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 3. 対応能力の確立

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 3. ESTABLISH RESPONSE CAPABILITIES" 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。

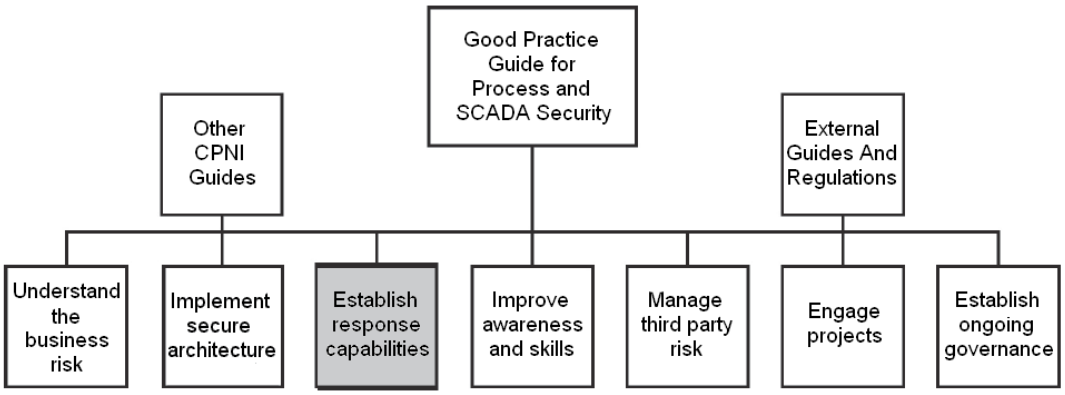
1.3 プロセス制御セキュリティ・フレームワーク

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『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処する 7 つの要素で構成されたフレームワークを提案している。本ガイド「対応能力の確立」は、高度なフレームワークで提供される基盤に基づいており、プロセス制御と SCADA システムにおける、デジタル・セキュリティ脅威に関する対応能力の確立に関するガイドを示す。

本ガイドは、詳細な対応計画や手順については言及していない。対応計画や手順は組織ごと、およびシステムごとで異なるためである。

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. 対応機能の確立についての要約

プロセス制御環境を採用している組織は、ディザスタ・リカバリ（DR）と事業継続性計画（BCP）を既に整えていることとなる。しかし、既に説明したように、プロセス制御オペレーション環境に変更が生じることにより、こうした計画は、電子攻撃の脅威に対処する上で不十分なものとなることが少なくない。

情報セキュリティでシステムを完全に保護することはできない。なぜなら、技術的脆弱性および非技術的脆弱性の両方が、保護セキュリティ体制とは無関係に存在し続けるからである。したがって、情報セキュリティ戦略では、脅威のあらゆる変化を特定して対応する機能に加え、システムの残余リスクが存在し続けていて管理を必要としていることを認識することが不可欠である。

分析によれば、電子攻撃の観点から見たプロセス制御セキュリティ・インシデントは、発生自体が稀な上、それにより引き起こされる被害は最小限に留まるとされていた。しかし現在、そのようなインシデントは以前よりも発生回数が増えており[3]、組織ではこれに備えた計画を立てる必要性に迫られている。計画を立てる上では、保護セキュリティ体制の立て直しと、インシデント対応の方針および手順の策定や見直しの両方を行うこととなる。

考慮すべき問題のひとつは、オフィス環境に適用されるような標準的情報セキュリティ・アプローチが、プロセス制御システムに適さない場合があることである。そのようなシステムは、様々な課題や制約に直面することが多い。わずかな違いかも知れないが、それらを考慮することは、特に、情報セキュリティ要求の策定とインシデント対応計画の準備を行う上で重要である。

その一例として、セキュリティ・パッチの適用やソフトウエアのアップデートが挙げられる。これらについては、多くの場合、稼動中のシステムへの導入に先立ち、パッチのテストと認定がプロセス制御システムベンダーにおいて行われることが必要とされる。この間、システムは攻撃を受けやすい状態となる可能性がある。よって、パッチを適用しないことによる潜在的な脅威と適切な対策の必要性について検討を行う必要がある。

別な例を挙げてみると、これらのシステムは、しばしば、安全上重要な装置の制御を直接行うことがある。そして、侵入者を検出した場合には、信用できなくなったシステムを隔離することがよく行われる。これにより装置は、妨害を受けることなく、その機能を発揮し続けることが可能となる。従来の IT システムでは、このような場合に攻撃者がシステム内に残ることを許す場合がある。ただしその場合は、攻撃者の動向を監視して、訴訟を起こす場合に備えた情報収集を行ったり、脆弱性や、システムへのアクセスに使用された方法を理解したりする。

