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1

～2015 年 ウクライナ 大規模停電～

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。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、2015 年 12 月にウクライナで発生した大規模停電に関する米国 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. 2015 年 12 月 ウクライナで発生した大規模停電

1.1. インシデント概要

2015 年 12 月 23 日、ウクライナ（イバノフランコフスク、チェルノフツィ、キエフ）で発生した電力会社へのサイバー攻撃は、様々な要因が重なった結果、大規模停電を引き起こしたとされる。発生から復旧までに最大で 6 時間を要し、22 万 5 千人の顧客に影響を与えた。

図 1-1 ウクライナにおけるインシデント発生地域

攻撃者は、対象となる企業のシステムやネットワークを 6 ヵ月以上前から入念に調査した上で、サイバー攻撃を計画していたのではないかとされている。最終攻撃に向けた段階で、対象企業のアカウント情報（ID やパスワード）を入手していたと考えられており、VPN による接続やリモート管理ツールの使用など正規の通信経路をたどり、リモートから制御システム環境へ接続していたと想定されている。

サイバー攻撃は 30 分以内に複数箇所で実行されたとみられ、同時多発的な攻撃とそれによる複合的な被害の発生を意図していたのではないかともいわれている。最終的に、それら諸条件が整った結果、大規模な停電が引き起こされた。

