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2

～2016 年 ウクライナ マルウェアによる停電～

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。著名な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、2016 年 12 月にウクライナで発生したサイバー攻撃による停電事象と制御システムを標的としたマルウェアに関する米国 ICS-CERT などの公的機関の公開情報（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。

最新動向をキャッチアップし、リスクアセスメントの効率化を行いながら、自社にノウハウを残していく取組みのきっかけになることを期待している。

対象読者

制御システムのリスクアセスメント担当者

1. 2016 年 12 月 ウクライナ 電力施設へのサイバー攻撃による停電

1.1. インシデント概要

2016 年 12 月 17 日、ウクライナ（キエフ）で発生した電力会社へのサイバー攻撃は、マルウェアによって意図しないコマンド（ブレーカー遮断）が送信され、当該地域で最大 1 時間 15 分の停電が発生することとなった。

図 1-1 ウクライナにおけるインシデント発生地域

当該インシデントが発生する数日前から、同国のインフラ事業者へのサイバー攻撃が確認されていたという。また、2015 年のサイバー攻撃と同様の攻撃手法によって制御システム環境まで侵入したとみられているが、最終的な攻撃はマルウェアから直接制御システムへコマンドを送信することで、停電させたとされる。

本サイバー攻撃に使用されたマルウェアは CrashOverride（別名 Industroyer）と呼ばれる。バックドア、データ消去機能、特定製品に対しての DoS 攻撃機能、さらに、制御システム特有のプロトコルへの対応等が行われており、それぞれの機能がモジュール化されていたとする解析結果が公表されている

CrashOverride が対応する制御プロトコルは、「IEC 60870-5-101（IEC 101）」、「IEC 60870-5-104（IEC 104）」、「IEC 61850」、「OPC DA」の 4 種類となる。電力業界で使用されることが多いプロトコルが実装されており、2015 年のインシデント（参考情報[5-1]）から 1 年で攻撃者は、より高度な攻撃を容易に実行できる能力を保持したと考えられている。

本事例に関して、詳細なシステム構成情報は公開されていないが、攻撃の流れを理解する上で、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。

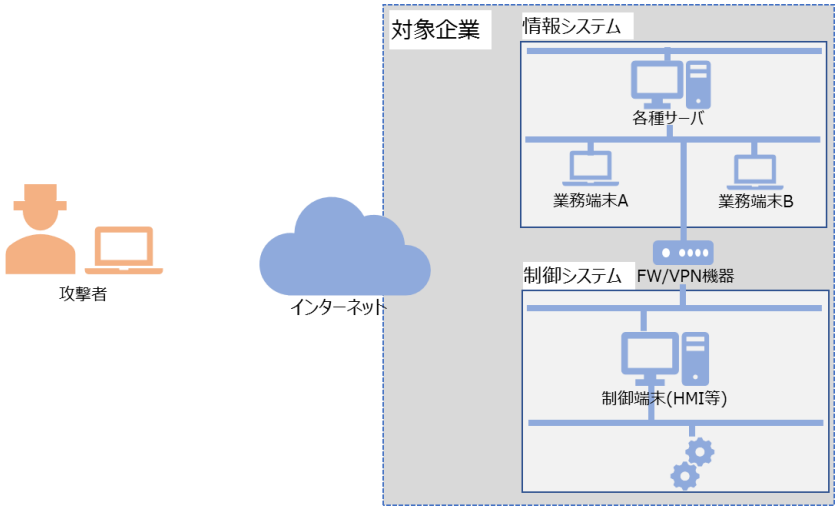


図 1-2　事例理解のための仮想システム構成図（実際のシステム構成とは異なる）

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 4 つの局面に分けて解説する。

1.2.1.　【攻撃局面 1】対象企業の情報収集とマルウェアへの感染誘導

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、標的型攻撃メールを送付し、業務端末のマルウェア感染を誘う[1]。

