制御システムセキュリティセンター活動紹介

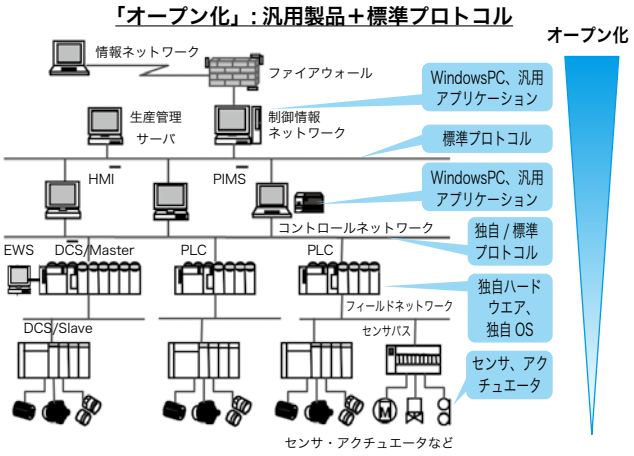
～セキュアな制御システムを世界へ未来へ～

技術研究組合制御システムセキュリティセンター（CSSC）
専務理事 研究開発部長 CSSC認証ラボラトリー長
小林　偉昭

1 はじめに

制御システムは、最近では Windows や UNIX などの汎用 OS の採用、さらに Ethernet や TCP/IP の標準プロトコルが採用されている。このため情報システムで起きているセキュリティの脅威（サイバー攻撃）が増大してきている。図 1 に示すような汎用製品と標準プロトコル採用によるオープン化が進展しているという認識を持つことが大切である。プラント設備（生産ライン制御等）におけるオープン化の割合は、外部ネットワークとの接続が 36.8%、設備内の OS の利用状況として Windows が 88.9%、UNIX 系が 13.7% と報告されている。

制御システムへのサイバー攻撃の衝撃的な事例が、2010 年イラン核施設への Stuxnet である。制御システムのセキュリティの安全神話は崩壊してしまった。米国の国土安全保障省（DHS）の ICS-CERT※1 からのレポートによると、米国における重要インフラ事業者に対する攻撃のインシデント報告件数は、図 2 に示すように 2010 年が 34 件であったのが、2013 年には 257 件と約 8 倍となっている。



■ 例：プラント設備（生産ライン制御等）におけるオープン化の割合

- 外部ネットワークとの接続　36.8%
- 設備内の OS の利用状況　Windows：88.9% UNIX 系：13.7%

経済産業省サイバーセキュリティと経済 研究会中間とりまとめ（案）：
http://www.meti.go.jp/committee/kenkyukai/shoujo/cyber_security/report01.html

図 1　制御システムの状況

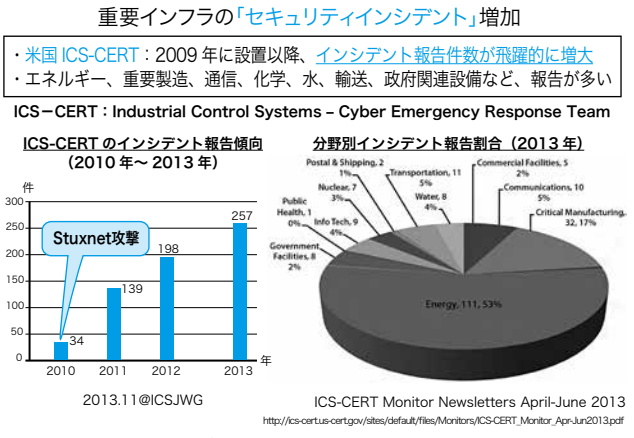


図 2　重要インフラのセキュリティインシデント発生傾向（米国 ICS-CERT）

2 CSSC の設立経緯と概要

2.1　CSSC の設立経緯

2010 年の Stuxnet によるイラン核施設へのサイバー攻撃を受けて、経済産業省は 2010 年 12 月に「サイバーセキュリティと経済研究会」を立ち上げた。研究会は、サイバー攻撃に対する情報共有、制御システムのセキュリティ確保及び人材育成が、これからのセキュアな社会インフラを守るためには必要だと提言した。これを受けて、2011 年 10 月に「制御システムセキュリティ検討タスクフォース」を立ち上げた。ここでの目標の一つが、日本の社会インフラのセキュリティ確保である。もう一つは、ベンダが製品を輸出するときに、国際標準に対応したセキュリティを実装し、競合力を高めることである。

【脚注】

※1　ICS-CERT：米国国土安全保障省（DHS）が運営する制御システムに特化したインシデント対応機関。制御システムに関する国内のインシデント報告を受け、専門家による分析・対応サービスを提供する。
http://www.us-cert.gov/control_systems/ics-cert/

