平成 22 年度
内閣官房情報セキュリティセンター委託調査

制御システムのオープン化が重要インフラの情報セキュリティに与える影響の調査

財団法人未来工学研究所

平成 23 年 3 月

制御システムのオープン化が重要インフラの情報セキュリティに与える影響の調査

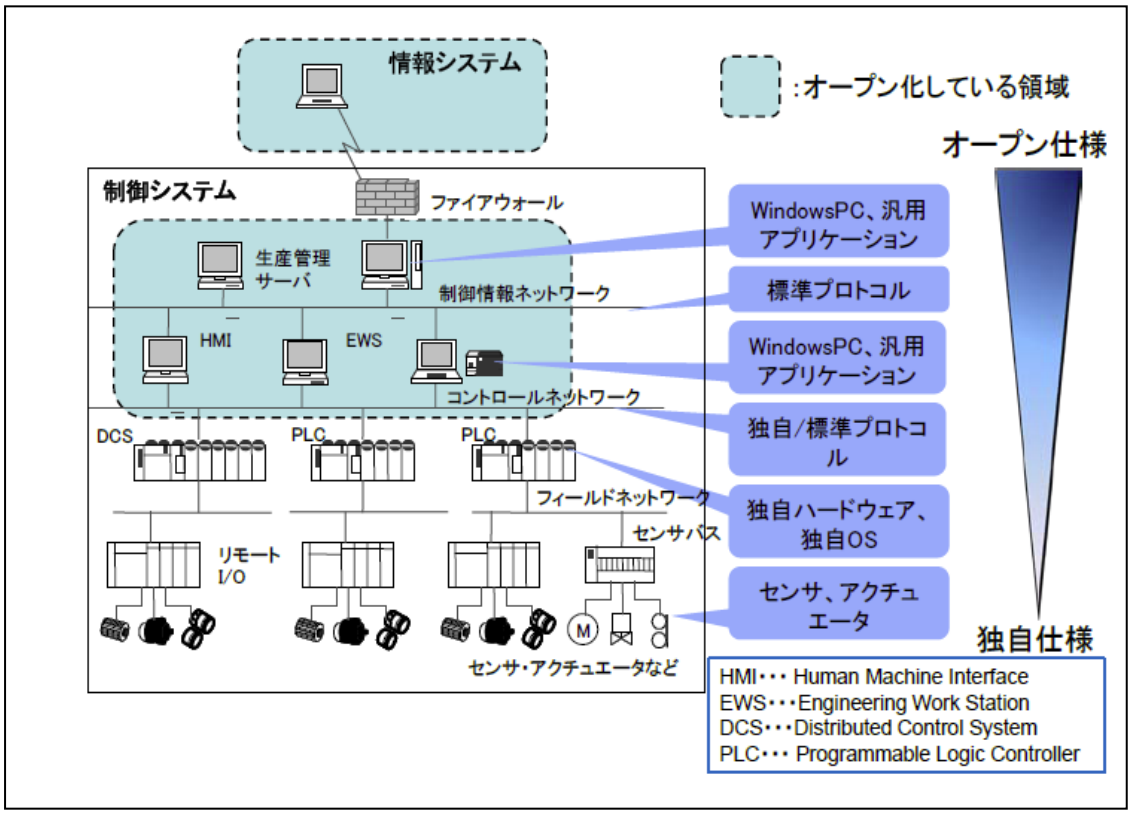
1. 制御システムのオープン化に係る環境変化の概要

1.1 制御システムの定義

制御システムのセキュリティについて2008年度と2009年度の２年間にわたって詳細な調査を行った「独立行政法人・情報処理機構（IPA）」の「重要インフラの制御システムセキュリティとITサービス継続に関する調査」[1]と「制御システムセキュリティの推進施策に関する調査報告書」[2]は、制御システムについて広義と狭義の二つの定義を与えている。

それによれば、狭義の制御システムは「センサやアクチュエータなどのフィールド機器、コントローラ、監視・制御用に用いるサーバやクライアントPCなどをネットワークで接続した機器群（システム）」とされ、それらのシステム開発と構築、システムの運用、システムに係るガイドラインや政策を含めて広義の制御システムとしている。下の図表1-1がIPAの定義する「制御システム」概念である。

図表1-1 IPAの定義する「制御システム」



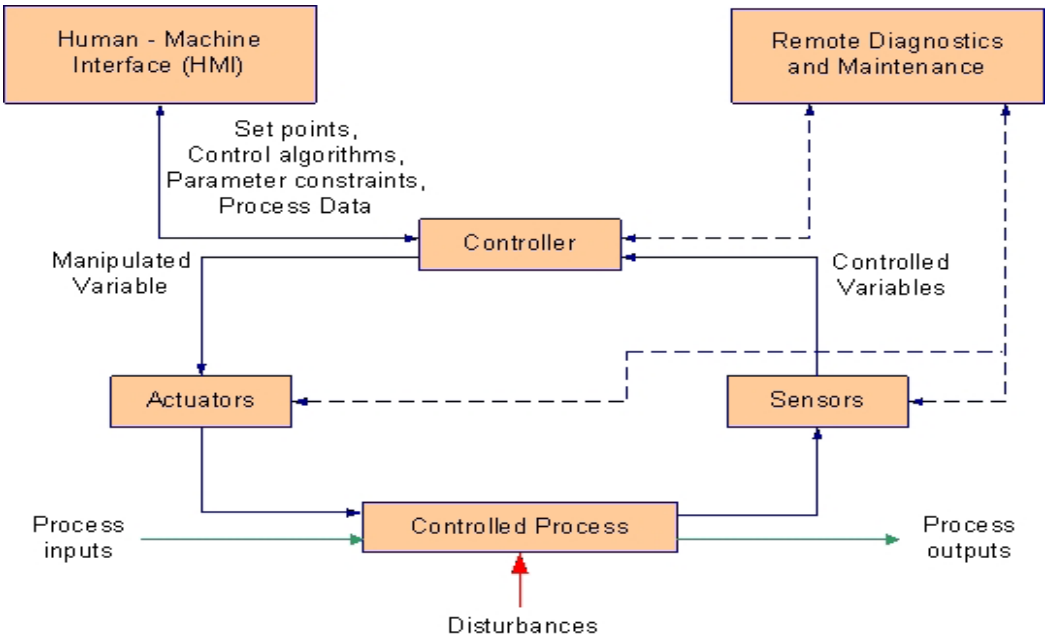
出典：ＩＰＡ制御システムセキュリティの推進施策に関する調査報告書（脚注 2）より

[1] IPA、重要インフラの制御システムセキュリティと IT サービス継続に関する調査、2009 年 3 月

[2] IPA、制御システムセキュリティの推進施策に関する調査報告書、2010 年 5 月

また、米国のNIST（商務省国立標準技術研究所）は、制御システムのセキュリティに関する最新の最重要文書であるNISTSP800-82[3]において、制御システム（米国では産業制御システム=ICSと呼ぶ場合が多い）を、「SCADA(Supervisory Control And Data Acquisition=監視制御・データ取得)システム、DCS（分散制御システム)、PLC(Programmable Logic Controllers)のような制御システム構成などを網羅する一般的な用語である」と定義している。図表 1-2 にNISTSP800-82 が示す制御システムの概念図を掲げた。

図表1-2 NISTSP800-82が掲げる制御システムの運用概念図



出典：脚注3より

1.2 制御システムのオープン化とSCADA

重要インフラの制御システムは、1970年代から80年代のメインフレームシステム時代に開発され、今日まで運用されてきた。制御システムが開発された当時、その仕様も通信規格もベンダの独自製品であり、制御システムのネットワークも情報システムと分離され、インターネットとも未接続であった。これがいわゆるレガシーシステムである。

しかしながら、近年のIT技術の急速な発展を背景に、①製品開発コストや運用コストの抑制のためにWINDOWSやLinuxなどの汎用OSの導入が進み、②マルチベンダー化に対応するために制御システム内でもEthernetなどの汎用通信規格の利用が広がり、③生産・在庫情報管理などのために情報システムと制御システムが接続され、④部分的にはインターネットとの結合も進んできた。これらが制御システムのオープン化と呼ばれる状況である。

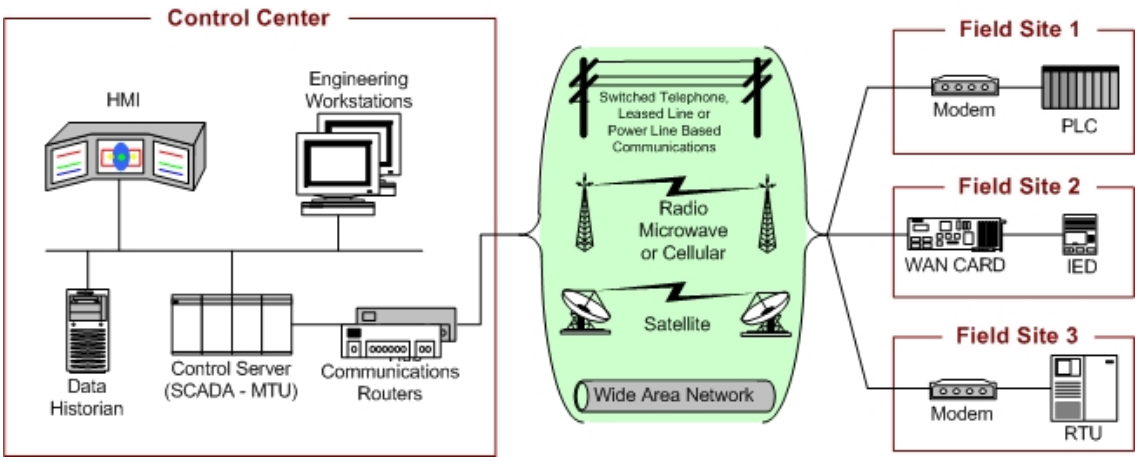
このような状況を踏まえ、1.1で引用したIPAの調査では、「汎用製品の採用及び標準プ

[3] NIST Special Publication 800-82, Guide to Industrial Control Systems (ICS) Security, Sep 2008

ロトコルの採用の両方を含めて、制御システムのオープン化」と呼ぶと定義している。

また、同じく1.1で引用したNISTSP800-82文書では、制御システムのオープン化という用語は特に用いていないが、SCADAという概念で「制御システムのオープン化」を示しているようである。同文書では、SCADAは「中央集中型のデータ取得と制御がシステム運用に死活的に重要な、しばしば数千平方ｷﾛﾒｰﾄﾙにも及ぶ地理的に分散したアセットを制御するために用いられる高度に分散化したシステム」と定義している。図1-3はNISTSP800-82が示すSCADAの概念図である。

図表1-3 NISTSP800-82が示すSCADAの概念図



出典：脚注3より

わが国では、PLCなどの制御機器の監視を汎用PC上で実行するためのソフトウェアをSCADAと呼ぶ場合が多いが、上に紹介したIPAの調査報告では、SCADAを「制御システムのうち汎用製品、標準プロトコルが採用されているシステムをさすこととする」として、SCADAの概念を事実上「制御システムのオープン化」と同義に用いている。

また、NISTSP800-82の筆者でもあるキース・ストーファーが2007年に提出したプレゼンテーション[4]では、①ベンダ独自規格に代わるオープンプロトコルの採用、②経営管理システムなど他のシステムとの結合、③共有の通信システムやインターネットのへ依存の拡大を、近年のSCADAの傾向として挙げている。

なお、制御システムのセキュリティに関しては、わが国ではIPAが行った調査研究（脚注1及び2）が幅広く詳細を極めている。また、米国ではNISTSP800-82（脚注3）がこの問題に対する中心的な文書となっている。本報告ではこの二つの文書を中心として「制御システムの情報セキュリティ」という課題を紹介し、必要に応じて欧州の状況や最新の動向や対策などを付け加えて報告することとする。

