広島大学におけるクラウド化手順とISMSの取り組み

情報メディア教育研究センター
財務・総務室情報部
西村 浩二

ISMSセミナー ～クラウドサービス利用に潜むリスクとは～

自己紹介

- 西村 浩二 (にしむら こうじ)
  - 1991年 広島大学大学院工学研究科博士課程前期修了
  - 1991年 全日空システム企画(株)
    (現、ANAシステムズ(株))
  - 1994年 広島大学総合情報処理センター助手
  - 2002年 博士(工学)(広島大学大学院工学研究科)
  - 2007年 同情報メディア教育研究センター准教授
    - ユーザーサービス部門長(サービス運用責任者)
  - 2011年 同情報メディア教育研究センター教授
    - 情報セキュリティ研究部門長(セキュリティ教育・啓蒙、ガイドライン等の検討・策定)
  - 2017年 同情報メディア教育研究センター長
    - 情報セキュリティ研究部門長、ユーザーサービス部門長、財務・総務室情報部長(併任)
    - 情報処理安全確保支援士(登録番号：第001322号)
  - 2018年 情報科学部教授(併任)

- 広島大学クラウドサービス利用ガイドライン
  - https://www.media.hiroshima-u.ac.jp/news/cloudguide
    → 広島大学におけるクラウドサービス利用のためのガイドライン
- 平成25年度国家課題対応型研究開発推進事業「アカデミッククラウド環境構築に係るシステム研究」提案
  - 「コミュニティで紡ぐ次世代大学ICT環境としてのアカデミッククラウド」セキュリティ分野担当
  - http://www.icer.kyushu-u.ac.jp/ac
    → アカデミックな組織がクラウドサービスを利用する際のガイドライン
- 高等教育機関における情報セキュリテイポリシー推進部会
  - 高等教育機関の情報セキュリティ対策のためのサンプル規程集
    → クラウドサービス利用に関するガイドライン

本日のお話

【概要】
組織におけるクラウド化の推進においては、本質を見失い、クラウド環境への移行そのものが目的化してしまうケースが見受けられます。
本講演では、広島大学におけるクラウドの導入手順を例に、ISMSおよびISMSクラウドセキュリティとの関係、取り組みについて紹介します。

- 広島大学におけるクラウドサービス利用の取り組み
  - 広島大学クラウドサービス利用ガイドライン
  - 広島大学のクラウド化手順
  - 広島大学のクラウド化の状況
    - 電子計算機システム(HUC12)
- 広島大学におけるISMS/ISMS-CLSの取り組み
  - ISMS＋ISMSクラウドセキュリティ
  - 「クラウドサービスを利用する」ということ
- クラウド利用に関する対外的な取り組み
  - 情報セキュリティガバナンス実態調査
- クラウド化の先に見えたもの
  - 「クラウド化」の実態と問題点

広島大学の概要

- キャンパス，遠隔地区・施設，県外・海外拠点施設等
  - ①東広島キャンパス，②霞キャンパス，③東千田キャンパス，④～⑱遠隔地区
  - 県外オフィス(東京、大阪、福岡)
  - 海外オフィス(北京，上海，ジャカルタ，バンドン，ベトナム，ブラジル，韓国，台湾，トムスク，ケニア，カイロ，ミャンマー，グアナファト，カンボジア，リトアニア，ザールラント，モンゴル)
- 部局等(2019年4月1日現在)
  - 12学部、1専攻科、13研究科(うち2研究科は学生募集停止)
  - 1附置研究所，1全国共同利用施設，2共同利用・共同研究拠点，1中国・四国地区国立大学共同利用施設、26学内共同教育研究施設等
  - 5図書館、3博物館等、大学病院(診療科：34医科、13歯科)
- 構成員数19,226名(2019年5月1日現在)
  - 学部学生10,695名，大学院生4,575名，専攻科学生11名，研究生・科目等履修生339名
  - 役員10名，教員1,794名，職員1,682名

広島大学における

クラウドサービス利用の取り組み

情報系センター(部門)を取り巻く状況

- クラウドサービスの充実
  - 積極的利用への圧力
    - 財政的メリット(本当？)を求める経営層からの圧力
    - 便利さ・手軽さを求める利用者層からの圧力
  - 計算リソースの調達方法の変化
    - 従量課金への対応
    - セキュリティポリシーとの折り合いをどうつける？

  → ガバナンス喪失の恐れ
- インフラ整備の必要性
  - (これまで)大学が情報環境(情報端末)を整備・提供
  - (これから)PC必携化(BYOD)、無線LAN整備(インフラのみ)

  → ガバナンス喪失の恐れ
- サイバーセキュリティ基本法・個人情報保護法
  - クラウドサービスの利用の可否判断
  - 迅速かつ適切なインシデント対応

  → 情報セキュリティに対する責任は増大傾向に

⇒ ガバナンス維持のための対策の必要性

ガイドライン整備の背景

- クラウドサービスの利用
  - クラウド事業者との間で外部委託契約
  - 事業者(メーカ、Sier)によっても定義が異なる(プライベート？パブリック？オンプレミス？オフプレミス？)
  - 現時点ではクラウド事業者および使用するサービス内容に対する基準等が定められていない
- セキュリティポリシーとの整合性
  - 広島大学情報セキュリティポリシー(2005年4月1日)
    - https://www.hiroshima-u.ac.jp/about/initiatives/jyoho_ka/security_policy
  - 2011年度あたりから問合せが急増
    - 「Dropboxで大学の情報を扱って良いか？」
    - 「サービスの良い使い方、悪い使い方を教えて欲しい」
- 2012年度に1年かけて検討
  - 具体的、わかりやすい、実行可能
    - 2013年3月、第一版を公開
    - その後、2回の改訂(現在、第三版)

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

クラウドサービス利用ガイドライン　チェックリスト

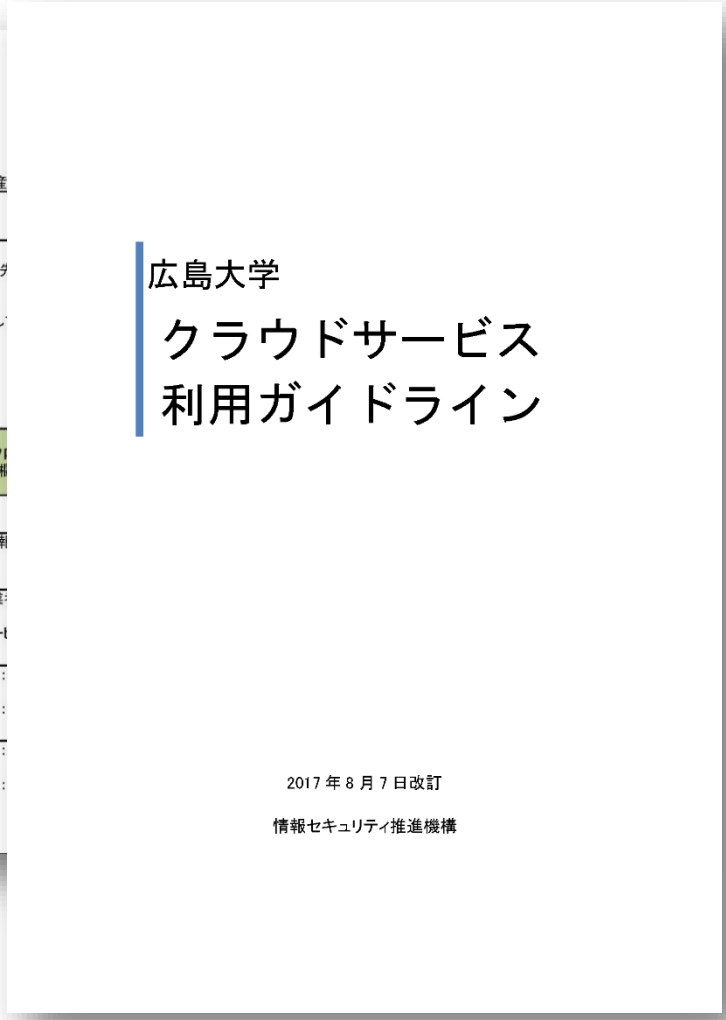
チェックリスト提出先: 学術・社会産

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
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
	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 クラウドサー
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

2017 年 8 月 7 日改訂

情報セキュリティ推進機構

- 第三版(2017年8月7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)

https://www.media.hiroshima-u.ac.jp/news/cloudguide/

「広島大学クラウドサービス利用ガイドライン」における 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

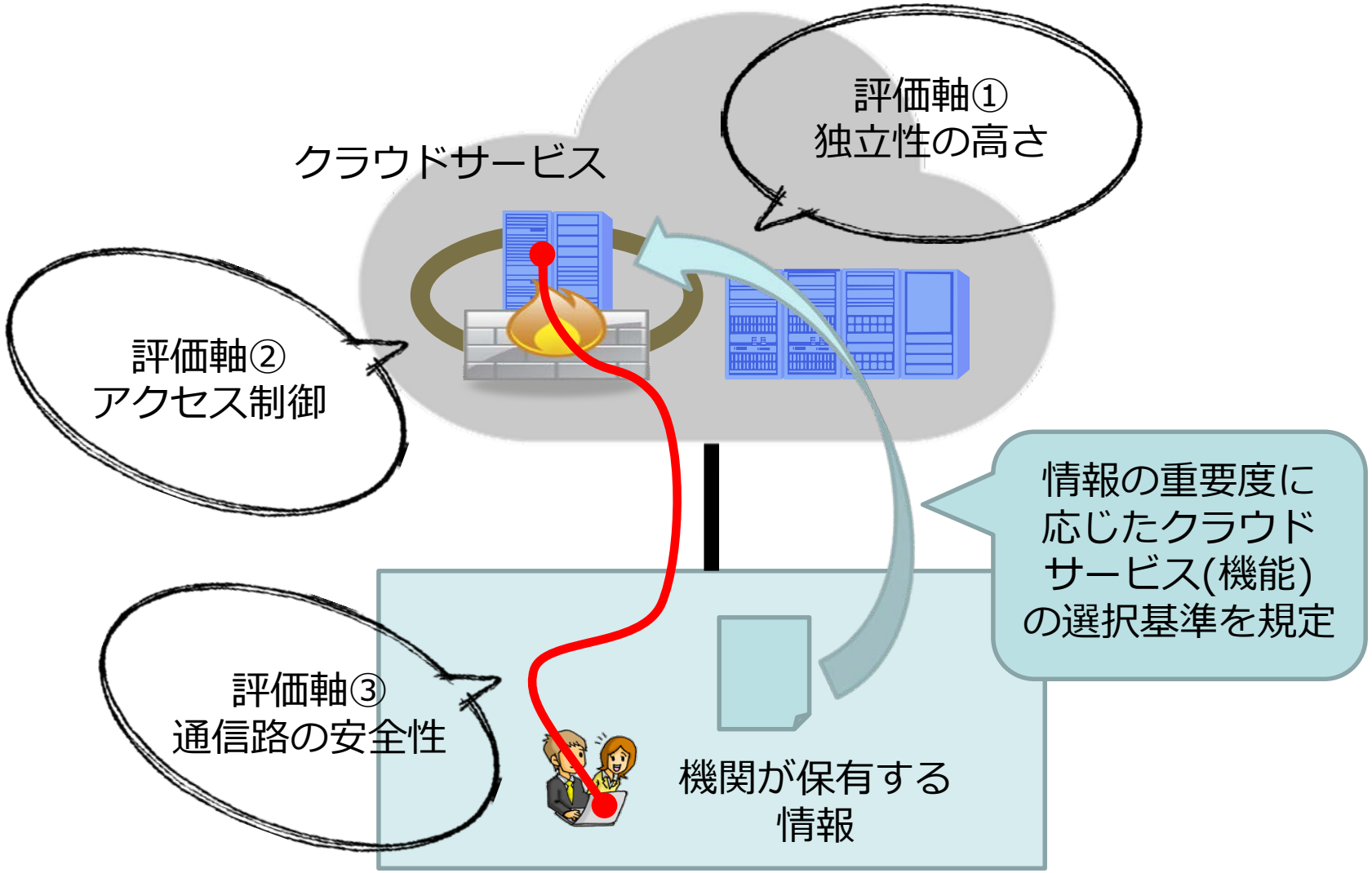
- 責任範囲とペナルティ
  - 責任範囲の明確化(2)
  - クラウド事業者のペナルティ
- データの所有権、返却・消去
  - データの所有権
  - データの返却(2)
  - データの消去(2)
- 準拠法と管轄裁判所
  - 準拠法
  - 管轄裁判所

