# 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 1. 事業リスクの理解

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 1. UNDERSTAND THE BUSINESS RISK " 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。

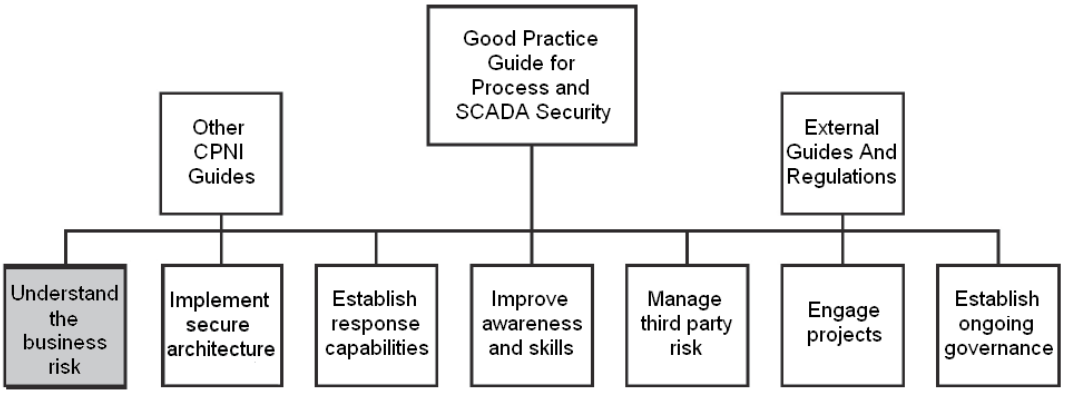
これらの脆弱性が攻撃されれば重大な結果を招く恐れがある。プロセス制御システムに対する電子的攻撃の影響としては、例えば、悪意ある攻撃、DoS 攻撃、プロセスの不正な制御、完全性の損失、機密性の欠如、世評の下落、健康・安全・環境への悪影響などがありうる。

[1] 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。

## 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。

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「**事業リスクの理解**」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。

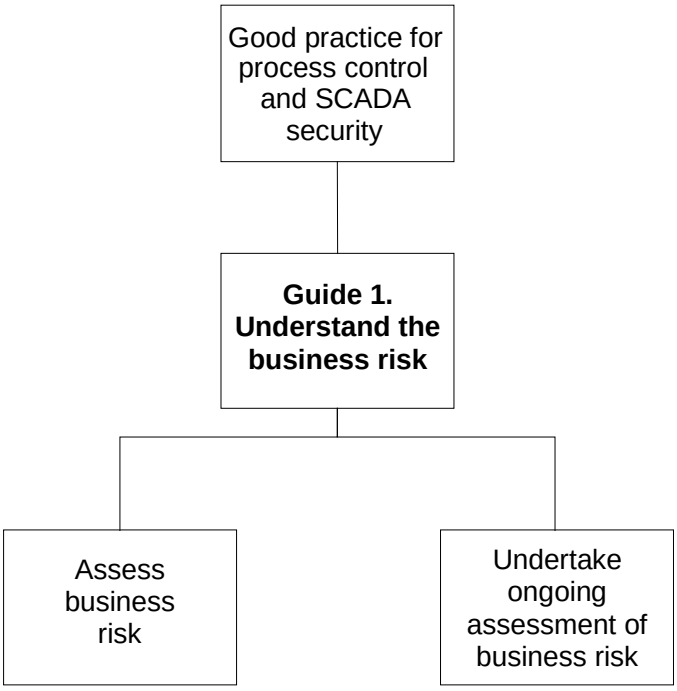
- プロセス制御とオートメーション、SCADA テレメトリ技術者
- 情報セキュリティ専門家
- 物理セキュリティ専門家
- 事業リーダー
- リスク管理者
- 健康・安全管理者
- オペレーション技術者
- 監査人

## 2. 事業リスクの理解についての要約

プロセス制御システムのセキュリティを改善するための第一歩は、電子セキュリティの観点から見た事業リスクを完全に理解することである。事業リスクは、脅威、影響、脆弱性のそれぞれと相関関係にある。企業では、事業リスクを十分に理解して初めて、適切なレベルのセキュリティ保護を実現するために必要なことが判別できるようになる。

セキュリティ上のいかなる改善も、問題のシステムが現在直面しているリスクの程度を基準に実施される必要がある。これは、適切なレベルの保護を確実なものとするためである。例えば、低リスクのシステムでは、高リスクのシステムの場合よりも、保護の要求レベルが低くなると考えられる。しかしながら、セキュリティの効果を十分に発揮させるには、その保護対策を適切に講じていく必要がある。そのような保護対策を講じていく上で重要となるのが、事業リスクについての理解である。

