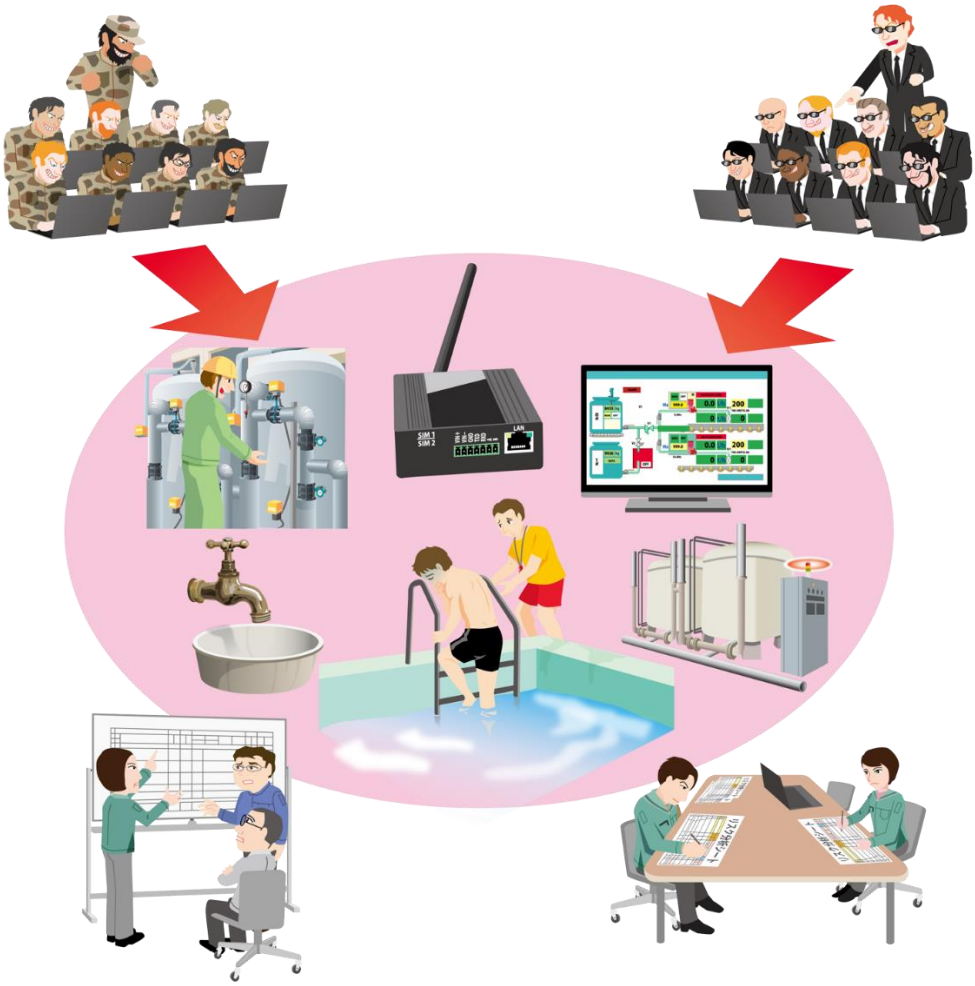
制御システムのセキュリティリスク分析ガイド補足資料

制御システム関連のサイバーインシデント事例 13

～2025 年　ポーランドの市民プールへの攻撃～



2026 年 7 月

Beyond Digital

独立行政法人
情報処理推進機構
Innovation Platform Agency, Japan

セキュリティセンター

目 次

はじめに

「セキュリティ対策を推進する上で、過去の事例に学ぶことは有益です。」

制御システムを保有する事業者にとって、国内外で発生したサイバーインシデント事例の情報をもとに、自社の制御システムに対して同様の脅威が発生した場合のリスクアセスメント（リスクの特定・分析・評価）を実施することは、セキュリティリスク管理の強化につながる。

IPA（情報処理推進機構）は、制御システムにおけるリスクアセスメントの具体的な手順を解説した『制御システムのセキュリティリスク分析ガイド』を公開している。このガイドでは、制御システム保有事業者の事業に重大な被害を与えるサイバー攻撃からの回避に重点を置いた「事業被害ベースのリスク分析手法」を紹介している。自社の制御システムに対して、過去の事例と同様の脅威が発生した場合の事業への影響、脅威の発生可能性、発生した脅威の受容可能性／脅威に対するセキュリティ対策の有効性を分析することは、事業者にとって有益であると考えられる。

「制御システム関連のサイバーインシデント事例」シリーズは、『制御システムのセキュリティリスク分析ガイド』の補足資料として作成した。制御システムのサイバーインシデント事例をもとに、その概要と攻撃の流れ（攻撃ツリー）を紹介している。これらの情報をもとに、事業被害ベースのリスク分析を実施する際に、事例に相当する攻撃ツリーの作成、セキュリティ対策の策定に活用することが出来る。

