

ICSJWG 四半期ニュースレター (2014年6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, June 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約220名が参加。各種講演やデモ、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) 等を通じ、産業用制御システム (ICS) に関する最新の取組に関する情報を共有。

次回、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で開催予定。

◆ICSJWG Webinar (ウェブセミナー)

第2回 ICSJWG Webinar を、6月25日に開催。アイダホ国立研究所 (INL) による同研究所が開発した「Sophia」(ICS の通信を一覧表示し、異常な (想定外の) 通信の発見を支援するツール) の解説、Yokogawa IA Global Marketing Center の Graham Speake 氏、NexDefense 社の Michael Sayre 氏によるリアルタイム監視による変更検知や、Sophia の補足的ツールとなる Dragos Security 社の CyberLens の解説を放映。

◆Cyber Security Evaluation Tool (CSET) 6.1

CSET の最新版 6.1、2014年8月のリリースを目指して最終調整中。CSET 6.1 は、新たに2つの基準 (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」) に対応したほか、自組織独自の質問 (要求事項) を作成できるカスタマイズ機能を追加。独自に作った質問 (要求事項) は、プロファイルとして組織内・組織間で共有可能。

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。

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

◆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。

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

◆FY2014 年度・2015 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。

<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 9 月 29 日～10 月 3 日(※北米): 〳切り済

2014 年 10 月 13 日～17 日(※国際): 〳切り済

*2014 年 11 月 3 日～7 日(※北米)

*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、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記載のうえ、ICSJWG.Communications@dhs.govまで⁵。

⁴ FY2014:2013 年 10 月～2014 年 9 月

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

◆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。

◆ICS セキュリティに関する寄稿記事

本号には、以下 4 件の記事が寄稿されている。詳細は原文を参照のこと。

- 「産業用制御システムのトレーニングコース: 受講経験に基づく概要解説」

A Recent View of Industrial Controls Security Training

Ernie Hayden, Securicon LLC

※紹介されているのは、以下の 3 組織が提供する 4 コース

- SANS Institute: 「ICS410 ICS/SCADA Security Essentials」(有料)
- ISA: 「Using the ANSI/ISA-62443 Standards to Secure Your Control System」(有料)
- ICS-CERT: 「100W Operational Security (OPSEC) for Control Systems」(無料)
「210W Cybersecurity for Industrial Control Systems」(無料)

- 「事業者はサイバーセキュリティ意識の改革を! 『安全』と同じレベルで『セキュリティ』への取組みを」

Treating Security like Safety

Mike Baldi & Shawn Gold, Honeywell Process Solutions

- 「ハードウェアベースのセキュリティソリューションによる、産業用制御システムのエンドポイント機器のセキュリティ向上」

Hardware-based solutions improved security of end-points in industrial control systems

Michael Armentrout, Infineon Technologies North America

- 「Patch and Update Management Program: パッチマネジメントと検証のシンプル化」

Simplifying Patch Management and Validation... - Do I Have Your Attention?

Lindsey Hale, FoxGuard Solutions

次号、ICSJWG 四半期ニュースレター(9 月号)への記事の寄稿の〆切は、9 月 12 日。掲載希望者は、ICSJWG.Communications@dhs.govまで。

以上