JPCERT CC®

制御システムセキュリティガイドライン、標準及び認証への取組みに関する分析

一般社団法人 JPCERT コーディネーションセンター

要旨

制御システムの高機能化や一般の事務管理用システムとの連携の緊密化の進展とともに、事務管理用システムにおけるセキュリティ問題が、同様に制御システムにおいても発生する可能性が高まってきている。さらに、セキュリティ事故が起きた場合の影響は、制御対象によっては物理的な財産や人命にかかわる恐れもある。重要インフラ用の制御システムの場合には、これらのシステムが危険にさらされたり、利用不能になったりした場合、都市、地域または国に重大な影響を及ぼす可能性がある。このため、制御システムのセキュリティ問題に対する関心が高まっており、海外では、制御システムのサイバーセキュリティガイドライン及び標準を作成するための数多くの取組みが行われている。

これらの取組みのいくつかは、製品を海外輸出している制御システムのベンダばかりでなく、重要インフラをはじめとする我が国の制御システムのセキュリティ向上施策のための参考あるいは規準として重要と考えられる。

この文書は、制御システムのセキュリティに対する米国における取組み状況を日本国内の関係者に紹介するため、Digital Bond 社の調査資料をもとに、重要な制御システムのセキュリティガイドライン、標準及び認証への取組み、それぞれの取組みによって最も影響を受けるセクター及び地理的地域、取組みの動向などについてまとめたものである。

この報告書は次の 3 つの節で構成される。

1. 主要なガイドライン、標準、及び認証の取組み – これらは最も大きな影響を及ぼす可能性が高いため、注意を払うべき最も重要な取組みである。数は少ないが、潜在的な影響が大きく、またその標準化をめぐる政治的な駆け引きは技術的な詳細と同等に重要である。

2. プロトコル – この節では認証及び暗号化といったセキュリティ機能を統合した 5 つの制御システムプロトコルを取り上げる。これが重要なのは、プロトコルがセキュアになるということだけでなく、各種のセキュリティ機能が今後のプロトコルにも取り入れられる可能性が高いからである。Secure DNP3 の機能コード/認証手法や、OPC UA の完全な証明書ベースの手法などの将来性を交えて検証する。

3. マイナーもしくは中止された活動 – 最後の節では、そのほかの 2 種類の取組みの詳細を取り上げる。1 つめは中止された活動である。AGA 12、PCSF、PCSRF、その他の組織には相当なリソースが費やされたが、それらは公式に断念されたか、または事実上放棄されている。これらは依然として制御システムセキュリティ分野の概要でしばしば言及されるが、なぜ支持を得られなかったのかという議論の材料とする以外に特に重要性はない。

   もう 1 つは、進行中だが影響を与えるとは思われないマイナーな取組みである。例と

しては、APTA 鉄道セキュリティガイドラインの取組みがある。しかしながらこの節でも、記載しているのはマイナーもしくは中止された活動のなかでも最も重要なものだけである。取組みはほかにも多数存在しており、ここでは網羅的なリストの作成は意図していない。

この文書で取り上げるガイドライン、標準、及び認証の取組みの大部分はアメリカ主導の取組みである。これは、アメリカが制御システムセキュリティに先駆的に取り組み、この分野に最大のリソースを提供し続けているという事実に由来しているが，国際及び地域の制御システム会議は増え続けており、それに伴って制御システム標準及びガイドラインの国際的な活動も増加すると予測される。

JPCERT CC®

目次

1　主要なガイドライン、標準、及び認定の取組み

多数の制御システムセキュリティガイドライン、標準、及び認定の取組みが進行中である。アメリカが群を抜いて最も活動的な地域であるが、開発のさまざまな段階にある国際的、または地域的な取組みも存在する。資産所有者やベンダにとっての課題は、どの組織または文書に対して注意を払い、取り組むべきかということである。

この節では、Digital Bond が最も重要であると判断した、制御システムのサイバーセキュリティへの取組みについて述べる。節内の項目はアルファベット順であり、取組みをランク付けしているわけではない。読者は各取組みが自分の状況に適用可能かを判断するために、セクターや地域にも注意を払う必要がある。

1.1　DHS Control System Security Program

アメリカ国土安全保障省（DHS：Department of Homeland Security）の国家サイバーセキュリティ部門内に、Control System Security Program（CSSP）局がある。CSSP のプロジェクトの一つは、ベストプラクティスを記述、収集することである。これらのベストプラクティスは通常、DHS との契約のもと国立研究所、またはサードパーティによって記述され、ベストプラクティスに含める前に DHS によりレビューされる。現在のベストプラクティスは次のとおり。

