2013 年 8 月 21 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（2013 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 2013 Issue”の概訳となります。内容の詳細につきましては、原文をご確認ください。

原文は、ICSJWG にメール頂き、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 5.1 が完成

Cyber Security Evaluation Tool（CSET）5.1 が、4 月に完成。6 月初旬に一般公開され、数週間後には ICS-CERT のウェブサイトからもダウンロードが可能になる予定（IPA 注： 8/22 現在リリース済）。5.1 版は、Committee on National Security Systems Instruction（CNSSI）No.1253[1]などにも対応したほか、同じ質問に何度も答えなければならない状況の改善など、様々な機能性の向上を実現した。また、わかりやすく具体的なビデオチュートリアルを提供している。

ICSJWG 2013 Fall/Spring Meeting

ICSJWG は、関係者の各分野の専門知識やスキルを財産としており、今後も顔を見ながらコミュニケーションができる有効な場であるべく務めている。そのために、従来の会合とは別の形式の会合や、オンラインコラボレーションツール、電話会議やバーチャル会議を通じたローカルな会合なども検討している。アイデアや意見があれば、是非 ICSJWG@hq.dhs.gov まで寄せて欲しい。

ホームランドセキュリティ情報ネットワーク（HSIN）ポータル　－　リリース 3（R3）

この度、HSIN Legacy サイトが、新プラットフォーム「HSIN Release3（R3）」に統合された。新しい HSIN R3 は、性能や使いやすさが向上したほか、最新のセキュリティを搭載している。また、お知らせ（”Alert Me”）機能があり、更新があれば知らせてくれる。希望者はポータルから登録を。

なお、ログインには別途 R3 用アカウントが必要となる（HSIN Legacy サイトの ID とパスワードではログインできない）。HSIN R3 アカウントが必要な関係者は、所属団体、関係する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。

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、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）でもフォロー可能。

---

[1] “CNSSI 1253: Security Categorization and Control Selection for National Security Systems” – 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

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[2]の開催日＞

2013 年　9 月 9 日～13 日：〆済
2013 年 10 月 7 日～11 日（インターナショナルパートナー）：〆済
2013 年 11 月 4 日～ 8 日：受付中

※変更等の可能性があるため、詳細は、トレーニング・カレンダーを継続的にチェック要
※IPA 補足：受講は、北米の重要インフラ事業者・関係者優先となっています。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ください

ICSJWG サブグループの活動状況

ICSJWG サブグループの活動状況を下記に示す。サブグループのメンバ登録を希望する場合は、ICSJWG にメールするか、各サブグループの代表者に連絡のこと。

- 「研究・開発」サブグループ
  研究・開発サブグループでは、6 月 20 日に会合を行い、前回行われた会合以来の活動要点、および研究・開発の要件をまとめた。

- 「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
  同サブグループ内のサブコミッティでは、『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）』の改定案を取りまとめた。今後は改定案を文書に落とし込む作業に入る。

- 「ベンダ」サブグループ
  ベンダサブグループでは、パッチが適用できなくなったシステムをどう改善、廃止、入れ替えるかについてのドキュメントの作成を開始した。概要のドラフトができたのを受け、執筆を手伝ってくれるボランティアを募集中。希望者は、メールタイトルを”Vendor Document Development”として、ICSJWG までメ

[2] 2012 年 10 月～2013 年 9 月

ールを。

- 「専門家養成」サブグループ
  専門家育成サブグループは、ICS 独自のコアスキルを、定義と職務分野を明確にしてグルーピングし、整理したフレームワーク（ICS-specific Professional Development Framework）を確立するべく検討中。他の ICSJWG コミュニティがレビューした後、他の ICS コミュニティにも展開する予定。本サブグループへの参加を希望する場合は、ICSJWG にメールで連絡のこと。

- 「標準」サブグループ
  標準サブグループは、2013 年 4 月に第 1 回キックオフを開催した。以降、毎月ミーティングを実施し、グループの憲章や成果物について議論を行ってきた。また、米標準技術局（NIST）や国防総省（DoD）に対し、両者の ICS 標準に関する支援や助言を提供するなど、グループ本来の任務でも成果を挙げている。グループでは、様々な ICS 標準の比較検証と主要標準化組織の展望の取りまとめに向けて、メンバを募集中。

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 5 記事が寄稿されている。詳細は原文を参照のこと。
※次号（2013 年 9 月号）への寄稿の締切は 9 月 6 日

- 「『国防総省リスク管理フレームワーク（RMF）』と『国家安全保障システム委員会指示（CNSSI）1253』に見る産業制御システムのセキュリティ確保への取組」
  Overview of the DoD Risk Management Framework (RNF) and the CNSSI 1253 Industrial Control Systems (IC) – Platform IT (PIT) Overview
  Daryl Haegley 氏（OCP、CCO）
  Michael Chipley 氏 (PhD PMP LEED AP)

- 「予防策としての攻撃対象領域（Attack Surface）の最小化」
  Minimizing the Attack Surface as a Preventative Measure
  Joseph J. Januszewsk III 氏（CISSP、CHSP、CNAn）

- 「産業制御システムの脆弱性評価に関するリスクの最小化の事例」
  Minimizing Risks Asso0ciated with Performing Vulnerability Assessment on Industrial Control Systems
  Alexander Benitez 氏（Sr. Scientist, ComSource, Inc., a GlobeComm company）

- 「要塞ホストの 10 のセキュリティホール」
  10 Security ‘Gotchas’ with Homegrown Jump Servers
  Yariv Lenchner 氏（Cyber-Ark Software）