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

「広島大学クラウドサービス利用ガイドライン」における利用シーンと評価軸

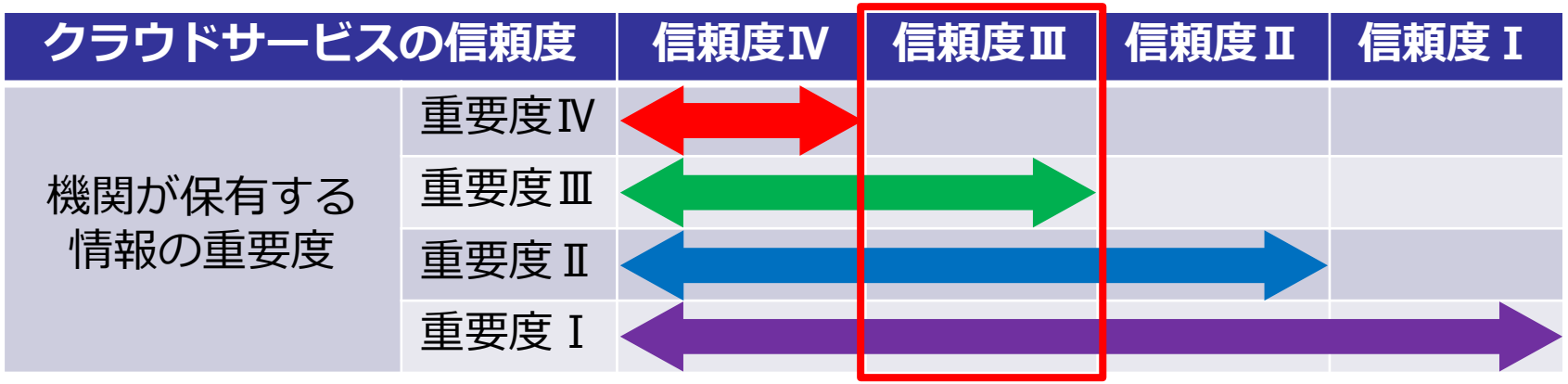


「広島大学クラウドサービス利用ガイドライン」における機関が保有する情報の重要度

広島大学

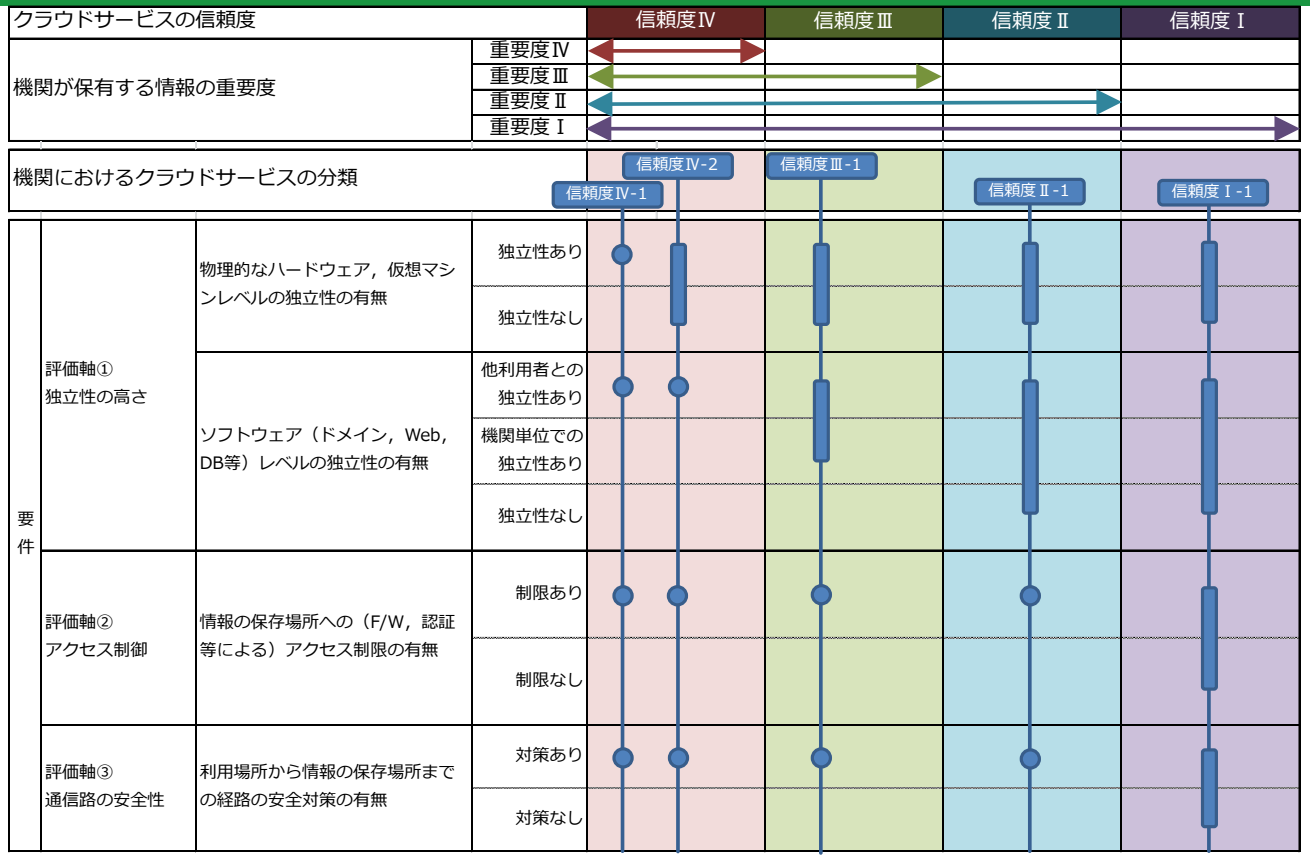
区分	区分の説明	情報の種類	情報の類型(抜粋)
重要度Ⅳ	情報が流出(漏えい)、紛失、改ざん等した場合、機関の業務に深刻かつ重大な影響を及ぼすもの	特定の関係者以外に対し厳重に機密を保持すべきもの	学籍簿、成績原簿に関する情報 指導要領の情報
重要度Ⅲ	情報が流出(漏えい)、紛失、改ざん等した場合、機関の業務に重大な影響を及ぼすもの	特定の職制、グループ又は部署等以外に対して機密を保持すべきもの	学生指導(卒論、修論等)に関する情報 住所 氏名
重要度Ⅱ	情報が流出(漏えい)、紛失、改ざん等した場合、機関の業務に軽微な影響を及ぼすもの	公開を前提としていないもの	学術講演会に関する情報 入試の実施計画に関する情報
重要度Ⅰ	情報が流出(漏えい)、紛失、改ざん等した場合、機関の業務にほとんど影響を及ぼさないもの	積極的な公開を前提としたもの	公開講座等に関する情報 大学案内や広報誌に掲載している情報

クラウドサービスの信頼度



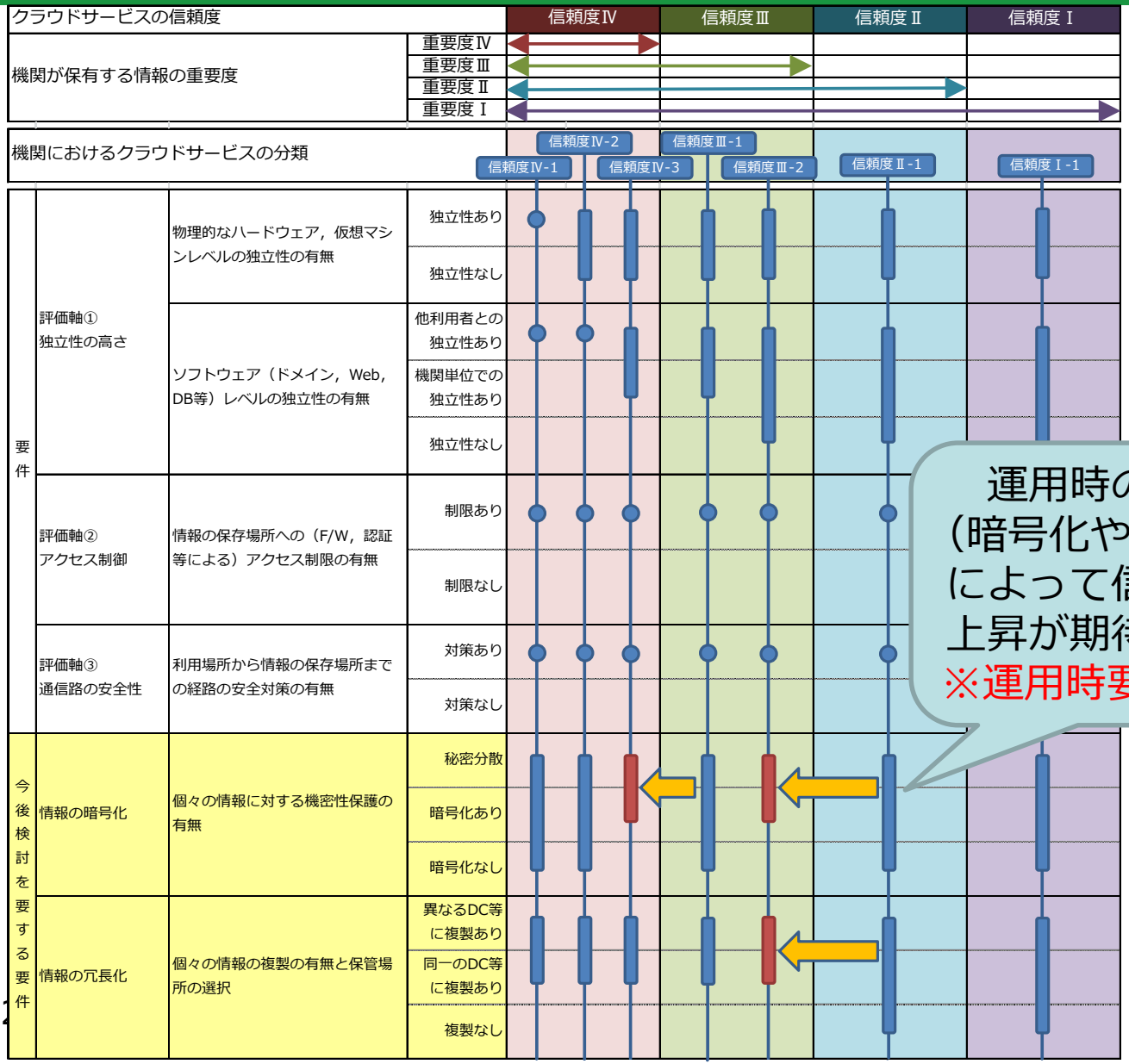
- 信頼度の評価軸
  - ① 独立性の高さ(他の利用者との隔離)
  - ② アクセス制御(データアクセスのための利用者認証)
  - ③ 通信路の安全性(暗号化やアクセス区域の制限)
- 機関が保有する情報の重要度との関連付け
  - 例) 信頼度Ⅲのクラウドサービスには、機関が保有する重要度Ⅲ以下の情報を保存できる

「広島大学クラウドサービス利用ガイドライン」における
クラウドサービス利用基準

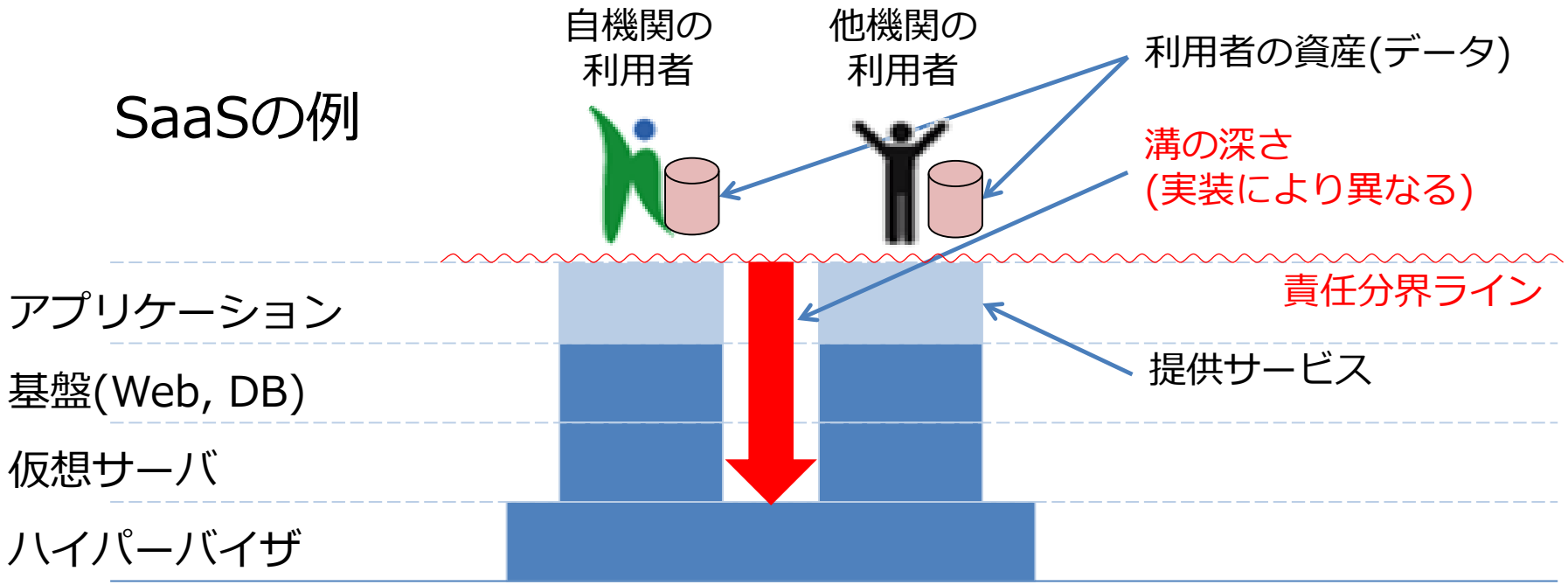


- 運用時の基準として、以下の要件の検討が必要
  - 情報の暗号化(個々の情報に対する機密性保護の要否)
  - 情報の冗長化(個々の情報の複製の要否と保存場所の選択)

