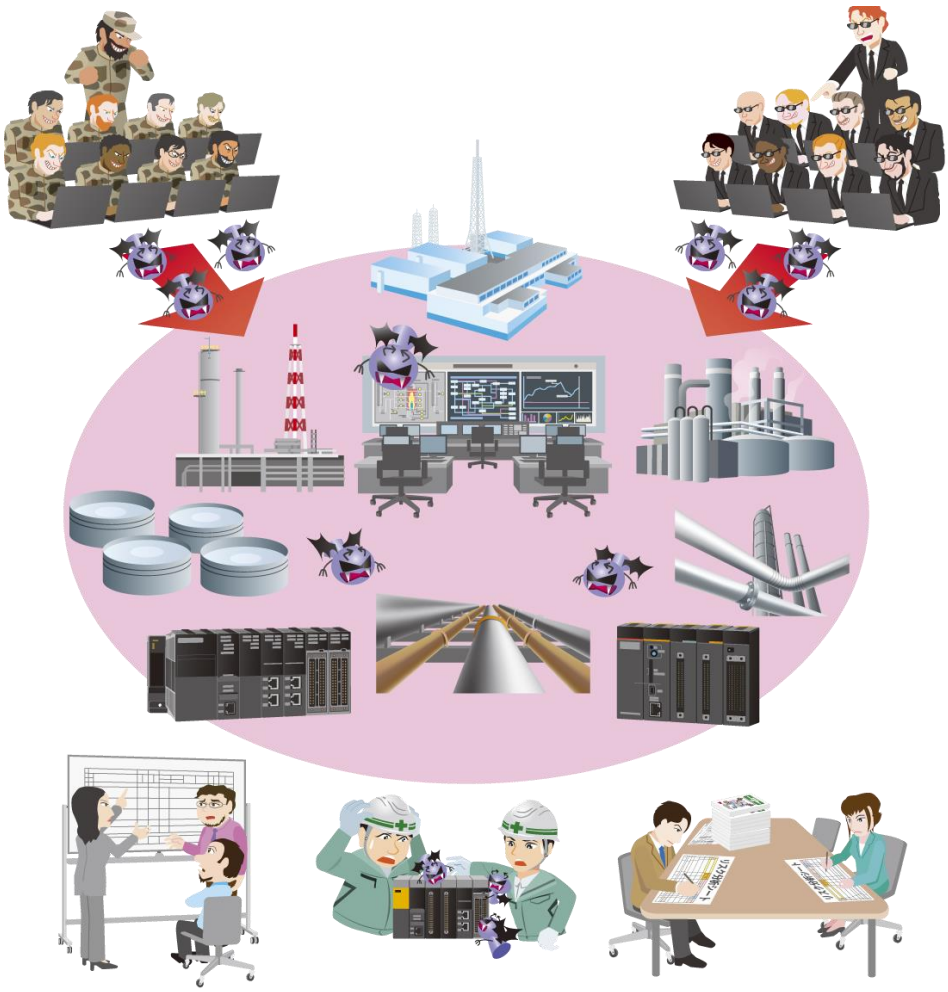
制御システムのセキュリティリスク分析ガイド補足資料

制御システム関連のサイバーインシデント事例3

～2017 年　安全計装システムを標的とするマルウェア～



2019 年 7 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。

本資料の位置づけ

前半では、2017 年 12 月に公表された安全計装システムを標的とするマルウェアと中東のプラントで発生したとされる操業停止事象に関する米国 ICS-CERT などの公開情報（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。【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。

後半では、当該インシデントに関係する情報を整理し、攻撃シナリオやツリー・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. 2017 年 安全計装システムを標的とするマルウェアによる操業停止

1.1. インシデント概要

2017 年 12 月に公表されたマルウェア「HATMAN（別名:TRITON / TRISIS）」は、安全計装システム（以下、SIS：Safety Instrumented System）を標的とした初のマルウェアである。当該マルウェアは中東の企業で使用されていた Schneider Electric 社製の SIS コントローラー(Triconex)や関連製品に対して、サイバー攻撃を行うために開発・使用されたという。結果的に SIS のフェールセーフ機能が作動し、操業が一時停止する事態となった[1]。

