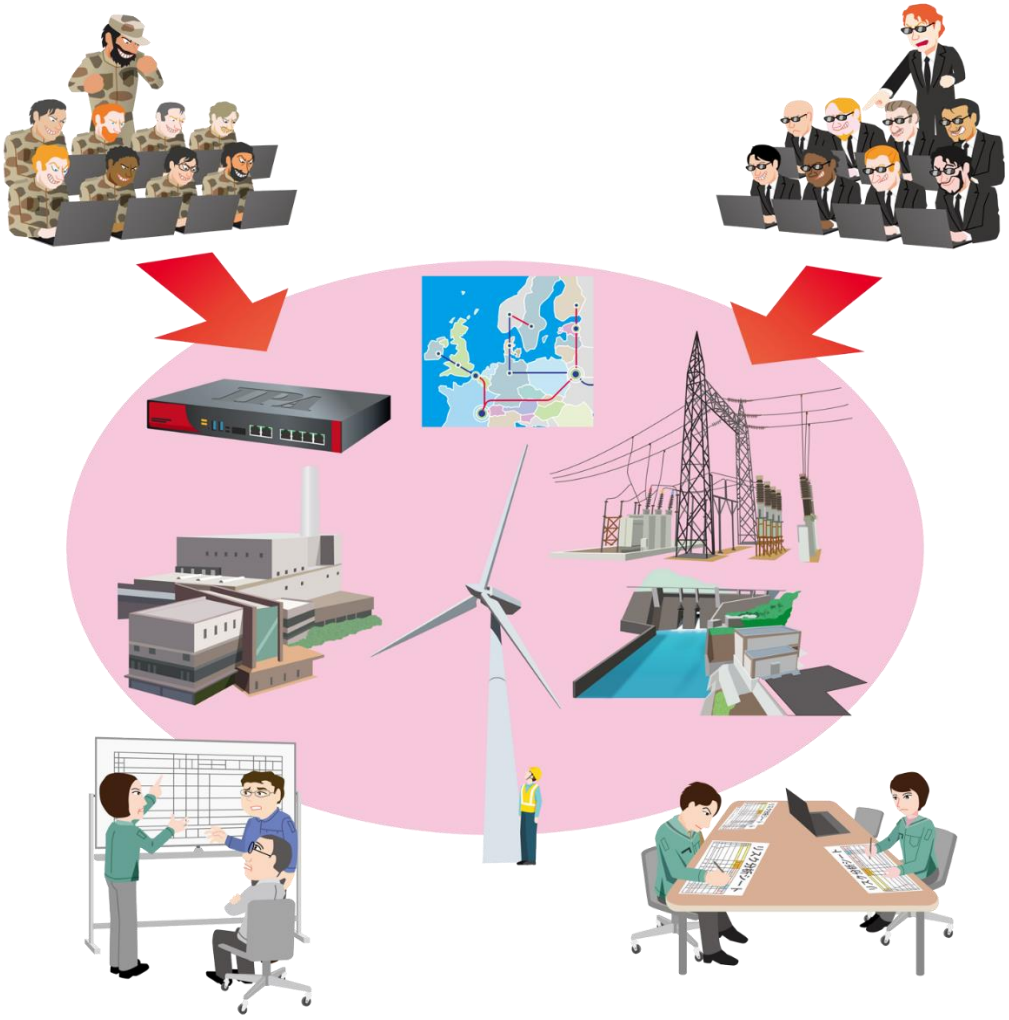
制御システムのセキュリティリスク分析ガイド補足資料

制御システム関連のサイバーインシデント事例 12

～2023 年 デンマークの複数のエネルギー関連企業へのサイバー攻撃～



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できる。

本資料の位置付け

2023 年 5 月、デンマークのエネルギー関連企業 22 社（社名非公開）が大規模なサイバー攻撃にさらされ、いくつかの企業では、制御システムにアクセスされ、いくつかの企業では操業をアイランドモード（発電所をネットワークから切り離し、スタンドアロンで動作させる）とすることを余儀なくされた。

本資料では、デンマークの非営利団体 SektorCERT[1]による詳細な報告をもとに、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。[1]

後半では、当該インシデントに関係する情報を整理し、電力システムを想定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。

【参考資料】の詳細は、リンク先の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]）、巻末の参考資料は角括弧付き番号（例[1]）で表している。

