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 5. サード・パーティ・リスクの管理

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 5. MANAGE THIRD PARTY 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。

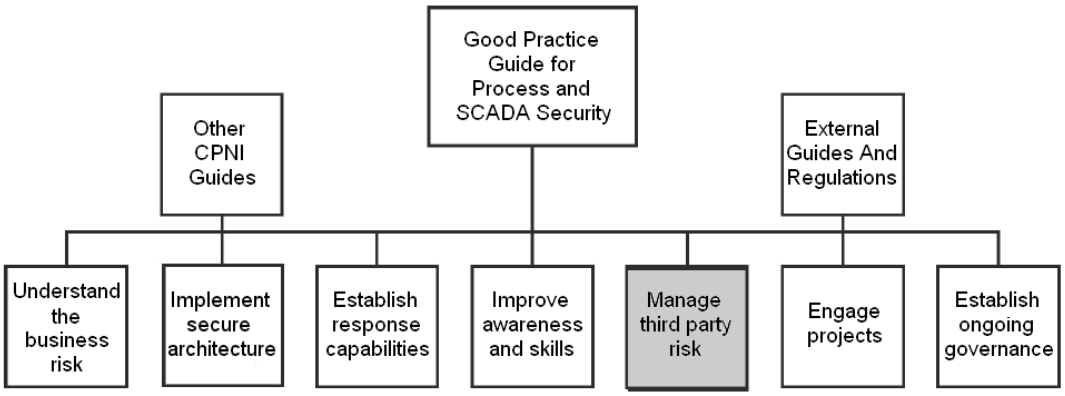
1.3 プロセス制御セキュリティ・フレームワーク

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

[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。

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。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「**サード・パーティ・リスクの管理**」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

2. サード・パーティ・リスクの管理についての要約

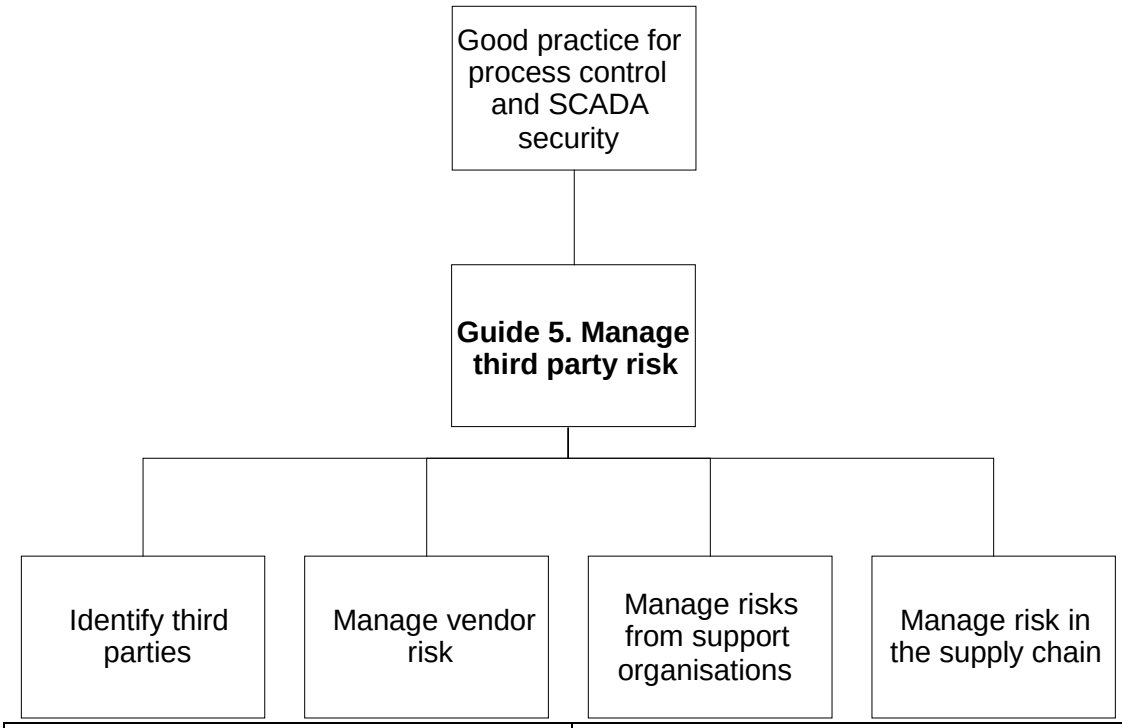
プロセス制御システムは、ベンダー、サポート組織、サプライ・チェーン内の他の関係者等のサード・パーティにより重大なセキュリティ・リスクがもたらされることがあるので、十分な注意を払う必要がある。ダイヤルアップ接続やインターネットのような容易に接続を設定できる技術は、組織外からの新しい脅威の種となる。したがって、サード・パーティもかかわりを持たせ、このようなリスクを減少するための手段を講じなければならない。

過去のプロセス制御システムは、大抵社内で書かれ、注文で作ったシステムであった。現在はほとんどの制御システムは、専門のサード・パーティとベンダーにより開発される。その結果、サード・パーティの製品とサービスが、ほぼすべてのプロセス制御システムの中に存在する。そのため、それらに付随するリスク要因も存在する。

