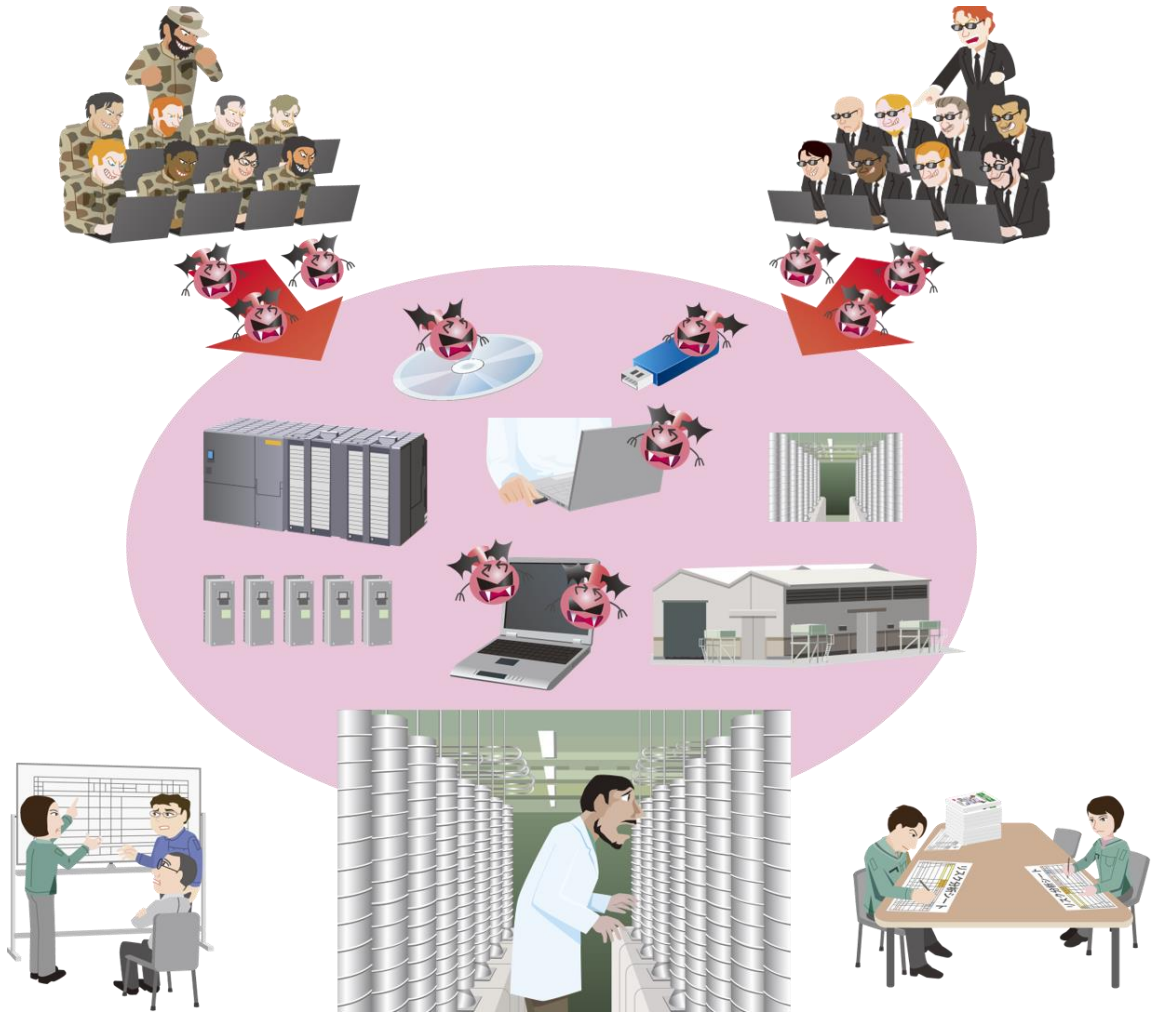
制御システムのセキュリティリスク分析ガイド補足資料

制御システム関連のサイバーインシデント事例4

～Stuxnet：制御システムを標的とする初めてのマルウェア～



2020 年 3 月

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。

本資料の位置付け

2019 年 9 月に長らく謎だった、世界初の制御システムを標的としたマルウェア、Stuxnet の感染経路が公表された。これを機に、当インシデントについて改めて振り返ってみたい。本稿の前半では、2010 年 6 月に発見された核燃料施設を標的とするマルウェアとイランのプラントで発生した操業停止（濃縮工程における遠心分離器の破壊）事象に関する米国 ICS-CERT などの公開情報（巻末【参考資料】）をもとに、2019 年に公表された感染経路に関する報告等を加え、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、Stuxnet 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。

【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]）、巻末の参考資料はカッコ付き番号（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. Stuxnet:制御システムを標的とする初めてのマルウェア

1.1. インシデント概要

2010 年 9 月に、イランのナタンズに所在する核燃料施設のウラン濃縮用遠心分離機を標的として、サイバー攻撃があったことが公表され、世界初の制御システムを標的とするサイバー兵器とも言われた。

図 1-1 イランにおけるインシデント発生地域

Stuxnet と呼ばれるマルウェアが核燃料施設に持ち込まれ、マルウェアに感染させられたコンピュータによって、遠心分離機を制御する PLC の設定ロジックが改ざんされ、周波数変換器[1]が攻撃されたことにより、約 8,400 台の遠心分離機のうち約 1,000 台[2]が稼働不能に陥り、操業が一時停止する事態となった[1]。

Stuxnet は独 SIEMENS 社製 PCS7(プロセス制御システム[3])において、PCS7 を構成する S7(PLC[4])/WinCC(SCADA[5])/STEP7(EWS[6])をターゲットとしているマルウェアであった。

(WinCC/STEP7 はどちらも S7 に対するインターフェース・ソフトウェアであり、Microsoft Windows 上で動作する。本文では以降便宜上、S7 を PLC、WinCC を SCADA、STEP7 を EWS と称することとする。)

一般的に認識されるワームウイルスのようにマルウェア自らが拡散感染するが、感染を秘匿する、ネットワーク的に隔離された制御システムを狙って拡散する、制御ロジックを改ざんして制御システムの監視画面をダミー表示にすり替えたり警報アラームを密かに停止したりする、といったような特徴的な機能を保有していた。

---

1 注:出力周波数を変換することで、モーターの速度を制御できる装置

2 注:数に関して四半期毎の IAEA(国際原子力機関) SafeGuard Report が情報源となっているが、元々の遠心分離機の初期不良率が高く、どこまでが Stuxnet によるものか正確な把握が困難だったため報告書によりばらつきがある(例えば、Israel defence: https://www.israeldefense.co.il/では 2000 台と報告)と推測される。

3 注:同社は PCS7 を DCS と位置付けているが WinCC を SCADA(製品カテゴリを SCADA と位置付けており、システム構成図上では HMI としている場合もある)、コントローラを PLC と明記しているため、国内で一般的に DCS として認識されているシステムというよりも PLC 計装システムに近い DCS システムであると推測される。

