2015 年 4 月 9 日
独立行政法人情報処理推進機構（IPA）

ICS-CERT モニター（2014 年 9 月～2015 年 2 月号）概要

本概要は、米国土安全保障省の運営する ICS-CERT（Industrial Control Systems Cyber Emergency Response Team）発行の“ICS-CERT Monitor September 2014 – February 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/sites/default/files/Monitors/ICS-CERT_Monitor_Sep2014-Feb2015.pdf

1. インシデント対応活動

（1）2014 会計年度（FY2014）のインシデント対応／脆弱性ハンドリングの総括

FY2014（2013 年 10 月～2014 年 9 月）に報告されたインシデントは 245 件で、業界としてはエネルギー業界がもっとも多く 79 件（32%）、次いで重要製造業界が 65 件（27%）であった（その他の業界は、2 件（1%）～15 件（6%））。約 55%が APT（Advanced Persistent Threat）または高度な攻撃者によるものであったが、ログなど調査に必要なデータが無いため攻撃者像が特定できないケースも多かった（97 件（38%））。

侵入の手口は様々で、例として以下のような手口が見られた。

- インターネットに繋がっている制御システムを介した不正アクセス
- 制御システム機器およびソフトウェアの脆弱性の悪用
- 物理的に独立した制御システムのマルウェア感染
- ウェブアプリケーションの脆弱性の悪用
- ネットワークからネットワークへの侵入（セグメント超え）
- スピアフィッシング
- 水飲み場型攻撃など戦略的なウェブサイトの改ざん

245 件というのはあくまで ICS-CERT に報告されたインシデントの数であり、氷山の一角と思われる。報告してもらえれば、報告者に類似の事例や別のインシデントで使われた手口や特徴などの情報を提供できるほか、ICS-CERT によるインシデント対応や対策強化といった支援も提供可能。共有された情報は重要インフラ情報保護（CIIP）プログラムに基づき、法や裁判等による情報公開要求から保護される。重要インフラ事業者には、不審な活動に気がついたら積極的に ICS-CERT に報告するようお願いしたい。

一方、FY2014 に報告された制御システムの脆弱性は 159 件であった。製品としてはエネルギー業、重要製造業、上下水道業で利用されているシステムが多く、脆弱性の種別としては認証、バッファオーバーフロー、サービス不能（DoS）の脆弱性が多かった。

その他、FY2014 には Havex や BlackEnergy を使用した、ICS を狙ったと見られるマルウェアキャンペーンが発覚した。ICS-CERT では、リモート／オンサイト支援を通じて Havex および BlackEnergy の解析を行い、攻撃手法、使用されたツール、マルウェアの機能、推奨対策・回避策などを発信し、対策を促した。

（2）セキュリティ意識向上への取組み

重要インフラ業界におけるセキュリティ意識向上のための取組みとして、ICS-CERT では FBI と連携し、全米を巡って重要インフラ事業者・関係者とミーティングを行う“Action Campaign”を実施した。2014 年 12 月 1 日～11 日に掛けて、シアトル、デンバー、シカゴ、カンザスシティ、タンパなど 15 都市を回り、2 時間のミーティングの中で ICS を狙ったマルウェアキャンペーンの詳細や、攻撃の検知・対策方法等について、機密情報を交えて情報を提供。どの都市でもすぐに定員が埋まり、合計で 16 業界から約 1,600 名が参加した。なお、他にも幅広い情報の展開を目的に、機密情報は扱わないミーティングや、Web セミナー（webinars）も実施した。

（3）ICS-CERT によるセキュリティレビュー

ICS-CERT では 2014 年 9 月～2015 年 2 月に掛けて、37 のオンサイト評価を行った。うち 18 は Cyber Security Evaluation Tool（CSET）によるレビュー、13 は Design Architecture Review（DAR）によるレビュー、6 は Network Architecture Verification and Validation（NAVV）によるレビューであった。

- CSET レビュー
  政府基準・業界標準に照らして、セキュリティ対策状況を確認可能なツール「CSET（Security Evaluation Tool）」を使用した汎用的な評価
- DAR レビュー
  設計や構成、相互依存性やアプリケーションなど、対象組織の ICS ネットワークに特化した、より詳細な評価
- NAV レビュー
  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

