Edgecross

セキュリティガイドライン　概要版

Ver. 1.0.0

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-TE4-0004-01-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

DMG森精機株式会社

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

改定履歴

Ver.	改定内容	発行年月
1.0.0	初版	2019 年 9 月

目次

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やプラント等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 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 システムの使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
		要点 5. つながりで波及するリスクを想定する	2.3
		要点 6. 物理的なリスクを認識する	2.3
		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

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」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 つを柱とする取り組みを継続的に行います。

・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公的機関と連携し、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
CPU	Central Processing Unit
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
I/F	Interface
IoT	Internet of Things
IP	Internet Protocol
IT	Information Technology
LAN	Local Area Network
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
PC	Personal Computer
PIN	Personal Identification Number
PLC	Programmable Logic Controller
SCADA	Supervisory Control and Data Acquisition
TLS	Transport Layer Security
TPM	Trusted Platform Module
USB	Universal Serial Bus
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。
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。
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。

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）

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があります。また、関連ソフトウェアとして開発キット等があります。

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。

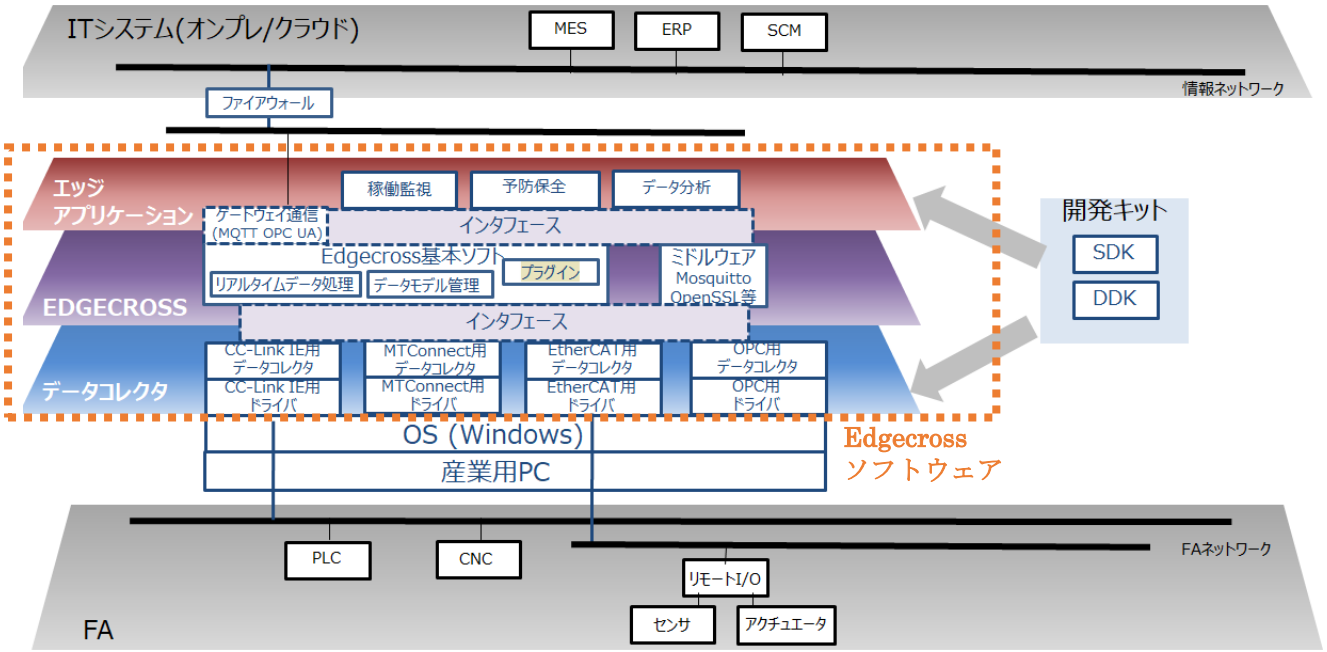

図 2-1 Edgecross における保護すべき資産

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産業用 PC へ不正にログインされる脅威が想定されます。

