資料9

クラウドを実用的に利用するための セキュリティ

- SaaSとPaaSで安全を確保するためのアプローチ-

日本マイクロソフト株式会社
チーフセキュリティアドバイザー
高橋　正和

平成23年度第3回学術情報基盤オープンフォーラム

目次

- クラウド上でのデータ保護
- ユーザー認証とアカウント管理
- 事業継続
- クラウドサービスを利用することで
  セキュリティを強化する
- 大学でのクラウド利用例

  “大学 CIO ハンドブック (クラウド導入・活用編)“から

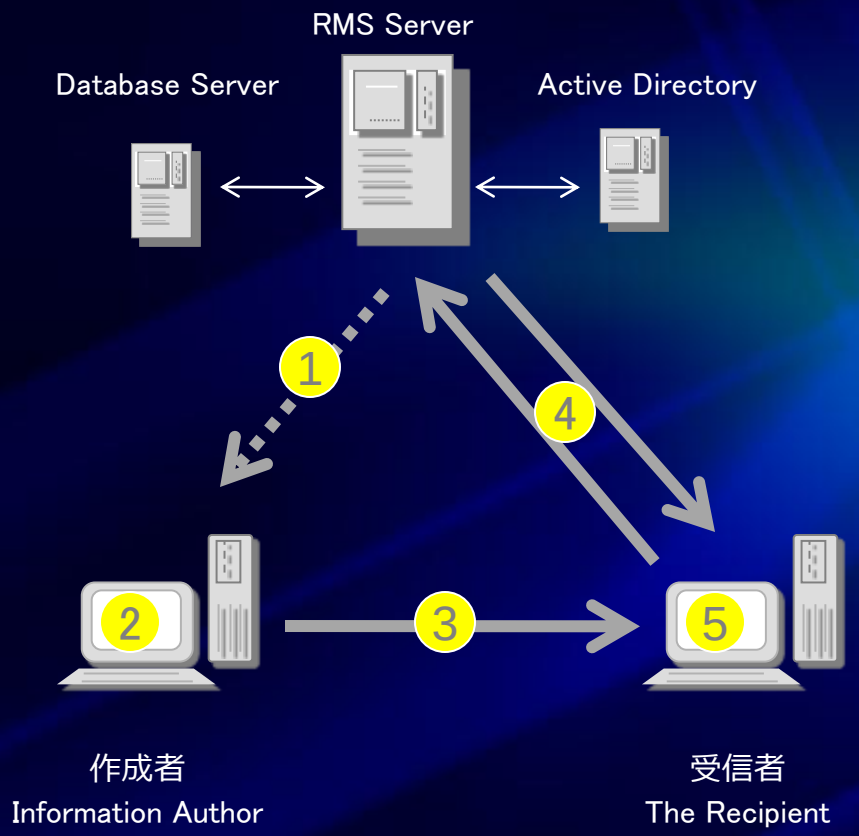
クラウド上のデータ保護

クラウドを前提としたデータ保護

- RMS (Rights Management System)
  主にOffice 365
  - クライアント側でのRMS
    サーバー上のデータで複合は出来ない
    - 各Office レベルでのRMS
    - Outlook を使ったRMS
  - クラウド側でのRMS
    クラウド上は平文で格納され、読み出し時に暗号化される
    - SharePoint Online
- Azure
  - 任意の暗号化が可能（.NET CSP）

http://msdn.microsoft.com/ja-jp/magazine/ee291586.aspx

データレベルの暗号化（RMS）の基本的な動作と利点



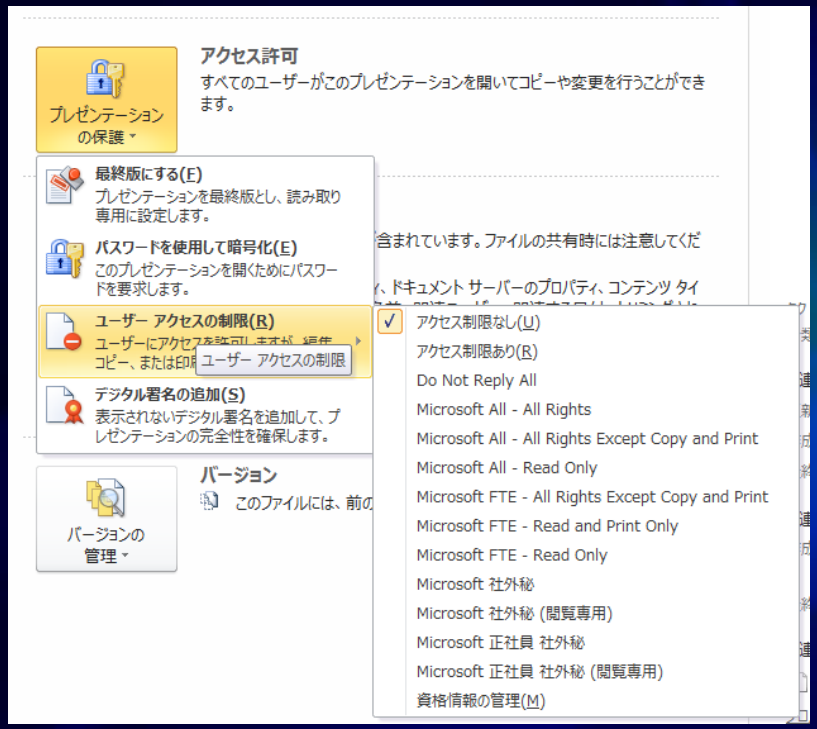
RMSの基本的な動作

① 作成者は、RMSの設定に際して、RMSサーバからクライアントライセンス証明書を受け取る。
② 作成者は、一連の権利とルールを定義する。アプリケーションは、RMSクライアントソフトを使って“発行ライセンス”を作成し、ファイルを暗号化する
③ 作成者は、必要に応じて任意の方法でファイルを配信する。
④ 受信者が、ファイルを開くと、RMSサーバを呼び出す。RMSサーバはユーザーの検証を行い、使用ライセンスを発行する。
⑤ アプリケーションは、ファイルを複合化し、使用ライセンスにおいて定義された権利を適用する。

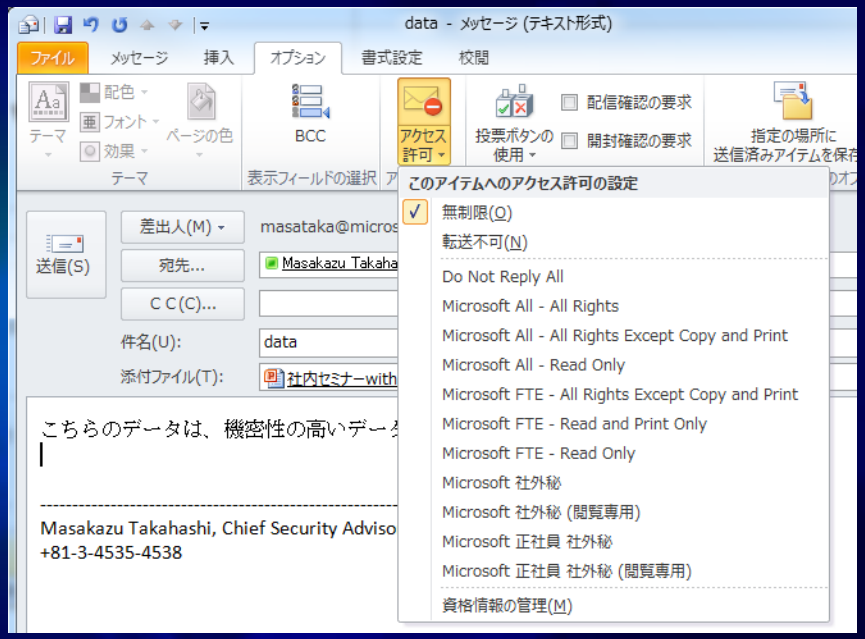
RMSの利点

•ファイルが移動しても、暗号や付与した権利が維持される。
•万一、社外にファイルが流出しても、情報が漏れる可能性は極めて少ない。
•ファイルを開く際に、必ずRMSサーバにアクセスが行われるので、ファイルアクセスの追跡ができる。
• 特定のドキュメントへのアクセスを、後から禁止することもできる。