サード・パーティ・リスクの認識し可視化することが、そのリスクを管理し始めることを可能にする鍵である。潜在的なセキュリティ・ギャップを認識することにより、特定されたリスクを緩和するため、ベンダーやサポート組織の適切な関与を求めることを可能にする。

プロセス制御システムについてのサード・パーティ・リスクは、運用中の制御システムへのリモート・アクセス接続だと一般的に考えられることが多い。しかし、全体像はこのような接続の懸念よりはるかに広いので、フレームワークの中で、このテーマを専門に扱うグッド・プラクティス・ガイドが必要である。サード・パーティには、制御システム・ベンダー、サポート・プロバイダ、サプライ・チェーン内の様々な要素などの、様々な種類がある。これらのそれぞれが、固有の問題を抱えている。

プロセス制御システムの脆弱性を考慮するとき、サプライ・チェーンを広く評価することの重要性を、うっかり見落としてしまうことがある。システムサポートを提供する見たところ人畜無害のシステムが、重要なシステムに大きな直接または間接の影響を及ぼすことがある。



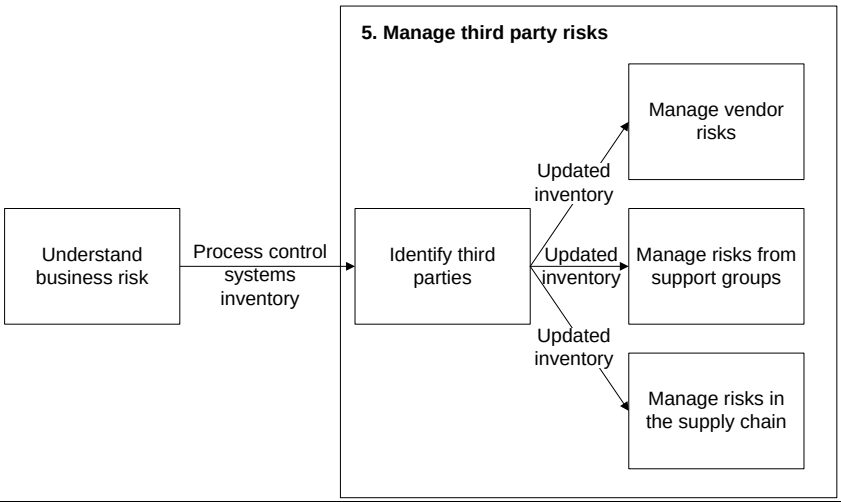
Good practice for process control and SCDA security	プロセス制御と SCADA のセキュリティに関するグッド・プラクティス
Guide 5. Manage third party risk	ガイド 5. サード・パーティ・リスクの管理
Identify third parties	サード・パーティの特定
Manage vendor risk	ベンダー・リスクの管理
Manage risks from support organisations	サポート組織リスクの管理
Manage risk in the supply chain	サプライ・チェーン・リスクの管理

図 2 – サード・パーティ・リスクの管理の文書構造

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

フレームワークの本要素は、プロセス制御システムのセキュリティに関連するすべてのサード・パーティを特定することがポイントである。これには、「**事業リスクの理解**」で製作されたプロセス制御セキュリティの目録を参照することを含む。リスクを適切に管理するのを確実にするために、関連するサード・パーティ・リスクを特定するためにその目録を参照する。

本「サード・パーティ・リスクの管理」内では、「サード・パーティの特定」は、残りの 3 セクションに対する基礎である。



Understand business risk	事業リスクの理解
Process control systems inventory	プロセス制御システムの目録
5. Manage third party risks	サード・パーティ・リスクの管理
Identify third parties	サード・パーティの特定
Updated inventory	更新された目録
Manage vendor risks	ベンダー・リスクの管理
Manage risks from support groups	サポート・グループからのリスクの管理
Manage risks in the supply chain	サプライ・チェーン内のリスクの管理

図 3 – フレームワーク内における「サード・パーティの特定」の位置づけ

3.2 論理的根拠

どのサード・パーティがプロセス制御資産に関連しているかを特定することにより、サード・パーティが引き起こすリスクに備え、軽減することができる。

3.3　グッド・プラクティスの原則

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

- プロセス制御システムと関係するベンダー、サービス・プロバイダ、サプライ・チェーン内の他の関係者を含めすべてのサード・パーティを特定する。

3.4　グッド・プラクティスの手引き

本セクションは、全サード・パーティを特定するための出発点となるプロセス制御システム目録を必要とする。プロセス制御システムの目録作成は、フレームワークの「**事業リスクの理解**」に記載されている。目録の各項目に対して、どのサード・パーティ（もしあれば）が各項目と関連しているかを決定する。1 つの目録項目がいくつかの異なるサード・パーティに関連することもある。この分析を実施するとき、以下の質問を考慮すべきである。

- システム・ベンダーは誰か?
- 誰がサポートを提供するか?
- どのようにサポートは提供されるか?
- どのようなサービスレベル協定（SLA）があるか?
- どの下請け業者が係わっているか?

