パブコメ版

クラウドサービス（PaaS/SaaS）セキュリティの技術的評価ガイド

第 1.0 版

平成**年*月

特定非営利活動法人 日本セキュリティ監査協会

目次

1. 本書の位置付け及び目的

本書は、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）に記載された管理策及び実装指針に対する実装並びにその運用を監査するための指針を提供する。本書は、ISO/IEC 27001:2013 の付属書 A に記載された管理策及び実装指針に対して新たに指針を追加している。

また、クラウドサービスのうち利用者に抽象化されたコンピュータリソースを提供する PaaS/SaaS を想定して、監査に必要な技術的な着目点及び監査方法を解説する。

なお、クラウドサービスの定義はクラウドサービス事業者が提供するサービスおよび顧客がクラウドサービス上の情報システムの運用によりエンドユーザに提供するサービス全体を指す。一方で、本文書が示す監査の対象は、クラウドサービス利用者が行うクラウドサービス上の情報システム（PaaS/SaaS）（以下、単に「クラウドサービス上の情報システム」という）における情報セキュリティ管理策の実装である。

クラウドサービス上の情報システムは、千差万別であり、技術的進歩が著しいことから日々変化する。本書は特定のシステムを想定したものではなく、監査の方法、留意点、監査対象などについての実践指針である。また、IaaS に対して全般的に適用される共通事項に関しては別に定める「クラウドサービス（IaaS） の技術的評価ガイド」の解説に基づくものとする。

クラウドサービス上の情報システムクラウドサービス上の情報システムクラウドサービス上の情報システム

本書は、監査人に対してクラウドサービス上の情報システムに特有な監査ポイント（評価対象における責任範囲の特定等）の会得を提供する、また、監査を受ける側の技術者には、どのようにサービスが評価され、どのように証跡を示すべきかのヒントを与えるものである。

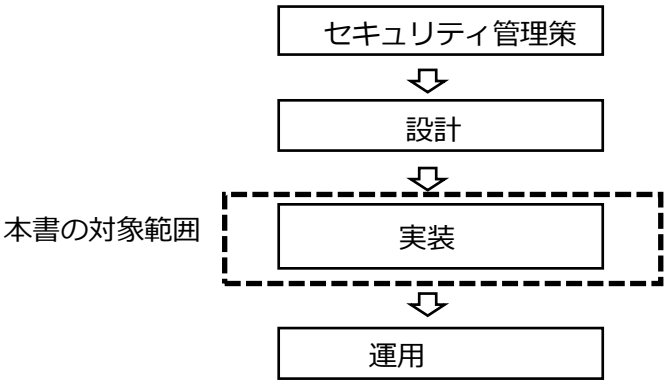

図 1　本書の対象範囲

2. 国際標準との関係

ISO/IEC 27017 に加え、次の規格が関連している。

(1) ISO/IEC 22123-1 Information technology – Cloud computing – Vocabulary

本書は、ISO/IEC 22123 に規定するクラウドコンピューティングに関する用語を準用する。

(2) ISO/IEC 22123-2 Information technology – Cloud computing – Concepts

本書は、ISO/IEC 22123 に規定するクラウドコンピューティングに関する概観を準用する。

3. 本書の構成

本書は、まず PaaS/SaaS を想定したクラウドサービス環境モデルを提示する。このモデルは、リソース種別と仮想化との関係、クラウドサービス利用者とテナントの概念を定義する。
監査要件は、共通事項、サービス管理、サーバ、ネットワーク及びストレージの各々について、次の順に記述している。

(1) 技術的解説

仮想化の実装に関する技術的要素と手引きの説明。複数の実装方式がある場合には、典型的な幾つかの方式を列挙する。

(2) ISO/IEC 27017 で規定されている管理策

仮想化に関連する ISO/IEC 27017 の管理策の引用。

(3) ISO/IEC 27017 の管理策に対する監査方法

ISO/IEC 27017 の管理策に対する監査方法の指針。複数の実装がある場合は、その１つを示す。

```
管理策　（27017 に記載された管理策）
クラウドサービス事業者のための実装指針　（27017 に記載された実装指針）
追加技術情報
1　技術的解説(その 1)
　セキュリティ実装基準　（詳細管理策）
　セキュリティ実装基準する技術的解説
　1.1　実装ガイド、想定される証拠、監査技法（その１の１）
　　実装ガイド
　　想定される証拠
　　監査技法
　1.2　実装ガイド、想定される証拠、監査技法（その１の 2）
　　実装ガイド
　　想定される証拠
　　監査技法
　・・・
2　技術的解説(その 2)
　セキュリティ実装基準（詳細管理策）
　セキュリティ実装規準に関する技術的解説
　2.1　実装ガイド、想定される証拠、監査技法（その２の 1）
　　実装ガイド
　　想定される証拠
　　監査技法
　2.2　実装ガイド、想定される証拠、監査技法（その２の 2）
　　実装ガイド
　　想定される証拠
　　監査技法
　・・・
```

