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認証機関認定基準及び指針

JIP-CSAC100-1.0

2014 年 7 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	2013.7.30	パイロット認証用として 0.8 版制定	
0.8a	2014.3.13	パイロット認証を経て次の項目を改訂 ・IEC 62443-2-1 の表記を CSMS 認証基準で統一・目次に附属書 A,B,C を追加 ・9.2.3.3 CSMS 審査固有の要素に「ぜい弱性の分析」追加 ・附属書 A（参考）に A.3 を追加 ・附属書 B（参考）を新規作成 ・附属書 C（参考）を新規作成	
1.0	2014.7.2	正式運用開始として 1.0 版に改訂 ・CSMS 認証基準(IEC 62443-2-1)Ver.1.0 が発行されたことによる参照箇条の見直し。 ・9.1.3 “附属書 C に，審査工数を決定する際に参考となる追加の事項を示す。”を追記 ・9.2.3.1 “セキュリティポリシー及び／又は事業上の根拠”の“又は”を削除	

目　　次

まえがき

この基準及び指針は，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）認証業務を行っている第三者機関（以下，認証機関という）が，その業務遂行に関して適格であり信頼できると承認されるために遵守すべき一般要求事項及び指針を定めている。

備考1：この基準及び指針では，IEC 62443-2-1:2010 英和対訳版（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，この基準及び指針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。

2：この基準及び指針で参照している規格で西暦年の付記がないものは，最新版（追補を含む）を意味している。

序文

組織のマネジメントシステムを審査及び認証する機関に対する基準を規定する日本工業規格として，JIS Q 17021 がある。このような審査及び認証する機関を，CSMS認証基準（IEC 62443-2-1）との適合性に関するCSMSの審査及び認証を目的として，JIS Q 17021 に適合しているとして認定するためには，JIS Q 17021 に対して追加の要求事項及び手引が必要である。この基準及び指針は，このような追加の要求事項及び手引を提供する。

この基準及び指針は，JIS Q 17021 の構成に沿っている。また，JIS Q 17021 をCSMS 認証に適用するためのCSMS固有の追加の要求事項及び手引は，“CS”という表記によって識別されている。

この基準及び指針において，“～なければならない”という表現は，JIS Q 17021 及びCSMS認証基準 （IEC 62443-2-1）の要求事項を反映する必須要件の規定を示すために用いられている。“～ことが望ましい”という表現は，推奨事項を示すために用いられている。

この基準及び指針の目的の一つは，認定機関が認証機関を評価しようとする場合に用いる規格の適用を，より有効に整合できるようにすることである。

注記　この基準及び指針において，“マネジメントシステム”及び“システム”という用語は，区別なく用いられている。マネジメントシステムの定義は，JIS Q 9000:2006 に規定されている。この規格で用いられているマネジメントシステムを，他の種類のシステム，例えば，IT システムと混同すべきではない。

1　適用範囲

この基準及び指針は，JIS Q 17021:2011 及びCSMS認証基準（IEC 62443-2-1）（以下、CSMS認証基準という。）に規定する要求事項に加えて，CSMS の審査及び認証を行う機関に対する要求事項を規定し，かつ，手引を提供する。この基準及び指針は，CSMS 認証を行う認証機関の認定を支援することを主として意図している。

この基準及び指針に含まれる要求事項は，CSMS 認証を行う機関によって，その力量及び信頼性の観点から実証される必要があり，また，この基準及び指針に含まれる手引は，CSMS 認証を行う機関に対し，要求事項に関する追加の解釈を提供する。

注記　この基準及び指針は，認定，同等性評価又は他の審査プロセスに対する基準文書として使用できる。

2　引用規格

次に掲げる規格は，この基準及び指針に引用されることによって，この基準及び指針の規定の一部を構成する。これらの引用規格のうちで，西暦年を付記してあるものは，記載の年の版を適用し，その後の改正版（追補を含む。）は適用しない。西暦年の付記がない引用規格は，その最新版（追補を含む。）を適用する。

JIS Q 17021 適合性評価－マネジメントシステムの審査及び認証を行う機関に対する要求事項

IEC 62443-2-1 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ー
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

JIS Q 19011 マネジメントシステム監査のための指針

3　用語及び定義

この基準及び指針で用いる主な用語及び定義は，JIS Q 17021 及びCSMS認証基準 によるほか，次による。

3.1

登録証（certificate）

認証機関が認定の条件に従って発行する，認定シンボル又は認定の表明が記載されている登録証。

3.2

認証機関（certification body）

公表されているCSMS 規格及び依頼組織のCSMS の下で要求される他の補足文書に対して，そのCSMS を審査し，かつ，認証する第三者機関。

3.3

認証文書（certification document）

依頼組織のCSMS が，特定したCSMS 規格及び依頼組織のCSMS の下で要求される他の補足文書に適合していることを示す文書。

3.4

マーク（mark）

法的に登録された商標，又はその他の方法によって保護されたシンボルで，認定機関又は認証機関の規則に基づいて発行されるもの。このマークは，組織の運用するマネジメントシステムに対する十分な信頼が実証されていること，又は関連する製品若しくは個人が特定の規格の要求事項を満たしていることを示す。

3.5

組織（organization）

法人化されているか否か，公営か民営かにかかわらず，会社，法人，事業所，企業，当局，団体若しくはそれらの一部又は組合せで，自らを律する機能と管理とが存在し，サイバーセキュリティを働かせることを確実にできるもの。

