ISMSクラウドセキュリティ認証の概要

一般財団法人 日本情報経済社会推進協会
参事　高取　敏夫

2016年4月26日

http://www.isms.jipdec.or.jp/

- ISO/IEC 27017:2015の概要
- ISO/IEC 27017:2015の構成
- 追加のクラウドサービス固有の実施の手引(1/5～5/5)
- 附属書A　クラウドサービス拡張管理策(1/6～6/6)

ISO/IEC 27017:2015の概要

Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services.

ISO/IEC 27002に基づくクラウドサービスのための情報セキュリティ管理策の実践の規範を提供する国際規格。この規格は、ISO/IEC 27002に規定する指針に追加し、これを補うものである。

・ISO/IEC 27002に定める関係する管理策への追加の実施の手引
・クラウドサービスに特に関係する追加の管理策及びその実施の手引

ISO/IEC 27017:2015の構成

0. 序文
1. 適用範囲
2. 引用規格
3. 定義及び略語
4. クラウド分野固有の概念
5. 情報セキュリティのための方針群
6. 情報セキュリティのための組織
7. 人的資源のセキュリティ
8. 資産の管理
9. アクセス制御
10. 暗号
11. 物理的及び環境的セキュリティ
12. 運用のセキュリティ
13. 通信のセキュリティ
14. システムの取得・開発及び保守
15. 供給者関係
16. 情報セキュリティインシデント管理
17. 事業継続マネジメントにおける
    情報セキュリティの側面
18. 順守

附属書A
　クラウドサービス拡張管理策集
附属書B
　クラウドコンピューティングの情報セキュリティ
　リスクに関する参考文献
参考文献

1. 適用範囲

・この規格は、クラウドサービス提供及び利用に適用できる情報セキュリティ管理策のための指針を示す。
・この指針の管理策及び実施の手引は、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双方に対して提供する。

2. 引用規格

・ISO/IEC 17788：情報技術－クラウドコンピューティング－概要及び用語
・ISO/IEC 17789：情報技術－クラウドコンピューティング－
参照アーキテクチャ
・ISO/IEC 27000：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－概要及び用語
・ISO/IEC 27002：2013　情報技術－セキュリティ技術－
情報セキュリティ管理策の実践のための規範

4. クラウド分野固有の概念(1/2)

4.1 概要

クラウドサービス固有の情報セキュリティの脅威及びリスクに対処するため、ISO/IEC 27002に基づきクラウドサービス固有の追加の実施の手引を提供し、また、追加の管理策を提供する。

4.2 クラウドサービスにおける供給者関係

クラウドサービスの提供及び利用は、クラウドサービスカスタマを調達者、クラウドサービスプロバイダを供給者とする一種の供給者関係である。

4.3 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

この供給者関係において、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がその情報セキュリティ要求事項を満たすために必要な情報及び技術支援を提供することが望ましい。

4. クラウド分野固有の概念(2/2)

4.4 クラウドサービスにおける情報セキュリティリスクの管理

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は、いずれも情報セキュリティリスクマネジメントプロセスを備えていることが望ましい。情報セキュリティマネジメントシステムにおけるリスクマネジメントを実施するための要求事項については、ISO/IEC 27001を参照することを勧める。

4.5 規格の構成

この規格は、ISO/IEC 27002の箇条5～箇条18を包含している。ISO/IEC 27002で規定する管理目的及び管理策が、追加の情報を必要とすることなく適用できる場合は、ISO/IEC 27002への参照だけを示す。

この規格の附属書A(規定)は、クラウドサービス拡張管理策集として、追加の管理目的、管理策及び実施の手引を記載している。

追加のクラウドサービス固有の実施の手引(1/5)

