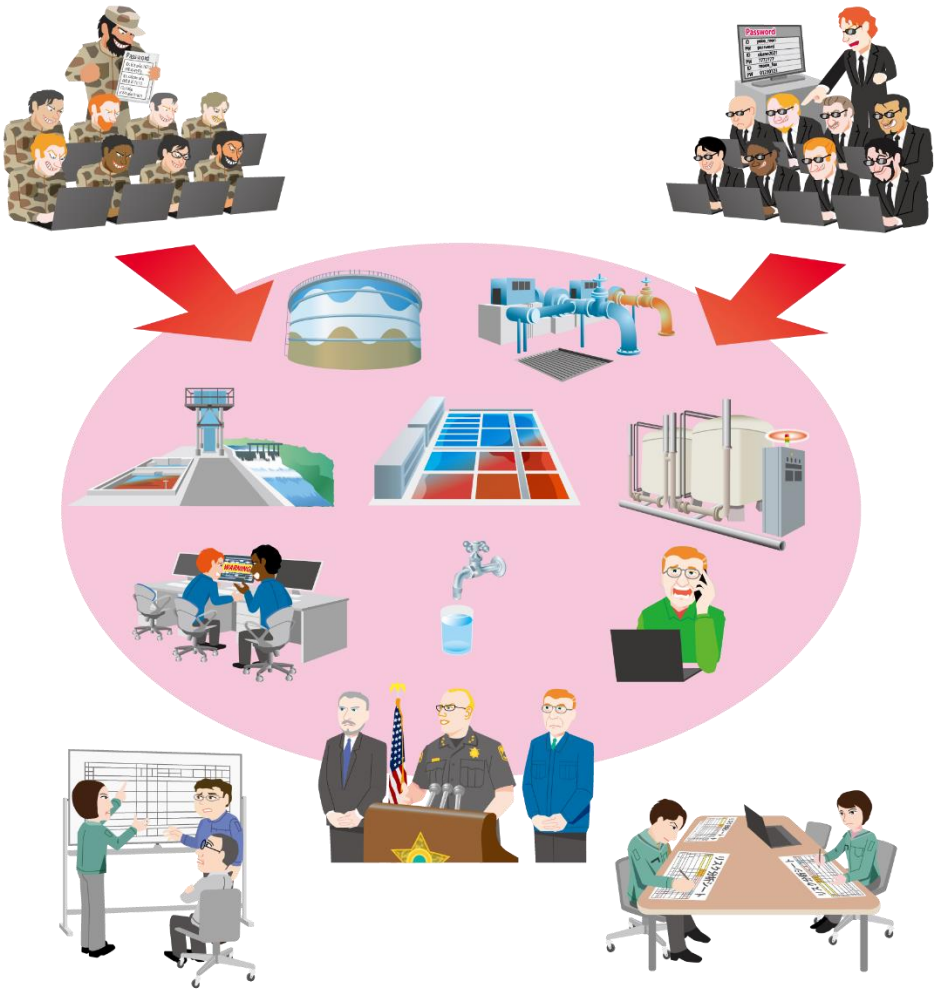
制御システムのセキュリティリスク分析ガイド補足資料

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 独立行政法人情報処理推進機構
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

2021 年 2 月米国フロリダ州 Oldsmar の水道局で、飲料水に投入する薬液設定量が何者かによって変更され、一時的に大量の薬液が投入されるというインシデントが発生した[1]。

本書では、当局や政府機関、セキュリティベンダ等の公開情報（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. 2021 年 水道局への不正侵入と飲料水汚染未遂

