ISMSクラウドセキュリティ認証の受審報告

情報メディア教育研究センター
西村 浩二

大学等におけるクラウドサービス利用シンポジウム2017

2年前の報告

広島大学

ISMS（情報セキュリティマネジメントシステム）

広島大学

- 情報メディア教育研究センターでISMS認証を取得
  - 基本方針（一部）
    - センターは情報セキュリティの主要3要素である機密性・完全性・可用性の確保に努める
    - 特に、本学構成員に提供している情報サービスの可用性、またセンターで管理している個人情報および認証情報の機密性をより確実なものとする
  - 登録範囲
    - 情報メディア教育研究センターにおける情報サービスのための利用者／認証情報の管理・運用
  - 適用規格
    - ISO/IEC 27001:2013 (JIS Q 27001:2014)

⇒年度内取得見込み
- 本審査（平成27年3月2～4日）
- 判定委員会（平成27年3月27日予定）

2015/3/20　大学等におけるクラウドサービス利用シンポジウム2015　34

ISMS認証取得の表示

広島大学

http://www.media.hiroshima-u.ac.jp/

ISMS認証取得の取り組み

広島大学

登録範囲

ISO/IEC27001:2013（JIS Q 27001:2014）
情報メディア教育研究センターにおける情報サービスのための利用者／認証情報の管理・運用
登録情報（JIPDECへ）

JIP-ISMS517-1.0
次のクラウドサービスのクラウドサービスカスタマとしての利用に係るISMSクラウドセキュリティマネジメントシステム
・Microsoft Azure、Office 365 Education
・Hitachi Cloud：エンタープライズクラウドサービス、出前クラウドサービス、フェデレーテッドクラウド

記念写真

登録証を手にする情報メディア教育研究センター長（CIO）

これを印刷

HINET2014

検索
サイトを検索 検索

メディアセンター入門
広島大学 クラウドサービス 利用ガイドライン
情報セキュリティ・コンプライアンス教育
セキュリティ情報
IMCサービス稼働情報
ICE端末利用状況
ICE端末利用状況 For Mobile

ISMS認証取得
ISO/IEC 27001:2013
JIS Q 27001:2014
（情報メディア教育研究センター）

言語を選択
Powered by Google 翻訳

広島大学情報メディア教育研究センター Copyright © Information Media Center, Hiroshima University, all rights reserved.

http://www.media.hiroshima-u.ac.jp/news/isms/

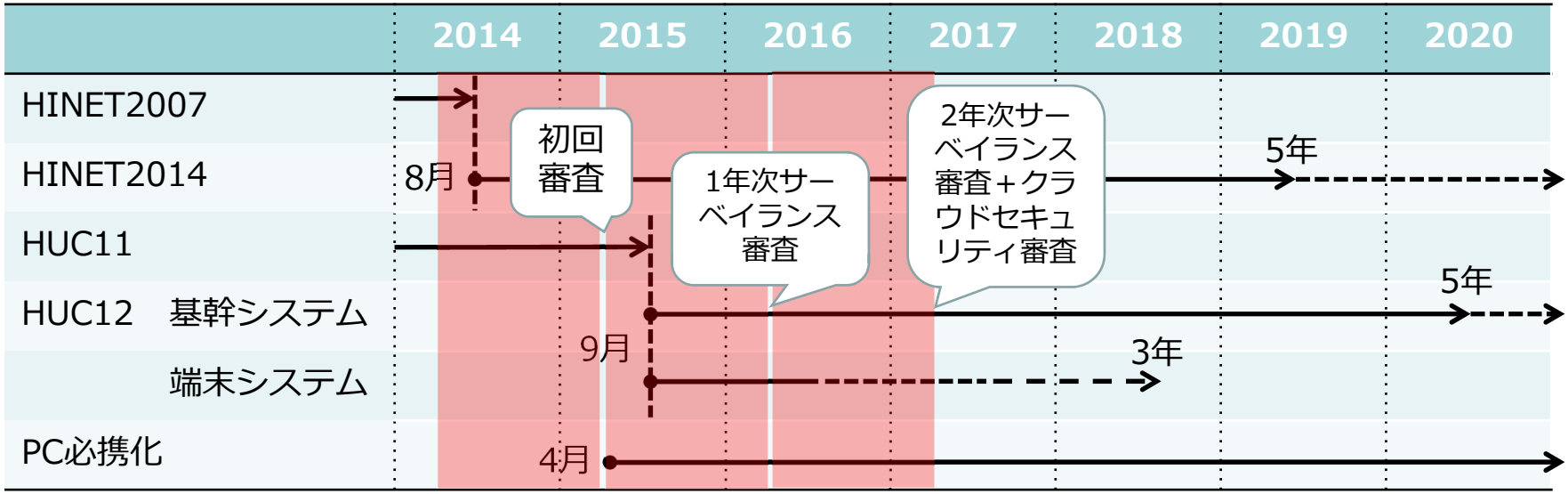
情報メディア教育研究センターについて

広島大学

- 日本語名称（略称）
  - 情報メディア教育研究センター（メディアセンター）
- 英語名称（略称）
  - Information Media Center（IMC）
- 目的（広島大学情報メディア教育研究センター規則第２条）
  - センターは，広島大学(以下「本学」という。)の学内共同教育研究施設として，本学の情報通信基盤を支え，情報メディアを活用した教育の企画・立案・実施の支援及び業務への支援を行い，情報メディア活用のための研究開発の推進を図ることを目的とする。
- 沿革
  - 情報メディア教育研究センター（2001年4月～）
    - 4センターを統合
      - 総合情報処理センター（1962年4月～）
      - 情報教育研究センター（1996年10月～）
      - 外国語教育研究センター（1997年4月～2004年3月）
      - 情報メディア教育研究霞センター（1999年10月～）
    - 外国語教育研究センターが分離独立（2004年4月～）

メディアセンターの状況について

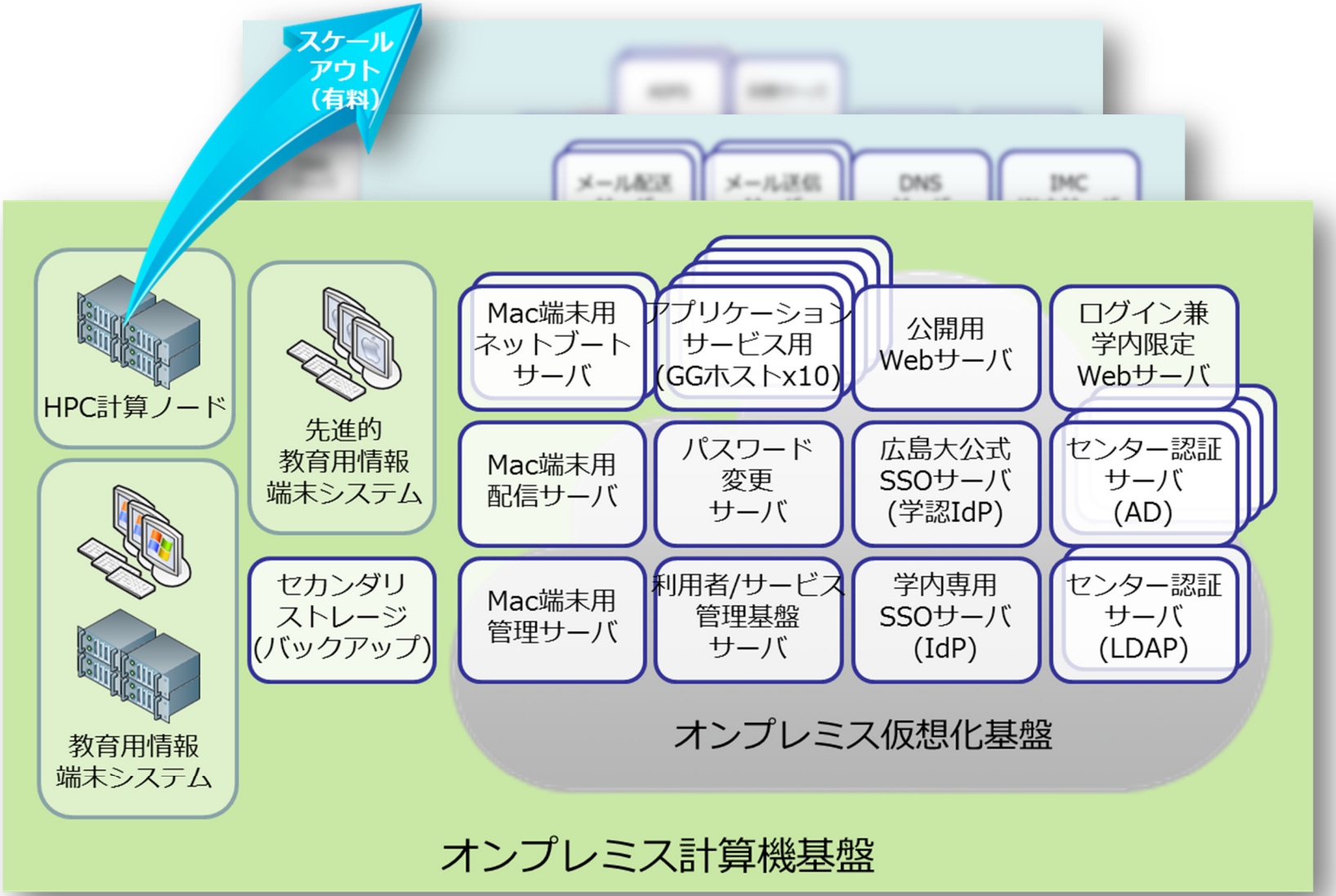
広島大学



- メディアセンターシステムの管理・運用を取り巻く状況
  - HINET2014は2014年8月運用開始（1年目）
  - PC必携化は2015年度新入生（2015年4月）より開始
  - HUC12は2015年9月運用開始（HUC11は2015年8月末運用終了）
    - 基幹システムの運用期間は5年間
    - 端末システムは3年後に終息予定（PC必携化の進捗状況により判断）
- 2016年度はHUC12運用の定常化およびセキュリティ体制強化
  - 利用者管理（認証）システムを中心とした**適用対象の再確認と拡大**
  - **クラウドサービスカスタマ**として、**ISMSクラウドセキュリティ認証**（ISO/IEC 27017:2015）の取得

