2016 年 3 月 30 日
独立行政法人情報処理推進機構（IPA）

ICS-CERT モニター（2016 年 1･2 月号）概要

本概要は、米国土安全保障省（DHS） Industrial Control Systems Cyber Emergency Response Team（ICS-CERT）発行の“*ICS-CERT Monitor January/February 2016*”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-MM201602

1. インシデント対応活動

（1） 直近の事例 ～ 事業者も知らないリモートアクセスの口や遠隔操作通信の存在が発覚 ～

ICS-CERT では、ローカルコミュニティに電力および水道サービスを提供している事業者から要請を受け、制御ネットワークへの攻撃の侵入状況を調査するべくオンサイト調査を行った。許可を得てネットワーク監視装置を設置し、ホストおよびネットワークデータの収集、ICS 機器の調査等を行ったところ、水道ネットワーク全体で軽度のマルウェア感染が見つかった。電力ネットワークには感染の痕跡はなかった。

電力の配電･送電制御センターでは、事業者が電力ネットワークとは繋がっていないと信じていたワイヤレスルータが実は繋がっており、制御ネットワークに外部から直接アクセス可能であったことが判明した。また、水道の制御センターでは、制御スイッチ（main water switch）にセルラーモデムが接続されているのが見つかった。事業者にも何のために設置されたものか分からず調査したところ、ベンダのリモートアクセス用であることが判明した（アクセス制限は簡単な ID/PW だけであった）。他にも、運用端末や請求書システム等の攻撃価値の高いホストと外部のホストの間で TeamViewer（PC の遠隔操作を可能にするフリーソフト）による通信が発生しているのが見つかった。これらの通信は事業者が正規の通信でないことを確認し、直ちに遮断した。

事業者は ICS-CERT による調査報告とベストプラクティスの提示を受けて対策に取り組むことを決め、改めて ICS-CERT に支援を要請した。

（2） ICS-CERT によるセキュリティ評価

2016 年 1 月･2 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 7 件、政府施設が 5 件、化学業界が 4 件、通信業界が 2 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

- NAVV
  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

＜インシデントへの備え＞

例え最良のサイバーセキュリティ対策を導入していたとしても、インシデントは起こる。“その時”に備えて準備を行い、計画を立てておくことが、インシデント対応に必要不可欠となる。問題の迅速な検知、損害の最小化、悪用された脆弱性や問題の低減、システムやサービスの復旧には、インシデントの発生源を特定し、影響／被害の範囲を確認する能力が必要であり、適切な準備と計画を行うことで必要な情報が必要な時に利用できるようになる。

インシデント対応チームには、重要な判断をタイムリーに行えるよう、技術部門の上位の責任者を入れる必要がある。また、必要に応じて問題となっている事柄の専門家、IT 側の関係者、広報、法務、警察等を加える。インシデント対応担当者はツール等の使い方について日頃から訓練を行い、必要時に困らないようにするほか、インシデントに備えて準備しておくべきことのチェックリストを作成し、年 1 回は机上演習を通じて見直しを行うことが望ましい。外部組織（CSIRT[1]やパートナー企業等）が必要とするだろう情報など、インシデント発生時に収集すべき情報のリストも作成しておくとよい。

非常時用の通信手段を検討しておくことも重要である。インシデントに関する通信は、こちらが攻撃に気付いたことを攻撃者に気付かせないよう、既に攻撃者に侵入されている可能性のある通信システム（メールや VoIP など）は使用しないことが望ましい。また、インシデント対応に関するファイルはネットワーク上に置かないようにするべきである。

ログはインシデント対応の重要な要素となる。システムやネットワークのログはもちろんのこと、ファイアウォール、プロキシ、DNS、DHCP、ウェブアプリケーション、音声・映像、侵入検知システム、侵入防止システム、ホスト、アプリケーション等のログの取得を検討することが望まれる。制御システムでは機器やシステムにログ機能があればそれが使えるが、無い場合にはネットワークのログが唯一の手掛かりとなる可能性があるため、ルータやスイッチ、パケットキャプチャによるログやデータの取得も検討する。また、ログが改ざんされては意味がないため、定期的にバックアップを行い、ハッシュ値を取って別のシステムに保管することが望まれる。

最後に、「証拠」として使うためには、データを適切に収集・保管することが必須となる。データフォレンジックに詳しいコンサルタント等に相談し、アドバイスを受けることが望ましい。

[1] Computer Security Incident Response Team。セキュリティインシデントに対応するための専門チーム／組織。社内組織であったり、商用組織（サービス）であったり、（半）公的組織であったり、様々な形態の CSIRT がある。

3. ICS-CERT ニュース

（1） CSET 7.1 公開

ICS-CERT は、2016 年 2 月に CSET の最新版 7.1 をリリースした。CSET は、ステップ・バイ・ステップのプロセスを通じて、事業者が組織の IT/OT のセキュリティ対策状況を様々なサイバーセキュリティ基準に照らして確認することを可能にするツールである。

