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 2. セキュア・アーキテクチャの実装

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 2. IMPLEMENT SECURE ARCHITECTURE" 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、悪意の攻撃、DoS、プロセスの不正な制御、完全性の欠如、守秘性の欠如、世評の下落、健康・安全・環境への悪影響などがありうる。

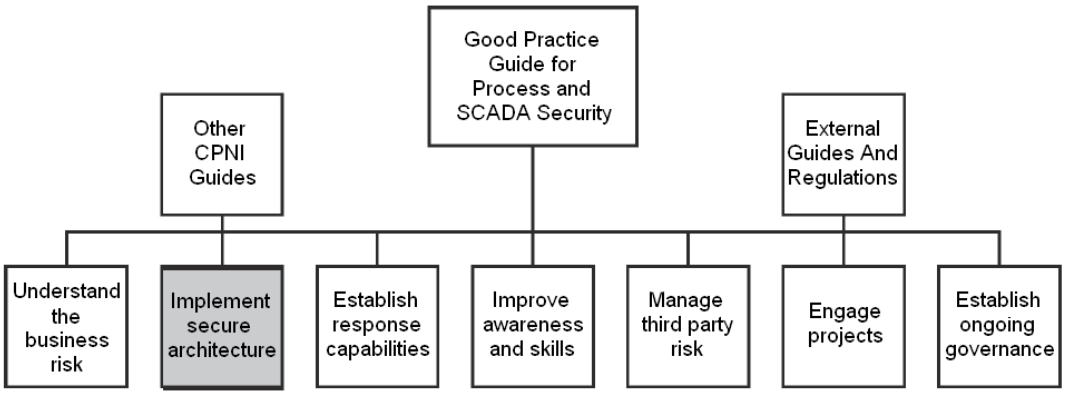
1.3 プロセス制御セキュリティ・フレームワーク

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。この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「**セキュア・アーキテクチャの実装**」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。

本ガイドは詳細なリスク評価手法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、SCADA 、産業オートメーション技術者
- 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. セキュア・アーキテクチャの実装についての要約

グッド・プラクティス・フレームワークに含まれるこの「**セキュア・アーキテクチャの実装**」要素では、制御システムのセキュア・アーキテクチャに関する定義と実装を取り扱う。

制御システムの安全を確保する必要に迫られた場合に通常簡単にすぐ実施される方法が、ファイアウォールのインストールやウイルス対策ソフトウエアの導入などの、明確なセキュリティ手段の実装である。しかしながら、無計画な展開が行われる場合、そのような行動は、資金や人材といった貴重なリソースの最適な投資にはならない可能性がある。したがって、グッド・プラクティスとして考慮されるのは、制御システムが直面しているリスクを十分に理解した上で保護対策を選択・実装することである。これにより、利用可能なリソースを最適な手法で目標とすることができる。

上述のリスクを理解するには、リスク評価を実施する必要がある。このリスク評価では、制御システムの範囲の評価と、そのシステムが直面する脅威、影響、脆弱性の検討を行う。リスク評価については、本フレームワークの「**事業リスクの理解**」要素でより詳しく説明する。このリスク評価により、取り組むべき最重要領域が決定される。また、利用可能なリソースが最もリスク低減効果を発揮できる領域に分配されるようにする選択プロセスの情報源も、リスク評価からもたらされる。

