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

IPA®
独立行政法人 情報処理推進機構
セキュリティセンター

本ページは白紙です

目次

1. はじめに

1.1.本調査の背景と目的

1.1.1　調査の背景

多くの重要インフラのシステムには、情報システムと制御システムの二つの系統がある。このうち制御システムは、他の機器やシステムの動作を管理、指示、制御するシステムであり、センサやアクチュエータ等のフィールド機器、制御用ネットワーク、コントローラ、監視・制御システム（SCADA：Supervisory Control And Data Acquisition とも呼ばれる）等で構成されている。最近の制御システムは、標準プロトコル（TCP/IP やイーサネットなど）や汎用製品の導入が進展し、さらに、競争力強化といった経営面からの要請により、情報システムとの連携が進み、ネットワークを介してシステム接続するケースが増大してきている。このような状況において制御システムは様々な脅威（たとえば不正アクセスや情報漏えい等）に直面していることが指摘されており、万が一攻撃を受けた場合のサービス提供への影響は大規模かつ広範囲になると予測されている。

そこで、今後課題が顕著化してくると想定される重要インフラにおける制御システムの情報セキュリティに関する国内外の現状調査と制御システムの IT 障害発生時におけるサービス継続への対応の現状調査を行うことにした。

1.1.2　調査の目的

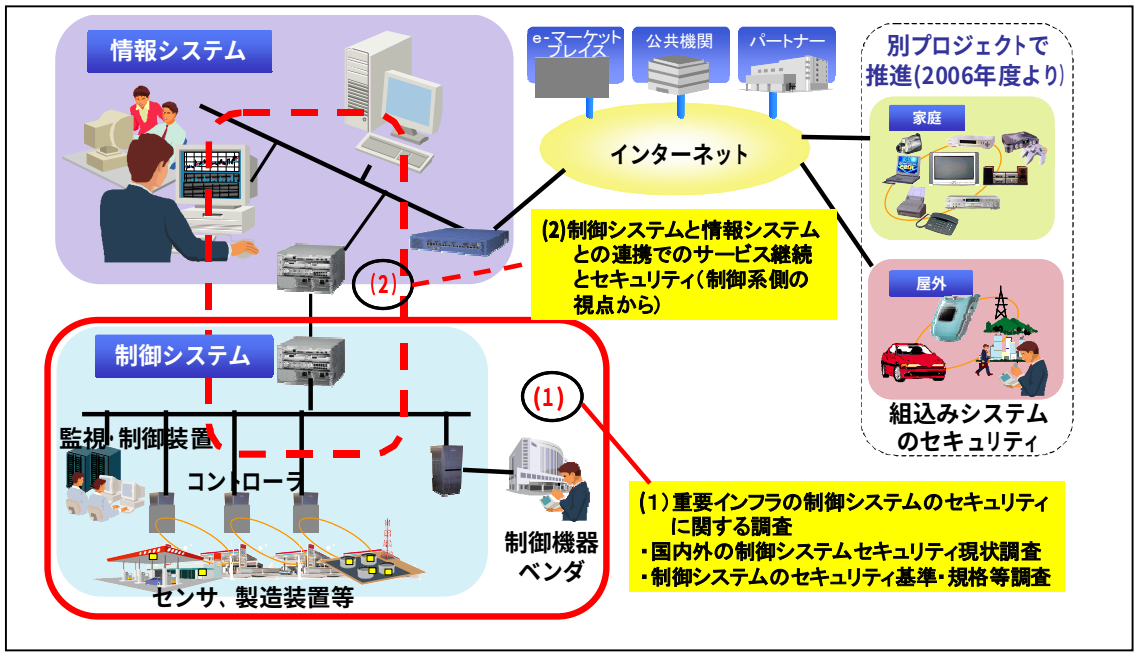
本調査は、今後、情報セキュリティ上の課題が顕在化してくると想定される重要インフラにおける制御システムを対象として、情報セキュリティに関する国内外の現状、IT 障害発生時におけるサービス継続への対応に関する現状を把握することを目的として実施する。また、制御システムの研究・開発者や情報セキュリティ専門家などによる有識者の検討会を設置し、上記調査内容をもとに、重要インフラにおける制御システムを対象とした情報セキュリティに関する課題整理、情報セキュリティ対策のあり方、意識向上策等について検討を行うことを目的とする。

1.2.本調査の概要

1.2.1　調査の内容

本調査は、図表 1-1 に示すように、重要インフラの制御システムのセキュリティに関する調査と、制御システムと情報システムとの連携におけるサービス継続とセキュリティに関する調査からなる。これら二つの調査と有識者による検討会での議論を踏まえ、我が国における制御システムセキュリティの課題と対策のあり方を整理した。

図表 1-1 調査の内容



（1）重要インフラの制御システムセキュリティの調査

重要インフラの制御システムセキュリティについては、以下の方式で各調査項目を実施した。

【調査１】：海外・国内調査

以下に示す米国現地での国際会議参加及びヒアリング、国内でのヒアリングにより、制御システムセキュリティに関わる現状について調査を行った。

＜海外調査＞

- PCSF（Process Control Systems Forum）が主催する 2008 Annual Meeting に参加
- 米国研究機関、大学への研究状況のヒアリングを実施
- 制御システム専門コンサルタントへのヒアリングを実施

＜国内調査＞

- JEMIMA（Japan Electric Measuring Manufactures' Association：社団法人 日本電気計測器工業会）会員でもある制御機器・システムメーカとの意見交換を実施
- 大学研究者へのヒアリングを実施

【調査２】：制御システムに対するセキュリティ基準・規格等の調査

制御システムに関連するセキュリティ基準・規格等の策定状況及び、今回調査において基本になると考えられる次に示す基準・規格等の内容について調査を行った。

- NIST（National Institute of Standards and Technology） SP（Special Publication）800-82　Guide to Industrial Control Systems（ICS）Security
- NIST SP 800-53　Recommended Security Controls for Federal Information Systems
- ANSI/ISA.99.00.01　Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and Models
- NERC（North American Electric Reliability Corporation）Standards CIP（Critical Infrastructure Protection）-002～CIP-009

【調査３】：過去の国内関連活動内容の把握

1997 年 9 月～2000 年 3 月に設置された「大規模プラント・ネットワーク・セキュリティ対策委員会（PSEC：large-scale Plant network Security Committee)」では、制御システムセキュリティに対する、マネジメント面、技術面の両面から検討を行っており、特に、PSEC 報告書にて課題として示されている内容を整理した。この部分は、制御システムのセキュリティ対策に関する状況が､2000 年当時と現在とでどのように変わっているかを確認するためのものであり、本報告書では付録 3 として掲載した。

（2）制御システムと情報システムとの連携でのサービス継続とセキュリティについての調査

以下により、制御システム側の視点での調査を実施した。

(a) 制御システムとして情報システムとの連携をどのように捉えているか。
(b) 制御システムとして情報システム側からの脅威をどのように捉えているか。また、その脅威に対して制御システム側でどのような対策がなされているか。
(c) 制御システムの機能停止、フィールド（設備系や製造ラインなどの制御対象）の処理停止を起こしうるものとして､どのような脅威､事象を想定しているか､また、そのような脅威、事象発生時のサービス継続（機能維持、処理継続）についてどのような考え方をもっているか。
(d) 上記（c）で想定する脅威、事象発生時のサービス維持（機能維持、処理継続）を実現するために、どのような対策・対応（有事発生時の対応計画、インシデ

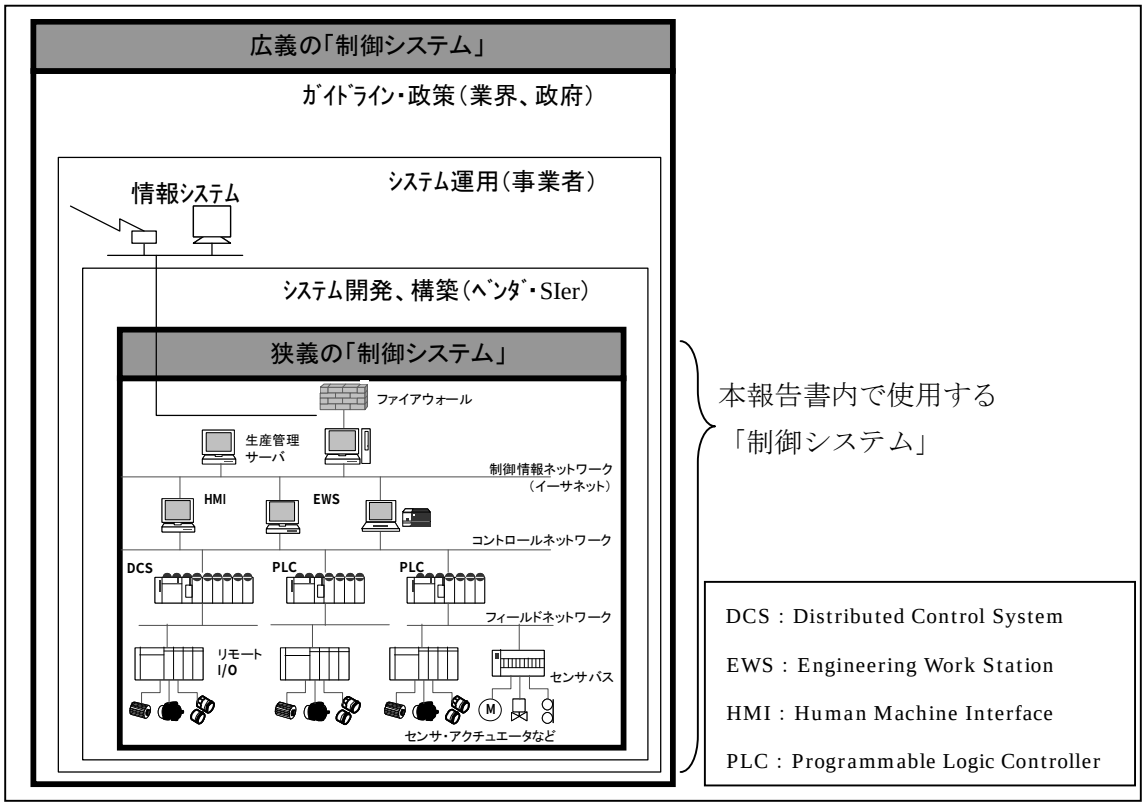
ントレスポンス体制などの体制・運用面も含む）がなされているか。

1.2.2　本調査における用語の定義

（1）本調査における「制御システム」の定義

「制御システム」は、狭義と広義に分けて捉えることができる（図表 1-2）。

図表 1-2 狭義の「制御システム」と「広義」の制御システムの関係



資料：JEMIMA 資料および各種資料より作成

本調査では、特に言及が無い場合には狭義の意味で「制御システム」という表現を使用する。すなわち、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）をさすこととする。

実際のケースでは、制御システムの範囲を広くとらえた広義の制御システムの捉え方も存在する。すなわち、制御システムの開発・構築ベンダ側のセキュリティ対応方針、事業者としてのシステム運用方針、さらに業界や公的なガイドラインを踏まえたシステム運用方針など、人や制度を含め制御システムと捉える考え方である。

（2）本調査における「オープン化」の定義

本調査では、汎用製品の採用および標準プロトコルの採用の両方を含めて「オープン化」という表現を使用する。上記のどちらか片方だけに限定する場合は、「汎用製品の採用」、「標準プロトコルの採用」というように区別して使用する。

図表 1-3 「オープン化」、「汎用製品」、「標準プロトコル」の関係例

ハードウェア	通信プロトコル		オープン化	汎用製品	標準ﾌﾟﾛﾄｺﾙ
市販 PC と同規格	TCP/IP	→	○	○	○
市販 PC と同規格	ベンダ独自プロトコル	→	×	○	×
ベンダ独自規格機器	TCP/IP	→	×	×	○

資料：各種資料より作成

1.2.3　調査の方法

本調査では、以下に示す公開資料調査及びヒアリング調査を実施した（図表 1-4）。

図表 1-4 調査方法

調査方法	概　　要
公開資料調査	制御システムセキュリティに関する各種文献、先進的な取り組みを推進する政府機関、関係組織のウェブサイト等で公表された最新情報などの公開資料を調査した。
ヒアリング調査	制御システムセキュリティを検討するにあたり、国内制御機器メーカ、海外での取り組みを推進する政府機関、関係組織へのヒアリング調査を実施した。

さらに、本調査で設置する有識者による検討会を次表に示すように連動させることにより、調査内容の深化、有用性の向上を図った（図表 1-5）。

図表 1-5 調査の観点と進め方

検討会（3回開催）	調査（事務局調査チーム）
	・研究会の目的、進め方、スケジュール等についての案を作成 ・調査先候補に関する事前調査実施
【第1回検討会（2008年6月）】 ・研究会の目的、進め方、スケジュール等についての確認 ・ICSセキュリティに関するテーマプレゼンテーション	
	・第1回検討会での決定内容に基づき調査実施 ・調査内容の分析・まとめ
【第2回検討会（2008年10月）】 ・調査内容についての議論 ・調査内容に基づき重要インフラ制御システムにおける情報セキュリティの課題等について検討	
	・第2回検討会での議論内容に基づき調査報告書（案）作成
【第3回検討会（2008年12月）】 ・調査報告書（案）についての議論 ・重要インフラ制御システムの情報セキュリティのあり方や意識向上策等について議論	
	・第3回検討会での議論内容を踏まえて最終報告書作成

1.2.4　調査の対象

（1）国内調査

＜制御機器ベンダへのヒアリング＞

国内制御システムベンダ 6 社

＜大学へのヒアリング＞

長岡技術科学大学、名古屋工業大学、国士舘大学、奈良先端科学技術大学院大学

＜業界団体との意見交換＞

社団法人 日本電気計測器工業会（JEMIMA）PA（Process Automation）・FA（Factory Automation）計測制御委員会セキュリティ調査研究 WG

（2）海外調査（米国）

＜政府機関へのヒアリング＞

- NIST

＜研究機関、大学へのヒアリング＞

- INL（Idaho National Laboratory）、I3P（Institute for Information Infrastructure Protection）、Dartmouth 大学

＜セキュリティ関連ベンダへのヒアリング＞

- MITRE Corporation、Digital Bond

＜カンファレンスでの情報収集＞

- Process Control Systems Industry Conference 2008
  ［PCSF（Process Control Systems Forum）主催］

1.3.用語および略語の定義

1.3.1　用語定義一覧

本報告書で使用する用語の意味を以下に定義する（図表 1-6）。

図表 1-6 用語定義一覧

用語	定　義
オープン化	本調査では、汎用製品の採用及び標準プロトコルの採用の両方を含めて「オープン化」と呼ぶ。なお、上記のどちらか片方だけに限定して記述する場合は、「汎用製品の採用」、「標準プロトコルの採用」というように明確に区別して記述する。
制御システム	「制御システム」は、狭義と広義に分けて捉えることができる。 本調査では、特に言及が無い場合には狭義の意味で「制御システム」という表現を使用する。すなわち、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）をさすこととする。
SCADA	Supervisory Control And Data Acquisition の略称。 主に、地理的に分散した制御対象を広域ネットワークを介して遠隔集中監視するシステムを SCADA システムと呼ぶが、日本では、PLC などの制御機器の監視を、マンマシンインタフェース（HMI）である汎用 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。 本調査では、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。

1.3.2 略語一覧

本報告書で使用する略語は以下の通りである（図表 1-7）。

図表 1-7 略語一覧

略語	名称
AGA	American Gas Association
ANL	Argonne National Laboratory
ANSI	American National Standards Institute
API	American Petroleum Institute
BCP	Business Continuity Plan
CERT/CC	Computer Emergency Readiness Team / Coordination Center
CIP	Critical Infrastructure Protection
CIPAC	Critical Infrastructure Partnership Advisory Council
CPNI	Centre for the Protection of National Infrastructure
CS2SAT	Control System Cyber Security Self-Assessment Tool
CSSP	Control Systems Security Program
DCS	Distributed Control System
DHS	Department of Homeland Security
DOE	Department of Energy
DOC	Department of Commerce
E-SCSIE	European SCADA and Control Systems Information Exchange
EWS	Engineering Work Station
FA	Factory Automation
FERC	Federal Energy Regulatory Commission
HMI	Human Machine Interface
I3P	Institute for Information Infrastructure Protection
ICS	Industrial Control System
IEC TC（数字）	International Electrotechnical Commission Technical Committee
IED	Intelligent Electronic Device
IEEE	The Institute of Electrical and Electronics Engineers,Inc.
INL	Idaho National Laboratory
ISA	the International Society of Automation
JEITA	Japan Electronics and Information Technology Industries Association：社団法人電子情報技術産業協会
JEMIMA	Electric Measuring Instruments Manufacturers' Association： 社団法人日本電気計測器工業会
IPA	Information Technology Promotion Agency ,Japan： 独立行政法人 情報処理推進機構 セキュリティセンター
JPCERT/CC	Japan Computer Emergency Readiness Team / Coordination Center：有限責任中間法人 JPCERT コーディネーションセンター
JVN	Japan Vulnerability Notes
LBNL	Lawrence Berkeley National Laboratory

略語	名称
MTU	Master Terminal Unit
NCSD	National Cyber Security Division
NERC	North American Electric Reliability Corporation
NISC	National Information Security Center : 内閣官房情報セキュリティセンター
NIST	National Institute of Standards and Technology
NRC	Nuclear Regulatory Commission
NSTB	National SCADA Test Bed （Program）
NVD	National Vulnerability Database
OE	Office of Electricity Delivery and Energy Reliability
ORNL	Oak Ridge National Laboratory
PA	Process Automation
PCIS	Partnership for Critical Infrastructure Security
PLC	Programmable Logic Controller
PSEC	large-scale Plant network Security Committee
PCSF	Process Control Systems Forum
PCSRF	Process Control Security Requirements Forum
PNNL	Pacific Northwest National Laboratory
RTU	Remote Terminal Unit
SCADA	Supervisory Control And Data Acquisition
SCSIE	The SCADA and Control Systems Information Exchange
SHARP	Security-Hardened Attach Resistant Platform
SICE	The Society of Instrument and Control Engineers : 社団法人計測自動制御学会
SNL	Sandia National Laboratory
US-CERT	United States Computer Emergency Readiness Team
VPN	Virtual Private Network

