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 6. プロジェクトへの参画

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 6. ENGAGE PROJECTS" をご参照ください。

また、翻訳監修主体は本文書に記載されている情報により生じる損失または損害に対し、いかなる人物あるいは団体にも責任を負うものではありません。

なお、当文書に関わる最新情報は以下の CPNI のホームページをご参照ください。

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

目次

1.1 用語

本フレームワーク全体で、「プロセス制御システム」および「プロセス制御とSCADA」という用語は、すべての産業制御、プロセス制御、DCS、SCADA、産業オートメーション、その他関連する安全システムを含む、包括的な用語として使用する。

1.2 背景

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

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

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

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

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

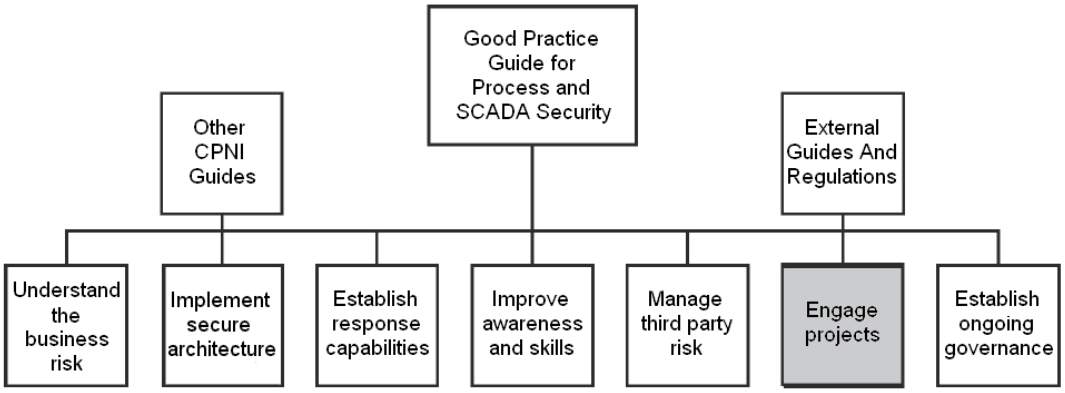
1.3 プロセス制御セキュリティ・フレームワーク

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

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

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

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



Good Practice Guide for Process and SCADA Security	プロセス制御と SCADA セキュリティに関するグッド・プラクティス
Other CPNI Guides	その他の CPNI ガイド
External Guides And Regulations	外部のガイドおよび規範
Understand the business risk	事業リスクの理解
Implement secure architecture	セキュア・アーキテクチャの実装
Establish response capabilities	対応能力の確立
Improve awareness and skills	意識とスキルの改善
Manage third party risk	サード・パーティ・リスクの管理
Engage projects	プロジェクトへの参画
Establish ongoing governance	継続した統制の確立

図1 –グッド・プラクティス・ガイドフレームワーク内における本ガイドの位置づけ

上記の要素はそれぞれ、個別の文書内で詳細に解説されている。本文書は、事業リスクの理解に関するグッド・プラクティスの手引きを示すものである。グッド・プラクティス・ガイド・フレームワークの文書はすべて、次のリンク先から入手できる。

http://www.cpni.gov.uk/ProtectingYourAssets/scada.aspx

1.4 本ガイドの目的

CPNIの「Good Practice Guide Process Control and SCADA Security」（日本語版：「グッド・プラクティス・ガイド ー 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「**プロジェクトへの参画**」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。

プロセス制御のセキュリティ要件の詳細はシステムごとに異なるため、本ガイドはこれらについては言及していない。

1.5 想定読者

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

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

2. プロジェクトへの参画についての要約

プロセス制御システムは普通、耐用年数が長く、その耐用年限中のシステム変更は、ごく少ないことを期待して設置される。しかし、使用しているすべての制御システムに対してこのように言うのは、たぶん一般化のし過ぎである。多くの組織では、大抵いつの時点でも、いくつかのプロセス制御システム関連のプロジェクトが実施されていて、セキュリティの問題を秘めている。