事業リスクを理解することは、1 回限りのことではなく、それ以降も続く。一旦リスク評価を行い、その結果に基づくセキュリティの改善策を講じた後は、時間が経過し、脅威が変化し、更なる脆弱性が特定されるにつれて事業リスクがどのように推移するのかを見守り続けることが重要となる。




| | |
|---|---|
| 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 1. Understand the business risk | ガイド 1. 事業リスクの理解 |
| Assess business risk | 事業リスクの評価 |
| Undertake ongoing assessment of business risk | 事業リスクの継続的な評価の保証 |

**図2 - 事業リスク文書の構造の理解**

**定義**

**リスク** – 制御システムに影響が及ぶ可能性。リスクをもたらす事象は、1 つの脅威の結果の場合と、複数の脅威の組合せの結果の場合がある。

**リスク許容度 –** リスクのレベル。受容可能なリスクを決めるために使用する。

**脅威** – 不正なアクセス、データの破壊、公開、改ざん、サービス拒否などを通じて情報システム（IS）に悪影響を及ぼす可能性を秘めたあらゆる状況や出来事。

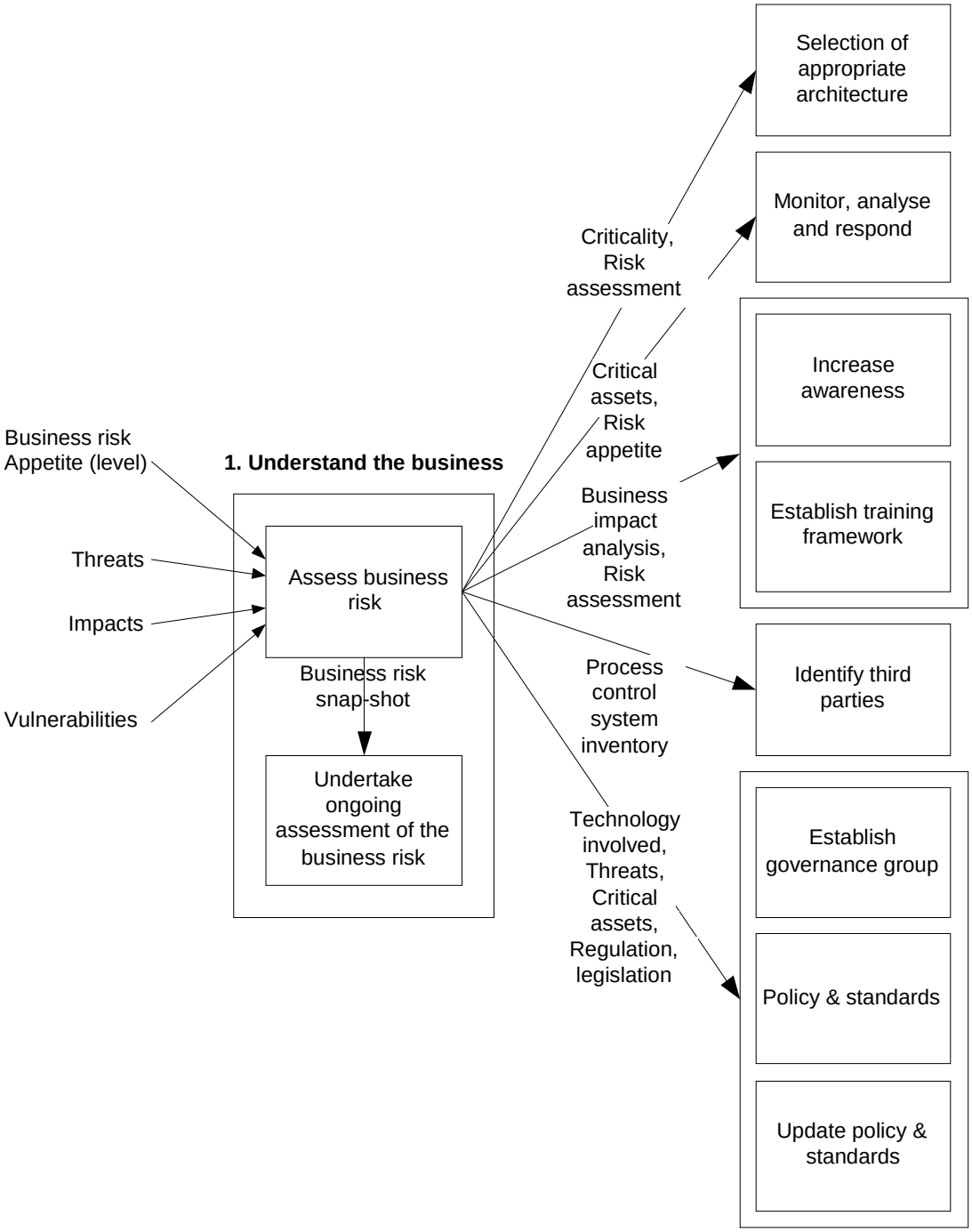
**可能蓋然性** – ある具体的な結果が発生する確率。

**影響** – 脅威の発生により生ずる結果。

**脆弱性** – ソフトウエア・システムやコンポーネントが、不正な情報のアクセス、改ざん、公開などに対して曝された状態となり、システム・サービスの妨害や混乱が生じやすくなる度合い。

## 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

事業リスクの評価は、このプロセス制御セキュリティのフレームワークに内包されるすべてのテーマの出発点となる。そしてこの評価の結果は、フレームワーク内の他の様々な要素によって活用される。



