

NJ/NXコントローラ セキュリティガイドライン

おことわり

- 本資料には安全に関する注意事項を含め、使用する際の詳細内容については記載していません。必ず、本資料で使用する各機器のマニュアルや取扱説明書を入手し、「安全上の注意」、「安全上の要点」、「使用上の注意」などの安全に関する注意事項を含め、内容を確認した上で使用してください。
- 本資料の内容の一部または全部を、オムロン株式会社の許可なしに複写、複製、転載することを禁じます。
- 本資料の内容に関しては、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。
- 本資料の内容に関しては、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、お手数ですが担当者までご連絡ください。

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。
- 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、ドイツ Beckhoff Automation GmbH によりライセンスされた特許取得済み技術であり登録商標です。
- ODVA、CIP、CompoNet、DeviceNet、EtherNet/IP 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

- 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/ をご覧ください。

はじめに

本書の目的

本書は、お客様に当社の FA 製品のセキュリティの取り組みをご理解いただくことと、当社 FA 製品を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を示すことを目的とし、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を示します。
FA システムセキュリティガイドラインおよび関連マニュアルとあわせてお読みください。

対象となる読者の方々

本書は、セキュリティ対策を計画、検討、実施される次の方々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

対象となる製品

本書は以下の製品を対象にしています。

- NX シリーズ CPU ユニット
- NJ シリーズ CPU ユニット

各製品の仕様については、製品のマニュアルを参照してください。

免責事項

本書におけるお客様への推奨事項は、当社が行った分析、および検討の結果に基づいています。適切なセキュリティ対策はお客様の環境によって異なるため、当該推奨事項をもって、お客様の環境におけるすべてのセキュリティ被害の防止を保証するものではありません。本書を参考に、お客様自身にて、お客様の環境に沿った分析および適切な対策を検討し、実施してください。

目次構成

		1
1	NJ/NXコントローラによる多層防御	2
2	資産を守るNJ/NXセキュリティ機能	3
3	セキュリティパッチを適用する	4
4	装置を安全に廃棄する	A
A	付録	

目次

はじめに.....	1
本書の目的.....	1
対象となる読者の方々.....	1
対象となる製品.....	1
免責事項.....	1
目次構成.....	3
関連ガイドライン・マニュアル.....	6
改訂履歴.....	7

第 1 章 NJ/NX コントローラによる多層防御

1-1 NJ/NX コントローラの使用環境.....	1-2
1-2 NJ/NX コントローラを活用した技術層のセキュリティ対策.....	1-3

第 2 章 資産を守る NJ/NX セキュリティ機能

2-1 通信回線上のデータを保護する.....	2-2
2-1-1 セキュア通信機能.....	2-2
2-1-2 セキュアソケットサービス機能.....	2-2
2-1-3 OPC UA サーバ機能.....	2-3
2-1-4 DB 接続機能.....	2-4
2-2 コントローラへの外部からの攻撃を遮断する.....	2-6
2-2-1 パケットフィルタ機能.....	2-6
2-2-2 TCP/UDP ポートクローズ機能.....	2-6
2-3 コントローラへの不正接続を防止する.....	2-8
2-3-1 ユーザ認証機能.....	2-8
2-3-2 CPU ユニット名称、シリアル ID.....	2-9
2-4 コントローラの不正操作を防止する.....	2-10
2-4-1 操作権限認証機能.....	2-10
2-5 プロジェクトファイル・ユーザプログラムを保護する.....	2-11
2-5-1 プロジェクトファイルのパスワードプロテクト.....	2-11
2-5-2 データプロテクト.....	2-11
2-5-3 ソースなしライブラリ.....	2-12
2-5-4 ユーザプログラム復元情報なし転送.....	2-12
2-5-5 CPU ユニットへの書込プロテクト.....	2-12
2-6 コントローラの不正利用を防止する.....	2-14
2-6-1 ユーザプログラム実行用 ID 認証機能.....	2-14
2-7 コントローラの安定動作を保護する.....	2-16
2-7-1 コントローラのタスク周期の設定.....	2-16
2-8 否認を防止する.....	2-18
2-8-1 アクセスログ機能.....	2-18

第 3 章 セキュリティパッチを適用する

3-1 NJ/NX コントローラをアップデートする.....	3-2
3-1-1 ファームウェアアップデート禁止機能.....	3-2

3-1-2	ファームウェアアップデート履歴表示	3-2
3-2	Sysmac Studio をアップデートする	3-3
3-3	パソコンの OS をアップデートする	3-4

第 4 章 装置を安全に廃棄する

4-1	NJ/NX コントローラ内の資産を消去する	4-2
4-1-1	データ完全消去機能	4-2
4-2	NJ/NX コントローラを破壊する	4-3

付録

A-1	本書および当社 FA 製品に関するお問い合わせ	A-2
-----	-------------------------------	-----

関連ガイドライン・マニュアル

本書に関連するガイドライン・マニュアルは、下表のとおりです。あわせてお読みください。

文書名称	No.	用途
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。
NJ/NX シリーズ CPU ユニット ユーザーズマニュアル ソフトウェア編	SBCA-467	NJ/NX シリーズ CPU ユニットに搭載しているセキュリティ機能の詳細、使い方を知りたいとき。
Sysmac Studio Version 1 オペレーションマニュアル	SBCA-470	Sysmac Studio に搭載しているセキュリティ機能の詳細、使い方を知りたいとき。
NJ/NX シリーズ CPU ユニット内蔵 EtherNet/IP TM ポート ユーザーズマニュアル	SBCD-377	NJ/NX シリーズ CPU ユニットの内蔵 EtherNet/IP ポートに搭載しているセキュリティ機能の詳細、使い方を知りたいとき。
NJ/NX シリーズ CPU ユニット ユーザーズマニュアル OPC UA 編	SBCD-374	NJ/NX シリーズ CPU ユニットに搭載している OPC UA サーバ機能の詳細、使い方を知りたいとき。
NJ/NX シリーズ データベース接続 CPU ユニット ユーザーズマニュアル	SBCA-411	NJ/NX シリーズ CPU ユニットに搭載しているデータベース接続サービス機能の詳細、使い方を知りたいとき。
NJ/NX シリーズ トラブルシューティング マニュアル	SBCA-469	NJ/NX シリーズ CPU ユニットに登録するアクセスログについて知りたいとき。

改訂履歴

改訂記号は、表表紙・裏表紙に記載されているカタログ番号の後尾に付記されます。

カタログ番号 **SBCA-142B**

↑ 改訂記号

改訂記号	改訂年月	改訂理由・改訂ページ
A	2025 年 3 月	初版
B	2025 年 7 月	• NJ シリーズ、形 NX502、形 NX102、形 NX1P2 の CPU ユニット Ver.1.69 へのバージョンアップに伴う改訂 • 形 NX701 の CPU ユニット Ver.1.36 へのバージョンアップに伴う改訂

