重要社会インフラのための プロセス制御システム（PCS）の セキュリティ強化ガイド

邦訳： 一般社団法人 JPCERT コーディネーションセンター

作成： SCADA と制御システムの情報セキュリティに関する情報共有フォーラム（スウェーデン）

The Swedish forum for information sharing concerning information security - SCADA and process control systems (FIDI-SC)

タイトル：重要社会インフラのためのプロセス制御システム（PCS）のセキュリティ強化ガイド

[邦訳注] この文書は、日本の制御システム関係者の参考とするために、JPCERT/CC がスウェーデン緊急管理庁(SEMA: Swedish Emergency Management Agency)の許可を得て英語版から邦訳したものである。

[原典情報]
SEMA 発行
英語版 ISBN： 978-91-85797-23-3
SEMA:s dnr： 0451/2008
デザイン：AB Typoform

この文書の英語版は、SEMA の Web サイト（下記 URL）からダウンロード可能である。
http://www.msb.se/

JPCERT CC®

目次

JPCERT CC®

英語版と日本語版のための序文

この文書は、プロセス制御システム（PCS：Process Control System）のセキュリティに関する意識向上を意図してスウェーデン語で作成された文書の英訳版を邦訳して作成された。

PCS のセキュリティを強化する方法については、すでに多数の推奨事項が示されているほか、いくつかの標準化作業も進められている。

そのような状況にもかかわらず SEMA（スウェーデン緊急管理庁；Swedish Emergency Management Agency）が PCS のセキュリティ強化に関するガイドの制作を決定した理由は、スウェーデン語で流通している情報量が少ないことである。スウェーデン語の情報は、基幹的インフラを運用する中小規模事業者から特に強い要望があった。

SEMA では、この文書を E-SCSIE（European SCADA and Control Systems Information Exchange）などの国際協業パートナーに配布できるようにすべく、この英訳版を作成した。日本語版は、JPCERT/CC が英訳版から SEMA の許可を得て邦訳し作成した。

E-SCSIE は、ヨーロッパの産官学の各界が、さまざまな共通的課題に共同で取り組むことによる恩恵を受けられるようにすること、また、必要に応じて集中的な取り組みとリソースの共有を行うことを目的としている。E-SCSIE の目標は、それがヨーロッパ全体の SCADA（Supervisory, Control and Data Acquisition：監視制御データ収集システム）や PCS に採用され、保護レベルの向上に資することである。

また、スウェーデンの情報共有フォーラム FIDI-SC（次のセクションを参照）参加組織のいくつかは、ヨーロッパのさまざまな地域で積極的に活動を展開している。この文書の英語版は、そのような組織にとっても有用であると考えられる。

この文書の執筆にあたっては、すでに確立している多数の推奨事項や標準を参考にしている。参考文献リストに挙げたすべての組織における貴重な貢献に対し、執筆者一同から感謝の意を表したい。読者諸氏にも、各文献を直接参照して当分野の理解を一層深められることを強くお勧めする。

JPCERT CC®

序文

PCS は、電力、暖房、水道、燃料、運輸（旅客・物流）などの提供を支えるシステムを構成する重要な要素の 1 つである。経営管理用の IT システムでは情報処理自体が最終目的になる場合が多いが、PCS はそうではない。PCS の運用に支障をきたすと、そのシステムに対応した物理的なプロセスに支障をきたす場合もある。究極的には、必要不可欠な社会サービスの提供が妨げられる事態につながる可能性さえある。

現在、PCS を稼働させるためにインターネットなどの公衆ネットワークが使われるケースも増え続けている。したがって、PCS が一般的な IT システムと同じテクノロジを使って提供され、経営管理用 IT システムと結合されるケースも珍しくなくなっている。こうした傾向は、リスクに関する状況に根本的な変化をもたらしている。

SEMA （ Swedish Emergency Management Agency）は 2005 年から、デジタル制御システムのセキュリティ強化に関する FIDI-SC フォーラムを主宰している。このグループの活動は、イギリスの政府機関 CPNI（Centre for the Protection of National Infrastructure）が策定した信頼ベースの情報共有モデルに基づいている。

PCS を扱う複数の産業部門の代表者が定期的に集まり、情報と経験の共有を図っている。FIDI-SC に現在参加している組織は、Banverket（Swedish Rail Administration）、E.ON AB、Fortum AB、SEMA、Norrvatten、Preem Petroleum AB、Stockholm Transport（SL）、Stockholm Vatten AB、Affärsverket Svenska Kraftnät（SvK）、the Swedish Security Service、及び Vattenfall AB である。

この文書の目的は、PCS のセキュリティ強化の必要性に対する注意を喚起することである。ここに示す推奨事項は FIDI-SC メンバの賛同を得たものである。この文書の作成は同フォーラムメンバの惜しみない協力のもと、きわめて円滑に進められた。

この文書『*重要社会インフラのためのプロセス制御システム（PCS）のセキュリティ強化ガイド*』の執筆者は、Åke J. Holmgren（Information Assurance Department, SEMA）、Erik Johansson（Industrial Information and Control Systems, Royal Institute of Technology）、Robert Malmgren（Robert Malmgren AB）の 3 名であり、この文書の最終的な内容について責を負う。

2008 年 10 月 1 日、ストックホルム

Arvid Kjell

SEMA 情報保安部門責任者

目的

この文書の目的は、PCS（Process Control System：プロセス制御システム）のセキュリティ強化に向けた活動を支援することである。制御システムが通常使われている分野として、電力や水道の供給、石油産業、鉄道などが挙げられる。

近年、PCS のセキュリティは大きな注目を集めるようになり、今では、これに関して策定された国際的な推奨事項が多数存在する。

この文書は、PCS のセキュリティに関する基礎的な推奨事項について述べ、また、関連情報を入手するためのヒントも示す。ここに示す推奨事項は、すでに認知されている推奨事項、推奨プラクティス、標準作業手順などを基にしている。

この文書の最初のパート A の部分は、管理職の立場でセキュリティ関連事項にかかわる読者を対象としている。パート B 以降の各セクションは、PCS における実際的なセキュリティにかかわる読者を主な対象として、比較的詳細な内容を述べている。

対象範囲と参考文献の選定基準

この文書は、PCS に固有のセキュリティに主眼をおいており、IT セキュリティ全般をカバーすることが目的ではない。

参考文献として示した標準、ガイドライン、推奨事項は、PCS のセキュリティ強化のため広く適用可能であるものを中心に選定し、特定産業部門に特化せず汎用的な内容であると判断されるものを優先した。また、スウェーデン語と英語で書かれていて、可能な限りインターネットから無償で入手できる資料のみを選んだ。

この文書は次に示す 3 つのパートで構成されている。

パート A

前提条件及び全般的な推奨事項

パート B

各種推奨事項及び確立されたガイドラインに関する詳細なガイダンス

パート C

参考文献リスト及びコメント

その他の情報

この文書は定期的な改訂を予定しているため、内容に関するコメントを歓迎する。

FIDI-SC 及び SEMA へのメッセージは、次の電子メールアドレス宛てに送付されたい。

scada@kbm-sema.se

JPCERT CC®

パート A

前提条件及び
全般的な推奨事項

PCS（プロセス制御システム）

重要社会インフラ機能（電力や水道の供給、地域熱供給、鉄道など）は、その中核にある物理的プロセスの管理・規制・監視において、コンピュータベースのシステムに依存している。

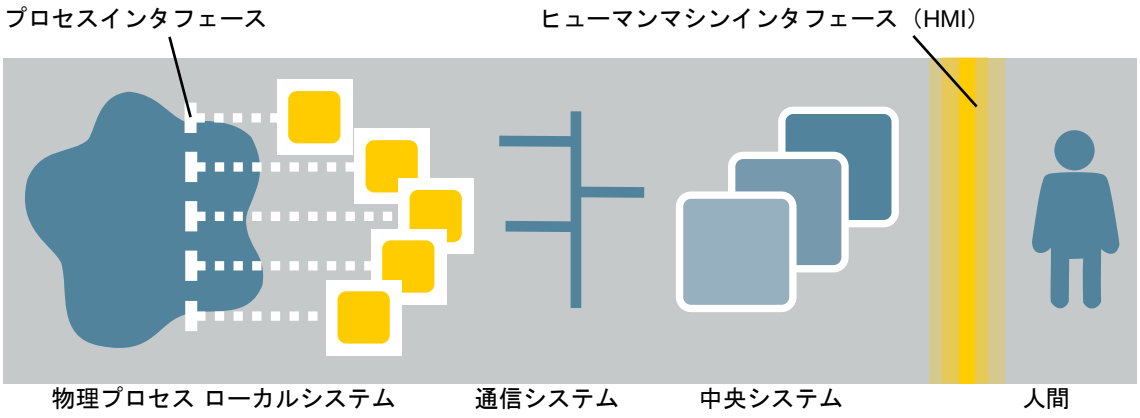
そのようなコンピュータベースの管理・制御システムを指す用語は多数あり、それぞれ微妙に異なっている。この文書では統一して PCS（Process Control System：プロセス制御システム）という用語を使うが、ほかに、同様の概念を表す用語として SCADA（Supervisory, Control and Data Acquisition：監視制御データ収集システム）や、デジタル制御システム、産業情報制御システム、プロセス IT、テクニカル IT システム、DCS（Distributed Control System：分散制御システム）、RTE（Real-Time Embedded：リアルタイム組込み）システムなどもある。これらは厳密には技術的な違いも存在するが、そうした点について、ここでは特に必要のない限り無視した。

図 1 は、制御システムの基本的な構造を示したものである。**物理的プロセス**内には、非常に多くの測定ポイントが（地理的にも非常な広域に分散して）配置されることがある。プロセスインタフェース（物理世界とコンピュータとをつなぐ手段）は、監視用センサや制御用作動装置などである。

ローカルシステムは、センサから送られる信号を収集し、制御信号を制御装置へと送信する。ローカルシステムは多機能化する傾向にあり、たとえば中央システムとの通信が中断している間などは、独立したシステムのように動作することも多い。ローカルユニットは、アナログ・デジタル双方の入出力を備えていることが多い。IED（Intelligent Electronic Device：インテリジェント電子デバイス）、PLC（Programmable Logic Controller：プログラマブルロジックコントローラ）、RTU（Remote Terminal Unit：リモート端末ユニット）などといった機器が含まれるが、それらの違いはあいまいになってきている。

たとえば、高い計算処理能力と、プロセス内の多数の要素から取得される多量のデータを必要とするような重要性の高い機能は、（場合によっては複数の）**中央システム**において実現される。また、データの蓄積や、ピーク時間帯におけるシステム機能間の優先順位付けなども中央システムが行うことがある。

図 1：デジタル制御システムの模式図［Cegrell and Sandberg（1994）の図をもとに改変］



制御システムを構成する各種要素間の**通信**は、携帯電話網などの無線網や、光ファイバや電話網などの有線網を介して、さまざまなプロトコルを用いて行われる。

データの表示や対話的操作のためには、HMI（Human Machine Interface：**ヒューマンマシンインタフェース**）が必要である。HMI は、システム設定（プロセスデータ及びプロセス機能の定義）、プロセスの運用（制御及び監視）、制御システムの保守（システムの変更及び更新）などに利用される。

デジタル制御システムの主要な機能は、次のとおりである。

- **データ収集**（データ蓄積、変換とスケール調整、タイムスタンプ付与、実現可能性評価など）
- **監視**（状態の監視、動向の監視、制限値の監視、パフォーマンスの監視、イベントと警告の管理など）
- **制御**（直接制御、セットポイント制御、シーケンス制御など）
- **計画とフォローアップ**（リアルタイム性を要求されない機能。計画立案、ログと履歴の管理、フォローアップと分析など）
- **保守と変更**（運用の開始、運用状態からの停止、アップグレード、開発環境の管理など）

参考文献

Boyer, S. A. (2004) *SCADA: Supervisory control and data acquisition*. The Instrumentation, systems, and automation society (ISA), Research Triangle Park, N.C.

