2016 年 1 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 11･12 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 November/December 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-MM201512

1. インシデント対応活動

（1） 直近の事例

ICS-CERT のセキュリティ評価チームが、ある事業者の Network Architecture Validation and Verification（NAVV）中に、不審な通信を発見。インシデント対応チームを呼びパケットキャプチャにより取得したデータやログの解析を行った結果、システムがマルウェアに感染し、インターネット上の不審な IP アドレスと通信を行っていることが判明。感染経路の特定はできなかったものの、本件を機に、事業者のセキュリティ強化につなげることができた。

ICS-CERT によるセキュリティ評価やインシデント対応、マルウェア解析の支援を希望する事業者は、https://ics-cert.us-cert.gov/ で詳細を確認し、申込みを。

（2） ICS-CERT によるセキュリティ評価

2015 年 11 月･12 月は、4 業界で 18 件のセキュリティ評価を実施した。

業界別では、水道業界が 11 件、化学業界が 4 件、エネルギー業界が 2 件、IT 業界が 1 件であった。

また、評価の種別では、Cyber Security Evaluation Tool（CSET）による評価が 5 件、Design Architecture Review（DAR）による評価が 8 件、Network Architecture Verification and Validation（NAVV）による評価が 5 件であった。

- CSET
  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確認するツール「CSET」を使用した汎用的な評価サービス
- DAR
  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
- NAV
  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

各評価の詳細については、https://ics-cert.us-cert.gov/Assessments を参照のこと。

2. セキュリティトピックス

＜医療機器の脆弱性と ICS-CERT による取扱い＞

ICS-CERT は、世界中のセキュリティ研究者から脆弱性の届出を受ける。ICS-CERT が届出に対して報奨金を支払ったり、特定の分野やベンダ製品の調査を依頼している訳ではなく、基本、研究者は脆弱性が是正されることを願って届け出を行っている。自社の製品に脆弱性を発見したベンダ自身が、より広くユーザに周知する手段として届け出ることもしばしばある。

この数年間、医療機器の脆弱性の届出は急増している。サイバーセキュリティの世界において医療機器は比較的新しい分野となる。医療機器の脆弱性を公表することで患者が危険に晒されるリスクが高まるのではとの懸念も示されていることから、ICS-CERT では医療分野のベンダに対し、ICS-CERT が脆弱性の公表を調整する目的や情報の取扱方針を理解してもらうべく努めている。

ICS-CERT が届け出られた脆弱性についてベンダに通知すると、ベンダは発見者について知りたがるが、ICS-CERT が仲介することはベンダ・研究者どちらにとってもメリットがある。ベンダは公表前に対策版を開発し、配布する時間を稼げるし、研究者は発見者としてスキルと協力を政府機関に評価されるほか、1 箇所に報告するだけで済む。ベンダが脆弱性に関して通知を受けたのち、対策が完了する前にベンダの同意なしに研究者が脆弱性を暴露するのを防ぎたいのであれば、最良の方法は進捗（対策版の準備状況と、脆弱性公表時期）を ICS-CERT と共有することである。前述したように研究者の目的は「脆弱性が是正されること」であり、状況がわかれば、ICS-CERT がより上手く両者の間を取り持つことが可能となる。

脆弱性を公表することで患者（利用者）を危険に晒すとして、わざわざ公表することを疑問視する声もある。しかし、問題が存在することを知らなければ、利用者はその問題に対して何もできない。脆弱性公表の信条は、問題の存在と対策を周知し、利用者が自分の身を守れるようにすることで、利用者を守ることにある。また、ベンダから、「自社製品の利用者は全て把握しており別途通知しているのに、一般にまで脆弱性の存在を公表する必要があるのか」と問われることも多い。ICS-CERT のこれ迄の経験から言えば、企業は売られたり買われたり名前が変わったりするほか、製品が転売されることもあり、ベンダが自社製品の全利用者を正確に把握するのは非常に困難である。ICS-CERT アドバイザリであれば幅広く発信されるほか、National Vulnerability Database（NVD）[1]にも登録されるため、利用者の目に留まるチャンスは上がる。