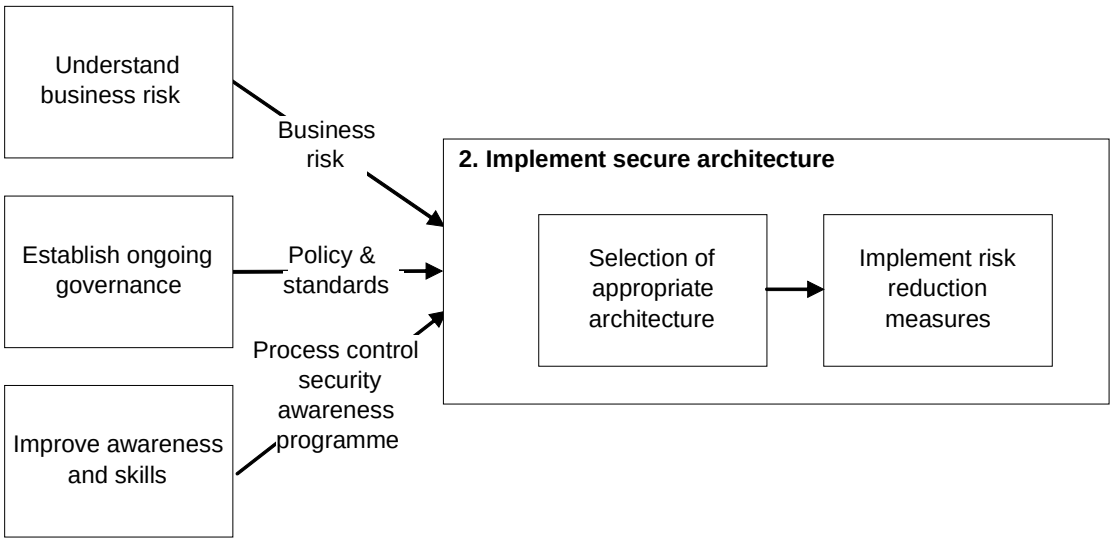
事業リスクを十分に理解した後は、一組のリスク低減（セキュリティ改善）手段を選択して、制御システムのための総合的なセキュア・アーキテクチャを構築することができるようになる。ここで「アーキテクチャ」は、技術のみならずシステムの人的要素をも含む広い意味で使用される。セキュア・アーキテクチャは、プロセス、手順、管理のための様々な保護対策で構成される。技術的なソリューションだけで構成されるものではない。

プロセス制御セキュリティ手段の選択は決して精密科学ではなく、すべてに対応できる「万能」なものでもまったくない。プロセス制御セキュリティの分野がまだあまり成熟していないことや、多種多様なレガシー・システムが現存していることもあり、国際的基準の遵守は一筋縄では済まない。業界全体にわたり現在発展中の業界基準は多数存在するが、標準的なセキュリティ保護対策一式を単に実装できるようになるまでにはまだ程遠い。

セキュリティ・アーキテクチャを選択したら、あとはそれを実装するだけである。単純に聞こえるかもしれないが、これらのソリューションの実装プロセスは、注意深く管理しないと、危険な場合があったり、システムの機能停止を招いたりすることがある。

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

このセクションでは、「**事業リスクの理解**」セクションで得られた結果を使用して、適切なセキュリティ手段一式の選択と、セキュア・アーキテクチャの構築を行う。構築したセキュア・アーキテクチャは、制御システムの安全性を確保する目的で実装することができる。



Understand business risk	事業リスクの理解
Establish ongoing governance	継続管理の確立
Improve awareness and skills	意識とスキルの改善
Business risk	事業リスク
Policy & standards	方針および基準
Process control security awareness programme	プロセス制御セキュリティへの意識向上プログラム
2. Implement secure architecture	2. セキュア・アーキテクチャの実装
Selection of appropriate architecture	適切なアーキテクチャの選択
Implement risk reduction measures	リスク低減手段の実装

図2 – フレームワーク内における「セキュア・アーキテクチャの実装」の位置づけ

3.2 論理的根拠

制御システム用のセキュア・アーキテクチャを設計するということは、困難な作業である。なぜなら、様々なタイプのシステムがあまりにも多く存在するばかりか、予想されるソリューションも数が多く、中にはプロセス制御環境に適さないものまで存在するからである。リソースが限られているとすれば、重要となるのは、選択プロセスで保護のレベルを事業リスクに適したものに設定することと、その防衛面で1つのセキュリティ手段に頼らないようにすることである。

3.3 グッド・プラクティスの原則

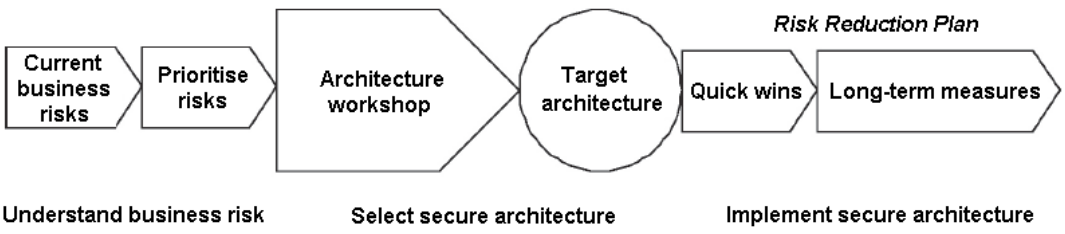
包括的な文書「Good Practice Guide Process Control and SCADA Security」（日本語版：「グッド・プラクティス・ガイド ー プロセス制御とSCADAセキュリティ」）に記載されているグッド・プラクティスの原則は次の通りである。

