2013 年 2 月 27 日
独立行政法人情報処理推進機構（IPA）

ICSJWG 四半期ニュースレター（2012 年 12 月発行）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 2012 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/pdf/ICSJWG_Quarterly_Newsletter_December_2012.pdf

Cyber Security Evaluation Tool（CSET）のバージョン 5 が完成

Cyber Security Evaluation Tool（CSET）のバージョン 5 が完成。実地試験を経て、2013 年 1 月中旬～下旬にリリース予定（補記：CSET ウェブサイトにてリリース済）。

バージョン 5 では、CS2SAT から CNET に変わった時以来の大きな変更が行われている。評価プロセスに、制御システム基準から抽出した質問を使った新しいアプローチを採用しているほか、規制業界向けに、より要件ベースな評価を可能としている。また、新しい分析機能が追加された。バージョン 5 は.Net Framework を使っており、ウィンドウのドッキングや質問のフィルタリングなどできるようになった。そのほか、北米電力信頼度協議会（NERC）の CIP リビジョン 4 や運輸保安局（TSA）のパイプライン・ガイドラインなどの新しい基準にも対応している。

ICSJWG 2013 Spring Meeting 情報

ICSJWG 2013 Spring Meeting は、2013 年 5 月 6 日～9 日まで、アリゾナ州フェニックスのフェニックス・ハイアット・リージェンシー（Phoenix Hyatt Regency）で開催予定。

また、海外パートナーが参加する ICSJWG 2012 Spring International Partners Day は、9 日に開催される。アジェンダ等、詳細については今後ウェブサイトに掲載予定。

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・トレーニングを開催

◇各地での開催（初級・中級クラス）

以下の各地で、初級（101）、中級（201：講義のみ、202：講義およびラボ実験）のトレーニングを開催する。

＜開催日＞

2013 年 3 月 25～29 日：ヒューストン（テキサス州）
2013 年 6 月 24～28 日：ボストン（マサチューセッツ州）
2013 年 8 月 12～16 日：シアトル／タコマ（ワシントン州）
2013 年 9 月 16～20 日：未定

◇Control Systems Security Program（CSSP）での開催（上級クラス）

アイダホ州アイダホ・フォールズにある Control Systems Analysis Center において、上級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

＜開催日＞

2013 年 2 月 11～15 日
2013 年 3 月 11～15 日
2013 年 4 月 8～12 日
2013 年 4 月 22～26 日
2013 年 5 月 20～24 日（海外パートナー向け）
2013 年 6 月 17～21 日
2013 年 7 月 15～19 日
2013 年 9 月 9～13 日

ICSJWG サブグループの活動状況

- 「研究・開発」サブグループ

  Fall Meeting において憲章の改定案の批准と承認を行い、12 月の会合で、アクションアイテムの確認と、研究・開発サブコミッティの新設を討議について検討。

- 「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ッティを新設。

  また、ICS Cybersecurity Standard Subgroup の新設とメンバーの募集を行った。このサブグループでは、国土安全保障省が策定した制御システム関連基準や、実際に改善に役立った脆弱性対策やインシデント対応事例の教訓のメンテナンスを行い、基準等が公的にアップデートされる際に、標準化団体（組織）にインプットを行う予定。

- 「ベンダー」サブグループ

  脆弱性公開フレームワークの取り纏め後、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）の検討を実施。

- 「専門家養成」サブグループ
  議長の交代あり。現在、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。

制御システムセキュリティに関する寄稿

- 「第 7 回　重要インフラ防護に関わる情報処理国際連合（IFIP）ワーキンググループ 11.10 国際会議論文募集」
  Zachary Tudor 氏（SRI International）

  補足：募集は〆切済

- 「産業制御システム向けの振る舞いベースの脅威検知」
  Leonard Jacobs 氏（Netsecuris 社　代表取締役兼最高経営責任者）

- 「産業制御システムにおける有効な変更管理を阻害する 6 つの要因」
  Jacob Kitchel 氏（Industrial Defender 社　Security and Compliance シニアマネージャ）

- 「SCADA システムに対する脅威識別のためのインテリジェント分析エンジンおよびイベント相関モデル」
  Sandeep K. Shukla 教授（バージニア工科大学　電気・コンピュータ工学部　Hume Center for National Security & Technologies）

- 「APT 攻撃を防ぐため、開発工程で産業制御システムの脆弱性を正す方法およびシステムライフサイクル後期に生じるパッチ管理の問題を軽減する方法」
  Bart Pestarino 氏、CISSP（Codenomicon 社）

- 「ファイアウォールをすり抜ける 13 の方法」
  Andrew Ginter 氏（Waterfall Security Solutions 社 Industrial Security ディレクター）

  補足：ICSJWG 2012 Fall Meeting における講演内容に基づく寄稿。2012 Fall Meeting のウェブサイトで Ginter 氏の講演資料を公開している

- 「特権アカウントと ID 管理　－攻撃者の聖杯」
  Yariv Lenchener 氏（Cyber-Ark 社　シニアプロダクトマネージャ）

以上