開催レポート

クラウドサービス利用に潜むリスクとは

～カスタマにおける ISMS クラウドセキュリティ認証取得の必要性～

モデレータ　JIPDEC ISMS 専門部会主査　駒瀬 彰彦 氏

パネリスト　広島大学情報メディア教育研究センター センター長　西村 浩二 氏

稲垣隆一法律事務所 弁護士　稲垣 隆一 氏

日本マネジメントシステム認証機関協議会

情報技術委員会委員長 中村 良和 氏

ISMS 認証企業がクラウドサービスのリスクを特定する際、クラウドを利用する上でのクラウドサービスカスタマ（CSC）の視点で見たリスクと、クラウドサービスを社内展開する、または取引先企業に提供するプロバイダとしての視点から見た運用リスクを考慮する必要があります。

2020 年 2 月 20 日に開催された ISMS セミナー「クラウドサービス利用に潜むリスクとは」のパネルディスカッションでは、広島大学におけるクラウド化の取り組みを事例に、モデレータ JIPDEC ISMS 専門部会主査 駒瀬 彰彦氏の進行で、広島大学情報メディア教育研究センター センター長 西村 浩二氏、稲垣隆一法律事務所 弁護士 稲垣 隆一氏、日本マネジメントシステム認証機関協議会 情報技術委員会委員長 中村 良和氏にクラウドサービスの利用検討のポイントやリスクへの対応、さらにカスタマとして ISMS クラウドセキュリティ認証を取得することの意義を議論していただきました。

本レポートでは、JIPDEC 事務局が要約した当日のディスカッション内容をご紹介します。
（当日の全プログラムの内容はこちら（セミナー告知ページへのリンク）をご覧ください(本レポートも講演レポートと同じ扱いにする場合)）