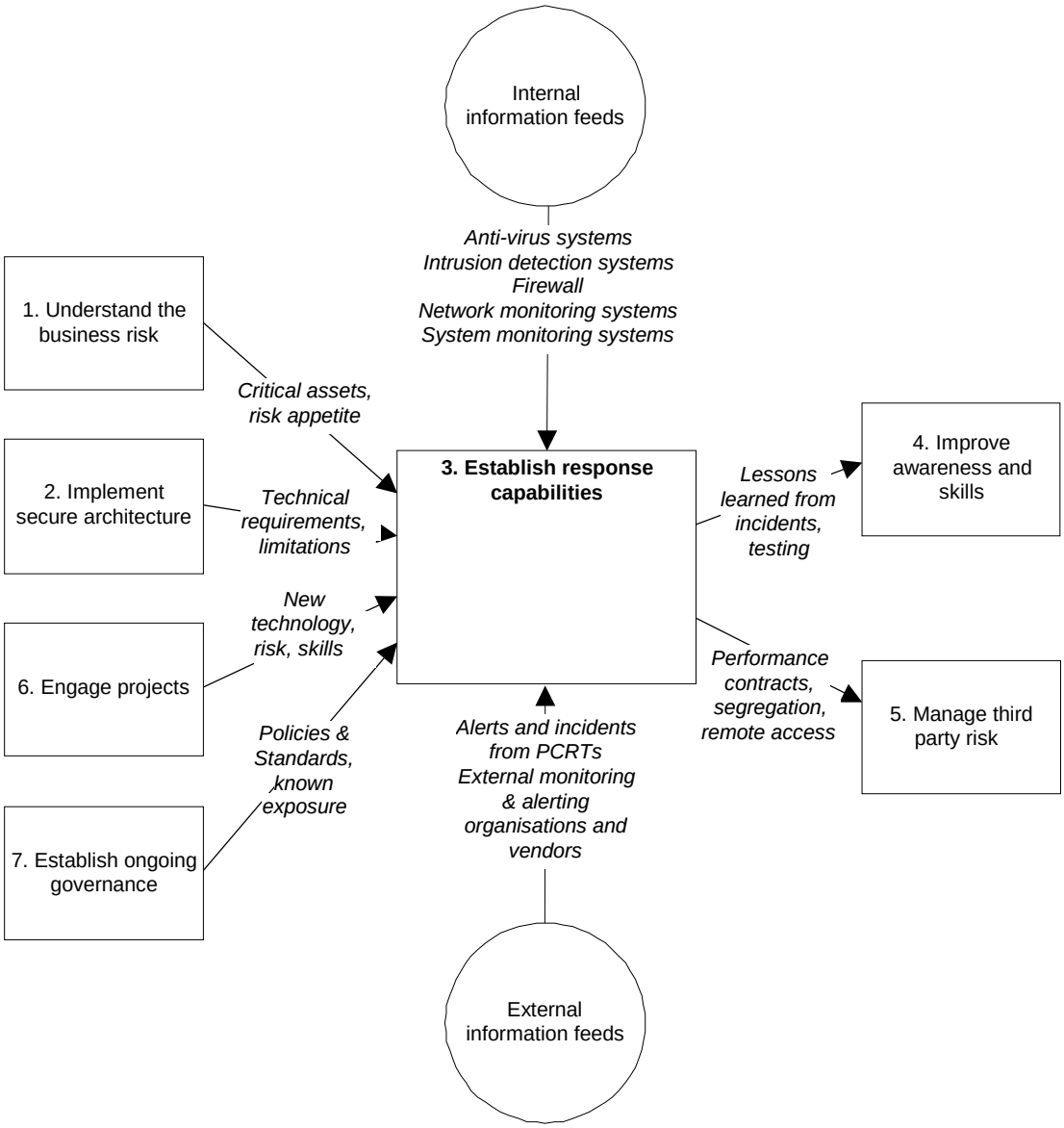
本グッド・プラクティス・フレームワークでは、全体を通じて 3 つの原則を指針として採用している。それは、保護、検出、対応の 3 原則である。本フレームワーク

[3] 2001 年から 2003 年にかけて発生したセキュリティ・インシデントのうち 70%は外的原因により発生したものである。これに対し、1982 年から 2000 年の期間に占める外的原因の割合は 31%であった。41%のインシデントは減産という結果を招き、さらに 29%については、プロセス監視機能が損なわれたことが報告されている – *The Myths and Facts behind Cyber Security Risks for Industrial Control Systems – Eric Byres & Justin Lowe*

に含まれる指針の大半は、様々なセキュリティ手段の導入によるプロセス制御システムの保護に関係している。本ガイドは、潜在的インシデントの検出と、インシデントの範囲および影響を最小化または完全に回避するための適切な対応の 2 つに重点を置いている。

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

効果的なインシデント対応機能を確立することは、本グッド・プラクティス・ガイダンス・フレームワークに含まれる他のすべての要素と密接に関係している。セキュリティ・イベントに対して効果的な対応を行うための機能は、セキュリティ関連イベントの監視・検出を行う機能と、直ちに使用可能な対応計画の特性に依存する。同様に、十分な安全確保と監視がなされたシステム、効果的で明確な管理、人材が持つスキルと意識にも依存する。



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
6. Engage projects	6. プロジェクトの予約

7. Establish ongoing governance	7. 継続管理の確立
Critical assets, risk appetite	重要資産、リスク許容度
Technical requirements, limitations	技術的要件、制約
New technology, risk, skills	新しい技術、リスク、スキル
Policies & Standards, known exposure	方針と基準、既知のエクスポージャー
Internal information feeds	内部における情報供給
Anti-virus systems	ウイルス対策システム
Intrusion detection systems	侵入検知システム
Firewall	ファイアウォール
Network monitoring systems	ネットワーク監視システム
System monitoring systems	システム監視システム
3. Establish response capabilities	3. 対応機能の確立
Alerts and incidents from PCRTs	PCRT による警告とインシデント
External monitoring & alerting organisations and vendors	監視・警告を行う外部の組織やベンダー
External information feeds	外部からの情報供給
Lessons learned from incidents, testing	インシデントから得た教訓、テスト
Performance contracts, segregation, remote access	パフォーマンス・コントラクト、隔離、リモート・アクセス
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

図2 – フレームワーク内における「対応機能の確立」の位置づけ

3.2 論理的根拠

警告とインシデントの両方に対応するための機能は、プロセス制御セキュリティ・フレームワークの重要な要素である。管理サポートの獲得、責任の決定、通信チャネルの確立、方針や手順の草案作成、事前定義された処理の特定、適切な訓練の実施、インシデント発生前における全プロセスの訓練。これらを実行することにより、

