Edgecross

ユーザ向けセキュリティガイドライン　詳細版

Ver. 2.0.0

Edgecross コンソーシアム　テクニカル部会　セキュリティガイドライン策定 WG

ECD-TE4-0006-02-JA

テクニカル部会　セキュリティガイドライン策定WG
参加企業(敬称略、順不同)

株式会社立花エレテック

日本電気株式会社

株式会社日立製作所

富士通株式会社

三菱電機株式会社

マカフィー株式会社

日本マイクロソフト株式会社

トレンドマイクロ株式会社

改定履歴

Ver.	改定内容	発行年月
1.0.0	初版発行	2020 年 6 月
2.0.0	・セキュリティ対策事例集の追加 ・チェックリストの追加 ・その他、記載の充実	2022 年 9 月

目次

別冊　工場全体のセキュリティ脅威詳細
別冊_セキュリティ対策事例集
別冊_ユーザ向けセキュリティガイドライン_チェックリスト

1. はじめに

1. 1 概要

製造業ではいま、競争力強化や新たな価値の創出に向け、IoT(Internet of Things)活用が加速しています。『Edgecross コンソーシアム』はこの時流を踏まえ、企業・産業の枠を超え、コンソーシアム会員が共に構築し、FA(Factory Automation)と IT(Information Technology)との協調を実現するオープンな日本発のエッジコンピューティング領域のソフトウェアプラットフォーム『Edgecross』を提供しています。FA と IT との協調により工場の生産性向上などが期待できる反面、FA システムの内外から攻撃を受ける脅威も増します。脅威の低減には、人的、物理的、さらには接続されるネットワーク等の様々な対策を多層に施すのが望ましいと考えます。

本書は、Edgecross の典型的なユースケースにおいて想定される具体的な脅威を例示した上で、Edgecross を用いた FA システムを構築する際に考慮すべきセキュリティのポイントを示し、安全・安心を確保するためのガイドラインです。お客様にて導入されることを推奨しているセキュリティ対策として、ハードウェア/OS、セキュリティソフトウェア、Edgecross 基本ソフトウェア、ネットワーク観点からポイントを概要版よりも詳細に記載しています。

1. 2 本書の対象範囲

本書の対象読者として、Edgecross システムを構築する技術者、Edgecross システムの管理者、および、Edgecross システムの運用者を想定しています。

本書は、IoT 推進コンソーシアム/総務省/経済産業省が刊行する「IoT セキュリティガイドライン」を元に、Edgecross システムのセキュリティ対策の指針を具体化したものです。

表 1-1 にセキュリティ対策指針の要点と、本書の記載箇所の対応を示します。

表 1-1 セキュリティ対策指針の要点と記載箇所

「IoT セキュリティガイドライン」ver 1.0 (IoT 推進コンソーシアム/総務省/経済産業省) セキュリティ対策指針一覧			本書の記載箇所
大項目	指針	要点	
方針	指針1 IoT の性質を考慮した基本方針を定める	要点 1. 経営者が IoT セキュリティにコミットする	1.3
		要点 2. 内部不正やミスに備える	1.3
分析	指針2 IoT のリスクを認識する	要点 3. 守るべきものを特定する	2.2
		要点 4. つながることによるリスクを想定する	2.3, 2.5
		要点 5. つながりで波及するリスクを想定する	2.3, 2.5
		要点 6. 物理的なリスクを認識する	2.3, 2.5
		要点 7. 過去の事例に学ぶ	2.4
設計	指針3 守るべきものを守る設計を考える	要点 8. 個々でも全体でも守れる設計をする	3.1
		要点 9. つながる相手に迷惑をかけない設計をする	3.1
		要点 10. 安全安心を実現する設計の整合性をとる	3.1
		要点 11. 不特定の相手とつなげられても安全安心を確保できる設計をする	3.1
		要点 12. 安全安心を実現する設計の検証・評価を行う	3.1
構築・接続	指針4 ネットワーク上での対策を考える	要点 13. 機器等がどのような状態かを把握し、記録する機能を設ける	3.2, 3.3, 3.4
		要点 14. 機能及び用途に応じて適切にネットワーク接続する	3.2, 3.3, 3.4, 3.5
		要点 15. 初期設定に留意する	3.2, 3.3, 3.4, 3.5
		要点 16. 認証機能を導入する	3.2, 3.3
運用・保守	指針5 安全安心な状態を維持し、情報発信・共有を行う	要点 17. 出荷・リリース後も安全安心な状態を維持する	4.1
		要点 18. 出荷・リリース後も IoT リスクを把握し、関係者に守ってもらいたいことを伝える	4.2
		要点 19. つながることによるリスクを一般利用者に知ってもらう	4.2
		要点 20. IoT システム・サービスにおける関係者の役割を認識する	4.2
		要点 21. 脆弱な機器を把握し、適切に注意喚起を行う	4.2

なお、FA 関連のセキュリティ文献として、制御システムのセキュリティ規格 IEC62443 等もありますので、必要に応じて参照してください。

1. 3 基本方針

1. 3. 1 サイバーセキュリティ経営

IoT を活用したシステムのサイバーセキュリティ対策においては、IoT システムの性質を考慮した基本方針を定めることが重要です。セキュリティ対策にはコストがかかることがあり、また、運用現場の裁量を越える判断が求められる状況に直面する事態も想定されます。よって、経営者層のレベルが率先してセキュリティ対策の方針を示す必要があります。

セキュリティ対策には、各所が連携して対応するための体制の構築、セキュリティ技術を活用できる人材の育成なども必要となります。更に、安全を脅かす内部不正の可能性や、意図せず発生するミスなど、人為的な脅威への対応も求められます。

経済産業省 独立行政法人 情報処理推進機構より刊行されている「サイバーセキュリティ経営ガイドライン」では、サイバーセキュリティに関して、経営者のリーダーシップによって取り組むべき 10 項目について説明されています。特に、以下に記す項目は Edgecross システムのサイバーセキュリティ対策において重要な取り組みであるため、実施を推奨します。

・サイバーセキュリティリスクの把握とリスク対応に関する計画の策定
　Edgecross システムに対するサイバー攻撃の脅威と影響度からサイバーセキュリティリスクを把握し、Edgecross システムを運用する上で必要なリスク対応を計画する。
・サイバーセキュリティリスクに対応するための仕組みの構築
　本書で示すようなセキュリティ対策を適切かつ確実に実施できるように、サイバーセキュリティリスクに対応できる仕組みを構築する。
・インシデントによる被害に備えた復旧体制の整備
　インシデントにより Edgecross システムが被害を受けた場合に備えて、復旧対応体制を整備する。
・ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握
　Edgecross システムを構成する基本ソフトウェアや各コンポーネントの提供元が実施しているセキュリティ対策について、提供元の Web サイトなどで確認する。
・情報共有活動への参加を通じた攻撃情報の入手とその有効活用及び提供
　Edgecross システムを構成する基本ソフトウェアや各コンポーネントに関係する攻撃情報を、提供元の Web サイトや JPCERT/CC（https://www.jpcert.or.jp/）等の公的機関から入手する。入手した攻撃情報をもとにセキュリティ対策を実施する。

上記の項目に限らず、「サイバーセキュリティ経営ガイドライン」を参考に、組織としてセキュリティ対策に取り組んでください。

また、Edgecross コンソーシアムでは、Edgecross システムに関するセキュリティ情報を発信していますので、併せて活用してください。

1. 3. 2 Edgecross コンソーシアム

Edgecross コンソーシアムは、産業界の発展のためのプラットフォームを普及促進する団体として、お客様の利用環境における安全・安心の維持・向上に貢献するように、以下の 3 つを柱とする継続的な取り組みを行います。

・安全・安心を確保するための組織・体制の構築
　本コンソーシアムは、セキュリティに関する問題に迅速に対応するための体制を整備しセキュリティインシデント発生時には JPCERT/CC と連携して迅速な対応とお客様への情報提供を行います。また、脅威動向・技術・制度などを調査し、本コンソーシアム会員企業およびお客様全体に対しセキュリティに対する正しい知識と高い意識を保つべく、周知に努めます。

・安全・安心を実現する製品開発
　本コンソーシアムは会員企業と共に、守るべき資産や想定する脅威を分析し、堅牢な製品設計を行い、出荷・リリース後も安全・安心な状態を維持できるよう、開発者向けセキュリティガイドラインを策定し、適切なセキュリティ対策が施されるように製品開発を行います。

・お客様向けセキュリティガイドラインの提供

本コンソーシアムは、脅威の低減には、人的、物理的、ネットワークなどの様々な対策を多層に施すのが望ましいと考えます。このため、本コンソーシアムは Edgecross 対応製品を導入した FA システムにおける適切な運用に向けたセキュリティガイドラインを提供し、『Edgecross』の利用環境におけるセキュリティ対策導入／維持向上を支援します。

1. 4 略称

BIOS	Basic Input Output System
C&C	Command and Control
CPU	Central Processing Unit
CSV	Comma Separated Values
DB	Data Base
DCS	Distributed Control System
DDoS	Distributed Denial of Service
DMZ	DeMilitalized Zone
DoS	Denial of Service
ERP	Enterprise Resources Planning
EWS	Engineering WorkStation
FA	Factory Automation
FW	FireWall
GW	GateWay
HDD	Hard Disk Drive
HMI	Human Machine Interface
ID	Identification
IPS	Intrusion Prevention System
I/F	Interface
IoT	Internet of Things
IP	Internet Protocol
IPA	Information-technology Promotion Agency
IT	Information Technology
JPCERT/CC	Japan Computer Emergency Response Team Coordination Center
LAN	Local Area Network
L2SW	Layer 2 Switch
MES	Manufacturing Execution System
MQTT	Message Queuing Telemetry Transport
NC	Numerical Control
OPC	OLE (Object Linking and Embedding) for Process Control
OPC UA	OPC Unified Architecture
OS	Operating System
OSS	Open Source Software
PC	Personal Computer
PIN	Personal Identification Number
PLC	Programmable Logic Controller
SCADA	Supervisory Control and Data Acquisition
SD	Secure Digital
SNMP	Simple Network Management Protocol
SOC	Security Operation Center
TLS	Transport Layer Security
TPM	Trusted Platform Module
USB	Universal Serial Bus
UPS	Uninterruptible Power Supply
VPN	Virtual Private Network
WWW	World Wide Web

1. 5 用語

本書で用いる用語を表 1-2 に示します。

表 1-2 用語

用語	説明
IT システム	IT を用いて生産現場からのデータ を活用するシステム。本文書では特に、生産現場と LAN やインターネットを介し接続する外部システムの意味で用いる。
Edgecross システム	Edgecross を利用したシステム。
Edgecross ソフトウェア	Edgecross 基本ソフトウェア、エッジアプリケーション、データコレクタ、IT ゲートウェイの総称。
Edgecross 基本ソフトウェア	Edgecross の機能を実装したソフトウェア。エッジアプリケーションと連携して、生産現場のデータの分析･診断などの実行、およびオンプレミスやクラウドの IT システムとの間でデータのやり取りを行うことができる。
Edgecross 搭載 PC	Edgecross 基本ソフトウェアを搭載した産業用 PC。
エッジアプリケーション	エッジコンピューティング領域で、Edgecross から提供される機能を活用して、生産現場のデータ活用のための様々な処理を実行するソフトウェア。特に本書では Edgecross コンソーシアムの認定試験に合格しその認証を受けたものを指す。
データコレクタ	各ネットワークを介し、生産現場のデータを収集するソフトウェアコンポーネントで、各種ネットワークおよび接続対象機器向けに各ベンダが提供。
IT ゲートウェイ	生産現場のデータを活用するために IT システムと通信するソフトウェアコンポーネントで、各ベンダが提供。
脅威	保護すべき資産に対して危害を与える事象。
脆弱性	プログラムの不具合や設計上のミスが原因となって発生したセキュリティ上の欠陥。
アタックサーフェス	サイバー攻撃を受ける可能性のある領域。
セキュリティインシデント	マルウェア感染や情報窃取等、セキュリティ上の問題である事象。
マルウェア	不正かつ有害な動作を行う意図で作成された悪意のあるソフトウェアや悪質なコードの総称。
ランサムウェア	身代金の要求を目的としたマルウェア。
DoS / DDoS	DoS(Deinal of Service)は攻撃目標のサーバ等に対して大量のデータを送り付けるサービス妨害攻撃。DDoS(Distributed DoS)は複数の機器を乗っ取って DoS を仕掛ける攻撃。
権限昇格攻撃	ソフトウェアの実行権限を管理者権限に昇格させて不正を実行する攻撃。
C&C (Command and Control)サーバ	乗っ取った機器を制御したり、同機器に命令を出したりする外部サーバ。
ファイアウォール	ネットワーク間の通信可否を制御して不正アクセスを防ぐセキュリティ対策。
パーソナルファイアウォール	コンピュータにインストールし、外部との通信を監視して不正アクセスを防ぐファイアウォール。
IPS (Intrusion Prevention System)	通信を監視して管理者に通知し、不正な通信を遮断する侵入防止システム。
セグメンテーション	複数のサブネットワークに分割して、サブネットワーク毎にポリシーを定めて運用するセキュリティ対策。
DMZ (DeMilitalized Zone)	インターネット等の外部ネットワークと社内ネットワークの中間に設けるネットワーク上のセグメント。

セキュリティパッチ	アプリケーションの脆弱性を解消するための修正プログラム。
仮想パッチ	セキュリティパッチが早急に提供されない場合に、暫定的なセキュリティを担保する対策。
ブラックリスト方式	あらかじめ定義した危険なプログラムの実行を阻止する方式。
ホワイトリスト方式	あらかじめ定義した安全なプログラムのみを実行する方式。
TPM (Trusted Platform Module)	コンピュータのマザーボードに搭載されるハードウェア部品であり、データ暗号化・復号、鍵ペアの生成、ハッシュ計算、デジタル署名の生成・検証等の機能を提供する。
証明書	サーバとクライアント間の安全な通信やデータのやり取りを確立するために使用される証明書。サーバはサーバ証明書、クライアントはクライアント証明書をそれぞれ用いる。
PIN (Personal Identification Number)認証	個人識別番号(PIN)により個人を識別してユーザを認証する方式。
バイオメトリックス認証	指紋、静脈、顔等の身体や行動の特徴により個人を識別してユーザを認証する方式。
二段階認証/多要素認証	2 種類以上の認証(例えば PIN 認証とバイオメトリックス認証)を組み合わせてユーザを認証する方式。
SOC (Security Operation Center)	ネットワークやデバイスを常時監視して、サイバー攻撃の検出や分析、対策のアドバイスを行う組織。

1. 6 関連資料

本書の関連資料を表 1-3 に示します。

表 1-3 関連資料

No.	資料名称	資料 No	入手方法
1	IoT セキュリティガイドライン ver 1.0 平成 28 年 7 月 IoT 推進コンソーシアム, 総務省, 経済産業省	-	http://www.soumu.go.jp/main_content/000428393.pdf
2	サイバーセキュリティ経営ガイドライン Ver 1.0 平成 27 年 12 月 経済産業省 独立行政法人 情報処理推進機構	-	http://www.meti.go.jp/press/2015/12/20151228002/20151228002-2.pdf
3	Edgecross 仕様書 概要説明編	ECD-TE1-0002	Edgecross コンソーシアム会員用ホームページ
4	Edgecross 基本ソフトウェア Windows 版ユーザーズマニュアル	ECD-MA1-0001	マーケットプレイス(Edgecross 基本ソフトウェア Windows 版 商品ドキュメント)
5	制御システムのセキュリティリスク分析ガイド 第 2 版	-	https://www.ipa.go.jp/files/000069436.pdf
6	サイバー・フィジカル・セキュリティ対策フレームワーク Version 1.0 平成 31年 4 月 経済産業省	-	https://www.meti.go.jp/press/2019/04/20190418002/20190418002-2.pdf

2. Edgecross システム

本章では、システムの特徴、保護すべき資産、想定される脅威、セキュリティインシデント事例を示します。

2. 1 システムの特徴

Edgecross は、FA と IT の協調を実現するオープンなエッジコンピューティング領域のソフトウェアプラットフォームです。エッジコンピューティング領域においてマルチベンダのコンポーネントの組み合わせによるエコシステムの構築を可能とします。

エッジコンピューティングは、生産現場から収集したデータを生産現場側でデータ処理します。生産現場と物理的に近い場所にある産業用 PC 上でアプリケーションを実行することにより、リアルタイムな応答が要求されるシステムを実現します。

また、IT システムを活用して複数拠点や長期間のデータを扱うため、エッジコンピューティングにより生産現場と IT システムのシームレスな連携も実現します。

2. 2 保護すべき資産

Edgecross における保護すべき資産の全体を図 2-1 に示します。各種のセキュリティ脅威から保護すべき資産として、ここでは大きく、データ、ハードウェア/OS、Edgecross ソフトウェアおよび関連ソフトウェア、ネットワークの 4 種類に分類します。

データには稼動情報、センサー情報など、工作機械、産業用ロボットが生成するデータや NC プログラムなど、操作するために必要となるデータが含まれますが、Edgecross では NC プログラムなどは扱いません。

ハードウェア/OS には、産業用 PC、Windows OS 等があります。

Edgecross ソフトウェアには、リアルタイムデータ処理やデータモデル管理を実行する Edgecross 基本ソフトウェア、生産現場のデータを活用して様々な処理を実行する稼働監視等のエッジアプリケーション、後述の FA ネットワークを介して生産現場のデータを収集するデータコレクタ、IT システムとのシームレスなデータ連携を実現する IT ゲートウェイ、Mosquitto や OpenSSL 等のミドルウェアがあります。また、関連ソフトウェアとして開発用ソフトウェア等があります。

ネットワークには、生産現場のデータを転送する制御ネットワークやフィールドネットワーク等の FA ネットワーク、MES や ERP 等の IT システムと連携する情報ネットワークがあります。

