2016 年 9 月 9 日
独立行政法人情報処理推進機構（IPA）

ICS-CERT　制御システムセキュリティ評価サマリーレポート（FY2015）　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“*Industrial Control Systems Assessment Summary Report FY2015*”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-FY-2015-Assessment-Report

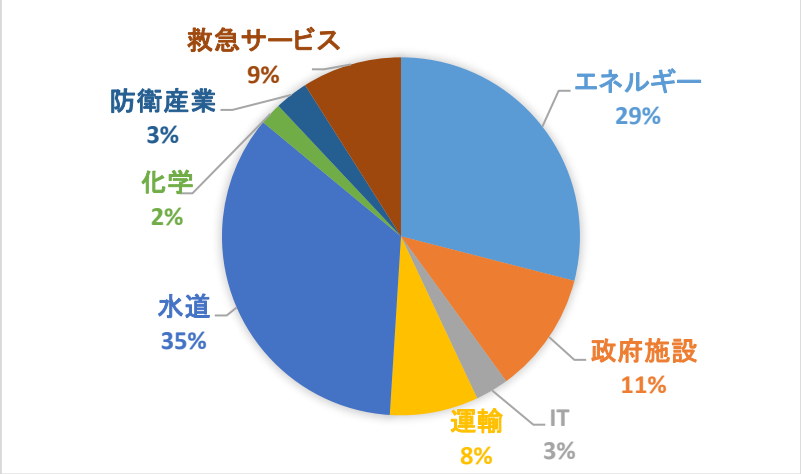
ICS-CERT は、重要インフラ事業者を対象に、以下の制御システム向けセキュリティ評価サービスを提供している[1]。

- Cyber Security Evaluation Tool （CSET）を用いたセキュリティ評価
  政府基準や業界標準等に照らして、組織のセキュリティ対策状況をステップ・バイ・ステップで確認するツール「CSET」を使用した、汎用的な評価サービス
- Design Architecture Review（DAR）
  組織の制御システム／ネットワークの設計や構成、相互依存性、利用しているアプリケーションなどに合わせた、よりカスタマイズされた評価サービス
- Network Architecture Validation and Verification（NAVV）
  ネットワークを流れるパケットの解析による、機器間の通信の洗い出しと確認を行うサービス

原文表 1. セキュリティ評価サービスの実施状況

サービス	FY2009	FY2010	FY2011	FY2012	FY2013	FY2014	FY2015	計
CSET	20	57	81	83	60	49	38	**388**
DAR	N/A	N/A	N/A	2	10	35	46	**93**
NAVV	N/A	N/A	N/A	4	2	20	28	**54**
計	**20**	**57**	**81**	**89**	**72**	**104**	**112**	**535**

原文図 2. FY2015 に評価を実施した重要インフラ分野



[1] ICS-CERT Assessments　https://ics-cert.us-cert.gov/Assessments

Industrial Control Systems Assessment Summary Report FY 2015 は、ICS-CERT が上記のセキュリティ評価サービスを通じて発見した、制御システムにおいてよく見られるセキュリティ上の問題を事業者と共有することで、対策の見直し・強化を促進するものである。

FY 2015 の評価結果をまとめると以下となる。

- FY 2015 は、112 件のセキュリティ評価を実施
- これらの評価を通じて、638 件のセキュリティ上の問題を発見
- 問題をカテゴリに分類したところ、全 638 件のうち 36%が上位 6 つのカテゴリに集中
- 最も多く見られたのは、カテゴリでいうところの「境界保護（boundary protection）」に関する問題（FY2014 も同様）
- 全 638 件のうち 21%が、1 位の「境界保護（boundary protection）と 2 位の「機能の最小化（least functionality）」に関する問題
- 主な傾向として、仮想マシン、リモートアクセス、VLAN、BYOD、クラウドサービスの利用、ICS ネットワークの監視などに関する問題が広く存在

