2012 年 9 月 5 日
独立行政法人情報処理推進機構（IPA）

ICS-CERT マンスリー・モニター（2012 年 6 月/7 月合併号）概要

本概要は、米国土安全保障省の運営する ICS-CERT（Industrial Control Systems Cyber Emergency Response Team）発行の“ICS-CERT Monthly Monitor June/July 2012”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/ICS-CERT_Monthly_Monitor_June-July2012.pdf

1. インシデントレスポンス活動

（1）石油・天然ガス業界を狙ったサイバー攻撃活動（4 月号続報）

マンスリー・モニター2012 年 4 月号で紹介した天然ガス業界を標的とするサイバー攻撃活動について、その後の ICS-CERT の調査・分析によれば、不正アクセスに有益な情報など、制御システム環境に関する情報が窃取されていることが判明した。

（2）ICS-CERT インシデント・サマリ・レポート公開

ICS-CERT インシデント・サマリーレポート（2012 年 6 月 28 日発行）では、2009 年の ICS-CERT 設立から、2011 年までの、インシデント対応活動の概要をまとめている。

※同レポートの内容については、別紙 ICS-CERT インシデントレスポンス・サマリーレポート概要参照

（3）ICS-CERT におけるインシデント対応フロー紹介

ICS-CERT におけるインシデント対応フローは、次のようになっている。先ず、攻撃を受けた事業者からインシデントの報告を受けると、受付担当者が受付チケットを発行し、対応担当者を割当てる。対応担当者は当該案件の ICS-CERT の窓口となり、事業者と協力して情報の収集および復旧を支援する。収集した情報は AAA（Advanced Analytical Laboratory）に送り解析を行う。AAA は指標報告書、媒体解析報告書を作成し、直接事業者に提出する。事業者の要請があり、且つ条件が合った場合には、現地にオンサイト対応チームを派遣する。オンサイト対応チームは通常、チームリーダ、解析担当者、制御システムの専門家から構成され、現地でログ等の解析や復旧・対策支援を行う。オンサイト対応終了後、対応担当者は事業者と連携し、支援を継続しつつ、追加の解析報告書の準備等を行う。ICS-CERT の解析が完了し、事業所に報告書を提出し、事業者と話し合い、これ以上の支援は必要ないことが確認できると、受付担当者が案件をクローズし、対応終了となる。

2. オンサイトレスポンス活動

（1）エネルギー事業者（5 月）

ログ分析からは、攻撃は成功しなかったと見られる。安全のため、ビジネスネットワークを含む全てのネットワークから切り離した。事業者は、当初制御システムをネットワークから切り離すのは不可能という認識であったが、検分したところ、リアルタイムアクセスの必要はなく、ルーチンワーク（データ取得など）を手動で行うことで問題ないことが判明したため、今後もネットワークから切り離したままとした。

（2）製造事業者（6 月）

1,700 を超える機器のログ、プロキシのログ等の分析を行い、侵入の痕跡を発見。その後もスピアフィ

ッシングメールが届くなど攻撃が続いており、製造事業者と協力し対応継続中。

オンサイト対応では、両事業者を通じて、ビジネス/制御システムネットワークおよび通信アーキテクチャのレビュー、ビジネスネットワーク/制御システムネットワークの接続ポイントの確認と、よりセキュアなシステム形態の検討、技術スタッフおよび経営陣へのサイバー攻撃に関するブリーフィングを実施した。

ICS-CERT では、多層防御への取組みを勧めるとともに、今後もソーシャルエンジニアリングを利用したサイバー攻撃について、教育を行っていく。また、ICS-TIP-12-146-01A-Targeted Cyber Intrusion Mitigation Strategies(標的型攻撃緩和対策)、ICS-CERT:Incident Handling Brochure(インシデント対応の心得)についても参照可能。

なお、2009 年～2011 年までの活動内容は、ICS-CERT Incident Summary Report を参照。(抄訳はこちら)

3. 今月のトピックス

(1)ネットワーク機器に広く見られる「弱い認証鍵」

ICS-CERT では、SSH と SSL 証明書の脆弱性について、ミシガン大学、カリフォルニア大学サンディエゴ校の研究者と調整を行った。研究(Mining Your Ps and Os:Detection of Widespread Weak Keys in Network Devices)では、暗号鍵や証明書の使い回し、暗号化時の鍵のランダム性の不足が原因と見られる。ICS-CERT では、影響を受けるベンダの支援・対応を進めている。

(2)エネルギー省(DoD)、リスク管理ガイドラインを公開

エネルギー省(DoD)、標準技術研究所(NIST)、北米電力信頼度協議会(NERC)と連携し、Electricity Subsector Cybersecurity Risk Management Process を公開。

4. CSSP(Control Systems Security Program)ニュース

ICSJWG (Industrial Control Systems Joint Working Group)2012 Fall Meeting が、2012 年 10 月 15～18 日に、米コロラド州デンバーにて開催される。制御システムセキュリティの最新動向に関するセッションやミーティング、訓練等を提供。参加無料。

※米国民以外は、10 月 18 日の International Partners Day のみ参加可

5. NCCIC(National Cybersecurity and Communications Integrity Center)ニュース

2012 年 6 月に、国家サイバーセキュリティ・通信統合センター(NCCIC) ディレクターに、Larry Zelvin 氏が就任。前ホワイトハウスの National Security Staff として、2010 年メキシコ湾原油流出事故等に対応。

※NCCIC は、米国のサイバーネットワークおよび通信ネットワークのセキュリティと運用を確保すべく、24 時間 365 日定常ベースで、連邦・州・地方機関、民間からの情報を集約し、活動の調整を行っている

6. 今月のオープンソースニュース(ハイライト)

- 米国の産業制御システムに対するサイバー攻撃が急増 (2012-06-29)
- 国土安全保障省(DHS)、政府機関に対し「サイバー脅威対策パック」を提供 (2012-06-26)
- 研究者ら、RSA SecurID トークンの暗号鍵を破る攻撃方法を公開 (2012-06-25)
- サイバーセキュリティ法案、企業の利益と国の安全保障の対立 (2012-06-25)
- イラン、原子力施設に対する「大規模サイバー攻撃」を検知したと報道 (2012-06-21)
- ハッキング被害に遭った企業、第三者を雇って犯人のシステムを逆にハッキングさせるなどの報復に転じる企業も (2012-06-19)

- 生命維持に直結する医療機器用ソフトウェアのアップデート版をダウンロードするのは非常に危険（2012-06-19）
- 米研究者ら、SCADA セキュリティ関連企業、国防企業、大学等へのサイバー攻撃について、中国が関わっていると推察（2012-06-13）
- Flame マルウェアの製作者ら、手掛かりを残さないよう、自己破壊機能を配信して感染 PC から Flame の痕跡削除を図る（2012-06-07）
- 米エネルギー省（DOE）：SCADA セキュリティを改善する 21 のステップ（2012-06-05）
- 米国土安全保障省（DHS）から重要インフラ事業者へ：サイバー攻撃を検知した場合、証拠となるデータを保全すること（2012-05-29）
- 英研究者ら、世界で初めてチップにバックドアを発見。チップ上の情報の変更をモニタリング可能（2012―05-29）
- 米エネルギー省（DOE）、電力業界向けのリスク管理プロセスガイドラインを公開（2012-05-23）

7. 今後のイベント

※原文の UPCOMING EVENTS をご参照ください。

8. 最近公表された制御システム関連の脆弱性

※原文の RECENT PRODUCT RELEASES をご参照ください。

以上