

日本 ISMS ユーザグループ／日本ネットワークセキュリティ協会 主催
情報セキュリティマネジメント・セミナー2025

ISO/IEC 27017 ポイント解説

2025年12月5日

NTTテクノクロス株式会社

土屋 直子

ISO/IEC JTC1 SC27 WG1国内委員会委員

目次

1. ISO/IEC 27017 ポイント解説

1-(1) ISO/IEC 27002:2013 と ISO/IEC 27017:2015 の関係

1-(2) ISO/IEC 27002:2022 と ISO/IEC 27017:20XX の関係

2. ISO/IEC 27017 改訂の方向性

1. ISO/IEC 27017 ポイント解説

1-(1) ISO/IEC 27002:2013 と ISO/IEC 27017:2015 の関係

1-(2) ISO/IEC 27002:2022 と ISO/IEC 27017:20XX の関係

2. ISO/IEC 27017 改訂の方向性

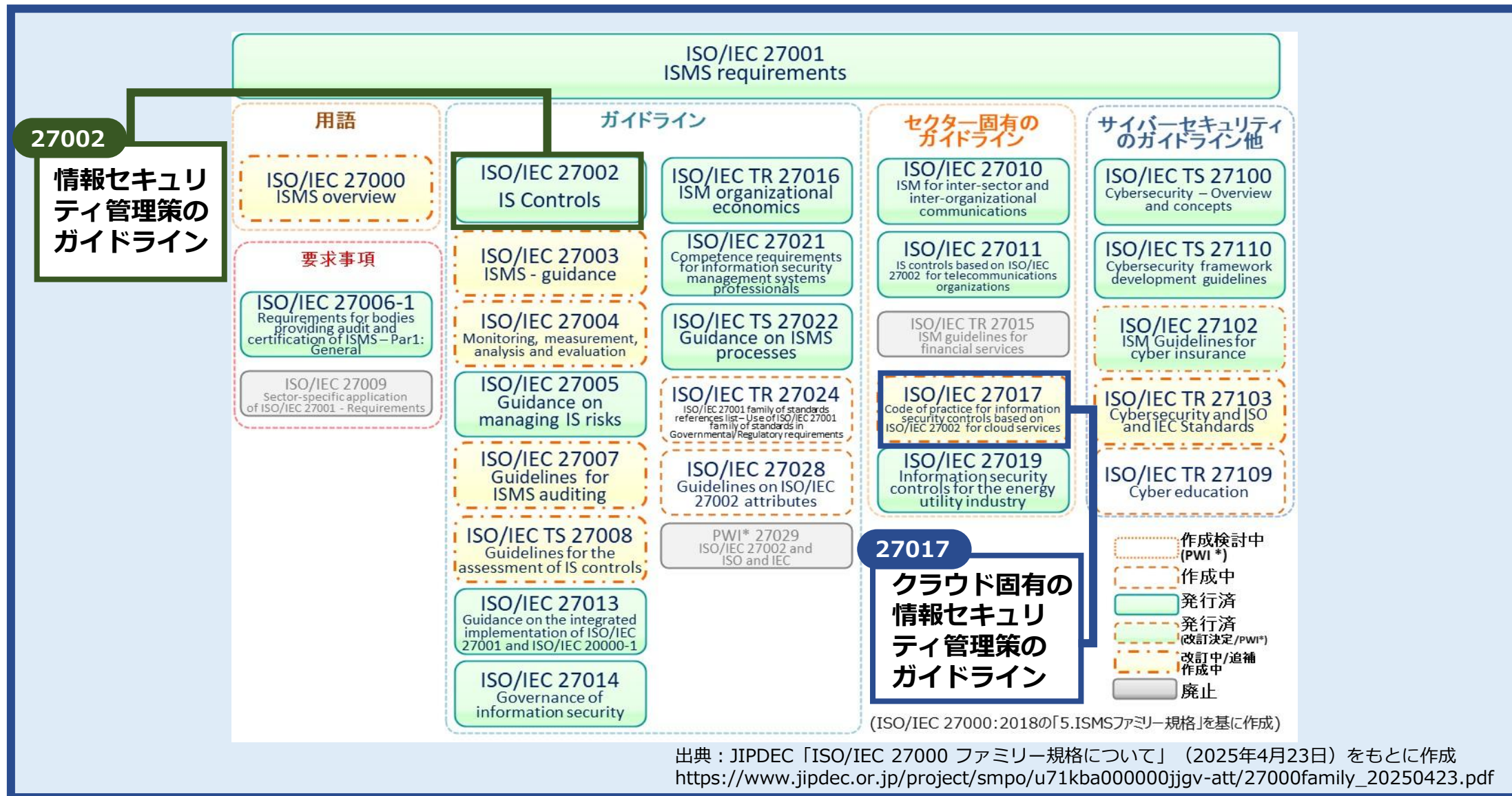
はじめに

ISO/IEC 27002:2022 では「5.23 クラウドサービスの利用における情報セキュリティ」の管理策をはじめとして、その他の管理策の手引でも「クラウドサービス」について数多く言及されています。

