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
(付録)

2009 年 3 月

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

付録 1. 基準･規格等の内容

本付録では、報告書本文の 2.1.5 節で示した基準・規格等の中で、中心となっていると考えられる次の 4 つの基準・規格等の内容について示す。

＜標準化団体策定基準・規格等＞

1. NIST SP 800-82
2. ANSI/ISA-99.00.01
3. NIST SP 800-53

＜セクタ基準・規格等＞

4. NERC Standard CIP-002-1～CIP-009-1

1　NIST SP 800-82（Final Public Draft）

Guide to Industrial Control Systems（ICS）Security

SCADA systems, DCS, and other control system configuration such as PLC

NIST SP 800-82 は 2008 年 9 月に Final Public Draft が発行されている状況であり、以下では、この Final Public Draft の内容について示す。

1.1 ドキュメントの構成

セキュアな ICS を実現するためのガイダンスの提供を目的として、以下の項目を記述。

・ICS の全体像
・ICS の特徴、脅威と脆弱性
・ICS セキュリティプログラムの開発と展開
・ネットワークアーキテクチャ
・ICS セキュリティ管理策

以下、これら各項目で示されている概要と、特徴的な点を示す。

1.2 ICS の全体像

Industrial control systems (ICS)は、次のような制御システムのタイプを含む、制御システムの総称として使われている。

・Supervisory Control And Data Acquisition （SCADA） systems
・Distributed Control Systems （DCS）
・Programmable Logic Controllers （PLC）などの他のシステム構成

（1）ICS オペレーションの主要な要素

ICS オペレーションにおける主要な要素として次の 3 つが挙げられる。

(a) コントロールループ

[センサからの制御対象プロセスの情報]
→[コントローラによるアクチュエータへの制御指示]
→[アクチュエータによる制御対象プロセスの制御]
という、一連の制御の流れを示す。

(b) ヒューマン・マシン・インタフェース（HMI）

オペレータが HMI を通じて、制御対象プロセスのモニタ、コントローラに対するパラメータや制御アルゴリズムの設定などを実施。

(c) リモート診断・保守設備

制御対象プロセスの異常や障害の防止、検知、回復を行う。

（2）SCADA システムと DCS

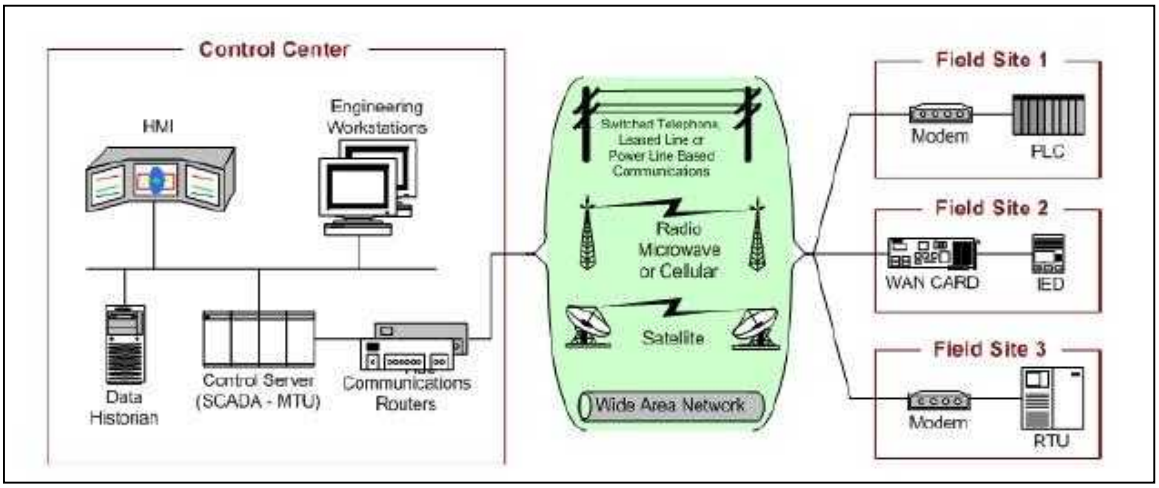
本ドキュメントでは、SCADA システムと DCS は次のように示されている。

(a) SCADA システム

SCADA システムは、分散した対象を制御する上で、分散した制御対象に関する情報の中央での把握が制御のために重要となるシステムで用いられる。配水システム、石油やガスのパイプライン、配電システムなどの地理的に分散した配給システム（distribution system）で用いられる。

SCADA システムは、フィールド情報を収集し、中央のコントロールセンタに送信し、コントロールセンタでオペレータが地理的に分散した制御対象全体をリアルタイムでモニタ、コントロールすることを可能とする構成となっている。SCADA システムの一般的な構成を付録図表 2-1 に示す。