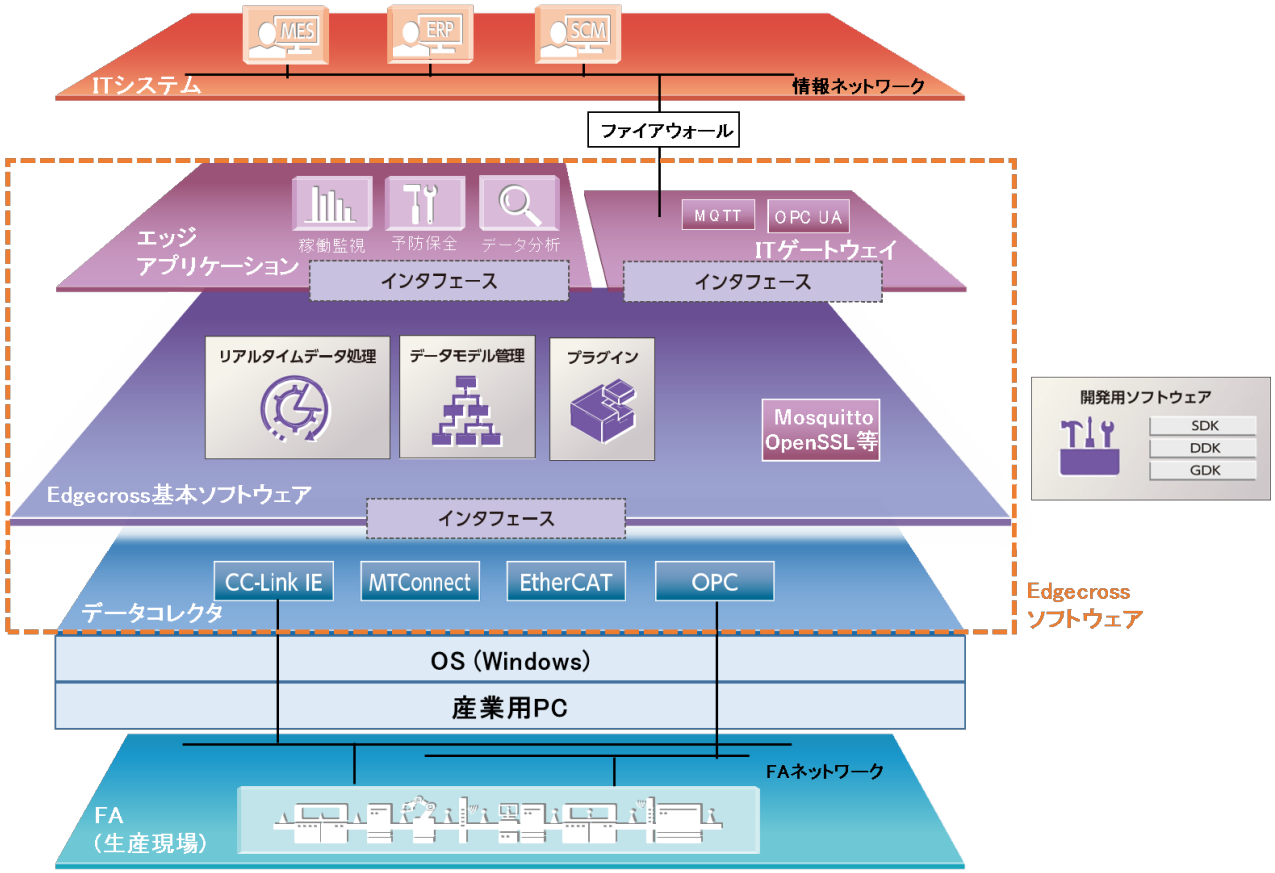


図 2-1 Edgecross における保護すべき資産

2. 3 想定される脅威

前述のシステムにおいて想定されるセキュリティ脅威を列挙します。これらの脅威による影響としては、製品の供給停止、火災などの事故、不良品の生産などが想定されます。

(1) なりすまし

他の利用者の Windows アカウント(ID とパスワード)が類推あるいは不正に入手され、本人になりすまされることにより Edgecross 搭載 PC へ不正にログインされる脅威が想定されます。

(2) 情報窃取

Edgecross 基本ソフトウェアで収集した生産現場のデータ等が不正に読み取られる脅威が想定されます。また、Edgecross ソフトウェアが Edgecross 搭載 PC から不正に読み取られる脅威も想定されます。

(3) マルウェア

マルウェアが Edgecross 搭載 PC にインストールされる脅威が想定されます。

(4) 不正通信

Edgecross 搭載 PC に潜むマルウェアが外部機器と不正に通信する脅威が想定されます。

(5) 改ざん

Edgecross 搭載 PC に潜むマルウェアが Edgecross ソフトウェアを不正に書き換えて、同ソフトウェアの機能が阻害される脅威が想定されます。また、マルウェアにより Edgecross 基本ソフトウェアで収集した生産現場のデータ等が不正に書き換えられ、不適切な集計結果や、次の処理を起動するための不適切なトリガを生成する脅威が想定されます。

(6) 高負荷攻撃の踏み台

マルウェアに感染した Edgecross 搭載 PC がサーバに対する DoS/DDoS 攻撃の踏み台に利用される脅威が想定されます。

(7) 脆弱性の悪用

OS やインストールされたソフトウェアの脆弱性が悪用されて、マルウェアが Edgecross 搭載 PC にインストールされるといった脅威が想定されます。

(8) 物理的な攻撃

不審者が物理的に侵入して、Edgecross 搭載 PC を窃盗するといった物理的な攻撃の脅威が想定されます。

2. 4 制御システムのセキュリティインシデント事例

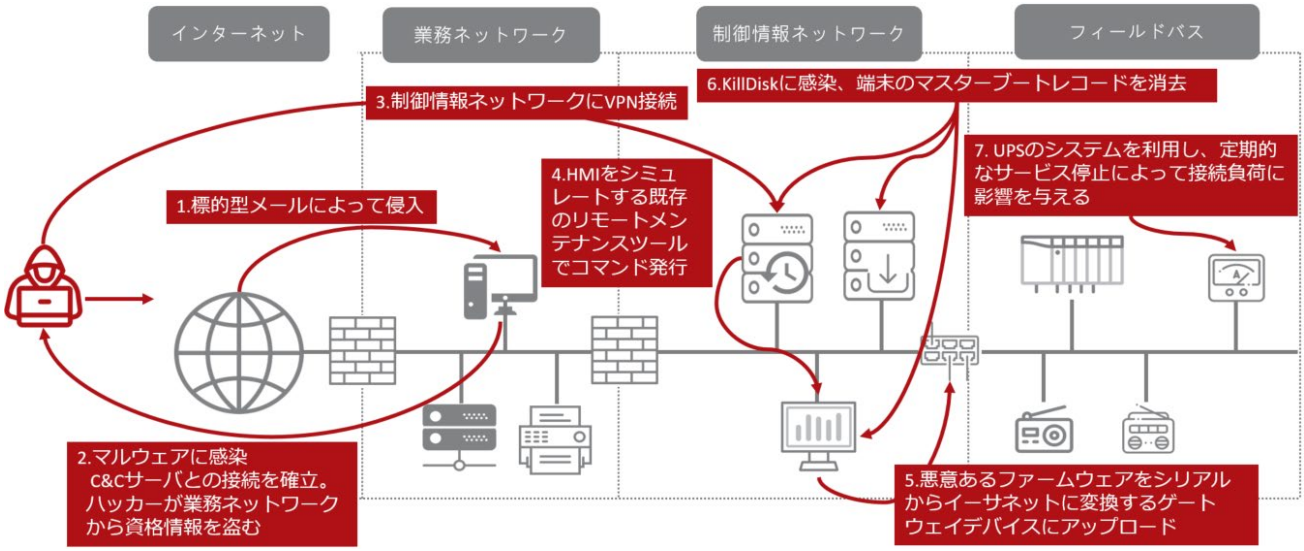
まずは、ウクライナで発生した発電施設のインシデント事例を示します。

2015 年 12 月、ウクライナ各地域の電力会社 3 社が、複数のサイバー攻撃による予期しない停電に追い込まれました。停電は 3 時間に及び、約 25 万人の顧客が影響を受けたと報道されています。

攻撃者は、「仮想プライベートネットワーク（Virtual private Network、VPN）」を乗っ取って SCADA ネットワークにアクセスし、発電施設を制御しました。これにより、顧客を停電に追い込むだけでなく、施設のオペレーションも操作不能に陥りました。

この事例は、直接インターネットに接続していない制御システム環境であっても、サイバー攻撃の被害を受ける可能性があることを示しています。

Edgecross システムが配置される工場環境でも、これと同様にインターネットに接続していない場合があります。たとえオフライン環境であってもセキュリティリスクが残っていると認識し、被害にあわないためのセキュリティ対策を講じなくてはなりません。



（出典：トレンドマイクロ 脅威データベース・セキュリティ Blog https://blog.trendmicro.co.jp/archives/14203）

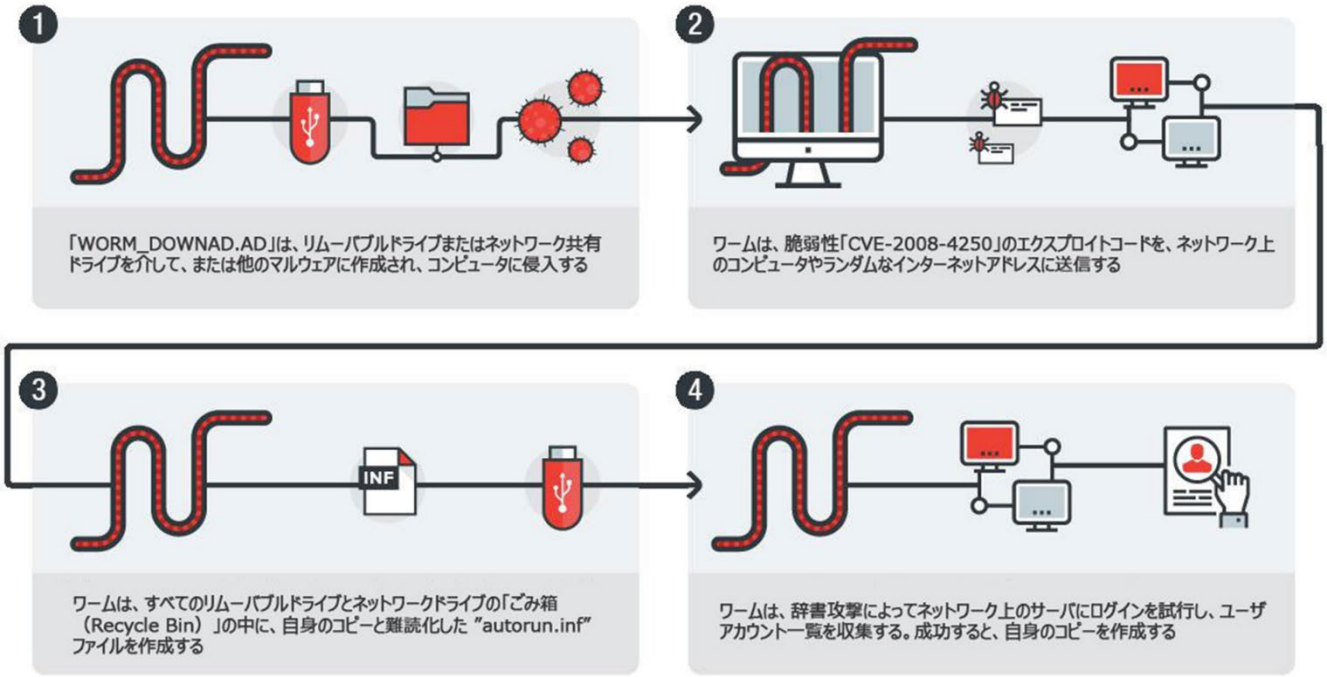
次は、未だに工場で拡散し続ける DOWNAD(別名：Conflicker)の事例を示します。

DOWNAD が初めて脅威として台頭したのは、2008 年 11 月のことでした。初めて脅威が確認されてから瞬く間に世界中で何十万ものコンピュータが DOWNAD に感染したと報告されています。ここで重要なことは、全盛期から 12 年経ったの現在でも、DOWNAD は「古くなったシステムに対して威力を発揮し続けているマルウェア」であるということです。

「WannaCry」や「PETYA」のように、より現代的なマルウェアとして、一般の方々にとって興味を掻き立てられるマルウェアではありませんが、サポート対象外になって脆弱性が更新されることがない古いシステムがネットワーク内にある限り、依然として脅威であり、今後もこのような状況が変化することはないでしょう。

この事例は、外部から持ち込まれるリムーバブルメディアによってマルウェアが侵入し、LAN 上の端末やネットワークドライブに拡散してしまう二次被害につながる可能性があることを示しています。

Edgecross システムが配置される工場環境でも、保守・メンテナンスなどの理由により、USB メモリや CD-ROM などのリムーバブルメディアを使う場合があります。持ち込み端末や、リムーバブルメディアを利用する場合は、保守担当者の不注意によるセキュリティリスクが残っていると認識し、被害にあわないために事前確認を行うなどのセキュリティ対策を講じなくてはなりません。



（出典：トレンドマイクロ　脅威データベース・セキュリティ Blog　https://blog.trendmicro.co.jp/archives/16614）

2. 5 ユースケース

2.5.1 システム構成

Edgecross 利用時の典型的なシステム構成として、大規模工場と小規模工場の 2 つのケースを示します。

【パターン1】大規模工場の場合（図 2-2）

大規模工場では、管理棟で使用する進捗管理用パソコンなどが接続する情報ネットワークと工場内で使われるネットワークに分かれており、情報ネットワークと工場内のネットワークとの通信やインターネットへの通信はファイアウォール経由で行われるようになっています。

工場内のネットワークは、エンジニアリングツールや MES Client が接続する情報制御ネットワーク [1]、工作機械が接続する制御ネットワーク [2]、PLC・制御機器や HMI が接続するフィールドネットワーク [3]に分かれています。

Edgecross を搭載した PC（Edgecross 搭載 PC）は、制御ネットワークまたは情報制御ネットワークに接続して使われます。

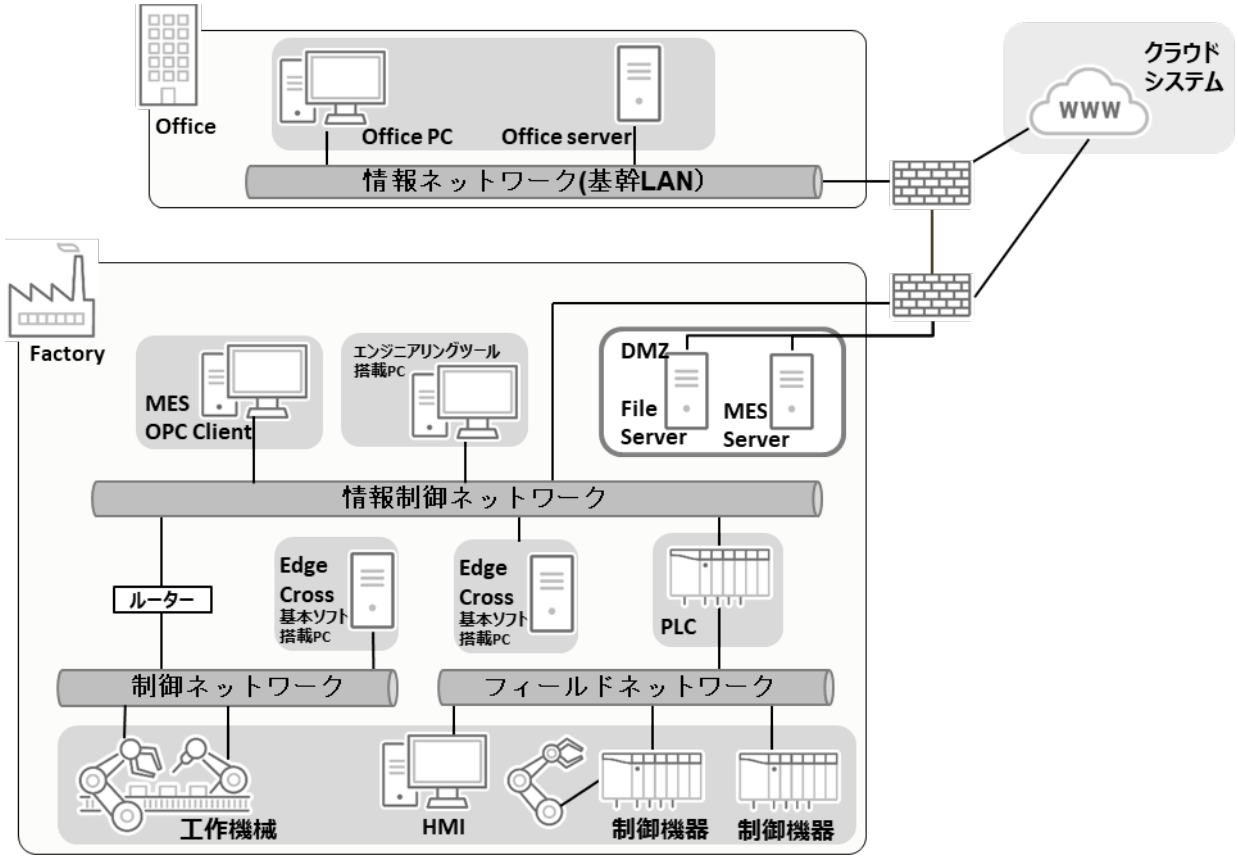


図 2-2【パターン1】システム構成の例（大規模工場）

【パターン2】小規模工場の場合（図 2-3）

小規模工場では、事務所内にある事務用パソコン、エンジ PC、FileServer などと工作機械が一つのネットワークに接続されています。

Edgecross 搭載 PC も同じネットワークに接続して使われます。

[1] 工場内ネットワークにおいて、パソコンやサーバなどを接続する情報系ネットワーク
[2] イーサネットベースのプロトコルにより制御用通信を行うネットワーク
[3] コントローラ間とフィールド機器間の制御用通信を主目的とするネットワーク