図２　ISO/IEC 27017 の管理策に対する監査方法の指針

4. クラウドサービス環境モデル

4.1 モデル導入の意義

クラウドサービスに用いられる技術は多岐にわたることから、これらを仔細に取り上げることは個別且つ具体的過ぎる。また、クラウドサービスに用いられるコンピューティング技術は新しい分野であり、技術的に発展途上にある。これらのことから、個別且つ具体的な技術に基づく評価の方法を定めることは標準化になじまない。これに対してモデルは管理策の意図するところを具体的な技術としてイメージすることができるため、評価に際しての具体的な方法を示すことができる。実際に評価を行う際に、このモデルを念頭に置き、管理策のために実装されている実際の技術が、管理策の意図に沿ったものであるか、また、評価者である監査人等が、それらの評価のための証拠の収集はどのようにするかを、判断できる。

4.2 モデルと構成要素

本書が想定するクラウドサービス上の情報システムの監査における対象を図 2 に範囲を示す。

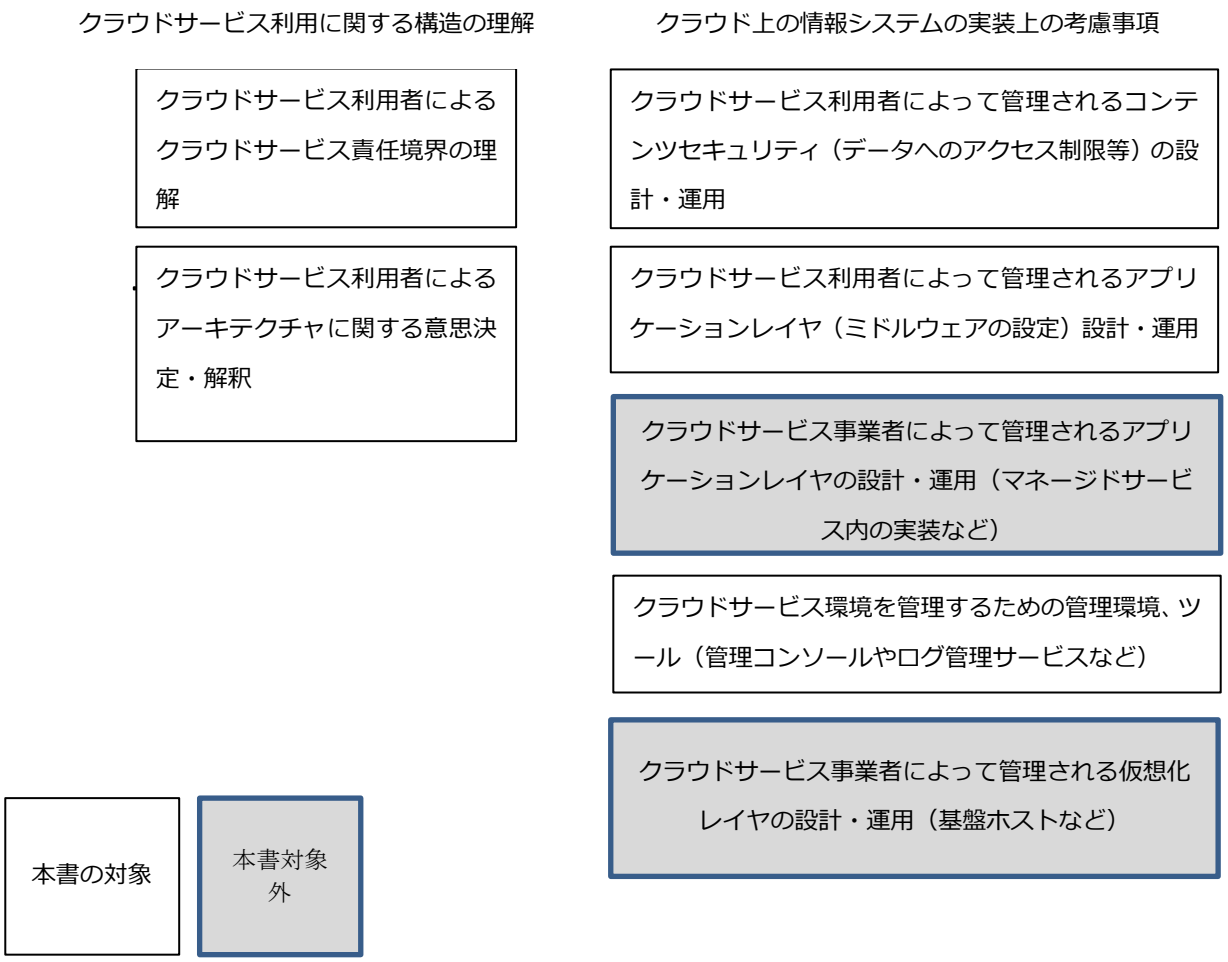

図 3　クラウドサービス上の情報システムの環境モデルと本書の対象範囲

4.3　環境モデル

本モデルの重要な概念は、クラウドサービス利用者の管理およびミドルウェアおよびアプリケーション管理の抽象化と分離である。IaaS においては、ミドルウェアおよびアプリケーションは、クラウド利用者により管理されていたが、SaaS/PaaS においてはサービス毎にクラウドサービス事業者によって提供される機能の範囲が異なる。

(1) クラウドサービスとクラウドサービス上の情報システムの関係性の理解

クラウドサービスは、スケーラビリティの提供（プロビジョニングによるリソースの利用状況に応じたコンピューティングリソース伸縮の自動化）、レジリエンシーの向上（自動化されたバックアップや障害の発生したインスタンスの自動復旧や切り替え）、リソース管理の省力化（パッチ適用の自動化や管理対象の抽象化）、他のサービスとの連携（イベントの監視および発動、API の提供）などの要素により、利用者が手軽に情報処理を行えることが一般的にメリットと考えられている。

