

ICSJWG 四半期ニュースレター (2013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 2013」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>

◆Cyber Security Evaluation Tool(CSET)6.0、2014年1月リリース

新バージョン 6.0 のリリースが、2014年1月下旬に確定。6.0には、初めて民間の商用規格として、Interstate National 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についても改訂等がされている。

機能面も向上しており、評価が複数行えるだけでなく、複数拠点の評価を比較したり、複数の評価を1つに統合することも可能となる。

◆ICSJWG 2013 Fall Meeting

ICSJWG 2013 Fall Meeting は、11月6日、7日に、メリーランド大学シェイディ・グローブ・キャンパス(メリーランド州ロックヴィル)のNIST施設において開催された。2日間のカンファレンスでは、連邦予算の強制削減への対応に伴うICSJWGの活動形態の見直し、およびサイバーインテリジェンスの分析、NISTのICSガイドライン、ファジング、医療業界におけるICTセキュリティなどについて議論がなされた。

講演資料は、Homeland Security Information Network で公開している。

※IPA 補足: 講演資料は、ICSJWG にメールでリクエストし、入手することも可能です(一部提供の無いものもあり)。

詳細は ICSJWG ウェブサイトを参照ください。

(<http://ics-cert.us-cert.gov/Industrial-Control-Systems-Joint-Working-Group-ICSJWG>)

◆Webinar(ウェブセミナー)の活用

多くのメンバが Fall Meeting に参加できなかったため、ICSJWG では Homeland Security Information Network(HSIN)を通じて、12月12日に Fall Meeting での講演を webinar で提供した。

今後、ICSJWG では webinar を活用してインタラクティブな会合を増やしていくものとし、四半期ベースで webinar を開催する予定。開催の頻度や柔軟性が増すことにより、ICS 関係者が ICS コミュニティとアイデアや経験を共有する機会が広がることを期待している。

¹ Control System Cyber Security Guidelines for the Natural Gas Industry

² Cyber Security Plan for Nuclear Power Reactors

◆サブグループの廃止

ICSJWG では、ICSJWG の活性化に向け、メンバがより主導的に活動を行えるようにするため、固定のサブグループを廃止し、今後はよりアドホックにグループを組織し、活動できるようにする。なお、サブグループ下で作成された(または作成中の)成果物については引き継ぎ、取組みを継続する。

<継続する活動の例>

- 既存の ICS 標準の把握と比較・検証
- ICS に応用されようとしている技術は IT 向けであり、ICS には適用が難しいと言われる問題を取り上げたレポートの作成
- ICS 向けの人材育成フレームワークの確立に向けた取組み
- 「Cross-Sector Roadmap for Cybersecurity of Control Systems」の改訂

上記活動への参加希望、または新たな活動の提案等があれば、icsjwg@hq.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、制御システムのサイバーセキュリティ関係者に向けて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 に関する最新ニュースは、ツイッター(@ICSCERT)でもフォロー可能。

◆FY2014 年度³ 制御システムサイバーセキュリティトレーニング 上級コース開催スケジュール

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、上級コースのトレーニングを提供する。

<トレーニング内容>

- 1 日目:挨拶、ICS-CERT および制御システムセキュリティの概要、インターネットを介した制御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

<FY2014 年度の開催日>

2014 年 2 月 10 日~14 日: ✕切済

*2014 年 3 月 10 日~14 日: 受付中

*カレンダーより IPA 補記分

³ 2013 年 10 月~2014 年 9 月

日付と内容は変更となる可能性があるため、詳細はカレンダー(<http://ics-cert.us-cert.gov/Calendar>)を確認のこと。また、受講は北米の重要インフラ関係者優先となる。北米以外からの参加希望者は、インターナショナルパートナー向けの表示があるコースを参照のこと。

◆制御システムセキュリティに関する寄稿記事

本号には、以下の4記事が寄稿されている。詳細は原文を参照のこと。

- 「ビッグデータの活用と予測分析: 重要インフラを高度な脅威から守る」
Big Data and Predictive Analytics: Protecting Your Critical Infrastructure from Advanced Threats
Odin Olson, Director of Engineering, Damballa
- 「連邦エネルギー規制委員会(FERC)の「Order 791」(CIP ver.5を承認)と電力制御システム」
Industrial Control Systems in the Power Sector Under FERC Order 791
Joseph. J. Jamuzewski, III, CISSP
(Head of Cyber Security Research Lab, EADS Innovation Works, UK)
- 「ジョン・ホプキンス大学応用物理研究所、重要インフラのサイバー演習を主催」
John Hopkins University Applied Physics Lab Hosts Critical Infrastructure Cyber Exercise
Beth S. Hoenicke, Johns Hopkins University Applied Physics Laboratory
- 「重要インフラセキュリティ確立への道程」
Building the Road to Infrastructure Security
Chris Blask

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7日。掲載希望者は、icsjwg@hq.dhs.gov まで。

以上