このタスクフォースの検討を受け、2012 年 3 月に民間企業の技術研究組合として「制御システムセキュリティセンター」が発足した。2012 年 7 月にお台場に東京研究センターを、2013 年 5 月に宮城県多賀城市に東北多賀城本部を設置し、「セキュアな制御システムを世界へ未来へ」という目標を掲げて活動を開始した。

東北多賀城本部にはファクトリーオートメーション FA、プロセスオートメーション PA、ビルオートメーション BA などの 7 つの制御システムの模擬プラントを設置し、これらのテストベッドを中心に、制御システム向けの高セキュリティ機能や評価認証技術を研究・開発し、普及啓発コンテンツを整備している。この経緯を図 3 に示す。

2.2　CSSC の概要

CSSC の組織と概要を図 4、図 5 に示す。運営委員会のもとに 4 つの委員会を設置し、下記の活動を進めている。

- 制御システムにおける可用性を高める高セキュア化技術の研究開発
- 広域連携システム（スマートコミュニティ等）における高セキュアシステム技術の研究開発
- システムセキュリティ検証・認証技術の研究開発と認証実証事業への展開
- 国際標準化と国際連携
- 制御セキュリティテストベッドの研究開発と人材育成や普及啓発への展開
- サイバーセキュリティ事業を震災復興、減災に展開

さらに、2013 年 8 月には CSSC 内に CSSC 認証ラボラトリーを新設し、2013 年 9 月に日本適合性認定協会 JAB に認証機関として認定申請し、2013 年 11 月には ISCI（ISA Security Compliance Institute）へ加入し、制御機器の認証実証事業を推進している。

グローバルな社会インフラの制御システムセキュリティ向上に貢献していくために、米国の国土安全保障省 DHS や欧州の ENCS（European Network for Cyber Security）などと国際連携を進めている。

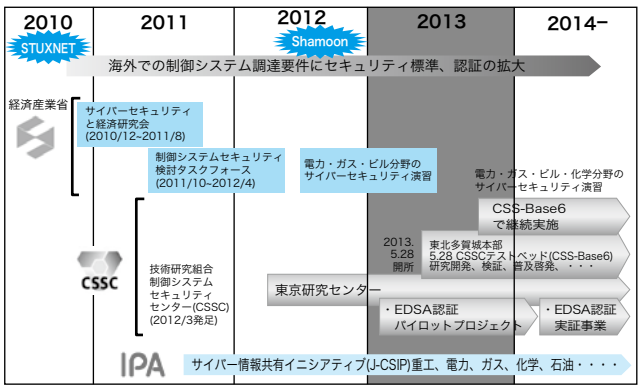


図 3　制御システムセキュリティへの日本の取り組み状況

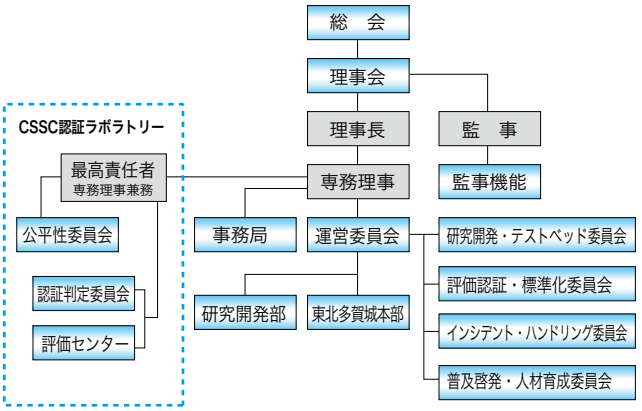


図 4　CSSC の組織体制

CSSC の概要			
名称	技術研究組合 制御システムセキュリティセンター （英文名）Control System Security Center （略称）CSSC	組合員 （50 音順）	全 23 社（2013 年 12 月現在）　　*：創設時メンバー 8 社 アズビル株式会社 *、エヌ・アール・アイ・セキュアテクノロジーズ株式会社、エヌ・ティ・ティ・コミュニケーションズ株式会社、オムロン株式会社、独立行政法人産業技術総合研究所 *、独立行政法人情報処理推進機構、国立大学法人電気通信大学、株式会社東芝 *、東北インフォメーション・システムズ株式会社、株式会社トヨタ IT 開発センター、トレンドマイクロ株式会社、日本電気株式会社、一般財団法人 日本品質保証機構、株式会社日立製作所 *、富士通株式会社、富士電機株式会社、マカフィー株式会社、三菱重工業株式会社 *、株式会社三菱総合研究所 *、三菱電機株式会社、森ビル株式会社 *、横河電機株式会社 *、株式会社ラック
	※経済産業大臣認可法人		
設立日	2012 年 3 月 6 日（登録完了日）		
所在地	【東北多賀城本部 (TTHQ)】 宮城県多賀城市桜木 3-4-1 （みやぎ復興パーク F-21 棟 6 階）		
	【東京研究センター（TRC）】 東京都江東区青海 2-4-7 （独立行政法人産業技術総合研究所 臨海副都心センター別館 8 階）	連携団体 （予定含む）	一般社団法人 JPCERT コーディネーションセンター、一般社団法人日本電機工業会、公益社団法人計測自動制御学会、一般社団法人電子技術情報産業協会、一般社団法人日本電気計測器工業会、一般財団法人製造科学技術センター、電気事業連合会、一般社団法人日本ガス協会、一般社団法人日本化学工業協会