4 注:プログラマブルロジックコントローラ(登録商標としてシーケンサと呼ぶメーカもある)

5 注:Supervisory Control And Data Acquisition(監視制御および情報取得を行うシステム)

6 注:Engineering Work Station(エンジニアリングワークステーション)

本書では、それらの情報を過去のサイバー攻撃事例の侵入ステップにて補完・推考しながら、最終的な攻撃までの流れを IEC 62443 や NIST SP800-82 Rev.2 など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。

なお、Stuxnet は大きく特徴の異なる 2 種のコードがある事が知られている。一つは 2007 年に作成された初期のもので、もう一つは 2009 年に作成された後期のものである（後期型には、展開時に利用する脆弱性の違い等でさらにいくつかの亜種がある）。ここでは、標的施設以外にも拡散し専門家の間で詳細分析がなされている後期型を中心に説明を行う。初期型と後期型の違いはコラムを参照いただきたい。

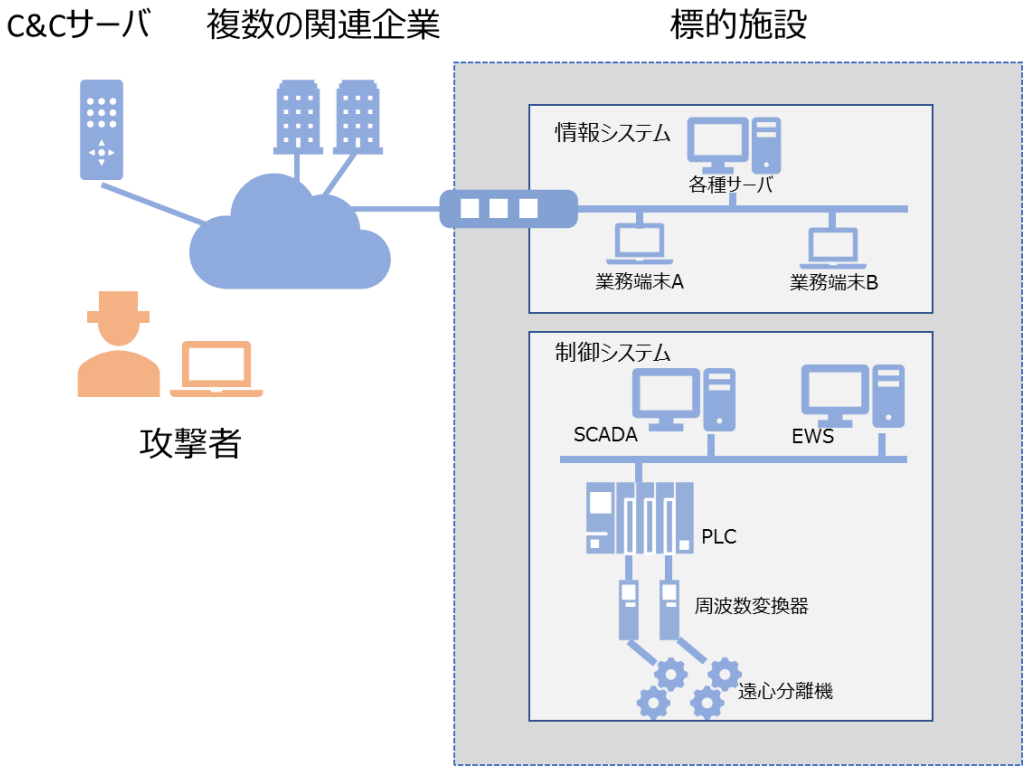


図 1-2 事例理解のための仮想システム構成図（実際のシステム構成とは異なる）

【コラム】Stuxnet の登場と現在に至るまでの経緯について

Stuxnet は、2010 年 6 月 17 日、VirusBlokAda 社（ベラルーシ）によって初めて報告され[2]、当時、世界中で報告が相次いだが報告事案の 6 割程度がイランに集中していた[3]。

コンピュータに感染すると潜伏して活動を開始するマルウェアは Stuxnet と名付けられ、当時のコード解析結果としては、機能的には感染経路としてインターネット経由での拡散機能の他、感染したコンピュータに接続した USB フラッシュドライブ[7]を媒介として、エアギャップ（他と接続のないスタンドアローンネットワークとして隔絶されていること）を乗り越えて、次に USB フラッシュドライブが挿入されたコンピュータでも発症することが確認されていた[3]。

後年、Stuxnet は米国とイスラエルによるサイバー攻撃である事が報道され（2012 年 6 月ニューヨーク・タイムズは、米国家安全保障局：NSA とイスラエル軍情報機関が、このマルウェアをイラン攻撃用に開発したと報じた[4]。 また、元 NSA 職員エドワード・スノーデンも 2013 年 7 月独シュピーゲル誌のインタビューで、NSA とイスラエルが共同で開発したと証言している[5] ）、さらに 2019/9、Stuxnet 研究で著名な米国のセキュリティジャーナリスト Kim Zetter 氏の調査結果が Yahoo News[6]によって公開され 感染経路を含む全貌があきらかになってきた。

Stuxnet 登場の背景と経緯

Stuxnet の目的はイランの核開発を遅らせることにあった。イランの核開発と Stuxnet の開発は以下のような経緯をたどる。

- 1970 年代 パキスタンの核科学者 Abdul Qadeer Khan がオランダに定住。オランダ、アルメロ(Almelo)にあるイギリス・ドイツ・オランダのコンソーシアムの遠心分離法によるウラン濃縮プラントの知見を得る[7]。
- 1975 年 Abdul Qadeer Khan がパキスタンに向かい、その後オランダに戻らず核開発にあたる。この技術はのちに、北朝鮮、イラン、リビアに売られたとの事[7]。
- 2002 年 イラン反体制派により、イランがナタンズとアラーク(Arak)に核燃料施設を建設していたことが暴露され、核開発疑惑が持ち上がる[9]。
- 2003 年 アルメロで使われている遠心分離機の部品の密輸が発覚する事件があった（この部品が米オークリッジに運ばれ遠心分離機に組み立てられ研究に用いられる）[6]
- 2003/9 IAEA 理事会は、イランに対しウランの濃縮・再処理活動の停止を求める理事会決議を採択。2004/11 にパリ合意が成立[9]。
- 2005/6 イランで強行保守派のアフマディジャドが大統領に就任し、ウラン濃縮活動を再開[9]。