ICS-CERT による脆弱性取扱いの目的は、医療業界を含む米国の 16 の重要インフラを守り、セキュリティを強化することにある。他の業界同様、医療機器の脆弱性を低減し、セキュリティを強化する最善の方法は、ベンダと協力して発見された脆弱性を解消し、影響を受ける関係者や一般と広く情報を共有していくことである。

3. ICS-CERT ニュース

（1） FY2015 のインシデント対応（統計）

FY2015（2014 年 10 月～2015 年 9 月）の ICS-CERT によるインシデント対応件数は 295 件で、うち 97 件（33%）は重要製造業であった（原文 Figure 1）。同業界の前年度（65 件、27%）[2]からの急増は、期間中に行われた重要製造業に対する大規模な標的型攻撃に起因するものと推察される。

---

[1] 米標準技術研究所（NIST）が運営する脆弱性対策情報データベース。 https://nvd.nist.gov/home.cfm

[2] ICS-CERT Monitor September 2014 – February 2015
https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Sep2014-Feb2015.pdf

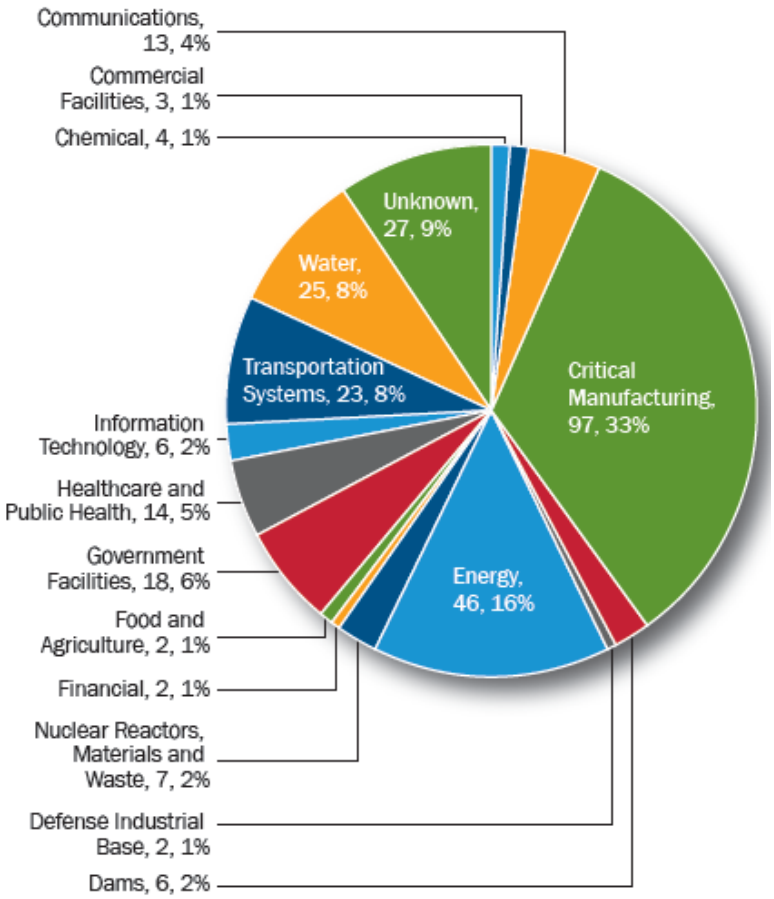

Figure 1. FY 2015 Incidents by Sector, 295 total.

侵入のレベルに関しては、攻撃されたものの侵入は確認されなかったケースが増加（FY2014：49% → FY2015：69%）したのは良しとして、制御システムへの侵入が確認されたケースも増加（FY2014：9% → FY2015：12%）している点が懸念される（原文 Figure 3）。