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。

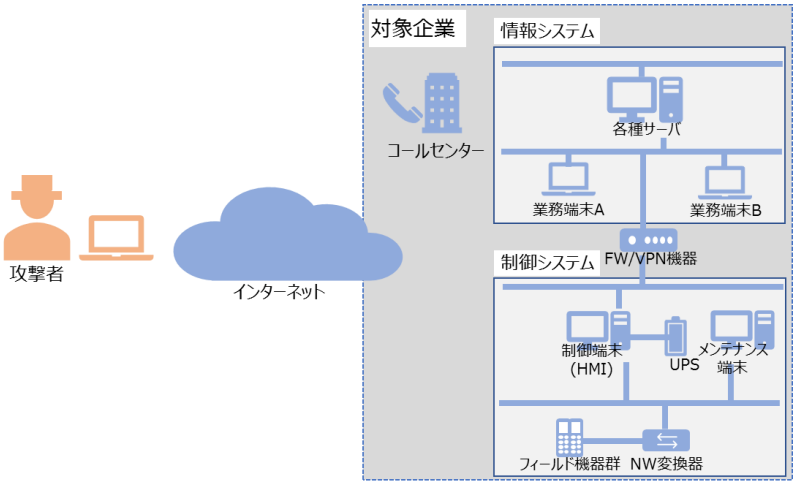


図 1-2　事例理解のための仮想システム構成図（実際のシステム構成とは異なる）

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 5 つの局面に分けて解説する。

1.2.1.　【攻撃局面 1】攻撃に向けての情報収集

サイバー攻撃を実行する前に、標的となった企業に関する情報（組織・人・システム）や取引先企業の情報など様々な情報収集を実施する[1]。

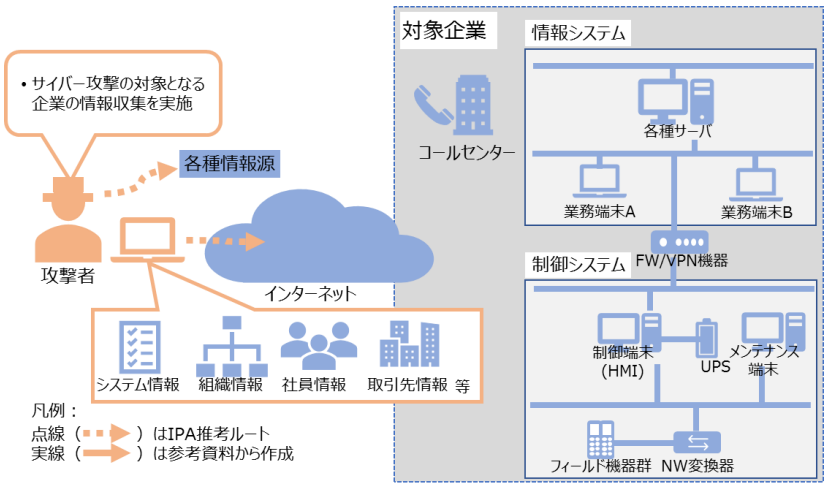


図 1-3【攻撃局面 1】攻撃に向けての情報収集

[1] [2-2] スライド 5、[3-1] pp.4-5 参照

1.2.2. 【攻撃局面 2】マルウェアへの感染誘導

インターネット等で収集した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 A のマルウェア感染を誘う[2]。

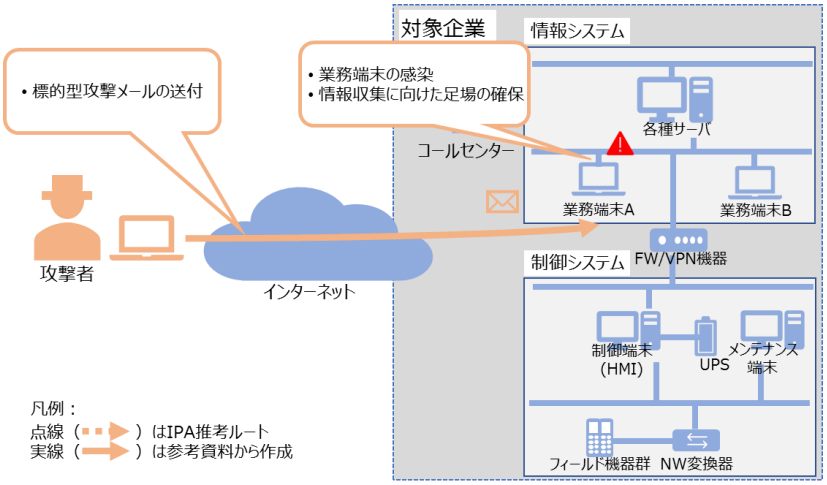


図 1-4 【攻撃局面 2】マルウェアへの感染誘導

1.2.3. 【攻撃局面 3】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 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・収集を行い、制御システムへのリモート接続の正規認証情報やシステム構成が取得されたと推測される。[3]

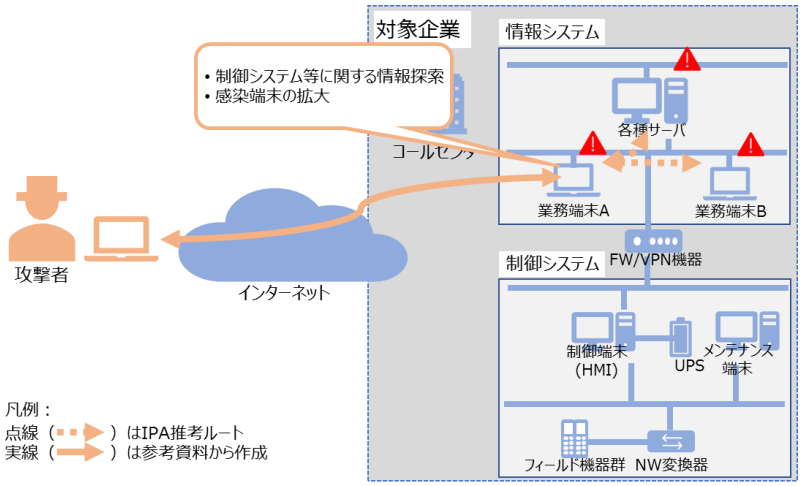


図 1-5 【攻撃局面 3】活動範囲の拡大と情報収集

[2] [1-1] Details、[2-2] スライド 5-6、[3-1] pp.1-6 参照
[3] [1-1] Details、[2-2] スライド 5-6、[3-1] pp.1-6 参照

