クラウドサービス提供における

情報セキュリティ対策ガイドライン

～利用者との接点と事業者間連携における実務のポイント～

（案）

平成 26 年　月

総務省

目次

第 Ⅰ 部　序編 **1**

1．　目的 1
2．　ISO/IEC 27002:2013 及び他のガイドライン等との関係 2
3．　供給者関係のモデル 4
4．　クラウドサービス提供における利用者接点の実務の５つのポイント 5
5．　第Ⅱ部の構成とクラウド事業者への適用方法 9
6．　用語及び定義 11

第 Ⅱ 部　管理策の実装技術と利用者接点における実務 **14**

6．　情報セキュリティのための組織 14
6.1　内部組織 *14*
6.1.1　情報セキュリティの役割及び責任 *14*
6.1.2　職務の分離 *15*
6.2　モバイル機器及びテレワーキング *15*
6.2.1　モバイル機器の方針 *16*
6.3　クラウド利用者と供給者間における情報提供 *17*
6.3.1　クラウドサービスの情報セキュリティマネジメントに係る提供条件の明確化 *17*
6.3.2　利用者接点とサプライチェーンにおける情報提供・共有 *18*
8．　資産の管理 23
8.1　資産に対する責任 *23*
8.1.1　資産目録 *23*
8.1.2　資産の管理責任 *24*
8.1.5　クラウド利用者から預託された情報の返却 *24*
8.2　情報分類 *25*
8.2.1　情報の分類 *26*
8.2.3　資産の取扱い *26*
9．　アクセス制御 27
9.1　アクセス制御に対する業務上の要求事項 *27*
9.1.1　アクセス制御方針 *27*
9.1.2　ネットワーク及びネットワークサービスへのアクセス *28*
9.2　利用アクセスの管理 *30*
9.2.3　特権的アクセス権の管理 *30*
9.2.4　利用者の秘密認証情報の管理 *30*
9.4　システム及びアプリケーションのアクセス制御 *31*
9.4.1　情報へのアクセス制限 *32*
9.4.4　特権的なユーティリティプログラムの使用 *33*
9.5　仮想化されたクラウドサービスのアクセス制御 *35*
9.5.1　仮想化資源の分離の確実な実施 *35*
１０．暗号 36
１０.１　暗号による管理策 *36*
１０.１.１　暗号による管理策の利用方針 *36*

１０.１.２　鍵管理 37
１２．運用のセキュリティ 38
１２.１　運用の手順及び責任 38
１２.１.１　操作手順書 38
１２.１.２　変更管理 39
１２.１.３　容量・能力の管理 40
１２.２　マルウェアからの保護 41
１２.２.１　マルウェアに対する管理策 42
１２.３　バックアップ 43
１２.３.１　情報のバックアップ 43
１２.４　ログ取得及び監視 44
１２.４.１　イベントログ取得 44
１２.４.２　ログ情報の保護 45
１２.４.３　実務管理者及び運用担当者の作業ログ 46
１２.５　運用ソフトウェアの管理 47
１２.５.１　運用システムに関わるソフトウェアの導入 47
１２.６　技術的ぜい弱性管理 48
１２.６.１　技術的ぜい弱性の管理 48
１２.７　情報システムの監査に対する考慮事項 49
１２.７.１　情報システムの監査に対する管理策 49
１３．通信のセキュリティ 50
１３.１　ネットワークセキュリティ管理 50
１３.１.４　仮想ネットワークにおいて重視すべき脆弱性 51
１３.２　情報の転送 51
１３.２.２　情報転送に関する合意 52
１３.２.４　秘密保持契約又は守秘義務契約 53
１５．供給者関係 53
１５.１　供給者関係における情報セキュリティ 53
１５.１.１　供給者関係のための情報セキュリティの方針 54
１５.１.３　*ICT*サプライチェーン 55
１５.２　供給者のサービス提供の管理 56
１５.２.１　供給者のサービス提供の監視及びレビュー 56
１５.２.２　供給者のサービス提供の変更に対する管理 57
１６．情報セキュリティインシデント管理 58
１６.１　情報セキュリティインシデントの管理及びその改善 58
１６.１.２　情報セキュリティ事象の報告 59
１６.１.４　情報セキュリティ事象の評価及び決定 60
１６.１.７　証拠の収集 60
１７．事業継続マネジメントにおける情報セキュリティの側面 62
１７.２　冗長性 62
１７.２.１　情報処理施設の可用性 62
１８．順守 63
１８.１　法的及び契約上の要求事項の順守 63
１８.１.１　適用法令及び契約上の要求事項の特定 64

１８.１.２　知的財産権 64
１８.１.３　記録の保護 65
１８.１.４　プライバシー及び個人を特定できる情報（*PII*）の保護 66
１８.１.５　暗号化機能に対する規制 66
１８.２　情報セキュリティのレビュー 67
１８.２.１　情報セキュリティの独立したレビュー 67
１８.２.２　情報セキュリティのための方針群及び標準の順守 68
１８.２.３　技術的順守のレビュー 68

第 I 部　　序編

1.　目的

社会経済活動の ICT への依存が高まる中で、情報システムの構築の迅速化及び柔軟化並びに管理・運用費用の低廉化を実現する有効な手段として、クラウドサービスの利用が拡大している。近年では、行政、金融等の機微な情報を取り扱う分野においてもクラウドサービスの利用が進展しており、クラウドサービスは今日の社会経済活動を支える重要な ICT 基盤となっている。他方、クラウドサービスについては、情報漏えい等の情報セキュリティマネジメント上の課題及びデータの保管場所・処理方法が不明確であることの危険性が指摘されているところである。

クラウドサービスの導入が本格化するにつれて、クラウドサービスのサービスメニューもアプリケーション領域（ASP・SaaS）から実行環境・インフラ領域（PaaS、IaaS 等）に拡大し、クラウドサービスの提供形態も分業が進んできた。元々は単独のクラウド事業者がサービスを提供する形態が多かったが、現在はインフラや実行環境ごとサービス提供する基幹事業者（以後、「基幹事業者」という。）と、そのインフラを借り受けてアプリケーションサービスを中心にサービスを提供する事業者に分かれて協業が進んでいるほか、アプリケーションサービスを提供する事業者同士が連携してサービスを提供する事例も急増している。このように、ICT サプライチェーンを編成してクラウドサービスを提供する形態が現在の主流であると言える。このサービス提供形態の複雑化は、上述した情報セキュリティマネジメント上の課題やデータの保管場所・処理方法が不明確であることの危険性を、さらに増長させる恐れがあると言われている。

このようなクラウドサービスを取り巻く環境の変化に対応するためには、クラウドサービスを安全・安心に利用するための十全な情報セキュリティマネジメントが不可欠である。クラウドサービスであっても、ICT システムを用いてサービスを提供する以上、ICT システムに係る通常の情報セキュリティマネジメントを実施することは基本である。現在、ICT システムに基づく組織における情報セキュリティマネジメントの基盤を与えているのは ITU-T や ISO/IEC などの国際標準化機関が定める国際規格であり、ISO/IEC 27001（「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」）及び ISO/IEC 27002（「情報技術－セキュリティ技術－情報セキュリティ管理策の実践のための規範」）に基づいて情報セキュリティマネジメントを実施することが可能となっている。それらの規格上で、クラウドサービスの利用・提供及び監査に特化した情報セキュリティマネジメントに係るガイドライン等が、国内外の機関・団体によって策定・公表・検討が進められている。これらガイドライン等（例：ISO/IEC 27017）に従って対策することで、クラウドサービスの情報セキュリティマネジメントを構築することは可能であると言えよう。

一方で、クラウドサービスは、クラウド利用者とクラウド事業者が利用規約や SLA の合意に基づいて役割と責任を分担するという側面がある。ICT サプライチェーンを編成する場合は、さらに供給者であるクラウド事業者間でも役割と責任の分担が発生する。また、クラウド事業者が多数のクラウド利用者を同時に相手にすること（以後、「マスサービス提供」という。）により、クラウド事業者の利用者個別対応の限界も顕在化する。この役割と責任の分担やマスサービス提供に伴って発生する全体としての統制の欠如、コミュニケーション不足、コンプライアンスの欠如、テナント分離の失敗、及びその結果として生じる利害対立、債務不履行、認識の食い違い、信頼の損失等に焦点を当て、これを解消・緩和するための対策実務（以後、「利用者接点の実務」という。）に係る指針を示したガイドラインは未だ作成されておらず、上述したガイドラインにおいても本対策実務のレベルまでの言及はない。本ガイドラインは、この役割を果たす指針として新たに作成されたものである [1]。

---

[1] 本ガイドラインでは、利用者接点の実務の中でも、特にコミュニケーション不足を解消するためのクラウド利用者への情

本ガイドラインは、ISO/IEC 27002 に基づく情報セキュリティマネジメントを行うための知識を有しているクラウド事業者を読み手として想定している。そして、この読み手が、クラウド利用者及び ICT サプライチェーンを構成する他の供給者との間で十分な信頼と協力関係を築き上げ、安全・安心なクラウドサービスを提供することができるよう、実践するべき利用者接点の実務を理解するために読んでいただきたい。

本ガイドラインは、ICT サプライチェーンの供給者の中でも、特に、インフラを借り受けてアプリケーションサービスを中心にサービスを提供するクラウド事業者が読むのに適している。これらのクラウド事業者は、インフラや実行環境に求められる情報セキュリティ対策を基幹事業者に任せることができる。このため、クラウドサービスを提供するにあたっての主たる関心事である、利用者接点の実務に集中することができるからである。

一方で、基幹事業者においても、ICT サプライチェーンの供給者の一員として、利用者接点の実務を知ることは必要であり、本ガイドラインが役立つ。しかし、本ガイドラインからは、インフラに求められる情報セキュリティ対策技術の実装についての指針は得られないため、別途、特定非営利活動法人日本セキュリティ監査協会：クラウド情報セキュリティ管理基準等を参照していただきたい。

2． ISO/IEC 27002:2013 及び他のガイドライン等との関係

既に述べたように、本ガイドラインは、ISO/IEC 27002 に基づく情報セキュリティマネジメントを行うための知識を有しているクラウド事業者を読み手として想定している。これを前提として、読者の理解を助けるため、本ガイドラインの第Ⅱ部の指針は、目次構成を概ねISO/IEC 27002:2013に合わせてあり、他の文献等を参考として一部の項目のみを新たに追記している。また、管理のための目的と管理策の記述についても、新たに追記した部分を除けば、ISO/IEC 27002:2013 より引用している。これにより、読者はクラウドサービスを提供する ICT システムに対する通常の情報セキュリティマネジメントの実践のための規範と、利用者接点の実務の指針を簡単に対応づけて確認することができるため、理解しやすく、実践もしやすいものとなっている。

一方で、本ガイドラインは、クラウド事業者がクラウドサービスを提供する場合に特に重視すべき、クラウド利用者との接点において対応すべき実務を深掘りし、新規で記述している。このため、クラウドサービスの提供において特に重視すべき事項を含まない管理策は、一般的な情報セキュリティマネジメントで十分であるとして、本ガイドラインには含まれていない。この管理策の抜粋は、下記の 7 基準に基づいて実施している。

1) 国内外の関連団体が、それぞれの基準やガイドラインにおいて、クラウド利用者への情報提供等の、クラウドサービスを提供する際に特に重視すべき利用者接点の実務を記述している場合
2) 仮想化技術の適用と関連が深い管理策
3) 監査・認証の取得、証拠収集、捜査による媒体押収等に直面した場合に求められるテナント分離の実務との関連が深い管理策
4) モバイル端末を用いたクラウドサービスの利用に係る管理策
5) 運用管理におけるポイントに係る管理策（例：容量・能力の管理、バックアップ、ログ管理、暗号化等）

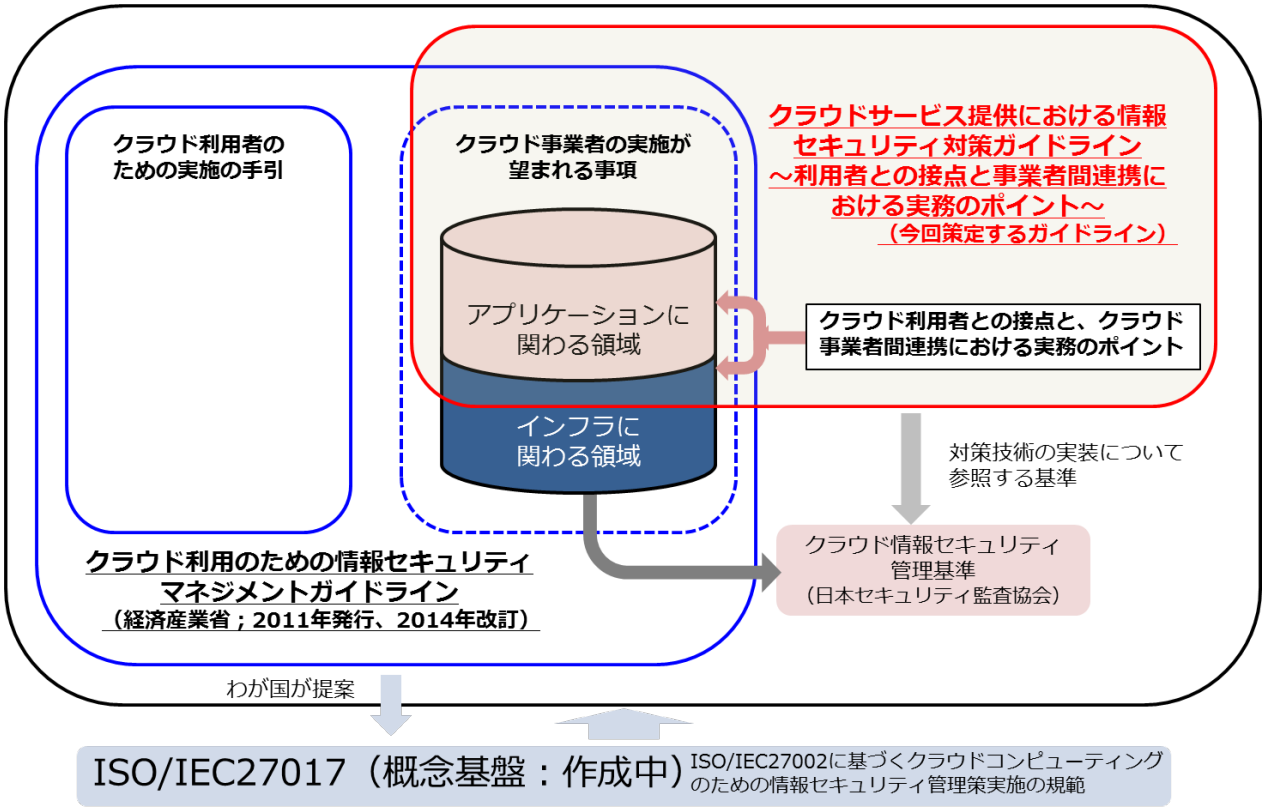
報公開・開示の実務について特に重点を置いて記述している。

6) ICT サプライチェーンと供給者関係に係る実務についての管理策

7) 複数国を跨いでクラウドサービスを提供するにあたり、コンプライアンス上課題となる管理策

現在、経済産業省において策定済みの「クラウド利用における情報セキュリティマネジメントガイドライン(2011 年)」に基づき、ISO/IEC JTC1 では、「ISO/IEC27002 に基づくクラウドコンピューティングサービスのための情報セキュリティ管理策の実践規範」を策定中であり、2015 年の完成に向けて国際標準化の検討を進めているところである。ISO/IEC JTC1 で策定中の上記実践規範は、クラウドサービスのためのハイレベルな管理策をガイドしているが、本書のガイドラインでは、利用者接点の実務に対象を絞り込んで詳しい記述を行っているため、ISO/IEC JTC1 における実践規範の内容と大きな重複はなく、基本的にはクラウド利用者と供給者間の接点において、その対策のための実務内容を詳述するものとなる。これらの実務内容については、クラウド事業者からクラウド利用者への情報提供に係る望ましい実践などとして抽出・整理することで、クラウド利用者から見ても、クラウド事業者を選択する上での具体的な判断材料にできるものと期待できる。上記のような既存/策定中のガイドラインと本書のガイドラインとの位置づけについては、図表 1 のような関係に整理される。

図表 1 クラウドセキュリティに関する既存/策定中のガイドラインと本書のガイドラインの位置づけ



３． 供給者関係のモデル

本ガイドラインでは、クラウド利用者とクラウド事業者の間の役割と責任の分担、及び ICT サプライチェーンの供給者間の役割と責任の分担に伴って発生する様々な問題に焦点を当てている。このため、本ガイドラインの内容を正しく理解するためには、クラウド利用者と ICT サプライチェーンの供給者がどのような関係にあるのかの類型（以後、「供給者関係のモデル」という。）を理解している必要がある。本ガイドラインでは、供給者関係のモデルを、エンドユーザ（組織）と複数のクラウド事業者がどのような契約形態を取るかによって、「垂直連携型」と「水平連携型」の 2 つのモデルに分類する。

「垂直連携型」とは、エンドユーザ（組織）にクラウドサービスを提供するクラウド事業者が、アグリゲーションサービス事業者である場合である。この場合、アグリゲーションサービス事業者が、ICT サプライチェーンの全ての供給者を代表してエンドユーザ（組織）と契約を締結し、ワンストップサービスを提供する。クラウド利用者は、ICT サプライチェーンの存在を気にかける必要はない。このため、クラウド利用者とクラウド事業者の接点における実務は単純になるが、ICT サプライチェーン間ではアグリゲーションサービス事業者が他の供給者全体を統制する必要が生じる。

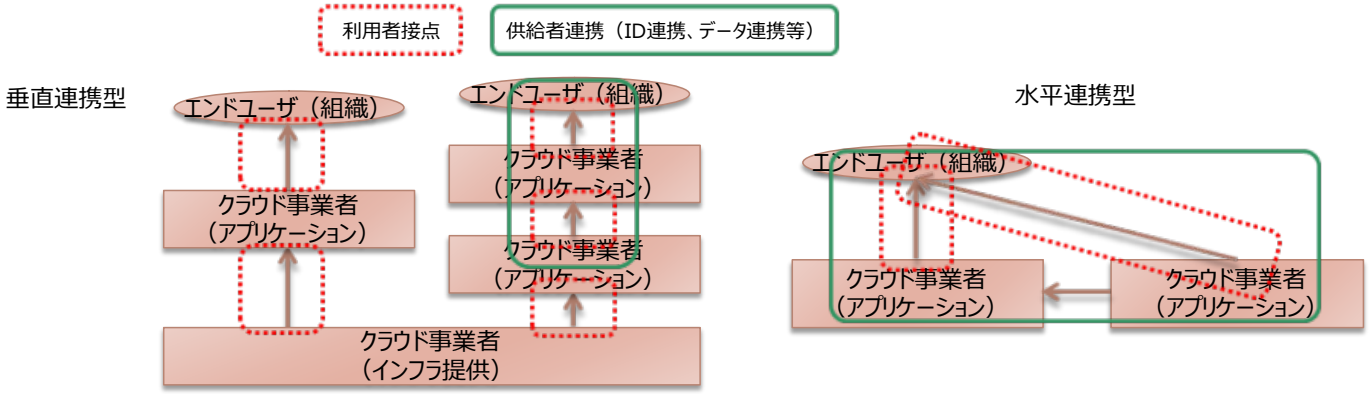
「水平連携型」とは、エンドユーザ（組織）が ICT サプライチェーンの供給者と個別に契約を結ぶ形態を取る場合である。クラウド利用者が複数の供給者と別々に契約を結ぶため、クラウド事業者間で実務対応に違いが出て供給者間での綿密な調整が必要になるなど、クラウド事業者とクラウド利用者の接点における実務対応は複雑になる。

クラウド事業者は、ICT サプライチェーンを構築し提供しているクラウドサービスが、垂直連携型なのか水平連携型なのかを良く理解した上で、各モデルの特徴に従って利用者接点の実務を実施することが求められる。垂直連携型では、アプリケーションサービス提供側がアグリゲーションサービス事業者となって、基幹事業者からインフラ又は実行環境を借り受ける。サービス品質の良いインフラを提供し続けるのは基幹事業者の役割であり、エンドユーザ（組織）との間の接点の実務を処理するのはアプリケーションサービス提供側の役割となる。水平連携型では、ICT サプライチェーンを構成する供給者は、エンドユーザ（組織）との契約関係においても、エンドユーザ（組織）との接点の実務を処理する責任についても対等である。一方、ICT サプライチェーン全体での統制を取る役割の供給者がいないことから、クラウドサービスの品質は最低のサービスレベルを提供する供給者によって決まってしまう。

ICT サプライチェーンにおいて、クラウド利用者と複数のクラウド事業者が連携して ID 連携、データ連携等を行う場合がある。この場合には、関係する全てのステークホルダー組織が構成する供給者連携に対して、クラウド情報セキュリティマネジメントの実務を行う必要がある。例えば、ID 連携やデータ連携における責任の切り分けと役割の分担の設定や技術面での協力関係の構築等は、全てのステークホルダー組織の間で定めていく必要がある。このように、クラウド利用者との接点における実務を実践するに当たり、ICT サプライチェーンにおける供給者連携についても考慮する必要がある。

