

## ICSJWG 四半期ニュースレター (2013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 2013 Issue”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。(※本文中のリンク先は、全て英文となります)

URL: [http://ics-cert.us-cert.gov/sites/default/files/ICSJWG-Archive/ICSJWG\\_Quarterly\\_Newsletter\\_March\\_2013.pdf](http://ics-cert.us-cert.gov/sites/default/files/ICSJWG-Archive/ICSJWG_Quarterly_Newsletter_March_2013.pdf)

### Cyber Security Evaluation Tool (CSET) の 5.1 は夏にリリース予定

2月にリリースされた Cyber Security Evaluation Tool (CSET) 5.0 への関心が徐々に広がる。次バージョンの開発も進んでおり、バージョン 5.1 では、機能や操作性の改善に加え、Committee on National Security Systems Instruction (CNSSI) No.1253<sup>1</sup> や、NIST SP 800-53 の最新版 Rev.4 などにも対応する予定。初夏のリリースを目指す。

### ICSJWG 2013 Spring Meeting は中止

ICSJWG 2013 Spring Meeting は、歳出の強制削減措置の影響により急遽中止。代替の場については、今後検討し、アナウンスする予定。

### ICS-CERT 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、ICS-CERT の最新の活動状況を報告するため、マンスリー・モニター・ニュースレターを発行している。

また、ICS-CERT に関する最新ニュースは、ツイッター (@ICSCERT) にて。

### 2013年度 制御システムサイバーセキュリティトレーニング 上級コースを開催予定

アイダホフォールズ(アイダホ州)の Control Systems Analysis Center において、今年も攻撃チームと防御チームによる対戦訓練を含めた、上級コースのトレーニングを開催。

#### <トレーニング内容>

- 1日目: 挨拶、ICS-CERT、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セキュリティ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、攻撃チーム/防御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、攻撃チーム/防御チームに分かれての作戦会議

<sup>1</sup> 国家安全保障情報 (National Security Information) を処理、保管、送信する全ての情報システム向けのセキュリティ分類およびセキュリティ管理策をまとめたガイドライン [http://www.cnss.gov/Assets/pdf/Final\\_CNSSI\\_1253.pdf](http://www.cnss.gov/Assets/pdf/Final_CNSSI_1253.pdf)

- 4日目:攻撃チーム/防御チームに分かれての12時間のサイバー演習
- 5日目:演習から学んだことなどを話し合う懇談会

#### <FY2013年度<sup>2</sup>の開催日>

2013年6月17日～21日

2013年7月15日～19日

2013年9月9日～13日

※変更の可能性があるため、[レーニング・カレンダー](#)を継続的にチェックしてください

#### ICSJWG サブグループの活動状況

「産業制御システムをセキュアにするためのロードマップ」サブグループおよび「ベンダ」サブグループの Government Coordinating Council (GCC) 側の共同議長が空席となったのに伴い、ボランティアの申し出または提案を募集中。共同議長の主な業務は、当該サブグループの憲章の改定、メンバ登録および参加の推薦・審査、業務の割振り、会合の準備・取纏め等。(詳細、応募・推薦は原文参照)

- 「研究・開発」サブグループ
  - 1月に会合を行い、先頃改定された憲章のレビュー、および未決定のアクションアイテムについて議論を実施。
- 「産業制御システムをセキュアにするためのロードマップ」サブグループ
  - 同サブグループ下に、『制御システムのサイバーセキュリティのための分野横断ロードマップ (Cross-Sector Roadmap for Cybersecurity of Control Systems)』の更新に関して責任を担うサブコミュニティを立ち上げ。また、ICSJWG 下に「ICS サイバーセキュリティ標準サブグループ」の立ち上げに成功(後述)。
- 「ベンダ」サブグループ
  - [脆弱性公開フレームワーク](#)の発行が終わった為、今後はベンダの観点から、制御システムのセキュリティ改善に向けて、ICS コミュニティの進むべき方向性や、対策(パッチプロセス、パッチが適用できないシステムに対する最善策など)の検討に注力。
- 「専門家養成」サブグループ
  - 専門家育成フレームワークの一端となる、スキルモデルの整理に取組中。最終版を今度の会合で議論する予定。
- ICS サイバーセキュリティ標準サブグループ
  - 現在メンバを募集中。このサブグループでは、現行の制御システム関連基準の洗い出しおよび評価を行い、ベースラインとなる要件の取纏めおよび改定を行っていく予定。