- セキュア・アーキテクチャを構築するための適切なセキュリティ手段（事業リスクを基礎とする）の選択事業
- 選択したリスク低減手段の実装

3.4 グッド・プラクティスの手引き

フレームワークに含まれるこの要素では、問題となっているプロセス制御システムのセキュア・アーキテクチャについての定義と実装を取り扱う。その実現のために適切な保護対策を選択する。これにより、特定された事業リスクに対して効率的に取り組むことができる。以下に、アーキテクチャの選択や実装に適用可能なプロセスを高次の観点から見た全体像として示す。

- 事業リスクの理解
- 事業リスクに基づく事業の脆弱性の優先順位決定
- アーキテクチャ・ワークショップの開催
- 目標とするアーキテクチャへの合意
- 実装計画の明確化
- セキュリティ改善手段の実装



Risk Reduction Plan	リスク低減計画
Current business risks	現在の事業リスク
Prioritise risks	リスクの優先順位決定
Architecture workshop	アーキテクチャ・ワークショップ
Target architecture	目標とするアーキテクチャ
Quick wins	短期的目標
Long-term measures	長期的手段
Understand business risk	事業リスクの理解
Select secure architecture	セキュア・アーキテクチャの選択
Implement secure architecture	セキュア・アーキテクチャの実装

図3 – 高次のセキュア・アーキテクチャ実装のプロセス

このプロセス全体を通じて考慮すべき重要な要素については、後のセクションで説明する。

3.4.1 事業リスクに基づく脆弱性の優先順位決定

セキュリティ手段を決定する場合は、事前に、制御システムが直面している事業リスクを十分に理解しておくことが重要である。制御システムの安全を確保する必要に迫られた場合に非常によく実践されるのが、ファイアウォールやウイルス対策ソフトウエアなどの明確なセキュリティ手段の実装である。しかも広い視野からのリスク検討を行わない状態でのことである。このようなアプローチはシステムセキュリティを確保することにはならない場合がある。これは、それら保護対策すべてがアーキテクチャ全体を対象としている、とはみなされないからである。事業リスクをよく理解することは、システムの保護が事業リスクとバランスの取れたものとなるように適切なセキュリティ手段を選択する上で必要とされる。つまり、システムは、保護し過ぎる（リソースの活用が非効率）ことも、しなさ過ぎる（セキュアでないシステム）こともないようにする。

事業リスクは、以下に挙げる 4 つの主要な要素に焦点を絞って理解する。これらについて詳しくは、フレームワークの「**事業リスクの理解**」要素で説明する。

- システムの理解
- 脅威の理解
- 影響の理解
- 脆弱性の理解

このプロセスの結果は、主要システムと、その主要システムがもたらす脅威、利用され得る脆弱性の理解に繋がる。このことは、セキュア・アーキテクチャを定義する上で不可欠な前提条件となる。

3.4.2 リスク低減ワークショップの開催

事業リスクを十分に理解しさえすれば、脆弱性についてひとつひとつ対処するための保護対策の選択という主要な作業を実施することができるようになる。この作業は、ワークショップ形式で行うことが最良である場合も少なくない。ワークショップでは、問題に対する考え方がそれぞれ異なる多くのグループが力を合わせることにより、適切な保護対策の選択を可能とする。アーキテクチャの選択は、1 人の者が単独で行うべきではない。1 人では、システム全体を見据えることができないばかりか、異なる視点から問題を捉えた場合の知識を持っていない可能性があるからである。

このようなワークショップに参加するチームを結成する場合は、少なくとも以下のグループを考慮する必要がある。

- プロセス制御について総合的な責任を負う者（SPA）
- プロセス制御チームのメンバー
- 事業リーダー
- 作業チームの代表者
- IT セキュリティの代表者
- IT インフラストラクチャの代表者
- IT ソフトウエアの代表者
- プロセス制御ベンダー

