2014 年 7 月 31 日
独立行政法人情報処理推進機構（IPA）

ICS-CERT モニター（2014 年 1 月～4 月号）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 Monitor January – April 2014”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、全て英語となります）
URL：
http://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_%20Jan-April2014.pdf

1. インシデントレスポンス活動

（1）インターネットに接続された制御システム

SHODAN や Google のような検索エンジンの存在や、制御システムに関する公開情報が増加したこと等も相俟って、インターネットに繋がっている制御システム機器の探索が容易になり、制御システム機器への不正アクセスのリスクが高まっている。また、多くの場合、機器へのアクセス制御が適切に設定されていないことが、不正アクセスを許してしまうリスクを更に高めている。

最近のインシデント事例（下表）でも、事業者は自分たちの制御システム機器がインターネットからアクセスできる状態であることに気づいていないことがあった。事業者は、攻撃者によって SHODAN や Google といったツールを使った探索が行われていることを理解し、自組織の重要機器がインターネットに繋がっていないか、至急見直すことが望まれる。

インターネットに接続された制御システム機器に関する最近のインシデント事例

	事例 1	事例 2	事例 3
概要	制御システムネットワークへの不正侵入	制御システムサーバへの不正アクセス	空調システム、エネルギー管理システムが、外部からアクセス可能な状態であることが発覚
問題の発見者／攻撃者	第三者（不明）	第三者（不明）	セキュリティ研究者
認証等の有無	パスワードによる簡単な認証機能があったが、総当り攻撃で容易に破ることが可能だった	ファイアウォール等の設置なし、アクセス制御なし	認証なし
備考	調査の結果、以前にも侵入されていた痕跡あり。	SCADA プロトコル、HTTP プロトコルを使用してアクセス。 長期間に渡って不正アクセスされていたと見られるが、調査の結果、不正な操作やコードのインストールは確認されず。	ソチオリンピックの会場となったアリーナのシステム。オリンピックの開会前に対策を実施。

ICS-CERT が提供する参考情報：
インターネットからアクセス可能な制御機器に関する注意喚起
http://ics-cert.us-cert.gov/alerts/ICS-ALERT-11-343-01A
http://ics-cert.us-cert.gov/alerts/ICS-ALERT-10-301-01

【 IPA 補足 】

IPA では、インターネットに接続されている自組織の機器を SHODAN を利活用してチェックする方法や対策を纏めたレポートを公開しています。併せてご参照ください。

「IPA テクニカルウォッチ：増加するインターネット接続機器の不適切な情報公開とその対策」

http://www.ipa.go.jp/about/technicalwatch/20140227.html

（2）2013 年度の脆弱性状況

2013 年度は、181 件の制御システムの問題点が報告され、うち 177 件が脆弱性と確認された。このうち、87%がリモートから攻撃可能な脆弱性であった。ハードコードされた ID・パスワードや弱い認証鍵など、認証関連の問題が最も多く見られた。これらの問題は、スキルの低いハッカーによる攻撃も可能にしてしまうため、最も懸念が高いと言える。また、2013 年度は食品・医薬品局（FDA）との連携を確立し、医療機器の脆弱性についても取り組んだ。これに伴い、FDA では昨夏、医療機関や医療機器ベンダ等に向けたセキュリティベストプラクティスの公開も行っている[1]。また、DNP3 の実装に関する脆弱性も多く報告され、ICS-CERT からアドバイザリを発行した[2]。

報告された脆弱性の 65%は、深刻度が CVSS 7.0 以上の危険なものであった。基本的な対策として、ネットワークへの接続を最低限に抑え、ファイアウォールによりインターネットから直接アクセスできないようにするほか、パッチやアップデートが出た場合は、必要な検証を行い、現実的なレベルで可能な限り早くあてることが重要である。

（3）オンサイト対応

2014 年第 2 四半期（2014/1/3/31）には、20 件のオンサイト対応（CSET を用いたセキュリティ評価、設計・アーキテクチャのレビュー（DAR）、ネットワークのトラフィック分析（NAVV）等）を行った。半数超の 11 件が水道業界で、残りは、電気・運輸・核施設であった。