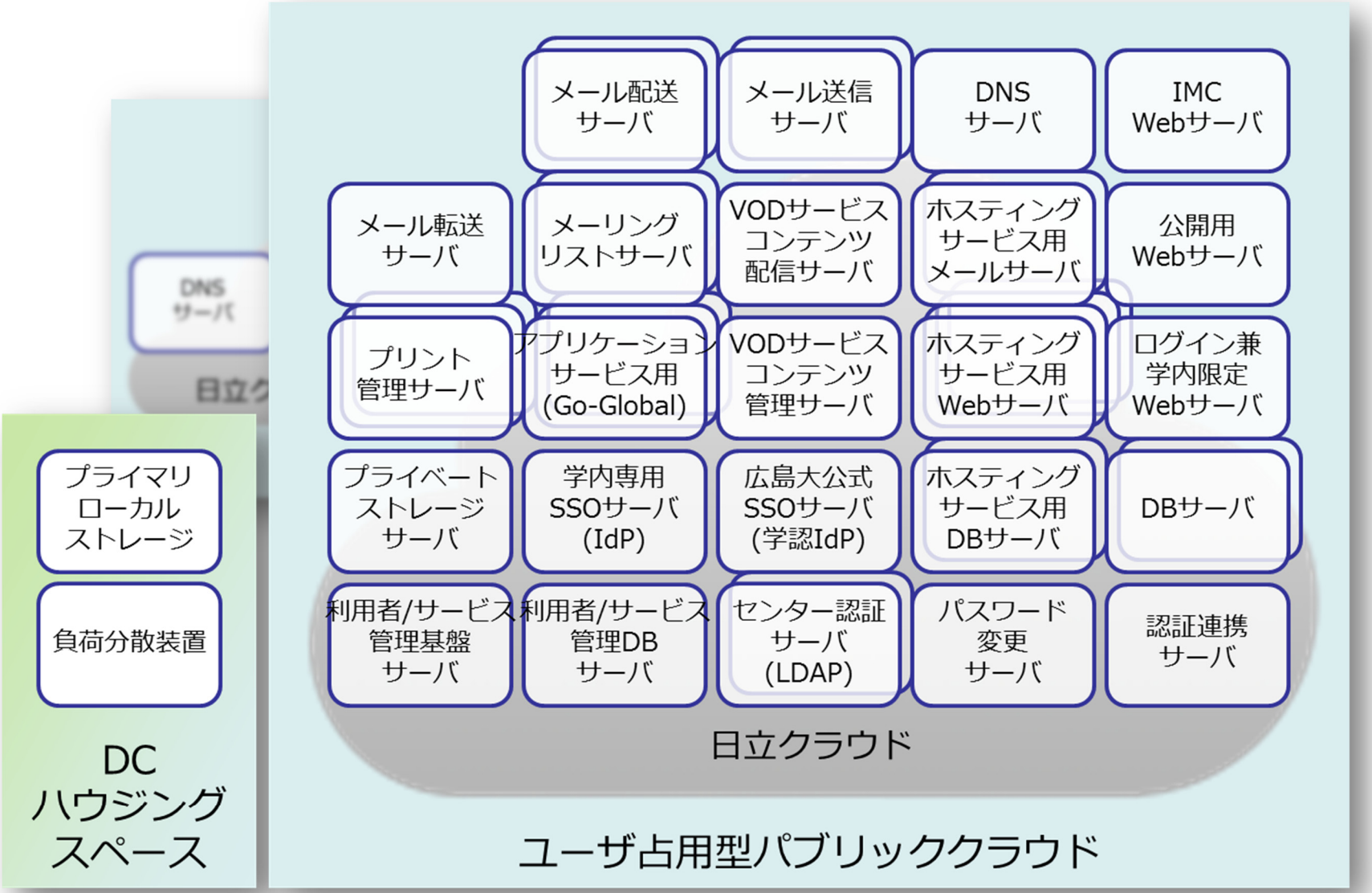
HUC12構成（オンプレミス計算機／仮想化基盤）

広島大学

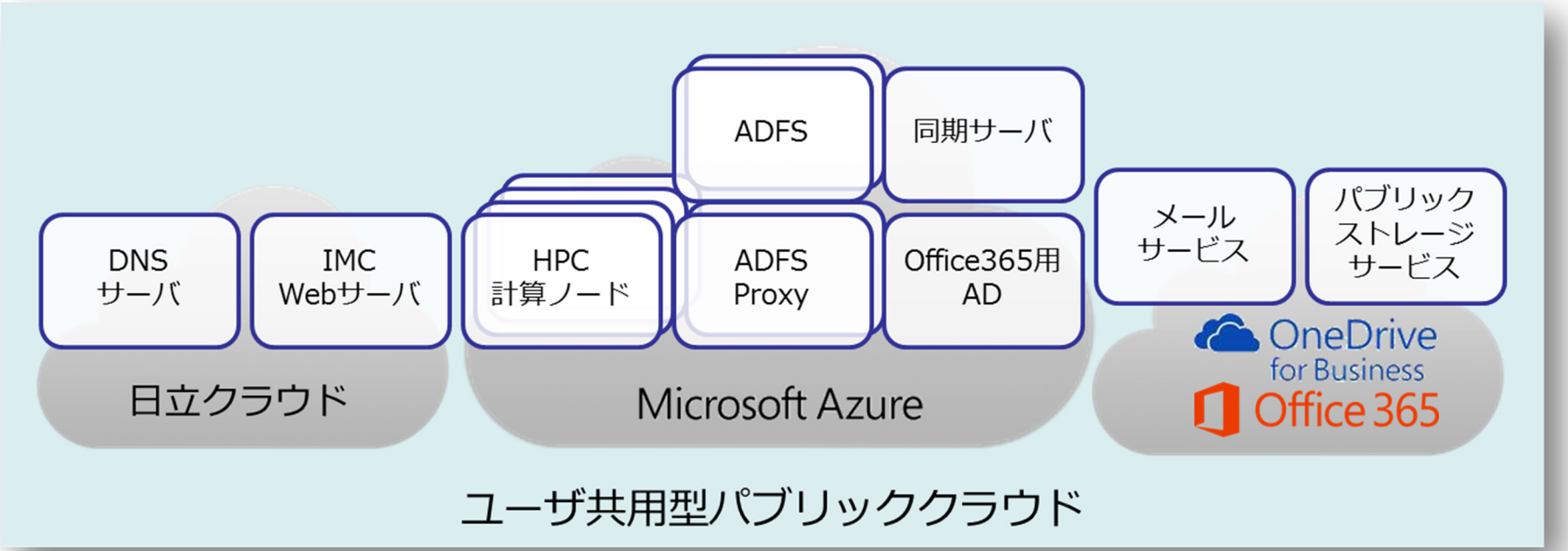


HUC12構成（ユーザ占用型パブリッククラウド）

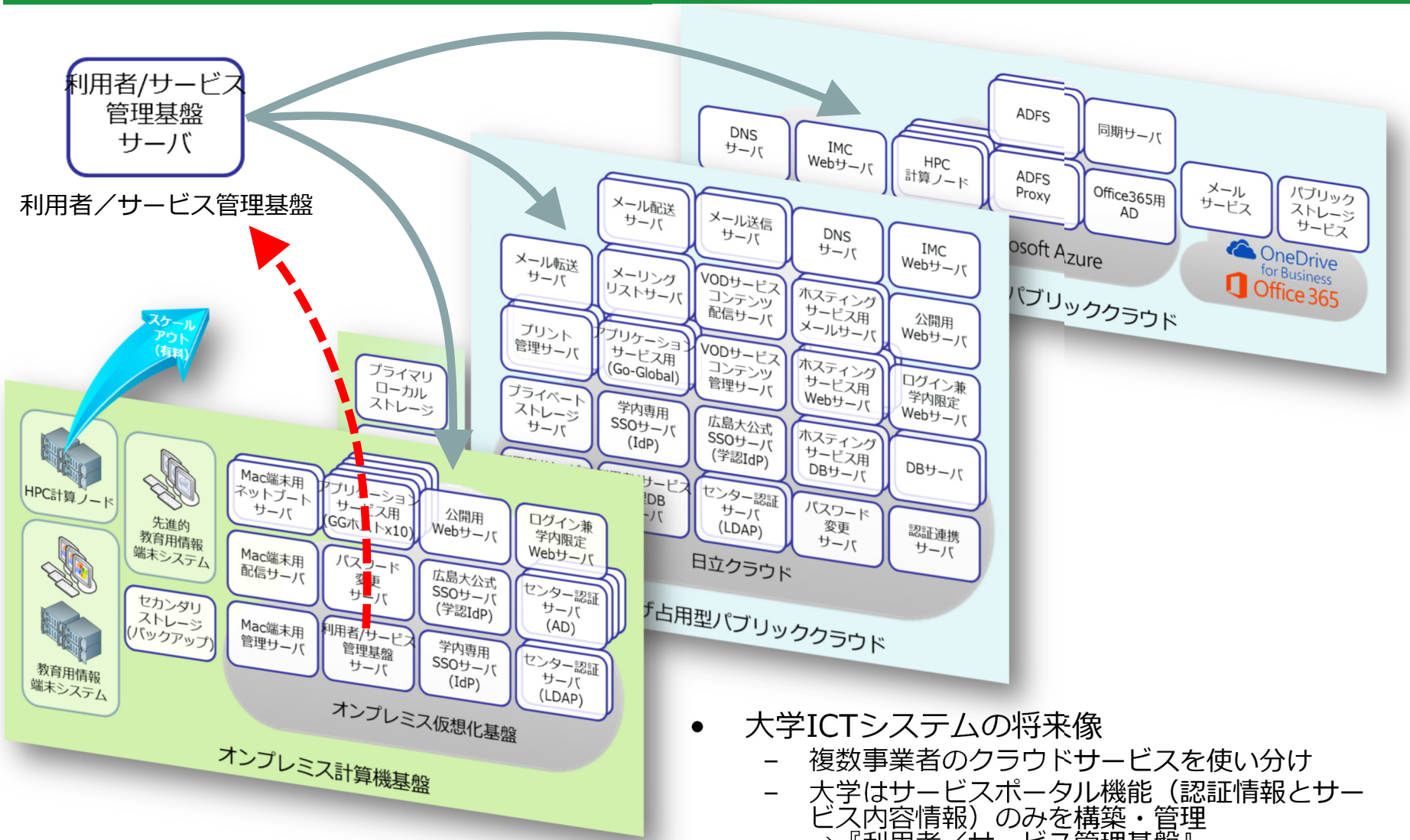
広島大学



HUC12構成（ユーザ共用型パブリッククラウド）



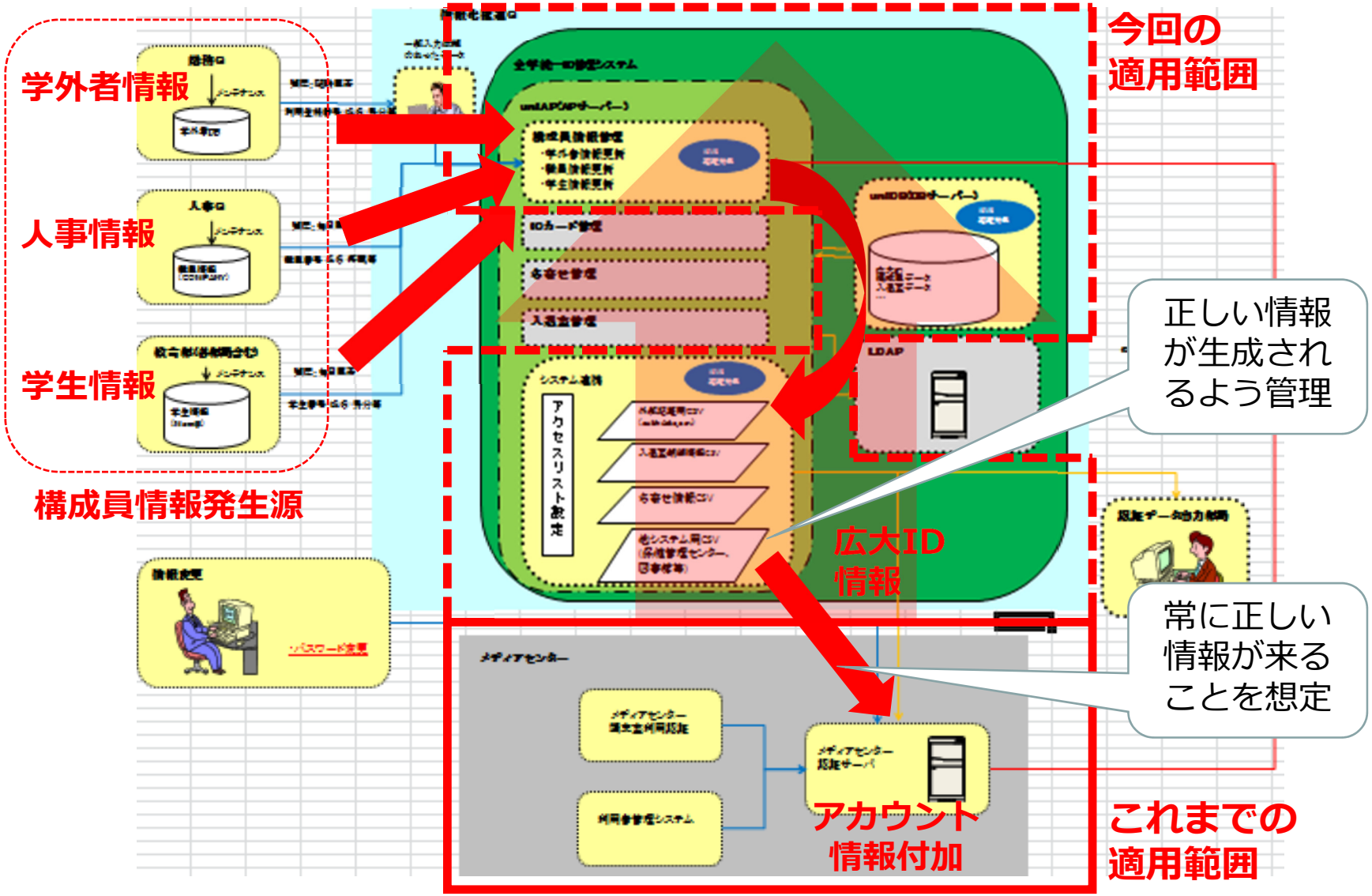
HUC12全体構成(2017年2月現在)



- 大学ICTシステムの将来像
  - 複数事業者のクラウドサービスを使い分け
  - 大学はサービスポータル機能（認証情報とサービス内容情報）のみを構築・管理
    →『利用者／サービス管理基盤』

適用範囲拡大の考え方
～利用者管理(認証)情報の流れを遡る～

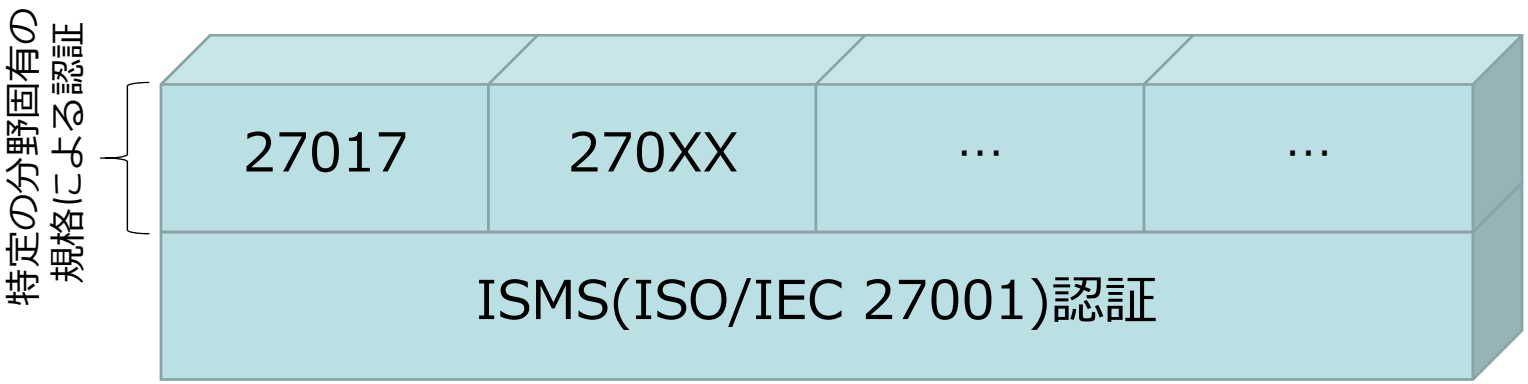
広島大学



ISMSクラウドセキュリティ認証制度とは

広島大学

- ISO/IEC 27001のアドオン認証としての認証登録制度
  - 一般社団法人　日本情報経済社会推進協会 (JIPDEC) ISMS適合性評価制度における
    - ISMSクラウドセキュリティ認証の認証基準、及び認証基準の概要
    - ISMS認証機関認定基準及び指針 JIP-ISAC100-3.1
    - 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



