FUSION Cloudにおける認証認可アーキテクチャについて

April/12/2013

Fusion Communications Corp.
http://www.fusioncom.co.jp/

Contents

フュージョン・コミュニケーションズでは、IaaS型パブリック・クラウドサービスである FUSION Cloud を商用サービスとして提供しています。

FUSION Cloudでは、サービス管理機能を提供するための共通基盤として、OpenAMを使った認証認可機能とMule ESBを使ったシステム間連携機能を実現しています。

当講演では、その認証認可のアーキテクチャとOpenAMの役割を中心にご紹介します。

具体的には下記の内容についてご説明いたします。

1. フュージョン・コミュニケーションズの紹介
2. FUSION Cloudの設計思想とOpenAMの役割
3. FUSION Cloudの本格商用サービス化にあたってのOpenAM採用の経緯
4. FUSION Cloudと外部システムとの連携の実現とメリット
5. SaaSの具体例
6. まとめ

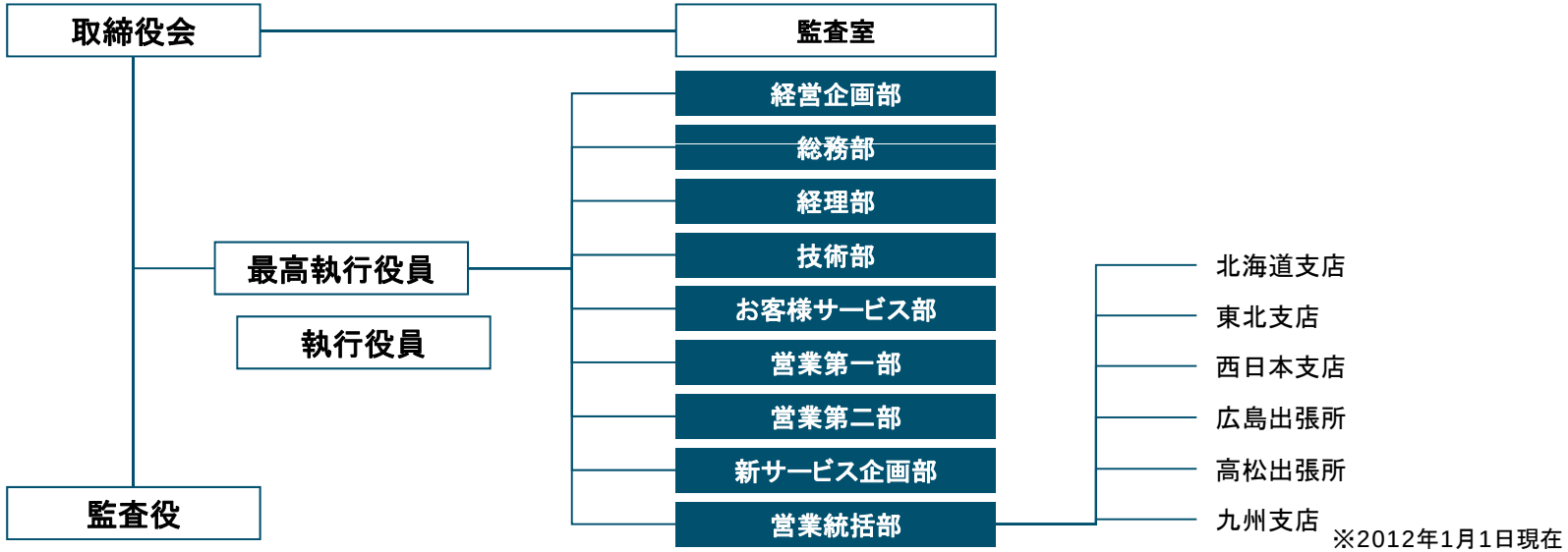
1. フュージョン・コミュニケーションズの紹介

フュージョン会社概要

企業情報

会社名	フュージョン・コミュニケーションズ株式会社
設立	2000年3月13日
代表者	代表取締役会長　三木谷　浩史　／　代表取締役社長　相木　孝仁
事業内容	電気通信事業
資本金	20億円
主な株主	楽天株式会社　54.78% 丸紅株式会社　38.00%

組織図



※2012年1月1日現在

フュージョン会社沿革-1

-Everything Over IP- の実現に向けて

2000年　創業

IP電話のパイオニアとして、斬新で高品質なサービスを展開

・2001年　国内初の24時間・全国一律料金の画期的な市外電話サービス開始
・2003年　050番号を使った『FUSION IP-Phone/IP-Centrex』開始
・2004年　携帯電話使い分けサービス『モバイルチョイス』開始
・2005年　Skype社とIP電話サービスで協業開始

