サイバーセキュリティマネジメントシステム
（Cyber Security Management System）

CSMS ユーザーズガイド

－CSMS 認証基準（IEC 62443-2-1）対応－Ver.1.2

平成２７年５月

一般財団法人日本情報経済社会推進協会

はじめに

当協会では、平成 24 年度補正予算事業である「グローバル認証基盤整備事業」のテーマの一つとして、組織のマネジメントシステムのうち制御システムセキュリティに関する第三者認証等に対する基盤整備の事業を実施しました。

制御システム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 シリーズがある。本事業では、その中で制御システムセキュリティの国際標準である IEC 62443-2-1 : 2010 をベースとして、CSMS 認証基準（IEC 62443-2-1）を策定しました。

本書は、CSMS パイロット認証事業から得られた知見をもとに、制御システム関係者が、CSMS を構築・運用し、認証取得をめざす取り組みに資する CSMS の基本的な考え方や認証基準の解釈、留意点を紹介します。

1 章では、CSMS の役割とメリット等を説明し、2 章以降では、CSMS の構築・運用、審査の流れに沿って構成しています。
文中の四角枠には、CSMS 認証基準（IEC 62443-2-1）の最新版に記載された該当箇所を引用しています。

本書が CSMS 認証基準（IEC 62443-2-1）を理解する上での一助となり、CSMS を構築・運用する際の参考とな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、CSMS 技術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 27 年 5 月

一般財団法人日本情報経済社会推進協会

目　次

1. CSMS とはなにか

CSMS（Cyber Security Management System）とは、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）を対象としたサイバーセキュリティ[1]のマネジメントシステムです。サイバーセキュリティマネジメントシステムは、組織の事業活動全般及び直面するリスクに対する考慮のもとで、適切にリスクを管理し、利害関係者への信頼を得るための仕組みのことです。CSMS は、ISMS と同様にリスクマネジメントプロセスを適用することにより、IACS のサイバーリスクに対処します。

なお、ISMS では情報自体を重要な資産と捉え、情報の機密性（Confidentiality）、完全性（Integrity）及び、可用性（Availability）の喪失に伴うリスクを特定し、必要に応じて効果的なリスク対応を実施することが重要と考えられています。一方、CSMS では最も避けるべき事態として操業の中断を挙げており、IACS の可用性の維持を重視するとともに、HSE[2]に対するリスクを考慮することが特徴といえます。

本章では、CSMS の全体像について紹介します。

1.1. 背景

IACS は、エネルギー分野（電力、ガス等）や石油・化学、鉄鋼等のプラント、鉄道等の交通インフラ、機械、食品等の生産・加工ラインなど社会・産業基盤を支える産業用オートメーション及び制御システムです。

IACS は、従来、専用システムで構成され、外部ネットワークとは接続されていないことから、サイバーセキュリティ上の脅威は殆ど意識されていませんでした。しかし、近年、業務システム向けに開発された汎用技術（PC やサーバの基盤環境、TCP/IP 等のプロトコル等）、ネットワーク（遠隔操作、遠隔保守等）、メディア（データ抽出、パラメータ変更）の活用が進んだ結果、いわゆるサイバー攻撃の対象となりうる状況にあります。

IACS がサイバー攻撃を受けて停止した場合、社会インフラやビジネスの継続に深刻な影響を及ぼすだけでなく、HSE に対する深刻な影響が生じる可能性もあります。したがって、IACS を構築・運用する上で、サイバーセキュリティの確保はもはや不可欠といえるでしょう。

ただし、IACS は、そのライフサイクルの全体にわたり保護されるべき対象であり、運用期間が 10～20 年と非常に長期間にわたるものや、24 時間・365 日の稼働が求められるものが多く、リスクアセスメントの結果に応じてセキュリティ管理策を柔軟に適用することが

---

[1] 「CSMS 認証基準（IEC 62443-2-1）（JIP-CSCC100-1.0）」によると，サイバーセキュリティとは，「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。

[2] 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。

難しいケースがあることも否めません。したがって、IACS のセキュリティマネジメントに取り組む上で、そうした特徴にも十分に配慮する必要があります。

1.2. IACS を守るために

IACS を守るためには、製品・システムの安全性を高めるアプローチと、IACS の管理を強化するアプローチがあります。これらはどちらか一方で他方をカバーするのは困難であり、両方とも必要になります。たとえば、製品にぜい弱性があれば、そこから攻撃される可能性があります。また、システムに問題がなくても、デフォルトあるいは容易に推測可能なアカウントやパスワードが使用されているといった管理の甘さから、アカウントが奪取されシステムに不正侵入されるかもしれません。

技術面、管理面の両面から IACS を守るためには、コンポーネント（制御機器、装置等）を開発・提供するベンダ、それらを組み合わせて IACS を構築する事業者（システムインテグレータ）や運用・保守事業者、さらに保有する IACS を活用してサービスや製品を提供する事業者（アセットオーナー）が協力して実現する必要があります。

1.3. CSMS の役割とメリット

1.3.1. CSMS の役割

IACS の構築・運用を担う組織にとって、セキュリティの根本的な向上の為には、セキュリティマネジメントシステムの確立が有効です。情報システムの管理・運用については、ISO/IEC 27001 に示される情報セキュリティマネジメントシステム（ISMS）の適用が一般的ですが、1.2.節に示したように、IACS については、その特徴や性質に配慮したセキュリティマネジメントの仕組みが必要となります。そこで、ISMS をベースにした、IACS のためのセキュリティマネジメントシステムが IEC 62443-2-1 として規格化されています。この IEC 62443-2-1 に基づき、IACS 分野のセキュリティマネジメントシステム認証基準として「CSMS 認証基準（IEC 62443-2-1）（JIP-CSCC100-1.0）」（以下、「CSMS 認証基準」という。）が策定されました。

1.3.2. CSMS の対象者

CSMS 適合性評価制度は、対象となる組織が、IACS の構築・運用に関するセキュリティマネジメントシステムを確立し、第三者である認証（審査登録）機関が客観的にその適合性と有効性を評価するものです。以下が CSMS 認証の対象者となります。

- 制御システムを保有する事業者（アセットオーナー）
- 制御システムの運用・保守事業者

・ 制御システムの構築事業者（システムインテグレータ）

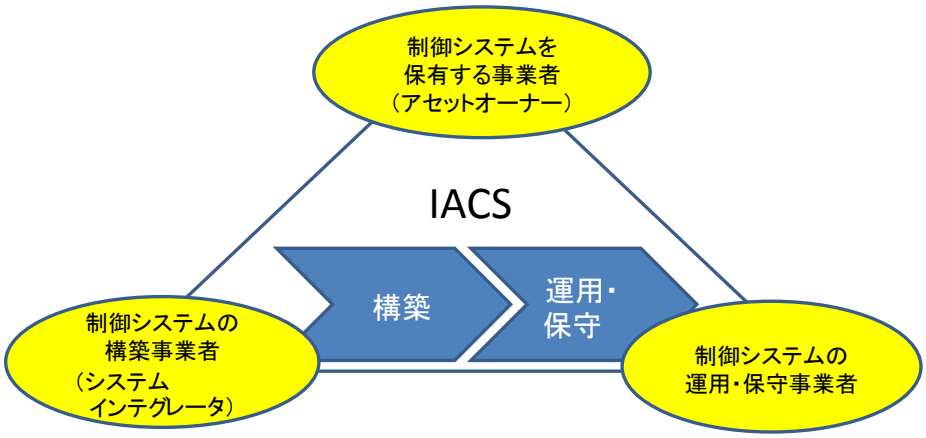


図 1-1 CSMS の対象者

1.3.3. CSMS のメリット

(1) サイバー攻撃に対するリスクの低減

IACS がサイバー攻撃を受け、システムが停止した場合の社会的影響は大きく、企業にも多大な損害をもたらすことが懸念されます。そのため、セキュリティリスクを許容可能なレベルまで低減することは必須であり、CSMS に基づくセキュリティ管理策を実施することが有効です。将来的には、そうしたセキュリティへの取り組みが事業者の競争力に反映されることも期待されます。

(2) IACS の運用担当者に対するセキュリティ管理策の行動指針の徹底

IACS の運用担当者に対して、行動指針を徹底することで、ヒューマンエラーや組織に起因するセキュリティ事故の発生可能性を低減することができます。行動指針は、定期的に見直しを行うことにより、運用の品質を落とすことなく維持できるメリットがあります。

さらに、第三者機関からの認証を取得することで、セキュリティ管理策の実施状況が客観的に評価されます。

(3) 事業者の担う社会的責任の遂行

情報セキュリティ政策会議「重要インフラの情報セキュリティ対策に係る第３次行動計画」（平成 26 年 5 月 19 日発表）では、「重要インフラ事業者等は事業主体として、また社会的責任を負う立場としてそれぞれに対策を講じ、また継続的な改善に取り組む」ことが求められています。また、重要インフラ事業者に限らず、認証を取得することで、プラントの安全面のリスクを考慮して緊急停止装置の信頼性を設定し安全性を向上する安全計装システム(SIS)の役割と同様に、事業者としてセキュリティ管理策を実施し、社会的責任を果たし

