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-CSAC100-2.0

2016 年 1 月 15 日

一般財団法人　日本情報経済社会推進協会

〒106-0032　東京都港区六本木一丁目９番９号
六本木ファーストビル内
Tel.03-5860-7570　　Fax.03-5573-0564
URL　http://www.isms.jipdec.or.jp/

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	
2.0	2016.1.15	JIS Q 17021-1:2015 発行に伴う改訂	

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 17021-1 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 17021-1 に適合しているとして認定するためには，JIS Q 17021-1 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 17021-1 の構成に沿っている。また，JIS Q 17021-1 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 17021-1 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 17021-1 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ことを意図しており，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 17021-1 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－第1部：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

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 17021-1 及びCSMS認証基準 によるほか，次による。

3.1

認証文書（certification document）

依頼者のCSMS が，特定したCSMS 規格及び依頼者の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。

4　原則

原則は，JIS Q 17021-1 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 17021-1 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 17021-1 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，次の業務を遂行してもよい。

a) 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，公開されており入手可能な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，b)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。

b) 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(9.1.3.6 参照)

c) 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。

d) 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

e) 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者のCSMS の内部のサイバーセキュリティレビューを提供してはならない。さらに，認証機関は，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 17021-1 の5.3 による。

6 組織運営機構に関する要求事項

組織運営機構に関する要求事項は，JIS Q 17021-1の箇条6による。

7 資源に関する要求事項

7.1 要員の力量

要員の力量は，JIS Q 17021-1 の7.1 によるほか，次の要求事項及び手引による。

7.1.1 CS 7.1 一般考慮事項

7.1.1.1 一般的な力量要求事項

認証機関は，審査する依頼者のCSMS に関連する技術,法的及び規制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，JIS Q 17021-1の表A.1に規定する認証の機能別に力量要求事項を定めなければならない。認証機関は，JIS Q 17021-1に規定する全ての要求事項，並びにこの規格の箇条7.1.2及び7.2.1に規定する全ての要求事項（これは自身が定めたCSMSにおける専門分野に関連する。）を考慮しなければならない。

7.1.2 CS 7.1.2 力量の判断基準の決定

JIS Q 17021-1 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。

7.1.2.1 CSMS審査に関する力量要求事項

7.1.2.1.1 一般要求事項

認証機関は，次の事項を確実にするために，審査チームメンバーの経歴の検証，及び特定の教育・訓練又は概要説明（ブリーフィング）に関する基準をもたなければならない。

a) サイバーセキュリティについての知識
b) 審査対象となる活動についての専門的知識
c) マネジメントシステムについての知識
d) 監査の原則についての知識

注記 監査の原則についての詳細はISO 19011に示されている。

e) CSMS の監視，測定，分析及び評価についての知識

このような上記a)～e)の要求事項は，審査チームの審査員間で分担できるb)を除き，審査チームの全ての審査員に適用する。

審査チームは，依頼者のCSMSにおけるサイバーセキュリティインシデントを示すものから適切なCSMSの要素まで遡れることのできる力量をもっていなければならない。

審査チームは，上記項目の適切な業務経験を持ち，かつ，こ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。）。

7.1.2.1.2 サイバーセキュリティマネジメントの用語，原則，実務及び技術

審査チームの全てのメンバーは，全体として，次の知識をもたなければならない。

a) CSMSに固有な文書の構造，階層及び相互関係
b) サイバーセキュリティマネジメントに関連するツール，方法及び技法，並びにこれらの適用
c) サイバーセキュリティリスクアセスメント及びリスクマネジメント

各審査員は，a)，c)を満たさなければならない。

7.1.2.1.3 サイバーセキュリティマネジメントシステムの規格及び規準文書

CSMS審査に関与する審査員は，次の知識をもたなければならない。
a) CSMS認証基準に含まれる全ての要求事項。
審査チームの全てのメンバーは，全体として，次の知識をもたなければならない。
b) 次のように分類される，CSMS認証基準に規定される全ての詳細管理策，及びその実施。
1) 事業継続計画
2) 要員のセキュリティ
3) 物理的及び環境的セキュリティ
4) ネットワークの分割
5) アクセス制御－アカウント管理
6) アクセス制御－認証
7) アクセス制御－認可
8) システムの開発及び保守
9) 情報及び文書のマネジメント
10) インシデントの計画及び対応

