ＩＳＭＳユーザーズガイド
追 補
～クラウドを含む新たなリスクへの対応～

ISMS: Information Security Management System
情報セキュリティマネジメントシステム

平成 30 年 3 月 30 日
情報マネジメントシステム認定センター（ISMS-AC）

目　次

０．序文

0.1 本追補の位置づけ

本追補は、クラウドサービスを提供又は利用する組織が情報セキュリティマネジメントシステム（ISMS）を構築・運用する際の参考として、JIS Q 27017 の概要及び ISMS クラウドセキュリティ認証の要求事項について解説するものです。

ISMS クラウドセキュリティ認証とは、JIS Q 27001 をベースとした従来の ISMS 認証を前提として、その適用範囲内に含まれるクラウドサービスの提供もしくは利用に関して、クラウドサービスに関するガイドラインである JIS Q 27017 に規定されるクラウドサービス固有の管理策が実施されていることを認証する仕組みです。つまり、「ISO/IEC 27017:2015 に基づく ISMS クラウドセキュリティ認証に関する要求事項（JIP-ISMS517）」に従って、ISMS 適合性評価制度※のもとで実施される認証です。
なお、「ISO/IEC 27017 認証」とある場合は、この JIP-ISMS517 に従った「ISMS クラウドセキュリティ認証」以外の認証も含まれますので、ご留意ください。

ISMS クラウドセキュリティ認証は JIS Q 27001 認証（ISMS 認証）の拡張であることから、本追補も ISMS ユーザーズガイド（JIP-ISMS111-3.0）の拡張版として作成しました。このため、ISMS ユーザーズガイドを前提とした記載になっておりますので、ISMS ユーザーズガイドと併せてお読みいただければと思います。

クラウドサービスのための情報セキュリティに関して、特に留意が必要なのは、効果的なリスク対策のためには、単に既存の ISMS にクラウドサービス固有の管理策を追加することではなく、クラウドというサービスについて品質や運用上の課題といったことも考慮して、クラウドサービス全体に対するリスクを ISMS に組み込み対応するということです。本追補では、このような視点から、クラウドのリスクへの対応についても解説します。

※ ISMS 適合性評価制度とは、認定機関（情報マネジメントシステム認定センター(略称：ISMS-AC)）によって認定された認証機関が組織の ISMS を審査・認証する、国際的な枠組みのことです。

0.2 ISO/IEC 27017 発行の経緯（日本提案の国際規格）

クラウドサービスは 2010 年頃より急速に普及が進み、近年では利便性やコストメリットなどから多くの企業が利用するようになってきました。一方で、クラウドコンピューティング環境におけるサーバ内のデータ消失や意図しない者とのデータ共有等の事例が発生するようになり、クラウドサービス利用における情報セキュリティの不安も高まっています。

そうした中、2011 年に JIS Q 27002（情報セキュリティ管理策の実践のための規範）と整合性をとった「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」が経済産業省から公表されました（その後 2014 年に改訂）。同ガイドラインを元に日本からクラウドサービスにおける情報セキュリティのガイドラインを ISO（国際標準化機構）と IEC（国際電気標準会議）との合同専門委員会 JTC 1 へ提案した結果、国際標準化が決定し 2015 年 12 月に ISO/IEC 27017:2015（情報技術－セ

キュリティ技術－ISO/IEC 27002 に基づくクラウドサービスのための情報セキュリティ管理策の実践の規範）が発行され、これに一致する JIS Q 27017 も、1 年後の 2016 年 12 月に発行されました。

0.3 JIS Q 27017 と JIS Q 27001、JIS Q 27002

JIS Q 27001 は、情報セキュリティのマネジメントシステムについて規定した本文と、具体的な対策（管理策）集である附属書 A から構成されています。特に、附属書 A については、詳細なガイドラインである JIS Q 27002 が発行されており、JIS Q 27017 は上述の通り、この JIS Q 27002 に基づいています。

JIS Q 27001 の要求事項に基づく ISMS において、JIS Q 27002 は情報セキュリティ管理策を実施するための汎用的なガイドであり、JIS Q 27017 はクラウドサービスを対象とした追加のガイドという位置づけです。

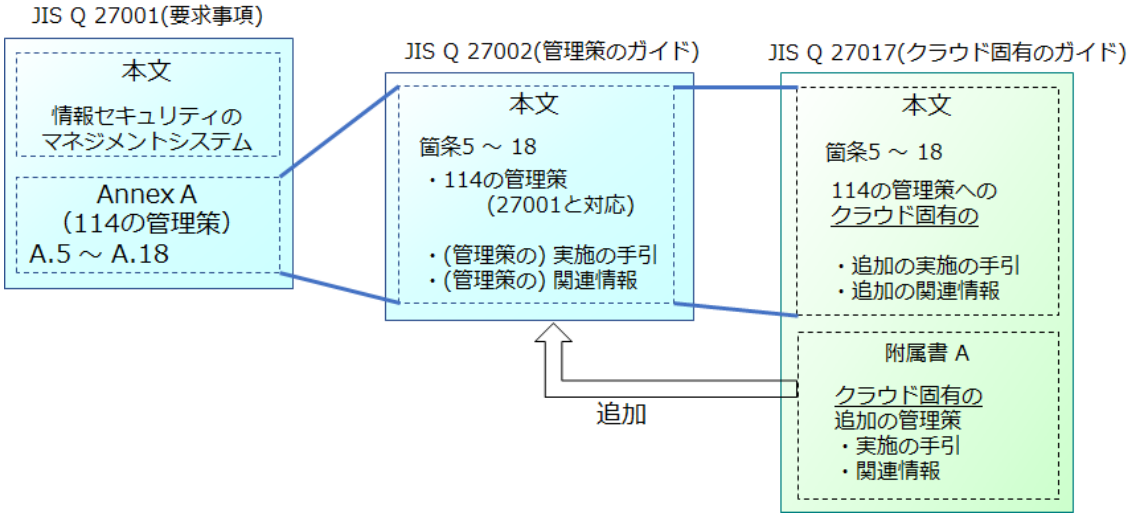


図 0-1 JIS Q 27017 の位置づけ

つまり、図 0-1 で示す通り、JIS Q 27017 は、JIS Q 27001 に基づく ISMS を実施する際に、クラウドサービスに関するガイドラインを提供するものであり、ISMS を実施する中で適用されます。
重要なことは、JIS Q 27017 の個々の対策を単に実施することではなく、クラウドサービス固有のリスクを組織の ISMS に組み込み、リスクマネジメントを実施していくことです。その際、ISMS を運用する活動のなかでリスクアセスメント、リスク対応を実施し、JIS Q 27017 を確認することが必要になります。

0.4 ISMS クラウドセキュリティ認証

情報マネジメントシステム認定センター（略称：ISMS-AC）では、クラウドサービスに対する情報セキュリティ認証を求める声を受けて、2016 年 8 月に、ISMS 適合性評価制度の下で、ISO/IEC 27017（JIS Q 27017）に基づく ISMS クラウドセキュリティ認証の認定業務を開始しました。
本認証の開始にあたって、JIS Q 27017 がガイドラインであり、認証のための要求事項ではないことから、JIS Q 27017 を ISMS（JIS Q 27001）に組み込むための認証基準として、「ISO/IEC

27017:2015 に基づく ISMS クラウドセキュリティ認証に関する要求事項（JIP-ISMS517）」を策定しました。
JIP-ISMS517 では、ISMS クラウドセキュリティ認証の適用範囲や、クラウドサービスに関するリスクアセスメント、リスク対応などを組織が満たすべき要求事項として明記しており、特に ISO/IEC 27017 に記載の管理策をリスク対応に盛り込むことを明確に要求しています（詳細は、「３．ISMS クラウドセキュリティ認証について」を参照してください）。
そのため、要求事項である JIP-ISMS517 に沿って JIS Q 27001 に JIS Q 27017 の管理策を採り入れることによって、客観的で外部者からもわかりやすいクラウドサービスに特化したマネジメントを組み込んだ ISMS を実施することが可能になります。また、企業に対して説明責任が求められている昨今、ISMS 適合性評価制度のもとで実施される ISMS クラウドセキュリティ認証は、社会にクラウドセキュリティへの取組みを表明する一つの手段として活用することができます。

0.5 27000 ファミリーの他のセクター規格

27000 ファミリーには、JIS Q 27017 の他、JIS Q 27011（電気通信業界対象）、ISO/IEC 27799（保険医療業界対象）などのセクター規格がありますが、これらの規格も構成としては JIS Q 27017 と同じく JIS Q 27002 と整合しており、マネジメントシステム部分については JIS Q 27001 の ISMS を適用することが可能です。
ISMS は、様々な情報セキュリティリスクに対して汎用的に適用可能であり、そのなかでリスク対応に関する具体的な対策についてはこのようなセクター規格を参照することによって補完できます。

0.6 サービス系の規格との融合性

クラウドサービスには、その特性から、いつ、どこからでも、止まらずに利用できるという可用性が高く求められることから、クラウドサービス提供者にとってサービスの可用性を確保することは重要です。そのためには、クラウドサービスの運用に関するリスク、すなわち運用するクラウドサービスの品質等に関するリスクも考慮する必要があります。ISMS はよく機密性について注目されますが、その本質は情報の機密性、完全性、可用性をバランスよく保護することです。したがって、情報の可用性や完全性も考慮に入れることによってより有効な ISMS を実施することを可能とし、さらにクラウドサービスの質の向上にもつなげられます。

また、サービスの運用に関しては、JIS Q 20000 という IT サービスマネジメントシステム（ITSMS）に関する規格があります。ITSMS は名前の通り、IT サービスの品質を維持向上する仕組みを対象としたものです。IT サービスの品質とは、IT を利用したサービスが止まらないようにしたり、性能を維持したりすることで、この規格は、クラウドサービス提供者がサービス品質の改善・向上や顧客満足度の向上を図るのに有用です。JIS Q 20000 は JIS Q 27001 との親和性も高いことから、両規格を統合して実施することによって、安全で質の高いサービスの提供につなげることが可能です。

サービスに関する規格としては JIS Q 9001 も参考になります。JIS Q 9001 は提供する製品（物やサービス）の品質向上と顧客満足の継続的な向上を目指していくマネジメントシステムであり、JIS Q 20000 は提供する IT サービスの品質向上を目指すもので、どちらも目的は同じため共通点も多く見受