ていることの客観的な証明として活用できます。

(4) 第三者の観点から見た新たな気づき

CSMS では、内部監査により自らの取り組みの問題点・課題を明らかにすることが求められますが、経緯や実情を熟知する社内の監査員では、かえってそうした問題点や課題が見えなくなってしまうことがあります。認証機関の審査員による第三者監査を通じて、関係者には見つけにくい新たな気づきを得ることができます。

(5) リスクマネジメントに対する理解の促進

CSMS の導入・運用を通じて、社内において制御システムのセキュリティやリスクに対する理解が進むことが期待されます。特に、許容できるリスクについては新たな管理策が必要ないこと、また許容できないリスクに対する対応の一つとして、必要な管理策の適用を進めることについての理解が進み、目的意識の高い取り組みが期待できます。

(6) サイバーセキュリティに関する対外的な説明

システムインテグレータの場合、CSMS 認証を取得することによって、制御システムセキュリティに関する提案・設計・納入・設置について信頼性や説得力を付加できると考えられます。

また、海外に拠点を展開している事業者やシステムインテグレータの場合、CSMS 認証を取得することで、海外の政府機関や取引先にサイバーセキュリティの取り組みに関する客観的な説明が可能になります。

（参考）ISMS 認証のメリット

認証のメリットの観点から、実績の多い ISMS（Information Security Management System）の認証に関する評価を取り上げます。あくまで ISMS 認証の評価ですので、CSMS 認証の評価に直接的には繋がらないかもしれませんが、以下のような結果と類似の効果が得られることが期待できると考えます。

- ISMS に取り組んだことで、事故件数や費用など、明確な数字で効果が出ている。
- 現場の担当者が顧客にセキュリティの話をして、アピールできるようになった。
- 事故や違反をすぐに報告し、原因を分析して予防・改善につなげるという意識が定着してきた。
- PDCA の意識付けができ、セキュリティ事故防止の実効性が向上した。
- 従業員の情報セキュリティに対する理解が高まった。
- 現場運用者と管理者のコミュニケーションが強化され、真剣に意見をぶつけ合う機会が増えた。

2. CSMS プログラムの開始

本章では、CSMS の構築に着手する段階について説明します。

2.1. 事業上の根拠の策定

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-CSCC100-1.0 より引用

組織が IACS に関した事業を行う上で、サイバーセキュリティを管理すべき根拠を文書化して、組織全体における共通認識とすることをめざすよう要求されます。

根拠は、IACS におけるサイバーセキュリティ上のリスクが経営幹部の関心事に対しどのような事態を招きうるか、そうしたリスクの要因となる現実的な脅威やそれを回避するためのコストなどについて具体化することが望まれるからです。予想される事態として、たとえば IACS の停止や破壊だけでなく、それに伴うサービスの中断やコアビジネスの停滞、法律違反、さらに HSE（Health、 Safety and Environment）への悪影響などがあげられます。

ここで、組織とは、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ます。たとえば、企業、工場・事業所、特定の部署等、マネジメントシステムを構築・運用する単位が考えられます。

2.2. CSMS の適用範囲の策定

4.3.2.2　CSMS の適用範囲

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、プロセス及びタイミングを説明しなければならない。

CSMS 認証基準(IEC 62443-2-1) JIP-CSCC100-1.0 より引用

CSMS の適用範囲は、以下の観点から明確にする必要があります。

・ 体制・要員
・ 物理的拠点
・ システム・ネットワーク構成　等

認証審査に際しては、適用範囲を規定した「適用範囲定義書」の類を策定することが必要です。また、なぜこの範囲を適用範囲として選択したかの理由についても明確にすることが望まれます。

適用範囲の策定に際しては、境界が明確で、その境界における情報の IN/OUT をコントロールできることが望まれます。ただし、すべての領域を自身でコントロールできないこともあります。このような場合でも、適用範囲定義書に「ネットワーク管理が他部門に依存している」、「第三者も入室が可能な領域」などとして記載し、リスクアセスメントから詳細管理策の選択に至る流れの中で、対応方法を明確にする必要があります。

(例) ・特定の部署を CSMS の適用範囲としたが、ネットワークインフラは当該組織を含む企業全体の情報システム部門が管理しているため、当該部門間においてシステム運用に対する同意書（覚書など）を策定し、ネットワークインフラに係る両部門のセキュリティ管理に関する責任範囲を明確化した。

・特定のサーバルームを CSMS の適用範囲としたが、顧客や委託先の要員とも共用の部屋なので、入室を断ることはできない。そのため、入退室管理（記録簿の徹底、共連れができない仕組み、監視カメラの設置）を徹底し、不正な行動を監視できるようにした。

2.3. ステークホルダーの関与

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-CSCC100-1.0 より引用

組織は、CSMS の構築・運用を担当する中核的なチーム（ステークホルダーチーム）を編成する必要があります（5.4 節参照）。この中核的なチームは、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（ステークホルダー）で構成されます。一般にステークホルダーというと、社外の顧客等をイメージしますが、ここでは組織内の要員をメインとし、必要であれば適宜組織外の要員を含むことが望まれます。

2.4. 経営幹部のコミットメント、支援及び資金供給の獲得

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-CSCC100-1.0 より引用

CSMS の構築・運用及び認証審査に際して、経営幹部の支援は不可欠です。なぜなら、IACS の関連組織において、サイバーセキュリティの重要性が浸透していない場合、経営幹部からの要請抜きで、従業員が CSMS 構築へ協力的に対応することは期待できません。

経営幹部は、事業上の根拠や CSMS の戦略的目標に基づき、組織における CSMS の推進を明言し、そのために CSMS 担当チームに必要な権限やリソースを付与するとともに、その取り組みを支援するよう関係各所に働きかけることが期待されます。

認証審査の際には、経営陣へのインタビューにおいて、サイバーセキュリティポリシーに関する見解やリーダーシップ等経営陣の参画を必ず確認されます。

3. 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。これは、詳細なぜい弱性を調べることから着手すると、サイバーリスクの全体像を見失い、そのサイバーセキュリティの取り組みの焦点をどこに置くかを決定するのが難しくなることが、これまでの経過から分かっているからです。（IEC 62443-2-1 Annex：A2.3.3.3 より引用）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。

3.1. リスクの識別、リスクの優先順位のアセスメント

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[3]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。

4.2.3.2　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。

CSMS 認証基準(IEC 62443-2-1) JIP-CSCC100-1.0 より引用

上位のリスクアセスメントの方法としては、たとえば、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組織が直面するリスクをシナリオとして作成する

CSMS では可用性（A）に関するリスクを重視することが特徴とされています。ただしそれは、完全性（I）や機密性（C）に関するリスクを無視してよいという意味ではありません。

また、リスクシナリオは、システムの開発、導入、変更、更新、廃棄などライフサイクルを想定して作成します。

[3] 脅威やぜい弱性がもたらす影響の度合いを示している。

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。具体的には、表 3-1 のような基準を設定します。

表 3-1 可能性の尺度の例

カテゴリ	説明
高	今後 1 年以内に発生する可能性が高い脅威／ぜい弱性
中	今後 10 年以内に発生する可能性が高い脅威／ぜい弱性
低	これまでに発生したことがなく、発生する可能性がほとんどないと考えられる脅威／ぜい弱性

（出所：IEC 62443-2-1 AnnexA より引用）

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。具体的には、表 3-2 のような基準を設定します。

表 3-2 結果の尺度の例

	リスク領域								
	事業継続計画の作成		情報セキュリティ			産業活動の安全性		環境的安全性	全国的な影響
カテゴリ	1 サイトでの製造停止	複数サイトでの製造停止	コスト（単位:100 万$）	法的	公衆の信頼	サイト内の人	サイト外の人	環境	基盤及びサービス
高	>7 日	>1 日	>500	重い刑事犯罪	ブランドイメージの喪失	死亡	死亡又は重大な地域インシデント	地域機関もしくは国家機関からの召喚、又は広範囲に及ぶ長期間の重大な損傷	複数の事業分野に対する影響又は地域サービスの大規模な動作中断
中	>2 日	>1 時間	>5	軽い刑事犯罪	顧客の信頼の喪失	休職又は重傷	苦情又は地域社会への影響	地域機関からの召喚	1 社の事業分野を超えるレベルへの影響の可能性。地域のサービスへの影響の可能性
低	>1 日	<1 時間	<5	なし	なし	応急手当又は記録可能な負傷	苦情なし	報告可能限度を下回る小規模かつ限定的な放出	個別会社の事業分野を超えるレベルへの影響はほとんどない。地域のサービスへの影響はほとんどない。

（出所：IEC 62443-2-1 AnnexA を基に作成）

④ リスクの優先順位を設定する

リスクについてランク付けをすることで、優先順位を明らかにします。リスクのランク付けは、リスクの発生する可能性と影響の大きさに基づいて設定されます。具体的には、表 3-3 のような基準を設定します。

