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

Information security management guidelines for the use of cloud computing services

2013 年度版

経 済 産 業 省

目　次

ページ

「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 2013 年度版」の公表にあたって

0.1 背景

「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」（以下，「初版」という。）の公表（2011 年 4 月 1 日）から約 2 年が経過した。この間，東日本大震災を背景とした事業継続の意識の高まり，政府機関並びに大手企業における情報セキュリティ事件・事故に伴う機密情報の流出及び大手金融機関における大規模システム障害の発生を契機にリスク対応の重要性が再認識されている。

クラウドサービスに着目すると，サービスの本格的な普及が進む中，国内外のクラウドサービスにおいて大規模な障害や障害対応過程における情報漏えいの発生など，リスクが顕在化した事例が見受けられるようになっている。一方，クラウドセキュリティに関する基準策定や国際標準策定が国内外で進められており，クラウドセキュリティに関する検討が深まっている。

クラウドサービスを取り巻くこのような環境の変化を踏まえ，「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 2013 年度版」（以下，「2013 年度版」という。）では，「クラウド利用者と事業者における信頼関係の強化に役立てる」ことに寄与するため，ガイドライン初版の内容を追補した。

0.2 2013 年度版のポイント

2013 年度版におけるポイントは次の 2 点である。

(1) 顕在化したリスクに対するセキュリティ要求事項の追加

昨今クラウドサービスにおいて顕在化したリスクを踏まえ，クラウド事業者に求められるセキュリティ要求事項を「クラウド事業者の実施が望まれる事項」に追加した。セキュリティ要求事項を明確化するにあたり，クラウドサービスにおける障害やトラブルなどのインシデント事例を分析するとともに，クラウド事業者に対してインタビュー調査を実施し，顕在化したリスクへの実際の対応及び自社では発生していないが想定されるリスクへの対応状況を調査した。

(2) 国際的な動向を踏まえた追補

クラウドサービスにおける情報セキュリティに関する国際会議などでの検討や海外政府の取組みなどの動向を踏まえて追補した。さらに，海外事業者へのインタビュー調査も踏まえて事業者の視点として反映した。

0.3 2013 年度版における追補の概要

(1) クラウドサービスにおける事業者の情報開示のあり方の反映

クラウドサービスの普及に伴い，クラウドサービスの本質に対する理解が深まっている。クラウドサービスの本質は，「標準的なサービスを多数の顧客に提供する」ことであり，従来のようなオンプレミスの情報システムの外部委託請負サービスとは異なるという点にある。2013 年度版では，次の考え方に基づき，初版の「クラウド利用者のための実施の手引」及び「クラウド事業者の実施が望まれる事項」を追補した。

a) 利用者への情報提供について事業者自らが方針を定めて利用者に提示し，利用者は提示された方

針及び方針に基づき提供された情報によってクラウドサービス利用に係るリスクを評価する。

b) クラウド事業者は，クラウド利用者との合意に基づき情報を開示する。

c) クラウド利用者には，クラウド事業者から情報を得た範囲で自らの責任においてリスクアセスメントを行い，対応や対策を決定する責任がある。

(2) 箇条書きへの変更

第三者評価などにおける客観的なチェックポイントをより明確にすべく，「クラウド利用者のための実施の手引」及び「クラウド事業者の実施が望まれる事項」において，箇条書きで示すことが適切な箇所については箇条書きに変更した。

(3) 例示の充実化

「クラウドサービスの関連情報」において，参考情報として例を示すことが有用な箇所については，クラウド事業者へのヒアリング調査なども踏まえて例示を充実させた。なお、参考情報の中に、『期待される』という表現で推奨事項を記載している。

序文

0.1　一般

クラウドコンピューティングは，「IT の所有」から「IT の利用」への転換を促すと予想され，その利用によって，組織が情報システムの構築・運用作業から解放されることが期待される。クラウドコンピューティングを利用することは，運用管理コストの低減，需要に応じた柔軟かつ迅速な調達に応えると同時に，大規模データ解析，最先端のアプリケーション利用が安価に実現できるため，IT 業界のみならず，農業や商業など，様々な業界からその普及，発展が期待されている。

そのような期待があるにもかかわらず，現時点で我が国でのクラウドコンピューティング利用は限定的である。その原因の一つとして，情報セキュリティに対する懸念がある。クラウドコンピューティングは，クラウド事業者の管理の下で他の利用者とコンピュータ資源を共有するため，情報の機密性・完全性・可用性にかかわる情報セキュリティについて懸念されているからである。

国内の組織の情報セキュリティには，国際的な規格（ISO/IEC 27002:2005）に準拠した JIS Q 27002:2006 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の実践のための規範（以下「JIS Q 27002（実践のための規範）」という。）に基づく管理策の実施が推奨されており，実際に多く利用されている。JIS Q 27002（実践のための規範）には，第三者の提供するサービスの利用に関する管理策があるが，組織が IT を所有せずに全面的にクラウドコンピューティングを利用する場合には，この管理策が求める事項だけでは組織の情報セキュリティを確保するためには不足があるのが実情である。

そのため，クラウド利用者の視点から JIS Q 27002（実践のための規範）の各管理策を再考し，クラウドコンピューティングを利用する組織においてこの規格に基づいた情報セキュリティ対策が円滑に行われることを目的として，このガイドラインを作成した。

このガイドラインには，組織がクラウドコンピューティングを全面的に利用する極限状態を想定し，①自ら行うべきこと，②クラウド事業者に対して求める必要のあること，さらに，③クラウドコンピューティング環境における情報セキュリティマネジメントの仕組みについて記載している。

組織において，このガイドラインを参考にクラウドコンピューティングに対応した情報セキュリティの仕組みを整備するとともに，クラウド利用者のみで行うことができない管理策を認識し，クラウド利用者がクラウド事業者に対して様々な情報を求める必要がある。

クラウド事業者においても，このガイドラインを参考に適切な情報を提供し，利用者との協力関係を向上することが望まれる。

このガイドラインの利活用によって，クラウド利用者がクラウドコンピューティングの利用にあった情報セキュリティ対策を実施し，クラウドコンピューティングの活用が促進されることが望まれる。

0.2　クラウドサービス及び情報セキュリティ

0.2.1　このガイドラインにおけるクラウドサービス及び情報とは何か

高速なネットワークの普及とともに，仮想化などの技術を利用してネットワーク上でコンピュータリソースを共有できるようになった。共有するコンピュータリソースは CPU，メモリ，ストレージ，ネットワーク，オペレーティングシステム，アプリケーションの実行環境，アプリケーション本体，データベースなど多岐にわたっており，組織内にコンピュータリソースをもつことなく，ネットワーク経由で様々な情

報処理サービスを利用できるようになった。

このガイドラインでは，クラウドコンピューティングを「共有化されたコンピュータリソース（サーバ，ストレージ，アプリケーションなど）について，利用者の要求に応じて適宜・適切に配分し，ネットワークを通じて提供することを可能とする情報処理形態」と定義し，クラウドサービスをネットワークサービスの一つとして取り扱う。

クラウドサービスの中で，CPU，メモリ，ストレージ，ネットワークなどをサービスとして提供するものを IaaS，オペレーティングシステム，データベース，開発環境，実行環境を提供するものを PaaS，すぐに使えるアプリケーションを提供するものを SaaS と定義する。IaaS，PaaS，SaaS の区分については，商業的に提供するクラウド事業者によって定義が異なることもあり，このガイドラインの中で詳細な定義をするものではない。提供するリソースを目安としてクラウドサービスを IaaS，PaaS，SaaS に分類している。

JIS Q 27002（実践のための規範）序文 0.2.1 によれば，情報は，紙に印刷若しくは手書きされ，電磁的に保存され，郵便若しくは電磁的な手段によって伝達され，映写され，又は会話として話されるなど，多くの形態で存在することができる。一方，クラウドコンピューティングにおいて情報は，電磁的に保存され，電磁的な手段によって伝達されるのであり，紙，郵便，会話などの非電磁的な形態で存在することはない。

クラウドサービス利用を前提とするこのガイドラインにおいては，電磁的な形態にある情報のみを取り扱う。

0.2.2　クラウドサービス利用のための情報セキュリティはなぜ必要か

JIS Q 27002（実践のための規範）序文 0.2.2 によれば，情報セキュリティマネジメントには，組織内のすべての従業員の参加が最低条件として要求されるが，外部組織の参加は必ずしも要求されない。「外部組織の参加が必要な場合もある」とされるにとどまる。

組織事業の基礎を成す情報資産の多くを組織内に保持しつつ，補完的に外部組織を利用する場合と，その大部分を組織内から外部組織に移行した場合とでは，情報セキュリティにかかわる主要なリスクの所在とコントロールの方法は全く異なった様相を呈する。前者の場合は，組織は自らリスクを検知して，それを直接コントロールすることができるのに対し，後者の場合は外部組織を介してリスクを検知し，外部組織にコントロールをゆだねる。つまり，組織は自らの事業の基礎を成す情報セキュリティを間接的にしかコントロールすることができない。したがって，この場合の情報セキュリティマネジメントには，組織内すべての従業員の参加だけでなく，それ以上に外部組織の何らかの関与が最低条件として要求されることになろう。

外部組織が提供するクラウドサービスを利用するということは，情報を取り扱うプロセス，システム並びにネットワークという情報資産を自組織の外部に置くことを意味する。クラウド利用者は，外部組織であるクラウド事業者からこれらの情報資産を利用できるサービスの提供を受け，これを利用して組織事業の基礎を成す情報の大部分を保存し又は処理するものとすれば，外部組織に依拠せずに情報セキュリティのマネジメントをすることはできない。これがクラウドサービス利用のための情報セキュリティが求められる理由である。

0.2.3　クラウド利用者がセキュリティ要求事項を確立する方法

JIS Q 27002（実践のための規範）序文 0.2.3 によれば，組織が組織自体のセキュリティ要求事項を導出する方法の一つに，以下を挙げている。

a) 一つには，組織全体における事業戦略及び目的を考慮して，組織に対するリスクアセスメントを実施することによって得られるものである。リスクアセスメントによって資産に対する脅威を特定し，事故に対するぜい弱性及び事故の可能性を評価し，潜在的な影響を推定する。

前述のとおり，クラウドサービスを利用して，組織事業の基礎を成す情報の多くを保存し又は処理する組織は，資産の多くをクラウド事業者に依拠している。したがって，上記 a）の方法によって組織自体のセキュリティ要求事項を導出しようとすれば，組織内の資産だけでなく，クラウド事業者内のクラウドサービスの提供にかかわる「資産に対する脅威を特定し，事故に対するぜい弱性及び事故の可能性を評価し，潜在的な影響を推定」することになる。

しかし，クラウド事業者はクラウド利用者とは独立した組織である。クラウドサービスの提供にかかわる資産に対する脅威，ぜい弱性及び事故の可能性の評価に資するような，何らかの情報を開示するかどうかは，専らクラウド事業者自らの事業判断にゆだねられている。

したがって，クラウド利用者がセキュリティ要求事項を確立するには，クラウド利用者自らが行うリスクアセスメントに必要な情報を指定して，その情報を開示するよう，クラウド事業者に対して協力を要請することが望まれる。

0.2.4　クラウド利用者の管理策の選択

JIS Q 27001:2006 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（以下「JIS Q 27001（要求事項）」という。）を活用した情報セキュリティマネジメントシステムを構築している多くの組織が存在する。JIS Q 27001（要求事項）を満たす情報セキュリティマネジメントによれば，組織は，リスクアセスメントを行い，情報セキュリティの要求事項及びリスクを識別し，リスク対応の決定に基づいて，識別されたリスクを受容可能なレベルにまで確実に低減するように管理策を選択する。組織がクラウドサービスを導入するならば，クラウド事業者からリスクアセスメントに必要な情報の開示を受けて，情報セキュリティの管理と責任の変化を検討することから始まり，管理策の選択と実施に至る（図 1 参照）。

管理策について JIS Q 27001（要求事項）は，JIS Q 27002（実践のための規範）の管理目的及び管理策を引用し，規格の一部を構成している。JIS Q 27002（実践のための規範）の箇条 5～15 は，JIS Q 27001（要求事項）の附属書 A.5～15 までに規定した管理策を支える，導入への助言と最適な実施のための手引となっている。

したがって，JIS Q 27002（実践のための規範）に基づいたクラウドサービス利用のための実施の手引があれば，組織はより簡便に管理策の選択を行うことができる。

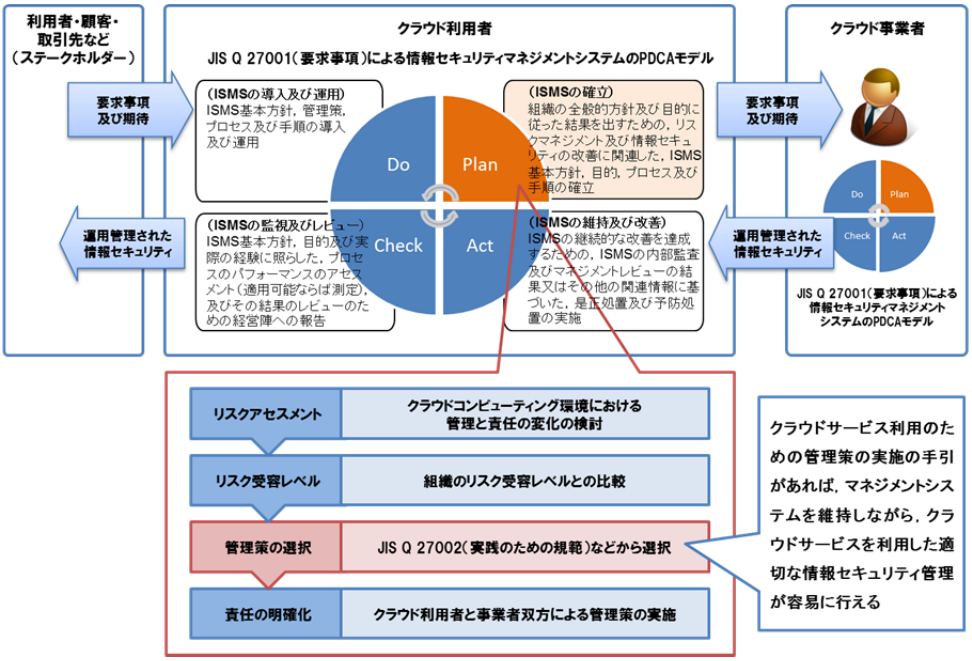

図 1　クラウドサービス利用にかかわる管理策の選択

0.3　このガイドラインの位置づけ及び構成

0.3.1　このガイドラインの位置づけ

このガイドラインは，クラウドサービスの利用にかかわるリスク対応のために JIS Q 27002（実践のための規範）から適切な管理策を選択し，導入するための助言とその最適な実施のための手引を提供する。JIS Q 27002（実践のための規範）がすべての組織に適用できることを意図しているのに対して，このガイドラインは，組織事業の基礎を成す情報資産の多くをクラウドサービスにゆだねる組織に適用できることを意図している。また，このガイドラインは JIS Q 27002（実践のための規範）の箇条 5～15 に記載された管理策の実施を支持し，管理目的を満たすための，クラウドサービス利用に着目した情報を提供する。

すなわち，このガイドラインは，JIS Q 27002（実践のための規範）に示された一般的原則の上に立ちながら，全面的にクラウドサービスを利用するという特殊な場合を想定するものである。

情報資産の多くを組織内に保持しつつ補完的にクラウドサービスを利用する場合には，組織内の情報資産については従来通りの管理策を実施し，クラウドサービス利用にかかわるプロセスについてはこのガイドラインを参考にして，適宜，必要となる管理策を選択することが望まれる。

0.3.2　このガイドラインの構成

このガイドラインの箇条 5～15 は，クラウド利用者が JIS Q 27002（実践のための規範）の箇条 5～15 の管理策を実施するための補足として活用できるように，次のように構成する。

目的

JIS Q 27002（実践のための規範）における目的をそのまま引用する。

管理策

JIS Q 27002（実践のための規範）における管理策をそのまま引用する。

クラウド利用者のための実施の手引

クラウドサービス利用において，クラウド利用者が実施する管理策を支持し，管理目的を満たすための情報を提供する。この手引にはすべての場合に適していないものもあるため，他の方法でその管理策を実施する方がより適切な場合もある。

クラウド事業者の実施が望まれる事項

クラウドサービス利用において，クラウド事業者の協力が必要となる管理策については，クラウド利用者が実施する管理策を支持し，管理目的を満たすために，クラウド事業者の実施が望まれる事項にかかわる情報を提供する。また，クラウド利用者が管理策を実施するにあたり事業者の協力が必要となる事項のみならず，クラウド事業者が自らの情報セキュリティマネジメントのために実施することが特に望まれる事項にかかわる情報についても提供する。

なお，クラウド事業者が実施する管理策として記載されている事項は，すべての場合に適していないものもあるため，他の方法でその管理策を実施する方がより適切な場合もある。

クラウドサービスの関連情報

クラウドサービス利用において考慮が必要と思われる関連情報（関連するクラウドサービスの種類，利用環境又は利用技術に関する情報など）を提供する。

なお，このガイドラインには，参考として附属書 A，B がある。附属書 A は，クラウドサービス利用にかかわるリスクを例示し，附属書 B は，クラウドサービス利用におけるリスクアセスメントの実施例の一つを示す。

1　適用範囲

このガイドラインは，次の 2 点を満たす組織に対して適用される。

(1) 組織事業の基礎を成す情報資産の多くを，外部組織であるクラウド事業者が提供するクラウドサービスにゆだねようとする組織が，

(2) JIS Q 27002（実践のための規範）に規定された管理目的を達成するための管理策を実施しようとする場合

このガイドラインは，クラウドサービス利用の観点から，JIS Q 27002（実践のための規範）の「実施の手引」を補足した「クラウド利用者のための実施の手引」を提供し，クラウド事業者の協力が必要となる場合には「クラウド事業者の実施が望まれる事項」を提供する。クラウドサービスを利用しても，一般にその実施には影響がないと思われる管理策や，現時点の技術水準又は社会的な合意が形成されていない現況においてその実施を望むことが現実的でないと思われる事項については，「クラウド利用者のための実施の手引」又は「クラウド事業者の実施が望まれる事項」には記載していない。

2　引用規格

次に掲げる規格は，このガイドラインに引用されることによって，このガイドラインの規定の一部である，「目的」及び「管理策」をそのまま構成する。引用規格のうちで，西暦年を付記してあるものは，記

載の年の版を適用し，その後の改正版（追補を含む。）には適用しない。

JIS Q 27002:2006　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の実践のための規範

注記　対応国際規格：ISO/IEC 17799:2005, Information technology―Security techniques―Code of practice for information security management （IDT）
なお，対応の程度を表す記号（IDT）は，ISO/IEC Guide 21 に基づき，一致していることを示す。

3　用語及び定義

このガイドラインで用いる主な用語及び定義は，次による。

3.1

資産 （asset）

組織にとって価値をもつもの（JIS Q13335-1:2006）。

3.2

可用性 （availability）

認可されたエンティティが要求したときに，アクセス及び使用が可能である特性（JIS Q13335-1:2006）。

3.3

クラウドコンピューティング（cloud computing）

共有化されたコンピュータリソース（サーバ，ストレージ，アプリケーションなど）について，利用者の要求に応じて適宜・適切に配分し，ネットワークを通じて提供することを可能とする情報処理形態。

注記　これよりも広い定義が使われることもある。

例 1　（クラウドコンピューティングの定義の例）

1) クラウドコンピューティングとは，「ネットワークを通じて，情報処理サービスを，必要に応じて提供／利用する」形の情報処理の仕組み（アーキテクチャ）をいう。（経済産業省，「クラウドコンピューティングと日本の競争力に関する研究会報告書」，2010 年 8 月 16 日）。

2) Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. (NIST, Special Publication 800-145 September 2011)

3.4

クラウドサービス（cloud service / cloud computing service）

クラウドコンピューティングを提供するサービス。

3.5

クラウド利用者 （cloud customer）

クラウドサービスを利用する組織。

3.6

クラウドサービスの利用者 （cloud user / cloud service user）

クラウド利用者（クラウドサービスを利用する組織）において，クラウドサービスを利用する者。

3.7

クラウド事業者 （cloud service provider）

クラウドサービスを提供する組織。ただし，クラウド事業者も，提供するサービスの様態によっては，クラウド利用者となる場合がある。

3.8

管理策 （control）

リスクを管理する手段（方針，手順，指針，実践又は組織構造を含む。）であり，実務管理的，技術的，経営的又は法的な性質をもつことがあるもの（JIS Q 27002:2006）。

3.9

指針 （guideline）

方針の中に設定された目標を達成するために成すべきこと及びその方法を明らかにした記述（JIS Q13335-1:2006）。

3.10

情報セキュリティガバナンス （information security governance）

社会的責任にも配慮したコーポレート・ガバナンスと，それを支えるメカニズムである内部統制の仕組みを，情報セキュリティの観点から企業内に構築・運用すること（経済産業省，「企業における情報セキュリティガバナンスのあり方に関する研究会報告書」，平成 17 年 3 月）。

3.11

機密性 （confidentiality）

認可されていない個人, エンティティ又はプロセスに対して, 情報を使用不可又は非公開にする特性（JIS Q13335-1:2006）。

3.12

情報処理設備 （information processing facilities）

情報処理のシステム，サービス若しくは基盤のいかなるもの，又はそれらを収納する物理的場所（JIS Q 27002:2006）。

3.13

情報セキュリティ （information security）

情報の機密性，完全性及び可用性を維持すること。さらに，真正性，責任追跡性，否認防止及び信頼性のような特性を維持することを含めてもよい（JIS Q 27002:2006）。

3.14

情報セキュリティ監査 （information security audit）

情報セキュリティにかかわるリスクのマネジメントが効果的に実施されるように，リスクアセスメントに基づく適切なコントロールの整備，運用状況を，情報セキュリティ監査を行う主体が独立かつ専門的な

立場から，国際的にも整合性のとれた基準に従って検証又は評価し，もって保証を与えあるいは助言を行う活動（経済産業省，「情報セキュリティ監査研究会報告書」，2003 年 3 月 26 日）。

3.15

情報セキュリティ事象 （information security event）

システム，サービス又はネットワークにおける特定の状態の発生。特定の状態とは，情報セキュリティ基本方針への違反若しくは管理策の不具合の可能性，又はセキュリティに関連するかもしれない未知の状況を示していることをいう（ISO/IEC TR 18044:2004）。

3.16

情報セキュリティインシデント （information security incident）

望まない単独若しくは一連の情報セキュリティ事象，又は予期しない単独若しくは一連の情報セキュリティ事象であって，事業運営を危うくする確率及び情報セキュリティを脅かす確率が高いもの（ISO/IEC TR 18044:2004）。

3.17

情報セキュリティマネジメントシステム，ISMS （information security management system）

マネジメントシステム全体の中で，事業リスクに対する取組み方に基づいて，情報セキュリティの確立，導入，運用，監視，レビュー，維持及び改善を担う部分（JIS Q 27001:2006）。

注記 マネジメントシステムには，組織の構造，方針，計画作成活動，責任，実践，手順，プロセス及び経営資源が含まれる。

3.18

IaaS （Infrastructure as a Service）

CPU，メモリ，ストレージ，ネットワークなどのハードウェア資産をサービスとして提供するクラウドサービス。

3.19

インフラ事業者 （infrastructure provider）

データセンター，ネットワークなどのインフラ資産を提供する事業者。

3.20

完全性 （integrity）

資産の正確さ及び完全さを保護する特性（JIS Q13335-1:2006）。

3.21

PaaS （Platform as a Service）

オペレーティングシステムや実行環境をサービスとして提供するクラウドサービス。

3.22

リスク （risk）

事象の発生確率と事象の結果との組合せ（TR Q 0008:2003）。

3.23

リスク分析 （risk analysis）

リスク因子を特定するための，及びリスクを算定するための情報の系統的使用（TR Q 0008:2003）。

3.24

リスクアセスメント （risk assessment）

リスク分析からリスク評価までのすべてのプロセス（TR Q 0008:2003）。

3.25

リスク評価 （risk evaluation）

リスクの重大さを決定するために，算定されたリスクを与えられたリスク基準と比較するプロセス（TR Q 0008:2003）。

3.26

リスクマネジメント （risk management）

リスクに関して組織を指揮し管理する調整された活動。

注記 リスクマネジメントは一般にリスクアセスメント，リスク対応，リスクの受容及びリスクコミュニケーションを含む（TR Q 0008:2003）。

3.27

リスク対応 （risk treatment）

リスクを変更させるための方策を，選択及び実施するプロセス（TR Q 0008:2003）。

3.28

SLA （Service Level Agreement）

書面にしたサービス提供者と顧客との合意であって，サービス及び合意したサービスレベルを記述したもの（JIS Q 20000-1:2007）

3.29

SaaS （Software as a Service）

アプリケーションやデータベースをサービスとして提供するクラウドサービス。

3.30

第三者 （third party）

当該問題に関して，当事者と無関係であると認められる個人又は団体（ISO/IEC Guide 2:1996）。

注記 第三者には，構造的に，クラウド事業者が利用するクラウド事業者も含まれる。

3.31

脅威 （threat）

システム又は組織に損害を与える可能性があるインシデントの潜在的な原因（JIS Q13335-1:2006）。

3.32

ぜい弱性 （vulnerability）

一つ以上の脅威がつけ込むことができる，資産又は資産グループがもつ弱点（JIS Q13335-1:2006）。

4 クラウドサービス利用における情報セキュリティガバナンス及び情報セキュリティマネジメント

4.1 クラウドサービス利用における情報セキュリティガバナンス

4.1.1　クラウドサービス利用がもたらす情報セキュリティガバナンスの変化

組織事業の基礎を成す情報及びその情報を取り扱うプロセス，システム並びにネットワークの多くを組織内に保持する場合，これらは経営陣によって管理できる。したがって，経営陣は，組織の情報セキュリティについて方向づけ（Direct）を与え，コミットメントを行い，PDCA の進捗・達成状況をモニタリング（Monitor）し，評価（Evaluate）し，利害関係者に報告（Report）することを通じて，組織の実効ある情報セキュリティガバナンスを確立することができる。

一方，クラウドサービス利用では，入力，演算，保存，出力という一連の情報処理プロセスのうち，主に入力と出力をクラウド利用者，演算と保存をクラウド事業者が分担するものとすれば，情報セキュリティガバナンスの主体は，互いに独立したクラウド利用者とクラウド事業者に分断される。

一般に，自組織の内部統制は，外部組織には及ばない。したがって，組織事業の基礎を成す情報資産の多くを外部組織にゆだねるクラウド利用者の経営陣は，組織の情報セキュリティにかかわる経営責任を全うすることができない。これを放置するならば，その組織の経営陣はその経営責任を，監査役はその監督責任を問われかねないため，情報セキュリティガバナンスは，クラウドサービスを利用するにあたって検討しなければならない大きな課題の一つとなっている。

4.1.2　クラウドサービス利用における情報セキュリティガバナンスのフレームワーク

クラウドサービス利用における情報セキュリティガバナンスの課題を解決するために，クラウド利用者とクラウド事業者の両経営陣がどのようなタスクを実施することが望ましいかを，情報セキュリティガバナンスのフレームワークで示されたモデルに従って示すことにする（図 2 参照）。

