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 7. 継続した統制の確立

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 7. ESTABLISH ONGOING GOVERNANCE" 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。

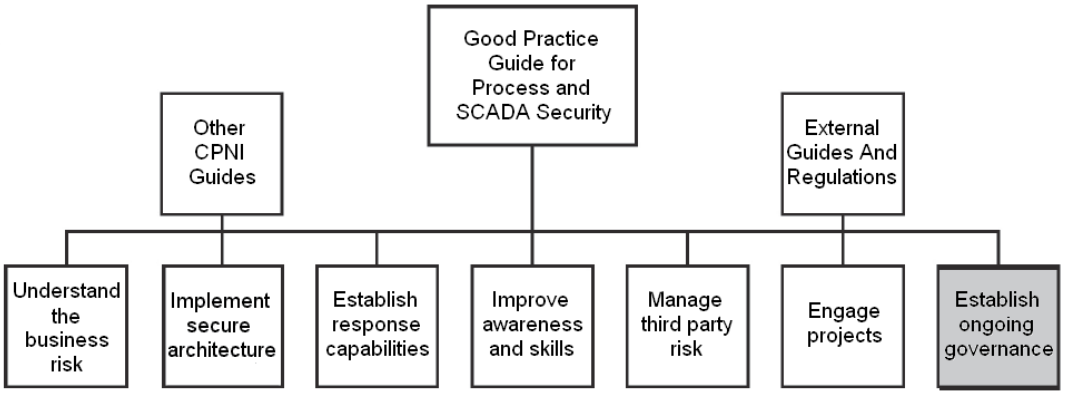
1.3 プロセス制御セキュリティ・フレームワーク

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。

---

[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。

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

「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「継続した統制の確立」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。

本ガイドはポリシーや標準、あるいは手順には言及していない。

1.5 想定読者

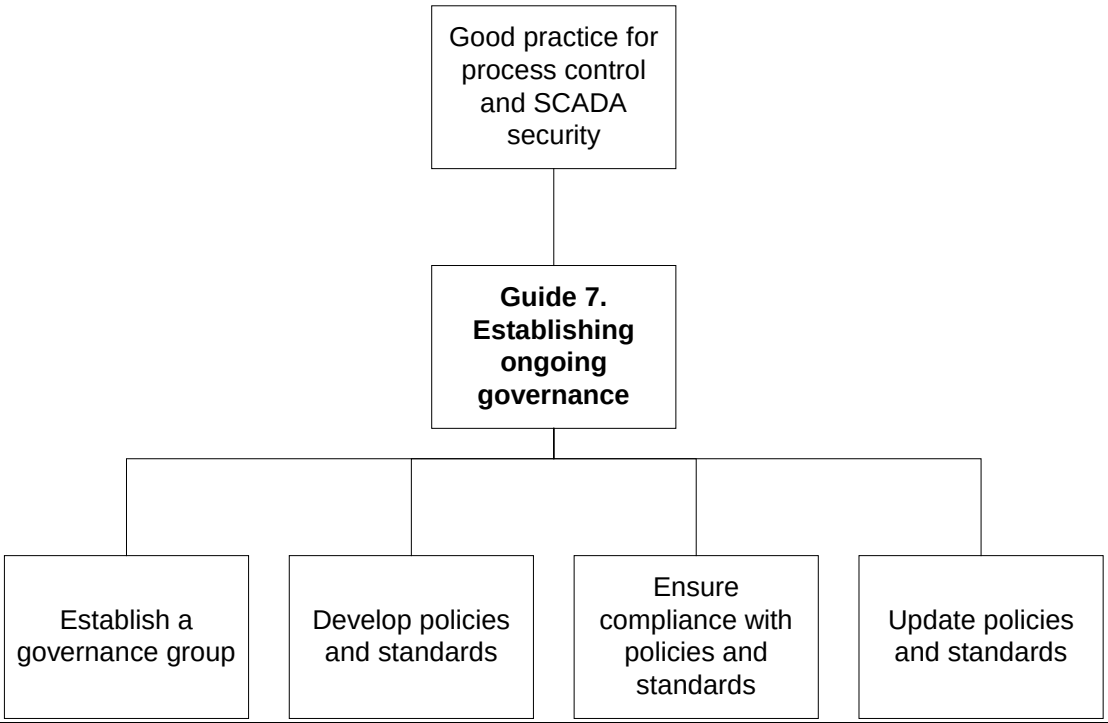
本ガイドは、プロセス制御のセキュリティ、SCADA、産業オートメーション・システムに従事する、以下のような人たちを対象としている。

- 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. 継続した統制の確立についての要約

プロセス制御システムのセキュリティ管理の正式な統制により、首尾一貫した適切な手法が組織全体で行われることを確実にする。そのような統制なしでは、プロセス制御システムの防護はその場限りかまたは不十分であり、組織をリスクに曝す。効果的な統制フレームワークは、明確な役割と責任、プロセス制御セキュリティのリスク管理についての最新のポリシーおよび標準を明確にし、このポリシーおよび標準が守られることを保証する。

統制: *組織を指揮監督する体制*



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 7. Establishing ongoing governance	ガイド 7. 継続した統制の確立
Establish a governance group	統制グループの確立
Develop policies and standards	ポリシーおよび標準の作成
Ensure compliance with policies and standards	ポリシーおよび標準遵守の保証
Update policies and standards	ポリシーおよび標準の更新