図 5　CSSC の概要

3 CSSC の活動

研究開発と評価認証・検証技術について紹介する。

3.1 研究開発

2012 年度には、CSS-Base6 にセキュリティでの攻撃（サイバー攻撃）が発生した時、臨場感を持った疑似体験ができるよう研究・開発し、PA、FA、BA や広域連携システム及び電力事業者やガス事業者向けの７つの模擬プラントを構築した。2013 年度は、この７つの模擬プラントを活用して経営者向けの啓蒙活動を実施している。

①排水・下水用 PA 用模擬プラント（写真 1）

圧力、流量、温度などのプロセス量をバルブや電磁流量計等で管理するもので、このプラントでは沈殿槽を模擬した汚水排水設備でのサイバー攻撃が体験できる。

②化学用 PA 用模擬プラント

流量調節弁などを制御する水槽の水位レベル制御設備でサイバー攻撃が体験できる。

③ BA 用模擬プラント

ビル全体の温度管理、エレベータ管理、空調管理、照明管理など多くの管理システムが防災センターで監視されている。この模擬プラントでは照明管理の制御のサイバー攻撃が体験できる。

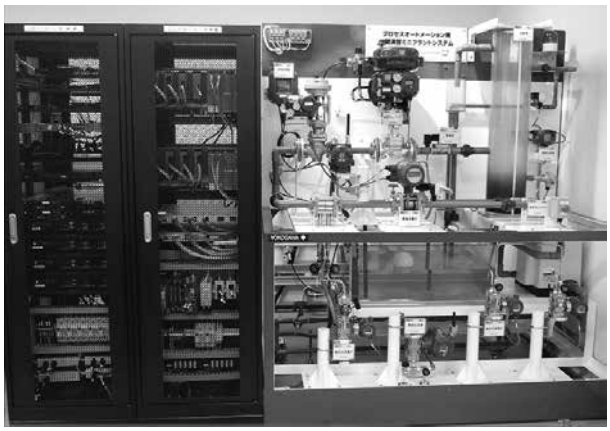


写真１　排水・下水用 PA 用模擬プラント

写真２　FA 用模擬プラント

④ FA 用模擬プラント（写真 2）

自動車工場の生産現場を模擬し、部品供給ロボット制御を使用したサイバー攻撃が体験できる。

⑤火力発電所用模擬プラント

火力発電所の管理用シミュレータを利用してサイバー攻撃発生時の体験ができる。

⑥ガス事業者用模擬プラント

エアタンク圧力一定装置を利用して、ガス事業者向けの各種サイバー攻撃が体験できる。

⑦広域連携用模擬プラント

スマートグリッドやスマートコミュニティを構成する配電設備へのサイバー攻撃が体験できる。

2014 年度には、2013 年度の研究開発の成果を反映することにより、これらの模擬プラントを利用してサイバー攻撃への対策を検討することも可能にする予定である。

テストベッドの設計・研究・開発に加え、システムを止めない、暴走させないための可用性を高める研究や万が一の場合にも最悪の事態を避けるなどの制御システムのセキュリティを高める研究を推進している。

3.2 評価認証・検証技術

製品を海外に輸出するときに、セキュリティ標準に準拠していることが国際石油メジャーからの要件となってきている。また、国内の社会インフラを構築する制御システムに対しても一定のセキュリティ標準に準拠していることが製品選択する時の基準になることが期待されている。

