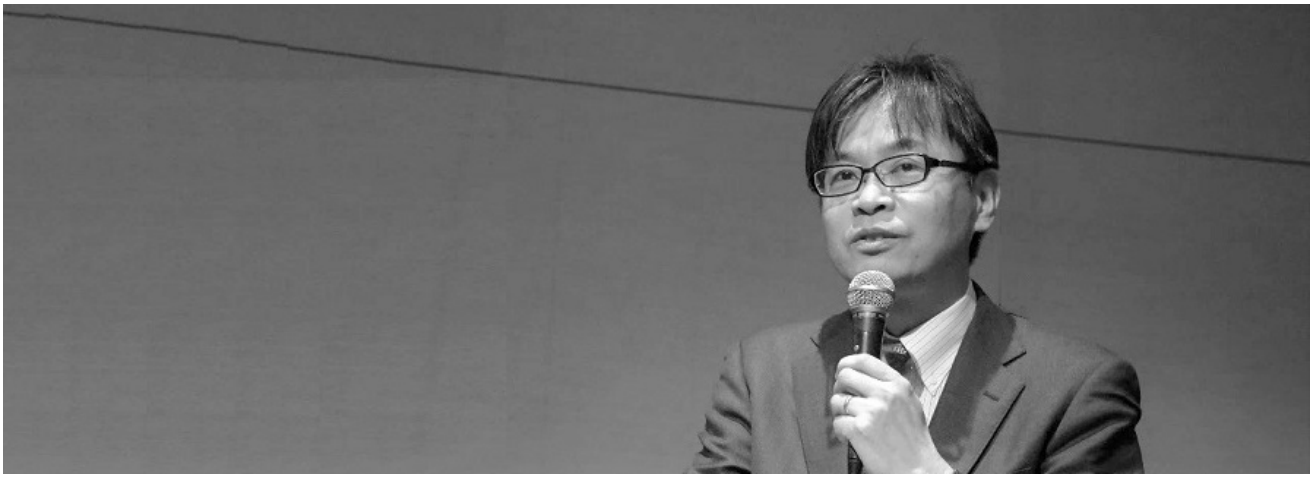
講演レポート

広島大学におけるクラウド化手順と ISMS の取り組み

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



広島大学は、構成員が約２万人で、地方としては大規模な総合大学である。また、よく言われることだが、大学は中小企業経営者の集まりのようなもので、全体で何かを進めていくことが非常に難しい環境となっている。

しかし、広島大学は、2017 年に日本の大学として初めて ISMS クラウドセキュリティ認証（クラウドサービスカスタマとしての認証）を取得した。本日は、大学のクラウド化推進の取り組みや、クラウドサービス選定・利用のために策定したガイドラインの内容、ISMS クラウドセキュリティ認証取得に至った経緯などを紹介したい。

■クラウドサービス利用の取り組み

クラウドサービスの利用を始めたきっかけは、コスト削減を期待する経営層からの要請と、クラウドサービスの利便性を知った利用者側からの要望という双方向からの声を受けてのことである。一方で、実際に導入するにはどのように調達するのかといった課題や、大学ネットワークへはこれまでは大学設置の PC からの接続に限られていたものが、BYOD の推進によって学生の私物 PC 等からも接続可能になることによってガバナンスが効かなくなる恐れがあるという課題もあった。さらに個人情報保護法やサイバーセキュリティ基本法等が制定され、組織としての責任は増大傾向にあり、このような状況の中でクラウドサービスを利用していくには、ガバナンスを維持するための対策を講じることが必要であった。

■「広島大学クラウドサービス利用ガイドライン」整備の背景

実際にクラウドサービスの選定に際して気付いたのは、例えばプライベートクラウド等の言葉の意味や対象がメーカや SIer といった事業者によって異なってるということだった。そのため、事業者とのやりとりでの齟齬をなくすためには、それぞれの言葉の定義を揃える必要があった。