RMSによるデータ保護

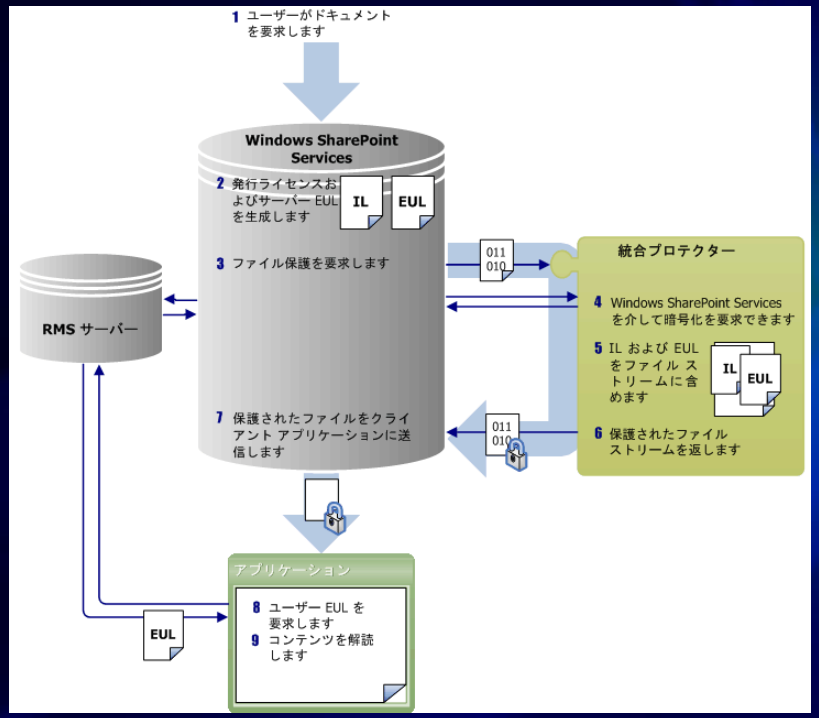


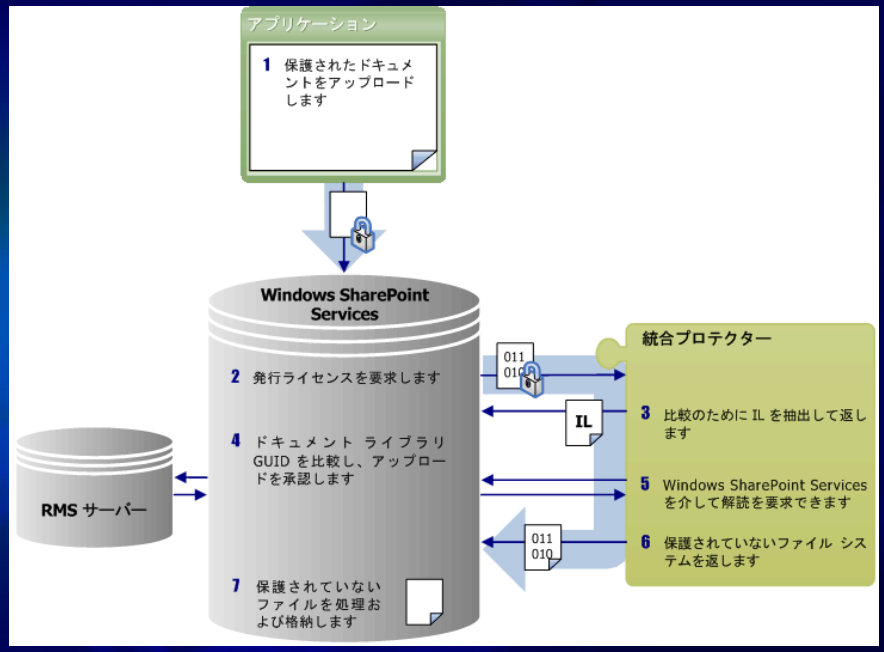
Officeドキュメントの保護（PowerPointの例）



Officeドキュメントの保護（Outlookの例）

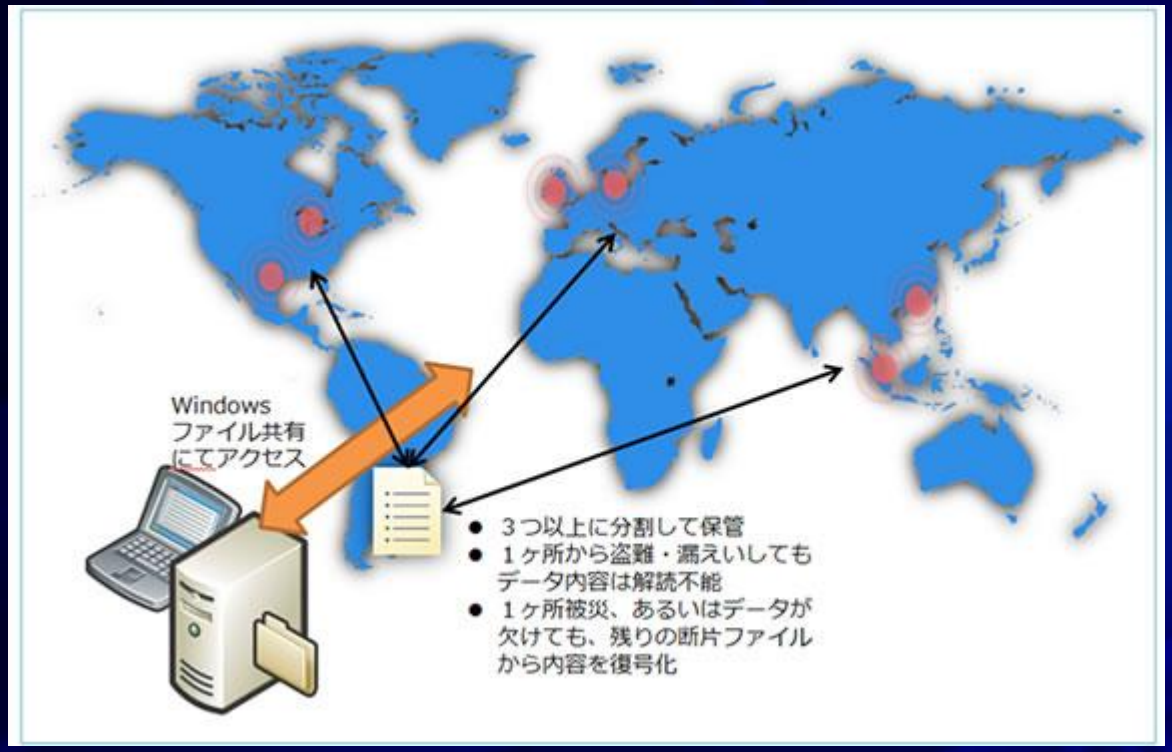
SharePointを使ったRMSの自動化





SharePoint Foundation での IRM フレームワーク アーキテクチャ
http://msdn.microsoft.com/ja-jp/library/ms439625.aspx