項番/管理策		カスタマ	プロバイダ
5.1.1	情報セキュリティのための方針群		
	ISO/IEC 27002の5.1.1に定める管理策並びに付随する実施の手引及び関連情報を適用する。次のクラウドサービス固有の実施の手引も適用する。	○	○
6.1.1	情報セキュリティの役割及び責任		
	ISO/IEC 27002の6.1.1に定める管理策並びに付随する実施の手引及び関連情報を適用する。次のクラウドサービス固有の実施の手引も適用する。	○	○
6.1.3	関係当局との連絡		
	ISO/IEC 27002の6.1.3に定める管理策並びに付随する実施の手引及び関連情報を適用する。次のクラウドサービス固有の実施の手引も適用する。	○	○
7.2.2	情報セキュリティの意識向上、教育及び訓練		
	ISO/IEC 27002の7.2.2に定める管理策並びに付随する実施の手引及び関連情報を適用する。次のクラウドサービス固有の実施の手引も適用する。	○	○
8.1.1	資産目録		
	ISO/IEC 27002の8.1.1に定める管理策並びに付随する実施の手引及び関連情報を適用する。次のクラウドサービス固有の実施の手引も適用する。	○	○
8.2.2	情報のラベル付け		
	ISO/IEC 27002の8.2.2に定める管理策並びに付随する実施の手引及び関連情報を適用する。次のクラウドサービス固有の実施の手引も適用する。	○	○

追加のクラウドサービス固有の実施の手引（2/5）

項番/管理策		カスタマ	プロバイダ
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		
	ISO/IEC 27002の9.1.2に定める管理策並びに付随する実施の手引及び関連情報を適用する。次のクラウドサービス固有の実施の手引も適用する。	○	－
9.2.1	利用者登録及び登録削除		
	ISO/IEC 27002の9.2.1に定める管理策並びに付随する実施の手引及び関連情報を適用する。次のクラウドサービス固有の実施の手引も適用する。	－	○
9.2.2	利用者アクセスの提供		
	ISO/IEC 27002の9.2.2に定める管理策並びに付随する実施の手引及び関連情報を適用する。次のクラウドサービス固有の実施の手引も適用する。	－	○
9.2.3	特権的アクセス権の管理		
	ISO/IEC 27002の9.2.3に定める管理策並びに付随する実施の手引及び関連情報を適用する。次のクラウドサービス固有の実施の手引も適用する。	○	○
9.2.4	利用者の秘密認証情報の管理		
	ISO/IEC 27002の9.2.4に定める管理策並びに付随する実施の手引及び関連情報を適用する。次のクラウドサービス固有の実施の手引も適用する。	○	○
9.4.1	情報へのアクセス制限		
	ISO/IEC 27002の9.4.1に定める管理策並びに付随する実施の手引及び関連情報を適用する。次のクラウドサービス固有の実施の手引も適用する。	○	○
9.4.4	特権的なユーティリティプログラムの使用		
	ISO/IEC 27002の9.4.4に定める管理策並びに付随する実施の手引及び関連情報を適用する。次のクラウドサービス固有の実施の手引も適用する。	○	○

追加のクラウドサービス固有の実施の手引（3/5）

項番/管理策		カスタマ	プロバイダ
10.1.1	暗号による管理策の利用方針		
	ISO/IEC 27002の10.1.1に定める管理策並びに付随する実施の手引及び関連情報を適用する。次のクラウドサービス固有の実施の手引も適用する。	○	○
10.1.2	鍵管理		
	ISO/IEC 27002の10.1.2に定める管理策並びに付随する実施の手引及び関連情報を適用する。次のクラウドサービス固有の実施の手引も適用する。	○	–
11.2.7	装置のセキュリティを保った処分又は再利用		
	ISO/IEC 27002の11.2.7に定める管理策並びに付随する実施の手引及び関連情報を適用する。次のクラウドサービス固有の実施の手引も適用する。	○	○
12.1.2	変更管理		
	ISO/IEC 27002の12.1.2に定める管理策並びに付随する実施の手引及び関連情報を適用する。次のクラウドサービス固有の実施の手引も適用する。	○	○
12.1.3	容量・能力の管理		
	ISO/IEC 27002の12.1.3に定める管理策並びに付随する実施の手引及び関連情報を適用する。次のクラウドサービス固有の実施の手引も適用する。	○	○
12.3.1	情報のバックアップ		
	ISO/IEC 27002の12.3.1に定める管理策並びに付随する実施の手引及び関連情報を適用する。次のクラウドサービス固有の実施の手引も適用する。	○	○
12.4.1	イベントログ取得		
	ISO/IEC 27002の12.4.1に定める管理策並びに付随する実施の手引及び関連情報を適用する。次のクラウドサービス固有の実施の手引も適用する。	○	○
12.4.3	実務管理者及び運用担当者の作業ログ		
	ISO/IEC 27002の12.4.3に定める管理策並びに付随する実施の手引及び関連情報を適用する。次のクラウドサービス固有の実施の手引も適用する。	○	–
12.4.4	クロックの同期		
	ISO/IEC 27002の12.4.4に定める管理策並びに付随する実施の手引及び関連情報を適用する。次のクラウドサービス固有の実施の手引も適用する。	○	○