適切な対応を迅速かつ効果的に行って、事業への影響とそれに伴うコストを最小限に留めることができる。場合によっては、そのようなインシデントが将来発生することを回避できる。このような利点があるにもかかわらず、プロセス制御システムを網羅する包括的な電子攻撃対応計画を用意していない組織が多数存在する。

3.3 グッド・プラクティスの原則

最も重要な文書「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。

- セキュリティ・インシデントに対応するためのプロセス制御セキュリティ対応チーム（PCSRT）の編成
- 適切なインシデント対応と事業継続性計画がすべてのプロセス制御システムについて運用されていることの確保
- すべての電子セキュリティ計画について、保守、予行演習、テストが定期的に行われることの確保
- 適切な人材にセキュリティ警告とインシデントを通知する早期警告システムの確立
- セキュリティ警告とインシデントについて監視、評価、対応開始を行うためのプロセスおよび手順の確立。なお、対応としては、警戒の強化、システムの隔離、パッチの適用、プロセス制御システム対応チームの動員などが考えられる。
- すべてのプロセス制御セキュリティ・インシデントについて正式な報告と見直しが行われることの確保
- 得られた教訓をフィード・バックすることによる計画の改善ならびに方針と基準の更新

グッド・プラクティスの原則のさらなる詳細については、NISCCの「First Responders' Guide: Policy and Principles」を参照のこと。このガイドは、マルウエアへの感染やハッカーによるシステムへの侵入などのインシデントに備えた対応計画の確立に重点を置いている。もともとは従来のITを対象として起草されたものであるが、この文書に含まれている原則の多くはプロセス制御やSCADAシステムに転用することができる。

本「**対応機能の確立**」は「First Responders' Guide」に合わせたものとなっているが、例えばセキュリティ警告に対する対応やシステムへのパッチ適用などの一部の予防分野については、「First Responders' Guide」よりも詳細な説明を行っている。こうした予防は、企業の IT システムよりも、制御システム環境にとって、より大きな課題となる。

3.4 グッド・プラクティスの手引き

3.4.1 プロセス制御セキュリティ対応チーム（PCSRT）の編成

プロセス制御セキュリティ対応チーム（PCSRT）は、組織における対応機能の中核をなす要素であり、警告やインシデントへの対応について監視、分析、管理を効果的に行うための基礎となる。PCSRT は、状況の監視プロセス、電子攻撃に生じた変化の分析プロセス、適切な対応の開始プロセスにおいて、至る所に関与する必要がある。

PCSRT を成功させるための鍵は、適切な知識とスキルを備えた適切な人材の参加を確保することである。チームは、パートタイム制とフルタイム制のいずれでもよく、また、多数の事業分野の代表者を含む様々なソースから人材を招集することができる。その例としては、以下のものが挙げられる。

- プロセス制御、SCADA、オートメーション・チーム
- IT セキュリティ
- IT インフラストラクチャ
- 業務管理
- 運用
- 内部業務監査機関
- 法務部
- 企業の広報
- 企業のセキュリティ・チーム

組織における考慮事項

PCSRT は様々な方法で構築することができ、調整センター（CC）としての集中運営、各部署での運営、この 2 つを組み合わせた運営のいずれかが可能である。

大規模な組織では、イベントの監視と分析を実行可能な CC を設置することで、各部署に対する適切な行動のアドバイスと部署の行動調整を行える場合がある。CC では、インシデント対応に対するさらに優れたアプローチを提供することができる。CC は、理論上、他のグループの情報を共有・取得するために設置されるのが一般的だからである。なお、他のグループとしては、事業パートナー、ベンダー、他のインシデント対応チーム、法執行機関、NISCC のようなインフラストラクチャ保護チームなどが挙げられる。

CC はまた、多くの場合、個々の部署内チームの寄せ集めよりも少ないリソースで、効果の高い活動を年中無休で実施することができる。ただし、CC にもデメリットは存在する。例えば、ある部署のオペレーション環境やそこで作業に従事する者を十分に理解するには、当該部署に関する CC の知識が不十分な場合がある。

その穴を埋めるのが、部署内チームの知識である。このチームを構成するスタッフは、通常業務の傍らにパートタイムでインシデント対応任務を遂行している場合が

ある。部署内チームは、部署固有の問題やオペレーション環境に関する幅広い知識を持っている。

実際問題として、混合的アプローチが好ましい場合が少なくない。つまり、CC と、運用部署内のチームとが情報を共有することが好ましい。このようなモデルでは、日常の監視業務の実施に CC の効果が発揮されるため、各部署では、その中心となる通常業務に集中することができる。ただし、CC から勧告があった場合のインシデントや警告に対する対応は例外となる。

このような好ましい運用モデルとは関係なく、この分野では、運用、対人関係、技術、インシデント管理に関する必要なスキルを備えた人材の利用可能性が、1 つの大きな問題となっている。チームの効果を十分に発揮できるようにするには、その前に膨大な訓練を実施することが必要とされる。

