

広島大学における クラウド導入のポイント

情報メディア教育研究センター
西村 浩二

学術情報基盤オープンフォーラム2016

2016/5/28



広島大学



- 西村 浩二（にしむら こうじ）
- 経歴
 - 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）
 - 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）
- 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>
→ 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
- 高等教育期間における情報セキュリティポリシー推進部会
 - 高等教育期間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のテンプレート

- AXIES2014クラウド部会パネル（2014年12月12日）
「大学におけるクラウドのニーズと今後の展望」にて

ユーザと事業者が歩み寄るために



- クラウド利用を妨げている要因（障壁）は何か？
 - ユーザは何が満たされれば「クラウドでGo!」なのかを示す必要がある
- 「ガバナンスを失わない」ために
 - ユーザはどこまで事業者任せにすることができ、どこまで自由にできる必要があるかを示す必要がある
- クラウドはユーザの選択肢の幅を広げたが...
 - (クラウド・SI) 事業者は目的や予算に見合う構成やサービスの提案ができる必要がある

2015年度に行った
電子計算機システム
(HUC12) 調達で
何を検討し、どう
対応したのか？

- クラウド利用を妨げている要因（障壁）は何か？
 - ユーザは何か満たされれば「クラウドでGo!」なのかを示す必要がある
 - クラウド利用に際して確認および対応の検討が必要な項目は？
 - クラウドサービス利用ガイドライン
- 「ガバナンスを失わない」ために
 - ユーザはどこまで事業者任せにすることができ、どこまで自由にできる必要があるかを示す必要がある
 - クラウド化された大学は何を管理するようになるか？（将来像）
 - 利用登録システム
 - 大学が運用するシステムのセキュリティ対策は万全か？
 - ISMS（情報セキュリティマネジメントシステム）
- クラウドはユーザの選択肢の幅を広げたが…
 - （クラウド・SI）事業者は目的や予算に見合う構成やサービスの提案ができる必要がある
 - 仕様書作成や調達過程における大学と業者の役割は適切か？
 - 仕様書の作成方法や調達手順の変更

- クラウド利用を妨げている要因（障壁）は何か？
 - ユーザは何が満たされれば「クラウドでGo!」なのかを示す必要がある
 - クラウド利用に際して確認および対応の検討が必要な項目は？
 - クラウドサービス利用ガイドライン

クラウドサービス利用ガイドライン

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: 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

