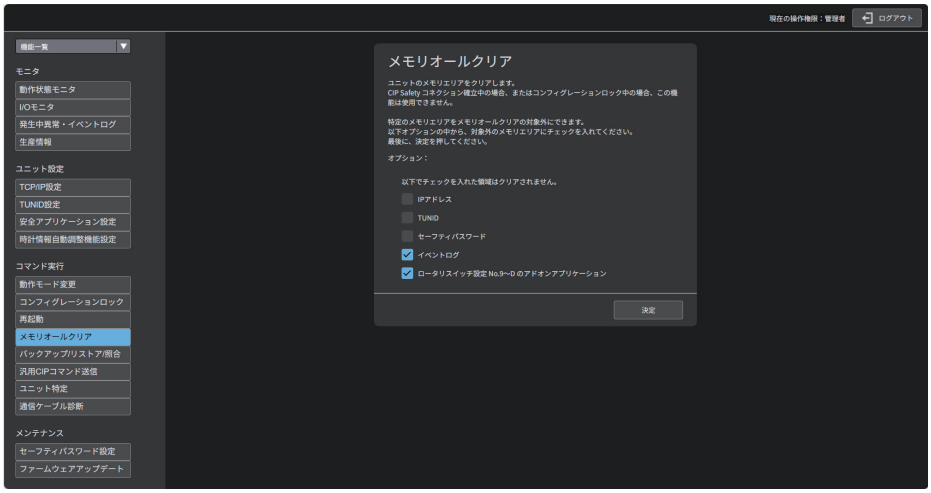
参考

CIP Safety ターゲットデバイス操作画面からも実行可能です。
1）マルチビューエクスプローラでセーフティ PLC（初期表示 new_SafetyCPU_0）を選択し、画面上部のメニューバーから、［ツール］-［CIP Safety ターゲットデバイス操作設定］を選択します。
2）［IP アドレス］にセーフティ I/O ターミナルの IP アドレスを入力します。



Web UI での使用手順

Web UI のメモリオールクリア画面で、セーフティ I/O ターミナルの設定をオールクリアします。
この画面は、管理者の権限を持つユーザだけが設定できます。



設定の手順は、以下のとおりです。

1 **メモリクリアしない項目にチェックを入れて［決定］ボタンを押します。**
以下のようなメッセージが表示されます。



2 **セーフティパスワードを入力して、［実行］ボタンを押します。**
メモリオールクリアが実行され、以下の画面が表示されます。



3 **[OK] ボタンを押します。**
Web UI からログアウトします。

8-2-3 メモリオールクリア機能の詳細

メモリオールクリア機能の対象データは、以下のとおりです。
メモリオールクリア機能を、Sysmac Studio で実行した場合と Web UI で実行した場合とで、対象データは異なります。

分類	内容	Sysmac Studio による実行	Web UI による実行
CIP Safety 通信設定	IP アドレス	対象（選択可）	対象（選択可）
	TUNID	対象（選択可）	対象（選択可）
	IP アドレスと TUNID を除く CIP Safety 通信設定全般	対象	対象
安全アプリケーション設定	ユーザ定義アプリケーションの設定、リモート I/O モード用アプリケーションの I/O 構成設定	対象	対象
	アドオンアプリケーションの設定	対象外	対象（選択可）
非安全機能の設定データ	EtherNet/IP 通信設定、TCP/IP 設定、LINK 設定、Ethernet ポート有効／無効設定、LLDP 機能設定、渡り配線出力用電源遮断機能有効／無効設定、SNTP 設定	対象	対象
セーフティパスワード	セーフティパスワード	対象（選択可）	対象（選択可）
イベントログ	システムイベントログ、アクセスイベントログ	対象外	対象（選択可）

8-3 HTTPS 通信機能

HTTPS 通信機能は、Web UI を使用する際にパソコンとセーフティ I/O ターミナル間の通信を暗号化する機能です。
HTTPS 通信機能を使用するためには、セーフティ I/O ターミナルの Web サーバ証明書に対する CA 証明書を、使用するパソコンの Web ブラウザにインストールする必要があります。CA 証明書は、オムロンのホームページからダウンロードします。一度インストールすれば、そのパソコンでは継続して HTTPS 通信機能が使用できます。

使用上の注意

Web UI を使用する方法には、IP アドレスを入力する方法とドメイン名を入力する方法があります。セキュリティ性が高いのは、ドメイン名を入力する方法です。ここで説明する内容は、ドメイン名を入力する方法を使用する場合に必要なものです。IP アドレスを入力する方法、ドメイン名を入力する方法の詳細は、「IP アドレスを入力する方法 (P.7-20)」、「ドメイン名を入力する方法 (P.7-20)」を参照してください。

8-3-1 HTTPS 通信機能の目的

HTTPS 通信機能の目的は、パソコンとセーフティ I/O ターミナル間の通信路の盗聴による情報漏えいを防止することです。

8-3-2 HTTPS 通信機能の使用手順

HTTPS 通信機能を使用して、Web UI を使用する手順は、以下のとおりです。

1 **オムロンのホームページから、CA 証明書をダウンロードします。**

2 **パソコンの Web ブラウザに、CA 証明書をインストールします。**

3 **生産エリアにドメインネームサーバを設置し、ドメインネームサーバによる名前解決を行います。これにより、セーフティ I/O ターミナルの IP アドレスにユーザが定義するドメイン名を割り当てます。**

ドメイン名は、「*.NXR-SXD.local」としてください。
「*」には、任意の文字列を設定します。ただし、セーフティ I/O ターミナルの IP アドレスごとに異なる文字列を設定してください。以下に、ドメイン名の例を示します。

IP アドレス	ドメイン名
192.168.250.1	device1.NXR-SXD.local
192.168.250.2	device2.NXR-SXD.local

4 **セーフティ I/O ターミナルの EtherNet/IP ポートとパソコンの Ethernet ポートを、Ethernet ケーブルで接続します。**

5 **パソコンで Web ブラウザを起動します。**

6 **Web ブラウザに、手順 3 で割り当てたドメイン名を入力します。たとえば、以下のように入力します。「https://device1.NXR-SXD.local」**
Web UI が起動します。
手順 1～3 は、パソコンごとに一度行うだけです。二度め以降は、手順 4 以降を行うだけで Web UI が起動します。

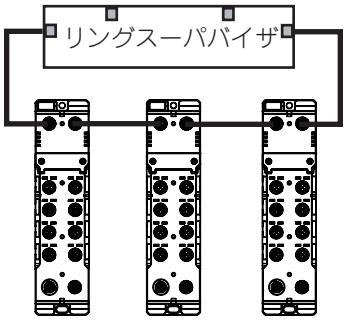
8-3-3 HTTPS 通信機能の詳細

CA 証明書には有効期限があります。有効期限を過ぎた場合は、最新の CA 証明書の再インストールが必要です。CA 証明書のダウンロード元および有効期限は、オムロンのホームページで確認してください。

セーフティ I/O ターミナルの Web サーバのサーバ証明書にも有効期限があります。有効期限を過ぎた場合は、Web ブラウザでセーフティ I/O ターミナルにアクセスした際に、「NET::ERR_CERT_DATE_INVALID」のエラーメッセージが表示されます。サーバ証明書は、ファームウェアアップデート機能を実行することで更新できます。ファームウェアアップデート機能の詳細は、「8-14 ファームウェアアップデート機能 (P.8-34)」を参照してください。

8-4 Device Level Ring(DLR)機能

Device Level Ring(DLR)機能は、通信ケーブルを下図のようにリング状に接続する機能です。



8-4-1 DLR 機能の目的

EtherNet/IP ネットワークの通信ケーブルが断線すると、通常は断線箇所から先のユニットとの通信が行えなくなります。DLR 機能の目的は、通信ケーブルが 1 か所断線しても正常な通信を維持できるようにすることです。DLR 機能を使用するには、リングスーパバイザを介して通信ケーブルをリング状に接続します。これにより、通信ケーブルが 1 か所断線しても逆回りの経路で通信を維持することが可能になります。

8-4-2 DLR 機能の使用手順

DLR 機能を使用するために、特別な設定は不要です。リングスーパバイザを介して、通信ケーブルをリング状に接続するだけで DLR 機能が使用できます。

8-4-3 DLR 機能の詳細

DLR 機能を使用するためには、ビーコンベースのリングノードに対応したリングスーパバイザが必要です。リングスーパバイザの推奨品を、以下に示します。

機器の種類	メーカ	形式
マネージドスイッチ	ロックウェル・オートメーション	Stratix 5400 switches
EtherNet/IP タップ	ロックウェル・オートメーション	1756-EN2TR

使用上の注意

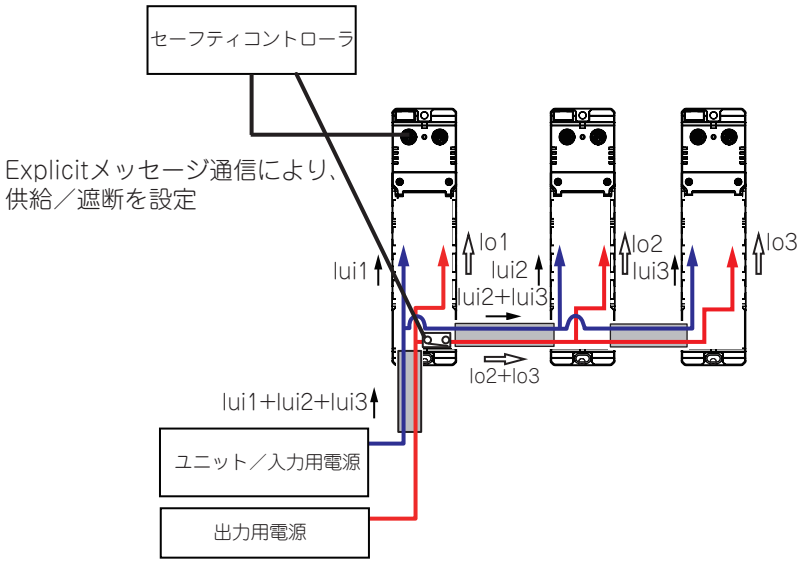
セーフティ I/O ターミナルをリングノードとして使用する場合、リングトポロジ上のリングノード台数は 128 以下にしてください。

8-5 渡り配線出力用電源遮断機能

渡り配線出力用電源遮断機能は、出力用電源を複数のユニットに渡り配線で接続している場合に、そのユニット以降の出力用電源の供給を遮断する機能です。

8-5-1 渡り配線出力用電源遮断機能の目的

渡り配線出力用電源遮断機能の目的は、電源の使用量を低減させることです。セーフティ出力端子の出力が ON であっても OFF であっても、通常は渡り配線で接続されている各ユニットへの出力用電源の供給は継続されています。渡り配線出力用電源遮断機能を使用すると、そのユニット以降の出力用電源の供給が遮断されます。



使用上の注意

渡り配線出力用電源遮断機能は、電源の使用量を低減させるためのものであり、安全機能ではありません。装置の安全性は、別の手段で確保してください。

8-5-2 渡り配線出力用電源遮断機能の使用手順

渡り配線出力用電源遮断機能は、Explicit メッセージ通信を使用して実行します。
渡り配線出力用電源遮断機能実行のための送信コマンドは、以下のとおりです。

実施内容	送信コマンドの項目	送信コマンドの値
渡り配線出力用電源の供給	サービスコード	10Hex(Set_Attribute_Single)
	クラス ID	380Hex（Unit Manager オブジェクト）
	インスタンス ID	01Hex
	アトリビュート ID	28(Cross-Wiring Output Power Shut-off Control)
	サービスデータ	TRUE：渡り配線出力用電源を供給する（デフォルト）。 FALSE：渡り配線出力用電源を供給しない。
	反映タイミング	即時
	再起動時の動作	渡り配線用出力用電源を供給する。

実施内容	送信コマンドの項目	送信コマンドの値
渡り配線出力用電源遮断機能有効／無効切り替え	サービスコード	10Hex(Set_Attribute_Single)
	クラス ID	380Hex（Unit Manager オブジェクト）
	インスタンス ID	01Hex
	アトリビュート ID	29(Cross-Wiring Output Power Shut-off Enable)
	サービスデータ	TRUE：渡り配線出力用電源遮断機能を使用する（デフォルト）。 FALSE：渡り配線出力用電源遮断機能を使用しない。
	反映タイミング	即時
	再起動時の動作	再起動する前の設定を継続する。

CIP オブジェクトへの Explicit メッセージによるアクセス方法は、「Explicit メッセージサーバ機能 (P.6-6)」を参照してください。

8-6 I/O 配線チェック機能

I/O 配線チェック機能は、セーフティ I/O ターミナルのセーフティ入出力端子への配線が正しく行われていることを確認する機能です。

8-6-1 I/O 配線チェック機能の目的

セーフティ I/O ターミナルのセーフティ入出力端子への配線に誤りがあると、重大な事故につながる可能性があります。しかし、アプリケーションによっては配線が複雑になり、配線の確認が容易ではない場合もあります。I/O 配線チェック機能の目的は、セーフティ入出力端子への配線の確認を確実かつ簡単に行えるようにすることです。

8-6-2 I/O 配線チェック機能の動作

I/O 配線チェック機能のセーフティ出力端子の動作は、以下のとおりです。
I/O 配線チェック機能で動作確認できるのは、セーフティ入力端子 Si00-Si03 とセーフティ出力端子 So00-So03 です。セーフティ入力端子 Si04-Si11 の動作確認は、セーフティ入力 LED を目視することで行ってください。

セーフティ出力端子	動作
So00	Si00 が TRUE、かつイネーブルスイッチが押されている間 TRUE。それ以外は FALSE。
So01	Si01 が TRUE、かつイネーブルスイッチが押されている間 TRUE。それ以外は FALSE。
So02	Si02 が TRUE、かつイネーブルスイッチが押されている間 TRUE。それ以外は FALSE。
So03	Si03 が TRUE、かつイネーブルスイッチが押されている間 TRUE。それ以外は FALSE。

8-6-3 I/O 配線チェック機能の I/O 構成設定

I/O 配線チェック機能では、セーフティ入力端子 Si06、Si07 に接続されたイネーブルスイッチを押すことによって I/O 配線チェックすることを想定しています。I/O 構成設定は、以下のとおりです。

入力

Input	Device	Test Output Mode
Si00/T00	任意（シングル）	Power Supply Output
Si01/T01	任意（シングル）	Power Supply Output
Si02/T02	任意（シングル）	Power Supply Output
Si03/T03	任意（シングル）	Power Supply Output
Si04/T04	任意（シングル）	Power Supply Output
Si05/T05	任意（シングル）	Power Supply Output
Si06/T06	イネーブルスイッチ（デュアルチャネル同値入力）	Test Output
Si07/T07	イネーブルスイッチ（デュアルチャネル同値入力）	Test Output
Si08/T08	任意（シングル）	Power Supply Output
Si09/T09	任意（シングル）	Power Supply Output
Si10/T10	任意（シングル）	Power Supply Output
Si11/T11	任意（シングル）	Power Supply Output

出力

Output	Device
So00	シングルチャネル（テストパルスなし）
So01	シングルチャネル（テストパルスなし）
So02	シングルチャネル（テストパルスなし）
So03	シングルチャネル（テストパルスなし）

8-6-4 I/O 配線チェック機能の使用手順

I/O 配線チェック機能の使用手順は、以下のとおりです。

1 **セーフティ I/O ターミナルのセーフティ入出力端子に、任意の配線を行います。**

2 **セーフティ I/O ターミナルのロータリスイッチの SETTING SW1、SW2 を両方とも「E」に設定して、電源を投入します。**

3 **セーフティ I/O ターミナルのセーフティ入力端子に任意の入力を行います。それに対応するセーフティ出力端子から適切な出力が行われていることを確認します。または、I/O LED が適切に点灯していることを確認します。**

8-7 汎用 CIP コマンド送信機能

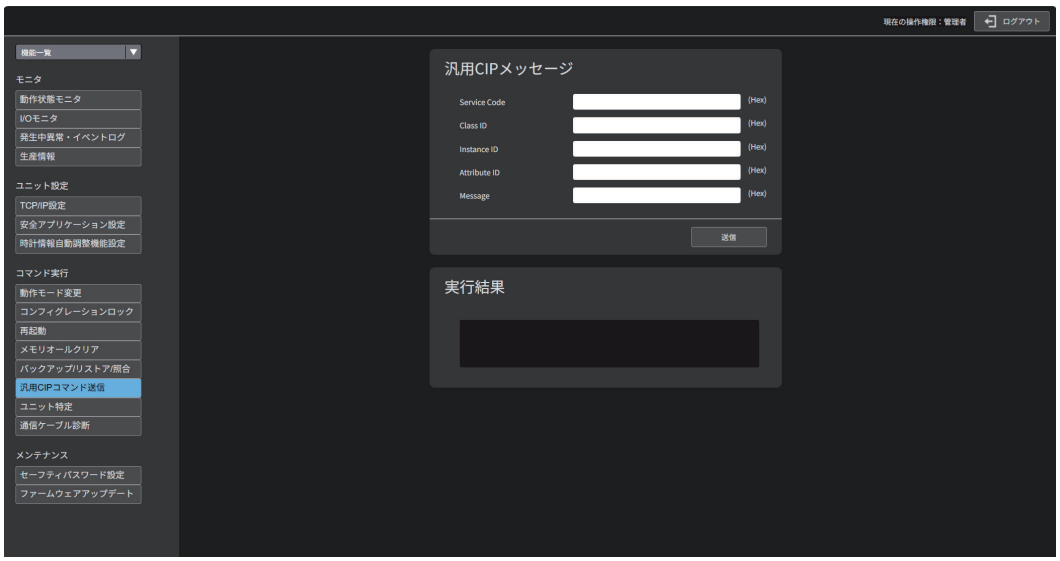
汎用 CIP コマンド送信機能は、セーフティ I/O ターミナルが持つ CIP オブジェクトに対して任意の CIP メッセージコマンドを発行する機能です。

8-7-1 汎用 CIP コマンド送信機能の目的

汎用 CIP コマンド送信機能の目的は、専用ツールや Safety Network Configuration Tool（SNCT）なしで、セーフティ I/O ターミナルが持つ CIP オブジェクトの機能を実行することです。

8-7-2 汎用 CIP コマンド送信機能の使用手順

Web UI の汎用 CIP コマンド送信画面で、CIP メッセージコマンドを発行します。
この画面は、管理者の権限を持つユーザだけが設定できます。
CIP オブジェクトの仕様の詳細は、「A-4 サポートする CIP オブジェクト (P.A-15)」を参照してください。



設定の手順は、以下のとおりです。

1 **［Service Code］、［Class ID］、［Instance ID］、［Attribute ID］、［Message］の各項目を入力して［送信］ボタンを押します。**
当該ユニットに汎用 CIP コマンドが送信されます。

2 **［実行結果］欄を確認します。**

8-8 ユニット特定機能

ユニット特定機能は、当該ユニットのユニット特定表示 LED を点滅させる機能です。

8-8-1 ユニット特定機能の目的

ユニット特定機能の目的は、複数のセーフティ I/O ターミナルを使用している場合に、ユニット特定表示 LED を点滅させることで、操作中のユニットを特定することです。

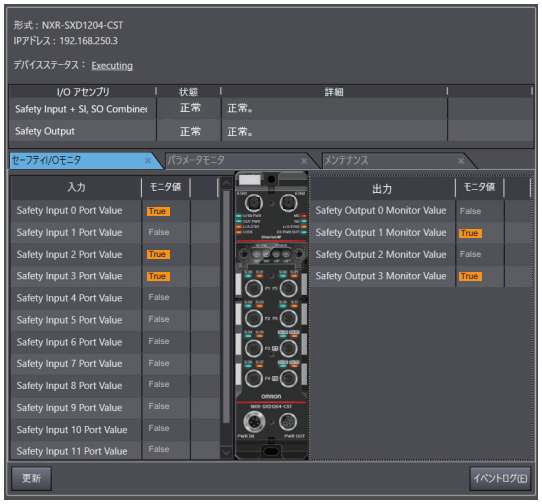
8-8-2 ユニット特定機能の使用手順

ユニット特定機能には、Sysmac Studio を使用する方法、および Web UI を使用する方法があります。

Sysmac Studio での使用手順

Sysmac Studio での使用手順は、以下のとおりです。

1 **Sysmac Studio の CIP Safety モニタ画面で、セーフティ I/O ターミナルを選択します。**
以下の画面が表示されます。



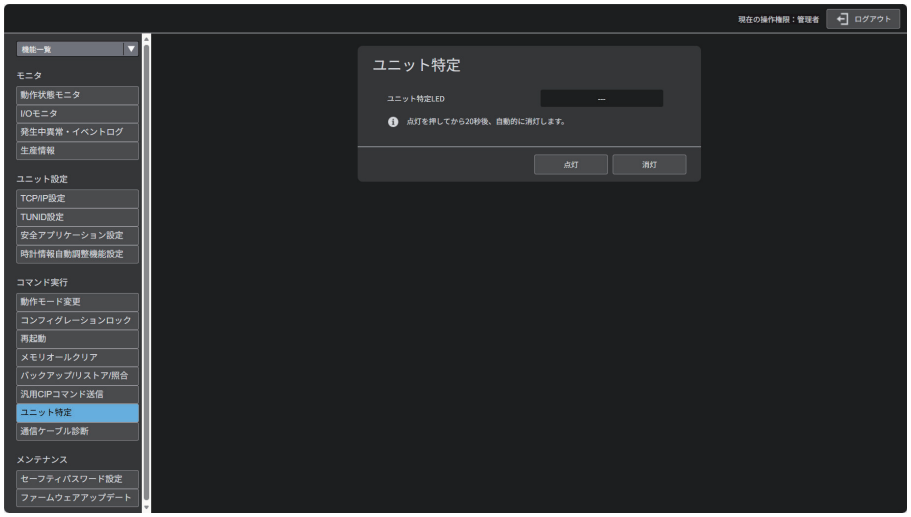
2 **［メンテナンス］タブを選択します。**
以下の画面が表示されます。



3 **［ユニット特定機能］の［実行］ボタンを押します。**
指定したユニットのユニット特定表示 LED が点滅します。

Web UI での使用手順

Web UI のユニット特定画面で、操作中のユニットのユニット特定表示 LED を点滅させます。



設定の手順は、以下のとおりです。

1 **［点灯］ボタンを押します。**
当該ユニットに対してユニット特定機能が実行され、ユニット特定表示 LED が点滅します。［ユニット特定 LED］欄に、［点灯中］と表示されます。

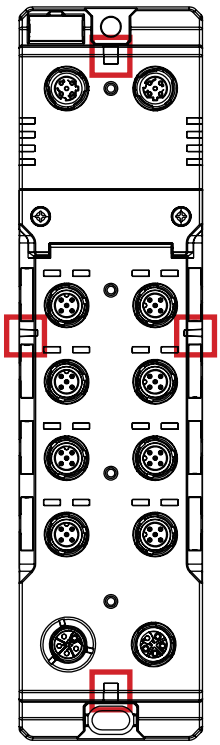
2 **［消灯］ボタンを押します。**
ユニット特定機能が停止し、ユニット特定表示 LED が消灯します。［ユニット特定 LED］欄に、［消灯中］と表示されます。

［消灯］ボタンを押さなくても、［点灯］ボタンを押してから 60 秒後に、ユニット特定表示 LED は自動的に消灯します。

8-8-3 ユニット特定機能の詳細

ユニット特定機能を実行すると、下図の 4 か所のユニット特定表示 LED が以下のように点滅します。

- 各 LED が時計回りに 100ms ずつ順番に点灯することを 4 回繰り返す。
- その後、4 か所すべての LED が 500ms 消灯する。
- 上記を 60 秒間繰り返す。



8-9 IP アドレス表示機能

IP アドレス表示機能は、Sysmac Studio または Web UI で設定されたセーフティ I/O ターミナルの IP アドレスを、ユニットの I/O LED を使用して表示する機能です。

8-9-1 IP アドレス表示機能の目的

IP アドレス表示機能の目的は、Sysmac Studio または Web UI で設定されたセーフティ I/O ターミナルの IP アドレスを、サポートソフトなどの特別なツールを使用せずに確認することです。

8-9-2 IP アドレス表示機能の使用手順

IP アドレス表示機能の使用手順は、以下のとおりです。

1 **当該ユニットを、ネットワークから離脱させます。**

2 **ロータリスイッチの SETTING SW1、SW2 を、両方とも「8」に設定します。**

3 **ユニットを再起動します。**
I/O LED が IP アドレスを意味する点灯を開始します。

8-9-3 IP アドレス表示機能の詳細

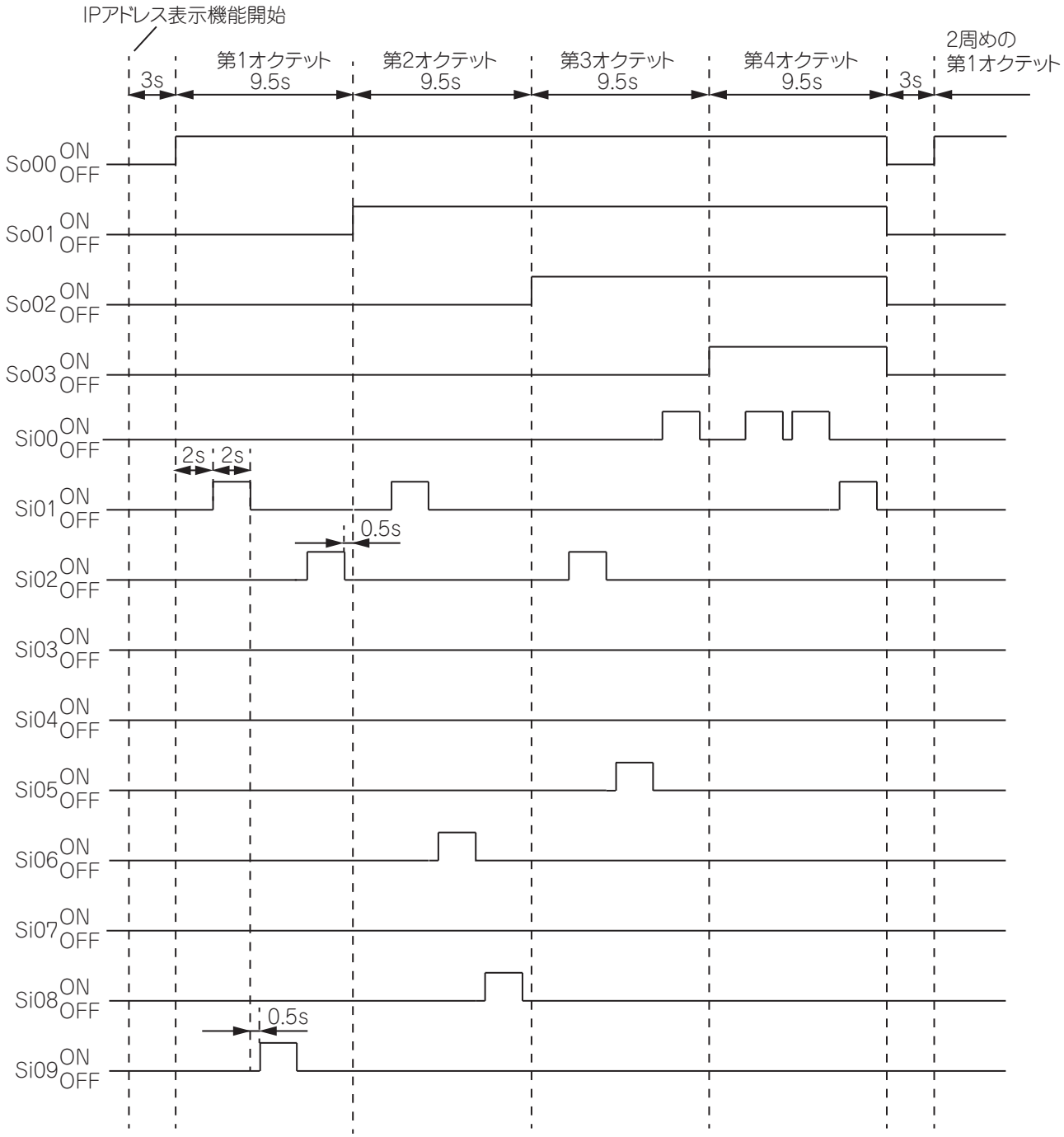
IP アドレスは、第 1 オクテット、第 2 オクテット、第 3 オクテット、第 4 オクテットの順に表示されます。各オクテットを表す I/O LED は以下のとおりです。まず第 1 オクテットの I/O LED が 9.5 秒間点灯します。同じことが第 2 オクテット、第 3 オクテット、第 4 オクテットの I/O LED の順番で実行されます。

オクテット	I/O LED
第 1 オクテット	So00
第 2 オクテット	So00～So01
第 3 オクテット	So00～So02
第 4 オクテット	So00～So03

各オクテットの 3 桁の数字は、各桁が 2 秒間ずつ順番に点灯されることで表示されます。各点灯の間には、0.5 秒間の消灯が入ります。各数字を表す I/O LED は以下のとおりです。

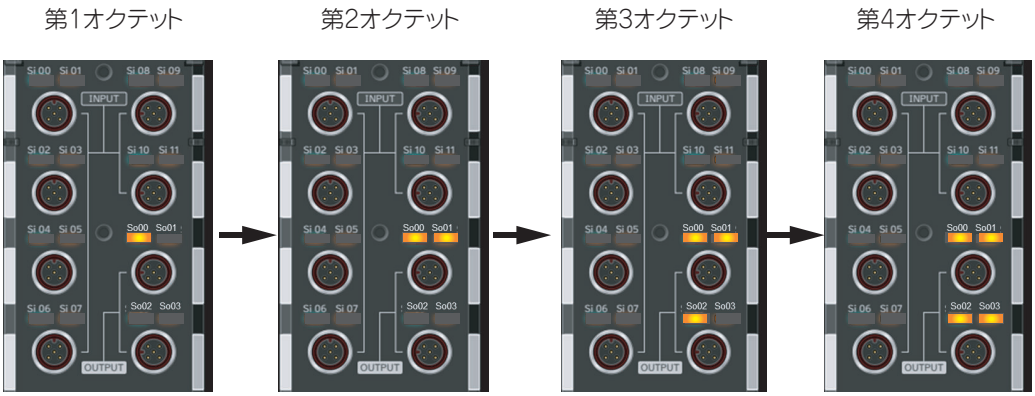
数字	I/O LED
0	Si00
1	Si01
2	Si02
3	Si03
4	Si04
5	Si05
6	Si06
7	Si07
8	Si08
9	Si09

IP アドレス表示機能を開始してから 3 秒後に、第 1 オクテットの点灯が開始されます。また、第 1 オクテットの点灯を開始してから 2 秒後に、第 1 オクテットの 1 桁めの点灯が開始されます。
例として、IP アドレス「192.168.250.001」を表示する場合の I/O LED のタイミングチャートを示します。



同じことがロータリスイッチの値を変更するまで繰り返されます。

第 1 オクテットから第 4 オクテットを示す I/O LED の実際の様子は、以下のようになります。
この図は、形 NXR-SXD1204-CST の場合です。


第1オクテット
第2オクテット
第3オクテット
第4オクテット
INPUT
OUTPUT

8-10 電源モニタ機能

電源モニタ機能は、セーフティ I/O ターミナルの電源電圧値と電源電流値を確認する機能です。

8-10-1 電源モニタ機能の目的

セーフティ I/O ターミナルが正常動作するためには、電源電圧値と電源電流値がともに正常範囲内である必要があります。電源モニタ機能の目的は、電源電圧値と電源電流値が正常範囲内にあるかどうかを確認し、正常範囲内にない場合は適切な処置を行えるようにすることです。

8-10-2 電源モニタ機能の使用手順

電源モニタ機能では、以下の値を確認することができます。

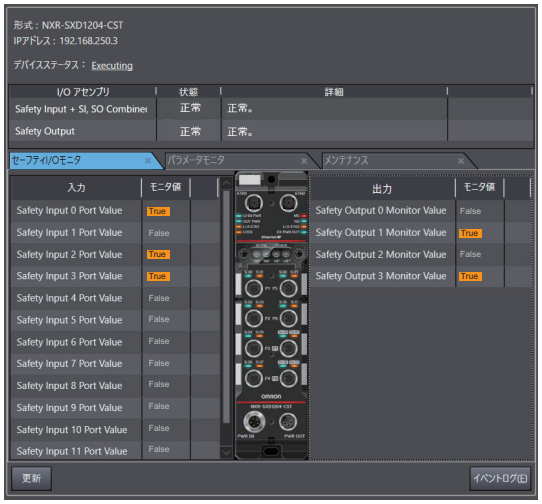
- ユニット／入力用電源電圧
- 出力用電源電圧
- ユニット／入力用電源電流
- 出力用電源電流

電源モニタ機能には、Sysmac Studio を使用する方法と Web UI を使用する方法があります。

Sysmac Studio での使用手順

Sysmac Studio での使用手順は、以下のとおりです。

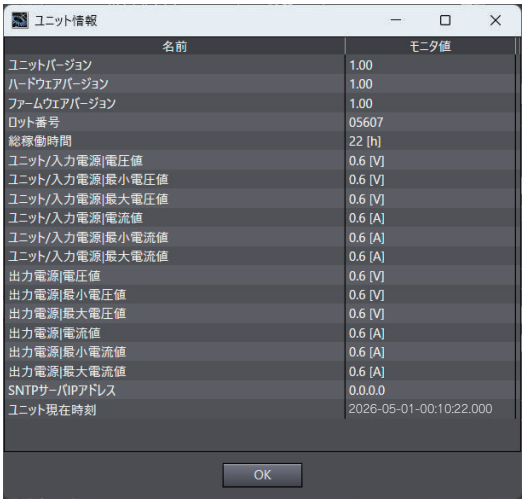
1 **Sysmac Studio の CIP Safety モニタ画面で、セーフティ I/O ターミナルを選択します。**
以下の画面が表示されます。



2 **［メンテナンス］タブを選択します。**
以下の画面が表示されます。



3 **［ユニット情報］の［読み出し］ボタンを押します。**
以下の画面が表示されます。



Web UI での使用手順

Web UI の動作状態モニタ画面で、当該ユニットのユニットステータスや電源ステータスを確認します。



8-10-3 電源モニタ機能の詳細

電源モニタ機能には、電源電圧のモニタと電源電流のモニタがあります。

電源電圧のモニタ

電源電圧をモニタします。ユニット／入力用電源電圧、および出力用電源電圧が正常値かどうかは、U/IN PWR LED および OUT PWR LED で確認することもできます。また、電圧異常の場合にはイベントが発生します。さらに、電源電圧が許容値を超えた場合には、自動的に電源入力が遮断されます。

● ユニット／入力用電源電圧

ユニット／入力用電源電圧値と LED の状態、モニタリングできる値、イベントの発生、および復旧方法の関係を、以下に示します。

電圧値[V]	状態	U/IN PWR LED	モニタリングできる値	イベント	復旧方法
0 - 低電圧検出しきい値	低電圧検知による電源遮断*1	消灯	モニタリングできない。	発生しない。	適切な値の電源を供給する。
低電圧検出しきい値 - 19.2	仕様範囲外電圧	点灯	電圧値	ユニット／入力用電源仕様範囲外電圧検知	適切な値の電源を供給する。
19.2 - 28.8	正常電圧	点灯	電圧値	発生しない。	復旧の必要なし
28.8 - 過電圧検出しきい値	仕様範囲外電圧	点灯	電圧値	ユニット／入力用電源仕様範囲外電圧検知	適切な値の電源を供給する。
過電圧検出しきい値を超える電圧	過電圧検知による電源遮断*2	消灯	モニタリングできない。	発生しない。	適切な値の電源を供給して再起動する。

***1.** ユニットの内部回路の電源が遮断されます。電源コネクタ OUT からのユニット／入力用電源の供給は遮断されません。電源コネクタ OUT からの出力用電源の供給は遮断されます。

***2.** ユニットの内部回路の電源が遮断されます。電源コネクタ OUT からのユニット／入力用電源は検知電圧により遮断される場合とされない場合があります。電源コネクタ OUT からの出力用電源の供給は、遮断されます。

● 出力用電源電圧

出力用電源電圧値と LED の状態、モニタリングできる値、イベントの発生、および復旧方法の関係を、以下に示します。

電圧値[V]	状態	OUT PWR LED	モニタリングできる値	イベント	復旧方法
0 - 低電圧検出しきい値	低電圧検知による電源遮断*1 すべてのセーフティ出力が OFF	消灯	電圧値	出力用電源異常	適切な値の電源を供給する。
低電圧検出しきい値 - 19.2	仕様範囲外電圧	点灯	電圧値	出力用電源仕様範囲外電圧検知	適切な値の電源を供給する。
19.2 - 28.8	正常電圧	点灯	電圧値	発生しない。	復旧の必要なし
28.8 - 過電圧検出しきい値	仕様範囲外電圧	点灯	電圧値	出力用電源仕様範囲外電圧検知	適切な値の電源を供給する。
過電圧検出しきい値を超える電圧	過電圧検知による電源遮断*2 すべてのセーフティ出力が OFF	消灯	電圧値	出力用電源異常	適切な値の電源を供給して再起動する。

***1.** ユニットの内部回路の電源が遮断されます。電源コネクタ OUT からの出力用電源の供給は遮断されません。
***2.** ユニットの内部回路の電源が遮断されます。電源コネクタ OUT からの出力用電源の供給は、検知電圧により遮断される場合とされない場合があります。

電源電流のモニタ

電源電流をモニタします。過電流異常で電源が遮断された場合には、イベントが発生します。さらに、電源電流が許容値を超えた場合には、自動的に電源入力が遮断されます。

● ユニット／入力用電源電流

ユニット／入力用電源電流値とモニタリングできる値、イベントの発生、および復旧方法の関係を、以下に示します。

電流値[A]	状態	モニタリングできる値	イベント	復旧方法
0 - 9	正常電流	電流値	発生しない。	復旧の必要なし
9 - 過電流検出しきい値	仕様範囲外電流	電流値	ユニット／入力用電源仕様範囲外電流検知	適切な値の電源を供給する。
過電流検出しきい値を超える電流	過電流検知による電源遮断*1	モニタリングできない。	発生しない。	適切な値の電源を供給して再起動する。

***1.** ユニットの内部回路の電源が遮断されます。電源コネクタ OUT からのユニット／入力用電源と出力用電源の供給も遮断されます。

● 出力用電源電流

出力用電源電流値とモニタリングできる値、イベントの発生、および復旧方法の関係を、以下に示します。

電流値[A]	状態	モニタリングできる値	イベント	復旧方法
0 - 9	正常電流	電流値	発生しない。	復旧の必要なし
9 - 過電流検出しきい値	仕様範囲外電流	電流値	出力用電源仕様範囲外電流検知	適切な値の電源を供給する。

電流値[A]	状態	モニタリングできる値	イベント	復旧方法
過電流検出しきい値を超える電流	過電流検知による電源遮断 *1 すべてのセーフティ出力がOFF	電流値	出力用電源異常	適切な値の電源を供給して再起動する。