表 3-3 リスクレベルの基準の例

		結果		
		高	中	低
可能性	高	高リスク	高リスク	中リスク
	中	高リスク	中リスク	低リスク
	低	中リスク	低リスク	低リスク

（出所：IEC 62443-2-1 AnnexA を基に作成）

なお、リスクアセスメントを実施する際には、リスクアセスメントの方法を検討するとともに、リスクアセスメントを行う関係者に対してその方法を事前に教育し、スムーズに作業を進められるようにする必要があります。

3.2. 結果および根拠の文書化

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-CSCC100-1.0 より引用

上位リスクアセスメントの結果を文書化します。特に、リスクの発生可能性や結果（影響の度合い）、優先順位をどのように識別したか記録をとることで、次回のリスクアセスメント時の混乱を避けることができます。

文書化に際しては、組織の既存の品質管理マニュアルや文書管理ルールに従うことが適当です。

このようにプロセスの要所で記録をとる習慣が身に着くことで、CSMS の運用業務にも有益な効果が得られると期待できます。

4. 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。

4.1. IACS システム、ネットワーク及び装置の資産台帳の作成

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-CSCC100-1.0 より引用

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。

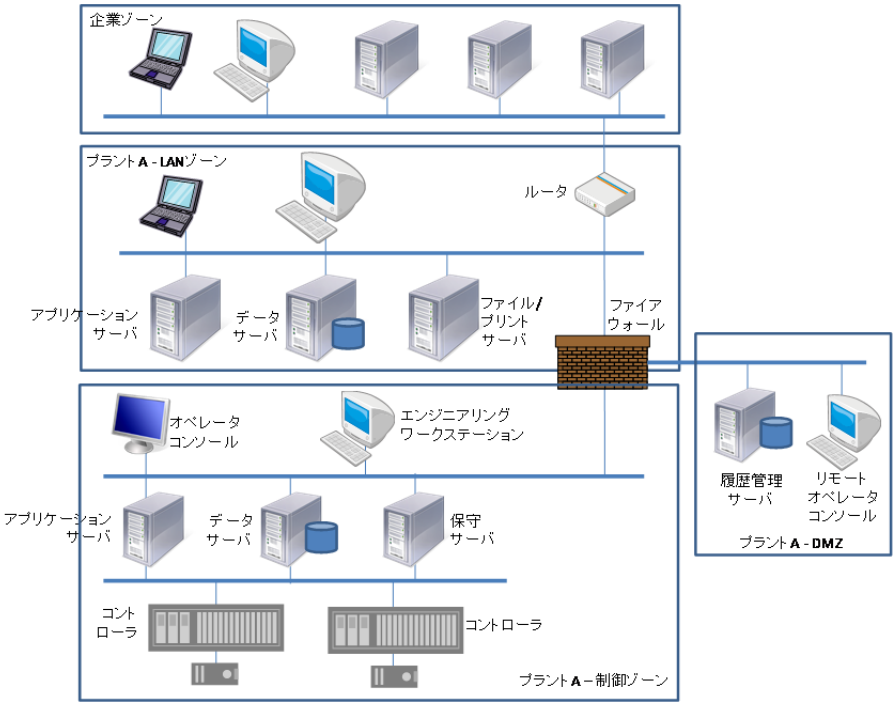


図 4-1 IACS の例に対するセキュリティゾーン

（出所： IEC 62443-2-1 AnnexA を基に作成）

また、ISMS を導入している組織の場合、ISMS 適用範囲の資産台帳やシステム構成図は既に整備済みであることから、台帳や構成図が二重管理とならないように工夫が必要です。

4.2. スクリーニング及び優先順位付け

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。

CSMS 認証基準(IEC 62443-2-1) JIP-CSCC100-1.0 より引用

組織において重要なシステムの管理策を優先することが望まれます。たとえば、上位レベルのリスクアセスメントで抽出されたリスクを踏まえ、その影響を受ける可能性があるシステムを優先する方法があります。また、機器の属するセキュリティゾーンでグループ分けした場合、そのセキュリティゾーンに求められるセキュリティレベルに応じて、優先順位を割り当てる方法も考えられます。

4.3. 詳細なぜい弱性の識別

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。

4.2.3.14　ぜい弱性アセスメントの記録の維持管理

IACSを構成するすべての資産について、最新のぜい弱性アセスメントの記録を維持管理しなければならない。

CSMS 認証基準(IEC 62443-2-1) JIP-CSCC100-1.0 より引用

IACS を構成する機器のハードウェア、ソフトウェア及び情報においては、ぜい弱性を内包する可能性があります。公開されているぜい弱性のリスト（例：JVN[4]、JVN iPedia[5]）や各ベンダが公開するぜい弱性情報等を参照するなどして、当該システム固有のぜい弱性を洗い出すことが望まれます。

また、上位レベルのリスクアセスメントの結果や、4.2 のシステムの優先順位に基づいて、詳細なアセスメントを適用する範囲を限定することも可能です。

---

[4] Japan Vulnerability Note: IPA と JPCERT/CC が共同運営するぜい弱性対策情報ポータルサイト https://jvn.jp/

[5] IPA が提供するぜい弱性情報データベース　http://jvndb.jvn.jp/

4.4. 関連するリスクの識別及び優先順位付け

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。

4.2.3.11　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。

CSMS 認証基準(IEC 62443-2-1) JIP-CSCC100-1.0 より引用

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

サイバーセキュリティの観点だけでなく、要員のセキュリティ、物理的・環境的セキュリティなどについても適切に考慮することが重要です。たとえば、以下のケースが考えられます。

- 無人になる時間帯がある部屋に装置・機器類が設置されている場合、火災が起きたり、侵入者が潜り込んだりしてもそのままでは検知することが難しい可能性があります。
- 共用のサーバルームの場合、自組織以外の要員が室内に入ることができる点について、リスクを検討する必要があります。
- バックアップメディアを再利用する場合、ファイルが復元できる可能性を考慮すれば、利用時だけでなく、利用が終わった後も同等のレベルで適切に管理する必要があります。

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。リスクレベルは、たとえば表 4-1 のような整理となります。

表 4-1 リスクレベルの例

リスクレベル	状況
高	操業上重要なシステムにおいて、極めて危険
中	既に発生する可能性のあるリスクがあり、発生した場合、操業に影響を与える可能性がある
低	発生する可能性は低く、仮に発生しても操業にはあまり大きな影響を与えない

5. セキュリティポリシー、組織及び意識向上の確立

サイバーセキュリティポリシーは、CSMS 認証基準によると「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」です。

5.1. ポリシー及び手順の作成、導入

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。

4.3.2.6.7　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。

5.2.1　要員のセキュリティポリシーの確立

セキュリティに対する組織のコミットメント及び要員のセキュリティ上の責任を明確に述べた、確立された要員のセキュリティポリシーが存在しなければならない（要員には、従業員、採用予定者、契約従業員及びサードパーティ契約者が含まれる）。

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

資産を保護するための物理的セキュリティとサイバーセキュリティの両方に対処するセキュリティのポリシー及び手順が確立されなければならない。

CSMS 認証基準(IEC 62443-2-1) JIP-CSCC100-1.0 より引用

サイバーセキュリティポリシーの作成に際しては、サイバー、要員、物理、環境の 4 つの観点に配慮する必要があります。CSMS 認証基準 5.3.1 のとおり、IACS を保護する上で、

物理的なセキュリティへの配慮も不可欠であり、これを意識したポリシーを作成することが求められています。

また、サイバーセキュリティポリシーの作成において、CSMS の適用範囲である組織もしくはそれが属する上位組織のセキュリティポリシーや情報管理規程との関係を整理しておく必要があります。たとえば、CSMS の適用範囲は特定の部署だが、ネットワークインフラは当該組織を含む企業全体の情報システム部門が管理している場合、特定部署としてのネットワーク管理ポリシーを独自に設定することが認められない可能性があります。

また、組織に他のマネジメントシステムが導入されている場合、そのポリシーと整合する必要があります。特に、ISMS を導入している組織の場合、ISMS の文書類を参照・活用することで効率化を図ることも可能です。全社と CSMS の対象組織の関係を前提としたセキュリティポリシーや管理規程・実施手順等の文書体系について、図 5-1 にイメージ例を示します。

