制御システムのセキュリティに関する業界動向と標準化

KPMG コンサルティング株式会社
武部　達明

2014 年のソチオリンピックでは、空調設備の制御システムがインターネットからアクセス可能となっていることがセキュリティ研究者によって発見され、すぐに担当者に通知されて事なきを得た。制御機器本体あるいは制御システム自体に十分なセキュリティが備わっていることはまれであり、オープン化の波に乗り、高機能、低価格、利便性の追求から、商用の汎用 IT 技術を製品・システム内に取り込んだ制御機器・制御システムには、外部からの侵入を許容しかねないリスクが潜んでいる。安全性を確保しながら制御システムの利便性を高めるには配慮と工夫が必要である。これを機に今一度、重要インフラを支える制御システムのセキュリティが点検され、2020 年の東京オリンピックが無事に開催されるよう祈念する次第である。

1. はじめに

黎明期には、独自 OS、独自プロトコル、閉じたネットワークで構成された制御システムは、オープン化の波に乗り、高機能、高付加価値、高生産性を目指して Linux OS、IP ネットワーク、Windows OS などの汎用 IT 技術、民生品（COTS: Commercial Off The Shelf）を取り込んで進化してきた。しかし、セキュリティ上の問題があることが判明し、情報機器・情報システムへの対策は進められたが、制御システムへの対策は出遅れた。

図 1 に示すように、セキュリティ攻撃ツール・手法は年々高度化し、操作も簡単になったため、攻撃に要するスキルの閾（しきい）値が下がり、その結果、誰もが攻撃者になれる危険性をはらむこととなった。これらのツールは民生品を対象として発展してきており、民生品を多用している制御システムにも適用可能であることを示唆している。

図 2 は、ICS-CERT に報告された制御システムのインシデントの原因を分類している。このうち Spear Phishing には、Adobe Reader の脆弱性を利用する Exploit コードを高度なセキュリティツールで PDF ファイルに組み込み、E-mail でオペレータに送付するなどの攻撃も含まれると推測される。

制御システムが担う役割の重要性と、事故が発生したときのインパクトの大きさから、制御システムのセキュリティについての議論が始まり、近年耳目を集めるようになった。各業界では、セキュリティに関する取組みが始まり、セキュリティの課題、統制、ベストプラクティスなどの成果が、業界の標準、さらには国際標準へ影響を与えることになる。