クラウドサービス利用者によっては、サービスが提供する便益よりも自らの運用設計による管理によってシステムに求める要件を効果的に実現する場合もあるため、組織が求める要件をクラウドサービス上の情報システムに反映し、利用するサービスを効果的に選択する必要がある。また、多くの IT システムは単一のクラウドサービスで提供されるものではなく、複数のクラウドサービスの組み合わせに依拠する場合もあり、要素ごとに求めるべき要件を特定する必要がある。

また、クラウドサービスの各要素がどのような機能を提供し、またクラウドサービス利用者はどのような範囲を管理すべきかを把握するため、各クラウドサービスの責任境界に対する理解が求められる。

クラウドサービス上の情報システムに対する情報セキュリティ監査においては、利用者が選択した要素や利用者の管理すべき範囲を、あらかじめ的確に把握しておくことが必要となる。

(2) クラウドサービス利用者に関する実装上の考慮事項

PaaS/SaaS クラウドサービスにおいては、仮想化レイヤは抽象化されクラウドサービス事業者によって管理される。一方、ミドルウェアおよびアプリケーションに関してはクラウドサービス事業者が提供するサービスによりその範囲および機能が異なる。監査対象となるクラウドサービス上の情報システムにおいて、利用者の管理範囲を監査に先立って確認する必要がある。

(3) クラウドサービス環境を管理するための管理環境、ツール

クラウドサービスの利用においては、クラウド環境自体の権限管理、ログやリソース管理、請求管理等の機能を提供する管理環境やツールを用いることがある。クラウドサービス利用者は、クラウドサービス事業者が提供する管理環境やツールを利用することも、サードパーティの事業者が提供するものを利用することもできる。いずれの場合も、クラウドサービス上の利用者の IT サービスに直接関連するリソースに加えて、これらの管理環境やツールに対する管理およびアクセス権限の付与を考慮する必要がある。

(4) PaaS/SaaS におけるクラウドサービス管理の分離

クラウドサービス利用者が認識する必要のあるアクセス制御対象は，以下の 3 つに分類することが可能である。

① 管理コンソールやクラウド事業者が提供する機能やリソース、ミドルウェアなど利用者のクラウド環境，アプリケーションなど利用者のクラウド環境

② 管理ツール：自動化やオーケストレーションなどクラウド環境上の様々な構成要素を制御するためのサービステナント：クラウド利用者自身の管理機能及びアプリケーション
③ コンテンツ：(①，②で伝送、処理、保管するデータ）および派生データ（サービスにより生成されるメタデータ等）

このうち、①および②は、利用者がクラウド事業者の提供するサービスを利用する場合、利用者独自技術を採用する場合、代理サービスを利用する場合など多様である。また、③はクラウドサービス固有のものではなく、扱うデータのアクセス制限や管理策（アクセスコントロールや暗号化など）の手段が利用者によって異なることが想定される。
本書では、利用者環境における利用者としての管理者をクラウドアドミニストレータと定義し、そのアドミニストレータ内において組織の職務分掌、アクセスポリシーに応じて複数の権限に応じた役割が設定されることを想定している。管理の仕方以下、表１にクラウドサービス利用における職務分離の例を示す。ただし、管理の仕方は組織によって異なり、必ずしも明確な職務分離が求められるものではない。

表１ クラウドサービスにおける職務分離の例

職務	役割	管理目的	管理対象の例	アクセス制御対象
エンドユーザ	アプリケーションの利用者	サービスの利用を行うもの。自らのコンテンツ利用に責任を負う。	アクセス可能なコンテンツに対する適正な利用	③
クラウドサービスアドミニストレータ	アプリケーションの管理者	アプリケーションレイヤにおける権限管理に責任を負う。 コンテンツへのアクセス管理の付与、アプリケーションの脆弱性管理などに責任を負う。	コンテンツ（アプリケーションに伝送、処理、保管されるデータ）および派生データ（アプリケーションにより生成されるメタデータ等）に対するアクセス制限	③
	クラウドサービス上の情報システム（単一もしくは複数のクラウドを利用）の管理者	クラウド上のリソースにおいて利用者が管理すべき領域に責任を負う。クラウド事業者が提供する機能に対する設定、設計などに責任を負う。	ミドルウェアやアプリケーションにおけるアクセス制限や設定	①②
	採用しているクラウドサービス自体のリソース	クラウド環境全体を管理するサービスの利用、管理に責任を負う。	クラウドサービスに付帯する管理コンソール、ログの集	①

	管理者		約化、複数のサービスの一元管理や自動化のためのオーケストレーションなどの設定、設計など。	
クラウドアーキテクト	クラウドアーキテクト	組織の要件をふまえた環境の設計に責任を負う。組織要件の把握、利用するクラウドの選択などに責任を負う。	要件の評価と定義	①