付録図表 2-1　SCADA システムの一般構成（NIST SP 800-82 Figure 2-2）



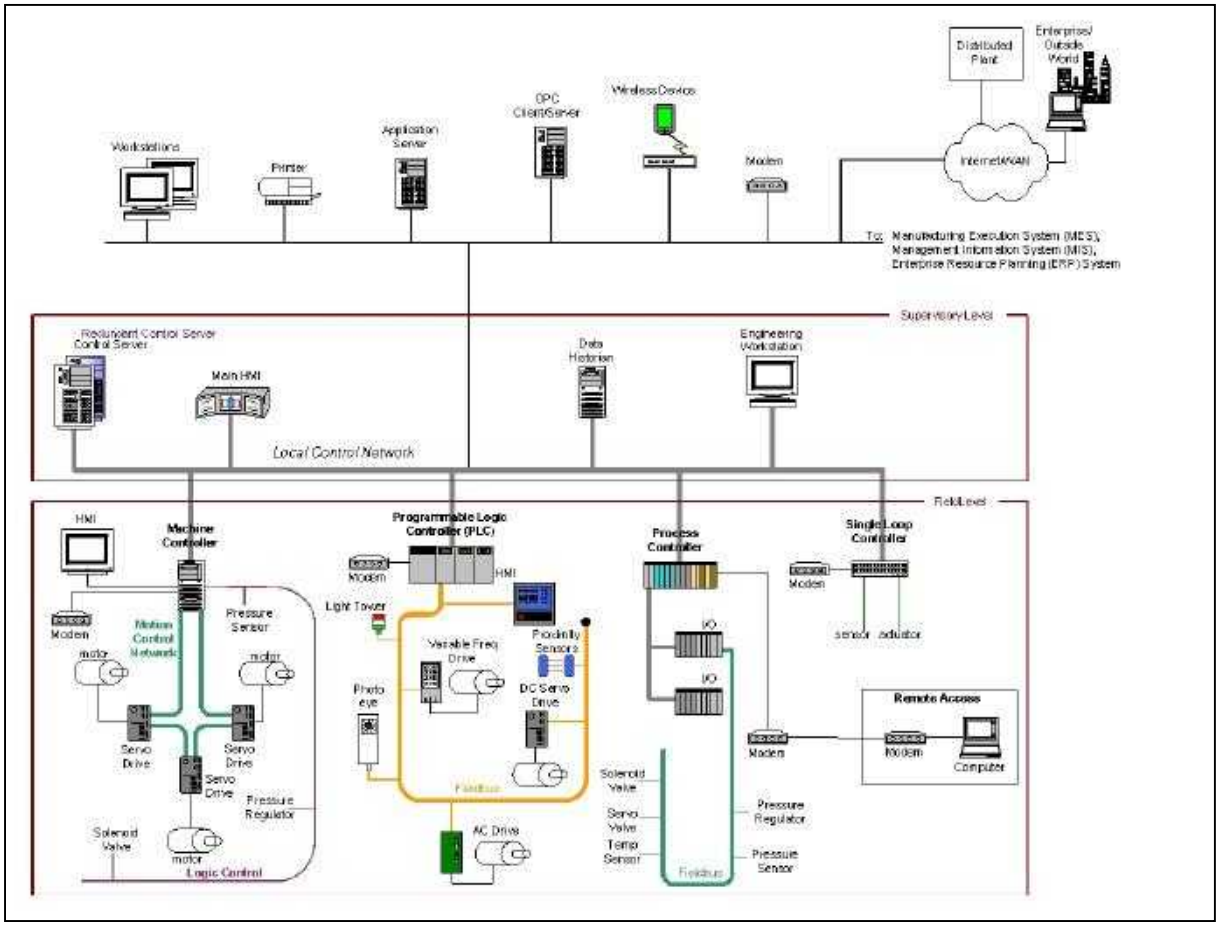
(b) DCS

DCS は、石油精製や浄水、発電プラントなどのような、地理的に同一場所に存在する生産システムを制御するために用いられる。DCS は、ローカルなコントロールループ（Field Level）と、それらを統合し全体を管理するコントロールループ（Supervisory Level）とから構成される。

また、最近の多くのシステムでは、生産プロセス情報を経営側の情報システムに提供するために、DCS は企業情報ネットワークとのインタフェースを持つようになってきている。

付録図表 2-2 に DCS の構成例を示す。

付録図表 2-2　DCS の構成例（NIST SP 800-82 Figure 2-7）



1.3 ICS の特徴

（1）IT システムと比較した ICS の特徴

IT システムと比較した ICS の特徴として次の項目が示されている。ICS と IT システムとの比較については付録図表 2-3 参照。

(a)パフォーマンスへの要求

ICS はタイムクリティカルであり、レスポンスの遅れやレスポンスタイミングの変動に対する許容レベルが存在するのが一般的。IT システムで典型的に要求される高スループットは本質的な要件とはならないのが通常。

(b)可用性への要求

ICS では連続運転が基本であり、高い可用性が要求される。ICS は制御対象の運用に影響を与えることなく停止・再スタートを行うことは困難であり、IT システムで用いられる再立ち上げのような対策は適用し難い。

(c)リスクマネジメントへの要求

ICS では、人に対する安全性、制御対象の損傷による社会や人命、生産工程などへの悪影響を防ぐことが第一の要件。ICS の運用、セキュリティ、保守に責任ある要員は、安全性とセキュリティとの重要な関連について理解していなければならない。

(d)アーキテクチャ上のセキュリティ重点箇所

ICS では、制御対象を直接制御するフィールド機器（PLC、DCS コントローラ、オペレータ端末など）の注意深い防護が重要。また、フィールド機器全体を制御する中央サーバの防護も重要。

(e)物理的な相互作用

ICS では物理的な制御対象との非常に複雑な相互作用が発生。ICS に組み込まれる全てのセキュリティ機能は、ICS の通常機能に悪影響を与えないことを保証するために十分にテストされなければならない。

(f)タイムクリティカルなレスポンス

ICS では応答時間に対して非常に緊急性が要求される場合があり、例えば、HMI（Human Machine Interface）端末での運用員のパスワード認証処理によって、運用員による緊急応答が妨げられるようなことがあってはならない。このような場合は、物理的なアクセス管理策によって HMI 端末へのアクセスを厳密に管理することが必要。

(g)システムオペレーション

ICS の OS やアプリケーションは、IT セキュリティ対策の適用が困難。レガシーの ICS では、IT セキュリティ対策組み込みによる負荷増加やタイミングの不安定性などは許容できない。制御ネットワークに関しても IT システムとは異なったレベルの専門性が要求される。

(h)リソースへの制約

ICS では、IT システムに比べて利用できるリソースに制限がある場合が多く、IT システムでのセキュリティ対策を ICS コンポーネントに組み込むことは困難。また、ICS ベンダとの関係から、サードパーティのセキュリティ製品を組み込むことが許されない場合もあり。

(i)通信

フィールド機器との通信で使われるプロトコルやコントローラ間での通信プロトコルは、IT システムとは異なり、独自プロトコルである場合が多い。

(j)変更管理

ICS ではソフトウェアの更新は、実装する前にソフトウェアベンダとエンドユーザによって十分にテストされることが必要。また、ICS への更新版の実装は、ICS の計画停止のタイミングでのみ可能。IT システムにおける自動化されたタイムリーなパッチ適用の対策を ICS で取ることは困難。

他の観点として、ICS では、ベンダのサポートサービスが切れた古いバージョンの OS が使用されている場合も多い。

(k)サポート

ICS では、通常シングルベンダによるサポートが行われる。IT システムのように、マルチベンダによる多様な相互運用性のあるサポートサービスは受けられないのが通常。