2007年　楽天グループの一員へ

コミュニケーションとインターネットの融合を加速

・2008年　コンシューマー向け『楽天ブロードバンド』開始
・2009年　『楽天モバイルfor Business』開始
・2010年　FUSION IP-Phone、Asterisk接続に正式対応
・2011年　コールセンター向けCloudテレフォニー『FUSION Connect』開始

2011年　丸紅による経営参画

次世代ICTサービスのさらなる拡充へ

FUSION COMMUNICATIONS　楽R天

フュージョン会社沿革-2

VoIP技術を駆使した最先端のサービスを提供

国内電話サービス

市外電話3分20円

フュージョン・コミュニケーションズ

今春から IP活用し全国一律

距離・時間帯関係なく…

一律3分20円

フュージョンの市外電話

IP活用、攻めの低価格

日経産業新聞
（2001年1月16日）

日経産業新聞
（2001年1月16日）

IP-Phone/Skype

IP電話 企業へ拡大

パソコンとの融合

IP電話元年

技術競争 低価格化促す

日経産業新聞
（2003年1月15日）

日経産業新聞
（2003年2月21日）

IP電話「スカイプ」

一般電話に番号通知

フュージョン 使い勝手高める

日経流通新聞
（2007年1月1日）

モバイル

楽天、PHS事業参入

ウィルコムの回線を利用 ネット通販と連携

日経新聞
（2009年1月20日）

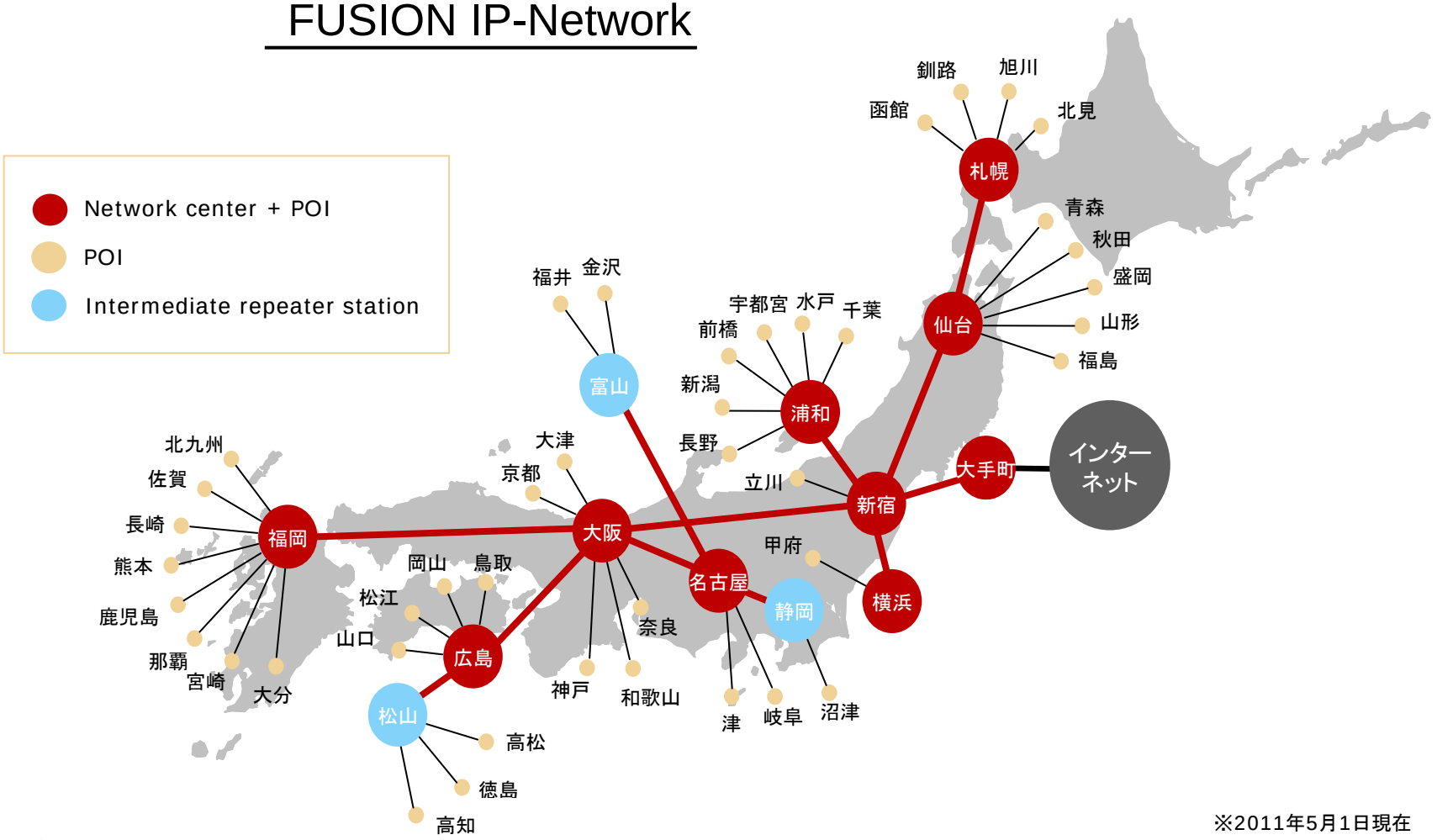
FUSION COMMUNICATIONS

楽天

フュージョン会社沿革-3

高品質な全国IP-Networkを保有

FUSION IP-Network



※2011年5月1日現在

フュージョンのサービス

固定電話サービス

■国内・国際電話サービス
- 圧倒的な安さの固定電話サービス

■FUSION IP-Phone
- 高機能・低価格050-IP電話

■フリーボイス
- 業界最安水準の0120/0800サービス

インターネット接続サービス

■FUSION GOL
- 企業向けメールサービス

■楽天ブロードバンド
- コンシューマー向けサービス

モバイルサービス

■楽天モバイル for Business
- 携帯するIP電話

■モバイルチョイス
- 携帯通話料の使い分けサービス

■ FUSION IP-Phone SMART
- スマホの通話料を安くする

次世代ICTソリューション

■Asteriskソリューション
- 次世代IP-Phoneソリューション

■FUSION Connect
- コールセンター向けCloudテレフォニー

■Call Insight(コール・インサイト)
- 電話による成果型報酬広告・効果測定ツール

クラウドサービス

■FUSION Cloud (IaaS)
- 楽天グループのパブリッククラウド
- 2012年4月27日商用開始

■FUSION iPaaS(PaaS)
- 楽天市場RMS APIに対応
- 2012年10月9日商用開始

■FUSION Secure Drive App (SaaS)
- スマートデバイスでセキュアにファイル
- 2013年2月1日商用開始

■FUSION Secure Drive (SaaS)
- 社内外とのファイル共有
- 2013年2月18日商用開始

FUSION CloudはIaaSに加えPaaS/SaaSに展開中

NIST(*) defines following 3 types of Cloud Service Model
(*) NIST: National Institute of Standards & Technology, U.S. Department of Commerce

Model 1: IaaS
Infra as a Service.
Infra: OS, server, etc.

Model 2: PaaS
Platform as a Service.
Platform: development for APP engineers, just focus on coding without thinking about server.