1.2.4. 【攻撃局面 4】制御システム環境への侵入

情報システム上で入手した正規アカウント情報やシステム構成などをもとに、VPN 経由で制御システムへの侵入を試み、制御端末（HMI 等）からシステム環境の把握をしながら攻撃実行に向けた準備を整える[4]。

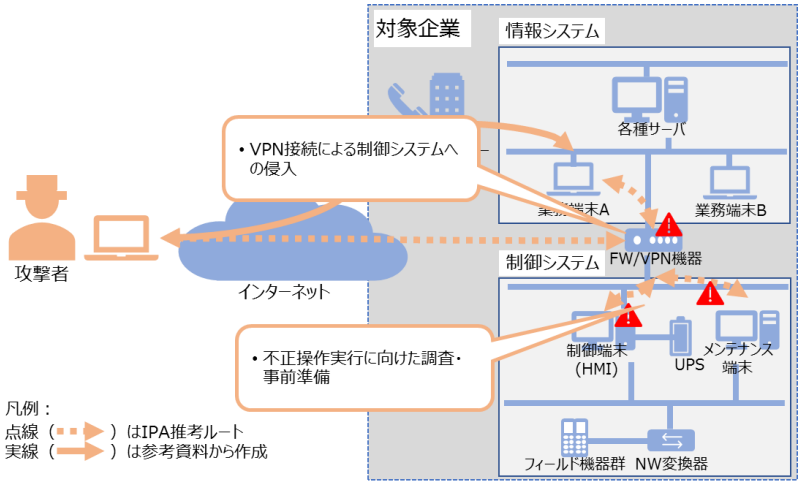


図 1-6 【攻撃局面 4】制御システム環境への侵入

1.2.5. 【攻撃局面 5】安定稼働の阻害と非定常状態の引き延ばし

攻撃に向けた準備が整った段階で、制御システム内の制御端末（HMI）を不正に操作し、停電を発生させた。

また、UPS（無停電電源装置）の管理画面から設定変更の試行、フィールド機器のファームウェア改ざん、さらに、マルウェア「KillDisk[5]」による制御端末（HMI 等）のシステム破壊などを行ったとされる。その結果として、大規模な停電が発生したと考えられる。なお、同時にコールセンターに対するサービス妨害攻撃(T-DOS)も行われていたという[6]。

[4] [1-1] Details、[2-2] スライド 5、[3-1] pp.1-2, p.8 参照
[5] KillDisk は、システム上で指定したファイルの削除などが可能であり、MBR（Master Boot Record）を破損させ、システムを動作不能とする。
[6] [1-1] Details、[2-1] スライド 6、[2-2] スライド 5-6、[3-1] pp.1-2, pp.7-10 参照