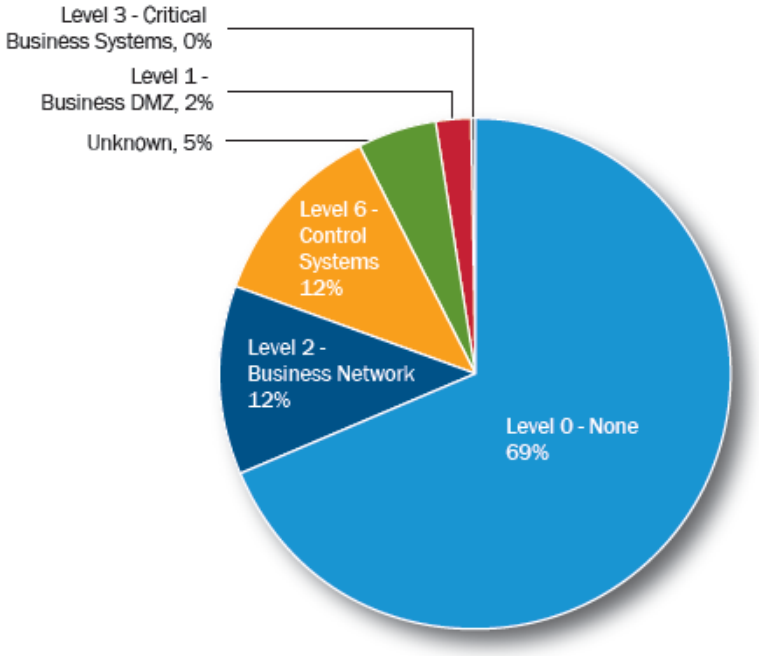

Figure 3. FY 2015 Observed Depth of Intrusion.

インシデントの中には、制御システムネットワークがインターネットや業務ネットワークに直接つながっているなど、ネットワーク構成の問題に起因するケースも相当数あった。また、38%のケースでは解析に必要なログ等が取られておらず、侵入経路を特定できなかった。セキュリティ対策の基本を守り、制御システムの外部ネットワークからの分離およびネットワークのモニタリング、ホストベースの侵入検知の導入等により、いち早い侵入の検知および対応、後日の解析を可能にすることが重要となる。

（2） ICS-CERT FY2015 のハイライト

- オバマ大統領が国家サイバーセキュリティ・通信統合センター（NCCIC）[3] Watch Floor を視察
- BackEnergy および Harvex に関する事業者への教育・啓発活動（Action Campaign）により、政府表彰を受賞（次点）
- 295 件のインシデント対応（FY2014 から 20%増加）
- 321 件の脆弱性取扱い（FY2014 から 39%増加）
- 112 件のセキュリティ評価の実施（内訳：CSET 38 件、DAR 46 件、NAVV 28 件）
- Virtual Learning Portal を連邦政府のクラウドアプリケーション基準に沿うようアップグレード
- CSET6.2 および 7.0 リリース。120 ヶ国で 7,400 枚以上を配布
- フロリダ州ペンサコーラに NCCIC Watch Floor を拡張
- NCCIC が、国土安全保障省（DHS）の長官直轄部門に昇格

（3） 制御システムセキュリティを大学の履修科目として試験的に開設

ブリガム・ヤング大学アイダホ校で、2015 年秋期の履修科目（専門科目）として、制御システムセキュリティを学ぶコースが試験的に開設される。ICS-CERT が履修内容を策定し、講師も務める。生徒は、先ず制御システムネットワークについて学んだ後、制御システムネットワークの外部ネットワークからの分離、マルウェア解析、フォレンジックデータの収集、インシデント対応等について、様々なツールを使用してハンズオン形式で学ぶ。履修した学生は、「制御システムの存在は知っていたが、制御システムを守るためのセキュリティ戦略がどれほど（IT システムと）異なるのか、初めて理解できた」と話す。

（4） ICSJWG 2016 Spring Meeting 開催日決定

次回、Industrial Control Systems Joint Working Group（ICSJWG） 2016 Spring Meeting の開催日と場所は以下に決定。

【日時】2016 年 5 月 3 日（火）～5 日（木）
【場所】アリゾナ州スコッツデール
【URL】https://ics-cert.us-cert.gov/Industrial-Control-Systems-Joint-Working-Group-ICSJWG

詳細は決まり次第、上記ウェブページに掲載予定。

4. 最近公開された脆弱性

※原文の Recent Product Releases を参照ください。

[3] ICS-CERT は、NCCIC を構成する 4 部門の 1 つ

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、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 11 月、12 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。

6. 今後のイベント

※原文の Upcoming Events を参照ください。

トレーニングコースの開催日程については、https://ics-cert.us-cert.gov/Calendar をご確認ください。

以上