チームの編成後は、特定されたリスク要因の検討作業と適切なリスク低減手段の選択作業をそのチームで進めることができる。

3.4.3 目標とするアーキテクチャへの合意

リスク低減ワークショップの主たる目的は、リスク評価で特定されたリスク要因と脆弱性を検討することである。リスクはそれぞれ順番に取り上げられて分析が行われる。

各リスクには、可能な対策が 3 種類用意されている。

- **リスク低減手段の展開（セキュリティ改善手段）** – リスク低減手段の選択について詳しくは、本セクションの後半で説明する。
- **継続的計画の展開** – フレームワークの「**対応機能の確立**」要素で説明する。
- **残存リスクとしての取り扱い（アクションなし）** – 残存リスクとして取り扱う決定をする場合は、事業指導者の合意を得ることと、リスク記録簿への記録が必要となる。残存リスクについては、見直しを定期的に行う必要がある。

3.4.4 セキュリティ手段の選択時に考慮すべき要因

リスク低減手段を選択する作業は、一見単純なように見えて、実際には想像よりはるかに難しい場合が多い。それは、手段の選択に影響する要因の幅が広く、それぞれに固有の制約がつきまとうためである。考慮を要するこれらの要因は、コスト、保護の効力、事業モデル、実装、展開、ソリューションの 6 つの分野に分類できる。

コスト

セキュリティ手段によっては、その実装コストが、既存システムの設定に対するちょっとした変更や、既存の作業プラクティスへのわずかな修正に伴い、比較的低く抑えられることがある。しかし、セキュリティ手段によっては、その実装には、新規システムや、新たな作業プラクティスまたは作業方法の創出が伴う。そしてその創出には追加の資金や収益支出が必要とされる。

解決策のコスト効果は、保護対策の効力との比較で考える必要がある。

セキュリティ保護対策の現行の運用コストを調べる必要がある。

防護の強さ

保護対策がどの程度の効力を有するかについて考えてみると、その判断が困難な場合がある。ただし、手段の効力についての程度を示す簡単な尺度を定義することにより、意思決定プロセスは単純なものとなる。

セキュリティは最も弱い部分を基準に考えるべきであり、重要なのは、セキュリティ・アーキテクチャの最も弱い部分を特定して管理することである。

セキュリティ手段の選択の指針となる原則は、多層防御を基礎とするアーキテクチャを選ぶことである。階層化したセキュリティ手段は、リスクに曝された場合にセキュリティ・アーキテクチャが効果を失う単一のセキュリティ手段よりも効果が高い。

事業モデル

制御システムのセキュリティ改善のための資金を確保するため、事業モデルを構築する必要が生じる場合がある。この事業モデルでは、現在のリスクとセキュリティ改善の必要性を明確にするべきである。本フレームワークの「事業リスクの理解」要素から得られた結果は、この事業モデルの構築に役立つ可能性がある（付録 A 参照）。この事業モデルは、提案された投資が制御システムの事業リスク・プロファイルをどのように変え、残余リスクがどう明確になるかを示すべきである。

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）

事業モデルを構築する場合、セキュリティ投資収益率（ROSI）を明確にすることが有用な場合が少なくない。ただし、プロセス制御と SCADA セキュリティ・インシデントについて利用可能なデータの不足により計算が困難となり、ROSI の判断が難しい可能性がある。

セキュリティのための詳細な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。

実装

セキュリティ手段の中には、他のものよりも実装しやすいことから短期的に現地で好まれるものがある。例えば、使用しなくなったダイヤル・アップ・モデムの接続を解除することは、限られた保護を実現するが、実装は簡単である。

セキュリティ手段によっては、既存システムの設定に対するちょっとした変更や、既存の作業プラクティスへのわずかな修正に伴い、その実装が比較的短期間で済む場合がある。しかし、セキュリティ手段によっては、実装は、新規システムや、新たな作業プラクティスまたは作業方法の創出を伴う。

一定の構成には役立つ一方、ある構成で機能しても別の構成には機能しない可能性もあるが、実装計画を決定するときはベンダーにアドバイスを求めるべきである。

セキュリティ・ソリューションを稼動中の制御システム環境に展開する前に、このソリューションに対してどのようなテストを行う必要があるかということを考慮すること。追加のテストを行うと、費用が別に発生する上、展開に要する時間も長くなる。