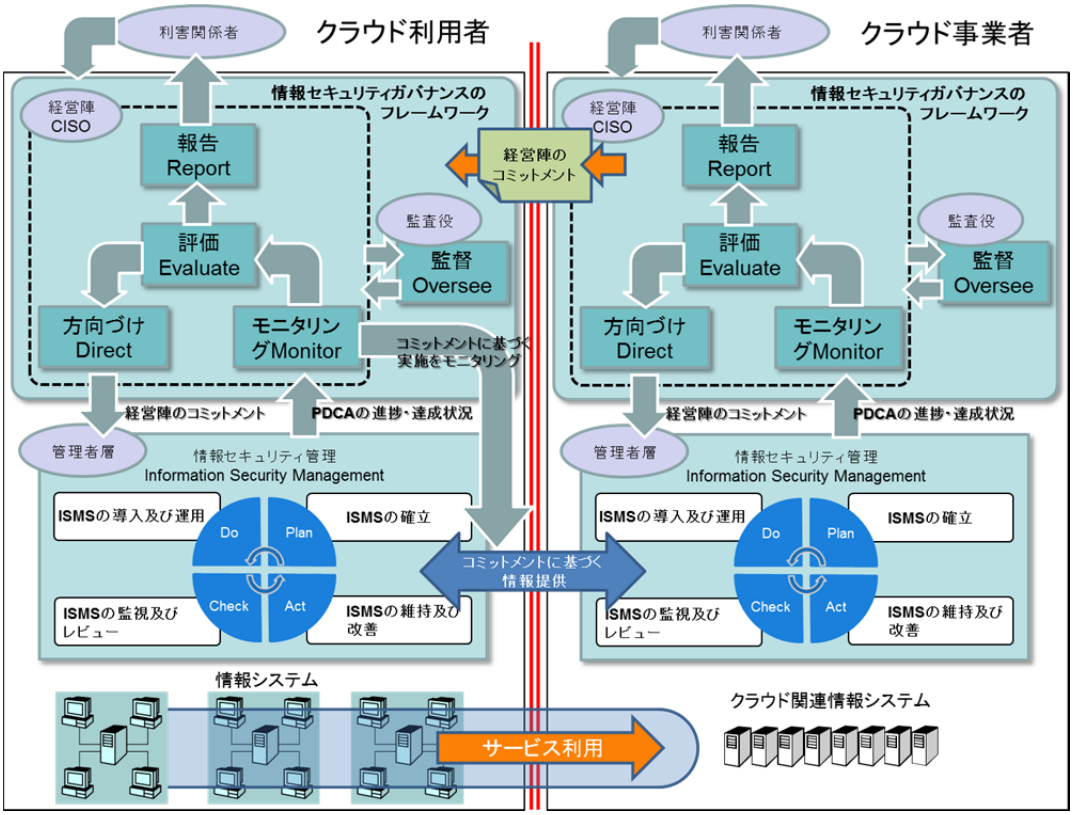

図 2　コミットメントに基づく情報セキュリティガバナンスのフレームワーク

クラウド事業者の経営陣は，クラウド利用者に対し，クラウドサービスの提供にかかわる情報セキュリティのガバナンス及びマネジメントに関するコミットメントを行う。このコミットメントはクラウド事業者の利害関係者たるクラウド利用者への報告（Report）の一部を成すが，一方的な報告ではなく，契約行為を含む双方向のコミットメントが望ましい。

このコミットメントに基づき，クラウド事業者はクラウド事業者の情報セキュリティガバナンスの報告（Report）を約束するとともに，クラウドの活動状況をクラウド利用者に提供することを約束する。

クラウド事業者によるクラウドの活動状況報告より，クラウド利用者は情報セキュリティ活動に必要な情報を入手し，理論的には自組織のシステムの延長のように，クラウドサービスを利用することが可能となる。例えば，クラウド利用者はクラウド事業者からクラウド事業者の情報セキュリティのマネジメントやコントロールにかかわる情報の提供を受け，これをクラウド利用者の点検（Check）の対象に含め，処置（Act）を検討する。処置にはクラウド利用者内で完結するものと，クラウド事業者による情報提供が必要なものがある。クラウド利用者は組織内で完結するものを解決するとともに，クラウド事業者による情報提供が必要な処置をクラウド事業者にフィードバックする。クラウド事業者は自組織内の処置（Act）に加え，クラウド利用者の要望である処置が可能かを検討する。

同様にクラウド利用者はクラウド事業者による情報提供を頼りに，クラウド利用者内の PDCA を実現できるようになる。もちろん，クラウド利用者とクラウド事業者は独立した経営主体であり，かつクラウド事業者は同時に多数のクラウド利用者から，時として矛盾する要望を受けることがあるので，おのずから情報提供の範囲には制約が生じ得る。クラウド利用者は，この制約を見定め受入れるか，又は別のクラウド事業者を求めるかの選択を迫られる場合もあるが，制約の存在を前提とした情報提供は可能であろう。

以上のような制約は存在するものの，一度クラウド利用者の PDCA サイクルが実現すると，クラウド利用者の経営陣の情報セキュリティガバナンス活動の基礎が形成される。クラウド利用者の経営陣は PDCA の進捗・達成状況をモニタリング（Monitor）することができるようになる。またクラウド利用者の経営陣は，クラウド事業者の経営陣から，彼らのコミットメントに基づく情報セキュリティガバナンス報告（Report）を受けることができる。クラウド利用者の経営陣は PDCA のモニタリング結果と，クラウド事業者の情報セキュリティガバナンス報告を基に評価（Evaluate）を行うとともに，クラウドを利用している組織としての報告（Report）を利害関係者に対して行うことができる。この利害関係者の中には，クラウド事業者も含まれる。この形態では，クラウド利用者の経営陣とクラウド事業者の経営陣は双方向に報告を行い，互いの状況を知ることとなる。

さらに，クラウド利用者の経営陣は評価（Evaluate）をベースに，情報セキュリティの経営陣のコミットメントとして，方向づけ（Direct）を行うことができる。この方向づけは，クラウド利用者の管理者の情報セキュリティ管理の入力となるとともに，一部はクラウド事業者への要望書となる。ここでもコミットメントに基づくクラウド利用者の限界が存在するが，クラウド利用者の経営陣の情報セキュリティガバナンス活動をベースとするクラウド事業者の経営陣への要望には，単なる PDCA に基づく要望以上の効力をもつと期待できる。クラウド利用者の経営陣は，方向づけの結果を，PDCA のモニタリングとクラウド事業者の情報セキュリティガバナンス報告から評価をし，最悪の場合，クラウド事業者を別に求めることになる。

以上の情報セキュリティガバナンスのフレームワークの有効性に対して監査役が監督（Oversee）を行う。

クラウド事業者の経営陣は，以上のコミットメントに基づくクラウド利用者に対する情報提供を可能とするための情報セキュリティガバナンスを確立していることをあらかじめ開示していることが望ましい。

4.2　クラウドサービス利用における情報セキュリティマネジメント

4.2.1　クラウドサービス利用におけるリスクアセスメントの留意点

JIS Q 27002（実践のための規範）4.1 によれば，リスクアセスメントは，セキュリティ要求事項及びリスク状況（例えば，資産，脅威，ぜい弱性，影響，リスク評価）の変化に対応できるように，定期的に及び重大な変化が発生したときに実施することが望ましい，とされている。つまり，リスクアセスメントでは，リスク状況の変化を把握することが重要である。

クラウドサービスを利用して組織事業の基礎を成す情報資産を組織内から外部組織に移行した場合には，次のようなリスク状況の変化に着目する必要がある。

クラウドコンピューティングで利用されている技術は，標準化された技術とは限らず，先進的な技術を自ら開発したクラウド事業者によってサービスが構築され，提供されている。そのため，当該事業者以外の専門家が対象技術そのものを評価し，ぜい弱性及び脅威を検証することは行われていない可能性があり，クラウドサービスを構成し，提供する技術そのものがぜい弱性を抱えているという懸念がある。クラウドサービスはクラウド利用者が機器構成内容や利用技術などを直接把握できず，これらの技術を客観的に検証することが難しいため，クラウドサービス上で問題が発生した際の対応計画を容易には構築できないということが情報セキュリティ上の問題とされている。

運用面においては，クラウド利用者とクラウド事業者との信頼関係や，データセンターの立地などにより，これまでのアウトソーシングに関連する情報セキュリティ問題だけではなく，コスト削減などに伴う情報管理の品質確保などの問題も併せて考慮しなければならない。

クラウドサービスを利用することにより直接管理できなくなったシステム，情報，監査ログなどを対象にして，情報セキュリティ対策の変化について検討することが望ましい。

また，クラウドサービスにかかわるリスクには，クラウド利用者自らが責任をもつにもかかわらず管理できない環境にある脅威及びぜい弱性が存在する。

例えば，クラウド利用者がクラウドサービスのすべての監査ログを入手することができないために，クラウドサービスの利用において問題が発生した場合，その原因を特定できず，再発防止のための対策を講じることができないというリスクが想定される。また，クラウドサービスの特徴であるマルチテナントの利用に起因するぜい弱性もある。自らの情報セキュリティ対策が十分であったとしても，実行環境となるゲスト OS が他のゲスト OS と同じハードウェア上に構成されている場合，他のゲスト OS が何らかの攻撃を受けた際に自らも不正アクセスや改ざんなどの被害を受ける可能性がある。

このようにシステムの管理主体がクラウド事業者にあることに起因して生じるぜい弱性については，クラウド利用者が技術的な対策を実施することが難しい。さらに，ネットワークに起因する脅威及びぜい弱性は，クラウドサービスに大きな影響を及ぼすリスクとなり得る。

4.2.2　クラウドサービス利用におけるマネジメントシステムの改善に向けた留意点

JIS Q 27001（要求事項）8.3 によれば，組織は，変化したリスクを特定し，大きく変化したリスクに注意を向けて，予防措置についての要求事項を特定しなければならない，とされている。情報セキュリティマネジメントシステムにおいては PDCA サイクルに基づいて，リスク状況の変化に伴う情報セキュリティ対策の見直しを行い，対策を検討することが求められている。

クラウドサービスではどのようなリスクの変化があり，どのような影響があるかを検討し，新たな情報セキュリティ対策の導入を計画することが望ましい。クラウドサービスの利用において変化するシステム環境，責任の所在，事故や事象の判断基準などを明確にすることで，適切なリスクマネジメントに向けた取組みが可能となる。

4.2.3　このガイドラインの情報セキュリティ監査への活用

JIS Q 27001（要求事項）を満たす情報セキュリティマネジメントによれば，点検（ISMS の監視及びレビュー）が要求される。クラウド事業者が適切な情報セキュリティ対策を実施しているかを点検するには，第三者の評価を利用することが効率的である。第三者の評価とは，情報セキュリティ関連の認定又は情報セキュリティ監査を指す。

しかしながら，クラウド事業者を国際的に認定する制度は整っておらず，これからのクラウド関連技術やビジネスモデルの発展を考慮すると，クラウド事業者に対する認定が実施されるのはまだ先になることが想定される。このような状況を踏まえると，情報セキュリティ監査によってクラウド事業者の情報セキュリティ管理状況の評価を知ることは有用だといえる。

このガイドラインはクラウド利用者が実施することが望ましい事項とクラウド事業者の実施が望まれる事項を示している。このガイドラインをクラウド利用者とクラウド事業者の両者が活用することにより，両者の関係において管理策が共有され，共有された管理策について情報セキュリティ監査を実施することができる（図 3 参照）。

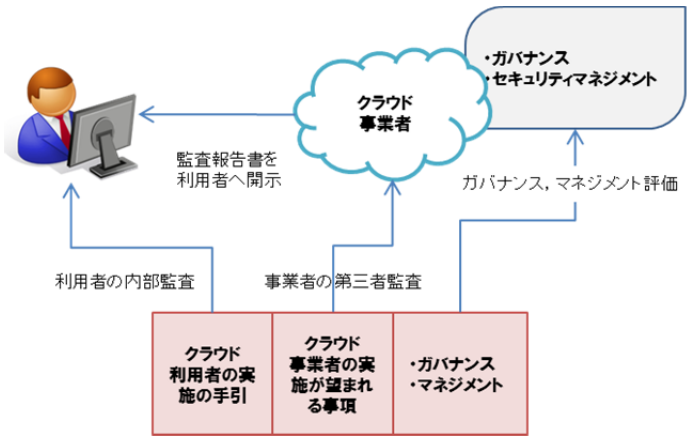

図 3　このガイドラインの監査への活用

4.2.4　このガイドラインのサプライチェーンへの活用

クラウドコンピューティングにおいては IaaS, PaaS 及び SaaS それぞれが関連しあってサプライチェー

ンを形成し，サービス全体を提供することがある。例えば，ある SaaS 事業者が PaaS 事業者のサービスを利用している場合，このガイドラインにおいては，その SaaS 事業者は PaaS の利用者となり，同様に PaaS 事業者が IaaS 事業者のクラウドサービスを利用している場合は，PaaS 事業者が IaaS の利用者となる。クラウドサービスを供給する側が利用する側に回ることで，サービスの供給と利用の連鎖が形成される（図 4 参照）。

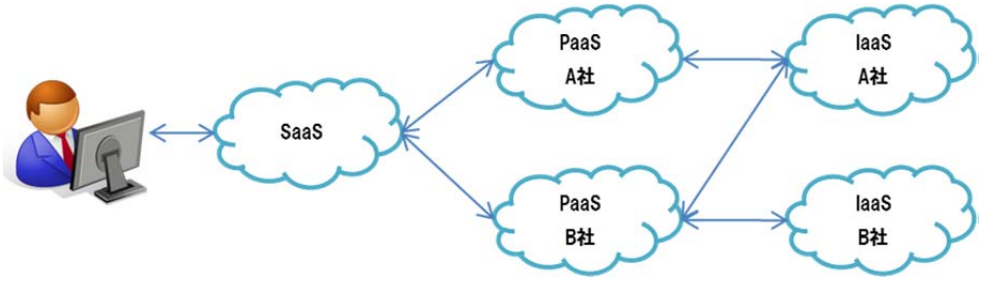

図 4　クラウド事業者のサプライチェーン

サプライチェーンを構成するクラウド事業者は自らの立場をクラウド利用者に置き換えて，このガイドラインの「クラウド利用者のための実施の手引」を自らの組織に活用できるだけでなく，「クラウド事業者の実施が望まれる事項」を自らが利用するクラウドサービスの供給者に対して要請し，サプライチェーンを形成するクラウド事業者の情報セキュリティマネジメントに活用することもできる。

5　セキュリティ基本方針

5.1　情報セキュリティ基本方針

目的：情報セキュリティのための経営陣の方向性及び支持を，事業上の要求事項，関連する法令及び規制に従って規定するため。

経営陣は，組織全体にわたる情報セキュリティ基本方針の発行及び維持を通じて，事業目的に沿った明確な情報セキュリティ基本方針の方向性を定め，情報セキュリティに対する支持及び責任を明示することが望ましい。

5.1.1　情報セキュリティ基本方針文書

管理策

情報セキュリティ基本方針文書は，経営陣によって承認され，全従業員及び関連する外部関係者に公表し，通知することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，組織の情報セキュリティ基本方針の適用範囲にクラウドコンピューティングの利用に関する事項を含めることが望ましい。クラウドコンピューティングの利用に関する情報セキュリティ基本方針は，リスクアセスメント及び次のような事項を考慮して定めることが望ましい。

a)　クラウドコンピューティング環境に保管するクラウド利用者組織の情報資産

b) クラウド事業者がアクセス及び管理するクラウド利用者組織の情報資産

c) クラウドコンピューティング環境においてクラウド利用者が実行するプロセス

d) クラウド利用者組織内のクラウドサービス利用者（一般利用者及び特権利用者）

クラウド利用者は，自らの情報セキュリティ基本方針とクラウド事業者の情報セキュリティ基本方針を比較し，その差異について検討することが望ましい。

クラウド利用者は，クラウド事業者が適切な情報セキュリティ基本方針に反しない管理を行っていることを確認し，その旨を経営陣（又は情報セキュリティ委員会）に報告することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，情報セキュリティ基本方針をクラウド利用者に明示することが望ましい。

クラウドサービスの関連情報

クラウド事業者の情報セキュリティ管理状況に関する第三者による評価結果（例えば，ISMS 認証取得証明書，外部監査報告書及び内部監査報告書など）や，情報セキュリティ管理に関する取組みについてクラウド事業者が提供する情報（例えば，ホワイトペーパーなど）は，クラウド事業者が情報セキュリティ基本方針に基づき適切な管理を行っていることを確認するための参考となり得る。

5.1.2 情報セキュリティ基本方針のレビュー

管理策

情報セキュリティ基本方針は，あらかじめ定められた間隔で，又は重大な変化が発生した場合に，それが引き続き適切，妥当及び有効であることを確実にするためにレビューすることが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービスを利用することによって重大な変化が発生する場合に，情報セキュリティ基本方針が引き続き適切，妥当及び有効であることを確実にするためにレビューすることが望ましい。特に情報の安全管理について，クラウドサービスの利用によって，自ら管理できない情報が存在する可能性を考慮して，情報セキュリティ基本方針の見直しを行うことが望ましい。

6 情報セキュリティのための組織

6.1 内部組織

目的：組織内の情報セキュリティを管理するため。

組織内において情報セキュリティを導入し，その実施状態を統制するための管理上の枠組みを確立することが望ましい。

経営陣は，情報セキュリティ基本方針を承認し，セキュリティに対する役割を割り当て，組織全体にわたるセキュリティの実施を調整し，レビューすることが望ましい。

必要ならば，専門的な情報セキュリティの助言の出所を明らかにし，組織内で利用できるようにすることが望ましい。業界の動向に遅れないようにし，規格及び評価方法に目を配り，情報セキュリティインシデントに対処するときの適切な連絡窓口を確保するために，関係当局を含む，外部のセキュリティ専門家又はその一団との連絡網を築くことが望ましい。情報セキュリティに対して多角的に取り組むことが望ま

しい。

6.1.1　情報セキュリティに対する経営陣の責任

管理策

経営陣は，情報セキュリティの責任に関する明りょうな方向づけ，自らの関与の明示，責任の明確な割当て及び承認を通して，組織内におけるセキュリティを積極的に支持することが望ましい。

クラウド利用者のための実施の手引

経営陣は，クラウドサービスの利用における情報セキュリティについて組織を横断する役割及び責任を明確にし，組織全体としての責任者を割当て，承認することが望ましい。

クラウドサービスの関連情報

クラウドサービスを利用した場合でも，情報セキュリティ管理全般に関するクラウド利用者の経営陣の責任は変化しない。しかしながら，クラウドサービスの内容（例えば，システム構成，契約内容など）を把握し，どのようなリスクが伴うのかについては，クラウド利用者の経営陣は十分に理解しておくことが期待される。クラウドサービスの利用における責任の所在が明確になるように，クラウド利用者の経営陣は情報システム環境の全体像を把握しておくことが期待される。

6.1.2　情報セキュリティの調整

管理策

情報セキュリティ活動は，組織の中の，関連する役割及び職務機能をもつ様々な部署の代表が，調整することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービス利用における組織の責任者を明確にし，情報セキュリティ委員会などの調整活動に参加させることが望ましい。クラウド利用者は，クラウドサービス利用における責任者を定め，情報セキュリティ管理者一覧などに追記することが望ましい。クラウドサービス利用におけるクラウド利用者の責任者は経営陣（又は情報セキュリティ委員会など）によって承認されることが望ましい。

クラウドサービスの関連情報

クラウドサービスの利用においては，情報システムの構築や利用に関する契約などが多者にわたる可能性があり，責任者を明確に決めて管理を行う必要がある。また，クラウドサービスに関する様々な情報を集約し様々な判断をする必要があるため，クラウドサービス利用における責任者は情報セキュリティ委員会などの組織の調整活動に参加することが期待される。

6.1.3　情報セキュリティ責任の割当て

管理策

すべての情報セキュリティ責任を，明確に定めることが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービス利用における情報セキュリティに関するクラウド利用者及びクラウド事業者の責任分界を確認することが望ましい。クラウド利用者は，情報セキュリティ責任について，クラウド利用者だけでは対応できない内容を明確にすることが望ましい。

クラウド利用者は，クラウド事業者の問合わせ窓口を確認し，窓口情報を最新に保つとともに，クラウ

ドサービス利用におけるリスクを識別・管理することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウド利用者，クラウド事業者及びインフラ事業者の間の責任分界を明確にし，文書化することが望ましい。

クラウド事業者は，クラウドサービスの情報セキュリティに関する窓口を明確にし，開示することが望ましい。

クラウドサービスの関連情報

クラウドサービスにおいては，情報セキュリティに関する一部の業務がクラウド事業者に委任される。しかしながら，情報セキュリティに関する全体の責任はクラウド利用者に残ったままであるため，クラウド事業者が情報セキュリティに関する業務を正しく実行していることを，クラウド利用者が判断することが期待される。また，個人が情報セキュリティに責任をもつ領域がクラウドサービスによって変化をする場合（例えば，ID 管理が一元化できずにパスワードの変更を個人が配慮して行わなければならないなど）には，クラウド利用者はその責任範囲を明確にし，クラウドサービスの利用者に伝えなければならない。

多くの場合には情報セキュリティ責任者は組織のすべての情報セキュリティに責任をもつが，クラウドサービスは多様性を有しており，これらのすべてを把握することは困難であることが想定される。このような場合は，情報セキュリティ責任者の補助としてクラウドセキュリティ責任者又は担当者を置くことを検討する必要がある。

データの管理責任，アクセス制御及びインフラ管理などに関する役割及び責任の定義が曖昧な場合，ビジネス上の若しくは法的な問題が引き起こされる恐れがある。

6.1.4　情報処理設備の認可プロセス

管理策

新しい情報処理設備に対する経営陣による認可プロセスを定め，実施することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，新たに利用する機器などを経営陣が認可するプロセスに，クラウドサービスを含めることが望ましい。クラウド利用者は，クラウドサービスの利用認可プロセスを策定することが望ましい。クラウド利用者は，クラウドサービスの利用認可プロセスを文書化することが望ましい。クラウドサービスの利用認可プロセスは，クラウド利用者の経営陣によって承認されることが望ましい。また，セキュリティ要求事項を満たしていることを確認するために情報セキュリティ委員会からも承認を得ることが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウド利用者がクラウドサービスの受入れを行うために必要な資料を作成し，提供することが望ましい。クラウド事業者は，SLA など，サービス開始前の合意事項を明確にすることが望ましい。クラウド事業者は， SLA など，サービス開始前の合意事項をクラウドサービスの利用を検討する者に明示することが望ましい。

クラウドサービスの関連情報

IaaS や PaaS の利用においては，既存の情報システム調達及び構築の標準や手順が適用可能な場合があ

る。SaaS では，アプリケーションのカスタマイズがクラウド利用者にとって容易ではないために，これまでの認可プロセスの標準に合致しない場合もある。その場合は，受入れについての標準や手順を再度検討し，標準の変更又は特例措置の検討を行う必要がある。

6.1.5　秘密保持契約

管理策

情報保護に対する組織の必要を反映する秘密保持契約又は守秘義務契約のための要求事項は，特定し，定めに従ってレビューすることが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，情報保護に対する組織の必要を反映する秘密保持契約をクラウド事業者と締結することが望ましい。クラウド利用者は，クラウド事業者との契約に必要な秘密保持契約の内容が含まれていることを確認することが望ましい。もし必要な事項が含まれていない場合は，別途，秘密保持契約を締結することが望ましい。クラウド利用者は，クラウド事業者との秘密保持契約に「保護される情報の定義」が記載されていることを確認することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウド利用者との契約時には秘密保持契約を締結することが望ましい。

クラウドサービスの関連情報

クラウドサービスの利用においてはコンピュータ資源をネットワーク上（多くの場合はクラウド事業者のデータセンター）に配置しているが，データの所在などをクラウド利用者が特定することは技術的に難しい。クラウド利用者がすべての情報を適切に管理するためにも，重要な情報を双方が正しく認識し，協力しあうことが期待される。

6.1.6　関係当局との連絡

管理策

関係当局との適切な連絡体制を維持することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウド事業者の監督官庁，管轄裁判所，関連団体，相談窓口などを確認することが望ましい。クラウド利用者は，利用するクラウド事業者の監督官庁，関連団体を調査し，事故発生時の連絡リストに追加することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，提供するクラウドサービスの情報セキュリティに関して関連する監督官庁などを明確にし，開示することが望ましい。クラウド事業者は，個人情報の保護に関して監督官庁などを明確にし，開示することが望ましい。

クラウドサービスの関連情報

クラウド利用者が複数のクラウド事業者と個別に契約し，複数のクラウドサービスを組み合わせて利用する場合には，それぞれのクラウド事業者の責任を明確にする必要がある。特に，様々なクラウドサービスを利用して一つのクラウドサービスとして提供する場合には，責任の切り分けが難しい場合もあるが，利用の前に責任分界点を明確にし，障害などに対応できるようにすることが期待される。

6.1.7　専門組織との連絡

管理策

情報セキュリティに関する研究会又は会議，及び情報セキュリティの専門家による協会・団体との適切な連絡体制を維持することが望ましい。

クラウドサービスの関連情報

クラウド利用者及びクラウド事業者は，次のような組織などを調査し，クラウドサービスに関する情報収集の対象とすることが期待される。

a) クラウドサービスを専門とする，又はクラウドサービスに関連する団体や組織
b) クラウドサービスの事業者団体
c) クラウドサービスに関連する省庁や団体
d) クラウドサービス関連のニュースソース

クラウドサービスでは，IaaS，PaaS，SaaS がサービスを共有して構成されている場合がある。例えば，複数の SaaS 事業者が同じ PaaS や IaaS を利用していたり，一つの SaaS 事業者が複数の PaaS を利用したりしている場合などがそれにあたる。この場合，クラウド事業者は，どのクラウド事業者のどのサービスを利用しているのかをクラウド利用者に開示することが望ましい。事前にこうした情報が開示されていれば，クラウド利用者は，あらかじめクラウドサービスやクラウド事業者の事故などが発生したときの影響と対策を検討することが可能になる。

6.1.8　情報セキュリティの独立したレビュー

管理策

情報セキュリティ及びその実施のマネジメントに対する組織の取組み（例えば，情報セキュリティのための管理目的，管理策，方針，プロセス，手順）について，あらかじめ計画した間隔で，又はセキュリティの実施に重大な変化が生じた場合に，独立したレビューを実施することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，情報セキュリティに関するマネジメントレビューにおいて，組織が保有する情報システムと同様に，クラウドサービスに関する事項を追加することが望ましい。クラウド利用者は，情報セキュリティに関するマネジメントレビューの計画書にクラウドサービスを追加することが望ましい。クラウド利用者は，リスクアセスメントに基づき，クラウドサービスを情報セキュリティ監査の対象に追加することが望ましい。

クラウドサービスの関連情報

クラウド利用者が，マネジメントレビューのための情報を提供する場合，クラウド事業者からクラウドサービスに関する情報を定期的に入手することが難しい場合がある。特にマルチテナントでクラウドサービスが展開されているクラウドサービスを利用している場合には，ログから得られる情報をクラウド事業者から提供してもらうために想定以上に時間を要する場合がある。そのため，事前にマネジメントレビューに必要な情報を精査し，それらの情報を得ることが可能であるかどうか，可能である場合は，必要な期間も併せてクラウド事業者に確認することが期待される。

6.2　外部組織

目的：外部組織によってアクセス，処理，通信，又は管理される組織の情報及び情報処理施設のセキュリティを維持するため。

外部組織の製品又はサービスの導入によって，組織の情報及び情報処理施設のセキュリティが弱められることは望ましくない。

外部組織による組織の情報処理施設へのアクセス，並びに情報の処理及び通信を管理することが望ましい。

組織の情報及び情報処理施設へのアクセスを要求する外部組織との活動が業務上必要となる場合，又は外部組織との間で製品及びサービスの受入れ若しくは提供を行う場合には，セキュリティ関連事項を決定し，要求事項を管理するためにリスクアセスメントを実施することが望ましい。管理策は，その外部組織との間で合意し，契約書に明記することが望ましい。

6.2.1　外部組織に関係したリスクの識別

管理策

外部組織がかかわる業務プロセスからの，組織の情報及び情報処理施設に対するリスクを識別し，また，外部組織にアクセスを許可する前に適切な管理策を実施することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，外部組織がかかわる業務プロセスの一つとしてクラウドサービスの利用を考慮することが望ましい。クラウド利用者は，業務プロセスへのクラウドサービスの関与と影響を特定することが望ましい。

クラウド利用者は，クラウドサービスの利用により生じる情報セキュリティに対するリスクを識別・検討し，必要に応じてクラウドサービスの利用を開始する前に管理策を実施することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウド利用者の情報セキュリティに重大な影響を与えると考えられるリスクを定義し，クラウド利用者にその情報を提供することが望ましい。

クラウド事業者がクラウド利用者と合意した場合，クラウド事業者は，クラウドサービスにおける情報セキュリティ対策や作業状況に関する情報（例えば，データの完全消去作業の実施報告書）を提供することが望ましい。

クラウドサービスの関連情報

クラウド事業者が開示する情報セキュリティ対策の内容は，多くの場合は限定的，抽象的なものであることに留意する。リスクを特定することが困難な場合に，クラウド利用者が実施できる有効な管理策の一つに情報の暗号化がある。

