2015 年 11 月 30 日
独立行政法人情報処理推進機構（IPA）

ICS-CERT モニター（2015 年 9･10 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 September/October 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-MM201510

1. インシデント対応活動

（1） 直近の事例

ある事業者が、US-CERT Secure Portal[1]で共有された“indicators of compromise”（マルウェアや攻撃を受けたシステムから抽出された、脅威や攻撃（侵入）の存在を示す痕跡情報）を用いて、自社ネットワークをスキャンしたところ、部分一致が検出された。事業者からディスクイメージ等の提出を受け、ICS-CERT で解析を行ったところ、侵入された形跡は見られず、攻撃ではなかったと結論付けられた。今回は幸いにも侵入されていなかったが、適切なログの取得、情報の共有、日常的なスキャンの実施、問題発見時の対応計画／手順の確立が、インシデントの早期検知・早期対応を可能にすることを示した。

（2） ICS-CERT によるセキュリティレビュー

2015 年 9 月・10 月は、5 業界で 13 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、エネルギー業界が 5 件、水道業界が 3 件、重要製造業が 2 件、政府機関・施設が 2 件、IT 業界が 1 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、Design Architecture Review（DAR）によるレビューが 6 件、Network Architecture Verification and Validation（NAVV）によるレビューが 5 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

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

[1] US-CERT の登録制ポータルサイトで、一般公開前、または未公開の脆弱性情報や攻撃情報なども提供。重要インフラ事業者および関連企業・組織で、登録を望者する場合は ics-cert@hq.dhs.gov まで。

2. セキュリティトピックス

（1） マルウェア動向

この 10 年の間、従来の PC からモバイル機器やスマート機器へと、人々の社会との関わり方は大きく変わった。技術の進歩と人々によるインターネットの利用拡大はサイバー攻撃の可能性も大きく広げ、金銭目的の犯罪者、テロリスト、国家など、目的によらず攻撃者にとってサイバー攻撃を非常に魅力的な手段としている。攻撃者は目的に合わせて様々なマルウェアを作成し、機能によってトロイの木馬、バックドア、スパイウェア、ランサムウェア等と呼ばれている。ランサムウェアは感染したユーザのデータを暗号化し、復号と引き換えに身代金（ランサム）の支払いを要求する手口で、2014 年第 4 四半期から 2015 年第 1 四半期の間に種類が 165%増加した。セキュリティソフトによるマルウェア検知技術も向上を続けているが、マルウェアによる検知を掻い潜る手法も進化を続けている。近年は現在のシステムのセキュリティ構造上検知が困難な BIOS や USB、ハードドライブなど、接続機器のファームウェアに潜伏するマルウェアも見られ、新たな課題となっている。

攻撃者が狙う“価値ある情報”についても、モバイル機器やソーシャルネットワークサービスの普及、情報の電子化等によって、より多様で大量のデータが生成されるようになっている。この傾向は、スマート家電やコネクテッドカー、モノのインターネット（IoT）につながる機器の増加により、一層の加速が見込まれる。こうして収集・共有される情報は、更に便利なサービスの享受を可能にする一方で、攻撃者に攻撃に有用な情報をもたらす諸刃の剣となる。新規に確認された Android マルウェアの数は 2015 年第 1 四半期から第 2 四半期の僅か 3 ヶ月で 27%増加するなど、只ならぬ割合で急増している。

従来、重要インフラの制御システムは外部ネットワークから切り離されており、一見、こうした傾向の影響を受けないように思われる。しかし、制御システムも業務システムとの連携による効率化、IoT の適用による産業改革（IIoT）、遠隔地の機器のリモートメンテナンス等のため、外部と「つながる」方向に急速に進んでいる。重要インフラの制御システムは社会や人々の生活にとって重要なだけに、攻撃者（テロリスト、国家、ハクティビスト等）の格好の標的となり得るため、サイバー攻撃対策が必須となる。とは言え、やるべきことはこれ迄と変わらない――ベストプラクティスを確実に行うことである。ICS-CERT Monitor 2015 年 7 月・8 月号で述べたように、ログを適切に取得し、管理者がネットワーク、機器、システムにおける不審な事象に気付ける環境を整備し、迅速に対処することが重要となる。

（2） サポート終了製品の廃棄ポリシー

多くの企業にはサポート終了（EoL）製品に関するポリシーが存在すると思われる。しかし、実際に使用を止める際にどうするか、手順までは定めていない企業は要注意である。

デジタル・ボンド社の K. Reid Wighman 氏、マンディアント社の Chris Sistrunk 氏、Context Industrial Security 社の Michael Toecker 氏の報告によれば、3 氏が eBay で中古の SCADA サーバが 20 ドル（約 2,500 円）以下で売りに出されているのを発見し、購入したところ、機微な情報の宝庫であったという。設定ファイルや単線結線図等のデータが簡単なパスワードもしくはパスワード無しの状態で存在したほか、前所有者と見られる会社およびシステム管理者の名前も筐体のタグに書かれていた。インターネットで連絡先を調べて連絡したところ、管理者は、機器は捨てる前に社内の廃棄物集積場でサニタイズしたとして、データが完全な状態で残っていたことに驚いていたという。この企業では EoL ポリシーは存在するが、サニタイズの手順等は特に決められていなかった。