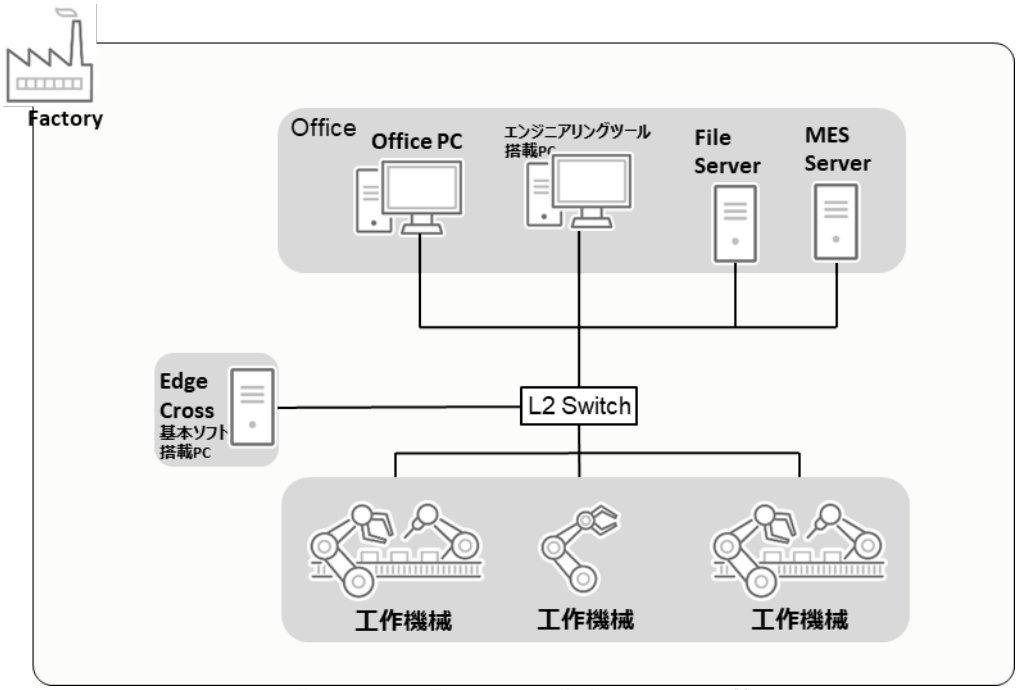


図 2-3 【パターン2】システム構成の例（小規模工場）

2.5.2 シナリオ例

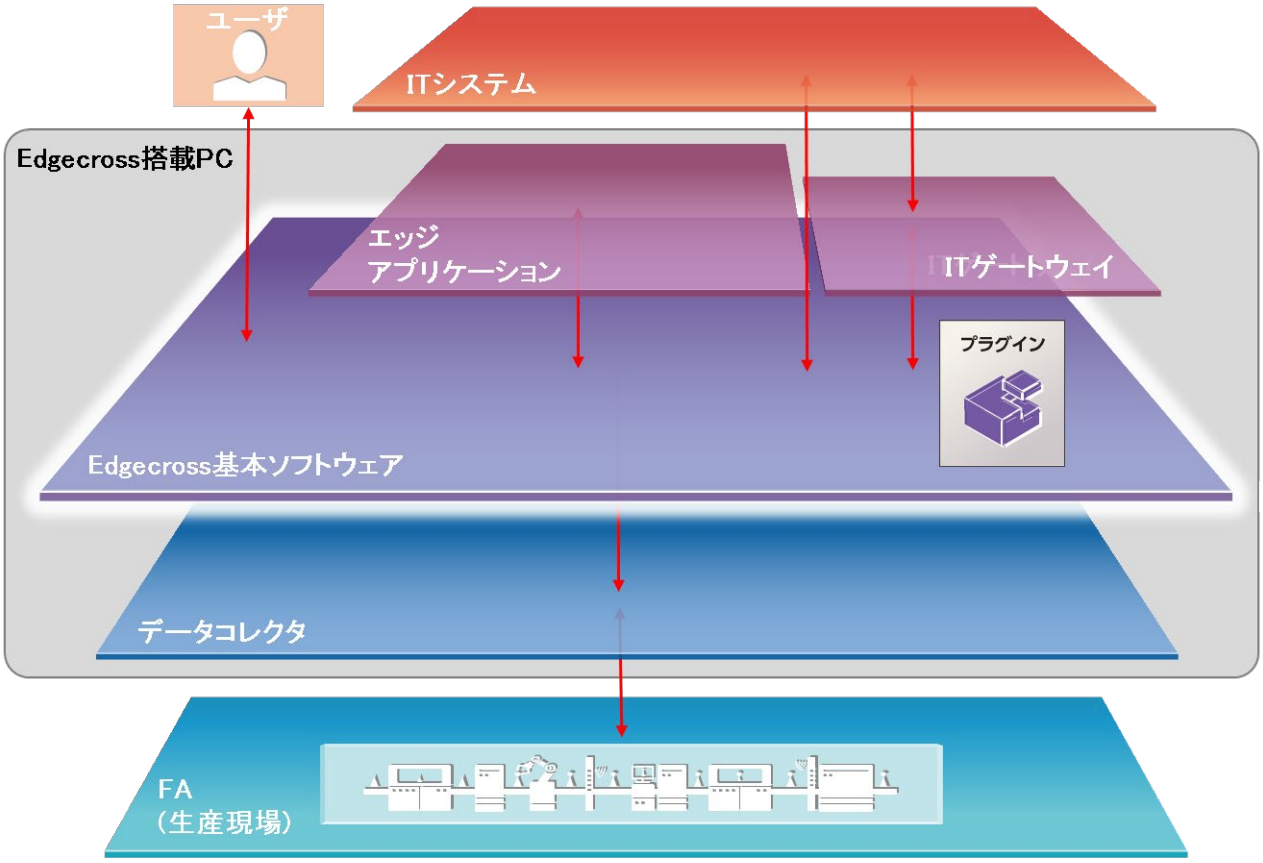


図 2-4 Edgecross ソフトウェア構成概略図

まず Edgecross ソフトウェアの構成を上図に示します。Edgecross 基本ソフトウェアは、データコレクタを通じて、生産現場設備のデータ収集やフィードバックを行います。エッジアプリケーションでは、データの分析・診断を行います。また、外部 IT システムとの間でデータのやり取りを行います。

Edgecross 基本ソフトウェアは、さらにリアルタイムフローマネージャ、リアルタイムフローデザイナ、マネジメントシェル、マネジメントシェルエクスプローラから構成されます。

リアルタイムフローマネージャは、生産現場のデータのリアルタイム診断･フィードバックを実現する機能を実装したソフトウェアです。データコレクタ(ネットワークを介し、生産現場のデータを収集するソフトウェア)を使用して、接続された機器、装置、またはラインのデータを収集し、データの加工および分析を行うことができます。また、プラグインを使用して、機能拡張を行うこともできます。リアルタイムフローデザイナより Windows サービスとして起動/停止されます。

リアルタイムフローデザイナは、リアルタイムフローマネージャの動作に必要な各種設定の作成、保存、表示、リアルタイムフローマネージャの動作開始/停止、および診断を行う機能を実装したソフトウェアです。

マネジメントシェルは、生産現場の機器、装置、またはラインに関するデータをモデル化し、階層構造として管理するソフトウェアです。データコレクタを使用して、接続された機器、装置、またはラインのデータの読出し、データの書込みを行うことができます。マネジメントシェルエクスプローラより Windows サービスとして起動/停止されます。

マネジメントシェルエクスプローラは、マネジメントシェルが管理するデータモデルの設定および参照を行い、マネジメントシェルの動作開始/停止を担います。

表 2-1 に、Edgecross を用いるシナリオ例を表 2-1 に示します。

表 2-1 Edgecross を用いるシナリオ例

	カテゴリ	シナリオ名	備考
(a)	設定	システム立ち上げ(リアルタイムフローデザイナ)	リアルタイムフローマネージャ経由での機器アクセス
(b)		システム立ち上げ(マネジメントシェルエクスプローラ)	マネジメントシェル経由での機器アクセス
(c)	データ収集	OPC UA によるエッジアプリケーション(MES Server など)からのデータアクセス	
(d)		エッジアプリケーションでのヒストリカルデータ利用	
(e)		FileServer でのデータ蓄積	
(f)		クラウドサービスでのデータ分析	パターン 2 では行われない。
(g)	フィードバック	エッジアプリケーションからのフィードバック	エッジアプリケーションでの診断＋フィードバック

(a) システム立ち上げ(リアルタイムフローデザイナを使うケース)

リアルタイムフローデザイナを起動して、リアルタイムフローマネージャに関する設定等を行います。

① ユーザはリアルタイムフローデザイナを起動して、使用するデータコレクタの選択、アクセス先機器設定を行います。
② 次に、「データロギングフロー設定」または「データ診断フロー設定」を行います。
③ 最後に設定を適用します。
④ データ診断等でエッジアプリケーションを使う場合、その設定を行います。

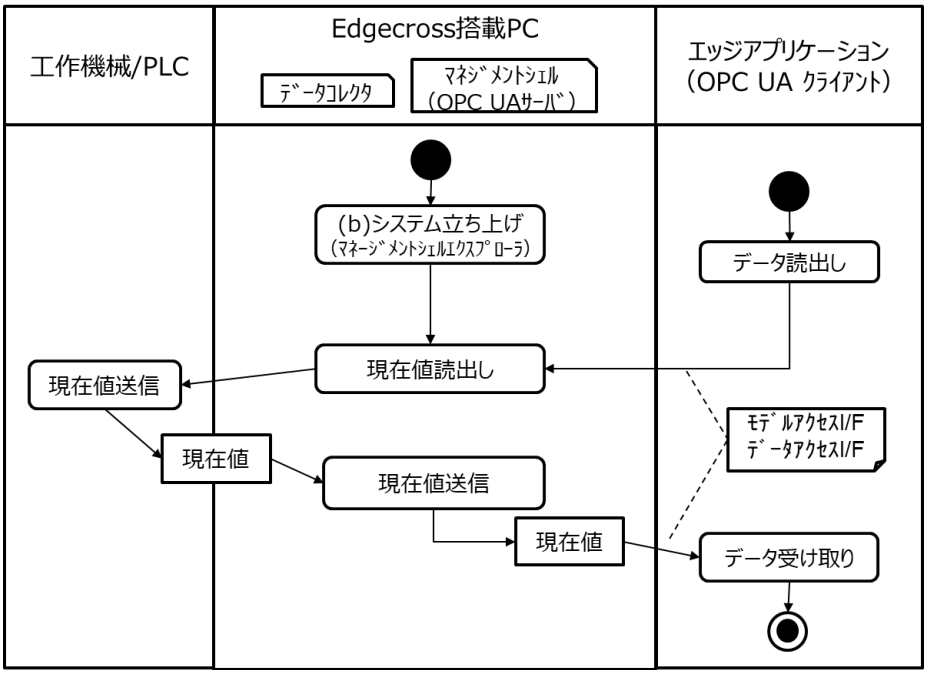
(b) システム立ち上げ(マネジメントシェルエクスプローラを使うケース)

マネジメントシェルエクスプローラを起動して、マネジメントシェルに関する設定等を行います。

① ユーザはマネジメントシェルエクスプローラを用いて、使用するデータコレクタの選択、アクセス先機器設定を行います。
② コンポーネントツリーの編集を行い、工場内システムのモデルを作成します。
③ IT ゲートウェイを使用する場合、ゲートウェイ設定を行います。
④ OPC UA を使用する場合、OPC UA 設定を行います。
⑤ 利用するエッジアプリケーションに応じて、OPC UA 通信の設定やデータモデルの参照先など、必要な設定を行います。

(c)　OPC UA によるエッジアプリケーション（MES サーバなど）からのデータアクセス

Edgecross のモデルアクセス I/F(OPC UA)、データアクセス I/F(OPC UA)を使用し、エッジアプリケーション（MES サーバなど）が工作機械／PLC の現在値を参照するケースです。



※このケースでは、マネジメントシェルを使用するため、事前に(b)システム立ち上げ（マネジメントシェルエクスプローラを使うケース）を実施します。

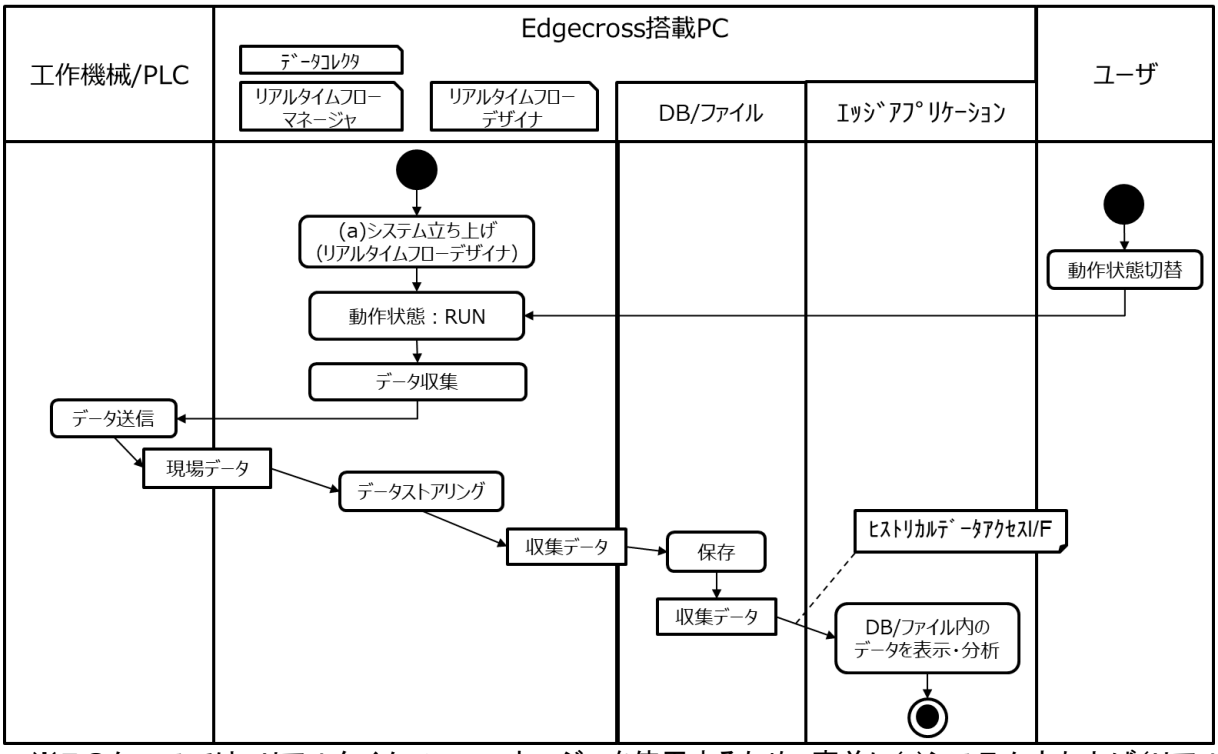
① エッジアプリケーションは、モデルアクセス I/F またはデータアクセス I/F により、マネジメントシェルにデータ読出しを行います。

② マネジメントシェルはデータコレクタ経由で、工作機械／PLC から現在値を読み出します。

③ 読み出した現在値は、要求元のエッジアプリケーションに送信します。

(d) エッジアプリケーションでのヒストリカルデータ利用

Edgecross のヒストリカルデータアクセス I/F を使用し、エッジアプリケーションがヒストリカルデータを分析などに利用するケースです。



※このケースでは、リアルタイムフローマネージャを使用するため、事前に(a)システム立ち上げ(リアルタイムフローデザイナを使うケース)を実施します。

① ユーザはリアルタイムフローデザイナからリアルタイムフローマネージャの動作状態を RUN に切り替えます。

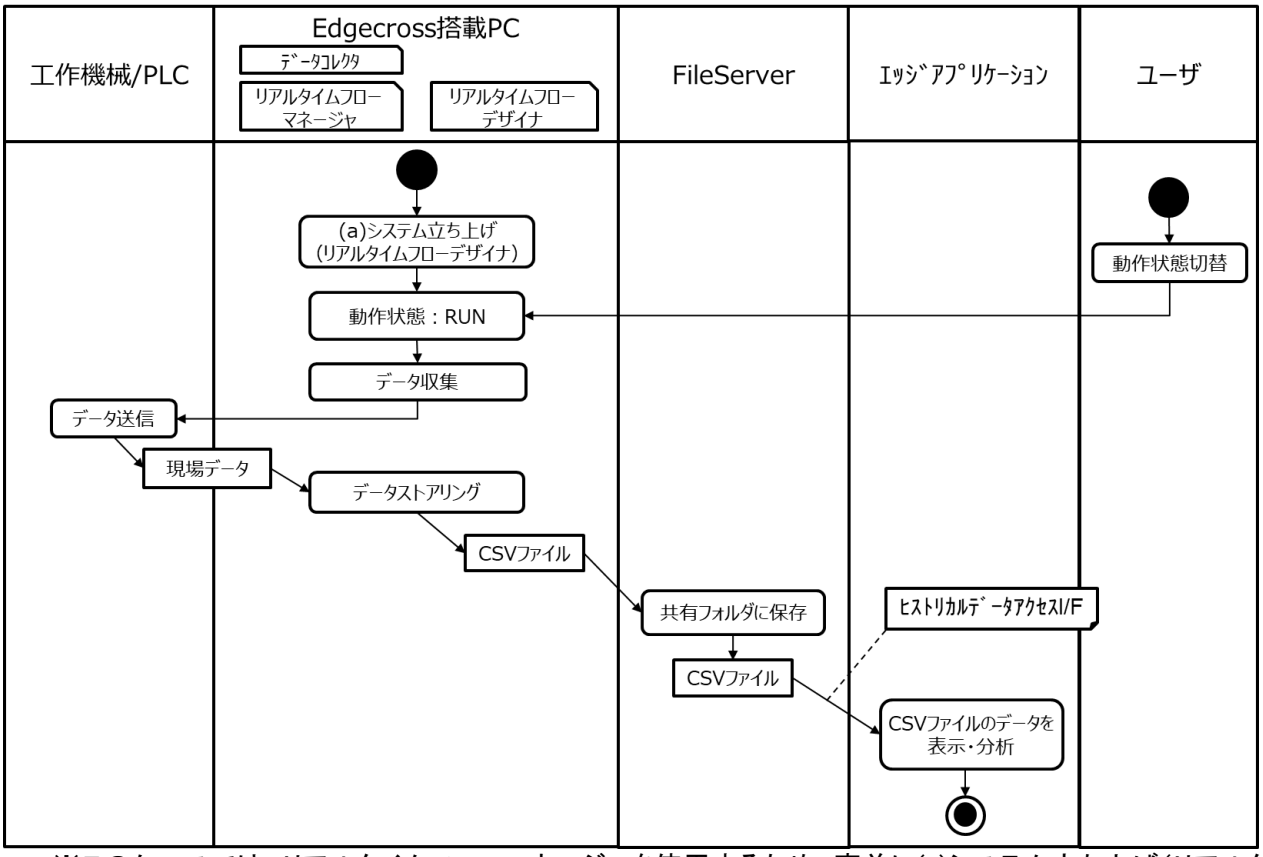
② リアルタイムフローマネージャはデータコレクタ経由で、工作機械／PLC からのデータ収集を行います。