制御システムの新設、制御システムの変更、IT システムの変更、管理システム情報の更新と実装、新接続の導入などを伴うプロジェクトは、プロセス制御セキュリティ・リスクを持ち込むので、リスク評価の対象にすべきである。

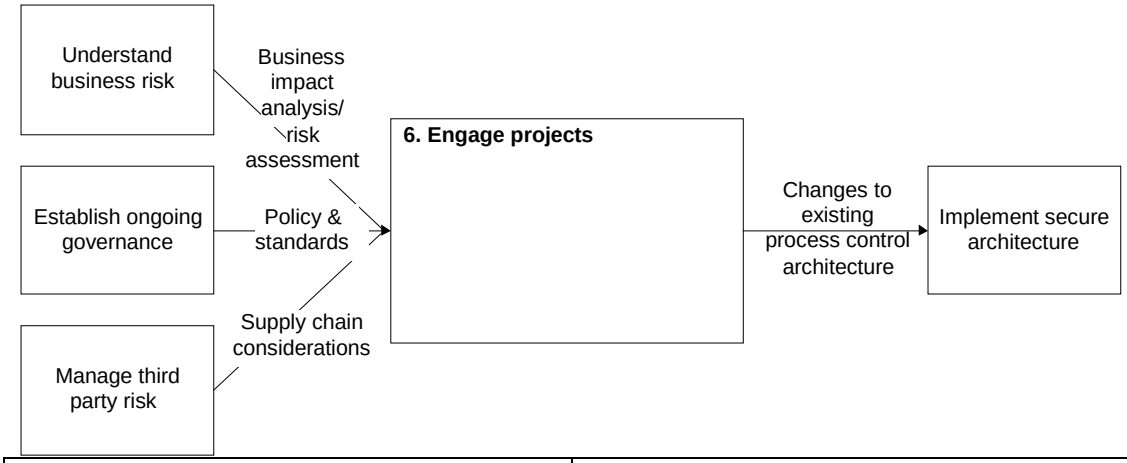
いったんシステムがリスク評価されると、それに影響を及ぼしうるプロジェクトはどれも、早い段階からプロジェクトにセキュリティを組み込めるように、関与する必要がある。「更地」の新システムは、設計の中にセキュリティ要件を組み込み、早い段階からプロセスを組み立てるべきであり、これらの要件が守られていることを、プロジェクト・ライフサイクルを通じて評価すべきである。

プロセス制御セキュリティの問題は大抵、プロジェクトの後の段階に追いやられる。この場合には、プロジェクトの早い段階で行われるプロジェクトの可能な選択肢の決定において、それぞれの選択肢のセキュリティ問題を検討しないことになる。要件仕様の早い段階でセキュリティを考慮しないと、プロジェクトの後の段階で時間とリソースに間違いなく影響を及ぼす、極めて重要な構成要素を放置していることになる。もっと深刻なことは、セキュリティ保護フレームワークの全体的効果も減らすことがある。

システムが構築され、使用状態になった後にそのシステムのセキュリティ保護対策を実施するのは大変困難で費用がかかることはよく知られている。更に重要なことは、稼働中のシステムにセキュリティ対策を施しても、効果が低いことが多いことである。プロジェクト開発プロセスの早い段階でセキュリティ・リスクに対する保護対策を組み込む方が、より効果的であるし、それにより見積価格の超過も防げるし、通常安くつく。

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

本ガイドは、ポリシーおよび標準、リスク評価、サード・パーティの検討事項に関して、グッド・プラクティス・ガイド・フレームワークからいくつかの他の要素を使用して、プロセス制御セキュリティ・プロジェクトへの参画に専用のガイドとして統合した。