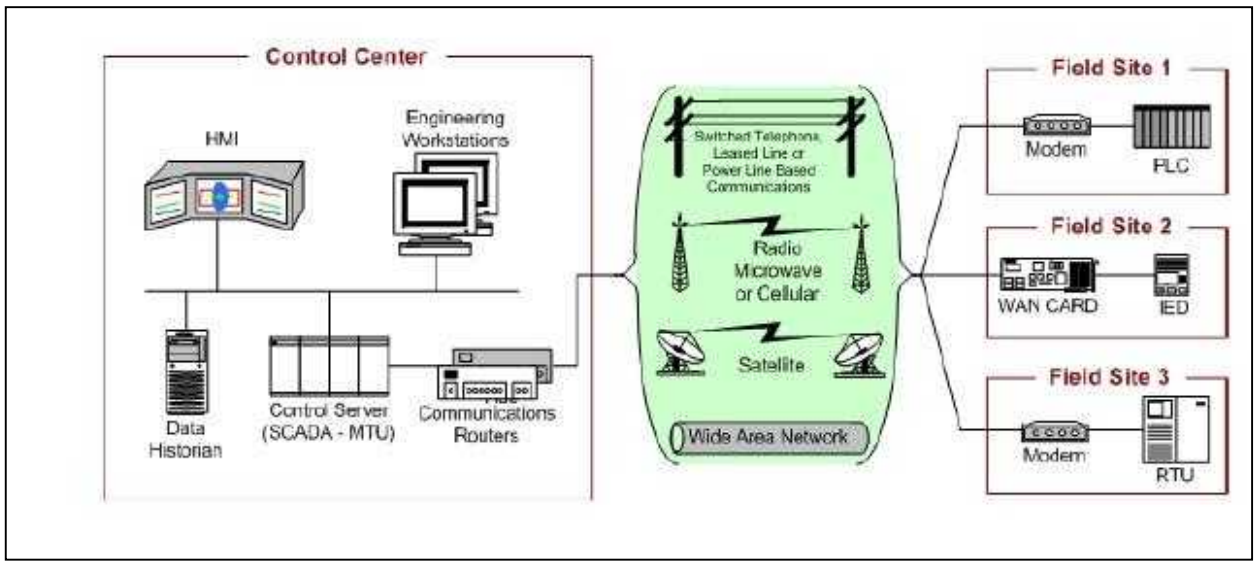
2. 重要インフラの制御システムセキュリティに関する調査

2.1.米国における状況

2.1.1　重要インフラの制御システムセキュリティに対する取り組み体制

米国では重要インフラ[1]の制御システムへの SCADA システムの採用が拡大している。SCADA システムは生産設備、プラント、パイプラインなどの監視や制御データの収集を目的としたシステムであり、広域に分散するシステム群の遠隔集中監視に用いられている（図表 2-1）。

図表 2-1 SCADA システムの一般的な構成図

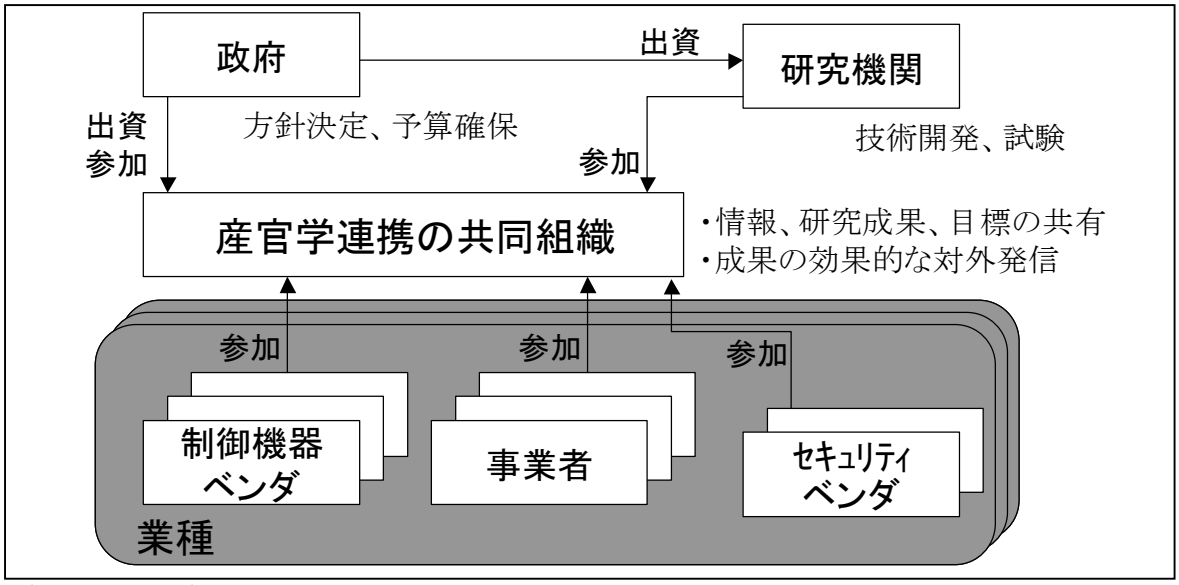


資料：NIST SP-800-82 Final Public Draft より抜粋

近年、SCADA システムへの PC などの汎用製品や標準化されたネットワークプロトコルの採用が進んでおり、外部からの攻撃に対する脆弱性などのセキュリティ上の課題が指摘されている。SCADA システムは多くの重要インフラの設備で使用されており、万一サイバー攻撃を受けた場合に、多大な経済損失や人命の危険を生じる可能性がある。そのため、SCADA システムの脆弱性問題を中心に重要インフラの制御システムへのセキュリティ対策への関心が高まっており、政府、事業者／業界団体、制御機器ベンダ、研究機関、セキュリティベンダなどによるクロスセクタの取り組みが進められている（図表 2-2）。

[1]米国では重要インフラとして、国家安全に関する大統領令 Homeland Security Presidential Directive 7（HSPD-7）と国家重要インフラ防護計画 National Infrastructure Protection Plan（NIPP）に基づき、農業・食料、銀行・金融、化学、商業施設、ダム、防衛産業基盤、緊急サービス、エネルギー、政府施設、情報技術、国定記念物・建築物、原子炉・核物質・核廃棄物、郵便・物流、公共衛生・ヘルスケア、通信、輸送、水道、重要製造業の 18 分野が定められている。

図表 2-2 米国における制御システムセキュリティ対策の取り組みイメージ



資料：各種資料より作成

米国におけるこれら活動に関連する主なプレーヤを図表 2-3 に示し、以下、これらの中での主要な活動の概要について記す。

（1）政府機関

（i）DHS

重要インフラのセキュリティ対策推進の中心に位置する省庁である DHS（Department of Homeland Security）では、重要インフラの制御システムにおけるリスクを削減することを目的とする施策として 2004 年に CSSP（Control Systems Security Program）を立ち上げ、制御システムのサイバーセキュリティ自己評価ツールの開発、制御システムセキュリティカタログの公開、参考事例の紹介、トレーニングプログラムの提供などの対策を推進している。また、制御システムのセキュリティ対策を推進するためのプログラムとして産官学共同で運営する PCSF を 2005 年より立ち上げ、政府、大学・研究機関、制御機器ベンダ、事業者など制御システム関係者が参加するカンファレンスを定期的に開催し、各種取り組みの促進、情報共有を図っている。

（ii）DOE

重要インフラ分野の中でも、電力、ガス、石油などのエネルギー関係のインフラは国民生活および産業への影響が大きいことからセキュリティ対策の強化が重要視され、DOE（Department of Energy）ではエネルギー関連事業者の制御システムのセキュリティ強化を支援するための取り組みを行っている。そこでは、エネルギー関連事業の制御システム特性に応じた次世代制御システム、システム脆弱性評価、統合リスク

分析などのプロジェクトが進められている。

また、「ナショナル SCADA テストベッド（National SCADA Test Bed）」を設置（2008 年）するなど、他業種に先行した研究開発の取り組みも進めている。テストベッドでは、制御システムの脆弱性を特定し解決するためのテスト環境を事業者や政府機関に提供している。

さらに、エネルギー業界団体や関連組織による「エネルギーセクタにおけるセキュアな制御システムのロードマップ（Roadmap to Secure Control Systems in the Energy Sector）」の策定（2006 年）を支援している。本ロードマップでは、サイバー攻撃に対する重要インフラの機能防御のための 10 年間のビジョン、取り組み、目標、マイルストンが示されている。

（iii）NIST

NIST は DOC（Department of Commerce）内の標準策定組織であり、連邦政府向けの制御システムのセキュリティ基準として SP 800-82（Guide to Industrial Control Systems（ICS） Security）や SP 800-53（Recommended Security Controls for Federal Information Systems）を策定している。

また、制御システムのセキュリティ強化を促進するプログラムとして、政府機関、制御機器ベンダ、事業者、セキュリティベンダなど 400 以上の組織が参加する PCSRF（Process Control Security Requirements Forum）を推進し、セキュリティの要件やアプリケーションの定義などに関する活動を行っていたが、2008 年以降は IEC や ISA（International Society of Automation）における標準化活動への参画、支援にシフトしている。

（2）産官学組織／クロスセクタ

（i）I3P

I3P（Institute for Information Infrastructure Protection）は、情報インフラ保護の研究のために 2001 年に設立された大学、政府の研究所、NPO 等から構成されるコンソーシアムであり、制御システムに関わるリサーチプロジェクトとして「Survivability and Recovery of Process Control Systems」を推進している。また、これ以外に「Human Behavior, Insider Threat, and Awareness」、「Business Rationale for Cyber Security」、「Safeguarding Digital Identity」の計４つのリサーチプロジェクトが推進されている。

I3P の研究資金元は DHS と NIST である。I3P では政府や企業と協力して、短期的ではなく中～長期（多くは 2-3 年）のセキュリティに関する課題を研究の対象にしている。政府とのコラボレーションでは、例えば DHS が提示するトピックスやアイデアに対して、I3P が研究の提案を行い、合意により着手し成果を報告書にまとめ提出

することで資金を得る。I3P は産業界とも協力しているが、資金提供は受けていない。

（ii）PCSF

PCSF（Process Control Systems Forum）は、よりセキュアな制御システムの開発、普及を促進することを目的とした、産官学からなるフォーラム組織である。産業界からは、制御機器ベンダ、システムインテグレータ、事業者及び業界団体、セキュリティベンダなどが参加している。また、政府機関では DHS が後援、DOE や NIST なども参加している。PCSF はオープン、協調的かつボランタリーなフォーラムであり、定期的な会議開催による情報共有、関係者の啓発などの利益団体的活動、ガイドライン作成などを目的としたワーキンググループ運営などの活動を行っている。2008 年は Process Control Systems Industry Conference（アニュアル・ミーティング）が開催され、米国を中心に約 200 名の参加者があり、制御システムのセキュリティの課題、セキュリティツールやソリューションの紹介、運用ガイドラインなどの多くのトピックスが発表された。

（iii）PCIS

PCIS（Partnership for Critical Infrastructure Security）は重要インフラの各セクタ代表がメンバとなる、クロスセクタの非営利組織であり、重要インフラの安全性と信頼性を高めるための官民協力を推進し、政府に対する政策提言を行っている。2007 年 4 月には行動計画（PCIS Business Plan 2007-2009）を策定し、重要インフラの安心安全を高めるためのクロスセクタの活動強化を提唱している。

（iv）CIPAC

CIPAC（Critical Infrastructure Partnership Advisory Council）は DHS により、政府の重要インフラ防護プログラムと民間および地方政府のインフラ防護活動をコーディネートすることを目的に設立された。CIPAC は政府と重要インフラおよびリソースの事業者及び運用者とのパートナーシップを実現し、重要インフラ防護のための様々な活動を支援するためのフォーラムを開催している。

（3）研究機関

（i）政府系研究機関

DOE 傘下の INL（Idaho National Laboratory）、SNL（Sandia National Laboratory）、PNNL（Pacific Northwest National Laboratory）、ANL（Argonne National Laboratory）、ORNL（Oak Ridge National Laboratory）、LBNL（Lawrence Berkeley National Laboratory）など

が、I3P や PCSF での制御システムセキュリティの研究に参画している。また、INL および SNL には SCADA のテストベッドが設置されている。

（ii）非営利研究機関、大学

MITRE Corporation、SRI international、Adventium Labs、RAND Corporation などの非営利研究機関やシンクタンクが、I3P でのツール開発や PCSF のワーキンググループなどに参加している。また、Purdue University、University of Tulsa、Columbia University、Massachusetts Institute of Technology、University of California（Davis 校および Berkeley 校）、Dartmouth College 他多数の大学も上記プロジェクトに参画している。

（4）業界団体

エネルギー関連では、NERC（North American Electric Reliability Corporation）、AGA（American Gas Association）、API（American Petroleum Institute）などの業界団体が制御システムのセキュリティ基準（Roadmap to Secure Control Systems in the Energy Sector）を策定している（2006 年）。また、水事業者セクタにおいては、エネルギーセクタのロードマップを参考として「水セクタにおけるセキュアな制御システムのロードマップ（Roadmap to Secure Control Systems in the Water Sector）」を策定（2008 年）している。またその他、核関連、化学などの重要インフラセクタの業界団体も PCSF などに参加し、制御システムのセキュリティ課題に関する取り組みを行っている。

（5）制御機器ベンダ

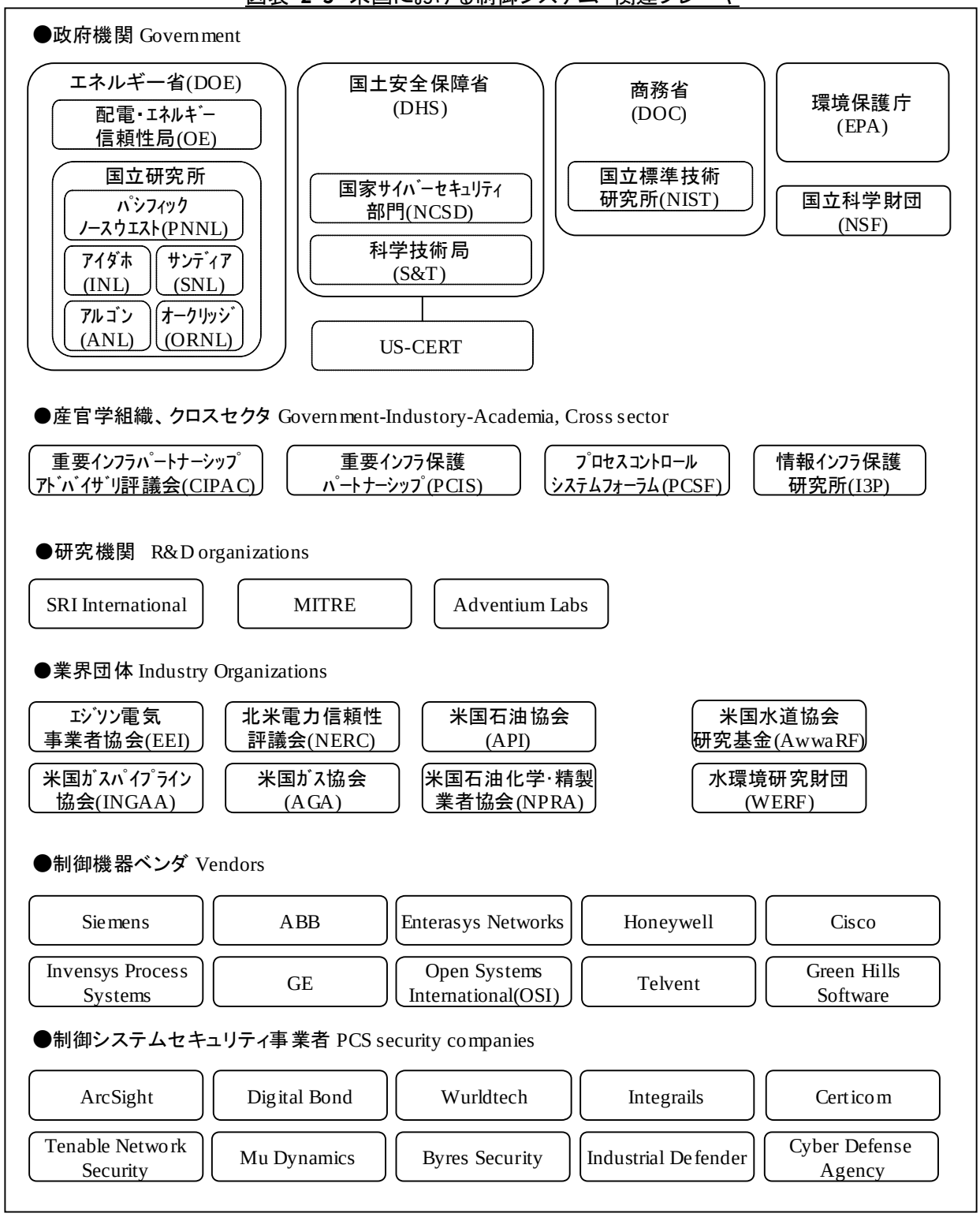
Siemens、ABB、Honeywell、GE、Cisco などの制御機器ベンダ、ネットワーク機器ベンダが、PCSF などの制御システムセキュリティ対策活動に参画している。

（6）制御システムセキュリティベンダ

ArcSight、Digital Bond、Wurldtech、Mu Dynamics などのソリューションプロバイダが、セキュリティ対策ツールの開発、脆弱性関連情報データベースの提供、セキュリティ認証サービスの提供などを行っている。

このように、米国における制御システムのセキュリティ対策は、重要インフラ分野を中心に政府と業界団体、産学官連携のイニシアチブにより推進されている。一方、その他一般の製造業などの民間部門においては脆弱性問題に対する認知度は依然低く、取り組みはこれからの段階である。

図表 2-3 米国における制御システム 関連プレーヤ



資料：各種資料より作成

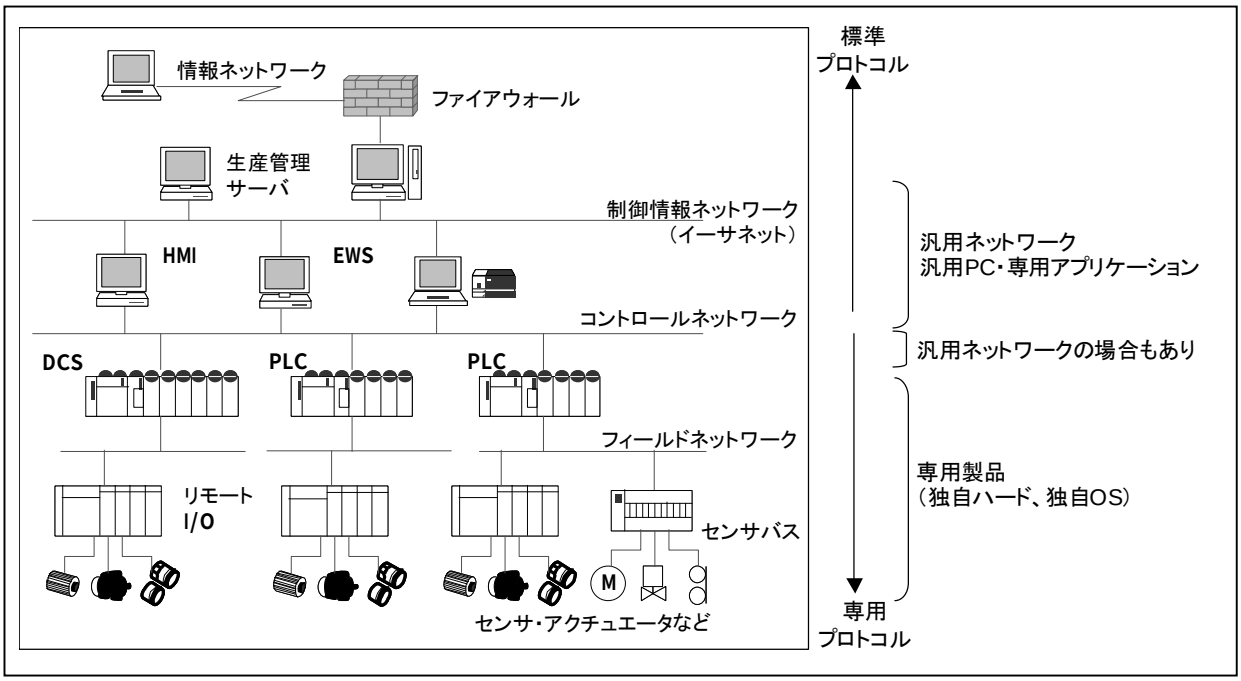
2.1.2　制御システムのオープン化の状況

制御システムは電力、ガス、石油パイプライン、水道、通信、大型プラントなど米国の多くの重要インフラで使われている。制御システムはもともと独立した専用システムとして設計され、使用される製品や技術もベンダ個別仕様のものであった。これらの重要インフラには多くの事業者が関与しているが、各事業者はそれぞれ独自のシステムを採用しており、制御システムのデータのやり取りにはインタフェースやデータ形式のカスタマイズが必要であった。