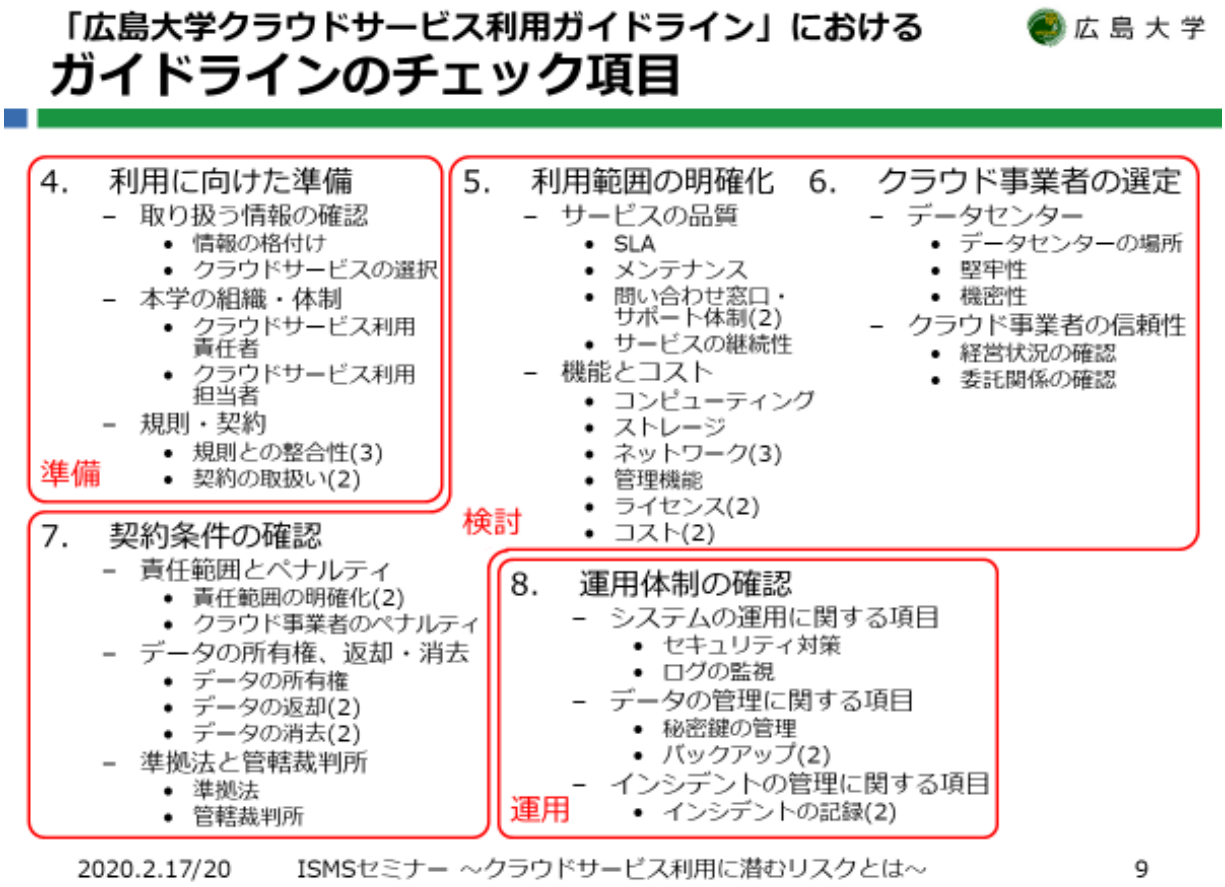
また、クラウド利用にあたって大学のセキュリティポリシーとの整合性も考慮する必要があると考えていたところ、2011 年度頃から、「どのサービスなら使ってよいか（例えば、Dropbox で大学の情報を扱ってよいか？）」「ダメな使い方はどのようなものがあるか」等、セキュリティポリシーとの関係に関する利用者からの問合せが急増してきた。

このような背景から、2012 年度に１年かけて「具体的、わかりやすい、実行可能」なガイドラインを目指して検討を進

め、2013 年 3 月に「広島大学クラウドサービス利用ガイドライン」の第一版を公開した。その後、見直しを重ね、これまで 2 回改訂しているが、内容そのものの大きな変更はない。最新版は、2017 年 8 月に公開した第三版である。