対象読者

制御システムのリスクアセスメント担当者

---

[1] https://sektorcert.dk/　デンマークの重要インフラに対する脅威を把握するためのセンサーネットワークを運営している非営利団体。重要インフラ分野の企業が所有・資金提供している。

1. デンマーク史上最大のサイバー攻撃

1.1. インシデント概要

2023 年 5 月、デンマークのエネルギー関連企業 22 社がほぼ同時に大規模なサイバー攻撃を受けた。この攻撃により、いくつかの企業は制御システムにアクセスされ、いくつかの企業は回線を切断した稼働を余儀なくされ、一部の企業はファイアウォールがダウンし通信不能となったが、電力供給自体に問題は生じなかった。

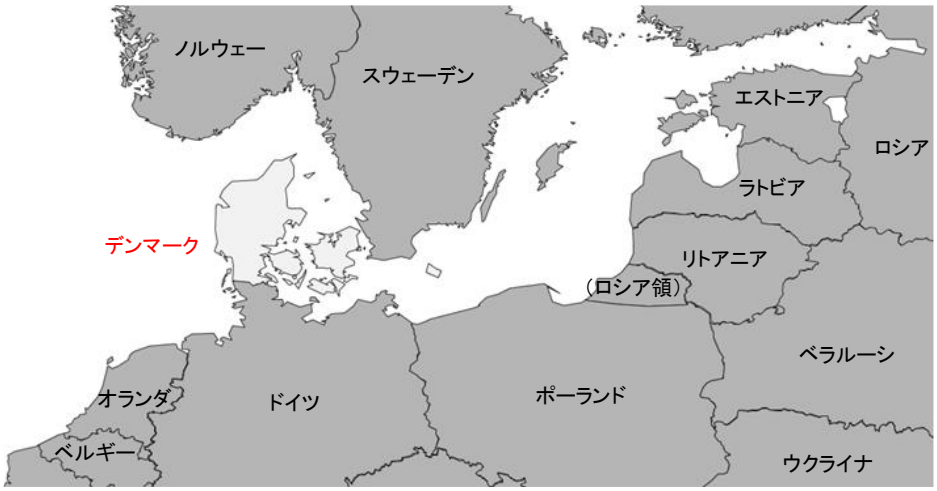


図 1-1 欧州におけるインシデント発生地域

この攻撃は、被害企業が使っていた Zyxel 社のファイアウォールの脆弱性（ゼロデイ脆弱性を含む）を狙った攻撃であったが、複数と考えられる攻撃者による侵入、DDoS 攻撃の踏み台化、ファイアウォールのシャットダウンなど、数日間にわたるインシデントであったと報告されている。
今回は、SektorCERT の分析結果を中心に、過去のサイバーインシデントの事例を参考に補完・考察しながら、被害拡大の状況を IEC 62443 や NIST SP 800-82 Rev.3 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。