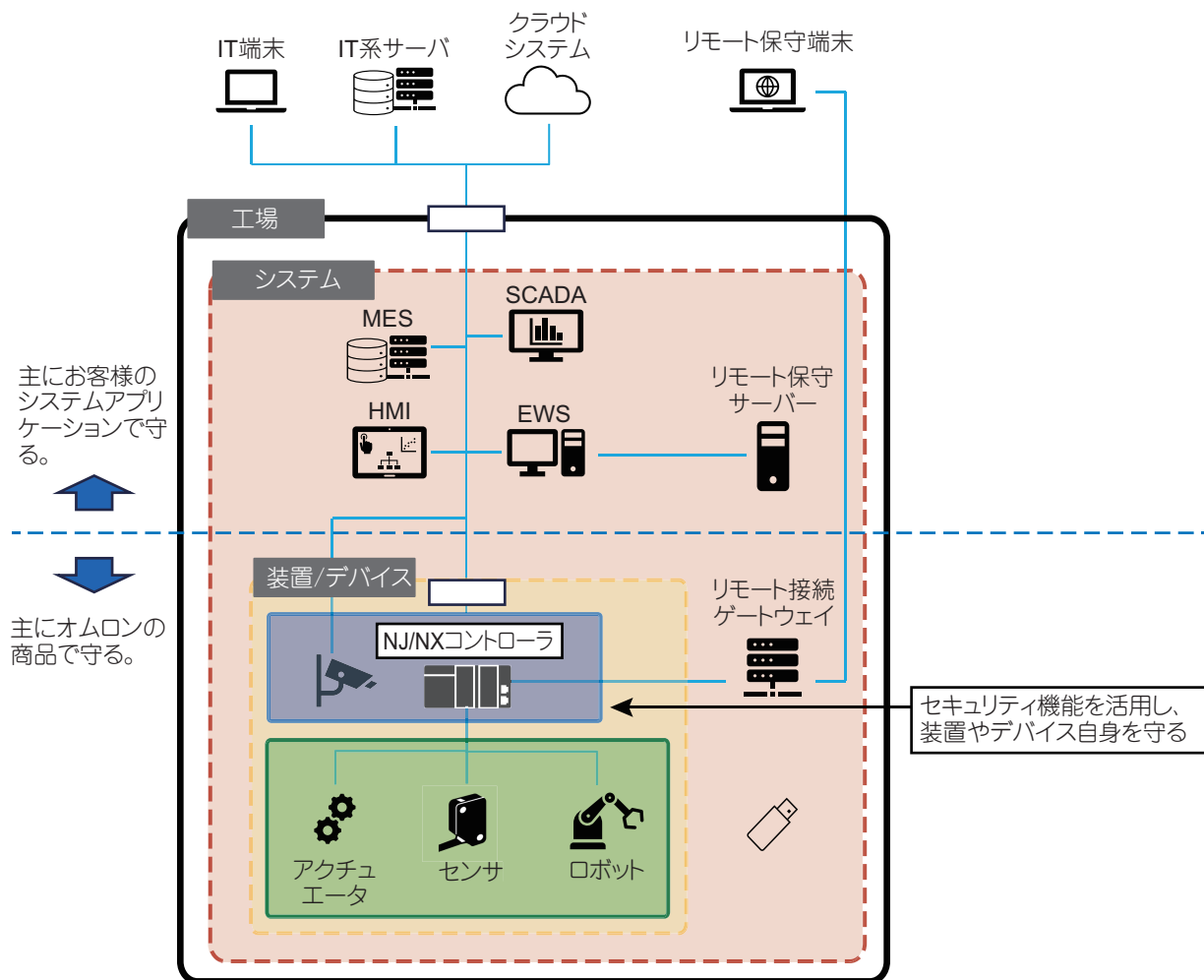
NJ/NX コントローラによる多層防 御

NJ/NX コントローラ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。
本章では、NJ/NX コントローラ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。

1-1	NJ/NX コントローラの使用環境.....	1-2
1-2	NJ/NX コントローラを活用した技術層のセキュリティ対策	1-3

1-1 NJ/NX コントローラの使用環境

NJ/NX コントローラは、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 NJ/NX コントローラの動作や資産を守ります。