「広島大学クラウドサービス利用ガイドライン」における
クラウドサービス利用基準(含運用基準)

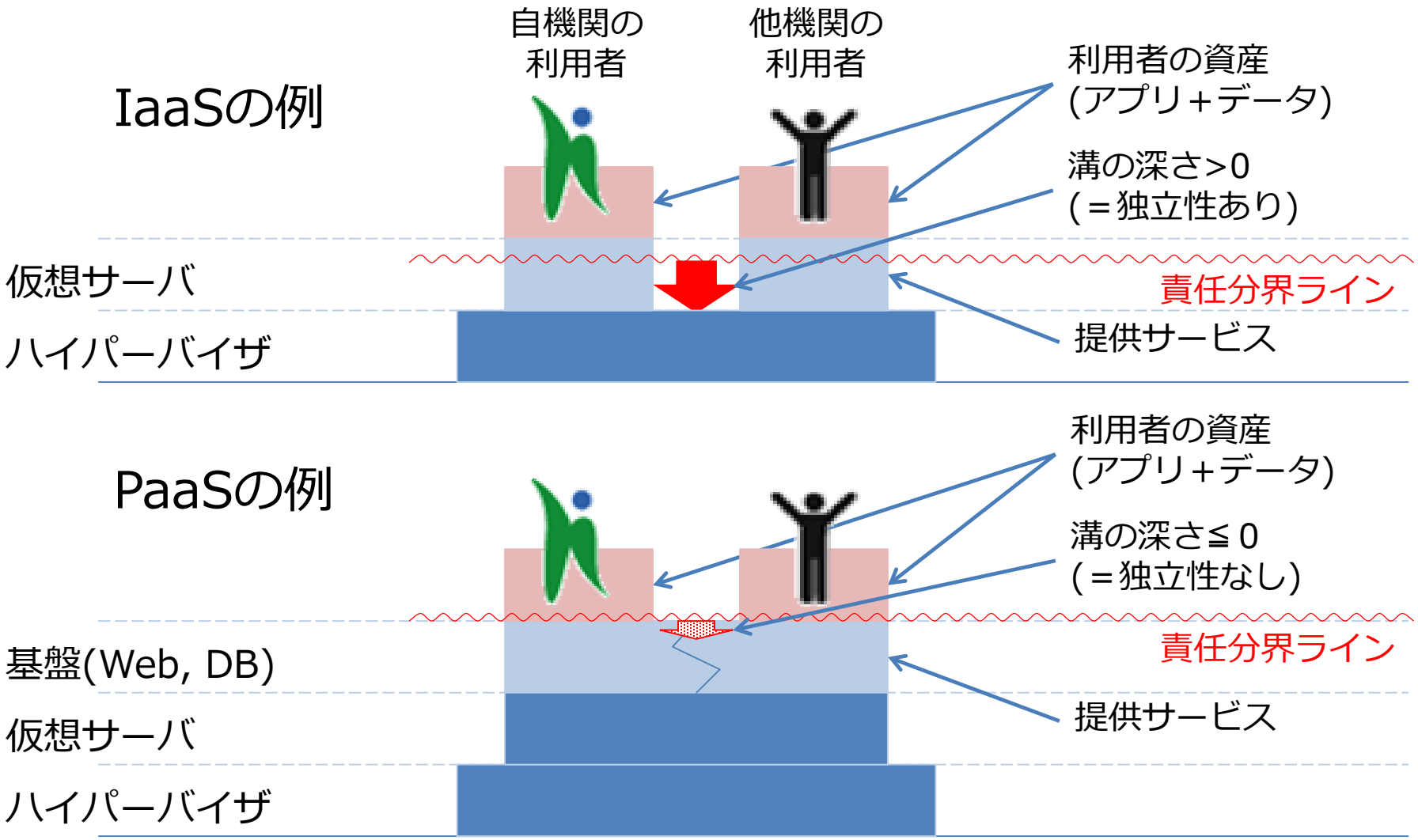


「広島大学クラウドサービス利用ガイドライン」における独立性の高さ

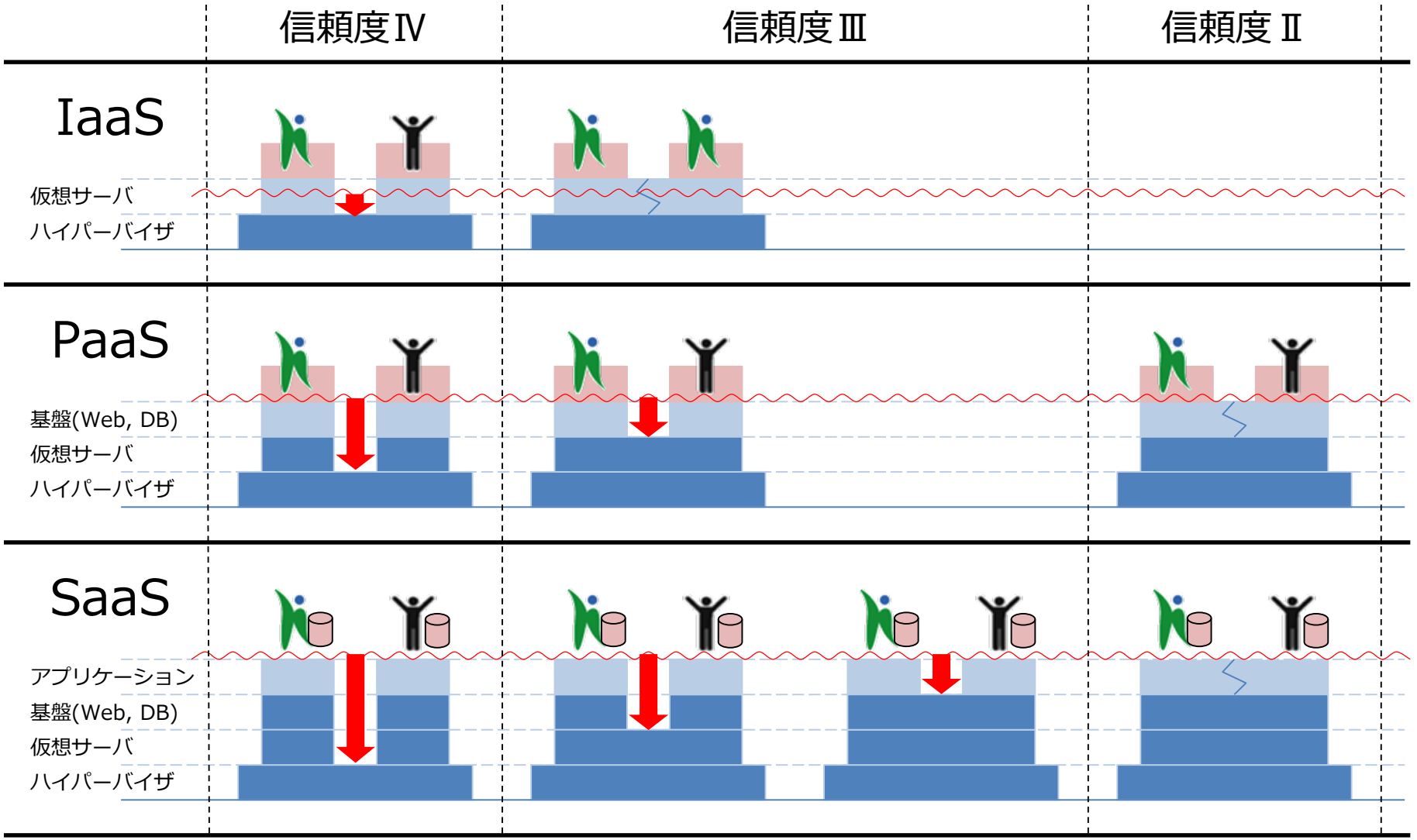


- クラウド事業者提供の情報(サービス仕様書やヒヤリング)から判断
  - サービスモデル(＝責任分界ライン)
  - 実装方法(＝溝の深さ)
- 「責任分界ラインより溝が深い」 → 独立性がある

「広島大学クラウドサービス利用ガイドライン」における独立性の高さ(つづき)



「広島大学クラウドサービス利用ガイドライン」における サービス(実装方法)と信頼度の対応



広島大学のクラウド化手順

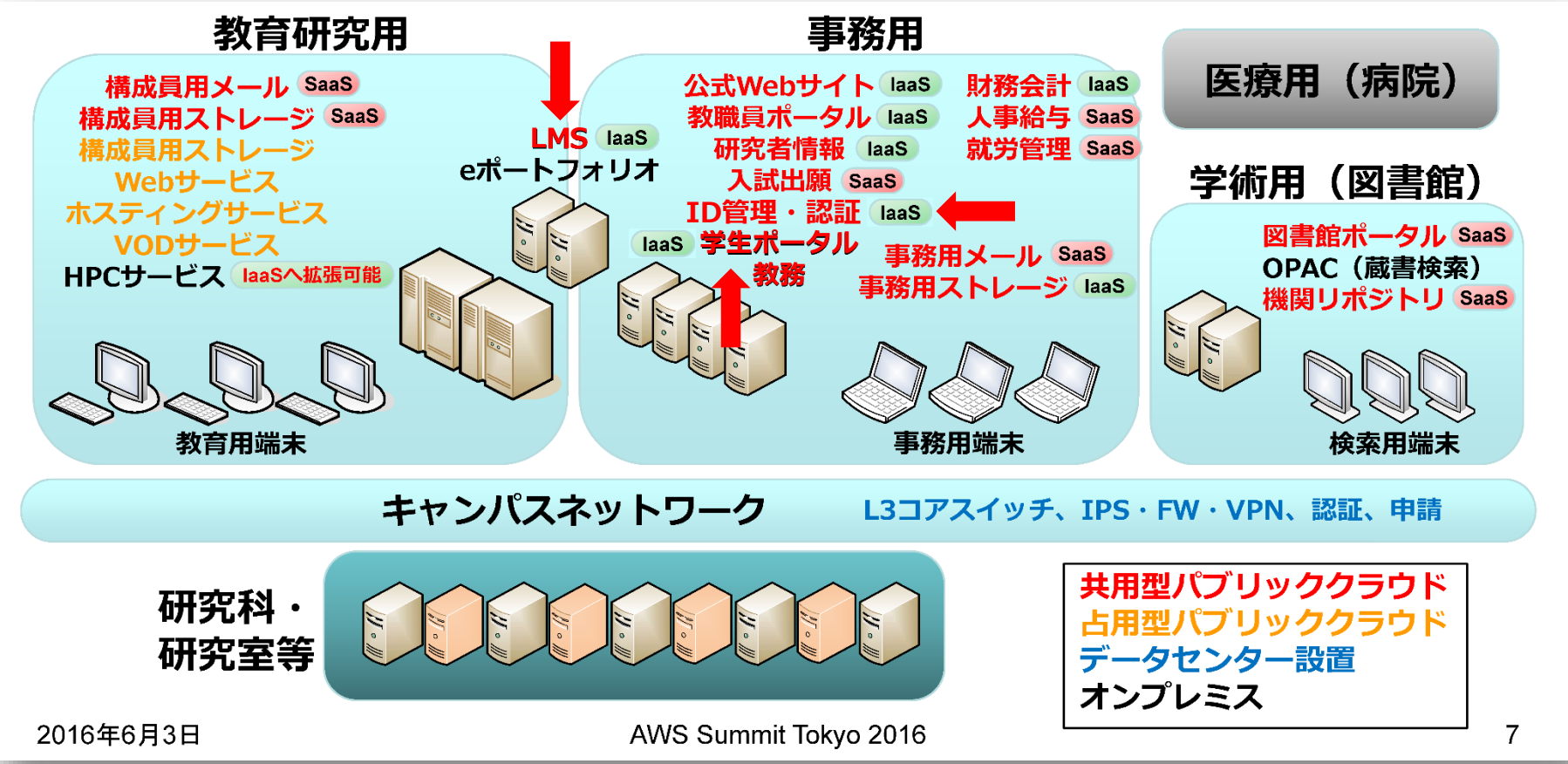
- クラウドサービス利用ガイドラインの整備
  - 全学的な統一基準としてガイドラインを策定
    - 情報セキュリティ委員会(全学委員会)にWGを設置して検討
  - 絶対的な基準を定めることは困難
    - 確認すべき要素の定義とチェックリストの提供
      - 運用上注意すべき項目の明確化
      - オンプレミスの場合でも同様の手順が必要

