CSMS システムインテグレータ向けガイド

－CSMS 認証基準（IEC 62443-2-1）対応－Ver.1.0

平成２８年１０月

一般財団法人日本情報経済社会推進協会

はじめに

産業用オートメーション及び制御システム（IACS：Industrial Automation and Control System）のセキュリティについては、製品面からの対策と関与する組織の管理体制面からの対策が重要であり、国際標準として IEC 62443 シリーズがあります。

当協会は、組織の管理体制面からの対策として、その国際標準である IEC 62443-2-1：2010 をベースに、2014 年に CSMS 認証基準（IEC 62443-2-1）を策定しました。

CSMS 認証の対象となる組織は、保有する IACS を活用して製品やサービスを提供する事業者（アセットオーナー）と、各種のコンポーネント（制御機器、装置等）を組み合わせて IACS を構築する事業者（システムインテグレータ）、さらにはその IACS の運用・保守を担う事業者になります。

IACS のセキュリティを高めるには、システムの構築・運用・保守に携わる上記の３つの事業者が協力し、三位一体となったセキュリティ管理を行うことが重要です。

特にシステムインテグレータは、システムのライフサイクルがスタートする時点において、セキュアな仕組みづくりに深く関与することから、セキュリティ強化のための重要な役割を担っているといえます。このようなシステムインテグレータの方々に向けて、IACS のセキュリティを守るための要求事項を新たに CSMS 認証基準へ加え、認証取得を目指す際の手引きとなるよう本書を作成しました。

本書を活用していただくことで、IACS のセキュリティに対する取り組みが広く普及し、産業分野全体におけるサイバーリスクの低減につながることを期待しています。

最後に、本書を作成するにあたり、制御システム SMS 専門部会の委員の皆様をはじめ、ご協力を頂いた関係各位に対し厚く御礼申し上げます。

平成 28 年 10 月

一般財団法人日本情報経済社会推進協会

目　次

1. CSMS の概要

1.1. 背景

IACS（Industrial Automation and Control System）とは「産業用オートメーション及び制御システム」のことであり、電力・ガス・石油等のエネルギー分野や、鉄鋼・化学等のプラント、鉄道・航空等の交通インフラ、電機・機械・食品等の生産ライン、商業施設・オフィスビル等の設備管理などで幅広く用いられています。

かつては独自のハードウェアやソフトウェアでシステムが構成されていましたが、現在では IT の進展でシステムのオープン化が進んでいます。一般的な情報システムと同様に、増大するセキュリティリスクに晒されているのが現実です。

しかしながら IACS の運用現場では、セキュリティに対する取り組みが十分に浸透しておらず、サイバー攻撃の被害が大規模かつ広範囲に拡大する危険をはらんでいます。IACS のセキュリティが思わぬ盲点となり、社会経済に大きな影響を及ぼすことが考えられるのです。

1.2. CSMS 認証とは

CSMS（Cyber Security Management System）とは、国際標準（IEC 62443-2-1）であり、IACS のセキュリティを守るためのマネジメントシステムのことです。組織が CSMS を確立・運用することにより、IACS のセキュリティを守る組織活動の仕組みが整備され、PDCA（Plan-Do-Check-Action）サイクルにより効果的なセキュリティ対策につながるのです。

この CSMS を確立・運用する組織に対して、国際標準への適合性と有効性を第三者（審査機関）が客観的に評価する仕組みが CSMS 認証（CSMS 適合性評価制度）です。この CSMS 認証を取得する組織として、以下３つの事業者があげられます。

- IACS を保有する事業者（アセットオーナー）
- IACS の構築事業者（システムインテグレータ）
- IACS の運用・保守事業者

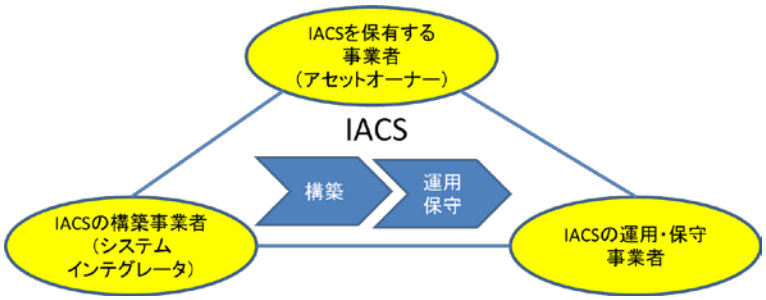

図　1-1　CSMS 認証の対象者

一般的にセキュリティの強度は鎖の強度に例えられます。一番弱い輪の強度が、鎖全体の強度へ影響するのです。よって IACS のセキュリティを高めるには、そのシステムの構築・運用・保守の各フェーズに携わる３つの事業者が協力し、三位一体となったセキュリティ管理を行うことが重要だといえます。

1.3. CSMS の役割とメリット

1.3.1. システムインテグレータにとっての CSMS

システムインテグレータとは、顧客（アセットオーナー）との直接・間接的な受託契約により IACS の構築を担う事業者のことです。日本の社会インフラを支える制御システムのセキュリティ対策を進めるためには、システムインテグレータの役割が重要であり、顧客（アセットオーナー）と一体となって IACS の全ライフサイクルに渡ってセキュリティ対策を担う必要があります。システムインテグレータが CSMS により守るべき IACS は、想定すべきリスクの側面から大きく以下の二つが考えられます。

1) **IACS の構築環境におけるリスク**

IACS の構築環境とは、システムインテグレータが IACS を構築して顧客へ引き渡すまでの構築環境です。システムインテグレータは、構築中の IACS をサイバー攻撃から守るために、IACS の構築環境においてリスクアセスメントを実施し、セキュリティ対策を施します。顧客へ IACS を引き渡すまでのシステムインテグレータが持つべき責任を考えると、このことは必然的といえます。

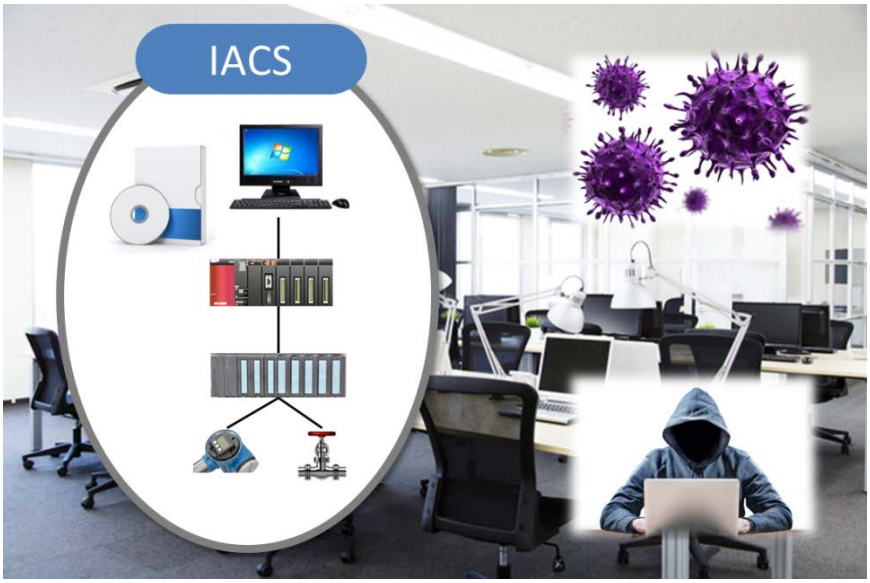

図 1-2　IACS の構築環境におけるリスク

2) IACS の運用環境におけるリスク

IACS の運用環境とは、システムインテグレータが IACS を構築して顧客へ引き渡した後、実際に顧客が IACS を運用する現場の環境です。システムインテグレータは顧客の IACS をサイバー攻撃から守るために、開発及び構築した後に運用される環境を想定してリスクアセスメントを実施し、IACS へ付加価値として必要なセキュリティ対策を顧客へ提案又は提供する役割があります。