Model 3: SaaS
Software as a Service.
Software: application

FUSION CLOUD 2012/4/27

FUSION iPaaS 2012/10/9

FUSION SecureDrive App 2013/2/1

FUSION SecureDrive 2013/2/18

順次機能追加を計画

順次追加を計画

順次追加を計画

商用サービス開始

FUSION COMMUNICATIONS 楽天

FUSION Cloud(IaaS)とは

■ 楽天グループのパブリッククラウド

2012年4月27日商用サービス開始

■ 特長

I. フュージョンが開発した基盤を使ったパブリック型クラウド(IaaS)

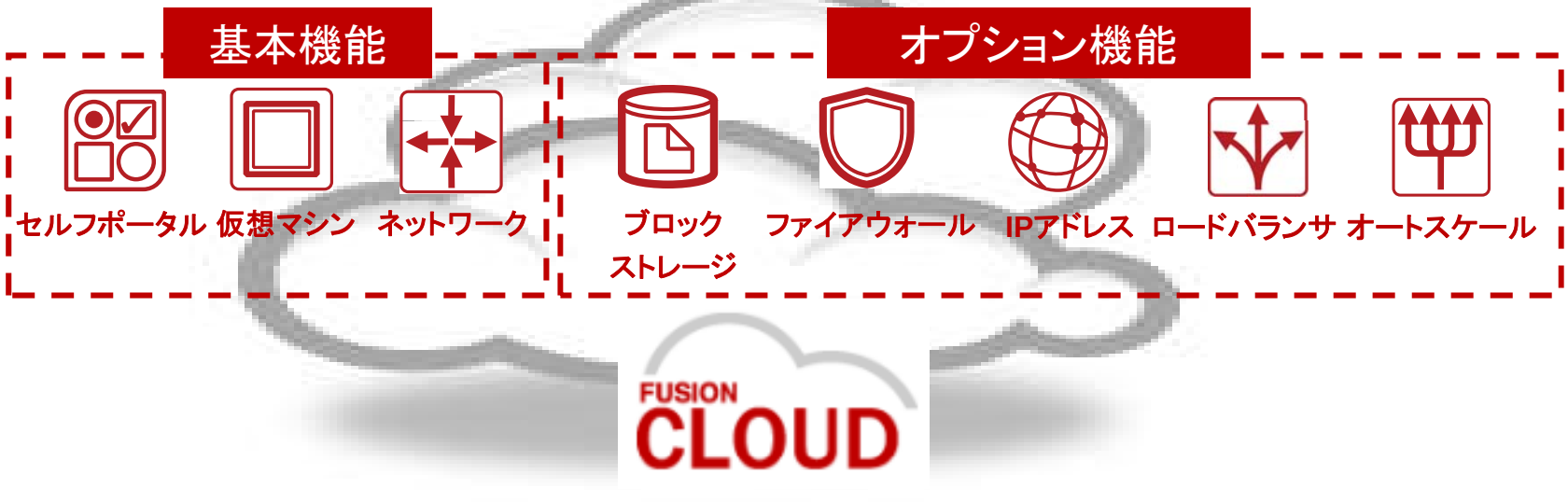
II. 高性能・高品質システム構成(H/WベースのFW/LBを採用、全冗長化)

