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
情報マネジメントシステム認定センター
星　昌宏

2016年6月28日
http://www.isms.jipdec.or.jp/

説明内容

- ISO/IEC 27017:2015
- ISMSクラウドセキュリティ認証

ISMSクラウドセキュリティ認証とは

JIS Q 27001(ISO/IEC 27001)
及び
ISO/IEC 27017※
に基づく
クラウドサービスを扱う組織のISMS認証

※ISO/IEC 27017
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**

＃認証基準ではないことに注意

【ISO/IEC 27017:2015】

- ISO/IEC 27017：2015発行の経緯
- 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 (1/4～4/4)
- 附属書A　クラウドサービス追加管理策 (1/2～2/2)

ISO/IEC 27017:2015発行の経緯

クラウドサービス
利用の普及･拡大

サーバ内のデータ消失、意図しない
者とのデータ共有等の事例

クラウドサービス利用に関する
情報セキュリティ上の不安

2011年4月　経済産業省情報セキュリティ政策室
「クラウドサービス利用のための情報セキュリティガイドライン」
ISO/IEC 27002 (ISMS実践のための規範) と整合

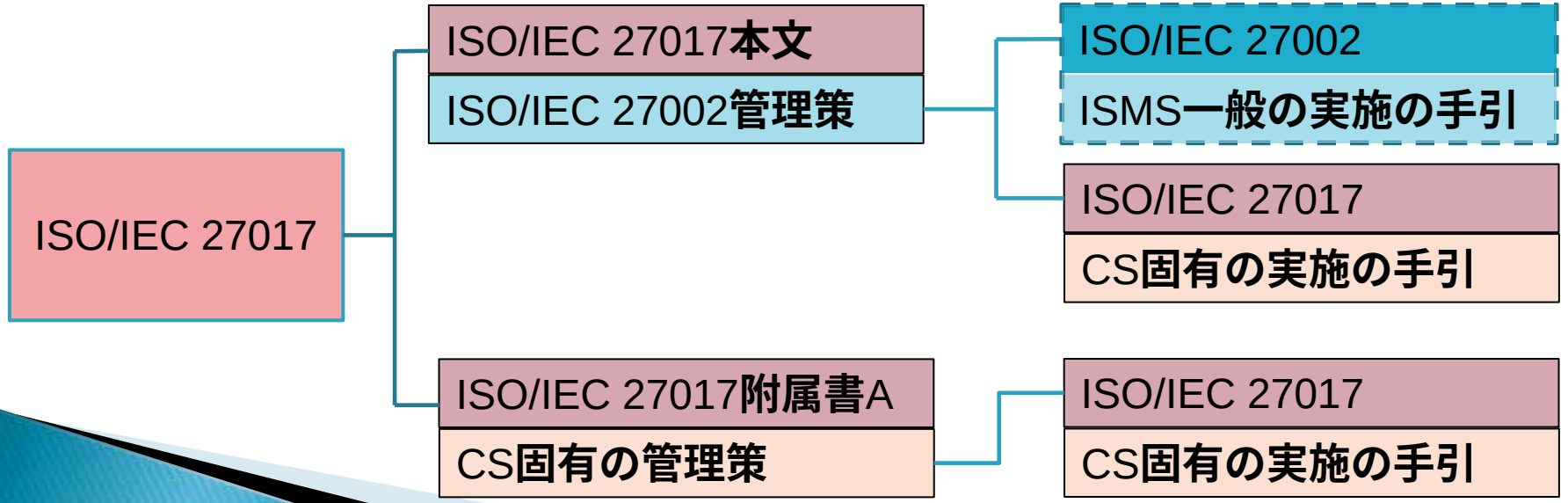
ISO/IECへ提案
国際標準化が決定

2015年12月15日
ISO/IEC 27017発行

ISO/IEC 27017:2015の概要

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

ISO/IEC 27002規定の指針に追加し、これを補うもの



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の管理策集
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
　リスクに関する参照文献
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。

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。

管理策に関連する追加のクラウドサービス固有の実施の手引を必要とする場合には、「クラウドサービスのための実施の手引き」に示す。

追加の実施の手引の例 (18.1.1)