③ 収集した現場データは、リアルタイムフローマネージャのデータストアリング機能により DB/ファイルに保存されます。(※データストアリング機能によりファイルに保存するケースもあります。)

④ エッジアプリケーションは、ヒストリカルデータアクセス I/F により、DB/ファイルから収集データを取得し、表示・分析などを行います。

(e) FileServer でのデータ蓄積

リアルタイムフローマネージャのデータストアリング機能により FileServer に CSV ファイルで保存された収集データをエッジアプリケーションでの分析などに用いるケースです。



※このケースでは、リアルタイムフローマネージャを使用するため、事前に(a)システム立ち上げ(リアルタイムフローデザイナを使うケース)を実施します。

① ユーザはリアルタイムフローデザイナからリアルタイムフローマネージャの動作状態を RUN に切り替えます。

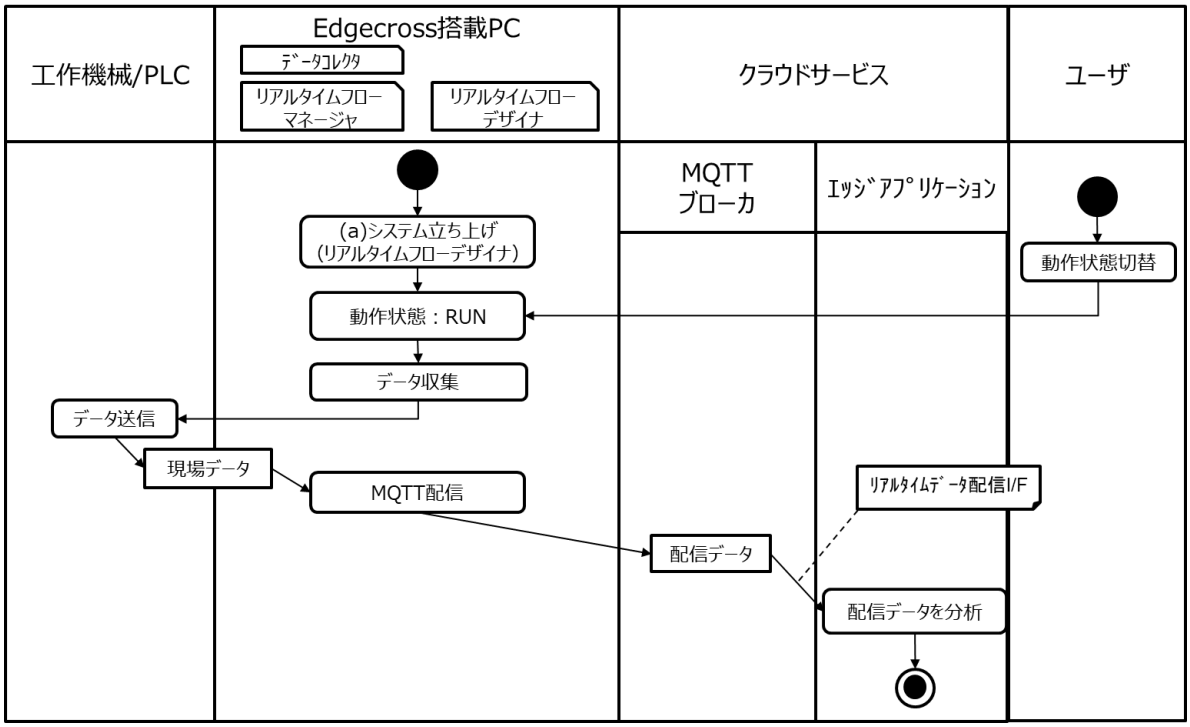
② リアルタイムフローマネージャはデータコレクタ経由で、工作機械や PLC からのデータ収集を行います。

③ 収集した現場データは、のデータストアリング機能により FileServer の共有フォルダ上の CSV ファイルに出力されます。

④ エッジアプリケーションは、ヒストリカルデータアクセス I/F により、FileServer 上の CSV ファイルから収集データを取得し、表示・分析などを行います。

(f)　クラウドサービスでのデータ分析

リアルタイムフローマネージャのデータ配信機能（MQTT 配信機能）により MQTT でクラウドサービスにデータを集積し、リアルタイムデータ配信 I/F に対応しているエッジアプリケーションでの分析などに用いるケースです。



※このケースでは、リアルタイムフローマネージャを使用するため、事前に(a)システム立ち上げ（リアルタイムフローデザイナを使うケース）を実施します。

① ユーザはリアルタイムフローデザイナからリアルタイムフローマネージャの動作状態を RUN に切り替えます。

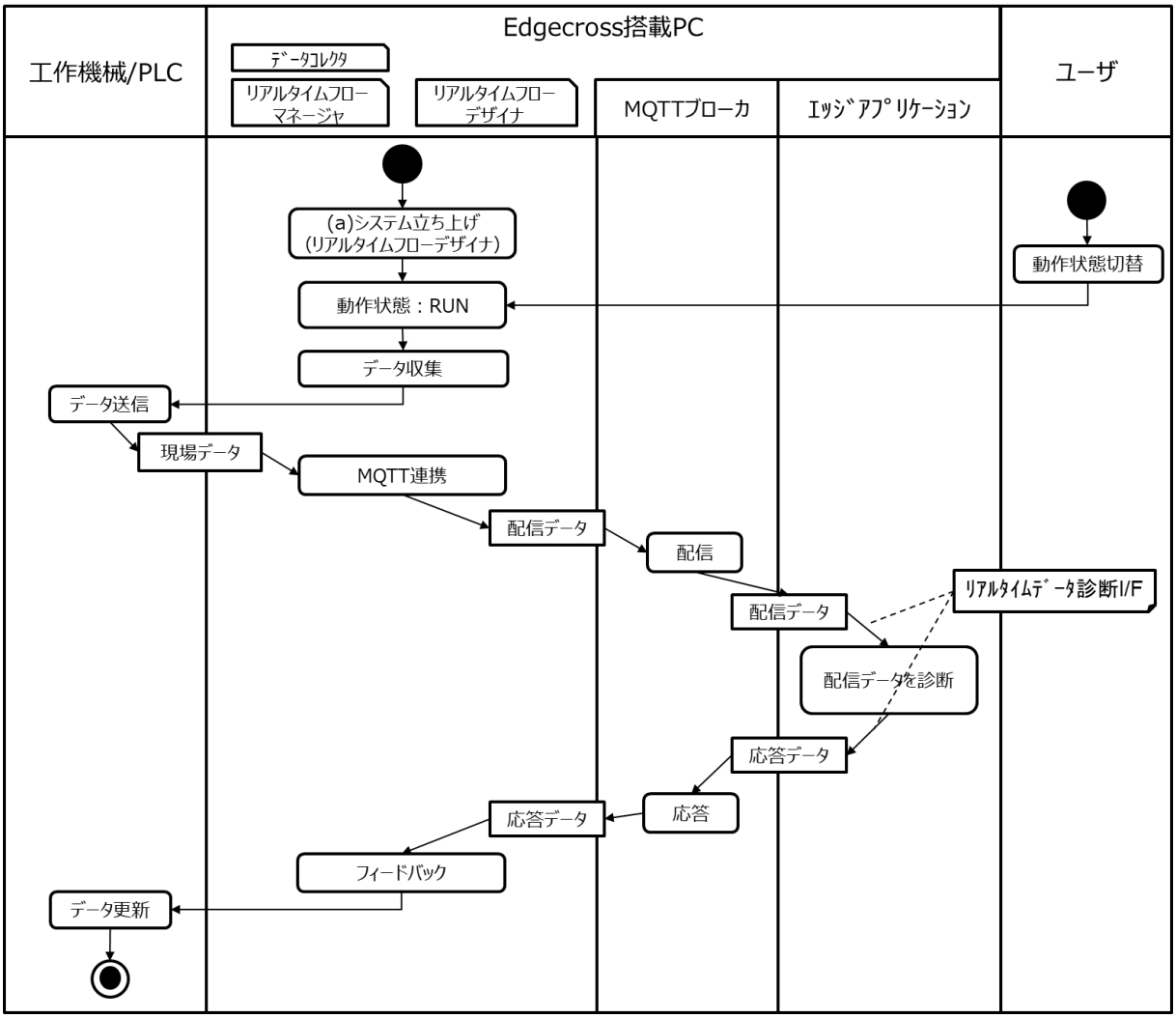
② リアルタイムフローマネージャはデータコレクタ経由で、工作機械や PLC からのデータ収集を行います。

③ 収集した現場データは、リアルタイムフローマネージャの MQTT 配信機能によりクラウドサービス上の MQTT ブローカに送信されます。

④ クラウドサービス上のエッジアプリケーションは、リアルタイムデータ配信 I/F により、MQTT ブローカから配信データを取得し、表示・分析などを行います。

(g) エッジアプリケーションからのフィードバック

リアルタイムフローマネージャのデータ診断機能（MQTT 連携）により、リアルタイムデータ診断 I/F（MQTT）に対応しているエッジアプリケーションにデータを配信し、診断・フィードバックを行うケースです。



※このケースでは、リアルタイムフローマネージャを使用するため、事前に(a)システム立ち上げ（リアルタイムフローデザイナを使うケース）を実施します。

① ユーザはリアルタイムフローデザイナからリアルタイムフローマネージャの動作状態を RUN に切り替えます。

② リアルタイムフローマネージャはデータコレクタ経由で、工作機械や PLC からのデータ収集を行います。

③ 収集した現場データは、リアルタイムフローマネージャの MQTT 連携機能により、MQTT ブローカに渡されます。

④ エッジアプリケーションは、リアルタイムデータ診断 I/F により MQTT ブローカから配信データを受信し、診断を行います。

⑤ 診断を完了したときの応答データは、エッジアプリケーションからリアルタイムデータ診断 I/F により MQTT ブローカに送信します。

⑥ リアルタイムフローマネージャは、MQTT 連携機能により、応答データを受信し、フィードバック実行機能により、データコレクタを介して、工作機械／PLC の機器データを更新します。

2.5.3 想定される脅威

2.5.1 システム構成に示すユースケースにおいて想定される脅威を表 2-2 に示します。

同表における脅威カテゴリは、IPA が刊行する「制御システムのセキュリティリスク分析ガイド 第 2 版」における脅威の分類に則っており、同ガイドに記載されている脅威カテゴリの因果関係を図 2-5 に示します。なお、パターン 1、パターン 2 は、それぞれ 2.5.1 に記載した「大規模工場」、「小規模工場」を示し、想定される脅威が該当するパターンには「〇」を記すとともにそのアタックサーフェスを記載しています。また、各脅威に対するセキュリティ対策を指し示すため、後述する 3. 構築におけるセキュリティ対策と 4. 運用におけるセキュリティ対策の該当章節番号を記載しています。

以下、表 2-2 の脅威カテゴリ毎に概要とインシデントを記載します。なお、Edgecross 搭載 PC を中心とした工場全体のセキュリティ脅威は、別冊に記載しています。

(1) 不正アクセス

悪意のある第三者がネットワーク経由で Edgecross 搭載 PC に侵入し、格納されている情報を改ざんする等の攻撃を実行する。

(2) 物理的侵入

悪意のある第三者や故意の内部関係者(社員や協力者のうち、Edgecross 搭載 PC へのアクセス権を有する者)が、入室が制限された Edgecross 搭載 PC 設置場所に不正侵入する。あるいはラックや箱内等により物理的アクセスが制限された Edgecross 搭載 PC の制限を解除する。

(3) 不正操作

(2)の後、Edgecross 搭載 PC のコンソール等を直接操作して、不正なソフトウェアを Web サイトからダウンロードしてインストールする等の攻撃を実行する。

(4) 過失操作

内部関係者の過失操作を誘発し、Edgecross 搭載 PC の OS に対して不正な設定を行う等の攻撃を実行する。Edgecross 搭載 PC に対して、正規の USB メモリや SD カード等の外部記憶装置を接続した結果、意図せずマルウェア感染等の攻撃が実行される。

(5) 不正媒体・機器接続

悪意のある第三者や故意の内部関係者が不正に持ち込んだ外部記憶装置を Edgecross 搭載 PC に接続し、生産情報やログを窃取する等の攻撃を実行する。

(6) プロセス不正実行

(1), (3), (4)により攻撃対象の Edgecross 搭載 PC 上に存在する正規のプログラムやコマンド、サービス等のプロセスを不正に実行する。

(7) マルウェア感染

(1), (3), (4), (5)により攻撃対象の Edgecross 搭載 PC にマルウェアを感染・動作させる。

(8) 情報窃取

(6)や(7)により Edgecross 搭載 PC 内に格納されている情報(生産情報、ログ、ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報)を窃取する。

(9) 情報改ざん

(6)や(7)により Edgecross 搭載 PC 内に格納されている情報を改ざんする。

(10)情報破壊

(6)や(7)により Edgecross 搭載 PC 内に格納されている情報を破壊する。

(11)不正送信

(6)や(7)により Edgecross 搭載 PC が工作機械や PLC 等の装置に不正な制御コマンド（設定値変更、電源断等）や不正なデータ（不正な値、不正な形式等）を送信する。

(12)機器停止

(6), (7), (13)により Edgecross 搭載 PC の機能を停止する。

(13)高負荷攻撃

(7)によりマルウェアに感染した Edgecross 搭載 PC が DDoS 攻撃等に加担して、File Server 等の他の機器に大量データを送信し、同機器の正常動作を妨害する。また、感染したマルウェアが Edgecross 搭載 PC の処理能力以上の処理を要求し、同 PC の正常動作を妨害する。

