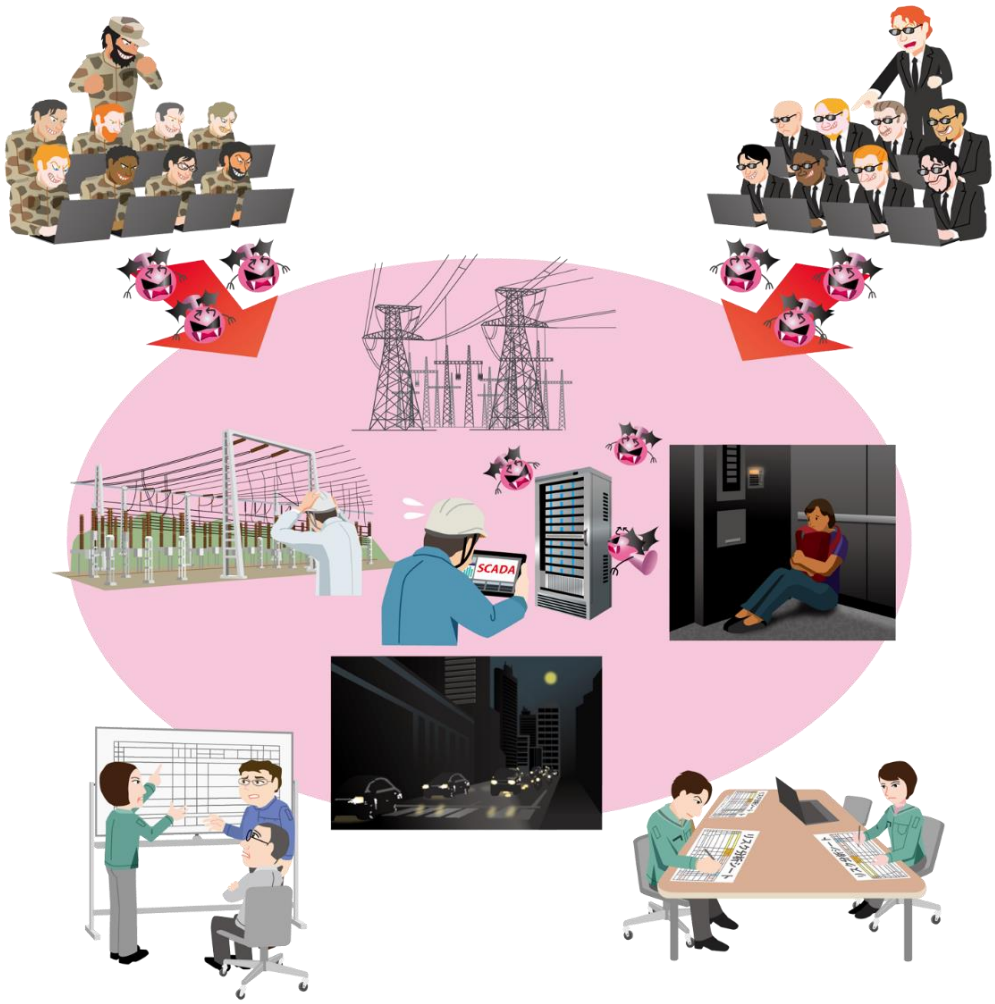
制御システムのセキュリティリスク分析ガイド補足資料

制御システム関連のサイバーインシデント事例 11

～2022 年　電力網への攻撃～



2024 年 3 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

2022 年 10 月 10 日ウクライナの電力会社の送電線網がサイバー攻撃を受け停電が発生した 。このサイバー攻撃はウクライナ全土の重要インフラを標的としたミサイル攻撃の開始[1]と同時に引き起こされていた[2]。

本書では、当局や、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. 2022 年 送電の停止

1.1. インシデント概要

2022 年 10 月 10 日ロシアのウクライナ侵攻が開始してから最も大規模な攻撃が始まった。ミサイル攻撃によりウクライナ国内の 8 地域の 11 の主要インフラが打撃を受け、国内の一部で電気、水道、暖房が使えなくなった。[1][3]。

