セキュリティインシデント事例②
水処理システムの事例

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

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

Musarubra Japan 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	2023 年 3 月

目次

1. はじめに

1. 1 概要

工場におけるセキュリティインシデントは絶えることがありません。Edgecross ユーザ企業からは工場におけるセキュリティインシデント動向として具体的な事例を知りたいとの声が Edgecross コンソーシアムに寄せられています。

このような背景から、本書では、過去のセキュリティインシデントのうち代表的な事例を取り上げ、想定されるリスクや関連する脆弱性情報とともに紹介します。そして、Edgecross ユーザ向けセキュリティガイドライン[1]、Edgecross 開発者向けセキュリティガイドライン[2]を活用できるように、Edgecross を用いた FA システムがインシデント事例と同様に攻撃されることを想定して、Edgecross 向けの推奨対策を提示することが最大の特色となっています。

想定読者は、工場管理者／従事者、Edgecross 運用者、Edgecross 開発者と幅広くカバーしています。各立場に応じて本書を活用してください。

1. 2 略称

AD	Active Directory
ID	Identification
IPS	Intrusion Prevention System
MQTT	Message Queuing Telemetry Transport
OS	Operating System
OSS	Open Source Software
PC	Personal Computer
PIN	Personal Identification Number
PoC	Proof of Concept
RAT	Remote Administration Tool
SCADA	Supervisory Control And Data Acquisition

1. 3 用語

本書で用いる用語を**エラー! 参照元が見つかりません。**に示します。

表 1-1 用語

用語	説明
セキュリティインシデント	マルウェア感染や情報窃取など、セキュリティ上の問題である事象。
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。
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。
バックドア	秘密裏に仕込まれた、遠隔操作のための接続口。
エクスプロイト	脆弱性を攻撃するプログラム。
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。
ペネトレーション	既に知られている手法を用いて実際に侵入や攻撃を試みるテスト。
Active Directory (AD)	ネットワーク上の機器、およびそのユーザのアカウントやアクセス権限などを一元的に管理する機能。
(デジタル)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。
ソーシャルエンジニアリング	人間の心理や行動の隙をついてパスワードなどを窃取する手口。

侵入防止システム (IPS)	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。
仮想パッチ	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)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。
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。

1. 4 関連資料

本書の関連資料を**エラー! 参照元が見つかりません。**に示します。

表 1-2 関連資料

No.	資料名称	資料 No	入手方法
1	Edgecross ユーザ向けセキュリティガイドライン 詳細版	ECD-TE4-0006-02-JA	https://www.edgecross.org/ja/data-download/pdf/ECD-TE4-0006-02-JA.zip
2	Edgecross 開発者向けセキュリティガイドライン	ECD-TE4-0008-01-JA	Edgecross コンソーシアム会員用ホームページ
3	制御システムのインシデント事例 8 ～2021 年 水道局への不正侵入と飲料水汚染未遂～ 2021 年 10 月 IPA	-	https://www.ipa.go.jp/files/000093824.pdf

2. セキュリティインシデント

本章では、フロリダの水道局で発生したセキュリティインシデントについて順を追って説明します。

2. 1 概要

2021 年 2 月に、米国のフロリダ州 Oldsmar（人口約 15,000 人）の水道局の水処理システムに何者かがインターネット経由で不正侵入し、水酸化ナトリウムの投入量を高く設定変更するというインシデントが発生しました。現場操作員が不正な操作に気付き、直ちに設定値を元に戻したため、供給される水は影響を受けず、人的被害は発生しませんでした。

2. 2 詳細

水酸化ナトリウムの濃度の異常値設定に至るサイバー攻撃は、下記の流れで行われたとされています。

(1) 事務用 PC への不正アクセス

攻撃者は、水道局内の情報ネットワークに接続された事務用 PC に TeamViewer(遠隔操作ソフトウェア)を利用して、不正にログインしました。

この水道局では、TeamViewer を利用した遠隔操作による業務が行われており、TeamViewer のパスワードは全 PC で共通のものが使用されていました。

認証情報の取得経路は不明です。

以下①②の事実より、外部から PC にインターネット経由で直接攻撃して、ハッキングした可能性があります。

①ファイアウォールなしで事務用 PC をインターネットに接続

②サポート切れの Windows7 を使用

またパスワードが共有されていたことから、従業員の誰かからアカウント情報が漏洩した可能性もあります。

(2) 事務用 PC から周辺ネットワークを探索

攻撃者は、事務用 PC からネットワークを探索し、SCADA 操作端末を発見しました。現場操作員は、事務用 PC が遠隔操作されている事を認識していましたが、遠隔操作による業務は日常的に行われていたため、不正操作であると気づきませんでした。