【参考資料】に関しての内容詳細は、リンクから原文を確認いただきたい。本資料では、脚注は上付き番号（例 [1]）、巻末の参考資料は[ ]付き番号（例 [1]）で表している。

本資料の位置付け

2025 年 8 月、ポーランドの首都ワルシャワの市民プールの水処理設備が乗っ取られ、水質パラメータの設定値を変更された[1]。ポーランドでは、上下水等水処理関連施設へのサイバー攻撃が多発しており、市民生活のインフラを脅かしている。

本書では、当局や政府機関、ニュースサイト等の公開情報（巻末の【参考資料】）をもとに、サイバーインシデントの概要と攻撃の流れを紹介している。後半では、当該インシデントに関係する情報を整理し、本インシデントをモデルとしたリスク分析を行う際の、攻撃シナリオや攻撃ツリー・ステップの作成例、対策・緩和策への活用例など、リスクアセスメントの際にどう活用するのかというアプローチを紹介している。

対象読者

制御システムのリスクアセスメント担当者

1. 2025 年 市民プールへの侵入と乗っ取り

1.1. インシデント概要

2025 年 8 月、ポーランドの首都ワルシャワにある市民プールの水処理設備が不正に操作され、遊離残留塩素、pH、水温などの水質パラメータの設定値が変更された。攻撃者はロシアのハクティビストであり、攻撃者が SNS にアップロードした SCADA とみられる操作画面を見ると**[1]**、結合塩素濃度（遊離残留塩素の設定値の変更に伴って変化したと考えられる）は 1.2 mg/L（厚生労働省の基準[2]では 1.0 mg/L 以下が望ましい）となっており、さらに水温は 50℃、pH は 14（強アルカリ性）に設定されるなど、遊泳には適さない条件に変更されていた。

ポーランドでは、2024 年頃から浄水場や下水処理場などの水処理関連施設へのサイバー攻撃が多発しており、本インシデントもその一例として受け止められている。CERT Polska（ポーランド・コンピュータ緊急対応チーム）[3] は、これらの水処理関連施設へのサイバー攻撃に関するレポートを公開している[4]。

これらのインシデントについては、具体的にどの施設に対してどのような攻撃手法が用いられたのかを示す明確な公開情報は見当たらない。しかし、代表例として、[4]のレポートに記載されている手法が本インシデントでも用いられたと仮定し、以下で解説を進める。

なお、解説で用いるシステム構成図として、事例理解のために作成した仮想システム構成図を掲載している。

図 1-1 欧州におけるインシデント発生地域

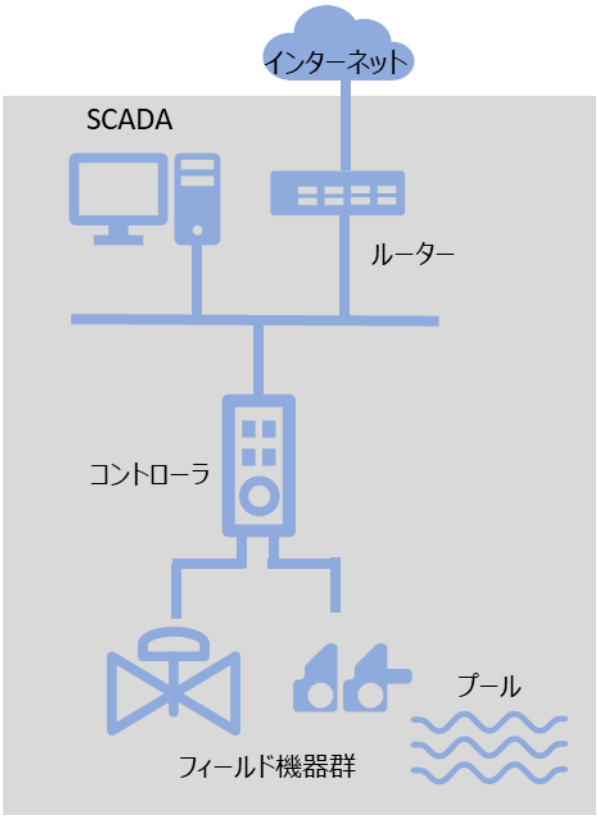


図 1-2　事例理解のための仮想システム構成図（実際のシステム構成とは異なる）

【コラム】プールへのサイバー攻撃

水処理関連施設に対するサイバー攻撃は、生活に直結するインフラへの影響が大きいため、世界各地でたびたび大きく報じられている。

中でも、浄水場で薬品の注入量を変更するような攻撃は、健康被害への懸念を連想させることから、センセーショナルに取り上げられやすい。しかし一般に、浄水場では非常に大量の水を扱っているため、薬品の設定値が変更されたとしても、短時間で重大事故につながるケースは多くない。

