CSMS 認証基準（IEC62443-2-1）

JIP-CSCC100-2.0

平成 28 年 10 月

一般財団法人日本情報経済社会推進協会

改 版 履 歴

版数	制定／改訂日	改定箇所、改訂理由	備考
0.8	2013.7.31	CSMS パイロット認証用として 0.8 版制定	初版
0.8a	2013.8.30	4.3「CSMS によるリスクへの対処」への「5.詳細管理策」の規定追加 誤記訂正： 4.3.2.5.1「復旧目標の規定」 5.10.2「4.3.3.7.2　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」の要求事項	
0.8b	2013.12.27	3.用語及び定義の追加「組織」 4.3.2.2.2「適用範囲では、CSMS の戦略目標、プロセス及びタイミングを説明しなければならない。」の及びタイミングを削除する。 用語の修正： 「事業継続性」は、「事業継続」とする。 誤記訂正： 4.3.3.1 は、4.3.4.3.1 とする。	
0.8c	2014.1.7	3.用語及び定義の追加「適用宣言書」、「管理策」、「サイバーセキュリティポリシー」 5.1「事業上の根拠」は、4.2.2「事業上の根拠」とする。 5.1.1「事業上の根拠の策定」は、4.2.2.1「事業上の根拠の策定」とする。	
0.8d	2014.2.7	3.用語及び定義の追加「産業用オートメーション及び制御システム（IACS)」、「不適合」。 欠番であった 4.3.2.1、4.3.3、4.3.3.1、4.3.4、4.3.4.1、4.4、4.4.1 を追加。 詳細管理策 5.2.1、5.4.1、5.4.2、5.4.3 を 4 章に移動。 4.3.1 に追加の管理策が選択できることを追記。	

1.0	2014.7.2	5 章へ移動した 4 章の項番を全て削除。 詳細管理策 5.2.1、5.4.1、5.4.2、5.4.3、5.14.1、5.14.2 を 4 章に移動し、5 章の項番を振り直した。 本基準と IEC 62443-2-1 及び附属書 A（参考）との対比表を参考資料として附属書 D を追加。 CSMS 制度用として制定。	
2.0	2016.10.4	4.3.1.1 IACS 開発・構築を専門に担う組織におけるリスク対応を追加。 4.3.2.2.2　適用範囲の内容に定義についての注記を追加。	

目　　次

まえがき

この基準は、制御システムセキュリティにおけるサイバーセキュリティマネジメントシステム（以下、CSMSという）を確立、実施、維持及び継続的に改善するための一般要求事項を定めている。

この基準は、以下の本文で特段の定めのない限り、IEC 62443-2-1:2010 「Industrial communication networks-Network and system security - Part2-1:Establishing an industrial automation and control system security program」をそのまま参照する。

なお、下線を施してある要求事項は、対応国際規格に追記した事項である。

備考　この基準では、IEC 62443-2-1:2010 邦訳版（一般財団法人 日本規格協会発行）で用いられている用語を使用する。IEC 62443-2-1:2010 と内容が一致する JIS が制定された時点で、この基準で用いられている表記及び用語を、JIS で用いられているものに読み替えるものとする。

０．序文

IEC 62443-2-1:2010の邦訳版「0　序文」を参照及び適用する。

１．適用範囲

IEC 62443-2-1:2010の邦訳版「1　適用範囲」を適用する。

２．引用規格

IEC 62443-2-1:2010の邦訳版「2　引用規格」を適用する。

３．用語及び定義

IEC 62443-2-1:2010の邦訳版「3　用語及び定義」を適用するほか、次による。

3.1　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。

3.2　適用宣言書

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

3.3　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。

3.4 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のこと。

3.5 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]。

3.6 産業用オートメーション及び制御システム（IACS）

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

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）、リモート端末装置（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装置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）。
- 先進的又は多変数制御、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。

3.7 不適合（JIS Q 27000:2014-2.53 参照）

要求事項を満たしていないこと。

４．サイバーセキュリティマネジメントシステム

4.1 一般要求事項

組織は、その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、文書化したCSMSを確立、導入、運用、監視、レビュー、維持及び改善しなければならない。CSMSに要求されている要素は、IACS（Industrial Automation and Control System）をサイバー攻撃から保護するためである。