近年になりコスト削減などの経済性や、状況に応じた迅速なフィールドプロセスの制御というユーザニーズを背景に、システム間の相互接続性の確保が求められるようになった。PC の高性能化、Windows や Linux の普及、インターネットや無線などネットワーク技術の高度化などにより、リモート環境でのリアルタイムのデータ通信ができる技術的環境が整い、制御システム全体において、他事業者システムを含むシームレスなデータ連携が図られるようになった。このような背景により、米国では個別の開発や維持費用が不要である汎用製品の採用、また接続性が担保されている標準プロトコルの採用という、制御システムのオープン化が進展している。

図表 2-4 に、制御システムの構成例を示す。

図表 2-4 制御システムの構成例



資料：JEMIMA 資料ほか各種資料より作成

図表 2-4 に示すとおり制御システムは一般に階層構造となっており、オープン化の進展は階層ごとに差がある。

コントロールネットワークより上位では、EWS（Engineering Work Station）や HMI（Human Machine Interface）用の機器として汎用製品である PC が採用され Windows、Oracle、MySQL、JAVA などの汎用ソフトウェアが搭載されている。

また、ファイアウォールを介して外部と接続している制御情報ネットワークにおいては、情報システムでは一般的なイーサネット、TCP/IP が用いられている。下位のコントロールネットワークやセンサーバスについても、従来のベンダ独自のプロトコルから業界標準のプロトコル採用へと置き換わってきている。しかし、コントロールネットワーク以下の業界標準プロトコルには、提唱ベンダ、地域、仕様などの違いにより、多種多様な規格が存在している。一部の標準規格には、特定の分野でデファクトスタンダードとなっているものもある。図表 2-5 に主なネットワーク規格を示す。

一方、センサやアクチュエータなどのフィールドデバイスは依然としてベンダ個別仕様の製品が中心であり、シリアル接続が用いられているものが多い。製品ライフサイクルも 10～20 年と長いため、すぐにオープン化されるといった状況ではない。一方で、フィールドデバイスは、有線ネットワークの敷設工事費用がかさんだり、可動式機器の場合有線では可動範囲が限られたりすることなどが課題として認識されており、この課題を解決するために、最近ではワイヤレスネットワークの適用が検討され始めている。実際にワイヤレスネットワークが採用可能となるには、従来から指摘されている通信の安定性、盗聴防止などの課題解決が前提となるが、これが実現されれば標準的なプロトコルの採用が進む動きとなる。このことから、フィールドデバイス部分においてもオープン化の方向に向かう動きもあるといえる。

図表 2-5 制御システムの主要なネットワーク規格

分類	名称	推進団体	普及地域	参加団体数	通信速度（bps）	伝送距離
コントロールネットワーク	ControlNet	ControlNet International	欧米	―	5M	1000m/2 ﾉｰﾄﾞ, 250m/48 ﾉｰﾄﾞ, 3000m/光ﾌｧｲﾊﾞｰ
	CAN Open	CAN in Automation	欧米日	15	50k～1M	40m（1M）～1000m（50k）
	FL-net	日本電機工業会（JEMA）	日本	20	10M	500（ﾘﾋﾟｰﾀをつけると 2.1km）
	EtherNet/IP	ODVA	北米、アジア	275	10, 100, 1000 Mbit/s	100m(10Mbps),100m(100Mbps), 100m(1Gbps)
フィールドネットワーク	Modbus	Modbus Organization	米欧	332	max19.2k	12m（RS232C）, 1200m（RS422）
	Modbus Plus	Schneider Electric（仏）	米欧	―	1M	500m×3ﾚﾋﾟｰﾀ
	Modbus TCP	Modbus Organization	米欧	―	10,100,1000M bit/s	―
	Device Net	ODVA	米欧日	871	125k, 259k, 500k	500m（125k）, 250m（250k）, 100m（500k）
	PROFIBUS-DP	PROFIBUS International	米欧日	1200	9.6k～12M	100m（12M）, 200m（1.5M）, 400m（0.5M）, 1km（187.5K）
	PROFIBUS-PA	PROFIBUS International	米欧日	1200	9.6k～12M	100m（12M）, 200m（1.5M）, 400m（0.5M）, 1km（187.5K）
	CC-Link	CC-Link 協会	日本、アジア	525	156k, 625k, 2.5M, 5M, 10M	1.2km（156k）, 600m（625k）, 200m（2.5M）, 150m（5M）, 100m（10M）
	Interbus	INTERBUS Club	米欧日	600	0.5M, 2.0M	ﾘﾓｰﾄﾊﾞｽ間 400m、ﾏｽﾀｰ～ﾘﾓｰﾄ間最大 12km
	Foundation Fieldbus	Fieldbus Foundation	米欧日	120	31.25k, 100M	低速ﾊﾞｽ（ｱﾅﾛｸﾞ代替）1900m, 高速 Ethernet100m, 光ケーブル 2000m
	LONWORKS	LONMARK 協会	米欧日中ほか	500	78k, 1.25M	500-2700m（78k）, 130m（1.25M）
	OPCN-1	日本電機工業会（JEMA）	日本	―	125k, 250k, 500k, 1M	1000m（125k）, 800m（250k）, 400m（500k）, 240m（1M）
センサバス	AS-I	AS-International	米欧日	100	2.5M	100m リピータで 300m
	EC-NET	マイクロネット	国内	4	2.5M/5M	100m
	CC-Link/LT	CC-Link 協会	日本	1000	156k～2.5M	500m（156k）, 100m（625k）, 35m（2.5M）
	CAN	CAN in Automation	欧米日	15	50k～1M	40m（1M）～1000m（50k）

資料：各種資料より作成

2.1.3　制御システムのセキュリティ課題の顕在化

前述のとおり、制御システムは独立した専用システムであることから、セキュリティへの対応はあまり考慮されていなかった。しかし、制御システムにおけるオープン化の進展により、以下のような課題が指摘されている。

【課題１：オープン化に伴う脆弱性リスクの混入】

- 制御システムに汎用製品が採用されるようになった結果、これらの汎用製品におけるハードウェア／ソフトウェアの脆弱性の課題も引き継ぐこととなった。汎用製品の脆弱性関連情報および対策のための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、後述の課題 3 で示すように、可用性重視の観点からは難しく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ことが理由である。
- 標準プロトコルのネットワークを採用することにより、ワームなどのウイルスの侵入や、機密情報漏えいの可能性も生じている。他システムとの接続部にファイアウォールを設置している例は多いものの、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。

【課題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】

- 制御システムのセキュリティに影響を与える問題として、制御システムの長期ライフサイクルがある。制御システムは通常 10～20 年におよび長期間にわたり使用されている。汎用製品やオープンネットワークの採用が進むとはいえ最新のものを使用しているわけではなく、セキュリティ対策も同様に最新のものではないことも十分に考えられる。

【課題 3：可用性重視に伴うセキュリティ機能の絞込み】

- セキュリティに対する考え方に関して、制御システムと情報システムには違いがある。情報システムにおいては機密性（Confidentiality）、完全性（Integrity）、可用性（Availability）という、いわゆる C.I.A の順であるのに対して、制御システムでは可用性が最も重視され、A.I.C の順番で重要とされている。
- 可用性重視の観点から、例えば、制御システムでは一般的に、システム上の負荷となるウイ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、課題 1 で示したように、もし、ウイルスが制御システム内に侵入した場合は、瞬く間に拡散する危険性がある。
- 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 5～10 年は遅れている状況であるとの指摘があるが、このようなセキュリティに対する考え方もその背

景にあると考えられる。

以上のことから制御システムは、もともとオープン化が前提となっている情報システムとは情報セキュリティに対する考え方が異なっていると言える（図表 2-6）。

図表 2-6 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）

資料：各種資料より作成

制御システムの情報セキュリティの課題が顕在化しつつあるといえるが、近年、実際に重要インフラにおけるセキュリティ事案が数例報告されている。また、外部からの制御システムへの攻撃の可能性についても調査が行われ、SCADA システムに脆弱性があることも報告されている。現時点では特定の制御システムが攻撃される可能性は低いと思われているが、以下事例にあるように不特定多数を狙った脆弱性に起因するセキュリティ事案発生の可能性は考えられる。

（1）制御システムへの攻撃可能性調査（Aurora Generator Test）

DHS は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ため、2007 年 3 月 Aurora Generator Test を実施した。実証実験は INL によって行われ、ハッカーによる侵害をシミュレートした結果、SCADA システムに深刻な脆弱性が発見された。実験での制御システムへのサイバー攻撃により、100 万ドルのディーゼル発電機は激しく振動して発煙し、その後機能停止に陥った。発電所のコントロールシステムのリモートアクセスを獲得して発電機を破壊することができてしまうことが実証された。この様子について DHS はビデオを製作し政府機関に配布した。

（2）制御システムのセキュリティ事案例

（i）原子力発電所の制御システムへのワーム侵入

2003 年 1 月、オハイオ州 Davis Besse 原子力発電所でマイクロソフトの SQL サーバを狙った Slammer（読み方：スラマー）ワームが VPN（Virtual Private Network）接

続を介して侵入・感染し、SCADA システムを約 5 時間にわたって停止させた。同施設のプロセス・コンピュータも停止し、再運用までに約 6 時間を費やしたほか、他の電力施設を結ぶ通信トラフィックも混乱し、通信の遅延や遮断に追い込まれた。

発電所のサーバはファイアウォールで外部ネットワークと遮断されていたが、ファイアウォール内部のネットワークに接続した、発電所のコンサルタント会社の端末が感染源となった。感染した Slammer ワームに対するパッチは、その時点で公開されていたが、発電所のシステムには該当パッチがあてられていなかった。これら 2 件が重なったことで、大規模なシステム停止につながった。

図表 2-7　Davis Besse 原子力発電所

資料：NRC（Nuclear Regulatory Commission）

（ii）鉄道の信号管理システムのウイルス感染による運行停止

2003 年 8 月、米国東部の鉄道会社 CSX 社の信号管理システムがコンピュータウイルスに感染し、ワシントン周辺の 3 路線で朝から昼にかけて通勤および貨物列車が停止、ダイヤ乱れが発生する事態となった。当時世界規模で感染が拡大していた W32/Blaster（読み方：ブラスター）ワームタイプのウイルスが原因と見られている。当初は、単純な信号システムの故障と見られたが、その後の調べで信号や配車のシステムなどの重要システムをつなぐネットワーク部分が、ワームによって断絶されたことが原因と判明した。

（iii）Zotob ワームによる自動車工場の操業停止

2005 年 8 月 18 日、ダイムラー・クライスラー（現ダイムラー）の米国にある 13 の自動車工場が単純なインターネットワームにより操業停止となる事故が発生した。

情報ネットワークと制御ネットワークの間にはファイアウォールが設置されていたにもかかわらず、Zotob（読み方：ゾトブ）ワームが制御システム内に入り込み、あっという間にプラント中に広がった（外部から持ち込まれ、制御システムに接続されたノート PC 経由の可能性も指摘されている）。各工場のシステムはオフラインになり、組み立てラインで働く 50,000 人の労働者は作業中断を余儀なくされ、自動車生産が 50 分間停止する状態となった。感染した Windows2000 システムにパッチをあてることで生産を再開したが、部品サプライヤへの感染も疑われ部品供給の懸念も生じ、およそ 1,400 万ドルの損害をもたらした。

2.1.4　制御システムのセキュリティ対策状況

（1）技術的な対策状況

制御システムに対しても、具体的なセキュリティ対策としては、情報システムで用いられているファイアウォールなどによる侵入防止、パッチ、アンチウイルスソフトなどを適用している。また、情報システムとネットワークで接続して制御システムを運用する場合には、セキュリティを高めるため、両システム間へのファイアウォールの設置や、情報システム側から制御システム側へのアクセス禁止機能の搭載など対策を図っている。しかし、前述の通り制御システムは情報システムと要件が異なっており、情報システムにおけるセキュリティ対策をそのまま適用できるわけではない。適用にあたっては、次に示すような制御システムの特性に応じた考慮が必要となる。

まず脆弱性への対応としては、パッチを当てることが主となるが、実際の適用に際しては多くの課題があり、情報システムで行われているように簡単にはできない。まず、パッチを適用してもシステム稼動に問題が無いかの検証が不可欠である。また、ほとんどの制御システムはカスタマイズされており、パッチも個別システムごとに対応する必要がある。したがって、パッチを適用するためには多くの費用と時間（1～2ヶ月かかることもある）を要することから、積極的に対応されているわけではない。

また外部からの侵入防止に関しては、ファイアウォールが多くの制御システムで採用されているが、アンチウイルスソフトについては、システムのパフォーマンスに影響を与える可能性があり、必ずしも全てのシステムに導入されているわけではない。

（2）国、重要インフラ分野における取り組み状況

米国の制御システムにおいて、情報系のセキュリティ対策が本格化したのは、2003年の東海岸における大停電事故がきっかけとされている。インターネットの隆盛期であった当時、通信分野におけるリスクの高さが認識されつつあったが、一方制御システムは従来通り高い安全性が保持されているとの認識が主であった。東海岸大停電の事故原因として当時猛威を振るっていたコンピュータウイルスが取り上げられたことで、事故による社会的影響も大きかっただけに、DOE 主導のもと、徹底的なセキュリティリスク調査が行われた。このような経緯の下で、エネルギーセクタの重要インフラにおけるセキュリティ対策は、DOE 主導で各種推進されている。

また、重要インフラ保護政策を推進する DHS でも、制御システムのセキュリティ強化を図るプログラムである CSSP を立ち上げ、サイバーセキュリティ自己評価ツールの開発やトレーニング実施などの対策を推進している。

その他、エネルギー、水、などの重要インフラセクタでは、制御システム強化に向けたロードマップ策定や対策の検討を行っている。

以下、DHS 主導による CSSP、DOE 主導による National SCADA Test Bed Program

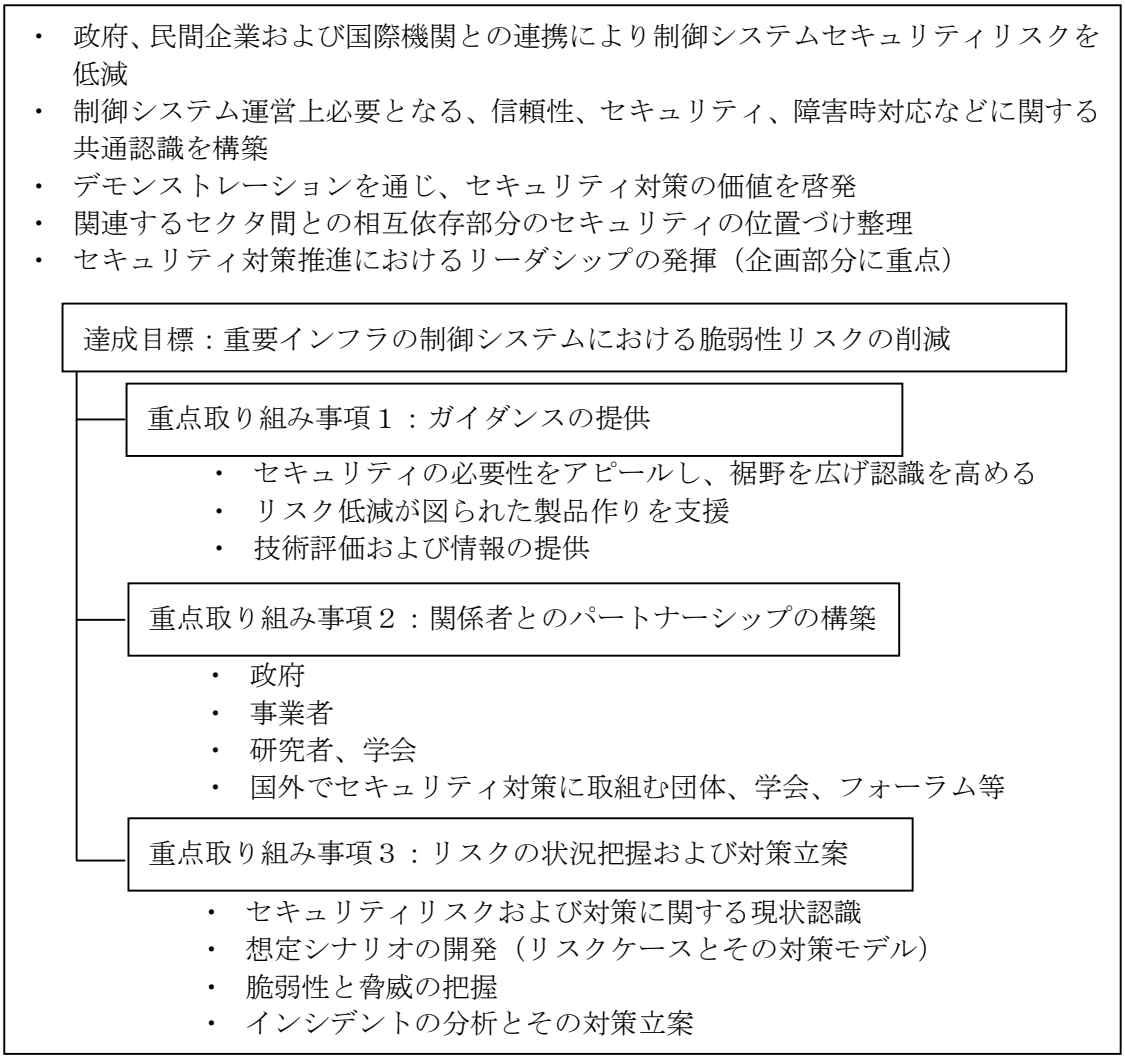
（NSTB）、エネルギー分野におけるセキュリティロードマップについて、それぞれの取り組みを示す。

（i）Control Systems Security Program（CSSP）

米国政府機関である DHS が主体となり進められている、制御システムにおけるセキュリティ対策強化の活動。従来から取り組まれてきた物理面でのセキュリティ対策に加え、近年ではサイバー面への対策にも注力した取り組みが進められている。

本プログラムでは、重要インフラ所有者の 70%から 80%を占める民間企業に対し、政府がイニシアチブをとって民間（事業者、研究者、制御機器ベンダ等）を指導する形でセキュリティ対策を推進する体制を確保している。国家の重要インフラである制御システムにおける脆弱性リスクの削減、および脅威への対応を図るための、国家レベルの対応能力を獲得することが目的とされている（図表 2-8）。

図表 2-8 CSSP のミッションと目的



資料：各種資料より作成

CSSP の活動によって提供される具体的なツールやドキュメントは、制御システム事業者および制御機器ベンダが、自発的にセキュリティ対策に取り組んでいく際に有効な内容となっている（図表 2-9）。