図1-1 欧州におけるインシデント発生地域

その後の報道によると[2]、この攻撃と同時に電力施設へのサイバー攻撃が行われていたとの事だった。

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 や過去の「制御システム関連のサイバーインシデント事例1 2015 年 ウクライナ 大規模停電」「制御システム関連のサイバーインシデント事例2 2016 年 ウクライナ マルウェアによる停電」、Mandiant 社によるレポート[4]等をもとに作成した仮想システム構成図(図 1-2)を用いて説明する。

【コラム】Sandworm Team

本インシデントの調査を行った Mandiant 社の報告によると[4]、攻撃者は Sandworm と呼ばれるロシアに関連する脅威グループと言われる。

この Sandworm グループは MITRE ATT&CK[1]によると IPA が公開している『制御システム関連のサイバーインシデント事例1 2015 年 ウクライナ大規模停電』、『制御システム関連のサイバーインシデント事例 2 2016 年 ウクライナ マルウェアによる停電』で取り上げたサイバーインシデントの攻撃者とも考えられている。

[1] 米国政府機関等をサポートする非営利組織 MITRE Corporation が公開している、脆弱性の悪用に基づく攻撃を分析的に表現するナレッジベース。ATT&CK は Adversarial Tactics,Techniques, and Common Knowledge (敵対的な戦術、技術及び共通知識と訳される)の略。

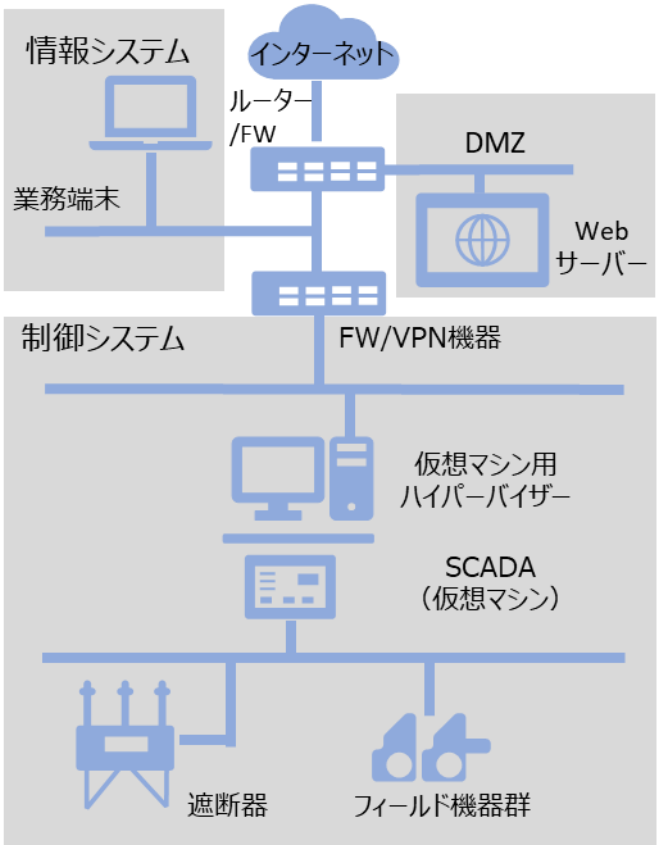


図 1-2 事例理解のための仮想システム構成図（実際のシステム構成とは異なる）

このシステム構成では SCADA[2]は仮想マシン用ハイパーバイザー[3]内に存在する仮想マシンにインストールされている。この SCADA から電源供給用の遮断器やフィールド機器群を制御するとしている。

【コラム】ハイブリッド戦争

『制御システム関連のサイバーインシデント事例 10』で取り上げた衛星通信サービスの停止は、ロシアのウクライナへの軍事侵攻の 1 時間前に発生した。このように多種多様な手段を使って、政治的な目的を達成するためにサイバー戦や情報戦、非正規戦などと正規戦を組み合わせた軍事戦略の手法をハイブリッド戦争と呼ぶ。今回の事例も、電力システム内への侵入は大規模な空爆が起こる数か月前に完了していたとの報告もある[4]。ミサイルやドローンなどによる爆撃と同時に電力システムへのサイバー攻撃が行われた本件もハイブリッド戦争の一つと考えられる。