4.2 リスク分析

4.2.1 概要

組織は次の事項を実行しなければならない。

4.2.2　事業上の根拠

組織は、次の事項を考慮し、事業上の根拠を策定しなければならない。

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。

4.2.3　リスクの識別、分類及びアセスメント

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。

4.2.3.2　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。

4.2.3.4　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。

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。

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。

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・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。

4.3.2 セキュリティポリシー、組織及び意識向上

4.3.2.1　要素グループの説明

4.3.2では、基本的なサイバーセキュリティポリシーの策定、サイバーセキュリティに対する責任を持つ組織、及びサイバーセキュリティの問題点に対する組織内の意識向上について、「CSMSの適用範囲」、「セキュリティを目的とした組織編成」、「スタッフの訓練及びセキュリティ意識向上」、「事業継続計画」及び「セキュリティのポリシー及び手順」を規定する。なお、「事業継続計画」については、「5.詳細管理策」に規定する。

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。

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。

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。

注記：ステークホルダーの定義は、IEC 62443-2-1:2010の3.1.40に定義されている。

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。

4.3.2.6　セキュリティのポリシー及び手順

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。

4.3.3　選ばれたセキュリティ対抗策

4.3.3.1　要素グループの説明

4.3.3では、適切に設計されたCSMSの一部である、セキュリティ管理策の主な種類のいくつかについて、「要員のセキュリティ」、「物理的及び環境的セキュリティ」、「ネットワークの分割」、「アクセス制御―アカウント管理」、「アクセス制御―認証」及び「アクセス制御―認可」を規定する。なお、これらの管理策については、「５．詳細管理策」に規定する。

4.3.4　導入

4.3.4.1　要素グループの説明

4.3.4では、CSMSの導入について、「リスクマネジメント及び導入」、「システム開発及び保守」、「情報及び文書のマネジメント」及び「インシデントの計画及び対応」を規定する。なお、「システム開発及び保守」、「情報及び文書のマネジメント」の一部、及び

「インシデントの計画及び対応」については、「5.詳細管理策」に規定する。

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。

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。

4.3.4.4　情報及び文書のマネジメント

4.3.4.4.1　IACS情報のライフサイクルマネジメントプロセスの策定

IACS情報のためのライフサイクル文書マネジメントプロセスが策定され，維持管理されなければならない。

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　CSMS の監視及び改善

4.4.1　概要

組織は次の事項を実行しなければならない。

4.4.2　適合

注記　JIS Q 19011:2012は、CSMSの定期的な監査の実施のための有益な手引きとなる場合がある。

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。

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。

4.4.3.4　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。

５．詳細管理策

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。

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

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）。

5.2.2　要員の初期段階の選別

政府の規制で禁止されていない限り，IACSへのアクセス（物理的アクセスとサイバーアクセスの両方）を付与されるすべての要員は，新規雇用及び機密を扱う地位への内部異動を含め，選別されなければならない。この選別には，職務応募プロセスにおける身元の検証及び経歴の確認を含まなければならない。

5.2.3　要員の継続的な選別

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。

5.2.4　セキュリティ上の責任への対処

要員のセキュリティポリシーでは，機密を扱う地位に対しては特に，採用から雇用終了に至るまでのセキュリティ上の責任に対処しなければならない。

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

セキュリティ上の期待事項及び責任が明確に文書化され，要員に定期的に伝達されなければならない。

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

雇用条件では，サイバーセキュリティに対する要員の責任が明確に述べられなければならない。これらの責任は，雇用終了後の妥当な期間にわたって延長さ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

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

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。

5.3.2　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。

5.3.3　入退管理の実施

各障壁又は境界で適切な入退管理が提供されなければならない。

5.3.4　環境的損傷からの資産の保護

火，水，煙，粉じん，放射線，腐食，衝撃などの脅威による環境的損傷から，資産が保護されなければならない。

5.3.5　セキュリティ手順に従うことの従業員への要求

確立された物理的セキュリティ手順に従い，これを施行することが従業員に要求されなければならない。

5.3.6　接続の保護

組織の管理下にあるすべての接続が，不正変更及び損傷から適切に保護されなければならない。

5.3.7　機器資産の保守

補助的な環境機器を含むすべての機器資産が，適切な運用を保証するために適切に保守されなければならない。

5.3.8　監視及び警報の手順の確立

監視の手順，及び物理的又は環境的セキュリティが侵害された場合の警報の手順が確立されなければならない。

5.3.9　資産を追加、除去及び廃棄する手順の確立

すべての資産の追加，除去及び廃棄に関する手順が確立され，監査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