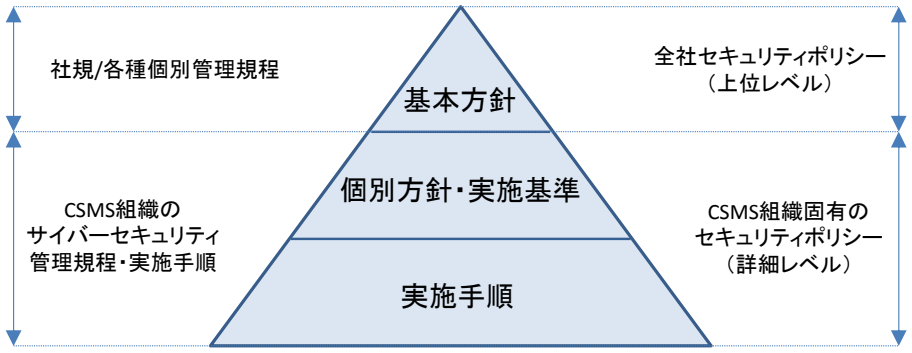


図 5-1 文書体系のイメージ例

なお、策定されたサイバーセキュリティポリシーは、経営陣の承認を受ける必要があります。

5.2. ポリシーの伝達

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。

CSMS 認証基準(IEC 62443-2-1) JIP-CSCC100-1.0 より引用

組織は、CSMS のサイバーセキュリティポリシーについて、関係する従業員に説明し、理解を得る必要があります。具体的には、CSMS 研修の実施が望まれますが、日程等の制約で実施が難しい場合には、組織全体の情報セキュリティ研修の中でカバーするケースも考

えられます。

また、サイバーセキュリティポリシーを社内のイントラネット上に公開する、サイバーセキュリティポリシーを掲載した文書を発行し社内に配布する、経営陣から従業員に向けてサイバーセキュリティポリシーの導入を説明するといった取り組みも有効です。

5.3. 訓練活動の策定

4.3.2.4　スタッフの訓練及びセキュリティ意識向上

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-CSCC100-1.0より引用

組織は、CSMS の構築・運用を担当する要員を対象に教育・訓練を行い、有効な人的リソースを確保することが望まれます。この際、教育・訓練の有効性を高めるため、何度でも学習・テストを繰り返すといった工夫が必要です。

CSMS の導入期には、IACS におけるサイバーセキュリティの訓練プログラムや指導者の調達が難しい場合もあるため、対応を検討する必要があります。

さらに、状況によっては、訓練プログラムの一部を組織全体の情報セキュリティ研修でカバーするケースも考えられます。

5.4. 組織の責任の割り当て

4.3.2.3　セキュリティを目的とした組織編成

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。

CSMS 認証基準(IEC 62443-2-1) JIP-CSCC100-1.0 より引用

組織は、CSMS の構築・運用を担当する中核的なチーム（ステークホルダーチーム）を編成する必要があります。当該チームは、活動を円滑に進めるために、あらかじめ当該チームの責任範囲と経営幹部の支援を得ておくことが望まれます。

要員は、職務の枠を超えて、関連するすべての部門から選出することが望まれます。たとえば、対象とする IACS を有する事業所やその管理・運用部門、関連する情報システム部門、さらに当該チームの責任者で構成されますが、場合によっては、広報部門、法務部門、総務部門など、担当部署以外の要員を含むケースもあります。さらに、親会社や子会社など、別会社であっても、CSMS 対象業務について密接に関係している場合には、連携することが望まれます。

6. 管理策の選択及び導入

リスクアセスメントの結果を踏まえ、必要な管理策を選択し、導入します。

CSMS 認証を前提としている場合、リスクアセスメントより先に、自らの業務内容や環境から不要な管理策を洗い出す作業から着手することも可能です。

なお、顧客の IACS を開発するシステムインテグレータの場合、認証基準中の「IACS」を「IACS の開発環境及びそこで開発されるアプリケーション」に読み替えた上で、管理策の要否を検討する必要があります。

6.1. リスク許容度の確立

> **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。
>
> CSMS 認証基準(IEC 62443-2-1) JIP-CSCC100-1.0 より引用

リスクに対する組織の許容度を設定し、リスクアセスメントにおいて抽出されたリスクに対する方針を明らかにします。たとえば表 6-1 のようなリスク許容度を設定した場合、リスクレベル(4.4 ②参照)が高と評価されたリスクについて、組織はプラントの計画停止やシステム更新まではそのリスクを許容するが、それ以上は許容できないという判断をしたことになります。

表 6-1 リスク許容度の例

リスクレベル	状況	対応方針
高	操業上重要なシステムにおいて、極めて危険	プラントの計画停止やシステム更新等に合わせ、管理策を実施する。
中	既に発生する可能性のあるリスクがあり、発生した場合、操業に影響を与える可能性がある	管理策実行については、ユーザと協議にて決定する。
低	発生する可能性は低いか仮に発生しても、操業にはあまり大きな影響を与えない	積極的な管理策は行わない。

6.2. 管理策の選択

※記載が冗長になるため、詳細管理策は表題だけの記載とする。

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。

5.2　要員のセキュリティ

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

5.3　物理的及び環境的セキュリティ

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

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

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
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

CSMS認証基準(IEC 62443-2-1) JIP-CSCC100-1.0より引用

CSMS 認証基準 5 章に示された詳細管理策の中から、対処すべきと判断されたリスクに対抗するために有効な管理策を選択します。また、管理策の採否やその理由についてとりまとめた「適用宣言書」を作成します。表 6-2 に適用宣言書のイメージ例を示します。

表 6-2 適用宣言書のイメージ例

項番	採否	理由
5.3.2 物理的セキュリティ境界の確立 保護される資産への認可されていないアクセスに対する障壁を提供する、一つ以上の物理的セキュリティ境界が確立されなければならない。	○	事業所、執務室、サーバルーム、検証室について入退管理システムや施錠管理を実施している。
5.6.2 システムの使用前のすべてのユーザの認証 入退管理技術と管理実践という補い合う組み合わせが存在しない場合は、要求されたアプリケーションを使用する前に、すべてのユーザが認証されなければならない。	×	事業所における入退管理システムと、端末及びサーバにおけるユーザ認証機能を運用しており、左記のケースに該当しないため不要

適用宣言書は、ISMS 同様 CSMS 認証の審査においても重要な役割を持っています。審査では、適用宣言書から、すでに実施済の管理策も含め、その管理策を採用することによって、どのようなリスクに対応し、どの資産を守ることができるかについて確認されます。また、管理策を採用しない場合、その理由が合理的であること（リスクが移転されている、リスクが存在していない等）を確認します。

6.3. 管理策の導入

4.3.4.2　リスクマネジメント及び導入

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-CSCC100-1.0 より引用

6.2 節で選択した管理策を導入します。リスクの対処は、組織が許容できる期間内に行う必要があるため、その期間を念頭に置いた管理策の適切な導入計画の策定が求められます。ただ、新たなプロセスや基準を持ち込むのではなく、従来から行っていた活動をブラッシュアップし、PDCA サイクルを適用する方向で整理し、CSMS の管理策へと発展させる方法も有効です。

管理策の導入・運用に係る課題は、内容や組織の状況によって異なりますが、CSMS 認証等で指摘を受けることが多い点として、たとえば以下のものが挙げられます。

・ 派遣や業務委託先の従事者等に対する採用基準の改訂

CSMS の観点が採用基準に反映されていない。

・ 重要サーバの管理の徹底

重要サーバは社内に設置されており、CSMS の適用範囲を意識した管理（施錠管理、アクセス権限管理等）を行っていない。

・ 記憶媒体の管理の徹底

記憶媒体の貸出時の管理は徹底されているが、返却後の管理に曖昧な点がある。

6.4. 共通の管理策の選択

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-CSCC100-1.0 より引用

物理的セキュリティとサイバーセキュリティが密接に関連している場合には､そのどちらかが損なわれると両方にダメージが及ぶケースもあります。したがって、物理面、サイバー面の両方に影響しうるリスクがある場合、これに対抗する管理策の役割は重要であり、その適用は必須と考えられます。

6.5. 新規システムの開発又は既存システムの変更

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

IACSのそれぞれの新しいコンポーネントのセキュリティ機能及び能力が事前に定義され、それが開発されるか、調達によって実現されなければならず、また、システム全体が望ましいセキュリティプロファイルに合致するように、このコンポーネントが他のコンポーネントとともにテストされなければならない。

5.8.2　変更管理システムの開発及び導入

IACS環境のための変更管理システムが開発され、導入されなければならない。変更管理プロセスは、利害の対立を防ぐため、職務分離の原則に従わなければならない。

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

提案された、IACSに対する変更は、明確に定義された基準を使用して、産業活動及びIACSシステムに関する技術的知識を持つ個人によって、HSEリスク及びサイバーセキュリティリスクに対してそれらの変更が及ぼす潜在的影響に関してレビューされなければならない。

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

既存のゾーン内のIACS環境に設置される新しいシステムのセキュリティ要求事項は、そのゾーン／環境において要求されるセキュリティのポリシー及び手順に合致していなければならない。同様に、保守によるアップグレード又は変更が、そのゾーンのセキュリティ要求事項に合致していなければならない。

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

サイバーセキュリティの変更管理手順が、既存のPSMの手順に統合されなければならない。

5.8.6　ポリシー及び手順のレビュー及び維持管理

セキュリティ上の変更によって安全性又は事業継続に対するリスクが増大しないことを確実にするために、運用及び変更管理のポリシー及び手順がレビューされ、最新の状態に維持されなければならない。

