2018 年 3 月 30 日
独立行政法人情報処理推進機構（IPA）

欧州ネットワーク情報セキュリティ機関（ENISA）「ICS／SCADA システムの通信ネットワークとセキュリティ」概要

本概要は、欧州ネットワーク情報セキュリティ機関（ENISA）発行の以下文書の概訳となります。
内容の詳細につきましては、原文をご確認ください。

Communications network dependencies for ICS/SCADA Systems
https://www.enisa.europa.eu/publications/ics-scada-dependencies

長距離通信ネットワーク、とりわけインターネットは、産業制御システム（ICS）／遠隔監視制御（SCADA）システムに変革をもたらし、リモートやリアルタイムでの運用保守に有効な手段を提供した。しかし同時に、ネットワーク化は ICS／SCADA システムに新たな脅威ももたらすことになった。

とはいえ、ネットワーク脅威は IT 分野では長く取り組まれてきた既知の脅威であり、利用可能な対策も存在している。本ガイドは、特に ICS／SCADA システム及び機器をつなぐネットワークに着目し、重要な資産、脅威、攻撃シナリオ、適用可能なグッドプラクティスを知見として示すことにより、ICS／SCADA システムに対するサイバー攻撃のリスク緩和を支援することを目的としている。

本概要では、同ガイドのうち以下の項目の概略を日本語で紹介している（【】内はガイド中の該当する章・節番号）。

- 対象読者【1.3】
- モデルとするアーキテクチャ【2.1】
- ICS／SCADA システムの相互依存性【3】
- 脅威と脆弱性【4.1、4.2】
- 攻撃シナリオ【5.1】
- 対策（グッドプラクティス）【7.9】
- 提言【8.1】