クラウド利用者は，組織の一般的な情報セキュリティリスクに加え，クラウド固有のリスクを情報セキュリティ リスクアセスメントプロセスの入力として含め，オンプレミスの情報システムとクラウドサービスとの間でリスクの違いを評価することが望ましい。なお，クラウドサービスにおいて考慮すべきリスクには次のようなものがある。

a) クラウド利用者の情報は，クラウド事業者が所有するハードウェアに格納されるため，クラウド

利用者は直接管理することができない。

b) クラウド事業者は，他のクラウド事業者が提供するクラウドサービスを利用してクラウドサービスを提供している場合があり，責任分界が曖昧である恐れがある。

c) 他のクラウド利用者と同一のコンピュータ環境を共用する場合があり，他のクラウド利用者の利用する環境との論理的な分割が適切に行われない恐れがある。

d) 一般的に，クラウドサービスの利用終了後，サービス利用中に使用されていたシステムリソースは再利用されるため，サービス利用終了後のデータ消去が適切に行われない場合，他のクラウド利用者によってデータがアクセスされる恐れがある。

情報セキュリティリスクは，クラウドサービスの利用によって高まる場合もあれば，低下する場合もある。クラウドサービスの利用においては，情報セキュリティ管理策の可視性及び情報セキュリティ管理レベルの達成度が限定されること，及び，リスクの識別が困難である傾向があることに留意する必要がある。

6.2.2 顧客対応におけるセキュリティ

管理策

顧客に組織の情報又は資産へのアクセスを許す前に，明確にしたすべてのセキュリティ要求事項を満たすように対処することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者が顧客に組織の情報又は資産へのアクセスを許可するために明確にしていたセキュリティ要求事項について，クラウドサービスを利用することによって変化するセキュティ要求事項を明確にし，明確にしたすべてのセキュリティ要求事項を満たすように対処することが望ましい。

クラウド利用者がセキュリティ要求事項の明確化を行うにあたっては，クラウドサービスの利用に伴い生じる顧客の作業及びリスクを識別することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド利用者が，クラウドサービスの利用に際してセキュリティ要求事項の順守状況を確認できるよう，クラウド事業者は，サービスの詳細に関する情報を提供することが望ましい。

クラウドサービスの関連情報

自らの顧客に内部統制報告の責任を負うクラウド利用者は，顧客に対して内部統制の報告を行うにあたり，クラウド事業者の情報セキュリティ監査報告書の入手が必要か否か，及び入手が可能かについてクラウドサービスの利用を開始する前に検討しておく必要がある。

クラウド利用者は，次の点について顧客に明示しておくことが期待される。

a) 個人情報保護法などの法令に基づき，利用者の同意なくクラウドコンピューティング環境上の情報への顧客のアクセスが制限される場合がある。

b) クラウド事業者は，他のクラウド利用者に情報が漏えいするリスクを完全に排除できない場合であっても，クラウド利用者に対してアクセスを付与する場合がある。

6.2.3 第三者との契約におけるセキュリティ

管理策

組織の情報若しくは情報処理施設が関係するアクセス・処理・通信・管理にかかわる第三者との契約，

又は情報処理施設に製品・サービスを追加する第三者との契約は，関連するすべてのセキュリティ要求事項を取り上げることが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，組織の情報若しくは情報処理施設が関係するアクセス・処理・通信・管理にかかわる第三者との契約，又は情報処理施設に製品・サービスを追加する第三者との契約に，クラウドサービスの利用契約が含まれるものとして考えることが望ましい。クラウド利用者は，クラウドサービスへのセキュリティ要求事項を明確化し，自組織のセキュリティ要求事項をすべて満たしているか，契約に含有されているかを確認する事が望ましい。また，クラウド事業者との契約を比較した結果が経営陣（又は情報セキュリティ委員会）に承認されていることが望ましい。

7　資産の管理

7.1　資産に対する責任

目的：組織の資産を適切に保護し，維持するため。

すべての資産を明らかにし，その管理責任者を指名することが望ましい。

管理責任者をすべての資産について明確にし，適切な管理策を維持する責任を割り当てることが望ましい。組織が適切と判断した場合には，管理責任者は具体的な管理策の実施を委任してもよいが，資産の適切な保護に関する責任は管理責任者にとどまる。

7.1.1　資産目録

管理策

すべての資産を明確に識別し，また，重要な資産すべての目録を作成し，維持することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドコンピューティング環境にある組織の資産を資産管理の適用範囲に含めることが望ましい。クラウド利用者は，資産目録にクラウドサービス名及びクラウド事業者名を追加することが望ましい。

クラウド利用者は，クラウド利用者による資産管理を支援する機能がクラウドサービスに付帯するかを確認することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウドコンピューティング環境にあるクラウド利用者の資産に関する資産目録の一覧を取得できる機能をクラウド利用者に提供することが望ましい。

クラウドサービスの関連情報

クラウド事業者は大規模な IaaS の上で PaaS や SaaS を展開している場合があり，クラウド利用者がクラウドサービスに関連するシステムのすべてを資産目録に詳細に記載することは困難である。また，データ管理のために様々なメタデータ（データに関する情報）などが付与されており，これらのすべてをクラウド利用者が管理することも困難である。しかしながら，クラウド利用者は，自らがクラウドコンピューティング環境においたデータやプログラムなどを資産目録に記載することは可能であり，これらをもれな

く記載することが期待される。

クラウドサービス環境にあるクラウド利用者の資産には，次のようなものがある。

a) 業務上の情報

b) 仮想化された装置

c) 仮想化されたストレージ

d) ソフトウェア

クラウド利用者の資産の種類はｑ，クラウドサービスに応じて多岐にわたる。例えば，SaaS 事業者が，提供する SaaS のインフラに IaaS を利用している場合，SaaS 事業者はクラウド利用者であり，SaaS において容量・能力及び資源などの監視・調整に使用するソフトウェアは，IaaS 事業者から見ると，自社の提供する IaaS サービス上にあるクラウド利用者の資産と解される場合がある。

7.1.2 資産の管理責任者

管理策

情報及び情報処理施設と関連する資産のすべてについて，組織の中に，その管理責任者を指定することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，資産目録の管理責任者の項目にクラウドサービスに関連する項目を追加することが望ましい。

資産の管理責任者は，クラウドコンピューティング環境上の資産に関して次の責任をもつことが望ましい。

a) 情報及び情報処理に関連する資産が適切に分類されていることを確実にする。

b) 複数のクラウドサービスを連携し情報処理を行う場合には，適切な処理を管理するための方針，プロセス及び手順を定め，定期的に見直す。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウドコンピューティング環境にあるクラウド利用者の資産の責任者を明確にし，顧客対応のエスカレーションプロセスに追加することが望ましい。

7.1.3 資産利用の許容範囲

管理策

情報及び情報処理施設と関連する資産の利用の許容範囲に関する規則は，明確にし，文書化し，実施することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，利用するクラウドサービスごとに，どの資産が利用可能か，リスクアセスメントを行い，利用の許容範囲を明確にすることが望ましい。クラウド利用者は，クラウドサービスごとに，資産の利用可能性について検討することが望ましい。

7.2 情報の分類

目的：情報の適切なレベルでの保護を確実にするため。

情報の必要性，優先順位及びその情報を取り扱う場合に期待する保護の程度を示すために，情報を分類することが望ましい。

情報の，取扱いに慎重を要する度合い及び重要性の度合いは様々である。情報によっては，保護レベルの引上げ又は特別な取扱いが必要なこともある。情報の分類体系は，一連の適切な保護レベルを定め，特別な取扱い方法の必要性を伝えるために利用することが望ましい。

7.2.1　分類の指針

管理策

情報は，組織に対しての価値，法的要求事項，取扱いに慎重を要する度合い及び重要性の観点から分類することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，情報分類の指針にクラウドサービスを考慮した分類項目を追加することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，データの分類項目を明示することが望ましい。クラウド事業者は，クラウドコンピューティング環境にあるクラウド利用者の情報がどのように分離されて管理されているかを明確にし，開示することが望ましい。

クラウドサービスの関連情報

データの分類項目の例として，以下のようなものがある。

－データのタイプ
－データ源の管轄裁判所
－コンテキスト（背景や位置づけなど）
－法的制約
－契約上の制約
－価値，機微性
－組織における重要度
－第三者による不正を防止する義務
－許可されない開示や誤用に関する事項
など

7.2.2　情報のラベル付け及び取扱い

管理策

情報に対するラベル付け及び取扱いに関する適切な一連の手順は，組織が採用した分類体系に従って策定し，実施することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービスで利用する資産についてもラベル付けやマーキングができる仕組みを作ることが望ましい。クラウド利用者は，ラベル付けやマーキングをクラウドサービスの利用者が実施できるように手順書を作成することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウドコンピューティング環境にあるクラウド利用者の情報を分類するためにフォルダ分類やラベル付け機能を提供することが望ましい。クラウド事業者は，クラウド利用者との合意に基づき，ラベル付け機能について次の情報を提供することが望ましい。

a) ラベル付けを行うための機能

b) ラベル付けのカスタマイズを行うための機能

クラウド事業者は，クラウドコンピューティング環境にあるクラウド利用者の情報を一時的に分類するためにマーキングなどの機能を提供することが望ましい。

クラウドサービスの関連情報

SaaS や PaaS では標準的なオペレーティングシステムではなく，クラウド事業者独自のオペレーティングシステムを利用している場合がある。その場合，情報管理において使い慣れたインタフェースを利用することができず，情報のラベル付けの手段で対応できないことがある。利用するクラウドサービスのインタフェースを正しく理解して，利用者が自らラベル付けやマーキングができるように手順を見直す必要がある。

8 人的資源のセキュリティ

8.1 雇用前

目的：従業員，契約相手及び第三者の利用者がその責任を理解し，求められている役割にふさわしいことを確実にするとともに，盗難，不正行為又は施設の不正使用のリスクを低減するため。

セキュリティの責任は，雇用に先立って，適切な職務定義書及び雇用条件において，言及することが望ましい。

従業員，契約相手及び第三者の利用者のすべての候補者について，十分に審査することが望ましい。特に，慎重を要する業務に就く者については，そうすることが望ましい。

従業員，契約相手及び情報処理施設の第三者の利用者は，セキュリティの役割及び責任についての契約書に署名することが望ましい。

8.1.1 役割及び責任

管理策

従業員，契約相手及び第三者の利用者のセキュリティの役割及び責任は，組織の情報セキュリティ基本方針に従って定め，文書化することが望ましい。

8.1.2 選考

管理策

従業員，契約相手及び第三者の利用者のすべての候補者についての経歴などの確認は，関連のある法令，規則及び倫理に従って行うことが望ましい。また，この確認は，事業上の要求事項，アクセスされる情報の分類及び認識されたリスクに応じて行われることが望ましい。

8.1.3 雇用条件

管理策

従業員，契約相手及び第三者の利用者は，契約上の義務の一部として，情報セキュリティに関する，これらの者の責任及び組織の責任を記載した雇用契約書に同意し，署名することが望ましい。

8.2　雇用期間中

目的：従業員，契約相手及び第三者の利用者の，情報セキュリティの脅威及び諸問題，並びに責任及び義務に対する認識を確実なものとし，通常の業務の中で組織の情報セキュリティ基本方針を維持し，人による誤りのリスクを低減できるようにすることを確実にするため。

経営陣の責任は，組織内の構成員全体にセキュリティを適用することを確実にするために，明確にすることが望ましい。

起こり得るセキュリティリスクを最小とするために，すべての従業員，契約相手及び第三者の利用者にセキュリティ手順及び情報処理設備の正しい利用方法に関する十分なレベルの意識，教育及び訓練を与えることが望ましい。セキュリティ違反の取扱いに関する正式な懲戒手続を設けることが望ましい。

8.2.1　経営陣の責任

管理策

経営陣は，組織の確立された方針及び手順に従ったセキュリティの適用を，従業員，契約相手及び第三者の利用者に要求することが望ましい。

8.2.2　情報セキュリティの意識向上，教育及び訓練

管理策

組織のすべての従業員，並びに，関係するならば，契約相手及び第三者の利用者は，職務に関連する組織の方針及び手順についての適切な意識向上のための教育・訓練を受け，また，定めに従ってそれを更新することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，組織のすべての従業員，契約相手及び第三者の利用者を対象にした教育・訓練の範囲に，組織が保有する情報システムと同様に，クラウドサービスの情報セキュリティに関する事項を加えることが望ましい。クラウド利用者は，クラウドサービスの利用において必要な職務に関連する組織に対して，クラウドサービス利用に関する情報セキュリティの方針及び手順について，適切な意識向上のための教育・訓練の内容を盛り込むことが望ましい。

クラウドサービスの情報セキュリティに関する教育・訓練は，利用者のリテラシーレベルや認知度に応じた内容とし，次のような内容を追加することが望ましい。

a) クラウドサービス利用のための方針，基準及び手順などの規程類
b) クラウドサービスごとの情報セキュリティリスク及びその対策
c) クラウドサービスを使用するにあたり考慮すべきシステム及びネットワーク環境におけるリスク

クラウド利用者は，組織におけるクラウドサービス利用に関する教育，訓練及び意識向上プログラムの実施にあたり，利用するクラウドサービスの操作マニュアル，予防措置及び連絡先に関する情報提供を，

必要に応じてクラウド事業者に要求することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウド利用者がクラウドサービスに関する情報セキュリティ教育，訓練及び意識向上プログラムを実施するにあたり，自社が提供するクラウドサービスの操作マニュアル及び連絡先情報を必要に応じて提供することが望ましい。

クラウドサービスの関連情報

クラウド利用者とクラウド事業者の作業が重複する点は，お互いにおいて，教育を行い，訓練を協調して行うことが期待される。

8.2.3 懲戒手続

管理策

セキュリティ違反を犯した従業員に対する正式な懲戒手続を備えることが望ましい。

クラウドサービスの関連情報

クラウド事業者は，クラウドサービスに携わる者を懲戒した場合に，利用者に情報セキュリティ上の影響がある場合は，懲戒の内容を連絡する必要があることに留意する。

8.3 雇用の終了又は変更

目的：従業員，契約相手及び第三者の利用者の組織からの離脱又は雇用の変更を所定の方法で行うことを確実にするため。

責任者は，従業員，契約相手及び第三者の利用者の組織からの離脱を管理し，すべての装置の返却及びすべてのアクセス権の解除の完了を確実にすることが望ましい。

組織内の責任及び雇用の変更は，この箇条に沿って対応する責任又は雇用の終了として管理することが望ましい。また，新規の雇用は，8.1 に示すとおりに管理することが望ましい。

8.3.1 雇用の終了又は変更に関する責任

管理策

雇用の終了又は変更の実施に関する責任は，明確に定め，割り当てることが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウドサービスの提供終了や事業終了に伴う義務を明確に定義することが望ましい。

8.3.2 資産の返却

管理策

すべての従業員，契約相手及び第三者の利用者は，雇用，契約又は合意の終了時に，自らが所持する組織の資産すべてを返却することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，すべての従業員，契約相手及び第三者の利用者が，雇用，契約又は合意の終了時に返却する自らが所持する組織の資産に，クラウドサービスを加えることが望ましい。クラウド利用者は，クラウドサービスの利用者が，雇用，契約又は合意の終了時に返却する資産をクラウド利用者が管理でき

る機能を，自らの資産の返却プロセスに組み込むことが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウドサービスにおいて，クラウドサービスの利用者が，雇用，契約又は合意の終了時に返却する資産を，クラウド利用者が管理できる機能を提供することが望ましい。また，そのような機能について，クラウドサービスの利用を検討する者に明示することが望ましい。

クラウドサービスの関連情報

クラウド利用者は，リモート環境から利用可能なクラウドサービスについては，資産の返却時期に特に留意する必要がある。

8.3.3　アクセス権の削除

管理策

すべての従業員，契約相手及び第三者の利用者の情報及び情報処理施設に対するアクセス権は，雇用，契約又は合意の終了時に削除し，また，変更に合わせて修正することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービスの利用者に対するアクセス権を，雇用，契約又は合意の終了時に削除し，また，変更に合わせて修正することを，自らのアクセス権の管理プロセスに組み込むことが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウドサービスの利用者に対するアクセス権を，クラウド利用者が，雇用，契約又は合意の終了時に削除し，また，変更に合わせて修正する機能を提供することが望ましい。また，そのような機能について，クラウドサービスの利用を検討する者に明示することが望ましい。

クラウドサービスの関連情報

クラウド利用者は，クラウド事業者との契約内容によっては，クラウドサービスの利用者との雇用，契約又は合意の終了後も，そのアクセス権を一定期間失効させることができない可能性があることに留意する必要がある。

9　物理的及び環境的セキュリティ

9.1　セキュリティを保つべき領域

目的：組織の施設及び情報に対する認可されていない物理的アクセス，損傷及び妨害を防止するため。

重要又は取扱いに慎重を要する情報処理設備は，適切なセキュリティ障壁及び入退管理を伴う明確なセキュリティ境界によって保護された，セキュリティが保たれた領域の中に設置することが望ましい。これらの設備は，認可されていないアクセス，損傷及び妨害から，物理的に保護することが望ましい。

取る保護は，識別されたリスクに相応することが望ましい。

9.1.1　物理的セキュリティ境界

管理策

情報及び情報処理施設のある領域を保護するために，物理的セキュリティ境界（例えば，壁，カード制

御による入口，有人の受付）を用いることが望ましい。

クラウドサービスの関連情報

クラウド事業者は，複数のデータセンターを利用する場合にセキュリティの保護に差異が生じないように留意し，物理セキュリティ境界を用いることが期待される。

クラウド事業者は，クラウド利用者に対する情報提供に伴う情報セキュリティリスクを考慮し，取扱いに慎重を要する情報が露見しないよう，物理的セキュリティ境界及び関連する管理策に関する情報（例えば，データセンターの所在地，物理的アクセスの管理策など）の開示範囲を決定する必要がある。

9.1.2　物理的入退管理策

管理策

セキュリティを保つべき領域は，認可された者だけにアクセスを許すことを確実にするために，適切な入退管理策によって保護することが望ましい。

クラウドサービスの関連情報

クラウド事業者は，データセンターなどの間でデータを交換する場合，共通の物理的入退管理策が講じられたセキュリティエリアでデータが交換される必要があることに注意を要する。

9.1.3　オフィス，部屋及び施設のセキュリティ

管理策

オフィス，部屋及び施設に対する物理的セキュリティを設計し，適用することが望ましい。

クラウドサービスの関連情報

クラウド事業者は，オフィス，部屋及び施設に対する物理的セキュリティに関する指針に差異が発生しないように留意することが期待される。

9.1.4　外部及び環境の脅威からの保護

管理策

火災，洪水，地震，爆発，暴力行為，及びその他の自然災害又は人的災害による被害からの物理的な保護を設計し，適用することが望ましい。

9.1.5　セキュリティを保つべき領域での作業

管理策

セキュリティを保つべき領域での作業に関する物理的な保護及び指針を設計し，適用することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービスを利用する場合に，セキュリティを保つべき領域が拡大しないか確認し，セキュリティを保つべき領域が拡大する場合は，作業に関する物理的な保護及び指針を設計し，適用することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウドサービスによって，クラウド利用者の利用環境を拡大させるような機能が存在する場合は，その機能を開示することが望ましい（例えば，モバイルコンピューティングからの利用が可能になる，など）。

9.1.6　一般の人の立寄り場所及び受渡場所

管理策

一般の人が立ち寄る場所（例えば，荷物などの受渡場所）及び敷地内の認可されていない者が立ち入ることもある場所を管理し，また，可能な場合には，認可されていないアクセスを避けるために，それらの場所を情報処理施設から離すことが望ましい。

クラウドサービスの関連情報

クラウド事業者は，データセンターなどの間でデータを交換する場合，一般の人の立寄り場所及び受渡場所に関する指針に差異が発生しないように留意することが期待される。

9.2　装置のセキュリティ

目的：資産の損失，損傷，盗難又は劣化，及び組織の活動に対する妨害を防止するため。

装置は，物理的及び環境的脅威から保護することが望ましい。

装置（構外で用いるもの及び移動するものを含む。）の保護は，情報への認可されていないアクセスのリスクを低減し，損失又は損傷から情報を保護するために必要である。装置の保護に関しては，装置の設置場所及び処分についても考慮することが望ましい。物理的な脅威から保護するため，また，サポート設備（例えば，電源，ケーブル配線施設）を保護するために，特別な管理策が要求される場合がある。

9.2.1　装置の設置及び保護

管理策

装置は，環境上の脅威及び災害からのリスク並びに認可されていないアクセスの機会を低減するように設置又は保護することが望ましい。

クラウドサービスの関連情報

クラウド事業者は，機器や，データセンターなどの間でデータを交換する場合，装置の設置及び保護の管理策に差異が発生しないよう留意することが期待される。

9.2.2　サポートユーティリティ

管理策

装置は，サポートユーティリティの不具合による，停電，その他の故障から保護することが望ましい。

クラウドサービスの関連情報

クラウド事業者は，機器や，データセンターなどの間でデータを交換する場合，サポートユーティリティの保護に差異が発生しないよう留意することが期待される。

9.2.3　ケーブル配線のセキュリティ

管理策

データを伝送する又は情報サービスをサポートする通信ケーブル及び電源ケーブルの配線は，傍受又は損傷から保護することが望ましい。

クラウドサービスの関連情報

クラウド事業者は，データセンター間でデータを交換する場合，データセンターごとのケーブル配線のセキュリティに差異が生じないように留意することが期待される。

9.2.4　装置の保守

管理策

装置は，可用性及び完全性を継続的に維持することを確実とするために，正しく保守することが望ましい。

クラウドサービスの関連情報

クラウド事業者は，データセンター間でデータを交換する場合，データセンターごとの保守の差異が生じないように留意することが期待される。

9.2.5　構外にある装置のセキュリティ

管理策

構外にある装置に対しては，構外での作業に伴った，構内での作業とは異なるリスクを考慮に入れて，セキュリティを適用することが望ましい。

9.2.6　装置の安全な処分又は再利用

管理策

記憶媒体を内蔵した装置は，処分する前に，取扱いに慎重を要するデータ及びライセンス供与されたソフトウェアを消去していること，又は問題が起きないように上書きしていることを確実にするために，すべてを点検することが望ましい。

クラウドの利用者のための実施の手引

クラウド利用者は，クラウドサービスの利用を終了した場合，使用されていた機器などが再利用されることに留意することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，バックアップを含め，取扱いに慎重を要するデータ及びライセンス供与されたソフトウェアを含む情報の取扱いに留意することが望ましい。クラウド事業者は，記憶媒体を内蔵した装置を処分する場合には，記録された情報を復元できないように安全に処分することが望ましい。また，記憶媒体を内蔵した装置を再利用する場合には，機密情報の漏えいに対する対策を実施することが望ましい。

9.2.7　資産の移動

管理策

装置，情報又はソフトウェアは，事前の認可なしでは，構外に持ち出さないことが望ましい。

クラウドの利用者のための実施の手引

クラウド利用者は，クラウドサービスでは，事前にクラウド利用者の許可なく，データの物理的な所在が移動される可能性があることに留意することが望ましい。

10　通信及び運用管理

10.1　運用の手順及び責任

目的：情報処理設備の正確，かつ，セキュリティを保った運用を確実にするため。

すべての情報処理設備の管理及び運用のための責任体制及び手順を確立することが望ましい。この手順

には，適切な操作手順の策定を含む。

不注意又は故意によるシステムの不正使用のリスクを低減するために，適切ならば，職務の分割を実施することが望ましい。

10.1.1 操作手順書

管理策

操作手順は，文書化し，維持していくことが望ましい。また，その手順は，必要とするすべての利用者に対して利用可能とすることが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，利用するクラウドサービスの操作手順を作成することが望ましい。クラウド利用者は，手順書作成にあたり，クラウド事業者の情報提供方針を確認することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウド利用者がクラウドサービスの操作手順を作成する際の情報提供に関する方針を定め，クラウド利用者に提示することが望ましい。クラウド事業者による情報提供の例として，次のようなものがある。

a) 利用者向け操作手順書の提示

b) 問合せ窓口

クラウドサービスの関連情報

クラウド利用者は，クラウドサービスの環境においては，サービスの変更が一斉に行われ，操作手順の変更が発生する可能性があることに留意することが期待される。

クラウド利用者が他のクラウドサービスを利用して内部又は外部の利用者にサービスを提供する場合（例えば，IaaS を利用して SaaS を提供する場合など），クラウド利用者は，サービス仕様及びサービスレベルの提供を維持するためにクラウド事業者に対して，システム及びサービスに関する変更情報を要求することが想定される。

10.1.2 変更管理

管理策

情報処理設備及びシステムの変更は，管理することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウド事業者からクラウド利用者に影響が及ぶ情報処理設備及びシステムの変更の通知を受けた場合は，その影響を確認し，記録することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウドサービスの情報処理設備及びシステムの変更において，クラウド利用者に影響を及ぼすものをあらかじめ定義し，クラウド利用者に通知することが望ましい。クラウド事業者は，クラウドサービスの情報処理設備及びシステムの変更においてクラウド利用者に通知する項目並びに変更履歴を，クラウドサービスの利用を検討する者及びクラウド利用者に明示することが望ましい。

クラウドサービスの関連情報

クラウド利用者は，クラウドサービスの環境においては，情報処理設備及びシステムの変更が一斉に行

われ，個別の環境や条件が考慮されない可能性に留意することが望ましい。クラウド利用者，クラウド事業者ともに，IaaS などで利用される仮想化環境では，資産調達と連動せずに機器（例えば，仮想マシンなど）やソフトウェアのライセンスなどの追加が可能になることに留意することが期待される。

クラウド事業者がクラウド利用者に通知する項目の例として，次のようなものがある。

a) システム変更の実施予定日時

b) システム変更の内容

- 新規ソフトウェアのインストール又はパッチの適用
- ハードウェア変更
- ネットワーク変更
- ソフトウェア変更
- サービスの変更
- サブプロバイダの変更
- システムの物理的な移動

c) 変更に関するリスク評価

d) システム変更の開始及び完了の通知

e) 事前の取決めに基づく確認又は承認

10.1.3 職務の分割

管理策

職務及び責任範囲は，組織の資産に対する，認可されていない若しくは意図しない変更又は不正使用の危険性を低減するために，分割することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービスにおいて，組織の資産に対する，認可されていない又は意図しない変更又は不正使用の危険性を低減するために，分割すべき職務及び責任範囲を特定し，分割することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，提供するクラウドサービスにおいて，組織の資産に対する，認可されていない又は意図しない変更又は不正使用の危険性を低減するために，クラウド利用者において分割することが望ましい職務及び責任範囲（例えば，ID の使用者と登録者など）を明示することが望ましい。

クラウドサービスの関連情報

クラウドサービスにおいては，クラウド利用者にとって重要な処理であっても，職務の分割が技術的に実装されていない場合は，クラウド利用者は，職務の分割を運用で実装することが求められる場合がある。

10.1.4 開発施設，試験施設及び運用施設の分離

管理策

開発施設，試験施設及び運用施設は，運用システムへの認可されていないアクセス又は変更によるリスクを低減するために，分離することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，開発，試験及び運用環境を分離するため，必要に応じて仮想環境を利用することが望ましい。

クラウドサービスの関連情報

クラウド利用者は，クラウドサービスの環境においては，開発施設，試験施設及び運用施設の分離が，物理的に困難である可能性に留意することが期待される。

10.2 第三者が提供するサービスの管理

目的：第三者の提供するサービスに関する合意に沿った，情報セキュリティ及びサービスの適切なレベルを実現し，維持するため。

組織は，提供されるサービスが第三者と同意したすべての要求事項を満たしていることを確実にするために，合意の実施状況を点検し，その合意への順守状況を監視し，また，順守状況の変化を管理することが望ましい。

10.2.1 第三者が提供するサービス

管理策

第三者が提供するサービスに関する合意に含まれる，セキュリティ管理策，サービスの定義及び提供サービスレベルが，第三者によって実施，運用及び維持されることを確実にすることが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービスにおいて，クラウド事業者が，第三者（クラウドサービスを構成するためのネットワークを提供するプロバイダや関係するほかのクラウド事業者など。以下同じ。）が提供するサービスに関する合意に含まれる，セキュリティ管理策，サービスの定義及び提供サービスレベルが，クラウド事業者によって実施，運用及び維持されることを，確実にしていることを確認することが望ましい。クラウド利用者は，クラウド事業者が，第三者が提供するサービスに関する合意に含まれる，セキュリティ管理策，サービスの定義及び提供サービスレベルによって，クラウド利用者が影響を受ける可能性についてあらかじめ考慮していることが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，提供しているクラウドサービスにおいて利用している第三者が提供するサービスのうち，利用者の情報セキュリティ管理に影響のあるものを開示することが望ましい。

