2016 年 7 月 28 日
独立行政法人情報処理推進機構（IPA）

ICS-CERT モニター（2016 年 5･6 月号）概要

本概要は、米国土安全保障省（DHS） Industrial Control Systems Cyber Emergency Response Team（ICS-CERT）発行の“*ICS-CERT Monitor May/June 2016*”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：https://ics-cert.us-cert.gov/monitors/ICS-MM201606

1. インシデント対応活動 ～ SHODAN[1]で見つかった制御機器に関する ISP を通じた注意喚起 ～

ICS-CERT では、インターネットに接続された制御機器が多数存在することを確認した。多くの機器はインターネットサービスプロバイダ（ISP）の IP アドレスを使用しており所有者が特定できないため、ICS-CERT では ISP に対して、「制御機器が意図せずインターネットに晒されている可能性がある」および「支援が必要であれば ICS-CERT に連絡して欲しい」とのメッセージを、当該機器の所有者（ISP にとっては顧客）に転送してくれるよう依頼した。その結果、ある水道施設のベンダ／SIer から支援依頼があり、現在対応を実施中。

2. セキュリティトピックス

（1） 自組織の制御システム／ネットワークを攻撃者視点で視る

ICS-CERT では、以下のセキュリティ評価サービスを通じて、事業者における重要インフラサービスの監視・制御システムのサイバーセキュリティ対策状況を調査している。

評価サービス	目的
Cyber Security Evaluation Tool（CSET）	「はい／いいえ」で回答するタイプの質問による、ライフサイクルを通じた運用管理に関する対策状況の確認
Design Architecture Review（DAR）	ネットワーク構成に関する、より自由な質疑応答を通じた情報収集および実状の把握
Network Architecture Verification and Validation（NAVV）	ネットワーク境界点におけるデータトラフィックの分析による実状の把握

これまでの経験から、事業者のサイバーセキュリティ対策の成熟度（maturity level）は、組織が自分たちの制御システムおよびネットワークについてどれだけ知っており、理解しているかによると考えられる。

評価チームは、公開情報調査や SHODAN による調査、ICS ネットワークのポートスキャンといった手法を教示し、攻撃者が当該組織について何を知っており、どう攻撃に生かしてくるかを学び、対策に役立てられるよう支援している。

---

[1] SHODAN https://www.shodan.io/ インターネットに接続されたコンピュータ機器のサーチエンジン。概要・活用方法については、以下の IPA テクニカルウォッチを参照。
「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（改訂版）」
https://www.ipa.go.jp/security/technicalwatch/20160531.html

（2） 重要インフラ情報保護プログラムの適用を受ける方法

前号（ICS-CERT モニター（2016 年 3･4 月号）[2]）では、事業者が政府と共有したインシデント情報等について、政府による厳格な取扱いとセキュリティ対策の実施、および情報が一般に公開されないことを保証する「重要インフラ情報保護（Protected Critical Infrastructure Information（PCII））プログラム」について説明した。今号では、事業者が PCII の適用を受けるにはどうしたらよいかを説明する。

PCII プログラムの適用手続きは、情報共有時に「Express Statement[3]」を添付し、当該情報が PCII プログラムによって保護されることを前提として共有されるものであることを明言することにより始まる。署名がされ、手続きが完了すれば、プログラムが定める保護が適用される。事業者に代わり、SIer が Express Statement を提出しても構わない。

留意点として、もし事業者の属する重要インフラ業界が法規によりインシデント発生時に規制当局への届け出を義務付けられている場合、ICS-CERT は PCII プログラムに従い一切の情報提供や証言ができないため、事業者自身が別途届け出る必要がある。

PCII プログラムに関して質問や明確化が必要な点があれば、ICS-CERT まで。

3. ICS-CERT によるセキュリティ評価

2016 年 5 月･6 月は、5 業界で 21 件のセキュリティ評価を実施した。

業界別では、水道業界が 11 件、運輸業界が 5 件、食品･農業が 3 件、政府施設が 1 件、IT 業界が 1 件であった。

評価の種別では、CSET による評価が 8 件、DAR による評価が 6 件、NAVV による評価が 7 件であった。

- CSET
  政府基準や業界標準等に照らして、組織のセキュリティ対策状況を確認するツール「CSET」を使用した汎用的な評価サービス
- DAR
  設計や構成、相互依存性や利用しているアプリケーションなど、組織の制御システム／ネットワークに合わせた、より詳細な評価サービス
- NAVV
  ネットワークを流れるパケットの解析による、機器間の通信の洗い出しと確認を行うサービス