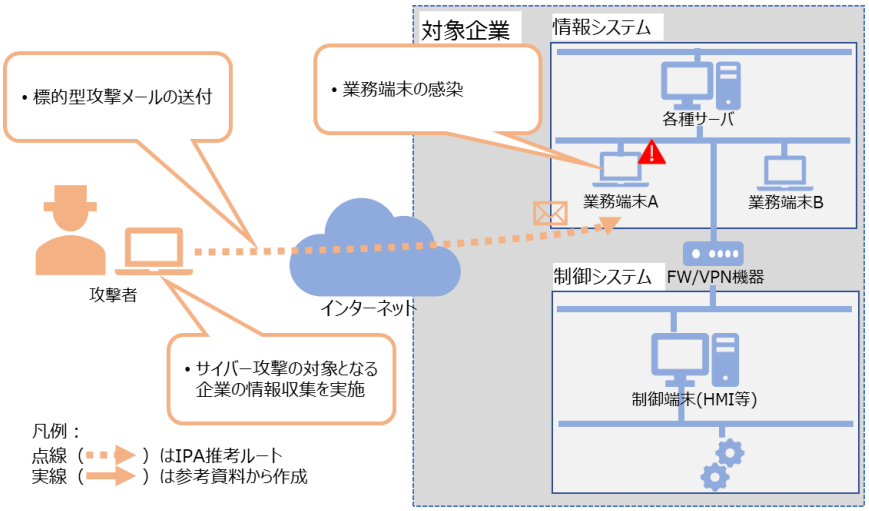


図 1-3　企業情報の収集とマルウェアへの感染誘導

[1] [4-1] ICS Cyber Kill Chain Mapping - Stage 1 参照

1.2.2. 【攻撃局面 2】活動範囲の拡大と情報収集

マルウェアに感染した業務端末を起点として、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[2]。

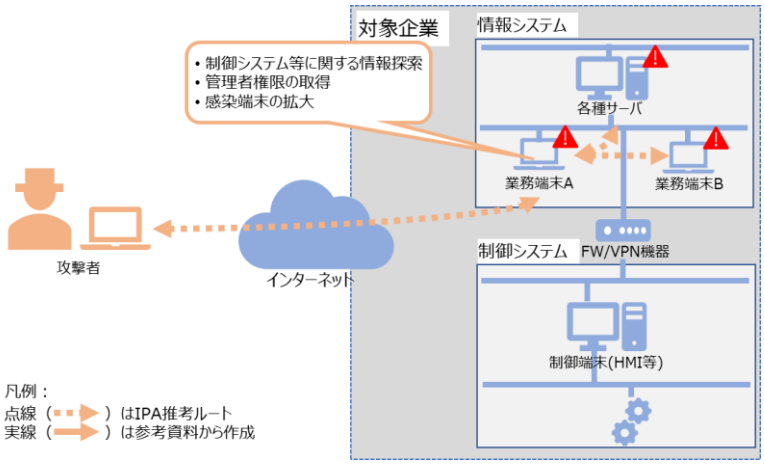


図 1-4 活動範囲の拡大と情報収集

1.2.3. 【攻撃局面 3】制御システム環境への侵入と感染・潜伏

何らかの方法で制御システムへの侵入を成功させる(図 1-5 では、制御システムへ接続可能な VPN 機器を経由して制御システムへ侵入したと仮定している。)。

制御端末(HMI 等)をマルウェアに感染させる。攻撃対象機器の情報を収集し、攻撃対象機器に合わせた攻撃プログラムを追加開発する。その後、マルウェアは攻撃実行の日時まで潜伏する[3]。

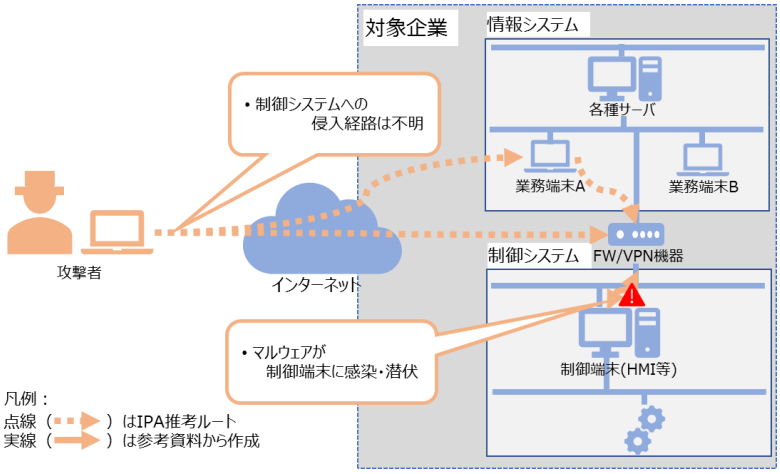


図 1-5 制御システム環境への侵入と感染・潜伏

[2] [4-1] ICS Cyber Kill Chain Mapping – Stage 1 参照
[3] [4-1] ICS Cyber Kill Chain Mapping – Stage 2 参照

1.2.4. 【攻撃局面 4】ブレーカー遮断コマンドの送信

指定された日時に、マルウェアは自動で起動し攻撃を開始する。その機器に対して、ブレーカーを開閉するコマンドを連続して送信することで停電を引き起こしたとされる[4]。

