2014 年 5 月 23 日
独立行政法人情報処理推進機構（IPA）

ICS-CERT 2013 年度活動総括　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）が発行する、“ICS-CERT Year in Review 2013”の抄訳となります。内容の詳細につきましては、原文をご参照ください。

URL：http://ics-cert.us-cert.gov/ICS-CERT-Year-Review-2013

国家としての備え：国土安全保障省の取組み

米国民の安全および豊かな生活は、重要インフラの信頼性とレジリエンスに掛かっている。国土安全保障省（DHS）は、大統領政策指令第 8 号（PPD-8）に基づき、Industrial Control Systems Cyber Emergency Response Team（ICS-CERT）等を通じて重要インフラのセキュリティ確保に取り組んでいる。

Ⅰ．予防（Prevention）

ICS-CERT では、重要インフラ事業者（所有者・運用者）およびベンダから成る ICS コミュニティとのパートナーシップを通じて関係者への啓発活動を行い、サイバー脅威の予防に取り組んでいる。

1 つには、連邦捜査局（FBI）など他の連邦機関と連携し、機密情報を含め、事業者に脅威や対策について説明する Action Campaign Briefing を行っている。2013 年度は全米各地で 14 回実施し、述べ 750 人以上が参加した。また、事業者やベンダに加え、地方政府やセキュリティ研究者なども加わった Industrial Control Systems Joint Working Group（ICSJWG）の会合も開催しており、メリーランド州ロックヴィルで行われた 2013 年秋の会合では、最新の話題や課題、技術などについて議論がなされた。

Ⅱ．防止（Protection）

ICS-CERT では、無料の訓練プログラムやツールの提供を通じて、重要インフラシステムをサイバー攻撃から守るために必要なスキルの習得や対策を支援している。

1 つには、初級・中級・上級の 3 段階の ICS 向けサイバーセキュリティ訓練プログラムの提供しており、特に上級コースは 1 週間のプログラムで、レッドチーム／ブルーチームに分かれての実際的な演習も含まれている。2013 年度は上級コースだけで 11 回開催し、442 人が受講した。なお、初めての試みとして、ICS-CERT（アイダホ州アイダホフォールズ）だけでなく、他都市においても開催した。また、各事業者における対策状況を、既存の標準やガイドラインに基づき確認できる評価ツール「Cyber Security Evaluation Tool（CSET）」を提供している。最新の CSET6.0 では、新たな標準等が追加されたほか、過去の評価と比較し改善成果が確認できるようになるなど、機能と利便性が向上している。

Ⅲ．緩和（Mitigation）

ICS-CERT は、サイバー攻撃への対策について、順応性があり、繰り返し適用可能なアプローチを確立しており、重要インフラ事業者やベンダに中核的なインシデントレスポンス力を提供することを可能にしている。重要インフラ事業者と協力し、それぞれの事業者に特有の脅威やニーズに対応することがで

きる。2013 年度は、報告を受けた 257 件のインシデントに対応しており、56%以上がエネルギー業界であった。インターネットに接続された SCADA 機器への不正アクセスや、独立している制御システムネットワークにおけるウィルス感染など、様々な攻撃が見られた。

Ⅳ. 対応(Response)

DHS の National Cybersecurity and Communications Integration Center(NCCIC)は、重要インフラのサイバーセキュリティに関わる活動の中心となるハブ的存在であり、4 つの部門からなる。

United States Computer Emergency Readiness Team(US-CERT)は、米国のネットワークを標的とする悪意ある活動に対処すべく、連邦・州・地方行政機関や民間企業などに脅威情報や対策情報を提供している。ICS-CERT は、官民パートナーシップを通じて、ICS のセキュリティ強化に取り組んでいる。National Coordination Center(NCC) for Telecommunication は、通信サービス・設備の維持を担っている。NCCIC Operation and Integration は、全体の取組みの企画・調整・統制を行い、年中無休でサイバーセキュリティに関する重要情報に対応している。