Cegrell, T. & Sandberg, U. (1994) *Industriella styrsystem*. SIFU förlag, Borås.

JPCERT CC®

PCS のセキュリティが重要である理由

ここでは、PCS のセキュリティに、これまで以上に強い関心をもって取り組む必要性をさまざまな側面から説明する。挙げた項目は必ずしも重要な順ではなく、また、内容にある程度重複している部分もある。

重要社会インフラ機能が PCS に依存している

PCS は、電力、暖房、水道、燃料、運輸（旅客・物流）などを社会に提供するシステムを構成する基幹的なコンポーネントの 1 つである。経営管理用 IT システムでは情報処理自体が最終目的になる場合が多いが、PCS はそうではない。PCS の通信、コンピュータシステム、あるいはアプリケーションの運用に支障をきたすと、そのシステムに対応した物理的なプロセスにまで影響が及びかねない。そのため、究極的には、重要な公益サービスの提供が妨げられる事態につながる可能性さえある。

PCS と経営管理用 IT システムとの接続が劇的に増えている

従来は、周囲と隔離する、または、強力な物理的セキュリティを施して PCS の高度なセキュリティ要求を実現した事例もあった。しかし、今日ではプロセス・システムに対する事業上の観点から、PCS と経営管理用 IT システム（資産管理システム、請求システムなど）とが、しだいに密に結合されるようになっている。また、高度な柔軟性と効率性を実現すべく、インターネットその他の公衆ネットワークによって PCS へのアクセスができる場面も拡大している。こうした接続が、インターネット上などに存在する脅威に対し PCS の脆弱性を露出させている。

PCS の更改ペースは緩やかで、システム全体が一度に入れ替えられることはまずない

PCS は、長期間にわたり運用されることが多く、世代の異なる制御システム（いわゆるレガシーシステム）に基づく技術ソリューションを含む場合がある。導入後の制御システムは、高い可用性と良好なレベルの機能性を長年にわたって維持するよう期待されている。したがって、多くの組織は、定常的に運用されているシステムの中で稼働中の装置に対し、システム設定変更や、システムコンポーネントなどの入替えは極力避けたいと考える。そうした考え方から、既知の IT セキュリティホールへの対処が非常に遅れる、あるいは対処が行われないといった事態が生じうる。

コンポーネントの標準化によってベンダの役割が変化し、ユーザが果たすべき役割が高度化している

従来、PCS のベンダは、総合ベンダとして自ら設計・構築したシステムを提供することがほとんどであった。しかし今日では、従来の IT 領域から発生した技術やコンポーネントの標準化が進行して COTS（Commercial-Off-The-Shelf；市販の既製品）などと呼ばれるようになり、PCS にも使われることが多くなっている。Microsoft 製のオペレーティングシステム、IP ベースの通信技術、Oracle 製のデータベースソリューションなどが COTS の例である。こうした標準コンポーネントの採用に伴い、ベンダの役割は、システムベンダからシステムインテグレータへと変化しつつある。したがって、統合システムを構成する重要コンポーネントの内容をベンダが細かく把握したり調整したりできないといった事態が生じる場合がある。その結果、ベンダ側にもシステムのエンドユーザが利用するデジタル制御システムについて、セキュリティに関する高度な知識が要求されるようになっている。

PCS に対するサイバー攻撃が現実の脅威となっている

サイバー・セキュリティは、PCS の設計において決定的な要素とは見なされてこなかった。装置、システム、ソフトウェアの各ベンダ側にも、それらを購入する側にも、セキュリティに関する意識は概して不足している。そのため、要求仕様の策定時にセキュリティが十分考慮されておらず、システムの設計がセキュリティを適切に扱える内容になっていないのが現状である。インターネットには、サイバー攻撃を

仕掛けるための洗練された無料ツールが出回っている。相互に接続されてネットワークを形成する状況、標準化された IT コンポーネントを使って構築される状況が進行する現在、PCS が、サイバー攻撃の標的となるリスクは非常に大きくなっている。

PCS は高可用性システムであるため、ありふれたサイバー・セキュリティ問題が運用上の深刻な不都合につながる可能性がある

PCS は物理的なプロセスをリアルタイムで監視・制御するものであるため、非常に高い可用性を維持するように開発されている。悪意のあるコードやコンピュータへの侵入など従来からあるサイバー・セキュリティの問題が、プロセス制御の中で発生すると、制御システムの可用性や運用上のセキュリティを損なう可能性がある。たとえば、ウィルスに感染したシステムは、応答性能が実用に耐えないレベルまで低下することがある。その結果、収集データ、警報、コマンドなどの受信が、設計時の本来の意図どおりに行われなくなる可能性もある。

PCS のセキュリティについて検討を進める際に、セキュリティ部門間の文化的な摩擦が生じる

PCS において高度なセキュリティを実現するには、従来からの IT セキュリティに関する知識と、PCS の知識、基礎をなす物理的プロセスの知識とのいずれもが必要である。したがって、セキュリティの作業を能動的に進めるには、異なる文化的背景を持ち、セキュリティに関して異なる流儀を有し、守備範囲の異なる部門の人々との共同作業が必要となる。IT セキュリティの従来知識をそのまま PCS に当てはめることはできない。セキュリティのヒントを含んだ最新の文書の記載や推奨事項は、そのままでは制御装置には適用しにくいものが多い。システムの堅牢化（不要・未知・未使用のソフトウェアを削除し、使用するソフトウェアの設定を強化する）は、実運用中の制御システムにおける実施は非常に難しく、システムベンダが慎重な評価作業を重ねた上でない限り、技術的にも法規制の観点からも、不可能な場合が多い。

PCS のセキュリティに対する関心は高まり続けており、それがセキュリティ要件の標準化につながっている

PCS のセキュリティをどのように確立すべきかについて、標準や推奨事項を策定するための国際的な作業がいくつも進められている。また、この分野に強い関心を寄せる政府機関なども多い。現段階でセキュリティの検討作業に率先して取り組めば、今後 PCS に適用されることになるセキュリティ要件の内容に PCS のユーザやベンダが積極的な影響を及ぼすことができ、ひいては、セキュリティシステムの実装に関して競合上の優位性を獲得できる可能性もある。なお、すでに確立したセキュリティ要件が存在する産業部門もあり、たとえば、アメリカの電力事業者は NERC CIP 標準に準拠することを求められている。

PCS のセキュア化は事業的にも見返りがあるが、そのためには良きセキュリティ風土の醸成と長期的な関与が不可欠である

PCS のセキュリティは、第一義的には技術の問題ではない。もっとも重要なのは、組織としてリスクとコストのバランスを適正化することである。現在ある IT 関連の脅威に対抗できるセキュリティ風土を確立することは、長期的な組織変革であり、組織トップマネジメントの支持のもとで推進する必要がある。一方、今後発生するセキュリティ問題に前もって取り組むことにも多大なメリットがある。従来の IT システムと同様に、PCS も、導入後のシステムに発生したセキュリティ問題の解決の方が、事前対策に比べてはるかに大きなコストが発生するからである。経営管理用 IT システムと制御システムとの接続が進むことは、セキュリティの問題を増大させているばかりではない。そうすることによって、製造プロセスの最適化を通じて、一段と高い効率性や生産性を見込めるという効果もある。

参考文献

Johansson, E., Christiansson, H., Andersson, R., Björkman, G. & Vidström, A. (2007) *Aspekter på antagonistiska hot mot SCADA-system i samhällsviktiga verksamheter.*（スウェーデン語）Swedish Emergency Management Agency, Stockholm.この報告書は次の URL からダウンロード可能である。
http://www2.msb.se/upload/Publikationsservice/KBM/Ovrigt/SCADA_studie%20_070903.pdf

Shaw, W. T. (2006) *Cybersecurity for SCADA systems.*PennWell Corp., Tulsa

JPCERT CC®

経営管理用ITシステムとPCSとの違い

経営管理用 IT システムと PCS との間で共通性が高まっているのは確かであるが、両者には依然として大きな違いもある。表 1 は重要な相違点をまとめたものである。前のセクションで述べた認識と対比しつつ確認されたい。

PCS にセキュリティを適用するには、PCS の特性をよく知ることが不可欠なことはもちろんである。しかし、よく知られている IT 攻撃や、概念的な攻撃手法、IT システム悪用のさまざまな手口（経営管理用 IT 環境においては古典的であったり、常識的であったりするもの）の多くは、デジタル制御システムにも使えるということを認識しておかなくてはならない。

参考文献

NIST (2007) *Guide to Industrial Control Systems (ICS) Security*. SP 800-82, National Institute of Standards and Technology (NIST), Gaithersburg. この報告書は次の URL からダウンロード可能である。
http://csrc.nist.gov/publications/drafts/800-82/draft_sp800-82-fpd.pdf

表 1: 経営管理用 IT システムと PCS との重要な相違点［NIST（2007）の表をもとに執筆者らが改変］

分類	経営管理用 IT システム	PCS
パフォーマンスの要件	リアルタイムでない	リアルタイム
	応答の一貫性が必須	応答の時間が重要
	スループット速度が厳しく要求される	ほどほどのスループットで十分
	遅延と遅延の変動が許容される	遅延も遅延の変動も深刻な問題
可用性の要件	再起動による対応が許容される	産業プロセスの可用性要件により、再起動による対応は許容されない場合がある
	システムの運用要件によっては可用性の一時的欠如も許容されることが多い	停止には数日～数週間前からの計画・スケジュール設定が必須
リスクマネジメントの要件	データの秘密保持（機密性）と正確さ（完全性）がもっとも重要	安全性がもっとも重要（人間、運用システムの両方について）
	耐故障性の重要度は低い－短時間の停止ならば深刻なリスクになることは少ない	耐故障性は非常に重要。ごく短時間の停止も許容されない
	事業上の業務の中断が最大のリスク	人命や、処理設備、操業能力の喪失が最大のリスク
セキュリティアーキテクチャ	コンピュータ関連資産及び格納・伝送される情報の保護に主眼	端末装置（制御装置、PLC など）の保護に主眼
	場合によっては中央サーバに特別のセキュリティが必要	中央サーバの保護は重要