■ガイドラインの構成・ポイント

このガイドラインは 8 章で構成されている。1～3 章は、ガイドラインの目的・位置づけや構成、また、クラウドサービス自体の説明やクラウドサービス利用における主な要件等について記載している。4～8 章は、準備段階（4 章）、検討段階（5～7 章）、運用段階（8 章）と、クラウドサービス導入の段階に分けて構成されている。これらの章では、クラウドサービスの利用を決める前に知っておきたいリスクと、それを回避するために確認しておくべき内容について解説している。また、別紙のチェックリストは 4 章以降の解説に合わせた構成になっているので、このチェックリストを用いることによってこのガイドラインに沿って比較的簡単にクラウドの点検が行えるようになっている。

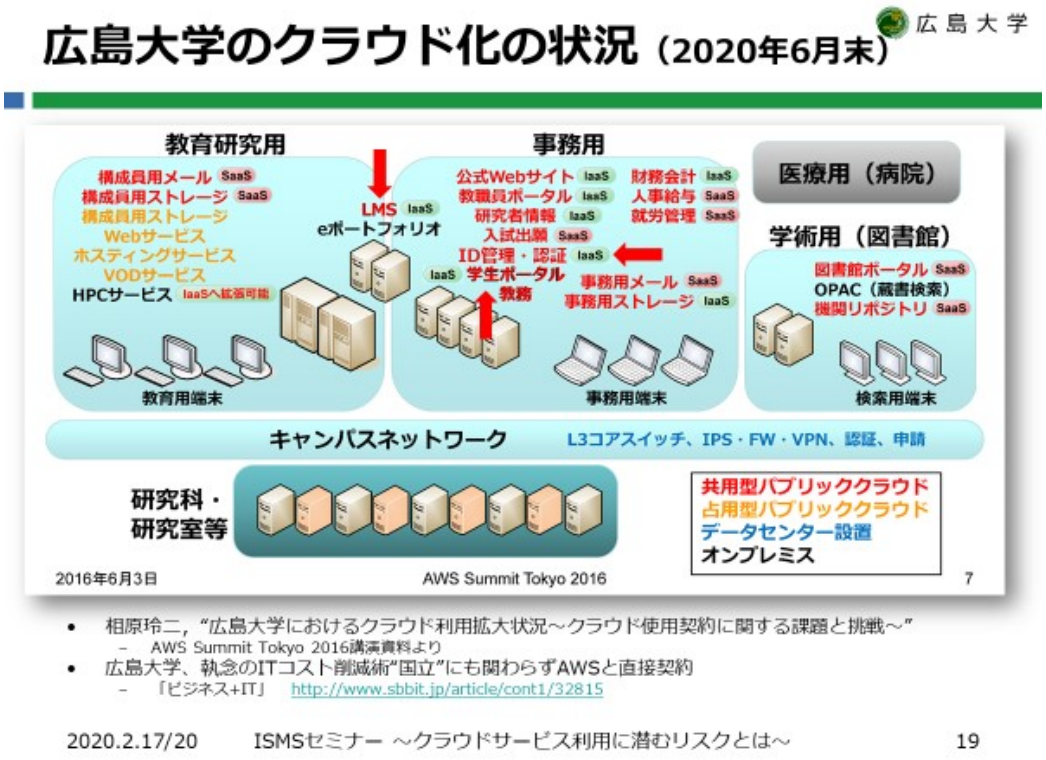


4～7 章の準備段階・検討段階で、セキュリティポリシーの確認や責任者の明確化、求めるサービスレベルやセキュリティ要件、契約条件の確認等をチェックできる内容となっているが、本ガイドラインではさらに踏み込んで、選定したクラウドサービスの運用体制についても 8 章にチェック項目として盛り込み、機能面だけでなく運用体制まで意識した利用を促している。

■広島大学のクラウド化

このガイドラインを整備することによって、全学のシステム担当者レベルでの確認・判断が可能となったことから、ガイドラインを活用して、最初に、既存の財務会計システムを IaaS で、人事給与システムを SaaS でクラウド化した。

一方で、事務系と教研（教育研究）系の情報担当部署が異なるため、認証連携システムのクラウド化については後回しとなっているが、まず事務系システムのクラウド化を進めている。現在は学生ポータルの移行作業を実施しており、事務系システムについては、クラウド化をほぼ完了させたところである。



