2015 年 9 月 29 日
独立行政法人情報処理推進機構（IPA）

# ICS-CERT モニター（2015 年 7･8 月号）概要

本概要は、米国土安全保障省の ICS-CERT（Industrial Control Systems Cyber Emergency Response Team）発行の“ICS-CERT Monitor July/August 2015”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/monitors/ICS-MM201508

## 1. インシデント対応活動

### （1）直近の事例

2015 年 7 月、複数の重要インフラ業界を標的とする APT 攻撃が発見された。この攻撃では、ユーザがスピアフィッシングメール内のリンクをクリックすると、Adobe Flash Player のゼロデイ脆弱性（CVE-2015-3113）を突く悪意のあるファイルを配布するウェブサイトにリダイレクトされる仕組みとなっていた。

この APT 攻撃の攻撃者によるサイバー攻撃は、2014 年初めにも観測されている。その時にはソーシャルエンジニアリングを活用し、あるケースでは採用応募者の振りをして標的企業の社員に連絡を取り、履歴書へのフィードバック依頼を口実に悪意のあるファイルを送りつけ、当該社員の PC をマルウェアに感染させた。

ICS-CERT ではセキュアポータル [1]を通じて注意喚起（ICS-ALERT-15-198-01P: APT Spearphishing Campaign Against Multiple Sectors）を発行し、警戒を呼び掛けた。

### （2）ICS-CERT によるセキュリティレビュー

2015 年 7 月、8 月は、5 業界で 22 件のオンサイト･セキュリティレビューを実施した。

業界別では、緊急通報受理機関 [2]が 10 件、政府機関･施設が 4 件、化学業界が 3 件、エネルギー業界が 3 件、水道業界が 2 件であった。

また、セキュリティレビューの種別では、Cyber Security Evaluation Tool（CSET）によるレビューが 2 件が、Design Architecture Review（DAR）によるレビューが 14 件、Network Architecture Verification and Validation（NAVV）によるレビューが 6 件であった。

- CSET レビュー
  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ツール「CSET」を使用した汎用的な評価サービス
- DAR レビュー
  設計や構成、相互依存性や利用しているアプリケーションなど、組織の制御システム／ネットワークに合わせた、より詳細な評価サービス
- NAVV レビュー
  ネットワークを流れるパケットの解析による、機器間の通信フローの洗い出しと確認を行うサービス

[1] US-CERT の登録制ポータルサイト（https://portal.us-cert.gov）。重要インフラ事業者および関連企業･組織で、登録を希望する場合は ics-cert@hq.dhs.gov まで。
[2] 警察、消防、救急など、有事の際に治安および人命･財産を守る公共サービスを提供する機関。

各レビューの詳細は、https://ics-cert.us-cert.gov/Assessments を参照。

## 2. セキュリティトピックス

### (1)ログの活用

ログは、ソフトウェアがあるオペレーションやイベントがいつ発生したかという追跡可能な記録である。ログを生成するのは、オペレーティングシステム(OS)であったり、OS上で動作するアプリケーション自身であったりする。何をどれだけ記録するか、ログの詳細度は各ソフトウェアによって異なるが、ユーザはシステム等で発生している問題を見つけたり判断するのに、ログを活用することができる。定期的にシステムやデータベースのログをチェックし、平時のログのパターンに親しむことで、異常時の平時と異なるログのパターンに気付くことができるようになる。

ログの活用の第一歩は、使用しているソフトウェアがどんなログを取得できるのか、ログ機能について理解することから始まる。詳細度の高いログを取得するソフトウェアもあれば、ログ機能が無いソフトウェアもありえる。後者の場合は、サードパーティ製のログ取得ソリューションを使用することになる。

最大の課題は、メモリ使用量や保存可能なデータ量などを鑑み、ログの取得にあたっての「適切なレベル」を見極めることである。情報は多過ぎるとノイズと化してしまうし、少な過ぎると必要な時に役に立たない。参考資料として、米標準技術研究所(NIST)が「適切なレベル」の判断を支援するガイドラインを提供しており[3]、これを参照することができる。