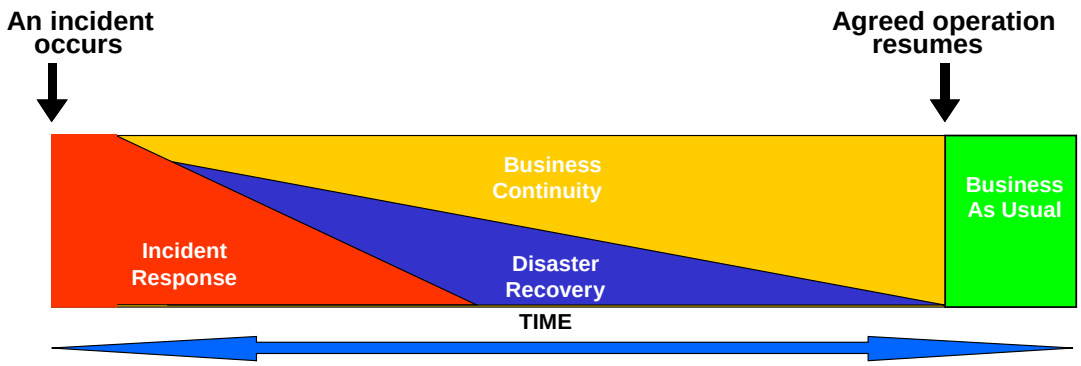
3.4.2 セキュリティ対応と継続性計画の確立

多くの組織では、多種多様な対応計画や継続性計画が存在している場合が少なくない。そのような計画には、事業継続性、ディザスタ・リカバリ、安全性、健康上および環境上のインシデント、組織や業界に特有のその他の緊急対策などがある。

しかしながら、既存の計画で制御システムの様々な潜在的脅威に十分対処できるケースはほとんどない。一言で言えば、電子攻撃による脅威は、既存の計画が最初に持ち上がった時点で、実際にはまったく認知されていなかったものである。例えば、制御センターを物理的インシデントから保護する目的でインストールされたディザスタ・リカバリ・システムを考えてみる。このディザスタ・リカバリ・システムをメイン制御センターと同じネットワークに接続したとすると、メイン・システムで発生したマルウエア・インシデントの影響はディザスタ・リカバリ・システムに及び、その結果、ディザスタ・リカバリ・システムは事実上役に立たなくなると考えられる。

電子攻撃インシデントの管理を既存の計画に組み込むことで、時間と労力を節約することは可能である。しかし、これには注意を要する。関係のあるすべてのプロセス制御の脅威が十分に網羅され、様々な計画が必ず十分に相互運用される必要がある。

インシデント対応、ディザスタ・リカバリ、事業継続性計画がどのように組み合わされるかについては、しばしば混乱が生じることがある。下記の図 3 は、これらの計画の一部についてその相互関係を示すものである。



An incident occurs	インシデントの発生
Agreed operation resumes	運用再開の合意
Incident Response	インシデント対応
Business Continuity	事業継続性
Disaster Recovery	ディザスタ・リカバリ
Business As Usual	通常業務
TIME	時間

図3 – 様々なタイプの対応計画

この図から、インシデント対応計画においてインシデント発生直後の短い時間がいかに重視されているかがわかる。インシデント対応計画では、直ちに処理を実行することにより、イベントへの対応を即座に行うことが焦点に置かれる。インシデントの推移に伴い、その焦点は、事業継続性（インシデント中の営業継続の確保）とディザスタ・リカバリ（失われたり損害を受けたりしたデータやシステムの復元）の開始へとシフトする。

プロセス制御システムのための効果的な対応計画の確立では、インシデント対応に重点を置く必要がある。それは、デジタル・セキュリティ・イベントは、予告なく突然発生する場合が少なくないからである。また、インシデントが発生（回避の可否にかかわらず）した場合にその影響を最小限に抑える上で、迅速かつ効果的な対応が要求されるからでもある。

3.4.3 インシデント対応計画の基本的内容

プロセス制御セキュリティ対応計画は、多くの場合、その範囲が極めて広い上、選択した運用モデル（例：CC または各部署）に従って立案することが必要とされる。ただし、最低限、以下の内容を含んでいる必要がある。

- インシデント報告方法に関する手順
- 対応計画の呼び出しプロセス
- 対応チームのメンバーの詳細、代表者、任務、職責、常時連絡可能な詳しい連絡先
- 重要な部署、システム、資産
- 予め特定した起こり得るシナリオに対する事前定義済みの手順（セクション▪を参照）
    - o 各シナリオの認定方法についての明確な定義
    - o シナリオが進行中と認定された場合の明確な行動計画

- 明確なエスカレーション経路、ならびにエスカレーションの許可要件
- 利用可能なサポート・ツールのリスト
- 連絡先情報（内部および外部のエージェント、企業、法執行機関、ベンダー、他）
- 明確な連絡計画
    - 連絡方法
    - 連絡事項
    - 連絡対象者
    - 連絡の時期および頻度
- インシデントを排除する上で満たすべき基準

3.4.4 計画について保守、予行演習、テストが定期的に行われることの保証

慎重に計画を立てたにもかかわらず、そうした計画や人材が現実の状況では予定と異なる動きをすることが少なくない。人材については、その全員に対して計画の実行時に訓練を実施する必要がある。また、計画については、定期的にテストを実施して予定通りに機能することを確認する必要がある。

この問題については、グッド・プラクティス・フレームワークの「**意識とスキルの改善**」要素において詳しく説明する。

重要なシステムや高リスクのシステムについては、計画の見直しを年に 1 回以上実施する必要がある。脅威や保護セキュリティ要求、システムそのもの、組織構造のいずれかに何らかの変更があった場合は、計画を修正する。また、演習中やインシデント発生後に得られた教訓についても、計画に組み込むことが必要とされる。

3.4.5 早期警告システムの確立

十分な定義と予行演習がなされた早期警告システムを備えることにより、組織では、セキュリティ警告とインシデントに対して迅速かつ効果的な対応を行い、コストと被害を最小限に抑えることが可能となる。

対応計画と継続性計画を準備している組織は多い。しかし、それらは、セキュリティ・インシデントを特定して適切な処理を決定し、対応計画を発動する上で効果がない場合が少なくない。

よく発生する問題は、組織の意思決定の基礎となる内部および外部の適切な情報へのアクセスがタイムリーに行われないというものである。また、効果的な処理を行えないほど大量の情報を受けてパンクしてしまうという問題もある。そのため、多くの組織が問題とその対処法に不安を抱えている。