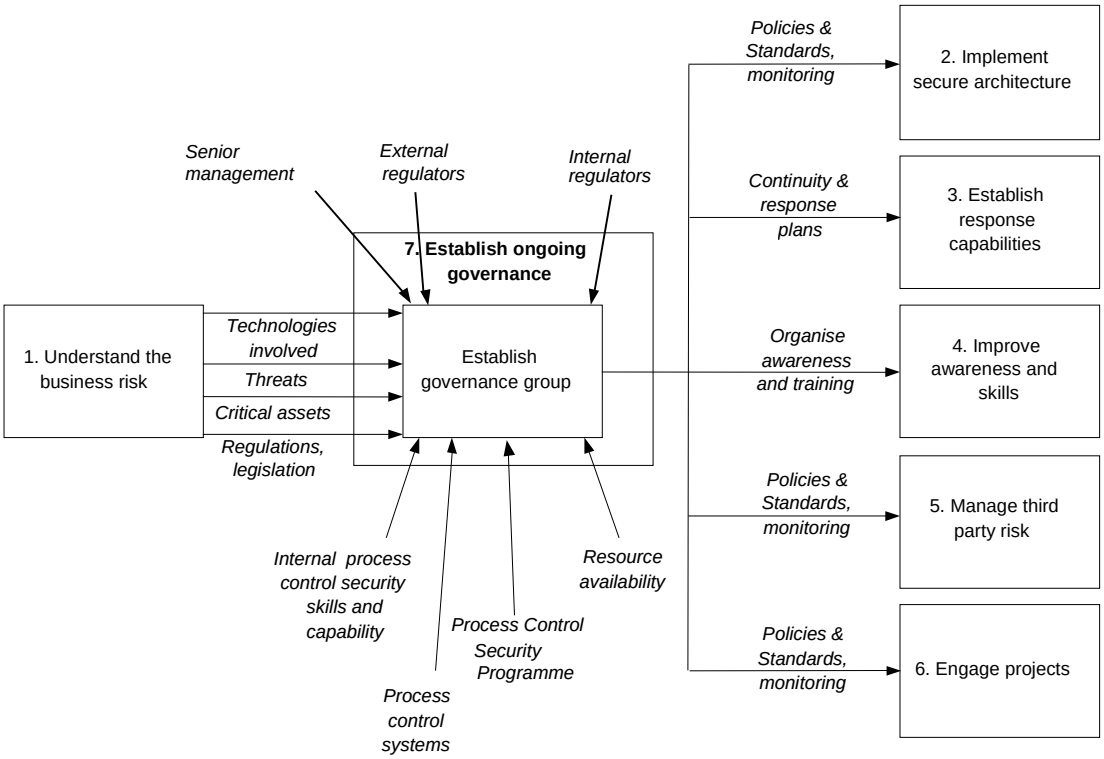
図 2 – 継続した統制の確立の文書構造

これらの各構成要素について、以下のセクションで詳細を述べる。

3. 統制グループの確立

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

統制グループ（時には委員会や評議会とも呼ぶ）は、フレームワークの 7 要素のそれぞれを統制することによって、中枢の役割を果たす。統制グループは、プロセス制御セキュリティ・リスクおよび影響に責任を持ち、それ故、プロセス制御セキュリティ・フレームワークの全テーマに係わる。下図は、統制グループに最も適切なメンバーを決定する際に役に立つ簡単な情報の流れを示すとともに、メンバーを選定するときの主要考慮事項を示す。



1.Understand the business risk	1.事業リスクの理解
2. Implement secure architecture	2.セキュア・アーキテクチャの実装
3. Establish response capabilities	3.対応能力の確立
4. Improve awareness and skills	4.意識とスキルの改善
5. Manage third party risk	5.サード・パーティ・リスクの管理
6. Engage projects	6.プロジェクトへの参画
7. Establish ongoing governance	7.継続した統制の確立
Establish governance group	統制グループの確立
Senior management	経営者

Technologies involved	関連技術
Threats	脅威
Critical assets	重要資産
Regulations, legislation	規制、法律
External regulators	外部規制当局
Internal regulators	内部監査委員
Internal process control security skills and capability	内部プロセス制御セキュリティ・スキルおよび能力
Process control systems	プロセス制御システム
Process Control Security Programme	プロセス制御セキュリティ・プログラム
Resource availability	リソースの可用性
Policies & Standards, monitoring	ポリシーおよび標準、監視
Continuity & response plans	事業継続・対応計画
Organise awareness and training	意識向上と訓練の計画

図 3 – フレームワーク内における「統制グループの確立」の位置づけ

3.2 論理的根拠

プロセス制御セキュリティ・リスクを効果的かつ包括的に確実に管理するには、統制グループをはっきり規定し、その役割と責任を明確にすることが不可欠である。どの組織にも収まるような統制グループを規定するのは不可能であるが、グループのメンバーは、意思決定者と適切な専門分野の技術専門家から混成されるべきである。このグループは、組織の既存の統制および報告構造に収まる必要があり、戦略および運用の両レベルで組織のプロセス制御を統制する権限を持つ必要がある。

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。

- 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。
- 法令の要件がプロセス制御セキュリティに与える影響を特定する。
- プロセス制御システムのセキュリティの扱いを事業や運用の必要性に沿ったものにする。
- 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。

- プロセス制御のセキュリティ・リスクに対する責任者を任命する。組織の規模により、これは 1 人のこともあり、最高責任部者に報告するいくつかの地域の責任者であることもある。

3.4 グッド・プラクティスの手引き

組織がどのような統制手法を好むかにかかわらず、最低でも下記の機能を実現する必要がある。

- 事業 – 事業が何を必要としているかの全体像を提供する。1 人以上の上級管理者が適任かもしれない。
- プロセス制御 – プロセス制御を代表し、性能、重要資産の特定、資産が曝される既存の脅威の情報を提供する。
- セキュリティ – 知識および物理セキュリティの専門技術、経験、統合に関する展望を提供する。
- エンジニアリング – エンジニアリングがプロセス制御とは独立した機能の場合、実践的な運用／実装手引きを確実にするための入力が必要なこともある。
- 安全・健康・環境 – 安全、健康、環境の事項に沿い準拠することを確実にする主要な手引きである。

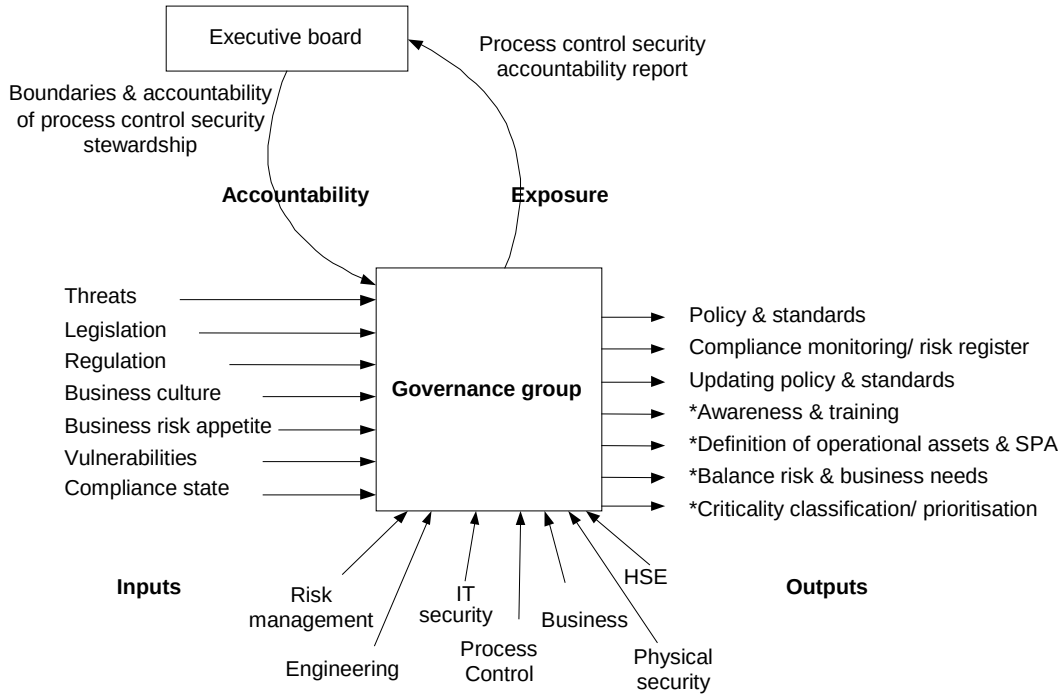
プロセス制御セキュリティ統制グループの上記の各機能は、事業のプロセス制御セキュリティ要求をバランスよく満たすために不可欠である。この他の示すべき機能には、事業／運用リスク管理者、事業継続および緊急対策の立案、IT インフラストラクチャ、通信および物理的セキュリティがある。それらは、中核の役割に含めることもできるが、事業によっては、役割を独立に示すこともできる。