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。

クラウドサービスカスタマ

クラウドサービスカスタマは，関連する法令及び規制には，クラウドサービスカスタマの法域のものに加え，クラウドサービスプロバイダの法域のものもあり得ることを考慮することが望ましい。

クラウドサービスカスタマは，その事業のために必要な，関係する規制及び標準に対するクラウドサービスプロバイダの順守の証拠を要求することが望ましい。第三者の監査人が発行する証明書を，この証拠とする場合がある。

(英和対訳版　ISO/IEC 27017:2015から引用)

追加の実施の手引の例 (18.1.1)

18.1.1 適用法令及び契約上の要求事項の特定

クラウドサービスプロバイダ

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クラウドサービスに適用される法域を知らせることが望ましい。

クラウドサービスプロバイダは，関係する法的要求事項 (例えば，PII 保護のための暗号化) を特定することが望ましい。この情報は，また，求められたときに，クラウドサービスカスタマに提供することが望ましい。

クラウドサービスプロバイダは，適用法令及び契約上の要求事項について，現在の順守の証拠をクラウドサービスカスタマに提供することが望ましい。

(英和対訳版　ISO/IEC 27017:2015から引用)

追加のクラウドサービス固有の実施の手引(1/4)

	○印：実施の手引き有り	
項番/管理策	カスタマ	プロバイダ
5. 情報セキュリティのための方針群 (Information security policies)		
5.1.1 情報セキュリティのための方針群(Policies for information security)	○	○
6. 情報セキュリティのための組織(Organaization of information security)		
6.1.1 情報セキュリティの役割及び責任 (Information security roles and responsibilities)	○	○
6.1.3 関係当局との連絡(Contact with authorities)	○	○
7. 人的資源のセキュリティ(Human resource security)		
7.2.2 情報セキュリティの意識向上、教育及び訓練 (Information security awareness, education and training)	○	○
8. 資産の管理 (Asset management)		
8.1.1 資産目録(Inventory of assets)	○	○
8.2.2 情報のラベル付け(Labelling of information)	○	○

追加のクラウドサービス固有の実施の手引 (2/4)

項番/管理策	カスタマ	プロバイダ
9. アクセス制御 (Access control)		
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** (Access to networks and network services)	○	–
9.2.1 **利用者登録及び登録削除**(User registration and deregistration)	–	○
9.2.2 **利用者アクセスの提供**(User access provisioning)	–	○
9.2.3 **特権的アクセス権の管理**(Management of privileged access right)	○	○
9.2.4 **利用者の秘密認証情報の管理** (management of secret authentication information of users)	○	○
9.4.1 **情報へのアクセス制限**(Information access restriction)	○	○
9.4.4 **特権的なユーティリティプログラムの使用**(Use of privileged utility programs)	○	○
10. 暗号 (Cryptographic controls)		
10.1.1 **暗号による管理策の利用方針**(Policy on the use of cryptographic controls)	○	○
10.1.2 **鍵管理**(Key management)	○	–
11. 物理的及び環境的セキュリティ (Physical and environmental security)		
11.2.7 **装置のセキュリティを保った処分又は再利用** (Secure disposal or reuse of equipment)	○	○

追加のクラウドサービス固有の実施の手引 (3/4)

項番/管理策	カスタマ	プロバイダ
12. 運用のセキュリティ (Operations security)		
12.1.2 **変更管理**(Change management)	○	○
12.1.3 **容量・能力の管理**(Capacity management)	○	○
12.3.1 **情報のバックアップ**(Information backup)	○	○
12.4.1 **イベントログ取得**(Event logging)	○	○
12.4.3 **実務管理者及び運用担当者の作業ログ**(Administrator and operator logs)	○	–
12.4.4 **クロックの同期**(Clock synchronization)	○	○
12.6.1 **技術的ぜい弱性の管理**(Management of technical vulnerabilities)	○	○
13. 通信のセキュリティ (Communications security)		
13.1.3 **ネットワークの分離**(Segregation in networks)	○	○
14. システムの取得、開発及び保守		
14.1.1 **情報セキュリティ要求事項の分析及び仕様化** (Information security requirements analysis and specification)	○	○
14.2.1 **セキュリティに配慮した開発のための方針**(Secure development policy)	○	○