2 Supervisory Control And Data Acquisition。制御システムで、設定や表示、制御監視など様々な役割を担う機器

3 仮想マシンを作成したり動作させるためのプラットホームを提供する、コンピュータ上で動作するソフトウェア

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

Mandiant 社によると、対象組織への侵入の経路はあきらかになっていない。しかしながら対象組織内での Sandworm の活動が最初に確認されたのは WEB サーバーだったとの事である。攻撃者は脆弱性等を利用して WEB サーバーへと悪意あるファイルを置く(図 1-3)。

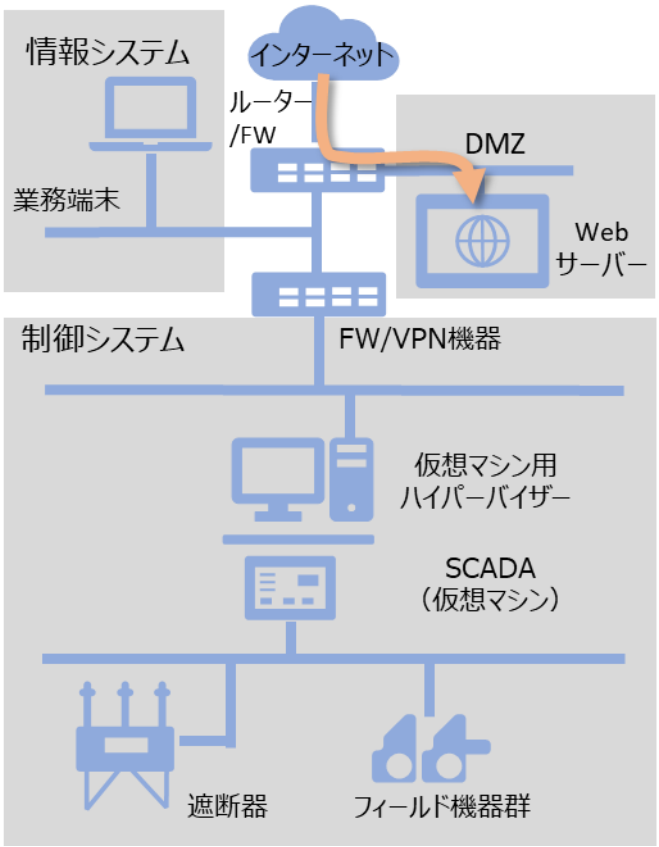


図 1-3 対象組織への侵入

1.2.2【攻撃局面 A2】ネットワーク内部の調査と横展開

攻撃者は対象組織の内部ネットワークへと侵入し、制御系を管理するの仮想マシンがインストールされているハイパーバイザーに侵入し特権を窃取する。(図 1-4)。

