2015 年 8 月 31 日
独立行政法人情報処理推進機構（IPA）

ICS-CERT：FY2014 の ICS セキュリティ評価実施状況　総括

本概要は、米国土安全保障省が運営する ICS-CERT（Industrial Control Systems Cyber Emergency Response Team）発行の“Industrial Control Systems Assessments FY2014 Overview and Analysis”の概訳となります。内容の詳細につきましては、以下の原文をご参照ください。URL：
https://ics-cert.us-cert.gov/sites/default/files/documents/2014_Year_End_Assessment_Report_v4_S508_C.pdf

ICS-CERT は、米国土安全保障省（DHS）配下の組織で、官民パートナーシップを通じて制御システムのセキュリティおよびレジリエンス強化を支援し、米国の重要インフラのサイバーセキュリティリスクを低減することをミッションとしている。

その一環として、ICS-CERT では重要インフラを対象に様々なセキュリティ評価ツールやサービスの無償提供を行い、重要インフラにおけるサイバーセキュリティリスクへの理解を促すとともに、指針となる標準や取るべき対策（ベストプラクティス）等を示している。

本レポートでは、ICS-CERT が提供しているセキュリティ評価サービスの概要と、FY2014（2013 年 10 月～2014 年 9 月）の実施状況の総括として、件数や事業者に共通して見られる問題点などをまとめている。

1. ICS-CERT が提供するセキュリティ評価サービス

セキュリティ評価は、重要インフラ事業者による以下の支援を目的とし、「NIST SP800-53：連邦政府情報システムにおける推奨セキュリティ管理策 [1]」および「NIST SP800-82：産業制御システム（ICS）セキュリティ [2]」の分類や項目を用いて行っている。

- 制御システムのサイバーセキュリティ上の問題点の特定
- サイバーセキュリティ上の脅威や脆弱性の理解
- 一定のセキュリティ対策の実施
- 追加のリスク低減策の検討

提供しているセキュリティ評価サービスは 3 種類ある。

（1） Cyber Security Evaluation Tool（CSET）レビュー

ICS-CERT が開発した、政府基準や業界標準に照らして組織のセキュリティ対策状況を確認することができるツール「CSET[3]」を使用した、汎用的なセキュリティ評価サービス。評価に要する日数は通常 1 日。2014 年度は 48 件実施。

[1] NIST SP 800-53: Security and Privacy Controls for Federal Information Systems and Organizations Rev.4
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
[2] NIST SP 800-82: Guide to Industrial Control Systems (ICS) Security Rev.2
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf
[3] Cyber Security Evaluation Tool (CSET)
https://ics-cert.us-cert.gov/Assessments

原文図 2. CSET レビューの大まかな流れ

（2） Design Architecture Review（DAR）

設計や構成、相互依存性やネットワークの接続性、多層防御の有無などを、評価対象組織の ICS に合わせてレビューする、より詳細な評価を行うサービス。以下に重点を置いて行われる。

- ICS 資産の棚卸し
- ICS ネットワークアーキテクチャ確認
- セキュリティ対策（防御、検知）の確認

評価に要する日数は通常 2 日。2014 年度は、NAVV と併せて 56 件実施。

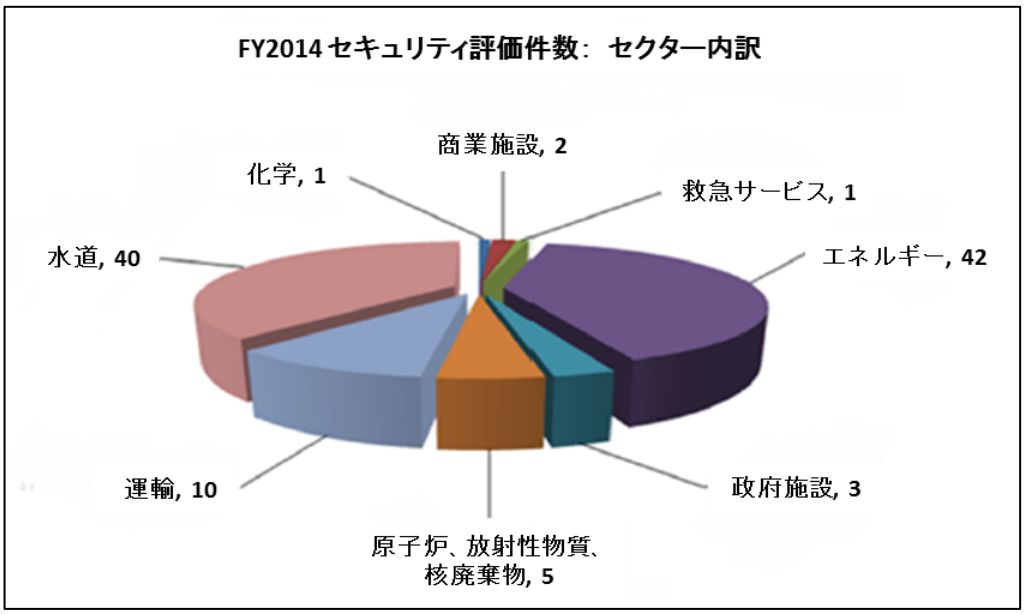
（3） Network Architecture Verification and Validation（NAVV）