[7] USB メモリの事であるが、元資料の表現をそのまま利用し、本資料では USB フラッシュドライブとした。

- 2007 年　オランダがイラン人のエンジニアを工作員としてナタンズに侵入させることに成功。ナタンズ核燃料施設を標的にするためのコードなど重要なデータを入手し、Stuxnet を感染させるための内部アクセス情報も提供したとされている[6]。
- 2007/5　イランで最初の 1700 機の遠心分離器の設置[7]。
- 2007/9　Stuxnet が完成。この Stuxnet は、遠心分離機の出口バルブを閉じる事で、遠心分離装置の内圧を設計値以上に高くし、遠心分離機を損傷させることを狙いとした[8][11]。持ち込みは USB フラッシュドライブの利用で、インターネットに接続されていなかったナタンズの核燃料施設に上記工作員が感染させた。その後 2008 年まで妨害工作を行い、原因究明のために数カ月の遅延が発生した。（2008 年に工作員は理由不明で引き上げ）[6]
- 2009 年　攻撃の効果を上げるため、当時未公開の Windows の脆弱性を利用した新しいバージョンの Stuxnet が開発される[3]。
- 2009/6~2010/5　この Stuxnet はナタンズに出入りするシステムベンダー5 社に配布され、USB フラッシュドライブ経由と考えられる方法で新しい Stuxnet が核燃料施設に持ち込まれる。新しい Stuxnet は PLC に接続された周波数変換器の周波数を異常値に設定し、遠心分離機を故障させる機能を持つ。これらの新型のコードはインターネット接続がある場合バックドアを生成し C&C サーバと通信し自らをアップデートする。なおシステムベンダーのエンジニアは自分達が Stuxnet を持ち込んでいるとは気付いていなかった（USB フラッシュドライブ上で自己を隠蔽する機能がある）[3][8][12]。
- 2010/6　この新型の Stuxnet がセキュリティベンダーに発見される[2]。
  この新型には複数の拡散メカニズムが組み込まれていたため、請負業者の他顧客や、国外にまで拡散が広がり、Stuxnet の存在が明らかになってしまったとみられている[6]。
- 2010/11　ナタンズの 8400 台の遠心分離機すべてが停止。ウラン濃縮活動も停止[10]。
- 2010/11/29　アフマディジャド大統領が、同国の核燃料施設の遠心分離機がコンピュータウィルスに感染していたことを明らかにする[10]。

なお、Stuxnet 発見当時、イラン ブシェール原子力発電所においても Stuxnet が見つかり、チェルノブイリ原発事故に匹敵する大惨事につながった可能性もあると、一部で報道があったが、「コードの攻撃シーケンスは、原子炉またはその関連システムを標的にしているようには見えない」との結論に至っている[11]。

1.2. 被害発生にいたる攻撃の流れ

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いたるまでの流れを次の局面に分けて解説する[8]。(2007 年には送り込まれた内部犯行者を通じて Stuxnet が持ち込まれたが、2009 年のコード更新時には制御システムのベンダー、サプライヤーやエンジニアリングを担うイランの請負業者 5 社が Stuxnet に感染し、これらの会社のエンジニアが知らずにナタンズの核燃料施設に持ち込んだ[12]。ここではこの 2009 年のコード更新以降の流れを取り上げている。)

(1) 制御ネットワーク環境へ侵入までの攻撃局面(☞ 1.2.1 項)
ナタンズの核燃料施設にインターネット接続された情報ネットワークが存在していたか明確な記録は見当たらないため、以下の2通りの経路が考えられるが、本説明では類似した攻撃手順としてまとめて説明を行う。
(ア) 外部接続のある情報ネットワークが存在する場合(図 1-2 のケース)、核燃料施設内部でマルウェアが活動し、上記エンジニアが制御ネットワークに持ち込む。
(イ) 外部接続のある情報ネットワークが存在しない場合、上記請負業者内でマルウェアが活動し、それをエンジニアが核燃料施設の制御ネットワークに持ち込む。
制御ネットワークへの持ち込み方法は USB フラッシュドライブと考えられている。
(2) 制御システム環境内での攻撃局面(☞ 1.2.2 項)
各燃料施設の制御ネットワーク内での活動

1.2.1. 制御ネットワーク環境までの攻撃局面

参考資料[3][6][12]から、事業被害ベースのリスク分析で攻撃の侵入口や経路等を想定する上で、制御ネットワーク環境までの Stuxnet の侵入攻撃の挙動を以下に示す。
本項では、外部から Stuxnet が侵入し非制御ネットワークに拡散するまでを【攻撃局面 A】として記載する。

(1) マルウェアの持ち込み
前記の請負業者に Stuxnet が持ち込まれる[9] [12]。(図 1-3)
Windows コンピュータがマルウェアに感染。
(2) システム上で感染範囲を拡大と特権の奪取[3]
Windows のネットワーク共有機能や当時の 4 件のゼロデイ脆弱性を含む Windows の脆弱性を利用して感染範囲を広げ、特権の奪取をおこなった。特に Windows シェル

[8] 前述したが、ここでは 2009 年に作成された後期型の Stuxnet について説明する。

[9] Stuxnet には侵入した履歴が保存されており、その履歴のスタートが 5 社であったことから、その以前は侵入によるものではないと考えらえる。よってこの 5 社には標的型のメールまたは USB フラッシュドライブで送り込まれたと考えられる。

の脆弱性 MS10-046[13]は、Windows Explorer で表示しただけで感染する脆弱性であり、ネットワーク経由でも外部記憶媒体経由でも有効な攻撃手段であった。)

(3) 隠蔽と活動の永続化[3]

Stuxnet は、特権昇格が成功すると、防御策の回避と永続化をはかる。

(ア) 自身を隠蔽するために rootkit[10] をインストール

(イ) アンチウィルスなどのセキュリティ関連プロセスを終了させる

(4) 感染後 C&C サーバとアクセスして攻撃をはかる[3](図 1-4)

(ア) 標的の内部ネットワークからインターネットへのアクセスが可能な端末に感染すると、Stuxnet は当該端末を踏み台としてインターネット上の C&C サーバに接続して命令を受け取り、また自身をアップデートすることも可能

(イ) 踏み台経由で間接的にインターネットにアクセスが可能で、ネットワーク内に他にも感染した Stuxnet が存在すれば、自身のバージョンと比較して P2P[11]通信を介して最新版にアップデートする

(ウ) ネットワーク内で収集した情報をアップロードする機能も有する

(5) 標的システムへの持ち込みと感染の展開(図 1-5)