ISO/IEC 27001要求事項との関係

広島大学

ISO/IEC 27001　情報セキュリティマネジメントシステム―要求事項

ISO/IEC 27000 本文
マネジメントプロセス要求

ISO/IEC 27001 附属書A
管理目的と管理策

JIP-ISMS517-1.0
ISMSクラウドセキュリティ認証に関する要求事項

管理策実践の規範を認証要求事項に変換

クラウド固有要素を拡張

クラウド固有要素を追加

ISO/IEC 27017:2015　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

ISO/IEC 27017 本文

①ISO/IEC 27002を参照

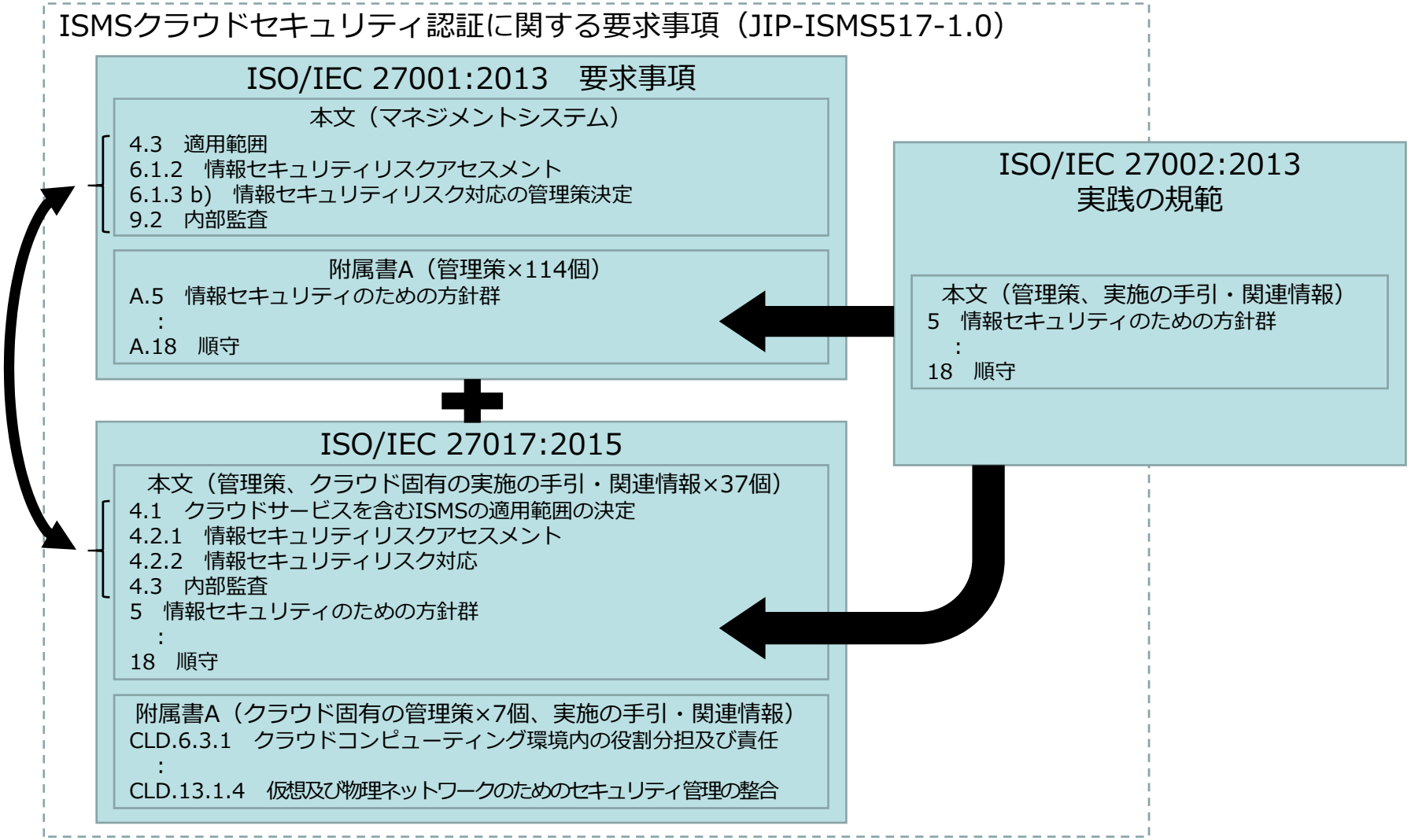
②クラウド固有の実施の手引、関連情報を追加

ISO/IEC 27002 情報セキュリティ管理策の実践のための規範
管理目的と管理策、実施の手引、関連情報

＋ クラウド固有の管理策の追加

ISO/IEC 27017 附属書A
クラウド固有の管理目的と管理策、実施の手引、関連情報を追加

JIP-ISMS517-1.0の構造



カスタマとプロバイダの立場を区別

広島大学

外部の
クラウド
サービス
プロバイダ

サービス
利用

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組織で、
利用に際しての情報セキュリティを
ISMSクラウドセキュリティ認証に
よって確保したい組織

