2014 年 3 月 13 日
独立行政法人情報処理推進機構（IPA）

ICS-CERT モニター（2013 年 10 月/11 月/12 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 October, November, December 2013”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：
http://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Oct-Dec2013.pdf

1. インシデント対応活動 ― 2013 年度の傾向 ―

（1）概要

2013 年、ICS-CERT では計 256 件のインシデント対応を行った。インシデントの報告は、事業者から直接受けたケースもあれば、関連組織から受けたケースもある。大多数のインシデントは業務ネットワークで検知されており、ICS-CERT では、侵入が業務ネットワークから制御ネットワークに及んでいないか、また、業務ネットワークから制御ネットワークの情報が収集されていないかに焦点を当てて調査を行った。主な侵入手口は、インターネットに繋がっている機器への不正アクセス、外部記憶媒体を通じたマルウェア感染、脆弱性の悪用、スピアフィッシング等であった。

これらはあくまで報告された件数であり、実際にはもっと発生していると考えられる。また、検知力やログ収集力の不足により、検知できていないインシデントも多いと推測される。

（2）業界

インシデント 256 件のうち、151 件（59%）はエネルギー業界であった。報告件数が群を抜いている背景には、エネルギー業界におけるセキュリティ意識の向上、および ICS-CERT とエネルギー業界の間の信頼関係の向上もあると見られる。また、重要機器製造メーカも 50 件（20%）と 2 番目に多く、制御システムやサプライチェーンをつけ狙う攻撃者らの存在を伺わせる。

（3）特筆点

インシデント 256 件のうち、79 件は「侵入を確認」または「侵入された疑いが高いと判断」、57 件は「侵入がなかったことを確認」、残り 120 件は「どちらとも判断不能」または「不明」となっており、攻撃の検知力およびログ収集力の不足が浮き彫りとなっている。手口は、直接標的システムを狙うのではなく、水飲み場型攻撃やスピアフィッシングなど、あらゆる攻撃ルートを通じて標的組織に侵入し、ネットワークやシステムを“移動”して最終標的となるシステムを狙う。

インターネットに繋がったシステムや機器も引き続き多く存在しており、ICS-CERT では事業者に対して機密情報の共有を含む説明会を行い、セキュリティ意識の更なる向上を支援すると共に、各事業者における対策およびインシデントの報告が進むことを願います。

（4）Network Architecture Verification and Validation（NAVV）を活用した原子力発電所の評価

ICS-CERT では、オンサイト評価の中で NAVV を利用した評価を行っている。NAVV は、制御システムネット

ワークのトラフィックを分析するツールであり、Cyber Security Evaluation Tool（CSET）、Design Architecture Review（DAR）と共に、ICS-CERT が提供する評価ツールの 1 つである。CSET は、組織のサイバーセキュリティレベルを、国家的に幅広く認められている基準やガイドラインに照らして評価し、改善のための推奨施策を提言する。DAR はより深く、制御システムネットワークの多層防御対策に焦点をあて、ネットワークへのアクセスや外部への通信、設計、設定、ルールなどの検証、システムの相互依存性、脆弱性や回避策など、包括的な評価を行う。ある発電所の評価では 60 ギガバイト超のデータを収集し、外部への不審な通信を検知した。

2. トピックス

（1）制御システム環境におけるアプリケーションホワイトリスト（後編）

アプリケーションホワイトリスト（AWL）の概念はシンプルだが、許可するアプリケーションの判断やホワイトリストのメンテナンスなど、実装には課題が多い。以下に課題解決のためのアプローチを示す。

- 守る機器の絞り込み（重要なサーバ、システム、フィールド機器にアクセスするコンピュータ等）
- マスターイメージ（gold image）の作成（バックアップ用として存在していればそれで可）
- ポリシー（ホワイトリスト）の策定
- 監視モード（monitor-only mode）での運用
- テスト環境での運用
- 利用可能なセキュリティ設定（ベンダ推奨設定）の適宜有効化
- 防御モード（secure mode）での運用
- 微調整の実施
- 変更・テスト・微調整の繰り返し

ICS 環境は IT 環境と比べて予測可能で変更が少ないため、AWL に適しているとも言える。AWL で全ての攻撃が防げる訳ではないが、対策の 1 つとして上手に活用されることが望まれる。

なお、AWL とウィルス対策ソフト、および AWL とセキュリティパッチは、セキュリティ対策として相互補完的なものであり、相互排他的なものではない。どちらか一方ではなく、組み合わせて使うことが肝要となる。