以降に、同ガイドの概要を記す。

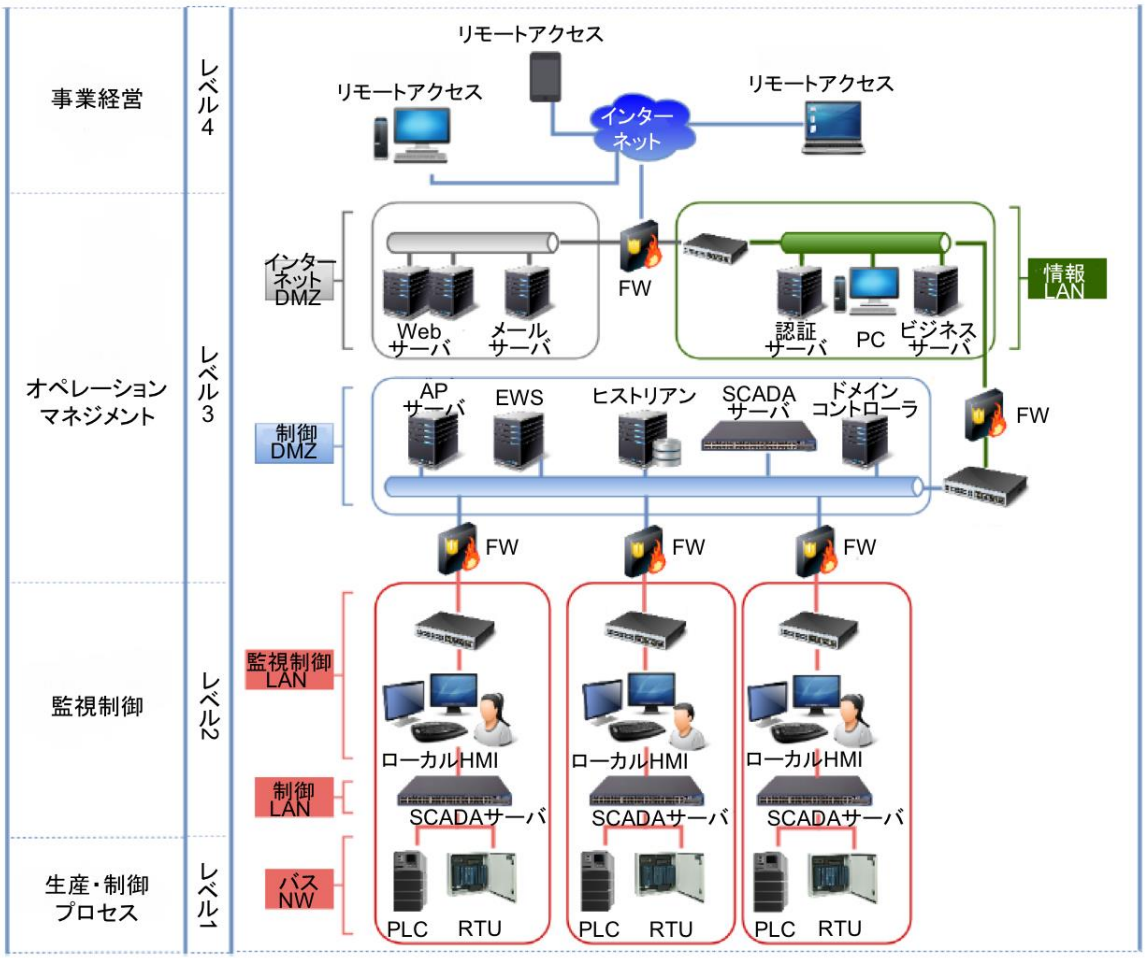
対象読者【1.3】

本ガイドは、主に以下の分野の ICS／SCADA システム運用事業者を対象としている。

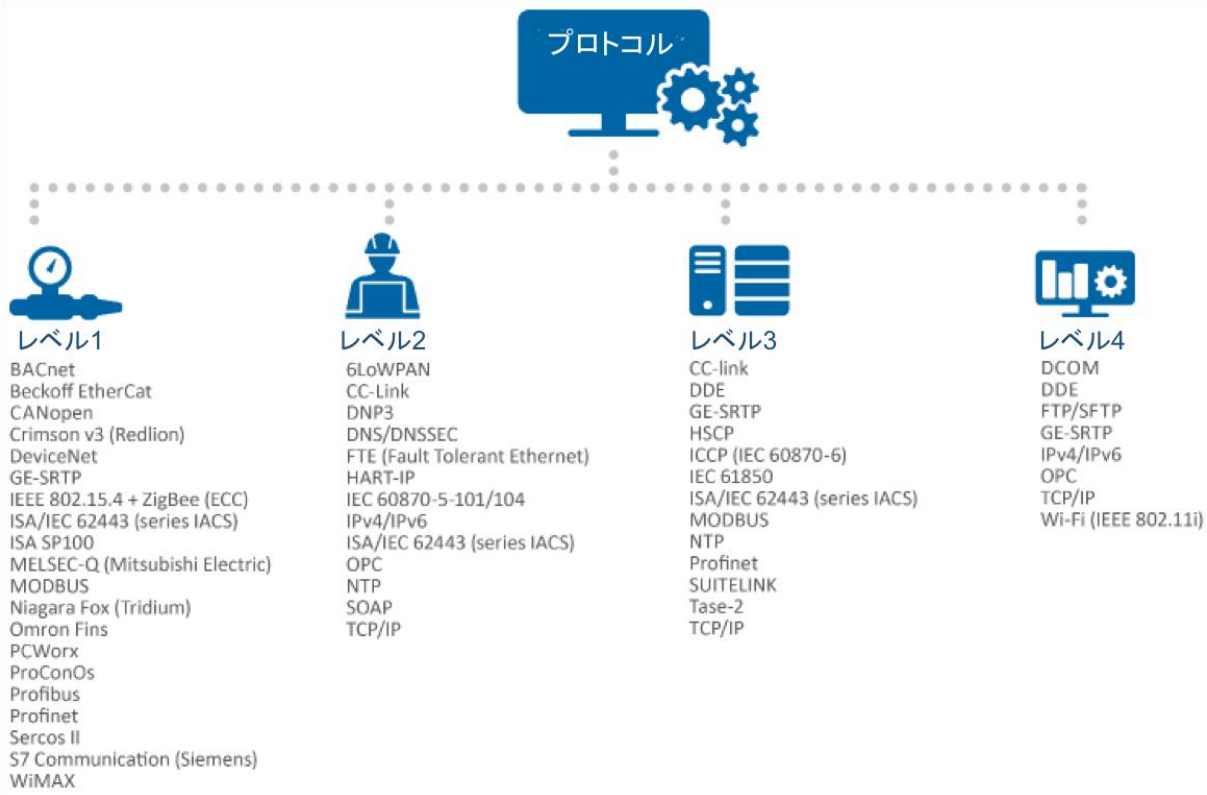
- 電力
- 石油
- ガス
- 輸送
- ヘルスケア
- 水道
- 製造
- 製薬