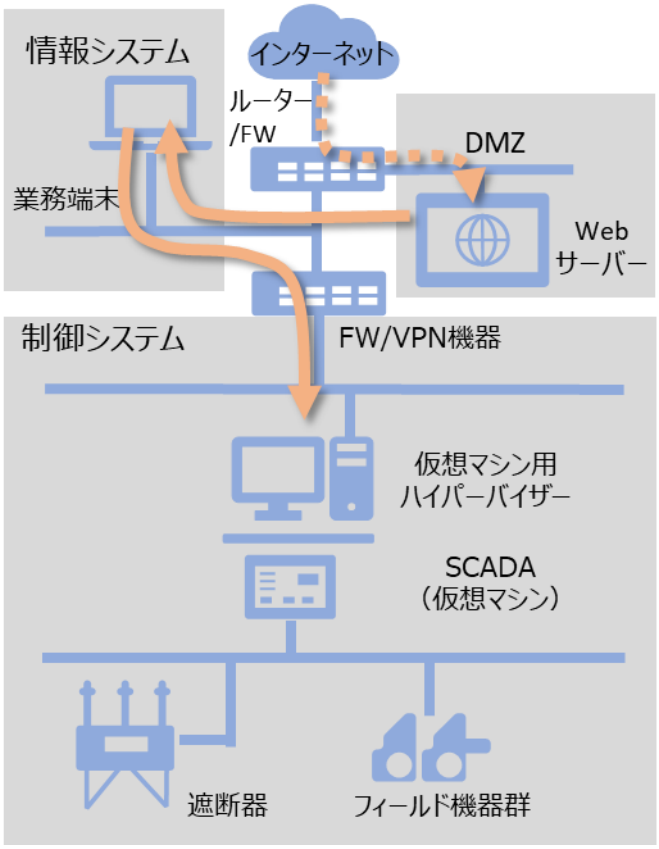


図 1-4 ネットワーク内部の調査と横展開

1.2.3【攻撃局面 A3】SCADA 仮想環境の構築

攻撃者は CDROM からソフトウェアをインストールするように、仮想イメージファイル(iso ファイル)を使ってハイパーバイザー上にあらたな SCADA 環境を構成した。(図 1-5)
ちなみに対象組織で侵害された SCADA ソフトウェアは既にサポートが終了している古いバージョンのものだった[5]。

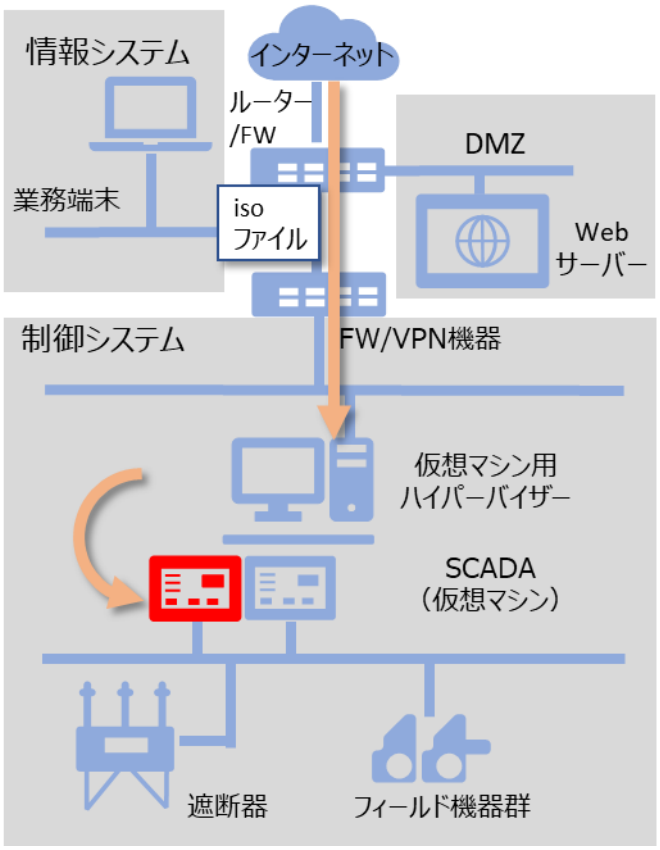


図 1-5 攻撃の足場確立

1.2.4【攻撃局面 A4】回路遮断命令の実行

攻撃者は、仮想マシンとして新たに構築された SCADA から、フィールドに設定されている回路遮断器に対し SCADA の持つコマンドを使って回路を遮断したと考えられる。
この命令により電力の供給がストップし、停電が発生した。(図 1-6)