4　原則

原則は，JIS Q 17021 の箇条4 による。

5　一般要求事項

5.1　法的及び契約上の事項

法的及び契約上の事項は，JIS Q 17021 の5.1 による。

5.2　公平性のマネジメント

公平性のマネジメントは，JIS Q 17021 の5.2 によるほか，次のCSMS 固有の要求事項及び手引による。

5.2.1 CS 5.2 利害抵触

認証機関は，コンサルティングとみなされずに，かつ，利害抵触の可能性があるとされずに，次の業務を遂行できる。

a) 認証業務。これには，情報連絡会議，計画の打合せ，文書の調査，審査（CSMS 内部監査又は内部のCSMSの評価ではない。），又は不適合のフォローアップを含む。
b) 研修コースの手配及び講師としての参加。ただし，このコースがサイバーセキュリティマネジメント，関連するマネジメントシステム又は審査に関連する場合は，認証機関は，誰でも自由に入手できる一般的な情報及び助言の提供にとどめなければならない。つまり，c)の要求事項に違反するような，企業固有の助言を提供してはならない。
c) 認証審査規格の要求事項についての認証機関の解釈を記載した情報の，要請に応じた提供又は公開(9.1.1.1参照)
d) 認証審査を受ける準備が整っているかの決定のためだけを目的とする審査前の活動。ただし，そのような活動が，5.2.1 の違反になるような勧告又は助言をしてはならない。また，認証機関は，審査前活動が5.2.1 の要求事項に違反しないこと，及び結果的に認証審査期間の短縮根拠として利用されないことを確認できなければならない。
e) 認定範囲以外の規格又は規制に従った，第二者審査及び第三者審査の実行
f) 認証審査及びサーベイランスにおける価値の付加。例えば，特定の解決策の提示を含まない，審査中に明らかになった改善の機会の明示。

認証機関は，認証の対象となる依頼組織のCSMS のCSMS 内部監査を提供する機関（個人を含む。）から独立していなければならない。

5.3 債務及び財務

債務及び財務は，JIS Q 17021 の5.3 による。

6 組織運営機構に関する要求事項

6.1 組織構造及びトップマネジメント

組織構造及びトップマネジメントは，JIS Q 17021 の6.1 による。

6.2 公平性委員会

公平性委員会は，JIS Q 17021 の6.2 による。

7 資源に関する要求事項

7.1 経営層及び要員の力量

経営層及び要員の力量は，JIS Q 17021 の7.1 によるほか，次のCSMS 固有の要求事項及び手引による。

7.1.1 CS 7.1.1 一般考慮事項

CSMS 認証を遂行するために要求される力量における必須の要素は，審査対象の活動及び関連するサイバーセキュリティの課題に対して，個々の要員の技能及びそれら要員の全体としての力量が適切となるように要員を選定し，供給し，かつ，管理することである。

7.1.1.1 力量分析及び契約のレビュー

認証機関は，審査する依頼組織のCSMS に関連する技術及び法律の動向に関する知識をもっていることを確実にしなければならない。

認証機関は，業務を行う全ての専門分野において，サイバーセキュリティマネジメントに関して認証機関が利用可能とすることが必要な力量を分析する有効なシステムをもたなければならない。

各依頼組織について，認証機関は，契約をレビューする前に，各産業分野の要求事項についての力量分析（評価されたニーズに応じた技能のアセスメント）を完了していることを，実証できなければならない。認証機関は，次に，この力量分析の結果に基づいて，依頼組織との契約をレビューしなければならない。認証機関は，特に，次の活動を遂行する力量をもっていることを実証できなければならない。

a) 依頼組織の活動分野及び関連する事業リスクを理解する。
b) その組織の特定された活動，並びにサイバーセキュリティに関する，IACS資産に対する脅威，ぜい弱性及び

依頼組織に及ぼす影響に関連して，認証を行うために認証機関に必要とされる力量を特定する。
c) 必要な力量を利用できることを確認する。
注記 NACEコードのように詳細な産業分野による力量分析を、必ずしも求めない。

7.1.1.2 資源

認証機関の経営層は，審査員が活動する認証の範囲で要求される審査員の業務を遂行する力量を個々の審査員がもっているか否かを判断するために必要なプロセス及び資源をもたなければならない。認証機関は，審査員の力量を，検証された経歴，及び特定の教育・訓練又は要点説明（ブリーフィング）によって立証してもよい。認証機関は，サービスを提供する全ての依頼者と情報交換を有効にできなければならない。

7.1.2 CS 7.1.2 力量の判断基準の決定

JIS Q 17021 の力量の判断基準を支援する知識及び技能に関する追加の情報を，附属書Bに示す。

7.2 認証活動に関与する要員

認証活動に関与する要員は，JIS Q 17021 の7.2 によるほか，次のCSMS 固有の要求事項及び手引による。

7.2.1 CS 7.2 認証機関の要員の力量

認証機関は，次の事項に対する力量をもつ要員をもたなければならない。
a) 審査に適切な審査チームとなるようCSMS 審査員を選定し，その力量を検証する。
b) CSMS 審査員に要点説明を行い，必要な教育・訓練を手配する。
c) 認証の授与，維持，取消し，一時停止，拡大，又は縮小を決定する。
d) 苦情及び異議申立てのプロセスを定め，それを運用する。

7.2.1.1 審査チームの教育・訓練

認証機関は，次の事項を確実にするために，審査チームの教育・訓練に関する基準をもたなければならない。
a) CSMS 規格及び他の関連する規準文書の知識
b) サイバーセキュリティについての理解
c) 事業上の観点からのリスクアセスメント及びリスクマネジメントについての理解
d) 審査対象となる活動についての専門的知識
e) CSMS に関連した規制要求事項についての一般知識
f) マネジメントシステムについての知識
g) JIS Q 19011 に基づく監査の原則についての理解
h) CSMS の有効性のレビューについての知識

このような教育・訓練の要求事項は，審査チームのメンバー間で分担できるd)を除き，審査チームの全てのメンバーに適用する。
7.2.1.1.1 ある特定の認証審査を担当させる審査チームを選定する場合，認証機関は，その審査チームの技能が担当する審査に対して適切であることを確実にしなければならない。審査チームは，次の事項を満たさなければならない。
a) 認証が求められているCSMS の範囲内の特定の活動に関する適切な専門的知識をもち，かつ，該当する場合は，それらの特定の活動に関連する手順及びそれら特定の活動の潜在的なサイバーセキュリティリスクについての適切な専門的知識をもつ（審査員でない技術専門家がこの役割を果たしてもよい。）。
b) 依頼組織の活動，製品又はサービスのサイバーセキュリティ面の管理に関して，信頼できるCSMS 認証審査を行うのに十分な程度，依頼組織について理解している。
c) 依頼組織のCSMS に適用される規制要求事項を適切に理解している。
7.2.1.1.2 必要な場合，審査チームは，審査に関係する専門分野において特定の力量を，実証できる技術専門家によって補強されてもよい。その場合，技術専門家はCSMS 審査員の代わりとしての役割を果たすことができないが，審査対象のマネジメントシステムに照らして，技術的な適切性に関する事項について審査員に助言できることに留意することが望ましい。認証機関は，次を行うための手順をもたなければならない。
a) 力量，教育・訓練，資格及び経験に基づいて，審査員及び技術専門家を選定する。
b) 初めに審査員及び技術専門家の認証審査中の行動を評価し，その後も審査員及び技術専門家のパフォーマンスを監視する。