関連企業または情報ネットワークから、外部記憶媒体を利用して Stuxnet が標的システムへ持ち込まれ、ネットワーク内で各種の脆弱性を使って感染範囲を拡大する。

Stuxnet は標的システム内でも上記(2)～(4)の活動をしていたと推定される。

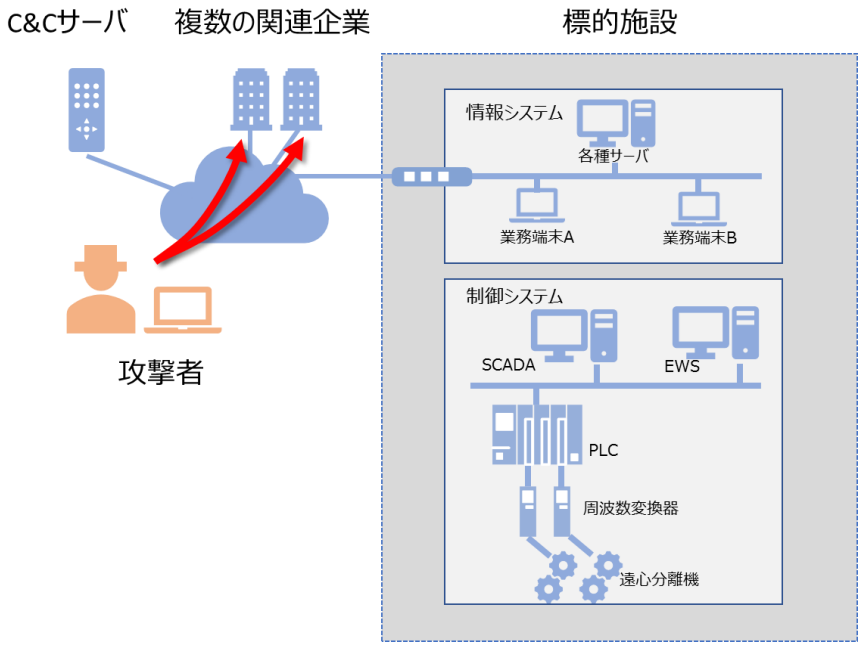


図 1-3【攻撃局面 A】制御ネットワーク環境までの攻撃局面-1

[10] 注:コンピュータへの不正侵入に成功した攻撃者が、侵入後に遠隔操作で活動するために必要なソフトウェア一式をまとめたパッケージ

[11] 注:Peer to Peer 端末同士の一対一の通信

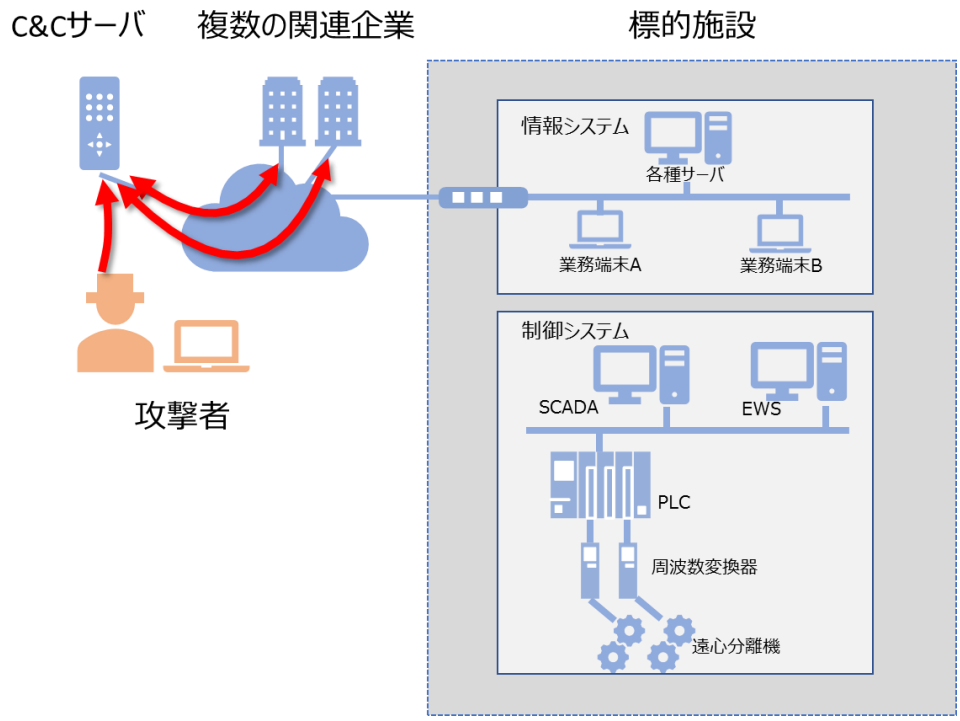


図 1-4【攻撃局面 A】 制御ネットワーク環境までの攻撃局面-2

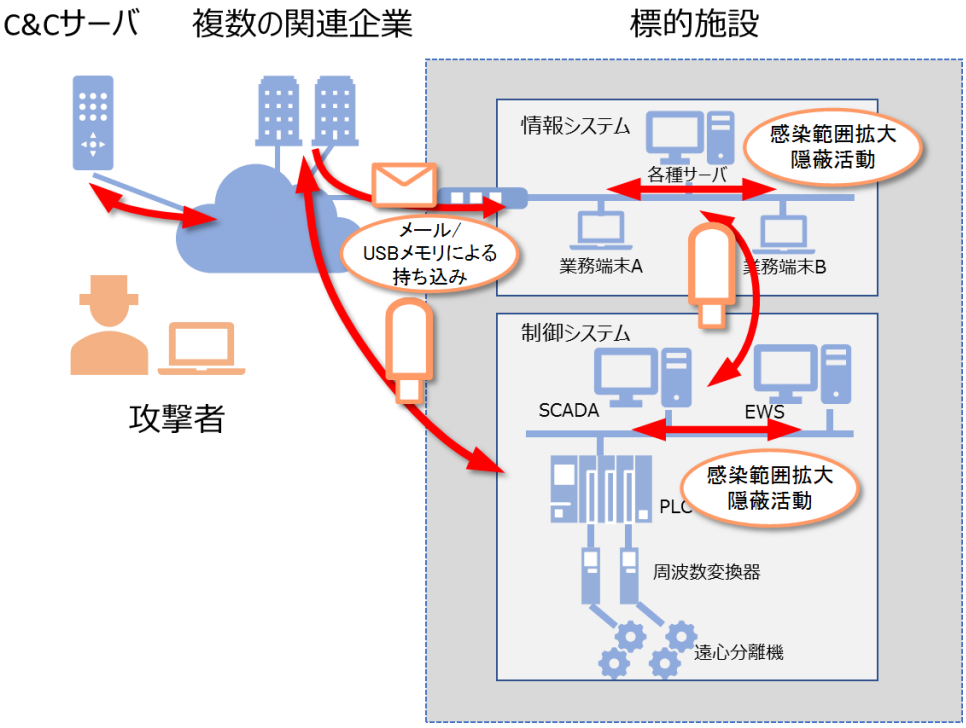


図 1-5【攻撃局面 A】 制御ネットワーク環境までの攻撃局面-3

1.2.2. 制御システム環境での攻撃局面（図 1-6,1-7）

参考資料[3]から事業被害ベースのリスク分析で攻撃の侵入口や経路等を想定する上で、制御システム環境に到達した後の Stuxnet の攻撃手法を以下に示す。

本項では、Stuxnet がネットワークに拡散後、特定のターゲットに対して改ざん工作を行う段階を【攻撃局面 B】として記載する。

(1) 制御ネットワークに侵入した Stuxnet は、標的となる SCADA を発見すると攻撃を開始する[10]。

(ア) SCADA を発見後、Stuxnet は開発元によってシステム内にハードコードされたパスワード[12]の脆弱性（CVE-2010-2772[13]）を利用してログインする。