III. セルフポータルによる簡単操作

IV. 定額制(月額課金)、従量制(時間課金)

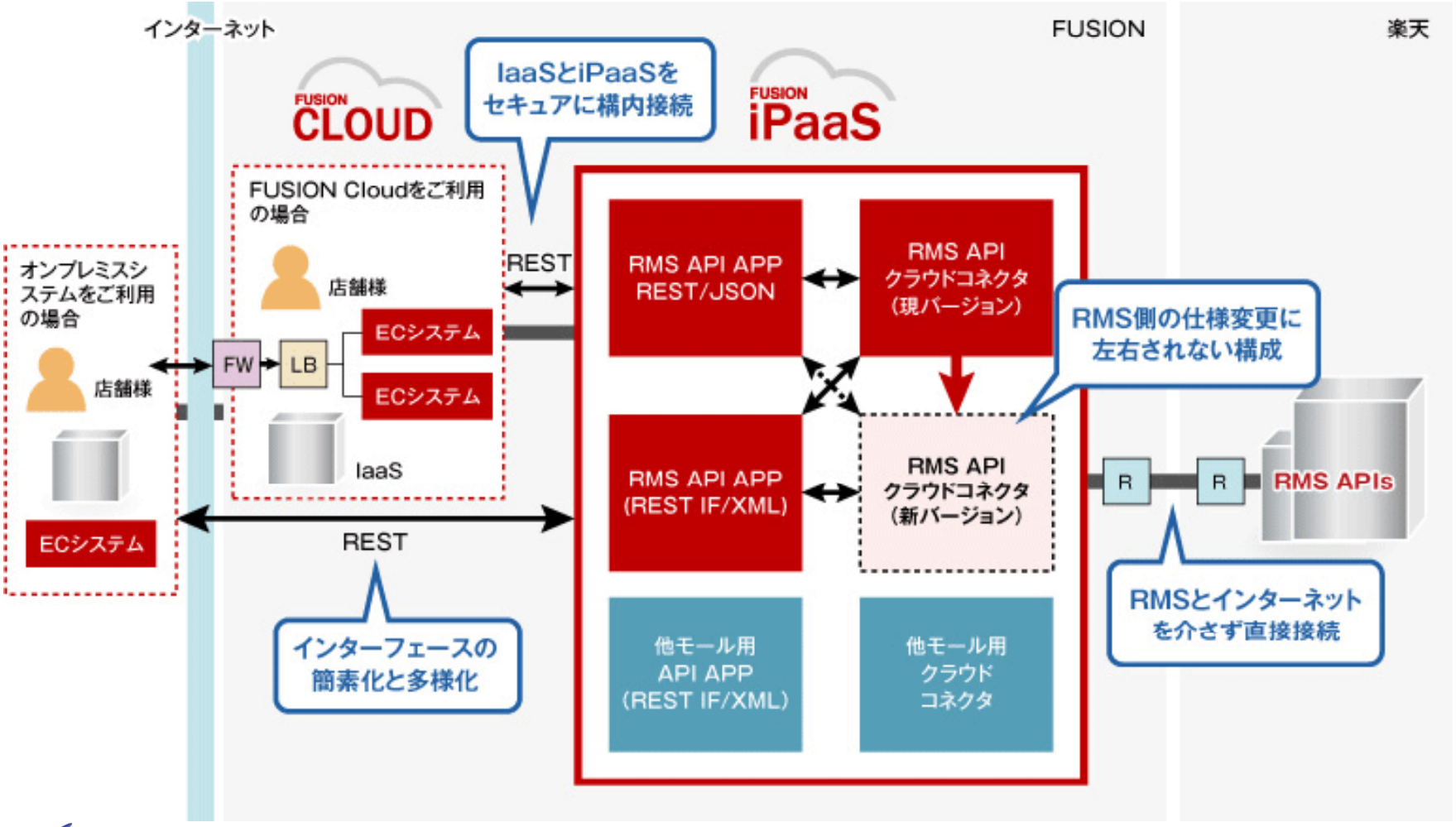
V. 24/365の監視保守運用

※アンダーラインの部分は認証認可に関係した機能。



FUSION iPaaSとは

