2012 年 8 月 9 日

独立行政法人情報処理推進機構(IPA)

2009-2011 ICS-CERT インシデントレスポンス・サマリーレポート概要

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)の 2009 年～2011 年の活動報告である“ICS-CERT Incident Summary Report”(2012/6/28 公開)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_Incident_Response_Summary_Report_09_11.pdf

1. 2009～2011 年に報告されたインシデント件数および ICS-CERT による現地対応件数

重要インフラを狙ったサイバーインシデントの報告は、ICS-CERT が設立された 2009 年は 9 件、2010 は年 41 件、2012 年は 198 件が寄せられており、急増の一途にある。セクタとしては、電力と水道における件数が突出しており、全体の半数以上を占めている(表 1)。

また、上記のうち、原因調査・対策支援のため ICS-CERT がインシデントレスポンスチームを派遣して現地対応を行ったのは、2009 年は 2 件、2010 年は 8 件、2011 年は 7 件となっている(表 2)。

【表 1】インシデント報告件数(()内その年の合計件数に占める割合)

セクタ	インシデント件数(%)			計
	2009 年	2010 年	2011 年	
電力	**3(33%)**	**18(44%)**	**31(16%)**	**52(21%)**
水道	**3(34%)**	**2(5%)**	**81(41%)**	**86(35%)**
その他(化学、核、政府、運輸、ダム他)	3(33%)	21(51%)	86(43%)	110(44%)
計	9(100%)	41(100%)	198(100%)	248(100%)

【表 2】ICS-CERT による現地対応件数

	セクタと現地対応件数						計
	水道	電力	核	製造	政府	化学	
2009 年	1	1					2
2010 年		5	1	2			8
2011 年	2	2			2	1	7
計	3	8	1	2	2	1	17

2. 現地対応において確認された主な事項及び傾向

ICS-CERT による現地対応の中で観察された主な事項・傾向は以下:

- ✓ 制御システムネットワークに直接侵入したと見られるケースはなかった。
- ✓ 判明した侵入経路では、スピアフィッシングが目立つ(7 件)。業界向けニュースレターを装うなど、巧妙な文面による高度な手口も見られた。また、USB メモリを介した侵入もあった(1 件)。
- ✓ ログ管理が十分でなかったり、マルウェアの侵入発見時にウィルス対策ソフトを走らせた為、証跡とな

るログが上書きされてしまい、侵入の有無の特定や、詳細な分析ができないケースが多い。（インシデント対応時の考慮事項について、ICS-CERT は Incident Handling Brochure を提供している）

- ✓ 侵入の検知については、事業者自身でなく、外部組織や、ベンダやコンサルタント等の第三者によって検知・告知されているケースも多い（5 件）。
- ✓ 侵入の痕跡が認められたケースの半数以上は、マルウェア配布サイトとされる既知の IP アドレスやドメインのブロック、ログイン制御やネットワークのセグメント化など、一般的に推奨されているセキュリティ対策を実践していれば、検知または防止可能であった。

3. 制御システム環境におけるセキュリティ対策と運用のギャップ

ICS-CERT による現地対応や、CSET（Cyber Security Evaluation Tool）を使った、事業者による自己診断結果から、制御システムにおけるセキュリティ対策と現実の運用状況の間には、以下のセキュリティギャップが存在する傾向があり、制御システムの脆弱性となっている。

（1）人的要因

- ✓ セキュリティ意識の低さによる、脅威とリスクに対する理解の欠如
- ✓ 不適切なセキュリティポリシーや対策が制御システムにもたらす影響の大きさに対する理解の欠如
- ✓ セキュリティ対策の必要性に対する理解とリソースの欠如

（2）プロセス的要因

- ✓ セキュリティ対策を業務を支えるビジネス基盤の一つとして落とし込むためのポリシーまたはプロセスの欠如
- ✓ 組織内にセキュリティを浸透させるのに必要な戦略やポリシーの欠如
- ✓ 制御システムなど環境にあった、必要な機能基準、運用基準、セキュリティ基準、教育基準等の策定
- ✓ 適切なインシデント予防策、インシデントレスポンス計画、検知施策、証跡保全手順、復旧手順の欠如

（3）技術的要因

- ✓ 不十分なリスクアセスメントによる、守るべき資産の特定漏れや不適切な優先順位付け
- ✓ セキュリティフレームワークの欠如（不整合・不統一なセキュリティ対策）
- ✓ パッチマネジメントの欠如
- ✓ ユーザアクセス制御の欠如
- ✓ 不適切なネットワーク構成、通信の適切なフィルタリングの欠如
- ✓ 不適切なファームウェア、OS の利用・運用

4. 今後の取組

より多くの情報が ICS-CERT に集まり、調査・分析を行えることが、重要インフラを取り巻く攻撃の全体像の把握に必要。重要インフラ事業者には、インシデントを報告し、調査・支援を ICS-CERT に依頼するよう奨励する。ICS-CERT では、基本的対策を纏めた ICS-TIP-12-146-01-Targeted Cyber Intrusion Detection and Mitigation Strategies 等のガイダンスも提供しており、今後も資料の提供や支援に努めていく予定。

以上