1.1. インシデント概要

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、人的被害は発生しなかった[2]。

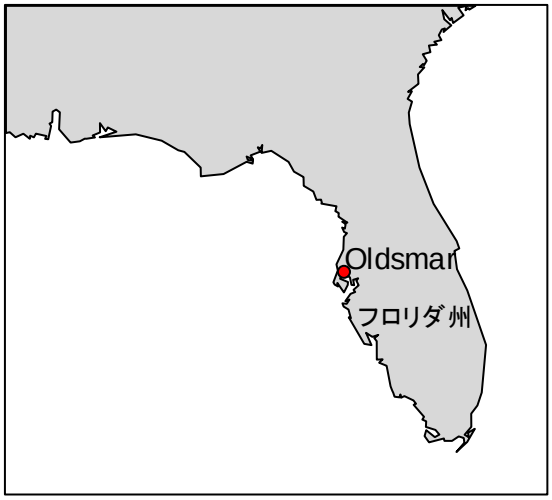


図1 米国におけるインシデント発生地域

このときの設定値は、通常の水酸化ナトリウム濃度の 100ppm から 100 倍以上の 11,100ppm まで高められた[1]。水酸化ナトリウムは、水処理施設において酸性度の中和に用いられるが、液体排水管クリーナー等の主成分として用いられる危険な薬品でもある。

高濃度の水酸化ナトリウムは飲み込むと嘔吐や吐き気、下痢等の症状をひきおこす劇物に指定されている。

今回の水処理施設においては、処理水を供給するまでに 24 時間から 36 時間を要するため、汚染された水の供給を阻止することが出来たと考えられるが、発見が遅れた場合、重大な人的被害を及ぼす恐れのあるインシデントであった。

今回は報道やセキュリティ企業の情報を参考に補完・推考しながら、サイバー攻撃の状況を IEC 62443 や NIST SP800-82 Rev.2 等をもとに作成した仮想システム構成図（図 1-1）を用いて説明する。

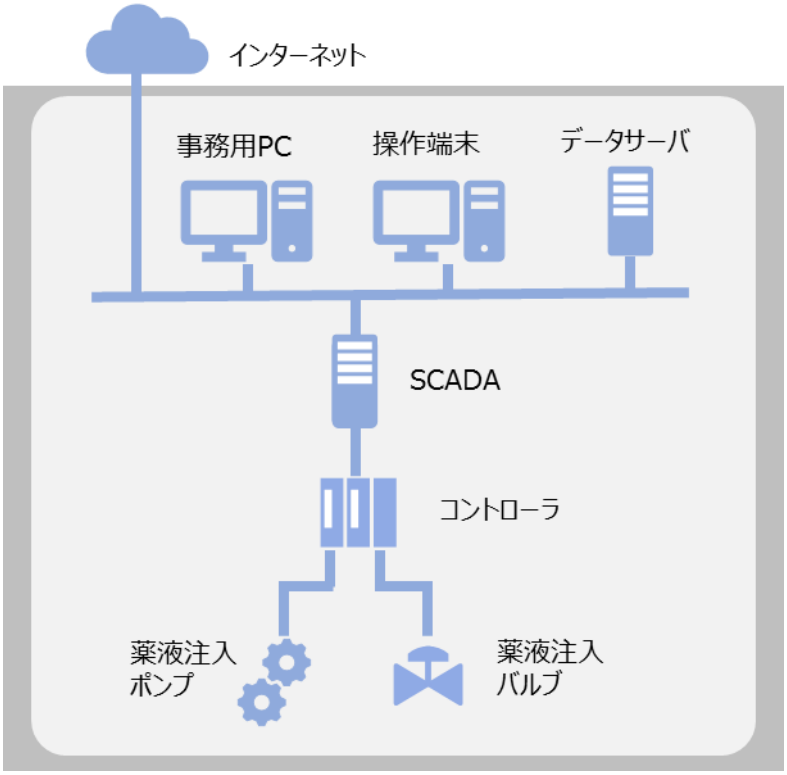


図 1-1　事例理解のための仮想システム構成図（実際のシステム構成とは異なる）[1]

【コラム】攻撃者は単一とは限らない

フロリダの水道局が狙われた本インシデントは 2021 年 2 月に発生しすぐに報道されたが、2021 年 5 月に新たな事実が発表された。Dragos の調査によると[3]、フロリダの水インフラ建設企業のホームページが 2020 年 12 月 20 日に改ざんされ、2021 年 2 月 16 日までの 58 日間、訪問者の情報を窃取していた。このホームページはフロリダを中心とした水上事業者、州および地方政府機関、水道関連企業などがアクセスしており、いわゆる「水飲み場攻撃」に悪用されていたと分析されている。