***1.** ユニットの内部回路の電源が遮断されます。電源コネクタ OUT からの出力用電源の供給も遮断されます。

8-11 I/O モニタ機能

I/O モニタ機能は、I/O 端子の値を表示する機能です。

8-11-1 I/O モニタ機能の目的

セーフティ I/O ターミナルの動作確認や異常の原因特定を行う際には、セーフティ入出力のデータがどのようになっているかを確認することが有効です。I/O モニタ機能の目的は、セーフティ入出力のデータを確認することで、セーフティ I/O ターミナルの動作確認や異常の原因特定にかかる時間を短縮することです。

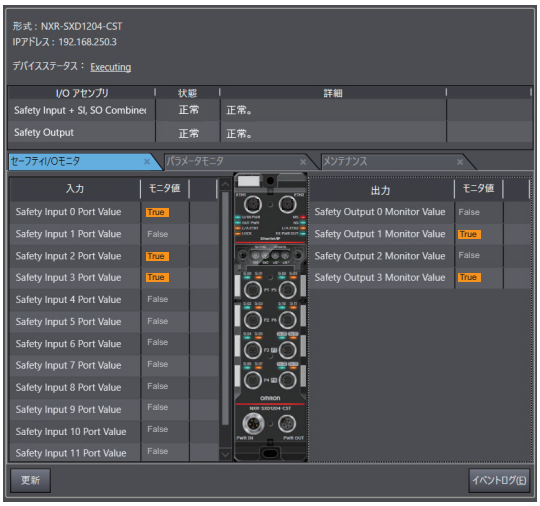
8-11-2 I/O モニタ機能の使用手順

I/O モニタ機能には、Sysmac Studio を使用する方法と Web UI を使用する方法があります。

Sysmac Studio での使用手順

Sysmac Studio での使用手順は、以下のとおりです。

1 **Sysmac Studio の CIP Safety モニタ画面で、セーフティ I/O ターミナルを選択します。**
以下の画面が表示されます。



2 **［セーフティ I/O モニタ］タブを選択します。**
セーフティ入出力データの値が表示されます。

Web UI での使用手順

Web UI の I/O モニタ画面で、I/O 端子の値を確認します。


現在の操作権限：管理者
ログアウト
機能一覧
モニタ
動作状態モニタ
I/Oモニタ
発生中異常・イベントログ
生産情報
ユニット設定
TCP/IP設定
安全アプリケーション設定
時計情報自動調整機能設定
コマンド実行
動作モード変更
コンフィグレーションロック
再起動
メモリオールクリア
バックアップ/リストア/照合
汎用CIPコマンド送信
ユニット特定
通信ケーブル診断
メンテナンス
セーフティパスワード設定
ファームウェアアップデート
自動更新
手動更新
テスト出力
入力ポート
入力ポート
出力ポート
Si 00
Si 01
Si 08
Si 09
T 00
T 01
T 08
T 09
Si 02
Si 03
Si 10
Si 11
T 02
T 03
T 10
T 11
Si 04
Si 05
T 04
T 05
Si 06
Si 07
T 06
T 07
So 00
So 01
So 02
So 03
ON
OFF

8-12 接点動作回数モニタ機能

接点動作回数モニタ機能は、接点動作回数（単位：回）を確認する機能です。
セーフティ入力端子、およびセーフティ出力端子ごとに ON/OFF 回数をカウントし、カウント現在値として保持します。
それを CIP メッセージ通信（Explicit メッセージ通信）により、カウント現在値として取得します。
また、カウント現在値はクリアもできます。

8-12-1 接点動作回数モニタ機能の目的

接点動作回数モニタ機能の目的は、接点動作回数をモニタすることでメンテナンスの時期を確認することです。

参考

しきい値、および しきい値を超えたことを通知する機能ではありません。

8-12-2 セーフティ入力端子における使用手順

セーフティ入力端子において、接点動作回数モニタ機能は CIP メッセージ通信（Explicit メッセージ通信）を使用して実行します。
送信コマンドは、以下のとおりです。

実施内容	送信コマンドの項目	送信コマンドの値
セーフティ入力端子のカウント現在値を取得	サービスコード	0EHex(Get_Attribute_Single)
	クラス ID	3DHex(Safety Discrete Input Point (SDIP) オブジェクト)
	インスタンス ID	01Hex-0CHex (セーフティ入力端子ごとのインスタンスを指定する)
	アトリビュート ID	102(Maintenance Counter)
セーフティ入力端子のカウント現在値をクリア	サービスコード	10Hex(Set_Attribute_Single)
	クラス ID	3DHex(Safety Discrete Input Point (SDIP) オブジェクト)
	インスタンス ID	01Hex-0CHex (セーフティ入力端子ごとのインスタンスを指定する)
	アトリビュート ID	102(Maintenance Counter)
	サービスデータ	00000000Hex （0 を書き込むことで、値をクリアする）

CIP メッセージ通信（Explicit メッセージ通信）での手順は、「Explicit メッセージサーバ機能 (P.6-6)」を参照してください。

8-12-3 セーフティ出力端子における使用手順

セーフティ出力端子において、接点動作回数モニタ機能は CIP メッセージ通信（Explicit メッセージ通信）を使用して実行します。
送信コマンドは、以下のとおりです。

実施内容	送信コマンドの項目	送信コマンドの値
セーフティ出力端子のカウント現在値を取得	サービスコード	0EHex(Get_Attribute_Single)
	クラス ID	3BHex(Safety Discrete Ouput Point (SDOP) オブジェクト)
	インスタンス ID	01Hex-04Hex (セーフティ出力端子ごとのインスタンスを指定する)
	アトリビュート ID	102(Maintenance Counter)
セーフティ出力端子のカウント現在値をクリア	サービスコード	10Hex(Set_Attribute_Single)
	クラス ID	3BHex(Safety Discrete Ouput Point (SDOP) オブジェクト)
	インスタンス ID	01Hex-04Hex (セーフティ出力端子ごとのインスタンスを指定する)
	アトリビュート ID	102(Maintenance Counter)
	サービスデータ	00000000Hex （0 を書き込むことで、値をクリアする)

CIP メッセージ通信（Explicit メッセージ通信）での手順は、「Explicit メッセージサーバ機能 (P.6-6)」を参照してください。

8-13 通信ケーブル診断機能

通信ケーブル診断機能は、通信異常が発生した場合にその原因が通信ケーブルの断線や短絡かどうかを確認するための機能です。また、断線や短絡が発生している箇所の位置の目安も確認できます。

8-13-1 通信ケーブル診断機能の目的

EtherNet/IP ポート 1 およびポート 2 を使用して実行する通信において、通信異常が発生する原因は複数考えられます。通信ケーブル診断機能の目的は、通信異常の原因を確認することです。

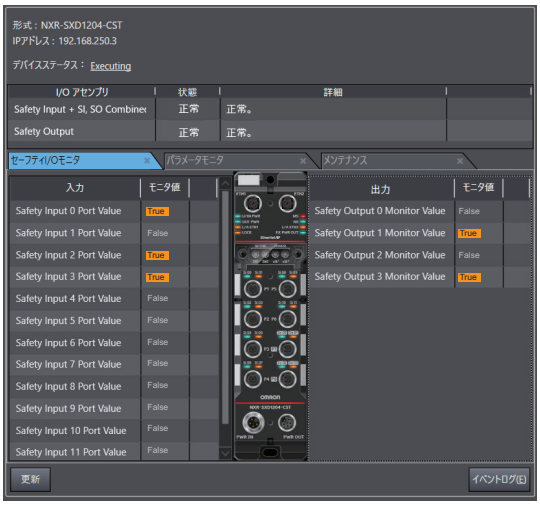
8-13-2 通信ケーブル診断機能の使用手順

通信ケーブル診断機能には、Sysmac Studio を使用する方法、Web UI を使用する方法、および Explicit メッセージ通信を使用する方法があります。

Sysmac Studio での使用手順

Sysmac Studio での手順は、以下のとおりです。

1 **Sysmac Studio の CIP Safety モニタ画面で、セーフティ I/O ターミナルを選択します。**
以下の画面が表示されます。



2 **［メンテナンス］タブを選択します。**
以下の画面が表示されます。



3 **［ケーブル診断］の［診断実行］ボタンを押します。**

ポート 1 およびポート 2 に対して、ケーブルが正常か断線しているかが表示されます。断線の場合は、ユニットから通信ケーブルが断線している位置までの距離の参考値も表示されます。



Web UI での使用手順

Web UI の通信ケーブル診断画面で、EtherNet/IP 通信ケーブルの断線や短絡の有無を確認します。



［実行］ボタンを押すと、EtherNet/IP ポート 1 の診断結果が［ETH1 ポート］欄に、EtherNet/IP ポート 2 の診断結果が［ETH2 ポート］欄に表示されます。
表示される内容は、以下のいずれかです。

- 01：正常
- 02：短絡（参考値□m） □には、数値が入る。
- 03：断線（参考値□m） □には、数値が入る。
- 04：ポート無効
- F1：診断中
- F2：読み出し失敗
- F3：その他診断異常

Explicit メッセージ通信での使用手順

通信ケーブル診断実行および診断結果取得のための送信コマンドは、以下のとおりです。

実施内容	送信コマンドの項目	送信コマンドの値
通信ケーブル診断実行	サービスコード	3AHex(Exec_Cable_Diagnosis)
	クラス ID	F6Hex（Ethernet Link オブジェクト）
	インスタンス ID	01Hex : Port1 02Hex : Port2
通信ケーブル診断の結果	サービスコード	0EHex(Get_Attribute_Single)
	クラス ID	F6Hex（Ethernet Link オブジェクト）
	インスタンス ID	01Hex : Port1 02Hex : Port2
	アトリビュート ID	100(Communication Cable Diagnosis)
	レスポンスデータ	「Communication Cable Diagnosis の値 (P.A-47)」参照

Explicit メッセージ通信での手順は、「Explicit メッセージサーバ機能 (P.6-6)」を参照してください。

8-13-3 通信ケーブル診断機能の詳細

通信ケーブル診断機能には、以下の制約があります。

- リンクが確立しているポートの診断結果は、常に正常となる。
- 通信ケーブルの送信線と受信線が短絡している場合は、断線を検知できない。診断結果が正常となる。
- コネクションタイムアウト、またはコネクション確立不可が発生している場合、その原因が通信ケーブルの伝送特性によるものであれば、診断結果が正常となる場合がある。

ネットワークトポロジと通信ケーブル診断機能を実行するためのパソコンの接続形態には、以下の関係があります。ネットワークトポロジの詳細は、「1-3-2 ネットワークトポロジ (P.1-13)」を参照してください。

ネットワークトポロジ	パソコンの接続形態
ライン型、リング型	スイッチングハブに接続
スター型、ツリー型	セーフティ I/O ターミナルの未使用の Ethernet ポートに接続

8-14 ファームウェアアップデート機能

ファームウェアアップデート機能は、セーフティ I/O ターミナルの通信機能関係およびセーフティ機能関係のファームウェアを更新する機能です。
最新のファームウェアファイルの入手方法については、オムロンのホームページを確認してください。

8-14-1 ファームウェアアップデート機能の目的

ファームウェアアップデート機能の目的は、セーフティ I/O ターミナルのセキュリティ上の脆弱性を改善することです。

8-14-2 ファームウェアアップデート機能の使用手順

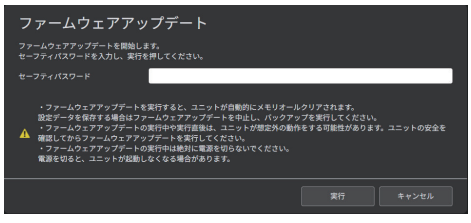
ファームウェアアップデート機能は、Web UI のファームウェアアップデート画面を使用して実行します。
この画面は、管理者の権限を持つユーザだけが設定できます。



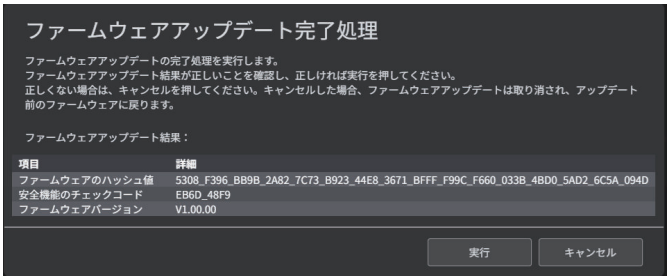
設定の手順は、以下のとおりです。

1 **[ファイル選択] ボタンを押し、パソコン内のファームウェアファイルを選択します。**
選択したファイルが、表示されます。また、選択したファームウェアのハッシュ値、安全機能のチェックコード、およびファームウェアバージョンが表示されます。

2 **ファームウェアのハッシュ値、安全機能のチェックコード、およびファームウェアバージョンに問題がないことを確認して、[決定] ボタンを押します。**
以下のメッセージが表示されます。



3 **セーフティパスワードを入力して、[実行] ボタンを押します。**
以下のメッセージが表示されます。



4 **ファームウェアのハッシュ値、安全機能のチェックコード、およびファームウェアバージョンに問題がないことを確認して、［実行］ボタンを押します。**

ファームウェアアップデート完了処理が実行されます。以下のメッセージが表示されます。



5 **セーフティ I/O ターミナルの電源を再投入します。**

6 **Web UI の生産情報画面で、ファームウェアバージョンが変わっていることを確認します。**

8-14-3 ファームウェアアップデート機能の詳細

ファームウェアアップデート機能を実行した場合、セーフティ I/O ターミナルの状態は、MS LED とユニット特定表示 LED で確認できます。セーフティ I/O ターミナルの状態と MS LED およびユニット特定表示 LED の状態との関係を、以下に示します。

セーフティ I/O ターミナルの状態	MS LED	ユニット特定表示 LED
ファームウェアアップデート準備中	消灯	すべて点灯
ファームウェアアップデート実行中	0.5sON、0.5sOFF で緑点滅	すべて点灯
ファームウェアアップデート成功	緑点灯	すべて点灯
ファームウェアアップデート失敗	赤点灯	すべて点灯

ファームウェアアップデート機能に、ファームウェアバージョンの制約はありません。バージョンアップだけでなく、バージョンダウンすることも可能です。

使用上の注意

- ファームウェアアップデート機能を実行中に電源を OFF しないでください。再起動できなくなる場合があります。

9

安全応答性能

この章では、セーフティ I/O ターミナルの安全応答性能（セーフティリアクションタイム）の計算方法について説明しています。

9-1　セーフティ I/O ターミナルの安全応答性能 9-2
9-1-1　安全応答性能の計算方法 9-2
9-1-2　安全応答性能の検証 9-5

9-1 セーフティ I/O ターミナルの安全応答性能

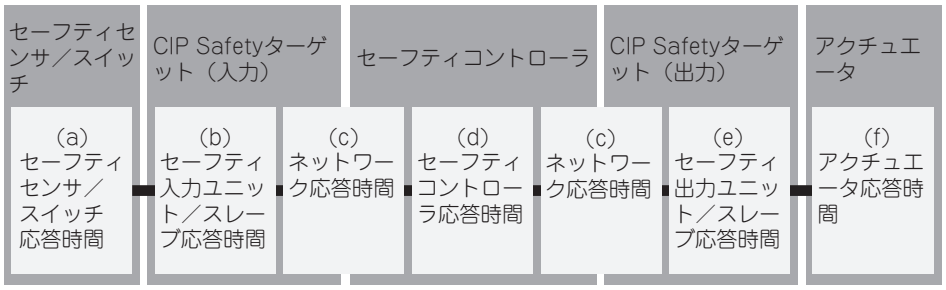
安全応答性能（セーフティリアクションタイム）とは、セーフティチェーン*1 における、障害や故障の発生も考慮した出力遮断に要する最大時間のことです。
安全システム設計においては、安全応答性能から安全距離を求めることになります。
すべてのセーフティチェーンにて、セーフティ入力からの稼動装置の停止までの最長時間が要求仕様を満足している必要があります。
ここでは、セーフティ I/O ターミナルの安全応答性能について説明します。

***1.** セーフティチェーンとは、セーフティ入力機器からセーフティ I/O ターミナルやセーフティコントロールユニットを経由しセーフティ出力までつながる、セーフティ機能を実現するための論理的なつながりのことです。

9-1-1 安全応答性能の計算方法

CIP Safety 通信を使用する場合と使用しない場合に分けて、安全応答性能の計算方法を記載します。

a. CIP Safety 通信を使用してセーフティコントローラで安全制御をする場合
安全応答性能は、下図のように(a)セーフティセンサ／スイッチ応答時間、(b)セーフティ入力ユニット／スレーブ応答時間、(c)ネットワーク応答時間、(d)セーフティコントローラ応答時間、(e)セーフティ出力ユニット／スレーブ応答時間、および(f)アクチュエータ応答時間の和となります。
各要素の数や時間はセーフティチェーンの経路に応じて異なります。



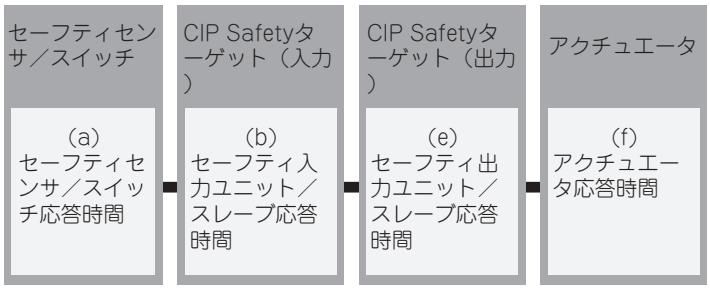
記号	時間要素	値
(a)	セーフティセンサ／スイッチ応答時間	ライトカーテンなどのセーフティセンサやスイッチの ON→OFF 応答時間。使用するセンサ／スイッチにより定義された値です。
(b)	セーフティ入力ユニット／スレーブ応答時間	CIP Safety ターゲットの入力応答時間。 入力端子のチャネルモードと安全要求レベルにより、以下の 3 通りの時間があります。 • デュアルチャネルの場合 10ms • シングルチャネル、かつセーフティ入力の危険側故障がない場合（安全要求レベルが Cat.2/PLc/SIL1） 10ms • シングルチャネルの場合、かつセーフティ入力の危険側故障を考慮した場合（安全要求レベルが Cat.2/PLd/SIL2） 260ms セーフティ I/O ターミナルの入力応答時間は、上記の時間に入力端子の ON→OFF 遅延時間を加算してください。
(c)	ネットワーク応答時間	CIP Safety コネクションの応答時間。 NJ/NX/NY シリーズの場合は、Sysmac Studio で計算、表示されます。*1 ネットワーク応答時間の確認方法については、「コネクションのパラメータ編集手順 (P.7-30)」を参照してください。

記号	時間要素	値
(d)	セーフティコントローラ応答時間	セーフティコントローラの応答時間。 Safety CPU ユニットの場合、『NX シリーズ セーフティコントロールユニット／通信コントロールユニット ユーザーズマニュアル(SGFM-723)』を参照してください。*1
(e)	セーフティ出力ユニット／スレーブ応答時間	CIP Safety ターゲットの出力応答時間。 出力端子のチャネルモードと安全要求レベルにより、以下の 2 通りの時間があります。 • デュアルチャネルの場合 5ms • シングルチャネルの場合 5ms（シングルチャネルは Up to Cat.2 であるため、故障がない前提の応答時間） セーフティ I/O ターミナルの出力応答時間は、上記の時間に出力端子の ON→OFF 遅延時間を加算してください。 また、セーフティ I/O ターミナルのロジック機能を使用する場合、ロジック実行時間もこの時間に含まれます。
(f)	アクチュエータ応答時間	セーフティリレーなどのアクチュエータの ON→OFF 応答時間。使用するアクチュエータにより定義された値です。

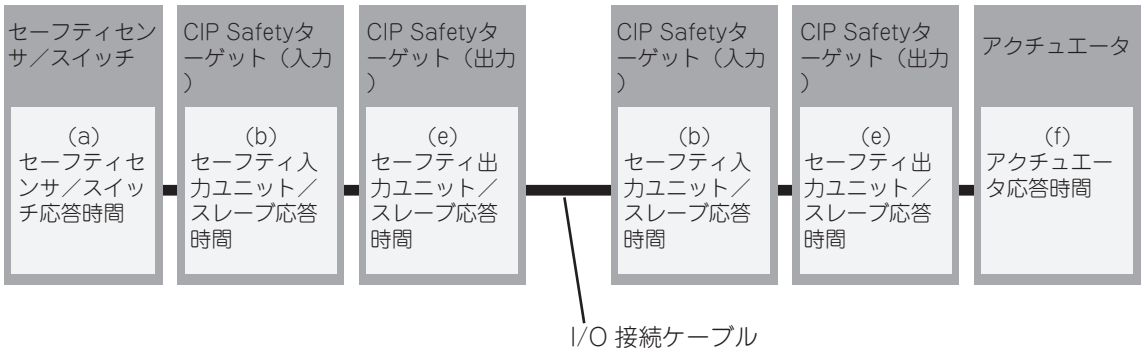
***1.** 他社コントローラに接続する場合は、接続するコントローラのサポートソフトの取扱説明書を確認してください。

b. CIP Safety 通信を使用しないで安全アプリケーションで安全制御をする場合
安全応答性能は、セーフティ I/O ターミナル内で入出力の処理を行うため、a.の(c)と(d)の時間を除外します。

• セーフティ I/O ターミナル単体の構成



• 2 台のセーフティ I/O ターミナルを I/O 接続ケーブルで接続する構成
安全応答性能は、(b)と(e)の合計時間をセーフティ I/O ターミナルの接続台数分加算します。



使用上の注意

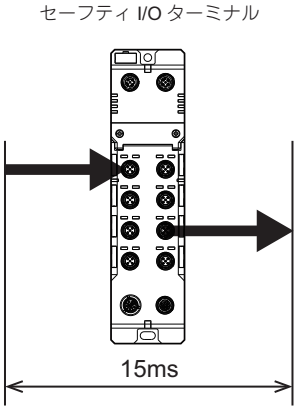
• 安全応答性能の計算は、“入力端子の ON→OFF 遅延時間”および“出力端子の ON→OFF 遅延時間”の影響分を加算してください。

セーフティ I/O ターミナル単体構成時

セーフティ I/O ターミナル単体のスレーブ応答時間（入出力応答時間）は、セーフティ入力およびセーフティ出力の設定の組み合わせによって、以下のとおりです。

セーフティ入力	セーフティ出力	安全要求レベル	スレーブ応答時間
デュアルチャネル	デュアルチャネル	Cat.4/PLe/SIL3	15ms (=10ms+5ms)
デュアルチャネル	シングルチャネル	Cat.2/PLc/SIL1	15ms (=10ms+5ms)*1
シングルチャネル	デュアルチャネル	Cat.2/PLd/SIL2	265ms (=260ms+5ms)
シングルチャネル	シングルチャネル	Cat.2/PLc/SIL1	15ms (=10ms+5ms)*1

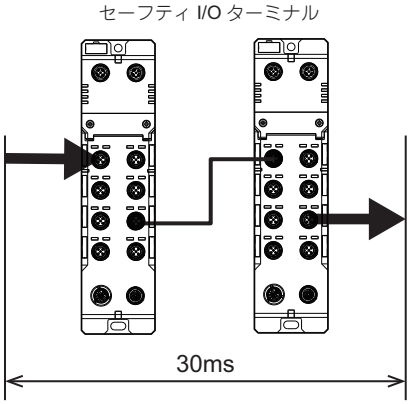
***1.** 安全要求レベルは Cat2/PLc/SIL1 であり、故障がない前提の応答時間です。セーフティ出力をシングルチャネルで使用する場合、故障検出時間は 265ms ＋ネットワーク応答時間となります。故障の状態は、CIP Safety 通信または EtherNet/IP 通信の Input アセンブリの出力端子ステータスに反映されます。詳細は「2-1-3 安全仕様 (P.2-4)」を参照してください。



I/O ケーブル接続構成時

セーフティ I/O ターミナルを I/O ケーブルで 2 台接続し、以下の条件で安全アプリケーションを使用する場合の入出力応答性能は、30ms となります。

- CIP Safety 通信を使用していない
- 安全入力端子と安全出力端子をすべてデュアルチャネルに設定している
- “入力端子の ON→OFF 遅延時間”および“出力端子の ON→OFF 遅延時間”を加算していない



9-1-2 安全応答性能の検証

すべてのセーフティチェーンで、算出した安全応答性能が要求仕様を満たしているかを確認してください。
算出した安全応答性能が要求仕様を満たしていない場合は、以下のいずれかを検討して、ソフトウェア設計またはハードウェア設計を見直してください。

- CIP Safety コネクションのデータパケットインターバル(EPI)値を小さくする。
  データパケットインターバル(EPI)は、「コネクションのパラメータ編集手順 (P.7-30)」を参照してください。

10

セキュリティガイドライン

この章では、セーフティ I/O ターミナルを使用するうえでのセキュリティガイドラインについて説明しています。
FA システム全体としてのセキュリティ対策については、『FA システム セキュリティガイドライン(SBCA-140)』を参照してください。また、NJ/NX シリーズ CPU ユニットを用いて実施できるセキュリティ対策については、『NJ/NX コントローラ セキュリティガイドライン(SBCA-142)』を参照してください。

10-1 セーフティ I/O ターミナルによる多層防御 10-2
10-1-1 セーフティ I/O ターミナルの使用環境 10-2
10-1-2 セーフティ I/O ターミナルを活用した技術層のセキュリティ対策 10-3

10-2 資産を守るセーフティ I/O ターミナルのセキュリティ機能 10-5
10-2-1 通信回線上のデータを保護する 10-5
10-2-2 セーフティ I/O ターミナルへの外部からの攻撃を遮断する 10-7
10-2-3 セーフティ I/O ターミナルの不正操作を防止する 10-9
10-2-4 セーフティ I/O ターミナルの資産の改ざんを防止する 10-10
10-2-5 安全アプリケーションファイル、バックアップファイルを保護する 10-11
10-2-6 否認を防止する 10-12

10-3 セキュリティパッチを適用する 10-13
10-3-1 セーフティ I/O ターミナルをアップデートする 10-13
10-3-2 Sysmac Studio をアップデートする 10-13
10-3-3 パソコンの OS をアップデートする 10-13

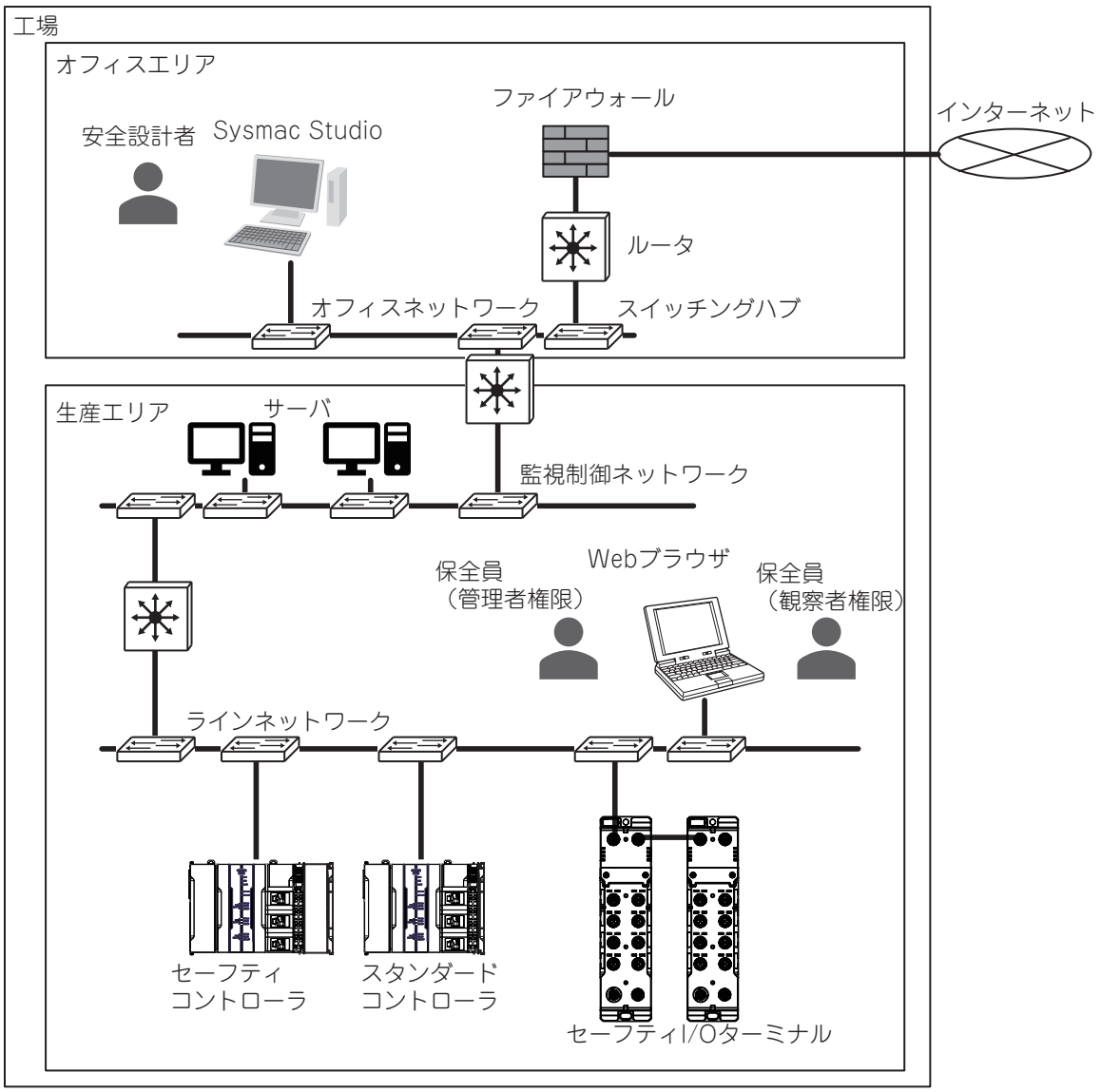
10-4 装置を安全に廃棄する 10-14
10-4-1 セーフティ I/O ターミナル内の資産を消去する 10-14

10-1 セーフティ I/O ターミナルによる多層防御

セーフティ I/O ターミナルは複数のセキュリティ機能により、多層防御を実現します。
ここでは、セーフティ I/O ターミナルのセキュリティ機能が実現する多層防御について説明します。

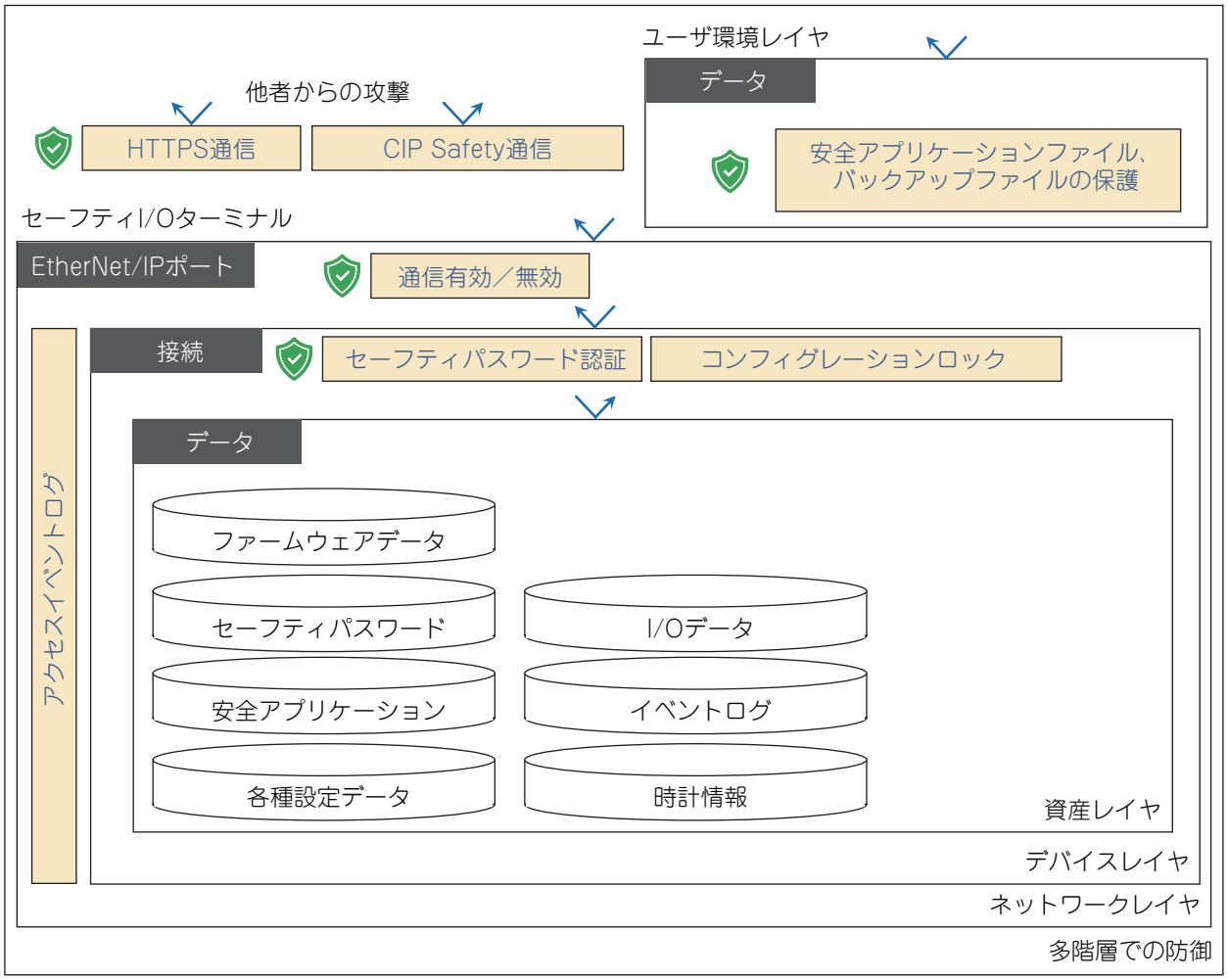
10-1-1 セーフティ I/O ターミナルの使用環境

セーフティ I/O ターミナルは、そのセキュリティ機能を有効に活用することにより、装置やセーフティ I/O ターミナルの動作や資産を守ります。
下図のように、ネットワークをオフィスエリアと生産エリアに分けるなどのセグメント化を行うと、外部から攻撃を受けた場合の影響範囲を小さくするのに有効です。また、セーフティ I/O ターミナルの周辺機器へのセキュリティ対策も実施してください。具体的な方法は、周辺機器のマニュアルを参照してください。



10-1-2 セーフティ I/O ターミナルを活用した技術層のセキュリティ対策

セーフティ I/O ターミナルは守るべき資産に対し、多層防御で保護できるようにセキュリティ機能を搭載しています。攻撃者がひとつの層を突破できたとしても、資産により近い層のセキュリティ機能により、資産を守ることができます。
目的、脅威に応じて、『FA システム セキュリティガイドライン(SBCA-140)』に示す対策、および本章で示す複数のセキュリティ機能を組み合わせて、多層防御を講じてください。
なお、本章ではお客様に特に対応いただきたいことを各セキュリティ機能の説明に示しています。併せてお読みいただき、対策を実施してください。
また、各セキュリティ機能が意図したとおりに動作していることをお客様自身で必ず確認してください。



各レイヤで提供している機能を以下に示します。

資産を守るレイヤ	目的	セーフティ I/O ターミナルが搭載している機能	参照先
ネットワークレイヤ	通信回線上のデータを保護する	HTTPS 通信機能(Web UI)	「HTTPS 通信機能(Web UI) (P.10-5)」
		CIP Safety 通信機能	「CIP Safety 通信機能 (P.10-5)」
	セーフティ I/O ターミナルへの外部からの攻撃を遮断する	通信有効／無効設定機能	「通信有効／無効設定機能 (P.10-7)」
デバイスレイヤ	セーフティ I/O ターミナルの不正操作を防止する	セーフティパスワード認証機能	「セーフティパスワード認証機能 (P.10-9)」
	セーフティ I/O ターミナルの資産の改ざんを防止する	コンフィグレーションロック機能	「コンフィグレーションロック機能 (P.10-10)」

資産を守るレイヤ	目的	セーフティ I/O ターミナルが搭載している機能	参照先
ユーザ環境レイヤ	安全アプリケーションファイル、バックアップファイルを保護する	安全アプリケーションファイル、バックアップファイルの保護	「安全アプリケーションファイル、バックアップファイルの保護 (P.10-11)」
レイヤ共通	否認を防止する	アクセスイベントログ機能	「アクセスイベントログ機能 (P.10-12)」

10-2 資産を守るセーフティ I/O ターミナルのセキュリティ機能

ここでは、セーフティ I/O ターミナルが搭載しているセキュリティ機能について説明します。

10-2-1 通信回線上のデータを保護する

ネットワークに接続する装置では、ネットワークを介してサイバー攻撃を受けるリスクがあります。通信回線を流れるデータからの情報漏えいや改ざん、サービス妨害を防止します。

HTTPS 通信機能(Web UI)

HTTPS 通信機能は、Web ブラウザとセーフティ I/O ターミナル間の通信のセキュリティ向上を目的とした機能です。
通信データを暗号化し、またハッシュ値を付けて送受信を行うため、第三者による通信データの盗聴や改ざんを防止するのに役立ちます。
HTTPS 通信機能の詳細については、「7-2 Web UI の概要 (P.7-16)」を参照してください。

● 対策できる脅威

S: なりすまし	T: 改ざん	R: 否認	I: 情報漏えい	D: サービス妨害	E: 権限昇格
○	○		○	○	

● お客様に実施していただきたいこと

- セキュリティ性向上のために、最新バージョンの Web ブラウザで Web UI を使用してください。
- 制御システムや装置のネットワークはファイアウォール（未使用通信ポートの遮断、通信ホストの制限）を導入し、IT ネットワークからの分離を行い、Web UI のセーフティコントロールシステムへの接続はファイアウォール内で行うようにしてください。
- Web UI から制御システムや装置へのリモートアクセスが必要な場合は、仮想プライベートネットワーク(VPN)を使用してください。
- HTTPS 通信機能を使用するには、CA 証明書が必要です。オムロンのホームページから CA 証明書をダウンロードし、Web ブラウザにインストールしてください。CA 証明書がない状態で、セーフティ I/O ターミナルにアクセスすると、Web ブラウザでエラーが出ます。詳細は、「8-3 HTTPS 通信機能 (P.8-8)」を参照してください。
- Web UI を起動する方法には、IP アドレスを入力する方法とドメインを入力する方法があります。IP アドレスを入力する方法を使用する場合は、パソコンとセーフティ I/O ターミナルの間に不正デバイスが介入して情報が漏えいすることがないように対策を実施してください。対策の詳細は、「7-2-5 Web UI の起動手順 (P.7-19)」を参照してください。

CIP Safety 通信機能

CIP Safety 通信機能は、CIP Safety オリジネータ（セーフティコントローラ）と CIP Safety ターゲット（セーフティ I/O ターミナル）間でサイクリックにデータ交換するための安全機能です。TUNID、SCCRC、および SCTS などの仕組みにより通信の信頼性を保証します。
CIP Safety 通信機能の詳細については、「6-2 CIP Safety 通信 (P.6-4)」を参照してください。