図表 2-9 CSSP の成果物として提供されるツールやドキュメント例

- 制御システム向けセキュリティカタログ（標準開発者への推奨事項を記載）
- 制御システムにおけるセキュリティの自己評価ツール
  （CS2SAT：Control System Cyber Security Self-Assessment Tool）
- CSSP ドキュメント（調査報告、政府・業界動向等）
- 重要インフラおよび制御システム向けのセキュリティカリキュラム
- 制御システム調達時にサイバーセキュリティ対策を織り込んだ要求仕様とするための文例集
- 推奨事例
- トレーニングコース
  例：①Web サイト経由で提供される e-learning 学習コンテンツ
  ②学会、ベンダ主催イベントとの共催で制御システム管理者向け短時間無料研修（1 コース 8 時間）の提供）

活動情報・ツールの公開 URL： http://www.US-CERT.gov/control_systems/

資料：各種資料より作成

CSSP では制御システムの脆弱性評価の取り組みも行われており、製品単位の評価やオンサイト（稼動中システム）の評価に分けられる（図表 2-10）。

図表 2-10 CSSP による製品および稼動中システムの評価事例

【製品単位の評価例】
- Mesto2005
- Emerson
  －Delta V-Bus Technology 2005
  －Delta V SIS 2007
- Siemens
  －Spectrum v1.8 2005
  －Spectrum v4.4 2006
  －PCS7 2007
- Honeywell Experion PKS 2006
- ABB
  －800xA 2007
- Invensys
  －Wonderware 2008

【オンサイトでの評価例】
- シアトルシティ
- 米国交通関連企業
- PacifiCorp
- 干拓局（bureau of reclamation）

他

資料：各種資料より作成

（ii）National SCADA Test Bed Program（NSTB）

CSSP の中で、特にエネルギー関連事業者における制御システムの脆弱性削減にむけた、民間事業者と政府の連携をサポートする活動として、DOE や OE（Office of Electricity Delivery and Energy Reliability）が主体となって取り組んでいる活動としてNSTB（National SCADA Test Bed Program）がある（図表 2-11、12、13）。

この NSTB は INL、SNL 内に設立された実験施設で、実運用環境に近い条件で脆弱性検証試験が行えるサービスを提供している。また、この評価費用の半額は、国が負担するスキームとなっている。

図表 2-11 NSTB が提供するサービス

- ベンダや事業者に対して、脆弱性に関する調査報告を評価し公表
- 制御システムセキュリティに対する裾野を広げる活動と訓練機会の提供（NERC 認証の教育コースを利用し、1800 名以上に対し訓練を実施）
- DHS、NCSD（National Cyber Security Division）、CSSP の活動、サービス向上に向けた情報提供
- エネルギーセクタの制御システムにおけるセキュリティロードマップのアップデート
- 評価結果を受けた対策の検討（リスク/被害の無害化）

資料：各種資料より作成

図表 2-12 NSTB を利用した評価の内容

・制御システムにおける脆弱性ポイントを理解するため、システム周辺との入出力関係、および利用されている技術・プロトコルを明らかにする
・35 の評価を実施
・アセスメントの最初の半年で行う評価は以下
　－研究所内での評価は、平均 800 時間かけ、制御システムおよびネットワークに対して、400 項目の評価を実施
　－オンサイトでの評価は、平均 275 時間かけ、制御システムおよびネットワークに対して、500 項目の評価を実施
　－2,000～6,000 行のプログラムをリバースエンジニアリングを実施
　－1,000～20,000 行のプログラムの脆弱性を評価
　－一度の評価において、1～14 件の成果/発見事項を獲得
　－5～18 件の脆弱性、12～83 件の提言/発見（＝脆弱性のポテンシャルを有する事項）
・制御システムのサイバーセキュリティ被害低減に向け、評価を行った制御システム所有事業者と情報を共有

資料：各種資料より作成

図表 2-13 NSTB を利用した大規模システムにおける評価受査実績

・ 3-ABB Network Manager	・ Siemens
・ 2-AREVA e-terra	・ Telvebt
・ GE XA/21	・ OSI International

資料：各種資料より作成

制御システムにおけるセキュリティ対策を国際的に広げる活動として、重要インフラのセキュリティ対策に取り組むフォーラム「International Electricity Infrastructure Assurance Forum」に参画し、オーストラリア、カナダ、ニュージーランド、英国との協力体制を構築している。

また、より高度な専門家向けのトレーニング機会の提供として「International Watch & Warning Network」が開催される予定（参加はメンバ国限定：2009 年春予定）。本カンファレンスは、DHS と独 Federal Ministry of the Interior の協力によって 2004 年に設立され、15 の加盟国（イタリア、英国、オーストラリア、オランダ、カナダ、スイス、スウェーデン、ドイツ、日本、ニュージーランド、ノルウェイ、ハンガリー、フィンランド、フランス、米国）で構成される。

（iii）Roadmap to Secure Control Systems

制御システムにおけるセキュリティ対策の進め方を示すロードマップの作成が、政府および業界関係者による取り組みとして進められている。先行してエネルギー分野（電気、石油、天然ガス）で、ついで水関連分野での取り組みが開始。エネルギーまたは水分野ごとのワーキンググループが設けられ、成果の共有や、関連組織への情報発信が行われている（図表 2-14）。

図表 2-14 Roadmap to Secure Control Systems（エネルギー分野）における取り組み事項

(i) アライアンスの構築（事業者と運用者、部品ベンダ、工場組織、政府、研究者）

(ii) トピックスの概要整理と優先順位の決定・共有

(iii) ieRoadmap の作成（90 以上のプロジェクトが、ロードマップ内に位置づけられ活動中。内容は Web で共有 →https://www.pcsforum.org/roadmap/ ）

（参考：「ieRoadmap」の「ie」は「Interactive Energy」の頭文字）

(iv) 専門家による検討会の運営

【2015 年 プロジェクト目標最終年度の達成目標】

- 全てのエネルギー分野の制御システムにおいて、完全にセキュアな状況下でネットワークを活用した自動制御、リアルタイム制御が可能
- 次期制御システムのコンポーネントおよびシステムに組み込まれている新技術が、古い制御システムと入れ替わり、端から端までセキュリティ対策が完了
- 制御システムに対して攻撃が行われた場合は、自動的に対策、救済の措置が行われる
- エネルギー分野における事業者、従業員に加え、政府、エネルギー分野の関係者全てが連携し、更なるセキュリティ対策の発展に向け協力した取組みが行われている

資料：Energy Sector Control System Working Group ほか各種資料より作成

エネルギー分野における本取り組みは 2006 年より開始され、10 年計画で課題解決にむけた取り組みを行っている。これは制御システムが、製品のライフサイクルが長いこと、失敗ややりなおしに伴う損失が大きいこと、対象事業者がもれなく対応すべき等といった特性をもつことから、検討・検証に必要な時間をとって確実な対応を図ろうとしているといえる。

具体的な制御システム向けセキュリティ管理ツールとして、脆弱性確認ツールおよびネットワーク管理ツールなどが共有されている（図表 2-15）。

図表 2-15 制御システム向けセキュリティ管理ツール例

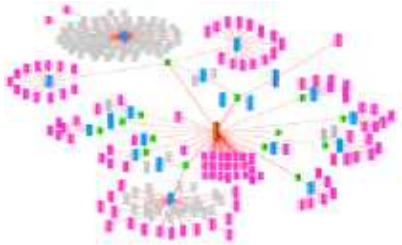
例 1 ：Digital Bond 社提供 “Bandolier”

- Web ベースで提供される ASP サービス
- サイトに自社利用製品を入力すると、現在明らかになっている脆弱性関連情報の確認や、ベストプラクティスとの比較情報を得られる（機器の評価は Digital Bond 社が実施）
- http://www.digitalbond.com（利用会費 100 ドル/年）

画面イメージ

例 2：Sandia National Laboratories 提供
“Advanced Network Toolkit for Assessments and Remote Mapping （ANTFARM）”

- 制御システムのネットワーク構成をビジュアルに表記するためのオープンソースソフトウェア
- NERC CIP 標準を参照
- http://antfarm.rubyforge.org（オンライン下での通常利用は無料）



ネットワーク構成表記イメージ

資料：Energy Sector Control System Working Group ほか各種資料より作成

今後、2015 年に向けた最終目標達成に向け、CEO（経営幹部）へのセキュリティ対策の重要性アピールに向けた活動ほか、以下の取り組みを計画している（図表 2-16）。

図表 2-16 Energy Sector Control System Working Group における今後の取り組み計画

- ロードマップのゴール到達に向けた、研究者とのすり合わせおよび連携強化
- NSTB のレビュー実施および DOE 制御システムセキュリティ検討部門への評価結果のフィードバック
- エネルギー分野企業の CEO への継続的な情報提供によるセキュリティ対策意識の更なる向上獲得
- 工場部門への継続的な情報提供によるセキュリティ対策意識の更なる向上獲得
- ゴール達成に向けた長期的取組みの継続

資料：Energy Sector Control System Working Group ほか各種資料より作成

（iv）I3P のプロジェクト

制御システムセキュリティに関するツールとして開発したものに「リスクマップ」がある。これはシステムのリスクをモデリングし予見するためのツールで、技術者・研究者向けの、多くのスプレッドシートとスクリプトからなっている。このようなツールの知的所有権は I3P ではなくメンバに属している。政府のファンドにより知的所有権を開発したメンバが、他の会社へライセンス供与しソフトウェアを開発している。一方、政府は知的財産権など基本的な権利を持っており、他社が付加した部分のみの費用を支払う。I3P の研究成果の全てに政府はアクセスする権利を有している。

I3P のプロジェクトはツール開発を含んでいる。その一つのプロジェクトがプロセスコントロールである。同プロジェクトは 3 年間取り組まれており、さらに今後 18 ヶ月継続され、その成果としていくつかのツールが出来上がってくる予定である。現在、バッファオーバーフローを検知するツールを開発中である。もう一つのツールは複数のセキュリティポリシーを競合させずに調和させ、照合するツールである。また、プラットフォームを強固にするためのツールとして SHARP（Security-Hardened Attach Resistant Platform）がある。これはコントロールシステムにおいてセキュリティの高いネットワーク環境を提供するためのものである。

（v）民間における認証プログラム

INL による評価は、国が主導する評価であるが、民間企業による制御機器のセキュリティ認証プログラムが Wurldtech 社、Mu Technologies 社により提供されている。

Wurldtech 社が ACHILLES という認証プログラムを、Mu Technologies 社が MUSIC という認証プログラムを提供している。

これらは、いずれも、評価ツールを用いたブラックボックステストを実施して評価するとのことである。また、MUSIC の場合は、Mu Technologies 社自体が評価するのではなく、認証希望事業者にツールを提供し事業者側での自己ツール評価結果により認証を与えるという点が特徴である。

2.1.5　制御システムに対するセキュリティ基準・規格等の策定状況

米国において、重要インフラの安全性（セーフティ）に関する規制は多々あるが、セキュリティに関してはあまりないのが現状である。また、産業界は規制を必ずしも快く思っておらず、自分達で解決するのを好む傾向が強い。しかしながら、業界全体では信頼性やセキュリティに関する基準がない場合もあり、まだ十分とは言えない。

米国政府では NIST が、制御システムに関する政府機関向けの標準（SP800-82）を作成している。これはドラフトであり、2008 年 12 月には最終版を発表する予定であったが 2009 年 1 月 30 日現在発表されていない。SP800-82 は民間に対する強制力は無いが、多くの場面で参考にされている。また、連邦政府へのセキュリティリクワイアメントである SP800-53 にも制御システムに関するものが含まれている。この SP800-53 は SP800-82 のベースラインになっている。一方、IEC では制御システムセキュリティのスタンダード 62443 を作成している。組織は別であるが、これら 2 つの標準は互いにリンクしている。NIST は ISA-SP99 の WG、IEC TC65/WG10 と協力関係にある。

図表 2-17 に米国における制御システムセキュリティ基準・規格等の全体状況を示す。また、これら基準・規格等の概要を図表 2-18 に示す。

（1）標準化団体策定規格の動向

図表 2-17 に示す標準化団体策定規格の中では、IEC TC65/WG10 が策定している IEC 62443（図表 2-17、2-18 の①）、ISA99 Committee が策定している ISA 99（図表 2-17、2-18 の②）、NIST が策定している NIST SP 800-82（図表 2-17、2-18 の③）が、米国において中心となる制御システムのセキュリティ規格と考えられる。

（i）ISA と IEC の動き

ISA（the International Society of Automation）により、次の制御システム向けセキュリティ規格が策定中である。現在 Part1 が発行されており、これは ANSI（American National Standards Institute）の規格となっている。

・ISA99 Industrial Automation and Control Systems Security Standards

また、国際標準化組織である IEC の TC65/WG10 により次の制御システム向け規格が策定中である。

・IEC 62443　Security for industrial process measurement and control　- Network and system security

なお、これら、ISA 99 と IEC 62443 とは、今後一本化されることになっている。規格名称は 2 つ残るが、同一内容の規格となる予定である（2010 年予定）。

（ii）NIST の動き

NIST は米国連邦政府向け基準を策定する米国国立標準技術研究所であり、制御システム向けのセキュリティ規格として、次のものを策定中である。2008 年 9 月に Final Public Draft が発行されている状況である。

・NIST Special Publication 800-82 Guide to Industrial Control Systems （ICS） Security

NIST は、これまで、米国連邦政府の情報システムを対象として種々のセキュリティ規格を策定してきているが、その中で中心の一つとなるものが、次の NIST SP 800-53 である。これは、米国連邦政府の情報システムを対象としたセキュリティ管理策のカタログという位置付けのものである。

・NIST Special Publication 800-53 Recommended Security Controls for Federal Information Systems

（図表 2-17、2-18 の④）

前述した NIST SP 800-82 も、制御システム向けのセキュリティ管理策としては、この SP-800-53 で示されている管理策を採用し、それをどのように制御システムに適用するかという基本的な考え方をガイドとして提供している。

また、この NIST SP 800-53 においても、2007 年 12 月に発行された 2nd edition で、Appendix I として、情報システムを対象とした個々の管理策に対して、それらを制御システムに適用する場合のガイドラインが追加されている。

上記で示したように、NIST が策定する制御システム向けのセキュリティ規格においては、制御システム向けの専用の管理策は記載されていない。これは、セキュリティ管理策として実施する項目そのものは、情報システム、制御システムで変わらず、その適用の仕方が変わるのみである、という考え方に NIST が基づいていると推察される。

また、NIST SP 800-53 は、米国連邦政府、民間を問わず、米国における情報システムのセキュリティ管理策のデファクトという位置付けになっているとの事であり、制御システムに対しても、このような位置付けにある SP 800-53 をうまく活用して、制御システムのセキュリティ対策の普及を図ろうという NIST の思惑があるのではないかと推察される。

なお、NIST は、2001 年に PCSRF（Process Control Security Requirements Forum）を設立し、この PCSRF にて、制御システムを対象として、ISO/IEC 15408 で規定されているプロテクションプロファイルを策定している。

・System Protection Profile for Industrial Control Systems （SPP-ICS）
（図表 2-17、2-18 の⑤）

しかし、この SPP-ICS は 2004 年以降改定されておらず、NIST へのヒアリングでは PCSRF の活動も休止状態であり、PCSRF の活動は ISA 99 Committee の活動に統合されている状況との事である。

図表 2-17 に示すように、NIST は、ISA99 Committee、IEC TC65/WG10 と協力関係にある。NIST が、ISA99 Committee、IEC TC65/WG10 と協力しながら制御システムセキュリティ規格策定に関する活動を推進していることより、一本化される ISA99 及び IEC62443 と、NIST SP 800-82 との関係も今後、整理されていくものと想定される。

（iii）その他関連する動き

情報系の世界でセキュリティ基準の基本となっている国際標準である、ISO/IEC 27000 シリーズ（27001、27002 他）（図表 2-17、2-18 の⑥）及び ISO/IEC 15408（図表 2-17、2-18 の⑦）がある。NIST SP 800-53 は ISO/IEC 27002 も参照しており、また、SPP-ICS は ISO/IEC 15408 に基づき策定されたものである。

制御システム対象の基準・規格等においても、情報系において培われたセキュリティ対策の標準である、これら ISO 規格がバックグラウンドとなっていると考えられる。

（2）セクタ基準・規格等の動向

米国においては、Energy Sector（Electric Sector、Oil & Natural Gas Sector）において、次の規格が策定されている。

・電力分野
North American Electric Reliability Council （NERC） Cyber Security Standards
（図表 2-17、2-18 の⑧）
・ガス分野
American Gas Association （AGA） Standard 12, Cryptographic Protection of SCADA Communications （図表 2-17、2-18 の⑨）
・オイル分野
American Petroleum Institute （API） Standard 1164, Pipeline SCADA Security
（図表 2-17、2-18 の⑩）

特に、電力分野の規格である、NERC Cyber Security Standards CIP-002 ～CIP-009 に対しては、2008 年 1 月に、FERC（U.S. Federal Energy Regulatory Commission）が、電力分野事業者に本基準への遵守を要請しており、電力セクタの中で強制力を持つ基準となっている。

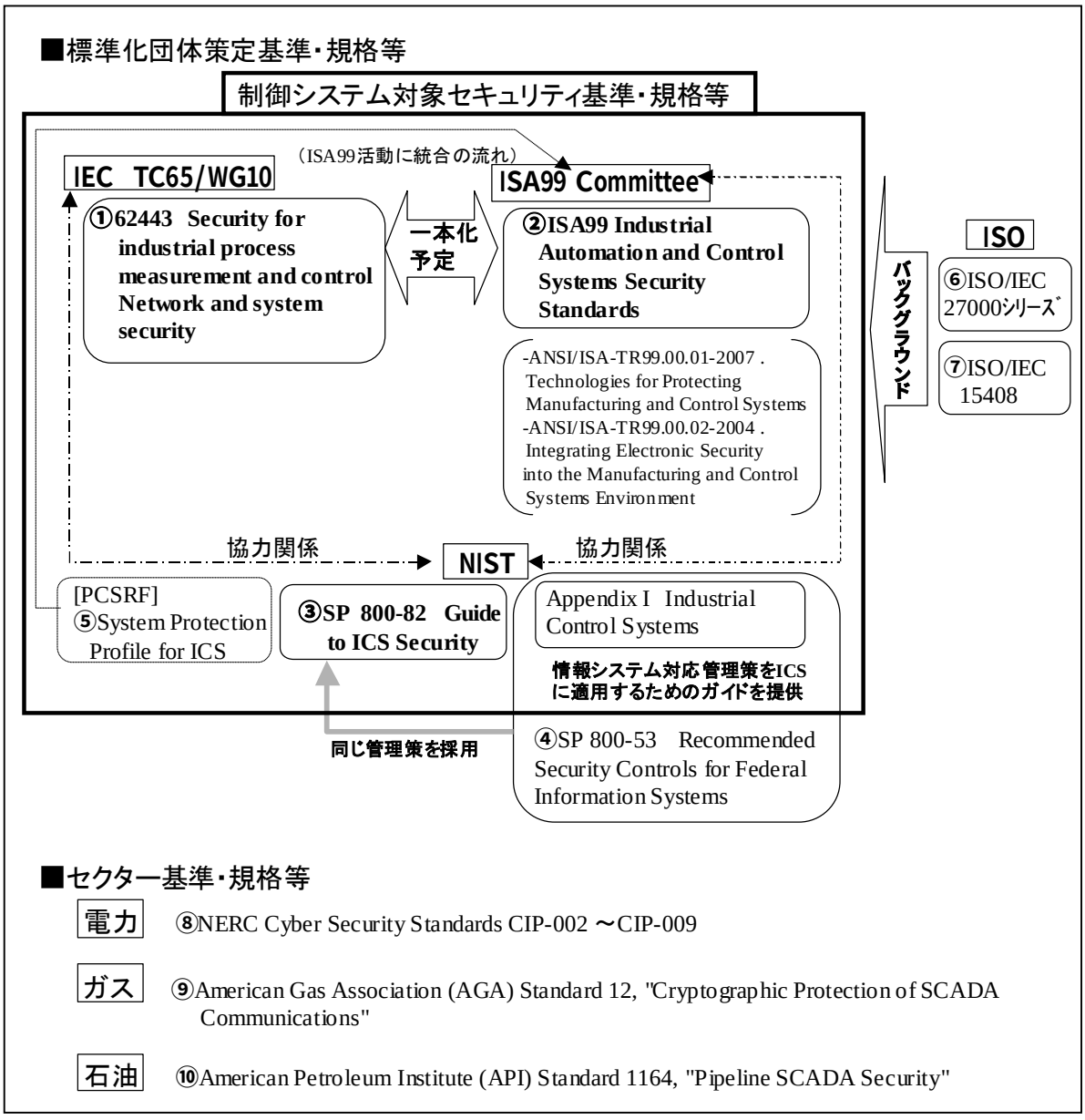
一方、FERC は NERC に対しても、現状の基準に対し、技術的要件面での拡充、遵守のためのガイダンス面での拡充を要請しており、本基準は今後改訂がなされる予定のものである。