供給者関係のモデルについて図表 2 に示す。

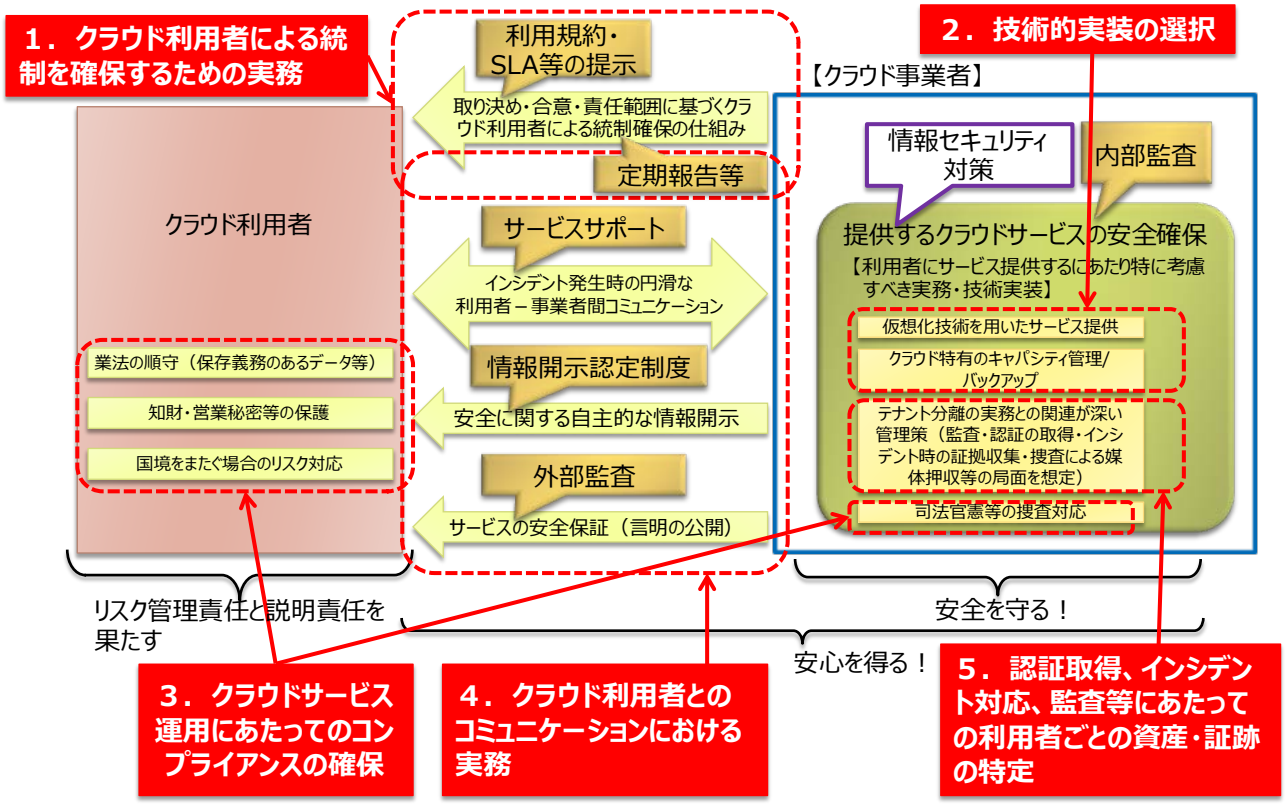
図表 2 供給者関係のモデル



4． クラウドサービス提供における利用者接点の実務の５つのポイント

クラウド事業者が、クラウド利用者との接点において対応すべき実務は、「クラウド利用者による統制を確保するための実務」「技術的実装の選択」「クラウドサービス運用にあたってのコンプライアンスの確保」「クラウド利用者とのコミュニケーションにおける実務」「認証取得、インシデント対応、監査等にあたっての利用者ごとの資産・証跡の特定」から構成される。その構造について、図表３に示す。本ガイドラインでは、特に「クラウド利用者とのコミュニケーションにおける実務」に重点を置いて実務の指針を作成している。

図表 3 クラウドサービス提供における利用者接点の実務の５つのポイント



(1) クラウド利用者による統制を確保するための実務

クラウド利用者による統制を確保するための実務とは、クラウド利用者がクラウド事業者を自らの方針に従って統制できるように、必要な取り決め・合意・責任の分担の設定等を行うことである。ICT サプライチェーンの供給者間においては、アグリゲーションサービス事業者が ICT サプライチェーン全体を統制する実務と、供給者間で責任と役割の分担を設定する実務がある。それぞれの実務についての本ガイドラインにおける記述の概要を図表 4 に示す。

図表 4 クラウド利用者による統制を確保するための実務の概要

分類	実務の概要
クラウド利用者 – クラウド事業者間の実務	・クラウド利用者とクラウド事業者の責任の分担の設定 ・クラウド利用者のポリシーに沿うクラウドサービス選択を促進するための支援 ・クラウド利用者の運用措置（監査、預託情報のバックアップ等）の支援と役割分担の明確化　等
アグリゲーションサービス事業者 – 他の供給者間の実務（垂直連携型の場合）	・ICT サプライチェーン全体としてのサービスレベル確保 ・ICT サプライチェーン全体としての管理要求の統制　等
供給者間の実務（水平連携型の場合）	・供給者間の責任と役割の分担の設定 ・他の供給者が提供するサービスに及ぼす影響や、他の供給者が提供するサービスから受ける影響を緩和するための措置　等

(2) 技術的実装の選択

技術的実装の選択とは、クラウドサービスの情報セキュリティマネジメントを実践するにあたり、技術の適切な実装方法を選択し、その選択によってクラウド利用者の運用管理の実務に変更の必要性が生じた場合は、必要な技術情報をクラウド利用者に提供することである。

(3) クラウドサービス運用にあたってのコンプライアンスの確保

クラウドサービス運用にあたってのコンプライアンスの確保とは、クラウドサービスを運用することによって生じうるクラウド利用者側及びクラウド事業者側のコンプライアンス違反の予防である。特に、クラウド利用者から預託されたデータを裁判管轄権を跨いで保存した場合のコンプライアンス確保への対処が重要になる。本ガイドラインでは、以下に列挙する実務について指針を示している。

- クラウド利用者が業法による要求事項等を確保できるようにするための支援（サービス機能の提供等）
- 国際的に展開されたクラウドサービスにおいて、海外における適用法の違いによってクラウド利用者及び預託された情報に生じるリスクを緩和するための、クラウド利用者側及びクラウド事業者側の措置に係る

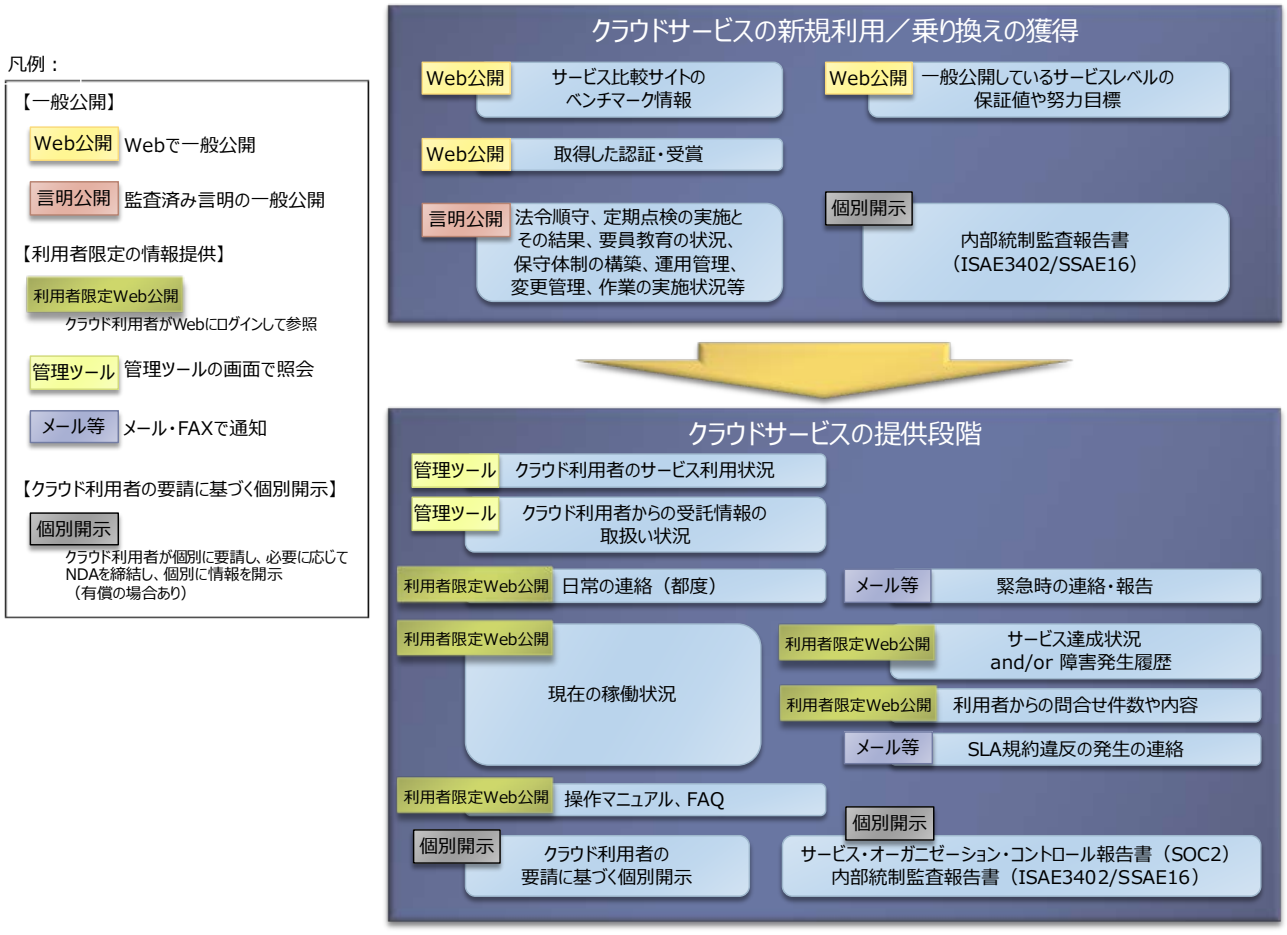
実務

- 司法官憲等の捜査等により、海外にある資産・サービスに起因するクラウドサービス全体の停止等を予防するための実務　等

(4) クラウド利用者とのコミュニケーションにおける実務

クラウド利用者とのコミュニケーションにおける実務とは、クラウドサービス提供の各段階において、クラウド事業者からクラウド利用者に対して行う情報の公開・開示である。具体的には、クラウドサービスの新規顧客/乗り換えを獲得する段階と、クラウドサービスを提供する段階で、クラウド利用者に対して提供する情報の内容や提供手段は異なる。図表 5 にその概要を示す。

図表 5 クラウドサービス提供の各段階と公開・開示する情報の関係



クラウドサービスの新規顧客/乗り換えを獲得する段階では、クラウドサービスが保証または努力目標とする

サービスレベルの公開、取得した認証・受賞の公開、実施している監査の言明の公開 [2]を行う。クラウドサービスが保証または努力目標とするサービスレベルの具体的な指標としては、例えば故障回復時刻、故障通知時刻、サービス提供時間、ヘルプデスク提供時間、サービス稼働率、平均応答時間、情報セキュリティ対策・設備の措置、ログ記録、サービス継続のための措置、バックアップ、暗号化に対応できるサービスの範囲などが設定される。また、SLA 文書の内容を公開している例も見られる。

クラウドサービスの提供段階では、クラウド利用者に対する情報提供を行う。提供する情報としては、クラウド利用者のサービス利用状況、クラウド利用者が預託された情報の取扱い状況、日常の連絡、緊急時の連絡・報告、現在の稼働状況、サービス達成状況（障害発生履歴の情報公開を含む）、クラウド利用者からの問合せ件数や内容、SLA 規約違反の発生の連絡、操作マニュアル・FAQ、サービス・オーガニゼーション・コントロール報告書（SOC2）、その他クラウド利用者個別に提供する詳しい情報がある。

クラウド利用者のサービス利用状況としては、利用者のログイン実績、利用時間、利用ログなどが情報開示されている。日常の連絡としては、計画的サービス停止/定期保守の案内、バージョンアップの案内、マニュアル類の最新版公開の案内、利用規約/SLA の改訂、技術的ぜい弱性情報・情報漏洩に繋がる脅威情報（フィッシング、マルウェア等）、サービス提供に係る関係国の適用法に関連したリスク情報等が提供されている。緊急時の連絡・報告としては、障害発生/復旧時刻の通知、障害経過の通知、障害内容・原因・対処・再発防止策等に係る事後報告等の情報が提供される。サービス達成状況については、稼働率、平均応答時間、サポートサービス応答率などの月次実績等を情報提供していることが多いが、これらの指標の値を提供する代わりに、障害発生履歴を詳しく提供しているクラウド事業者も多い。その他クラウド利用者個別に提供する詳しい情報としては、例えばクラウド利用者が希望する種別のインシデント情報（月次等で定期報告）、第三者機関による監査レポート・ぜい弱性検査レポート、クラウド事業者が行うバックアップの仕様（範囲・スケジュール、方法・データフォーマット、保存期間、バックアップデータの完全性確認やリストアの手順等）、イベントログ記録の仕様（ログ記録のタイプとタイプ別の保存期間、クラウド利用者がログを検査する権利と検査手順等）、ID 管理の権限設定の細かさ・ID 連携の有無、供給者関係の中で誰がどこでデータを保管し何を記録しているか、契約終了後の受託情報の抹消方法、SLA の内容等の情報提供が行われている。

なお、クラウド利用者個別の情報開示を行うにあたっては、以下の 5 点にも留意すべきである。

- クラウド事業者は、以下の２つのトレードオフを判断すべき。
  - クラウド利用者にとっての知るメリットと、同様の情報が他のクラウド利用者にも共有されることによるデメリットの間のトレードオフ
  - クラウド利用者にとっての知るメリットと、クラウド事業者にとっての情報開示するデメリットの間のトレードオフ
- クラウド利用者が細かい情報を要求し、自ら詳しく判断・管理しようとする場合は、クラウド利用者にオンプレミスを勧めるべき
- 有償の場合がある

[2] NDA を締結した上で監査報告書を個別開示する場合もある。

- 通常は NDA を締結の上で情報開示する
- 監査済みの言明公開により、対策の実施状況を、クラウド利用者に対し、保証することも検討すべき

一方、上述した情報をクラウド利用者に提供する手段としては、管理ツールによる情報照会機能の提供、利用者限定 Web 公開、メール等による通知、クラウド利用者の要請に基づく個別開示が行われている。提供する情報と用いる手段の関係については図表 5 を確認していただきたい。

(5) 認証取得、インシデント対応、監査等にあたっての利用者ごとの資産・証跡の特定

認証取得、インシデント対応、監査等にあたっての利用者ごとの資産・証跡の特定とは、クラウド利用者やクラウド事業者による認証取得・監査、並びにインシデント対応等にあたり、クラウド事業者が特に要求された場合に、クラウド利用者ごとの資産（預託された情報）・証跡を特定・分離することである。マルチテナントサービスを提供する場合のテナント分離の要求であると言える。

5． 第Ⅱ部の構成とクラウド事業者への適用方法

第Ⅱ部は、ISO/IEC 27002:2013の目次構成に基づき、情報セキュリティマネジメントに係る10領域25目的に重点化して、クラウドサービスとしての情報セキュリティマネジメントに係る利用者接点の実務の具体的な内容を記述している。第Ⅱ部の構成を図表 6 に示す。本ガイドラインを読むに当たり、その内容を理解するためには、ISO/IEC 27002 に基づく情報セキュリティマネジメントを行うための知識を有していることが望ましい。

図表 6 第Ⅱ部の構成

領域	目的
6. 情報セキュリティのための組織	6.1 内部組織
	6.2 モバイル機器及びテレワーキング
	6.3 クラウドサービスの利用者とクラウド事業者の関係
8. 資産の管理	8.1 資産に対する責任
	8.2 情報分類
9. アクセス制御	9.1 アクセス制御に対する業務上の要求事項
	9.2 利用アクセスの管理
	9.4 システム及びアプリケーションのアクセス制御
	9.5 共有された仮想化環境下での利用者データへのアクセス制御
10. 暗号	10.1 暗号による管理策
12. 運用のセキュリティ	12.1 運用の手順及び責任
	12.2 マルウェアからの保護
	12.3 バックアップ
	12.4 ログ取得及び監視
	12.5 運用ソフトウェアの管理
	12.6 技術的ぜい弱性管理

	12.7 情報システムの監査に対する考慮事項
13. 通信のセキュリティ	13.1 ネットワークセキュリティ管理
	13.2 情報の転送
15. 供給者関係	15.1 供給者関係における情報セキュリティ
	15.2 供給者のサービス提供の管理
16. 情報セキュリティインシデント管理	16.1 情報セキュリティインシデントの管理及びその改善
17. 事業継続マネジメントにおける情報セキュリティの側面	17.2 冗長性
18. 順守	18.1 法的及び契約上の要求事項の順守
	18.2 情報セキュリティのレビュー

クラウド事業者が情報セキュリティマネジメントを実践する際には、次の考え方で実施する（図表 7 参照）。

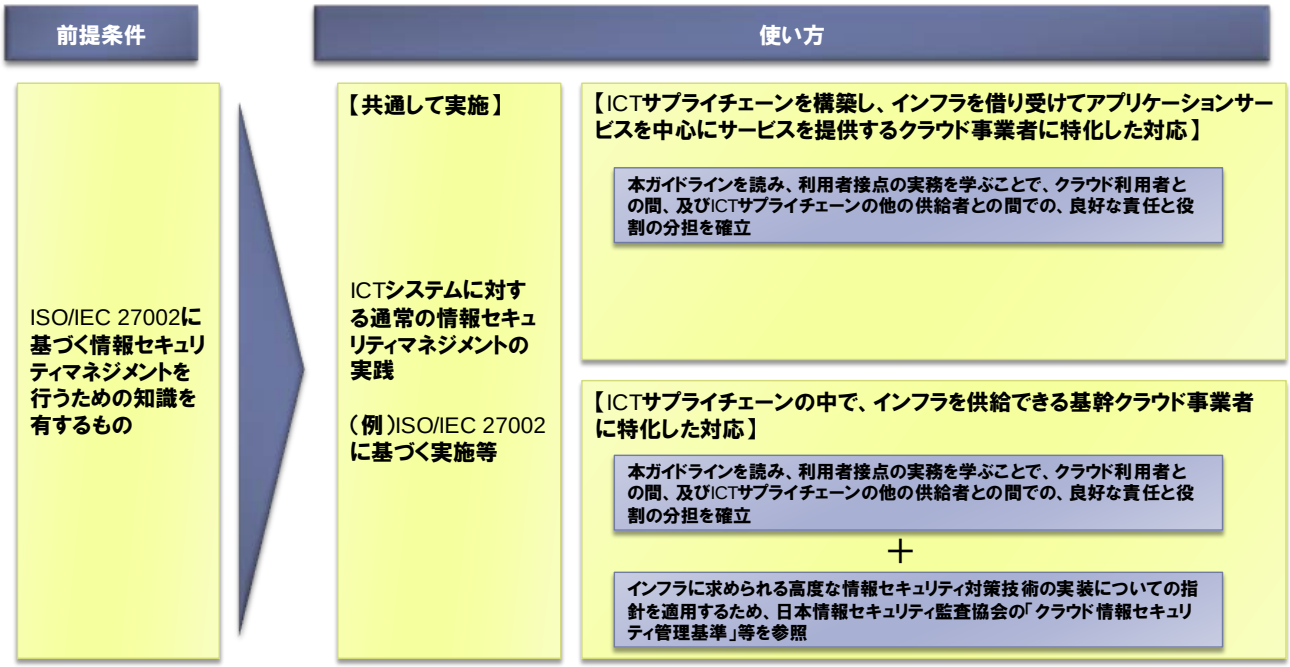
① 情報システムとしての情報セキュリティマネジメントの実践（例：ISO/IEC 27002 に基づく実施）

② クラウドサービスとしての情報セキュリティマネジメントに係る利用者接点の実務の実践（本ガイドラインによる）

③ クラウドサービスとしての情報セキュリティマネジメントの技術的実装並びに監査の実践（日本情報セキュリティ監査協会：クラウド情報セキュリティ管理基準等による）

ICT サプライチェーンを構築し、インフラを借り受けてアプリケーションサービスを中心に提供するクラウド事業者は①②を実施することが求められ、さらに③にある監査に取り組むことでサービスの信頼を高めることができる。一方、ICT サプライチェーンの中で、インフラを供給できる基幹クラウド事業者は、①②③の全てを実施することが望ましい。

図表 7 本ガイドラインの使い方



本ガイドラインを基に、クラウドサービスとしての情報セキュリティマネジメントに係る利用者接点の実務を実践する場合は、以下の手順に従って利用されたい。

① 第Ⅰ編を読み、本ガイドラインの背景にある概念（供給者のモデル、クラウドサービス提供における主要な課題、クラウドサービス提供における利用者接点の実務のポイント）と用語の定義を理解する

② 第Ⅰ編を読み、本ガイドラインの構成、他の標準・基準との関係、本ガイドラインの利用方法を確認する。

③ 第Ⅱ編を読み、管理策ごとに、クラウド利用者との接点における具体的実務の内容を確認し、実践する。

なお、本ガイドラインの第Ⅱ編において、大半の指針は主語がクラウド事業者になっている。このため、「クラウド事業者は」という主語を省略して表記している。読者は、文章に主語がない場合は、クラウド事業者が主語であるとして読んでいただきたい。

６． 用語及び定義

本ガイドラインで使用する用語の定義は、基本的に ISO/IEC 27000 に従う。本ガイドラインに特化して用いる用語または用語の定義について、以下に示す。

i. クラウドコンピューティング

利用者による共有が可能であり、利用者の要求に応じたセルフサービス提供と管理の機能を併せ持つ、拡張性と弾力性に富んだ物理又は仮想資源のプールに、ネットワークを通じてアクセスすることを可能にする情報処理形態

ii. クラウドサービス

クラウドコンピューティングを提供するサービス

iii. クラウド利用者

クラウドサービスを利用する組織。エンドユーザ（組織）と、クラウドサービスを提供するため別の組織が提供するクラウドサービスを利用する組織に分かれる。

iv. エンドユーザ

クラウドサービスの提供は行わず、クラウドサービスの利用のみを行う者。個人を示す場合は、エンドユーザ（個人）、組織を示す場合はエンドユーザ（組織）と表記することがある。本ガイドラインでは、エンドユーザ（組織）の中に個人事業主を含めている。

v. 特権ユーザ

特権的な管理ツールの使用を許可された個人。クラウド事業者とクラウド利用者のどちらに所属するかは問わない。

vi. クラウド事業者

クラウドサービスを提供する組織。クラウドサービスを提供するため別の組織が提供するクラウドサービスを利用するこ

ともありうる。

vii. アグリゲーションサービス

複数のクラウド事業者が提供するクラウドサービスを集積し、1 つのクラウドサービスとして利用できるようにしたサービス形態

viii. アグリゲーションサービス事業者

アグリゲーションサービスを提供するクラウド事業者。クラウド利用者との契約は、アグリゲーションサービス事業者が行う。

ix. ICT サプライチェーン

複数のクラウド事業者が連携してクラウドサービスを提供する際に構築される、各事業者の情報処理施設がネットワークで連結された形態

x. 供給者

ICT サプライチェーンの一部を構成するクラウド事業者

xi. 利用者接点

クラウド利用者とクラウド事業者の間に存在する、資産・サービス等に係る責任・役割等の分担の境界、情報提供のインターフェイス等

xii. 供給者連携

ICT サプライチェーンを構成する全ての、又は 3 者以上の供給者によるデータ、サービス等の連携

xiii. 個別契約連携クラウドサービス

ICT サプライチェーンでクラウドサービスを提供する際に、アグリゲーションサービスを編成せず、各供給者が個別にクラウド利用者と契約を締結するサービス形態

xiv. 個別契約連携クラウド事業者

個別契約連携クラウドサービスを提供する供給者

xv. ASP・SaaS（Software as a Service）

アプリケーションをサービスとして提供するクラウドサービス

xvi. 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

xvii. 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

xviii. 脅威

組織に損害や影響を与えるリスクを引き起こす要因

xix. ぜい弱性

脅威によって悪用される可能性がある欠陥や仕様上の問題

xx. リスク

目的に対して不確かさが与える影響

xxi. 管理策

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）

xxii. 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）

xxiii. 情報公開

一般に向けた、又は範囲を限定した、情報の公表・周知

xxiv. 情報開示

電子メール、電子ファイル、FAX、紙文書等の手段による、受領者に対する情報の引き渡し

xxv. 情報提供

情報公開、又は情報開示の実施

第 II 部　　管理策の実装技術と利用者接点における実務

６．　情報セキュリティのための組織

６.１ 内部組織

【目的】

組織内で情報セキュリティの実施及び運用に着手し、これを統制するための管理上の枠組みを確立するため。

【クラウドサービスの提供において特に留意すべき課題との関係】

クラウド利用者とクラウド事業者の間、並びに供給者間において、ガバナンスの実態が異なる組織が利用者接点を形成することから、その両側の組織の間で情報セキュリティマネジメントの統制が不十分になりやすく、これに対する管理策が必要である。