7.2.1.2 認証に関する決定プロセスの管理

管理機能を担う者は，CSMS認証基準 の要求事項に対するCSMS 認証の授与，維持，拡大，縮小，一時停止，及び取消しに関する決定プロセスを管理する，専門的な力量及び能力をもたなければならない。

7.2.1.3 CSMS 審査を行う審査員の教育，業務経験，審査員研修及び審査経験に関する前提条件のレベル

附属書Aを参照して，認証機関はCSMS 審査チームの各審査員が満たすべき基準を定めなければならない。

7.3 個々の外部審査員及び外部技術専門家の起用

個々の外部審査員及び外部技術専門家の起用は，JIS Q 17021 の7.3 によるほか，次のCSMS 固有の要求事項及び手引による。

7.3.1 CS 7.3 外部審査員及び外部技術専門家の審査チーム構成員への起用

審査チームの構成員として外部審査員及び外部技術専門家を活用する場合，認証機関は，当該審査員又は技術専門家が力量をもち，この規格の該当規定を順守していることを確実にしなければならない。また，認証機関は，CSMS 又は関連するマネジメントシステムの設計，導入又は維持に，直接的であれ又は雇用主を介してであれ，当該審査員又は技術専門家が公平性を損なうような形で関与していないことを確実にしなければならない。

7.3.1.1 技術専門家の起用

プロセス及びサイバーセキュリティの課題，並びに依頼組織に影響する法令に関して，特定の知識をもっているが，7.2 の基準を完全には満たしていない技術専門家を審査チームに加えてもよい。技術専門家は審査員の監督の下で業務を行わなければならない。

7.4 要員の記録

要員の記録は，JIS Q 17021 の7.4 による。

7.5 外部委託

外部委託は，JIS Q 17021 の7.5 による。

8 情報に関する要求事項

8.1 一般にアクセス可能な情報

一般にアクセス可能な情報は，JIS Q 17021 の8.1 によるほか，次のCSMS 固有の要求事項及び手引による。

8.1.1 CS 8.1 認証の授与，維持，拡大，縮小，一時停止及び取消しに関する手順

認証機関は，依頼組織に対して，CSMS認証基準 及び認証に必要な他の文書に適合する，文書化され，かつ，導入されたCSMS をもつよう要求しなければならない。

認証機関は，次の事項についての文書化された手順をもたなければならない。

a) JIS Q 17021 及びその他の関連文書に従って行う，依頼組織のCSMS の初回認証審査。
b) JIS Q 17021 に従って定期的に実施する依頼組織のCSMS のサーベイランス及び再認証審査。このサーベイランス及び再認証審査は，依頼組織のCSMS が該当する要求事項に継続的に適合していること，及び依頼組織が全ての不適合を是正するために適時に是正処置をとっていることを検証し，かつ，記録するために行う。

8.2 認証文書

認証文書は，JIS Q 17021 の8.2 によるほか，次のCSMS 固有の要求事項及び手引による。

8.2.1 CS 8.2 CSMS 認証文書

認証機関は，CSMS を認証した各依頼組織に対し，権限を与えられた者が署名した，書簡又は登録証のような認証文書を交付しなければならない。これらの認証文書は，依頼組織及び認証の対象となるシステムのために，授与された認証の範囲と，CSMS を認証するに当たって基準としたCSMS 規格であるCSMS認証基準とを明記しなければならない。また、登録証には，適用宣言書の特定の版の引用を含めなければならない。

注記 適用宣言書への変更で，認証範囲における管理策の適用（coverage）を変更しないものは，登録証の更新は、必ずしも求められない。

8.3 被認証組織の登録簿

被認証組織の登録簿は，JIS Q 17021 の8.3 による。

8.4 認証の引用及びマークの使用

認証の引用及びマークの使用は，JIS Q 17021 の8.4 によるほか，次のCSMS 固有の要求事項及び手引による。

8.4.1 CS 8.4 認証マークの管理

認証機関は，CSMS 認証マークの所有権，使用及び表示を適切に管理しなければならない。認証機関がCSMS が認証されていることを示すためにマークを使用する権利を与えたときには，認証機関は，依頼組織が指定されたマークを，認証機関が書面で承諾した方式でだけ使用することを確実にしなければならない。認証機関は，認証マークを，製品に付けること，又は製品の適合性を示すと解釈されるような方法で使用する権利を依頼組織に与えてはならない。

8.5 機密保持

機密保持は，JIS Q 17021 の8.5 によるほか，次のCSMS 固有の要求事項及び手引による。

8.5.1 CS 8.5 組織の記録へのアクセス

認証機関は，認証審査の前に，機密情報又は取扱いに慎重を要する情報を含んでいるために，審査チームによるレビューに利用できないCSMS の記録がある場合は，報告するよう依頼組織に求めなければならない。認証機関は，これらの記録がなくてもCSMS が適切に審査できるかを判断しなければならない。認証機関は，これらの特定された機密又は取扱いに慎重を要する記録のレビューなしではCSMS の審査を適切に行えないという結論に達した場合には，適切なアクセスの手配を依頼組織が行うまで，認証審査を開始できないことを依頼組織に通知しなければならない。

