

ICSJWG 四半期ニュースレター (2013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 2013”(11月公開)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)の6.0 開発中

現在、Cyber Security Evaluation Tool(CSET)の6.0が開発中。サポートする標準が更新されるほか、ユーザインターフェースもより使い易くなる。公開は2014年1月を予定。

◆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/>)にて。

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 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、今年度も攻撃チームと防御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開催する。

<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、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
- 4日目:攻撃チーム/防御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¹の開催日>

- 2013年10月7日~11日: 済
- 2013年11月4日~8日: 済
- 2013年12月2日~6日: 済

¹ 2013年10月~2014年9月

*2014年 1月 13日～17日: 不済

*2014年 2月 10日～14日: 受付中

*IPA 補記分

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。

◆ICSJWG 2013 Fall Meeting

※IPA 補記

ICSJWG 2013 Fall Meeting は、11月6日、7日にメリーランド州ロックヴィルで開催されました。講演資料はICSJWGにメールでリクエストし、入手することが可能です。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>)

◆ICSJWG サブグループの活動状況

- 「研究・開発」サブグループ
会合を行い、研究・開発分野で利用されているツール(NP-View、Möbius、ADVISE、LZFuzz、AMILYZER など)を紹介。
- 「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
『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的ロードマップ(Cross-Sector Roadmap for Cybersecurity of Control Systems)』を改訂中。協力希望者は、ICSJWG まで連絡を請う。
- 「ベンダ」サブグループ
制御システムに応用されているセキュリティ技術はIT向け(IT-Grade)で、制御システム向け(Control Grade)でないという問題を取り上げ、制御システム事業者・ベンダの互いにとって、拡張可能で費用効果が高く、適切なセキュリティを提供するソリューションの提示を目的とする。現在、ドラフト版を関係者がレビュー中。
- 「専門家養成」サブグループ
ICS に携わるのに必要な ICS 特有の知識(knowledge)、スキル(skills)と能力(abilities)を整理した「Competency Model」を策定。現在関係者がレビュー中。現時点では、必要とされるコンピテンシーが網羅されているか、包括性の観点を重視してレビューを実施している(2013年10月までを予定)。入手は、ICSJWG@hd.dhs.gov までメールにて、もしくは HSIN(Homeland Security Information Network)から。
- 「標準」サブグループ
様々な ICS 標準の比較検証を行い、それらの共通項の洗い出し(標準化)、および各 ICS 標準化団体のもつ展望(landscape)の分析に取り組み中。

※IPA 補足

ICSJWG ではその後サブグループを終了し、今後は必要時にアドホックにワーキンググループを作って

活動する形態に移行しています。サブグループで仕掛かり中のプロジェクトについては、残存作業として引き継がれるとのことです。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>)

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 3 記事が寄稿されている。詳細は原文を参照のこと。

- 「制御システムセキュリティの教育プログラムへの取り込み ～ソフトウェアエンジニアリングの見直しと活用を～」

Integrating Control System Security Into Educational Programs

Joseph J. Januszewski, III 氏 (CISSP)

- 「一般的な”3 Tier”モデルのセキュリティソリューションの死角」

Your security system might not be ready to protect up to 92% cyberattacks

Jules Ferdinand Pagna Disso 博士

(Head of Cyber Security Research Lab, EADS Innovation Works, UK)

- 「制御システムのサイバーセキュリティ ～ベンダから適切な回答を引き出すための正しい質問の仕方～」

Asking ICS Suppliers the Right Questions about Cybersecurity: Standards and Best Practices

Nadya Bartol 氏 (Senior Cybersecurity Strategist, CISSP, CGEIT, Utilities Telecom Council)

以上