このような背景を踏まえ、本稿では、米国、ヨーロッパ、日本におけるセキュリティの標準化活動について述べ、また国際標準の動向についても説明する。

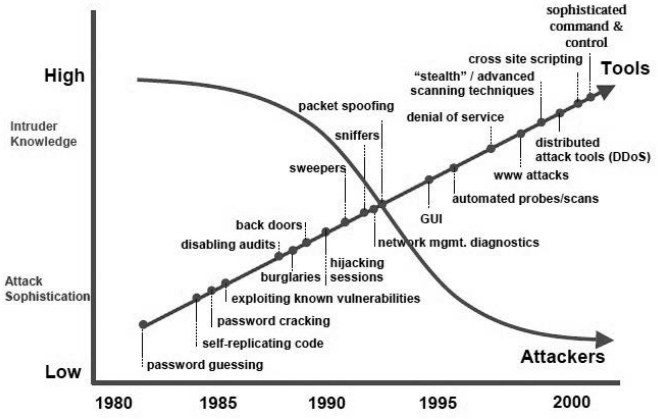


図 1 攻撃ツールの高度化 vs 攻撃者技術力

出典：CMU/SEI-2002-SR-009、Page10

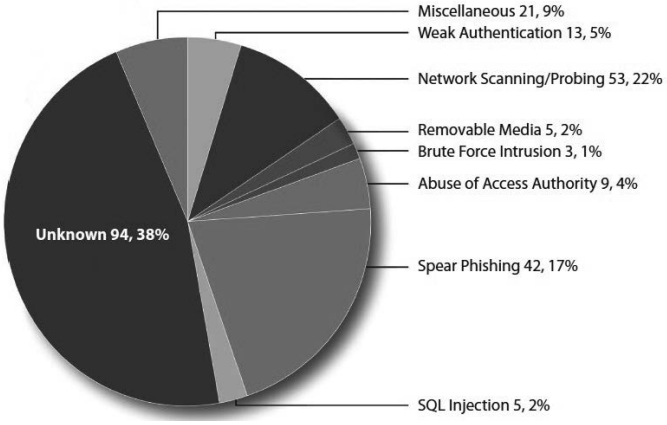


図 2 インシデントの分類

出典：ICS-CERT Monitor September 2014 – February 2015 より

2. 米国の動向

図3に、米国を中心として展開された各セキュリティプロジェクトのスコープを、分野ごとに制御システムのライフサイクル上に記したものを示す。
業界分野として、電力、石油・ガス、化学薬品、上下水道、運輸・鉄道、通信が挙げられている。

ライフサイクルでは、要件、研究、開発、テスト、評価、デモ、導入、運用のフェーズが定義されている。

図を見ると、全分野にまたがっての要件定義を考慮した活動がPCSRF、研究フェーズのセキュリティを検討したのがAGA、電力分野で研究から開発初期までをカバーしたのがTCIP、電力と石油・ガスの一部の分野で開発・テスト・評価フェーズに渡って検討したのがNSTB、電力分野で導入フェーズを考慮したのがFERC、NERC、石油・ガス分野で研究から導入まで考慮したのがI3P SCADA、ガス・石油分野でテストから導入まで考慮したのがLOGIIC、電力、石油・ガス、化学薬品分野で研究、開発、運用フェーズで考慮したのがISA99ということがわかる。

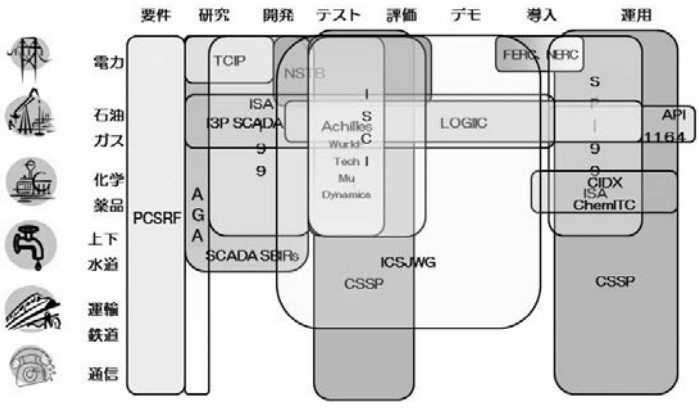


図3 米国制御システムセキュリティ・カバレッジ

2.1 全体像

DHS[1] はPCSF（Process Control Systems Forum）を立ち上げ、政府、大学、産業などから330を超す組織を集め、活動を展開した。PCSFは、制御システムのセキュリティ標準、ツール、教育・トレーニング、セキュリティ要件、セキュリティテストなど、多くのテーマで成果物を出した。この活動は、ICSJWG（Industrial Control Systems Joint Working Group）に引き継がれ、年2回のミーティングとして開催されている。ミーティングでは、制御システムセキュリティに関する課題、成果、対抗策、業界の動向などにおける研究から実運用までのテーマが発表されており、政府、大学、事業者、ベンダ、システムインテグレータ、セキュリティコンサルタントなど幅広い層の参加者を集めている。

DHS はCSSP（Control Systems Security Program）で制御システムのセキュリティ評価を行い、結果を「Common Cyber Security Vulnerabilities Observed in DHS Industrial Control Systems」という報告書としてまとめ、脆弱性の原因が、プログラムソースコード品質、Webサービス、ネットワークプロトコル、パッチ不適用、不十分な識別・認証、暗号不使用、セグメント化しないネットワーク設計などに起因するとしている。

DHS はINL[2] で、上級セキュリティトレーニングを開催し、4日間のトレーニング後、丸1日かけて、攻撃チーム（Red Team）、守備チーム（Blue Team）に分かれ、用意されたミニプラント設備を使った演習を行う。この演習の参加者は、セキュリティ守備の難しさ、攻撃によるダメージの深刻さを理解し、制御システムのセキュリティを推進する立場となる。これにより、制御システムユーザ、ベンダ、システムインテグレータの意識改革がなされる仕組みとなっている。

[1] Department of Homeland Security、http://www.dhs.gov
[2] Idaho National Laboratory、http://www.inl.gov