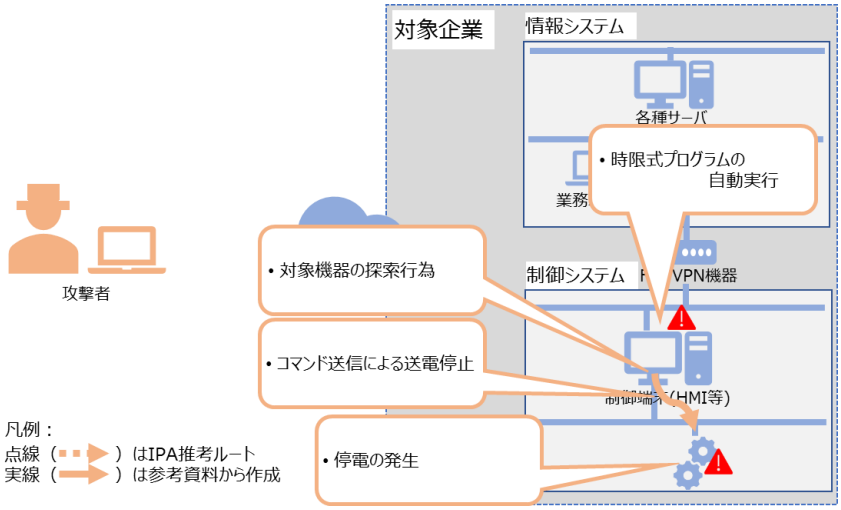


図 1-6 ブレーカー遮断コマンドの送信

[4] [1-1] Description、[2-1] Summary、[3-2] スライド 5-6 参照

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。また、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	制御機器（ブレーカー）への不正コマンド送信により停電が発生する。			
	攻撃シナリオ	攻撃拠点	攻撃対象	最終攻撃
	何らかの方法で制御システムへ不正侵入し、制御端末をマルウェアに感染させ、制御端末から制御機器（ブレーカー）へ不正コマンドを送信することで停電が発生する。	制御端末（HMI 等）	制御機器（ブレーカー）	制御機器（ブレーカー）への不正コマンド送信

また、事業被害に至る攻撃ルートの例を以下に示す。

表 2-2 攻撃ルートの例（下線はリスク分析をする上での想定）

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	*業務端末 A*	*（FW/VPN 機器）～制御端末*	制御端末（HMI 等）	制御機器（ブレーカー）	不正コマンド送信

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シナリオ・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 制御機器への不正コマンド送付による停電の発生の例

攻撃局面	項番	攻撃シナリオ 攻撃ツリー・ステップ ＜何らかの方法で制御システムへ不正侵入し、制御端末をマルウェアに感染させ、制御端末から制御機器（ブレーカー）へ不正コマンドを送信することで停電が発生する＞
【1】	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。
【1】	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。
【2】	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。
【3】	S4	収集した情報をもとに制御システムへリモート接続する。
【3】	S5	制御端末（HMI 等）をマルウェアに感染させ、攻撃の準備をする。
【4】	S6	時限式のプログラムが指定時間に起動し、制御ネットワークのスキャンを開始し、対象となる機器を探索する。
【4】	S7	対象制御機器（ブレーカー）にコマンド（ブレーカ遮断）を送信する。
【4】	S8	停電が発生する。

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、1.2.1 項～1.2.4 項で紹介した 4 つの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整理例

分析要素		内容（下線はリスク分析をする上での想定）
攻撃用途		
	侵入口	情報システムの業務端末 A
	攻撃対象	制御機器（ブレーカー）
	攻撃拠点	制御端末（HMI 等）
	経由	詳細は不明(*FW/VPN 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		停電
攻撃シナリオ		何らかの方法で制御システムへ不正侵入し、制御端末をマルウェアに感染させ、制御端末から制御機器（ブレーカー）へ不正コマンドを送信することで停電が発生させる。
最終攻撃（目的）		制御機器（ブレーカー）への不正コマンド送信（結果的に停電発生）
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 リモート接続 自動実行 スキャン(探索行為) 不正コマンドの送信

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。蓄積した情報は、攻撃シナリオの候補や攻撃ツリーを検討する際に有効であり、効率的に分析作業を進める上で必要な情報ともなる。

2.4. 対策・緩和策の整理

対策・緩和策の検討を進める上で、US-CERT から公表された TA17-163A[5]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おける緩和策を整理した。表 2-5 は、当該レポートに記載された緩和策をまとめたものとなる。

表 2-5 TA17-163A で紹介されている制御システム向け緩和策例

項番	対策・緩和策
D1	アプリケーションホワイトリスティングの導入
D2	認証や認可に関する仕組みの導入
D3	破壊的マルウェアへの対応
D4	適切な設定・パッチマネジメントの実施
D5	多層防御環境の構築
D6	セキュアなリモート接続の実装
D7	監視と対応