Understand business risk	事業リスクの理解
Establish ongoing governance	継続した統制の確立
Manage third party risk	サード・パーティ・リスクの管理
Business impact analysis/risk assessment	事業影響の分析／リスクの評価
Policy & standards	ポリシーおよび標準
Supply chain considerations	サプライ・チェーンの考慮事項
6. Engage projects	6.1. プロジェクトへの参画
Changes to existing process control architecture	既存のプロセス制御アーキテクチャの変更
Implement secure architecture	セキュア・アーキテクチャの実装

図 2 – フレームワーク内における「1. プロジェクトへの参画」の位置づけ

3.2 論理的根拠

設計に良質のセキュリティ要件を埋め込むことにより、早い段階でプロセス制御システムの中にセキュリティを組み込み、プロセスを構築する。システム構築後にセキュリティを組み込むのは、効果がはるかに少なく、大抵費用が余計にかかる。

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。

- プロセス制御システムに影響を与えるすべてのプロジェクトを特定し、その開発の初期段階から参画する。
- プロジェクトの全ライフサイクルにわたってセキュリティ・リスク管理の責任者となるセキュリティ・アーキテクトを指名する。
- すべての購入契約に標準セキュリティ条項と仕様を含める。
- プロジェクトの設計と仕様にセキュリティ要件を含め、すべての適切なセキュリティ・ポリシーと標準が守られるようにする。
- プロジェクト開発の全ライフサイクルにわたってセキュリティ審査を実施する。例えば、人の健康と安全チェックと同時にセキュリティ審査を行う。
- プロジェクト開発ライフサイクルの重要なポイント（入札、試運転、工場での受入検査と試運転）でセキュリティ試験を行うよう計画する。

3.4 グッド・プラクティスの手引き

3.4.1 全プロセス制御プロジェクトの特定および参画

プロジェクトに関係するプロセス制御セキュリティ・リスクを効果的に管理するために、どのプロジェクトが計画され実施されているかをよく見通せることが必要である。多くの組織において、どのプロジェクト活動が計画され実施されているかを知ることは難しく、プロジェクト・ライフサイクルの終わりごろ、やっとプロジェクトが見つかるが、その時にはセキュリティ要件を組み込むのに遅すぎることがよくある。

プロセス制御セキュリティ考慮事項があるかもしれないプロジェクトを、早い段階で見つかるようにするプロセスを確立すべきである。プロセス制御要素がかかわるプロジェクトの登録または目録を維持すべきであり、それにより、すべてのプロジェクトが開発プロセスの中にセキュリティを組み込むように、プロジェクト開発プロセスを修正すべきである。

プロセス制御セキュリティが係わる可能性のあるプロジェクトの種類の例には、以下がある。

- 事業所内のファイアウォールの更新
- インフラストラクチャの更新または変更
- オフィス・ネットワークのインターネットへの接続
- オフィス・ネットワークのプロセス制御ネットワークへの接続
- 制御システムのアップグレードまたは取り替え
- 新制御システム

- 操作手順の変更
- 情報システム／ヒストリアンの更新
- 経営情報システム（MIS）、生産実行システム（MES）、生産高報告システム、プロセス・ヒストリアンの実装
- サード・パーティの接続
- 埋め込みコード（ファームウエア）の変更

3.4.2 セキュリティ・アーキテクトの参画

プロセス制御セキュリティに関係するプロジェクトでは、プロジェクト・ライフサイクルを通してセキュリティ問題に責任を持つセキュリティ・アーキテクトを任命すべきである。セキュリティ・アーキテクトは、そのプロジェクトに非常勤で働いてもよく、プロジェクトがどのようにセキュリティ要件を組み込むべきか助言し、引き渡されるシステムが適切に保護されていることを保証する。

ポリシーおよび標準のセキュリティ要件を、プロジェクト仕様の中に組み込むことのできる形に翻訳できる専門家を持つことは、極めて費用効率が高い決定である。セキュリティ問題に関する品質と責任を、設計とプロジェクト・ライフサイクルに組み込むことにより、プロセス制御セキュリティ要件が忘れ去られることがなく、プロジェクトの中で、決定事項がセキュリティにどう関係するかを常に認識させることができる。