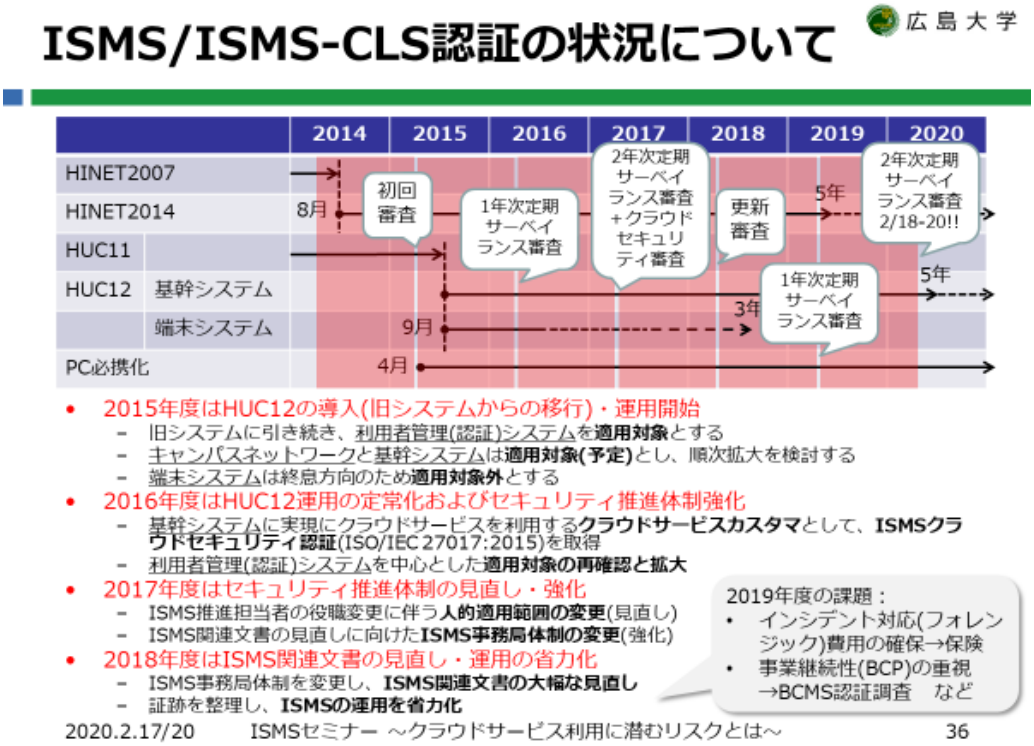
- 相原玲二，“広島大学におけるクラウド利用拡大状況～クラウド使用契約に関する課題と挑戦～”
  - AWS Summit Tokyo 2016講演資料より
- 広島大学、執念のITコスト削減術“国立”にも関わらずAWSと直接契約
  - 「ビジネス+IT」 http://www.sbbit.jp/article/cont1/32815

2020.2.17/20　ISMSセミナー ～クラウドサービス利用に潜むリスクとは～　19

また、ガイドラインを策定したことによって、確認すべきポイント（問題点）が明確になり、これまで安全神話化して手をつけにくかったオンプレミスの安全性についても徹底的にクラウドと比較確認を実施することができた。さらに、クラウド化したことにより、システム調達もハードウェア指向からサービス指向へとシフトしていったため、システム構築手法見直しの契機となった。