NRI 分散ストレージサービス



- 複数のデーターセンターに、ビットレベルで分散
- ひとつのデータセンターがダウンしても、そのまま運用が可能
- ひとつのデータセンターを、差し押さえられても、情報の複合ができない

NRI: 世界分散ストレージサービス
http://www.nri-secure.co.jp/service/global/gss.html

ユーザー認証とアカウント管理

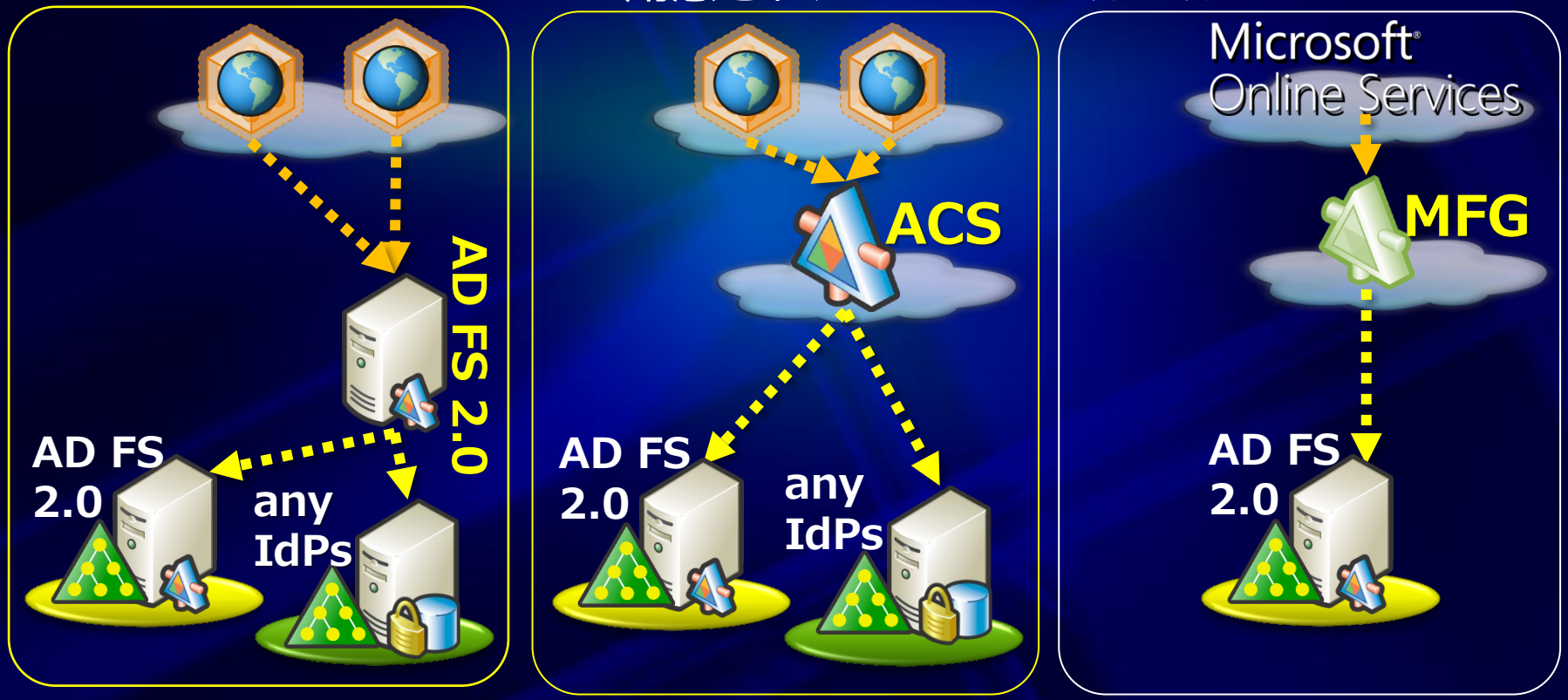
クラウドのシングルサインオンの方式

- STS(Security Token Service) により「使用目的」と「出来ること」が異なる

【 AD FS 2.0 】
高機能な STS
オンプレミスに配備

【 ACS 】
クラウド上に
用意された STS

【 MFG 】
Microsoft Online Services
用に用意された STS

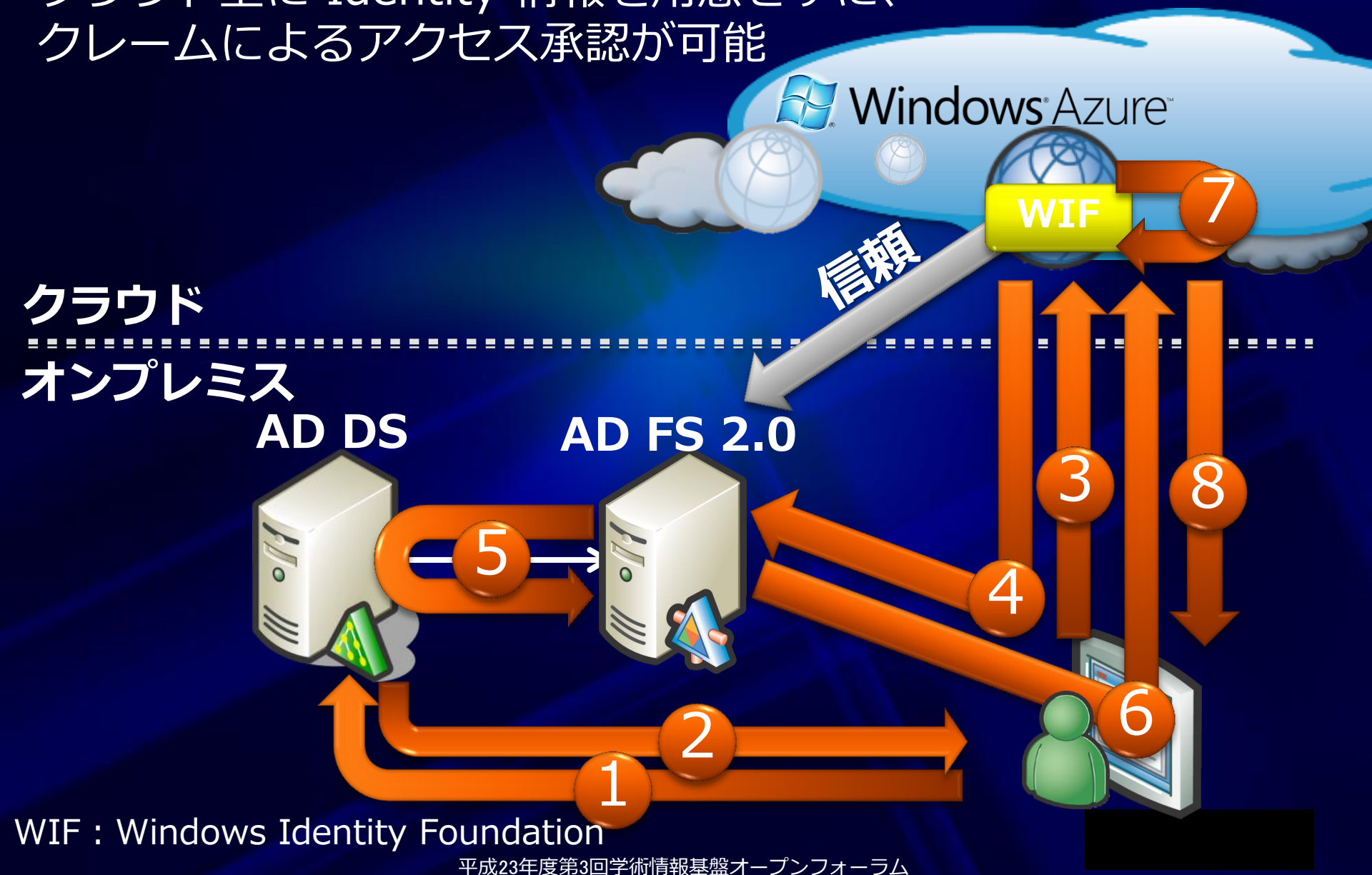


MFG：Microsoft Federation Gateway
ACS：Windows Azure platform AppFabric Access Control Service

信頼

ADFSを使ったアカウント管理の連携

クラウド上に Identity 情報を用意せずに、
クレームによるアクセス承認が可能



WIF : Windows Identity Foundation

Office 365
Active Directory Federationの利用

Office 365では、ADFSとのシングルサイオンが利用可能

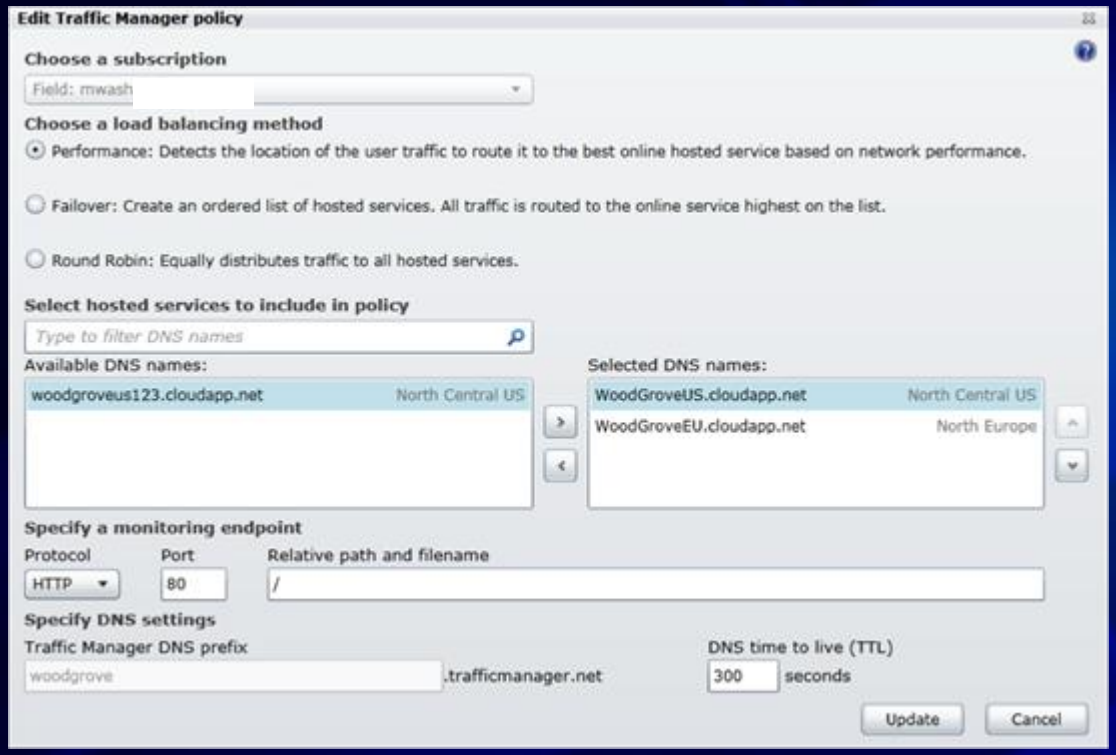
シングル サインオンを利用するには、次の操作が必要

- **Active Directory を Windows Server 2003 オペレーティング システム、Windows Server 2008、または Windows Server 2008 R2 に展開し、混合モードまたはネイティブ モードの機能レベルで実行する。**
- **AD FS 2.0 を Windows Server 2008 または Windows Server 2008 R2 に展開する計画を立て、実行する。ユーザーが会社のネットワークの外部から接続している場合は、AD FS 2.0 プロキシも展開する必要があります。**
- **Windows PowerShell 用 Microsoft Online Services モジュールを使用して、Office 365 と信頼関係を確立する。**
- **Office 365 の必須の更新プログラムを Office 365 ダウンロード ページからインストールし、ユーザーが Windows 7、Windows Vista、Windows XP のいずれかの最新の更新プログラムを実行していることを確認する。Office 365 ダウンロード ページにアクセスするには、Office 365 ポータルにサインインし、[リソース] の下の [ダウンロード] をクリックします。Office 365 の機能は、オペレーティング システム、ブラウザー、およびソフトウェアが適切なバージョンでないと、正常に動作しません。詳細については、「Office 365 のソフトウェア要件」、「Office 365 用にデスクトップをセットアップする」、および「Office 365 用にデスクトップを手動で更新して構成する」を参照してください。**

Office 365 シングルサインオンを準備する
http://onlinehelp.microsoft.com/ja-jp/office365-enterprises/ff652540.aspx