● 対策できる脅威

S: なりすまし	T: 改ざん	R: 否認	I: 情報漏えい	D: サービス妨害	E: 権限昇格
○	○			○	

10-2-2 セーフティ I/O ターミナルへの外部からの攻撃を遮断する

インターネットに接続する装置では、ネットワークを介してサイバー攻撃を受けるリスクがあります。外部からの攻撃を遮断し、生産装置の異常や事故を防止します。

通信有効／無効設定機能

通信有効／無効設定機能は、セーフティ I/O ターミナルが持つ各通信機能を有効にしたり無効にしたりする機能です。使用しない通信機能を無効化し、外部からセーフティ I/O ターミナルへのアクセス経路を減らすことで情報漏えいや攻撃を防止します。
通信有効／無効設定機能は、以下の対象に対して実行できます。

対象	内容
EtherNet/IP ポート	EtherNet/IP ポート 1、2 での Ethernet 通信機能を、ポートごとに有効または無効に設定できる。工場出荷状態では、いずれのポートも有効。
DHCP（IP アドレス設定）	DHCP サーバから IP アドレスを取得する機能を、有効または無効に設定できる。工場出荷状態では、無効。
SNTP（時計情報自動調整機能）	SNTP サーバから時計情報を取得する機能を、有効または無効に設定できる。工場出荷状態では、無効。

● EtherNet/IP ポートの通信有効／無効設定

EtherNet/IP ポートの通信有効／無効設定は、Explicit メッセージ通信を使用して行います。
送信コマンドは、以下のとおりです。

実施内容	送信コマンドの項目	送信コマンドの値
EtherNet/IP ポートの通信有効／無効設定	サービスコード	10Hex(Set_Attribute_Single)
	クラス ID	F6Hex(Ethernet Link オブジェクト)
	インスタンス ID	01Hex : Port1 02Hex : Port2
	アトリビュート ID	101(Communication Port Enable)
	サービスデータ	TRUE : 有効 FALSE : 無効

CIP オブジェクトへの Explicit メッセージによるアクセス方法は、「Explicit メッセージサーバ機能 (P.6-6)」を参照してください。

● DHCP の通信有効／無効設定

Sysmac Studio で DHCP の通信有効／無効設定を行うには、IP アドレスを設定する画面で、［DHCP サーバから取得］を以下のように設定します。
Web UI で DHCP の通信有効／無効設定を行うには、Web UI の TCP/IP 設定画面で、IP アドレスの［DHCP サーバから取得］を以下のように設定します。

DHCP の通信	［DHCP サーバから取得］
有効	チェックを入れる。
無効	チェックをはずす。

Sysmac Studio で IP アドレスを設定する手順は、「7-10-3 Sysmac Studio による設定 (P.7-72)」を参照してください。
Web UI の TCP/IP 設定画面の詳細は、「7-10-4 Web UI による設定 (P.7-74)」を参照してください。

● SNTP の通信有効／無効設定

Sysmac Studio で SNTP の通信有効／無効設定を行うには、時計情報自動調整機能を設定する画面で、［SNTP 設定］を以下のように設定します。
Web UI で SNTP の通信有効／無効設定を行うには、Web UI の時計情報自動調整機能設定画面で、［NTP/SNTP サーバ IP アドレス］を以下のように設定します。

SNTP の通信	設定
有効	IP アドレスを設定する。
無効	IP アドレスを設定しない。

Sysmac Studio で時計情報自動調整機能の設定を行う手順は、「Sysmac Studio での使用手順 (P.7-87)」を参照してください。
Web UI の時計情報自動調整機能設定画面の詳細は、「Web UI での使用手順 (P.7-88)」を参照してください。

● 対策できる脅威

S: なりすまし	T: 改ざん	R: 否認	I: 情報漏えい	D: サービス妨害	E: 権限昇格
○	○		○	○	

● お客様に実施していただきたいこと

- DHCP および SNTP プロトコルでは、セキュリティ対応していません。DHCP および SNTP プロトコルをご使用になる場合は、お客様のアプリケーションにてセキュリティを確保してください。
- ファイアウォールを設置してセーフティ I/O ターミナルに不正なパケットが到達しないようにするなど、他の対策と組み合わせて使用してください。

10-2-3 セーフティ I/O ターミナルの不正操作を防止する

セーフティ I/O ターミナルの不正操作を防止し、お客様の大切な知的財産である安全アプリケーションや装置を、盗用、不正利用、および生産装置の異常や事故から守ります。

セーフティパスワード認証機能

セーフティ I/O ターミナルの設定データの変更や操作は、人的被害や物的被害を与える危険性があります。操作者の権限により操作できる機能を制限し、権限を持たない操作者からの操作を防止します。セーフティ I/O ターミナルのセーフティパスワード認証の機能は以下のとおりです。

機能	内容
機能安全に影響する操作の制限	メモリオールクリア、再起動、コンフィグレーションロックとロック解除、動作モード変更、およびセーフティパスワードの機能を実行する場合に、セーフティパスワードによる認証が必要である。
Web UI の操作の制限	Web UI には、管理者と観察者の操作権限がある。設定データの変更ができるのは管理者だけである。管理者として Web UI を使用するには、セーフティパスワードによる認証が必要である。

機能安全に影響する操作の制限の詳細は、各機能のページを参照してください。Web UI の操作権限の詳細は、「7-2-2 Web UI の操作権限 (P.7-16)」を参照してください。セーフティパスワードの設定の詳細は、「7-18 セーフティパスワードの設定 (P.7-100)」を参照してください。

● 対策できる脅威

S: なりすまし	T: 改ざん	R: 否認	I: 情報漏えい	D: サービス妨害	E: 権限昇格
○	○	○	○	○	○

● お客様に実施していただきたいこと

- セーフティ I/O ターミナルには、必ずセーフティパスワードを設定してください。
- セーフティパスワードはお客様ご自身で、定期的に変更してください。
- セーフティパスワードが第三者に不正利用されないよう適切な設定、管理をしてください。
- ブルートフォース攻撃などによるパスワード解析が想定されるため、複雑なパスワード（8 文字以上、複数の文字種別）を設定してください。
- セーフティパスワードの機密性を高めるため、他の装置と同じパスワードを設定しないでください。
- 本製品が準拠する CIP Safety は、工場などの FA 用途において機器安全の実現を目的としたセーフティ通信の仕組みです。本製品に対する不正操作などのセキュリティリスクについては、本製品の機能に加え、生産エリアへの入退室やネットワークへのアクセス制限など、システム全体として適切な対策を講じてください。

10-2-4 セーフティ I/O ターミナルの資産の改ざんを防止する

お客様の大切な知的財産である設定データの改ざんや、意図しない安全アプリケーションの不正実行を防止します。

コンフィグレーションロック機能

コンフィグレーションロック機能は、セーフティ I/O ターミナルのセーフティ関連の設定データや、実行する安全アプリケーションが意図せずに変更されることを防止する機能です。コンフィグレーションロック状態のセーフティ I/O ターミナルは、設定データの変更ができません。また、選択中の安全アプリケーションを変更し、別の安全アプリケーションを実行することができません。
コンフィグレーションロック機能の詳細は、「7-17 コンフィグレーションロック (P.7-95)」を参照してください。

● 対策できる脅威

S: なりすまし	T: 改ざん	R: 否認	I: 情報漏えい	D: サービス妨害	E: 権限昇格
	○				

● お客様に実施していただきたいこと

- セーフティ I/O ターミナルの本稼働前に、必ずコンフィグレーションロックを実施してください。

10-2-5 安全アプリケーションファイル、バックアップファイルを保護する

お客様の大切な知的財産である設計資産の不正利用を防止します。

安全アプリケーションファイル、バックアップファイルの保護

ファイルの不正利用を防ぐため、安全アプリケーションファイルおよびバックアップファイルは、パスワードで保護されています。ファイルを保護するパスワードは、それぞれ安全アプリケーションファイルパスワード、バックアップファイルパスワードです。
安全アプリケーションファイルパスワードの詳細は、「7-9-5 安全アプリケーションファイルのエクスポート (P.7-66)」を参照してください。バックアップファイルパスワードの詳細は、「7-19 バックアップ (P.7-104)」を参照してください。

● 対策できる脅威

S: なりすまし	T: 改ざん	R: 否認	I: 情報漏えい	D: サービス妨害	E: 権限昇格
	○				

● お客様に実施していただきたいこと

- 安全アプリケーションファイルパスワード、バックアップファイルパスワードが第三者に不正利用されないよう適切な設定、管理をしてください。
- ブルートフォース攻撃などによるパスワード解析が想定されるため、複雑なパスワード（8 文字以上、複数の文字種別）を設定してください。

10-2-6 否認を防止する

資産を守るためには、不正な操作をされたことを把握することも大切です。また、セキュリティインシデントの発生時にはその原因や経緯を明らかにする必要があります。セキュリティ違反やサイバー攻撃を記録することにより、誰が、いつ、何の操作をしたかを確認することができ、問題発生時の否認防止として使うことができます。

アクセスイベントログ機能

セーフティ I/O ターミナルでは、セーフティ I/O ターミナルに対してユーザが Sysmac Studio や Web UI を使用して行った操作をアクセスイベントログとして登録します。アクセスイベントログは、Sysmac Studio または Web UI を用いて読み出しやクリアができます。
アクセスイベントログ機能の詳細は、「11-2-1 イベントログ機能 (P.11-6)」を参照してください。

● 対策できる脅威

S: なりすまし	T: 改ざん	R: 否認	I: 情報漏えい	D: サービス妨害	E: 権限昇格
		○			

● お客様に実施していただきたいこと

- アクセスイベントログがクリアされると否認防止できません。セーフティ I/O ターミナルのアクセスイベントログは、記録可能件数を超えてイベントが発生した場合、古い情報から上書きされます。定期的にバックアップを取り、一定期間保存することを推奨します。

10-3 セキュリティパッチを適用する

日々進歩するサイバー攻撃から資産や生産を守るためには、使用している機器を最新の状態にしてセキュリティ強度を高めることが有効です。
ここでは、アップデートに関し、セーフティ I/O ターミナルが搭載している機能について説明します。

10-3-1 セーフティ I/O ターミナルをアップデートする

機能の追加や操作性の改善、セキュリティの強化のため、セーフティ I/O ターミナルは、常に最新のバージョンにアップデートして使用してください。

ファームウェアアップデート機能

ファームウェアアップデート機能は、セーフティ I/O ターミナルが使用するファームウェアを最新のバージョンにアップデートする機能です。
ファームウェアアップデート機能の詳細は、「8-14 ファームウェアアップデート機能 (P.8-34)」を参照してください。
ファームウェアアップデートをした場合、イベントログに記録が残ります。変更履歴を参照する時は「11-2-1 イベントログ機能 (P.11-6)」で確認してください。
最新のファームウェアファイルの入手方法については、オムロンのホームページを確認してください。

● お客様に実施していただきたいこと

- セーフティ I/O ターミナルのファームウェアが最新のバージョンになっているか、定期的に確認してください。
- ファームウェアアップデート機能実行後にバックアップファイルをリストアした場合は、セキュリティ性を向上させるため、セーフティパスワードを設定してください。

10-3-2 Sysmac Studio をアップデートする

機能の追加や操作性の改善、セキュリティの強化のため、Sysmac Studio は、常に最新のバージョンにアップデートして使用してください。
Sysmac Studio のオートアップデートの詳細は、『Sysmac Studio Version 1 オペレーションマニュアル (SBCA-470)』を参照してください。

10-3-3 パソコンの OS をアップデートする

OS の脆弱性に起因するセキュリティリスクを回避するために、SysmacStudio、Web UI、およびその周辺ツールを使用するパソコンの OS を常に最新の状態にしてください。

10-4 装置を安全に廃棄する

ここでは、廃棄に関し、セーフティ I/O ターミナルが搭載している機能について説明します。

10-4-1 セーフティ I/O ターミナル内の資産を消去する

セーフティ I/O ターミナルを廃棄、または譲渡する場合、セーフティ I/O ターミナルに保存している設定データなどの情報を第三者に見られて、情報が漏えいするおそれがあります。
廃棄、または譲渡する前に、お客様が責任を持って設定データを消去してください。

メモリオールクリア機能

メモリオールクリア機能は、セーフティ I/O ターミナル内の設定データを完全に消去する機能です。設定データを完全に消去するには、Web UI でメモリオールクリア機能を選択し、「イベントログ」、「Web UI で設定した安全アプリケーション」も消去してください。Sysmac Studio のメモリクリア機能を実行した場合は、「イベントログ」や「Web UI で設定した安全アプリケーション」は消去されないので注意してください。
メモリオールクリア機能の詳細は、「8-2 メモリオールクリア機能 (P.8-4)」を参照してください。
メモリオールクリアに失敗する場合は、セーフティ I/O ターミナルの故障が考えられます。最寄りの当社支店、営業所までご連絡ください。

11

異常発生時の処置

この章では、セーフティ I/O ターミナルの異常発生有無の確認方法と、異常発生時の対処方法について説明しています。

11-1 異常の確認 11-2
11-1-1 異常の通知方法と確認する情報 11-2
11-1-2 異常の確認手順 11-2
11-1-3 動作状態モニタ機能 11-3

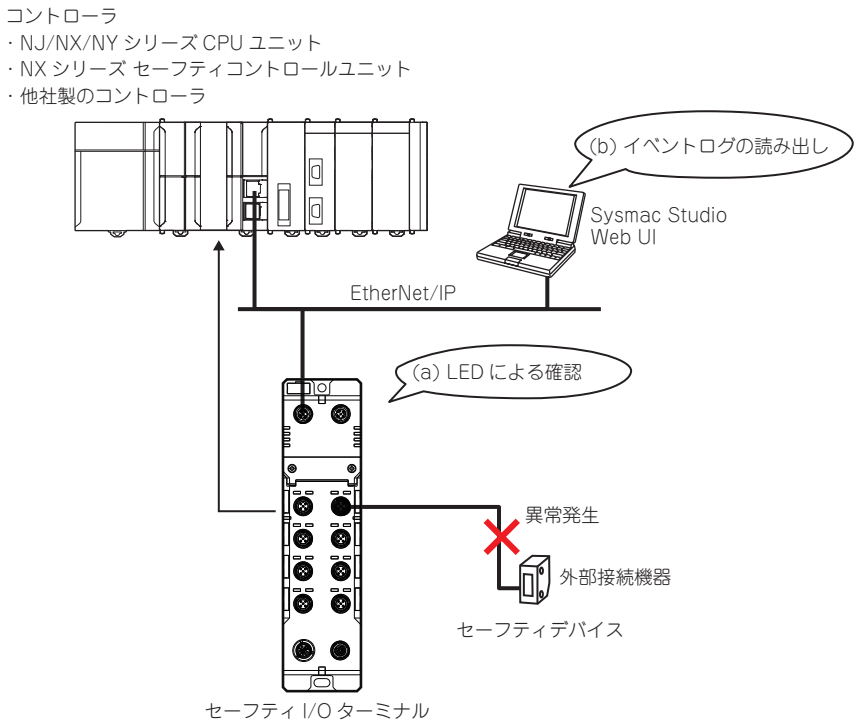
11-2 イベントによる異常の確認と対処方法 11-6
11-2-1 イベントログ機能 11-6
11-2-2 Sysmac Studio によるイベントの確認 11-6
11-2-3 Web UI によるイベントの確認方法 11-9
11-2-4 イベントの内容と対処方法 11-12

11-1 異常の確認

ここでは異常の通知と確認方法、および異常を確認するための基本的な手順について説明します。

11-1-1 異常の通知方法と確認する情報

セーフティ I/O ターミナルは、異常を検出すると以下の方法で通知します。
異常が通知された場合、ユニットの状態を確認して対処します。



記号	通知方法	確認方法	参照
(a)	セーフティ I/O ターミナルの異常を LED で通知	セーフティ I/O ターミナルの各 LED の状態を目で確認	「3-2-1 ステータス LED (P.3-5)」 「3-2-2 I/O LED (P.3-7)」
(b)	セーフティ I/O ターミナルの異常発生とその内容をイベントで通知	セーフティ I/O ターミナルのイベントを Sysmac Studio の CIP Safety モニタ画面、または Web UI の動作状態モニタ画面で読み出して確認	「11-2 イベントによる異常の確認と対処方法 (P.11-6)」

11-1-2 異常の確認手順

異常を確認するための基本的な手順は以下のとおりです。

手順	項目	内容	参照
1	異常発生の把握	LED の点灯状態で、異常発生有無を把握する。	「3-2-1 ステータス LED (P.3-5)」 「3-2-2 I/O LED (P.3-7)」

手順	項目	内容	参照
2	異常原因の特定	異常が発生しているときは、以下を確認して原因を特定する。	—
		セーフティ I/O ターミナル各ステータス情報を確認する。	「11-1-3 動作状態モニタ機能 (P.11-3)」
		セーフティ I/O ターミナルのイベントログを確認する。	「11-2 イベントによる異常の確認と対処方法 (P.11-6)」
3	異常原因の対処	異常原因を特定したら、その対処をする。	—

11-1-3 動作状態モニタ機能

動作状態モニタ機能は、セーフティ I/O ターミナルの各ステータス情報を表示する機能です。

動作状態モニタ機能の目的

動作状態モニタ機能の目的は、各ステータス情報から、セーフティ I/O ターミナルの現在の状況を把握することです。

動作状態モニタ機能の使用手順

Web UI の動作状態モニタ画面で、当該ユニットの動作状態を確認します。



動作状態モニタ機能の詳細

動作状態モニタ機能では、［ユニットステータス］、［電源ステータス］、［コネクションステータス］、［通信設定］および［セーフティ設定］が確認できます。

● ユニットステータス

［ユニットステータス］には［動作モード］、［コンフィグレーションロック］、［発生中異常］、および［I/O 端子］が表示されます。

a. 動作モード
現在の動作モードが表示されます。動作モードの詳細については、「6-8 動作モード (P.6-47)」を参照してください。

b. 発生中異常
［発生中異常］として表示される情報は、以下のとおりです。

表示	内容
正常	ユニットが正常な状態
異常発生中	ユニットで異常が発生している状態

［異常発生中］が表示された場合、［詳細］ボタンを押すと、「発生中異常・イベントログ画面」に遷移します。

c. コンフィグレーションロック
［コンフィグレーションロック］として表示される情報は、以下のとおりです。

表示	内容
コンフィグレーションロック中	コンフィグレーションロックが実行されている状態
コンフィグレーションロック解除中	コンフィグレーションロックが解除されている状態

コンフィグレーションロック機能の詳細は、「7-17 コンフィグレーションロック (P.7-95)」を参照してください。

d. I/O 端子
［I/O 端子］として表示される情報は、以下のとおりです。

表示	内容
正常	セーフティ入出力端子が正常な状態
異常発生中	セーフティ入出力端子で異常が発生している状態

［異常発生中］が表示された場合、［詳細］ボタンを押すと、「I/O モニタ画面」に遷移します。

● 電源ステータス

［電源ステータス］には、各電源端子の状態と数値が表示されます。表示される情報は、以下のとおりです。

項目	内容
状態	正常または異常*1
詳細	電圧値、電流値

***1.** 出力用電源（PWR OUT ポート）を使用していない場合は、出力用電源（PWR OUT ポート）の状態欄に OFF と表示されます。

● 通信設定

［通信設定］には、各種通信設定情報が表示されます。表示される情報は、以下のとおりです。

- IP アドレス
- サブネットマスク
- デフォルトゲートウェイ
- MAC アドレス
- SNN（Safety Network Number）
- TUNID(Target Unit Network Identifier)

- ETH1 ポートが有効か無効か、および通信速度と通信モード
- ETH2 ポートが有効か無効か、および通信速度と通信モード

● セーフティ設定

［セーフティ設定］には、各種セーフティ設定情報が表示されます。表示される情報は、以下のとおりです。

項目	内容
コンフィグレーション	コンフィグレーション済みまたはコンフィグレーション無し
ロータリスイッチ(SETTING)	SETTING のロータリスイッチの値
CFUNID	CFUNID（Configuration Unique Identification）の値
アプリケーション名	設定されている安全アプリケーションの名称
作者名	設定されている安全アプリケーションの作者名
コメント	任意のコメント
SCCRC	SCCRC（Safety Configuration CRC)の値
SCTS	SCTS(Safety Configuration Time Stamp)の値

また、パラメーター覧として、すべてのコンフィグレーションアセンブリデータの値を表示することもできます。コンフィグレーションアセンブリデータの詳細は、「A-2-3 コンフィグレーションアセンブリデータ (P.A-7)」を参照してください。

11-2 イベントによる異常の確認と対処方法

ここでは発生中異常のイベントやイベントログによる異常の確認と対処方法について説明します。
イベントの確認は、Sysmac Studio または Web UI を使用します。

11-2-1 イベントログ機能

イベントログログ機能は、以下のカテゴリに分類してイベントを記録する機能です。

a. システムイベントログ
セーフティ I/O ターミナル内部で発生した状態変化や安全停止の原因、通信異常などを記録します。
安全機能が正しく動作しているかの確認、異常や停止原因の特定、および安全性維持に活用することを目的とします。

b. アクセスイベントログ
ユーザまたは他のデバイスがセーフティ I/O ターミナルに対して行った設定やコマンド実行を記録します。
データ改ざんや情報漏えいなどのセキュリティ上の問題発生時に実行者を特定する、または実行者の否認を防止することを目的とします。

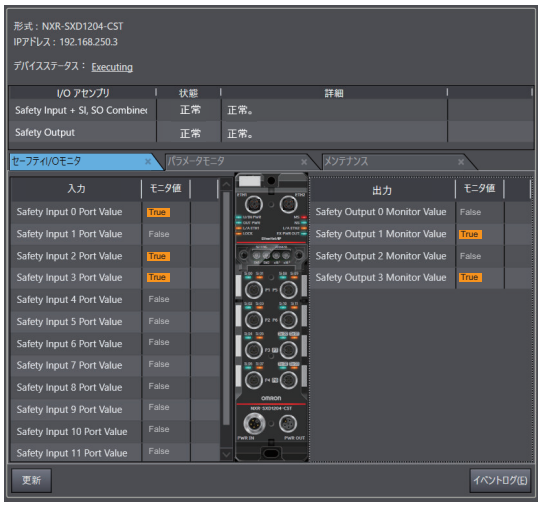
11-2-2 Sysmac Studio によるイベントの確認

発生中異常画面およびイベントログ画面でイベントを確認できます。

発生中異常画面およびイベントログ画面の表示方法

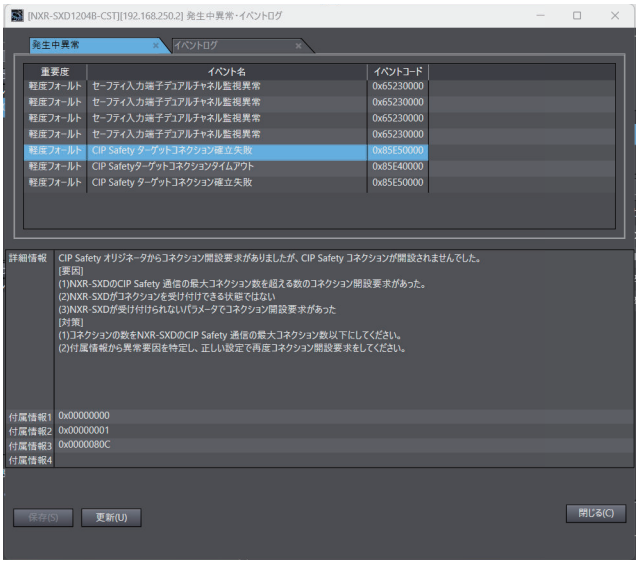
Sysmac Studio による発生中異常およびイベントログのイベントを表示する方法を記載します。

1 **［ツール］-［CIP Safety モニタ］をクリックし、CIP Safety モニタ画面を立ち上げます。**

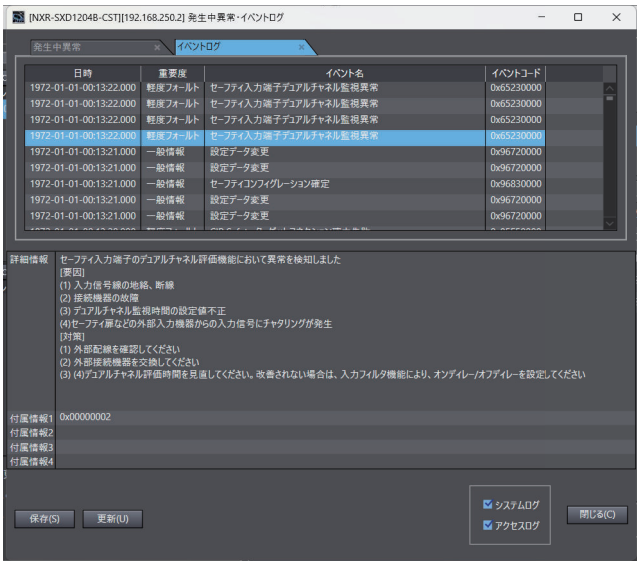


2 **［CIP Safety ターゲット一覧］からセーフティ I/O ターミナルを選択します。**
セーフティ I/O ターミナルのデバイスステータス、I/O アセンブリの発生中異常が表示されます。

3 **右下にある［イベントログ］ボタンをクリックします。**
発生中異常が表示されます。

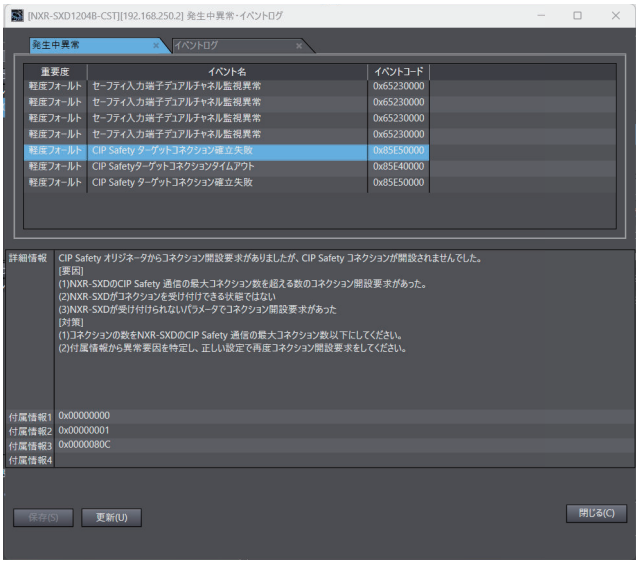


4 **[イベントログ] タブをクリックします。**
イベントログが表示されます。



発生中異常画面

発生中異常画面の表示項目および操作ボタンの機能を説明します。



- 表示項目

項目	内容
重要度	異常（イベント）による制御に対する影響の大きさを表します。
イベント名	発生したイベント名を表示します。
イベントコード	セーフティ I/O ターミナルで発生した異常（イベント）のコードです。
詳細情報	選択されたイベントの要因、対策、および付属情報が表示されます。
付属情報 1～4	

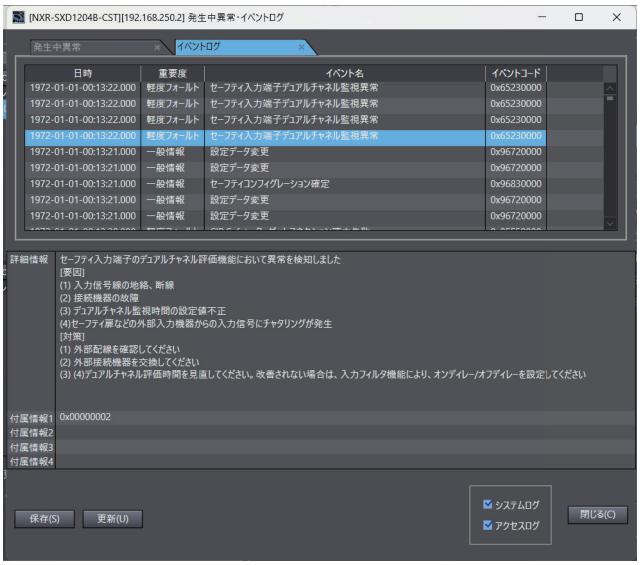
- 操作ボタン

  a）更新

  発生中異常の情報を最新に更新します。

イベントログ画面

イベントログ画面の表示項目および内容は下記のとおりです。



- 表示項目

項目	内容
日時	発生した日時を表示します。*1
重要度	異常（イベント）による制御に対する影響の大きさを表します。
イベント名	発生したイベント名を表示します。 本ユニットでは、最新 100 件が表示可能です
イベントコード	セーフティ I/O ターミナルで発生した異常（イベント）のコードです。
詳細情報	選択されたイベントの要因、対策、および付属情報が表示されます。
付属情報 1～4	

***1.** 本ユニットが時刻情報を持っていないときは、“-----”と表示されます。

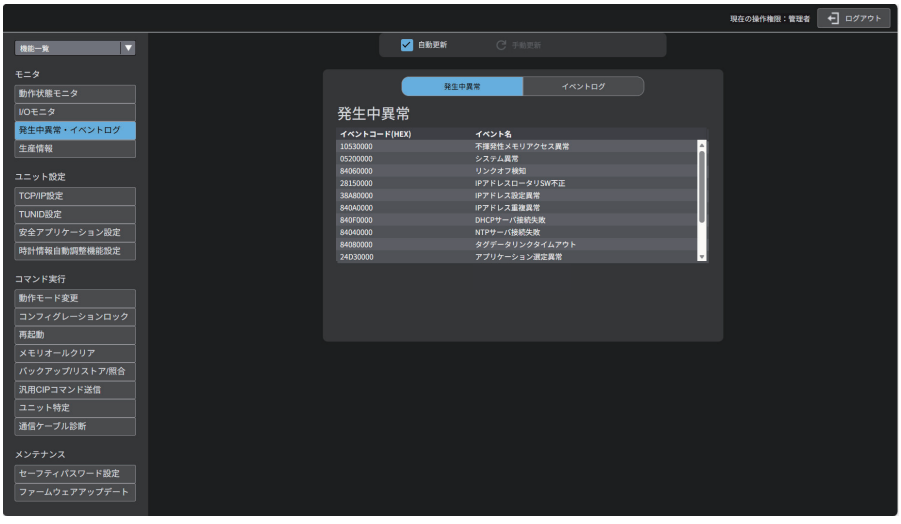
- 操作ボタン
  a）更新
  イベントログのデータを最新に更新します。
  b）保存
  イベントログの保存します。
  c）クリア
  イベントログを消去します。消去するにはセーフティパスワードが必要です。
  d）「システムログ」と「アクセスログ」のチェックボックス
  選択したログが表示されます。デフォルトはどちらもチェックされています。

11-2-3 Web UI によるイベントの確認方法

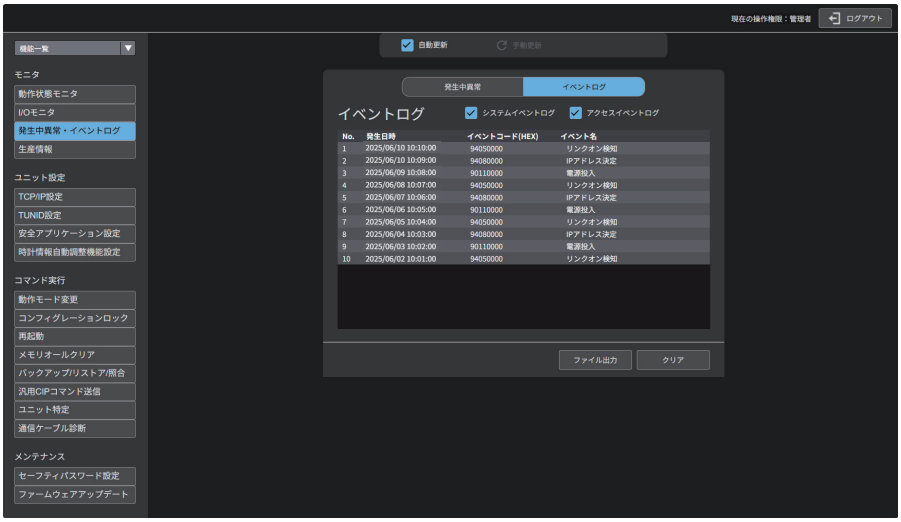
Web UI の発生中異常・イベントログ画面で、イベントを確認します。
発生中異常・イベントログ画面は、当該ユニットの発生中異常およびイベントログを表示する画面です。
イベントログをパソコンに CSV 形式で保存することができます。また、セーフティ I/O ターミナルの内部メモリからイベントログをクリアすることもできます。

発生中異常画面とイベントログ画面の表示方法

1 **左メニューより［発生中異常・イベントログ］をクリックします。**
以下の発生中異常画面が表示されます。

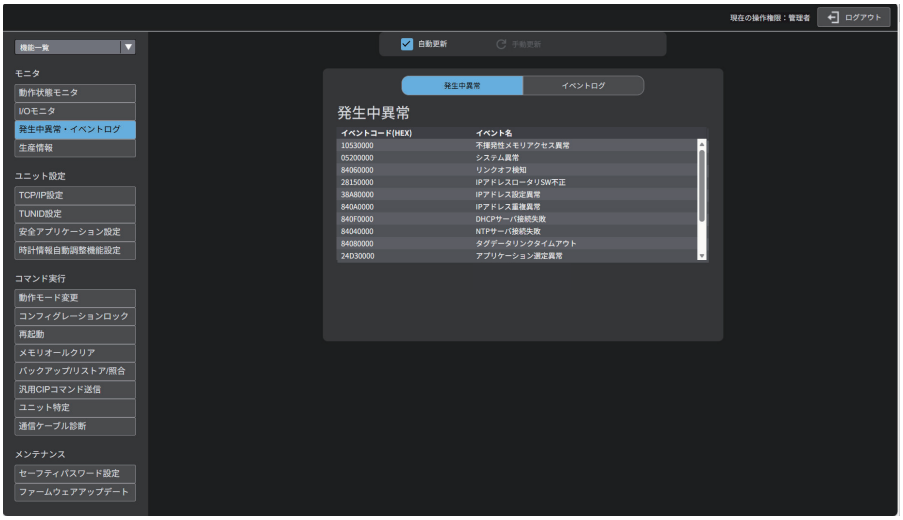


2 **［イベントログ］ボタンを押します。**
以下のイベントログ画面が表示されます。



発生中異常画面

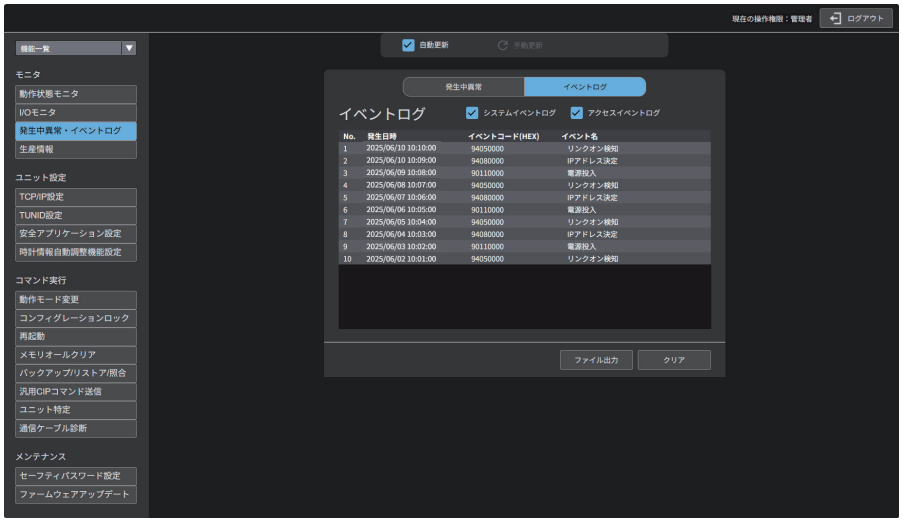
［発生中異常画面］には、発生している異常について以下の情報が表示されます。



項目	内容
イベントコード(Hex)	発生した異常のイベントコード
イベント名	発生した異常のイベント名
付属情報	発生した異常の付属情報

イベントログ画面

［イベントログ画面］には、これまでに発生したイベントログについて以下の情報が表示されます。



項目	内容
発生日時	イベントが発生した日時
重要度	発生したイベントの重要度
イベント名	発生したイベントのイベント名
イベントコード(Hex)	発生したイベントのイベントコード
付属情報	発生したイベントの付属情報

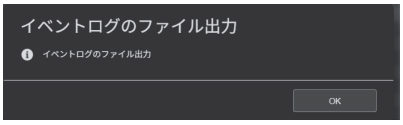
［システムイベントログ］にチェックを入れるとシステムイベントログが表示されます。［アクセスイベントログ］にチェックを入れるとアクセスイベントログが表示されます。両方表示することも可能です。

● イベントログの保存

イベントログの保存では、［システムイベントログ］、［アクセスイベントログ］のチェックの有無に関係なく、両方のイベントログが保存されます。

1 イベントログ画面で［ファイル出力］ボタンを押します。

パソコンのダウンロードフォルダに、イベントログが記述されたファイルが CSV 形式で保存されます。ファイルには、システムイベントログ、アクセスイベントログ、ファームウェアバージョン、製品のシリアル番号、および IP アドレスも記述されます。
以下のメッセージが表示されます。



2 ［OK］ボタンを押します。

● イベントログのクリア

イベントログのクリアでは、［システムイベントログ］、［アクセスイベントログ］のチェックが入っているイベントログがクリアされます。

1 イベントログ画面で［クリア］ボタンを押します。

以下のメッセージが表示されます。



2 **セーフティパスワードを入力して［実行］ボタンを押します。**
イベントログのクリアが実行され、以下のメッセージが表示されます。



3 **［OK］ボタンを押します。**

11-2-4 イベントの内容と対処方法

ここでは、イベントの確認と対処方法について説明します。
発生中のイベントは、解除されない限り保持されます。
イベントを解除するには、発生している異常の要因を取り除くことが必要です。異常の要因を取り除かずに解除しても、同じイベントが再度発生します。

イベント一覧

ここでは、発生するイベント（異常）の一覧を示します。
NJ/NX シリーズのすべてのイベントコードについては、『NJ/NX シリーズ トラブルシューティングマニュアル (SBCA-469)』を参照してください。
NY シリーズのすべてのイベントコードについては、『NY シリーズ トラブルシューティングマニュアル (SBCA-438)』を参照してください。

● イベント一覧の見方

イベント一覧の内容は、次のとおりです。

項目	説明
イベントコード	セーフティ I/O ターミナルで発生した異常（イベント）のコードです。 16 進数 8 桁で表されます。
イベント名	異常（イベント）の名称です。
内容	異常（イベント）の内容です。
発生要因 （推定原因）	推定される異常（イベント）発生の要因です。
重要度	異常（イベント）による制御に対する影響の大きさを表します。 略称は以下を意味しています。 全: 全停止フォールトレベル 部: 部分停止フォールトレベル 軽: 軽度フォールトレベル 監: 監視情報 般: 一般情報 記号は以下を意味しています。 ○: システムにより定義されている重要度 ⊙: ユーザが変更可能な重要度 *1