(14)窃盗

(2)の後、Edgecross 搭載 PC を窃盗する。

(15)盗難・廃棄時の分解による情報窃取

(14)の後、盗難にあった Edgecross 搭載 PC や廃棄した同 PC が分解され、PC 内部に保存されていた情報が窃取される。

(16)盗聴・通信データ改ざん

悪意のある第三者が Edgecross 搭載 PC–File Server 間のネットワーク上に流れる情報を盗聴したり、改ざんしたりする。

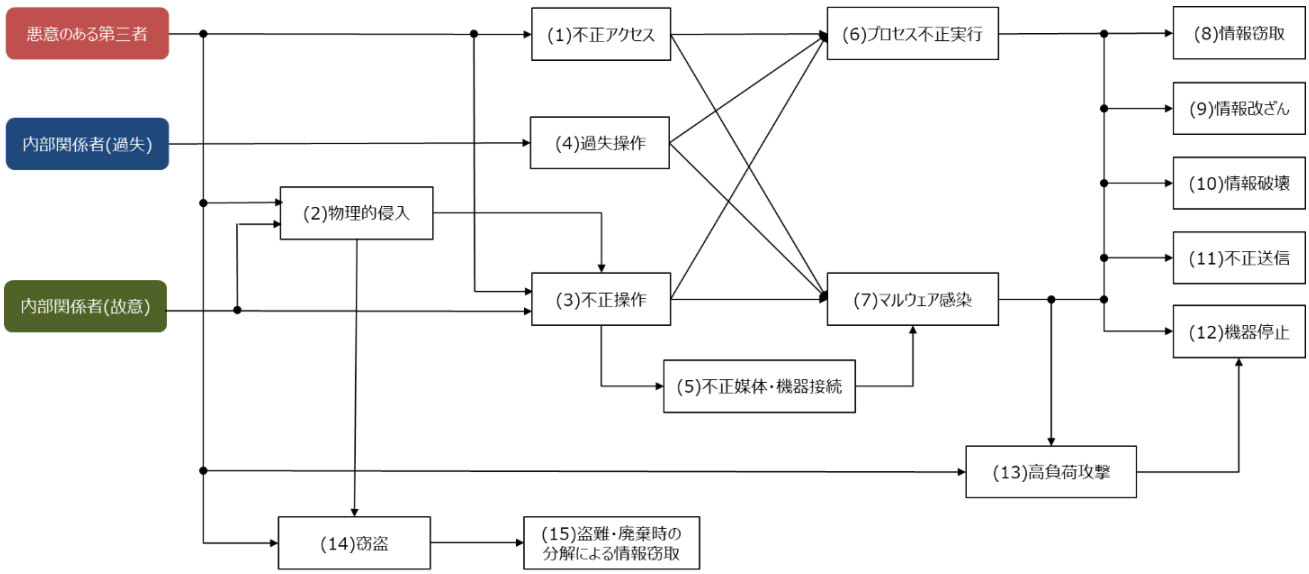


図 2-5 脅威カテゴリの因果関係

表 2-2 Edgecross ユースケースにおける想定脅威一覧

No.	脅威カテゴリ	想定される脅威	STRIDE 分類 ※	パターン1 (Attack Surface)	パターン2 (Attack Surface)	対策
1	01. 不正アクセス	パスワード窃取や脆弱性利用などの手段により、工場外回線(インターネット)からEdgecross搭載PC内部へ不正アクセスされる。	なりすまし	○ (インターネット-Edgecross)		3.2.2 (1)(3) 3.4.2 (1) 3.4.3 (1) 3.4.4 (1) 3.5 (4)(6)(12) 4.1
2		外部の不正者に乗っ取られた正規のサーバ・PCからEdgecross搭載PC内部に不正アクセスされる。	なりすまし	○ (サーバ-Edgecross)		3.5 (5)
3		クライアントPCなどの工場内機器、不正接続された機器、工場内に感染したマルウェアなどにより、情報制御ネットワーク内からEdgecross搭載PC内部へ不正アクセスされる。	–	○ (機器-Edgecross)	○ (機器-Edgecross)	3.5 (5)(9)
4		Edgecross搭載PCへの不正なアクセスや操作があっても、気がつくのが遅れたり、見逃したりしてしまうことで被害が拡大していく。	–	○ (人/機器-Edgecross)	○ (人/機器-Edgecross)	3.5 (5)(6)
5		Edgecross搭載PCをリモート操作できる端末に通信相手を認証する仕組みがなく、不正な命令を実行してしまい、Edgecross搭載PCが不正操作される。	なりすまし	○ (リモート端末-Edgecross)	○ (リモート端末-Edgecross)	3.5 (5)(12)
6		MESになりすました攻撃者から、Edgecross搭載PCが不正な指示を受信する。	なりすまし	○ (MES-Edgecross)	○ (MES-Edgecross)	3.5 (6)
7	02. 物理的侵入	Edgecross搭載PCをリモート操作できる端末が設置されている区画への入退室が適切に管理されておらず、所定の作業員以外によってEdgecross搭載PCを不正操作される。	–	○ (リモート端末-Edgecross)	○ (リモート端末-Edgecross)	3.2.1 (2)
8	03. 不正操作	正規利用者が離席中に、操作中のEdgecross搭載PCに操作権限を持たない作業員がアクセスする。	なりますし	○ (人-Edgecross)	○ (人-Edgecross)	3.2.2 (1)
9		Edgecross搭載PCをリモート操作できる端末が専用の管理区画に設置されておらず、所定の作業員以外によってEdgecross搭載PCを不正操作される。	なりすまし	○ (リモート端末-Edgecross)	○ (リモート端末-Edgecross)	3.2.1 (2) 3.4.2 (1) 3.4.3 (1)
10		作業を許可された作業員以外により、Edgecross搭載PCの画面を盗み見される。	–	○ (人-Edgecross)	○ (人-Edgecross)	3.2.1 (2)
11		作業員になりすました攻撃者の直接操作により、不正なソフトがEdgecross搭載PCにインストールされる。	なりすまし	○ (人-Edgecross)	○ (人-Edgecross)	3.2.2 (1) 3.3.1
12		脆弱性を突いた権限昇格攻撃により、不正なソフトがEdgecross搭載PCにインストールされる。	権限昇格	○ (人/機器-Edgecross)	○ (人/機器-Edgecross)	3.3.1 3.4.4 (1) 4.1
13		作業員により、インターネットから取得した不正なソフトがEdgecross搭載PCにインストールされる。	–	○ (人-Edgecross)		3.3.1 3.3.2
14	04. 過失操作	正規アクセス権限者の操作誤りにより、Edgecross搭載PCへの異常設定、情報喪失、ソフト不正実行などが発生する。	–	○ (人-Edgecross)	○ (人-Edgecross)	3.3.1
15	05. 不正媒体・機器接続	Edgecross搭載PC、あるいはEdgecross搭載PCの外部通信経路に、不正機器(USBデバイス、イーサネットデバイス、無線デバイスなど)を接続され、不正操作が行われる。	–	○ (機器-Edgecross)	○ (機器-Edgecross)	3.2.2 (2) 3.5 (3)(8)(11)(12)
16	06. プロセス不正実行	不正アクセス、不正操作、マルウェア感染などの結果、Edgecross搭載PC内で意図しないプロセスが実行される。	–	○ (人/機器-Edgecross)	○ (人/機器-Edgecross)	3.4.3 (4)
17	07. マルウェア感染	セキュリティチェックがされていない外部持込端末(保守端末)を接続され、外部持込端末(保守端末)経由で、Edgecross搭載PCがマルウェアに感染する。	–	○ (外部端末-Edgecross)	○ (外部端末-Edgecross)	3.3.1 3.5 (9)(12)
18		ネットワーク機器の空きポートが接続可能な状態で放置されており、不正端末を接続され、Edgecross搭載PCにマルウェアを送り込まれる。	–	○ (機器-Edgecross)	○ (機器-Edgecross)	3.3.1 3.5 (5)
19		サーバにセキュリティチェックがされていない外部媒体(USB等)や外部持込端末(保守端末)を接続され、それらを経由してEdgecross搭載PCがマルウェアに感染する。	–	○ (外部端末-Edgecross)	○ (外部端末-Edgecross)	3.3.1 3.5 (8)(9)(12)
20		FileServerから取得したファイルを通してEdgecross搭載PCがマルウェアに感染する。	–	○ (FileServer-Edgecross)	○ (FileServer-Edgecross)	3.3.1 3.5 (4)(5)
21		インターネットから取得したファイルを通してEdgecross搭載PCがマルウェアに感染する。	–	○ (インターネット-Edgecross)		3.3.1 3.5 (4)
22		Edgecross搭載PCがマルウェアに感染し、他機器へ感染が拡大することによって生産に影響を及ぼす。	–	○ (Edgecross-機器)	○ (Edgecross-機器)	3.3.1 3.5 (5)
23		感染したマルウェアにより不正なソフトがEdgecross搭載PCにインストールされる。	–	○ (人/機器-Edgecross)	○ (人/機器-Edgecross)	3.3.1
24	08. 情報窃取	不正アクセス、不正操作、マルウェア感染などの結果、Edgecross搭載PC内の情報が窃取/改ざん/破壊される。	情報漏洩	○ (人/機器-Edgecross)	○ (人/機器-Edgecross)	3.3.2
25	09. 情報改ざん	作業員になりすました攻撃者の直接操作により、Edgecross搭載PCの設定が不正に変更される。	改ざん	○ (人-Edgecross)	○ (人-Edgecross)	3.3.2
26	10. 情報破壊	不正アクセスにより、Edgecross搭載PC内にある必要なログデータを消去される。	否認	○ (人/機器-Edgecross)	○ (人/機器-Edgecross)	3.3.1
27		Edgecross搭載PC内の認証情報の削除により、サービス妨害される。	–	○ (人/機器-Edgecross)	○ (人/機器-Edgecross)	3.3.1
28	11. 不正送信	Edgecross搭載PC経由で、PLCに適切ではない目標値を入力されることにより、設備が不正な動作をして破壊される。	–	○ (Edgecross-PLC)	○ (Edgecross-PLC)	3.4.2 (1)(2)(3) 3.4.3 (1)(2)(3)(5)(6) 3.5 (5)
29		Edgecross搭載PCがマルウェアに感染し、不正なコマンドが実行され、生産に悪影響を及ぼす。	–	○ (Edgecross-PLC)	○ (Edgecross-PLC)	3.3.1 3.5 (5)
30		Edgecross搭載PCに感染したマルウェアからPLCに不正な指示が送信される。	–	○ (Edgecross-PLC)	○ (Edgecross-PLC)	3.3.1 3.5 (5)
31		感染したマルウェアにより、不正なファイルがEdgecross搭載PCからFileServerにアップロードされる。	–	○ (Edgecross-FileServer)	○ (Edgecross-FileServer)	3.3.1 3.5 (4)(5)
32		作業員になりすました攻撃者の直接操作により、不正なファイルがEdgecross搭載PCからFileServerにアップロードされる。	なりすまし	○ (Edgecross-FileServer)	○ (Edgecross-FileServer)	3.2.2 (1) 3.5 (4)(5)
33		感染したマルウェアにより、Edgecross搭載PC内の情報がインターネット外に送信される。	–	○ (Edgecross-インターネット)		3.3.1 3.3.2 3.4.2 (4) 3.4.3 (2)(7) 3.5 (4)(5)(6)
34		作業員になりすました攻撃者の直接操作により、Edgecross搭載PC内の情報がインターネット外に送信される。	なりすまし	○ (Edgecross-インターネット)		3.2.2 (1) 3.3.2 3.4.2 (4) 3.4.3 (2)(7) 3.5 (4)(5)(6)(12)
35		正規のサーバ・PCに偽装したサーバやPCを接続し、Edgecross搭載PCからデータを送信させる。	なりすまし	○ (Edgecross-サーバ)	○ (Edgecross-サーバ)	3.3.2 3.4.2 (4) 3.4.3 (2)(7) 3.5 (4)(5)
36	12. 機能停止	作業員になりすました攻撃者の直接操作により、Edgecross搭載PCが停止状態にさせられる。	なりすまし	○ (人-Edgecross)	○ (人-Edgecross)	3.2.2 (1)
37		感染したマルウェアにより、Edgecross搭載PCが過負荷・停止状態にさせられる。	–	○ (人/機器-Edgecross)	○ (人/機器-Edgecross)	3.3.1
38	13. 高負荷攻撃	ITゲートウェイやデータモデル管理機能に対して、高負荷な通信を行い、サービス妨害を行う。	DoS攻撃	○ (インターネット-Edgecross)	○ (インターネット-Edgecross)	3.5 (4)(5)
39	14. 窃盗	工場内に人為的に侵入され、Edgecross搭載PCに対して物理攻撃、窃盗などが行われる。	–	○ (人-Edgecross)	○ (人-Edgecross)	3.2.1 (2)
40	15. 盗難・廃棄時の分解による情報窃取	廃棄・窃盗されたEdgecross搭載PCのリバースエンジニアリングによる情報窃取が行われる。	情報漏洩	○ (人-Edgecross)	○ (人-Edgecross)	3.3.2
41	16. 盗聴・通信データ改ざん	Edgecross搭載PCからFileServerへの送受信データに漏えい・改ざんが行われる。	情報漏洩 改ざん	○ (Edgecross-FileServer)	○ (Edgecross-FileServer)	3.3.2
42	17. Windows関連	互換性検証がされないまま、予期しないWindowsUpdateが実行され、予期せぬShutdown、Rebootが発生したり、システムに障害が発生する。	–	○	○	3.2.2 (3) 4.1 (3)
43		WindowsUpdateが実行され、Edgecross搭載PCのリソースが枯渇し、必要な処理が実行できなくなる。	–	○	○	3.2.2 (3) 4.1 (3)
44		Windowsテレメトリーの負荷が高く、必要な処理が実行できなくなる。	–	○	○	3.2.2 (3) 4.1 (3)
45		WindowsUpdateが実施されなくて、既知の脆弱性が累積していく。	–		○	3.2.2 (3) 3.5 (7) 4.1 (3)
46		Windowsのサポートが終了したまま利用していくことによる、既知の脆弱性の累積。	–	○	○	3.2.2 (3) 3.5 (7) 4.1 (3)

※STRIDE とは、Spoofing(なりすまし)、Tampering(改ざん)、Repudiation(否認)、Information disclosure(情報漏洩)、Denial of service(DoS 攻撃)、Elevation of privilege(権限昇格)の頭文字をとった脅威分析手法のひとつ。

3. 構築におけるセキュリティ対策

3. 1 要点

Edgecross システムは、FA 領域と IT 領域を橋渡しする境界に位置します。そのため、セキュリティ観点上、生産現場設備と IT システムの両方のアクセスを考慮する必要があります。

また、Edgecross 基本ソフトウェアにてユーザが動作を規定することができ、加えて、データコレクタ、エッジアプリケーション、プラグインなど、様々なソフトウェアを組み合わせることにより、自由度の高いシステムを構築することができます。セキュリティ確保のため、どのようなシステムを構築し、どのように守るかを、ユーザが主導する必要があります。

Edgecross システムの構築にあたり、守るべき対象を明確にし、その対象を守れるように以下の(1)～(5)の観点でシステム設計を行ってください。

「IoT セキュリティガイドライン」には下記の要点が記載されています。Edgecross システムにおいても、「IoT セキュリティガイドライン」を参照して構築を行ってください。

(1) 個々でも全体でも守れる設計

外部インタフェース経由/内包/物理的接触によるリスクに対して個々の機器・システムで対策を検討してください。また、個々の機器・システムで対応しきれない場合は、それらを含む上位の IoT 機器・システムで対策を検討してください。

(2) つながる相手に迷惑をかけない設計

機器・システムの異常を検知できる設計を行い、異常を検知したときの適切な振る舞いを検討してください。

(3) 安全安心を実現する設計の整合性の確保

安全安心を実現するための設計を見える化してください。また、安全安心を実現するための設計の相互の影響を確認してください。

(4) 不特定の相手とつなげられても安全安心を確保できる設計

機器・システムがつながる相手やつながる状況に応じてつなぎ方を判断できる設計を検討してください。

(5) 安全安心を実現する設計の検証・評価

つながる機器やシステムは、IoT ならではのリスクも考慮して安全安心を実現する設計の検証・評価を行ってください。

脅威の低減には、人的、物理的、さらには接続されるネットワーク等の様々な対策を多層に施すのが望ましいと考えます。以下のようなセキュリティ対策をお客様にて導入されることを推奨しています。

3. 2 ハードウェア/OS

3.2.1 ハードウェア

(1) 調達

Edgecross は様々なメーカーの産業用 PC に搭載可能です。安全・安心な機器構築のため、産業用 PC は十分に信頼できる調達元から調達してください。

調達元に機器のサポートを受ける窓口があり、かつ容易にアクセス可能なこと、機器の諸元やファームウェアのアップデートなど技術情報が公開されていること等を確認してください。

なお、信頼できるメーカーの製品であっても、流通経路に問題がある可能性についても留意してください。例えば、悪意をもってマルウェアを混入させた中古販売品が販売されているケースなどが考えられます。

Edgecross コンソーシアムでは、Edgecross 基本ソフトウェア Windows 版の動作を認定した、推奨産業用 PC を紹介しています。詳しくは Edgecross コンソーシアムのホームページ (https://www.edgecross.org/)をご覧ください。

(2) 設置

産業用 PC を設置する際には、物理的攻撃に対する防護にも留意してください。

・セキュリティワイヤのロックや、施錠できる PC ラックによる物理的盗難の対策
・USB/LAN 物理ロックによる物理的接続の対策
・オペレータの入出制限

これらの対策は使用環境によって変わりますので、環境に応じて実施してください。

(3) 初期設定

産業用 PC にはセキュリティに関するいくつかの設定があります。使用環境および動作させるソフトウェアにあわせて適切に設定してください。代表的な設定項目を下記に列挙します。詳しくは産業用 PC のマニュアル等を参照してください。

・BIOS パスワード、HDD パスワードなどのパスワード設定
・ブートドライブの設定
・USB 設定
・Wake on Lan など外部制御を可能にする機能の設定
・TPM などのセキュリティチップの設定
※TPM の使用を推奨します。

(4) アップデート

CPU やチップセットのファームウェア・BIOS、ストレージやネットワークカードのファームウェアやドライバなどを適切にアップデートしてください。アップデートソフトウェアの取得は、信頼できる Web サイトを利用するなど、改ざんされていないことが保障できる手段をとってください。

また、各ハードウェアが出荷されてから実際に使用するまでの期間に、ファームウェア等が更新されている可能性があることを留意し、最新のハードウェアであっても、構築時に必ずファームウェア等の更新情報を確認してください。

(5) 運用

ハードウェア(および付帯ソフトウェア)のサポート期間を確認してください。サポート期間内での運用を推奨します。

サポート期間を過ぎた継続運用を行わざるを得ない場合、現用機器のサポート期間が過ぎていることのリスクを認識した上で適切な管理を行ってください。

機器が未使用状態となり管理対象から外れる場合、非管理機器が動作していることがセキュリティリスクとなる可能性がありますので、該当機器の電源を切ってください。

3.2.2 OS

Edgecross 基本ソフトウェア Windows 版は、Microsoft® Windows® 10 Operating System（以下、Windows）上で動作します。本章では、Windows の運用について基本的なガイドラインを記載しますが、実際の実施内容については Edgecross 機器の運用環境に応じて適切に選択してください。

なお、Windows の機能や用語などは今後のアップデートで変更される可能性もあります。詳しくは Microsoft 社のホームページなどの情報を参照してください。

(1) アカウント・パスワード

Windows には、ユーザ毎にアカウントおよびパスワードを管理する機能が備わっています。ユーザの役割に応じてアカウントを設定するとともに、他者が推定しにくいパスワードを設定するなど、適切な管理を実施してください。

ユーザ認証にあたっては、Windows アカウント・パスワードの他、PIN 認証、バイオメトリックス認証や、それらを組み合わせた二段階認証/多要素認証を利用することも可能です。

Windows のシステムに重要な変更が行われる場合、管理者権限ユーザに許可を求めるセキュリティ機能（ユーザアカウント制御機能）が備わっています。本機能を有効にすることを推奨します。

Windows には、各種のユーザ名・パスワードを記憶する機能が備わっています。ネットワークアクセスの資格情報や、Web ページのユーザ名・パスワードなどの情報をシステム内に記憶することは、セキュリティ上のリスクに繋がる可能性がありますので、必要がない限り記憶させないことを推奨します。

(2) 設定

Windows は様々なアプリケーションやサービスを内包しています。Edgecross の運用にあたり、不要な機能は無効にすることを推奨します。特に、カメラ機能やマイク機能など Edgecross に不要なパーソナルユース機能は無効化してください。また、USB や Bluetooth など外部からの物理アクセスは、可能な限り制限もしくは無効化してください。

マルウェア対策として、Windows に搭載されたセキュリティ機能を利用するか、もしくは、サードパーティ製セキュリティソフトウェアを導入してください。また、パーソナルファイアウォールにて不要なネットワークアクセスを遮断することを推奨します。

(3) アップデート

Windows は、Windows Update により更新プログラムを適用して、常に最新の状態に保つための機能が備わっています。汎用的に利用する環境では常に最新の状態に更新することを推奨します。

ただし、更新プログラムには、再起動を伴うもの、更新に時間がかかるものがあります。動作環境と相性の問題や、不具合があるものも存在するため、実際には Edgecross の運用に問題ないことを確認してから更新することを勧めます。