8.6 認証機関とその依頼者との間の情報交換

認証機関とその依頼者との間の情報交換は，JIS Q 17021 の8.6 による。

9 プロセス要求事項

9.1 一般要求事項

一般要求事項は，JIS Q 17021 の9.1 によるほか，次のCSMS 固有の要求事項及び手引による。

9.1.1 CS 9.1.1 CSMS 審査に対する一般要求事項

9.1.1.1 認証審査基準

依頼者のCSMS を審査するための基準は，CSMS認証基準 及び依頼者が遂行する機能に関連する認証に必要なその他の文書に示されているものでなければならない。特定の認証プログラムにこれらの文書を適用することについての説明が求められる場合に，提供する内容は，所要の専門能力をもつ適切で公平な委員会又は個人が作成し認証機関が公表しなければならない。

9.1.1.2 方針及び手順

認証機関の文書には，認証プロセスの実施に関する方針及び手順を含めなければならない。これには，CSMS の認証に用いる文書の利用及び適用の点検と，依頼組織のCSMS の審査及び認証の手順の点検とを含む。

9.1.1.3 審査チーム

認証機関は，審査チームを正式に任命し，そのチームに適切な作業文書を与えなければならない。審査計画及び審査日は，依頼組織と合意しなければならない。審査チームに与える業務を明確に定め，依頼組織にも通知しなければならない。この業務命令は，依頼組織の組織運営機構，方針及び手順を調査し，かつ，これらが認証範囲に関する全ての要求事項を満足していることを確認し，さらにこれらの手順が実施され，依頼組織のCSMS に対して信頼を与えるものであることを確認するよう，審査チームに要求しなければならない。

9.1.2 CS 9.1.2 認証範囲

審査チームは，定義された範囲に含まれる依頼組織のCSMS を，全ての適用される認証要求事項を基準として審査しなければならない。認証機関は，依頼組織のCSMS の適用範囲及び境界が，事業・組織・所在地・IACS資産・技術の特徴の見地から，明確に定義されていることを確実にしなければならない。認証機関は，依頼組織が自らのCSMS の適用範囲の中でCSMS認証基準に規定する要求事項を取り扱っていることを確認しなければならない。

認証機関は，CSMS認証基準 の規定するように，依頼組織のサイバーセキュリティのリスクアセスメント及びリスク対応が当該組織の活動を適切に反映しており，その活動の境界まで及んでいることを確実にしなければなら

ない。また，認証機関は，依頼組織のCSMS の適用範囲及び適用宣言書の中にこのことが反映されていることを確認しなければならない。

認証機関は，依頼組織が，CSMS の適用範囲に完全には含まれないサービス又は活動とのインタフェースを，認証の対象となるCSMS の中で取り扱っていること，及び自らのサイバーセキュリティのリスクアセスメントに含めていることを確実にしなければならない。このような状況の一例には，他の組織と施設を共有するケースがある（例えばITシステム，データベース，通信システム）。

9.1.3 CS 9.1.3 審査工数

認証機関は，初回審査，サーベイランス審査又は再認証審査に関連する全ての活動を行うのに十分な時間を審査員に与えなければならない。割り当てられる時間は，次の要素を考慮しなければならない。

a) CSMS 適用範囲の規模
b) CSMS の複雑さ
c) CSMS の適用範囲内で行われる事業の種類
d) そのCSMS の様々な構成要素を導入する場合に使用される，技術の範囲及び多様性
e) 事業所の数
f) 以前に実証されたCSMS のパフォーマンス
g) CSMS の適用範囲内で用いられる外部委託及び第三者との取り決めの範囲
h) 認証に適用される規格及び規制

認証機関は，初回審査，サーベイランス審査及び再認証審査に使用する工数の根拠を具体的に示すことができるように，又はその正当性を示すことができるように準備しておかなければならない。附属書Cに，審査工数を決定する際に参考となる追加の事項を示す。

9.1.4 CS 9.1.4 複数サイト（Multiple sites）

9.1.4.1 CSMS 認証における複数サイトのサンプリングに関する決定は，品質マネジメントシステムにおける同様の決定より更に複雑である。依頼組織が次のa)～c)の基準を満たす複数の事業所（sites）をもっている場合，認証機関は，複数サイトの認証審査に対してサンプルに基づいた手法の利用を検討してもよい。

a) 全ての事業所が同一のCSMS の下で運営されている。このCSMS は，中央で管理・監査されており，かつ，中央でマネジメントレビューが行われる。
b) 全ての事業所が，依頼組織のCSMS 内部監査プログラムに含まれている。
c) 全ての事業所が，依頼組織のCSMS マネジメントレビュープログラムに含まれている。

9.1.4.2 サンプルに基づいた手法の適用を希望する認証機関は，次の事項を確実にするための手順を備えなければならない。

a) 最初に行う契約のレビューによって，サンプリングの適切なレベルが決定されるように，事業所間の違いを可能な限り特定する。
b) 認証機関が，次の要求事項を考慮して，代表し得る数の事業所をサンプリングしたものである。
   1) 本部及びその事業所の内部監査の結果
   2) マネジメントレビューの結果
   3) 各事業所の規模の違い
   4) 各事業所の事業目的の違い
   5) そのCSMS の複雑さ
   6) 各種事業所のIACS の複雑さ
   7) 作業慣行の違い
   8) 行っている活動の違い
   9) 重要なIACS，又は取扱いに慎重を要する情報を処理するIACS との潜在的相互作用
   10) 法的要求事項の違うもの全て
c) 依頼組織のCSMS の適用範囲内における全ての事業所から，代表サンプルを選択する。この選択は，無作為的要素だけでなく，b)の要因を反映する判断に基づく選択によらなければならない。
d) 認証に先立って，そのCSMS に含まれる，重大なリスクの対象となる全ての事業所を審査する。
e) 審査プログラムが，上記の要求事項に照らして作成されており，また，3年以内にCSMS の認証の範囲内の代表サンプルを，網羅するようになっている。
f) 本部又はある一つの事業所で不適合が観察された場合は，その是正処置の手順をその登録証に含まれる本部及び全ての事業所に適用する。

