2015 年 1 月 30 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 12 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, December 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

◆2014 の活動

2014 年度は、インディアナ州インディアナポリス、アイダホ州アイダホフォールズで会合を開催。ライトニングトークの取り入れや、デモンストレーションの増加、最新施設の見学ツアーの企画など常に新しいことを行い、活気があり、多くの人に参加してもらえるよう会合であり続けるよう取組みを推進。

◆ICSJWG Webinar（ウェブセミナー）

ウェブセミナーでは、ICS におけるファジング、リアルタイム監視、セキュリティパラダイムのシフトなど、ICS のサイバーセキュリティに関する講演を実施。2015 年も、サイバーセキュリティ普及のため行っていく予定。詳細は、ICSJWG からのアナウンスを参照。

◆Cyber Security Evaluation Tool（CSET）6.1

現在、CSET の最新版 6.1 を提供中。CSET 6.1 は、標準技術研究所（NIST）の「サイバーセキュリティ・フレームワーク[1]」および「NIST SP800-82 産業用制御システムセキュリティガイド（Revision2 ドラフト版）[2]」）の 2 つの基準に新たに対応したほか、組織独自の要求事項の作成が可能になっている。

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 を使用したオンサイトでのセキュリティ評価サービスを提供。所要時間は約 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[3]。

◆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」（210W）の提供を開始。このコースでは、ICS セキュリティの基本として、IT システムと ICS の違い、ICS に特有な脆弱性対策や対策について学ぶ。申込みは以下より。

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

---

[1] Framework for Improving Critical Infrastructure Cybersecurity
http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf
同文書の日本語仮訳を IPA のホームページで公開しています。
https://www.ipa.go.jp/security/publications/nist/

[2] NIST SP800-82 Guide to Industrial Control Systems (ICS) Security (Revision 2 Initial Public Draft)
http://csrc.nist.gov/publications/drafts/800-82r2/sp800_82_r2_draft.pdf

[3] 依頼資格（依頼企業の国籍等）の有無については、ICSJWG にご確認ください

◆FY2015 年度[4] 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。本コースは、ハンズオントレーニングのほか、協同作業を通じた、同業者や関係者とのネットワーキングの機会を提供。

＜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＞

*2015 年 1 月 12 日～16 日：〆切り済

*2014 年 2 月 9 日～13 日：〆切り済

2015 年 3 月 9 日～13 日：受付中

*カレンダーより IPA 補記分

※2015 年より、北米以外からの受講希望者向けのコース（従来の“International Partners“）の設定を廃止し、毎回、人数を限定して北米以外からの受講者を受け入れる運用に変更。
スケジュールの変更を含め、詳細は http://ics-cert.us-cert.gov/Calendar を確認のこと。

◆Homeland Security Information Network（HSIN）

HSIN は、ICSJWG が利用し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、資料、策定中や完成したドキュメント類がアップされる。HSIN の利用申請は、氏名・所属企業・重要インフラ業界などを記載のうえ、ICSJWG.Communications@dhs.gov まで[5]。

◆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。

[4] FY2015：2014 年 10 月～2015 年 9 月
[5] 申請資格（申請者・所属組織の国籍等）の有無については、ICSJWG にご確認ください

◆ICS セキュリティに関する寄稿記事

本号には、以下 3 件の記事が寄稿されている。詳細は原文を参照のこと。

- 「物理セキュリティシステムに対するサイバー脅威」
  Cyber Threats to Physical Security Systems
  Jorge Lozano

- 「情報のレジリエンス　ー　情報は今日の情報経済の中心であり、そのレジリエスの確保はもはやビジネス上の絶対条件」
  Information Resilience - A Business Imperative in Today's Information Economy
  Nader Mehravari, CERT Cyber Risk and Resilience management Team、CMU

- 「制御システムのセキュリティ対策上、やってはいけない 10 のこと」
  Ten "Don'ts" in Operational/Informational Technology Convergence Security
  Joseph, J. Januszewski, III：
  - ＃1.　インターネットにつなげる
  - ＃2　外部請負業者や子会社等が、システムに直接アクセスできるようにする
    ＃3　有効な多層防御になっていない
  - ＃4　ネットワークがセグメント化されていない
  - ＃5　OS の付随ソフト等、不要なソフトウェアをそのまま（インストールしたまま）にしておく
  - ＃6 ビジネスネットワークと制御系ネットワークで共有のメディア（USB メモリ等）を使用する
  - ＃7　ログを無視する（活用しない）
  - ＃8　パッチをあてない
  - ＃9　内部不正対策は、お決まりの教育等で済ます
  - #10　対策して終わりに（満足）する

次号、ICSJWG 四半期ニュースレター（3 月号）への記事の寄稿の〆切は、3 月 13 日。掲載希望者は、ICSJWG.Communications@dhs.gov まで。

以上