(l)コンポーネントのライフタイム

ICS では、コンポーネントのライフタイムは通常、15～20 年。IT システムの 3～5 年よりもずっと長く使用される。

(m)コンポーネントへのアクセス

ICS コンポーネントは、通常、隔離された遠隔地にあり、アクセスに対しては多数の物理的防御がなされている。

付録図表 2-3　IT システムと ICS との差異（NIST SP 800-82 Table 3-1）

Category	Information Technology System	Industrial Control System
Performance Requirements	Non-real-time Response must be consistent High throughput is demanded High delay and jitter may be acceptable	Real-time Response is time-critical Modest throughput is acceptable High delay and/or jitter is not acceptable
Availability Requirements	Responses such as rebooting are acceptable Availability deficiencies can often be tolerated, depending on the system's operational requirements	Responses such as rebooting may not be acceptable because of process availability requirements Availability requirements may necessitate redundant systems Outages must be planned and scheduled days/weeks in advance High availability requires exhaustive pre-deployment testing
Risk Management Requirements	Data confidentiality and integrity is paramount Fault tolerance is less important – momentary downtime is not a major risk Major risk impact is delay of business operations	Human safety is paramount, followed by protection of the process Fault tolerance is essential, even momentary downtime may not be acceptable Major risk impacts are regulatory non-compliance, environmental impacts, loss of life, equipment, or production
Architecture Security Focus	Primary focus is protecting the IT assets, and the information stored on or transmitted among these assets. Central server may require more protection	Primary goal is to protect edge clients (e.g., field devices such as process controllers) Protection of central server is also important
Unintended Consequences	Security solutions are designed around typical IT systems	Security tools must be tested (e.g., off-line on a comparable ICS) to ensure that they do not compromise normal ICS operation
Time-Critical Interaction	Less critical emergency interaction Tightly restricted access control can be implemented to the degree necessary for security	Response to human and other emergency interaction is critical Access to ICS should be strictly controlled, but should not hamper or interfere with human-machine interaction
System Operation	Systems are designed for use with typical operating systems Upgrades are straightforward with the availability of automated deployment tools	Differing and possibly proprietary operating systems, often without security capabilities built in Software changes must be carefully made, usually by software vendors, because of the specialized control algorithms and perhaps modified hardware and software involved
Resource Constraints	Systems are specified with enough resources to support the addition of third-party applications such as security solutions	Systems are designed to support the intended industrial process and may not have enough memory and computing resources to support the addition of security capabilities
Communications	Standard communications protocols Primarily wired networks with some localized wireless capabilities Typical IT networking practices	Many proprietary and standard communication protocols Several types of communications media used including dedicated wire and wireless (radio and satellite) Networks are complex and sometimes require the expertise of control engineers
Change Management	Software changes are applied in a timely fashion in the presence of good security policy and procedures. The procedures are often automated.	Software changes must be thoroughly tested and deployed incrementally throughout a system to ensure that the integrity of the control system is maintained. ICS outages often must be planned and scheduled days/weeks in advance. ICS may use OSs that are no longer supported
Managed Support	Allow for diversified support styles	Service support is usually via a single vendor
Component Lifetime	Lifetime on the order of 3-5 years	Lifetime on the order of 15-20 years
Access to Components	Components are usually local and easy to access	Components can be isolated, remote, and require extensive physical effort to gain access to them

（2）脅威

ICS に対する脅威として次の項目が示されている。

・アタッカー
・ボットネットオペレータ
・犯罪者グループ
・海外の諜報機関
・内部者
・フィッシング実行者
・スパマー
・スパイウェア/マルウェア作成者
・産業スパイ

（3）潜在的な脆弱性

以下の項目について、それぞれの潜在的な脆弱性が示されている。各項目で示されている内容は基本的には IT システムに対する脆弱性と同内容である。

(a)ICS に対するポリシー、手続きの脆弱性

(b)プラットフォームの脆弱性

・コンフィグレーションに対する脆弱性
・ハードウェアに対する脆弱性
・ソフトウェアに対する脆弱性

-Distributed Network Protocol（DNP）3.0、Modbus、Profibus などの業界標準 ICS プロトコルではセキュリティ対策が考慮されていないことが脆弱性として指摘されている。

・マルウェア防御に対する脆弱性

(c)ネットワークの脆弱性

・コンフィグレーションに対する脆弱性
・ハードウェアに対する脆弱性
・ネットワーク境界の脆弱性

-制御ネットワークで、IT ネットワークに実装されている DNS や DHCP を利用するケースが脆弱性として指摘されている。

・ネットワークロギング、モニタリングの脆弱性
・コミュニケーションの脆弱性
・ワイヤレスコネクションの脆弱性

（4）リスク要因

ICS に対するリスクを高める要因として次の項目が示されている。

(a)標準プロトコル、標準技術の適用

MS Windows、UNIX-like OS、TCP/IP

(b)接続先の拡大

・ICS ネットワークと企業情報ネットワークとの接続

・経営層（デシジョンメーカー）が制御システムの情報を必要なタイミングで入手し的確な経営判断を可能とする、また、制御システム側への指示を送ることを可能とし、競争力、経営効率強化

(c)非セキュアな接続

・ベンダのメンテナンスのための dial-up modems による管理者権限でのリモートアクセスルート

(d)公開情報

・ICS 仕様や接続関係、メンテナンス情報などのインターネットでの公開（潜在顧客への製品選択のサポート）

・標準仕様製品採用による ICS の共通化により、一箇所の内部情報入手により、同仕様の多数の ICS へのアタックが可能

1.4 ICS セキュリティプログラムの開発と展開

ICS セキュリティを実現するためのプログラムの概要と、その構築、展開方法について示されている。基本的には IT システム分野で実施されている ISMS（情報セキュリティマネジメントシステム）での考え方と同じであるとみなすことが出来る。

ICS セキュリティプログラム構築の流れとして次のステップが示されている。なお、より詳細な情報の参照先として、ANSI/ISA TR99.00.02: Integrating Electronic Security into the Industrial Automation and Control Systems Environment
が示されている。

（1）シニアマネージャの取り込み

ICS セキュリティプログラムを成功に導くためには、シニアマネージャの関与が必須。IT と ICS の両方を管理するレベルのシニアマネジメントであることが必要。

（2）クロスファンクショナルチームの編成

少なくとも、IT スタッフ、コントロールシステムエンジニア、コントロールシステムオペレータ、セキュリティ専門家、マネジメントスタッフから構成するクロスファンクショナルチームを編成。また、このチームには制御システムベンダ、インテグレータも含めるべき。

（3）役割と範囲の定義

セキュリティプログラムの目的、関係する事業組織、対象となる全てのコンピュータシステムとネットワーク、必要な予算と資源、責任部署を決定し文書化。

（4）ICS 特定のセキュリティポリシーと手続き（Procedure）の定義

ICS 特定のセキュリティポリシーと手続きを定義し、既に存在する情報部門の運用/マネジメントポリシーと統合。既存の情報分野ポリシーが ICS の脅威に対応できるかどうかという観点から評価し、必要に応じて ICS 向けに修正するというアプローチが示されている。

（5）ICS システムとネットワーク資産の目録作成

ICS 内のアプリケーションとコンピュータシステム（PLC、DCS、SCADA、HMI など全ての要素)、ICS と接続しているネットワークを識別し目録としてドキュメント化。