2.2 業界動向

石油・ガス業界では大学の研究機関主導のプロジェクトであるI3P[3]で、制御システムセキュリティのリスク分析など、6つの分野で成果をあげた。

LOGIIC[4]は、石油・天然ガス会社とDHS S&T（Science and Technology）とで行っているプロジェクトであり、争点となっているセキュリティのテーマについて、研究・対策を発表している。

API[5]は、パイプラインシステムのセキュリティに関するガイダンスドキュメントをAPI 1164として出版した。

AGA[6]は、SCADAの通信を暗号メカニズムによって保護するため、AGA 12を企画した。Part 2はRetrofit Link Encryption for Asynchronous Serial Communicationである。

CIDX（Chemical Industry Data eXchange）では、Cybersecurity Vulnerability Assessment Methodologiesでサイバーセキュリティ上の脆弱性を評価する手法をまとめ、IEC 62443-2-1の制御システム特有のマネジメントとして結実し、活動はChemITC[7]に引き継がれている。

電力業界では、多数存在する規模の異なる電力供給業者のセキュリティに対する信頼性を確保するため、NERC CIP 002-5、CIP 003-5、CIP 004-5、CIP 005-5、CIP 006-5、CIP 007-5、CIP 008-5、CIP 009-5、CIP 0010-1、CIP 0011-1が制定された。現在Version 5であり、法的強制力を伴う監査に使用される。

NISTは、スマートグリッドに対して、ガイドラインNIST IR 7628を公開した。これには、電力市場7ドメインでの相互運用性、各ドメイン間サービス、ユースケースの列挙とセキュリティ要件の分析などが書かれている。

SGIP[8]のCSWG（Cyber Security Working Group）は、ユースケースを分析し、リスクチェックを行った後、上位レベルのセキュリティ要件を定義し、セキュリティアーキテクチャ、既存のスマートグリッド標準を使い適合性評価をできるようにしている。

また、CSWGは、セキュリティバグに対応するため、AMI（Advanced Metering Infrastructure）Smart Meterのファームウェアアップデートのテストフレームワークも用意している。

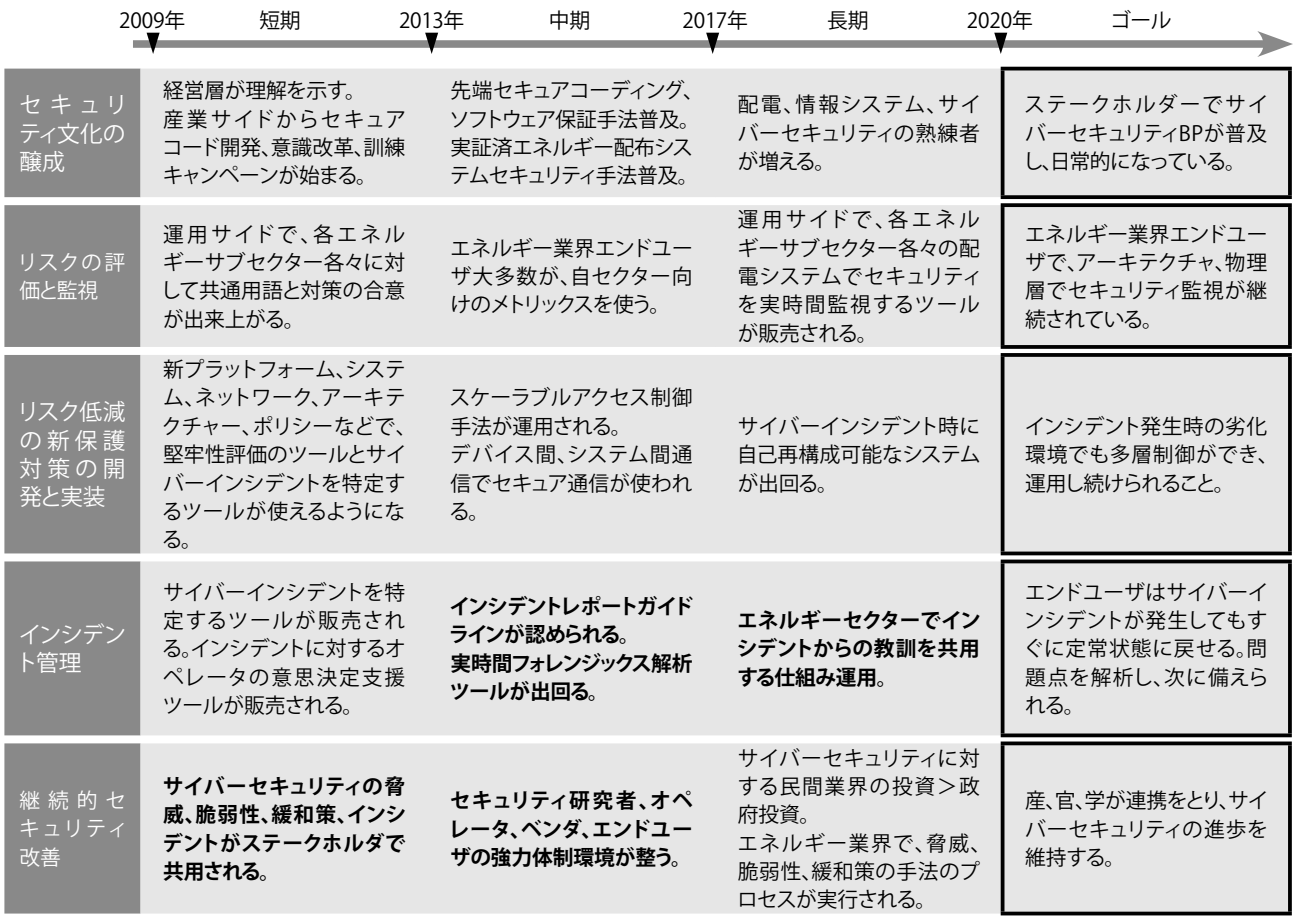
DOEは制御システムのセキュリティについてプロジェクトを通した評価を行うことで、セキュリティに関する実情と課題を明らかにし、課題を克服する目標に向かってマイルストーンを設定したロードマップを提案した（図4）。