分類	経営管理用 IT システム	PCS
セキュリティソリューション	セキュリティソリューションは一般的な IT システム向けに設計されている	セキュリティツールが制御システムの通常の運用を妨げないことを保証するテストは必須
対話操作の即時性	非常時における対話性の重要度は低い	非常時における対人応答性やその他の応答性がきわめて重要
	システムリソースへのアクセスは管理上望ましい程度に制限可能	制御システムへのアクセスには厳格な規制が必要－操作性を阻害してはならない（非常時には特に重要）
システム運用と変更管理	標準的な OS を使うように設計されたシステム	特定用途向けに開発または改変された OS と、標準的な OS の混在
	アップグレード作業は単純、セキュリティポリシーや定形的な手順に従って実施－既存の自動化ツールがある	改造されたハードウェアやソフトウェアが存在するなどの理由により、ソフトウェアアップグレードは段階的に実施すべきで、多くの場合はシステムベンダの関与が必要
リソースに関する制約	サードパーティ製アプリケーション（セキュリティソリューション）の追加に対応する十分なシステムリソースを使用可能	システムは産業プロセスに特化して設計されている。メモリ容量や処理能力リソースによりセキュリティソリューションが制限されることがある
通信	標準的な通信プロトコル	独自の通信プロトコルが多数あり（商用）、標準プロトコルも使用
	主に有線通信網と無線 LAN	さまざまな種類の通信媒体。たとえば、光ファイバ、無線リンク、衛星通信（私設網の場合でさえ）など
	IT ネットワークの一般的な慣行に基づいて構築された通信ネットワーク	制御システムの技術的知識を必要とする複雑な通信ネットワーク
サポート	さまざまな形態、多数のベンダ	普通は少数のベンダのみ
サービス稼働期間	コンポーネントとシステムの更改期間が短い（通常 3～5 年程度）	コンポーネントもシステムも更改期間が長い（通常 15～20 年程度）
物理的アクセス	コンポーネントは普通、近辺に設置され、アクセスが容易	コンポーネントは、隔離して設置され、地理的にも遠隔地で、アクセスが困難な場合がある

良きセキュリティ風土 — 基本的な要件の１つ

PCS のセキュリティを確保するための、円滑に機能する行動を確立するには、良きセキュリティ風土を組織に根づかせる必要がある。すなわち、実効性のある全般的なリスク管理と、体系的な情報セキュリティを伴った業務作業である。図 2 は、体系的なリスク管理に含まれるべきさまざまな活動の間の関係を示している。

この文書で示した推奨事項は、ISO/IEC 27001（ISO、2005）の情報セキュリティ管理モデルをはじめとする、ISO の情報セキュリティ標準（27000 シリーズ）に準拠している。

IT システムのリスク分析に関しては非常に多くの分析手法が存在する。SEMA では、基本的な情報セキュリティ水準について定めた BITS と、それに対応した情報セキュリティ分析ツール（BITS Plus）を公表している。BITS と BITS Plus を利用すると、組織内で、情報セキュリティに関する作業に着手し、上記の ISO 標準などを導入することが容易になる。BITS や BITS Plus 以外にも、IT システムのリスク分析に関する汎用的なモデルを示した、米国の NIST による報告書 SP 800-30 などがある（NIST、2002a）。また、NIST 報告書 SP 800-34 は、IT システムにおける緊急時対応計画を扱っている（NIST、2002b）。

今のところ、特に PCS のサイバー・セキュリティを対象とした確立されたリスク分析手法は、執筆者らの知る限りでは存在しない。

参考文献

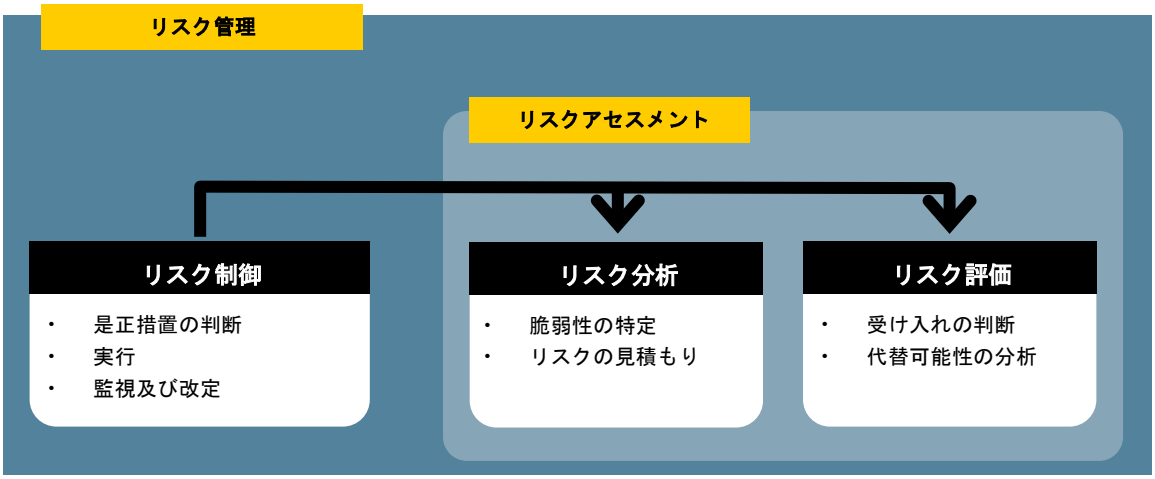
IEC (1995) *Dependability Management - Part 3: Application Guide - Section 9: Risk Analysis of Technological Systems.* International Electrotechnical Commission (IEC), Geneva.

ISO (2005) *Information technology - Security techniques - Information security management systems - Requirements.* ISO/IEC 27001:2005, International Organization for Standardization (ISO), Geneva.

NIST (2002a) *Risk Management Guide for Information Technology Systems.* SP 800-30, National Institute of Standards and Technology (NIST), Gaithersburg.この報告書は次の URL からダウンロード可能である。
http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

NIST (2002b) *Contingency Planning Guide for Information Technology Systems.* SP 800-34, National Institute of Standards and Technology (NIST), Gaithersburg.この報告書は次の URL からダウンロード可能である。
http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf

図 2：リスク管理［IEC（1995）をもとに執筆者らが改変］



PCS のセキュリティ強化のための推奨事項の要約

パート B で、各種推奨事項及び確立されたガイドラインの、より詳細なガイダンスについて述べる前に、このパート A においては、特に重要な推奨事項を要約しておく。

これらの推奨事項は、FIDI-SC における議論と、執筆者らが参加した実践的なプロジェクトをとおして得られた経験に基づいて選定したもので、国際的な推奨事項や広く知られたプラクティスにも沿っている。

次に示す推奨事項が、PCS のセキュリティを強化していく作業の第一歩である。

1. **PCS のセキュリティを強化する必要性について組織全体の意識を向上させる。**
   これは組織使命に係る重要な事項なので、早い段階から組織のトップマネジメントが関与すべきである。

2. **PCS のセキュリティに関する基礎的なトレーニングを実施する。**
   制御システムのオペレータに、従来の IT セキュリティに関する知識を教える必要がある。また、IT 担当者は、PCS とそれに対応する物理的プロセスについて一層深く学ぶ必要がある。PCS の調達及び運用計画の関係者にも、これらの事項に関するトレーニングが必要である。

3. **可能な限り PCS と経営管理用 IT システムとを分離しておく。**
   PCS の現状を調査し、PCS への接続点を洗い出す必要がある。PCS と経営管理用 IT システムとの結合は、例外的な場合だけに限定すべきである。結合する場合にも、非常に高度な仕組みで、両システム間の論理的分離をはかる必要がある。

4. **セキュリティ要件をすべての PCS 調達文書とサービス契約に書き込む。**
   セキュリティ問題に前もって取り組むことにより、多大なメリットが得られる。従来の IT システムと同様に、PCS も、導入後のシステムに発生したセキュリティ問題を解決するためのコストの方が、事前対策のコストに比べて、はるかに大きいからである。

JPCERT CC®

パート B

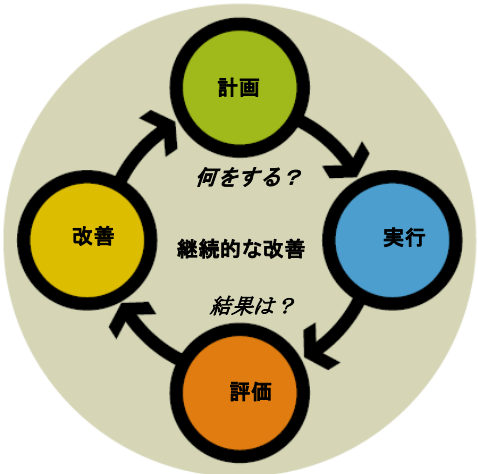
各種推奨事項及び確立されたガイドラインに関する詳細なガイダンス

推奨事項の策定のための基礎

このセクションでは、PCS のセキュリティ強化のための推奨事項を示す。推奨内容は、FIDI-SC における議論と、執筆者らが参加した実践的なプロジェクトをとおして得られた経験に基づいて選定したもので、海外の報告書や広く知られたプラクティスとも整合したものである。推奨事項の順序は必ずしも重要な順ではなく、相互に重複した内容も含まれる。

以下の推奨事項が示唆している活動は、品質にかかわる日常的な作業の一部に位置づけられるものである。継続的な作業の一環としてこれらの活動を行うことの重要性がよくわかるように、有名なデミングサイクル（図 3）との関連を示した。デミングサイクルの考え方は、PDCA（Plan-Do-Check-Act ; 計画・実行・評価・改善）モデルとも呼ばれ、情報セキュリティマネジメントシステム (ISMS) の標準である ISO/IEC 27000 シリーズなど、いくつかの国際標準にも採用されている。目的とするところは、組織における PCS セキュリティのための作業が、このモデルに従い、情報・セキュリティ・品質に関するその他の作業と自然に連携して進められるようにすることである。

図 3 : 継続的な改善活動の重要性を強調し、推奨事項を体系的に整理するために、この文書では PDCA モデル（デミングサイクル）を採用する



Plan（計画）フェーズ
ポリシー・目標・プロセス・定形手順を確立する。

Do（実行）フェーズ
ポリシー・措置・プロセス・定形手順を導入及び実施する。

Check（評価）フェーズ
査定・測定・報告によって監視及び監査を行う。

Act（改善）フェーズ
維持・改善を行う（すなわち、改善のための是正措置を決める）。

以降の各セクションでは、より詳細な情報への手引きとなるヒントを示した。参照すべき、すでに確立されているガイドラインや標準は、**パート C** で詳しく述べる。以降では、それらを表 1 のように略号で示している。

表 1　参照すべきガイドラインと標準

NERC CIP	サイバー・セキュリティ標準 Cyber security standard CIP-002-1 - 009-1
NIST 800-82	工業用制御システムのセキュリティのためのガイド Guide to industrial control systems (ICS) security
CPNI GPG	プロセス制御と SCADA セキュリティ・ガイド Good practice guide process control and SCADA security
DOE 21 Steps	SCADA 網のサイバー・セキュリティ強化のための 21 カ条 21 steps to improve cyber security of SCADA networks
OLF 104	PCS と安全システムと支援 ICT システムのための情報セキュリティ基本要件 Information security baseline requirements for process control, safety, and support ICT systems
PL	PCS の調達におけるサイバー・セキュリティの文言 Cyber security procurement language for control systems