上位 20 の問題

特定された問題を NIST SP 800-53 の対策サブカテゴリ[2]で分類したところ、上位 20 は以下であった。

原文表 4. 特定された問題のカテゴリ上位 20

	NIST SP 800-53 に示された対策（サブカテゴリ）		件数
1	SC-7	境界保護	85
2	CM-7	機能の最小化	46
3	IA-5	認証コードの管理	27
4	IA-2	ユーザ識別および認証	25
5	AC-6	特権の最小化	23
6	SA-2	リソースの割り当て　　上位 6 で全体の 35.8%	23
7	AU-6	監査記録の監視、分析および報告	22
8	PE-3	物理的アクセス制御	19
9	SI-2	欠陥の修正	19
10	CM-4	構成変更の監視	19
11	AT-2	セキュリティの意識向上	17
12	CP-9	情報システムのバックアップ	17
13	CM-6	構成設定	16
14	AT-3	セキュリティトレーニング	15
15	CM-3	構成変更管理	14
16	SA-8	セキュリティエンジニアリングの原則	13
17	AC-17	リモートアクセス	11
18	SC-8	伝送する情報の完全性	11
19	AC-2	アカウント管理	10
20	SA-4	調達	10

[2] NIST SP 800-53　http://csrc.nist.gov/publications/PubsSPs.html#800-53

【AC】アクセス制御　【AT】意識向上およびトレーニング　【AU】監査および責任追跡性　【CM】構成管理　【CP】緊急時対応計画　【IA】識別および認証　【PE】物理的および環境的な保護　【SA】システムおよびサービスの調達　【SC】システムおよび通信の保護　【SI】システムおよび情報の完全性

上位 6 の問題：リスクと対策

以下に、全体の 35.8%を占めた上位 6 カテゴリの問題のリスクと対策を簡略に示す。

原文表 2.および表 5.より抜粋　上位 6 カテゴリのリスクと推奨対策

	カテゴリ	不十分な対策によるリスク／推奨される対策	
1	境界保護 （SC-7）	リスク	• 攻撃を検知することが困難となる • ICS に対するリスクが増加する
		対策	• 業務／外部ネットワークから分離し、DMZ を設置する • 業務システムから ICS データへのアクセスのための専用サーバ（ジャンプサーバ）を DMZ に設置する　ほか
2	機能の最小化 （CM-7）	リスク	• ICS への不正アクセスにつながる攻撃ベクトルを与える • ICS への不正アクセスの機会を与える
		対策	• 必要なサービス、ポート、プロトコル、アプリケーション等を明確にし、必要なもの以外は使用を制限する　ほか
3	認証コードの管理 （IA-5）	リスク	• セキュアでないパスワードの運用により、パスワードが漏洩する • パスワードの漏洩により、成りすましによる ICS への不正アクセスが可能となる
		対策	• 強いパスワードの使用や暗号による保護など、運用ポリシーを策定し、実施する • リモートアクセスにあたっては、多要素認証の要求など、別途対策を追加する　ほか
4	ユーザ識別および認証 （IA-2）	リスク	• 個々のユーザによる操作に関して責任の所在の確認および追跡ができない • 離職時のアカウント管理が困難となる（特に管理者権限を有する従業員の離職時に重要）
		対策	• アカウントはできるだけ個人ごとに作成し、共有アカウントを認める場合は厳格に記録する • 共用アカウントを認める場合は、他の手段で責任の所在が確認できるようにする　ほか
5	特権の最小化 （AC-6）	リスク	• ユーザ（アカウント）の持つ権限が高ければ高い程、（アカウント情報を窃取した）攻撃者が実施可能な操作や範囲が大きくなる
		対策	• 「特権の最小化」を全システムで実施する。高い権限を必要とするユーザの場合、必要な権限を必要な時だけ使えるようにする　ほか
6	リソースの割り当て （SA-2）	リスク	• セキュリティ担当者の不足により監視やインシデント対応に手が周らず、インシデントがもたらす被害が増大する
		対策	• 平時の運用と早期検知策（ログのレビュー等）に掛かるコストとメリットを適切に評価し、人材の雇用やリソースの割り当てを行う