特定の用途で利用する産業用 PC などでは、更新プログラムの適用を一時延期し、更新プログラムの動作検証用に試験用機器を用意するなどの対策が有効です。Microsoft 社は組織内の Windows 更新プログラムの適用を制御するためのソリューションとして、Windows Server Update Services (WSUS)を提供しています。

Windows 更新プログラムの入手元として WSUS を選択する場合、グループ ポリシーを使って Windows PC を WSUS サーバに向けるように設定します。Windows Update から更新プログラムが定期的に WSUS サーバにダウンロードされ、WSUS 管理コンソール または グループ ポリシーを通じて 管理、承認、展開され、企業の更新プログラムの管理が合理化されます。

もしタイムリーな Windows Update が行えない場合、次世代 IPS を活用することで仮想パッチによる一時的な緩和策をとることができます。

3. 3 セキュリティソフトウェア

セキュリティソフトウェアは、コンピュータセキュリティ対策のために用いられるアプリケーションソフトウェアの総称で、マルウェアの侵入やそれによる感染を防止したり、不正アクセスや情報窃取/改ざん、他のシステムに対する攻撃の踏み台を防いだりする目的で使われます。Edgecross 基本ソフトウェアおよび認定製品、推奨産業用 PC 等において、お客様にて適切なセキュリティソフトウェアの導入を推奨します。

3. 3. 1 マルウェア対策ソフトウェア

具体的な検討にあたっては、システムの用途や運用に沿ったセキュリティソフトウェアの選定が必要になります。マルウェア対策ソフトウェアとして、以下のような方式がありますので参考までに記します。詳しくは、製品販売元や販売代理店にお問い合わせのうえ、導入を進めてください。

ブラックリスト方式
強み: 豊富な多層防御技術の実装。
弱み: 最新脅威に対応するタイムリーアップデート。OS のサポートライフサイクルに準じた製品サポート。

ホワイトリスト方式(特定用途化によるロックダウン)
強み: サポートライフサイクルの長さ。システム更新サイクルに準じたアップデート。リソースの平準化。
弱み: システム特性とのマッチング(頻繁な実行ファイルの変更処理や書き出しがある場合など)

万が一、マルウェア等に感染した場合には、一般の Windows マシンが感染した場合と同様、例えば以下のような影響が起こります。このような症状が疑われる場合、アプリケーションのインストールを行わずにマルウェアの有無を確認することができる USB 型マルウェアチェック・駆除ツールがあるので、必要に応じて活用されることを推奨します。

・不正なソフトウェアがインストールされる
・各種データの改ざん、消失、漏洩
・不正なファイル暗号化、脅迫文の表示
・他のシステムへの攻撃の踏み台にされる

不正なファイル暗号化、脅迫文の表示は、いわゆるランサムウェア感染による影響であり、対策としてバックアップの取得が有効です。

マルウェア対策ソフトウェアの導入後は、次の 3 点について考慮しておくことも推奨します。

(1) 契約の更新
マルウェア対策ソフトウェアには、ライセンス契約により、1 年や複数年といった利用期間の制限があるケースがあります。システム稼働中は継続して使用できるようにライセンス契約を更新することが必要です。

(2) アップデート
マルウェア対策ソフトウェアは、外的脅威の変化に対応するために機能向上を目的としたアップデートが必要になる場合があります。マルウェアの検出パターンは日々、更新されることが多いため、ブラックリスト方式のマルウェア対策ソフトウェアを利用される場合は定期的なアップデートが必要です。ホワイトリスト型のマルウェア対策ソフトウェアを利用される場合は、システム更改のタイミングでリスト更新が必要になります。マルウェア対策ソフトウェアの脆弱性が公開された際は、製品バージョンアップやセキュリティパッチが別途提供される場合があります。脆弱性情報に注意のうえ適用することを検討してください。

(3) システムスキャン
定期的に、システム全体をスキャンします。スキャン実行中は CPU 負荷が大きくなるため、システムの稼働状況に応じて実行することを推奨します。マルウェア対策ソフトウェアをインストールする常駐型と、ソフトウェアのインストールが必要ない非常駐型(USB 型マルウェア検査・復旧ツール)などがあります。

3.3.2 その他のセキュリティソフトウェア

不正アクセスや踏み台の対策として、OS 内蔵パーソナルファイアウォールやサードパーティ製通信アクセス制御ソフトウェアの導入を推奨します。

情報窃取/改ざん対策のうち、Edgecross 搭載 PC と外部との通信における同対策は 3. 4 Edgecross 基本ソフトウェアの通信暗号化を参照ください。Edgecross 搭載 PC 内部のデータに対する情報窃取/改ざん対策はサードパーティ製の暗号化ソフトウェアや改ざん対策ソフトウェアの導入を推奨します。関連して、暗号鍵や証明書の配布・管理・廃棄は、Edgecross システムの規模が大きいほど煩雑なことから、必要に応じてサードパーティ製の鍵管理ソフトウェアの活用も推奨します。

3. 4 Edgecross 基本ソフトウェア

3.4.1 構成

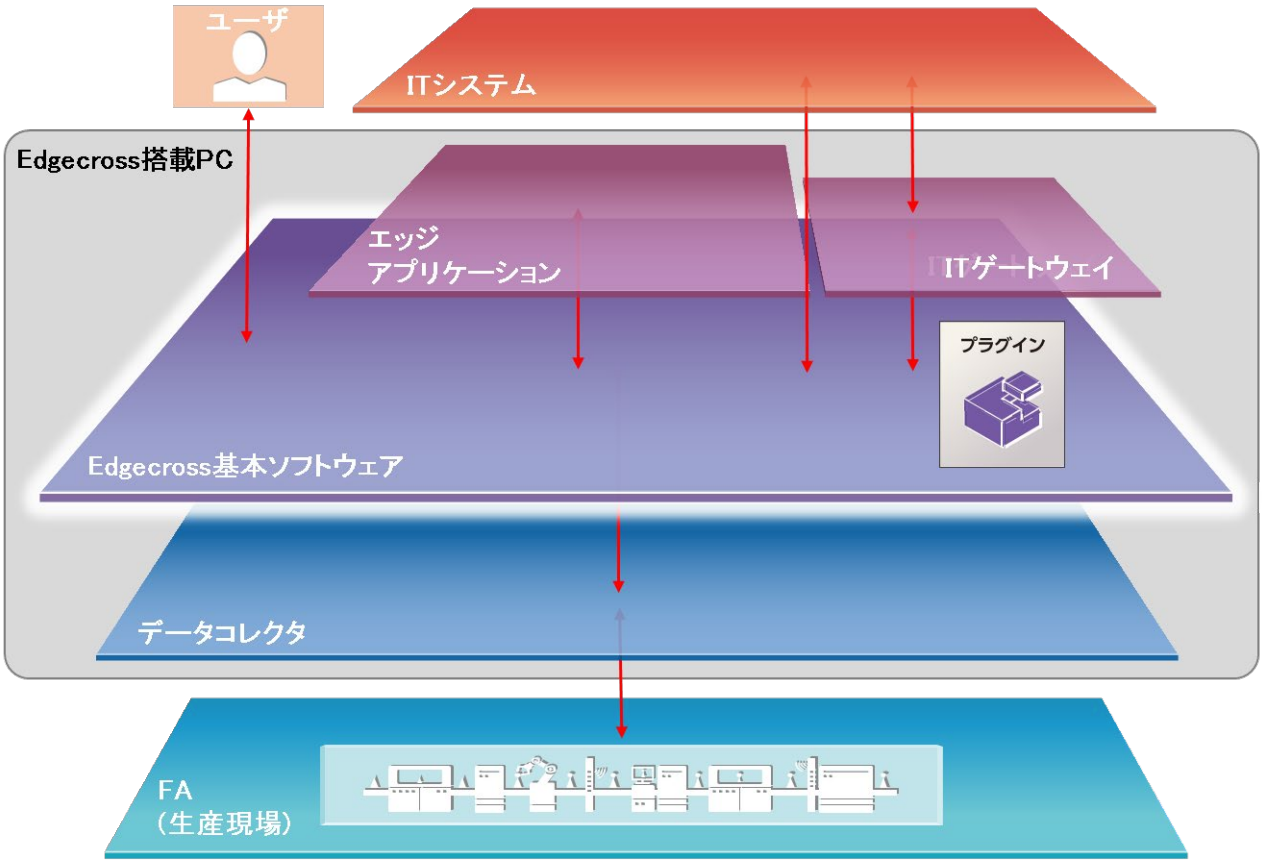


図 3-1 Edgecross ソフトウェア構成概略図

上図は Edgecross ソフトウェア構成の概略図です。

Edgecross 基本ソフトウェアは、データコレクタを通じて、生産現場設備のデータ収集やフィードバックを行います。エッジアプリケーションでは、データの分析・診断を行います。また、外部 IT システムとの間でデータのやり取りを行います。

データコレクタは、生産現場設備を直接制御可能なソフトウェアです。データコレクタ、および、データコレクタに(Edgecross 基本ソフトウェアを通じて)アクセス可能なソフトウェアであるエッジアプリケーションおよび IT ゲートウェイは、十分に信頼できるソフトウェアを使用してください。

外部の IT システムから Edgecross へのアクセスには、2 種類の形態があります。

1つは、Edgecross 基本ソフトウェアへ直接アクセスする形態です。この形態では、Edgecross 基本ソフトウェアとエッジアプリケーションとのインタフェースを外部 IT システムへ公開することにより実現します。インタフェースを外部に公開することのセキュリティ上のリスクについて留意してください。インタフェースの詳細については、3.4.2 データモデル管理、および、3.4.3 リアルタイムデータ処理を参照してください。

もう1つは、IT ゲートウェイを介して Edgecross 基本ソフトウェアにアクセスする形態です。この形態では、Edgecross へのアクセスが IT ゲートウェイ経由に限定されます。また、IT ゲートウェイにセキュリティ機能が備わっていれば、その機能を利用することも可能です。

ユーザは OS にログインして Edgecross 基本ソフトウェアの各種操作を行います。

Edgecross 基本ソフトウェアの操作では、情報閲覧のみではなく、データコレクタを通じた生産現場設備へのアクセスも可能です。Edgecross 基本ソフトウェアにアクセス可能なユーザは、生産現場設備にアクセス可能であること(即ち、生産現場設備の不正操作が可能であること)に留意してください。Edgecross 基本ソフトウェ

アにはユーザ毎にアカウントを制御する機能はありませんので、OS のアカウント制御を利用してください。

表 3-1 Edgecross 基本ソフトウェアの構成

機能	ソフトウェア	内容
リアルタイムデータ処理	リアルタイムフローマネージャ	生産現場のデータのリアルタイム診断･フィードバックを実現する機能を実装したソフトウェアです。 データコレクタ（ネットワークを介し、生産現場のデータを収集するソフトウェア）を使用して、接続された機器、装置、またはラインのデータを収集し、データの加工および分析を行うことができます。また、プラグインを使用して、機能拡張を行うこともできます。 リアルタイムフローデザイナよりWindowsサービスとして起動/停止されます。
	リアルタイムフローデザイナ	リアルタイムフローマネージャの動作に必要な各種設定の作成、保存、表示、リアルタイムフローマネージャの動作開始/停止、および診断を行う機能を実装したソフトウェアです。
データモデル管理	マネジメントシェル	生産現場の機器、装置、またはラインに関するデータをモデル化し、階層構造として管理するソフトウェアです。 データコレクタを使用して、接続された機器、装置、またはラインのデータの読出し、データの書込みを行うことができます。 マネジメントシェルエクスプローラよりWindowsサービスとして起動/停止されます。
	マネジメントシェルエクスプローラ	マネジメントシェルが管理するデータモデルの設定および参照を行い、マネジメントシェルの動作開始/停止を担います。

Edgecross 基本ソフトウェアは、上表のソフトウェアで構成されています。詳細については、Edgecross 基本ソフトウェア Windows 版ユーザーズマニュアルを確認ください。

Edgecross 基本ソフトウェアは大別して、リアルタイムデータ処理とデータモデル管理の 2 つの機能があります。各々の機能の詳細と、セキュリティ上留意すべき点を以降に記載します。

3.4.2 データモデル管理

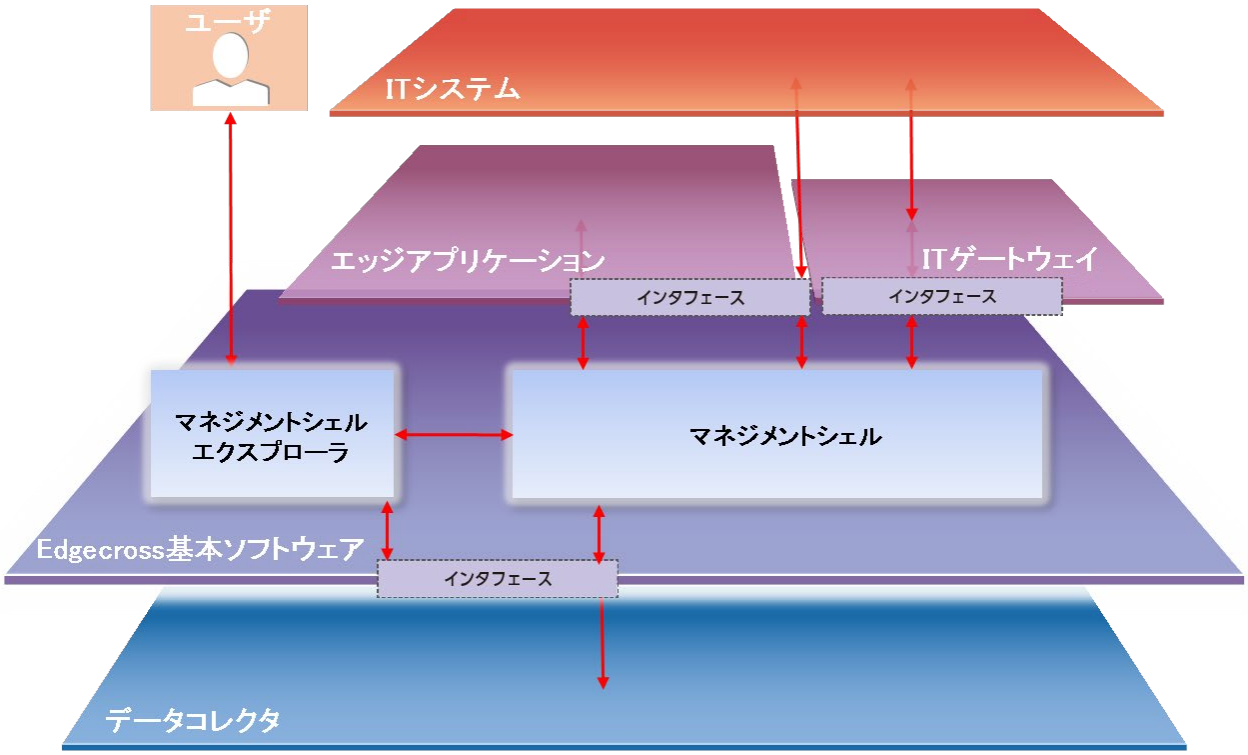


図 3-2 データモデル管理概略図

データモデル管理は、生産現場の機器、装置、またはラインに関するデータをモデル化し、階層構造として管理する機能で、データコレクタを使用して、接続された機器、装置、またはラインのデータの読出し、データの書込みを行うことができます。セキュリティの観点では、データコレクタを通じて生産現場機器を操作できる能力をもつことに留意してください。

データモデル管理を実行する主体には、ユーザ、エッジアプリケーション、外部 IT システムの3つがあります。

ユーザはマネジメントシェルエクスプローラをユーザインタフェースとして操作を行います。

エッジアプリケーションは、OPC UA サーバをアプリケーションインタフェースとして操作を行います。

外部 IT システムは、OPC UA サーバ、および、IT ゲートウェイをインタフェースとして操作を行います。

(1) マネジメントシェルエクスプローラ

マネジメントシェルエクスプローラを操作することで、マネジメントシェルが管理するデータモデルの設定および参照が可能です。即ち、生産現場の装置・機器からデータを読み出したり、書き込んだりすることができます。マネジメントシェルエクスプローラが不正なユーザに操作されると生産現場の停止やデータの漏洩・改ざん等を招く恐れがあります。その対策として、Edgecross 搭載 PC には信頼できるユーザのみがログイン(Windows へのログイン)できるように設定してください。

なお、マネジメントシェルの起動・停止、OPC UA サーバの設定などは、Windows の管理者権限をもつユーザ(もしくは管理者権限アカウントのパスワードを知るユーザ)のみが実行可能です。

(2) OPC UA

マネジメントシェルが OPC UA サーバとして動作し、OPC UA クライアントであるエッジアプリケーションに対してモデルアクセス I/F、データアクセス I/F を提供する機能(OPC UA 接続機能)を持ちます。この際、エッジアプリケーションのクライアント証明書を用いた認証を行うことが可能です。また、通信中は暗号化を行うことができます。

OPC UA インタフェースも、データコレクタを介した生産現場機器の操作が可能であることに留意してください。OPC UA のクライアント証明書の所有者も同様に、生産現場機器の操作が可能となります。

(3) エッジアプリケーション

エッジアプリケーションは OPC UA を経由して、データモデル管理の操作が可能です。また、Windows 上のアプリケーションとして動作するため、データモデル管理以外の動作も行うことも可能です。悪意のあるエッジアプリケーションを導入した場合、生産現場の停止やデータの漏洩・改ざん等を招く恐れがあります。

エッジアプリケーションは、Edgecross マーケットプレイスなど、信頼できる提供元から入手することを推奨します。

(4) IT ゲートウェイ

IT ゲートウェイは、外部 IT システムと Edgecross 基本ソフトウェアの間の通信を提供するソフトウェアコンポーネントになります。

IT ゲートウェイが利用可能であれば、前述の OPC UA は Edgecross 搭載 PC 外からのアクセスを禁止し、エッジアプリケーションを Edgecross 搭載 PC 内に配置する構成を推奨します。このような構成にすることにより、外部 IT システムからの Edgecross へのアクセスを IT ゲートウェイ経由に限定できるため、外部アクセスに対して堅牢なシステムを構築することが可能です。IT ゲートウェイの使用方法は、IT ゲートウェイのマニュアルを IT ゲートウェイ提供元から入手して参照ください。