[4] “Supervisory control and data acquisition(SCADA) security,” Keith Stouffer, Feb. 2007

2. 制御システムのオープン化と情報セキュリティに係る最近の動向と将来予測

2.1 制御システムのオープン化と情報セキュリティ課題の顕在化

2.1.1 わが国IPAの指摘する制御システムの脆弱性分析

かつては各個独立した専用システムであった制御システムが、汎用製品や標準プロトコルを採用することで、情報システムが固有に持っているセキュリティ上の課題を有するようになり、近年では制御システムの脆弱性に由来すると見られるインシデントも顕在化するに至った。IPAの調査（脚注1）では、制御システムのオープン化に伴うセキュリティ課題として以下の３点を挙げている(要約)。

①オープン化に伴う脆弱性リスクの混入

・汎用製品の採用に伴い、汎用製品が有するハードウェア・ソフトウェアの脆弱性をそのまま引き継ぐことになった。汎用製品の脆弱性関連情報および対策のためにパッチが公開されるが、稼動中の制御システムへそのまま適用することは、制御システムの可用性重視の観点からほとんど行われていない。パッチ適用によるシステムの再起動や不具合などによってサービスが停止する恐れがあるからである。

・標準プロトコルのネットワークを採用することにより、ワームなどのウィルスの侵入や機密情報漏えいの可能性が生じた。他システムとの間にファイアウォールを設置している例が多いが、脆弱性はゼロではなく、また制御システム外部から持ち込まれたPC やUSB メモリなどの記憶デバイスなどから、自動化されたワームが侵入する可能性も考えられる。

②製品の長期利用に伴うセキュリティ対策技術の陳腐化

・制御システムは通常10年～20年のライフサイクルで使用される、それに伴って制御システムが利用する汎用製品や標準プロトコルも、情報系における最新製品（通常5年前後のサイクルで更新される）ではなく、その結果セキュリティ対策も陳腐化しがちである。

③可用性（Availability）重視によるセキュリティ機能の絞込み

・セキュリティへの考え方が制御システムと情報システムで大きな違いがある。情報システムでは、機密性（Confidentiality）、完全性（Integrity）、可用性（Availability）の順、すなわちC.I.Aの順で重視されるが、制御システムではA.I.Cの順で重視される。

・制御システムでは、可用性（Availability）を重視するので、一般にウィルス監視やチェックプログラムの自動更新などは行われない。従って、ウィルスが制御システムに侵入した場合、たちまち拡散する可能性がある。

・制御システムのセキュリティレベルは情報システムと比べて5～10年は遅れているが、このようなセキュリティへの考え方の差があると考えられる。

2.1.2 わが国IPAの指摘する制御システムと情報システムの差異

以上のような分析に従って、制御システムと情報システムにおける情報セキュリティの考え方の違いについて、IPAは次の図表2.1を示している。

図表2-1　制御システムと情報システムにおける情報セキュリティの考え方の違い

	制御システム	情報システム
セキュリティ優先順位	A.I.C（可用性重視）	C.I.A（機密性重視）
セキュリティの対象	モノ（設備、製品） サービス（連続稼動）	情報
システム更新	10-20 年	3-5 年
稼働時間	24 時間 365 日連続	通常業務時間内
運用管理	現場技術部門	情報システム部門

*C（Confidentiality：:機密性）、I（Integrity：完全性）、A（Availability：可用性）

出典：脚注1より。

2.1.3 米国NISTの指摘する制御システムと情報システムの比較考察

一方、NISTが2009年10月に制御システムサイバーセキュリティワークショップに提出したプレゼンテーション[5]では、情報システムと制御システムのセキュリティ環境の違いを、図表2-2のようにまとめている。

図表2-2　情報技術VS.制御技術

	情報技術	制御技術
性能要求の違い	非リアルタイム	リアルタイム
	応答の信頼性	応答はタイムクリティカル
	高いスループットが要求される	相応のスループットでよい
	遅れや揺れが許容される	遅れや揺れは重大な問題
信頼性要求の違い	スケジュール化された運用	連続的運用
	時々の不具合に寛容	停止は致命的
	フィールドでのベータテスト可	完全なテストが期待される
リスク管理要求の違い デリバリ対セイフティ	データの統合性が絶対的必要	人間の安全性が絶対的必要
	リスクの影響はデータの喪失とビジネス運用の喪失	リスクの影響は人命、設備、製品の喪失と環境へのダメージ
	リブートによるリカバリが可能	フォールトトレランスが必須

出典：脚注5より

2.1.4　NISTの指摘する制御システムの脆弱性

さらに、NISTSP800-82では、制御システムの脆弱性について、①ポリシーと手続きに係

[5] Industrial Control System Security, NIST Industrial Control System Cyber Security Workshop, October 2009

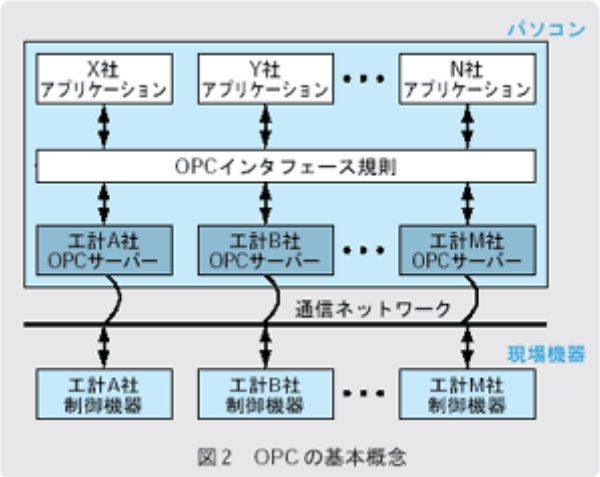
る脆弱性、②プラットフォームの脆弱性、③ネットワークの脆弱性の３点にわたって、以下のような詳細な分類を行っている。やや詳細にわたるが、制御システムの脆弱性の全貌を示す記述として以下に約出・引用する。

①ポリシーと手続きに係る脆弱性
a) 制御システムについての不適切なセキュリティポリシー
b) 制御システムセキュリティについての訓練と告知の不在
c) 不適切なセキュリティアーキテクチャと設計
d) 制御システムのセキュリティ用に開発されたセキュリティ手続き書が存在しないこと
e) 制御システム装置の実施ガイドラインの不在または不十分
f) セキュリティ強化の組織的メカニズムの欠如
g) 制御システムについてのオーディットの不在
h) 制御システム独自の運用継続・災害復旧計画がないこと
i) 制御システム独自の配置変更マネジメントの欠如

②プラットフォームの脆弱性
a) プラットフォーム配置の脆弱性
・セキュリティ脆弱性が発見されてから時間が経たないとOSとベンダーのソフトウェアパッチが開発されないこと。
・OSとアプリのセキュリティパッチがメンテされないこと
・OSとアプリのセキュリティパッチが消耗テストを経ないで実施されること
・デフォルトの配置が使用されること
・死活的に重要な配置がバックアップされていない
・ポータブルデバイスのデータが保護されていない
・適切なパスワードポリシーの欠如
・パスワードが使用されていない
・パスワードが公開されている
・推測されるパスワードの使用
・不適切なアクセスコントロールが用いられている
b) プラットフォームハードウェアの脆弱性
・セキュリティ変更の不適切な試験
・重要システムの不適切な物理的防護
・権限を持たない人物の装置への物理的アクセス
・制御システムコンポーネントへの安全ではないリモートアクセス
・ネットワーク間をつなぐデュアル・ネットワークインタフェイスカード(NIC)
・書面に乗っていないアセット

・無線電磁パルス（EMP）
・バックアップ電力の欠如
・環境制御の喪失
・重要コンポーネントの多重性欠如
c）プラットフォームソフトウェアの脆弱性
・バッファのオーバーフロー
・インストールされたセキュリティ能力がデフォルトで無効化されている
・サービス拒否攻撃（DoS）
・未定義、不完全定義、あるいは非合法条件の取扱いミス
・リモートプロシデュアコール(RPC)と分散コンポーネントオブジェクトモデル上のプロセス制御のOLE（OPC）（OPCについては図表2-3参照）
・産業全体に広がった不安全な制御システムプロトコルの使用
・平文の使用
・不必要なサービスの運用
・会議や定期刊行物で論じられた知的財産の使用
・コンフィギュレーションとプログラミングソフトウェアへの不適切な権限付与とアクセス
・侵入検出と防止ソフトウェアがインストールされていない
・ログが取られていない
・インシデントが検出されない

図表2-3　OPCの基本概念



出典：MS技研社ホームページ[6]

[6] http://www.m-system.co.jp/mstoday/plan/mame/b_network/9710/index.html

d）プラットフォームマルウェア防護の脆弱性
・マルウェア防護ソフトウェアがインストールされていない
・マルウェア防護ソフトウェアもしくはその定義が現行のものではない
・マルウェア防護ソフトウェアに消耗試験がなされていない

③ネットワークの脆弱性
a）ネットワーク配置の脆弱性
・弱体なネットワークセキュリティアーキテクチャ
・データフロー制御が行われていない
・セキュリティ装置がうまく配置されていない
・ネットワークデバイス配置の在庫やバックアップがない
・トランジット中のパスワードに暗号化されていない
・ネットワークデバイス中にパスワードが無限に存在する
・不適切なアクセスコントロールが適用されている
b）ネットワークハードウェアの脆弱性
・ネットワーク装置の不適切な物理的防護
・不安全な物理ポート
・環境制御の喪失
・重要ではない人物が装置とネットワーク結合にアクセスを持っている
・重要ネットワークの多重性欠如
c）ネットワーク周辺の脆弱性
・セキュリティ周辺の未定義
・ファイアウォールの不在または不適切な配置
・無コントロールトラフィックに使われるコントロールネットワーク
・コントロールネットワーク外で用いられるコントロールネットワーク
d)ネットワークモニタリングとロッギングの脆弱性
・不適切なファイアウォールとルータのログ
・制御システムネットワークへのセキュリティモニタリングなし
e）通信の脆弱性
・重要なモニタリングとコントロールパスが特定されていない
・標準的でよく書面化された通信プロトコルが平文テキストで用いられている
・ユーザ、データ、デバイスの権限付与が不十分か存在しない
・通信への統合的チェックの欠如
f）無線通信の脆弱性
・クライアントとアクセスポイントの間の不適切な権限付与
・クライアントとアクセスポイントの間の不適切なデータ防護