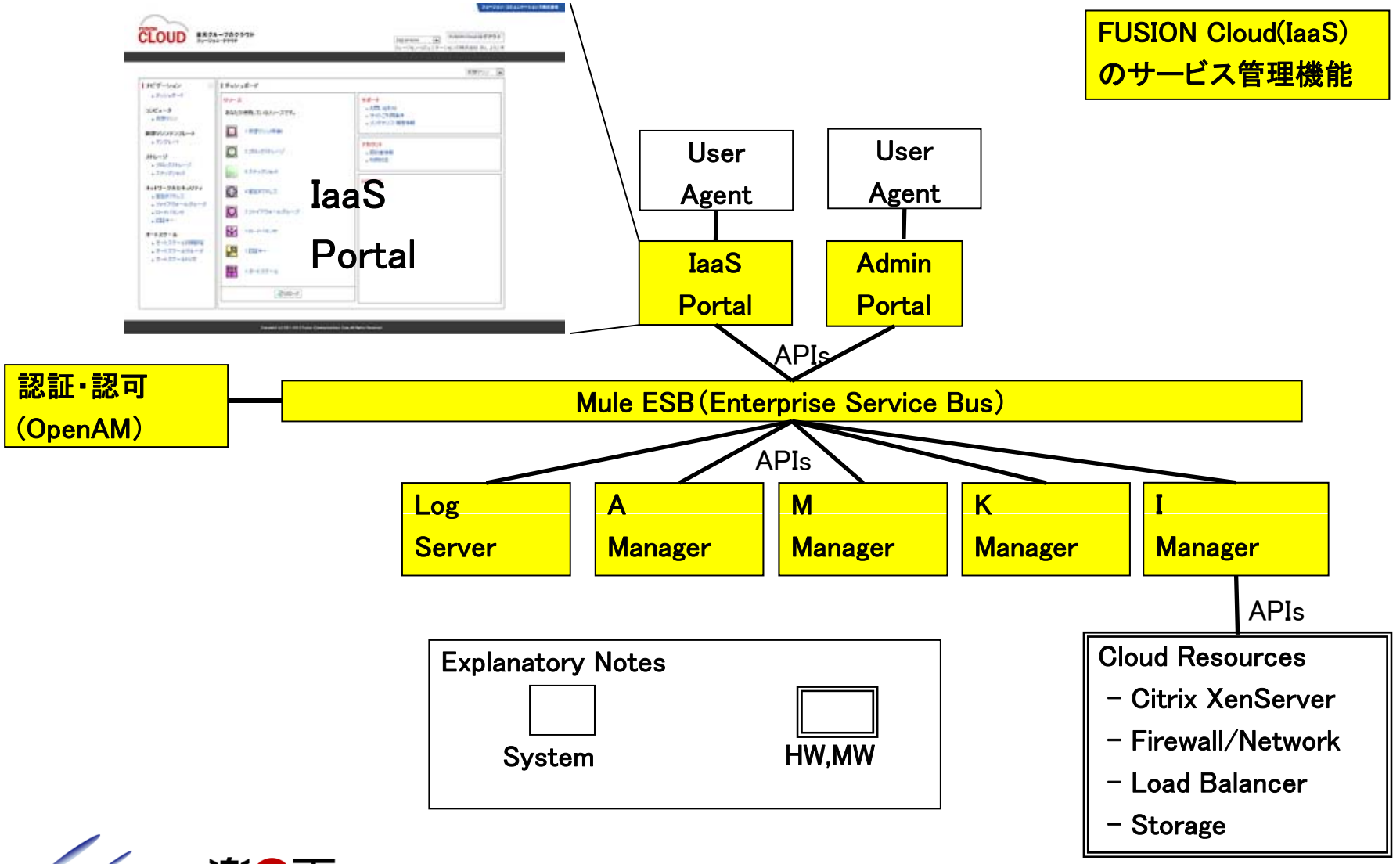
FUSION iPaaSは、最初のステップとして、楽天市場の出店店舗向けAPIであるRMS APIに対して、REST APIでの接続を可能とすることにより、出店店舗のAPI開発コストを削減するクラウドサービス。