また、Oldsmar の当該水道局も 2 月 5 日、つまりインシデントが発生した当日に、このサイトにアクセスした記録が残されていた。

しかしながら、この水飲み場攻撃と本インシデントの関連は薄いと判断されている。その一つの根拠は、このサイトにアクセスした時間が午前 9 時 49 分であったことに対し、Oldsmar への正体不明者の最初の侵入は午前 8 時頃だったことがあげられる。[4]

即ち、複数の攻撃者がフロリダの水道局を狙っていたと考えられている。

[1] SCADA: Supervisory Control And Data Acquisition

1.2. 被害発生にいたる攻撃の流れ

1.2 節では、参考情報で公開されている内容をもとに、サイバー攻撃から被害発生にいたるまでの流れを次の 2 つの局面に分けて解説する。

1.2.1【攻撃局面 A1】対象組織への不正侵入

攻撃者はインターネット上から遠隔操作ソフトウェア TeamViewer[2]を用いて事務用 PC にログインする[5]。TeamViewer は ID とパスワードの様な認証情報が必要だが、今回のインシデントにおいてどのような方法でその情報を入手したのかははっきりしていない。前ページのコラムに書いたように、当該システム上のコンピュータから外部の Web ページを閲覧しており、そこからの情報の漏えいの可能性がある。

あるいは、当該システムはファイアウォールも無くインターネットに直結されていたことから、Shodan[3]による検索などの手法で IP アドレスやオープンポート、位置などの情報を収集することができ、これらを利用されたとの見方もある。

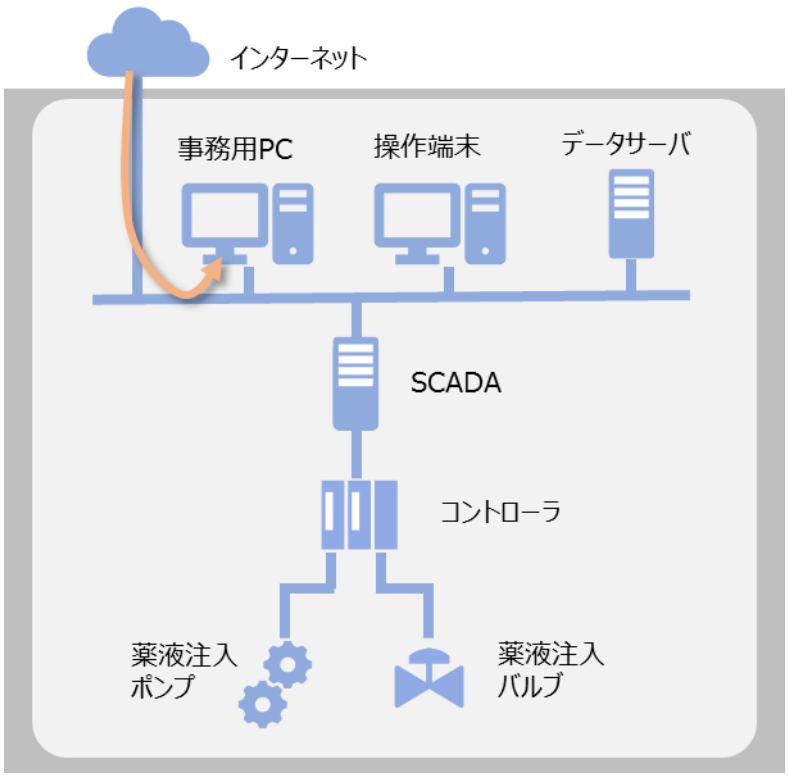


図 1-2 対象組織への侵入

[2] Teamviewer.com

[3] インターネットに直結された Web カメラ、IoT 機器、制御機器等の検索エンジン

1.2.2【攻撃局面 A2】ネットワーク内部の調査

攻撃者は水道局内のネットワークを探索し、制御系の操作が可能な操作端末を探す。

本インシデントでは、2021 年 2 月 5 日午前 8 時に最初の侵入があったことが報告されている[1]。この時点は制御系の操作は行われておらず、ネットワーク内部の探索が行われた可能性がある。(図 1-3)。