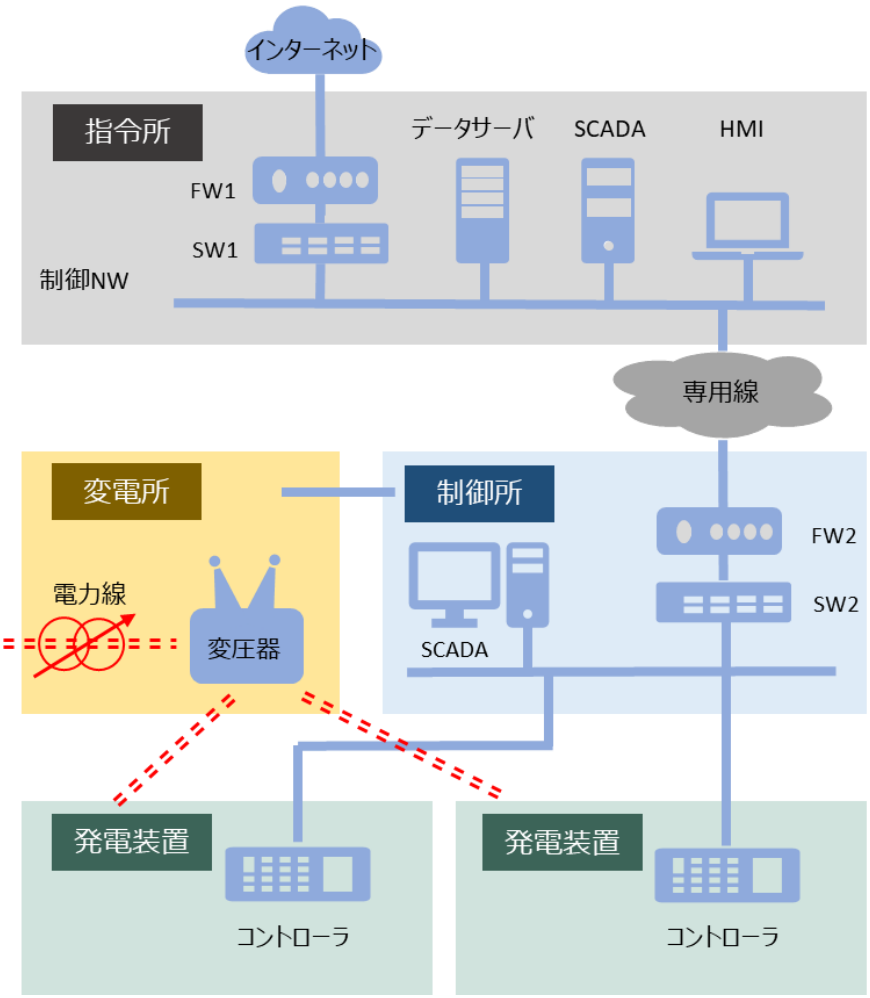


図 1-2 事例理解のための仮想システム構成図（実際のシステム構成とは異なる）

1.2. 被害発生に至る攻撃の流れ

1.2 節では、参考資料で公開されている内容から、サイバー攻撃から被害発生に至るまでの流れを次の局面に分けて解説する。背景としてデンマークの電力網は EU の他国と接続されており電力を輸出入することで需給バランスを取っている[2]。デンマーク国内における風力発電が急成長しており、2022 年にはデンマーク国内の総電力使用量の半分以上を風力で賄っている [3] 。

1.2.1. 第 1 波の攻撃局面-偵察【攻撃局面 A-1】

ここで紹介するサイバー攻撃は大きく 2 回に分けられ、1 回目はファイアウォールの既知の脆弱性を狙った攻撃、2 回目はゼロデイ脆弱性を利用した攻撃であった。

最初の攻撃では、2023 年 4 月に NVD[2]に登録された CVE-2023-28771 Zyxel ZyWALL ファームウェアの脆弱性[4]が利用されている。この脆弱性は、デバイスのユーザー名やパスワードを知らなくても、認証なしに管理者権限でコマンドを実行できるというものだった。この脆弱性の深刻度（深刻度については次ページコラム参照）は CVSS v3（共通脆弱性評価システム: Common Vulnerability Scoring System ver.3）の評価基準で 9.8 の「緊急」とされる、きわめて深刻な脆弱性と公表された。

Zyxel 社は台湾のネットワーク機器製造会社で、Zyxel 社のファイアウォール ZyWALL はデンマークでは中小規模の重要インフラにおいて広く利用されている。

攻撃者はまずターゲット企業に対し、この脆弱性が利用できるかを調査したと考えられる。

当時、この Zyxel のファイアウォールは VPN 利用時を想定して、インターネット側にデフォルトでポート（UDP 500）を開いている仕様であった。これは実際に VPN を使わない場合でも開いた状態だったため、このポートを調べることで、攻撃者はターゲット企業を容易に絞ることが出来たと考えられる。