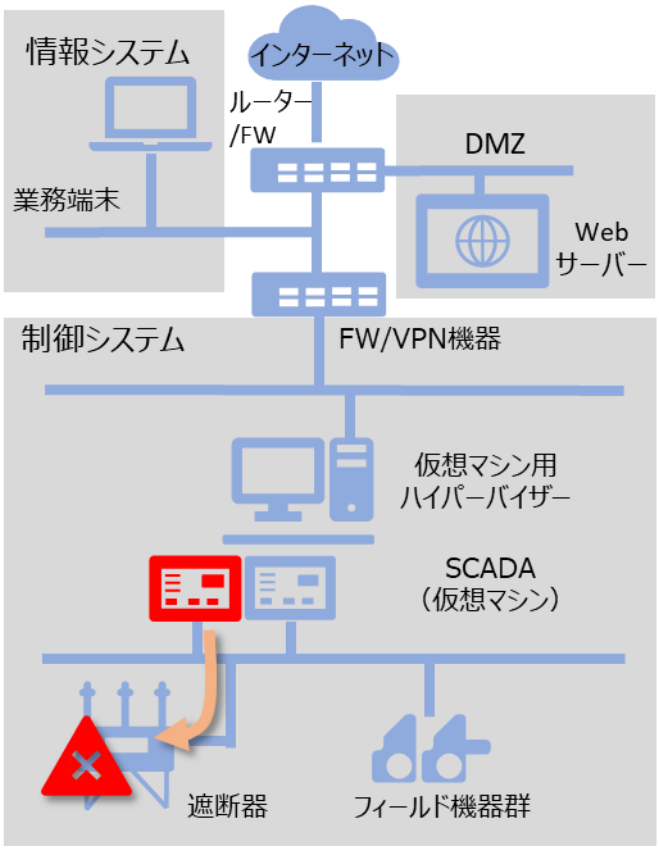


図 1-6 回路遮断命令の実行

1.2.5【攻撃局面 A5】コンピュータ内部情報の消去

攻撃者は、停電を引き起こした2日後、コンピュータ内部の証拠隠滅と復旧を困難にして混乱を長引かせるため、CADDYWIPER[4]と呼ばれる物理ディスクの内容すべてを消去するワイパーソフトウエアを使って、対象組織内のコンピュータを利用不可能にした。(図 1-7)

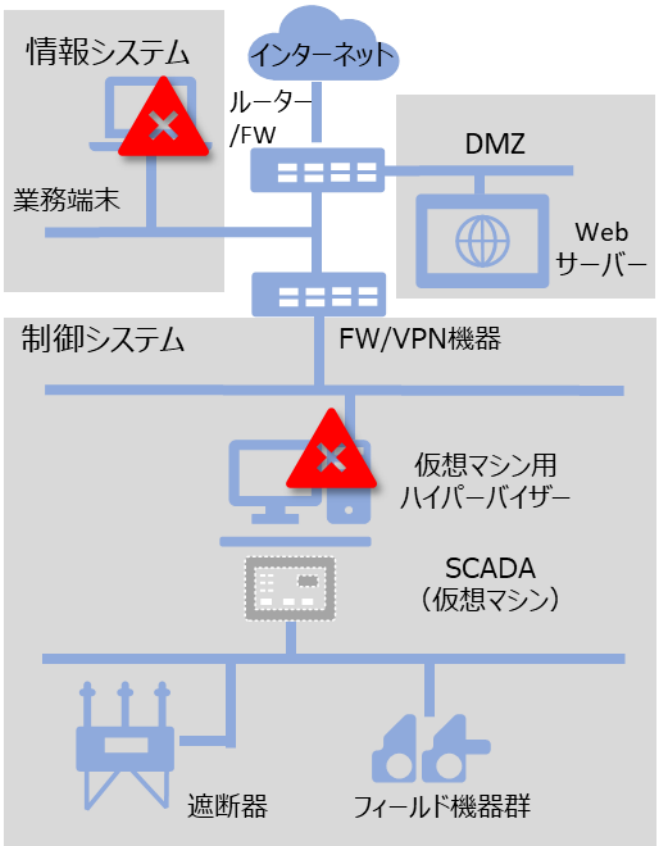


図 1-7 コンピュータ内部情報の消去

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、一般化した形で検討した事業被害の例を表 2-1 に示す。

事業被害 1 は、本インシデントにより発生した事業被害であり、事業被害を引き起す可能性のある攻撃シナリオもあわせて記載する。2.2 節では、この事業被害 1 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（攻撃拠点、攻撃対象は多数有）

項番	事業被害			
1	回路遮断による電力供給の停止			
	攻撃シナリオ	攻撃拠点	攻撃対象	最終攻撃
	Web サーバーの脆弱性の利用による侵入後、仮想環境に SCADA を構築し、回路遮断器へ不正なコマンドを発令し電力を遮断	SCADA	遮断器	不正なコマンドの発行

