ISO/IEC 27017:2015 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-ISMS517-1.0 draft3

2016 年 6 月 27 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
1.0 draft	2016.4.21	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
1.0 Draft2	2016.5.27	用語の統一及びそれに伴う表記の見直し 要件 → 要求事項	
1.0 Draft3	2016.6.27	4.3 内部監査 a) 2)の表記見直し	

序文

本文書は、ISMSクラウドセキュリティ認証に必要なマネジメントシステムを確立、実施、維持及び継続的に改善するための要求事項を提供するために作成された。

本文書は、以下の本文で特段の定めのない限り、JIS Q 27001：2014「情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－ 要求事項」をそのまま適用する。

1. 概要

本文書は、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について、クラウドサービスカスタマへの報告（Report）の一部を成すとともに、クラウド活動状況をクラウドサービスカスタマに提供することを約束（コミットメント）する。このコミットメントにより、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、クラウドサービスを利用、またはクラウド上にシステムを構築することができる。

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の立場に立つかを明確にする必要がある。

特にクラウドサービスを利用する場合、どのようなリスクの変化があり、どのような影響があるのかを検討し、新たな情報セキュリティ対策の導入を計画することで適切なリスクマネジメントの取り組みが可能となる。

（出典：「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」
経済産業省 2013 年度版を参考に作成した）

2. 引用規格

JIS Q 27001：2014（ISO/IEC 27001：2013）
情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－ 要求事項

ISO/IEC 27017:2015
Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud services

3. 用語及び定義

本文書で用いる主な用語及び定義は、JIS Q 27000 及び ISO/IEC 27017 による。

4. 要求事項

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。

4.1 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、クラウドサービス名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、リスクアセスメントの範囲にクラウドサービスカスタマとの関係を含めたリスク対応を検討することが必要である。

4.2 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。

・4.2.1 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。

・4.2.2 情報セキュリティリスク対応【 JIS Q 27001 の 6.1.3 】

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）4.2.2b)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[4.2.2 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、ISO/IEC 27017 の本文に実施の手引が示されている管理策、及び ISO/IEC 27017 の附属書 A 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 に記載されている実施の手引を参照し、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。

但し、サービスの種類によって、管理策が存在しない場合には、適用除外することができる。

4.3 内部監査【 JIS Q 27001 の 9.2 】

組織は、ISMS 内のクラウドサービスが次の状況にあるか否かに関する情報を提供するために、あらかじめ定めた間隔で内部監査を実施しなければならない。

a) 次の事項に適合している。

1) ISMS に関して、組織自体が規定した要求事項

2) 本文書(JIS Q 27001:2014 を含む)の要求事項

b) 有効に実施され、維持されている。

注記 1：内部監査の一部として、第三者による独立したレビュー（外部監査など）の結果を利用することができる。

注記 2：クラウドサービスプロバイダのコミットメント（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）が適正に実施されていることを確認することが望ましい。

参考 A

この参考 A では、ISMS クラウドセキュリティ認証に関する要求事項を、より深く理解するためのガイドを記載している。

A.1　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。

- 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 18.1.1 の実施の手引に記載された対策の適用が強く求められる。
- クラウドサービスに係るリスクについては、クラウドサービスカスタマ自らが最終責任を持つことになるが、クラウドサービスプロバイダの管理範囲に関しては、クラウドサービスプロバイダが責任を持つとともに、その責任が果たされていることをクラウドサービスカスタマに開示する必要がある。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 18.2.1 の実施の手引の適用が強く求められる。

なお、本文書の要求事項を実施するにあたって、「クラウドセキュリティガイドライン活用ガイドブック（経済産業省　商務情報政策局 2013 年度版）」が有効な情報を提供している。

A.2 クラウドセキュリティにおける適用範囲の考え方

JIS Q 27001 の「4.3 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」の要求事項では、「組織は、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」と規定している。

