2016 年 11 月 22 日
独立行政法人情報処理推進機構（IPA）

ICS-CERT：多層防御による制御システムセキュリティの強化　概要

本概要は、米国土安全保障省（DHS） Industrial Control Systems Cyber Emergency Response Team（ICS-CERT）発行の“*Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies*”の概訳となります。内容の詳細につきましては、原文をご参照ください。（※特記が無い限り、本文中のリンク先は全て英語となります）
URL：https://ics-cert.us-cert.gov/ICS-CERT-releases-Recommended-Practice-Improving-Industrial-Control-System-Cybersecurity-Defense

セキュリティ対策における「多層防御」とは、セキュリティ対策を組み合わせて階層（レイヤー）を築くことで、1 つの対策が破られても次の（またその次の）対策が攻撃を抑止し、重要部への侵入前に攻撃の検知および対応できるようにする、リスクベースの総合的なセキュリティアプローチを指す。

多層防御という考え方自体は新しいものではなく、多くの重要インフラ事業者でも情報技術（IT）環境では採用されているが、産業制御システム（ICS）環境では採用されていない。これは、以前の ICS は外部と繋がっておらず、独自プロトコル等であったため、そうしたアプローチが必要なかったことも影響していると思われる。

しかし近年では重要インフラへのサイバー攻撃が増加し、大規模なインシデント事例が報告されるなど、ICS においても多層防御が必須となって来ている。

「ICS-CERT：多層防御による制御システムセキュリティの強化」は、大まかに以下の 4 構成となっている。

1. 背景と概要（Background and Overview）
   ICS セキュリティの現状
2. ICS における多層防御（ICS Defense-in-Depth Strategies）
   ICS のセキュリティ強化と多層防御
3. 攻撃（Security Attacks）
   攻撃者による攻撃手法と考えられる影響
4. ICS のセキュリティ強化のための推奨策（Recommendations for Securing ICS）
   ICS のセキュリティ強化に活用できる標準、ツール、サービス等

以降に、各章の概要を記す。

1. 背景と概要

ICS は、従来の「外部から隔離されたシステム」「独自プロトコル」という特性から、物理セキュリティに重きをおいて対策が行われてきた。しかし、近年多くの重要インフラ事業者がレガシーな技術から新しい技術への移行を進めており、オープンアーキテクチャや汎用プロトコルが使われるようになって来ている。その結果、データ収集や相互運用性など、利便性や効率が向上するといったメリットが得られた一方、サイバー攻撃の脅威という、これまで存在しなかった脅威に晒されるというデメリットも発生し、セキュリティ対策が必須となっている。

2. ICS における多層防御

攻撃者は、「技術」「人」「運用」の脆弱性のいずれかまたは組合せを悪用して侵入を図る。事業者は以下を理解し、ベストプラクティスや標準等を基に多層的な対策を実装することが求められる。

- ICS を構成する／支える「技術」「人」「運用」
- 攻撃者の「目的／意図」「攻撃能力」「攻撃機会」
  （備えるべき脅威、攻撃機会を与えうる脆弱性（技術的、人的、運用上のものを含む）等）
- セキュリティ標準、実施可能な対策

多層防御では、「攻撃者にとっての“攻撃コスト”を上げ、攻撃するためのハードルを上げること」、また、「攻撃が行われた場合の検知力・防止力を向上すること」の 2 点によってセキュリティを向上させる。

表 2 は、多層防御を実装するにあたっての重要項目と対策を示している。

表 2. 多層防御の構成要素

多層防御の構成要素		
項目	**対策**	**参照節**
リスク管理	• 脅威の特定 • リスクの把握 • 資産一覧の作成／メンテ	2.1
サイバーセキュリティアーキテクチャ	• 標準／推奨策 • ポリシー • 手順	2.2
物理セキュリティ	• 現場機器のロックダウン • 制御センターへのアクセス制御 • リモート拠点のカメラ監視、アクセス制御、塀（防壁）	2.3
ICS ネットワークアーキテクチャ	• 共通のアーキテクチャ毎でのゾーン分け • DMZ • 仮想 LAN	2.4
ICS ネットワーク境界セキュリティ	• ファイアウォール／一方向ゲートウェイ • リモートアクセス＆認証 • ジャンプサーバ／ホスト	2.5
ホストセキュリティ	• パッチ、脆弱性管理 • 現場機器 • 仮想マシン	2.6
セキュリティ監視	• 侵入検知システム（IDS） • セキュリティ監査ログの取得 • セキュリティインシデント／イベント監視	2.7
ベンダ管理	• サプライチェーン、マネジメント • マネージドサービス／アウトソーシング • クラウドサービスの活用	2.8