定義:

ベンダー – 有料またはサービスとの交換で、ソフトウエア、ハードウエア、ファームウエアおよび／または文書を提供する人、企業またはインテグレータ。

サポート – プロセス制御システム「に関する能力の提供」または「と連係する」能力（例：システム監視、パスワードの再設定、問題、バグの修正等）。

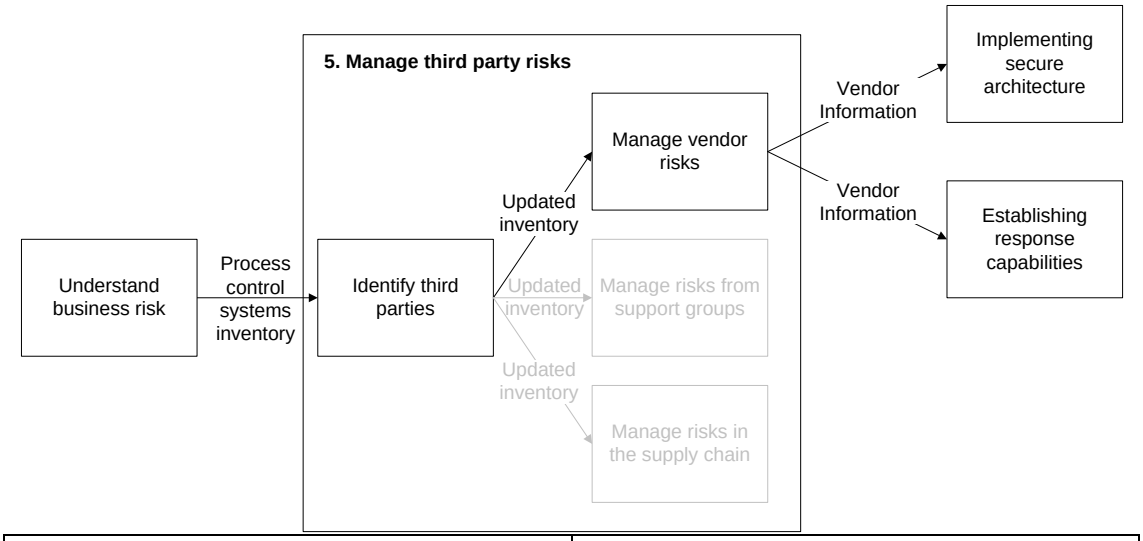
下請け業者 – サービスまたはタスクを実施するため、主契約業者と契約を結ぶ人または事業体。

最初のサード・パーティ目録見直しに要する期間は、作成されている目録の規模に完全に依存する。サード・パーティ・データを記録するとき、適切なバランスを取るように注意すべきである。記録するのが少な過ぎると、後の段階で更に分析を進めるのに十分でないかもしれない。記録するのが多過ぎると、維持するのが難しいだろう。目録照合中に十分に詳細なサード・パーティ情報が入手できなかった場合は、その情報は、フレームワークの本要素の一部として捜し出すべきである。新しい情報があれば目録に加えて、最新の状態に維持すべきである。

4. ベンダー・リスクの管理

4.1 フレームワーク内全体における本セクションの位置づけ

ベンダーからのリスクの管理は、前セクションの「サード・パーティの特定」の上に組み立てられ、特にプロセス制御システム・ベンダーと協力することに焦点を合わせている。本セクションからの出力は、「**セキュア・アーキテクチャの実装**」および「**対応能力の確立**」の中で使用される。



Understand business risk	事業リスクの理解
Process control systems inventory	プロセス制御システムの目録
5. Manage third party risks	サード・パーティ・リスクの管理
Identify third parties	サード・パーティの特定
Updated inventory	更新された目録
Manage vendor risks	ベンダー・リスクの管理
Manage risks from support groups	サポート・グループからのリスクの管理
Manage risks in the supply chain	サプライ・チェーン内のリスクの管理
Vendor information	ベンダー情報
Implementing secure architecture	セキュア・アーキテクチャの実装
Establishing response capabilities	対応能力の確立

図 4 – フレームワーク内における「ベンダー・リスクの管理」の位置づけ

4.2 論理的根拠

関係する制御システム・ベンダーとの良好な関係を築き上げることにより、ベンダーが問題を軽減するためセキュリティ要件に取り組むように影響を及ぼすことができ、可能な場合、将来の設計または製品のセキュリティ性能に影響を及ぼすことができる。

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 ー プロセス制御とSCADAセキュリティ」）に記載されている関連するグッド・プラクティスの原則は次の通りである。

- 契約前に全購入契約書の中にセキュリティ条項を詳細に確実に記載する。
- ベンダーが供給したシステム内に脆弱性が**現在**および**将来**発見された場合、それを特定し、速やかにユーザに通知するよう、すべてのベンダーと継続的に関係を維持する。
- 現在の制御システムに対するセキュリティ手引きと、将来のシステム開発に対するセキュリティ・ロードマップを提供するようベンダーに要求する。
- すべてのベンダーがそのプロセス制御システム内に適切なウイルス対策措置を組み込むようにさせる。
- 効果的なソフトウエア・パッチ・プロセスをベンダーと共に確立する。
- 稼働中のプロセス制御システムに対するベンダー・システムの強化手順についてベンダーと合意する。
- すべての脆弱性を管理できるように、プロセス制御システム内で使われているすべての要素技術（例、データベース）を特定する。
- すべてのベンダーについて定期的なセキュリティ審査と監査を実施する。