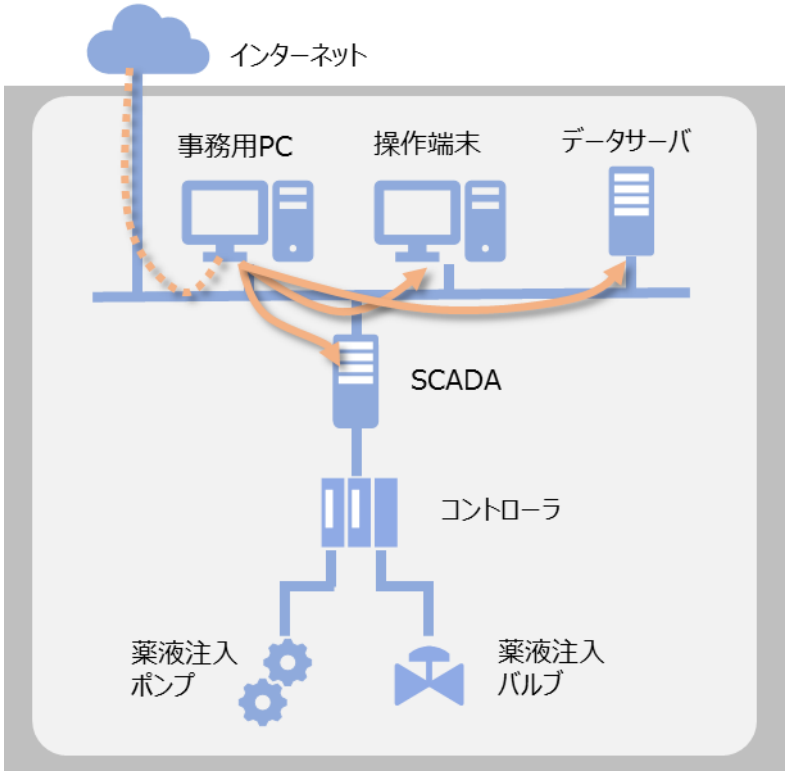


図 1-3 ネットワーク内部の調査

1.2.3【攻撃局面 A3】 操作端末へのリモートログイン

ネットワーク内部の調査により判明した SCADA の操作端末の TeamViewer ログイン ID（おそらくコンピュータ名等の情報から容易に推測できた）と事務用 PC にログインした際に利用したパスワードを使って、操作端末にログインする。このログインは、最初の侵入があった同日の 2021 年 2 月 5 日 13:30 に行われたと報道されている[1]。

本インシデントでは、局内の TeamViewer のパスワードは、全ての PC で共通な値が使用されていた、報道されている。（図 1-4）。

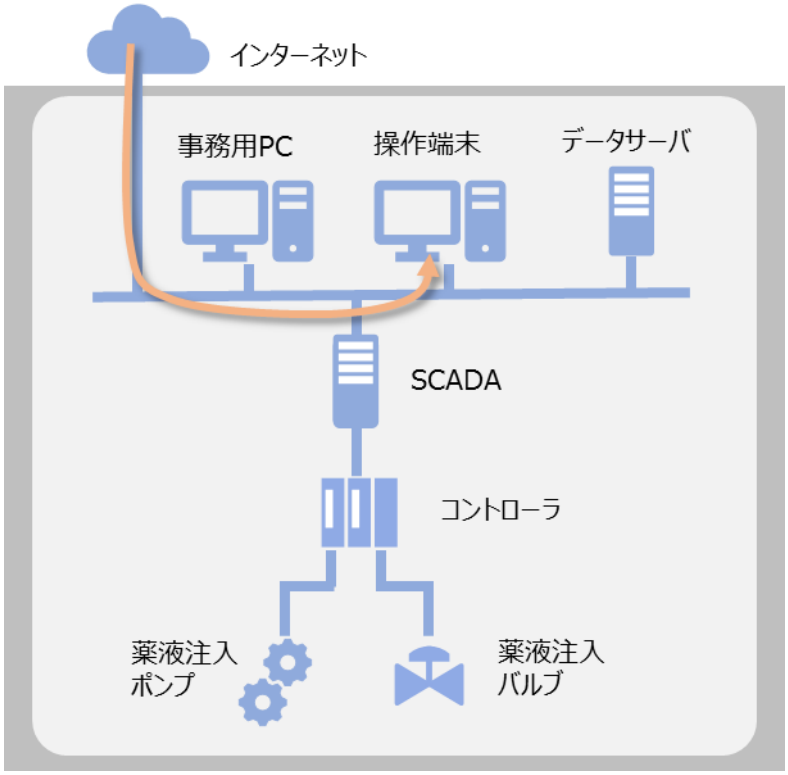


図 1-4 操作端末へのリモートログイン

1.2.4【攻撃局面 A4】 制御装置の遠隔操作

SCADA の操作画面から、水酸化ナトリウムの濃度を正常値の 100ppm から、11,100ppm に変更した。(図 1-5)