追加のクラウドサービス固有の実施の手引（4/5）

項番/管理策		カスタマ	プロバイダ
12.6.1	技術的ぜい弱性の管理		
	ISO/IEC 27002の12.6.1に定める管理策並びに付随する実施の手引及び関連情報を適用する。次のクラウドサービス固有の実施の手引も適用する。	○	○
13.1.3	ネットワークの分離		
	ISO/IEC 27002の13.1.3に定める管理策並びに付随する実施の手引及び関連情報を適用する。次のクラウドサービス固有の実施の手引も適用する。	○	○
14.1.1	情報セキュリティ要求事項の分析及び仕様化		
	ISO/IEC 27002の14.1.1に定める管理策並びに付随する実施の手引及び関連情報を適用する。次のクラウドサービス固有の実施の手引も適用する。	○	○
14.2.1	セキュリティに配慮した開発のための方針		
	ISO/IEC 27002の14.2.1に定める管理策並びに付随する実施の手引及び関連情報を適用する。次のクラウドサービス固有の実施の手引も適用する。	○	○
15.1.1	供給者関係のための情報セキュリティの方針		
	ISO/IEC 27002の15.1.1に定める管理策並びに付随する実施の手引及び関連情報を適用する。次のクラウドサービス固有の実施の手引も適用する。	○	－
15.1.2	供給者との合意におけるセキュリティの取扱い		
	ISO/IEC 27002の15.1.2に定める管理策並びに付随する実施の手引及び関連情報を適用する。次のクラウドサービス固有の実施の手引も適用する。	○	○
15.1.3	ICTサプライチェーン		
	ISO/IEC 27002の15.1.3に定める管理策並びに付随する実施の手引及び関連情報を適用する。次のクラウドサービス固有の実施の手引も適用する。	－	○

追加のクラウドサービス固有の実施の手引（5/5）

項番/管理策		カスタマ	プロバイダ
16.1.1	責任及び手順		
	ISO/IEC 27002の16.1.1に定める管理策並びに付随する実施の手引及び関連情報を適用する。次のクラウドサービス固有の実施の手引も適用する。	○	○
16.1.2	情報セキュリティ事象の報告		
	ISO/IEC 27002の16.1.2に定める管理策並びに付随する実施の手引及び関連情報を適用する。次のクラウドサービス固有の実施の手引も適用する。	○	○
16.1.7	証拠の収集		
	ISO/IEC 27002の16.1.7に定める管理策並びに付随する実施の手引及び関連情報を適用する。次のクラウドサービス固有の実施の手引も適用する。	○	
18.1.1	適用法令及び契約上の要求事項の特定		
	ISO/IEC 27002の18.1.1に定める管理策並びに付随する実施の手引及び関連情報を適用する。次のクラウドサービス固有の実施の手引も適用する。	○	○
18.1.2	知的財産権		
	ISO/IEC 27002の18.1.2に定める管理策並びに付随する実施の手引及び関連情報を適用する。次のクラウドサービス固有の実施の手引も適用する。	○	○
18.1.3	記録の保護		
	ISO/IEC 27002の18.1.3に定める管理策並びに付随する実施の手引及び関連情報を適用する。次のクラウドサービス固有の実施の手引も適用する。	○	○
18.1.5	暗号化機能に対する規制		
	ISO/IEC 27002の18.1.5に定める管理策並びに付随する実施の手引及び関連情報を適用する。次のクラウドサービス固有の実施の手引も適用する。	○	○
18.2.1	情報セキュリティの独立したレビュー		
	ISO/IEC 27002の18.2.1に定める管理策並びに付随する実施の手引及び関連情報を適用する。次のクラウドサービス固有の実施の手引も適用する。	○	○