※原文には、上位 6 カテゴリのリスクや推奨対策に関して、より詳細な記載があります。詳しくは原文をご確認ください。

技術のシフトに関する所見

重要インフラ事業者との会合では、ICS-CERT が発見した問題の共有だけでなく、制御システム環境で利用されている技術のシフトについても知見を得ることができた。FY2015 は、とりわけ利用される技術に変化が見られ、それらの技術のセキュアな実装に課題が生じていることが窺えた。以下に 6 つの課題について記す。

（1） 仮想マシンにおける不適切なアクセス制限

資本設備の縮小、復旧の効率化、1 台のコンピュータ上での複数 OS の利用手段として、制御システム環境でも仮想化技術の利用が進んでいる。しかし、ハイパーバイザーの管理インターフェースへのアクセス制限が不適切なケースも多く見られる。不適切な導入により、単一障害点（SPOF）となる可能性もあるほか、DMZ と監視制御サーバを同一の物理ホスト上に構築している場合など、ネットワーク／ネットワークインターフェースに対して適切な設定・対策を行っていないと、ブリッジ（移動）を許してしまう可能性がある。

（2） リモートアクセスの不適切な実装

新しい技術ではないが、リモートアクセスの不適切な実装も大きな問題となっている。業務ネットワークからにせよ、自宅からにせよ、攻撃者が制御システムにリモートアクセスできるユーザアカウント／PC の乗っ取りに成功した場合、制御システムへの侵入を許してしまう可能性がある。事業者はリスクを許容範囲内に低減できるまで、当該リモートアクセスを誰が何のために必要としているのか、どうセキュリティを確保するかを検討する必要がある。例えば、多要素認証を利用し、VPN によるアクセスを対策・監視を強化したジャンプサーバに制限することなどでリスクを低減できると考えられる。

（3） VLAN の不適切な使用

VLAN は標準的なセキュリティ対策として既に長い間利用されているが、設定に問題があると VLAN から VLAN への“ジャンプ”も可能となってしまう。

（4） ICS における BYOD のリスク

一般における普及や利便性などから、制御システム環境でも運用、メンテナンス、エンジニアリングにおけるタブレット、スマートフォン、ノート PC 等の利用が増加している。しかし、多くの場合これらのモバイル機器は事業者によって管理されておらず、事業者の定めるセキュリティポリシー（対策）がこれらのモバイル機器には実装されていないことも多い。制御システムにアクセスするモバイル機器が個人メール、ウェブサイト、SNS へのアクセスにも使われることは高いリスクを伴う。事業者はリスクを認識し、モバイル機器管理（MDM）システムの導入など、必要な対策を導入するべきである。

（5） クラウドサービス：重要機能を外部ホスティングする場合のセキュリティ強化の必要性

クラウドストレージを活用している事業者や、クラウドを制御システムのサポートに活用できないか検討している事業者も見受けられる。事業者は、外部にホスティングされた制御システム関連要素についても、制御システムに求められる高いセキュリティレベルが維持されることを保障しなければならない。

サービスレベル合意書（SLA）などの法的文書が非常に重要となり、サポート内容を全て明確に規定する必要がある。事業者が必要とするサポートがすべて明示されていることにより、何か問題が発生しても、事業者が問題に対応するのに必要十分なサポートをプロバイダから受けられることが保証される。

なお、クラウドにシフトする際に見過ごされる問題として、インターネットサービスプロバイダ（ISP）への依存と利用帯域の増大がある。負荷分散や、他の ISP 契約者による帯域圧迫の影響なども考慮に入

れておく必要がある。

（6） 多層防御の核としての ICS ネットワークの監視

多層防御（Defense in Depth）は、侵入の早期検知により、最重要箇所に侵入される前に防止措置が取れるようにすることを柱としている。しかし、多くの事業者が業務システムネットワークではある程度の監視を行っているのに対し、制御システムネットワークでは殆ど行っていない。

ネットワークの監視には、様々な方法がある。フリーツールによるログ収集や、様々なログを収集・相関分析する Security Information and Event Management（SIEM）、Canary やハニーポット／ハニーネット等を活用することも考えられる。

以上