なお、上記で示した NIST SP-800-82、ISA99 Part1、NIST SP 800-53、NERC CIP の内容については、付録 2 にて示す。

（3）制御システムにおける安全性とセキュリティの位置付け

制御システムでは安全性が重要な要件であり、このための、Functional Safety（機能安全）についての国際標準が IEC 61508 として制定されている。この 2nd edition において、IEC 61508 において規定されている「hazard and risk analysis」のフェーズで悪意を持った権限外の行動についてもリスクとして考慮することが検討されている。2010 年策定予定との事であり、最終的にどうなるかは分からないが、今後、安全性とセキュリティの総合的な取り扱いがなされるようになることが考えられる。

図表 2-17 制御システムセキュリティ規格 全体マップ



資料：各種資料より作成

図表 2-18 制御システムの情報セキュリティに関する基準

標準化団体策定基準等	
① IEC 62443 Security for industrial process measurement and control. Network and system security	
策定元	International Electrotechnical Commission（IEC） Technical Committees 65（TC65） WG10
策定年	2010 年規格化完了予定
目的・対象	制御システムのセキュリティを確保するための方針、実践策、原則の確立
概要	SP 99 参照（②）
その他	ISA99 と一本化（同一内容、別名称）される予定
② ISA99 Industrial Automation and Control Systems Security Standards	
策定元	ISA
策定年	Part1 が 2007 年 10 月発行。2010 年規格化完了予定
目的・対象	セキュアな制御システムの実現のための手順を提示
概要	ISA99 は次の4つのパートから構成される予定 ・ ISA99.00.01. Part 1: Terminology, Concepts and Models（2007 年発行） ・ ISA99.00.02. Part 2: Establishing an Industrial Automation and Control System Security Program（レビュー中） ・ ISA99.00.03. Part 3: Operating an Industrial Automation and Control System Security Program（今後策定予定） ・ ISA99.00.04. Part 4: Technical Security Requirements for Industrial Automation and Control Systems（今後策定予定） また、次の 2 つのテクニカルレポートが発行されている ・ ANSI/ISA-TR99 00.01-2007 Technologies for Protecting Manufacturing and Control Systems ・ ANSI/ISA-TR99 00.02-2004 Integrating Electronic Security into the Manufacturing and Control Systems Environment
その他	IEC 62443 と一本化（同一内容、別名称）される予定
③ NIST Special Publication 800-82 Guide to Industrial Control Systems（ICS） Security	
策定元	NIST
策定年	2008 年 9 月　final public draft 発行
目的・対象	セキュアな制御システムを実現するためのガイダンスの提供
概要	次の内容を示す。 ・ 制御システムの全体像 ・ 典型的なシステム構成 ・ 情報システムと制御システムとの違い ・ 制御システムに典型的な脅威と脆弱性 ・ 推奨されるセキュリティ管理策のリストと制御システムに適用する際のガイダンス
その他	セキュリティ管理策は NIST SP 800-53 のものを用い、NIST 他基準と整合性が取れるようになっている。
④ NIST Special Publication 800-53 Recommended Security Controls for Federal Information Systems	
策定元	NIST
策定年	2007 年（2nd edition）
目的・対象	・ 連邦政府向け情報システムのセキュリティ管理策を選択するためのガイドラインを提供 ・ Appendix I （Industrial Control Systems）に制御システムを対象としたセキュリティ管理策のガイダンスを 2nd edition にて追加することにより、制御システムオーナーにも、本ガイドの情報システム向け推奨セキュリティ管理策を有効に活用してもらうことを目的とする。

（続き） ④ NIST Special Publication 800-53 Recommended Security Controls for Federal Information Systems	
概要	Appendix I では、各セキュリティ管理策に対し、次のガイダンスを追加。 ・ ICS Tailoring Guidance 情報システム向けのコントロールを制御システムの特徴に合わせて補う情報 ・ ICS Security Control Enhancements 制御システムの要件に応じたコントロールの強化についての情報 ・ ICS Supplemental Guidance コントロールとそのエンハンスメントを制御システムに適用する際の補足的情報
⑤ System Protection Profile for Industrial Control Systems（SPP-ICS）	
策定元	Process Control Security Requirements Forum（PCSRF）
策定年	2004 年
目的・対象	制御システムへのセキュリティ要件のベースラインとなることを目的
概要	制御システムを対象として、ISO/IEC 15408 で規定されているプロテクションプロファイル（PP）を作成したもの
その他	PCSRF は 2001 年に NIST が設立。現在は活動しておらず、主要メンバは ISA99 で活動（NIST ヒアリング情報）。
⑥ ISO/IEC 27000 シリーズ	
策定元	ISO
策定年	基本となる 2 規格は 2005 年発行。他は策定中
目的・対象	情報分野を対象とした ISMS（Information Security Management System）構築のための要求事項、ガイダンスを提供することを目的
概要	次の 2 規格が基本となる基準 ・ ISO/IEC 27001 Information technology - Security techniques . Information security management systems - Requirements（2005 年発行）[情報セキュリティマネジメントシステム－要求事項（JIS Q 27001）] ・ ISO/IEC 27002 Security Techniques - Code of Practice for Information Security Management（2005 年発行）[情報セキュリティマネジメントの実践のための規範（JIS Q 27002）]
その他	上記以外に下記を含むシリーズ化がなされる。 ・ ISO/IEC 27000 ISMS Overview and Vocabulary ・ ISO/IEC 27003 ISMS Implementation Guidance ・ ISO/IEC 27004 Information Security Management Measurements ・ ISO/IEC 27005 ISMS Risk Management
⑦ ISO/IEC 15408, Information Technology - Security Techniques - Evaluation Criteria for IT Security	
策定元	ISO
策定年	2005 年
目的・対象	製品、システムを対象として、技術面でのセキュリティ対策が適切に設計され実装されていることを評価、認証するための認証基準
概要	次の3つのパートから構成される。 ・Part1：概説と一般モデル ・Part2：セキュリティ機能コンポーネントシステムや製品が満足すべきセキュリティ機能を機能要件として記載 ・Part3：セキュリティ保証コンポーネント Part2 の機能要件から選択された機能が正しくシステムや製品に実装されていることを保証するために確認すべき項目を保証要件として記載
その他	・ Common Criteria for Information Technology Security Evaluation Version 3.1 が、CCMB（CC Maintenance Board）により 2006 年発行済み。今後 ISO 化される予定。 ・ 現在の評価・認証制度では認証基準として CCVersion3.1 が用いられている。

セクタ基準・規格等	
⑧ NERC Cyber Security Standards	
策定元	North American Electric Reliability Council（NERC）
策定年	2006 年
目的・対象	発電設備と伝送システムに対するセキュリティリスクを低減するため
概要	次の各項目について、要件、要件に適合ための手段、適合性モニタリングプロセスについて示す。 ・ CIP-002 Critical Cyber Assets ・ CIP-003 Security Management Controls ・ CIP-004 Personnel and Training ・ CIP-005 Electronic Security ・ CIP-006 Physical Security ・ CIP-007 Systems Security Management ・ CIP-008 Incident Reporting and Response Planning ・ CIP-009 Recovery Planning
その他	電力セクタで強制力を持つ基準。今後改定される予定。
⑨ American Gas Association（AGA） Standard 12, Cryptographic Protection of SCADA Communications	
策定元	American Gas Association
策定年	2006 年に Part1 発行。Part2 はレビュー中。Part3、4 は今後策定
目的・対象	・ サイバーインシデントからSCADAコミュニケーションを守るための推奨方策を示す。具体的には、暗号化による SCADA コミュニケーションの防護のための推奨実践策を示す。 ・ 推奨方策の提示により、SCADA システムオーナーの負荷を減らすことを目的とする。
概要	次の 4 つのパートから構成される予定。 ・ AGA 12-1 Background, Policies and Test Plan（2006 年 3 月　発行） ・ AGA 12-2 Retrofit Link Encryption for Asynchronous Serial Communications（レビュー中） ・ AGA 12-3 Protection of Networked Systems（今後策定） ・ AGA 12-4 Protection Embedded in SCADA Components（今後策定）
その他	上下水システムなど他の SCADA ベースの配送システムに適用可能。
⑩ American Petroleum Institute（API） Standard 1164,　Pipeline SCADA Security	
策定元	American Petroleum Institute
策定年	2004 年
目的・対象	・ オイルと天然ガスパイプラインのオペレータが SCADA システムの integrity と security を管理するためのガイダンスを提供する。 ・ 中小クラスで限られた IT リソースのパイプラインのオペレータをターゲットとする。
概要	SCADA システムセキュリティのための実践策を提供するとともに、SCADA システムによるパイプラインオペレーションのセキュリティを向上する手段として以下を提供 ・ SCADA システムのインシデント発生可能性の識別と分析のためのプロセス ・ コアとなるアーキテクチャの堅牢化のための実践策 ・ 推奨実践策の提示
その他	オイルと天然ガスだけでなく、多くの SCADA システムに適用可能。

資料：各種資料より作成

2.1.6　制御システムに関する脆弱性関連情報の公開状況

情報システム全般における脆弱性や脅威に関する情報は CERT/CC から配信されており、その中に制御システムの脆弱性関連情報も含まれておりデータベース内で公開されている。CERT/CC からの情報を活用し、米国では US-CERT が自国内向けに情報発信を行っている（図表 2-19）。しかし制御システムに関する脆弱性や脅威に関する情報は公開されているが件数は 15～20 件しかなく、パッチがあるものに限られているため、利用者は制御システムのセキュリティに関して適切な情報を得られていないと感じているとの指摘がある。公開データベースに情報が蓄積されない理由としては、脆弱性が発覚した際には、制御機器ベンダから直接事業者へ情報提供および対策処置が行われるため、公開情報に対する必要性が低いという背景がある。制御機器ベンダは脆弱性関連情報や脅威に関する情報を公開することにより、企業の信頼性やブランドに傷が付くと考えており、実際には、公開されている以上に該当事案があるのではないかとの指摘がある。脆弱性関連情報が確認された場合は、制御機器ベンダがユーザグループに直接知らせており、制御機器ベンダが脆弱性関連情報を公にリリースすることはほとんどないのが実態である。

SCADA システムベンダ間など制御システム関係者どうしの情報共有に関して、英国では CPNI（Centre for the Protection of National Infrastructure）の Information Exchange があるが、米国では PCSF などのフォーラムを利用している。

図表 2-19 US-CERT で公開されている制御システムの脆弱性関連情報の例

資料：US-CERT（http://www.us-cert.gov/）

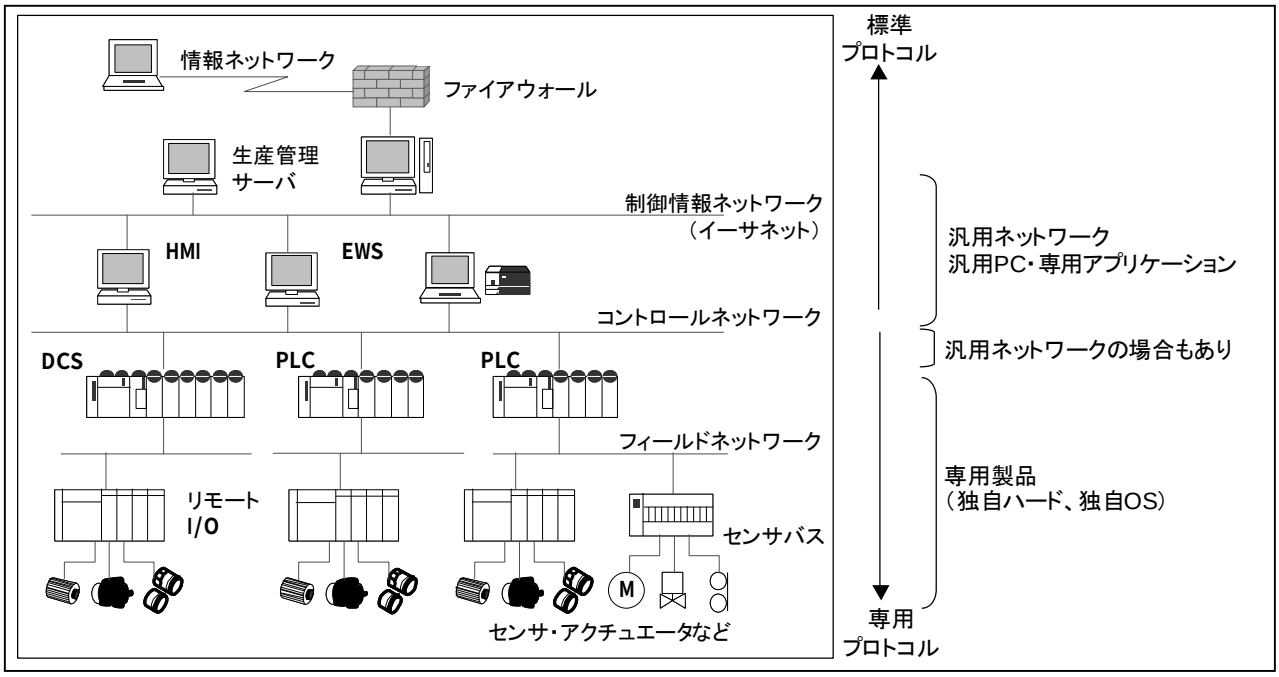
2.2.国内における状況

2.2.1　制御システムにおけるオープン化の状況

日本の重要インフラ分野で利用されている制御システムにおいては、事業者ごとの独自仕様でシステム構成されており、情報システム分野のような業種別パッケージという共通化は見られない。しかし、システムの部品として採用されるサーバ、クライアント、ネットワーク機器などについては、汎用製品の採用が進展している。オープン化の進み具合において日米間で差があるが、システム構成パターンに差異はない（図 2-20）。

汎用製品の採用にあたり、制御機器ベンダ側では汎用製品のライフサイクル（数ヶ月～数年）と、制御システムのライフサイクル（10～20 年）の差異への対策として、制御機器ベンダ側で保守部品の長期保管や、顧客への部品交換促進（ディスクなどの消耗品）を実施している。

図表 2-20 制御システムの構成例



資料：JEMIMA 資料ほか各種資料より作成

制御システムのネットワークに関しても、独自のプロトコルから業界標準プロトコルの採用が広がっている。しかし、前述（図表 2-5）のように多くの業界標準が存在していることと、同じネットワークを採用していてもデータ形式などに違いがあることなどから、機器のマルチベンダ化や他の制御システムとの接続にはインタフェースの改造が必要となり、あまり行われていない状況である。

2.2.2 制御システムのセキュリティ課題と対策

（1）制御システムのセキュリティ課題

日本では、制御システムはベンダごとの個別仕様が中心で、他システムと分離された独立性の高いシステムである。そのため、情報セキュリティは必ずしも明確に認識されていないが、制御システムへの汎用製品と標準プロトコルの採用は進展していることから、米国における場合と同様のセキュリティ上の課題を抱えていると言える（図表 2-21）。

図表 2-21 情報セキュリティ課題の視点で捉えた制御システムの特徴

課題１：オープン化に伴う脆弱性リスクの混入 課題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 課題３：可用性重視に伴うセキュリティ機能の絞込み

（2）制御システムにおいて情報システムのセキュリティ対策が採用されない背景

制御システムにおいて、情報システムでは一般的なセキュリティ対策が採用されていない背景には、制御システムは情報システムにみられるセキュリティリスクとは分離されており安全である、という共通認識が存在している状況がある。一方で制御システムをとりまく環境は変化しており、従来の考え方、取り組み方ではセキュリティを確保できなくなっているという指摘もあがった。

以下に日本での調査で得られた制御システムに対する共通認識と、その認識に対して考慮すべき事項について整理する（図表 2-22）。

図表 2-22 情報セキュリティ課題における共通認識および考慮すべき事項

	セキュリティ課題における共通認識	考慮すべき事項
1	制御システム管理者は、現在のシステムを把握できている	・ 悪意を持ったハッカーやアタッカーは日々変化し続けている ・ システム部品（コンポーネント）の詳細（コーディングレベル）検証は不十分 ・ マルチベンダ化が進むと、事業者や取りまとめベンダにとって全システム部品の詳細検証は困難となる ・ 接続している情報システムとの運営管理上の連携は薄い
2	制御システムへの攻撃者は、制御システムに関する知識は持っていない	・ 利用されているパスワードが弱い（平文、容易に想像できる、変更間隔が長い等） ・ システム上を流れるデータは平文であり流出データの解読は容易

	セキュリティ課題における共通認識	考慮すべき事項
		・ 内部者による悪意のある、または偶発的な操作ミスなどによる障害リスクが存在 ・ 制御システムには、仕様が一般公開されている機器、プロトコルが含まれる
3	制御システムには攻撃者がアクセスすることはできない	・ 情報システム経由で攻撃が及ぶ恐れがある
4	制御システム上を流れるデータは、機器を制御する数値であり、データ自身が売買されるような価値は持たないため、盗聴、漏えいリスクはない	・ 制御システムから情報漏えいがあった、という事実があれば、市場での企業価値の下落、取引先からの契約停止などの経済的被害が発生する可能性がある
5	入退館管理や、外部 PC の接続制限など、物理セキュリティ対策で補えている	・ 未熟練労働者による操作ミスなど故意でない操作が原因となる可能性が存在 ・ 内部関係者による悪意ある攻撃の恐れがある
6	制御システムのうち、汎用機器および技術が利用されているのはモニタリング部分であり、汎用機器および技術部分でセキュリティリスクがあっても、制御機器部分への影響は少ない	・ 制御システム全体が複雑化しており、モニタリング機能がない状況下では実質制御機器の運転が不可能なケースが増加

資料：ヒアリング他資料より作成

（3） 制御システムにおけるセキュリティ対策の取り組み事例

（i） 内閣官房情報セキュリティセンター（NISC）による重要インフラのセキュリティ政策

日本では、内閣官房情報セキュリティセンター（NISC）が中心となり、重要インフラ[2]の情報セキュリティ確保に向けた政策を推進している。2006 年に「重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針」が発表され、重要インフラにおける IT 化の進展や相互の依存関係の増大に伴う、情報セキュリティ対策強化の必要性から、重要インフラ事業者等において分野ごとに安全基準を策定し、自ら検証することを求めている。この安全基準は継続して、見直しと検証が行われている（図表 2-23）。