６.１.１　　情報セキュリティの役割及び責任

【管理策】

全ての情報セキュリティの責任を定め、割当ることが望ましい。

【クラウドサービスの提供において特に留意すべき課題との関係】

クラウド利用者とクラウド事業者の間、並びに供給者間において、ガバナンスの実態が異なる組織間で管理責任等の範囲を設定することから、その範囲の設定に当たっての合意内容やその内容に関する解釈が不明確になりやすいため、資産と情報セキュリティプロセスの識別を慎重に行い、明確な責任の範囲の割当を行うことが求められる。

【利用者接点とサプライチェーンにおける実務のポイント】

個々の情報資産の保護と特定の情報セキュリティプロセスの実施に対する責任を明確に規定し、その責任を個人に割当、責任の規定と割当について定めたことを文書化することが求められる（ISO/IEC27002:2013 6.1.1 実施の手引 a）b)c)参照）。さらに、クラウドサービスの提供にあたっては、実務上以下を実施することが望ましい。

(a) クラウド利用者とクラウド事業者の間で、それぞれの管理責任の範囲に関わる点に特に注意を払い、個々の情報資産の保護と特定の情報セキュリティプロセスの実施に対する責任を分担し、文書化すること。PaaS の場合、提供されるサービスによって、クラウド利用者が自ら管理できる情報資産や情報セキュリティプロセスの範囲にかなり幅があるため、クラウド利用者との管理責任の分担や免責の範囲が不明確になりやすく、特に慎重に責任の範囲を定めること。

(b) クラウドサービスの提供に係る供給者間の委託先管理の責任を明確に規定し、従業員に割当、文書化すること。

(c) (a)(b)の実施にあたり必要となるクラウド利用者とクラウド事業者の間、並びに供給者間における情報セキュリティマネジメントの側面の調整及び管理に関する事項を、エンドユーザ（組織）との契約形態、統制、順守、

情報提供の範囲、技術協力の範囲、緊急時対応の役割分担等に係る要求の観点から特定し、文書化すること。

(d) クラウド利用者と締結する SLA を保証するため、ICT サプライチェーン全体で分担する責任についての調整及び管理に関する事項について定め、文書化すること。

(e) クラウド利用者に対する説明責任の主体と詳細を明確に定めること。説明責任の遂行にあたっては、Web 等を用いた情報公開によるクラウド利用者への周知とクラウド利用者個別の情報開示の範囲を明確にし、クラウド事業者として個別対応が可能な範囲について、統制の観点からクラウド利用者に通知すること。

6.1.2 職務の分離

【管理策】

相反する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、分離することが望ましい。

【クラウドサービスの提供において特に留意すべき課題との関係】

システム設計・構築やサービス運用・設定における人為的ミスが、多数のクラウド利用者に影響を及ぼし、クラウド事業者の信用低下に繋がる恐れがあることから、人為的ミスを発見して取り除くための確認を徹底することが求められる。

【利用者接点とサプライチェーンにおける実務のポイント】

多数のクラウド利用者に影響を及ぼす事象（クラウド事業者での内部不正、システム誤動作・誤運用、管理用インターフェイスの悪用、DDoS/DoS 攻撃等）の発生に繋がるぜい弱性として、システム設計・構築やサービス運用・設定における人為的ミスを排除するため、クラウドサービスの提供にあたっては、実務上以下に特に注意を払うことが望ましい。

(a) サービス運用・設定の実務を行う者と認可を行う者の役割と責任を明確に分離すること。

(b) システム設計・構築を行う者と認可を行う者の役割と責任を明確に分離すること。

(c) ASP・SaaS の場合は、開発・保守の実務を行う者と運用を行う者の役割と責任を明確に分離すること。

6.2 モバイル機器及びテレワーキング

【目的】

モバイル機器の利用及びテレワーキングに関するセキュリティを確実にするため。

【クラウドサービスの提供において特に留意すべき課題との関係】

モバイル機器から業務用クラウドサービスを利用する際の課題は、モバイル機器からの情報漏洩、クラウド事業者によるモバイル機器から取得されたビジネス価値の高い情報の不正利用等である。これらに対する管理策が求められている。

6.2.1 モバイル機器の方針

【管理策】

モバイル機器を用いることによって生じるリスクを管理するために、方針及びその方針を支援するセキュリティ対策を採用することが望ましい。

クラウドサービスを利用するエンドユーザ（組織）の従業員等がモバイル機器を業務で利用する際には、モバイル機器にキャッシュされる秘密認証情報や業務データが漏洩するリスクが高く、これを防止する対策が求められる。特に BYOD などにより、対応が不十分なモバイル機器が利用されることで、エンドユーザ（組織）における情報セキュリティマネジメントに関する統制が取れず、その結果、エンドユーザ（組織）で講じている管理策の全てが徹底されず、不正プログラムが入ったり情報が漏えいする恐れがあるため、十分な対策が求められる。

モバイル機器には、スマートフォン/タブレット、携帯電話、ノートPC等のデバイスがある。これらのデバイスごとに、取るべき対策の内容や、対策の取りやすさも異なっている。しかし、共通しているのは、クラウドサービスが、それぞれのデバイスに適合した認証方法を提供することにより、アクセス制御を確実にすることが求められるということである。

他方、モバイル機器からの業務用 ASP・SaaS 利用においては、今後、クライアントアプリケーションを開発してクラウド利用者に配布し、モバイル機器にインストールして利用する形態が増えていく。このクライアントアプリケーションの不具合により、モバイル機器から個人情報や業務データが意図せず漏洩する事象が発生しうることから、クライアントアプリケーションの試験には特に注意が必要となる。モバイル機器の位置情報のように、ビジネス等で価値の高い情報を、クライアントアプリケーションを用いて収集することも可能になるため、クラウド利用者から収集する情報の内容や利用方法を、アプリケーション設計時から明確にしておくことが求められる。

また、モバイル機器からの業務用 ASP・SaaS 利用において、モバイル機器のブラウザ等を用いてクラウドサービスを利用する場合、HTML5 等の先進的な Web 技術を用いるケースが増えており、これらに特有の脆弱性を持ち込む可能性が高まるため、Web サービスの開発段階から留意する必要がある。

【利用者接点とサプライチェーンにおける実務のポイント】

モバイル機器を業務用 ASP・SaaS で用いる場合、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、物理的な保護、ソフトウェアのインストール制限、OS 等のセキュリティホールへの対応、情報サービスへの接続制限、モバイル機器の事前登録、アクセス制御、暗号化、モバイル機器上のデータのバックアップ、マルウェアからの保護、遠隔操作による機器の無効化・データの消去又はロック等の情報セキュリティ対策を実施することが求められる（ISO/IEC27002:2013 6.2.1 実施の手引参照）。特に、業務用ASP・SaaSがモバイル機器に適合した認証方法を用いたアクセス制御を確実にすることが重要である。

モバイル機器の中では、特に、近年急速に普及しているスマートフォン/タブレットに対する対策が難しくなっている。そこで以下では、業務用 ASP・SaaS においてスマートフォン/タブレットの利用が可能なサービスを提供することに焦点を絞り、実務上実施することが望ましい事項について示す。詳しくは、一般社団法人日本スマートフォンセキュリティ協会の「スマートフォンの業務クラウド利用における、端末からの業務データの情報漏洩を防ぐことを目的とした、企業のシス

テム管理者のための開発・運用管理ガイド　スマートフォンの情報漏洩を考える」を参照されたい。

(a) クラウド利用者に対し、不正改造されたり、マルウェアに感染したモバイル機器をクラウドサービスに接続させないように要求すること。
(b) クラウド利用者への運用上の要求事項も含めて、モバイル機器上で、スクリーンショット・スクリーンキャスト録画・クリップボード履歴保存・キーロガー等を実行させないための対策を講じること。
(c) クラウド利用者に配布する、モバイル機器用のクライアントアプリケーションには、キャッシュ保存機能を持たせないか、又は十分な強度の鍵長とロジックでキャッシュデータを暗号化する機能を持たせること。
(d) モバイル機器において、クラウド利用者に、一定強度以上のパスワード設定を義務付けること。また、業務用クラウドサービスへの接続時に一定強度以上のパスワードが設定されているかの有無をチェックすること。
(e) モバイル機器と業務用クラウドサービスの間の通信は十分な強度の暗号を用いて暗号化すること。
(f) クラウド利用者への運用上の要求事項も含めて、モバイル機器の業務データを他のシステムと同期させないための対策を講じること。

一方、モバイル機器からの業務用 ASP・SaaS 利用において、HTML5 等の先進的な Web 技術を用いる場合には、これらに特有の脆弱性を持ち込まないための管理策を、Web サービスの開発段階から実施することが望ましい。具体的な管理策については、JPCERT/CC「HTML5 を利用した Web アプリケーションのセキュリティ問題に関する調査報告書」を参照されたい。

6.3 クラウド利用者と供給者間における情報提供

【目的】

クラウド利用者の情報セキュリティマネジメント方針に適合したクラウドサービスの選択を確実にするため。

【クラウドサービスの提供において特に留意すべき課題との関係】

クラウドサービスは、その特性から、クラウド利用者による個別の情報セキュリティ要求に応えられる範囲が限定される。このため、クラウドサービス提供にあたり、どこまでがクラウド利用者の責任範囲であり、クラウド利用者がクラウドサービスの情報セキュリティマネジメントをどこまで統制することができ、どこまでのサービスレベルが得られ、どこまでの範囲で個別対応が可能かについて、クラウド利用者の理解を深めることにより、クラウド利用者のニーズに適合したクラウドサービスを選択できる環境を構築していくことが求められる。

6.3.1 クラウドサービスの情報セキュリティマネジメントに係る提供条件の明確化

【管理策】

クラウドサービスの情報セキュリティマネジメントに係る責任範囲、サービスレベル、クラウド利用者個別に対応可能な範囲等の提供条件を明確に定め、文書化することが望ましい。

【クラウドサービスの提供において特に留意すべき課題との関係】

クラウド利用者に、クラウドサービスの情報セキュリティマネジメントに係るクラウド利用者とクラウド事業者の責任範囲、サービスレベル、クラウド利用者個別に対応可能な範囲等の提供条件を正しく理解していただくために、予め文書化しておくことが求められる。さらに、この文書に係る情報提供により、提供条件を理解しているクラウド利用者の範囲を広げることで、自らのニーズに適合するクラウドサービスを選択するクラウド利用者を増やしていくことが望ましい。この文書化や情報提供に係る要求等は、エンドユーザ（組織）と供給者の間のみならず、アグリゲーションサービス事業者が他の供給者のクラウドサービスを選択する場合にも適用される。

【利用者接点とサプライチェーンにおける実務のポイント】

6.1.1【利用者接点とサプライチェーンにおける実務のポイント】(a)(b)(c)(d)(e)参照。さらに、クラウドサービスの提供にあたっては、実務上以下を実施することが望ましい。なお、以下の実務ポイントは、エンドユーザ（組織）と供給者の間のみならず、アグリゲーションサービス事業者が他の供給者のクラウドサービスを選択する場合にも適用される。

(a) 文書化されたクラウド事業者自身の責任範囲を、6.3.2【利用者接点とサプライチェーンにおける実務のポイント】(b)(f)(i)から手法を選択して、SLA 等によりクラウド利用者に明確に示すこと。
(b) クラウド利用者が自組織が求める統制を満たすにあたり、クラウド事業者が提供できる機能・サービスを、6.3.2【利用者接点とサプライチェーンにおける実務のポイント】(b)(f)(i)から手法を選択して、SLA 等によりクラウド利用者に明確に示すこと。
(c) (b)を実施するにあたり、クラウド利用者個別に対応可能な範囲を予め明文化しておき、この文書に基づいて、クラウド利用者に個別対応範囲がかなり限定されることを理解していただくための措置を講じること。

クラウドサービスの提供にあたり、複数の供給者によって提供サービス間に依存関係がある ICT サプライチェーンが構築されている場合がある。この場合、クラウド利用者から見た契約形態は 2 種類存在している。1 つはクラウド利用者が複数の供給者と個別に利用契約を締結する形態であり、もう 1 つはアグリゲーションサービス事業者がクラウド利用者との利用契約を一本化する形態である。クラウド利用者が複数の供給者と個別に利用契約を締結しなければならない場合は、クラウド利用者がそれぞれの供給者と情報セキュリティマネジメントに係るサービス提供条件を個別に合意する必要がある。このため、情報セキュリティマネジメントに係る責任範囲の構造が複雑化し、その分担が不明確になりやすいため、供給者としても特別な注意を払う必要がある。

6.3.2 利用者接点とサプライチェーンにおける情報提供・共有

【管理策】

目的や場面に応じて、クラウド利用者が必要とする情報を提供できる仕組みを構築することが望ましい。インシデント発生時には、ICT サプライチェーンで情報を共有し、クラウド利用者が必要とする情報を早く提供することが望ましい。

【クラウドサービスの提供において特に留意すべき課題との関係】

クラウド事業者からクラウド利用者への情報提供の目的は、クラウドサービス提供の段階によって異なる。ここで、情報とは「情報セキュリティマネジメントに影響を及ぼす情報」のことを指す。1 つめの目的はクラウドサービスの新規利用/乗り換え利用を目論むクラウド利用者への情報提供であり、もう 1 つの目的はクラウドサービスを提供している段階でのクラウド利用者への情報提供である。

新規利用者への情報提供においては、クラウド利用者が自組織の統制要求を満たすことができないクラウドサービスを選択してしまうと、係争の原因となるばかりでなく、利用者個別の要求を増加させる要因にもなる。このため、クラウド利用者の選択に必要な情報を提供し、自組織の統制を満たすことができるクラウドサービスを選択することを促すことが求められる。

一方、クラウドサービス提供段階では、ガバナンスの実態が異なる組織であるクラウド利用者とクラウド事業者の信頼関係を損なわないように、情報セキュリティマネジメントの統制に係る協力的な情報提供を確立することが求められる。情報セキュリティインシデント発生時には、長時間サービスが停止したり、クラウド利用者が納得する状況報告が適時にできないことにより、クラウド利用者からの信用を失ってしまう恐れがある。このため、ICT サプライチェーン全体でクラウド利用者に提供する情報を共有し、クラウド利用者に早く正確な情報を提供することが求められる。

【利用者接点とサプライチェーンにおける実務のポイント】

クラウドサービスの新規利用/乗り換え利用を目論むクラウド利用者への情報提供にあたっては、自組織のガバナンス規定を順守するために、クラウド利用者が、必要な統制機能及び能力を有しているクラウドサービス及びこれを提供するクラウド事業者を選定できることが求められる。この目的で提供される情報を以下に例示する。

- クラウドサービスが保証または努力目標とするサービスレベル
- 取得した認証・受賞
- 実施している監査の言明または監査報告書

また、これらの情報をクラウド利用者に提供する手段を以下に例示する。

- Web による一般公開
- 利用者個別の要請に基づく情報開示

上述した提供手段によりクラウド利用者に情報提供を行うにあたっては、実務上以下を実施することが望ましい。

(a) クラウドサービスの比較 Web サイト（例：クラウドサービス情報開示認定サイト https://www.fmmc.or.jp/cloud-nintei/）を活用し、そのベンチマーク指標に基づいて、クラウドサービスに係る情報を一般公開することを検討すること。

(b) Web 等による一般向けの情報公開システムを構築し、提供しているクラウドサービスのサービスレベルの保証値又は努力目標を情報公開すること。また、取得した認証（情報セキュリティ対策実施に関するもの、内部統制監査に関するもの等）や受賞を、一覧できる形式で情報公開すること。

(c) 監査済みの「情報セキュリティ対策の設計・実装・運用に係る言明」がある場合は、(b)の一般向け情報公開システムを用いて情報公開すること[3] [4]。

クラウドサービス提供段階では、クラウド利用者に限定し、必要とする情報を提供する。この目的で提供される情報を以下に例示する。

- クラウド利用者のサービス利用状況
- クラウド利用者が預託された情報の取扱い状況
- 日常の連絡
- 緊急時の連絡・報告
- 現在の稼働状況
- サービス達成状況（障害発生履歴の情報公開を含む）
- クラウド利用者からの問合せ件数や内容
- SLA 規約違反の発生の連絡
- 操作マニュアル・FAQ
- サービス・オーガニゼーション・コントロール報告書（SOC2）
- クラウド利用者の要請に基づく個別開示情報

また、これらの情報をクラウド利用者に提供するための、クラウド利用者に限定した手段を以下に例示する。

- 管理ツールを利用した情報照会機能
- 利用者限定 Web による情報公開（ログイン認証付きの Web サイト）
- 電子メール・FAX
- 利用者個別の要請に基づく情報開示

上述した提供手段によりクラウド利用者に情報提供を行うにあたっては、実務上以下を実施することが望ましい。

---

[3] 特定非営利活動法人日本セキュリティ監査協会（JASA）では、クラウドセキュリティ推進協議会（JCISPA）において、クラウド情報セキュリティ監査制度の検討を進めており、その中で言明要件の検討も実施しているので、参考にされたい。

[4] クラウド利用者の内部統制確保を保証するため、内部統制監査報告書の情報開示を求められることも多い。この場合は NDA を締結した上で情報開示することも選択肢となる。但し、内部統制監査報告書は情報セキュリティマネジメントの全般をカバーするものではないことを、クラウド利用者にも理解していただくことが望ましい。

(d) クラウドサービスの情報セキュリティに関する窓口（ヘルプデスク等）を分かりやすく公開すること。

(e) クラウド利用者からの個別要求に基づき、NDA を締結して、個別の情報開示を行うにあたり、その窓口をできる限りワンストップ化すること。また、個別の情報開示におけるクラウド利用者のコンタクト窓口を特定し、管理すること。

(f) ログイン認証付き Web サイトでは、日常の都度の連絡（計画的サービス停止/定期保守、バージョンアップ、マニュアル類の最新版公開の案内など）、サービス達成状況（サービス稼働率、平均応答時間、サポートサービス応答率等）又は障害発生履歴、現在の稼働状況、利用者からの問合せ件数/内容などの情報公開を検討すること。

(g) 管理ツールでは、クラウド利用者のサービス利用状況（ログイン実績、利用時間、利用ログ提供等）、クラウド利用者から預託された情報の保守取扱い実績などの情報照会機能を検討すること。

(h) 電子メール・FAX では、緊急時の連絡・報告（クラウドサービス内で発生した情報セキュリティインシデントについての情報：障害発生/復旧時刻・障害経過の通知、障害内容・原因・対処等に係る事後報告等）の情報提供を検討すること。

(i) クラウド利用者からの個別要求に基づき、NDA を締結して、個別の情報開示（例：クラウド利用者が希望する種別のインシデント履歴、第三者機関による監査・ぜい弱性検査レポート、クラウド利用者から預託されたデータ・利用ログ記録等の保存場所等）を行う場合は、クラウド利用者にとっての知るメリットとクラウド事業者にとっての情報開示のデメリット（業務負荷の増大も含む）のトレードオフを検討すること。代替案として、監査済みの言明公開や NDA を締結した上での監査報告書（サービス・オーガニゼーション・コントロール報告書（SOC2）、内部統制監査報告書（ISAE3402/SSAE16）[5]等）の情報開示により、対策の実施状況をクラウド利用者に対し保証することも検討すること。

緊急時の連絡・報告の情報提供については、さらに実務上以下を実施することが望ましい。

(j) クラウド利用者に影響を及ぼす情報セキュリティインシデントの発生後、その情報を適切に設定された時間以内に、(h)の手法により、クラウド利用者に通知すること。その後も、適切な時間間隔で情報の通知を続け、クラウド利用者が受領した情報を追跡できるようにすること。

(k) クラウド利用者に一斉周知する情報は、16.1.4【利用者接点とサプライチェーンにおける実務のポイント】(d)に従って提供すること。

(l) クラウド利用者によって発見された情報セキュリティインシデントの情報の受付窓口を設置し、利用者に分かりやすく示すこと。

(m) より正確な情報を相互に交換するために、情報セキュリティインシデントの情報を ICT サプライチェーンで共有するための合意を形成して文書化すること。

(n) (m)の合意に基づき、ICT サプライチェーンを構成する供給者は、情報セキュリティインシデントの際のコンタクト窓口を設置すること。

---

[5] 内部統制監査報告書は情報セキュリティマネジメントの全般をカバーするものではないことを、クラウド利用者にも理解していただくことが望ましい。

(o) 個別契約連携クラウドサービスを提供する場合は、クラウド利用者の便益を考慮し、供給者間の情報共有を積極的に行うこと。

個別契約連携クラウドサービスを提供する場合は、クラウド利用者に対する情報提供は、各供給者が個別に行うことになるため、各々が提供する情報に不整合や質や早さの違いが生じ、結果としてクラウド利用者の不信を招く恐れがある。このため、ICT サプライチェーンを構成する供給者間の情報提供に係る役割分担（例：情報提供窓口の一本化等）を定め、クラウド利用者と合意することが望ましい。

8. 資産の管理

8.1 資産に対する責任

【目的】

組織の資産を特定し、適切な保護の責任を定めるため。

【クラウドサービスの提供において特に留意すべき課題との関係】

クラウド利用者による、重要度が高い預託情報に対する格別の保護要求と、クラウド事業者及びそのサービスに係る情報セキュリティマネジメント並びにそのガバナンスの実態とが整合せず、預託情報の保護に支障をきたすことを防ぐ必要がある。