3.4.3 セキュリティ要件を購入契約書に組み込む

セキュリティ条項は、思慮不足のため契約書から抜け落ちることが多く、あっても不適切なことがある。急いでセキュリティ要件をまとめるため、企業 IT 環境の仕様を殆ど考慮せずに「借用」することもある。また、セキュリティ事項を考慮するのが遅すぎて、購入契約書に一体化できないこともよくある。

早い段階でプロセス制御セキュリティ要件を明確にし、適切な条項を購入契約書内に含めることにより、セキュリティがシステムの基本的な要件の 1 つであるとベンダーが認識し、システムの一部としてセキュリティが組み込まれるはずである。

ソフトウエアのコーディング・エラーは脆弱性を生み出すおそれがある。これは、通常の IT アプリケーション・ソフトウエアはもちろん、制御システムにもあてはまる。購入契約書にセキュリティに関するコーディングを条項として含めることは、コードがセキュリティ上安全に開発され、テストが実行されるようにするうえで不可欠である。

購入契約書は、システム設計および実装で従うべき（社内または産業の）ポリシーや標準に言及すべきである。

契約書は、引き渡されるシステムに期待されるセキュリティ要件を詳細に述べるべきである。しかし、契約上の要件が規範的になり過ぎないように、詳細度のレベルを適正に設定することも重要である。契約書は、どの要件が必須であり、どの要件が任意であるかも明確に示すべきである。契約書内でどのセキュリティ条項が考慮

されるべきかについての詳しい手引として、フレームワーク要素「**サード・パーティ・リスクの管理**」を参考されたい。

購入契約書は、セキュリティ要件を提示することに加えて、ライフサイクルを通したセキュリティ保証に対する期待を明確に提示すべきである。この期待の例を以下に挙げる。

- ヘルスチェックのセキュリティ設計審査
- 安全なコーディングの確認
- セキュリティ試験
- データを格納する不良部品（例えばハーディスク）の安全な取替え

多くのベンダーが、ユーザから安全なシステムを提供しないとの非難を受けている。しかし、そのようなセキュリティ要件は、システム仕様書や購入契約書にめったに含まれていない。設計要件の中でセキュリティ要求が記述されていない場合に、提案の中に相当なセキュリティ対策を含めると、そのベンダーの提案は費用が高くなり、選定プロセスで不利なことがある。購入契約書の中でセキュリティ要件を明確に提示することにより、ユーザはセキュリティで期待することを明確に伝えることができ、競合ベンダー間に公平な競争条件を保証することができる。プロセス制御システムに対するセキュリティは、中核の要件であり、任意の余分のものではないと考えるべきである。

このセキュリティ要件に関する詳細なガイドについては、『Cyber Security Procurement Language for Control Systems』（Idaho National Laboratory 作成）および『Catalog of Control System Security Requirements』（DHS 作成）に記載されている。これらの文書へのリンクは付録 A に示す。

3.4.4 設計仕様書にセキュリティ要件を組み込む

プロジェクト段階で設計と構築プロセスの中にプロセス制御セキュリティを組み込むことは明白なことに見えるが、多くの組織で頻繁に見落とされたり、まったく行われなかったりしている。プロジェクト段階での比較的少ない投資をした方が、後でのセキュリティの付加、見積価額超過の処理、またはシステム全体に影響を及ぼす設計変更よりはるかに安くつく。