2. FUSION Cloud（IaaS）の設計思想とOpenAMの役割

FUSION Cloud(IaaS)はフュージョン独自

FUSION Cloud(IaaS)のサービス管理機能（黄色部分）をフュージョンにて独自開発してきた。



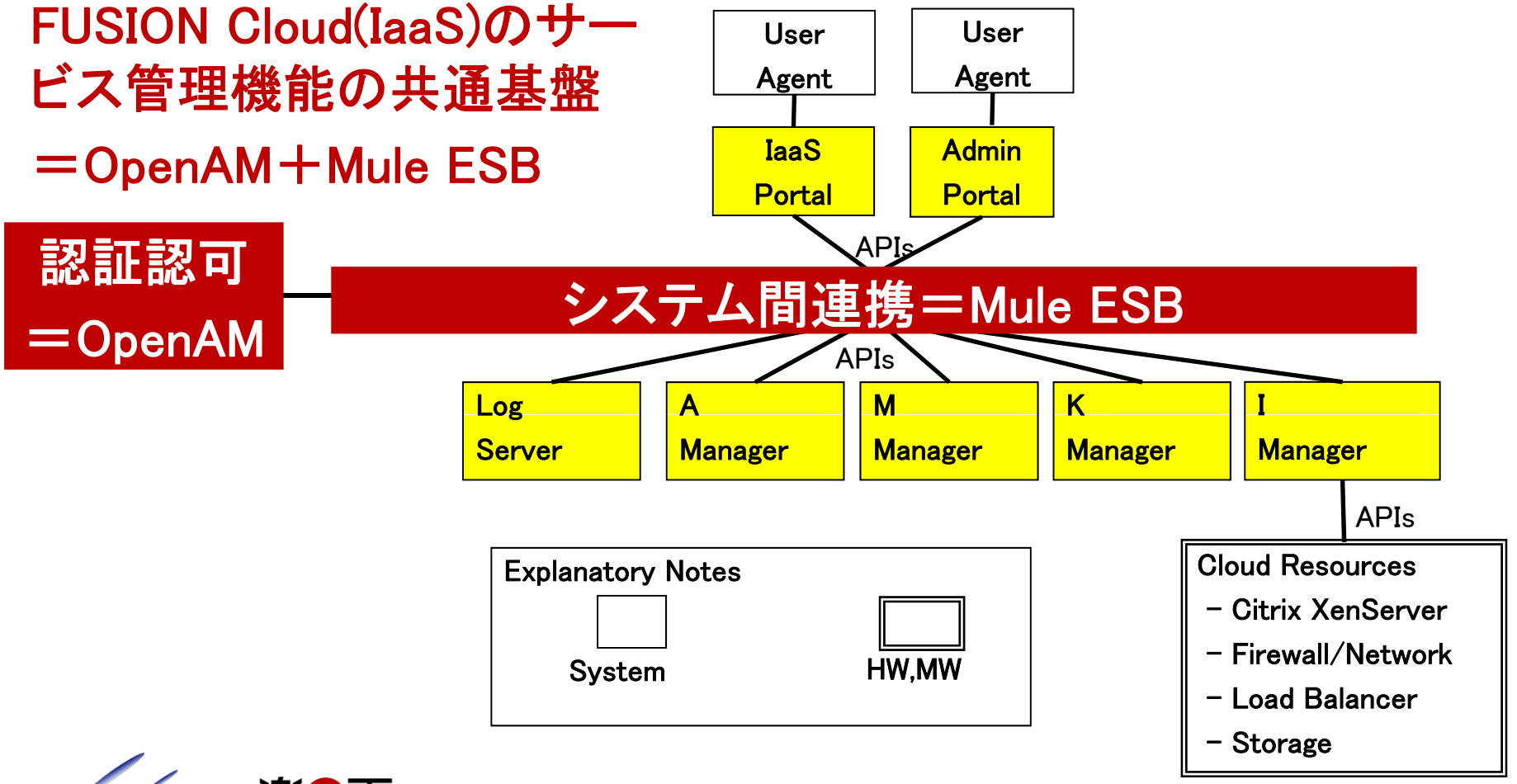
FUSION Cloud(IaaS)の設計思想とOpenAMの役割

FUSION Cloud(IaaS)のサービス管理機能（黄色部分）をフュージョンにて独自開発してきた。