なお、2019 年 4 月には、米国のセキュリティベンダから HATMAN（別名:TRITON / TRISIS）に関連した追加情報[2]が公表された。その中には、重要インフラ事業者に対する同様のサイバー攻撃を観測した（被害には至っていない）との情報が含まれている。本インシデントで使用されたマルウェアは、SIS にとって依然脅威であり、事業関係者は十分な留意が必要である。

一方、本事例に関して公開情報では、どのように企業の SIS 環境まで侵入したのかなどの詳細な情報は公開されていない。しかしながら、マルウェア HATMAN や侵害された環境に関する一部の情報は確認することができる。

今回は、それらの部分的な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 SIS に対する攻撃までの流れを 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 1-1）を用いて説明する。

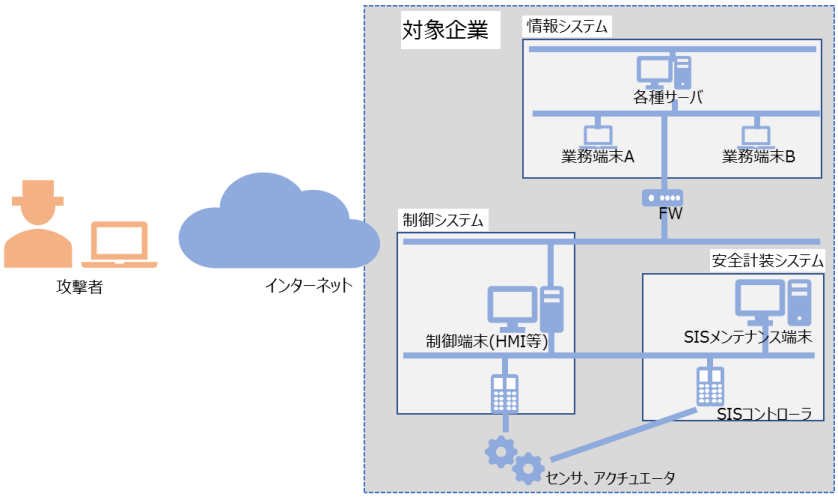


図 1-1 事例理解のための仮想システム構成図（実際のシステム構成とは異なる）

[1] [3-1]
[2] [3-2]

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に代表的なサイバー攻撃の流れを補完することで、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。

① SIS 環境までの攻撃局面（☞ 1.2.1 項）
② SIS 環境での攻撃局面（☞ 1.2.2 項）

1.2.1. SIS 環境までの攻撃局面

参考資料では、攻撃者がどのように SIS 環境まで到達したか、どのようにマルウェア HATMAN が持ち込まれたかについて明らかになっていない。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、過去のサイバー攻撃の代表的な手法を以下に示す。

(1) 外部からネットワーク経由で情報システム環境に侵入し、SIS 環境まで到達した可能性
(2) 外部記憶媒体で制御システム環境や SIS 環境にマルウェアが持ち込まれた可能性

1.2.2. SIS 環境での攻撃局面

何らかの方法で SIS 環境に侵入し、攻撃者が SIS メンテナンス端末にリモート接続できる状況である。

SIS メンテナンス端末に導入した不正プログラムから攻撃用スクリプトを SIS コントローラーに対して送信する。SIS コントローラーへの書き込みが行われ、最終的に SIS 側でのフェールセーフ機能が作動することによって、操業が停止するに至ったとされる[3]。