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

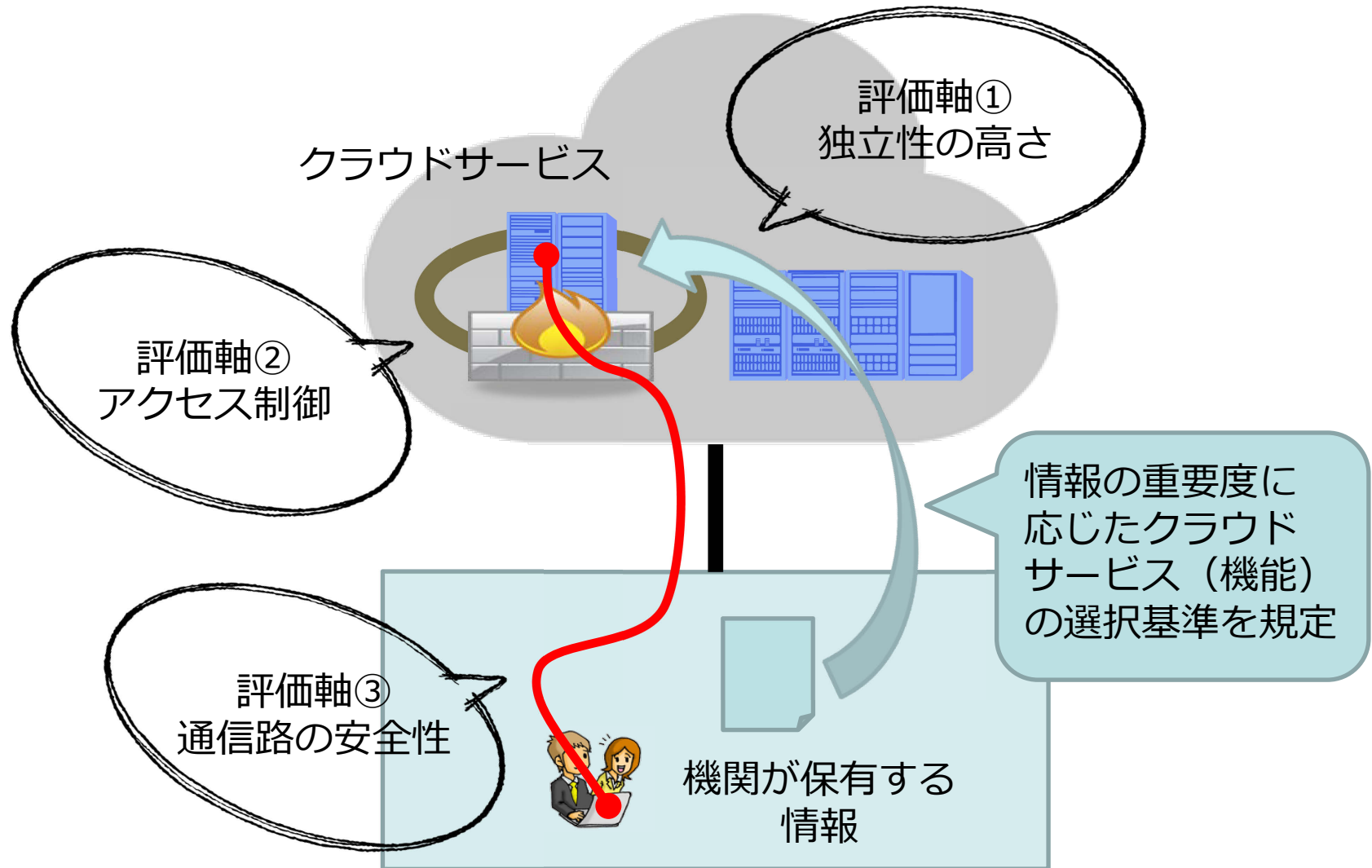
- ガイドラインチェック項目: 46個
- 詳細チェック項目: 88個

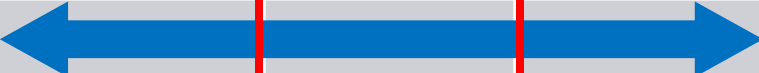
(サービス類型により異なる) <http://www.media.hiroshima-u.ac.jp/news/cloudguide/>

機関が保有する情報の重要度

区分	区分の説明	情報の種類
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
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、グループ又は部局等以外に対して機密を保持すべきもの
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（機関内限定）
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

利用シーンのモデル化と信頼度の評価



クラウドサービスの信頼度		信頼度Ⅳ	信頼度Ⅲ	信頼度Ⅱ	信頼度Ⅰ
機関が保有する情報の重要度	重要度Ⅳ				
	重要度Ⅲ				
	重要度Ⅱ				
	重要度Ⅰ				

- 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

クラウドサービス利用基準

クラウドサービスの信頼度				信頼度Ⅳ	信頼度Ⅲ	信頼度Ⅱ	信頼度Ⅰ
機関が保有する情報の重要度		重要度Ⅳ					
		重要度Ⅲ					
		重要度Ⅱ					
		重要度Ⅰ					
機関におけるクラウドサービスの分類				信頼度Ⅳ-2	信頼度Ⅲ-1	信頼度Ⅱ-1	信頼度Ⅰ-1
要件	評価軸① 独立性の高さ	物理的なハードウェア、仮想マシンレベルの独立性の有無	独立性あり				
			独立性なし				
		ソフトウェア（ドメイン、Web、DB等）レベルの独立性の有無	他利用者との独立性あり				
			機関単位での独立性あり				
			独立性なし				
	評価軸② アクセス制御	情報の保存場所への（F/W、認証等による）アクセス制限の有無	制限あり				
			制限なし				
	評価軸③ 通信路の安全性	利用場所から情報の保存場所までの経路の安全対策の有無	対策あり				
			対策なし				

- 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有無）
 - － 情報の冗長化（個々の情報の複製の有無と保存場所の選択）

クラウドサービス利用基準(含運用基準)

クラウドサービスの信頼度				信頼度Ⅳ	信頼度Ⅲ	信頼度Ⅱ	信頼度Ⅰ	
機関が保有する情報の重要度		重要度Ⅳ						
		重要度Ⅲ						
		重要度Ⅱ						
		重要度Ⅰ						
機関におけるクラウドサービスの分類				信頼度Ⅳ-2	信頼度Ⅲ-1			
				信頼度Ⅳ-1	信頼度Ⅳ-3	信頼度Ⅲ-2	信頼度Ⅱ-1	信頼度Ⅰ-1
要件	評価軸① 独立性の高さ	物理的なハードウェア、仮想マシンレベルの独立性の有無	独立性あり					
			独立性なし					
		ソフトウェア（ドメイン、Web、DB等）レベルの独立性の有無	他利用者との独立性あり					
			機関単位での独立性あり					
			独立性なし					
	評価軸② アクセス制御	情報の保存場所への（F/W、認証等による）アクセス制限の有無	制限あり					
			制限なし					
	評価軸③ 通信路の安全性	利用場所から情報の保存場所までの経路の安全対策の有無	対策あり					
			対策なし					
	今後検討を要する要件	情報の暗号化	情報の暗号化					
			暗号化あり					
			暗号化なし					
情報の冗長化		個々の情報の複製の有無と保管場所の選択	異なるDC等に複製あり					
			同一のDC等に複製あり					
			複製なし					