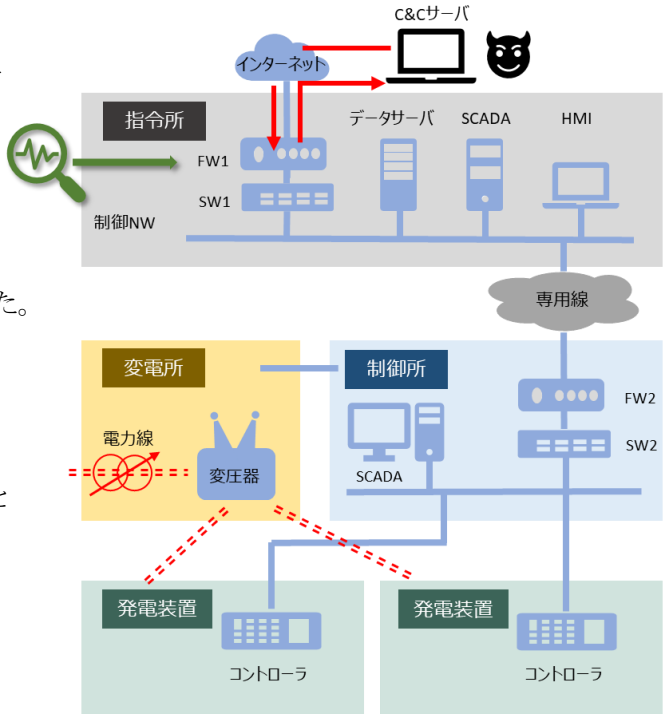


図 1-3 第 1 波の攻撃局面-偵察

1.2.2. 第 1 波の攻撃局面-情報窃取【攻撃局面 A-2】

2023 年 5 月 11 日、攻撃者はこの脆弱性が利用可能かを確かめるために、ターゲットとしたデンマークのエネルギー関連企業 16 社のファイアウォールに対し、悪意あるパケット（通信信号）を送信し、11 社のファイアウォールが侵害を受け、攻撃者は、管理者コマンドにより、ファイアウォールの現在のユーザー名と設定情報を取得した。

SektorCERT はこの活動に気付き、即座にインシデントレスポンスチームを結成し、攻撃を受けたファイアウォールのファームウェアアップデートが未適用の企業に連絡を行い、ファームウェアのアップデートを行わせた。

[2] National Vulnerability Database

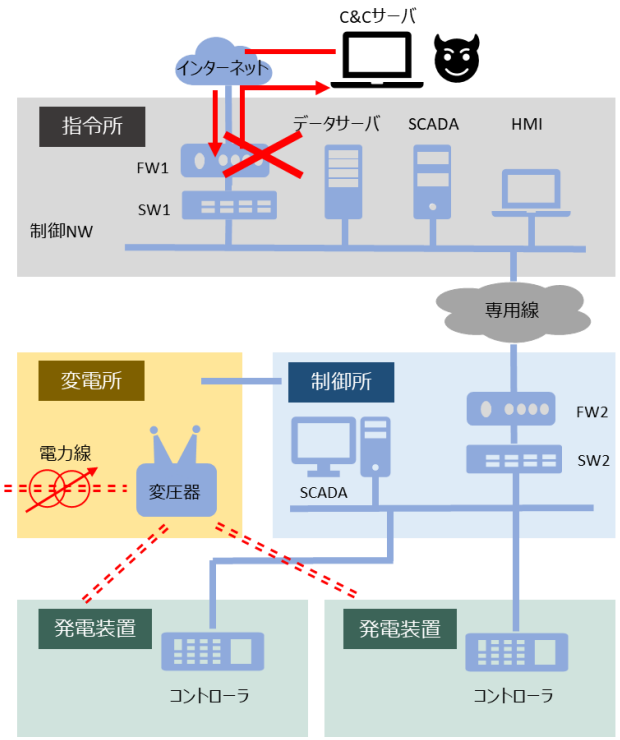


図 1-4 第 1 波の攻撃局面-情報窃取

【コラム】

共通脆弱性評価システム CVSS とは[5]

共通脆弱性評価システム CVSS は、情報システムの脆弱性に対するオープンで包括的、汎用的な評価手法の確立と普及のため、米国家インフラストラクチャ諮問委員会（NIAC: National Infrastructure Advisory Council）のプロジェクトで 2004 年に原案が作成され、その後更新が続いています。

CVSS は、情報システムの脆弱性に対するオープンで汎用的な評価手法であり、ベンダーに依存しない共通の評価方法を提供しています。CVSS を用いると、脆弱性の深刻度を同一の基準の下で定量的に比較できるようになります。

CVSS は以下の 3 つの基準で脆弱性を評価します。

(1)基本評価基準(Base Metrics)

(2)現状評価基準(Temporal Metrics)

(3)環境評価基準(Environmental Metrics)