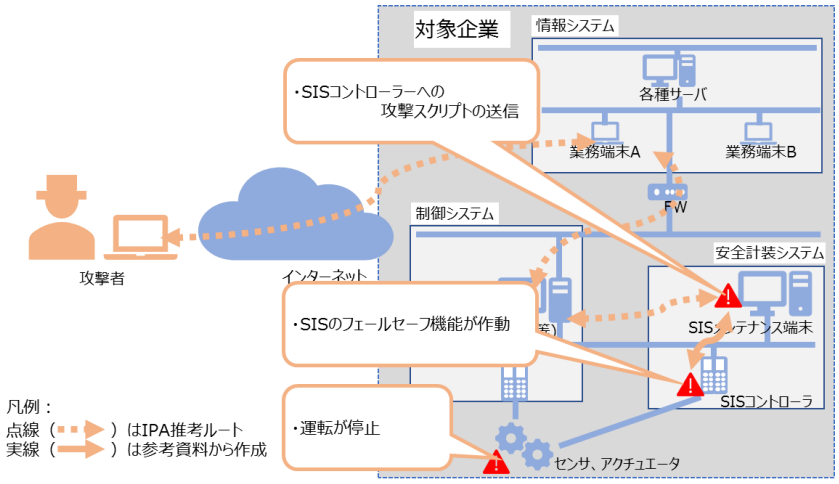


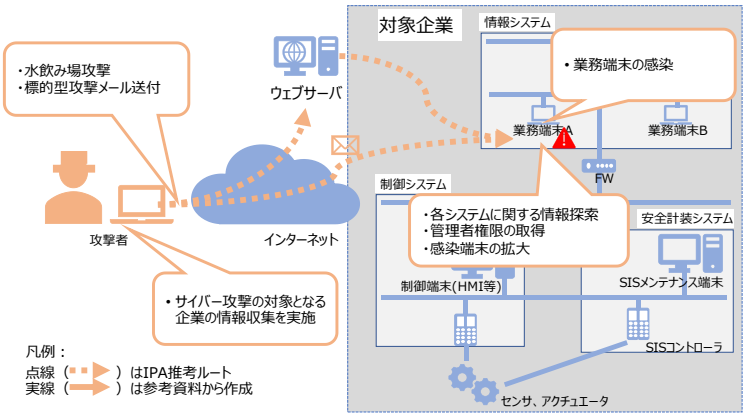
図 1-2 【攻撃局面 B】SIS コントローラーへの攻撃スクリプトの送信

[3] [1-1] Analysis、[2-1] スライド 7-9 参照

【コラム】仮想の攻撃局面：SIS 環境までの侵入

過去のサイバー攻撃の代表的な手法として、1.2.1 項 (1) で挙げたインターネットから侵入された場合の攻撃手法と経路を記載する。事業被害ベースのリスク分析を行う上での参考にして欲しい。

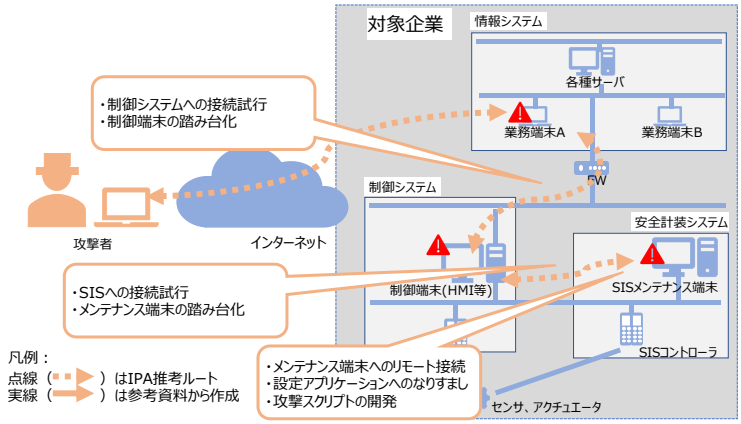
【仮想の攻撃局面 A1】対象企業に対しての情報収集とマルウェアへの感染
【仮想の攻撃局面 A2】活動範囲の拡大とそれに伴う内部情報の収集



インターネット等で収集した標的となった企業に関する情報の中から社員情報などをもとに、標的型攻撃メールの送付や水飲み場攻撃を介して、業務端末 A のマルウェア感染を誘う。また、マルウェアに感染した業務端末 A を起点として、業務端末や各種サーバへ活動範囲を拡大（横断的侵害）しながら内部情報の探索・収集を行う。

図 1-3 【仮想の攻撃局面 A1】攻撃に向けての情報収集・
【仮想の攻撃局面 A2】活動範囲の拡大とそれに伴う内部情報の収集

【仮想の攻撃局面 A3】SIS への侵入と設定アプリケーションへのなりすまし・スクリプトの開発



標的企業の内部探索によって収集した各種情報をもとに、リモート接続による SIS への侵入を試み、SIS メンテナンス端末上の設定アプリケーションになりすまし、攻撃用スクリプトの開発が行われる。