- Control Systems Cyber Security Defense in Depth Strategies
- Creating Cyber Forensics Plans for Control Systems
- Good Practice Guide on Firewall Deployment
- Hardening Guidelines for OPC Hosts
- Mitigations for Security Vulnerabilities Found in Control System Networks
- Recommended Practice for Patch Management of Control Systems
- Securing Control System Modems
- Securing WLANs Using 802.11i（ドラフト）
- Securing ZigBee Wireless Networks in Process Control System Environments（ドラフト）
- Using Operational Security (OPSEC) to Support a Cyber Security Culture in Control Systems Environments（ドラフト）

これらの文書は、本書で取り上げる他の文書とは多少異なり、同業者による査読や投票は行われていない。単に、ベストプラクティスがどのようなものであるかを定める政府の情報源である。とは言っても、とても有用かつ詳細なガイドライン情報を提供している。

地域：名目的には、これらのベストプラクティスはアメリカ国内を前提としたものだが、他のいかなる組織や国でも適用可能である。アメリカは制御システムに対して手法や製品の開発で先行しているので、他国の産業組織もこれらの文書を参考にする可能性が高い。

セクター：ベストプラクティスはセクターに依存しない。

状況：CSSP はベストプラクティスの開発を続行する可能性が高い。

予測される影響：驚くべきことに、これらの文書はアメリカまたは世界の垂直セクターにごくわずかな影響しか与えていない。しかし、このことは文書の品質が低いということを意味しているわけではない。文書の品質は、差はあるものの平均して高い。それよりも次の 2 つの要因が理由と考えられる。1 つめは、DHS の国立サイバー・セキュリティ局（NCSD：National Cyber Security Division）がこれらの文書を市場に流通させ、人々にそれが利用可能で価値のあるものであることをきちんと知らしめていないこと。2 つめは、これらの文書の後ろ盾となる産業界の専門家グループが存在しないこと、である。ほとんどのガイドライン及び標準化組織にはこうした文書に何年にもわたって取り組んでいる人々のグループがある。彼らは個人的なつながりや公式なマーケティング努力を通じて、これらの文書がセクター内で知られるようにしている。前述のベストプラクティスは、このような状況になっていない。

1.2 ISA99

国際計測制御学会（ISA:International Society of Automation）は制御システムセキュリティに関して最も古くかつ活動的な組織である。サイバーセキュリティにかかわる作業のほとんどは SP99 - Manufacturing and Control Systems Security 委員会で実施されている。

SP99 委員会はまた、SP100 - Wireless Systems for Automation 及び SP84 - Electrical/Electronic/Programmable Electronic Systems (E/E/PES) for Use in Process Safety Applications の各委員会とも連携している。セキュリティは、開発中の無線標準にとって不可欠の要素である。SP100 委員会が無線セキュリティにかかわるほとんどの活動を実施してきたが、SP99 がこの活動のレビューを開始している。SP84 Safety のコミュニティでは、セキュリティシステムと安全システムの共通部分についての調査を始めている。安全システムは制御システムと相互に連携するため、これは大きな課題になりつつある。

地域：ISA は最近、ISA の"I"を Industrial から International へと変更した。ISA は国際的な組織になることを明言しているが、まだアメリカが多数派を占めている。SP99 委員会は、国際的に認識されている。

ISA99 標準は IEC 62443 と関連している。IEC は、独自に標準セキュリティの取組みを開始した後、ISA99 と連携して IEC が ISA と同時に承認できる標準を開発することにした。これが現実となれば、制御システムセキュリティの世界標準を開発するという ISA にとって大きな動きとなる。

セクター：ISA 標準に頼る主要なセクターは製造業だが、ISA はすべての制御システムの制御システムセキュリティ標準及びガイドラインの主要な組織になるというさらに大きな野心を持っている。この野心は何年も持ち続けられてきたが実現には至っていない。たとえば、電力セクターはアメリカで最も活発な制御システムセキュリティセクターであるにもかかわ

らず、ISA は電力セクターにほとんど影響力を持っていない。石油、ガス、輸送、また水道のセクターは、それぞれ独自に制御システムセキュリティガイドライン及び標準の活動を行ってきたため、ISA の影響力は小さい。

詳細及び状況：SP99 委員会は最近、複数パートからなる開発中の ISA99 標準の構成を変更した。委員会は IACS（Industrial Automation and Control Systems）という表現を制御システムの汎用的な表現として用いている。

- パート 1 ― 共通

  このパートでは、標準の残りの部分の枠組みを説明している。これは、ISA 標準のパート 1 の代表的な目的である。99.01.03 はこの文書のほかの標準とは少し異なり、厳密な情報というより、むしろ規範に沿った参考という位置づけである。

  99.01.01 - Terminology, Concepts and Models（用語、概念及びモデル）（以前の構成でリリース済み）

  99.01.02 - Master Glossary of Terms and Abbreviations（用語及び略語のマスタ用語集）（以前の構成でリリース済み）