(イ) SCADA の SQL データベースに新たなテーブルを生成し、悪質な実行プログラムの書き込みを行い、実行する。

(ウ) SCADA から PLC のプログラムファイル（プロジェクトファイル）を本来意図して設定しようとした動作とは異なる動作を組み込んで、異常プロセスを実行する[14]

(2) EWS（S7 ソフトウェア）は、複数の命令の集合体であるライブラリファイルを使用して PLC との通信を行う。Stuxnet はこのライブラリファイルの一部の命令を改ざんする[3]。
（この改ざんによって意図しない攻撃ブロックが生成されてしまう）
PLC の CPU モジュールが攻撃対象の遠心分離機に接続された特定の型番であった場合、Stuxnet は悪意のあるコードのインジェクションを実行する。

(3) 攻撃対象は非常に高速（807Hz～1210Hz）で動作する遠心分離機の周波数変換器[15] を持つシステムであり、Stuxnet は該当するシステムにおける制御系システムの通常動作を妨害し、何か月にもわたって出力周波数を短時間のうちに変化させて遠心分離機に高い負荷をかけて破壊する[3]。
同時に、遠心分離機の異常状態を隠すために SCADA と PLC 間の通信機能に目隠しを挿入する。この動作により、異常動作時でもオペレータには何の問題も生じていないように見せかける[3]。（図 1-7）

---

12 注：プログラムに規定値として組み込まれているパスワード

13 注：Siemens Simatic WinCC および PCS 7 の脆弱性
（https://jvndb.jvn.jp/ja/contents/2010/JVNDB-2010-001829.html）

14 注：参考資料 19 は「Stuxnet は WinCC/STEP7/S7 をターゲットとする」としているが、攻撃コードの解析からは「WinCC/STEP7/S7 が分散して共有するプロジェクトファイル」がターゲットであることが分かる。

15 注：出力周波数を変換することで、モーターの速度を制御できる装置

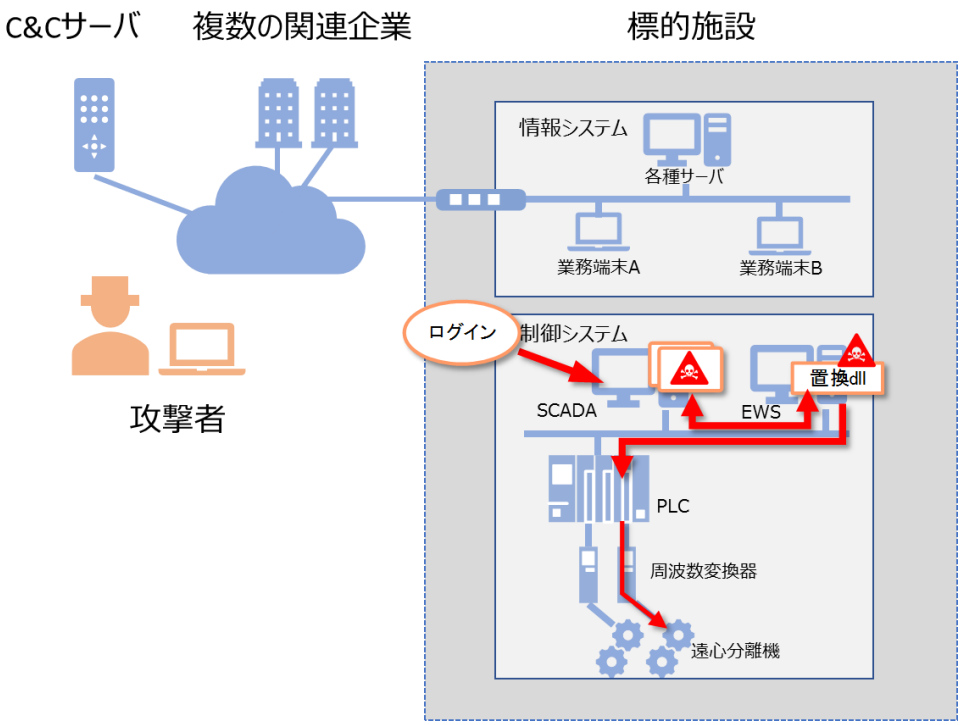


図 1-6【攻撃局面 B】 制御ネットワーク環境での攻撃局面-1

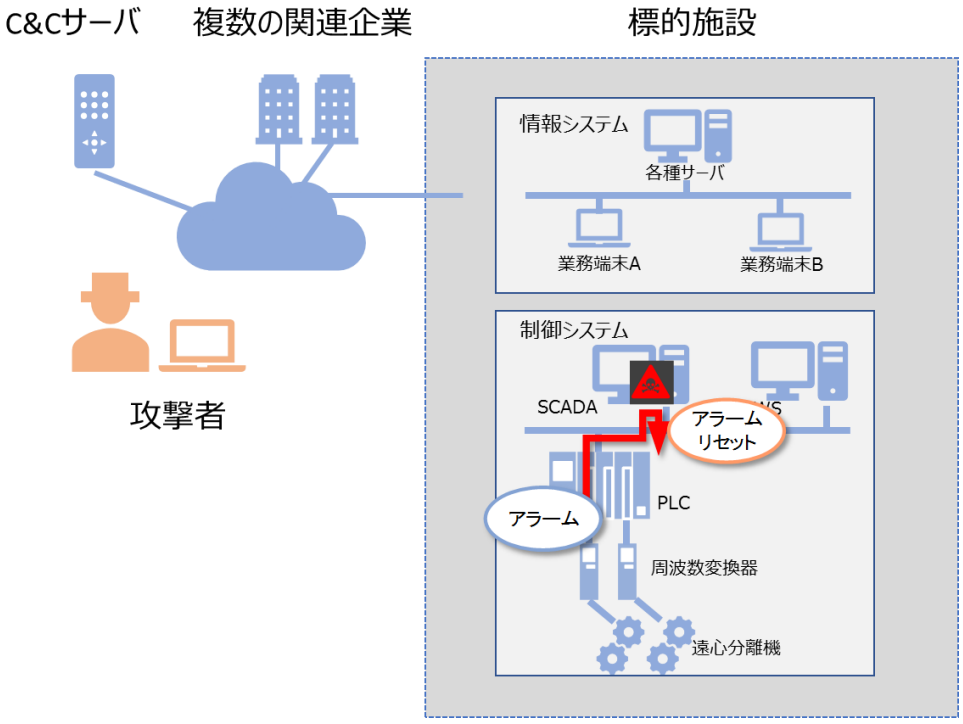


図 1-7【攻撃局面 B】 制御ネットワーク環境での攻撃局面-2

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、Stuxnet と類似のインシデントを想定したリスク分析を紹介しているため、1 章で紹介した Stuxnet のインシデントに IPA の推定部分が加わる事に注意されたい。