  → 担当者レベルでの確認・判断が可能となった
- 財務会計・人事システム等をクラウド化
  - アプリケーションを(原則)そのまま移行

  → 事務系システムの心臓部のクラウド化がほぼ完了

- 認証連携は後回し
  - ガイドラインで認証システムのクラウド上設置が判断可能に
    - センター等にいちいち相談する必要がなくなった
  - 事務系と教研系の情報担当部署が異なるという事情
    - 認証連携は教研系(メディアセンター)が主導

広島大学のクラウド化の状況（2020年6月末）



- 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

ガイドライン策定の功罪？！

広島大学

- 確認すべきポイント(問題点)の明確化
  - オンプレミスの安全神話化
    - PDCAサイクルの重要性を再認識

    → **ISMS認証取得(2015年3月取得、2018年2月更新、継続中)**
    ISMS-CLS認証取得(2017年3月取得、2018年2月更新、継続中)
  - 担当者レベルでの確認・判断
    - 安易なクラウド化を助長する、かも…

    → **定期的なチェック義務化が必要(第二版で明文化)**
- システム構築手法見直しの契機
  - ハードウェアのライフサイクルの変化
    - これまでの調達手続き(4～5年単位)とのミスマッチ

    → **大型システムの調達をどうするか？(単価契約)**
  - ハードウェア指向からサービス指向へ
    - 機能性能の評価方法

    → **(HPC以外の)ベンチマークをどうするか？**
    - ソフトウェアライセンスのクラウド上での利用

    → **BYOL(Bring Your Own License)できるか？**

電子計算機システム(HUC12)

- キーワードは「トランジション」(スムーズな移行)
  - ハードウェア指向からサービス指向へ
    - オンプレミスからクラウド利用へ
    - 端末システムの大学による整備からBYODへ
- 基本方針
  - 更新時期と運用期間
    - 2015年9月から5年間　→ 2020年9月更新予定
  - 利便性の向上と運用効率化のためのサービスの再配置
    - パブリッククラウドの活用 → 電子メールはOffice365へ移行
  - 全学情報基盤の整備・充実
    - プライベートクラウドの構築・活用
  - HINET2014およびSINET5(2016年4月～)の活用
    - 安全かつシームレスなネットワーク環境
  - 学内外の各種情報システムとの連携
    - ID／認証連携
  - 構成員が所有する計算機資源の有効活用
    - パソコン必携化 → 2015年4月入学生から
    - 教育用端末の運用 → 2017年度末で終了 → 規模を縮小して継続

大学等におけるクラウドサービス利用

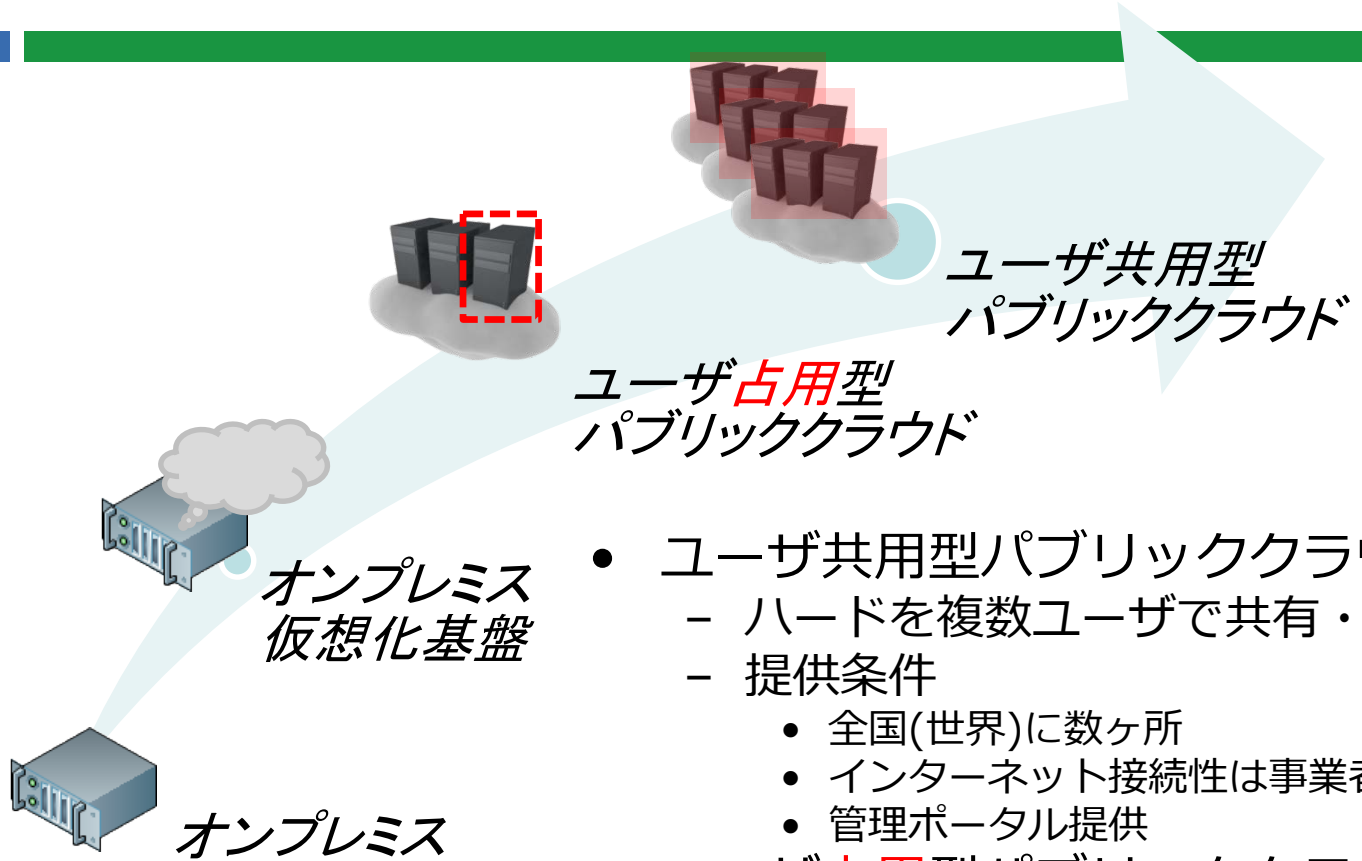
広島大学

- クラウド選択の際の２つの軸
  - 占用？共用？
    - ハードを単一ユーザ(組織)で占用するか、複数ユーザ(組織)で共用するか
  - 近い？遠い？(速い？遅い？)
    - 応答時間に厳しいサービスとそうでもないサービス

  ⇒地域のDCと全国(世界)規模のDCを使い分ける
    - これらの組み合わせが一括して(横断的に)管理できること
- (大学のシステムとして)クラウドを利用しにくいサービス
  - HPC
    - 大量・高性能な計算リソースを使用
    - 稼働率が高い

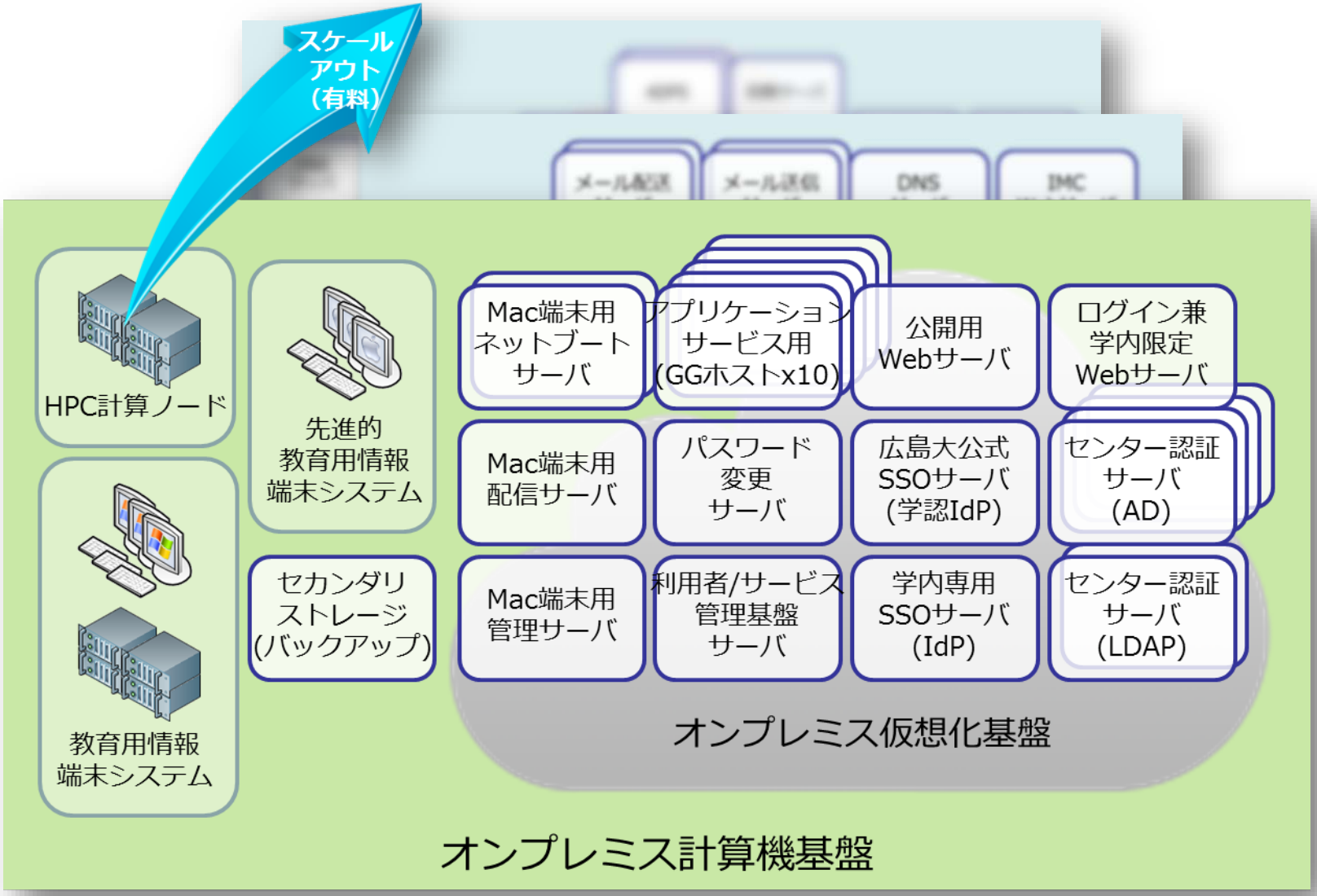
    ⇒必要最小限をオンプレミスで構築し、パブリッククラウドにスケールアウト可能に(有料)
  - 利用者／認証情報・データ
    - データ管理上は…オンプレがオリジナル、クラウドはキャッシュ
    - データ利用上は…クラウドをプライマリ、オンプレはバックアップ