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。

5.4　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

IACSのリスクレベルに基づいて，セキュリティゾーンを採用したネットワーク分割対抗策の戦略がIACS装置用に策定されなければならない。

5.4.2　高リスクIACSの隔離又は分割の採用

セキュリティレベル又はリスクの異なる他のゾーンから高リスクIACSが隔離されているか、そのようなゾーンから高リスクIACSを分離するための障壁装置が高リスクIACSで採用されていなければならない。

5.4.3　障壁装置による不要な通信のブロック

重要な制御機器が含まれているセキュリティゾーンで送受信されるすべての不要な通信が，障壁装置によってブロック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

5.5.1　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

アクセスアカウントに対して導入されるアクセス特権は，組織の認可セキュリティポリシー（5.7.1参照）に従って確立されなければならない。

5.5.2　個人の識別

すべてのサイバーセキュリティ管理策において，個人に対するアクセスアカウントを選択するかチームに対するアクセスアカウントを選択するかは，脅威，リスク及びぜい弱性を考慮して決定されなければならない。この場合の考慮事項には，個々の管理策のHSEリスク，補助的な物理的セキュリティ管理策を使用した軽減，説明責任の要求事項，及び管理／運用上の必要事項が含まれなければならない。

5.5.3　アカウントアクセスの認可

アクセスの付与，変更又は取り消しは，適切な責任者の権限によって行われなければならない。

5.5.4　アクセスアカウントの記録

すべてのアクセスアカウントの記録が維持管理されなければならない。この記録には，アカウントの使用を認可された一人以上の個人及び装置の詳細，そのアカウントの許可，及び認可を与えた責任者が含まれなければならない。

5.5.5　不要なアカウントの一時停止又は削除

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。

5.5.6　アカウントの許可のレビュー

すべての確立されたアクセスアカウントは，一人以上の個人及び装置が必要最小限の許可のみを有することを確実にするために，定期的にレビューされなければならない。

5.5.7　デフォルトパスワードの変更

IACSを稼働させる前に，アクセスアカウントのデフォルトパスワードが変更されなければならない。

5.5.8　アカウント管理の監査

アカウント管理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。

5.6　アクセス制御－認証

5.6.1　認証方針の策定

会社は，使用する一つ以上の認証方法を定義する認証戦略又は認証アプローチを有していなければならない。

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。

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

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。

5.6.4　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

重要なシステムに対するすべてのアクセス試行がログファイルに記録されなければならず、成功したアクセス試行及び失敗したアクセス試行を確認するためにログファイルがレビューされなければならない。

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

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

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

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。

5.6.8　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

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

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

5.7.1　認可セキュリティポリシーの定義

明確に文書化され，認証を受けたすべての要員に適用される認可セキュリティポリシーにおいて，アクセスアカウントに基づいて様々な職務役割の要員に認可される特権を定義した規則が定義されていなければならない。

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

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

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

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

5.8.1　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。

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

情報分類レベル（例えば，社外秘，制限付き及び公開）が，アクセス及び制御（要求されている保護レベルに適した共有，コピー，伝達及び配布を含む）のために定義されなければならない。

5.9.2　すべてのCSMS情報資産の分類

CSMSの適用範囲内にあるすべての論理的資産（つまり，制御システムの設計情報，ぜい弱性アセスメント，ネットワーク図及び産業活動プログラム）は，その認可されていない開示又は改変がもたらす結果に見合った，要求されている保護を示すために，分類されなければならない。

5.9.3　適切な記録管理の保証

すべての資産の保持，物理的な及び完全性の保護，破棄並びに廃棄について詳細に記述するポリシー及び手順が，資産の分類（書面の及び電子的な記録，機器又は情報が含まれているその他の媒体を含む）に基づいて，法律又は規制の要求事項を考慮したうえで策定されなければならない。