JPCERT CC®

PCSのセキュリティ強化のための推奨事項

01 PCS のセキュリティに関する役割と責任範囲を明確化する。

02 PCS の調査とリスク分析のための手順を確立する。

03 PCS の変更管理のための手順を確立する。

04 PCS の緊急時対応計画とインシデント管理のための手順を確立する。

05 PCS のセキュリティ要件に関する記載を、最初から、すべての計画・調達作業に含める。

06 良きセキュリティ風土を醸成し、PCS におけるセキュリティの必要性に関する意識を向上する。

07 PCS 内に何重ものセキュリティ対策を作り込む（多層防御）。

08 24時間体制の侵入検知とインシデント監視体制を PCS に導入する。

09 PCS のリスク分析を実施する。

10 PCS 及び関連ネットワークに対し、技術的なセキュリティ監査を定期的に実施する。

11 PCS の物理的なセキュリティ水準を継続的に評価する。

12 セキュアでかつ適切なものだけしか PCS に接続されていないことを確認する。

13 システムベンダの協力を得て、PCS を堅牢化及びアップグレードする。

14 自組織の PCS で発生したインシデントの経過を追跡管理するとともに、組織外で起きたセキュリティ問題について情報を収集し分析する。

15 ユーザグループ、標準化機関、その他のネットワークとの間に、PCS のセキュリティ強化を目的とした連携協力関係を構築する。

01 PCS のセキュリティに関する役割と責任範囲を明確化する

■ **NERC CIP**（003-1） ■ **NIST SP 800-82**（4.2 章、6.1 章、6.2 章）
■ **CPNI GPG**（GPG 4、GPG 7） ■ **DOE 21 Steps**（No. 12、16、20） ■ **OLF 104**（No. 1、3）

経営管理用 IT システムに関しては多くの組織で、作業分担指向の管理を行うことが一般化している。この管理モデルでは、システム主管者、情報主管者、統括管理者、運用管理者、システム管理者などといった役割が割り当てられていることが多い。

一方、制御システムにおいては、こうした役割や責任範囲が割り当てられていないことが多い。それは、責任モデルと管理モデルの双方が欠落していることを意味する。IT 技術者やシステム管理者がいないことから、技術サポートはベンダの担当者に任せきりとなっていることもままある。さらに、制御システムのサイバー・セキュリティに関して何の知識も持っていないプロセス技術者によってシステム管理作業が行われている場合も見受けられる。このため、PCS の IT 関連の技術について、当該システムを運用する組織がほとんど知らない、あるいはまったく知らないという状況が生じる。その結果、技術とその利用を管理するための能力水準が低下し、管理策も甘くなる。

セキュリティ問題に関する責任の所在を明らかにするには、PCS のためのセキュリティポリシーを作成するのがもっとも簡単な方法である。このポリシーを規定する文書は、独立したものであっても組織の情報セキュリティポリシーの一部であってもよい。ただし、独立した文書の場合は、組織内のその他のポリシー文書と関連づけられていることが必要である。

経営管理用 IT システムに関する役割及び責任範囲の割当と、制御システムに関するそれらの割当との間には整合性が必要である。どのシステムが組織の本部 IT 部門によって管理され、どのシステムが製造部門でローカル管理されるかが明確化されていなければならない。これを純粋に実際的なレベルでどのように達成するかは、当該組織が、防護策や防御壁の階層を IT 環境全体の中にどう実装しているかと関係している。プロセスと密接に関係したシステムの大部分を現場がローカルに管理するとしても、セキュリティ問題についての全体的な統合性や統一的アプローチの確立に関しては、組織の本部 IT 部門が責任を持つ必要がある。情報セキュリティに組織として統一的にアプローチすることが必要とされる大きな理由として、制御システムと管理システムの間で広範なデータ交換がなされることが一般的になりつつある動向を挙げることができる。

リスクと問題の例

IT 部門の人間が、制御システムの主管者やシステム調整者やシステム管理者に誰も任命されていなかった場合、定形的なセキュリティ関連作業（ソフトウェア更新、いなくなった契約社員のアカウント閉鎖など）が実施されていないか、適切なタイミングで実施されていない可能性が大きい。

たとえば、システムが悪意のあるコードなどに感染しても、そのインシデントに対処する責任を誰も感じないか、感じたとしても、そのインシデントへの対応のために自分にどのような権限があるのかわからない。そのため、被害の拡大防止行動が遅れ、運用に必要以上の悪影響が生じる可能性がある。

JPCERT CC®

02 PCS の調査とリスク分析のための手順を確立する

■ **NERC CIP**（002-1） ■ **DOE 21 Steps**（No. 13） ■ **OLF 104**（No. 2、3、11）

PCS のセキュリティを実現するためには、組織内の情報の流れ及びシステム依存関係（さまざまなシステムや運用の間に存在している結びつき）を調査し把握するための手順を確立することが重要である。

組織のプロセス、システム、情報に関する分析は、なんらかの機能が故障または停止した場合に、プロセスと組織にどのような影響が及ぶかを理解したうえで行われなくてはならない。この前提条件は、もっとも重要なシステムと情報に関して、適切なリスク評価や分類を行うために重要である。

組織及びシステムに関する調査を通じて、可能性があるアクセスと接続、システム分類、及び運用優先度の分類に関する各種のリストを作成する。重要なコンポーネントやシステムを特定できるように、十分に詳細な情報を書き込んだ PCS システム図が必要である。システム図に含まれるべき情報は、たとえば、コンピュータリソースの OS に関する情報、IP アドレス、通信プロトコル、ローカルユニット（PLC など）の技術情報などである。サイバー・セキュリティ上の境界線を設定するには、PCS に対する接続をすべて洗い出す必要がある。この接続には、イントラネットのほか、協業パートナーやベンダに対するリモート接続、インターネット接続などが含まれる。このとき、すべての無線接続はリモート接続ポイントとして扱い、また、組織の経営管理用 IT システム（イントラネット）に対する接続は外部接続として扱わなくてはならない。

組織にとっての基幹的な重要資産については、リスクベースのアプローチによって特定する必要がある。この分析に基づいて、重要サイバー資産が特定される。この作業を行うには、リスク分析のための手順と、どのような条件の時にリスク分析を見直すべきかを明文化しておく必要がある。採用するリスク分析手法は、分析の目的と利用可能な情報に応じて選定する。リスク分析の見直しをしやすいように、不必要に高度なリスク分析手法を採用することは避けなければならない。

リスクと問題の例

PCS のリスク分析や調査のための手順を組織として標準化しておかないと、組織のリスクが時間の経過に伴ってどのように変化したかを比較・監視することが困難になる。

また、組織がリスクアセスメントを実施していない場合、重要な PCS が保護されない状態で放置される可能性がある。その一方で、組織の存続にかかわるほど重要とはいえないような情報リソースを保護することに必要以上のリソースを費やしている可能性がある。

03 PCS の変更管理のための手順を確立する

■ **NERC CIP**（003-1） ■ **DOE 21 Steps**（No. 17） ■ **OLF 104**（No. 10、15）

パラメータ構成や、設定、データファイル、プログラムに関する、適切な変更管理とバージョン管理が、デジタル制御システムのサービス中断や無用なトラブルシューティング作業、深刻な問題などが発生するのを防ぐために、重要である。たとえば、産業プロセスで長期にわたって使用するシステムやアプリケーションに対して、変更管理を厳格に行うためには特別な定めが必要である。

ソフトウェアのアップグレードは段階的に実施し、法律上及び技術上の理由により、多くの場合はシステムベンダの立ち会いが必要となる。PCS 環境では、システムが現在どのように設定され、どのような運用状態にあるかについて、すべての関係者（ベンダ、システム管理者、ユーザ）が共通の正しい認識を持っていることが重要である。経営管理用 IT システムの場合、テスト環境、開発環境、運用環境が別々に用意されることが一般的であるが、これは PCS には残念ながら当てはまらない。したがって、PCS においては、適切な変更管理ができる条件づくりのために追加の財源が必要となる場合もある。

PCS に対する変更を承認する方法について、公式な手順が定められていなくてはならない。いかなる変更も、公式な承認を経ずして行われてはならない。これは、一時的な変更や補助的な装置に対する変更についても同様である。基幹的なシステムのセキュリティを良好に保つには、明示的に許可されていないことは原則としてすべて禁止すべきである。

変更管理の公式手順において定義されるべき項目には、変更の実施を承認する手続き、変更前後のテスト実施方法の記述（別個のテスト環境におけるテストを要する変更についての説明を含む）、変更実施後の文書更新の方法に関する要件、及び、変更に関する情報を各人員に伝達する方法（たとえば、オペレータに対して特別なトレーニングが必要となる場合など）がある。

リスクと問題の例

あるベンダが、テストシステム上で変更を検証したが、そのテストシステムの構成が顧客の運用している実稼働システムとは異なっていた。後日、その変更を実稼働環境に適用すると、予期しない事態が発生して PCS が不安定になってしまった。

制御システムの設定変更がローカルで実施されていたことを、ベンダは知らされていなかった。その後に、プログラム更新が行われると、システムが機能しなくなり、セキュリティ問題に対する修正も未適用の状態になり、パラメータも出荷時のデフォルト設定に戻ってしまった。

PCS は、情報システムと比べてソフトウェアの状態が変化しないものが多く、そのため定期的なバックアップがあまり頻繁に実施されない傾向がある。システムの稼働開始時や大幅な変更を実施するタイミングでしかバックアップを作成していない事例もある。こうした場合、バックアップコピーから再インストールを実施する際に、変更内容が失われたり、再適用作業が見落とされたりするリスクがある。

JPCERT CC®

04 PCSの緊急時対応計画とインシデント管理のための手順を確立する

■ **NERC CIP**（008-1、009-1） ■ **NIST 800-82**（6.2.3 章） ■ **CPNI GPG**（GPG 3）
■ **DOE 21 Steps**（No. 19） ■ **OLF 104**（No. 7、16）

深刻なサービス中断の事態が発生したときにも組織を確実に存続させるには、非常時における役割と責任範囲などを明確に定めた、緊急時対応計画を用意しておくことが不可欠である。深刻な事態としては、停電、制御システムの故障、重要な運用担当者の傷病などが考えられる。

緊急時対応計画については、計画内容の検討と変更を継続的に行うことに加え、要員に対応準備トレーニングを受けさせたり、非常時にも十分に運用が維持できることを確認するテストを定期的に実施することが重要である。また、PCS については、バックアップを確実に保存し、システムの復旧に使用できる状態を維持しておくことが特に重要である。緊急時対応計画に盛り込むべき重要な事項としては、次のようなものがある。

- 運用操作を手動で行う（コンピュータの支援なしでプロセスを制御する）場合の手順
- データ及び設定内容を復旧し、プロセスを再開するための手順
- オペレータ、サービス技術者、その他担当要員、ベンダ、サポートの連絡先情報
- 制御システムの中核的コンポーネントを入れ替える方法
- 事態が深刻な場合における、非常時の運用方法と緊急時指令センターの設置場所