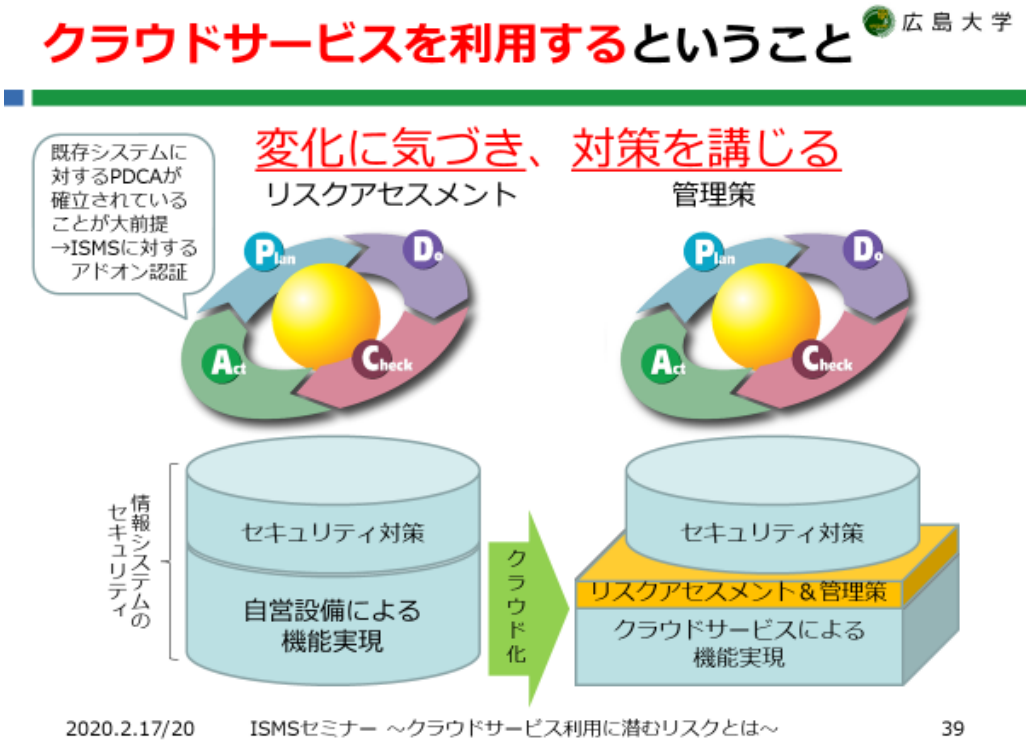
■広島大学における ISMS/ISMS-CLS の取り組み

認証の取り組みとしては、広島大学情報メディア教育研究センターとして、2014 年度末に ISMS 認証を取得し、その後 2017 年 3 月に ISMS クラウドセキュリティ認証（ISMS-CLS 認証）を取得した。ISMS 認証取得後は、毎年見直しを行い、継続的に審査を受けており、2019 年度はインシデント対応（フォレンジック）費用、事業継続性（BCP）の確保を課題として ISMS の運用を行った。



認証の範囲は、情報メディア教育研究センターで管理している電算システムのうち利用者情報・サービス情報に関わる部分にしている。ただ、実質的にはそこに誰がアクセスするか、どのように利用するか、までを管理するとしているためシステム全体を網羅できるようになっている。対象範囲を絞り、ISMS 認証取得・維持への対応をシンプルにしつつ、システム全体の設計・調達・運用方法が適切かどうかを ISMS クラウドセキュリティ認証の仕組みを使って確認している。

クラウド化によって、これまですべてオンプレミスに実施していたセキュリティ対策が、きれいにカバーできなくなるという変化が生じる。しかし、クラウドの観点でのリスクアセスメントを実施することによってこうした変化に気づき、そのアセスメント結果に沿ってクラウド利用におけるリスク対策（管理策）を講じることが、クラウドセキュリティを確保することだと捉えている。私たちの取り組みでは、まず既存システムに対する PDCA を ISMS で確立し、クラウド移行に伴って見直した PDCA を ISMS 認証に追加して審査・認証される ISMS クラウドセキュリティ認証で確認することで、オンプレミスからクラウド化したことで生まれた変化（ギャップ）に対応している。



■「クラウド化」の先に見えたもの

今回、私たちが行ったクラウド化の多くは、IaaS（ハードウェアの置換え）での移行であったことから、ハード構成・リソースをそのままに外部へ移行すること＝クラウドを使いこなしている、といえるのかと感じている。また、クラウドサービスで提供される多種多様な機能を適切に選んで利用できているのか、適切なリサイジングを行う必要があるのではないか、自分で好きなように行っていた運用方法も見直す必要があるのではないか、という点も今後の課題であると感じている。

また、このようなクラウド化の場合は容易である一方で、ハードウェア更新のタイミングがなくなるため見直しの機会が失われ、固定化（サイロ化）しやすいという問題がある。しかし、ISMS/ISMS-CLS 認証を維持すること（＝毎年の審査を受けること）は、この失われた「機会」の代わりとなり、有効であると考えている。