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">周波数変換器の設定が本来の設定と異なることによる遠心分離機の不具合（破損）</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>EWS 端末からエンジニアが意図しない改ざんされた値を周波数変換器に設定されてしまう。異常な制御が作動し遠心分離機を破損[3]。</td><td>EWS
端末</td><td>PLC</td><td>PLC に対する攻撃スクリプトの送信</td></tr>
<tr><td rowspan="3">2</td><td colspan="4">緊急時に SCADA[16]から正常な監視・操作ができないことによる物理的な被害の拡大</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>PLC と SCADA 間の通信機能に目隠しを挿入し、センサ測定値異常時に SCADA には異常状態が表示されなくする[3]。</td><td>SCADA</td><td>SCADA</td><td>SCADA のファイル改ざんと悪意のあるファイルを挿入</td></tr>
</table>

[16] 注：HMI（Human Machine Interface）と置き換えて考えてもよい。Siemens 社は WinCC を SCADA とも HMI とも表記する。

また、事業被害に至る攻撃ルートの例を以下に示す。侵入口、経由に相当する情報は明らかになっていないため判明している範囲の情報で、最も経路の長くなる攻撃局面を想定した。

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*[17]	*オペレーションに使用する USB フラッシュドライブや脆弱性を利用してマルウェアを拡散*	EWS 端末	PLC	PLC に対する攻撃スクリプトの送信
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*[17]	*オペレーションに使用する USB フラッシュドライブや脆弱性を利用してマルウェアを拡散*	SCADA	SCADA	SCADA のファイル改ざんと悪意のあるファイルを挿入

さらに、今回の事例に限らず一般的なシステムにおいては、以下の様な侵入方法も考えられる。

- ファイアウォールの脆弱性や管理ポートからパスワードを分析して侵入。管理者権限を奪取し ACL を書き換える
- 開いているポートからの侵入（Telnet など）
- 使用中のサービスの脆弱性を利用した侵入
- リモート接続口からの侵入
- USB フラッシュドライブと同様にメンテナンス用の持ち込み PC を媒体とした侵入

17 ここで「インターネットに接続されたネットワーク」と記載しているのは、核処理施設の内部のインターネットに接続された情報ネットワーク、または、核処理施設に出入りする業者のネットワークかは定かではないため、両方の可能性をまとめた表記としている。

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、表 2-4 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 1：遠心分離機の破壊の例

攻撃局面	項番	攻撃シナリオ 攻撃ツリー・ステップ ＜情報ネットワーク上の端末感染から、情報収集・感染拡大、リモートアップデートで攻撃ファイルをアップデートさせながら侵入し、SCADA を踏み台として SCADA/EWS/PLC のプロジェクトファイルを改ざん。異常な制御を実行し、遠心分離機を破壊＞
【A1】	S1-1	侵入口=インターネットに接続されたネットワーク上の端末 A(以下端末 A) 攻撃者が情報システム内の端末 A で USB フラッシュドライブを使用してマルウェア感染を誘導する。
【A1】	S1-2	端末 A がマルウェアに感染する。C&C サーバとの通信が確立する。
【A2】	S1-3	攻撃者は、C&C サーバから端末 A 経由で他業務端末や各種サーバに対して情報探索や感染拡大を行い制御システムに関連する情報を収集する。
【A3】	S1-4	収集した情報をもとに攻撃用コードをアップデートする。
【A3】	S1-5	マルウェアが USB フラッシュドライブの持ち込みにより制御ネットワーク上の SCADA に感染する。
【B1】	S1-6	SCADA 上でプロジェクトファイル群へのアクセス権を奪取して改ざんし、アクセス権を利用して EWS 端末にマルウェアを感染させる。
【B2】	S1-7	EWS 端末上で攻撃用のプログラムファイルを用意し、エンジニアリング機能で PLC へ攻撃スクリプトを送信する。
【B2】	S1-8	PLC に送信された攻撃スクリプトによって、異常な制御が発生し、遠心分離機が破損する。

表 2-4 事業被害 2:表示の偽装の例

攻撃局面	項番	攻撃シナリオ 攻撃ツリー・ステップ ＜情報ネットワーク上の端末感染から、情報収集・感染拡大、リモートアップデートで攻撃ファイルをアップデートさせながら侵入し、SCADA を踏み台としてSCADA/EWS/PLC のプロジェクトファイルを改ざん。監視画面をダミーにしてオペレータに気付かせないまま異常な制御を実行し、遠心分離機を破壊＞
【A1】	S2-1	侵入口=インターネットに接続されたネットワーク上の端末 A(以下端末 A) 攻撃者が情報システム内の端末 A で USB フラッシュドライブを使用してマルウェア感染を誘導する。
【A1】	S2-2	端末 A がマルウェアに感染する。C&C サーバとの通信が確立する。
【A2】	S2-3	攻撃者は、C&C サーバから端末 A 経由で他業務端末や各種サーバに対して情報探索や感染拡大を行い制御システムに関連する情報を収集する。
【A3】	S2-4	収集した情報をもとに攻撃用コードをアップデートする。
【A3】	S2-5	マルウェアが USB フラッシュドライブ経由で制御ネットワーク上の SCADA に感染する。
【B1】	S2-6	SCADA 上で、周波数変換器の正常動作データを窃取する
【B2】	S2-7	SCADA 上で、悪意あるプログラムを作動させ、PLC からの周波数変換器の稼働状況データを、ダミーの正常動作データに置き換えて表示する
【B2】	S2-8	PLC から遠心分離機に高い負荷をかける設定を送り破損させる。

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 2-5 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（下線は【コラム】仮想の攻撃局面より）
攻撃用途		
	侵入口	USB フラッシュドライブ（インターネットに接続されたネットワーク上の端末）
	攻撃対象	PLC（事業被害 1）、SCADA（事業被害 2）
	攻撃拠点	EWS 端末（事業被害 1）、SCADA（事業被害 2）
	経由	ネットワーク経由およびオペレーションで使用する USB フラッシュドライブ経由
攻撃者		悪意のある外部の攻撃者
事業被害		異常な制御が実行されることによる遠心分離機の破損
攻撃シナリオ		SCADA・EWS 端末・PLC のプロジェクトファイルを改ざんし、SCADA 上の監視状態を正常に見せかけながら、EWS から PLC へ攻撃スクリプトを送信。異常な制御を実行して遠心分離機を破壊。
最終攻撃（目的）		PLC に対する攻撃スクリプトの送信
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		標的型攻撃メールの送付 C&C（Command & Control）サーバとの通信確立 情報探索 感染拡大（ネットワーク経由/運用する USB フラッシュドライブ経由での横断的侵害） 設定アプリケーションへのなりすまし 攻撃スクリプトの開発 攻撃スクリプトの書き込み

