

DX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

- 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。
 - ODVA, CIP, CompoNet, DeviceNet, EtherNet/IP はODVA の商標です。
 - SpeedBee Synapseは株式会社ソルティスターの商標です。
 - GrafanaはGrafana Labs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、<https://www.fa.omron.co.jp/product/tool/dx-info/index.html> 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、DX シリーズ データフローコントローラ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。

- ・ 生産現場のデータ活用システムを設計、運用される方
- ・ 生産現場の保全システムを設計、運用される方

対象となる製品

本書は以下の製品を対象にしています。

- ・ DX シリーズ データフローコントローラ（以降、「DX コントローラ」と記載します。）

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	DXコントローラのセキュリティ対策	2
2	DXコントローラのセキュリティ機能	3
3	セキュリティパッチを適用する	4
4	機器を安全に廃棄する	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 DX コントローラのセキュリティ対策

1-1 DX コントローラの使用環境.....	1-2
1-2 DX コントローラの技術層のセキュリティ対策.....	1-3

第 2 章 DX コントローラのセキュリティ機能

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
2-2 DX コントローラへの不正接続を防止する.....	2-4
2-2-1 アカウント管理（ユーザ認証）機能（DX コントローラ）.....	2-4
2-2-2 USB ポート管理機能.....	2-4
2-3 DX コントローラの不正操作を防止する.....	2-6
2-3-1 アカウント管理（操作権限認証）機能（DX コントローラ）.....	2-6
2-4 アプリケーションへの不正接続を防止する.....	2-7
2-4-1 アカウント管理（ユーザ認証）機能（アプリケーション）.....	2-7
2-5 アプリケーションの不正操作を防止する.....	2-8
2-5-1 操作権限認証機能（アプリケーション）.....	2-8
2-6 否認を防止する.....	2-9
2-6-1 ログ機能.....	2-9

第 3 章 セキュリティパッチを適用する

3-1 DX 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の履歴.....	3-2
3-2 パソコンの OS をアップデートする.....	3-3
3-3 ブラウザをアップデートする.....	3-4

第 4 章 機器を安全に廃棄する

4-1 DX コントローラ内のデータを消去する.....	4-2
4-1-1 初期化（ファクトリーリセット）機能.....	4-2

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。
DX シリーズ データフローコントローラ ユーザーズマニュアル	SBSB-538	DX シリーズ データフローコントローラに搭載しているセキュリティ機能と使い方を知りたいとき。
DX シリーズ Web UI 操作マニュアル	SBSB-539	DX シリーズ データフローコントローラに搭載しているセキュリティ機能の設定方法を知りたいとき。

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	SBSB-030A
--------	------------------