クラウド事業者は，第三者が提供するサービスにおけるセキュリティ管理策，サービスの定義及びサービスレベルをクラウド利用者が定期的にレビューできるよう，必要に応じて次のような情報を提供することが望ましい。

a) 情報セキュリティに係るサービス運用報告書
b) 情報セキュリティに係る監査報告書
c) サービスレベル報告書

クラウド事業者は，提供するクラウドサービスがサプライチェーンを形成する場合には，リスク管理に関する目標を他の事業者に提示し，各事業者に対してリスク管理の実施及び目標の達成を求めることが望ましい。

クラウドサービスの関連情報

クラウド利用者は，クラウドサービスの環境においては，様々な階層のサービスが複雑に作用するため，クラウド事業者の提供するクラウドサービスが特に依存する第三者サービスがないか（例えば，第三者のPaaS を利用した SaaS サービスであるか，など）留意することが期待される。

クラウド事業者は，クラウドサービスの環境においては，様々な階層のサービスが複雑に作用するため，お互いに実施したり，協同で実施したりすべきことに留意し，円滑な運用を図ることが期待される。

10.2.2 第三者が提供するサービスの監視及びレビュー

管理策

第三者が提供するサービス，報告及び記録は，常に監視し，レビューすることが望ましい。また，監査も定期的に実施することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービスにおいて，クラウド事業者によって，第三者が提供するサービス，報告及び記録が，常に監視され，レビューされていることを確認することが望ましい。クラウド利用者は，クラウドサービスにおいて，クラウド事業者によって，第三者が提供するサービスが，監査されていることを確認することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，提供しているクラウドサービスについて，クラウド利用者に対して次のような情報提供を必要に応じて行うことが望ましい。

d) 第三者が提供するサービス，報告及び記録を，常に監視し，レビューしていることの開示
e) 第三者が提供するサービス，報告及び記録を，常に監視し，レビューした記録の明示
f) 第三者が提供するサービスを監査していることの開示
g) 第三者が提供するサービスを監査した結果をまとめた報告書などの提示

クラウドサービスの関連情報

クラウド利用者は，クラウドサービスの環境においては，様々な階層のサービスが複雑に作用するため，クラウドサービスが連鎖していること（例えば，IaaS を利用した PaaS を利用した SaaS サービスである，など）に留意することが期待される。

10.2.3 第三者が提供するサービスの変更に対する管理

管理策

関連する業務システム及び業務プロセスの重要性，並びにリスクの再評価を考慮して，サービス提供の変更（現行の情報セキュリティ方針，手順及び管理策の保守・改善を含む。）を管理することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービスにおいて，クラウド事業者の利用する第三者のサービス提供の変更が影響を及ぼす可能性を確認することが望ましい。

クラウド利用者は，組織の情報セキュリティに影響を与える可能性のあるクラウド事業者の利用する第三者のサービス提供の変更について，クラウド利用者の変更管理プロセスに基づき，必要な対応を実施することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウドサービスにおいて，第三者のサービス提供の変更による影響を管理することが望ましい。

クラウド事業者は，組織の情報セキュリティに影響を与える可能性のある，クラウド事業者の利用する第三者のサービス提供の変更について，クラウド利用者への通知の方針を定め，クラウド利用者に通知することが望ましい。

クラウドサービスの関連情報

クラウド事業者が，第三者のサービスの変更に関してクラウド利用者に通知する事項の例として，次のようなものがある。

a) システム変更の実施予定日時
b) システム変更の内容
c) 変更に関するリスク評価
d) システム変更の開始及び完了の通知
e) 事前の取決めに基づく確認又は承認

クラウド利用者は，クラウドサービスの環境においては，様々な階層のサービスが複雑に作用するため，クラウドサービスが連鎖していること（例えば，IaaS を利用した PaaS を利用した SaaS サービスである，など）に留意することが期待される。

10.3 システムの計画作成及び受入れ

目的：システム故障のリスクを最小限に抑えるため。

必要とされるシステム性能を満たす十分な容量及び資源の可用性を確実にするためには，事前の計画及び準備を行う必要がある。

システムの過負荷のリスクを低減するために，将来の容量・能力の要求を予測することが望ましい。新しいシステムの運用上の要求事項を，その受入れ及び利用に先立って，設定し，文書化し，試験することが望ましい。

10.3.1 容量・能力の管理

管理策

要求されたシステム性能を満たすことを確実にするために，資源の利用を監視・調整し，また，将来必要とする容量・能力を予測することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，要求されるシステム性能を満たすことを確実にするために，次の事項を実施することが望ましい。

a) クラウドサービスにおける容量・能力の限界値を把握する。
b) クラウドサービスにおける容量・能力の限界値が，要求されるシステム性能を満たすことを確認する。
c) クラウドサービスにおいて，資源の利用を監視・調整する仕組みがあることを確認し，現状の資

源の利用を監視・調整する仕組みに組み込む。

クラウド利用者は，将来必要とする容量・能力を予測する仕組みに，クラウドサービスを組み込むことが望ましい。クラウド利用者は，クラウドサービスの環境においては，契約形態に応じた容量・能力の割当ての変更や，容量・能力の利用に応じた課金について留意することが望ましい。クラウド利用者は，クラウドサービスの容量・能力の追加が，容易にできるか確認することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，重大なインシデントを防ぐために，物理的な容量・能力の全体量を考慮して仮想化されたコンピューティング資源の全体量を監視し，適切に管理することが望ましい。

クラウド事業者は，クラウドサービスにおいて，システム全体の容量・能力の限界値及びクラウド利用者に割り当てられる容量・能力の限界値を把握することが望ましい。

クラウドサービスの関連情報

10.3.2 クラウドサービスによっては，CPU 利用率などの急激な上昇・降下が発生し，サービスの安定稼働に影響を及ぼす場合がある。このような事象は原因を特定できないことも多く，特定のしきい値を設けた監視による完全な予測や事前対応が難しい。そのため，クラウド利用者は，クラウドサービスにおける CPU 利用率などの急激な上昇・降下に伴うリスクを評価した上でクラウドサービスを利用することが期待される。一方，クラウド事業者は，そのようなリスクをクラウド利用者が識別・評価できるよう，あらかじめ示しておくことが期待される。システムの受入れ管理策

新しい情報システム及びその改訂版・更新版の受入れ基準を確立し，また，開発中及びその受入れ前に適切なシステム試験を実施することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，新規のクラウドサービスや，利用中のクラウドサービスの改訂版・更新版に関して，受入れ基準を確立し，開発中及びその受入れ前にシステム試験を実施し，結果をクラウド事業者に通知することが望ましい。

クラウド利用者は，クラウドサービスの選定にあたり，クラウド事業者に対して次の情報を求めることが望ましい。

a) SLA（アクセスネットワークの容量・能力及び冗長化を含む）

b) 試用に関する詳細（料金，試用期間及び免責事項を含む）

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウドサービスの改訂版・更新版の提供プロセスを，クラウド利用者に明示することが望ましい。クラウド事業者は，クラウドサービスにおいて，クラウド利用者へ改訂版・更新版の受入れ準備のための期間を提供することが望ましい（例えば，通知後一週間で運用環境に適用する，など）。クラウド事業者は，クラウド利用者が円滑にクラウドサービスの改訂版・更新版へ移行できるように，旧版との併用ができる期間を設けることが望ましい。

クラウドサービスの関連情報

クラウド利用者は，クラウドサービスにおいて，新しい情報システム及びその改訂版・更新版の提供は，

クラウド事業者によって，不定期に行われる可能性があることに留意することが期待される。

10.4 悪意のあるコード及びモバイルコードからの保護

目的：ソフトウェア及び情報の完全性を保護するため。

悪意のあるコード及び認可されていないモバイルコードの侵入を防止し，検出するために予防対策が必要となる。

ソフトウェア及び情報処理設備は，悪意のあるコード（例えば，コンピュータウィルス，ネットワークワーム，トロイの木馬，ロジック爆弾，スパイウェア）に対してぜい弱である。利用者には，悪意のあるコードの危険性を知らせることが望ましい。管理者は，適切な場合には，悪意のあるコードを防止し，検知し，取り除くための管理策を導入することが望ましく，また，モバイルコードを管理することが望ましい。

10.4.1 悪意のあるコードに対する管理策

管理策

悪意のあるコードから保護するために，検出，予防及び回復のための管理策，並びに利用者に適切に意識させるための手順を実施することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，悪意のあるコードから情報やシステムを保護するために，検出，予防及び回復のための管理策だけでなく，クラウドサービスの利用者に対してクラウドサービス利用時の考慮事項を適切に意識させるための手順を策定して，実施することが望ましい。

クラウド利用者は，クラウドサービスにおいて，クラウド事業者が，悪意のあるコードからクラウド利用者を保護するために実施している次のような事項を確認することが望ましい。

a) 悪意のあるコードの検出，予防及び回復のための管理策

b) 悪意のあるコード及びその対策・対応について，クラウド利用者に適切に意識させるために実施している管理策とその実行結果

c) 悪意のあるコードに感染した場合のクラウド事業者における報告手順

クラウド利用者は，組織が実施している悪意のあるコード対策とクラウド事業者の悪意のあるコード対策を併せてリスク評価し，必要に応じて自ら追加の対策を実施することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウドサービスの提供において，悪意のあるコードへのクラウド事業者の責任範囲と，クラウド利用者の責任範囲を明らかにすることが望ましい。クラウド事業者は，クラウドサービス内で，悪意のあるコードからクラウドサービスの利用者を保護するために，検出，予防及び回復のための管理策を実施し，また，クラウド利用者に適切に意識させるための手順を実施することが望ましい。

クラウドサービスの関連情報

クラウドサービスを構成する環境においては，様々な階層のサービスが複雑に関連するため，それぞれの階層において，悪意のあるコードへの独自の対策が行われている可能性がある。そのため，クラウド利用者とクラウド事業者は，それぞれの階層における対策方式や検出精度の違いから検出結果の違いが発生

する可能性に留意する必要がある。クラウド事業者は，ウイルス対策製品を導入した場合，パフォーマンスの問題や，可用性に影響を生じさせることに留意する必要がある。

10.4.2 モバイルコードに対する管理策

管理策

モバイルコードの利用が認可された場合は，認可されたモバイルコードが，明確に定められたセキュリティ方針に従って動作することを確実にする環境設定を行うことが望ましい。また，認可されていないモバイルコードを実行できないようにすることが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，マルウェア感染の拡大を防ぐため，特定のクラウド利用者に対するサービスの停止を含むモバイルコード利用の方針を定めることが望ましい。また，クラウド事業者は，クラウドサービスにおけるモバイルコード利用の方針をクラウド利用者に提示し，方針に対する協力を求めることが望ましい。

クラウドサービスの関連情報

クラウド事業者は，クラウドサービスにおいてモバイルコードを利用する場合，利用の可否をクラウド利用者が判断し，認可できるような仕組みを提示し，認可されたモバイルコードが，明確に定められたセキュリティ方針に従って動作することを確実にする方法をクラウド利用者に明示することが期待される。また，同時に，クラウド事業者は，クラウドサービスの環境において，認可されていないモバイルコードを実行できないようにする方法を，クラウド利用者に明示することが期待される。

クラウド利用者は，悪意のあるコードに関する次のような事項について，クラウド事業者の情報提供方針を確認することが期待される。

a) セキュリティ関連の設定及び使用されているオプション
b) セキュリティ管理策及び対象システムコンポーネント（例えば，ネットワーク，ゲスト OS レイヤなど）
c) ソフトウェア更新・パッチ適用に関するスケジュール及び情報（例えば，パッチの種類，パッチ適用の頻度及び対象システムなど）
d) ぜい弱性の検出，報告及び改善のための基準及び手順（例えば，ベンダーの公開情報，侵入テストツールなど）
e) 隣接する VM や VMM（Virtual Machine Monitor，仮想マシンモニタ／ハイパーバイザー）などの異なるクラウドコンポーネントの感染に備えたインシデント対応手順及び復旧手順
f) 利用者側で実装すべき悪意のあるコード対策
g) サービスレベル報告書に含まれる内容
   - 未対応のぜい弱性に関するパッチ情報及び管理策
   - 補完的統制に関する情報
   - 特定のぜい弱性に関する情報及び傾向（例えば，仮想化レイヤなどに対するぜい弱性の分類及び重要度スコアなど）

10.5 バックアップ

目的：情報及び情報処理設備の完全性及び可用性を維持するため。

データのバックアップ取得と時機を失しないデータ復旧の訓練とに関する，合意されたバックアップ方針及び戦略（14.1 参照）を実施するために，日常の作業手順を確立することが望ましい。

10.5.1 情報のバックアップ

管理策

情報及びソフトウェアのバックアップは，合意されたバックアップ方針に従って定期的に取得し，検査することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービス上で扱う情報，ソフトウェア及びソフトウェアの設定において，バックアップの必要性を確認することが望ましい。クラウド利用者は，自らが利用するクラウドサービスの特性を理解して，クラウドサービス上で扱う情報，ソフトウェア及びソフトウェアの設定において，バックアップの可能性を確認することが望ましい。クラウド利用者は，自らが利用するクラウドサービスの特性を理解し，クラウドサービス上で扱う情報，ソフトウェア及びソフトウェアの設定のバックアップ手順を，次の事項を考慮して策定することが望ましい。

a) クラウドサービスに付帯するバックアップ機能及び復元機能
b) 利用者自身が追加開発するバックアップ機能及び復元機能
c) バックアップデータの暗号化（暗号化の必要性を含む）
d) バックアップデータのローカルでの保管及び隔地保管
e) バックアップデータの保管期間

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウド利用者が行うべきバックアップ取得について明確にすることが望ましい。また，利用者自身によるバックアップ取得が必要な場合，バックアップ取得を支援する情報若しくは機能を提供することが望ましい。クラウド事業者は，利用者にバックアップ機能及び復元機能を提供する場合には，利用者が実施する手順を明確にすることが望ましい。

クラウドサービスの関連情報

クラウドサービスでは，クラウドサービスによってバックアップ不可能な情報がある点に留意する必要がある。クラウドサービス以外のシステム運用におけるバックアップ手順において，差分バックアップ，増分バックアップ，完全バックアップなど，バックアップ対象の特性に応じて使い分けている場合は，それぞれの手法による実施の可否を確認することが期待される。

IaaS サービスにおいては，作成された仮想イメージファイルを明示的にバックアップしておくことで，ある時点での環境を再現することができるが，バックアップを指定しない場合には再現することが難しい。クラウド事業者は，クラウド利用者が必要に応じて仮想イメージファイルをバックアップできる手段を用意しておくことが期待される。

PaaS サービスにおいては，作成したアプリケーションなどのソースファイルなどをバックアップすることができないこともある。アプリケーションの開発中など，頻繁に機能の追加や削除を行う場合に備えて，

開発途中の状態を維持できるかどうかを確認することが望ましい。また，実行環境や試験データなどが再現できるかどうかを確認することが期待される。

SaaS サービスでは，アプリケーションで利用するデータだけではなく，利用者アカウントの管理など，クラウドサービスの管理情報についてバックアップが可能かどうかを確認することが期待される。

10.6 ネットワークセキュリティ管理

目的：ネットワークにおける情報の保護，及びネットワークを支える基盤の保護を確実にするため。

組織の境界を越えて広がることもあるネットワークのセキュリティ管理には，データの流れ，法的背景，監視，保護についての注意深い考慮が必要である。

公衆ネットワークを通過する，又は取扱いに慎重を要する情報の保護には，追加の管理策が要求される場合もある。

10.6.1 ネットワーク管理策

管理策

ネットワークを脅威から保護するために，また，ネットワークを用いた業務用システム及び業務用ソフトウェア（処理中の情報を含む。）のセキュリティを維持するために，ネットワークを適切に管理し，制御することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービスの利用に際して，ネットワークサービスに関する情報をクラウド事業者に求めることが望ましい。

クラウド利用者は，必要に応じて，私設網又は暗号化された通信経路を介してクラウドサービスを利用することが望ましい。

クラウド事業者の実施が望まれる事項

仮想化技術を用いて構築されたクラウドコンピューティング環境における仮想ネットワークは，物理ネットワーク上の仮想インフラ上に構成されており，物理・論理ネットワークのセキュリティポリシーが適切に調和していない場合，ネットワークのぜい弱性が生じ，システム停止やアクセス制御違反が発生する恐れがあるため，クラウド事業者は，物理ネットワークのセキュリティポリシーを考慮した仮想ネットワークのセキュリティポリシーを定めることが望ましい。また，クラウド事業者は，仮想ネットワークのセキュリティ設定マニュアルを定め，運用担当者に配付することが望ましい。

クラウドサービスの関連情報

クラウド事業者は，仮想化されたネットワークを通じての脅威が存在することを念頭におき，対策を行うことが望ましい。特に，IaaS においては，スイッチやファイアウォールもネットワークと同じホスト OS 上で，仮想化サービスとして提供されることがあるため，ホスト OS のぜい弱性が，スイッチングやフィルタリング，ブロッキングなどのネットワーク関連機能に影響を与える可能性に留意する必要がある。

10.6.2 ネットワークサービスのセキュリティ

管理策

すべてのネットワークサービス（組織が自ら提供するか外部委託しているかを問わない。）について，

セキュリティ特性，サービスレベル及び管理上の要求事項を特定し，また，いかなるネットワークサービス合意書にもこれらを盛り込むことが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービスに含まれるすべてのネットワークサービス（組織が自ら提供するか外部委託しているかを問わない。）について，セキュリティ特性，サービスレベル及び管理上の要求事項に適合することを確認することが望ましい。クラウド利用者は，クラウドサービスに含まれるすべてのネットワークサービスについて，セキュリティ特性，サービスレベル及び管理上の要求事項を，クラウド事業者との合意書に盛り込むことが望ましい。クラウド利用者はクラウドービスに含まれるネットワークサービスが，セキュリティを保つ能力を見定め，常に監視することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウドサービスに含まれるすべてのネットワークサービスについて，セキュリティ特性，サービスレベル及び管理上の要求事項を，クラウド利用者と合意することが望ましい。クラウド事業者は，クラウド利用者と合意したクラウドサービスに含まれるネットワークサービスがセキュリティを保つ能力について，クラウド利用者が監視できる機能を提供することが望ましい。クラウド事業者は，クラウドサービスにおけるこれらの対策の実施を確実にすることが望ましい。クラウド事業者は，クラウドサービスについて，セキュリティ特性，サービスレベル及び管理上の要求事項が，適切に実行されていることを監査などで確認し，必要に応じてクラウド利用者に監査結果などを明示することが望ましい。

10.7 媒体の取扱い

目的：資産の認可されていない開示，改ざん，除去又は破壊，並びにビジネス活動の中断を防止するため。

媒体を管理し，かつ，物理的に保護することが望ましい。

認可されていない（情報）開示，改ざん，除去及び破壊から文書，コンピュータの媒体（例えば，テープ，ディスク），入力データ，出力データ及びシステムに関する文書を保護するために，適切な操作手順を確立することが望ましい。

10.7.1 取外し可能な媒体の管理

管理策

取外し可能な媒体の管理のための手順は，備えることが望ましい。

クラウドサービスの関連情報

クラウド事業者は，クラウドサービスのデータのバックップを媒体などで実施する場合には，その管理に留意する必要がある。

10.7.2 媒体の処分

管理策

媒体が不要になった場合は，正式な手順を用いて，セキュリティを保ち，かつ，安全に処分することが望ましい。

10.7.3 情報の取扱手順

管理策

情報の取扱い及び保管についての手順は，その情報を認可されていない開示又は不正使用から保護するために，確立することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービス上の組織の情報を認可されていない開示又は不正使用から保護するために，取扱い手順を確立することが望ましい。クラウド利用者は，作成したクラウドサービス上の情報の取扱い手順を，クラウドサービスの利用者に周知徹底することが望ましい。

10.7.4 システム文書のセキュリティ

管理策

システム文書は，認可されていないアクセスから保護することが望ましい。

10.8 情報の交換

目的：組織内部で交換した及び外部と交換した，情報及びソフトウェアのセキュリティを維持するため。

組織間での情報及びソフトウェアの交換は，正式な交換方針に基づいていること，情報交換に関する合意に沿って実施していること，また，いかなる関連法令をも順守していることが望ましい（箇条 15 参照）。

配送中の情報及び情報を格納した物理的媒体を保護するための手順及び標準を確立することが望ましい。

10.8.1 情報交換の方針及び手順

管理策

あらゆる形式の通信設備を利用した情報交換を保護するために，正式な交換方針，手順及び管理策を備えることが望ましい。

クラウドサービスの関連情報

クラウド事業者は，情報交換の機能を含むクラウドサービスを提供する場合，この情報交換を保護するための機能を検討し，必要に応じて実装することが期待される。クラウド事業者は，クラウドサービスを利用した情報交換を保護するための機能及び利用手順を，クラウドサービスの利用を検討する者に明示することが期待される。クラウド事業者は，クラウドサービスを利用した情報交換を保護するための機能が適切に動作していることを監査などによって確認し，クラウド利用者にその実施の事実又は結果を明示することが期待される。クラウド利用者及びクラウド事業者は，クラウドサービスにおいて，通信経路が暗号化できず，データの改ざんチェック機能も備えていない機能がある可能性に留意する必要がある。

10.8.2 情報交換に関する合意

管理策

組織と外部組織との間の情報及びソフトウェアの交換について，両者間での合意が成立することが望ましい。

10.8.3 配送中の物理的媒体

管理策

情報を格納した媒体は，組織の物理的境界を越えた配送の途中における，認可されていないアクセス，不正使用又は破損から保護することが望ましい。

10.8.4 電子的メッセージ通信

管理策

電子的メッセージ通信に含まれた情報は，適切に保護することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービスにおいて，電子的メッセージ通信を利用する場合は，電子的メッセージ通信に含まれた情報を適切に保護する機能があることを確認することが望ましい。クラウド利用者は，クラウドサービスにおいて，電子的メッセージ通信を利用する場合は，電子的メッセージ通信に含まれた情報を適切に保護する機能が適切に動作していることを，クラウド事業者が監査していることを確認することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウドサービスにおいて，電子的メッセージ通信を提供する場合は，電子的メッセージ通信に含まれた情報を適切に保護する機能を提供することが望ましい。クラウド事業者は，クラウドサービスにおいて，電子的メッセージ通信を提供する場合は，電子的メッセージ通信に含まれた情報を適切に保護する機能を，クラウドサービスの利用を検討する者に明示することが望ましい。クラウド事業者は，クラウドサービスにおいて，電子的メッセージ通信を提供する場合は，電子的メッセージ通信に含まれた情報を適切に保護する機能が適切に動作していることを監査などによって確認し，必要に応じてクラウド利用者に監査結果を明示することが望ましい。

10.8.5 業務用情報システム

管理策

業務用情報システムの相互接続と関連がある情報を保護するために，個別方針及び手順を策定し，実施することが望ましい。

10.9 電子取引サービス

目的：電子商取引サービスのセキュリティ，及びそれらサービスのセキュリティを保った利用を確実にするため。

電子商取引サービス（オンライン取引を含む。）の利用に関連するセキュリティ上の影響及び管理策のための要求事項を考慮することが望ましい。公開されているシステムを通じて電子的に発行した情報の完全性及び可用性についても，考慮することが望ましい。

10.9.1 電子商取引

管理策

公衆ネットワークを経由する電子商取引に含まれる情報は，不正行為，契約紛争，認可されていない開示及び改ざんから保護することが望ましい。

10.9.2 オンライン取引

管理策

オンライン取引に含まれる情報は，次の事項を未然に防止するために，保護することが望ましい。

－不完全な通信

－誤った通信経路設定

－認可されていないメッセージの変更

－認可されていない開示

－認可されていない複製又は再生

10.9.3 公開情報

管理策

認可されていない変更を防止するために，公開システム上で利用可能な情報の完全性を保護することが望ましい。

10.10 監視

目的：認可されていない情報処理活動を検知するため。

システムを監視することが望ましく，また，情報セキュリティ事象を記録することが望ましい。

システム運用担当者の作業ログ及び障害ログは，情報システムの問題を識別することを確実とするために利用することが望ましい。

組織は，監視及び記録の活動に適用されるすべての関連した法的要求事項を順守することが望ましい。

システムの監視は，採用している管理策の有効性の点検及びアクセス方針モデルに対する適合性の確認のために利用することが望ましい。

10.10.1 監査ログ取得

管理策

利用者の活動，例外処理及びセキュリティ事象を記録した監査ログを取得することが望ましく，また，将来の調査及びアクセス制御の監視を補うために，合意された期間，保持することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービス上で取得されるクラウドサービスの利用者の活動，例外処理及びセキュリティ事象を記録した監査ログの存在を確認することが望ましい。クラウド利用者は，クラウドサービス上で取得された監査ログは，将来の調査及びアクセス制御の監視を補うために，適切な期間，保持されることを確認することが望ましい。クラウド利用者は，クラウドサービス上で取得される監査ログが，クラウドサービスの利用者の活動，例外処理及びセキュリティ事象を記録できていることを確認することが望ましい。クラウド利用者は，クラウドサービス上で取得された監査ログが提供される方法，提供のタイミングについて，適切かどうか確認することが望ましい。クラウド利用者は，クラウドサービス上で取得された監査ログが保持される期間が，将来の調査及びアクセス制御の監視を補うために適切かどうか確認することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウドサービス上で取得するクラウドサービスの利用者の活動，例外処理及びセキュリティ事象を記録した監査ログを特定し，取得する機能をクラウド利用者に提供することが望ましい。クラウド事業者は，クラウドサービス上で取得された監査ログは，クラウド利用者の将来の調査及びアクセス制御の監視を補うことを考慮し，保持する期間を定めることが望ましい。クラウド事業者は，クラウ

ドサービス上で取得する利用者の活動，例外処理及びセキュリティ事象を記録した監査ログについて，クラウドサービスの利用を検討する者に明示することが望ましい。クラウド事業者は，クラウドサービス上で取得した監査ログの提供方法，提供のタイミングについて，クラウドサービスの利用を検討する者に明示することが望ましい。クラウド事業者は，クラウドサービス上で取得した監査ログを保持する期間を，クラウドサービスの利用を検討する者に明示することが望ましい。

クラウドサービスの関連情報

クラウド事業者は，ログの取扱いについて，個別のクラウド利用者の要請に応じることができることを考慮することが期待される。監査ログの内容及び提供方法に関しては，クラウド利用者とクラウド事業者が合意した形式で実施することが期待される。

10.10.2 システム使用状況の監視

管理策

情報処理設備の使用状況を監視する手順を確立すること，及び監視活動の結果を定めに従ってレビューすることが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービスの使用状況を監視する手順を確立することが望ましい。また，監視活動の結果を定めに従ってレビューすることが望ましい。

クラウド利用者は，クラウドコンピューティングサービスの利用状況の監視手順を策定するために，クラウド事業者に次のような事項を確認することが望ましい。

a) 利用状況の記録の種類

b) 利用状況の記録の表示方法

c) 利用状況の記録の保持期間

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウドサービス上で使用状況をクラウド利用者が監視できる機能を提供することが望ましい。

10.10.3 ログ情報の保護

管理策

ログ機能及びログ情報は，改ざん及び認可されていないアクセスから保護することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービス上のログ機能及びログ情報が，改ざん及び認可されていないアクセスから保護されていることを確認するために，次のような情報をクラウド事業者に対して求めることが望ましい。

a) ログ情報の保護に関する方針

b) ログ情報の保護機能の概要

c) ログ情報の保護が適切に動作していることに関するクラウド事業者による監査の実施状況又は結果

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウドサービス上のクラウド利用者のログ機能及びログ情報が，改ざん及び認可されていないアクセスから保護されていることを確実にすることが望ましい。

クラウドサービスの関連情報

クラウド事業者は，クラウドサービス上でログ情報を一括して取得し，一括した改ざん防止を行っている場合，必要なログとして提供されるログの完全性が担保できない可能性があることに留意することが期待される。

10.10.4 実務管理者及び運用担当者の作業ログ

管理策

システムの実務管理者及び運用担当者の作業は，記録することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービス上に構築した利用者システムの実務管理者及び運用担当者の作業が，記録されていることを確認することが望ましい。クラウド利用者は，クラウドサービス上で記録された，システムの実務管理者及び運用担当者の作業の記録を，規定に従ってレビューすることが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウドサービス上で，クラウド利用者のシステムの実務管理者及び運用担当者の作業を，記録する機能を提供することが望ましい。クラウド事業者は，クラウドサービス上で，クラウド利用者のシステムの実務管理者及び運用担当者の作業を記録する機能を，クラウドサービスの利用を検討する者に明示することが望ましい。

クラウドコンピューティング環境に対する特権操作がクラウド利用者にゆだねられる場合，責任分界を明確にするために，クラウド事業者及びクラウド利用者双方の作業ログを取得・保管することが望ましい。