事業継続

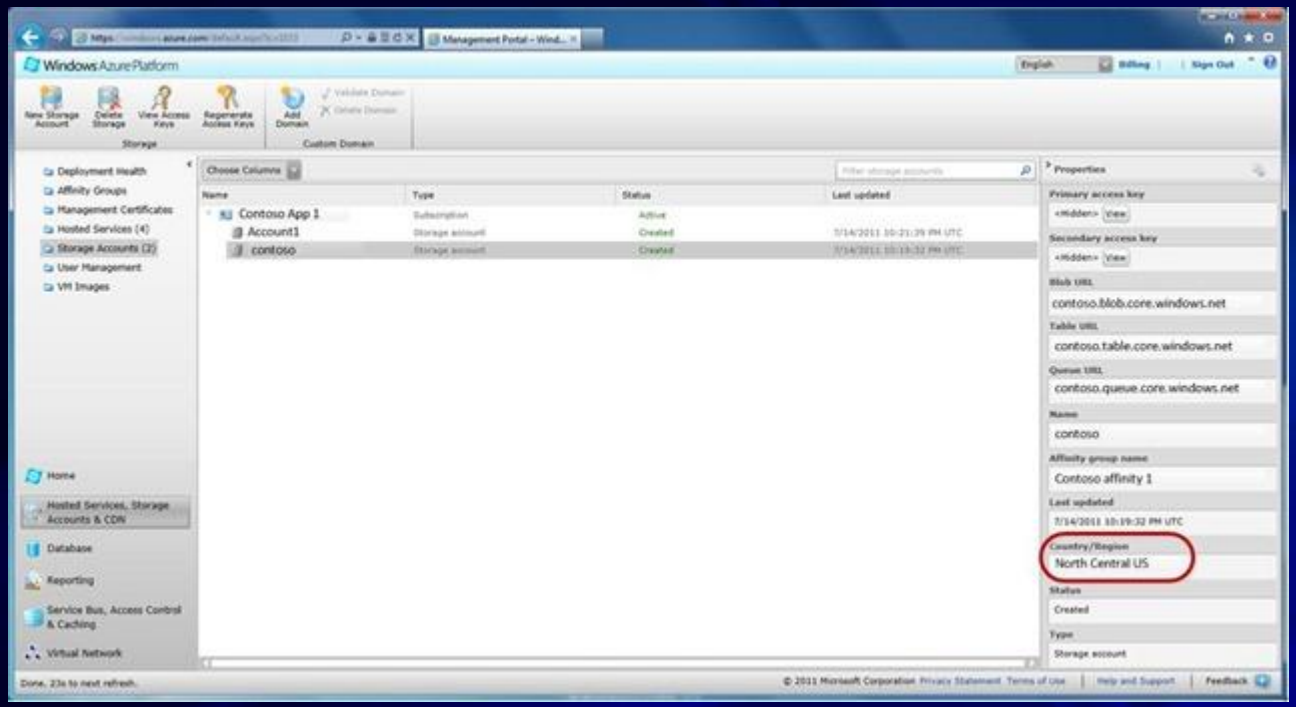
Traffic Manager



提供するロードバランシング

- **Performance:**
  - ネットワークパフォーマンスに基づいた、ロードバランシング
- **Failover:**
  - 設定した順位に基づいたFailover
- **Round Robin:**
  - ラウンドロビン方式のロードバランシング

Geo-Replication



Primary	Secondary
North Central US	South Central US
South Central US	North Central US
North Europe	West Europe
West Europe	North Europe
South East Asia	East Asia
East Asia	South East Asia

- 自動的に、Secondaryのデーターセンターにreplicationを行う
  - Secondaryのロケーションは自動的に設定される
- Primaryのデータセンターに回復ができない障害が発生した場合、利用者に通知の上、Secondaryに切り替える