後で実施する分析作業のために、PCS の中断（サービスを利用できない、または機能が制限される状況など）につながるすべての事態を文書化する必要がある。インシデント管理について注意すべきは、通常の業務プロセスの障害になるとの懸念なしにインシデントを報告できるような、バランスのとれた構造を決めておくことである。また、インシデントを報告することの目的を周知して、組織に協力意識を醸成することや、インシデント管理の成果を伝えることも重要である。こうした周知活動を行わないと、インシデントや問題点を報告するモチベーションを維持できない可能性がある。

リスクと問題の例

ある組織で深刻な障害が発生し、ミッションクリティカルな PCS を完全に復旧せざるを得なくなった。バックアップは定期的に実施されていたが、バックアップテープの取扱いが不適切で、復旧不可能なほどテープが劣化してしまっていた。

ある組織で、PCS の運用責任者が休暇中に死亡した。しかし、その人の職務を代行できる人が組織内に誰もおらず、大問題となった。さらに、特殊なシステム変更を実施するための非常に重要なパスワードや、中核的システムの一部の設定方法を、死亡した責任者だけしか知らなかったことが後で判明した。

JPCERT CC®

05 PCS のセキュリティ要件に関する記載を、最初から、すべての計画・調達作業に含める

■ **NIST 800-82**（6.1.3 章） ■ **CPNI GPG**（GPG 6） ■ **OLF 104**（No. 8、9）
■ **PL**（すべての章）

組織におけるセキュリティの問題は、できる限り早い時期に計画作業に盛り込むことが非常に重要である。

PCS の実装が済んだ後に満足なレベルのセキュリティを実現することは難しく、コスト負担も大きい。セキュリティ要件は、システム仕様の策定とニーズ分析において最初の段階から盛り込まれるべきものである。多くの場合、システムソリューションはその一部または全部を外部から調達することになるので、調達時にも、セキュリティについて特段の注意を払う必要がある。

PCS のセキュリティについて、調達のための文書、検収テスト及び引渡し管理、契約、また、保守やサービスの実施に関する指示文書の中で明文化すべきである。調達は、新規にソリューションを導入する場合にも、既存ソリューションの一部または全部を入れ替える場合にも行われる可能性がある。したがって、サービス契約や保守契約も含め、ベンダとのあらゆる契約書に、セキュリティ要件を重要な要素として盛り込むべきである。あらゆる制御システムの調達に際し、Cyber Security Procurement Language for Control Systems（PL）が技術的な参考になる。

PCS を更新する際には、IT セキュリティの問題について特別の配慮が必要である。というのも、そうした変更は、既存の制御システムに対し、当初の設計者が想定していなかった影響を及ぼす可能性が非常に大きいからである。たとえば、古い制御システムは、装置のある場所に物理的に出向く以外の方法で装置にアクセスできない前提で設計されていたものが多かった。しかし、今日では物理的に隔離しておくことが不可能な場合が増えた。むしろ PCS を構成するさまざまな要素間をどのようにして論理的に分離するかが問題となっている。

要件の収集は、さまざまな調査や、脅威及びリスクの分析によって実施する必要がある。ベンダは、システムやアプリケーションのセキュリティ機能及び保護機能に関する詳細要件を満たすだけでなく、セキュリティに関する作業の品質を保証するための手法や手順（たとえば、社内開発者向けハンドブックなど）を示すことができなければならない。

リスクと問題の例

調達時にセキュリティ要件が考慮されていないと、追加発注が必要になって大きなコストが発生したり、追加されたセキュリティソリューションの質が低くなったり、必要以上に複雑になってしまったりする可能性がある。

調達時にセキュリティ要件が見落とされると、PCS が無用の脆弱性を抱えたまま、システムの寿命が尽きるまで運用されることになる可能性もある。

JPCERT CC®

06 良きセキュリティ風土を醸成し、PCS におけるセキュリティの必要性に関する意識を向上する

■ **NERC CIP**（004-1） ■ **DOE 21 Steps**（No. 21） ■ **OLF 104**（No. 5）

PCS のセキュリティはミッションクリティカルの問題であるという理解を定着させることが重要である。考え方を理解し行動に結びつけるまでには、時間をかけた取り組みが必要である。セキュリティ関連の問題は常にそうであるが、トップマネジメントによる積極的な関与も非常に重要である。これは、PCS のセキュリティには追加のリソースが必要になり、通常は一緒に仕事をすることがない部署間の共同作業が必要になるためである。

PCS の高度なセキュリティを実現するには、従来からの IT セキュリティに関する知識と、PCS の知識、基礎をなす物理的プロセスの知識がいずれも必要である。したがって、セキュリティの作業を先行的に進めるには、文化的背景も異なり、セキュリティに関する流儀も異なり、所属部門も異なる人々の間の連携と信頼関係が必要となる。そのためには、IT 担当者と制御システムオペレータの両方に対して教育やトレーニングを定期的に実施しなくてはならない。

PCS は、非常にサービス提供期間の長いシステムソリューションに組み込まれるものである。したがって、そのシステムが将来的にどう使われる（あるいは誤用される）可能性があるかを想像する努力が特に重要である。ごく普通の活動でも、知識が不足していたり定形作業が不明確だったりした場合には、潜在的なセキュリティ問題につながる危険性をはらんでいる。

組織は、IT に対する全般的なアプローチのために、管理上のセキュリティプログラムを確立すべきである。それにより、セキュリティ意識を向上させ、批判的な思索を促し、セキュリティ強化につながるやり方で作業する前向きの態度を引き出すことができる。

リスクと問題の例

ある運用者が、定形的な運用において暇な時間帯に運用者用のコンピュータを使ってインターネットのスポーツ中継（ビデオとオーディオのストリーミング放送）を視聴すると同時に、IRC を使って友人とチャットした。これが原因で、運用者用コンピュータがスパイウェアに感染し、やがて使用不能な状態になってしまった。

数人のサービス技術者が、実稼働システムのある施設でベンダのフィールド担当者と一緒に作業していた時、ソフトウェアやデータを 2 つの IT 環境間で受け渡す必要が生じた。通常、データ移動には特殊なリムーバブルハードディスクを使うことになっていたが、彼らはハードディスクを取りに行かずに済ませようと、本来別々のネットワーク上にある 2 台のコンピュータをネットワークケーブルで互いに接続してデータを受け渡した。就業時間が終わった時に、彼らはネットワークケーブルを外すのを忘れて帰ってしまった。普段そのコンピュータを使っている運用者は、ケーブルはそのままにしておくべきだと考えた。こうして PCS は、物理的に隔離された状態から、イントラネットに直結された状態となった。この組織では、制御システムは常に物理的に隔離されていることを前提としていたため、ウィルス対策ソフトをインストールする必要性はないと考えられていた。

JPCERT CC®

07 PCS 内に何重ものセキュリティ対策を作り込む（多層防御）

■ **NERC CIP**（005-1、007-1） ■ **CPNI GPG**（GPG ファイアウォール展開）
■ **DOE 21 Steps**（No. 5、15） ■ **OLF 104**（No. 4、13） ■ **PL**（すべての章）

現在の IT システムの保護に用いられる 1 つの基本的な考え方として、多層防御の構成、つまり、複数のセキュリティ階層と、複数の重複させたセキュリティ機構を導入する方法がある。重複させるセキュリティ機構は、同じ種類である場合もあれば（複数層のファイアウォールなど）、相互補完的な複数種類のセキュリティ機構である場合もある（ネットワークセキュリティ保護策としてのファイアウォールと、IT システムアクセス用の強力な認証を組み合わせるなど）。

どのような種類の組織も、情報の取扱いにおける効率化について強い圧力を受けているので、作業の重複を避けるため、情報システム間を接続する（1 つの IT システムに格納されている情報を別のシステムに人手をかけて再入力するといった作業を不要にする）ことが推進されている。しかし、古い PCS（つまり、製造現場内のコンピュータ）には、物理的なセキュリティさえ確保されていればよかった時代に開発され、サイバー・セキュリティなどまったく考慮されていないものが多い。経営管理用 IT システムの世界では、何年も前に修正されている既知の欠陥や脆弱性が、PCS においては長期間残存していることも珍しくない。そのため、さまざまなネットワークを相互接続すると、PCS が、なんら対策を講じていない脅威にさらされ、それらシステムへの外部接続が重大なリスクが生む可能性がある。したがって、制御システムと経営管理用 IT システムを結合する際には、前もって基本的なリスク分析を実施しなくてはならない。システム間の相互接続には、きわめて質の高い IT セキュリティが必要である。

遅かれ早かれ必ず実施しなくてはならない作業の 1 つは、PCS と運用システムの周りにファイアウォールを形成することである。概念レベルにおいて、組織内で、あるシステムのデジタル的な全体状況を決定しているシステムと、それ以外のシステムとを見分けられることが重要である。

PCS 内は、各種システムの重要性の程度に応じた段階的なセキュリティレベルに基づいて、いくつかのゾーンに分割されるべきである。すなわち、重層的なセキュリティメカニズムによってネットワーク内に区画を設け、あまりセキュアでないサービスや接続を、いわゆる非武装地帯（DMZ）に配置する、ということである。

ほかの外部システム（ビジネスシステムなど）が接続された DMZ 経由で、デジタル制御システム同士のデータ交換を行う作業は、限定的に、かつ管理された状態で実施すべきである。制御システムからビジネスシステムへの外部接続は、使用するサービスの種類とポートを制限しなくてはならない。一つのネットワーク内でも通信相手に応じて異なる通信プロトコルを使用することが適切な場合もある。たとえば、制御システムと DMZ の間で使用する通信プロトコルは、DMZ と組織の経営管理用 IT システムとの接続に使用する通信プロトコルとは違っていることが望ましい。

制御システム内の通信でも、やはり保護が必要である。フィールド装置（PLC など）とローカルシステムとの通信は、セキュリティが弱い（または存在しない）産業用プロトコルによって行われるのが普通だからである。

リスクと問題の例

ある組織では、「知らせないことによるセキュリティ」（嘘や隠蔽によるセキュリティ）では、セキュリティソリューションとしての実効性がないことを認識し、強力で包括的な機能を備えているはずのセキュリティファイアウォールを導入した。ところが、ある社員がワークステーションをセキュリティ保護のない接続を介してインターネットに接続したため、ファイアウォールのセキュリティに穴ができた。多層防御されていない状態では、いったんシステムに侵入されると、そこから先はセキュリティメカニズムがないため、悪意のあるコードやハッカーによる被害を食い止められない。

物理的セキュリティと電子的セキュリティに作業量やリソースをどう配分するかについては、バランスを保つことが重要である。コンピュータのバックアップ、鉄扉など、物理的セキュリティは、抽象的なサイバー・セキュリティよりもわかりやすいため、バランスはともすると物理的セキュリティに偏りやすい。しかし、誤った考えによって物理的セキュリティ偏重に陥ると、例えば、物理的にシステムを二重化したのに、ネットワークのブロードキャストストームなどデジタル的な原因または、基幹ネットワーク機器のハードウェア故障など物理的な原因から、プライマリ・システムにもセカンダリ・システムにも同じ問題が発生して正常に動作しないことになりかねない。