展開

セキュリティ手段によっては、その実装に際して、現地レベルで利用可能な財源やスタッフ資源による制約を受けるものがある。

ここで、セキュリティ手段実装の責任を負う者について考えてみる。特に、そのような責任を負う者は、プロセス制御スタッフの現メンバーを参加させる必要がある手段と、特定したスタッフが共同で作業する時間を確保できるかどうかを確認する必要がある。

組織は、適切なアーキテクチャの選択に際して、「即効性のある手段」と「長期的」手段の両方を把握しておく必要がある。

セキュリティ手段を検討する際は、スタッフの訓練の必要性と、現在行っているサポートや保守のことも忘れずに考慮する必要がある。これは単なる財政的コストで終わる場合もあるが、別のリモート・アクセス要求や、ハードウエアまたはソフトウエアのアップグレードの必要性などが、このことにより発生する可能性がある。

ソリューション

リスク低減手段は、アーキテクチャにおいて全体的に捉える必要がある。つまり、1組の手段であり、単なる局所的ソリューションではない。

可能な場合には、既に利用可能となっている標準的なソリューションを活用してアプローチの共通化を図ることにより、コストと複雑さを最小限に留めつつ以下のような他のメリットを実現する。

- **実績あるソリューションの再利用** – 適用できる場合には、実績あるアーキテクチャ・ソリューションを再利用する。
- **既知の品質基準** – 既存ソリューションの再利用により、プロセス制御システムの別々の部分や異なる複数の現地において、同レベルの品質の再現が確実なものとなる。
- **管理のし易さ** – 問題やエクスポージャーが同じ方法で処理されれば、インシデントへの対応は管理しやすいものとなる。これは、同一のアプローチを使用したすべてのプロセス制御システムに、同じソリューションを展開できるためである。
- **規模による経済性** – 特定の製品やサプライヤを組織全体にわたって採用すると、より大きな購買力となり、セキュリティ設計の改善にも何らかの影響が及ぶ。
- **スキルと専門技術** – 実績ある制御システム・セキュリティ・アプローチを再利用することにより、組織において、開発と、セキュリティ手段のサポートに必要な訓練を制限することが可能となる。サポートをサード・パーティに依存している場合は、サポート・コストを節約することにもなる。

可能であれば、制御システム・ベンダーが承認するソリューションの採用を検討する。こうしたソリューションは、細部にわたる統合がなされており、ベンダーの認定も受けている。このようなテストと認定の実施ベンダーによる保証を要求すること。

セキュリティ手段の選択は、リスクに基づいて行うこと。資金のもっと良い使い道が他にあるにもかかわらず、低リスクの脅威や最小限の影響に対処するために強力で高価なセキュリティ手段に資金を投入することは無駄である。

可能であれば、常に、ファイアウォールに親和性のある通信プロトコルを使用する。ファイアウォールに親和性のないプロトコル（例：OPC[3]）の場合は、ファイアウォールのルール基盤を厳密に設定できない。

セキュア・アーキテクチャの選択と関係があるのは、技術的手段だけではない。関連プロセスや、手順と管理の要求についても配慮が必要とされる。

可能であれば、IT 部門が提供するような、既に利用できる状態となっているサービスやソリューションを使用することを考える。ソリューションは、例えばウイルス

[3] ウィキペディアでの「OPC（OLE (Object-Linking and Embedding) for Process Control）」の定義。この標準は、異なるメーカーの制御デバイス間における、リアルタイムのプラント・データ通信を定めている。

対策アップデートの段階的導入など、制御システムの運用環境に合わせて調整する必要がある。

考え得るセキュリティ手段を構築する場合は、効力やおそらくコストもそれぞれ異なる様々なオプションを多数開発する。このことは、財政上の意思決定プロセスに役立つ。

社内サービスを利用できない場合は、サード・パーティからの供給を検討する。外部から供給可能なサービスとしては、例えば以下のものが挙げられる。

- ファイアウォールの管理および監視
- ネットワークおよび電話回線など
- インフラストラクチャの管理および監視
- サーバの管理および監視

アウトソーシングの詳細については、CPNI の『Good Practice Guide Outsourcing: Security Governance Framework for IT Managed Service Provision』（付録 A 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。