けられます。両規格についての説明は、 ITSMS ユーザーズガイド ～導入のための基礎～（ https://isms.jp/itsms/doc/JIP-ITSMS112-21.pdf ）の「6.QMS ユーザのための ITSMS 入門「JIS Q 9001 から見た JIS Q 20000」を参照して下さい。

ISO/IEC 27017 と JIS Q 27017

国際規格「ISO/IEC 27017」は、ISO（International Organization for Standardization: 国際標準化機構）が発行する国際規格であり、原文は英語です。
これを日本国内での使用のために日本語に翻訳し、国内規格として発行したものが「JIS Q 27017」です。翻訳された JIS Q 27017 は、ISO 規格と同じ内容であることが認められています。

注記：本追補では JIS Q 27017 を引用していることから、原則として JIS Q 27017 と表記します。

１．クラウドセキュリティについて

１．１　クラウドとは

クラウドと一般的に呼ばれているものには、クラウドサービスとクラウドコンピューティングがあります。
クラウドサービスとは、クラウドコンピューティング（環境）を利用したサービスのことですが、クラウドコンピューティングとは、単に仮想化技術を利用したコンピューティング環境のことではありません。

NIST（米国国立標準技術研究所）が提供している SP800-145*では、クラウドコンピューティグの特徴について、次の 5 つを挙げています。日本語翻訳版については IPA（独立行政法人情報処理推進機構）が提供していますので、ここではそれを併記します。

1. On-demand self-service（オンデマンド・セルフサービス）
2. Broad network access（幅広いネットワークアクセス）
3. Resource pooling（リソースの共用）
4. Rapid elasticity（スピーディな拡張性）
5. Measured Service（サービスが計測可能であること）

出典：NIST(National Institute of Standards and Technology：米国国立標準技術研究所)
SP800-145/ IPA（独立行政法人情報処理推進機構）訳

＊SP800-145　The NIST Definition of Cloud Computing（NIST によるクラウドコンピューティングの定義）

また、JIS Q 27017 の引用規格である JIS X 9401*では、クラウドコンピューティングを次のように定義しています。

クラウドコンピューティング（cloud computing）
セルフサービスのプロビジョニング（provisioning）及びオンデマンド管理を備える，スケーラブルで伸縮自在な共有できる物理的又は仮想的なリソース共用へのネットワークアクセスを可能にするパラダイム。
注記　リソースの例には，サーバ，OS，ネットワーク，ソフトウェア，アプリケーション及びストレージが含まれる。

（JIS X 9401:2016　3.2.5 クラウドコンピューティング　より引用）

＊JIS X 9401:2016 情報技術－クラウドコンピューティング－概要及び用語
（ISO/IEC 17788：2014 Information technology-Cloud computing-Overview and vocabulary）

上記の SP800-145 と JIS X 9401 では定義において若干の違いがあるものの、特徴として挙げているのは「セルフサービス」、「オンデマンド」、「スケーラブル（迅速・柔軟）」、「リソース共有」、「計測」となります。
例えば、クラウドコンピューティングは、クラウドで提供されるサービス（リソース共有）において、利用者が（セルフサービス）、自らの環境から API を使用して（オンデマンド）、リソースを柔軟に増減でき（スケーラブル）、その使用量などが計測される（計測）仕組みを有するもの、量に応じて課金（従量課金）する仕組みを有するものとみなすことができます。

なお、JIS X 9401 において、クラウドサービスは次のように定義されています。

> クラウドサービス（cloud service）
> 定義されたインタフェースを使って呼び出されるクラウドコンピューティング経由で提供される一つ以上の能力
> （JIS X 9401:2016 3.2.8 クラウドサービス より引用）

定義にある「能力」という用語は、わかりにくいかもしれませんが、単体のコンピュータリソースのこともあれば、それを活用したアプリケーションのこともあるということで、このような書き方になっています。また、ネットワーク経由ではなく、クラウドコンピューティング経由となっているところもこの定義の特徴です。定義されたインタフェースというのがウェブブラウザであったり、API（アプリケーションプログラムインタフェース）であったり、様々な形態で利用できるということを示しています。

1．2 クラウドのリスク

クラウドのリスクといった場合、クラウドコンピューティングにおけるリスクとクラウドサービスにおけるリスクを考慮することが一般的です。

クラウドコンピューティングに関するリスクの場合には、サービスの提供環境のことのみを指し、運用を含めたリスクについては、クラウドサービスに関するリスクと考えることができます。
また、クラウドサービスは、クラウドコンピューティング環境を利用することから、クラウドサービスのリスクを考慮する場合には、クラウドコンピューティングに関するリスクも包含することになります。しかしながら、クラウドサービスのリスクは、クラウドコンピューティングに関するリスクを保有したままの状態というわけではありません。クラウドサービスプロバイダが、サービス化する際にクラウドコンピューティングに関するリスク低減などを行なっていることもあり、既知のリスクについては解決していることも少なくありません。

JIS Q 27017 は「JIS Q 27002 に基づくクラウドサービスのための情報セキュリティ管理策の実践の規範」という名称で、クラウドサービスについてのリスクを検討し、必要となる管理策を提供しています。

引用規格である JIS X 9401 では、クラウドサービスを構成するにあたって、3 つのプレイヤーが存在するとしています。クラウドサービスプロバイダ、クラウドサービスカスタマ、クラウドサービスパートナがそれにあたります。
クラウドサービスはこれらの 3 者によって、目的となる環境が構成されています。
JIS Q 31000 にあるように、リスクとは「目的に対する不確かさの影響」であるため、これら 3 者によって、またクラウドコンピューティング環境において目的を確実にすることを阻害するものをリスクの要因として考えます。

クラウドサービスのリスクについて検討する際に重要なのは、自らがクラウドサービスプロバイダ、クラウドサービスカスタマ、クラウドサービスパートナのどれであるかを認識するとともに、それぞれが果たすべき役割を全うしていることを確実にすることです。

JIS Q 27017 では、クラウドサービスカスタマとクラウドサービスプロバイダの実践規範について記載をしています。クラウドサービスパートナについての記載がないのは、JIS Q 27017 の基となる国際標準（ISO/IEC 27017）が検討される際に、JIS X 9401 の基になる国際標準（ISO/IEC 17788）が確定していなかったことに依ります。

クラウドサービスのリスク要因と解決策については、経済産業省が発行した「クラウドサービスセキュリティガイドライン活用ガイドブック」が参考になります。また、クラウドサービスは毎年多くのものが新規に提供されていますので、それぞれのサービスの特徴をよく理解しつつ、リスクの検討をする必要があります。

２．JIS Q 27017 概要

JIS Q 27017 は、クラウドサービスに関する情報セキュリティ対策を実施するためのガイドラインです。
規格の名称は、次の通りです。

■JIS Q 27017:2016 情報技術―セキュリティ技術―JIS Q 27002 に基づくクラウドサービスのための情報セキュリティ管理策の実践の規範

規格の名称が示すように、幅広い情報セキュリティ管理策の手引である JIS Q 27002 に規定された管理策（管理目的、管理策、実施の手引）に対して、JIS Q 27017 にはクラウドサービス固有の管理策や実施の手引が記載されています。

２．１　規格の対象者

JIS Q 27017 はクラウドサービスを提供するクラウドサービスプロバイダとクラウドサービスを利用するクラウドサービスカスタマを対象としており、実施の手引も対象者ごとに分けて記述されています。
なお、JIS X 9401 に規定されたクラウドサービスパートナ（クラウド監査人及びクラウドサービスブローカを含む）は、前述の通り、JIS Q 27017 では、対象とはなっていません。

参 考

3.2.15 クラウドサービスプロバイダ（cloud service provider）
クラウドサービス（3.2.8）を利用できるようにするパーティ（3.1.6）。

3.2.11 クラウドサービスカスタマ（cloud service customer）
クラウドサービス（3.2.8）を使うためにビジネス関係にあるパーティ（3.1.6）。
注記 ビジネス関係は，必ずしも金銭的な合意を伴うとは限らない。

3.2.3 クラウド監査人（cloud auditor）
クラウドサービス（3.2.8）の供給及び利用について監査を行う責任のあるクラウドサービスパートナ（3.2.14）。

3.2.9 クラウドサービスブローカ（cloud service broker）
クラウドサービスカスタマ（3.2.11）とクラウドサービスプロバイダ（3.2.15）との関係を取り決めるクラウドサービスパートナ（3.2.14）。

3.2.14 クラウドサービスパートナ（cloud service partner）
クラウドサービスプロバイダ（3.2.15），クラウドサービスカスタマ（3.2.11）の一方，又はその両者の，活動をサポートする，又は補助する役割を担うパーティ（3.1.6）

（JIS X 9401:2016 より引用）

２．２　実施の手引の様式

表 2-1 で示すように、クラウドサービス固有の実施の手引は、クラウドサービスカスタマに対応するものと、クラウドサービスプロバイダに対応するものが対になっています。これは、クラウドサービスに関する有効な情報セキュリティを実現するためには、クラウドサービスカスタマとクラウドサービスプロバイダの双方が、お互いに協力して適正に運用・管理することが必要であることを意味しています。

JIS Q 27017 では、多くの場合、次の「JIS Q 27017 における実施の手引の様式の例」に示す通り、クラウドサービスカスタマ及びクラウドサービスプロバイダの両方の手引が記載されていますが、一方だけの手引を記載しているものや、両方に対して同一の手引を記載している場合もあります。

JIS Q 27017 における実施の手引の様式の例

9.2.4 利用者の秘密認証情報の管理

JIS Q 27002 の9.2.4 に定める管理策並びに付随する実施の手引及び関連情報を適用する。次のクラウドサービス固有の実施の手引も適用する。

クラウドサービスのための実施の手引

クラウドサービスカスタマ	クラウドサービスプロバイダ
クラウドサービスカスタマは，パスワードなどの秘密認証情報を割り当てるための，クラウドサービスプロバイダの管理手順が，クラウドサービスカスタマの要求事項を満たすことを検証することが望ましい。	クラウドサービスプロバイダは，秘密認証情報を割り当てる手順，及び利用者認証手順を含む，クラウドサービスカスタマの秘密認証情報の管理のための手順について情報を提供することが望ましい。

（JIS Q 27017:2016 より引用）

２．３　クラウドサービスにおける供給者関係（クラウドサービスの形態）

クラウドサービスプロバイダの多くは ICT サプライチェーンを形成しています。例えば、SaaS 事業者が他の IaaS/PaaS 事業者が提供するクラウドサービスを利用して自らのクラウドサービスを実現するような場合が該当します。このようなケースでは、その SaaS 事業者はクラウドサービスプロバイダであるとともにクラウドサービスカスタマでもあり、JIS Q 27017 で示されている管理策の実施の手引の両方の立場を考慮する必要があります。