08 24 時間体制の侵入検知とインシデント監視体制を PCS に導入する

■ **NERC CIP**（005-1） ■ **DOE 21 Steps**（No. 8）

インシデント事例収集（公開情報に基づく分析）や、リスク分析の見直し作業とは異なり、侵入検知及びセキュリティ監視は、当該組織に対する攻撃の試みそのものを分析することを目的とする。公開された情報と、自組織のシステム及び通信に関する十分な監視結果を組み合わせると、攻撃手法の変化の動向や悪意あるコードの最新情報など、脅威の全般的な状況をかなり的確に把握できる。

侵入検知システム（IDS）には 2 つの種類がある。1 つは通信フローを分析することで攻撃の試みを認識するシステム（ネットワークベースの侵入検知システム、NIDS）であり、もう 1 つは、コンピュータシステム上のイベントやアプリケーション内での利用パターンを監視するシステム（ホストベースの侵入検知システム、HIDS）である。また、IDS が進化した侵入防止システム（IPS）と呼ばれる種類のものは、攻撃を検知するだけでなく能動的に攻撃を無効化する機能を備えている。

PCS 内に IPS を設置する場合、適切な分類を行わないと正当なトラフィックが遮断される（いわゆるフォールスポジティブが発生する）可能性があるため、注意が必要である。事前予測できないような条件で、制御コマンドや結果コードを遮断するセキュリティシステムは、PCS には受け入れられない。

実際に試みられている攻撃を検知するために、いわゆるハニーポットという手法も用いられる。制御システムに適した単純なソリューションとしては、通常はトラフィックを受信しないコンピュータをネットワーク上に設置し、これがトラフィックを受信した場合に警報を発信するという方法が考えられる（このようなハニーポットは、カナリーあるいはハニートラップと呼ばれることもある）。このコンピュータに対してなんらかの通信が試みられたということは、攻撃が現に行われているか、敵対者がネットワークの状況を調べて攻撃の準備を進めている可能性を示唆している。

IDS によって収集されるログや追跡データは、詳細な調査が後日必要になる場合に備えて十分な長期間にわたり保存することが重要である。最初の兆候を見つけるために数ヶ月前の記録までさかのぼることが必要になる場合も多い。

リスクと問題の例

ある IDS は、PCS で使われる特殊な通信プロトコルを理解するように設計されていなかったため、攻撃や攻撃試行の検知に失敗した。

あるネットワークベースの IPS は、通信に対して不適切な反応を示し、正当なトラフィックを遮断して運用の中断を引き起こした。

JPCERT CC®

09 PCS のリスク分析を実施する

■ **NERC CIP**（002-1） ■ **NIST SP 800-82**（3.2～3.6 章） ■ **DOE 21 Steps**（No. 14、18）
■ **OLF 104**（No. 2）

セキュリティ担当部門においてもっとも重要な活動の 1 つは、リスク分析を定期的に実施してその結果を評価することである。運用の中断、事業上の損失、あるいは、死傷者の発生や環境への打撃を生じる最悪のケースを避けるためにとるべき措置の判断材料となる情報を得るうえで、リスク分析はもっとも重要な手段である。

IT システムのリスクアセスメントを行う際に出発点とすべきもっとも基本的な前提は、「敵はこちらのシステムを知っている」（シャノンの原理）ということである。しかし残念なことに、PCS においては、ベンダ特有のソリューションを外部の者が詳しく知っているはずがない、と思い込んでいる人が多い。この思い込みは、隠蔽によるセキュリティあるいはあいまいであることによるセキュリティなどと呼ばれるが、敵対者には攻撃手法や攻撃ポイントなどに関して非常に広範な選択肢が与えられており、有効に機能することはまずない。つまり、通信プロトコル、暗号化ソリューション、OS などがベンダ特有だとしても、それはセキュリティを保証する要素にはまったくならない。実際に PCS を広く研究者や専門技術者に検証させると、むしろ、セキュリティが容易に破られる結果になる場合のほうが多いほどである。

リスク分析は、特定のサブシステムに対して実施したり、より全般的な運用に関して実施したりしてもよい。組織では、事前に確立し文書化した手法に従って定期的にリスク分析を見直す必要がある。個々のケースでどのようなリスク分析手法を採用するかは、分析の目的と、対象システムについて入手できる情報の内容（そのシステムに対する脅威の情報も含む）に応じて決定する。リスク分析見直しのために、システム調査の見直しも必要になる場合もあるが、システム調査が目標とするところは、システム図などの文書を常に最新の状態に保つことである。また、当該組織においては、以前実施した運用分析に基づいて、どのシステムや情報リソースがミッションクリティカルな重要性を持っているかは特定してあるはずである。

リスク分析の文書化作業は、事前に定義した方法で行われるべきである。文書には、少なくとも、発見された脆弱性、リスクアセスメント、また、考えられる対応措置の説明と優先順位づけを盛り込む必要がある。リスク分析を実施するために必要な情報は、インシデントや障害に関するデータ（ログ及び公知の情報源から得た資料）、セキュリティ監査の実施結果（セキュリティテストと管理査定）、及びチェックリストなどである。

リスクと問題の例

ある組織では、リスク分析の見直しが高々年に 1 回しか実施されず、実稼働システムに最近実施された大幅なシステム変更がリスク分析に反映されていなかった。このため、現在はミッションクリティカルなものとなった制御システムの権限要件が非常に低いままとなっていた。このような状況では、管理担当の人員がシステムにログインし、施設内の機密区画に変更を加えることや、システムベンダがサービス用アカウントでログインし、自社納入システム以外にアクセスしたり変更を加えたりすることができてしまう。

JPCERT CC®

10 PCS 及び関連ネットワークに対し、技術的なセキュリティ監査を定期的に実施する

DOE 21 Steps（No. 9、11）

実際にセキュリティ監査と技術的チェックを実施すると、システムとインストール済み機能のセキュリティについて、一層現実に近い状況を把握できる。

セキュリティテストを経営管理用 IT システムに対して行う場合と、PCS で使われる IT 装置に対して行う場合とでは、非常に重要な相違点がいくつかある。制御システムで使われる大部分の装置（たとえば、PLC、RTU などのフィールド装置）は、セキュリティに関しては貧弱な機能しか備えていない。ささいなプログラミングエラーが原因で装置の動作が中断したり、攻撃を受けたりすることはしばしばある。単純なセキュリティテストがテスト対象ユニットのクラッシュ、再起動、誤動作などを引き起こすことも、残念ながら珍しくない。また、実稼働中の装置が現存する唯一の個体である場合、セキュリティテストに使えるテスト環境や開発環境を用意できないことがある。

PCS のセキュリティテストを実施するにあたっては、テストによって異常が発生した場合の対応方法のリハーサルなど含め、前もって慎重な計画を立てなくてはならない。テスト計画は組織のマネジメント層の承認を得なくてはならない。基本原則として、経営管理用 IT システムの侵入テストに使うような自動ツールではなく、単純かつ基礎的な手法と聞き取り調査によるテスト方法を採用すべきである。PCS のテストについて十分な知識を持っている IT コンサルタントは非常に少ない。多くの PCS は目的に非常に強く特化されたものとなっており、IP ネットワーク以外の技術をより深く理解していることが要求される。この理由により、セキュリティテストを実施する際はそのことをシステムベンダに前もって連絡しておくことも望ましい。

PCS の調査において、ホストコンピュータ、ノード、ネットワークを確認するために、ping スイープなどの従来手法を用いるとシステム運用の妨げになる可能性がある。とはいえ、制御システムのインベントリ情報を得ることはテストプロセスにおける非常に重要な手順の 1 つである。そこで、自動ツールを使うのではなく、文書を慎重に調べたり、プロセスの現場に出向いて接続やコンピュータの物理的状況を確認したりすることがしばしば必要となる。サービスの現状や各種サービスの脆弱性に関するインベントリ情報を確認する際、運用中の実稼働システムに対して能動的なスキャン（たとえば、Nmap、Nessus といったツールによるポートスキャンや脆弱性スキャン）を実行することは避け、受動的手法や、ルータの設定を手動で確認するなどの方法をとるべきである。別個のテスト用システムや運用に入っていない制御システムに対しては能動的なテストを実施してよい。

リスクと問題の例

ある PLC に対し、実稼働環境内でテストが実施された。この装置の運用がテストによって中断し、やがて、重要な制御コマンドを取りこぼしたり、動作しなくなったりした。

JPCERT CC®

11 PCS の物理的なセキュリティ水準を継続的に評価する

■ **NERC CIP**（006-1） ■ **NIST 800-82**（6.2.2 章） ■ **DOE 21 Steps**（No. 10）
■ **PL**（9 章、11 章）

PCS（特にセンター施設）には、強力な物理的セキュリティが適用されてきた経緯があり、重要施設の物理的な保護方法については、多くの業界において要件が確立されている。

反面、地理的に分散（非集中化）していることが多く、そのため、遠隔地の小規模な施設については十分な物理的セキュリティを確保することが難しい。制御システムに対する攻撃は、フィールドに設置された装置から実行される可能性がある。PLC や RTU などのローカルユニットには非常に高度な機能を持つものがあり、たとえば、最近の RTU などは Web サーバ機能と Ethernet ポート（または Bluetooth）を備えている。このため、物理的に十分なセキュリティを確保することは重要である。ケーブルは、許可のない者による物理的なアクセスとネットワークへの接続を防止できる形で配線しなくてはならない。

システムコンポーネントに対する物理的アクセスを許すと、PCS への電子的アクセスは格段に容易になってしまう。したがって、電子的・物理的な防御境界線のチェックが必要である。

物理的セキュリティを確保する方法はいくつかあるが（多層防御の原則も適用可能）、次のような要素を含めるべきである。

- 機密性を要する建物の保護（物理的セキュリティファイアウォール、無断立入りの防止、侵入警報装置、監視カメラ、防火設備など）
- 権限管理（許可を得ない者が機密情報や運用上の重要区画にアクセスすることの禁止）
- 人員及び資産の追跡管理（人員や装置があるべき場所から出ないよう確認。たとえば、PLC プログラミング用のノートブック PC は、監督の行き届かない状態で放置してはならない）
- 環境的なチェック（換気、電力供給など）

注意すべきは、監視は、セキュリティの許可を得た人員に対しても継続的に行われなくてはならないことである。また、そのような人員が管理施設に入る場合にも入場管理が適用されなくてはならない。

リスクと問題の例

ある社員が、自分用のノートブック PC を自宅に持ち帰った。社員の子供がその PC を使ってオンラインゲームで遊んだため、PC は悪意のあるコードに感染してしまった。社員が出勤して PC を PCS ネットワークに接続したため、悪意のあるコードが実行され、ファイアウォールの内側で攻撃者の活動が始まった。

12 セキュアでかつ適切なものだけしか PCS に接続されていないことを確認する

■ **CPNI GPG**（GPG 2、GPG ファイアウォール展開） ■ **DOE 21 Steps**（No. 1、2、3、7）
■ **OLF 104**（No. 10、12） ■ **PL**（10 章、11 章）