4.4 グッド・プラクティスの手引き

プロセス制御システム・ベンダーと生産的な対話を行うことにより、ベンダーとの良好な関係を築くことができ、ベンダーの製品およびサービスの能力と限界を更によく理解できる。この関係により、アプリケーションのユーザ固有の必要性と付随するセキュリティ要件について、ベンダーに更に詳しく伝えることができる。

ベンダーとの双方向の対話から利益を得られる主要なセキュリティの側面がある。これを次のセクションで述べる。

4.4.1 ベンダー・リスクを管理する契約上の措置

適切な契約上のフレームワークを作成することは、ベンダー・リスクを管理する上で不可欠の部分である。契約書作成の手間の多くは法務部門かまたは調達部門が行っていそうだが、固有のプロセス制御セキュリティ条項がベンダーとの契約書内に確実に含まれるようにすることは重要である。典型的なセキュリティ条項は以下を含む。

非開示の合意 – ベンダーはユーザのデリケートな情報に触れているかもしれないので、情報が悪用されないこと、ユーザの許可なく使用されないことが不可欠である。この情報は、ファイアウォール・ルールの理解からシステム情報および他の知的財産に及ぶことがある。

脆弱性の開示 – 適切な措置を取れるように、ベンダーが現在および将来発見する脆弱性をシステム所有者に伝達することは重要である。

身元調査／内部セキュリティ・チェック – ベンダーのスタッフが従業員としてまたは請負人として従事する前に、適切な身元のセキュリティ調査が済んでいる保証をベンダーに要求すべきである。雇用前のスクリーニングに関する詳細については、CPNI の Personnel Security Measures ウェブサイトに公開されている『A Good Practice Guide on Pre-Employment Screening』および BS7858 に記載されている。これらの文書の入手先については、付録 A を参照のこと。

ベンダー認定 – ベンダーの選定と認定の手続きにプロセス制御セキュリティ要件を組み込むことにより、望ましいセキュリティ文化と手法を調達の判断に組み込むことができる。その結果得られる承認されたベンダーのリストを作っておけば、作業の重複を減らすことができ、見込みのあるベンダーについての保証が得られるので、ユーザはコストと時間を節約することができる。ベンダーの視点からは、認定ベンダーリストに載れば、受注の可能性が増すので、リストに掲載されるよう努力する意欲が生まれる。

新プロジェクトに関するセキュリティ要件 – 新プロセスまたは新システムに関するプロジェクトを計画する場合、特に新規ベンダーの場合、契約の話し合いの中でセキュリティ要件を早くから含めることが不可欠である。ガイド 6．**プロジェクトへの参画**を参照のこと。

セキュリティ審査 – 定期的なセキュリティ実績審査をベンダーと行い、未解決のセキュリティの問題、軽減および改善計画の進捗状況を打ち合わせ、セキュリティ・ロードマップを話し合うべきである。

この主題の詳細については、Idaho National Laboratory による『Cyber Security Procurement Language for Control Systems』という文書に記載されている（付録 A 参照）。

4.4.2 考慮すべきベンダー関連の主要テーマ

ベンダーと協力することにより、ベンダー関連リスクを軽減する様々な方法がある。以下にその例を示す。

アンチウイルス – アンチウイルスによる保護が制御システムに確実に組み込まれるようにベンダーと協力する。

パッチ適用プロセス – セキュリティ・パッチを試験し認定するのにどのようなプロセスを使用するかをベンダーと合意する。考慮すべき質問を以下に挙げる。

- ベンダーはパッチを認定しているか?
- ベンダーは顧客に認定したパッチを通知し、配布するか?

- 認定するのにどれくらい期間がかかるか?
- 配布されるパッチにインストール指示書か手引きを付けるか?

ベンダーの中には、配布の承認前にセキュリティ・パッチの試験に十分な時間をかけるところもある。この項には、ベンダーから直接受取ったパッチやアップデートだけが、システムを更新するのに有効であるとの規定を含んでもよい。ただし、ユーザー側の変更管理やその他の都合によって、実際にユーザ側の環境のセキュリティが確保されるまでに遅延があることを、ベンダー側にも認識させることも重要である。

システム強化手引き – 大抵のプロセス制御システムと機器は、当初非常に「開放された状態」つまりすべての機能を使用できる状態にして提供される。ユーザの要件は比較的特定の限られたものであるので、残りの使用されない機能は、不要なセキュリティ・リスクを防ぐために使用不能にすることが重要である。システムの機能を不能にするまたは強化する手引きを提供するようベンダーに依頼すべきである。

要素技術 – プロセス制御アプリケーションの中には、セキュリティ・リスクを引き起こす恐れのある要素技術を使用しているものがある。データベース要素を有するいくつかのプロセス制御システムは、ユーザからは見えないが、パッチの適用と維持が必要なことがある。

