2013 年 1 月 10 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 10 月/11 月/12 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 October/November/December 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。（※特記が無い限り、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_Oct-Dec2012.pdf

1. インシデントレスポンス活動

（1）制御システム環境におけるウィルス感染

ICS-CERT では、ある発電所で、制御システムの設定ファイルのバックアップに使用した USB を介して、システム運用に不可欠なワークステーション 2 台がマルウェアに感染したインシデントについて、オンサイト対応（※補足 1）を行った。この 2 台はバックアップが取られておらず、下手にクリーンアップを行うと制御システムの運用に多大な影響を及ぼす恐れがあるため、ICS-CERT では当該システムのベンダと密接に連携して対応にあたった。

制御システム環境でウィルス対策ソフトを運用するのは大変であるが、入っていれば USB やワークステーションの感染を検知できたと思われる。また、USB の感染がバックアップ運用に悪影響を及ぼさないような手順を確立すべきである（例えば、毎回 USB のウィルスチェックを実施する、CD-R や DVD-R を用いるなど）。加えて、運用に不可欠なワークステーションは全てバックアップを行うよう徹底すべきである。

※補足 1

ICS-CERT は、制御システムに関する脆弱性情報の受付、ベンダとの調整、脆弱性および対策情報の提供のほか、必要に応じて攻撃に遭った組織にオンサイト対応チームを派遣し、データの収集や調査、対策の検討支援を行い、持ち帰ったデータの分析なども行っています。ICS-CERT のオンサイト対応については「ICS-CERT マンスリー・モニター（6 月/7 月合併号）概要」で紹介していますので、ご参照ください。

（2）電力会社におけるウィルス感染

2012 年 10 月初旬、電力会社から ICS-CERT に、システムのアップデート作業者が使用した USB を介して、制御システムネットワーク上の 10 台のコンピュータがウィルスに感染したとの報告があった。システムはアップデート作業のため停止中であったが、これにより再稼働が約 3 週間遅延した。

重要インフラ事業者には、ウィルス定義を常に最新にしておくこと、セキュリティパッチの管理、リムーバブルメディアの使用に関する統制など、基本的なセキュリティポリシーを策定し、実施すべきであると重ねて強調したい。また、インシデントの影響を低減するためには多層防御も必須である。詳細は「多層防御戦略による産業制御システムのサイバーセキュリティ改善（Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies）」を参照のこと。

2. 今月のトピックス

(1)共通脆弱性評価システム(CVSS)

ICS-CERT では、公開する脆弱性の深刻さを理解する上での一助としてもらうため、脆弱性に CVSS 基本値を付けて公開している。

＜CVSS とは＞

元はグローバルな脆弱性公開フレームワークの確立を目指し、複数の脆弱性評価手法の使用に伴う問題を解決するべく、NIAC(National Infrastructure Advisory Council)の後援で進められていたが、現在は FIRST(Forum of Incident Response and Security Team)が運用している。最新版は Version 2。

CVSS 値は 0～10 で示され(10 が最も深刻)、「基本値」「現状値」「環境値」の 3 つの値で算出される。現状値と環境値はオプションであるが、評価時点における脆弱性への脅威の存在や利用環境も値として算出し、一般値である基本値を、評価したいシステムに合わせてカスタマイズすることができる。

ICS-CERT では CVSS の算出に、標準技術研究所(NIST)が提供するツール「CVSS Version 2 Calculator」を使用している(CVSS に関する詳細は FIRST の CVSS ページ参照)。なお、米国の脆弱性情報データベース「National Vulnerability Database(NVD)」に掲載されているほぼ全ての脆弱性についても、深刻度として CVSS 基本値が採用されている(※補足 2)。

※補足 2

日本の脆弱性対策情報データベース「JVN iPedia」も、脆弱性の深刻度に CVSS 基本値を採用しています。また、CVSS については、IPA のホームページにおいても日本語で CVSS 概説および CVSS 計算ツールを公開していますので、ご活用ください。