7.1.2.1.4 ビジネスマネジメントの実務

CSMS審査に関与する審査員は，次の知識をもたなければならない。
a) 産業界における優れたサイバーセキュリティの慣行，及びサイバーセキュリティ手順
b) サイバーセキュリティの方針及び事業上の要求事項
c) 一般的なビジネスマネジメントの概念，実務，及び方針と目的と結果との相互関係
d) マネジメントプロセス及び関連する用語
注記 マネジメントフロセスには，人的資源のマネジメント，内部及び外部のコミュニケーション，並びにその他の関連する支援プロセスも含む。

7.1.2.1.5 依頼者の事業分野

CSMS審査に関与する審査員は，次の知識をもたなければならない。
a) 地理及び法的管轄区といった，特定のサイバーセキュリティ領域における法的及び規制の要求事項
注記 法的及び規制の要求事項の知識とは，法律に関する高度に専門的な経歴を意味するものではない。
b) 事業分野に関連するサイバーセキュリティリスク
c) 依頼者の事業分野に関する一般的な用語，プロセス及び技術
d) 関連する事業分野の実務
基準a)は，審査チーム内で分担できる。

7.1.2.1.6 依頼者の製品，プロセス及び組織

CSMS審査に関与する審査員は，全体として，次の知識をもたなければならない。
a) 外部委託を含む，組織の種類，規模，ガバナンス，構造，機能及び関係が，CSMSの開発及び実施並びに認証活動に及ぼす影響
b) 広い視野から見た複雑な業務
c) 製品又はサービスに適用される法的及び規制の要求事項

7.1.2.2 CSMS審査チームの指揮に関する力量要求事項

7.1.2.1の要求事項に加えて，審査チームリーダーは，次の要求事項を満たさなければならない。この要求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しなければならない。
a) 認証審査プロセス及び審査チームを管理する知識及び技能
b) 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の実証
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。

7.1.2.3 申請のレビューの実施に関する力量要求事項

7.1.2.3.1 サイバーセキュリティマネジメントシステムの規格及び規準文書

審査チームに要求される力量を判定し，審査チームメンバーを選定し，審査工数を決定するための申請のレビューを実施する要員は，次の知識をもたなければならない。
a) 認証プロセスで用いられる関連するCSMS規格及びその他の規準文書

7.1.2.3.2 依頼者の事業分野

審査チームに要求される力量を判定し，審査チームメンバーを選定し，審査工数を決定するための申請のレビューを実施する要員は，次の知識をもたなければならない。

a) 依頼者の事業分野に関連する一般的な用語，プロセス，技術及びリスク

7.1.2.3.3 依頼者の製品，プロセス及び組織

審査チームに要求される力量を判定し，審査チームメンバーを選定し，審査工数を決定するための申請のレビューを実施する要員は，次の知識をもたなければならない。

a) 外部委託機能を含む，CSMSの開発及び実施並びに認証活動に関する，依頼者の製品，プロセス，組織の種類，規模，ガバナンス，構造，機能及び関係

7.1.2.4 審査報告書のレビュー及び認証の決定に関する力量要求事項

7.1.2.4.1 一般

審査報告書のレビュー及び認証の決定を行う要員は，認証範囲の適切性及び認証範囲の変更の適切性を検証でき，特にインタフェース及び依存関係並びにその関連リスクの特定が継続して妥当かどうかについて，審査の有効性に対するその変更の影響を検証することができる知識をもたなければならない。