リモート・サポート – ベンダーの関与を得て取り組む必要のある主要なリスク関連の課題として、リモート・サポートがある。リモート・サポートは、安全な接続を通して提供されるべきであるが、話はそれだけではない。接続を行うベンダーのシステムも、物理的かつ電子的に安全であるべきである。接続する要員は、身元調査を済ましてあり適切な訓練を終了しているべきであり、顧客の機密情報（システム文書等）はすべて適切に守られるべきである。ユーザは、これらのテーマについて保証（たぶん現場視察や監査を通じて）を求めるべきである。

セキュリティ試験 – ベンダー製品のセキュリティの脆弱性を特定し除去するために、ベンダー製品のセキュリティ試験を実施するように、ベンダーに働きかけるべきである。セキュリティ試験は、システム設計審査またはペネトレーション・テストの形態をとってもよい。最近の調査で、遠隔端末装置（RTU）やプログラマブル論理制御装置（PLC）などの低級制御機器にいくつかのセキュリティの脆弱性があることが明らかとなった。これらの低級制御機器が適切に試験され、セキュリティの脆弱性がないことの保証を求めるべきである。また、埋め込み制御機器の試験および保証についての手引きは、本シリーズのガイド 6 に記載がある。

システム通信方法の開示 – 使用されているプロトコルとともに、どのポートが使用されているかも列挙するように、ベンダーに働きかけるべきである。

4.4.3 セキュリティ文化へのベンダーの関与

ベンダーが提供する機能が、最低でもユーザの要件を満たすように、ユーザはベンダーのセキュリティ機能や考え方にも関与すべきである。具体的には、以下に示すような措置をベンダー協力のもとに行う。これらの働きかけの一部は強制してもよい。

- 定期的なセキュリティ審査

- セキュリティ監査
- セキュリティと意識向上の文化
- 脆弱性についての率直な対話
- ベンダーの改善に向けたセキュリティ・ロードマップ
- セキュリティ・ベンダーとの関係

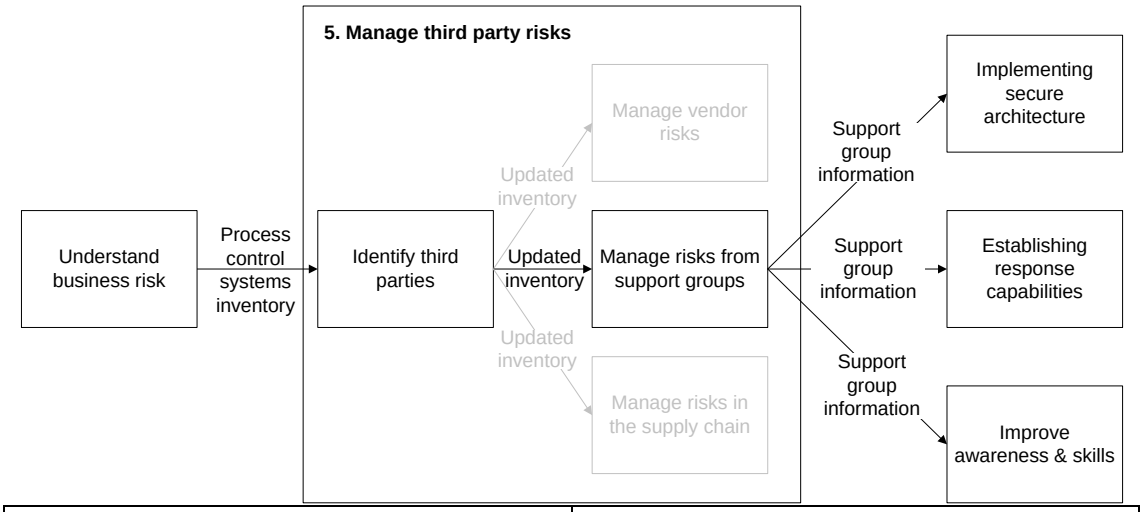
4.4.4 ベンダーのセキュリティ・ロードマップに影響を及ぼす

ベンダーと良好な仕事上の関係を築くことにより得られる主要な利点は、ベンダーのセキュリティ開発に向けた方向性とスケジュールを示すセキュリティ・ロードマップに、ユーザの意見を反映させることが可能になる点である。これにより、ベンダーは市場に関して貴重な洞察を得ることができ、ユーザはベンダーの製品とサービスの改善を通じて脆弱性を軽減することができるので、「win-win」の関係となる可能性がある。

実際、いくつかの主要ベンダーがアンチウイルス・ソフトウエアとオペレーティング・システムのパッチ認定について最近前進を見せたが、これには、プロセス制御システムのセキュリティ改善を目指すいくつかの大口ユーザがその購買力で影響を与えたことも影響している。ユーザは、ベンダーと対話を継続することで、その優先事項とプロセス制御システムのウイルス保護不在についての懸念を伝えることができた。いくつかのユーザからこれらの要件を伝えられたベンダーは、この分野の研究開発を正当化する事業モデルを作ることができ、結果として、制御システム製品のセキュリティ機能の向上につながった。