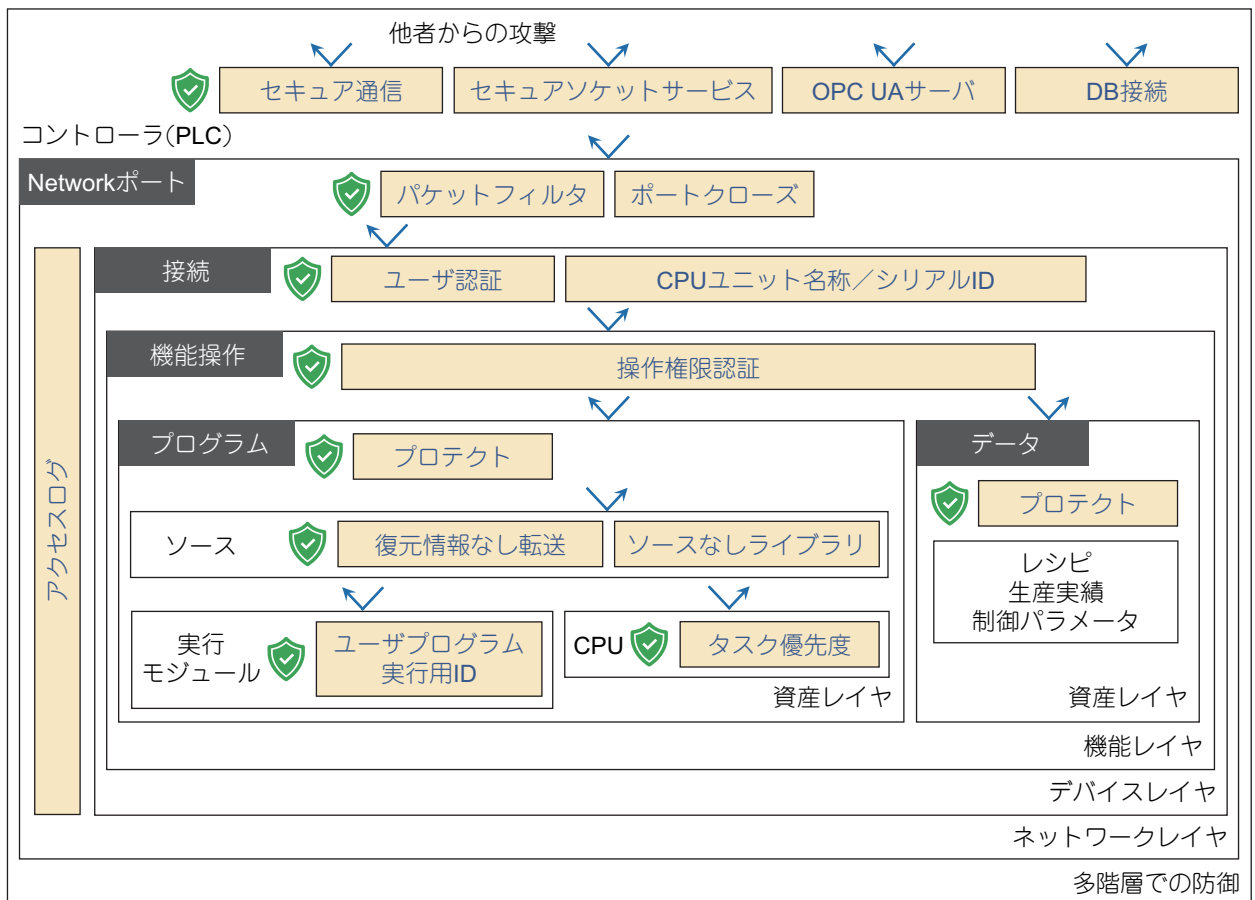


1-2 NJ/NX コントローラを活用した技術層のセキュリティ対策

NJ/NX コントローラ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1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、および本書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、本書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。



各層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	当社製品が搭載している機能	本書参照先
ネットワークレイヤ	通信回線上のデータを保護する	セキュア通信機能	P.2-2
		セキュアソケットサービス機能	P.2-2
		OPC UA サーバ機能	P.2-3
		DB 接続機能	P.2-4
	コントローラへの外部からの攻撃を遮断する	パケットフィルタ機能	P.2-6
		TCP/UDP ポートクローズ機能	P.2-6
デバイスレイヤ	コントローラへの不正接続を防止する	ユーザ認証機能	P.2-8
		CPU ユニット名称、シリアル ID	P.2-9
機能レイヤ	コントローラの不正操作を防止する	操作権限認証機能	P.2-10
資産レイヤ	プログラム・データの流出を防止する	プロジェクトファイルのパスワードプロテクト	P.2-11
		データプロテクト	P.2-11
		ソースなしライブラリ	P.2-12
		ユーザプログラム復元情報なし転送	P.2-12
		CPU ユニットへの書込プロテクト	P.2-12
	プログラムの不正利用を防止する	ユーザプログラム実行用 ID 認証機能	P.2-14
	コントローラの安定動作を保護する	コントローラのタスク周期の設定	P.2-16
レイヤ共通	否認を防止する	アクセスログ機能	P.2-18

資産を守る NJ/NX セキュリティ機能

本章では、NJ/NX コントローラが搭載しているセキュリティ機能について説明します。

2-1	通信回線上のデータを保護する	2-2
2-1-1	セキュア通信機能	2-2
2-1-2	セキュアソケットサービス機能	2-2
2-1-3	OPC UA サーバ機能	2-3
2-1-4	DB 接続機能	2-4
2-2	コントローラへの外部からの攻撃を遮断する	2-6
2-2-1	パケットフィルタ機能	2-6
2-2-2	TCP/UDP ポートクローズ機能	2-6
2-3	コントローラへの不正接続を防止する	2-8
2-3-1	ユーザ認証機能	2-8
2-3-2	CPU ユニット名称、シリアル ID	2-9
2-4	コントローラの不正操作を防止する	2-10
2-4-1	操作権限認証機能	2-10
2-5	プロジェクトファイル・ユーザプログラムを保護する	2-11
2-5-1	プロジェクトファイルのパスワードプロテクト	2-11
2-5-2	データプロテクト	2-11
2-5-3	ソースなしライブラリ	2-12
2-5-4	ユーザプログラム復元情報なし転送	2-12
2-5-5	CPU ユニットへの書き込みプロテクト	2-12
2-6	コントローラの不正利用を防止する	2-14
2-6-1	ユーザプログラム実行用 ID 認証機能	2-14
2-7	コントローラの安定動作を保護する	2-16
2-7-1	コントローラのタスク周期の設定	2-16
2-8	否認を防止する	2-18
2-8-1	アクセスログ機能	2-18

2-1 通信回線上のデータを保護する

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。通信回線を流れるデータからの情報漏洩や改ざん、サービス妨害を防止します。

2-1-1 セキュア通信機能

セキュア通信機能は、Sysmac Studio とコントローラ間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。

セキュア通信の詳細については、『NJ/NX シリーズ CPU ユニット ユーザーズマニュアル ソフトウェア編(SBCA-467)』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: 情報漏洩	D: サービス妨害	E: 権限昇格
○	○		○	○	