さらに，審査報告書のレビュー及び認証の決定を行う要員は，次の知識をもたなければならない。

a) マネジメントシステム全般
b) 審査プロセス及び手順
c) 審査の原則，実務及び技術

7.1.2.4.2 サイバーセキュリティマネジメントの用語，原則，実務及び技術

審査報告書のレビュー及び認証の決定を行う要員は，次の知識をもたなければならない。

a) 7.1.2.1.2の箇条書きのa)及びc)に列挙する項目
b) サイバーセキュリティに関連した法的及び規制の要求事項

7.1.2.4.3 サイバーセキュリティマネジメントシステムの規格及び規準文書

審査報告書のレビュー及び認証の決定を行う要員は，次の知識をもたなければならない。

a) 認証プロセスで用いられる関連するCSMS規格及びその他の規準文書

7.1.2.4.4 依頼者の事業分野

審査報告書のレビュー及び認証の決定を行う要員は，次の知識をもたなければならない。

a) 関連の事業分野の実務に関する一般的な用語及びリスク

7.1.2.4.5 依頼者の製品，プロセス及び組織

審査報告書のレビュー及び認証の決定を行う要員は，次の知識をもたなければならない。

a) 依頼者の製品，プロセス，組織の種類，規模，ガバナンス，構造，機能及び関係

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 17021-1 の7.2 によるほか，次の要求事項及び手引による。

7.2.1 CS 7.2 審査員の知識及び経験の実証

認証機関は，審査員が知識及び経験をもっていることを次の事項によって実証しなければならない。

a) CSMS固有の認知された資格
b) 該当する場合には，審査員としての登録
c) CSMS研修コースへの参加，及び該当する資格証明書の取得
d) 専門能力開発についての最新の記録
e) 他のCSMS審査員の立ち合いによる，CSMS審査

7.2.1.1 審査員の選定

7.1.2.1に加えて，審査員の選定基準は，各審査員が附属書AのA.1の事項を満たすことが望ましい。

7.2.1.2 審査チームを指揮する審査員の選定

7.1.2.2及び7.2.1.1に加えて，審査チームを指揮する審査員の選定基準は，当該審査員が附属書AのA.2の事項を満たすことが望ましい。

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 17021-1 の7.3 によるほか，次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

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。技術専門家に対する最小限の要求事項は，7.2.1.1に記載されている。

7.4 要員の記録

要員の記録は，JIS Q 17021-1 の7.4 による。

7.5 外部委託

外部委託は，JIS Q 17021-1 の7.5 による。

8 情報に関する要求事項

8.1 情報の公開

情報の公開は，JIS Q 17021-1 の8.1 による。

8.2 認証文書

認証文書は，JIS Q 17021-1 の8.2 によるほか，次の要求事項及び手引による。

8.2.1 CS 8.2 CSMS 認証文書

認証文書は，権限を与えられた者が署名しなければならない。認証文書は，適用宣言書の版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，認証文書の更新は、必ずしも求められない。

8.3 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 17021-1 の8.3 による。

8.4 機密保持

機密保持は，JIS Q 17021-1 の8.4 によるほか，次の要求事項及び手引による。

8.4.1 CS 8.4 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 に関連する情報（例えばCSMSの記録又は管理策の設計及び有効性の情報）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，これらの情報がなくても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情報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者が行うまで，認証審査を開始できないことを依頼者に通知しなければならない。

8.5 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 17021-1 の8.5 による。

9 プロセス要求事項

9.1 認証活動に先立つ事項

9.1.1 申請

申請は，JIS Q 17021-1 の9.1.1 によるほか，次の要求事項及び手引による。

9.1.1.1 CS 9.1.1 申請の準備

認証機関は，依頼者に対して，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。

9.1.2 申請のレビュー

申請のレビューは，JIS Q 17021-1 の9.1.2 によるる。

9.1.3 審査プログラム

審査プログラムは，JIS Q 17021-1 の9.1.3 によるほか，次の要求事項及び手引による。

9.1.3.1 CS 9.1.3 一般

CSMS審査のための審査プログラムでは、決定されたサイバーセキュリティ管理策を考慮しなければならない。

9.1.3.2 CS 9.1.3 審査方法

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，依頼者のCSMS がCSMS認証基準 に規定する要求事項並びに依頼者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。

9.1.3.3 CS 9.1.3 初回審査のための一般準備

認証機関は，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へのアクセスのための必要な手配を全て行うことを依頼者に要求しなければならない。

依頼者は，認証審査の第一段階の間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認証基準で規定する必要なCSMS 文書の写し及び必要な場合，関連文書の写し