(5) クラウドサービス上の情報システムにおける監査の役割と手法

クラウドサービス利用者の環境に対するセキュリティ監査としては、クラウドサービスの関係性の理解を通じ、組織が選択したクラウドサービス環境がクラウドサービス利用者のニーズを反映しているものであるか、クラウドサービス事業者が提供するサービスとの責任境界を適切に理解したうえでサービス設計を行っているかを、サービス取得時のレビューやリスクアセスメント結果を通じて評価することが望ましい。また、クラウドサービスによっては機能の追加や仕様の変更を踏まえた継続的な評価が必要となる場合もある。

そのうえで、監査人は組織のクラウドサービス管理の分離に基づき、どのような責任が定義され、どのような設計、運用が行われているかを評価する。分離の程度は組織および選択したクラウドサービスによって異なることに留意する。

本書では、クラウドサービス事業者が管理する環境においては対象外としているが、一般にクラウドサービス事業者が公開するドキュメントや第三者監査の結果報告書を通じてクラウドサービス利用者が主体的に判断するものとなる。

5. 環境モデル監査手続の共通実践事項

監査人は、クラウドサービス利用者に対する監査に際し、以下の事項を考慮する。

5.1 組織の期待の特定

クラウドサービス利用者が組織の期待する目的や目標に基づき定義した管理策を確認する。

5.2 管理策に基づく監査範囲の特定

クラウドサービス上の情報システムの監査において各管理策に対し評価すべき監査範囲を特定する。
SaaS/PaaS を提供するクラウドサービス事業者は必ずしもすべての管理策を満たすサービスを提供しているとは限らない。そのため、クラウドサービス利用者は、組織が求めるセキュリティの基準を達成するために、それぞれの詳細管理策に対し、クラウドサービス事業者が提供する機能の範囲と、組織として採用するその他の管理策（外部サービスの利用もしくは、組織の運用業務設計）を適用する場合がある。

5.3 利用者の責任範囲の特定

監査に先立ち評価対象における責任範囲を特定することで、監査範囲を決定する。
クラウドサービス事業者により提供される機能に対する責任範囲は、サービスの特性に応じて異なる場合がある。例えば、ライセンス、保守や脆弱性に対する対応、サービス運用（バックアップやプロビジョニング）、商用ソフトウェアやオープンソースに対する免責等はサービスによって異なる。

5.4 評価対象と基準の突合

組織が求める基準と評価対象から得られる監査証跡（設定値や観察によって得られる事実）に基づき、監査対象を評価する。

また、クラウドサービスの利用に際し、クラウドサービス事業者もしくは第三者がセキュリティに対するベストプラクティスなどの規範を提供している場合がある。組織がそのような基準を採用している場合、あわせて評価を行う。

なお、評価対象となる監査証跡はクラウドサービス事業者が提供する機能により提供される場合と、クラウドサービス上の情報システムの機能や他のクラウドサービスの利用などにより、クラウドサービス利用者が自ら実装し出力する場合があることに留意する。

5.5 外部の活用

組織が求めるセキュリティの基準を達成するために対象となるクラウドサービス以外に適用している管理策がある場合、監査目的を踏まえ必要に応じて評価を行う。

6. 環境モデル監査手続

本文書では、対象となる管理策が異なっていても、同一の監査手続によって監査評価が可能なものをグループ化して記載している。

管理策を評価する際には、その管理策に基づく統制目標の達成を評価するために適切な監査手続に従い、監査証跡を評価する必要がある。
手続きが同一となるものを特定し、一つの監査手続によって複数の管理策の評価を行うことができれば、監査を効率的に進め、監査資源をより有効に活用することにつながる。
本文書では次のような場合は監査手続を同一のものとしてグループ化し、監査手続の効率化に資することができるものとしてガイドを提供する。

- 統制目標の対象や抽象度が異なるだけで実際の監査手続、監査証跡は同一のものであると想定される場合（例えば、変更管理として、ネットワーク管理の変更もプログラムの変更も同一の管理システムを導入している場合など）
- 組織の業務設計により、異なる管理策に対しても同一の業務手続きによって管理される場合（例えば、チケット管理システムを利用し、承認行為や認証認可の付与、失効などを一元的に管理している場合など）
- ISO 上では管理策として定義されているが、実際の利用上では他の管理策の一環として評価可能な場合（例えば、ユーティリティプログラムの管理は、対象自体があいまいであり、監査のためにわざわざユーティリティプログラムを被監査組織ごとに定義し、監査手続に組み込むことは非効率であり、実際には権限管理の一環として評価ができる）

実際には被監査組織の業務設計などにより、すべてを単純に同一の監査手続によって評価できるものではない。また、監査手続は同一でも監査目標を達成するために個別の監査手続として実施すべき場合も存在する。
ただし、監査計画において、効率的な評価手続きを計画し、監査人と被監査人が合意することができれば、監査資源をより効率的に配分することが可能となる。