3.4.3 リアルタイムデータ処理

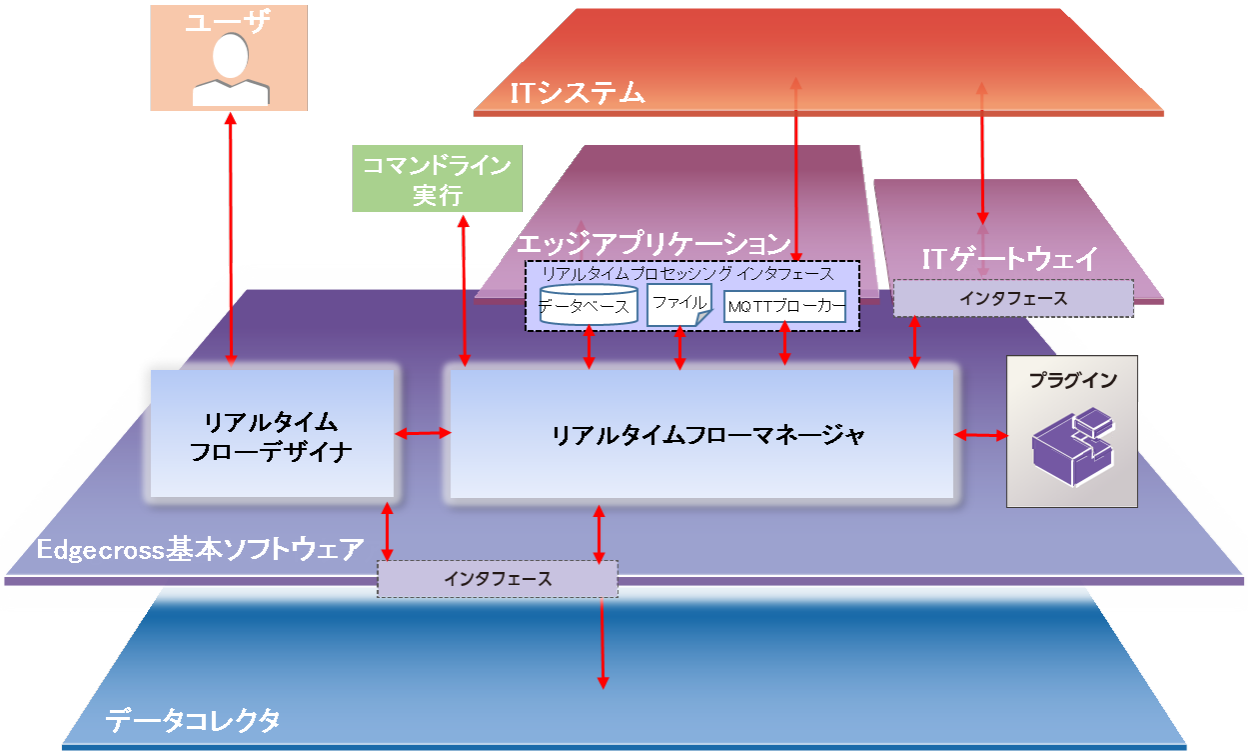


図 3-3 リアルタイムデータ処理概略図

リアルタイムデータ処理は、データコレクタより生産現場のデータを収集し、データの加工・分析を行います。データの加工・分析結果を（データコレクタを介して）生産現場機器にフィードバックすることもできます。更に IT システムとのデータ送受信が可能です。その他、OS 上でコマンドラインプログラムを実行する機能が備わっています。

リアルタイムフローマネージャはデータのフローを担うサービスであり、リアルタイムフローデザイナによりユーザが動作フローを作成します。

エッジアプリケーションやプラグインを導入することにより、データ加工・分析機能を拡張することができます。

エッジアプリケーションは MQTT やファイル、データベースを介してリアルタイムフローマネージャと通信が行われます。

プラグインはリアルタイムフローマネージャより直接呼び出されます。

外部 IT システムと Edgecross 基本ソフトは、エッジアプリケーションと同じインタフェース（MQTT、ファイル、データベース）、および、IT ゲートウェイ経由で通信します。

リアルタイムデータ処理もデータモデル管理と同様、不正なユーザ操作に備える必要があります。加えて、リアルタイムデータ処理は、生産現場のデータ、および、それらを加工したデータを扱い、動作を行うことに留意してください。即ち、不正ユーザによる操作の他に、不正データによる不正アクセスに備える必要があります。

例えば、MQTT へ配信されたデータを、データコレクタ経由で現場機器へ転送するフローを作成した場合、MQTT への不正データ配信により、現場機器の不正操作を引き起こす危険性があります。この場合、配信する現場機器へのデータは、信頼できるエッジアプリケーション内で生成した正常データに限定するようにフローを構築するなど、不正データアクセスの防止策を講じる必要があります。

(1) リアルタイムフローデザイナ

ユーザはリアルタイムフローデザイナを操作することで、リアルタイムフローマネージャの動作に必要な各種設定を作成することができます。データモデル管理と同様、リアルタイムフローデザイナが不正なユーザ

に操作され、リアルタイムフローマネージャの設定が書き換えられると生産現場の停止やデータの漏洩・改ざん等を招く恐れがあります。その対策として、Edgecross 搭載 PC には信頼できるユーザのみがログイン（Windows へのログイン）できるように設定してください。

(2) MQTT

MQTT は、リアルタイムフローマネージャからエッジアプリケーションへのデータ(収集データ、加工データ)配信、エッジアプリケーションから応答データの受信に使用されます。また、外部 IT システムとの通信にも使用されます。

MQTT は広く使われている通信規格ですが、不適切な設定などが原因で、しばしばセキュリティリスクを発生させています。2018 年に、インターネット上に脆弱な状態の MQTT サーバ（ブローカ）が何万台も発見されたという報告もあります。Edgecross システムにおいては、情報漏洩のみならず、不正なデータ注入による現場機器の不正操作に至る可能性もありますので、脆弱な状態で MQTT を公開しないように注意してください。

下記は、Edgecross システムでの MQTT の典型的な設定例になります。

①リアルタイムフローマネージャとエッジアプリケーションの間のデータ送受信

エッジアプリケーションおよび MQTT ブローカを Edgecross 搭載 PC 内に配備し、MQTT を PC 外に公開しない（パーソナルファイアウォールで、MQTT の PC 内部方向への通信を禁止する）設定とする。

②外部 IT システムへのデータ送信

外部 IT システム側に MQTT ブローカを配備して、Edgecross システムから外部 IT システムへのデータ送信に限定し、Edgecross と MQTT ブローカの間を TLS で暗号化する。

上記①②とも、Edgecross システム側の MQTT を外部公開せず、Edgecross システムへのデータ注入を避ける構成となります。

(3) ファイル/データベース

ファイルやデータベースをインタフェースとした通信は、MQTT の通信と同様の性質を持ちます。即ち、ファイルの公開は情報漏洩に、ファイルの書き込みは不正データ注入につながる可能性を持ちます。ファイル/データベースの公開は MQTT と同様に慎重に行ってください。

Edgecross 基本ソフトウェアの機能として、ファイルをリモート共有フォルダに配置することが可能です。共有フォルダには適切なユーザアカウント/パスワードを設定して下さい。

ユーザアカウントを使用しない共有フォルダを使用することもできますが、この場合、リモート共有フォルダのアクセス権が「ANONYMOUS LOGON」となることに留意して下さい。これは、リモート PC にアクセス可能な全ユーザが、認証なしで、ファイルにアクセス可能であることを意味します。

ユーザアカウントを使用しないリモート共有フォルダは十分信頼できるネットワーク内で限定して使用するか、もしくは、このようなリモート共有フォルダを使用しないことを推奨します。

(4) コマンドライン実行

リアルタイムフローマネージャには、指定したプログラムをコマンドラインから実行する機能があります。また、診断データをプログラム引数に指定することができます。指定したプログラムはシステム権限で動作するため、Edgecross 搭載 PC のほとんどの操作が可能になります。

診断データを引数に指定してコマンドラインプログラムを実行する機能は、セキュリティ観点で攻撃者から見ると、悪意あるデータを注入することでシステムを操作する機会を得る可能性があることを意味します。本機能を使用する際には、十分な検討を行い、悪意あるデータがプログラムで実行される可能性について考慮して下さい。

データ注入による攻撃について懸念が払拭できない場合、診断データをプログラム引数に指定する機能を使用しないことを推奨します。

(5) エッジアプリケーション

エッジアプリケーションは MQTT、ファイル、データベースを経由して、データの加工・分析を担いますが、Windows 上のアプリケーションとして動作するため、データ加工・分析以外の動作も行うことも可能です。悪意のあるエッジアプリケーションを導入すると、生産現場の停止やデータの漏洩・改ざん等を招く恐れがあります。

エッジアプリケーションは、Edgecross マーケットプレイスなど、信頼できる提供元から入手することを推奨します。

(6) プラグイン

プラグインは、リアルタイムデータ処理の実行制御下に置かれ、リアルタイムデータ処理から呼び出されるソフトウェアです。プラグインはシステム権限で動作し、Edgecross 搭載 PC のほとんどの操作が可能になります。悪意のあるプラグインが混入した場合、生産現場の停止やデータの漏洩・改ざん等を招く恐れがあります。

プラグインは、Edgecross マーケットプレイスなど、信頼できる提供元から入手することを推奨します。

(7) IT ゲートウェイ

IT ゲートウェイは、外部 IT システムと Edgecross 基本ソフトウェアの間の通信を提供するソフトウェアコンポーネントになります。

3.4.2(3)「IT ゲートウェイ」に記載の内容と同じく、外部 IT システムからの Edgecross へのアクセスを IT ゲートウェイ経由として堅牢なシステムを構築することが可能です。IT ゲートウェイの使用方法は、IT ゲートウェイのマニュアルを IT ゲートウェイ提供元から入手して参照ください。

3.4.4 保守・運用

(1) ソフトウェア更新

最新の Edgecross 基本ソフトウェアには、既知の脆弱性への対処が織込まれているため、Edgecross 基本ソフトウェアは最新版を利用するようにしてください。バージョンアップにおいては動作検証の上、実行することを推奨します。また、関連する OSS についても脆弱性の対処を実施して下さい。

詳しくは、4.1「脆弱性対策」を参照してください。

(2) 履歴保存

セキュリティインシデント発生時のみならず、故障やソフトウェア不具合の発生時などにも、イベント情報は有用な情報をもたらすことが多々あります。Edgecross システムの管理者は、イベント情報の履歴をチェックしてください。

Edgecross 基本ソフトウェアは、リアルタイムフローマネージャ、マネジメントシェルおよびこれらが使用しているデータコレクタで発生したイベント情報を取得し、イベントの履歴とイベントの詳細情報・原因・処置方法を診断情報として表示します。イベント履歴は、リアルタイムフローマネージャを動作させている産業用 PC の電源を OFF にしても保存されるため、産業用 PC を再起動してからの確認、または前後の操作情報の確認によって問題の発生要因を追及する際に使用することができます。また、エラー発生時にエラーコードが確認できない場合にも使用することができます。

3. 5 ネットワーク

保護すべき資産に対するセキュリティ対策としてネットワークを活用した手法について以下に示します。

[ネットワークへのセキュリティ対策箇所例]

図 3-4 にネットワークへのセキュリティ対策箇所の例を示します。

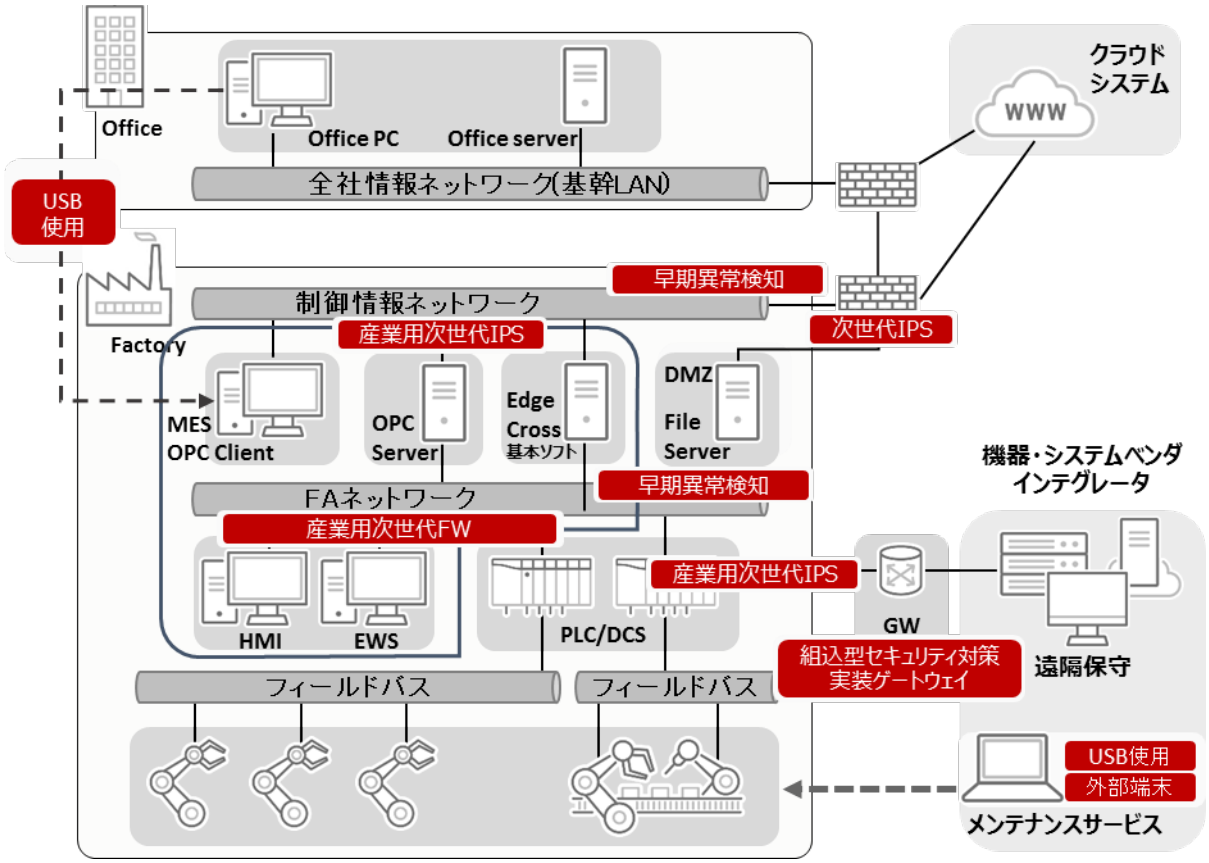


図 3-4 ネットワークへのセキュリティ対策箇所例

[ネットワークでの対策]

工場内に存在するネットワークを、利用箇所に応じ“制御情報ネットワーク”“FA ネットワーク”“フィールドバス”と階層に分けて説明します。

(1) 対策方針

ネットワーク上で、感染防止、感染後の検知を行い、端末側で感染状態の確認・検知・駆除を行う対策を取ることで、ネットワークに接続される際に発生するリスクを最大限取り除くことが必要です。

(2) 資産管理

守るべき資産を把握できていないと、セキュリティ対策漏れがあったり、インシデント発生時に迅速な状況の確認ができなかったりする可能性があります。よって、制御情報ネットワークや FA ネットワーク上の機器やその機器で使用されるアプリケーション(通信プロトコル)などの情報をリストアップし、資産管理一覧を作成する必要があります。既存システムや既存ネットワークに影響を与えない、通信パケットのモニターなどからネットワーク上の機器を検出し、資産管理などが可能なネットワーク可視化装置の設置を推奨します。

(3) ネットワーク構成管理

ネットワークの構成を把握できていないと、インシデントが発生した場合に、迅速に影響範囲の確認ができない可能性があります。よって、制御情報ネットワークや FA ネットワークの物理構成や論理構成、データの流れなどが分かるネットワーク構成図の作成が必要です。通信パケットのモニターや SNMP などによる

データ収集によりネットワーク構成図を描画できるネットワーク監視装置やネットワーク可視化装置の設置を推奨します。

(4) ネットワーク境界対策

工場の出入口となる制御情報ネットワークと、通常の全社情報システムネットワーク（以下、IT系ネットワーク）を接続する場合、IT系ネットワークからのマルウェア進入を防ぐため、ファイアウォール装置（以下、FW 装置）を設置します。また、単なる FW 装置の設置だけではなく、制御情報ネットワーク配下の産業制御システムの脆弱性対策なども鑑みると、侵入防止システム（次世代 IPS）の追加、もしくは、これに準ずる機能を搭載した次世代 FW の設置を推奨します。

(5) 早期異常検知対策

制御情報ネットワークには、ネットワーク上の機器が万が一マルウェアに感染した時を考慮し、ネットワーク通信から不正な振る舞いや異常を検知し、リスク脅威と対応優先度を可視化する内部対策装置（サイバー攻撃検知センサー）の設置を推奨します。

(6) 不正通信検知対策

工場ネットワークの運用においては、人為的なミスに加え、悪意を持った関係者により深刻な事態に陥ることも予想されます。また、対策を導入する上では、既存のシステムやネットワークに負荷をかけず、後付けで簡単に導入でき、ネットワークの高度な知識、設定工数などを不要とする考慮が必要です。誤った操作や疑わしい通信を防ぎ、設定を自動生成する機能を備えたホワイトリスト(アクセス許可リスト)スイッチでの対策が有効です。外部からの攻撃はもちろん、許可されていない内部からのアクセスも防ぐことができます。

(7) 長期可用性を求められる汎用 OS を使った SCADA や HMI（パネコン等）、IPC への対策

設備によっては、システムリソースが限られたパネコン等を使って SCADA や HMI を運用しているケースがあります。事情によりセキュリティ対策ソフトウェアの追加が困難な制御端末に関しては、代替案として装置の LAN ポートに産業用次世代 IPS の接続を行うことを推奨します。これにより、脆弱性対策の緩和措置を行うだけではなく、産業制御プロトコルや制御コマンドに対応したプロトコルホワイトリスト機能を活用することによって、Edgecross 基本ソフトウェアが実装された IPC の上位通信を MQTT と OPC-UA だけに絞るといった対策を講じることができます。

