グッド・プラクティス・ガイド
プロセス制御と SCADA セキュリティ

作成：**PA Consulting Group for CPNI**

Centre for Protection of National Infrastructure

邦訳：一般社団法人 **JPCERT** コーディネーションセンター

本ガイドは、プロセス制御、産業オートメーション、DCS、SCADA 等の産業制御システムのセキュリティを確保するためのグッド・プラクティスを普及することを目的としている。このようなシステムは重要国家インフラストラクチャにおいて広く使われている。本ガイドはそのようなシステムを電子的攻撃から守るための有用なアドバイスを示すものであり、PA Consulting Group for CPNI が作成した。

Disclaimers

Reference to any specific commercial product, process or service by trade name, trademark manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation or favouring by CPNI or PA Consulting Group. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes.

CPNI and PA Consulting Group shall also accept no responsibility for any errors or omissions contained within this document. In particular, CPNI and PA Consulting Group shall not be liable for any loss or damage whatsoever, arising from the usage of information contained in this document.

本翻訳文書は、一般社団法人 JPCERT コーディネーションセンターが、原書の著作権を保有する英国 CPNI：Centre for Protection of National Infrastructure の許諾を得て翻訳したものです。

日本語版の内容について、原書に沿ってできるだけ忠実に翻訳するよう努めていますが、完全性、正確性を保証するものではありませんので、必要に応じて CPNI のホームページより原書 " GOOD PRACTICE GUIDE　PROCESS CONTROL AND SCADA SECURITY " をご参照ください。

また、翻訳監修主体は本文書に記載されている情報により生じる損失または損害に対し、いかなる人物あるいは団体にも責任を負うものではありません。

なお、当文書に関わる最新情報は以下の CPNI のホームページをご参照ください。

http://www.cpni.gov.uk/

目次

1.1 目的と目標

本書の目的は、プロセス制御と SCADA セキュリティに対するグッド・プラクティスの原則を示すことである。具体的には

- プロセス制御と SCADA システム・セキュリティの必要性を概説する。
- プロセス制御や SCADA システム・セキュリティと IT セキュリティの間の違いを明らかにする。
- 本書作成時に使用した主要原則を述べる。
- プロセス制御システム・セキュリティに対応するための 7 つのステージを示し、各ステージにおけるグッド・プラクティスの原則を示す。

1.2 用語

1.2.1 プロセス制御と SCADA システム

本フレームワーク全体で、「プロセス制御システム」および「プロセス制御と SCADA」という用語は、すべての産業制御、プロセス制御、DCS、SCADA、産業オートメーションその他関連する安全システムを含む包括的な用語として使用する。

1.2.2 グッド・プラクティス

本書ではグッド・プラクティスを以下のように定義する。

> *調査と評価により効果的であると示された、戦略、活動、方法等の最良のプラクティス。*

本書に要約されたグッド・プラクティスは、単に指針を示したものである。環境やプロセス制御システムによっては、これらの原則のすべてを実施することはできないだろう。例えば

- **グッド・プラクティス・ステートメント.** ワークステーションやサーバにアンチウイルス・ソフトウエアを搭載してプロセス制御システムを保護する。

  困難な場合. プロセス制御システムのワークステーションやサーバにアンチウイルス・ソフトウエアを搭載できない場合もある。

- **グッド・プラクティス・ステートメント.** 目的に合致しないソフトウエアを搭載する前にプロセス制御システム・ベンダからベンダ認定と設定手引きを入手する。

  困難な場合. アンチウイルス・ソフトウエアを認定しないベンダもあるし、その様なソフトウエアをサポートしていないプロセス制御システムもある。

上記のような場合には、他の防護手段を調査すべきである。

2.1 概要

プロセス制御と SCADA システムは、標準 IT 技術を利用しており、それにますます依存するようになった。Microsoft Windows、TCP/IP、ウェブ・ブラウザ、さらに最近ではワイヤレス技術等の標準 IT 技術は、従来の非標準技術に置き換わり、注文設計のプロセス制御システムを市販ソフトウエアで置き換えることを可能にしている。

このような発展は事業上の利点があるものの、2 つの重要な懸念が生じている。

1 つ目の懸念は、プロセス制御システムが伝統的に、機能、安全性、信頼性を達成するために物理的セキュリティを主に考慮した設計された、閉じたシステムであったことである。これらのシステムは標準 IT 技術と接続されることが多くなり、対策が取られていない新しい脅威（例えば, ワーム, ウイルス、ハッカー） に曝されるようになった。プロセス制御ネットワークが数を増し、拡大し、接続が増えるに従い、電子的脅威からのリスクも高まっている。

プロセス制御システムをサポートする手順も、この問題を更に深刻なものにしている。それは、ベンダがダイヤルアップ接続やインターネットを介して遠隔でこれらシステムを日常的にサポートするようになったからである。モデムの使用に関してセキュリティの高い手順があることはまれであるので、このようなベンダからの接続は、ウイルスを受け取ったり、ハッカーからの直接攻撃に利用されたりすることが知られている。

プロセス制御システムは最近、より広範囲なサプライ・チェーンに接続されるようになってきた。例えば、タンク・レベル・センサのデータを基に自動的に、部材を供給会社に再発注することがある。このような接続が増えると、脆弱なプロセス制御システムは供給会社のシステムからの脅威にさらされ、サプライ・チェーン中の他のシステムのリスクも高まる。

2 つ目の懸念は、各社固有のプロセス制御システムに代わって市販ソフトウエアや汎用ハードウェアが使われるようになったことである。そのようなソフトウエアやハードウェアは個別のプロセス制御環境の独自性、複雑性、リアルタイム性、安全性の要件に合わないことがよくある。これらの技術と通常一緒に使用される標準的 IT セキュリティ保護対策の多くは、プロセス制御環境で採用されていない。その結果、制御システムを保護し、その環境のセキュリティを高めるための十分なセキュリティ対策が利用できないことがある。