（6）リスクと脆弱性評価の実施

ICS のリスクアセスメントを実施し、対応するリスクの優先順位付けを実施。優先度の高いリスクに対して、詳細な脆弱性評価を実施。

（7）管理策の定義

リスクアセスメント結果に基づき、リスク低減のための管理策を決定。

（8）トレーニングとアウエアネスの提供

従業員が、何故上記で決定した ICS 管理策が必要か、それらがどのようにリスク低減に役立つか、それらが実施されなかった場合の被害、などについての理解を促進するために有効となるトレーニング、アウエアネスの設計及び提供を実施。

1.5 ネットワークアーキテクチャ

ICS ネットワークと企業情報ネットワークの分離について、ファイアウォール（FW）による分離方法のタイプとして次の 4 形態を示している。

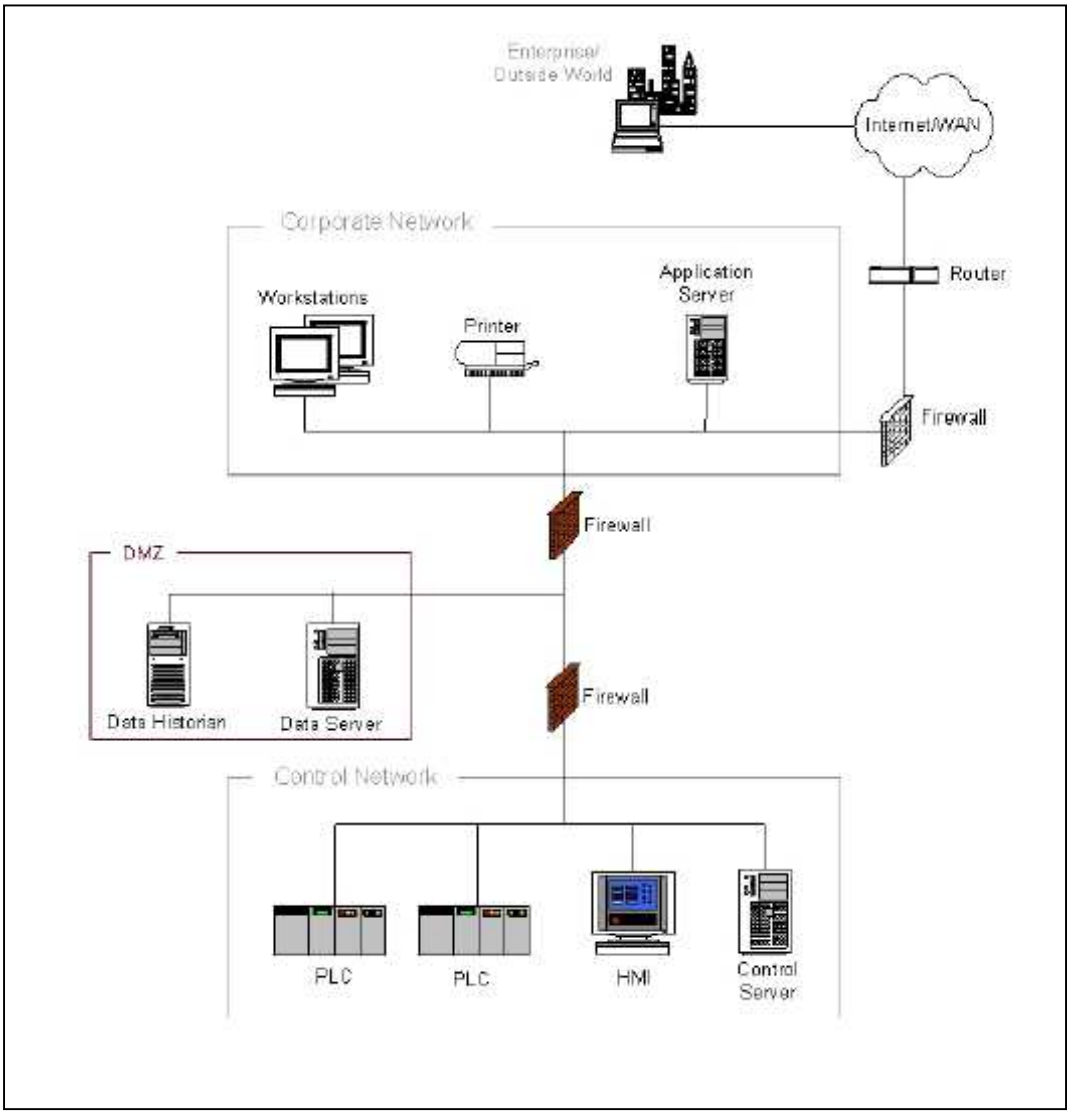
（1）企業情報ネットワークと制御ネットワークの間への FW の設置

（2）企業情報ネットワークと制御ネットワークの間への FW とルーターの設置

（3）企業情報ネットワークと制御ネットワークの間への DMZ（Demilitarized Zone）をもった FW の設置

（4）企業情報ネットワークと制御ネットワークの間へのペアとなる FW の設置（付録図表 2-4）

付録図表 2-4　企業情報ネットワークと制御ネットワークの分離の一形態
（NIST SP 800-82 Figure 5-4）



1.6 ICS のセキュリティ管理策

NIST SP 800-53（Recommended Security Controls for Federal Information Systems）で示されているコントロールの概要の説明と、そのコントロールに対する、ICS Specific Recommendations and Guidance を必要に応じて示している。

（１）800-53 で示されているコントロールは以下。各項目の内容については本付録の 3 章を参照。

(i) Management Controls

- Risk Assessment （RA）
- Planning （PL）
- System and Services Acquisition （SA）
- Certification, Accreditation, and Security Assessments （CA）

(ii) Operational Controls

- Personnel Security （PS）
- Physical and Environmental Protection （PE）
- Contingency Planning （CP）
- Configuration Management （CM）
- Maintenance （MA）
- System and Information Integrity （SI）
- Media Protection （MP）
- Incident Response （IR）
- Awareness and Training （AT）

(iii) Technical Controls

- Identification and Authentication （IA）
- Access Control （AC）
- Audit and Accountability （AU）
- System and Communications Protection （SC）

※Technical Controls では ISA TR99.00.001 を参照している

（２）ICS Specific Recommendations and Guidance の例

＜Risk Assessment （RA）＞

- ICS に発生したインシデントも考慮する。
- 制御システムから企業情報ネットワークに流すデータの重要性の考慮必要。
- セキュリティ対策の実装は、リスクとコストのバランス（経済性）が重要。しかし、制御システムでは、経済面よりも、安全や健康に対するリスクへの考慮が重要となるケースもある。