  99.01.03 - System Security Compliance Metrics（システムセキュリティ準拠基準）（2010 年完成予定）

- パート 2 – セキュリティプログラム

  このパートでは、IACS のセキュリティ管理策の詳細を説明している。このパートの最初の 2 つの文書では、制御システムの構築及び操作/保守についてそれぞれ述べられている。99.02.03 は特定分野の管理策についての文書であり、他の 2 つとは対象とするレイヤが異なっている。理論的には、この文書の各論部分は 99.02.01、99.02.02 に含めることができる。すでに完了し、承認されている 99.02.01 を除き、進行中または予定されている作業は非常に少ない。活動は現在、パート 3 及び 4 を構成する技術要件に向けられている。

  99.02.01 - Establishing an IACS Security Program（IACS セキュリティプログラムの構築）（以前の構成でリリース済み）

  99.02.02 - Operating an IACS Security Program（IACS セキュリティプログラムの運用）（未定）

  99.02.03 - Patch Management in an IACS Environment（IACS 環境におけるパッチ管理）（未定）

- パート 3 – 技術的システム

  技術要件の文書は、以前の構造ではパート 4 単体になる予定であったが、非常に大きく複雑になっていた。これが構成変更の主な理由である。

99.03.01 - Security Technologies for IACS（IACS のセキュリティ技術）（技術レポート 1 として完成、ISA99 標準へ移行中）

以前の技術レポート 1 が 99.03.01 を構成し、ファイアウォール、トークン、及び役割ベースのアクセス制御といったセキュリティ技術と、制御システムへのそれらの適用可能性について述べている。

99.03.02 - Target Security Assurance Levels for Zones and Conduits（ゾーン及びコンジットのターゲットセキュリティ保証レベル）（2009 年完了予定）

この文書はどのように IACS をゾーンに分割し、またゾーンを結ぶ情報ルートをどのように割り当てるかを述べている。

99.03.03 - System Security Requirements and Security Assurance Levels（システムセキュリティ要件及びセキュリティ保証レベル）（2009 年完了予定）

この文書ではゾーンのセキュリティ保証レベル（Security Assurance Level（SAL）を定義し、SAL の要件をリストアップしている。

99.03.04 - Product Development Requirements（製品開発要件）（2010 年～2011 年完了予定）

構成を変更した ISA99 のこの新しい文書で、ベンダ及びインテグレータに対する製品開発要件を記述している。

- パート 4 – 抽出技術（2010 年～2011 年完了予定）

このタイトルの「抽出」の意味するところは、特定の種類の機器に対するパート 4 の要件が、パート 3 で記述されたものより、一般的な技術要件から派生しているものだということである。これは、ISA99 標準のなかで最も具体的かつテスト可能な要件のセットである。

99.04.01 - Embedded Devices（組み込み系機器）

99.04.02 - Host Devices（ホスト機器）

99.04.03 - Network Devices（ネットワーク機器）

99.04.04 - Applications, Data and Functions（アプリケーション、データ及び関数）

ISA 及びほかの標準化団体は往々にしてスケジュールが遅れることから、このスケジュールが守られる可能性は低い。また、標準の改訂された構造とパート 3 及びパート 4 の技術要件の目的がコンセンサスによる標準化プロセスで達成できるかが疑問である。

予測される影響：これを予測するのはとても困難である。今日までにリリースされた ISA99 の技術レポート及び標準は高く評価されている。文書を記述し、査読しているチームは評判が高く、高い品質の成果を出している。したがって、ISA99 は最も使用される制御システムセキュリティガイドラインの 1 つとして存続すると思われる。

2009 年はパート 3 及び 4 の技術要件に関心と取組みが集中しているが、ISA99 の計画は非常に意欲的なものであるため、パート 3、4 が実際の試験及び認証に耐える標準化につながるにはまだ時間がかかるものと思われる。

ISA は各種の試験計画に対して、制御システムのセキュリティソリューションの試験を行い認証するための Security Compliance Institute（SCI）を立ち上げた。SCI は、標準の基準部分に関する試験を行い認証が与えられる最初の標準の一つとして ISA99 を考えていた。しかしこれは今では考えにくい。なぜなら ISA 99 の完成までに数年かかると思われ、SCI が閉鎖される可能性が非常に高いからである。

1.3 NERC CIP

北米電力信頼度協議会（NERC：North American Electric Reliability Council）は大規模な停電のあとに設立された業界団体である。大規模な電気事業体で構成され、共同で自主規制を行っている。9/11 のテロ攻撃のあと、NERC はサイバーセキュリティへ関心を集中し始めた。取組みは、コンセンサスの取組みの大多数がそうであるように、非常にゆっくりとしたものであった。しかし、結果として NERC Cybersecurity Critical Infrastructure Protection（CIP）標準として知られている標準が作成された。