高レベルなインシデントの優先順位付けプロセスの例について、その概略を図 4に示す。この図では、イベントに対する対応の中の 3 つの主要な段階について説明している。

- **監視** – 組織の内外から情報セキュリティ・データを収集すること。収集されるデータには、警告、ウイルス感染、脅威、パッチ通知、インシデント通知、ネットワークやパフォーマンス監視システムのデータなどがある。
- **分析** – 様々な情報源から収集した情報を多様なレベルと種類の潜在的脅威に分類し、対応を必要とするデータを取り出すこと。
- **対応** – 脅威の種類・分類や組織に関連のあるリスクに基づいて対応すること。

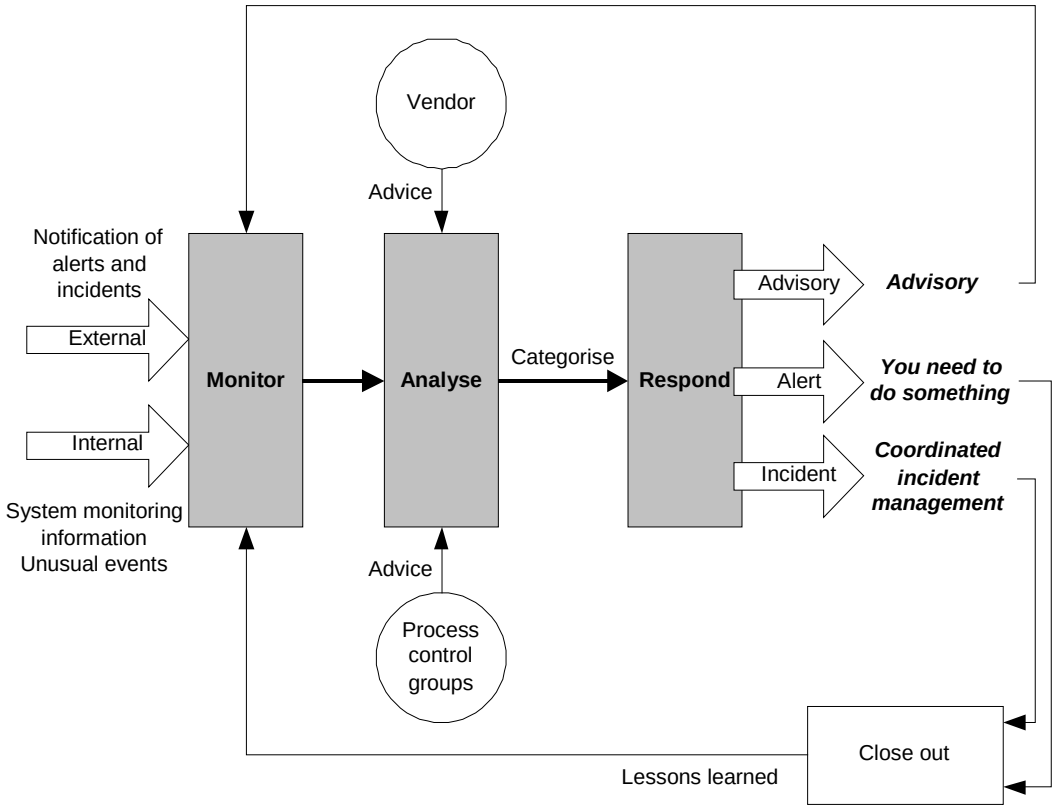


図 4 – プロセス制御セキュリティ対応の概要

Notification of alerts and incidents	警告とインシデントの通知
External	外部
Internal	内部
System monitoring information	システム監視情報
Unusual events	異常なイベント
Monitor	監視

Vendor	ベンダー
Advice	勧告
Analyse	分析
Advice	勧告
Process control groups	プロセス制御グループ
Categorise	分類
Respond	対応
Advisory	勧告
Alert	警告
Incident	インシデント
Advisory	勧告
You need to do something	何らかの対処が必要
Coordinated incident management	調和のとれたインシデント管理
Lessons learned	得られた教訓
Close out	排除

監視段階

正常な状態のオペレーションでは、内部と外部の両方の情報供給について、関連するイベント（例えば、セキュリティ警告、マルウエア、脆弱性の通知、異常なシステム動作など）の有無が監視される。利用可能なすべての断片的情報の処理（これにはリソースの大量消費が必要）と、重要な警告やインシデントを見逃さない十分なデータの収集との間のバランスが必要とされる。

監視は、システムに該当する脅威に合わせて行う必要がある。脅威に合わせたシステム監視を実施するには、セキュリティ警告を、プロセス制御システムの目録と照合する。大部分の組織では、一般的に利用される内外の標準的な情報源が多数存在する。その中の一部を以下に挙げる。

一般的な内部の情報源

内部の情報源としては、例えば以下のものが挙げられる。

- ファイアウォール監視システム
- 侵入検知システム
- システムとネットワークのパフォーマンス監視システム
- ウイルスとマルウエアに関する報告
- システム障害に関する報告
- ヘルプ・デスクからの報告

一般的な外部の情報源

外部の情報源としては、例えば以下のものが挙げられる。

- インフラストラクチャ保護チーム（例：NISCC）
- コンピュータ・セキュリティ・インシデント対応チーム（CSIRT）
- US-CERT
- CPNI Information Exchanges
- 制御システムベンダーやアプリケーション・ソフトウエア・ベンダー
- オペレーティング・システム・ベンダー
- ウイルス対策企業
- 外部のセキュリティ監視組織（例：ファイアウォールや IDS 監視の外部委託）
- 技術的媒体
- ニュースグループ
- セキュリティ・フォーラム
- 法執行機関