一方、プールの場合、浄水場と比べて容積が限られており、短時間で水質の調整が必要なため、消毒のために用いられている薬液の制御範囲が広いと考えられ、影響は比較的大きい。

実際、2024 年 7 月にワルシャワのレクリエーションセンターのプールで塩素中毒事故が発生し、20 人以上が負傷し病院に搬送されたというケースがあった[4]。なおこの事件は、サイバー攻撃との直接の関係があったとはされていない。

1.2. 被害発生にいたる攻撃の流れ

1.2 節では、公開されている参考情報に基づき、サイバー攻撃が被害の発生に至るまでの流れを、次の二つの局面に分けて解説する。なお、このプールに対する具体的な攻撃手法は公表されていないため、ここでは、CERT Polska が OT システムの保護強化に関する提言の中で示している攻撃手順[5]を参考例として紹介する。ちなみに、同じ CERT Polska が公表しているエネルギー分野のインシデントレポート[6]などにも OT に対する攻撃の情報があり、参考となる。

1.2.1【攻撃局面 A1】 対象機器の探索

攻撃者はまず、Shodan[7]、Zoomeye[8]、Censys[9]などのスキャナを利用し、インターネットに直結されているターゲットを探した。本件では特定のセルラールーター[1]がターゲットとなった。例えば実際に Shodan を使って LTE を検索すると、多数の端末が検出されることがわかる。

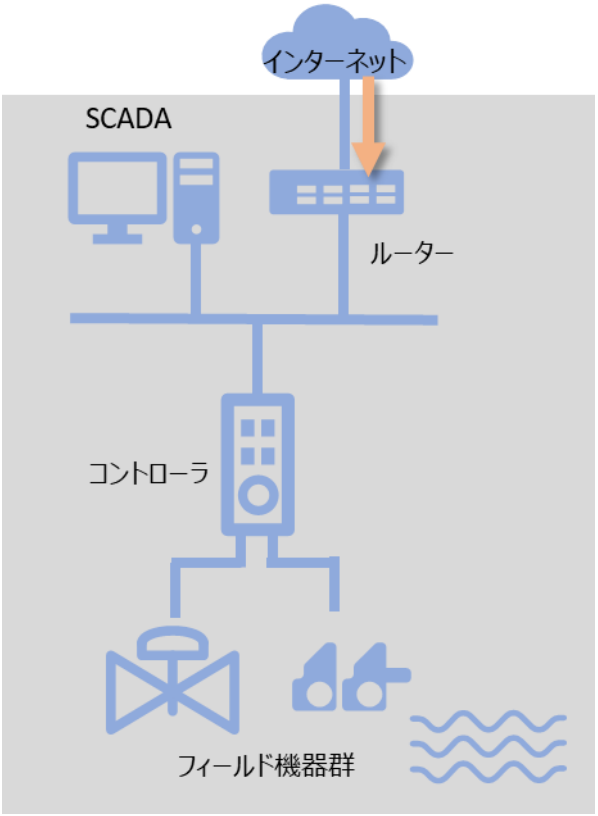


図 1-3 対象機器の探索

[1] 携帯電話回線を使って複数の機器からインターネット接続できるルーター

1.2.2【攻撃局面 A2】 ネットワーク内部の調査と横展開

本件で利用されていたと仮定する ELMARK 社製セルラールーターでは、デフォルト設定のまま WAN 側に設定用 Web パネルが公開されていた。加えて、認証情報も初期値のまま変更されていなかった。

当該 Web パネルでは SSH[2]によるアクセスの設定が可能であり、攻撃者は SSH サービスを有効化し、SSH コマンドを用いて侵害ルーター上に不正に SOCKS プロキシを構築した。SOCKS プロキシは、接続元コンピュータとインターネットの間を中継する機能であり、Web 通信のみを対象とする HTTP プロキシに比べ、より汎用的に TCP 通信（または TCP/UDP 通信[3]）を中継できる。