2.1.5　NISTの指摘する制御システムのリスクファクター

NISTSP800-82は、制御システムのリスクファクターとして次の４点を挙げている。

①標準化されたプロトコルと技術の採用、

②汎用プロトコルによる接続の増加、

③安全でない虚偽的な接続、

④インターネットを介した公共的接続。

これらのリスクファクターについては、2.1.1 で述べたIPAによる制御システムの脆弱性分析と重複するので、ここでは詳述しないこととする。

2.2 制御システムのオープン化に伴うと見られる最近のセキュリティインシデント事案

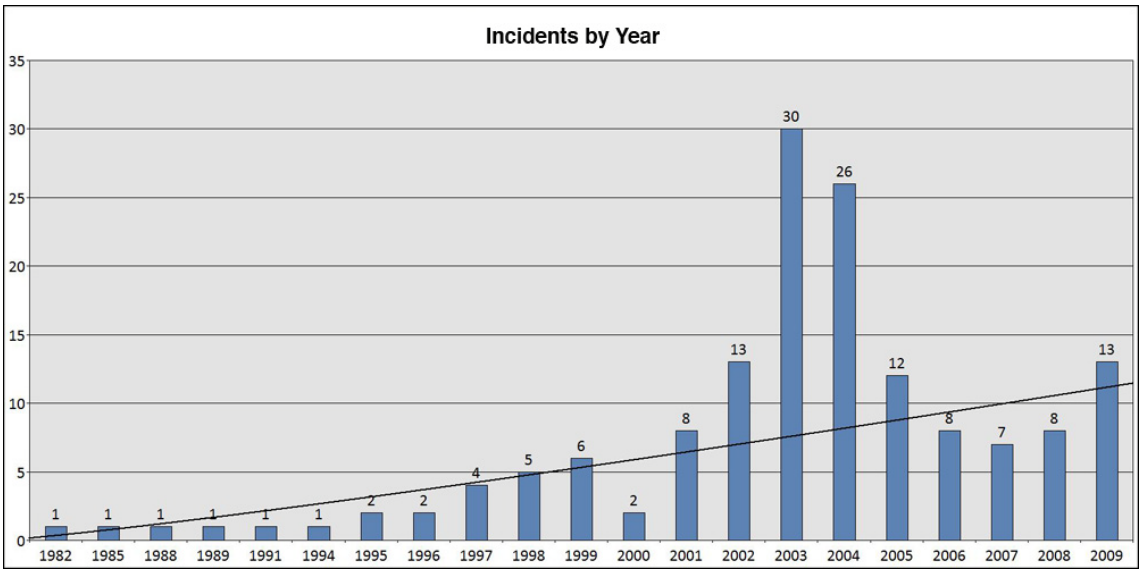
2.2.1 RISIデータベースによるセキュリティインシデントの近年の動向

2001に設立されたIndustrial Security Incidents Databaseを前身とする ”Repository of Industrial Security Incidents (RISI)”[7]は、「プロセス制御、産業自動化、SCADAに関係するサイバーセキュリティ関連インシデントのデータベース」(RISIホームページより)であり、米国を本拠とした非営利団体である。会員は重要インフラ関連民間企業、制御システムのベンダ、業界団体などであり、わが国からはJPCERT/CCと横河電気が会員となっている。

RISIのデータベースには、1992年以来の180件を越すインシデントが収録されているが、下の図表2-4が示すように近年インシデント数は増加する傾向にある。なお、下図には加えられていないが、2010年に報告されたインシデント数は10件である（2011年３月末時点)。以下、主にRISIのインシデントデータベースに基づいて、欧米における最近のインシデント事例を紹介する。

[7] Repository of Industrial Security Incidents (RISI)
http://www.securityincidents.net/index.asp

図表2.4 RISIデータベースによる近年のインシデント事例数の動向



出典：RISIホームページ

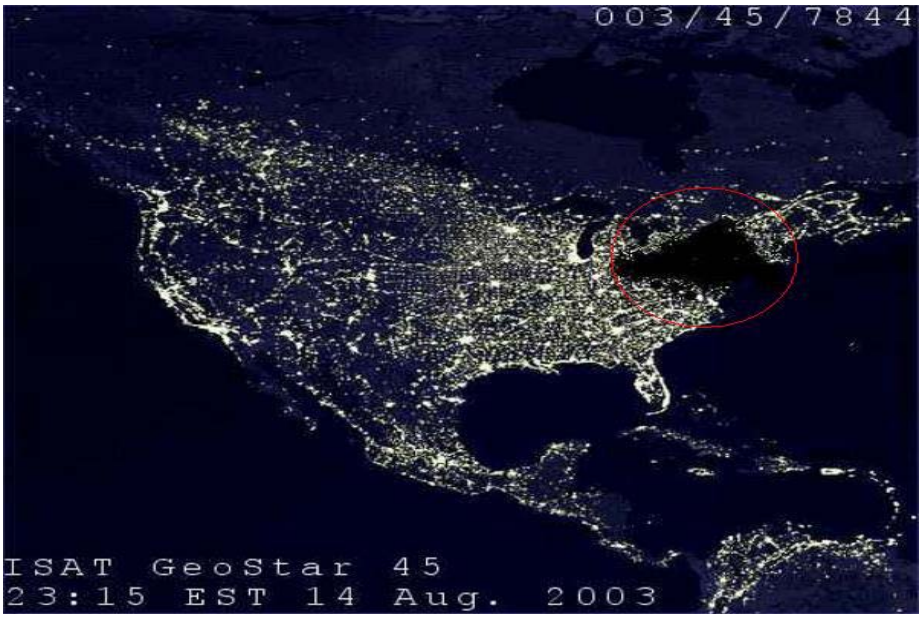
2.2.2 制御システムに係る近年のインシデント事例（米国）

① 米国東海岸の大停電（2003年8月）

米東部時間14日午後４時（日本時間15日午前５時）ごろ、米東海岸、五大湖周辺の一部、カナダに及ぶ広範囲で大規模停電が発生した。停電は数10都市に及び、約5000万人に影響する米史上最大の停電になった。マンハッタン中心部の電力回復は予想より大幅に遅れて、15日早朝（日本時間同夜）となった。

停電が始まったファーストエネルギー社の電力管理システム（EMS）ベンダーは、GEハリス社のXM21システムであったが、このシステムのアラーム処理アプリケーションの不具合がインシデントんほ引き金になったとされている。このインシデントの背後にサイバー攻撃者の存在が疑われ、米国における制御システムのセキュリティが課題としてフォーカスされる契機となった事件であった。

図表　　米国東海岸の大停電の衛星写真（赤枠が停電エリア）



http://www.teamrenzan.com/archives/writer/omnibus/web_larva.html

②トランスアラスカ・パイプライン漏洩（2010年5月25日）

トランスアラスカ・パイプラインから約5000バレルが漏洩。長さ800マイルのパイプラインからの３番目に大量の漏洩となった。アリエスカ・パイプライン・サービス社は、デルタジャンクション近傍の第９ポンプステーションで漏洩を発見してから３日間に渡ってパイプラインを閉鎖した。ポンプステーションが停止したとき、アリエスカ社はそのコマンドシステムの試験を行っていた。電力は電力グリッドからバッテリーシステムに切り替えられた。パイプラインは内部からの増大する圧力を防止するバルブを開放した。バルブが開き石油が部分的に満たされていたタンクに流出した。バッテリーシステム内の一制御回路が開放バルブの閉鎖に失敗し、石油がタンクを満たし、次いで二次封じ込めエリアに流出した。二次封じ込めエリアは非透過性ライナーを備えていたので、このエリアから流出した石油はなかった。パイプラインは2010年５月28日に再開した。パイプラインの閉鎖時間は79時間であった。損害は1日4500万ドルのノーススロープ石油生産と1300万ドルの州税収入であった。石油除去と操業再開のために125人の人員を現場に必要とした。

③ワシントンDCの地下鉄事故（2009年6月22日）

コンピュータ化されたシステムが自動モードで運転されていた列車を停止させることに失敗した。非常ブレーキが掛けられたが列車は停止しなかった。二つの地下鉄が衝突した。列車は1200フィート以内に接近しないはずであった。安全への懸念から、連邦政府は古くなった列車群を退役させようとしたが、新しい列車を購入する資金がないために、交通当局は古い列車を走らせ続けた。国家運輸委員会は、衝突にも生き残れるように古い列車を

置きかえるか改装することを望んだが、両方とも行われなかった。列車の衝突で9人が死亡、80人が負傷した。

④ジョージア州ハッチ原子力発電所の停止（2008年3月7日）

コントラクタがプラントのビジネスネットワークコンピュータのソフトウェアをアップデートした後に、ハッチ原子力発電プラントが48時間に渡って閉鎖された。そのコンピュータは、プラントの主要制御システムの一つからの化学及び診断データの監視に使われていた。アップデートされたソフトウェアは双方のシステムを同期するために設計されていた。アップデートされたコンピュータがリブートされたとき、それは制御システムのデータをリセットした。制御システムはデータの欠如が燃料棒冷却水の水位の低下であると解釈された。その結果、安全システムが原子炉のシャットダウンを命じた。ソフトウェアのエンジニアは制御システムが同期されることも、リブートが制御システムをリセットすることも知らなかった。発電所は48時間閉鎖された。事故対応として、影響されたサーバ間のすべてのネットワークコネクションが除去された。

⑤オーロラ発電機試験の実施

このケースはインシデント事例とは性格が違い、制御システムへのハッカー攻撃の可能性を実証するための試験であった。

2007年3月、DHSはアイダホ国立研究所において、電力ネットワークへのサイバー攻撃の可能性を検証するAurora Generator Testを行った。このシミュレーション実験の結果、SCADAシステムに深刻な脆弱性が発見され、一基100ドルのディーゼル発電機は激しく振動して動作を停止するに至った。この実験で、ハッカーが発電所の制御システムへのリモートアクセスを獲得して、発電機を破壊できることが証明された。ハッカーが発電機を破壊できることを実証する試験の模様はビデオで撮影され、広く公開されている[8]。

2.2.3 制御システムに係る近年の事例（欧州）

①ロンドン地下鉄の誤進路への侵入（2010年9月8日）

ラッシュアワー中にロンドンの地下鉄が他の列車の線路に送られた。ロンドン交通局は「信号の不規則性」が、西行き列車をプライストウ駅の他の列車に向かう東行き線路に乗せることになったといった。交通局の幹部は「このような信号の間違いは大事故を引き起こす可能性を有している」と語った。駅を離れて間もなく、運転手は間違った方向に進んでいることに気づき、急ブレーキを掛けた。事故調査が行われている間、交通は約６時間に渡って中断した。プライストウ駅の信号装置に故障が発見された。

[8] http://www.militaryphotos.net/forums/showthread.php?121081-AURORA-test-validated-fears-of-Dept.-of-Homeland-Security

②エアフランス447便の大西洋での墜落（2009年6月１日）

エアフランス447便が大西洋に墜落した。ブラックボックスは発見されなかったが、物理的な証拠と送信された自動メンテナンスメッセージの情報に基づけば、風速センサーから始まったシステムの不具合のカスケードが、コンピュータの停止にまで及んだと信じられている。リオデジャネイロからパリに向かうエアバスA330は、嵐の中で大西洋に墜落した。全乗客228名が死亡した。

③ダブリン港トンネルの閉鎖（2008年2月27日）

ダブリン・ポート・トンネルで、自動車の高さ検出システム、消火メカニズム、クローズドサーキットテレビシステム、及び緊急照明に責任のあるSCADA安全システムが崩壊して、交通はカオス状態になった。国家道路局(NRA)は、SCADA安全システムの「耐久性と信頼性」に「重大な懸念」を表明した。NRAのスポークスマンはこのトンネル閉鎖を「緊急事態」であると表現した。不具合による閉鎖を避けるために、このシステムは「一個一個」置き換えるか修理されるだろうと付け加えた。