様々な監視者からの情報は、多種多様な形式で届けられる。例えば、未加工のシステム・ログ、電子メール、Web サイト、RSS フィード、書面、あるいは携帯電話からのテキスト・メッセージで届く場合もある。受け取ったデータを評価する作業には非常に時間がかかる場合がある。そのため、余分なデータを除外し、重要な情報だけをできるだけ明快な方法で表示させるプロセスを導入することは有意義である。

一部の専門組織では、特定組織のニーズに合わせた警告サービスを提供することがある。そのようなサービスにより、内部の監視システムにかかる負担は大幅に軽減される。残念ながら、このような情報は、プロセス制御システムに直接関係がある問題よりも、一般的な IT セキュリティ問題に焦点を当てていることが多い。また、情報の内容は技術的性格が極めて強く、効果的な分析を行うには熟練者が必要となる場合もある。

以下をはじめとして、情報の提供と入手の両方に使用可能な情報共有サービスが数多く存在する。

- WARPS
- CPNI information sharing.

参考文献は付録 A に示す。

分析段階

大量のシステム・データや内部/外部の情報供給を対象とする分析は、迅速かつ効果的に実施する必要がある。例えば、新たなワームによって問題が組織に提示されていることを判断するために 10 日もかかったのでは、ほとんど意味がない。とうの昔にシステムがその新ワームに感染してしまっている恐れがあるからである。

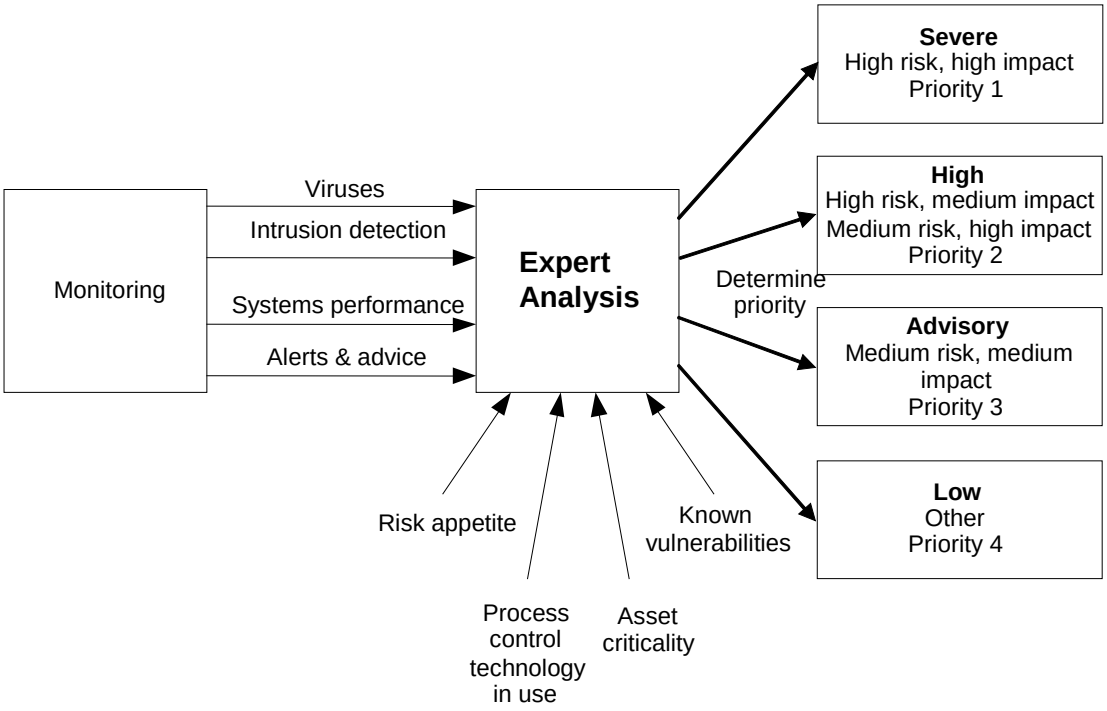
重要なのは、セキュリティ警告、インシデント報告、情報供給を分析できる専門知識を持った人材を備えることである。現在の制御システムは標準的 IT 技術を基礎としている場合が多い。しかしながら、環境が 2 つあれば、その間には相違が存在する。例えば、ネットワーキング・スキルとアプリケーション・ソフトウエアに関する知識を持った人材は、プロセス制御環境を除けば IT 問題全般を理解できる。プロセス制御環境については、そのシステムの知識を持った人材も採用することが必要となる。

警告に関しては、そのひとつひとつについて評価を行い、稼動中のプロセス制御システムに及ぶ可能性のある影響や、合意済みの適切な処理の有無を判断する必要がある。評価は複雑に入り組んでいることがあるため、評価結果の分析は、明快かつ簡潔な方法で表現してから PCSRT チームに伝える必要がある。そのための一方法として有効なのは、情報を例えば脅威（図 5）に基づいて分類する方法である。

- **重大** － 現在のインシデントまたは極めて大きな脅威（例：インターネット、企業、プロセス制御ネットワークなどにおけるワームの大発生）
- **高** － 危険度の高い脆弱性（例：重要な外部活動）
- **勧告** － 現時点において危険度の低い脆弱性であり、さらなる監視が必要（例：インターネット上の活動）
- **低** － 制御システムにとってわずかな直接的脅威（例：プロセス制御システムに電子メール機能が装備されていない場合における電子メール・ウイルス）