| | |
|---|---|
| Business risk Appetite (level) | 事業リスク許容度（レベル） |
| Threats | 脅威 |
| Impacts | 影響 |
| Vulnerabilities | 脆弱性 |
| 1. Understand the business | 1．事業の理解 |
| Assess business risk | 事業リスクの評価 |
| Business risk snap-shot | 事業リスクのスナップショット |
| Undertake ongoing assessment of the business risk | 事業リスクの継続的な評価の保証 |
| Criticality, Risk assessment | 重要度、リスク評価 |
| Critical assets, Risk appetite | 重要資産、リスク許容度 |
| Business impact analysis, Risk assessment | 事業影響度分析、リスク評価 |
| Process control system inventory | プロセス制御システムの目録作成 |
| Technology involved, Threats, Critical assets, Regulation, legislation | 関連技術、脅威、重要資産、規制、法律制定 |
| Selection of appropriate architecture | 適切なアーキテクチャの選択 |
| Monitor, analyse and respond | 監視、分析、対応 |
| Increase awareness | 気付きの向上 |
| Establish training framework | トレーニング体制の確立 |
| Identify third parties | サード・パーティの特定 |
| Establish governance group | 管理グループの設立 |
| Policy & standards | 方針および基準 |
| Update policy & standards | 方針および基準の更新 |

**図 3 – フレームワーク内における「事業リスク評価」の位置づけ**

## 3.2 論理的根拠

組織は自分たちの事業が直面しているリスクを理解する必要がある。これは、適切なリスク許容度（リスク・レベル）を判断し、このリスク許容度に収まるようリスクへの暴露水準を引き下げるため、どんなセキュリティ上の改善事項が必要となるかを判断するためである。

## 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 ― プロセス制御とSCADAセキュリティ」）に記載されている、関連したグッド・プラクティスの原則は次のとおりである。

次の各項を目的として、プロセス制御システムについての正式なリスク評価を開始すること。

- **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および評価を実施せよ。この作業の全体を通じて重要なことは、既存システムの種類、各システムの役割、業務面および安全面から見た既存システムの危険度、既存システムの設置場所、各システムの指定所有者・管理者・サポート担当者、既存システムとやり取りを行う方法を、すべて把握して文書化し、変更管理の下に置くことである。システムの範囲と、すべてのインタフェース、ハードウエア、ソフトウエアを特定せよ。

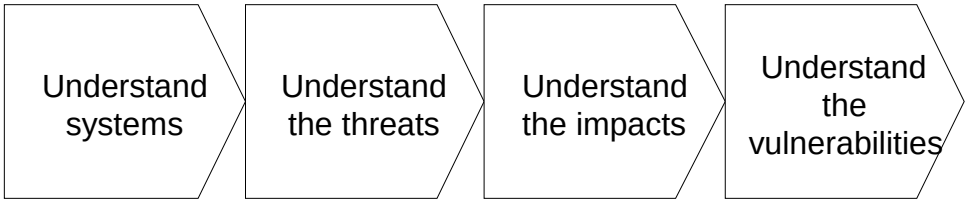
- **脅威の理解** – プロセス制御システムが直面している脅威を特定し評価せよ。可能性として考えられる脅威としては、サービス拒否、標的型攻撃、偶発的な出来事、不正な制御、ウイルス、コンピュータにインストールされた悪意あるコード、ワーム、トロイの木馬感染などが挙げられる。

- **影響の理解** – 脅威が現実のものになったと仮定した場合にプロセス制御システムが被ると予想される影響およびその結果を特定せよ。結果としては、例えば、世評の下落、（健康、安全、環境などの）規制要件違反、業務目標の達成不能、財政上の損失などが挙げられる。

  注意：プロセス制御システムが他の主要サービスへの供給における重要な要素となっている場合、影響は、業務の範囲にとどまらず、それ以外で深刻かつ致命的な結果をもたらす可能性がある。

- **脆弱性の理解** – プロセス制御システムの脆弱性評価を開始せよ。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、コンポーネント・ソフトウエア、ネットワーク接続、リモート・アクセスの接続性、プロセス、手順などを評価すべきだ。

## 3.4 グッド・プラクティスの手引き




| | |
|---|---|
| Understand systems | システムの理解 |
| Understand the threats | 脅威の理解 |
| Understand the impacts | 影響の理解 |
| Understand the vulnerabilities | 脆弱性の理解 |