5.9.4　長期記録の取得の保証

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。

5.9.5　情報の分類の維持管理

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

5.10.1　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。

附属書Ａ

IEC 62443-2-1:2010 の「附属書 A（参考） CSMS の要素の開発に関する手引き」を参照する。

附属書Ｂ

IEC 62443-2-1:2010 の「附属書 B（参考）CSMS 開発のプロセス」を参照する。

附属書Ｃ

IEC 62443-2-1:2010 の「附属書 C（参考）要求事項の ISO/IEC 27001 へのマッピング」を参照する。

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。

附属書Ｄ（参考）

本基準と IEC 62443-2-1 及び附属書 A（参考）との対比表

CSMS認証基準（Ver.2.0）	IEC 62443-2-1	
	本文	附属書A
4. サイバーセキュリティマネジメントシステム	4. サイバーセキュリティマネジメントシステム	
4.1 一般要求事項	4.1 一般要求事項	
4.2 リスク分析	4.2 リスク分析	
4.2.1 概要	4.2.1 概要	
4.2.2 事業上の根拠	4.2.2 事業上の根拠	
4.2.2.1 事業上の根拠の策定	4.2.2.1 事業上の根拠の策定	A.2.2.2、A.2.2.3、A.2.2.4
4.2.3 リスクの識別、分類及びアセスメント	4.2.3 リスクの識別、分類及びアセスメント	
4.2.3.1 リスクアセスメント方法の選択	4.2.3.1 リスクアセスメント方法の選択	A.2.3.3.2、A.2.3.3.4、A.2.3.3.5
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 リスクアセスメントの背景情報の提供	—
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 上位レベルのリスクアセスメントの実行	A.2.3.3.3、A.2.3.3.6、A.2.3.3.7
4.2.3.4 IACSの識別	4.2.3.4 IACSの識別	A.2.3.3.8.2、A.2.3.3.8.3
4.2.3.5 単純なネットワーク図の策定	4.2.3.5 単純なネットワーク図の策定	A.2.3.3.8.4
4.2.3.6 システムの優先順位付け	4.2.3.6 システムの優先順位付け	A.2.3.3.8.5、A.2.3.3.8.6
4.2.3.7 詳細なぜい弱性アセスメントの実行	4.2.3.7 詳細なぜい弱性アセスメントの実行	A.2.3.3.8.7
4.2.3.8 詳細なリスクアセスメントの方法の識別	4.2.3.8 詳細なリスクアセスメントの方法の識別	A.2.3.3.8.7
4.2.3.9 詳細なリスクアセスメントの実行	4.2.3.9 詳細なリスクアセスメントの実行	A.2.3.3.8
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	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	A.2.3.3.8.7
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 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	A.2.3.3.8.9
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 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	A.2.3.3.8.10
4.2.3.13 リスクアセスメントの文書化	4.2.3.13 リスクアセスメントの文書化	A.2.3.3.8.7
4.2.3.14 ぜい弱性アセスメントの記録の維持管理	4.2.3.14 ぜい弱性アセスメントの記録の維持管理	A.2.3.3.8.7
4.3 CSMSによるリスクへの対処	4.3 CSMSによるリスクへの対処	
4.3.1 概要	4.3.1 概要	—
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		
4.3.2 セキュリティポリシー、組織及び意識向上	4.3.2 セキュリティポリシー、組織及び意識向上	
4.3.2.1 要素グループの説明	4.3.2.1 要素グループの説明	
4.3.2.2 CSMSの適用範囲	4.3.2.2 CSMSの適用範囲	
4.3.2.2.1 CSMSの適用範囲の定義	4.3.2.2.1 CSMSの適用範囲の定義	A.3.2.2.2
4.3.2.2.2 適用範囲の内容の定義	4.3.2.2.2 適用範囲の内容の定義	A.3.2.2.2
4.3.2.3 セキュリティを目的とした組織編成	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	4.3.2.3.1 経営幹部の支援の獲得	A.3.2.3.3