最近の評価結果の傾向としては、以下の 3 つの問題点が多く見られた。

1. セグメント分割／ゾーニングの欠如
   ネットワークの殆どが、セグメント分割／ゾーニングがされておらず、フラットなネットワーク構成であった。レイヤー2／レイヤー3 ネットワーク機器を使ってセグメントを分割し、ネットワークを監視するポイントを作ることが望ましい。また、情報系ネットワーク（社内 LAN）と制御ネットワークは分割するべきである。

---

[2] ICS-CERT モニター（2016 年 3･4 月号） https://www.ipa.go.jp/files/000052706.pdf

[3] 「Protected Critical Infrastructure Information Procedures Manual」に、Express Statement や必要な関連ドキュメントの見本あり。
https://www.dhs.gov/publication/pcii-program-procedures-manual

2. 設定上の問題

設定ミスや矛盾した設定がある。また、不必要なサービスやポートが無効化されていない。

3. ID 管理／認証の問題

多くの制御システムでは、共通アカウントやグループアカウントが使われており、誰が何をしたのかの特定を困難にしている。操作者はそれぞれ個別のアカウントを使用することが望ましい。それが難しいのであれば、各操作者の操作責任を明確にする仕組みを別途導入するべきである。

もう 1 つの問題は、リモートアクセス時の多要素認証の欠如である。リモートアクセスは最大のリスクの 1 つであり、リモートアクセスユーザの認証には一層の警戒が必要となる。多要素認証の実現には、時刻同期型の RSA トークンや、コールバックによる確認といった、簡単な方法を採用することも考えられる。

4. ICS-CERT ニュース ～ ICSJWG Spring 2016 Meeting の振り返り ～

Industrial Control Systems Joint Working Group（ICSJWG）Spring 2016 Meeting は、2016 年 5 月 3～5 日にかけて、アリゾナ州スコッツデールで開催された。これ迄で最大規模となり、世界中から 300 人以上の ICS 関係者が参加した。

会合には ICS-CERT の Advanced Analytical Laboratory（AAL）も参加し、進化を続けるマルウェアの動向や、攻撃者の戦術について講演を行った。ランサムウェアへの感染は検知されることが前提である一方で、他のマルウェアには検知を回避することに多大な労力が注ぎ込まれている。攻撃の追跡は容易ではなく、イベントログやパケットなど、ネットワーク上の多様なリソースから得られる様々なデータが必要となる。最も迅速・簡単な解決策である「感染システムのネットワークからの切り離し」は、攻撃を遅らせるだけの結果になったり、攻撃者を警戒させてしまう可能性がある。また、下手な対応をすると、調査および対策に必須な証跡（データ）を失うことになってしまう。AAL では前述の講演のほかに、必要なデータを保全するためハードディスクおよびメモリイメージを取得するハンズオンセミナーも行った。

侵入やマルウェアへの感染に気付いた場合の対応の留意点をまとめた以下資料も参照のこと。

Fact Sheet: So You Think You've Been Compromised… (June 2016)
～ 侵入が疑われる場合に取るべき行動／取ってはいけない行動 ～
https://ics-cert.us-cert.gov/Information-Products

次回 ICSJWG Fall Meeting 2016 Meeting は、2016 年 9 月 13～15 日にフロリダ州フォートローダーデールで開催予定。

詳細は、https://ics-cert.us-cert.gov/Industrial-Control-Systems-Joint-Working-Group-ICSJWG を参照。

5. 最近公開された脆弱性やレポート等

※原文の Recent Product Releases を参照ください。

6. 協調的な脆弱性の公開に協力頂いたセキュリティ研究者の方々

ICS-CERT では、発見した脆弱性を一般への公開前にベンダに通知し、パッチや対策版の提供を可能にする「協調的な脆弱性の公開（coordinated vulnerability disclosure）」を奨励しており、そのための仕組みを提供している。様々な事情により困難な場合もあるかもしれないが、是非活用頂き、協調的な公開への協力をお願いしたい。

※2016 年 5 月、6 月に協調的な公開に協力頂いた研究者の方々については、原文の Coordinated Vulnerability Disclosure を参照ください。

7. 今後のイベント

※原文の Upcoming Events を参照ください。

以上