2014 年 6 月 12 日
独立行政法人情報処理推進機構（IPA）

ICSJWG 四半期ニュースレター（2014 年 3 月）概要

本概要は、米国土安全保障省の運営するICSJWG（Industrial Control Systems Joint Working Group）発行の“ICSJWG Quarterly Newsletter, March 2014 の概訳となります。内容の詳細につきましては、原文をご確認ください。

原文は、ICSJWG にメールでリクエストし、入手する形となります。詳細は以下のページをご覧ください。

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

◆ICSJWG 2014 Spring Meeting

ICSJWG 2014 Spring Meeting は、6 月 3 日～5 日に、インディアナ州インディアナポリスにて開催。プログラムには、これまで同様の講演、パネルディスカッション、デモ、パネル展示、Lunch & Learn（昼食を取りながらの勉強会）に加え、今回初めて Lightning Round Talk（ライトニングトークとそれを受けてのラウンドテーブルディスカッション）を予定。産業用制御システム（ICS）に関する最新の技術やベストプラクティス、ツール、課題、興味深い話題を関係者と共有する機会を提供。

◆ICSJWG Webinar（ウェブセミナー）

記念すべき第 1 回 ICSJWG Webinar となる「我思う、ゆえに我ファジングす！（I Think, Therefore I Fuzz!）」が、3 月 27 日の 13：00～14：00 に開催。Southfork Security 社の Corey Thuen 氏が、ファジングの概要や、脆弱性の発見を通じてファジングがセキュリティ向上に果たす役割や効果を解説。

◆Cyber Security Evaluation Tool（CSET）6.0

CSET の最新版 6.0 がリリース。初めて民間の商用規格として、Interstate Natural Gas Association of America（INGAA）の「天然ガス業界向け制御システムサイバーセキュリティガイドライン [1]」、および Nuclear Energy Institute（NEI）の「原子炉のサイバーセキュリティ設計 [2]」の 2 つが取り入れられている。また、標準技術研究所（NIST）の NIST IR7628（「スマートグリッドのサイバーセキュリティガイドライン」）が追加されたほか、NIST SP800-53（「連邦政府情報システムにおける推奨セキュリティ管理策」）、NIST SP800-82（「産業制御システムセキュリティガイド」）Rev.1 についても追加等がなされた。

機能面も向上しており、複数の評価が行えるだけでなく、複数拠点の評価を比較したり、複数の評価の統合や、時間軸を設定して改善状況の分析することなどが可能。

また、国土安全保障省（DHS）では、ICS-CERT のセキュリティ専門家による CSET を使ったオンサイトでのセキュリティ評価サービスを提供。所要時間は大体 1 日で、依頼組織の費用負担はなし。希望者は ICS-CERT@hq.dhs.gov まで。

---

[1] Control Systems Cyber Security Guidelines for the Natural Gas Industry
[2] Cyber Security Plan for Nuclear Power Reactors

◆ICS サイバーセキュリティトレーニング　オンラインコース

ICS-CERT では、講義形式で提供している「初級コース」（101）、「中級コース」（201）の e-Learning 版となるサイバーセキュリティトレーニングコース「ICS セキュリティ」（201W）の提供を開始。

ICS-CERT Virtual Learning Portal：https://ics-cert-training.inl.gov/ （登録要）

◆FY2014 年度[3] ICS サイバーセキュリティトレーニング　上級コース

ICS-CERT では、米アイダホ州アイダホフォールズの Control Systems Analysis Center において、今年度も攻撃側（レッドチーム）と防御側（ブルーチーム）による対戦演習を含む、「上級コース」（301）を提供する。

＜トレーニング内容＞

- 1 日目：挨拶、ICS-CERT および ICS システムセキュリティの概要、インターネットを介した ICS システムへのサイバー攻撃のデモ、ネットワーク発見手法の体験学習など
- 2 日目：ネットワーク上の脆弱性発見手法の体験学習、Metasploit の使い方の学習、レッドチーム／ブルーチームへのチーム分け
- 3 日目：ネットワーク侵入手法、ネットワーク防御手法の体験学習、レッドチーム／ブルーチームに分かれての作戦会議
- 4 日目：レッドチーム／ブルーチームに分かれての 12 時間にわたるサイバー演習
- 5 日目：演習から学んだことなどを話し合うラウンドテーブルディスカッション