セキュリティ手段の実装には少々時間を要する場合がある（例：ネットワークの再設計やファイアウォールの実装）。そのため、簡単であまりコストのかからない暫定的な手段を検討する必要がある。そのような暫定手段によっても、短期的には保護をある程度強化することができる。

すぐに実装できる比較的簡単なセキュリティ手段としては、多数のものが考えられる。そのうちのいくつかを以下に挙げる。

- 既存システムの構成の改良
- ウイルス対策
- アクセス制御の強化
- バックアップおよび回復の機能
- 物理的セキュリティ
- 使用されていない接続の解除

3.4.5 リスク低減手段のチェックリスト

ターゲットとするセキュリティ・アーキテクチャの特定後は、以下のチェックリストを利用して完全性をチェックする。このリストは、中核となる「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」）の高レベル・セクションに掲載されているものと同一のものである。

- ネットワーク・アーキテクチャ
- ファイアウォール

- リモート・アクセス
- ウイルス対策
- 電子メールおよびインターネット・アクセス
- システムの強化
- バックアップおよびリカバリ
- 物理的セキュリティ
- システム監視
- ワイヤレス・ネットワーキング
- セキュリティ・パッチの適用
- スタッフの経歴チェック
- パスワードおよびアカウント
- 文書化したセキュリティ・フレームワーク
- 回復力の高いインフラストラクチャと設備
- 脆弱性管理
- 起動・分離プロセス
- 変更管理
- セキュリティ・テスト
- デバイスの接続手順

上記の項目を詳細に解説した様々なガイドが存在する。例えば、以下のガイドが提供されている。

- Best Practice Guide on Firewall Deployment for SCADA and Process Control Networks
- Good Practice Guide Outsourcing: Security Governance Framework for IT Managed Service Provision
- Good Practice Guide Patch Management
- Best Practice Guide Commercially Available Penetration Testing
- A Good Practice Guide on Pre-Employment Screening
- CPNI guide on Personnel Security Measures
- 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

（付録 A 参照）

3.4.6 実装計画への合意

セキュア・アーキテクチャへの合意が成立し、予算見積が済んで資金提供を受けたら、次の作業は実装計画を明確にすることである。一見簡単なように見えるが、制御システム環境におけるセキュリティ改善手段の実装は、複雑な場合がある。また、リスク低減手段を実装することにより、システム崩壊という重大なリスクが引き起こされる可能性もある。システム・オペレーション崩壊のリスクを最小化するためには慎重な計画が必要とされる。また、稼動中の環境における実装手段より先に、テストの実施を検討する必要がある。さらに、問題が発生した場合に備え、後戻りするための計画も実装計画に盛り込んでおく必要がある。

実装計画で検討すべき要因を以下に挙げる。

- **システムの優先順位** – 一般的に、包括的なシステムに取り組んだ後、重要度の低いシステムに取り掛かる。
- **予算見積** – リスク軽減手段をすべて同時に実装することは、予算の都合上困難な場合がある。そのような場合には、暫定的なセキュリティ手段を検討する必要がある。
- **リソースの可用性** – リスク低減手段の実装に必要とされる人材は、極めて不足している場合が多い。多くの場合、適切なスキルを身に付けている人材は非常に少ない上、そうした人材はたいてい、競合する他のイニシアチブに取り組むよう求められている。したがって、実装計画は、適切な人材の可用性に左右されることが少なくない。
- **変更制限の割合** – 業務において 1 回で吸収できる変更の量には限度がある。リスクが低く規則正しい配置を維持するには、あまり無理のない実装計画を立てることが重要である。
- **段階的アプローチ** – リスク低減手段の実装は長期間かけて行われることがある。大規模な計画や込み入った計画の場合は、実装問題が発生するリスクを最小限に抑えるため、段階的アプローチを検討する必要がある。
- **依存関係** – 実装計画では、特定されているすべての依存関係を考慮に入れる必要がある。一部の依存関係については既に言及した（例：リソース）が、リスク低減手段の中には、他に先駆けて実装することが必要なものもある。例えばモデムを取り外す場合は、モデムの代わりとなり、なおかつ依存関係を持つセキュアなリモート・アクセス手段が先に使用可能となっていることが必要とされる。