項目	説明
参照先	異常（イベント）の詳細が記載されているページです。

***1.** 変更可能な重要度がある場合にだけ記載します。

● イベントの一覧

イベントコード	イベント名	内容	発生要因（推定原因）	重要度				参照先
				部	軽	監	般	
05200000Hex	システム異常	ハードウェアの自己診断によりハードウェア異常を検出しました。	• ソフトエラーや過度なノイズなどの一過性要因によるメモリ異常。 • ハードウェアの故障。		○			P. 11-20
05210000Hex	セーフティ入力端子内部回路異常	セーフティ入力端子内部回路の故障を検知しました。	• セーフティ入力端子内部回路の故障。 • ソフトエラーや過度なノイズなどの一過性要因によるメモリ異常または信号異常。		○			P. 11-20
05220000Hex	テスト出力端子内部回路異常	テスト出力端子内部回路の故障を検知しました。	• テスト出力端子内部回路の故障。 • ソフトエラーや過度なノイズなどの一過性要因によるメモリ異常または信号異常。		○			P. 11-21
05230000Hex	セーフティ出力端子内部回路異常	セーフティ出力端子内部回路の故障を検知しました。	• セーフティ出力端子内部回路の故障。 • ソフトエラーや過度なノイズなどの一過性要因によるメモリ異常または信号異常。		○			P. 11-21
155E0000Hex	不揮発性メモリアクセス異常	不揮発性メモリの読み書きに失敗しました。	• 設定データ誤り。 • 設定データ書き込み中の電断。 • 不揮発性メモリの故障。		○			P. 11-22
24D30000Hex	安全アプリケーション用ロータリスイッチ設定不正	安全アプリケーション用ロータリスイッチ設定が不正です。	安全アプリケーション用ロータリスイッチの設定値が不正。		○			P. 11-23
28150000Hex	コンフィグレーションロック後のロータリスイッチ設定変更	コンフィグレーションロックを実行した時のロータリスイッチ設定と現在の設定が不一致です。	コンフィグレーションロック実行後、ロータリスイッチを変更して起動した。		○			P. 11-23
359E0000Hex	IP アドレス設定可能状態外での設定変更	IP アドレス設定可能状態外で IP アドレスを変更しました。	• IP アドレス設定可能状態外で IP アドレス用ロータリスイッチを変更して起動した。 • IP アドレス設定可能状態外で DHCP サーバの設定を変更し、異なる IP アドレスを割り当てた。		○			P. 11-24

イベントコード	イベント名	内容	発生要因（推定原因）	重要度				参照先
				部	軽	監	般	
38A80000Hex	IP アドレス設定異常	IP アドレス設定の異常を検知しました。	• 設定データ誤り。 • TCP/IP 設定の書き込み中の電断。 • DHCP サーバから取得した IP アドレスが不正。 • 不揮発性メモリアクセス異常。		○			P. 11-25
38A90000Hex	TUNID 設定後の IP アドレス変更	TUNID 設定の異常を検知しました。	• TUNID 設定後に IP アドレス用ロータリスイッチを変更して起動した。 • TUNID 設定後に DHCP サーバの設定を変更し、TUNID 設定時と異なる IP アドレスを割り当てた。		○			P. 11-26
55030000Hex	デュアルチャネル出力間のデータ異常	誤ったセーフティ出力データが書き込まれました。	デュアルチャネルに設定されたセーフティ出力に異なる値が書き込まれた。		○			P. 11-26
65210000Hex	電源遮断テスト異常	出力電源遮断テストで異常を検出しました。	配線異常、もしくはハードウェア故障。		○			P. 11-27
65220000Hex	セーフティ入力端子外部接続機器異常	セーフティ入力端子のテストパルス評価機能において異常を検知しました。	• 入力信号線に電源（+側）が接触。 • 入力信号線間の短絡。 • 外部接続機器の故障。 • 該当セーフティ入力端子と組み合わせて使用しているテスト出力端子で異常が発生。		○			P. 11-27
65230000Hex	セーフティ入力端子デュアルチャネル監視異常	セーフティ入力端子のデュアルチャネル評価機能において異常を検知しました。	• 入力信号線の地絡、または断線。 • 接続機器の故障。 • デュアルチャネル監視時間の設定値不正。 • セーフティ扉などの外部入力機器からの入力信号にチャタリングが発生。 • 該当セーフティ入力端子と組み合わせて使用しているテスト出力端子で異常が発生。		○			P. 11-28
65240000Hex	テスト出力端子過電流異常	テスト出力端子で過電流を検知しました。	• 出力信号線の地絡。 • 外部接続機器の故障。		○			P. 11-28
65250000Hex	テスト出力端子出力 ON 固着異常	テスト出力端子で ON 固着を検知しました。	• 出力信号線に電源（+側）が接触。 • 内部回路の故障。 • ソフトエラーや過度なノイズなどの一過性要因によるメモリ異常または信号異常。 • 該当セーフティ入力端子と組み合わせて使用しているテスト出力端子で異常が発生。		○			P. 11-29

イベントコード	イベント名	内容	発生要因（推定原因）	重要度				参照先
				部	軽	監	般	
65270000Hex	セーフティ出力端子地絡異常	セーフティ出力端子において地絡を検知しました。	出力信号線の地絡。		○			P. 11-29
65280000Hex	セーフティ出力端子出力 ON 固着異常	セーフティ出力端子において ON 固着を検知しました。	• 出力信号線に電源（+側）が接触。 • 出力電源が仕様範囲外。 • 内部回路の故障。 • ソフトエラーや過度なノイズなどの一過性要因によるメモリ異常または信号異常。		○			P. 11-30
65290000Hex	出力用電源異常	出力用電源の不正を検出しました。	• 出力用電源が接続されていない。 • 出力用電源の電圧が低下して検出閾値を下回り、出力用電源が遮断された。 • 出力用電源の電圧が上昇して検出閾値を上回り、出力用電源が遮断された。 • 出力用電源の電流が上昇して検出閾値を上回り、出力用電源が遮断された。		○			P. 11-30
652B0000Hex	EDM 異常	EDM で異常を検知した。	• 出力信号線の断線 • 出力信号線の地絡 • 出力信号線が電源と接触していないか • 外部配線機器であるコンタクタおよびリレー接点の溶着 • 外部配線機器の断線、地絡		○			P. 11-31
84040000Hex	NTP サーバ接続失敗	NTP サーバとの接続に失敗しました。	• 設定データの誤り。 • サーバダウン。 • 通信経路の異常発生。		○			P. 11-31
840F0000Hex	DHCP サーバ接続失敗	DHCP サーバとの接続に失敗しました。	• サーバ設定の誤り。 • サーバダウン。 • 通信経路の異常発生。		○			P. 11-32
85E20000Hex	IP アドレス重複異常	IP アドレスが重複しています。	IP アドレスが、他ノードの IP アドレスと重複している。		○			P. 11-32
85E30000Hex	タグデータリンクタイムアウト	タグデータリンクでタイムアウトが発生しました。	• オリジネータノードの電源 OFF。 • オリジネータノードの通信停止。 • EtherNet/IP の Ethernet ケーブルのコネクタのはずれ。 • EtherNet/IP の Ethernet ケーブルの断線。 • EtherNet/IP ポートのリンクオフ。 • ネットワーク通信負荷による経路上でのパケットロスト。 • ノイズ。		○			P. 11-33

イベントコード	イベント名	内容	発生要因（推定原因）	重要度				参照先
				部	軽	監	般	
85E40000Hex	CIP Safety ターゲットコネクションタイムアウト	CIP Safety ターゲットコネクションでタイムアウトが発生しました。	• ケーブルの断線。 • オリジネータデバイスがコネクションを受け付けられない状態に遷移した。 • 通信設定のタイムアウト値が短すぎる。 • EtherNet/IP ポート設定、および経路上の機器の Packet Filter（簡易）機能、Packet Filter 機能でオリジネータノードからの CIP Safety パケットが許可されていない。 • オリジネータノードの［CIP メッセージサーバ］が［使用しない］に設定されている。 • オリジネータノードの PacketFilter 機能が有効の場合にターゲットノードからの CIP Safety パケットが許可されていない。 • ノイズ。 • EtherNet/IP ポート設定の［CIP Safety 通信］が［使用しない］に設定されている。		○			P. 11-34
652F0000Hex	ユニット/入力用電源仕様範囲外電圧検知	ユニット/入力用電源の電圧が仕様範囲外であることを検知しました。	ユニット/入力用電源の電圧が仕様範囲外であることを検知した。			○		P. 11-34
65300000Hex	ユニット/入力用電源仕様範囲外電流検知	ユニット/入力用電源の電流が仕様範囲外であることを検知した。	ユニット/入力用電源の電流が仕様範囲外であることを検知した。			○		P. 11-34
65310000Hex	出力用電源仕様範囲外電圧検知	出力用電源の電圧が仕様範囲外であることを検知しました。	出力用電源の電圧が仕様範囲外であることを検知した。			○		P. 11-35
65320000Hex	出力用電源仕様範囲外電流検知	出力用電源の電流が仕様範囲外であることを検知しました。	出力用電源の電流が仕様範囲外であることを検知した。			○		P. 11-35
85E10000Hex	リンクオフ検知	Ethernet のリンクオフを検知しました。	• Ethernet ケーブルの断線、ゆるみ、はずれ。 • スイッチングハブの電源 OFF。 • 通信速度不一致。 • ノイズ。 • 再起動又はメモリオールクリアを実行。			○		P. 11-36
85E50000Hex	CIP Safety ターゲットコネクション開設要求	CIP Safety オリジネータからコネクション開設要求がありました。	CIP Safety オリジネータからコネクション開設要求があった。				○	P. 11-36
90110000Hex	電源投入	電源が投入されました。	電源を投入した。				○	P. 11-36

イベントコード	イベント名	内容	発生要因（推定原因）	重要度				参照先
				部	軽	監	般	
94080000Hex	IP アドレス決定	正しく IP アドレスが決定し、Ethernet 通信動作を開始できる状態になりました。	正しく IP アドレスが決定し、Ethernet 通信動作を開始できる状態になった。				○	P. 11-37
966C0000Hex	コンフィグレーションロック	コンフィグレーションロックが実行されました。	コンフィグレーションロック実行。				○	P. 11-37
966D0000Hex	コンフィグレーションロック解除	コンフィグレーションロック解除が実行されました。	コンフィグレーションロック解除実行。				○	P. 11-37
96710000Hex	出力用電源(PWR OUT)の OFF	電源コネクタ PWR OUT から供給される出力用電源が OFF されました。	「渡り配線出力用電源の遮断指示」で渡り配線出力用電源の遮断を指示した。				○	P. 11-38
96720000Hex	設定データ変更	設定データが変更されました。	設定データが変更された。				○	P. 11-38
96730000Hex	ログイン	ログインしました。(Web UI)	Web UI を使ってログインした。				○	P. 11-39
96750000Hex	安全アプリケーションの削除	安全アプリケーションデータがユニットから削除されました。	Web UI からの削除を受け付けた。				○	P. 11-39
96760000Hex	セーフティパスワード不一致	セーフティパスワードが必要なサービス実行時にセーフティパスワード不一致を検出しました。	セーフティパスワードが必要なサービスでパスワード不一致を検出した。				○	P. 11-39
96770000Hex	出力用電源(PWR OUT)の ON	電源コネクタ PWR OUT から供給される出力用電源が ON されました。	「渡り配線出力用電源の復帰指示」で渡り配線出力用電源の復帰を指示した。				○	P. 11-40
96780000Hex	ファームウェアアップデート実行	ファームウェアアップデートを実行しました。	ファームウェアアップデートが実行された。				○	P. 11-40
96790000Hex	メモリオールクリア	メモリオールクリアが実行されました。	メモリオールクリアが実行された。				○	P. 11-40
967A0000Hex	リンクオン検知	Ethernet のリンク確立を検知しました。	Ethernet のリンク確立を検知した。				○	P. 11-41
967B0000Hex	動作モードの変更	動作モード変更が実行されました。	動作モード変更実行。				○	P. 11-41
967C0000Hex	セーフティパスワードの変更	セーフティパスワードを変更しました。	セーフティパスワードを変更した。				○	P. 11-41
967D0000Hex	安全アプリケーションの転送	安全アプリケーションデータがユニットへ転送されました。	• Web UI での転送を受け付けた。 • セーフティコントローラから Type1 Safety Open 処理を受け付けた。				○	P. 11-42
967E0000Hex	イベントログのクリア	イベントログをクリアしました。	イベントログをクリアした。				○	P. 11-42
967F0000Hex	バックアップ実行	バックアップを実行しました。	バックアップが実行された。				○	P. 11-42

イベントコード	イベント名	内容	発生要因（推定原因）	重要度				参照先
				部	軽	監	般	
96800000Hex	リストア実行	リストアを実行しました。	リストアが実行された。				○	P. 11-43
96810000Hex	オムロン保守の実行	オムロンの保守担当者による保守作業が実行されました。	オムロンの保守担当者による保守作業が実行された。				○	P. 11-43
96820000Hex	再起動	再起動が実行された。	再起動が実行された。				○	P. 11-43
96830000Hex	セーフティコンフィグレーション確定	セーフティコンフィグレーションデータが確定した。	セーフティコンフィグレーションデータが確定した。				○	P. 11-44
96840000Hex	IP アドレス表示機能実行	IP アドレス表示機能が実行されました。	SW1=SW2=8（IP アドレス表示機能）で起動した。				○	P. 11-44
96850000Hex	I/O 配線チェック機能実行	I/O 配線チェック機能が実行されました。	SW1=SW2=E（I/O 配線チェック機能）で起動した。				○	P. 11-44

イベントの内容

ここでは、各イベントの内容を説明します。

● イベント内容の見方

各異常の説明で使用する表の各項目の意味を［ ］内に示します。

イベント名	［異常（イベント）の名称です。］			**イベントコード**	［異常（イベント）のコードです。］	
内容	［異常（イベント）の内容です。］					
発生源	［異常（イベント）が発生した箇所です。］		**発生源詳細**	［発生源の詳細です。］	**検出タイミング**	［異常検出のタイミングです。］
異常の属性	**重要度**	［制御に対する影響の大きさです。］*1	**復旧方法**	［復旧方法です。］*2	**ログカテゴリ**	［保存されるログの種類です。］*3
発生の影響	**ユーザプログラム**	［ユーザプログラムの実行状態です。］*4	**動作**	［異常（イベント）発生時の動作に関する特記事項です。］		
発生要因とその処置	**発生要因（推定原因）**		**処置対策**		**再発防止**	
	［異常（イベント）の発生要因と処置対策、再発防止方法です。］					
付属情報	［Sysmac Studio／表示器で表示される付属情報内容です。］*5					
注意点／備考	［その他の注意点、制約事項、補足説明などです。ユーザが選択可能な重要度がある場合は、選択可能な重要度、復旧方法、動作などの関連事項を記載します。］					

***1.** 次のいずれかです。
- 全停止フォールト: 全停止フォールトレベル
- 部分停止フォールト: 部分停止フォールトレベル
- 軽度フォールト: 軽度フォールトレベル
- 監視情報
- 一般情報

***2.** 処置対策後にコントローラの異常状態を解除するための方法で、次のいずれかです。
- 自動復旧: 要因が除去されたとき自動的に正常に戻ります。
- 異常解除: 要因を除去後、異常解除を実行することで正常に戻ります。
- 電源再投入: 要因を除去後、コントローラの電源再投入することで正常に戻ります。
- コントローラリセット: 要因を除去後、コントローラリセットすることで正常に戻ります。
- 発生要因依存: 発生要因に依存します。

***3.** 次のいずれかです。
- システム: システムイベントログ
- アクセス: アクセスイベントログ

***4.** 次のいずれかです。
- 継続: ユーザプログラムの実行を継続します。
- 停止: ユーザプログラムの実行を停止します。
- 開始: ユーザプログラムの実行を開始します。

***5.** 表示器のトラブルシュータの対応範囲については、『NJ/NX シリーズ トラブルシューティングマニュアル(SBCA-469)』、または『NY シリーズ トラブルシューティングマニュアル(SBCA-438)』を参照してください。

● イベントの説明

イベント名	システム異常			**イベントコード**	05200000Hex	
内容	ハードウェアの自己診断によりハードウェア異常を検出しました。					
発生源	—		**発生源詳細**	—	**検出タイミング**	常時
異常の属性	**重要度**	軽度フォールト	**復旧方法**	電源再投入	**ログカテゴリ**	システム
発生の影響	**ユーザプログラム**	継続	**動作**	該当ユニットは動作を停止し、入出力データを安全状態に遷移させます。		
発生要因とその処置	**発生要因（推定原因）**		**処置対策**		**再発防止**	
	• ソフトエラーや過度なノイズなどの一過性要因によるメモリ異常。 • ハードウェアの故障。		電源を再投入してください。 再発する場合は、ユニットを交換してください。		電源再投入で正常に動作を再開できる場合は、ユニット周辺で過度なノイズが発生している可能性がありますので、ノイズ対策を検討してください。	
付属情報	付属情報 1: システム情報 付属情報 2: システム情報 付属情報 3: システム情報 付属情報 4: システム情報					
注意点／備考	なし					

イベント名	セーフティ入力端子内部回路異常			**イベントコード**	05210000Hex	
内容	セーフティ入力端子内部回路の故障を検知しました。					
発生源	—		**発生源詳細**	—	**検出タイミング**	• Idle 時 • Executing 時
異常の属性	**重要度**	軽度フォールト	**復旧方法**	• 電源再投入 • 再起動の実行	**ログカテゴリ**	システム
発生の影響	**ユーザプログラム**	継続	**動作**	電源が再投入されるまで、該当セーフティ入力端子はセーフティ状態に維持されます。		
発生要因とその処置	**発生要因（推定原因）**		**処置対策**		**再発防止**	
	セーフティ入力端子内部回路の故障。		電源を再投入してください。 再発する場合は、ユニットを交換してください。		電源再投入で正常に動作を再開できる場合は、ユニット周辺で過度なノイズが発生している可能性がありますので、ノイズ対策を検討してください。	
	ソフトエラーや過度なノイズなどの一過性要因によるメモリ異常または信号異常。					
付属情報	付属情報 1: 端子番号					
注意点／備考	なし					

イベント名	テスト出力端子内部回路異常			**イベントコード**	05220000Hex	
内容	テスト出力端子内部回路の故障を検知しました。					
発生源	—		**発生源詳細**	—	**検出タイミング**	• Idle 時 • Executing 時
異常の属性	**重要度**	軽度フォールト	**復旧方法**	• 電源再投入 • 再起動の実行	**ログカテゴリ**	システム
発生の影響	**ユーザプログラム**	継続	**動作**	電源が再投入されるまで、該当テスト出力端子はセーフティ状態に維持されます。また、該当テスト出力端子をテストソースとして使用しているセーフティ入力端子には、イベント「セーフティ入力端子外部接続機器異常」(65220000Hex)が発生します。		
発生要因とその処置	**発生要因（推定原因）**		**処置対策**		**再発防止**	
	テスト出力端子内部回路の故障。		電源を再投入してください。 再発する場合は、ユニットを交換してください。		電源再投入で正常に動作を再開できる場合は、ユニット周辺で過度なノイズが発生している可能性がありますので、ノイズ対策を検討してください。	
	ソフトエラーや過度なノイズなどの一過性要因によるメモリ異常または信号異常。					
付属情報	付属情報 1: 端子番号					
注意点／備考	なし					

イベント名	セーフティ出力端子内部回路異常			**イベントコード**	05230000Hex	
内容	セーフティ出力端子内部回路の故障を検知しました。					
発生源	—		**発生源詳細**	—	**検出タイミング**	• Idle 時 • Executing 時
異常の属性	**重要度**	軽度フォールト	**復旧方法**	• 電源再投入 • 再起動の実行	**ログカテゴリ**	システム
発生の影響	**ユーザプログラム**	継続	**動作**	電源が再投入されるまで、該当セーフティ出力端子はセーフティ状態に維持されます。		
発生要因とその処置	**発生要因（推定原因）**		**処置対策**		**再発防止**	
	セーフティ出力端子内部回路の故障。		電源を再投入してください。 再発する場合は、ユニットを交換してください。		電源再投入で正常に動作を再開できる場合は、ユニット周辺で過度なノイズが発生している可能性がありますので、ノイズ対策を検討してください。	
	ソフトエラーや過度なノイズなどの一過性要因によるメモリ異常または信号異常。					
付属情報	付属情報 1: 端子番号					
注意点／備考	なし					

<table>
<tr><td>イベント名</td><td colspan="2">不揮発性メモリアクセス異常</td><td>イベントコード</td><td colspan="2">155E0000Hex</td></tr>
<tr><td>内容</td><td colspan="5">不揮発性メモリの読み書きに失敗しました。</td></tr>
<tr><td>発生源</td><td colspan="2">—</td><td>発生源詳細</td><td>検出タイミング</td><td>常時</td></tr>
<tr><td>異常の属性</td><td>重要度</td><td>軽度フォールト</td><td>復旧方法</td><td>ログカテゴリ</td><td>システム</td></tr>
<tr><td>発生の影響</td><td>ユーザプログラム</td><td>継続</td><td>動作</td><td colspan="2">該当ユニットは動作を停止し、入出力データを安全状態に遷移させます。</td></tr>
<tr><td>発生要因とその処置</td><td colspan="2">発生要因（推定原因）</td><td colspan="2">処置対策</td><td>再発防止</td></tr>
<tr><td></td><td colspan="2">設定データ誤り。</td><td colspan="2" rowspan="2">付属情報から異常要因を特定してください。
• 付属情報 1=01Hex の場合
電源を再投入してください。</td><td>なし</td></tr>
<tr><td></td><td colspan="2">設定データ書き込み中の電断。</td><td>設定データの書き込み中は当該ユニットの電源を OFF しないでください。</td></tr>
<tr><td></td><td colspan="2">不揮発性メモリの故障。</td><td colspan="2">• 付属情報 1=02Hex の場合
付属情報 2 の値により、以下を実行してください。
02xx～05xxHex: 各設定を再度行ってください。
20xxHex:
-CST 形式の場合: メモリオールクリアを実行し、安全アプリケーションを再設定してください。
-EIT 形式の場合: ロータリスイッチを SW1 = SW2 = 0 に合わせてからメモリオールクリアを実行し、安全アプリケーションを再設定してください。
21xxHex: 安全アプリケーションを再設定してください。
FExxHex: ファームウェアアップデートを行ってください。

上記で復旧しない場合は、ユニットを交換してください。</td><td>なし</td></tr>
<tr><td>付属情報</td><td colspan="5">付属情報 1: 要因
01Hex 不揮発性メモリへのアクセス失敗
02Hex データ破損
付属情報 2: 検知対象
02xxHex: リンク設定
03xxHex: Ethernet ポートの有効／無効設定
04xxHex: SNTP 設定
05xxHex: 渡り配線出力用電源遮断機能の有効／無効設定
20xxHex: その他安全関連データ
21xxHex: 安全アプリケーションデータ
80xxHex: QoS 設定
81xxHex: LLDP 機能設定
FExxHex: ファームウェアデータ
上記以外: その他システムデータ</td></tr>
<tr><td>注意点／備考</td><td colspan="5">なし</td></tr>
</table>

イベント名	安全アプリケーション用ロータリスイッチ設定不正			**イベントコード**	24D30000Hex	
内容	安全アプリケーション用ロータリスイッチ設定が不正です。					
発生源	—		**発生源詳細**	—	**検出タイミング**	• 電源投入時 • 再起動実行時
異常の属性	**重要度**	軽度フォールト	**復旧方法**	• 電源再投入 • 再起動の実行	**ログカテゴリ**	システム
発生の影響	**ユーザプログラム**	継続	**動作**	該当ユニットは動作を停止し、入出力データを安全状態に遷移させます。		
発生要因とその処置	**発生要因（推定原因）**		**処置対策**		**再発防止**	
	安全アプリケーション用ロータリスイッチの設定値が不正。		安全アプリケーション用ロータリスイッチの設定値が正しいことを確認してください。		なし	
付属情報	付属情報 1: 現在の安全アプリケーション用ロータリスイッチの設定値 表示フォーマットは [SW1,SW2]。 例: SW1=1、SW2=E の場合 ⇒ 1E					
注意点／備考	なし					

イベント名	コンフィグレーションロック後のロータリスイッチ設定変更			**イベントコード**	28150000Hex	
内容	コンフィグレーションロックを実行した時のロータリスイッチ設定と現在の設定が不一致です。					
発生源	—		**発生源詳細**	—	**検出タイミング**	• 電源投入時 • 再起動実行時
異常の属性	**重要度**	軽度フォールト	**復旧方法**	• 電源再投入 • 再起動の実行	**ログカテゴリ**	システム
発生の影響	**ユーザプログラム**	継続	**動作**	該当ユニットは動作を停止し、入出力データを安全状態に遷移させます。		
発生要因とその処置	**発生要因（推定原因）**		**処置対策**		**再発防止**	
	コンフィグレーションロック実行後、ロータリスイッチを変更して起動した。		• ロータリスイッチの設定値をコンフィグレーションロックを実行した時の設定値に戻してください。 • コンフィグレーションロックを解除した後にメモリオールクリアを実行し、再設定してください。 いずれの処置を行った場合も、実施後に電源再投入または再起動を実行してください。		コンフィグレーションロックを実行した後は、ロータリスイッチの設定値を変更しないでください。	
付属情報	付属情報 1: 現在のロータリスイッチの設定値 表示フォーマットは、[SW1,SW2,x16^{1},x16^{0}] 例: SW1=F、SW2=F、x16^{1}=0, x16^{0}=1 の場合 ⇒ FF01Hex 付属情報 2: コンフィグレーションロックを実行した時ロータリスイッチの設定値 表示フォーマットは、[SW1,SW2,x16^{1},x16^{0}] 例: SW1=3、SW2=3、x16^{1}=0, x16^{0}=1 の場合 ⇒ 3301Hex					
注意点／備考	なし					

<table>
<tr><td>イベント名</td><td colspan="3">IP アドレス設定可能状態外での設定変更</td><td>イベントコード</td><td colspan="2">359E0000Hex</td></tr>
<tr><td>内容</td><td colspan="6">IP アドレス設定可能状態外で IP アドレスを変更しました。</td></tr>
<tr><td>発生源</td><td colspan="2">—</td><td>発生源詳細</td><td>—</td><td>検出タイミング</td><td>• 電源投入時
• 再起動実行時</td></tr>
<tr><td>異常の属性</td><td>重要度</td><td>軽度フォールト</td><td>復旧方法</td><td>• 電源再投入
• 再起動の実行</td><td>ログカテゴリ</td><td>システム</td></tr>
<tr><td>発生の影響</td><td>ユーザプログラム</td><td>継続</td><td>動作</td><td colspan="3">該当ユニットは動作を停止し、入出力データを安全状態に遷移させます。</td></tr>
<tr><td>発生要因とその処置</td><td colspan="2">発生要因（推定原因）</td><td colspan="2">処置対策</td><td colspan="2">再発防止</td></tr>
<tr><td></td><td colspan="2">• IP アドレス設定可能状態外で IP アドレス用ロータリスイッチを変更して起動した。
• IP アドレス設定可能状態外で DHCP サーバの設定を変更し、異なる IP アドレスを割り当てた。</td><td colspan="2">• IP アドレス用ロータリスイッチを元の値に戻してください。
• DHCP サーバの設定を元の値に戻してください。
• メモリオールクリアを実行し、IP アドレスを再設定してください。
上記で復旧しない場合は、ユニットを交換してください。</td><td colspan="2">IP アドレス設定可能状態外で、IP アドレス用ロータリスイッチの操作および DHCP サーバの設定を変更しないでください。</td></tr>
<tr><td>付属情報</td><td colspan="6">付属情報 1: 現在の IP アドレス
例）192.168.250.100 の場合は、C0A8FA64Hex となります。
付属情報 2: 設定可能状態で設定した IP アドレス
例）192.168.250.100 の場合は、C0A8FA64Hex となります。</td></tr>
<tr><td>注意点／備考</td><td colspan="6">なし</td></tr>
</table>

<table>
<tr><td>イベント名</td><td colspan="3">IP アドレス設定異常</td><td>イベントコード</td><td colspan="2">38A80000Hex</td></tr>
<tr><td>内容</td><td colspan="6">IP アドレス設定の異常を検知しました。</td></tr>
<tr><td>発生源</td><td colspan="2">—</td><td>発生源詳細</td><td>—</td><td>検出タイミング</td><td>• 電源投入時
• 再起動実行時</td></tr>
<tr><td>異常の属性</td><td>重要度</td><td>軽度フォールト</td><td>復旧方法</td><td>• 電源再投入
• 再起動の実行</td><td>ログカテゴリ</td><td>システム</td></tr>
<tr><td>発生の影響</td><td>ユーザプログラム</td><td>継続</td><td>動作</td><td colspan="3">EtherNet/IP 通信不可。
CIP Safety 通信不可。</td></tr>
<tr><td rowspan="4">発生要因とその処置</td><td colspan="2">発生要因（推定原因）</td><td colspan="2">処置対策</td><td colspan="2">再発防止</td></tr>
<tr><td colspan="2">設定データ誤り。</td><td colspan="2" rowspan="4">IP アドレスはデフォルト値の 192.168.250.1 となります。次のいずれかの処置を行ってください。
• 付属情報から異常要因を特定し、正しい値を再度設定してください。
• メモリオールクリアを実行するか、再度設定を書き込んでください。
• DHCP サーバが提供する IP アドレスの設定を当該ユニットの規定されている範囲に修正してください。
いずれの処置を行った場合も、実施後に電源再投入または再起動を実行してください。
上記で復旧しない場合は、ユニットを交換してください。</td><td colspan="2">なし</td></tr>
<tr><td colspan="2">TCP/IP 設定の書き込み中の電断。</td><td colspan="2">TCP/IP 設定の書き込み中は当該ユニットの電源を OFF しないでください。</td></tr>
<tr><td colspan="2">DHCP サーバから取得した IP アドレスが不正。</td><td colspan="2">DHCP サーバが提供する IP アドレスの設定を当該ユニットの規定されている範囲に修正してください。</td></tr>
<tr><td colspan="2">不揮発性メモリアクセス異常。</td><td colspan="2">なし</td></tr>
<tr><td>付属情報</td><td colspan="6">付属情報 1: 異常の種別
01Hex：不揮発性メモリアクセス異常
02Hex：設定値に矛盾がある
付属情報 2: 異常内容の詳細（付属情報 1 が 02Hex の場合）
11Hex：IP アドレス不正
12Hex：サブネットマスク不正
13Hex：デフォルトゲートウェイ不正</td></tr>
<tr><td>注意点／備考</td><td colspan="6">なし</td></tr>
</table>

イベント名	TUNID 設定後の IP アドレス変更			イベントコード	38A90000Hex	
内容	TUNID 設定の異常を検知しました。					
発生源	—		発生源詳細	—	検出タイミング	• 電源投入時 • 再起動実行時
異常の属性	重要度	軽度フォールト	復旧方法	• 電源再投入 • 再起動の実行	ログカテゴリ	システム
発生の影響	ユーザプログラム	継続	動作	該当ユニットは動作を停止し、入出力データを安全状態に遷移させます。		

発生要因とその処置	発生要因（推定原因）	処置対策	再発防止
	TUNID 設定後に IP アドレス用ロータリスイッチを変更して起動した。	IP アドレス用ロータリスイッチを TUNID 設定時点の値に戻してください。	TUNID 設定後は、IP アドレス用ロータリスイッチの操作および DHCP サーバの設定を変更しないでください。
	TUNID 設定後に DHCP サーバの設定を変更し、TUNID 設定時と異なる IP アドレスを割り当てた。	DHCP サーバの設定を TUNID 設定時点の値に戻してください。	
		または、メモリオールクリアを実行し、TUNID を再設定してください。 上記で復旧しない場合は、ユニットを交換してください。	

付属情報	付属情報 1: 現在の IP アドレス 例）192.168.250.1 の場合は、C0A8FA01Hex となります。 付属情報 2: TUNID 設定時点の IP アドレス（TUNID の IP アドレス部分） 例）192.168.250.100 の場合は、C0A8FA64Hex となります。
注意点／備考	なし

イベント名	デュアルチャネル出力間のデータ異常			イベントコード	55030000Hex	
内容	誤ったセーフティ出力データが書き込まれました。					
発生源	—		発生源詳細	—	検出タイミング	• Idle 時 • Executing 時
異常の属性	重要度	軽度フォールト	復旧方法	セーフティ出力端子をインアクティブにする	ログカテゴリ	システム
発生の影響	ユーザプログラム	継続	動作	異常が解除されるまで、該当セーフティ出力端子はセーフティ状態に維持されます。		

発生要因とその処置	発生要因（推定原因）	処置対策	再発防止
	デュアルチャネルに設定されたセーフティ出力に異なる値が書き込まれた。	セーフティプログラムを確認し、デュアルチャネルに設定されたセーフティ出力に同じ値を書き込んでください。	あらかじめ処置対策の内容を考慮してセーフティプログラムを設計してください。

付属情報	付属情報 1: 端子番号
注意点／備考	なし

イベント名	電源遮断テスト異常			イベントコード	65210000Hex	
内容	出力電源遮断テストで異常を検出しました。					
発生源	—		発生源詳細	—	検出タイミング	• 電源投入時 • 再起動実行時
異常の属性	重要度	軽度フォールト	復旧方法	• 電源再投入 • 再起動の実行	ログカテゴリ	システム
発生の影響	ユーザプログラム	継続	動作	該当ユニットは運転を継続しますが、入出力データはセーフティ状態を維持します。		

発生要因とその処置	発生要因（推定原因）	処置対策	再発防止
	配線異常、もしくはハードウェア故障。	以下を確認のうえ、定格にあった電源を供給してください。 • 電源電圧が仕様の範囲内か • 配線に誤りや断線がないか • セーフティ出力端子に DC24V が印加されていないか、または電源（+側）に接触していないか 電圧を測定し正常である場合、ユニットの故障が考えられます。その場合はユニットを交換してください。	あらかじめ処置対策の内容を考慮して設計してください。

付属情報	なし
注意点／備考	なし

イベント名	セーフティ入力端子外部接続機器異常			イベントコード	65220000Hex	
内容	セーフティ入力端子のテストパルス評価機能において異常を検知しました。					
発生源	—		発生源詳細	—	検出タイミング	• Idle 時 • Executing 時
異常の属性	重要度	軽度フォールト	復旧方法	セーフティ入力端子をインアクティブにすることで復旧	ログカテゴリ	システム
発生の影響	ユーザプログラム	継続	動作	異常が解除されるまで、該当セーフティ入力端子はセーフティ状態に維持されます。		

発生要因とその処置	発生要因（推定原因）	処置対策	再発防止
	入力信号線に電源（+側）が接触。	外部配線を確認してください。	あらかじめ処置対策の内容を考慮して設定や配線をしてください。
	入力信号線間の短絡。		
	外部接続機器の故障。	外部接続機器を交換してください。	
	該当セーフティ入力端子と組み合わせて使用しているテスト出力端子で異常が発生。	テスト出力端子で発生している異常を確認し処置対策を行ってください。	テスト出力端子で発生している異常の再発防止を行ってください。

付属情報	付属情報 1: 端子番号
注意点／備考	なし

イベント名	セーフティ入力端子デュアルチャネル監視異常			イベントコード	65230000Hex	
内容	セーフティ入力端子のデュアルチャネル評価機能において異常を検知しました。					
発生源	—		発生源詳細	—	検出タイミング	• Idle 時 • Executing 時
異常の属性	重要度	軽度フォールト	復旧方法	セーフティ入力端子をインアクティブにすることで復旧	ログカテゴリ	システム
発生の影響	ユーザプログラム	継続	動作	異常が解除されるまで、該当セーフティ入力端子はセーフティ状態に維持されます。		

発生要因とその処置	発生要因（推定原因）	処置対策	再発防止
	入力信号線の地絡、または断線。	外部配線を確認してください。	あらかじめ処置対策の内容を考慮して設定や配線をしてください。
	接続機器の故障。	外部接続機器を交換してください。	
	デュアルチャネル監視時間の設定値不正。	デュアルチャネル評価時間を見直してください。改善されない場合は、入力フィルタ機能により、オンディレーやオフディレーを設定してください。	
	セーフティ扉などの外部入力機器からの入力信号にチャタリングが発生。		
	該当セーフティ入力端子と組み合わせて使用しているテスト出力端子で異常が発生。	テスト出力端子で発生している異常を確認し処置対策を行ってください。	テスト出力端子で発生している異常の再発防止を行ってください。

付属情報	付属情報 1: 端子番号
注意点／備考	なし

イベント名	テスト出力端子過電流異常			イベントコード	65240000Hex	
内容	テスト出力端子で過電流を検知しました。					
発生源	—		発生源詳細	—	検出タイミング	• Idle 時 • Executing 時
異常の属性	重要度	軽度フォールト	復旧方法	自動復旧	ログカテゴリ	システム
発生の影響	ユーザプログラム	継続	動作	異常が解除されるまで、該当テスト出力端子をテストソースとして使用しているセーフティ入力端子は、セーフティ状態に維持されます。		

発生要因とその処置	発生要因（推定原因）	処置対策	再発防止
	出力信号線の地絡。	外部配線を確認してください。	あらかじめ処置対策の内容を考慮して設定や配線をしてください。
	外部接続機器の故障。	外部接続機器を交換してください。	

付属情報	付属情報 1: 端子番号
注意点／備考	なし

イベント名	テスト出力端子出力 ON 固着異常			**イベントコード**	65250000Hex	
内容	テスト出力端子で ON 固着を検知しました。					
発生源	—		**発生源詳細**	—	**検出タイミング**	• Idle 時 • Executing 時
異常の属性	**重要度**	軽度フォールト	**復旧方法**	自動復旧	**ログカテゴリ**	システム
発生の影響	**ユーザプログラム**	継続	**動作**	異常が解除されるまで、該当テスト出力端子をテストソースとして使用しているセーフティ入力端子は、セーフティ状態に維持されます。		
発生要因とその処置	**発生要因（推定原因）**		**処置対策**		**再発防止**	
	出力信号線に電源（+側）が接触。		外部配線を確認してください。		あらかじめ処置対策の内容を考慮して設定や配線をしてください。	
	内部回路の故障。 ソフトエラーや過度なノイズなどの一過性要因によるメモリ異常または信号異常。		電源を再投入してください。 再発する場合は、ユニットを交換してください。		電源再投入で正常に動作を再開できる場合は、ユニット周辺で過度なノイズが発生している可能性がありますので、ノイズ対策を検討してください。	
付属情報	付属情報 1: 端子番号					
注意点／備考	なし					