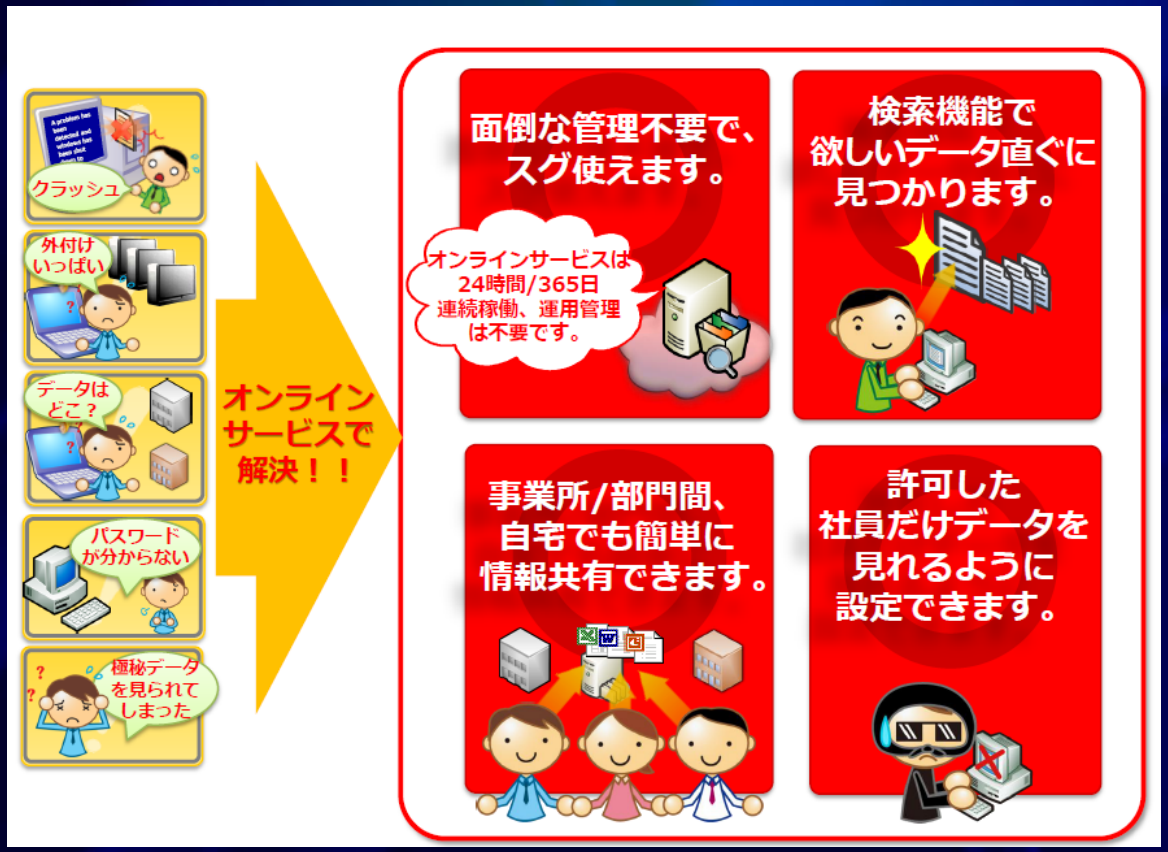
クラウドサービスを利用することでセキュリティを強化する

ドキュメントの履歴管理とアクセス制御

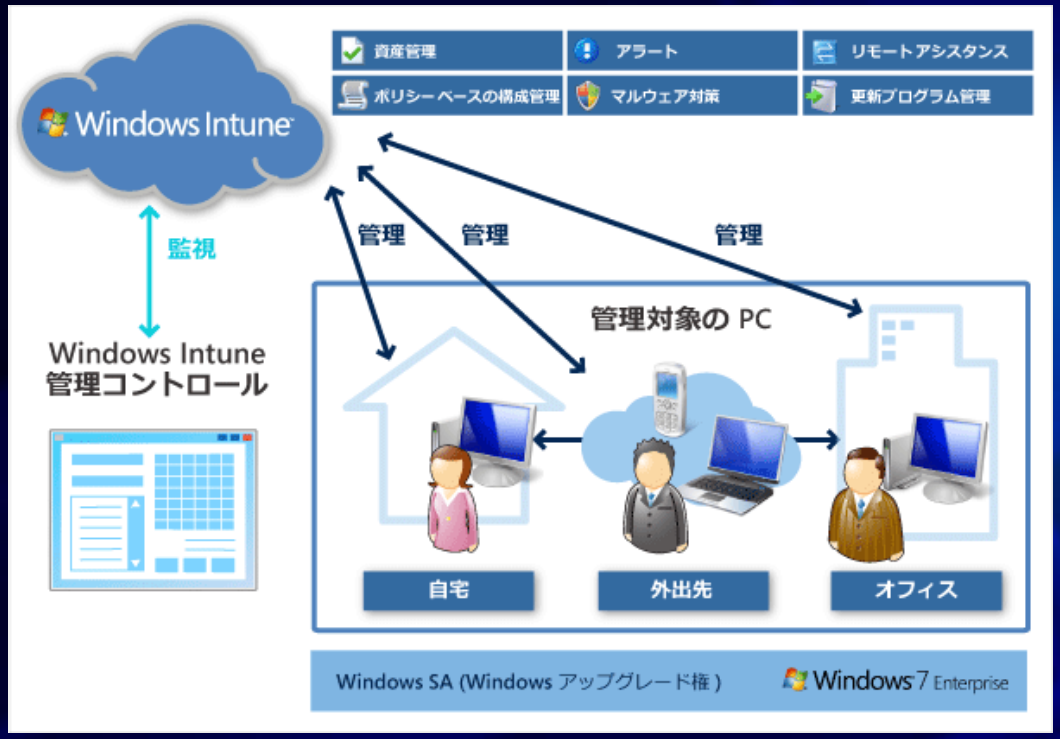
- JSOX対応にみるドキュメント管理の問題
  - JSOXは会計業務の適切さを保証するもの
  - ITシステム全般の話はもちろんだが、経理などの EXCEL のデータシートの管理が問題となるケースが多い
    - EXCELデータのバージョン管理ができない
    - 承認プロセスに乗りにくい
      - Check In / Check Outができない
    - アクセスコントロールができない
      - パスワードの保護はあるのだけれど
    - 担当者のPCにEXCELデータが管理されている

SharePoint Online

- ファイルサーバーではなく、SharePoint Onlineを利用する
  - ファイル管理の一元化
  - 履歴の管理
  - Check in / Check out
  - アクセス管理
  - RMSによるデータ保護



セキュリティ用途のクラウド Windows Intune



通達型のセキュリティ運用は限界

- PCのセキュリティをクラウドを使って管理
  - マルウエア対策
  - 更新プログラム
  - 構成管理
  - 試算管理
  - アラート
  - リモートアシスタント
- 幅広い管理の対象
  - オフィス内
  - 自宅
  - 外出先