附属書A　クラウドサービス拡張管理策（1/6）

CLD 6.3/6.3.1

項番	ISO/IEC 27001 管理策	項番	ISO/IEC 27017 管理策	項番	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 管理策
A.6.2	**A.6.2　モバイル機器及びテレワーキング**	6.2	**6.2　モバイル機器及びテレワーキング**	11.7	**11.7 モバイルコンピューティング及びテレワーキング**
A.6.2.1	**A.6.2.1　モバイル機器の方針**	6.2.1	**6.2.1　モバイル機器の方針**	11.7.1	**11.7.1 モバイルのコンピューティング及び通信**
A.6.2.2	**A.6.2.2　テレワーキング**	6.2.2	**6.2.2　テレワーキング**	11.7.2	**11.7.2 テレワーキング**
		CLD.6.3	**クラウドサービスカスタマとクラウドプロバイダとの関係** 目的 情報セキュリティマネジメントに関して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間で共有し分担する役割及び責任について、両者間の関係を明確にするため。		
		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共有及び分担** 管理策 クラウドサービスの利用に関して共有し分担する情報セキュリティの役割を遂行する責任は、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のそれぞれにおいて特定の関係者に割当て、文書化し、伝達し、実施することが望ましい。		

附属書A　クラウドサービス拡張管理策

CLD 8.1/8.1.5　（2/6）

項番	ISO/IEC 27001 管理策	項番	ISO/IEC 27017 管理策	項番	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 管理策
A.8.1	A.8.1　資産に対する責任	8.1	8.1　資産に対する責任	7.1	7.1 資産に対する責任
A.8.1.1	A.8.1.1　資産目録	8.1.1	8.1.1　資産目録	7.1.1	7.1.1 資産目録
A.8.1.2	A.8.1.2　資産の管理責任[a)]	8.1.2	8.1.2　資産の管理責任	7.1.2	7.1.2 資産の管理責任者
A.8.1.3	A.8.1.3　資産利用の許容範囲	8.1.3	8.1.3　資産利用の許容範囲	7.1.3	7.1.3 資産利用の許容範囲
A.8.1.4	A.8.1.4　資産の返却	8.1.4	8.1.4　資産の返却	8.3.2	8.3.2 資産の返却
		CLD.8.1	資産に対する責任 ISO/IEC 27002の8.1に定める管理目的を適用する。		
		CLD.8.1.5	クラウドサービスカスタマの資産の除去 管理策 クラウドサービスプロバイダの施設にあるクラウドサービスカスタマの資産は、クラウドサービスの合意の終了時に、時期を失せずに除去又は必要な場合には返却されることが望ましい。		

注：a）6.1.2及び8.1.3では、情報セキュリティのリスクを運用管理することについて、責任及び権限を持つ人又は主体をリスク所有者としている。情報セキュリティにおいて多くの場合、資産の管理責任を負う者は、リスク所有者でもある。