これらの役割にどのように責任を配分するかについては、組織の文化、利用できるリソース、選択した統制構造、地理的広がり等に依存したものになるだろう。プロセス制御セキュリティの統制に含まれうる典型的な責務を以下に示す。

- 事業の必要性と緩和措置のコストをバランスさせる。
- プロセス制御セキュリティの中に安全・健康・環境要件を組み込む。
- 法的要件を考慮する。
- プロセス制御セキュリティの人材との関係を考慮する。
- プロセス制御の意識向上および伝達計画を管理する。
- プロセス制御セキュリティ状況を監視し、取締役会に報告する。
- 設計の専門家を参画させる。
- 運用の範囲と境界を設定する。
- 責任を定める。
- プロセス制御プロジェクトの登録簿を維持する（プロジェクト情報への不正アクセスを防ぐ適切なセキュリティの保証）。

- プロセス制御セキュリティ関連リスク登録簿に関する企業リスク登録簿の所有権を維持する。
- プロセス制御セキュリティ戦略（短期および長期計画）を所有し維持する。
- プロセス制御セキュリティ・プログラムを所有する。

執行委員会は、プロセス制御セキュリティ統制グループにその責任を、組織、その規模、文化、既存の報告構造等を考慮して、直接またはいくつかの報告レベルを経由して委任する。プロセス制御に非常に依存する組織またはプロセス制御システムが損なわれた場合に重大な影響を受ける組織は、執行委員会に密接に関連する統制グループを持つであろう。統制グループは、委任された責務に対して、組織の資産が曝される脅威のレベルと、インシデントへの対策プランを明確にしておく必要がある。事業への重要な影響が理解され、適切なレベルで検討されるようにするため、プロセス制御インシデントからの潜在的な影響の大きさが明確に伝達されることを確実にするために、強力な報告チャネルが不可欠である。統制グループが、自分達に委任された責任の境界を明確に理解することも非常に重要である。下図に統制グループの考慮事項の概要を示す。



Key functions represented

Executive board	執行委員会
Boundaries & accountability of process control security stewardship	プロセス制御セキュリティ執事職の境界と責任
Process control security accountability report	プロセス制御セキュリティ責任報告
Accountability	責任
Exposure	提示
Threats	脅威
Legislation	法律
Regulation	規制
Business culture	事業文化
Business risk appetite	事業リスク許容度
Vulnerabilities	脆弱性
Compliance state	遵守状況
Governance group	統制グループ
Policy & standards	ポリシーおよび標準
Compliance monitoring/risk register	遵守の監視／リスクの登録

Updating policy & standards	ポリシーおよび標準の更新
*Awareness & training	*意識向上および訓練
*Definition of operational assets & SPA	*運用資産と最高責任の所在の定義
*Balance risk & business needs	*リスクと事業の必要性のバランス
*Criticality classification/prioritisation	*重要性分類／優先順位付け
Inputs	入力
Risk management	リスク管理
Engineering	エンジニアリング
IT security	IT セキュリティ
Process control	プロセス制御
Business	事業
Physical security	物理的セキュリティ
HSE	安全・健康・環境
Outputs	出力
Key functions represented	表明される主要機能

* 他のフレームワーク要素で詳細に扱われているテーマを示す。

図 4 – 統制グループの機能

通常、プロセス制御統制グループの役割は、必要なときに割り当てられる。統制グループの職務でどのくらいの時間を費やすかは、リスクの大きさおよびどのような既存構造が既にあるかにかかっている。統制グループの任務は以下の通りである。

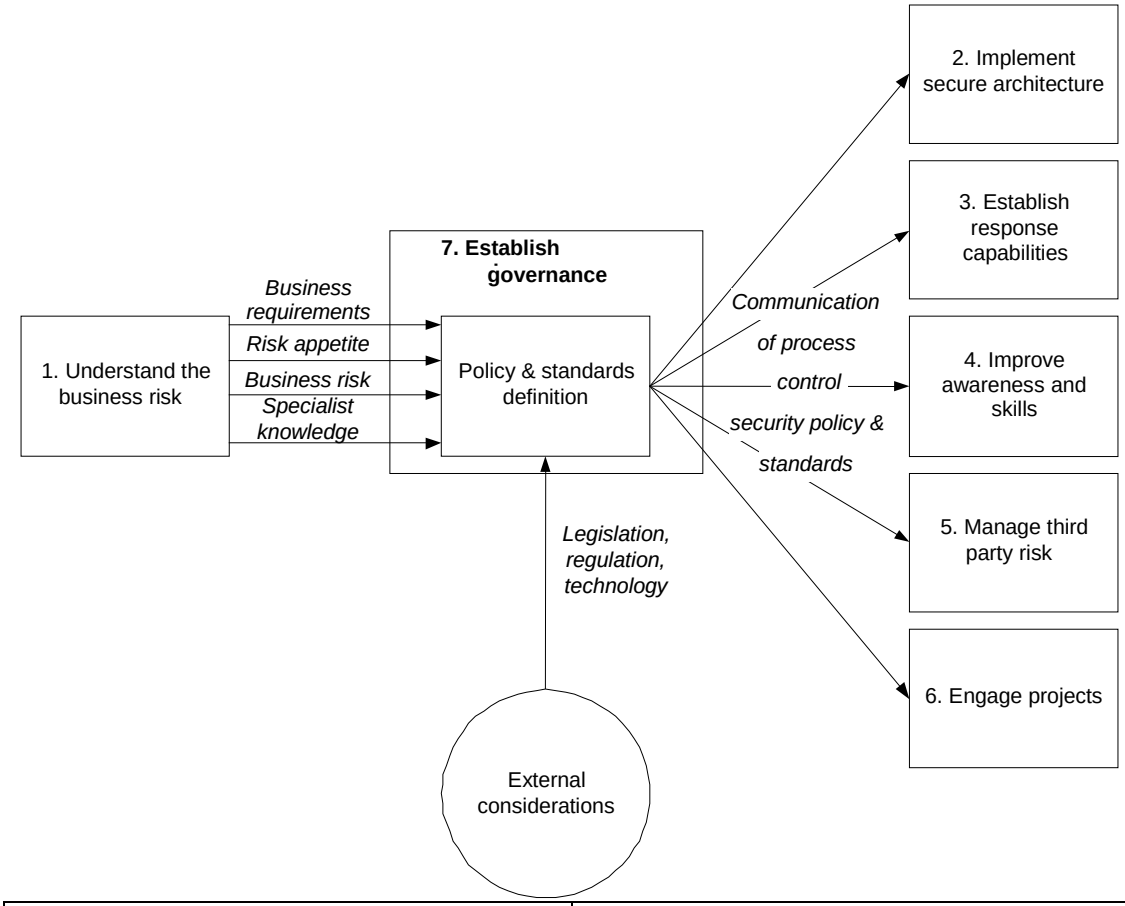
戦略 – プロセス制御セキュリティ・ポリシーの設定、プロセス制御セキュリティ・プログラムの開始。