9.1.3.4 CS 9.1.3 レビュー期間

認証機関は，少なくとも一つのマネジメントレビュー及び一つのCSMS内部監査（認証範囲をその対象に含む）が運用されるまでは，CSMSを認証してはならない。

9.1.3.5 CS 9.1.3 認証範囲

審査チームは，定義された範囲に含まれる依頼者の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，依頼者の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，依頼者が自らの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，認証範囲ごとに，少なくとも1つの適用宣言書があることを検証しなければならない。

認証機関は，依頼者が，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，業務機能の外部委託）。

9.1.3.6 CS 9.1.3 認証審査基準

依頼者のCSMS を審査するための基準は，CSMS認証基準でなければならない。また，依頼者が遂行する機能に関連する認証のために，その他の文書を要求してもよい。

9.1.4 審査工数の決定

申審査工数の決定は，JIS Q 17021-1の9.1.4によるほか，次の要求事項及び手引による。

9.1.4.1 CS 9.1.4 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。審査工数全体の計算には，審査報告書作成のための十分な時間を含めなければならない。また，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。

9.1.5 複数サイトサンプリング

複数サイトサンプリングは，JIS Q 17021-1の9.1.5によるほか，次の要求事項及び手引による。

9.1.5.1 CS 9.1.5 複数サイト（Multiple sites）

9.1.5.1.1 依頼者が次の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，依頼者の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，依頼者のCSMS マネジメントレビュープログラムに含まれている。

9.1.5.1.2 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) 各種事業所のIACS の複雑さ
   6) 作業慣行の違い
   7) 行っている活動の違い
   8) 管理策の設計及び運用の違い
   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
   11) 地理的及び文化的側面
   12) サイトのリスクの状況
   13) 特定のサイトのサイバーセキュリティインシデント

c) 依頼者の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。

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，依頼者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。

9.1.6 複数のマネジメントシステム

複数のマネジメントシステムは，JIS Q 17021-1の9.1.6によるほか，次の要求事項及び手引による。

9.1.6.1 CS 9.1.6 CSMS 文書と他のマネジメントシステム文書との統合

認証機関は，（例えば，サイバーセキュリティ，品質，安全衛生，環境に関する）組み合わせた文書を許可してもよい。ただし，他のマネジメント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。

9.1.6.2 CS 9.1.6 マネジメントシステム複合審査

CSMS 審査は，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には，他のマネジメントシステムの審査と複合してもよい。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 審査の計画作成

9.2.1 審査の目的，審査範囲及び審査基準の決定

審査の目的，審査範囲及び審査基準の決定は，JIS Q 17021-1の9.2.1によるほか，次の要求事項及び手引によ

る。

9.2.1.1 CS 9.2.1 審査目的

審査目的には，依頼者がリスクアセスメントに基づいて該当する管理策を実施しており，かつ，確立したサイバーセキュリティ目的を達成していることを確実にするために，マネジメントシステムの有効性の決定を含めなければならない。

9.2.2 審査チームの選定及び割当て

審査チームの選定及び割当ては，JIS Q 17021-1の9.2.2によるほか，次の要求事項及び手引による。

9.2.2.1 CS 9.2.2 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。審査チームに与える業務を明確に定め，依頼者にも通知しなければならない。審査チームは1名で構成してもよいが，その人は，7.1.2.1の基準を全て満たしていなければならない。

9.2.2.2 CS 9.2.2 審査チームの力量

7.1.2 に記載の要求事項を適用する。サーベイランス活動及び特別審査活動については，計画されたサーベイランス活動及び特別審査活動に関する要求事項だけとする。

ある特定の認証審査を担当させる審査チームを選定及び管理する場合，認証機関は，その審査チームの力量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(技術専門家がこの役割を果たしてもよい。)。

b) 依頼者の活動，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，組織内におけるCSMSの適用範囲及び状況において，信頼できるCSMS認証審査を行うのに十分な程度，依頼者について理解している。