ICS ネットワークを流れるパケットデータの解析による、機器間の通信フローの洗い出しと見直しを行うサービス。以下を可能にする。

- 既存の ICS ネットワークダイアグラムの正確性の確認
- 不正なデバイス、設定が間違っているデバイス、不審な通信の特定
- 境界保護が意図した通りに機能しているかの確認
- ゾーニングやペリメータセキュリティの改善余地の検討
- ICS ネットワークの基準値（ベースライン）の把握
- ICS ネットワーク内で発生する通信の実践的な監視および検証方法の習得

NAVV は通常 DAR の拡張として実施するが、単独で行う場合もある。2014 年度は、DAR と併せて 56 件実施。

なお、CSET レビュー、DAR、NAVV（計 104 件）の重要インフラセクター別内訳は以下の通り。



原文図 5. FY2014 セクターごとのセキュリティレビューの実施件数

2. 共通して見られた問題点

FY2014 に実施した評価では、以下の分野における対策の欠如や不十分さが事業者・セクターを通じて見られた。

原文表 2. FY2014 よく見られた問題点とリスク

FY2014 DAR/NAVV において共通して見られた問題点		
NIST SP 800-53 セキュリティ管理策ファミリ	管理策	対策の欠如・不十分さがもたらすリスク
システムおよび通信の保護（SC）	境界保護	・ 悪意ある／不正な活動の検知は、適切な ICS ネットワークの境界保護なしには非常に困難。また、境界保護の欠如は、制御プロセスに直結する機器やシステムに対して多様な攻撃ベクトルを与えることになる。 ・ ICS ネットワークが従来の企業（IT）ネットワーク（またはインターネット等の信頼のおけないネットワーク）から論理的に切り離されていない場合、制御システムの運用に対する脅威およびリスクは著しく増加する。
アクセス制御（AC）	情報フロー制御の実施	・ ICS ネットワーク内の通信、および ICS ネットワークを送信元／宛先とする通信の両方の可視化と包括的な把握なしには、実際にインシデントが発生するまで、悪意ある／不正な通信に気付くことができない可能性が高い。 ・ 攻撃者は、使用可能なポート、サービス、通信チャネルを使って不正通信を行う経路を確立する。事業者は、ICS 機器における堅固なユーザ認証技術の利用、強いパスワードの使用、専用端末以外のモバイル端末からの ICS への接続制限・監視に加え、ICS ネットワーク内で起こる事象をモニタリングし、悪意ある／不正な活動を検知する能力を備えることが必須となる。
アクセス制御（AC）	リモートアクセス	・ リモートアクセスは、ICS へのアクセスによく使われる攻撃ベクトルである。リモートアクセスのセキュリティ対策が弱いと、ICS の重要機器に（恐らくは検知されずに）アクセスする手段を与えてしまう。 ・ 攻撃ベクトルとしては、インターネットにつながっている ICS 機器、ICS へのアクセス権限を有する第三者ベンダや請負業者、VPN のセキュリティ設定の弱さ、私物デバイスの使用、OS のサービスや設定の脆弱性などが考えられる。
アクセス制御（AC）	特権の最小化	・ 攻撃者や悪意のある内部関係者は、ICS にアクセスするのに、信頼されているドメインまたはネットワークセグメントのユーザ／コンピュータアカウントを活用する。 ・ 日常業務の実行に必要とされる以上の権限を付与することは、意図的な（攻撃者／悪意のある内部関係者による）不正行為、または非意図的な（思いがけない）不正行為を引き起こしかねない。 ・ 日常業務に高い権限や管理者権限を使用しているユーザは ICS の運用に大きな影響を及ぼす可能性があり、リスクが高くなる。不要な権限の付与の例としてよく見られる問題には、「許可されていない／テストしていないソフトウェアのインストール」、「重要なデバイス上でのマルウェアや悪意のあるアプリケーションの実行」、「セキュリティ機能や対策（ウィルス対策ソフト、ホストベースのファイアウォール等）の無効化」、「アプリケーションの権限や設定の変更」などがある。
物理的および環境的な保護（PE）	物理的アクセス制御	・ 攻撃者にしろ、悪意のある内部関係者にしろ、ICS 機器への直接的／物理的なアクセスは、ICS 機器のクライアント端末を通じた直接操作（プログラム改竄やフィールドコントローラの妨害等）を可能にしてしまう。
システムおよび通信の保護（SC）	セキュリティ機能の隔離	・ フラットなネットワーク構成では、ICS への不正アクセスや悪用を非常に容易にしてしまう。 ・ 適切な境界保護、多層での認証や対策が無いと、攻撃者は企業（IT）ネットワーク環境または信頼されている第三者ネットワーク環境のアカウントを使って、ダウンストリームの ICS 機器にアクセスできてしまう可能性がある。 ・ フラットなネットワーク構成では、システムやデバイス間の悪意のある／不正な通信のモニタリングがやり難い。