8.1.1 資産目録

【管理策】

情報及び情報処理施設に関連する資産を特定することが望ましい。また、これらの資産の目録を、作成し、維持することが望ましい。

【クラウドサービスの提供において特に留意すべき課題との関係】

クラウドサービスがクラウド利用者の持つ重要な情報に対する保護要求方針を満足できないにも関わらず、クラウド利用者がこの重要情報をクラウドサービスに預託してしまうと、この預託情報の保護が困難になる恐れがある。そこで、クラウド利用者自身が、その重要度判断とその保護要求方針に従って、クラウドサービス上で取り扱うことができるクラウド利用者の情報を選別して預託できるように、その判断に必要な情報を提供することが求められる。

【利用者接点とサプライチェーンにおける実務のポイント】

クラウド利用者は、情報のライフサイクル（作成、処理、保管、送信、削除及び破棄を含む）に関連したクラウド利用者の情報を特定し、その重要度と業務上の価値を自ら判定し、資産目録として記録・維持（正確かつ最新に保つ）する（ISO/IEC 27002:2013 8.1.1 実施の手引 参照）。クラウド利用者のこの作業を支援するため、クラウド利用者から預託された情報について、実務上以下を実施することが望ましい。

(a) クラウド利用者から預託された情報と、クラウドサービスを運用するための内部情報を、別の資産として分類すること。
(b) 仮想化資源を用いてクラウドサービスを提供している場合は、仮想化資源をラベル付けすること。
(c) (a)(b)等に係るクラウドサービスの特性に基づき、管理水準が異なる預託情報をクラウド利用者が分類するために必要な情報を、6.3.2【利用者接点とサプライチェーンにおける実務のポイント】(i)の手法に基づき、クラウド利用者に提供すること。

8.1.2 資産の管理責任

【管理策】

目録の中で維持される資産は、管理されることが望ましい。

【クラウドサービスの提供において特に留意すべき課題との関係】

クラウド利用者が作成し管理する目録の中の各々の預託情報が求める管理水準を確実にするため、これらの資産が保存されるクラウド事業者の情報処理施設等（仮想化資源を含む）の管理ポリシーに基づいて、クラウド利用者の要求に沿う管理水準を提供できるサービスを選択することが求められる。

【利用者接点とサプライチェーンにおける実務のポイント】

クラウド利用者が作成し管理する目録の中の各々の預託情報が保存されるクラウド事業者の情報処理施設等（仮想化資源を含む）のそれぞれについて、個別に管理ポリシーと管理水準に関する情報を、6.3.2【利用者接点とサプライチェーンにおける実務のポイント】(i)の手法に基づいてクラウド利用者に提供し、クラウド利用者が適切なサービスを選択できるように支援することが望ましい。

8.1.5 クラウド利用者から預託された情報の返却

【管理策】

クラウド利用者がクラウドサービスの利用を終了するにあたり、預託された情報を、クラウド利用者が取扱うことができる形でクラウド利用者に返却し、クラウドサービスの提供に供する情報処理施設等から二度と取り出せないようにすることが望ましい。

【クラウドサービスの提供において特に留意すべき課題との関係】

クラウド利用者がクラウドサービスの利用を終了するにあたり、他のクラウドサービスへの乗換を行うことが想定される。クラウド利用者によるクラウドサービス選定の自由を守るため、預託された情報を他のクラウドサービスに引継ぐことを確実にすることが求められる。

また、クラウドサービス利用終了後に、クラウド事業者から預託情報が流出しないようにすることが求められる。

【利用者接点とサプライチェーンにおける実務のポイント】

クラウド利用者がクラウドサービスの利用を終了するにあたり、預託されていた情報をクラウド利用者が取扱うことができる書式で返却することに加え、有料であるかどうかも含めてその対応方針をクラウド利用者に情報提供し、クラウド利用者が自らのポリシーに沿う返却方法を提供できるクラウド事業者及びサービスを選定できるようにすることが求められる。

また、クラウドサービスの利用終了後に、クラウドサービスに供する情報処理施設等から預託された情報が漏洩しないように、情報を二度と取り出せないようにすることが求められる。

さらに、これらの実施方針がクラウド利用者に周知されることが求められる。

上記を実現するため、実務上以下を実施することが望ましい。

(a) 個々のクラウド利用者の預託情報を、特定して抽出するための措置を講じること。
(b) 13.2.2【利用者接点とサプライチェーンにおける実務のポイント】(e)の事前合意に基づき、預託された情報をクラウド利用者またはその指示によって他のクラウド事業者が取扱うことができる形式で、クラウド利用者に返却すること。
(c) (b)の対応が有料である場合は、その旨をクラウド利用者に周知すること。
(d) クラウドサービスの利用終了後に、預託された情報を二度と取り出せないように消去または破壊すること。
(e) (b)(d)を実現する方法について、クラウド事業者/クラウドサービスを選定するにあたり参考にできるような形で、クラウド利用者（潜在利用者を含む）に情報提供すること。
(f) (e)について詳細な情報の開示を求められた場合には、6.3.2【利用者接点とサプライチェーンにおける実務のポイント】(i)の手法に従って情報開示することを検討すること。

8.2 情報分類

【目的】

組織に対する情報の重要性に応じて、情報の適切なレベルでの保護を確実にするため。

【クラウドサービスの提供において特に留意すべき課題との関係】

クラウドサービスの提供にあたっては、多数のクラウド利用者が存在することに伴い、クラウド利用者の預託情報が、他のクラウド利用者の預託情報と明確に分離できる形で管理されていない恐れがある。さらに、複数のクラウドサービスを提供する場合には、クラウド利用者の預託情報が、サービスごとに分類されていない恐れがある。その結果として、クラウド利用者から預託された情報に対し、クラウドサービスごとに適切な情報セキュリティポリシーや管理水準が適用されなかったり、預託情報がクラウド利用者ごとに保護されなかったりといった事態を生じうる。従って、クラウド利用者から寄託を受ける情報、及び提供するそれぞれのクラウドサービスにおいて供する情報資産等について、クラウド利用者ごと、及びクラウドサービスごとに適切に管理ができるように、必要となる情報の分類を行うことが求められる。

8.2.1　　情報の分類

【管理策】

情報は、法的要求事項、価値、重要性、及び認可されていない開示又は変更に対して取扱いに慎重を要する度合いの観点から、分類することが望ましい。

【クラウドサービスの提供において特に留意すべき課題との関係】

クラウドサービスにおいては、一つの資源を用いて同時に複数のサービスを提供することがある。その場合、クラウド利用者が預託する情報は、それぞれのサービスで重要度が異なることがあるにもかかわらず、同一の管理が行われることになる。その結果として、預託情報の重要度に応じた管理ができないために、クラウド利用者の重要な預託情報が脅威にさらされる恐れがある。これを避ける観点から、クラウド利用者から預託を受けた情報をクラウドサービスごとに区分し、その重要度に応じた管理を行うことが求められる。

【利用者接点とサプライチェーンにおける実務のポイント】

クラウド利用者から預託された情報を、提供するクラウドサービスごとに分類し、その分類に応じた情報セキュリティマネジメントを実施するとともに、クラウド利用者からの求めがあった場合に、その分類ごとの情報セキュリティマネジメントの実施状況を情報開示しうる状況にしておくため、実務上以下を実施することが望ましい。

(a) 複数のクラウドサービスを提供している場合には、提供するサービスに応じてクラウド利用者からの預託情報の分類を行うこと。
(b) (a)の各分類に対し、対応しているクラウドサービスの種類に応じて、預託情報の価値、重要性等を定義すること。
(c) 各々のクラウドサービスの提供において、クラウド利用者からの預託情報を、(b)の定義を踏まえて管理すること。
(d) クラウドサービスの提供にあたり、仮想化された資源を利用している場合は、クラウド利用者からの預託情報を明確に分類できる措置を施すこと。

8.2.3　　資産の取扱い

【管理策】

資産の取扱いに関する手順は、組織が採用した情報分類体系に従って策定し、実施することが望ましい。

【クラウドサービスの提供において特に留意すべき課題との関係】

クラウドサービスにおいては、複数のクラウド利用者から預託を受けた情報を、同一の資源において取り扱うことになる。預託されたクラウド利用者の情報が、他のクラウド利用者のものと明確に分離できる形で管理されていない場合には、預託された情報の返却等が生じた場合に、他のクラウド利用者から預託を受けた情報を混同して返却してしまう等、情報漏えいを生じる恐れがある。

【利用者接点とサプライチェーンにおける実務のポイント】

複数のクラウド利用者から預託を受けた情報を誤って情報漏えいしないよう、それぞれのクラウド利用者から預託を受けた情報を明確に分離して管理できる措置を講じることが望ましい。具体的には、実務上、以下を実施することが望ましい。

(a) クラウド利用者から預託を受けた情報については、それぞれを容易に分離できるような措置を講じること。

(b) 仮想化された資源を用いて預託を受けた情報を管理する場合には、各クラウド利用者から預託された情報を特定できるような措置を講じること。

9. アクセス制御

9.1 アクセス制御に対する業務上の要求事項

【目的】

情報及び情報処理施設へのアクセスを制限するため。

【クラウドサービスの提供において特に留意すべき課題との関係】

クラウドサービスは、インターネットを経由してサービス提供されることから、クラウド事業者、クラウド利用者以外の第三者による不正なアクセスや攻撃の脅威にさらされる。

加えて、クラウドサービスでは、複数の供給者によるサービス連携がなされうること、サービスに供する資源を複数のクラウド利用者が利用することなどから、アクセス制御に係る脆弱性などにより、クラウド事業者やクラウド利用者による不正アクセス等も生じうる。また不完全なアクセス制御などに伴う、サービス提供の不完全性などの課題も生じる。

このようなアクセス制御の脆弱性や不完全性により、クラウド事業者及びそのサービスの信用に大きな悪影響を及ぼす恐れがある。しかし、クラウド事業者は、その高いリスクを認識していないことも多い。このリスクに対処するため、アクセス制御サービスの提供機構の冗長化、ソフトウェアの高信頼化と試験の徹底、操作ミスの防止、運用手順書の質の向上など、幅広い対策を考慮することが求められる。

9.1.1 アクセス制御方針

【管理策】

アクセス制御方針は、業務及び情報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。

【クラウドサービスの提供において特に留意すべき課題との関係】

クラウドサービスにおいては、他の供給者によるクラウド利用者のアクセス制御に依拠してサービスを提供し、あるいは自身の行うアクセス制御に基づいて他の供給者がサービス提供を行うことがある。その際に、供給者間においてアクセス制御に関する業務方針が共有されていないことにより、それぞれの供給者において本来依拠すべきアクセス制御の

方針が順守できない恐れがある。これに伴い、他の供給者による認可されていないアクセスの可能性や供給者内従業員の特権の悪用などの不正、及び特権の勝手な拡大によるアクセス制御/認証/権限付与等への影響を排除できない等の影響が生じる。

【利用者接点とサプライチェーンにおける実務のポイント】

クラウドサービス提供にかかるクラウド利用者のアクセス制御について、複数の供給者間で依存関係がある場合には、それぞれの供給者におけるアクセス制御の方針の間に齟齬が生じて、アクセス制御に支障を来す恐れがある。その可能性を低減するため、導入しているアクセス制御に係る方針を供給者間で文書化し、合意することが求められる。また、供給者間でのアクセス制御に関する役割と責任の分担を定め、技術的対応のために必要な取決めを行うことが望ましい。

具体的には、クラウドサービスの提供にあたり、実務上以下を実施することが望ましい。

(a) アクセス制御サービスを提供している情報処理施設等の冗長化を行うこと。
(b) ソフトウェア更新時の切替試験を徹底して行うこと。
(c) 運用上の設定を行う者とそれを認可する者を分離すること。
(d) 運用手順書のレビューを徹底し、その品質を向上させること。
(e) クラウド利用者が、提供されるクラウドサービスにおいて実施可能なアクセス制御機能を、判断し選択できるようにするため、クラウド利用者から個別に要請を受けた場合は、6.3.2【利用者接点とサプライチェーンにおける実務のポイント】(i)に従い、アクセス制御方針について以下の情報の提供を検討すること。
  - クラウド利用者に付与するアクセス制御権限及び内部統制が機能した権限付与プロセス
  - 導入している ID 管理のフレームワーク（シングル・サイン・オン等の ID 連携を組み込む能力があるか、等）
  - 認証の強度（認証対象とする要素及び数、各要素における技術的・運用的な措置による堅牢性等）
  - シングル・サイン・オン等の ID 連携への対応状況
(f) シングル・サイン・オンや ID 連携を実施する場合は、ICT サプライチェーンにおける管理責任の範囲の設定、役割と責任の分担、技術的対応のための取り決め（仕様書、運用規約・手順等）について明確に定め、文書化すること。なお、個別契約連携クラウドサービスの形態でサービス提供している場合は、クラウド利用者との管理責任の範囲の合意が、通常のクラウド利用者対クラウド事業者の場合よりも複雑なので、責任の所在が不明確になる課題が生じうるため、特に注意を要する。
(g) クラウド利用者から個別に要請を受けた場合は、シングル・サイン・オンや ID 連携の実現と運用に係る技術情報等を、6.3.2【利用者接点とサプライチェーンにおける実務のポイント】(i)に従って提供することを検討すること。

9.1.2 ネットワーク及びネットワークサービスへのアクセス

【管理策】

利用することを特別に認可したネットワーク及びネットワーク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。

【クラウドサービスの提供において特に留意すべき課題との関係】

クラウドサービスでは、クラウド利用者が、クラウド事業者の情報セキュリティの管理外からアクセスすることが一般的である。このため、アクセス制御の対象となるクラウドサービスに供するネットワーク、ネットワークサービス等が適切にコントロールされていない場合には、第三者による不正アクセスをもたらす恐れがある。

またクラウド利用者が、許可されていない情報資産等へのアクセスを行うことにより、クラウドサービス上のクラウド利用者情報の盗聴、改ざん、システムの破壊のほか、利用が許諾されていないサービスへのアクセス等の不適切な利用などの事態を招く恐れがある。

さらに、外部ネットワークサービスの選択によってクラウドサービスが直面しうる脅威と責任の所在について、クラウド利用者に正しく理解していただくための情報提供を行うことが求められる。

【利用者接点とサプライチェーンにおける実務のポイント】

クラウド事業者がネットワーク及びネットワークサービスのアクセス制御を適正に実施しないことにより、上述のように 2 つの問題が生じる。1 つめの問題は第三者による不正アクセスが生じ、クラウド利用者のデータの盗聴、情報漏えい、システムの改ざん、破壊等が生じうることである。2 つめの問題は、クラウド利用者に対するアクセス制御が適切に行われないことにより、他のクラウド利用者のデータ等に対する不正なアクセス、システム等の改ざん、破壊等、また許可されていないサービスへのアクセス等が生じうることである。さらに、クラウド利用者が本来利用できるサービスを適切に利用できないことなども想定される。

これらの問題に対処するため、クラウドサービスに供するネットワーク及びネットワークサービスに対して、第三者による不正アクセスを防止するとともに、クラウド利用者の適正な利用を確保するためのアクセス制御に係る措置を講じることが求められる。具体的には、実務上以下を実施することが望ましい。

(a) クラウドサービスの提供に供するネットワーク及びネットワークサービスについては、クラウド利用者を認証した後のみ内部的なネットワーク等にアクセスできる等の適正なアクセス制御の措置を講じること。
(b) クラウドサービスを利用できる対象者を限定している場合（例：国内からクラウドサービスを利用するクラウド利用者に限定）は、アクセス元サーバに対する認証を行う、又は許可されたクラウド利用者以外からのアクセスを制限する等、第三者からの不要なアクセスを排除する措置を講じること。
(c) クラウドサービスの提供に供するネットワーク及びネットワークサービスで利用するネットワーク機器等における脆弱性について定期的に確認するほか、脆弱性が露見した場合には速やかに対応できる措置を講じること。
(d) 他の供給者と連携してクラウドサービスを提供するために用いるネットワーク及びネットワークサービスについて、連携する供給者間で必要なアクセス制御措置について確認し、これを実施すること。
(e) クラウド利用者による不正なネットワーク及びネットワークサービスの利用がないことを、アクセス制御の設定を確認すること、あるいはクラウド利用者の内部的なネットワーク等のアクセス状況を監視すること等を定期的に行うことにより、確認すること。

9.2 利用アクセスの管理

【目的】

システム及びサービスへの、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。

【クラウドサービスの提供において特に留意すべき課題との関係】

クラウドサービスではクラウド事業者、クラウド利用者、第三者等による認可されていないアクセスによって、システム及びサービスが侵害され、クラウドサービスに供する情報資産の機密性と完全性を危険に曝す事態を招く恐れがある。このような事態を避けるため、秘密認証情報の割当を正式なプロセスによって管理運用することが求められる。

9.2.3 特権的アクセス権の管理

【管理策】

特権的アクセス権の割当て及び利用は、制限し、管理することが望ましい。

【クラウドサービスの提供において特に留意すべき課題との関係】

他の供給者のクラウドサービスを利用してクラウドサービスの提供を行う供給者に所属する特権ユーザは、特権的アクセス権を付与されて他の供給者が提供している特権的なユーティリティプログラムを使用することができる場合がある。この特権的アクセス権が第三者に詐称されると、他の供給者が提供している特権的ユーティリティプログラムが悪用され、9.4.4 で述べるように、第三者が他の供給者が提供するクラウドサービスに不正アクセスするための踏み台とされる恐れがある。この課題を解決するため、特権的アクセス権の保護には、一般のエンドユーザ（個人）とは異なる格別の対策が求められる。

【利用者接点とサプライチェーンにおける実務のポイント】

特権的アクセス権を保護するため、特権的アクセス権を有する特権ユーザに対し、多要素認証技術を適用した認証を行う等の強力な認証機能を提供することが望ましい。これと同時に、9.4.4【利用者接点とサプライチェーンにおける実務のポイント】(a)(b)(c)(d)(e)を確実に実施し、特権的なユーティリティプログラムの監視と保護を強化することが望ましい。

9.2.4 利用者の秘密認証情報の管理

【管理策】

秘密認証情報の割当ては、正式な管理プロセスによって管理することが望ましい。

【クラウドサービスの提供において特に留意すべき課題との関係】

クラウドサービスは一般に規模の大きな共有サービスとなるため、ぜい弱な秘密認証情報の割当てによってアクセス制御が破られた場合の影響が大きくなる恐れがある。特に、特権的なユーティリティプログラムの秘密認証情報が漏えいした場合の影響は深刻である。このため、秘密認証情報の割当てに係る管理を厳しくし、アクセス制御を確実にすることが求められる。

【利用者接点とサプライチェーンにおける実務のポイント】

クラウド利用者のユーザ（個人）が、クラウドサービスが要求する強度の秘密認証情報の割当てを実行できる仕組みを確実に提供することが求められる。

また、秘密認証情報に関する管理情報をクラウド利用者に提供することによって、クラウド利用者がクラウドサービスの提供機能の利用判断をしやすくするため、上記を実現するための手順や秘密認証情報の割当て手順に係る情報を、6.3.2.【利用者接点とサプライチェーンにおける実務のポイント】(b)(f)(i)から手法を選択してクラウド利用者に情報提供することが望ましい。

シングル・サイン・オンや ID 連携を行う場合は、秘密認証情報を複数の供給者間で共有することから、当該情報の管理元からの情報漏えいは、複数の供給者に幅広く影響を及ぼす。このため、秘密認証情報の管理元は、当該情報の情報セキュリティに格別の注意を払うことが求められる。

なお、クラウド事業者が導入すべき正式な管理手続として参考となるものに、Paymant Card Industry(PCI)データセキュリティ基準の要件 8 などがある。

９.４ システム及びアプリケーションのアクセス制御

【目的】

システム及びアプリケーションへの、認可されていないアクセスを防止するため。

【クラウドサービスの提供において特に留意すべき課題との関係】

クラウドサービスは、オープンなネットワーク及びネットワークサービスを用いてサービスが提供されることも多く、クラウド事業者、クラウド利用者以外の第三者による不正なアクセスや攻撃が生じやすい。従って、システム及びアプリケーションに対するアクセス制御のための措置を十分講じていないと、クラウドサービスに供するシステム、アプリケーション、データ等の情報資産に対する改ざん、破壊、情報漏えい等が生じる恐れがある。

加えて、クラウドサービスでは、複数の供給者によるサービス連携が行われる場合があること、サービスに供する資源を複数のクラウド利用者が利用することなどから、アクセス制御に係る脆弱性などにより、クラウド事業者やクラウド利用者による不正アクセス等の事態も生じうる。また不完全なアクセス制御などに伴う、サービス提供の不完全性などを生

じる恐れもある。

これらの課題に対応するため、システム及びアプリケーションへのアクセスを認可されている者に限定するための措置を講じるほか、逆に認可しているアクセスについては、完全に機能できるような対応を図ることが求められる。

9.4.1 情報へのアクセス制限

【管理策】

情報及びアプリケーションシステム機能へのアクセスは、アクセス制御方針に従って、制限することが望ましい。

【クラウドサービスの提供において特に留意すべき課題との関係】

クラウドサービスではクラウド利用者が、クラウド事業者の情報セキュリティの管理外からアクセスすることが一般的である。このため、アクセス制御の対象となるクラウドサービスに供する情報及びアプリケーション機能等が適切に管理されていない場合には、第三者による不正アクセスをもたらす恐れがある。

またクラウド利用者が、許可されていない情報資産等へのアクセスを行うことにより、クラウドサービス上のクラウド利用者から預託された情報の盗聴、改ざん、システムの破壊のほか、利用が許諾されていないサービス機能へのアクセス等の不適切な利用などの事態を招く恐れも生じる。

また、クラウド利用者側の環境（利用する Web ブラウザ、OS、その他のアプリケーション、デバイス等）における脆弱性により、クラウドサービスへの重大な影響が生じる恐れがあるため、これに対応する措置を講じる必要がある。

【利用者接点とサプライチェーンにおける実務のポイント】

第三者からの不正アクセスを防止するため、情報及びアプリケーション機能に対して、第三者による不要なアクセスを防止する措置を講じる必要がある。また、クラウド利用者に対しても、適正な情報及びアプリケーション機能に対するアクセス制御のための措置を講じることが求められる。さらに、クラウド利用者に対する脆弱性の周知、管理責任の範囲の合意などの措置も求められる。具体的には、実務上以下を実施することが望ましい。