運用時（暗号化や）によって上昇が期待※運用時

運用時の基準
(暗号化や冗長化)
によって信頼度の
上昇が期待できる
※運用時要検討

ガイドラインのチェック項目

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

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

検討

8. 運用体制の確認

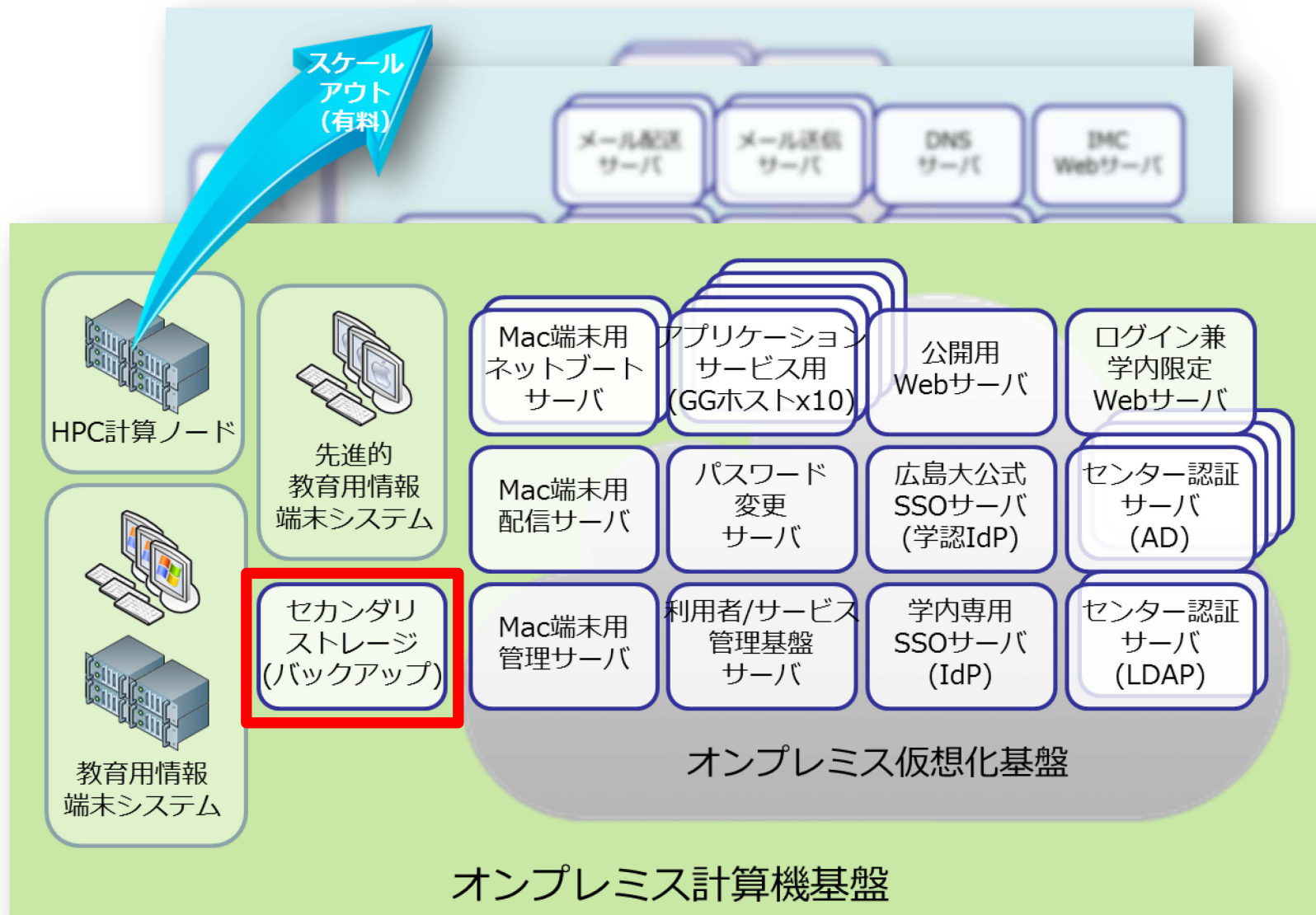
- システムの運用に関する項目
 - セキュリティ対策
 - ログの監視
- データの管理に関する項目
 - 秘密鍵の管理
 - バックアップ(2)
- インシデントの管理に関する項目
 - インシデントの記録(2)