この数値は 0～10 までの数値として算定され、CVSS v3 では以下のようなレベル分けを使い、わかりやすい表現としています。

深刻度	スコア
緊急	9.0～10.0
重要	7.0～8.9
警告	4.0～6.9
注意	0.1～3.9
なし	0

1.2.3. 第 2 波の攻撃局面【攻撃局面 B】

最初の攻撃から 11 日後の 5 月 22 日に発生した第 2 波のサイバー攻撃も、ファイアウォールのファームウェアの脆弱性を狙ったものだった。攻撃者は SektorCERT の加入企業のファイアウォールに対し、ゼロデイ脆弱性を悪用して任意のシェルコマンドを実行させた。

SektorCERT は監視していたトラフィックから、このファイアウォールが新しいソフトウェアをダウンロードし、Mirai ボットネット[3]の一部として動作し始め、米国と香港の企業への DDoS 攻撃に参加していることも分かり、明らかな第 2 波のサイバー攻撃が行われていることを把握した。

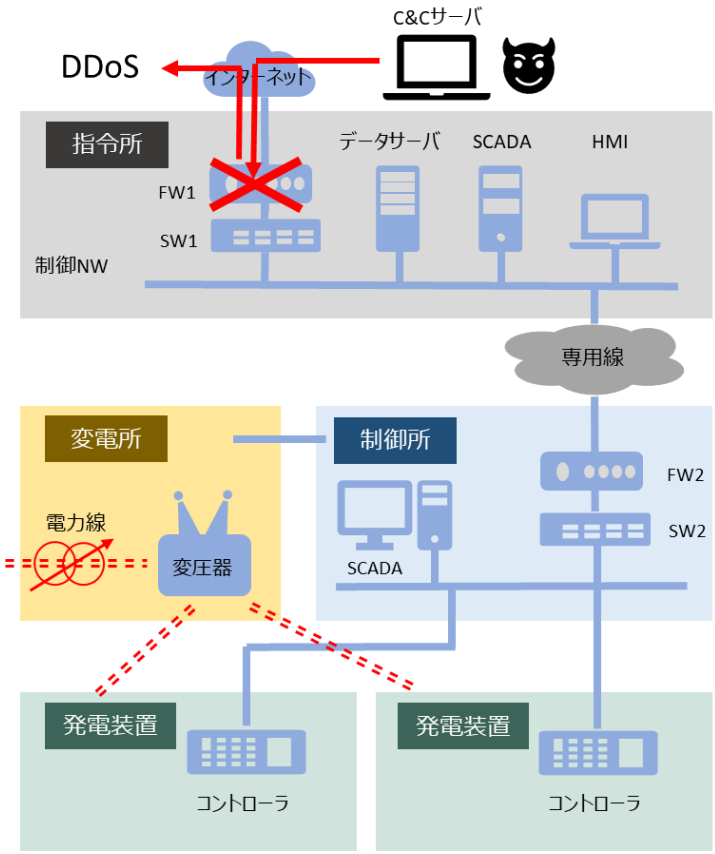


図 1-5 第 2 波の攻撃局面

[3] Mirai は IoT を狙うマルウェアで、感染すると自動的に特定のターゲットを標的とする DDoS 攻撃などの装置となる。また、それらの感染した機器群をボットネットと呼ぶ。

1.2.4. ゼロデイ脆弱性への対応【攻撃局面 B】

この時点でファイアウォールは既にファームウエアが更新されていたにも関わらず問題が発生していた点から、SektorCERT はこの挙動の原因が未知の脆弱性（ゼロデイ脆弱性）であると考え、被害企業のファイアウォールを交換するよう提案した。事業者は交換するためにファイアウォールを停止し、制御ネットワークは他のネットワークと切り離したアイランド（孤島）モードでの稼働とせざるを得なくなった。そのため、一部の企業では指令所から発電状況のモニタリングやオンラインのメンテナンスができなくなり、直接現地へ向かう必要があった。

2 日後、Zyxel 社から 2 つの新たな脆弱性、CVE-2023-33009[6]と CVE-2023-33010[7]が発表された。これら 2 つの脆弱性は最初の攻撃後にアップデートされたファームウェアにも存在し、その深刻度は「緊急」であった。