クラウドサービスの関連情報

クラウド利用者は，クラウド事業者がログ情報を一括して取得し，一括した管理を行っている場合，必要なときに必要なログが提供されない可能性に留意する必要がある。

クラウド利用者は，作業ログに関する仕様を確認したり，第三者タイムスタンプ及び WORM（Write-Once-Read-Many，書込み 1 回のみ可能かつ消去・変更不可）デバイスの否認防止機能の有無を確認することが期待される。

クラウド利用者は，クラウドサービスにおいて運用担当者のログが提供されない場合には，どのようなログをクラウド事業者が取得しているかについて情報提供を求めることが期待される。

10.10.5 障害のログ取得

管理策

障害のログを取得し，分析し，また，障害に対する適切な処置をとることが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービス上の障害のログを取得し，分析し，また，障害に対する適切な処置をとることが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウド利用者に提供する，障害のログの範囲を定めることが望ましい。クラウド

事業者は，クラウド利用者に障害のログを提供する機能を提供することが望ましい。クラウド事業者は，クラウド利用者に提供する，障害のログの範囲を，クラウドサービスの利用を検討する者に明示することが望ましい。クラウド事業者は，クラウド利用者に提供する，障害のログの提供方法を，クラウドサービスの利用を検討する者に明示することが望ましい。

クラウドサービスの関連情報

クラウド利用者は，クラウド事業者がログ情報を一括して取得し，一括した管理を行っている場合，必要なログが提供されない可能性に留意する必要がある。

10.10.6 クロックの同期

管理策

組織又はセキュリティ領域内のすべての情報処理システム内のクロックは，合意された正確な時刻源と同期させることが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービスと組織内のシステムとの時刻差が発生するか確認することが望ましい。クラウド利用者は，クラウドサービスと組織内のシステムとの時刻差を定期的に監視・記録し，時刻差が発生することによって，影響がある事項を洗い出し，管理策を検討することが望ましい。クラウド利用者は，分析などにおいて，ログに記録された時刻など，クラウドサービスの時刻の差を考慮することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウドサービスのすべての情報処理システム内のクロックを，合意された正確な時刻源と同期させることが望ましい。クラウド事業者は，クラウドサービスのすべての情報処理システム内のクロックを，合意された正確な時刻源と同期させる仕組みを，クラウドサービスの利用を検討する者に明示することが望ましい。

クラウドサービスの関連情報

クラウド事業者は，標準時の異なる複数の地域にまたがるシステムのクロックのずれに留意することが望ましい。クラウド事業者は，IaaS においては，仮想環境の時刻ずれのリスクに留意する必要がある。

11 アクセス制御

11.1 アクセス制御に対する業務上の要求事項

目的：情報へのアクセスを制御するため。

情報・情報処理設備及び業務プロセスへのアクセスにおいては，業務及びセキュリティの要求事項に基づいて管理することが望ましい。

アクセス制御規則には，情報を伝える範囲及びアクセスの認可に対する方針を考慮することが望ましい。

11.1.1 アクセス制御方針

管理策

アクセス制御方針は，アクセスについての業務上及びセキュリティの要求事項に基づいて確立し，文書

化し，レビューすることが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，既存のアクセス制御方針が，クラウドサービスが提供するアクセス制御機能で実現できるか確認することが望ましい。クラウド利用者は，クラウドサービスのアクセス権を既存のアクセス制御方針に組み込むことが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，提供するクラウドサービスにおいて，利用者のアクセス制御機能を提供することが望ましい。クラウド事業者は，提供するクラウドサービスにおいてクラウド利用者が実施可能なアクセス制御機能について，クラウド利用者に明示することが望ましい。

クラウドサービスの関連情報

クラウドサービスのアクセス権を既存のアクセス制御方針に組み込む際に，クラウド利用者が考慮するポイントとして次のような事項がある。

a) アクセス制御に係る職務の分離（例えば，ID の使用者と登録者など）

b) アクセス権限付与に関する承認プロセス

c) クラウド利用者に付与されるアクセス制御権限

11.2 利用者アクセスの管理

目的：情報システムへの，認可された利用者のアクセスを確実にし，認可されていないアクセスを防止するため。

情報システム及びサービスへのアクセス権の割当てを管理するための正式の手順が備わっていることが望ましい。

この手順は，利用者アクセスのライフサイクル（すなわち，新しい利用者の初期登録から，情報システム及びサービスへのアクセスを必要としなくなった利用者の最終的な登録削除まで）におけるすべての段階を対象とすることが望ましい。アクセスの特権を与えると，システムの管理策ではその利用者を制御することができなくなる。適切な場合には，アクセス特権の付与を管理する必要性について，特別の注意を払うことが望ましい。

11.2.1 利用者登録

管理策

すべての情報システム及びサービスへのアクセスを許可及び無効とするために，利用者の登録・登録削除についての正式な手順を備えることが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，すべての情報システム及びサービスへのアクセスを許可及び無効とするために，利用者 ID の登録・削除についての正式な手順に，クラウドサービスの利用を考慮することが望ましい。クラウド利用者は，必要に応じてクラウド事業者に利用者 ID の登録・削除機能に関する情報を求め，クラウド事業者が提供する機能で組織の正式な手順が実現できることを確認することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウド利用者のクラウドサービス利用者 ID の登録・削除機能を提供することが望ましい。また，このような機能について，必要に応じて次の情報を提供することが望ましい。

a) 利用者 ID 登録・削除の手順

b) 利用者 ID 登録・削除に必要な情報

c) 利用者の同一性検証の仕様

d) サービスの一部として利用者 ID 管理ツールを提供している場合は，利用者 ID 管理ツールの仕様

クラウドサービスの関連情報

クラウド利用者は，クラウドサービスの形態によっては，クラウドサービスの利用者 ID を登録する際に，クラウド利用者が自ら設定できる場合や，クラウド提供者が登録を代行する場合など，様々な形態が存在することを考慮する必要がある。クラウドサービスの提供のために，クラウド利用者の環境にデフォルトユーザが存在する場合や，クラウド利用者の環境にクラウド事業者が利用する利用者 ID を作成する必要がある場合は，クラウド利用者とクラウド提供者の間でその管理責任を明確に定義することが期待される。

11.2.2 特権管理

管理策

特権の割当て及び利用は，制限し，管理することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，特権の割当て及び利用を管理する既存の仕組みが，クラウドサービス上で実現できるか確認し，クラウドサービス利用における特権を管理することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウド利用者に特権を付与する場合には，クラウド利用者がクラウドサービスにおける特権を管理する機能を提供することが望ましい。また，このような機能について，次のような情報をクラウド利用者に提供することが望ましい。

a) クラウド利用者の特権の種類及び役割

b) クラウド利用者の特権アカウント使用の監視・管理機能の仕様

c) クラウド利用者の特権アカウント使用に関するログ

クラウドサービスの関連情報

クラウド利用者はクラウドサービスの形態においては，特権を登録する際に，クラウド利用者が自ら設定できる場合や，クラウド事業者が登録を実施するなど，様々な形態が存在することに留意する必要がある。クラウドサービスの提供のために，クラウド利用者の環境にデフォルトユーザとして特権が存在する場合や，クラウド利用者の環境にクラウド事業者の特権を作成する必要がある場合は，クラウド利用者とクラウド事業者の間でその管理責任を明確に定義することが期待される。

11.2.3 利用者パスワードの管理

管理策

パスワードの割当ては，正式な管理プロセスによって管理することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，パスワードの割当てに関する既存の正式な管理プロセスが，クラウドサービスが提

供する機能で実現できるか確認することが望ましい。クラウド利用者は，クラウド事業者があらかじめ設定したパスワード（初期パスワードなど）を，システム又はソフトウェアのインストール後に変更することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウドサービスにおいて利用するパスワードの割当ての管理機能を提供することが望ましい。クラウド事業者は，クラウドサービスにおいて利用するパスワードの割当ての管理プロセスの機能について，次のような情報を提供することが望ましい。

a) パスワードの発行，変更及び再発行の手順

b) パスワード割当てにおける認証及び認証の仕組み（例えば，多要素認証を用いた認証方法など）

クラウドサービスの関連情報

クラウドサービスの利用者パスワードの管理機能は，利用するクラウドサービスの形態によっては，適切なインタフェースをクラウド利用者が設計する必要があることに留意する必要がある。

11.2.4 利用者アクセス権のレビュー

管理策

管理者は，正式なプロセスを使用して，利用者のアクセス権を定められた間隔でレビューすることが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，アクセス権を一覧化する機能の仕様について，クラウド事業者に情報を求めることが望ましい。

クラウド利用者は，クラウドサービスの利用者のアクセス権をレビューする正式なプロセスが，クラウドサービスの機能で実現できることを確認することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウドサービスにおいて，クラウド利用者がアクセス権をレビューする機能を提供することが望ましい。

11.3 利用者の責任

目的：認可されていない利用者のアクセス，並びに情報及び情報処理設備の損傷又は盗難を防止するため。

認可されている利用者間の協力は，有効なセキュリティのために不可欠である。

利用者に，有効なアクセス制御を維持するための自分自身の責任を認識させることが望ましい。特にパスワードのセキュリティ及び利用者が利用する装置のセキュリティに関して，その責任を認識させることが望ましい。

クリアデスク・クリアスクリーン方針は，書類，媒体及び情報処理設備に対する認可されていないアクセス又は損傷のリスクを低減するために，実施することが望ましい。

11.3.1 パスワードの利用

管理策

パスワードの選択及び利用時に，正しいセキュリティ慣行に従うことを，利用者に要求することが望ま

しい。

クラウドサービスの関連情報

クラウド事業者は，クラウド利用者が，パスワードの選択及び利用をする際に，正しいセキュリティ慣行に従うことができる機能を提供することが期待される。クラウドサービスでは，複数のサービスを組み合わせて一つのパスワードを利用する場合があるので，クラウド事業者は，質の良いパスワードを用いることをクラウド利用者に助言することを考慮する必要がある。

11.3.2 無人状態にある利用者装置

管理策

利用者は，無人状態にある装置が適切な保護対策を備えていることを確実にすることが望ましい。

クラウドサービスの関連情報

クラウド利用者は，共有環境でクラウドサービスを利用する場合には，認可されないアクセスについて留意する必要がある。

11.3.3 クリアデスク，クリアスクリーン方針

管理策

書類及び取外し可能な記憶媒体に対するクリアデスク方針，並びに情報処理設備に対するクリアスクリーン方針を適用することが望ましい。

11.4 ネットワークのアクセス制御

目的：ネットワークを利用したサービスへの認可されていないアクセスを防止するため。

内部及び外部のネットワークを利用したサービスへのアクセスを，制御することが望ましい。

ネットワーク及びネットワークサービスへの利用者のアクセスは，次の条件を確実にすることによって，ネットワークサービスのセキュリティを損なわないことが望ましい。

a) 組織のネットワークと他の組織が管理するネットワーク又は公衆ネットワークとの間に適切なインタフェースを備える。

b) 利用者及び装置に適切な認証機構を適用する。

c) 情報サービスへの利用者アクセスを制御する。

11.4.1 ネットワークサービスの利用についての方針

管理策

利用することを特別に認可したサービスへのアクセスだけを，利用者に提供することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，ネットワークサービスの利用に関する方針に，クラウドサービスの利用に関する考慮事項を含めることが望ましい。クラウド利用者は，適切なクラウドサービスの利用者のみクラウドサービスが利用できるようネットワークを構成する方針を定めることが望ましい。

クラウド利用者は，クラウドサービスのネットワークの利用に関する方針に次の事項を含めることを確実にすることが望ましい。

a) ネットワークアクセス制御方針

b) アクセス管理サービス方針

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウド利用者がネットワークサービスの利用に関する方針を策定できるよう，クラウドサービス利用の管理に係る情報の種類及びその内容を提示することが望ましい。

クラウドサービスの関連情報

クラウド事業者は，仮想化ソフトウェア固有の課題（例えば，仮想マシンから他仮想マシンへの攻撃など，仮想化ソフトウェア内での攻撃）を考慮し，各仮想マシンの隔離設計に留意する必要がある。クラウド事業者は，隔離設計は，物理ネットワーク側での対応や，ゾーン機能やプライベート VLAN 機能などの機能を活用する方法や，同機能を有するサードパーティ製品の活用などに留意する必要がある。

11.4.2 外部から接続する利用者の認証

管理策

遠隔利用者のアクセスを管理するために，適切な認証方法を利用することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，自らが管理していないネットワーク（公衆無線 LAN や携帯電話網による接続など）からクラウドサービスを利用する際に，適切な認証方法を利用することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウドサービスへの接続方法に応じた認証方法を提供することが望ましい。クラウド事業者は，クラウドサービスへの接続方法に応じた認証方法を，クラウドサービスの利用を検討する者に明示することが望ましい。

11.4.3 ネットワークにおける装置の識別

管理策

特定の場所及び装置からの接続を認証するための手段として，自動の装置識別を考慮することが望ましい。

クラウドサービスの関連情報

クラウド事業者は，クラウドサービスに接続する装置において，識別を可能にする機能（電子証明書や IC チップなどを利用した識別機能）を提供することが期待される。

11.4.4 遠隔診断用及び環境設定用ポートの保護

管理策

診断用及び環境設定用ポートへの物理的及び論理的なアクセスは，制御することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウド利用者がクラウドサービスの遠隔診断用及び環境設定ポートを管理する場合には，厳密に管理することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウドサービスに遠隔診断用及び環境設定ポートが存在する場合は，クラウドサービスの利用を検討する者に明示することが望ましい。

クラウドサービスの関連情報

クラウド事業者は, クラウドサービスのホスト OS 上で動作する仮想スイッチや仮想ファイアウォールなどの遠隔診断用及び環境設定ポートが存在する場合は，厳密に管理することが期待される。

11.4.5 ネットワークの領域分割

管理策

情報サービス，利用者及び情報システムは，ネットワーク上，グループごとに分割することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウド事業者のネットワークにおける分離を要求する必要性について考慮することが望ましい。

クラウド利用者は，クラウドサービスのネットワークを分離するため，ネットワークを異なるドメインに分離する機能の使用について，必要に応じてクラウド事業者に情報を求めることが望ましい。

クラウド利用者は，クラウドサービスの利用者のアクセス権限に基づいて，クラウドサービスのネットワークを論理的に分離することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，各クラウド利用者に割り当てたコンピューティング資源に，他のクラウド利用者や許可されていないユーザがアクセスできないように管理し，物理的な設定や移行にかかわらず，仮想環境の分離を確実にすることが望ましい。

ネットワーク若しくはインタフェースの分離がなされていない場合，クラウド事業者は，アプリケーションレイヤの通信のエンドツーエンドでの暗号化を考慮することが望ましい。

クラウド事業者は，クラウド利用者の情報及びソフトウェアへのバックドアアクセスの可能性を識別するために，クラウド環境における情報セキュリティについて評価を実施することが望ましい。

クラウドサービスの関連情報

クラウド事業者は, クラウドサービスのホスト OS 上で動作する仮想スイッチや仮想ファイアウォールなどのネットワークを構成に応じて論理的に分離する必要がある。

クラウド利用者がクラウド事業者にネットワークの分離を要求するケースとして，次のような場合が想定される。

a) クラウド環境内に同業他社が共存する場合

b) 規制要件によりネットワーク通信の分離・隔離が求められる場合

11.4.6 ネットワークの接続制御

管理策

共有ネットワーク，特に，組織の境界を越えて広がっているネットワークについて，アクセス制御方針及び業務用ソフトウェアの要求事項に沿って，利用者のネットワーク接続能力を制限することが望ましい（11.1 参照）。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービスのネットワークについて，アクセス制御方針及び業務用ソフトウェアの要求事項に沿って，利用者のネットワーク接続を許可する範囲を制限することが望ましい。利用者のネットワークへのアクセス権は，アクセス制御方針の要求に従って，維持・更新することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウドサービスで利用可能なネットワークサービスを特定することが望ましい（例えば，電子メールなどのメッセージ通信，ファイル転送など）。クラウド事業者は，クラウドサービスで利用可能なネットワークサービスを，クラウドサービスの利用を検討する者に明示することが望ましい。

クラウドサービスの関連情報

クラウド事業者は，クラウドコンピューティングで利用できるサービスを増やすことで，他のゲストOSや，外部から受ける影響の増加に留意する必要がある。

11.4.7 ネットワークルーティング制御

管理策

コンピュータの接続及び情報の流れが業務用ソフトウェアのアクセス制御方針に違反しないことを確実にするために，ルーティング制御の管理策をネットワークに対して実施することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，コンピュータの接続及び情報の流れが業務用ソフトウェアのアクセス制御方針に違反しないことを確実にするために，クラウドサービスを，ルーティング制御の管理策に加えることが望ましい。

クラウド事業者が，ホストOS上のネッワークルーティングを行う場合は，クラウド利用者は，その設定が，コンピュータの接続及び情報の流れが業務用ソフトウェアのアクセス制御方針に違反していないことを確認することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，ホストOS上のネットワークルーティングについて，適切に設定することが望ましい。クラウド事業者は，ホストOS上のネットワークルーティングについて，適切に設定していることを利用者に明示することが望ましい。

クラウドサービスの関連情報

ホストOS上のネットワークルーティングについて，クラウド利用者が設定できる場合は，影響を考慮して設定する必要がある。

11.5 オペレーティングシステムのアクセス制御

目的：オペレーティングシステムへの，認可されていないアクセスを防止するため。

オペレーティングシステムにアクセスする者を，認可された利用者に限定するために，セキュリティ設備を用いることが望ましい。それらの設備は，次の能力をもつことが望ましい。

a) 既定のアクセス制御方針に従って認可されている利用者本人であることの認証

b) システムへの認証の成功及び失敗の記録

c) 特別なシステム特権の使用の記録

d) システムセキュリティ方針に違反したときの警告発信

e) 認証のための適切な手段の提供

f) 適切な場合，利用者の接続時間の制限

11.5.1 セキュリティに配慮したログオン手順

管理策

オペレーティングシステムへのアクセスは，セキュリティに配慮したログオン手順によって制御することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービスのオペレーティングシステムにログオンする場合，セキュリティに配慮したログオン手順によって制御されることを確認することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウドサービスのオペレーティングシステムにクラウド利用者がログオンする場合，セキュリティに配慮したログオン手順で制御する機能を提供することが望ましい。また，そのような機能について，クラウドサービスの利用を検討する者に明示することが望ましい。

クラウドサービスの関連情報

クラウドサービスの形態においては，オペレーティングシステムが複数存在し，その利用者も異なる可能性があるため，クラウド事業者は，クラウド利用者の資産と権限に留意し，ログオン手順を定めることを求めることが期待される。

11.5.2 利用者の識別及び認証

管理策

すべての利用者は，各個人の利用ごとに一意な識別子（利用者 ID）を保有することが望ましい。また，利用者が主張する同一性を検証するために，適切な認証技術を選択することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービスにおいて，すべてのクラウドサービスの利用者が，各個人の利用ごとに一意な識別子（利用者 ID）を保有することができるか確認することが望ましい。また，クラウドサービス利用者が主張する同一性を検証するために，クラウドサービスにおいて，適切な認証技術の選択が可能であるかを確認することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウドサービスにおいて，すべてのクラウドサービス利用者に，各個人の利用ごとに一意な識別子（利用者 ID）を保有することができるようにすることが望ましい。また，クラウドサービス利用者が主張する同一性を検証するために，クラウドサービスにおいて，適切な認証技術を選択することができる機能を提供することが望ましい。クラウド事業者は，クラウドサービスにおいて，すべてのクラウドサービス利用者に，各個人の利用ごとに一意な識別子（利用者 ID）を保有することができるかどうか，クラウドサービスの利用を検討する者に明示することが望ましい。クラウド事業者は，クラウドサービスにおいて，選択できる認証技術を，クラウドサービスの利用を検討する者に明示することが望ましい。

クラウドサービスの関連情報

クラウド事業者は，ID 管理をするサービスが，クラウドサービス利用者 ID を個別に発行できるように設定することが期待される。クラウド事業者は，ID 管理をするサービスが，共有 ID を発行する場合は，

利用者が共有IDの利用者を個別に認識する必要があるか,検討が必要なことを明示することが期待される。

11.5.3 パスワード管理システム

管理策

パスワードを管理するシステムは，対話式とすることが望ましく，また，良質なパスワードを確実とするものが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービスのパスワードを管理するシステムが，対話式であり，また，良質なパスワードを確実とする機能があることを確認することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウドサービスのパスワードを管理するシステムを，対話式とすることが望ましい。クラウド事業者は，クラウドサービスのパスワードを管理するシステムを，良質なパスワードを確実とすることが望ましい。クラウド事業者は，クラウドサービスのパスワードを管理するシステムは，対話式であることを，開示することが望ましい。クラウド事業者は，クラウドサービスのパスワードを管理するシステムは，良質なパスワードを確実とする機能があることを，利用を検討する者に明示することが望ましい。

クラウドサービスの関連情報

クラウド事業者は，ID 管理をするサービスが，パスワード管理を適切に行われるように設定すると同時に，その設定を機能させるインタフェースを提供することが期待される。クラウド事業者は，ID 管理をするサービスのみを提供する場合は，パスワードの管理が適切に行われるように設定する手順や，その設定を機能させるインタフェースを作成するための手順を利用者に明示することが期待される。

11.5.4 システムユーティリティの使用

管理策

システム及び業務用ソフトウェアによる制御を無効にすることのできるユーティリティプログラムの使用は，制限し，厳しく管理することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービスのシステム及び業務用ソフトウェアによる制御を無効にすることのできるユーティリティプログラムの使用を，制限し，厳しく管理することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，システム及び業務用ソフトウェアによる制御を無効にすることのできるユーティリティプログラムを特定することが望ましい。クラウド事業者は，システム及び業務用ソフトウェアによる制御を無効にすることのできるユーティリティプログラムを，クラウドサービスの利用を検討する者に明示することが望ましい。

クラウドサービスの関連情報

システム管理者の利便性を重視するクラウドサービスの機能は，システム及びアプリケーションの管理策を無効化できるユーティリティプログラムである場合がある。クラウド利用者組織におけるクラウドサービス利用者に対しては，そのようなユーティリティプログラムの使用は制限し，厳密に管理することが

期待される。

11.5.5 セッションのタイムアウト

管理策

一定の使用中断時間が経過したときは，使用が中断しているセッションを遮断することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービスの利用中に，一定の使用中断時間が経過したときは，使用が中断しているセッションが遮断されることを確認することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウドサービスの利用中に，一定の使用中断時間が経過したときは，使用が中断しているセッションを遮断する機能を提供することが望ましい。クラウド事業者は，クラウドサービスの利用中に，一定の使用中断時間が経過したときは，使用が中断しているセッションを遮断する機能について開示することが望ましい。

クラウドサービスの関連情報

クラウド利用者は，利用するクラウドサービスによっては，タイムアウトによる遮断をしてはならないサービスもあることに留意する必要がある。クラウド事業者は，仮想 OS の管理アクセス対応機能ではホスト OS へのアクセス制御において，セッションタイムアウトに未対応のものがあることに留意する必要がある。クラウド利用者は，セッションタイムアウトについて端末のスクリーンセイバーの制限など他の管理策を実施できることに留意する必要がある。

11.5.6 接続時間の制限

管理策

リスクの高い業務用ソフトウェアに対しては，更なるセキュリティを提供するために，接続時間の制限を利用することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，利用におけるリスクが高いと判断したクラウドサービスに対しては，接続時間の制限を利用できるか確認することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，利用におけるリスクが高いと判断されたクラウドサービスは，接続時間の制限を利用できる機能を提供することが望ましい。クラウド事業者は，リスクの高いクラウドサービスに対しては，接続時間の制限を利用できるかどうかを，開示することが望ましい。

クラウドサービスの関連情報

クラウド事業者は，仮想 OS の管理アクセス対応機能ではホスト OS へのアクセス制御において，管理アクセス通信の接続時間の制限が未対応のものがあることに留意する必要がある。クラウド利用者は，接続時間について端末の利用時間の制限など他の管理策を実施できることに留意する必要がある。

11.6 業務用ソフトウェア及び情報のアクセス制御

目的：業務用ソフトウェアシステムが保有する情報への認可されていないアクセスを防止するため。

業務用ソフトウェアシステムへのアクセス及びその中でのアクセスを制限するために，セキュリティ機能を用いることが望ましい。

業務用ソフトウェア及び情報への論理的アクセスは，認可されている利用者に制限することが望ましい。業務用ソフトウェアシステムは，次の条件を満たすことが望ましい。

a) 既定のアクセス制御方針に従って，情報及び業務用ソフトウェアシステム機能への利用者アクセスを制御する。

b) システム又は業務用ソフトウェアの制御を無効にできるユーティリティ，オペレーティングシステムのソフトウェア及び悪意のあるソフトウェアによる認可されていないアクセスから保護する。

c) 情報資源を共有しているほかの情報システムのセキュリティを脅かさない。

11.6.1 情報へのアクセス制限

管理策

利用者及びサポート要員による情報及び業務用ソフトウェアシステム機能へのアクセスは，既定のアクセス制御方針に従って制限することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウド利用者及びクラウド利用者のサポート要員によるクラウドサービスへのアクセスを，既定のアクセス制御方針に従って制限することが望ましい。クラウド利用者は，複数のシステムや情報を内包できるクラウドサービスでは，その重要性に応じて，アクセス権を強固にする必要があることに留意し，必要な管理策を設定できるような機能を準備することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウド利用者におけるクラウドサービスへのアクセス制限の要求モデルを定めることが望ましい。クラウド事業者は，クラウド利用者が行える要件を定め，クラウドサービスの利用を検討する者に明示することが望ましい。

クラウドサービスの関連情報

仮想マシンを操作するクライアントソフトウェアからは，ホスト OS のサービスコンソール部分だけでなくゲスト OS も操作することが可能な場合がある。その場合は，クラウド利用者は，権限管理をクラウドサービスの利用者ごとに細やかに設定して内部不正やシステム障害のリスクを減らすか，各仮想マシンへの管理アクセスは従来通りの方式で行うなど，仮想マシンを操作するクライアントソフトウェア経由でのアクセス時の権限管理を慎重に実施する必要があることに留意する必要がある。

11.6.2 取扱いに慎重を要するシステムの隔離

管理策

取扱いに慎重を要するシステムは，専用の（隔離された）コンピュータ環境をもつことが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，取扱いに慎重を要するシステムを，クラウドコンピューティングを利用して，構築する場合には，専用の（隔離された）コンピュータ環境上に構築できることを確認することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，取扱いに慎重を要するシステムを，クラウドコンピューティング内に構築する場合

に備えて，専用の（隔離された）コンピュータ環境上に構築できる機能を提供することが望ましい。

クラウドサービスの関連情報

クラウド利用者は，PaaS/IaaS 環境など，複数のシステムを内包できるクラウドサービス上では，そのシステムの重要性に応じて，アクセス権を強固にすることが期待される。クラウド事業者は，システム間の隔離をする管理策に留意する必要がある（仮想スイッチ上の arp スプーフィング防止機能など）。仮想マシンを操作するクライアントソフトウェアからは，ホスト OS のサービスコンソール部分だけでなくゲスト OS も操作することが可能な場合がある。その場合は，クラウド利用者は，権限管理をクラウドサービスの利用者ごとに細やかに設定して内部不正やシステム障害のリスクを減らすか，各仮想マシンへの管理アクセスは従来通りの方式で行うなど，仮想マシンを操作するクライアントソフトウェア経由でのアクセス時の権限管理を慎重に実施することが期待される。

11.7 モバイルコンピューティング及びテレワーキング

目的：モバイルコンピューティング及びテレワーキングの設備を用いるときの情報セキュリティを確実にするため。

要求される保護は，これら特異な作業形態が引き起こすリスクに応じたものであることが望ましい。モバイルコンピューティングを用いるとき，保護されていない環境における作業のリスクを考慮し，適切な保護を施すことが望ましい。テレワーキングに関しては，組織は，テレワーキングを行う場所に保護を施し，この作業形態のために適切な取決めがあることを確実にすることが望ましい。