図 1-3　IACS の運用環境におけるリスク

1.3.2. 認証取得のメリット

IACS のセキュリティを強固にするには、そのシステムのライフサイクルが始まる上流工程（早い段階）から、セキュアな仕組みづくりを進めることが必要です。つまり、セキュリティリスクを考慮したシステムの設計がポイントになるということです。

ここで重要な役割を担うのがシステムインテグレータです。顧客の要求仕様から，IACS に対して必要と思われる適切なセキュリティ対策を施す役目があると考えられるからです。

システムインテグレータにとって CSMS 認証を取得するメリットは、IACS へ適切なセキュリティ対策を施せる組織力を、顧客へ客観的に示せる点にあります。従来からのシステム構築そのものでは競合他社との受注競争が一層激しくなる中、セキュリティの側面から付加価値の高いサービスを顧客に訴求することで、ビジネス上の競争優位につながることが期待できます。

また、システムインテグレータとして自社の高いセキュリティ環境で IACS を構築できることを対外的に証明することができます。

2. システムインテグレータに対する追加要求事項

2.1. 目的

IACS を構築するシステムインテグレータの方々へ向けて、さらなる IACS のセキュリティ向上のために、開発・構築後に運用される IACS に対するリスクアセスメントを実施し、顧客に対して適切なソリューションを提案することを目的としています。なお、この要求事項は、IACS の運用環境におけるリスク評価ができることが前提となるため、運用後のリスク評価が役割上できない場合は除くことができます。例えば、「エンジニアリング部門からの依頼により IACS の開発・構築をする場合」などです。

CSMS 認証基準（Ver.2.0）で新たに追加された要求事項が以下です。

> **4.3.1.1　IACS の開発・構築を専門に担う組織におけるリスク対応**
>
> IACS の開発・構築を専門に担う組織は、開発及び構築した後に運用される IACS をサイバー攻撃から保護するために対処すべきリスクについても評価しなければならない。
>
> 注記：運用される IACS へのリスク評価が役割上できる場合には、この要求事項を適用しなければならない。
>
> CSMS 認証基準(IEC 62443-2-1) JIP-CSCC100-2.0 より引用

これは、システムインテグレータが IACS の構築にあたり、顧客（アセットオーナー）の運用環境で想定されるセキュリティリスクに対し、適切なセキュリティ対策の提案（さらには提供）へつながることを意図しています。

最終的に守るべき IACS のセキュリティは顧客の運用環境です。しかしながら、顧客が IACS に対するセキュリティの重要性を認識し、適切なセキュリティ対策を進めるには大きな課題があります。自社で IACS のセキュリティを専門にする要員の確保が難しく、取り組みが十分進まないことです。

その課題の解決に一翼を担うのがシステムインテグレータです。システムインテグレータが CSMS を理解し、IACS の構築を通じて顧客のセキュリティ対策を支援していくことが重要になるのです。

IACS を構築するシステムインテグレータとして CSMS 認証を取得するためには、この新たな要求事項に応えるために、以下の事項を考慮する必要があります。

(1) リスクアセスメントの実行について

「IACS の構築環境におけるリスク」に加えて、「IACS の運用環境におけるリスク」の評価が必要になります。

(2) リスクアセスメントのエビデンス（証拠）について

認証を受ける際には、4.2.3.13（リスクアセスメントの文書化）の要求事項から、(1)の２つのリスクに対する「リスクアセスメントの方法と結果」の文書が必要です。

(3) リスク対応に関するエビデンス（証拠）について

「IACS の構築環境におけるリスク対応」については、選択した管理策を示す「適用宣言書」の作成が必要です。但し、「IACS の運用環境におけるリスク対応」については、対処すべきリスク対応として適切なセキュリティ対策を顧客へ提案又は提供したこと（組織の活動）を客観的に示すために、その内容がわかる提案書や設計書等のドキュメント類が必要になります。

2.2. 認証審査の留意事項

システムインテグレータが IACS を構築するにあたり、顧客の運用環境で想定されるセキュリティリスクに対して、適切なセキュリティ対策の提案が必要です。

例えば、IEC 62443-2-4（Security program requirements for IACS service providers : IACS サービスプロバイダーのためのセキュリティプログラム要求事項）等のセキュリティ要件を開発及び運用される IACS の要件に含めることにより、セキュリティ要件とされる対策事項について準備することができます。

(1) 初回審査（第一段階、第二段階）について

「IACS の運用環境におけるリスク」の評価については、まず顧客へセキュリティ対策を提案した案件のエビデンス（証拠）が必要です。さらに、提案した案件を実際に受注している場合には、その進行状況に関するエビデンス（証拠）も示す必要があります。

(2) サーベイランス審査と再認証審査について

継続した組織の活動を示すには、少なくても前回審査から「IACS の運用環境におけるリスク」の評価を新たに実施したエビデンス（証拠）が必要です。

3. CSMS の確立・運用

3.1. はじめに

3.1.1. 全体の流れ

CSMS の確立・運用の進め方を、以下の項目に沿ってポイントを説明します。

① サイバーセキュリティポリシーの策定
② 教育訓練の実施
③ 内部監査による評価
④ マネジメントレビューからの改善

図 3-1　CSMS の確立・運用

3.1.2. CSMS 認証基準の参照

CSMS 認証基準は、国際標準（IEC62443-2-1）をベースに、第三者による審査の評価基準に適するよう一部内容が変更されています。CSMS 認証を取得するには、CSMS 認証基準への適合が求められます。よって、CSMS を確立・運用する際には CSMS 認証基準の内容を理解し、自らの組織へ適用することが必要です。

本章では、CSMS 認証基準の中でポイントとなる要求事項を引用しながら、説明を進めます。ただし、CSMS 認証基準の全ての要求事項を網羅していないので、留意してください。

3.2. サイバーセキュリティポリシーの策定

本章では、IACS のセキュリティ管理のために必要な方針や体制、対策基準、運用手順な

どをまとめてサイバーセキュリティポリシーと呼びます。組織の慣習等に応じて「ガイドライン」「規程」「マニュアル」などで呼ばれることもあります。

サイバーセキュリティポリシーの内容は、組織の事業規模や形態、対象とする IACS の特性等によって変わってきます。組織の目指すべき目標やレベルに応じて策定する必要があるのです。

以下、サイバーセキュリティポリシー策定の流れを大きく３つに分けて説明します。

① 基本方針

② リスクアセスメント

・上位レベルのリスクアセスメント

・詳細なリスクアセスメント

③ 管理策の選択及び提供

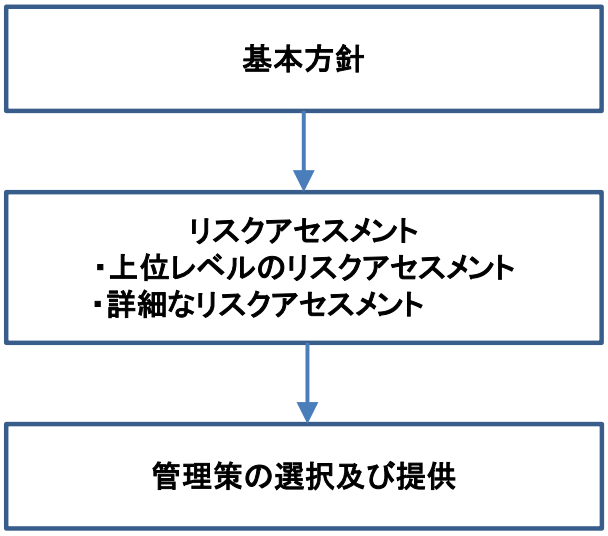

図 3-2　サイバーセキュリティポリシー策定の流れ

3.2.1. 基本方針

> **4. 2. 2. 1　事業上の根拠の策定**
>
> 組織は, IACS のサイバーセキュリティを管理するための組織の取り組みの基礎として, IACS に対する組織の固有の依存性に対処する，上位レベルの事業上の根拠を策定しなければならない。
>
> CSMS 認証基準(IEC 62443-2-1) JIP-CSCC100-2.0 より引用