2 ANSI/ISA99.00.01 Part 1: Terminology, Concepts and Models

2.1 ISA99 シリーズのドキュメント構成

ISA99 は、次の 4 つのドキュメントから構成される予定である。2007 年 10 月に Part1 が ANSI/ISA 規格として発行されている状況であり、2010 年に規格化完了予定である。以下では、この Part1 の内容について示す。

- 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
- ISA99.00.03. Part 3: Operating an Industrial Automation and Control System Security Program
- ISA99.00.04. Part 4: Technical Security Requirements for Industrial Automation and Control Systems

また、テクニカルレポート（TR）として次の 2 つが発行されている。

- ANSI/ISA-TR99.00.01-2007 - Technologies for Protecting Manufacturing and Control Systems

  本 TR は 2007 年に update された。また、今後定期的に update される予定である。
- ANSI/ISA-TR99.00.02-2004 - Integrating Electronic Security into the Manufacturing and Control Systems Environment

  上記 ISA99 Part2 完成後は、本 TR はこの Part2 に代替される予定である。

2.2 Part1 の構成

Part1 では、以下のサイバーセキュリティに関する基本的なコンセプトとモデルが示されている。

- この基準で参照するレファレンス、使用する語句の定義
- Industrial automation and control systems のセキュリティに関する現状のオーバービューの提示
- Industrial automation and control systems セキュリティのスコープについての課題や基本的なコンセプトの提示
- Industrial automation and control systems のセキュリティに対する基本コンセプトを適用するためのモデルの提示

2.3 制御システムの置かれている状況の認識

制御システムは、独自 OS と独自ネットワークの隔離された個別システムから、COTS（commercial off the shelf）技術（OS とプロトコル）を用い接続されたシステムへと変化してきている。制御システムは、事業利益向上の観点から、次のような統合化の傾向にある。

（１）制御システムの動作に対する可視性の増大。生産コスト低減、生産効率向上という事業上の要求に対応するため、ビジネスレベルで制御システム状況を把握し分析可能となるように統合化。

（２）制御システムからビジネスレベルの情報に、より直接アクセスできるように統合化。

（３）システム全体のサポートコストの低減、遠隔サポートの容易性、という観点から共通インタフェースの採用。

（４）サポートコストの低減と制御プロセスで発生した問題の早期解決を可能とするための、制御システムのリモートモニタリングの実施。

2.4 制御システムのコンセプト

（１）基本的なセキュリティ要件

基本的なセキュリティ要件として、次の 7 項目が示されている。

(a) Access Control
(b) Use Control
(c) Data Integrity
(d) Data Confidentiality
(e) Restrict Data Flow
(f) Timely Response to Event
(g) Resource Availability

（２）脅威-リスクアセスメント

脅威-リスクアセスメントにおける概念について示している。

(a)資産（Asset）

物理的、論理的、人的資産が存在。

(b)脆弱性

物理環境（人間含む）とサイバー環境との間の相互作用における脆弱性を理解することは、有効な制御システム構築のために重要。

(c)リスク

リスクには次のものが含まれる。

・人的安全性に対するリスク（personnel safety risk）
・プロセスの安全性に対するリスク
・情報セキュリティに対するリスク

・環境に対するリスク
・事業継続に対するリスク

(d)脅威

Accidental、Nonvalidated change の脅威を例示。また、脅威エージェントとして、信頼できる人間（Insider)、信頼できない人間（Outsider)、自然災害（Natural)、の 3 つが例示されている。

(e)対策

リスクを許容可能なレベルに低減するため、セキュリティポリシーに準拠するために取られるものであり、例として次の項目が示されている。

・authentication of users and/or computers
・access controls
・intrusion detection
・encryption
・digital signatures
・resource isolation or segregation
・scanning for malicious software
・system activity monitoring
・physical security

（3）セキュリティプログラムの成熟度

セキュリティプログラムの成熟度を示すものとして、付録図表 2-5 のフェーズが示されている。

付録図表 2-5　セキュリティ成熟度のフェーズ

フェーズ	ステップ
Concept	Identification Concept
Functional Analysis	Definition
Implementation	Functional Design Detailed Design Construction
Operation	Operation Compliance Monitoring
Recycle and Disposal	Disposal Dissolution

2.5 制御システムのモデル

（1）リファレンスモデル

制御システムのリファレンスモデルとして付録図表 2-6 に示すモデルが提示されている。

付録図表 2-6　リファレンスモデル

<table>
<tr><td>レベル４</td><td>Enterprise Systems
（Business Planning & Logistics）</td><td></td></tr>
<tr><td>レベル３</td><td>Operations Management</td><td rowspan="4">制御システム（ Industrial Automation and Control Systems）</td></tr>
<tr><td>レベル２</td><td>Supervisory Control</td></tr>
<tr><td>レベル１</td><td>Basic Control
Safety and Protection</td></tr>
<tr><td>レベル０</td><td>Process（Equipment under control）</td></tr>
</table>

（2）Asset モデル

制御システムの資産のモデル化がなされている。設備系の資産要素としては、センサ・アクチュエータ、フィールド I/O、コントロール設備、監視コントロール設備、ライン/ユニット/セル/ビークル、エリア、リモートサイト、コントロールセンタ、地理的サイト、企業などが示されている。また、ネットワーク系の資産要素として I/O ネットワーク、コントロールネットワーク、コミュニケーションネットワークなどが示されている。

（3）リファレンスアーキテクチャ

制御システムのリファレンスアーキテクチャの典型的な例が示されている。

（4）セキュリティゾーンと Conduit モデル

リファレンスアーキテクチャの中で用いる次の 2 つのモデルが支援されている。

- セキュリティゾーン：共通のセキュリティレベルが要求される論理的、物理的資産のグループ
- Conduit：セキュリティの確保された通信経路の論理的グループ

3　NIST SP 800-53
Recommended Security Controls for Federal Information Systems

3.1 全体の概要

・連邦政府向け情報システムのセキュリティコントロールを選択するためのガイドライン
・情報システムを、それが扱う情報の重要性に応じて、Low、Moderate、High の 3 レベルに分けることを前提として、それらレベルごとに、recommendation for minimum security controls をカタログ化して提示
・Appendix I に ICS を対象としたセキュリティコントロールのガイダンスを 2nd edition で追加