「D3. 破壊的マルウェアへの対応」は、仮にデータを消去するなどのマルウェアに感染した場合の迅速な復旧を目指す上で、事前にその方針や準備が必要であるという事であり、「D4. 適切な設定・パッチマネジメントの実施」は、現在の設定が適切であるのかの確認、また、脆弱性への対応方針などを決めることが必要となる。

制御システム環境におけるセキュリティ機能の実装（項番 D1、D2、D6）は、多層防御の観点からも必要であり、その他の項番も含め、方針やルール、運用フローの見直しなどバランスよく取り組み「D7. 監視と対応」ができる環境を構築していくことが肝要となる。

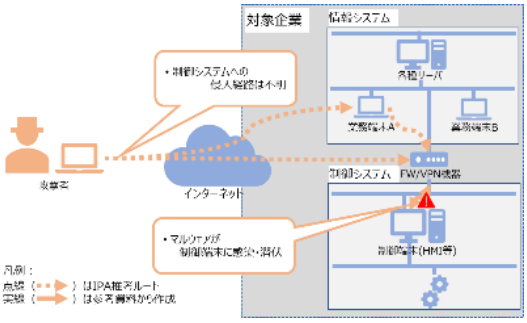
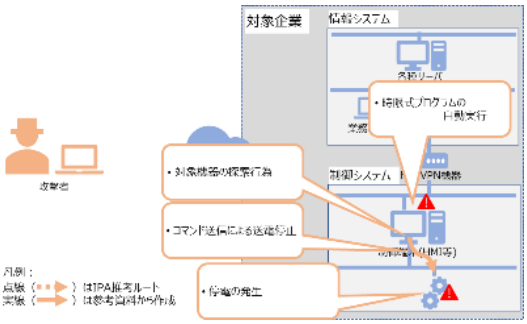
分析ガイドでは、表 2-5 以外にもセキュリティ対策として技術的対策候補の一覧が整理されている。対策状況の分析を進める上でも、技術面、管理面からの網羅的な分析・対策の検討を心掛けていただきたい。

[5] [1-1] Solution

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、制御システムへの侵害が行われた【攻撃局面 3】や【攻撃局面 4】と表 2-5 の代表的な対策・緩和策を紐づけた例が表 2-6 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
【攻撃局面 3】 	リモート接続 [S4]	• セキュアなリモート接続の実装 [D6] • 認証・認可に関する仕組みの導入 [D2]	• NW 機器 • 制御端末
	マルウェアへの感染 [S5]	• 適切な設定・パッチマネジメントの実施 [D4]	• 制御端末
【攻撃局面 4】 	時限式プログラムの起動 [S6]	• アプリケーションホワイトリスティングの導入 [D1]	• 制御端末
	スキャン探索行為 [S6]	• 監視や対応(ネットワーク監視) [D7]	• 制御 NW
	不正コマンドの送信 [S7]	• 監視や対応(ネットワーク監視) [D7]	• 制御 NW

実際の分析作業において、対策・緩和策を検討する場合には、表 2-6 を参考に、セキュリティ対策の基本である「多層防御」を考慮し、立案することを心掛けていただきたい。

[6] [S]は表 2-3 の項番と対応。 [D]は表 2-5 の項番と対応。

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. US-CERT

[1-1] TA17-163A CrashOverride Malware

https://www.us-cert.gov/ncas/alerts/TA17-163A

2. ICS-CERT

[2-1] ICS-ALERT-17-206-01 CRASHOVERRIDE Malware

https://ics-cert.us-cert.gov/alerts/ICS-ALERT-17-206-01

3. 一般社団法人 JPCERT コーディネーションセンター

[3-1] 制御システムセキュリティの現在と展望 2017

https://www.jpcert.or.jp/present/2017/20170221_CSC-JPCERTCC01.pdf

[3-2] 制御システムセキュリティの現在と展望　～この一年を振り返って～

https://www.jpcert.or.jp/present/2018/ICS2018_02_JPCERTCC01.pdf

4. SANS Institute

[4-1] ICS Defense Use Case No. 6: Modular ICS Malware

https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_6.pdf

5. 独立行政法人　情報処理推進機構

[5-1] 制御システム関連のサイバーインシデント事例 1　～2015 年ウクライナでの大規模停電～

https://www.ipa.go.jp/security/controlsystem/incident.html

更 新 履 歴

2019年7月31日	初版	ー
2019年8月2日	1.1版	P8~P10：攻撃対象を制御機器（ブレーカー）に変更 その他：誤字修正

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 2

～2016 年 ウクライナ マルウェアによる停電～

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