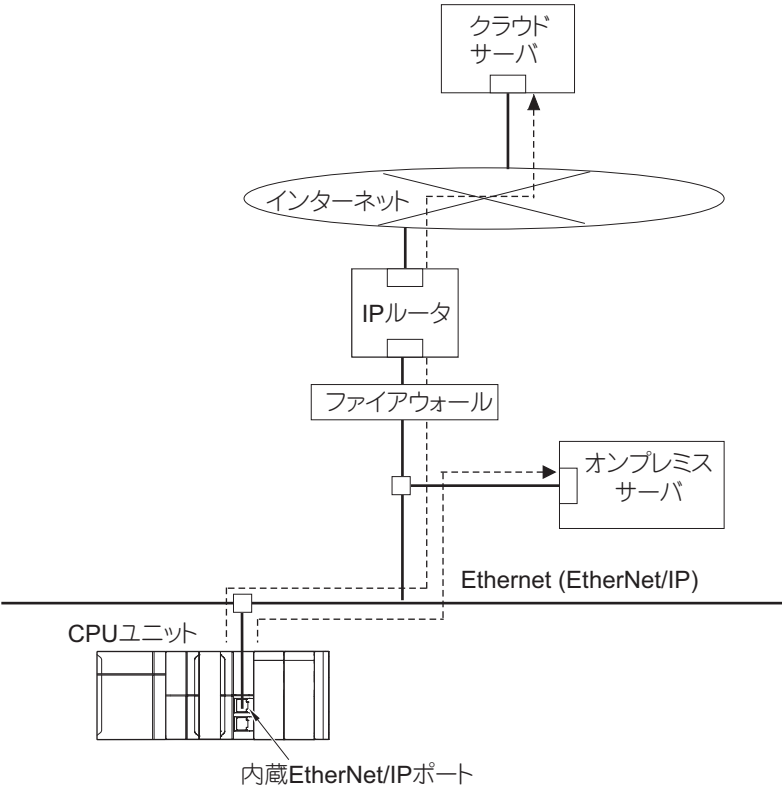
お客様に実施していただきたいこと

- セキュリティ性向上のために、Microsoft Windows サポート期限内の OS に Sysmac Studio をインストールして使用してください。
- セキュア通信機能により、通信応答性能、一部の命令の実行処理性能に影響することがあります。セキュア通信機能に対応した CPU ユニットを使用する場合には、事前に十分な動作確認を行ってください。影響がある場合は「セキュア通信未対応の Sysmac Studio、NA 接続許可」を設定することを検討してください。
- EtherNet/IP の設定をセキュアに行う必要がある場合は Network Configurator ではなく、Sysmac Studio を利用してください。
- SysmacGateway は認証機能をサポートしていません。必要な場合は利用するアプリケーション側で認証機能を実現してください。
- SD カードのファイル転送をセキュアに行う必要がある場合は、FTP クライアントではなく、Sysmac Studio を利用してください。FTP クライアントで転送する必要がある場合は、以下の対策を講じてください。
 - a) 攻撃者が用意した機器とコントローラが通信しないように、セキュリティが確保されたエリアに相手機器を設置する。
 - b) IP フィルタ機能やユーザシステム（ファイアウォールなど）を利用し、接続できる相手先を限定する。
- 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、Sysmac Studio の制御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。
- Sysmac Studio 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。

2-1-2 セキュアソケットサービス機能

セキュアソケットサービス機能では、CPU ユニットの内蔵 EtherNet/IP ポートがクライアントとなり、プライベートのネットワークのオンプレミスサーバや外部ネットワーク上のクラウドサーバと、

セキュアなソケット通信を行うことができます。TLS を用いた暗号化通信で行い、クライアントの秘密鍵、証明書に対応し、安全な通信を確保します。
セキュアソケットサービス機能の詳細については、『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)』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: 情報漏洩	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

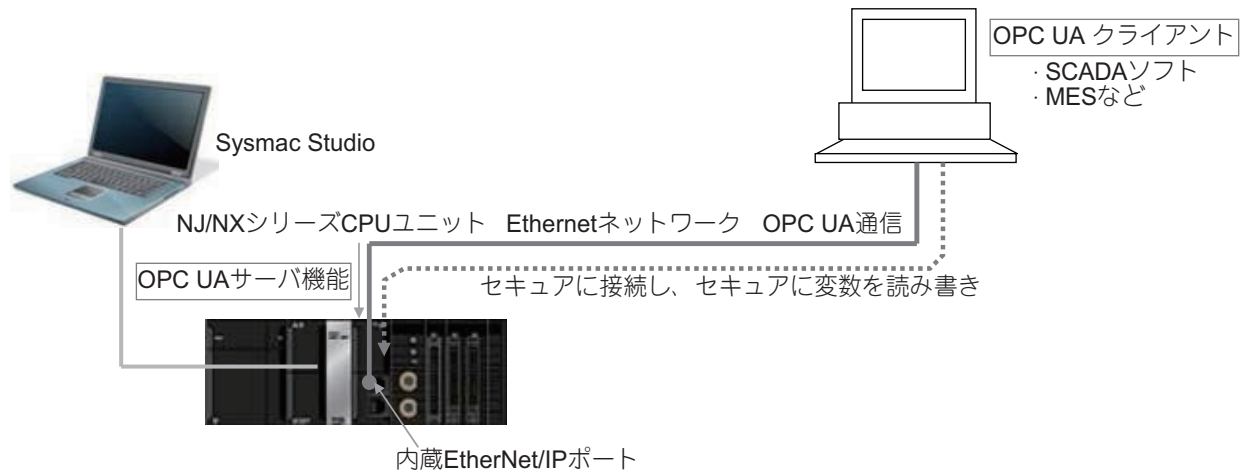
- Network Configurator はセキュア通信を使用していません。セキュリティが担保できないネットワークからの Network Configurator のコントローラ接続は、IP フィルタ機能やユーザシステム（ファイアウォール）などで禁止してください。
- 攻撃者が用意した機器がコントローラと通信しないよう、コントローラに接続する機器は、セキュリティが確保されたエリア内に設置してください。
- 正しい機器と接続していることはユーザアプリケーションで検証してください。

2-1-3 OPC UA サーバ機能

OPC UA サーバ機能は、NJ/NX シリーズ CPU ユニットの「OPC UA サーバ」として動作させる機能です。
この機能により、OPC UA クライアントから、OPC UA サーバ機能としての NJ/NX シリーズ CPU ユニットの、内蔵 EtherNet/IP ポートに Ethernet ネットワークで接続し、OPC UA 通信を使用して、CPU ユニット内の変数を読み書きすることができます。接続方式の汎用性とセキュリティリスク対応を同時に実現した OPC UA 通信をサポートしているため、SCADA、MES などの OPC UA 対応の

上位システムからの製造進捗情報収集、製造指示などを、セキュアにやりとりすることが可能となります。

OPC UA サーバ機能の詳細や使い方は『NJ/NX シリーズ CPU ユニット ユーザーズマニュアル OPC UA 編(SBCD-374)』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: 情報漏洩	D: サービス妨害	E: 権限昇格
○	○		○	○	