3.2 セキュリティコントロールの構成

（1）セキュリティコントロール全体構成

本規格で示されているセキュリティコントロールの一覧とその概要を付録図表 2-7 に示す。

付録図表 2-7　セキュリティコントロール一覧

CLASS	FAMILY	略称	概要
Management（管理）	Risk Assessment（リスクアセスメント）	RA	リスクアセスメントに関するポリシー策定や手順（分類、リスク評価、更新、システムの脆弱性に対するスキャニング）が規定されている。
	Planning（計画）	PL	情報システムのセキュリティ計画の策定と運用、情報システムの利用者に課される要件、プライバシー保護方針について規定されている。
	System and Services Acquisition（システムおよびサービスの調達）	SA	システムとサービスのサイフサイクルに（計画、リソースの配分、購入、構成管理など）セキュリティ要件を考慮にいれたポリシーや手順が規定されている。
	Certification, Accreditation, and Security Assessments（評価、認可及びセキュリティ分析）	CA	システムに対するセキュリティ評価、運用認可の方法やセキュリティ分析のための計画、モニタリング要求などが規定されている。

CLASS	FAMILY	略称	概要
Operational（運用）	Personnel Security（人的セキュリティ）	PS	人的セキュリティに関するポリシー策定や手順（選考・雇用の終了時・異動時・処罰・第三者など）が規定されている。
	Physical and Environmental Protection（物理的および環境的な保護）	PE	物理的なアクセスコントロール、情報システムの設置環境における対策、テレワークの要件について規定されている。
	Contingency Planning（緊急時対応計画）	CP	コンティンジェンシープランに関するポリシー策定や具体的な対策（要員教育、テスト、代替施設、リカバリなど）が規定されている。
	Configuration Management（構成管理）	CM	構成管理に関するポリシー策定や具体的な対策（ベースラインの設定、変更管理、モニタリングなど）が規定されている。
	Maintenance（保守）	MA	情報システムの保守に関するポリシー策定や手順（計画立案、実施方法など）が規定されている。
	System and Information Integrity（システムおよび情報の完全性）	SI	システムの完全性維持（脆弱性・障害監視および管理、入力の妥当性確認、エラー処理等）に関するポリシー策定や具体的な対策が規定されている。
	Media Protection（記録媒体の保護）	MP	記録媒体の保護に関するポリシー策定や手順（利用、保管、搬送、廃棄など）が規定されている。
	Incident Response（インシデント対応）	IR	侵入妨害に関するポリシー策定や手順（組織的・物理的・技術的な対策、侵入妨害発生時の対応など）が規定されている。
	Awareness and Training（意識向上およびトレーニング）	AT	ユーザへの情報セキュリティに対する意識付けや訓練について、方針、内容、回数などが規定されている。

CLASS	FAMILY	略称	概要
Technical（技術）	Identification and Authentication（識別および認証）	IA	識別と認証に関するポリシー策定や具体的な対策（利用者、装置、管理方法など）が規定されている。
	Access Control（アクセス制御）	AC	アクセス制御に関わるコントロールに対する要求事項と、それらのコントロールのマネジメント（管理）に関する要求事項が記載されている。
	Audit and Accountability（監査および責任追跡性）	AU	監査の方針、記録や説明責任について、監査証跡の要求や、監査における説明責任を担保するログなどの記憶容量、否認防止などが規定されている。
	System and Communications Protection（システムおよび通信の保護）	SC	システムレベル及び他のシステムとの通信に関するポリシー策定や具体的な対策（含：構築・運用）が規定されている。

（2）各コントロールの構成

付録図表 2-7 で示される Family の各コントロールの構成は次のようになっている。

・Control：

このコントロールが実現しようとしているセキュリティ機能の簡潔な記述

・Supplemental Guidance：

セキュリティコントロールについての補足的な情報。コントロールを自システムに適用、実装するときに有益な情報など。

・Control Enhancements：

コントロールのセキュリティ強度を向上することが必要な場合に追加する機能

（3）コントロールの例

付録図表 2-8 にコントロールの例を示す。

付録図表 2-8　コントロールの例

AU-2　AUDITABLE EVENTS

Control: The information system generates audit records for the following events: [*Assignment: organization-defined auditable events*].

Supplemental Guidance: The purpose of this control is to identify important events which need to be audited as significant and relevant to the security of the information system. The organization specifies which information system components carry out auditing activities. Auditing activity can affect information system performance. Therefore, the organization decides, based upon a risk assessment, which events require auditing on a continuous basis and which events require auditing in response to specific situations. Audit records can be generated at various levels of abstraction, including at the packet level as information traverses the network. Selecting the right level of abstraction for audit record generation is a critical aspect of an audit capability and can facilitate the identification of root causes to problems. Additionally, the security audit function is coordinated with the network health and status monitoring function to enhance the mutual support between the two functions by the selection of information to be recorded by each function. The checklists and configuration guides at http://csrc.nist.gov/pcig/cig.html provide recommended lists of auditable events. The organization defines auditable events that are adequate to support after-the-fact investigations of security incidents. NIST Special Publication 800-92 provides guidance on computer security log management.

Control Enhancements:

(1) The information system provides the capability to compile audit records from multiple components throughout the system into a systemwide (logical or physical), time-correlated audit trail.

(2) The information system provides the capability to manage the selection of events to be audited by individual components of the system.

(3) The organization periodically reviews and updates the list of organization-defined auditable events.

LOW AU-2	MOD AU-2 (3)	HIGH AU-2 (1) (2) (3)

3.3 Appendix I の概要

（1）目的

ICS owners にも、SP 800-53 での推奨コントロールカタログ（Low、Moderate、High）を、ICS のセキュリティ対策策定に有効に活用してもらうためのガイダンスを提供する。

（2）構成

・ICS Tailoring Guidance

情報システム向けのコントロールを ICS の特徴に合わせて補う情報

・ICS Security Control Enhancements

ICS 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 ICS に適用する際の補足的情報。ICS で情報システム向けコントロールがそのまま使えないケースとその理由（仕組み的に適用不可、Performance や Safety などで問題が発生する、など）、代替策についても記述。

3.4 Appendix I と NIST SP 800-82 との関係についての考察

（1）SP 800-82 で示されているガイダンスについては、SP 800-82 を参照することと示しており、SP 800-82 との重複はないようになっている。

（2）SP 800-82 は、SP 800-53 コントロールのファミリーレベルに対して ICS recommendations and Guidance を示しており、SP 800-53 カタログ構成に則ったものではない。Appendix I では、次のように、SP 800-53 のカタログ構成に従ったガイダンスを示している。