2.2.4 制御システムに係る近年の事例（わが国）

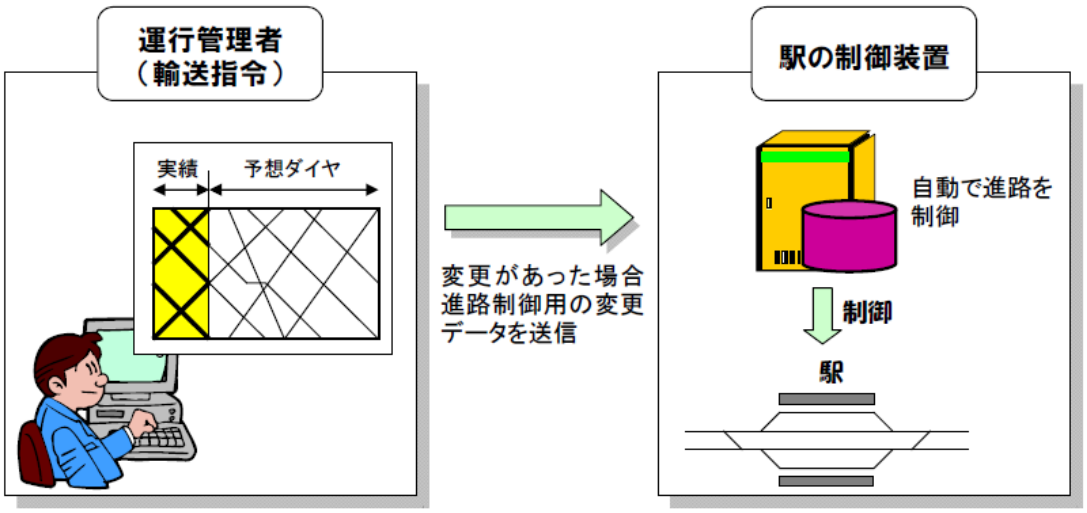
①JR東日本新幹線の全線停止（2011年１月17日）

東北、上越などJR東日本管内の新幹線が1時間強にわたりすべて運転停止となった。データ修正数がシステムの限度値を超えたため、輸送指令を行う運行管理者がダイヤの変更入力を行う端末画面の表示が消え、全列車を止める対応が取られた。

全新幹線の停止に至ったきっかけは、東北新幹線新白河駅と福島駅でポイントが転換できない異常が発生したためで、運行管理者は24本の列車を駅間に止めないようにするダイヤ変更入力を行った。新幹線運行管理システム「COSMOS」は、変更入力を行うと、その後のダイヤにデータ修正が必要な個所を表示する仕組みになっている。運行管理者がこれらを一つ一つ変更する入力作業をしているうち、データ修正数が必要な個所がシステムの限度を超えてしまったのであった。システムは1分ごとにデータ修正が必要な個所をチェックするが、600件を超すと予想ダイヤを表示できないようになっていた。

JR東日本は今後の対策として、以下の2点を発表した。(1)データ修正が必要な箇所が多く生じる入力を連続して行う場合、修正箇所を解消してから新たな入力を行う。(2)データ修正が必要な箇所が600 件を超えても、予想ダイヤを表示できるようにプログラムを改修することを検討する。

図表2-5　JR東日本新幹線運行システム「COSMOS」の概要



出典　JR東日本記者発表　2011年1月18日
http://www.jreast.co.jp/press/2010/20110106.pdf

②みずほ銀行のシステム障害（2002年4月、2011年3月）

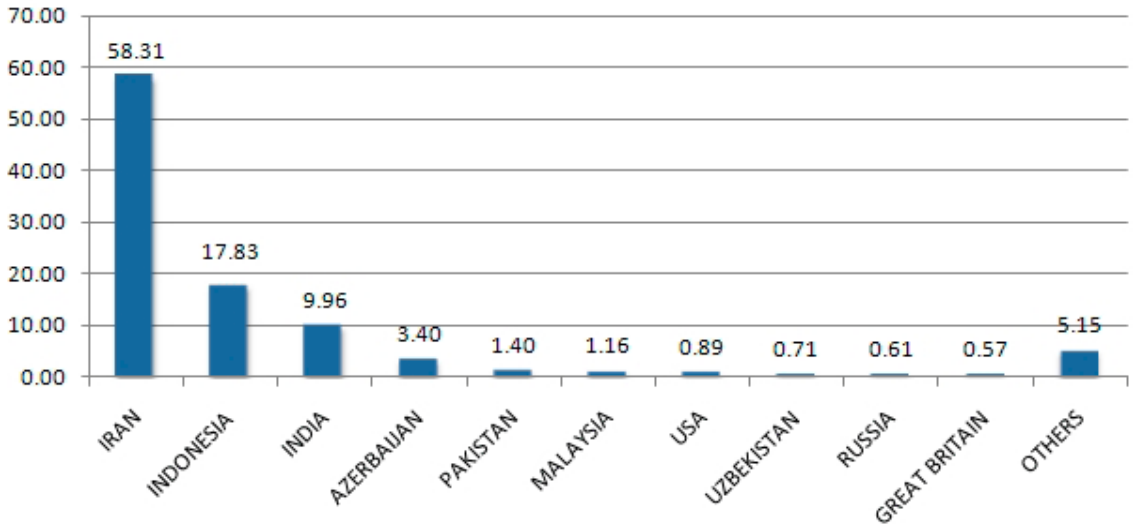
2002年4月、第一勧業銀行、富士銀行、日本興業銀行が合併してみずほ銀行となったが、4月1日の合併当日から、コンピュータの不具合から大規模なシステム障害が発生した。障害はATM系と口座振替系の双方に及び、最終的に収束するまでATM系で約10日間、口座振替系約１月間混乱が継続した。同年6月19日に記者会見を行ったみずほホールディングスの前田晃伸社長は、トラブルの原因を「プログラムやJCL（ジョブ制御言語）の不具合，入力データの不備などが重なって起こったもの」と説明し、その背景を。「テストやリハーサルなどの事前準備が不十分だった。統合プロジェクトの管理体制に問題があり，進ちょく状況を正しく認識できなかった。大規模なトラブルが発生したときのコンテンジェンシー・プランもなかったので，復旧に手間取った」と語った。
http://itpro.nikkeibp.co.jp/free/NC/NEWS/20020619/1/

また、同行は2011年3月の東日本大震災に際しても再び大規模なシステム障害を起こし、振込取引、送金処理が大幅に遅延し、店舗外ATMの閉鎖などが1週間以上にわたって継続した。大震災に際しての義援金振込の集中などが原因ではないかと見られているが、2011年3月末現在、その原因究明について本格的な発表はなされていない。
http://www.toyokeizai.net/business/strategy/detail/AC/5cd01c05cd9819b64569b21fd977221f/

2.2.5 Stuxnetの事例

2010年6月、ベラルーシのアンチウィル会社がウィンドウズ上で動作する新種のマルウェアを発見した。同年7月には、Verisign, Siemens, Microsoftなど、このウィルスに関連する各社から相次いで情報提供やセキュリティパッチの提供が公表され、Stuxnetの名前が世界に知られることになった。そして、2010年11月にシマンテック社がこのマルウェアに関する詳細なリポート[9]を刊行し、Stuxnetのメカニズムの大要が解明された。同社のリポートによれば、2010年9月29日時点で、Stuxnetは世界中で約10万のホストコンピュータに感染しており、その国別分布は下の図表2-5のようになっている。

図表 2-5　Stuxnet の国別感染ホスト分布



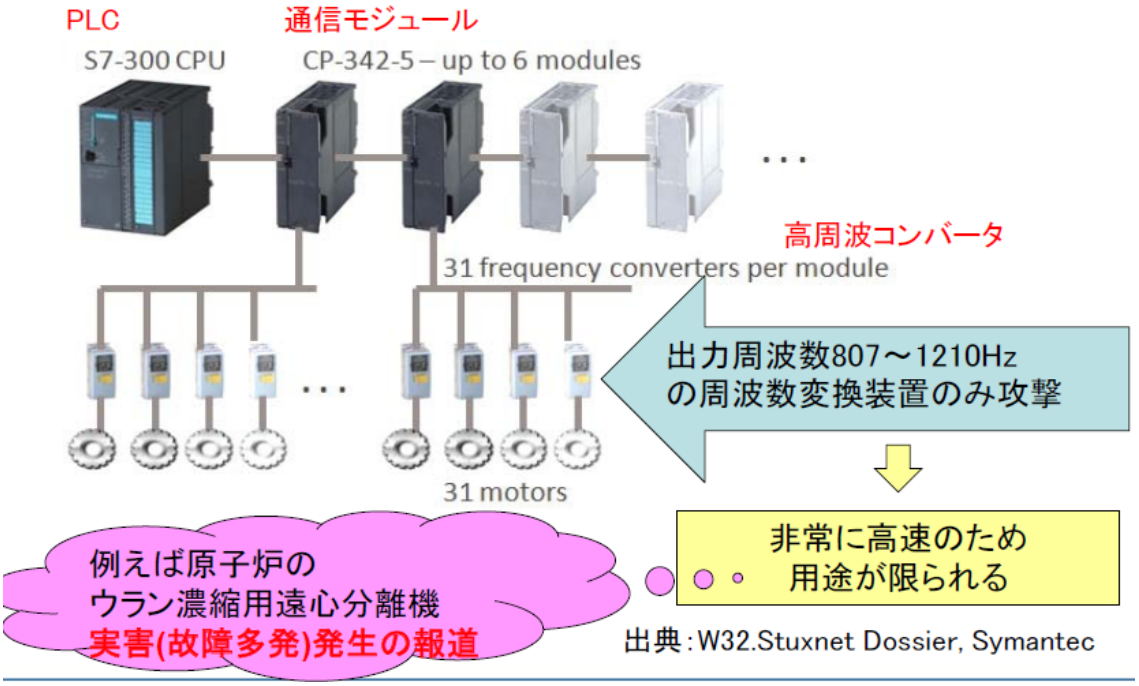
出典：脚注9

シマンテックの調査によれば、Stuxnetの攻撃は4つの段階から成っている。①ゼロデイ脆弱性（未知の脆弱性）を利用してウィンドウズOSに感染し、②ウィンドウズのネットワーク共有やUSBメモリなどを利用してウィンドウズ上で動作するSiemens社製のSCADA制御ソフトウェア、PCS7, WINCC Step7に感染し、③同ソフトウェアが制御するSiemens社製S7PLCをStuxnetが乗っ取り、④特定のベンダの特殊な周波数変換ドライブ（動作周波数807Hz～1210Hz）があるPLCを制御して本来の動作とは異なったプロセスを実行させる。

上に示した第４段階におけるStuxnetの動作メカニズムを、シマンテックの報告書は下の図表2-5のように示している。

9 W32.StuxnetDossier
http://www.symantec.com/connect/blogs/w32stuxnet-dossier

図表2-5　標的となった周波数変換ドライブへの攻撃の概要



出典：　脚注 9

Stuxnetの狙いは、イランの原子力開発施設（ナタンズプラント）のウラン濃縮用遠心分離機の破壊だったと見られている。攻撃の巧妙さと精緻さから、イスラエルなどの国家機関の関与も疑われており、制御システムのセキュリティに大きな問題提起をした事件であった。

米国のシンクタンクISISの2010年12月のリポート[10]は、ナタンズ原子力プラントの約1000機（全体の10%）の遠心分離機が2010年6月頃までに破壊されたと推測している。Stuxnetの攻撃は、「恐らく過剰な振動と歪みを与えて遠心分離機を破壊するために、モーターの回転スピードを、最初は上げ、次に下げるように設計されたように見える。もしその目的が、速やかに全遠心分離機を破壊することであるなら、Stuxnetは失敗した。しかし、もしその目的がウィルスの検出を難しくして、一部の遠心分離機を破壊し、イランの核開発計画を遅らせることであるなら、それは部分的に成功したといえるだろう」と述べている。

10 “Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? “ http://www.isis-online.org/uploads/isis-reports/documents/stuxnet_FEP_22Dec2010.pdf

2.3 新しいタイプの攻撃（Stuxnet）が示した重要インフラセキュリティの将来予測

2.3.1 IPAの考察

わが国のIPAはStuxnet攻撃を受けて、「『新しいタイプの攻撃』に関するリポート」[11]を2010年12月に発表した。海外でAPT(Advanced Persistent Threats)と呼ばれているStuxnetタイプの攻撃を、このIPAリポートは『新しいタイプの攻撃』と表現し、その特性を、システムへの潜入を狙った「共通攻撃手法」と、情報窃取等の目標に応じた「個別攻撃手法」を結合した新しいサイバー攻撃と定義している。