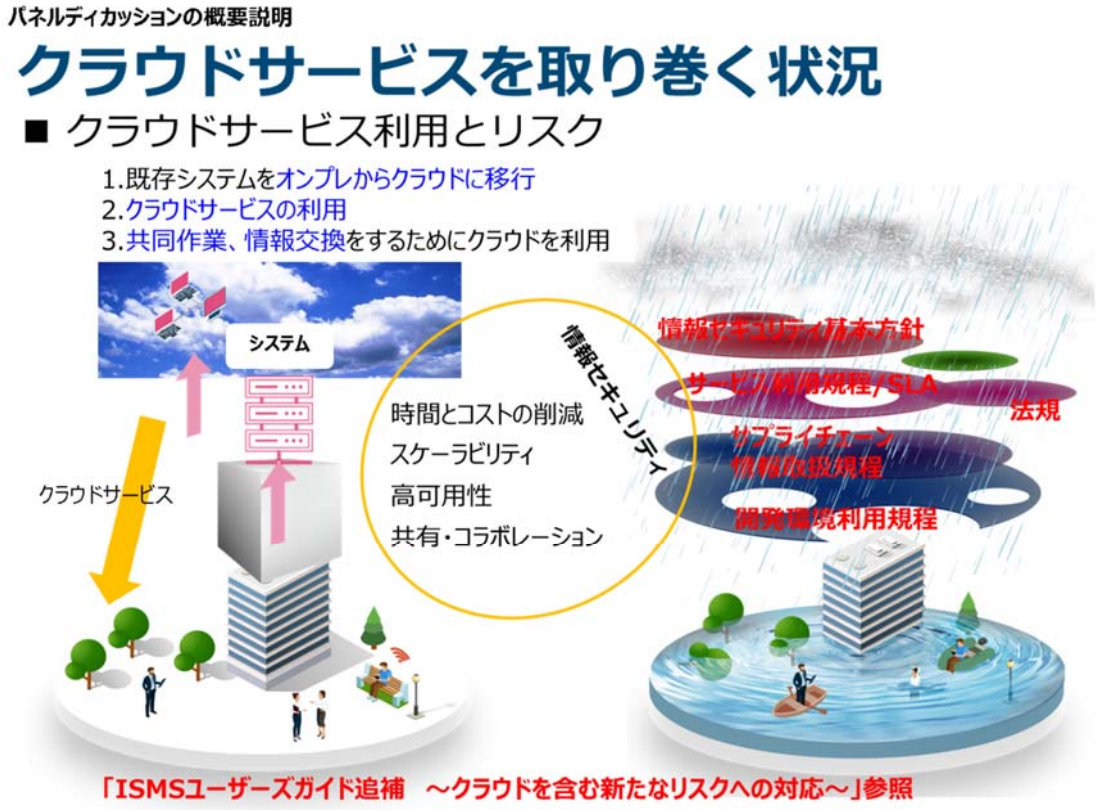
■クラウドサービスを取り巻く環境　～サービス利用におけるリスク～

現在、ビジネスにおいてクラウドサービスの利用が本格化してきている。システム運用の面からはコストダウンと拡張の容易性が期待され、利用面からは、利便性の高いサービスが利用できる点や、働き方改革への対応としてリモート環境構築、共同開発や情報交換の業務効率向上等のニーズが高まり、導入が進んでいる。

一方で、従来のオンプレミスで運用していたシステムとは設計・構築・運用環境も介在する当事者も異なるため、情報セキュリティという観点から当事者間の責任の分掌等を明確にしておかなければ、Society5.0 に向けてリスクが顕在化し、事業全体に大きな影響を与える。クラウド化がもたらすメリット（時間・コスト削減、スケーラビリティ、高可用性、コラボレーション容易性等）が変化の部分であり、その部分の情報セキュリティリスクとその対策を検討する必要がある。クラウドサービス利用におけるリスクとしては、

- 自社の情報セキュリティポリシー違反
- 利用するクラウドサービス障害による業務停止
- 情報の取り扱いに関するガバナンスの喪失
- サプライチェーン、外部委託先管理の喪失
- 適用法令の違いからくるデータの差し押さえ

等が挙げられる。



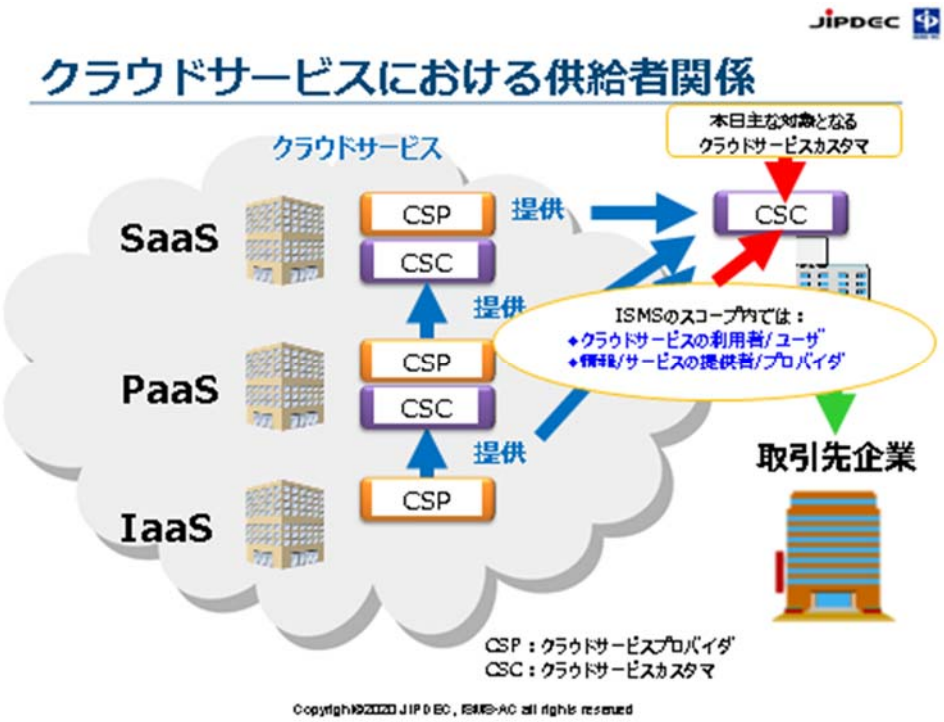
■ISO/IEC 27017 と ISMS クラウドセキュリティ認証

こうしたクラウド特有のリスクを管理するための国際的な規範が ISO/IEC 27017 であり、この規格をベースにした認証が ISMS クラウドセキュリティ認証である。ISO/IEC 27017 そのものはガイドラインであり認証基準ではないことから、ISO/IEC 27017 に基づく認証基準※が JIPDEC により作成されており、ISMS 認証を前提とし、その上でクラウドを利