なお、TeamViewer では、遠隔操作をしている画面がそのままローカルに表示されていたため、現場のオペレータが異常な設定にすぐに気づいて設定値を元の正常値に戻し、接続を遮断し、大きな被害にはならなかった。

また水道局には各種のセンサがあり、例え濃度が変更されても異常を検知可能な仕組みを備えている。しかしながら、サイバー攻撃によっては、Stuxnet の例[6]に示される様に、センサの値が詐称される場合もあり、別系統の検出機構があるから十分な対策を実施済みとは必ずしも言い切れない。

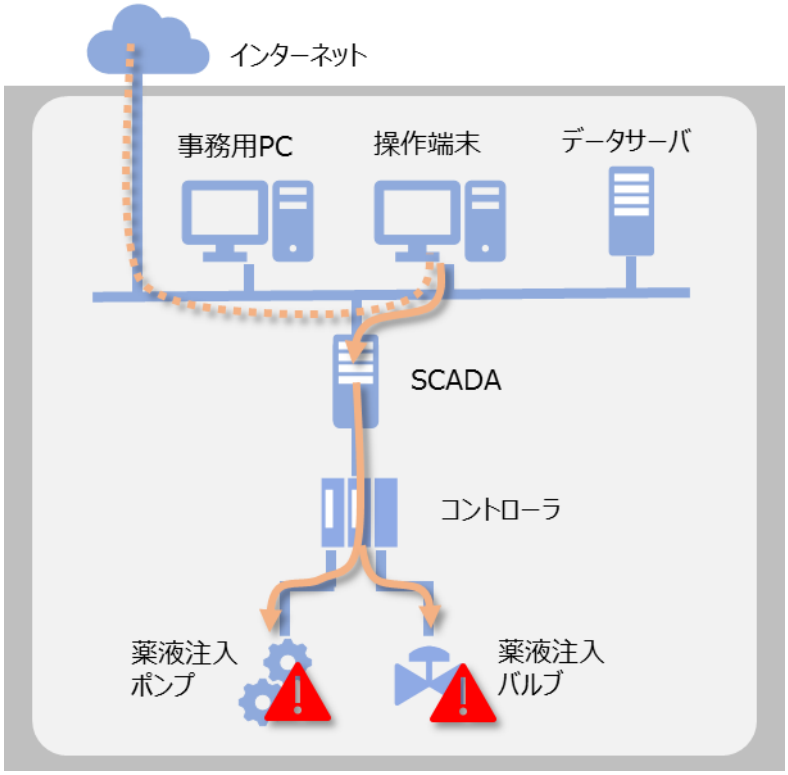


図 1-5 SCADA による薬液注入量の悪意ある変更

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	飲料水の供給停止			
	攻撃シナリオ	攻撃拠点	攻撃対象	最終攻撃
	飲料水に異常な量の薬液が注入され、有害で飲料として供給できなくなる。	SCADA	コントローラ	薬液注入量の変更

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（下線はリスク分析をする上での IPA による想定）

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	遠隔操作ソフトからの侵入	SCADA	コントローラ	設定値の変更

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:製造システムの操業停止の例

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 ＜遠隔操作ソフトに不正アクセスして SCADA を遠隔操作し、設定値を変更する。＞
【A1】	S1	侵入口= インターネット*1[4]から TeamViewer が稼働している事務用 PC に侵入する
【A2】	S2	事務用 PC から局内ネットワークを探索し SCADA を操作する操作端末のコンピュータ ID を窃取する
【A3】	S3	操作端末の TeamViewer にログインする
【A4】	S4	操作端末の SCADA の操作画面で、薬液投入量の設定値を変更する