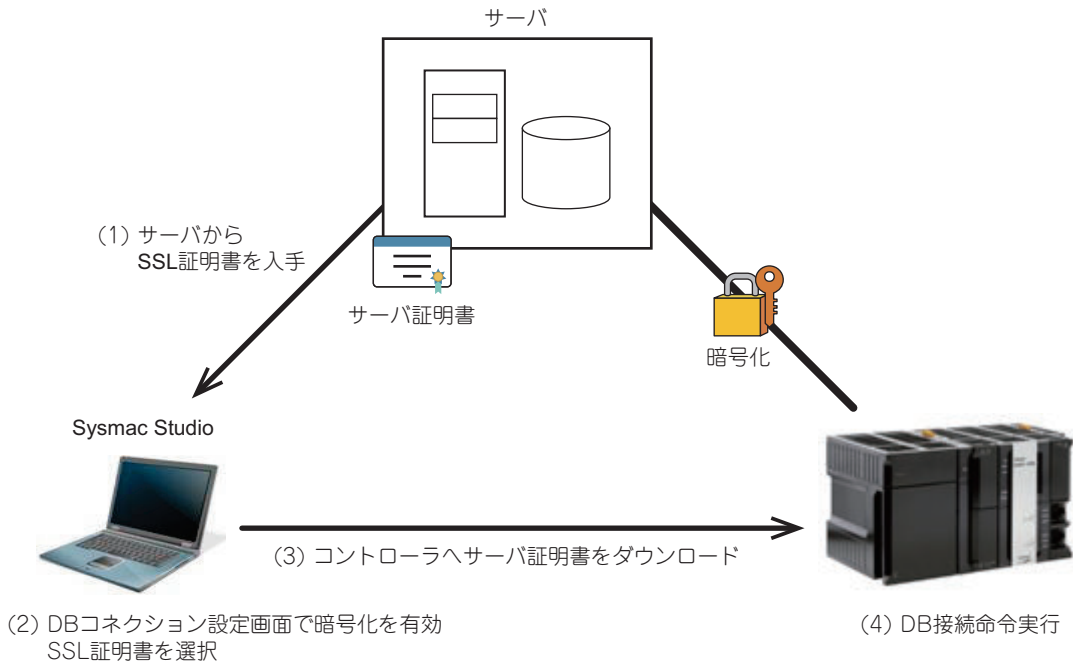
お客様に実施していただきたいこと

- Network Configurator のコントローラへの接続はユーザ認証、クライアント認証、通信暗号に対応していません。セキュアな通信を行う必要がある場合は EtherNet/IP の利用を無効とする設定を行い、代わりに OPC UA を利用してください。
- アプリケーションとの通信で認証が必要な場合は OPC UA を利用してください。または IP フィルタ機能を利用し、接続できる相手先を限定してください。
- クライアント機能を作成する場合、ログインする前に、ユーザに通知を行うよう、実装してください。
- 変数からの情報漏洩を防止するため、ネットワーク公開する変数は必要最低限にしてください。グローバル変数はネットワーク公開しないことを推奨します。公開が必要な場合は、下記対策を実施してください。
 - a) 攻撃者が用意した機器とコントローラが通信しないように、セキュリティが確保されたエリアに相手機器を設置する。
 - b) IP フィルタ機能やユーザシステム（ファイアウォールなど）を利用し、接続できる相手先を限定する。
 - c) EtherNet/IP の利用を無効とする。
- 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。
- 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。

2-1-4 DB 接続機能

DB 接続サービスでは、SSL/TLS 暗号化通信を用いて暗号化通信を行います。

暗号化通信は、コントローラと DB の間の通信データを暗号化することによって、盗聴や改ざんを防止する機能です。暗号化通信は、DB 接続サービスのバージョンが Ver.2.00 以降で、Sysmac Studio の DB コネクション設定を行うことによって使用できます。暗号化通信の設定の詳細については、『NJ/NX シリーズ データベース接続 CPU ユニット ユーザーズ マニュアル(SBCA-411)』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: 情報漏洩	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

- TLS1.2 に対応している DB を使用してください。
- Oracle Database 以外はサーバ認証が行えません。Oracle Database を用いてサーバ認証を行うか、ユーザのアプリケーションで正しいサーバであることを確認するか、または攻撃者が用意したサーバとコントローラが通信しないように、セキュリティが確保されたエリアにサーバを設置してください。

2-2 コントローラ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。

2-2-1 パケットフィルタ機能

内蔵 EtherNet/IP ポートの受信処理にて IP パケットをフィルタリングすることにより、外部機器からのアクセスに対して制限をかける機能です。
Packet Filter 機能は特定のクライアントのみ特定のサーバ機能の使用を許可するなど、より詳細な設定が可能です。
Packet Filter 機能の使い方は『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)』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: 情報漏洩	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

- ・ コントローラのパケットフィルタ機能により送信元（FTP クライアント）の IP アドレス、TCP/UDP ポートを制限することが可能です。
- ・ ファイアウォールを設置してコントローラに不正なパケットが到達しないようにする、使用しないポートをクローズしてコントローラが不正なパケットを受け付けないようにする、など、他の対策と組み合わせて使用してください。

2-2-2 TCP/UDP ポートクローズ機能

コントローラに不正アクセスし、ユーザプログラムなどのデータを盗まれるリスクがあります。リスクを低減するため、未使用のポートをクローズし、不正アクセスを防止します。
NJ/NX コントローラでは、内蔵 EtherNet/IP ポートに搭載しているサーバ機能が使用する TCP/UDP ポートをクローズすることができます。これにより、ユーザのシステムで使用する TCP/UDP ポートのみをオープンすることができます。
内蔵 EtherNet/IP ポートに搭載しているサーバ機能の詳細は、『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)』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: 情報漏洩	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

- ・ 通信の完全性を検証する必要がある場合は、TCP 通信を利用してください。

- FINS プロトコル仕様では、暗号化通信を規定していません。よって、通信経路上の FINS メッセージは平文で送受信されるため、容易に傍受することができます。また、FINS メッセージの改ざんを検知することができません。FINS プロトコルの脆弱性の悪用リスクを抑えるため、FINS を無効化する、パケットフィルタ機能などを用いて不正アクセスを防止するなどの対策を講じてください。FINS 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。
- SNMP 機能は、利用しない場合は無効化することができますが、認証用にコミュニティ名を指定したり、IP フィルタを利用したりすることで、相手を限定して通信することもできます。
- 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。
FTP はパスワードロック機能を有していません。パスワードロック機能が必須の場合、FTP 機能を無効化してください。
- 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。
- ファイアウォールを設置してコントローラに不正なパケットが到達しないようにする、パケットフィルタを使用してコントローラが不正なパケットを受け付けないようにする、など、他の対策と組み合わせて使用してください。

2-3 コントローラへの不正接続を防止する

お客様の大切な知的財産であるユーザプログラムや装置を盗用や不正利用から守るため、容易にコントローラにアクセスできないようにコントローラ接続時に認証する機能を使用します。

2-3-1 ユーザ認証機能

オンライン接続時にユーザ名とパスワードによるユーザ認証を行い、オンライン操作するユーザを特定します。

ユーザ認証機能は、コントローラを操作するユーザをあらかじめコントローラに登録しておき、コントローラをオンライン操作するユーザを特定する機能です。コントローラにオンライン接続する際に、ユーザ名とパスワードの入力が要求されます。ユーザ名およびパスワードがあらかじめ設定されたものと一致しないと、オンライン接続することができません。

さらに、各ユーザには、管理者、設計者、保全者、操作者、または観察者のいずれかの操作権限を割り当てます。これにより、各ユーザが自分に割り当てられた権限範囲でしかコントローラへのオンライン操作ができないようにします。

ユーザ名、パスワード、およびそのユーザの操作権限の情報などのユーザ認証設定は、コントローラに保存されます。したがって、別のパソコンからコントローラに接続しても、ユーザ認証機能を使用することができます。

