

ISO/IEC 27017 に基づく
ISMS クラウドセキュリティ認証に関する要求事項
JIP-ISMS517-2.0

2026 年 10 月 14 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

URL <https://www.jipdec.or.jp/>

JIPDEC の許可なく転載することを禁じます

改 版 履 歴

版数	制定／改訂日	改定箇所、改訂理由	備考
1.0	2016.8.1	ISO/IEC 27017:2015 に基づく ISMS クラウドセキュリティ認証用として制定	初版
2.0	2026.10.14	ISO/IEC 27017:2026 発行に伴い、文書全般について対応箇所の変更、要求事項の明確化、及び表現の修正を実施 対応箇所の変更、要求事項の明確化、及び表現の修正 修正に伴い一部の項番を移動 序文(削除→ 新 4.1 へ)、4.1(新たに追加。以降、項番を繰り下げ) 旧 4.3(削除→新 4.1 等に包含)	

1. 概要

本文書は、ISO/IEC 27017 に基づいて、クラウドサービスを含む情報セキュリティマネジメントシステム（以下、ISMS という。）を確立し、実施し、維持し、継続的に改善するための ISMS クラウドセキュリティ認証のための要求事項を提供する。

クラウドサービスプロバイダは、クラウドサービスカスタマに対し、クラウドサービスの提供にかかる情報セキュリティガバナンス及びマネジメントに関するコミットメントを明示するとともに、クラウドサービスにおける活動状況に関する情報を提供することが求められる。これにより、クラウドサービスカスタマは、情報セキュリティ活動に必要な情報を入手し、それらを踏まえてクラウドサービスプロバイダが提供するクラウドサービスを利用する、又はその上にシステムを構築することが可能となる。

したがって、認証取得にあたっては、クラウドサービスプロバイダ、クラウドサービスカスタマのいずれか、または両方の立場にあるのかを明確にし、それぞれの役割に応じた情報セキュリティ対策を実施する必要がある。

特にクラウドサービスを利用する場合、その利用によってどのようなリスクの変化が生じ、組織の情報セキュリティにどのような影響を及ぼすかを検討する必要がある。その上で、必要となる新たな情報セキュリティ対策の導入を計画・実施することにより、クラウドサービスの利用に伴うリスクを適切にマネジメントすることが可能となる。

2. 引用規格

- JIS Q 27001:2025 (ISO/IEC 27001:2022+Amd 1:2024)
 - JIS Q 27001:2025 情報セキュリティ, サイバーセキュリティ及びプライバシー保護－情報セキュリティマネジメントシステム－要求事項（追補 1）
 - JIS Q 27001:2023 情報セキュリティ, サイバーセキュリティ及びプライバシー保護－情報セキュリティマネジメントシステム－要求事項
- ISO/IEC 27017:2026
Information security, cybersecurity and privacy protection -- Information security controls based on ISO/IEC 27002 for cloud services

注記：ISO/IEC 27017:2026と内容が一致する JIS Q 27017 が発行された後は、それに読み替えるものとする。

3. 用語及び定義

本文書で用いる主な用語及び定義は、ISO/IEC 27017 による。

4. 要求事項

4.1 一般

特段の定めのない限り、JIS Q 27001:2025「情報セキュリティ, サイバーセキュリティ及びプライバシー保護－情報セキュリティマネジメントシステム－要求事項」を全て適用しなければならない。

そのうえで、組織は、次の要求事項に従って、クラウドサービス固有のリスクへの対応を自らの ISMS の確立、実施、維持及び継続的改善の中に組み込まなければならない。カッコ【】内は、対応する JIS Q 27001 の項番を示す。

ISO/IEC 27017 の管理策及び手引の「～することが望ましい」は、「～しなければならない」と読み替える。

4.2 クラウドサービスを含む情報セキュリティマネジメントシステムの適用範囲の決定

【 JIS Q 27001 の 4.3 】

組織は、クラウドサービスを含めた ISMS の適用範囲を定めるために、その境界及び適用可能性を決定しなければならない。

クラウドサービスを含めた ISMS の適用範囲は、クラウドサービスを特定して、識別できる情報（A.1 を

参照)を含む文書化した情報として利用可能な状態にしておかなければならない。

適用範囲を定める際、クラウドサービスプロバイダが自らのサービスを提供するに当たり、別のクラウドサービスを利用している場合は、クラウドサービスプロバイダ及びクラウドサービスカスタマの両方を適用範囲としなければならない。

注記：ISO/IEC 27017 の箇条 4 では、クラウドサービスプロバイダの情報セキュリティ管理の対象は、クラウドサービスカスタマの情報セキュリティ対策のための情報提供や機能提供を含むものと規定されている。これに従い、クラウドサービスプロバイダは、クラウドサービスカスタマとの関係を含めた適用範囲を検討することが必要である。