大学でのクラウド利用例

－ 大学 CIO ハンドブック (クラウド導入・活用編) －

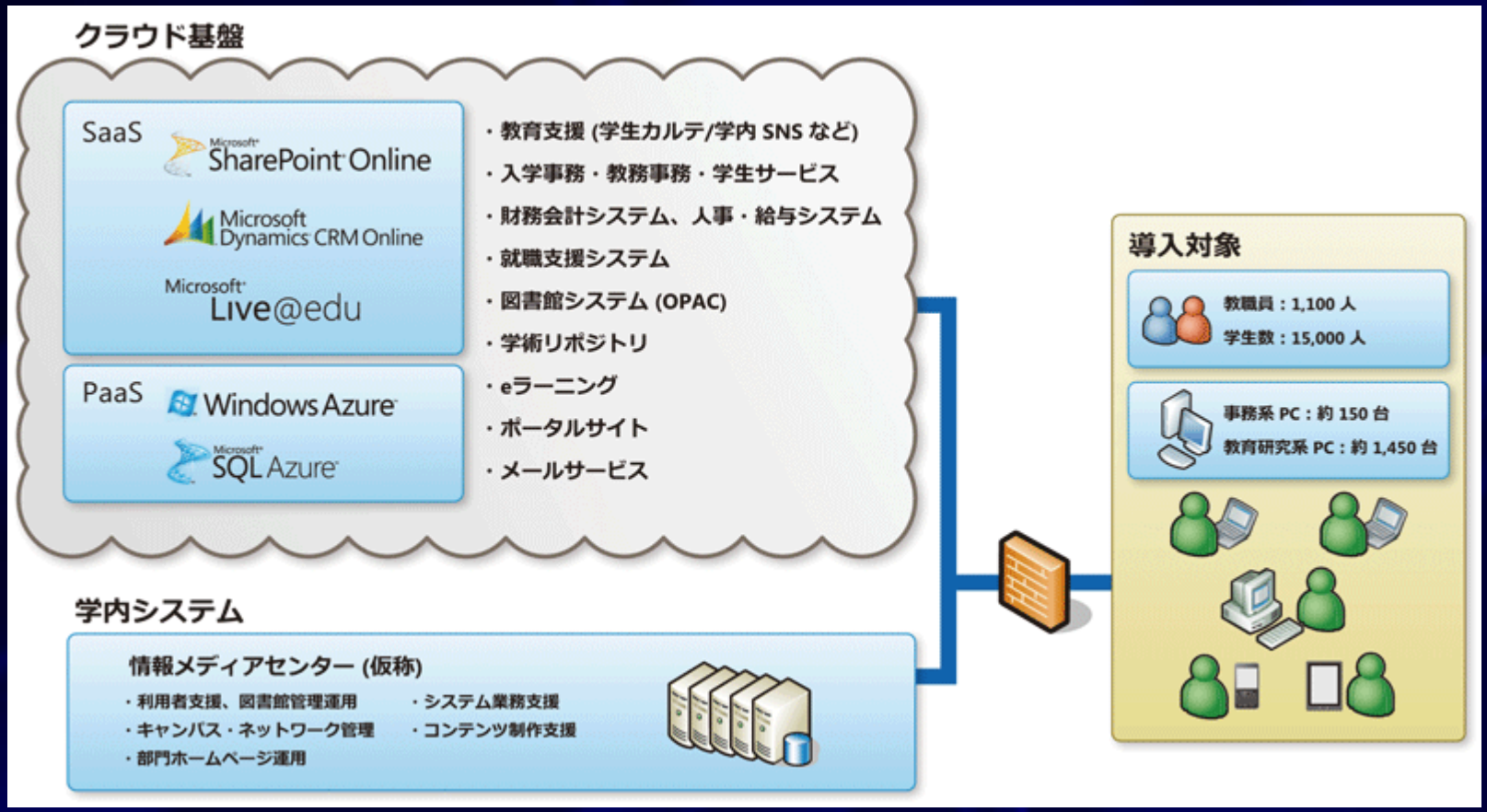
大学のクラウド導入事例

図表3-1　大学のクラウド導入事例

領域	大学	導入時期	概要
フルクラウド化	国士舘大学	2011年５月（一部稼働）	全学システムのフルクラウド化を実施。プラットフォームはWindows Azureに統一。
	徳島大学	2012年４月（予定）	サーバーの用途で、パブリッククラウド、プライベートクラウドを使い分け。クライアントはシンクライアント化。
サーバー統合	静岡大学	2010年３月	Webサーバーなどをプライベートクラウド化。研究用にはパブリックを活用。業務システムはハウジングを利用。
	鹿児島大学	2009年３月	学内向けに実施しているホスティング・ハウジングサービスを、仮想化技術で提供。
	東京大学	2009年９月	事務計算機システム導入に当たり、比較的負荷の少ないシステムに仮想化技術を適用。
	東京工業大学	2010年11月	スパコン（TSUBAME）をクラウドとして、学内教育から先端研究まで幅広く利用。
	大阪大学	2010年	プライベートクラウドを構築。
	北海道大学	2011年10月（予定）	学術・研究者向けキャンパスクラウドを提供予定。全体は「北海道大学アカデミッククラウド」と呼称。
メールクラウド化	福岡大学	2010年６月	学生、教員約３万名向けにMicrosoft Live@eduの電子メール機能を導入。
	明治学院大学	2010年４月	学生、教員約２万名向けにMicrosoft Live@eduの電子メール機能を導入。
	東京大学	2009年11月	教職員にYahoo!メールを提供。
	岡山大学	2009年４月	Google Appsにより全学メールサービスを提供。卒業後も利用可能（生涯メールサービス）。
	早稲田大学	2008年２月	学生、教職員、卒業生にYahoo!メールを提供。
デスクトップサービス	明治大学	2010年７月	キャンパスクラウドシステムを理工学部に試行導入。教員や学生は自宅など学外からも学内と同じ環境でPCを利用可。
	北陸先端科学技術大学院大学	2010年３月	学内の全ユーザーが研究、教育、事務作業に利用するデスクトップサービスを仮想化技術で提供。
Eラーニング	慶應義塾大学	2009年４～９月	OCWをフォーマルラーニングに活用するeラーニングシステムを開発、実証。
図書検索	帝京大学	2010年11月	図書横断検索システムをSaaS型で提供。学内図書館および公共図書館、他大学の図書館を横断的に検索。

大学 CIO ハンドブック（クラウド導入・活用編）
https://www.microsoft.com/japan/msbc/redirect.aspx?ru=http://download.microsoft.com/download/0/D/2/0D2693DC-7B61-4F3D-A6DE-457D769F52A7/cio_handbook_cloud.pdf