↑ 改訂記号

改訂記号	改訂年月	改訂理由・改訂ページ
A	2025 年 9 月	初版

DX コントローラのセキュリティ対策

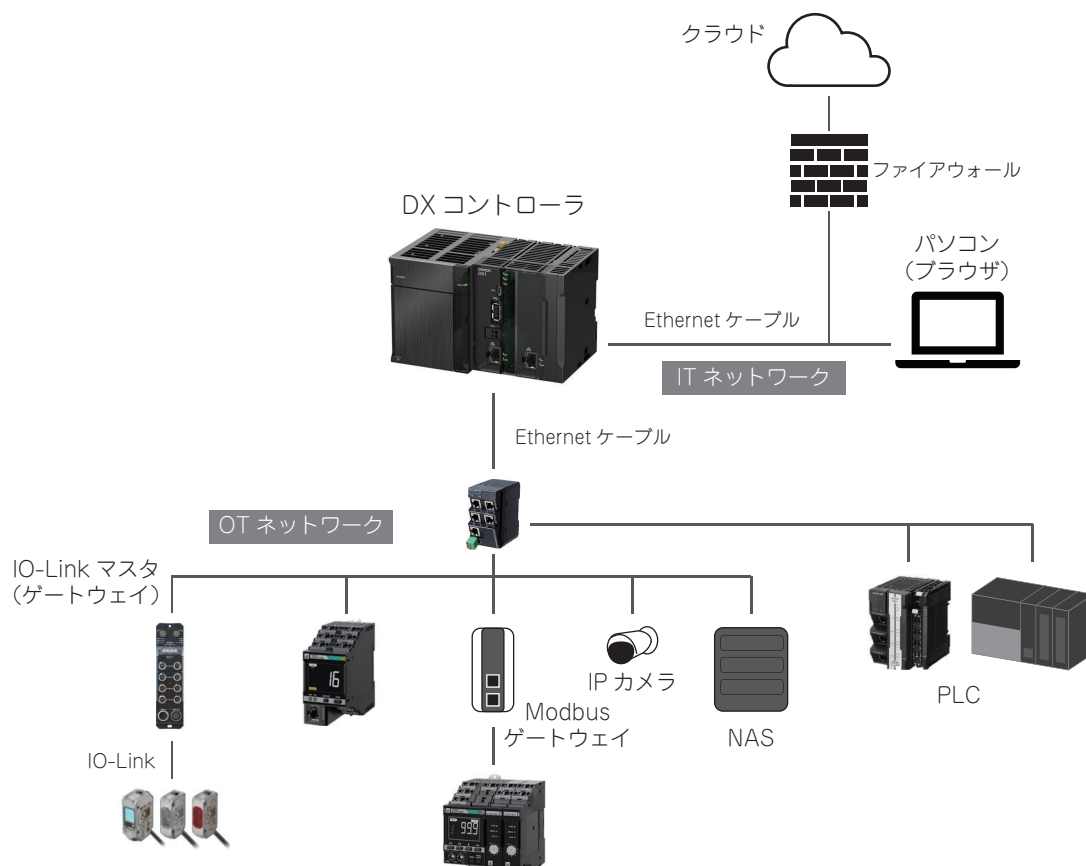
DX コントローラは複数のセキュリティ機能により、多層防御を実現します。
本章では、DX コントローラを使用する環境と DX コントローラのセキュリティについて説明します。

1-1	DX コントローラの使用環境.....	1-2
1-2	DX コントローラの技術層のセキュリティ対策.....	1-3

1-1 DX コントローラの使用環境

DX コントローラは、そのセキュリティ機能を活用することにより、システムや装置のセキュリティを維持したままデータの収集や可視化の機能を追加できます。DX コントローラでは、装置やデバイスから収集したデータを守るために不正接続や不正操作を防止します。

DX コントローラを使用する環境では、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)』に示す対策を組み合わせ、多層防御を講じてください。