その結果、攻撃者はルーターを経由して、インターネットから標的システム内部へ接続するための通信経路を確立した。

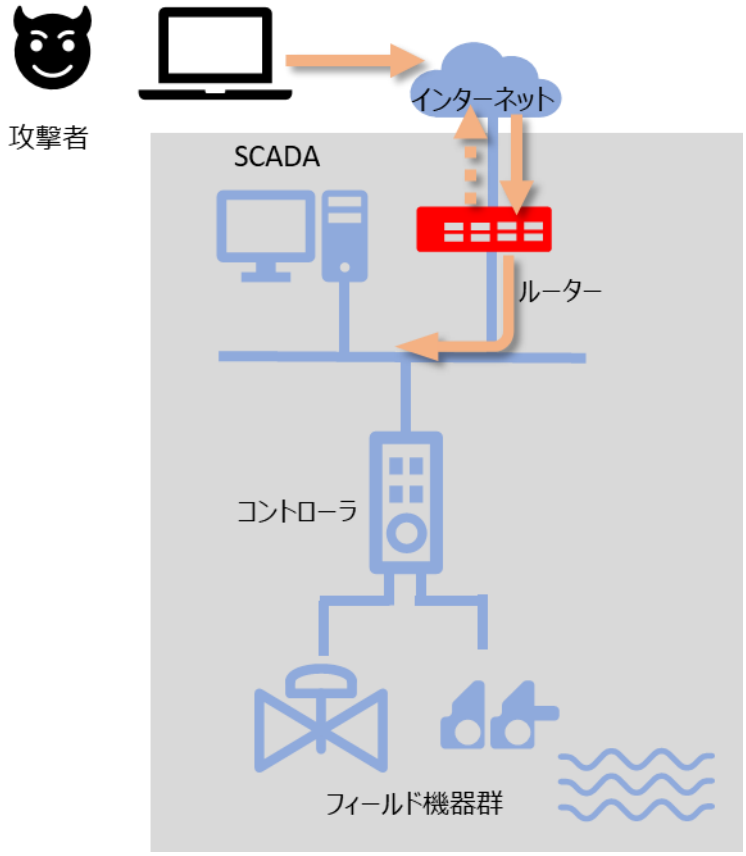


図 1-4　ネットワーク内部の調査と横展開

[2] SSH(セキュアシェルプロトコル):リモート操作を暗号化された通信を使うプロトコル（通信方式）
[3] 新しいバージョンの SOCKS5 は TCP/UDP に対応。それ以前のバージョンは TCP のみ。

1.2.3【攻撃局面 A3】 SCADA の攻略

攻撃者は、ネットワーク内の SCADA を見つけ、ログインした。SCADA の認証情報はデフォルトのままであったために、容易に SCADA にログインする事が出来た。(以降図の攻撃者は省略)

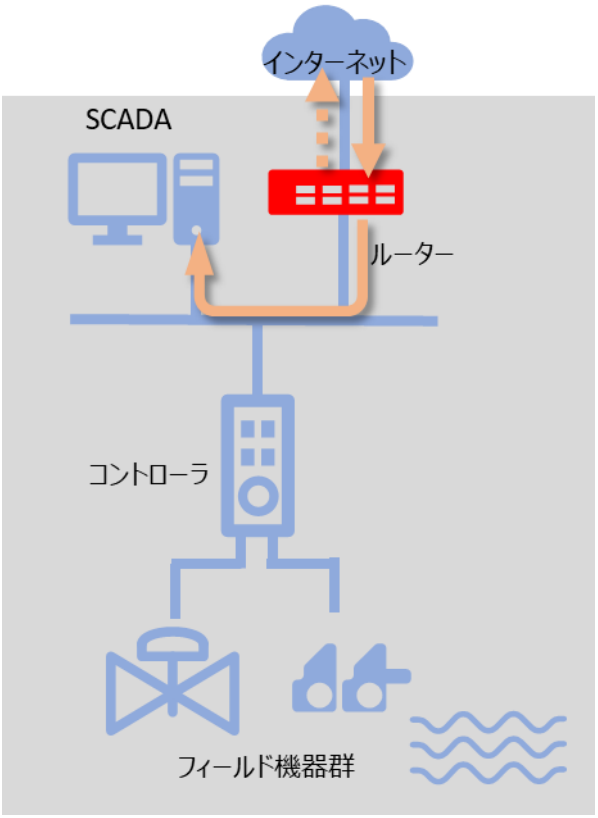


図 1-5 SCADA の攻略

1.2.4【攻撃局面 A4】 SCADA パラメータの悪意ある設定

攻撃者は、プールに悪影響を与えられるよう、水温、残留塩素量、pH のパラメータを異常値に設定した。この操作は正規のユーザーによる設定変更であるため、疑いなく設定が可能であった。