11.7.1 モバイルのコンピューティング及び通信

管理策

モバイルコンピューティング設備・通信設備を用いた場合のリスクから保護するために，正式な方針を備え，また，適切なセキュリティ対策を採用することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，モバイルコンピューティング設備・通信設備を用いた場合のリスクから保護するための正式な方針に，クラウドサービスを加え，適切な情報セキュリティ対策を採用することが望ましい。クラウドサービスにおいてモバイルコンピューティングを利用できる機能がある場合は，クラウド利用者は，その機能がモバイルコンピューティング設備・通信設備を用いた場合のリスクから保護するための正式な方針に，適合しているか確認することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウドサービスにおいて，モバイルコンピューティングを利用できる機能を提供する場合は（一般的に，SaaS 又はアプリケーションレイヤにおけるサービスにおいて該当する），適切な情報セキュリティ対策を採用し，講じている情報セキュリティ対策を，クラウドサービスの利用を検討する者に明示することが望ましい。

クラウドサービスの関連情報

モバイルコンピューティング設備・通信設備 （例えば，ノート型コンピュータ，パームトップコンピュータ，ラップトップコンピュータ，IC カード，携帯電話） を用いる場合，業務情報が危険にさらされない

ことを確実にするために，特別な注意を払う必要がある。モバイルコンピューティング方針は，保護されていない環境におけるモバイルコンピューティング装置を用いた作業のリスクを考慮に入れる必要がある。クラウドサービスでは，スマートフォンなどの携帯端末での利用を前提として提供されている場合があるため，それらの端末の利用についても留意する必要がある。

11.7.2 テレワーキング

管理策

テレワーキングのための方針，運用計画及び手順を策定し，実施することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービスをテレワーキングで利用する場合，テレワーキングのための方針，運用計画及び手順を策定し，実施することが望ましい。クラウドサービスにおいてテレワーキングを利用できる機能がある場合は，クラウド利用者は，その機能が，テレワーキングのための方針，運用計画及び手順に適合することを確認することが望ましい。

クラウド事業者の実施が望まれる事項

クラウドサービスにおいてテレワーキングを利用する機能を提供する場合は，テレワーキングの適切な保護を実施することが望ましい。クラウド事業者は，提供するクラウドサービスにおいて，テレワーキングを利用する機能を提供する場合は，講じているセキュリティのための管理策を，クラウドサービスの利用を検討する者に明示することが望ましい。

12 情報システムの取得，開発及び保守

12.1 情報システムのセキュリティ要求事項

目的：セキュリティが情報システムに欠くことのできない部分であることを確実にするため。

情報システムには，オペレーティングシステム，システム基盤，業務用ソフトウェア，既成の製品，サービス及び利用者が開発したソフトウェアが含まれる。業務プロセスを支える情報システムの設計及び実装は，セキュリティへの影響が極めて大きい。セキュリティ要求事項は，情報システムを開発及び／又は実装する前に，特定し，合意することが望ましい。

すべてのセキュリティ要求事項は，プロジェクトの要求仕様検討段階で特定して，その正当性を実証し，合意した上で，情報システムの包括的な作業の一環として，文書化することが望ましい。

12.1.1 セキュリティ要求事項の分析及び仕様化

管理策

新しいシステム又は既存の情報システムの改善に関する業務上の要求事項を記述した文書では，セキュリティの管理策についての要求事項を仕様化することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，システム構築の標準を記載した規程にクラウドサービス利用時の項目を追加することが望ましい。クラウド利用者は，システム利用標準に外部のクラウドサービスを利用する場合に必要な項目を追加することが望ましい。クラウド利用者は，システム利用標準には組織のセキュリティ基本方針

とクラウド事業者のセキュリティ基本方針が組織のセキュリティ基本方針に反しないことを確認することが望ましい。

クラウド利用者は，クラウドサービスにおいて実施されている管理策が，組織のセキュリティ上の要求事項と整合しているかを分析・評価することが望ましい。この分析・評価の結果，情報セキュリティ要求事項を満たしていないと判断した場合，クラウドサービスの利用の制限や他の管理策の導入について検討することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウドサービスで実装（提供）している情報セキュリティ対策及び機能を列記し，開示することが望ましい。

クラウドサービスの関連情報

クラウド事業者によっては独自のオペレーティングシステムなどを利用している場合がある。この場合は標準的なオペレーティングシステムと違ってクラウド事業者からしかぜい弱性情報などを得ることができないことに留意すること。その場合，クラウド利用者は，クラウドサービスを単なるアウトソーシングと想定せずに，自らのシステムの一部としてクラウドサービスを把握し，クラウド事業者とのコミュニケーションをとりながら，情報セキュリティ対策を考慮することが期待される。

12.2 業務用ソフトウェアでの正確な処理

目的：業務用ソフトウェアにおける情報の誤り，消失，認可されていない変更又は不正使用を防止するため。

利用者が開発した業務用ソフトウェアを含め，正しい処理を確実にするために，業務用ソフトウェアに適切な管理策を設計して組み入れることが望ましい。これらの管理策には，入力データ，内部処理及び出力データの妥当性確認を含めることが望ましい。

慎重な取扱いを要する，価値の高い，又は重要な情報を処理するシステム，又はそれらに影響を及ぼすシステムには，更なる管理策が必要となる場合もある。そのような管理策は，セキュリティ要求事項及びリスクアセスメントに基づいて決めることが望ましい。

12.2.1 入力データの妥当性確認

管理策

業務用ソフトウェアに入力するデータは，正確で適切であることを確実にするために，その妥当性を確認することが望ましい。

12.2.2 内部処理の管理

管理策

処理の誤り又は故意の行為によって発生する情報の破壊を検出するために，妥当性確認の機能を業務用ソフトウェアに組み込むことが望ましい。

12.2.3 メッセージの完全性

管理策

業務用ソフトウェアの真正性を確実にするための要求事項及びメッセージの完全性を保護するための要

求事項を特定し，また，適切な管理策を特定し，実装することが望ましい。

12.2.4 出力データの妥当性確認

管理策

業務用ソフトウェアからの出力データは，保存する情報の処理が正しく，かつ，状況に対して適切であることを確実にするために，妥当性確認をすることが望ましい。

12.3 暗号による管理策

目的：暗号手段によって，情報の機密性，真正性又は完全性を保護するため。

暗号による管理策の利用に関する方針を策定することが望ましい。暗号技術の利用を支持するために，かぎ管理を備えることが望ましい。

12.3.1 暗号による管理策の利用方針

管理策

情報を保護するための暗号による管理策の利用に関する方針は，策定し，実施することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービス上で利用する情報の暗号化機能が提供されていることを確認することが望ましい。クラウド利用者は，クラウドサービスにおいて提供されている情報の暗号化機能が，暗号による管理策の利用に関する方針に照らして適切であるか確認することが望ましい。

クラウド利用者は，クラウドサービスを利用するネットワーク経路が暗号化されていることを確認することが望ましい。クラウド利用者は，クラウドサービスで利用する情報がシステム上で暗号化されていることを確認することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，暗号化に対応しているサービスを明確にし，クラウド利用者に明示することが望ましい。クラウド事業者は，暗号化されないサービスについて代替機能があれば明確にし，開示することが望ましい。

クラウドサービスの関連情報

クラウドサービスの暗号化では特殊なデータ管理を行っている場合が多く，組織の手順書に定めた暗号化技術が適用できない場合がある。そのため，クラウド利用者は，資産分類に従った機密性確保のための暗号化が実施できるかどうかを確認し，サービスの選択，付加機能の選択を行うことが期待される。

12.3.2 かぎ（鍵）管理

管理策

組織における暗号技術の利用を支持するために，かぎ管理を実施することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービスで管理すべき暗号かぎを識別し，かぎ管理手順を定めることが望ましい。

クラウド利用者は，クラウドサービスにおけるかぎ管理手順について，必要に応じて次のような情報を求めることが望ましい。

a) かぎの種類

b) かぎのライフサイクル（生成，変更，更新，保管，失効，回収，維持，破壊）の各プロセスにおける手順を含むかぎ管理システムの仕様

c) クラウド利用者側での実施が推奨される事項

クラウド事業者の実施が望まれる事項

クラウド事業者は，提供するクラウドサービスにおけるかぎ管理をクラウド利用者が実施できるよう，かぎ管理に関する情報提供の方針を定め，クラウド利用者に明示することが望ましい。

クラウドサービスの関連情報

クラウドサービス（特に SaaS）においては独自の認証を行っている場合があり，既に運用している認証とかぎ管理の仕組みとの連携がとれない場合がある。クラウド利用者は，システムの要求事項に適応したかぎ管理ができるかどうかを確認し，必要に応じて要求を満たす認証方式と連携して管理することが期待される。

12.4 システムファイルのセキュリティ

目的：システムファイルのセキュリティを確実にするため。

システムファイル及びプログラムソースコードへのアクセスを制御することが望ましい。IT プロジェクト及びサポート活動は，セキュリティを確保した上で実施することが望ましい。取扱いに慎重を要するデータが試験環境から漏えいすることを防止するように留意することが望ましい。

12.4.1 運用ソフトウェアの管理

管理策

運用システムにかかわるソフトウェアの導入を管理する手順を備えることが望ましい。

クラウドサービスの関連情報

PaaS では実行環境のみが提供され，試験運用のプログラムと本番運用のプログラムを区別することが難しい場合がある。そのように，試験運用と本番運用のプログラムを実行環境上で区別することができない場合には，実行時に試験運用のプログラムを削除するか，試験運用と本番運用で別のアカウントを取得し，個別に管理することが期待される。

12.4.2 システム試験データの保護

管理策

試験データは，注意深く選択し，保護し，管理することが望ましい。

12.4.3 プログラムソースコードへのアクセス制御

管理策

プログラムソースコードへのアクセスは，制限することが望ましい。

クラウドサービスの関連情報

PaaS ではスクリプト言語を利用しているものが多く，ソースをそのまま実行環境に置かざるをえないことが多い。クラウド利用者は，プログラムソースコードの保護の観点で，どのようにコードを管理するかを明確にし，新たな手順を作成することが期待される。

12.5 開発及びサポートプロセスにおけるセキュリティ

目的：業務用ソフトウェアシステムのソフトウェア及び情報のセキュリティを維持するため。

プロジェクト及びサポート環境は，厳しく管理することが望ましい。

業務用ソフトウェアシステムに責任をもつ管理者は，プロジェクト又はサポート環境のセキュリティにも責任を負うことが望ましい。変更によってシステム又は運用環境のセキュリティが損なわれないことを点検するために，管理者は，提案されているすべてのシステム変更のレビューを，確実にすることが望ましい。

12.5.1 変更管理手順

管理策

変更の実施は，正式な変更管理手順の使用によって，管理することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，変更管理手順にクラウドサービスに関する内容を追加することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウドサービスの変更に関して，必要に応じて次の事項を実施することが望ましい。

a) システム変更の実施に関するクラウド利用者への通知

b) システム機能の追加・変更に関するクラウド利用者への通知

c) ソフトウェアの更新についての版数の管理

d) システム変更についての監査証跡・変更履歴の管理及び利用者への提示

クラウドサービスの関連情報

クラウドサービスの利用においてはスケーラビリティの確保が十分になされているとはいえ，マルチテナントであることを考慮すれば，ある一定時期に十分なサービスが得られない場合があることに留意すること。また，IaaS や PaaS の契約形態においては自動的に帯域を確保する機能を有していないものもある。スケーラビリティ以外の変更管理においても同様に，自動化されたシステムに依存せずに，クラウド利用者自らが管理できる手順を明確にすることが期待される。

12.5.2 オペレーティングシステム変更後の業務用ソフトウェアの技術的レビュー

管理策

オペレーティングシステムを変更するときは，組織の運用又はセキュリティに悪影響がないことを確実にするために，重要な業務用ソフトウェアをレビューし，試験することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，オペレーティングシステムやウェブブラウザのクラウドサービスへの対応状況を確認することが望ましい。クラウド利用者は，業務用ソフトウェアのレビュー手順にオペレーティングシステムやウェブブラウザのクラウドサービスへの対応状況の確認を追加することが望ましい。クラウド利用者は，利用しているクラウドサービスが対応するオペレーティングシステムやウェブブラウザやクライアント（端末含む）の対応状況を確認することが望ましい。

クラウド利用者は，クラウドサービスのオペレーティングシステムに変更があった場合，クラウド利用者が管理するアプリケーションの技術的レビューを実施することが望ましい。

クラウド利用者が管理するアプリケーションに重大な影響を及ぼす可能性があるクラウドサービスのオペレーティングシステム変更については，クラウド事業者により情報が提供されることを確実にし，アプリケーションの技術レビューを実施することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウドサービスを利用することができるオペレーティングシステムやウェブブラウザの種類とバージョンを明示することが望ましい。クラウド事業者は，クラウドサービスを利用することができるオペレーティングシステムやウェブブラウザの種類とバージョンに変更が生じる場合は，あらかじめクラウド利用者に通知することが望ましい。

クラウドサービスの関連情報

クラウドサービスのクラウド利用者側のインタフェースはウェブブラウザを利用することが多い。クラウドサービスではリッチインタフェースの実現のために様々な技術を提供している場合があるが，ブラウザの種類やバージョンによってはそれらの機能を活用できない場合がある。オペレーティングシステムのバージョンアップとともにクライアントのウェブブラウザがアップデートされることも考慮して，オペレーティングシステムアップデートの際には動作テストを行うことが期待される。

12.5.3 パッケージソフトウェアの変更に対する制限

管理策

パッケージソフトウェアの変更は，抑止し，必要な変更だけに限ることが望ましい。また，すべての変更は，厳重に管理することが望ましい。

12.5.4 情報の漏えい

管理策

情報の漏えいの可能性を抑止することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，情報漏えいが起きないように，クラウドサービスの利用手順を策定することが望ましい。クラウド利用者は，情報漏えいの可能性を考慮して，クラウドサービスの利用者にリスクと対策を周知することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウドサービスにおける情報漏えいに関する対策を行い，円滑なシステムの運用に支障のない範囲でクラウド利用者にその対策内容を開示することが望ましい。

クラウドサービスの関連情報

クラウドサービスではデータを一つのサーバ上に保存するのではなく，複数のサーバ上に分散して配置され，更に冗長性を高めるために，分割されたデータが複製されて複数のサーバ上に配置されることも多い。そのため，データの移動や削除などに伴ってすべてのデータが完全に消去をされず，残存オブジェクトとしてデータの一部が残ってしまう可能性がある。そのため，資産分類において完全消去を前提としているデータについては取扱いに慎重を要する。

12.5.5 外部委託によるソフトウェア開発

管理策

組織は，外部委託したソフトウェア開発を監督し，監視することが望ましい。

12.6 技術的ぜい弱性管理

目的：公開された技術的ぜい弱性の悪用によって生じるリスクを低減するため。

技術的ぜい弱性の管理は，効果的，体系的及び再現可能な方法で，その効果を確かめるための測定を伴って実施することが望ましい。これらの考慮は，利用しているオペレーティングシステム及びあらゆる業務用ソフトウェアに適用することが望ましい。

12.6.1 技術的ぜい弱性の管理

管理策

利用中の情報システムの技術的ぜい弱性に関する情報は，時機を失せずに獲得することが望ましい。また，そのようなぜい弱性に組織がさらされている状況を評価し，それと関連するリスクに対処するために，適切な手段をとることが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，技術的ぜい弱性についての情報収集について手順化し，利用しているクラウドサービスとの関連の有無を確認することが望ましい。クラウド利用者は，クラウド事業者から技術的ぜい弱性について情報を収集することが望ましい。クラウド利用者は，クラウド事業者以外の信頼できる情報源からぜい弱性について情報を収集することが望ましい。

クラウド利用者は，クラウドサービスにおける技術的ぜい弱性の管理について理解することが望ましい。クラウドサービスにおける技術的ぜい弱性の管理がクラウド利用者のセキュリティ要求事項に適合しない場合，クラウド利用者による対策の実施を検討することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，提供するクラウドサービスに関連するリスクについて情報収集を行うことが望ましい。クラウド事業者は，必要に応じてぜい弱性や脅威に関する情報をクラウド利用者に通知することが望ましい。

クラウドサービスの関連情報

クラウドサービスではクラウド事業者が独自技術を利用している事が多く，仕様が公開されていないためにクラウド利用者自らがぜい弱性に対応することが難しい。また，クラウド利用者同士の情報交換が難しいために，セキュリティ関連の情報についてクラウド事業者依存となる可能性が高い。クラウド利用者が，独自技術を利用してクラウドサービスを展開しているクラウド事業者と契約する際には，ぜい弱性に関する情報提供が行われるように要求することが期待される。また，クラウドサービスでは，クラウド事業者が用意したソフトウェアであっても，クラウド利用者にその管理権限と責任があり，クラウド事業者がそのソフトウェアの技術的ぜい弱性を管理しない場合がある。したがって，クラウド利用者は技術的ぜい弱性の管理責任にかかわるサービス内容及び契約内容を確認することが期待される。なお，技術的ぜい弱性の管理は，変更管理の従属機能とみなすことができるため，変更管理のプロセス（10.1.2）及び手順

（12.5.1）が利用できる。

13 情報セキュリティインシデントの管理

13.1 情報セキュリティの事象及び弱点の報告

目的：情報システムに関連する情報セキュリティの事象及び弱点を，時機を失しない是正処置をとることができるやり方で連絡することを確実にするため。

事象の報告及び段階的取扱いの正式な手順を備えることが望ましい。すべての従業員，契約相手及び第三者の利用者に，組織の資産のセキュリティに影響を及ぼす場合がある様々な形態の事象及び弱点についての報告手順を認識させておくことが望ましい。すべての従業員，契約相手及び第三者の利用者に，いかなる情報セキュリティの事象及び弱点も，できるだけすみやかに指定された連絡先に報告するよう要求することが望ましい。

13.1.1 情報セキュリティ事象の報告

管理策

情報セキュリティ事象は，適切な管理者への連絡経路を通して，できるだけすみやかに報告することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービスの利用者が利用中に気づいた事象について報告し，集約できる体制を構築することが望ましい。クラウド利用者は，クラウドサービスにおける情報セキュリティインシデントを定義することが望ましい。クラウド利用者は，情報セキュリティインシデントをクラウドサービスの利用者が理解し，発生時に報告できるようにすることが望ましい。クラウド利用者は，情報セキュリティインシデントをクラウド事業者に報告できる手順を策定することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，情報セキュリティインシデントを受け付ける窓口を設置することが望ましい。クラウド事業者は，クラウドサービス自体のトラブル発生時でも情報セキュリティインシデントに対応できる窓口を運用することが望ましい。

クラウドサービスの関連情報

組織事業の基礎を成す情報及びその情報を取り扱うプロセス，システム並びにネットワークの多くを，組織内に保持する場合と比べて，クラウドサービス利用においてはサーバの監視やログの取得が自由にできないことが多い。リアルタイム監視や膨大なログの解析といったことを前提としたインシデントレスポンスを行うことができない場合は，事前に取得できる情報を明確にし，それを前提に判断できる内容を情報セキュリティインシデントとして定義しなおすことが期待される。

13.1.2 セキュリティ弱点の報告

管理策

すべての従業員，契約相手並びに第三者の情報システム及びサービスの利用者に，システム又はサービスの中で発見した又は疑いをもったセキュリティ弱点は，どのようなものでも記録し，また，報告するよ

うに要求することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービスのセキュリティ上の弱点に気づいた場合に記録し，報告する手順を策定することが望ましい。クラウド利用者は，当該サービスにおいてセキュリティ上の問題を発見した場合に，クラウド事業者に報告する手順を策定することが望ましい。

13.2 情報セキュリティインシデントの管理及びその改善

目的：情報セキュリティインシデントの管理に，一貫性のある効果的な取組み方法を用いることを確実にするため。

情報セキュリティの事象及び弱点の報告があったとき直ちに，それらを効果的に取り扱える責任体制及び手順を備えることが望ましい。情報セキュリティインシデントへの対応，並びに情報セキュリティインシデントの監視，評価及び包括的管理に対して，継続的改善の手続をとることが望ましい。

証拠が必要となる場合は，法的要求事項を順守することを確実にするために，証拠を収集することが望ましい。

13.2.1 責任及び手順

管理策

情報セキュリティインシデントに対する迅速，効果的で整然とした対応を確実にするために，責任体制及び手順を確立することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，情報セキュリティインシデントに対する迅速な対応ができるように体制を構築することが望ましい。クラウド利用者は，クラウドサービスにおける情報セキュリティインシデント発生時の対応責任者を決めることが望ましい。クラウド利用者は，情報セキュリティインシデント対応の手順にクラウドサービスに関連する内容を追加することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウドサービスにおける重大な情報セキュリティインシデントを定義することが望ましい。また，インシデント対応についての情報提供の方針を定め，クラウド利用者に提示することが望ましい。

クラウド事業者は，他の事業者との合意に基づき，サプライチェーン上で重大な情報セキュリティインシデントが生じたときに共有すべき情報を文書化することが望ましい。

クラウドサービスの関連情報

クラウドサービスではサーバのリアルタイム監視や，ログの柔軟な管理が困難なため，情報セキュリティインシデントにクラウドサービスの利用者が最初に気づく可能性がある。このため，情報セキュリティインシデントのエスカレーション手順を見直し，クラウドサービスの利用者からの情報提供が行われやすい環境を考慮する必要がある。

13.2.2 情報セキュリティインシデントからの学習

管理策

情報セキュリティインシデントの形態，規模及び費用を定量化し監視できるようにする仕組みを備えることが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービスの情報セキュリティインシデントについて記録し定量化することが望ましい。クラウド利用者は，クラウドサービスに関するセキュリティインシデントを記録し，定量化することが望ましい。クラウド利用者は，事故の発生や影響を軽減するために定量化した情報をクラウド事業者と共有することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド利用者が情報セキュリティインシデントを評価できるよう，クラウド事業者は，クラウド利用者との合意に基づき次の情報を提供することが望ましい。

a) 情報セキュリティインシデントの統計情報
b) 情報セキュリティインシデントによる影響
c) 情報セキュリティインシデントへの対応
d) 情報セキュリティインシデントへの予防策

クラウドサービスの関連情報

クラウドサービスではサーバの監視やログ管理が困難なために，クラウド利用者は，サーバ上の情報セキュリティインシデントに関する情報を自ら取得することが難しい。そのため，クラウド利用者は，クラウド事業者の情報を基に情報セキュリティインシデントの定量化を行い，情報セキュリティインシデントの予測などを行うことができる体制づくりを考慮する必要がある。

13.2.3 証拠の収集

管理策

情報セキュリティインシデント後の個人又は組織への事後処置が法的処置（民事又は刑事）に及ぶ場合には，関係する法域で定めている証拠に関する規則に従うために，証拠を収集，保全及び提出することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，情報セキュリティ事故が法的処置に及ぶ場合を想定して，必要な証拠の収集，保全を実施することが望ましい。また，クラウド事業者がそれらの情報を保管しているか確認することが望ましい。

クラウド事業者がクラウド利用者の法的証拠となり得る情報を管理する場合，クラウド利用者は，次の手順を実施することが望ましい。

1. クラウド利用者にとって法的証拠となり得る情報を明確にする
2. クラウド事業者によって管理されている情報が記録され，適切に保管されているかを確認する
3. クラウド事業者によって管理されている情報を収集・保持する
4. 収集した情報の中で、クラウド利用者にとって証拠として活用できる情報を識別し、保全する

クラウド利用者は，クラウド事業者がクラウド利用者にとって法的証拠となり得る情報を管理する場合，

クラウド事業者に情報を求めることが望ましい。
クラウド利用者は，クラウドサービスに関して法的な要求に基づいてログなどの証拠を取得することが望ましい。クラウド利用者は，クラウドサービスに関して法的な要求に基づいてログなどの証拠を必要期間保存することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，法的な証拠となる可能性がある情報については記録し，適切に保管しておくことが望ましい。クラウド事業者は，どのような記録がどの程度の期間保管されているかをクラウド利用者に明示することが望ましい。

クラウドサービスの関連情報

クラウドサービスの利用においてはコスト削減のために保存データの容量を必要最低限にすることがある。そのため，外部の継続的証拠保全のためのサービス（e-discovery サービスやリモートジャーナリングサービスなど）を別途契約するなどの方法もある。

14 事業継続管理

14.1 事業継続管理における情報セキュリティの側面

目的：情報システムの重大な故障又は災害の影響からの事業活動の中断に対処するとともに，それらから重要な業務プロセスを保護し，また，事業活動及び重要な業務プロセスの時機を失しない再開を確実にするため。

組織への影響を最小に抑えるため，及び予防的管理策と回復のための管理策との組合せによって，情報及び情報処理施設に関連する資産の損失（例えば，自然災害，事故，装置の故障及び悪意による行為の結果の場合がある。）を受容可能なレベルにまで回復するために，事業継続管理手続を実施することが望ましい。この手続では，重要な業務プロセスを識別すること，並びに運用，要員配置，資材，配送及び設備といった点で関連する，情報セキュリティ管理面以外の事業継続の要求事項と情報セキュリティ管理面の事業継続の要求事項とを統合することが望ましい。

災害，セキュリティ不具合及びサービス停止の結果，並びにサービスの可用性を，事業の影響分析の対象とすることが望ましい。必要不可欠な運用の時機を失しない再開を確実にするために，事業継続計画を策定し，実施することが望ましい。情報セキュリティは，組織の包括的な事業継続手続及びその他の管理手続の，必要不可欠な部分であることが望ましい。

事業継続管理には，リスクを特定して低減するための管理策のほか，リスクアセスメントの手続に加え，損害を与えるインシデントの影響を抑制するための管理策，及び業務プロセスに必要な情報が常に利用可能であることを確実にするための管理策を含むことが望ましい。

14.1.1 事業継続管理手続への情報セキュリティの組込み

管理策

組織全体を通じた事業継続のために，組織の事業継続に必要な情報セキュリティの要求事項を取り扱う，管理された手続を，策定し，維持することが望ましい。

14.1.2 事業継続及びリスクアセスメント

管理策

業務プロセスの中断を引き起こし得る事象は，そのような中断の発生確率及び影響，並びに中断が情報セキュリティに及ぼす結果とともに，特定することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービス利用が事業継続にどのような影響を及ぼすかを判断し，要求事項としてまとめることが望ましい。クラウド利用者は，クラウドサービスが関与する業務を特定することが望ましい。クラウド利用者は，クラウドサービスが関係する資産を特定し，クラウドサービス利用に関連する情報セキュリティインシデントが業務に及ぼす影響を特定し，クラウドサービスの利用に係る事業継続についてリスク識別し，評価することが望ましい。

クラウド利用者は，リスクアセスメントにおいてはクラウド事業者と調整し，技術的・運営的な背景なども検討することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウドサービスのサービスレベルについて中断の発生確率及び影響，並びに中断が情報セキュリティに及ぼす結果とともに，特定することが望ましい。

クラウドサービスの関連情報

クラウドサービスにおけるサービスレベルは SaaS, PaaS, IaaS がそれぞれ依存関係にある場合もあり，特に SaaS では高稼働率を実現することが難しい場合がある。そのため，業務において本来必要な稼働率を検討し（例えば，システムの最大許容停止時間及び目標復旧時間の設定），SLA などによって確認することが期待される。

14.1.3 情報セキュリティを組み込んだ事業継続計画の策定及び実施

管理策

重要な業務プロセスの中断又は不具合発生の後，運用を維持又は復旧するために，また，要求されたレベル及び時間内での情報の可用性を確実にするために，計画を策定し，実施することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，リスクアセスメントの結果に応じて，クラウドサービスにおける冗長化の状況を確認することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウドサービスを提供するシステムの冗長化を図ることが望ましい。

クラウド事業者は，クラウドサービスの冗長化の状況を，クラウドサービスの利用を検討する者に明示することが望ましい。

クラウドサービスの関連情報

事業継続管理におけるクラウドサービスの関係は情報システムの稼働率だけではなく，クラウドサービス上で作成されたデータを他のシステムに持ち出すことができるか，また現在利用しているシステムからデータを容易に持ち込むことができるかなども検討することが期待される。さらに，システムの最大許容停止時間を考慮してこれらの課題に対して検討する必要がある。クラウドサービスを提供するシステムの

冗長化を図る観点として，次のようなものがある。

a) データのバックアップ

b) データセンター

c) サポートユーティリティ（例えば，電源，ケーブル配線施設やそれらのコントローラなど）

d) ハードウェア

e) クラウドプラットフォーム

f) クラウド制御システム

14.1.4 事業継続計画策定の枠組み

管理策

すべての計画が整合したものになることを確実にするため，情報セキュリティ上の要求事項を矛盾なく取り扱うため，また，試験及び保守の優先順位を特定するために，一つの事業継続計画の枠組みを維持することが望ましい。