**図 4 – 事業リスク評価の主要手順**

### 3.4.1 システムの理解

事業に対して立ちはだかるプロセス制御セキュリティ・リスクを理解するには、その事業を構成するシステムを隅々まで把握する必要がある。このプロセスではまず、このリスク分析の適用範囲について同意を取りつける。適用範囲の境界線は明確に引く必要がある。また、適用範囲外と認定されたシステムについては、誰が担当する適用範囲に所属するのか明確にする必要がある。さらに、適用範囲外とされたシステムのセキュリティ保護レベルについてもそれ相応の保証を求めておく必要がある。

多くの場合、プロセス制御システムは何年も前からすでにインストールされた状態にあり、その動作や構成に関する詳細な情報がない場合がある。事業リスクを理解するためには、このような情報を（直ちに利用できないポイントについて）決定し、システムの完全な棚卸台帳にまとめあげる必要がある。

目録の作成には、以下に示す多くの条件を考慮する必要がある。

- 拠点数、サイト数、システムの数、資産の数
- 当該サイトに設置されたシステムの種類
- バリュー・チェーンまたはサプライ・チェーン全体におけるサイトやシステムの位置づけ
- 各サイトまたは各システムにおける業務上および運用上の重要箇所
- プロセスや人的安全に対するシステムの役割

- サイトごとの生産または運用の内容
- 安全性や、衛生および環境面、その他の規制との係わり合いの有無
- 資産が国家の重要インフラストラクチャ（CNI）の一部を構成しているかどうか（CNIにあたるかどうかについて詳しくは、http://www.cpni.gov.uk を参照のこと）
- 各サイト、システム、資産について総合的な責任を負う者（SPA: Single Point of Accountability）
- システムに関係する主要なベンダーとサード・パーティ
- サイトでの主要なサポート組織（IT 部門、プロセス制御部門、外部サード・パーティ、常駐サード・パーティ、組織内）
- サイトにおける重要なシステム資産
- 制御システムとの間に存在する接続およびデータ供給（手動のデータ供給ならびに電子的接続を含む）
- システムに関する既知の問題の有無
- 進行中のプロジェクトまたは予定されているプロジェクト
- 地方の担当者やベンダーに関する連絡先の詳細
- サイトに関する依存関係の種類
- システムおよびネットワークの概略図や詳細な図面の有無
- すべての文書に対するセキュリティ対策と変更手続管理の有無

上記の問に回答することにより、プロセス制御システムの棚卸ができる。システムの棚卸は、プロセス制御セキュリティ・フレームワークの根幹を成す要素であり、他の多くのテーマやセクションの情報源となる。この棚卸調査は、リスク判断を正しく行うために十分な精度で行われるべきだ。

システムの棚卸の作成ならびに最新状態維持が困難なことはよく知られている。理想は、要約した情報と詳細な情報を共にひとつの棚卸台帳として保持することである。大規模な組織では、単一の詳細な棚卸台帳を作成することが現実的でないかも知れない。高次の中央棚卸台帳が、詳細を記録したローカル・サイトの棚卸台帳へのリンクと併せて保持されているような、階層型の棚卸台帳の方が適している可能性が高い。

こうした棚卸台帳は機密情報源であり、攻撃者にとって極めて有益な情報となっている。したがって、これらの棚卸台帳は適切な手法により安全性を確保する必要がある。棚卸台帳にアクセスできる者を、その必要性を持つ最小限の人員に制限する必要がある。

**依存関係：**システム間のあらゆる依存関係を把握することが（範囲内外のシステムにとって）重要である。工業システムひとつを部分的に見ても、サプライ・チェーンの別のシステムからの出力に依存している場合がある。例えば、石油精製所は原油の供給をパイプラインに依存している。したがって、石油精製所の事業リスクを

決定する場合は、供給パイプラインなどの「上流工程」の依存関係をリスク評価で十分に考慮しておく必要がある。「下流工程」の依存関係についても同様に考慮すべきである。上記の例を拡大して石油精製所から出る副産物を使用する化学薬品工場もターゲットとして含めると、この化学薬品工場は「下流工程」の依存関係に相当し、リスク評価においてある程度綿密な調査を行うことが必要とされる。

### 3.4.2 事業リスクの評価

事業リスクを定義する様々な方法がある。ひとつの有用な定義は、リスク発生の可能性と、そのリスク発生の結果として予想される影響との関数でリスクを表すものである。

事業リスク = F（可能性x 影響）[2] (1)

リスク発生の可能性は、脅威と、標的の魅力、脆弱性の 3 つの因子を使って表すことができる。

可能性 = F（脅威 x 魅力 x 脆弱性） (2)

「魅力」は、潜在的な攻撃者にとって標的がどの程度魅力のあるものかを示している。一例を挙げれば、ある攻撃者は、ペーパー・バッグ製造工場よりも原子力発電所の方が魅力的な標的だと考えるかもしれない。この「魅力」は、ワーム感染など、一部のリスクには適用されない場合がある。大部分のワームは無差別に感染するため、脆弱性を持ったシステムはすべてリスクに曝される。したがって、この場合は「魅力」が問題にはならない。

「魅力」は、リスク発生の可能性の大小に影響を及ぼす（つまり、魅力的な標的ほど攻撃を受けやすい）が、単純化を図るため「脅威」の因子に含められることも少なくない。

（1）と（2）を組み合わせることにより、事業リスクが「脅威」、「魅力」、「影響」、「脆弱性」で表される。

事業リスク = F（脅威 x 魅力 x 脆弱性 x 影響） (3)

事業リスクを理解する上で必要とされる他の要素については、この後のセクションで説明する。

[2] 固定化学拠点におけるセキュリティ脆弱性を分析・管理するための指針。 AIChE - 2003.