(a) クラウドサービスの提供に係る情報及びアプリケーション機能へのアクセス制御について、自社が提供するシステム・プログラム等における脆弱性を定期的に確認するほか、利用する OS、ミドルウェア等における脆弱性に関する情報及び対応策を確認し、必要な措置を講じること。
(b) クラウドサービスの提供において他の供給者と連携する際に、その供給者が提供するアクセス制御に依存している場合は、アクセス制御に係る合意した方針に基づいて他の供給者が実施する措置を確認し、課題が存在する場合は具体的な対応策を協議して、これを実施すること。
(c) 不要なアクセス権限の設定、必要なアクセス権限設定の遺漏等が生じないように、クラウド利用者が利用可能な情報、システム等とクラウド利用者の ID との関係を定期的にレビューする等の措置を講じること。
(d) アグリゲーションサービス事業者は、他の供給者が提供するサービスへのアクセス制御も含めた措置を講じること。

(e) クラウドサービスを利用するのに必要なクラウド利用者側の環境（利用する Web ブラウザ、OS、その他のアプリケーション、デバイス等）の脆弱性に関する情報収集を行い、クラウド利用者に対して必要な情報の提供、対応措置の依頼等の措置を講じること。
(f) クラウド利用者側のシステム/ネットワーク環境におけるアクセス制御に係る脆弱性が原因となって、クラウド利用者からの預託情報に損害等が発生した場合の、クラウド事業者の免責等について、クラウド利用者と予め合意しておくこと。
(g) クラウドサービスを利用するのに必要なクラウド利用者の認証に係る情報の漏えいについて、特にフィッシングやマルウェアなどに関する情報収集を行い、クラウド利用者に対して必要な情報の提供、対応措置の依頼等の措置を講じること。
(h) 認証に係る情報がクラウド利用者から漏えいしたことにより、クラウド利用者からの預託情報に損害等が生じた場合の、クラウド事業者の免責等について、クラウド利用者と予め合意しておくこと。

さらに、クラウド事業者が提供するアクセス制御の範囲と、クラウド利用者が利用可能なアクセス制御機能に基づいて、クラウド利用者がクラウドサービス選択の判断をできるようにするため、アクセス制御方針に係る以下の内容を、6.3.2.【利用者接点とサプライチェーンにおける実務のポイント】(b)(f)(i)から手法を選択してクラウド利用者に情報提供することが望ましい。

(a) 情報アクセス制御手法
(b) アクセス可能な範囲、粒度
(c) 権限管理者、権限付与・変更手順

また、クラウドサービスを提供するために他の供給者のクラウドサービスを利用している場合は、クラウド利用者の ID 管理の利便性を向上させるサービス機能等に係る以下の情報を、6.3.2.【利用者接点とサプライチェーンにおける実務のポイント】(b)(f)(i)から手法を選択してクラウド利用者に情報提供することが望ましい。

(d) シングル・サイン・オン・メカニズムへの対応状況
(e) ID 連携管理の有無

シングル・サイン・オンや ID 連携を実施する場合は、ICT サプライチェーンの供給者間における管理責任の範囲の設定、役割と責任の分担、技術的対応のための取り決め（仕様書、運用規約・手順等）について明確に定め、文書化すること。個別契約連携クラウドサービスの形態である場合は、クラウド利用者との管理責任の範囲の合意が、通常のクラウド利用者対クラウド事業者の場合よりも複雑なので、責任の所在が不明確になるという課題が生じうるため、特に注意を要する。

9.4.4 特権的なユーティリティプログラムの使用

【管理策】

システム及びアプリケーション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。

【クラウドサービスの提供において特に留意すべき課題との関係】

クラウドサービスでは、クラウドサービスの提供を目的とするクラウド利用者に対して、サービス提供に必要な範囲で特権的ユーティリティプログラムを利用できるようにする場合がある。この場合に、特権的ユーティリティプログラムに関するアクセス制御が適切に実施されない等の脆弱性がある場合には、第三者あるいは供給者による、他の供給者が提供するサービスに対する不正アクセス等が生じる恐れがある。

またエンドユーザ（組織）の管理者に対して、サービス利用の管理に関する特権的なユーティリティプログラムを利用できるようにするケースがあるが、この場合も、特権的ユーティリティプログラムに関するアクセス制御が適切に実施されない、あるいは情報セキュリティに関する脆弱性がある場合には、クラウド利用者による他のクラウド利用者の情報資産への不正アクセス等の可能性が生じる。その結果、組織の評判、顧客の信頼および従業員の経験等にも間接的な影響がもたらされる。このため、クラウド事業者は特権的な機能を有するユーティリティプログラムの使用にかかる権限管理を徹底することが求められる。

【利用者接点とサプライチェーンにおける実務のポイント】

クラウドサービスがネットワークを通じて提供される性格を有するものであることから、第三者による特権的ユーティリティプログラムへの不正アクセスを防止するための措置を講じる必要がある。

また、供給者内部での特権的ユーティリティプログラムの管理に加え、クラウドサービスの提供を目的とするクラウド利用者に対して、サービス提供に必要な範囲で特権的ユーティリティプログラムを利用できるようにする際には、他の供給者が提供するサービスへの不正アクセスにより、システムの改ざんや破壊、情報資産の盗聴や漏えい等が生じないようにするための措置を講じる必要がある。なお ICT サプライチェーンを形成している場合には、「１５.２　供給者のサービス提供の管理」の措置を併せて講じることが望ましい。

さらにエンドユーザ（組織）の管理者に対して、クラウドサービス利用の管理に関する特権的なユーティリティを利用できるようにする際には、クラウド利用者による他のクラウド利用者の預託情報への不正アクセスにより、他のクラウド利用者からの預託情報の改ざん、破壊、盗聴、漏えい等が生じないようにするための措置を講じる必要がある。

具体的には主要なシステムと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特権的ユーティリティプログラム等については、以下の対応策を講じることが望ましい。

(a) 特権的ユーティリティプログラム等を外部からの攻撃にさらされにくい環境に隔離すること。
(b) 特権的ユーティリティプログラム等へのアクセス状況を定期的にレビューし、不正なアクセスの監視を行うこと。
(c) クラウドサービスの提供を目的とするクラウド利用者が特権的ユーティリティプログラムを利用できるように権限を付与する場合には、特権的ユーティリティプログラムのアクセス権限及び権限付与・変更手順等を文書化すること。また、アクセス権限付与に関する証跡を記録し、不要なアクセス権限の設定がないかを、定期的なレビューにより確認すること。
(d) クラウドサービスの提供を目的とするクラウド利用者が特権的ユーティリティプログラムを利用する場合には、当

該クラウド利用者に対しても特権的ユーティリティプログラムの利用に関する監視を求め、必要があればこれに関する情報の提供を求めること。

(e) エンドユーザ（組織）の管理者に対して、サービス利用の管理に関する特権的なユーティリティプログラムを利用できるようにする場合には、当該プログラムを通じて、他のクラウド利用者の預託情報へのアクセスがなされていないかを、定期的なレビューにより確認すること。

９.５ 仮想化されたクラウドサービスのアクセス制御

【目的】

仮想化されたクラウドサービスにおいて認可されていないアクセスを防止するため。

【クラウドサービスの提供において特に留意すべき課題との関係】

仮想化されたクラウドサービスにおいては、ソフトウェアによる分離機能のぜい弱性によって、クラウド利用者からの預託情報やクラウドサービス提供のために用いられるクラウド事業者の情報処理施設等に対する不正アクセスが生じることがある。これに対する管理策が求められる。

９.５.１ 仮想化資源の分離の確実な実施

【管理策】

クラウドサービス上のクラウド利用者の仮想化資源を、他のクラウド利用者の仮想化資源やクラウドサービスの内部管理用の仮想化資源と確実に分離し、アクセス制御を確実にすることが望ましい。

【クラウドサービスの提供において特に留意すべき課題との関係】

仮想化された資源を用いてクラウドサービスを提供する場合は、クラウド利用者のニーズに合わせて個別に仮想化マシンを構成することで、マルチテナント型のクラウドサービスを提供している。この場合、仮想化マシンの分離は物理的な分離ではなく、ソフトウェアにより実現されているため、ソフトウェアの分離機能に脆弱性が生じると、マルチテナント環境において、クラウド利用者が、他のクラウド利用者やクラウドサービス提供に係る情報やシステムに対して不正アクセスし、情報、システム等の改ざん、破壊、盗聴、漏えい等を行う恐れがある。このため、仮想化マシンの分離を適切に実施し、アクセス制御を確実にするための措置を講じる必要がある。

【利用者接点とサプライチェーンにおける実務のポイント】

仮想化された資源を用いてクラウドサービスを提供するクラウド事業者は、ソフトウェアの分離機能の技術的ぜい弱性を管理するとともに、クラウド利用者がクラウドサービス上にインストールするソフトウェアに起因する脅威も考慮して、仮想化マシンによるクラウド利用者の利用環境の分離（テナント分離）が適切に実施されるための措置を講じる必要がある。具体的には以下の対応策を講じることが望ましい。

(a) 仮想化マシンを構成するのに用いるソフトウェアの脆弱性について定期的に確認を行い、技術的脆弱性が露見した場合には、適切な措置を講じること。

(b) IaaS・PaaS の場合は、クラウド利用者がクラウドサービス上にインストールしたソフトウェアに潜在するマルウェア等のリスクについても考慮すること。具体的には、ソフトウェアのインストールや変更に係る履歴を取る等の対策により、情報セキュリティ事象が当該インストールソフトウェアに起因するものであることを切り分けられるようにしておくこと。

(c) 仮想化されたアプリケーション、OS、ストレージ、ネットワークについて、テナント間の分離及びテナントとクラウド事業者の内部管理の間の分離を確実に行うこと。さらに、分離された資源に対するアクセス制御を確実にするための措置を講じること。

１０.暗号

１０.１　暗号による管理策

【目的】

情報の機密性、真正性及び／又は完全性を保護するために、暗号の適切かつ有効な利用を確実にするため。

【クラウドサービスの提供において特に留意すべき課題との関係】

クラウドサービスは、オープンなネットワーク及びネットワークサービスを用いてサービスが提供されることが多いことから、暗号は、情報セキュリティマネジメント上非常に重要な役割を担っている。クラウドサービスにおける暗号の適用範囲、暗号化の強度、暗号鍵管理の確実性はサービスレベルに依存することから、クラウド利用者が、自らが求める要求レベルを確保したクラウドサービスを確実に選択できる環境整備が求められる。

１０.１.１　　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。

【クラウドサービスの提供において特に留意すべき課題との関係】

クラウドサービス提供において、暗号は、保管又は伝送される情報の機密性確保/完全性・真正性の検証、アクセス制御における認証、否認防止等に役立てられるため、情報セキュリティマネジメント上非常に重要な役割を担っている。しかし、これらに係るサービスレベルはクラウド事業者により異なることから、クラウド利用者が、自らが求める要求レベルに達しないクラウドサービスを誤って選択すると、クラウド利用者から預託された情報が容認できないリスクにさらされる恐れがある。これを防止するための管理策が求められる。

【利用者接点とサプライチェーンにおける実務のポイント】

暗号による管理策の利用方針は、クラウドサービスにおいて、暗号を用いて保管又は伝送される情報の機密性確保/完全性・真正性の検証、アクセス制御における認証、否認防止等を行う範囲をどこまでとするか、及びこれをどの程度の管理レベルで実施するか（ISO/IEC 27002:2013 10.1.1 実施の手引参照）によって定まる。クラウドサービス提供においては、クラウド利用者が暗号化に関し、自らが求める要求レベルを確保したクラウドサービスを確実に選択できるようにするため、実務上以下を実施することが望ましい。

(a) 暗号化に対応しているサービスを、6.3.2【利用者接点とサプライチェーンにおける実務のポイント】(b)(f) から手法を選択して、クラウド利用者に情報公開すること。また、暗号化されていないクラウドサービスについては、暗号化を代替する機能がある場合は、同じ手法を用いて、これをクラウド利用者に情報公開すること。

(b) クラウドサービスにおいて、保管又は伝送される情報の機密性確保/完全性・真正性の検証、アクセス制御における認証、否認防止等について、暗号化を適用する範囲を明確にし、6.3.2【利用者接点とサプライチェーンにおける実務のポイント】(i)に従って、クラウド利用者に情報開示すること。

(c) (b)を実施するにあたり、外部組織とクラウド事業者の間で転送する情報と長期間保存するクラウド利用者の情報（バックアップ等）の取扱いについて、特に留意すること。

(d) 暗号による管理策の運用実態について、クラウド利用者から個別に情報開示を要求された場合は、6.3.2【利用者接点とサプライチェーンにおける実務のポイント】(i)に基づいて情報開示することを検討すること。

１０.１.２　鍵管理

【管理策】

暗号鍵の利用、保護及び有効期間（lifetime）に関する方針を策定し、そのライフサイクル全体にわたって実施することが望ましい。

【クラウドサービスの提供において特に留意すべき課題との関係】

クラウド事業者が管理する暗号鍵の不正利用は、クラウドサービスの機密性・完全性を損なう。また、クラウド事業者が管理する暗号鍵の喪失は、クラウド利用者の暗号化されたデータの完全性を損なう。このため、暗号鍵の保護と管理（暗号鍵を実際に用いる段階での管理を含む）を確実にすることが求められる。

【利用者接点とサプライチェーンにおける実務のポイント】

一般に、暗号鍵には使用期日を定め、そのライフサイクル全体で（生成→保管→保存→読出し→配布→使用停止→破壊）改変・漏洩・紛失から保護する必要がある。ここで、暗号アルゴリズム、鍵の長さ及びその使用法は、最適な慣行に従って選定する。公開鍵の真正性は認証局により確保することが望ましく、認証局との間では、賠償責任・サービスの信頼性・サービス提供の応答時間を含む契約または SLA を締結することが望ましい（ISO/IEC 27002:2013 10.1.2 実施の手引参照）。これに加えて、クラウドサービス提供においては、実務上以下を実施することが望ましい。

(a) クラウド利用者に対し、暗号化の強度（鍵タイプ、暗号アルゴリズム、鍵の長さ）と鍵管理徹底の実態

（例：鍵管理システムの仕様、推奨する鍵管理手順）を明確に示すため、個別の情報開示や監査済みの言明公開により（6.3.2【利用者接点とサプライチェーンにおける実務のポイント】(c)(i)参照）、クラウド利用者に情報提供すること。

(b) クラウド利用者が、クラウドサービスに預託した情報の暗号化に用いる鍵を、個別に管理できるツールを提供すること。

１２.運用のセキュリティ

１２.１　運用の手順及び責任

【目的】

情報処理施設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。

【クラウドサービスの提供において特に留意すべき課題との関係】

クラウド利用者とクラウド事業者の間で締結したSLA等に基づくクラウドサービスの提供は、サービス設計、構築、運用に至る過程で処理等の不整合が発生した場合、責任不履行といった事態を招く恐れがある。このような事態を回避するためにも、提供するクラウドサービスの SLA 等に係る適切な利用ができるように、運用管理情報やクラウド利用者が必要とする運用操作に関する情報を提供することが望ましい。

１２.１.１　　操作手順書

【管理策】

操作手順は、文書化し、必要とする全ての利用者に対して利用可能とすることが望ましい。

【クラウドサービスの提供において特に留意すべき課題との関係】

クラウド利用者の不適切な操作等に起因して、クラウドサービスの機密性・完全性・可用性が守れなくなることがある。この課題の克服のために、クラウド利用者がそのエンドユーザ（個人）のために作成する操作手順書の活用が効果的である。そこで、クラウド利用者が操作手順書を作成するにあたり基になる情報を提供することが求められる。

【利用者接点とサプライチェーンにおける実務のポイント】

クラウド利用者が、クラウドサービスの情報セキュリティ関連機能（例：ログイン認証機能）の操作手順書を作成し、エンドユーザ（個人）に徹底することを支援することが望ましい。このため、クラウド利用者に対し、6.3.2【利用者接点とサプライチェーンにおける実務のポイント】(f)(i)から手法を選択して、操作手順書作成に必要な情報を提供することが望ましい。また、不明点の解消機能として、6.3.2【利用者接点とサプライチェーンにおける実務のポイント】(d)に基づいて FAQ や問合せ窓口を提供することが望ましい。

１２.１.２　変更管理

【管理策】

情報セキュリティに影響を与える、組織、業務プロセス、情報処理施設及びシステムの変更は、管理することが望ましい。

【クラウドサービスの提供において特に留意すべき課題との関係】

クラウドサービスは、ネットワークを通じてサービス提供を行うため、第三者等からサービスに供するシステムに対する攻撃がなされる脅威があり、これによって悪意のあるプログラムの改ざん、変更、破壊等がなされる恐れがある。また、クラウドサービスにおいては、クラウド利用者が多数に及ぶことがあるため、過失等により誤ったプログラムの適用や削除、破壊等が生じることで、クラウドサービスの提供に影響を及ぼす。これによって、多数のクラウド利用者に影響するサービス停止やサービスレベル低下をきたす可能性が生じ、その影響によってサービスや企業の信頼が低下する恐れがある。このため、クラウド事業者は定期的に変更管理の状況を確認するとともに、変更管理に関する手順等を文書化し、適切な変更管理を行うとともに、意図しない変更が行われた場合に、速やかに元の構成に戻せる措置を講じることが求められる。

【利用者接点とサプライチェーンにおける実務のポイント】

クラウドサービスに供するシステムに対して、第三者、あるいはクラウド利用者/クラウド事業者における特権ユーザによる不正なプログラムの改ざん、変更、破壊等が生じないようにするため、あるいは生じた場合に、可及的速やかに発見できるようにするため、実務上以下を実施することが望ましい。

(a) クラウドサービスに供するシステムに関するプログラムは、安全に隔離された資源において管理を行うこと。
(b) クラウドサービスに供するシステムの変更のために、特権を利用する場合には、その利用を管理できるよう、手順を作成し、記録を作成すること。
(c) クラウドサービスに供するシステムのプログラム変更等について、必要なログ等を取得し、変更管理の状況について定期的にレビューを行うこと。
(d) 仮想化されたデバイス（サーバ、ネットワーク、ストレージ等）の導入・変更・削除、クラウドサービスの停止、バックアップ＆リストア等にあたっては、その障害がクラウドサービスを提供する資産に復旧できない損害を与える恐れがあることから、その手順を文書化し、実務運用者と実施判断者の両方に徹底すること。
(e) アグリゲーションサービスを提供している場合は、他の供給者が提供するクラウドサービスの変更についても、6.3.2【利用者接点とサプライチェーンにおける実務のポイント】(f)(i)から手法を選択し、クラウド利用者に情報提供すること。

上記に加えて、クラウドサービスに供するシステムの変更を行う際に、誤ったプログラムのリリースや削除、破壊などを防止し、また誤ったシステム変更が行われた場合に、可及的に速やかにサービスを復旧できるようにするために、以下の対応策を行うことが望ましい。

(f) クラウドサービスに供するシステムに関するプログラムの変更手順を明確に定め、変更後の確認を、変更した者以外の者が行う等、変更に対するチェック体制を構築すること。

(g) クラウドサービスに供するシステムの変更を行うにあたり、システムにおける直前の構成管理を明らかにし、変更結果から元の構成に戻すことができるように必要なバックアップを取る等の対応を行うこと。

１２.１.３　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。

【クラウドサービスの提供において特に留意すべき課題との関係】

クラウドサービスは、ネットワークを通じてサービス提供を行うため、第三者等からサービスに対する攻撃を受ける脅威があり、これによって不測の資源不足が発生し、これに伴うサービスの停止、低下が生じる恐れがある。またクラウド利用者による悪意のあるサービス利用や、一部のクラウド利用者による不正な資源の占有などにより、これに伴うサービスの停止、サービスレベル低下が生じる恐れがある。

またクラウドサービスはオンデマンドサービスとしての性格を持つため、クラウドサービスの提供に必要な資源は統計的な予測に従って割り当られていることが多い。そのため、予測の範囲を超えたクラウド利用者のニーズの集中が発生すると、資源が枯渇し、クラウドサービスの提供に支障を来す恐れが生じる。具体的には、資源の設定・割り当てに際して、不正確なモデリング又はクラウドのインフラ基盤に対する不十分な投資の下で行われることで、クラウド事業者において、以下の事態を招く可能性がある。

(a) 特定の資源を集中的に使用するアプリケーションが存在する場合に、その資源使用の予測に必要な仕組みを構築しないことに伴い、特定の資源の枯渇が予測できなかった場合には、アプリケーションの起動が停止し、または著しく動作が低下するなどにより、サービスの停止、クラウド利用者が預託するデータの滅失などが生じる。

(b) システムに必要な資源の枯渇により、システムの停止等が生じ、その結果として例えばIPSのフィルタリング機能が動作しないままで運用されてしまう等の脆弱性が生じ、アクセス制御が侵害される。

(c) クラウド利用者のサービス利用に関する要求や求められるサービスレベルの達成に対応することができず、クラウド事業者において、経済的損失、評判の低下等が生じる。

(d) 資源のニーズに関する不正確な予測によって、サービス提供に際して、インフラ資源の過剰な拡張が生じ、これに伴う費用の拡大等により収益性の悪化が生じる。

このため、すべてのクラウドサービス提供に供する資源に求められる容量・能力の監視・調整を行うとともに、6.3.2【利用者接点とサプライチェーンにおける実務のポイント】(f)(g)から手法を選択し、クラウド利用者に現状に関する情報を適切に提供する必要がある。

【利用者接点とサプライチェーンにおける実務のポイント】

サービス提供にあたり、第三者からの攻撃やクラウド利用者の不正な資源の利用が生じないようにするために、以下の対応策を講じることが望ましい。

(a) クラウドサービスに供するシステムで使用される資源の容量・能力等に不足が生じないように、状況に応じて必要な措置を講じるため、資源を常時監視すること。

(b) 外部からの攻撃や、利用者による不正な資源の利用により、サービス提供に必要な資源が枯渇する危険性が生じた場合には、それらを遮断、分離、停止できる対応策を講じること。

(c) 他のクラウド利用者に対するサービスを阻害するような資源の利用をした場合にサービス利用凍結を含めた措置を行う旨の、資源の利用に関する合意を、クラウド利用者との間で行うほか、クラウド利用者が過大な資源の占有を行わないようにするための対策を講じること。

(d) クラウド利用者がクラウドサービスの資源逼迫状況や兆候を把握し、そのリスク管理等に役立てるため、資源の使用率や停止している資源の状況等を 6.3.2【利用者接点とサプライチェーンにおける実務のポイント】(f)(g)から手法を選択し、情報提供すること。

さらに、クラウドサービスの提供にあたり、必要な容量・能力を十分かつ効率的に確保するため、以下の対応策を講じることが望ましい。

(e) 資源確保の予測を的確に行えるようにするため、最適な資源配分を行う仕組みの有効性と運用設定の妥当性を定期的にレビューすること。

(f) クラウド利用者が要求する論理資源を十分に割り当てるため、物理資源使用の限界を超えた論理資源の総和を設定すること。この際、論理資源の総和が物理資源を超過するような資源の割当は、物理資源の最繁時の同時使用率を考慮して行うこと。