戦術 – プロセス制御セキュリティ・プログラムの実装、プロセス制御セキュリティの認識向上および訓練についての助言、ポリシーおよび標準遵守の監視、予算の作成と承認。

作戦 - 警報とインシデントを監視、分析、対応するプロセス制御セキュリティ対応チームの編成と連絡、リスク脅威の監視。

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

プロセス制御セキュリティのポリシーおよび標準を作成することは、フレームワーク要素の「事業リスクの理解」と密接に関係している。組織ごとに特定された事業リスクの多くが、組織内のプロセス制御セキュリティに関する適切なポリシーの設定に直接使用できる。ポリシー決定のプロセスは、事業リスクに基づくものであり、通常は経営者レベルで行われる。事業リスクと組織のリスク許容度を考慮後、経営者は、有効なポリシーを決めるため、制御チーム、IT セキュリティ、安全健康環境、事業から情報を求める。どのような外部規制や法律を考慮する必要があるか、どの軽減対策や技術が現在利用可能かを考慮することも重要である。



1.Understand the business risk	1.事業リスクの理解
2. Implement secure architecture	2.セキュア・アーキテクチャの実装
3. Establish response capabilities	3.対応能力の確立
4. Improve awareness and skills	4.意識とスキルの改善
5. Manage third party risk	5.サード・パーティ・リスクの管理
6. Engage projects	6.プロジェクトへの参画

7. Establish ongoing governance	7.継続した統制の確立
Policy & standards definition	ポリシーおよび標準の定義
Business requirements	事業要件
Risk appetite	リスク許容度
Business risk	事業リスク
Specialist knowledge	専門知識
Communication of process control	プロセス制御の伝達
security policy & standards	セキュリティポリシーおよび標準
Legislation, regulation, technology	法律、規制、技術
External considerations	外部考慮事項

図 5 – フレームワーク内における「ポリシーおよび標準の作成」の位置づけ

残りのプロセス制御セキュリティ・フレームワーク要素は、組織のプロセス制御セキュリティポリシーおよび標準を参照し使用する。ごく大まかな概観を以下に述べる。

4.2 論理的根拠

プロセス制御セキュリティポリシーは、組織のリスク許容度を、措置が取れる境界に翻訳したものである。そして、その標準は、プロセス制御システム構成要素の作成、維持、除去を規定する反復可能なビルディング・ブロックである。ポリシーは組織の境界を規定し、標準は決められたポリシーの望ましい品質を達成するための首尾一貫した組織としての解釈を示したものである。

例：ポリシーは、大まかではあるが、どのトラフィックが許可されるかを記述することもある。例えば、「オフィス・システムから発信されたトラフィックはプロセス制御システムに入れることはできない」

ポリシーおよび標準は、要求されるプロセス制御セキュリティ防護のレベルおよびこれがどのように達成されるべきかを伝達するためのメカニズムである。

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 ― 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とおりである。

- プロセス制御システム・セキュリティに関する正式な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。

- ポリシーおよび標準は、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することを確実にする。
- 関連する当事者全員がポリシーおよび標準に合意するようにする。

4.4 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ポリシーおよび標準の作成は、まったく独自のものとしてもよいし、IT セキュリティ標準やエンジニアリング標準と組み合わせてもよい。どちらを選ぶにもいくつかの理由があるが、明確にされた事業要件に合わせてプロセス制御システムを防護するのに必要な品質と詳細を正確に表現する限り、どちらも同等にうまく機能する。

以下に該当する場合、IT システムとは独立したポリシーおよび標準のセットを作成することになるだろう。

- プロセス制御システムが事業に決定的に重要であるかまたは安全に影響を及ぼす。
- 十分なプロセス制御リソース能力がある。
- 現行のセキュリティポリシーおよび標準はプロセス制御システムを含めるには十分でない。
- 他の文化的や歴史的な理由がある。

以下に該当する場合、プロセス制御セキュリティポリシーおよび標準を既存のセキュリティポリシーおよび標準と組み合わせるか、またはプロセス制御セキュリティ・セクションをこれらの標準文書に加えるのが適切であろう。

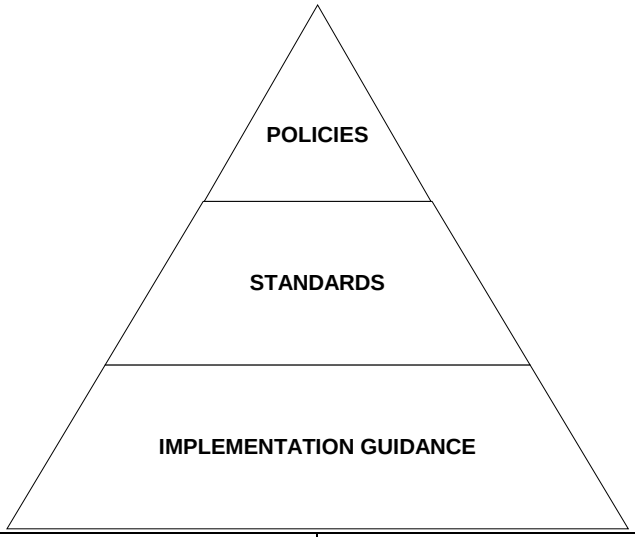
- プロセス制御システムは事業にとって非常に重要であり、主要な事業プロセスと密接に一体化している。
- セキュリティ、プロセス制御、IT サポートの間で係わりが深い。
- 企業のセキュリティ管理と、安全なプロセス制御システムに要求される管理にかなり合致する。
- プロセス制御リソースおよび能力が限られている。

ポリシーおよび標準を組み合わせる場合、明確な所有者、品質の合意、セキュリティ原則、その他多くの事項があいまいなところがなく規定され、IT とプロセス制御の両セキュリティ目標が効果的に達成されるように注意しなければならない。IT セキュリティとプロセス制御セキュリティの運用要件は、バージョンの更新などのいくつかの基本的な点で異なっているので、組み合わせることは簡単なプロセスでないことが多い。