モデルとするアーキテクチャ【2.1】

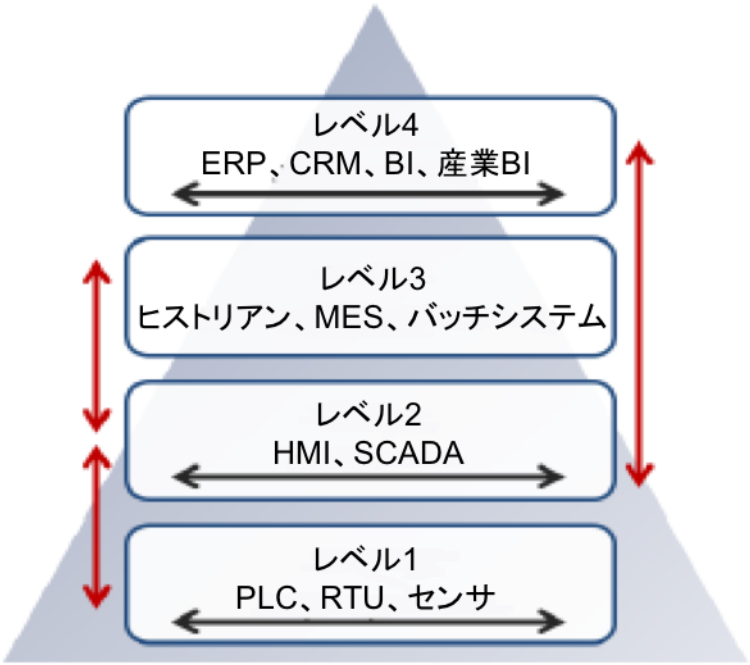
本ガイドでは、検討にあたっての ICS／SCADA システムとネットワークの階層モデルとして、ISA95 を用いる。図 2 に ISA95 レベルの ICS／SCADA アーキテクチャへの適用例を、図 3 に各レベルでやり取りされる通信プロトコルを、図 4 に各レベル内及びレベル間で想定される通信を示す。



