2012 年 10 月 16 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 9 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, September 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://www.us-cert.gov/control_systems/pdf/ICSJWG-Newsletter-2012-09.pdf

ICS-CERT、脆弱性情報公開方針を変更

ICS-CERT は、脆弱性情報公開方針を変更し、発見された脆弱性に関してベンダの対応が鈍い場合、または、ベンダが提示するパッチの準備に必要なタイムスケジュールが妥当ではないと思われる場合、ベンダに脆弱性発見の通知をした日から 45 日目以降に、パッチや回避策の在る無しに関わらず、脆弱性情報を公開することがある旨を追加した。但し、公開日については、攻撃が活発に行われている、脅威が特に深刻である、現状確立されている決まりごとを変更する必要性があるなど、状況によって早まったり、遅れたりすることがある旨も併せて記している。

この変更は、ICS-CERT と協力し、積極的に脆弱性の是正に取り組んでいるベンダには何ら影響を与えるものではなく、脆弱性対策にあまり積極的でないベンダに対する対策実施の推進力になることを願っている。

ICSJWG 2012 Fall Meeting 情報

ICSJWG 2012 Fall Meeting は、10 月 15 日～17 日まで、コロラド州デンバーのグランド・ハイアット・デンバー（Grand Hyatt Denver）で開催予定。

また、海外関係者も参加する ICSJWG 2012 Fall International Partners Day は、18 日に開催される。アジェンダ等、詳細については、ホームページを参照。

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。

2012 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

Control Systems Security Program（CSSP）では、アイダホ・フォールズにある Control Systems Analysis Center において、制御システムをサイバー攻撃から守るためのハンズオン・トレーニングを提供。

＜トレーニング内容＞

- 1 日目：挨拶、CSSP、制御システムセキュリティの簡単な解説、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：演習の教訓確認、ラウンドテーブル

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
  『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）』の改訂に取り組んでおり、次版に含める予定のロードマップの評価計画について検討中。
- 「ベンダー」サブグループ
  ICS ベンダ、SIer などの意見に基づく、脆弱性公開フレームワークを公開。また、今後の検討事項として、タイムリーなパッチ適用の重要性、パッチの適用ができないシステムの扱いなどを取り上げていく予定。
- 「専門家養成」サブグループ
  必要な要件や、National Initiative on Cybersecurity Education（NICE）フレームワーク、北米電力信頼度協議会（NERC）の CIP、ISA99 などを参考に、必要な知識・スキル・能力を産業制御システムに合うよう見直し中。
- 「研究・開発」サブグループ
  7 月に会合を開き、研究開発要件についての様々な事項について議論を実施。また、グループの憲章について検討を実施。

制御システムセキュリティに関する寄稿

- 「安全でないプラットフォームに構築されるシステムのセキュリティを確保するには」
  汎用 OS やアプリケーションの利用が広がり、制御システムのセキュリティ対策が必須となっている。しかし、制御システムをネットワーク上で動作しているアプリケーションの一種に過ぎないと考えている運用者も多い。制御システムの端末にゲームがインストールされている、または、インターネットから自由にアクセス可能な状態になっているなどというのは、重要インフラの制御システムのセキュリティが人命に影響を及ぼす可能性があるということを未だ認識していないことを示している。制御システムを他のネットワークやシステムから隔離しても、スタックスネットからは守れなかった。同様に、ファイアウォーの設置も、適切なパスワードの管理も、USB メモリの使用ポリシーも、生体認証によるアクセス制限も、ただそれだけでは無意味であり、重要なのは、多層防御および定期的な健全性のチェックなしには、どんな個々の対策も決して有効に機能し得ないということである。

- 「制御システムに対する大規模なスパイ活動および攻撃の阻止」
  多くのケースにおいて、制御システムは企業システムと繋がっており、インターネットにも直接または企業ネットワークを介して繋がっている。制御システムと企業システムは互いを攻撃の入口として、攻撃者に攻撃の機会を与えており、片方を守りたければ両方を守る必要がある。
  数億にもおよぶセキュアでない装置から構成される制御システムのセキュリティをすぐに是正することは不可能であり、脅威の危険度によって優先順位をつけて対策をしていく必要がある。

  ＜優先的に対策すべき脅威＞
  - 優先度第 1 位：リモートネットワーク攻撃

ルータブルな TCP/IP アドレスを使っており、直接または間接的にインターネットに接続された制御システムが最も脅威が大きい。標的の幅が広大で、攻撃の反復性が高く、攻撃者側のリスクは低く、費用も掛からない。

- 優先度第 2 位：ルータブルなネットワークへのローカル攻撃
  スパイ活動や攻撃の仕掛けを行うのに、意図的にせよ意図的でないにせよ、誰かが少なくとも一時的に標的システムに近づける必要がある。攻撃者側のリスクも高くなり、標的の幅も狭く、攻撃の反復性も低くなる。
- 優先度第 3 位：非ルータブルなネットワークへのローカル攻撃
  意図をもった攻撃者が、持続的に標的システムに近づける状態にあり、かつ標的システムに関する実際的な知識を有する必要がある。サイバー攻撃として、最も攻撃者側のリスクが高く、規模が小さく、反復性が低く、費用の掛かる攻撃といえる。

また、各製品ベンダが提供する、個々の対策の寄せ集めでは、制御システム全体のセキュリティは確保できない。従って、ベンダに依存しないソリューションが必要となる。その一つが、多層防御の一層として、既存の機器に外付けし、通信の認証と暗号化を実現する「Bump in the Wire」の実装である。制御システムへの攻撃は、不正なデータをある時間以上挿入させることで、物理プロセスに影響を生じさせるものであり、継続的な認証を実施し、認証できない制御通信を拒否することで、攻撃の回避や、物理的影響を生じさせるのに必要な攻撃時間を与えないようにすることができる。

- 「グリッド・セキュリティ」
  電力網における SCADA システムは、サイバー・フィジカル・システム（補足：実世界（物理世界）と IT 技術が密接に統合されたシステム）であり、サイバー攻撃を阻止するには、IT セキュリティと SCADA セキュリティが揃っていなければならない。それでも、攻撃者は電力網を攻撃する手段を見つけ出してくるに違いない。電力網は、システム全体の状態を把握し、制御の判断を下す、状態推定装置（State Estimator（SE））によって維持・制御されている。攻撃者の目的は、何らかの方法で SE に不正なデータを供給することで、電力網の稼働を脅かすことである。不正なデータを検知するアルゴリズムは実装されているが、最近発表された研究によって検知を回避できることが実証されるなど、懸念もある。市場では多くの対策が提案されているが、電力網の崩壊が阻止可能だとは言い難く思われる。

  ＜攻撃防止システムの開発の障害と思われる問題＞
  - SCADA テストベッドの不足（米国および欧州に幾つかあるが、アジアにはない）
  - SE がより多くの情報に基づいて判断を行うのを支援するソリューションの欠如
  - 誤判定に伴う影響の大きさのための、重要インフラ運用者のセキュリティ対策に対する信頼の欠如
  - 時折問題が発生する、ソフトウェアのアップグレードに対する信頼の欠如
  - 重要インフラの制御システムが持つリアルタイム性から、警告メカニズムには、一般的な SCADA の情報処理サイクルよりずっと速い速度が要求される

以上