## 3. ICS-CERT ニュース

### (1)ICS-CERT の国際連携の取組

サイバー攻撃はグローバルで、地理的な制約を受けない。インターネット経由でどこからでも攻撃される可能性があるし、制御システムを支えるベンダやサプライチェーンもグローバルである。仮に何処かでサイバー攻撃が起こり、それが米国の重要インフラに影響を及ぼすものではなかったとしても、後日同じ手口で狙われる可能性がある。サイバー攻撃への対応には、国際的な協力が戦略的にも実運用的にも不可欠である。

とはいえ、制御システムのセキュリティに責任を負う組織や体制は国によって異なる。国土安全保障省(DHS)では、Office of Cybersecurity and Communications(CS&C)の International Affairs Programs が国際的な窓口となっているほか、ICS-CERT は通常、United States Computer Emergency Readiness Team(US-CERT)が持つコネクションを活用するべく US-CERT と協働することが多い。しかし、今年は ICS-CERT の国際連携の取組の一環として、国際原子力機関(IAEA)による原子力システムのサイバーセキュリティ問題を検討する初のカンファレンスに参加した。また、Forum of Incident Response and Security Teams(FIRST)の年次総会に参加し、60 ヶ国以上から集まった Computer Security Incident Response Team(CSIRT)と交流を図るなどして、国際連携に取り組んでいる。

読者や読者の組織が ICS-CERT の国際連携の取組に関心がある場合は、以下のアドレスまで連絡を: ICS-CERTInternational@hq.dhs.gov 。

[3] NIST SP800-92: Guide to Computer Security Log Management
http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf

（2）CSET 7.0 リリース

ICS-CERT では、2015 年 8 月に Cyber Security Evaluation Tool（CSET）の最新版 7.0 をリリースした。7.0 では以下が追加・更新されている。

- 基準・標準等の追加
  - Cybersecurity Capability Maturity Model（C2M2） 1.1 版
  - Department of Defense（DoD） Instruction 8510.01：国防総省（DoD）IT のためのリスク管理フレームワーク
  - NIST IR 7628 vo.1, rev.1 版：スマートグリッドのサイバーセキュリティガイドライン
- ユーザーインターフェースの全面改訂

  今風で、より直感的なインターフェースに刷新。大きなセクションの区切りごとに新たなランディングページを用意し、次のセクションの観点や意義などの説明を提示。
- 質問ページの機能拡充
  - 質問事項（評価要件）のカスタマイズ機能
  - テキストサイズの変更機能　ほか
- 評価結果ファイルの暗号化機能の追加

ダウンロードは、https://ics-cert.us-cert.gov/assessments より。

## 4. 最近公開された脆弱性

※原文の Recent Product Releases を参照ください。

## 5. オープンソースニュース（ハイライト）

- 米連邦航空局（FAA）、航空機へのサイバー攻撃防止に関する委員会を開催（2015/6/29）
  http://thehill.com/policy/cybersecurity/246415-faa-convenes-panel-to-thwart-airline-cyberattacks

## 6. 協調的な脆弱性の公開に協力頂いたセキュリティ研究者の方々

ICS-CERT では、発見した脆弱性を一般への公開前にベンダに通知し、パッチや対策版の提供を可能にする「協調的な脆弱性の公開（Coordinated Vulnerability Disclosure）」を奨励しており、そのための仕組みを提供している。様々な事情により困難な場合もあるかもしれないが、是非活用頂き、協調的な公開への協力をお願いしたい。

2015 年 7 月、8 月に協調的な公開に協力頂いた研究者の方々については、原文の Coordinated Vulnerability Disclosure を参照のこと。

## 7. 今後のイベント

※原文の Upcoming Events を参照ください。

以上