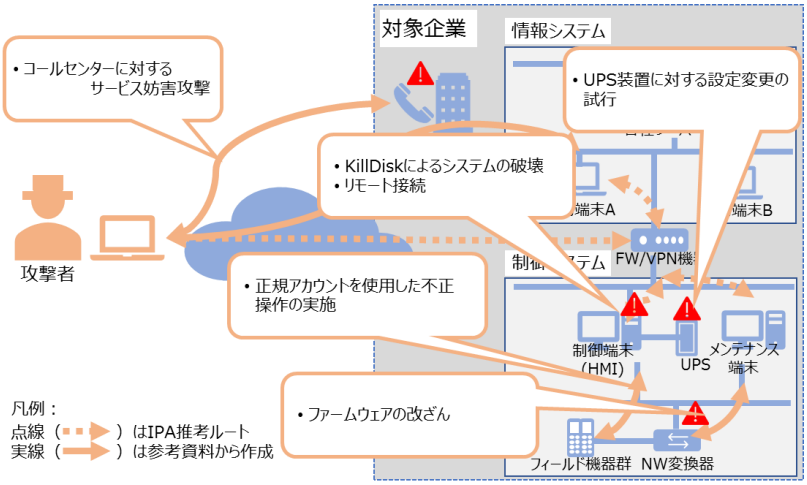


図 1-7 【攻撃局面 5】不正操作と非定常状態の引き延ばし

攻撃者は、複数の手段を用いて同時にサイバー攻撃を実行していた。結果的に、当該システムの不正操作による安定稼働の阻害とそれによる非定常状態が続くこととなった。

なお、本事例においてマルウェア「Black Energy 3」の使用が取り上げられているレポートも存在するが、停電発生に直接影響を与えたか否か詳細は不明であり、本資料における【攻撃局面 2】や【攻撃局面 3】で使用されたのではないかとも考えられている。

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 事業被害と攻撃シナリオの例

事業被害	1: 制御機器の不正操作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
1	制御端末にリモート接続し、制御機器へ停電を発生させる不正操作を行う	制御端末（HMI 等）	制御機器	不正操作（停止）
事業被害	2: 停電時に制御システムに不具合が発生し、状況把握の妨害・システム復旧の遅延が起きる			
#	攻撃シナリオ	攻撃拠点	攻撃対象	最終攻撃
2-1	制御端末がマルウェア感染し利用不能となり、状況把握の妨害・システム復旧の遅延が起きる	制御端末（HMI 等）	制御端末（HMI 等）	マルウェア感染（KillDisk 実行）
#	攻撃シナリオ	攻撃拠点	攻撃対象	最終攻撃
2-2	ネットワーク変換器のファームウェア書き換えによって、正常に機能しなくなり、状況把握の妨害、システム復旧の妨害・遅延が起こる	制御端末（HMI 等）	ネットワーク変換器	ファームウェア変更
#	攻撃シナリオ	攻撃拠点	攻撃対象	最終攻撃
2-3	UPS 装置が不正に設定変更され、停電時に制御機器が動作せず、状況把握の妨害・システム復旧の遅延が起きる	制御端末（HMI 等）	UPS 装置	設定変更
事業被害	3: 停電時にコールセンターがサービス妨害攻撃を受け、状況把握の妨害が起こる			
#	攻撃シナリオ	攻撃拠点	攻撃対象	最終攻撃
3	インシデント発生中に、コールセンターに対してサービス妨害攻撃、コールセンターが機能しなくなる	電話端末	コールセンター	T-DOS

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）

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*	*業務端末 A*	*FW/VPN 機器 ～ 制御端末*	制御端末（HMI 等）	制御機器	不正操作（停止）
2-1	*悪意のある外部の第三者*	*FW/VPN 機器*	*制御端末*	制御端末（HMI 等）	制御端末（HMI 等）	マルウェア感染（KillDisk 実行）
2-2	*悪意のある外部の第三者*	*FW/VPN 機器*	*制御端末*	制御端末（HMI 等）	ネットワーク変換器	ファームウェア変更
2-3	*悪意のある外部の第三者*	*FW/VPN 機器*	*制御端末*	制御端末（HMI 等）	UPS 装置	設定変更
3	*悪意のある外部の第三者*	電話回線	—	電話端末	コールセンター	T-DOS

2.2. 攻撃ツリーの作成

2.1 節で整理した情報をもとに、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～表 2-7 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 制御機器の不正操作による停電発生

攻撃局面	項番	攻撃シナリオ	攻撃ツリー・ステップ
		1	＜制御端末にリモート接続し、制御機器へ停電を発生させる不正操作を行う＞
【1】	S1-1		侵入口=業務端末 A 攻撃者が標的型攻撃メール（フィッシングメール）を送信する。
【1】	S1-2		業務端末 A で、当該メールを開封する。C&C サーバとの通信が確立する。
【2】	S1-3		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する情報を収集する。
【3】	S1-4		収集した情報をもとに制御システムへ VPN 経由で接続する。
【4】	S1-5		制御端末（HMI 等）に接続し、情報収集や攻撃に向けた準備をする。
【5】	S1-6		制御機器へ停電を発生させる不正操作を行う（安定稼働を阻害し、非定常状態を引き起こす）。