管理策		9.1.2 Access to networks and network services 9.2.1 User registration and deregistration 9.2.3 Management of privileged access rights 9.2.4 Management of secret authentication information of users 9.4.1 Information access restriction CLD.12.1.5　実務管理者の運用のセキュリティ	
実施の手引		クラウドサービス事業者は，クラウドサービスのリソースに対する認証および認可を実装する方法について，クラウドサービス利用者に情報を提供することが望ましい。次の事項は，クラウドサービス利用者が，当該変更が情報セキュリティに与える可能性のある影響を特定するのに役立つ。 －認証認可を行うための仕組み －認証認可の対象となる主体（仮想ネットワークを構成するリソース、仮想サーバインスタンス等） －認証認可を行う対象に関する技術的な説明 －認証認可に対する証跡（アクセスコントロールマトリクス、ネットワーク環境の可視化、ネットワークダイアグラム） －外部サービスの利用の可否と可能な場合の実装方法 クラウドサービスおよびクラウドサービス上のリソースによって異なる認証認可の仕組みが必要となる場合がある。	
追加技術情報		認証認可を行う主体は人的リソースのみならず、サーバやサービスなどが認証認可の主体となることもある。 これらの認証認可の仕組みの対象範囲や特権の定義は、多岐に渡り、クラウドサービス利用者に対する影響度も異なる。このため、一般に、どの対象範囲に対してどのような仕組みを適用するかは、クラウドサービス利用者の設計に依存する。 また、認証認可機能の提供を目的とした外部のサービスを利用することで、管理の効率化や一元管理を実現することが可能な場合もある。	
1	セキュリティ実装基準（詳細管理策）	アクセスコントロールにおいては、直接的、間接的に影響を受ける主体および利用する認証認可の仕組みを特定し適切に設定する。	
	セキュリティ実装基準の技術的解説	クラウドサービス事業者はクラウドサービス上の主体に対する認証認可の仕組みを提供しているが、その対象となる主体および認証認可の粒度はクラウドサービス事業者によって異なる場合があるため、監査人は監査の目的を踏まえて監査の評価対象を特定する。（監査手続１．１） 続いて組織の管理基準に定義された職務分掌やリスクコントロールマトリクスとクラウドの実装を突合し評価を行う（監査手続１．２） なお、組織によっては認証認可の仕組みを他のサービスや自社の認証基盤に依拠している場合があるため、認証の連携方法を評価する必要がある。（監査手続 1.3）	
	1.1	監査実施ガイド	評価対象の特定 クラウドサービス利用者が評価対象となるリソースに対する認証認可の仕組みを特定しているかを確認する。 ネットワークのアクセスとして管理対象となる主体が、仮想ネットワーク上のネットワーク機能（ファイヤウォールやルーター等）により管理することもあれば、クラウドサービス事業者が提供する認証認可の仕組みによって管理される場合もある。 PaaS 領域におけるクラウドサービス利用者の管理領域に関して、OS やミドルウェアに対する管理権限がクラウドサービス利用者に提供される場合があり、クラウドサービスが提供する管理機能とは別に IaaS 環境と同様に OS やミドルウェアの管理機能の設定が必要な場合がある
		想定される証拠	クラウドサービスにおける認証認可の仕組みを利用した設定対象と、組織の定めるアクセスコントロールマトリクスの突合 対象となるネットワークのネットワークダイアグラムと実際の仮想環境上のネットワークアクセス管理の実装
		監査技法	観察および閲覧
	1.2	監査実施ガイド	評価対象と基準の突合 クラウド上の主体に個別の認証認可の実装が必要となる場合、対象となる主

			体と実装手段が特定され, 認証認可の仕組みが適切に実装されていることを確認する。
		想定される証拠	対象となる主体毎の認証認可の仕組みの対象と、組織の定めるアクセスコントロールマトリクスの突合
		監査技法	観察
	1.3	監査実施ガイド	補足 外部の活用 外部の認証認可サービスを利用している場合、対象となる主体と実装手段が特定され，認証認可の仕組みが適切に実装されていることを確認する。
		想定される証拠	外部の認証認可サービスの機能にもとづく仕組みおよび対象の特定と、組織の定めるアクセスコントロールマトリクスの突合
		監査技法	観察

管理策		CLD.9.5.1 Segregation in virtual computing environments 13.1.3 Segregation in networks CLD.13.1.4 Alignment of security management for virtual and physical networks	
実施の手引		クラウドサービス事業者は，クラウドサービスのリソースに対する隔離の実装機能および情報を提供することが望ましい。次の事項は，クラウドサービス利用者が，当該変更が情報セキュリティに与える可能性のある影響を特定するのに役立つ。 －隔離を行うための仕組み －隔離の対象となる主体（仮想ネットワークを構成するリソース、仮想サーバインスタンス等） －隔離を行う対象に関する技術的な説明 －隔離に対する証跡（アクセスコントロールマトリクス、ネットワーク環境の可視化、ネットワークダイアグラム） クラウドサービスおよびクラウドサービス上のリソースによって異なる隔離の仕組みが必要となる場合がある。	
追加技術情報		これらの認証認可の仕組みの対象範囲は、多岐に渡り、クラウドサービス利用者に対する影響度も異なる。このため、一般に、どの対象範囲に対してどのような仕組みを適用するかは、クラウドサービス利用者の設計に依存する。リソース間の隔離をネットワークセキュリティの仕組みとして実装している場合もあれば、リソースに対する認証認可の仕組みにより実装している場合もある。 隔離機能の提供を目的とした外部のサービスを利用することで、管理の効率化や一元管理を実現することが可能な場合もある。	
1	セキュリティ実装基準（詳細管理策）	アクセスコントロールにおいては、直接的、間接的に影響を受ける主体および利用する隔離の仕組みを特定し適切に設定する。	
	セキュリティ実装基準の技術的解説	クラウドサービス事業者はクラウドサービス上のリソースに対する隔離の仕組みを提供しているが、隔離の実装に関しては、クラウドサービス利用者の設計によって異なる場合がある。そのため監査人はクラウドサービス利用者がどのように論理的な分離を実装しているかをはじめに特定する必要がある。(管理手続き 1.1) その上で、対象となる主体に対する論理的な分離が組織が求める要件に合致しているかを確認する。(管理手続き 1.2)	
	1.1	監査実施ガイド	評価対象となるリソースに対する隔離の仕組みをクラウドサービス利用者が特定しているかを確認する。
		想定される証拠	クラウドサービスにおける隔離の仕組みを利用した設定対象と、組織の定めるアクセスコントロールマトリクスの突合 対象となるネットワークのネットワークダイアグラムと実際の仮想環境上のネットワークアクセス管理の実装
		監査技法	観察および閲覧
	1.2	監査実施ガイド	クラウド上の主体に個別の実装が必要となる場合、対象となる主体と実装手段が特定され，認証認可の仕組みが適切に実装されていることを確認する。
		想定される証拠	対象となる主体毎の仕組みの対象と、組織の定めるアクセスコントロールマトリクスの突合
		監査技法	観察
	1.3	監査実施ガイド	外部の認証認可サービスを利用している場合、対象となる主体と実装手段が特定され，認証認可の仕組みが適切に実装されていることを確認する。
		想定される証拠	外部の認証認可サービスの機能にもとづく仕組みおよび対象の特定と、組織の定めるアクセスコントロールマトリクスの突合
		監査技法	観察