(2)プロジェクト「SHINE(SHodan Intelligence Extraction)」

セキュリティ研究者 Bob Radvanovsky 氏と Jake Brodsky 氏による、インターネットに繋がっているコンピュータ機器を検索する検索エンジン「SHODAN」を使って、インターネットに接続された制御システム関連機器を探し、リストアップするプロジェクトで、約 50 万台の制御システム関連機器を発見した。中にはログイン認証を必要としない機器もあったという。SHINE の目的はセキュリティ意識の向上を促すことであり、SHODAN を使用して、誰でもこれらの機器を見つけ、制御システムに不正アクセスできてしまう危険性を警告している。ICS-CERT では、両氏からの報告を受けてこれらの機器を業種、所属組織、場所などで整理し、約 98,000 が米国内の組織であることを確認した。そのうちの多くは直接的に制御システムと関連するものではなく、最終的には約 7,200 が制御システム関連の機器と判明した。米国外のものについては、これまでに 100 ヶ国以上の CERT に通知を行っている。

ICS-CERT では、ベストプラクティスに従い、制御システム機器を直接インターネットに接続しない、ファイヤウォールの内側に設置する、リモートアクセスが必要な場合 VPN 等を使う、ログインのロックアウトを設定するなどの対策を取ることを推奨する。詳細は、以下のドキュメントを参照のこと。

- 多層防御戦略による産業制御システムのサイバーセキュリティ改善(Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies)
- 増大する産業制御システムへの脅威(Increasing Threat to Industrial Control Systems)

（3）「Action Campaign」イニシアチブ

ICS-CERT では、重要インフラシステムの所有者や関係者に対して、積極的なセキュリティブリーフィングを実施している。2011 年から 2012 年にかけて、石油・ガスパイプラインや電力網などエネルギー業界へのサイバー攻撃が急増しており、2012 年だけでも ICS-CERT に報告されたインシデントの 4 割を超えている。

ICS-CERT では、エネルギー省や他の連邦政府機関と連携し、「Action Campaign」と称する、機密情報を扱う、または一般情報のみを扱うブリーフィングを、ニューヨーク、シカゴ、ダラス、ヒューストン、アラスカなどの主要マーケットの関係者らと行い、サイバー攻撃の傾向や事例、制御システムの脆弱性、セキュリティ戦略やベストプラクティスなどについて情報提供をしている。また、ビデオカンファレンスによるブリーフィングも行っている。こうした活動が重要な役割を果たすと信じており、今後もこうしたブリーフィングを、情報のアップデートも兼ねて定期的に行っていく予定である。

3. ICS-CERT ニュース

（1）ICS-CERT の FY2012 の活動概要

FY2012（2011/10～2012/9）に、ICS-CERT では 198 件のインシデント対応を行った。そのうちの 41%はエネルギー業界におけるインシデントであり、23 件が石油・ガス業界だった。分析の結果、制御システムにリモートから不正アクセスや操作を行うのに使えそうな情報を含む、制御システム環境に関する情報が盗まれていた。

水道業界のインシデントが 2 番目に多く、全体の 15%を占めた（スピアフィッシングと、インターネットに接続されたシステムに起因するインシデントが主）。なお、メディアでも大きく取り上げられたイリノイ州スプリングフィールドの事件ではオンサイト対応を行ったが、制御システムに侵入された痕跡はなく、ポンプの障害は摩耗による事故と思われる。

原子力業界からも、OA ネットワークに侵入され、情報が盗まれたとの報告が 6 件あった。OA ネットワークから制御ネットワークへの侵入を狙った標的型攻撃の可能性を考え、ICS-CERT では事業者と共にネットワークトポロジーや侵入を許すような経路が無いか調査を行ったが、制御システムへの侵入は確認されなかった。

（2）インターネットに接続された制御システム機器

FY2012 は、インターネットに接続された制御システム機器が懸念となった年でもあった。SHODAN や ERIPP（Every Routable IP Project）を使用して、インターネットから不正アクセス可能な制御システム関連機器を 2 万以上発見した研究者もいる。多くは州や地方行政機関が所有する機器であり、他は海外であった。海外のものは、当該システムの所有者や運用者に通知を行うべく、他国の 63 の CERT と連携を進めている。

ICS-CERT では、事業者に対し、実際のインターネットへの接続状況や認識に関わらず、不適切な設定やデフォルトパスワードを使用していないかなどを再確認するため、制御システムの監査の実施を奨励する。

（3）脆弱性の報告とベンダとの調整

より多くの研究者が、ICS-CERT を ICS ベンダとの調整役として活用するようになったこともあり、多くの脆弱性が報告されるようになった。FY2012 は 171 の脆弱性を取り扱い、55 のベンダと調整を行った。脆弱性の数は FY2011 から増加しており、最も多く報告された脆弱性はバッファオーバーフローで、FY2011 の 46%からは落ちるものの、26%であった。