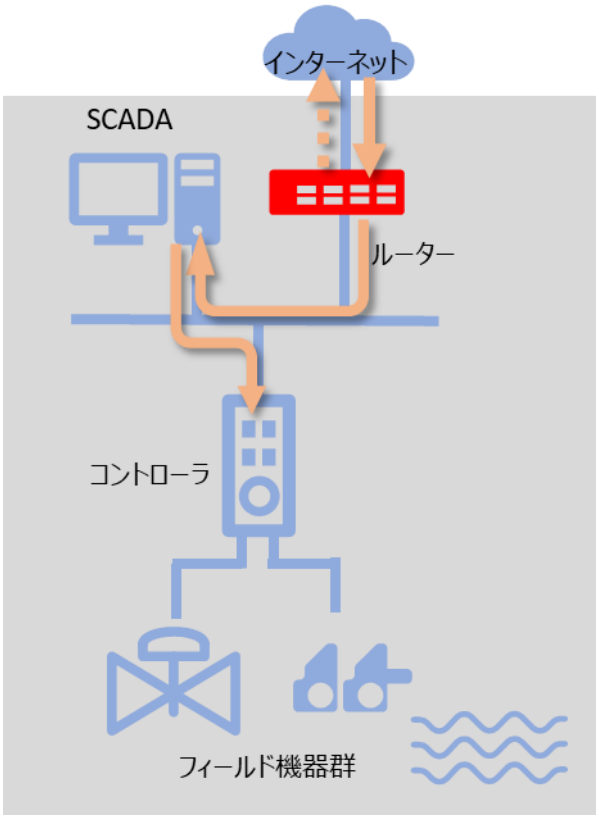


図 1-6 SCADA パラメータの悪意ある設定

1.2.5【攻撃局面 A5】 水質の改悪

攻撃者は、SCADA の操作画面をキャプチャし SNS へ投稿、影響力を誇示した。なお、この攻撃により発生した明確な被害は報告されていない。

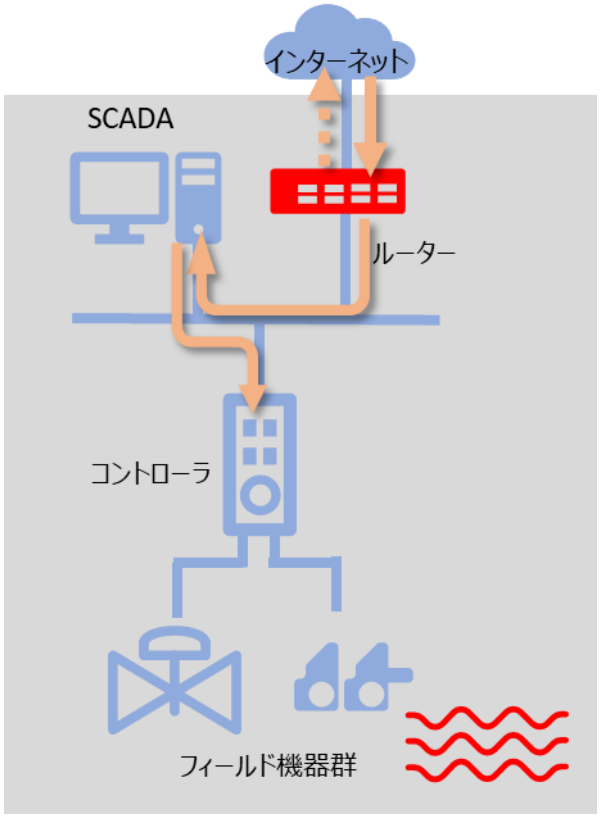


図 1-5 水質の改悪

2. リスク分析（事業被害ベース）の素材としてのインシデント情報の整理

2.1. 事業被害と攻撃シナリオの検討

本インシデントを参考に、検討した事業被害の例を表 2-1 に示す。

2.2 節では、この事業被害と攻撃シナリオに至る攻撃ツリーを検討する。

表 2-1 事業被害の例

項番	事業被害			
1	プール利用者に健康被害が発生する			
	攻撃シナリオ	攻撃拠点	攻撃対象	最終攻撃
	SCADA操作により、プールの水質パラメータを異常値に設定される	SCADA	コントローラ	異常値の設定

また、事業被害に至る攻撃ルートの例を表 2-2 に示す。

表 2-2 攻撃ルートの例

項番	誰が	どこから	どうやって	どこで		何をする
	攻撃者	侵入口	経由	攻撃拠点	攻撃対象	最終攻撃
1	悪意ある外部者	インターネット	セルラールーター経由の侵入	SCADA	コントローラ	異常値の設定

2.2. 攻撃ツリーの作成

今回のインシデント事例をリスク分析における攻撃ツリー・ステップの枠組みにあてはめ整理した内容が表 2-3 となる。分析対象の範囲などによっては切り出し方のパターンは考えられるが、一例として参照いただきたい。

表 2-3 事業被害：インターネット接続停止の例

攻撃局面	攻撃ステップ項番	攻撃シナリオ 攻撃ツリー・ステップ ＜モデムの機能を損ない、インターネット接続を不能にする＞
【A1】	S1	侵入口= インターネットからセルラールーターにデフォルトの認証情報を利用し侵入する
【A2】	S2	セルラールーターの Web 設定画面で SOCKS プロキシを立ち上げ、システム内部ネットワークへ侵入する
【A3】	S3	デフォルトのパスワードを使い SCADA へログインする
【A4】	S4	SCADAの操作画面からプールの水質設定値を変更する
【A5】	S5	設定値の変更によりプールの水質が不適切な状態となる