また、事業被害 1 に至る攻撃ルートの例を表 2-2 に示す。対象企業のシステム構成図、攻撃者、経由に相当する情報は明らかになっていないため、仮説としている。

表 2-2 攻撃ルートの例（斜線アンダーラインは仮説）

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
悪意のある外部の第三者	*Web サーバー*	*不明*	*SCADA*	*遮断器*	不正なコマンドの発行

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。分析対象の範囲等によっては、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 業務端末からの制御システムへの感染・攻撃実行の例

攻撃局面	項番	攻撃シナリオ 攻撃ツリー・ステップ ＜標的型メールによりマルウェアが組織内ネットワークに侵入。バックドアから内部の特権情報を取得され、製造関連コンピュータが暗号化され生産停止＞
【A1】	S1	侵入口=Web サーバー 脆弱性を利用して Web サーバー上に悪意あるファイルを設置する
【A2】	S2	業務端末が Web サーバーと通信した時に、悪意あるファイルをダウンロードする
【A2】	S3	攻撃者は、悪意あるファイルにより業務端末からの通信が確立した C&C サーバー[4]から業務端末経由で対象企業のネットワークやアカウント情報を調査する
【A2】	S4	収集した情報をもとに仮想環境の構築されているコンピュータのハイパーバイザーにアクセスし、特権を得る
【A3】	S5	ハイパーバイザーの特権を利用して新たな SCADA を保有する仮想マシンを構築する
【A4】	S6	構築した SCADA から遮断器に対して不正なコマンドを送出し、送電を停止させる
【A5】	S7	証拠隠滅と復旧の妨害のため、対象企業のネットワーク内のコンピュータ内部の情報を消去する

[4] Command & Control サーバー：攻撃者が、悪意あるプログラムに命令を送出したり盗みだしたりした情報を受け取るためにインターネット上に設置したサーバー

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、0 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	Web サーバー
	攻撃対象	遮断器
	攻撃拠点	SCADA（仮想環境に新設した仮想マシン）
	経由	ー
攻撃者		Sandworm
事業被害		回路遮断による電力供給の停止
攻撃シナリオ		Web サーバーの脆弱性の利用による侵入後、仮想環境に SCADA を構築し、回路遮断器へ不正なコマンドを発令し電力を遮断
最終攻撃（目的）		不正コマンド発行による遮断器の操作
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		Web サーバーの脆弱性の利用 C&C（Command & Control）サーバーとの通信確立 情報探索 特権の取得 仮想マシンのインストールと実行 コンピュータ内部情報の削除

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等の情報収集を行い、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、一般的な観点から、CISA[5]から公開された CISA,FBI[6],NSA[7]の共同サイバーセキュリティ アドバイザリーA22-011A、「Understanding and Mitigating Russian State Sponsored Cyber Threats to U.S. Critical Infrastructure」[6]、NCSC[8]が公開しているガイダンス「Actions to take when the cyber threat is heightened」[7]等を参考にして、リスク分析作業に活用するための安全計装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	システムのバックアップを作成し、リストアの確認を行う[7]
D2	ソフトウェアやファームウェアに最新のパッチを適用する[6][7]
D3	アンチウィルスを導入する[6][7]
D4	強力なパスワードを使い、多要素認証を正しく設定する[6][7]
D5	ネットワークのセグメント分割、ゾーンの整理とトラフィックの監視[6]
D6	ユーザアカウントの強化[7]

「D1. **システムのバックアップを作成し、リストアの確認を行う**」 バックアップが正しく実行されていることを確認し、バックアップからの復元のテストを行う。また、ネットワークから隔離されたバックアップを行い内容が最新のものである事を確認する。また、秘密鍵やアクセストークン、システムの状態もバックアップされている事を確認する。

「D2. **ソフトウェアやファームウェアに最新のパッチを適用する**」 利用するソフトウェアや利用するデバイスのファームウェアに最新のパッチが適用されていることを確認する。また、最新のパッチが適用できない場合には代替の緩和策を講じる。

「D3. **アンチウィルスを導入する**」 アンチウィルスを導入し、プログラム及びパターンファイル情報が最新であることを確認する。

「D4 **強力なパスワードを使い、多要素認証を正しく設定する**」 簡単にわからない十分に強力かつ一意なパスワードを利用する。さらに、多要素認証を採用し、正しく構成されている事を確認する。