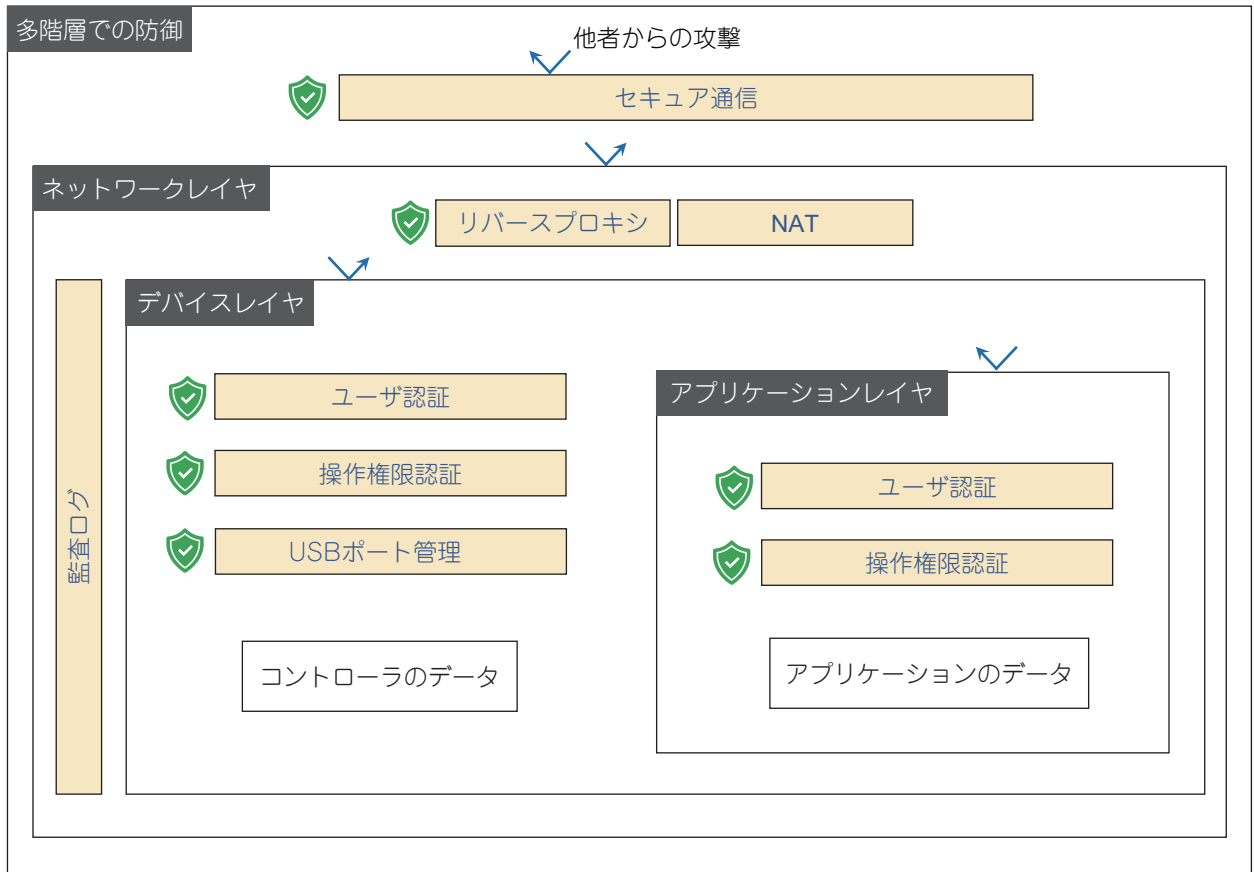


お客様に実施していただきたいこと

- 装置やデバイスのネットワークはファイアウォールやパケットフィルタリングを導入してください。
- IT ネットワーク（パソコン、サーバ、MES などのネットワーク）と OT ネットワーク（装置、デバイスのネットワーク）は分離してください。
- 以下を使用する場合は、それらを安全に使用できるネットワーク環境で運用してください。
NTP, DNS, mDNS, DHCP
- 装置やデバイス自身のセキュリティ機能を有効に活用してください。
- セキュアな運用を行うために、システムや装置／デバイス、および DX コントローラの設置区画への入退室管理や物理的施錠を行ってください。

1-2 DX コントローラの技術層のセキュリティ対策

DX コントローラは守るべきデータに対し、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。攻撃者からの不正接続や不正操作を防止することでデータを守ることができます。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。

お客様にて設定や作業をしていただきたい機能については 2 章で説明していますので参照してください。

データを守るレイヤ	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
	DX コントローラへの外部からの攻撃を遮断する	リバースプロキシ • アプリケーションの Web サーバの IP アドレスを外部から隠蔽し、外部から直接アプリケーションにアクセスすることを防ぎます。	—
		NAT • データフローコントローラ内の IP アドレスを外部から隠蔽し、外部からの攻撃を防ぎます。	—
デバイスレイヤ	DX コントローラへの不正接続を防止する	アカウント管理（ユーザ認証）機能（DX コントローラ）	P.2-4
		USB ポート管理機能	P.2-4
	DX コントローラの不正操作を防止する	アカウント管理（操作権限認証）機能（DX コントローラ）	P.2-6
アプリケーションレイヤ	アプリケーションへの不正接続を防止する	アカウント管理（ユーザ認証）機能（アプリケーション）	P.2-7
	アプリケーションの不正操作を防止する	アカウント管理（操作権限認証）機能（アプリケーション）	P.2-8
レイヤ共通	否認を防止する	監査ログ機能	P.2-9

2

DX コントローラのセキュリティ機能

2

本章では、DX 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
2-2	DX コントローラへの不正接続を防止する	2-4
2-2-1	アカウント管理（ユーザ認証）機能（DX コントローラ）	2-4
2-2-2	USB ポート管理機能	2-4
2-3	DX コントローラの不正操作を防止する	2-6
2-3-1	アカウント管理（操作権限認証）機能（DX コントローラ）	2-6
2-4	アプリケーションへの不正接続を防止する	2-7
2-4-1	アカウント管理（ユーザ認証）機能（アプリケーション）	2-7
2-5	アプリケーションの不正操作を防止する	2-8
2-5-1	操作権限認証機能（アプリケーション）	2-8
2-6	否認を防止する	2-9
2-6-1	ログ機能	2-9