なお、上記 NISC 活動は、重要インフラ事業者として提供する IT に関わるサービスの継続を主眼としており、分野によっては制御システムも含まれるが、現状では、制御システムに対するセキュリティを直接対象としたものとはなっていないのではないかとの検討会での指摘があった。

[2] 日本では、重要インフラとして、「情報通信」、「金融」、「航空」、「鉄道」、「電力」、「ガス」、「政府・行政サービス」、「医療」、「水道」、「物流」の 10 分野が指定されている。

図表 2-23 重要インフラ事業者分野の安全基準一覧(2008 年 2 月時点)

分野		安全基準等の名称
情報通信	電気通信	電気通信事業法、電気通信事業法施行規則、事業用電気通信設備規則等(関連する告示を含む) 情報通信ネットワーク安全・信頼性基準 電気通信分野における情報セキュリティ確保に係る安全基準(第1版)
	放送	放送における情報インフラの情報セキュリティ確保に関わる「安全基準等」策定ガイドライン
金融		金融機関等におけるセキュリティポリシー策定のための手引き 金融機関等コンピュータシステムの安全対策基準・解説書 金融機関等におけるコンティンジェンシープラン策定のための手引書
航空	航空運送	航空運送事業者における情報セキュリティ確保に係る安全ガイドライン
	航空管制	航空管制システムにおける情報セキュリティ確保に係る安全ガイドライン
鉄道		鉄道分野における情報セキュリティ確保に係る安全ガイドライン
電力		電力制御システム等における技術的水準・運用基準に関するガイドライン
ガス		製造・供給に係る制御系システムの情報セキュリティ対策ガイドライン
政府・行政		地方公共団体における情報セキュリティポリシーに関するガイドライン
医療		医療情報システムの安全管理に関するガイドライン第2版
水道		水道分野における情報セキュリティガイドライン
物流		物流分野における情報セキュリティ確保に係る安全ガイドライン

資料:NISC

また、2008 年 6 月に発表した政策「セキュア・ジャパン 2008」では、「持続的な情報セキュリティ対策の推進体制の構築に向けた基盤整備」として、「情報処理基盤の安全性等の確保(経済産業省)」が必要であるとしている。具体的には、「サイバー攻撃の局所化、攻撃手法の洗練化・隠蔽化、攻撃の対象となるシステム(制御システム等)の拡大に対応するため、攻撃に利用される技術、手法等に関する分析能力の強化を推進するとともに、国内外の産官学の関係組織間におけるマルウェア検体、検知情報、脆弱性関連情報、分析技術・ツール等の共有体制の整備を図る。またインシデント対応支援や IT 製品・システムの開発者に対するセキュアな製品開発手法や検証手法に関する情報提供、イントラ管理者、IT 利用者等に対する普及啓蒙活動や時代に即応した技術的対応策の開発等を通じて、適切な情報処理環境の整備を図る。」としている。

（ii）独立行政法人 情報処理推進機構（IPA）による取り組み

情報処理推進機構（IPA）は、IT の安全性向上に向けた情報セキュリティ対策の強化の観点から、技術・人材の開発や、オープンなソフトウェア基盤の整備等の取り組みを行っている。活動の一環として制御システムにおけるセキュリティ対策に着目し、「大規模プラント・ネットワーク・セキュリティについて（2000 年）」や、「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（本調査：2008 年）」、「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（2008 年）」などに取り組み、関係者共通の課題把握や問題提起、対策にむけた啓発活動を推進している。

（iii）JPCERT コーディネーションセンター（JPCERT/CC）による取り組み

JPCERT/CC では、CERT/CC や欧州 CPNI など海外で捕捉された脆弱性関連情報を日本の窓口として受け取り、主に日本国内のソフトウェア製品開発者へ展開する活動を行っている。国内で発見された脆弱性関連情報は、IPA などを経由して JPCERT/CC に集められる。集められた情報の展開は、脆弱性関連情報の分析結果より該当するソフトウェア製品を開発する事業者への連絡に加え、JVN（Japan Vulnerability Notes）という脆弱性関連情報を提供する Web ポータルサイトを通じて広く公開されている。そのうち制御監視系システムプロトコルにおける脆弱性の情報公開は 10 件行われている（2007 年実績）。

また重要インフラ事業者等の特定組織向けへの脆弱性対策支援として、制御監視系システムプロトコルの脆弱性調査（2008 年）を実施。インターネット定点観測システム[3]などとあわせ、国内向けに技術情報を配信し、注意喚起や情報共有体制の維持・拡大に取り組む。

JPCERT/CC は広く情報システム全般を対象にした活動を行っているが、近年重要インフラにおけるセキュリティに着目し、技術情報調査やセミナーを通じた関係者の意識を高める活動に取り組んでおり、2009 年には更に踏み込んで制御システムに特化した「制御システムセキュリティカンファレンス」を開催する。

（iv）日本電気計測器工業会（JEMIMA）による取り組み

JEMIMA は制御システムで採用されている機器を含む電気計測器の製造・販売等に携わる企業により、2005 年に 6 社により設立された工業会である。

その中にあるセキュリティ調査研究 WG では、製造業分野におけるセキュリティ標準化動向、技術等の調査・研究活動を進め、会員企業および事業者にフィードバックすることを目的とした活動を行っている。

具体的な活動例としては、ISA SP99TR（Technical Report）2 を利用したセキュリテ

[3] インターネット定点観測システム（ISDAS）：脆弱性インシデントの予測と捕捉を目的に、ネットワークトラフィック情報の収集分析や、定期的なセキュリティ予防情報の提供を行うシステム。

ィ対策の実践や、PCSFR の SPP-ICS Ver1.0 を利用したセキュリティ要件の分析および役割分担（機能で切り分けた原因の分析、および対応者の特定）が簡便に行えるツールの開発などが挙げられる。

（v）電気事業連合会による取り組み

電気事業連合会では、電力供給に関わる制御系システムにおける情報セキュリティの強化に向け、電力系統の監視等に極力影響を及ぼさないよう、以下のような必要な対策を講じているとしている。

①制御システム構成面の対策

- 制御系システムの多重化（同一システムの重複設置）
- バックアップ化（設置箇所被災時の代替場所での対応等）
- 電力会社専用の通信ネットワーク（電力保安通信網）の利用
- インターネット等外部ネットワークとは、直接接続しない　等

②運用・体制面の対策

- 24 時間 365 日でシステムの稼働状況を監視
- システム障害発生時、現地技術員による監視・操作の実施
- 厳格な入退管理、システム利用権限付与等によるシステム利用者の制限
- 訓練、教育の実施　等

（vi）電力中央研究所における制御システムセキュリティの検証

財団法人電力中央研究所（電中研）では、電力、エネルギー、環境問題などをテーマに種々の研究を行っており、その一環として電力事業者の制御システムのセキュリティに関する研究も実施している。研究成果は電力事業者に活用されているほか、報告書として電中研のホームページ（http://criepi.denken.or.jp/index.html）で一般向けに公開されている。

2.2.3　セキュリティ標準規格への対応

日本国内においては、事業者ごとの独自システム仕様を実現する手段（採用製品）が、結果的に標準品や業界デファクト品になることはあっても、事業者から明確な要求仕様として示されることは少ない。したがってセキュリティへの対応も、制御機器ベンダごとに異なっている。一方、国内の制御機器ベンダにおいて米国等の海外向けに製品を輸出する場合には、海外におけるセキュリティ認証への対応が応札条件となることもあり、認証の取得が必要となるケースが発生している。

セキュリティに関する規格認証については、現状では海外の認定事業者で実施せざるを得ず、資料の英語化対応等の工数負荷、ならびに独自技術の全面開示に伴う技術情報の漏えいリスクなど、負荷が大きいことから余り進んでいない。制御システムの市場性（新興国を中心とした需要増加）を考慮すると、グローバル対応製品の育成支援は重要な観点であり、日本における認証機構の設立は、検討の価値が高いのではないかとの指摘もあり、今後検討するべき課題と考えられる。

社団法人 日本電気計測器工業会（JEMIMA）では SICE（The Society of Instrument and Control Engineers：社団法人計測自動制御学会）、JEITA （Japan Electronics and Information Technology Industries Association： 社団法人電子情報技術産業協会）と共同して、生産制御システムの「セキュリティ規格とライフサイクル」を中心とした調査・研究を進め、SICE での講演、「計測展 2008 OSAKA」でセミナーを開催する等の普及活動を行っている。この活動の中で、2.1.5 で示した、ISA99、IEC 62443、SPP-ICS 規格の調査を行っており、その調査結果も発表している。

2.2.4　制御システムに関する脆弱性関連情報の公開状況

制御システムの情報セキュリティに対する認知度は、従来個別システムであったため必然性が低かったことから、依然として低い状況である。また、制御システムにおける情報セキュリティの重大事案が日本国内ではあまり報告されていないことも、一因と考えられる。しかしながら、海外における制御システムへの情報セキュリティ攻撃などの事例は、数多く報告されるようになっており、情報セキュリティ対策に向けた取り組みも進められていることから、認知度向上に向けた取り組みを今後進めていく必要があろう。

制御システムの脆弱性関連情報は、JPCERT/CC が独自情報や各国の CERT/CC からの情報をもとに公開しており、公開件数は増加傾向にある。2008 年に JVN で公開されている制御システム関連の脆弱性関連情報は次の 7 件である（2009 年 1 月 30 日時点）。

・2008-1-28　JVNVU#180876 GE Fanuc Proficy Information Portal が認証情報を平文で送信する問題
・2008-1-28　JVNVU#308556 GE Fanuc CIMPLICITY HMI にヒープバッファオーバーフローの脆弱性
・2008-1-28 JVNVU#339345 GE Fanuc Proficy Information Portal が任意のファイルをアップロードおよび実行を許可する問題
・2008-5-7　JVNVU#596268 Wonderware SuiteLink における NULL ポインタ参照の脆弱性
・2008-9-29　JVNVU#343971 ABB PCU400 にバッファオーバーフローの脆弱性
・2008-11-4　JVNVU#981849 Automated Solutions Modbus Slave ActiveX Control における脆弱性
・2008-12-3　JVNVU#976484 DATAC RealWin にバッファオーバーフローの脆弱性

（出典：http://jvn.jp/）

制御システムにおける脆弱性関連情報の公開を進めるにあたっての課題、公開の意義、考慮点としては、以下が挙げられる。

①制御系システムにおける脆弱性関連情報の取り扱い上の課題

（i）調整機関における取り扱い上の課題

- 脆弱性関連情報開示に関する関連コミュニティの風土や理解が成熟していない
- 製品や技術の利用分野が細分化していて見えにくい

（ii）公表された脆弱性関連情報を受け取る側における取り扱い上の課題

- パッチなどの本格的対策を即時に取ることが難しい
- 本格的対策を取るまでのつなぎとして、各利用組織が影響軽減策や運用上の配慮など暫定的な対策を立案する必要がある

②制御系システムにおける脆弱性関連情報公開の意義

・製品に組み込まれる脆弱性の低減

開発者に脆弱性関連情報を（事前および事後に）除去する努力を促し、また、脆弱性事例の知見の共有を促して再発を防ぐという観点から、脆弱性関連情報の公開の意義は高い

③実施にあたって考慮すべき事項（公開時期および公開情報の内容）

- 対策を取る関係者への配慮から、脆弱性関連情報の公開とあわせて対策方法を提供する、情報公開によってパニックや風評が起こらないよう開示対象や手段を選別するなど、情報システムとは異なる特別な工夫をする必要がある。

3. 制御システムと情報システムとの連携でのサービス継続とセキュリティの調査

3.1.制御システムと情報システムとの連携の拡大

制御システムは、発電プラントや製造工場で利用される機器の制御や、機器の状態を監視するセンサ等からの情報収集を目的に発展してきた。そのため、本来は制御対象機器向けに最適化され、高信頼性、高速処理が重要視された、独立性の高いシステムである。また重要インフラの中で利用されている制御システムに着目すると、1 業種の中で事業を展開している事業者数が少なく、かつ事業者内で制御システムを含む運用仕様の多くが非公開かつ独自に設計されてため、ハードウェア・ソフトウェアともに、事業者および納品ベンダによる独自仕様製品で構成されることが一般的である。

しかし近年では、制御システムの大規模化、運用管理の高度化・省力化などの進展に伴い、従来の独立した制御システム（機器とコントローラ群）から、それらをネットワークで接続し、全体をモニタリングしながら制御システム全体をコントロールする、という利用形態に変化している。

その変化要因には、大きく経営的要因と技術的要因の 2 点があげられる。

経営的要因の例としては、制御システム以外の管理・分析システムとの連携による生産性の向上や、分散する制御システム（機器とコントローラ群）の監視・制御を集中化し、省力化することによる原価低減などがあげられる。

技術的要因の例としては、情報システム機器における標準プロトコルの採用拡大および信頼性向上や、汎用製品の採用による接続対象システムの開発および相互接続性検証のコスト・時間の削減などがあげられる。

日本よりも早いスピードで制御システムのオープン化が進展しているのは米国である。米国においては 1 業種の中で複数事業者が事業展開しており、また事業のフェーズごとに事業者が分かれているという事業環境の違いがあげられる[4]。この事業背景の違いにより、日本より事業者同士のコスト・サービス競争が厳しく、制御機器ベンダに対してコスト下げ圧力が高まり、その結果汎用製品や標準プロトコルの採用が速い速度で進展している。加えて複数事業者による協業が必要なため、汎用製品や標準的なプロトコルの採用は、協業関係者全体へのシステム開発・運用コストの軽減につながるなど、メリットが大きい。セキュリティや脆弱性については、汎用製品や標準的なプロトコルの採用によりリスクが高まる側面は否定しないものの、一方で対策につながる製品強化を業界共通負担で、セキュリティ専門家の支援を得て進められるため、総じて高い安全性を確保できるという考え方が普及している。

日本では制御システムは独立性が高く安全が担保されている、という共通認識があるが、今後は米国同様に外部システムとの接続が広まる方向性にあるといえる。

[4] 例えば、日本の電力供給事業の場合、1 電力事業者が発電から配電までを 1 社が担っている。一方米国では、発電事業者と、配電事業者が異なっており、複数事業者による協業は不可避である。

3.2.制御システムから見た情報システムとの連携によるセキュリティリスク

制御システムは制御対象機器向けに最適化され、高信頼性、高速処理が重要視された、独立性の高いシステムという前提で発展してきたため、情報システムとは大きく運用ポリシーが異なる（図表 3-１）。

図表 3-1 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）

資料：各種資料より作成

制御システムは従来技術的およびネットワーク的に、独立したシステムとして運用されてきたが、システム利用の高度化に伴った情報システムとの接続や、共通の汎用機器・標準プロトコルの採用が増加している。

制御システムと情報システムは、ファイアウォールなどを利用し論理的に分離し運用することで、外部ネットワークや情報システムに起因するシステム障害を排除するシステム構成を採用している。しかしファイアウォール等の脆弱性の可能性をゼロにすることは論理的に不可能であるため、物理的に外部ネットワークと接続するチャネルを設けたということは、間接的ではあっても制御システムも外部ネットワーク接続のリスクを抱えることになる。

また、制御システム内で採用されている機器やプロトコルについては、情報システムとの共通性が高まっているため、情報システム側で発生したシステム障害被害の制御システム側への拡大や、汎用製品や標準プロトコルの採用に伴う脆弱性リスクの混入などが可能性として考えられる。また、業務の観点では情報システムとの連携が高まることで、情報システム側のシステム不具合を原因とした、制御システムのサービス停止の可能性も生じているといえる。

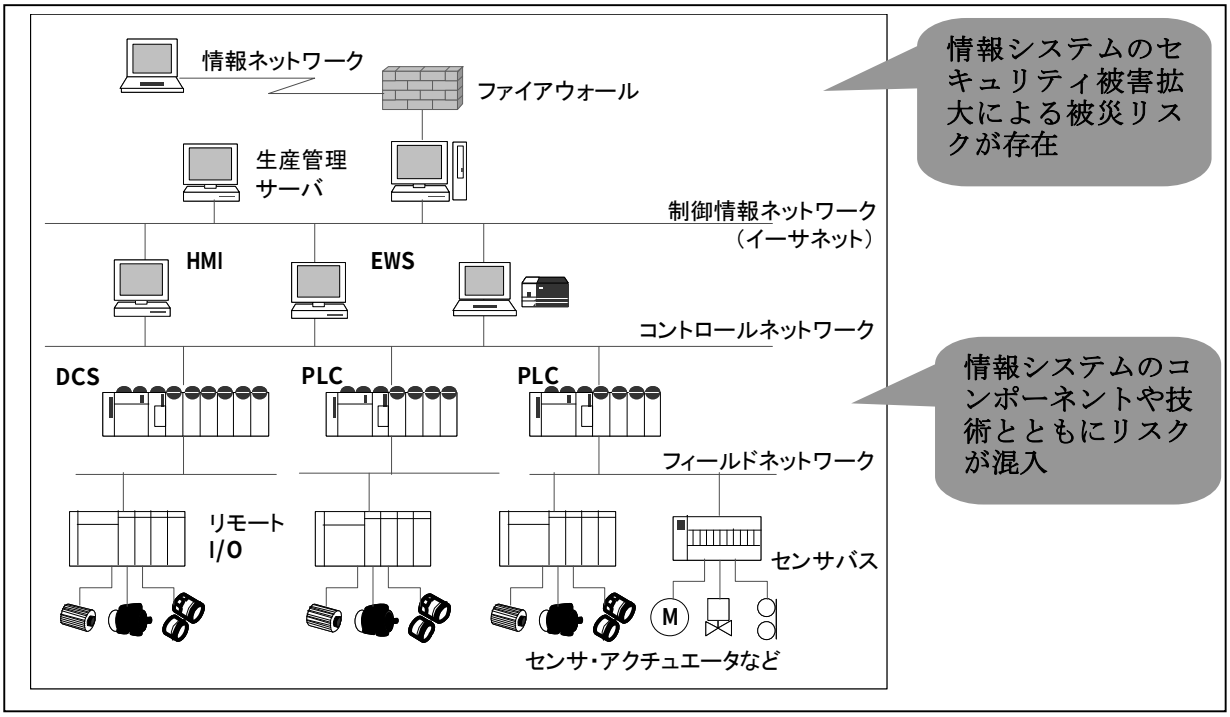
以上の述べたように、制御システムと情報システムの連携が進展することにより、制御システムにおけるセキュリティリスクは高まっているといえる。

3.3.サービス継続を可能とするためのセキュリティ対策の現状と方向性

制御システムにおけるセキュリティ対策が必要とされるようになった背景には、「制御システムに採用されている、情報システムのコンポーネントや技術とともにリスクが混入するようになった」ということと、「情報システムとネットワークを介した接続がとられることで、情報システムのセキュリティ被害拡大によるリスクが存在するようになった」という 2 面がある（図表 3-2）。

制御システムと情報システムは、それぞれの特性からセキュリティ対策に対する考え方や対応方法が異なっており、両者を包括したセキュリティへの取り組みは今後の課題であるといえる。

図表 3-2 制御システムと情報システムの連携によるセキュリティリスク



資料：各種資料等より作成

（1）情報システムのコンポーネントや技術採用増加に伴うセキュリティリスクの混入

制御システムと情報システムは、両者の性質が異なるため、接点を最小化することでリスクの最小化を図っている。制御システム、情報システム双方とも、管理体制およびポリシーともに独立させて、相互干渉していないというケースも多く聞かれた。