このような脆弱性が悪用されれば、重大な結果を招く可能性がある。プロセス制御システムに対する電子的攻撃の影響として、例えば、DoS 攻撃、プロセスの不正な制御、完全性の喪失、機密性の喪失、評判の失墜、人の健康・安全や環境への影響が考えられる。

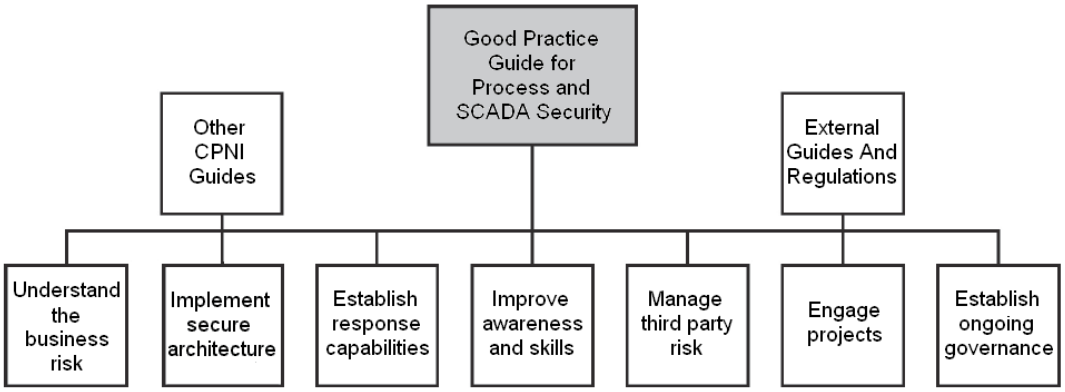
2.2 プロセス制御セキュリティ・フレームワーク

IT システムのセキュリティを高めるために広く使われている標準やソリューションは、プロセス制御環境には不適切なことがよくある。今ではプロセス制御システムが標準 IT 技術に基づいていることが多いが、その運用環境は、企業の IT 環境と大きく異なる。プロセス制御システムの保護に使用できる標準セキュリティ・ツールや技術もあるが、その適用には注意が必要であり、改造が必要なこともある。他のセキュリティ対策によっては、制御環境にまったくあわないものや、対応できないものもある。

例えば、旧来のシステムのプロセッサの能力不足、古いオペレーティング・システム、ベンダ認定が得られない等の理由でアンチウイルス・ソフトウエアをプロセス制御システムにインストールできない場合もある。また、プロセス制御システムのセキュリティ試験は慎重に行う必要がある。セキュリティ・スキャンが多くの制御機器の動作に重大な影響を与えることがありうる。専用のテスト環境があることはまれであるし、定期的テスト、パッチ、保守のためにシステムをオフラインにできる機会もほとんどない。

本書はプロセス制御システムを電子的攻撃から保護するためのフレームワークを提供するために作成した。このフレームワークは、プロセス制御と IT セキュリティにおける産業界のグッド・プラクティスに基づいており、以下の 7 つの重要テーマに的を絞っている。

- 事業リスクの理解
- セキュア・アーキテクチャの実装
- 対応能力の確立
- 意識とスキルの改善
- サード・パーティ・リスクの管理
- プロジェクトへの参画
- 継続した統制の確立



Good Practice Guide for Process and SCADA Security	プロセス制御と SCADA セキュリティに関するグッド・プラクティス
Other CPNI Guides	その他の CPNI ガイド
External Guides And Regulations	外部のガイドおよび規制

Understand the business risk	事業リスクの理解
Implement secure architecture	セキュア・アーキテクチャの実装
Establish response capabilities	対応能力の確立
Improve awareness and skills	意識とスキルの改善
Manage third party risk	サード・パーティ・リスクの管理
Engage projects	プロジェクトへの参画
Establish ongoing governance	継続した統制の確立

図 1 - グッド・プラクティス・ガイド・フレームワーク内における本ガイドの位置づけ

上記の要素はそれぞれ、個別の文書内で詳細に解説されている。本文書は、グッド・プラクティス・ガイド・フレームワークにおける、すべてのガイドの概要を示すものである。グッド・プラクティス・ガイド・フレームワークのガイドはすべて、CPNIのウェブサイト（www.cpni.gov.uk/protectingyourassets/scada.aspx）から入手できる。

2.2.1 指針となる原則

本フレームワークを構築する際に、以下の三つの指針となる原則を用いた。

i. *保護し、検出し、対応する*

いかなるシステムに対するものであるにせよ、セキュリティ・フレームワークの構築は、単に保護対策を講じることではない。攻撃らしいものを検出し、その影響を最小限にするために適切に対応できることが重要である。

保護: プロセス制御システムに対する電子的攻撃を防ぎ、攻撃意欲を削ぐ具体的保護対策を講じる。

検出: 本当または疑わしい電子的攻撃を迅速に見つける仕組みを確立する。

対応: プロセス制御システムに対するセキュリティインシデントと確定したものに対して適切に対応措置をとる。

ii. *多層防御*

システムの保護対策がひとつの場合、それに弱点があることが見つかり、悪用されれば、実質的に保護がないも同然になる。セキュリティ対策にはいつでも脆弱性や弱点が見つかる可能性があり、ひとつの対策では万全ではない。このようなひとつの欠陥で脆弱になるリスクを減らすには、複数の保護対策を直列に講じる。