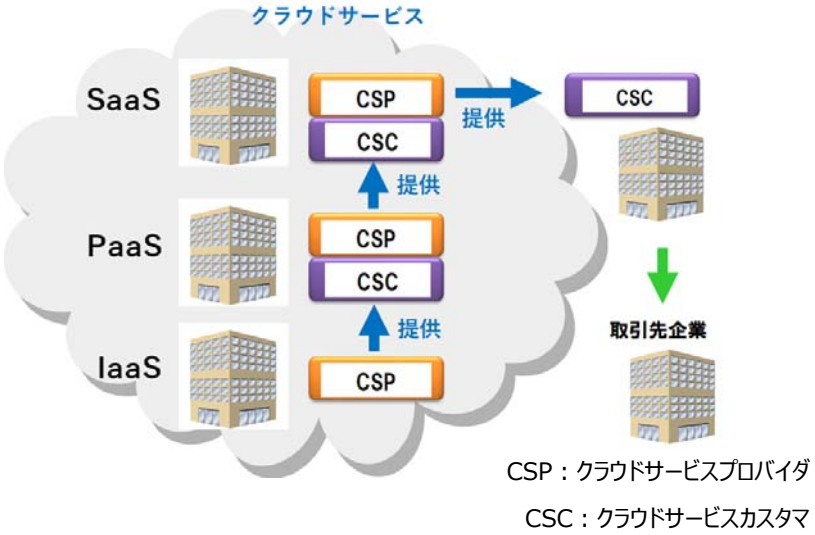


図 2-1　クラウドサービスにおける供給者関係

２．４　クラウドサービスにおける情報セキュリティリスクの管理

JIS Q 27017 はクラウドサービス固有のリスクに対応するための対策集であり、この規格では次に示す通り、情報セキュリティのリスクマネジメントを実施するための JIS Q 27001 で要求するプロセスを備えていることを前提としています。

> クラウドサービスカスタマ及びクラウドサービスプロバイダは，いずれも，情報セキュリティリスクマネジメントプロセスを備えていることが望ましい。情報セキュリティマネジメントシステムにおけるリスクマネジメントを実施するための要求事項については JIS Q 27001 を参照し，情報セキュリティリスクマネジメントそのものの更なる指針については，ISO/IEC 27005 を参照することを勧める。
>
> （JIS Q 27017:2016 4.4 クラウドサービスにおける情報セキュリティリスクの管理　より引用）

ここで「前提とする」という意味は、JIS Q 27017 では、規格に記載されている事項の単なる確認（例：～を確認していますか、～検証していますか）ではなく、それによって特定したリスクを JIS Q 27001 のリスクアセスメント、リスク対応、内部監査等につなげることが必要ということです。

例えば、クラウドサービスカスタマの場合は、JIS Q 27017 の管理策では「～をプロバイダに確認すること望ましい」といった表現が大半ですが、確認すること自体が目的ではなく、確認することによってどの程度のリスクを保有しているのかをリスク評価し、必要となるリスク対応を JIS Q 27001 の要求事項に基づいて、自社のリスク対応に追加するということです。

ここでは、JIS Q 27017 の 12.3.1 の情報のバックアップを参照し、クラウドサービスカスタマ側における具体的な活動について説明します。JIS Q 27017 の 12.3.1 では、クラウドサービスカスタマ向けの実施の手引に「バックアップ機能の仕様を要求することが望ましい。」、「その仕様がバックアップに関する要求事項を満たすことを検証することが望ましい。」とありますが、ここでは単に「要求」、「検証」することを意図

しているわけではありません。この「バックアップに関する要求事項」は、JIS Q 27001 の 12.3.1 に記載の管理策のことであり、その内容に従って、利用しているクラウドサービスが要求事項を満たしているかを確認することが求められています。

JIS Q 27017 の 12.3.1 と JIS Q 27001 の A.12.3.1 の関係

12.3.1 情報のバックアップ

JIS Q 27002 の12.3.1 に定める管理策及び付随する実施の手引を適用する。次のクラウドサービス固有の実施の手引も適用する。

クラウドサービスのための実施の手引

クラウドサービスカスタマ	クラウドサービスプロバイダ
クラウドサービスプロバイダがクラウドサービスの一部としてバックアップ機能を提供する場合は，クラウドサービスカスタマは，クラウドサービスプロバイダにバックアップ機能の仕様を要求することが望ましい。また，クラウドサービスカスタマは，その仕様がバックアップに関する要求事項を満たすことを検証することが望ましい。 クラウドサービスプロバイダがバックアップ機能を提供しない場合は，クラウドサービスカスタマがバックアップ機能の導入に責任を負う。	クラウドサービスプロバイダは，クラウドサービスカスタマに，バックアップ機能の仕様を提供することが望ましい。その仕様には，必要に応じ，次の情報を含めることが望ましい。 （以下、省略）

（JIS Q 27017:2016 12.3.1 情報のバックアップ より引用）

A.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，検査しなければならない。

（JIS Q 27001:2014 12.3.1 A.12.3.1 情報のバックアップ より引用）

上記のように、JIS Q 27017 の管理策は、JIS Q 27001 の管理策（ここでは、A.12.3.1）と併せて適用する必要があります。A.12.3.1 の管理策に記載されている通り、クラウドサービスカスタマは、バックアップについて、バックアップ方針に従って定期的に取得し、検査する必要があり、検査の結果として例えば、クラウドサービスプロバイダの提供するバックアップ機能が自組織の管理策を満たさない場合には、JIS Q 27001 のリスクセスメントを実施して、必要なリスク対応を計画する際、対策に漏れがないかを JIS Q 27017 の 12.3.1 等を参考に確認することが要求されることを意図しています。

２．５ クラウドサービス特有のリスク

クラウドサービスのリスクには、1 章に記載したようにクラウドコンピューティングに関するリスクとクラウドサービスの運用面に伴うリスクに大別されます。

クラウドコンピューティングに関するリスク源については、JIS Q 27017 に次の通り記載されています。クラウドサービスにおける有効なリスクマネジメントを実施するためには、こうした情報を参考に情報リスクを特定し管理することが重要となります。

> 情報セキュリティリスクマネジメントプロセスの一般的な適用性とは対照的に，クラウドコンピューティングには，その特性（例えば，ネットワーク，システムのスケーラビリティ及び弾力性，資源共有，セルフサービスプロビジョニング，オンデマンド管理，法域を超えたサービスの提供及び管理策の実施についての可視性が限られていること）に由来する，固有の，脅威及びぜい弱性を含むリスク源がある。附属書 B に，クラウドサービスの提供及び利用における，これらのリスク源及び関連するリスクについて，情報を提供する参考文献を示す。
>
> （JIS Q 27017:2016 4.4 クラウドサービスにおける情報セキュリティリスクの管理 より引用）

クラウドサービスにおいては、その形態、提供されるリソースやアプリケーションによってリスクが異なります。
また、運用面のリスクとしては、提供／利用するクラウドサービスそのもののリスクも考慮する必要があり、クラウドサービスプロバイダ側又はクラウドサービスカスタマ側の立場によってリスクの内容は異なります。
クラウドサービスの運用面に伴うリスクの具体的な事例については、JIS Q 27017 の附属書 B（主にクラウドサービスプロバイダを対象）またはクラウドセキュリティガイドライン活用ガイドブック（経済産業省）（クラウドサービスプロバイダ及びクラウドサービスカスタマの両方を対象）を参照して下さい。

３．ISMS クラウドセキュリティ認証について

３．１　ISMS クラウドセキュリティ認証の概要

ISMS クラウドセキュリティ認証は、JIS Q 27001(ISO/IEC 27001）に適合した ISMS において、その適用範囲内に含まれるクラウドサービスの提供もしくは利用に関して、クラウドサービス向けの国際規格である ISO/IEC 27017（JIS Q 27017）に規定されるクラウドサービス固有の管理策が実施されていることを認証するものです。

> ■規格名称
> ISO/IEC 27017:2015 Code of practice for information security controls based on ISO/IEC 27002 for cloud services
> （JIS Q 27017:2016 ISO/IEC 27002 に基づくクラウドサービスのための情報セキュリティ管理策の実践の規範）

本来、JIS Q 27017 は、実践の規範であるため認証基準ではありません。そのため、組織がクラウドサービス固有の情報セキュリティを含めた ISMS 認証を取得するためには、組織が JIS Q 27017 の管理策を取り込むための認証基準が必要となります。
このため、ISMS クラウドセキュリティ認証のための新たな認証基準として、「ISO/IEC 27017:2015 に基づく ISMS クラウドセキュリティ認証に関する要求事項（JIP-ISMS517）」※が策定されました。
策定された認証基準は JIS Q 27001 に対する追加の要求事項であるため、ISMS クラウドセキュリティ認証を希望する組織は、JIS Q 27001 及び JIP-ISMS517 への適合が求められます。

したがって、ISMS クラウドセキュリティ認証とは、ISMS 認証を前提として、JIS Q 27017 のガイドラインに沿ったクラウドサービスの情報セキュリティ管理の要求事項に対応した組織に対して、JIP-ISMS517 を用いて適合性を評価し、認証するものです。

※JIP-ISMS517 では、本要求事項における ISO/IEC 27017:2015 は、JIS Q 27017:2016 と読み替えるものとします。

３．２　対象組織と認証範囲

ISMS クラウドセキュリティ認証を取得できる対象組織は、JIS Q 27017 のガイドラインに沿った「クラウドサービスプロバイダ」と「クラウドサービスカスタマ」となります（「2.1　規格の対象者」を参照）。前述の通り、JIS X 9401 によって定義づけられた「クラウドサービスパートナ」や「クラウドサービスブローカ」と呼ばれるサービス事業者であり、提供するサービスが、本書の１．１に記載の「クラウドコンピューティング」や「クラウドサービス」の定義を満たさない場合は、当該サービスは認証の対象とならない場合があることに留意する必要があります。

JIS X 9401 では、クラウドサービスパートナを、「クラウド監査人」や「クラウドサービスブローカ」を含む、「クラウドサービスプロバイダ，クラウドサービスカスタマの一方，又はその両者の活動をサポートする，又は補助する役割を担うパーティ」として定義しています。