4 当該システムはファイアウォール無しに直接インターネットに接続されていたと報道されている。

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	インターネット
	攻撃対象	コントローラ
	攻撃拠点	SCADA
	経由	操作端末
攻撃者		悪意ある外部者
事業被害		飲料水の供給停止
攻撃シナリオ		SCADA の設定値の変更により飲料水に異常な量の薬液が注入され、有害で飲料として供給できなくなる。
最終攻撃（目的）		薬液投入量の変更
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 ネットワーク上のコンピュータのスキャン SCADA の遠隔操作

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 ICS-CERT から公表された、AlertAA21-042A[7]、Water ISAC が公開している『15 Cybersecurity Fundamentals for Water and Wastewater Utilities[8]』を例に、リスク分析作業に活用するための制御システムに対する緩和策を整理した。表 2-5 は、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	オペレーティングシステムを最新バージョンに更新する[4]
D2	多要素認証の使用[4]
D3	強力なパスワードを使用して、リモート接続を保護する[4]
D4	制御ネットワークのインターネットとの境界の設置[5]
D5	ウィルス対策、スパムフィルター、ファイアウォールの利用と適切な構成[4]
D6	全てのリモート接続プロトコルの監査ログをとる[4][5]
D7	ソーシャルエンジニアリングの試みを特定して報告するようユーザをトレーニングする[4]
D8	リモートコントロールソフトウェアの手動起動の設定[4]

「D1. オペレーティングシステムを最新バージョンに更新する」は、ベンダーがサポートしている OS を用いるとともに、アップデートを確実に行い、公表された脆弱性への対策を行うということを意味している。本インシデントでは 2020 年 1 月にサポートが終了した[5]Windows 7 を使用し続けていた[5]。

「D2. 多要素認証の使用」 OS やリモートソフトのログイン方法として多要素認証を使うことで安全性を高める。

「D3. 強力なパスワードを使用して、リモート接続を保護する」 簡単に推測できないパスワードを利用し、ユーザやコンピュータ毎に異なるパスワードを利用する。本インシデントでは、複数の利用者でリモートソフト TeamViewer の同じパスワードが利用されていたと報告されている。

「D4. 制御ネットワークのインターネットとの境界の設置」 インターネットと制御ネットワークの境界にはルータやファイアウォールなどを設置し、制御ネットワークをインターネットから保護する。

[5] Windows 7 でも、「Windows 7 Extended Security Update(ESU)」という個別サポートサービスを Microsoft 社で提供しており、この適用により 2023 年までサポートを受け続けることは可能。

「**D5. ウィルス対策、スパムフィルター、ファイアウォールの利用と適切な構成**」は、可能であればアンチウィルス、スパムフィルター、ファイアウォールを導入し、導入するだけでなくファームウェアやパターンファイルを常に最新の状態に保つことが重要である。

「**D6. 全てのリモート接続プロトコルの監査ログをとる**」は、外部からのリモート接続の時間や接続元などの情報を記録しておくことで、インシデント発生時の対応をスムースに行うことができる。

「**D7. ソーシャルエンジニアリングの試みを特定して報告するようユーザをトレーニングする**」システムへのログイン ID やパスワード、コンピュータ名を聞きだす行為に関して、ユーザに敏感になってもらえるようトレーニングをおこなう。

「**D8 リモートコントロールソフトウェアの手動起動の設定**」は、リモート接続が可能なアプリケーションと関連するバックグラウンドサービスを、必要が無い時に停止し、必要な時のみ手動起動を行うよう設定する。

【コラム】サイバーフィジカルのセキュリティ対策

ICS-CSRT の AlertAA21-042A では、前ページまでで説明した、制御システムのサイバーセキュリティの視点からの対策に加えて、サイバーフィジカルの視点からのセキュリティ対策についても言及されている。

具体的には、水道設備へのサイバー攻撃を軽減するための物理的なシステムの事であり、以下の様な項目が AlertAA21-042A に物理的な安全システム制御としてリストアップされている。