以下に、EoL ポリシーに含めておくべ事柄を幾つか挙げる。

- 慎重な取扱いを要する機器のリスト（そうした扱いが必要な理由も記す）
- そうした機器の写真（産業用サーバにはモニターやキーボードが無い場合もあり、サーバと認識されずに必要な処理が漏れるのを防ぐ）
- 設定情報やバックアップ用パスワードの削除方法、工場出荷状態に戻す（初期化）方法
- 従業員に対し、各機器のマニュアルを読んでおくよう指示すること（機器によっては、設定情報やメンテナンスパスワード等の削除など、別々の操作を必要とすることがあるため）
- ハードドライブ、メディア、USB、メモリカードなどを全て外すこと
- 制御システムのセキュリティを研究している大学等を後援し、古い機器を寄付する。その際、機微な情報が残っていた場合には教えてくれるよう条件をつける

こうした項目も加え、具体的かつ必要な事柄を全てカバーした EoL ポリシーを整備し、実施することで、使用製品がサポート終了前／終了済によらず、機微な情報が外部に流出するのを防ぐことができる。

3. ICS-CERT ニュース

（1） DEF CON および Black Hat への参加

ICS-CERT では昨年に引き続き、リサーチコミュニティの動向の把握、研究者とのネットワーキング、講演におけるゼロデイ脆弱性の公表への対応などのため、8 月に米ラスベガスで開催された DEF CON および Black Hat に参加した。DEF CON、Black Hat 共に非常に認知度の高いイベントに成長し、参加者も前者が 22,000 人以上、後者が 11,000 人以上と盛況であった。娯楽的な価値が高い一方で、サイバーセキュリティ情報の収集および専門家と知り合う場としての価値も高い。今年も多くの研究者と意見を交わすことができ、直接会って話すことで、より理解を深め、重要な問題について話し合うことができた。また、講演の中で公表された脆弱性について、6 つの注意喚起（Alert）を発行した。

（2） ICS-CERT Virtual Learning Portal（VLP）のアップグレード

UCS-CERT では e-ラーニングプログラム「Virtual Learning Portal（VLP）」をアップグレードし、GUI の改善等などを行った。また、旧コース（「ICS サイバーセキュリティ（210W）」）を 10 の個別コースに分割した。「210W-01」から順に受講することが望ましいが、独自のラーニングパスを策定することも可能。

ICS サイバーセキュリティ（210W）

- 210W-01：ICS における違い
- 210W-02：共通の IT コンポーネントの ICS における影響
- 210W-03：共通の ICS コンポーネント
- 210W-04：IT／ICS の各ドメインにおけるサイバーセキュリティ
- 210W-05：サイバーセキュリティリスク
- 210W-06：ICS における現在の脅威傾向
- 210W-07：ICS における現在の脆弱性動向
- 210W-08：サイバーセキュリティインシデントの影響の判断
- 210W-09：IT および ICS における攻撃方法
- 210W-10：IT 環境における多層防御対策の ICS 環境へのマッピング

受講は、ICS-CERT VLP（https://ics-cert-training.inl.gov/lms/）にて（登録要）。

（3） 経営幹部のための ICS サイバーセキュリティ 6 箇条

ICS-CERT では、Industrial Control Systems Joint Working Group（ICSJWG）の意向を受け、経営幹部向けの説明資料として、“ICS-Cybersecurity for the C-Level”を作成した。これは、経営幹部に対して制御システムのセキュリティ対策を改善が必要であることを効果的に伝える、「簡潔な」資料が入用だというICS 関係者からの強い要望に答えるものである。

資料では、高度なマルウェアを用いた攻撃の事例、ICS のセキュリティ対策の鍵となるポイント、対策に役立てることができる ICS-CERT の提供サービス等をまとめている。

ICS-Cybersecurity for the C-Level
https://ics-cert.us-cert.gov/sites/default/files/FactSheets/ICS_C-Level_FactSheet_20150915_S508C.pdf

（4） NCCIC/ICS-CERT に関するニュース記事

- 国土安全保障省（DHS）サイバーセキュリティ・通信室（OC&C）次官補 兼 国家サイバーセキュリティ・通信統合センター（NCCIC）ディレクター アンディ・オスメント博士のインタビュー
  http://www.govtech.com/blogs/lohrmann-on-cybersecurity/Where-Next-for-Government-Cybersecurity.html
- ICS-CERT マーティ・エドワード ディレクター執筆記事
  https://www.controldesign.com/articles/2015/u-s-government-resources-for-cybersecurity/
- 医療機器のサイバーセキュリティに関する ICS-CERT マーティ・エドワード ディレクターのコメント
  http://breakthroughs.kera.org/smart-medical-devices-call-for-smarter-cyber-security/

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）

- 医療機器のサイバーセキュリティ規制が実現しない事情（2015/10/19）
  http://motherboard.vice.com/read/why-arent-there-better-cybersecurity-regulations-for-medical-devices
- WaterISAC: サイバーセキュリティ ― 10 の基本的対策（2015/10/14）
  https://ics-cert.us-cert.gov/sites/default/files/documents/10_Basic_Cybersecurity_Measures-WaterISAC_June2015_S508C.pdf
- 海軍艦艇の新しい防衛対策: サイバー攻撃からの保護（2015/9/18）
  http://www.ecnmag.com/news/2015/09/new-defense-navy-ships-protection-cyber-attacks?et_cid=4823349&et_rid=745317555&location=top

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。

以上