CSMS認証基準(Ver.2.0)	IEC 62443-2-1	
	本文	附属書A
4.3.2.3.2　セキュリティ組織の確立	4.3.2.3.2　セキュリティ組織の確立	A.3.2.3.2
4.3.2.3.3　組織の責任の定義	4.3.2.3.3　組織の責任の定義	A.3.2.3.2
4.3.2.3.4　ステークホルダーチームの構成の定義	4.3.2.3.4　ステークホルダーチームの構成の定義	A.3.2.3.3
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　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	4.3.2.4.1　訓練プログラムの策定	A.3.2.4.2
4.3.2.4.2　手順及び設備に関する訓練の提供	4.3.2.4.2　手順及び設備に関する訓練の提供	A.3.2.4.2
4.3.2.4.3　サポート要員に対する訓練の提供	4.3.2.4.3　サポート要員に対する訓練の提供	A.3.2.4.2
4.3.2.4.4　訓練プログラムの検証	4.3.2.4.4　訓練プログラムの検証	A.3.2.4.2
4.3.2.4.5　訓練プログラムの経時的な改訂	4.3.2.4.5　訓練プログラムの経時的な改訂	A.3.2.4.2
4.3.2.4.6　従業員の訓練記録の維持管理	4.3.2.4.6　従業員の訓練記録の維持管理	A.3.2.4.2
4.3.2.6　セキュリティのポリシー及び手順	4.3.2.6　セキュリティのポリシー及び手順	
4.3.2.6.1　セキュリティポリシーの策定	4.3.2.6.1　セキュリティポリシーの策定	A.3.2.6.2
4.3.2.6.2　セキュリティ手順の策定	4.3.2.6.2　セキュリティ手順の策定	A.3.2.6.5
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　リスクマネジメントシステム間の一貫性の維持	A.3.2.6.3
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	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	A.3.2.6.2
4.3.2.6.5　リスクに対する組織の許容度の決定	4.3.2.6.5　リスクに対する組織の許容度の決定	A.3.2.6.3
4.3.2.6.6　組織へのポリシー及び手順の伝達	4.3.2.6.6　組織へのポリシー及び手順の伝達	A.3.2.6.2、A.3.2.6.5
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	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	A.3.2.6.4
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	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	A.3.2.6.2
4.3.3　選ばれたセキュリティ対抗策	4.3.3　選ばれたセキュリティ対抗策	
4.3.3.1　要素グループの説明	4.3.3.1　要素グループの説明	
4.3.4　導入	4.3.4　導入	
4.3.4.1　要素グループの説明	4.3.4.1　要素グループの説明	
4.3.4.2　リスクマネジメント及び導入	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	4.3.4.2.1　IACSリスクの継続的管理	A.3.4.2.2、A.3.4.2.3
4.3.4.2.2　共通する一連の対抗策の採用	4.3.4.2.2　共通する一連の対抗策の採用	A.3.4.2.4
4.3.4.4　情報及び文書のマネジメント	4.3.4.4　情報及び文書のマネジメント	
4.3.4.4.1　IACS情報のライフサイクルマネジメントプロセスの策定	4.3.4.4.1　IACS情報のライフサイクルマネジメントプロセスの策定	A.3.4.4.2
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	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	A.3.4.4.2
4.4　CSMSの監視及び改善	4.4　CSMSの監視及び改善	
4.4.1　概要	4.4.1　概要	
4.4.2　適合	4.4.2　適合	