(g) 運用者向けの手順書のレビューにおいて、容量及び能力が設計時の想定を超えた場合の対応手順（仮想資源の再配置のためのライブマイグレーション及び仮想ネットワークの変更手順等）が確実に行われるようにすること。

１２.２ マルウェアからの保護

【目的】

情報及び情報処理施設がマルウェアから保護されることを確実にするため。

【クラウドサービスの提供において特に留意すべき課題との関係】

クラウドサービスの特性上、クラウド事業者がサービスに供するシステムにマルウェアが感染した場合には、サービスに供するシステムの改ざん、破壊等による、システムの停止、管理しているクラウド利用者の預託データ等の漏えい等の発生、クラウド利用者が利用するシステム等への感染といった深刻な事態を招く恐れがある。

また、あるクラウド利用者が利用するシステム等へのマルウェア感染によって、提供しているクラウドサービスが影響を受け、あるいはクラウド事業者のシステムに感染するなどにより、上述のような事態が生じることもありうる。

このため、マルウェア対策を行うとともに、クラウド事業者のどの情報処理施設が感染したのかを、6.3.2【利用者接点とサプライチェーンにおける実務のポイント】(f)(h)から手法を選択して、クラウド利用者に情報提供することが求められる。

１２.２.１　マルウェアに対する管理策

【管理策】

マルウェアから保護するために、利用者に適切に認識させることと併せて、検出、予防及び回復のための管理策を実施することが望ましい。

【クラウドサービスの提供において特に留意すべき課題との関係】

クラウドサービスは、オープンなネットワーク及びネットワークサービスを用いてサービスが提供されることが多いため、第三者による攻撃のほか、クラウド利用者を経由して、クラウド事業者がサービス提供に供するシステムに感染する可能性がある。このため、マルウェアに対する管理策をクラウド事業者において行うとともに、クラウド利用者に対してもマルウェア対策などを呼びかけ、対応を促す必要がある。

またマルウェアに感染した場合は、クラウド事業者のどの情報処理施設が感染したのかを、クラウド利用者に迅速に情報提供する仕組みを構築することが求められる。

【利用者接点とサプライチェーンにおける実務のポイント】

クラウドサービスに供する情報処理施設等へのマルウェアの感染を防止し、あるいは感染後、二次的な被害の発生（情報の漏えい、クラウド利用者への感染等）を防止するための措置を講じる必要がある。さらに、感染後、サービス再開に向けた必要な対応策を講じる必要がある。具体的には、実務上以下を実施することが望ましい。

(a) クラウドサービスに供する情報処理施設等に侵入したマルウェアのスキャン＆検出を毎日実施するほか、第三者からの攻撃等が生じた場合等のマルウェアへの感染が疑われる情報セキュリティ事象が生じた場合にも、マルウェアのスキャン＆検出を速やかに行うこと。また、これに必要な情報収集を日常的に行うこと。

(b) クラウドサービスに供する情報処理施設等に対するマルウェアの感染が認められた場合には、速やかなマルウェアの駆除、外部ネットワークとクラウド事業者が管理するクラウド利用者の預託データとの分離等の、二次的な被害の発生を防止するための措置を講じること。

(c) クラウド利用者の情報処理施設等でマルウェア感染の可能性が生じた場合には、クラウドサービスに供する情報処理施設等においても、速やかにマルウェア検出のための措置を講じること。

(d) マルウェア感染に伴いクラウドサービスが停止した場合には、速やかにクラウド利用者に対してその事実を示すとともに、クラウド利用者の情報処理施設等のマルウェア感染の確認を促す等の措置を講じること。さらに、クラウド利用者に対し、必要に応じて、被害状況、サービスの復旧見込み等についての情報を、6.3.2【利用者接点とサプライチェーンにおける実務のポイント】(h)の手法によって提供する。

(e) アグリゲーションサービス事業者は、提供するクラウドサービスのICTサプライチェーンの一部の情報処理施設等にマルウェアの感染が認められた場合であっても、影響範囲が確認できるまで、ICT サプライチェーン全体で(b)(c)の措置を講じること。その上で原因が特定され、影響範囲が明確になった段階で、ICT サプライチェーンにおいてクラウド利用者に影響が及ばない措置を講じたうえで、サービスの提供を再開すること。

また自社のサービス利用に供するクラウド利用者の情報処理施設等を攻撃対象としたマルウェアへの感染を防ぐため、以下の対応策を講じることが望ましい。

(f) 自社のサービス利用に供するクラウド利用者の情報処理施設等を攻撃対象としたマルウェアに関する情報を日常的に収集し、6.3.2【利用者接点とサプライチェーンにおける実務のポイント】(f)の手法により、クラウド利用者に提供すること。

(g) マルウェアが伝送されてくる等、特定のクラウド利用者がマルウェアに感染した兆候を検知した場合は、その事実をクラウド利用者に通知するとともに、必要があれば当該利用者のクラウドサービス利用を一時停止できるよう、契約上及び技術上の措置を講じること。

１２.３ バックアップ

【目的】

データの消失から保護するため。

【クラウドサービスの提供において特に留意すべき課題との関係】

クラウドサービスでは、一部のクラウド利用者の預託データについて、証拠提出の要請や、司法官憲等による押収などが生じた場合に、当該クラウド利用者に関するデータだけではなく、他のクラウド利用者の預託データまでもが一緒に押収されてしまう恐れがある。ハードディスクが押収された場合だけでなく、クラウド事業者が取得したバックアップが押収された場合も同等のことが生じうる。これによって、多くのクラウド利用者の預託データが第三者の管理下に置かれる等の事態を生じ、結果としてクラウド事業者やクラウドサービスの信用低下などに繋がりかねない。従って、これを防止する措置を講じることが求められる。

１２.３.１ 情報のバックアップ

【管理策】

情報、ソフトウェア及びシステムイメージのバックアップは、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。

【クラウドサービスの提供において特に留意すべき課題との関係】

クラウドサービスでは、マルチテナントサービスとしての特性から、複数のクラウド利用者の預託データを一括してバックアップを取得することが多い。このため、一部のクラウド利用者が預託したデータについて、証拠提出の要請や、司法官憲等による押収などが生じた場合に、当該クラウド利用者に関する預託データだけではなく、クラウドサービス提供に不可欠な設定などに関するデータや、他の多くのクラウド利用者の預託データも含んだバックアップが押収の対象となってしまう可能性がある。この場合、クラウドサービスの継続性が阻害される恐れがあるため、これを防止する措置を講じる必要がある。

【利用者接点とサプライチェーンにおける実務のポイント】

クラウド事業者が取得するバックアップについて、特定のクラウド利用者の預託データの押収等が生じた場合でも、クラウドサービスを継続できるようにするため、実務上以下を実施することが望ましい。

(a) クラウド事業者が取得するバックアップのうち、クラウドサービス提供に不可欠な設定などに関するデータのバックアップと、クラウド利用者の預託データのバックアップを分離すること。

(b) クラウド利用者の預託データのバックアップにおいて、個々のクラウド利用者の預託データを特定できる、ないしは検索可能な措置を講じること。

(c) 特定のクラウド利用者の預託データの押収等がなされた場合でも、(b)によりその対象を最小限の範囲に限定することで、無関係なクラウド利用者の預託データのバックアップが、外部の第三者の管理下におかれないようにすること。

１２.４　ログ取得及び監視

【目的】

イベントを記録し、証拠を作成するため

【クラウドサービスの提供において特に留意すべき課題との関係】

クラウドサービスの特徴として、ネットワークを活用すること、複数の供給者や多数の利用者がクラウドサービス提供に係る資源にアクセスすることなどが挙げられる。このため、外部及び内部からの攻撃等の脅威にさらされやすくなるため、ログを取得して監視を行うことで、分析等に基づく予防的対策や、情報セキュリティインシデントの事後のトレース等に役立てることができる。

クラウドサービスにおけるログの取得に関しては、二つの重要な課題が存在している。

一つは、複数の供給者が構成する ICT サプライチェーンにおいて、供給者間でのログ取得・管理に対するポリシーや取得範囲等に対する合意がない、又はこれらが不明確・曖昧であるために、供給者によっては必要なイベント等のログ取得がなされない、あるいは取得されたログが保持されないといった課題が生じうることである。

もう一つは、マルチテナントサービスとしての性質上、多数のクラウド利用者に係るログを、ひとまとめにして取得している場合の課題である。この場合、一部のクラウド利用者の行為に関して、第三者から法令等に基づくログ提出を求められたり、あるいは司法官憲等からのログの押収等があった場合に、他の多数のクラウド利用者のログまでもが対象となってしまう恐れがある。その結果として、他のクラウド利用者のログが第三者の管理下に置かれることになり、クラウド事業者やクラウドサービスの信用低下などに繋がる場合がある。

１２.４.１　　イベントログ取得

【管理策】

利用者の活動、例外処理、過失及び情報セキュリティ事象を記録したイベントログを取得し、保持し、定期的にレビューすることが望ましい。

【クラウドサービスの提供において特に留意すべき課題との関係】

クラウドサービスでは、多数のクラウド利用者がサービス提供に供する同一の資源を利用するため、一部のクラウド利用者の不正行為や、不適切なサービス利用により、他のクラウド利用者に対するサービス提供が損なわれ、サービスレベル低下や事業者の信用低下などに至る恐れがある。また特権ユーザによる悪意の行為や外部からの攻撃などによっても、情報の漏えい等が発生する可能性がある。

これらへの対応措置の一つとして、脅威となるイベント等に対するログ取得が挙げられる。しかし、クラウドサービス提供にあたり複数の供給者が構成する ICT サプライチェーンにおいて、供給者間でのログ取得・管理に対するポリシーや取得範囲等に対する合意がない、又はこれらが不明確・曖昧であるために、供給者によっては必要なイベント等のログ取得がなされない、あるいは取得されたログが保持されないといった課題が生じうる。そこで、供給者間で取得するログの範囲、内容、粒度等について合意しておくことが望ましい。特に、アグリゲーションサービス事業者においては、アグリゲーションサービス全体について、統一したポリシーでログ取得等を行うことが求められる。

【利用者接点とサプライチェーンにおける実務のポイント】

アグリゲーションサービスを提供する場合には、アグリゲーションサービス事業者が主導し、他の供給者との間で取得するログの範囲、内容、粒度等に関して合意するために、実務上以下を実施することが望ましい。

(a) アグリゲーションサービス事業者は、他の供給者との間で、取得できるログの範囲、内容、粒度等について情報を共有すること。
(b) アグリゲーションサービス事業者は、他の供給者のイベントログ取得ポリシーを確認し、これを踏まえて ICT サプライチェーン全体で、一貫して適用するイベントログ取得ポリシーの範囲を明示・調整すること。

１２.４.２　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。

【クラウドサービスの提供において特に留意すべき課題との関係】

ログ機能及びログ情報の保護に関する管理策が行われていないと、必要なログの記録の削除や、改ざん、設定の変更などによって、クラウド利用者や特権ユーザによる不正なサービス資源の利用等や、外部からの攻撃の監視が不十分になる恐れがある。さらに、アグリゲーションサービスを提供する場合は、他の供給者との間でログ情報の保護に関する方針や対応策について合意が取れていない場合には、アグリゲーションサービス全体として講ずべき情報セキュリティマネジメントに必要なログの保護がなされない恐れが生じる。

【利用者接点とサプライチェーンにおける実務のポイント】

クラウド利用者や特権ユーザによる不正アクセスや外部からの攻撃等からログ情報を保護することが求められる。さらに、クラウドサービス提供にあたっては、一部のクラウド利用者や特権ユーザの犯罪行為等に伴う記録媒体の押収、ク

ラウド利用者等による不正な行為への対応のためのログ記録の提出等により、提供するサービスの停止等が生じないための措置を講じることが求められる。具体的には、実務上以下を実施することが望ましい。

(a) 適切なアクセス制御、資源の分離等の保護対策を適用し、ログ情報の記録の削除や、改ざん、ログ取得設定の変更などを防止すること。
(b) 一部のクラウド利用者等の犯罪行為等に伴う記録媒体の押収等によるサービス停止を防ぐため、ログ情報のバックアップを作成するとともに、ログ情報をエンドユーザ（個人）/特権ユーザ単位に管理できる措置を講じること。
(c) アグリゲーションサービス事業者は、他の各供給者のログ情報の保護ポリシーを確認し、ICT サプライチェーン全体で適用できるポリシーの範囲を明らかにすること。

１２.４.３　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、記録し、そのログを保護し、定期的にレビューすることが望ましい。

【クラウドサービスの提供において特に留意すべき課題との関係】

クラウドサービスでは、複数の供給者によるサービスを連携して提供することがあるが、供給者は連携関係にある他の供給者のクラウドサービスの利用者として、当該サービスが有する管理機能等により特権利用を行うことがある。管理機能に対して適切な権限設定やログ機能に対する保護措置が取られていない場合には、管理機能を悪用する危険性がある。

また、クラウド利用者（エンドユーザ、他の供給者のクラウドサービスを利用する供給者）の特権利用状況を全体的に把握するためには、全ての供給者において取得するログを突合する必要等が生じるが、供給者間で取得するログで対象とするイベントの範囲や、イベントにおける詳細事項について合意が取れていない場合には、ログの分析に必要な情報が記録されない恐れがある。

【利用者接点とサプライチェーンにおける実務のポイント】

実務管理者や運用担当者の特権利用について、他の連携する供給者が提供する管理機能等を利用する場合も含めて監視できるよう、ICT サプライチェーンの供給者間で、取得するログで対象とするイベントの範囲やその詳細事項について合意することが求められる。さらに、特権の悪用から保護する措置の一環として、取得したログに対する適切な保護対策を講じるとともに、定期的なレビューを行う必要がある。これらの措置を確実にするため、以下の対応策を講じることが望ましい。

(a) 特権利用に基づく資源利用に係るログを特権ユーザ単位で取得し、管理者による不正行為に対する措置を講じられるようにすること。また、クラウド事業者による特権利用のログと突合し、クラウド利用者とクラウド事業者の適正な運用責任の分担を検証できるようにすること。
(b) システムの脆弱性、サービス管理のためのアプリケーションなどの脆弱性を利用した管理用インターフェイスの悪

用を防ぐため、管理アプリケーションに対する利用状況やそのためのプログラム等の構成管理状況のログを取得し、監視等の措置を講じること。

(c) (a)(b)の求めに応じて定めるログ取得方針について、ICT サプライチェーンの供給者間で合意すること。

(d) 取得した特権利用に関するログについて、発生したイベントの妥当性等を検証し、あるいは不正なアクセスの可能性を分析するなど、適切なレビューを行うための措置を講じること。

また、アグリゲーションサービス事業者は、クラウドサービス全体に対する監視が求められることから、サービス提供のためのICTサプライチェーン全体で適用できるログ取得・保護方針の範囲を明らかにすることが求められる。具体的には、以下の対応策を講じることが望ましい。

(e) アグリゲーションサービス事業者は、各供給者のログ取得及び記録保護等に関するポリシーを確認し、ICT サプライチェーン全体で一貫して適用できるポリシーの範囲を明らかにすること。

(f) アグリゲーションサービス事業者は、ICT サプライチェーン全体でどのようなログ情報を一貫して取得できるのかを確認し、各供給者間で突合が可能なログ情報の範囲を明らかにすること。

１２.５ 運用ソフトウェアの管理

【目的】

運用システムの完全性を確実にするため。

【クラウドサービスの提供において特に留意すべき課題との関係】

クラウド利用者がクラウド上にインストールしたソフトウェアが悪意を持った動作をすることで、クラウドサービスの継続や信用に影響を及ぼす恐れがある。このため、これに対する管理策が求められる。

１２.５.１ 運用システムに関わるソフトウェアの導入

【管理策】

運用システムに関わるソフトウェアの導入を管理す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提供において特に留意すべき課題との関係】

クラウド利用者がクラウドサービスに供する資源上にインストールしたソフトウェアが悪意を持った動作をすることで、当該クラウドサービス資源上に脆弱性が生じ、DDoS 攻撃の踏み台となったり、情報漏えいが生じたり、サービスの利用が困難になる恐れがある。さらに、これらに伴い、司法官憲等による犯罪証拠の押収を受ける可能性も生じる。

このため、クラウド利用者がクラウドサービス上にインストールするソフトウェアについて、マルウェアに感染していないことを事前に確認すること、アップロードや変更の証跡を記録しその記録を保存・保護すること、不正な挙動を示した場合はその原因となったソフトウェアを特定できる措置を講じること等が求められる。

【利用者接点とサプライチェーンにおける実務のポイント】

クラウドサービス上に、クラウド利用者が供するソフトウェアのインストールを行うことができる資源を提供する場合、当該ソフトウェアの悪意ある動作に対応するため、以下の対応策を実施することが望ましい。

(a) 情報セキュリティマネジメントの観点から必要である場合には、クラウド利用者がクラウドサービス上にインストールできるソフトウェアの範囲に制限を設け、クラウド利用者と合意すること。

(b) クラウド利用者がクラウドサービス上にインストールしたソフトウェアにより、クラウドサービスに情報セキュリティマネジメント上の脆弱性が生じた場合には、当該クラウド利用者が利用する資源を隔離して、安全にサービスを提供できるような措置を講じること。

(c) クラウド利用者がクラウドサービス上にインストールしたソフトウェアにより、クラウドサービスに情報セキュリティマネジメント上の脆弱性が生じたため、安全なサービスの提供が継続できない場合には、速やかにクラウドサービスの全部または一部を停止する等の講じること。

(d) 利用規約等によって、クラウド利用者の運用により、マルウェアに感染したソフトウェアをクラウドサービス上にインストールさせないことを求めること。

(e) クラウド利用者がインストールしたソフトウェアに起因して、他のクラウド利用者に影響を及ぼすような情報セキュリティ事象が発生した場合に、その原因を切り分けられるように、クラウド利用者によるソフトウェアのアップロード及び変更の履歴を保持すること。

１２.６　技術的ぜい弱性管理

【目的】

技術的ぜい弱性の悪用を防止するため。

【クラウドサービスの提供において特に留意すべき課題との関係】

技術的ぜい弱性の悪用により、クラウドサービスの継続に影響を被ることに留まらず、クラウド利用者の事業・権利保護・コンプライアンス確保に支障をきたすことがありうる。この場合、クラウド事業者のサービス・組織・経営等に対する、クラウド利用者からの信頼を失う恐れがある。このため、技術的ぜい弱性の悪用防止には、重点を置いて取り組むことが求められる。

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、時期を失せずに獲得することが望ましい。さらに、それら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。

【クラウドサービスの提供において特に留意すべき課題との関係】

技術的ぜい弱性が、攻撃者による攻撃、クラウド利用者の不正、クラウド事業者の内部不正等で悪用された場合、

クラウド利用者の預託データの機密性・完全性が失われたり、DDoS 攻撃・インシデント対応・司法官憲等による犯罪証拠の押収等によって長時間サービスが停止して可用性が失われたり、他のクラウド利用者の不正行為によって利用しているクラウドサービスの IP アドレスが外部サービスによりブロックされたりといった事態が発生する恐れがある。このため、技術的ぜい弱性の悪用を防止する管理策を実施することが求められる。

【利用者接点とサプライチェーンにおける実務のポイント】

一般には、技術的ぜい弱性管理のためには、適切な IT 資産管理による完全な資産目録の維持、管理のための役割と責任の確立、情報の収集、技術的ぜい弱性が発見された際の処置選択の判断及び処置実施に係る対応プロセスの確立、監査ログの保持、対応プロセスの有効性の監視・評価等を行う必要がある（ISO/IEC 27002:2013 12.6.1 実施の手引参照）。さらに、クラウドサービスの提供にあたっては、実務上以下を実施することが望ましい。

(a) クラウドサービスとその資源に適用される技術的ぜい弱性管理についての情報を、6.3.2【利用者接点とサプライチェーンにおける実務のポイント】(f)(i)から適切な手法を選択して、クラウド利用者に提供すること。
(b) ISO/IEC 27002:2013 の 12.6.1 の実践の規範が示すポイントを実現する手法についても、(a)と併せてクラウド利用者に情報提供することを検討すること。
(c) クラウド事業者が実施する技術的ぜい弱性の同定作業に伴い、計画的なサービス停止が発生する場合は、6.3.2【利用者接点とサプライチェーンにおける実務のポイント】(f)に従って、クラウド利用者に事前に情報公開すること。
(d) 個別のクラウド利用者に係る技術的ぜい弱性情報を、他のクラウド利用者に提供しないこと。

１２.７　情報システムの監査に対する考慮事項

【目的】

運用システムに対する監査活動の影響を最小限にするため。

【クラウドサービスの提供において特に留意すべき課題との関係】

運用システムの点検を伴う監査要求事項及び活動は、クラウドサービスの運用業務プロセスの中断を招く恐れがある。このため、監査要求事項及び活動がクラウドサービスのサービスレベル低下に繋がらないための措置を講じることが求められる。

１２.７.１　　情報システムの監査に対する管理策

【管理策】

運用システムの検証を伴う監査要求事項及び監査活動は、業務プロセスの中断を最小限に抑えるために、慎重に計画し、合意することが望ましい。

【クラウドサービスの提供において特に留意すべき課題との関係】

運用システムの点検を伴う監査要求事項及び活動が、クラウドサービスの運用業務プロセスの中断を招くことがないように、監査に必要な点検活動を最小限に留め、運用業務プロセスの中断リスクを最小化する措置を講じることが求められる。

【利用者接点とサプライチェーンにおける実務のポイント】

クラウドサービスの監査については、最小限の点検によって管理策の十分性を確認できるような対応策を講じて、運用業務プロセスの中断リスクを最小限にすることが望ましい。また、クラウド事業者の負担を軽減し、クラウドサービス中断リスクを低減するため、クラウド利用者からの個別の監査対応要請を減ずるための措置を講じることが求められる。具体的には、実務上以下を実施することが望ましい。

(a) 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、監査対象となる資源とサービス提供に係る情報資産等の分類を適切に行い、監査対象を明確にし、最小限の監査により、管理策の十分性を確認できるようにする等、効果的な監査を実施できるようにする措置を講じること。

(b) クラウド利用者からの個別の監査対応要請を少なくするために、監査済みの言明公開、監査報告書の情報開示等、その他必要な情報の開示、認証の取得等、クラウド利用者が行う監査対応を簡素化するための措置を講じること[6]。

また、財務諸表に関連する場合に限定されるが、クラウド利用者は、米国公認会計士協会（AICPA）の米国保証業務基準書第16号（SSAE16）、又は日本公認会計士協会の監査・保証実務委員会実務指針第86号に基づく監査を受けているクラウド事業者を優先的に選択する場合がある。このような場合には、これらの基準/指針に基づく内部統制監査報告書をNDAを締結した上で情報開示することによっても、クラウド利用者が行う情報システム監査対応の簡素化に貢献できることが多く、検討に値する。