多層防御の構成要素		
項目	対策	参照節
人的セキュリティ	• ポリシー • 手順 • 訓練、意識向上	2.9

原文では 2.1～2.9 節において、各項目（対策）の実装の目的、ポイント、留意点等が説明されている。

3. 攻撃

多層防御の実装には、攻撃者による攻撃方法を理解しておくことも重要である。攻撃に使える脆弱性や新たな攻撃手法の発見と、それらを防ぐ対策の開発や実施はいたちごっこであり、新たな脅威の出現に備えて守るべきシステムや機器を継続的に監視し、アップデートしていくことが肝要となる。

通常、攻撃は標的システムに関する情報収集から目的の遂行まで、段階的に進んで行く（図 9）。

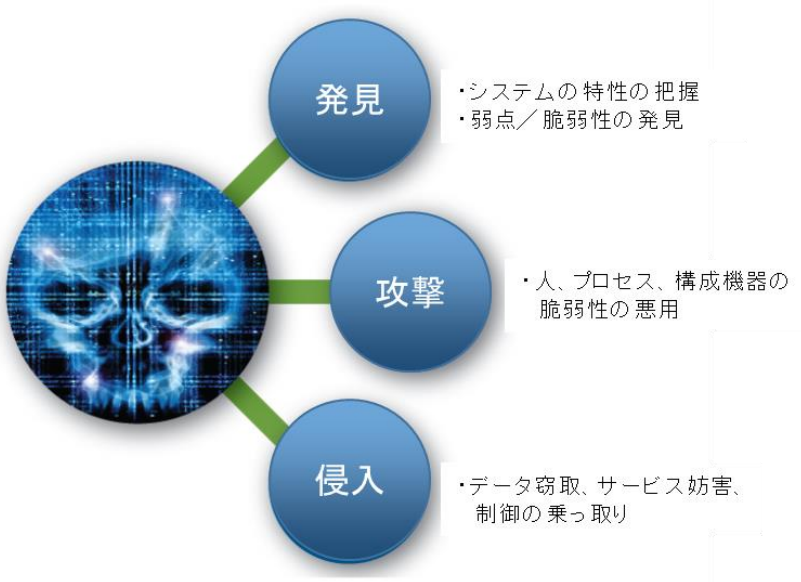

図 9. 攻撃のシークエンス

本概要では例として、重要インフラへの攻撃によく使われている攻撃手法（原文「3.3 ICS Attack Methods」の概要を記す。

■ BlackEnergy（原文 3.3.1）

BlackEnergy は 2007 年に確認されて以降進化を重ねているマルウェアで、標的型攻撃によって標的組織の従業員や関係者に送られ、開かれるとトロイの木馬や悪意のある実行ファイルをインストールし、侵入する。特定の産業用 HMI 製品が狙われており、HMI にインターネットからアクセスできるような構成／運用になっている組織が影響を受けやすい。BlackEnergy の検知や対策に関しては、ICS-CERT のアラートを参照のこと[1]。

[1] ICS-ALERT-14-281-01：Ongoing Sophisticated Malware Campaign Compromising ICS (Update E)
https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01B

■ 不正アクセス（原文 3.3.2）

多くの ICS は、公衆電話回線または専用線を通じてリモートアクセスを可能とする設計となっている。対策が何もされていない場合、攻撃者による悪用を簡単に許してしまうほか、監視やログ取得も行っていない場合、検知もできないことになる。仮にモデムに ID/PW が設定されていても、ロックアウト機能がほとんど実装されていない現状ではウォーダイヤリングや総当り攻撃を防ぐことはできず、攻撃を防ぐのに十分とは言えない。標準的な通信プロトコルの使用が可能なフィールド機器が増加していることからも、フィールド機器も ICS を構成する一要素であると認識し、対策を検討する必要がある。

■ データベース／SQL インジェクション（原文 3.3.3）

現在の ICS では、データベースは ICS の核となるアプリケーションとなっている。ウェブインターフェースを持っている場合も多く、SQL インジェクション等の脆弱性が存在する可能性がある。また、ICS が使用するデータベースは業務ネットワーク上のデータベースやコンピュータと繋がっていることも多く、その接続性が悪用される可能性もある。