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 2-5 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、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	制御ネットワークと情報ネットワークの物理的な分離[15]（ネットワーク分離）
D1’	制御ネットワークと情報ネットワークの論理的な分離[15]（FW の導入とネットワークセグメンテーション）
D2	パッチの適用・外部記憶媒体の管理/利用制限・アンチウイルスソフトの導入[16]
D3	侵入検知のためのログ管理[15]
D4	EWS 端末やコントローラの適切な管理・運用[15]
D5	物理的な入退管理
D6	ホワイトリストによるプロセスの起動制限[16]

「D1. **制御ネットワークと情報ネットワークの物理的な分離（ネットワーク分離）**」は、制御ネットワークを他のネットワークから分離するため理想的には見えるが、今回の様な持ち込みのケースもありうる。本緩和策のみでは、USB フラッシュドライブを経由して侵入する未知のマルウェアについては対応が難しくなるため、項番 D2、D3 との複合的なリスクマネジメントが、対策・緩和策の重要な砦の 1 つとなる。しかし、システム構成や運用の合理化等の理由から他ネットワークへの接続が必要な場合は、FW 等によるアクセス制御およびネットワークセグメンテーション（項番 D1’）、侵入検知のための NW 間の通信ログ監視（項番 D3）など複数のセキュリティ施策による運用を期待する。

「D2. **パッチの適用・外部記憶媒体の管理・アンチウイルスソフトの導入**」は、脆弱性攻撃を緩和するために Windows アップデート（パッチ）の適用・組織の社内ポリシーを確認し外部記憶媒体を無効にするための保護対策を確立、検出/駆除のためアンチウイルスソフト導入を推奨している。

「D3. **侵入検知のためのログ管理**」は、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。攻撃の初期段階での検知が出来れば、深刻化する前にインシデント対応をすることが期待出来る。

「D4. EWS **端末やコントローラの適切な管理・運用**」は、EWS の保管や運用において、項番 D2 同様組織の社内ポリシーの確認が重要である。異常の察知方法の検討など課題はあるが、まずは HSE の整備とリスクマネジメントをどのように確立するかが重要である。

「D5. 物理的な入退管理」は、制御システムエリアへの部外者の立ち入りを厳しくチェックすることで項番 D1 の対策としても有効になることが期待できる。

「D6. ホワイトリストによるプロセスの起動制限」は、制御に不要なプログラムの動作を制限する事で、マルウェアの活動の抑制が期待できる。

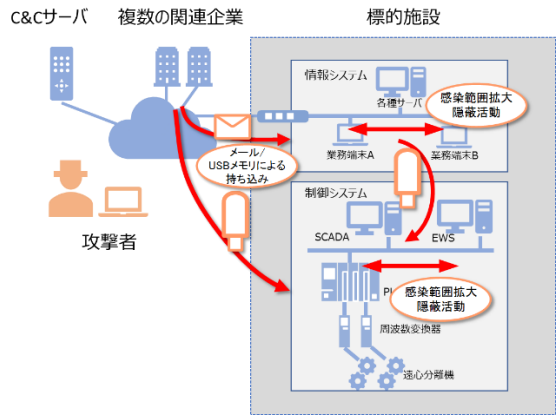
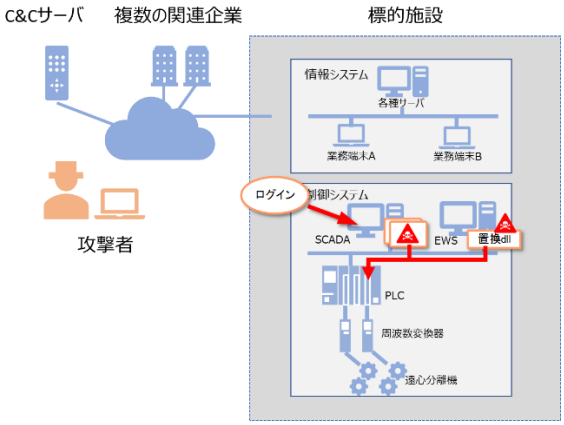
以上が本ケースにおける緩和策となるが、基本的に未知のマルウェアによる侵入に対しては、出来るだけ内部への侵入を遅らせてその間に検知できるようなシステム構成と、迅速なインシデント対応を可能とする体制・管理・運用面の強化が、対策・緩和策として検討いただきたい項目である。

インシデント事例のサイバー攻撃要素の整理同様、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。

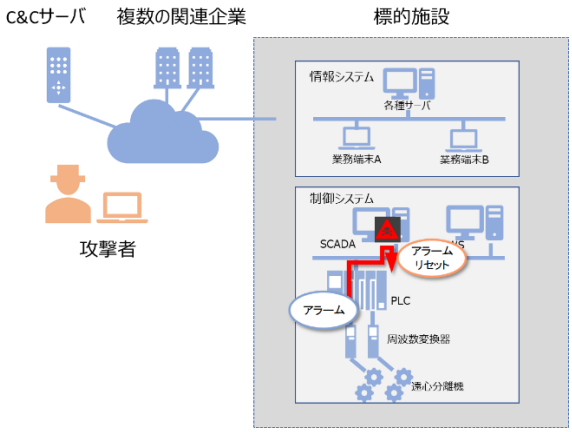
2.5. 攻撃ステップと対策・緩和策の関連付け

2.4 節までの情報をもとに、制御ネットワーク環境への侵害が行われた【攻撃局面 A3】や【攻撃局面 B】と代表的な対策・緩和策を紐づけた例が表 2-7 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 2-7 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[18]	対策・緩和策	対象システム・資産
攻撃局面【A3】 	ネットワーク経由・USB フラッシュドライブ経由の感染 [S1-5] [S2-5]	•パッチの適用・外部記憶媒体の管理/利用制限・アンチウイルスソフトの導入 [D2] •メンテナンス端末やコントローラの適切な管理・運用 [D4] •物理的な入退管理 [D5]	•SCADA •EWS
攻撃局面【B1】 	攻撃スクリプト送信 [S1-7]	•侵入検知のためのログ管理 [D3] •EWS 端末やコントローラの適切な管理・運用 [D4] •ホワイトリストによる起動制限[D6]	•EWS •SCADA •PLC