運用

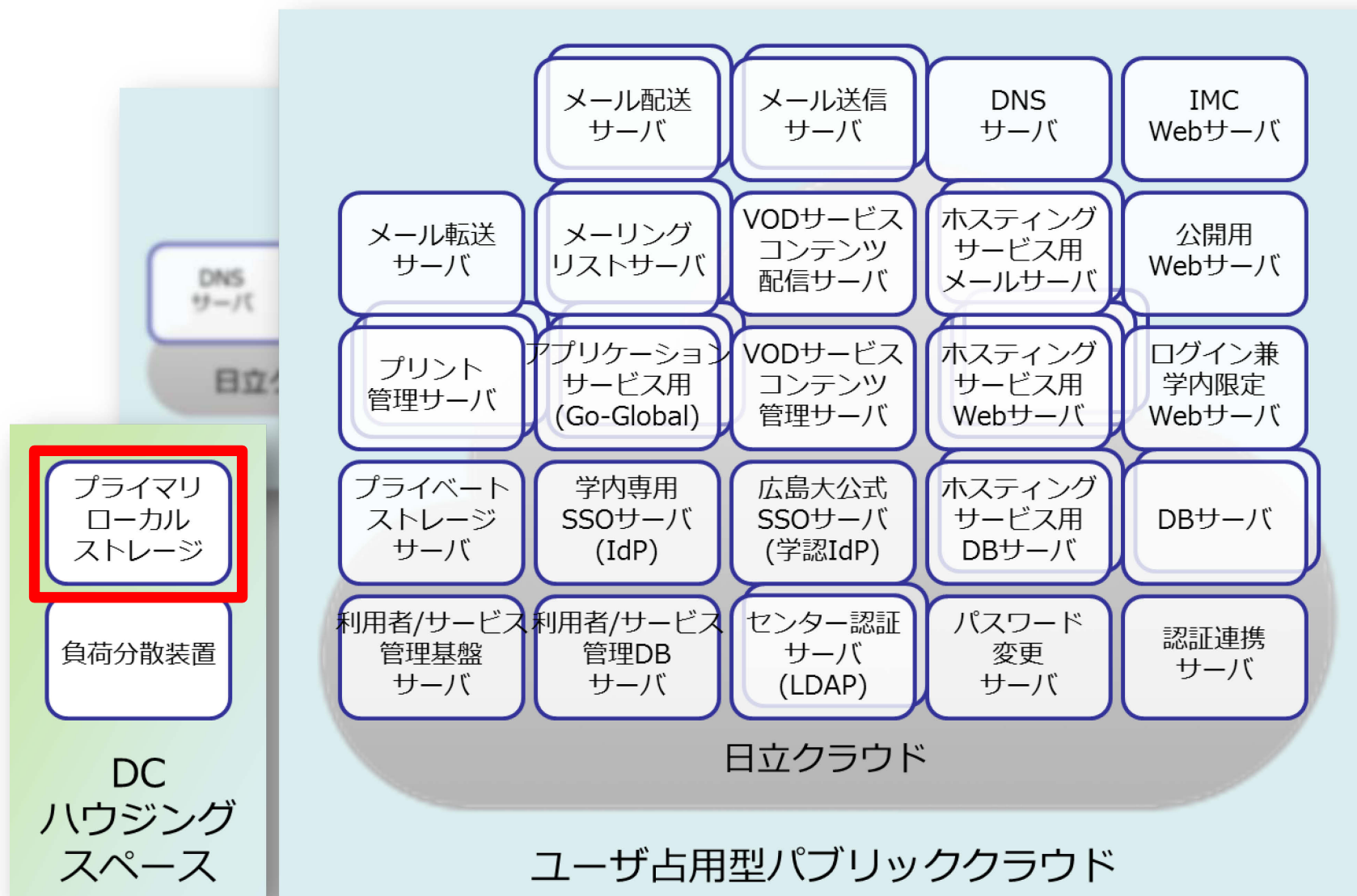
HUC12のチェックリスト(占有型クラウド)

[illegible]