クラウド本格利用に向けたトランジション

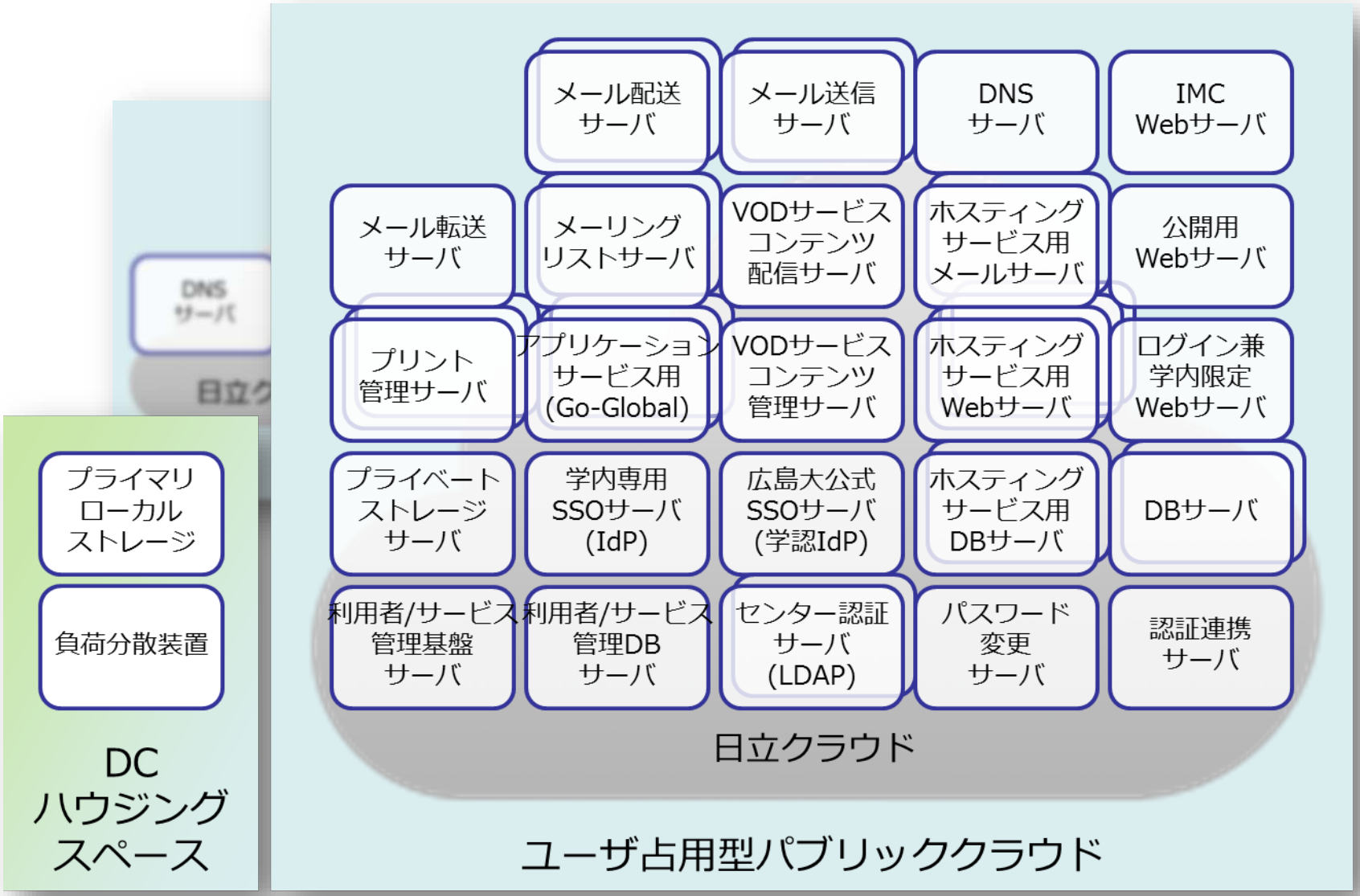


- ユーザ共用型パブリッククラウド
  - ハードを複数ユーザで共有・インスタンス単位課金
  - 提供条件
    - 全国(世界)に数ヶ所
    - インターネット接続性は事業者が提供
    - 管理ポータル提供
- ユーザ占用型パブリッククラウド
  - ハードを単一ユーザで占用・ハード単位課金
  - 提供条件
    - ユーザ拠点の近く
    - インターネット接続性は利用者が提供
    - 共用型と共通の管理ポータルから制御可能

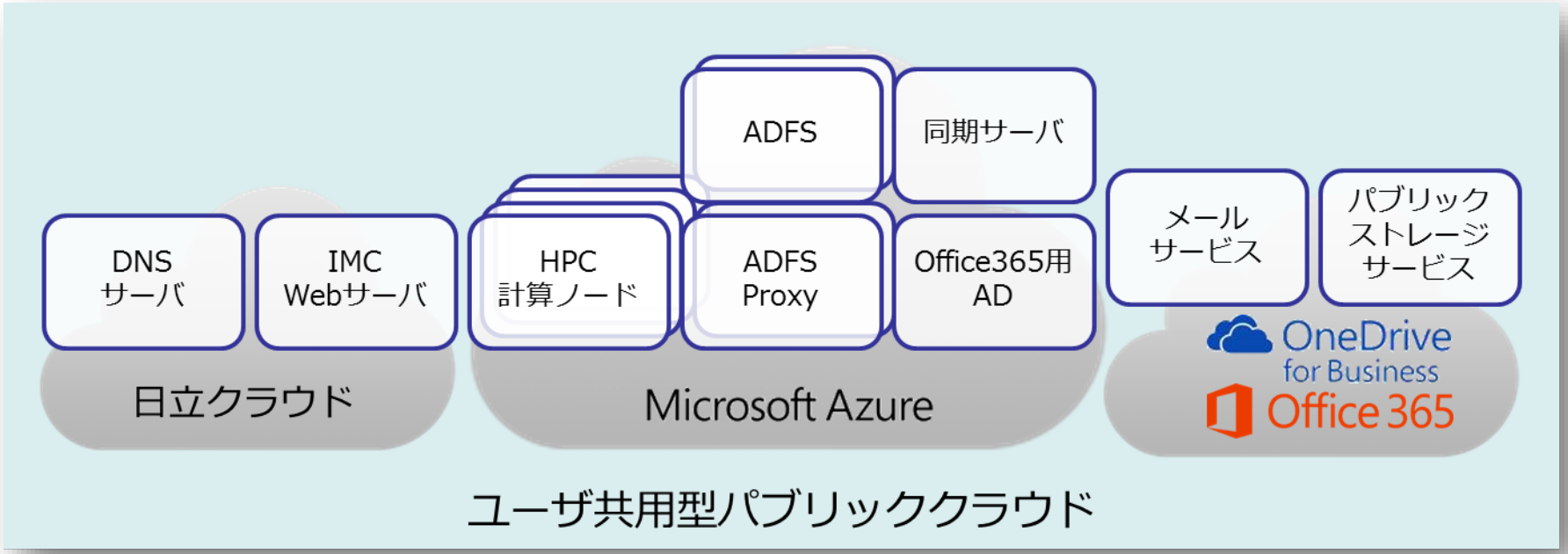
HUC12構成(オンプレミス計算機／仮想化基盤)



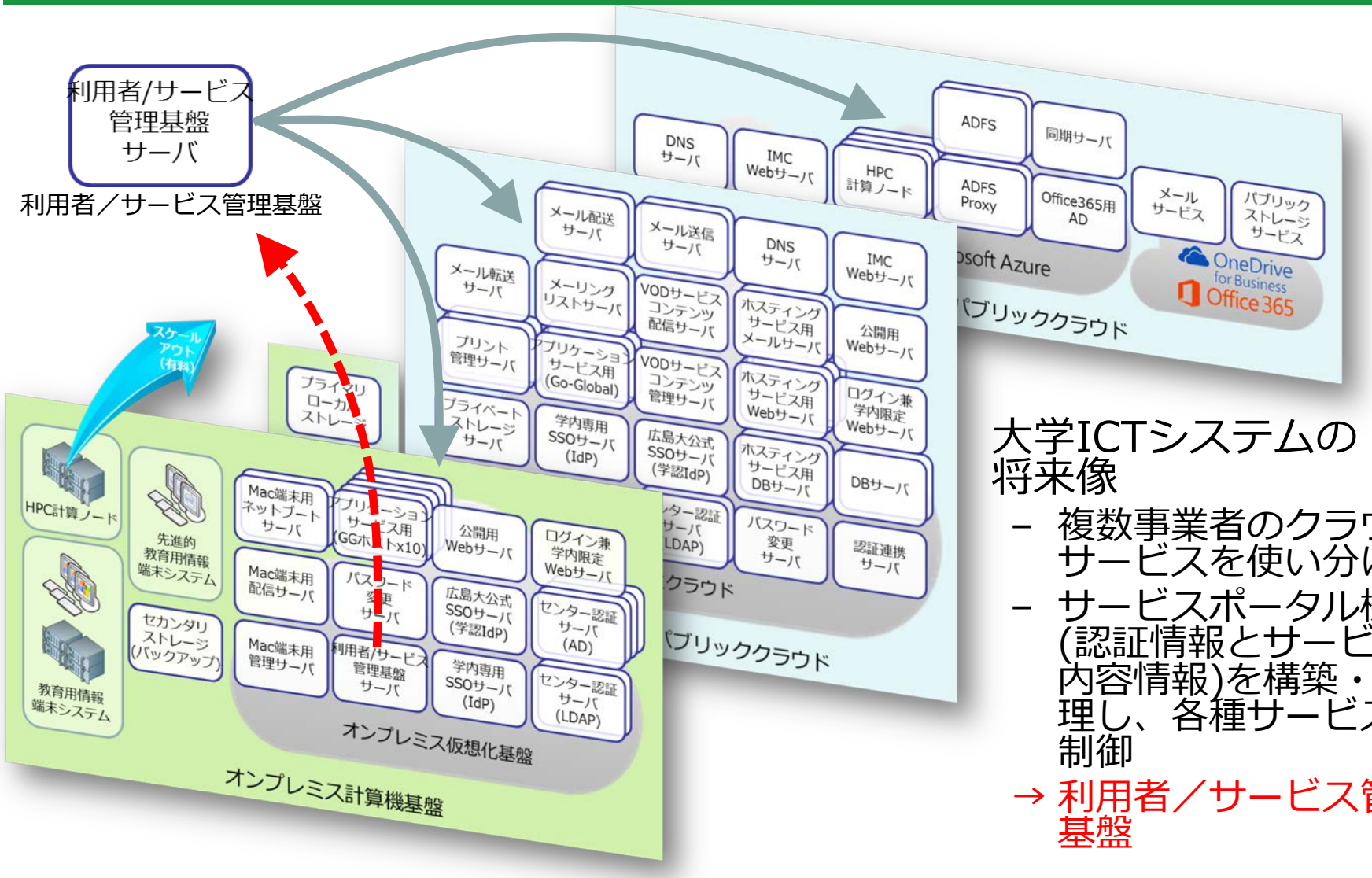
HUC12構成(ユーザ占用型パブリッククラウド)



HUC12構成(ユーザ共用型パブリッククラウド)



HUC12全体構成



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
- サービスポータル機能(認証情報とサービス内容情報)を構築・管理し、各種サービスを制御

→ 利用者／サービス管理基盤

広島大学における

ISMS/ISMS-CLSの取り組み

ISMS(情報セキュリティマネジメントシステム)

- 情報メディア教育研究センターでISMS認証を取得
  - 2014年度末認証取得
    - 登録日(2015年3月27日)
    - 更新日(2018年3月27日)、継続中
    - ISMS認証取得組織検索(ISMS-AC)
  - 適用規格
    - ISO/IEC 27001:2013(JIS Q 27001:2014)
- 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
    - 前のスライドを思い出してください

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

大学ICTの将来像
大学はサービスポータル機能（認証情報とサービス利用情報）を構築・管理し、各種サービスを制御

- リスクアセスメントと管理策の策定
  - オンプレミスとパブリッククラウドのリスクを「冷静に」比較できた
  - クラウドサービス利用ガイドラインでも確認

ISMS規格のクラウド対応

ISMS

2015年3月認証取得
(2018年３月更新、継続中)

ISO/IEC 27001:2013

ISO/IEC 27002:2013

経済産業省
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

http://www.meti.go.jp/policy/netsecurity/downloadfiles/cloudsec2013fy.pdf

ISO/IEC 27017:2015

クラウドセキュリティ
- アカウント管理、仮想化技術、ストレージ管理等のシステム管理
- 事業継続性、障害復旧などへのマネジメント対策等

AddOn

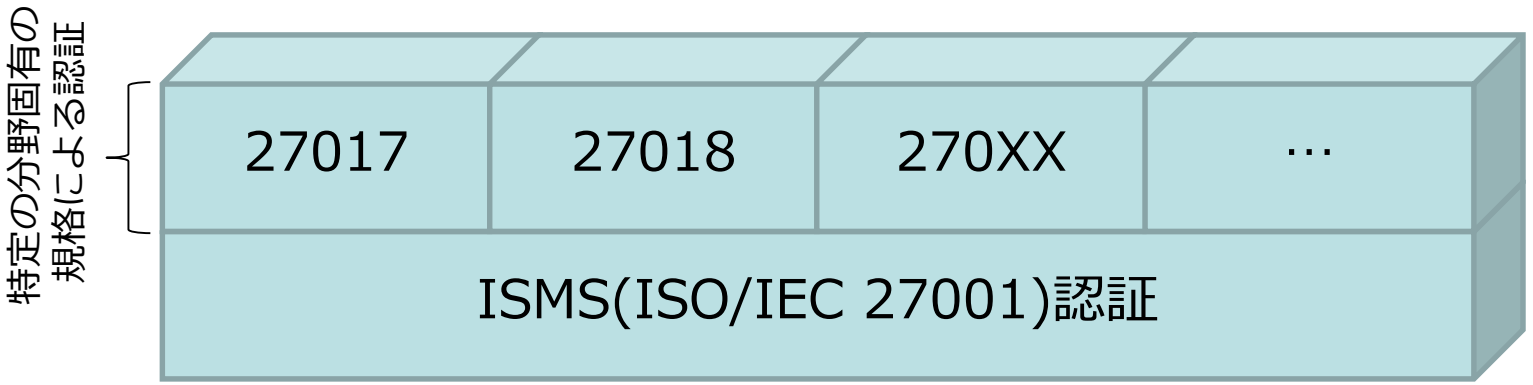
ISMS-CLS

2017年3月認証取得
(2018年3月更新、継続中)