また、クラウドサービスブローカは、クラウドサービスを販売する組織のことを指します。販売に際して提案などを行うコンサルティングなどもクラウドサービスブローカの業務となり得ます。国内では SIer やリセラーがそれにあたります。
一方、自らクラウドサービスを構築し販売している場合は、クラウドサービスプロバイダと言えます。またマネージドサービスなどを行っている場合は、クラウドサービスカスタマとしてサービス提供をしていることになりますので、当該サービスは認証取得の対象とすることが可能です。

ここで、認証取得の対象となる業務について整理してみます。

クラウドサービスプロバイダ
クラウドサービスを利用可能にする組織（クラウドサービスを提供する組織）。ただしクラウドサービスプロバイダも、提供サービスの様態によっては、クラウドサービスカスタマとなります。

クラウドサービスカスタマ
クラウドサービスを利用する目的のための取引関係がある組織（クラウドサービスを利用する組織）。

認証範囲について
ISMS クラウドセキュリティ認証は、ISMS 認証を前提として JIS Q 27017 のガイドラインに沿ったクラウドサービスの情報セキュリティ管理を満たしている組織を認証する仕組みであるため、本認証を取得しようとする組織は、認証範囲を ISMS 認証の範囲内とする必要があります。

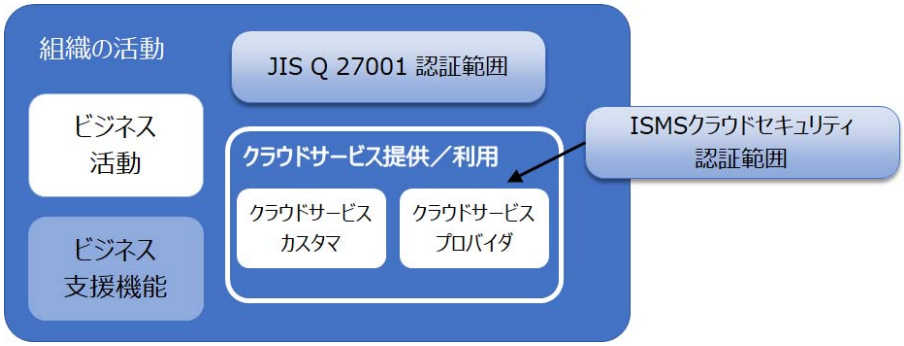
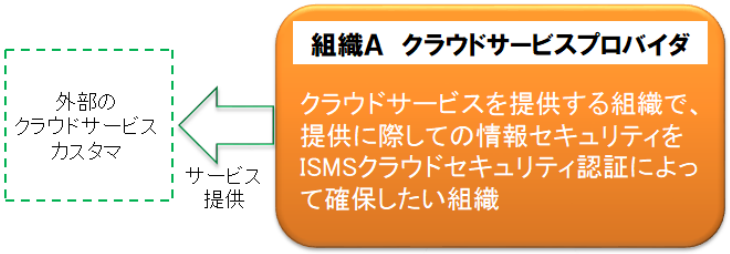


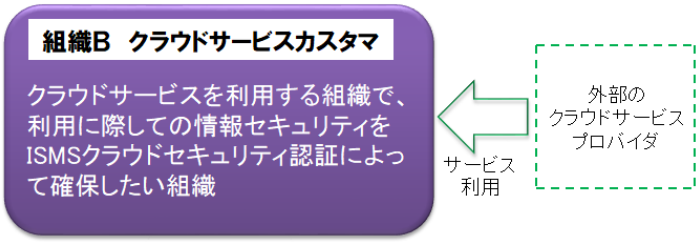
図 3-1 認証範囲のイメージ

対象となる組織の例としては次の３つが想定されます。

１．自社にインフラを持ちクラウドサービスを提供している組織



２．クラウドサービスを利用している組織



３．クラウドサービスを利用及び提供している組織

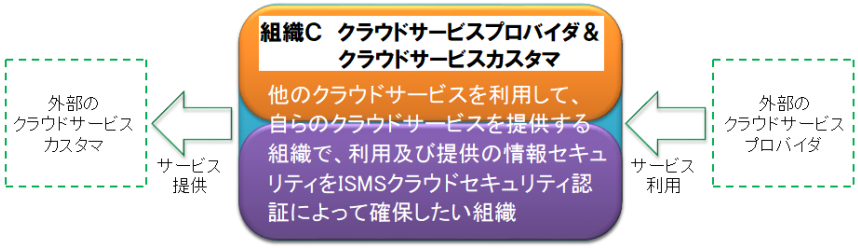


図 3-2　対象組織のイメージ

ISMS クラウドセキュリティ認証の適用範囲の考え方の詳細は、4 章を参照して下さい。

３．３　JIS Q 20000 との関連

ISMS クラウドセキュリティ認証では、前述の通り、クラウドサービスプロバイダとクラウドサービスカスタマが対象組織であり、クラウドサービスパートナ（SIer など）が提供するサービスは認証の対象とならないケースがあります。しかしながら、クラウドの技術の進展及び高度化により、クラウドサービスカスタマがクラウドサービスパートナを利用し、クラウドサービスパートナがクラウドサービスカスタマに代わり、クラウドサービスを運用するようなケースにおいては、クラウドサービスパートナが提供する運用サービスは、「IT サービス」となり得るため、JIS Q 20000-1 の運用を検討することは、サービスの品質を向上させるためには有用となります。JIS Q 20000-1 には、情報セキュリティに関する要求事項も包含しているため、この規格を利用し、管

理策の採用としてクラウドの管理策（JIS Q 27017）を適用し、運用することを検討されることは妥当であると考えられます。

■規格名称
JIS Q 20000-1:2012 情報技術－サービスマネジメント－第 1 部：サービスマネジメントシステム要求事項
（ISO/IEC 20000-1：2011 _Information technology-Service management-Part 1: Service management system requirements）

SIer として外部のクラウドサービスを利用して構築したシステムの運用を行っている場合には、クラウドサービスカスタマとしての認証を取得することが可能と考えられます。また、基盤となる IT システムにおける情報セキュリティ管理には ISMS（クラウドセキュリティを含む）を適用し、サービス提供の部分には ITSMS（JIS Q 20000-1 を認証基準としたサービスマネジメントの認証制度）を適用することが有効と考えられます。

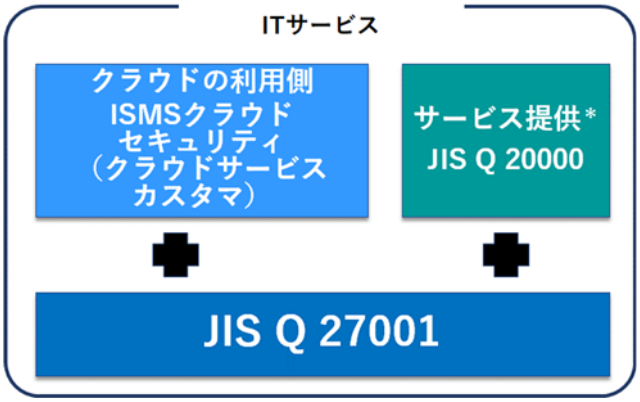


図 3-3 ISMS クラウドセキュリティ、JIS Q 27001、JIS Q 20000 の関係

＊図中の「サービス提供」のサービスとは、クラウドサービスでなく、クラウドを運用する IT サービスのことを指します。

４．ISMS クラウドセキュリティ認証の要求事項

本章では、ISMS クラウドセキュリティ認証に関する要求事項（JIP-ISMS517）について、要求事項の構成に沿って解説します。

４．１　クラウドサービスを含む情報セキュリティマネジメントシステムの適用範囲の決定【JIS Q 27001 の 4.3】

（１）「適用範囲」の解説

ISMS クラウドセキュリティ認証において、適用範囲の設定は非常に重要となります。前章までの対象組織や用語の定義、JIS Q 27017 などを参考に、JIP-ISMS517 はクラウドサービスプロバイダ及びクラウドサービスカスタマを対象とした要求事項であることに留意して下さい。
適用範囲の決定にあたって、JIP-ISMS517 の 4.1 では、次のように定めています。

> 4.1　クラウドサービスを含む情報セキュリティマネジメントシステムの適用範囲の決定
> 【 JIS Q 27001 の 4.3 】
> 組織は、クラウドサービスを含めた ISMS の適用範囲を定めるために、その境界及び適用可能性を決定しなければならない。
> クラウドサービスを含めた ISMS の適用範囲は、クラウドサービス名を含む文書化した情報として利用可能な状態にしておかなければならない。
> 適用範囲を定める際、クラウドサービスプロバイダが自らのサービスを提供するに当たり、別のクラウドサービスを利用している場合は、クラウドサービスプロバイダ及びクラウドサービスカスタマの両方を適用範囲としなければならない。
>
> 注記：ISO/IEC 27017 の箇条 4 では、クラウドサービスプロバイダの情報セキュリティ管理の対象は、クラウドサービスカスタマの情報セキュリティ対策のための情報提供や機能提供を含むものと規定されている。これに従い、クラウドサービスプロバイダは、リスクアセスメントの範囲にクラウドサービスカスタマとの関係を含めたリスク対応を検討することが必要である。
>
> （ISO/IEC 27017:2015 に基づく ISMS クラウドセキュリティ認証に関する要求事項（JIP-ISMS517-1.0）より引用）

上記のとおり、まず適用範囲としてどのクラウドサービスのカスタマであるのか、どのクラウドサービスのプロバイダとしてなのかを定義したサービス名を記載することが要求されています。

具体的には２章で説明した次の３つのパターンで適用範囲を検討します。

a) 自社にインフラを持ちクラウドサービスを提供している組織（クラウドサービスプロバイダ）
当該組織のパターンでは特に他のクラウドサービスを利用していないため、プロバイダの側面としてサービスを特定します。

例としては、コンピュータリソースを提供する IaaS や、自社のインフラを利用しアプリを提供する SaaS などが挙げられます。
SaaS において、複数のサービスを提供している場合、個別の提供サービス名を特定する必要があります。

b) クラウドサービスを利用している組織(クラウドサービスカスタマ)