まず CSMS によるセキュリティ管理を進めるにあたって、その活動の前提となる事由をまとめます。これを CSMS 認証基準では「事業上の根拠」と呼んでいます。事業上の根拠の策定にあたっては、システムインテグレータが IACS の構築（製品やサービスの提供）を

事業とする目的や、IACS を提供する主要な顧客の事業環境などを考慮する必要があるはずです。

「なぜ IACS のセキュリティが重要なのか」「サイバーインシデントの発生でどの程度の被害が想定されるのか」といった、組織が CSMS を進めるにあたっての根底となるものです。

4.3.2.6.1　セキュリティポリシーの策定

組織は，経営陣の承認を受けた，IACS 環境のための上位レベルのサイバーセキュリティポリシーを策定しなければならない。

4.3.2.6.2　セキュリティ手順の策定

組織は，サイバーセキュリティポリシーに基づいてサイバーセキュリティ手順を策定及び承認し，ポリシーを満たす方法に関する手引を提供しなければならない。

4.3.2.6.3　リスクマネジメントシステム間の一貫性の維持

IACS のリスクに対処するサイバーセキュリティのポリシー及び手順は，他のリスクマネジメントシステムによって作成されたポリシーに対して一貫性があるか，又はそれらを拡張したものでなければならない。

4.3.2.6.4　サイバーセキュリティのポリシー及び手順の準拠要求事項の定義

IACS環境用のサイバーセキュリティのポリシー及び手順には，準拠要求事項が含まれていなければならない。

4.3.2.6.5　リスクに対する組織の許容度の決定

組織は，ポリシーの作成及びリスクマネジメント活動の基礎として，組織のリスク許容度を決定し，文書化しなければならない。

4.3.2.6.6　組織へのポリシー及び手順の伝達

IACS 環境用のサイバーセキュリティのポリシー及び手順が，すべての適切な要員に伝達されなければならない。

4.3.2.6.7　サイバーセキュリティのポリシー及び手順のレビュー及び更新

サイバーセキュリティのポリシー及び手順は，定期的にレビューされ，それらが最新であり守られていることを確認するために検証され，それらが適切であり続けることを確実にするために必要に応じて更新されなければならない。

4.3.2.6.8　サイバーセキュリティに対する経営幹部の支援の表明

経営幹部は，サイバーセキュリティポリシーを是認することによって，サイバーセキュリティへのコミットメントを表明しなければならない。

CSMS認証基準(IEC 62443-2-1) JIP-CSCC100-2.0より引用

CSMS によるセキュリティ管理の中では、リスクアセスメントの結果評価や必要なリスク対応の検討、インシデントの識別など、それぞれの場面において組織的な判断が必要となります。その判断の拠り所となる大きな方向性が「上位レベルのサイバーセキュリティポリシー」です。上位レベルのサイバーセキュリティポリシーは、経営陣のコミットメントとして関係者へ広く浸透させることが重要です。

4.3.2.2.1　CSMS の適用範囲の定義

組織は，サイバーセキュリティプログラムの適用範囲を，正式な書面の形で策定しなければならない。

4.3.2.2.2　適用範囲の内容の定義

適用範囲では，CSMS の戦略的目標及びプロセスを説明しなければならない。

注記：IACS の開発及び構築を専門に担う組織では、開発及び構築する IACS を CSMS の適用範囲の中に含めるものとする。

CSMS 認証基準(IEC 62443-2-1) JIP-CSCC100-2.0 より引用

適用範囲とは、CSMS でセキュリティ管理の対象とする範囲や領域を示します。適用範囲は、IACS のサイバーリスクを考える際のスコープ（目的の範囲）となるため、「事業上の根拠」や「上位レベルのサイバーセキュリティポリシー」などを踏まえながら決定する必要があります。一般的には、事業場所や組織構造、業務プロセス等の接点を境界として考えることが多いでしょう。

例えば、システムインテグレータの CSMS の適用範囲を組織構造から考えるなら、顧客との受託契約により IACS の構築を担う部署等（例：「制御システム技術部」）を対象にするなどです。

また、4.3.2.2.2 の注記については、顧客へ納品する IACS を構築する環境を適用範囲に含める必要があることを述べています。これは、構築環境におけるリスクを分析し、セキュリティ対策を施すことが重要であるからです。

4.3.2.3.1　経営幹部の支援の獲得

組織は，サイバーセキュリティプログラムに対する経営幹部の支援を得なければならない。

4.3.2.3.2　セキュリティ組織の確立

経営陣の主導によって確立（又は選抜）された，IACSのサイバー的側面に関する明確な指示及び監督を提供する責任を持つ，ステークホルダーの組織，構造又はネットワークが存在しなければならない。

4.3.2.3.3　組織の責任の定義

サイバーセキュリティ及び関連する物理的セキュリティ活動に関する組織の責任が明確に定義されなければならない。

4.3.2.3.4　ステークホルダーチームの構成の定義

ステークホルダーの中核チームは，IACS のすべての部分におけるセキュリティに対処するために必要な技能が結集されるように，職務の枠を超えた性質のものでなければならない。

CSMS 認証基準(IEC 62443-2-1) JIP-CSCC100-2.0 より引用

CSMS によるセキュリティ管理の体制と責任を明確にします。一つはマネジメント層から構成する組織体（例：CSMS 委員会）で、CSMS に関わる意思決定や承認行為、報告内容のレビュー等の実施が考えられます。もう一つはデベロップメント層を中心する組織体（例:CSMS 推進チーム)で､CSMS の手順レベルでの管理が考えられます｡いずれも CSMS の適用範囲の関係者が、組織横断的に協力し合える体制づくりを行うことが重要です。

なお、ステークホルダーについては、「５.用語の定義 (6)ステークホルダー」を参照して下さい。

3.2.2. リスクアセスメント

4.2.3.1 リスクアセスメント方法の選択

組織は，組織のIACS資産に関連するセキュリティ上の脅威，ぜい弱性及び結果に基づいてリスクの識別とその優先順位付けを行う，リスクのアセスメント及び分析のための特定のアプローチ及び方法を選択しなければならない。

4.2.3.4　IACSの識別

組織は，各種の IACS を識別し，装置に関するデータを収集してセキュリティリスクの特性を識別し，それらの装置を論理的システムにグループ化しなければならない。

4.2.3.5　単純なネットワーク図の策定

組織は，論理的に統合されたシステムのそれぞれについて，主要装置，ネットワークの種類及び機器の一般的な場所を示す単純なネットワーク図を策定しなければならない。

CSMS 認証基準(IEC 62443-2-1) JIP-CSCC100-2.0 より引用

1) IACS の構築環境におけるリスクアセスメント

ここではまず、リスクアセスメントを行うにあたって必要となる、CSMS の適用範囲に存在する IACS を洗い出します。

IACS の構築では、実際に開発を行う環境が存在します。その開発から納入までの工程の中で、開発される各種の IACS（ハードウェア、ソフトウェア等）がリストアップされていると思います。しかしながら、その IACS が製品や機器の個別単位のままだと、リスクアセスメントの中で個々の IACS がどのように影響するのか、リスクの評価が難しくなることが考えられます。そのような場合、個々の IACS を機能や特性等に応じてグループ単位（IACS グループ）にまとめることで、適切な評価につながるはずです。さらに、個々の IACS だけだと、リスクアセスメントでの影響範囲がわかりづらいことも考えられます。その際には、開発環境全体が把握できる概要レベルでネットワーク図をまとめるといいでしょう。

2) IACS の運用環境におけるリスクアセスメント

また、IACS の運用環境におけるリスクアセスメントの方法については、顧客の要求（リスクアセスメントに対する基本的な考え方）を考慮する必要があるため、その方法を適切に修整（テーラリング）できることが望まれます。リスクアセスメントの方法及び結果については文書としてまとめ、維持・管理する必要があります。