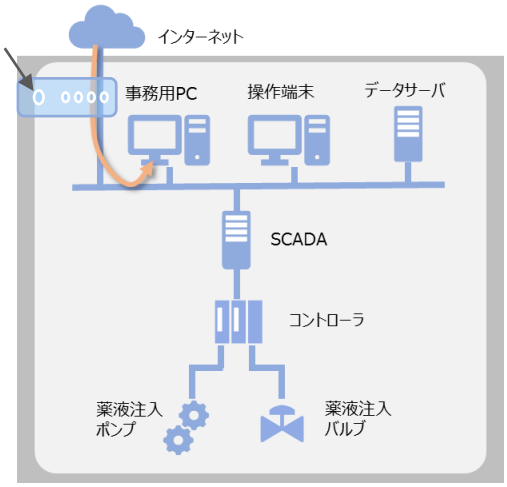
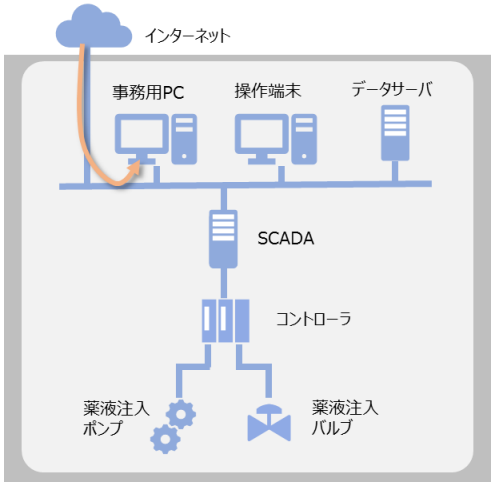
・薬液用ポンプのサイズ
・薬液用タンクのサイズ
・バルブのギア比
・圧力スイッチ　等

これらの物理的な措置（薬液投入量の上限値の制限）により、短時間に標準的な供給量を大きく上回る薬液が投入されるリスクは低減することができる。

2.5. 攻撃ステップと対策・緩和策の関連付け

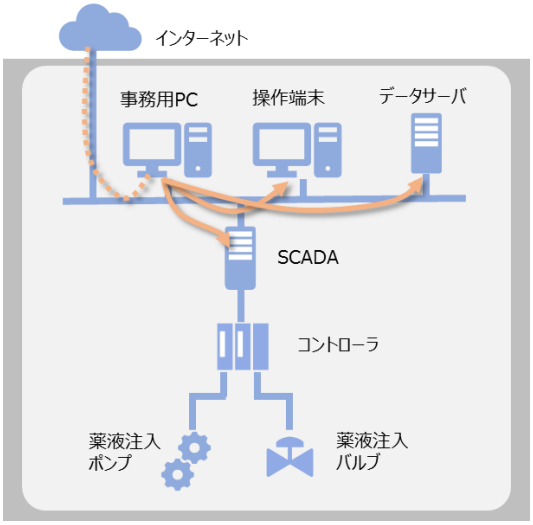
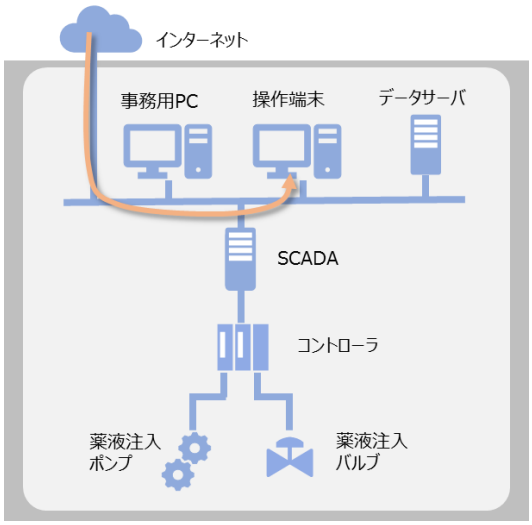
2.3 節までの情報をもとに、【攻撃局面 A1～A4】の代表的な対策・緩和策を紐づけた例が表 2-6 となる。セキュリティ対策の基本である「多層防御」を考慮し、緩和策を立案することがポイントとなる。