附属書A　クラウドサービス拡張管理策（3/6）

CLD 9.5
/9.5.1
/9.5.2

項番	ISO/IEC 27001 管理策	項番	ISO/IEC 27017 管理策	項番	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 管理策
A.9.4	A.9.4 システム及びアプリケーションのアクセス制御	9.4	9.4 システム及びアプリケーションのアクセス制御	11.5	11.5 オペレーティングシステムのアクセス制御
				11.6	11.6 業務用ソフトウェア及び情報のアクセス制御
A.9.4.1	A.9.4.1 情報へのアクセス制限	9.4.1	9.4.1 情報へのアクセス制限	11.6.1	11.6.1 情報へのアクセス制限
				11.6.2	11.6.2 取扱いに慎重を要するシステムの隔離
A.9.4.2	A.9.4.2 セキュリティに配慮したログオン手順	9.4.2	9.4.2 セキュリティに配慮したログオン手順	11.5.1	11.5.1 セキュリティに配慮したログオン手順
				11.5.6	11.5.6 接続時間の制限
A.9.4.3	A.9.4.3 パスワード管理システム	9.4.3	9.4.3 パスワード管理システム	11.5.3	11.5.3 パスワード管理システム
A.9.4.4	A.9.4.4 特権的なユーティリティプログラムの使用	9.4.4	9.4.4 特権的なユーティリティプログラムの使用	11.5.4	11.5.4 システムユーティリティの使用
A.9.4.5	A.9.4.5 プログラムソースコードへのアクセス制御	9.4.5	9.4.5 プログラムソースコードへのアクセス制御	12.4.3	12.4.3 プログラムソースコードへのアクセス制御
		CLD.9.5	共有する仮想環境におけるクラウドサービスカスタマデータのアクセス制御 目的 クラウドコンピューティングにおける共有する仮想環境利用時の情報セキュリティリスクを低減するため。		
		CLD. 9.5.1	仮想コンピューティング環境における分離 管理策 クラウドサービス上で稼働するクラウドサービスカスタマの仮想環境は、他のクラウドサービスカスタマ及び認可されていない者から保護することが望ましい。		
		CLD. 9.5.2	仮想マシンの要塞化 管理策 クラウドコンピューティング環境の仮想マシンは、事業上のニーズを満たすために要塞化することが望ましい。		

附属書A　クラウドサービス拡張管理策（4/6）

CLD 12.1/12.1.5

項番	ISO/IEC 27001 管理策	項番	ISO/IEC 27017 管理策	項番	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 管理策
A.12.1	**A.12.1　運用の手順及び責任**	12.1	**12.1　運用の手順及び責任**	10.1	**10.1 運用の手順及び責任**
A.12.1.1	**A.12.1.1　操作手順書**	12.1.1	**12.1.1　操作手順書**	10.1.1	**10.1.1 操作手順書**
A.12.1.2	**A.12.1.2　変更管理**	12.1.2	**12.1.2　変更管理**	10.1.2	**10.1.2 変更管理**
A.12.1.3	**A.12.1.3　容量・能力の管理**	12.1.3	**12.1.3　容量・能力の管理**	10.3.1	**10.3.1 容量・能力の管理**
A.12.1.4	**A.12.1.4　開発環境，試験環境及び運用環境の分離**	12.1.4	**12.1.4　開発環境，試験環境及び運用環境の分離**	10.1.4	**10.1.4 開発施設，試験施設及び運用施設の分離**
		CLD.12.1	**運用の手順及び責任** ISO/IEC 27002の12.1に定める管理目的を適用する。		
		CLD.12.1.5	**実務管理者の運用のセキュリティ** 管理策 クラウドコンピューティング環境の管理操作のための手順は、これを定義し、文書化し、監視することが望ましい。		

附属書A　クラウドサービス拡張管理策

CLD 12.4/12.4.5　（5/6）

項番	ISO/IEC 27001 管理策	項番	ISO/IEC 27017 管理策	項番	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 管理策
A.12.4	**A.12.4　ログ取得及び監視**	12.4	**12.4　ログ取得及び監視**	10.1	**10.10 監視**
A.12.4.1	**A.12.4.1　イベントログ取得**	12.4.1	**12.4.1　イベントログ取得**	10.10.1	**10.10.1 監査ログ取得**
A.12.4.2	**A.12.4.2　ログ情報の保護**	12.4.2	**12.4.2　ログ情報の保護**	10.10.3	**10.10.3 ログ情報の保護**
A.12.4.3	**A.12.4.3　実務管理者及び運用担当者の作業ログ**	12.4.3	**12.4.3　実務管理者及び運用担当者の作業ログ**	10.10.4	**10.10.4 実務管理者及び運用担当者の作業ログ**
A.12.4.4	**A.12.4.4　クロックの同期**	12.4.4	**12.4.4　クロックの同期**	10.10.6	**10.10.6 クロックの同期**
		CLD.12.4	**ログ取得及び監視** ISO/IEC 27002の12.4に定める管理目的を適用する。		
		CLD.12.4.5	**クラウドサービスの監視** 管理策 クラウドサービスカスタマは、クラウドサービスカスタマが利用するクラウドサービスの操作の特定の側面を監視する能力をもつことが望ましい。		