Supplemental Guidance → ICS Supplemental Guidance

Control Enhance → ICS Enhancement Supplemental Guidance

（3）ICS Control というものは規定されていない。セキュリティコントロール項目そのものは、情報系、制御系で変わらない、その適用の仕方が変わるという考え方と推察される。これは SP 800-82 でも同じと考えられる。

4 NERC Cyber Security Standards
Critical Infrastructure Protection （CIP） -002 ～ CIP-009

NERC Cyber Security Standards は、2008 年 1 月に、U.S. Federal Energy Regulatory Commission（FERC）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。

なお、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いる。すなわち、本基準は今後改訂がなされる予定のものであるが、以下では、2006 年に発行されたバージョンの内容について示す。

4.1 規格の構成

CIP002～CIP009 は、全て次の構成をとっている。

（1）Introduction

（2）Requirements

ここで示される要件に適合することを要求

（3） Measures

上記要件に適合していることを示す手段

（4） Compliance

・ Compliance Monitoring Process

・Levels of Non-Compliance

4.2 Standard CIP-002-1 Cyber Security - Critical Cyber Asset Identification

クリティカルサイバー資産の識別と文書化を要求。クリティカルサイバー資産の識別はリスクベースのアセスメントにより行われる。

Requirements として次の項目が提示されている。

・Critical Asset Identification Method

・Critical Asset Identification

・Critical Cyber Asset Identification

・Annual Approval

4.3 Standard CIP-003-1 Cyber Security - Security Management Controls

クリティカルサイバー資産を防御するために、責任主体が適切な最小限のセキュリティマネジメントコントロールを実施することを要求。

Requirements として次の項目が提示されている。

・Cyber Security Policy

・Leadership

・Exceptions

・Information Protection
・Access Control
・Change Control and Configuration Management

4.4 Standard CIP-004-1 Cyber Security - Personnel & Training

クリティカルサイバー資産にアクセスする権限を持った人員に対して、適切なレベルでのリスク評価、訓練、セキュリティについての意識付けの実施を要求。

Requirements として次の項目が提示されている。

・Awareness
・Training
・Personnel Risk Assessment
・Access

4.5 Standard CIP-005-1 Cyber Security - Electronic Security Perimeter（s）

クリティカルサイバー資産が内在する電子的なセキュリティ範囲と境界上のアクセスポイントの識別と防御を要求。

Requirements として次の項目が提示されている。

・Electronic Security Perimeter
・Electronic Access Controls
・Monitoring Electronic Access
・Cyber Vulnerability Assessment
・Documentation Review and Maintenance

4.6 Standard CIP-006-1 Cyber Security - Physical Security of Critical Cyber Assets

クリティカルサイバー資産を防御するための物理的セキュリティプログラムの実装を要求。

Requirements として次の項目が提示されている。

・Physical Security Plan
・Physical Access Controls
・Monitoring Physical Access
・Logging Physical Access
・Access Log Retention
・Maintenance and Testing

4.7 Standard CIP-007-1 Cyber Security - Systems Security Management

責任主体による、クリティカルサイバー資産のセキュリティを確保するための手法、プロセス、手続きの定義を要求。

Requirements として次の項目が提示されている。

・Test Procedures
・Ports and Services
・Security Patch Management
・Malicious Software Prevention
・Account Management
・Security Status Monitoring
・Disposal or Redeployment
・Cyber Vulnerability Assessment
・Documentation Review and Maintenance

4.8 Standard CIP-008-1 Cyber Security - Incident Reporting and Response Planning

クリティカルサイバー資産に関連するセキュリティインシデントの識別、分類、レスポンス、報告の実施を要求。

Requirements として次の項目が提示されている。

・Cyber Security Incident Response Plan
・Cyber Security Incident Documentation

4.9 Standard CIP-009-1 Cyber Security - Recovery Plans for Critical Cyber Assets

クリティカルサイバー資産に対するリカバリープランの策定を要求。確立された事業継続とディザスタリカバリの技術やプラクティスに基づくこと。

Requirements として次の項目が提示されている。

・Recovery Plans
・Exercises
・Change Control
・Backup and Restore
・Testing Backup Media

付録 2. PSEC での調査時点（2000 年）と現在の状況との比較分析

1. PSEC 活動状況概要の整理

（1）PSEC 活動の概要

「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）」は 1998 年 9 月に通商産業省（当時）により、大規模で広範な社会経済基盤におけるサイバーテロリズム・クラッキング対策のあり方について検討を行うため設置された委員会である。

PSEC では、石油精製、石油化学、電力、鉄鋼、紙パルプ関連などのエネルギー・製造業のシステムのユーザ、ベンダ、エンジニアリング企業が一堂に会し、大規模プラント・ネットワークのセキュリティ対策についての検討を行い、次に示す中間報告書（1998 年 2 月）、最終報告書（2000 年 3 月）を取りまとめている。

（http://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」

「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」

また、IPA はこの PSEC 活動を支援するとともに、関連した調査、技術開発事業を行った。

（2）PSEC における WG 活動

PSEC では、次の 5 つのワーキンググループ（WG）を設置し、技術的および非技術的観点からのセキュリティ対策を検討した。

・ＷＧ１：セキュリティ技術開発テーマの洗い出しと開発企画
・ＷＧ２：プラント・ネットワークのリスク分析手法の研究
・ＷＧ３：プラント・ネットワーク・セキュリティ運用ガイドライン の策定
・ＷＧ４：制御系システムに求められるセキュリティ要件の 記述の試み
・ＷＧ５：情報セキュリティ・マネージメントの研究

（3）PSEC 最終報告書で示されている課題

PSEC による最終報告書では、付録図表 3-1 に示す課題が示されている。

付録図表 3-1　「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 3 月）」最終報告書で示されている課題