一般的に情報システムは、利用するソフトウェアを最新化することで、セキュリティ対策の強化を図るモデルで運用されている。バージョンアップやパッチ提供は日常頻繁に実施され、自動更新を採用する企業も多い。自動更新の対象外とされる PC は、動作検証を要する一部の業務アプリケーション搭載 PC やソフトウェア開発用 PC な

ど限定的であるケースが一般的であり、システム運用上例外的な扱いとされる。その際に、バージョンアップやパッチ対応に必要なデータのダウンロード負荷、更新負荷、OS の再起動対応などが必要となるが、情報システムでは、これらの負荷より、セキュリティ対策強化の優先順位を高く設定している。実際の業務において、上述の対策処理負荷によって致命的な業務効率低下に陥るケースは少ない。

一方、制御システムは高い信頼性と安定的な継続稼動、ミリ秒単位でのデータ連携を必要とするシステムであり、またシステム動作不良は最悪で人命被害を引き起こすことにつながるため、情報システムで行われるセキュリティ対策である、ソフトウェアの更新に伴う動作不安定化や、更新処理によるデータ処理負荷の増加は受け入れ難い（図表 3-3）。

情報システムと制御システムのセキュリティ対策における背景については、日米とも同じ認識であった。

図表 3-3 制御システムと情報システムのセキュリティ対策における背景の違い

セキュリティ上必要となる要件	情報システム	制御システム
技術のサポート期間	3-5 年	20 年以上
パッチ提供サイクル	頻繁・定期的	制御機器ベンダごとに不定期、長期間間隔で実施（公表値なし）
システム上を流れるデータの処理速度	データ受け取り遅延が致命的な被害となるケースは少ない	システム/機器制御にはリアルタイムなデータ受け取り処理が不可欠
可用性（Availability）	再起動は許容範囲	24 時間 365 日の安定稼動が不可欠（再起動は許されない）
セキュリティに関する意識	民間企業、公的機関とも意識が行き渡り、対策されている	発展途上にあり未成熟。情報システム技術の適用で対応するケースもある
セキュリティに関する標準化	標準が確立されている	取り組み始められたばかり
被害の結果	金銭的損失 プライバシー被害	人命損失の可能性

資料：公表資料およびヒアリングより作成

このように、条件が異なる制御システムにおいて、情報システムのコンポーネントおよび技術を利用するということは、制御システム側では十分なセキュリティ対策が取れないことを意味する。

現状の対策としては、外部からの悪意を持ったアタックを防ぐために外部ネットワークとの接続の遮断や、内部システム利用者向けの物理セキュリティの強化（入退館チェック、未許可 PC・デバイスの接続禁止）などを図っている。

（2）外部システムとの接続増加に伴う、情報システムを原因とする被害拡大リスク

制御システムは独立性の高いシステムとして利用されてきたが、近年では需要予測システムや資材管理システムなど、情報システム側で管理、運用されるシステムとのデータ連携を要するケースが増加し、ネットワークで接続して利用されるケースが増加する傾向にある。

制御システムは、セキュリティ対策において情報システムとは異なる考え方や対応方法をとっているため、情報システムから拡大してくるセキュリティ被害が、ネットワークを介して制御システム側に及んだ場合、被害への対策および収拾が困難であるという指摘がある。

この点に関する認識については、日米間で大きな違いは無かった。

以下に情報システムでセキュリティリスクを分析する際の視点を用いて、制御システムにおける脆弱性を分析する（図表 3-4）。

図表 3-4　情報システムのセキュリティリスク観点から分析した制御システムの脆弱性

システム間のデータ連携
・ 制御システムと外部接続システムとの間のデータ交換は平文で行われるケースが多く、盗み見やプロトコルのリバースエンジニアリングの標的になりうる ・ 情報ネットワークと制御システム間の接続において、動的なアドレス割り当てが行われている場合、未承認機器の接続などが容易になり、内部の人が介在した攻撃機会を与えることになる
アクセスコントロール
・ 一般的にパスワード管理が不十分なケースが多い ・ ユーザ名が容易に想像できるケースがある ・ ファイアウォール、IDS の設定が不十分なケースが存在する
利用者認証
・ 一般的に、認証を必要とするアクセス制御を行っているケースは少ない
システムの内容
・ 古いバージョンのアプリケーションやサービスが利用されている。これらは既知の脆弱性を含んでいる可能性がある ・ 現時点で提供されているパッチがあてられることは少ない

プログラムコーディング
・ セキュリティが考慮されたプログラムコーディングになっていないケースがある（例えばデータのオーバフローに対処するためのバッファの確保など）
Web サービス
・ パッチがあてられていないブラウザが利用されている ・ 利用者の認証が不十分（機能/運用が脆弱、または行われていない） ・ セキュリティ対策が不十分なプログラムを利用することで SQL インジェクションなどの脆弱性から悪影響を受ける
情報の管理
・ 関係者内でシステム設定関係の情報が共有されている ・ ユーザ名やパスワードがアプリケーションコード内から読み取ることができる ・ ベンダ情報やバージョン情報が Web サーバや OS から読み取ることができる

資料： 公表資料およびヒアリングより作成

（3） 制御システム側と情報システム側でのセキュリティ対策における認識の不一致

制御システム部門の技術者・運用者と、情報システム部門の技術者・運用者では、図表 3-5 に示すようなセキュリティ対策における認識の食い違いがあることが指摘されている。この点に関する認識については、日米間で大きな違いは無かった。

トータルシステムとしてのセキュリティを実現するためには、制御システム部門と情報システム部門とが、互いを良く理解し連携してゆく体制、環境づくりが必要である。

図表 3-5 情報系と制御系の視点

情報系からの視点	制御系からの視点
• 制御システムは、情報システムに対するセキュリティリスクである • 制御システム側は従わない、協力しない • 制御システムはセキュアではない • 制御システム側は会社のスタンダードを遵守しない • 制御システム側は変化に抵抗する	• 情報システムは、制御システムに対する信頼性リスクである • 情報システム側はオペレーション上の制約を理解しない • 情報システム側はプラントのオペレーションに悪影響を及ぼす手段に固執する

資料：公表資料およびヒアリングより作成

3.4. 日米における対応状況の違い

制御システムおよび情報システム間の違いに起因するセキュリティ対策の状況（不十分さ）については、日米における根本的な違いはない。

日米の違いは、この状況に対する認識と、対策への取り組みにおいて現れる。

この状況を問題視して、国家レベルでセキュリティ対策の取り組みを進めているのが米国であり、今後はこの取り組みが中心となって制御システム利用者側である事業者の意識変革も進んでいくと推測される。

米国においても、事業者分野ごとに認識に差があり、最も進んだ取り組みが行われているのはエネルギー分野（電気、石油、天然ガス）、次いでエネルギー分野の取り組みを受けて水事業分野などが取り組みを進めている状況である。

日本におけるエネルギー分野においては、例えば、電気事業者においては、発電から供給まで一貫して一事業者で対応するというように、各事業者別の取り組みが行われている。今後、市場開放に伴う他事業者の参入などが必要となった場合には、従来とは異なる制御システム運用ポリシーや技術が必要となり、それに伴い新たなセキュリティ対策が必要となる可能性がある。また、エネルギー供給の管理体制がグローバルに行われるようになった場合には、日本国内の運用やシステムの仕様から、グローバル標準仕様への切り替えが要請される可能性もある。

制御システムと情報システムは、それぞれの特性からセキュリティ対策に対する考え方や対応方法が異なっているため、独立したセキュリティポリシーの元で運営されてきた。しかし両者の接点が増加することに伴い、両者を包括したセキュリティリスクの分析および対策の立案は、今後の重要な課題であるといえる。

4. 調査結果から明らかになった制御システムセキュリティの特徴と課題

4.1. 日本と米国の現状についての考察

前章までの米国及び日本の制御システムの情報セキュリティに関する現状の調査内容を下記表にまとめた。汎用製品や標準プロトコルの採用などの面で米国が先行しており、それに伴って制御システムの情報セキュリティ対策においても重要インフラを中心に、政府主導による産官学連携での対策が進められている。

しかしながらセキュリティ対策の必要性に関する認知度などの面では日本と米国ともいずれも不十分であり、今後一層の取り組みが求められる。

日本と米国における制御システムにおけるセキュリティ対策の現状について以下に整理する（図表 4-1）。

図表 4-1 日本と米国における制御システムセキュリティの現状

項目	共通傾向	差異および特徴的な傾向	
		米国	日本
(1) 制御システムのオープン化状況			
	①コントロールセンタ側ではオープン化が進展（PC 等の汎用製品、標準プロトコルの採用） ②フィールド系は個別のシリアル接続が中心	(A) 標準仕様に準拠した制御システム（SCADA）が普及 (B) ワイヤレスネットワークの導入の検討が進展	(a) 社会インフラ系で利用される制御システムにおいては事業者ごとの独自仕様（ハード、通信、業務プログラム含むソフトウェア等）が中心 (b) 日本は米国と比べて、事業者間の連携やコスト削減圧力が少なくオープン化が進んでいない 今後はコスト削減を要求される分野から汎用製品および各種標準プロトコルの採用などのオープン化が進展すると予想
(2) 制御システムセキュリティの課題			
	①制御システムにオープン製品、または汎用製品、標準プロトコルの採用が進んだことで、情報システムと同種類のセキュリティリスクおよび脆弱性を内在する ②製品の長期利用に伴い最新のセキュリティ対策が施せない ③可用性が重視され、搭載されるセキュリティ対策機能が限定的	(A) 情報システムとの接続により自動化されたワームなどの脅威が顕在化（情報システムは外部ネットワークと接続している）	(a) セキュリティ対策不十分を原因とした被害がなく、関係者内のセキュリティ対策への優先順位は低い (b) 日本は米国に比べ重要インフラへの攻撃事例が少ない ［関係者認識例］ ・制御システムは外部と切り離されているため、悪意ある攻撃を受けるリスクはほぼ皆無 ・システムから切り離された情報自体は価値を持たず、情報漏えいや盗難による損害は少ない

項目	共通傾向	差異および特徴的な傾向	
		米国	日本
(3) セキュリティ対策状況			
	①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5～10年の遅れ ②対策は情報システム向けセキュリティと同様の技術を利用し、ファイアウォール、パッチ、アンチウイルスソフトの導入が主 ③多くの制御システムはカスタマイズされており、パッチも個別の事前検証対応が必要（時間と費用が問題）	(A) DOEではSCADAテストベッドを開設し、セキュリティ技術の開発、検証を実施（主にエネルギーセクタ対象） (B) 公開されているセキュリティチェックツールや、第三者機関によるセキュリティテストなどを利用することで、一定のセキュリティレベルが担保されていることを確認・保証可能 (C) 製品認証機関による認証製品を利用することで、一定のセキュリティレベルが担保されていることを確認・保証可能	(a) 事業者または制御機器ベンダ内で共通的に利用可能なセキュリティテスト環境等はない
(4) 脆弱性関連情報の公開			
	①日米とも事業者と制御機器ベンダで必要な情報共有、対策は実施されており、システム維持管理上、公開の必要性は少ない。 ②脆弱性関連情報の収集および公開の仕掛けはあるが、利用度は低い ③制御機器ベンダからの脆弱性関連情報の公開はほとんど無し （NVD（National Vulnerability Database）にも知らせない） ⑤脆弱性関連情報の公開が企業イメージダウンなどへの懸念となっており、脆弱性関連情報を公開したがらない	(A) US-CERTは制御システムの脆弱性関連情報のデータベースを持つが15～20件と少数 (B) 制御機器ベンダが脆弱性関連情報をユーザグループに直接通知、対策し、ユーザグループ内での解決を図る	(a) 情報開示による事業者のメリットはなく、匿名化しても関係者には分かるため、現状では積極的な情報共有および活用は困難 (b) JPCERT/CCでは制御システムの脆弱性関連情報の収集・公開を実施。但し件数は少ない
(5) 推進体制			
	（日米の差異大）	(A) 国家安全保障の観点から政府が主導し、産官学連携のセキュリティ対策体制を構築 (B) (A) の成果であるテスト環境やツールを事業者や制御機器ベンダが活用できる (C) 国立研究所が技術的なバックボーンを担当	(a) 事業者または制御機器ベンダによる独自の対策が行われている (b) NISC他による調査・情報共有の機会が増えつつあるが、まだ少ない

項目	共通傾向	差異および特徴的な傾向	
		米国	日本
(6) 利用者側の認識			
	①利用者側の認識は徐々に高まりつつあるが、まだ不十分	(A) エネルギーセクタ（電気、ガス、オイルなど）、水セクタでは制御システムセキュリティのロードマップ作成（認識は高まりつつある） (B) 一般の製造業における認識は依然低い状況	(a) 全般的に制御システムのセキュリティに対する認識は低い (b) 電中研などの取り組みにあるように電力などの一部セクタでは認識されている
(7) 標準化、規格化			
	（日米の差異大）	(A) NIST では制御システムに関する政府機関向けの標準（SP800-82）を作成 (B) 連邦政府向けセキュリティ対策要件（SP800-53）にも制御システムへの適用を記述 (C) ISA99、IEC62443 など策定中	(a) 標準品や業界デファクト品が明確な要求仕様として示されることは少ない (b) 米国向けにおいては、規格対応が応札条件となるケースがあり、認証取得が進展中 (c) 事業者または制御機器ベンダ（JEMIMA 含む）独自の標準化対応・検証活動に留まる
(8) 情報システムと制御システムの連携			
	①情報システムと制御システムの連携は進展の方向	(A) 表示やモニタリングのためにデータを引き出す目的で統合が進展 (B) 制御システムと情報システムとをつなげることにより業務フローを適切に評価しフィードバックすることが可能	(a) 制御システムと情報システムとの接続は増加傾向にあり、LAN 上のサーバと、生産計画、実績情報、需要予測などとの情報連携が進展 (b) 保守用を含み、外部ネットワークとの直接接続は実施せず (c) 情報システムと制御システムの運用管理は、独立した体制、規定で実施

資料：ヒアリングにより作成

4.2.制御システムの捉え方に関する考察

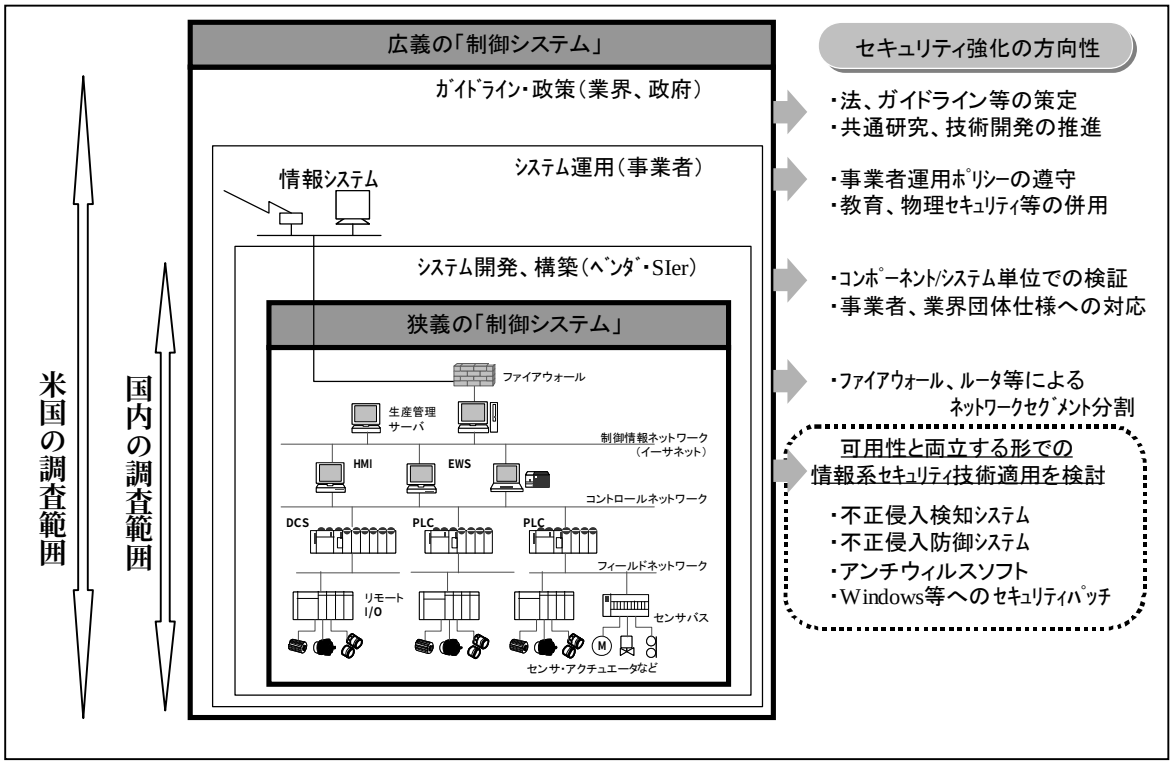
本調査で実施した事実把握調査を元に、検討会で議論した論点について以下に記載する。

4.2.1 「広義の制御システム」の一部としての「狭義の制御システム」の考え方

「制御システム」は、狭義と広義に分けて捉えることができる。本調査では、国内は制御機器ベンダおよび研究者へのインタビュー調査を中心に行ったため、図表 4-2 でいう「狭義の制御システム」に焦点を絞り調査を行った。一方米国における調査は、PCSF というフォーラムを中心に行ったため、業界、政府等による各種施策を含めた「広義の制御システム」に言及した情報を多く得る結果となった。米国での調査結果より、制御システムのセキュリティ向上にあたっては、事業者や制御機器ベンダの枠を超えた、継続的かつ包括的な活動が有効であるという示唆が得られた。

制御システムのセキュリティと IT サービスの継続性を考える場合には、広義の制御システムをターゲットとして、狭義の制御システムはその一部として、リスクの分析と対策の検討を行うことが不可欠である。

図表 4-2 制御システムのセキュリティ強化に向けた検討課題



資料：JEMIMA 資料および各種資料より作成

4.2.2　制御システムにおける「オープン化」の考え方

セキュリティリスクが高まった大きな要因である「オープン化」については、調査開始前は、「情報システムとの連携強化」という、外部との接続増加がセキュリティリスクの重要な要因であるという仮説を設定したが、実際には別の意味があった。

制御システムにおける「オープン化」には、前述の外部との接続増加に加え、「脆弱性リスクの混入や、ウイルス等不特定多数を対象とした攻撃を受けるリスクを持つ汎用製品」と、「インターネット接続等外部ネットワークとの接続性が高いことが外部からのアタックリスクとなる標準プロトコル」が存在することが明らかとなった。但し注意すべき点は、標準プロトコルでもローカル接続を前提とした規格（例：RS-232C）は、セキュリティリスクとはならないため、標準プロトコルといってもセキュリティの観点では区別が必要である。

従って、オープン化に伴うセキュリティリスク対策は、「情報システムとの連携」に加え、「汎用製品」、「標準プロトコル」への対策の観点が必要である。

4.2.3　制御システムと情報システムにおけるセキュリティの考え方

制御システムは、もともとオープン化が前提となっている情報システムとは情報セキュリティに対する考え方が異なっていると言える（図表 4-3）。

図表 4-3 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）

資料：各種資料より作成

制御システムにおいては可用性が最重要視されるため、システム稼動の不安定要素となる、ソフトウェアの更新（最新化およびパッチ対応）やウイルスチェックは採用されにくい。しかし、制御システムに情報システムのコンポーネントが含まれるようになったこと、および情報システムとの連携が拡大しているという状況を考慮すると、事業者のサービス継続性または BCP（Business Continuity Plan：事業継続計画）の観点より、情報システムと整合性を図ったシステム運用の重要性は高まっていく。