（原文）Figure 2： ISA95 レベルの ICS／SCADA アーキテクチャへの適用



（原文）Figure 3：プロトコル



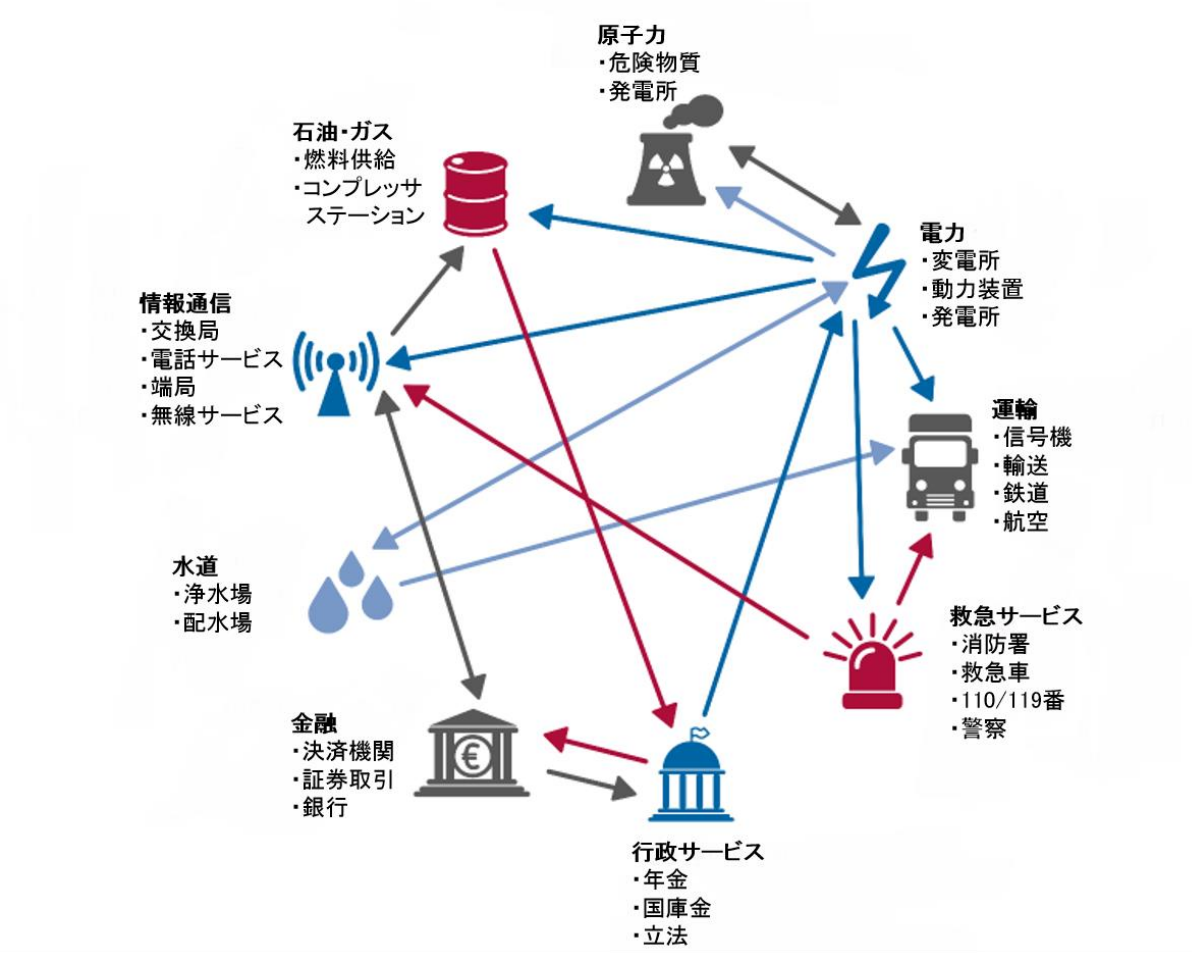
（原文）Figure 4：レベル内／レベル間の通信

ICS／SCADA システムの相互依存性【3】

ICS／SCADA システムの依存性は、4 つに大別される。

- 物理的：あるインフラが、別のインフラの物理的生産物を必要とするケース（e.g. あるインフラの物理的アプトプットが、別のインフラの物理的インプットとなっている）
- 地理的：あるインフラの運用が、その場所の環境的事象に影響を受けるケース
- サイバー：あるインフラの運用が、情報通信インフラによってもたらされる情報によって決まるケース（e.g. 消費者の電力使用量に応じた発電量の調整）
- 論理的：あるインフラの運用が、別のインフラの運用に物理、地理、サイバー以外の要因によって影響を受けるケース（e.g. 意思決定プロセス等の人的要因）

図 5 に、重要インフラ間の主な依存関係を図示する。電力は他インフラによる依存性が高く、最も重要なインフラの 1 つとなっている。



（原文）Figure 5：重要インフラの相互依存性

脅威と脆弱性【4.1、4.2】

4 章では、ICS／SCADA システム（ネットワーク）のセキュリティに影響を及ぼす脅威及び脆弱性を洗い出している。表 1 には主な脅威、及びその発生可能性と影響度を、表 2 には脆弱性（運用上のものを含む）をまとめている。

（原文）Table 1： ICS／SCADA システムに影響を及ぼす可能性のある脅威

	脅威	発生可能性	影響度
1	標的型攻撃（APT）	低	高
2	マルウェア（ウィルス、トロイの木馬、ワーム）	非常に高い	高
3	攻撃ツール、ルートキット	中	高
4	内部脅威	低	高／致命的
5	通信システム（ネットワーク）障害	低	高／致命的
6	盗聴（中間者攻撃、通信のハイジャック）	低	致命的
7	サービス運用妨害（DDoS）	低	中／高
8	データ／機微な情報の漏洩	低	中／高