セキュリティ要件は、他の機能要件と同じに考慮すべきである。これらの要件は明確に表現し、どの機能設計仕様書にも含めるべきである。

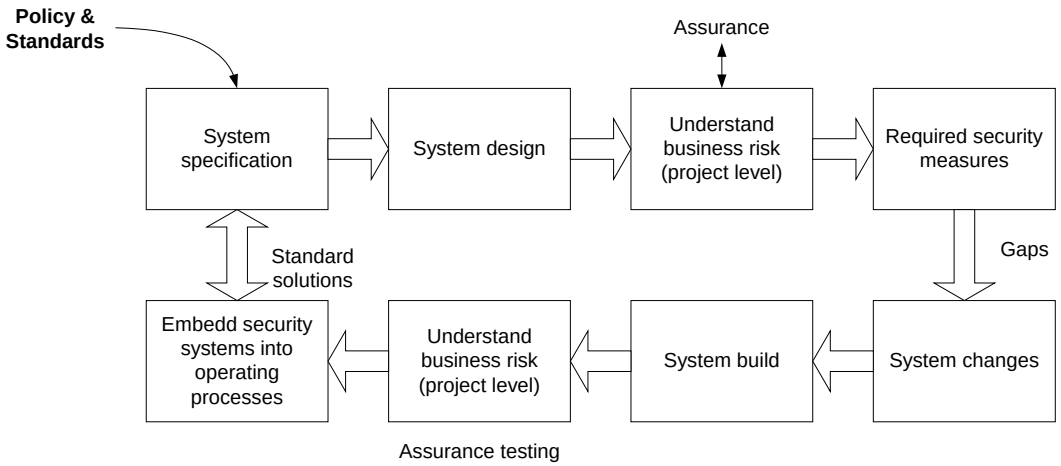
システムのセキュリティ要件は、事業リスクに基づくことが重要である。リスクの低いシステムは、より重要なシステムまたは高リスクのシステムよりセキュリティ防護は軽くてもよい。事業リスクが考慮されていない場合、システムが過剰に保護されていることもあるし（リソースの浪費で、そのリソースは他の所で有効に使用できたかもしれない）、システムが十分に保護されていない結果になることもある。

システム・セキュリティ要件を作成するとき考慮すべき項目のリストに関しては、組織のポリシーおよび標準ならびに「**セキュア・アーキテクチャの実装**」を参照されたい。

この要件に関する詳細なガイドについては、『Cyber Security Procurement Language for Control Systems』（Idaho National Laboratory 作成）および『Catalog of Control System Security Requirements』（DHS 作成）に記載されている。これらの文書へのリンクは付録 A に示す。

3.4.5 開発ライフサイクルを通したセキュリティの審査

セキュリティはプロジェクト・ライフサイクル全体を通して重要であるが、早い段階で特に考慮すべきである。下図は、開発ライフサイクルを通してセキュリティの問題をどのように考慮すべきかを示す。



Policy & Standards	ポリシーおよび標準
Assurance	保証
System specification	システム仕様
System design	システム設計
Understand business risk (project level)	事業リスクの理解（プロジェクト・レベル）
Required security measures	必要なセキュリティ対策
Standard solutions	標準ソリューション
Gaps	ギャップ
Embedded security systems into operating processes	運用プロセスに埋め込まれたセキュリティ・プロセス
System build	システム構築
System changes	システム変更
Assurance testing	確認試験

図 3 – 開発ライフサイクル内のセキュリティ

開発ライフサイクルにおける主な段階は以下のセクションで説明する。ライフサイクルの考慮事項に関する詳細なガイドについては、『Using Operational Security (OPSEC) to support a Cyber Security Culture in Control Systems Environments』（付録 A 参照）に記載されている。

3.4.6 システム設計セキュリティ審査

プロジェクトの設計が進み、大枠の設計とアーキテクチャが合意された段階に、その設計をセキュリティ仕様書および要件に照らして審査すべきである。この段階では、システムは存在しないが、この審査は、本物のシステムと類似のやり方を机上で演習する。詳しい手引きは、グッド・プラクティス・ガイド・フレームワーク・アーキテクチャの「事業リスクの理解」の中で述べている。審査では、提案された設計と、セキュリティ要件、仕様、ポリシーおよび標準との間の食い違い（ギャップ）を特定すべきである。

この審査の主要な目的は、設計が、ポリシーおよび標準、セキュリティ要件、仕様に準拠していることの保証である。もうひとつの目的は、セキュリティ・ギャップとリスクのリストであり、それは開発ライフサイクルのまだかなり早い段階で設計に組み込むように見直すか、または残されたリスクとして受入れるべきかを判断する。