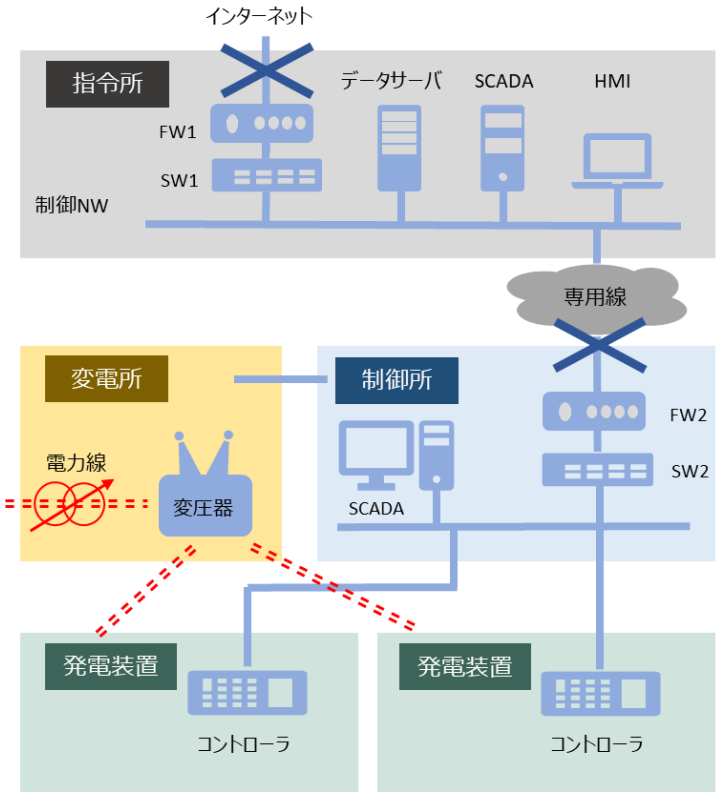


図 1-6 ゼロデイ脆弱性への対応

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。本章以降、事業被害 1 と 2 は、本インシデントにより発生した事業被害であり、事業被害を引き起こ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 2 つ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

<table>
<tr><th>項番</th><th colspan="4">事業被害</th></tr>
<tr><td rowspan="3">1</td><td colspan="4">ファイアウォールの機能が無効化され、メンテナンスやサービスに障害が発生する</td></tr>
<tr><td>攻撃シナリオ</td><td>攻撃拠点</td><td>攻撃対象</td><td>最終攻撃</td></tr>
<tr><td>ファイアウォールの管理者権限が奪取され、機密情報が窃取される</td><td>ファイアウォール</td><td>ファイアウォール</td><td>ユーザ情報、設定情報の窃取</td></tr>
<tr><td rowspan="3">2</td><td colspan="4">ファイアウォールから悪意あるコマンドが発行され、外部サイトへの DDoS 攻撃に加担する</td></tr>
<tr><td>攻撃シナリオ</td><td>攻撃拠点</td><td>攻撃対象</td><td>最終攻撃</td></tr>
<tr><td>ファイアウォールの管理者権限が奪取され、悪意あるコマンドが発行されてしまう。</td><td>ファイアウォール</td><td>ファイアウォール</td><td>DDoS 攻撃の実行</td></tr>
</table>

また、事業被害に至る攻撃ルートの例を以下に示す。本件では、ファイアウォールの管理者権限が窃取されたものの、事業者ネットワーク内部への侵入に関する記述はない。

表 2-2 攻撃ルートの例（下線はリスク分析をする上での想定）

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	*悪意のある外部の第三者*	*インターネットに接続されたネットワーク*	*-（ファイアウォール内部）*	ファイアウォール	ファイアウォール	ユーザ情報、設定情報の窃取
2	*悪意のある外部の第三者*	*インターネットに接続されたネットワーク*	*ファイアウォール～インターネット*	ファイアウォール	組織外のシステム	DDoS 攻撃の実行

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当てはめ整理した内容が表 2-3、表 2-4 である。分析対象の範囲などによっては切り出し方のパターンが考えられるが、一例として参照いただきたい。

表 2-3 事業被害 1 脆弱性による情報漏えいの例

攻撃局面	項番	攻撃シナリオ 攻撃ツリー・ステップ ＜ファイアウォールの管理者権限が奪取され、機密情報が窃取される＞
【A-1】	S1-1	侵入口＝インターネットに接続された Zyxel のファイアウォールを探る
【A-2】	S1-2	ファイアウォールは脆弱性を利用され、現在のユーザー名と設定情報を攻撃者へと伝える

