

ICSJWG 四半期ニュースレター (2014年9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, September 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 Fall Meeting

ICSJWG 2014 Fall Meeting は、10月7日～9日にアイダホ州アイダホフォールズにて開催され、重要インフラ事業者やベンダ、政府担当者や研究者などが、産業用制御システム (ICS) のセキュリティに関する最新の動向や取組を共有。

※講演資料は、以下より入手可能 (一部講演については掲載なし)

<https://ics-cert.us-cert.gov/Agenda-Available-Presentations-2014-ICSJWG-Fall-Meeting>

◆ICSJWG Webinar (ウェブセミナー)

第3回 ICSJWG Webinar を、10月30日に開催。Securecon 社の Ernie Hayden 氏が「新たなセキュリティパラダイム: 侵入を前提とした対策」というテーマに基づき、ICS と業務システムの多層防御およびインシデント対応について解説。

◆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 (Revision 2 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た。ICSJWG ミーティングでは今後の開発の方向性を話し合う場も設けられ、欲しい機能を伝えることも可能。

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

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。

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

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)

◆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>

2014 年 12 月 8 日～12 月 12 日(※北米関係者向け): ✕ 切り済

*2015 年 1 月 12 日～16 日: ✕ 切り済

*2014 年 2 月 9 日～13 日: ✕ 切り済

*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 ウェブサイト(<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 2 件の記事が寄稿されている。詳細は原文を参照のこと。

- 「安心かつ信頼のおける水供給を確保するためのサイバーセキュリティ」
単一方向ゲートウェイによる、ビジネスネットワークとの制御システムのデータの安全な共有
Cybersecurity to Ensure the Reliable Delivery and Safety of Water Supply
Dennis Lanahan, Owl Computing Technologies
- 「ハッカーグループ『Dragonfly』によるサイバー攻撃への対策」
Defining Against the Dragonfly Cyber Security Attacks
Joel Langill, SCADAHacker.com
※この記事は、第 508 条(障害者に対するウェブアクセシビリティの確保)に準拠していないため、掲載
することができません。

【IPA 補足】本記事は、以下からも入手可能です。

<http://info.belden.com/a-cyber-security-dragonfly-bc-lp>

次号、ICSJWG 四半期ニュースレター(12 月号)への記事の寄稿の〆切は、12 月 12 日。掲載希望者は、ICSJWG.Communications@dhs.gov まで。

以上