地域：NERC CIP 標準は、アメリカ及びカナダで適用可能である。ほかの地域での、これらの標準を採用または修正することは可能だが、多くの面で北米の大規模電力システムの相互接続の性質は特有のものである。

セクター：NERC CIP 標準は大規模電力システム、つまり主に送電と大規模発電に影響を与える。

ほかの地域やセクターでも、Critical Cyber Assets（重要サイバー資産）の定義を変更することで簡単にこの標準を修正し、完全かつ監査可能な標準を作成することができる。しかし、現時点でそのような試みがなされた形跡はない。成り行きを見守っているようである。

詳細及び状況：NERC CIP サイバーセキュリティ標準には長く、ねじれた歴史がある。当初、NERC CIP サイバーセキュリティ標準は完全に NERC 会員のための NERC による自主規制であった。ところが、US Energy Act（アメリカエネルギー法）が連邦エネルギー規制委員会(FERC :Federal Energy Regulatory Commission)に対してサイバーセキュリティを含む、電力網の信頼性確保に対する責任を与えたため、状況が変化した。法令には、サイバーセキュリティ標準を作成、施行する電力信頼度機関（ERO：Electric Reliability Organization）を FERC が指名するよう定められていた。

興味深いことに FERC には詳細な権限はほとんどなかったが、ERO の活動を選択、承認することはできた。FERC は NERC を ERO として選択した。これは驚くべきことではなかった。実際、ほかに選択肢は存在しなかった。そして NERC は NERC CIP を ERO が使用するサイバーセキュリティ標準として提案した。

8 個の NERC CIP サイバーセキュリティ標準が存在する。

- CIP-002: Critical Cyber Asset Identification
- CIP-003: Security Management Controls
- CIP-004: Personnel and Training
- CIP-005: Electronic Security Perimeters
- CIP-006: Physical Security
- CIP-007: Systems Security Management
- CIP-008: Incident Reporting and Response Planning
- CIP-009: Recovery Plans for Critical Cyber Assets

これらの標準には実際の要件として、必須、推奨、監査要件があるが、資産所有者に対して非常に大きな自由度を与えている。多くの IT セキュリティ専門家が包括的なサイバーセキュリティプログラムと認めるであろう定義がされているが、資産所有者はシステムのセキュリティに影響する多くの判断を行わなければならない。

一つの単純な例が CIP-002 に存在する。この標準は資産所有者に、Critical Assets（重要資産）及びそれらに関連する重要 IT 資産を特定するよう要求している。資産所有者はこの特定のための方法論及び決定に関する裁量権を持つ。ほかのすべての CIP セキュリティ要件が重要 IT 資産に基づいているため、この選択はシステムセキュリティに対して大きな影響を与える。

規制当局の観点から見ると、この裁量権は厄介で、標準の監査をより難しいものにしている。電力会社は、セキュリティ管理策が必要な（あったとしても）少数の重要 IT 資産を特定するようなプログラムまたはアプローチを構築することによって、必要な作業とその結果のセキュリティを最小限にしようとしているとする発言が数多くある。

予測される影響：NERC CIP サイバーセキュリティ標準は完全に失敗する可能性があるにもかかわらず、多くの意味で制御システムセキュリティ分野における最も影響力のある取組みである。影響力があると言っているのは、サイバーセキュリティに関して何の関係もなくなる可能性のある多くの電力会社が大きな取組みを行っているという事実にある。この標準は、どんなセクターや地域よりもはるかに大きいアメリカ/カナダの大規模電力システムに対して、巨大な影響を与えている。

予想される影響の判断は政治的な駆け引きの理由からとても困難だが、あえて予測するとすれば、NERC CIP 標準は大幅に置き換えられ、NERC は 2010 年に ERO としての指名を失うと考える、というのが Digital Bond の予測である。新しい ERO は NIST SP800-53 を修正し、それを NERC CIP と置き換えると予想される。

これは大規模電力システムのサイバーセキュリティを強化するために、何がより有効かということの反映ではない。むしろ、これは現実的政治の反映である。議会は NERC が十分な働きをしていないと確信している。そして FERC はその判断を支持している。議会が耳を傾けている人々は SP800-53 こそが解決策だと主張している。何が最も有効かという問題ではなく、政治なのである。

1.4 NIST

アメリカ国立標準技術研究所（NIST：National Institute of Standards and Technology）は SP800 シリーズと名付けたコンピュータセキュリティに関する特別文書（Special Publications）を作成している。2 つの文書が制御システムコミュニティに当てはまる。

- SP800-53 Recommended Security Controls for Federal Information Systems（連邦政府情報システムにおける推奨セキュリティ管理策）

  これはアメリカの政府機関にとって重要な文書である。アメリカ政府のコンピュータシステムのための運営管理上及び技術上の管理策について詳しく述べている。Tennessee Valley Authority や Bonneville Control Systems といった電力会社のようなアメリカ政府の制御システムを含め、アメリカ政府の機関はこれらの管理策に対する遵守の監査を受ける。