- ISO/IEC 27017:2015によって
  - クラウドサービス提供者(プロバイダ)は、カスタマに提供すべき情報がわかる
  - クラウドサービス利用者(カスタマ)は、プロバイダに要求すべき情報がわかる
- クラウドサービス利用ガイドライン／チェックリスト
  - 認証取得を通してカスタマ向けチェックリストとして機能するか検証

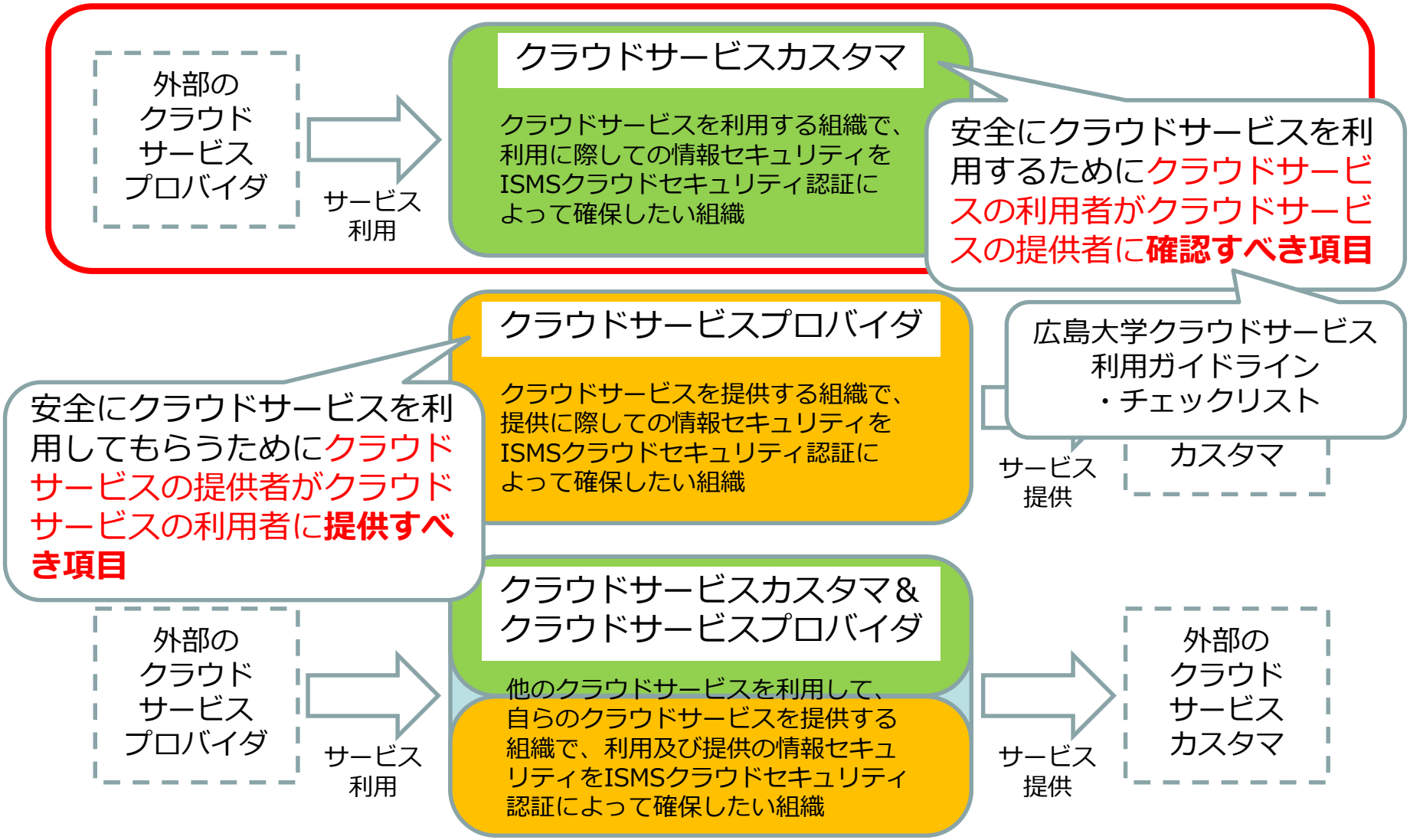
ISMSクラウドセキュリティ認証とは

- 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 情報マネジメントシステム認定センター（ISMS-AC） 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
  - 「アドオン認証」とは？
    - ISO/IEC 27001を取得している(情報セキュリティの基礎が整っている)ことを前提とする
      - ISO/IEC 27017単独での認証取得はできない



ISMSクラウドセキュリティの内側 ～カスタマとプロバイダの立場を区別～

広島大学



ISMS/ISMS-CLS登録証

Japan Audit and Certification Organization for Environment and Quality

051

国立大学法人広島大学
情報メディア教育研究センター
広島県東広島市鏡山1-4-2

登録証

登録番号:IC14J0392

ISO/IEC 27001:2013・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

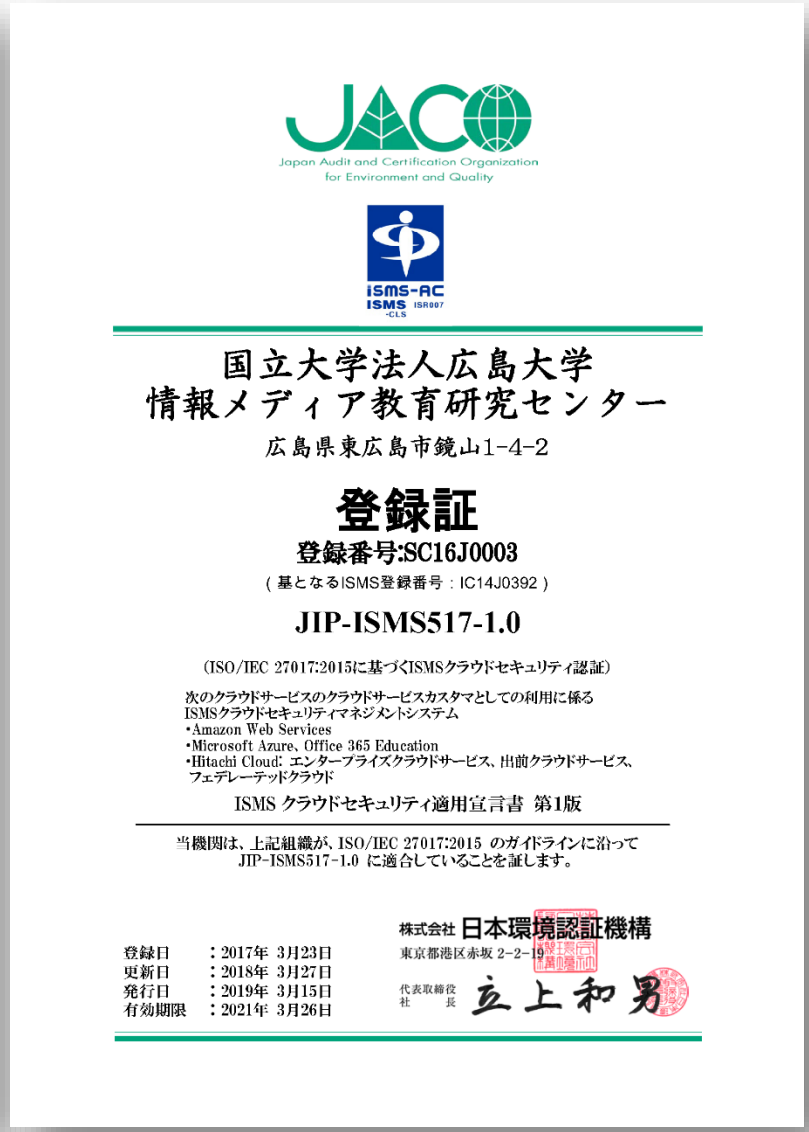
ISMS適用宣言書 第2版

当機関は、上記組織が、当該マネジメントシステム
要求事項に適合していることを証します。

登録日 ：2015年 3月27日
更新日 ：2018年 3月27日
発行日 ：2019年 3月15日
有効期限 ：2021年 3月26日

株式会社 日本環境認証機構
東京都港区赤坂 2-2-19
代表取締役社長 立上和男

本証は登録証の一部ですので、付属書と合わせてご覧ください。



Japan Audit and Certification Organization for Environment and Quality

国立大学法人広島大学
情報メディア教育研究センター
広島県東広島市鏡山1-4-2

登録証

登録番号:SC16J0003

（基となるISMS登録番号：IC14J0392）

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）

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
・Amazon Web Services
・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

ISMS クラウドセキュリティ適用宣言書 第1版

当機関は、上記組織が、ISO/IEC 27017:2015 のガイドラインに沿って
JIP-ISMS517-1.0 に適合していることを証します。

登録日 ：2017年 3月23日
更新日 ：2018年 3月27日
発行日 ：2019年 3月15日
有効期限 ：2021年 3月26日

株式会社 日本環境認証機構
東京都港区赤坂 2-2-19
代表取締役社長 立上和男

ISMS/ISMS-CLS認証取得の表示

ISMS/ISMS-CLS認証取得の取組み

広島大学

株式会社日本環境認証機構（JACO）様からのエンドースメント

国立大学法人広島大学（情報メディア教育センター）様では、全学への情報サービスを提供する基幹システムにおいて、クラウドサービスの積極的な活用を推進されておられます。 それに伴う情報セキュリティ強化の一環として、2015年に情報セキュリティマネジメントシステム（ISMS）認証を取得され、今回、更なる強化・改善を図るべく、学術関連では日本で初めて、ISMSクラウドセキュリティ認証も取得されました。JACOは審査の基本姿勢として、「認証の取得を、ゴールにしない」を掲げておりますが、国立大学法人広島大学様の持続可能な発展のために、今後とも審査を通じて継続的にサポートさせて頂きながら、クラウドセキュリティの更なる改善及び他の大学等への知見の展開を期待いたします。

株式会社日本環境認証機構
ISビジネスユニット長 有吉 英也 様

記念写真

JACO様から27001（左）と27017（右）の登録証を授与されました

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

ISMS認証取得

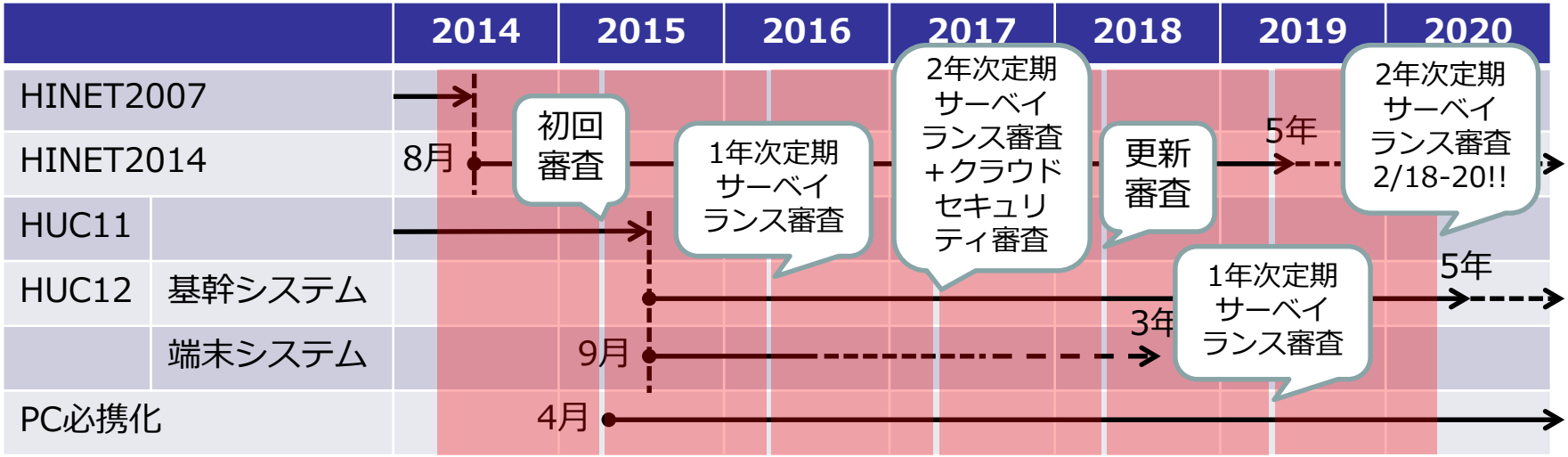
JIS Q 27001:2014
(ISO/IEC 27001:2013)