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。通信回線を通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

セキュア通信は DX コントローラと、その他の機器やシステムとの間の通信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。

DX コントローラは、以下の機器との間でセキュア通信を利用できます。

- ブラウザ（パソコン）
- 他の DX コントローラ

ブラウザ（パソコン）との間のセキュア通信を設定する手順については、『DX シリーズ CPU ユニット ユーザーズマニュアル(SBSB-538)』を参照してください。

なお、設定が以下となっていれば、ブラウザ（パソコン）との間のセキュア通信ができます。

- 証明書と鍵が登録されており、それぞれで「有効/無効」が「有効」、[ステータス] が「Available」となっている。
- [TLS 設定] で「TLS を有効にする」にチェックが入っている。

The first screenshot shows the '証明書&鍵管理' (Certificates & Keys Management) page. It has a tab for '証明書' (Certificates) which is highlighted. Below the tab is a table with columns: 証明書名 (Certificate Name), 有効/無効 (Valid/Invalid), 作成方法 (Creation Method), タイプ (Type), アルゴリズムの種類 (Algorithm Type), 証明書の長さ (Certificate Length), ステータス (Status), and 操作 (Action). The table contains one entry: dxc-dx1.crt, Valid, Import, Public, sha512WithRSAEncryption, 2057, Available, and a menu icon.

The second screenshot shows the '証明書&鍵管理' (Certificates & Keys Management) page. It has a tab for '鍵' (Keys) which is highlighted. Below the tab is a table with columns: 鍵名 (Key Name), 有効/無効 (Valid/Invalid), 作成方法 (Creation Method), タイプ (Type), アルゴリズムの種類 (Algorithm Type), 鍵の長さ (Key Length), ステータス (Status), and 操作 (Action). The table contains one entry: dxc-dx1.key, Valid, Import, Public, RSA, 3272, Available, and a menu icon.

The third screenshot shows the 'リバースプロキシ設定' (Reverse Proxy Settings) page. It has a section for 'TLS設定' (TLS Settings) with two radio buttons: 'TLSを有効にする' (Enable TLS) which is selected, and 'TLSを無効にする' (Disable TLS). There is an '適用' (Apply) button at the bottom right.

DX コントローラ同士の間でセキュア通信を設定する手順については、『DX シリーズ ユーザーズマニュアル（工場監視パッケージ編）(SGTE-731)』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、サポート期限内の OS のパソコンやデバイス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、パソコンの DX コントローラ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。
- NTP、DHCP、DNS のサーバは信用できる内部ネットワーク内に配置し、サーバのセキュリティ対策を講じてください。
- アプリケーションの機能を用いて他の機器と通信を行うときに、暗号化通信の設定がある場合は暗号化通信を使用することを推奨します。

たとえば、SpeedBee Synapse のコンポーネントの中には、暗号化通信を設定できるものがあります。コンポーネントについては、『DX シリーズ SpeedBee Synapse ユーザーズマニュアル (SBSB-540)』を参照してください。暗号化通信が可能なコンポーネントについては暗号化機能が説明されています。

暗号化通信ができない場合は、セキュアな運用を行うために、システムや装置／デバイス、および DX コントローラの設置区画への入退室管理や物理的施錠を行ってください。

- セキュア通信に関するサーバ証明書／秘密鍵の第三者による盗難、情報漏えい、改ざんにより、データの不正取得、データの改ざん、通信不可などセキュリティ上の問題になる可能性があります。お客様自身で、証明書、秘密鍵の管理と、盗難、情報漏えい、改ざん防止対策の十分な措置を講じてください。特に、秘密鍵を取得する場合には暗号化された安全な通信経路を使用するなど情報漏えいしないようにしてください。また、秘密鍵の管理では流出する可能性を極力排除した場所に保管するなどしてください。

2-2 DX コントローラへの不正接続を防止する

お客様の大切な生産情報データを盗用や不正利用から守るため、容易に DX コントローラにアクセスできないように DX コントローラ接続時に認証する機能を使用します。