2.3. 事業被害ベースのリスク分析の分析要素のまとめ

本インシデントをリスク分析の際の素材として活用するために、1.2 節で紹介した攻撃局面を分析ガイドで説明している事業被害ベースの分析要素毎にまとめた結果が表 2-4 となる。

表 2-4 各種情報をもとにした分析要素のまとめ

分析要素		内容
攻撃用途		
	侵入口	セルラールーター
	攻撃対象	コントローラ
	攻撃拠点	SCADA
	経由	—
攻撃者		悪意ある外部者
事業被害		プールの水質の悪化
攻撃シナリオ		SCADA操作により、プールの水質パラメータを異常値に設定する
最終攻撃（目的）		水質の悪化
攻撃ルート		表 2-2 を参照
攻撃ツリー		表 2-3 を参照
攻撃手法		不正アクセス リモートサービスの悪用 ネットワーク上のコンピュータのスキャン SCADA への有効なアカウントによるログイン SCADA の操作

リスク分析を進める上では、日々の活動を通じて実際のインシデント事例などの情報収集を行い、最新動向をキャッチアップし、事例毎に表 2-4 のように整理した情報を蓄積していくことが肝要となる。

2.4. 対策・緩和策の整理

対策・緩和策の検討を進める上で、本資料でも参照している CERT.Polska が公開している「OT システムの保護強化に関する提言」[5]、上記提言で記載されているセルラールーターの製造元 ELMARK 社[10]が公開しているセキュリティ対策[11]を元に、制御システムに対する主な緩和策を整理した。
表 2-5 は、当事例に参考となる代表的な対策・緩和策をまとめたものとなる。

表 2-5 代表的な対策・緩和策の例

項番	対策・緩和策
D1	携帯電話ネットワークを利用する場合は、プライベート APN[4]を使用する[5]
D2	リモートアクセスが必要な場合は必要最小限とし、多要素認証とする[5][11]
D3	VPN アクセスを特定の IP アドレスに制限する[5]
D4	ネットワークのセグメント分割を行う [5]
D5	デフォルトの認証情報を変更して強力なパスワードとする[5][11]
D6	トラフィックの監視[5]
D7	ファームウェアが最新であることを確認する[11]
D8	ログの取得[11]

「D1. 携帯電話ネットワークを利用する場合は、できればプライベート APN を使用する」携帯電話ネットワークを介したテレメトリーデータのリモート通信が必要な場合、プライベート APN を利用する事を推奨する。プライベート APN では、インターネットを介さず通信キャリアのネットワーク内通信を行う事ができる。

「D2. リモートアクセスが必要な場合は必要最小限とし、多要素認証とする」リモートアクセス機能が不要な場合はサービスを止め、必要な場合は必要なアカウントにのみ多要素認証を用いて使用させる。特に、携帯電話モデムや下請け業者のリモートアクセス方法には注意を払う。

「D3. VPN アクセスを特定の IP アドレスに制限する」 可能な限り VPN アクセスを受け入れる IP アドレスを利用業者や国内等で制限する。

「D4. ネットワークのセグメント分割を行う」内部ネットワークを複数のセグメントに分割して運用することで、被害範囲が容易に拡大する事を防ぐ。

[4]インターネット回線を介さず、閉域網や企業ネットワーク回線に直接接続するゲートウェイ。APN:アクセスポイント名(Access Point Name)

「D5. デフォルトの認証情報を変更して強力なパスワードとする」デフォルトで設定されているパスワードは利用せず、強力なパスワードに変更する。また、使用していないアカウントを無効にする。

「D6. トラフィックの監視」通信機器への出入口に監視機能を追加し、予期しない通信やアクセスを監視する。

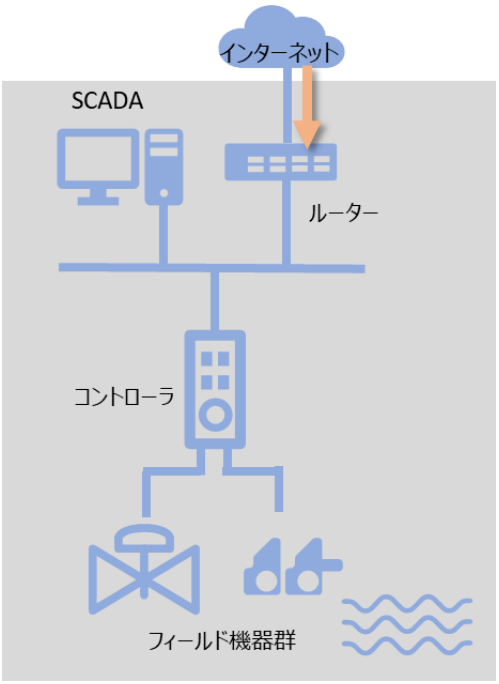
「D7. ファームウェアが最新であることを確認する」 脆弱性の発見されたソフトウェアやファームウェアに対し、すぐにアップデートを行えるようにし、常にシステムを最新の状態を保つ。