ユーザ認証設定は、プロジェクトには保存されません。ユーザ認証機能を使用するコントローラごとに、ユーザ認証設定を行います。

対策できる脅威

S: なりすまし	T: 改ざん	R: 否認	I: 情報漏洩	D: サービス妨害	E: 権限昇格
○	○	○	○	○	○

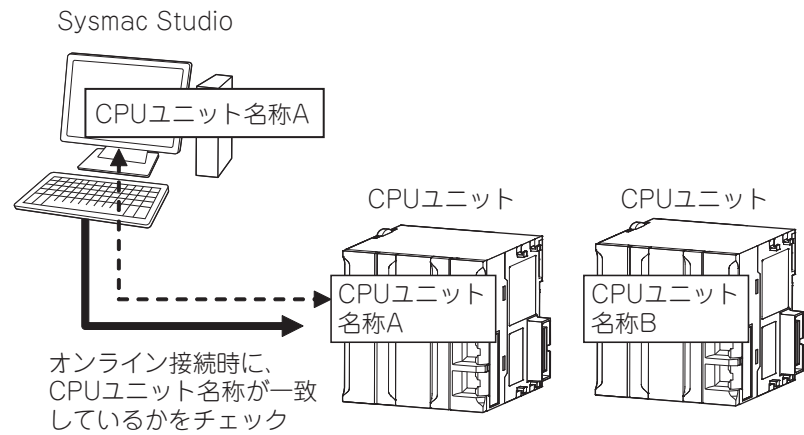
ユーザ認証機能では Sysmac Studio を CPU ユニットにオンライン接続する際にユーザ名とパスワードを入力すると、割り当てられている権限範囲で操作できるようになります。操作方法の詳細は、『Sysmac Studio Version 1 オペレーションマニュアル(SBCA-470)』を参照してください。

お客様に実施していただきたいこと

- ・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。
- ・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。
- ・SysmacStudio のコントローラとのオンライン接続や OPC UA サーバ機能ではユーザ認証をサポートしていますので、この機能を使用してください。それ以外の通信では認証機能をサポートしていませんので、必要のない通信は利用しない（無効にする）ようにしてください。必要な場合は利用するアプリケーション側で認証機能を実現してください。たとえば、ユーザ認証をサポートしている機器を利用する、SysmacGateway/Compolet などを使いアプリケーションで認証機能を実現する、などが挙げられます。アプリケーションで認証機能を実現する場合は、以下に注意してください。
 - a) パスワードはシステムで固定値とならないよう、デフォルトの値は必ず変更するなどの対応を行ってください。
 - b) パスワードなどを定期的に更新するような仕組みの提供を検討してください。
 - c) パスワードなどの漏洩を防ぐ対策を行ってください。

2-3-2 CPU ユニット名称、シリアル ID

Sysmac Studio からのオンライン接続時に、プロジェクト上の CPU ユニット名称と接続先 CPU ユニットの CPU ユニット名称が一致しているかどうかを確認できます。
これにより、Sysmac Studio から誤った CPU ユニットへの接続を防止することができます。特に、EtherNet/IP ネットワークを介した操作のときに有効です。



さらに、CPU ユニット名称以外に、CPU ユニットの生産情報にもとづくシリアル ID を識別することもできます（オプション）。

対策できる脅威

S: なりすまし	T: 改ざん	R: 否認	I: 情報漏洩	D: サービス妨害	E: 権限昇格
	○		○	○	○

CPU ユニット名称、シリアル ID の使い方は、『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。

2-4 コントローラの不正操作を防止する

コントローラの不正操作を防止し、お客様の大切な知的財産であるユーザプログラムや装置を盗用や不正利用、生産装置の異常や事故から守ります。

2-4-1 操作権限認証機能

コントローラのデータを変更する場合、操作ミスにより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、操作ミスを防止します。

操作権限認証機能を用いて、管理者が操作権限ごとにパスワードを設定し、スキルに応じて操作権限名とパスワードを使用者に連絡することで運用します。

対策できる脅威

S: なりすまし	T: 改ざん	R: 否認	I: 情報漏洩	D: サービス妨害	E: 権限昇格
	○		○	○	○

操作権限認証機能の設定は『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。

お客様に実施していただきたいこと

- 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。
- 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。

2-5 プロジェクトファイル・ユーザプログラムを保護する

お客様の大切な知的財産であるプロジェクトファイル・ユーザプログラムの盗用や不正利用を防止します。複数の防御策を講じておくことで、1つの防御策が破られたとしても、次の防御策で被害拡大を食い止めることができます。複数の機能を組み合わせて使用してください。

2-5-1 プロジェクトファイルのパスワードプロテクト

プロジェクトファイルに含まれるユーザプログラムや設定の閲覧や改ざんを防止するため、プロジェクトファイル全体にパスワードプロテクトをかけます。

使用方法是『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。

対策できる脅威

S: なりすまし	T: 改ざん	R: 否認	I: 情報漏洩	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、Microsoft Windows サポート期限内の OS に Sysmac Studio をインストールして使用してください。
- ・設定するパスワードが他人から不正に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。
- ・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。

2-5-2 データプロテクト

複数人で設計、保守する場合など、プロジェクトファイルに含まれるデータの一部だけをプロテクトしたい場合に使用します。データ単位でパスワードを設定し、表示や変更、複製を禁止（アクセス制限）します。

使用方法是『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。

対策できる脅威

S: なりすまし	T: 改ざん	R: 否認	I: 情報漏洩	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、Microsoft Windows サポート期限内の OS に Sysmac Studio をインストールして使用してください。
- ・設定するパスワードが他人から不正に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。
- ・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。

2-5-3 ソースなしライブラリ

悪意を持った攻撃者がプロジェクトファイル内のユーザプログラムにアクセスできないよう、ユーザプログラムの復元情報（ソース）を含まないライブラリファイル（ソースなしライブラリ）を作成します。プロジェクトからソースなしライブラリを参照することで、保護したいソースコードを含まないプロジェクトファイルを作ることができます。

使用方法是『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。

対策できる脅威

S: なりすまし	T: 改ざん	R: 否認	I: 情報漏洩	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、Microsoft Windows サポート期限内の OS に Sysmac Studio をインストールして使用してください。
- ・攻撃者が保守端末パソコンからプロジェクトファイルを盗用できないよう、保守端末パソコンへのアカウント設定やセキュリティが確保されたエリアに設置してください。

2-5-4 ユーザプログラム復元情報なし転送

ユーザプログラムを他のパソコンでアップロードしたときに、ユーザプログラムを表示できないよう、CPU ユニットにプログラムの復元情報（ソース）を転送しません。現場でユーザプログラムを保守することがなく、かつユーザプログラムデータの盗用を防止したいときに使用します。

ユーザプログラム復元情報なし転送機能については、『NJ/NX シリーズ CPU ユニット ユーザーズマニュアル ソフトウェア編(SBCA-467)』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: 情報漏洩	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、Microsoft Windows サポート期限内の OS に Sysmac Studio をインストールして使用してください。