---

5 Cybersecurity and Infrastructure Security Agency：サイバーセキュリティ・インフラセキュリティ庁
6 Federal Bureau of Investigation：連邦捜査局
7 National Security Agency：アメリカ国家安全保障局
8 National Cyber Security Centre：英 国家サイバーセキュリティセンター

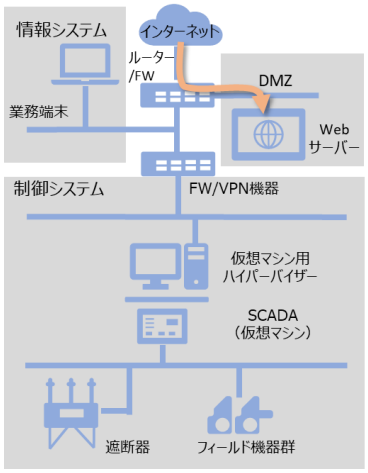
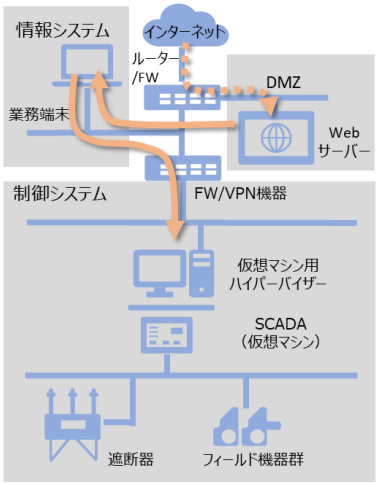
「D5 **ネットワークのセグメント分割、ゾーンの整理とトラフィックの監視**」 情報ネットワークと制御ネットワークを分離し、情報ネットワークが侵害されても制御ネットワークを侵害できないように制限する。制御ネットワークを分割しネットワークのトラフィックを監視制御する。

「D6 **ユーザアカウントの強化**」 ユーザアカウントを確認し、古いアカウントや使用されていないアカウントを削除する。

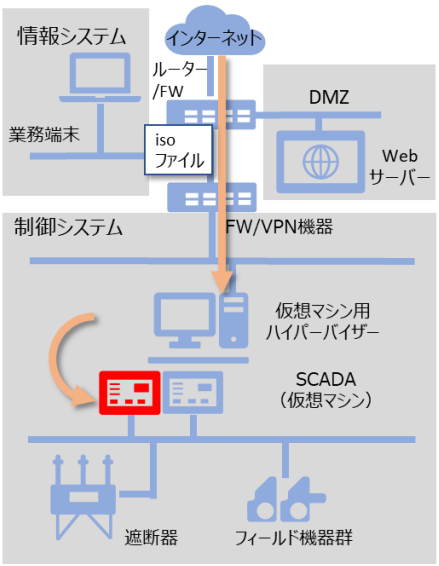
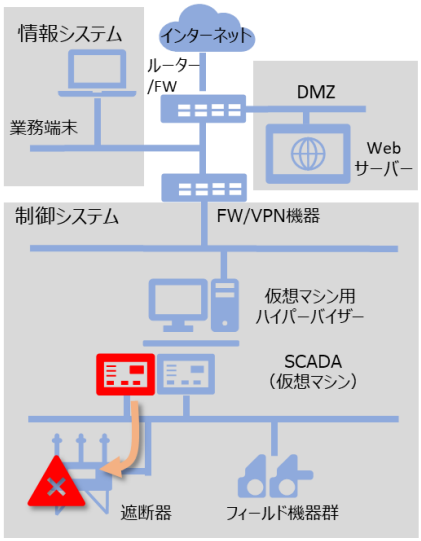
2.5. 攻撃ステップと対策・緩和策の関連付け