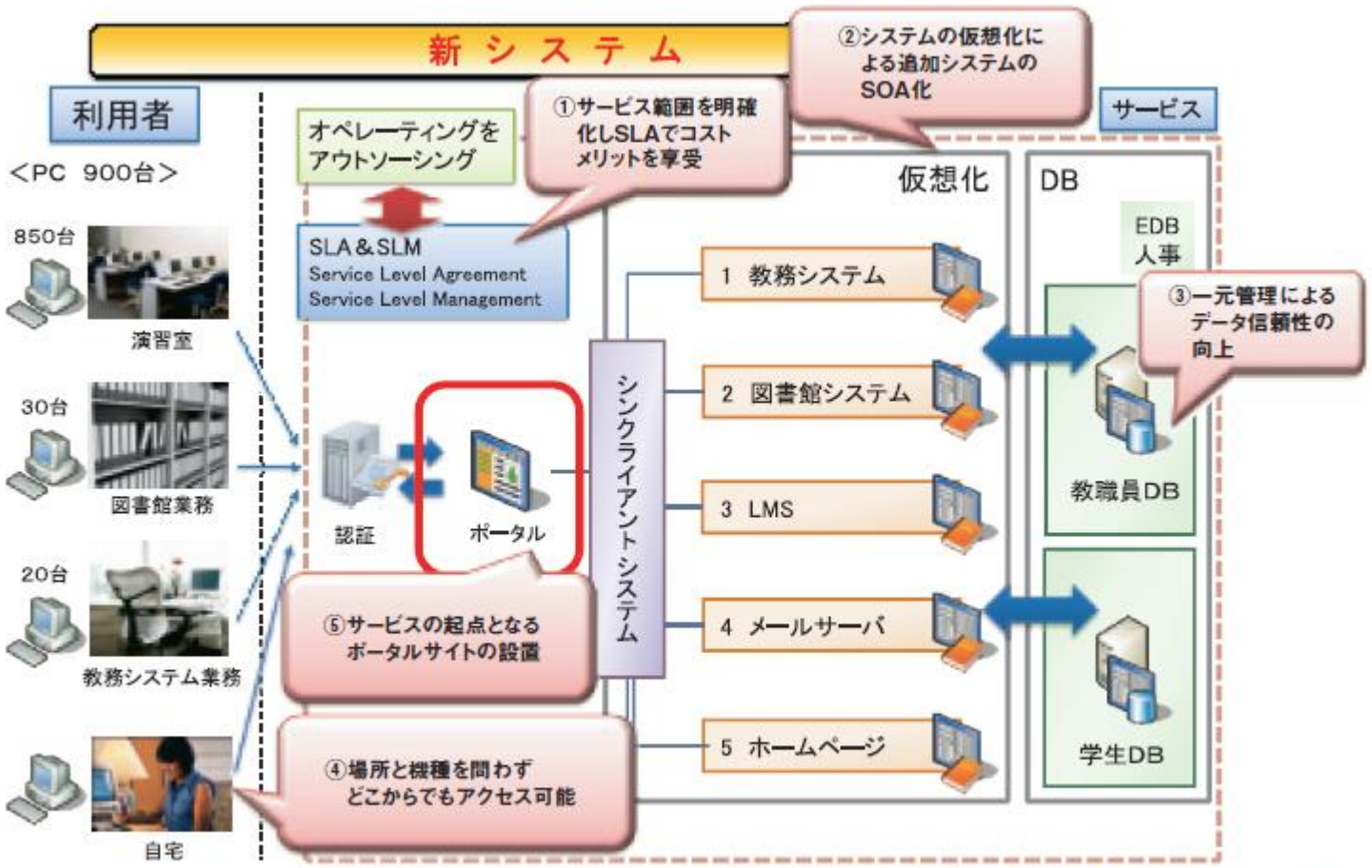
国士舘大学



http://www.microsoft.com/ja-jp/casestudies/kokushikan-uni.aspx

徳島大学

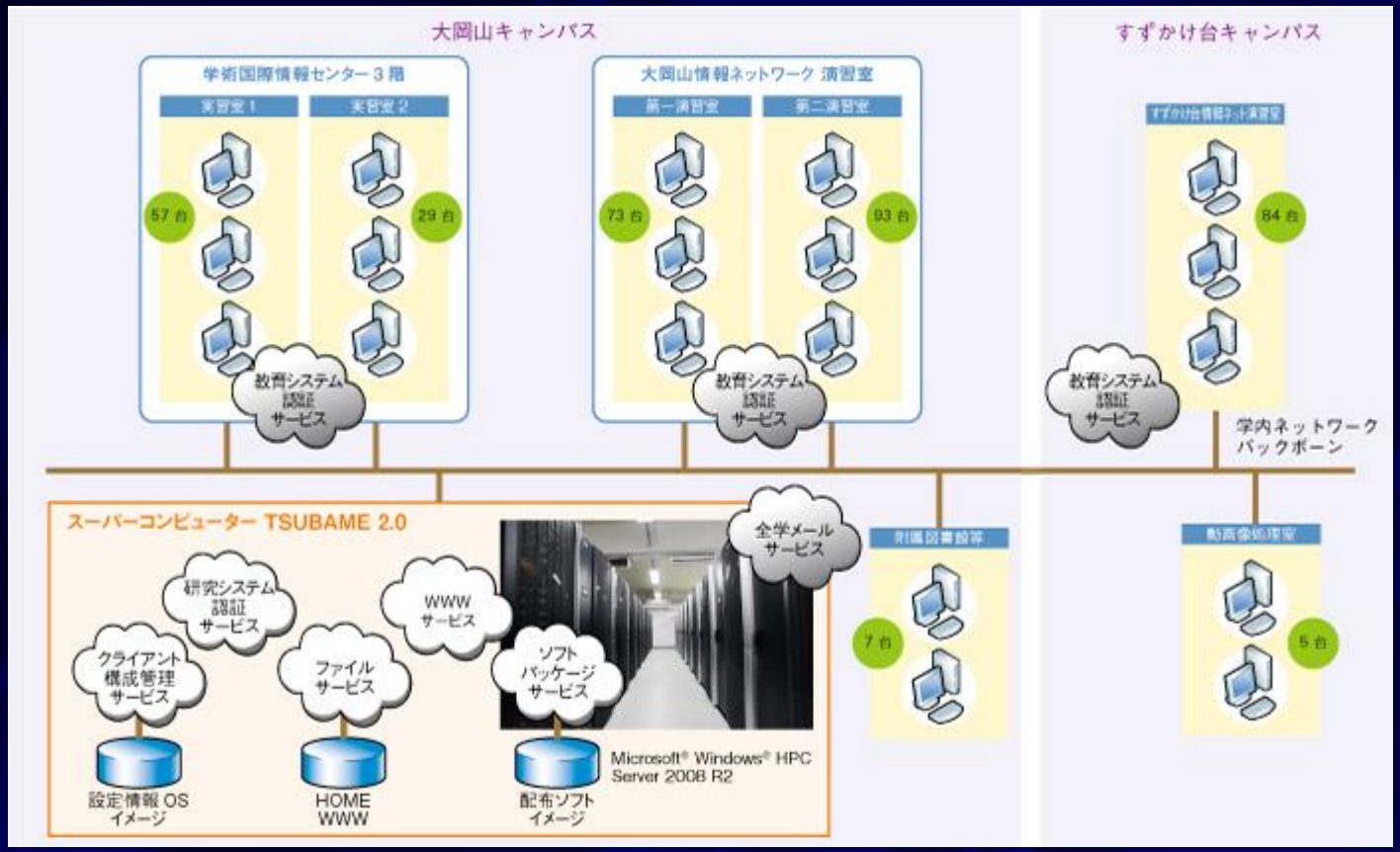
図表3-3　徳島大学　新システムのシステム構成



出所：第9回大学CIOフォーラム資料、徳島大学情報化推進センター
センター長　矢野米雄「大学におけるクラウド活用の事例について」(2011年5月27日)

大学 CIO ハンドブック (クラウド導入・活用編)
https://www.microsoft.com/japan/msbc/redirect.aspx?ru=http://download.microsoft.com/download/0/D/2/0D2693DC-7B61-4F3D-A6DE-457D769F52A7/cio_handbook_cloud.pdf