CS 9.1.5 に規定する審査は，一つのCSMS が全ての事業所に適用されること，及びそれが中央の管理を運用レベルに行き渡らせることを確実にするために，依頼組織の本部の活動を取り扱わなければならない。この審査では，上記の事項を全て取り扱わなければならない。

9.1.5 CS 9.1.5 審査方法

認証機関は，依頼組織に次の事項を実証するように要求する手順をもたなければならない。次の事項とは，CSMS内部監査を計画していること，並びにそのプログラム及び手順を運用可能であり，それが運用可能となっていることを示せることである。

認証機関の手順は，CSMS を導入する特定の方法，又は文書及び記録の特定の様式を前提としてはならない。認証の手順は，依頼組織のCSMS がCSMS認証基準 の要求事項並びに依頼組織のポリシー及び目的を満たしていることの確立に焦点を当てなければならない。

審査計画は，適切に，その審査で利用されるネットワーク支援の審査手法を特定しなければならない。

注記　ネットワーク支援の審査手法には，例えば，電話・テレビ会議，ウェブ会議，双方向インターネットによる情報伝達，及びCSMS 文書及び／又はCSMS プロセスへの電子的な遠隔アクセスを含めてもよい。このような手法の狙いは，審査の有効性及び効率性を高めること，並びに審査プロセスの完全性を支えるものであることが望ましい。

9.1.6 CS 9.1.6 認証審査報告書

9.1.6.1　認証機関の報告の手順は，次の事項を確実にしなければならない。

a) 依頼組織の審査現場を離れる前に審査チームと依頼組織の経営層との間で会議をもつ。その会議では，審査チームは，依頼組織に次の事項を提供する。
   1) 特定の認証要求事項に対する依頼組織のCSMS の適合性に関する書面又は口頭による指摘
   2) 所見及びその根拠について依頼組織が質問する機会
b) 審査チームは，全ての認証要求事項に対する依頼組織のCSMS の適合性に関する所見の審査報告書を認証機関に提出する。

9.1.6.2　この審査報告書は，次の情報又は次の情報への参照を提供しなければならない。

a) 文書レビューの要約を含む審査の詳細
b) 依頼組織のサイバーセキュリティリスク分析に関する認証審査の詳細
c) 審査工数の実績合計，並びに文書レビュー，リスク分析の評価，現地審査，及び審査報告書の作成に要した時間の内訳
d) 審査で使用した調査項目，それらを選択した根拠及び採用した方法

9.1.6.3　審査報告書は，十分に詳細で，認証の決定を裏付けし，かつ，それを支えなければならない。また，この報告書は，次の事項を含まなければならない。

a) 審査で対象とした範囲（例えば，認証要求事項及び審査対象とした事業所）。これには，重要な審査証跡及び利用した審査方法を含める（CS 9.1.5 参照）。
b) 観察された事項，肯定的（例えば，特筆すべき特性）及び否定的（例えば，潜在的な不適合）なもの。
c) 特定された全ての不適合の詳細で，これらが不適合とされる客観的証拠，及びこれらを不適合とするCSMS認証基準 の要求事項又は認証のために要求される他の文書類の要求事項の引用によって裏付けられたもの。
d) 依頼組織のCSMS の認証要求事項に対する適合性に関する見解。これには，不適合についての明確な表明，適用宣言書の版の引用，及び該当する場合には，依頼組織の以前の認証審査の結果との有用な比較を含める。

回答が記入された質問状，チェックリスト，観察記録，ログ，又は審査員のノートは，審査報告書を構成する一部となる場合もある。これらの方法を使用する場合，認証の決定に裏付けを与える証拠として，これらの文書を認証機関に提出しなければならない。審査中に評価したサンプルに関する情報を，この審査報告書又は他の認証文書に含めなければならない。

この報告書では，依頼組織がそのCSMS に信頼を与えるために採用している内部の組織体制及び手順の適切性を考慮しなければならない。

報告に関する要求事項は，JIS Q 17021 の9.1.10 による。さらに，この報告書には，次の事項を含めなければならない。

- CSMS 内部監査及びマネジメントレビューに対する信頼度
- CSMS の導入及び有効性に関する，否定的並びに肯定的な最も重要な観察された事項の要約
- 依頼組織のCSMS を認証することが望ましいか否かについての審査チームの推薦。これには，この推薦を立証する情報を含める。

9.2 初回審査及び認証

初回審査及び認証は，JIS Q 17021 の9.2 によるほか，次のCSMS 固有の要求事項及び手引による。

9.2.1 CS 9.2.1 審査チームの力量

審査チームの力量は，7.2 によるほか，次の認証審査に関する要求事項による。サーベイランス活動については，計画されたサーベイランス活動に関する要求事項だけとする。

次の要求事項は，審査チーム全体に適用する。

a) 次のそれぞれについて，審査チームは認証機関の基準を満たしていなければならない。
   1) 審査チームの管理
   2) CSMS に適用可能な，マネジメントシステム及びプロセス
   3) 該当する特定のサイバーセキュリティ分野における法令及び規制の要求事項に関する知識
   4) サイバーセキュリティに関連するインシデントの傾向の特定
   5) 依頼組織のぜい弱性の特定，これらのぜい弱性が悪用される可能性の理解，及びその影響の理解，それらに対する軽減策及び管理策についての理解
   6) CSMS管理策及びその導入についての理解
   7) CSMSの監視・評価についての知識
   8) 関連及び／又は関係するCSMS 規格，産業界における最適な慣行
   9) インシデント取扱い方法及び事業継続についての知識
   10) 有形・無形のIACS 資産及び影響分析についての知識
   11) セキュリティに関連するか，又はセキュリティが課題となっている最新技術の知識
   12) リスクマネジメントのプロセス及び方法についての知識
b) 審査チームは，依頼組織のCSMS におけるセキュリティインシデントを示すものから適切なCSMS の要素まで遡ることのできる力量をもっていなければならない。
c) 審査チームは，上記項目の適切な業務経験をもち，かつ，それらを具体的に適用したことがなければならない（これは，一人の審査員がサイバーセキュリティの全領域の経験を全てもつ必要があることを意味するものではなく，審査チーム全体として，審査対象のCSMS 適用範囲を網羅するのに十分な認識及び経験をもっていなければならない。）。