### 3.4.3 脅威の理解

プロセス制御セキュリティにとっての脅威は非常に数多く存在し、それらは多種多様な原因から発生している。一般的な脅威を考慮することは重要であるが、特定の企業や組織形態についても視野に入れる必要がある。例えば、世界でも特に不安定な地域で活動する石油企業は、英国国内だけで営業する運送会社とは別の傾向の脅威をもつ可能性がある。

考慮を要する脅威の原因には以下のようなものがある（ただし、これらに限定されるものではない）。

- ハッカー
- 内部の攻撃者
- 犯罪者
- 違法な情報ブローカー
- 不満を抱いているスタッフ
- 許可されていない行動をするスタッフ（例：インターネットへのアクセス）
- 企業スパイ
- 請負業者
- 外国のスパイ
- 組織犯罪集団
- テロリスト
- 抗議団体および活動家（例：環境保護、政治、動物保護）

考慮を要する脅威の種類には以下のようなものがある（ただし、これらに限定されるものではない）。

- ワーム（一般型、標的型）
- ハッカー（内部者、外部者、内部事情に精通する外部者）
- ウイルス
- トロイの木馬やバックドア
- ボットやスパイウエア
- 完全性の喪失
- 可用性の喪失（サービス不能）
- 機密性の喪失
- 権限を超えた制御

ここに挙げた脅威はやや一般的なものであるため、シナリオ例に当てはめて考えることが有効である。これにより、影響や、関係のある脆弱性をより具体的に考慮することができる。以下に結果のシナリオ例を示す。ただし、シナリオ例はこれらに限定されるものではない。

- 特定のオペレーティング・システム（例：Windows、Unix、VMS、他）をベースとするすべてのコンピュータのシステム破壊
- Ethernet/IP ネットワーク技術のシステム破壊
- プロセス制御システムの機能破壊（または機能縮小）
- プロセス制御システムと以下に挙げるものとの間の接続破壊
    - 企業ネットワーク
    - 他のシステム（例：サプライ・チェーン、実験システム、それ以外の企業）
    - リモート・フィールド・デバイス
- 悪意ある行動や不注意な行動により無許可で行われる設定値や構成の変更
- 権限を持つユーザの過失によるシステム構成の変更
- 不満を抱く被雇用者による攻撃
- 履歴データの完全性または可用性の喪失
- プロセスおよび関連情報の機密性喪失

### 3.4.4 影響の理解

脅威を脅威シナリオに置き換えると、そこから派生する影響がかなり考慮し易くなる。サイト別、システム別、サブ・システム別のシナリオをそれぞれ考慮し、特定のシステムに現実に発生する可能性がある影響について検討する。また、これに留まらず、その特定システムに依存するすべてのシステムに関しても考慮する。例えば、化学薬品工場の発電所を制御する DCS について検討する場合は、この DCS が損なわれた場合にその化学薬品工場の運営に及ぶ影響の度合を、安全面も含めて検討する。このような影響が判明した場合は、棚卸台帳および依存関係にそれを反映させる。

**影響の分類：**リスク評価では、発生し得る影響や脅威の結果を金銭的価値に置き換えて定量化することが一般的によく行われる。特に財務上のリスクを検討する場合には、このような手段を採るのが普通である。しかし、プロセス制御セキュリティ・リスクを検討するに当たっては、セキュリティ・インシデントに起因する財務上の影響を正確に特定することが難しい場合がある。財務上の影響を定量化することは、それ自体が一つの専門分野になっており、適切なセキュリティ対策を決定するためのプロセス制御セキュリティ・リスクの評価に必要な以上の大仕事になりうる。

リスクによる影響を簡易に判断するため、影響を、金銭としてではなく、事業特有の言葉で表現できる場合がよくある。例えば、プロセス制御システムが晒されている潜在的な脅威の影響を、そのシステムへの影響に置き換えて伝達できれば、リスクがずっと分かりやすくなる。例えば制御システムがワームに感染したことによる影響は、工場の操業停止決定という結果を招きかねない。

以下は、発生する可能性がある「実生活」への影響の記述例である。

***安全上、健康上、環境上の事象や設備損害*** － 人体への危害、環境破壊、設備損害のいずれかを招く事象。

***比較的重要性の低い安全上、健康上、環境上の事象を伴なう規制要件の不遵守***－ サイトにおいて規制要件が遵守されていない状態を招く事象。例えば、一貫した規制要件違反（例：化学薬品工場や石油精製所の操業開始時あるいは操業停止時における過度のフレアリング）や、規制履歴データの喪失。