クラウドサービスプロバイダ

クラウドサービスを提供する組織で、
提供に際しての情報セキュリティを
ISMSクラウドセキュリティ認証に
よって確保したい組織

サービス
提供

外部の
クラウド
サービス
カスタマ

外部の
クラウド
サービス
プロバイダ

サービス
利用

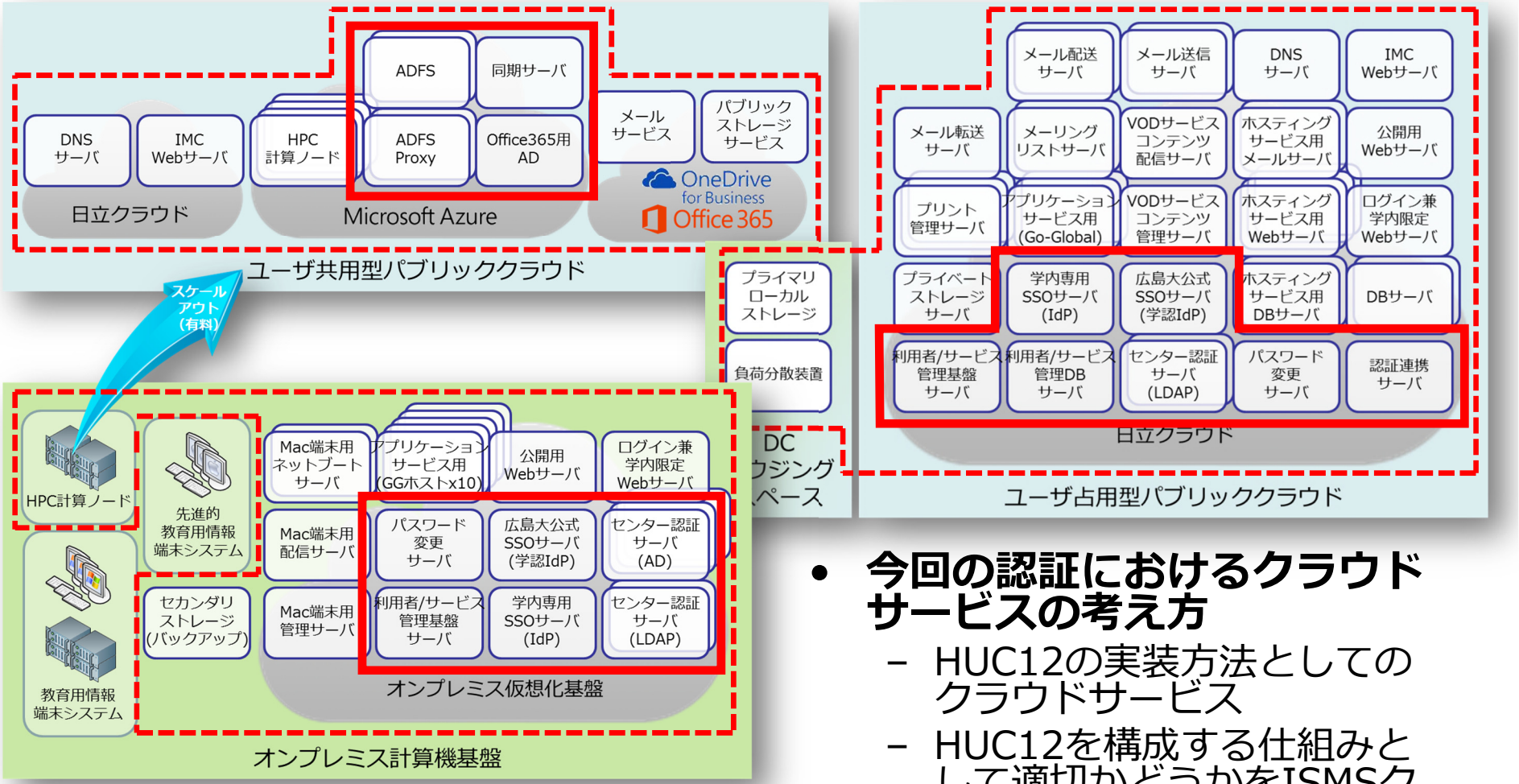
**クラウドサービスカスタマ＆
クラウドサービスプロバイダ**

他の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提供する
組織で、利用及び提供の情報セキュ
リティをISMSクラウドセキュリティ
認証によって確保したい組織

サービス
提供

外部の
クラウド
サービス
カスタマ

適用範囲（ISMS+CLD）



- **今回の認証におけるクラウドサービスの考え方**
  - HUC12の実装方法としてのクラウドサービス
  - HUC12を構成する仕組みとして適切かどうかをISMSクラウドセキュリティの仕組みを用いて確認する

広島大学クラウドサービス利用ガイドライン・チェックリスト

広島大学

クラウドサービス利用ガイドライン　チェックリスト

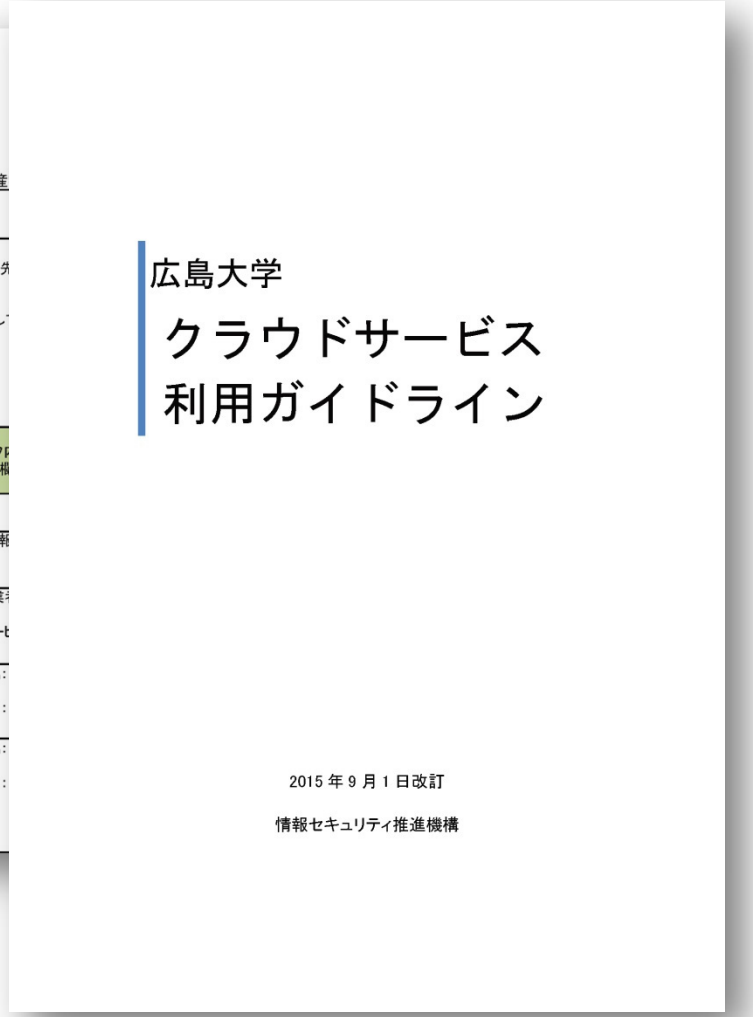
チェックリスト提出先：学術・社会産

確認情報　実施日：＿＿＿＿＿＿　対象等：＿＿＿＿＿＿

記入者情報　所属：＿＿＿＿＿＿　氏名：＿＿＿＿＿＿　連絡先

チェックリストの使い方
1. チェック欄は、空欄：未確認　○：確認した、基準をクリアしている　△：確認したが利用しない　×：基準をクリアしていない　のいずれかを選択し
2. チェック内容メモ欄は、確認した内容の備忘録として利用してください（項目名が入っている欄は必ず記入してください）。
3. 文書管理者（グループリーダー、支援室長等）への報告の際にご利用ください。
4. クラウドサービスの類型によって、確認すべき項目が異なります。
5. 導入前および導入後1年を超えない期間ごとに確認を行い、その結果を情報化推進グループ（上記参照）に提出してください。
6. クラウドサービスの利用状況の把握やインシデント対応等のため、内容について説明を求められることがあります。

ガイドライン見出し	ガイドライン小見出し	ガイドライン	No.	チェック欄	ガイドラインチェック項目	チェックメモ欄
4. 利用に向けた準備（必須確認項目）						
4.1. 取り扱う情報の確認	情報の格付け	どの情報をクラウドサービス上に保存するのか（どの業務をクラウドサービスに移行するのか）を検討します。	1		保存する情報の重要度は明確になっていますか？（ガイドライン表1参照）	保存する情報
	クラウドサービスの選択	クラウドサービス利用基準に照らして、情報の重要度に応じたクラウドサービスを選択します。	2		クラウドサービス利用基準を満たしていますか？（ガイドライン図3参照）	クラウド事業者 クラウドサービ
4.2. 本学の組織・体制	クラウドサービス利用責任者	クラウドサービスの利用に関する責任者を決めます。責任者が不明だと、契約事項の確認やインシデント発生時の対応が難しくなります。	3		クラウドサービスの利用について、本学側の責任者が明確になっていますか？	責任者所属： 責任者氏名：
	クラウドサービス利用担当者	クラウドサービス事業者との窓口となる担当者を決めます。担当者は、クラウドサービス事業者との連絡のほか、ユーザアカウントの登録や削除、利用マニュアルの整備や指導、ヘルプデスクなどの業務を担当します。	4		クラウドサービスの利用について、本学側の担当者を指名していますか？また担当者は、利用するクラウドサービスの機能について理解していますか？	担当者所属： 担当者氏名：



広島大学

クラウドサービス
利用ガイドライン

2015 年 9 月 1 日改訂

情報セキュリティ推進機構

- 第二版（2015（平成27）年9月1日改訂）
- チェックリスト
  - ガイドラインチェック項目：46個
  - 詳細チェック項目：88個　　（それぞれ最大．サービス類型により異なる）

ガイドライン整備の流れ

広島大学

広島大学情報セキュリティポリシー
（2005年（平成17年）～）

- クラウドコンピューティングの概要と推奨事項
- クラウドコンピューティング
  情報セキュリティに関わる利点・リスクおよび推奨事項
- 中小企業のためのクラウドサービス安全利用の手引き
  クラウド事業者による情報開示の参照ガイド
- 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

↓

広島大学クラウドサービス利用ガイドライン・チェックリスト
第一版（2013年（平成25年）3月15日策定）

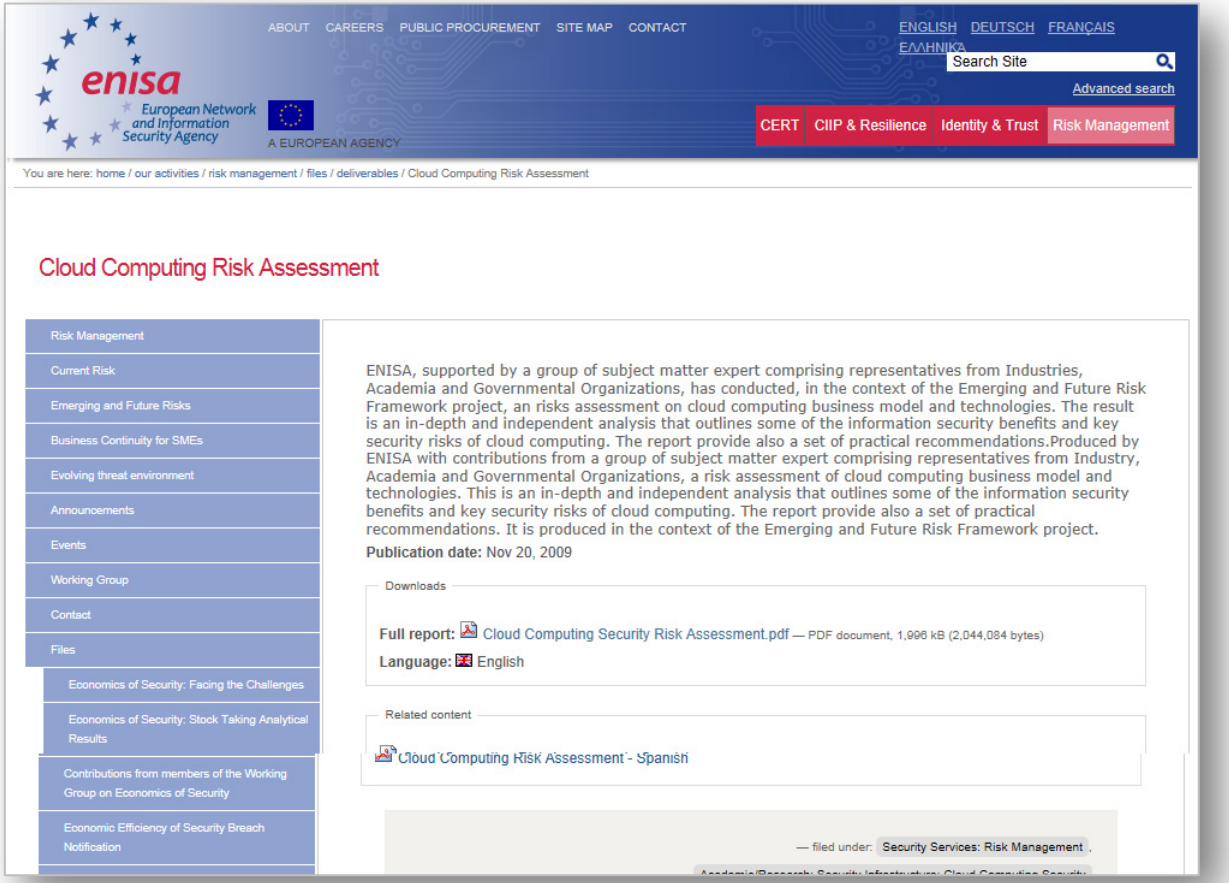
↓

広島大学クラウドサービス利用ガイドライン・チェックリスト
第二版（2015年（平成27年）9月1日改訂）

↓

クラウドコンピューティング
情報セキュリティに関わる利点・リスクおよび推奨事項

広島大学



- http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment
- http://www.ipa.go.jp/security/publications/enisa/documents/Cloud%20Computing%20Security%20Risk%20Assessment.pdf（日本語訳）