・共通攻撃手法

① インターネットやUSBメモリを通じた情報システムへのウィルス感染

② システムの脆弱性を利用することによる情報システム環境内部でウィルスの拡散

③ バックドアを作成し、外部の指令サーバ(C&Cサーバ)と通信することにより、ウィルスの増強や新たなウィルスのダウンロードの実行

※ウィルスの増強やダウンロードは以降④⑤の手順でも実行される可能性あり。

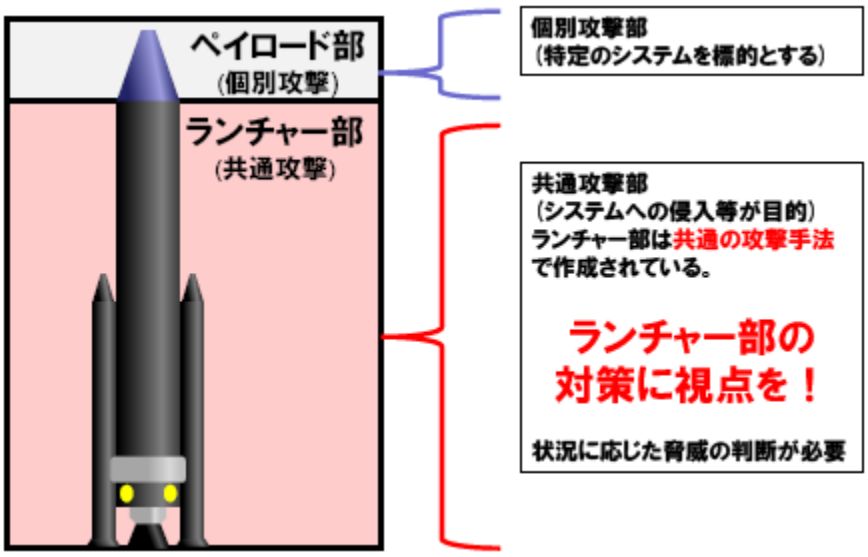
・個別攻撃手法

④ 原子力システム等を制御する装置が配備してある、制御システムへの侵入

⑤ 制御システム上にある装置に対する攻撃の実行

上に記した「新しいタイプの攻撃」の概念を、IPAは下の図表2-6のように図示している。

図表2-6



出典：脚注11

11 IPA「『新しいタイプの攻撃』に関するリポート」 2010年12月

2.3.2 JPCERT/CCの考察

また、JPCERT/CCは、2011年2月に発表したプレゼンテーション[12]で、Stuxnetを「制御システムを狙った初のマルウェア」と定義して、Stuxnetが打ち砕いた（制御システムに係る）「安全神話」を以下の５点だとして列挙している。

①制御システムはサイバー攻撃と無縁だ。
②制御システムをインターネットと切り離しておけば100%安全だ。
③特殊なシステム構成だから外部にいる攻撃者に分かるはずがない。
④新品のUSBメモリだけ使っていれば安全だ
⑤マルウェアに感染するとコンピュータ自体の動きが異常になる(制御システムは異常停止しない限り，稼働させ続ければよい)。

以上のような制御システムのセキュリティ課題に対して、ベンダやユーザがいかに対処すべきかを、Stuxnetの教訓としてJPCERT/CCは下の図表2-7のように示している。

図表2-7　JPCERT/CCが示すStuxnetの教訓

Stuxnetにおける事実	Stuxnetに耐えるために求められるもの
脆弱性を衝いて侵入された	・脆弱性を作り込まない**技術力** ・事前に脆弱性を除去しておく**組織力** ・部分的に多少の脆弱性があっても耐えられる(多層防御)ようにシステムを構成しておく**技術力**
開発者は標的の制御システムを知り尽くしていたと見られる	・システム構成に関する情報が攻撃者に知られても耐えられる防衛ラインを作り込む**技術力**
特定の環境でのみ攻撃動作	・異常を検知する**眼力(人)**
異常をHMIで表示されないよう隠蔽	・制御システムの異常も疑ってみて総合的に判断する**眼力(人)**
今でもStuxnetを知らない制御システム運用者も少なくない	・**情報収集**のための**組織力**
ゼロデイ脆弱性が悪用されているので，普通の復旧では再び侵入される	・すみやかなシステム**復旧**と業務継続のための戦略

出典：　脚注12

12 Stuxnet－制御システムを狙った初のマルウエアー　JPCERT/CC 2011 年 2 月

3. 制御システムのオープン化が重要インフラの情報セキュリティに与える影響の考察

3.1　米国の制御システムのセキュリティ対策

3.1.1.脆弱性関連情報のデータベース

情報システムにおける脆弱性や脅威に関する情報は、世界規模でCERT/CCに集約され、各国のCERTに配信されることになっている。米国ではUS-CERT[13]が国内向けに情報の提供を行っている。制御システム関連の脆弱性については、US-CERTの下にICS-CERT[14]が置かれ制御システム関連の脅威や脆弱性に関する情報提供を行っている。

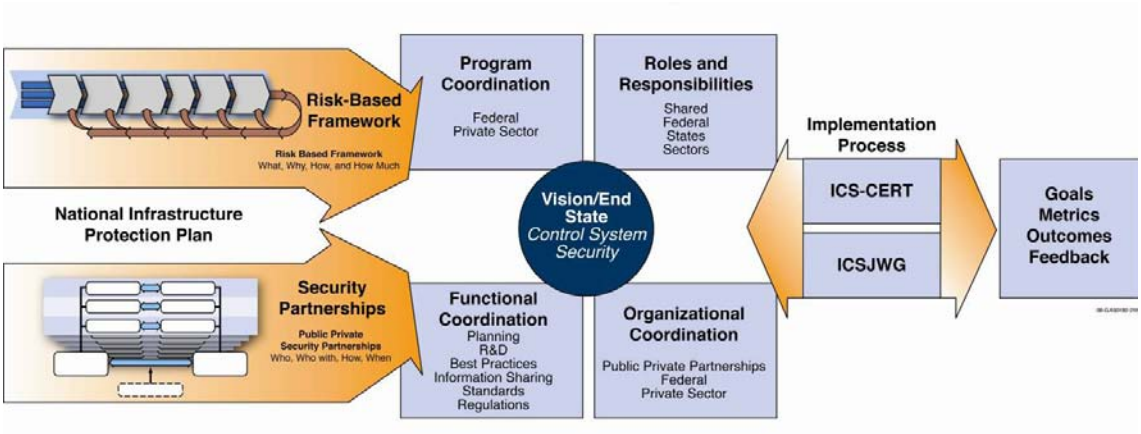
また、民間ベースでは2.2で紹介したRISIが、重要インフラに特化したインシデント情報の収集と共有に当たっている。

3.1.2　国土安全保障省における取組み

米国において重要インフラのセキュリティに対応する主力官庁が、全 18 分野の重要インフラ・キー資源セクター（CIKRS）のうち 11 分野の重要インフラを担当する国土安全保障省（DHS）である。DHS は国家サイバーセキュリティ局によってサイバーセキュリティ全般を管轄しているが､その下に制御システムのセキュリティを担当する CSSP(Control Systems Security Program) を運用している。

DHSが 2009 年 10 月に公刊した「制御システムの安全戦略」[15]は、制御システムセキュリティに係る官・産の協調体制を以下のようにイメージ化している。

図表 3.1　アメリカにおける制御システムセキュリティの協調体制



出典：　脚注 15

13 http://www.us-cert.gov/index.html
14 http://www.us-cert.gov/control_systems/ics-cert/
15 “Strategy for securing control systems,” homeland security October 2009 http://www.us-cert.gov/control_systems/pdf/Strategy%20for%20Securing%20Control%20Systems.pdf

上の図が示すように、CSSP は、US-CERT と ICSJWG(ICS Joint Working Group)を通じて、制御システムセキュリティの情報共有と戦略立案を推進している。ICSJWG には６つのサブグループが置かれ日常的な活動を行っている。

①情報共有サブグループ
②国際協力サブグループ
③研究開発サブグループ
④安全な制御システムへのロードマップサブグループ
⑤ベンダサブグループ
⑥人材開発サブグループ

また、CSSP は、重要インフラの所有者・オペレータ・ベンダなどに対して、推奨プラクティス、標準・参照・ガイダンス、人材訓練なども提供している。

3.1.3　米国エネルギー省の SCADA テストベッド計画（NSTB）

DHSが中心となって実施されているCSSPのなかで、DoE（エネルギー省）やその下のOE（配電・エネルギー信頼性局）が中心となって取り組んでいるのが、NSTB[16](National SCADA Test Bed Program)である。NSTBは、①現存する脆弱性を特定し緩和する、②セキュリティ基準の開発促進、③SCADA装置と制御システムを試験する独立施設として奉仕、④サイバーセキュリティのベストプラクティスを特定し促進する、⑤エネルギーセクタ内での制御システムの認知の増加、⑥より安全で強固な先進的制御システムアーキテクチャと技術の開発、の６項目を目的として掲げている。

NSTB はエネルギー省傘下のアイダホとサンディアの二つの国立研究所などで、実運用に近い環境下で脆弱性評価検証試験が行える実験施設を提供している。このような実験費用の半分は、国が負担することとなっている。すでに、このテストベッドで、2-ABB Nrtwork Manager ,GE XA/21, Siemens, Telvebt などの有力ベンダやセキュリティベンダの製品が検証を受けている。

3.1.4 制御システムのセキュリティ技術開発ロードマップ

脆弱性評価の他にNSTBが中心となり、DHSや電力・エネルギー業界のサポートを得て行われているのが、エネルギー分野の制御システムにおけるセキュリティロードマップの作成である。”Roadmap to Secure Control System”の第１版は 2006 年に作成されたが、5 年後の 2011 年に”Roadmap to Secure Energy Control System”として改訂されている[17]（2011