  制御システムは典型的な SP800-53 の監査方法や要件のいくつかによって悪影響を受ける可能性があるため、NIST は産業用制御システムに対する補足のガイドを提供している。

- SP800-82 Guide to Industrial Control System Security（産業用制御システムセキュリティのためのガイド）

  このガイド文書には必須の要件や監査は含まれていないが、制御システムに特化した唯一のアメリカ政府の公式文書である。

地域：NIST の文書はアメリカ国内でのみ適用可能である。

セクター：公式には、これらの文書はアメリカ政府が運用する制御システムにのみ適用される。

状況：SP800-53 は公開後、定期的に更新されている。SP800-82 は 2008 年末時点ではまだ案（draft）として掲載されている。しかし、これは NIST の長く形式的なレビュープロセスだけが原因である。NIST の Web サイトから最終形式に近いと思われるものが入手可能である。

予測される影響：アメリカ国内の重要インフラの大部分はアメリカ政府ではなく民間産業に所有されている。したがって、SP800-53 は適用されないため、理論上影響は少ないはずである。しかし、まったく逆のことが現実になる可能性が高くなってきている。SP800-53 はアメリカで最も重要な制御システムセキュリティ文書になる可能性がある。

その理由は、アメリカ政府が重要インフラ制御システムに対して規制強化の方向へ向かっているように思われるためである。そしてこの政治的な風向きは、SP800-53 がアメリカ政府に適用可能な標準であるならば、民間産業に所有されている重要インフラのセキュリティがそれ以下であるべき理由は存在しないと議会が考えていることを示唆している。FERC に NERC CIP 標準を SP800-53 と一致するように変更することを検討するよう働きかける積極的な取組みが政府内に多数存在している。今後のすべての規制は SP800-53 の手法に従うように推し進められる可能性が高い。

2　プロトコル

制御システムのプロトコルは多数存在するが、重要インフラ制御システムで使用されるこの重要なプロトコル群にセキュリティを付加しようという取組みはほとんどなされていない。多くの点でこれは驚きである。なぜなら、制御システムに対して論理的にアクセスが可能な任意の攻撃者が、フィールド機器及び多くのケースではその基礎的な処理を完全に制御できる能力を持つことを意味するからである。これらのプロトコルの多くは IP （Internet Protocol） に対応しており、企業ネットワークなどの比較的セキュアでないネットワークに相互接続されていることから、攻撃者に制御を乗っ取られることを想像するのは難しくない。私たちは、なぜ IP にカプセル化されるすべてのプロトコルで、セキュアなバージョンが開発されていないのかを考えなければならない。

この節に掲げる以下の 5 つのプロトコルは、制御システムプロトコルを保護しようという試みの先駆者を代表している。

・Secure DNP3

・IEC 62351-3

・OPC Unified Architecture（UA）

・Wireless HART

・ISA 100

近い将来に最も影響を持つであろうと思われるプロトコルは Secure DNP3 / IEC 62351-3 である。これは、すばやく実装でき、所有者や運用担当者に使いやすいためである。

2.1　Secure DNP3 / IEC 62351-3

DNP3 及び対応する IEC のプロトコルは電力セクターで広く使用されており、ほかのセクターの市場にもいくらか浸透してきている。DNP フォーラム及び IEC 委員会は、それぞれのプロトコルに発信元及び内容に対する認証機能を追加しようという協調的な取組みを行っている。両者はほとんど同一であり、以下この項では Secure DNP3 と呼ぶ。

手法としては、チャレンジ/レスポンス認証のために 5 つの機能コードを追加するというものであった。この手法によって、Secure DNP3 はシリアル、TCP/IP 及びハイブリッドネットワークの両方での作動が可能となる。チャレンジ/レスポンス認証は通信の重要性に合わせて、いろいろな時点で実行するように構成することができる。たとえば、認証をセッションの確立時、及びその後は定期的に実行させることができる。または、重要な機能コードの前で認証を実行させることもできる。したがって、書き込みには認証が必要だが、読み取りには必要ないということも可能である。

Secure DNP3 標準は事前共有鍵を前提としている。それぞれのグループが、鍵のライフサイクルにかかわる課題を自動化するために鍵管理標準に取り組んでいる。

地域：これら 2 つのプロトコル標準の市場を組み合わせると、世界規模の範囲となる。

セクター：電力セクターが主要な DNP3 のユーザであり、Secure DNP3 の主要なユーザになると思われる。ほかのセクター、特に水道は Modbus がニーズを満たせない場合に DNP3 を使用することがある。たいていの場合、これは自律応答または、より長い応答パケットに対するニーズがあることによる。