---

<sup>2</sup> 2012年10月～2013年9月

## ICSJWG ガイドおよびクロスセクター・ロードマップガイドの公開

下記2件のガイドは、ICSJWG Government Coordinating Council (GCC) および Sector Coordinating Council (SCC) の承認を受けたドキュメントであり、それぞれのサブグループの会合において、レビューおよび活用できる。

- ICSJWG ガイド

ICSJWG の背景、サブグループのミッションや詳細について説明

[https://cs.hsin.gov/C2/C3/GCC%20%20SCC/Document%20Library/ICSJWG-Guide\\_2013\\_FINAL.pdf](https://cs.hsin.gov/C2/C3/GCC%20%20SCC/Document%20Library/ICSJWG-Guide_2013_FINAL.pdf)

(Homeland Security Information Network (HSIN) のアカウント要)

- クロスセクタ・ロードマップガイド

『制御システムのサイバーセキュリティのための分野横断ロードマップ (Cross-Sector Roadmap for Cybersecurity of Control Systems)』の背景および参照情報

[https://cs.hsin.gov/C14/C1/RoadmapToSecureICS/Document%20Library/ICSJWG-Roadmap-Guide\\_2013\\_FINAL.pdf](https://cs.hsin.gov/C14/C1/RoadmapToSecureICS/Document%20Library/ICSJWG-Roadmap-Guide_2013_FINAL.pdf)

(Homeland Security Information Network (HSIN) のアカウント要)

これらのガイドについては、一般向けに公開している [ICSJWG ウェブサイト](#) にもアップされる可能性あり。

### 【IPA 補足】

- ・ICSJWG ガイドは、現在はアップされていません
- ・クロスセクタ・ロードマップガイドは、FINAL 版でなく、2012/9/30 版であればアップされています

## Homeland Security Information Network (HSNI) ポータル

ICSJWG が使用している情報共有ツール。お知らせ ("Alert Me") 機能があり、更新があればメールで知らせてくれる。アカウントを持っていない場合は、所属団体、重要インフラセクタ、氏名、連絡先、所属サブグループを ICS-CERT までメールし、申請のこと。

## 米標準技術研究所 (NIST) ウェブミーティング

行政命令第 13636 号 (E.O.13636) により、NIST は、重要インフラ向けのサイバーセキュリティフレームワーク確立の責任を担う機関に任命された。ミーティングでは、ステークホルダを集め、現行のリスク管理施策、フレームワーク、基準、ガイドライン、ベストプラクティス等に関して事業者からヒアリングを実施し、検討を行う。フレームワークおよびミーティングの詳細については、[NIST ウェブサイト](#) 参照。

## 制御システムセキュリティに関する寄稿

本号には、以下の3記事が寄稿されている。詳細は原文を参照。

- 「産業制御システムにおける知的財産窃盗の検知および防御 (Protecting Against and Detecting Intellectual Property Theft in Industrial Control Systems)」  
Jacob Kitchel 氏 (Industrial Defenders 社 シニアマネージャ)
- 「産業制御システムにおける懸念事項 (Computing Concerns in Industrial Control Systems)」  
Joseph J. Januszewski Ⅲ 氏 (CISSP、CHSP、CNA)

- 「情報共有にあたっての教訓を学ぶ(Learning Lessons on Information Sharing)」  
Chris Blask 氏 (ICS-ISAC 議長)

※次号(2013年6月)への寄稿の締切は6月11日

以上