---

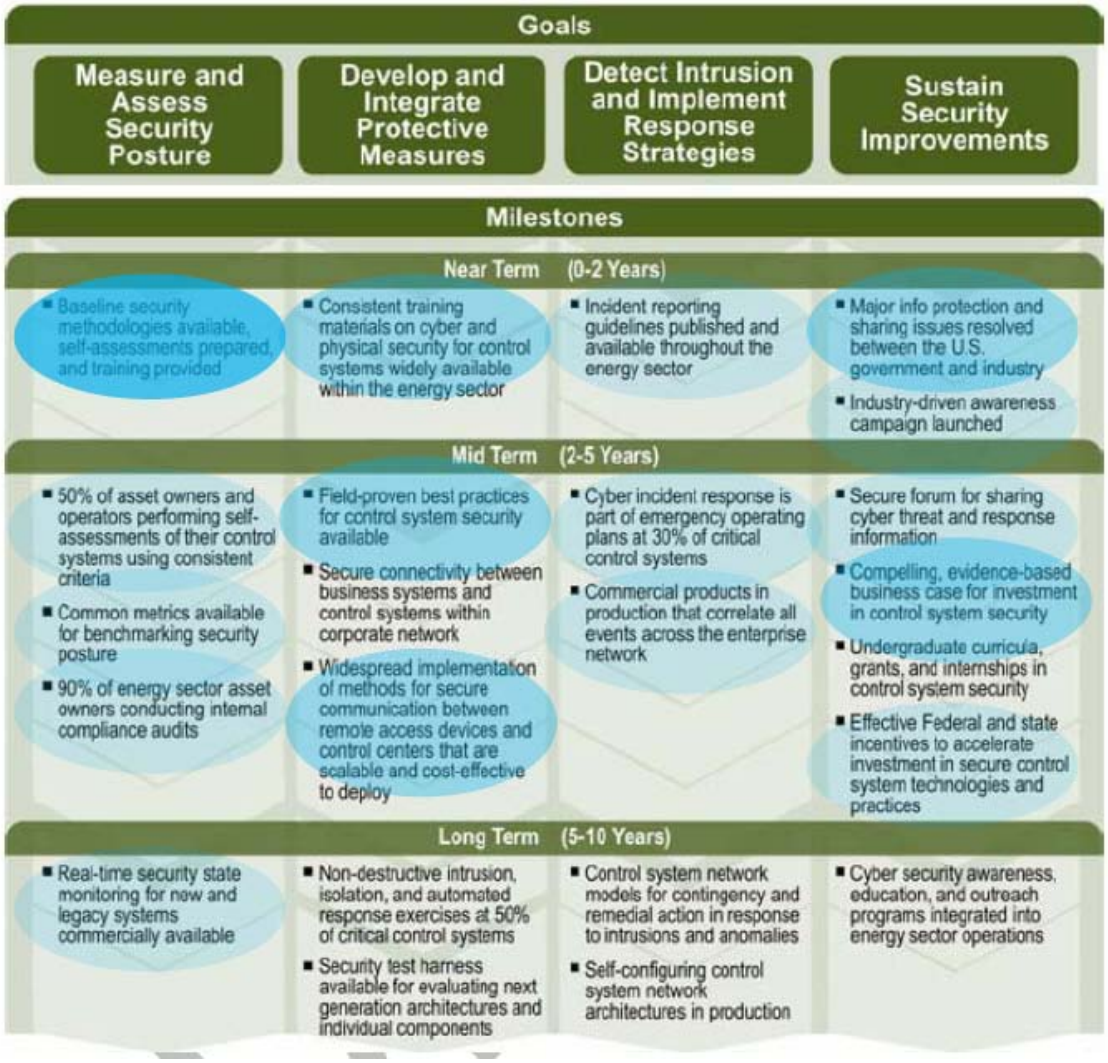
[16] National SCADA Test Bed Program
http://www.oe.energy.gov/nstb.htm

[17] “Roadmap to Secure Energy Control System,” Energy Sector Control System Working Group, Jan. 2011
http://www.controlsystemsroadmap.net/pdfs/2011_roadmap_draft.pdf

年１月にドラフトが公表された)。

このロードマップにおいては、①セキュリティ態勢の測定と評価、②防護手段の開発と統合、③侵入検出と対応戦略の実施、④セキュリティ改善の維持という４分野について、短期（2 年以内)、中期（2-5 年)、長期（5-10 年）の三つの期間に分けて、達成すべき目標が明示されている。図表 3-2 に最新のロードマップの概要を示す。

図表 3-2　Roadmap to Secure Energy Control System



出典：脚注 17

3.1.5 I3P の制御システム関連プロジェクト

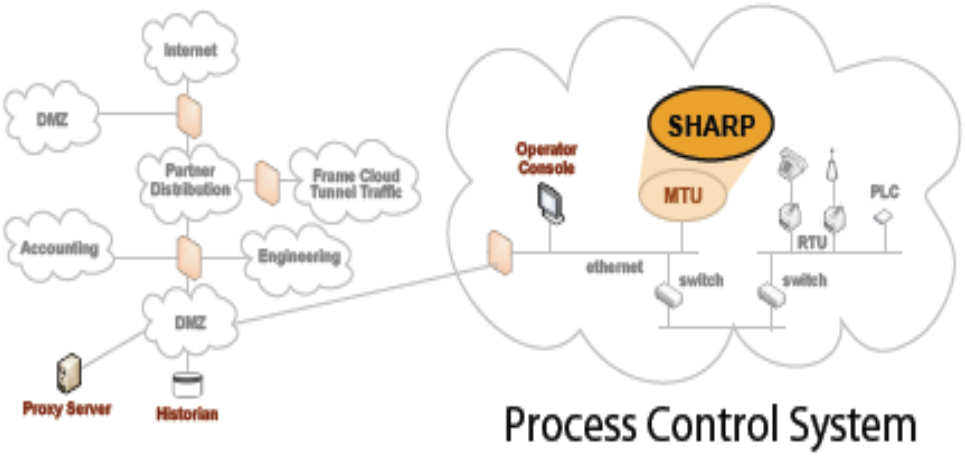
I3P(Institute for Information Infrastructure Protection)[18]は、大学、国立研究所な

[18] http://www.thei3p.org/about/

どをメンバーとして情報インフラ防護を目的として 2002 年に設立された非営利団体であり、政府資金によってセキュリティ関連の研究開発を実施している。主として情報セキュリティ系の研究を行っているが、制御システムについてもその研究対象としている。

I3Pが開発したセキュリティツールの一つに、SHARP[19]（Security-Hardened Attack Resistant Platform）がある。このツールは、現存する制御システムに対して、セキュリティの高いネットワーク環境を提供するツールである。図表 3-3 にSHARPの概念図を示す。

図表 3-3　SHARP の概念図



出典：　脚注 19

3.2　欧州の制御システムのセキュリティ対策

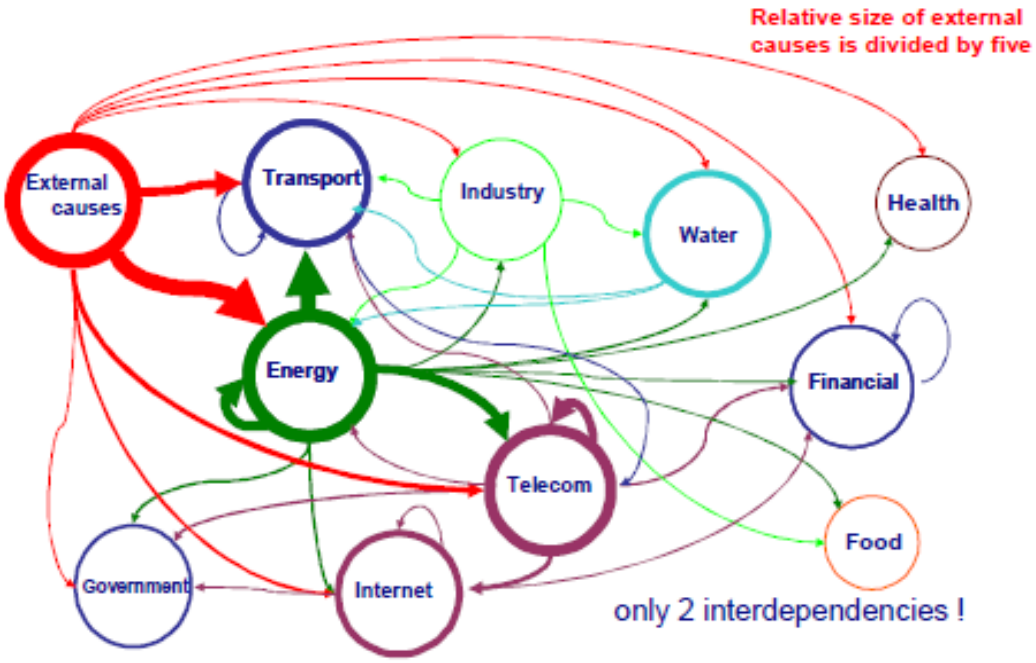
3.2.1 脆弱性関連情報のデータベース

欧州では、オランダのTNO（オランダ応用科学研究機構））がロッテルダムの統一産業・港湾消防局と共同で、FACTS（Failure and Accidents Technical Information System）[20]と称する産業事故の世界的データベースを長く運用してきた。このデータベースには、過去 90 年間に発生した約 24,000 件の産業事故が記録されている。FACTSデータベースはオンライン閲覧サービスを提供しているが、そのサービスは有料である。

FACTSのデータのうち、重要インフラ事故のデータベースは”Critical Infrastructure Disruption Database”と呼ばれ、2008年9月25日現在で164カ国、2,650件の事例、1090件のカスケード効果（重要インフラ事故の他の重要インフラへの連鎖的波及）が登録されている。TNOの防衛・セキュリティ・安全部門の発表した一論文[21]では、重要インフラ間のカスケード波及について下の図表3-4を掲げ、エネルギー分野（全体の64%）と情報通信分野（全体の24%）に、著しいカスケード効果が見られるとしている。

19 http://www.thei3p.org/docs/publications/factsheet-Sharp-2-26-08.pdf
20 http://www.factsonline.nl/tabid/173/Default.aspx
21 http://critis08.dia.uniroma3.it/pdf/CRITIS_08_40.pdf

図表3-4 ヨーロッパにおける重要インフラの実証的知見



出典： 脚注21

3.2.2 制御システムオープン化に関するEUの取組み（IPSCとENISA）

欧州連合（EU）では、欧州委員会傘下で二つの組織が制御システムのセキュリティに係る取組みを行っている。EU共同研究センター（JRC=Joint Research Center）の市民防護セキュリティ研究所（IPSC=Institute for Protection and Security for Citizens）[22]と、欧州ネットワーク情報セキュリティ庁（ENISA）である。

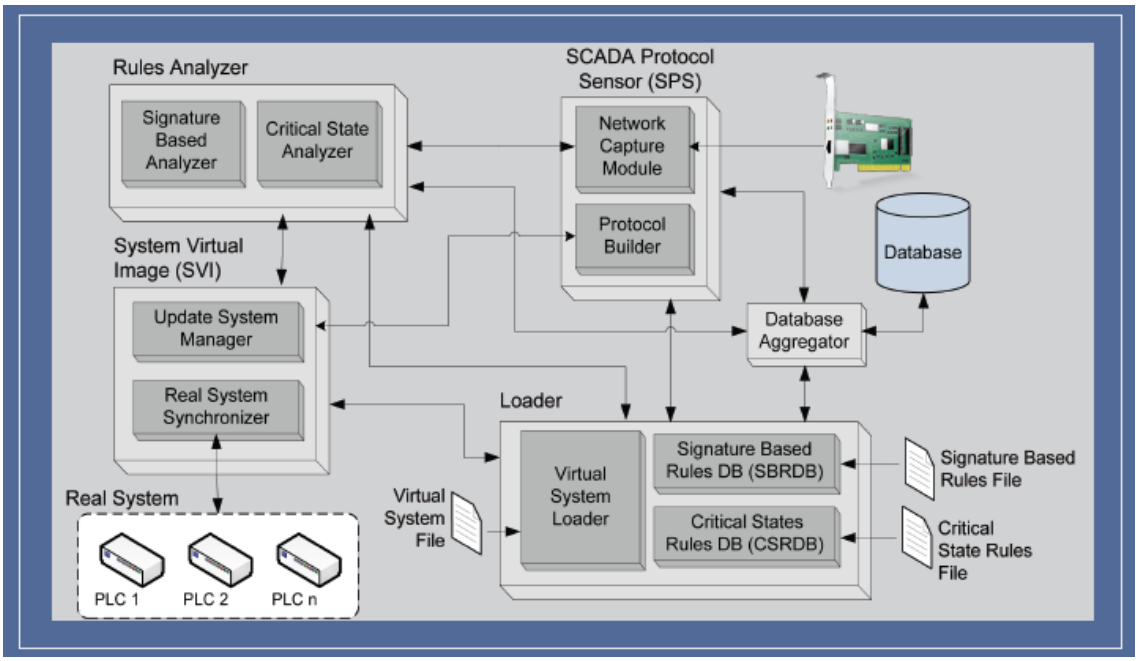
IPSCは2007年～2013年までのEU第7次フレームワークプログラム（FP7）に基づいて研究活動を行っているが、2011年段階ではその対象領域は、①グローバルセキュリティと危機管理、②海洋問題、③構造アセスメントのヨーロッパラボ、④セキュリティ技術アセスメント、⑤トレーサビリティと脆弱性アセスメント、⑥エコノメトリックスと応用統計の6つなっている。制御システムのセキュリティに関する研究は、このうち④セキュリティ技術アセスメントの一つ、CIP（Critical Infrastructures Protection）[23]として行われている。