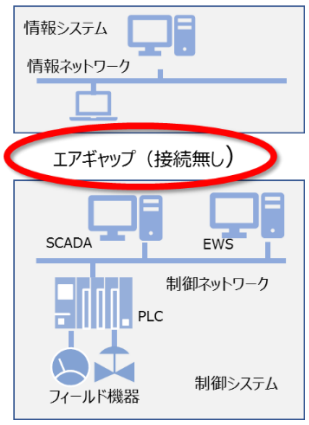
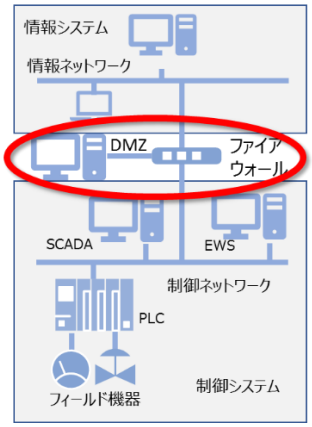
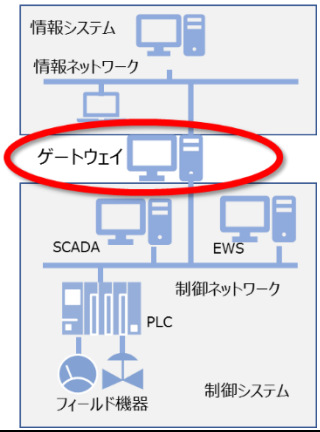
[18] [S]は表 2-3 の項番と対応。 [D]は表 2-6 の項番と対応。

攻撃局面（つづき）	攻撃ステップ[19]	対策・緩和策	対象システム・資産
攻撃局面【B2】  	データの窃取と偽の表示 [S2-7]	•パッチの適用・外部記憶媒体の管理/利用制限・アンチウイルスソフトの導入 [D2] •メンテナンス端末やコントローラの適切な管理・運用 [D4] •ホワイトリストによる起動制限[D6]	•SCADA

なお、一般的なシステム構成についてはいくつかの分類が考えられることから、その代表的な構成例と推奨度、また、それぞれにおける対策例を表 2-8 にまとめた。今後、セキュリティ対策・緩和策を検討する際の一例として活用いただきたい。

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

表 2-8 セキュリティを考慮した推奨構成と構成毎の対策例

構成	エアギャップで分離 （1 方向ゲートウェイなどもこれに含むものとする）	制御ネットワークが情報ネットワークと接続 境界防御　有 （FW で DMZ が構成され、通信を中継するサーバが存在）	制御ネットワークが情報ネットワークと接続 境界防御　無 （DMZ が無く、アプリケーションゲートウェイがデュアルホーム）
推奨度	◎ 推奨構成	○ 次善構成	△ 検討が必要な構成
イメージ図			
対策・検討ポイント例	• パッチの適用・外部記憶媒体の管理・アンチウイルスソフトの導入[D2] • 侵入検知のためのログ管理[D3] • EWS 端末やコントローラの適切な管理・運用[D4] • 入退室管理[D5] • ホワイトリストによるプロセスの起動制限[D6]	• **NW構成の見直し・切り離しの厳選[D1]** • パッチの適用・外部記憶媒体の管理・アンチウイルスソフトの導入[D2] • 侵入検知のためのログ管理[D3] • EWS 端末やコントローラの適切な管理・運用[D4] • リモート接続の管理 • 入退室管理[D5] • ホワイトリストによるプロセスの起動制限[D6]	• **NW 構成の見直し・切り離しの厳選[D1]** • **境界防御装置の導入検討[D1']** • パッチの適用・外部記憶媒体の管理・アンチウイルスソフトの導入[D2] • 侵入検知のためのログ管理[D3] • EWS 端末やコントローラの適切な管理・運用[D4] • リモート接続の管理 • 入退室管理[D5] • ホワイトリストによるプロセスの起動制限[D6]

注：ただし、「システム構成（および対策設置）」だけで全ての攻撃を緩和でき得る訳ではないので、リスクマネジメントによる「攻撃の兆候検知」と「インシデント対応体制の整備」が必要不可欠。
（Stuxnet は推奨構成のエアギャップを乗り越えて攻撃するマルウェアであることに注意）

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] Institute for Science and International Security:
Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Preliminary Assessment（2010/12/22）
https://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-Natanz-enrichment-plant/8

[2] VirsBlokAda:Rootkit.TmpHider
http://www.anti-virus.by/en/tempo.shtml

[3] Symantec: W32.Stuxnet Dossier
https://docs.broadcom.com/docs/security-response-w32-stuxnet-dossier-11-en
（ https://www.wired.com/images_blogs/threatlevel/2011/02/Symantec-Stuxnet-Update-Feb-2011.pdf）

[4] New York Times:
Obama Order Sped Up Wave of Cyberattacks Against Iran（2012/6/1）
https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html

[5] SPIEGEL:
Edward Snowden Interview, The NSA and Its Willing Helpers（2013/7/8）
https://www.spiegel.de/international/world/interview-with-whistleblower-edward-snowden-on-global-spying-a-910006.html

[6] Yahoo News:
Revealed: How a secret Dutch mole aided the U.S.-Israeli Stuxnet cyberattack on Iran（2019/9/3）
https://news.yahoo.com/revealed-how-a-secret-dutch-mole-aided-the-us-israeli-stuxnet-cyber-attack-on-iran-160026018.html

[7] deVolkskrant:
AIVD speelde cruciale rol bij sabotage kernprogramma Iran（2019/9/2）
https://www.volkskrant.nl/nieuws-achtergrond/aivd-speelde-cruciale-rol-bij-sabotage-kernprogramma-iran~ba24df9f/?referer=https%3A%2F%2Fwww.google.com%2F

[8] Ralf Langner: TO KILL A CENTRIFUGE（2013/11）
https://www.langner.com/to-kill-a-centrifuge/

[9] 日本原子力研究開発機構: イラン核問題
https://www.jaea.go.jp/04/iscn/archive/nptrend/nptrend_01-06.pdf

[10] JPCERT/CC: Stuxnet-制御システムを狙った初のマルウェア（2011/2/18）
https://www.jpcert.or.jp/ics/2011/20110210-oguma.pdf

[11] Institute for Science and International Security:
Stuxnet Malware and Natanz（2011/2/16）
http://isis-online.org/isis-reports/detail/stuxnet-malware-and-natanz-update-of-isis-december-22-2010-reportsupa-href1/

[12] カスペルスキー: Stuxnet の起源：最初に狙われた 5 つの組織（2014/11/28）
https://blog.kaspersky.co.jp/stuxnet-victims-zero/5532/

[13] MS10-046
https://docs.microsoft.com/ja-jp/security-updates/securitybulletins/2010/ms10-046

[14] IPA:
制御システムにおけるセキュリティマネジメントシステムの構築に向けて
https://www.ipa.go.jp/files/000014265.pdf

[15] McAfee: What Is Stuxnet?
https://www.mcafee.com/enterprise/ja-jp/security-awareness/ransomware/what-is-stuxnet.html

[16] CISA: ICS Advisory (ICSA-10-238-01B) Stuxnet Malware Mitigation (Update B) (2014/1/8)
https://www.us-cert.gov/ics/advisories/ICSA-10-238-01B

更 新 履 歴

2020 年 3 月 16 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 4

～Stuxnet:制御システムを標的とする初めてのマルウェア（2010 年）～

[発　　行]　2020 年 3 月 16 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、木下　弦

協力者　桑名　利幸　木下　仁　小助川　重仁