現在、ISO/IEC 27017 の改訂が進められていますが、ISO/IEC 27002:2022 におけるクラウドサービス関連の情報セキュリティ管理策や手引と、ISO/IEC 27017におけるクラウド固有の管理策や手引の関係はどのようになるのでしょうか？

本講演では、この2つの規格の位置づけや関係を整理し、ISO/IEC 27017の理解を深めるためのトピックを提供します。

ISO/IEC 27002 と ISO/IEC 27017 の位置づけ



「ISO/IEC 27017 ポイント解説」 NTTテクノクロス 土屋直子

ISO/IEC 27017 規格の概要

- ISO/IEC 27017:2015
 - Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud services
 - 情報技術－セキュリティ技術－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
 - 2015/12/15発行
- ISO/IEC 27017:2015は、**クラウドサービスプロバイダ（CSP）とクラウドサービスカスタマ（CSC）の双方**に情報セキュリティ管理策及び実施の手引を提供するガイドライン。
- ISO/IEC 27002に定義された管理策に**クラウドサービス固有**の管理策を追加。

ISO/IEC 27002:2013 における「クラウドサービス」の言及

ISO/IEC 27002:2013では、「クラウドサービス」の言及はほぼなかった

ISO/IEC 27002:2013
15.1.3 ICT サプライチェーン
関連情報

ここ一箇所のみ

「…ICTサプライチェーンには、**クラウドコンピューティングサービス**も含まれる。」

ISO/IEC 27002:2013 と ISO/IEC 27017:2015 の関係

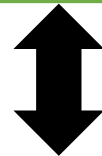
2つの規格の関係は明確であった

ISO/IEC 27002:2013

「情報セキュリティ管理策の実践のための規範」

あらゆる組織に一般的に適用される幅広い情報セキュリティ管理策に関する手引

一般的な
情報セキュリティ



明確な関係

ISO/IEC 27017:2015

「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」

クラウドサービスの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

クラウドセキュリティ

1. ISO/IEC 27017 ポイント解説

1-(1) ISO/IEC 27002:2013 と ISO/IEC 27017:2015 の関係

1-(2) ISO/IEC 27002:2022 と ISO/IEC 27017:20XX の関係

2. ISO/IEC 27017 改訂の方向性

ISO/IEC 27002:2022 における「クラウドサービス」の言及

組織がクラウドサービスを利用するのが一般的になったという昨今の状況がISO/IEC 27002:2022に反映され、「クラウドサービス」の言及が増えた

ISO/IEC 27002:2022 にて「クラウドサービス」の言及がある情報セキュリティ管理策

■ 5. 組織的管理策

- 5.10 情報及びその他の関連資産の許容される利用
- 5.14 情報の転送
- 5.19 供給者関係における情報セキュリティ
- 5.20 供給者との合意における情報セキュリティの取扱い
- 5.21 ICT サプライチェーンにおける情報セキュリティの管理
- 5.23 クラウドサービスの利用における情報セキュリティ**
- 5.34 プライバシー及びPIIの保護

■ 8. 技術的管理策

- 8.6 容量・能力の管理
- 8.8 技術的ぜい弱性の管理
- 8.9 構成管理
- 8.10 情報の削除
- 8.11 データマスキング
- 8.12 データ漏えい防止
- 8.13 情報のバックアップ
- 8.14 情報処理施設・設備の冗長性
- 8.15 ログ取得
- 8.17 クロックの同期
- 8.28 セキュリティに配慮したコーディング
- 8.33 テスト用情報

「クラウド」で検索すると123件ヒット

クラウドに特化した
5.23管理策の新規追加

5.23以外の管理策でも
クラウドサービスの
言及多数

5.23 クラウドサービスの利用における情報セキュリティ (ISO/IEC 27002:2022)

クラウドサービスの利用に関する新規管理策のISO/IEC 27002:2022への追加

ISO/IEC 27002:2022

5.23 クラウドサービスの利用における情報セキュリティ

クラウドサービスを利用するプロセスを確立する

- 手引の内容例
 - (1) クラウドサービスの調達プロセス
クラウドサービスの選定基準、他
 - (2) クラウドサービスの利用・管理プロセス
クラウドサービスの利用を監視・レビュー・評価、他
 - (3) クラウドサービスの利用終了プロセス
クラウドサービスの出口戦略、他