オンサイト評価から分析するに、多くの施設には共通のセキュリティ上の問題がある（下表）。

ICS-CERT 評価チームが特定した、よく見られる脆弱性や弱点

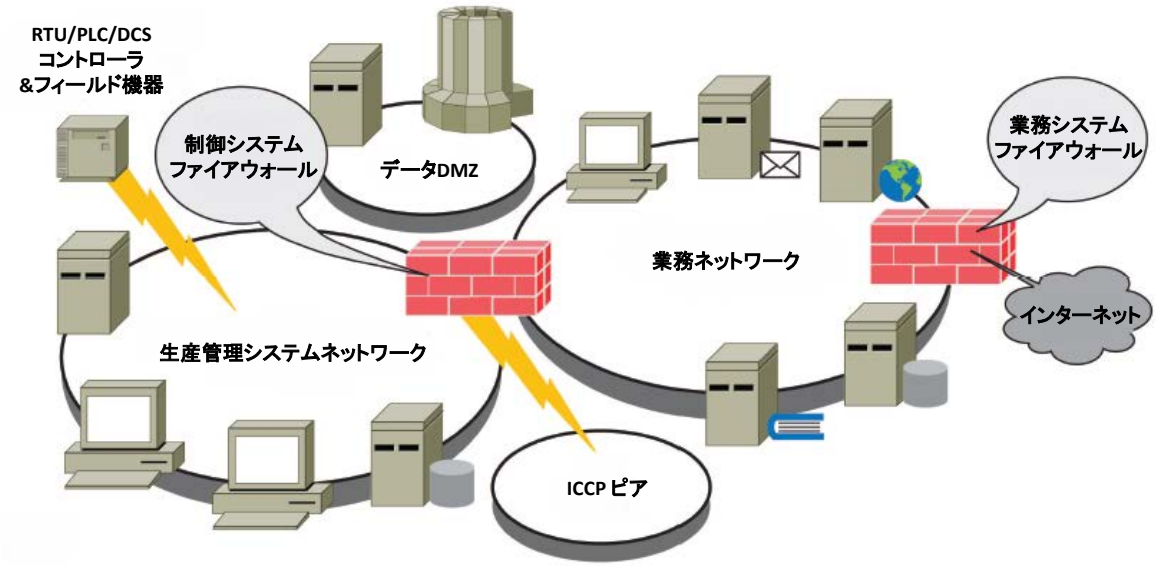
カテゴリー	共通する問題点
認可・権限・アクセス制御の問題	システムへのアクセス制御が不十分
不適切な認証	システムの認証が不十分
証明書・パスワードの管理	認証情報の保護が不十分
	弱いパスワードの使用
セキュリティ構成・管理	テスト環境が乏しい
	パッチ管理が乏しい（パッチ管理が制限されている）
	バックアップ／リストアが十分かつ適切にできていない
計画／ポリシー／手順	セキュリティ関連文書のドキュメント化およびメンテナンスができていない
	文書が正式に作成されていない
	災害復旧プロセスが周知されて（浸透して）いない

[1] 医療機器および病院のネットワークにおけるサイバーセキュリティ（FDA 安全情報）
http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm356423.htm

[2] DNP3 の実装に関わる脆弱性：
http://ics-cert.us-cert.gov/advisories/ICSA-13-291-01B

カテゴリー	共通する問題点
ネットワーク設計上の問題	共通して見られる ICS ネットワークの設計上の問題
	セキュリティパラメータが決められていない
	ネットワークがセグメント化されていない
	機能的な DMZ が実装されていない
	ファイアウォールを設置していない、または設定が不適切
ネットワークコンポーネントの設定（実装）上の脆弱性	ネットワーク機器の設定が不適切 ポートのセキュリティ対策がされていない

特に、ネットワーク設計上の問題がよく見受けられる。DMZ を含め、ネットワークのセグメント化を適切に行うことで、侵入のハードルを上げることができる。



3. ICS-CERT ニュース

（1）Enhanced Cybersecurity Services（ECS）プログラム [3]の新設

ECS は、サイバーセキュリティベンダや、情報機関を含む政府機関など、幅広い組織を情報源としたサイバー脅威情報や攻撃情報の共有サービスで、重要インフラ事業者に脅威や攻撃の検知のためのインディケータ（indicators）等を提供する。共有される情報には、最高機密（Top Secret）扱いの機密情報なども含まれる。重要インフラ事業者は、ECS が規定する条件を満たした Commercial Service Provider（CSP）を通じて情報を受け取ることができる。（現在認可済の CSP は、AT&T と Century Link の 2 社）

（2）STIX に準拠した情報配信

ICS-CERT では、サイバー脅威情報や攻撃情報の配信にあたり、STIX（Structured Threat Information eXpression）[4]に沿ったフォーマットで配信している。STIX は機械読み取り可能なフォーマットであり、将来的な機械処理による対応時間や手間の短縮に向けて、ICS-CERT では、STIX で記載された情報を TAXII（Trusted

[3] Enhanced Cybersecurity Services
http://www.dhs.gov/enhanced-cybersecurity-services
[4] STIX
http://stix.mitre.org/

Automation eXchange of Indicator Information）[5]で配信・共有する取組みに着手した。

（3）ウェブベースの ICS トレーニングの提供を開始

ICS-CERT では、ウェブベースの ICS トレーニングコースとなる「Cybersecurity for Industrial Control Systems（201W）」の提供を開始した。同コースは、講義形態で提供されている「初級コース（101）」「中級コース（201）」の e ラーニング版となっている。詳細は、ICS-CERT の Training ページを参照のこと。

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. オープンソースニュース(ハイライト)