表 2-4 事業被害 2 ゼロデイ脆弱性による DDoS 攻撃の例

攻撃局面	項番	攻撃シナリオ	
			攻撃ツリー・ステップ
		＜ファイアウォールの管理者権限が奪取され、悪意あるコマンドが発行され、他組織のシステムへ DDoS 攻撃を行う＞	
【B-1】	S2-1		侵入口＝インターネットに接続されたファイアウォールに悪意あるコマンドが送られる。
【B-1】	S2-2		ファイアウォールに DDoS 攻撃用のプログラムがダウンロードされ、実行させられる。

2.3. 事業被害ベースのリスク分析における分析要素のまとめ

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ごとにまとめた結果が表 2-5 となる。

表 2-5 各種公開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	ファイアウォール（事業被害 1）、他システム（事業被害 2）
	攻撃拠点	ファイアウォール
	経由	ファイアウォール（事業被害 2）
攻撃者		悪意のある外部の攻撃者
事業被害		機密情報の漏えい（事業被害 1）、他システムへの攻撃（事業被害 2）
攻撃シナリオ		ファイアウォールの管理者権限が奪取され、機密情報が窃取される（事業被害 1） ファイアウォールの管理者権限が奪取され、悪意あるコマンドが発行され、他組織のシステムへ DDoS 攻撃を行う（事業被害 2）
最終攻撃（目的）		ファイアウォール（事業被害 1） 他組織のシステム（事業被害 2）
攻撃ルート		表 2-2 を参照
攻撃ツリー		表 2-3、表 2-4 を参照
攻撃手法		情報探索 不正アクセス プロセス不正実行 情報窃取

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、事例ごとに表 2-5 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デンマーク SektorCERT から公表されている「The attack against Danish, critical infrastructure[1]」に記載されている一般的な 25 の推奨セキュリティ緩和策を例に、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 2-6 は、代表的な対策・緩和策をまとめたものとなる。

表 2-6 代表的な対策・緩和策の例

項番	対策・緩和策
D1	不要なサービスをネットワークに露出させない
D2	ファームウェアアップデートの適用
D3	侵入検知のためのログ管理
D4	ネットワーク分離

「D1. 不要なサービスをネットワークに露出させない」

インターネット側で利用できるサービスは VPN を含み最小限に制限する。

「D2. ファームウエアアップデートの適用」

脆弱性に関する情報を常にウォッチし、必要な場合に速やかにアップデートを行うことができる環境を構築する。

「D3. 侵入検知のためのログ管理」

不正侵入のために攻撃者が行うであろう、本来は発生しないはずのマシン間の通信や、攻撃を有利に展開するための権限昇格などを検知するための、設定や構成およびログの監視・分析による対策である。今回のように攻撃の初期段階で検知できれば、深刻化する前にインシデント対応を行うことが期待できる。

「D4. ネットワーク分離」

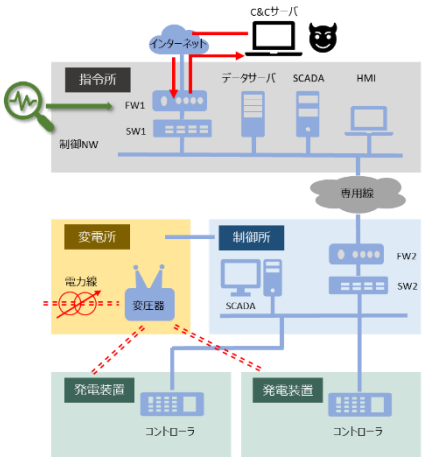
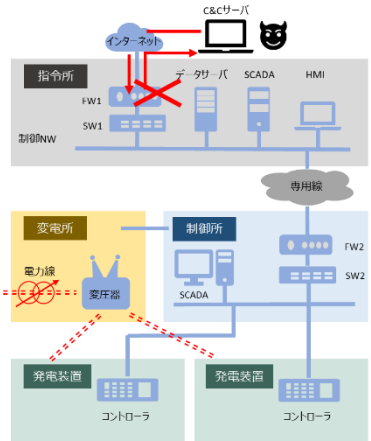
ゼロデイ脆弱性により、完全にシステムを保護する事ができないケースはあり得る。その場合、組織内部のネットワークセグメントを分割しておく事で、被害の拡大を困難にし、最小限に抑える。