5.8.7　パッチマネジメント手順の確立及び文書化

パッチマネジメントの手順を確立し、文書化し、それに従わなければならない。

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

ウイルス対策／マルウェアマネジメントの手順を確立し、文書化し、それに従わなければならない。

5.8.9　バックアップ及び復元の手順の確立

コンピュータシステムのバックアップ及び復元並びにバックアップコピーの保護のための手順が確立され、使用され、適切なテストによって検証されなければならない。

CSMS認証基準(IEC 62443-2-1) JIP-CSCC100-1.0より引用

システムの開発・保守に伴う CSMS の取り組みです。例えば、顧客の IACS の開発・保守を行うシステムインテグレータの場合、本項の取り組みを通じて、顧客の IACS 環境を保護することができます。ただし、IACS のセキュリティの必要性を判断するのは顧客であり、システムインテグレータは IACS のセキュリティ強化の重要性を説明し、管理策を提案する立場です。

6.6. 上位レベル及び詳細なリスクアセスメントの更新

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。

CSMS 認証基準(IEC 62443-2-1) JIP-CSCC100-1.0 より引用

適切なタイミングで上位レベル及び詳細なリスクアセスメントを更新する必要があります。更新のトリガーとしては、たとえば以下のケースが挙げられます。

・IACS の新規システム導入時
・IACS のシステム更新時
・IACS のシステムの変更
・法律・規制の変更
・IACS に対するリスクの変化

6.7. 事業継続性及びインシデント対応計画の更新

6.7.1. 事業継続計画

5.1 事業継続計画

5.1.1 復旧目標の規定

組織は、事業継続計画を作成する前に、事業上の必要性に基づいて関与するシステムの復旧目標を規定しなければならない。

5.1.2 各システムに対する影響及び結果の決定

組織は、重大な動作中断による各システムへの影響と、システムの一つ以上が喪失することに関連する結果を決定しなければならない。

5.1.3 事業継続計画の策定及び導入

ビジネスプロセスを復旧目標に従って復元できることを確実にするために、継続計画が策定及び導入されなければならない。

5.1.4 事業継続チームの結成

IACS及びその他のプロセスの所有者が含まれている事業継続チームが結成されなければならない。重大な動作中断が発生した場合は、このチームが、運用を再確立するための重要な業務システム及びIACSシステムの優先順位を決定しなければならない。

5.1.5 具体的な役割及び責任の定義及び伝達

事業継続計画は、計画の各部分の具体的な役割及び責任を定義し、伝達しなければならない。

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

組織は、事業継続計画を支援するバックアップ及び復元の手順（5.8.9参照）を作成しなければならない。

5.1.7 事業継続計画のテスト及び更新

事業継続計画は、定期的にテストされ、必要に応じて更新されなければならない。

CSMS 認証基準(IEC 62443-2-1) JIP-CSCC100-1.0 より引用

事業継続計画は、原因を問わず、重要な機能が失われたと仮定して、許容される停止時間がどれだけあるか、その間に機能を回復するためにどうすればよいかを分析して導出した、必要な手順や準備に関する計画です。

事業継続計画については、単に計画を策定するだけでなく、演習や訓練を通じて、計画の検証・改善、実装を図ることが必要です。

以下に、一般的な事業継続計画の策定・運用に関する作業を例示します。

① 復旧目標の規定
② 事業継続計画の策定及び導入
③ 事業継続チームの結成
④ バックアップ手順の作成
⑤ 事業継続計画のテスト及び更新

6.7.2. インシデントの計画及び対応

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

責任を持つ要員を識別し、指定された個人によって実行されるアクションを定義するインシデント対応計画を、組織は導入しなければならない。

5.10.2 インシデント対応計画の伝達

すべての適切な組織に、インシデント対応計画が伝達されなければならない。

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

組織は、実際にはサイバーセキュリティインシデントである可能性がある通常と異なる活動及び事象を伝達するための報告手順を確立しなければならない。

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

従業員は、サイバーセキュリティインシデントを報告する責任及びこれらのインシデントを報告する方法に関して、教育を受けなければならない。

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

組織は、タイムリーな方法でサイバーセキュリティインシデントを報告しなければならない。

5.10.6 インシデントの識別及び対応

インシデントが識別された場合、組織は、確立された手順に従って直ちに対応しなければならない。

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

組織は、失敗した及び成功したサイバーセキュリティ侵害を識別するための手順を導入しなければならない。

5.10.8　インシデントの詳細の文書化

インシデント、対応、学んだ教訓、及びこのインシデントを踏まえてCSMSを変更するためにとられたあらゆるアクションを記録するために、識別されたインシデントの詳細が文書化されなければならない。

5.10.9　インシデントの詳細の伝達

インシデントの文書化された詳細が、すべての適切な組織（つまり、経営陣、IT、プロセス安全性、オートメーション及び制御の工学的セキュリティ並びに製造）に、時機を逸しない方法で伝達されなければならない。

5.10.10　発見された問題点に対する対処及び修正

発見された問題点に対処し、それらが修正されていることを確実にするための事業上の方法を、組織は導入しなければならない。

5.10.11　演習の実行

インシデント対応プログラムを定期的にテストするために、演習が実行されなければならない。

CSMS認証基準(IEC 62443-2-1) JIP-CSCC100-1.0より引用

IACS の場合、情報系と同様のマルウェアの検出ツールが少なく、インシデントの把握が難しいとされています。サイバー攻撃を受けていても、影響が明確に顕在化しなければ、オペレータが異常を検知するのは困難です。また、問題が顕在化した際も、その原因がサイバー攻撃によるものとすぐに判断できる可能性は低いと考えられます。

そのため、発生したインシデント情報を迅速に収集する仕組みが必要です。併せて、インシデント未遂（ヒヤリハット）の情報についても収集し、内在する問題について改善を図る取り組みも有効です。

7. CSMS の維持管理

CSMS は構築するだけでなく、適切に運用されなければなりません。本章では、CSMS の維持管理に必要な作業について解説します。

7.1. 法律及び規制の制約の監視

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。

CSMS 認証基準(IEC 62443-2-1) JIP-CSCC100-1.0 より引用

適用範囲におけるサイバーセキュリティに関連する法令を識別しなければなりません。たとえば、IACS が関わる業務分野に影響する法令として、次のものが挙げられます。

- 刑法
- 不正アクセス行為の禁止等に関する法律
- 建築基準法／同施行令
- 消防法／同施行令／同施行規則
- 不正競争防止法
- 著作権法
- その他各種業法（IACS が関わる業種・業界の規制法等）

これらの法令については、どのような基準に基づいて遵守性を判断するかなど、監視や測定の具体的なフレームを用意することが求められます。また法令の改正状況については、常に監視することが必要です。

7.2. 業界の実践の監視

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。

CSMS 認証基準(IEC 62443-2-1) JIP-CSCC100-1.0 より引用

同業他社の CSMS の導入・運用状況を監視し、優れた取り組みがあれば参考にして、自身への適用可能性について検討することが望まれます。参考にするポイントとしては、たとえば、リスクの捉え方、リスクへの対処（有効性、合理性、低コスト、技術的ハードル等）

が挙げられます。

7.3. CSMS の有効性の測定

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。

CSMS 認証基準(IEC 62443-2-1) JIP-CSCC100-1.0 より引用

CSMS の有効性を客観的に把握するために、できる限り定量的な指標が必要とされます。たとえば､インシデント件数､ヒヤリハット事例､ルール不遵守といったトラブルの頻度や、ぜい弱性対応状況、従業員による CSMS の理解度、内部監査の指摘数などの指標を活用することが考えられます。

7.4. CSMS への準拠の監査

4.3.4.4.7　情報及び文書のマネジメントプロセスの監査

情報及び文書のマネジメントポリシーへの準拠に関する定期的なレビューが実行されなければならない。

4.4.2　適合

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-CSCC100-1.0より引用

CSMS に関する内部監査は、改善が必要な事項を明確にするために行います。内部監査を実施するためには、チェックリストと要員の確保が必要となります。

チェックリストとして、たとえば CSMS 認証基準の 4 章、5 章（うち 6.2 節で選択した詳細管理策）の要求項目に基づきチェック項目を作成するとともに、監査の対象を設定します。

また、CSMS に関する内部監査員をどのように確保するか、監査員としての力量をどのように判断するかも CSMS 導入段階の課題となります。特に、内部監査資格者に求められる能力について規定すること、また担当者が十分な力量を有することを客観的に説明できるよう、エビデンスを用意することが望まれます。

さらに、監査作業においては、確認した内容や証跡を記録することが重要です。将来的には、基準への適合性のみならず、CSMS における PDCA サイクル（Plan－Do－Check－Act）が回っており、有効性が確保されているかを確認することも重要となります。

内部監査の詳細は、ISO19011:2011「マネジメントシステム監査のための指針」を参照してください。

7.5. CSMS のレビュー

4.4.3　CSMSのレビュー、改善及び維持管理

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。

4.4.3.5　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。

CSMS認証基準(IEC 62443-2-1) JIP-CSCC100-1.0より引用

組織は、CSMSに関する過去の有効性と今後の見込みのアセスメントを行うため、CSMSの状況を定期的にレビューすることが求められます。

個別の取り組みについては、活動計画にレビューの時期を定め、進捗を管理することが望まれます。その際、目的はCSMS認証基準を網羅することではなく、IACSの保護であることを周知し、PDCAが「作業のための作業」に陥らないように留意すべきです。