4.3 ISO/IEC 27017 の規格に沿ったクラウド情報セキュリティ対策の実施

注記：JIS Q 27001 は、組織の状況の下で ISMS を確立し、実施し、維持し、継続的に改善するための要求事項を規定している。また、組織のニーズに応じて調整した情報セキュリティのリスクアセスメント及びリスク対応を行うための要求事項について規定している。

・4.3.1 情報セキュリティリスクアセスメント【 JIS Q 27001 の 6.1.2 c) 】

組織は、次の事項を行う情報セキュリティリスクアセスメントのプロセスを定め、適用しなければならない。

c) 次によって情報セキュリティリスクを特定する。

- 1) ISMS の適用範囲内におけるクラウドサービスに関する情報の機密性、完全性及び可用性の喪失に伴うリスクを特定するために、情報セキュリティリスクアセスメントのプロセスを適用する。
- 2) これらのリスク所有者を特定する。

・4.3.2 情報セキュリティリスク対応【 JIS Q 27001 の 6.1.3 a)～d)】

組織は、次の事項を行うために、情報セキュリティリスク対応のプロセスを定め、適用しなければならない。

- a) ISMS の適用範囲内におけるクラウドサービスのリスクアセスメントの結果を考慮して、適切な情報セキュリティリスク対応の選択肢を選定する。
- b) 選定した情報セキュリティリスク対応の選択肢の実施に必要な全ての管理策を決定する。
- c) 4.3.2b)で決定した管理策を JIS Q 27001 の附属書 A 及び ISO/IEC 27017 に示す管理策と比較し、必要な管理策が見落とされていないことを検証する。
- d) 次を含む適用宣言書を作成する。
 - 必要な管理策[4.3.2 の b)及び c)参照]
 - それらの管理策を含めた理由

- それらの必要な管理策を実施しているか否か
- JIS Q 27001 の附属書 A 及び ISO/IEC 27017 に示す管理策を除外した理由

注記 1 : ISO/IEC 27017 に示す管理策には、JIS Q 27001 の管理策に対してクラウドサービスのための手引を追加した管理策、及びクラウドサービス固有の管理策が含まれる。

注記 2 : クラウドセキュリティに基づくリスク分析の結果に基づいて、ISO/IEC 27017 に記載されているクラウドサービスのための手引を参照し、クラウドサービス固有のリスクに対する管理策として、必要な事項を選択し、実施する。

注記 3 : ISO/IEC 27017 に示す管理策は、クラウドサービスプロバイダ及びクラウドサービスカスタマに対する固有の管理策であるため、原則は全ての管理策の評価を実施することとなる。

ただし、サービスの種類によって、管理策が該当しない場合には、適用除外することができる。

注記 4 : ISMS クラウドセキュリティ認証の適用宣言書を JIS Q 27001 の適用宣言書と別に作成する場合は、基となる JIS Q 27001 の適用宣言書との関連を明確にする必要がある。

参考 A

本文書の要求事項をより深く理解するためのガイドを以下に示す。

A.1 クラウドサービスを含む ISMS の適用範囲の決定

クラウドサービスを含む ISMS の適用範囲*の決定（本文書の 4.2 参照）に際しては、当該適用範囲が JIS Q 27001 の適用範囲（ISMS の適用範囲）を越えないことを確保する必要がある。すなわち、当該適用範囲は、以下の 2 つの場合のいずれかに限られる。

- 1) JIS Q 27001 の適用範囲の一部である。
- 2) JIS Q 27001 の適用範囲と一致する。

クラウドサービスが JIS Q 27001 の適用範囲に一部しか含まれていない場合又は全く含まれていない場合は、JIS Q 27001 の適用範囲の拡張を含む見直しにより、上記 1) 又は 2) のいずれかに該当させる必要がある。

また、クラウドサービスを含む ISMS の適用範囲を示す文書については、当該適用範囲に含まれるクラウドサービス名を記載すること等により、当該適用範囲に含まれないクラウドサービスと明確に区別できるよう、誤解を招かないようにすることが重要である。

なお、クラウドサービスを含む ISMS の適用範囲が上記 1) 又は 2) のいずれかに該当する場合は、JIS Q 27001 の適用範囲を示す文書の内容に変更を求めるものではない。

*ここでいう「クラウドサービスを含む ISMS の適用範囲」とは、本文書（ISO/IEC 27017 に基づく ISMS クラウドセキュリティ認証に関する要求事項）に従って定義した適用範囲である。

A.2 クラウドセキュリティにおけるリスクアセスメント・リスク対応

ISMSクラウドセキュリティ認証においては、クラウドサービスの情報セキュリティリスクアセスメントの結果による管理策の追加および管理策の補充（クラウドサービス固有の追加的な対策の実施）が必要である。