開発サイクルの様々な異なる段階で、いくつかの審査が必要かもしれない。これは、システムの規模や複雑さ、および段階的に実装するかどうかに依存する。これらは、安全性の審査など既存のシステム審査に可能な限り組み込まれるか、情報を共有できるようにしておく。

3.4.7 システム試験

全体の試験計画の一部として考慮すべき、いくつかのセキュリティ事項がある。プロセス制御プロジェクト内では、セキュリティ試験は大抵、実装の非常に遅い段階まで考慮されないか、または、まったく含まれないことがある。非常に多くの場合、セキュリティ試験で予期しない脆弱性が見つかるが、脆弱性はライフサイクルの早い段階で特定することが重要である。

いったんプロセス制御システムが稼働すると、セキュリティ試験や脆弱性試験を実行することは非常に難しい。セキュリティ試験で、セキュリティ上の大事件を引き起こした例が記録されている。したがって、システム稼働前に、できるだけ多くのセキュリティ試験を実行することは大きな価値がある。この試験の結果は、システム稼働後のシステムの脆弱性管理体制にフィードバックできる。

したがって、セキュリティ試験は、プロジェクトの初期に計画し始めるべきであり、以下のセクションで記述する様々な領域を考慮すべきである。

システム試験の様々な段階において、現在実施している確認事項の他、未知の脆弱性に対処するための基準を決めておくべきである。この基準には少なくとも以下の項目を含めるべきである。

- IP アドレス

- ポート、プロトコル、サービス
- ホスト上で実行されるプロセス
- 標準的な動作パラメータ（例：CPU 使用率、ネットワーク帯域幅）

ユニット試験: セキュリティ試験の要素は、システム開発サイクルを通して含まれるべきである。システムをセクションまたはユニットで開発する場合、これらユニットの機能試験を行うことが多い。早い段階で問題を特定するために、セキュリティ試験を、これらの単体試験の中で計画すべきである。すなわち、問題が大きな影響を引き起こす前にライフサイクルの初期に取り組むようにする。

組込みシステム試験: 最近の調査で、組込みシステム、たとえば下位層のコントローラ、PLC、RTU などに広範囲な脆弱性があることが判明している。頻繁に引用されるのは、正規のセキュリティ・スキャンがその工場内の PLC の多くを破壊して、操業に大混乱を招いた製造会社の例である。特定された脆弱性の多くはごく小さいものかもしれないが、重大な脆弱性もあり、機器がどのように実装されるかによっては、安全に影響を及ぼす。

したがって、運用のため配備される前に、機器がセキュリティ試験で影響を受けないかの保証を得ることはグッド・プラクティスとして勧められる。PLC のセキュリティ試験を提供している組織も存在する（Mu Security や Wuridfech など）が、この種の試験を提供している組織の詳細は、付録 A に記載されている。

本ガイド執筆時点では、この保証を実行するための業界標準はなく（ただし、ISA が策定中）、この試験を実施する認定機関もない。しかし、制御装置レベルの試験専用の試験ツールが登場し始めている。配備する前に、入手可能なツールのいずれかを使用してこのような装置の試験を行うことをグッド・プラクティスとして推奨する。

工場受入検査: 通常の運用に入る（それ以降は試験が難しくなる）前にシステム全体を試験する大事な機会である。この段階は普通ベンダーの敷地で実行され、通常、顧客または（顧客に代わって）認定されたサード・パーティが実行する様々な受け入れ検査を含む。この試験は普通、プロジェクトの早い段階で規定された機能上の要件および仕様書に基づいて行う。システムが受け入れ検査をいったん通過すると、セキュリティ問題を是正するためにシステムを変更することは非常に難しいので、セキュリティ要件が機能要件に組み入れられたときに、セキュリティ試験も受け入れ試験に組み入れるべきである。