***強制制御による運転停止*** － 非常停止システムが人を介さずに自動的に呼び出される結果となる事象。例えば、製造工程のビューの全体または一部が写らなくなった場合が挙げられる。

***選択制御による運転停止*** － サイトにおいて運転停止が選択される結果となる事象。例えば、製造工程のビューの全体または一部が写らなくなった場合が挙げられる。

***稼動効率の低下*** － 工場において、効率性や利益率が低い手法で操業を続けるかまたは減産する結果となる事象。例えば、原料の配合が変わると、製品は比較的効率の低い手法で製造される結果となる。

***影響なし*** － 操業への影響なし。

考慮する必要性のあるその他の影響は、以下のとおりである。

- 機密情報の喪失
- 国家の重要インフラの損壊
- 事業継続性の喪失
- 世評
- バリュー・チェーンやサプライ・チェーン

**影響の経時変化：**特定の脅威から生ずる影響について検討する場合は、その脅威が時間の経過と共にどのように変化するのかということを視野に入れることが重要となる。例えば、当初はわずかな影響しか与えないインシデントでも、長い期間を経ると、その影響の深刻さが増してしまうことがある。その一例が、環境監視情報の喪失である。この情報の喪失による影響は、短期的に見れば深刻なものではないが、長期的に見た場合、極めて重大なものとなることが予想される。これは、この情報の有効性と完全性について法的要件および規制要件が存在するからである。

**連続的影響：**同時発生または連続して発生する影響の結果を検討する必要がある。共通した原因の障害が原因とされる場合には、このことが特に重要となる。

### 3.4.5 脆弱性の理解

脆弱性の理解には、すべてのシステム要素（例：サーバ、ワークステーション、ネットワークインフラストラクチャ、他）を詳細に検討して現存する脆弱性を判断する作業が伴う。一般的に脆弱性を有する分野には以下のようなものがある（ただし、これらに限定されるものではない）。

- 他のシステムへの接続
- リモート・アクセス
- 物理的セキュリティ
- ウイルス対策保護
- アクセス制御
- パスワードおよびアカウント
- セキュリティ・パッチの適用
- システム監視
- システムの復元性および継続性
- 工場システム向けのコードを作成するサード・パーティ

システム全体のセキュリティを検討する際は、最も弱い部分で、システム全体の保護水準が決まるという点を念頭におくことが重要である。例えば、よく管理された厳重な構成のファイアウォールがあったとしても、保護がしっかりしていないモデムによる外部への接続が存在する場合は、ファイウォールが迂回されてしまうため、ファイアウォールを有するメリットがほとんどなくなってしまう。

### 3.4.6 事業リスク理解から得られるもの

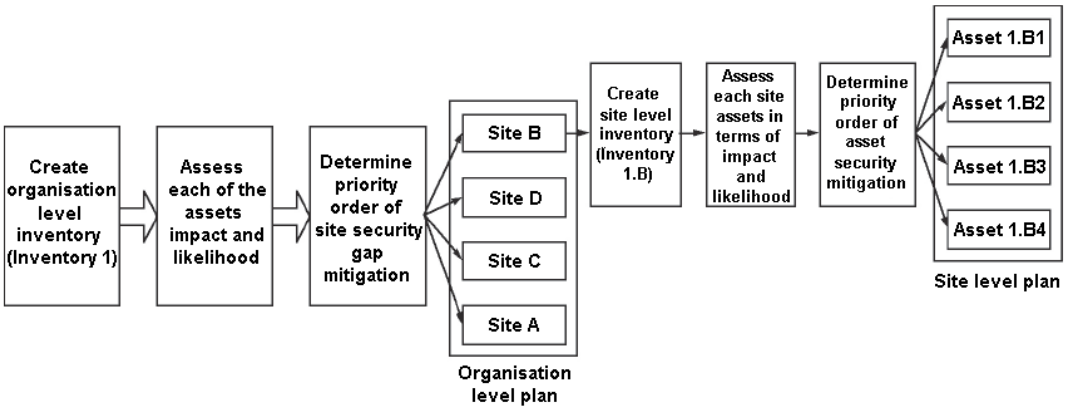
主に以下のものが得られる。

- システムの棚卸
- 優先順位が割り当てられたサイトおよびシステム
- 影響の評価に基づく主だった脅威のリスト
- 優先順位が割り当てられた脆弱性

## 3.5　リスク評価手法の適用

本手引きの大部分は、サイト・レベルやシステム・レベルに照準が合わせられている。多数のサイトや形態を有する大規模組織の場合、本手引きと同じレベルで調査することが実際的ではないことがある。よって、課題全体を、比較的管理しやすいタスクのレベルにまで小分けすることが必要となる。そのためには、図 5 のように、