認証登録番号：IC14J0392

JIP-ISMS517-1.0

認証登録番号：SC16J0003

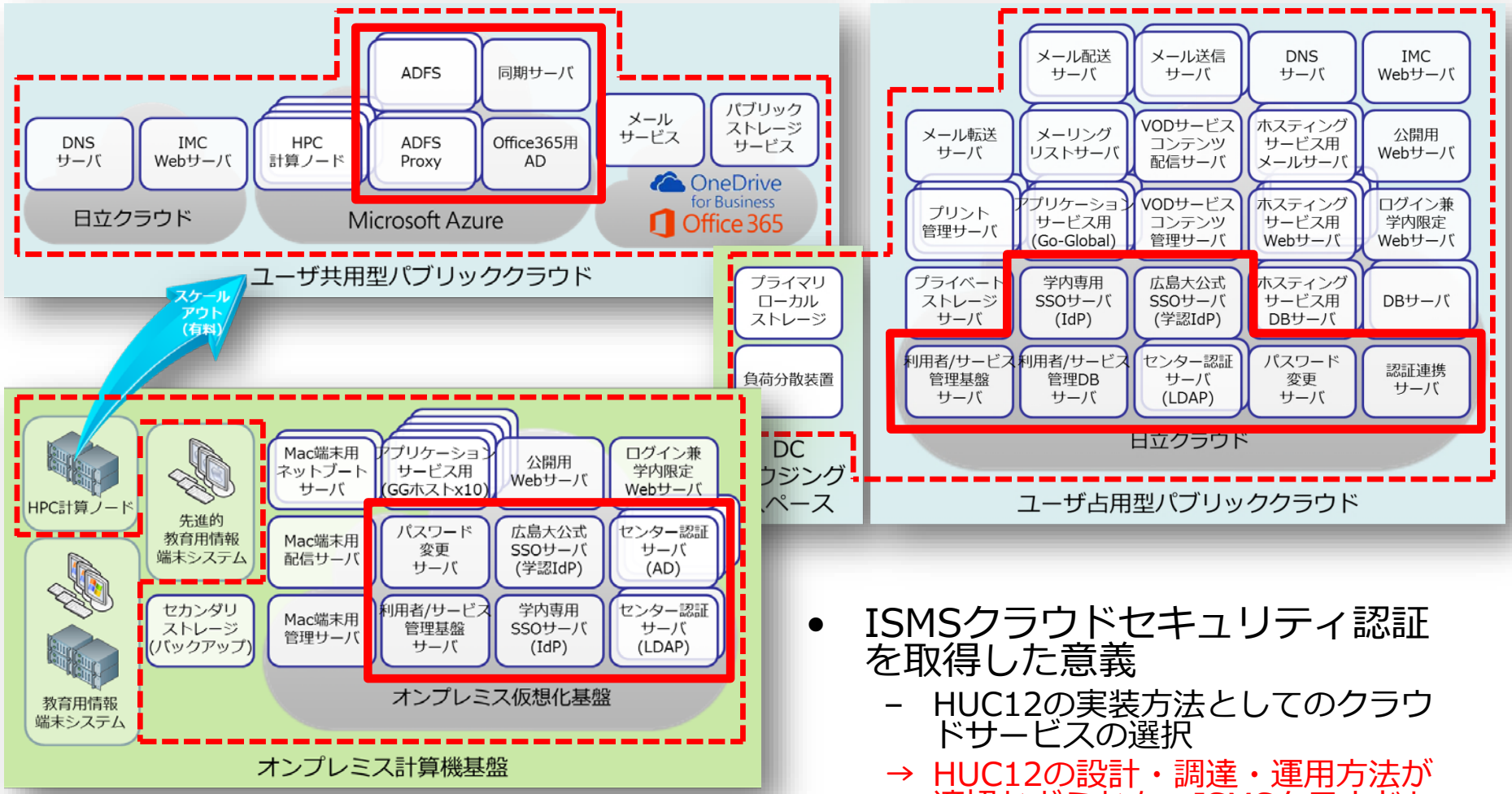
ISMS/ISMS-CLS認証の状況について



- 2015年度はHUC12の導入(旧システムからの移行)・運用開始
  - 旧システムに引き続き、利用者管理(認証)システムを**適用対象**とする
  - キャンパスネットワークと基幹システムは**適用対象(予定)**とし、順次拡大を検討する
  - 端末システムは終息方向のため**適用対象外**とする
- 2016年度はHUC12運用の定常化およびセキュリティ推進体制強化
  - 基幹システムに実現に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**として、**ISMSクラウドセキュリティ認証**(ISO/IEC 27017:2015)を取得
  - 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**
- 2017年度はセキュリティ推進体制の見直し・強化
  - ISMS推進担当者の役職変更に伴う**人的適用範囲の変更**(見直し)
  - ISMS関連文書の見直しに向けた**ISMS事務局体制の変更**(強化)
- 2018年度はISMS関連文書の見直し・運用の省力化
  - ISMS事務局体制を変更し、**ISMS関連文書の大幅な見直し**
  - 証跡を整理し、**ISMSの運用を省力化**

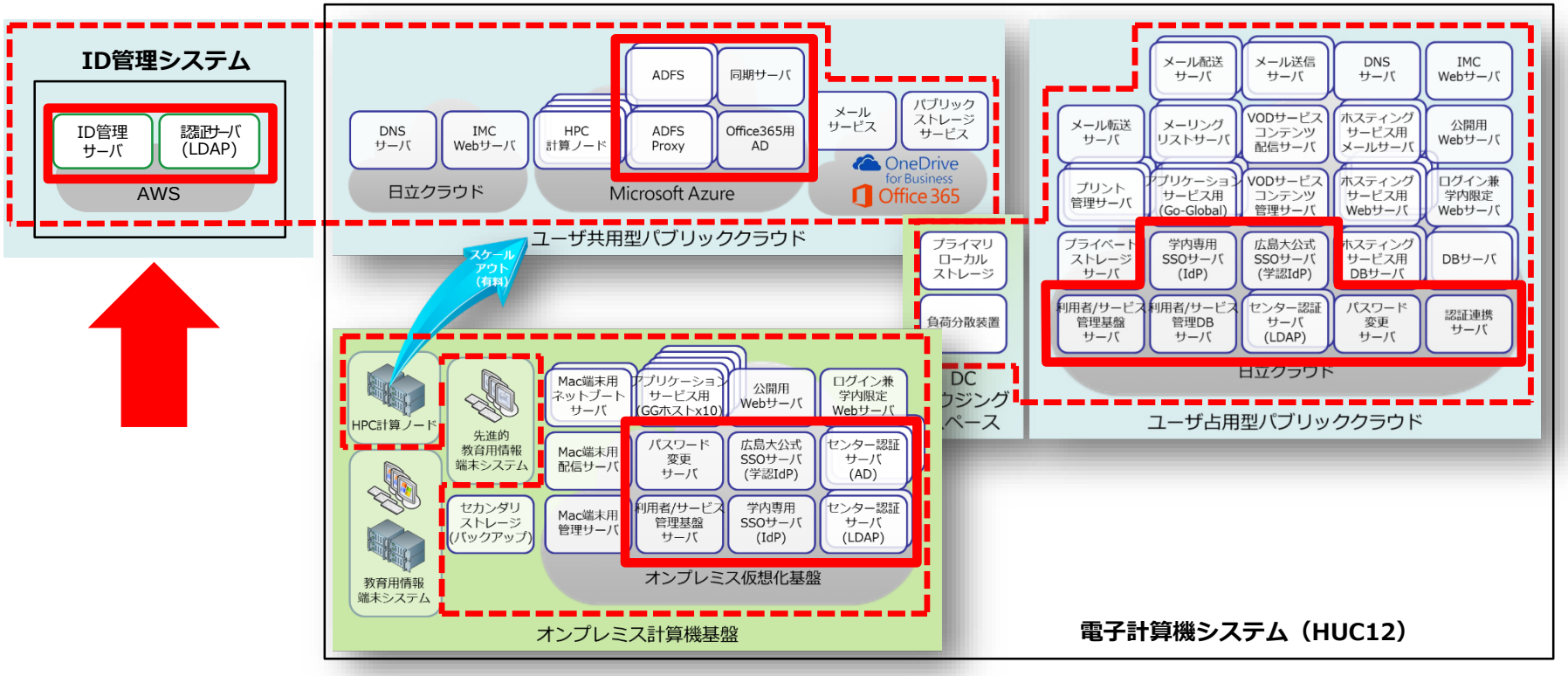
2019年度の課題：
- インシデント対応(フォレンジック)費用の確保→保険
- 事業継続性(BCP)の重視
  →BCMS認証調査　など

HUC12全体構成
技術的適用範囲(ISMS/ISMS-CLS)



- ISMSクラウドセキュリティ認証を取得した意義
  - HUC12の実装方法としてのクラウドサービスの選択
  - → HUC12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用いて確認する

HUC12全体構成
技術的適用範囲(ISMS/ISMS-CLS)の拡大



- ISMSクラウドセキュリティ認証を取得した意義
  - HUC12の実装方法としてのクラウドサービスの選択
  - → HUC12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用いて確認する

クラウドサービスを利用するということ

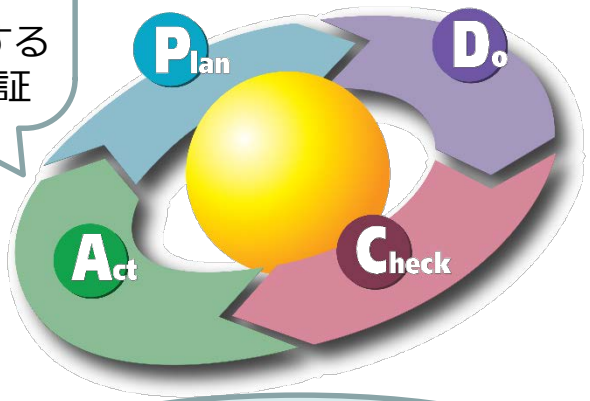
広島大学

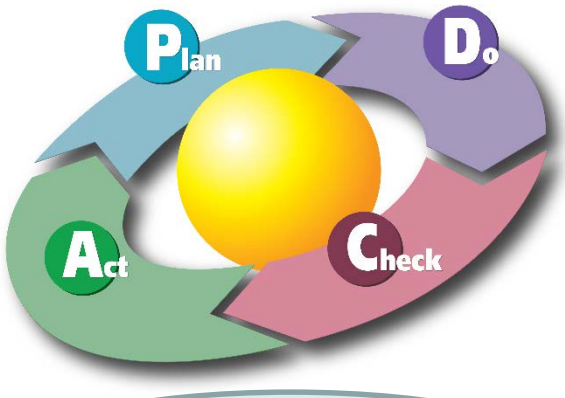
既存システムに対するPDCAが確立されていることが大前提
→ISMSに対するアドオン認証

変化に気づき、対策を講じる

リスクアセスメント

管理策





情報システムのセキュリティ

セキュリティ対策

自営設備による機能実現

クラウド化

セキュリティ対策

リスクアセスメント＆管理策

クラウドサービスによる機能実現

クラウドサービス利用に関する

対外的な取組み(学外への展開)

情報セキュリティガバナンス実態調査

広島大学

NIIオープンフォーラム2019@学術総合センター, 2019/5/29

2018年度学術機関向け情報セキュリティガバナンス実態調査報告

-参加組織の取組みから見る評価上昇の

渡邉英伸

広島大学 情報メディア教育研究セ

HIROSHIMA UNIVERSITY

実態調査の目的

HIROSHIMA UNIVERSITY

- 本実態調査は、学術機関の情報セキュリティガバナンスの実態を把握し、クラウドサービス利用促進させるためのツールを提供することを目的としている
- 実態調査結果により、学術機関全体の傾向から自組織のクラウドサービス利用に対する意識や情報セキュリティガバナンスに関する現状の問題点・課題を明らかにすると同時に、貴組織が次に実施すべき情報セキュリティガバナンスの取組みを明確にすることを目指します。

3

実態調査質問概要

- **質問1**
  - 内容：情報セキュリティに関する組織的な制度・体制、対策導入・運用、評価・点検、見直しの各実態を把握する内容
  - 出題形式：多者択一
  - 質問数：25問
  - 回答条件：必須
  - 有効回答率：100% (43／43機関)
    - 2017年度： 100% (31／31機関)、 2016年度：100% (28／28機関)

ガバナンスの現状の把握

- **質問2**
  - 内容：組織が運用している情報システム名、種別、オンプレミスおよびクラウドの運用・検討状況の各実態を把握する内容
  - 出題形式：記述形式＋多者択一(リスト化)
  - 回答条件：任意
  - 有効回答率：58% (25／43機関)
    - 2017年度： 58% (18／31機関)、 2016年度：82% (23／28機関)