(3) SCADA 操作端末への不正ログイン

攻撃者は、TeamViewer を利用し、インターネットから SCADA 操作端末へ不正にログインしました。TeamViewer の認証情報として、ID はマシン名などから推測したのではないかと考えられます。また、パスワードは事務用 PC と共通のものが利用されていました。

(4) 制御装置の遠隔操作

攻撃者は、SCADA 操作端末を利用して、水酸化ナトリウムの濃度を正常値の 100ppm から、異常値 11,100ppm に改ざんしました。

その後、TeamViewer の遠隔操作画面がそのままデスクトップに表示されていたため、現場操作員が異常に気が付き、正常値に再設定しました。このため、供給される水は影響を受けなかたことから人的な被害は発生せず、幸い大きな被害には至りませんでした。

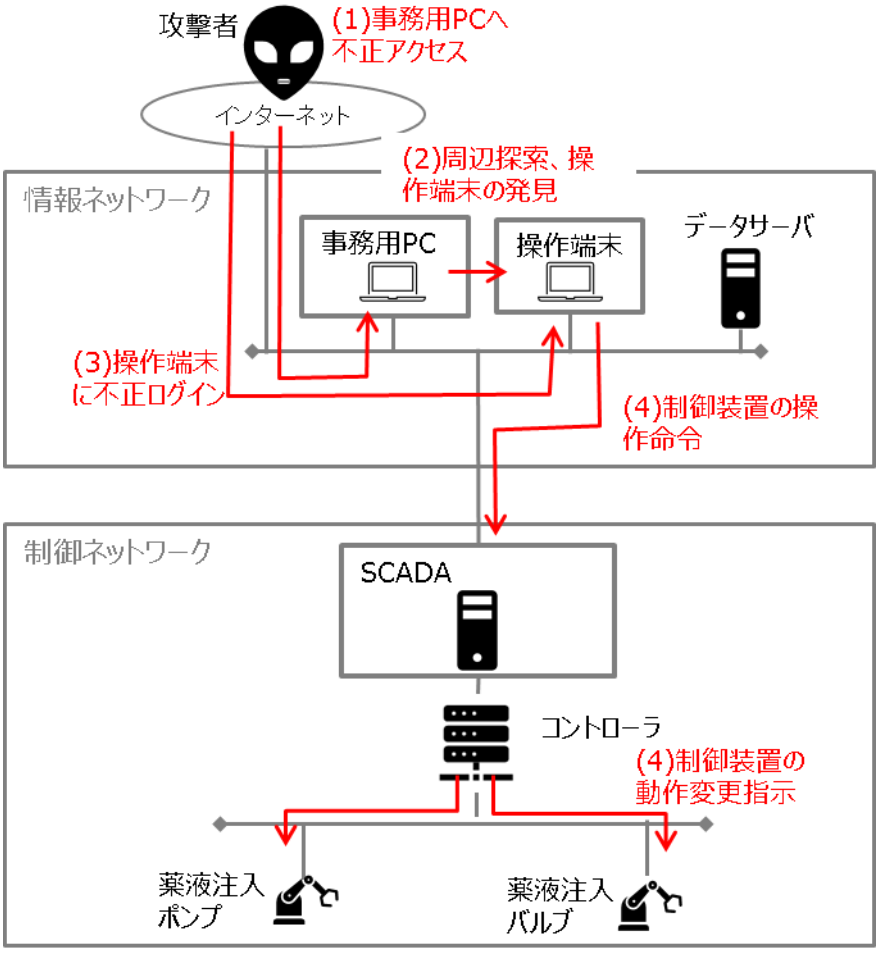

図 2-1 攻撃の流れ※

※システム構成は、実態が定かでないため、推測となります。

3. 想定されるリスク

本章では、セキュリティインシデントにより想定されるリスクについて説明します。

セキュリティインシデントが発生した場合に想定されるリスクとして、以下のものが考えられます。

(1) プラントの目的達成のための安定的かつ継続的な稼働、コスト低減が妨げられる
プラントは、事業の目的を達成するために、コスト低減を図るとともに、安定的かつ継続的に稼働するシステムであり、その安定・連続稼働（可用性）が求められます。セキュリティインシデントの発生により、プラントの可用性が損なわれると、目的達成のための安定的かつ継続的な稼働、コスト低減が妨げられるリスクがあります。