追加のクラウドサービス固有の実施の手引 (4/4)

項番/管理策	カスタマ	プロバイダ
15. 供給者関係 (Supplier relationships)		
15.1.1 **供給者関係のための情報セキュリティの方針** (Information security policy for supplier relationships)	○	–
15.1.2 **供給者との合意におけるセキュリティの取扱い** (Addressing security within supplier agreements)	○	○
15.1.3 ICT**サプライチェーン** (Information and communication technology supply chain)	–	○
16. 情報セキュリティインシデント管理 (Information security incident management)		
16.1.1 **責任及び手順**(Responsibilities and procedures)	○	○
16.1.2 **情報セキュリティ事象の報告**(Reporting information security events)	○	○
16.1.7 **証拠の収集**(Collection of evidence)	○	
18. 順守 (Compliance)		
18.1.1 **適用法令及び契約上の要求事項の特定** (Identification of applicable legislation and contractual requirements)	○	○
18.1.2 **知的財産権**(Intellectual property rights)	○	○
18.1.3 **記録の保護**(Protection of records)	○	○
18.1.5 **暗号化機能に対する規制**(Regulation of cryptographic controls)	○	○
18.2.1 **情報セキュリティの独立したレビュー** (Independent review of information security)	○	○

附属書A　クラウドサービス追加管理策(1/2)

追加の管理目的	
	追加の管理策
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共有及び分担
	CLD.8.1.5　クラウドサービスカスタマの資産の除去
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	
	CLD.9.5.1　仮想コンピューティング環境における分離
	CLD.9.5.2　仮想マシンの要塞化

附属書A　クラウドサービス追加管理策(2/2)

追加の管理目的	
	追加の管理策
	CLD.12.1.5　実務管理者の運用のセキュリティ
	CLD.12.4.5　クラウドサービスの監視
	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

【ISMSクラウドセキュリティ認証】

- 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認証基準
- ISMSクラウドセキュリティ認証の適用範囲
- JIP-ISMS517-1.0の概要
- ISMSクラウドセキュリティ認証の認証文書（登録証）

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組織

※クラウドサービスの分類(IaaS, PaaS, SaaS)は問わない

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認証基準

JIP-ISMS517-1.0

ISO/IEC27017:2015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

実践の規範であるISO/IEC 27017を要求事項として扱うための基準

JIP-ISMS517-1.0 の概要

JIS Q 27001:2014 に対する追加の要求事項

1.概要

2.引用規格

3.用語及び定義

4.要求事項

参考A

ISMSクラウドセキュリティ認証に関する要求事項(文書番号:JIP-ISMS517-1.0) (1/4)

4. 要求事項

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に対応】

・クラウドサービスを含めたISMSの適用範囲を定める

・適用範囲は、文書化した情報として利用可能な状態にする

・別のクラウドサービスを利用してサービスを提供しているプロバイダは、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する

ISMSクラウドセキュリティ認証に関する要求事項(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) に対応】

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。

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要求事項(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】
情報セキュリティリスク対応のプロセスを定め、適用する。

a) 適切な情報セキュリティリスク対応の選択肢を選定
b) 選定した選択肢の実施に必要な管理策を決定
c) 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
d) 適用宣言書を作成

ISMSクラウドセキュリティ認証に関する要求事項(文書番号:JIP-ISMS517-1.0) (4/4)

4.3内部監査【JIS Q 27001の9.2】

クラウドサービスが次の状況にあるか否かを確認する

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。

※クラウドサービスプロバイダの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。

ISMSクラウドセキュリティ認証の認証文書（登録証）

- 認証規格はJIP-ISMS517-1.0
  ISO/IEC 27017:2015を記載する場合は、ガイドラインであることを明記する

- クラウドサービスカスタマ、クラウドサービスプロバイダのどちら、又は両方の立場での認証かを明記する

- 適用範囲の記述の中で、クラウドサービスが特定でき、誤解を招かない表現で明確に記載する
  ※ISMSクラウドセキュリティ認証は組織に対するマネジメントシステム認証であり、製品又はサービスそのものに対する認証ではない。

- 基となるISMS(JIS Q 27001)認証への識別を明記する
  認証の有効期限は、基となるISMS認証を越えない

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