＜直近の開催日＞

~~2014 年 5 月 19 日～23 日~~：終了済

2014 年 6 月 9 日～13 日（北米）：〆切済

*2014 年 7 月 14 日～18 日（北米）：〆切済

*2014 年 9 月 8 日～12 日（北米）：6 月中旬より受付開始予定

*カレンダーより IPA 補記分

各コースは北米の受講希望者向け（北米）、または北米以外からの受講希望者向け（国際）のどちらか向けとなっており、申込みにあたっては、記載区域からの希望者が優先される。また、日付と内容は変更される場合があるため、詳細はカレンダー（http://ics-cert.us-cert.gov/Calendar）を確認のこと。

◆Homeland Security Information Network（HSIN）

HSIN は、ICSJWG が使っている米国の官民情報共有プラットフォーム。ミーティングの通知や、議事録、当日の資料、開発中や完成したドキュメント類がアップされる。利用申請は、氏名・所属企業・重要インフラ業界などを沿え、ICSJWG.Communications@dhs.gov まで。

◆マンスリーモニター＆ツイッターによる情報発信

ICS-CERT では、最新の活動状況を紹介するため、ニュースレター（ICS-CERT Monitor Newsletter）を発行している。入手は、ICS-CERT ウェヴサイト（http://ics-cert.us-cert.gov/）より。

また、ICS-CERT に関する最新情報は、ツイッター（@ICSCERT）でもフォロー可能。

[3] 2013 年 10 月～2014 年 9 月

◆ICS セキュリティに関する寄稿記事

本号には、以下 6 件の記事が寄稿されている。詳細は原文を参照のこと。

- 「The C³ Voluntary Program: 重要インフラのサイバーセキュリティ強化のための官民パートナーシップ」
  The C³ Voluntary Program, a Public-Private Partnership to Strengthen Critical Infrastructure Cybersecurity
  Thad Odderstol, Director, Industry Engagement & Resilience, DHS

  ※IPA 補足:
  2014 年 2 月に公開された「NIST Cybersecurity Framework」の普及・促進プログラム。大統領令第 13636 号(EO13636)により、Cybersecurity Framework の策定は標準技術研究所(NIST)、運用(普及・促進)は DHS の役割となっている。

- 「大統領令第 63 号(PDD-63)から 16 年 ー北米電力業界は NERC CIP を放棄すべきか(結論:絶対にすべきでない)」
  Sixteen Years Later: Abandon the CIP or Stay the Course
  Venkat Pothamsetty, Industrial Defender

- 「コンプライアンスとセキュリティ: 『悪』はコンプライアンスにあらず ー コンプライアンスをセキュリティにつなげるために」
  Positioning yourself in the battle of compliance vs. security
  Perry Pederson

- 「PLC セキュリティ:ICS ネットワークに侵入されることを前提に、制御機器の抜本的な脆弱性対策を」
  PLC Security: Are you treating the symptom or the cure?
  Dr. Alex Tarter, Technical Director Cybersecurity Programs, Ultra Electronics

- 「サイバー攻撃から ICS システムを守る ー DualDiode による制御ネットワークと業務ネットワークのセキュアな分離事例」
  Protecting Industrial Control Systems from Cyber-Attack
  Erica Taguiam

- 「デジタルとアナログ ー どちらかでなく、よりリスクが低く『安全』を守れる技術の適宜活用を」
  Back to the Future: Putting analog hard stops to cyber attacks
  Perry Pederson

次号、ICSJWG 四半期ニュースレター(6 月号)への記事の寄稿の〆切は、6 月 13 日。掲載希望者は、ICSJWG.Communications@dhs.gov まで。

以上