（2）破壊型マルウェアへの備え

Shamoon（正式名称「W32.DistTrack」）や最近の CryptoLocker に見られるように、破壊型マルウェアの脅威は企業にとって既に現実的な脅威である。このような破壊型マルウェアに備えるには、万一の場合の迅速な復旧を可能にするべく尽力することである。先ずはビジネス影響度分析（BIA）を行い、自社のインフラ、重要なアプリケーションやデータ、相互依存性、問題点を把握する。戦略としては、システムコンポーネントのセキュリティ対策とモニタリングに重点を置き、特に、運用に必要な情報資産の多くに影響を及ぼすようなコンポーネントに留意する。また、モニタリングと復旧計画が有効か確認するため、実践的なテストを行うことを忘れてはならない。ICS-CERT と US-CERT では、破壊型マルウェアに備えるにあたってのガイドラインを提供しているのでそちらを参照のこと。

（3）CSET 6.0 ― 新しい機能が追加

Cyber Security Evaluation Tool（CSET）は、幅広く使われている既存の基準やガイドラインと、ステップ・バイ・ステップのウィザードを使って、自組織のサイバーセキュリティ対策状況を体系的に評価できるようにしたツールである。6.0 では、新しく、以下の基準が追加された。

- CNSSI 1253[1]
- CNSSI ICS Overlay アップデート
- NEI 08-09[2]
- NISTIR 7628[3]
- INGAA[4]
- NIST SP800-53 R4[5]
- NIST SP800-82[6] など

また、過去と現在の評価を比較し、対策による改善の可視化を可能にするなど、機能も追加された。

- ビデオチュートリアル(You Tube)の提供
- 評価事項(設問)を、当該分野の担当者らに振り分け、後から回答をマージする機能を追加
- 事業単位や部門単位に行った評価を統合し、組織全体の評価を可能にする機能を追加 など

3. 最近公開された脆弱性

※原文の RECENT PRODUCT RELEASES をご参照ください。

4. オープンソースニュース(ハイライト)

- 米連邦捜査局(FBI)、国土安全保障省(DHS)および国家テロ対策センター(NCTC)、テロよりサイバー攻撃の方が脅威と議会に宣言(2013/11/26)
- 北大西洋条約機構(NATO)、史上最大規模のサイバーセキュリティ演習を実施(2013/11/26)
- 重要インフラのサイバー物理システム(CPS)に対する脅威が増加(2013/11/21)
- 米国に対するサイバー攻撃の実状把握のため、議会が連邦ネットワークへの攻撃の報告を義務付ける法案を検討(2013/11/8)
- 北米電力信頼度協議会(NERC)、スマートグリッドにサイバー攻撃。36 時間にわたるサイバー演習を実施(2013/11/7)
- 重要インフラ防護施策:元米国土安全保障省サイバーセキュリティ担当副次官 Mark Weatherford 氏インタビュー(2013/11/6)
- ユーザが最大最弱の脅威:米標準技術研究所(NIST)がセキュリティ教育・訓練のガイドライン(ドラフト)を公開(2013/11/5)
- 制御システムが狙われる - ハッカーの次の標的は貴方の会社のシステムかも(2013/11/4)
- 大統領宣言 ー 重要インフラセキュリティ・レジリエンス月間(2013/10/31)
- 米標準技術局(NIST)、Cybersecurity Framework(ドラフト)を公開(2013/10/31)
- セキュリティ vs. エンドユーザ(2013/10/25)
- サイバー攻撃の発信元、インドネシアが中国を抜いてトップに(2013/10/18)
- 重要インフラシステムで使用される通信プロトコルに脆弱性。北米の発電所にサイバー攻撃によって乗

[1] Committee on National Security Systems Instruction (CNSSI) 1253 - Security Categorization and Control Selection for National Security Systems
[2] Nuclear Energy Institute (NEI) 08-09 - Cyber Security Plan for Nuclear Power Reactors
[3] National Institute of Standard and Technology Interagency Report (NISTIR) 7628 - Guideline for Smart Grid Cyber Security
[4] Interstate Natural Gas Association of America
[5] National Institute of Standard and Technology Special Publication (NIST SP) 800-53 - Recommended Security Controls for Federal Information Systems and Organizations
[6] National Institute of Standard and Technology Special Publication (NIST SP) 800-52 -Guide to Industrial Control Systems (ICS) Security