CSET 7.1 で更新されたのは以下:

- NIST SP800-161「Supply Chain Risk Management Practices for Federal Information Systems and Organizations」追加
- NERC CIP Violation Risk Factors に基づく対策の優先度づけ
- ダッシュボードの改善
- 対策要件の並び替え機能（基準ごと）の追加
- パラメーター値のカスタマイズ機能（頻度など、基準でカスタマイズが認められている値）
- ネットワークコンポーネントのひな型の増加（ICS、IT、医療など）

（2） S4 カンファレンスに参加

ICS-CERT は、2016 年 1 月にマイアミビーチで開催された S4 Conference（S4x16）に参加した。ICS セキュリティ業界を代表する人物らによる基調講演をはじめ、新たな脆弱性や最新の技術などについての発表がなされた。ICS-CERT もこの機会を活用し、最近の動向に関して情報収集を行ったり、未知の脆弱性の公表について調整を行ったり、ベンダと良好な関係の構築を図ったり、他の CERT との交流を深めたりすることができた。

（3） GovDelivery

ICS-CERT が注意喚起やアドバイザリを公開した場合、以前は US-CERT Security Portal から通知が送られていたが、現在では送られていない。これは、ICS-CERT が新しい購読システム「GovDelivery」を立ち上げたためである。登録希望者は以下から手続きを:

https://public.govdelivery.com/accounts/USDHSUSCERT/subscriber/new

（4） ICSJWG 2016 Spring Meeting 開催日決定

次回、Industrial Control Systems Joint Working Group（ICSJWG）2016 Spring Meeting の開催日と会場は以下に決定した。

【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 Chaparral Suites Scottsdale（近い内に Embassy Suites Scottsdale に改名予定）
【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。

（5） ICS-CERT Fact Sheets

ICS-CERT では、ICS のセキュリティ対策に関する 8 種類の Fact Sheet を公開している。ICS-CERT のウェブサイトからは、トップページ → メニューの「Information Products」 → 「Fact Sheets」タブ からアクセス可能。

1. Industrial Control Systems Cyber Emergency Response Team
   ICS-CERT、および ICS-CERT が提供するセキュリティ支援サービスの紹介
   https://ics-cert.us-cert.gov/sites/default/files/FactSheets/ICS-CERT_FactSheet_ICS-CERT_S508C.pdf
2. Preparing for Cyber Incident Analysis
   インシデントに備え、行っておくべきことおよび留意事項
   https://ics-cert.us-cert.gov/sites/default/files/FactSheets/ICS-CERT_FactSheet_Cyber_Incident_Analysis_S508C.pdf
3. Industrial Control Systems Joint Working Group
   ICS-CERT が後援する制御システムセキュリティのための官民パートナーシップ「Industrial Control Systems Joint Working Group（ICSJWG）」の紹介
   https://ics-cert.us-cert.gov/sites/default/files/FactSheets/ICS-CERT_FactSheet_ICSJWG_S508C.pdf
4. Control Systems Architecture Analysis Services
   ICS-CERT が提供する制御システムのセキュリティ評価サービス「Design Architecture Review（DAR）」および「Network Architecture Verification and Validation（NAVV）」の紹介
   https://ics-cert.us-cert.gov/sites/default/files/FactSheets/ICS-CERT_FactSheet_CS_Architecture_Analysis_Services_S508C.pdf
5. Cyber Security Evaluation Tool
   ICS-CERT が開発・提供する制御システムセキュリティの自己評価ツール「Cyber Security Evaluation Tool（CSET）」の紹介
   https://ics-cert.us-cert.gov/sites/default/files/FactSheets/ICS-CERT_FactSheet_CSET_S508C.pdf
6. Cyber Resilience Review and Cyber Security Evaluation Tool
   DHS が提供する運用面のレジリエンス（レジリエンス・マネジメント）評価サービス「Cyber Resilience Review（CRR）」の紹介
   https://ics-cert.us-cert.gov/sites/default/files/FactSheets/ICS-CERT_FactSheet_CRR_CSET_S508C.pdf
7. Training
   ICS-CERT が提供する制御システムのセキュリティに関するトレーニングコース（初級～上級）の紹介
   https://ics-cert.us-cert.gov/sites/default/files/FactSheets/ICS-CERT_FactSheet_Training_S508C.pdf
8. Strategy for Securing Control Systems
   制御システムのリスクマネジメントに関するガイド
   https://ics-cert.us-cert.gov/sites/default/files/FactSheets/ICS-CERT_FactSheet_Securing_CS_S508C.pdf

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. 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。

※2016 年 1 月、2 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 を参照ください。

6. 今後のイベント

※原文の Upcoming Events を参照ください。

以上