審査チームは1 名で構成してもよいが，その人は，a)の基準を全て満たしていなければならない。

9.2.1.1 CS 9.2.1.1 審査員の力量の実証

審査員は，9.2.1 のa)～c)に示したような，自らの知識及び経験を，例えば，次の事項によって実証できなければならない。

a) CSMS 固有の認知された資格
b) 審査員としての登録
c) 承認CSMS 研修コース
d) 専門能力の継続的開発についての最新の記録
e) 実際の依頼組織システムのCSMS 審査プロセスを遂行する審査員について，立会いによる実証

9.2.2 CS 9.2.2 初回審査のための一般準備

認証機関は，認証審査の実施に必要な手配を全て行うことを依頼組織に要求しなければならない。この手配には，認証機関が行う認証審査，再認証審査及び苦情解決を目的とした，文書の調査，並びに全ての領域，記録（内部監査報告書及びサイバーセキュリティに関する独立したレビューの報告書を含む。）及び要員へのアクセスのための用意を含む。

依頼者は，現地での認証審査前に少なくとも次の情報を提供しなければならない。

a) CSMS 及びその対象となる活動に関わる一般情報
b) CSMS認証基準で要求されるCSMS 文書の写し及び必要な場合，関連文書の写し

9.2.3 CS 9.2.3 初回認証審査

9.2.3.1 CS 9.2.3.1 第一段階審査

審査のこの段階で，認証機関は，CSMS認証基準で要求されている文書を含む，依頼組織のCSMSの設計に関する文書を入手しなければならない。

第一段階審査の目的は，依頼組織のCSMSのセキュリティポリシー及び事業上の根拠に照らしてそのCSMS を理解すること，及び，特に，依頼組織の審査に対する準備状況を理解することによって，第二段階審査を計画する上での焦点を明確にすることである。

第一段階審査は，文書レビューを含まなければならないが，これに限定しないことが望ましい。認証機関は，いつどこで文書レビューを行うかについて，依頼組織と合意しなければならない。全ての場合において，文書レビューは，第二段階審査を開始する前に完了させておかなければならない。

第一段階審査の結果は，報告書として文書化しなければならない。認証機関は，第二段階審査への移行を決定する前に，第二段階審査のための必要な力量を備えた審査チームメンバーを選定するために，第一段階審査の審査報告書をレビューしなければならない。

認証機関は，第二段階審査では，詳細な調査のために別種の情報及び記録が追加して必要になるかもしれない

ことを，依頼組織に知らせておかなければならない。

9.2.3.2 CS 9.2.3.2 第二段階審査

9.2.3.2.1 第二段階審査は，常に依頼組織の事業所で実施する。認証機関は，第一段階審査の審査報告書に文書化された所見に基づき，第二段階審査を行うための審査計画を立案する。第二段階審査の目的は，次のとおりである。

a) 依頼組織が自らのポリシー，目的及び手順を守っていることを確認する。
b) そのCSMS がCSMS認証基準 の全ての要求事項に適合していること，並びにCSMS が依頼組織のポリシー及び目的を達成しつつあることを確認する。

9.2.3.2.2 そのために，この審査は，依頼組織の次の事項に焦点を当てなければならない。

a) サイバーセキュリティに関するリスクのアセスメント，及びそのアセスメントが比較可能で，かつ，再現可能な結果を生み出すこと
b) CSMS認証基準に掲げられた文書化に関する要求事項
c) そのリスクアセスメント及びリスク対応のプロセスに基づいた，管理策の選択
d) そのCSMSのポリシー・目的に照らして報告及びレビューされる，CSMSの有効性のレビュー
e) CSMS 内部監査及びマネジメントレビュー
f) サイバーセキュリティポリシーに対する経営陣の責任
g) 選択・導入された管理策，適用宣言書，リスクアセスメント・リスク対応のプロセスの結果，及びサイバーセキュリティポリシー・目的の間の対応
h) プログラム，プロセス，手順，記録，内部監査，及びそのCSMSの有効性のレビュー。これらは，経営陣の決定，並びにサイバーセキュリティポリシー及び目的が，これらからたどれることを確実にするものである。

9.2.3.3 CS 9.2.3.3 CSMS 審査の固有の要素

認証機関の役割は，サイバーセキュリティに関する，IACS 資産に対する脅威，ぜい弱性，及び依頼組織に及ぼす影響を，特定，調査及び評価するための手順の確立及び維持において，依頼組織が一貫していることを確立することである。認証機関は，次の事項を実施しなければならない。

a) セキュリティに関する脅威及びぜい弱性の分析が依頼組織の運営にとって関連があり，かつ，適切であることを実証するよう依頼組織に求める。
   注記 依頼組織は，その組織のサイバーセキュリティに関連するリスクのうちどれが重大かを特定するための基準を定め，かつ，これを行うための手順を確立する責任を負う。
b) サイバーセキュリティに関する，IACS 資産に対する脅威，ぜい弱性及び影響を特定，調査及び評価するための依頼組織の手順，並びにこの手順を適用した結果が，依頼組織のポリシー及び目的と整合しているかどうかを確立する。

さらに，認証機関は，重大さの分析に用いられる手順が確かで，適切に導入されているか否かを確立しなければならない。サイバーセキュリティに関する，IACS 資産に対する脅威，ぜい弱性，又は依頼組織に及ぼす影響が，重大であると特定される場合，それらはCSMS 内で管理されていなければならない。

9.2.3.3.1 法令及び規制の順守

法規制順守の維持及び評価は，その依頼組織の責任である。この点において，認証機関は，自らの役割を，CSMSが機能していることの信頼を確立するためのチェック及びサンプリングに限らなければならない。認証機関は，依頼組織が，サイバーセキュリティのリスク及び影響に適用される法規制順守を達成するマネジメントシステムをもっていることを，検証しなければならない。