5.23の管理策以外にも、ISO/IEC 27002:2022 の各種管理策の手引にクラウドサービスの言及が増えた

ISO/IEC 27002:2022 組織的管理策の手引の例

5.14 情報の転送

情報をクラウドストレージなどの外部サービスを利用する場合の留意点

5.19 供給者関係における情報セキュリティ

供給者としてクラウドサービスプロバイダを利用する際の留意点

5.21 ICT サプライチェーンにおける情報セキュリティの管理

ICT サプライチェーンには、クラウドサービスも含まれる

5.23 クラウドサービスの利用における情報セキュリティ

クラウドサービスの調達、利用、管理及び利用終了における情報セキュリティ

ISO/IEC 27002:2022 技術的管理策の手引の例

8.6 容量・能力の管理

容量・能力の管理におけるクラウドサービスの弾力性及びスケーラビリティの特性

8.8 技術的ぜい弱性の管理

利用するクラウドサービスの技術的ぜい弱性管理

8.9 構成管理

クラウドサービスを含むサービスの構成管理

8.12 データ漏えい防止

信頼できない第三者のクラウドサービスに情報がアップロードされた場合

8.13 情報のバックアップ

クラウドサービス環境にある組織の情報、アプリケーション及びシステムのバックアップ

8.14 情報処理施設・設備の冗長性

クラウドサービスを利用した冗長性

ISO/IEC 27002:2022 と ISO/IEC 27017 の関係

この2つの規格の関係はどうか？

ISO/IEC 27002:2022

「情報セキュリティ管理策」

あらゆる組織に一般的に適用される幅広い情報セキュリティ管理策に関する手引

一般的な情報セキュリティ
(クラウドサービスの利用含む?)

関係は？

ISO/IEC 27017:20XX

「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」

クラウドサービスの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

クラウドセキュリティ？

よくある誤解

(A) 一般的な組織がコミュニケーションサービスやストレージサービスなどのSaaSを利用するケース

(B) AWSなどのIaaS基盤を利用して、SaaSを開発して、お客様に提供するプロバイダなどのケース

ISO/IEC 27002:2022, 5.23

ISO/IEC 27017



規格の本来の意図としては、
ISO/IEC 27002:2022, 5.23 と **ISO/IEC 27017** のどちらも
(A)(B)両方の場面が想定されている。

ISO/IEC 27017 のスコープ

あらためて ISO/IEC 27017 のスコープを確認すると

ISO/IEC 27017 のスコープ

クラウドサービスの**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

- ISO/IEC 27002の管理策への**追加**の手引
- クラウドサービスに係る**追加**の管理策及びその手引



ISO/IEC 27017 には、ISO/IEC 27002 に規定されていない
クラウドサービスに関する**追加**の管理策や手引を規定する。



ISO/IEC 27002 との具体的な関係は？

ISO/IEC 27017 の特徴

ISO/IEC 27017 には、ISO/IEC 27002 ではカバーできない、クラウド固有の内容を規定する

ISO/IEC 27017 の特徴

“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いう二者を想定し、両者が協調して情報セキュリティマネジメントシステム（ISMS）を構築するという関係を前提としている”

ISO/IEC 27017 が必要とされる理由

- (1) “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取り交わされるべき、情報セキュリティの情報及び機能の標準規格に対するニーズが存在する”
- (2) “クラウドコンピューティングに用いられる特徴的な技術”

(出典) 永宮直人 編著「ISO/IEC 27017:2015 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 解説と活用ガイド」日本規格協会、2017年

ISO/IEC 27002:2022 と ISO/IEC 27017 の関係の基本方針

ISO/IEC 27002 と ISO/IEC 27017 の関係は、
ISO/IEC 27002 が2022年版になっても、基本的には変わらない

1. クラウド固有の内容は **ISO/IEC 27017** で示す

ISO/IEC 27002:2022 でクラウドサービスへの言及が多数あるが、5.23 を除いて、その内容は（基本的には）クラウド固有の内容ではない。

（仮にこれらのクラウドサービスへの言及が ISO/IEC 27002:2022 になかったとしても、管理策と手引から読み取れる内容。次頁からのバックアップやログ取得の例を参照。）

2. **ISO/IEC 27002:2022, 5.23** と **ISO/IEC 27017** との関係について

ISO/IEC 27017で前提としている多くの場面は、クラウドサービスカスタマである組織と個々のクラウドサービスプロバイダとの、1対1の関係。

ISO/IEC 27002:2022, 5.23 の場面では、組織は、特定のクラウドサービスプロバイダを想定していない。

組織が（複数の）クラウドサービスを利用することに対する一般的な備えである。

ISO/IEC 27002:2022とISO/IEC 27017の関係の具体例 – バックアップ

クラウドサービスカスタマ

27002

27002:2022
新規管理策

5.23 クラウドサービスの利用における情報セキュリティ
クラウドサービスの調達、利用、管理及び利用終了のプロセスを確立する

27017

自組織のセキュリティ要求事項を満たすかを検証する
満たさない場合、自組織で追加のバックアップ機能を実装する

27002

8.13 情報のバックアップ
バックアップを維持、検査する。
(クラウドサービスのバックアップ機能を利用したクラウドサービス上の情報のバックアップを含む)