表 2-4　KillDisk を用いたシステム破壊の例

攻撃局面	項番	攻撃シナリオ	
			攻撃ツリー・ステップ
		2-1	＜制御端末がマルウェア感染し利用不能となり、状況把握の妨害・システム復旧の遅延が起きる＞
【3】	S2-1-1		侵入口=FW/VPN 機器 表 2-3　項番 S1-3 で収集した情報をもとに制御システムへ接続する。
【4】	S2-1-2		制御端末（HMI 等）上で KillDisk 実行の準備をする。
【5】	S2-1-3		KillDisk が実行され、システムが破壊され、状況の把握ができなくなったり、システム復旧に時間がかかったりする。

表 2-5　NW 変換器のファームウェア書き換えの例

攻撃局面	項番	攻撃シナリオ	
			攻撃ツリー・ステップ
		2-2	＜ネットワーク変換器のファームウェア書き換えによって、正常に機能しなくなり、状況把握の妨害、システム復旧の妨害・遅延が起こる>
【3】	S2-2-1		侵入口=FW/VPN 機器 表 2-3　項番 S1-3 で収集した情報をもとに制御システムへ接続する。
【4】	S2-2-2		メンテナンス端末上で、NW 変換器のファームウェア書き換えに向けた準備をする。
【5】	S2-2-3		NW 変換器に対してファームウェアの書き換えを行う。
【5】	S2-2-4		NW 変換器が正常に機能しなくなったり、システムの復旧に時間がかかったりする。

表 2-6　UPS 装置の設定変更の例

攻撃局面	項番	攻撃シナリオ	
			攻撃ツリー・ステップ
		2-3	＜UPS 装置が不正に設定変更され、停電時に制御機器が動作せず、状況把握の妨害・システム復旧の遅延が起きる>
【3】	S2-3-1		侵入口=FW/VPN 機器 表 2-3 項番 S1-3 で収集した情報をもとに制御システムへ接続する。
【4】	S2-3-2		制御端末（HMI 等）から UPS のリモート管理画面にアクセスする。
【5】	S2-3-3		リモート管理画面から UPS 装置の設定を変更する。
【5】	S2-3-4		UPS が意図した動作をしなくなる。

表 2-7　コールセンターに対するサービス妨害攻撃の例

攻撃局面	項番	攻撃シナリオ	
			攻撃ツリー・ステップ
		3	＜インシデント発生中に、コールセンターに対してサービス妨害攻撃、コールセンターが機能しなくなる>
【1】 【3】	S3-1		侵入口=なし（電話回線） コールセンターに対してサービス妨害攻撃（T-DOS）を行う。
【5】	S3-2		コールセンターが機能しなくなり、顧客からの問い合わせに対応できなくなる。

2.3. 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 ICS-CERT から公表された IR-Alert-H-16-056-01[7]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 2-8 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 2-8 IR-Alert-H-16-056-01 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	信頼できるハードウェアやソフトウェアの調達やライセンシング
D2	戦略的な技術刷新
D3	緊急時対応計画の策定
D4	ハードウェアとソフトウェアの自動的な資産管理
D5	ネットワークセグメンテーションの実施
D6	リモートアクセスの制限
D7	アプリケーションホワイトリスティングの導入
D8	不使用のポートやサービスの無効化
D9	多要素認証の導入
D10	脆弱性管理
D11	システムへの適切なパッチ適用

「D2. 戦略的な技術革新」や「D3. 緊急時対応計画の策定」は、事業レベルでの検討が必要な項目であり、「D1. 信頼できるハードウェアやソフトウェアの調達やライセンシング」や「D4. ハードウェアとソフトウェアの自動的な資産管理」、「D10. 脆弱性管理」などは、管理施策として整理できる。