まず高レベルで軽度のリスク評価を組織や企業の全体について実施し、次に、より詳細な評価をシステムやサイトそれぞれについて実施する。




| | |
|---|---|
| Create organisation level inventory (Inventory 1) | 組織全体レベルの棚卸（棚卸台帳 1） |
| Assess each of the assets impact and likelihood | それぞれの資産に対する影響と可能性を評価 |
| Determine priority order of site security gap mitigation | サイト・セキュリティのギャップ緩和に関する優先順位の決定 |
| Site B | サイト B |
| Site D | サイト D |
| Site C | サイト C |
| Site A | サイト A |
| Organisation level plan | 組織全体レベルの計画 |
| Create site level inventory (Inventory 1.B) | サイト・レベルの棚卸（棚卸台帳 1.B） |
| Assess each site assets in terms of impact and likelihood | サイトの各資産を影響と可能性の観点から評価 |
| Determine priority order of asset security mitigation | 資産のセキュリティ緩和に関する優先順位の決定 |
| Asset 1.B1 | 資産 1.B1 |
| Asset 1.B2 | 資産 1.B2 |
| Asset 1.B3 | 資産 1.B3 |

| | |
|---|---|
| Asset 1.B4 | 資産 1.B4 |
| Site level plan | サイト・レベルの計画 |

**図5 – 高レベルの企業リスク評価**

### 3.5.1 ステップ 1 - 企業についての高レベル・リスク評価

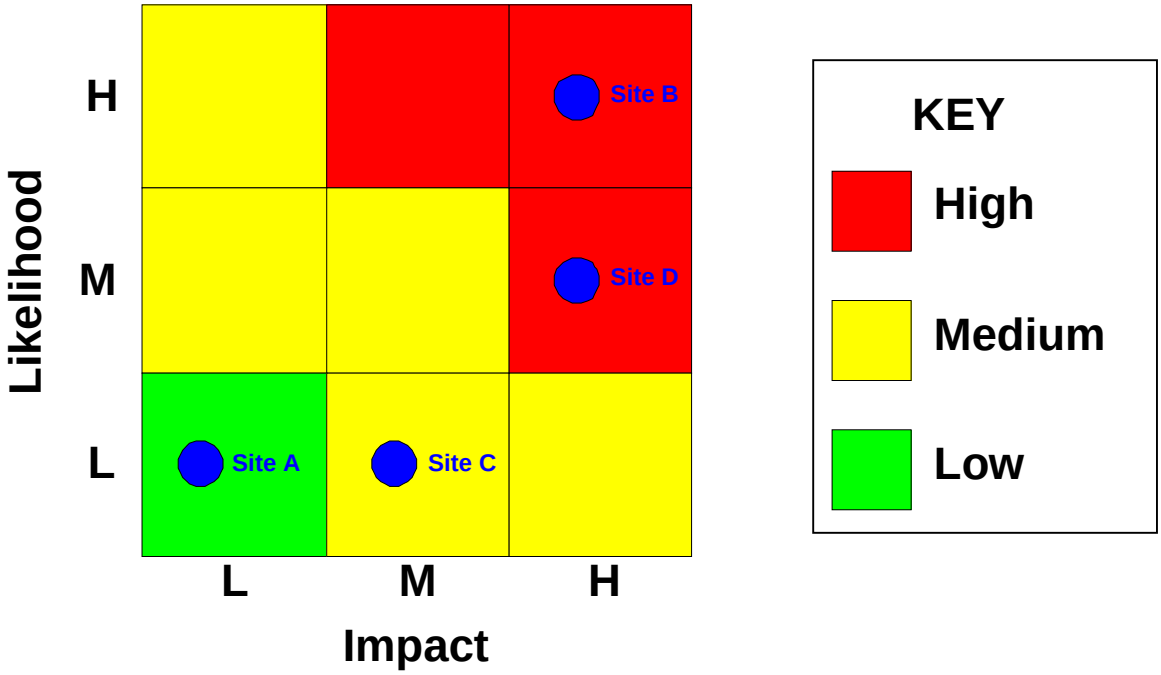
最初のリスク評価により、企業レベルから見たプロセス制御セキュリティ・リスクが判明する。このリスク評価では、「バリュー・チェーン」、相互依存関係、企業レベルでの重要性を備える影響を考慮して、企業に大きな影響を与えるセキュリティ・ギャップが示される。分析結果では、優先すべきセキュリティ問題と最初に取り組むべきサイトの両方が示される。

優先順位を決定する簡単な方法は、Boston Grid（リスク・マトリックス）上に資産スコアをプロットすることである。ここまでに取り上げたリスク・パラメータは、サイト・リスク表（表 1）に記入することができる。各因子（脅威、魅力、脆弱性）は、均等に重み付けされる場合もあれば、状況が反映されるよう重み付けされる場合もある。リスク・プロファイルが歪む可能性があるため、別々のサイトを集約するときは、それらのサイトで同一のリスク評価を使用するよう注意するべきである。