受入検査に含めることを考慮すべき主要項目は、以下の通りである。

- セキュリティ設定
- システム全体の脆弱性スキャン
- ペネトレーション試験
- ファイアウォール・ルール試験
- フェイルオーバ／障害回復試験
- バックアップ試験

- パッチ適用試験
- アンチウイルス更新試験
- リモート・アクセス試験
- システム強化確認

試運転試験: 受入検査に続いて、システムを実環境に組み入れ、通常はいくつかの試運転試験を実行し、システムが正しく設置および設定されていることを確認する。

これらの試運転試験には、セキュリティ要素も正しく構成されていることを確認するセキュリティ試験を含めるべきである。

試験の要件に関する詳細なガイドについては『Cyber Security Procurement Language for Control Systems』（Idaho National Laboratory 作成）に記載されている（付録 A 参照）。

3.4.8 システムの引渡し

大規模システム開発プロジェクトは通常、専門のプロジェクト・チームにが管理する。プロジェクト・チームはシステムの運用開始以降システムを管理保守する運用チームとは異なることが多い。運用チームにシステムを引き渡すプロセスの一環として、システムのセキュリティ・フレームワークのサポートに必要な、プロセスと手順がすべて体系化され、日常業務（business as usual）として以下のような要素が埋め込まれる必要がある。この例として以下がある。

- システム・ログの監視
- 日常保守業務
- ファイアウォールの管理および監視
- アンチウイルスの配備と確認
- 対応および業務継続計画
- 変更管理手順
- フェイルオーバ試験
- パッチ適用プロセス
- システム隔離
- ビュー喪失手順（loss of view procedures）
- 継続保証（フレームワーク・ガイドの「**事業リスクの理解**」を参照）
- ハードディスク上のすべてのソフトウエアと、ファームウエアの確認
- 最新のシステム文書
- 工場受入検査および試運転検査の結果

この項目に関する詳細な解説については、『Using Operational Security (OPSEC) to support a Cyber Security Culture in Control Systems Environments』（付録 A 参照）に記載されている。

3.4.9 廃棄

装置を置き換える場合、廃棄の問題に十分対処することが不可欠となる。プロセス制御システムの多くは、事業の競合相手、ID 窃盗などの犯罪者、テロリストなど、様々なグループにとって利用価値のある機密情報を含んでいる。例えば、スタッフの氏名と住所、パスワード、ユーザ・アカウント、電話番号、製品情報、顧客の詳細、データ保護法の対象となる情報、技術仕様、化学/生物学的データなどが機密情報に該当する。テロリスト・グループは、最後の 2 つの領域に関心を示すことが知られている。

デジタル・メディアは乱数データで複数回上書きし、元のデータを回復できないようにする必要がある。上書き処理は、ファイル・アロケーション・テーブルだけでなく、アドレス指定可能な場所のデータすべてを対象にするべきである。上書きという方法が使用できない場合は、強力な磁界を用いた消磁、または物理的な破壊によってメディアを破棄するべきである。

機密情報を含む資産の廃棄に関する詳細については、BS8470 に記載されている（付録 A 参照）。

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 **3.4.3**

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

セクション **3.4.5**

Using Operational Security (OPSEC) to Support a Cyber Security Culture in Control Environments
http://csrp.inl.gov/Documents/Opsec%20Rec%20Practice.pdf

セクション **3.4.7**

The Achilles Certification Program
http://www.wurldtech.com/cyber-security/achilles-certification/achilles-certification.aspx

MU Security Industrial Control (MUSIC) Certification
http://www.musecurity.com/support/music.html

セクション **3.4.8**

Using Operational Security (OPSEC) to Support a Cyber Security Culture in Control Environments
http://csrp.inl.gov/Documents/Opsec%20Rec%20Practice.pdf

セクション **3.4.9**

BS 8470:2006 Secure destruction of confidential material. Code of practice
http://shop.bsigroup.com/en/ProductDetail/?pid=000000000030127562

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