2-5-5 CPU ユニットへの書込プロテクト

CPU ユニット内のデータを Sysmac Studio から書き換えできないよう、プロテクトします。

使用方法是『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。

対策できる脅威

S: なりすまし	T: 改ざん	R: 否認	I: 情報漏洩	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

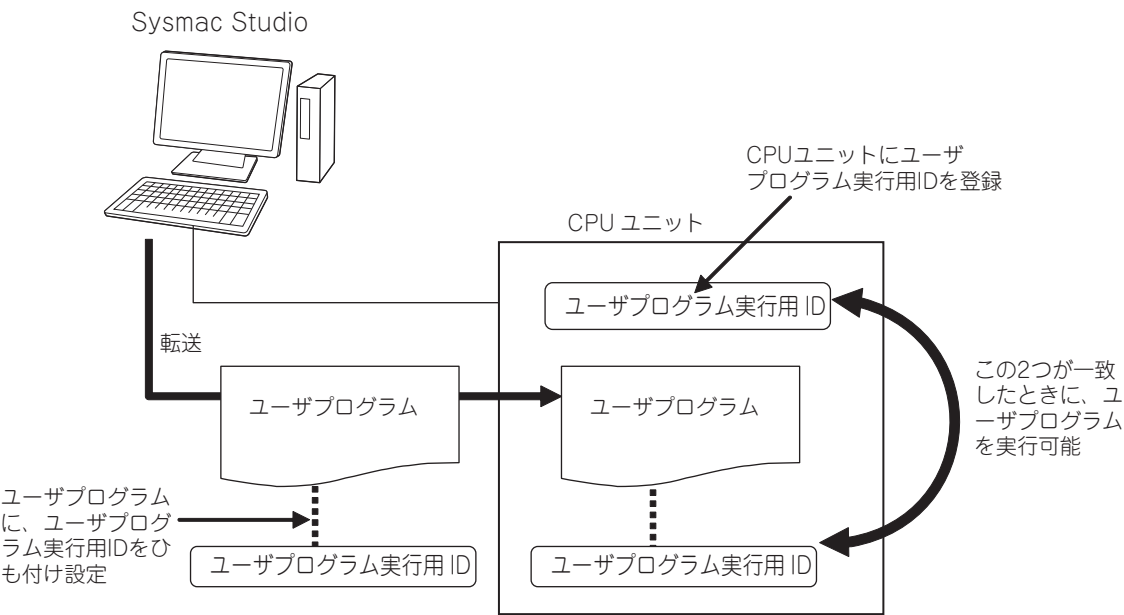
- セキュリティ性向上のために、Microsoft Windows サポート期限内の OS に Sysmac Studio をインストールして使用してください。

2-6 コントローラの不正利用を防止する

お客様の大切な知的財産であるユーザプログラムや装置を盗用や不正利用から守ります。

2-6-1 ユーザプログラム実行用 ID 認証機能

ユーザプログラムが盗難されたとしても、そのユーザプログラムの実行を防止し、不正利用から守ります。
あらかじめコントローラに特定の ID（「ユーザプログラム実行用 ID」と呼ぶ）を入力しておき、それと同じ ID を紐付け設定したユーザプログラムのみを実行可能とすることができます。



この機能により、

- あるコントローラは、特定のユーザプログラムしか実行できないように制限することができます。
- あるユーザプログラムを、異なるコントローラ（ハードウェア）では使用できないようにすることができます。

なお、本機能は、プロテクト機能とは異なり、ユーザプログラムの表示・編集は可能です。
ユーザプログラム実行用 ID の詳細については、『NJ/NX シリーズ CPU ユニット ユーザーズマニュアル ソフトウェア編(SBCA-467)』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: 情報漏洩	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、Microsoft Windows サポート期限内の OS に Sysmac Studio をインストールして使用してください。
- 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、Sysmac Studio の制御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。

- Sysmac Studio 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。

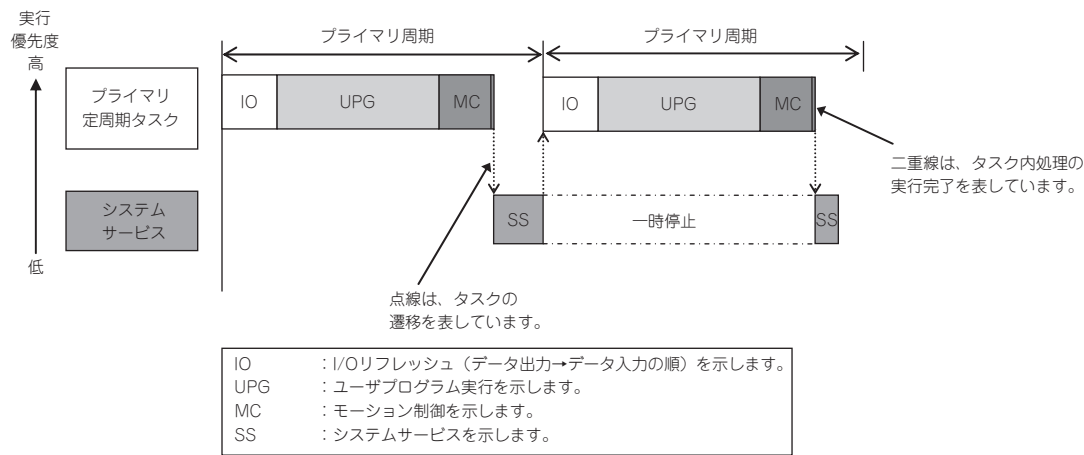
2-7 コントローラの安定動作を保護する

悪意を持った第三者やウイルス感染した生産パソコンから、DOS 攻撃などを用いてコントローラに対し過剰な制御・通信負荷を発生させた場合、コントローラの制御処理や通信処理で遅延が発生し、設備に動作遅延や異常停止が発生する可能性があります。これによる生産タクトタイムの遅延や生産停止、設備や人への危害、生産する製品の品質低下などを防止します。