(2) 情報漏えい

Edgecross 基本ソフトウェアに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、エッジアプリケーション等のソフトウェアが産業用 PC から不正に読み取られる脅威も想定されます。

(3) 不正ソフトウェア

マルウェア等の不正ソフトウェアが産業用 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

産業用 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

産業用 PC に潜むマルウェアがエッジアプリケーション等の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 基本ソフトウェアに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) DoS/DDoS 攻撃の踏み台

マルウェアに感染した産業用 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、マルウェアが産業用 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、産業用 PC を盗難するといった物理的な攻撃の脅威が想定されます。

2. 4 セキュリティインシデント事例

図 2-2 にウクライナで発生した発電施設のインシデントの事例を示します。電力供給会社にサイバー攻撃があり、公共インフラを含む 140 万世帯に大規模停電が発生しました。この攻撃では外部からの標的型攻撃メールから始まり、従業員端末を感染させ内部拡散を図り、最終的には SCADA システムを通じて発電施設を誤作動させた事例です。

この事例は、直接インターネットに接続してはいない制御システムの環境でもサイバー攻撃の被害を受ける可能性を示しています。

Edgecross システムが配置される工場環境も同様のインターネットに接続されてない環境でありますが、セキュリティリスクが残っていると認識しセキュリティ対策を講じなくてはなりません。