2-2-1 アカウント管理（ユーザ認証）機能（DX コントローラ）

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、DX コントローラを操作するユーザをあらかじめ DX コントローラに登録しておき、DX 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。DX 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、または保全者のいずれかのロールを割り当てます。これにより、各ユーザが自分に割り当てられたロールの権限範囲でしか DX 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ロールの情報などのユーザ認証設定は、DX 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 DX 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。

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パソコンから DX コントローラの Web UI 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ロールの権限範囲で DX コントローラを操作できるようになります。操作方法の詳細は、『DX シリーズ Web UI 操作マニュアル(SBSB-539)』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

- ・ 初期登録されているユーザアカウントは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。
- ・ 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。
- ・ DX コントローラでは、外部システムから DX コントローラにアクセスするためのユーザ毎のアクセストークン（認証キー）を生成できます。アクセストークンは第三者に知られないように厳重に管理してください。

2-2-2 USB ポート管理機能

DX コントローラの USB ポートを使用しない場合に、USB ポートを使用できる状態にしておくとし USB ポートから DX コントローラにアクセスされる危険性があります。USB ポートを使用しない場合は USB ポートを無効化しておくことで、第三者が USB ポートから DX コントローラにアクセスできないようにします。

USB ポートの無効化の方法については、『DX シリーズ Web UI 操作マニュアル(SBSB-539)』の USB ポート管理の説明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
	○		○	○	

2-3 DX コントローラの不正操作を防止する

DX コントローラの不正操作を防止し、お客様の大切な生産情報データの盗用や不正利用、およびシステムの異常を防ぎます。

お客様に実施していただきたいこと

- セキュアな運用を行うために、システムや装置／デバイス、および DX コントローラの設置区画への入退室管理や物理的施錠を行ってください。

2-3-1 アカウント管理（操作権限認証）機能（DX コントローラ）

DX コントローラのデータを変更する場合、操作ミスによりデータの収集や利活用が正しく行えないなどの被害を与える危険性があります。操作者に与えるロール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、管理者が操作者ごとに役割に応じたロールを設定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、『DX シリーズ Web UI 操作マニュアル(SBSB-539)』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。

2-4 アプリケーションへの不正接続を防止する

お客様の大切な生産情報データを盗用や不正利用から守るため、容易に DX コントローラ内のデータ収集や可視化のアプリケーションにアクセスできないように各アプリケーションへの接続時に認証する機能を使用します。

2-4-1 アカウント管理（ユーザ認証）機能（アプリケーション）

DX コントローラ内のアプリケーションへの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。DX コントローラに接続するためのユーザ認証に加えて、さらにアプリケーション毎に個別にアカウント管理を行ってユーザ認証を行うことで、セキュリティを向上します。

アプリケーションのユーザ認証機能は、アプリケーションを操作するユーザをあらかじめアプリケーションに登録しておき、アプリケーションをオンライン操作するユーザを特定する機能です。DX コントローラ内のアプリケーションに接続する際に、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、アプリケーションに接続することができません。

さらに、各ユーザには、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アプリケーションの操作ができないようにします。

ユーザ名、パスワード、およびその権限の情報などのユーザ認証設定は、DX 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 DX コントローラに接続しても、アプリケーションのユーザ認証機能を使用することができます。

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
○	○	○	○	○	○

アプリケーションのユーザ認証機能では、DX コントローラ内のアプリケーションに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の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、SpeedBee Synapse については『DX シリーズ SpeedBee Synapse ユーザーズマニュアル(SBSB-540)』を、Grafana については Grafana のマニュアルを参照してください。また、パッケージについては『DX シリーズ ダッシュボードジェネレータ ユーザーズマニュアル (SGTE-729)』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

- ・ 初期登録されているユーザアカウントは無効化または削除してください。
- ・ 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。
- ・ 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。
- ・ アクセストークンは第三者に知られないように厳重に管理してください。

2-5 アプリケーションの不正操作を防止する

DX コントローラ内のアプリケーションの不正操作を防止し、お客様の大切な生産情報データの盗用や不正利用、およびシステムの異常を防ぎます。

お客様に実施していただきたいこと

- ・ エクスポートしたファイルに機密情報が含まれる場合は、第三者に漏洩したり改ざんされたりしないように、利用者にて暗号化して厳重に管理してください。また、インポートするデータを入手したときにはハッシュ値が期待した値と一致しているかを確認し、改ざんされていないことを確認してください。