管理策			12.1.2 Change management CLD.12.4.5 Monitoring of Cloud Services 12.3.1　情報のバックアップ 12.4.1 イベントログ取得 12.4.3　administrator and operator logs 12.4.4　Clock synchronization 12.6.1　技術的ぜい弱性の管理 16.1.2 Reporting information security events 16.1.7 Collection of evidence
実施の手引			クラウドサービス事業者は，クラウド上のリソースに対する設定の推奨値に関する情報を提供し、意図しない設定を検知する機能を提供することが望ましい。 次の事項は，クラウドサービス利用者が，当該変更が情報セキュリティに与える可能性のある影響を特定するのに役立つ。 －設定の推奨値 －設定の対象となる主体（仮想ネットワークを構成するリソース、仮想サーバインスタンス等） －設定の対象に関する技術的な説明 －設定に対する証跡（ログや設定変更の承認に対する記録） －設定に対する変更の履歴（特定のリソースに行われた変更履歴の取得） －設定の変更を禁止する手段の特定（アクセスコントロールの実装） －設定の変更に対する検知および通知手段の特定（アクセスコントロールの実装） －外部サービスの利用の可否と可能な場合の実装方法 クラウドサービスおよびクラウドサービス上のリソースによって異なる設定管理の仕組みが必要となる場合がある。
追加技術情報			設定管理の監視および対応を目的とした外部のサービスを利用することで、管理の効率化や一元管理を実現することが可能な場合もある。 クラウドを構成する設定項目は、一般に CSPM (CloudSecurity Posture Management)により管理されている。 これらの設定変更の仕組みの対象範囲は、多岐に渡り、クラウドサービス利用者に対する影響度も異なる。このため、一般に、どの対象範囲に対してどのような仕組みを適用するかは、クラウドサービス利用者の設計に依存する。
1	セキュリティ実装基準（詳細管理策）		アクセスコントロールにおいては、直接的、間接的に影響を受ける主体および利用する設定管理の仕組みを特定し適切に設定する。
	セキュリティ実装基準の技術的解説		クラウドサービス事業者はクラウドサービス上のリソースに対する設定管理の仕組みを提供しているが、その対象となる主体および設定管理の粒度はクラウドサービス事業者および対象となるリソースによって異なる場合がある。 PaaS 領域を管理する場合、クラウドサービスのリソース自体に関する設定の変更および意図しない変更に対する検知及び通知、PaaS として管理の対象となるリソースに対する管理権限がクラウドサービス利用者に提供される場合があり、かつ、クラウドサービスが提供する管理機能とは別に PaaS 環境と同様に設定管理を実施する外部のサービスが存在する場合がある。(管理手続き 1.1) 設定における推奨値は必ずしもクラウドサービス事業者が提供しているわけではなく、第三者によって提供される場合もある。(管理手続き 1.2)
	1.1	監査実施ガイド	クラウドサービス利用者が評価対象となるリソースに対する設定項目を特定しているかを確認する。かつ、推奨値がある場合はその適用対象を特定しているかを確認する。
		想定される証拠	組織が採用するクラウドサービスにおける設定対象に対する推奨値の情報 組織が対象とするクラウドサービス上のリソースの特定
		監査技法	観察および閲覧
	1.2	監査実施ガイド	クラウドサービスのリソースに対する推奨値の適用方法を特定し、その粒度（自動化の可否、評価の頻度、推奨値の更新頻度)を評価する。
		想定される証拠	対象となるリソースに対する評価結果と組織が求める設定の差分を評価する。
		監査技法	観察および閲覧

	1.3	監査実施ガイド	外部の設定管理サービスを利用している場合、対象となる主体と実装手段が特定され，設定管理の仕組みが適切に実装されていることを確認する。
		想定される証拠	外部の設定管理サービスの機能にもとづく仕組みおよび対象の特定と、組織が定める設定の差分の突合
		監査技法	観察