7.6. CSMSの改良

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。

4.4.3.8　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-CSCC100-1.0より引用

CSMSに何らかの問題がある場合、適切な是正処置や予防処置の導入が必要になります。是正処置の対象は、たとえばセキュリティ事故やヒヤリハット、ルール不遵守等から抽出される問題点が該当します。したがって、それらを把握するための情報収集の仕組みを整備することが望まれます。

また、従業員からのセキュリティ上の改善提案を収集し、活用する仕組みを整えることで、合理的に是正処置や予防処置を識別するとともに、従業員の参加意識も高めることができます。

8. システムインテグレータにとっての CSMS

顧客の IACS を開発するシステムインテグレータは、CSMS 認証基準における「IACS」の記載を「IACS の開発環境及びそこで開発されるアプリケーション」に読み替える方向で、CSMS の導入や認証取得に取り組むことが想定されています。「IACS の開発環境」とは開発・検査・出荷に関わるシステムであり、「そこで開発されるアプリケーション」とは納入システム（生産設備を制御するシステム）をさしています。

ただし、実際は、機械的な読み替えは困難です。パイロット認証を通じて明らかになった、特に読み替えが難しいと思われる CSMS 認証基準の項目について、以下に記載します。

(1) 4.2.3.1　リスクアセスメント方法の選択

条文では、「組織の IACS 資産に関連するセキュリティ上の・・・」の冒頭から始まり、この“組織の IACS 資産”は、明らかにプラント事業者の IACS 設備と読み取れます。ただし、本箇条はリスクアセスメント方法についての CSMS 認証基準独自の重要な要件との判断から、パイロット認証では読み替えを選択しました。

(2) 4.2.3.4　IACS の識別

セキュリティリスクを識別する対象が“装置”とあることから、IACS 実運用環境における装置を指し、読み替えることは難しいと考えられます。

(3) 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

システムインテグレータ向けの HSE をどう捉えるかが課題となります。適用範囲の開発環境（OA 環境）の観点では、火災・震災等に備えた管理策が考えられます。

(4) 5.4.1　ネットワーク分割アーキテクチャの策定

IEC62443 におけるセキュリティゾーンの考え方は、「重要な IACS 装置を共通のセキュリティレベルを持つゾーンで分離する」とあり、CSMS 認証基準においても、ネットワーク分割対抗策の対象が「IACS 装置」となっています。システムインテグレータでも、開発環境における重要システムを社内ネットワークと分割する管理策を導入している場合、重要システムが IACS 装置と同様な位置づけとみなせると考えられます。

(5) 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

この「IACS 装置」を、たとえば適用範囲における開発環境の重要システムとして位置付け、論理的許可や物理的許可の権限管理についての対応を検討する方向が考えられます。

(6) 5. 8.1　セキュリティ機能及び能力の定義及びテスト

開発・導入する新たなコンポーネントを納入システムに適用するか、あるいは開発環境のセキュリティ機能に適用するかで判断が分かれます。システムインテグレータとしては、前者で扱うことが考えられます。

(7) 5.8.5 サイバーセキュリティ及びプロセス[6]安全性マネジメント（PSM: Process Safety Management）の変更管理手順の統合

本来プラントに求められる PSM をシステムインテグレータの開発環境（たとえば一般的な情報システムとネットワーク）に適用するのは難しいところですが、たとえば HSE と同義と捉えることも考えられます。

(8) 5.8.6　ポリシー及び手順のレビュー及び維持管理

システムインテグレータとしては、CSMS のライフサイクルにおける変更により増大するリスクにおいて、納入するシステムが客先環境で安全であることまで配慮した、開発プロセスにおける変更のレビューを考慮することが望まれます。

[6] Process は本来プラントにおける製造装置，タンク，配管やボイラー等を指す。

9. CSMS 認証の取得

2～7 章では、CSMS の構築・運用に関する取り組みを紹介しました。CSMS 適合性評価制度（以下、CSMS 制度[7]という。）は、これらの取り組みが適切に実施され、CSMS 認証基準に適合していることを第三者から認証してもらう仕組みです。

認証審査等のプロセスの流れは、以下の通りです。

① 準備・申請
② 第一段階審査
③ 第二段階審査
④ サーベイランス（定期審査）
⑤ 再認証審査

9.1. 準備・申請

9.1.1. 認証基準に基づく文書・規程・体制等の整備

CSMS 認証においては、CSMS 認証基準に適合していることを確認できるように、文書類を用意する必要があります。

・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提供する基本的な方針を明文化します。場合によっては、組織が IACS のサイバーセキュリティを管理しなければならない事業上の根拠も記載します。

・適用範囲定義書

CSMS の適用範囲として、体制・要員、物理的拠点、システム・ネットワーク構成等を明記した資料。その際、文書改訂の頻度等を考慮し、適用対象の人数等変動する可能性が高い情報については別紙に記載して、本紙から参照するほうが合理的です。

・資産台帳

CSMS の適用範囲となる IACS 及びその関連機器、情報について洗い出し、管理します。

・CSMS 適用宣言書

リスクアセスメントの結果に基づき、対処が必要なリスク項目について、5 章に記載された詳細管理策の適用を行うかどうかの判断とその理由を記載した文書です。その際、ある管理策が別のリスクを招く可能性に留意する必要があります。たとえば、可用性確保のためにバックアップをとることで、機密性を損ねる可能性が生じ

[7] CSMS 制度における「CSMS」とは、制御システムに関するセキュリティマネジメントシステムのことである。（2014 年 4 月 25 日付経済産業省発行ニュースリリース）

ます。

これらの取り組みに際し、以下の点に留意することが望まれます。

- 適切な文書管理のため、文書番号や改訂履歴を整えることが望まれます。
- 業界内の特殊な専門用語については、可能な範囲で理解しやすい一般的な用語に置き換えることが望まれます。
- CSMS 認証基準について読み込み、既存の作業との適合性を検討することによって、文書・規程の整備や管理策適用の作業をより合理的に、かつ導入コストを下げる形で進めることができます。

9.1.2. レビュー、監査の実施

第二段階審査までに、リスクアセスメントや管理策の適用だけでなく、内部監査やマネジメントレビュー等のプロセスまで一通り完了することが求められます。

マネジメントレビューは、CSMS の運用が適切、妥当かつ効果的であることを経営陣が確認するために重要です。マネジメントレビューのインプットは、リスク対応の計画や実施状況、内部監査の結果等に加え、従業員からの改善提案、取引先や委託先等の利害関係者からのフィードバック等も反映することが望まれます。マネジメントレビューの結果は、第二段階審査で確認されます。

また、内部監査の結果、指摘事項がある場合は、その是正処置についても第二段階審査で確認される点に留意しましょう。

9.2. 第一段階審査

第一段階審査は、主に第二段階審査への準備が整っているかどうかを審査員が判断します。内容としては、重大な指摘事項の可能性の確認、サイトツアー、文書類の確認が行われます。

第一段階審査では、主に文書類の整備状況を中心に審査されます。最終的には、このまま放置すると第二段階審査で指摘事項となる懸念がある項目（懸念領域）が抽出されます。

懸念領域として以下が確認された場合、第二段階審査への移行が認められません。

・適用範囲に妥当性がない

・重大な不適合の可能性がある

・内部監査、マネジメントレビューを第二段階審査までに実施する計画がない

万が一、審査結果などに異議がある場合には、異議申し立てを行う制度があります。

9.3. 第二段階審査

第一段階審査の結果を踏まえ、審査員が当該組織の運用する CSMS の要求事項への適合状況と有効性を評価し、認証に向けて推薦できるか否かを審査員が判断します。

第二段階審査では、経営陣へのインタビュー、従業員へのインタビューなどを含め、主に CSMS の運用状況を中心に審査されます。たとえば、リスクアセスメントにより抽出された対処すべきリスクについて、第二段階審査より前に管理策の適用や改善に関する計画を策定することが求められます。また、内部監査の結果やマネジメントレビューの結果及びその是正処置、さらに、第一段階審査で懸念領域との指摘を受けた点についての対応状況も確認されます。

重大な不適合が指摘された場合には、認証の推薦がなされないことがあり、再審査となります。万が一、判定などに異議がある場合には、異議申し立てを行う制度があります。

9.4. サーベイランス（定期審査）

認証登録は、認証書の発行日から 3 年間有効です。次の認証更新まで状況を維持・改善していくためには、定期審査を受ける必要があります。定期審査は、認証の有効期間中、定期的に行われる審査で、通常は 1 年毎[8]に実施されます。サーベイランスでは、前回審査で指摘された是正処置の実施状況の確認（フォローアップ）と、運用状況の確認（要求事項に対する適合性、有効性）という観点で審査が行なわれます。