	活動項目		報告書で示されている課題
(a)	非技術的事項	**セキュリティマネージメント** 制御系ネットワークにおけるサイバーテロリズム対策に焦点を当てた情報セキュリティマネジメントを検討	・専門家の不足 情報セキュリティの専門家が不足。セキュリティ、IT（制御システム）双方を熟知している専門家は極端に少ない。 ・コミュニケーションギャップ IT（制御システム）担当者と、経営者を含めた他部門との間にコミュニケーションギャップが存在。IT 担当者あるいはセキュリティ担当者による教育啓発活動が不可欠。
(b)		**セキュリティ運用ガイドライン** 「コンピュータ不正アクセス対策基準」（2000 年に通産省（現経産相）策定）をプラントネットワーク用に改定することにより、「プラント・ネットワーク・セキュリティ運用ガイドライン」を策定	・策定したセキュリティ運用ガイドラインの運用方法を示すガイドラインの作成（石油精製プラントなどの具体的なネットワーク例を示すなど）と普及
(c)	技術的事項	**セキュリティ技術開発** 今後の制御システムのオープン化、ネットワーク化の流れから情報セキュリティ技術の導入の必要性が高まることは自明の理であることより、実際にプラントに適用することを前提として開発が必要な技術テーマを定義し、その機能概要を定めた※1	・オープンなプロトコルであるフィールドバスのセキュリティ対策の検討 ・制御 LAN がオープン化された場合の、認証や暗号化などのセキュリティ技術仕様の検討 ・制御系システム分野におけるウィルス対策の検討
(d)		**セキュリティリスク分析手法** セキュリティエンジニアリングのフレームワーク（プラントライフサイクルに即したリスク分析の位置づけ）の検討及びプラントネットワークに対するリスク分析手法の適用性検討の実施	・プラントセキュリティエンジニアリング セキュリティエンジニアリングのためにネットワーク用リスク分析手法を系統化するためのネットワークの設計手法の検討※2 ・プラントネットワークに対するリスク分析 FTA・ETA、HAZOP※3 手法の統合の検討（共通利用のできるフレームの構築）

	活動項目		報告書で示されている課題
(e)		**セキュリティ評価基準** 制御系システム設計時におけるセキュリティ要件を明らかにするためにISO/IEC 15408（CC：Common Criteria）の枠組みをもとに、その可能性を検討	・システムを対象とするPPを記述することに内在する課題（システムの機能が経営管理上の権限・機構を規定する論法になっている） ・PP記述形式上の課題（英語/日本語の場合） ・個別機器のPP検討への発展可能性

※1：制御系ステム専用のアクセス制御機能、制御系システムのセキュリティ検査機能、分散制御システムのログ記録機能、制御系システム専用の認証機能、制御系情報LAN上での侵入検知機能、「リモートアクセス環境でのセキュリティ」評価機能、統合試験機能、「高速暗号技術」の評価機能、実証実験（統合アタック実験）実施

※2：プラントエンジニアリングでは基本設計から詳細設計へと各設計段階に応じた系統的な設計手法とリスク分析手法が確立され、プラントエンジニアリングに対するセーフティエンジニアリングの位置づけが確定している。

※3：HAZOP（Hazard And Operability Study）：危険シナリオ分析手法の一つで、化学プロセスにおける複数の独立した事象が複雑に絡む故障を取り扱うために開発された手法。

2. PSEC 報告書での課題（2000 年度における状況認識）と現時点での状況の分析

（１）全体状況についての考察

2000 年時点に比べて、国内における情報セキュリティに対する認識は、特に情報システム分野において大きく向上している。

個人情報保護法や不正アクセス禁止法などの法制度面での整備や、ISMS（情報セキュリティマネジメントシステム）適合性評価制度、情報セキュリティ監査制度などのセキュリティに対する第 3 者評価の環境などが整ってきている。

また、調査報告書の中でも示したように、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 の情報セキュリティ確保に向けた政策が推進されている。

一方、制御システム分野における情報セキュリティについての認識は、調査報告書で示したように、独自 OS と独自ネットワークの隔離された個別システムというこれまでの制御システムの特徴、また安全性という制御システム特有の要件から、情報システム分野に比べると低い認識であると考えられる。

しかし、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、制御システムにおいても汎用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状況であることは調査報告書で示したとおりである。

このような背景のもとで、2000 年に PSEC 報告書で指摘された課題については、今後、それらへの対処がますます重要になってくると考えられる。この際、次に示すような 2000 年時点からの状況の変化を踏まえた対応が必要になると考えられる。また、これら課題については、今回調査で実施したように、制御システム関係者により適宜見直してゆくことも必要であろう。

- 情報セキュリティに対する認識、技術やそれらの普及、国としての体制、制度面などについては 2000 年時点と比べて大きく進展しており、これら状況を有効に活用した課題解決に向けた取組み
- 2000 年時点と比較して、経営的な観点から制御システムと情報システムとの連携による統合化が進んでおり、このような状況でのサービス継続のために制御システムで果たすべきセキュリティ要件の識別とその実現に向けた取組み

（２）各課題についての考察

(a) セキュリティマネジメント

2000 年の状況に比べて、情報セキュリティマネジメントは、情報システム分野を中心として認識が大きく向上し広く普及しており、大きな状況の進展が見られる。このような情報システム分野の状況により、制御システム分野にも情報セキュリティマネジメントの考え方は浸透しつつある状況と考えられる。

このような状況の進展を踏まえて、今後、制御システムにおいても、情報システム部門と連携して情報セキュリティマネジメントの実践を定着してゆくことが必要であると考えられる。

(b) セキュリティ運用ガイドライン

2000 年の状況に比べて、情報システム分野においてはセキュリティ運用ガイドラインが整備されており、大きな状況の進展が見られる。

このような状況の進展を踏まえ、情報システム分野で整備されているガイドラインを活用し、日本としての制御システムセキュリティガイドラインの確立、普及が必要であると考えられる。

(c) セキュリティ技術開発

2000 年時点で課題として指摘されていた制御システムのオープン化は、調査報告書で示したように、制御システムへの情報システム向けの汎用製品や標準プロトコルの採用が今後さらに進んでいくことが想定されるため、PSEC で示された課題は引き続き対応していくことが必要と考えられる。

なお、ここで重要となる観点は、情報システムを対象としたセキュリティ対策技術は 2000 年に比べて大きく進展、普及しているという点であり、このような情報システム向けセキュリティ対策技術を、いかに制御システムの特徴にあわせて適用していくかという点が、一つの重要なポイントであると考えられる。

(d) セキュリティリスク分析手法

2000 年の状況に比べて、情報セキュリティマネジメントの一環としてのセキュリティリスク分析の必要性の認識が広まり、また、そのガイドラインも発行されており、大きな状況の進展が見られる。ただし、これらセキュリティリスク分析の手法自体は対象を限定したものではないが、主に情報システム分野を想定した内容となっている。

このような状況の進展を踏まえ、今後、制御システム分野の特徴を考慮したリスク分析方法及びガイドラインの策定が必要であると考えられる。

(e) セキュリティ評価基準

2000 年の状況に比べて、ISO/IEC 15408 に基づく IT 製品、システムの評価認証制度が国内でも運用されており、大きな進展が見られる。なお、米国では、国立研究所や民間企業による制御システムに特化した認証が行われている。

今後、経営者のインセンティブによる促進を図るという観点で、制御システムを対象とした評価基準、それに基づく認証制度の検討が必要ではないかと考えられる。