イベント名	セーフティ出力端子地絡異常			**イベントコード**	65270000Hex	
内容	セーフティ出力端子において地絡を検知しました。					
発生源	—		**発生源詳細**	—	**検出タイミング**	• Idle 時 • Executing 時
異常の属性	**重要度**	軽度フォールト	**復旧方法**	セーフティ出力端子をインアクティブにすることで復旧	**ログカテゴリ**	システム
発生の影響	**ユーザプログラム**	継続	**動作**	異常が解除されるまで、該当セーフティ出力端子はセーフティ状態に維持されます。		
発生要因とその処置	**発生要因（推定原因）**		**処置対策**		**再発防止**	
	出力信号線の地絡。		外部配線を確認してください。		あらかじめ処置対策の内容を考慮して設定や配線をしてください。	
付属情報	付属情報 1: 端子番号					
注意点／備考	出力用電源に異常が発生した場合、セーフティ出力端子が地絡していなくても本異常が登録されることがあります。					

イベント名	セーフティ出力端子出力 ON 固着異常			イベントコード	65280000Hex	
内容	セーフティ出力端子において ON 固着を検知しました。					
発生源	—		発生源詳細	—	検出タイミング	• Idle 時 • Executing 時
異常の属性	重要度	軽度フォールト	復旧方法	セーフティ出力端子をインアクティブにすることで復旧	ログカテゴリ	システム
発生の影響	ユーザプログラム	継続	動作	異常が解除されるまで、該当セーフティ出力端子はセーフティ状態に維持されます。		
発生要因とその処置	発生要因（推定原因）		処置対策		再発防止	
	出力信号線に電源（+側）が接触。		外部配線を確認してください。		あらかじめ処置対策の内容を考慮して設定や配線をしてください。	
	出力電源が仕様範囲外。		出力電源を確認してください。			
	内部回路の故障。 ソフトエラーや過度なノイズなどの一過性要因によるメモリ異常または信号異常。		電源を再投入してください。 再発する場合は、ユニットを交換してください。		電源再投入で正常に動作を再開できる場合は、ユニット周辺で過度なノイズが発生している可能性がありますので、ノイズ対策を検討してください。	
付属情報	付属情報 1: 端子番号					
注意点／備考	出力用電源に異常が発生した場合、セーフティ出力端子が ON 固着していなくても本異常が登録されることがあります。					

イベント名	出力用電源異常			イベントコード	65290000Hex	
内容	出力用電源の不正を検出しました。					
発生源	—		発生源詳細	—	検出タイミング	常時
異常の属性	重要度	軽度フォールト	復旧方法	自動復旧 ただし、出力用電源の電流が上昇して検出閾値を上回り、出力用電源が遮断された場合、出力用電源の電源再投入後に復旧	ログカテゴリ	システム
発生の影響	ユーザプログラム	継続	動作	該当ユニットは運転を継続しますが、出力データはセーフティ状態を維持します。		
発生要因とその処置	発生要因（推定原因）		処置対策		再発防止	
	• 出力用電源が接続されていない。 • 出力用電源の電圧が低下して検出閾値を下回り、出力用電源が遮断された。 • 出力用電源の電圧が上昇して検出閾値を上回り、出力用電源が遮断された。 • 出力用電源の電流が上昇して検出閾値を上回り、出力用電源が遮断された。		以下を確認のうえ、定格にあった電源を供給してください。 • 電源電圧が仕様の範囲内か • 配線に誤りや断線がないか • 電源配線の短絡による過電流が発生していないか 電圧を測定し正常である場合、ユニットの故障が考えられます。その場合はユニットを交換してください。		あらかじめ処置対策の内容を考慮して設計してください。	
付属情報	なし					
注意点／備考	なし					

イベント名	EDM 異常			イベントコード	652B0000Hex	
内容	EDM で異常を検知した。					
発生源	—		発生源詳細	—	検出タイミング	Executing 時
異常の属性	重要度	軽度フォールト	復旧方法	FB の出力とフィードバック入力の関係をインアクティブ状態にすることで復旧	ログカテゴリ	システム
発生の影響	ユーザプログラム	継続	動作	異常が解除されるまで、該当セーフティ出力端子はセーフティ状態に維持されます。		
発生要因とその処置	発生要因（推定原因）		処置対策		再発防止	
	以下の項目を確認してください。 • 出力信号線の断線 • 出力信号線の地絡 • 出力信号線が電源と接触していないか • 外部配線機器であるコンタクタおよびリレー接点の溶着 • 外部配線機器の断線、地絡		外部配線を確認してください。		あらかじめ処置対策の内容を考慮して設定や配線をしてください。	
付属情報	付属情報 1: 異常が発生した EDM の出力端子番号 0: So00～3: So03					
注意点／備考	なし					

イベント名	NTP サーバ接続失敗			イベントコード	84040000Hex	
内容	NTP サーバとの接続に失敗しました。					
発生源	—		発生源詳細	—	検出タイミング	NTP 動作時
異常の属性	重要度	軽度フォールト	復旧方法	自動復旧 サーバ指定を修正して再度ダウンロードした場合、電源再投入、または再起動の実行	ログカテゴリ	システム
発生の影響	ユーザプログラム	継続	動作	NTP による時刻の取得不可		
発生要因とその処置	発生要因（推定原因）		処置対策		再発防止	
	設定データの誤り。		接続先サーバの指定に間違いがある場合には、サーバ指定を修正して再度ダウンロードしてください。		接続先サーバの設定が正しいことを確認してください。	
	サーバダウン。		接続先サーバが正常に稼働しているか確認し、正常に稼働していない場合は正しく稼働させてください。		接続先サーバが正常に稼働していることを確認してください。	
	通信経路の異常発生。		サーバへの通信経路に問題がないかを調査し、問題がある場合には対策を行ってください。		なし	
付属情報	なし					
注意点／備考	処置完了後に［TCP アプリケーション機能の起動］がイベントログに記録されていれば、CPU ユニットが DNS サーバと正常に接続していることが確認できます。					

イベント名	DHCP サーバ接続失敗			イベントコード	840F0000Hex	
内容	DHCP サーバとの接続に失敗しました。					
発生源	—		発生源詳細	—	検出タイミング	DHCP 動作時
異常の属性	重要度	軽度フォールト	復旧方法	自動復旧	ログカテゴリ	システム
発生の影響	ユーザプログラム	継続	動作	EtherNet/IP 通信不可 DHCP サーバから応答があるまで DHCP サーバへ要求継続		

発生要因とその処置	発生要因（推定原因）	処置対策	再発防止
	サーバ設定の誤り。	接続先サーバの設定を修正してください。	接続先サーバの設定が正しいことを確認してください。
	サーバダウン。	接続先サーバが正常に稼働しているか確認し、正常に稼働していない場合は正しく稼働させてください。	接続先サーバが正常に稼働していることを確認してください。
	通信経路の異常発生。	サーバへの通信経路に問題がないかを調査し、問題がある場合には対策を行ってください。	なし

付属情報	なし
注意点／備考	なし

イベント名	IP アドレス重複異常			イベントコード	85E20000Hex	
内容	IP アドレスが重複しています。					
発生源	—		発生源詳細	—	検出タイミング	IP アドレス決定時
異常の属性	重要度	軽度フォールト	復旧方法	• 電源再投入 • 再起動の実行	ログカテゴリ	システム
発生の影響	ユーザプログラム	継続	動作	EtherNet/IP 通信不可 CIP Safety 通信不可		

発生要因とその処置	発生要因（推定原因）	処置対策	再発防止
	IP アドレスが、他ノードの IP アドレスと重複している。	次のいずれかの処置をしてください。 • 他ノードの IP アドレスを確認し、重複しないように IP アドレスの設定を修正する。 • IP アドレスが重複している他ノードをネットワークから離脱させる。 いずれの処置を行った場合も、実施後に電源再投入または再起動を実行してください。	ネットワーク内で、各ノードの IP アドレスが互いに重複しないように割り当ててください。

付属情報	付属情報 1: 重複した IP アドレス 例）192.168.250.1 の場合は、C0A8FA01Hex となります。
注意点／備考	設定された IP アドレスで ARP を送信し、ARP 応答があればアドレス重複異常となります。

イベント名	タグデータリンクタイムアウト			**イベントコード**	85E30000Hex	
内容	タグデータリンクでタイムアウトが発生しました。					
発生源	—		**発生源詳細**	—	**検出タイミング**	常時
異常の属性	**重要度**	軽度フォールト	**復旧方法**	自動復旧	**ログカテゴリ**	システム
発生の影響	**ユーザプログラム**	継続	**動作**	該当ユニットは運転を継続します。		

発生要因とその処置	**発生要因（推定原因）**	**処置対策**	**再発防止**
	オリジネータノードの電源 OFF。 オリジネータノードの通信停止。	オリジネータノードの状態を確認し、正常に起動してください。	オリジネータノードが正常に運転していることを確認してから、タグデータリンクを行ってください。
	EtherNet/IP の Ethernet ケーブルのコネクタのはずれ。	コネクタが正しく嵌合しているかを確認し、再接続してください。	コネクタを確実に接続してください。
	EtherNet/IP の Ethernet ケーブルの断線。	Ethernet ケーブルを交換してください。	なし
	EtherNet/IP ポートのリンクオフ。	リンクオフの発生要因も含めて「リンクオフ検知」(85E10000Hex)を参照してください。オリジネータノードおよび、経路上の機器の Firewall、Packet Filter 機能で CIP 通信を許可してください。	リンクオフの発生要因も含めて「リンクオフ検知」(85E10000Hex)を参照してください。
	ネットワーク通信負荷による経路上でのパケットロスト。	コネクションタイムアウト値を大きくするか、RPI を大きくしてください。またはネットワーク環境・機器を見直してください。	ネットワーク環境が過負荷にならないようにネットワークを設計してください。
	ノイズ。	ノイズが多い場合はノイズ対策を行ってください。	ノイズが多い場合はノイズ対策を行ってください。

付属情報	付属情報 1: オリジネータの IP アドレス 例）192.168.250.1 の場合は、C0A8FA01Hex となります。 付属情報 2: Assembly Instance No 025CHex: Input Assembly 1 03C0Hex: Input Assembly 2 03C1Hex: Input Assembly 3
注意点／備考	同一ノードで複数コネクションの異常が発生している場合、発生中の 1 コネクションだけイベントログを登録します。

イベント名	CIP Safety ターゲットコネクションタイムアウト			イベントコード	85E40000Hex	
内容	CIP Safety ターゲットコネクションでタイムアウトが発生しました。					
発生源	—		発生源詳細	—	検出タイミング	Executing 時
異常の属性	重要度	軽度フォールト	復旧方法	自動復旧	ログカテゴリ	システム
発生の影響	ユーザプログラム	継続	動作	該当ユニットは運転を継続しますが、異常を検出したセーフティコネクションの入出力データはセーフティ状態を維持します。		

発生要因とその処置	発生要因（推定原因）	処置対策	再発防止
	ケーブルの断線。	ケーブルの断線がないか確認してください。	処置対策の内容をあらかじめ考慮の上、システム構築を行ってください。
	オリジネータデバイスがコネクションを受け付けられない状態に遷移した。	オリジネータデバイスがコネクションを受け付けできる状態か確認してください。	
	通信設定のタイムアウト値が短すぎる。	通信設定のタイムアウト値が妥当か確認してください。	
	EtherNet/IP ポート設定、および経路上の機器の Packet Filter（簡易）機能、Packet Filter 機能でオリジネータノードからの CIP Safety パケットが許可されていない。	EtherNet/IP ポート設定、および経路上の機器の Packet Filter（簡易）機能、Packet Filter 機能でオリジネータノードからの CIP Safety パケットが許可されているか確認してください。	
	オリジネータノードの［CIP メッセージサーバ］が［使用しない］に設定されている。	オリジネータノードの［CIP メッセージサーバ］［使用する］に設定されているか確認してください。	
	オリジネータノードの PacketFilter 機能が有効の場合にターゲットノードからの CIP Safety パケットが許可されていない。	オリジネータノードの PacketFilter 設定にターゲットノードからの CIP Safety パケットが許可されているか確認してください。	
	ノイズ。	ノイズの影響がないか確認してください。	
	EtherNet/IP ポート設定の［CIP Safety 通信］が［使用しない］に設定されている。	EtherNet/IP ポート設定の［CIP Safety 通信］が［使用する］に設定されているか確認してください。	

付属情報	付属情報 1: Assembly Instance No
注意点／備考	なし

イベント名	ユニット/入力用電源仕様範囲外電圧検知			イベントコード	652F0000Hex	
内容	ユニット/入力用電源の電圧が仕様範囲外であることを検知しました。					
発生源	—		発生源詳細	—	検出タイミング	常時
異常の属性	重要度	監視情報	復旧方法	自動復旧	ログカテゴリ	システム
発生の影響	ユーザプログラム	継続	動作	影響なし		

発生要因とその処置	発生要因（推定原因）	処置対策	再発防止
	ユニット/入力用電源の電圧が仕様範囲外であることを検知した。	ユニット/入力用電源の電圧を仕様範囲内の正常値に調整してください。	なし

付属情報	付属情報 1: ユニット/入力用電源の電圧モニタ値 100mV 単位
注意点／備考	なし

イベント名	ユニット/入力用電源仕様範囲外電流検知		イベントコード	65300000Hex		
内容	ユニット/入力用電源の電流が仕様範囲外であることを検知した。					
発生源	—		発生源詳細	—	検出タイミング	常時

異常の属性	重要度	監視情報	復旧方法	自動復旧	ログカテゴリ	システム
発生の影響	ユーザプログラム	継続	動作	影響なし		
発生要因とその処置	発生要因（推定原因）		処置対策		再発防止	
	ユニット/入力用電源の電流が仕様範囲外であることを検知した。		ユニット/入力用電源の電流を仕様範囲内の正常値に調整してください。		なし	
付属情報	付属情報 1: ユニット/入力用電源の電流モニタ値 100mA 単位					
注意点／備考	なし					

イベント名	出力用電源仕様範囲外電圧検知			イベントコード	65310000Hex	
内容	出力用電源の電圧が仕様範囲外であることを検知しました。					
発生源	—		発生源詳細	—	検出タイミング	常時
異常の属性	重要度	監視情報	復旧方法	自動復旧	ログカテゴリ	システム
発生の影響	ユーザプログラム	継続	動作	影響なし		
発生要因とその処置	発生要因（推定原因）		処置対策		再発防止	
	出力用電源の電圧が仕様範囲外であることを検知した。		出力用電源の電圧を仕様範囲内の正常値に調整してください。		なし	
付属情報	付属情報 1: 出力用電源の電圧モニタ値 100mV 単位					
注意点／備考	なし					

イベント名	出力用電源仕様範囲外電流検知			イベントコード	65320000Hex	
内容	出力用電源の電流が仕様範囲外であることを検知しました。					
発生源	—		発生源詳細	—	検出タイミング	常時
異常の属性	重要度	監視情報	復旧方法	自動復旧	ログカテゴリ	システム
発生の影響	ユーザプログラム	継続	動作	影響なし		
発生要因とその処置	発生要因（推定原因）		処置対策		再発防止	
	出力用電源の電流が仕様範囲外であることを検知した。		出力用電源の電流を仕様範囲内の正常値に調整してください。		なし	
付属情報	付属情報 1: 出力用電源の電流モニタ値 100mA 単位					
注意点／備考	なし					

イベント名	リンクオフ検知			イベントコード	85E10000Hex	
内容	Ethernet のリンクオフを検知しました。					
発生源	—		発生源詳細	—	検出タイミング	常時
異常の属性	重要度	監視情報	復旧方法	自動復旧	ログカテゴリ	システム
発生の影響	ユーザプログラム	継続	動作	EtherNet/IP 通信不可。		
発生要因とその処置	発生要因（推定原因）		処置対策		再発防止	
	Ethernet ケーブルの断線、ゆるみ、はずれ。		Ethernet ケーブルを確実に接続してください。 ケーブルが断線している場合にはケーブルを交換してください。		Ethernet ケーブルを確実に接続してください。また、使用するケーブルが断線していないことを確認してください。	
	スイッチングハブの電源 OFF。		スイッチングハブの電源を ON にしてください。 スイッチングハブが故障している場合は、スイッチングハブを交換してください。		スイッチングハブの電源を切らないでください。	
	通信速度不一致。		通信相手ノードと同じ通信速度になるように設定を修正してください。		通信相手ノードと同じ通信速度の設定を行ってください。	
	ノイズ。		ノイズが多い場合は、ノイズ対策を行ってください。		ノイズ対策を行ってください。	
	再起動又はメモリオールクリアを実行。		なし。左記の操作を行うと本イベントが発生します。		なし。左記の操作を行うと本イベントが発生します。	
付属情報	付属情報 1: リンクオフを検出した EtherNet/IP 通信コネクタ 1: EtherNet/IP 通信コネクタ 1 (ETH1) 2: EtherNet/IP 通信コネクタ 2 (ETH2)					
注意点／備考	なし					

イベント名	CIP Safety ターゲットコネクション開設要求			イベントコード	85E50000Hex	
内容	CIP Safety オリジネータからコネクション開設要求がありました。					
発生源	—		発生源詳細	—	検出タイミング	• Idle 時 • Executing 時
異常の属性	重要度	一般情報	復旧方法	—	ログカテゴリ	アクセス
発生の影響	ユーザプログラム	継続	動作	影響なし		
発生要因とその処置	発生要因（推定原因）		処置対策		再発防止	
	CIP Safety オリジネータからコネクション開設要求があった。		—		—	
付属情報	付属情報 1: 予約 付属情報 2: Assembly Instance No 付属情報 3: CIP 仕様で定義された General Status 付属情報 4: CIP 仕様で定義された Extended Status					
注意点／備考	なし					

イベント名	電源投入			イベントコード	90110000Hex	
内容	電源が投入されました。					
発生源	—		発生源詳細	—	検出タイミング	電源投入時
異常の属性	重要度	一般情報	復旧方法	—	ログカテゴリ	システム
発生の影響	ユーザプログラム	継続	動作	動作開始		
発生要因とその処置	発生要因（推定原因）		処置対策		再発防止	
	電源を投入した。		なし		なし	
付属情報	なし					
注意点／備考	なし					

イベント名	IP アドレス決定			イベントコード	94080000Hex	
内容	正しく IP アドレスが決定し、Ethernet 通信動作を開始できる状態になりました。					
発生源	—		発生源詳細	—	検出タイミング	• 電源投入時 • 再起動実行時
異常の属性	重要度	一般情報	復旧方法	—	ログカテゴリ	システム
発生の影響	ユーザプログラム	継続	動作	影響なし		
発生要因とその処置	発生要因（推定原因）		処置対策		再発防止	
	正しく IP アドレスが決定し、Ethernet 通信動作を開始できる状態になった。		なし		なし	
付属情報	付属情報 1: IP アドレス 例）192.168.250.1 の場合は、C0A8FA01Hex となります。					
注意点／備考	なし					

イベント名	コンフィグレーションロック			イベントコード	966C0000Hex	
内容	コンフィグレーションロックが実行されました。					
発生源	—		発生源詳細	—	検出タイミング	コンフィグレーションロック実行時
異常の属性	重要度	一般情報	復旧方法	—	ログカテゴリ	アクセス
発生の影響	ユーザプログラム	継続	動作	影響なし		
発生要因とその処置	発生要因（推定原因）		処置対策		再発防止	
	コンフィグレーションロック実行。		なし		なし	
付属情報	付属情報 1: 予約 付属情報 2: SCCRC 付属情報 3: コンフィグレーションロックを実行した時のロータリスイッチの設定値 表示フォーマットは [SW1, SW2, x16^{1}, x16^{0}] 例: SW1=3、SW2=3、x16^{1}=0、x16^{0}=1 の場合、3301Hex となります。					
注意点／備考	なし					

イベント名	コンフィグレーションロック解除			イベントコード	966D0000Hex	
内容	コンフィグレーションロック解除が実行されました。					
発生源	—		発生源詳細	—	検出タイミング	コンフィグレーションロック解除実行時
異常の属性	重要度	一般情報	復旧方法	—	ログカテゴリ	アクセス
発生の影響	ユーザプログラム	継続	動作	影響なし		
発生要因とその処置	発生要因（推定原因）		処置対策		再発防止	
	コンフィグレーションロック解除実行。		なし		なし	
付属情報	付属情報 1: 予約					
注意点／備考	なし					

イベント名	出力用電源(PWR OUT)の OFF			イベントコード	96710000Hex	
内容	電源コネクタ PWR OUT から供給される出力用電源が OFF されました。					
発生源	—		発生源詳細	—	検出タイミング	出力用電源(PWR OUT)OFF 時
異常の属性	重要度	一般情報	復旧方法	—	ログカテゴリ	アクセス
発生の影響	ユーザプログラム	継続	動作	電源コネクタ PWR OUT から供給される出力用電源が OFF されます。		
発生要因とその処置	発生要因（推定原因）		処置対策		再発防止	
	「渡り配線出力用電源の遮断指示」で渡り配線出力用電源の遮断を指示した。		なし		なし	
付属情報	なし					
注意点／備考	なし					

イベント名	設定データ変更			イベントコード	96720000Hex	
内容	設定データが変更されました。					
発生源	—		発生源詳細	—	検出タイミング	設定変更時
異常の属性	重要度	一般情報	復旧方法	—	ログカテゴリ	アクセス
発生の影響	ユーザプログラム	継続	動作	影響なし		
発生要因とその処置	発生要因（推定原因）		処置対策		再発防止	
	設定データが変更された。		なし		なし	
付属情報	付属情報 1: 予約 付属情報 2: 変更対象 0100Hex: TCP/IP 設定(IP 決定方式) 0101Hex: TCP/IP 設定(IP アドレス) 0102Hex: TCP/IP 設定(Encapsulation Inactivity Timeout) 0200Hex: LINK 設定 0300Hex: 通信ポート有効無効機能の設定 0400Hex: 時計情報自動調整機能の設定(NTP/SNTP サーバの IP アドレス) 0401Hex: 時計情報自動調整機能の設定(タイムゾーン) 0500Hex: 渡り配線出力用電源遮断機能の設定 2000Hex: セーフティパスワード 2006Hex: コンフィグレーションロック状態 2008Hex: リストア実行中フラグ 2001Hex: TUNID 2002Hex: Alarm Enable 2003Hex: Warning Enable 2004Hex: Output Connection Owner 2005Hex: CFUNID 21*1Hex: コンフィグレーションデータ 21*2Hex: SCID 21*5Hex: アプリケーション名 21*6Hex: バージョン 21*7Hex: 作成者 (*はアプリケーション番号を示す 0～F の値) 8000Hex: QoS 設定(DSCP Urgent) 8001Hex: QoS 設定(DSCP Scheduled) 8002Hex: QoS 設定(DSCP High) 8003Hex: Qos 設定(DSCP Low) 8004Hex: Qos 設定(DSCP Explicit) 8100Hex: LLDP 設定(LLDP Enable) 8101Hex: LLDP 設定(LLDP Tx Interval) 8102Hex: LLDP 設定(LLDP Tx Hold)					
注意点／備考	なし					

イベント名	ログイン			**イベントコード**	96730000Hex	
内容	ログインしました。(Web UI)					
発生源	—		**発生源詳細**	—	**検出タイミング**	ユーザ操作時 (Web UI)
異常の属性	**重要度**	一般情報	**復旧方法**	—	**ログカテゴリ**	アクセス
発生の影響	**ユーザプログラム**	継続	**動作**	影響なし		
発生要因とその処置	**発生要因（推定原因）**		**処置対策**		**再発防止**	
	Web UI を使ってログインした。		なし		なし	
付属情報	付属情報 1: 接続元の IP アドレス 例）192.168.250.100 の場合は、C0A8FA64Hex となります。 付属情報 2: ログイン権限種別 0: 管理者権限によるログイン 1: 観察者権限によるログイン					
注意点／備考	なし					

イベント名	安全アプリケーションの削除			**イベントコード**	96750000Hex	
内容	安全アプリケーションデータがユニットから削除されました。					
発生源	—		**発生源詳細**	—	**検出タイミング**	ユーザからの指示（削除）時
異常の属性	**重要度**	一般情報	**復旧方法**	—	**ログカテゴリ**	アクセス
発生の影響	**ユーザプログラム**	継続	**動作**	影響なし		
発生要因とその処置	**発生要因（推定原因）**		**処置対策**		**再発防止**	
	Web UI からの削除を受け付けた。		なし		なし	
付属情報	付属情報 1: 予約 付属情報 2: アプリケーション番号					
注意点／備考	なし					

イベント名	セーフティパスワード不一致			**イベントコード**	96760000Hex	
内容	セーフティパスワードが必要なサービス実行時にセーフティパスワード不一致を検出しました。					
発生源	—		**発生源詳細**	—	**検出タイミング**	パスワードが必要なサービス実行時
異常の属性	**重要度**	一般情報	**復旧方法**	—	**ログカテゴリ**	アクセス
発生の影響	**ユーザプログラム**	継続	**動作**	該当ユニットは運転を継続します。		
発生要因とその処置	**発生要因（推定原因）**		**処置対策**		**再発防止**	
	セーフティパスワードが必要なサービスでパスワード不一致を検出した。		正しいセーフティパスワードを入れてサービスを再実行してください。		なし	
付属情報	付属情報 1: 予約					
注意点／備考	なし					

イベント名	出力用電源(PWR OUT)の ON			イベントコード	96770000Hex	
内容	電源コネクタ PWR OUT から供給される出力用電源が ON されました。					
発生源	—		発生源詳細	—	検出タイミング	出力用電源(PWR OUT)ON 時
異常の属性	重要度	一般情報	復旧方法	—	ログカテゴリ	アクセス
発生の影響	ユーザプログラム	継続	動作	電源コネクタ PWR OUT から供給される出力用電源が ON されます。		
発生要因とその処置	発生要因（推定原因）		処置対策		再発防止	
	「渡り配線出力用電源の復帰指示」で渡り配線出力用電源の復帰を指示した。		なし		なし	
付属情報	なし					
注意点／備考	なし					

イベント名	ファームウェアアップデート実行			イベントコード	96780000Hex	
内容	ファームウェアアップデートを実行しました。					
発生源	—		発生源詳細	—	検出タイミング	ファームウェアアップデート時
異常の属性	重要度	一般情報	復旧方法	—	ログカテゴリ	アクセス
発生の影響	ユーザプログラム	継続	動作	影響なし		
発生要因とその処置	発生要因（推定原因）		処置対策		再発防止	
	ファームウェアアップデートが実行された。		なし		なし	
付属情報	付属情報 1: 接続元の IP アドレス 例）192.168.250.100 の場合は、C0A8FA64Hex となります。 付属情報 2: 実行結果 0000Hex: 成功 0001Hex: 失敗 付属情報 3: 書き込んだファームウェアのバージョン(BCD) 例）Ver.1.10.01 の場合は、01100100Hex となります。					
注意点／備考	なし					

イベント名	メモリオールクリア			イベントコード	96790000Hex	
内容	メモリオールクリアが実行されました。					
発生源	—		発生源詳細	—	検出タイミング	メモリオールクリア実行時
異常の属性	重要度	一般情報	復旧方法	—	ログカテゴリ	アクセス
発生の影響	ユーザプログラム	継続	動作	リセット後、動作開始。		
発生要因とその処置	発生要因（推定原因）		処置対策		再発防止	
	メモリオールクリアが実行された。		なし		なし	
付属情報	付属情報 1: 予約 付属情報 2: リセット種別 1: メモリオールクリア（付属情報 3 のデータをすべて削除） 2: メモリオールクリア（付属情報 3 のデータの一部を削除） 付属情報 3: 初期化されなかったデータ（該当 Bit の値が 1 のデータは初期化されていない）*1 Bit0: IP Address Bit2: TUNID Bit3: Password Bit4: CFUNID Bit5: Output Connection Owner					
注意点／備考	なし					

***1.** 付属情報 2 が［2］の時だけ有効になります。

イベント名	リンクオン検知			イベントコード	967A0000Hex	
内容	Ethernet のリンク確立を検知しました。					
発生源	—		発生源詳細	—	検出タイミング	リンク確立時
異常の属性	重要度	一般情報	復旧方法	—	ログカテゴリ	システム
発生の影響	ユーザプログラム	継続	動作	影響なし		
発生要因とその処置	発生要因（推定原因）		処置対策		再発防止	
	Ethernet のリンク確立を検知した。		なし		なし	
付属情報	付属情報 1: リンクオンを検出した EtherNet/IP 通信コネクタ 1: EtherNet/IP 通信コネクタ 1（ETH1） 2: EtherNet/IP 通信コネクタ 2（ETH2）					
注意点／備考	なし					

イベント名	動作モードの変更			イベントコード	967B0000Hex	
内容	動作モード変更が実行されました。					
発生源	—		発生源詳細	—	検出タイミング	動作モード変更実行時
異常の属性	重要度	一般情報	復旧方法	—	ログカテゴリ	アクセス
発生の影響	ユーザプログラム	継続	動作	影響なし		
発生要因とその処置	発生要因（推定原因）		処置対策		再発防止	
	動作モード変更実行。		なし		なし	
付属情報	付属情報 1: 予約 付属情報 2: 変更後の動作モード 2: Idle 3: Executing					
注意点／備考	なし					

イベント名	セーフティパスワードの変更			イベントコード	967C0000Hex	
内容	セーフティパスワードを変更しました。					
発生源	—		発生源詳細	—	検出タイミング	ユーザからの指示（転送）時
異常の属性	重要度	一般情報	復旧方法	—	ログカテゴリ	アクセス
発生の影響	ユーザプログラム	継続	動作	影響なし		
発生要因とその処置	発生要因（推定原因）		処置対策		再発防止	
	セーフティパスワードを変更した。		なし		なし	
付属情報	付属情報 1: 予約					
注意点／備考	なし					

イベント名	安全アプリケーションの転送			イベントコード	967D0000Hex	
内容	安全アプリケーションデータがユニットへ転送されました。					
発生源	—		発生源詳細	—	検出タイミング	• ユーザからの指示（転送）時 • Type1 Safety Open 受付時
異常の属性	重要度	一般情報	復旧方法	—	ログカテゴリ	アクセス
発生の影響	ユーザプログラム	継続	動作	影響なし		
発生要因とその処置	発生要因（推定原因）		処置対策		再発防止	
	• Web UI での転送を受け付けた。 • セーフティコントローラから Type1 Safety Open 処理を受け付けた。		なし		なし	
付属情報	付属情報 1: 予約 付属情報 2: アプリケーション番号 付属情報 3: SCCRC 付属情報 4: 設定方法 1: Type1 Safety Open 2: Web UI 機能での設定					
注意点／備考	なし					

イベント名	イベントログのクリア			イベントコード	967E0000Hex	
内容	イベントログをクリアしました。					
発生源	—		発生源詳細	—	検出タイミング	常時
異常の属性	重要度	一般情報	復旧方法	—	ログカテゴリ	アクセス
発生の影響	ユーザプログラム	継続	動作	影響なし		
発生要因とその処置	発生要因（推定原因）		処置対策		再発防止	
	イベントログをクリアした。		なし		なし	
付属情報	付属情報 1: 接続元の IP アドレス 例）192.168.250.1 の場合は、C0A8FA01Hex となります。 付属情報 2: クリア対象 0: 全カテゴリのログをクリア 1: システムイベントログをクリア 2: アクセスイベントログをクリア					
注意点／備考	なし					

イベント名	バックアップ実行			イベントコード	967F0000Hex	
内容	バックアップを実行しました。					
発生源	—		発生源詳細	—	検出タイミング	バックアップ時
異常の属性	重要度	一般情報	復旧方法	—	ログカテゴリ	アクセス
発生の影響	ユーザプログラム	継続	動作	影響なし		
発生要因とその処置	発生要因（推定原因）		処置対策		再発防止	
	バックアップが実行された。		なし		なし	
付属情報	付属情報 1: 接続元の IP アドレス 例）192.168.250.100 の場合は、C0A8FA64Hex となります。 付属情報 2: 実行結果 0000Hex: 成功 0001Hex: 失敗					
注意点／備考	なし					

イベント名	リストア実行			**イベントコード**	96800000Hex	
内容	リストアを実行しました。					
発生源	—		**発生源詳細**	—	**検出タイミング**	リストア時
異常の属性	**重要度**	一般情報	**復旧方法**	—	**ログカテゴリ**	アクセス
発生の影響	**ユーザプログラム**	継続	**動作**	影響なし		
発生要因とその処置	**発生要因（推定原因）**		**処置対策**		**再発防止**	
	リストアが実行された。		なし		なし	
付属情報	付属情報 1: 接続元の IP アドレス 　例）192.168.250.100 の場合は、C0A8FA64Hex となります。 付属情報 2: 実行結果 　0000Hex: 成功 　0001Hex: 失敗					
注意点／備考	なし					

イベント名	オムロン保守の実行			**イベントコード**	96810000Hex	
内容	オムロンの保守担当者による保守作業が実行されました。					
発生源	—		**発生源詳細**	—	**検出タイミング**	オムロン保守の実行時
異常の属性	**重要度**	一般情報	**復旧方法**	—	**ログカテゴリ**	アクセス
発生の影響	**ユーザプログラム**	継続	**動作**	影響なし		
発生要因とその処置	**発生要因（推定原因）**		**処置対策**		**再発防止**	
	オムロンの保守担当者による保守作業が実行された。		なし		なし	
付属情報	付属情報 1: 接続元の IP アドレス 　例）192.168.250.100 の場合は、C0A8FA64Hex となります。					
注意点／備考	なし					

イベント名	再起動			**イベントコード**	96820000Hex	
内容	再起動が実行された。					
発生源	—		**発生源詳細**	—	**検出タイミング**	再起動実行時
異常の属性	**重要度**	一般情報	**復旧方法**	—	**ログカテゴリ**	アクセス
発生の影響	**ユーザプログラム**	継続	**動作**	影響なし		
発生要因とその処置	**発生要因（推定原因）**		**処置対策**		**再発防止**	
	再起動が実行された。		なし		なし	
付属情報	付属情報 1: 予約					
注意点／備考	なし					

イベント名	セーフティコンフィグレーション確定			イベントコード	96830000Hex	
内容	セーフティコンフィグレーションデータが確定した。					
発生源	—		発生源詳細	—	検出タイミング	• 電源投入時 • 再起動実行時
異常の属性	重要度	一般情報	復旧方法	—	ログカテゴリ	システム
発生の影響	ユーザプログラム	継続	動作	影響なし		
発生要因とその処置	発生要因（推定原因）		処置対策		再発防止	
	セーフティコンフィグレーションデータが確定した。		なし		なし	
付属情報	付属情報 1: アプリケーション番号 付属情報 2: SCCRC 付属情報 3: コンフィグレーションロック状態 0: ロック解除 1: ロック 付属情報 4: 電源投入時モード 0: Idle 1: Executing					
注意点／備考	なし					

イベント名	IP アドレス表示機能実行			イベントコード	96840000Hex	
内容	IP アドレス表示機能が実行されました。					
発生源	—		発生源詳細	—	検出タイミング	• 電源投入時 • 再起動実行時
異常の属性	重要度	一般情報	復旧方法	—	ログカテゴリ	システム
発生の影響	ユーザプログラム	継続	動作	影響なし		
発生要因とその処置	発生要因（推定原因）		処置対策		再発防止	
	SW1=SW2=8（IP アドレス表示機能）で起動した。		なし		なし	
付属情報	なし					
注意点／備考	なし					

イベント名	I/O 配線チェック機能実行			イベントコード	96850000Hex	
内容	I/O 配線チェック機能が実行されました。					
発生源	—		発生源詳細	—	検出タイミング	• 電源投入時 • 再起動実行時
異常の属性	重要度	一般情報	復旧方法	—	ログカテゴリ	システム
発生の影響	ユーザプログラム	継続	動作	影響なし		
発生要因とその処置	発生要因（推定原因）		処置対策		再発防止	
	SW1=SW2=E（I/O 配線チェック機能）で起動した。		なし		なし	
付属情報	なし					
注意点／備考	なし					

12

保守点検

この章では、セーフティ I/O ターミナルの保守点検について説明しています。

12-1　清掃と点検 12-2
12-1-1　清掃方法 12-2
12-1-2　点検方法 12-2
12-2　ユニットの交換 12-4
12-2-1　ユニット交換時の注意事項 12-4
12-2-2　バックアップ機能を使ったユニット交換 12-4
12-2-3　バックアップ機能を使わないユニット交換 12-5

12-1 清掃と点検

ここでは、日常の機器のメンテナンスとして、清掃方法と点検方法について説明します。
セーフティ I/O ターミナルの機能を最良の状態で使用していただくために、日常あるいは定期的な点検をお願いします。

12-1-1 清掃方法

機器を常に最良の状態で使用するために、次のように定期的に清掃を行ってください。

- 日常の清掃時には、乾いたやわらかい布で乾拭きしてください。
- 乾拭きでも汚れが落ちないときは、布を十分に薄めた中性洗剤(2%)で湿らせて、固く絞ってから拭いてください。
- ユニットにゴムやビニール製品、テープなどを長時間付着させておくと、シミが付くことがあります。付着している場合は、清掃時に取り除いてください。

使用上の注意

ベンジンやシンナーなどの揮発性の溶剤や化学雑巾などは、絶対に使用しないでください。製品の刻印および印刷が変質する恐れがあります。

12-1-2 点検方法

機器を最良の状態でご使用いただくためにも、定期点検を欠かさず行ってください。
点検は、通常は 6 ヶ月～1 年に 1 回（安全性能確認テストは 1 ヶ月に 1 回）の間隔で実施してください。
ただし、極端に高温多湿の環境やほこりの多い環境などで使用する場合は、点検間隔を短くしてください。
もし判定基準内から外れているときは、基準内に入るように処置してください。判定基準に関しては「点検項目(P.12-3)」を参照してください。

- ユニットの仕様範囲内で使用されていることを確認してください。
- ユニットの取付状態や配線が正常であることを確認してください。
- 安全機能の作動信頼性を一定の水準に維持するために、安全機能の診断を行ってください。
- 診断処理の一部は、通常処理のアイドル時間中に分割して実行されるため、すべての診断を完了するには、本製品を最低 8 時間連続稼働させてください。

点検に必要な機材

● 日常的に必要なもの

- プラスドライバ
- トルクレンチ
- テスタまたはデジタルボルトメータ
- 工業用アルコールと純綿布

● 場合により必要なもの

- オシロスコープ
- 温度計、湿度計

点検項目

以下の項目について、判定基準から外れていないかどうかを点検します。
判定基準から外れているときは、基準内に入るように周囲の環境を改善するか、本体を調整してください。

点検項目	点検内容	判定基準	点検手段
環境状態	周囲および盤内温度は適当か	−10～55℃	温度計
	周囲および盤内湿度は適当か	25～85%（結露なきこと）	湿度計
	ほこりが積もっていないか	ほこりのないこと	目視
取り付け状態	ユニットはしっかり固定されているか	ゆるみのないこと	プラスドライバ
	各ケーブルおよび防水カバーは適切なトルクでユニットのコネクタに締め付けられているか	規定のトルク値	トルクレンチ
	ロータリスイッチ用カバーはゆるんでいないか	ゆるみのないこと	プラスドライバ
	接続ケーブルは切れかかっていないか	外観に異常のないこと	目視
安全性能確認テスト（ユーザテスト）	すべての安全機能が正しく動作するか	意図とおりに正しく動作すること	安全機能を作動させるための操作を行う。