リスク項目 (R1～R35)

広島大学

- ポリシーと組織関連のリスク
  - (R1) ロックイン
  - (R2) ガバナンスの喪失
  - (R3) コンプライアンスの課題
  - (R4) 他の共同利用者の行為による信頼の喪失
  - (R5) クラウドサービスの終了または障害
  - (R6) クラウドプロバイダの買収
  - (R7) サプライチェーンにおける障害
- 技術関連のリスク
  - (R8) リソースの枯渇（リソース割当の過不足）
  - (R9) 隔離の失敗
  - (R10) クラウドプロバイダ従事者の不正－特権の悪用
  - (R11) 管理用インタフェースの悪用（操作、インフラストラクチャアクセス）
  - (R12) データ転送途上における攻撃
  - (R13) データ漏えい（アップロード時、ダウンロード時、クラウド間転送）
  - (R14) セキュリティが確保されていない、または不完全なデータ削除
  - (R15) DDoS攻撃（分散サービス運用妨害攻撃）
  - (R16) EDoS攻撃（経済的な損失を狙ったサービス運用妨害攻撃）
  - (R17) 暗号鍵の喪失
  - (R18) 不正な探査またはスキャンの実施
  - (R19) サービスエンジンの侵害
  - (R20) 利用者側の強化手順と、クラウド環境との間に生じる矛盾
- 法的なリスク
  - (R21) 証拠提出命令と電子証拠開示
  - (R22) 司法権の違いから来るリスク
  - (R23) データ保護に関するリスク
  - (R24) ライセンスに関するリスク
- クラウドに特化していないリスク
  - (R25) ネットワークの途絶
  - (R26) ネットワークの管理（ネットワークの混雑、接続ミス、適切でない使用）
  - (R27) ネットワークトラフィックの改変
  - (R28) 特権の（勝手な）拡大
  - (R29) ソーシャルエンジニアリング攻撃（なりすまし）
  - (R30) 運用ログの喪失または改ざん
  - (R31) セキュリティログの喪失または改ざん（フォレンジック捜査の操作）
  - (R32) バックアップの喪失、盗難
  - (R33) 構内への無権限アクセス（装置その他の設備への物理的アクセスを含む）
  - (R34) コンピュータ設備の盗難
  - (R35) 自然災害

ガイドラインのチェック項目

広島大学

4. 利用に向けた準備
- 取り扱う情報の確認
  - 情報の格付け
  - クラウドサービスの選択
- 本学の組織・体制
  - クラウドサービス利用責任者
  - クラウドサービス利用担当者
- 規則・契約
  - 規則との整合性(3)
  - 契約の取扱い(2)

準備

5. 利用範囲の明確化
- サービスの品質
  - SLA
  - メンテナンス
  - 問い合わせ窓口・サポート体制(2)
  - サービスの継続性
- 機能とコスト
  - コンピューティング
  - ストレージ
  - ネットワーク(3)
  - 管理機能
  - ライセンス(2)
  - コスト(2)

6. クラウド事業者の選定
- データセンター
  - データセンターの場所
  - 堅牢性
  - 機密性
- クラウド事業者の信頼性
  - 経営状況の確認
  - 委託関係の確認

検討

7. 契約条件の確認
- 責任範囲とペナルティ
  - 責任範囲の明確化(2)
  - クラウド事業者のペナルティ
- データの所有権、返却・消去
  - データの所有権
  - データの返却(2)
  - データの消去(2)
- 準拠法と管轄裁判所
  - 準拠法
  - 管轄裁判所

8. 運用体制の確認
- システムの運用に関する項目
  - セキュリティ対策
  - ログの監視
- データの管理に関する項目
  - 秘密鍵の管理
  - バックアップ(2)
- インシデントの管理に関する項目
  - インシデントの記録(2)