意思決定プロセスを簡略化するためには、それぞれの分類について事前に基準を定義して合意を済ませておくことが有用である。なお、必ずしもすべての脅威に事前定義基準を簡単に適用できるとは限らない。事前定義基準を適用できない脅威については、IT 専門家とプロセス制御専門家が経験に基づいて分析を行い、利用可能な情報の解釈と適切な意思決定を行う必要がある。

様々な脅威レベルの詳細な解説は US-CERT の文書に記載されている。参考文献は付録 A を参照のこと。



Monitoring	監視
Viruses	ウイルス
Intrusion detection	侵入検知
Systems performance	システム・パフォーマンス
Alerts & advice	警告と勧告
Expert Analysis	専門家による分析
Risk appetite	リスク許容度
Process control technology in use	使用中のプロセス制御技術
Asset criticality	資産の重要度
Known vulnerabilities	既知の脆弱性
Determine priority	優先順位の決定
Severe	重大
High risk, high impact	高リスク、影響度大
Priority 1	優先順位 1
High	高
High risk, medium impact	高リスク、影響度中

Medium risk, high impact	中程度のリスク、影響度大
Priority 2	優先順位 2
Advisory	勧告
Medium risk, medium impact	中程度のリスク、影響度中
Priority 3	優先順位 3
Low	低
Other	その他
Priority 4	優先順位 4

図5 – プロセス制御セキュリティにおける脅威データの分類

インシデント対応に際し、プロセス制御システムのベンダーを分析プロセスに巻き込むことが必要となる場合がある。例えば、特定のソフトウエア・パッチを適用することの是非についてベンダーの指示を仰いだり、脆弱性を持つソフトウエア・コンポーネントがシステムに使用されているか否かについてベンダーと議論したりすることが必要となる。

プロセス制御システムベンダーの多くは、稼動システムへの導入前に、パッチについてテストと認定を行うことを要求する。また、一部のベンダーでは現在、オペレーティング・システム・パッチがリリースされるとすぐに評価を自動的に実施し、パッチ導入の是非について助言を行っている。このような作業をベンダーが自動的に行ってくれない場合は、特に依頼してそうした評価を行ってもらう必要がある。制御システムに対するパッチ適用の指針については、セクション 3.4.6 で詳しく説明する。

対応段階

ここでは、インシデントへの適切な対応を時宜を得た方法で開始することについて説明する。通常は、先の分析段階の結果をトリガーとして対応が開始される。そのような状況の代表的なものを以下に挙げる。

- セキュリティ警告（例：発生するおそれがあるインシデント、ハッカー活動の増加、発生のおそれがあるマルウエア問題などに関する事前警告）
- 脆弱性の通知（例：制御システムに関する脆弱性確認やソフトウエア・パッチのリリースなど）
- マルウエア感染（例：制御システムにおけるワームやウイルスの検出）
- ハッカーの侵入（例：ハッカーにより制御システムが危険に曝されている）

3.4.6 プロセスおよび手順の確立

対応計画を作成する場合に考慮すべき事柄の例は、CPNI の『First Responders' Guide Policy and Principles』に記載されている。この文書の入手先については、付録 A を参照のこと。

プロセス制御対応計画に盛り込む手順では、運用環境、潜在的脅威、脆弱性、過去のインシデント経験を考慮する必要がある。対応計画に盛り込むことができる手順として思いつくものをいくつか以下に挙げる。

- マルウエア感染と削除
- ハッカー侵入疑惑
- サービス不能（DoS）攻撃
- 制御システムと他のネットワークとの接続解除（可能な場合）
- 制御システムと他のネットワークとの接続再確立
- プラントの状態確認不能（監視機能の喪失）
- プラントの制御不能（制御機能の喪失）
- 緊急ウイルス対策と侵入検知システムの署名更新
- 通常業務と緊急のセキュリティ・パッチ適用プロセス
- システムのバックアップと復元
- システム操作が正しいことの確認（システムが正常に稼動していることの検証手順）

以下のセクションでは、こうした手順の一部に関する考慮事項について検討を行う。

セキュリティ・パッチの適用

以前は、プロセス制御システムに対するセキュリティ・パッチの適用が重大問題となることは決してなかった。それは、プロセス制御システムが独自の技術を基礎としていたり、他のシステムから隔離されていたりしたことによるものである。パッチが実際に必要とされるのは、システムの更新やバグ修正を行う場合に限られていた。そのため、そうしたパッチの適用は、通常、整然としたインストール・プロセスの中に組み込むことが可能であった。

現在はほとんどの制御システムが標準の IT 技術を基礎としており、しかも他のシステムに接続されているため、危殆化や感染のリスクを背負っている。ファイアウォールなどの保護対策を制御システムに適用することは、防御における重要な要素である。ただし現在では、単一の強固な防御層に依存することは、プロセス制御システムの保護において適切なプラクティスとはみなされず、多層防御モデルが求められている。そのようなモデルにおいて重要となるのは、保護範囲内に存在するデバイスを様々な手段で確実に強化することである。その主要な手段のひとつが、セキュリティ・パッチの適用である。

パッチを適用すべきか、せざるべきか。それが問題だ。

セキュリティ警告やインシデントが発生した場合の主な検討事項は、セキュリティ・パッチを導入するか否かである。これはおおむね分析段階でのリスク評価を受けて行われる。ただし、パッチの適用がリスクと無縁なわけではない。そこには、パッチが原因でシステムの動作に異常が発生するかもしれないというリスクが存在する。また、パッチを導入しないリスクよりも、パッチを適用する上でシステムを生産から切り離す際の努力と混乱を重視する必要がある。可能であれば、システムは、パッチを簡単に適用できる設計とするべきである。例えば、デュアル・サーバを採用すれば、1 台のサーバにパッチを適用しながら、もう 1 台のサーバで動作を維持することができる。あるいは、テスト・サーバやバックアップ・サーバを用意する。これにより、システム上でパッチをテストしてから稼動システムに適用することが可能となる。