プロセス制御システムを電子的攻撃（例、ハッカー、ワーム、ウイルス）から守るには、企業の IT ネットワークを保護するように作られたひとつのファイアウォールだけに頼るのは不十分であろう。より効果的なセキュリティ・モデルは、企業用ファイアウォールを基本として、それに専用のプロセス制御ファイアウォールを追加し、アンチウイルス・ソフトウエアや侵入検出等の他の防護対策を講じることである。このような多層のセキュリティは多層防御と呼ばれる。

iii.　　技術面、手順面、管理面の保護対策

セキュリティ対策を実装する際、ほとんどの努力を技術的要因に注ぐ傾向がある。技術は重要ではあるが、それだけでは、堅牢な保護を実現するには不十分である。

例えば、ファイアウォールの実装は、単にインストールし設定すればよいというものではない。手順面や管理面の要件にも注意を払う必要がある。

- 手順面の要件としては、変更制御とファイアウォール監視等がある。
- 管理面の要件としては、ファイアウォール保証、標準、保証と訓練等がある。

3.1 概要

セキュリティ改善プログラムを開始する前に、まずプロセス制御システムが侵害された場合の事業に対するリスクを理解する必要がある。事業リスクは、脅威、影響、脆弱性の関数である。事業リスクをよく理解して始めて、情報に基づいて、セキュリティの適切なレベルは何か、改善すべき作業実施方法は何か等を判断できるようになる。脅威は刻々と変わるので、それに合わせて事業リスクを継続的に再評価するプロセスを確立する必要がある。

3.2 目標

要求されるセキュリティ保護レベルを知り、その保護を実施するために、プロセス制御システムに対する脅威からの事業リスクをしっかり理解する。

3.3 グッド・プラクティスの原則

3.3.1 事業リスクの評価

- 以下を理解するため、プロセス制御システムの正式なリスク評価を実施する。

i. システムの理解

- プロセス制御システムの正式な棚卸監査と評価を実施する。このとき、どのようなシステムが存在し、各システムの役割は何で、事業の安全性に重大な影響を与えるか、どこにあるか、指定された所有者は誰か、誰が管理しているか、誰がサポートしているか、システム間でどのような相互作用があるか、を理解し、文書化し、変更管理に登録することが重要である。

ii. 脅威の理解

- プロセス制御システムに起こりうる脅威を特定し、評価する。可能性のある脅威としては、DoS 攻撃、ターゲットを絞った攻撃、偶発的なインシデント、不正な制御、ウイルスやワームやトロイの木馬への感染、がある。

iii. 影響の理解

- 脅威が実際に起こった際のプロセス制御システムへの影響と結果の可能性を特定する。結果の例としては、評判の失墜、コンプライアンスおよびガバナンスに対する違反（人の健康や安全、環境への影響）、事業上の約束を履行できない、財務上の損失、がある。

  注: プロセス制御システムが他の重要なサービスの提供を支える重要な要素の場合、影響は自社の事業に閉じたものではなく、人々の生活を脅かす重大な結果を招く恐れがある。

iv. 脆弱性の理解

- プロセス制御システムの脆弱性を評価する。これには、インフラストラクチャ、オペレーティング・システム、アプリケーション、構成要素となるソフトウエア、ネットワーク接続、リモート・アクセス接続、プロセスと手順等の評価が含まれる。

3.3.2 事業リスクの継続評価

- 事業リスクは、脅威、影響、脆弱性の関数である。パラメータ（例、システム変更）が変われば、事業リスクも変わる。そのため、これらの変更を特定し、事業リスクを再評価し、適切なセキュリティ改善を図るために、継続したリスク管理プロセスが必要である。

詳細なグッド・プラクティス・ガイドは以下のサイトで入手できる。

www.cpni.gov.uk/protectingyourassets/scada.aspx

4. セキュア・アーキテクチャの実装

4.1 概要

組織は、事業リスクの評価に基づいて、プロセス制御システムのセキュリティを高めるため、技術面、手順面、管理面の保護対策を選択し、実施するべきである。

4.2 目標

事業リスクに相応しく、プロセス制御システム運用環境のセキュリティを確保できる、技術面および関係する手順面のセキュリティ対策を実施する。

4.3 グッド・プラクティスの原則

- セキュア・アーキテクチャを形成する、適切なセキュリティ手段を（事業リスクに基づいて）選択する。
- 選択したリスク低減手段を実装する。

適切なセキュリティ対策を採択実装し、セキュア・アーキテクチャを形成する方法に関する詳細なガイドは、『セキュア・アーキテクチャの実装』に示されている。

以下のセクションは、セキュア・アーキテクチャ全体の形成に用いることが可能な、考え得るセキュリティ手段に関する主要なグッド・プラクティス設計原則を示す。

4.3.1 ネットワーク・アーキテクチャ

- プロセス制御システムへのすべての接続を特定する。
- プロセス制御システムへの接続数を減らす。正当な事業上の理由がある接続だけを残す。
- できる限り、プロセス制御システムを他のネットワークから分離し、隔離する。
- 安全上重要なプロセス制御システムには専用のインフラストラクチャを用意する。
- できる限り、安全システム （例、緊急停止システム）とプロセス制御システムまたは他のネットワークの間で TCP/IP 接続を使わない。これが不可能な場合は、リスク分析を行うべきである。

4.3.2 ファイアウォール

- プロセス制御システムと他のシステムの間の接続は、ファイアウォールと非武装セグメント（DMZ）アーキテクチャを用いて保護する。[1]
- ファイアウォールは厳密な設定規則を使用して設置する。
- ファイアウォールの設定は定期的に審査すべきである。
- ファイアウォールの変更は厳密な変更管理の下で管理すべきである。
- 適切なファイアウォール管理と監視規則を実施すべきである。
- ファイアウォールは適切に訓練された管理者が管理すべきである。
- ファイアウォールの管理と監視を 24 時間 365 日実施できる体制を築くべきである。