**表1 – サイト・リスク表**

| サイト | 脅威（T） | 魅力（A） | 脆弱性（V） | 可能性（T x A x V） | 影響（I） |
|---|---|---|---|---|---|
| サイト A | 中 | 低 | 低 | 低 | 低 |
| サイト B | 高 | 高 | 高 | 高 | 高 |
| サイト C | 低 | 低 | 低 | 低 | 中 |
| サイト D | 中 | 中 | 低 | 中 | 高 |

このリスク表に基づいて、「可能性」と「影響」の値による「ボストン・グリッド」（図 6）にサイトをプロットし、高リスクのサイトを示すことができる。また、サイトについて適切な優先順位を判断することができる。




| | |
|---|---|
| Likelihood | 可能性 |
| Impact | 影響 |
| L | 低 |
| M | 中 |
| H | 高 |
| Site A | サイトA |
| Site B | サイトB |
| Site C | サイトC |
| Site D | サイトD |
| KEY | 優先順位 |
| High | 高 |
| Medium | 中 |
| Low | 低 |

**図6 – 高レベルの企業リスク・マトリックス**

### 3.5.2 ステップ 2 - 個別サイト/システムのリスク評価

サイト・リスク評価は、高レベルの「企業」リスク評価に基づき、特定された主要なリスク領域についてまとめられる。サイト・リスク評価では、やや詳細なリスク分析を行うと共に、重要資産について詳細な検討を行う。

組織に対して、最初のサイト優先順位を選択した後は、同一のプロセスをサイト・レベルに適用することで、各サイトにおいてオンサイトの優先順位を決定することができる。各サイトでは、より詳細な棚卸がなされた後、個々の資産について、脅威、影響、脆弱性の観点から評価が行われる。この方法により、どの資産やサービスに最初に取り組むべきかという優先順位をサイトで決定することができるようになる。

企業リスク評価の実施後は、システム、脅威、影響、脆弱性を理解するためのプロセスと同じようなプロセスを、サイト、システム、資産の各レベルに適用して、このレベルに関係のある事業リスクを理解する必要がある。

## 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

本セクションでは、事業リスク評価を「通常業務」や現行の BAU（business as usual）保証に組み入れることについて述べる。このプロセスは、システムが現行基準を遵守しているということを保証する管理と関係しており、また許可されないシステム変更が実施されていないことを保証する。

## 4.2 原理

合意済みの事業リスク許容度に釣りあった適切なシステム・セキュリティを保証する。

## 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。

- 事業リスクは、脅威、影響、脆弱性と相関関係にある。パラメータの変化（例：システム変更）は、事業リスクを変化させる可能性がある。したがって、すべてのパラメータの変化の特定、事業リスクの再評価、適切なセキュリティ改善への着手のためには、継続的なリスク管理プロセスが必要とされる。

## 4.4 グッド・プラクティスの手引き

事業リスク評価の実施は極めて長いプロセスとなる場合がある。また、多数の利害関係者や人的資源からの情報源が必要となる。評価プロセスを開始する「トリガー」を定義することにより、必要な場合にのみこのプロセスが実行されることが保証できる。なおこのようなトリガーは、プロセスの種類、現行のセキュリティ・レベルおよびアーキテクチャ、リソース、などに応じて組織ごとに異なる。一般的なトリガーの例は、次に示すようなものとなる。

- 変化
    - 脅威レベルに対するもの
    - リスク許容度に対するもの
- システムの重要度およびリスク
- 遵守保証の要求
- 新規プロジェクト

- システム変更
- 合併や買収
- 政治的状況（例：特に発展途上国において、政府の交代によりその国のインフラストラクチャの安定度が変動することがある。このため政府の交代を要因に入れておく必要がある）
- 時間経過
- 主要インシデント

事業リスクの再評価後は、多くの項目についても再評価を行い、これらの項目が現在も全体の事業リスクに沿ったものであるかどうかを確認することが重要である。再評価が必要な項目には以下のようなものがある。

- **プロセス制御セキュリティ・プログラム** – 全体としての方向性が現在も事業リスクに適用していることを確認する。
- **管理** – 構造や構成が事業リスクの要求に適合していることを確認する。
- **棚卸** – 棚卸台帳の変更は、その変更の内容を問わず正式な変更要求と変更制御を通過させる必要がある。またその変更内容は、適切な利害関係者に通知される。
- **対応計画** – 現行のシステムやプロセスを正確に反映する必要がある。

再評価のプロセスは、通常、リソースを多用する。また、重要なシステムに対するリスクに比例した関係となっている必要がある。サイト、システム、資産をそれぞれ毎年検討するといったセキュリティ評価の標準ルーチンを構築する上で自然な傾向が存在している。しかし、これはリソースの最も効果的な使用とはいえない。サイトによって、検討の回数が多過ぎたり、少な過ぎたりする場合があるからである。再評価の頻度は、システムの重要度や、企業やサプライ・チェーンに与える影響に適した回数とすること。事業リスクの毎回の再評価に基づく主要な成果のひとつに、リスク再評価の実行頻度に関する指標がある。

## 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