用する際のセキュリティ管理の審査を行う追加の認証として ISMS クラウドセキュリティ認証が実施されている。

この ISMS クラウドセキュリティ認証では、その基となる ISO/IEC 27017 に従って、プロバイダの立場としてだけでなく、カスタマの立場でも認証を受けることができる。

※認証基準：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）



今回は、特にカスタマの立場での ISMS クラウドセキュリティ認証を取得された広島大学における事例を中心に、ISMS の視点におけるクラウドサービスの利用に関する考慮すべきリスク等についてパネルディスカッションを行った。

■広島大学におけるクラウド化

✧　検討の指標

広島大学は、2012 年度から開始したクラウド化への取り組みの中で、2017 年 3 月に大学として初めて ISMS クラウドセキュリティ認証を取得した。取り組み開始当時、経営層にはコストダウンとしてクラウド利用に対する期待が高まっていた。また、システム管理部門では、従来の大学システムに不必要な部分を高コストと捉えていたが、刷新するまでには至っていなかった。そこに、ハードウェア置換えのタイミングが重なったため、CIO からクラウド利用検討の指示があり、具体的な移行を検討することとなった。

移行にあたっては、環境変化を望まない関係者の理解も促す必要がある。広島大学では、まずは学内のクラウドに対する偏見をなくすため、誰もが客観的に判断できるようなガイドライン、チェックリストを作成し、冷静に各自がメリット・デメリットを正しく判断できる状況を作ることで、クラウド化に対する合意形成を進めていった。

✧　クラウドサービス信頼度の評価基準

広島大学が策定したクラウドサービス利用ガイドラインでは、

①独立性の高さ（他の利用者との隔離）

②アクセス制御（データアクセスのための利用者認証）
③通信路の安全性（暗号化とアクセス区域の制限）
においてオンプレミス同様の対策が取られているかを信頼度の評価軸とし、それぞれに運用面も含めた詳細な要件を明示している。これに情報ごとに重要度を分析しその結果を紐づけることで、保存したい情報の重要度レベルごとに利用可能なクラウドサービスの判断基準を明確にした。

広島大学のアプローチは、通常の ISMS で行われる資産ベースの整理とは異なるが、ISMS では特に「この手法でなければならない」という決まりがあるわけではない。それぞれの組織が、自らが捉えたリスクに対し適切にリスクアセスメントを行い、その結果が組織として有効なものとなることが重要となる。

■クラウドサービスカスタマにおけるリスク

✧　クラウドサービスのカスタマに求められる力 ～ 責任分掌の把握 ～

オンプレミスからクラウドサービスに移行することで、調達の際の仕様も変化する。オンプレミスの場合はハードウェア機能も要件となるため、調達側が求める仕様に合致するハードウェアをサービス提供側が提案することが多いが、クラウドでは利用条件や監視・監督の関与度合いが調達要件となるため、サービス提供側からの提案ベースとなることが多い。このため、カスタマ側は提案内容の妥当性を判断する力を必要とされる。

日本では、クラウド環境にシステムを構築する場合、SIer を介する場合が多い。カスタマとプロバイダが直接交渉する場合は、プロバイダ側も責任を明確にする必要があるためリスク開示を含め詳細を確認できるが、その間に SIer が入ることにより、概念・定義が不明確で理解に齟齬が生じた状態で契約となってしまう可能性がある。これを避けるためにもカスタマ側には、契約相手に関わらず提案内容を判断できる能力が求められる。

また、審査における視点としては、広島大学が取得したクラウドサービスカスタマとしての ISMS クラウドセキュリティ認証では、どこまでがカスタマとプロバイダの責任分界点なのかを明確に理解しているか、経営陣がリスクをどのように認識しているか、が重要なポイントとなる。SIer はクラウドサービスプロバイダではないため、SIer との関係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関係にはならない。そのため SIer との関係は、ISMS クラウドセキュリティ認証の範疇ではなく、ISMS における委託先との関係（供給者管理）の中でリスクアセスメントに基づき整理することが必要になる。

✧　SaaS 利用に際して

クラウド利用において、IaaS は実際のサービス部分は自組織での運用となるため、ユーザの制御が比較的容易だが、SaaS の場合、どこまで利用制限をかけるか、またユーザを監視するかが問題になる。

広島大学では、大学として認めているものが Office365 と OneDrive のみで、それ以外のサービスについては、担当者本人がチェックリストで情報の重要性と使用するサービスのリスクを確認した上で利用している。ただし、２万人の学生・教職員に対し、毎年セキュリティ教育、試験を実施し、試験に合格しない限りアカウントが利用できない仕組みを取り、実効性の確保に努めている。このような仕組みを整備した結果、セキュリティインシデントも大幅に減少した。