5.1 フレームワーク全体における本セクションの位置づけ

サポート組織からのリスクの管理は、特定されたサード・パーティの上に築かれ、特にサポート組織と協力することに焦点を合わせている。本セクションの出力は、グッド・プラクティス・フレームワーク内の「**セキュア・アーキテクチャの実装**」「**対応能力の確立**」「**意識とスキルの向上**」で使用されるだろう。



Understand business risk	事業リスクの理解
Process control systems inventory	プロセス制御システムの目録
5. Manage third party risks	サード・パーティ・リスクの管理
Identify third parties	サード・パーティの特定
Update inventory	目録の更新
Manage vendor risks	ベンダー・リスクの管理
Manage risks from support groups	サポート・グループからのリスクの管理
Manage risks in the supply chain	サプライ・チェーン内のリスクの管理
Support group information	ベンダー情報
Implementing secure architecture	セキュア・アーキテクチャの実装
Establishing response capabilities	対応能力の確立
Improve awareness & skill	意識とスキルの改善

図 5 – フレームワーク内における「サポート組織リスクの管理」の位置づけ

5.2 論理的根拠

サード・パーティ・サポート組織との関係を発展させることにより、付随する潜在的なセキュリティ・リスクを管理することができる。

5.3 グッド・プラクティスの原則

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

- サポート組織のリスクを定期的に評価し、必要な対策が確実に実施されるようにする。
- 起こりそうなセキュリティ侵害を防ぐまたは軽減する適切な対策が実施されるまで、サポート組織によるプロセス制御システムへのアクセスを防止する。接続条件を規定する契約書を作成し同意する。
- 企業プロセス制御システムと相互に作用するベンダー・システム内の脆弱性を現在および将来発見した場合、ベンダーが特定しユーザに通知することを確実にするため、継続して全サポート組織と連携する。
- サポート組織がサポートしているプロセス制御システムを十分に理解し、合意したセキュリティ手順に従ってそのサポートを行うことに同意するように、全サポート組織の意識を高める。

5.4 グッド・プラクティスの手引き

IT 環境内の多くの分野と同様に、何らかの方法でサード・パーティによりサポートされているプロセス制御システムは多い。その結果、プロセス制御システムのセキュリティはしばしば、以下に示すように、サポート組織とその提供するサービスに決定的に依存する。

- ネットワークと通信の提供とサポート
- IT インフラストラクチャの管理
- アプリケーションとシステムの監視とサポート

プロセス制御システムのサード・パーティ・サポートは、専門家のサポートを受けられると同時に、要員の訓練および採用に関連する費用を減らすこともできる。新技術や新サービスが導入されるとき、サード・パーティは、効果的なサポートを提供する適切なリソースが確実にあるようにしなければならない。

上記のよくあるサービスに加えて、サード・パーティが広範囲のセキュリティ・アーキテクチャの一環として、さらにセキュリティと管理サービスも提供するよう依頼するかもしれない。そのようなサービスには、以下の例がある。

- システム運用、セキュリティ、性能監視
- セキュリティ・パッチの適用
- ファイアウォールの管理と監視

- 侵入検知監視
- アンチウイルスによる保護
- 例えばログ監視、リモート・アクセス接続、パスワード変更等の定型的セキュリティ監視日常業務

どのサービスをサード・パーティにサポートしてもらうかは、システムの重要さ、必要なサポート、適切なスキルを持つ内部リソースの利用可能性、保守範囲に基づいて選定する必要がある。

アウトソーシングの詳細については、CPNI ガイドに記載されている。このガイドの入手先については付録 A 参照のこと。

プロセス制御システムをサポートするためサード・パーティ・サポート組織を雇うことは、セキュリティ・ソリューションの一部であるのと同じようにリスクを持ち込む。考慮すべき主要リスク分野を以下に挙げる。

- リモート・サポート接続
- 要員のセキュリティ
- 契約上の問題
- セキュリティ意識向上と訓練
- 物理的な安全
- 守秘義務

これらの各項目について、次のセクションで更に述べる。

サード・パーティ・サポート組織は大抵、制御システム・ベンダーと同様の機能とサービスを実施する。そのため、グッド・プラクティスの原則は、ベンダー・リスクの管理について作成された原則と非常に似ており、明確な契約上の合意、良好な仕事関係、はっきりした伝達経路が重要である。

5.4.1 リモート・サポート接続

サード・パーティ・サポート組織は、安全なプロセス制御システムに導入する新技術について、ユーザから許可を得なければならない。遠隔または時間外のサポートを可能にするモデムやルータなどの機器の付加は、潜在的なリスクであり、ユーザの事前承認を得た後でのみ使用し、適切に保護すべきである。便利とセキュリティの間にトレードオフがあり、サード・パーティの多くは、リモート・サポート使用による著しい価格割引を申し出るかもしれない。リモート・アクセス／サポートに付随するリスクを最小限に抑えるために、以下の事項を考慮しなければならない。

- 接続が防護されるまでアクセスを拒否する。
- アクセス権を定期的に審査および検査する。
- 接続に使用するサポート組織の設備とシステムも、物理的および電子的に確実に安全にする。

- 顧客のすべての機密情報（システム文書等）が、安全に保管されることを確実にする。
- ユーザは現場視察、審査、監査を通じて上記の項目についての保証を得たいと望んでもよい。
- 接続には時間制限を適用する。