9.2.3.3.2 CSMS 文書と他のマネジメントシステム文書との統合

依頼組織は，組織のCSMS 文書と他のマネジメントシステム（例えば，品質，安全衛生，環境）文書とを組み合わせることができる。ただし，他のシステムとの適切なインタフェースを備え，そのCSMS を明確に識別できることが条件となる。

9.2.3.3.3 マネジメントシステム複合審査

認証機関は，CSMS の認証に組み合わせて他のマネジメントシステムの認証を提供してもよいし，又はCSMS の認証だけを提供してもよい。

CSMS 審査は，他のマネジメントシステムの審査と複合することができる。この複合が可能なのは，その審査がそのCSMS の認証のための要求事項を全て満たしていることを実証できる場合である。CSMSにとって重要な要素全てが審査報告書に明確に記載されており，容易に識別できるようになっていなければならない。審査を複合することによって，審査の質に悪影響が及ばないようにしなければならない。

9.2.4 CS 9.2.4 初回認証授与に関する情報

認証の決定の基礎を提供するために，認証機関は，この決定を行うのに十分な情報を提供する，明確な報告書を審査チームに要求しなければならない。

認証機関への審査チームからの報告書は，認証審査プロセスの様々な段階で必要とされる。ファイルにある情報と組み合わせて，これらの報告書は，少なくともCS 9.1.6 で要求されている情報を含まなければならない。

9.3 サーベイランス活動

サーベイランス活動は，JIS Q 17021 の9.3 によるほか，次のCSMS 固有の要求事項及び手引による。

9.3.1 CS 9.3 サーベイランス審査

9.3.1.1 サーベイランスの手順は，この規格に規定する依頼組織のCSMS の認証審査に関する手順と整合していなければならない。

サーベイランスの目的は，承認されたCSMS が引き続き実施されていることを検証し，依頼組織の運営の変更の結果として生じた，そのシステムへの変更の影響を検討し，かつ，認証要求事項の継続的な順守を確認することである。サーベイランス審査プログラムは，次の事項を含まなければならない。

a) そのシステム維持の要素，すなわちCSMS 内部監査，マネジメントレビュー，並びに予防処置及び是正処置
b) CSMS認証基準 及び認証に必要な他の文書で要求されている，外部からの情報
c) 文書化されたシステムへの変更
d) 変更された領域
e) CSMS認証基準の中の選択した要素
f) 該当するその他の選択した領域

9.3.1.2 認証機関によるサーベイランスは，少なくとも，次の事項をレビューしなければならない。

a) 依頼組織のサイバーセキュリティポリシーの目的達成の点から見たCSMS の有効性
b) 関連するサイバーセキュリティに関する法規制の順守を，定期的に評価しレビューする手順が機能していること
c) 前回審査で特定された不適合についてとられた処置

9.3.1.3 認証機関によるサーベイランスは，JIS Q 17021 でサーベイランス審査に要求されている項目を網羅しなければならない。さらに，次の事項を含まなければならない。

a) 認証機関は，サーベイランスプログラムを，IACS資産に対しる脅威，ぜい弱性及び依頼組織への影響に関連するサイバーセキュリティの課題に対して対応できるようにしなければならず，かつ，このプログラムの正当性を示せなければならない。
b) 認証機関のサーベイランスプログラムは，その認証機関が決定しなければならない。訪問の具体的日程は，被認証組織との間で合意することができる。
c) サーベイランス審査は，他のマネジメントシステムの審査と組み合わせてもよい。その場合，報告は，それぞれのマネジメントシステムに関連する側面を明確に示さなければならない。
d) 認証機関は，登録証の適切な使用を監督しなければならない。

サーベイランス審査において，認証機関は，認証機関にもち込まれた異議申立て及び苦情の記録を点検し，かつ，認証要求事項を満たす上での不適合又は不備が明らかな場合は，依頼組織が，自らのCSMS 及び手順を調査して，適切な是正処置をとったことを確認しなければならない。

サーベイランス報告書には，特に，以前に発見された不適合の解決に関する情報を含まなければならない。サーベイランスから上げる報告書は，少なくとも，全体としてa)の要求事項を含むように作成しなければならない。

9.4 再認証

再認証は，JIS Q 17021 の9.4 によるほか，次のCSMS 固有の要求事項及び手引による。

9.4.1 CS 9.4 再認証審査

再認証審査の手順は，この規格に規定する依頼組織のCSMS 認証審査に関する手順と整合していなければならない。

認証機関は，認証の維持に関する状況及び条件を規定した明確な手順をもっていなければならない。サーベイランス又は再認証の審査において，不適合のあることが見いだされた場合，この不適合は，認証機関が合意した期間内に有効に是正されなければならない。合意した期間内に是正がなされない場合は，認証機関は，認証範囲の縮小，又は登録証の一時停止若しくは取消しを行わなければならない。是正処置を実施するために認める期間は，その不適合の重大さの程度に応じ，かつ，依頼組織の製品又はサービスが特定の要求事項を満たすことを保証するに当たってのリスクに応じたものでなければならない。

9.5 特別審査

特別審査は，JIS Q 17021 の9.5 によるほか，次のCSMS 固有の要求事項及び手引による。

9.5.1 CS 9.5 特別なケース

CSMS の認証を受けた依頼組織がそのシステムに重大な変更を加える場合，又はその認証の基盤に影響を与えるような他の変化が起きる場合，特別審査を行うために必要な活動は，特別な規定によらなければならない。

9.6 認証の一時停止，取消し，又は認証範囲の縮小

認証の一時停止，取消し，又は認証範囲の縮小は，JIS Q 17021 の9.6 による。

9.7 異議申立て

異議申立ては，JIS Q 17021 の9.7 による。

9.8 苦情

苦情は，JIS Q 17021 の9.8 によるほか，次のCSMS 固有の要求事項及び手引による。

9.8.1 IS 9.8 苦情

苦情は，潜在的な不適合についての情報源である。認証機関は，被認証組織に対し，苦情を受け取った場合には，苦情の原因を確立し，必要な場合には，認証機関に報告するよう要求しなければならない。苦情の原因には，もともと不適合の原因となるような(又はその傾向のある)，被認証組織のCSMS の中にある要因が含まれている。