状況：Secure DNP3 は DNP 委員会によって承認されている。鍵管理標準は最終案に近く、専門家によりレビューが行われている。鍵管理標準は今年承認される可能性が高いが、実装は単に Secure DNP3 を実装するよりは難しい。

予測される影響： DNP3 は、ほとんどの制御システムにおけるセキュリティ上の最大の懸念である、発信元及びデータの認証に力を注いできた。この標準は資産所有者のコミュニティでは大きな支持や注目を得ていないものの、DNP3 スタックを提供するほとんどのベンダは Secure DNP3 プロトコルスタックに取り組んでいる。そのため、2 年以内には販売されるほとんどの DNP3 モジュールが Secure DNP3 オプションを備えるようになると思われる。

鍵管理を持たない Secure DNP3 の実装は単純である。そのため大部分のユーザが Secure DNP3 を実装すると思われる。これらのユーザが鍵管理を実装する可能性はかなり低い。これは、能力の高い攻撃者は鍵付与の関係を狙うことでシステムを侵害することが可能だが、市場の大部分を占める初心者や中程度のスキルの攻撃者にはそれができないことを意味する。このため、Secure DNP3 は北米で非常に大きな影響力を持ち、IEC 62351-3 は国際的に大きな影響力を持つことになる。

この標準の成功はまた、ほかの標準に影響する可能性がある。手法は単純で再現可能である。

2.2　OPC Unified Architecture（UA）

OPC は制御システム向けの汎用的な変換の仕組みである。実際の監視や制御に使用されることはほとんどないが、さまざまなベンダのシステムどうしでデータをやり取りすることが可能になるため、非常に重要である。ほぼすべての制御システムコンポーネントは OPC インタフェースを持つため、「操作」に使用されることがほとんどないにもかかわらず、OPC は非常に重要なプロトコルである。

OPC UA は OPC プロトコルの次世代プロトコルである。セキュリティは OPC UA の主要な設計目標の 1 つであった。要求及び応答パケットのそれぞれの発信元及び内容を認証することができ、機密保護のための暗号化オプションも備えている。

Digital Bond はプロトコル文書及びソフトウェア開発キット（SDK：Software Development Kit）のソースコードの詳細な適用評価を実施した。OPC Foundation は、全部ではないとしても、多くの明らかになっている脆弱性に対応している。しかし、これらの脆弱性が修正され

たとしても、OPC UA 標準は各ベンダが OPC UA セキュリティの非標準部分をどのように実装するかに応じて、セキュリティに対する姿勢が大きく異なる可能性がある。たとえば、X.509 証明書の受け入れ及び承認はこの標準の一部ではない。それぞれの実装が異なる処理を行うことになる。

地域：OPC UA は国際的なプロトコルである。アメリカで最も人気が高いが、競合は基本的に存在せず、世界中で広く使用されている。

セクター：OPC は異なるベンダのシステム間での相互運用性のために広く使用されている。したがって、OPC UA は多くの垂直セクターで使用されると思われるが、実際の監視や制御に使用されることはほとんどない。システムが大きく複雑になるほど、相互運用性が課題になる可能性が高くなるため、OPC、そしていずれは OPC UA が使用されることになる。

状況：OPC UA は複数パートからなる標準である。いくつかの標準案が発行済みで、現在のバージョンの標準及びソフトウェア開発キットは 2009 年の第 1 四半期にリリースされた。標準文書が落ち着くまでにまだいくつかの改訂があると予想されるが、変更は徐々に少なくなっている。

多くのベンダが、早い場合には 2008 年に OPC UA のサポートを発表しているが、2009 年 3 月の時点では標準がまだ変更されているため、本当の OPC UA の実装は存在しない。

予測される影響：OPC UA プロトコルのセキュリティは、数が多く広範な OPC UA ユーザだけでなく、ほかの制御システムプロトコルにも大きな影響を与えると考えられる。OPC Foundation は OPC UA のセキュリティ機能と利点を重点的にマーケティングしている。

Digital Bond の予想によると最初の OPC UA クライアント及びサーバが 2009 年内に入手可能になるということである。ただし、制御システムのコミュニティはやむをえない理由がない限りは変わろうとしないため、OPC UA が OPC を置き換えるには非常に長い時間がかかると思われる。

OPC UA は広く利用されている OPC クライアント及びサーバに対する下位互換性を提供している。これは展開のスピードアップに寄与するはずだが、多くの所有者、運用管理者は OPC を使い続けるだろう。なぜなら、彼らにとって現状の OPC に何ら問題がないからである。

2.3 Wireless HART / ISA 100

Digital Bond のレポートにおいては Wireless HART と ISA 100 を同じグループとしている。この理由は、両者とも比較的新しい無線 LAN ソリューションで、プロトコルの開発当初からセキュリティに取り組んでいるからである。DCS での使用のために設計され、有線のソリューションを置き換えるものである。