(2) プラントの安全確保、提供サービスの品質確保が妨げられる
プラントの安全確保や品質確保を実現するために、プラントおよび機器が正常に動作する状態を保つことが求められます。セキュリティインシデントの発生により、機能・制御の完全性が損なわれると、プラントの安全確保や品質確保が妨げられるリスクがあります。

(3) プラントのシステムおよび機器の正常動作確保や、適正なフィードバック制御の実現を妨げられる
プラントのシステムおよび機器が正常に動作する状態を保つためには、システムおよび機器の機能・制御の仕方を設定・指示(命令)するデータが正しいこと、すなわちデータが壊れたり改ざんされたりしていないことが求められます。また、システムおよび機器の制御・稼働・運用の最適化・自動化(自律化)を図る目的で、システムおよび機器の稼働状態に応じたフィードバック制御を実現するために、システムおよび機器の稼働状態にかかわるデータを収集・分析・監視し、その時点の状態に基づき、システムおよび機器の機能・制御の仕方にかかわる設定・指示(命令)を変更していく運用の実現が必要になってきています。セキュリティインシデントの発生により、データの完全性が損なわれると、システムおよび機器の正常動作確保や、適正なフィードバック制御の実現が妨げられるリスクがあります。

(4) プラントの稼働にかかわる情報やデータの外部漏えい
プラント事業にとって、サービス稼働や生産方法における優位点の模倣を防ぎ、差異および競争優位性を確保することは重要であり、サービスや生産(ノウハウ)にかかわる情報やデータが外部に漏えいしないようにすることが求められます。セキュリティインシデントの発生により、データの機密性が損なわれると、サービスや生産(ノウハウ)にかかわる情報やデータの外部漏えいが起こるリスクがあります。

(5) プラントで発生したセキュリティインシデントにより、事業者責任を問われる
プラント内で発生したセキュリティインシデントにより、プラントの目的が達成できなかったり、サービスが提供不能になったりする問題を引き起こす可能性があります。セキュリティインシデントの発生により、期待されているサービスが提供できなかったり、プラントが外部から不正に利用・制御されたりすることで、プラントの管理責任を問われたり、損害賠償請求を受けたりするなどのリスクがあります。

上記のリスクを防止/抑止するために、セキュリティインシデントを対象としたセキュリティ対策を検討する必要があります。

4. 関連する脆弱性情報

今回事例で紹介しているサイバーインシデントは TeamViewer を利用して攻撃が行われましたが、このような正規ツールを利用してサイバー攻撃を行うことは多数確認されています。

以下の表は、ランサムウェアの攻撃にて悪用されることが多い正規ツールをまとめたものです。

ツール	正規の想定用途	ランサムウェア攻撃での悪用方法	ツールの悪用を確認しているランサムウェア攻撃
Cobalt Strike	ペネトレーションツール（脅威エミュレーション）	横展開（ラテラルムーブメント）、バックドア、遠隔操作ツール（RAT）としての多数の機能	Clop 、Conti 、DoppelPaymer 、Egregor 、Hello （WickrMe ）、Nefilim 、NetWalker 、ProLock、RansomExx、Ryuk
PsExec	遠隔でのプロセス実行	任意のコマンドシェルの実行、横展開	DoppelPaymer 、Nefilim 、NetWalker 、Maze、Petya、ProLock、Ryuk、Sodinokibi
Mimikatz	PoC ツール（脆弱性の実証）	認証情報の窃取	DoppelPaymer 、Nefilim 、NetWalker 、Maze、ProLock、RansomExx、Sodinokibi
Process Hacker	システムリソースの監視、ソフトウェアのデバッグ、不正プログラムの検出	セキュリティ製品などの正規プロセス／サービスの探索と停止	Crysis、Nefilim、Sodinokibi
AdFind	Active Directory（AD）検索	AD 探索、横展開時の情報収集	Nefilim、NetWalker、ProLock、Sodinokibi
MegaSync	クラウドストレージとの同期	窃取データの外部送出	Hades、LockBit、Nefilim

また、セキュリティ対策ソフトウェアによる攻撃の検知を避けるため Windows に標準搭載されている Powershell を利用し攻撃を行う活動なども多数のマルウェアにて確認されています。