上記を目標に、制御システムセキュリティ標準の要件検討から図 6 に示すように当初の評価認証の対象を次のように決定し、推進している。

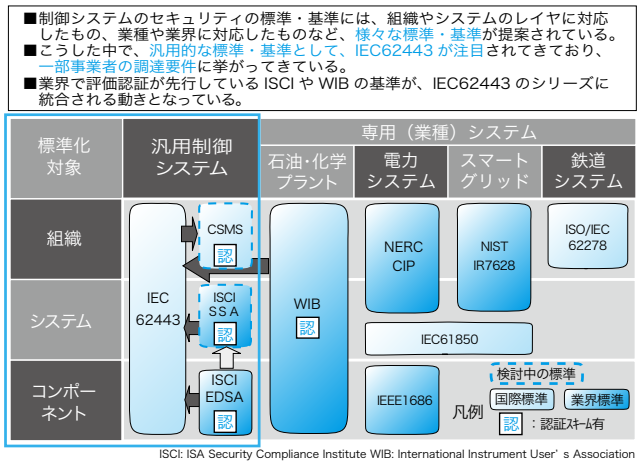


図６　制御システム分野での標準化に関する技術動向

・IEC62443（Industrial Network and System Security）を汎用的国際標準として選択
・標準確立、評価認証を一体で推進する
・IEC62443 対応の認証標準として ISCI で先行している標準に対応する

なお、業界対応に様々な標準があり、北米の電力システム用や欧米のスマートグリッド関係の標準化も進んでいることから、この分野の調査も進めている。

（1）国際標準 IEC62443 の概要

IEC62443 は、四つのレイヤからできている。

・1 番目が総論である。
・2 番目が管理・運用・プロセスの標準である。JIS Q 27001（ISO/IEC 27001）ISMS（Information Security Management System）は、情報システム向けのセキュリティマネジメントであるが、制御システム向けのセキュリティマネジメントが IEC62443-2-1 の CSMS（Cyber Security Management System）である。
・3 番目は、制御システムについてのセキュリティ標準である。
・4 番目はコンポーネントで､製品対応のセキュリティ標準である。

IEC62443 には 13 の標準がある。独立行政法人情報処理推進機構（IPA）は、既に国際標準になっている 3 つの標準を翻訳し、2012 年 10 月に日本規格協会から出版している。

（2）評価認証の推進状況

次に 3 つの評価認証への取り組みとその現状・方向性を紹介する。EDSA（Embedded Device Security Assurance）と SSA（System Security Assurance）については、ISCI が先行して認証標準を決めているが、IEC62443 に取り込まれていく予定である。図 6 参照。

＜ EDSA 認証＞

ISCI が、スキームオーナとしてグローバルな EDSA 認証を推進している。EDSA は次の 3 種類の標準で構成されている。

・CRT（Communication Robustness Testing）は、通信レベルでの評価の標準である。ファジングという手法によりランダムなデータをぶつけて、矛盾が起きないかを主に検証する。
・FSA（Functional Security Assessment）は、セキュリティの機能についての評価の標準である。
・SDSA（Software Development Security Assessment）はソフト開発プロセスの評価の標準である。

現在、米国の 2 社の四つの製品がこの認証を取っている。日本の製品ベンダが海外に行って認証を取るのではなく、日本で、日本語で認証を取りたいという要求がある。このため CSSC では、2013 年度から EDSA 認証パイロットプロジェクトを開始し、2014 年度から認証実証事業を開始し、普及を目指している。CSSC で認証を取得すると国際相互承認され、グローバルに認証された製品として認められる。

＜ SSA 認証＞

制御システムの認証を実現する SSA が現在検討されている。ISCI では 2014 年初めまでに実現しようとしている。

＜ CSMS 認証＞

日本情報経済社会推進協会（JIPDEC）が認定機関になって、情報システム向けの ISMS の活動を推進している。JIPDEC は、制御システムへ CSMS を展開するため、2013 年度に CSMS 認証パイロットプロジェクトを開始している。

（3）検証技術

制御機器に対する評価検証の技術及び評価体制を整備するため、ワーキンググループを設置し、ISCI　EDSA の 3 つの標準に対するテスト仕様書を整備した。2013 年度の EDSA 認証パイロットプロジェクトにより、更に実態に合った仕様書にしていく。

現在 CSSC は、複数の PLC や DCS などの制御システムを整備し、さらにファジングテストツール等も複数製品活用している。これらのツールは、CSS-Base6 で組合員による利用も可能にしている。

4 おわりに

発足時の組合員は 8 組織だったが、2013 年 12 月末現在 23 組織に拡大している。さらに賛助会員制も立ち上げて、研究開発成果の普及に努めている。重要インフラ事業者を始めとする制御システム関係者の CSSC への参画を期待している。また、CSSC の認証実証事業などを多賀城市をはじめとして連携を進め、復興支援にも貢献していく所存である。

今後とも CSSC は、「セキュアな制御システムを世界へ未来へ」という目標を掲げてグローバルに活動を進めていきます。