運用

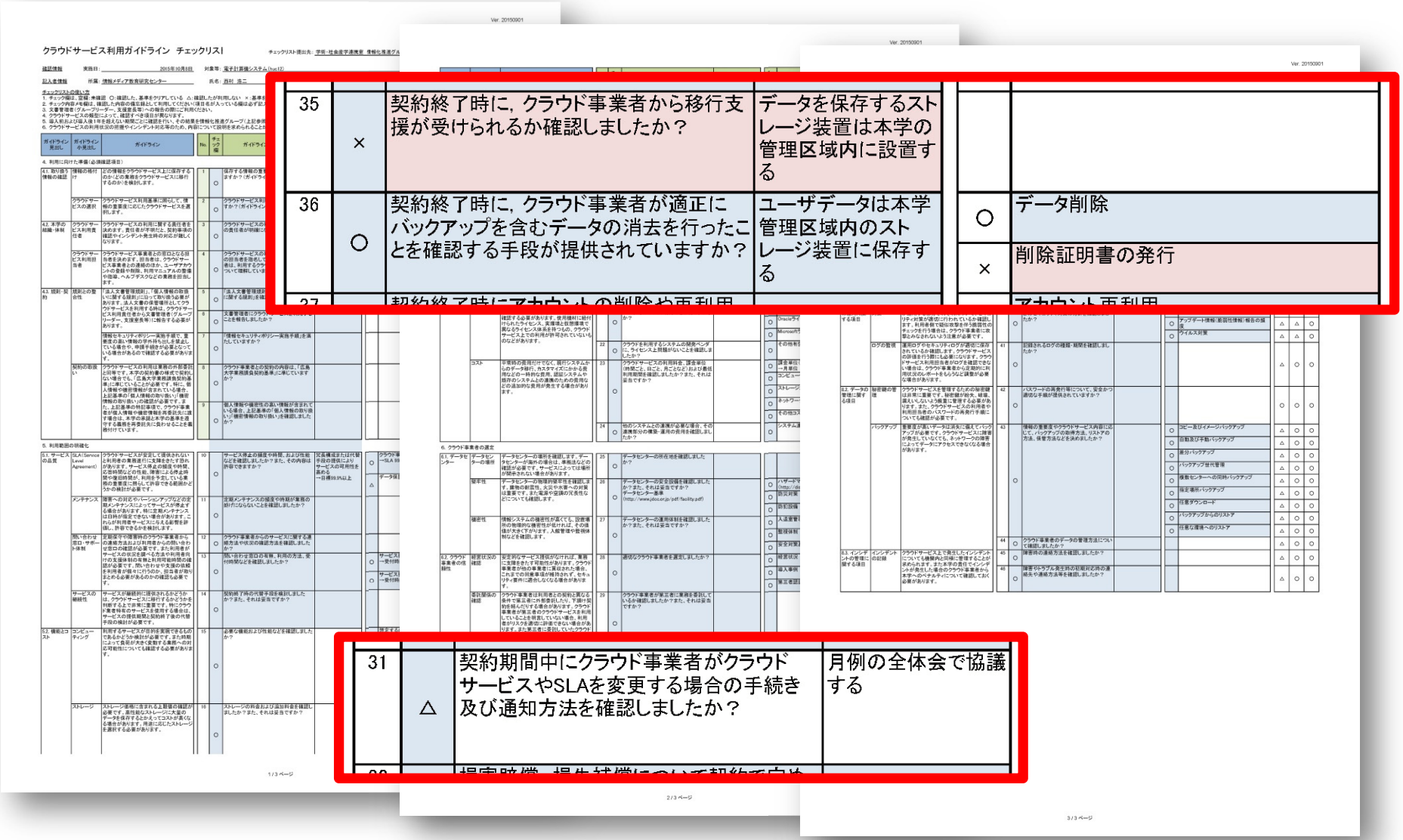
クラウドサービス利用ガイドライン・チェックリスト – リスク対応表

広島大学

ENISA「クラウドコンピューティング　情報セキュリティに関わる利点、リスクおよび推奨事項」			ポリシーと組織関連のリスク							技術関連のリスク														法的なリスク				クラウドに特化していないリスク										
リスク番号			R1	R2	R3	R4	R5	R6	R7	−	R8	R9	R10	R11	R12	R13	R14	R15	R16	R17	R18	R19	R20	R21	R22	R23	R24	R25	R26	R27	R28	R29	R30	R31	R32	R33	R34	R35
リスク内容（●：該当，○：関連あり）			ロックイン	ガバナンスの喪失	コンプライアンスの課題	他の共同利用者の行為による信頼の喪失	クラウドサービスの終了または障害	クラウドプロバイダの買収	サプライチェーンにおける障害	リソース・インフラの高集約によるインシデントの影響の拡大	リソースの枯渇（リソース割り当ての過不足）	隔離の失敗	クラウドプロバイダ従事者の不正ー特権の悪用	管理用インタフェースの悪用（操作、インフラストラクチャアクセス）	データ転送途上における攻撃	データ漏えい（アップロード時、ダウンロード時、クラウド間転送）	セキュリティが確保されていない、または不完全なデータ削除	DDoS攻撃（分散サービス運用妨害攻撃）	EDoS攻撃（経済的な損失を狙ったサービス運用妨害攻撃）	暗号鍵の喪失	不正な探査またはスキャンの実施	サービスエンジンの侵害	利用者側の強化手順と、クラウド環境との間に生じる矛盾	証拠提出命令と電子証拠開示	司法権の違いから来るリスク	データ保護に関するリスク	ライセンスに関するリスク	ネットワークの途絶	ネットワークの管理（ネットワークの混雑、接続ミス、適切でない使用）	ネットワークトラフィックの改変	特権の（勝手な）拡大	ソーシャルエンジニアリング攻撃（なりすまし）	運用ログの喪失または改ざん	セキュリティログの喪失または改ざん（フォレンジック捜査の操作）	バックアップの喪失、盗難	構内への無権限アクセス（装置その他の設備への物理的アクセスを含む）	コンピュータ設備の盗難	自然災害
リスクレベル			高	高	高	中	中	中	中	−	中	高	高	中	中	中	中	中	中	中	中	中	中	高	高	高	中	中	高	中	中	中	中	中	中	中	中	中
経済産業省「クラウドサービスにおけるリスクと管理策に関する有識者による検討結果　2011年度版」			L12	L13	−	H02	−	−	L14	H01	H04	H05	M07	M08	M09	−	M10	M11	L15	L16	L17	H06	−	L18	L19	L20	L21	−	−	−	−	−	−	−	−	−	−	−
広島大学「広島大学クラウドサービス利用ガイドライン・チェックリスト　第二版」																																						
4.1. 取り扱う情報の確認	(1) 情報の格付け	1. 保存する情報の重要度は明確になっていますか？（ガイドライン表１参照）	●	●								○													○	●												
	(2) クラウドサービスの選択	2. クラウドサービス利用基準を満たしていますか？（ガイドライン図３参照）	●	●	●	●						○													●	●												
4.2. 本学の組織・体制	(1) クラウドサービス利用責任者	3. クラウドサービスの利用について、本学側の責任者が明確になっていますか？		●																																		
	(2) クラウドサービス利用担当者	4. クラウドサービスの利用について、本学側の担当者を指名していますか？また担当者は、利用するクラウドサービスの機能について理解していますか？		●																																		
4.3. 規則・契約	(1) 規則との整合性	5. 「法人文書管理規則」「個人情報の取扱いに関する規則」を確認しましたか？		●	●																				○	●												
		6. 文書管理者にクラウドサービスを利用することを報告しましたか？		●	●																				○	●												
		7. 「情報セキュリティポリシー実施手順」を満たしていますか？		●	●																				○	●												
	(2) 契約の取扱い	8. クラウド事業者との契約の内容は、「広島大学業務請負契約基準」に準じていますか？		○	○																																	
		9. 個人情報や機密性の高い情報が含まれている場合、上記基準の「個人情報の取り扱い」「機密情報の取り扱い」を確認しましたか？		○	○																																	
5.1. サービスの品質	(1) SLA（Service Level	10. サービス停止の頻度や時間、および性能などを確							●	○	○	○											●															
	(2) メンテナンス	11. 定期メンテナンスの頻度や時期が業務の妨げにならないことを確認しましたか？							●														●															
	(3) 問い合わせ窓口・サポート体制	12. クラウド事業者からのサービスに関する連絡方法や状況の確認方法を確認しましたか？							●	○	○	○	○	○	○	○	○	○	○	○	○	○	○															
		13. 問い合わせ窓口の有無、利用の方法、受付時間などを確認しましたか？							●	○	○	○	○	○	○	○	○	○	○	○	○	○	○															
	(4) サービスの継続性	14. 契約終了時の代替手段を検討しましたか？また、それは妥当ですか？					●	●	●																													
5.2. 機能とコスト	(1) コンピューティング	15. 必要な機能および性能などを確認しましたか？																																				
	(2) ストレージ	16. ストレージの料金および追加料金を確認しましたか？また、それは妥当ですか？																																				
	(3) ネットワーク	17. データ転送速度を確認しましたか？また時期によって負荷が大きく変動する業務への対応可能性についても確認しましたか？																																				
		18. 必要な機能および性能などを確認しましたか？																																				
		19. ネットワーク利用に必要なコスト、回線使用料は確認しましたか？また、それは妥当ですか？																																				
	(4) 管理機能	20. 必要とする管理ツールの機能を満たしているか、または代替手段があるか確認しましたか？																																				
	(5) ライセンス	21. ライセンス数及びユーザ数は揃っていますか？またCPUやコア数などを確認しましたか？																																				
		22. クラウドを利用するシステムの開発ベンダに、ライセンス上問題がないことを確認しましたか？																																				
	(6) コスト	23. クラウドサービスの利用料金、課金単位（時間ごと、日ごと、月ごとなど）および最低利用期間を確認しましたか？また、それは妥当ですか？																																				
		24. 他のシステムとの連携が必要な場合、その連携部分の構築・運用の費用を確認しましたか？																																				
6.1. データセンター	(1) データセンターの場所	25. データセンターの所在地を確認しましたか？																																			●	●
	(2) 堅牢性	26. データセンターの安全設備を確認しましたか？また、それは妥当ですか？データセンター基準（http://www. jdcc.or.jp/pdf/facility.pdf）																																			●	●
	(3) 機密性	27. データセンターの運用体制を確認しましたか？また、それは妥当ですか？																																			●	●
6.2. クラウド事業者の信頼性	(1) 経営状況の確認	28. 適切なクラウド事業者を選定しましたか？					●	●																														
	(2) 委託関係の確認	29. クラウド事業者が第三者に業務を委託しているか確認しましたか？また、それは妥当ですか？					●	●	●																													
7.1. 責任範囲とペナルティ	(1) 責任範囲の明確化	30. 利用者とクラウド事業者の責任範囲（責任分解点）は明確になっていますか？また、それは妥当ですか？								●																												
		31. 契約期間中にクラウド事業者がクラウドサービスやSLAを変更する場合の手続き及び通知方法を確認しましたか？																																				
	(2) クラウド事業者のペナルティ	32. 損害賠償、損失補償について契約で定めてありますか？また、それは妥当ですか？								●																												
7.2. データの所有権、返却・消去	(1) データの所有権	33. クラウドサービスに保存したデータの知的財産権，所有権及び利用権の取扱いを確認しましたか？また、それは妥当ですか？	●	●			●	○																														
	(2) データの返却	34. クラウドサービス利用中や契約終了時に，クラウドに保存したデータを取り出す方法があるか確認しましたか？	●	●			●	○																														
		35. 契約終了時に，クラウド事業者から移行支援が受けられるか確認しましたか？	●	●			●	○																														
	(3) データの消去	36. 契約終了時に，クラウド事業者が適正にバックアップを含むデータの消去を行ったことを確認する手段が提供されていますか？	●	●			●	○																														
		37. 契約終了時にアカウントの削除や再利用の禁止が可能であることを確認しましたか？					○	○																														
7.3. 準拠法と管轄裁判所	(1) 準拠法	38. 準拠法を確認しましたか？また、それは妥当ですか？																																				
	(2) 管轄裁判所	39. 管轄裁判所を確認しましたか？また、それは妥当ですか？																																				
8.1. システムの運用に関する項目	(1) セキュリティ対策	40. バージョンアップ、設定変更、パッチ適用などのセキュリティ対策の方針を確認しましたか？								●																												
	(2) ログの監視	41. 記録されるログの種類・期間を確認しましたか？								●																												
8.2. データの管理に関する項目	(1) 秘密鍵の管理	42. パスワードの再発行等について、安全かつ適切な手順が提供されていますか？																																				
	(2) バックアップ	43. 情報の重要度やクラウドサービス内容に応じて、バックアップの取得方法、リストアの方法、保管方法などを決めましたか？	●				○		○								○				○					○							●	●	●			
		44. クラウド事業者のデータの管理方法について確認しましたか？	●				○		○								●				●					●							●	●	●			
8.3. インシデントの管理に関する項目	(3) インシデントの記録	45. 障害時の連絡方法を確認しましたか？					●		●	●	●	●	●	●	●	●	●	●	●	●	●	●	○	●				●	●	●	●	●	●	●	●			
		46. 障害やトラブル発生時の初期対応時の連絡先や連絡方法等を確認しましたか？					●		●	●	●	●	●	●	●	●	●	●	●	●	●	●	○	●				●	●	●	●	●	●	●	●			

クラウドサービス利用ガイドライン・チェックリスト – チェック例

広島大学



35	×	契約終了時に，クラウド事業者から移行支援が受けられるか確認しましたか？	データを保存するストレージ装置は本学の管理区域内に設置する
36	○	契約終了時に，クラウド事業者が適正にバックアップを含むデータの消去を行ったことを確認する手段が提供されていますか？	ユーザデータは本学管理区域内のストレージ装置に保存する
31	△	契約期間中にクラウド事業者がクラウドサービスやSLAを変更する場合の手続き及び通知方法を確認しましたか？	月例の全体会で協議する

○	データ削除
×	削除証明書の発行

ISMSクラウドセキュリティ適用宣言書(一部)

広島大学

ISMSクラウドセキュリティ適用宣言書　1.01　IMC110-014-00

管理策	適用	適用除外
ISO/IEC 27001:2013附属書A	34	80
ISO/IEC 27017:2015附属書A（カスタマ/プロバイダ）※1	5	2
合計	39	82

※1 いずれか、もしくは両方に○

管理策	管理策を含めた理由	27001[管理策]の実施状況	27017[管理策](実施 カスタマ	プロバイダ	適用/除外	管理策又は除外理由	証跡、理由等 確認するチェックリストの項目（見出し－小見出し）	資料等
ISO/IEC 27001:2013附属書A								
ISO/IEC 27017:2015附属書A								
A.5 情報セキュリティのための方針群								
A.5.1 情報セキュリティのための経営陣の方向性								
A.5.1.1 情報セキュリティのための方針群	情報セキュリティの基本方針を管理層が承認し、センタースタッフ及び関連する外部関係者に周知するため。	○	○	○	○	全学的なクラウドサービス利用の方針として策定された「広島大学クラウドサービス利用ガイドライン・チェックリスト」を活用し、説明会やシンポジウム、講演等により学内外に周知する。	4.2 本学の組織・体制－クラウドサービス利用担当者 5.2 機能とコスト 7.2 データの所有権、返却・消去 7.3 準拠法と管轄裁判所	・センターWeb「広島大学クラウドサービス利用ガイドライン」（http://www.media.hiroshima-u.ac.jp/news/cloudguide） ・講演資料 ・HUC12説明会 ・20161115-ISMS研修会
A.5.1.2 情報セキュリティのための方針群のレビュー		○	－	－	×	27017には追加の実施の手引なし		
A.6 情報セキュリティのための組織								
A.6.1 内部組織								
A.6.1.1 情報セキュリティの役割及び責任	センタースタッフの役割を明確にするため。				×	27017には追加の実施の手引なし		
A.6.1.2 職務の分離					○	チェックリストで確認する。 必要に応じて稼働維持の月次定例会議で確認する。	7.3 準拠法と管轄裁判所 8.2 データの管理に関する項目－秘密鍵の管理	・HUC12≫01_システム全体≫01_打合せ資料（稼働維持）≫第x回定例会議 ・サーバ証明書の発行手順等（NII）
A.6.1.3 関係当局との連絡	関係機関・組織との協力体制を確保するため。				○	チェックリストで確認する。	6.2 クラウド事業者の信頼性 8.1 システムの運用に関する項目	・AXIESクラウドサービスカタログ ・学認クラウドチェックリスト(No.70) ・Compliance Framework document.pdf ・MCIO ISO 27001 Certificate IS 533913 Year 2016.pdf ・Azure ISO 27001_27018 Assessment Report Year 2016.pdf ・Microsoft ISO 27017 Certificate.pdf ・Office 365 ISO 27001-ISO 27018-ISO 27017 Audit Assessment Report Year 2016.pdf
A.6.1.4 専門組織との連絡								
A.6.1.5 プロジェクトマネジメントにおける情報セキュリティ								
A.6.2 モバイル機器及びテレワーキング								
A.6.2.1 モバイル機器の方針					×	27017には追加の実施の手引なし		
A.6.2.2 テレワーキング					×	27017には追加の実施の手引なし		
CLD.6.3 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との関係								

2 / 12 ページ

学認クラウド 導入支援サービス
大学向けクラウドソリューションカタログ

広島大学

https://cloud.gakunin.jp/ https://axies.jp/

審査報告書

広島大学

様式CA0314F01 (3/3)

組織名称	作成日
国立大学法人広島大学 情報メディア教育研究センター	2017年3月1日

審査の種類: 本審査

マネジメントシステム審査結果概要（JIP-ISMS517-1.0）

マネジメントシステム評価

項番	要求事項項目	適合		不適合		別紙コメントNo.
		審査充足	改善の余地	B	A	
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	V				
4.2.1	情報セキュリティリスクアセスメント		V			1
4.2.2	情報セキュリティリスク対応		V			2