図 1-4 【仮想の攻撃局面 A3】SIS への侵入とマルウェアの開発

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。

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。

事業被害 2 は、参考資料において事業被害となる可能性が指摘されているため[4]、参考として記載した。

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">SIS コントローラーのフェールセーフ機能が作動することによる運転の停止</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>SIS メンテナンス端末から攻撃スクリプトを SIS コントローラーへ送信。フェールセーフ機能が作動し、運転が停止。</td><td>SIS メンテナンス端末</td><td>SIS コントローラー</td><td>SIS コントローラーに対する攻撃スクリプトの送信</td></tr>
<tr><td>2</td><td colspan="4">緊急時に SIS コントローラーが正常動作しないことによる物理的な被害発生</td></tr>
</table>

また、事業被害 1 に至る攻撃ルートの例を以下に示す。攻撃者、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、【コラム】仮想の攻撃局面 を利用した。

表 2-2 攻撃ルートの例（下線は【コラム】仮想の攻撃局面より）

<table>
<tr><th>誰が</th><th>どこから</th><th>どうやって</th><th colspan="2">どこで</th><th>何をする</th></tr>
<tr><th>攻撃者</th><th>侵入口</th><th>経由</th><th>攻撃拠点</th><th>攻撃対象</th><th>最終攻撃</th></tr>
<tr><td>悪意のある外部の第三者</td><td>業務端末 A</td><td>（FW 機器）～制御端末</td><td>SIS メンテナンス端末</td><td>SIS コントローラー</td><td>攻撃スクリプト送信</td></tr>
</table>

[4] [1-1] IMPLICATIONS

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 リモートアクセス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 ＜情報システムの業務端末感染から、情報収集・感染拡大、リモート接続で安全計装システムへ侵入し、SIS メンテナンス端末から攻撃スクリプトを SIS コントローラーへ送信。フェールセーフ機能が作動し、運転が停止＞
【A1】	S1	侵入口=情報システムの業務端末 A(以下業務端末 A) 攻撃者が情報システム内の業務端末へのマルウェア感染への感染を誘導する。
【A1】	S2	業務端末 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】	S3	攻撃者は、C&C サーバから業務端末 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】	S4	収集した情報をもとに制御端末へリモート接続する。
【A3】	S5	収集した情報をもとに SIS メンテナンス端末へリモート接続する。
【A3】	S6	SIS メンテナンス端末上で設定アプリケーションになりすまし、攻撃スクリプトを開発する。
【B】	S7	SIS メンテナンス端末上で設定アプリケーションになりすましたプログラム経由で、SIS コントローラーへ攻撃スクリプトが送信される。
【B】	S8	書き込まれたスクリプトによって、SIS のフェールセーフ機能が作動し、運転が停止する。

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	不明（情報システムの業務端末）
	攻撃対象	SIS コントローラー
	攻撃拠点	SIS メンテナンス端末
	経由	詳細は不明（（FW 機器）～制御端末）
攻撃者		詳細は不明（悪意のある外部の第三者）
事業被害		フェールセーフ機能が作動することによる運転の停止
攻撃シナリオ		SIS メンテナンス端末から攻撃スクリプトを SIS コントローラーへ送信。フェールセーフ機能が作動し、運転が停止。
最終攻撃（目的）		SIS コントローラー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 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（横断的侵害） リモート接続 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 2-4 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、ICS-CERT から公表された MAR-17-352-01 HATMAN[5] を参考に、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	SIS と他 NW の物理的な分離（ネットワーク分離）[5]
D1’	SIS と他 NW の論理的な分離（FW の導入）[5]
D2	プログラムモードへの設定変更管理 [5]
D3	外部記憶媒体の管理 [5]
D4	メンテナンス端末やコントローラーの適切な管理・運用 [5]

「D1. SIS と他 NW の物理的な分離（ネットワーク分離）」は、SIS が、他ネットワークと接続されているか否かが焦点となる。物理的分離は、対策・緩和策の重要な砦の 1 つとなる。そのため、可能な限り物理的に分離された構成を検討いただきたい。しかし、システム構成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[D1’]や NW 間の通信監視など複数のセキュリティ施策による運用を期待する。