認証機関は，被認証組織が修正処置及び是正処置の方法を策定するために，そのような調査を行っていることを確認しなければならない。とる処置には，次の方策を含めなければならない。

a) 法律で要求されている場合は，該当する当局への通知
b) 適合への復旧
c) 再発の防止
d) セキュリティインシデント及びその影響の評価及び軽減
e) CSMS の他の構成要素との満足できる関わり方を確実にする。
f) 採用した修正及び是正の方策の有効性の評価

認証機関は，CSMS の認証を受けた依頼組織のそれぞれに対して，全ての苦情の記録，及びCSMS認証基準の要求事項に従ってとった全ての是正処置の記録を，認証機関が求めたときは利用できることを要求しなければならない。

9.9 申請者及び依頼者に関する記録

申請者及び依頼者に関する記録は，JIS Q 17021 の9.9 による。

10 認証機関に関するマネジメントシステム要求事項

10.1 マネジメントシステムに関する選択肢

マネジメントシステムに関する選択肢は，JIS Q 17021 の10.1 による。

10.2 選択肢1：JIS Q 9001 に従ったマネジメントシステムの要求事項

JIS Q 9001 に従ったマネジメントシステムの要求事項は，JIS Q 17021 の10.2 による。

10.3 選択肢2：一般マネジメントシステムの要求事項

一般マネジメントシステムの要求事項は，JIS Q 17021 の10.3 による。

附属書 A（参考）

CSMS 審査を行う審査員の教育，業務経験，審査員研修及び審査経験に関する前提条件のレベル

A.1 CSMS 審査チームの各審査員は，次の事項を満たすか，あるいは同等の知識及び経験を有していることが望ましい。

a) 中等レベルの教育[1)]を修了している。
　注[1)] 中等レベルの教育とは，初等教育の後にくる国家の教育制度の一部で，大学又は同等の教育機関への入学前に修了するものをいう。
b) 情報技術分野において分野において4 年以上の常勤による実務経験があり，このうちの2 年以上は，サイバーセキュリティに関連した役割又は職務に就いている。
c) 5 日間の研修を成功裏に修了している。この研修は，研修の範囲が，CSMS 審査及び審査のマネジメントを含む場合には適切とみなす。
d) 審査員として活動する職責を担う前に，サイバーセキュリティの全審査過程を経験している。この経験は，文書のレビュー，CSMS 導入の審査，並びに審査報告の作成を含む，最低4 回延べ20日間以上にわたる認証審査への参加によって得ていることが望ましい。
e) これらの経験は全て合理的な範囲で最近のものである。
f) 複雑な業務を広い視野から理解できる，また，より大きな依頼組織においては個々の部門の役割を理解できる。
g) サイバーセキュリティ及び審査に関する知識及び技能を，専門能力の継続的開発を通して最新の状態に維持している。

技術専門家は，a)，b)，e)及びf)の基準を満たすことが望ましい。

A.2 A.1の事項に加えて，審査チームリーダーは，次の事項を満たすことが望ましい。この事項を満たしていることを，指導及び監督の下での審査において実証することが望ましい。

a) 認証審査プロセスを管理する知識及び特質をもっている。
b) 少なくとも3 回の完全なCSMS 審査において，審査員を経験している。
c) 口頭及び書面の両方で，効果的な意思疎通の能力があることを実証している。

注記 A.1，及びA.2の事項については，JIS Q 27006:2012の7.2.1.3の事項に加えて，CSMSの知識及び技能に関する継続的専門的能力開発（CPD）により実証することもできる。

附属書 B（参考）

審査員の力量の領域例

CSMS審査員の力量の領域例は，JIS Q 27006:2012の附属書Bと次のCSMS固有の力量の例による。

CSMS に関連する代表的な知識
・認証の対象者（制御システムを利用する事業者（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））の各々の立場からの次に関する知識
－サイバーセキュリティ分野の法規制、法順守に関する知識
－サイバーセキュリティ関連の脅威、ぜい弱性、影響，それらを減少させ管理するための技術
－CSMSの詳細管理策に関する知識
－CSMSのパフォーマンス及び有効性
－関連するCSMS規格、業界のベストプラクティス、セキュリティポリシー及び手順
－インシデント対応手順及び事業継続
－セキュリティが関係する、あるいは問題となっている最近の技術動向
－有形及び無形のIACSと影響分析

例えば、「関連する CSMS 規格、業界のベストプラクティス、セキュリティポリシー及び手順」について、IACS固有の各箇条について適切に審査するには、業界知識、IEC62443シリーズ全般の知識が重要である。

例1：4,5章で表現される「ゾーン」の概念。IACSのネットワーク分割の条文が詳細管理策5.4 ネットワークの分割で記載されているが、セキュリティレベルモデルに沿ってIACSでは情報系・制御情報系・制御系を階層的にゾーン分割し、リスクアセスメントの結果から各装置を適正なゾーンに配置するといった概念を念頭に置かなければならず、これはCSMS独自のアプローチであり、これらの背景が審査側においても前提知識として求められる。

例2：パッチマネジメントの管理（5.8.7 パッチマネジメント手順の確立及び文書化）では、標題通りの説明文しか記載されていない。本来IACSは可用性が優先される為、情報系システムと同様のアプローチで、リリースされた最新のパッチを即座に適用する、といったことが実現できない課題である。パッチ適用により再起動が伴うことへの配慮が必要であり、またパッチ適用によるIACSへの影響を事前に検証しなければならない。尚、IEC62443-2-1の付属書Aでは、事前検証の重要性について説明している。このような背景は審査側においても前提知識として求められる。

附属書 C（参考）

審査工数

審査工数は，JIS Q 27006:2012の附属書Cを参考されたい。また、工数増減の要因として次のCSMS固有の要因が例として挙げられる。

・認証の対象者
　－制御システムを利用する事業者（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）
・対象となるIACS
・IACS の対象プラント
・制御システムセキュリティの製品認証である「EDSA認証」等のIACSを設置

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。