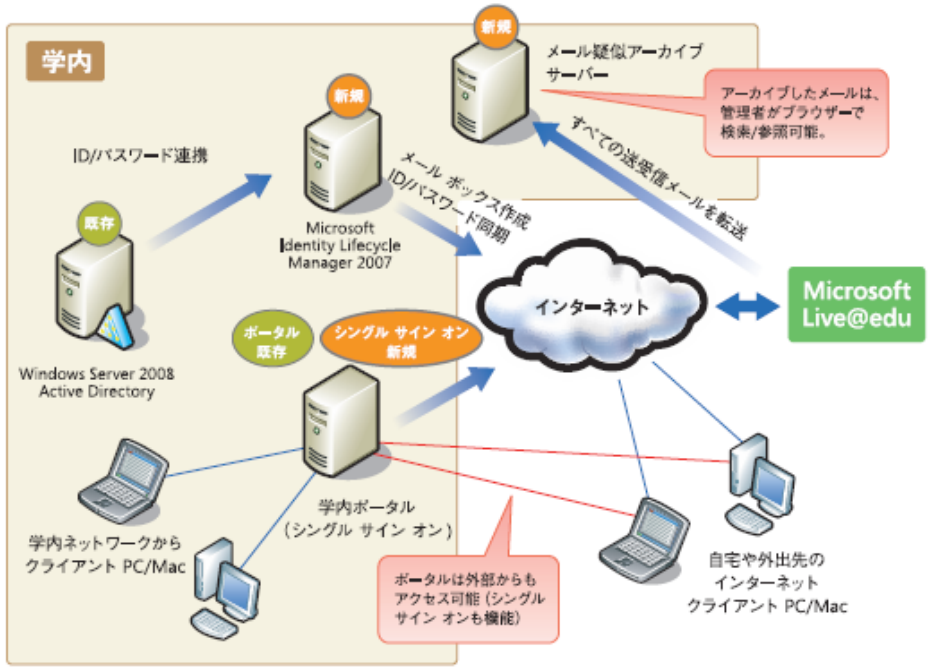
東京工業大学

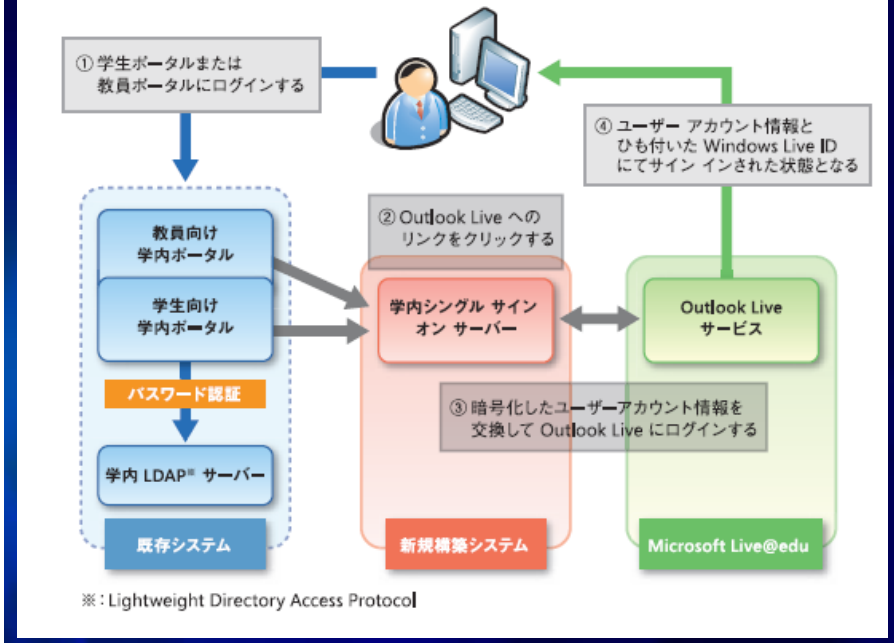


http://www.microsoft.com/ja-jp/casestudies/titech2.aspx

明治学院大学

図表3-8　明治学院大学　メールシステム構成





大学 CIO ハンドブック（クラウド導入・活用編）
https://www.microsoft.com/japan/msbc/redirect.aspx?ru=http://download.microsoft.com/download/0/D/2/0D2693DC-7B61-4F3D-A6DE-457D769F52A7/cio_handbook_cloud.pdf

Microsoft®