c) 依頼者のCSMSに適用される法的及び規制の要求事項を適切に理解している。

注記 「適切に理解している」とは，法律に関する高度に専門的な経歴を意味するものではない。

9.2.3 審査計画

審査計画は，JIS Q 17021-1の9.2.3によるほか，次の要求事項及び手引による。

9.2.3.1 CS 9.2.3 一般

CSMS審査のための審査計画では，決定されたサイバーセキュリティ管理策を考慮しなければならない。

9.2.3.2 CS 9.2.3 ネットワーク支援の審査手法

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。

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。

9.2.3.3 CS 9.2.3 審査のタイミング

認証機関は，被審査組織と，その組織の適用範囲全体を最も良く実証するであろう審査時期について合意することが望ましい。この検討考慮には，適宜，季節，月，曜日／日付及び勤務シフトを含むことができる。

9.3 初回認証

初回認証は，JIS Q 17021-1 の9.3 によるほか，次の要求事項及び手引による。

9.3.1 CS 9.3.1 初回認証審査

9.3.1.1 CS 9.3.1.1 第一段階

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，依頼者のCSMSの設計に関する文書を入手しなければならない。

認証機関は，依頼者の組織，リスクアセスメント及び対応（決定された管理策を含む），サイバーセキュリティポリシー及び目的に照らしてそのCSMS の設計に対する十分な理解を得なければならず，かつ，特に，依頼者の審査に対する準備状況について，十分に理解しなければならない。これによって，第二段階のための計画が可能になる。

第一段階の結果は，報告書として文書化しなければならない。認証機関は，第二段階への移行を決定する前に，第二段階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，依頼者に知らせておかなければならない。

9.3.1.2 CS 9.3.1.2 第二段階

9.3.1.2.1 認証機関は，第一段階の審査報告書に文書化された所見に基づき，第二段階を行うための審査計画を策定する。第二段階の目的は，CSMSの有効な実施を評価することのほか，次のとおりである。

a) 依頼者が自らのポリシー，目的及び手順を守っていることを確認する。

9.3.1.2.2 そのために，この審査は，依頼者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ポリシー及び目的に対する，トップマネジメントのリーダーシップ及びコミットメント

b) CSMS認証基準に掲げられた文書化に関する要求事項

c) サイバーセキュリティに関連するリスクのアセスメント，及びそのアセスメントが繰り返し実施された場合に，一貫性及び妥当性があり，かつ，比較可能な結果を生み出すこと

d) そのサイバーセキュリティ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，管理目的及び管理策の決定

e) そのCSMSの目的に照らして報告及びレビューされる，サイバーセキュリティパフォーマンス及びCSMSの有効性のレビュー

f) 選択・導入された管理策，適用宣言書，サイバーセキュリティ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

g) 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，トップマネジメントの決定，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。

9.4 審査の実施

審査の実施は，JIS Q 17021-1の9.4によるほか，次の要求事項及び手引による。

9.4.1 CS 9.4 一般

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 17021-1に従って行う，依頼者のCSMSの初回認証審査

b) JIS Q 17021-1に従って定期的に実施する依頼者の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，依頼者のCSMSが該当する要求事項に継続的に適合していること，及び依頼者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。

9.4.2 CS 9.4 CSMS 審査の固有の要素

認証機関は，審査チームをその代表として，次の事項を実施しなければならない。

a) サイバーセキュリティに関するリスクアセスメントがCSMSの適用範囲内におけるCSMSの運用に関連があり，かつ，適切であることを実証するよう依頼者に求める。

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，依頼者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，リスク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。

9.4.3 CS 9.4 審査報告書

9.4.3.1 JIS Q 17021-1の9.4.8の報告書に関する要求事項に加えて，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) 依頼者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) 審査計画からの逸脱(例えば，予定された活動を超えるか又はそれよりも少ない時間)

d) CSMSの適用範囲

9.4.3.2 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) 重要な審査証跡及び利用した審査方法を含める（9.1.3.2 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 17021-1 の9.4.8 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 の要求事項及び管理策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
－ 依頼者の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。