「D8. ログの取得」 システム上で行われるリモート操作はすべて、時間、目的、および作業の発生源を明確に識別できる方法でログに記録する必要がある。

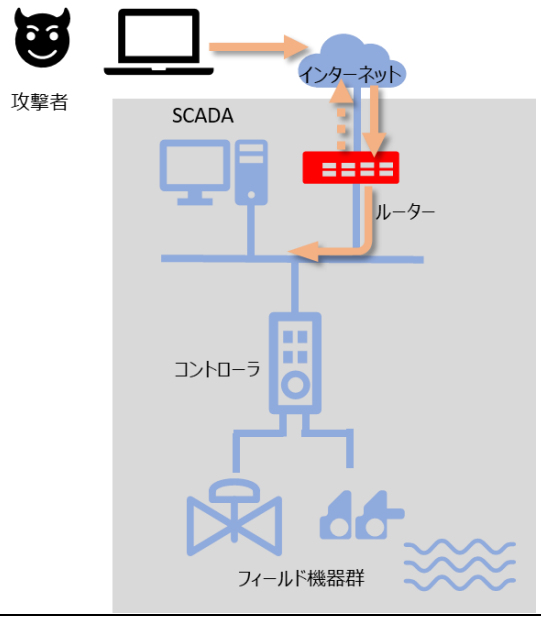
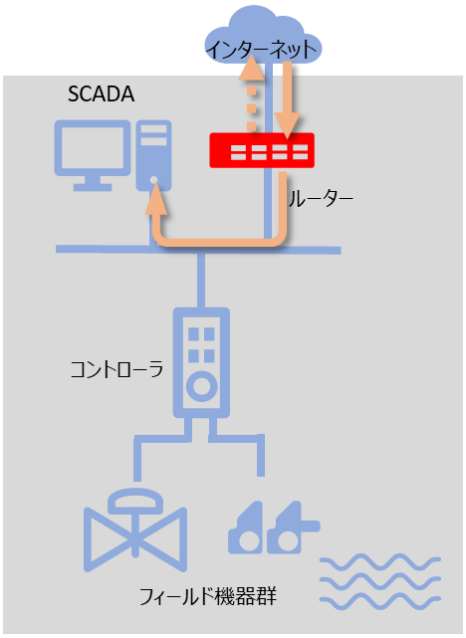
2.5. 攻撃ステップと対策・緩和策の関連付け

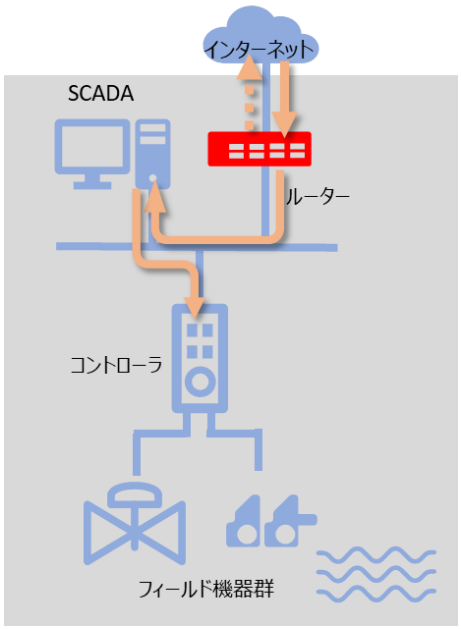
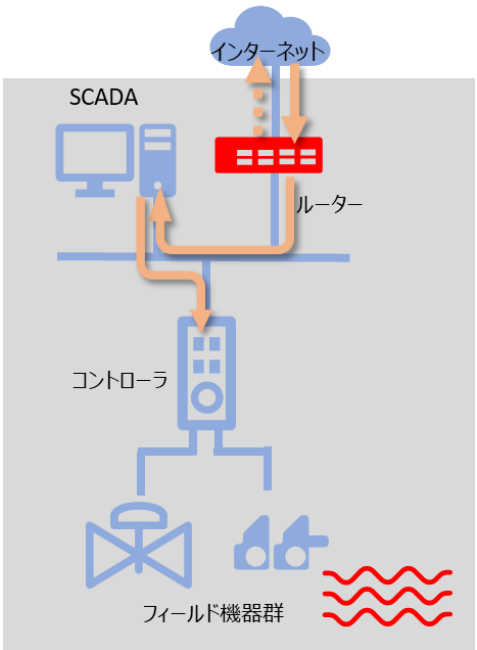
2.4 節までの情報をもとに、【攻撃局面 A1～A4】の代表的な対策・緩和策を紐づけた例が表 2-6 となる。セキュリティ対策の基本である「多層防御」を考慮し、緩和策を立案することがポイントとなる。