これらのプロトコルのセキュリティ、特に ISA 100 は、暗号化と認証を備えた包括的なものである。ISA 100 は実際に鍵管理のための公開鍵基盤を含んでいる。

地域：この 2 つのプロトコルは世界中で使用される。

セクター：これは LAN プロトコルであるため、DCS に適用可能で、SCADA には適用されない。製造、電力生産、水処理、及びほかの DCS などさまざまなセクターで使用されると思われる。

状況：Wireless HART はすでにリリースされ、展開済みである。ISA 100 はまだ開発中である。ISA 100 ソリューションは 2009 年後半または 2010 年前半に入手可能になるはずである。ISA 100 委員会は Wireless HART との相互運用性を含める取組みを進めている。

予測される影響：ある意味では、これらは競合する標準であり、ISA 100 には非常に多くの政治的駆け引きがからんでいる。見方を変えると、導入の可否をめぐって競合しているわけではない。HART 利用者とベンダのコミュニティは非常に忠実で、無線の使用を決定した場合は Wireless HART を使用すると考えられる。多くのベンダが ISA 100 を推進しているが、彼らは競合する構想及び標準への要望を持っているため、遅れが発生しており最終的な成果はまだ不確かである。

無線が今後も有効なネットワークソリューションとみなされ続ける限り、ISA 100 及び Wireless HART はともに多くの支持と導入がなされると予想するのが妥当であろう。

ベンダコミュニティは無線を推進しつつ、多くのセキュリティ問題を回避している。セキュリティ専門家からの警告にもかかわらず、多くがプロジェクトを推進し、無線を監視、制御の両方に使用している。重要な処理の制御にさえも使用している。

無線セキュリティ問題に対する認識が高まるにつれて、セキュリティ問題に対する「ソリューション」としてこれら 2 つの標準の利用が増えていくと考えられる。

3　マイナーもしくは中止された活動

ここ 8 年の間に制御システムセキュリティへの取組みが数えきれないほどなされてきた。それらの多くがほとんど影響を与えることなく消えていった。いくつかはまだ残っているが、大きな地域やセクターに影響を与えたとは言えない。この節では、いくつかの興味深いマイナーもしくは中止された制御システムセキュリティへの活動を簡単に紹介する。

3.1　AGA 12

アメリカガス協会（AGA：American Gas Association）は、制御システムのサイバーセキュリティに取り組んだ最初の組織の一つである。セキュリティになじみのない人々の多くがそうであるように、AGA-12 は「暗号化 ＝ セキュリティ」と信じ、まず暗号化に集中した。また、IP プロトコルではなく、シリアルプロトコルの暗号化に焦点を絞ることにした。シリアルに焦点を絞ることにしたのは、その当時 SCADA 及び DCS の通信の大部分がシリアル回線を通じて行われていたからである。これは今日現在も同じである。

しかしこの決定は、シリアルネットワークがルーティング可能なネットワークではなく、比較的わかりにくいプロトコルを使用しているため、シリアルネットワークへのアクセスがはるかに難しいという事実を看過していた。シリアルネットワークのセキュリティを侵害するには通常、物理的なアクセスが必要であり、物理的なアクセスを得れば、サイバー攻撃より物理的な攻撃の方が簡単である。IP プロトコルがセキュリティの注目のほとんどを集めたのは、インターネットまたは企業ネットワークからの攻撃者がこれらのネットワークにルーティング可能で、攻撃者には無料で入手可能な多くの種類の IT 攻撃ツールがあるからである。

AGA 12 のシリアル暗号化仕様は完成し、サンプルユニットが開発及び試験される間にプロジェクトに対する関心は薄れていった。アメリカ政府は財源を削減した。Thales や Mykotronx といったベンダは製品を開発し販売する取組みを放棄した。鍵管理標準を開発する取組みも存在したが、これもほとんど放棄された。ついには、このプロジェクトに割り当てられていたスタッフが解放された。

AGA 12 グループはいくつかのガイドライン文書も開発したが、これらはほとんどがほかのデータの寄せ集めであり、オリジナルの文書も第 1 節の文書ほど有用ではない。

AGA はパイプライン業界内の重要な組織である。今後セキュリティガイドラインまたは標準への取組みを始めると考えられるが、シリアル暗号化プロトコル標準の更新を行うとは考えにくい。

3.2　API 1164

アメリカ石油協会（API：American Petroleum Institute）は API 1164 Pipeline SCADA Security を 2004 年に発行した。これはガイドライン文書で、小規模のパイプライン運用者を対象にしていた。文書内の手引きは極端に単純化されており、多くの場合、間違っていた。この文

書になんらかの価値があるとすれば、制御システムセキュリティプログラムを始めたばかりの SCADA または DCS 所有者、管理者にとってであるが、それでもほかのガイドライン文書を使用した方がよいだろう。