クラウドセキュリティにおけるリスクアセスメント・リスク対応での考慮事項は、以下の通りである。

- 1) ISO/IEC 27017 の管理策を参照した、リスクアセスメント・リスク対応
 - ・（ISMS の適用範囲内における）クラウドサービスのリスクアセスメントを実施する。
 - ・ リスク対応にあたっては、特に、本文書の 4.3.2 の注記 2 に記載のとおり、「クラウドセキュリティに基づくリスク分析の結果に基づいて、ISO/IEC 27017 に記載されているクラウドサービスのための手引を参照し、クラウドサービス固有のリスクに対する管理策として、必要な事項を選択し、実施する。」ことが必要となる。
 - ・ ISO/IEC 27017 におけるクラウドサービス固有の管理策の属性は、管理策の特性を示すものであることから、リスク対応を行う際の参考となる。
- 2) 「適用宣言書」における ISO/IEC 27017 適用の記載方法
 - ・ 本文書の 4.3.2 d) に基づき、ISO/IEC 27017 に記載されているクラウドサービスのための手引についての実施の可否についても確認できるように、適用宣言書に、ISO/IEC 27017 に記載されている手引についても含めることが望ましい。また、JIS Q 27001 附属書 A の全ての管理策を含めるか参照することで、ISO/IEC 27017 以外のクラウドに関連する ISMS 管理策の実施の可否（詳細は A.4 参照）も確認できるようにすることが望ましい。詳細については、「A.3 適用宣言書」を参照。

A.3 適用宣言書の例

ISMSクラウドセキュリティ認証では、本文書の4.3.2 d) に基づき適用宣言書を作成する。次に適用宣言書の一例を示す。

適用宣言書 (カスタマ) / (プロバイダ) ※1

※1 いずれか、もしくは両方に○。

管理策	管理策を含めた理由	27001[管理策]の実施	27017[管理策]の実施		除外理由
			カスタマ	プロバイダ	
5 組織的管理策					
5.1 情報セキュリティのための方針群	・～のため	○	○	○	
5.2 情報セキュリティの役割及び責任	・～のため	○	○	○	
5.3 職務の分離	・～のため	○	－	－	27017 には追加の手引なし
(中略)					
5.38 CLD クラウドコンピューティング環境における役割及び責任の共有及び分担	・～のため	－	○	○	
5.39 CLD クラウドサービスパートナーの役割及び責任に関する合意	・～のため	－	○		
6 人的管理策					
6.1 選考	・～のため	○	－	－	27017 には追加の手引なし
6.2 雇用条件	・～のため	○	－	－	27017 には追加の手引なし
6.3 情報セキュリティの意識向上、教育及び訓練	・～のため	○	○		
(中略)					

8 技術的管理策					
8.1 利用者エンドポイント機器	・～のため	○	－	－	27017 には追加の手引なし
8.2 特権的アクセス権	・～のため	○	○	○	
8.3 情報へのアクセス制限	・～のため	○	○	○	
(中略)					
8.34 監査におけるテスト中の情報システムの保護	・～のため	○	－	－	27017 には追加の手引なし
8.35 CLD 仮想コンピューティング環境における分離	・～のため	－	○	○	
8.36 CLD クラウドサービスの認可されていない利用の検出及び防止	・～のため	－	○	○	

＊ 管理策名称の冒頭に「CLD」の付く番号の管理策は、ISMS 管理策に加えて規定されたクラウドサービスプロバイダ及びカスタマに対する固有の管理策であるため、原則は全ての管理策の評価を実施することとなるが、クラウドサービスの種類によっては、管理策が該当しない場合がある。そのような場合は、管理策を適用除外とすることができる。

A.4 考慮事項

いくつかの管理策の実施については、クラウドサービス固有のリスクへの対策として有効な方策を提供しているので、これらの方策の導入が強く求められる。

- ・クラウドサービスにおいては、クラウドサービスカスタマ及びクラウドサービスプロバイダが各々に割り当てられた役割及び責任（責任共有モデル）に基づいてそれぞれの責任を果たすことが重要である。特にクラウドサービスプロバイダは、クラウドサービスカスタマの情報セキュリティを支援するため、責任共有モデルにおける役割及び責任を明確にするとともに、必要な情報及び機能を提供することが強く求められる（例えば、ISO/IEC 27017 の 5.1 及び 5.38 等）。
- ・適用法令及び契約上の要求事項の特定については、ISO/IEC 27017 の 5.31 のクラウドサービスのための手引に記載された対策の適用が強く求められる。
- ・クラウドサービスプロバイダの管理範囲およびその責任が遂行されていることに関する開示は、一方的なものではなく、契約行為を含む取り決めが必要となる。情報セキュリティのレビューに関しては、ISO/IEC 27017 の 5.35 のクラウドサービスのための手引の適用が強く求められる。
- ・ISO/IEC 27017 のクラウドサービスのための手引には含まれないが、クラウドセキュリティへの関与が強い ISMS の管理策に関しては、それらの管理策を適用することが強く求められる（例えば、5.15 アクセス制御、8.22 ネットワークの分離等）。

以上