さらなるガイドについては、ファイアウォールに関する CPNI グッド・プラクティス・ガイドに記載されている。このガイドの場所については、付録 A を参照のこと。

4.3.3 リモート・アクセス

- すべてのリモート・アクセス接続と種類（例、VPN、モデム）の目録を維持する。
- リモート・アクセス接続は事業上必要なものだけにする。
- リモート・アクセス接続に適切な認証手段（例、強い認証）を適用する。
- 不正なリモート・アクセス接続がないよう定期的に監査する。
- リモート・アクセス接続の可／不可の設定に適切な手順と保証を実施する。
- リモート・アクセスは特定マシン、特定ユーザ、そして可能ならば特定時間、に限定する。
- 制御システムへリモート・アクセスするすべてのサード・パーティのセキュリティ審査を実施する。
- リモート・アクセス・コンピュータには適切なセキュリティ対策（例、アンチウイルス、アンチスパムおよびパーソナルファイアウォール）を講じる。

[1] Firewall Deployment for SCADA and Process Control Networks に関する追加情報が CPNI のウェブサイトに掲載されている。

4.3.4 ウイルス対策

- ワークステーションやサーバにアンチウイルス・ソフトウエアを搭載してプロセス制御システムを保護する。アンチウイルス・ソフトウエアを搭載できない場合は、他の保護対策（例、ゲートウェイ・アンチウイルス・スキャン、人手によるメディア・チェック）を実施する。

- その様なソフトウエアを搭載する前にプロセス制御システムのベンダから認定と設定手引きを受け取る。

4.3.5 電子メールとインターネット・アクセス

- プロセス制御システムからの電子メールとインターネット・アクセスをすべて不可にする。

4.3.6 システムの強化

- ネットワーク経由の攻撃を防ぐため、プロセス制御システムを強固にする。不正使用を防ぐため、オペレーティング・システムの、使用されていないサービスやポートを撤去または使用不能にする。

- 開いているポートおよびデバイス（特に PLC や RTU などの埋め込みデバイス）が使用するサービスとプロトコルを理解する。これは、テスト環境におけるポート・スキャンによって可能である。不要なポートおよびサービス（例：埋め込みウェブ・サーバ）はすべて無効にすべきである。

- すべての組み込まれたシステム・セキュリティ機能は有効にする。

- できるだけリムーバブル・メディア（例：CD、フロッピー・ディスク、USB メモリ・スティック）の使用を制限する。可能であれば、リムーバブル・メディアは使用しない。リムーバブル・メディアを使用する必要のある場合は、マルウェアが含まれていないかどうかを使用前に確認する手順を行うべきである。

4.3.7 バックアップと回復

- 特定された電子的および物理的脅威に対して適切で効果的なバックアップと回復手順を定める。これは審査し、定期的にテストすべきである。

- 完全復旧プロセスにより定期的にバックアップの完全性をテストする。

- バックアップは現場と別の場所に保存する。

- メディアは、セキュリティで保護して持ち運び、安全な場所に適切に保管するべきである。

4.3.8 物理的セキュリティ

- プロセス制御システムと関連するネットワーキング装置を物理的攻撃や内部の不正アクセスから守るため、物理的セキュリティ保護対策を講じる。複数

の対策を組み合わせる必要があるだろう。例えば、ドライブ・ロック、不正操作を防ぐケース、セキュリティの高いサーバ室、アクセス制御システム、監視カメラである。

4.3.9 システム監視

- 電子的インシデントの結果と思われる異常動作（例、ネットワークのトラフィックが増えたのはワームに感染したからかもしれない）を検出するため、プロセス制御システムをリアルタイムで監視する。様々なパラメータを定義し、リアルタイムで監視し、異常動作検出のための正常動作基準と比較すべきである。

- 可能な限り、ネットワーク活動をより細かく見るために侵入検出と防護を実装する。これらのシステムは、プロセス制御環境に合うように改造すべきである。

- 定義した一連のプロセス制御システム・ログファイルを定期的に調べ分析する。重要なログファイルのバックアップをとり、不正なアクセスや変更から防護する。

- 建物や施設内に監視カメラや不正操作警報装置等の物理監視システムの設置を考慮する。これは遠隔現場で特に重要である。

- パスカードを使ったセキュリティ・エリアへの入場はログとして残す。

4.3.10 ワイヤレス ネットワーキング

- 可能な限り、プロセス制御システムでワイヤレス・ネットワークは使わない。どうしてもワイヤレス・ネットワークを使用する必要がある場合には、徹底的にリスク評価を行い、適切な保護対策を講じる。

- ワイヤレス・セキュリティの分野は常に変化しており、わずか数年前に安全と考えられていたソリューションでも現在は脆弱と認識される。ワイヤレス・システムは、業界のベスト・プラクティスを参考にして、最新のセキュリティ保護対策をとるべきである。最新のベスト・プラクティスに改訂されていないかどうか、定期的に確認するべきである。

- ワイヤレス・ソリューションを設計し、展開する場合は、そのソリューションで使用されるセキュリティ・メカニズムを理解し、正しく設定すること。

- ワイヤレス・システムのセキュリティ保護に関する詳細については、付録 A の一覧に示すガイドを参照のこと。

4.3.11 セキュリティ・パッチ

- プロセス制御システムへのセキュリティ・パッチの適用に関するプロセスを確立する。

- このプロセスを支援するため、監査とパッチ適用ツールを活用すべきである。

- このプロセスは、パッチ適用前にそのパッチに対するベンダの認定を受け、パッチをテストすること、および変更により支障が起こる危険を最小限にするために段階的に適用するプロセスを考慮すべきである。