分析ガイドでは、セキュリティ対策として主に技術的対策候補の一覧が整理されているが、対策状況の分析を進める上では、組織体制やルールといった観点での対策状況も加味しながら分析作業を進めることでより網羅的な分析・対策の検討につながる。

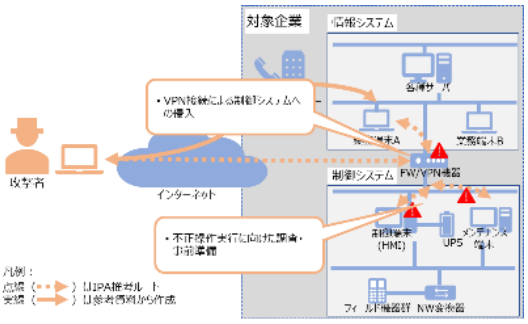
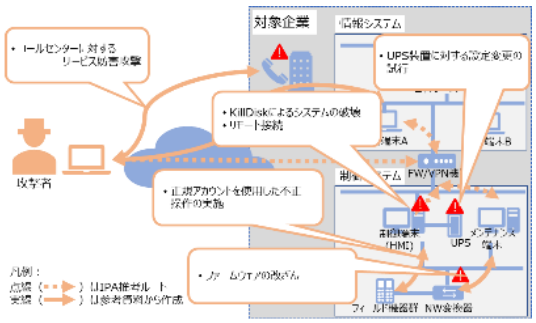
インシデント事例は、対策・緩和策などの情報も表 2-8 のように抜き出し、収集して整理・蓄積することを心掛けていただきたい。

[7] [1-1] MITIGATION

2.4. 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、制御システムへの侵害が行われた【攻撃局面 4】や【攻撃局面 5】と表 2-8 の代表的な対策・緩和策を紐づけた例が表 2-9 となる。

表 2-9 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[8]	対策・緩和策[8]	対象システム・資産
【攻撃局面 4】  	VPN 経由のリモート接続 [S1-4]	•ネットワークセグメンテーションの実施[D5][9] •リモート接続の制限[D6] •不使用のポートやサービスの無効化[D8] •多要素認証の導入[D9] •緊急時対応計画の策定[D3]	•制御システム •制御端末(HMI 等)
【攻撃局面 5】  	不正操作 [S1-6]	•多要素認証の導入[D9]	•制御端末(HMI 等)
	KillDisk の実行 [S2-1-3]	•アプリケーションホワイトリスティングの導入[D7]	•制御端末(HMI 等)
	ファームウェア書き換え [S2-2-3]	•信頼できる HW や SW の調達やライセンシング [D1] •多要素認証の導入[D9] •適切なパッチの適用 [D11]	•メンテナンス端末 •NW 変換器
	設定変更 [S2-3-3]	•多要素認証の導入[D9]	•制御端末
	サービス妨害攻撃 [S3-1]	•緊急時対応計画の策定[D3]	•コールセンター

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 2-9 を参考とし、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。

8 [S…]は表 2-3～表 2-7 の項番と対応。 [D・]は表 2-9 の項番と対応。

9 例えば、VPN に接続できる端末は情報システムと隔離された企業内端末に限定。

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] IR-ALERT-H-16-056-01：Cyber-Attack Against Ukrainian Critical Infrastructure
https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01

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 2016
http://www.jpcert.or.jp/present/2016/20160217_CSC-JPCERT01.pdf

[2-2] 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. SANS Institute

[3-1] Analysis of the Cyber Attack on the Ukrainian Power Grid
https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

更 新 履 歴

2019年7月31日	初版	ー
2019 年 8 月 2 日	1.1 版	P4:図 1-1 図中の誤記を修正 P11:表 2-3 項番 S1-6 攻撃ステップの記載内容を修正 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 1

～2015 年 ウクライナ 大規模停電～

[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