CSMS認証基準(Ver.2.0)	IEC 62443-2-1	
	本文	附属書A
4.4.2.1　監査プロセスの方法の規定	4.4.2.1　監査プロセスの方法の規定	A.4.2.2
4.4.2.2　定期的なIACSの監査の実行	4.4.2.2　定期的なIACSの監査の実行	A.4.2.2
4.4.2.3　適合の尺度の確立	4.4.2.3　適合の尺度の確立	A.4.2.3
4.4.2.4　文書の監査証跡の確立	4.4.2.4　文書の監査証跡の確立	—
4.4.2.5　非適合に対する懲罰処置の定義	4.4.2.5　非適合に対する懲罰処置の定義	—
4.4.2.6　監査員の能力の確保	4.4.2.6　監査員の能力の確保	—
4.4.3　CSMSのレビュー，改善及び維持管理	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	A.4.3.5
4.4.3.2　CSMSの定期的な評価	4.4.3.2　CSMSの定期的な評価	A.4.3.3
4.4.3.3　CSMSの評価のトリガーの確立	4.4.3.3　CSMSの評価のトリガーの確立	A.4.3.3
4.4.3.4　是正処置及び予防処置の識別及び導入	4.4.3.4　是正処置及び予防処置の識別及び導入	A.4.3.3
4.4.3.5　リスク許容度のレビュー	4.4.3.5　リスク許容度のレビュー	A.4.3.3
4.4.3.6　業界のCSMS戦略の監視及び評価	4.4.3.6　業界のCSMS戦略の監視及び評価	A.4.3.3
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	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	A.4.3.4
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の要求及び報告	—
5．詳細管理策		
5.1　事業継続計画	4.3.2.5　事業継続計画	
5.1.1　復旧目標の規定	4.3.2.5.1　復旧目標の規定	A.3.2.5.2
5.1.2　各システムに対する影響及び結果の決定	4.3.2.5.2　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	4.3.2.5.3　事業継続計画の策定及び導入	A.3.2.5.3
5.1.4　事業継続チームの結成	4.3.2.5.4　事業継続チームの結成	A.3.2.5.3
5.1.5　具体的な役割及び責任の定義及び伝達	4.3.2.5.5　具体的な役割及び責任の定義及び伝達	A.3.2.5.3
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	4.3.2.5.6　事業継続計画を支援するバックアップ手順の作成	A.3.4.3.8
5.1.7　事業継続計画のテスト及び更新	4.3.2.5.7　事業継続計画のテスト及び更新	A.3.2.5.3
5.2　要員のセキュリティ	4.3.3.2　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	4.3.3.2.1　要員のセキュリティポリシーの確立	A.3.3.2.2
5.2.2　要員の初期段階の選別	4.3.3.2.2　要員の初期段階の選別	A.3.3.2.2
5.2.3　要員の継続的な選別	4.3.3.2.3　要員の継続的な選別	A.3.3.2.2
5.2.4　セキュリティ上の責任への対処	4.3.3.2.4　セキュリティ上の責任への対処	A.3.3.2.2
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	4.3.3.2.5　セキュリティ上の期待事項及び責任の文書化及び伝達	A.3.3.2.2
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	4.3.3.2.6　サイバーセキュリティに関する雇用条件の明確な記述	A.3.3.2.2

CSMS認証基準(Ver.2.0)	IEC 62443-2-1	
	本文	附属書A
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　適切な抑制と均衡を維持するための職務の分離	A.3.3.2.2
5.3　物理的及び環境的セキュリティ	4.3.3.3　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　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	A.3.3.3.2.2
5.3.2　物理的セキュリティ境界の確立	4.3.3.3.2　物理的セキュリティ境界の確立	A.3.3.3.2.3
5.3.3　入退管理の実施	4.3.3.3.3　入退管理の実施	A.3.3.3.2.4
5.3.4　環境的損傷からの資産の保護	4.3.3.3.4　環境的損傷からの資産の保護	A.3.3.3.2.5
5.3.5　セキュリティ手順に従うことの従業員への要求	4.3.3.3.5　セキュリティ手順に従うことの従業員への要求	A.3.3.3.2.6
5.3.6　接続の保護	4.3.3.3.6　接続の保護	A.3.3.3.2.8
5.3.7　機器資産の保守	4.3.3.3.7　機器資産の保守	A.3.3.3.2.9
5.3.8　監視及び警報の手順の確立	4.3.3.3.8　監視及び警報の手順の確立	A.3.3.3.2.10
5.3.9　資産を追加、除去及び廃棄する手順の確立	4.3.3.3.9　資産を追加、除去及び廃棄する手順の確立	A.3.3.3.2.11
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　重要資産の暫定的保護のための手順の確立	A.3.3.3.2.14
5.4　ネットワークの分割	4.3.3.4　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	4.3.3.4.1　ネットワーク分割アーキテクチャの策定	A.3.3.4.2
5.4.2　高リスクIACSの隔離又は分割の採用	4.3.3.4.2　高リスクIACSの隔離又は分割の採用	A.3.3.4.2
5.4.3　障壁装置による不要な通信のブロック	4.3.3.4.3　障壁装置による不要な通信のブロック	A.3.3.4.2
5.5　アクセス制御－アカウント管理	4.3.3.5　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	4.3.3.5.1　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	A.3.3.5.3.2
5.5.2　個人の識別	4.3.3.5.2　個人の識別	A.3.3.5.3.7
5.5.3　アカウントアクセスの認可	4.3.3.5.3　アカウントアクセスの認可	A.3.3.5.3.8
5.5.4　アクセスアカウントの記録	4.3.3.5.4　アクセスアカウントの記録	A.3.3.5.3.11
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　不要なアカウントの一時停止又は削除	A.3.3.5.3.9
5.5.6　アカウントの許可のレビュー	4.3.3.5.6　アカウントの許可のレビュー	A.3.3.5.3.10
5.5.7　デフォルトパスワードの変更	4.3.3.5.7　デフォルトパスワードの変更	A.3.3.5.3.13
5.5.8　アカウント管理の監査	4.3.3.5.8　アカウント管理の監査	A.3.3.5.3.14
5.6　アクセス制御－認証	4.3.3.6　アクセス制御－認証	
5.6.1　認証方針の策定	4.3.3.6.1　認証方針の策定	A.3.3.6.5.1(a)
5.6.2　システムの使用前のすべてのユーザの認証	4.3.3.6.2　システムの使用前のすべてのユーザの認証	A.3.3.6.5.1(b)
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　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	A.3.3.6.5.1(c)
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	4.3.3.6.4　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	A.3.3.6.5.3(b)
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　適切なレベルでのすべてのリモートユーザの認証	A.3.3.6.5.3(a)