2. ICS-CERT ニュース

（1）オバマ大統領、重要インフラのサイバーセキュリティ強化に向けた新たな大統領令を発布

2015 年 1 月 13 日に National Cybersecurity and Communications Integration Center（NCCIC）で行ったスピーチの中で、オバマ大統領が新たなサイバーセキュリティ法の制定を提案。サイバー攻撃を米国の経済と安全保障を脅かす最も深刻な脅威の 1 つと位置付け、米国の重要インフラを守るため、官民におけるサイバー攻撃・脅威情報の共有強化の必要性を訴えると共に、政府が企業から提供を受けた情報を悪用することはないと請負う。その後 2 月 13 日のスタンフォード大学におけるサミットで、情報共有強化を進める大統領令に署名。

NCCIC におけるスピーチ
https://www.whitehouse.gov/the-press-office/2015/01/13/remarks-president-national-cybersecurity-communications-integration-cent
スタンフォード大学のサミットにおけるスピーチ
https://www.whitehouse.gov/the-press-office/2015/02/13/remarks-president-cybersecurity-and-consumer-protection-summit

（2）セキュリティイベントにおける ICS 機器を用いた“「ハノイの塔」チャレンジ”の開催

ICS-CERT では、ニューヨーク大学工科大学（NYU Polytechnic School of Engineering）が主催する学生運営のサイバーセキュリティイベント「Cyber Security Awareness Week Conference（CSAWC）」において、フエニックスコンタクト社と連携し、セキュリティコンペティションを開催。フエニックスコンタクト提供の PLC に ICS-CERT が仕掛けた「ハノイの塔」的なチャレンジを解くコンペティションで、クリアするとゲットできるトークンの獲得を目指し、15 の学生チームが挑戦。8 チームが最終日まで掛かったものの、クリアに成功。参加した学生の 1 人は疲れ果てた顔ながら、「難しかったが楽しかった！」と話した。

（3）CSET に要望する機能（アンケート）

ICS-CERT では今年 1 月に CSET 6.2 を公開した。昨年秋のICSJWG(Industrial Control System Joint Working Group)において更新内容の説明を行い、その際に利用者が「あると良い」と考える機能についてのアンケートを行った。

要望が多かった機能は以下（約 80%～95%が「あるとよい」と回答）:

- 自社の制御システムアーキテクチャがどうあるべきか、テンプレートを提示してくれる機能
- ファイアウォールやスイッチの設定を読み込ませると、解析を行い、設定ミスを指摘したり、推奨される対策や優先度などを提示してくれる機能
- CSET ダッシュボード上に表示される ICS-CERT の注意喚起とアドバイザリについて、自社に関係のあるものだけに絞って表示できる機能
- ネットワークトラフィックを解析して pcap ファイルを生成し、CSET に取り込んでネットワークダイアグラムとして表示できる機能
- 独自の質問セットを作成し、CSET と一緒に配布できる機能
- ICS-CERT からの攻撃・脅威情報をリアルタイムに取得し、優先度に変更があれば教えてくれる機能

（4）ICSJWG Fall 2014 Meeting／ICSJWG Spring 2015 Meeting

Fall 2014 Meeting は 2014 年 10 月 7 日～9 日にアイダホ州アイダホフォールズで行われ、約 175 人が参加した。同年の Spring Meeting で好評であったデモやライトニングトークを増やしてより参加型なカンファレンスとし、参加者同士の情報交換が促進できた。次回 Spring 2015 Meeting は、6 月頃の開催を予定。

3. 最近公開された脆弱性

※原文の RECENT PRODUCT RELEASES を参照ください。

4. オープンソースニュース(ハイライト)