これによると、セキュリティ文化の醸成、リスクの評価と監視、リスク低減の新保護対策の開発と実装、インシデント管理、継続的セキュリティ改善の分野で、短期、中期、長期、ゴールのフェーズ毎の目標が定められている。

最終的には、セキュリティ文化として、関係者にサイバーセキュリティのベストプラクティスが日常的に普及し、エンドユーザサイトで制御システムのセキュリティアーキテクチャおよび物理層でのセキュリティが評価・監視され、リスク低減の施策として、インシデント発生時も問題解析を即時実行し、問題点の特定後、定常状態に戻せるようになっており、継続的セキュリティ改善として、産官学が連携を取り、サイバーセキュリティの進歩を維持することができることを目指している。

---

3 Institute for Information Infrastructure Protection、http://www.thei3p.org
4 Linking to the Oil and Gas Industry to Improve Cybersecurity、http://logiic.automationfederation.org
5 American Petroleum Institute、http://www.api.org
6 American Gas Association、http://www.aga.org
7 Chemical Information Technology Center、http://chemitc.americanchemistry.com
8 Smart Grid Interoperability Panel、http://www.sgip.org



	2009年 短期	2013年 中期	2017年 長期	2020年 ゴール
セキュリティ文化の醸成	経営層が理解を示す。 産業サイドからセキュアコード開発、意識改革、訓練キャンペーンが始まる。	先端セキュアコーディング、ソフトウェア保証手法普及。 実証済エネルギー配布システムセキュリティ手法普及。	配電、情報システム、サイバーセキュリティの熟練者が増える。	ステークホルダーでサイバーセキュリティBPが普及し、日常的になっている。
リスクの評価と監視	運用サイドで、各エネルギーサブセクター各々に対して共通用語と対策の合意が出来上がる。	エネルギー業界エンドユーザ大多数が、自セクター向けのメトリックスを使う。	運用サイドで、各エネルギーサブセクター各々の配電システムでセキュリティを実時間監視するツールが販売される。	エネルギー業界エンドユーザで、アーキテクチャ、物理層でセキュリティ監視が継続されている。
リスク低減の新保護対策の開発と実装	新プラットフォーム、システム、ネットワーク、アーキテクチャー、ポリシーなどで、堅牢性評価のツールとサイバーインシデントを特定するツールが使えるようになる。	スケーラブルアクセス制御手法が運用される。 デバイス間、システム間通信でセキュア通信が使われる。	サイバーインシデント時に自己再構成可能なシステムが出回る。	インシデント発生時の劣化環境でも多層制御ができ、運用し続けられること。
インシデント管理	サイバーインシデントを特定するツールが販売される。インシデントに対するオペレータの意思決定支援ツールが販売される。	**インシデントレポートガイドラインが認められる。 実時間フォレンジックス解析ツールが出回る。**	**エネルギーセクターでインシデントからの教訓を共用する仕組み運用。**	エンドユーザはサイバーインシデントが発生してもすぐに定常状態に戻せる。問題点を解析し、次に備えられる。
継続的セキュリティ改善	**サイバーセキュリティの脅威、脆弱性、緩和策、インシデントがステークホルダで共用される。**	**セキュリティ研究者、オペレータ、ベンダ、エンドユーザの強力体制環境が整う。**	サイバーセキュリティに対する民間業界の投資＞政府投資。 エネルギー業界で、脅威、脆弱性、緩和策の手法のプロセスが実行される。	産、官、学が連携をとり、サイバーセキュリティの進歩を維持する。