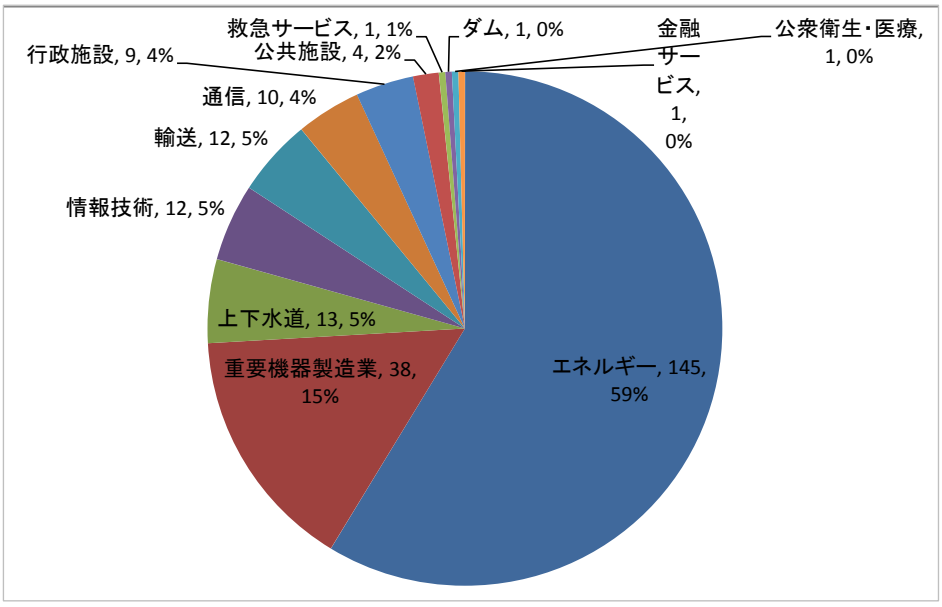
こうした“連携”には、重要インフラのモデリングやシミュレーションも可能な Industrial Control Systems Consequence Effects and Analysis(ICS-CEA)といったコラボレーションツールも活用し、分野横断的な影響等についても検討を行っている。

Ⅴ. 復旧(Recovery)

ICS-CERT では、サイバー攻撃の影響を受けた重要インフラ事業者に対し、復旧および中長期的な対策の改善を支援している。2013 年度は、72 件のオンサイト(現地)対応を行った。事業者は ICS-CERT に CSET による評価や Architecture Review を依頼することができ、後者は、特定の制御システムやネットワークについて、詳細かつ包括的な評価を提供する。各事業者によって攻撃の影響は異なるが、攻撃を受けた事業者のシステムやネットワークの脆弱性や弱い箇所には、類似点も多く見られた。

統計

2013 年度のインシデント対応件数と分野



オンサイト対応件数（財政年度[1]）

セクタ	2011	2012	2013	累計
化学	0	4	0	4
公共施設	10	2	0	12
通信	1	0	2	3
重要製造業	2	1	0	3
ダム	0	0	0	0
防衛産業（DIB）	0	12	1	13
救急サービス	2	3	0	5
エネルギー	11	7	18	27
金融サービス	1	6	0	7
農業＆食糧	5	0	0	5
行政施設	5	3	2	10
公衆衛生・医療	6	1	5	12
情報技術	3	5	2	10
原子炉、核資源、核廃棄物	2	8	8	18
輸送	7	10	10	27
上下水道	21	25	24	70
計 （対応セクタ数/全セクタ数）	**76** （13/16）	**87** （13/16）	**72** （9/16）	**235** （15/16）

主な対応項目（財政年度）

NCCIC/ICS-CERT　主要対応項目	2011 計	2012 計	2013 計
報告された制御システムのインシデント（対応数）	140	197	257
オンサイト対応	7	6	7
報告された制御システム関連の脆弱性（対応数）	139	137	187
情報公開	243	347	295
CSETの配布／ダウンロード	5,100	6,631	5,085
オンサイト評価	81	89	72
ICS-CERTでトレーニングを受けた専門家	1,686	2,327	693
開催したトレーニング	47	56	17
ICSJWGメンバー	1,012	1,371	1,476
講演	137	205	162
展示会等	20	22	2

以上

[1] 10 月 1 日～9 月 30 日（例：FY2013 は、2012 年 10 月 1 日～2013 年 9 月 30 日）