附属書A　クラウドサービス拡張管理策（6/6）

CLD 13.1/13.1.4

項番	ISO/IEC 27001 管理策	項番	ISO/IEC 27017 管理策	項番	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 管理策
A.13.1	**A.13.1　ネットワークセキュリティ管理**	13.1	**13.1　ネットワークセキュリティ管理**	10.6	**10.6 ネットワークセキュリティ管理**
A.13.1.1	**A.13.1.1　ネットワーク管理策**	13.1.1	**13.1.1　ネットワーク管理策**	10.6.1	**10.6.1 ネットワーク管理策**
A.13.1.2	**A.13.1.2　ネットワークサービスのセキュリティ**	13.1.2	**13.1.2　ネットワークサービスのセキュリティ**	10.6.2	**10.6.2 ネットワークサービスのセキュリティ**
A.13.1.3	**A.13.1.3　ネットワークの分離**	13.1.3	**13.1.3　ネットワークの分離**	11.4.5	**11.4.5 ネットワークの領域分割**
		CLD.13.1	**ネットワークセキュリティ管理** ISO/IEC 27002の13.1に定める管理目的を適用する。		
		CLD. 13.1.4	**仮想及び物理ネットワークのセキュリティ管理の整合** 管理策 仮想ネットワークを設定する際には、クラウドサービスプロバイダのネットワークセキュリティ方針に基づいて、仮想ネットワークと物理ネットワークとの間の設定の整合性を検証することが望ましい。		

ISMSクラウドセキュリティ認証の概要

- ISMSクラウドセキュリティ認証の背景
- ISMSクラウドセキュリティ認証の対象者
- ISMSクラウドセキュリティ認証の枠組み
- ISMSクラウドセキュリティ認証の考え方
- ISMSクラウドセキュリティ認証の適用範囲
- ISMSクラウドセキュリティ認証に関する基本的要件（1/4～4/4）
- 今後のスケジュール

ISMSクラウドセキュリティ認証の背景

クラウドサービスの本格的な普及に伴い、クラウドサービスに求められるセキュリティ要求事項を明確化することの重要性を認識。

クラウドサービス向けの国際規格ISO/IEC 27017（Code of practice for information security controls based on ISO/IEC 27002 for cloud services）が2015年12月15日に発行された。

このような状況を踏まえ、ISMSに基づき、クラウドサービスの信頼性を保証するISMSクラウドセキュリティ認証を開始する予定。

ISMSクラウドセキュリティ認証の対象者

ISMSクラウドセキュリティ認証は、ISO/IEC 27017のガイドラインに沿った、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両方を対象とする。

※ クラウドサービスプロバイダ：

クラウドサービスを利用可能にする組織 （クラウドサービスを提供する組織）。ただし、クラウドサービスプロバイダも、提供するサービスの様態によっては、クラウドサービスカスタマとなる場合がある。