＜FY2012 に報告された脆弱性の種類と報告件数＞

Vulnerability Type	
Buffer Overflow	44
Input Validation	13
Resource Exhaustion	8
Authentication	8
Cross-site Scripting	8
Path Traversal	8
Resource Management	8
Access Control	7
Hard-coded Password	7
DLL Hijacking	6
SQL Injection	4
Credentials Management	3
Cryptographic Issues	3
Insufficient Entropy	3
Use After Free	3
Use of Hard-coded Credentials	2
Cross-Site Request Forgery	2
Privilege Management	2
Write-what-where Condition	2
Integer Overflow or Wraparound	2
Inadequate Encryption Strength	2
Missing Encryption of Sensitive Data	1
Code Injection	1
Forced Browsing	1
Miscellaneous	15
Total	171

Figure 5: Vulnerabilities by type, Fiscal Year 2012.

その他に特筆すべき点として、ハードウェア（ICS ネットワーク機器や医療機器など）に関連する脆弱性が多く見られるようになっていること、デジタルボンド社の Project Basecamp において主要 ICS ベンダのプログラマブル・ロジック・コントローラ（PLC）に多くの脆弱性が見つかったこと、異なる制御システムを統合できることで影響の大きい Tridium Niagara AX Framework のソフトウェアに複数の脆弱性が見つかったこと等が挙げられる。これらの脆弱性に関するベンダとの長きにわたる調整の結果、ICS-CERT では、脆弱性公開ポリシーを見直し、ベンダの対応如何によってはパッチや回避策の有無に関わらず、ベンダへの通知から 45 日経過後に脆弱性を公開する可能性がある旨の変更を行った。これは制御システムコミュニティのセキュリティ情報を必要とするというニーズと、ICS ベンダの対策に時間を必要とするというニーズのバランスを考慮した結果であり、最終的な判断は全関係者の最大の利益を考慮して決定する。

（4）情報発信

ICS-CERT では、FY2012 に 332 件の情報を発信し、制御システムに影響を及ぼす可能性のある様々な脆弱性や脅威を警告した。2013 年も引き続き情報やサービスの改善に努めるが、鍵は関係者との情報共有で

あり、重要インフラにおけるサイバーリスクの低減とセキュリティ改善に向けて取り組んでいく。

（5）ICSJWG 秋季会合

国土安全保障省は、10/15～18 にコロラド州デンバーにおいて ICSJWG（Industrial Control Systems Joint Working Group）の秋季会合を開催した。269 人が集まり、多くの講演を通じて知識を深めたが、Billy Rois 氏の制御システムへのハッキングのデモンストレーションは、参加者がハッカーのモチベーションや考え方、攻撃手法を理解するのに大いに役立ったと思われる。

4. 最近公開された脆弱性

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

5. 今月のオープンソースニュース（ハイライト）

- 新しいマルウェア、殆どのマルウェア対策ソフトで検知されず（2012/11/28）
- 国際原子力機関（IAEA）、盗まれた情報がハッカーサイトに掲載されたと報告（2012/11/27）
- コロンビア大の研究者ら、組込みシステムの CPU 上で独立して動作し、サイバー攻撃を阻止するセキュリティ機能「symbiotes（シンビオート）」を研究中（2012/11/26）
- セキュリティベンダ ReVuln、SCADA ソフトウェアの未知の脆弱性を 9 つ発見したと発表。会社の「資産」であり、ベンダに情報提供するつもりは一切なしと公言（2012/11/21）
- ミシガン大学に、米国初の医療機器のセキュリティに関する講義が開設（2012/11/16）
- 標準技術研究所（NIST）、効果的な継続的監視（continuous monitoring）のためのガイドラインを公開（2012/11/16）
- 4G 携帯ネットワーク（LTE）、単純なジャミング手法を使うことで無効化が可能（2012/11/15）
- ICS-CERT こそ、米国のサイバーディフェンスの要となるセキュリティエキスパート（2012/11/14）
- 自己回復機能を備えた電力網の 7 要素（2012/11/13）
- サイバーエコシステム（機械学習と情報共有によって、自動的に脅威を検知し、回避し、対応する）は政府ネットワークを守れるか（2012/11/7）
- 北米電力信頼度評議会（NERC）のセキュリティ標準 CIP v5、片方向にしかデータを流さないセキュリティ・ゲートウェイの採用を奨励（2012/11/5） ※原文 URL リンク切れのため、別サイトの URL を掲載
- ホワイトハウス、諜報機関に対して民間企業とセキュリティ情報を共有するよう指示（2012/10/20）
- 「フレーム」に、規模は小さいがより凶悪な同族マルウェアが存在か（2012/10/15）
- セキュリティベンダ Gleg、SCADA＋ Exploit Pack と Agora Exploit Pack の最新版をリリース。未知の脆弱性の攻撃コードも含む（2012/10/10）
- 科学は犯罪を止められるか（2012/10/10）
- 米国の銀行を狙ったサイバー攻撃、攻撃の核となるツールがサウジアラビアで発見される（2012/10/5）
- サイバー攻撃を行う場合、システムにアクセスするためにはソーシャルエンジニアリングによる「人」のハッキングが効果的（2012/9/26）
- 初期の Cult of the Dead Cow からアノニマスまで、ハクティビストの思想や文化に迫るドキュメンタリー「We are Legion： The Story of Hacktivists」がリリース（2012/9/24）
- ORing Industrial Networking 社のネットワーク機器の脆弱性、石油・ガス会社をサイバー攻撃のリスクに晒す（2012/9/21）
- ナポリターノ国土安全保障省長官、サイバーセキュリティに関する行政命令（EO）が完成真近と話す（2012/9/19）