様式SA0314F03 (4/5) 5/6

組織名称	作成日
国立大学法人広島大学 情報メディア教育研究センター	2017年3月1日

審査の種類: 本審査

審査所見の詳細

※管理策の項番末尾で、Cはクラウドサービスカスタマ、Pはクラウドサービスプロバイダに対する所見であることを示しています。

No./規格	要求事項／評価	審査所見
No.1	① JIP-ISMS517-1.0 細別番号 c) 2. 組織のMS文書	＜要求事項＞ c) 次によって情報セキュリティリスクを特定する。 1) ISMSの適用範囲内におけるクラウドサービスに関する情報の機密性、完全性及び可用性の喪失に伴うリスクを特定するために、情報セキュリティリスクアセスメントのプロセスを適用する。 （関連）ISO/IEC 27001:2013 6.1.2 b)

様式SA0314F03 (5/5)

組織名称	作成日
国立大学法人広島大学 情報メディア教育研究センター	2017年3月1日

審査の種類: 本審査

審査所見の詳細

※管理策の項番末尾で、Cはクラウドサービスカスタマ、Pはクラウドサービスプロバイダに対する所見であることを示しています。

No./規格	要求事項／評価	審査所見
No.4	① JIP-ISMS517-1.0 細別番号 2. 組織のMS文書	＜要求事項＞ マネジメントレビューは、次の事項を考慮しなければならない。 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 ＜具体的事実/説明＞ マネジメントレビューの報告に改善の余地があります。

JACO Japan Audit and Certification Organization for Environment and Quality

様式MA0313F03 (1/1)

国立大学法人広島大学
情報メディア教育研究センター 様

審 査 報 告 書

ISO/IEC 27017:2015に基づくISMSクラウドセキュリティ認証
JIP-ISMS517-1.0
本審査

審査結果の受理及び確認　　日付: 2017 年 3 月 1 日

（組織 署名）　西原玲二　　（JACO 署名）　羽田野尚登

S000936

本報告書の所有権は、(株)日本環境認証機構に帰属します。
組織が本報告書を公開する場合は、本報告書全体を公開する必要があります。（部分的な公開は厳禁です。）

JACO 様式CA0314F01 (1/5) 2/6

ISMSクラウドセキュリティ認証	審査報告書

S000936

組織名称及び代表者 国立大学法人広島大学 情報メディア教育研究センター 情報メディア教育研究センター長 相原 玲二 様		報告書作成日	2017 年 3 月 1 日
		審査の種類	実施日
	本審査		2017 年 2 月 27 日～ 2017 年 3 月 1 日
			年 月 日～ 年 月 日
所在地（登録サイトの筆頭住所） 〒 739 － 8511 広島県東広島市鏡山1-4-2	審査チーム（審査員氏名） リーダ：羽田野 尚登		
登録範囲 次のクラウドサービスのクラウドサービスカスタマとしての利用に係るISMSクラウドセキュリティマネジメントシステム ・Microsoft Azure、Office 365 Education ・Hitachi Cloud：エンタープライズクラウドサービス、出前クラウドサービス、フェデレーテッドクラウド			
適用規格	JIP-ISMS517-1.0	適用宣言書	IMC110-014-00 V1.01
認定機関	□JIPDEC	判定委員会申請予定日	2017 年 3 月 23 日

Ⅰ. 審査チームの結論
組織のマネジメントシステムは規格要求事項に適合し有効に実施されていると判断し、認証の授与を推薦します。
［組織との合意事項（付帯条件等）］
ISMSクラウドセキュリティ認証のもとになるISMS認証の登録番号は、IC14J0392です。

Ⅱ. 審査所見総括
1) 概要 ：
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マネジメントシステムが、構築され運用が開始されていることを確認しました。2015年9月より運用開始しているHUC12基幹システムでは、広島大学クラウドサービス利用ガイドラインに基づき、積極的にクラウドサービスの導入・活用が行われています。ISMSクラウドセキュリティマネジメントシステムの構築にあたっても、その実績・知見が活用されています。

2) 要点 ：
a) 規格への適合性
ISMSクラウドセキュリティ対応として、ISMSマニュアルをはじめとするISMS関連文書の改定、並びに、ISMSクラウドセキュリティ適用宣言書及びISMSクラウドセキュリティ要求事項対応等の文書も整備され、規格に適合したマネジメントシステムが構築され、運用が開始されています。ISMSクラウドセキュリティ適用宣言書では、広島大学クラウドサービス利用ガイドライン／チェックリストの確認する項番や証跡となる資料等が記載され、規格への適合性を確実なものとしています。

b) マネジメントシステムの有効性
広島大学クラウドサービス利用ガイドライン／チェックリストを活用し、各クラウドサービスのリスクが分析され、必要なリスク対応が実施されています。また、内部監査指摘により、サイバー攻撃といった新たな脅威に対するリスク対応計画（多要素認証、試行失敗回数制限）が作成され、対応状況がフォローされています。

c) 内部監査の実施、有効性
ISMSと併せた内部監査が、2017年1月16日の事前調査に始まり、2月6日～2月8日の現場監査まで、訓練を受けた3名の内部監査員により実施されました。1件のB−指摘（是正回答書要）は是正が完了しています。2件のB+指摘（是正回答書不要）は、次回の監査時に確認が予定されています。チェックリストにより全43項目の要求事項全てが監査されており内部監査は有効に機能しています。

d) マネジメントレビューの実施、有効性
2017年2月22日に臨時のマネジメントレビューが実施され、内部監査結果、ISMS達成計画と現状課題、関連文書の整備状況等が報告され、トップマネジメントにより運用開始状況がレビューされ、4つの具体的な指示事項が出されています。

JACO (2/5)

3) 課題及び次回審査の着眼点 ：
ISMSクラウドセキュリティのパフォーマンス及びマネジメントシステムの有効性評価について確認します。

4) 修正及び是正処置の要求 ：
修正及び是正処置を要求する不適合はありません。

Ⅲ. 収集した情報及び証拠の評価
・ISMSクラウドセキュリティマネジメントシステムの実施状況については、文書類（適用範囲、情報セキュリティ方針、リスクアセスメント、リスク対応計画、適用宣言書、管理策実施のための手順書）の整備及び実施状況を、ドキュメント、各階層へのインタビュー、現場及び記録類により確認しましたので、情報・証拠は妥当であると判断します。
・ISMSクラウドセキュリティマネジメントシステムの有効性については、セキュリティ計画の実施状況、違反・事故の監視及び処置、管理策実施・有効性測定項目並びに順法項目を中心にサンプリングチェックしましたが、いずれも関連文書、記録、インタビューなどによって確認できましたので、情報・証拠は妥当であると判断します。

Ⅳ. 組織の活動範囲に対する確認事項
1) 登録組織名及び住所等は、別紙「登録組織名称及び認証範囲等確認書」により確認
2) 組織のマネジメントシステム文書の状況
ISMSマニュアル　1.03 版　2017 年 2 月 21 日

Ⅴ. その他
・審査目的: 「審査の進め方」及び「審査計画書」に記載
・審査計画書の引用: ☑既に配付している審査計画書との変更無し
□既に配付している審査計画書との変更有り
・免責事項: 審査はサンプリングにより実施しています。従って本報告書は、記載以外の不適合がないことを証明するものではありません。
・受審側の権利: 審査報告書の記載内容に納得できない場合には、受審側は本報告書への署名を保留する権利を有しています。また、審査業務に関して、受審側は当機関に対して苦情及び異議申し立ての権利を有しています。
・特記事項 特にありません。

本報告書の所有権は、(株)日本環境認証機構に帰属します。
組織が本報告書を公開する場合は、本報告書全体を公開する必要があります。（部分的な公開は厳禁です。）

審査報告書(2/6)

広島大学

Ⅰ．審査チームの結論

組織のマネジメントシステムは規格要求事項に適合し有効に実施されていると判断し、認証の授与を推薦します。

「組織との合意事項（付帯条件等）」

ISMSクラウドセキュリティ認証のもとになるISMS認証の登録番号は、IC14J0392です。

Ⅱ．審査所見総括

1）概要　：

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マネジメントシステムが、構築され運用が開始されていることを確認しました。2015年9月より運用開始しているHUC12基幹システムでは、広島大学クラウドサービス利用ガイドラインに基づき、積極的にクラウドサービスの導入・活用が行われています。ISMSクラウドセキュリティマネジメントシステムの構築にあたっても、その実績・知見が活用されています。

2）要点　：

a）規格への適合性

ISMSクラウドセキュリティ対応として、ISMSマニュアルをはじめとするISMS関連文書の改定、並びに、ISMSクラウドセキュリティ適用宣言書及びISMSクラウドセキュリティ要求事項対応等の文書も整備され、規格に適合したマネジメントシステムが構築され、運用が開始されています。ISMSクラウドセキュリティ適用宣言書では、広島大学クラウドサービス利用ガイドライン／チェックリストの確認する項番や証跡となる資料等が記載され、規格への適合性を確実なものとしています。

b）マネジメントシステムの有効性

広島大学クラウドサービス利用ガイドライン／チェックリストを活用し、各クラウドサービスのリスクが分析され、必要なリスク対応が実施されています。また、内部監査指摘により、サイバー攻撃といった新たな脅威に対するリスク対応計画（多要素認証、試行失敗回数制限）が作成され、対応状況がフォローされています。