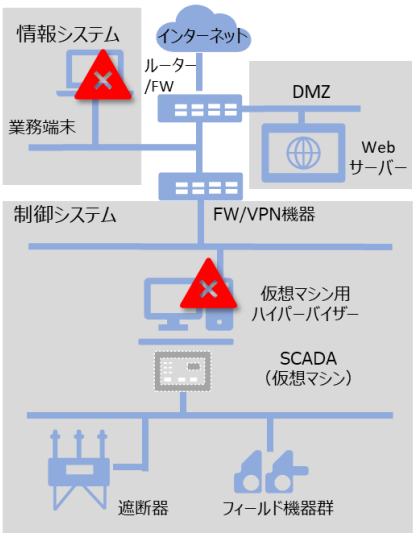
2.4 節までの情報をもとに、各攻撃ステップにおける代表的な対策・緩和策を紐づけた例が表 2-6 となる。セキュリティ対策の基本である「多層防御」を考慮し、緩和策を立案することがポイントとなる。

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[9]	対策・緩和策[9]	対象システム・資産
【攻撃局面 A1】  	[S1] 悪意あるファイルの設置	•パッチ適用【D2】 •アンチウィルス【D3】 •強力なパスワード【D4】 •ユーザアカウントの強化【D6】	•Web サーバー
【攻撃局面 A2】  	[S2] 悪意あるファイルのダウンロード 【S3】 攻撃者による内部調査 【S4】 ハイパーバイザーの奪取	・パッチ適用【D2】 ・アンチウィルス【D3】 ・強力なパスワード【D4】 ・ネットワークのセグメント分割と監視【D5】 ・ユーザアカウントの強化【D6】	•情報システム •制御システム •仮想マシン用ハイパーバイザー

[9] [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（つづき）	攻撃 ステップ	対策・緩和策	対象 システム・資産
【攻撃局面 A3】  	【S5】 SCADA 仮想環境の構築	・パッチ適用【D2】 ・強力なパスワード【D4】 ・ユーザアカウントの強化【D6】	•仮想マシン用ハイパーバイザー
【攻撃局面 A4】  	【S6】 不正コマンドの送出	・強力なパスワード【D4】 •ユーザアカウントの強化【D6】	•SCADA •遮断器

攻撃局面（つづき）	攻撃 ステップ	対策・緩和策	対象 システム・資産
【攻撃局面 A5】  	[S7] コンピュータ内部情報の消去	•バックアップとリストア【D1】 •パッチ適用【D2】 •アンチウィルスの導入【D3】	•情報システム •仮想マシン用ハイパーバイザー

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] REUTER； Blackouts after Russian strikes deepen Ukraine's concerns before winter
https://www.reuters.com/world/europe/blackouts-after-russian-strikes-deepen-ukraines-concerns-before-winter-2022-10-10/

[2] REUTER； Russian spies behind cyber attack on Ukraine power grid in 2022 - researchers
https://www.reuters.com/technology/cybersecurity/russian-spies-behind-cyberattack-ukrainian-power-grid-2022-researchers-2023-11-09/

[3] REUTER；Russia launches biggest air strikes since start of Ukraine war
https://www.reuters.com/world/europe/russias-ria-state-agency-reports-fuel-tank-fire-kerch-bridge-crimea-2022-10-08/

[4] Mandiant；Sandworm が OT(運用技術)に対する新たな攻撃を使用してウクライナの電力供給を妨害
https://www.mandiant.jp/resources/blog/sandworm-disrupts-power-ukraine-operational-technology?mkt_tok=NTY1LVBFSS05NTIAAAGPwgYi577Rv4arg4S4sGAv93fmjLm6qL_8l5aaJse-hcA3RMIfjX8eaCqwzenyaQ1ZjRVummAmCGIRqGo3w8CESYzIqhLdxE0IEfqR3JrhPTA

[5] MITRE ATT&CK； Sandworm Team
https://attack.mitre.org/groups/G0034/

[6] CISA；Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure
https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-011a

[7] NCSC；Actions to take when the cyber threat is heightened
https://www.ncsc.gov.uk/guidance/actions-to-take-when-the-cyber-threat-is-heightened

更 新 履 歴

2024 年 3 月 4 日	初版	ー
2024 年 4 月 18 日	2 版	裏表紙の記述を修正

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 11

～2022 年　電力網への攻撃～

[発　　行]　2024 年 4 月 18 日　第 2 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　木下　弦　小助川　重仁　木下　仁　高見　穣