リスクアセスメントを行うタイミングとしては、IACS 構築の上流工程（システムの企画や設計フェーズ等）での実施と、システムの設計変更が生じた場合の再実施などが考えられます。

4.2.3.2　リスクアセスメントの背景情報の提供

組織は，リスクの識別を開始する前に，リスクアセスメント活動の参加者に対して，方法に関する訓練などの適切な情報を提供しなければならない。

4.2.3.3　上位レベルのリスクアセスメントの実行

IACSの可用性，完全性又は機密性が損なわれた場合の財務的結果及びHSE（health, safety and environment）に対する結果を理解するために，上位レベルのシステムリスクアセスメントが実行されなければならない。

4.2.3.6　システムの優先順位付け

組織は，各論理制御システムのリスクを軽減するため，基準を策定して優先順位を割り当てなければならない。

4.2.3.7　詳細なぜい弱性アセスメントの実行

組織は，組織の個々の論理IACSの詳細なぜい弱性アセスメントを実行しなければならない。このアセスメントは，上位レベルのリスクアセスメントの結果及びそれらのリスクにさらされるIACSの優先順位付けに基づいて適用範囲を決定してもよい。

4.2.3.8　詳細なリスクアセスメントの方法の識別

詳細なぜい弱性アセスメントで識別された詳細なぜい弱性に優先順位を付けるための方法が，組織のリスクアセスメントの方法に含められなければならない。

4.2.3.9　詳細なリスクアセスメントの実行

組織は，詳細なぜい弱性アセスメントで識別されたぜい弱性を組み込んだ詳細なリスクアセスメントを行わなければならない。

4.2.3.10　再アセスメントの頻度及びトリガーになる基準の識別

組織は，技術，組織又は産業活動の変化に基づいた，再アセスメントのトリガーになるあらゆる基準を識別するだけでなく，リスク及びぜい弱性の再アセスメントの頻度も識別しなければならない。

4.2.3.11　物理的リスクのアセスメントの結果とHSE上のリスクのアセスメントの結果とサイバーセキュリティリスクのアセスメントの結果の統合

資産のリスク全体を理解するために，物理的リスクのアセスメントの結果とHSE上のリスクのアセスメントの結果とサイバーセキュリティリスクのアセスメントの結果が統合されなければならない。

4.2.3.12　IACSのライフサイクル全体にわたるリスクアセスメントの実行

開発，実装，変更及び廃棄を含む，技術ライフサイクルのすべての段階にわたって，リスクアセスメントが行われなければならない。

4.2.3.13　リスクアセスメントの文書化

リスクアセスメントの方法及びリスクアセスメントの結果は文書化されなければならない。

CSMS認証基準(IEC 62443-2-1) JIP-CSCC100-2.0より引用

次にリスクアセスメントの方法を取り決めます。CSMS 認証基準では、リスクアセスメントの実行として、上位レベルと詳細レベルを求めているため、それぞれどのようなアプローチや方法で行うのか検討が必要です。

ここでシステムインテグレータにとって、非常に重要なポイントがあります。リスクアセスメントを行う上で考慮すべきセキュリティリスクは、以下の２つが想定されることです。

1) IACS の構築環境におけるリスク
   顧客へ IACS を引き渡す前の段階であり、構築環境下で想定されるセキュリティリスクです。
2) IACS の運用環境におけるリスク
   顧客へ IACS を引き渡した後の段階であり、顧客が IACS を運用する現場で想定されるセキュリティリスクです。

3.2.2.1. 上位レベルのリスクアセスメント

上位レベルのリスクアセスメントは、「一般的な種類のサイバーセキュリティのぜい弱性による影響がどのようなものである可能性があるか、及びこれらのぜい弱性が脅威によって利用される可能性を調べるが、これらのぜい弱性の具体的な例も、既に導入されている関連する対抗策も考慮しない。」（IEC 62443-2-1 AnnexA: A.2.3.3.3 より引用）とされています。つまり、現状自組織で行われている管理策を一旦無視し、何も行われていないものと仮定して、どのようなリスクがあるかを網羅的に考える必要があります。リスクを考える際には、特定されたリスクにより組織の財務的結果や HSE（Health, Safety and Environment）の結果がどのように影響するかをわかるようにする必要があります。これらの結果はシステムの優先順位付（認証基準の箇条 4.2.3.6)として利用可能となります。

上位レベルのリスクアセスメントの方法としては、例えば、以下の手順が想定できます。

① IACS に対する脅威や IACS のぜい弱性によって機密性、可用性、完全性が損なわれた場合に組織が直面するリスクをシナリオとして作成する

② リスクが発生する可能性を分類する

シナリオに基づき、リスクが発生する可能性について、分類します。

③ リスクがもたらす結果（影響の度合い）を想定する

シナリオに基づき、リスクがもたらす影響の度合いについて、分類します。

④ リスクを特定する

①～③のシナリオを基にリスクを特定します。特定したリスクにより組織における財務的結果や HSE の結果にどのように影響するかを把握します。

3.2.2.2. 詳細なリスクアセスメント

詳細なリスクアセスメントは、「既存の技術的対抗策、アカウントマネジメント手順への準拠、特定の制御システムネットワーク上の個別のホストごとのパッチ及び開いているポートの状態、ファイアウォールの分離と構成などのネットワーク接続特性などの詳細に対する調査を含んだ、詳細なぜい弱性アセスメントによって支援される。」（IEC 62443-2-1 AnnexA: A.2.3.3.3 より引用）とされています。

対象とする IACS のシステムやネットワークを識別し、分類します。たとえば、IACS の機器をセキュリティゾーンでグループ化する方法があります。セキュリティゾーンは、物理的ネットワークセグメントに沿って分けることが可能です。

詳細なリスクアセスメントの方法として、たとえば以下の手順が想定できます。

① 詳細なぜい弱性アセスメントの結果を踏まえた IACS のリスクをシナリオとして作成する

② 制御システムの重要度と、リスクの発生可能性から、リスクレベルを識別する

作成したリスクについて、リスクレベルを明確にして、重大なリスクは、CSMS 責任者による管理リスクとします。

4.3 CSMSによるリスクへの対処

4.3.1 概要

「CSMSによるリスクへの対処」であり、組織は次の事項を実行しなければならない。

「4.3 CSMS によるリスクへの対処」に規定する CSMS のプロセスの一部として「５．詳細管理策」より管理策を選択しなければならない。選択した管理策及びそれらを選択した理由、並びに管理策の中で適用除外とした管理策及びそれらを適用除外とすることが正当である理由を示した「適用宣言書」を作成しなければならない。また、「５．詳細管理策」に規定した管理策は、すべてを網羅していないので、追加の管理策を選択してもよい。

4.3.1.1 IACS の開発・構築を専門に担う組織におけるリスク対応

IACS の開発及び構築を専門に担う組織は、開発及び構築した後に運用される IACS をサイバー攻撃から保護するために対処すべきリスクについても評価しなければならない。

注記：運用される IACS へのリスク評価が役割上できる場合には、この要求事項を適用しなければならない。

4.3.4.2.1　IACSリスクの継続的管理

組織は，設備の使用期間全体にわたって，受け入れられるレベルになるようにリスクを管理するために，IACS装置及び対抗策の選択及び導入を含んだリスクマネジメントの枠組みを採用しなければならない。

4.3.4.2.2　共通する一連の対抗策の採用

物理的セキュリティリスクとサイバー上のセキュリティリスクの両方に対処するための，共通する定義済みの一連の対抗策（技術的及び管理的）が定義され，特定のリスクが識別されているすべての組織全体にそれが適用されなければならない。

CSMS 認証基準(IEC 62443-2-1) JIP-CSCC100-2.0 より引用

リスクアセスメントの結果、評価されたリスクに対して必要なリスク対応を行います。リスク対応とは、リスクの低減・保有・回避・移転といった選択肢を選び、その実施に必要な管理策を CSMS 認証基準の 5 章（詳細管理策）から選択することです。選択した管理策は、組織のセキュリティ対策として具現化します。