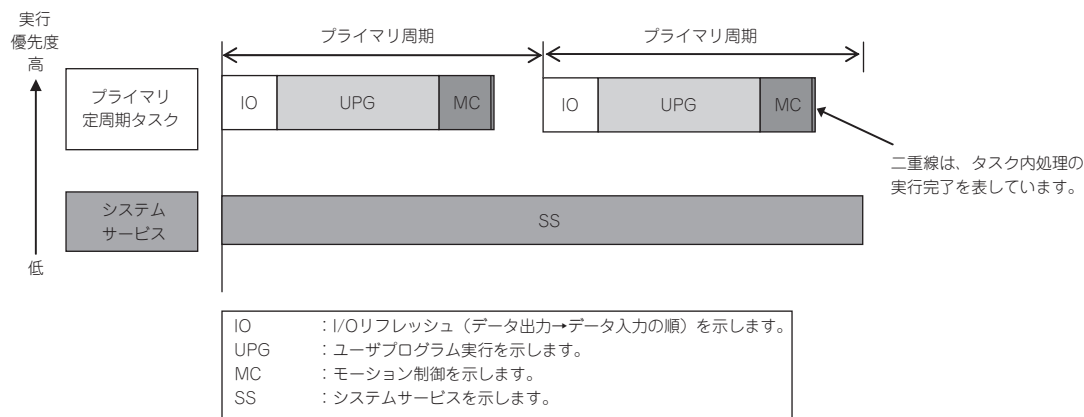
2-7-1 コントローラのタスク周期の設定

NJ/NX コントローラはマルチコア CPU の採用やタスクの優先度管理により、外部からの通信などによる DoS 攻撃が発生しても制御周期に影響しません。制御周期を確実に守る必要があるタスクは優先度を高くするような設計をすることで、生産設備の制御を守ることができます。

NJ コントローラではタスク優先度管理により、システムサービスはタスク実行の空き時間に実行されます。DoS 攻撃が発生しても、制御用のタスクは影響を受けず、制御周期に影響しません。



NX コントローラではマルチコア CPU を搭載しており、タスク実行とシステムサービスを並列に実行します。DoS 攻撃が発生しても、制御用のタスクは実影響を受けず、制御周期に影響しません。



タスクのしくみや種類については『NJ/NX シリーズ CPU ユニット ユーザーズマニュアル ソフトウェア編(SBCA-467)』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: 情報漏洩	D: サービス妨害	E: 権限昇格
				○	

2-8 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。

2-8-1 アクセスログ機能

NJ/NX コントローラでは、コントローラに対してユーザがツールを使用して行ったオンライン操作をアクセスログとして登録します。また、ユーザ認証機能を使用している場合はセキュリティ上重要となるアクセスログにはユーザ名を記録します。
登録するアクセスログは、『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。

対策できる脅威					
S: なりすまし	T: 改ざん	R: 否認	I: 情報漏洩	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

- ログが消去されると否認防止できません。NJ/NX コントローラのアクセスログは、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。

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。

本章では、アップデートに関し、NJ/NX コントローラが搭載している機能について説明します。

3-1	NJ/NX コントローラをアップデートする	3-2
3-1-1	ファームウェアアップデート禁止機能	3-2
3-1-2	ファームウェアアップデート履歴表示	3-2
3-2	Sysmac Studio をアップデートする	3-3
3-3	パソコンの OS をアップデートする	3-4

3-1 NJ/NX コントローラ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、NJ/NX コントローラは、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についての詳細は、当社営業担当者まで問い合わせてください。

3-1-1 ファームウェアアップデート禁止機能

悪意を持った第三者が不正に機器を更新しないよう、NJ/NX コントローラのアップデートを禁止します。
Sysmac Studio で、ファームウェアアップデートを禁止する／しないを設定します。設定方法の詳細は、『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。

対策できる脅威

S: なりすまし	T: 改ざん	R: 否認	I: 情報漏洩	D: サービス妨害	E: 権限昇格
	○			○	

3-1-2 ファームウェアアップデート履歴表示

NJ/NX コントローラのファームウェアのアップデート履歴を表示します。
ファームウェアアップデート履歴の表示については、『NJ/NX シリーズ CPU ユニット ユーザーズマニュアル ソフトウェア編(SBCA-467)』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: 情報漏洩	D: サービス妨害	E: 権限昇格
		○			

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、本ソフトウェアは、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。

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。

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 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。

4

装置を安全に廃棄する

本章では、廃棄に関し、NJ/NX コントローラが搭載している機能について説明します。

4

4-1	NJ/NX コントローラ内の資産を消去する	4-2
4-1-1	データ完全消去機能	4-2
4-2	NJ/NX コントローラを破壊する	4-3

4-1 NJ/NX コントローラ内の資産を消去する

当社商品を廃棄、または譲渡する場合、機器に保存しているユーザデータなどの情報を第三者に見られて、情報が漏洩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ユーザデータを消去してください。

4-1-1 データ完全消去機能

ユーザデータを完全消去するためのデータ完全消去機能は、CPU ユニット内の、ユーザが設定したデータを完全に消去する機能です。

メモリオールクリア機能では、メモリ内のデータは完全に消去されないため、データを復元される可能性があります。しかし、データ完全消去機能は、メモリオールクリア後にユーザプログラムと各種設定を保存する内蔵不揮発性メモリの未使用の領域に、ランダムなデータを書き込むことにより、データの復元を防止します。

データ完全消去機能の詳細は、『NJ/NX シリーズ CPU ユニット ユーザーズマニュアル ソフトウェア編(SBCA-467)』を参照してください。

4-2 NJ/NX コントローラを破壊する

NJ/NX コントローラを廃棄する際には、製品内のユーザデータの漏洩を防ぐため、データ完全消去機能を用いて、ユーザデータを消去してください。データ消去に失敗する場合は、NJ/NX コントローラの故障が考えられますので、物理的、電氣的な破壊を推奨します。破壊方法については、当社営業担当者にご相談ください。



付録

A-1	本書および当社 FA 製品に関するお問い合わせ	A-2
-----	-------------------------------	-----

A

A-1 本書および当社 FA 製品に関するお問い合わせ

本書や当社 FA 製品に関するお問い合わせは、以下リンク先の最寄りの当社支店・営業所までご連絡ください。

日本国内のお問い合わせ先

<https://www.fa.omron.co.jp/sales/local/ocShoplist/>

海外でのお問い合わせ先

<https://www.fa.omron.co.jp/sales/global/>

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



0120-919-066

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)

クイック

オムロン



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ください。緊急時のご購入にもご利用ください。

www.fa.omron.co.jp

本誌には主に機種のご選定に必要な内容を掲載しており、ご使用上の注意事項等を掲載していない製品も含まれています。

本誌に注意事項等の掲載のない製品につきましては、ユーザーズマニュアル掲載のご使用上の注意事項等、ご使用の際に必要な内容を必ずお読みください。

- 本誌に記載の標準価格はあくまで参考であり、確定されたユーザ購入価格を表示したものではありません。本誌に記載の標準価格には消費税が含まれておりません。
- 本誌にオープン価格の記載がある商品については、標準価格を決めていません。
- 本誌に記載されているアプリケーション事例は参考用ですので、ご採用に際しては機器・装置の機能や安全性をご確認の上、ご使用ください。
- 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。
- 規格認証/適合対象機種などの最新情報につきましては、当社Webサイト(www.fa.omron.co.jp)の「規格認証/適合」をご覧ください。

オムロン商品のご用命は

カタログ番号 SBCA-142B

2025年7月現在

©OMRON Corporation 2025 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