API は 2009 年または 2010 年中に発行される API 1164 の更新版の作業を行っている。この文書は現在のバージョンよりも飛躍的に良くなるはずである。

3.3 PCSF

アメリカ国土安全保障省（DHS：Department of Homeland Security）は 2005 年に、制御システムのコミュニティを 1 つにまとめ、産業界、政府、学会、研究機関、及びそのほか任意の関心のある組織の間で情報を交換するための組織としてプロセス制御システムフォーラム（PCSF：Process Control Systems Forum）を設立した。その使命は非常に広範だったが、標準の開発は含まれなかった。しかし、取組みの重複を防ぐため、異なる標準やガイドラインの取組みの間での情報の共有を行う予定であった。

PCSF は高い質を維持することと多くの参加があった年次総会については大成功を収めた。ワーキンググループでプロジェクトを完了させることについてはうまくいかず DHS による支援のスタンスの変更がこの組織に大きくマイナスの影響を与えた。ガイドライン文書の開発の試み及び業界の取組みはほとんど失敗した。多少の成功を見た統合用語集プロジェクトも存在した。基本的に PCSF には大成功の年次総会のほかには特に何もなかった。

PCSF は 2008 年の総会の後に解体させられた。不満を持った制御システムコミュニティのメンバーにより監査が強制され、PCSF に対する DHS の資金提供に不法なものが存在した。

2009 年に DHS は産業用制御システム共同ワーキンググループ（ICSJWG：Industrial Control System Joint Working Group）を設立し、PCSF の産業界と政府の間の連携部分と置き換えた。このワーキンググループが何をするのかは明らかではないが、初期の兆候では PCSF のような年次総会は行わないようである。代わりに、まだ明示されてはいないが特定の作業項目に焦点を絞るようである。PCSF が成功を収められなかった分野での成功を狙い、PCSF が最も成功を収めた分野を追いかけないところが興味深い。

3.4 PCSRF プロテクションプロファイル

プロセス制御セキュリティ要件フォーラム（PCSRF：Process Control Security Requirements Forum）はアメリカの最も早い制御システムセキュリティの取組みの一つで、国立標準技術研究所（NIST：National Institute of Standards and Technology）の資金援助を受けていた。最初の数回の会合後、PCSRF はプロテクションプロファイルの形で要件を開発するためにコモンクライテリア（情報技術セキュリティ評価基準）を使用することに決定した。

3 つのプロテクションプロファイルが開発された

- System Protection Profile

- Control Center Protection Profile
- Field Device Protection Profile

System 及び Control Center Protection Profile はコモンクライテリアに厳密には沿っておらず、システムへのアプローチの変更を試みている。これらの文書について、コモンクライテリアのもとでの認証につながるセキュリティターゲットを開発することはできなかった。しかしながら、一部の情報は非常に有用である。たとえば、System Protection Profile には制御システムに関するリスク評価を実施する際に非常に役に立つ項がある。

Field Device Protection Profile はコモンクライテリアの形式に厳密に従っており、セキュリティターゲットの基礎とすることができる。

結局、要件文書のためにコモンクライテリアの形式を使用するという PCSRF の初期の選択は間違いであった。コモンクライテリアの文言や構造は容易でなく、相当な努力をもってしても理解するのは難しい。PCSRF の中でさえ、これらの文書の作成やレビューを行えるのはごくわずかだった。ベンダにとっての主な関心はプロテクションプロファイルに合わせて製品が認証されることであり、難しいコモンクライテリアの議論は敬遠された。やがて興味は失せ、最終的には、NIST も PCSF に注力するようになった。

3.5 APTA Rail Security

アメリカ公共交通協会（American Public Transportation Association）は Technical Recommended Practice for Securing Control and Communications Systems in Transit Environments（輸送環境における制御及び通信システムのセキュリティ確保のための技術的ベストプラクティス）に取り組んでいる。APTA 制御及び通信セキュリティワーキンググループ（APTA Control and Communications Security Working Group）は NIST の SP800-53 を主要なソース文書として使用し、次に鉄道セクターに当てはまる情報や用語を追加していった。

この文書は北アメリカのみに適用でき、旅客鉄道はアメリカではほかのほとんどの地域に比べて比較的マイナーである。ワーキンググループには多少の国際的な参加者もおり、これが国際的な活動の火付け役となるかもしれない。

進展は遅いが、アメリカの鉄道資産所有者の関与も増しており、2009 年中には文書が完成し、発行されるはずである。しかし、ベストプラクティス文書はガイドライン文書であり、全体に大きな影響を与えるものは少ないと考える。ガイドライン文書は、少数だがサイバーセキュリティ対策を実装したい鉄道所有者/運用管理者にとっては助けとなるだろう。それ以外の鉄道所有者/運用管理者は、制御システムのサイバーセキュリティ対策について、興味を持つことも、対策を講じることもない。