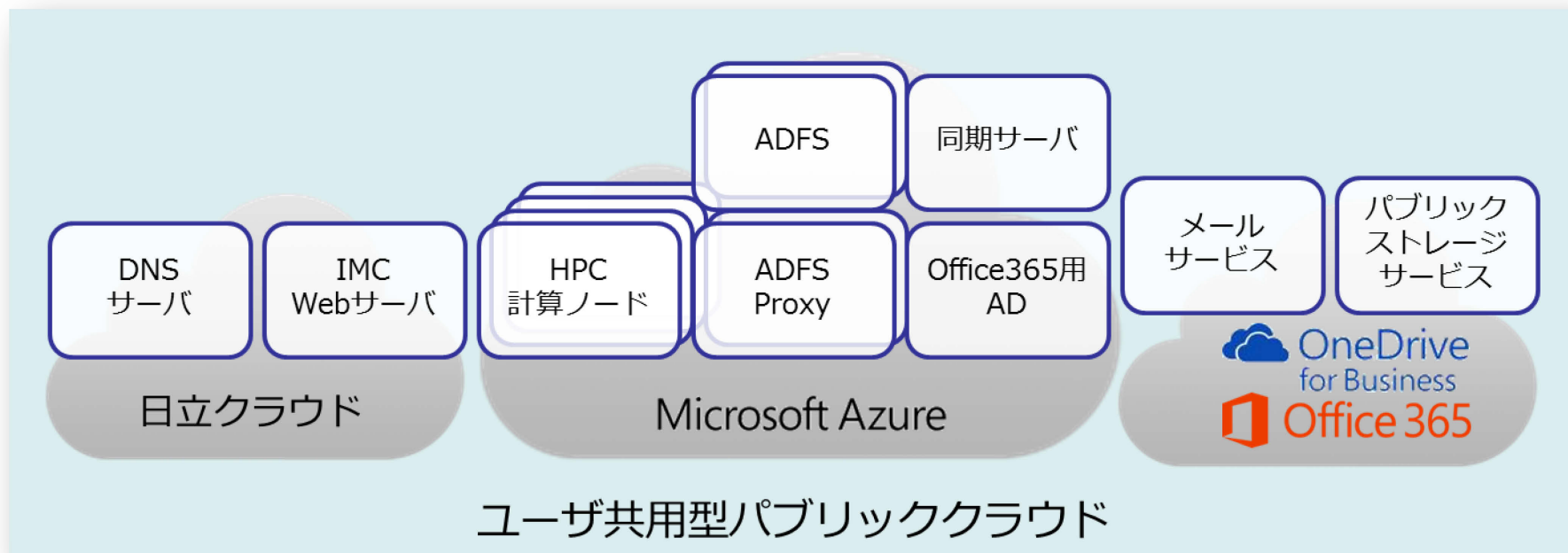
HUC12構成(オンプレミス計算機／仮想化基盤)



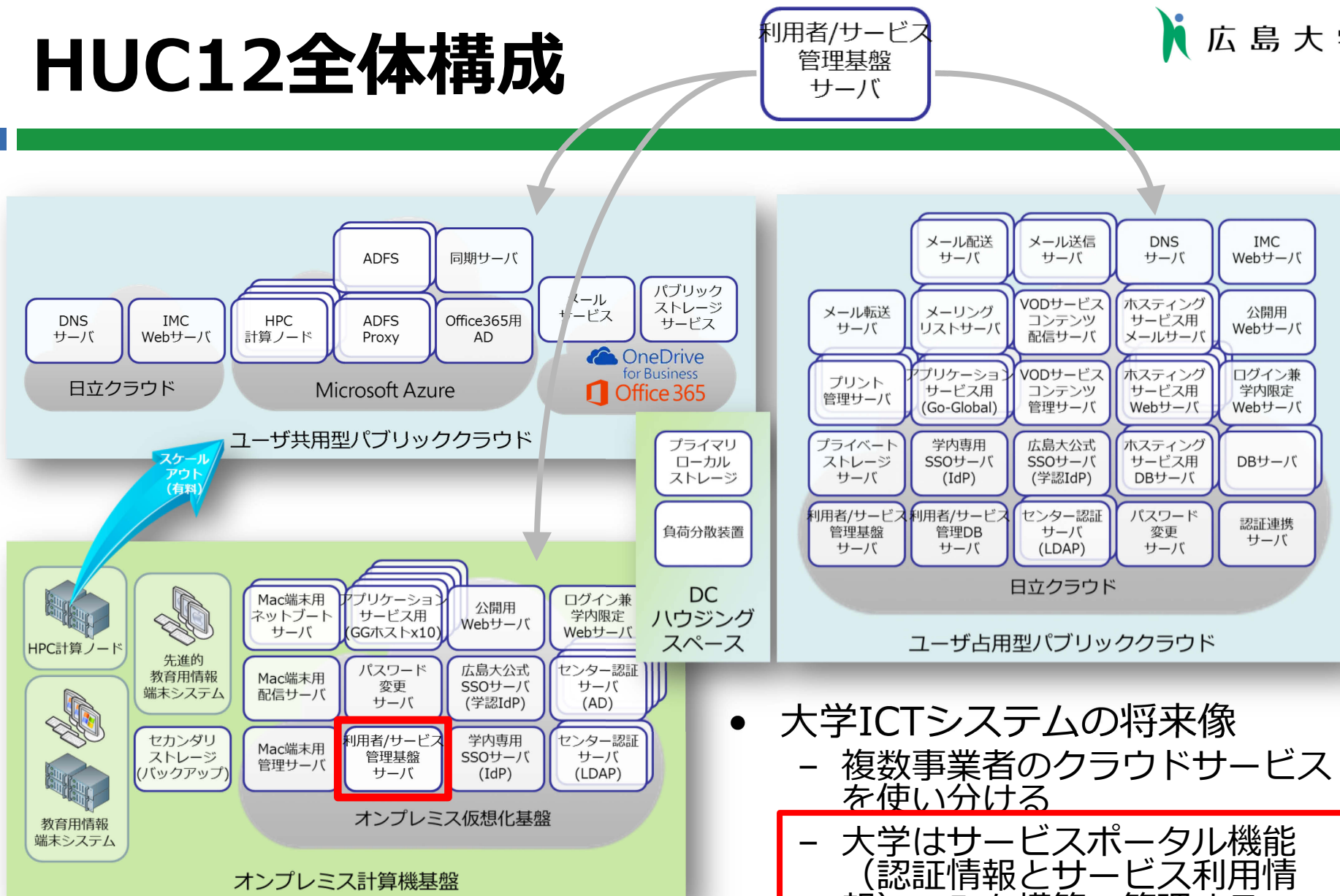
HUC12構成(ユーザ占有型パブリッククラウド)