c）内部監査の実施、有効性

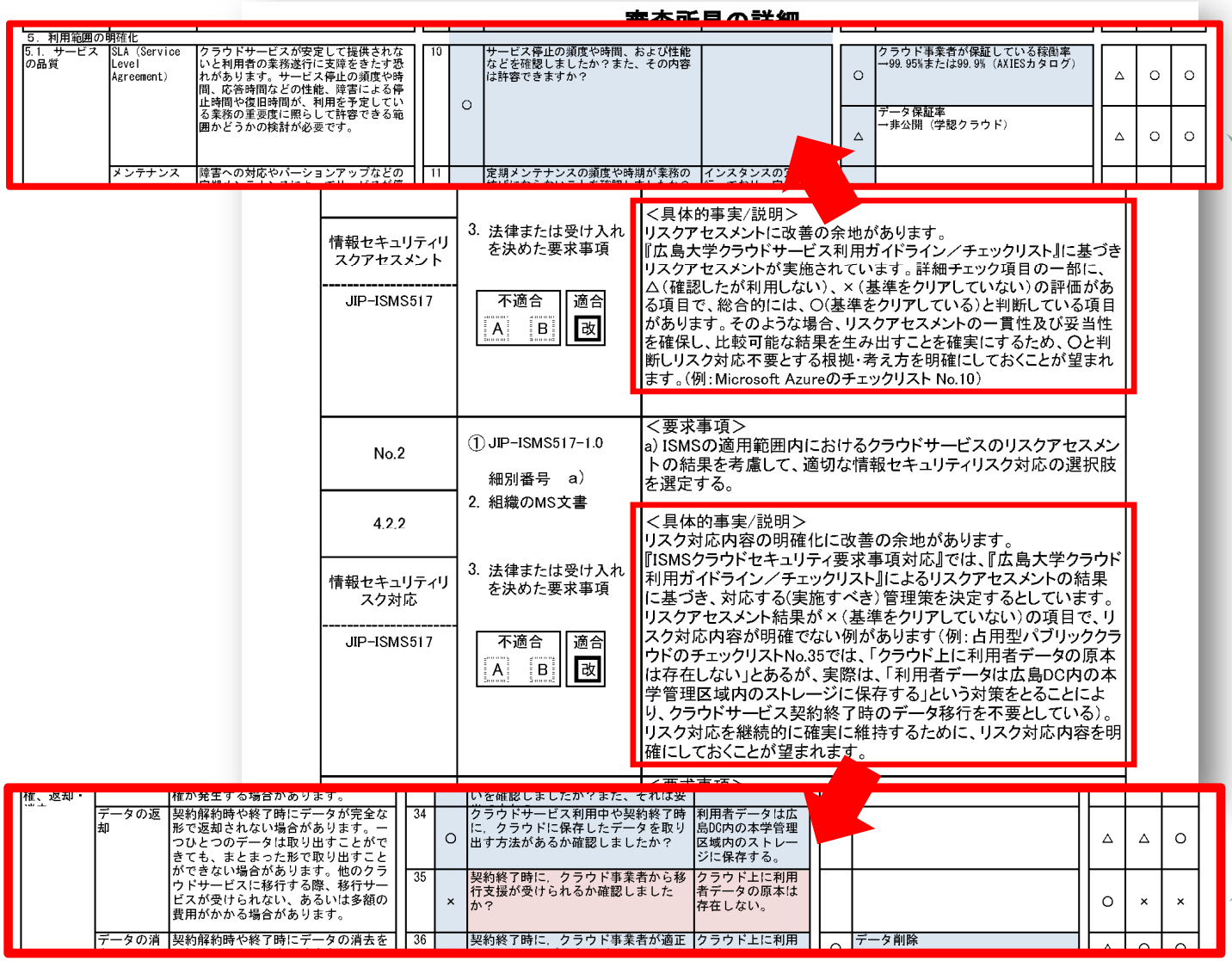
ISMSと併せた内部監査が、2017年1月16日の事前調査に始まり、2月6日～2月8日の現場監査まで、訓練を受けた3名の内部監査員により実施されました。1件のB-指摘（是正回答書要）は是正が完了しています。2件のB+指摘(是正回答書不要）は、次回の監査時に確認が予定されています。チェックリストにより全43項目の要求事項全てが監査されており内部監査は有効に機能しています。

d）マネジメントレビューの実施、有効性

2017年2月22日に臨時のマネジメントレビューが実施され、内部監査結果、ISMS達成計画と現状課題、関連文書の整備状況等が報告され、トップマネジメントにより運用開始状況がレビューされ、4つの具体的な指示事項が出されています。

審査報告書(5/6)

広島大学



5．利用範囲の明確化											
5.1. サービスの品質	SLA（Service Level Agreement）	クラウドサービスが安定して提供されないと利用者の業務遂行に支障をきたす恐れがあります。サービス停止の頻度や時間、応答時間などの性能、障害による停止時間や復旧時間が、利用を予定している業務の重要度に照らして許容できる範囲かどうかの検討が必要です。	10	○	サービス停止の頻度や時間、および性能などを確認しましたか？また、その内容は許容できますか？		○	クラウド事業者が保証している稼働率→99.95%または99.9%（AXIESカタログ）	△	○	○
							△	データ保証率→非公開（学認クラウド）	△	○	○
	メンテナンス	障害への対応やバージョンアップなどの	11		定期メンテナンスの頻度や時期が業務の	インスタンスの					

情報セキュリティリスクアセスメント JIP-ISMS517	3. 法律または受け入れを決めた要求事項 不適合 A B 適合 改	＜具体的事実/説明＞ リスクアセスメントに改善の余地があります。 『広島大学クラウドサービス利用ガイドライン／チェックリスト』に基づきリスクアセスメントが実施されています。詳細チェック項目の一部に、△（確認したが利用しない）、×（基準をクリアしていない）の評価がある項目で、総合的には、○（基準をクリアしている）と判断している項目があります。そのような場合、リスクアセスメントの一貫性及び妥当性を確保し、比較可能な結果を生み出すことを確実にするため、○と判断しリスク対応不要とする根拠・考え方を明確にしておくことが望まれます。（例：Microsoft Azureのチェックリスト No.10）	Microsoft Azure チェックリスト No.10
No.2 4.2.2 情報セキュリティリスク対応 JIP-ISMS517	① JIP-ISMS517-1.0 細別番号　a） 2. 組織のMS文書 3. 法律または受け入れを決めた要求事項 不適合 A B 適合 改	＜要求事項＞ a) ISMSの適用範囲内におけるクラウドサービスの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。 ＜具体的事実/説明＞ リスク対応内容の明確化に改善の余地があります。 『ISMSクラウドセキュリティ要求事項対応』では、『広島大学クラウド利用ガイドライン／チェックリスト』によるリスクアセスメントの結果に基づき、対応する（実施すべき）管理策を決定するとしています。リスクアセスメント結果が×（基準をクリアしていない）の項目で、リスク対応内容が明確でない例があります（例：占用型パブリッククラウドのチェックリストNo.35では、「クラウド上に利用者データの原本は存在しない」とあるが、実際は、「利用者データは広島DC内の本学管理区域内のストレージに保存する」という対策をとることにより、クラウドサービス契約終了時のデータ移行を不要としている）。リスク対応を継続的に確実に維持するために、リスク対応内容を明確にしておくことが望まれます。	占用型パブリッククラウド チェックリスト No.35

権、返却・		権が発生する場合があります。			いを確認しましたか？また、それは妥						
	データの返却	契約解約時や終了時にデータが完全な形で返却されない場合があります。一つひとつのデータは取り出すことができても、まとまった形で取り出すことができない場合があります。他のクラウドサービスに移行する際、移行サービスが受けられない、あるいは多額の費用がかかる場合があります。	34	○	クラウドサービス利用中や契約終了時に，クラウドに保存したデータを取り出す方法があるか確認しましたか？	利用者データは広島DC内の本学管理区域内のストレージに保存する。			△	△	○
			35	×	契約終了時に，クラウド事業者から移行支援が受けられるか確認しましたか？	クラウド上に利用者データの原本は存在しない。			○	×	×
	データの消	契約解約時や終了時にデータの消去を	36		契約終了時に，クラウド事業者が適正	クラウド上に利用	○	データ削除			

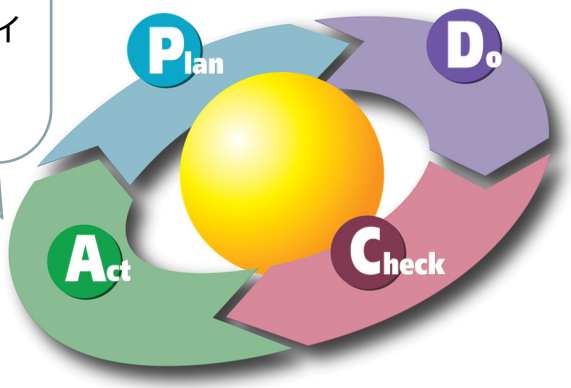
クラウドサービスを利用するということ

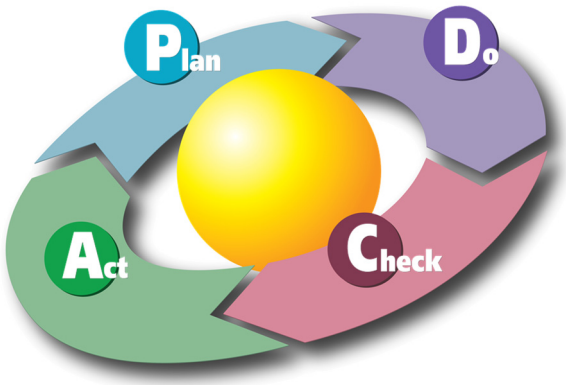
広島大学

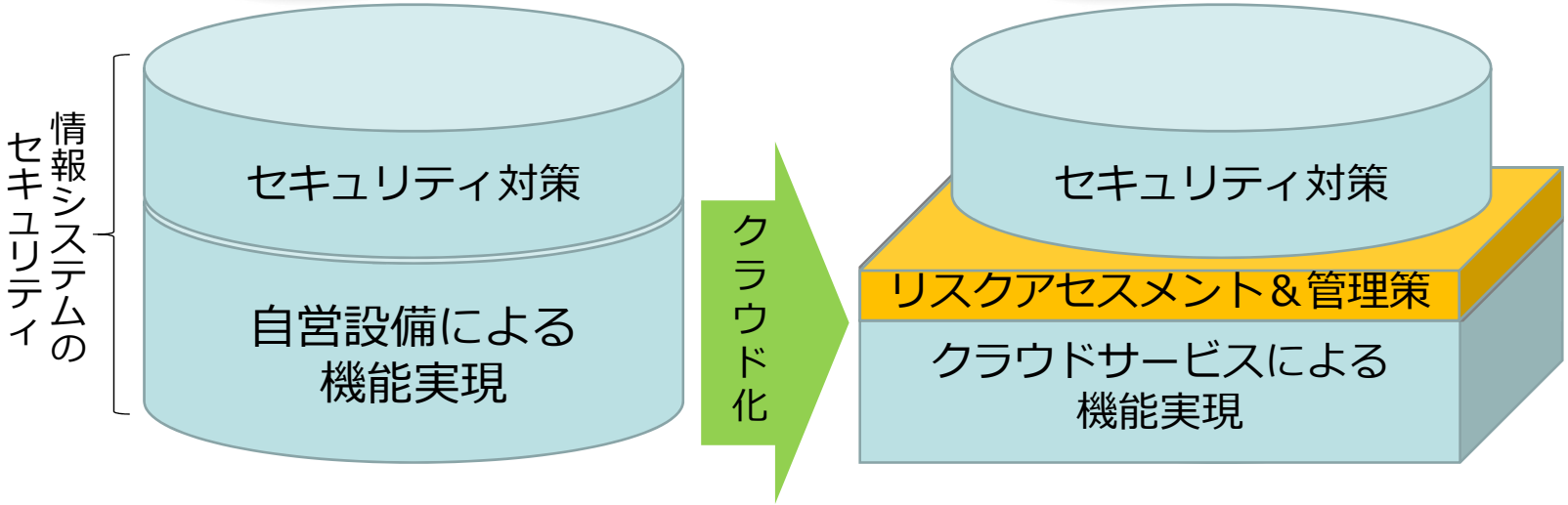
既存システムに対するPDCAが確立されていることが前提
→セキュリティガバナンス実態調査

変化に気づき、対策を講じる

リスクアセスメント　　管理策







まとめ

広島大学

- ISMSクラウドセキュリティ認証を受審してみた
  - JIP-ISMS517-1.0（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）
    - 本審査は2017年2月27日～3月1日
    - 判定委員会は2017年3月23日（予定）
      - クラウドサービスカスタマとして日本初の認証取得
  - 広島大学クラウドサービス利用ガイドライン／チェックリストのリスクアセスメント手法としての有効性を検証
    - チェックリスト作成のための資料も有効活用
      - 学認クラウド 導入支援サービス（チェックリスト）
      - AXIES 大学向けクラウドソリューションカタログ2016
- 認証審査を通して
  - 「クラウドサービスを利用する」ということ
    - 「変化に気づき、対策を講じる」
  - 既存システムに対するPDCAが確立している必要あり
    - ISMS本体とISMSクラウドセキュリティの関係と同じ建付け
    - セキュリティガバナンス実態調査（渡邉報告）