１３.通信のセキュリティ

１３.１　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情報処理施設の保護を確実にするため。

【クラウドサービスの提供において特に留意すべき課題との関係】

[6] 特定非営利活動法人日本セキュリティ監査協会（JASA）では、クラウドセキュリティ推進協議会（JCISPA）において、クラウド情報セキュリティ監査制度の検討を進めており、その中で言明要件の検討も実施しているので、参考にされたい。

ネットワークの設計ミスや設定ミスは、クラウドサービスの提供に広範囲な影響を及ぼしやすく、クラウドサービスの全面停止や可用性喪失を生じやすい。その結果、多数のクラウド利用者に影響を及ぼし、クラウド事業者及び提供するサービスに対する著しい信頼低下をきたす恐れがある。このため、クラウドサービスの提供にあたっては、ネットワークの設計・設定ミスの防止について、特に慎重な管理を行うことが求められる。

１３.１.４　仮想ネットワークにおいて重視すべき脆弱性

【管理策】

仮想ネットワークの複雑な構成や設定に伴う管理ミスを防止する措置を講じることが望ましい。

【クラウドサービスの提供において特に留意すべき課題との関係】

仮想ネットワークを構築してクラウドサービスを提供する場合、仮想ネットワークの構成や設定が複雑で、物理ネットワークの構成や設定と一貫していない場合には、運用管理に係る経験やノウハウが共通化されず、仮想ネットワークの管理ミスを生じやすくなる。また、IaaS/PaaS を提供している場合は、クラウド利用者がオンプレミスからクラウドサービスに移行するタイミングを狙い撃ちして悪意の攻撃を行い、これによって潜在した脅威を、クラウドサービスの新しい仮想ネットワーク上に持ち込ませることが増えており、注意を要する。

【利用者接点とサプライチェーンにおける実務のポイント】

仮想ネットワークを構築してクラウドサービスを提供する場合には、仮想ネットワークの管理ミスを防止し、オンプレミスから移行するクラウド利用者に対する移行中の悪意の攻撃にも留意するため、実務上以下を実施することが望ましい。

(a) クラウドサービスの提供にあたり、仮想ネットワークを新たに構築する場合は、物理ネットワーク構成との対応関係が明確になるように仮想ネットワークを構成すること。

(b) 仮想ネットワークの運用設定方針と設定承認方針を、物理ネットワークの運用経験とノウハウに基づいて実施しやすい形で定義し、文書化すること。

(c) PaaS/IaaS を提供している場合は、クラウド利用者の構内設備をクラウドサービスに移行させる際に、仮想/物理ネットワークの再構成、移行、試験運用のプロセスで悪意の攻撃を受けないように、クラウド利用者にセキュリティ管理の徹底を助言すること。

１３.２　情報の転送

【目的】

組織の内部及び外部に転送した情報のセキュリティを維持するため。

【クラウドサービスの提供において特に留意すべき課題との関係】

クラウドサービス提供においては、情報転送は不可欠であり、安全な情報転送が確保されないと、クラウドサービスの提供自体の安全性が損なわれることになる。

具体的には、情報転送に必要な資源の割当がなされないと、サービス低下を招く可能性があるほか、複数の供給者のサービス利用において、所定の情報転送がなされないと、サービスの完全性を損なうことにつながる。さらに内外の情報転送において、必要な安全措置が講じられていないと、盗聴等の情報漏えいが生じる等の可能性を生じる。

１３.２.２　情報転送に関する合意

【管理策】

合意では、組織と外部関係者との間の業務情報のセキュリティを保った転送について、取り扱うことが望ましい。

【クラウドサービスの提供において特に留意すべき課題との関係】

ICT サプライチェーンにおいて、データ連携に係る標準的な規格や仕様等に係る合意ができないことにより、供給者間の情報転送において遅延や欠損等が生じ、クラウドサービス提供の完全性を損なう恐れがある。

また提供するクラウドサービス内、あるいは外部とのデータ連携において、必要な暗号化や資源の隔離等がなされていない、あるいはクラウド利用者のユーザ ID 窃取に対する必要な措置が施されていない場合には、盗聴等による情報漏えい等が生じる恐れがある。

さらに、クラウドサービスの利用終了時に、預託された情報の返却を行うにあたり、事前にデータ規格、仕様等についての合意がなされていない場合には、クラウド利用者に対して適正な形で預託情報を返却できず、クラウド利用者からの信頼喪失などを招く恐れがある。

これらの３つの課題に対応する管理策の実施が求められる。

【利用者接点とサプライチェーンにおける実務のポイント】

ICT サプライチェーンを構成する供給者間でのデータ連携に係る標準的な規格・仕様、クラウドサービス内又は外部とのデータ連携における暗号化・資源の隔離及びクラウド利用者のユーザ ID 窃取に対する措置、クラウド利用者から預託された情報の返却に係るデータ規格・仕様等について必要な合意を確立し、これらのデータ連携や預託情報の返却に係る情報転送を確実かつ安全に実施できるようにすることが求められる。このため、実務上以下を実施することが望ましい。

(a) ICT サプライチェーンを構成してクラウドサービスを提供する場合には、他の供給者との間で、クラウドサービスの提供におけるデータ転送に係る方針、標準的な規格・仕様等及びこれに対する保守方針等について調整し、データ転送が確実かつ安全に実施できるように、必要な合意を行うこと。

(b) ICT サプライチェーンを構成してクラウドサービスを提供する場合には、他の供給者のサービスが停止した場合のデータ転送の安全確保等に係る措置を講じること。

(c) クラウドサービス内又は外部とのデータ連携を行うにあたり、暗号化・資源の隔離等の、情報転送を確実かつ安全に実施できる措置を講じること。

(d) フィッシング対策等の秘密認証情報窃盗への対応、及びクラウド利用者への注意喚起を行うことにより、クラウド利用者からの ID 等の秘密認証情報の転送の安全を確保するための措置を講じること。

(e) クラウドサービスの利用終了時に、預託された情報を安全かつ完全な形で返却するために、クラウド利用者への情報転送のためのデータ規格、仕様等について事前に合意すること。

１３.２.４　秘密保持契約又は守秘義務契約

【管理策】

情報保護に対する組織の要件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し、文書化することが望ましい。

【クラウドサービスの提供において特に留意すべき課題との関係】

クラウドサービスは複数国の資源やサービスを利用してサービス提供を行うことがあるため、これらの資源やサービスを提供する他国の供給者に対して、サービス運用・技術等に係る情報を提供する場合には、秘密保持契約や守秘義務契約を締結する。しかし、知的財産に関する法制度の違いから秘密が保持されない、あるいは適用法や裁判管轄の違いから各種契約に基づく強制力が及ばない等の事態が生じうる。

【利用者接点とサプライチェーンにおける実務のポイント】

複数国の資源やサービスを利用してクラウドサービス提供する場合に、契約締結を行う他国の供給者との機密保持契約等の順守が確保されるために必要な対応策を講じる必要がある。具体的には、実務上以下を実施することが望ましい。

(a) 複数国の資源やサービスを利用してクラウドサービス提供する場合に、機密保持契約等の順守に必要となる、裁判管轄や適用法に関する規定、損害賠償の約定、担保措置等の措置が講じられていることを事前に確認した上で、他国の供給者との秘密保持契約、守秘義務契約の締結を行うこと。

１５.供給者関係

１５.１　供給者関係における情報セキュリティ

【目的】

供給者がアクセスできる組織の資産の保護を確実にするため。

【クラウドサービスの提供において特に留意すべき課題との関係】

クラウドサービスの一つの特徴として、複数の供給者が ICT サプライチェーンを構成してサービスを提供するケースが多いことが挙げられる。これにより、供給者は効率的に自らの資源を活用するための「選択と集中」が実施しやすくなり、

エンドユーザ（組織）においても、様々なサービスの比較を行いながら、柔軟な形でクラウドサービスを選択することができるようになる。

他方、供給者が複数に渡ることにより、供給者間でのサービス連携がうまくいかず、結果としてエンドユーザ（組織）へのサービス提供に支障をきたす恐れがある。例えば、供給者間の情報セキュリティマネジメントに対するポリシーの違いに起因した脆弱性の発生や、障害時における対応等に係る管理責任等の範囲についての認識の齟齬などに伴う対応の遅延等などを挙げることができる。

このように、クラウド事業者が複数にわたることに伴うポリシーの違い等から生じる実装面、運用面のリスクへの管理策が必要となる。

１５.１.１　供給者関係のための情報セキュリティの方針

【管理策】

組織の資産に対する供給者のアクセスに関連するリスクを軽減するための情報セキュリティ要求事項について、供給者と合意し、文書化することが望ましい。

【クラウドサービスの提供において特に留意すべき課題との関係】

クラウドサービスの提供を複数の供給者で行う場合に、提供するサービスおよびこれに関連する対応範囲を供給者間で明確にする必要がある。供給者間で対応範囲の認識に不一致があると、ガバナンスの喪失が生じ、これに伴う情報セキュリティ対応に未実施、あるいは不完全な部分が生じる。このため、クラウド利用者において不測の情報漏えいや障害等が発生し、あるいはアグリゲーションサービスにおいて、予期しないシステムの機密性、完全性、可用性の喪失が生じる恐れがある。

また、供給者間において、依拠するガバナンスに対する調整が行われない場合には、クラウドサービス全体として均一なガバナンスが確保されないことになり、これに伴う提供サービスの制限、不完全等が生じうるほか、不測のセキュリティホールや情報漏えい等の可能性が高まる。

クラウドサービスを連携して提供する場合に、いずれかのサービスの障害等に伴い、エンドユーザ（組織）が利用するサービス全体の完全性が損なわれたり、あるいは連携する他のサービスでも障害が誘発されるケースがある。この場合、供給者間で障害に対する対応方針の調整が事前に取れていない場合には、障害発生後の対応が円滑に行われないことにより、障害の影響範囲が拡大する恐れが高まることになる。

供給者間で、クラウドサービスにおける管理方針等についての調整が取れていない場合には、管理責任や管理権限の範囲が、本来の管理対象と整合しない事態が生じうる。そのため、例えば管理用インターフェイスの悪用や、管理機能の欠如などの事象が発生しうる。

クラウドサービス提供に関わる供給者の従事者に対するガバナンス等の方針について、供給者間で調整が取れていない場合には、サービス提供に係るモラルの均一化が図れないほか、従業者の業務対応の管理が不十分であることに伴う不正の発生等が生じ、これが他の供給者に対する不測のサービス提供上のリスクを生じさせる。

またクラウドサービスの提供に関して、一連のサービス提供状況、アクセス管理状況等の証跡については、各供給者

が自らのシステムに関するものは記録、管理しているものの、記録対象となる情報内容や取得方法が異なる可能性がある。また接続しているサービス間での証跡が、事前の方針等の取り決めがないために、全ての供給者において記録されない可能性がある。

【利用者接点とサプライチェーンにおける実務のポイント】

クラウドサービスを連携して提供するにあたっては、供給者間で情報セキュリティマネジメント措置を講じる範囲や対策に係る方針の調整を行い、明確にすることが求められる。サービス提供における資源、運用に関する基本的な方針についても明らかにすることで、サービス提供の継続性を維持し、あるいは不正な管理対応を未然に防止することが期待できる。そこで、実務上、以下のような対応を行うことが望ましい。

(a) ICT サプライチェーンを構成して提供されるクラウドサービスにおいて、情報セキュリティマネジメントに関する基本的な方針等に関し、各供給者が適用する情報セキュリティポリシー等を供給者間で調整し、適用範囲と内容を明確にすること。また ICT サプライチェーンを構成して提供されるクラウドサービスに必要な技術的仕様、サービスレベル、運用手順等について供給者間で調整し、明確にすること。

(b) ICT サプライチェーンを構成して提供されるクラウドサービスについて、サービス提供における情報セキュリティマネジメントの要求事項に係る責任の所在を、クラウド利用者に対して明確に示し、あるいは責任が分散している場合には、その旨を明示すること。

(c) 供給者以外が提供するサービスを、クラウド利用者がクラウドサービスと併せて利用する場合、クラウド利用者の管理責任や供給者の免責の範囲、運用方針等を明確にし、利用規約等を通じてクラウド利用者と合意すること。

(d) 供給者間で、証跡の記録・管理に関する方針等を取り決めるほか、供給者間でのサービス接続において生じる証跡の記録等の管理責任等の範囲を明確にし、これに基づいて必要な措置を講じること。

１５.１.３　ICT サプライチェーン

【管理策】

供給者との合意には、情報通信技術（以下、ICT という。）サービス及び製品のサプライチェーンに関連する情報セキュリティリスクに対処するための要求事項を含めることが望ましい。

【クラウドサービスの提供において特に留意すべき課題との関係】

ICT サプライチェーンを構成して提供されるクラウドサービスにおいて、一部の供給者が提供するサービスにおいて情報セキュリティ要求事項が満たされないことにより、ICT サプライチェーン全体のサービス継続性が損なわれ、あるいは不測のセキュリティホールが生じる等のリスクがある。

【利用者接点とサプライチェーンにおける実務のポイント】

ICT サプライチェーンを構成して提供されるクラウドサービスにおいて、一部の供給者が提供するサービスにおいて情報セキュリティ要求事項が満たされないことを防止するために、供給者間で、情報セキュリティマネジメントに関する要

求事項に係る合意を形成することが求められる。そこで、実務上以下を実施することが望ましい。

(a) ICT サプライチェーンを構成して提供されるクラウドサービスにおいて、サービス継続に必要な情報セキュリティ要求事項に関し、供給者間で合意を行うこと。

(b) ICT サプライチェーンを構成して提供されるクラウドサービスにおいて、供給者間でクラウドサービスの接続に関する情報セキュリティマネジメント上のリスクを明確にし、その管理策及び管理責任の内容・範囲や役割分担等を明らかにすること。

(c) 供給者以外が提供するサービスを、クラウド利用者がクラウドサービスと併せて利用する場合、供給者以外が提供するサービスに係る情報セキュリティマネジメント上の要求事項についての管理責任の範囲やクラウド事業者の免責の範囲を、利用規約等を通じてクラウド利用者と合意すること。

１５.２ 供給者のサービス提供の管理

【目的】

供給者との合意に沿って、情報セキュリティ及びサービス提供について合意したレベルを維持するため。

【クラウドサービスの提供において特に留意すべき課題との関係】

ICT サプライチェーンにおいては、15.1.3 により合意、又は明確になった情報セキュリティマネジメントの要求事項が一部の供給者により管理されないことで、クラウドサービス全体の提供品質や情報セキュリティに影響を及ぼす恐れがある。

１５.２.１　供給者のサービス提供の監視及びレビュー

【管理策】

組織は、供給者のサービス提供を定常的に監視し、レビューし、監査することが望ましい。

【クラウドサービスの提供において特に留意すべき課題との関係】

ICT サプライチェーンを構成して提供されるクラウドサービスにおいては、自社が提供するサービスの提供状況を監視するだけでは、自社が定めるサービスレベルを達成できないことがある。例えば他の供給者が提供するサービスにおいて情報セキュリティマネジメント上の脆弱性がある場合に、連携する自社のサービスへの影響が生じることも想定される。

特にアグリゲーションサービス事業者の場合には、他の供給者のサービス提供状況に起因する、クラウドサービス全体としてのサービスレベル低下に対する責任が生じるため、他の供給者全体のサービスに対する管理が求められる。

【利用者接点とサプライチェーンにおける実務のポイント】

ICT サプライチェーンを構成して提供されるクラウドサービスにおいては、他の供給者と連携する事項に関して、情報セキュリティマネジメントにおける脆弱性を監視・レビューするとともに、他の供給者において脆弱性が生じた場合でも、

自社が提供するサービスが被る影響を最小限に抑える措置を講じることが求められる。

またアグリゲーションサービスの場合には、クラウドサービス提供に影響を及ぼす他の供給者のサービスレベル低下を未然に防止し、あるいは円滑なサービス回復を実現するため、ICT サプライチェーンの全ての供給者のサービス提供状況を監視することが求められる。

これらの対応を図るために、実務上、以下を実施することが望ましい。

(a) ICT サプライチェーンを構成して提供されるクラウドサービスにおいて、各供給者は供給者間の合意に基づいて、自らのサービスに関する情報セキュリティマネジメントに係る要求事項の実施状況を管理し、必要なレビューを行うこと。
(b) ICT サプライチェーンを構成して提供されるクラウドサービスにおいて、各供給者は、他社のサービスと連携する事項（データ、インターフェース等）について、情報セキュリティマネジメントに係る脆弱性を監視・レビューするとともに、他の供給者において脆弱性が生じた場合でも、自社が提供するサービスが被る影響を最小限とする措置を講じること。
(c) アグリゲーションサービス事業者は、提供するクラウドサービス全体についての監視、レビュー、監査実施に対する責任を果たすこと。

１５.２.２　供給者のサービス提供の変更に対する管理

【管理策】

関連する業務情報、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、供給者によるサービス提供の変更（現行の情報セキュリティの方針群、手順及び管理策の保守及び改善を含む。）を管理することが望ましい。

【クラウドサービスの提供において特に留意すべき課題との関係】

ICT サプライチェーンを構成して提供されるクラウドサービスにおいては、一部の供給者が提供するサービスの変更が、他の供給者のサービスや、クラウドサービス全体に影響を及ぼす恐れがある。これに伴い、不測の原因によって、クラウドサービス上の障害や情報漏えいを生じる可能性が生じる。

【利用者接点とサプライチェーンにおける実務のポイント】

ICT サプライチェーンを構成して提供されるクラウドサービスでは、自社のサービスの変更に起因して、他の供給者が提供するサービスに不測の障害等が生じないようにするための管理策を取ることが求められる。

特にアグリゲーションサービス事業者においては、一部の供給者におけるサービスの変更が、クラウドサービス全体に影響を生じさせないように管理する責任があるため、その管理策が求められる。このため、実務上以下を実施することが望ましい。

(a) ICT サプライチェーンを構成して提供されるクラウドサービスにおいては、自社が提供するサービスの変更に伴う影響範囲等について事前に把握し、他の供給者に対して必要な情報を提供し、必要に応じて対応策を講じ

ること。

(b) アグリゲーションサービス事業者は、一部のクラウド事業者が行う変更に関する管理を行い、クラウドサービス全体として変更に伴う影響を最小限にするための対応策を講じること。

１６.情報セキュリティインシデント管理

１６.１ 情報セキュリティインシデントの管理及びその改善

【目的】

セキュリティ事象及びセキュリティ弱点に関する伝達を含む、情報セキュリティインシデントの管理のための、一貫性のある効果的な取組みを確実にするため。

【クラウドサービスの提供において特に留意すべき課題との関係】

情報セキュリティインシデントに関し、特に留意すべき課題は以下に示すように数多く存在している。

(a) 供給者関係におけるそれぞれの事業者における不明確な管理責任等の範囲
(b) 仮想化に伴うネットワーク管理とサーバ管理の管理責任の範囲の不明確化（仮想スイッチ等）
(c) (a)(b)等に起因する情報セキュリティ事象の発見の遅れや対応切り分けの失敗
(d) 発見された情報セキュリティ事象の通報受付体制の不備による対応の起動の遅れ
(e) 深刻な情報セキュリティインシデントをそうでないと誤判断したことによる、対応やクラウドサービス利用者等への初報の遅れ
(f) 資源やインフラの集約による情報セキュリティインシデントの影響範囲の拡大
(g) (a)(b)等に起因する不十分な対応による情報セキュリティインシデントの影響範囲の拡大
(h) SLA を守れないことや、クラウド利用者が納得する状況報告ができないことによるクラウド事業者、又はクラウドサービスに対する信用の失墜
(i) 監督官庁が定める業法、知的財産権や個人情報の保護等の法令を守れないことによるクラウド事業者、又はクラウドサービスに対する信用の失墜
(j) クラウド利用者やクラウド事業者間のコミュニケーション不足による状況認識の食い違いや紛争の発生
(k) クラウド利用者に捜査が及んだ場合の記録媒体や共有資源（RAM、ネットワーク等）のテナント分離の限界に伴う情報漏えい
(l) 複数の司法権を跨がるデータ格納に伴うデータの押収・漏えいやサービス停止の発生

情報セキュリティインシデントの兆候を早期に把握し、明確な管理責任や役割の範囲の分担に基づいて対応を的確に切り分け、深刻な情報セキュリティインシデントを判別して円滑に対応（クラウドサービス利用者等への初報を含む）を起動し、影響範囲を限定し、クラウド利用者と合意した SLA や報告義務を順守し、法令を順守し、他の供給者と状況認識を共有し、クラウド利用者の不正行為に対する証拠を情報漏えいを生じることなく収集し、司法権管轄の違いに対応する。こういった一連の情報セキュリティインシデント対応において、一貫性のある効果的な取組みを行うことが求められる。

１６.１.２　　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、できるだけ速やかに報告することが望ましい。

【クラウドサービスの提供において特に留意すべき課題との関係】

仮想化によるネットワーク管理に対する管理責任等の内容や範囲の不明確化、供給者間における管理責任等の範囲に関する理解の齟齬等に起因して、情報セキュリティ事象の発見や対応切り分けに支障が出やすいため、これを克服するための技術的対策及び供給者間の管理責任等の分担範囲の明確化が求められる。

以上の環境整備を前提とし、その上で、内部組織に限らず、クラウド利用者やICTサプライチェーンを構成する他の供給者等が先に情報セキュリティ事象を発見した場合であっても、情報セキュリティ事象の情報を早期に集約できる体制を構築することが求められる。

【利用者接点とサプライチェーンにおける実務のポイント】

資産管理の責任をもれなく個人に割当、これらの責任者に対し、報告すべき情報セキュリティ事象の内容、その明確な連絡先（時機を失しない対応ができることが望ましい。）並びに可能な限り速やかな報告の実施を徹底する。ここで、報告すべき情報セキュリティ事象の内容には、効果のないセキュリティ管理策、情報の完全性・機密性・可用性に関する期待に対する違反、人的ミス、個別方針又は指針の不順守、物理的セキュリティの取決めに対する違反、管理されていないシステム変更、ソフトウェア又はハードウェアの誤動作、アクセス違反が含まれる（ISO/IEC 27002:2013 16.1.2 実施の手引 a）-h)参照）。