- **訓練計画** – 実装計画には、訓練に必要なすべての事項も盛り込む必要がある。その場合、単なるソリューション展開技術に留まらず、サポートや保守のための人材、システムの全ユーザおよび全オペレータを考慮に入れる。
- **連絡と意識** – 実装計画には、変更があった場合に利害関係者に知らせる上で必要な連絡と意識の要素を盛り込む必要がある。
- **手順の開発およびテスト** – 実装計画には、リスク低減手段をサポートするすべての関連手順の開発も盛り込む必要がある。なお、このような手順は、単に作成して公表すれば済むというものではなく、多くの場合は多大な労力を費やして日々の業務に組み込むことが必要とされる。
- **テスト** – 実装計画には、テストに関係のあるすべての要素を盛り込む必要がある。これには、統合テスト、配置テスト、手段が正しく実装されたことの保証が含まれる。これは、正式なセキュリティ検査の形式で実施することもあれば、実装後の点検という形で行われることもある。

3.4.7 セキュリティ改善手段の実装

実装計画が完成し、点検と同意が済んだら、リスク低減手段の実装に着手することができる。実装プロセス全体を通して、考慮すべき事項が多数存在する。

- **変更管理** – 制御システムに対するすべての変更は、適切な変更管理システムの下で実施する必要がある。制御システムの変更は、制御システムと、バリュー・チェーンのはるか下に位置する IT システムの両方に影響を及ぼす可能性がある。そのため、変更の管理は、プラント・システム用と IT システム用など、それぞれ別の変更システム下で行う必要がある。

  変更が行われた場合は、システムの設計図、目録、リスク評価の更新が確実に行われることを変更管理システムで保証する必要がある。変更プロセスにおいてこれらの更新が保証されない場合は、すべての情報が最新の状態になっていることを確認するための点検を行う。また、システム情報を常に最新の状態とするためのプロセスの修正も、実施する価値がある。
- **実装後の点検** – リスク低減手段の実装後は、保証試験を実施して、手段がセキュリティ・アーキテクチャのデザインに従って導入されていることを確認する必要がある。保証試験は、実装チェックリストからセキュリティの完全点検や完全検査に至るまで、多様な形態で実施することができる。ただし、ペネトレーション試験だけは厳密な条件（例：プラントのシャットダウン）の下で実施される。この種のテストとして、制御システムのシャットダウンや、プロセス・プラント・コントローラの改悪を行うことは普通では考えられないことだからである。
- **連絡と意識** – 実装プロセス全体を通じて重要なことは、適切な連絡を行うことにより、該当する利害関係者がすべて実装プロジェクトの最新の状態や開発について確実に意識できるようにすることである。

プロセス制御セキュリティの仕事は、すべてのリスク低減手段を実装して完全なセキュリティ・アーキテクチャを構築したからといって、それで終わりというわけではない。これは、制御システムのセキュリティ・ライフサイクルにおける 1 つのマ

イルストーンに過ぎない。制御システムが将来もセキュアな状態に正しく維持するための作業は、常に継続している。この作業には以下のことに関係する。

- 常に最新の脅威に対応した方針、基準、プロセスの状態の維持
- 制御システムがセキュリティ・ポリシーや基準を遵守していることの継続的保証
- すべての技術者、ユーザ、管理者がセキュリティ意識を持っており、プロセスや手順がセキュアな手法で実装されている状態の保証
- セキュリティの脅威に変更があった場合に対応するための適切な対応機能の確保
- サード・パーティのリスクが管理されている状態の確保

リスクが積極的に管理され、定めたプロセスと手順が守られるようにするため定期的に監査を実施すること。リスクの管理に関する詳細については、本フレームワークの「事業リスクの理解」に示されている。

これらの作業については、本グッド・プラクティス・ガイダンス・フレームワークの残りの部分で詳しく説明する。

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 **3.4.2**
Guide to Industrial Control (ICS) Systems
http://csrc.nist.gov/publications/PubsDrafts.html

セクション **3.4.5**
Best 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

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

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

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.us-cert.gov/control_systems/pdf/Catalog_of_Control_Systems_Security_Recommendations.pdf

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?section=homeandtemplate=/TaggedPage/getStandards.cfmandMicrositeID=988andCommitteeID=6821

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

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 NISCCCPNI 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: 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: 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