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る
 - 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）のみを構築・管理する
→『利用者／サービス管理基盤』

- クラウド利用を妨げている要因（障壁）は何か？
 - ユーザは何か満たされれば「クラウドでGo!」なのかを示す必要がある
 - クラウド利用に際して確認および対応の検討が必要な項目は？
 - クラウドサービス利用ガイドライン
- 「ガバナンスを失わない」ために
 - ユーザはどこまで事業者任せにすることができ、どこまで自由にできる必要があるかを示す必要がある
 - クラウド化された大学は何を管理するようになるか？（将来像）
 - 利用登録システム
 - 大学が運用するシステムのセキュリティ対策は万全か？
 - ISMS（情報セキュリティマネジメントシステム）

～利用登録システム～

メディアセンター利用登録システム

広大IDでログインする場合にはこちらから ([login by HIRODAI ID](#))
 広大IDでログインすると、個人アカウントの設定が行えます。

アカウントでログイン ([login by Account](#))
 クラスアカウントを設定するには、こちらからログインしてください。

シングルサインオン機能を使用しています。
 ● [シングルサインオン](#) (別のページを開きます)
 SSOでログインできない場合は [こちら](#) (広大ID / アカウント)

アカウント新規登録時の注意

アカウント登録後はメールが利用できません。
 メール利用はアカウント登録から1週間程度待ちます。



広島大学

HIROSHIMA UNIVERSITY

広島大学 学術認証フェデレーション ログイン
Hiroshima University GakuNin Login

以下のサイトがあなたに認証を求めています。そして認証相機として「広島大学」が選択されました。
 The web site below has asked you to log in, and "Hiroshima University" has been selected as
 your home institution.

このサービスを利用するためには、**広島IDとそのパスワードによる認証が必要**です。
 You need to provide your **HIRODAI ID** and **its password** to use this service.

広島ID / HIRODAI ID

72550712

パスワード / Password

・・・・・・・・・・

Login

メディアセンター 登録システム
 メディアセンター 登録システム

メディアセンターに所属する各種サービスの登録・変更を行うサービスです。

- ▶ ソフトウェアキーボードの表示/非表示
 Show or Hide the Software Key
- ▶ 広島IDとは何ですか？
 What is HIRODAI ID?
- ▶ パスワードを忘れましたか？
 Forgot your password?
- ▶ お手伝いが必要ですか？
 Need Help?
- ▶ シングルサインオン認証について
 About Single Sign-On (SSO)

広島大学は学術認証フェデレーション（学術：GakuNin）に参加しています
 Hiroshima University is a member of Academic Access Management Federation in Japan (GakuNin).

Copyright © 2014 Hiroshima University.
 All rights reserved.

広大IDは
広大構成員に付与
<人の管理>



情報メディア 教育研究センター

Information Media Center

情報メディア教育研究センター サービスログイン

Information Media Center Service Login

以下のサイトがあなたに認証を求めています。
The web site below has asked you to log in.

このサービスを利用するには、IMCアカウントとそのパスワードによる認証が必要です。
You need to provide your IMC Account and its password to use this service.

IMCアカウント / IMC Account

パスワード / Password

Login

メディアセンター登録システム
メディアセンター登録システム 

メディアセンターを利用する各種サービスの登録・変更等はこちらサービスです。

- ソフトウェアキーボードの表示/非表示
- Show or Hide the Software Keyboard
- IMCアカウントとは何ですか？
- What is IMC Account?
- パスワードを忘れましたか？
- Forgot your password?
- お手伝いが必要ですか？
- Need Help?
- シングルサインオン認証について
- About Single Sign-On (SSO)

【72550712 / 西村 浩一】

メディアセンター利用登録システム

ログイン

ログアウト

メニュー (Menu)

- トップページ (Top Page)
- 所有アカウント: kouji (Account function change)
- パスワード変更 (Password change)
- アカウント自主ロック (Account Lock)
- アカウント再取得申請 (Account delete application)

トップページ (広大ID)

お知らせ (News)

お知らせはありません。

サービス受付処理状況 (Service Usage State)