法律的に考えると、本来、大学でも学生でも、企業の従業員でも、自分が接続する相手とは契約関係が成立しており、契約相手が予定しない危害を加えてはならないことになっている。また、現在、接続先や接続主体が複雑化し、接続の方向によっては契約関係における立ち位置も複雑に変化している。学生や従業員との関係では単純に契約上の問題

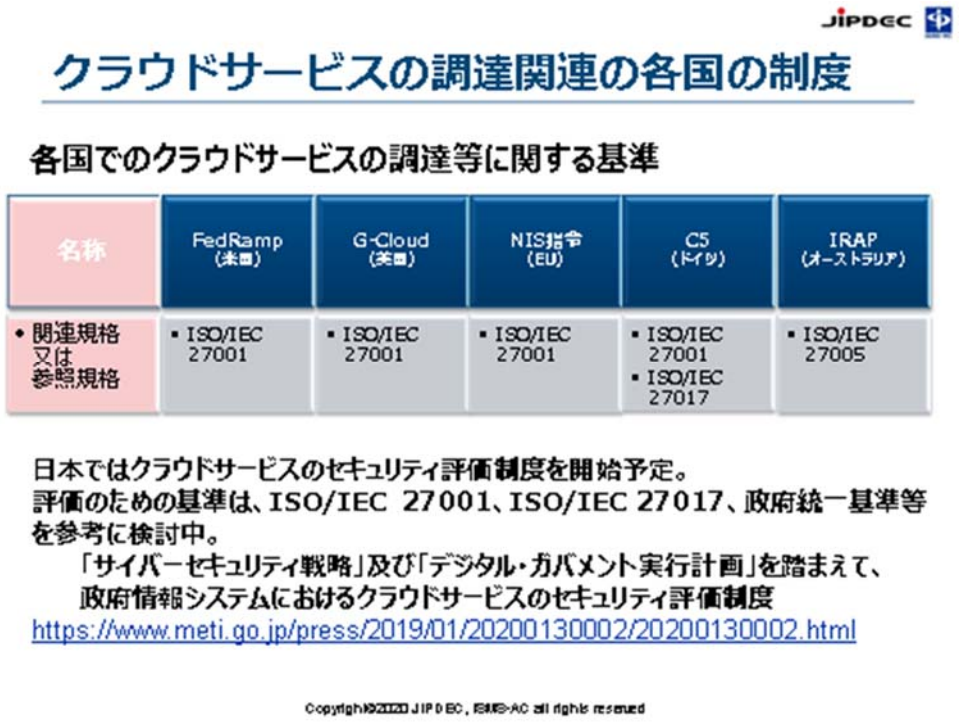
として処理することもできない中で、何をしたらよいかという点は明確になっておらず、今後の課題であろう。

ISO/IEC 27017 は、このような状況で対処すべき点が整理されているので、ガイドとして有用である。さらに、自らが取り組んでいるという事実を第三者の認証を得ることで、対外的な説明責任を果たすこともできる。

■クラウドサービス利用における、ISMS クラウドセキュリティ認証の役割

ISMS クラウドセキュリティ認証の対象となるクラウドサービスカスタマは、組織のクラウドサービス管理者を指している。クラウドサービスのユーザはあくまでも Office365 などのクラウドサービスを利用する者であり、ユーザ管理の在り方を認証するのは ISO/IEC 27001 に基づく ISMS 本体となる。

日本から提案して ISO/IEC で審議・発行された ISO/IEC 27017 は、世界の国、企業、あらゆる組織がクラウドへの期待と情報セキュリティガバナンスの喪失を懸念している中、複雑なサプライチェーンを構成するクラウドサービスにおいて、関係者間の役割・責任について理解・整理する意味でも非常に参考となる規格である。JIPDEC が公開している ISMS ユーザーズガイドの追補部分※で、クラウド利用のマネジメントに関する詳細が解説されているので、国内外の多くの企業に活用してもらいたい。



※ 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～
クラウドサービスに関連する国内外の制度・ガイドラインの紹介

その他参考情報：

「ISMS 認証に関するガイド類」

「ISMS クラウドセキュリティ認証」（ISMS-AC）