管理策			10.1.1 Policy on the use of cryptographic controls 10.1.2 Key management
実施の手引			クラウドサービス利用者は、リスク分析に基づき、クラウドサービスの利用に暗号制御を実装する必要がある。クラウドサービス利用者は、クラウドサービスの利用に関して、リスク分析に基づく場合、暗号管理を実施すべきである。 クラウドサービス事業者が暗号機能を提供する場合、クラウドサービス利用者は、クラウドサービス事業者から提供された情報をレビューし、その暗号機能がクラウドサービス利用者のポリシーに適合しているかどうかを確認する必要がある。 - クラウドサービス利用者のポリシー要件を満たしていること. - クラウドサービス利用者が使用する他の暗号保護と互換性があること. - クラウドサービス利用者は、クラウドサービス事業者から提供された暗号化機能を確認する必要がある。
追加技術情報			クラウドサービス上のリソースに外部の暗号化機能を適用することが可能な場合がある。 これらの暗号化機能の仕組みの対象範囲は、多岐に渡り、クラウドサービス利用者に対する影響度も異なる。このため、一般に、どの対象範囲に対してどのような仕組みを適用するかは、クラウドサービス利用者の設計に依存する。
	セキュリティ実装基準（詳細管理策）		アクセスコントロールにおいては、直接的、間接的に影響を受ける主体および利用する暗号化管理の仕組みを特定し適切に設定する。
	セキュリティ実装基準の技術的解説		クラウドサービス事業者がクラウドサービス上のリソースに対する暗号化機能に関する情報を提供している場合、その対象となる主体および暗号化機能はクラウドサービス事業者および対象となるリソースによって異なる場合がある。 監査人はクラウドサービス利用者が暗号化機能の対象範囲およびその実装を定義していることを評価する（管理手続き 1.1 管理策 10.1.1） また、暗号化機能の利用に際し適用される鍵管理機能を評価する。（管理手続き 1.2 管理策 10.1.2） なお、暗号化機能は必ずしもクラウドサービス事業者が提供しているわけではなく、第三者によって提供される場合もある。（管理手続き 1.3）
	1.1	監査実施ガイド	クラウドサービス利用者が評価対象となるリソースに対する暗号化機能およびその実装方法を特定しているかを確認する
		想定される証拠	組織が採用する暗号化機能の推奨値の情報 組織が対象とするクラウドサービス上のリソースの特定
		監査技法	観察および閲覧
	1.2	監査実施ガイド	クラウドサービスのリソースに対する暗号化機能の適用方法を特定し、その粒度（アルゴリズム、鍵の所有、鍵管理、鍵の保管、鍵のアクセス管理）を評価する。
		想定される証拠	対象となるリソースに対する暗号化機能の実施状況と組織が求める設定の差分を評価する。
		監査技法	観察および閲覧
	1.3	監査実施ガイド	外部の暗号化機能を利用している場合、対象となる主体と実装手段が特定され，暗号化管理が適切に実装されていることを確認する。
		想定される証拠	外部の暗号化の機能にもとづく仕組みおよび対象の特定と、組織が定める設定の差分の突合
		監査技法	観察

管理策		12.1.3　容量・能力の管理	
実施の手引		クラウドサービス事業者は，リソース不足による情報セキュリティインシデントの発生を防ぐため，リソース全体の容量・能力を監視することが望ましい。	
追加技術情報		監査人はクラウドサービス利用者が、クラウドサービスの利用に際し、モニタリングの対象とするリソースとその手段、運用上の閾値の設定に対する基準およびその実装を特定する。(管理手続き 1.1) さらに運用上の閾値に対する手続きとその証跡を評価する。手続きは手動で行われる場合もあれば自動化されている場合もあり、組織の運用上の要求に合致しているかを評価する。(管理手続き 1.2)	
1	セキュリティ実装基準（詳細管理策）	コンピューティングリソースの追加などが必要となる水準を定め、当該水準に達した際に必要な措置を講じる。	
	セキュリティ実装基準の技術的解説	コンピューティングリソースについて、一定の閾値を定め、使用量がこれを超える場合には警告が発せられるような監視を行なう。 監視は、クラウドシステム、IT 機器、ソフトウェア等により、コンピューティングリソースの使用状況を監視することで行なわれる。	
	1.1	監査実施ガイド	クラウドシステムにおいて、キャパシティ管理が必要となるコンピューティングリソースについて、必要な監視が行なわれているか確認する。
		想定される証拠	クラウド監視システムの監視定義 キャパシティの使用状況のレポート出力
		監査技法	観察
	1.2	監査実施ガイド	使用キャパシティが閾値を超えた場合、警告が発せられることを確認する。
		想定される証拠	クラウド監視システムの警告設定（閾値による警告発生が定義されていることの確認） クラウド監視システムのイベントログ(過去に警告が発せられたことの確認)
		監査技法	観察