っ取られるリスク（2013/10/18）

- Project SHINE、多くの SCADA/ICS 関連機器がインターネットからアクセス可能になっている現状を暴く（2013/10/16）
- サウジアラムコ社に対するデータ破壊型のマルウェア攻撃、石油・ガス業界に自組織がサイバー攻撃の標的になり得るとのセキュリティ意識を持たせる転機に（2013/10/14）
- サイバー脅威の質、より破壊的で危険な方向に変化（2013/10/11）
- マイクロソフト社、国家のサイバーセキュリティ戦略策定にあたってのベストプラクティスガイドを公開（2013/10/4）
- 雇われハッカー集団による政府関連組織への攻撃（2013/9/30）
- ドイツの研究者、ネットワークカードなどの周辺機器に潜むマルウェアを検知する手法をデモ（2013/9/26）
- サウジアラビアのサウジアラムコ社、カタールのラスガス社、米国のシェブロン社など、大手石油会社に対するサイバー攻撃が業界に警鐘（2013/9/23）
- 安全な「長い」パスワード、場合によってはサーバーを DoS 状態に陥らせる可能性も（2013/9/17）
- シマンテック社、中国の雇われハッカー集団 Hidden Lynx がオーロラ作戦など有名なサイバースパイ活動の背後にいた可能性を指摘（2013/9/17）
- ヘルスケア業界、Windows XP からの移行を進める　ー　60%は「間に合う」と回答、残りは 2015 年後半まで掛かる見込み（2013/9/9）

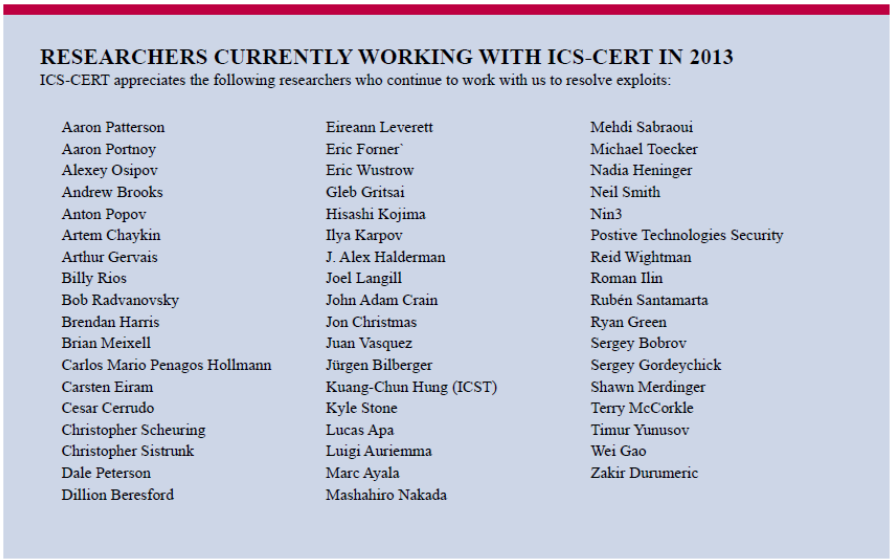
5. 今後のイベント

※原文の UPCOMING EVENTS をご参照ください。

6. 協調的な脆弱性の公開（CVD）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、ベンダとの調整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・脆弱性については、原文の COORDINATED VULNERABILITY DISCLOSURE を参照ください。

7. 脆弱性対策に協力頂いたセキュリティ研究者の方々（2013 年）



RESEARCHERS CURRENTLY WORKING WITH ICS-CERT IN 2013

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

Aaron Patterson	Eireann Leverett	Mehdi Sabraoui
Aaron Portnoy	Eric Forner`	Michael Toecker
Alexey Osipov	Eric Wustrow	Nadia Heninger
Andrew Brooks	Gleb Gritsai	Neil Smith
Anton Popov	Hisashi Kojima	Nin3
Artem Chaykin	Ilya Karpov	Postive Technologies Security
Arthur Gervais	J. Alex Halderman	Reid Wightman
Billy Rios	Joel Langill	Roman Ilin
Bob Radvanovsky	John Adam Crain	Rubén Santamarta
Brendan Harris	Jon Christmas	Ryan Green
Brian Meixell	Juan Vasquez	Sergey Bobrov
Carlos Mario Penagos Hollmann	Jürgen Bilberger	Sergey Gordeychick
Carsten Eiram	Kuang-Chun Hung (ICST)	Shawn Merdinger
Cesar Cerrudo	Kyle Stone	Terry McCorkle
Christopher Scheuring	Lucas Apa	Timur Yunusov
Christopher Sistrunk	Luigi Auriemma	Wei Gao
Dale Peterson	Marc Ayala	Zakir Durumeric
Dillion Beresford	Mashahiro Nakada	

以上