PowerShell はスクリプト言語で、システム管理者がオペレーティングシステム（OS）の管理タスクを自動化させるのに役立ちます。PowerShell は、Windows XP SP2 のリリース以降、標準機能として Windows に組み込まれており、PowerShell を利用することで、レジストリや証明書ストアなど、基盤となる OS へのアクセスを高速かつ向上させることができます。これによりユーザおよび管理者は、システムが持つ多くの機能をローカルまたはリモート環境からでも管理できるようになります。また、PowerShell はオープンソースでもあるため、十分に開発されたスクリプト言語が存在します。PowerShell は Windows に加え、Linux や macOS など、他のプラットフォームにも対応しています。

PowerShell は Windows の標準機能であるため、ほとんどの Windows 環境で利用可能です。加えて攻撃者は PowerShell を利用することで、.NET framework を介してホスト全体にアクセスできるようになります。つまり、攻撃者にとって PowerShell は不正活動を実行する上で好都合な機能であると言えます。そのうえ、ペイロードの拡散活動に適用可能なスクリプトが容易に開発できること、さらに、PowerShell 自体が信頼されるアプリケーションであるため、実行されるスクリプトが不正なものであったとしても、不正なプロセスとはみなされないこ

となど、攻撃者にとって多くの利点があります。

2014 年に PowerShell を利用したマルウェアが初めて報告されて以来、攻撃者はソーシャルエンジニアリングの手法を利用してシステムに感染するための拡散活動を展開したり、PowerShell を他の脆弱性攻撃コード(「エクスプロイト」)と組み合わせたり、あるいはサイバー犯罪の研究や開発の一環と見せかけて、他の不正活動に類似させた攻撃手法を利用したりしています。

5. 推奨される対策

本章では、分類した脅威と、それぞれの対策・緩和策について記述します。

表 5-1 に、本インシデント事例に関連した 6 種類の脅威と、それぞれの脅威に対しての対策・緩和策の概要を示しています。また、それぞれの対策・緩和策の対応を、Edgecross を活用する工場組織における、どの立場の人が行うべきかをマトリクスで示します。チェックマーク「✔」がついている立場の人が、対象者となります。

なお、本表の対象者は一例であり、対象となる組織などの構成を考慮して、対応する対象者に読み替えてください。

表 5-1 脅威の種別と対策・緩和策の概要

#	脅威	対策・緩和策	対象者			
			Edgecross 運用者	Edgecross 開発者	工場 従事者	工場 管理者
(1)	不正アクセス	・ファイアウォール設置			✔	✔
(2)	ソフトウェアの不正使用	・ソフトウェア資産管理の徹底	✔		✔	✔
(3)	脆弱性の存在	・最新 OS/ソフトウェアに更新	✔		✔	✔
(4)	なりすまし	・認証の強化	✔		✔	✔
(5)	データ改ざん	・認証の強化	✔		✔	✔
(6)	ソーシャルエンジニアリング	・セキュリティ教育/啓発	✔		✔	✔