- S4x15 ビデオ： カスペルスキーが取組む制御システム用の独自 OS（2015/2/25）
  http://www.digitalbond.com/blog/2015/02/23/s4x15-video-kaspersky-control-system-os/
- 米沿岸警備隊、海事セキュリティにおけるサイバーセキュリティ問題を語る（2015/1/15）
  http://inhomelandsecurity.com/us-coast-guard-addresses-maritime-cybersecurity-issues/
- Windows7 メインストリームサポートの終了（2015/1/14）
  http://windows.microsoft.com/en-us/windows/lifecycle
- ポッドキャスト： セキュリティと産業用モノのインターネット（IIoT）（2015/1/13）
  http://csis.org/multimedia/enabling-internet-things-conversation-marty-edwards
- 米エネルギー省、エネルギー業界向けのサイバーセキュリティフレームワーク実施要綱を公開（2015/1/8）
  http://www.energy.gov/oe/downloads/energy-sector-cybersecurity-framework-implementation-guidance
- 制御システムにおける測定データの破損（2015/1/5）
  http://chemical-facility-security-news.blogspot.jp/2015/01/measurement-data-corruption.html 他
- 2015 年に我々が直面する最も重大なセキュリティ脅威（2015/1/4）
  http://www.wired.com/2015/01/security-predictions-2015/他
- キルチェーンの活用（2014/12/12）
  http://www.darkreading.com/attacks-breaches/leveraging-the-kill-chain-for-awesome/a/d-id/1317810 他
- セキュリティ研究者、既知の正規の ICS/SCADA ファイルのデータベースを公開（2014/12/1）
  https://threatpost.com/researcher-releases-database-of-known-good-ics-and-scada-files/109652
- リモートファイルアクセスのセキュアでない現実（2014/11/14）
  http://www.net-security.org/secworld.php?id=17637

- Nuix 社調査： 境界セキュリティに限界 ― セキュリティ対策に変化（2014/11/13）
  http://www.scmagazine.com/73-percent-of-survey-respondent-say-infosec-needs-have-changed/article/383231/他
- ハッカー辞典：ゼロデイとは？（2014/11/11）
  http://www.wired.com/2014/11/what-is-a-zero-day/他
- SANS Institute InfoSec Reading Room： テスト駆動開発（TDD）ならぬ攻撃駆動開発（EDD：Exploit Driven Development）によるセキュアなソフトウェアの開発（2014/11/11）
  http://www.sans.org/reading-room/whitepapers/application/secure-design-exploit-infusion-35587
- 重要インフラを脅かす BlackEnergy（2014/11/9）
  http://www.gsnmagazine.com/node/42887
- ハッカーら、新しいシンプルなフィッシング手法を考案（2014/11/5）
  http://www.darkreading.com/attacks-breaches/hackers-devise-new-simplified-phishing-method/d/d-id/1317242
- なぜ二要素認証が大事なのか（2014/10/21）
  http://www.infosecisland.com/blogview/24045-Why-Two-Factor-Authentication-is-Too-Important-to-Ignore.html 他
- トレンドマイクロ： Sandworm Team、SCADA システムが標的か（2014/10/20）
  http://www.securityweek.com/sandworm-team-targeted-scada-systems-trend-micro 他
- Project SHINE、インターネットに繋がっている重要な制御機器の多さ・深刻さを浮き彫りに（2014/10/7）
  http://www.securityweek.com/project-shine-reveals-magnitude-internet-connected-critical-control-systems

5. 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、脆弱性を ICS-CERT に報告してベンダと調整を行う、協調的な脆弱性の公開（Coordinated Vulnerability Disclosure）に協力くださったセキュリティ研究者の方々に感謝の意を表し、当該研究者の方々の功績として、氏名と対象の脆弱性の一覧を掲載しています。実際の氏名および脆弱性については、原文の COORDINATED VULNERABILITY DISCLOSURE を参照ください。

6. 脆弱性対策に協力頂いたセキュリティ研究者の方々

RESEARCHERS CURRENTLY WORKING WITH ICS-CERT

ICS-CERT appreciates the following researchers who continue to work with us to resolve exploits:

Adam Crain	Chris Sistrunk	Marc Ayala
Aditya Sood	Darius Freamon	Matthew Luallen
Alexander Tlyapov	Dillon Beresford	Neel Mehta
Alexey Osipov	Eric Forner	Ralf Spenneberg
Andrea Micalizzi	Glib Gritsai	Reid Wightman
Artem Chaykin	Ilya Karpov	Ricardo Narvaja
Avair Liimets	Ivan Sanchez	Sergey Gordeychick
Billy Rios	Jim Denaro	Stephen Roettger
Bob Radvanovsky	Joel Langill	Terry McCorkle
Brian Meixell	Kirill Nesterov	Timur Yunusov
Cesar Cerrudo	Laisvis Lingvevicius	Tudor Enache

7. 今後のイベント

※原文の UPCOMING EVENTS を参照ください。

以上