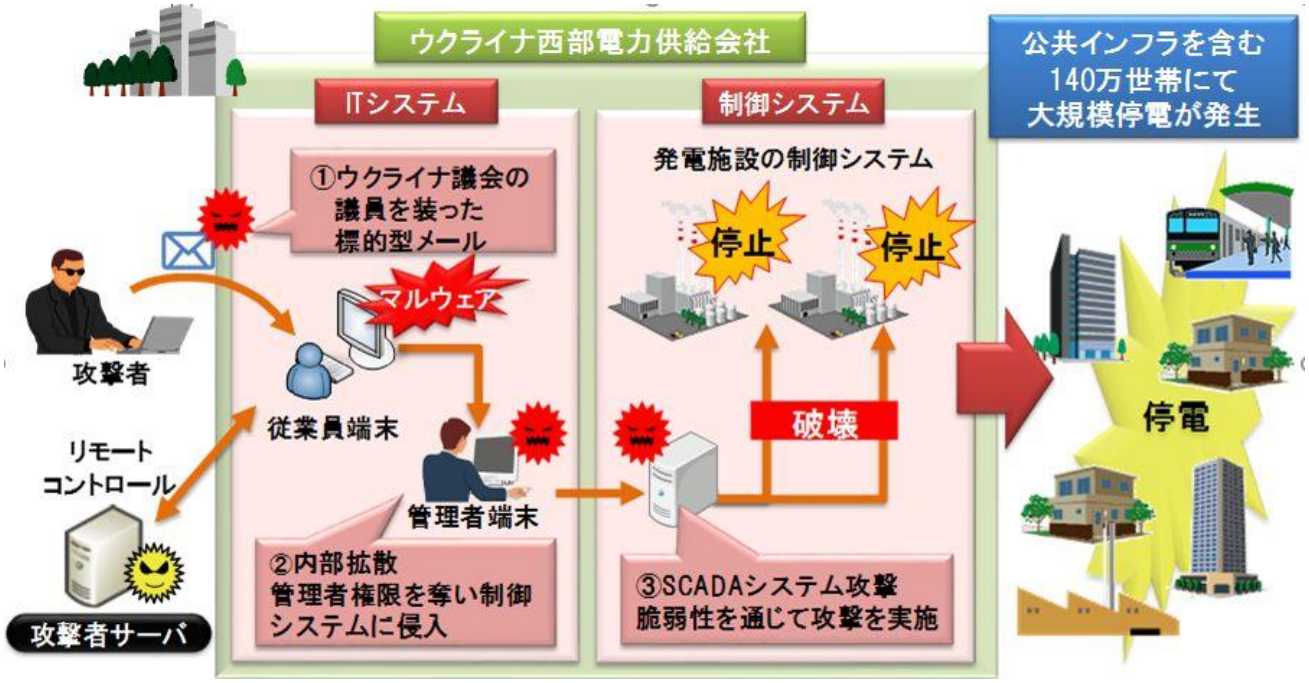

図 2-2 発電施設のインシデント事例

3. 構築

3. 1 構築要点

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。

(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

(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(ユーザー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 にて更新プログラムを適用する機能が備わっています。環境に応じて最新の状態に更新することを推奨します。ただし、現実問題として、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、動作環境と相性の悪いもの、不具合があるものも存在するため、Edgecross の運用に支障をきたす可能性があることに留意してください。

運用機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 Update を設備メンテナンスの一環と位置づけ、計画的に運用することを推奨します。

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す。

これらソフトウェアの一般的な機能は、システムへの侵入やマルウェアへの感染を防止することです。

Edgecross 基本ソフトウェアおよび認定製品や、推奨産業用 PC 等における不正ソフトウェアの起動への対策(マルウェア等の起動や動作を検知・防止する)ために、お客様にてセキュリティソフトウェアの導入を推奨します。

導入にあたっては、セキュリティソフトウェアの製品販売元に問い合わせの上、導入してください。

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あります。

・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
・他のシステムへの攻撃の踏み台にされる

セキュリティソフトウェアの導入後は、次の 3 点を考慮することを推奨します。

(1) 契約の更新

セキュリティソフトウェアには、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

セキュリティソフトウェアの機能をアップデートして、セキュリティの脅威への検出機能を強化します。

マルウェア検出パターンは日々、更新されることが多いため、定期的なアップデートが必要です。

また、セキュリティソフトウェアの大規模な機能強化が行われた場合にはバージョンアップが行われるので、これを導入することを検討ください。

(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。

3. 4 Edgecross 基本ソフトウェア

Edgecross 基本ソフトウェアは、Windows 上で動作し、下記のソフトウェアで構成されています。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、または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ます。

表 3-1 Edgecross 基本ソフトウェアの構成

ソフトウェア	内容
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	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	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、WindowsサービスとしてWindows上のバックグラウンドで動作します。 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	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うソフトウェアです。

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、Edgecross 基本ソフトウェアにおける主なセキュリティ関連機能及び留意点としては以下があります。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。

(1) OPC UA 接続機能

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。

(2) MQTT を用いたエッジアプリケーション連携機能

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にデータ(収集データ, 加工データ)を配信し、エッジアプリケーションから応答データを受け取る際に TLS にて暗号化を行うことができます。

(3) イベント履歴

リアルタイムフローマネージャおよびリアルタイムフローマネージャ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。

(4) ファイル保存機能

リアルタイムフローマネージャが収集/加工したデータまたは診断した結果のデータのファイル保存機能において、保存先としてリモート共有フォルダを指定する場合、適宜 Windows のファイアウォールによるアクセス制限などを行うことを推奨しています。

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 3-1 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。