2-5-1 操作権限認証機能（アプリケーション）

アプリケーションのデータを変更する場合、操作ミスによりデータの収集や利活用が正しく行えないなどの被害を与える危険性があります。操作者に与える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、管理者が操作者ごとに役割に応じた権限を設定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、SpeedBee Synapse については『DX シリーズ SpeedBee Synapse ユーザーズマニュアル(SBSB-540)』を、Grafana については Grafana のマニュアル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。

2-6 否認を防止する

データを守るためには、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。

2-6-1 ログ機能

DX コントローラでは、DX コントローラに対してユーザが Web UI を使用して行ったオンライン操作のうちセキュリティに関わる重要操作を操作ログに登録します。操作内容、時刻、ユーザ名、実行結果（成功／失敗）を記録します。また、DX コントローラ上のアプリケーションもそれぞれ独自にログに登録し、そのうちのセキュリティに関わるログを監査ログとして利用できます。なお、アプリケーションのログは、データフローコントローラに登録するログとアプリケーション内部に登録するログの2つがあります。

DX コントローラのログについては、『DX シリーズ CPU ユニット ユーザーズマニュアル (SBSB-538)』を参照してください。

アプリケーションのログに関しては、SpeedBee Synapse については『DX シリーズ SpeedBee Synapse ユーザーズマニュアル(SBSB-540)』を、Grafana については Grafana のマニュアルを参照してください。また、パッケージについては『DX シリーズ ダッシュボードジェネレータ ユーザーズマニュアル(SGTE-729)』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

- 記録されたログの日時が正確でないと否認防止できない可能性があります。DX コントローラとパソコンの時刻は正しく設定してください。正しい日時を維持するために NTP での日時設定を推奨します。
- ログが消去されると否認防止できません。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。また、アプリケーションのログは、初期化（ファクトリーリセット）により消去されます。ご利用の環境、運用でのログが残る期間をもとに定期的にログをダウンロードして、一定期間保存することを推奨します。

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データを守るためには、使用している機器を最新の状態で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、DX 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	DX 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の履歴	3-2
3-2	パソコンの OS をアップデートする	3-3
3-3	ブラウザをアップデートする	3-4

3-1 DX 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、DX 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、『DX シリーズ CPU ユニット ユーザーズマニュアル (SBSB-538)』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

- アップデートには USB メモリを使用します。正当な作業者によってのみアップデート作業が行われるように、適切な操作権限の設定、および入退室管理や物理的施錠などを行ってください。
- アップデートで USB メモリを使用するときには USB ポートを有効にする必要があります。アップデート前に USB ポートを無効にしていた場合は、アップデート後に USB ポートを無効に戻してください。

3-1-1 ファームウェアアップデートの履歴

DX コントローラのログにて、ファームウェアのアップデート履歴を確認します。
DX コントローラのログの確認方法については、『DX シリーズ Web UI 操作マニュアル(SBSB-539)』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 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、Web UI 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。

3-3 ブラウザをアップデートする

ブラウザ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、Web UI に接続するブラウザを常に最新の状態にしてください。

4

機器を安全に廃棄する

本章では、廃棄に関し、DX 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	DX コントローラ内のデータを消去する	4-2
4-1-1	初期化（ファクトリーリセット）機能	4-2

4-1 DX コントローラ内のデータを消去する

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 初期化（ファクトリーリセット）機能

初期化（ファクトリーリセット）機能は、DX コントローラ内の設定を工場出荷時の状態に戻す機能です。ユーザが設定したデータも消去されます。

ファクトリーリセット機能の詳細は、『DX シリーズ CPU ユニット ユーザーズマニュアル (SBSB-538)』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

- DX コントローラには設定の初期化（ファクトリーリセット）などを行うためのディップスイッチがあります。セキュアな運用を行うために、ディップスイッチの不正操作を防止するための対策を実施してください。たとえば入退室管理や物理的施錠などを行ってください。



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（DX シリーズ専用）

お客様
相談室

✉ メールでのお問い合わせ（お問い合わせフォーム）

<https://www.fa.omron.co.jp/dx1/contact/>

対応時間：9:00～17:00（土・日・12/31～1/3を除く）



マニュアル動画

<https://www.fa.omron.co.jp/dx1/video-manual/ja/>



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 SBSB-030A

2025年9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