専門のアーキテクチャおよび標準ワーキング・グループを編成することもできる。このグループは統制委員会に報告し、IT とプロセス制御の両グループがポリシーおよび標準を定めるのに参加することを確実にする。

図 6 は、ポリシー、標準、実施要項の間での文書の詳細度と数の違いを示したものである。三角形の上に上がるほど、詳細でなくなり、文書数が少なくなり、変更が

少なくなる。三角形の下に下がるとその逆で、実施要項は最も詳細で、定期的に更新される必要性が高い。



POLICIES	ポリシー
STANDARDS	標準
IMPLEMENTATION GUIDANCE	実施要項

図 6 ポリシー、標準、実施要項の関係

4.4.1 ポリシー

ポリシーは、組織による明確な目標を示す具体的な原則または行動指針の宣言と、首尾一貫した意思決定およびリソース配分の根拠となる価値観または意図の宣言と、現在および将来の決定を導き定める明確な方法または手順、を示す必要がある。ポリシーの典型的な特徴は、以下の通りである。

- 広範囲に適用できる。
- まれにしか変更されない。
- 大抵幅広い用語で表現される。
- 技術文書ではない。
- 「何を」および／または「何故」の宣言である。
- 主要な運用上の問題を扱う。

プロセス制御セキュリティポリシーは大抵、必要な事業の内容や技術に関する基本的な「フレームワーク」となる大枠を示す文書である。大半の場合に、関連する標準のないポリシーだけでは、何を行う必要があるかを伝達するには大まか過ぎるであろう。ポリシー目標を必要な品質レベルで実施するために必要な情報を示すのが、標準（および実施要項である）である。

ポリシーの文書に含むべき最低限の項目を以下に示す。

- 趣旨のポリシー宣言 – 「この品質で必要な制御」
- ポリシーは何にまたは誰に適用されるか – 「ポリシーの範囲または境界」
- 誰がポリシーを所有するか – 「誰が発表し更新するか」
- 何がポリシーの更新のきっかけとなるか – 「ポリシーはいつ見直すべきか」
- 例外の基準とプロセス – 「ポリシーが適用されないのはどのような場合か」

ポリシー作成時に、既存の事業ポリシーおよび標準などいくつかの要因とプロセス制御セキュリティポリシーの関係も無視できない。事業、運用、財務へ与える影響を考慮せずに、プロセス制御セキュリティポリシーを書くことはまったく容易である。しかし、この方法で書かれた文書は、事業により承認され受入れられることはありそうもないので、貴重な努力が無駄になるだろう。

プロセス制御セキュリティポリシーを書くとき、以下の標準に合っているか絶えずチェックすることが重要である。

- 事業戦略との整合
- IT 戦略およびポリシーとの整合
- 安全・健康・環境ポリシーとの整合
- 組織の物理的セキュリティポリシーとの整合
- 既存／確立した用語の一貫した使用
- 他のポリシーとの、そのレベルおよび対象の一貫性

統制グループはプロセス制御セキュリティポリシーを設定し、組織が必要とするレベルで承認を得る責任がある。

4.4.2 標準

ポリシーに対する標準の特徴は以下の通りである。

- 適用範囲が狭い。
- 変更が多い。
- 大抵詳細に述べられている。
- 技術詳細を含んでもよい。
- 「どのように」「いつ」時には「誰が」の宣言を含む。
- 関連プロセスを記述する。

プロセス制御セキュリティ標準の文書は、組織全体で従うべき共通の手法を示す。そして、一般に仕事の複雑さを減少し周知の品質で、迅速な引き渡しを可能にする。標準は、特定の組織向けに合わせた専門知識を共有することにより重複を減らす一

貫した反復可能な手法を示す。良質の標準を作成することにより、仕事を管理可能な塊に分解し、仕事および緩和されるリスクについての、理解を容易にするだろう。

標準の草案は、専門の内部作成グループまたはサード・パーティの支援で、作られるであろう。標準は、ポリシー文書に述べられた品質および能力を満たすために必要な境界線を定める。標準は、関連する法律および規制（安全衛生、英国貿易産業省、環境）、既存の産業標準、利用可能技術、将来の事業または産業の要件により強く影響される。

標準に何を含めるべきかを考慮するとき、標準文書に期待される最小限の項目は次の通りである。

- 標準が適用されるポリシーの項目– 「ポリシーの中のどれ」
- 意図する読者 – 「詳細のレベル」
- 標準の定義と適用 – 「それは何であり、人、プロセス、技術の面でどのように適用されるか」
- 標準は何にまたは誰に適用されるか – 「標準の範囲または境界」
- 誰が標準を所有するか – 「誰が発表し更新するか」
- 標準の更新– 「標準はいつ見直すべきか」
- 例外の基準– 「標準を適用しないのはどのような場合か」

標準の詳細は頻繁に変更されるため、統制グループレベルだけで承認するのが普通である。このことは、プロセスが厳格さで劣るということではなく、詳細を理解し審査できるのは限られたグループであることを意味している。

4.4.3 実施要項

標準を補助するためには、通常「実施要項」と呼ばれる第 3 のグループの文書がよく利用される。標準にいくつかの適用可能な選択肢がある部分では、この実施要項が詳細を加えることにより、標準自体を複雑にし過ぎることなく、標準を適切に翻訳できるようにする。実施要項は一般に全文書の中で最も詳細であり、必要な「標準」に合わせた特定のファイアウォールの設定方法など、個別の技術や要素にだけ焦点を合わせている。

4.4.4 標準と要項の主要情報源

プロセス制御セキュリティ標準の作成に関して、ベンダー、政府機関、産業規制当局からいくつかの役に立つ情報が得られる。これらの要項の多くは、必要な品質期待値を定めるのに役立つだろう。標準と要項の主要情報源のいくつかを以下に挙げる。

- CPNI - Centre for the Protection of National Infrastructure, (www.cpni.gov.uk)
- CPNI Best Practice Guide on Firewall Deployment for SCADA and Process Control Networks

- CPNI Good Practice Guide Outsourcing: Security Governance Framework for IT Managed Service Provision
- CPNI Good Practice Guide Patch Management
- CPNI Best Practice Guide Commercially Available Penetration Testing
- CPNI guide on Personnel Security Measures
- ISO 17799 － International Code of practice for information security management
- ISO 27001 (旧 BS 7799-2) － International Specification for Information Security Management
- PCSRF － Process Control Security Requirements Forum
- IEEE － Institution of Electrical and Electronics Engineers
- IEC － International Electrotechnical Commission
- 業界 － API、NERC、AGA、OLF、CIGRE などの組織が提供する個別のガイド
- ベンダー固有のガイド
- Recommended Practices Guide for Securing ZigBee Wireless Networks in Process Control System Environments
- Securing WLANs using 802,11i
- Using Operational Security (OPSEC) to support a Cyber Security Culture in Control Systems Environments
- Cyber Security Procurement Language for Control Systems
- NERC Critical Infrastructure Protection (CIP)
- DHS Catalog of Control System Security Requirements
- NIST Guide to Industrial Control (ICS) Systems
- ISA SP99, Manufacturing and Control Systems Security