- セキュリティ・パッチが不可能か、現実的でない場合は、それに代わる適切な防護手段を考慮すべきである。

一般的なパッチ管理の詳細なガイドは、CPNI ガイドに記載されている。このガイドの入手先については付録 A を参照のこと。このガイドは一般的な文書であり、プロセス制御と SCADA システムに特化したものではない。

4.3.12 要員の身元確認

- プロセス制御システムの運用または管理のためにアクセスできるすべての要員は適切に審査する。詳細については BS7858 を参照。

雇用前スクリーニングの詳細については、CPNI ガイドや CPNI のウェブサイト、BS7858 に記載されている。ガイドの入手先については、付録 A を参照のこと。

4.3.13 パスワードとアカウント

- すべてのプロセス制御システムについて、パスワードの強さと有効期限を含むパスワード・ポリシーを適用する。 パスワードは頻繁に変更することを推奨する。これが不可能か、現実的でない場合は、それに代わる適切な防護手段を考慮すべきである。

- 定期的にすべてのアクセス権を審査し、古いアカウントは無効にする。

- デフォルトの設定から変更が可能ならばベンダ・パスワードを変更する。

- 機能によっては、パスワードが不要と判断される場合もある（例、閲覧のみのモード）

- 重要な機能に対してはより強い認証方法を考慮する。

4.3.14 文書セキュリティ・フレームワーク

- プロセス制御システムとその構成要素のすべてを含む目録を文書化する。

- プロセス制御システム に対するセキュリティのフレームワークを文書化し、現在の脅威を反映するよう定期的に審査し更新する。この文書は、リスク評価、前提、既知の脆弱性、採用されている防護対策の詳細を記述すべきである。

- すべてのプロセス制御システムに関する文書は安全に保管し、権限のある者だけが閲覧できるようにする。

4.3.15 回復力の高いインフラストラクチャと設備

- システムは適切なインフラストラクチャ（冗長ネットワークなど）を使用してインストールするべきである。

- 適切な環境条件に装置が維持されるよう、装置は、環境管理区域に配置すべきである。

- 必要であれば、制御システムを保護するための防火システムを取り付けるべきである。

4.3.16 脆弱性管理

- プロセス制御環境における脆弱性を最小限にとどめるため、脆弱性管理体系を実装すること。脆弱性管理の一般的な手法は、セキュリティ・スキャンである。プロセス制御システムのスキャンは重大なリスクを伴う可能性がある。スキャンは、条件を注意深く選択して実行すべきである。例えば、プラントの停止時に実行したり、テスト環境で実行したりすること。スキャンを実行する前には必ず完全なリスク評価を実施すること。

4.3.17 転入者と転出者用のプロセス

- 転入者がプロセス制御チームに加わった場合に、適切なアカウント、権限レベルを与え、セキュリティ訓練を実施する手順を作る。

- プロセス制御チームの要員が転出するか、その役割や責任が変わった場合に、機密情報や文書を回収し、アカウントを使用不可にし、パスワードを変更する手順を作る。

4.3.18 変更管理

- すべてのシステムに、厳格な変更管理プロセスを設ける。これらのプロセスにはセキュリティ評価を含めるべきである。変更を複数の変更管理プロセスで評価し承認する必要がある場合もある（例、ファイアウォールの変更は IT とプラントの両変更管理プロセスの対象となる）。

4.3.19 セキュリティ試験

- 可能な限り、セキュリティ試験を実施する。例えばペネトレーション試験である。稼働中の環境でセキュリティ試験を実施できることはまれである。したがって、専用のテスト環境またはバックアップ・システム上で行うか、プラント停止中に行う。

- IP 化された制御機器はすべて、よくある DoS 攻撃に対して脆弱ではないことを保証するためセキュリティ試験を行うべきである。

ペネトレーション試験に関する詳細については、CPNI ガイド（このガイドの場所については、付録 A を参照）に記載されている。このガイドは一般的な文書であり、プロセス制御と SCADA システムに特化したものではない。

4.3.20 セキュリティ・スキャン

- 可能な限り、セキュリティ・スキャンを実施する。セキュリティ・スキャンは IT ネットワークにおける脆弱性管理のツールとして広く使われている。

4.3.21 機器接続手順

- 機器をプロセス制御ネットワークに接続する前にそれがウイルスやワームに感染していないことを確認する手順を作成する。

詳細なグッド・プラクティス・ガイドは以下のサイトで入手できる。

www.cpni.gov.uk/protectingyourassets/scada.aspx

5.1 概要

プロセス制御システムに対するセキュリティ措置は一回だけ行えばよいものではない。プロセス制御システムのセキュリティや運転に対する脅威は、刻々と変わるので、プロセス制御システムのセキュリティ評価は継続的に行うべきである。その中には、新しい脆弱性、セキュリティ脅威の変化、電子的セキュリティインシデント（例、ワームまたはハッカーによる攻撃）を特定し、評価し、対応することが含まれる。定式化された対応管理プロセスを確立することにより、リスクの変化をできるだけ早く見つけ、必要な是正措置を速やかに講じることが可能になる。

5.2 目標

様々な電子的セキュリティ問題の発生を監視し、評価し、適切な対応措置を取る手順を確立する。

5.3 グッド・プラクティスの原則

- セキュリティインシデントが疑われる事態に対応するプロセス制御セキュリティ対応チーム（PCSRT）を組織する。PCSRT を組織したい重要国家インフラ企業は、UNIRAS に連絡すれば助言や支援を受けることができる。
- すべてのプロセス制御システムに対して、適切な電子的セキュリティ対応計画と事業継続計画を作成する。
- すべての電子的セキュリティ対応計画は定期的に維持し、模擬演習をし、テストする。
- セキュリティ警報やインシデントを適切な要員に通知する早期警戒システムを構築する。
- セキュリティ警報やインシデントを監視し、評価し、対応を始動するプロセスと手順を確立する。
- すべてのプロセス制御セキュリティインシデントは正式に報告し、レビューし、学ぶべき事項を書き留める。

詳細なグッド・プラクティス・ガイドは以下のサイトで入手できる。

www.cpni.gov.uk/protectingyourassets/scada.aspx

6.1 概要

全体的なセキュリティ対策には、技術、手順、社会などあらゆる観点から対応する必要がある。セキュリティ保護対策の技術や手順が上手く行くかどうかは最終的には人にかかっている。従業員は最も重要な資源であると同時に、セキュリティに対する最大の脅威でもある。プロセス制御システム要員は IT セキュリティになじみがないことが多いし、IT セキュリティ要員はプロセス制御システムやその稼働環境になじみがないことが多い。一般的な意識向上プログラムや教育により理解を深めさせたり、訓練によりスキルを高めさせたりすることにより、この状況を改善することができる。

6.2 目標

組織全体のプロセス制御セキュリティ意識を底上げし、すべての要員がその任務を果たすのに必要な適切な知識とスキルを持たせる。

6.3 グッド・プラクティスの原則

6.3.1 意識向上

- 企業経営者と共になって、プロセス制御セキュリティ・リスクが事業に与える影響を理解させ、リスク管理に率先して取り組むようにさせる。
- 一般的なセキュリティ理解を深めるために意識向上プログラムを確立する。これらのプログラムでは、セキュリティ責任を明確にし、現在の脅威に注意を向けさせ、警戒心を高めさせる。
- プロセス制御セキュリティ・プログラムを支援する投資対効果モデルを構築する。

6.3.2 訓練フレームワークの確立

- IT 要員に、プロセス制御システムとその稼働環境を理解させ、プロセス制御システムのセキュリティと IT セキュリティの違いを明確にする。
- プロセス制御チーム員が適切な IT セキュリティ・スキルを持つよう訓練すると同時に／または、適切な IT 支援サービスを提供する。

6.3.3 協力関係の醸成

- IT セキュリティチームとプロセス制御チームの間の協力関係を確立し、互いに協力し、スキルを共有し、知識の移転を容易にする。

詳細なグッド・プラクティス・ガイドは以下のサイトで入手できる。

www.cpni.gov.uk/protectingyourassets/scada.aspx

7. サード・パーティ・リスクの管理

7.1 概要

プロセス制御システムは、ベンダ、サポート組織、サプライ・チェーン内の他の関係者等のサード・パーティにより重大なセキュリティ・リスクがもたらされることがあるので、十分な注意を払う必要がある。ダイヤルアップ接続やインターネットのような容易に接続を設定できる技術は、組織外からの新しい脅威の種となる。したがって、サード・パーティもかかわりを持たせ、このようなリスクを減少するための手段を講じなければならない。

7.2 目標

ベンダ、サポート組織、その他のサード・パーティからのすべてのセキュリティ・リスクを管理する。

7.3 グッド・プラクティスの原則

7.3.1 サード・パーティを特定する

- プロセス制御システムと関係するベンダ、サービス・プロバイダ、サプライ・チェーン内の他の関係者を含めすべてのサード・パーティを特定する。

7.3.2 ベンダからのリスクの管理

- 購入契約締結前にすべての購入契約のセキュリティ条項は詳細に記述する。
- ベンダが供給したシステム内に脆弱性が現在および将来発見された場合、それを特定し、速やかにユーザに通知するよう、すべてのベンダと継続的に関係を維持する。
- 現在の制御システムに対するセキュリティ手引きと、将来のシステム開発に対するセキュリティ・ロードマップを提供するようベンダに要求する。
- すべてのベンダがそのプロセス制御システム内に適切なウイルス対策措置を組み込むようにさせる。
- 効果的なソフトウエア・パッチ・プロセスをベンダと共に確立する。
- 稼働中のプロセス制御システムに対するシステムの堅牢化手順についてベンダと合意する。
- すべての脆弱性を管理できるように、プロセス制御システム内で使われているすべての要素技術（例、データベース）を特定する。
- すべてのベンダについて定期的なセキュリティ審査と監査を実施する。

7.3.3　サポート組織からのリスクの管理

- サポート組織のリスク評価を定期的に実施し、必要な対策を講じる。

- セキュリティ違反の可能性を防ぐか削減する適切な措置が講じられるまで、サポート組織がプロセス制御システムにアクセスできないようにする。接続の条件を定め契約を作り、締結する。

- 基幹のプロセス制御システムと連携するサポート組織のシステム内に脆弱性が現在および将来発見された場合、それを特定し、速やかにユーザに通知するよう、すべてのサポート組織と継続的に連携する。

- すべてのサポート組織が、自組織がサポートしているプロセス制御システムを完全に理解するようその意識を向上させ、合意したセキュリティ手順にしたがってサポートを実施するよう合意を取り付ける。

7.3.4　サプライ・チェーン内のリスクの管理

- プロセス制御のセキュリティ・リスクが管理されているとの保証が得られるよう、組織と連携する。そのような組織として、供給会社、販売会社、製造会社、顧客が考えられる。

詳細なグッド・プラクティス・ガイドは以下のサイトで入手できる。

www.cpni.gov.uk/protectingyourassets/scada.aspx

8.1 概要

システムが構築され、使用状態になった後にそのシステムのセキュリティ保護対策を実施するのは大変困難で費用がかかることはよく知られている。更に重要なことは、稼働中のシステムにセキュリティ対策を施しても、効果が低いことが多いことである。プロジェクト開発プロセスの早い段階でセキュリティ・リスクに対する保護対策を組み込む方が、より効果的であるし、それにより見積超過も防げるし、通常安くつく。

8.2 目標

プロセス制御システムに影響を与えるすべてのプロジェクトのライフサイクルを早期に特定し、その設計や仕様に適切なセキュリティ対策を組み込む。

8.3 グッド・プラクティスの原則

- プロセス制御システムに影響を与えるすべてのプロジェクトを特定し、その開発の初期段階から参画する。
- プロジェクトの全ライフサイクルに渡ってセキュリティ・リスク管理の責任者となるセキュリティ・アーキテクトを任命する。
- すべての購入契約に標準セキュリティ条項と仕様を含める。
- プロジェクトの設計と仕様にセキュリティ要件を含め、すべての適切なセキュリティ・ポリシーと標準が守られるようにする。
- プロジェクト開発の全ライフサイクルに渡ってセキュリティ審査を実施する。例えば、人の健康と安全チェックと同時にセキュリティ審査を行う。
- プロジェクト開発ライフサイクルの重要なポイント（入札、試運転、工場での受入検査と試運転）でセキュリティ試験を行うよう計画する。

Idaho National Laboratory 作成の『Cyber Security Procurement Language for Control Systems』には調達に関する詳細が記載されている（付録 A 参照）。

詳細なグッド・プラクティス・ガイドは以下のサイトで入手できる。

www.cpni.gov.uk/protectingyourassets/scada.aspx

9.1 概要

プロセス制御システム・セキュリティの管理を公式に統制することにより、組織全体で一貫した、適切な対策を取れるようになる。そのような統制がないと、プロセス制御システムの保護は場当たり的で不十分のものになり、その組織はさらなるリスクに曝される。効果的な統制フレームワークには、プロセス制御のセキュリティ・リスク管理に関する明確な役割と責任、更新ポリシー、標準、さらに、そのポリシーや標準が守られていることの保証が含まれる。

9.2 目標

プロセス制御システムのセキュリティとリスク管理について明確な指針を与え、そのポリシーと標準が継続的に守られ見直されているようにする。

9.3 グッド・プラクティスの原則

9.3.1 役割と責任の定義

- プロセス制御のセキュリティ・リスクに対する責任者を任命する。
- プロセス制御セキュリティのすべての要素の役割と責任を定義する。
- プロセス制御システム・セキュリティについて経営者の支持を得る。

9.3.2 ポリシーと標準の作成

- プロセス制御システム・セキュリティに関する公式化されたポリシーと標準を定め、文書化し、周知し、変更管理の下で管理する。そのポリシーと標準は、組織の要求条件を正確に反映し、事業の要求条件をサポートし、すべての関係者が合意したものとする。
- プロセス制御セキュリティに関する、法令および規制による要件の影響を特定する。特定された内容は、必ずポリシーや標準に組み込む。
- プロセス制御システムのセキュリティ・プラクティスを、事業面および運用面のニーズに合わせるようにする。

9.3.3 ポリシーと標準の遵守

- プロセス制御システム・ポリシーと標準が継続して遵守されるようにする保証プログラムを実施する。

9.3.4　ポリシーと標準の更新

- プロセス制御のセキュリティ・ポリシーと標準を定期的に審査し、現在の脅威、法令の変更、事業と運転の要求条件の変更に合わせて更新する、継続したプログラムを確立する。

詳細なグッド・プラクティス・ガイドは以下のサイトで入手できる。

www.cpni.gov.uk/protectingyourassets/scada.aspx

付録 A： 本ガイドで使用した参考文献および参考ウェブサイト

セクション **2.2.1**
Using Operational Security (OPSEC) to Support a Cyber Security Culture in Control Environments
http://csrp.inl.gov/Documents/Opsec%20Rec%20Practice.pdf

セクション **4.3.2**
Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks
http://www.cpni.gov.uk/Docs/re-20050223-00157.pdf

セクション **4.3.10**
Recommended Practices Guide for Securing ZigBee Wireless Networks in Process Control System Environments Draft
http://csrp.inl.gov/Documents/Securing%20ZigBee%20Wireless%20Networks%20in%20Process%20Control%20System%20Environments.pdf

Securing WLANs using 802,11i
http://csrp.inl.gov/Documents/Wireless%20802.11i%20Rec%20Practice.pdf

セクション **4.3.11**
Good Practice Guide Patch Management
http://www.cpni.gov.uk/Docs/re-20061024-00719.pdf

セクション **4.3.12**
A Good Practice Guide on Pre-Employment Screening
http://www.cpni.gov.uk/Products/bestpractice/3351.aspx

Personnel Security Measures
http://www.cpni.gov.uk/ProtectingYourAssets/personnelSecurity.aspx

BS 7858:2006: Security screening of individuals employed in a security environment. Code of practice
http://shop.bsigroup.com/ProductDetail/?pid=000000000030194702

セクション **4.3.18**
Best Practice Guide Commercially Available Penetration Testing
http://www.cpni.gov.uk/Docs/re-20060508-00338.pdf

セクション **8.3**
Cyber Security Procurement Language for Control Systems
http://www.msisac.org/scada/documents/12July07_SCADA_procurement.pdf

一般的な SCADA 参考文献

BS 7858:2006: Security screening of individuals employed in a security environment. Code of practice
http://shop.bsigroup.com/ProductDetail/?pid=000000000030194702

BS 8470:2006 Secure destruction of confidential material. Code of practice
http://shop.bsigroup.com/en/ProductDetail/?pid=000000000030127562

Best Practice Guide Commercially Available Penetration Testing
http://www.cpni.gov.uk/Docs/re-20060508-00338.pdf

Best Practice Guide on Firewall Deployment for SCADA and Process Control Networks
http://www.cpni.gov.uk/Docs/re-20050223-00157.pdf

CPNI First Responders f Guide: Policy and Principles
http://www.cpni.gov.uk/docs/re-20051004-00868.pdf

CPNI SCADA Good Practice Guides
http://www.cpni.gov.uk/ProtectingYourAssets/scada.aspx

CPNI Information Sharing
http://www.cpni.gov.uk/ProtectingYourAssets/InformationSharing.aspx

CPNI Personnel Security measures
http://www.cpni.gov.uk/ProtectingYourAssets/personnelSecurity.aspx

Good Practice Guide Patch Management
http://www.cpni.gov.uk/Docs/re-20061024-00719.pdf

Good Practice Guide Outsourcing: Security Governance Framework for IT Managed Service Provision
http://www.cpni.gov.uk/Docs/re-20060802-00524.pdf

Good Practice Guide on Pre-Employment Screening
http://www.cpni.gov.uk/Products/bestpractice/3351.aspx

An Introduction to Forensic Readiness Planning
http://www.cpni.gov.uk/docs/re-20050621-00503.pdf

Personnel Security Measures
http://www.cpni.gov.uk/ProtectingYourAssets/personnelSecurity.aspx

DHS Control Systems Security Program
http://www.us-cert.gov/control_systems/practices/Introduction.html

DHS Control Systems Security Program Recommended Practice
http://www.us-cert.gov/control_systems/practices/

Guide to Industrial Control Systems (ICS)
http://csrc.nist.gov/publications/PubsDrafts.html

Securing WLANs using 802,11i
http://csrp.inl.gov/Documents/Wireless%20802.11i%20Rec%20Practice.pdf

Using Operational Security (OPSEC) to support a Cyber Security Culture in Control Systems Environments
http://csrp.inl.gov/Documents/OpSec%20Rec%20Practice.pdf

DHS Catalog of Control System Security Requirements
http://www.dhs.gov

Manufacturing and Control Systems Security
http://www.isa.org/MSTemplate.cfm?MicrositeID=988&CommitteeID=6821

ISO 17799 International Code of Practice for Information Security Management
http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39612

ISO 27001 International Specification for Information Security Management
http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103

Cyber Security Procurement Language for Control Systems
http://www.msisac.org/scada/documents/12July07_SCADA_procurement.pdf

MU Security Industrial Control (MUSIC) Certification
http://www.musecurity.com/support/music.html

Control System Cyber Security Self-Assessment Tool (CS2SAT)
http://www.us-cert.gov/control_systems/pdf/CS2SAT.pdf

Department of Homeland Security Control Systems Security Training
http://www.us-cert.gov/control_systems/cstraining.html

Recommended Practices Guide for Securing ZigBee Wireless Networks in Process Control System Environments
http://www.us-cert.gov/control_systems/pdf/Zigbee%20Rec%20Pract%20-%20draft-posted%207-10-07.pdf.

Achilles Certification Program
http://www.wurldtech.com/cyber-security/achilles-certification/achilles-certification.aspx
American Gas Association (AGA)
http://www.aga.org

American Petroleum Institute (API)
http://www.api.org

Certified Information Systems Auditor (CISA)
http://www.isaca.org/

Certified Information Systems Security Professional (CISSP)
http://www.isc2.org/

Global Information Assurance Certification (GIAC)
http://www.giac.org/

International Council on Large Electric Systems (CIGRE)
http://www.cigre.org

International Electrotechnical Commission (IEC)
http://www.iec.ch

Institution of Electrical and Electronics Engineers (IEEE)
http://www.ieee.org/portal/site

National Institute of Standards and Technology (NIST)
http://www.nist.gov

NERC Critical Infrastructure Protection (CIP)
http://www.nerc.com/page.php?cid=2|20

Norwegian Oil Industry Association (OLF)
http://www.olf.no/en/

Process Control Security Requirements Forum
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.76.3845&rep=rep1&type=pdf

US Cert
http://www.us-cert.gov/control_systems/

WARPS
http://www.warp.gov.uk

謝辞

PA と CCPNI は、本グッド・プラクティス・ガイドライン・フレームワーク作成中に、the SCADA and Control Systems Information Exchange から、また世界中の CNI 保護の関係者から受け取ったコメントや提案に感謝する。多くの寄書を感謝して受理したが、その数が余りに多いので個々に謝辞を述べることはできない。

著者について

本文書は、PA Consulting Group と CPNI が共同で作成した。

Centre for the Protection of National Infrastructure
Central Support
PO Box 60628
London
SW1P 9HA
Fax: 0207 233 8182
Email: enquiries@cpni.gov.uk
Web: http://www.cpni.gov.uk

プロセス制御と SCADA セキュリティについて CPNI から更なる情報を得るには下記を利用されたい。
Web: http://www.cpni.gov.uk/ProtectingYourAssets/scada.aspx

PA Consulting Group
123 Buckingham Palace Road
London
SW1W 9SR
Tel: +44 20 7730 9000
Fax: +44 20 7333 5050
Email: info@paconsulting.com
Web: www.paconsulting.com

プロセス制御と SCADA セキュリティについて PA Consulting Group から更なる情報を得るには下記を利用されたい。
Email: process_control_security@paconsulting.com
Web: www.paconsulting.com/process_control_security