2016 年 5 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 3･4 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 March/April 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-MM201604

## 1. インシデント対応活動

＜水道事業者がランサムウェアに感染 ～ バックアップ／復旧計画の重要性 ～＞

水道事業者で、ビジネスシステムと顧客データがランサムウェアによって暗号化される事例が発生。当該事業者ではランサム（身代金）を払わずに復旧を行った。ビジネスシステムは感染の殆どが仮想マシンで、バックアップも直近まで存在したため、データ喪失はあったものの許容できる程度に留まり、迅速に復旧することができた。一方、顧客データはバックアップが古く復旧が限定的となり、多くのデータを失う結果となった。

バックアップ計画および復旧計画は、インシデント対応計画に不可欠な要素である。バックアップ計画を立てる際には、コスト（工数、ストレージ費用）、データの可用性（データ喪失に対する許容度）等をよく考慮し、バックアップの取得方法（フル、差分）、取得タイミング、リストア演習の実施などを検討することが重要となる。

## 2. セキュリティトピックス

（1） ICS-CERT におけるインシデント・ハンドリング

何事もなくそろそろ 1 日の業務を終えようという頃、小さな地方自治体の水道システムの管理者から、ポンプ場のコントロールパネルから通常と異なる IP アドレス宛に大量の通信が流れ始めたと連絡が入った。数分のうちにネットワーク構成図が ICS-CERT に送付され、IP アドレスのホワイトリスト化および通信ポートの変更（標準ポート→別ポート）が行われた。数日後にはフォレンジックイメージが送付され、ICS-CERT Advanced Analytics Laboratory（AAL）でマルウェアのリバースエンジニアリングやログの解析を行い、攻撃者、侵入方法、不正アクセスされたデータを特定し、同様の攻撃を防ぐための対処方法を検討した。

制御システムのセキュリティに単純な解決策はなく、開発者から現場のエンジニアまであらゆる関係者の努力、堅固なシステム設計、徹底したライフサイクルマネジメント、能動的なネットワーク監視、しっかりとしたインシデント対応、包括的な対策など、1 つ 1 つの取組みが全体のセキュリティ確保に寄与している。

（2） 重要インフラ情報保護プログラム

事業者が ICS-CERT とのインシデント情報の共有やセキュリティ評価サービスの利用を渋る理由の 1 つは、機密情報や機微な情報が適切に守られないのではないかとの危惧にある。そうした懸念を払拭すべく、国土安全保障省（DHS）では 2002 年の重要インフラ情報（CII）法の下、重要インフラ情報保護（PCII）プログラムを立ちあげた。PCII プログラムでは、共有された情報に対して厳格なセキュリティ対策と取扱い条件を課すとともに、情報公開法（FOIA）、州や地方レベルの情報公開法、規制措置、民事訴訟などによる情報公開

の対象外とし、情報が一般に公開されないことを保証している。

ICS-CERT は米国の重要インフラを守ることをミッションとしている。ICS-CERT との協同に興味がある組織は、共有された情報は守られるものと安心してほしい。

（3） 強固なパスワードの使用

どんなに長くランダムなパスワードも、必要な時間とコンピューティングパワーを費やせば解読することは可能である。これを無効化するためには、パスワードを定期的に変更することが望ましい。また、否認防止（nonrepudiation）の観点から、ID／パスワードの共用は認めるべきではない。

＜パスワードの条件＞

- 最低 12 文字
- 大文字、小文字、記号、数字を織り交ぜる
- 辞書に載っているような一般的な言葉は使わない
- 簡単に推測できないものにする
- 覚えていられるものにする（紙等に書き留めておかなくても大丈夫なものにする）

＜パスワードの取扱い＞

- 定期的に変更する
- 他人のパスワードを使わない
- 他人に見せない
- 上述の条件を満たすパスワードを使用する

## 3. ICS-CERT によるセキュリティ評価

2016 年 3 月・4 月は、6 業界で 18 件のセキュリティ評価を実施した。

業界別では、エネルギー業界が 6 件、化学業界が 3 件、通信業界が 3 件、政府施設が 2 件、運輸業界が 2 件、水道業界が 2 件であった。

評価の種別では、Cyber Security Evaluation Tool（CSET）による評価が 4 件、Design Architecture Review（DAR）による評価が 7 件、Network Architecture Verification and Validation（NAVV）による評価が 7 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。

## 4. ICS-CERT ニュース

＜ウクライナ電力網へのサイバー攻撃＞

2015 年 12 月 23 日に発生したウクライナの電力システムに対するサイバー攻撃について、米政府は国土安全保障省（DHS）、連邦捜査局（FBI）、エネルギー省（DOE）を筆頭にクライナ政府と協働し、事件の解明にあたってきた。2016 年 3 月 31 日から 4 月 29 日にかけて、ICS-CERT と FBI では事業者や州・地方政府関係者の脅威に対する意識向上のためミーティングやウェブセミナー（webinar）を行い、今回の攻撃の事象、手口、リスク低減のための戦略や対策などの情報提供を行った。

参加できなかった関係者は、US-CERT/ICS-CERT Secure Portal に掲載している「IR-ALERT-H-16-043-01BP：Cyber-Attack Against Ukrainian Critical Infrastructure」を参照のこと。また、本件やその他の ICS に関する問題について ICS-CERT とミーティングを希望する場合は、ICS-CERT@hq.dhs.gov まで。

## 5. 最近公開された脆弱性やレポート等

※原文の Recent Product Releases を参照ください。

## 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。

※2016 年 3 月、4 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。

## 7. オープンソースニュース（ハイライト）

- Ponemon Institute のアンケート調査によれば、経営幹部（C-level executives）の 3 分の 1 がサイバーセキュリティインシデントについて一度も知らされたこと無し（2016/4/6）
  http://www.esecurityplanet.com/network-security/34-percent-of-c-level-executives-are-never-updated-on-security-incidents.html

## 8. 今後のイベント

※原文の Upcoming Events を参照ください。

以上