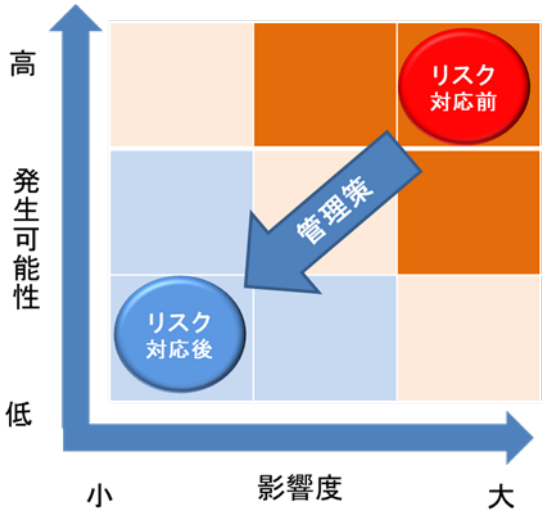

図 3-3　管理策によるリスクの低減

システムインテグレータにおけるリスク対応は、想定されるリスクに応じて以下の２つが必要です。

1)　IACS の構築環境におけるリスク対応

構築環境のリスクに応じた管理策を選び、具体的なセキュリティ対策を施します。ま

た、選択した管理策を示す「適用宣言書」を作成します。

2) IACS の運用環境におけるリスク対応

顧客の管理策として適切なソリューション（製品やサービス、及びその組み合わせ）を提案します。この場合のソリューションとは、ハードウェア及びソフトウェア製品による機能の提供など、一連のセキュリティ対策を示します。

顧客は、システムインテグレータが提案するセキュリティ対策のソリューションを導入するかどうかを評価し、システムインテグレータとの契約に反映します。システムインテグレータは、契約に基づき顧客へセキュリティ対策を提供します。顧客へ管理策として適切なソリューションが提供できるよう、システムインテグレータはそのプロセスや手順等をあらかじめ整備しておきます。

また、システムインテグレータは、リスクの評価として顧客へどのようなセキュリティ対策を提案又は提供したのか客観的に示せるよう、関連する文書（提案書や設計書など）をリスクアセスメントの文書とあわせて維持・管理する必要があるでしょう。

3.2.3. 管理策の選択及び提供

3.2.3.1. IACS の構築環境における管理策の選択

システムインテグレータは、IACS の構築環境に対して自ら管理策を選択し、実施しなければなりません。管理策の中で適用除外とした場合には、適用除外とすることが正当である理由を示した「適用宣言書」を作成する必要があります。CSMS 認証基準の 5 章で示された詳細管理策をあげて説明を進めます。

なお、詳細管理策の内容については、「CSMS ユーザーズガイド（Ver.1.2）８．システムインテグレータにとっての CSMS」を参照して下さい。

(1) 5.1 事業継続計画

5.1.1 復旧目標の規定
5.1.2 各システムに対する影響及び結果の決定
5.1.3 事業継続計画の策定及び導入
5.1.4 事業継続チームの結成
5.1.5 具体的な役割及び責任の定義及び伝達
5.1.6 事業継続計画を支援するバックアップ手順の作成
5.1.7 事業継続計画のテスト及び更新

・ IACS の構築環境

自社の事業継続計画を踏まえながら、IACS を構築する業務の継続性に関して、必要なプロセスや手順等を整備することが考えられます。

(2) 5.2 要員のセキュリティ

5.2.1 要員のセキュリティポリシーの確立
5.2.2 要員の初期段階の選別
5.2.3 要員の継続的な選別
5.2.4 セキュリティ上の責任への対処
5.2.5 セキュリティ上の期待事項及び責任の文書化及び伝達
5.2.6 サイバーセキュリティに関する雇用条件の明確な記述
5.2.7 適切な抑制と均衡を維持するための職務の分離

・ IACS の構築環境

IACS の構築は、顧客との受託契約ごとにプロジェクト体制をとるのが一般的です。プロジェクトには複数の協力会社が関与することも多いため、組織横断的に適用できるポリシーの策定が望まれます。

(3) 5.3 物理的及び環境的セキュリティ

5.3.1 補助的な物理的セキュリティ及びサイバーセキュリティポリシーの確立
5.3.2 物理的セキュリティ境界の確立
5.3.3 入退管理の実施
5.3.4 環境的損傷からの資産の保護
5.3.5 セキュリティ手順に従うことの従業員への要求
5.3.6 接続の保護
5.3.7 機器資産の保守
5.3.8 監視及び警報の手順の確立
5.3.9 資産を追加、除去及び廃棄する手順の確立
5.3.10 重要資産の暫定的保護のための手順の確立

・ IACS の構築環境

すでに自社で実施している、物理的及び環境的なセキュリティ対策に準ずることが考えられます。また IACS を構築するプロジェクトの特性に応じて、個別に実施すべき手順等を整備することも重要です。

(4) 5.4 ネットワークの分割

5.4.1 ネットワーク分割アーキテクチャの策定
5.4.2 高リスク IACS の隔離又は分割の採用
5.4.3 障壁装置による不要な通信のブロック

・ IACS の構築環境

IACS を構築するプロジェクトでは、社内のネットワーク環境との接続点を最小限とし、かつ、接続点には適切な防御措置を講じることが推奨されます。特に、OA 環

境からの影響を最小限にする必要があります。

(5) 5.5 アクセス制御－アカウント管理

5.5.1 アクセスアカウントでの認可セキュリティポリシーの導入
5.5.2 個人の識別
5.5.3 アカウントアクセスの認可
5.5.4 アクセスアカウントの記録
5.5.5 不要なアカウントの一時停止又は削除
5.5.6 アカウントの許可のレビュー
5.5.7 デフォルトパスワードの変更
5.5.8 アカウント管理の監査

5.6 アクセス制御－認証

5.6.1 認証方針の策定
5.6.2 システムの使用前のすべてのユーザの認証
5.6.3 システム管理及びアプリケーション構成での強い認証方法の要求
5.6.4 重要なシステムに対するすべてのアクセス試行の記録及びレビュー
5.6.5 適切なレベルでのすべてのリモートユーザの認証
5.6.6 リモートログイン及びリモート接続のポリシーの策定
5.6.7 失敗したリモートログイン試行の後のアクセスアカウントの無効化
5.6.8 リモートシステムの活動がなくなった後の再認証の要求
5.6.9 タスク間通信での認証の採用

5.7 アクセス制御－認可

5.7.1 認可セキュリティポリシーの定義
5.7.2 IACS 装置にアクセスするための適切な論理的及び物理的許可方法の確立
5.7.3 役割に基づくアクセスアカウントによる、情報又はシステムへのアクセス制御
5.7.4 重要な IACS に対する複数の認可方法の採用

ここでは、アクセス制御という一つの機能にまとめて管理策をみていきます。

・ IACS の構築環境

顧客へ納品する IACS のアクセス制御は、一般的には IACS の運用環境で求められるポリシーに準じたものにすることが望まれます。また、IACS を構築するプロジェクトで固有の特性等があれば、それに応じたアクセス制御のポリシーを取り決める必要があります。

(6) 5.8 システムの開発及び保守

5.8.1 セキュリティ機能及び能力の定義及びテスト
5.8.2 変更管理システムの開発及び導入
5.8.3 IACS を変更することのすべてのリスクアセスメント
5.8.4 システムの開発又は保守による変更に対するセキュリティポリシーの要求
5.8.5 サイバーセキュリティ及びプロセス安全性マネジメント（PSM）の変更管理手順の統合
5.8.6 ポリシー及び手順のレビュー及び維持管理
5.8.7 パッチマネジメント手順の確立及び文書化
5.8.8 ウイルス対策／マルウェアマネジメント手順の確立及び文書化
5.8.9 バックアップ及び復元の手順の確立