3. 推奨策

「2. 共通して見られた問題点」に対する是正策として、以下に推奨策を示す。

システムおよび通信の保護

OT 環境を構成しているシステムやデバイス、ネッワークのアーキテクチャを正しく把握していなければ、境界を引くことも、効果的な防御（対策）を行うこともできない。先ずは全ての ICS 構成機器の棚卸しを行い（ハード、ソフト、ICS が依存しているシステム等を含む）、ゾーニングの再確認、DMZ や監視・防御をし易くする“チョークポイント”の設置など、必要に応じて守りやすい環境を整備する。

アクセス制御 ー 情報フロー制御の実施

ICS ネットワークを流れる通信を理解することは、通信を検証するための、強力な監視・検知能力の確立に欠かせない。ICS 機器間や ICS を送信元・宛先とする通信を漏らさず洗い出し、通信の正当性や頻度等を確認のうえ、想定されるベースライン（基準値）を確立し、不要・不審な通信を遮断する。

アクセス制御 ー リモートアクセス

利便性と引き換えに、セキュリティを疎かにしてはならない。安易なリモートアクセスを認めないことはもちろん、ICS 機器や ICS に接続する機器を、インターネット等の信頼のおけないネットワークに直接接続してはならない。業務上リモートアクセスが必要な場合、ICS-DMZ の jump-box（要塞ホスト）を介してアクセスさせるなどの対策を行う。また、第三者ベンダ等からのリモートアクセスが必要な場合、常時接続を許すのではなく、必要時にのみアクセスを許可し、それ以外は許可しないことも検討する。

アクセス制御 ー 特権の最小化

事業者は、ユーザの操作権限ついて、「特権の最小化」の考え方に基づき、付与する権限を日常業務の実行に最低限必要とされる権限に留めることが望ましい。（しかし多くの事例では、従業員が業務に必要となる以上の権限を持っていることが多く、結果的に不正行為につながっているケースもある。）また、操作ログの収集や監視、定期的な監査等を通じて、権限昇格や書き換えといった操作の検知に加え、悪意ある行動を思い留まらせる抑止力となることが期待される。

物理的および環境的な保護

攻撃者に物理的に侵入された場合、機器やデータ等の窃盗や物理的な破壊、機器の直接操作による設定変更等が行われる可能性がある。また、ICS 機器は広い地理的エリアに分散し、人が常時居られない場所に設置されている機器も多い。そうした機器がハッキングされ、ICS 中枢へのアクセスを許してしまう可能性もある。ドアや窓以外の侵入口への侵入防止（警報）装置の設置、監視カメラ等のデフォルトパスワードの無効化（変更）、PLC の run モードでの運用の検討など、物理的な不正アクセスの制限と検知、およびリスク低減につとめる。

なお、本レポートで紹介したよく見られる問題点や推奨策は、それだけやればいいという見方をするのではなく、自組織の対策を見直す中で、特に気をつけて確認するポイントとして利用することが望ましい。

以上