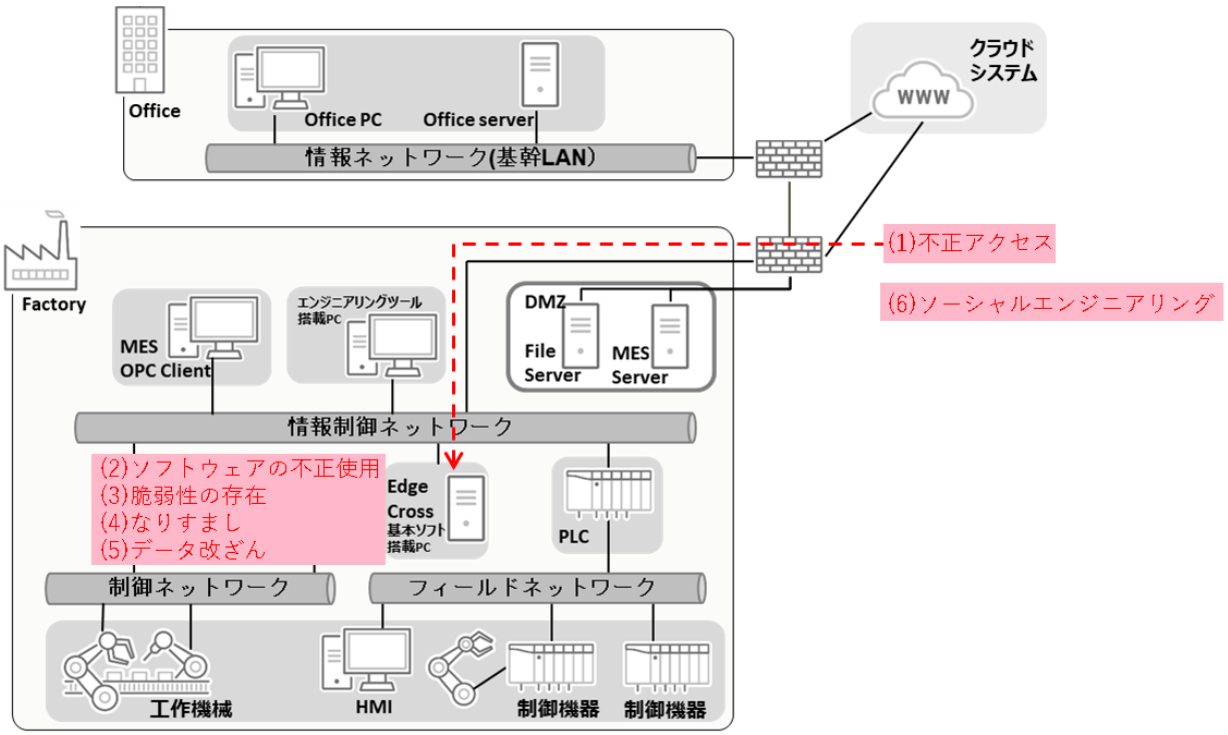

図 5-1 脅威の種別

以降に、6 種類のそれぞれの脅威に対して、どのような対策・緩和策を行うべきかの詳細を示します。

5.1 不正アクセス

本事例では、インターネットからシステム内部に直接アクセスされました。インターネットとの境目にファイアウォールが設置されていなかった可能性があります。ファイアウォールを設置して、外部からの通信を制御することが基本です。

また、単なるファイアウォールの設置だけではなく、情報制御ネットワーク配下の制御システムの脆弱性対策なども鑑みて、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ファイアウォールの設置を推奨します。

5.2 ソフトウェアの不正使用

本事例では、TeamViewer を悪用されました。不要なソフトウェアは導入しないことに加えて、必要であっても TeamViewer のような PC 操作を可能とするソフトウェアは危険性を考慮しての使用（例えば接続クライアントを限定するなど）を徹底する必要があります。

Edgecross の動作 OS である Windows には、様々なアプリケーションやサービスがあります。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。

5.3 脆弱性の存在

OS やソフトウェアが最新化されていないことが原因で脆弱性が存在し、それを悪用した攻撃で端末を侵害されることがあります。OS・ソフトウェアを最新にすることで、そのような脅威を低減することが可能となります。

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推奨します。

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もできます。

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、関連する OSS についても脆弱性の対処を実施して下さい。

5.4 なりすまし

本事例では、TeamViewer の認証情報が事務用 PC と操作端末で共通に使われていたことが原因で、操作端末にログインすることができました。

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、適切な管理を実施することが重要です。TeamViewer のような認証機能のあるソフトウェアを用いる場合も同様です。

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で、端末への不正ログインの可能性を低減できます。

また、本事例では、操作端末から SCADA 操作をする際に認証がなかったことが原因で、攻撃者の SCADA 操作が成功しました。SCADA に認証機能を追加することが対策となります。リモートで SCADA へアクセスする場合には、リモートの認証を通した後、2 段階目の認証（限られた人に付与された SCADA アクセスの認証）を実装することで攻撃が防げます。

5.5 データ改ざん

本事例では、操作端末を利用して、水酸化ナトリウムの濃度を正常値から異常値に改ざんされました。

Edgecross 基本ソフトウェアの操作では、情報閲覧のみでなく、データコレクタを通じた生産現場設備への書き込みによる不正操作も可能です。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。

また、Edgecross において MQTT やファイル、データベースをインタフェースとする通信は、不正データ注入につながる可能性があるため、外部に公開しないことを推奨します。

5.6 ソーシャルエンジニアリング

本事例では、攻撃者は操作端末における TeamViewer の認証情報を何らかの手段で手に入れました。人が原因でパスワードが漏えいした可能性もあります。システムへのログイン ID やパスワードを聞き出す行為に対して組織構成員が敏感になるトレーニングにより、認証情報が漏えいする可能性を低減できます。

6. 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、本文書を活用ください。
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/