・ IACS の構築環境

システムインテグレータが顧客から受託する、主要業務（開発及び保守）に対する管理策です。IACS そのものを開発及び保守する際のリスクを考えると、基本的に運用環境で実施するセキュリティ対策との違いはないと考えられます。

(7) 5.9 情報及び文書のマネジメント

5.9.1 情報分類レベルの定義
5.9.2 すべての CSMS 情報資産の分類
5.9.3 適切な記録管理の保証
5.9.4 長期記録の取得の保証
5.9.5 情報の分類の維持管理

・ IACS の構築環境

自社の文書管理ポリシーに従うことが基本です。但し、IACS を構築するプロジェクトに制約条件等があり、顧客の文書管理ポリシーに準ずることも考えられます。

(8) 5.10 インシデントの計画及び対応

5.10.1 インシデント対応計画の導入
5.10.2 インシデント対応計画の伝達
5.10.3 通常と異なる活動及び事象に関する報告手順の確立
5.10.4 サイバーセキュリティインシデントの報告に関する従業員の教育
5.10.5 タイムリーな方法によるサイバーセキュリティインシデントの報告
5.10.6 インシデントの識別及び対応
5.10.7 失敗した及び成功したサイバーセキュリティ侵害の識別
5.10.8 インシデントの詳細の文書化
5.10.9 インシデントの詳細の伝達

5.10.10　発見された問題点に対する対処及び修正
5.10.11　演習の実行

・　IACS の構築環境

自社の基本的なセキュリティ方針に従い、インシデント対応についてのプロセスや手順等を取り決めて実践します。

3.2.3.2. IACS の運用環境における管理策の提案

システムインテグレータは、IACS の運用環境に対して管理策をどのようなソリューション（セキュリティ対策）として提案するのか、CSMS 認証基準の 5 章で示された管理策（10 項目）を参考として提示します。

なお 5.1、5.2、5.3、5.9、5.10 については、運用環境におけるリスク評価には関連しないが例として記載しています。

(1) 5.1　事業継続計画

・　IACS の運用環境

顧客がもつ全社的な事業継続計画や、関連するシステムを考慮した計画立案の支援（コンサルティングサービス）が求められます。顧客の事業環境に応じて具体的な内容へ落とし込めるよう、あらかじめ計画策定に必要となる文書をテンプレート化しておくといいでしょう。

(2) 5.2　要員のセキュリティ

・　IACS の運用環境

顧客企業の職務規定等を踏まえながら、各種ポリシーの作成支援が求められると考えられます。

(3) 5.3　物理的及び環境的セキュリティ

・　IACS の運用環境

システムインテグレータが持つ技術ノウハウを活かし、顧客へ効果的なソリューションを提供することが期待されます。ポリシーや手順の作成のためのコンサルティング、保護を確実とするシステム設計、入退室管理システムの導入等、IACS のリスクに応じた適切な製品やサービスの提案が求められます。

(4) 5.4　ネットワークの分割

・　IACS の運用環境

ゾーン分割のためのネットワーク設計、ファイアウォール製品の選定や導入、アクセスコントロールリスト（ACL）の作成等が考えられます。これらを適切に実施で

きるようネットワークの設計基準を整備し、文書化しておくといいでしょう。また、近年では IACS 環境で無線 LAN が用いられるケースも少なくないため、それらのセキュリティ対策も十分考慮する必要があります。

(5) 5.5～5.7　アクセス制御－アカウント管理・認証・認可

・ IACS の運用環境

アクセス制御を統合管理するセキュリティ対策製品の導入は、アカウント管理、認証、認可の機能を備え、一元的にポリシー管理を行うことができます。システムインテグレータには、顧客へアクセス管理システムとしてこれらの製品を提案、設計、導入することが考えられます。

また、比較的小規模なシステム構成では、顧客が必要とするポリシーや手順の作成支援や、それぞれのサーバやネットワーク機器の管理設定等を担うことになるでしょう。

入退室管理システムとの機能連携、リモートアクセスや無線 LAN 機器の認証等の保護対策についても十分考慮が必要です。

(6) 5.8　システムの開発及び保守

・ IACS の運用環境

システムインテグレータは、IACS を新たに導入するだけでなく、その後のシステムの改造や更新などの委託業務が継続するのが一般的です。システム変更に伴うセキュリティリスク低減のために、プロセスや手順を確立し、それらを文書化することが求められます。

また、IACS は、外部ネットワークとの接続や上位システムとの連携等を制限するのが一般的です。そのようなシステム環境下の中で、どのようにパッチマネジメントやウイルス対策を施すべきか、適切なソリューションの提供が求められます。

(7) 5.9　情報及び文書のマネジメント

・ IACS の運用環境

顧客の文書管理ポリシーに従い、情報及び文書の取り扱いについての手順を確立し、それを適切に実施することが考えられます。

(8) 5.10　インシデントの計画及び対応

・ IACS の運用環境

顧客が適切なインシデント管理を実践できるよう、必要なコンサルティングサービスを提供することが考えられます。管理策として、インシデント計画の立案、体制の確立、必要な教育訓練の実施等の支援が求められます。

また、システムインテグレータは、顧客に重大なインシデントが発生した際、迅速なインシデント対応の支援ができるよう、あらかじめ契約事項としてサービスの内容や体制を整備しておくといいでしょう。

3.3. 教育訓練の実施

4.3.2.4.1　訓練プログラムの策定

組織は，サイバーセキュリティの訓練プログラムを設計及び導入しなければならない。

4.3.2.4.2　手順及び設備に関する訓練の提供

すべての要員（従業員，契約従業員及びサードパーティ契約者を含む）は，初めに及びその後定期的に，正しいセキュリティ手順及び情報処理設備の正しい使用に関する訓練を受けなければならない。

4.3.2.4.3　サポート要員に対する訓練の提供

リスクマネジメント，IACS のエンジニアリング，システム管理／保守，及び CSMS に影響を与えるその他の取り組みを実行するすべての要員は，これらの取り組みのセキュリティ目的及び産業活動について訓練を受けなければならない。

4.3.2.4.4　訓練プログラムの検証

要員がセキュリティプログラムを確実に理解し，要員が適切な訓練を確実に受けるように，訓練プログラムが継続的に検証されなければならない。

4.3.2.4.5　訓練プログラムの経時的な改訂

新たな又は変化する脅威及びぜい弱性を説明するために，サイバーセキュリティの訓練プログラムが必要に応じて改訂されなければならない。

4.3.2.4.6　従業員の訓練記録の維持管理

従業員の訓練記録及び訓練更新のスケジュールが維持管理され，定期的にレビューされなければならない。

CSMS 認証基準(IEC 62443-2-1) JIP-CSCC100-2.0 より引用

CSMS の運用にあたって必要となるのが教育訓練です。CSMS の適用範囲のすべての要員に対して、それぞれの役割や責任に応じた教育プログラムが必要です。また教育は初回の実施だけでなく、変化するセキュリティ環境への追従や要員のさらなる意識向上のため、定期的な実施が求められます。さらには、専門スキルを持つ要員の育成が必要です。専門スキルは短期で身につくものではないため、中長期的な視点で計画することが重要になります。

3.4. 内部監査による評価

4.4.2.1　監査プロセスの方法の規定

監査プログラムは，監査プロセスの方法を規定しなければならない。

4.4.2.2　定期的なIACSの監査の実行

IACS が CSMS に適合していることを検証する。セキュリティのポリシー及び手順が意図したとおりに機能しており，ゾーンのセキュリティ目的に合致していることを検証するための IACS の定期的な監査が，CSMS に含まれていなければならない。

4.4.2.3　適合の尺度の確立

組織は，CSMS への適合を監視するために使用されるパフォーマンス指標及び成功基準を定義しなければならない。それぞれの定期的監査からの結果は，セキュリティのパフォーマンス及びセキュリティの傾向を示すために，これらの尺度に対するパフォーマンスの形で表されなければならない。