- GPS の先導者、妨害（サイバー攻撃）による影響の重大さを懸念（2014/2/14）
- クラウドサービスのサイバー犯罪への悪用（2014/2/14）
- ホワイトハウス、サイバーセキュリティ・フレームワークの活用を促す（2014/2/12）
- バンキング・決済サービス最大手 Fidelity National Information Services（FIS）、サイバーセキュリティへの取組みでマイクロソフトと連携（2014/2/12）
- 電力システムのセキュリティ確保、権限を有する所轄機関を 1 つに絞るべき（2014/2/12）
- 米政府、Target 等の小売業に対するサイバー攻撃について、米国経済を狙った組織的攻撃ではなかったと判断（2014/2/10）
- 米保健福祉省（HHS）観察総監室（OIG）、医療機器のセキュリティを見直し（2014/2/10）
- 調査：国防総省（DOD）の生命線である「燃料供給」の管理にサイバーリスク（2014/2/7）
- 調査：多くのセキュリティ担当者ら、インシデントに対処できるか不安を感じていると回答（2014/2/13）
- セキュリティ研究者ら、政府機関やエネルギー企業を狙ったサイバー活動（「The Mask」）を発見（2014/2/11）
- 米国防総省（DOD）、コンペティションの開催を通じて軍人のサイバーセキュリティ訓練・スキルアップを図る（2014/2/6）
- 重要インフラのサイバーセキュリティ対策強化を目指す法案、下院で巡回中（2014/2/15）
- サイバー攻撃が増加 ― とりわけヘルスケアデータが標的に（2014/2/5）
- 米国土安全保障省（DHS）、大統領令第 13686 号に基づき、サイバーセキュリティ・フレームワークの利活用促進策を検討（2014/1/31）
- GAO、911 番のような緊急システムに対するサイバー攻撃を警告（2014/1/30）
  ※911 番は、日本における 110 番・119 番
- 空軍の研究者ら、プログラマブル・ロジック・コントローラ（PLC）のファームウェアに隠蔽できるルートキットのプロトタイプを開発（2014/1/27）
- 電力システムのサイバーセキュリティに関する規制で物議（2014/1/24）
- コンピュータ機器のレジリエンシー、年々進化し「防御」を提供（2014/1/21）
- 調査：通信速度が遅く、警告が表示されるシステムにハッカーは長居せず（2014/1/17）
- Proofpoint 社、モノのインターネット（IoT）を踏み台にしたサイバー攻撃を発見（2014/1/16）
- ミシガン大学の研究者ら、ゼロデイ脆弱性を見つけたとして、すぐ攻撃すべきか待つべきか、最適

[5] TAXII
http://taxii.mitre.org/

の「攻撃タイミング」を算出する数学的モデルを提示（2014/1/15）

- 米軍サイバーコマンドの予算、ほぼ倍に（2014/1/14）
- 国防総省（DOD）高官ら、サイバーセキュリティは最大のテロの脅威を話す（2014/1/6）
- 物理対策とサイバーセキュリティ対策、両輪での対策が重要（2014/12/19）
- 米下院、サイバーセキュリティ法案 H.R.3696 を提出（2013/12/16）
- 15 人の兵士ら、陸軍のサイバー戦闘員養成コースを終了（2013/12/6）
- 北大西洋条約機構（NATO）、過去最大のサイバー演習を実施（2013/11/26）

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

※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 COORDINATED VULNERABILITY DISCLOSURE を参照ください。

8. 脆弱性対策に協力頂いたセキュリティ研究者の方々

RESEARCHERS CURRENTLY WORKING WITH ICS-CERT

ICS-CERT appreciates the following researchers who continue to work with us to resolve exploits:

Aaron Patterson	Eric Wustrow	Neil Smith
Aaron Portnoy	Gleb Gritsai	Ng Yi Teng
Adam Crain	Hisashi Kojima	Nicholas Miles
Aivar Liimets	Ho Ping Hou	Nin3
Alex Timorin	Ilya Karpov	Postive Technologies Security
Alexey Osipov	J. Alex Halderman	Ralf Spenneberg
Amisto0x07	J Andrew Brooks	Reid Wightman
Andrew Brooks	Joel Langill	Roman Ilin
Anton Popov	John Adam Crain	Rubén Santamarta
Artem Chaykin	Jon Christmas	Ryan Green
Arthur Gervais	Juan Vasquez	Ryan Lee
Billy Rios	Jürgen Bilberger	Sascha Zinke
“Blake”	Kirill Nesterov	Sergey Bobrov
Bob Radvanovsky	Kuang-Chun Hung (ICST)	Sergey Gordeychick
Brendan Harris	Kyle Stone	Seyed Dawood Sajjadi Torshizi
Brian Meixell	Ling Toh Koh	Shawn Merdinger
Carlos Mario Penagos Hollmann	Llya Karpov	Stephen Dunlap
Carsten Eiram	Lucas Apa	Terry McCorkle
Cesar Cerrudo	Lucian Cojocar	Timur Yunusov
Christopher Scheuring	Luigi Auriemma	Wei Gao
Christopher Sistrunk	Marc Ayala	Yury Goltsev
Dale Peterson	Mashahiro Nakada	Zakir Durumeric
Dillion Beresford	Mehdi Sabraoui	Z0mb1E
Dmitry Serebryannikov	Michael Messner	0x7A240E67
Eireann Leverett	Michael Toecker	
Eric Forner`	Nadia Heninger	

以上