12-2 ユニットの交換

稼働しているセーフティ I/O ターミナルの故障やメンテナンス等で交換を行うための方法について説明します。
ユニット交換には以下の２つの方法があります。
バックアップ機能を使ったユニット交換では、お客様が設定した全ての安全アプリケーションと非安全機能の設定データを一括して設定することができます。
バックアップ機能を使用しない場合、必要な設定を個別に設定してください。
- バックアップ機能を使ったユニット交換
- バックアップ機能を使わないユニット交換

12-2-1 ユニット交換時の注意事項

点検などで不良を発見して本体を交換するときは、次の点に注意してください。
- 必ず安全制御の知識がある作業者が交換作業を行ってください。
- 作業者の安全のため、アクチュエータなどの危険源の電源を OFF にしてください。
- セーフティ I/O ターミナルは、ネットワークを構成する機器です。ユニットが故障した場合、ネットワーク全体に影響を及ぼすことがありますので、速やかに修復作業を行ってください。ネットワーク機能の修復をできるだけ早く行うために、交換用に予備の機器を用意するようお勧めします。
- 交換後は、新しい機器にも異常がないか確認してください。
- 不良機器を修理のために返却される場合は、不良の内容についてできるだけ詳細に記載した用紙を機器に添付して、当社支店または営業所へお送りください。
- 接触不良の場合は、接点をきれいな純綿布に工業用アルコールを染み込ませたもので拭いてください。

12-2-2 バックアップ機能を使ったユニット交換

ここでは、バックアップ機能を使ったセーフティ I/O ターミナルのユニット交換について説明します。
あらかじめバックアップ機能を使ってバックアップファイルを作成しておくことで、設定データの復旧が簡単にでき、復旧にかかる工数が低減できます。コンフィグレーションロック時にバックアップをとることを推奨します。バックアップ機能の詳細につきましては「7-19 バックアップ (P.7-104)」、リストア手順につきましては「リストア (P.7-105)」を参照してください。

交換手順を以下に示します。

手順	項目	内容	使用ツール
1	バックアップの実行*1	バックアップを実行します。 本手順は、交換作業前に事前に実施しておいてください。 装置の立上時に実施しておくことを推奨します。	Web UI
2	取り付けと配線	交換元のセーフティ I/O ターミナルを取り外し、交換するセーフティ I/O ターミナルを取り付けます。 ロータリスイッチの設定を、交換元ユニットと同じ設定にします。 Ethernet、電源、I/O ケーブルを配線します。 パソコンをセーフティ I/O ターミナルに接続します。	不要
3	セーフティパスワードの設定*1	セーフティ I/O ターミナルのセーフティパスワードを設定します。	Web UI
4	リストアの実行*1	セーフティ I/O ターミナルへのリストアを実行します。	Web UI
5	電源の OFF/ON	セーフティ I/O ターミナルの電源を OFF/ON、もしくは再起動します。	不要

手順	項目	内容	使用ツール
6	CIP Safety コネクションと EtherNet/IP コネクションの確立	CIP Safety オリジネータおよび EtherNet/IP オリジネータは、セーフティ I/O ターミナルとコネクションを確立します。	不要

***1.** 作業には、セーフティパスワードが必要です。

12-2-3 バックアップ機能を使わないユニット交換

ここでは、バックアップ機能を使わないセーフティ I/O ターミナルのユニット交換について説明します。

- セーフティコントローラが制御する構成（Type 1 Safety Open によるコンフィグレーション）の場合
「7-1-1 セーフティコントローラが制御する構成（Type 1 Safety Open によるコンフィグレーション）の設定手順 (P.7-3)」のうち、セーフティ I/O ターミナルに対する設定のみ実行してください。
リモート IO 用安全アプリケーションは、セーフティコントローラとセーフティ I/O ターミナル間の Type1 Safety Open コネクションが確立する際に、セーフティコントローラによってコンフィグレーションされます。

- セーフティコントローラが制御する構成（Web UI によるコンフィグレーション）の場合
「7-1-2 セーフティコントローラが制御する構成（Web UI によるコンフィグレーション）の設定手順 (P.7-6)」のうち、セーフティ I/O ターミナルに対する設定のみ実行してください。
リモート IO 用安全アプリケーションは、Web UI を使用してセーフティ I/O ターミナルに安全アプリケーションファイルをダウンロードすることでコンフィグレーションされます。

- プリセットされた安全アプリケーションでセーフティ I/O ターミナルが制御する構成の場合
「7-1-3 プリセットされた安全アプリケーションでセーフティ I/O ターミナルが制御する構成の設定手順 (P.7-9)」のうち、セーフティ I/O ターミナルに対する設定のみ実行してください。
セーフティ I/O ターミナルの固定アプリケーションは、ロータリスイッチの SETTING SW1、SW2 で設定できます。

- ユーザが設計した安全アプリケーションでセーフティ I/O ターミナルが制御する構成（集中管理型）の場合
「7-1-4 ユーザが設計した安全アプリケーションでセーフティ I/O ターミナルが制御する構成（集中管理型）の設定手順 (P.7-11)」のうち、セーフティ I/O ターミナルに対する設定のみ実行してください。
ユーザ定義アプリケーションは、セーフティコントローラとセーフティ I/O ターミナル間の Type1 Safety Open コネクションが確立する際に、セーフティコントローラによってコンフィグレーションされます。

- ユーザが設計した安全アプリケーションでセーフティ I/O ターミナルが制御する構成（分散管理型）の場合
「7-1-5 ユーザが設計した安全アプリケーションでセーフティ I/O ターミナルが制御する構成（分散管理型）の設定手順 (P.7-13)」のうち、セーフティ I/O ターミナルに対する設定のみ実行してください。
アドオンアプリケーションは、Web UI を使用してセーフティ I/O ターミナルに安全アプリケーションファイルをダウンロードすることでコンフィグレーションされます。

A

付録

この章では、セーフティ I/O ターミナルの外形寸法、セーフティ I/O アセンブリデータなど、本文の補足的情報について説明します。

A-1　外形寸法 A-2

A-2　セーフティ I/O アセンブリデータ A-4
A-2-1　セーフティ入力アセンブリデータ A-4
A-2-2　セーフティ出力アセンブリデータ A-5
A-2-3　コンフィグレーションアセンブリデータ A-7

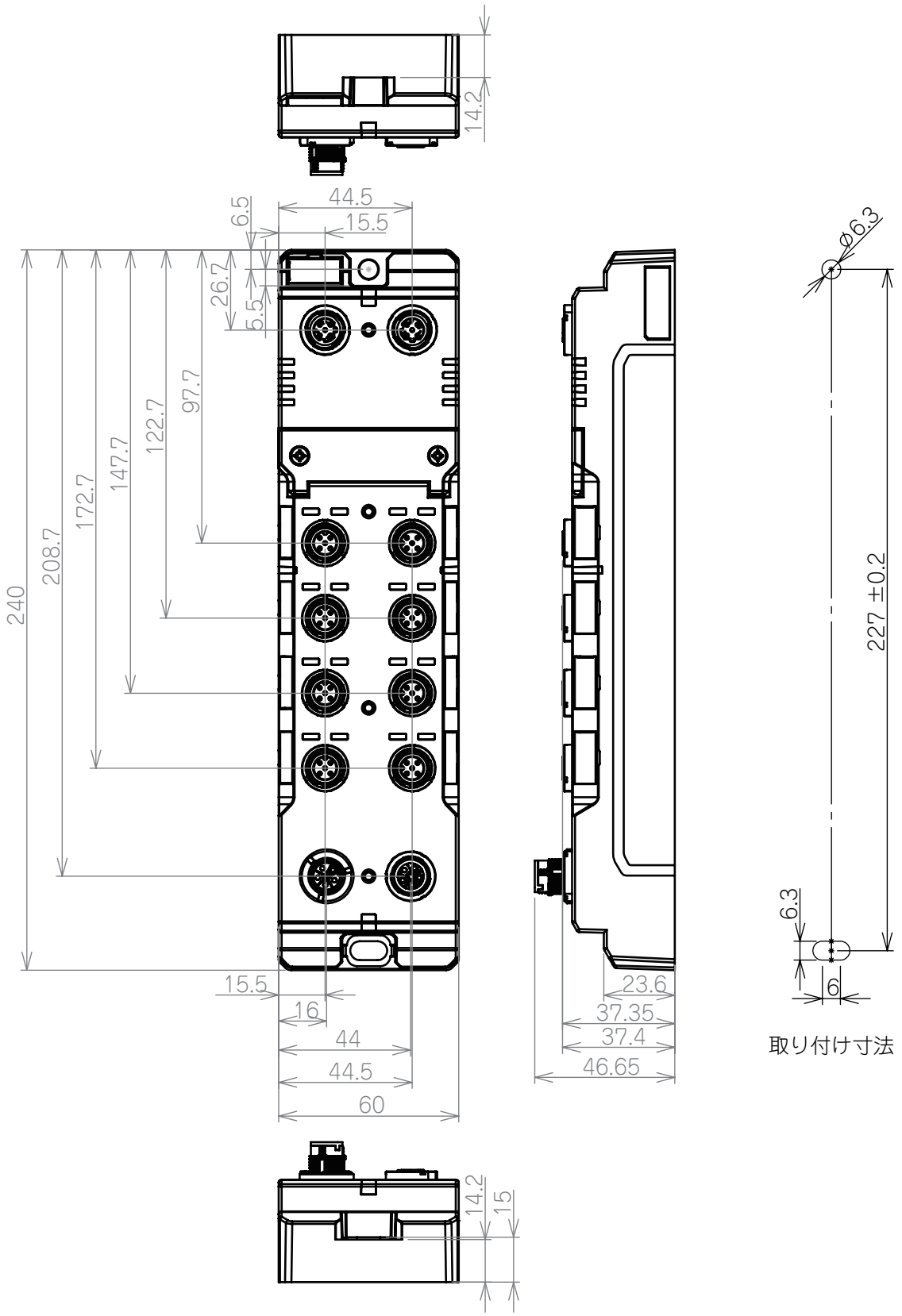
A-3　I/O アセンブリのポートと対応するセーフティ I/O アセンブリデータの要素 A-13

A-4　サポートする CIP オブジェクト A-15
A-4-1　Identity オブジェクト（クラス ID：01Hex） A-16
A-4-2　Assembly オブジェクト（クラス ID：04Hex） A-18
A-4-3　Unit Manager オブジェクト（クラス ID：380Hex） A-21
A-4-4　Event History Log オブジェクト（クラス ID：34BHex） A-25
A-4-5　Error Event オブジェクト（クラス ID：34CHex） A-28
A-4-6　Safety Discrete Input Point (SDIP)オブジェクト（クラス ID：3DHex） A-31
A-4-7　Safety Discrete Ouput Point (SDOP)オブジェクト（クラス ID：3BHex） A-33
A-4-8　Device Level Ring (DLR)オブジェクト（クラス ID：47Hex） A-35
A-4-9　QoS オブジェクト（クラス ID：48Hex） A-37
A-4-10　TCP/IP Interface オブジェクト（クラス ID：F5Hex） A-39
A-4-11　Ethernet Link オブジェクト（クラス ID：F6Hex） A-43
A-4-12　LLDP Management オブジェクト（クラス ID：109Hex） A-48
A-4-13　LLDP Data Table オブジェクト（クラス ID：10AHex） A-50
A-4-14　Logic Process オブジェクト（クラス ID：309Hex） A-55

A-5　適合宣言書 A-57

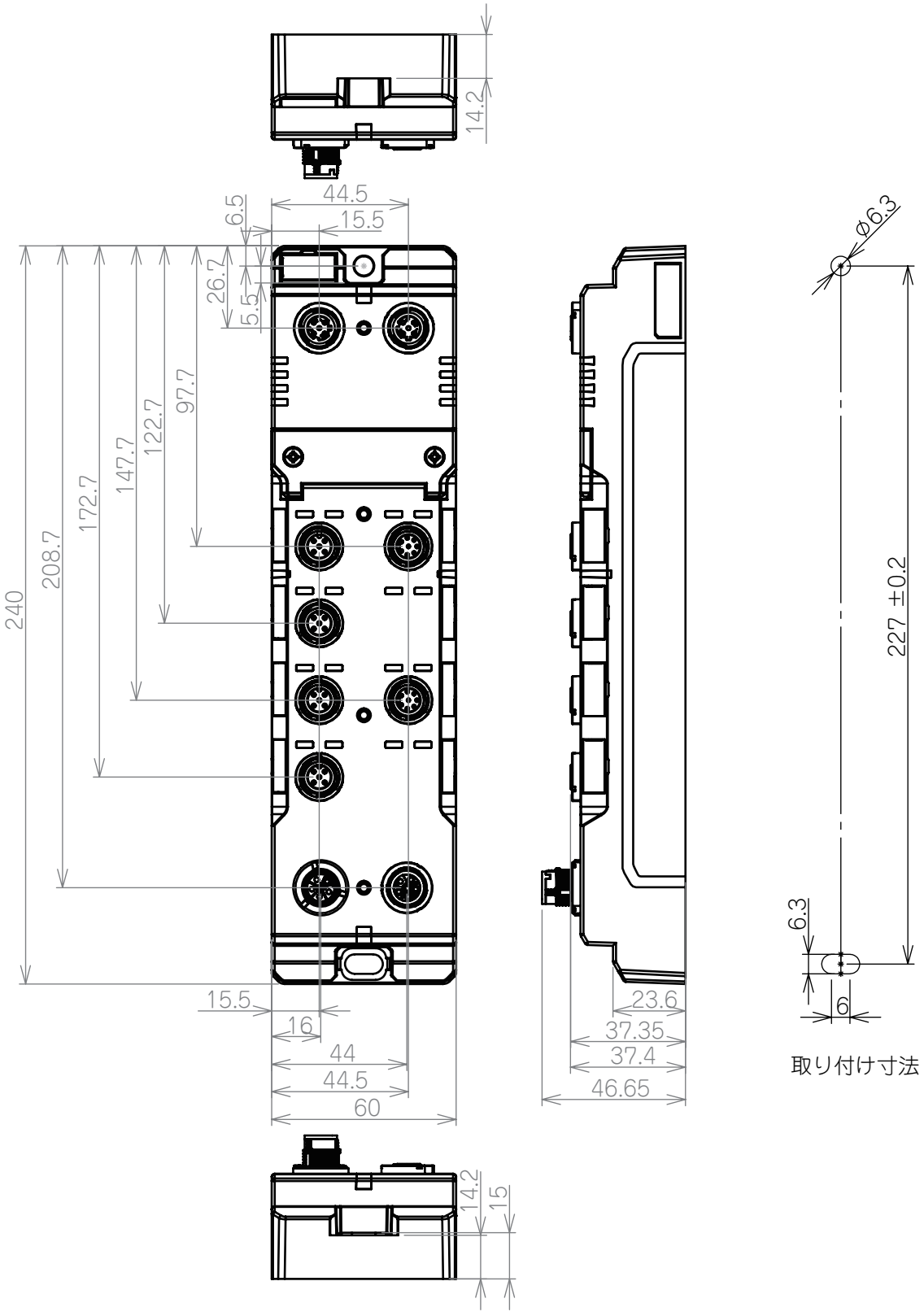
A-1 外形寸法

形 NXR-SXD1204-CST



取り付け寸法

形 NXR-SXD1204B-CST



取り付け寸法

A-2 セーフティ I/O アセンブリデータ

セーフティ I/O ターミナルの I/O アセンブリデータは、以下のとおりです。

A-2-1 セーフティ入力アセンブリデータ

セーフティ入力アセンブリデータを示します。
データ内の各要素の意味は、以下のとおりです。

要素	意味	属性
Safety Input N	セーフティ入力端子 Si N の値 0：セーフティ入力端子 OFF、または異常発生中 1：セーフティ入力端子 ON	安全
Safety Input N Status	セーフティ入力端子 Si N のステータス情報 0：異常発生中 1：正常（異常なし）	安全
Safety Input Status	セーフティ入力端子のステータス情報（集約） 0：いずれかのセーフティ入力端子に異常あり 1：すべてのセーフティ入力端子が正常	安全
Test Output N Monitor	テスト出力端子 T N の値 0：テスト出力端子 OFF、または異常発生中 1：テスト出力端子 ON	非安全
Test Output N Status	テスト出力端子 T N のステータス情報 0：異常発生中 1：正常（異常なし）	非安全
Safety Output N Monitor	セーフティ出力端子 So N に実際に出力されている値 0：セーフティ出力端子 OFF 1：セーフティ出力端子 ON	非安全
Safety Output N Status	セーフティ出力端子 So N のステータス情報 0：異常発生中 1：正常（異常なし）	安全
Safety Output Status	セーフティ出力端子のステータス情報（集約） 0：いずれかのセーフティ出力端子に異常あり 1：すべてのセーフティ出力端子が正常	安全
Output Power Supply Error Flag	出力用電源エラーフラグ 0：出力用電源が正常 1：出力用電源が異常、または電源 OFF	非安全
Application Number	安全アプリケーションの番号	非安全
Cnxn Status	コネクションのステータス情報 0：コネクションが確立していない 1：コネクションが確立している	非安全

Input Data (Assembly 604 - 25CHex), Size 2 bytes

byte	bit							
	7	6	5	4	3	2	1	0
0	Safety Input 7	Safety Input 6	Safety Input 5	Safety Input 4	Safety Input 3	Safety Input 2	Safety Input 1	Safety Input 0
1	Safety Input Status	Safety Output Status	Output Power Supply Error Flag	Cnxn Status	Safety Input 11	Safety Input 10	Safety Input 9	Safety Input 8

Input Data (Assembly 960 - 3C0Hex), Size 5 bytes

byte	bit							
	7	6	5	4	3	2	1	0
0	Safety Input 7	Safety Input 6	Safety Input 5	Safety Input 4	Safety Input 3	Safety Input 2	Safety Input 1	Safety Input 0
1	Safety Input 3 Status	Safety Input 2 Status	Safety Input 1 Status	Safety Input 0 Status	Safety Input 11	Safety Input 10	Safety Input 9	Safety Input 8
2	Safety Input 11 Status	Safety Input 10 Status	Safety Input 9 Status	Safety Input 8 Status	Safety Input 7 Status	Safety Input 6 Status	Safety Input 5 Status	Safety Input 4 Status
3	Safety Input Status	Safety Output Status	Output Power Supply Error Flag	Cnxn Status	予約	予約	予約	予約
4	Application Number							

Input Data (Assembly 961 - 3C1Hex), Size 9 bytes

byte	bit							
	7	6	5	4	3	2	1	0
0	Safety Input 7	Safety Input 6	Safety Input 5	Safety Input 4	Safety Input 3	Safety Input 2	Safety Input 1	Safety Input 0
1	Safety Input 3 Status	Safety Input 2 Status	Safety Input 1 Status	Safety Input 0 Status	Safety Input 11	Safety Input 10	Safety Input 9	Safety Input 8
2	Safety Input 11 Status	Safety Input 10 Status	Safety Input 9 Status	Safety Input 8 Status	Safety Input 7 Status	Safety Input 6 Status	Safety Input 5 Status	Safety Input 4 Status
3	Safety Output 3 Monitor	Safety Output 2 Monitor	Safety Output 1 Monitor	Safety Output 0 Monitor	Safety Output 3 Status	Safety Output 2 Status	Safety Output 1 Status	Safety Output 0 Status
4	Test Output 7 Status	Test Output 6 Status	Test Output 5 Status	Test Output 4 Status	Test Output 3 Status	Test Output 2 Status	Test Output 1 Status	Test Output 0 Status
5	Test Output 3 Monitor	Test Output 2 Monitor	Test Output 1 Monitor	Test Output 0 Monitor	Test Output 11 Status	Test Output 10 Status	Test Output 9 Status	Test Output 8 Status
6	Test Output 11 Monitor	Test Output 10 Monitor	Test Output 9 Monitor	Test Output 8 Monitor	Test Output 7 Monitor	Test Output 6 Monitor	Test Output 5 Monitor	Test Output 4 Monitor
7	Safety Input Status	Safety Output Status	Output Power Supply Error Flag	Cnxn Status	予約	予約	予約	予約
8	Application Number							

A-2-2 セーフティ出力アセンブリデータ

セーフティ出力アセンブリデータを示します。
データ内の各要素の意味は、以下のとおりです。

要素	意味	属性
Safety Output N	セーフティ出力端子 So N への ON/OFF 0 : セーフティ出力 OFF 1 : セーフティ出力 ON	安全
Standard Output N	テスト出力端子 T N へのスタンダード出力の ON/OFF 0 : スタンダード出力 OFF 1 : スタンダード出力 ON	非安全
Remote N Output M	リモート出力 Ro N - M の ON/OFF 0 : リモート出力 OFF 1 : リモート出力 ON	安全

Output Data (Assembly 563 - 233Hex), Size 1 byte

byte	bit							
	7	6	5	4	3	2	1	0
0	予約	予約	予約	予約	Safety Output 3	Safety Output 2	Safety Output 1	Safety Output 0

Output Data (Assembly 881 - 371Hex), Size 3 bytes

byte	bit							
	7	6	5	4	3	2	1	0
0	予約	予約	予約	予約	予約	予約	Remote1 Output 1	Remote1 Output 0
1	Standard Output 7	Standard Output 6	Standard Output 5	Standard Output 4	Standard Output 3	Standard Output 2	Standard Output 1	Standard Output 0
2	予約	予約	予約	予約	Standard Output 11	Standard Output 10	Standard Output 9	Standard Output 8

Output Data (Assembly 882 - 372Hex), Size 1 bytes

byte	bit							
	7	6	5	4	3	2	1	0
0	予約	予約	予約	予約	予約	予約	Remote2 Output 1	Remote2 Output 0

Output Data (Assembly 883 - 373Hex), Size 1 bytes

byte	bit							
	7	6	5	4	3	2	1	0
0	予約	予約	予約	予約	予約	予約	Remote3 Output 1	Remote3 Output 0

Output Data (Assembly 896 - 380Hex), Size 3 bytes

byte	bit							
	7	6	5	4	3	2	1	0
0	予約	予約	予約	予約	Safety Output 3	Safety Output 2	Safety Output 1	Safety Output 0
1	Standard Output 7	Standard Output 6	Standard Output 5	Standard Output 4	Standard Output 3	Standard Output 2	Standard Output 1	Standard Output 0
2	予約	予約	予約	予約	Standard Output 11	Standard Output 10	Standard Output 9	Standard Output 8

A-2-3 コンフィグレーションアセンブリデータ

コンフィグレーションアセンブリデータを示します。
データ内の各要素の意味は、以下のとおりです。

要素	意味
Power-on Mode	電源投入時モード 0 : 停止(Idle) 1 : 実行(Executing)
Test Output N Mode	テスト出力端子 T N の使用モード 0 : Not Used 1 : Standard Output 2 : Test Output 3 : Power Supply Output
Safety Output Error Latch Time	セーフティ出力端子の出力エラーラッチ時間
Safety Output N Channel Mode	セーフティ出力端子 So N の使用モード 0 : 使用しない 1 : テストパルスなしで使用 2 : テストパルスありで使用
Safety Output N/N+1 Dual Channel Mode	セーフティ出力端子 So N と So N+1 の使用モード 0 : シングルチャネル 1 : デュアルチャネル
Safety Input Error Latch Time	セーフティ入力端子の入力エラーラッチ時間
Safety Input N Off_On_Delay	セーフティ入力端子 Si N の OFF→ON 遅延時間
Safety Input N On_Off_Delay	セーフティ入力端子 Si N の ON→OFF 遅延時間
Safety Input N Channel Mode	セーフティ入力端子 Si N の使用モード 0 : 使用しない 1 : テスト出力端子とともに使用 2 : 半導体入力機器として、テストパルスなしで使用 3 : スタンダード入力として、テストパルスなしで使用
Safety Input N Test Source	セーフティ入力端子 Si N と接続して使用するテスト出力端子番号
Safety Input N/N+1 Dual Channel Mode	セーフティ入力端子 Si N と Si N+1 の使用モード 0 : シングルチャネル 1 : デュアルチャネル同値入力 2 : デュアルチャネル反転入力
Safety Input N/N+1 Discrepancy Time	デュアルチャネル監視時間
Output Logic N Off_On_Delay	セーフティ出力端子 So N の OFF→ON 遅延時間
Output Logic N On_Off_Delay	セーフティ出力端子 So N の ON→OFF 遅延時間
Output Logic N Output Condition	セーフティ出力端子 So N のロジックの出力値条件
Output Logic N EDM Feedback	セーフティ出力端子 So N に EDM フィードバック値を入力するのに使用するセーフティ入力端子番号
Input Logic N Input Condition1	セーフティ入力端子 Si N およびリモート出力のロジックの、入力条件演算の条件
Input Logic N Reset Condition	セーフティ入力端子 Si N およびリモート出力のロジックの、リセット演算の条件
Input Logic N Reset Minimum ON Pulse Width	セーフティ入力端子 Si N およびリモート出力に対するリセット信号の、最小 ON パルス幅

要素	意味
Input Logic N Reset Maximum ON Pulse Width	セーフティ入力端子 Si N およびリモート出力に対するリセット信号の、最大 ON パルス幅

Configuration (Assembly 864 - 360Hex), Size 340 bytes

データ	サイズ(byte)	オフセット(byte)
Power-on Mode	1	0
Padding	1	1
Test Output 0 Mode	1	2
Test Output 1 Mode	1	3
Test Output 2 Mode	1	4
Test Output 3 Mode	1	5
Test Output 4 Mode	1	6
Test Output 5 Mode	1	7
Test Output 6 Mode	1	8
Test Output 7 Mode	1	9
Test Output 8 Mode	1	10
Test Output 9 Mode	1	11
Test Output 10 Mode	1	12
Test Output 11 Mode	1	13
Safety Output Error Latch Time	2	14
Safety Output 0 Channel Mode	1	16
Safety Output 1 Channel Mode	1	17
Safety Output 2 Channel Mode	1	18
Safety Output 3 Channel Mode	1	19
Safety Out 0/1 Dual Channel Mode	1	20
Safety Out 2/3 Dual Channel Mode	1	21
Safety Input Error Latch Time	2	22
Safety Input 0 Off_On_Delay	2	24
Safety Input 0 On_Off_Delay	2	26
Safety Input 0 Channel Mode	1	28
Safety Input 0 Test Source	1	29
Safety Input 1 Off_On_Delay	2	30
Safety Input 1 On_Off_Delay	2	32
Safety Input 1 Channel Mode	1	34
Safety Input 1 Test Source	1	35
Safety Input 2 Off_On_Delay	2	36
Safety Input 2 On_Off_Delay	2	38
Safety Input 2 Channel Mode	1	40
Safety Input 2 Test Source	1	41
Safety Input 3 Off_On_Delay	2	42
Safety Input 3 On_Off_Delay	2	44
Safety Input 3 Channel Mode	1	46
Safety Input 3 Test Source	1	47
Safety Input 4 Off_On_Delay	2	48
Safety Input 4 On_Off_Delay	2	50
Safety Input 4 Channel Mode	1	52
Safety Input 4 Test Source	1	53
Safety Input 5 Off_On_Delay	2	54
Safety Input 5 On_Off_Delay	2	56

データ	サイズ(byte)	オフセット(byte)
Safety Input 5 Channel Mode	1	58
Safety Input 5 Test Source	1	59
Safety Input 6 Off_On_Delay	2	60
Safety Input 6 On_Off_Delay	2	62
Safety Input 6 Channel Mode	1	64
Safety Input 6 Test Source	1	65
Safety Input 7 Off_On_Delay	2	66
Safety Input 7 On_Off_Delay	2	68
Safety Input 7 Channel Mode	1	70
Safety Input 7 Test Source	1	71
Safety Input 8 Off_On_Delay	2	72
Safety Input 8 On_Off_Delay	2	74
Safety Input 8 Channel Mode	1	76
Safety Input 8 Test Source	1	77
Safety Input 9 Off_On_Delay	2	78
Safety Input 9 On_Off_Delay	2	80
Safety Input 9 Channel Mode	1	82
Safety Input 9 Test Source	1	83
Safety Input 10 Off_On_Delay	2	84
Safety Input 10 On_Off_Delay	2	86
Safety Input 10 Channel Mode	1	88
Safety Input 10 Test Source	1	89
Safety Input 11 Off_On_Delay	2	90
Safety Input 11 On_Off_Delay	2	92
Safety Input 11 Channel Mode	1	94
Safety Input 11 Test Source	1	95
Safety Input 0/1 Dual Channel Mode	1	96
padding	1	97
Safety Input 0/1 Discrepancy Time	2	98
Safety Input 2/3 Dual Channel Mode	1	100
padding	1	101
Safety Input 2/3 Discrepancy Time	2	102
Safety Input 4/5 Dual Channel Mode	1	104
padding	1	105
Safety Input 4/5 Discrepancy Time	2	106
Safety Input 6/7 Dual Channel Mode	1	108
padding	1	109
Safety Input 6/7 Discrepancy Time	2	110
Safety Input 8/9 Dual Channel Mode	1	112
padding	1	113
Safety Input 8/9 Discrepancy Time	2	114
Safety Input 10/11 Dual Channel Mode	1	116
padding	1	117
Safety Input 10/11 Discrepancy Time	2	118
Output Logic 0 Off_On_Delay	2	120
Output Logic 0 On_Off_Delay	2	122
Output Logic 0 Output Condition	4	124
Output Logic 0 EDM Feedback	1	128
Padding	1	129
Output Logic 1 Off_On_Delay	2	130
Output Logic 1 On_Off_Delay	2	132

データ	サイズ(byte)	オフセット(byte)
Output Logic 1 Output Condition	4	134
Output Logic 1 EDM Feedback	1	138
Padding	1	139
Output Logic 2 Off_On_Delay	2	140
Output Logic 2 On_Off_Delay	2	142
Output Logic 2 Output Condition	4	144
Output Logic 2 EDM Feedback	1	148
Padding	1	149
Output Logic 3 Off_On_Delay	2	150
Output Logic 3 On_Off_Delay	2	152
Output Logic 3 Output Condition	4	154
Output Logic 3 EDM Feedback	1	158
Padding	1	159
Input Logic 0 Input Condition	4	160
Input Logic 0 Reset Condition	1	164
Padding	1	165
Input Logic 0 Reset Minimum ON Pulse Width	2	166
Input Logic 0 Reset Maximum ON Pulse Width	2	168
Input Logic 1 Input Condition	4	170
Input Logic 1 Reset Condition	1	174
Padding	1	175
Input Logic 1 Reset Minimum ON Pulse Width	2	176
Input Logic 1 Reset Maximum ON Pulse Width	2	178
Input Logic 2 Input Condition	4	180
Input Logic 2 Reset Condition	1	184
Padding	1	185
Input Logic 2 Reset Minimum ON Pulse Width	2	186
Input Logic 2 Reset Maximum ON Pulse Width	2	188
Input Logic 3 Input Condition	4	190
Input Logic 3 Reset Condition	1	194
Padding	1	195
Input Logic 3 Reset Minimum ON Pulse Width	2	196
Input Logic 3 Reset Maximum ON Pulse Width	2	198
Input Logic 4 Input Condition	4	200
Input Logic 4 Reset Condition	1	204
Padding	1	205
Input Logic 4 Reset Minimum ON Pulse Width	2	206
Input Logic 4 Reset Maximum ON Pulse Width	2	208
Input Logic 5 Input Condition	4	210
Input Logic 5 Reset Condition	1	214
Padding	1	215
Input Logic 5 Reset Minimum ON Pulse Width	2	216

データ	サイズ(byte)	オフセット(byte)
Input Logic 5 Reset Maximum ON Pulse Width	2	218
Input Logic 6 Input Condition	4	220
Input Logic 6 Reset Condition	1	224
Padding	1	225
Input Logic 6 Reset Minimum ON Pulse Width	2	226
Input Logic 6 Reset Maximum ON Pulse Width	2	228
Input Logic 7 Input Condition	4	230
Input Logic 7 Reset Condition	1	234
Padding	1	235
Input Logic 7 Reset Minimum ON Pulse Width	2	236
Input Logic 7 Reset Maximum ON Pulse Width	2	238
Input Logic 8 Input Condition	4	240
Input Logic 8 Reset Condition	1	244
Padding	1	245
Input Logic 8 Reset Minimum ON Pulse Width	2	246
Input Logic 8 Reset Maximum ON Pulse Width	2	248
Input Logic 9 Input Condition	4	250
Input Logic 9 Reset Condition	1	254
Padding	1	255
Input Logic 9 Reset Minimum ON Pulse Width	2	256
Input Logic 9 Reset Maximum ON Pulse Width	2	258
Input Logic 10 Input Condition	4	260
Input Logic 10 Reset Condition	1	264
Padding	1	265
Input Logic 10 Reset Minimum ON Pulse Width	2	266
Input Logic 10 Reset Maximum ON Pulse Width	2	268
Input Logic 11 Input Condition	4	270
Input Logic 11 Reset Condition	1	274
Padding	1	275
Input Logic 11 Reset Minimum ON Pulse Width	2	276
Input Logic 11 Reset Maximum ON Pulse Width	2	278
Input Logic 12 Input Condition	4	280
Input Logic 12 Reset Condition	1	284
Padding	1	285
Input Logic 12 Reset Minimum ON Pulse Width	2	286
Input Logic 12 Reset Maximum ON Pulse Width	2	288
Input Logic 13 Input Condition	4	290
Input Logic 13 Reset Condition	1	294

データ	サイズ(byte)	オフセット(byte)
Padding	1	295
Input Logic 13 Reset Minimum ON Pulse Width	2	296
Input Logic 13 Reset Maximum ON Pulse Width	2	298
Input Logic 14 Input Condition	4	300
Input Logic 14 Reset Condition	1	304
Padding	1	305
Input Logic 14 Reset Minimum ON Pulse Width	2	306
Input Logic 14 Reset Maximum ON Pulse Width	2	308
Input Logic 15 Input Condition	4	310
Input Logic 15 Reset Condition	1	314
Padding	1	315
Input Logic 15 Reset Minimum ON Pulse Width	2	316
Input Logic 15 Reset Maximum ON Pulse Width	2	318
Input Logic 16 Input Condition	4	320
Input Logic 16 Reset Condition	1	324
Padding	1	325
Input Logic 16 Reset Minimum ON Pulse Width	2	326
Input Logic 16 Reset Maximum ON Pulse Width	2	328
Input Logic 17 Input Condition	4	330
Input Logic 17 Reset Condition	1	334
Padding	1	335
Input Logic 17 Reset Minimum ON Pulse Width	2	336
Input Logic 17 Reset Maximum ON Pulse Width	2	338

A-3 I/O アセンブリのポートと対応するセーフティ I/O アセンブリデータの要素

以下にセーフティ I/O ターミナルの I/O アセンブリ、I/O アセンブリを I/O マップに展開した際のポート名を示します。
各ポートは、セーフティ I/O アセンブリデータの要素と 1 対 1 に対応しています。
セーフティ I/O アセンブリデータの要素の意味は、「A-2 セーフティ I/O アセンブリデータ (P.A-4)」を参照してください。

I/O アセンブリ	ポート	データ型	R/W	サイズ (bit)	対応するセーフティ I/O アセンブリデータの要素
Safety Input 1	Safety Input 0-11 Logical Value	SAFEBOOL	R	12	Safety Input N
	Safety Cnxn Status	SAFEBOOL	R	1	Cnxn Status
	Output Power Status	SAFEBOOL	R	1	Output Power Supply Error Flag
	Combined Safety Output Status	SAFEBOOL	R	1	Safety Output Status
	Combined Safety Input Status	SAFEBOOL	R	1	Safety Input Status
Safety Input 2	Safety Input 0-11 Logical Value	SAFEBOOL	R	12	Safety Input N
	Safety Input 0-11 Status	SAFEBOOL	R	12	Safety Input N Status
	Safety Cnxn status	SAFEBOOL	R	1	Cnxn Status
	Output Power Status	SAFEBOOL	R	1	Output Power Supply Error Flag
	Combined Safety Output Status	SAFEBOOL	R	1	Safety Output Status
	Combined Safety Input Status	SAFEBOOL	R	1	Safety Input Status
	Application Number	SAFEINT	R	8	Application Number
Safety Input 3	Safety Input 0-11 Logical Value	SAFEBOOL	R	12	Safety Input N
	Safety Input 0-11 Status	SAFEBOOL	R	12	Safety Input N Status
	Safety Output 0-3 Status	SAFEBOOL	R	4	Safety Output N Status
	Safety Output 0-3 Monitor Value	SAFEBOOL	R	4	Safety Output N Monitor
	Test Output 0-11 Status	SAFEBOOL	R	12	Test Output N Status
	Test Output 0-11 Value	SAFEBOOL	R	12	Test Output N Monitor
	Safety Cnxn status	SAFEBOOL	R	1	Cnxn Status
	Output Power Status	SAFEBOOL	R	1	Output Power Supply Error Flag
	Combined Safety Output Status	SAFEBOOL	R	1	Safety Output Status
	Combined Safety Input Status	SAFEBOOL	R	1	Safety Input Status
	Application Number	SAFEINT	R	8	Application Number
Safety Output	Safety Output 0-3 Value	SAFEBOOL	W	4	Safety Output N
Safety Remote Output 1 + Standard Output	Remote 1 Output 0-1	SAFEBOOL	W	2	Remote N Output M
	Test Output 0-11 Value	SAFEBOOL	W	12	Standard Output N
Safety Remote Output 2	Remote 2 Output 0-1	SAFEBOOL	W	2	Remote N Output M

I/O アセンブリ	ポート	データ型	R/W	サイズ (bit)	対応するセーフティ I/O アセンブリデータの要素
Safety Remote Output 3	Remote 3 Output 0-1	SAFEBOOL	W	2	Remote N Output M
Safety Output + Standard Output	Safety Output 0-3 Value	SAFEBOOL	W	4	Safety Output N
	Test Output 0-11 Value	SAFEBOOL	W	12	Standard Output N

A-4 サポートする CIP オブジェクト

サポートする CIP オブジェクトを以下に記載します。
セーフティ I/O ターミナルの CIP オブジェクトへは、Explicit メッセージでアクセスします。CIP オブジェクトへの Explicit メッセージによるアクセス方法については、「Explicit メッセージサーバ機能 (P.6-6)」を参照してください。