14.1.5 事業継続計画の試験，維持及び再評価

管理策

事業継続計画が最新で効果的なものであることを確実にするために，定めに従って試験・更新することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，事業継続計画の試験及び更新において，クラウド事業者が関与可能かを確認することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウド利用者の事業継続計画の試験・更新に関する協力可否について，クラウド利用者との合意に基づき情報を提供することが望ましい。

クラウドサービスの関連情報

クラウド利用者は，サービス可用性について適切な条項を契約に規定し，クラウド利用者の事業継続計画の試験・更新に組み込むことが推奨される。

クラウド事業者は，リソースやインフラなどの高集約によるインシデントの影響の拡大がクラウドの特徴であることを踏まえ，クラウドサービス提供にかかわるクラウド事業者組織における教育訓練の内容を適時に見直し，障害対応要員の定期的及び必要に応じた教育・訓練を実施することが期待される。

クラウド利用者が事業継続に係るリスクアセスメントを実施する際に考慮すべき事項には，次のようなものがある。

a) クラウドサービスの障害などによる停止

b) 法執行機関の要請によるサービスの一時停止

c) クラウドサービスの終了

d) 財務状況の変化に伴うクラウド事業者の変更

クラウド事業者は，クラウド利用者の事業継続計画策定・実施に関連して，クラウド利用者との合意に基づき，次のような情報を提供することが望ましい。

a) クラウド事業者の災害復旧計画

b) システムの多重化など，可用性を確実にするための対策

c) クラウドサービスの目標復旧時間

15 順守

15.1 法的要求事項の順守

目的：法令，規制又は契約上のあらゆる義務，及びセキュリティ上のあらゆる要求事項に対する違反を避けるため。

情報システムの設計，運用，利用及び管理には，法令，規制及び契約上のセキュリティ要求事項が適用される場合がある。

特定の法的要求事項については，組織の法律顧問又は適切な資格をもつ法律の実務家に助言を求めることが望ましい。法律の定める要求事項は，国ごとに異なっており，また，一つの国で作成され別の国へ伝送される情報（すなわち，国境を越えたデータの流れ）についても異なる場合がある。

15.1.1 適用法令の識別

管理策

各情報システム及び組織について，すべての関連する法令，規則及び契約上の要求事項並びにこれらの要求事項を満たすための組織の取組み方を，明確に定め，文書化し，また，最新に保つことが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドコンピューティングサービスに関する法執行機関が，複数の国／地域に関連し得ることを鑑み，クラウド事業者に対して情報提供を求めることが望ましい。クラウド利用者は，クラウドコンピューティングサービスに関する管轄裁判所について，クラウド事業者に対して情報提供を求めることが望ましい。

クラウド利用者は，クラウドサービスの利用目的に応じて，クラウド利用者自らが適用を受ける法令，規制及び契約上の要求事項などを洗い出すことが望ましい。クラウド利用者は，クラウドサービスの利用契約に定められた準拠法と裁判管轄を確認し，文書化することが望ましい。クラウド利用者は，クラウド事業者が適用を受ける法令を調査し，文書化することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，複数の国／地域の法執行機関がかかわるクラウドサービスを提供している場合，それらの国／地域についてクラウド利用者に知らせることが望ましい。クラウド事業者は，国家連合，国，州，地方自治体により法規制が異なるかを確認し，それぞれの国家連合，国，州，地方自治体の名称をクラウド利用者に明示することが望ましい。クラウド事業者は，関連する法規制について，それぞれの管轄裁判所の場所を明示することが望ましい。

クラウド事業者は，クラウド事業を営む地域（国，州など），データセンターの所在する地域（国，州など）及びクラウド事業者自らが適用を受ける法令，規制及び契約上の要求事項を明示することが望ましい。

クラウド事業者は，他のクラウド事業者が提供するクラウドサービスを利用している場合，利用しているクラウドサービスの裁判管轄及び適用を受ける法令・規制を確認・文書化し，最新に保つことが望ましい。

クラウド事業者は，クラウド利用者との合意に基づき，法令，規制及び契約上の要求事項が適用される地理的場所にクラウド利用者のデータが保持されていることを確実にするため，法的順守を監視することが望ましい。

クラウドサービスの関連情報

SaaS として契約しているクラウド事業者が国内企業であったとしても，そのバックボーンとなる PaaS や IaaS のクラウド事業者が海外の企業である場合もあるため，クラウド事業者が事業を行う国の法律や業界団体の慣習などについても洗い出し，検討することが期待される。

適用法令は，私法と公法を分けて識別することが望ましい。例えば，私人間に適用される法は「当事者が当該法律行為の当時に選択した地の法による」（法の適用に関する通則法第 7 条）である。つまり，契約時に準拠法を定めるのが一般的であるため，契約当事者間の適用法令が問題になることは少ない。一方，国家がかかわる公法の適用は，原則として属地的に定まる。外国法人でも日本国内において事業を行う限り，原則として国内法の適用を受け，逆に日本法人でも外国において事業を行う限り，外国法の適用を受けることがある。例えば，データセンターが外国にあっても我が国で事業を営む企業は，我が国の捜査機関の捜査を受け，外国のサーバ内の情報が差押えられることがあり，逆にデータセンターが国内にあっても外国で事業を営む企業は，その国の捜査機関の捜査を受け，我が国のサーバ内の情報が差押えられることがある。

15.1.2 知的財産権（IPR）

管理策

知的財産権が存在する可能性があるものを利用するとき，及び権利関係のあるソフトウェア製品を利用するときは，法令，規則及び契約上の要求事項の順守を確実にするための適切な手順を導入することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウド利用の目的に合せ，知的財産権の要求事項を確認することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，自らの知的財産権についてクラウド利用者に利用を許諾する範囲及び制約を，クラウド利用者に通知することが望ましい。

15.1.3 組織の記録の保護

管理策

重要な記録は，法令，規制，契約及び事業上の要求事項に従って，消失，破壊及び改ざんから保護することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービス上で利用する重要な記録は法令や規制に従って保護することが望ましい。クラウド利用者は，クラウドサービス上で利用する重要な記録は必要に応じて取り出せるように

保管することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，法令や規制に従って，クラウドサービス上の記録を保護することが望ましい。

クラウドサービスの関連情報

クラウドサービスでは，国内外問わず，様々なクラウド事業者を利用する事ができる。しかし，クラウド事業者の中には，特定国内における法律に対応できないクラウド事業者がある可能性もある。そのため，遵守すべき法律を考慮して記録の保管を適切に行うことができるクラウド事業者を選択するか，自ら記録を保管する体制を構築することが期待される。

15.1.4 個人データ及び個人情報の保護

管理策

個人データ及び個人情報の保護は，関連する法令，規制，及び適用がある場合には，契約条項の中の要求に従って確実にすることが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービスで個人情報を利用する際には，法令及び組織の個人情報護方針に従って利用できるように適切な手順を策定することが望ましい。

クラウド利用者は，クラウドサービスの利用目的に応じて，データ保護及び個人情報保護に係る，国内外の法令，規則及び契約上の要求事項を識別することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウド利用者がデータの保護及び個人情報保護に関する法規制を識別できるよう，自らのクラウドサービスに影響を及ぼす法的管轄に関する国／地域の情報を提供することが望ましい。

クラウドサービスの関連情報

個人情報保護法の要求事項及び当該要求事項の実現のために企業等が定める規程に対応できないクラウド事業者が存在するかもしれない。そのため，個人情報保護に関する基準や手順がクラウド事業者の提供するクラウドサービスに合致するかどうかを検討することが期待される。

15.1.5 情報処理施設の誤用防止

管理策

認可されていない目的のための情報処理施設の利用は，阻止することが望ましい。

15.1.6 暗号化機能に対する規制

管理策

暗号化機能は，関連するすべての協定，法令及び規制を順守して用いることが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，暗号技術をクラウドサービス上で利用する際には，輸出規制などに抵触しないか確認することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウド利用者が輸出規制などに抵触しないよう，暗号化機能にかかわる法令などの情報をクラウド利用者に提供することが望ましい。

クラウドサービスの関連情報

暗号化技術については輸出規制などの問題もあり，海外のクラウド事業者のデータセンターに配置できない場合もある。クラウドサービス上で暗号化機能を利用する場合には，輸出規制などに抵触する可能性について十分に検討する必要がある。

15.2 セキュリティ方針及び標準の順守，並びに技術的順守

目的：組織のセキュリティ方針及び標準類へのシステムの順守を確実にするため。

情報システムのセキュリティは，定めに従ってレビューすることが望ましい。

このようなレビューは，適切なセキュリティ方針及び技術的基盤と対照して行うことが望ましい。また適用されるセキュリティ実施標準及び文書化されたセキュリティ管理策を順守していることについて，情報システムを監査することが望ましい。

15.2.1 セキュリティ方針及び標準の順守

管理策

管理者は，セキュリティ方針及び標準類への順守を達成するために，自分の責任範囲におけるすべてのセキュリティ手順が正しく実行されることを確実にすることが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービスに関連する新しい規程や管理策が既存の規程や管理策同様に順守されるようにすることが望ましい。クラウド利用者は，クラウドサービスに関連する標準や手順が，既存の情報セキュリティ基本方針に合致しているかをレビューすることが望ましい。クラウド利用者は，クラウドサービスが情報セキュリティ基本方針に合致しない場合，原因を調査し，必要に応じて双方を是正することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，独立したレビュー及び評価（例えば，内部／外部監査，認証，ぜい弱性，ペネトレーションテストなど）を定期的に実施し，情報セキュリティ基本方針及び適用される法的要件を組織が遵守していることを確実にすることが望ましい。また，クラウド事業者は，クラウド利用者の個別の監査要求に応える代わりに，クラウド利用者との合意に基づき，独立したレビュー及び評価の結果を提供することが望ましい。

クラウドサービスの関連情報

クラウドサービスの利用においては現在運用している管理策やセキュリティ要件に合致する機能を有していない場合が考えられる。特に SaaS においては，個別に機能の付加が容易ではないため，必要に応じてその他のサービスを利用したり，代替する機能を検討したりすることが望ましい。PaaS においても場合によってはこれまでに利用してきた API などが利用できないこともある。そのため，実行環境の制限などを十分に精査して，セキュリティを損なわないように標準などを見直すことが期待される。

15.2.2 技術的順守点検

管理策

情報システムを，セキュリティ実施標準の順守に関して，定めに従って点検することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービスが組織の技術的なセキュリティ要求事項に適合しているかを定期的に点検することが望ましい。クラウドサービスでは様々な機能がクラウド事業者主導で追加されることがあるため，クラウド利用者は，これらの機能が組織の技術的なセキュリティ要求事項に合致しているかを確認し，必要に応じて様々な機能の利用の可否を決定することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウドサービスが組織の技術的なセキュリティ要求事項に適合しているかを定期的に点検し，その結果を情報提供の方針に基づいてクラウド利用者に開示することが望ましい。

クラウドサービスの関連情報

SaaS では機能の追加がされた場合に，一般利用者権限で機能の利用が可能になる場合がある。クラウド利用者は，セキュリティ要求事項に合致しない機能は管理者権限で停止できるかどうかを確認し，必要に応じて機能の制限ができることを確認することが期待される。

15.3 情報システムの監査に対する考慮事項

目的：情報システムに対する監査手続の有効性を最大限にするため，及びシステムの監査プロセスへの干渉及び／又はシステムの監査プロセスからの干渉を最小限にするため。

情報システムの監査中には，運用システム及び監査ツールを保護するための管理策があることが望ましい。

監査ツールの完全性を守るため，及びその不正使用を防止するための保護も要求される。

15.3.1 情報システムの監査に対する管理策

管理策

運用システムの点検を伴う監査要求事項及び活動は，業務プロセスの中断のリスクを最小限に抑えるために，慎重に計画され，合意されることが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービスの監査について方針を定めることが望ましい。クラウド利用者は，クラウドサービスを監査する場合において，全体的な業務プロセスの中断リスクを最小限にするための予防措置を行うことが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウドサービスの監査について方針を定め，監査を定期的に実施することが望ましい。クラウド事業者は，クラウドサービスを監査する場合において，全体的な業務プロセスの中断リスクを最小限にするための予防措置を行うことが望ましい。

また，クラウド事業者は，クラウド利用者との合意に基づき，利用者の情報システム監査実施に有用な情報を提供することが望ましい。

クラウドサービスの関連情報

クラウド事業者を監査対象に入れた場合，複数のデータセンターにデータが分散されていたり，実際のデータの所在がどのサーバにあるのかを特定することができないなど，物理的に幾つかの管理策に対して

監査が実施できないという問題に直面する可能性がある。そのため，クラウド事業者の監査についてはどのような監査を実施するか，あらかじめ監査項目や監査手順を明確にし，監査を実施することが期待される。

クラウド利用者は，利用するクラウドサービスについて自ら監査を実施する代わりに，クラウド事業者が提供する監査報告書を確認することができる。

15.3.2 情報システムの監査ツールの保護

管理策

情報システムを監査するツールの不正使用又は悪用を防止するために，それらのツールへのアクセスは，抑制することが望ましい。

附属書 A（参考）クラウドサービス利用にかかわるリスク

クラウドサービスの利用にかかわるセキュリティリスクを特定するため，先ずクラウドサービスと従来からある類似サービスとを比較する。

クラウドサービスは，共有化されたコンピュータリソース（サーバ，ストレージ，アプリケーションなど）について，利用者の要求に応じて適宜・適切に配分し，ネットワークを通じて提供することを可能とする情報処理サービスである。これと類似のサービスには，データセンターにおけるアウトソーシングの一形態として，ハウジングサービス，ホスティングサービス，又はアプリケーションサービスなどがある。

クラウドサービスとこれら従来型の類似サービスは，どちらもネットワークを通じてデータセンターから提供され，ファシリティやコンピュータリソースを他者と共有することがある点で共通の特徴をもつ。クラウドサービスにかかわるリスクを検討する場合，これら従来型の類似サービスにおけるリスクは依然として存在する（図 5 参照）。

一方，クラウドサービスは，共有化されたコンピュータリソースをクラウド利用者の要求に応じて適宜・適切に配分するために仮想化技術や分散技術を駆使して提供されることが多いが，従来型の類似サービスは，必ずしもこれらの技術が用いられているとは限らない。これらの技術がクラウドサービスのみに用いられているわけではないが，仮想化・分散技術にかかわるリスクとその技術の運用にかかわるリスクは，クラウドサービスにおいて特に考慮すべきリスクであるといえよう。

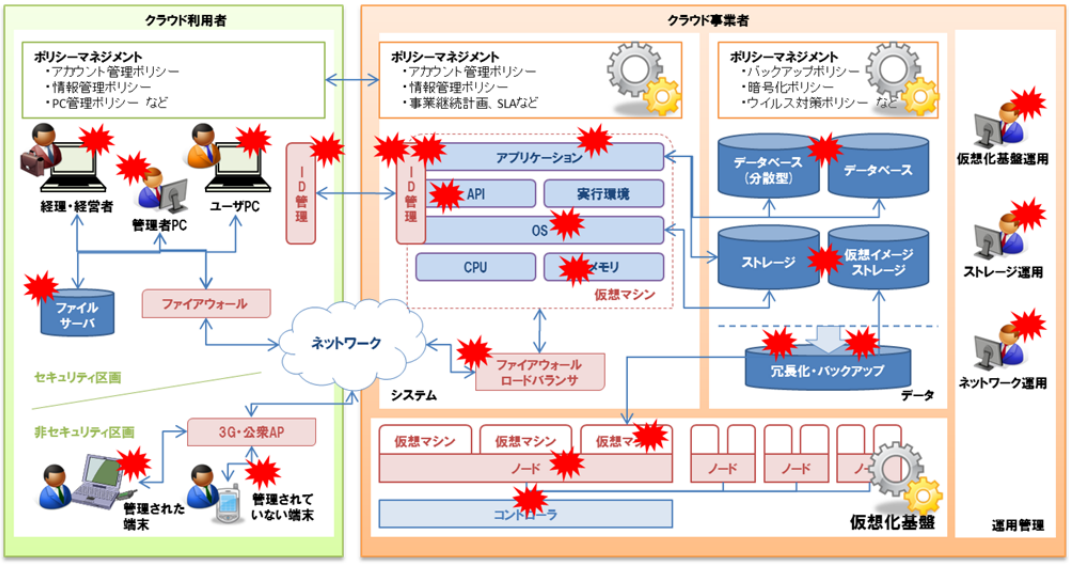

図 5　クラウドサービス利用にかかわるリスク

以下に，クラウドサービスにおいて考慮すべきリスクを例示する。セキュリティ以外の信頼性や稼働性に関するリスクについても参考までに含む。以下のリスクに関して，クラウド事業者は低減するべく努力をすることは当然のことであるが，クラウド利用者についてもリスクを認識し，クラウド事業者の対策を確認することが望ましい。

DoS 攻撃

クラウドサービスはネットワークで提供されるため，DoS 攻撃を受けた場合，すべてのサービスが停止してしまう可能性がある。DoS 攻撃を防御するための仕組がクラウド事業者に依存するため，クラウド利用者は対策を講じることができない。クラウド利用者は，このようにクラウド事業者しか対応できない問題については，あらかじめクラウド事業者に管理策を確認し，DoS 攻撃のリスクを受容するか検討を要する。

ID 管理

クラウドサービスによっては，クラウド利用者が既に利用している ID 管理とクラウドサービスにおける ID 管理を一元的に実施するためのインタフェースがない場合がある。その場合は，管理者の ID 管理に関する工数が増大し，一貫したセキュリティ対策及び管理を行うにあたってミスが発生する可能性が高くなる。そのためクラウド利用者は，ID 管理の連携ができるクラウドサービスを選ぶか，ID 管理が困難になるリスクを受容するか検討を要する。

アクセスポイント

公衆無線 LAN や 3G 回線などによる携帯電話網の普及によって，様々な場所からクラウドサービスを利用できるようになり，ネットワークにおけるアクセス制御が困難になっている。そのため，クラウド利用者は，アクセスポイントを制御できるクラウドサービスを選ぶか，あらかじめ，利便性はあがるが管理は困難になる，ということを認識してクラウドサービスを利用するリスクを受容するか検討を要する。

アクセス制御

利用するクラウドサービスによっては，あらかじめ定められたアクセス権限が，組織で想定するアクセス権とは異なり，アクセス制御が困難になる場合がある。そのため，クラウド利用者は，アクセス制御が管理できるクラウドサービスを選ぶか，あらかじめ，クラウドサービスが定めたアクセス制御を受入れることによるリスクを受容するか検討を要する。

アプリケーション

主に SaaS で提供されるアプリケーションはデスクトップ上で提供されるアプリケーションと違い，機能が制限されていることがある。例えば，デスクトップ用のアプリケーションデータをインポートした場合にすべての条件が反映されないような場合である。また，クラウドサービスで提供されるアプリケーション同士もデータの互換性が十分であるとはいえない。そのため，クラウド利用者は，互換性の高いクラウドサービスを選択するか，あらかじめ互換性に制限がある，ということを認識してクラウドサービスを利用するリスクを受容するか検討を要する。

インシデント管理

インシデント管理には様々な情報が必要になるが，クラウドサービス利用において自らが入手できる情報が制限される場合，クラウド利用者が主体となった対応ができなくなる可能性がある。特に，クラウド事業者が考えるインシデントやイベントのレベルと利用者組織のレベルが合致していないことにより，定められた対応がされなかったり，その発生によるビジネスに対する影響が明確にできなかったりする課題がある。そのため，クラウド利用者は，契約時にインシデントやイベントのレベルを合意するか，あらかじめクラウドサービスが定めたインシデントやイベントのレベルを受入れることによるリスクを受容するか検討を要する。

クラウド事業者の事業継続

クラウド事業者が何らかの理由により事業継続が困難となった場合，若しくは，クラウドサービス自体を戦略的に停止することになった場合，そのクラウド事業者が提供するクラウドサービス利用が制限され，クラウドサービス上の情報が利用できなくなり，クラウドサービス上に保存された情報が消失する可能性がある。そのため，クラウド利用者は通常の取引先としての信頼性の確認だけでなく，クラウドサービスを行う事業部の継続性も確認して，クラウドサービスの利用を決定し，また，クラウドサービスの停止はクラウド事業者が決定するというリスクを受容するか検討を要する。

システム運用・保守

クラウドサービスではシステム自体の保守をしなくても良いというのがメリットの一つではあるが，情報セキュリティの観点では業務の委託はできても責任をすべて委譲することはできない。クラウドを利用していない環境でのセキュリティ規程を満足させるために様々な情報が必要になる。

スケールアウト技術

クラウドコンピューティングにおけるスケールアウトという技術により，ハードウェアを仮想的に連携させ処理能力の高いハードウェアを形成することができる。ハードウェア単体における物理的な能力を超えた環境についての検証が十分できないことから，未知のトラブルが発生する可能性がある。新たな技術の導入に伴う未知のリスクは予知し難く，クラウド利用者は，リスク移転（利用料の減額など）が可能か，それともリスクを受容するか検討を要する。

データセンターの所在

様々な国や場所にデータセンターが設置される場合の，データセンターに従事する従業者の経験やモラルなどによる情報の取扱いの差が，クラウド利用者の懸念事項として挙げられている。様々な国のネットワークの接続性などに伴って，サービスの質などの差による影響が出る可能性が考えられている。そのため，クラウド利用者は，あらかじめデータセンターの所在地の法規の適用にかかわる問題を認識してリスクを受容するかの検討を要する。

データセンターの物理環境

利用者からみたデータセンターのありようは大きく変化していないと考えられるが，クラウドサービスを提供するために新たな技術や運用形態（コンテナ式など）を利用したデータセンターが運営されており，クラウド事業者が経験していない問題が発生する可能性がある。クラウド利用者は，新たな技術や運用形態に起因するリスクの移転（利用料の減額など）が可能か，それともリスクを受容するか検討を要する。

ヘルプデスク

海外のクラウドサービスを利用している場合，ヘルプデスクサービスの対応言語が異なったり，時差や営業日の違いによってサービス日・時間帯が国内と異なる場合がある。そのため，クラウド利用者は，あらかじめ対応言語や対応時間などにかかわるリスクを受容するか検討を要する。

マルチテナント

一つのプラットフォーム上に複数の契約者が同居することにより，プラットフォームを狙った攻撃が実施された場合に対象ではないほかの契約者にも影響が及ぼされることになる。特にクラウドサービス環境においては，どの契約者とどの契約者が同じシステム内で同居しているかがわからないことが問題となる。そのため，クラウド利用者の管理の不備によって引き起こされるリスクについて検討した後，他の契約者の管理不備によって引き起こされるリスクについても検討を要する。

メモリ管理

クラウド事業者では物理的なメモリ管理などが実行できないために，メモリ保護に関するトラブルが発生した場合の問題について，ハードウェアが原因か，仮想化などによる技術的な問題かを切り分けを行うことが難しい。クラウド利用者は，このような技術的なトラブルに対するリスク移転（利用料の減額など）が可能か，それともリスクを受容するか検討を要する。

メンテナンスユーティリティ

システムの状況を知るためのユーティリティが提供されないことによって，情報を適宜入手することができないという課題がある。情報を入手できないことでトラブルの事前判断ができないだけではなく，経営面からみてITの活用状況がわからないなどの課題もある。そのため，クラウド利用者は，あらかじめ情報の把握が困難になるリスクを受容するか検討を要する。

ライセンス管理

クラウドサービスを前提に作成されていないソフトウェアのライセンス体系により，クラウドサービス上でソフトウェアがどのように利用されているのかを正確に把握できないことがある。そのため，ソフトウェア監査におけるトラブルへ発展することがある。クラウド環境を見越したライセンス体系をもつソフトウェアも増加しており，クラウド利用者は，利用するソフトウェアのライセンスの再確認や，場合によっては契約の再確認を要する。

リカバリー

クラウドサービスを利用して顧客向けサービスを提供しているような企業や組織においては，復旧計画を正確に顧客に知らせることができないという問題が発生する。SLA による復旧予定を通知できる場合は，それを通知するが，それ以外の場合は，通知は困難である。また，クラウドサービスが顧客向けサービスの唯一のインタフェースである場合は，通知自体も不可能になるため，クラウド利用者は代替策を講じるか，リスクを受容するか検討を要する。

ログ監視

サーバへのアクセスなどネットワークに関するログを取得することができないクラウドサービスでは，サーバのスキャニングなどが行われていることなど，自らの資産が危機にさらされているかもしれないという事実を知ることが難しく，事前に対策をすることができないという課題がある。そのため，クラウド利用者は，ログ監視と対応を行っているクラウドサービスを選ぶか，あらかじめスキャニングなどの認知は困難である，ということを認識してクラウドサービスを利用するリスクを受容するか検討を要する。

暗号化

クラウドサービスの多くは SSL/TLS を利用した暗号化通信を選択することができるが，対応していないサービスを提供している事業者や，クラウド事業者内の経路では暗号化通信を行っていない場合もある。そのような場合には，機密データや重要データのやり取りにおいて暗号化を規定しているにもかかわらず，クラウド事業者のネットワーク上でデータが暗号化されないという課題がある。クラウド利用者は，暗号化されないことのリスクを受容するか検討を要する。

仮想化対応

仮想化環境においては，CPU やメモリなどの利用が物理的に行われた場合とは異なる管理が行われることがある。また，ネットワークやストレージなども仮想化され単一機器と動作が異なる場合もあり，リスクを生む可能性がある。仮想化環境を前提としたアプリケーションの設計が行われていない場合，処理速度が低下するだけではなく，必要以上のコンピュータリソースを使用することで，クラウド本来のメリットであるコスト削減などに寄与しないという問題も考えられる。このような問題に対して，クラウド利用者は，リスク移転（利用料の減額など）が可能か，それともリスクを受容するか検討を要する。

携帯電話・スマートフォン

携帯電話やスマートフォンは，PC に比べてセキュリティ対策を行うためのオプションが少なく，本格的な運用実績も少ないため，クラウドサービスが携帯電話やスマートフォンから利用できる場合は，トラブルに関する情報や対策についての十分な情報が得られないという課題がある。そのため，クラウド利用者は，携帯電話やスマートフォンによる利用を制御できるクラウドサービスを選ぶか，あらかじめ利便性はあがるが管理は困難になる，ということを認識してリスクを受容するか検討を要する。

最大許容停止時間

システムの最大許容停止時間について明確な指針が必要になる。最大許容停止時間は，クラウド事業者が定めるものであり，クラウド利用者は，クラウド事業者の定めに応じて復旧を待たねばならない。サービスにおける稼働率は SLA などの契約で定められるが，クラウド利用者は，最大許容停止時間の実態を確認するためにも過去のトラブルの状況などを問い合せ，これまでにどの程度サービスが停止したことがあるか，クラウド事業者の改善策によってその問題が解決しているかなどの確認を要する。

残存データ

メモリ上，ハードディスク上にデータが残ってしまった場合の処理について仮想化された環境で十分にこれらを制御することができるかどうか，可視化できない問題がある。そのため，クラウド利用者としては，クラウドサービスにおけるこれらの残存データの処理方法についてクラウド事業者が講じている技術的な処理方法についての情報を得るか，残存メモリ・残存オブジェクトが発生するリスクを受容するか検討を要する。

実行環境の制限

クラウドサービスでは提供される実行環境に制限がある場合が多い。アプリケーションによっては必要なライブラリが使えないことによって，動作しないことも考えられる。PaaS ベンダーによっては独自の開発言語やビジュアルエディタのみによる開発環境の提供により，他社のサービスを利用できないという問題が発生する。そのため，クラウド利用者は，汎用性のある実行環境を提供するクラウドサービスを選択するか，あらかじめ実行環境に制限があるリスクを受容するか検討を要する。

従量課金を利用した攻撃

クラウドサービスの契約形態によっては，利用したリソースに応じた使用料が課金される。この特性を利用して，処理を必要以上に増加させる攻撃が外部から行われることがある。DoS 攻撃のようにサービスの利用を妨げるのではなく，経済的に事業継続を不可能にする攻撃である。このような経済的な攻撃を EDoS（Economic Denial of Sustainability）と呼ぶことがある。クラウド利用者は，EDoS 攻撃により発生した使用料に関してクラウド事業者とあらかじめ取決めを交わすか検討を要する。

接続性

クラウドサービスは国内だけではなく，海外でも展開され，国内からの利用も増えている。国内外を問わず，事業者は様々な場所にクラウドサービスを提供するためのデータセンターを展開しており，かつそれらが連携して運用されている。そのため，ネットワーク構成が複雑になり，接続の信頼性を把握することができないという課題がある。そのため，クラウド利用者は，接続性にかかわるリスクの移転（利用料の減額など）が可能か，それともリスクを受容するか検討を要する。