ポリシー、標準、実施要項を書くとき、上記の参照箇所を出発点として、事業の要求条件、特徴、文化に基づき、組織固有の文書とすべきである。

主要な目的は、重要な要件を捉えることである。特定のサプライヤまたはハードウエア／ソフトウエアに基づいた希望リストを書く罠に陥るのを避けること。

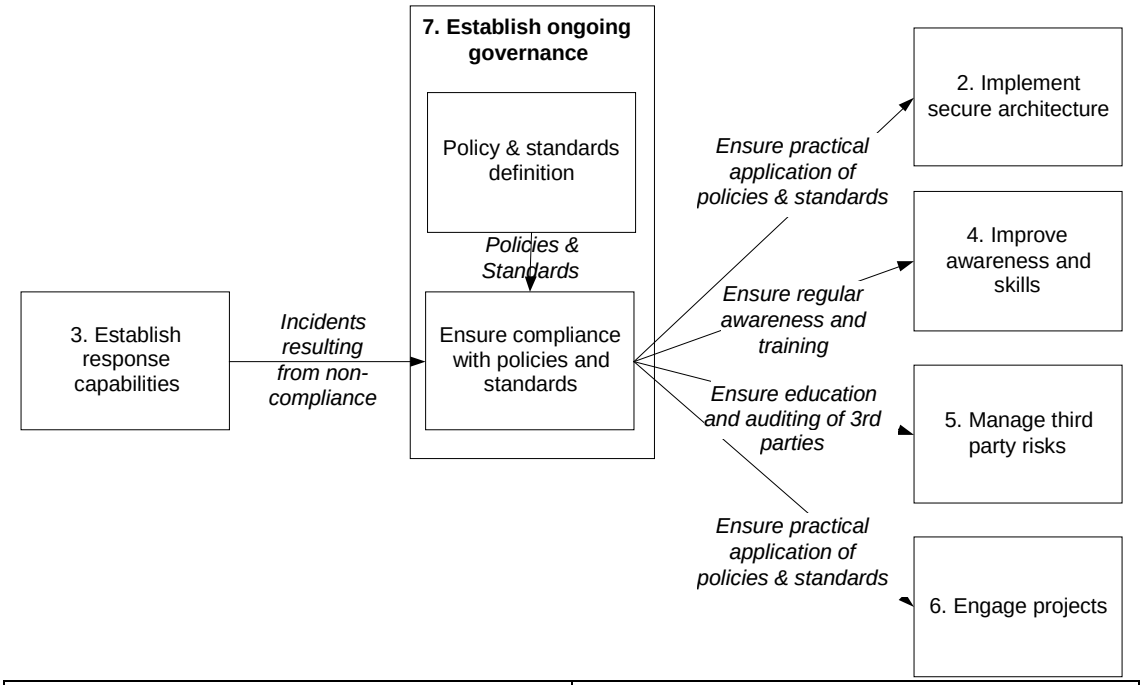
産業界のベスト・プラクティスを自社の環境に合わせることなく真似して、組織全体に適用しても、プロセス制御セキュリティを改善しないどころか、運用を妨げ、貴重な時間とリソースを浪費しかねない。しかし、グッド・プラクティスの原則を自分の組織の特定された脅威に適用すれば、組織のリスク許容度のレベルに応じて、問題を緩和するのに役立つだろう。

特定のリスク許容度および脅威に取り組むために書かれる良質の文書は、実施、監視、更新、遵守が容易で、汎用のベスト・プラクティスを真似するよりはるかに優れている。

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

効果的に統制するには、適切なポリシーおよび標準が存在するだけでなく、遵守を監視することも必要である。

遵守プロセスは、ポリシーおよび標準が抱える困難を発見するための非常に重要なフィード・バック・ループを提供し、既存の手引きが望ましい目標を達成しない箇所の更新または修正のきっかけになる。



2. Implement secure architecture	2.セキュア・アーキテクチャの実装
3. Establish response capabilities	3.対応能力の確立
4. Improve awareness and skills	4.意識とスキルの改善
5. Manage third party risk	5.サード・パーティ・リスクの管理
6. Engage projects	6.プロジェクトへの参画
7. Establish ongoing governance	7.継続した統制の確立
Policy & standards definition	ポリシーおよび標準の定義
Policies & standards	ポリシーおよび標準
Ensure compliance with policies and standards	ポリシーおよび標準の遵守
Incidents resulting from non-compliance	違反から生ずるインシデント

Ensure practical application of Policies & Standards	ポリシーおよび標準の実践的適用
Ensure regular awareness and training	定期的意識向上と訓練
Ensure education and auditing of 3rd parties	サード・パーティの教育および監査

図 7 – フレームワーク内における「ポリシーおよび標準の遵守の保証」の位置づけ

5.2 論理的根拠

ポリシーおよび標準の遵守を確実にする活動は、正しい品質要件に対し適切な行動が取られるのを保証にするのに不可欠であり、統制テーマを確立するための主要な機能である。ポリシーおよび標準の遵守は、以下のことをもたらす。

- プロセス制御システムが事業リスクに対して合意したレベルで防護されるのを保証する。
- 業務の無駄な重複を避け、一貫したソリューションが組織全体で利用されるのを確実にする。

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 ― 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。

- 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。

5.4 グッド・プラクティスの手引き

ポリシーおよび標準の遵守を確実にする方法はいくつかある。これらの方法はやはり、組織の文化、能力、既存のプロジェクトに合わせるべきである。どれは遵守され、どれは遵守されていないかの詳細な情報が欲しい組織もあるし、違反が記録された箇所を示すだけの例外報告を好む組織もある。遵守の仕事は、3 つの主要決定事項に分解できる。

- 何の情報をどのくらい詳細にいつ必要か。
- 情報は誰によりどのように収集されるか、すなわちどの遵守プロセスが使用されるか。
- 違反は事業にどのような影響を及ぼすか。

5.4.1 何の情報をどのくらい詳細にいつ必要か

最初の決定事項のために尋ねるべき質問は、「どのレベルの情報が意思決定に価値を持つ十分な詳細を提供すると同時に管理し易いか」である。

これは組織により変わるだろうが、情報が多過ぎるのは足りないのと同じくらい悪いことがあることを覚えておく価値がある。提出する情報が読まれていないと感じると、品質は直ちに低下するだろう。ポリシーや標準の問題を警告したいのだが、そうする場がない場合、自分自身の非公式のガイドを書き、会社の文書には口先だけで同意する可能性がある。