CSMS認証基準(Ver.2.0)	IEC 62443-2-1	
	本文	附属書A
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　リモートログイン及びリモート接続のポリシーの策定	A.3.3.6.5.3、A.3.3.6.5.4
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　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	A.3.3.6.5.3(c)
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　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	A.3.3.6.5.3(d)
5.6.9　タスク間通信での認証の採用	4.3.3.6.9　タスク間通信での認証の採用	A.3.3.6.5.4
5.7　アクセス制御－認可	4.3.3.7　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	4.3.3.7.1　認可セキュリティポリシーの定義	A.3.3.7.1.1(a)
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	A.3.3.7.1.1(b)
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　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	A.3.3.7.1.1(c)
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IACSに対する複数の認可方法の採用	A.3.3.7.1.3
5.8　システムの開発及び保守	4.3.4.3　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	4.3.4.3.1　セキュリティ機能及び能力の定義及びテスト	A.3.4.3.5
5.8.2　変更管理システムの開発及び導入	4.3.4.3.2　変更管理システムの開発及び導入	A.3.4.3.6
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	4.3.4.3.3　IACSを変更することのすべてのリスクアセスメント	A.3.4.3.6
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　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	A.3.4.3.3、A.3.4.3.6
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	4.3.4.3.6　ポリシー及び手順のレビュー及び維持管理	A.3.4.3.6
5.8.7　パッチマネジメント手順の確立及び文書化	4.3.4.3.7　パッチマネジメント手順の確立及び文書化	A.3.4.3.7
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	4.3.4.3.8　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	4.3.4.3.9　バックアップ及び復元の手順の確立	A.3.4.3.8
5.9　情報及び文書のマネジメント	4.3.4.4　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	4.3.4.4.2　情報分類レベルの定義	A.3.4.4.2
5.9.2　すべてのCSMS情報資産の分類	4.3.4.4.3　すべてのCSMS情報資産の分類	A.3.4.4.2
5.9.3　適切な記録管理の保証	4.3.4.4.4　適切な記録管理の保証	A.3.4.4.2
5.9.4　長期記録の取得の保証	4.3.4.4.5　長期記録の取得の保証	A.3.4.4.2
5.9.5　情報の分類の維持管理	4.3.4.4.6　情報の分類の維持管理	A.3.4.4.2
5.10　インシデントの計画及び対応	4.3.4.5　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	4.3.4.5.1　インシデント対応計画の導入	A.3.4.5.2

CSMS認証基準（Ver.2.0）	IEC 62443-2-1	
	本文	附属書A
5.10.2　インシデント対応計画の伝達	4.3.4.5.2　インシデント対応計画の伝達	A.3.4.5.2
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	4.3.4.5.3　通常と異なる活動及び事象に関する報告手順の確立	A.3.4.5.2
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	4.3.4.5.4　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	4.3.4.5.5　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	4.3.4.5.6　インシデントの識別及び対応	A.3.4.5.3
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	4.3.4.5.7　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	A.3.4.5.3
5.10.8　インシデントの詳細の文書化	4.3.4.5.8　インシデントの詳細の文書化	A.3.4.5.3
5.10.9　インシデントの詳細の伝達	4.3.4.5.9　インシデントの詳細の伝達	A.3.4.5.3
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する対処及び修正	A.3.4.5.4
5.10.11　演習の実行	4.3.4.5.11　演習の実行	A.3.4.5.2