相互運用性

クラウドサービスに関連する様々な標準化（技術，データ形式，サービス形態など）が行われていない現状では，アプリケーションのデータや作成されたシステムのイメージデータなどが，他のサービスで利用できなかったり，システム同士の連携ができなかったりという問題が発生する可能性がある。そのため，クラウド利用者は，相互運用性の高いクラウドサービスを選択するか，あらかじめ相互運用性にかかわるリスクを受容するか検討を要する。

中間者攻撃

データセンターが様々な場所で展開され，かつ連携していることを前提とした場合，1 対 1 の接続の場合に比べて中間者攻撃を受けやすくなっている。また，マッシュアップなどによってサービスが構成されている場合などは更に攻撃の機会が増えると考えられる。このような中間者攻撃に起因する被害の発生について，クラウド利用者は，リスク移転（利用料の減額など）が可能か，それともリスクを受容するか検討を要する。

分散管理

クラウドサービスでは冗長性や拡張性がそのメリットとして挙げられているが，反面これらのメリットを実現するための分散管理などの管理手法が，対象としている情報及びシステムの構造を複雑にし，クラウド利用者からの可視化を妨げており，情報やシステムの一元管理を実施しにくくしている。そのため，クラウド利用者は，クラウド事業者が使用する技術によっては，データの所在を明確に把握できないことによるリスクを受容するか検討を要する。

附属書 B（参考）クラウドサービス利用におけるリスクアセスメントの実施例

JIS Q 27002（実践のための規範）の管理目的及び管理策は，リスクアセスメントによって特定した要求事項を満たす形で実施することを意図している（図 6 参照）。情報セキュリティマネジメントにおいて，リスクアセスメントは，管理策を実施するリスク対応に先行するプロセスとして位置づけられるが，クラウドサービス利用におけるリスクアセスメントを実施した具体例はあまり知られていない。そこで，以下にクラウドサービス利用におけるリスクアセスメントの実施例を示す。

以下は，情報セキュリティマネジメント及びクラウドサービスに活用されている技術などを対象に，リスクが存在すると思われる要素を洗い出し，リスクアセスメントを実施したものである。

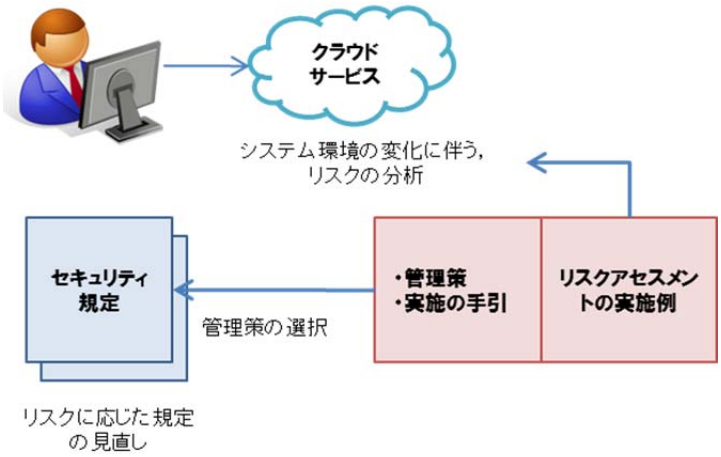

図 6　リスクアセスメントと管理策

クラウドコンピューティング環境とセキュリティリスク

クラウドコンピューティングでは，ネットワーク上に様々なリソースが配置されるとともに，管理主体がクラウド事業者にある。図 7 のようにクラウド環境の全体像を想定すると，管理対象を「クラウド利用者環境」，「クラウド事業者のシステム環境（仮想環境，データ環境）」，双方を接続する「ネットワーク」に分けることができる。また，運用環境においては「ID 管理」，「ログ管理」，「構成管理」，「物理的セキュリティ管理」に分類できる。

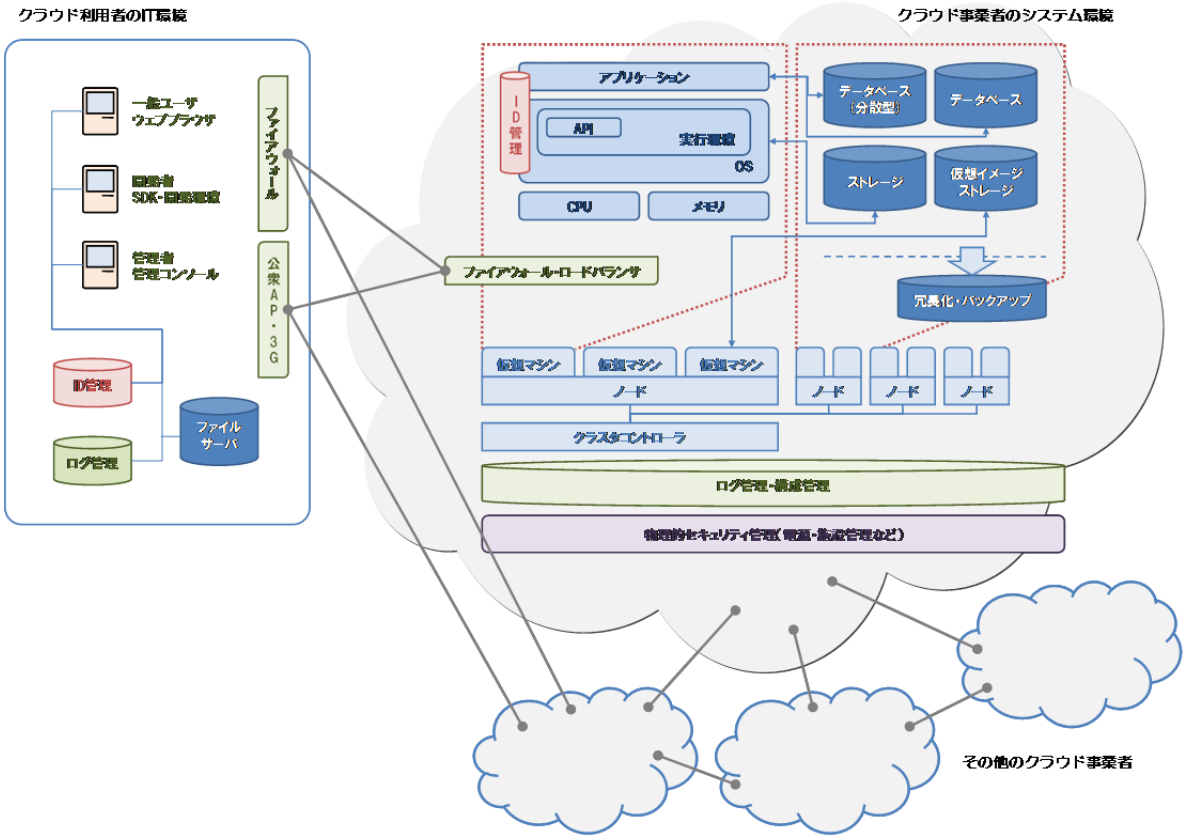

図 7　クラウド利用者からみたクラウドシステムの全体構成（例）

これらの分類を基に，クラウド利用者自らが管理したいにもかかわらず，自由に管理することができない管理対象，運用環境の部分は何かを精査することにより「プロセスに関するリスク」を洗い出すことができる。

組織内では，事故が発生した際に迅速に対応するために，情報セキュリティインシデントの検知機能や，インシデントを想定した回復策などを自ら用意することができた。しかしながら，クラウドコンピューティング環境においては，情報システムの停止の判断，侵入や不正アクセスの検知に関してクラウド事業者からの連絡を待つしかないこともある。

そのため，システムの停止にかかわるような事項については SLA などの契約によって対策を講じることができるが，日常的なシステム関連情報の収集は組織内ほど自由にはならない。

また，SLA の内容によっては短時間のサービス停止を対象としないなど，内容がクラウド事業者によって異なることがあり，個別に詳細を判断しなくてはいけない場合がある。組織内では自由に管理できたもので，ネットワーク上で自由に管理できないものにはデータが挙げられる。クラウドコンピューティング上で扱うデータを精査することにより「データに関するリスク」を洗い出すことができる。

クラウドコンピューティングによって取り扱われるデータの形態にはデータベース上のデータだけではなく，クラウドコンピューティング独自の分散技術を用いて管理されるもの，仮想化環境を構築するための仮想イメージデータ，それらのもととなる仮想イメージデータのテンプレートなどがある。

クラウドコンピューティング環境では, データが組織内のファイルサーバ上や個別の PC 上にあった場合のように機密レベルに応じて暗号化を行ったり，パスワードを付与したりという管理策を実施することができない場合もあり，データの管理方法について再度リスク分析を実施し，適切な管理策を選択する。
また，仮想化環境を構築する仮想イメージデータについてもクラウド利用者からは自由に扱うことが難しい。環境を構築する仮想イメージデータについての管理を適切に行うためにもクラウド事業者との連携を考慮する。

データ全般で考えれば，クラウド利用者は，バックアップの実施についても組織内のように管理することが難しい。バックアップのルールがクラウド事業者の定義による場合は，バックアップデータを，いつでも復旧できるような環境を構築することができない場合がある。その場合は，情報システムにおける事業継続管理において，データを自ら補完することを選択するか，サービス内容の検討を行うか，システム停止の受容レベルについて再度検討する。

クラウドコンピューティングではネットワーク経由でコンピュータリソースを利用するために，ネットワークの接続性と，十分な帯域が確保されていることが前提となる。組織が契約している外部ネットワークサービスに問題が発生した場合，コンピュータリソースの大半が利用できなくなるという問題もある。また, 組織のネットワークに問題がない場合でも, クラウド事業者のネットワークに問題が発生した場合, コンピュータリソースが利用できなくなる。

図 7 ではクラウド利用者とクラウド事業者，そしてクラウド事業者同士がネットワークを経由して接続されている様子を示している。サービスによってはクラウド事業者が連携して提供している場合もあれば, クラウド利用者が複数のクラウド事業者と契約して一つの業務システムを構築している場合もある。このような関係性を理解し，ネットワーク接続について精査することにより「ネットワークに関するリスク」を洗い出すことができる。

クラウド技術の一つである仮想化においては，それぞれの仮想環境を構築するために内部でネットワークが構築されている。それぞれの仮想環境を構成するハードウェア及びソフトウェアは暗号化通信又はネットワークの隔離を行うことにより経路上の安全を確保することができるが，クラウド利用者からは実施できない項目の一つとなっている。

管理的セキュリティの視点では，ID 管理，ログ管理，物理的セキュリティ管理などが，クラウド利用者にとって管理したくてもできない項目として挙げられることがある。

図 7 のように，クラウド上で提供されるアプリケーションやオペレーティングシステム，実行環境，API では, 単にシステム管理者への権限付与だけではなく, 利用者への ID が発行される場合がある。その際に, クラウド利用者が保有している ID 管理のシステムと整合性をとることができるか，またクラウド上の ID 管理がクラウド利用者の ID 管理のルールと適合するかどうかという問題がある。適切な情報セキュリティ管理を実施するために，クラウドサービスを利用するなら，クラウド事業者の ID 管理の方針を理解し，適合する。

同様の問題はログ管理においても考慮する。情報セキュリティインシデントに対する分析に際しては，ログを参照することが重要となるが，クラウド事業者が提供するログによっては，分析に足る情報が得られるとは限らない。

ID 管理やログ管理のようにクラウド利用者とクラウド事業者の双方が保有している場合は，整合をとる必要性について考慮する。

物理的セキュリティ管理はクラウド事業者の責任範囲であるが，データセンターによっては十分なサポートユーティリティが提供されないことがある。大規模なデータセンターの設営に対して，十分な電源が提供されない，災害によって十分なリソースが提供されないといった問題が考えられる。

データセンター内で業務を行う担当者の不正などについてはクラウドサービス以前と大きく変化はないが，データが集約されるクラウドサービスの環境では，影響の大きさを考慮しなければならない事項であり，クラウド事業者は人的な不正の発生を防ぐための物理的セキュリティを考慮する。

図 7 ではクラウドコンピューティング環境を簡単に示したが，実際には更に複雑な構造となっており，環境によっては新たな考慮事項が発生するかもしれない。しかしながら，基本的な形でのクラウドコンピューティング環境を把握しておくことにより，十分なリスクアセスメントを実施することができる。

リスクアセスメントの方法とマトリクスの活用例

本実施例では，提供されるリソースの変化，ユーザ環境，事業者におけるサービスにかかわるプレイヤーごとに，SaaS，PaaS，IaaS のそれぞれについて，管理情報及び取扱いデータにおける管理の可否について検討した。検討に当たっては，マトリクスを活用し，リスクを可視化する試みを行った。

なお，今回のリスクアセスメントにおいては，利用者組織を特定したわけではないため，情報資産の重要度や可用性，完全性，機密性が損なわれた場合の影響度については検討していない。

SaaS 利用時におけるリスク識別の実施例

以下のような組織を想定し，マトリクスを利用したリスクアセスメントを実行した。

利用者側には「一般ユーザ」及び一般ユーザを管理する「ユーザ管理者」の役割が存在する。一般ユーザは一般ユーザ権限の ID を所有し，SaaS で用意されている業務アプリケーションやオフィスアプリケーションを利用している。ユーザ管理者はそれら一般ユーザを管理するための ID を所有し，SaaS 事業者により用意されたユーザ管理インタフェースを利用できる権限をもつている。

クラウド事業者にはサービス提供中のシステムの「運用担当者」，サービスを開発している「開発技術者」が存在する。運用担当者は運用のための ID を所有し，サービス提供中のシステムの運用管理を行っている。システムの安定的な動作を維持するためのログ管理など，あらかじめ決められた定型のオペレーション業務以外は行わない。開発技術者は提供中のサービスの機能拡張や新サービスの開発，緊急トラブルへの対応などを行っており，特権 ID を使用可能であるが日常の運用管理は行っていない。責任者は提供中のサービスの動作やセキュリティに対しての責任を負っているがシステムを操作するための ID は所有していない。

この事例での SaaS 事業者はシステムのインフラも含めて自社で運用を行っており，他社の IaaS，PaaS といったサービスは利用していない。

表 1　SaaS におけるシステム管理面における管理の可否（例）

対象（クラウド上）		SaaS利用者		クラウド事業者	
		一般ユーザ	ユーザ管理者	運用担当者	開発技術者
ユーザアプリケーション	操作	●	−	−	−
	設定	●	−	−	−
	ログ閲覧	−	●	−	−
ID管理	操作	−	●	−	−
	設定	−	●	−	−
	ログ閲覧	−	●	−	−
API	操作	−	−	●	−
	設定	−	−	−	●
	ログ閲覧	−	−	●	●
実行環境	操作	−	−	●	−
	設定	−	−	−	●
	ログ閲覧	−	−	●	●
OS	操作	−	−	●	−
	設定	−	−	−	●
	ログ閲覧	−	−	●	●
ファイアウォール	操作	−	−	−	●
	設定	−	−	−	●
	ログ閲覧	−	−	●	●
仮想マシン	操作	−	−	−	●
	設定	−	−	−	●
	ログ閲覧	−	−	●	●
ホストマシン	操作	−	−	−	●
	設定	−	−	−	●
	ログ閲覧	−	−	●	●

システム管理の側面から，リスクアセスメントを実施した（表 1 参照）。

一般的な SaaS においては，利用者組織はアプリケーションの利用と ID 管理のみが実施できるようになっている。ID 管理においては組織内のワークフローに対応するような役職による設定を行うことができず，機能のオンオフしかできない場合もある。

表では「API」以下の項目について利用者は直接操作，設定，ログ閲覧などができず，運用状況の把握などもクラウド事業者の報告が必要となる。つまり，情報システムの状態を詳細に把握できないという問題が発生する。

表 2　SaaS におけるデータ管理面における管理の可否（例）

対象データ（クラウド上）		SaaS利用者		クラウド事業者	
		一般ユーザ	ユーザ管理者	運用担当者	開発技術者
ユーザアプリケーションデータ	閲覧	●	−	−	−
	変更	●	−	−	−
	削除	−	●	−	−
	暗号化	−	●	−	−
	分類	●	−	−	−
ストレージデータ	閲覧	−	−	●	●
	変更	−	−	−	●
	削除	−	−	−	●
	暗号化	−	−	−	●
	分類	−	−	−	●
仮想イメージデータ（運用中）	閲覧	−	−	●	●
	変更	−	−	−	●
	削除	−	−	−	●
	暗号化	−	−	−	●
	分類	−	−	−	●
仮想イメージデータ（テンプレート）	閲覧	−	−	●	●
	変更	−	−	−	●
	削除	−	−	−	●
	暗号化	−	−	−	●
	分類	−	−	−	●
バックアップ	作成	−	−	●	●
	削除	−	−	●	●

次にデータ管理の側面からリスクアセスメントを実施した（表 2 参照）。

ユーザが管理できるのは SaaS で提供されているアプリケーションのデータのみであり，完全な削除という点では管理者のみが実施できるように設定されていることがある。利用者はデータ全体のバックアップを実施したり，アプリケーションの設定状況などのバックアップを実施することができない場合がある。

SaaS で提供されるアプリケーションそのものが特別な場合もあるので，一概に判断することはできないが，データのバックアップや移行ができないという問題が発生する。

SaaS においては以下の問題をリスクとして識別することができた（一部抜粋）。

- システム管理において，システムの状態を把握することができない
- ID 管理においてアプリケーションが提供した粒度での管理のみ実施できる

- ID 管理におけるトレーサビリティの確保が難しい
- アプリケーションデータのバックアップができない
- アプリケーションデータの移行ができない
- アプリケーションデータの完全削除ができない
- アプリケーションデータの暗号化を一般的な暗号化ツールを利用して実施できない

このように，システム管理におけるリスクの識別，データ管理におけるリスクの識別に役立てることができる。ここで識別されたリスクと情報資産の重要性及び影響度を照らし合わせ，組織に見合った管理策及び実施の手引の選択を行う。

以下，PaaS，IaaS についても同様にマトリクスを利用してリスクの識別を行う。

PaaS 利用時におけるリスク識別の実施例

以下のような組織を想定し，マトリクスを利用したリスクアセスメントを実施した。

利用者側には「一般ユーザ」及び「アプリケーション開発者」，一般ユーザや開発者を管理する「ユーザ管理者」の役割が存在する。一般ユーザは一般ユーザ権限の ID を所有し，PaaS を利用して開発された業務ソフトウェアやオフィスソフトウェアを利用している。アプリケーション開発者は PaaS により提供されている API を利用して業務ソフトウェアやオフィスソフトウェアを開発している。ユーザ管理者は一般ユーザ及び開発者を管理するための ID を所有し，PaaS 事業者により用意されたユーザ管理インタフェースを利用できる権限をもつている。クラウド事業者にはサービス提供中のシステムの「運用担当者」，サービスを開発している「開発技術者」，サービスの「責任者」が存在する。運用担当者は運用のための ID を所有し，サービス提供中のシステムの運用管理を行っている。システムの安定的な動作を維持するためのログ管理など，あらかじめ決められた定型のオペレーション業務以外は行わない。開発技術者は提供中のサービスの機能拡張や新サービスの開発を行っており，特権 ID を使用可能であるが日常の運用管理は行っていない。

責任者は提供中のサービスの動作やセキュリティに対しての責任を負っているがシステムを操作するための ID は所有していない。

表 3　PaaS におけるシステム管理面における管理の可否（例）

対象（クラウド上）		PaaS利用者			クラウド事業者		
		一般ユーザ	アプリケーション開発者	ユーザ管理者	運用担当者	開発技術者	責任者
ユーザアプリケーション	操作	●	−	−	−	−	−
	設定	●	−	−	−	−	−
	ログ閲覧	−	−	●	−	−	−
ID管理	操作	−	−	●	−	−	−
	設定	−	−	●	−	−	−
	ログ閲覧	−	−	●	−	−	−
API	操作	−	●	−	−	−	−
	設定	−	●	−	−	−	−
	ログ閲覧	−	●	−	−	−	−
実行環境	操作	−	−	−	●	−	−
	設定	−	−	−	−	●	−
	ログ閲覧	−	−	−	●	●	−
OS	操作	−	−	−	●	−	−
	設定	−	−	−	−	●	−
	ログ閲覧	−	−	−	●	●	−
ファイアウォール	操作	−	−	−	−	●	−
	設定	−	−	−	−	●	−
	ログ閲覧	−	−	−	●	●	−
仮想マシン	操作	−	−	−	−	●	−
	設定	−	−	−	−	●	−
	ログ閲覧	−	−	−	●	●	−
ホストマシン	操作	−	−	−	−	●	−
	設定	−	−	−	−	●	−
	ログ閲覧	−	−	−	●	●	−

PaaS 環境はクラウドサービスごとにシステム環境が異なり，統一的なリスクアセスメントを実施することが難しい。ここでは，API が提供されて，ユーザがそれを利用して自らのアプリケーションやシステムを構築するタイプの PaaS を対象に，システム管理におけるリスクの洗い出しを実施した（表 3 参照）。

SaaS 同様にプラットフォームとなる環境についての情報を直接得ることはできず，環境に応じてプラットフォームの変更などを行うことも難しい。

自らが作成したアプリケーションに関してはログを取得して分析するなど，問題解決のための情報は一部入手することができる。しかし，問題がプラットフォームにあると判断できたとしても，それを自らが修正できるわけではないので，サービス管理のすべてを実施できるということにはならない。

表 4　PaaS におけるデータ管理面における管理の可否（例）

対象データ（クラウド上）		PaaS利用者			クラウド事業者		
		一般ユーザ	アプリケーション開発者	ユーザ管理者	運用担当者	開発技術者	責任者
ユーザアプリケーションデータ	閲覧	●	–	–	–	–	–
	変更	●	–	–	–	–	–
	削除	–	–	●	–	–	–
	暗号化	–	–	●	–	–	–
	分類	●	–	–	–	–	–
ストレージデータ	閲覧	–	●	●	–	–	–
	変更	–	●	●	–	–	–
	削除	–	●	●	–	–	–
	暗号化	–	●	●	–	–	–
	分類	–	●	●	–	–	–
仮想イメージデータ（運用中）	閲覧	–	–	–	●	●	–
	変更	–	–	–	–	●	–
	削除	–	–	–	–	●	–
	暗号化	–	–	–	–	●	–
	分類	–	–	–	–	●	–
仮想イメージデータ（テンプレート）	閲覧	–	–	–	●	●	–
	変更	–	–	–	–	●	–
	削除	–	–	–	–	●	–
	暗号化	–	–	–	–	●	–
	分類	–	–	–	–	●	–
バックアップ	作成	–	–	–	●	●	–
	削除	–	–	–	●	●	–

データ管理においてはストレージデータまでを利用できることを前提に，データ管理におけるリスクの洗い出しを実施した（表 4 参照）。

ストレージデータとは，アプリケーションから利用するデータ領域ではなく，プログラムを保管したり，ログを保管することのできる比較的自由度の高いストレージに保存されたデータを指している。

バックアップの柔軟さについては SaaS よりは自由度が高いといえる。自らがアプリケーションを作成していることから，関連するデータのバックアップなどを実施することは可能な場合が多い。

プログラムのデプロイに関しては，実行環境によって異なるために一概にリスクとして捉えることができないが，本番環境とテスト環境を明確に分けて実施することができないものもあるため，組織の方針に応じて運用によって対応をする。

IaaS 利用時におけるリスク識別の実施例

以下のような組織を想定し，マトリクスを利用したリスクアセスメントを実行した。

利用者側には「一般ユーザ」及び「アプリケーション開発者」，OS などのシステムインフラを管理する「システム管理者」の役割が存在する。一般ユーザは一般ユーザ権限の ID を所有し，IaaS を利用して自社開発された業務ソフトウェアやオフィスソフトウェアを利用している。アプリケーション開発者は IaaS で提供される OS 上で業務ソフトウェアやオフィスソフトウェアを開発している。システム管理者は OS を管理するための特権 ID を所有し，IaaS 事業者により用意されたシステム管理インタフェースを利用できる権限をもつている。さらに，アプリケーション開発者により開発されたサービスの運用を行っている。

クラウド事業者にはサービス提供中のシステムの「運用担当者」，サービスを開発している「開発技術者」，サービスの「責任者」が存在する。運用担当者は運用のための ID を所有し，サービス提供中のシステムの運用管理を行っている。システムの安定的な動作を維持するためのログ管理など，あらかじめ決められた定型のオペレーション業務以外は行わない。開発技術者は提供中のサービスの機能拡張や新サービスの開発を行っており，特権 ID を使用可能であるが日常の運用管理は行っていない。責任者は提供中のサービスの動作やセキュリティに対しての責任を負っているがシステムを操作するための ID は所有していない。

この事例では利用者は IaaS を利用してアプリケーションを自社開発し，自社のユーザ専用にサービス提供を行っている。

表 5　IaaS におけるシステム管理面における管理の可否（例）

対象（クラウド上）		IaaS利用者			クラウド事業者		
		一般ユーザ	アプリケーション開発者	システム管理者	運用担当者	開発技術者	責任者
ユーザアプリケーション	操作	●	–	–	–	–	–
	設定	●	–	–	–	–	–
	ログ閲覧	–	–	●	–	–	–
ID管理	操作	–	–	●	–	–	–
	設定	–	–	●	–	–	–
	ログ閲覧	–	–	●	–	–	–
API	操作	–	●	–	–	–	–
	設定	–	●	–	–	–	–
	ログ閲覧	–	●	–	–	–	–
実行環境	操作	–	–	●	–	–	–
	設定	–	–	●	–	–	–
	ログ閲覧	–	–	●	–	–	–
OS	操作	–	–	●	–	–	–
	設定	–	–	●	–	–	–
	ログ閲覧	–	–	●	–	–	–
ファイアウォール	操作	–	–	–	●	●	–
	設定	–	–	–	–	●	–
	ログ閲覧	–	–	–	●	●	–
仮想マシン	操作	–	–	–	●	●	–
	設定	–	–	–	–	●	–
	ログ閲覧	–	–	–	●	●	–
ホストマシン	操作	–	–	–	–	●	–
	設定	–	–	–	–	●	–
	ログ閲覧	–	–	–	●	●	–

IaaS においては一般的なハウジングサービスレベルでの管理を実施することができる（表 5 参照）。また，サービスに大きな差異が生じるわけではないので，リスクアセスメントについては他の組織が実施した結果が大いに参考になる。

しかし，仮想化におけるマルチテナントなどが実施されている場合には，プラットフォームでの状況について正しく把握することができないことがある。

問題発生時に実施できる対応は多く，適切な管理を実施することで事業継続における問題は少なくなると言える。しかしながら，プラットフォーム全体が攻撃されてしまった場合などは自らが対応することはできない。仮想環境やネットワーク以外のほとんどの管理を行うことができる。

表 6　IaaS におけるデータ管理面における管理の可否（例）

対象データ(クラウド上)		IaaS利用者			クラウド事業者		
		一般ユーザ	アプリケーション開発者	システム管理者	運用担当者	開発技術者	責任者
ユーザアプリケーションデータ	閲覧	●	–	–	–	–	–
	変更	●	–	–	–	–	–
	削除	–	–	●	–	–	–
	暗号化	–	–	●	–	–	–
	分類	●	–	–	–	–	–
ストレージデータ	閲覧	–	●	●	–	–	–
	変更	–	●	●	–	–	–
	削除	–	●	●	–	–	–
	暗号化	–	●	●	–	–	–
	分類	–	●	●	–	–	–
仮想イメージデータ（テンプレート）	閲覧	–	–	●	–	–	–
	変更	–	–	●	–	–	–
	削除	–	–	●	–	–	–
	暗号化	–	–	●	–	–	–
	分類	–	–	●	–	–	–
仮想イメージデータ（運用中）	閲覧	–	–	–	–	●	–
	変更	–	–	–	–	●	–
	削除	–	–	–	–	●	–
	暗号化	–	–	–	–	●	–
	分類	–	–	–	–	●	–
バックアップ	作成	–	–	●	●	●	–
	削除	–	–	●	●	●	–

データ管理においても OS をインストールしたハードディスクの管理レベルの内容は実施可能であると考えても良い（表 6 参照）。仮想環境で展開されたシステムがイメージデータとして保存されることで，環境のバックアップは実施しやすくなっている。しかし，バックアップ対象が展開されたシステム全体であること，個々のファイルによる差分ではなく，イメージ全体の差分となるために，バックアップは毎回完全バックアップを取得しなければならないという点，ネットワーク上でバックアップをダウンロードしなくてはならない点など，バックアップ容量の大きさが実施を困難とさせている。

技術的な面を差し引けば，IaaS では従来のハウジングサービスを参考に管理策及び実施の手引の選択ができるといえる。