表示する情報はありません。

広大IDでアカウントを管理

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

広大IDで アカウントを管理

アカウントは
サービスを利用する
広大構成員に付与
<サービスの管理>

[725507102 / 西村 浩二]

メディアセンター利用登録システム

ログイン
(login)

広大ID付属
browser.dll

トップページ(アカウント)

メニュー(Menu)

- ▶ トップページ
(Top Page)
- ▶ アカウトル情報
(Account Information)
- ▶ 利用サービス設定
(Service Settings)
- ▶ メールアドレスの管理
(Mail address transfer)
- ▶ 使用状況
(Size status)
- ▶ パスワード変更
(Password change)
- ▶ グループ管理
(Group Management)
- ▶ アクセスアカウント管理
(Access Account Management)
- ▶ トリアカウント管理
(Three Account Management)
- ▶ メーリングリスト
(Mailing List)
- ▶ ホステイング
(Hosting)

お知らせ (News)

お知らせはありません。

サービス受付処理状況 (Service Usage Status)

表示する情報はありません。

利用可能なサービス (Service available)

メールアドレス管理 (Mail)		
メールアドレス (mail)		
Webサービス (Web)		
Webサイト検索 (Private)		
公開利用 (Public)		
メール送信 (Email)		
メール受信 (Receive)		
メール転送 (Forward)		
ネット上の共有サービス (Network)		
共有サービス (Share)		
接続確認 (Item)		
Hinet Web認証		
教育研究支援サービス (Education)		
IC化教育用端末の利用		
HPC利用		
付加サービス (Additional service)		
グループ (group)	3	0
メーリングリスト (mailing list)	14	1
ホスティング (hosting)	10	1
アクセスアカウント (access account)	0	-
ゲストアカウント (guest account)	0	-
各付加サービスの管理者、利用管理者の存在を示しています		

※利用可能なサービス

アカウントで サービスを管理

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.

アカウントで サービスを管理

- 情報メディア教育研究センターでISMS認証を取得

- 平成26年度末認証取得

- 登録日 (2015年3月27日)

- [ISMS認証取得組織検索 \(JIPDEC\)](#)

- 適用規格

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



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

- 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 • • •

大学ICTの将来像

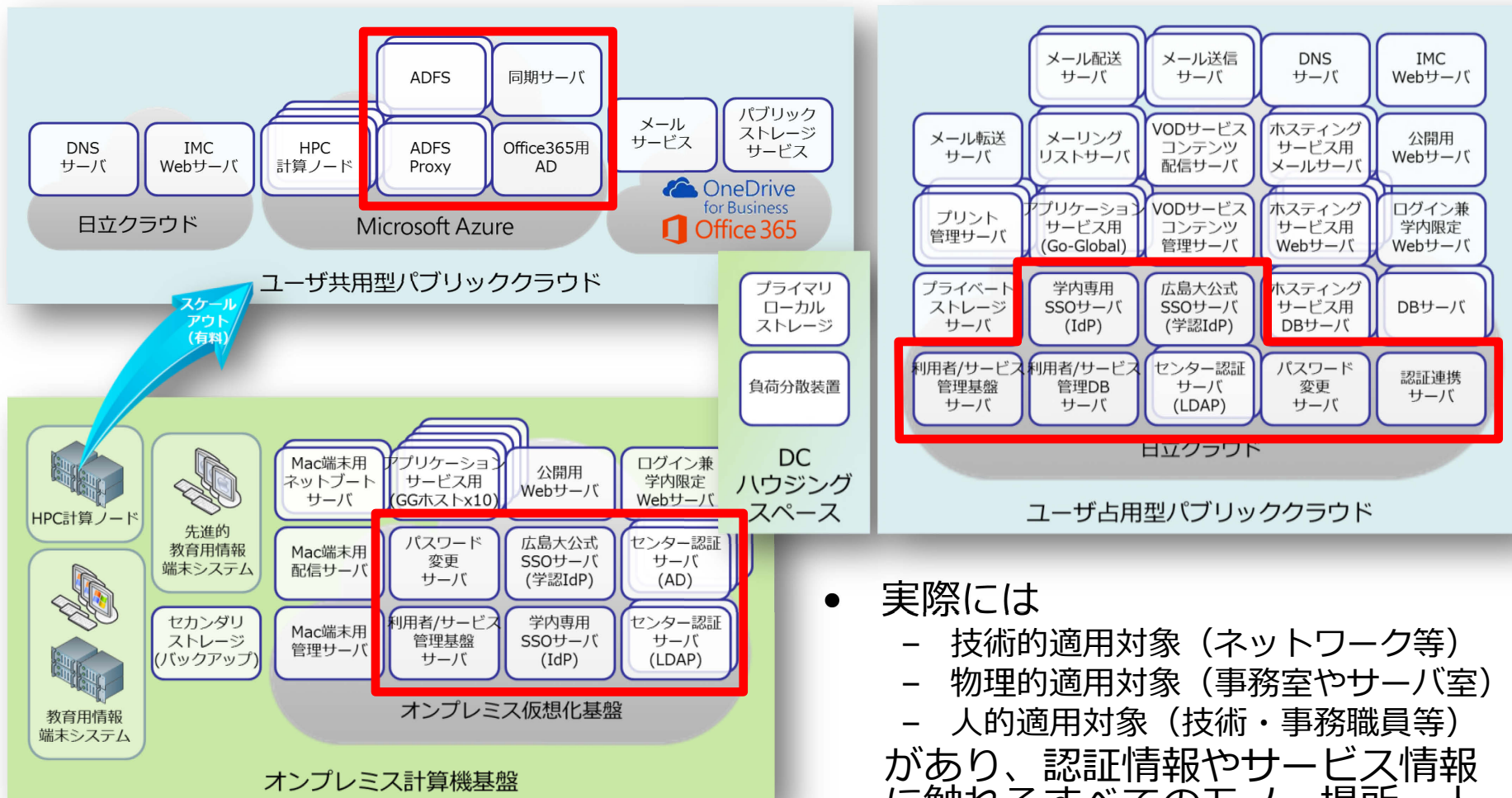
- 大学はサービスポータル機能
(認証情報とサービス利用情報)
のみを構築・管理する