表 2-6 制御システムにおける攻撃ステップと対策・緩和策の紐づけ例

攻撃局面	攻撃ステップ[5]	対策・緩和策	対象システム・資産
【攻撃局面 A1】  	[S1] 対象機器の探索	•携帯電話ネットワークを利用する場合は、プライベート APN を使用する[D1] •リモートアクセスが必要な場合は必要最小限とし、多要素認証とする[D2] •VPN アクセスを特定の IP アドレスに制限する[D3] •デフォルトの認証情報の変更[D5] •トラフィックの監視[D6] •ファームウェアが最新であることを確認する[D7] •ログの取得[D8]	•セルラールーター

[5] [S]は表 2-3 の項番と対応。[D]は表 2-5 の項番と対応。

攻撃局面	攻撃ステップ	・対策・緩和策	対象・システム・資産
【攻撃局面 A2】  	[S2] ネットワーク内部の調査と横展開	・ネットワークのセグメント分割を行う[D4] ・トラフィックの監視[D6] ・ログの取得[D8]	・ネットワーク
【攻撃局面 A3】  	[S3] SCADA の攻略	・デフォルトの認証情報の変更[D5] ・ファームウェアが最新であることを確認する[D7] ・ログの取得[D8]	・SCADA

攻撃局面	攻撃 ステップ	・対策・緩和策	対象 システム・資産
【攻撃局面 A4】  	[S4] SCADA パラメータの悪意ある操作	・ログの取得[D8]	・コントローラ
【攻撃局面 A5】  	[S5] 水質の改悪	-	・（プール）

おわりに

本資料では、制御システムにおけるインシデント事例を紹介すると共に、セキュリティリスクアセスメントへの活用方法について一つのアプローチを紹介した。

事業被害ベースのリスク分析においては、自社の制御システムにとって回避すべき事業被害を明確化し、被害に至る攻撃シナリオと攻撃ルートを漏れなく洗い出すことが重要である。攻撃シナリオは、過去に発生した制御システムのインシデント事例を含む各種の公開情報を参考にしつつ、自社の制御システムに生じ得る脅威とその影響を検討するが、具体的な攻撃ルート・攻撃手順を想定することで、セキュリティ対策を効率的に進めることが可能となる。

本資料が各社の制御システムのセキュリティ向上に活用されることを期待する。

参考資料

[1] CyberDefence24:Prorosyjscy haktywiści: „atakujemy polskie baseny”. Propaganda?
https://cyberdefence24.pl/cyberbezpieczenstwo/prorosyjscy-haktywisci-atakujemy-polskie-baseny-propaganda

[2] 厚生労働省:遊泳用プールの衛生基準について
https://www.mhlw.go.jp/bunya/kenkou/seikatsu-eisei01/pdf/02a.pdf

[3] The CERT Polska.
https://cert.pl/

[4] Masowe zatrucie na warszawskim basenie. Policja zatrzymała trzy osoby [WIDEO]
https://www.tvp.info/79508984/warszawa-zatrucie-chlorem-na-basenie-policja-zatrzymala-trzech-pracownikow

[5] CERT Polska: Rekomendacje dla wzmocnienia ochrony systemów OT
https://cert.pl/posts/2024/05/rekomendacje-ot/

[6] Cyberatak na infrastrukturę sektora energii w Polsce. Opublikowano szczegółowy raport CERT Polska
https://www.gov.pl/web/cyfryzacja/cyberatak-na-infrastrukture-sektora-energii-w-polsce-opublikowano-szczegolowy-raport-cert-polska

[7] Shodan: Search Engine for the Internet of Everything
https://www.shodan.io

[8] Zoomeye
https://www.zoomeye.ai/

[9] Censys
https://search.censys.io/

[10] ELMARK
https://www.elmark.com.pl/

[11] ELMARK: Sparrow NW10/NW20 - zadbaj o cyberbezpieczeństwo!
https://www.elmark.com.pl/blog/sparrow-nw10nw20-zadbaj-o-cyberbezpieczestwo

更 新 履 歴

2026 年 7 月 31 日	初版	ー

制御システムのセキュリティリスク分析ガイド補足資料

制御システム関連のサイバーインシデント事例 13

～2025 年 ポーランドの市民プールへの攻撃～

[発　行]　2026 年 7 月 31 日　第 1 版

[著作・制作]　独立行政法人情報処理推進機構　セキュリティセンター
編集責任　市野澤 昌弘
執筆者　福原　聡
協力者　内田　努，高見　穣, 松島　伸彰