(8) USB 使用対策

マルウェア進入経路となるIT系ネットワークを FW 装置で遮断していても、早期異常検知対策の必要性があるのは、Edgecross の設置により機器間がネットワーク接続された場合に、現場の運用にて利用する USB デバイスからの進入経路が無くならないからです。

ネットワークを介した情報収集を開始しても、すべてのポイントから USB の運用を取り除くことは難しく、また、取り除くとしてもそれが完了するまでにある程度の時間が必要になるため、現場内に USB デバイスが存在する場合、USB デバイスを使ったデータ収集を行うポイントでは、インストール不要のマルウェア検索・駆除ツールを使用し、端末の健全性を確保する必要があります。

インストール不要のツールを使用する背景には、マルウェア対策ソフトのインストールにより端末に与える負荷影響を抑える役割、また、メーカーから提供された組み込み端末等ではマルウェア対策ソフトのインストールが許容されないケースがあるためです。

(9) 持ち込み PC 対策

工場勤務者が、マルウェア感染した私有 PC を工場内のネットワークに接続し、社内への感染の拡大を招いたインシデントが報告されています。ドキュメントによるセキュリティ運用ルールだけではなく、工場ネットワークへの接続を制限する必要があります。工場ネットワークを保護するためには、既存ネットワーク構成に影響を与えない、未登録の端末や NG 登録された端末の接続を防止するネットワーク型の対策が有効です。未登録の持込み PC や私有スマートフォンなどを工場ネットワークから遮断することにより、不正アクセス、マルウェア感染による情報漏洩から工場ネットワークを守ります。

(10) 敷設するネットワークの導入設計の重要性

ここまでに記述した対策は、既存環境へネットワークを敷設する際に、工場内に展開されているネットワークの状態(設計)がわかっているケースでの対策となります。

これから導入を検討される上で

・現状のネットワーク環境がよくわからない

・設備単位に個々の最適ネットワーク環境が構築されていてそれらを相互接続することができない

・これから新たにネットワークを敷設する

こういった状態から Edgecross 導入を契機に、工場のネットワーク化を推進する場合、ネットワークを効率的に且つセキュアに敷設する必要があり、

・現状ネットワークの状態を可視化するためのネットワークアセスメント

・ネットワーク機器故障を想定した迂回ルートの考慮

・データ持ち出し・持ち込み時の検疫環境(DMZ の設定)

・設備同士の IP アドレス重複状態からアドレス変更せずに効率的に設備間を接続する手法
(L2SW による IP アドレス変換)

・マルウェア拡散防止目的のマイクロセグメンテーション
(感染時に他工程への感染を防ぐための工程別セグメント割付け)

・接続端末のアクセス管理(接続認証システム/不正端末接続検知システムの導入)

・正常運用時のトラフィック可視化と必要通信の明確化

こうした工場専用のネットワーク設計が必要となります。

環境調査(アセスメント)を行い、ネットワーク設計をした後に環境構築となりますが、IP ネットワーク構築専門のインテグレータに、ネットワーク導入の目的や将来的な利用方法を伝え、実現したいネットワークの設計・構築が可能となるように依頼することも可能です。

(11) 無線ネットワーク

AGV などの無線通信では無線信号の拡散が脅威となるため、無線信号は工場ネットワーク環境内で敷設することを推奨します。

(12) 機器、システムベンダインテグレータのメンテナンスサービス

大規模ネットワーク環境でメンテナンスサービスを提供する際に安全性を確保するため、遠隔 GW の接続を最低限とし、以下の防御の対策を推奨します。

1. Dynamic virtual private network (D-VPN)の利用
2. 接続する設備のホワイトリストアクセス制御
3. 産業用次世代 FW や GW 経由のインターネット接続

また、システムベンダインテグレータがメンテナンスサービスする際は工場の責任者と相談し、時間を制限することが望ましいです。

図 3-5 に最小構成でのネットワークへのセキュリティ対策箇所の例を示します。

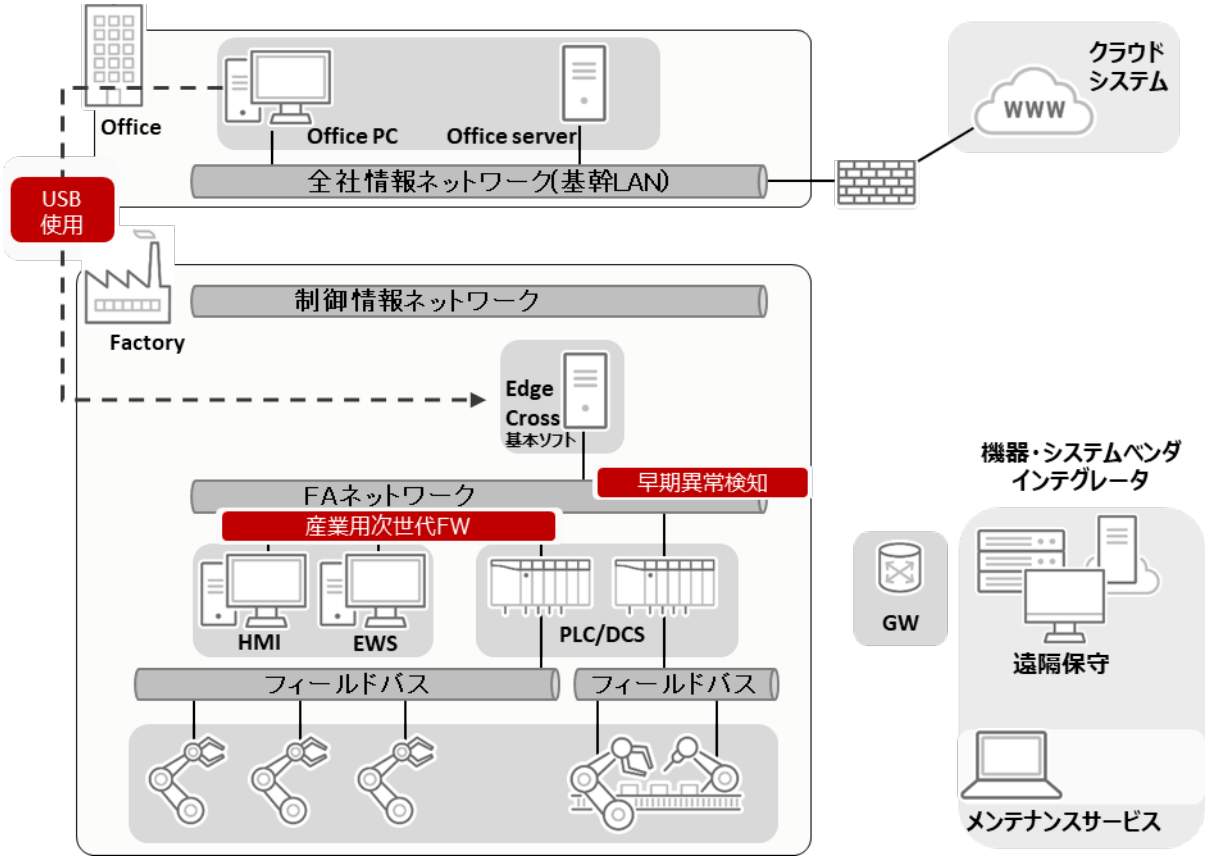


図 3-5 最小構成でのネットワークへのセキュリティ対策箇所例

[ネットワークでの対策]

工場内に存在するネットワークを、利用箇所に応じ“制御情報ネットワーク”“FA ネットワーク”“フィールドバス”と階層に分けて説明します。

(1) 対策方針

導入初期において、単独のネットワークを構成しインターネット接続がない段階では、office-Factory 間でデータ取得の為に使用する USB に対する対策、及び USB 等を使用した際に感染したことを想定した早期異常検知を目的とした産業用次世代 FW 対策を行います。

具体的な対策については、前項で示した USB 対策及び早期異常検知対策をご確認ください。

(2) 早期異常検知対策

制御情報ネットワークには、ネットワーク上の機器が万が一マルウェアに感染した時を考慮し、ネットワーク通信から不正な振る舞いや異常を検知し、リスク脅威と対応優先度を可視化する内部対策装置(サイバー攻撃検知センサー)の設置を推奨します。

(3) USB 使用対策

マルウェア進入経路となるIT系ネットワークと接続されていなくても、早期異常検知対策の必要性があるのは、Edgecross の設置により機器間がネットワーク接続された場合に、現場の運用にて利用する USB デバイスからの進入経路が無くならないからです。

ネットワークを介した情報収集を開始しても、すべてのポイントから USB の運用を取り除くことは難しく、また、取り除くとしてもそれが完了するまでにある程度の時間が必要になるため、現場内に USB デバイスが存在する場合、USB デバイスを使ったデータ収集を行うポイントでは、インストール不要のマルウェア検索・駆除ツールを使用し、端末の健全性を確保する必要があります。

インストール不要のツールを使用する背景には、マルウェア対策ソフトのインストールにより端末に与える負荷影響を抑える役割、また、メーカーから提供された組み込み端末等ではマルウェア対策ソフトのインストールが許容されないケースがあるためです。

4. 運用におけるセキュリティ対策

運用に先立って前述のような構成管理、利用者/運用者/管理者管理、アクセス管理、ログ管理等を整備するとともに、運用開始後はこれら管理に加えて脆弱性/脅威情報収集、脆弱性管理等のセキュリティ管理を継続的に実施することが重要です。また、インシデントに迅速に対応するため、監視、異常検知、問題対処(応急、恒久)、復旧の体制を整備する必要があります。

以下では、特に脆弱性対策およびセキュリティ管理・インシデント対応について詳述します。

4. 1 脆弱性対策

近年は工場現場にもマルウェアが侵入し、拡散活動をすることで工場の操業が停止する事案が度々発生しています。マルウェアは USB デバイスや持込み機器から侵入し、ネットワーク上にある機器の脆弱性を利用して、その他機器への感染拡大を図ります。

マルウェアの感染や拡散活動を抑えるためには、各機器の OS やアプリケーションなどの資産管理を適切に実施し、そのセキュリティパッチをタイムリーに適用することが求められます。

Edgecross 基本ソフトウェアが導入される産業用 PC のソフトのバージョン管理を実施し、必要に応じて Edgecross 基本ソフトウェア、OS、その他アプリケーションのアップデートなどを実施することで脆弱性の対応が可能となります。以下各部位についてアップデートの考え方を示します。

(1) Edgecross 基本ソフトウェア

脆弱性を無くすため Edgecross 基本ソフトウェアは最新版を利用するようにしてください。セキュリティパッチの適用やバージョンアップは動作検証の上、実行することを推奨します。

Edgecross 基本ソフトの最新版は Edgecross のマーケットプレイス上で公開していますので参考にしてください。

Edgecross 基本ソフトウェア Windows 版の関連する OSS を下表に示します。

セキュリティの観点から、動作確認がされており、かつ新しいバージョンを利用することが望ましいです。

また利用している OSS に脆弱性が公開された場合は、Edgecross コンソーシアムで可能な限り早く動作確認を実施して迅速な情報公開に努めます。

OSS の使用形態は 2 種類あります。

一つは、OSS ソースコードやライブラリを Edgecross 基本ソフトウェア内に取り込んで使用している形態です。この形態の OSS に脆弱性が公開され、対処の必要が生じた場合は、Edgecross 基本ソフトウェアのアップデートが必要となります。Edgecross 基本ソフトウェアアップデート時の Edgecross コンソーシアム対応を参照して対応してください。

もう一つは、Edgecross 基本ソフトウェア外で独立して動作する OSS です。この形態の OSS の脆弱性の対処はユーザに委ねられます。OSS の情報入手し、動作検証を実施の上、アップデート作業をお願いします。

なお最新の情報は以下で確認をお願いします。

https://www.edgecross.org/ja/data-download/

表 4-1 Edgecross 基本ソフトウェアの関連 OSS 一覧

	OSS 名称	使用形態
1	Eclipse Mosquitto	Edgecross 基本ソフトウェア内で使用
2	OpenSSL	Edgecross 基本ソフトウェア内で使用
3	PostgreSQL	Edgecross 基本ソフトウェア外
4	PSQLODBC.DLL	Edgecross 基本ソフトウェア外
5	pthread	Edgecross 基本ソフトウェア内で使用

(2) エッジアプリケーションおよびデータコレクタ

エッジアプリケーション、およびデータコレクタについては Edgecross の会員企業が開発していますので、その開発元やマーケットプレイスから情報を入手して脆弱性対策をしてください。

セキュリティパッチの適用やバージョンアップは動作検証の上、実施を推奨します。

Edgecross マーケットプレイス:
https://www.marketplace.edgecross.org/

(3) OS

Windows は、Windows Update により更新プログラムを適用して、常に最新の状態に保つための機能が備わっています。汎用的に利用する環境では常に最新の状態に更新することを推奨します。

ただし、更新プログラムには、再起動を伴うもの、更新に時間がかかるものがあります。動作環境と相性の問題や、不具合があるものも存在するため、実際には Edgecross の運用に問題ないことを確認してから更新することを勧めます。

特定の用途で利用する産業用 PC などでは、更新プログラムの適用を一時延期し、更新プログラムの動作検証用に試験用機器を用意するなどの対策が有効です。Microsoft 社は組織内の Windows 更新プログラムの適用を制御するためのソリューションとして、Windows Server Update Services (WSUS)を提供しています。

Windows 更新プログラムの入手元として WSUS を選択する場合、グループ ポリシーを使って Windows PC を WSUS サーバに向けるように設定します。Windows Update から更新プログラムが定期的に WSUS サーバにダウンロードされ、WSUS 管理コンソール または グループ ポリシーを通じて 管理、承認、展開され、企業の更新プログラムの管理が合理化されます。

(4) ハード、BIOS、ドライバ

産業用 PC やそれに接続された装置の BIOS やドライバについても脆弱性があれば対応が必要です。開発元から情報を入手し、動作検証の上、適用を推奨します。

なお、近年では、ソフトウェアの脆弱性が発見された場合、開発元から脆弱性対策のための更新プログラムや回避策が公開される前に、脆弱性を悪用したサイバー攻撃が行われることがあります。これをゼロデイ攻撃と呼びます。この攻撃が行われた場合には、事前の対策は限られており確実に防御することは困難とされています。

本書に記載の、インシデント対応体制の整備(4. 3 インシデント対応 参照)や、ネットワークの監視による検知やファイアウォールによる通信の遮断手段の整備(3.5 ネットワーク 参照)等の対応は、被害の予防や早期検知のための事前の対策として重要となります。

4. 2 セキュリティ管理

Edgecross システム内には、多様な機器が存在し 10 年以上の長期間利用される機器やシステムも想定されます。システム内への機器の追加や設定の更新、ネットワーク環境の変更など、多くの環境変化に伴う脆弱性の発生が危惧されます。更に、機器の変更を行わない場合でも、新たな脆弱性が発見されることもあります。

Edgecross システムの運用を開始した後も、継続的にセキュリティ管理・対応を行うことが重要です。システム全体では、各種機器の管理者やネットワーク管理者、システムの運用者、ソフトウェアや機器の供給メーカーなど、多くの関係者が存在しています。予め関係者の役割を整理して、組織的にセキュリティ管理・対応ができるよう、体制を整えてください。

・機器のセキュリティ上重要なアップデート等を必要なタイミングで適切に実施する方法を検討し、適用してください。
・Edgecross システムの構築者・運用者は、システムの脆弱性情報を収集・分析し、関係者に情報発信してください。
・システムへの不用意なつなぎ方によるリスクや、守ってもらいたいことを関係者へ周知してください。
・Edgecross システムの各種機器メーカーや提供者、システム管理者や運用者など、関係者の役割を整理してください。
・脆弱性を持つ機器を把握する仕組みを構築し、定期的な監視を組織的に行ってください。
・脆弱性を持つ機器を特定した場合には、該当する機器の管理者へ注意喚起を行い、できるだけ速やかに脆弱性対応を実施してください。

参考:「IoT セキュリティガイドライン ver 1.0」
2.5【運用・保守】 指針 5 安全安心な状態を維持し、情報発信・共有を行う

4. 3 インシデント対応

(1) 平時における準備
・インシデントに関する情報を収集して、Edgecross システムに与える影響を分析し、必要な対策を検討してください。Edgecross コンソーシアムでは、各種インシデント事例の紹介資料を順次公開していますので、参考にしてください。
・インシデント発生時に備えて、インシデント対応マニュアルを整備してください。そして、従業員にマニュアルの内容を研修で啓発したり、マニュアルに沿った訓練を実施したりすることが効果的です。

(2) インシデント発生時
・3. 4 Edgecross 基本ソフトウェアの履歴や 3. 5 ネットワークのログ等を確認する仕組みを構築して定期的な監視を行い、インシデントを早期に検知してください。なお、監視は高い専門性が要求されることから、人員の確保が難しい場合には外部の SOC サービスを活用することもできます。
・複数のインシデントが発生して対応しきれないことが予想される場合は、あらかじめ決めた基準に従って、インシデント間に優先順位を付けて対応してください。
・事前に整備した対応マニュアルに基づいて、影響の範囲を見定めて脅威を取り除き、被害が最小限となるようにしてください。

(3) インシデント発生後
・原因を究明し、同じインシデントが再度発生しないようにパッチ適用や設定変更等の対策を実施した後に、Edgecross システムを復旧させてください。
・再発防止の観点でも原因を分析し、対応マニュアル等にフィードバックしてください。

参考:「CSIRT ガイド」
6. インシデントハンドリング概論

5. まとめ

Edgecross を用いた FA システムの安全・安心を確保するため、本ガイドラインを活用ください。
なお、本書の記載に関する質問は、Edgecross コンソーシアムホームページのお問い合わせフォームに記入の上、問い合わせください。

Edgecross コンソーシアムお問い合わせフォーム　https://www.edgecross.org/ja/contact/form/