当該組織のパターンではクラウドサービスプロバイダとしての側面は範囲としないということが前提となりますので、（自社で利用する）どのクラウドサービスの利用で情報セキュリティの管理をしているかという観点になります。
例としては、クラウドサービスプロバイダが提供しているサービス名などが挙げられます。

c) クラウドサービスを利用及び提供している組織（クラウドサービスカスタマ及びクラウドサービスプロバイダ）

多くのクラウドサービスが ICT サプライチェーンよって構成されていることを考慮すると、本パターンによるケースが一番多いと推測されます。
具体的には IaaS 事業者が提供するインフラのクラウドサービスを利用し、その仮想環境上に自社で開発したアプリケーションなどを実装し SaaS 事業者としてサービスを提供するなどが挙げられます。
例としては、他組織が提供する IaaS を利用し、SaaS として自社サービスを提供するという形になります。

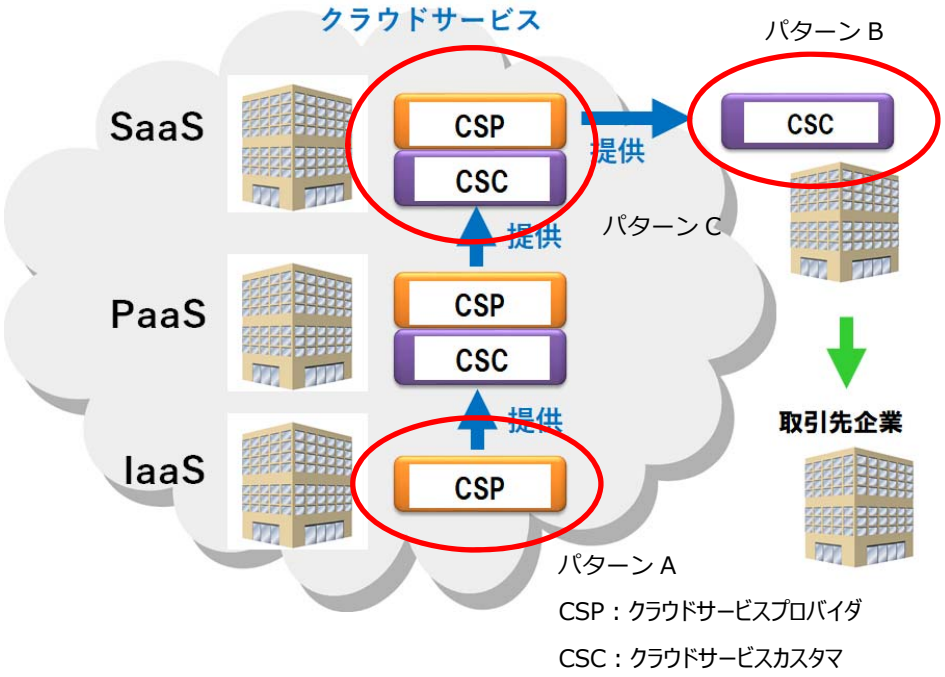


図 4-1　クラウドサービスにおける適用範囲の種類

一方、この c ）のパターンの場合には注意が必要です。
注意すべき事例として代表的なものを 2 つ挙げます。

① 他組織が提供するクラウドサービスのリセールに関する事例： 単純なクラウドサービスの代理店の場合、クラウドサービスのライセンス販売などが主たるサービスであり、クラウドサービスそのものの提供は行っていないため、クラウドサービスプロバイダとはなり得ません。同様に、他の SaaS 事業者が展開するサービスにおいて、そのサービスが有する機能について、効果的に利用するためのコンサルティングをソリューションとして提供するサービスの場合においても、当該クラウドサービスの提供者は SaaS 事業者であり、この組織自身は本書 1.1 で説明したクラウドサービスに準じたクラウドサービスを提供していないことから、クラウドサービスプロバイダとして、当該サービスを適用範囲とすることは困難です。

② クラウドを利用する組織の代わりにクラウドサービスを運用するシステムインテグレータの事例： システムインテグレータは、複数のクラウドサービスを組み合わせたシステムを設計することがあります。その上で、設計したシステムに対し、各サービスプロバイダにその構築を依頼するケースがあります。このような場合、本システムの利用者は、構築されたシステムの変更に際して、自組織では技術的なスキルを有していないため、システム設計に携わったシステムインテグレータにシステムの変更要求を提出し、システム変更を行ってもらうことがあります。このケースにおいてシステムインテグレータは、IT サービスとしてのサービスプロバイダではありますが、本書 1.1 で説明したクラウドサービスに準じたクラウドサービスを提供していないため、クラウドサービスプロバイダとして、当該サービスを適用範囲とすることは困難です。

（２） システム側面からの適用範囲

クラウドサービスの適用範囲を考えるにあたり、注意しなければならない点として、提供するクラウドサービスのシステム側面（クラウドコンピューティングの側面）があります。
特に、クラウドサービスプロバイダとして ISMS クラウドセキュリティ認証に関する要求事項（JIP-ISMS517）を適用する際には、システム側面での適用範囲に注意する必要があります。というのも、提供するクラウドサービスのセキュリティを確保するためには、そのクラウドサービスを提供するにあたり必要な IT システムは全て、適用範囲に含める必要があるからです。
全てのクラウドサービスを適用範囲とせず、主要なサービスから認証を取得しようとするスモールスタートを考慮した場合においても、それら主要なサービスを提供するにあたり必要な IT システムを全て適用範囲に含める必要があります。

例えば、クラウドサービスプロバイダが、クラウドサービスの提供やシステムの構成管理において必要不可欠となる IT システムが、クラウドサービスプロバイダのオンプレミス環境にあったとしてもそのクラウドサービスを認証取得の対象とする場合、オンプレミス環境も適用範囲に含める必要があります。

これは、図 4-2 に示すように、クラウドサービスプロバイダが、クラウド上で運用する仮想サーバと、自社のデータセンターに設置した DB サーバを連携させて SaaS サービスを提供する場合には、自社のデータセンターの DB サーバも当該サービスの適用範囲となるということを意味します。このデータセンターについては物理的な適用範囲としても含める必要がありますので、詳細については「（４）物理的な適用範囲」の②をご参照下さい。

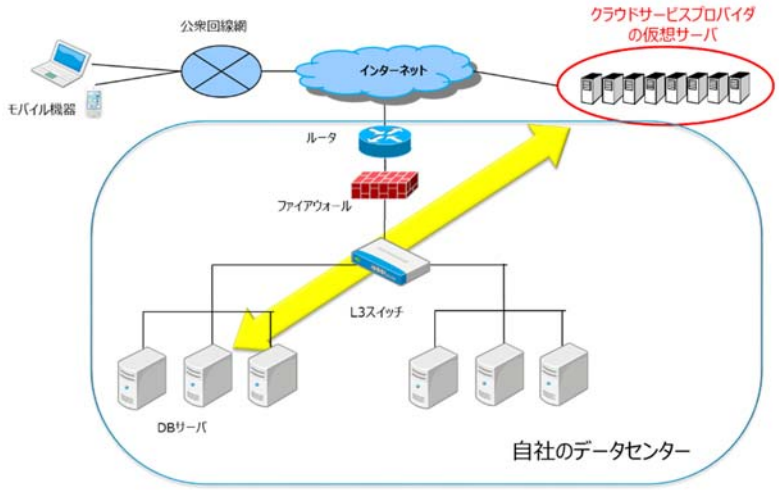


図 4-2 ネットワーク構成（例）

同様に、バックアップ機能などを提供しているシステムなどがオンプレミス環境にある場合であって、これらの機能が当該クラウドサービスの一部としてサービスカタログ※に記載され、告知されているのであれば、適用範囲に含める必要があります。

※サービスカタログとは、提供するサービスについての定義、サービスの種類やシステム構成などを記載したもので、顧客と SLA の合意を得る場合などに用いられます。

（３） 組織的な適用範囲

組織的な適用範囲については、組織構造を含め様々なものがありますが、なかでも要員については留意が必要です。これらは上記同様、当該クラウドサービスを適用範囲に含める際、そのサービスに係る活動を適用範囲を定めた文書で定義づけ、その定義に基づく合理的な要員を適用範囲に含める必要があります。

このことは、ISMS クラウドセキュリティ認証の適用範囲内の部門や委員会であっても、「ISMS クラウドセキュリティ認証マークを活用できる要員」（「クラウドセキュリティ要員」と呼ぶ。）は、ISMS に係る要員（ISMS 要員と呼ぶ。）と区別して考える必要があることを意味します。

例えば、クラウドサービスカスタマの場合、活用しているクラウドサービスの運用管理という業務を提供範囲として定義するのであれば、運用管理を担う担当者を適用範囲に含める必要はありますが、必ずしもクラウドサービス利用者全員を含めなくても良い場合もあります。すなわち、この例では、運用管理担当者は、「クラウドセキュリティ要員」であり、利用者は「ISMS 要員」であるということを示しています。一方、このような場合においても、「運用管理」という定義の中に、活用するクラウドサービスに対するインシデント対応、サービス停止に伴う事業継続活動などが含まれているのであれば、これらの活動に携わる要員も「クラウドセキュリティ要員」として適用範囲に含める必要があります。

同様な例として、以下のようなことが考えられます。

①ISMS 事務局などの ISMS 活動を推進する組織などにおいて、「ISMS 要員」ではあるが、対象となるクラウドセキュリティの運用のプロセスや管理策の実施に携わっていない場合は、「クラウドセキュリティ要員」とはならないことがあります。

②営業部門内のお客様との窓口業務を担う担当者で、各種契約、SLA、サービス仕様の合意など顧客対応のプロセスには関わるが、クラウドサービスの運用プロセスや管理策に直接関連しない場合は、「クラウドセキュリティ要員」とはならないことがありますし、営業部門としても ISMS の適用範囲ではあるものの、ISMS クラウドセキュリティ認証の適用範囲には含まれないこともあります。

（４） 物理的な適用範囲

物理的な適用範囲としては、サイトについて考慮する必要があります。特に、クラウドサービスプロバイダの場合には、システム側面からの適用範囲にも関連しますが、クラウドサービスの提供やシステムの構成管理において必要不可欠となる IT システムが設置されているサイトを全て含めることが重要です。
クラウドサービスプロバイダは、クラウドサービスを展開する上で、
①他のクラウドサービスを利用する、
②自社にインフラを保持する、もしくは
③データセンターにインフラを設置して運用する
などが考えられます。

①の他のクラウドサービスを利用している場合は、「供給者管理」という視点から他のクラウドサービスを管理するため、他のクラウドサービスの物理的な適用範囲を考慮する必要はありません（ただし管理策に該当する内容を網羅的に適用することは必要です）。

②の自社にクラウドサービスを展開するためのインフラを保持している場合、前述の（２）システム側面からの適用範囲に記載したとおり、提供するクラウドサービスを支えるインフラ全体を適用範囲に含める必要があるため、インフラを設置しているサイトを物理的な適用範囲として含める必要があります。