- 「サイバーインテリジェンス入門：インターネット上の産業制御システムの特定」
  Cyber Intelligence Brief: Identifying Online Industrial Control Systems
  Robert Huber 氏（President, Critical Intelligence Inc.）
  ※IPA 補足：本寄稿記事については、以下に概要をまとめています。

【寄稿記事】サイバーインテリジェンス入門：インターネット上の産業制御システムの特定

インターネットに接続されている脆弱な産業制御システム（ICS）が悪意のある人物に特定される危険性について、去年一昨年と騒がれている。この寄稿では、攻撃者がインターネットに接続されている産業制御システムを特定するのに使う可能性がある手法について、概要を説明する。他にも様々なツールや方法が存在するが、本稿では SHODAN、ERIPP、Google Dorks を紹介する。

＜SHODAN＞

SHODAN は、ルータやサーバなど、ある種のコンピュータを探すことができる検索エンジンである。NMAP に似た独自のプログラムを用いてインターネットをスキャンし、インターネットに接続されたコンピュータを見つけ、データベース化している。

一般的なプロトコル（HTTP、HTTPS、SMTP、Telnet、SMTP、SMB）を対象とするが、今後、産業制御システムでよく使われているものを含め、他のプロトコルが追加される可能性もある。

〇使用方法

- SHODAN ウェブサイトを開く。http://www.shodanhq.com/
- 制御システム名またはベンダ名を検索ボックスに入力する。
- 結果が表示される。

〇検索例：「Rockwell」で検索

- 例の場合、219 件のヒット。
- どのサービスポート（HTTP や SMTP 等）で見つかったか、ポートと件数が表示される。
  SNMP 181、HTTP 22 等
- 見つかった機器の実際の IP アドレスが表示される。また、IP アドレスの下部に、当該 IP アドレスを使っている企業・組織等の名称、データベースに登録された日付が表示される。
  222.120.203.186　Korea Telecom　01.02.2013
- 見つかったコンピュータの機器名等が表示される。
  Rockwell Automation 1769-LxxE

＜Every Routable IP Project (ERIPP)＞

ERIPP はインターネット上にあるIPアドレスへの接続を試みるプロジェクトである。具体的には、ポート番号 80（ブラウザがウェブページを見に行く際のデフォルトポート番号）へ接続する。これにより、接続している IP アドレスが、ウェブサーバとして稼動しているかがわかる。

ERIPP も、インターネットをスキャンし、結果をデータベース化している。ただし、対象はポート 80 のみ。

〇使用方法

- ERIPP ウェブサイトを開く。http://eripp.com/
- ウェブサーバ上で発見される可能性が高い、産業制御システム（ICS）関連のキーワードを入力する。
- 結果が表示される。

〇検索例：「Rockwell」で検索

- 結果が表示される。IP アドレス、DNS サーバ、タイトル、発見日が表示される。例の場合、199 件のヒットがあった。

- IP アドレスをクリックすると、検索キーワードを含むウェブページに接続する。
- タイトルは、見つかったウェブページの HTML title タグの内容が表示される。
- 発見日は、当該ウェブサーバが、データベースに登録された時期（1 year ago 等）が表示される。
- SHODAN もポート 80 を検索対象としているが、2 つのプロジェクトは違う手法を使用しているため、結果が異なる可能性がある。

＜Google Dorks＞

Google Dorks はグーグル検索エンジンに索引付けされたコンピュータを探す方法を指している。つまり、ユーザが、インターネットに接続されている産業制御システム機器を「グーグル検索」することを意味する。

Google には「intitle:」「inurl:」等、いくつもの高度な検索演算子が用意されている。これらの演算子を活用することで、検索の範囲やターゲットを絞り込むことができる。

〇使用方法

- Google ウェブサイトを開く。http://www.google.com/
- ウェブサーバ上で発見される可能性が高い、産業制御システム（ICS）関連のキーワードを入力する。
- 結果が表示される。

〇検索例：「intitle:"Rockwell Automation""Device Name""Uptime"」で検索

- HTML title タグがキーワードにあてはまるものだけが検索される。例の場合、15 件のヒット。
- 表示内容は、一般的なグーグル検索の結果と同様。
- 「Rockwell Automation」というタイトルのウェブページについて、IP アドレス、機器の名称、場所、シリアルナンバー、ステータス（Active 等）、稼動時間等が表示される。

＜＜リスクおよび軽減策＞＞

攻撃者がインターネットに接続された産業制御システムを発見した場合、以下の影響を及ぼすことが考えられる。

- 攻撃者が、発見された機器（サービス）に接続する。
- 攻撃者が、ハードコード化された ID/PW、デフォルトの ID/PW、よく使われる ID/PW 等を使って不正アクセスを試みる。
- 攻撃者が、発見された機器の既知の脆弱性を攻撃する。
- 攻撃者が、発見された機器が制御している機器やプロセスに介入する。

上記に挙げた「想定」は、実際に発生している。本稿で紹介したツールは、ごく一部であることを忘れてはならない。高度なスキルを持つ攻撃者であれば、類似した、より高機能なツールを使って攻撃してくることも予想される。

＜＜対策＞＞

- これらのツールを日常的に使用し、インターネットからアクセスできるべきでない自社ネットワーク上の機器や情報が表示されないか、監視する。
- 信頼できる第三者を雇い、モニターさせる。
- 以下のうち、1つ以上のことを行う：
  - インターネットから機器を外す。

- バナーを変える。
- 別のポートを使用する。
- SHODAN、ERIPP、Google その他から来る既知のスキャンや検索をブロックする。

以上