「D2. プログラムモードへの設定変更管理」は、SIS コントローラーの状態を切り替える機能を適切に管理する運用を意味している。プログラム可能なモードや運転モードなどコントローラーの状態を物理的なキーで切り替える機能を有している場合もあり、本事例では、プログラム可能なモードでなければコントローラーへの不正なスクリプトの埋め込みは防げたのではないかとされているからである。

安全計装システムにおける緩和策となるが、制御システムで使用されるコントローラーにおいても同様に物理的機能を有している場合もあることから、管理・運用面での対策・緩和策として検討いただきたい項目である。

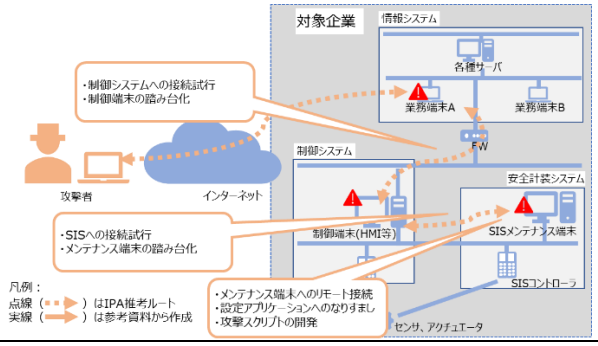
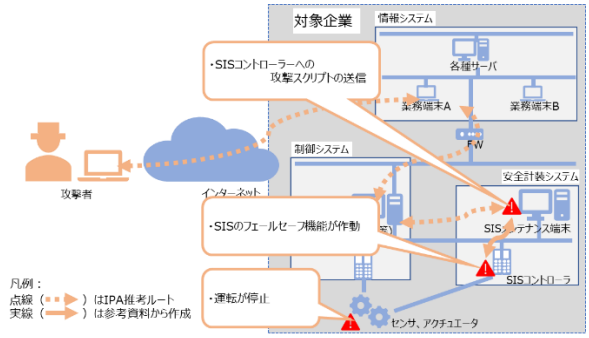
インシデント事例のサイバー攻撃要素の整理同様、対策・緩和策なども表 2-5 のように抜き出し、収集・整理することを心掛けていただきたい。

[5] [1-1] MITIGATIONS

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、SIS 環境への侵害が行われた【仮想の攻撃局面 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 2-6 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。

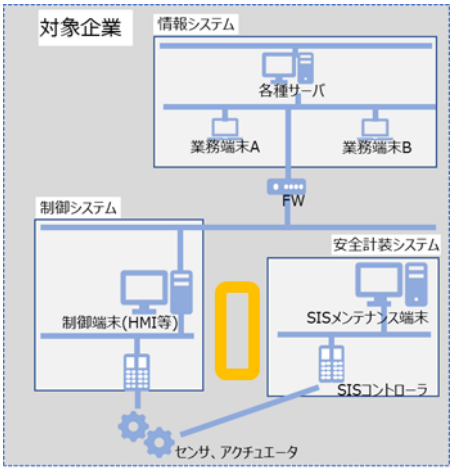
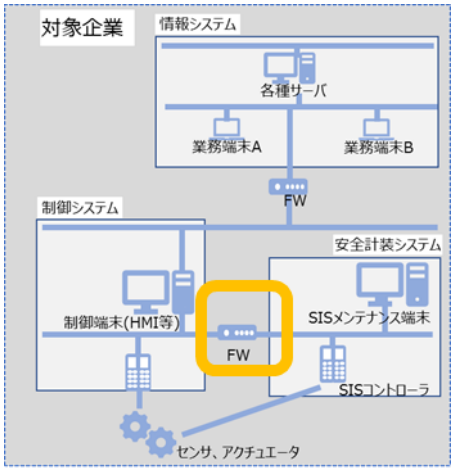
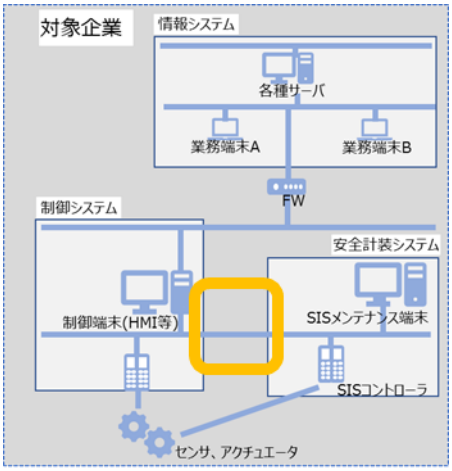
表 2-6 制御システムにおける攻撃ステップと対策・緩和策の紐づけ例