（原文）Table 2： 脆弱性（1／2）

脆弱性	説明
モニタリングの欠如	ネットワークを積極的に監視しない限り、不審な活動や潜在的な脅威を検知し、迅速に対策を行うことは難しい。とはいえ、侵入検知システム（IDS）を導入しても、ICS プロトコルに十分対応していないという問題もある。この問題は、異常検知システムによって多少カバーできる可能性がある。
通信内容の理解不足	マネージャは、どの通信を許可し、どの通信が不審かフィルタリングするために、どのようなトラフィックがどう流れているか、把握している必要がある。
関係者のセキュリティ経験不足	SCADA システムのスタッフやオペレータは、システムの信頼性と可用性を維持することに慣れており、セキュリティのために行う行為はこれらの維持に反するように思えたり、IT スタッフの言うこと受け入れ難いと感じたりする可能性がある。
OS の脆弱性	IT システム同様、SCADA システムにも脆弱性が存在する。しかし、SCADA システムは IT システムと比べて修正プログラムが適用されにくい。
アップデートの遅延／欠如	ICS/SCADA システムに十分なテストや影響の検討なしに「変更」を加えることはできないため、ICS/SCADA ソフトウェアを常に最新の状態にするというのは難しい。
リモートプロセッサ	リモートプロセッサには既知の脆弱性が確認されているものもあるが、処理能力とメモリ容量が小さくアップグレードが困難なため、また、機器が設置されたら 10 年かそれ以上は更新されないため、脆弱なまま長期間そのままとなる。
SCADA ソフトウェアの セキュリティ機能の非利用	SCADA アプリケーションとソフトウェアは通常それなりのセキュリティ機能を有している。しかし、セキュリティ機能がデフォルトで有効になっていることは少なく、また、オペレータがその存在を知らず、利用されないことも多い。

（原文）Table 2： 脆弱性（2／2）

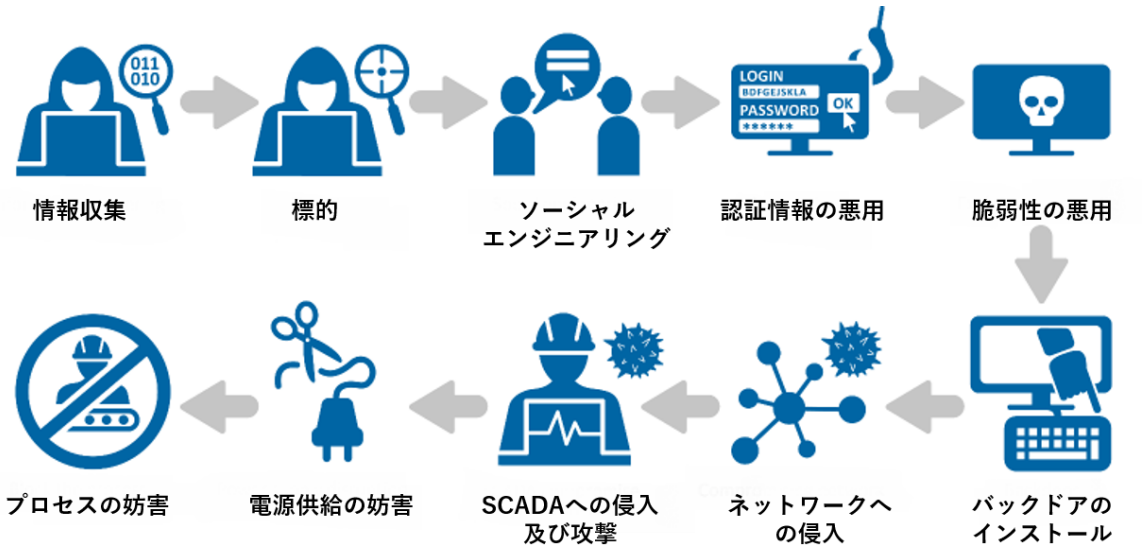
脆弱性	説明
重要な SCADA コンピュータへの 不適切なアプリケーションのインストール	SCADA のホストコンピュータにセキュリティ対策は殆どされないため、オペレータやシステム管理者が誤って不適切なソフトウェアをインストールしてしまうことがある。
SCADA 機器に関する知識不足	多くの SCADA システムは長い期間を掛けて徐々に発展してきたため、古い機器（技術）が使われていることも珍しくない。古い機器の維持管理のための知識の引き継ぎが重要となる。
認証の弱さ	認証は、適切に実装されなければ意味がない（認証なし、弱いパスワードの使用、パスワードのハードコード、認証情報の共有等）。古い機器には不適切な認証機能しかなかったり、生体認証や多要素認証が運用上難しい場合もある。
PLC/RTU のネットワーク通信の 認証の欠如	古い SCADA システムには基本的なセキュリティ機能がない機器がある。
リモートアクセスの管理	人員配置や運用の効率上、SCADA システムに対するリモートアクセスを認めているケースも珍しくない。その場合、リモートアクセスを制御・監視し、最低でも内部接続同様のセキュリティ対策を行うことが望ましい。
他ネットワークとの接続管理	SCADAシステムの外部ネットワークとの接続が増えれば増えるほど、リスクも増す。効率化を求める上からの圧力で情報ネットワークと接続するケースも多い。
ワイヤレス接続	SCADA システムではマイクロ波、無線、携帯網等も通信に利用している。実装によって、これらの通信の脆弱性が狙われることもある。
情報の公開	事業者が自社の SCADA システムに関する情報を公開しているケースや、コンサルティング会社やベンダが自社の導入事例として、顧客のシステムに関する情報を公開しているケースがあり、これらの情報が悪用されることがある。
情報を出さないことによりセキュリティが守れる（security through obscurity）という誤った思い込み	独自プロトコルを利用しているから安全とは限らない。「情報を出さないことでセキュリティを守る」というのはセキュリティ的に良い考え方とは言えず、誤った安心感につながる。
SCADA システムは外部ネットワークとつながっていないから安全という誤った思い込み	SCADA システムがインターネットにつながっていないから安全とは限らない。全てのネットワーク接続点を監視・制御するとともに、メンテナンスのため外部ネットワークにつながっている機器やリモートアクセスを許可している機器のネットワーク接続は必要な時の有効とすることが望ましい。
物理セキュリティ	ピンタンビラー錠、シリンダー錠、マスターキー等、どんな錠にも脆弱性がある。物理セキュリティを検討する際には、それぞれの錠のセキュリティ強度を考慮することが重要となる。