インシデント事例のサイバー攻撃要素の整理と同様に、対策・緩和策なども表 2-6 のように抜き出し、収集・整理することを心掛けていただきたい。

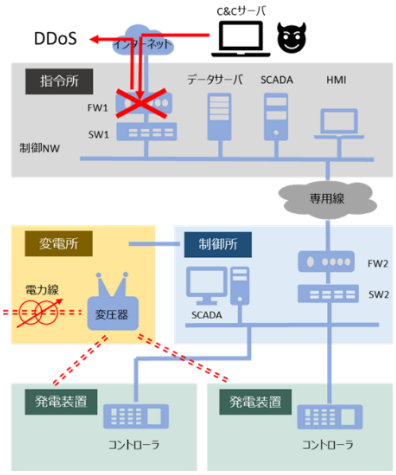
2.5. 攻撃ステップと対策・緩和策の関連付け

2.4 節までの情報をもとに、代表的な対策・緩和策を関連付けた例が表 2-7 となる。

表 2-7 制御システムにおける攻撃ステップと対策・緩和策の関連付け例

攻撃局面	攻撃ステップ[4]	対策・緩和策	対象システム・資産
攻撃局面【A-1】 	侵入口＝インターネットに接続された Zyxel のファイアウォールを探索する [S1-1]	•不要なサービスをネットワークに露出させない [D1] •侵入検知のためのログ管理[D3]	•FW
攻撃局面【A-2】 	脆弱性を利用し、現在のユーザ名と設定情報を窃取する[S1-2]	•ファームウエアアップデートの適用[D2]	•FW

[4] [S]は表 2-3 の項番と対応。 [D]は表 2-6 の項番と対応。

攻撃局面（表 2-7 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【B1】  	侵入口＝インターネットに接続されたファイアウォールに悪意あるコマンドが送られ、DDoS 攻撃用のプログラムがダウンロードされ、実行される。 [S2-1]	•侵入検知のためのログ管理[D3] •ネットワーク分離[D4] (内部にある FW の場合)	•FW

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ともに、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 1 つのアプローチを紹介した。

今回の事例は、インターネットとの境界に位置する機器の問題を扱ったものであり、攻撃ツリーを前提とした事業被害ベースのリスク分析の観点から見ると、自社の事業被害に直結するシナリオとしては捉えにくい側面がある。

しかしながら、ゼロデイ脆弱性の問題、そのゼロデイ攻撃が重要インフラで実際に発生していたという事実、自社システムに直接の影響はなくても、気付かないまま DDoS に加担してしまう可能性、さらに SectorCERT による早期警戒通知が被害拡大の抑制に寄与した点など、学ぶべき内容が多いことから、本事例を取り上げた。

本事例は、事業被害ベースのリスク分析における主要な被害シナリオの例として捉えるよりも、攻撃シナリオ検討時の視野を広げるための参考事例として位置付けるのが適切である。

事業被害ベースのリスク分析では、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にし、そこに至る攻撃シナリオや攻撃ルートを具体化していくことが基本となる。その際には、制御システム本体への直接的な攻撃だけでなく、インターネット境界の機器や周辺システムの侵害によって生じる間接的な影響についても考慮する必要がある。

本事例は、そうした想定漏れを防ぎ、脅威認識を補強するうえで有用な示唆を与えるものである。

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] SektorCERT: The attack against Danish, critical infrastructure
https://sektorcert.dk/wp-content/uploads/2023/11/SektorCERT-The-attack-against-Danish-critical-infrastructure-TLP-CLEAR.pdf

[2] Energinet: SECURITY OF ELECTRICITY SUPPLY IN DENMARK
https://en.energinet.dk/

[3] Danish Energy Agency (2021): Development and Role of Flexibility in the Danish Power System.
https://stateofgreen.com/jp/wp-content/uploads/2021/11/DEA レポート日本語版.pdf

[4] NVD:CVE-2023-28771 Detail
https://nvd.nist.gov/vuln/detail/cve-2023-28771

[5] IPA:CVSS とは
https://www.ipa.go.jp/security/vuln/scap/cvssv3.html

[6] NVD: CVE-2023-33009 Detail
https://nvd.nist.gov/vuln/detail/cve-2023-33009

[7] NVD: CVE-2023-33010 Detail
https://nvd.nist.gov/vuln/detail/cve-2023-33010

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 12

～デンマークの複数のエネルギー関連企業へのサイバー攻撃～

[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