攻撃局面	攻撃ステップ[6]	対策・緩和策 [6]	対象システム・資産
【仮想の攻撃局面 A3】 	リモート接続[S4] [S5]	•SIS と他 NW の物理的な分離[D1] •メンテナンス端末やコントローラーの適切な管理・運用 [D4]	•安全計装システム •SIS メンテナンス端末
【攻撃局面 B】 	攻撃スクリプト送信[S7]	•プログラムモードへの設定変更管理 [D2] •メンテナンス端末やコントローラーの適切な管理・運用 [D4]	•SIS コントローラー

なお、SIS のシステム構成はいくつか考えられることから、その代表的な構成例と推奨レベル、また、それぞれにおける対策例を表 2-7 にまとめた。今後 SIS も含めセキュリティ対策・軽減策を検討する際の一例として活用いただきたい。

6 [S]は表 2-3 の項番と対応。 [D]は表 2-5 の項番と対応。

表 2-7　SIS のセキュリティを考慮した推奨構成と構成毎の対策例

<table>
<tr><th>構成</th><th>SIS が他 NW と分離</th><th colspan="2">SIS が他 NW と接続</th></tr>
<tr><th></th><th></th><th>境界防御　有</th><th>境界防御　無</th></tr>
<tr><th>推奨度</th><td>◎推奨構成</td><td>○次善構成</td><td>△検討が必要な構成</td></tr>
<tr><th>イメージ図</th><td> 
</td><td> 
</td><td> 
</td></tr>
<tr><th>対策・検討ポイント例</th><td>・外部記憶媒体の管理[D3]
・メンテナンス端末の管理[D4]
・入退室管理</td><td>・<u>NW 構成の見直し・切り離しの厳選[D1]</u>
・外部記憶媒体の管理[D3]
・メンテナンス端末の管理[D4]
・リモート接続の管理[D4]
・入退室管理</td><td>・<u>NW 構成の見直し・切り離しの厳選[D1]</u>
・<u>境界防御装置の導入検討[D1']</u>
・外部記憶媒体の管理[D3]
・メンテナンス端末の管理[D4]
・リモート接続の管理[D4]
・入退室管理</td></tr>
</table>

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. ICS-CERT

[1-1] MAR-17-352-01 HATMAN—SAFETY SYSTEM TARGETED MALWARE
https://ics-cert.us-cert.gov/sites/default/files/documents/MAR-17-352-01%20HatMan%E2%80%94Safety%20System%20Targeted%20Malware_S508C.pdf

2. 一般社団法人 JPCERT コーディネーションセンター

[2-1] 制御システムセキュリティの現在と展望
https://www.jpcert.or.jp/present/2018/ICS2018_02_JPCERTCC01.pdf

3. FireEye, Inc.

[3-1] 産業制御システム(ICS)への新たな攻撃フレームワーク「TRITON」が重要インフラの運用停止を誘発
https://www.fireeye.jp/blog/jp-threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html

[3-2] TRITON を利用する攻撃者の TTP、カスタム攻撃ツール、検出結果、ATT&CK マッピング
https://www.fireeye.jp/blog/jp-threat-research/2019/04/triton-actor-ttp-profile-custom-attack-tools-detections.html

更 新 履 歴

2019 年 7 月 31 日	初版	ー
2019 年 8 月 2 日	1.1 版	P12 表 2-7:構成[境界防御 有][境界防御 無]の接続イメージ図を正しい図に修正 その他:誤字修正
2021 年 10 月 18 日	1.2 版	P4 SIS の名称を Safety Instrumented System と IEC61511 に沿った名称に修正

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 3

～2017 年 安全計装システムを標的とするマルウェア～

[発　　行]　2019 年 7 月 31 日　第 1 版
2019 年 8 月 2 日　第 1.1 版
2021 年 10 月 18 日　第 1.2 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　小助川　重仁　山田　秀和
協力者　桑名　利幸　木下　弦　福原　聡　木下　仁