③のデータセンターを利用する場合、展開するクラウドサービスに対し、データセンターが物理的にどう関与しているかを考慮することが重要です。
例えば、クラウドサービスプロバイダが、データセンターの利用についてフルマネージドサービスを受けてインフラを管理するケースがあります。その場合、クラウドサービスプロバイダはリモートによるインフラの運用管理を実施し、データセンターへの物理的な立会いを実施しない場合は、クラウドサービスプロバイダは、データセンターを ISMS クラウドセキュリティ認証の物理的な適用範囲には含める必要がありません。この場合は、このデータセンターが委託先として、どのようにデータセンター内のインフラを運用し、管理策を導入しているかなどの事項について委託元として管理責任が発生することから、供給者管理による管理策を適用することが適切であると考えられます。

一方で、フルマネージドサービスを利用しない場合においては、データセンターに対しては基本的には委託先管理に必要な管理策を適用することになりますが、データセンター内にインフラとして設置した機器の保守に際し、保守ベンダーをデータセンターに訪問させ、自らもそれらの作業に立ち会うなど、データセンターでの作業（物理的な作業）が発生すると考えられるため、データセンターを適用範囲として含めることが必要となる場合があります。

上記（１）～（４）のような考え方は、ISMS の適用範囲を決定する際に既に検討されている事項だと考えられますが、その一方で、ISMS クラウドセキュリティの適用範囲を検討する際に、ISMS の適用範囲を再確認し、必要に応じては ISMS の適用範囲を拡張させることが必要となる場合があります。
例えば、クラウドサービスカスタマにおいて、クラウドサービス管理をデータセンターに設置したホスト上の API（WebUI）などを介して実施している場合であって、当該 ISMS の適用範囲にそのデータセンターを含めていない場合、ISMS の適用範囲を拡張し当該データセンター含め、ISMS クラウドセキュリティ認証の適用範囲としても定義するといったことが必要となる場合もあります。

同様に、「クラウドセキュリティ要員」を検討する際、対象となる要員が ISMS 要員ではなかった等の場合、ISMS の適用範囲を検討し、適切にクラウドセキュリティ要員を ISMS の適用範囲に含めるよう拡張させ、クラウドセキュリティ要員として定義づけられるよう留意して下さい。

４．２ JIS Q 27001 に沿ったクラウド情報セキュリティ対策の実施

４．２．１ 情報セキュリティリスクアセスメント【JIS Q 27001 の 6.1.2c】

クラウドサービスの利用／提供を検討する際には、前提となる組織の状況、実際の運用において想定されるリスクを検討し、特定する必要があります。これらの考え方や要求事項については、JIS Q 27001 の要求事項に沿った活動が要求されます。

クラウドサービスについて、情報セキュリティリスクアセスメントを展開する上では、クラウドサービスに特化したリスクについて特定する必要があります。
これらのリスクには、次のようなものがあります。

（１） クラウドサービスの利用及び提供において前提となるリスク

1）内外の環境の変化に対応するための対策方針

クラウドサービスプロバイダ及びクラウドサービスカスタマは、クラウドコンピューティングと運用に関わるリスクを考慮して事業方針を拡充することが推奨されます。
特にクラウドサービスプロバイダでは、事業方針の拡充に際してサービス形態や保持しているリソース、他のサービスプロバイダとの関連性を考慮することが求められます。

また、クラウドサービスのために事業方針を定義・拡充する際に、既存の方針群等の内容を変更する必要が生じた場合、ISMS クラウドセキュリティ認証の前提となる ISMS 認証に立ち返ってその適合性を確認することが推奨されます。

2） 適用される法律・法令等

クラウドサービスプロバイダは、提供するクラウドサービスに適用される法律・法令等の情報を、クラウドサービスカスタマに提供することが推奨されます。

一方、クラウドサービスカスタマは、自社の事業に関連する法律・法令等を考慮する際に、クラウドサービスプロバイダに適用される法律・法令等も含め、それらの法律・法令等の順守の証拠をクラウドサービスプロバイダに求めることが推奨されます。

クラウドサービスプロバイダ及びクラウドサービスカスタマが意識すべき海外の法律・法令等には、例えば次のものが挙げられます。これらの法律・法令等は、各国の政策や各国間の情勢により変化するため、常に最新の動向・情報を意識して確認することが求められます。法律・法令等への順守は、ISMS クラウドセキュリティ認証のみならず、コーポレートガバナンスの一環として適切に管理することが必要です。
詳細は JIS Q 27017 の 18.1.1「適用法令及び契約上の要求事項の特定」を参照して下さい。

- 米国愛国者法(USA Patriot Act)
  - 2001 年 9 月 11 日に発生した同時多発テロ事件を受け、捜査機関の権限の拡大等を規定した法律。これにより、米国における捜査機関の情報収集に関する規制が緩和された。2015 年 5 月末に失効。改正された情報自由法(Freedom of Information Act)により情報収集が規制されることとなった。
  - 参考文献
    - 米国司法省 “The USA PATRIOT Act”
      https://www.justice.gov/archive/ll/highlights.htm

- EU 一般データ保護規則（GDPR）
  - EU 域内の個人情報保護を目的とした法律。GDPR は、EU を含む欧州経済領域（EEA）域内の個人データを EEA 域外に移転することを原則禁止するものであり、2018 年 5 月 25 日に適用が開始される予定。
  - 参考文献
    - EU “Protection of personal data”
      http://ec.europa.eu/justice/data-protection/index_en.htm
    - JETRO「「EU 一般データ保護規則（GDPR）」に関わる実務ハンドブック（入門編）(2016 年 11 月）」
      https://www.jetro.go.jp/world/reports/2016/01/dcfcebc8265a8943.html
- ワッセナー・アレンジメント（通常兵器及び関連汎用品・技術の輸出管理に関するワッセナー・アレンジメント）
  - 通常兵器の輸出管理に関する国際協定。日本を含めた 41 か国が参加している。輸出管理対象品目の中に暗号化技術が含まれている。日本からの輸出に関する対象品目は、経済産業省令「輸出貿易管理令別表第一及び外国為替令別表の規定に基づき貨物又は技術を定める省令」で規定している。
  - 参考文献
    - 外務省「通常兵器及び関連汎用品・技術の輸出管理に関するワッセナー・アレンジメント」

http://www.mofa.go.jp/mofaj/gaiko/arms/wa/index.html

✧ 輸出貿易管理令別表第一及び外国為替令別表の規定に基づき貨物又は技術を定める省令
http://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=403M50000400049&openerCode=1

（２） クラウドサービスの利用及び提供における運用上のリスク

クラウドサービスの利用及び提供における運用上のリスクの例としては、次が挙げられます。

1）情報セキュリティ方針の欠如

クラウドサービスプロバイダは、自社の情報セキュリティ方針において、提供するクラウドサービス特有の技術（仮想化、マルチテナント、クラウド管理者の特権的アクセス等）に起因するリスクへの対策を適切に実施するために、情報セキュリティ方針を拡充することが推奨されます。

一方、クラウドサービスカスタマは、クラウドサービス特有の状況（資産がクラウド上に置かれること、クラウド管理者が特権的アクセス権を持つこと、情報やデータの保管先である地理的所在地が移動する可能性があること等）に起因するリスクへの対策を適切に実施するために、クラウドコンピューティングのための情報セキュリティ方針を定義することが推奨されます。特に、情報セキュリティのための方針群の策定にあたっては、自社内の状況に加えて、クラウドサービスプロバイダが提供するクラウドサービス等の状況を勘案し、互いの役割と責任を考慮したリスクアセスメントを行い、その結果を踏まえることが求められます。

クラウドサービスのために定義・拡充した情報セキュリティ方針群は、既存の情報セキュリティ方針群等で定められた情報セキュリティリスクの受容可能なレベル（リスク受容基準）と矛盾しないものとすることが重要です。また、クラウドサービスのために情報セキュリティ方針群を定義・拡充する際に、既存の情報セキュリティ方針等の内容を変更する必要が生じた場合、ISMS クラウドセキュリティ認証の前提となるISMS 認証に立ち返ってその適合性を確認することが推奨されます。

詳細は JIS Q 27017 の 5.1.1「情報セキュリティのための方針群」を参照して下さい。

2）情報セキュリティの役割及び責任の欠如

クラウドサービスプロバイダは、別のクラウド事業者を含む供給者からサービスの提供を受ける場合、全てが自社ではコントロールできないといった問題が生じるリスクがあります。

一方、クラウドサービスカスタマは、クラウドサービスを利用することにより、情報の管理や処理をクラウド事業者に委ねることとなり、リスクの全てをコントロールできないといった問題が生じるリスクがあります。

そうしたリスクへの対策として、クラウドサービスにおける情報セキュリティの役割と責任について、クラウドサービスプロバイダとクラウドサービスカスタマで適切に割り当てることが必要です。クラウドサービスプロバイダ及びクラウドサービスカスタマは、提供する（利用する）クラウドサービスにおける情報セキュリティの役割と責任について、クラウドサービスプロバイダ、サードパーティ（供給者）、クラウドサービスカスタマで適切に割り当てることに合意し、文書化することが推奨されます。

詳細は JIS Q 27017 の 6.1.1「情報セキュリティの役割及び責任」を参照して下さい。

3）情報のバックアップの不備

クラウドサービスプロバイダ及びクラウドサービスカスタマは、クラウドサービス上で取り扱われる情報が様々なインシデント（自然災害を含む）によって損失するリスクに留意することが重要です。クラウドサービス上で行われるデータの冗長化に加えて、情報の重要性に応じたバックアップ手段を講じることが望まれます。

クラウドサービスプロバイダは、バックアップ方針を確立し、システム情報、ソフトウェア及びデータの全てのバックアップに関する組織の要求事項を定め、その内容をクラウドサービスカスタマと共有することが望まれます。また、想定する様々なインシデントに対して、システム全体を復旧させるために必要となるシステム情報、ソフトウェア及びデータの全てをバックアップ対象とし、インシデントの発生後でも、全ての重要な情報及びソフトウェアを回復できるように、適切なバックアップ設備を備えることが望まれます。 加えて、情報の消失を防ぐために、システム情報、ソフトウェア及びデータのバックアップを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れます。