CIPは重要インフラのセキュリティに係る幾つかの研究を行っているが、そのうちの一つにARCADEシステム[24]がある。ARCADEシステムはファイアウォール、侵入検出、危機状態モニ

22 http://ipsc.jrc.ec.europa.eu/
23 http://ipsc.jrc.ec.europa.eu/showaction.php?id=22
24 http://sta.jrc.ec.europa.eu/scni/pdf/arcade_web.pdf

ターを組み合わせたSCADAセキュリティシステムである。図表 3-5 にARCADEシステムの概要を示す。

図表 3-5 ARCADE システムの概要



出典：脚注 24

ENISA（European Network and Information Security Agency）は、EU におけるネットワークと情報セキュリティへの対応を行うための専門機関である。重要インフラを含むサイバーセキュリティについて加盟各国政府に助言や支援を提供する一方で、各国の CERT を支援している。ENISA は主として情報システムの側から制御システムのセキュリティ課題にアプローチしている。

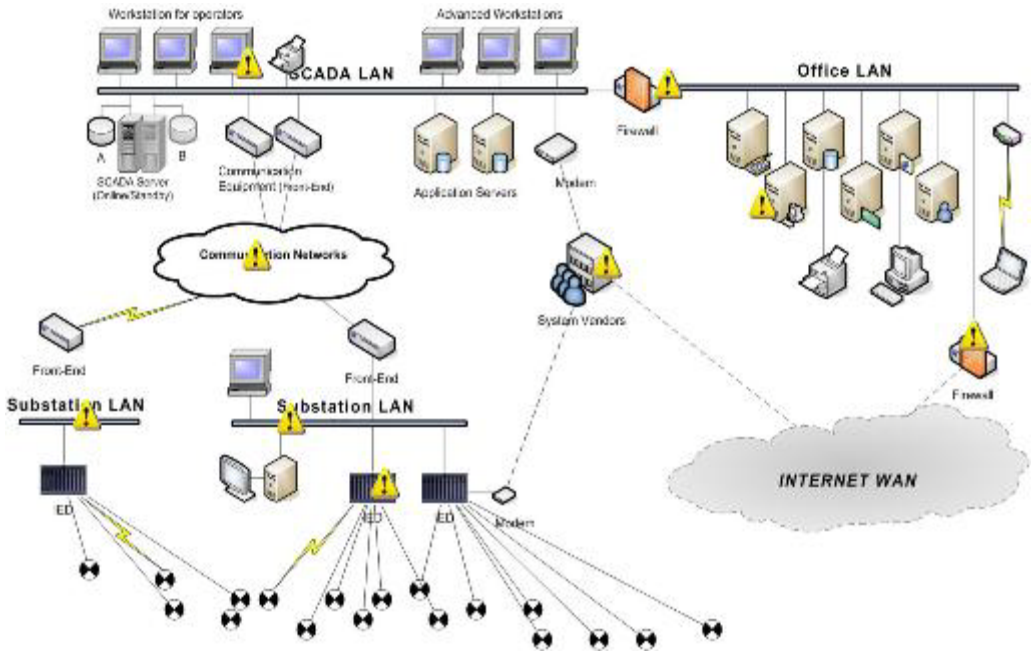
3.2.3 欧州における制御システムセキュリティ共同研究開発プロジェクト（VIKING）

欧州諸国は、EUの財政的支援の下に 2008 年 10 月VIKING（Vital Infrastructure, Networks, Information and Control Systems Management）[25]と略称する研究開発プロジェクトを立ち上げた。このプロジェクトには、５つの企業（ABB（ドイツのベンダ）、 E.ON（ドイツの電力会社）、 MML（スウェーデンの技術コンサルティング企業）、Astron Informatics（ハンガリーのSCADAシステム開発企業））と、三つの大学（ETH（スイス）と KTH（スウェーデン）、メリーランド（アメリカ））が参加し、主として電力関連のSCADAシステムのセキュリティに関して研究することとなっている。

[25] http://www.vikingproject.eu/new2/index.php

このプロジェクトは 2011 年 10 月末までの時限プロジェクトであり、最終報告書は 2012 年の１月に公表される予定となっている。VIKING プロジェクトの目的は以下の３つである。
①SCADA システムの脆弱性とその社会的コストの解明
②これらの脆弱性を緩和するための戦略と技術の提案・試験
③重要インフラとその防護の重要性の周知の向上。

図表 3-6　VIKING プロジェクトの研究対象の概略



出典：脚注 25

3.2.4 欧州各国の取組み

欧州各国はそれぞれ情報セキュリティに取組む国家機関を有している。英国の国家インフラ防護センター（CPNI=Center for the Protection of National Infrastructure）[26]、ドイツの情報セキュリティ庁（BSI=Bundesamt für Sicherheit in der Information stechnik）[27]などであるが、本報告書では詳細は省略する。

3.3　わが国の対策とその体制

3.3.1 情報セキュリティ戦略会議と NISC の取り組み

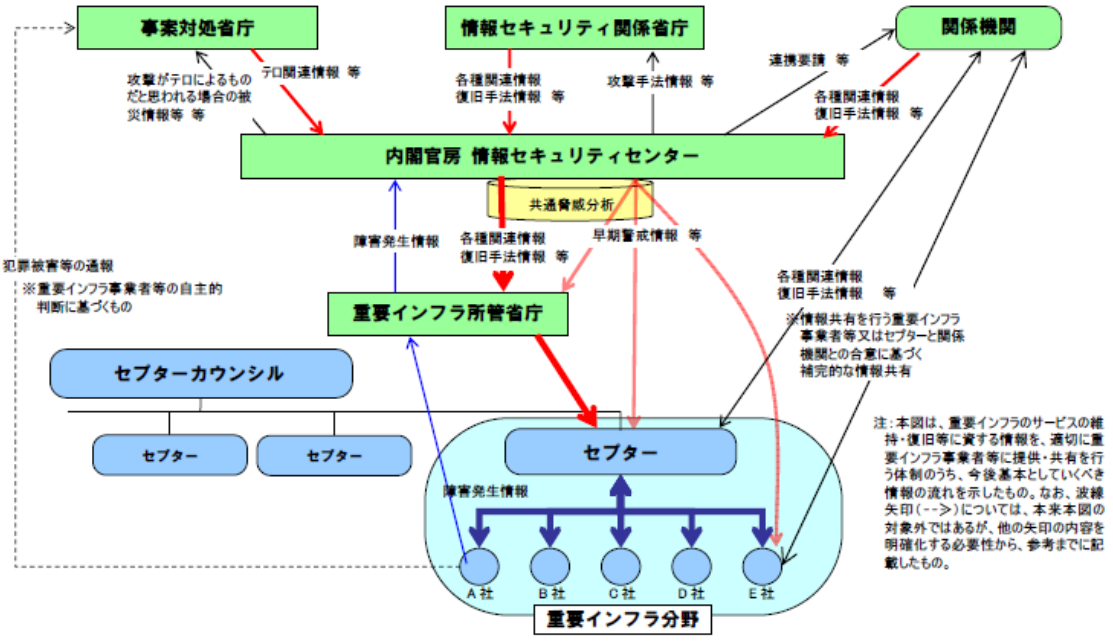
わが国の重要インフラセキュリティ対策に係る戦略組織は、平成17年に設置された情報セキュリティ政策会議であり、内閣官房情報セキュリティセンター（NISC）はその事務局

26 http://www.cpni.gov.uk/
27 https://www.bsi.bund.de/EN/TheBSI/thebsi_node.html

として関連施策の推進に当たっている。2006年には「第１次情報セキュリティ基本計画」が、2009年2月には「第2次情報セキュリティ基本計画」が策定されたが、情報セキュリティを巡る環境変化を背景に、2010年5月には「国民を守る情報セキュリティ戦略」が新たに策定され、2020年までに「世界最先端の情報セキュリティ先進国を実現することを目標に掲げている。

重要インフラに関しては、2005年に「重要インフラの情報セキュリティ対策に係る行動計画」が策定され、その改訂版として2009年には「重要インフラの情報セキュリティ対策に係る第２次行動計画」[28]が策定されている。第二次行動計画では、官民の情報共有・分析機能として「セプター」が設置され、セプター間の横断的情報共有体制として「セプターカウンシル」が設置されている。また、電力・ガス・水道の各分野において、「制御システムのセキュリティ」が対象となる重要システムとして取り上げられている。

図表 3-7　わが国における重要インフラのセキュリティ情報共有・分析体制



出典：　脚注 28

3.3.2　情報処理推進機構（IPA）の取り組み

独立行政法人の情報処理推進機構（IPA）は制御システムのセキュリティ対策について積極的な活動を行ってきた。2008年度の「重要インフラの制御システムセキュリティとITサービス継続性に関する調査」、「組込みソフトウェアエンジニアリング標準に関する調査 」、2009年度の「制御システムセキュリティの推進施策に関する調査報

[28] http://www.nisc.go.jp/active/infra/pdf/infra_rt2.pdf

告書」などである。

IPAは2007年から、脆弱性対策データベース（JVN iPedia）の運営を開始し、2010年末には、運用開始から累計9,600件の脆弱性対策情報を公開するに至っている。JVN iPediaでは、2008年頃からSCADAの脆弱性対策情報も公開されるようになり、2008年には8件、2009年には9件、2010年には6件のSCADA関連の脆弱性対策が公表されている[29]。

3.3.3 JPCERT/CC の取り組み

JPCERT/CC は有限責任中間法人であり、中立的組織としてコンピューティングセキュリティインシデントについて、インシデント報告の受け付け、インシデント対応支援、発生状況の把握や手口の分析などを技術的立場から行っている。

制御システムについては、PCERT/CCはIPAを経由した情報提供を受けて脆弱性情報を公開しているが、2008年からの公開情報の累計は34件に達している（2011年2月末現在）。また、2009年２月には、制御システムのベンダやシステムベンダなどをメンバーとした「制御システムベンダーセキュリティ情報共有タスクフォース」を発足させメンバー間の情報共有の促進に当たっている。

PCERT/CC は「国内の制御システムにおける汎用通信プロトコルの利用状況およびセキュリティへの取組み状況に関する調査」（2008 年）、「制御系プロトコルに関する調査研究」（2008 年）、「制御システムセキュリティガイドライン、標準、及び認証への取り組みに関する分析」（2009 年）などの調査報告を取りまとめている。

また、2010 年 5 月には、パッチ管理のガイドとして「グッド・プラクティス・ガイド　パッチ管理」を提供し、2011 年 2 月には制御システムセキュリティの簡易アセスメントツールとして、日本版 SCADA Self Assessment Tool（SSAT）の提供を開始している。両者を併用することで、制御システムの運用者によりよいセキュリティ環境を提供できるものと期待されている。

3.4　国際的な認証・標準化を巡る動向

3.4.1　近年の標準化進展の背景（安全性神話の喪失）

制御システムのオープン化とそれによるセキュリティ課題の登場は、制御システムがその脆弱性を攻撃される場合に少なからぬ経済的被害を発生するだけでなく、時には人命被害を生みだすまでに至ったことを示している。また、Stuxnet のような大規模攻撃の事例は、制御システムへの攻撃が一種の戦争手段（Warfare）として利用されるに至ったことを示している。

特に、Windows のゼロデイ脆弱性への攻撃のようなオープンな情報系部分だけでなく、制御システムの世界的最大手ベンダであるシーメンス社製の制御システムは、その奥深くま