- 米国務省の顧問弁護士、サイバー攻撃による自衛権の行使は可能と発言（2012/9/18）

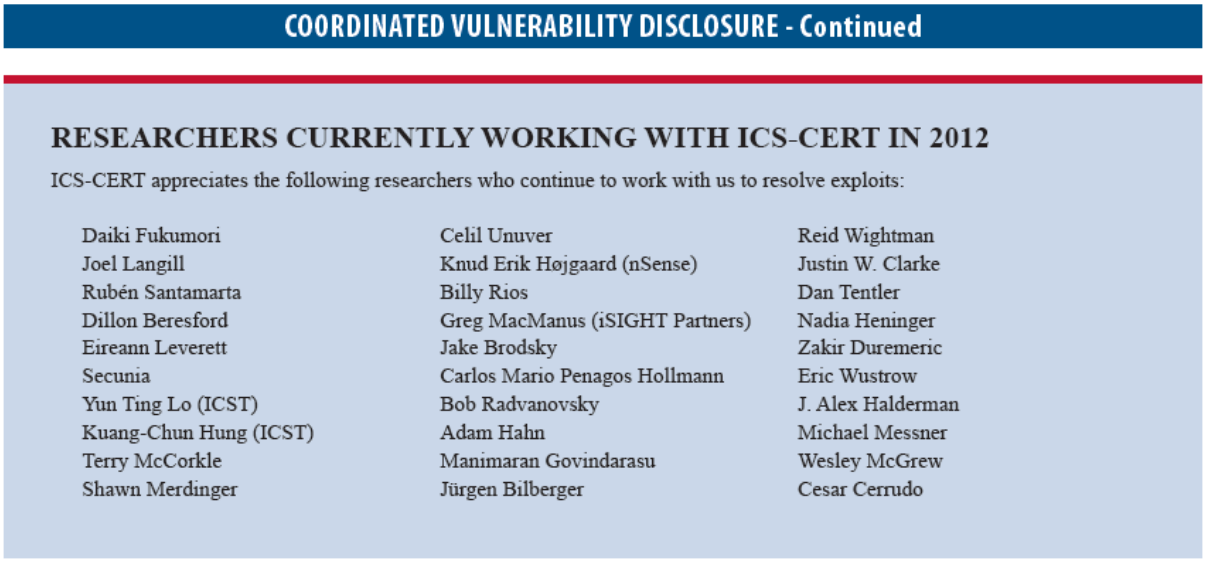
6. 今後のイベント

※原文の UPCOMING EVENTS をご参照ください。

7. 協調的な脆弱性の公開（CVD）に協力頂いたセキュリティ研究者の方々（2012 年第 4 四半期）

※ICS-CERT では、脆弱性を ICS-CERT に報告し、ベンダとの調整に協力くださったセキュリティ研究者の方々に感謝の意を表し、当該研究者の方々の功績として、氏名と対象の脆弱性の一覧を掲載しています。実際の氏名・脆弱性については、原文の RESEARCHERS ASSISTING ICS-CERT IN THE FOURTH QUARTER OF 2012 をご参照ください。

8. 脆弱性対策に協力頂いたセキュリティ研究者の方々（2012 年）



以上