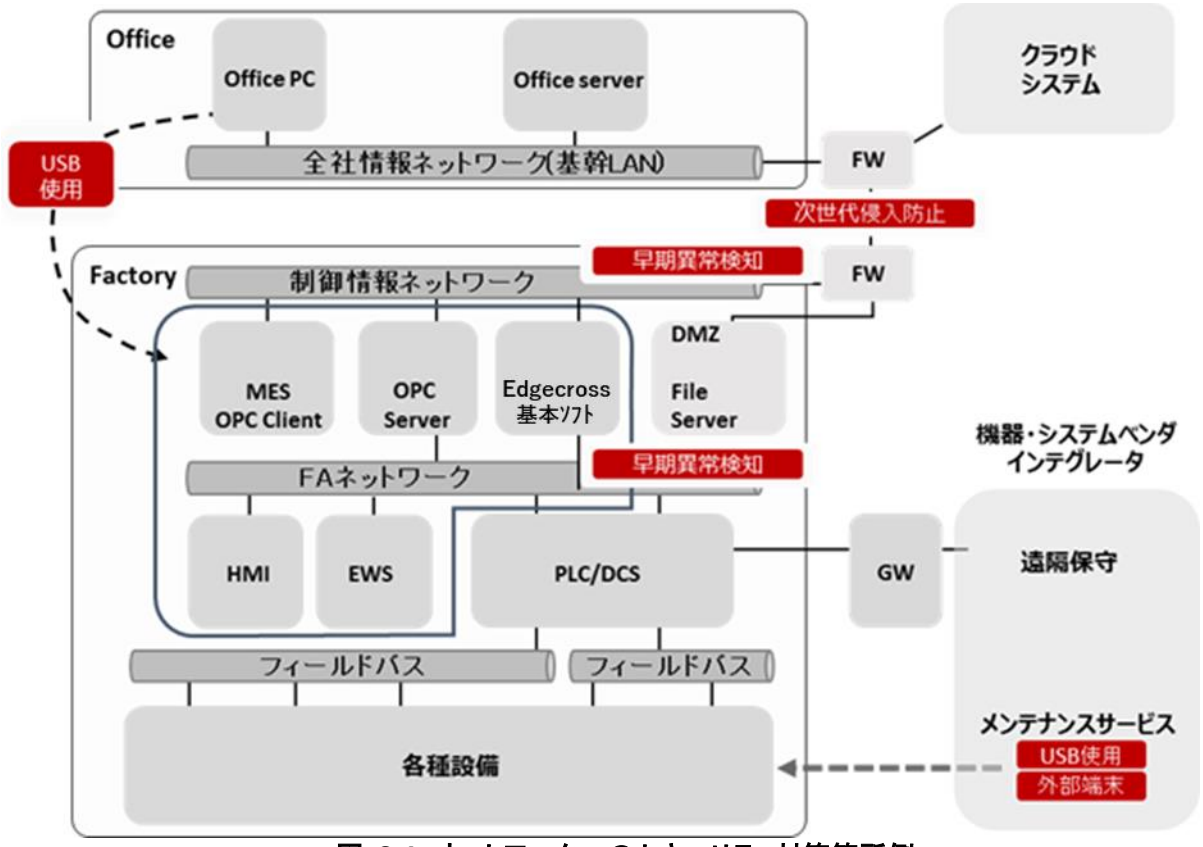

図 3-1 ネットワークへのセキュリティ対策箇所例

[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) ネットワーク境界対策

工場の入り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。ただし、単純な FW 装置ではなく、脆弱性対策を考慮した次世代型進入防止システムを具備した FW 装置であることを推奨します。

(3) 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感染した時を考慮し、マルウェア感染をネットワーク上で検知することが可能となる、最新の脅威を可視化、異常検知が可能な標準型サイバー攻撃検知センサー装置の設置も推奨します。

(4) 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。

(5) 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、ネットワーク状態がわかっているケースでの対策となります。

・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

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利用するためには、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や、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を用いた専用のネットワーク設計手法が必要となります。

そのため、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を推奨します。

4. 運用

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。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。

セキュリティの情報は Edgecross のホームページ上で公開していますので内容を確認の上、必要に応じて対応してください。

(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、開発元から情報を入手して脆弱性への対応をしてください。

バージョンアップにおいては動作検証の上、実行してください。

(3) OS

Edgecross 基本ソフトウェアがサポートする OS は Windows となっています。定期的に脆弱性が発表されており、Microsoft 社より OS の修正プログラムが定期的にリリースされています。定期的にアップデートすることを推奨します。

アップデートにおいては導入対象の産業用 PC メーカーや Microsoft 社から OS アップデートに関する情報を入手し、動作検証の上、実行してください。

(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。

4. 2 セキュリティ管理・対応

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、システム管理者や使用者など、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。

引用元:「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

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/