9.5. 再認証審査

再認証審査は 3 年毎に行われます。通常は、認証の有効期限が切れる数ヶ月前に実施します。

9.6. 適用範囲の拡大・展開

組織として、CSMS 認証の適用範囲を段階的に拡大することを選択する場合があります。拡大の方向としては、体制・要員（部署、事業・業務等）、物理的拠点（施設・設備、工場等）、システム・ネットワーク構成（システム・機器、ネットワークのレイヤ、セグメント等）などがあります。

組織において特定の物理的拠点・生産設備を最初の適用範囲とした場合、対象の拠点や設備を広げていく方向が考えられます。また、システムインテグレータにおいて特定の部署における特定システムの開発業務を最初の適用範囲とした場合、当該部署の別業務へ展開する

8 自組織と審査機関の合意により，もっと短い間隔で行う場合もある。

ことが考えられます。

なお、海外拠点に展開する場合、既存の適用範囲における取り組みをそのまま流用するのではなく、言語や文化、商慣習、法制度等の違いを考慮する必要があります。たとえば、サイバーセキュリティポリシーの内容をそのまま英語に訳しても、意図が正しく伝わらない可能性があります。

付録１　IEC 62443 と他の規格との関係

（１）IEC 62443 の構成

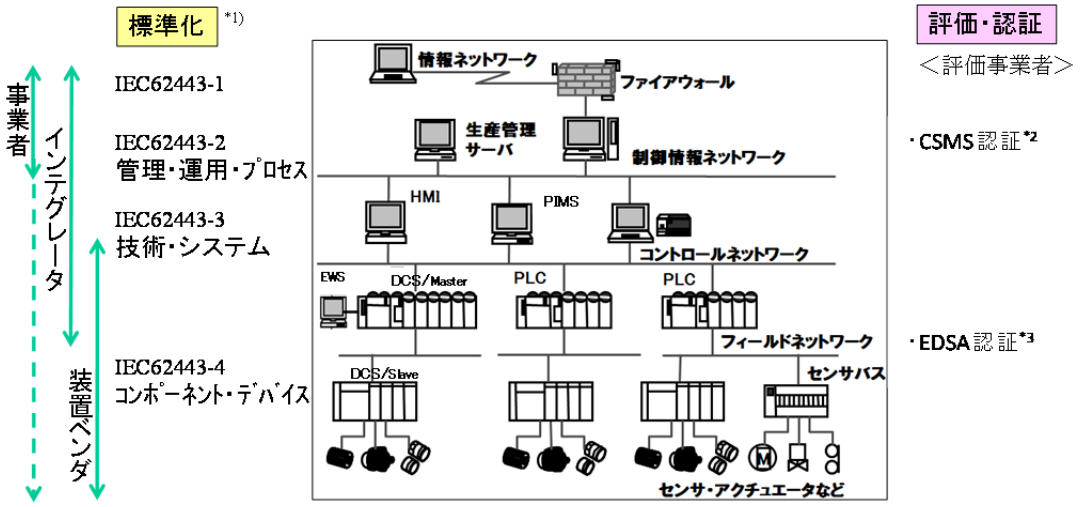
IEC 62443 シリーズは、制御システムのセキュリティ実現に活用できる基準の一つです。

・IEC 62443-1：この規格全体の用語・概念等の定義

・IEC 62443-2：組織に対するセキュリティマネジメントシステム

・IEC 62443-3：システムのセキュリティ要件や技術概説

・IEC 62443-4：部品(装置・デバイス)層におけるセキュリティ機能や開発プロセス要件



*1) IEC62443 の Cyber security の標準化作業は、IEC/TC65/WG10 が担当。(日本国内事務局は JEMIMA が対応)
*2) Cyber Security Management System：ISMS を制御システム関連組織向けに特化した要求事項を規定
*3) EDSA:Embedded Device Security Assurance：制御機器(コンポーネント)の認証プログラム→IEC62443-4 に提案されている

図 0-1 制御システムにおける IEC62443 セキュリティ標準の全体像

（出所：IPA「IEC62443 及び CSMS/EDSA 規格の詳細」[9]、 2013/03 に一部加筆修正）

（２）マネジメントシステム認証（CSMS）と製品認証（EDSA）の関係

マネジメントシステム認証（CSMS）は、システムオーナーや運用・保守事業者、システムインテグレータが対象ですが、製品認証（EDSA）は機器が対象の規格です。

なお、ISA Security Compliance Institute（ISCI）が制御システムコンポーネント（製品）の認証プログラムである EDSA 認証（Embedded Device Security Assurance Certification program）を実施しています。

IEC 62443-4-1 及び IEC 62443-4-2 については、現在標準化中(2014 年 6 月時点)です。

9　https://www.ipa.go.jp/files/000026445.pdf

（３）CSMS と ISMS の関係

CSMS 認証基準である IEC 62443-2-1 は、ISO/IEC 27001：2005 の要求事項を参考に、制御システムをサイバー攻撃から守るための固有のセキュリティ対策を追加して作成されているため、ISMS と同様の要件が多数記載されています。そのため、ISMS を既に取得している企業では、CSMS を実現するために必要なプロセスの多くを経験していると考えられます。

独立行政法人情報処理推進機構（IPA）のレポート[10]によると、IEC 62443-2-1 と ISO/IEC 27001：2005 に記載されている要件を比較した結果、「大半の要件は共通であり、固有要件は少数であることが明らかとなった」とされています（付録 2 参照）。

また、同レポートでは、リスク分析、対策立案、レビューの CSMS の各ステップにおいて、IEC 62443-2-1 にのみ記載されている要件をマッピングし、その結果から IEC 62443-2-1 では、「セーフティ（人、環境等）に対するリスクの洗い出しやライフサイクル全般（開発～廃棄）までの各ステップにおけるリスクの洗い出し」、「災害時やシステム更新時にセキュリティレベルや安全性が低下しないような対策機能の実装や運用」を実施することが求められていると指摘しています。

現在、ISO/IEC 27001:2005 版は改正され、ISO/IEC 27001:2013 版が発行されています。IEC 62443-2-1 と ISO/IEC 27001:2013 に記載されている要件を比較した結果については付録 3 に示す通りです。

ただし、ISO/IEC 27001：2013 附属書 A の A.17 の管理策では組織全体の事業継続管理には言及せず、事業継続管理（マネジメント）における情報セキュリティの側面に視点を置いているため、付録 3 にはその比較結果が反映されていないことに留意されたい。

---

[10] IPA「制御システムにおけるセキュリティマネジメントシステムの構築に向けて ～ IEC62443-2-1 の活用のアプローチ ～」,2012 年 10 月
https://www.ipa.go.jp/about/press/20121010.html

付録 2　ISO/IEC 27001：2005 になく CSMS 認証基準（IEC 62443-2-1）にだけある要求事項（CSMS 固有要件）

CSMS 認証基準（Ver.1.0）	IEC 62443-2-1	
	項番	要件
4．サイバーセキュリティマネジメントシステム		
4.2 リスク分析		
4.2.3　リスクの識別、分類及びアセスメント		
4.2.3.2　リスクアセスメントの背景情報の提供	4.2.3.2	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。
4.2.3.5　単純なネットワーク図の策定	4.2.3.5	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。
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	4.2.3.11	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	4.2.3.12	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。
4.3 CSMS によるリスクへの対処		

CSMS 認証基準（Ver.1.0）	IEC 62443-2-1	
	項番	要件
4.3.2 セキュリティポリシー、組織及び意識向上		
4.3.2.3.2　セキュリティ組織の確立	4.3.2.3.2	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。
4.3.2.4.5　訓練プログラムの経時的な改訂	4.3.2.4.5	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。
4.3.2.6.3　リスクマネジメントシステム間の一貫性の維持	4.3.2.6.3	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。
4.4　CSMS の監視及び改善		
4.4.3　CSMS のレビュー，改善及び維持管理		
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	4.4.3.1	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。
4.4.3.8　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	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（Ver.1.0）	IEC 62443-2-1	
	項番	要件
５．詳細管理策		
5.2　要員のセキュリティ		
5.2.3　要員の継続的な選別	4.3.3.2.3	要員に対しては，利害の対立又は適切な方法で職務を実行することに対する懸念を示唆する可能性がある変化を確認するために，継続的な調査も行われなければならない。
5.2.7　適切な抑制と均衡を維持するための職務の分離	4.3.3.2.7	IACS の機能的運用を変更するアクションに対する完全な制御をどの一個人も持つことがないように，要員間で任務を分離して，適切な抑制と均衡を維持しなければならない。
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	4.3.3.3.1	資産を保護するための物理的セキュリティとサイバーセキュリティの両方に対処するセキュリティのポリシー及び手順が確立されなければならない。
5.3.10　重要資産の暫定的保護のための手順の確立	4.3.3.3.10	例えば火災，浸水，セキュリティ侵害，中断，天災又はその他のあらゆる種類の災害が原因となって運用が中断しているときに重要なコンポーネントを確実に保護するための手順が確立されなければならない。
5.5　アクセス制御－アカウント管理		
5.5.5　不要なアカウントの一時停止又は削除	4.3.3.5.5	アクセスアカウントは，（例えば職務の変更によって）もはや不要になったらすぐに一時停止又は削除されなければならない。
5.6　アクセス制御－認証		