4.2.4　制御システムのセキュリティ対策を向上させるための環境の考え方

本調査においては、技術面、運用面の事実把握を中心に実施したが、それらに加えて制御システムをとりまく産業構造の変化や、国家安全保障の観点など、環境面からの視点の重要性が指摘された。

環境としての産業構造については、従来は国内制御機器ベンダが国内事業者向けのシステム提供を行うモデルが一般的であり、それに伴い独自仕様のシステムが普及した。しかし今後はグローバル企業対応に伴う制御システムの世界共通化や、新興国を中心とした販売先のグローバル化など、グローバル化への対応が重要性を増すと考えられる。すなわち標準規格への対応や、製品認証の取得などが、制御機器ベンダにとって競争力を発揮するために重要となってくる。

国家安全保障については、通常運用範囲の制御システムの事故に加え、テロ対策の観点より、国内全体のセキュリティレベルの向上や、実態の把握、リスク管理などにおいて、日本での対策を強化すべきという意見が出された。米国では重要インフラ所有者の 70%から 80%が民間であり、政府がイニシアチブをとって民間（事業者、研究者、制御機器ベンダ等）を指導する形でセキュリティ対策を推進する体制が確保されている。

また制御システムのセキュリティ対策の必要性については、特に現場レベル（システム利用者、管理者、制御機器ベンダ等）では理解されているが、事業者の優先順位上、下位に評価されるためセキュリティ対策が進まない側面があり、解決に向けては事業者経営者層の啓発や、米国のような共通的なテスト環境、技術・ツールの開発などが効果的ではないかという意見が出された。すなわち、事業者や制御機器ベンダの自主的な取り組みだけでなく、国策として制御システムのセキュリティ対策環境の整備が求められる。

4.3.調査結果から導き出される制御システムセキュリティの課題の整理

今回の調査結果および検討会での論点をふまえ、重要インフラの制御システムのセキュリティと IT サービスの継続性を確保する上で、今後検討すべき課題を、大きく（A）技術、（B）運用、（C）環境に分け以下の通り抽出した（図表 4-3）。

図表 4-4 制御システムのセキュリティ強化に向けた検討課題

分野		日本における課題	論　点
(A) 技術	1	既存制御システムにおけるセキュリティリスクの把握/評価	・ 分離独立／独自仕様だけでセキュリティ確保は十分といえるだろうか ・ セキュリティが確保できているという前提を確認する必要があるのではないか
	2	制御システムに利用される汎用製品、標準プロトコルに対するセキュリティリスクの把握/評価	・ 汎用製品、標準プロトコルを使用する際のセキュリティリスクの明確化が必要ではないか ・ 汎用製品、標準プロトコルの脆弱性が制御システム全体に及ぼす影響を評価する必要があるのではないか
	3	セキュリティリスク対策製品の認証/認定制度の整備	・ 認証／認定を受けることにより一定の免責を受けられるなど経営者のインセンティブによる促進を図ることが有効ではないか
	4	共通性の高いセキュリティ対策技術の継続的な調査開発体制の整備	・ 米国同様、政府予算等で継続的なセキュリティ対策知見およびツール類の蓄積、共有が必要ではないか ・ 海外のセキュリティ分析ツールや、テストツールなど、国内での効果的な活用方法を検討する必要があるのではないか
	5	新技術､新標準に対するリスク評価体制の整備	・ 制御システムのコンポーネントとして新しく加わる技術については、業界共通でセキュリティ等検証した方が効率的ではないか
(B) 運用	1	広義の制御システムを対象としたセキュリティリスクの評価と対策のガイドライン確立/評価	・ 人間系／インタフェースの脆弱性を考慮することも必要ではないか（情報系におけるセキュリティ事案の多くは、内部関係者が関与傾向）
	2	実効性の高いセキュリティ監査体制および検証ツールの整備	・ セキュリティを担保するための監査体制の確保および効率化するためのツール開発が必要ではないか
	3	情報システム運用ポリシーとの整合性を確保した､制御システム運用ポリシーの整備	・ 今後生産計画や予測システム等との連携拡大が予測。情報システムとの役割分担の明確化や、整合性のある運用ポリシーの確立が必要ではないか

分野		日本における課題	論　点
	4	制御システムに含まれる機器単位､および対応責任者単位の､リスク管理と対策の整備	・ オープン化が進む中、制御機器ベンダのみならずエンジニアリング会社、事業者など関連する事業者が協調したポリシーの明確化が必要ではないか
	5	セキュリティ対策投資強化にむけた、経営者の理解を獲得するための啓発活動	・ 事業者の経営層に対しセキュリティリスク対策への投資効果などを訴え、適正な費用確保が行われなければ、現場でのセキュリティ対策は進展しない
(C) 環境	1	産業構造の変化に伴う､制御システムセキュリティリスク変化の評価実施	・ コスト低減要求に対応するための汎用製品、標準プロトコルの採用が更に拡大するのではないか ・ グローバル企業向けの制御システムでは、海外仕様への対応が、日本国内でも必要になるのではないか ・ 制御システムの需要の多くが新興国で起こることより、海外向け事業強化を支援する施策が日本経済にとって有効ではないか
	2	国際的な製品認証/認定取得の省力化支援実施	・ 海外で認定を受ける際の費用や、英語による資料作成、申請手続き、現地対応等が企業の負担になっていないか ・ 国内外で異なる仕様製品を開発、保守することで製品または企業競争力が落ちるのではないか
	3	サイバーテロ動向を踏まえた制御システムセキュリティ対策	・ サイバーテロのターゲットが、情報システムから制御システムへ拡大する可能性への備えが必要ではないか ・ 汎用製品・標準プロトコルの採用やネットワーク化の進展によりサイバーテロの被害も拡大、重症化するのではないか
	4	制御システム向け規格策定等の国際的連携活動への参画	・ 米国、欧州など、制御システムのセキュリティ対策で連携する動きがみられるが、参加しないことで日本に不利益は無いのか
	5	制御システムセキュリティ対策における国家安全保障の視点	・ 国家安全保障の観点から、制御システムのセキュリティ対策に、国として人、モノ、金を確保すべきではないか ・ 現状事業者や制御機器ベンダの自主的な活動が中心 ・ NISC の活動等と連携を強化し、統合した継続的な活動体制を設ける必要があるのではないか

今後、これらの課題解決に向けた取り組みが求められるが、その際、米国における先行事例はおおいに示唆を与えると思われる。特に、政府機関が主導するテストベッドやツール開発、重要インフラ事業者団体のロードマップ作成、セキュリティベンダによる認証、さらには産学官のフォーラムによる情報共有などの取り組みが進められており、我が国における今後の取り組みにおいても、このような米国での取り組みを参考として進めることは有意義であると考える。一方、米国と日本の事業環境や商習慣の違いなどを考慮した上で、より実効性の高い施策を検討するためには、他国の事例から示唆を得ることも重要である。

サービスの継続性の観点では、広義の制御システム（図表 4-2）にも示したとおり、狭義の制御システムへの対策だけで実現はできない。また、今回の国内調査で対象とした制御機器ベンダだけで実現はできない。国にとっては国家安全保障リスクであり、事業者にとっては経営リスクである点を踏まえた、継続的かつ全体整合性のとれたセキュリティ対策を推進していくことが重要である。

5. 今後に向けた提言

5.1.さらなる調査深耕の必要性

本調査で明らかになったとおり、日本においても、コスト低減や競争力向上などの経営的な観点から制御システムと情報システムの連携が進み、また、汎用製品や情報システム分野での標準プロトコルの採用などが進展していることにより、重要インフラにおける制御システムのセキュリティについての課題が顕在化しつつある。今回の調査対象とした米国における取り組みの状況なども踏まえて、重要インフラ制御システムのセキュリティおよびサービス継続の確保・向上のための取り組みについてさらに深耕することが必要と考えられる。

5.1.1　制御システム全体像の調査と現状把握

すでに述べたとおり、今回の調査は、制御システム全体像の一部ファクトの調査として、米国における制御システムのセキュリティに対する取り組みと、日本における現状を調査したものであり、いわば、今後の調査範囲の整理のための基礎となる調査という位置付けである。今回調査内容に基づき、制御システム全体像を把握するために、技術面、運用面、制度面、関係する組織（制御機器ベンダ、事業者、業界団体、政府など）などにおいて、どの範囲の調査が必要か、また、その調査をどのように進めるかについての検討・整理が必要である。

5.1.2　欧州における制御システムセキュリティに対する取り組みの調査

今回の海外調査では米国に絞って実施したが、重要インフラの制御システムに関する状況は日本と米国で必ずしも同じではない。例えば米国では、政府がインフラ事業の運営に介入するものの、実務的にはインフラ事業者たちの自主規制を認める方式をとっている（セクトラル方式＋セーフ・ハーバ・ルール）。欧州では、国により政府の介入度合いは異なるが、国の監視を強力に進める方式や、政府のガイダンスを軸として事業者にインセンティブを与えるという比較的日本に近い方式などがある。

上記 5.1.1 の整理もふまえ、米国のみではなく欧州他の状況の調査を実施し、日本としての取り組み方法についての検討を深めることが有効と考えられる。

具体的な取り組みとしては、欧州においては、EU が第 7 次フレームワークプログラム（FP7）において重要インフラ防護の取り組みを推進している（ICT-SEC）。また、英国の CPNI が制御システムのセキュリティ強化に向けた取り組みとして、SCADA、制御系システムのセキュリティに関連する情報をシステム運用者間で共有する SCSIE（The SCADA and Control Systems Information Exchange）プログラムを 2003 年よ

り行っている。また、SCSIE を欧州全体に拡大する取り組みとして E-SCSIE（European SCADA and Control Systems Information Exchange）も 2005 年より始まっている。

米国に加え欧州の動向を把握することで、制御システムのセキュリティ対策における日本の現状を再確認し、今後の方向性を検討する必要がある。

5.1.3 政府における取り組みの方向性の調査

制御システム全体像を踏まえた上で、課題とその対応の方向性に対して、全体像のそれぞれのレベル、関与者においてどのような取り組みが必要か、また、その取り組みを実現するためのアプローチについて検討し、継続的に適切な組織等に提言してゆくことが重要であると考えられる。

今回の国内調査では制御システムのベンダの状況を中心としたが、重要インフラ防護の観点からどのような政策が行われようとしているか、政府部門の動向も把握することが必要である。現在、内閣官房情報セキュリティセンター（NISC）では重要インフラの情報セキュリティ対策を推進しているが、制御システムのセキュリティ強化に向けてどのような方向性で臨もうとしているかを理解することは、具体的な対策を考える上で重要である。また、このような調査を踏まえて、今後 IPA が果たすべき役割を検討することも有効であろう。

5.2.調査を踏まえたセキュリティ対策のあり方の検討

上記 5.1.にのべた調査の深耕により制御システムのセキュリティ課題および対策の方向性の全体像を踏まえた上で、具体的な対策のあり方を検討していく必要がある。また、全体像のそれぞれのレベル、関与者においてどのような取り組みが必要か、また、その取り組みを実現するためのアプローチについて検討し、継続的に適切な組織等に提言していくことが重要であると考えられる。特に制御システムの特性である、製品のライフサイクルの長さや、トラブルが発生したときの損失の大きさ、対象事業者がもれなく対応すべき等を考慮し、検討・検証に必要な時間をとって長期的視点で確実な対応を図ることが重要である。

5.2.1　日本としての制御システムセキュリティのガイドライン確立

米国では、政府が制御システムのセキュリティに関するガイドラインを設けようとしており、それを制御機器ベンダや事業者も参考としている。また、重要インフラのセクタでは、業界内のセキュリティ基準やセキュリティ強化に向けたロードマップを策定することで、対策の進展を図っている。

日本においても、米国やその他の取り組みを踏まえた上で、政府および業界団体の協力により、制御システムのセキュリティ対策におけるガイドラインを確立することが有効と考えられる。

5.2.2　制御機器ベンダおよび事業者に対する啓発

今回の調査では、日本における制御システムの脆弱性や外部からの攻撃リスクなどのセキュリティ課題の顕在化や、対策の必要性に関する認識は、米国同様に今後進展すると想定される。制御システムの目的や要件が情報システムとは異なっていることが背景にあるものの、今後オープン化の進展によるセキュリティリスクの増大は、避けることの出来ない方向といえる。有効な対策を行っていくためには、制御機器ベンダや事業者における認識を高めることが必要であり、そのための施策を検討する必要がある。

5.2.3　セキュリティ検証環境の整備

制御システムのセキュリティ対策を支援、実行するため必要となる、ツールの開発、共通技術の開発、実運用に近い環境で実施可能なテスト環境の提供が有効と考えられる。またセキュリティ実装の認証を行うことで、事業者、制御機器ベンダ双方にとってセキュリティ上問題のない製品を選別し採用できる環境が整備され、セキュリティ

向上のインセンティブにもつなげることができると考えられる。
実施にあたっては、政府が主導するのか、民間が自主的に行うのか、官民の協力によるべきかなど、欧米など諸外国の事例調査も踏まえ、日本として最適な方向性を検討すべきであろう。

5.2.4 国際協調の必要性

制御機器ベンダや事業者は、いまや一国のみならずグローバルに活動を展開している場合も多い。制御システムのセキュリティ対策の基準や、実施内容に、国・地域ごとの格差が大きい場合、セキュリティ対策強化のマイナス要因となる可能性もあり、国際標準の確立に日本としても積極的に参画することが重要となる。現時点では、日本の制御機器ベンダは国内向けの機器と、米国向けの機器とでは、異なるセキュリティ要件を満たす必要があり、国際標準に準拠した製品を展開できるようになれば、競争力の観点からもメリットは大きい。

以上、述べたように、今回の調査を土台として今後さらに調査を深耕し、対策が必要な具体的な項目をチェック、評価し、日本の社会インフラを構成する制御システムのセキュリティを維持・向上させていくための、方向性を明確化していくことが必要である。

〔調査資料一覧〕

（URL は 2009 年 1 月 30 日時点）

タイトル	発行機関	備考（URL/入手方法等）
ANSI/ISA.99.00.01.2007 Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and Models	ISA	ISA から購入
ANSI/ISA-TR99 00.01-2007 Technologies for Protecting Manufacturing and Control Systems	ISA	ISA から購入
ANSI/ISA-TR99 00.02-2004 Integrating Electronic Security into the Manufacturing and Control Systems Environment	ISA	ISA から購入
NIST Special Publication 800-82 FINAL PUBLIC DRAFT （2008） Guide to Industrial Control Systems （ICS） Security	NIST	csrc.nist.gov/publications/PubsSPs.html
NIST Special Publication 800-53 Revision 2 （2007） Recommended Security Controls for Federal Information Systems	NIST	csrc.nist.gov/publications/PubsSPs.html
NERC Cyber Security Standards ・Standard CIP-002-1 Cyber Security - Critical Cyber Asset Identification ・Standard CIP-003-1 Cyber Security - Security Management Controls ・Standard CIP-004-1 Cyber Security - Personnel & Training ・Standard CIP-005-1 Cyber Security - Electronic Security Perimeter（s） ・Standard CIP-006-1 Cyber Security - Physical Security of Critical Cyber Assets ・Standard CIP-007-1 Cyber Security - Systems Security Management ・Standard CIP-008-1 Cyber Security - Incident Reporting and Response Planning ・Standard CIP-009-1 Cyber Security - Recovery Plans for Critical Cyber Assets	North American Electric Reliability Council （NERC）	www.nerc.com

タイトル	発行機関	備考（URL/入手方法等）
System Protection Profile - Industrial Control Systems Version 1.0	Process Control Security Requirements Forum（PCSRF）	www.isd.mel.nist.gov/projects/processcontrol/
Functional Safety in Automation -Status and Perspective	IEC TC6	"IEC TC65 Meetings TOKYO 2008 Industrial Automation Forum"での講演資料
大規模プラント・ネットワーク・セキュリティについて ～ 重要システムのサイバーテロリズム・クラッキング対策のあり方～ 最終報告書 平成１２年３月	大規模プラント・ネットワーク・セキュリティ対策委員会	www.ipa.go.jp/security/fy11/report/contents/intrusion/psec/index3.html
大規模プラント・ネットワーク・セキュリティについて ～ 重要システムのサイバーテロリズム・クラッキング対策のあり方～ 平成 10 年３月 中間報告書	通商産業省 大規模プラント・ネットワーク・セキュリティ対策委員会	www.ipa.go.jp/security/fy11/report/contents/intrusion/psec/index3.html
American Gas Association	同左	www.aga.org
Argonne National Laboratory	同左	www.anl.gov
American Petroleum Institute	同左	www.api.org
Critical Infrastructure Partnership Advisory Council	同左	www.dhs.gov/xprevprot/committees/editorial_0843.shtm
Centre for the Protection of National Infrastructure	同左	www.cpni.gov.uk
Department of Homeland Security	同左	www.dhs.gov
Department of Energy	同左	www.energy.gov
Department of Commerce	同左	www.commerce.gov
Energy Sector Control System Working Group “ie Roadmap”	Energy Sector Control System Working Group	www.controlsystemsroadmap.net
European SCADA and Control Systems Information Exchange	同左	espace.cern.ch/EuroSCSIE/default.aspx
Federal Energy Regulatory Commission	同左	www.ferc.gov
Institute for Information Infrastructure Protection	同左	www.thei3p.org
International Society of Automation	同左	www.isa.org

タイトル	発行機関	備考（URL/入手方法等）
Idaho National Laboratory	同左	www.inl.gov
The Instrument Society of America	同左	www.isa.org
有限責任中間法人 JPCERT コーディネーションセンター	同左	www.jpcert.or.jp
Lawrence Berkeley National Laboratory	同左	www.lbl.gov
North American Electric Reliability Corporation	同左	www.nerc.com
National Institute of Standards and Technology	同左	www.nist.gov
Nuclear Regulatory Commission	同左	www.nrc.gov
Oak Ridge National Laboratory	同左	www.ornl.gov
Partnership for Critical Infrastructure Security	同左	www.pcis.org
Process Control Systems Forum	同左	www.pcsforum.org *但し、2009.1.15 時点アクセス不能 本 URL は PCSF2008 開催時に情報公開されていたサイト URL
Process Control Security Requirements Forum	同左	www.isd.mel.nist.gov/projects/process control/
Pacific Northwest National Laboratory	同左	www.pnl.gov
The SCADA and Control Systems Information Exchange	同左	www.cpni.gov.uk/Products/information.aspx
Sandia National Laboratory	同左	www.sandia.gov
United States Computer Emergency Readiness Team	同左	www.us-cert.gov
PCSF2008 配布資料	PCSF	フォーラム参加者に電子データ（USB メモリ格納）で配布
社団法人計測自動制御学会	同左	www.sice.or.jp
社団法人日本電気計測器工業会	同左	www.jemima.or.jp
電気事業連合会	同左	www.fepc.or.jp
社団法人電子情報技術産業協会	同左	www.jeita.or.jp
電力中央研究所	同左	criepi.denken.or.jp
内閣官房情報セキュリティセンター	同左	www.nisc.go.jp

〔図表一覧〕