システムへのパッチ適用に対する一貫した取り組みと、パッチの規則正しい導入を実現するためには、対応計画に詳細なパッチ適用プロセスを盛り込む必要がある。詳細なパッチ適用プロセスを定める際には、多数の基準を考慮することが必要となる。

- パッチの適用が必要となる可能性があるシステムの特定（プロセス制御システムの目録から取得可能）
- システムにおけるパッチの適用可能性
  - ベンダーからの指示や要求
  - 注意：古くなった技術にはパッチを適用できない場合がある
- パッチを適用できないシステムに対してとり得る処置
  - システムの交換またはアップグレード
  - システムの物理的隔離
  - システムの隔離（例：正しく構成されたファイアウォールの内側に設置）
  - 侵入防止システムによるシステムの保護
- パッチ適用の優先順位
- システムにパッチを適用する順序
- パッチの導入方法
  - 通常業務の状況下
  - 緊急のパッチ適用プロセス
- パッチの導入と検査に関して利用可能なツールおよび適切なツール
- 導入前に必要なテスト
  - システムへのパッチ適用前におけるベンダー認定の必要性の有無
  - 現地保証テストをテスト装置や訓練システムで実施することの可否

- ベンダーの許可を得る前にパッチをシステムに適用することの可否

- 導入プロセスの補助に使用可能な保証ツールや導入ツールの有無（注意：これらのツールについては使用前にベンダーの認定を得ることが必要である）

一般的なパッチ管理の詳細については、CPNI の『Good Practice Guide Patch Management』（日本語版：「グッド・プラクティス・ガイド ― パッチ管理」）（付録 A 参照）というガイドに記載されている。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。

システムの復元と解析

システムが危険に曝されている場合（例：マルウエアやハッカーが原因）は、システムを復元するべきか、それとも詳しい調査を行うために隔離しておくべきか、という点で難しい決断を迫られることが少なくない。通常は、できるだけ早急にシステムを稼動状態へと復元する差し迫った必要がある。その一環として、たいていの場合に、システムの再構築やバックアップからのシステム復元が行われる。ただし残念なことに、システムの再構築やバックアップを行うと、攻撃者の残した手掛りや監査証跡はたいてい破壊されてしまう。そのため、犯人を追跡して裁判にかけることのできる機会がほぼ失われることとなる。このような状況では、あらゆる監査証跡を維持する（そして動作の回復を遅らせる）べきか、犯人追跡のチャンスを犠牲にして動作を回復するべきか、その決断が重要となる。予備システムや冗長システムを備えていれば、動作の回復を実現しつつ、被害を受けたコンピュータを隔離して後日分析にかけることができる。

インシデント後に組織が犯人を追跡する可能性がある場合、当該システムの隔離をインシデント対応計画に組み込んで、当該システムを確実に隔離できるようにするべきである。この項目自体は専門家の領域に含まれる。詳細については、CPNI の『An Introduction to Forensic Readiness Planning』という文書に記載されている。この文書の入手先については、付録 A を参照のこと。

3.4.7 インシデント報告の確立

プロセス制御セキュリティ・インシデントは、機密として保持される傾向が極めて強い。また、組織の場合は、インシデント情報を外部の機関に非公開とする傾向が強く見られる。これは、評判を守り、外部からの詮索を避けるためである。

しかし、インシデントに関する情報を共有することにはメリットがある。インシデント情報を共有することにより、他の機関における詳しい調査の実施、他の組織における同様のインシデント発生の回避、制御システムに迫るリスクについてのさらなる理解が可能となる。

プロセス制御セキュリティ・インシデントの経験を持つ組織は、（匿名などの適切な方法で）この情報を共有することが強く推奨される。CPNI は、CSIRTUK を通じ、電子、物理、人材のどのセキュリティ領域かを問わず、国家インフラストラクチャ組織から、セキュリティに関する潜在的な脆弱性、インシデント、イベントについて聞き取り調査を実施したいと考えている。この情報は秘密として扱われ、必要な

場合は、個人や組織を特定する事柄がなくなるよう削除した上で、一般的なセキュリティ・アドバイスに組み入れられる。CSIRTUK ヘルプ・デスクは、電子メール経由（アドレスは csirtuk@cpni.gsi.gov.uk）で連絡を取ることができる。機密情報は、暗号化されていない電子メールで送信するべきではない。機密情報の送信方法に関するアドバイスについては、ヘルプ・デスクに問い合わせること。

CSIRTUK は、インシデント防止における協力と連携の強化、インシデントに対する迅速な対応の促進、メンバー間および一般コミュニティにおける情報共有の充実を目的として FIRST（Forum of Incident Response and Security Teams）に加入し、他の国際的 IRT（Incident Response Teams）と親交がある。

3.4.8 インシデントから得た教訓の確認

デジタル・セキュリティ警告やインシデントに対する対応が要求された場合に、教訓や考えられるプロセスの改善事項がすべて必ず特定され、実行されるようにすることが重要である。これは、対応プロセスが絶えず改善されるようにするためである。

インシデント後の検討は中央とローカルの両方で行う必要がある。この検討がきっかけとなって、対応計画の更新、方針と基準の更新、企業リスク・プロファイルの更新が行われる。

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

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

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

DHS Control Systems Security Program
http://csrp.inl.gov/

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

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

ISA SP99, Manufacturing and Control Systems Security
http://www.isa.org/mstemplate.cfm?section=home&template=/TaggedPage/getStandards.cfm&MicrositeID=988&CommitteeID=6821

セクション 3.4.5

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

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

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

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

セクション 3.4.6

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

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

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