従来の PCS は物理的に隔離されて外界との通信経路はまったくないか、ごくわずかな経路だけで接続されていた。ところが近年では、効率化指標や統合ニーズに対応するために、経営管理用 IT システムと PCS とがしだいに密接に接続されるようになっている。セキュリティを確保するには、あらゆる種類の接続を洗い出し、各組織のセキュリティ要件や各種の制御システムに適用される運用要件に応じたセキュリティメカニズムを装備する必要がある。

制御システムに対する接続の形態としては、ダイヤルアップ、ISDN、一般の電話回線または無線網、インターネットベースの接続などがある。その用途は、たとえば次のようなものである。

- ベンダ担当者による保守サービス
- PCS 装置に手早くアクセスする必要がある緊急対応デスク担当者のための接続機能
- 施設をリモート運用するための接続
- 施設内にあるセンサのリモート読取り用の接続
- 施設内の補助的な機能や周辺システムにアクセスするための接続（監視カメラ、警報装置、カード及び入退室管理、火災報知器など）

組織では、適切な通信経路だけが PCS に接続されていることを定期的かつ実地に確認し、確認された接続について可能な限り強力なセキュリティを確保すべきである。不要な接続を排除することは、セキュリティを強化するもっとも重要な措置の 1 つである。

ベンダ向けのリモートアクセスと緊急対応デスク担当者用のアクセスについては、特別な注意が必要である。十分なセキュリティを実現するためにはさまざまな手法の組合せが必要になると考えられる。たとえば、コールバック、接続回数制限、認証の強化、また、接続に使用する通信方法やコンピュータの制限などを組み合わせるべきである。

リスクと問題の例

あるプロセス環境の PCS と経営管理用コンピュータシステム（イントラネット）との間に、未知の接続が存在した。マーケティング部門のコンピュータが、インターネット経由でワームに感染した。そのワームの感染が拡大し、やがて、プロセス環境でも大規模に運用を混乱させた。

13 システムベンダの協力を得て、PCS を堅牢化及びアップグレードする

■ **CPNI GPG**（GPG 5） ■ **DOE 21 Steps**（No. 4、6） ■ **OLF 104**（No. 6、10、12、13）
■ **PL**（2 章）

コンピュータソリューション、システムコンポーネント、アプリケーションを堅牢化するには、未使用・不要・不明のソフトウェアコンポーネントや設定を削除し、セキュリティアップグレード（パッチ）をインストールする必要がある。堅牢化すると、攻撃を受ける可能性がある箇所が減り、リスクにさらされる可能性を低減できる。経営管理用 IT システムでは、堅牢化がセキュリティを強化する標準的な手法の 1 つになっている。その目的は、種々のシステム構成や設定のうち、もっともセキュアな選択肢を常に採用することにある。堅牢化の作業は、定められた変更管理手順に従って実施することが重要である。システムの攻撃可能な部分を減らすには、たとえば次のような方法がある。

- 出荷時の標準設定を変更する（デフォルトパスワードなど）
- アプリケーションや、ネットワーク機能、OS などの選択と設定において、よりセキュアなものを採用する
- アプリケーションや、ネットワーク、OS の機能のうち、使用していないものを止める
- システムにアクセスする必要がなくなったユーザのアカウントを停止、またはユーザのログインや権限を制限する
- アップグレード（パッチ）を適用して既知のセキュリティ問題を修正する

システム装置や、アプリケーション、OS の堅牢化と人手によりセキュリティホールをふさぐ作業は、PCS のセキュリティ文書で述べられていることもあるが、通常、実施するにはベンダの強力な支援を受けることが不可欠である。システムベンダやアプリケーションベンダの協力を得ずに装置またはソフトウェアの設定変更（パッチ適用を含む）を実施すると、運用の中断や制御システムの不安定化を招き、契約上の問題をも生じかねない。

リスクと問題の例

あるシステムベンダは、セキュアでないネットワークサービスやシステムコンポーネントを使って、PCS 機能を構築した。その結果、セキュアでない機能を無効化するわけにもいかず、望ましいレベルまでシステムを堅牢化することができなかった。

制御システムに精通していない人員にシステムの堅牢化を実施させると、必要不可欠な、しかし滅多に使われないようなコンポーネントが不用意に削除されてしまい、システムが不安定になる可能性もある。

システムを堅牢化しても、その堅牢化が不完全だった場合には、脆弱な部分は依然として残っているのに、誤った安心感を与えてしまうことがある。

14 自組織の PCS で発生したインシデントの経過を追跡管理するとともに、組織外で起きたセキュリティ問題について情報を収集し分析する

■ **NERC CIP**（008-1、009-1） ■ **NIST 800-82**（6.2.3 章） ■ **CPNI GPG**（GPG 3）
■ **DOE 21 Steps**（No. 19） ■ **OLF 104**（No. 16）

どのような改善活動においても重要なのは、発生が組織内か組織外かを問わず、過去のインシデントやセキュリティに関する経験を、組織として報告書や文書に記録し、教訓を得ることである。

経験やインシデントを記録した文書は、リスクアセスメントの見直し（リスク分析）作業において基礎資料となる。また、是正措置やリソース配分の優先順位の見直しにつながりうるものでなくてはならない。

インシデントを発見するには、組織のセキュリティに関する日常業務を継続的に監視し、状況を常に把握しておく必要がある。監視と追跡管理により、脅威への対処と、新たなセキュリティ欠陥（組織内で発生するものと、外部からもたらされるものがある）の発見をより的確に行うことができる。また、組織に影響を及ぼしうる外部のインシデントや事象にも注意を払う必要がある。物理的なインシデントも、IT のインシデントに関係する可能性がある。たとえば、ノートブック PC が盗難にあった場合、その行為はサイバー攻撃を仕掛けるための情報収集の一環かも知れない。

組織外で見つかったインシデントやセキュリティ問題を常に把握しておくと、新たな脅威や PCS の脆弱性に対応する事前の備えを維持することが容易になる。

経験や情報分析に関する問題として、公開されている PCS の事故事例情報がほとんどないことがある。今のところ、システムや施設の所有者が事故事例情報を容易に入手できるようなフォーラムや情報交換チャネルはほとんどない。

情報を収集する観点からいえば、PCS を利用する組織がグループを結成して、インシデントやリスクの問題について議論し、そうした問題が PCS のセキュリティに及ぼす影響を分析するための場とすべきである。このグループは、定期的に会合を開き、プロセス制御に携わる者と IT に携わる者の双方に参加してもらう必要がある。

リスクと問題の例

インシデントの報告が行われないと、定められたセキュリティに関する日常業務に欠陥（ファイアウォールの不適切な設定、ユニットの故障など）があることを見つけるのは難しい。

ささいなインシデントも、対処を怠ると、プロセス運用に実害や重大な機能停止をもたらす可能性がある。

15 ユーザグループ、標準化機関、その他のネットワークとの間に、PCS のセキュリティ強化を目的とした連携協力関係を構築する

PCS のセキュリティをどのように確立すべきかについて、標準や推奨事項を策定するための国際的な作業がいくつも進められている。ヨーロッパ、北アメリカ、アジア各地にある多くの政府機関が、この問題領域を重視している。現段階でセキュリティの検討作業に率先して取り組めば、今後 PCS に適用されることになるセキュリティ要件の内容に反映させることができる。

PCS ユーザが、さまざまな国の組織や国際組織、利益団体と共同で作業を進めれば、ベンダ、システムインテグレータ、アプリケーションデベロッパに対し、結束力を背景として、より強力で明確な要求を示すことができる。

PCS、アプリケーション、その他のセキュリティ関連機器を扱うベンダにとっては、現段階から率先して取り組めば、競合上の優位性を獲得できる可能性がある。すでに確立したセキュリティ要件が存在する産業部門もあり、たとえば、アメリカの電力事業者は NERC CIP 標準に準拠することを求められている。これは将来的には、ハードウェア及びソフトウェアを納入する場合の要件となろう。

ユーザグループ、標準化機関、その他のネットワークを通じて協業関係を築くことは、多くの中小規模ユーザやベンダにとって経済的な現実性のある選択肢であると考えられる。

リスクと問題の例

標準化活動やセキュリティ施策が、ベンダまたはユーザの立場の参加なしに進行すると、バランスを欠いたセキュリティ要件や技術的に的外れなセキュリティ要件が策定される可能性がある。

JPCERT CC®

パート C

参考文献リスト
及びコメント

JPCERT CC®

NERC(北米信頼性委員会) CIP-002-1～CIP-009-1　サイバー・セキュリティ標準

文書種別： 標準
発行者： NERC（北米信頼性委員会；North American Reliability Council、アメリカ）
版： 正式版（2006 年 6 月 1 日現在）
分量： 53 ページ（合計）

http://www.nerc.com/ (Standards → Reliability Standards →CIP)

NERC（北米信頼性委員会）CIP（重要インフラ保護基準）（CIP 002-1～009-1）の標準は、電力以外の事業分野にも適用できるよう汎用的な構成になっている（以下は執筆者らによる要約）。

NERC CIP 002-1 は、リスクベースのアプローチによって、重要資産を特定することを、PCS の利用組織に要求している。この分析に基づいて、重要サイバー資産が特定される。

NERC CIP 003-1 は、なんらかの経営管理用セキュリティプログラム（最小限のセキュリティ管理）を確立して重要サイバー資産を保護するために、セキュリティに関する、なんらかの管理面からの行動計画（最小限のセキュリティ管理施策）を確立することを、PCS の利用組織に要求している。

NERC CIP 004-1 は、電子的にまたは監視なしに物理的に、重要サイバー資産へのアクセスを許可された人員（さまざまな種類の部外者を含む）に対して、必要なトレーニングを施し、セキュリティ意識を身につけさせることを、PCS の利用組織に要求している。

NERC CIP 005-1 は、重要サイバー資産を取り囲む、いわゆる電子的なセキュリティ防衛線を特定して保護し、さらに、その防衛線上のすべてのアクセスポイントを特定し保護するよう、PCS の利用組織に要求している。

NERC CIP 006-1 は、重要サイバー資産を物理的に保護するための行動計画を策定・実施するよう、PCS の利用組織に要求するものである。

NERC CIP 007-1 は、重要サイバー資産であると自らが定めたシステムのセキュリティを確保するための手法、プロセス、手続きを定義するよう、PCS の利用組織に要求している。この規定は、いわゆる電子的なセキュリティ防衛線の内側に配置された、最重要でないサイバー資産にも適用される。

NERC CIP 008-1 は、重要サイバー資産に関連するセキュリティインシデントを特定し、分類し、これに対処し、報告を行うことが確実になされるよう、PCS の利用組織に要求している。

NERC CIP 009-1 は、重要サイバー資産に関する復旧計画を策定するよう、また、対応準備計画及び緊急時対応計画に対応して確立された業務慣行や技法に沿った復旧計画とするよう、PCS の利用組織に要求している。