※ クラウドサービスカスタマ：

クラウドサービスを利用する目的のための取引関係がある組織（クラウドサービスを利用する組織）

ISMSクラウドセキュリティ認証の枠組み

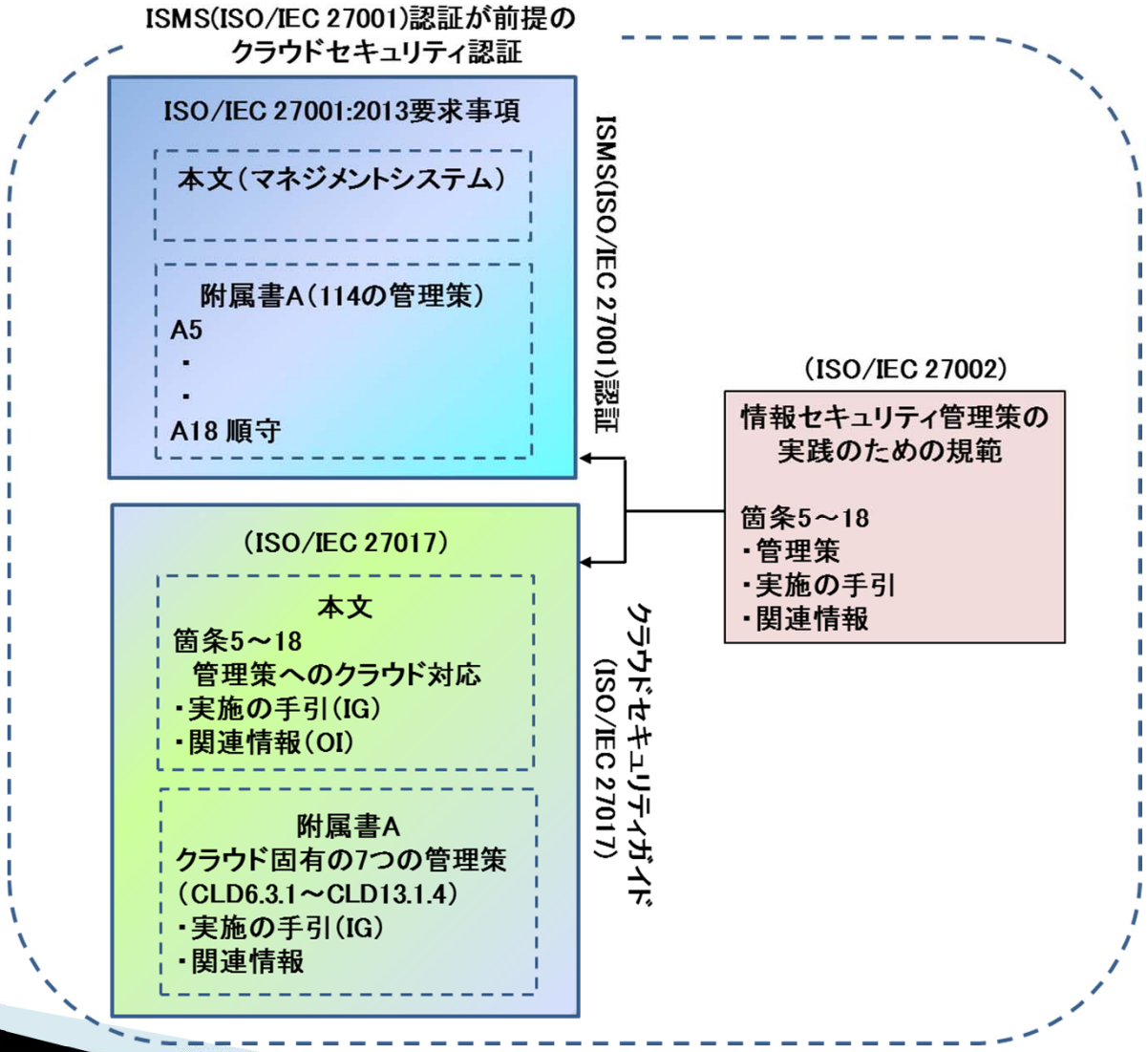
ISMSクラウドセキュリティ認証

ISMS（ISO/IEC 27001）認証を前提として、ISO/IEC 27017のガイドラインに沿ったクラウドサービスの情報セキュリティ管理を満たしている組織を認証する仕組みとする。