遵守報告で求められるべき主要情報は以下の通りである。

- 報告の結果を実施する責任者を特定する管理
- 遵守に関する責任者の所在
- ポリシーや標準からの意義のある逸脱
- 事業への影響の見込み
- 計画された解決の日付
- 関連する周囲状況（例：違反の理由）

5.4.2 情報は誰によりどのように収集されるか

これは、遵守を確実にする能力と利用可能性に関するものであり、いくつかの方法がある。遵守点検の量、品質、頻度次第で、組織は自己評価、同僚による審査、内部監査部門を使用する等、社内からリソースを選ぶことができる。この手法には、問題や長所の所有意識を増すなど多くの利点があるが、内部リソースである専門家の貴重な時間を取ることになる。別の手法は、プロセス制御セキュリティを専門にするサード・パーティに外注することである。これはより客観的な結果が得られ、問題が隠される可能性が少ないが、コストは余分にかかる。それに、セキュリティ情報がサード・パーティに伝えられ、潜在的な脆弱性が生じる問題もあるので、外部リソースの使用は慎重に考慮すべきである。外郭団体が係わる場合、違反は規制上の影響がある可能性があるので、違反を特定する必要がある。

外部による遵守監視は正式な監査である必要はなく、より非公式な反復型の方法でもよい。

選択肢の要約

- 自己評価 – 自部門により実施される評価
- 同僚による審査 – 関連部門による内部審査
- 内部監査 – 組織の内部監査組織により実施される監査
- 外部監査 – 外部組織により実施される監査
- 補助者付き自己評価 – プロセス制御セキュリティ専門家が補助して、自部門により行われる評価
- 外部ヘルスチェック – 外部組織により行われる産業特有の主要脆弱性の審査

監査に関する詳細なガイドについては、NIST の『Guide to Industrial Control Systems (ICS) Security』（付録 A 参照）に記載されている。

5.4.3 違反は事業にどのような影響を及ぼすか

最後の主要な決定は、組織のポリシーまたは標準からの著しい逸脱が報告された場合、もしあるとすればどんな追加の事業リスクがあるかである。違反についての十分な情報を得、詳細な情報を基に潜在的な脅威について判断し、このフレームワークの「事業リスクの理解」にフィードバックすることが重要である。

- このリスクが現実になる可能性はどのくらいか?
- どのくらい速く事業に影響を及ぼすか?
- どのような緩和措置が取られているかまたは計画されているか?

推奨されるプロセス制御セキュリティ遵守の最低限の監視：遵守に関して評価できる領域は多いが、多くのことと同様に、事実と状況依存との間のバランスを取る必要がある。いつも注意深く監視されるべき 3 つの領域は、隔離、システム監視および検知、パッチの適用である。大部分の組織にとって、これらの領域が事業に最大の脅威を与える。それ故、これらの領域に関するポリシーおよび標準があるべきであり、組織内で遵守を監視するために、以下のことに特別の注意を払うべきである。

- **隔離** – プロセス制御ネットワークをオフィス・ネットワークと外界から適切に隔離しているか。
- **監視および検知** – プロセス制御のファイアウォールをログは基本と審査しているか。ユーザ／システムの活動を監視しているか、アンチウィルスのログを監視しているか等。
- **パッチの適用** – どのくらい迅速にパッチを適用しているか、どこから受取るか、全部のマシンにパッチを適用しているか等。
- **アンチウィルスによる防護** – どのくらい速く更新しているか、スキャンの方法や頻度はどうか。
- **対応計画** – 計画を定期的に見直し更新しているか（例：毎年）
- **バックアップ** – バックアップと復旧手順はどうか。

典型的な遵守監視活動

- 適用できる（技術）標準に基づく自動化ツールまたはチェックリストの使用。
- 例えば意識を評価するために、システム所有者、ユーザ、管理者との面談
- プロセスが実行されたという証拠の文書の審査（例：変更管理、例外プロセス）
- ペネトレーション・テストや脆弱性スキャン（注意深く実施）

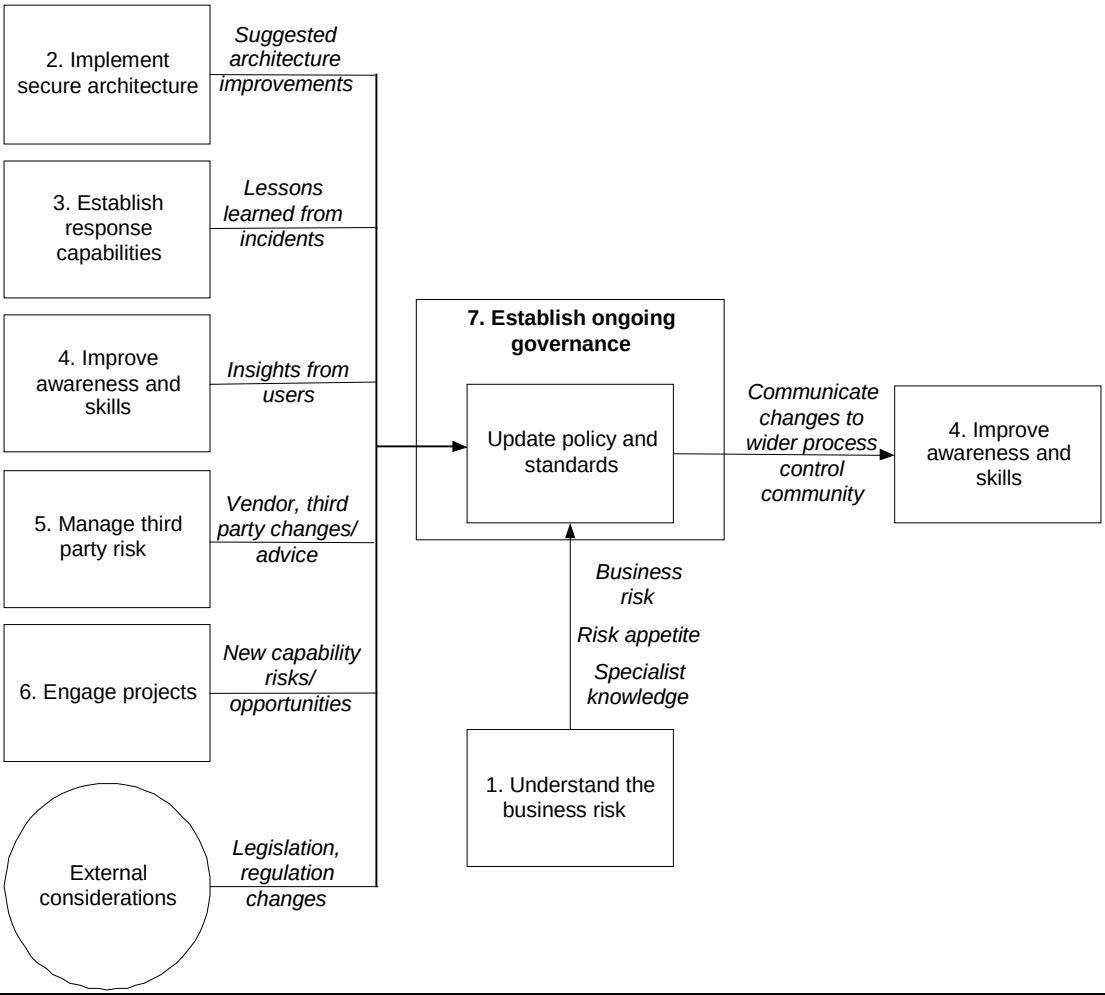
どのくらいの頻度で遵守点検を実行するかは、組織により異なる。自動システムで点検が可能な場合、毎日点検するのも珍しくはないが、アクセス権などの点検は、スタッフの異動、請負業者の使用等に依存して毎月または四半期ごとに行うことが多いだろう。全システム検査は毎年、システムのリスクが低い場合は、もっと少な