JPCERT CC®

NIST SP 800-82 — 工業用制御システム(ICS)のセキュリティのためのガイド

文書種別： 推奨事項
発行者： NIST（国立標準技術機関；National Institute for Standards and Technology、アメリカ）
版： 公開第 2 草案（2007 年 9 月）
分量： 157 ページ（付録含む）
http://csrc.ncsl.nist.gov/publications/PubsDrafts.html#SP-800-82

NIST SP 800-82 は、PCS が使われる各種の分野に適用できるよう汎用的な構成になっている。同文書の大まかな構成は次の 6 セクションに分かれている。

第 1 章：推奨事項の目的、適用範囲、対象グループを示す。

第 2 章：PCS の概要と、PCS の重要性について説明する。

第 3 章：PCS と経営管理用 IT システムとの違いについて述べ、各種の脅威、脆弱性、過去のインシデントについて説明する。

第 4 章:第 3 章で示した脆弱性のリスクを低減するためのセキュリティ行動計画について概要を説明する。

第 5 章：PCS の伝統的なネットワークアーキテクチャにセキュリティを統合する方法についての推奨事項を示す。特に、ネットワークの分割に関するプラクティスを強調している。

第 6 章: NIST SP 800-53（Recommended Security Controls for Federal Information Systems）に示されているさまざまな形の管理策（マネジメント、運用、技術的制御）を PCS に適用する方法についての推奨事項を示す。

また、同文書には 6 つの付録（A～F）が含まれている。付録の内容は、参考文献、略語一覧、用語集と、PCS のセキュリティ強化を目的としてアメリカで行われているさまざまな活動についての説明などである。

JPCERT CC®

プロセス制御と SCADA セキュリティ・ガイド

文書種別： 推奨事項
発行者： CPNI（Centre for the Protection of National Infrastructure、イギリス）
版： 正式版（日付は文書により異なる）
分量： 14～42 ページ（文書により異なる）
http://www.cpni.gov.uk/ProtectingYourAssets/scada.aspx

このシリーズの文書は、PCS が使われるすべての分野に適用できるよう汎用的な構成になっている。現在、要約ガイドと 8 つの各論の文書がある。

- PCS と SCADA セキュリティのためのグッドプラクティスガイド
- PCS と SCADA セキュリティのためのグッドプラクティスガイド ガイド-1： 事業リスクの理解
- PCS と SCADA セキュリティのためのグッドプラクティスガイド ガイド-2： セキュリティ・アーキテクチャの実現
- PCS と SCADA セキュリティのためのグッドプラクティスガイド ガイド-3： 対応体制の確立
- PCS と SCADA セキュリティのためのグッドプラクティスガイド ガイド-4： 気づきとスキルの向上
- PCS と SCADA セキュリティのためのグッドプラクティスガイド ガイド-5： 第三者リスクの管理
- PCS と SCADA セキュリティのためのグッドプラクティスガイド ガイド-6： プロジェクトにセキュリティを埋め込む
- PCS と SCADA セキュリティのためのグッドプラクティスガイド ガイド-7： 現状のガバナンスを確立
- SCADA と PCS 網のためのファイアウォール展開に関するガイド

JPCERT CC®

SCADA 網のサイバー・セキュリティ強化のための 21 カ条

文書種別： 推奨事項
発行者： DOE（Department of Energy；エネルギー省、アメリカ）
版： 正式版（2002 年 9 月）
分量： 10 ページ
http://www.oe.netl.doe.gov/docs/prepare/21stepsbooklet.pdf

この文書は、次に示す推奨事項をきわめて簡潔に説明している。

1. SCADA ネットワークに対する接続をすべて洗い出せ。
2. SCADA ネットワークへの不必要な接続を切断せよ。
3. 残った SCADA ネットワークへの接続すべてについて、セキュリティを評価及び強化せよ。
4. 不要なサービスを削除または無効化することで SCADA ネットワークを堅牢化せよ。
5. システムの保護を独自のプロトコルに頼らずに、システムを保護せよ。
6. デバイスベンダやシステムベンダが提供しているセキュリティ機能を実装する。
7. SCADA ネットワークへのバックドアになりうる、すべての媒体を厳格に管理せよ。
8. 種々の IDS を導入し、24 時間体制のインシデント監視を確立せよ。
9. SCADA の装置とネットワーク及び接続されているその他のネットワークに対して技術的監査を実施し、セキュリティ上懸念される点を洗い出せ。
10. 物理的セキュリティに関する調査を実施せよ。さらに、SCADA ネットワークに接続されているすべてのリモートサイトを査定し、セキュリティを評価せよ。
11. SCADA の「敵役」チームを組織して、考えうる攻撃シナリオを洗い出し評価せよ。
12. 組織管理者、システム管理者、ユーザのサイバー・セキュリティに関する役割、責任範囲、権限を明確に定義せよ。
13. ネットワークアーキテクチャを文書化し、特別な保護レベル強化が必要な、基幹的な機能を担うシステムや機密情報を格納したシステムを洗い出せ。
14. 厳格かつ継続的なリスク管理手順を確立せよ。
15. 多層防御の原則に基づくネットワーク保護戦略を策定せよ。
16. サイバー・セキュリティの要件を明確に洗い出せ。
17. 実効的な構成管理手順を策定する。
18. 定常的な自己評価を実施せよ。
19. システムバックアップ計画及び災害復旧計画を策定せよ。
20. 経営陣がサイバー・セキュリティのできばえに関する期待事項を設定し、各自に説明責任を負わせよ。
21. SCADA システムの設計、運用、セキュリティ管理策に関する機密情報を組織内の人員が不注意で外部に漏らす可能性を最小化するために、ポリシーを策定し、トレーニングを実施せよ。

JPCERT CC®

PCS と安全システムと支援 ICT システムのための情報セキュリティ基本要件

文書種別： 推奨事項（ガイドライン No. 104）
発行者： OLF (ノルウェー石油事業協会)
版： リビジョン No.：01 作成日：2007 年 1 月 4 日
分量： 6 ページ（ノルウェー語版）、32 ページ（英語版）

http://www.olf.no/guidelines/104-information-security-baseline-requirements-article2972-301.html

英語版では、次に示す推奨事項について説明している。

1. PCS と、安全システムと、支援 ICT システム環境に関する情報セキュリティポリシーを文書化せよ。
2. PCS と、安全システムと、支援 ICT システム及びネットワークに関するリスクアセスメントを実施せよ。
3. PCS と、安全システムと、補助 ICT システムに対する、システム責任者及びデータ責任者を指名せよ。
4. インフラストラクチャに VPN 提供機能を持たせ、すべての通信パスを管理下に置け。
5. PCS と、安全システムと、支援 ICT システムの利用者に、情報セキュリティの要件と ICT システムの適正利用に関する教育を施せ。
6. PCS と、安全システムと、補助 ICT システムを所定の目的以外に使用するな。
7. PCS と、安全システムと、支援 ICT システム用の災害復旧計画を文書化し、テストせよ。
8. ICT コンポーネントの情報セキュリティ要件の検討を、エンジニアリング、調達、システム導入の手順に組み込め。
9. 重要な PCS と、安全システムと、支援 ICT システムについて、サービスレベル及びサポートレベルを定義し、文書化せよ。
10. PCS と、安全システムと、支援 ICT システム及びネットワークに対するすべての接続と、これらに対するすべての変更について、変更管理及び作業承認の手続きを遵守させよ。
11. すべてのシステムコンポーネントと、ほかのシステムに対するインタフェースを含む、最新のネットワークトポロジ図を常に参照できるよう整備せよ。
12. PCS と、安全システムと、支援 ICT システムに接続する ICT システムを常に最新の状態に更新せよ。
13. PCS と、安全システムと、支援 ICT システムに、悪意のあるソフトウェアに対する、適切、最新、かつ能動的な防護対策を施せ。
14. アクセス要求は、明確に承認されたものを除きすべて拒否せよ。
15. 必要な運用手順及び保守手順を文書化し、最新に保て。
16. セキュリティ事象及びインシデントの報告手続きを文書化し、組織内に徹底せよ。

JPCERT CC®

PCS の調達におけるサイバー・セキュリティの文言

文書種別： 推奨事項
発行者： Idaho National Laboratory(アイダホ国立研究所)及び Department of Homeland Security（国土安全保障省）（アメリカ）
版： 2008 年 8 月
分量： 111 ページ（合計）
http://www.us-cert.gov/control_systems/pdf/SCADA_Procurement_DHS_Final_to_Issue_08-19-08.pdf

PCS の調達におけるセキュリティ要件の確立を目的とした文書である。主要な分野ごとに要求仕様の例（テスト基準を含む）を示している。内容は随時拡充されているが、現時点では次に示すセクションがある。

システムの堅牢化：不要なプログラムの削除、ハードウェアの構成、OS の更新などに関する要件を扱う。

セキュリティ境界の防御：ファイアウォール、ネットワーク IDS などに関する要求事項を扱う。

アカウントとパスワード：ゲストアカウント、パスワード及び認証、ログの記録、役割ベースのアクセス制御などに関する要求事項を扱う。

コーディングの方法：ベンダによって開発されるコードの文書化に関する要求事項を扱う。

欠陥改修：ベンダから提供されるメッセージや文書と、問題の報告に関する要求事項を扱う。

マルウェアの検知と防御：悪意のあるコードの検知及びそれに対する保護に関する要求事項を扱う。

ホスト名の解決：ネットワークにおけるアドレス割当てと DNS サーバの設定に関する要求事項を扱う。

ローカルユニット（末端機器）：IED、PLC、RTU などの装置におけるセキュリティを扱う。

リモートアクセス：制御システムに対する各種の接続に関する要求事項を扱う。

物理的セキュリティ：物理的セキュリティに関する要求事項（デジタルコンポーネントの可用性など）を扱う。

ネットワークの分割：ネットワークの分割単位及びアーキテクチャに関する要求事項を扱う。

推奨する情報リソース

PCS のセキュリティに関しては、いくつもの国際的な取り組みが現在進行中である。最新の動向を知るには、定評あるいくつかの Web サイトに掲載される情報を定期的にチェックするとよい。以下の各サイトはよい出発点になる。

CPNI（Centre for the Protection of National Infrastructure、イギリス）

`http://www.cpni.gov.uk/ProtectingYourAssets/scada.aspx`

US-CERT、Control Systems Security Program（Department of Homeland Security：国土安全保障省、アメリカ）

`http://www.us-cert.gov/control_systems/`

PCSF（Process Control Systems Forum、アメリカ）

［邦訳注］2005 年に組織され活発な活動を展開した後、2008 年に解散した。

SCADA Blog（Digital Bond、アメリカ）

`http://www.digitalbond.com/`

JPCERT CC®

＜お願い＞

引用の際は、引用元名、資料名、URL を明示してください。

なお、引用の際は引用先文書、時期、内容等の情報を JPCERT/CC 広報(office@jpcert.or.jp)までメールにてお知らせください。今後、より良い情報を提供するため、どこで、どのような方に、どのような場面で、お使いいただけているのかを把握し検討するため、ご協力をお願いいたします。

[原典情報]

Swedish Emergency Management Agency

P.O. Box 599

SE-101 31 Stockholm

Tel +46 8-593 710 00

Fax +46 8-593 710 01

kbm@kbm-sema.se

ISBN 978-91-85797-23-3