クラウドサービスカスタマは、クラウドサービスプロバイダとの間で合意したバックアップ方針により取得したバックアップからデータを復元する一連のプロセスが、自組織の事業継続計画の要求事項を確実に満たすことを確認する必要があります。また、定められたプロセス通りに実施されていることを確認するために、試験方法を定めて定期的に試験することが望まれます。法令等の要求により永久保存する複製物が必要な情報については、保管期間を定めて情報が確実にバックアップされることが求められます。
詳細は JIS Q 27017 の 12.3.1「情報のバックアップ」を参照して下さい。

4） クラウドサービスの監視の不備

クラウド環境では、仮想マシンの起動・シャットダウンが頻繁に行われるため、サービス監視をネットワーク越しから行うことが困難です。そこで、クラウドサービスプロバイダでは、個々のホスト上で監視を行うことが望まれます。しかし、ホスト上で監視機能（ホストベースの IDS（不正侵入検知）など）を稼働させると、システムのパフォーマンスに影響を与える可能性が高く、本来の業務に支障が出るリスクが高まります。また、クラウド環境でクラウドサービスカスタマ向けに提供している管理画面では、監視可能な項目が限定されていることが多く、期待される監視項目が含まれていないことがあります。

クラウドサービスプロバイダは、クラウドサービスカスタマが利用するサービスやシステムの異常を素早く検知してシステムダウンを未然に防ぐために、クラウドサービスの稼働状況をクラウドサービスカスタマが監視できる機能を提供し、支援することが望まれます。

クラウドサービスカスタマは、クラウドサービスの稼働状況の監視項目及び監視方法をあらかじめ定めておくことが望まれます。必要とする監視項目及び監視方法が、クラウドサービスプロバイダが提供する監視機能では不十分な場合には、追加の監視ツールを自ら導入する等により、監視項目及び監視方法を補完する必要があります。また、運用するクラウドサービスの利用を許可したユーザの利用状況（誤用、悪用、マルウェア感染などの状況確認を含む）の監視手順を策定するために、利用状況の記録の種類、記録の表示方法、記録の保持期間などを、クラウドサービスプロバイダに確認することが望まれます。
詳細は JIS Q 27017 の CLD.12.4.5「クラウドサービスの監視」を参照して下さい。

４．２．２ 情報セキュリティリスク対応【JIS Q 27001 の 6.1.3】

クラウドサービスプロバイダ及びクラウドサービスカスタマは、クラウドコンピューティングの利用と運用に関わるリスクを特定し、リスク対応のためのプロセスを定め、適用する必要があります。リスク対応のためのプロセスに関しては、既に策定されている JIS Q 27001 に準じたプロセスと同様な活動をすることになります。
ここでは、JIS Q 27001 の 6.1.3 の要求事項を参考にしながら、その内容について説明します。

6.1.3 情報セキュリティリスク対応
組織は，次の事項を行うために，情報セキュリティリスク対応のプロセスを定め，適用しなければならない。
a) リスクアセスメントの結果を考慮して，適切な情報セキュリティリスク対応の選択肢を選定する。
b) 選定した情報セキュリティリスク対応の選択肢の実施に必要な全ての管理策を決定する。
注記 組織は，必要な管理策を設計するか，又は任意の情報源の中から管理策を特定することができる。
c) 6.1.3 b) で決定した管策を附属書 A に示す管理策と比較し，必要な管理策が見落とされていないことを検証する。
注記 1 附属書 A は，管理目的及び管理策の包括的なリストである。この規格の利用者は，必要な管理策の見落としがないことを確実にするために，附属書 A を参照することが求められている。
注記 2 管理目的は，選択した管理策に暗に含まれている。附属書 A に規定した管理目的及び管理策
は，全てを網羅してはいないため，追加の管理目的及び管理策が必要となる場合がある。
d) 次を含む適用宣言書を作成する。
– 必要な管理策［6.1.3 の b) 及び c) 参照］及びそれらの管理策を含めた理由
– それらの管理策を実施しているか否か
– 附属書 A に規定する管理策を除外した理由
e) 情報セキュリティリスク対応計画を策定する。
f) 情報セキュリティリスク対応計画及び残留している情報セキュリティリスクの受容について，リスク所有者の承認を得る。
組織は，情報セキュリティリスク対応のプロセスについての文書化した情報を保持しなければならない。
注記 この規格の情報セキュリティリスクアセスメント及びリスク対応のプロセスは，JIS Q 31000 に規定する原則及び一般的な指針と整合している。

（JIS Q 27001:2014 6.1.3 情報セキュリティリスク対応 より引用）

要求事項である 6.1.3 の主な内容は次の４点となります。

① リスクアセスメントの結果を考慮して、情報セキュリティリスク対応の選択肢を選定する
② 情報セキュリティリスク対応の選択肢の実施に必要な全ての管理策を決定する
③ 決定した管理策に見落としがないか、附属書 A に示す管理策と比較する
④ 適用宣言書を作成する

それぞれの項目について、どのような点に留意し、クラウドサービスに係るリスク対応をするかについて説明していきます。

① リスクアセスメントの結果を考慮して、情報セキュリティリスク対応の選択肢を選定する

この項目に対する留意点は次の 2 点となります。

a) リスクアセスメントの結果の相違

本ガイドで例示したクラウドサービス特有のリスクなどを参照し、想定される脅威などリスク源において抜けがないかを確認し、抜けがある場合は、そのリスク源におけるリスクアセスメントを実施することが必要となります。またリスクアセスメントの結果を、ISMS 活動におけるリスク対応プロセスにフィードバックしておく必要があります。

例えば、追加したリスクアセスメントの結果の部分だけを記録化し、リスク対応のためのプロセスへの報告を怠るといった状況は、望ましい活動ではありません。不足していたリスクアセスメントに関しては、従来のリスク対応の活動にフィードバックし、改善の機会として ISMS 全般の活動における情報セキュリティを向上させる必要があります。

b) リスク対応の選択

情報セキュリティリスク対応の選択肢（6.1.3a)）の項目には、違いは特にありません。

但し、クラウドサービスにおける情報セキュリティリスク対応では、特にクラウドサービスカスタマは、クラウドサービスプロバイダが提供するクラウドサービスの情報セキュリティに係る運用面に依存することも多く、クラウドサービスプカスタマが求めるセキュリティ要求とクラウドサービスプロバイダが提供する情報セキュリティとのギャップ（リスク）を埋めるためにクラウドサービスカスタマも ISMS の管理策を追加し対応する必要がある場合があります。

具体的に言えば、リスク対応の選択肢としては、「一つ以上の他者とリスクを共有すること（契約及びリスクファイナンシングを含む。」（「ISMS ユーザーズガイドリスクマネジメント編」参照）という選択肢から導かれる管理策、例えば「A15 供給者関係」などが参考となる管理策であり、これに関連する JIS Q 27017 の実施の手引が役立つと考えられます。

また、クラウドサービスプロバイダにおいては、提供するサービスについて、必要に応じてリスク対応の状況をクラウドサービスカスタマへ公開するという対応が必要となります。特にクラウドサービスプロバイダにおける提供するサービス運用に係るリスク対応は、サービスの品質、クラウドサービスカスタマとの SLA に関わる事項について開示することも多く、JIS Q 27017 に記載の管理策だけではなく、JIS Q 20000 などのサービスマネジメントに関する規格も参考になります。

②情報セキュリティリスク対応の選択肢の実施に必要な全ての管理策を決定する

この項目に対する留意点は次の点となります。

上記で記載したリスク対応の選択に伴い、不足していた管理策が存在するのであれば、それらについて決定することになります。また、前述したように、新たに決定した管理策については、その部

分だけを取り出しリスク対応とするのではなく、従来の ISMS の活動にフィードバックし、具体的な実装などを含むリスク対応計画にその内容を追記することが期待される活動になります。
JIS Q 27017 の管理策だけではなく、従来の JIS Q 27001 の管理策を強化するための見直しなどが必要となることがあります。

③決定した管理策に見落としがないか、附属書 A に示す管理策と比較する

この項目に対する留意点は次の点となります。

JIS Q 27001 の附属書 A に加え、JIS Q 27017 に記載の実施の手引を参考に、それぞれクラウドサービスカスタマ、クラウドサービスプロバイダまたは両方の立場から、必要な管理策を見落としていないかを、利用するまたは提供するクラウドサービス毎に確認する必要があります。
比較する際、附属書 A の管理策の記載は「～しなければならない」といった記載ですが、JIS Q 27017 は、JIS Q 27002 と同様、実践のための手引であるため「～望ましい」といった記載です。「～望ましい」といった記載内容では管理策を比較する際に、その内容について判断しかねるケースがでてくることがあります。そのような場合は、JIS Q 27001 の附属書 A と同様に「～しなければならない」調に読み替えて、決定した管理策と JIS Q 27017 の管理策を比較して下さい。

④適用宣言書を作成する

この項目に対する留意点は次の 3 点となります。

a) 適用宣言書には、クラウドサービスカスタマ、クラウドサービスプロバイダ、または両方の立場であることを明記する

適用宣言書を作成するにあたり、JIP-ISMS517 の附属書 A.3 適用宣言書（SoA）を参照し、関連するクラウドサービス毎に、クラウドサービスカスタマ、クラウドサービスプロバイダ、または両方の立場であることを明記する必要があります。

特に SaaS 事業者においては、提供する各クラウドサービスにおいて、クラウドサービスカスタマ、クラウドサービスプロバイダの両方の立場である場合には、そのことについて明記し、JIS Q 27017 に記載のクラウドサービスカスタマ及びクラウドサービスプロバイダに関連する管理策について採用・不採用について、適用宣言書に明記する必要があります。また、JIS Q 27017 に記載のクラウドサービスカスタマ及びクラウドサービスプロバイダに関連する管理策を除外した場合は、その理由について記載する必要があります。

b) 適用宣言書の記載方法

JIS Q 27017 に記載の管理策は、本文と附属書 A（規定）に大別されます。ここで、本文というのは、JIS Q 27002 の箇条 5 ～18、すなわち、JIS Q 27001 の附属書 A 5 ～A18 に関連付けられたクラウドサービスカスタマ及びクラウドサービスプロバイダ向けの管理策についての記載のことを指します。

JIS Q 27017 の附属書 A（規定）には、JIS Q 27002 の管理目的または管理策に記載のない、追加のクラウドサービス特有の管理策についての記載があります。これらの管理策について、適用宣言書において、その採用、不採用を記載する必要があります。JIS Q 27017