く実施するだろう。主要な点は、監視の頻度をシステムの不安定さおよび認められるリスクに合わせることである。

6. ポリシーおよび標準の更新

6.1 フレームワーク全体における本セクションの位置づけ

ポリシーや標準の更新は、プロセス制御セキュリティ・フレームワークの他の要素がきっかけになることもある。組織がリスクに対する現在のスタンスを変更すると決定するするかもしれない。アーキテクチャのセキュリティの進歩が更新を促すかもしれない。あるいはファイアウォールの設置を外注することに決定しリスクが変わったためにポリシーや標準を変更することもある。よくある変更理由は、標準を実践してみたところ過剰な負担になったので、遵守を容易にするため標準をゆるめるか、修正することである。フレームワーク内のいくつかの構成要素でセキュリティ・プロセスを見直す必要が出てくる外部要因がいくつかある。そのような場合、ポリシーや標準を更新することになる。きっかけが何であれ、変更への要求に応え適切な措置を取る効果的なプロセスが不可欠である。



1.Understand the business risk	1.事業リスクの理解
2. Implement secure architecture	2.セキュア・アーキテクチャの実装
3. Establish response capabilities	3.対応能力の確立
4. Improve awareness and skills	4.意識とスキルの改善

5. Manage third party risk	5.サード・パーティ・リスクの管理
6. Engage projects	6.プロジェクトへの参画
7. Establish ongoing governance	7.継続した統制の確立
Update policy and standards	ポリシーおよび標準の更新
Suggested architecture improvements	アーキテクチャ改善の推奨
Lessons learned from incidents	インシデントから学んだ教訓
Insight from users	ユーザからの洞察
Vendor, third party changes/advice	ベンダー、サード・パーティの変更／助言
New capability risks/opportunities	新しい能力、リスク／機会
External considerations	外部考慮事項
Legislation, regulation changes	法令の変更
Business risk	事業リスク
Risk appetite	リスク許容度
Specialist knowledge	専門知識
Communicate changes to wider process control community	変更を広範囲のプロセス制御コミュニティに伝える

図 8 – フレームワーク内における「ポリシーおよび標準の更新」の位置づけ

ポリシーおよび標準の更新に続いて、広範囲のプロセス制御環境において意識の向上や新しいスキル能力の開発を図るため、変更を伝えることも非常に重要である。

6.2 論理的根拠

プロセス制御技術、法律、規制、脅威は、絶えず進歩し進化する。したがって、これらの変化に正しく応えるために、ポリシーおよび標準を定期的に更新することが不可欠である。

6.3 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。

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、更新する、継続したプログラムを確立する。これは、毎年見直すか、または以下のようなきっかけから見直す。

- 現在の脅威の変更
- 法令要件の変更
- 事業要件の変更
- 運用要件の変更
- 運用装置の変更
- 戦略または長期計画の変更

6.4 グッド・プラクティスの手引き

文書をたびたび更新することと、現状を文書に適切に反映することのバランスを保つ必要がある。そのため、ポリシーおよび標準の構成と詳細度を注意深く決める必要がある。品質がよく、柔軟性があり、曖昧性がないポリシーおよび標準を作ることに時間をかければ、特定のセクションだけの修正ですみ、完全な書き直しは必要がなくなるはずである。

ポリシーおよび標準を書くときの主要な原則は、更新を必要とするまでの期間はどのくらいかを考えることである。この手法は予期しない変更には対応できないが、技術の進歩は要因として織り込むことができるはずである。

ポリシーや標準の更新は、最初に作成するときと同様に、時間がかかる作業である。修正には、いくつかの利害関係者が検討して意見を述べる必要があり、プロセス制御システムへの影響と広範囲の事業の必要性を注意深く考慮すべきである。変更の中には単純なものがあり、変更を分類し、係わる必要がある関係者だけに更新の見直しを依頼するのはグッド・プラクティスである。分類は、組織構造および変更管理／見直しプロセスを考慮する必要があるが、いくつかの組織は次の分類を使用している。

- 現地での更新
- 国での更新
- 地域での更新
- 企業全体にわたる更新

ポリシーや標準の更新が限られた利害関係者の承認事項である場合でも、関連する情報が利用可能であり、適切に配布されることを確実にするため、統制グループは継続性を維持すべきことに注意が必要である。

更新ポリシーおよび標準が既存の日常活動になるように、安全・健康・環境の監査などの「平常業務」手順に組み込むのが好ましい。

ポリシーおよび標準に従うことが不可能な場合は、例外ポリシーを設けてこの不遵守が認定されたものであること、リスク評価を実施済みであること、および残留リスクが理解されていることを確実にする必要がある。

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 **4.4.4**

Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks
http://www.cpni.gov.uk/Docs/re-20050223-00157.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 Patch Management
http://www.cpni.gov.uk/Docs/re-20061024-00719.pdf

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

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

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

Process Control Security Requirements Forum
http://www.isd.mel.nist.gov/projects/processcontrol/

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

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

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

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

North American Electric Reliability Corporation (NERC)
http://www.nerc.com

American Gas Association (AGA)
http://www.aga.org

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

National Institute of Standards and Technology (NIST)

http://www.nist.gov

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

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

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

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

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

DHS Control Systems Security Program Recommended Practices
http://csrp.inl.gov/Recommended_Practices.html

ISA SP99, Manufacturing and Control Systems Security
http://www.isa.org/MSTemplate.cfm?MicrositeID=988&CommitteeID=6821

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

セクション 5.4.2
NIST Guide to Industrial Control Systems (ICS) Security
http://csrc.nist.gov/publications/drafts/800-82/draft_sp800-82-fpd.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