図 4 DOE security roadmap Version 2

出典：Roadmap to Achieve Energy Delivery Systems Cybersecurity、Exhibit 4.1.1 Strategies for Achieving Energy Delivery Systems Cybersecurity より

3. ヨーロッパの動向

英国では NISCC[9] が SCADA の 7 つのパートからなる Good Practice Guide を作成・公開したが、後に CPNI[10] に引き継がれた。

オランダでは、TNO[11] が SCADA Security Good Practices for the Drinking Water Sector を出した。これは、水道業界に対するガイドラインではあるが、他の業界にも有用な内容となっている。

WIB[12] は、ハーグに本拠地を置く制御システムエンドユーザの集まりで IEC 62443-2-4 の原型となる WIB 2.0 を作成した。これは、供給者のセキュリティの成熟度をランク分けしたセキュリティ要件を記述する。IEC 62443-2-4 では、供給者側からの意見を取り入れ、

9 National Infrastructure Security Coordination Centre

10 Centre for the Protection of National Infrastructure、http://www.cpni.gov.uk

11 Netherlands Organization for Applied Scientific Research、http://www.tno.nl

12 Working-party on Instrument Behavior、http://www.wib.nl

他の IEC 62443 シリーズとの重複を解消し、間もなく標準として公開される。

4. 日本の動向

日本では、制御システムのセキュリティについての活動は、2007 年～ 2008 年頃から活発化した。内閣官房はサイバーセキュリティ戦略で重要インフラ防護をテーマアップし、経済産業省は制御システムセキュリティ検討タスクフォースをスタートさせ、IPA[13] は、国内外の制御システムセキュリティについてヒアリングを行い、報告書を公開している。JPCERT/CC[14] は、制御システム関連ドキュメントのいくつかを翻訳し公開している。

制御システムのセキュリティについての保証をするためには評価が有効であるが、ISCI の評価基準を用いた評価を行える CSSC[15] が国家プロジェクトとして設立された。CSSC は、ISCI の評価ドキュメントを和訳した上で参加企業などから専門家を集めレビューをした後、評価の再現性を上げるためのフィードバックを行い、ISCI に貢献している。

5. 制御システムの脆弱性

制御システムの脆弱性は、存在してはならないものであるが、残念ながら簡単にはなくならない。これは、多くの関係者が指摘している。制御システムが設計、開発、実装された時代にはセキュリティの概念がなく、またセキュリティを備えた製品・システム・アプリケーションを設計・開発・実装するプロセスのオーバーヘッドが高いため供給者内で十分理解されず優先順位を落とされ、プロセスの確立に時間がかかったためである。セキュリティの概念がなかった時代に完成された製品が、10 年～ 20 年の寿命をまだ全うしていないので、制御システムの脆弱性は容易になくならない。生産性を上げるため、古いコードをレトロフィットして使い回していることも制御システムの脆弱性の原因としてあげられる。

もともと制御機器は、リソースが潤沢でない組み込み機器として発展してきたため、アセンブラで開発され、後にポータビリティとシステム記述能力に富んだ C 言語が使われるようになり、多くのソフトウェアが開発された。