5.4.2 要員のセキュリティ

どのシステム・セキュリティ・フレームワークにおいても、重要なのは人的要素である。サード・パーティのセキュリティを確実なものにするため、要員のセキュリティ面を考慮すべきである。

要員はすべて、サード・パーティの採用プロセスの決められた手順に則って、適切な身元セキュリティ調査を完了すべきである。

雇用前スクリーニングの詳細については、CPNI ガイドの『A Good Practice Guide on Pre-Employment Screening』および BS7858 に記載されている。これら文書の入手先については、付録 A を参照のこと。

CPNI は、雇用前スクリーニングだけでなく、従業員の継続的スクリーニングについてもアドバイスを提供している（付録 A 参照）。

5.4.3 ベンダー契約上の問題

サード・パーティ・サポート契約において考慮すべき、セキュリティ事項がある。

- **監査権** –サード・パーティのサービス、システム、施設を監査または審査する権利を保証する条項を含める。
- **情報の守秘義務** – 顧客の機密情報（システム文書等）の守秘義務を確実にする条項を含める。機密保持契約も確実に含める。
- **適正なサービスレベルの合意** – サービスレベルが契約書に明確に規定され、ユーザの要件に確実にふさわしいものにする。

5.4.4 セキュリティ意識と訓練

サード・パーティ・サポート要員は、適正なレベルのセキュリティ意識を持つべきである。全員がセキュリティの専門家である必要はないが、各人は、自分の役割を安全に果たすために、適切な技術面、手順面、運用面のセキュリティ意識を持つべきである。このテーマには以下の事項を含んでもよい。

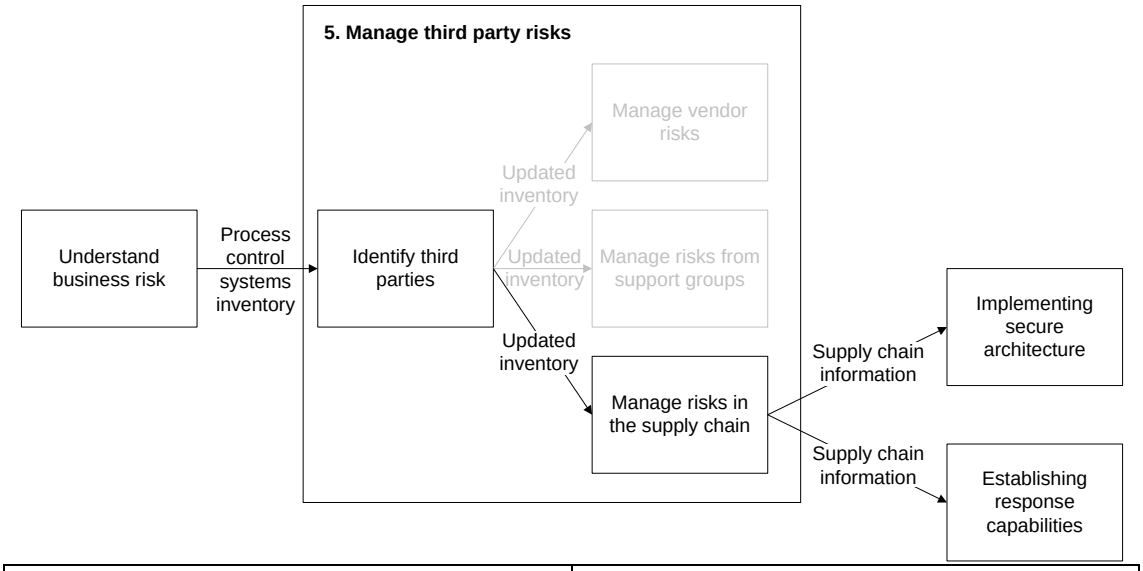
- **ポリシーおよび基準** – 要員すべてに、サポートしているシステムにどのポリシーおよび基準が適用されているかを確実に認識させる。
- **固有の事業セキュリティ・プロセス** – ユーザは、サード・パーティに伝達する必要のある固有のセキュリティ・プロセスを持っているかもしれない。
- **対応および業務継続計画** – サード・パーティ・サポート組織に、適切な対応および業務継続の計画を確実に用意させる。

- **スキル** – 要員がサポート機能を実施するための実践的スキルを有し、訓練を受けていることを確実にする。セキュリティとサポートに関するいくつかの産業標準資格が存在するが、要員が適切な実践的知識と公的資格の両方を有することの保証を得ることが重要である。

詳細については、グッド・プラクティス・ガイド『意識とスキルの改善』に記載されている。

6.1 フレームワーク全体における本セクションの位置づけ

フレームワークの本要素は、「**事業リスクの理解**」および付随するリスクの管理で特定されたサプライ・チェーン内の接続と依存関係の特定に焦点を合わせる。本要素の 2 つの主要な出力は、「**セキュア・アーキテクチャの実装**」および「**対応能力の確立**」である。