攻撃シナリオ【5.1】

実際の攻撃では、4 章に挙げた脅威や脆弱性の利用により、様々なレベルの被害や連鎖的被害が引き起こされる可能性がある。本ガイドでは攻撃シナリオの例として、4.3 節に 8 つの攻撃シナリオと各シナリオの簡単な内容（概要、発生可能性、影響）を、5 章に 3 つの攻撃シナリオと各シナリオの詳細な内容（概要、発生可能性、影響、影響を受ける資産、連鎖的被害のリスク、検知の容易性、関係者、攻撃ステップ、復旧に要する時間／労力、課題とギャップ、対策）を記載している。

本概要では 5 章の詳細事例から、「攻撃シナリオ 1：SCADA システムへの侵入」の概要を記す。

「攻撃シナリオ 1：SCADA システムへの侵入」は、SCADA システム機器の 1 つを乗っ取り、任意の不正操作やシャットダウンを目的とする攻撃シナリオである。



SCADA システムへの侵入	影響	発生可能性
	【致命的】SCADA システムへの侵入は、システムの不正操作やオペレーションの停止等を引き起こし、生産停止や物理的被害につながる可能性がある。	【低～中】SCADA システム及び機器は相互接続や外部ネットワークへの接続が進んでおり、過去にはなかった脅威をもたらしている。
	検知の容易性	連鎖的被害のリスク
	【中】検知する機能を無効にされない限り、改ざんはSCADAシステムやセンサーによって検知可能。冗長系や二次系のシステムがあれば、より検知し易くなる。	【低】SCADA システムへの不正操作等は、接続システムに直接影響を及ぼしたり、停電や洪水等、公共に直接影響を及ぼす可能性もある。
	影響を受ける資産	関係者
	SCADA システム、HMI（操作端末）、中央制御システム	最高情報セキュリティ責任者（CISO）及びセキュリティ担当者、SCADA オペレータ、エンジニア