7. ISO/IEC 27017 と本書の記載関係表

		本書の記載範囲	クラウドサービス(IaaS)の技術的評価ガイドの記載範囲				
章	タイトル		共通	サーバ仮想化	ネットワーク仮想化	ストレージ仮想化	サービス管理
5	情報セキュリティのための方針群	×	技術事項ではないため該当しない				
5.1	情報セキュリティのための経営陣の方向性	×	×	×	×	×	×
6	情報セキュリティのための組織	×	技術事項ではないため該当しない				
6.1	内部組織	×	×	×	×	×	×
6.2	モバイル機器及びテレワーキング	×	×	×	×	×	×
CLD.6.3	クラウドサービス利用者及びクラウドサービス事業者の関係	×	×	×	×	×	×
7	人的資源のセキュリティ	×	技術事項ではないため該当しない				
7.1	雇用前	×	×	×	×	×	×
7.2	雇用期間中	×	×	×	×	×	×
7.3	雇用の終了及び変更	×	×	×	×	×	×
8	資産の管理	×	物理リソースは範囲外のため該当しない				
8.1	資産に対する責任	×	×	×	×	×	×
CLD.8.1	資産に対する責任	×	×	×	×	×	×
8.2	情報分類	×	×	×	×	×	×
8.3	媒体の扱い	×	×	×	×	×	×
9	アクセス制御		・利用者のアクセス制御の記述は基本的にサービス管理内で完結する ・サービス事業者のオペレータのアクセス制御はこの章ではなく 12 章でカバーされる ・本章は、仮想化/仮想化リソースのための機能における利用者毎のアクセス制御の可能な設定をカバーする				
9.1	アクセス制御に対する業務上の要求事項	9.1.2	—	—	—	—	—
9.2	利用者アクセスの管理	9.2.1 9.2.3 9.2.4	→	→	→	→	9.2.1 9.2.2 9.2.3
9.3	利用者の責任	×	—	—	—	—	—
9.4	システム及びアプリケーションのアクセス制御	9.4.1 9.4.4	→	→	→	→	9.4.1 9.4.4
CLD.9.5	共有化された仮想環境におけるクラウドサービス利用者データのアクセス制御	CLD.9.5.1	→	CLD.9.5.1 CLD.9.5.2	cf. 13.1.3	CLD.9.5.1	←
10	暗号		仮想化を要する機能による暗号化のケースをカバーする				
10.1	暗号による管理策	10.1.1 10.1.2	×	10.1.1	10.1.1	10.1.1	10.1.1
11	物理的及び環境的セキュリティ	×	物理リソースは範囲外のため該当しない				
11.1	セキュリティを保つべき領域	×	—	—	—	—	—
11.2	装置	×	—	—	—	—	—
12	運用のセキュリティ		仮想化/仮想リソースに対するサービス事業者のオペレータ処理に焦点を当てている				
12.1	運用の手順及び責任	12.1.2 12.1.3	12.1.2 12.1.3	←	←	←	←
CLD.1	運用の手順及び責任	CLD.12.1.5	12.1.5	←	←	←	←

2.1							
12.2	マルウェアからの保護	×	—	—	—	—	—
12.3	バックアップ	12.3.1	→	→	→	12.3.1	←
12.4	ログ取得及び監視	12.4.1 12.4.3 12.4.4	12.4.1 12.4.4	←	←	←	←
CLD.12.4	ログ取得及び監視	CLD.12.4.5	12.4.5	←	←	←	←
12.5	運用ソフトウェアの管理	×	—	—	—	—	—
12.6	技術的ぜい弱性管理	12.6.1	12.6.1	←	←	←	←
12.7	情報システムの監査に対する考慮事項	×	—	—	—	—	—
13	通信のセキュリティ	×	ネットワークに焦点を当てたセキュリティ				
13.1	ネットワークセキュリティ管理	13.1.3	→	→	13.1.3	←	—
CLD.13.1	ネットワークセキュリティ管理	CLD.13.1.4	→	→	CLD.13.1.4	←	←
13.2	情報の転送	×	—	—	—	—	—
14	システムの取得、開発及び保守	×	技術モデルに直接関連しないため該当しない				
14.1	情報システムのセキュリティ要求事項	×	×	×	×	×	×
14.2	開発及びサポートプロセスにおけるセキュリティ	×	×	×	×	×	×
14.3	試験データ	×	—	—	—	—	—
15	供給者関係	×	技術事項ではないため該当しない				
15.1	供給者関係における情報セキュリティ	×	×	×	×	×	×
15.2	供給者のサービス提供の管理	×	—	—	—	—	—
16	情報セキュリティインシデント管理						
16.1	情報セキュリティインシデントの管理及び改善	16.1.2 16.1.7	→	→	→	→	16.1.2
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						
17.1	情報セキュリティ継続	×	×	×	×	×	×
17.2	冗長性	×	—	—	—	—	—
18	順守	×	技術事項ではないため該当しない				
18.1	法的及び契約上の要求事項の順守	×	×	×	×	×	×
18.2	情報セキュリティのレビュ	×	×	×	×	×	×

凡例　—：ISO/IEC 27017:201x においてクラウド事業者の管理策が規定されていない。

×：本書として技術面からの記載を必要としない。

→, ←：主に他の区分に記載される内容によって実装される。

管理策番号：本書において解説が加えられている。

【執筆者】

【編集】

クラウドサービス（IaaS）の技術的評価ガイド
JASA クラウドセキュリティ推進協議会（JCISPA）

平成
発　行：特定非営利活動法人日本セキュリティ監査協会
〒135-0016 東京都江東区東陽 3 丁目 23 番 21 号　プレミアム東陽町ビル
TEL 03-6675-3820 FAX 03-6675-3819 http://www.jasa.jp/