情報資産の管理状況の把握

- **質問3**
  - 内容：過去1年間に発生したクラウドサービス利用に起因する場合と起因しない場合における情報セキュリティインシデントと情報セキュリティトラブルの発生件数・対処時間の各実態を把握する内容
  - 出題形式：記述形式
  - 回答条件：任意
  - 有効回答率：58% (25／43機関)
    - 2017年度： 45% (14／31機関) 、2016年度：60% (17／28機関)

CSIRTの対応状況の把握

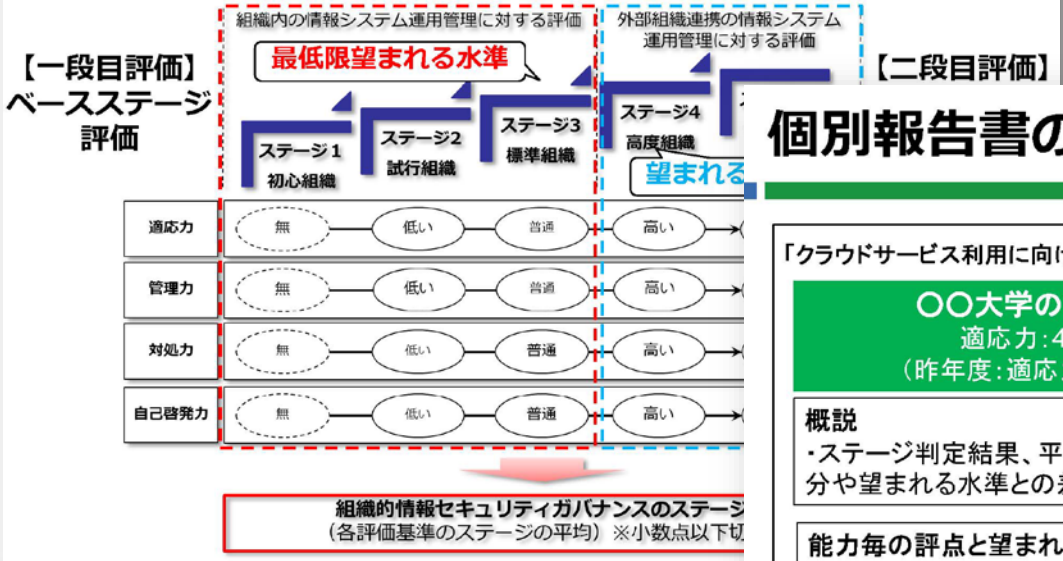
ISMS/ISMS-CLSの考え方に基づき、4つの評価基準で5つのステージに分類

広島大学

評価モデル

HIROSHIMA UNIVERSITY

4つの評価基準と5つのステージレベルで組織の情報セキュリティガバナンスを段階的かつ定量的に評価する（総合評価）



← ベースステージ(ステージ1～3)にステージ4, 5がアドオンして総合ステージが決まる

個別報告書のイメージ

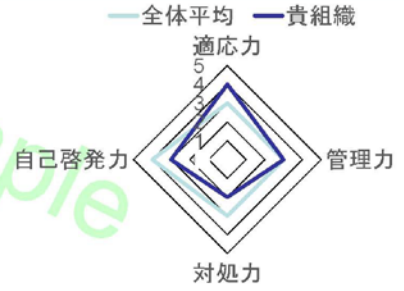
HIROSHIMA UNIVERSITY

「クラウドサービス利用に向けた学術機関のための情報セキュリティガバナンス実態調査」報告書

○○大学の評価結果：ステージ3.0（昨年度：ステージ2.5）
適応力：4.0、管理力：3.0、対処力：2.0、自己啓発力：3.0
（昨年度：適応力：3.0、管理力：2.0、対処力：2.0、自己啓発力：3.0）

概説
・ステージ判定結果、平均ステージとの差分や望まれる水準との差分の状況を記載

能力毎の評点と望まれる水準との差分
・適応力4.0：
・管理力3.0：
・対処力2.0：
・自己啓発力3.0：

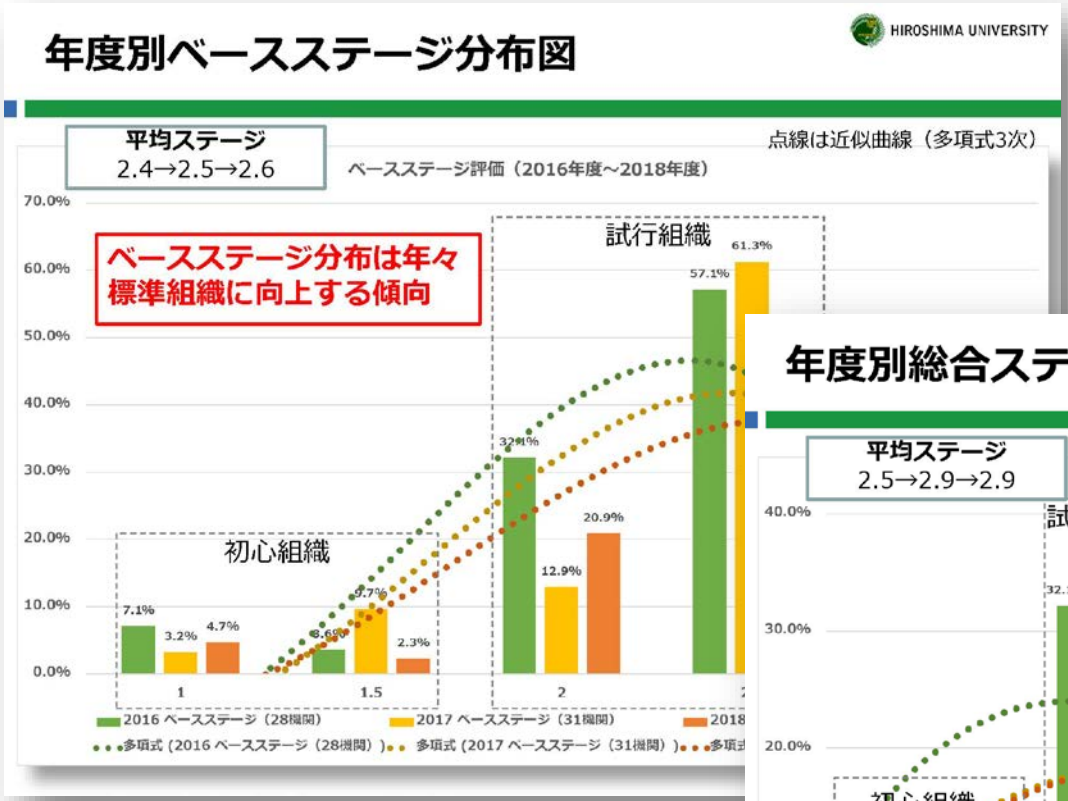


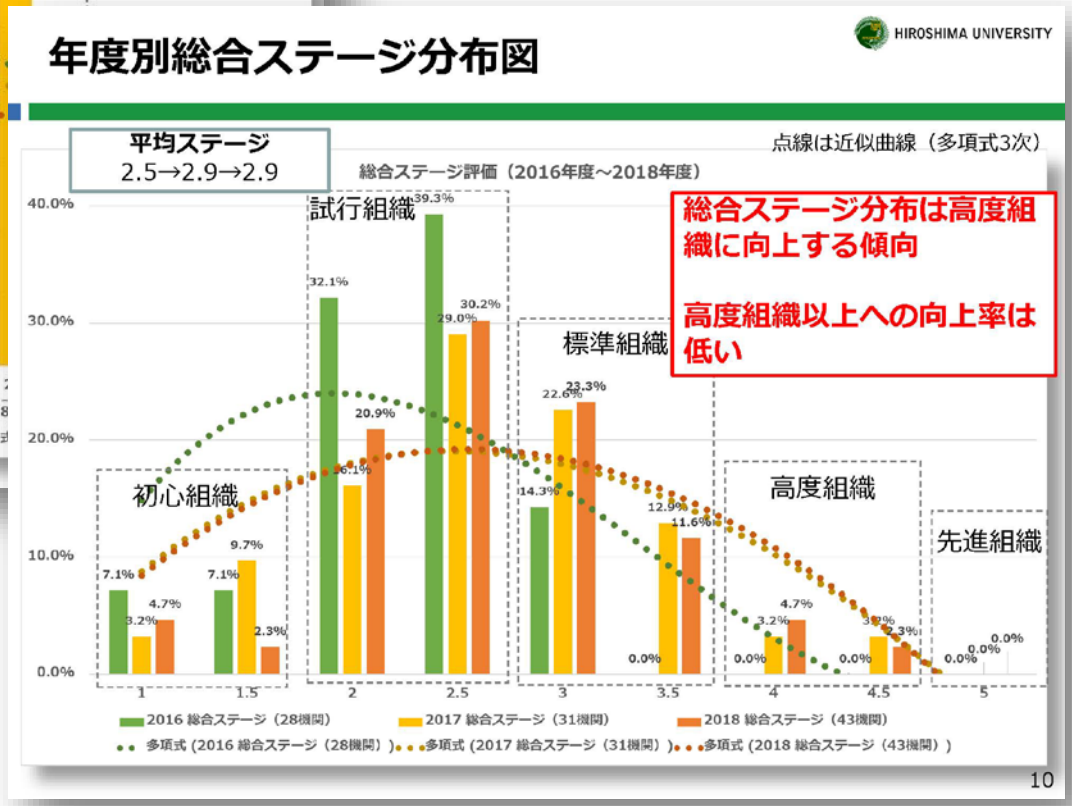
昨年度からの改善傾向 NEW!
・評点が向上した設問を列挙し、どの能力が改善傾向にあるかを記載
今後のポイント
・水準を満たしていない設問を列挙

Sample

6

ガバナンスの状況を経年変化で観測





実態調査質問概要(再掲)

広島大学

- **質問1**
  - 内容：情報セキュリティに関する組織的な制度・体制、対策導入・運用、評価・点検、見直しの各実態を把握する内容
  - 出題形式：多者択一
  - 質問数：25問
  - 回答条件：必須
  - 有効回答率：100% (43／43機関)
    - 2017年度： 100% (31／31機関)、 2016年度：100% (28／28機関)

ガバナンスの現状の把握

- **質問2**
  - 内容：組織が運用している情報システム名、種別、オンプレミスおよびクラウドの運用・検討状況の各実態を把握する内容
  - 出題形式：記述形式＋多者択一(リスト化)
  - 回答条件：任意
  - 有効回答率：58% (25／43機関)
    - 2017年度： 58% (18／31機関)、 2016年度：82% (23／28機関)

情報資産の管理状況の把握

- **質問3**
  - 内容：過去1年間に発生したクラウドサービス利用に起因する場合と起因しない場合における情報セキュリティインシデントと情報セキュリティトラブルの発生件数・対処時間の各実態を把握する内容
  - 出題形式：記述形式
  - 回答条件：任意
  - 有効回答率：58% (25／43機関)
    - 2017年度： 45% (14／31機関) 、2016年度：60% (17／28機関)

CSIRTの対応状況の把握

「クラウド化」の先に見えたもの

「クラウド化」の実際と問題点

- クラウド利用の判断基準
  - ガイドラインによる前例化・免罪符化
    - 過去の利用実績がある
    - ガイドラインで禁止されていない
- IaaS(ハードウェアの置換)での移行
  - 多種多様な機能がソフトウェア的に利用可能
    - 必要に応じて必要な機能を選択
    - 数多ある機能から適切な機能を適切に利用しているか
  - リソースのサイジング(見直し)は適切か
    - 「安全方向(オンプレ時と同じ)で」が多い
    - インスタンス(リソース)の利用率に同程度の余裕が必要？
  - 運用は相変わらず「自分でやりたい」
    - 冗長化，バックアップ，セキュリティ
    - クラウドの故障率に同程度の想定が必要？
- このような「クラウド化」は容易だが固定化(サイロ化)しやすい
  - ハードウェアの更新が不要となるため、見直しの機会を失う
  - フィット＆ギャップ分析などによる定期的な見直しが必要
- 「ISMS/ISMS-CLS認証を維持すること」はその「機会」になる

まとめ

- 広島大学におけるクラウドサービス利用の取り組み
  - 広島大学クラウドサービス利用ガイドライン
    - ハードウェア指向からサービス指向への後押し
    - ガイドラインの功罪
  - 広島大学のクラウド化の状況
    - 電子計算機システム(HUC12)
- 広島大学におけるISMS/ISMS-CLSの取り組み
  - ISMS＋ISMSクラウドセキュリティ
    - 技術的適用範囲の設定と拡大
  - 「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
- クラウド利用に関する対外的な取り組み
  - 情報セキュリティガバナンス実態調査
    - クラウド化は足元を固めることから始めよう
- 「クラウド化」の先に見えたもの
  - 「クラウド化」の実際と問題点
    - ISMS/ISMS-CLSの取り組みはサイロ化を防ぐ「機会」となる