- 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

主な対象(利用者・サービス管理基盤)



- 実際には
 - 技術的適用対象 (ネットワーク等)
 - 物理的適用対象 (事務室やサーバ室)
 - 人的適用対象 (技術・事務職員等)があり、認証情報やサービス情報に触れるすべてのモノ・場所・人が管理対象に含まれる

- クラウド利用を妨げている要因（障壁）は何か？
 - － ユーザは何か満たされれば「クラウドでGo!」なのかを示す必要がある
 - － クラウド利用に際して確認および対応の検討が必要な項目は？
 - クラウドサービス利用ガイドライン
- 「ガバナンスを失わない」ために
 - － ユーザはどこまで事業者任せにすることができ、どこまで自由にできる必要があるかを示す必要がある
 - － クラウド化された大学は何を管理するようになるか？（将来像）
 - 利用登録システム
 - － 大学が運用するシステムのセキュリティ対策は万全か？
 - ISMS（情報セキュリティマネジメントシステム）
- クラウドはユーザの選択肢の幅を広げたが…
 - － （クラウド・SI）事業者は目的や予算に見合う構成やサービスの提案ができる必要がある
 - － 仕様書作成や調達過程における大学と業者の役割は適切か？
 - 仕様書の作成方法や調達手順の変更

仕様書の作成方法や調達手順の変更

- ハードウェア指向からサービス指向へ
 - サービス仕様のみ記述（例）
 - アカウント登録
 - 5,000アカウントが2時間以内に登録可能であること
 - 認証サービス
 - 10秒間に40,000クエリの検索処理ができること
 - クラウドサービス
 - RTTが10ms以内（1ヶ月の平均値）となるようネットワークを構成すること
 - RTTが50ms以内（1ヶ月の平均値）となるようネットワークを構築すること
 - メールサービス
 - 1分間に2,000通以上の送信ができること
 - アプリケーション
 - 100名以上が同時利用できること
- チェックリストの実施と提出を義務付け
- 実装方法は応札業者が提案
 - ヒヤリングや協議を必須化
 - 技術審査への影響を明示
- 全入札予定業者との打合せ
 - 具体的な実装方法を元に意識合わせ
 - **入札予定業者のSI力**
 - 大学側はここで初めて具体的な実装を確認できる
 - クラウド事業者はクラウド部分しか提案しない
 - 実現可能性（技術面）、実行可能性（スケジュール面）をしつかりと確認・意見する
 - **大学の見極め力**
 - 技術審査の期間を短くして対応
- 技術審査
 - 字面による仕様確認からの脱却
 - 旧態依然とした入札や技術審査では、「おうむ返し」や「機能証明」による提案に対応できない

- 広島大学でクラウド導入にあたり検討・実施したこと
 - － クラウドサービス利用ガイドライン
 - クラウド利用に際して確認および対応の検討が必要な項目
 - チェックリストの使用例
 - － 利用登録システム
 - クラウド化の進んだ大学は何を管理するようになるか？
 - 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）のみを構築・管理するようになる
 - － ISMS（情報セキュリティマネジメントシステム）
 - 大学が運用するシステムのセキュリティ対策
 - － 仕様書の作成方法や調達手順の変更
 - 仕様書作成や調達過程における大学と業者の役割
 - － 業者のSI力と大学の見極め力
- 必要と感じたこと
 - － 大学はクラウド利用に関する自身の状況を正確に把握すること
 - － 大学と業者の協力体制（役割分担）がより重要に