■ OPC／DCOM 攻撃（原文 3.3.4）

侵入した攻撃者がよく狙うのが、OPC（OLE for Process Control）Classic の脆弱性である。OPC は Component Object Model（COM）／distributed COM（DCOM）をベースとした、製造元の異なる ICS 機器間でプラントデータをリアルタイムにやり取りするためのデータ通信プロトコルだが、セキュリティ上の問題や脆弱性があり、マルウェアのインストール、権限昇格、サービス妨害、意図せぬシャットダウン等が引き起こされる可能性がある。代替となるよりセキュアな仕組みも提供されているが、ICS のライフサイクルの長さゆえに、昔導入した OPC／DCOM を引き続き使い続けている事業者も多い。

■ 中間者攻撃（原文 3.3.5）

従来の ICS は外部と繋がっていない完全に独立したシステムであったため、ICS 内部でやり取りされるデータを守るという発想はなかった。しかし、業務システムなど外部ネットワークとの接続が進んだことで、無防備なデータを中間窃取し、データを閲覧したり改ざんしたりする中間者攻撃のリスクが指摘されるようになった。成功すれば、制御・監視データの窃取、改ざん、偽データの挿入などが行われる可能性がある。

■ ソーシャルエンジニアリング攻撃（原文 3.3.6）

基本的に、多くの人は人を疑わない。攻撃者はそれを知っており、同僚や取引のあるベンダ等を装い、正規のやり取りに見せかけて悪意あるメールを送ってくる。攻撃者は標的組織の ICS 環境に悪意あるコードを潜り込ませるため、ICS 関係者を狙ってスピアフィッシング（標的型攻撃）を仕掛けてくる。事業者は、業務システム環境と ICS 環境を分離し、両者の間のあらゆる接続を適切に制御することが必須となる。

同様に、攻撃者が ICS 環境に正規入場者と“共連れ”で入り込むことがないよう、物理セキュリティを固める必要がある。保守業者やベンダに入室を許可する前に身分証明書が正規のものであることを十二分に確認するとともに、作業中は傍を離れず監視し、未許可のメディア（USB メモリ、CD 等）等を使用させないようにすることが重要である。

4. ICS のセキュリティ強化のための推奨策

ICS が晒されているリスクを低減するためには、単純に IT 環境で使われているセキュリティ技術を ICS 環境に導入するだけでは有効な対策とならない場合がある。最近の ICS では汎用プロトコルの利用が進んでいるとはいえ、ICS 特有の可用性の重要さや、時間にシビアでセキュリティ対策の導入がもたらすレイテンシーが許容できない場合など、セキュリティ対策の導入ができない可能性もある。しかし、ICS が隔離されたシステムから業務システム等の外部ネットワークと繋がったシステムになる以上、ICS 管理者は ICS の機能を妨害することのないよう考慮しつつ、セキュリティを守らねばならない。

以下に、ICS のセキュリティ強化にあたって推奨される 5 つの取組みを記す。

1. ICS と外部ネットワークとの接続点の把握、最少化、およびセキュリティの堅牢化
2. 不必要なサービス、ポート、プロトコルの無効化、利用可能なセキュリティ機能の活用、堅固な構成管理の実施による ICS および関連システムのハードニング
3. ICS、ネットワーク、システム間／ネットワーク間の継続的なセキュリティ監視および評価
4. リスクベースの多層防御アプローチの実践
5. 「人」の管理 ー 自身の行動に対して責任を負わせる、ICS セキュリティに関する訓練の提供など

■ 参考: セキュリティ標準およびツール等

- NERC-CIP
  http://www.nerc.com/AboutNERC/Pages/default.aspx
- NIST ICS Framework
  https://www.nist.gov/cyberframework
- Specific Subsector Guide
  - Electricity Subsector：Electricity Subsector Cybersecurity Risk Management Process
    http://energy.gov/oe/downloads/cybersecurity-risk-management-process-rmp-guideline-final-may-2012
  - Process Control System Security Guidance for the Water Sector
    http://www.awwa.org/resources-tools/water-and-wastewater-utility-management/cybersecurity-guidance.aspx
  - Chemical Facility Anti-Terrorism Standards（CFATS）
    https://www.dhs.gov/chemical-facility-anti-terrorism-standards
  - TSA Pipeline Security Guidelines
    https://www.tsa.gov/sites/default/files/tsapipelinesecurityguidelines-2011.pdf
- ICS-CERT： Cyber Security Evaluation Tool（CSET）、Design Architecture Review（DAR）、Network Architecture Verification and Validation（NAVV）
  https://ics-cert.us-cert.gov/Assessments

以上