SCADA システムへの侵入

攻撃ステップ	
1. 攻撃者が、標的とする事業者の情報を収集する。 2. 標的とするコントロールセンターを絞り込む。 3. コントロールセンターの運用や従業員に関する情報を収集する。従業員に対するソーシャルエンジニアリング攻撃を行い、情報ネットワークへの侵入を図る。 4. 従業員の認証情報を窃取し、情報ネットワーク内の PC に侵入する。 5. 侵入した PC を拠点に情報収集を行い、脆弱なコンピュータを探す。 6. 脆弱なコンピュータを発見し、攻撃ツールによる攻撃を行う。 7. 侵入したコンピュータへの不正アクセスを維持できるよう、バックドアを仕込む。 8. 侵入したコンピュータが SCADA システムにアクセスできる機器ではなかった場合、他の機器を探す。 9. SCADA システムにアクセスできるコンピュータへの侵入を果たしたら、次の攻撃フェーズに移る。 10. 侵入したコンピュータを使って、SCADA システムへの攻撃を開始する。 11. SCADA システムのファームウェアをアップデートし、攻撃者によるアクセスを可能にするとともに、他からのアクセスを制限する。 12. SCADA システム全体が機能しなくなるよう、必要なシステム／機器の設定を改ざんする。 13. 電源システム及びバックアップシステムを無効化する。 14. SCADA システムが機能しなくなり、オペレーションが停止する。情報システムも使えなくなっているほか、SCADA システムの電源やバックアップシステムも立ち上がらない。コントロールセンターからは SCADA システムの状況が把握できず、対応できない状態となる。	
復旧に要する時間／努力	課題とギャップ
【中】影響を受けたシステム／機器によって、数時間から数日。	異常検知システムの導入とシステムの積極的な監視及びログ取得。
対策	
● SCADA システム資産を直接インターネットにつながない。 ● SCADA システムに修正プログラムを適用する。 ● 異常検知システムにより、不審なアクセスや不正なアクセスを見つける。 ● RACI（役割・責任分担）マトリクスを詳細化し、職務に就く場所や時間等の情報も加える。 ● アクセス権を持つユーザを管理し、妥当性を確認する。 ● 適切な認証を実装する（事前に共有した鍵、トークン、ワンタイムパスワード等）。 ● 通信を保護する（SSL/TSL による暗号化）。 ● ログを日々確認する。 ● インシデント発生時の調査用に、ログを取得し一定期間保管する。 ● 全ての機器についてデフォルトパスワードを変更し、設定を堅牢化する。 ● 定期的にシステムの監査及びリスク評価を実施する。 ● ネットワークをセグメント化する。	

対策（グッドプラクティス）【7.9】

本ガイドでは、7 章の 7.1 節～7.8 節に様々な対策とその解説を記載している。また、7.9 節では対策を以下のカテゴリに分類し、各対策の導入のし易さを「低」（現実的に可能な対策）と「中」または「高」（現実的に難しい対策）として評価している。

- SCADA ネットワークのセキュリティ
- セキュリティ設計（Security by Design）
- ソフトウェアアップデート
- 多層防御
- 通信セキュリティ
- 物理セキュリティ
- ワイヤレスネットワーク
- 従業員及び経営層のセキュリティ意識
- 資産管理
- サードパーティ
- ガバナンス及びコンンプライアンス
- マルウェア対策

本概要では、上記の各カテゴリにおいて、導入のし易さが「低」（現実的に可能）と評価された対策のみをまとめて示す。なお、各カテゴリ内の対策番号（1～49）は、全対策の通し番号となっている。

1. SCADA ネットワークのセキュリティ　－　導入のし易さ「低」の対策なし

2. セキュリティ設計　－　（原文）Table 5 抜粋

対策	関連する攻撃
11. セキュリティ設計：機器／コンポーネントの設計段階の初期から、セキュリティを検討する（組み込む）。	全ての攻撃

3. ソフトウェアアップデート　－　導入のし易さ「低」の対策なし

4. 多層防御　－　（原文）Table 7 抜粋

対策	関連する攻撃
15. セキュリティの確立と導入：制御システム向けのセキュイティポリシー、手順、訓練、教育教材を策定し、導入する。	情報窃取、ID 窃取、情報改ざん、内部脅威、マルウェア
18. アクセス制限：アクセス権限の付与を本当にその権限を必要とするユーザに限り、制御ネットワーク及び機器への物理的・論理的アクセスを制限する。	

5. 通信セキュリティ ー （原文）Table 8 抜粋

対策	関連する攻撃
25. リモートアクセスを管理するポイントの集約：リモートアクセスを管理するポイントを数ヶ所に限定し、全てのリモートアクセスはそれらの管理ポイントを通じて行わせる。	情報窃取、ID 窃取、情報改ざん、内部脅威
27. ウイルス対策ソフトの導入：ワークステーション及びサーバにウィルス対策ソフトをインストールする。インストールできない場合は、別のウィルス対策を導入する。	
28. 電子メール及びインターネットへのアクセス：制御システムからの電子メール及びインターネットへのアクセスをできなくする。	