ISMS クラウドセキュリティ認証における適用範囲は、以下の通りである。

1）JIS Q 27001 の適用範囲に、ISO/IEC 27017 の適用範囲が含まれる場合

2）JIS Q 27001 の適用範囲と ISO/IEC 27017 の適用範囲が同一の場合

クラウドサービスを含めた ISMS の適用範囲の文書は、クラウドサービス名称を明記し、誤解を招く表現とならないことが必要である。

A.3 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.要求事項」の「4.2 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」の 4.2.2 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 に記載されている実施の手引を参照し、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。

2)「適用宣言書（SoA）」における 27017 適用の記載方法

- 本文書の「4.要求事項」の 4.2.2 d)に基づき、ISO/IEC 27017 本文の実施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（SoA）に、ISO/IEC 27017 本文の実施の手引についても含めることが望ましい。詳細については、「A.4 適用宣言書（SoA）」を参照。

A.4　適用宣言書（SoA）

ISMS クラウドセキュリティ認証では、4.2.2 d) に従って適用宣言書を作成する。次に適用宣言書の例を示す。

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○。

※2ISO/IEC 27017 に実施の手引が示されている管理策

管理策	管理策を含めた理由	27001[管理策]の実施の可否	27017[管理策※2]の実施の可否		除外理由
			カスタマ	プロバイダ	
ISO/IEC 27001:2013 附属書 A					
A.5.1 情報セキュリティのための方針群					
A.5.1.1 情報セキュリティのための方針群	・～のため	○	○	○	
A.5.1.2 情報セキュリティのための方針群のレビュー	・～のため	○	—	—	27017 には追加の実施の手引なし
A.6.1 内部組織					
A.6.1.1 情報セキュリティの役割及び責任	・～のため	○	○	○	
A.6.1.2 職務の分離	・～のため	○	–	–	27017 には追加の実施の手引なし
A.6.1.3 関係当局との連絡	・～のため	○	○	○	
A.6.1.4 専門組織との連絡	・～のため	○	–	–	27017 には追加の実施の手引なし
A.6.1.5 プロジェクトマネジメントにおける情報セキュリティ	・～のため	○	–	–	27017 には追加の実施の手引なし
A.6.2 モバイル機器及びテレワーキング					
A.6.2.1 モバイル機器の方針	・～のため	○	–	–	27017 には追加の実施の手引なし
A.6.2.2 テレワーキング	・～のため	○	–	–	27017 には追加の実施の手引なし

（中略）					
A.9.1 アクセス制御に対する業務上の要求事項					
A.9.1.1 アクセス制御方針	・～のため	○	–	–	27017 には追加の実施の手引なし
A.9.1.2 ネットワーク及びネットワークサービスへのアクセス	・～のため	○	○	–	クラウドサービスプロバイダに対しては、27017には追加の実施の手引なし
A.9.2 利用者のアクセスの管理					
A.9.2.1 利用者登録及び登録削除	・～のため	○	–	○	クラウドサービスカスタマに対しては、27017 には追加の実施の手引なし
A.9.2.2 利用者アクセスの提供	・～のため	○	–	○	クラウドサービスカスタマに対しては、27017 には追加の実施の手引なし
A.9.2.3 特権的アクセス権の管理	・～のため	○	×*	○	カスタマ： 27001 では…だが、27017 では xxx であるため。
A.9.2.4 利用者の秘密認証情報の管理	・～のため	○	×*	×*	カスタマ： 27001 では…だが、27017 では xxx であるため。 プロバイダ： 27001 では…だが、27017 では xxx であるため。
A.9.2.5 利用者アクセス権のレビュー	・～のため	○	–	–	27017 には追加の実施の手引なし
A.9.2.6 アクセス権の削除又は修正	・～のため	○	–	—	27017 には追加の実施の手引なし
（中略）					
ISO/IEC 27017:2015 附属書 A					
CLD.6.3 クラウドサービスカスタマとクラウドサービスプロバイダとの関係					
CLD.6.3.1 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	・～のため	—	○	○	

共有及び分担					
CLD.8.1 資産に対する責任					
CLD.8.1.5 クラウドサービスカスタマの資産の除去	・～のため	―	×＊	○	カスタマ： 27017 では xxx であるため。
（中略）					
その他の管理策					

＊ 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、管理策が存在しない場合がある。そのような場合のみ、管理策を適用除外することができる。

以上