C 言語を使った初期の開発者達は、Brian W. Kernighan と Dennis M. Ritchie による「The C Programming Language」をバイブルとして、コードを書いたが、C 言語は、文字列操作、メモリ操作に関するライブラリを数多く提供しており、想定外の入力データからメモリを守れない。この弱点（脆弱性）を悪用する技術が発見され、任意のバイナリを実行する攻撃法が生み出された。脆弱性は IT 製品のいたるところで発見され、公開され続けている。また、この脆弱性に対応する攻撃方法も公開されつづけている。

脆弱性は、供給者視点ではバグであるが、攻撃者視点では攻撃コードを開発するネタとなり、マルウェアとして組み込まれて被害者のマシンで実行されるよう配備される。あるいは E-mail の添付ファイルに組み込まれ、あるいは E-mail で示される URL のリンク先からブラウザ経由でダウンロードされ実行される。関係者はこれらのリスクから制御機器・制御システムを守ることが求められている。

6. 国際標準

IEC 62443 シリーズのほとんどは、ISA 99 によって作成され、IEC TC 65/WG 10 での審議を経て国

13 Information-technology Promotion Agency、Japan（独立行政法人情報処理推進機構） http://www.ipa.go.jp
14 Japan Computer Emergency Response Team Coordination Center（JPCERT コーディネーションセンター）、http://www.jpcert.or.jp
15 Control System Security Center（技術研究組合　制御システムセキュリティセンター）、http://www.css-center.or.jp

際標準となる。

制御システムへのリスクは、日々変化していくため、リスクの捕え方、アプローチ方法によって、合意内容は変化する。IEC 62443 ではリスクに対するコントロールとして 4 レベルのグレード別にセキュリティ要件を決定した。

Part 1 は、当該標準の考え方の根底を成す概念、モデル、用語、Part 2 は、組織に対するセキュリティ要件、Part 3 は、制御システムのシステム全体としてのセキュリティについての要件、Part 4 は、制御システムを構成する制御機器、アプライアンス、アプリケーションについての要件を扱う。

IEC 62443 では、リスク評価をしながらサブシステム分割を行い、必要とするレベルを定め、必要なセキュリティ機能要件を FR1 ～ FR7 より選択し、設計、実装する。FR1 ～ FR7 の詳細は、システムセキュリティ要件として、IEC 62443-3-3 に記述される。

制御システムを構成する制御機器などに関する標準は、IEC 62443-4-1、IEC 62443-4-2 であり、それぞれ保証要件、機能要件を記述する。

ISCI は、IEC 62443 シリーズおよび ISO/IEC 15408（Common Criteria）、IEC 61508 Part 3、RTCA/DO-178B、The Security Development Lifecycle、OWASP CLASP などのセーフティおよびセキュリティのベストプラクティスを参照して評価基準を作成し、これらの成果を IEC 62443 シリーズに反映してきた。また、ISA 99 には、ISO/IEC JTC 1 SC 27 のエキスパートも参加しているため、今後ますます発展するものと思われる。

7. おわりに

IEC 62443 シリーズは、ISA 99、IEC TC 65/WG 10、WIB、ISCI、ISO/IEC JTC 1 SC 27 の活動により、制御システムのセキュリティに相応しい標準として日々発展を続けている。また、ISMS 認証、成熟度認証、制御機器評価・認証、制御システム評価・認証に使われ、得られた問題点を吸収しながら、時代の要望に即したものとして発展している。これらが活用され、制御システムのセキュリティ向上に役立つことを期待する。

【参考文献】

(1) Keith A. Stouffer、Joseph A. Falco、et al.、"The NIST Process Control Security Requirements Forum (PCSRF) and the Future of Industrial Control System Security、" TAPPI Paper Summit - Spring Technical and International Environmental Conference、2004、pp. 1337-1344
(2) IEC/TS 62443-1-1 Industrial communication networks - Network and system security - Part 1-1: Terminology、concepts and models
(3) IEC 62443-2-1 Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program
(4) IEC/TR 62443-3-1 Industrial communication networks – Network and system security - Part 3-1: Security technologies for industrial automation and control systems
(5) IEC 62443-3-3 Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels