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
ガイド 4. 意識とスキルの改善

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　GUIDE 4. IMPROVE AWARENESS AND SKILLS" 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 用語

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 背景

プロセス制御と SCADA システムは、標準 IT 技術を使用しており、ますますそれらに依存するようになってきた。Microsoft Windows、TCP/IP、ウェブ・ブラウザ、それに今後はワイヤレス技術等の技術が、従来の企業独自の技術に置き換わり、さらに市販品が、特注のプロセス制御システムに置き換わるようになった。

このような進展は事業上多くの利点があるが、2 つの重要な懸念が生まれてきた。

1 つ目は、伝統的に制御と安全だけを目指して設計されてきたプロセス制御システムが、かつては隔離されていたのだが、例えば、加工前のプラント情報を取り出すため、または直接製品ダウンロードを可能にするため、大規模なオープンネットワークへ接続されるようになり、ワーム [1]、ウイルス、ハッカー等、以前は遭遇するとは考えられなかった脅威にさらされるようになった。

2 つ目は、企業独自のプロセス制御システムに代わって、商用市販ソフトウエアや汎用ハードウエアが使われるようになったことである。これらの技術とともに通常使用される標準 IT セキュリティ保護対策の多くは、まだ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、セキュアな環境を保つのに十分なセキュリティ対策が講じられていない可能性がある。

これらの脆弱性が攻撃されれば重大な結果を招く恐れがある。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は、例えば、悪意ある攻撃、DoS攻撃、プロセスの不正な制御、完全性の損失、機密性の欠如、世評の下落、健康・安全・環境への悪影響などがありうる。

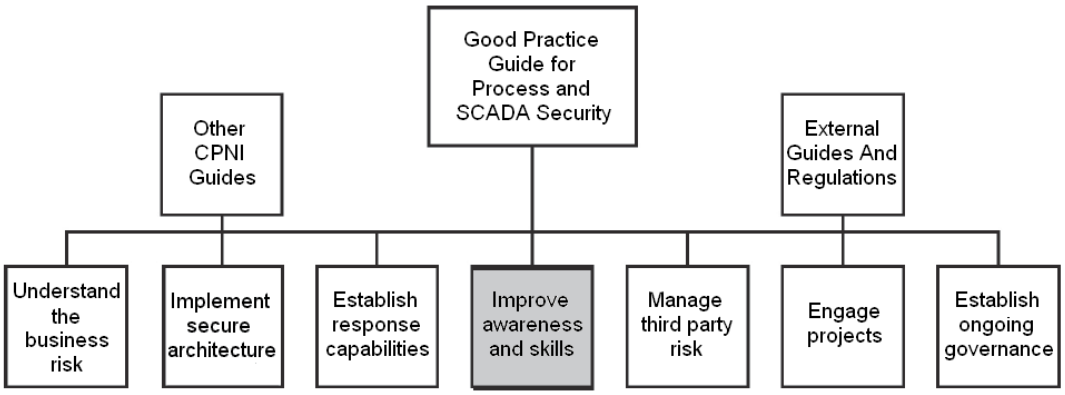
1.3 プロセス制御セキュリティ・フレームワーク

現在、プロセス制御システムは大抵、標準 IT 技術に基づいているが、その運用環境は、企業の IT 環境とは大きく異なっている。IT セキュリティ専門家の経験から学べる点は多い。また、標準的セキュリティ・ツールや手法は手直しをすることで、プ

[1] ワームについての Wikipedia の説明 – コンピュータ・ワームは、自己複製するコンピュータ・プログラムである。ネットワークを使って自己の複製を他のシステムに送信する。ユーザの介在なしに送信することもある。ウイルスと異なり、既存プログラムに取りつくことはない。ワームは常に（帯域を消費するだけとしても）ネットワークに悪影響を与える。一方、ウイルスは常に攻撃対象のコンピュータ上のファイルに感染したり、破壊したりする。

ロセス制御システムの保護に使用できるものもあれば、制御環境にはまったく不適切であったり、適用不能であったりするものもある。

プロセス制御セキュリティ・フレームワークは、プロセス制御や IT セキュリティ分野の業界のグッド・プラクティスに基づいており、プロセス制御と SCADA 環境における標準 IT 技術利用の増加に対応するための 7 つの重要なテーマを対象としている。本フレームワークは、組織がその必要性に適切に対応するプロセス制御セキュリティを開発・調整しようとするときに参考となる基準を示すことを意図している。本フレームワークの 7 つの要素を図 1 に示す。



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範
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、事業リスクの理解に関するグッド・プラクティスの手引きを示すものである。グッド・プラクティス・ガイド・フレームワークの文書はすべて、次のリンク先から入手できる。http://www.cpni.gov.uk/ProtectingYourAssets/scada.aspx

1.4 本ガイドの目的

- CPNIの「Good Practice Guide Process Control and SCADA Security」（日本語版：「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」）はプロセス制御セキュリティに対応するための 7 つの要素からなるフレームワークを提案している。本「**意識とスキルの改善**」ガイドは上位のグッド・プラクティス・ガイドで述べられた基礎に立って作られたものであり、プロセス制御システム・セキュリティのための適切な統制フレームワークを定義し実施するためのグッド・プラクティスを示す。

本ガイドはプロセス制御に必要なセキュリティ意識やトレーニングコースについては言及していない。

1.5 想定読者

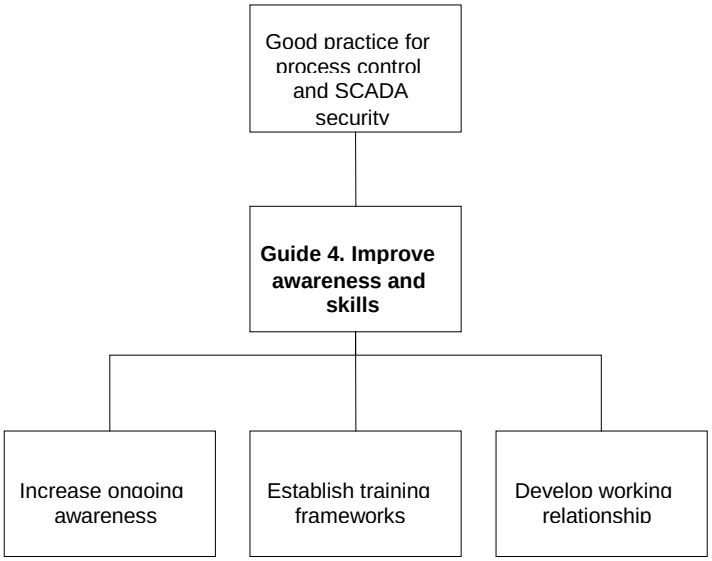
本ガイドは、プロセス制御のセキュリティ、SCADA、産業オートメーション・システムに従事する、以下のような人たちを対象としている。

- プロセス制御とオートメーション、SCADA テレメトリ技術者
- 情報セキュリティ専門家
- 物理セキュリティ専門家
- 事業リーダー
- リスク管理者
- 健康・安全管理者
- オペレーション技術者

2. 意識とスキルの改善についての要約

セキュリティ・フレームワークの成功は、最終的には人的要素にかかっている。人は、最も重要なリソースであると**同時に**、セキュリティにとって最大の脅威となる恐れも秘めている。プロセス制御環境において、プロセス制御担当者が IT セキュリティに精通していない場合や、その逆に IT セキュリティ担当者がプロセス制御システムを熟知していない場合は、少なくない。

セキュリティは、従来、企業 IT 環境の問題であり、プロセス制御環境の問題ではないと考えられてきた。またこれまでは、セキュリティの責任を負うのは IT 部門であると考えられてきた。さらに、利用可能なセキュリティ・ツールや技術が、プロセス制御システムとの互換性を明らかに欠いていたことが原因で、制御システムのセキュリティが不十分なものとなっていた。プロセス制御システムのセキュリティは、意識の向上、スキルの向上、IT セキュリティ担当者との緊密な関係の構築により、向上させることができる。



Good practice for process control 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
Guide 4. Improve awareness and skills	ガイド 4. 意識とスキルの改善
Increase ongoing awareness	継続的意識の向上
Establish training frameworks	トレーニング体制の確立
Develop working relationship	協力関係の構築

図2 – 意識とスキルの改善の概要

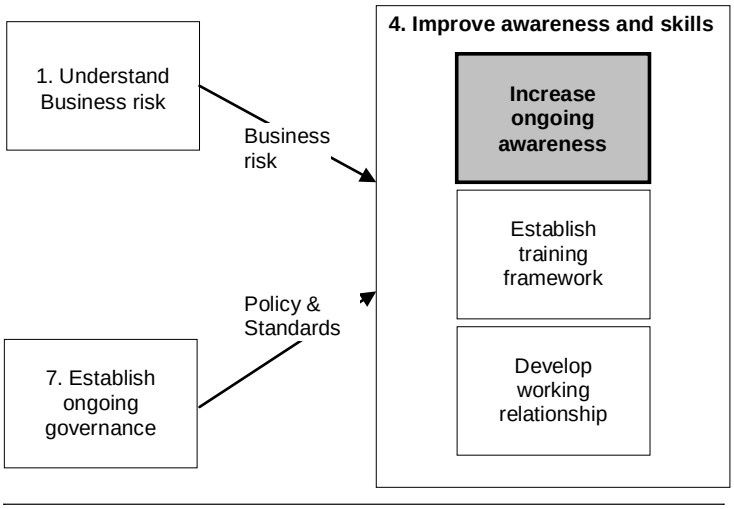
プロセス制御セキュリティの問題は、組織内の多数の人々に関わりを持っている。この問題に関する意識を向上させることにより、これらのシステムの脆弱性、脅威、リスクが浮き彫りとされる。また、プロセス制御セキュリティの障害により業務に及ぶ恐れのある影響も明確となる。サイバー・セキュリティ攻撃の成功を阻止するために導入可能な技術的および手順的な解決方法については、意識プログラムで検証を行う必要がある。

また、プロセス制御システムの安全を十分に確保する上で必要な知識を伝達するため、トレーニングを定める必要がある。このトレーニングでは、IT スキルからプロセス制御スキルまで、幅広い技術分野を取り扱うこととなる。このような特殊なニーズを対象としたトレーニング・コースはほとんど存在しない。そのため、セキュリティ・リスクに対する意識およびそのリスクに対処するための知識を関係者が確実に身につけられるように、トレーニング枠組みの目標を定めること。

意識と訓練により、プロセス制御部門と IT 部門の協力関係を密接なものとすることができる。これは、効果的なプロセス制御セキュリティ・プログラムの開発に使用できる共通の言語とプロセスがもたらされるからである。プロセス制御セキュリティを組織内に定着させることは、プロセス制御セキュリティ・プログラムの効果を継続的に発揮させる上で重要である。

3.1 フレームワーク全体における本セクションの位置づけ

フレームワークにおけるこの要素では、幅広い分野にわたってプロセス制御セキュリティ問題に関する**意識**を向上させることに焦点を当てている。またこの要素は、グッド・プラクティス・ガイド・フレームワークにおける「**事業リスクの理解**」と「**継続管理の確立**」の 2 つの要素の上に成り立っている。



1. Understand Business risk	1. 事業リスクの理解
7. Establish ongoing governance	7. 継続管理の確立
Business risk	事業リスク
Policy & Standards	方針および基準
4. Improve awareness and skills	4. **意識とスキルの改善**
Increase ongoing awareness	継続的意識の向上
Establish training framework	トレーニング体制の確立
Develop working relationship	協力関係の構築

図3 – フレームワーク内における「継続的意識の向上」の位置づけ

3.2 論理的根拠

意識を向上させることは、現在行われているプロセス制御セキュリティの作業において最も有益な行為となる可能性がある。意識を向上させるには、プロセス制御システム・セキュリティに関する知識と、セキュリティの一時的喪失により業務に及

び得る影響に関する知識を、すべての担当者に十分に身につけさせるようにする。担当者は、攻撃を阻止する場合やインシデントが発生した場合に何をなすべきかを知る必要がある。

3.3 グッド・プラクティスの原則

包括的な文書「Good Practice Guide Process Control and SCADA Security」（日本語版：「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」）に記載されているグッド・プラクティスの原則は次の通りである。

- 上級管理者との連動（事業におけるプロセス制御セキュリティ・リスクの意味が理解され、このリスクに対処するための設備投資を実現する上で役に立つ）
- セキュリティ全般に関する理解を深めるための意識プログラムの構築（このようなプログラムでは、セキュリティ責任の強調、現在の脅威に対する注意の喚起、警戒の強化がなされる）
- プロセス制御セキュリティ・プログラムを支援する事業モデルの構築

3.4 グッド・プラクティスの手引き

プロセス制御セキュリティの意識を促すメッセージは、対象者に合わせて作成する必要がある。また、こうしたメッセージでは、適切なメッセージを伝えて理解してもらうようにするために、組織とその作業環境を考慮する必要がある。

意識の向上は一度行えばよいというものではない。それは絶え間なく続くプロセスであり、これにより、組織の風土を変えていき、やがては組織内に定着させることが可能となる。意識を拡大するための方法は多数存在する。しかし、意図した対象者にこれらのメッセージを伝えるための最適な方法を考え出すには時間が必要とされる。意識向上への取り組み方は、組織ごとに異なる。また、組織の風土、規模、プロセス制御システムへの依存度、その他の要因などによっても異なる。

プロセス制御セキュリティ・プログラムを成功させる上で、意識に関係する 2 つの重要な要素を整える必要がある。それは、上級管理者の関与と、意識プログラムの構築である。さらにもう 1 つの主要な要素は、明瞭に伝達された、プロセス制御セキュリティ・プログラムを支援する事業モデルが存在すべきということである。

3.4.1 上級管理者の関与

プロセス制御セキュリティ問題に対する意識は、プロセス制御セキュリティについて実際に考える過程で高められる。しかし、上級管理者からの支持の存在はその問題の重要性を示すものであり、注目を要する。

上級管理者の支持と約束を取り付けることは、プロセス制御セキュリティ・メッセージをより多くの者に浸透させるための必須要件である。管理者の支援や利害関係者との取り決めがあれば、プロセス制御セキュリティの担当者は、メッセージが管理レベルを介して確実に遅滞なく順次伝達させ、多数の内部的な問題を解決することができる。

上級管理者を関与させるため、制御システムのセキュリティが事業にとっていかに重要かの証明が必要な場合がある。この証明には、セキュリティ・プログラムが存在しない場合のリスク、そしてセキュリティ・プログラムが存在する場合のコストと利点を示す事業モデルの開発が必要となる可能性がある。

上級管理者が関与することにより得られる主要なメリットの一部を以下に挙げる。

- リスクが存在することの理解
- プロセス制御セキュリティのプロファイル作成
- 管理階層と伝達経路を介して行われるメッセージの順次伝達
- 意識プログラムのための適切な予算の確保
- 残余リスクが存在することの理解
- 内部のリソースを隔てる境界撤廃の容易化

3.4.2 意識プログラムの構築

プロセス制御セキュリティは、複雑で、よく認知されていない技術や概念を採用していることがある。そのため、メッセージに手を加えて意識プログラムに導入することが必要とされる。意識メッセージの決定に際しては、意識の向上や定着が長期的なプロセスであり、1 回限りの努力ではない点を理解することが重要である。つまり、意識の向上や定着はマラソンであり、短距離走ではないのである。

いかなるプロセス制御セキュリティ意識プログラムであろうとも、重要なのは、適切な計画を行うことである。粗悪な計画を下手に実行しようとすると、プロセス制御セキュリティ・プログラムの妨げとなる恐れがある。意識プログラムの計画と実行が適切に行われるようにするには、多数の事項について考慮が必要となる。

- セキュリティ意識の目標
- 対象者の特定
- 組織内における連絡方法の理解
- 組織内に既に蓄積されている知識
- 取り上げる必要がある意識問題
- メッセージの伝達に使用可能な意識方法
- 組織内のセキュリティ意識定着方法
- メッセージの理解を高める方法

これらについては、以下にその詳細を説明する。

セキュリティ意識の目標：特定の意識目標または目的を持つことにより、メッセージを適切な対象者に伝えることに重点を置く。また、目標が設定されることでプログラムの成功度合いを測る必然も生まれる。セキュリティを組織に定着させるには時間がかかる。そして、定着のための最適な方法は、重要メッセージに焦点を当て、時間をかけて徐々に意識を高めていくことである。

対象者：様々な対象者を特定することと、対象者に応じてメッセージの詳細が変化する点を理解することが、プロセス制御セキュリティ・プログラムを成功させる上で重要となる。例えば、以下に挙げる者が対象者となる可能性を持つ。

- プロセス制御、オートメーション、SCADA、テレメトリ技術者
- 経営指導者
- プロセス制御セキュリティ対応チーム（PCSRT）
- 情報セキュリティの専門家
- 物理的セキュリティの専門家
- 事業ユーザ
- リスク管理者
- プロジェクトの管理者とチーム
- 運用担当者
- 健康と安全の担当役員
- サポート組織

既存の連絡：意識向上プログラムへの着手に先立ち、既に確立されている連絡の枠組みとツールを把握することが重要である。組織を取り巻く情報の流れ方、送受信されるメッセージの種類、連絡対象者、連絡計画の完成度および連絡の受け取られ方の程度、連絡責任者について理解することが極めて重要である。既に存在する仕組みを採用することにより、プロセス制御セキュリティの意識に関する連絡作業を容易なものとすることができる。

既存知識：明白であるにもかかわらずしばしば見過ごされてしまうステップのひとつに、既存知識の判定がある。この判定は、大まかな調査や、1 人 1 人に対する意見の問い合わせなどにより行われる。既存知識は、次に示す意識問題の基礎として利用される。

意識問題：プロセス制御セキュリティの意識プログラムにおいて取り上げられる可能性がある一般的な問題を以下に挙げる。

- 一般的なプロセス制御セキュリティ意識
- 警戒すべき事柄と対処法
- プロセス制御セキュリティ障害とその影響の例
- 利用可能な方針、基準、ソリューション
- 既存文書の更新
    - 方針および基準
    - ベンダーからの指示
- IT 専門家向けのプロセス制御の説明と理解

- プロセス制御専門家向けの IT セキュリティの説明と理解

意識方法：意識を向上させるための方法には様々なものがある。最も優れた方法は、そうした多種多様な方法を混合したものとなる可能性が高い。意識メッセージを目的の対象者に送り届けるための適切な方法を考えることは重要である。その方法には以下のようなものがある。

- 会議
- 電子メール連絡
- ニュースレター
- プロセス制御セキュリティ情報の集中保存
- 電話連絡
- ポスターを使用したキャンペーン
- ビデオや DVD
- Web サイトや Web キャスト
- ワークショップ
- 通常会議の議題への追加

定着：プロセス制御セキュリティを組織内に定着させることは、一朝一夕でできるものではない。プロセス制御セキュリティは、長い時間をかけて発展し、その結果最終的に組織の日常に溶け込むものである。意識プログラムについては、定期的に見直しを行うことが必要である。これは、メッセージが確実に受け取られ、理解され、行動の基礎とされるようにするためである。この定期的見直しにより、プロセス制御セキュリティ・プログラムが組織の優先順位の上位に位置し続け、通常業務として定着することとなる。

理解： 受け手が理解していなければ、プレゼンテーションやメッセージがいかに優れていても意味がない。正しいメッセージが受け取られているかどうかを確認するため、受け手からのフィードバックが必須である。意識プログラムの定期的な確認も行って、メッセージが最新であり、行動の基礎とされるようにすべきであり、プロセス制御セキュリティ・プログラムが組織の優先順位の上位に位置し続け、通常業務として定着することとなる。

3.4.3 事業モデルの構築

制御システムのセキュリティを強化するため、事業モデルの様々なレベルにおいて事業全体が十分理解されるようにすることが重要である。事業モデルの主な要素は次のとおりである。

- 事業リスク・プロファイルの概要（インシデントおよび脆弱性がもたらす潜在的な脅威を含む）
- 改善後の向上したリスク・プロファイルを含む、制御システムのセキュリティ改善の利点（事業上の利点）

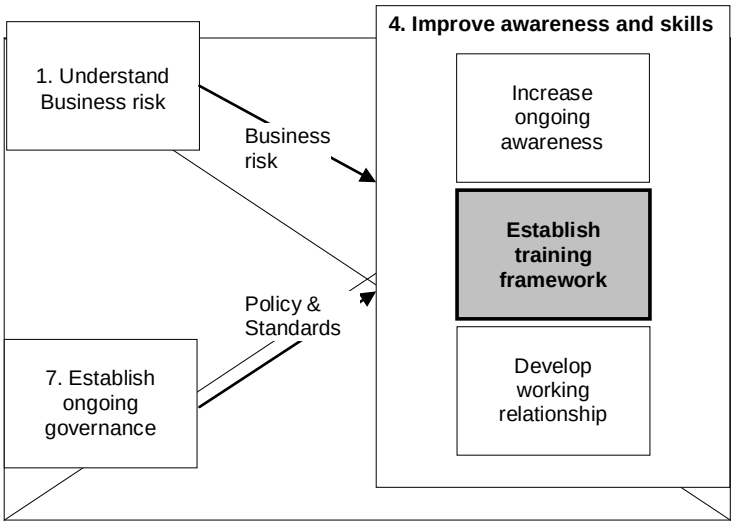
- セキュリティ・プログラム、主要な活動、リソース、およびコストに関する要件
- セキュリティ投資収益率（ROSI）

この活動は組織内の様々なレベルで実行が必要となる可能性がある。例えば、ある組織では、特定のサイトまたは制御システムを改善する低レベルの事業モデル構築が必要となるかもしれない。あるいは、大規模組織では、組織全体のための包括的事業モデルの構築が必要となる可能性がある。後者の主な利点は、中央で実行される事業モデルの施策が、各サイト・チームの具体的な活動を支援し、効率化を促すことである。

制御システムのための事業モデルの開発に関するガイドについては、NIST の『Guide to Industrial Control (ICS) Systems』（付録 A 参照）に記載されている。

4.1 フレームワーク全体における本セクションの位置づけ

フレームワークのこの要素では、トレーニング体制の確立により組織におけるプロセス制御セキュリティ・スキルの向上を図ることに焦点を当てている。これは、グッド・プラクティス・ガイド・フレームワークにおける「**事業リスクの理解**」と「**継続管理の確立**」の 2 つの要素の上に成り立っている。



1. Understand Business risk	1. 事業リスクの理解
7. Establish ongoing governance	7. 継続管理の確立
Business risk	事業リスク
Policy & Standards	方針および基準
4. Improve awareness and skills	4. 意識とスキルの改善
Increase ongoing awareness	継続的意識の向上
Establish training framework	トレーニング体制の確立
Develop working relationship	協力関係の構築

図4 – フレームワーク内における「トレーニング体制の確立」の位置づけ

4.2 論理的根拠

プロセス制御セキュリティの概念は比較的新しい。大部分の人々は、技術に関する理解の程度が低く、事業に及ぶ恐れのある影響についても、その意識をほとんど持っていない。採用可能な基準はほとんど存在せず、その上人材は、概して、要求さ

れるプロセス制御とセキュリティ業務の両方を実行するだけの適切なスキルを備えていない。このような状況は、プロセス制御セキュリティのための特別なトレーニング・コースが欠如した状態では、改善されない。

4.3 グッド・プラクティスの原則

包括的な文書「Good Practice Guide Process Control and SCADA Security」（日本語版：「グッド・プラクティス・ガイド ー プロセス制御とSCADAセキュリティ」）に記載されているグッド・プラクティスの原則は次の通りである。

- IT 担当者の教育による、プロセス制御システムおよびその運用環境に対する正しい意識と理解の育成。これにより、プロセス制御システムのセキュリティと IT セキュリティとの間の相違を際立たせる。
- プロセス制御チーム内の IT セキュリティ・スキルの育成と、このようなチームに対する適切な IT サポート・サービスの提供。

4.4 グッド・プラクティスの手引き

プロセス制御と IT 運用環境の相違の大部分は、つまるところ、プロセス制御システムの安定性に置かれる基本の重要性に行き着く。このニーズが原動力となって、安定性、堅牢性、反復可能性を備えるプロセスとシステムを重視した保守的なリスク・トレーニングが発達する。

トレーニング体制を確立する際は、主要な人材のトレーニングを対象とし、組織の脆弱性についての理解度、グッド・プラクティスを共有する上でアクセス可能な情報およびリソース、承認済みの軽減手段について詳しく定める必要がある。

トレーニング計画の作成は、多くの点で意識プログラムの作成に類似している。そのため、意識プログラムの場合と同様の手法を使用することができる。トレーニング体制で有用なプログラムが提供されるようにするには、多数の事項を考慮する必要がある。

- トレーニング体制の目標
- 対象者の特定
- トレーニング・ニーズの特定
- トレーニング実施方法の特定

これらについては、以下にその詳細を説明する。

トレーニング体制の目標：トレーニング体制の目標は、すべての人をプロセス制御セキュリティの専門家に育てることではなく、人材がその職務にふさわしいスキルを確実に備えるようにすることである。プロセス制御担当者が IT セキュリティを学ぶのと同様に、IT チームも、プロセス制御システムについての理解を十分に深める必要がある。トレーニング体制作成の目標は、中核となる事項を理解させることにより、プロセス制御担当者や IT チームが以下の項目を実行できるようにすることにある。

- 共有「言語」による効果的な連絡

- 異なる運用環境の理解
- プロセス制御環境に適用可能な優れた IT セキュリティ手段の実装と遵守をプロセス制御担当者が実行できるようにするための十分なスキルの伝達
- IT 担当者がプロセス制御セキュリティ要件を効果的にサポートできるようにするための十分なスキルの伝達

対象者の特定：トレーニング体制の目標ならびに様々な対象者についての分析を基礎とすることで、対象者それぞれのトレーニング・ニーズを判断することが可能となる。対象者を特定することは、トレーニング要件を具体化して管理可能な計画を作成し、関係者へのトレーニングの実施順を決定するための判断材料を提供する上で役立つ。様々な対象者の中には、以下の人々が含まれる。

- プロセス制御セキュリティの擁護者
- 総合的な権限を有する者（SPA）
- プロセス制御、オートメーション、SCADA、テレメトリ技術者
- IT 担当者
- 対応チーム
- 作業チーム

トレーニング・ニーズ：必要とされるトレーニングのレベルは人によって異なる（例：SPA は基準や規制に注意する必要があるのに対し、ファイアウォールに関する規則を管理する者は、ファイアウォールを管理するだけの技術力を備えていることが必要とされる）。

ただし、以下のように、多くの人について考慮し得るトレーニング問題も多数存在する。

- **方針と基準** – 基準や法律に焦点を当てる。
- **手順** – 手順の詳細、ならびに、手順と方針や基準との関係についての詳細を説明する。
- **インシデント対応** – インシデント発生時になすべき事柄を説明する。
- **アーキテクチャ** – 様々なシステムに関する相互接続および設定の方法を網羅するものであり、技術的性格を持つものとなる。
- **ベンダー固有のトレーニング** – ベンダーのシステムに特有のセキュリティ・トレーニングを伴う。
- **詳細な技術的トレーニング** – 通常、IT セキュリティ全般を網羅する。また、業界で正式に承認された認定を受けるための要素となることがある。

トレーニング実施方法：プロセス制御セキュリティを特に意図して設けられたコースは比較的少ない。一般的に利用可能な IT セキュリティ・コースの中から適切なレベルの理解を得られるコースを見つけることは、至難の業であり、時間を要する。この点で、トレーニング・ニーズの分析が大いに役立つ。そして、しっかりと確立された専門組織の運営するコースを選択することにより、ある程度のトレーニン

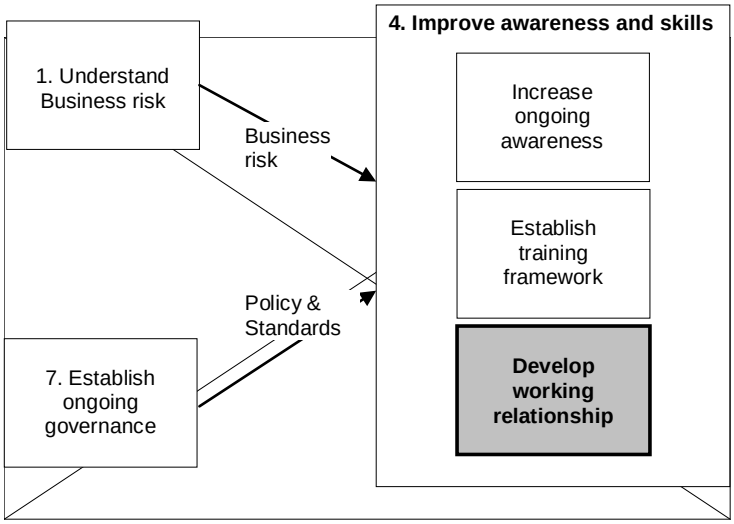
グ・ニーズは確実に満たされる。ただし、そうした専門組織で提供されるコースがすべてを網羅する完全なものとなっている可能性は低い。そのため、いくつかのトレーニング実施方法を複合的に利用することが必要となる。利用可能な方法の典型的なものとして、以下のものが挙げられる。

- **内部トレーニング** – 内部的に実施されるトレーニング。組織特有の問題を取り扱い、外部から得た知識を状況に当てはめて理解することができるため、最も効果的なトレーニングとなることが多い。ただし、内部トレーニングの計画と実施には、膨大な時間と貴重なリソースを費やすことが必要となる場合がある。
- **外部のトレーニング・コースと承認されたサード・パーティのトレーニング** – ベンダーまたはセキュリティ専門家のいずれかにより実施される。技術的性格が強く、各部署で発生する具体的な問題との関連付けが難しい場合も少なくない。様々な専門家団体がセキュリティ認定を実施している。そうした団体には、例えば、以下のようなものがある。
- セキュリティ保証 – 公認情報システム監査人（CISA：Certified Information Systems Auditor）– http://www.isaca.org/
- セキュリティ管理 – 公認情報セキュリティ・マネージャー（CISM：Certified Information Security Manager）– http://www.isaca.org/
- セキュリティ管理 – 公認情報システム・セキュリティ専門家（CISSP：Certified Information Systems Security Professional）– https://www.isc2.org/
- セキュリティ技術 – GIAC（Global Information Assurance Certification） – http://www.giac.org/
- コンピュータ・ベースのトレーニング、オンライン・トレーニング、ウェビナー（Webinar） – 比較的低いコストで個人やチームのトレーニングに利用可能。
- **カンファレンスやワークショップ** – カンファレンスへの出席は、プロセス制御セキュリティについて学ぶための良い方法である。また、カンファレンスを運営している業界団体の多くは、イベントの一環としてトレーニング・ワークショップを開催することが少なくない。
- **リフレッシャー・コース** – トレーニングは 1 回限りで終わるものではない。脅威や技術の変化に合わせて知識を常に最新の状態に保つとともに、スキル・レベルを維持するには、このようなコースの受講が必要となる。
- **マン・ツー・マン・トレーニング** – 重要関係者にとって有益な手段。人材の育成加速を可能とするとともに、メッセージが確実に理解されるようにする。
- **構造化されたトレーニング・コース** – 外部と内部のいずれでも実施可能。具体的なトレーニング問題や目標に重点を置く。
- **自己評価** – 自己評価は大切な手段である。これにより、組織においてプロセス制御セキュリティの維持や、緩和計画の成功度を図ることが可能となる。
- **総合的ワークショップ** – プロセス制御セキュリティの関係者を一堂に集めてセキュリティの改善についての議論を行うことにより、幅広い経験と知識をもって問題に取り組むことが可能となる。また、外部からの支援が必要なギャップを浮き彫りにすることができる。

米国の Department of Homeland Security は、ウェブベースのトレーニング・リソースを提供している（付録 A 参照）。

5.1 フレームワーク全体における本セクションの位置づけ

フレームワークのこの要素では、組織における協力関係の構築とプロセス制御セキュリティの定着により、組織内のプロセス制御セキュリティ・スキルの向上を図ることに焦点を当てている。この問題は、グッド・プラクティス・ガイド・フレームワークにおける「**事業リスクの理解**」と「**継続管理の確立**」の 2 つの要素の上に成り立っている。さらに、本書に含まれる「**継続的意識の向上**」と「**トレーニング体制の確立**」の要素もその基礎となっている。



1. Understand Business risk	1. 事業リスクの理解
7. Establish ongoing governance	7. 継続管理の確立
Business risk	事業リスク
Policy & Standards	方針および基準
4. Improve awareness and skills	4. 意識とスキルの改善
Increase ongoing awareness	継続的意識の向上
Establish training framework	トレーニング体制の確立
Develop working relationship	協力関係の構築

図5 – フレームワーク内における「協力関係の構築」の位置づけ

5.2 論理的根拠

プロセス制御の世界と IT の世界との間の距離が縮まるにつれ、この 2 つの世界が密接に協力し合うことが必要となる。これにより、両方の環境を効果的な方法で保護し、より優れた統合ソリューションの提供、スタッフの利用率改善、コスト削減を実現することが可能となる。

5.3 グッド・プラクティスの原則

包括的な文書「Good Practice Guide Process Control and SCADA Security」（日本語版：「グッド・プラクティス・ガイド ー プロセス制御とSCADAセキュリティ」）に記載されているグッド・プラクティスの原則は次の通りである。

- IT セキュリティ・チームとプロセス制御チームの連携を確立することにより、協力関係の確立、スキルの共有、知識の伝達促進を実現する。

5.4 グッド・プラクティスの手引き

従来、プロセス制御と IT は 2 つの別々な分野であった。近年、技術が収束し、2 つの環境の接続が求められる傾向にある。これにより明らかとなったのが、IT 部門とプロセス制御部門との関係強化の必要性である。互いの環境について知ることは、いずれのチームにとっても重要性を持つ。これにより、良好な協力関係を発展させ、知識や技能の共有を成功させることが可能となる。

プロセス制御担当者は、IT のアプリケーション、インフラストラクチャ、セキュリティに関するスキルを身につけることができる。同様に、IT 担当者は、業務上重要な変更管理やテスト・プラクティスを始めとする重要なプロセス制御スキルを伸ばすことができる。

相互関係を発展させることにより、双方に共通の多数のメリットが実現される。

- 知識の伝達拡大
- 豊富なセキュリティ・スキル・ベースへのアクセス
- 豊富なプロセス・スキル・ベースへのアクセス
- セキュリティ保護についてのより良い理解
- ベスト・プラクティス共有の機会
- 低コストのセキュリティ・ソリューション
- 効率性の高い作業プラクティス
- 迅速なプロジェクト実施

以下に挙げるいくつかの簡単な行動は、良好な協力関係を強化する上で役に立つ。

- プロセス制御セキュリティ対応チーム（PCSRT）に IT の代表者を送り込むこと
- 定期ミーティングを実施してセキュリティの開発と進捗状況について話し合うこと

- プロセス制御変更会議に IT 代表者を招聘すること
- 配信リストを拡大して適切な IT 担当者の連絡先を含めること
- 指導計画の作成
- 仕事の共有 – IT スタッフとプロセス制御スタッフのクロス・トレーニングを行い、互いの任務を遂行し合うこと
- プロジェクト・チームの合併

多くの組織では、IT 機能が様々なサービスの提供を組織に対して行っている。緊密な関係を築くことにより、プロセス制御環境において直接（変更は最小限）使用できる IT ソリューションや、プロセス制御環境の設定を変更することで使用できる IT ソリューションを特定することが可能となる。IT により供給される可能性がある優れたサービスには、例えば以下のようなものが含まれる。

- ウイルス対策
- ファイアウォールの管理および監視
- ネットワーク・システムの監視
- リモート・アクセスの管理
- インシデントや警告に対する対応
- セキュリティに関するトレーニングと意識
- 継続的保証の管理

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 **3.4.1**

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

セクション **3.4.3**

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

セクション **4.4**

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

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

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

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

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