27002:2022に
クラウド上のバック
アップ取得の手引追加

27002と27017の
関係は変わらない

27017

クラウドサービスの
バックアップ機能に
ついて情報要求

27017

クラウドサービスの
バックアップ機能の
情報及び機能の提供

- バックアップ範囲／スケジュール
- バックアップデータの保持期間
- バックアップの保存場所

など

クラウドサービスプロバイダ

27002

8.13 情報のバックアップ
バックアップを維持、検査する。
(クラウドサービス運用のためのバックアップを含む)

27002:2022に
クラウド上のバック
アップ取得の手引追加

ISO/IEC 27002:2022とISO/IEC 27017関係の具体例 – ログ取得

クラウドサービスカスタマ

27002

27002:2022
新規管理策

5.23 クラウドサービスの利用における情報セキュリティ

クラウドサービスの調達、利用、管理及び利用終了のプロセスを確立する

27017

自組織のセキュリティ要求事項を満たすかを検証する
満たさない場合、自組織で追加のログ取得機能を実装する

27002

8.15 ログ取得

ログを取得、保存、保護、分析する。
(クラウドサービスのログ取得機能を利用したクラウドサービス上のログ取得を含む)

27002:2022に
クラウド上のログ取得
の関連情報追加

27002と27017の
関係は変わらない

27017

クラウドサービスの
ログ取得について
情報要求

27017

クラウドサービスの
ログ取得の情報及び
機能の提供

クラウドサービスプロバイダ

27002

8.15 ログ取得

ログを取得、保存、保護、
分析する。
(クラウドサービス運用の
ためのログ取得を含む)

27002:2022に
クラウド上のログ取得
の関連情報追加

クラウドコンピューティングに用いられる特徴的な技術

クラウドコンピューティングに用いられる特徴的な技術も
ISO/IEC 27017 のスコープ

例) 仮想コンピューティング環境における分離

- マルチテナント環境におけるテナント間の分離
- クラウドサービスカスタマの環境と
クラウドサービスプロバイダの内部管理の環境の分離

まとめ（ISO/IEC 27002:2022 と ISO/IEC 27017 の関係）

- ISO/IEC 27002 と ISO/IEC 27017 の関係は、ISO/IEC 27002 が 2022年版になっても、基本的には変わらない
- ISO/IEC 27002 と ISO/IEC 27017 は、お互い補完しあっている
- クラウドサービスの観点から ISO/IEC 27002:2022 を読んでみると、各管理策配下に役に立つクラウドセキュリティの手引が記載されている
- ISMSクラウドセキュリティ認証の取得の有無に関わらず、ISO/IEC 27017 規格を読むと、クラウドサービスを利用・提供する際の参考情報を得ることができる

1. ISO/IEC 27017 ポイント解説

1-(1) ISO/IEC 27002:2013 と ISO/IEC 27017:2015 の関係

1-(2) ISO/IEC 27002:2022 と ISO/IEC 27017:20XX の関係

2. ISO/IEC 27017 改訂の方向性

ISO/IEC 27017 改訂の方向性

- ISO/IEC 27002 と ISO/IEC 27017 の基本的な関係や位置づけは継承
- ISO/IEC 27017 の特徴も継承
 - プロバイダとカスタマの双方にクラウド手引を提供
 - クラウドサービス固有の管理策を提供、など

ISO/IEC 27017 改訂の方向性

- ISO/IEC 27002:2022 の管理策構成に合わせる
- 新規のクラウド固有の管理策（CLD管理策）の追加
- ISO/IEC 27002:2022 で追加された新規管理策への、クラウドサービスのための手引の追加
- ISO/IEC 27017:2015 のクラウド固有の管理策（CLD管理策）の見直し（CLD管理策ではなく、ISO/IEC 27002:2022 の管理策のクラウドサービスのための手引とするもの含む）

全体まとめ

1. ISO/IEC 27017 ポイント解説

1-(1) ISO/IEC 27002:2013 と ISO/IEC 27017:2015 の関係

1-(2) ISO/IEC 27002:2022 と ISO/IEC 27017:20XX の関係

2. ISO/IEC 27017 改訂の方向性

ご清聴ありがとうございました。