オブジェクト名称	機能	参照先
Identity オブジェクト	セーフティ I/O ターミナルの製品情報を読み出す。	「A-4-1 Identity オブジェクト（クラス ID：01Hex）(P.A-16)」
Assembly オブジェクト	セーフティ I/O ターミナルに接続している外部接続機器の入出力データを結合する。	「A-4-2 Assembly オブジェクト（クラス ID：04Hex）(P.A-18)」
Unit Manager オブジェクト	セーフティ I/O ターミナルのユニット情報を集約する。	「A-4-3 Unit Manager オブジェクト（クラス ID：380Hex）(P.A-21)」
Event History Log オブジェクト	イベントログを管理する。	「A-4-4 Event History Log オブジェクト（クラス ID：34BHex）(P.A-25)」
Error Event オブジェクト	発生中異常のイベントを管理する	「A-4-5 Error Event オブジェクト（クラス ID：34CHex）(P.A-28)」
Safety Discrete Input Point (SDIP)オブジェクト	セーフティ入力端子を 1 端子ごとに管理する。	「A-4-6 Safety Discrete Input Point (SDIP) オブジェクト（クラス ID：3DHex）(P.A-31)」
Safety Discrete Output Point (SDOP)オブジェクト	セーフティ出力端子を 1 端子ごとに管理する。	「A-4-7 Safety Discrete Ouput Point (SDOP)オブジェクト（クラス ID：3BHex）(P.A-33)」
Device Level Ring (DLR)オブジェクト	DLR ネットワークの状態を示す。	「A-4-8 Device Level Ring (DLR)オブジェクト（クラス ID：47Hex）(P.A-35)」
QoS オブジェクト	Ethernet フレーム優先制御の IPv4 DiffServ Code Point （DSCP）の値を設定する。	「A-4-9 QoS オブジェクト（クラス ID：48Hex）(P.A-37)」
TCP/IP Interface オブジェクト	TCP/IP インタフェースの設定を行う。	「A-4-10 TCP/IP Interface オブジェクト（クラス ID：F5Hex）(P.A-39)」
Ethernet Link オブジェクト	Ethernet Link の各種情報を取得する。	「A-4-11 Ethernet Link オブジェクト(クラス ID：F6Hex）(P.A-43)」
LLDP Management オブジェクト	LLDP 機能を管理する。	「A-4-12 LLDP Management オブジェクト（クラス ID：109Hex）(P.A-48)」
LLDP Data Table オブジェクト	LLDP 機能のデータを管理する。	「A-4-13 LLDP Data Table オブジェクト(クラス ID：10AHex）(P.A-50)」
Logic Process オブジェクト	動作しているアプリケーションの番号を読み出す。	「A-4-14 Logic Process オブジェクト（クラス ID：309Hex）(P.A-55)」

使用上の注意

CIP オブジェクトのパラメータのデータ型が、INT、UINT、UDINT、ULINT、WORD、DWORD のいずれかの場合、書き込みデータはリトルエンディアンで格納してください。また、読み出しデータもリトルエンディアンで格納されます。
ただし、本マニュアルでの表記は、高位桁が左、低位桁が右という一般的な 16 進数の書き方を採用しています。

A-4-1 Identity オブジェクト（クラス ID：01Hex）

Identity オブジェクトは、セーフティ I/O ターミナルの製品情報の読み出しのためのオブジェクトです。

クラス ID、インスタンス ID

クラス ID とインスタンス ID は、以下のとおりです。

ID の種類	値(Hex)	内容
クラス ID	01	−
インスタンス ID	00	クラス自体を指定する。
	01	インスタンスを指定する。

アトリビュート ID

読み出す情報を指定します。

● クラス用アトリビュート ID

オブジェクト全体のアトリビュートを指定します。

アトリビュート ID	パラメータ名	内容	属性	データ	
				データ型	値(Hex)
1	Revision	オブジェクトのレビジョン	読出	UINT	0002

● インスタンス用アトリビュート ID

インスタンスごとのアトリビュート ID を指定します。

アトリビュート ID	パラメータ名		内容	属性	データ	
					データ型	値
1	Vendor ID		ベンダ ID	読出	UINT	002FHex
2	Device Type		デバイスタイプ	読出	UINT	0308Hex (Safety IO and Logic Device)
3	Product Code		製品コード	読出	UINT	形 NXR-SXD1204-CST : 0BF9Hex 形 NXR-SXD1204B-CST : 0BFAHex
4	Revision		機器の CIP リビジョン	読出	STRUCT	—
		Major Revision	メジャー・リビジョン		USINT	01Hex
		Minor Revision	マイナー・リビジョン		USINT	01Hex
5	Status		セーフティ I/O ターミナルのステータス	読出	WORD	下記「Status の値 (P.A-17)」を参照
6	Serial Number		シリアル番号	読出	UDINT	製品の個体ごとの固有の番号
7	Product Name		製品名	読出	SHORT STRING	下記「Product Name の値 (P.A-17)」を参照

● Status の値

ビット	名称	内容
0	Owned	セーフティ I/O ターミナルがターゲットとして、コネクションを開設していることを示す。 • TRUE: 開設している。 • FALSE: 開設していない。
1	予約	常に FALSE
2	Configured	セーフティ I/O ターミナルが、コンフィグレーションされていることを示す。 • TRUE: コンフィグレーションされている。 • FALSE: コンフィグレーションされていない。
3	予約	常に FALSE
4～7	Extended Device Status	*1
8	予約	常に FALSE
9	予約	常に FALSE
10	Major Recoverable Fault	• TRUE: MS LED が赤色に点滅する異常が発生している。 • FALSE: MS LED が赤色に点滅する異常が発生していない。
11	Major Unrecoverable Fault	• TRUE: MS LED が赤色に点灯する異常が発生している。 • FALSE: MS LED が赤色に点灯する異常が発生していない。
12～15	予約	常に FALSE

***1.** Extended Status の値の意味は、以下のとおりです。
- 0-1 : 予約
- 2 : Class1 通信（タグデータリンク）のコネクションで、ひとつ以上のタイムアウトが発生している。
- 3 : Class1 通信（タグデータリンク）のコネクションが確立していない。
- 4-5 : 予約
- 6 : ひとつ以上の Class1 通信（タグデータリンク）のコネクションが、運転モードで正常に通信を行っている。
- 7 : ひとつ以上の Class1 通信（タグデータリンク）のコネクションが確立していて、そのすべてが Idle mode である。
- 8-15 : 予約

● Product Name の値

形式	値(Hex)
形 NXR-SXD1204-CST	0F 4E 58 52 2D 53 58 44 31 32 30 34 2D 43 53 54
形 NXR-SXD1204B-CST	10 4E 58 52 2D 53 58 44 31 32 30 34 42 2D 43 53 54

サービスコード

実行させるサービスを、サービスコードで指定します。

サービスコード(Hex)	パラメータ名	内容	サポートするサービス範囲	
			クラス単位	インスタンス単位
01	Get_Attribute_All	すべてのアトリビュートの値を読み出す。	不可	可
0E	Get_Attribute_Single	指定したアトリビュートの値を読み出す。	可	可

A-4-2 Assembly オブジェクト（クラス ID：04Hex）

Assembly オブジェクトは、セーフティ I/O ターミナルに接続している外部接続機器機器の入出力データを結合するオブジェクトです。

クラス ID、インスタンス ID

クラス ID とインスタンス ID は、以下のとおりです。

ID の種類	値(Hex)	内容
クラス ID	04	—
インスタンス ID	00	クラス自体を指定する。
	25C、3C0、3C1	セーフティ入力アセンブリデータ
	233、371、372、373、380	セーフティ出力アセンブリデータ
	360	コンフィグレーションアセンブリデータ

アトリビュート ID

読み出す情報を指定します。

● クラス用アトリビュート ID

オブジェクト全体のアトリビュートを指定します。

アトリビュート ID	パラメータ名	内容	属性	データ	
				データ型	値(Hex)
1	Revision	オブジェクトのレビジョン	読出	UINT	0003

● インスタンス用アトリビュート ID

インスタンスごとのアトリビュート ID を指定します。
割り当てられているインスタンスが Standard Output だけの場合は書き込み可能です。

インスタンス ID が 25CHex のアトリビュート ID

アトリビュート ID	パラメータ名	内容	属性	データ	
				データ型	値
03	Data	入出力データ	読出	ARRAY OF BYTE	「Input Data (Assembly 604 - 25CHex), Size 2 bytes (P.A-4)」参照

インスタンス ID が 3C0Hex のアトリビュート ID

アトリビュート ID	パラメータ名	内容	属性	データ	
				データ型	値
03	Data	入出力データ	読出	ARRAY OF BYTE	「Input Data (Assembly 960 - 3C0Hex), Size 5 bytes (P.A-5)」参照

インスタンス ID が 3C1Hex のアトリビュート ID

アトリビュート ID	パラメータ名	内容	属性	データ	
				データ型	値
03	Data	入出力データ	読出	ARRAY OF BYTE	「Input Data (Assembly 961 - 3C1Hex), Size 9 bytes (P.A-5)」参照

インスタンス ID が 233Hex のアトリビュート ID

アトリビュート ID	パラメータ名	内容	属性	データ	
				データ型	値
03	Data	入出力データ	読出	ARRAY OF BYTE	「Output Data (Assembly 563 - 233Hex), Size 1 byte (P.A-6)」参照

インスタンス ID が 371Hex のアトリビュート ID

アトリビュート ID	パラメータ名	内容	属性	データ	
				データ型	値
03	Data	入出力データ	読出	ARRAY OF BYTE	「Output Data (Assembly 881 - 371Hex), Size 3 bytes (P.A-6)」参照

インスタンス ID が 372Hex のアトリビュート ID

アトリビュート ID	パラメータ名	内容	属性	データ	
				データ型	値
03	Data	入出力データ	読出	ARRAY OF BYTE	「Output Data (Assembly 882 - 372Hex), Size 1 bytes (P.A-6)」参照

インスタンス ID が 373Hex のアトリビュート ID

アトリビュート ID	パラメータ名	内容	属性	データ	
				データ型	値
03	Data	入出力データ	読出	ARRAY OF BYTE	「Output Data (Assembly 883 - 373Hex), Size 1 bytes (P.A-6)」参照

インスタンス ID が 380Hex のアトリビュート ID

アトリビュート ID	パラメータ名	内容	属性	データ	
				データ型	値
03	Data	入出力データ	読出	ARRAY OF BYTE	「Output Data (Assembly 896 - 380Hex), Size 3 bytes (P.A-6)」参照

インスタンス ID が 360Hex のアトリビュート ID

アトリビュート ID	パラメータ名	内容	属性	データ	
				データ型	値
03	Data	入出力データ	読出	ARRAY OF BYTE	「Configuration (Assembly 864 - 360Hex), Size 340 bytes (P.A-8)」

サービスコード

実行させるサービスを、サービスコードで指定します。

サービスコード(Hex)	パラメータ名	内容	サポートするサービス範囲	
			クラス単位	インスタンス単位
0E	Get_Attribute_Single	指定したアトリビュートの値を読み出す。	可	可

A-4-3 Unit Manager オブジェクト（クラス ID：380Hex）

Unit Manager オブジェクトは、セーフティ I/O ターミナルのユニット情報を集約したオブジェクトです。

クラス ID、インスタンス ID

クラス ID とインスタンス ID は、以下のとおりです。

ID の種類	値(Hex)	内容
クラス ID	380	
インスタンス ID	00	クラス自体を指定する。
	01	インスタンスを指定する。

アトリビュート ID

読み出す情報を指定します。

● クラス用アトリビュート ID

オブジェクト全体のアトリビュートを指定します。

アトリビュート ID	パラメータ名	内容	属性	データ	
				データ型	値(Hex)
1	Revision	オブジェクトのレビジョン	読出	UINT	0001

● インスタンス用アトリビュート ID

インスタンスごとのアトリビュート ID を指定します。

アトリビュート ID	パラメータ名	内容	属性	データ	
				データ型	値
1	Unit Version	ユニットバージョン	読出	DWORD	下記「Unit Version、Hardware Version の値 (P.A-23)」を参照
2	Hardware Version	ハードウェアバージョン	読出	DWORD	下記「Unit Version、Hardware Version の値 (P.A-23)」を参照
3	Firmware Version	ファームウェアバージョン	読出	DWORD	下記「Firmware Version の値 (P.A-23)」を参照
5	Unit/Input Power Voltage	ユニット/入力用電源電圧	読出	UINT	ユニット／入力電源電圧の現在値 *1 値は 100mV 単位 たとえば 24.1V なら値は 241 になる。
6	Max Unit/Input Power Voltage	ユニット/入力用電源電圧最大値	読出	UINT	ユニット／入力電源電圧の最大値 *1 値は 100mV 単位
7	Min Unit/Input Power Voltage	ユニット/入力用電源電圧最小値	読出	UINT	ユニット／入力電源電圧の最小値 *1 値は 100mV 単位
8	Output Power Voltage	出力用電源電圧	読出	UINT	出力電源電圧の現在値 *1 値は 100mV 単位

アトリビュート ID	パラメータ名	内容	属性	データ	
				データ型	値
9	Max Output Power Voltage	出力用電源電圧最大値	読出	UINT	出力電源電圧の最大値 *1 値は 100mV 単位
10	Min Output Power Supply Voltage	出力用電源電圧最小値	読出	UINT	出力電源電圧の最小値 *1 値は 100mV 単位
11	Operate Hours	ユニットの総稼働時間	読出	UDINT	ユニットの総稼働時間 (単位：h)
12	SNTP server IP address	SNTP サーバの IP アドレス	読書	UDINT	“0”：時計情報自動調整機能無効 “0”以外: SNTP サーバの IP アドレス 設定は、ユニットリスタート後に有効。 以下の値は設定不可。 • 0、127 または 255 で始まる IP アドレス • クラス D の IP アドレス (224.0.0.0-239.255.255.255) • クラス E の IP アドレス (240.0.0.0-255.255.255.255) • リンクローカルアドレス (169.254.0.0-169.254.255.255)
20	Unit/Input Power Current	ユニット/入力用電源電流	読出	UINT	ユニット／入力電源電流の現在値 *1 値は 100mA 単位 たとえば 5.1A なら値は 51 になる。
21	Max Unit/Input Power Current	ユニット/入力用電源電流最大値	読出	UINT	ユニット／入力電源電流の最大値 *1 値は 100mA 単位
22	Min Unit/Input Power Current	ユニット/入力用電源電流最小値	読出	UINT	ユニット／入力電源電流の最小値 *1 値は 100mA 単位
23	Output Power Current	出力用電源電流	読出	UINT	出力電源電流の現在値 *1 値は 100mA 単位
24	Max Output Power Current	出力用電源電流最大値	読出	UINT	出力電源電流の最大値 *1 値は 100mA 単位
25	Min Output Power Current	出力用電源電流最小値	読出	UINT	出力電源電流の最小値 *1 値は 100mA 単位
26	Unit/Input Power Supply Error Flag	ユニット／入力用電源エラーフラグ	読出	BOOL	TRUE : 電圧値が正常範囲外 FALSE : 電圧値が正常範囲内
27	Output Power Supply Error Flag	出力用電源エラーフラグ	読出	BOOL	TRUE : 電圧値が正常範囲外 FALSE : 電圧値が正常範囲内
28	Cross-Wiring Output Power Shut-off Control	渡り配線出力用電源の供給	読書	BOOL	TRUE : 渡り配線出力用電源を供給する（デフォルト値）。 FALSE : 渡り配線出力用電源を供給しない。 ただし、Cross-Wiring Output Shut-off Enable の値が TRUE の場合だけ有効。

アトリビュートID	パラメータ名	内容	属性	データ	
				データ型	値
29	Cross-Wiring Output Power Shut-off Enable	渡り配線出力用電源遮断機能有効／無効切り替え	読書	BOOL	TRUE：渡り配線出力用電源遮断機能を使用する（デフォルト値）。 FALSE：渡り配線出力用電源遮断機能を使用しない。 設定は、即時反映。
30	Communication Port Enable	通信有効／無効設定	読書	USINT	0：ポート 1、2 ともに有効（デフォルト値） 1：ポート 1 が有効、ポート 2 が無効 2：ポート 1 が無効、ポート 2 が有効 この設定は、リスタート後に有効になる。
100	Time	現在時刻	読出	DATE_AND_TIME	タイムゾーンに応じたローカルタイム。 時計情報自動調整機能(SNTP)により時間情報を取得する場合、SNTP によって補正された時刻になる。 SNTP を使用しない場合、1972 年 1 月 1 日 0 時 0 分 0 秒から計時した時刻になる。 デフォルト値は、 DT#1972-01-01-00:00:00.000
102	Time Zone Offset - Minutes	協定世界時(UTC)に対する Time の分単位のずれ	読書	INT	-720～840 協定世界時(UTC)と Time との分単位のずれを示す。たとえば UTC が 0 時で Time が 2 時 30 分の場合、Time Zone Offset - Minutes の値が 150 になる。 デフォルト値は 0 設定は、ユニットリスタート後に有効。
104	Firmware Hash Value	ファームウェアのハッシュ値	読出	ARRAY OF USINT	ファームウェアのハッシュ値 32 バイト

***1.** ユニットリスタートを実行すると、リセットされます。

● Unit Version、Hardware Version の値

ビット	名称	内容
0-15	予約	常に FALSE
16-23	マイナーバージョン番号フィールド	マイナーバージョンを BCD で表現する。 0～99
24-31	メジャーバージョン番号フィールド	メジャーバージョンを BCD で表現する。 0～9

たとえば、ユニットバージョンが 1.01 の場合、Unit Version の値は 01010000Hex となります。ユニットバージョンが 7.12 の場合は、Unit Version の値が 07120000Hex となります。

● Firmware Version の値

ビット	名称	内容
0-7	予約	常に FALSE
8-15	リビジョン番号フィールド	リビジョン番号を BCD で表現する。 0～99
16-23	マイナーバージョン番号フィールド	マイナーバージョンを BCD で表現する。 0～99
24-31	メジャーバージョン番号フィールド	メジャーバージョンを BCD で表現する。 0～9

たとえば、ファームウェアバージョンが 1.01.02 の場合、Firmware Version の値は 01010200Hex となります。ファームウェアバージョンが 7.00.10 の場合は、Firmware Version の値が 07001000Hex となります。

サービスコード

実行させるサービスを、サービスコードで指定します。

サービスコード (Hex)	パラメータ名	内容	サポートするサービス範囲	
			クラス単位	インスタンス単位
0E	Get_Attribute_Single	指定したアトリビュートの値を読み出す。	可	可
10	Set_Attribute_Single	指定したアトリビュートの値を書き込む。	不可	可
4B	Execute_WhereAmI	ユニット特定機能を実行する。	不可	可

Execute_WhereAmI（サービスコード: 4BHex）

ユニット特定機能を実行します。リクエストフォーマットは以下のとおりです。

● リクエストフォーマット

パラメータ名	内容	データ型	値
Service	サービスコード	USINT	4BHex
Request Path Size	リクエストパスのサイズ	USINT	03
Request Path	リクエストパス	Padded EPATH	210080032401Hex
Blink Duration	ユニット特定機能実行時間	UINT	0：ユニット特定機能を停止する。 5～1800：ユニット特定機能を指定した時間だけ実行する。単位は秒。 ユニット特定表示 LED が、Blink Duration で指定された期間、以下のように点灯または消灯を繰り返す。 • 時計回りに 100ms ずつ点灯することを、4 回繰り返す。 • 500ms の間、すべて消灯する。

A-4-4 Event History Log オブジェクト（クラス ID：34BHex）

Event History Log オブジェクトは、イベントログを管理するオブジェクトです。

クラス ID、インスタンス ID

クラス ID とインスタンス ID は、以下のとおりです。

ID の種類	値(Hex)	内容
クラス ID	34B	
インスタンス ID	01-02	インスタンスを指定する。 01：システムイベントログ（全 MPU 共通） 02：アクセスイベントログ（全 MPU 共通）

アトリビュート ID

読み出す情報を指定します。

● クラス用アトリビュート ID

オブジェクト全体のアトリビュートを指定します。

アトリビュート ID	パラメータ名	内容	属性	データ	
				データ型	値(Hex)
1	Revision	オブジェクトのレビジョン	読出	UINT	0001
2	Max Instance	最大のインスタンス番号	読出	UINT	0005
3	Number of Instance	インスタンスの数	読出	UINT	0005

● インスタンス用アトリビュート ID

インスタンスごとのアトリビュート ID を指定します。

アトリビュート ID	パラメータ名	内容	属性	データ	
				データ型	値
1	Max Number of Record	登録可能なレコード数	読出	UINT	インスタンス ID の値によって、以下のように異なる。 01Hex：100 件 02Hex：100 件
2	Number of Record	登録されているレコード数	読出	UINT	0～Max Number of Record
3	Undate Counter	カウンタ	読出	UINT	1～65535
4	Size of Record	読み出すレコードのバイトサイズ	読出	UINT	40

サービスコード

実行させるサービスを、サービスコードで指定します。

サービスコード (Hex)	パラメータ名	内容	サポートするサービス範囲	
			クラス単位	インスタンス単位
01	Get_Attribute_All	すべてのアトリビュートの値を読み出す。	可	可
0E	Get_Attribute_Single	指定したアトリビュートの値を読み出す。	可	可
34	Get Event Log	指定したイベントログの内容を読み出す。	不可	可

Get_Event_Log（サービスコード: 34Hex）

指定したイベントログの内容を読み出します。リクエストフォーマット、およびレスポンスフォーマットは以下のとおりです。

● リクエストフォーマット

パラメータ名	内容	データ型	値
Service	サービスコード	USINT	34Hex
Request Path Size	リクエストパスのサイズ	USINT	03
Request Path	リクエストパス	Padded EPATH	21004B032401 ～ 21004B032402Hex
Start Number of Read	読み出しを開始するレコード番号 先頭は 0	UINT	
Number of Read	読み出すレコード数*1	UINT	
Update Counter	事前に読み出したインスタンス用アトリビュート ID　3「Update Counter」の値*2 0：レコードの更新検知無効 0 以外：レコードの更新検知有効	UINT	

***1.** 指定した数のレコードが存在しない場合は、実際に読み出したレコード数がレスポンスの「Actual Number of Read」に格納されます。

***2.** 現在の「Update Counter」の値と異なる場合は、「Object state conflict」(0CHex)を返します。

● レスポンスフォーマット

パラメータ名	内容	データ型	値
Reply Service	Get Event Log サービスの応答	USINT	B4Hex
予約	予約	octet	00
General Status	正常を示すコード	USINT	00
Size of Additional Status	Additional ステータスのサイズ	USINT	00
Start Number of Read	実際に読み出した先頭レコード番号	UINT	
Actual Number of Read	実際に読み出したレコード数	UINT	
Update Counter	カウンタ	UINT	
Number of Record	登録されているレコード数	UINT	
Record	イベントログレコード	ARRAY OF STRUCT OF*1	

パラメータ名		内容	データ型	値
	Index	レコードのインデックス*2	UDINT	0～4294967295 1 件ずつインクリメントされ、最大値に達すると 0 に戻る。
	Time	イベントの発生時刻	DATE_AND_TIME	
	Product Code	プロダクトコード	DWORD	
	Event Code	イベントコード*3	DWORD	
	Event Priority	イベント重要度	WORD	3：軽度フォールト 4：監視情報 5：一般情報
	Additional Info Data Type1	イベントの付属情報 1 のデータ型	BYTE	
	Additional Info Data Type2	イベントの付属情報 2 のデータ型	BYTE	
	Additional Info Data Type3	イベントの付属情報 3 のデータ型	BYTE	
	Additional Info Data Type4	イベントの付属情報 4 のデータ型	BYTE	
	Additional Info1	イベントの付属情報 1*3	Additional Info Data Type1 で指定されたデータ型(4 octets)	
	Additional Info2	イベントの付属情報 2*3	Additional Info Data Type2 で指定されたデータ型(4 octets)	
	Additional Info3	イベントの付属情報 3*3	Additional Info Data Type3 で指定されたデータ型(4 octets)	
	Additional Info4	イベントの付属情報 4*3	Additional Info Data Type4 で指定されたデータ型(4 octets)	

***1.** 構造体のサイズは 40 バイトです。
***2.** インスタンス ID = 01Hex（システムイベントログ）とインスタンス ID = 02Hex（アクセスイベントログ）を通して採番されます。
***3.** 内容の詳細は、「11-2-4 イベントの内容と対処方法 (P.11-12)」を参照してください。

A-4-5 Error Event オブジェクト（クラス ID：34CHex）

Error Event オブジェクトは、発生中異常のイベントを管理するオブジェクトです。

クラス ID、インスタンス ID

クラス ID とインスタンス ID は、以下のとおりです。

ID の種類	値(Hex)	内容
クラス ID	34C	
インスタンス ID	00	クラス自体を指定する。
	01	インスタンスを指定する。

アトリビュート ID

読み出す情報を指定します。

● クラス用アトリビュート ID

オブジェクト全体のアトリビュートを指定します。

アトリビュート ID	パラメータ名	内容	属性	データ	
				データ型	値(Hex)
1	Revision	オブジェクトのレビジョン	読出	UINT	0001
2	Max Instance	最大のインスタンス番号	読出	UINT	0001
3	Number of Instance	インスタンスの数	読出	UINT	0001

● インスタンス用アトリビュート ID

インスタンスごとのアトリビュート ID を指定します。

アトリビュート ID	パラメータ名	内容	属性	データ	
				データ型	値
1	Max Number of Record	登録可能なレコード数	読出	UINT	
2	Number of Record	登録されているレコード数	読出	UINT	0～Max Number of Record
3	Undate Counter	カウンタ	読出	UINT	1～65535
4	Size of Record	読み出すレコードのバイトサイズ	読出	UINT	34

サービスコード

実行させるサービスを、サービスコードで指定します。

サービスコード (Hex)	パラメータ名	内容	サポートするサービス範囲	
			クラス単位	インスタンス単位
01	Get_Attribute_All	すべてのアトリビュートの値を読み出す。	可	可
0E	Get_Attribute_Single	指定したアトリビュートの値を読み出す。	可	可
34	Get Error Event	発生中の異常のイベントを取得する。	不可	可

Get_Error_Event（サービスコード: 34Hex）

発生中の異常のイベントを取得します。リクエストフォーマット、およびレスポンスフォーマットは以下のとおりです。

● リクエストフォーマット

パラメータ名	内容	データ型	値
Service	サービスコード	USINT	34Hex
Request Path Size	リクエストパスのサイズ	USINT	03
Request Path	リクエストパス	Padded EPATH	21004C032401Hex
Start Number of Read	読み出しを開始するレコード番号 先頭は 0	UINT	
Number of Read	読み出すレコード数*1	UINT	
Update Counter	事前に読み出したインスタンス用アトリビュート ID　3「Update Counter」の値*2 0：レコードの更新検知無効 0 以外：レコードの更新検知有効	UINT	

***1.** 指定した数のレコードが存在しない場合は、実際に読み出したレコード数がレスポンスの「Actual Number of Read」に格納されます。

***2.** 現在の「Update Counter」の値と異なる場合は、「Object state conflict」(0CHex)を返します。

● レスポンスフォーマット

パラメータ名	内容	データ型	値
Reply Service	Get Error Event サービスの応答	USINT	B4Hex
予約	予約	octet	00
General Status	正常を示すコード	USINT	00
Size of Additional Status	Additional ステータスのサイズ	USINT	00
Start Number of Read	実際に読み出した先頭レコード番号	UINT	
Actual Number of Read	実際に読み出したレコード数	UINT	
Update Counter	カウンタ	UINT	
Number of Record	登録されているレコード数	UINT	
Record	異常のイベントレコード	ARRAY OF STRUCT OF*1	

パラメータ名	内容	データ型	値
Index	レコードのインデックス*2	UDINT	0～4294967295 1 件ずつインクリメントされ、最大値に達すると 0 に戻る。
Product Code	プロダクトコード	DWORD	
Event Code	イベントコード*3	DWORD	
Event Priority	イベント重要度	WORD	3 : 軽度フォールト
Additional Info Data Type1	イベントの付属情報 1 のデータ型	BYTE	
Additional Info Data Type2	イベントの付属情報 2 のデータ型	BYTE	
Additional Info Data Type3	イベントの付属情報 3 のデータ型	BYTE	
Additional Info Data Type4	イベントの付属情報 4 のデータ型	BYTE	
Additional Info1	イベントの付属情報 1*3	Additional Info Data Type1 で指定されたデータ型(4 octets)	
Additional Info2	イベントの付属情報 2*3	Additional Info Data Type2 で指定されたデータ型(4 octets)	
Additional Info3	イベントの付属情報 3*3	Additional Info Data Type3 で指定されたデータ型(4 octets)	
Additional Info4	イベントの付属情報 4*3	Additional Info Data Type4 で指定されたデータ型(4 octets)	

***1.** 構造体のサイズは 34 バイトです。

***2.** 本オブジェクトは、現在発生中の異常のイベントを対象としています。「Index」は、異常のイベントが発生した時点で採番されるため、その後復旧した異常のイベントがあると、値が不連続になります。

***3.** 内容の詳細は、「11-2-4 イベントの内容と対処方法 (P.11-12)」を参照してください。

A-4-6 Safety Discrete Input Point (SDIP)オブジェクト（クラス ID：3DHex）

Safety Discrete Input Point(SDIP)オブジェクトは、セーフティ入力端子を 1 端子ごとに管理するオブジェクトです。

クラス ID、インスタンス ID

クラス ID とインスタンス ID は、以下のとおりです。

ID の種類	値(Hex)	内容
クラス ID	3D	
インスタンス ID	00	クラス自体を指定する。
	01-0C	セーフティ入力端子ごとのインスタンスを指定する。 01：セーフティ入力端子 Si00 02：セーフティ入力端子 Si01 03：セーフティ入力端子 Si02 04：セーフティ入力端子 Si03 05：セーフティ入力端子 Si04 06：セーフティ入力端子 Si05 07：セーフティ入力端子 Si06 08：セーフティ入力端子 Si07 09：セーフティ入力端子 Si08 0A：セーフティ入力端子 Si09 0B：セーフティ入力端子 Si10 0C：セーフティ入力端子 Si11

アトリビュート ID

読み出す情報を指定します。

● クラス用アトリビュート ID

オブジェクト全体のアトリビュートを指定します。

アトリビュート ID	パラメータ名	内容	属性	データ	
				データ型	値(Hex)
1	Revision	オブジェクトのレビジョン	読出	UINT	0001
2	Max Instance	最大のインスタンス番号	読出	UINT	000C
3	Number of Instance	インスタンスの数	読出	UINT	000C
8	Latch Input Error Time	Instance Attribute の Safety Status の、Alarm 状態のラッチ時間	読出 *1	UINT	0～65530 デフォルト値は、1000（DEC） 単位は ms 10ms 単位で設定可能

***1.** コンフィグレーションロック解除状態の場合に、書き込み可能です。

● インスタンス用アトリビュート ID

インスタンスごとのアトリビュート ID を指定します。

アトリビュートID	パラメータ名	内容	属性	データ	
				データ型	値
102	Maintenance Counter	Maintenance Counter の現在値	読書	UDINT	Maintenance Counter の現在値 セーフティ入力端子の接点動作回数（単位：回）を表す。 0 を書き込むことで、値をクリアする。

サービスコード

実行させるサービスを、サービスコードで指定します。

サービスコード(Hex)	パラメータ名	内容	サポートするサービス範囲	
			クラス単位	インスタンス単位
0E	Get_Attribute_Single	指定したアトリビュートの値を読み出す。	可	可
10	Set_Attribute_Single	指定したアトリビュートの値を書き込む。	不可	可

A-4-7 Safety Discrete Ouput Point (SDOP)オブジェクト（クラス ID：3BHex）

Safety Discrete Output Point(SDOP)オブジェクトは、セーフティ出力端子を 1 端子ごとに管理するオブジェクトです。

クラス ID、インスタンス ID

クラス ID とインスタンス ID は、以下のとおりです。

ID の種類	値(Hex)	内容
クラス ID	3B	
インスタンス ID	00	クラス自体を指定する。
	01-04	セーフティ出力端子ごとのインスタンスを指定する。

アトリビュート ID

読み出す情報を指定します。

● クラス用アトリビュート ID

オブジェクト全体のアトリビュートを指定します。

アトリビュート ID	パラメータ名	内容	属性	データ	
				データ型	値(Hex)
1	Revision	オブジェクトのレビジョン	読出	UINT	0001
2	Max Instance	最大のインスタンス番号	読出	UINT	0004
3	Number of Instance	インスタンスの数	読出	UINT	0004
8	Latch Output Error Time	Instance Attribute の Safety Status の、Alarm 状態のラッチ時間	読出	UINT	0～65530 デフォルト値は、1000(DEC) 単位は ms 10ms 単位で設定可能

● インスタンス用アトリビュート ID

インスタンスごとのアトリビュート ID を指定します。

アトリビュート ID	パラメータ名	内容	属性	データ	
				データ型	値
102	Maintenance Counter	Maintenance Counter の現在値	読書	UDINT	Maintenance Counter の現在値 セーフティ出力端子の接点動作回数（単位：回）を表す。 0 を書き込むことで、値をクリアする。

サービスコード

実行させるサービスを、サービスコードで指定します。

サービスコード(Hex)	パラメータ名	内容	サポートするサービス範囲	
			クラス単位	インスタンス単位
0E	Get_Attribute_Single	指定したアトリビュートの値を読み出す。	可	可

サービスコード(Hex)	パラメータ名	内容	サポートするサービス範囲	
			クラス単位	インスタンス単位
10	Set_Attribute_Single	指定したアトリビュートの値を書き込む。	不可	可

A-4-8 Device Level Ring (DLR)オブジェクト（クラス ID：47Hex）

Device Level Ring(DLR)オブジェクトは、DLR ネットワークの状態を示すオブジェクトです。

クラス ID、インスタンス ID

クラス ID とインスタンス ID は、以下のとおりです。

ID の種類	値(Hex)	内容
クラス ID	47	
インスタンス ID	00	クラス自体を指定する。
	01	インスタンスを指定する。

アトリビュート ID

読み出す情報を指定します。

● クラス用アトリビュート ID

オブジェクト全体のアトリビュートを指定します。

アトリビュート ID	パラメータ名	内容	属性	データ	
				データ型	値(Hex)
1	Revision	オブジェクトのレビジョン	読出	UINT	0003
2	Max Instance	最大のインスタンス番号	読出	UINT	0001
3	Number of Instance	インスタンスの数	読出	UINT	0001

● インスタンス用アトリビュート ID

インスタンスごとのアトリビュート ID を指定します。

アトリビュート ID	パラメータ名	内容	属性	データ	
				データ型	値
1	Network Topology	現在のネットワークトポロジのモード	読出	USINT	0 : Linear 1 : Ring リングスーパバイザがネットワーク上に存在する場合、常に 1 : Ring を示す。 リングスーパバイザがネットワーク上に存在しない場合、または設定されたリングパラメータが稼働中のリングスーパバイザでサポートされていない場合は 0 : Linear となり、その後はネットワークの状態に応じて Ring と Linear の間で遷移する。
2	Network Status	デバイスから見たネットワークの現在の状態	読出	USINT	下記「Network Status の値 (P.A-36)」を参照
3-9	Reserved 41 octets				

アトリビュート ID	パラメータ名	内容	属性	データ	
				データ型	値
10	Active Supervisor Address	アクティブリングスーパバイザの IP アドレスと MAC アドレス	読出	STRUCT	
	Supervisor IP Address	アクティブリングスーパバイザの IP アドレス		UDINT	デバイスのアクティブリングスーパバイザの IP アドレス*1
	Supervisor MAC Address	アクティブリングスーパバイザの MAC アドレス		ARRAY OF 6 USINTs	デバイスのアクティブリングスーパバイザの MAC アドレス*1
12	Capability Flags	デバイスが保持する DLR 上の機能	読出	DWORD	00000082Hex 固定 リング機能がビーコンフレームベース、かつ Flush_Table フレームをサポートしていることを意味する。

***1.** デフォルト値は、All0 です。アクティブリングスーパバイザが決定されると、その値に更新されます。

● Network Status の値

値	名称	内容
0	Normal	通常状態
1	Ring Fault	Ring Fault が検出された。 ネットワークトポロジが Ring の場合にだけ有効。
2	Unexpected Loop Detected	ネットワークでループが検出された。 ネットワークトポロジが Linear の場合にだけ有効。

サービスコード

実行させるサービスを、サービスコードで指定します。

サービスコード(Hex)	パラメータ名	内容	サポートするサービス範囲	
			クラス単位	インスタンス単位
01	Get_Attribute_All	すべてのアトリビュートの値を読み出す。	不可	可
0E	Get_Attribute_Single	指定したアトリビュートの値を読み出す。	可	可

A-4-9 QoS オブジェクト（クラス ID：48Hex）

QoS オブジェクトは、Ethernet フレーム優先制御の IPv4 DiffServ Code Point (DSCP) の値を設定するオブジェクトです。

クラス ID、インスタンス ID

クラス ID とインスタンス ID は、以下のとおりです。

ID の種類	値(Hex)	内容
クラス ID	48	
インスタンス ID	00	クラス自体を指定する。
	01	インスタンスを指定する。

アトリビュート ID

読み出す情報を指定します。

● クラス用アトリビュート ID

オブジェクト全体のアトリビュートを指定します。

アトリビュート ID	パラメータ名	内容	属性	データ	
				データ型	値(Hex)
1	Revision	オブジェクトのレビジョン	読出	UINT	0001
2	Max Instance	最大のインスタンス番号	読出	UINT	0001
3	Number of Instance	インスタンスの数	読出	UINT	0001

● インスタンス用アトリビュート ID

インスタンスごとのアトリビュート ID を指定します。

アトリビュート ID	パラメータ名	内容	属性	データ	
				データ型	値
4	DSCP Urgent	CIP Transport class 0/1 メッセージのうち、優先度を Urgent にした場合の DSCP 値	読書 *1	USINT	CIP Transport class 0/1 メッセージのうち、優先度を Urgent にした場合の DSCP 値 デフォルト値は、55('110111')
5	DSCP Scheduled	CIP Transport class 0/1 メッセージのうち、優先度を Scheduled にした場合の DSCP 値	読書 *1	USINT	CIP Transport class 0/1 メッセージのうち、優先度を Scheduled にした場合の DSCP 値 デフォルト値は、47('101111')
6	DSCP High	CIP Transport class 0/1 メッセージのうち、優先度を High にした場合の DSCP 値	読書 *1	USINT	CIP Transport class 0/1 メッセージのうち、優先度を High にした場合の DSCP 値 デフォルト値は、43('101011')
7	DSCP Low	CIP Transport class 0/1 メッセージのうち、優先度を Low にした場合の DSCP 値	読書 *1	USINT	CIP Transport class 0/1 メッセージのうち、優先度を Low にした場合の DSCP 値 デフォルト値は、31('011111')

アトリビュートID	パラメータ名	内容	属性	データ	
				データ型	値
8	DSCP Explicit	CIP Transport class 0/1 メッセージのうち、優先度を Explicit にした場合の DSCP 値	読書 *1	USINT	CIP Transport class 0/1 メッセージのうち、優先度を Explicit にした場合の DSCP 値 デフォルト値は、27('011011')

***1.** 設定はリスタート後に有効になります。

サービスコード

実行させるサービスを、サービスコードで指定します。

サービスコード(Hex)	パラメータ名	内容	サポートするサービス範囲	
			クラス単位	インスタンス単位
0E	Get_Attribute_Single	指定したアトリビュートの値を読み出す。	可	可
10	Set_Attribute_Single	指定したアトリビュートの値を書き込む。	不可	可