9.5 認証の決定

認証の決定は，JIS Q 17021-1の9.5によるほか，次の要求事項及び手引による。

9.5.1 CS 9.5 認証の決定

認定の決定は，JIS Q 17021-1 によるほか，審査報告書（9.4.3 参照）で示された審査チームによる認証の推薦に基づかなければならない。

認証の授与の決定を行う者又は委員会は，通常，審査チームの否定的な推薦を覆すことは望ましくない。そのような状況が生じた場合，認証機関は，審査チームの否定的な推薦を覆すという決定の根拠を文書化し，かつ，その根拠の正当性を示さなければならない。

依頼者のマネジメントレビュー及びCSMS内部監査のための取決めが導入されていて，かつ有効であり，かつ，維持されることを実証する十分な証拠が得られるまでは，依頼者に認証を授与してはならない。

9.6 認証の維持

サーベイランス活動は，JIS Q 17021-1 の9.6 によるほか，次のCSMS 固有の要求事項及び手引による。

9.6.1 一般

一般は，JIS Q 17021-1の9.6.1による。

9.6.2 サーベイランス活動

サーベイランス活動は， JIS Q 17021-1の9.6.2によるほか，次の要求事項及び手引による。

9.6.2.1 CS 9.6.2 サーベイランス活動

9.6.2.1.1 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，依頼者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（サイバーセキュリティリスクアセスメント及び管理策の維持， CSMS 内部監査，マネジメントレビュー，並びに是正処置など）
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求事項
f) 該当するその他の選択した領域

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

a) 依頼者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) 決定した管理策の変更，及びその結果生じるSoAの変更
d) 審査プログラムに従った，管理策の実施状況及び有効性

9.6.2.1.3 認証機関は，サーベイランスプログラムを，IACS資産に対する脅威，ぜい弱性及び依頼者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。

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，認証機関に持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，依頼者が自らの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，並びにSoAの版及び前回審査からの重要な変更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9.6.2.1.1及び9.6.2.1.2の要求事項を含むように作成しなければならない。

9.6.3 再認証

再認証は，JIS Q 17021 の9.6.3 によるほか，次の要求事項及び手引による。

9.6.3.1 CS 9.6.3 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者のCSMS 初回認証審査に関する手順と整合していなければならない。

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，関連するサイバーセキュリティリスクに応じたものでなければならない。

9.6.4 特別審査

特別審査は，JIS Q 17021 の9.6.4 によるほか，次の要求事項及び手引による。

9.6.4.1 CS 9.6.4 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。

9.6.5 認証の一時停止，取消し，又は範囲の縮小

認証の一時停止，取消し，又は認証範囲の縮小は，JIS Q 17021-1 の9.6.5 による。

9.7 異議申立て

異議申立ては，JIS Q 17021-1 の9.7 による。

9.8 苦情

苦情は，JIS Q 17021-1 の9.8 によるほか，次の要求事項及び手引による。

9.8.1 CS 9.8 苦情

苦情は，潜在的なインシデント及び潜在的な不適合を示す。

9.9 依頼者に関する記録

依頼者に関する記録は，JIS Q 17021-1 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

選択肢は，JIS Q 17021 の10.1 による。

10.2 選択肢A：マネジメントシステムに対する一般要求事項

マネジメントシステムに対する一般要求事項は，JIS Q 17021 の10.2 による。

10.3 選択肢B：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10.3 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) 大学教育と同等なレベルの専門的教育又は訓練を修了している。
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) 少なくとも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，再認証審査及びサーベイランス審査を含めて，最低4 回延べ20日間（そのうち最大5日間はサーベイランス審査への参加でもよい）以上にわたるCSMS認証審査への参加によって得ていることが望ましい。この参加には，文書及びリスクアセスメントのレビュー，CSMS導入の審査，並びに審査報告書の作成を含まれていることが望ましい。
e) 関連しかつ最近の経験がある。
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) 少なくとも3 回のCSMS 審査の全段階において積極的に参加している。この参加には初回の適用範囲の決定及び計画立案，文書及びリスクアセスメントのレビュー，CSMS導入の審査及び正式な審査報告書の作成が含まれていることが望ましい。

注記 A.1，及びA.2の事項については，ISO/IEC 27006:2015の7.2.1.1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，ISO/IEC 27006:2015の附属書B及び附属書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