の本文にあたる管理策の採否については、従来の適用宣言書に記載された項目を拡張し、JIS Q 27017 の管理策の採否について記載することが可能です。

一方、JIS Q 27017 の附属書 A（規定）に記載の管理策は、もとより JIS Q 27002 または JIS Q 27001 の附属書 A に記載のない管理策であるため、従来の適用宣言書に、これらの項目を追記し、その採否について記載する必要があります。

留意する点として、JIS Q 27017 の本文にあたる管理策の採否を記載する際、もとより JIS Q 27017 は、JIS Q 27002 を補完する位置づけで作成された手引であることから、適用宣言書において、JIS Q 27001 では、採用していない管理策が、JIS Q 27017 で採用しているということにはならないということに留意して下さい。仮にそのようなケースに遭遇した場合は、再度 ISMS の活動に戻り、関連する附属書 A に記載の管理策が本当に不採用なのかを確認し、誤りであった場合は修正をする必要があります。

c) 適用宣言書は、クラウドサービス毎に作成する。
特に、クラウドサービスプロバイダである事業者は、IaaS、PaaS、SaaS といった立場におけるクラウドサービスや、クラウドコンピューティングの形態は同じであっても、管理策が異なる様々なアプリケーションを含むサービスを展開されていることが考えられます。

その際、展開されているクラウドサービス毎に、サービスカタログも異なり、実施している管理策も異なることが想定されますので、認証取得したいクラウドサービス毎に識別可能で、利用者に誤解を与えないようなように適用宣言書を作成する必要があります。

なお、作成にあたっては、JIS Q 27017 はクラウドサービスに必要なものを記載していることから、JIP-ISMS517 の 4.2.2 の注記 3 に「ISO/IEC 27017 に示す管理策は、クラウドサービスプロバイダ及びクラウドサービスカスタマに対する固有の管理策であるため、原則は全ての管理策の評価を実施することとなる。」と記載の通り、全ての管理策を評価し、採用・不採用を決定する必要があります。また、不採用や除外をする際にも、その理由を明記する必要があります。ただし、ISO/IEC 27017 はクラウド固有の追加の管理策をガイドとして示しているため、クラウドサービスの提供及び利用においては、管理策を不採用とする妥当な理由は限定的であろうと考えられます。こうした手続きを踏み認証取得されたクラウドサービスは、全ての利用者（クラウドサービスカスタマを含む全ての利用者という意味）にとって、当該サービスを利用するかを決定する際、認証の適用範囲に当該サービス名が記載されていることを確認することにより、信用に足るサービスであるかを判定する際に役立つことが期待されます。

４．３ 内部監査【JIS Q 27001 の 9.2】

JIS Q 27017 では内部監査について明確に記載されている項目はありません。これらの記載（要求事項）については、JIP-ISMS517 に記載の内部監査の項目を確認する必要があります。一方、JIP-ISMS517 は、前提となる JIS Q 27001 の要求事項と比較し、ISMS クラウドセキュリティ認証にあたり、補完すべき項目についてのみの記載となっています。

したがって、ISMS のパフォーマンス評価等は ISMS クラウドセキュリティ認証においても重要な要素であり、必須項目ですが、その要求事項は、JIS Q 27001 をベースとした ISMS 認証が前提となっているため、JIP-ISMS517 には例えば、マネジメントレビューなどについての追記がありません。しかしながら、ISMS クラウドセキュリティ認証を取得時には、既存の ISMS の活動の中に、クラウドサービスに係るマネジメントシステムのパフォーマンス評価を含めておく必要があります。一方、JIS Q 27001 の「パフォーマンス評価」に関する要求事項についての詳細は、ISMS ユーザーズガイドの 9 章「パフォーマンス評価」の項を参照して下さい。

このように、クラウドサービスにおける情報セキュリティマネジメントの活動についても、ISMS 全体の活動と統合させ、マネジメントレビューにフィードバックするためにも、定期的に内部監査を実施し、トップマネジメントによるマネジメントレビューを実施し、今後の活動における方向性を決定するためにも、次の項目を検討することが重要です。

a）前回までのマネジメントレビューの結果とった処置の状況
b）ISMS に関連する外部及び内部の課題の変化
c）次に示す傾向を含めた，情報セキュリティパフォーマンスに関するフィードバック
　1）不適合及び是正処置
　2）監視及び測定の結果
　3）監査結果
　4）情報セキュリティ目的の達成
d）利害関係者からのフィードバック
e）リスクアセスメントの結果及びリスク対応計画の状況
f）継続的改善の機会

（JIS Q 27001:2014　9.3 マネジメントレビューより引用）

「b）ISMS に関連する外部及び内部の課題の変化」、「e）リスクアセスメントの結果及びリスク対応計画の状況」は本追補の４．２の結果をインプットとして使用できます。
クラウドサービスプロバイダ、クラウドサービスカスタマの立場としての利害関係が生じるため、「d）利害関係者からのフィードバック」は考慮することが必要になります。
また、「c）次に示す傾向を含めた，情報セキュリティパフォーマンスに関するフィードバック」の多くは、内部監査の結果からインプットされます。

上記の様々な‘フィードバック’を含む、マネジメントレビューへのインプットの内容に伴い、トップマネジメントは、次の要求事項に従い、クラウドサービスにおける情報セキュリティマネジメントの活動を含む ISMS の活動全般にわたる改善の機会や変更点に関する決定について、情報セキュリティに係る責任者に明確な指示を明示する必要があります。

マネジメントレビューからのアウトプットには、継続的改善の機会、及び ISMS のあらゆる変更の必要性に関する決定を含めなければならない。
組織は、マネジメントレビューの結果の証拠として、文書化した情報を保持しなければならない。

（JIS Q 27001:2014　9.3 マネジメントレビューより引用）

特に、クラウドサービスプロバイダ側におけるマネジメントレビューのアウトプットに関しては、提供するクラウドサービスの運用に係るリスク対策への指針を表すこととなり、単なる機密性の向上のみならず、サービス全体の品質や信頼（可用性、完全性等の側面）に係る、クラウドサービス全体の質の向上につながるアウトプットを策定することが期待されます。また、これらの指針は、場合によっては顧客に開示し、提供しているクラウドサービスの今後の展開についての説明として用いることも可能となります。

５．IT 発展に伴う新たなリスク

ISMS クラウドセキュリティ認証では、クラウドサービスカスタマ及びクラウドサービスプロバイダに対し、クラウドサービスを利用／提供するにあたり、従来型の情報システム（オンプレミス環境）に加えて、クラウド特有のサービスまでその管理策を広げ、適切なクラウドサービスの提供及び利用に広げることを目的としました。一方、IT の進歩はめざましいものがあり、そうした新しい IT は、クラウドコンピューティング環境で展開されることとなり、ISMS が適用範囲とすべき環境に対しても順次取り入れられることが想定されます。

例えば、政府が掲げる「働き方改革」に関連して、クラウドサービスを活用したテレワークや在宅勤務が普及しつつあり、情報システムの利用端末が職場以外のサテライトオフィスや自宅などに配置されるといった事例が増えてきました。こうした働き方の変化は、業務で利用する IT 環境にも変化をもたらします。従来は全ての IT 機器が会社支給であったのに対し、個人所有の機器を業務で使用する BYOD（Bring Your Own Device）等の環境のもと、組織の情報を共有するといった利用も増えています。また、サテライトオフィスや自宅などで BYOD を活用し、情報を共有するなどのケースも増えています。電子化された情報を、クラウドコンピューティングを活用して利用するケースが増える一方、情報が職場以外の場所に拡散するリスクもあります。

また、IoT(Internet of Things)の進展に伴い、産業分野における IT 環境にも変化が出始めています。多数のセンサーが工場や屋外の環境に設置され、それらが直接情報システムに接続されるようになってきました。インターネットとの接続を前提としてセキュリティ対策を強化した情報システムと、クローズドシステム（例えば、インターネットとは接続しないシステム）として運用されてきた工場等のシステムが接続されることで、想定すべきリスクや対策も大きく変化しています。加えて、昨今では人工知能(AI)が大きく進展しています。従来は人手で行ってきた情報システムの操作の一部が自動化されることも想定されます。このことにより、これまで人手での操作を想定して各種対策を行ってきた業務に対して、人工知能(AI)を前提とした対策を組み入れる必要が出てきます。

こうした IT の発展に伴う変化には、新たなリスクが生じるという負の面だけではなく、新しい IT を取り入れることでリスクの軽減が図られる面も含まれています。クラウドサービスの利用についても、クラウドサービス固有のリスクが生じる可能性はありますが、IT 資産をクラウドサービスで統治することで、これまで以上に企業のガバナンスを利かせることができる可能性があります。新しい IT を情報システムに取り入れる際には、それらがどのようなリスクや好機をもたらすのかを、十分に吟味する必要があります。新しいサービスや情報システムに固有のリスクを適切に把握し、そうしたリスクを含めたリスクマネジメントを行うことが重要です。

近年ではほとんどの企業の業務が IT に依存しており、サイバーセキュリティインシデントによる被害が、企業経営に対する重大課題となっています。企業経営を健全に保つための企業戦略として、適切なリスクマネジメントを行う上でのセキュリティ投資が必要です。事業継続性の確保やサイバー攻撃に対する防衛力の向上による企業価値向上のためには、どの程度のセキュリティ投資をすべきか等、経営判断が求められる時代となっています。

ISMS 専門部会　ISMS ユーザーズガイドの拡張検討ワーキンググループ

（順不同・敬称略）

氏名	会社・機関名
【主査】 駒瀬　彰彦	株式会社アズジェント
河野 省二	日本マイクロソフト株式会社
澤部 直太	株式会社三菱総合研究所
中村 良和	日本マネジメントシステム認証機関協議会 （BSI グループジャパン株式会社）

ISMS 専門部会

（順不同・敬称略）

氏名	会社・機関名
【主査】 駒瀬　彰彦	株式会社アズジェント
相羽　律子	株式会社日立製作所 情報・通信システム社
河野 省二	日本マイクロソフト株式会社
笹原英司	デロイト　トーマツ　リスクサービス株式会社
佐藤　慶浩	オフィス四々十六
澤部 直太	株式会社三菱総合研究所
中村 良和	日本マネジメントシステム認証機関協議会 （BSI グループジャパン株式会社）

ISMS-AC
情報マネジメントシステム認定センター
〒106-0032 東京都港区六本木１丁目９番９号 六本木ファーストビル
一般財団法人 日本情報経済社会推進協会内
TEL 03-5860-7570 FAX 03-5573-0564
URL https://isms.jp/