Understand business risk	事業リスクの理解
Process control systems inventory	プロセス制御システムの目録
5. Manage third party risks	サード・パーティ・リスクの管理
Identify third parties	サード・パーティの特定
Update inventory	目録の更新
Manage vendor risks	ベンダー・リスクの管理
Manage risks from support groups	サポート・グループからのリスクの管理
Manage risks in the supply chain	サプライ・チェーン内のリスクの管理
Supply chain information	サプライ・チェーン情報
Implementing secure architecture	セキュア・アーキテクチャの実装
Establishing response capabilities	対応能力の確立

図 6 – フレームワーク内における「サプライ・チェーン・リスク管理」の位置づけ

6.2 論理的根拠

プロセス制御システムをサプライ・チェーン内の他の要素に連結することにより、コストの低減と効率の向上等、著しい業務上の利点がもたらされる。しかし、そのような連結は、外部システムへのネットワークまたはシステムの接続を通じて、セキュリティ・リスクを持ち込むことがある。サプライ・チェーンに緊密に一体化すると、一層の依存関係が生まれ、サプライ・チェーン内の個別システムの途絶に対する、全体のチェーンの回復力が弱まる。その結果、サプライ・チェーン内の 1 システムのセキュリティ事象は、チェーン全体に影響を及ぼし、他の多くのシステムに混乱を引き起こす。いくつかの異なる会社に渡って混乱を引き起こすこともありうる。システムが大きなサプライ・チェーンの一部となっているところでは、上流と下流の依存関係を評価し、セキュリティ措置と対応能力を使用して全システムを適正に防護することが重要である。

6.3 グッド・プラクティスの原則

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

- サプライ・チェーンを通じてプロセス制御システムに連結された組織はすべて、それぞれのプロセス制御セキュリティ・リスクを管理しているとの保証を取り付ける。その組織の例には、サプライヤ、供給会社、製造会社、顧客またはジョイント・ベンチャーがある。

6.4 グッド・プラクティスの手引き

サプライ・チェーン・リスク管理の基本的要件は、サプライ・チェーンそれ自体と、その中に存在する依存関係を理解することである。サプライ・チェーンのクリティカル・パスも特定すべきである。システムまたは接続が、組織の境界をまたがるところでは、関連する当事者はセキュリティ責任の明確な取決めに合意すべきである。

サプライ・チェーン内の機能またはプロセスの多くが、自分が行う必要のあることだけを気に掛け、サプライ・チェーンを広く見たリスクを重要視しないという、自己中心的運用に流れる危険がある。

サプライ・チェーンの接続は、産業によって大きく変わる。サード・パーティ・サプライ・チェーン接続の例を以下に挙げる。

- 発電、配電、送電またはエネルギー取引システム間の接続
- 石油・ガス生産システムと取引システム間の接続
- 自動在庫発注システムとの接続
- パイプライン（上流および下流）との接続
- タンカー積み込み設備との接続
- 公益事業者（例、ガス、水道、電気、圧縮空気、蒸気）との接続
- 生産高報告のためのジョイント・ベンチャーとの接続

各サプライ・チェーンのインタフェースについて考慮すべき 2 つの主要リスク領域がある。

- インタフェース・セキュリティ
- サプライ・チェーン依存関係

6.4.1 インタフェース・セキュリティ

プロセス制御システム間のシステムのインタフェースは、制御システムへの裏口になる可能性があり、ウイルスやワームによる感染あるいは不正アクセスの経路となることがある。そのような接続は、シリアルライン、モデム接続、VPN、他のネットワーク、場合によってはインターネット経由の接続等、様々な形態がありうる。

そのような接続はすべて明確に特定し、プロセス制御システム目録に含め、システム図およびネットワーク図で文書化すべきであり、適切に保護および監視すべきである。対応および運用継続計画の一部として、切り離し計画も作成しておくべきである。

これらの接続については、インタフェース・セキュリティに加えて、以下に述べる依存関係についても考慮すべきである。

6.4.2 サプライ・チェーン依存関係

サプライ・チェーン内の各要素は、プロセス制御セキュリティの脅威に関して評価すべきである。重要な依存関係があるところ、すなわち自己のシステムが他のシステム（上流または下流）に依存しているところでは、それらのシステムがプロセス制御セキュリティの視点からどのように保護されているかについて、関連するサード・パーティに保証を求めるべきである。この保証を得るために、セキュリティ審査、ヘルスチェック、監査を行うことが考えられる。必要な場合には、各サプライ・チェーンの依存関係に対して、適正な対応および運用継続計画を設けるべきである。

付録 A： 本ガイドで使用した参考文献および参考ウェブサイト

セクション **4.4.1**

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

Personnel Security Measures
www.cpni.gov.uk/ProtectingYourAssets/personnelSecurity.aspx

BS 7858:2006: Security screening of individuals employed in a security environment. Code of practice
www.bsi-global.com/en/Standards-and-Publications/Industry-Sectors/Security/Security-Products/BS-78582006/

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

セクション **5.4.2**

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

Personnel Security Measures
www.cpni.gov.uk/ProtectingYourAssets/personnelSecurity.aspx

BS 7858:2006: Security screening of individuals employed in a security environment. Code of practice
www.bsi-global.com/en/Standards-and-Publications/Industry-Sectors/Security/Security-Products/BS-78582006/

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