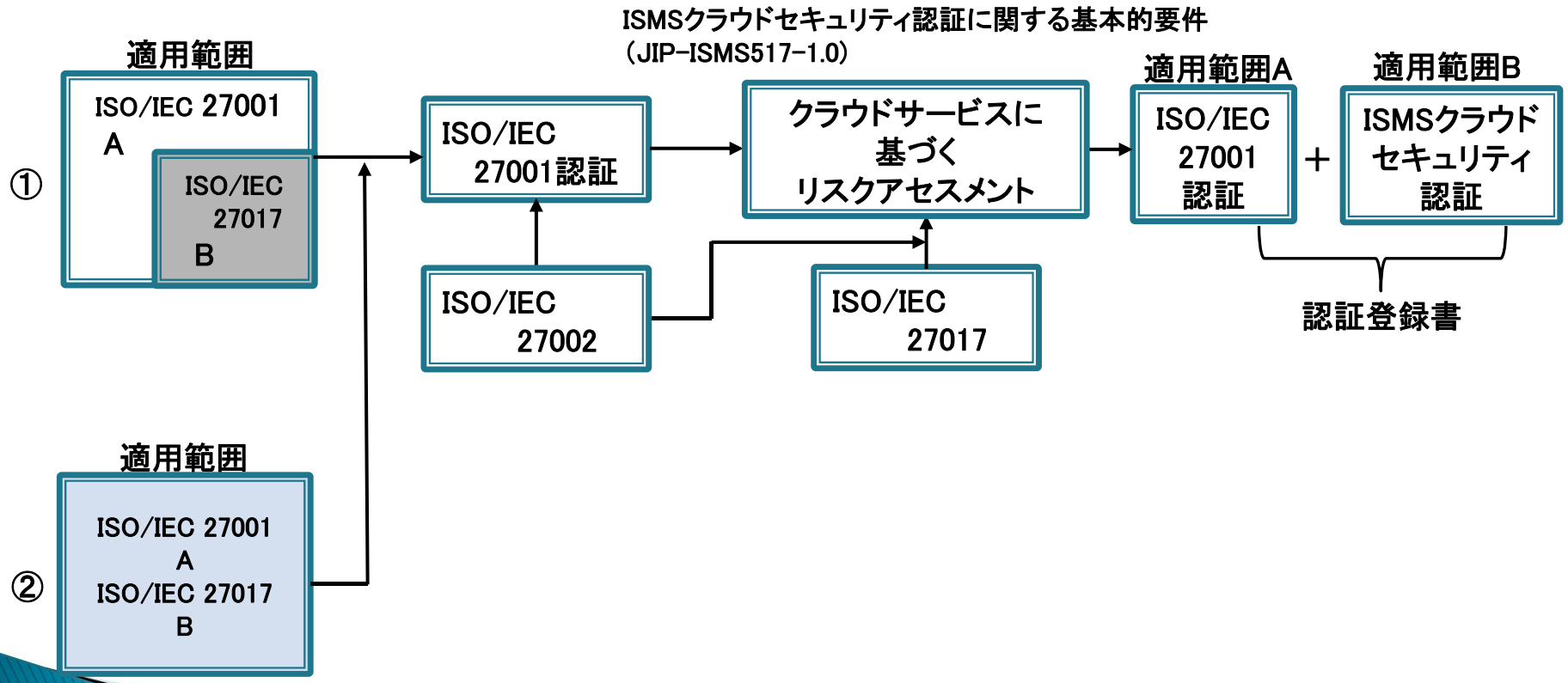
※ここでは、ISOの枠組みの中で、ISMS（ISO/IEC 27001）認証を前提として、 特定の分野固有の規格に準拠していることをいう。

ISMSクラウドセキュリティ認証の考え方

≪制度の枠組み≫



ISMSクラウドセキュリティ認証の適用範囲



ISMSクラウドセキュリティ認証に関する基本的要件（文書番号:JIP-ISMS517-1.0）（1/4）

4. 基本的要件

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/IEC27017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。

ISMSクラウドセキュリティ認証に関する基本的要件（文書番号:JIP-ISMS517-1.0）（2/4）

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

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

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。

ISMSクラウドセキュリティ認証に関する基本的要件(文書番号:JIP-ISMS517-1.0)(3/4)

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本文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。

ISMSクラウドセキュリティ認証に関する基本的要件(文書番号:JIP-ISMS517-1.0)(4/4)

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) この規格の要求事項
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。

スケジュール

■ 説明会の実施

2016年4月21日　ISMS認証機関への説明会

4月26日　認証取得に関心を有する組織への説明会

■ ISMSクラウドセキュリティ認証に関する広報

JIPDECホームページ等を通じて、広報を実施

■ ISMSクラウドセキュリティ認証の開始

ISMSクラウドセキュリティ認証の要件、ガイドライン等を整備し、2016年夏を目途に適合性評価を開始

ご清聴ありがとうございました。

【問い合わせ先】

一般財団法人 日本情報経済社会推進協会
情報マネジメントシステム認定センター
TEL: 03-5860-7570
FAX: 03-5573-0564
Web: http://www.isms.jipdec.or.jp/