4.4.2.4　文書の監査証跡の確立

監査証跡を確立するために要求される文書及び報告のリストが策定されなければならない。

4.4.2.5　非適合に対する懲罰処置の定義

組織は，CSMSへの非適合が何を意味するかを述べ，関連するいかなる懲罰処置の定義も行わなければならない。

4.4.2.6　監査員の能力の確保

適用範囲内にある特定のシステムを監査するために要求される能力が規定されなければならない。要求される独立性のレベルが，ガバナンスの一環として決定されなければならない。

CSMS 認証基準(IEC 62443-2-1) JIP-CSCC100-2.0 より引用

サイバーセキュリティポリシーを策定し、それに基づいて運用が定着すれば、次に必要なのが組織自らによる点検です。当事者ではない監査部門などが監査基準や監査手続きに則って、それを確認することを内部監査と呼びます。内部監査で行うことは、①組織のセキュリティ管理が CSMS 認証基準に適合しているか、②組織のサイバーセキュリティポリシーで定めたルールが適切に守られているかどうかの評価です。以下 JIS Q 19011：2012（マネジメントシステム監査のための指針）を参考に、内部監査の概念を示します。

・　監査基準

　監査証拠と比較する基準として用いる一連の方針、手順又は要求事項

・　監査証拠

　監査基準に関連し、かつ、検証できる、記録、事実の記述又はその他の情報

・　監査所見

　収集された監査証拠を、監査基準に対して評価した結果

・　監査結論

　監査目的及び全ての監査所見を考慮した上での、監査の結論

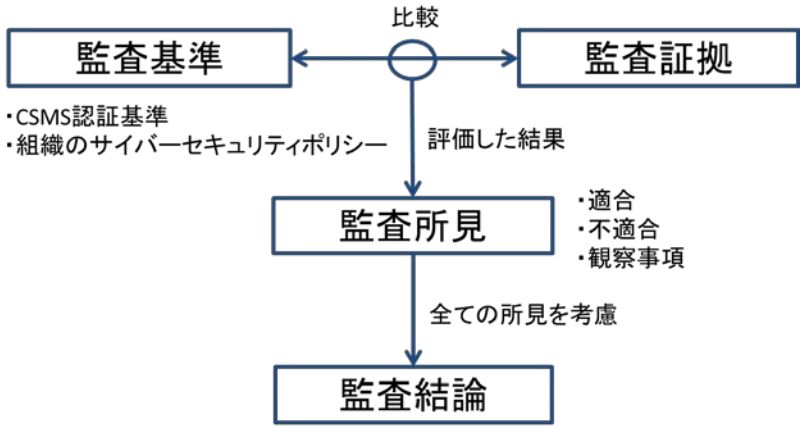

図 3-4　内部監査の概念

ここで重要なことは、その評価した内容から組織活動の改善につなげることです。これが内部監査の本質です。

では IACS を構築するシステムインテグレータにおいて、どのようなタイミングでどのように内部監査を実施すればいいのでしょうか。実はシステムインテグレータから見た IACS には大きな特徴があります。

それは顧客の IACS を構築するプロジェクト案件ごとに、開発プラットホームは異なる場合が多く、また顧客へ引き渡し後は自らの管理下に IACS が存在しなくなるからです。

これら管理対象の IACS が移り変わる中、それぞれの IACS に対して組織の CSMS が意図したどおりに適用できているかどうか、定期的に（例えば年一回）内部監査を実施することが考えられます。また、内部監査の効果をより高めるために、プロジェクト案件（例えば、IACS 開発及び構築においてリスクアセスメントを実施したプロジェクトなど）のマイルス

トーン（例えば、設計やテスト完了時点）で実施することも有効です。

3.5. マネジメントレビューからの改善

4.4.3.1　CSMS に対する変更を管理及び導入するための組織の割り当て

CSMS の変更の改良及び導入を管理及び調整し，定義された方法を使用して変更を策定及び導入するために組織が割り当てられなければならない。

4.4.3.2　CSMS の定期的な評価

管理を行う組織は，セキュリティ目的が満たされていることを確実にするために，CSMS 全体を定期的に評価しなければならない。

4.4.3.3　CSMSの評価のトリガーの確立

組織は，CSMSの関連要素のレビュー及び場合によって変更を行うきっかけとなる，設定されたしきい値を持つトリガーのリストを確立しなければならない。これらのトリガーには，少なくとも，重大なセキュリティインシデントの発生，法律及び規制の変更，リスクの変化及びIACSに対する大きな変更が含まれる。しきい値は，組織のリスク許容度に基づかなければならない。

4.4.3.4　是正処置及び予防処置の識別及び導入

組織は，セキュリティ目的を満たすためにCSMSを変更する適切な是正処置及び予防処置を，識別及び導入しなければならない。

4.4.3.5　リスク許容度のレビュー

組織，技術，事業目的，社内業務及び外部事象（識別された脅威及び社会状況の変化を含む）に対する大きな変化が存在するときは，リスクに対する組織の許容度のレビューが開始されなければならない。

4.4.3.6　業界のCSMS戦略の監視及び評価

マネジメントシステムの所有者は，リスクアセスメント及びリスク軽減のためのCSMSのベストプラクティスに関して業界を監視し，それらの適用可能性を評価しなければならない。

4.4.3.7　サイバーセキュリティに関連する適用法令の監視及び評価

組織は，サイバーセキュリティに関連する，適用及び変更される法令を識別しなければならない。

4.4.3.8　セキュリティ上の提案に関する従業員のフィードバックの要求及び報告

セキュリティ上の提案に関する従業員のフィードバックが，積極的に求められ，パフォーマンス上の欠点及び機会の点から経営幹部に必要に応じて報告が戻されなければならない。

CSMS 認証基準(IEC 62443-2-1) JIP-CSCC100-2.0 より引用

内部監査の結果を含め、組織のセキュリティ管理の状況を経営陣へ報告します。ここで経営陣の重要な役割としては、CSMS の取り組みを大きく変更する必要性を判断し、改善に向けての意思決定を行うことです。

細かな改善については、現場の管理レベルで適時見直しが進められます。しかしながら、大きく舵を切るべき改善は、組織内の統制（部門間での利害調整）や経営資源（人・モノ・金）の配分が伴うため、経営陣の関与や支援がないと実行が難しいからです。

3.6. 留意事項

3.6.1. CSMS 認証基準の理解

CSMS 認証基準のベースである国際標準（IEC 62443-2-1）は、システムの構築・運用・保守に携わる幅広い事業者にとって、IACS のセキュリティを守るために活用できるものです。しかしながら、自らの製品やサービスの提供のために IACS を保有する事業者（アセットオーナー）を主体に、内容が構成されているのは否めません。つまり、システムインテグレータの立場で CSMS 認証基準を見ると、内容の理解に難しい面があるということです。

CSMS 認証を取得するには、CSMS 認証基準の要求事項（4 章の全てと、5 章で選択する管理策）への適合が求められます。もし理解に苦しむ要求事項があっても、それを除くことはできません。

以下システムインテグレータにとって、理解が難しいと想定される要求事項の一部を取りあげて説明を加えます。

4.2.3.12　IACSのライフサイクル全体にわたるリスクアセスメントの実行

開発，実装，変更及び廃棄を含む，技術ライフサイクルのすべての段階にわたって，リスクアセスメントが行われなければならない。

CSMS 認証基準(IEC 62443-2-1) JIP-CSCC100-2.0 より引用

ここでは、「技術ライフサイクルのすべての段階」という部分をどう考えるかです。

・ IACS の構築環境

例えば IACS の構築で使用するテスト用のサーバ等、自社で所有管理している機器に対するリスクアセスメントだと理解すれば、技術ライフサイクルのすべての段階にわたり、実行できるのではないでしょうか。

> **4.3.4.2.1 IACSリスクの継続的管理**
>
> 組織は，設備の使用期間全体にわたって，受け入れられるレベルになるようにリスクを管理するために，IACS 装置及び対抗策の選択及び導入を含んだリスクマネジメントの枠組みを採用しなければならない。
>
> CSMS 認証基準(IEC 62443-2-1) JIP-CSCC100-2.0 より引用

