2015 年 6 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 3･4 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 March/April 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-MM201504

1. インシデント対応活動

（1）ネットワーク機器の設定ミスによる制御システム障害

水道事業者で、ネットワークインフラのアップグレード時にスパニングツリープロトコル（STP）の設定を誤り、ネットワークの輻輳によって制御システム（ICS）に障害が発生した。マルウェア感染を疑った事業者から ICS-CERT に支援依頼があり、ICS-CERT にてルータおよびスイッチの設定をレビューしたところ、設定ミスが発見された。事業者にて修正を行い現在は問題なく稼動中。ICS-CERT では、インフラに変更を加える際の留意点として、以下を推奨する：

- 既存システムとの互換性や設定に問題が無いよう、新システムのインテグレータとよく相談する
- 設定変更によって問題が生じないか、可能であればテスト環境でテストを行う
- 設定変更を実行する際にはインデグレータにも現場に居てもらい、インテグレータがいなくなってもあらゆる問題に対応できるよう、スタッフに情報やガイダンスを提供する

（2）ICS-CERT によるセキュリティレビュー

2015 年 3 月、4 月にかけて、ICS-CERT では 4 業界で 21 件のオンサイト評価を実施した。うち 8 件は Cyber Security Evaluation Tool（CSET）によるレビュー、7 件は Design Architecture Review（DAR）によるレビュー、6 件は Network Architecture Verification and Validation（NAVV）によるレビューであった。

- 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ことができるツール「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、相互依存性やアプリケーションなど、組織の ICS ネットワークに特化した、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データの解析による、機器間の通信フローの洗い出しと見直し

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

2. 多要素認証における留意事項

多要素認証はパスワード認証（単一要素認証）よりセキュアな認証方法として推奨されることが多い。しかし IC カードを使用している場合、Windows の実装ではアカウントにアサインされる乱数（パスワード値）が固

定のため、再生成のため定期的に SmartcardLogonRequired 設定の変更を行わないと、有効期限ごとに乱数が再生成されるパスワード認証よりもむしろ脆弱度が高くなってしまう。

Windows でシングルサインオン＋多要素認証を実施している場合、または実施を検討している場合、マイクロソフト社の情報等を参照し、多要素認証を有効に利活用できるよう注意する必要がある。詳細は、以下のベンダ情報を参照。

Microsoft Security TechCenter: Path-the-Hash（PtH）
https://www.microsoft.com/pth

3. ICS-CERT ニュース

（1）ICSJWG Spring Meeting 2015

次回の ICSJWG Spring Meeting 2015 は、6 月 23 日～24 日に、ワシントン D.C.の Wilbur J. Cohen Federal Building で開催される。また、非公開ミーティング（米国市民対象）を、6 月 25 日に別の会場で開催予定。詳細は、以下の ICSJWG ウェブサイトを参照。

ICSJWG
https://ics-cert.us-cert.gov/Industrial-Control-Systems-Joint-Working-Group-ICSJWG

（2）ICS-CERT Regional Training

ICS-CERT では、制御システムの設計者、運用者、監督者向けに、無料のセキュリティトレーニングを年に数回、全米各地で開催している。コースは以下の 3 種:

- 初級コース（101：Introduction to Industrial Control Systems Cybersecurity）
  時間：8 時間　形態：講義　定員：100 名　開催日：月、火
- 中級コース（201：Intermediate Cybersecurity for Industrial Control Systems）
  時間：8 時間　形態：講義　定員：100 名　開催日：月、火
- 中級コースⅡ（202：Intermediate Cybersecurity for Industrial Control Systems）
  時間：8 時間　形態：講義＋ハンズオントレーニング　定員：40 名　開催日：水、木

トレーニング内容の詳細、およびスケジュールについては、以下を参照。
https://ics-cert.us-cert.gov/Training-Available-Through-ICS-CERT
https://ics-cert.us-cert.gov/Calendar

（3）Cyber Security Evaluation Tool（CSET） 6.2

CSET は、ICS および IT システムで実施しているセキュリティ対策状況を、広く受け入れられている業界標準に照らして、ステップバイステップで確認できるセキュリティ評価支援ツールである。今年 1 月にリリースされた CSET 6.2 は、新しく以下の機能等が追加されている。

- 対応標準
  - North American Electric Reliability Corporation（NERC） CIP Version 5[1]
  - Committee on National Security Systems Instruction（CNSSI） No. 1253 Version 2[2]

[1] http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx
[2] http://www.sandia.gov/FSO/PDF/flowdown/Final_CNSSI_1253.pdf

- 図表機能
  - コンポーネントの説明を記載できる「description」フィールド
  - 新しいコンポーネントステンシル（Visio2013 でも利用可能）
- インポート／エキスポート機能
  - Visio 2013 とのダイアグラムのインポート／エキスポート機能
- 国防総省（DoD）ツール対応
  - Enterprise Mission Assurance Support Service （eMass）からのインポート機能

CSET の詳細、またはダウンロード（無料）は以下より。
https://ics-cert.us-cert.gov/Assessments

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）

- 米国とイスラエルのイラン核施設に対する共同作戦が公にされるのではとの懸念が高まる中、米統合参謀本部の元副議長に対する情報漏洩事件の捜査に二の足（2015/3/10）
  http://www.washingtonpost.com/world/national-security/leak-investigation-stalls-amid-fears-of-confirming-joint-us-israel-operation/2015/03/10/2a348b1e-c36c-11e4-9ec2-b418f57a4a99_story.html

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）」を奨励しおり、そのための仕組みを提供している。様々な事情に困難な場合もままあるが、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 3 月、4 月に協調的な公開に協力くださった研究者の方々については、原文の Coordinated Vulnerability Disclosure を参照。

7. 今後のイベント

※原文の Upcoming Events を参照ください。

以上