[29] http://www.ipa.go.jp/security/vuln/report/JVNiPedia2010q4.html

で侵入され蹂躙された。制御システムが独立性を有する孤立的システムであり、それゆえに安全であるという神話は失われつつある。制御システムの標準化・規格化が近年進められている背景はここにある。

3.4.2　制御システムセキュリティに関する標準化動向の概略

制御システムのセキュリティを巡るこうした状況を背景に、セキュリティ標準の規格化が各標準化機関の手によって進められている。その概要を「制御システムセキュリティカンファレンス 2010」におけるあるプレゼンテーション[30]は、情報系と制御系、システム運用とコンポーネントへのセキュリティ機能要件の二つの側面から、４つの象限における規格の概要を、下の図表 3-8 のように纏めている。

図表 3-8　近年の制御システムセキュリティに関するセキュリティ規格の分類

	管理運用視点 ・セキュリティ管理システム仕様 ・推奨実施例	コンポーネント視点 ・セキュリティ機能要件定義 ・評価・認証の枠組み
情報系セキュリティ	・ISO/IEC 27000シリーズ(27001:情報セキュリティ管理システム(ISMS)要求事項, 27002:ISMS 実践のための規範, 27005:情報システムのリスク管理, 27006:認証/登録プロセスの要求仕様) ・NIST SP800-53他	・ISO/IEC 15408 (Common Criteria;CCと称される。製品がセキュリティに配慮すべき事項)
制御系セキュリティ	・ISA-99 (生産制御システムセキュリティ) ・ISO/IEC 62443 (予定) (Industrial Process Measurement and Control – Net & System Security) ・NIST SP800-82	・PCSRF SPP-ICS (System Protection Profile - Industrial Control System)

出典：脚注 30

3.4.3 制御システムセキュリティ規格を巡る直近の動向

上の図表3-8で（予定）とされているISO/IEC 62443は、2010年11月にIEC 62443-2-1 Ed. 1.0として公式に制定され公表された。この規格は、「制御システム(IACS：industrial automation and control systems)のためのサイバーセキュリティ管理システム(CSMS：cyber security management system)の確立に必要な要素(ポリシー，手続，実施手順，要員)を定

30 「制御システムにおけるセキュリティ役割分担の取り組み」、制御システムセキュリティカンファレンス 2010、2010 年 2 月

義し，それら要素を策定するためのガイダンスを提供する」とされている。上の図表に現れるANSI/ISA 99とほぼ同じ内容である。

いずれも正式エディションとなったISA99、IEC 62443-2-1、及びNISTSP800-82が、今後セキュリティ規格の中心的存在としてとして、世界的に普及して行くものと予測される。

また、2010年１月、ISAは”Industrial Network Security, 2nd Ed.”[31]を刊行した。この制御システムのセキュリティに関するテキストブックは、管理者、技術者、技能者、オペレータのセキュリティ教育に最適の入門書であるとされている。

[31]http://www.isa.org/Template.cfm?Section=Books3&Template=/Ecommerce/ProductDisplay.cfm&ProductID=10879

4．今後の取り組みに向けた提言

①制御システムの情報セキュリティ課題の重要性認識と、対策への積極的取組み

サイバー攻撃を受けないとされてきた制御システムでStuxnetのように重大なインシデント事例が発生したことを考えると、制御システムに関わる重要インフラ関係者が情報セキュリティ課題をこれまでより一層真剣に受け止め、対策の策定に、より積極的に取り組む時期が来ている。制御システムのセキュリティの維持は、重要インフラサービスを継続的に提供するために重要な役割を果たすことから、単に重要インフラのセキュリティ部門だけに委ねられるのではなく、インフラ運営の最高責任者が常に関心を払わなければならない問題である。このような認識を関係者が広く共有する必要がある。

②情報共有体制の積極的整備

制御システムのセキュリティに関する情報共有は、充分に進展しているとは言い難いのが現状である。近年整備されつつある重要インフラ各分野のセプター、あるいはセプターカウンシルでの情報の共有を一層推進することで、重要インフラのセキュリティ対策を進展させる必要がある。

③制御システムの情報セキュリティに関する研究開発の積極的推進

制御システムは情報システムに比べてはるかに長寿命であり、その更新の時間差が制御システムの脆弱性に繋がっていると考えられる。また、脆弱性の補強（いわゆるパッチ当て）が、制御システムそのものの不具合を引き起こす可能性も存在している。これらの問題についての研究開発の積極的推進が必要である。例えば、パッチ適用についてのテストベッドの開発・設置などを検討する必要があると思われる。

④重要インフラの途絶の他インフラへのカスケード的波及に関する追跡調査の実施

我が国を直近に襲った東日本大震災をきっかけに、通信、物流、水道、ガス、電力、金融など重要インフラの幾つかは大打撃を受け、とりわけ電力インフラについてはいまなお日本経済のボトルネックとなっている。東日本大震災を契機とした重要インフラの途絶と、それが及ぼしたカスケード的波及について重要システムの維持・復旧の視点から綿密な追跡調査を実施し、調査結果を将来の危機的状況における波及の軽減や対策の作成に生かすことが重要である。

文献一覧

・情報処理機構による制御システムセキュリティに関する包括的な調査（初年度）
「IPA、重要インフラの制御システムセキュリティとITサービス継続に関する調査、2009年3月」

・情報処理機構による制御システムセキュリティに関する包括的な調査（次年度）
「IPA、制御システムセキュリティの推進施策に関する調査報告書、2010 年 5 月」

・米国 NIST による制御システムに関する包括的ガイドライン
“NIST Special Publication 800-82, Guide to Industrial Control Systems (ICS) Security, Sep 2008”

・NIST SP 800-82の著者の一人による2007 年のプレゼンテーション
“Supervisory control and data acquisition security,” Keith Stouffer, Feb. 2007

・NISTによる2009年制御システムワークショップでのプレゼンテーション
“Industrial Control System Security,” NIST Industrial Control System Cyber Security Workshop, October 2009

・制御システムにおけるOPCの役割についての専門ベンダによる解説
http://www.m-system.co.jp/mstoday/plan/mame/b_network/9710/index.html

・カナダに本拠を置く重要インフラインシデント事例データベースとそのホームページ
Repository of Industrial Security Incidents (RISI)
http://www.securityincidents.net/index.asp

・ウェブ上で見られる 2003 年 8 月の米国東海岸の宇宙からの夜間写真
http://www.teamrenzan.com/archives/writer/omnibus/web_larva.html

・DoE による Aurora Generator Test 風景で破壊された発電機の実験ビデオ
http://www.militaryphotos.net/forums/showthread.php?121081-AURORA-test-validated-fears-of-Dept.-of-Homeland-Security

・JR 東日本による COSMOS システム不具合の記者発表　2011 年 1 月 18 日
http://www.jreast.co.jp/press/2010/20110106.pdf

・日経 BP 及び東洋経済による 2002 年と 2011 年のみずほ銀行システム故障の記事
http://itpro.nikkeibp.co.jp/free/NC/NEWS/20020619/1/
http://www.toyokeizai.net/business/strategy/detail/AC/5cd01c05cd9819b64569b21fd9

77221f/

・シマンテック社による Stuxnet 事案の詳細解明報告
W32.StuxnetDossier
http://www.symantec.com/connect/blogs/w32stuxnet-dossier

・Stuxnet に関する科学・国際安全保障研究所のリポート
“Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? “
http://www.isis-online.org/uploads/isis-reports/documents/stuxnet_FEP_22Dec2010.pdf

・情報処理機構（IPA）による新しいタイプの攻撃(Stuxnet)についての報告
IPA「『新しいタイプの攻撃』に関するリポート」　2010 年 12 月
・「制御システムセキュリティカンファレンス 2011 」における JPCERT/CC による Stuxnet に関するプレゼンテーション
「Stuxnet－制御システムを狙った初のマルウエアー　JPCERT/CC 2011 年 2 月」

・US-CERT及びICS-CERTのホームページ
http://www.us-cert.gov/index.html
http://www.us-cert.gov/control_systems/ics-cert/

・米国DHSが2009年10月に公刊した「制御システムの安全戦略」
“Strategy for securing control systems,” homeland security October 2009
http://www.us-cert.gov/control_systems/pdf/Strategy%20for%20Securing%20Control%20Systems.pdf

・米国エネルギー省のSCADAテストベッド計画（NSTB）
National SCADA Test Bed Program
http://www.oe.energy.gov/nstb.htm

・2011年1月に公表されたDoEによる制御システムのセキュリティロードマップ（ドラフト）
“Roadmap to Secure Energy Control System,” Energy Sector Control System Working Group, Jan. 2011
http://www.controlsystemsroadmap.net/pdfs/2011_roadmap_draft.pdf

・米国I3P(Institute for Information Infrastructure Protection)のホームページ
http://www.thei3p.org/about/

・米国I3PによるSHARPプロジェクトの概略説明ページ
http://www.thei3p.org/docs/publications/factsheet-Sharp-2-26-08.pdf

・オランダのTNOが運用する産業事故に関するFACTSデータベースのトップページ
http://www.factsonline.nl/tabid/173/Default.aspx

・オランダのTNOが公表した重要インフラのカスケード波及に関する論文のサマリー
EMPIRICAL FINDINGS ON CRITICAL INFRASTRUCTURES DEPENDENCIES IN EUROPE
http://critis08.dia.uniroma3.it/pdf/CRITIS_08_40.pdf

・EUのEU共同研究センター（JRC=Joint Research Center）の下に置かれた市民防護セキュリティ研究所（ISPC）のホームページ
http://ipsc.jrc.ec.europa.eu/

・市民防護セキュリティ研究所（ISPC）における重要インフラ研究機構である Critical Infrastructures Protection (CIP) の紹介ページ
http://ipsc.jrc.ec.europa.eu/showaction.php?id=22

・CIP が展開している ARCADE プロジェクトに関する概略説明ページ
http://sta.jrc.ec.europa.eu/scni/pdf/arcade_web.pdf

・EU諸国が展開している重要インフラマネジメント研究開発、VIKING（Vital Infrastructure, Networks, Information and Control Systems Management）プロジェクト
http://www.vikingproject.eu/new2/index.php

・英国の国家インフラ防護センター（CPNI=Center for the Protection of National Infrastructure）のホームページ
http://www.cpni.gov.uk/

・ドイツの情報セキュリティ庁（BSI=Bundesamt für Sicherheit in der Information stechnik）のホームページ
https://www.bsi.bund.de/EN/TheBSI/thebsi_node.html

・情報セキュリティ政策会議、「重要インフラの情報セキュリティ対策に係る第２次行動計画」、2009 年
http://www.nisc.go.jp/active/infra/pdf/infra_rt2.pdf

・IPA が運用するJVN iPedia で公表された制御システムの脆弱性対策
http://www.ipa.go.jp/security/vuln/report/JVNiPedia2010q4.html

・「制御システムにおけるセキュリティ役割分担の取り組み」、制御システムセキュリティカンファレンス 2010、2010 年２月

・IEC による制御システムセキュリティの正式規格、IEC 62443-2-1 Ed. 1. 2010 年 11 月
http://www.iec.ch/cgi-bin/procgi.pl/www/iecwww.p?wwwlang=E&wwwprog=pro-det.p&He=IEC&Pu=62443&Pa=2&Se=1&Am=&Fr=&TR=&Ed=1#WG

・ISA による制御システムセキュリティテキストブックの 2010 年発行の最新版、
“Industrial Network Security, 2nd Ed.”
http://www.isa.org/Template.cfm?Section=Books3&Template=/Ecommerce/ProductDispl

ay.cfm&ProductID=10879