ここでも「設備の使用期間全体」という部分の考え方がポイントになります。

・ IACS の構築環境

例えば、IACS の構築環境における物理的な環境の全般が「設備」であると捉えるなら、組織の CSMS（リスクマネジメントの枠組み）による活動そのものだといえるでしょう。

3.6.2. 追加の管理策

ここでは、システムインテグレータが顧客の IACS を構築するプロセスそのものに焦点を当てたリスクへの対処として、IACS のライフサイクルの中で適切なセキュリティ対策を設計し、実施することを確実にするために、追加の管理策が必要となる場合があります。例えば、制御システムの開発・保守に関する追加の管理策等が考えられます。

4. CSMS 認証の取得

ここでは、CSMS 認証の取得に関して、以下の流れで説明します。

① CSMS の導入

② 初回審査

・第一段階

・第二段階

③ サーベイランス審査（維持審査）

④ 再認証審査（更新審査）

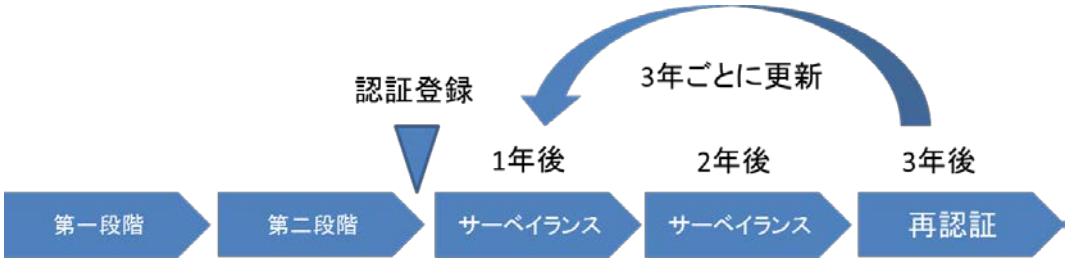

図 4-1　認証審査の流れ

4.1. CSMS の導入

認証取得にあたって、まずは 2 章で説明したように組織で CSMS の確立・運用を進める必要があります。そして CSMS を導入するスケジュールの中で、認証機関への審査の申請手続や審査日程等の調整を実施します。なお、審査手続に関する詳細については、各認証機関の審査窓口に相談をしてください。

4.2. 第一段階

初めて認証を取得する際の審査は 2 つの段階で実施されます。

第一段階では、主に組織の CSMS に関するドキュメント類の整備状況が審査されます。また、次の第二段階へ進むことができるかどうか、CSMS の確立・運用状況の確認が行われます。

ここで審査員から CSMS 認証基準に適合しない事項（不適合）が指摘された場合、次の第二段階までに CSMS の修正（是正）が必要です。

4.3. 第二段階

第二段階では、組織で実際にどのように CSMS が運用されているのか、実地審査が行わ

れます。経営陣に対するトップインタビュー（第一段階でも実施する場合がある）や CSMS を運用する方々へのヒアリング、IACS 構築の現場確認などです。

審査員は第二段階で、組織の CSMS が CSMS 認証基準に対する適合性と有効性の面で問題がないことを評価し、認証を推薦します。最終的に判定委員会又は判定委員が推薦内容を審議し、CSMS 認証の登録が行われるのです。

また、第二段階で発見された不適合が是正できない場合、認証登録を受けることができなくなりますので、十分な注意が必要です。

4.4. サーベイランス審査（維持審査）

認証登録は 3 年間有効で、有効期限が切れる前に再認証審査を受ける必要があります。但し、その再認証審査までの間、適切な CSMS の維持を確認するためのサーベイランス審査が毎年（1 年毎に）続きます。

4.5. 再認証審査（更新審査）

再認証審査は 3 年毎に行われます。認証の有効期限が切れる前に審査を受け、新しい認証登録書の発行を受ける必要があります。万が一の登録失効等にならないよう、審査を受ける認証機関と十分なスケジュール調整をしてください。

5. 用語の定義

本書における主要な用語の定義を以下に示します（五十音順）。

(1) HSE（health, safety and environment）

Health（健康）、Safety（安全）、Environment（環境）の頭文字であり、事業活動に伴う労働安全衛生問題や環境問題を示す [IEC 62443-2-1：2010 3.1.16より引用]。

(2) 管理策（JIS Q 27000:2014-2.16 参照）

リスクを修正（modifying）する対策。

[JIS Q 0073:2010の3.8.1.1参照]

注記1：管理策には、リスクを修正するためのあらゆるプロセス、方針、仕掛け、実務及びその他の処置を含む。

注記2：管理策が、常に意図又は想定した修正効果を発揮するとは限らない。

(3) サイバーセキュリティ

重要なシステム又は情報資産に対する無許可での使用、サービス不能攻撃、改変、開示、収益の逸失、又は破壊を防止するために要求されるアクションである [IEC/TS 62443-1-1 3.2.36より引用]。

(4) サイバーセキュリティポリシー

システム又は組織がその資産を保護するためにサイバーセキュリティサービスをどのように提供するかを規定又は統制する一連の規則。

(5) 産業用オートメーション及び制御システム（IACS: Industrial Automation and Control System）

産業プロセスの安全で、セキュアで、信頼できる運用に直接作用するか間接的に影響を及ぼす可能性がある要員、ハードウェア及びソフトウェアの集合[IEC/TC 62443-1-1：2009 3.2.57より引用]。

注記：これらのシステムには次のものが含まれるが、これらのみに限定されない。

- 分散制御システム（DCS）、プログラマブルロジックコントローラ（PLC）、リモート端末（RTU）、インテリジェント電子装置、監視制御及びデータ収集（SCADA）、ネットワーク化された電子検知制御並びに監視及び診断システムを含む、産業用制御システム。（この文脈において、プロセス制御システムには、基本的なプロセス制御システムの機能及び安全計装システム（SIS）の機能が含まれるが、それらの機能が物理的に分離されているか統合されているかは問わない。）
- 先進的または多変数制御、オンラインオプティマイザ、専用の機器モニタ、グラフィカルインタフェース、プロセス履歴管理、製造実行システム、工場情報マネジメントシステムなどの、関連する情報システム。
- 制御、安全及び製造作業機能を連続、バッチ、離散及びその他のプロセスに提供す

るために使用される、関連する内部、ヒューマン、ネットワーク又はマシンインタフェース。

(6) ステークホルダー

意図された結果の提供及び組織の製品及びサービスの存続可能性の維持に組織が成功することに対して利害関係を有する個人又はグループ。

注記：ステークホルダーは、プログラム、製品及びサービスに影響を与える。この特定の事例では、ステークホルダーは、サイバーセキュリティプロセスの推進及び監督に対して責任を持つ組織内の要員である。これらの要員には、サイバーセキュリティプログラムによって影響を受ける部門のすべてから選ばれた個人からなる職務の枠を超えたチームだけでなく、サイバーセキュリティプログラムの責任者も含まれる[IEC 62443-2-1：2010 3.1.40より引用]。

(7) 組織（JIS Q 27000:2014-2.57 参照）

自らの目的を達成するため、責任、権限及び相互関係を伴う独自の機能をもつ、個人又は人々の集まり。

注記：組織という概念には、法人か否か、公的か私的かを問わず、自営業者、会社、法人、事務所、企業、当局、共同経営会社、非営利団体若しくは協会、又はこれらの一部若しくは組合せが含まれる。ただし、これらに限定されるものではない。

(8) 適用宣言書[ISO/IEC 27001：2005 3.16より引用]

その組織のCSMSに関連して適用する管理目的及び管理策を記述した文書。

注記：管理目的及び管理策は、組織のサイバーセキュリティに対する、次のものに基づく。

－リスクアセスメント及びリスク対応のプロセスの結果及び結論

－法令又は規制の要求事項

－契約上の義務

－事業上の要求事項