また、情報セキュリティ事象の報告書式を定め、事象の発見者は、この書式に従って重要事項を詳細に記録し、直ちに予め定められた連絡先に報告することが望ましい。

さらに、クラウドサービスの提供にあたっては、実務上以下を実施することが望ましい。

(a) 6.3.1 の管理策により、ガバナンスの実態が異なる供給者間で、クラウドサービス提供におけるそれぞれの供給者の管理責任等の範囲を明確に設定すること。
(b) クラウド利用者や ICT サプライチェーンを構成する他の供給者等に対しても、クラウドサービスにおける情報セキュリティ事象の速やかな報告手順とその連絡先を認識させておくこと。
(c) クラウドサービスにおける情報セキュリティ事象を、クラウド利用者から受け付ける窓口を設置して周知し、情報セキュリティ事象に係る速やかな情報集約に努めること。
(d) ICT サプライチェーンの中で、情報セキュリティ事象の連絡を伝播させる連絡経路を、管理責任の分担と一体で明確にし、訓練によって正しく連絡を伝播できることを確認すること

クラウドサービスの提供にあたり、複数の供給者による提供サービス間に依存関係がある ICT サプライチェーンが構

築されている場合には、その契約形態に注意する。個別契約連携クラウドサービスの形態である場合は、クラウド利用者からの情報セキュリティ事象の報告は、緊急時における役割分担等が曖昧となっている場合には、適切な供給者に報告されない事態が生じる。これに対処するため、ICT サプライチェーンを構成する供給者間での情報共有の仕組みを強化する、クラウド利用者に対する窓口を一本化する等の対策を行うことが望ましい。

１６.１.４　情報セキュリティ事象の評価及び決定

【管理策】

情報セキュリティ事象は、これを評価し、情報セキュリティインシデントに分類するか否かを決定することが望ましい。

【クラウドサービスの提供において特に留意すべき課題との関係】

発生した情報セキュリティ事象を、情報セキュリティインシデントに分類することで、対応を本格化させ、クラウド利用者への連絡も起動させる。従って、判断ミスを抑え、対応や連絡の速やかな実施を確保するため、情報セキュリティインシデントの分類基準を確立することが求められる。

【利用者接点とサプライチェーンにおける実務のポイント】

クラウドサービスの提供にあたっては、実務上以下を実施することが望ましい。

(a) クラウドサービス提供における重大な情報セキュリティインシデントの明確な分類基準を定め、この基準を用いて情報セキュリティ事象を評価し、その事象を情報セキュリティインシデントに分類するかを決定すること。

(b) 情報セキュリティインシデントへの分類の判断において、クラウド利用者との間で認識の違いが生じると、情報提供に不満を感じる等の理由から、情報セキュリティインシデント対応に係るクラウド利用者からの信頼感を阻害する恐れがあるため、分類基準を明確に定めることに加えて、必要に応じてクラウド利用者と SLA を締結すること。

(c) 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て監視できるようにする仕組みを備えること。また、この仕組みを活用し、情報セキュリティインシデントの分類基準の妥当性をレビューし、必要に応じて改善を加えること。

(d) 情報セキュリティインシデントの事実関係、復旧/回復措置、復旧見込、影響範囲等の情報を、クラウド利用者に提示すること。情報提供の方法については、6.3.2【利用者接点とサプライチェーンにおける実務のポイント】(h)に基づくこととし、情報提供のタイミングは、随時または一定間隔とすること。また、この方針に従って、必要に応じてクラウド利用者と SLA を締結すること。

１６.１.７　証拠の収集

【管理策】

組織は、証拠となり得る情報の特定、収集、取得及び保存のための手順を定め、適用することが望ましい。

【クラウドサービスの提供において特に留意すべき課題との関係】

情報セキュリティインシデントの事後対応において、以下に示すような場合は、懲戒処置及び法的処置のための証拠収集・保全が必要になる。

(a) クラウド事業者自身の法順守を争う場合
(b) 内部組織や委託先の要員の不正を問う場合
(c) クラウド利用者の順法が問われ証拠がクラウドサービス上に存在する場合　等

このような場合には、以下に示す不都合な事象への対応が課題となる。

(d) 訴訟への発展を予見できず証拠を破壊してしまう事象
(e) 証拠の収集と保全に係る知識不足のため裁判で証拠として採用されない事象
(f) 共用された媒体・資源からの証拠の収集・保全プロセスにおける無関係な他のクラウド利用者の記録の破損や情報の漏えいの発生
(g) 複数の司法権を跨るデータ格納に伴うデータの押収・漏えいやクラウドサービスの停止　等

これらの不都合な事象に対応するため、証拠となり得る情報の特定、収集、取得及び保存のための手順を定め、適用することが求められる。クラウド利用者による、証拠として利用できる情報へのアクセス手順（要請・許諾・課金等）を確立することもこれに含まれる。

クラウド事業者自身の法順守を争う場合には、知的財産権や個人情報の保護等が論点となる場合が多いが、クラウド利用者の順法が問われ証拠がクラウドサービス上に存在する場合は、監督官庁が定める業法を始めとして、不正アクセス防止法、各種刑法等、多様な法制度が対象になる。

【利用者接点とサプライチェーンにおける実務のポイント】

懲戒措置及び法的処置のために証拠を取り扱う場合は、組織内部の手順を定めてこれに従うことが望ましい。

まず、証拠として利用できる情報は特定し、文書化しておく。証拠として利用できる情報は、紙文書として得られる情報、仮想マシンから得られる情報、ネットワークから得られる情報、SIEM から得られる情報、IPS から得られる情報等に分類される。

証拠となる情報の取り扱いはその種別（紙文書、コンピュータ媒体上の情報）により異なるため、それぞれについてフォレンジック（収集・保存・保全）の手順（保存期間も含む）を定めておくことが望ましい。特に、コンピュータ媒体上の情報を取り扱う場合は、フォレンジックの知識に基づく専門性の高い手順を適用する必要があるため、その事象が訴訟に発展するかどうか判然としない場合は、早めに弁護士、警察、フォレンジックの専門家等に相談し、助言を求めることが望ましい。また、可能であれば、フォレンジック情報が供給されるインターフェイスと API を把握しておき、コンピテ

ンシーが高い人物からフォレンジック実務の支援を受けることが望ましい。

さらに、クラウドサービスの提供にあたっては、以下に示す技術の実装を検討するとともに、実務上以下を実施することが望ましい。

(a) 可能であれば、複数のクラウド利用者で共用された媒体・資源へのフォレンジック調査中に、証拠の収集・保存・保全に無関係な他のクラウド利用者の記録の破損等の二次的な資産の損害を防止できる技術を適用すること。
(b) 可能であれば、複数のクラウド利用者で共用された媒体・資源へのフォレンジック調査中に、証拠の収集・保存・保全に無関係な他のクラウド利用者の機微情報を保護できる技術を適用すること。
(c) クラウド利用者が行う証拠収集の制限事項について定義し、クラウド利用者と合意すること。
(d) クラウド利用者が、証拠として利用できる情報へのアクセスを要請し、その許諾を得るための手順をクラウド利用者と合意すること。このアクセスに費用や料金が発生する場合は、それを文書化してクラウド利用者に示すこと。
(e) クラウドサービスにおいて、司法権を跨るデータ格納を行う場合は、各国の法制度を考慮するとともに、その情報をクラウド利用者にも提供し、この情報に基づいてクラウド利用者が自らデータ格納を行う国等を選択できる仕組みを提供すること。

１７.事業継続マネジメントにおける情報セキュリティの側面

１７.２　冗長性

【目的】

情報処理施設の可用性を確実にするため。

【クラウドサービスの提供において特に留意すべき課題との関係】

多数のクラウド利用者がクラウドサービスを利用しているため、クラウドサービスの停止は大規模かつ広範囲に影響を及ぼす。このため、サービス停止の影響は、単に可用性の低下に伴う SLA 違反による利用料の返還に留まらず、当該サービスやその提供元であるクラウド事業者の社会的信頼を失墜させる事態に陥る可能性も存在している。このため、クラウドサービス提供のための情報処理施設の可用性確保は、最優先事項として取り組むことが求められる。

１７.２.１　　情報処理施設の可用性

【管理策】

情報処理施設は、可用性の要求事項を満たすのに十分な冗長性をもって、導入することが望ましい。

【クラウドサービスの提供において特に留意すべき課題との関係】

クラウドサービスに、仮想化機能やサービス機能以外に ID 管理サービス等の単一障害点が存在していると、その機

能が停止することにより、サービス全体が停止してしまう恐れがある。このため、クラウドサービス提供のための情報処理施設の単一障害点を特定し、確実に冗長化を実施することが求められる。

【利用者接点とサプライチェーンにおける実務のポイント】

情報処理施設の可用性を保証するためには、情報処理施設の十分な冗長性を確保した上で、障害時には運用系から冗長系への切替を確実に行うことが求められる。運用系から冗長系への切替を確実にするためには、切替が意図通りに動作することを定期的に確認することが望ましい。

さらに、クラウドサービスの提供にあたっては、実務上以下を実施することが望ましい。

(a) ID 管理サービス、課金サービスなどの基幹機能において、単一障害点となっているものを特定し、十分な冗長性と障害時の円滑な切替を確保すること。
(b) 仮想化機能やサービス管理機能において、単一障害点となっている機能を特定し、十分な冗長化、障害時の円滑な切替、情報処理施設の管理単位分割等の対策を講じること。
(c) 情報処理施設やネットワークにおいて、単一障害点となっている設備を特定し、十分な冗長性と障害時の円滑な切替を確保すること。
(d) 障害の連鎖を食い止める防護機構を組み込むこと。
(e) クラウドサービスを広域災害から防護するため、データセンタを地理的に離れた複数の地域に設置することにより、(a)～(c)の対策を補完すること。
(f) 広域災害の発生に際しては、クラウドサービスの継続を優先するか、情報セキュリティ対策の確保を優先するかについての方針を定め、クラウド利用者と合意すること。

１８.順守

１８.１　法的及び契約上の要求事項の順守

【目的】

情報セキュリティに関連する法的、規制又は契約上の義務に対する違反、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。

【クラウドサービスの提供において特に留意すべき課題との関係】

クラウドサービスにおいては、越境サービスを行うことにより、サービス対象となる国が複数にわたるケースがあり、これに伴い複数の国による法規制が適用されることにより、サービス提供の完全性が損なわれ、あるいは不測の対応を求められる恐れがある。

また他国の供給者が提供するサービスと連携してクラウドサービスを提供する場合には、契約に係る紛争に対する適用法が異なることで、クラウドサービス提供の継続が困難となる恐れがある。

１８.１.１　　適用法令及び契約上の要求事項の特定

【管理策】

各情報システム及び組織について、全ての関連する法令、規制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を、明確に特定し、文書化し、また、最新に保つことが望ましい。

【クラウドサービスの提供において特に留意すべき課題との関係】

複数国のクラウド利用者に対してクラウドサービスを提供をする場合には、それぞれの国における適用法や司法権の管轄などが異なるため、クラウド利用者においてクラウドサービスの利用が継続できないリスクが生じる。また、複数の国等に存在する資源を用いてクラウドサービスを提供する場合には、当該資源が存在する国の法令等が適用され、差押えが行われる等により、クラウドサービスの提供ができない状態に陥る恐れがある。

またICTサプライチェーンを構成して提供されるクラウドサービスにおいて、他の供給者が国外事業者である場合に、適用法令の違いから不測の捜査を受けるなどにより、サービス提供の継続が困難になる恐れがある。

【利用者接点とサプライチェーンにおける実務のポイント】

クラウドサービスにおいては、特に国際間でサービス提供される場合に、適用される法令が国によって異なることによって、サービス提供の継続や、クラウド利用者のサービス利用の継続が困難になることがある。このため、実務上以下を実施することが望ましい。

(a) 複数国のクラウド利用者に対してサービス提供を行う、又は複数国の資源やサービスを利用してサービス提供を行うクラウド事業者は、サービス対象や利用資源が越境することによってクラウドサービスに生じうる、適用法の違いによるリスクを事前に把握すること。
(b) 複数国の資源やサービスを利用してサービス提供を行うクラウド事業者は、当該資源やサービスが存在する国において適用される法等に係るリスクに対して、サービス提供上必要な措置を講じること。

なお、適用法令及び契約上の要求事項の特定という観点では、利用規約やSLA等における一般的な契約上の要求事項に加えて、クラウド利用者から預託された情報の契約終了時の取扱いに係る要求事項等も考慮する必要がある。これらについては、総務省、経済産業省等からITアウトソーシングやSLA等に係るガイドラインが公表されているので、こちらを参照されたい。

１８.１.２　　知的財産権

【管理策】

知的財産権及び権利関係のあるソフトウェア製品の利用に関連する、法令、規制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実施することが望ましい。

【クラウドサービスの提供において特に留意すべき課題との関係】

複数国のクラウド利用者に対してクラウドサービスを提供する場合に、適用される知的財産法が異なることにより、クラウド利用者が不測の損害を被る恐れがある。具体的には、著作権法の適用の違いに伴う保護範囲の違いや、営業秘密等の取り扱いの違い等に基づくリスクが存在する。

また情報サービスの提供に供するライセンスを複数国の資源において利用している場合には、ライセンスの範囲やサポート等の契約内容に差異が生じる恐れがある。

【利用者接点とサプライチェーンにおける実務のポイント】

複数国のクラウド利用者に対してクラウドサービスを提供する場合や、複数国の資源やサービスを利用してクラウドサービスを提供する場合に生じうる、知的財産法の違いに伴うリスクを明確にし、必要な措置を講じることが求められる。また情報サービス利用に供するライセンスの範囲についての紛争に伴うサービス停止等が生じないようにするための管理が求められる。このため、実務上以下を実施することが望ましい。

(a) 複数国のクラウド利用者に対してサービス提供するクラウド事業者は、クラウドサービス利用において供するクラウド利用者の知的財産情報の権利に対し、国による知的財産保護法上の保護範囲の違いに起因して生じうるリスクを明らかにすること。
(b) 複数国のクラウド利用者に対してサービス提供するクラウド事業者は、クラウドサービスの提供にあたって利用する知的財産権の取り扱いについて、複数国でサービス提供することによって生じるリスクを把握し、必要な対策を講じること。

１８.１.３　　記録の保護

【管理策】

記録は、法令、規制、契約及び業務上の要求事項に従って、消失、破壊、改ざん、認可されていないアクセス及び不正な流出から保護することが望ましい。

【クラウドサービスの提供において特に留意すべき課題との関係】

クラウドサービスにおいて、サービス提供に供する資源やサービスが他国にある場合には、我が国とは異なる法令を適用した司法権の行使等が行われ、あるいは不測の差押え等が生じることで、クラウドサービスの提供が停止するほか、クラウド利用者から預託された情報やサーバ上の記録が流出し、あるいは回復不能となる恐れがある。

【利用者接点とサプライチェーンにおける実務のポイント】

他国の資源やサービスを利用してクラウドサービスの提供を行うクラウド事業者は、他国の司法権の行使等に伴う資源等の差押えや、これに伴う必要な記録や情報の流出により、クラウドサービスの提供を停止せざるをえなくなる恐れがある。そこで、実務上、以下の対応策を実施することが望ましい。

(a) 他国の資源やサービスを利用してクラウドサービスを提供するクラウド事業者は、他国の司法権の行使等に伴うサービス停止や資源等の流出に係るリスクを事前に確認し、必要な措置を講じること。

１８.１.４　　プライバシー及び個人を特定できる情報（PII）の保護

【管理策】

プライバシー及び PII の保護は、関連する法令及び規制が適用される場合には、その要求に従って確実にすることが望ましい。

【クラウドサービスの提供において特に留意すべき課題との関係】

複数国のクラウド利用者に対してクラウドサービスを提供する場合や、複数国の資源やサービスを利用してクラウドサービスを提供する場合に、クラウドサービスに供される個人情報保護法制が国や地域によって異なることから生じるリスクが存在しており、これに対する管理策が求められる。

【利用者接点とサプライチェーンにおける実務のポイント】

複数国のクラウド利用者に対してクラウドサービスを提供する場合や、複数国の資源やサービスを利用してクラウドサービスを提供する場合に、複数の国や地域における個人情報保護法制の違いなどに基づく、情報セキュリティマネジメントに関する要求事項の違いに対応する管理策を講じる必要がある。そこで、実務上、以下の対応策を実施することが望ましい。

(a) 複数国のクラウド利用者に対してクラウドサービスを提供するクラウド事業者、あるいは複数国の資源・サービス等を利用するクラウド事業者は、クラウド利用者の資源が存在する各国の法制に基づく個人情報保護に必要な取り扱いについて事前に把握し、必要な対策を講じること。

１８.１.５　　暗号化機能に対する規制

【管理策】

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

【クラウドサービスの提供において特に留意すべき課題との関係】

提供するクラウドサービスにおいて、サービスに供される情報等に対して、情報セキュリティマネジメントの観点から暗号化措置を講じることがある。しかし複数国のクラウド利用者に対してサービスを提供する場合や、複数国の資源やサービスを利用してサービスを提供する場合に、国によっては公的秩序等の観点から、暗号化通信等を禁止しているケースがあり、クラウドサービス提供における情報セキュリティマネジメント上の要求事項が満たされない恐れがある。逆にある国において法令上の要請から暗号化措置が求められている場合は、これを達成できない事態に陥る可能性がある。

【利用者接点とサプライチェーンにおける実務のポイント】

複数国のクラウド利用者に対してクラウドサービスを提供する場合や、複数国の資源やサービスを利用してクラウドサービスを提供する場合、複数の国や地域における暗号化措置に対する規制等の違いに基づく、情報セキュリティマネジメントに係る要求事項の違いに対応する管理策を行う必要がある。そこで、実務上、以下の対応策を実施することが望ましい。

(a) 複数国のクラウド利用者に対してクラウドサービスを提供するクラウド事業者、あるいは他国の資源、サービス等を利用するクラウド事業者は、クラウド利用者や資源が存在する各国における暗号利用に係る法律上の必要性、あるいは制約等について把握し、クラウドサービスの提供に際しての必要な対策を講じること。

１８.２ 情報セキュリティのレビュー

【目的】

組織の方針及び手順に従って情報セキュリティが実施され、運用されることを確実にするため。

【クラウドサービスの提供において特に留意すべき課題との関係】

ICT サプライチェーンを構成して提供されるクラウドサービスにおいては、自社が提供するサービス等に関する情報セキュリティマネジメントのレビューを実施するだけでは、目標とするサービスレベルを確保する方策としては不十分であり、ICT サプライチェーンを構成する他の供給者との関係でもレビューを実施することが求められる。

１８.２.１　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管理（例えば、情報セキュリティの管理目的、管理策、方針、プロセス、手順）に対する組織の取組みについて、あらかじめ定めた間隔で、又は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。

【クラウドサービスの提供において特に留意すべき課題との関係】

ICT サプライチェーンを構成して提供されるクラウドサービスにおいては、クラウド事業者が提供するサービスが他の供給者が提供するサービス等に依存し、あるいは影響を受ける部分を有することがある。このため自社が提供するサービスの範囲のみについて独立したレビュー・監査等を行うだけでは、自社のサービスを提供する上での管理として不十分となりうる。

また、アグリゲーションサービス事業者は、クラウドサービス全体に対する管理責任を有するが、供給者間でレビュー・監査における方針に齟齬がある場合には、クラウドサービス全体として必要なレビュー・監査が行えない恐れがある。

【利用者接点とサプライチェーンにおける実務のポイント】

ICT サプライチェーンを構成して提供されるクラウドサービスにおいて、クラウド事業者が提供するサービスが他の供給者が提供するサービス等に依存し、あるいは影響を受ける部分を有する場合には、他の供給者が提供するサービスに

おける情報セキュリティマネジメント上の課題等を監視できる対応策を講じることが求められる。またアグリゲーションサービス事業者は、クラウドサービス全体に対する管理責任を果たすのに必要なレビュー・監査等を実施できる対応策を講じることが求められる。そこで、実務上以下の対応策を実施することが望ましい。

(a) ICT サプライチェーンを構成して提供されるクラウドサービスにおいて、提供するサービスが他の供給者が提供するサービス等に依存し、あるいは影響を受ける部分を有する場合には、他の供給者が行う独立したレビュー・監査結果等を入手し、その結果を自社が行う独立したレビュー・監査に反映させる等の措置を講じること。

(b) アグリゲーションサービス事業者は、他の供給者が行う独立したレビュー・監査の実施方針について把握し、必要な調整を行うことで、ICT サプライチェーン全体においてレビュー・監査等に係る一貫した方針の適用が必要な範囲を明確にし、これを適用するための措置を講じること。

１８.２.２　情報セキュリティのための方針群及び標準の順守

【管理策】

権利者は、自分の責任の範囲内における情報処理及び手順が、適切な情報セキュリティのための方針群、標準類、及び他の全てのセキュリティ要求事項を順守していることを定期的にレビューすることが望ましい。

【クラウドサービスの提供において特に留意すべき課題との関係】

アグリゲーションサービス事業者は、サービス全体に対する管理責任を有するが、順守している情報セキュリティマネジメントのための方針群、標準類等が供給者間で一貫しておらず、結果としてクラウドサービス全体として適切な順守が確保されない恐れがある。

【利用者接点とサプライチェーンにおける実務のポイント】

アグリゲーションサービス事業者は、サービス全体に対する管理責任を果たすために、クラウドサービス全体として適切な情報セキュリティマネジメントのための方針群、標準類等が順守されているかを定期的にレビューすることが求められる。このため、実務上以下を実施することが望ましい。

(a) アグリゲーションサービス事業者は、他の供給者が行う情報セキュリティマネジメントのための方針群、標準類等の順守に係る定期的なレビュー結果を入手し、必要な調整を行うことで、ICT サプライチェーン全体において一貫した定期的レビューを行う範囲を明確にし、各供給者にこれを実施させるための措置を講じること。

１８.２.３　技術的順守のレビュー

【管理策】

情報システムを、組織の情報セキュリティのための方針群及び標準の順守に関して、定めに従ってレビューすることが望ましい。

【クラウドサービスの提供において特に留意すべき課題との関係】

ICT サプライチェーンを構成して提供されるクラウドサービスにおいて、提供するサービスが他の供給者が提供するサービス等に依存し、あるいは影響を受ける部分を有する場合には、他の供給者のサービス等に係る技術的な順守状況を監視することが求められるが、各供給者の機密であることを理由としてレビュー結果が提供されず、十分なレビュー等ができない恐れがある。

【利用者接点とサプライチェーンにおける実務のポイント】

ICT サプライチェーンを構成して提供されるクラウドサービスにおいて、他の供給者のサービス等に係る技術的な順守状況のレビュー結果等を入手する際に、十分な情報等の提供を受けるための措置を講じる必要がある。そこで、実務上以下を実施することが望ましい。

(a) ICT サプライチェーンを構成して提供されるクラウドサービスにおいては、他の供給者のサービス等に係る技術的な順守状況のレビュー結果等を入手する際に、機密的な内容が含まれる場合には、機密保持契約の締結等、必要な措置を講じること。