A-4-10 TCP/IP Interface オブジェクト（クラス ID：F5Hex）

TCP/IP Interace オブジェクトは、TCP/IP Interface の設定を行うオブジェクトです。

クラス ID、インスタンス ID

クラス ID とインスタンス ID は、以下のとおりです。

ID の種類	値(Hex)	内容
クラス ID	F5	
インスタンス ID	00	クラス自体を指定する。
	01	インスタンスを指定する。

アトリビュート ID

読み出す情報を指定します。

● クラス用アトリビュート ID

オブジェクト全体のアトリビュートを指定します。

アトリビュート ID	パラメータ名	内容	属性	データ	
				データ型	値(Hex)
1	Revision	TCP/IP Interface オブジェクトの対応レビジョン	読出	UINT	0004
2	Max Instance	最大のインスタンス番号	読出	UINT	0001
3	Number of Instance	インスタンスの数	読出	UINT	0001

● インスタンス用アトリビュート ID

インスタンスごとのアトリビュート ID を指定します。

アトリビュート ID	パラメータ名	内容	属性	データ	
				データ型	値
1	Status	TCP/IP インタフェースのステータス	読出	DWORD	下記「Status の値 (P.A-41)」を参照
2	Configuration Capability	TCP/IP インタフェースがサポートする各種機能についてのビットマップ	読出	DWORD	下記「Configuration Capability の値 (P.A-41)」を参照
3	Configuration Control	TCP/IP インタフェースの、コンフィグレーションの決定方法	読書	DWORD	下記「Configuration Control の値 (P.A-42)」を参照

アトリビュートID	パラメータ名	内容	属性	データ	
				データ型	値
4	Physical Link Object	物理層リンクオブジェクトへのパス	読出	STRUCT	
	Path size	WORD 単位のパスのサイズ		UINT	0000
	Path	物理層リンクオブジェクトの固定パス		Padded EPATH	All0Hex
5	Interface Configuration*1	インタフェースの設定	読書	STRUCT	
	IP Address	IP アドレス		UDINT	IP アドレス デフォルト値は、192.168.250.1 以下の値は設定不可。 • ホスト ID の全ビットが 0 または 1 の IP アドレス • 0、127 または 255 で始まる IP アドレス • クラス D の IP アドレス（224.0.0.0-239.255.255.255） • クラス E の IP アドレス（240.0.0.0-255.255.255.255） • リンクローカルアドレス（169.254.0.0-169.254.255.255）
	Network Mask	ネットワークマスク		UDINT	ネットワークマスク デフォルト値は、255.255.255.0 有効条件は、以下のとおり。 • 先頭からビットが連続していること。 • 192.0.0.0-255.255.255.252 の範囲内であること。
	Gateway Address	デフォルトゲートウェイ		UDINT	ゲートウェイアドレス デフォルト値は、0.0.0.0（ゲートウェイなしを示す） 以下の値は設定不可。 • 「IP Address」の設定条件を満たしていない。 • 「IP Address」で指定したネットワークアドレスと異なるセグメントの IP アドレスである。
	Name Server	DNS サーバのプライマリネームサーバ		UDINT	0.0.0.0 固定
	Name Server 2	DNS サーバのセカンダリネームサーバ		UDINT	0.0.0.0 固定
	Domain Name	ドメイン名		STRING	ドメイン名 デフォルト値は、""(NULL)
6	Host Name	ホスト名	読書	STRING	デバイスのホスト名を 64 文字以下の ASCII で設定する。 64 文字未満の場合は、残りの文字数分パディングする。
7	Safety Network Number	セーフティネットワーク番号（SNN）	読出	6 octets	セーフティネットワーク番号

アトリビュート ID	パラメータ名	内容	属性	データ	
				データ型	値
13	Encapsulation Inactivity Timeout	カプセル化の非アクティブタイムアウト時間	読書	UINT	0～3600 Encapsulation Inactivity Timeout の設定時間の間、EtherNet/IP による通信がなければ、TCP コネクションがクローズされる。 Encapsulation Inactivity Timeout = 0 の場合、TCP コネクションはクローズされない。 単位は、秒 デフォルト値は、120

***1.** IP アドレスの設定方法がロータリスイッチによる直接設定の場合、本アトリビュートへの書き込みは実行できません。

● Status の値

ビット	名称	内容
0-3	Interface Configuration Status	インスタンス用アトリビュート ID 05Hex（Interface Configuration）の設定状態 0 : 未設定または初期化中 1 : ハードウェアスイッチによる IP アドレス直接設定以外の IP アドレスの設定方法により IP アドレス設定済み 2 : ハードウェアスイッチによる IP アドレス直接設定により IP アドレス設定済み 3-15 : 予約
4	予約	常に FALSE
5	Interface Configuration Pending	TRUE : インスタンス用アトリビュート ID 05Hex（Interface Configuration）の設定内容が変更された。変更内容を有効にするには、セーフティ I/O ターミナルのリスタートが必要。 FALSE : インスタンス用アトリビュート ID 05Hex（Interface Configuration）が変更されていない。
6	AcdStatus	TRUE : IP アドレスの重複を検出した。ただし、この IP アドレスを使って CIP 通信は継続できる。 FALSE : IP アドレスの重複を検出していない。
7	AcdFault	TRUE : この IP アドレスを使って CIP 通信が継続できない。 FALSE : IP アドレスの重複を検出していない。あるいは、IP アドレスの重複を検出しているが、この IP アドレスを使って CIP 通信が継続できる。
8-31	予約	常に FALSE

● Configuration Capability の値

ビット	名称	内容
0	BOOTP Client	常に FALSE BOOTP クライアント機能使用不可
1	DNS Client	常に FALSE DNS クライアント機能使用不可
2	DHCP Client	常に TRUE DHCP クライアント機能使用可能
3	DHCP-DNS Update	常に FALSE DHCP-DNS Update 機能使用不可
4	Configuration Settable	常に TRUE Interface configuration アトリビュートが設定可能
5	Hardware Configuration	常に TRUE ハードウェアからの IP アドレス設定可能

ビット	名称	内容
6	Interface Configuration Change Requires Reset	常に TRUE 本アトリビュートの変更内容を有効にするためには、デバイスのリスタートが必要。
7	AcdCapable	常に FALSE IP アドレス重複検知機能使用不可
8-31	予約	常に FALSE

● Configuration Control の値

ビット	名称	内容
0-3	Configuration Method	セーフティ I/O ターミナルの IP アドレスの設定方法 0 : 不揮発メモリに保存した設定を使用する（デフォルト値）。 1 : BOOTP で設定する。 2 : DHCP で設定する。 3-15:予約
4	DNS Enable	常に FALSE DNS クライアント機能使用不可
5-31	予約	常に FALSE

サービスコード

実行させるサービスを、サービスコードで指定します。

サービスコード(Hex)	パラメータ名	内容	サポートするサービス範囲	
			クラス単位	インスタンス単位
0E	Get_Attribute_Single	指定したアトリビュートの値を読み出す。	可	可
10	Set_Attribute_Single	指定したアトリビュートの値を書き込む。	不可	可

A-4-11 Ethernet Link オブジェクト（クラス ID：F6Hex）

Ethernet Link オブジェクトは、Ethernet Link の各種情報を取得するオブジェクトです。

クラス ID、インスタンス ID

クラス ID とインスタンス ID は、以下のとおりです。

ID の種類	値(Hex)	内容
クラス ID	F6	
インスタンス ID	00	クラス自体を指定する。
	01-02	インスタンスを指定する。

アトリビュート ID

読み出す情報を指定します。

● クラス用アトリビュート ID

オブジェクト全体のアトリビュートを指定します。

アトリビュート ID	パラメータ名	内容	属性	データ	
				データ型	値(Hex)
1	Revision	Ethernet Link オブジェクトの対応レビジョン	読出	UINT	0004
2	Max Instance	最大のインスタンス番号	読出	UINT	0002
3	Number of Instance	インスタンスの数	読出	UINT	0002

● インスタンス用アトリビュート ID

インスタンスごとのアトリビュート ID を指定します。

アトリビュート ID	パラメータ名	内容	属性	データ	
				データ型	値
1	Interface Speed	インタフェースの通信速度	読出	UDINT	000AHex : 10Mbps 0064Hex : 100Mbps
2	Interface Flags	インタフェースのステータス	読出	DWORD	下記「Interface Flags の値 (P.A-46)」を参照
3	Physical Address	インタフェースの MAC アドレス	読出	ARRAY OF USINT*1	インタフェースの MAC アドレス

アトリビュートID	パラメータ名	内容	属性	データ	
				データ型	値
4	Interface Counters	インタフェースの通信統計情報	読出	STRUCT	
	In Octets	受信データバイト数		UDINT	受信データバイト数
	In Ucast Packets	Unicast 受信パケット数		UDINT	Unicast 受信パケット数
	In NUcast Packets	非 Unicast 受信パケット数		UDINT	非 Unicast 受信パケット数
	In Discards	破棄した受信パケット数		UDINT	破棄した受信パケット数
	In Errors	エラー受信パケット数		UDINT	エラー受信パケット数 ただし、「In Discards」の分は除く。
	In Unknown Protos	非サポートプロトコル受信パケット数		UDINT	非サポートプロトコル受信パケット数
	Out Octets	送信データバイト数		UDINT	送信データバイト数
	Out Ucast Packets	Unicast 送信パケット数		UDINT	Unicast 送信パケット数
	Out NUcast Packets	非 Unicast 送信パケット数		UDINT	非 Unicast 送信パケット数
	Out Discards	破棄した送信パケット数		UDINT	破棄した送信パケット数
	Out Errors	エラー送信パケット数		UDINT	エラー送信パケット数
5	Media Counters	インタフェースのメディア統計情報	読出	STRUCT	
	Alignment Errors	アライメントエラーフレーム受信数		UDINT	アライメントエラーフレーム受信数
	FCS Errors	FCS エラー受信回数		UDINT	FCS エラー受信回数
	Single Collisions	送信成功したが 1 回衝突を検出したフレーム数		UDINT	送信成功したが 1 回衝突を検出したフレーム数
	Multiple Collisions	送信成功したが 2 回以上衝突を検出したフレーム数		UDINT	送信成功したが 2 回以上衝突を検出したフレーム数
	SQE Test Errors	SQE テストエラー発生回数		UDINT	SQE テストエラー発生回数
	Deferred Transmissions	送信ディレーが発生したフレーム数		UDINT	送信ディレーが発生したフレーム数
	Late Collisions	パケットの送信に 512 ビット時間後に衝突が検出された回数		UDINT	パケットの送信に 512 ビット時間後に衝突が検出された回数
	Excessive Collisions	過度の衝突により送信が失敗したフレーム数		UDINT	過度の衝突により送信が失敗したフレーム数
	MAC Transmit Errors	MAC 層の送信エラーにより送信が失敗したフレーム数		UDINT	MAC 層の送信エラーにより送信が失敗したフレーム数
	Carrier Sense Errors	キャリアセンスエラーを検出した回数		UDINT	キャリアセンスエラーを検出した回数
	Frame Too Long	最大フレームサイズを超えたフレーム数		UDINT	最大フレームサイズを超えたフレーム数
	MAC Receive Errors	MAC 層の受信エラーにより受信が失敗したフレーム数		UDINT	MAC 層の受信エラーにより受信が失敗したフレーム数

アトリビュートID	パラメータ名	内容	属性	データ	
				データ型	値
6	Interface Control	インタフェースのコンフィグレーション	読書 *2	STRUCT	
	Control Bits	通信速度の決め方		WORD	下記「Control Bits の値 (P.A-46)」を参照 デフォルト値は、0001Hex
	Forced Interface Speed	Auto-Negotiation が無効の場合の通信速度		UINT	0064Hex : 100Mbps デフォルト値は、0000Hex *3*4
7	Interface Type	本インスタンスの物理インタフェースのタイプ	読出	USINT	02Hex 固定 : ツイストペア
8	Interface State	インタフェースの状態	読出	USINT	00Hex : 状態不明 01Hex : 送受信できる状態 02 : 無効状態 03 : テスト中 04-FFHex : 予約
10	Interface Label	インタフェース識別の文字列	読出	SHORT STRING	Instance 1: “Ethernet Port 1”固定 Instance 2: “Ethernet Port 2”固定
11	Interface Capability	インタフェースの通信性能	読出	STRUCT	−
	Capability Bits	通信性能設定		DWORD	下記「Capability Bits の値 (P.A-46)」を参照
	Speed/Duplex Options	インタフェースが取りうる通信速度と Duplex モードの組み合わせ		STRUCT	
	Speed/Duplex Array Count	通信速度／双方向配列サイズ		USINT	2 固定
	Speed/Duplex Array	通信速度／双方向配列		ARRAY OF STRUCT	
	Interface Speed	インタフェースの通信速度		UINT	0064Hex: 100Mbps
	Interface Duplex Mode	インタフェースの双方向モード		USINT	00Hex: Half Duplex
	Speed/Duplex Array	通信速度／双方向配列		ARRAY OF STRUCT	
	Interface Speed	インタフェースの通信速度		UINT	0064Hex: 100Mbps
	Interface Duplex Mode	インタフェースの双方向モード		USINT	01Hex: Full Duplex
14	Ethernet Errors	Interface Counters、Media Counters、HC Media Counters の合計値	読出	UDINT	Interface Counters、Media Counters、HC Media Counters の合計値 デフォルト値は、0
15	Link Down Counter	Ethernet ポートがリンクアップ状態からリンクダウン状態に遷移した回数	読出	UDINT	Ethernet ポートがリンクアップ状態からリンクダウン状態に遷移した回数 デフォルト値は、0

アトリビュート ID	パラメータ名	内容	属性	データ	
				データ型	値
100	Communication Cable Diagnosis	通信ケーブル診断の結果	読出	UINT	下記「Communication Cable Diagnosis の値 (P.A-47)」を参照

***1.** 配列サイズは 6 です。
***2.** 設定はリスタート後に有効になります。
***3.** 以下の場合、09Hex (Invalid Attribute Value)の異常になります。
- 「Control Bits」の bit2-15（予備ビット）のいずれかが TRUE の場合。
- 「Control Bits」の bit0 (Auto-negotiate)が FALSE、bit1 (Forced duplex Mode)が TRUE、かつ「Forced Interface Speed」に設定範囲以外の値を設定しようとした場合。

***4.** 以下の場合、0CHex (Object State Conflict)の異常になります。
- 「Control Bits」の bit0 (Auto-negotiate)が TRUE、bit1 (Forced duplex Mode)が FALSE、かつ「Forced Interface Speed」に何らかの値を設定しようとした場合。

● Interface Flags の値

ビット	名称	内容
0	Link Status	TRUE : Ethernet リンク確立済み FALSE : Ethernet リンク確立なし
1	Half/Full Duplex***1**	TRUE : Full Duplex FALSE : Half Duplex
2-4	Negotiation Status	0 : Auto-negotiation 実行中 1 : Auto-negotiation 失敗 通信速度 10Mbps の Half Duplex で動作する。 2 : Auto-negotiation 失敗 設定した通信速度の Half Duplex で動作する。 3 : Auto-negotiation 成功 4 : Auto-negotiation 無効
5	Manual Setting Requires Reset	TRUE : Interface Control Attribute を変更した後、デバイスリセット必要 FALSE : Interface Control Attribute を変更した後、デバイスリセット不要
6	Local Hardware Fault	TRUE : ハード異常あり FALSE : ハード異常なし
7-31	予約	常に FALSE

***1.** Link Status = 0 の場合は、意味を持ちません。

● Control Bits の値

ビット	名称	内容
0	Auto-negotiate	TRUE : Auto-negotiate 有効 FALSE : Auto-negotiate 無効。Forced Duplex Mode と Forced Interface Speed の設定に従って動作する。
1	Forced Duplex Mode	TRUE : Full Duplex FALSE : Half Duplex Auto-negotiate が FALSE の場合、本ビットを使用する。Auto-negotiate が TRUE の場合、本ビットを設定すると、0CHex(Object State Conflict)のエラーコードが返る。
2-15	予約	常に FALSE

● Capability Bits の値

ビット	名称	内容
0	Manual Setting Requires Reset	常に TRUE : Interface Control Attribute を変更した後、デバイスのリセットが必要であることを示す。
1	Auto-negotiate	常に TRUE : Auto-negotiation をサポート
2	Auto-MDIX	常に TRUE : Auto-MDIX をサポート
3	Manual Speed/Duplex	常に TRUE : Speed/Duplex の手動設定をサポート

ビット	名称	内容
4-31	予約	常に FALSE

● Communication Cable Diagnosis の値

ビット	内容
0-7	ポートからの異常発生位置 単位 m 診断結果異常の場合は、0
8-15	00Hex : 未実行 01Hex : 正常 02Hex : 短絡 03Hex : 断線 04Hex : ポート無効 F1Hex : 診断実行中 F2Hex : 診断結果異常 F3Hex : PHY 読出異常

サービスコード

実行させるサービスを、サービスコードで指定します。

サービスコード(Hex)	パラメータ名	内容	サポートするサービス範囲	
			クラス単位	インスタンス単位
0E	Get_Attribute_Single	指定したアトリビュートの値を読み出す。	可	可
10	Set_Attribute_Single	指定したアトリビュートの値を書き込む。	不可	可
3A	Exec_Cable_Diagnosis	通信ケーブル診断を実行する。*1	不可	可
4C	Get_and_Clear	指定したアトリビュートの値を読み出した後、アトリビュートの値をクリアする。*2*3	不可	可

***1.** リンク確立している通信ポートに対するインスタンスに本サービスを実行した場合、通信ケーブル診断は実行されず、常に異常なしになります。また、通信ケーブル診断実行中の通信ポートに対するインスタンスに本サービスを実行した場合、0CHex (Object State Conflict)の異常になります。

***2.** 本サービスをサポートするインスタンス用アトリビュートは、以下のとおりです。

- Interface Counters(04)
- Media Counters(05)
- Link_Down Counter(15)

上記以外のアトリビュートを指定した場合は、09Hex(Invalid attribute value)が、レスポンスコードとして返ります。

***3.** 以下の組み合わせにおいて、いずれかに対して本サービスを実行した場合、値が読み出されるのはどちらか一方だけになり、両方ともリセットされます。

- Interface Counters(04Hex)と HC Interface Counters(12Hex)
- Media Counters(05Hex)と HC Media Counters(13Hex)

A-4-12 LLDP Management オブジェクト（クラス ID：109Hex）

LLDP Management オブジェクトは、LLDP 機能を管理するオブジェクトです。

クラス ID、インスタンス ID

クラス ID とインスタンス ID は、以下のとおりです。

ID の種類	値(Hex)	内容
クラス ID	109	
インスタンス ID	00	クラス自体を指定する。
	01	インスタンスを指定する。

アトリビュート ID

読み出す情報を指定します。

● クラス用アトリビュート ID

オブジェクト全体のアトリビュートを指定します。

アトリビュート ID	パラメータ名	内容	属性	データ	
				データ型	値(Hex)
1	Revision	オブジェクトのレビジョン	読出	UINT	0001
2	Max Instance	最大のインスタンス番号	読出	UINT	0001
3	Number of Instance	インスタンスの数	読出	UINT	0001

● インスタンス用アトリビュート ID

インスタンスごとのアトリビュート ID を指定します。

アトリビュート ID	パラメータ名	内容	属性	データ	
				データ型	値
1	LLDP Enable	LLDP 有効	読書	STRUCT	
	LLDP Enable Array length	LLDP Enable Array で設定するポート数		UINT	LLDP 機能全体の設定も含むため、EthernetLink Object のインスタンス + 1 となる。 3 固定
	LLDP Enable Array	LLDP 機能全体、または各ポートの LLDP 有効／無効設定		ARRAY OF BYTE	下記「LLDP Enable Array の値 (P.A-49)」を参照
2	msgTxInterval	LLDP フレームの送信間隔	読書	UINT	LLDP フレームの送信間隔 1～3600 単位は秒 デフォルト値は、30

アトリビュートID	パラメータ名	内容	属性	データ	
				データ型	値
3	msgTxHold	LLDP フレームの TTL 値を決定するための乗数	読書	USINT	1～100 TTL 値は、msgTxInterval × msgTxHold で求められる。 デフォルト値は、4 したがって、TTL 値のデフォルト値は、30 × 4 =120 秒となる。 msgTxInterval × msgTxHold の結果が 65535 を超える場合、TTL 値は 65535 秒となる。
4	LLDP Datastore	LLDP データベースの取得方法	読出	WORD	1 固定 : SNMP による取得
5	Last Change	ローカル LLDP データベースのエントリが最後に変更されたときに取得した、sysUpTime の値	読出	UDINT	ローカル LLDP データベースのエントリが最後に変更されたときに取得した、sysUpTime の値 sysUpTime は、システムのネットワーク管理部分が最後に初期化されてからの時間を表す。単位は 0.01 秒。

● LLDP Enable Array の値

ビット	名称	内容
0	Global Enable	TRUE : LLDP 送受信有効（デフォルト値） FALSE : LLDP 送受信無効 TRUE から FALSE に値が変更されると、既存の全テーブルエントリが削除される。
1	Port 1 Enable	TRUE : ポート 1 からの LLDP 送信有効（デフォルト値） FALSE : ポート 1 からの LLDP 送信無効
2	Port 2 Enable	TRUE : ポート 2 からの LLDP 送信有効（デフォルト値） FALSE : ポート 2 からの LLDP 送信無効
3-7	予約	常に FALSE

サービスコード

実行させるサービスを、サービスコードで指定します。

サービスコード(Hex)	パラメータ名	内容	サポートするサービス範囲	
			クラス単位	インスタンス単位
0E	Get_Attribute_Single	指定したアトリビュートの値を読み出す。	可	可
10	Set_Attribute_Single	指定したアトリビュートの値を書き込む。	不可	可

A-4-13 LLDP Data Table オブジェクト（クラス ID：10AHex）

LLDP Data Table オブジェクトは、LLDP 機能のデータを管理するオブジェクトです。

クラス ID、インスタンス ID

クラス ID とインスタンス ID は、以下のとおりです。

ID の種類	値(Hex)	内容
クラス ID	10A	
インスタンス ID	00	クラス自体を指定する。
	01-30	インスタンスを指定する。

アトリビュート ID

読み出す情報を指定します。

● クラス用アトリビュート ID

オブジェクト全体のアトリビュートを指定します。

アトリビュート ID	パラメータ名	内容	属性	データ	
				データ型	値(Hex)
1	Revision	オブジェクトのレビジョン	読出	UINT	0001
2	Max Instance	現在生成されているインスタンス ID の最大値	読出	UINT	0000-0030
3	Number of Instance	現在生成されているインスタンスの数	読出	UINT	0000-0030

● インスタンス用アトリビュート ID

インスタンスごとのアトリビュート ID を指定します。

アトリビュート ID	パラメータ名	内容	属性	データ	
				データ型	値
1	Ethernet Link Instance Number	LLDP フレームを受信した Ethernet ポートとリンクする Ethernet Link オブジェクト(F6Hex)のインスタンス番号	読出	UINT	LLDP フレームを受信した Ethernet ポートとリンクする Ethernet Link オブジェクト(F6Hex)のインスタンス番号 不明の場合は、0

アトリビュートID	パラメータ名	内容	属性	データ	
				データ型	値
2	MAC Address	受信した LLDP フレームを送信してきた隣接デバイスの MAC アドレス	読出	ETH_MAC_ADDR	格納される値は、以下の優先順位で決定される。 優先順位 1 : TLV Type = 127、かつ Subtype = 2 の場合、CIP MAC Address 優先順位 2 : TLV Type = 1、かつ Subtype = 4 の場合、Chassis ID 優先順位 3 : TLV Type = 2、かつ Subtype = 3 の場合、Port ID 優先順位 4 : すべて 0
3	Interface Label	受信した LLDP フレームを送信してきた隣接デバイスのインタフェースラベル	読出	SHORT STRING	格納される値は、以下の優先順位で決定される。 優先順位 1 : TLV Type = 127、かつ Subtype = 3 の場合、CIP Interface Label 優先順位 2 : TLV Type = 1、かつ Subtype = 6 の場合、Chassis ID 優先順位 3 : TLV Type = 2、かつ Subtype = 5 の場合、Port ID 優先順位 4 : Null
4	Time to Live	隣接デバイスの情報が有効である時間	読出	UINT	隣接デバイスの情報が有効である時間 単位は秒 Time to Live = 0 の場合、本インスタンスを消去する必要があることを意味する。
5	System Capabilities TLV	隣接デバイスがサポートする機能	読出	STRUCT	
	System Capabilities	隣接デバイスがサポート可能な機能		WORD	下記「System Capabilities、Enabled Capabilities の値 (P.A-53)」を参照
	Enabled Capabilities	隣接デバイスで現在有効になっている機能		WORD	下記「System Capabilities、Enabled Capabilities の値 (P.A-53)」を参照
6	IPv4 Management Addresses	隣接デバイスのマネジメントアドレス	読出	STRUCT	
	Management Address Count	格納するマネジメントアドレスの数		USINT	格納するマネジメントアドレスの数 最大 255
	Management Address	マネジメントアドレスの値		ARRAY OF UDINT	マネジメントアドレスの値 ClassA、B、および C の場合に有効。All 0 やループバックアドレスの場合は、格納しない。

アトリビュートID	パラメータ名	内容	属性	データ	
				データ型	値
7	CIP Identification	隣接デバイスの CIP Identity	読出	STRUCT	
	Vendor ID	ベンダー ID		UINT	ベンダー ID 受信した LLDP フレームに対応する TLV が含まれていなければ、0
	Device Type	デバイスタイプ		UINT	デバイスタイプ 受信した LLDP フレームに対応する TLV が含まれていなければ、0
	Product Code	製品コード		UINT	製品コード 受信した LLDP フレームに対応する TLV が含まれていなければ、0
	Major Revision	メジャー・リビジョン		BYTE	メジャー・リビジョン 受信した LLDP フレームに対応する TLV が含まれていなければ、0
	Minor Revision	マイナー・リビジョン		USINT	マイナー・リビジョン 受信した LLDP フレームに対応する TLV が含まれていなければ、0
	CIP Serial Number	CIP シリアル番号		UDINT	CIP シリアル番号 受信した LLDP フレームに対応する TLV が含まれていなければ、0
8	Additional Ethernet Capabilities	Ethernet Preemption 機能の状態	読出	STRUCT	
	Preemption Support	隣接ノードの Preemption（TSN 機能）のサポート状況		BOOL	TRUE : サポートしている。 FALSE : サポートしていない。
	Preemption Status	隣接ノードの Preemption（TSN 機能）の有効／無効		BOOL	TRUE : 有効 FALSE : 無効
	Preemption Active	隣接ノードの Preemption（TSN 機能）がアクティブかどうか		BOOL	TRUE : アクティブ FALSE : 非アクティブ
	Additional Fragment Size	隣接ノードの Preemption（TSN 機能）が起こる前にフレーム送信しなければならないオクテット数		USINT	0 : 64 オクテット 1 : 128 オクテット 2 : 192 オクテット 3 : 256 オクテット 4～255 : 予約

アトリビュートID	パラメータ名	内容	属性	データ	
				データ型	値
9	Last Change	本インスタンスが最後に変更されたときに取得した、sysUpTime の値	読出	UDINT	本インスタンスが最後に変更されたときに取得した、sysUpTime の値 sysUpTime は、システムのネットワーク管理部分が最後に初期化されてからの時間を表す。単位は 0.01 秒。

● System Capabilities、Enabled Capabilities の値

ビット	内容
0	Other
1	Repeater
2	Bridge
3	Access Point
4	Router
5	Telephone
6	DOCSIS Cable Device
7	End Station
8	C-VLAN component
9	S-VLAN component
10	Two-port MAC Relay Component
11-15	予約

サービスコード

実行させるサービスを、サービスコードで指定します。

サービスコード (Hex)	パラメータ名	内容	サポートするサービス範囲	
			クラス単位	インスタンス単位
0E	Get_Attribute_Single	指定したアトリビュートの値を読み出す。	可	可
11	Find_Next_Object_Instance	次のオブジェクトを検索します。	可	可

Find_Next_Object_Instance（サービスコード: 11Hex）

次のオブジェクトを検索します。リクエストフォーマット、およびレスポンスフォーマットは以下のとおりです。

● リクエストフォーマット

パラメータ名	内容	データ型	値
Service	サービスコード	USINT	11Hex
Maximum Returned Values	Instance ID List の最大インスタンス ID メンバ数	USINT	

● **レスポンスフォーマット**

パラメータ名	内容	データ型	値
Reply Service	Find_Next_Object_Instance サービスの応答	USINT	91Hex
Number Of List Members	メンバの数	USINT	
Instance ID List	インスタンス ID のリスト	ARRAY OF UINT	

A-4-14 Logic Process オブジェクト（クラス ID：309Hex）

Logic Process オブジェクトは、動作しているアプリケーションの番号を読み出すオブジェクトです。

クラス ID、インスタンス ID

クラス ID とインスタンス ID は、以下のとおりです。

ID の種類	値(Hex)	内容
クラス ID	309	
インスタンス ID	00	クラス自体を指定する。
	01	インスタンスを指定する。

アトリビュート ID

読み出す情報を指定します。

● クラス用アトリビュート ID

オブジェクト全体のアトリビュートを指定します。

アトリビュート ID	パラメータ名	内容	属性	データ	
				データ型	値(Hex)
1	Revision	オブジェクトのレビジョン	読出	UINT	0001

● インスタンス用アトリビュート ID

インスタンスごとのアトリビュート ID を指定します。

アトリビュート ID	パラメータ名	内容	属性	データ	
				データ型	値
101	Application Number	アプリケーションの番号	読出	USINT	下記「Application Number の値 (P.A-55)」を参照

● Application Number の値

値	内容
0	リモート I/O モード用アプリケーション
1	固定アプリケーション 1 部分停止+全体停止アプリケーション
2	固定アプリケーション 2 部分停止+全体停止アプリケーション（EDM あり）
3	固定アプリケーション 3 作業者とロボットのオートスイッチングアプリケーション
4-7	予約
8	予約
9-13	アドオンアプリケーション 1-5
14	予約
15	ユーザ定義アプリケーション

ロータリスイッチの値が不正値や読み出し失敗の場合、ロック状態ならばロック時の値が返ります。ロック解除状態ならば FFHex が返ります。

サービスコード

実行させるサービスを、サービスコードで指定します。

サービスコード(Hex)	パラメータ名	内容	サポートするサービス範囲	
			クラス単位	インスタンス単位
0E	Get_Attribute_Single	指定したアトリビュートの値を読み出す。	可	可
10	Set_Attribute_Single	指定したアトリビュートの値を書き込む。	不可	可

A-5 適合宣言書

No. EUSP0001A

Original

OMRON

EU DECLARATION OF CONFORMITY

1. **Product Models/Products:**
   NXR-S series
2. **Name and address of the manufacturer:**
   OMRON Corporation
   Shiokoji Horikawa, Shimogyo-Ku, Kyoto, 600-8530 Japan
3. **This declaration of conformity is issued under the sole responsibility of the manufacturer.**
4. **Objects of the declaration:**
   NXR-S series, Remote Terminal
5. **The objects of the declaration described above are in conformity with the relevant Union harmonisation legislation:**
   2014/30/EU EMC Directive
   2006/42/EC Machinery Directive
   2011/65/EU RoHS Directive
6. **References to the relevant harmonised standards used or references to the other technical specifications in relation to which conformity is declared:**
   EMC Directive: EN 61131-2: 2007
   Machinery Directive: EN ISO 13849-1:2023
   RoHS Directive: EN IEC 63000: 2018
7. **Name, address, and identification number of Notified Body, Number of EC Type Examination**
   Notified body: TÜV Rheinland Industrie Service GmbH
   Address: Am Grauen Stein, 51105 Köln / Germany
   Notified Body identification No.: 0035
   Certificate for EU Type Examination: 01/205/6092.00/26

Signed and on behalf of: OMRON Corporation
Place and date of issue: Kyoto, Japan 13th Jul, 2026

Signature:
Name: Kozo Kando
Function: Senior General Manager, Controller Division, Industrial Automation Company

1/3
GQ-151845A1

No. EUSP0001A

Name and address of contact in EU

OMRON Europe B.V.
Quality & Environment Department
Attn: J.J.P.W. Vogelaar, European Quality & Environment Manager
Zilverenberg 2, 5234 GM, 's-Hertogenbosch, The Netherlands

2/3
GQ-151845A1

No. EUSP0001A

Additional information

Models List

Model	Type	EMI	EMS	RoHS	Rev
		EN61131-2	EN61131-2	EN IEC 63000	
NXR-SXD1204-CST	Safety I/O Block	2007	2007 zone B	2018	<A>
NXR-SXD1204B-CST	Safety I/O Block	2007	2007 zone B	2018	<A>
NXR-SXD1204-EIT	Safety I/O Block	2007	2007 zone B	2018	<A>

Model name may be followed by additional letter (s) and /or number (s) for sale purposes.

3/3
GQ-151845A1

I

索引

索引

D

Device Level Ring(DLR)機能....8-10

E

EPI....7-31
EtherNet/IP 通信コネクタ 1....3-2, 3-3
EtherNet/IP 通信コネクタ 2....3-2, 3-3
EX PWR OUT LED....3-7

H

HTTPS 通信機能....8-8

I

I/O LED....3-3, 3-4
I/O ケーブルの接続手順（スマートクリックコネクタ）5-17
I/O ケーブルの接続手順（ねじ式コネクタ）....5-19
I/O ケーブルの取り外し手順（スマートクリックコネクタ）.
....5-18
I/O ケーブルの取り外し手順（ねじ式コネクタ）....5-21
I/O コネクタ....3-2, 3-4
I/O 識別マーカ....3-3, 3-4
I/O 配線チェック機能....8-13
I/O モニタ機能....8-27
Implicit 通信....6-6
IP アドレス表示機能....8-19

L

L/A ETH1 LED....3-6
L/A ETH2 LED....3-7
LLDP 機能....7-40
LOCK LED....3-7

M

M12 アタッチメント....5-7, 5-19
M12 トルクレンチ....5-7, 5-19
MAC アドレス....31
MS LED....3-6

N

NS LED....3-6

O

OUT PWR LED....3-5

U

U/IN PWR LED....3-5

あ

安全応答性能....9-2

い

イベント....11-2
イベントログ機能....11-6
インポート....7-34

え

エクスポート....7-34

お

オープンタイプ....6-4

か

カバー固定穴....3-3, 3-4

こ

コンフィグレーションロック....7-95

さ

再起動....7-82
サイクリック通信....6-6

し

締め付け工具....5-7, 5-11, 5-19
締め付けトルク....5-10, 5-11, 5-21
出力用電源....4-2
出力用電源の総消費電流....4-7
使用する電源....4-19
初期セーフティパスワード変更....7-23

す

スター型....1-13
ステータス LED....3-3, 3-4

せ

生産情報画面....32
接点動作回数モニタ機能....8-29
セーフティ出力 LED....3-8
セーフティ出力ポート....3-13
セーフティ入出力ポート....3-13
セーフティ入力 LED....3-8
セーフティ入力ポート....3-12
セーフティパスワード....7-100
セーフティリアクションタイム....9-2

た

タグデータリンク..... 6-6
タグデータリンク通信の設定手順.....7-36
端子配列..... 3-11, 3-12

ち

直接供給.....4-3
直接供給での総消費電流の計算方法.....4-7
直接供給での電圧降下の計算.....4-10

つ

通信ケーブル診断機能..... 8-31
通信ケーブルの接続手順（スマートクリックコネクタ）5-5
通信ケーブルの接続手順（ねじ式コネクタ）.....5-7
通信ケーブルの取り外し手順（スマートクリックコネクタ）.
..... 5-6
通信ケーブルの取り外し手順（ねじ式コネクタ）..... 5-9
通信コネクタ.....3-11
ツリー型..... 1-13

て

電源ケーブルの接続手順..... 5-14
電源ケーブルの取り外し手順.....5-16
点検項目..... 12-3
電源コネクタ IN..... 3-2, 3-4, 3-12
電源コネクタ OUT.....3-3, 3-4, 3-12
点検に必要な機材..... 12-2
電源モニタ機能.....8-22
電源容量..... 4-19
データパケットインターバル(EPI)..... 7-31

と

動作状態モニタ機能.....11-3
動作モード変更.....7-91
時計情報自動調整機能..... 7-87

は

バックアップ..... 7-104
バックアップ機能を使ったユニット交換..... 12-4
バックアップ機能を使わないユニット交換..... 12-5
汎用 CIP コマンド送信機能.....8-15

ふ

ファームウェアアップデート機能.....8-34

ほ

ポート..... 3-12

め

メモリオールクリア機能.....8-4

ゆ

ユニット識別マーカ.....3-3, 3-4
ユニット特定機能.....8-16
ユニット特定表示 LED.....3-3, 3-4
ユニット取付穴.....3-3, 3-4
ユニット本体の取り付け.....5-3
ユニット／入力用電源.....4-2
ユニット／入力用電源の総消費電流.....4-7

ら

ライン型..... 1-13

り

リング型..... 1-14

ろ

ログアウト.....7-23
ログイン..... 7-21
ロット番号.....31
ロータリスイッチ.....3-3, 3-4
ロータリスイッチ用カバーの取り付け.....5-3

わ

渡り配線出力用電源遮断機能.....8-11
渡り配線による供給.....4-3
渡り配線による供給での総消費電流の計算方法.....4-12
渡り配線による供給での電圧降下の計算..... 4-15

オムロン株式会社 インダストリアルオートメーションビジネスカンパニー

製品に関するお問い合わせ先

お客様相談室

フリー通話 **0120-919-066**（クイック　オムロン）

携帯電話の場合、

055-982-5015（有料）をご利用ください。

受付時間：9:00～17:00（土・日・12/31～1/3を除く）

オムロンFAクイックチャット

www.fa.omron.co.jp/contact/tech/chat/

技術相談員にチャットでお問い合わせいただけます。（I-Webメンバーズ限定）

受付時間：平日9:00～12:00 / 13:00～17:00（土日祝日・年末年始・当社休業日を除く）

※受付時間、営業日は変更の可能性がございます。最新情報はリンク先をご確認ください。

その他のお問い合わせ：納期・価格・サンプル・仕様書は貴社のお取引先、または貴社担当オムロン販売員にご相談ください。オムロン制御機器販売店やオムロン販売拠点は、Webページでご案内しています。

オムロン制御機器の最新情報をご覧いただけます。緊急時のご購入にもご利用ください。 **www.fa.omron.co.jp**

●本誌に記載のない条件や環境での使用、および原子力制御・鉄道・航空・車両・燃焼装置・医療機器・娯楽機械・安全機器、その他人命や財産に大きな影響が予測されるなど、特に安全性が要求される用途に使用される際には、当社の意図した特別な商品用途の場合や特別の合意がある場合を除き、当社は当社商品に対して一切保証をいたしません。

●本製品の内、外国為替及び外国貿易法に定める輸出許可、承認対象貨物（又は技術）に該当するものを輸出（又は非居住者に提供）する場合は同法に基づく輸出許可、承認（又は役務取引許可）が必要です。

オムロン商品のご用命は

Man. No. SBCD-386B　2026年7月現在

©OMRON Corporation 2026 All Rights Reserved.
お断りなく仕様などを変更することがありますのでご了承ください