CSMS 認証基準（Ver.1.0）	IEC 62443-2-1	
	項番	要件
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	4.3.3.6.3	すべてのシステム管理者アクセスアカウント及びアプリケーション構成アクセスアカウントでは，強い認証実践（強いパスワードを要求するなど）が使用されなければならない。
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	4.3.3.6.7	リモートユーザによる一定回数の失敗したログイン試行の後に，システムがそのアクセスアカウントを一定期間無効にしなければならない。
5.6.9　タスク間通信での認証の採用	4.3.3.6.9	システムでは，アプリケーションと装置の間のタスク間通信に対する適切な認証方式が採用されなければならない。
5.7　アクセス制御－認可		
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	4.3.3.7.2	IACS 装置へのアクセスの許可は，論理的であるか（既知のユーザに，それらのユーザの役割に基づいてアクセスの付与又は拒否を行う規則），物理的であるか（実行中のコンピュータコンソールへのアクセスを制限する錠，カメラ及びその他の管理策），又はその両方でなければならない。
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	4.3.3.7.3	アクセスアカウントは，そのユーザの役割に対して適切な情報又はシステムへのアクセスを管理するために，役割に基づいていなければならない。役割を定義するときには，安全性に対する影響が考慮されなければならない。
5.7.4　重要な IACS に対する複数の認可方法の採用	4.3.3.7.4	重要な制御環境では，複数の認可方法を採用して，IACS へのアクセスを制限しなければならない。
5.8　システムの開発及び保守		

CSMS 認証基準（Ver.1.0）	IEC 62443-2-1	
	項番	要件
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	4.3.4.3.4	既存のゾーン内の IACS 環境に設置される新しいシステムのセキュリティ要求事項は，そのゾーン／環境において要求されるセキュリティのポリシー及び手順に合致していなければならない。同様に，保守によるアップグレード又は変更が，そのゾーンのセキュリティ要求事項に合致していなければならない。
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	4.3.4.3.5	サイバーセキュリティの変更管理手順が，既存の PSM の手順に統合されなければならない。
5.8.6　ポリシー及び手順のレビュー及び維持管理	4.3.4.3.6	セキュリティ上の変更によって安全性又は事業継続に対するリスクが増大しないことを確実にするために，運用及び変更管理のポリシー及び手順がレビューされ，最新の状態に維持されなければならない。
5.9　情報及び文書のマネジメント		
5.9.5　情報の分類の維持管理	4.3.4.4.6	特別な管理又は処置を必要とする情報は，特別な処置がまだ必要であることを検証するために，定期的にレビューを実行しなければならない。
5.10　インシデントの計画及び対応		
5.10.2　インシデント対応計画の伝達	4.3.4.5.2	すべての適切な組織に，インシデント対応計画が伝達されなければならない。
5.10.10　発見された問題点に対する対処及び修正	4.3.4.5.10	発見された問題点に対処し，それらが修正されていることを確実にするための事業上の方法を，組織は導入しなければならない。

付録 3　ISO/IEC 27001：2014 になく CSMS 認証基準（IEC 62443-2-1）にだけある要求事項（CSMS 固有要件）

CSMS 認証基準（Ver.1.0）	IEC 62443-2-1	
	項番	要件
4．サイバーセキュリティマネジメントシステム		
4.2 リスク分析		
4.2.3　リスクの識別、分類及びアセスメント		
4.2.3.3　上位レベルのリスクアセスメントの実行	4.2.3.3	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。
4.2.3.5　単純なネットワーク図の策定	4.2.3.5	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。
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	4.2.3.11	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。
4.3 CSMS によるリスクへの対処		
4.3.2 セキュリティポリシー、組織及び意識向上		

CSMS 認証基準（Ver.1.0）	IEC 62443-2-1	
	項番	要件
4.3.2.4.5　訓練プログラムの経時的な改訂	4.3.2.4.5	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。
4.3.2.6.3　リスクマネジメントシステム間の一貫性の維持	4.3.2.6.3	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。
4.4　CSMS の監視及び改善		
4.4.3　CSMS のレビュー，改善及び維持管理		
4.4.3.6　業界の CSMS 戦略の監視及び評価	4.4.3.6	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。
4.4.3.8　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	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。
5．詳細管理策		
5.2　要員のセキュリティ		
5.2.3　要員の継続的な選別	4.3.3.2.3	要員に対しては，利害の対立又は適切な方法で職務を実行することに対する懸念を示唆する可能性がある変化を確認するために，継続的な調査も行われなければならない。

CSMS 認証基準（Ver.1.0）	IEC 62443-2-1	
	項番	要件
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	4.3.3.3.1	資産を保護するための物理的セキュリティとサイバーセキュリティの両方に対処するセキュリティのポリシー及び手順が確立されなければならない。
5.3.10　重要資産の暫定的保護のための手順の確立	4.3.3.3.10	例えば火災，浸水，セキュリティ侵害，中断，天災又はその他のあらゆる種類の災害が原因となって運用が中断しているときに重要なコンポーネントを確実に保護するための手順が確立されなければならない。
5.6　アクセス制御－認証		
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	4.3.3.6.5	組織は，リモート対話ユーザを明確に識別するために，適切な強度レベルの認証方式を採用しなければならない。
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	4.3.3.6.6	組織は，失敗したログイン試行及び活動のない期間に対する適切なシステム対応を定義した，ユーザによる制御システムへのリモートログイン及び／又は制御システムへのリモート接続（例えば，タスク間接続）に対処するポリシーを策定しなければならない。
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	4.3.3.6.7	リモートユーザによる一定回数の失敗したログイン試行の後に，システムがそのアクセスアカウントを一定期間無効にしなければならない。

CSMS 認証基準（Ver.1.0）	IEC 62443-2-1	
	項番	要件
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	4.3.3.6.8	定義済みの，活動のない期間が経過した後は，リモートユーザがシステムに再度アクセスできるようになる前に，リモートユーザに再認証が要求されなければならない。
5.6.9　タスク間通信での認証の採用	4.3.3.6.9	システムでは，アプリケーションと装置の間のタスク間通信に対する適切な認証方式が採用されなければならない。
5.7　アクセス制御－認可		
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	4.3.3.7.3	アクセスアカウントは，そのユーザの役割に対して適切な情報又はシステムへのアクセスを管理するために，役割に基づいていなければならない。役割を定義するときには，安全性に対する影響が考慮されなければならない。
5.7.4　重要な IACS に対する複数の認可方法の採用	4.3.3.7.4	重要な制御環境では，複数の認可方法を採用して，IACS へのアクセスを制限しなければならない。
5.8　システムの開発及び保守		
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	4.3.4.3.4	既存のゾーン内の IACS 環境に設置される新しいシステムのセキュリティ要求事項は，そのゾーン／環境において要求されるセキュリティのポリシー及び手順に合致していなければならない。同様に，保守によるアップグレード又は変更が，そのゾーンのセキュリティ要求事項に合致していなければならない。

CSMS 認証基準（Ver.1.0）	IEC 62443-2-1	
	項番	要件
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	4.3.4.3.5	サイバーセキュリティの変更管理手順が，既存の PSM の手順に統合されなければならない。
5.9　情報及び文書のマネジメント		
5.9.4　長期記録の取得の保証	4.3.4.4.5	長期記録が取得できることを確実にするための適切な対策（つまり，より新しい形式へのデータの変換又はデータの読み取りが可能な旧式の機器の保持）が採用されなければならない。
5.10　インシデントの計画及び対応		
5.10.2　インシデント対応計画の伝達	4.3.4.5.2	すべての適切な組織に，インシデント対応計画が伝達されなければならない。
5.10.11　　演習の実行	4.3.4.5.11	インシデント対応プログラムを定期的にテストするために，演習が実行されなければならない。

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。

なお、サイバーセキュリティとは、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) **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。
- 記憶媒体、センサ、アクチュエータ。

(5) 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]。

(6) 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。

(7) 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

参考文献

・一般財団法人日本情報経済社会推進協会「CSMS 認証基準（IEC 62443-2-1）（JIP-CSCC100-1.0）」、 2014/6

・一般財団法人 日本規格協会「IEC 62443-2-1 国際規格　産業用通信ネットワーク – ネットワーク及びシステムセキュリティ – 第 2-1 部：産業用オートメーション及び制御システムセキュリティプログラムの確立」第 1 版、 2010/11

・独立行政法人 情報処理推進機構「制御システムにおけるセキュリティマネジメントシステムの構築に向けて～ IEC62443-2-1 の活用のアプローチ ～」、 2012/10

・一般財団法人日本情報経済社会推進協会「ISMS ユーザーズガイド -JIS Q 27001:2014(ISO/IEC 27001:2013)対応-」、 2014/4

本資料は、経済産業省の平成 24 年度補正事業「グローバル認証基盤整備事業」の一環として作成されたものである。