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

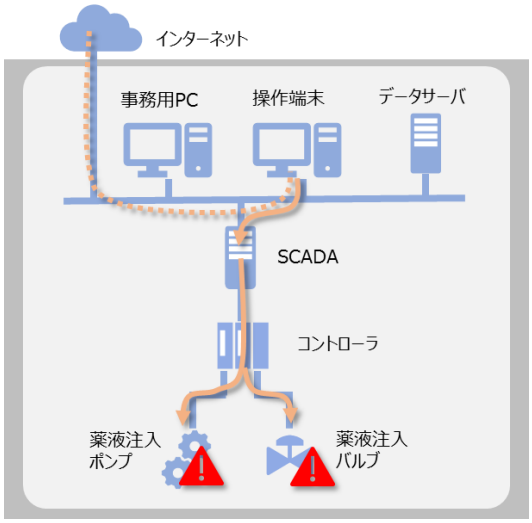
攻撃局面	攻撃ステップ[6]	対策・緩和策	対象システム・資産
【攻撃局面 A1-1】 ファイアウォール 	[S1]対象組織への侵入	•制御ネットワークとインターネットとの境界（ファイアウォール）の設置[D4] •ファイアウォールの利用と適切な構成[D5]	•ファイアウォール[7]
【攻撃局面 A1-2】 	[S1]対象組織への侵入	オペレーティングシステムを最新バージョンに更新する[D1] ・多要素認証の使用**[D2]** ・強力なパスワードを使用**[D3]** ・リモート接続プロトコルの監査ログ**[D6]** ・ソーシャルエンジニアリング対策トレーニング**[D7]** ・リモートコントロールソフトウェアの手動起動**[D8]**	•事務用 PC

6 [S]は表 2-3 の項番と対応。 [D]は表 2-5 の項番と対応。

7 例えばクラウド利用のリモートソフト等では本対策が有効でないケースもある。

攻撃局面	攻撃ステップ[8]	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	•オペレーティングシステムを最新バージョンに更新する [D6] •ウィルス対策の利用と適切な構成**[D5]** •	•操作端末 •データサーバ •SCADA
【攻撃局面 A3】  	[S3] 操作端末へのリモートログイン	•多要素認証の使用[D2] •強力なパスワードを使用して、リモート接続を保護する**[D3]** ・ソーシャルエンジニアリング対策トレーニング**[D7]** • リモートコントロールソフトウェアの手動起動の設定**[D8]**	・操作端末

[8] [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[9]	・対策・緩和策	対象システム・資産
【攻撃局面 A4】  	[S4] SCADA による薬液注入量の悪意ある変更	・多要素認証の使用[D4]	・SCADA

9 [S]は表 2-3 の項番と対応。 [D]は表 2-5 の項番と対応。

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] Tampa Bay Times: Someone tried to poison Oldsmar's water supply during hack, sheriff says
https://www.tampabay.com/news/pinellas/2021/02/08/someone-tried-to-poison-oldsmars-water-supply-during-hack-sheriff-says/

[2] YouTube Pinellas Sheriff Channel: Treatment Plant Intrusion Press Conference
https://www.youtube.com/watch?v=MkXDSOgLQ6M

[3] Dragos: When Intrusions Don't Align: A New Water Watering Hole and Oldsmar
https://www.dragos.com/blog/industry-news/a-new-water-watering-hole/

[4] Pinellas County Sheriff's Office: 21-015 Detectives Investigate Computer Software Intrusion at Oldsmar's Water Treatment Plant
https://pcsoweb.com/21-015-detectives-investigate-computer-software-intrusion-at-oldsmar's-water-treatment-plant

[5] Commonwealth of Massachusetts: Cybersecurity Advisory for Public Water Suppliers
https://www.mass.gov/service-details/cybersecurity-advisory-for-public-water-suppliers

[6]IPA:制御システム関連のサイバーインシデント事例 4
https://www.ipa.go.jp/files/000080701.pdf

[7] ICS-CERT: Compromise of U.S. Water Treatment Facility
https://us-cert.cisa.gov/ncas/alerts/aa21-042a

[8] Water ISAC: 15 Cybersecurity Fundamentals for Water and Wastewater Utilities
https://www.waterisac.org/fundamentals

更 新 履 歴

2021 年 10 月 18 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 8

～2021 年 水道局への不正侵入と飲料水汚染未遂～

[発　　行]　2021 年 10 月 18 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　辻　宏郷
執筆者　福原　聡
協力者　桑名　利幸　木下　仁　高見　穣　小助川　重仁