6. 物理セキュリティ ー （原文）Table 9 抜粋

対策	関連する攻撃
31. 物理セキュリティ対策：制御システム及びネットワーク機器を物理攻撃や不正アクセスから守るため、物理セキュリティ対策を導入する。	不正な物理アクセス

7. ワイヤレスネットワーク ー 導入のし易さ「低」の対策なし

8. 従業員及び経営層のセキュリティ意識 ー （原文）Table 11 抜粋

対策	関連する攻撃
33. 従業員の身元調査：制御システムへの運用・管理権限を与える全ての従業員について、適性を審査する。	ソーシャルエンジニアリング、内部脅威、マルウェア
34. パスワード及びアカウント：全ての制御システムにパスワードポリシーを適用する。ポリシーにはパスワードの強度と有効期限を含める。パスワードは頻繁に変更することが推奨される。	
35. オペレータ加入時の手順：新しいオペレータが運用チームに加わる際に、適切なアカウント、権限、セキュリティ訓練が与えられるようにする手順を確立する。	
36. 機器の接続：制御ネットワークに機器を接続する前に、当該機器がマルウェアに感染していないことを検証する手順を確立する。	

9. 資産管理 ー （原文）Table 12 抜粋

対策	関連する攻撃
38. セキュリティフレームワークのドキュメント化：制御システムの全体像を把握するため、レガシーシステムを含め、制御システムを構成する全てのシステム及び機器を洗い出した資産一覧を作成する。資産一覧には脆弱性と想定される影響も記載し、メンテナンスを行う。	不正アクセス、悪意あるコード、ネットワーク障害

10. サードパーティ　－　導入のし易さ「低」の対策なし

11. ガバナンス及びコンンプライアンス　－　（原文）Table 14 抜粋

対策	関連する攻撃
41. 役割と責任の定義：制御システムのセキュリティを担う全てのコンポーネントの役割と責任を定義し、どのコンポーネントがどのセキュリティリスクを負うか定める。	コントロールセンターへの攻撃、データ窃取、認証の悪用
42. ポリシー、基準の策定：制御システムに関する正式なセキュリティポリシー及び基準を策定、文書化、通達し、変更管理を含めて管理する。ポリシーや基準は組織にとっての要件やサポートビジネスの要件を満たし、全関係者の合意を得る。	
43. ポリシーと基準への準拠の確認：制御システムに関するポリシーと基準が守られていることを確認するセキュリティ計画を策定する。	
44. ポリシーと基準の更新：制御システムに関するポリシーと基準を定期的に見直し、新たな脅威、法規制、要件、事業や運用の変化に合わせて更新する仕組みを確立する。	
45. インシデント対応：セキュリティインシデントへの対応手順を確立する。対応手順は検知、調査、分析、復旧、事後評価（再発防止策の検討・導入）の各段階について定める。	全ての攻撃（迅速な検知、低減、防止）

12. マルウェア対策　－　導入のし易さ「低」の対策なし

提言【8.1】

本ガイドでは、ICS／SCADA システムのセキュリティ及びレジリエンスの向上を支援するため、以下の 8 つの提言を行っている（各提言の詳細については、原文 8.2 節を参照）。

（原文）Table 16：提言

ID	提言
1	制御システムの設計段階からセキュリティを組み込む。
2	制御システムを運用する人員の役割を特定・確立する。
3	相互運用性を考慮に入れ、ネットワークアーキテクチャ及び通信技術を決める。
4	制御システム／機器のライフライクルに関わる様々な関係者が、ニーズや解決策について意見を交わせるブレインンストーミングの場及びコミュニケーション手段を確立する。
5	制御システムの主要オペレーションに、制御システム機器の定期的なアップデートを組み込む。
6	社内において、定期的な制御システムのセキュリティ訓練及び意識向上キャンペーンを行う。
7	EU レベルでの政策決定者、制御システムメーカー、制御システム運用事業者の連携強化を促進する。
8	頼りにできる、適切なサイバーセキュリティ保険の条件を定めるためのガイドラインを策定する。

以上