そのサービス管理機能の共通基盤として、OpenAMを使った認証認可機能とMule ESBを使ったシステム間連携機能を商用レベルで設計・実現した（赤色部分）。

FUSION Cloud(IaaS)のサービス管理機能の共通基盤

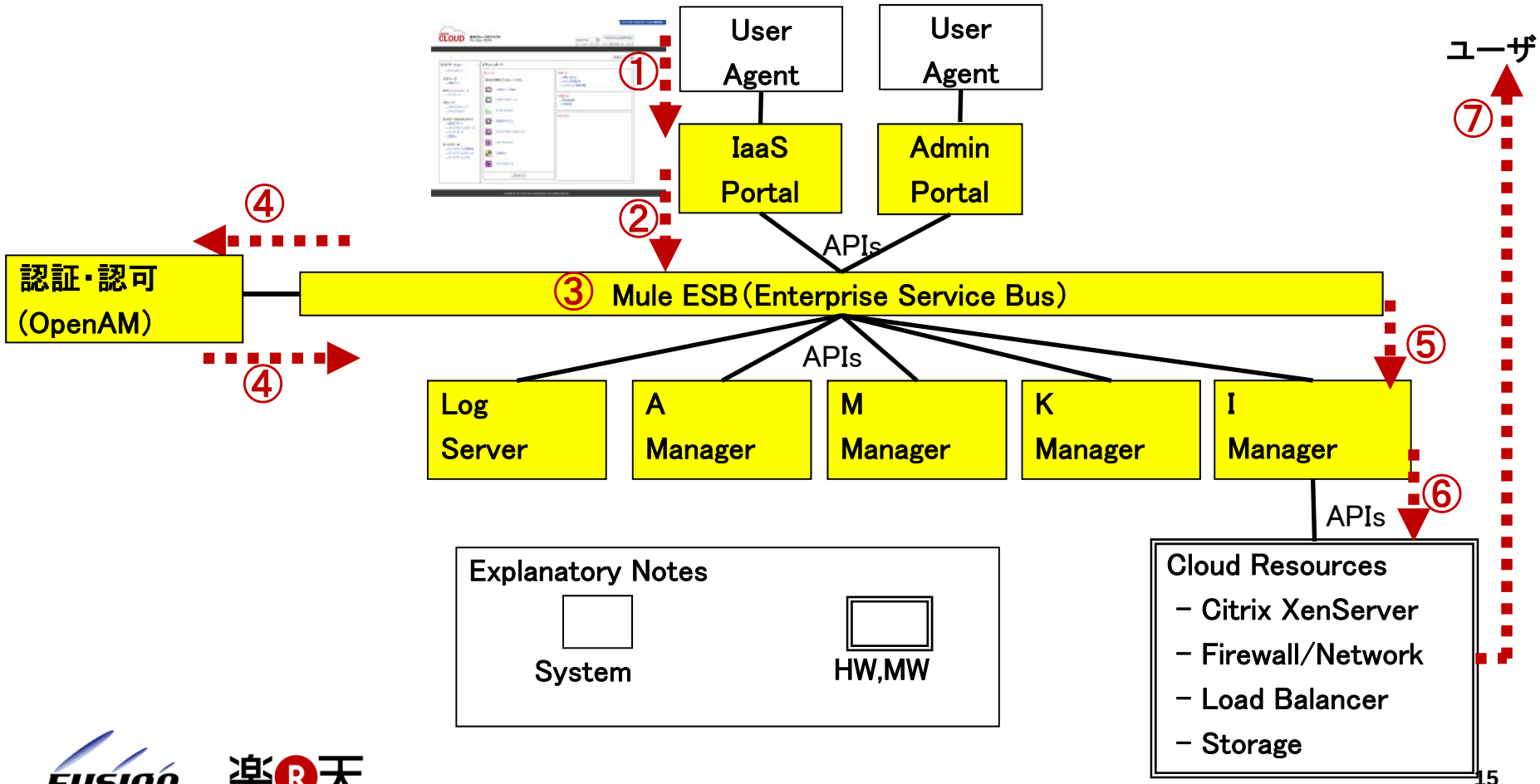
＝OpenAM＋Mule ESB



FUSION Cloud(IaaS)におけるVM起動の流れ

IaaS PortalでVM起動を行った場合のユーザへのVM引き渡しまでの流れは下記の通り。

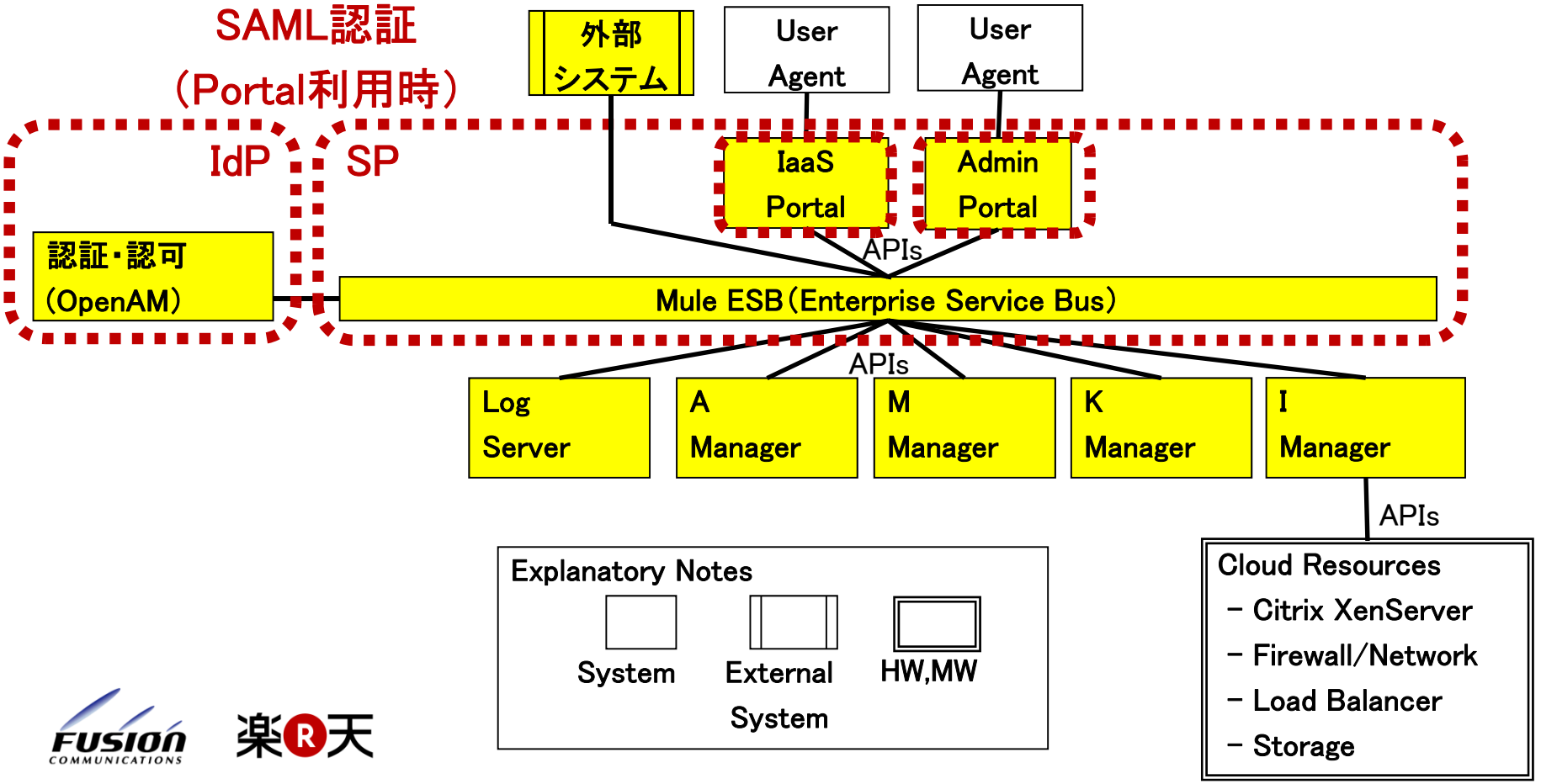
- ①User AgentがIaaS PortalでVM起動を行うと、②IaaS PortalはMule ESBのVM起動APIを起動し、③Mule ESB（Enterprise Service Bus）は④認証認可を介して⑤I ManagerのAPIを起動。
- その際に⑥I Managerは、Cloud Resourcesにある Server, FW, NW, LB, Storageから所要のVMを作成して、⑦ユーザに引き渡す。



OpenAMによる認証（Portalの場合）

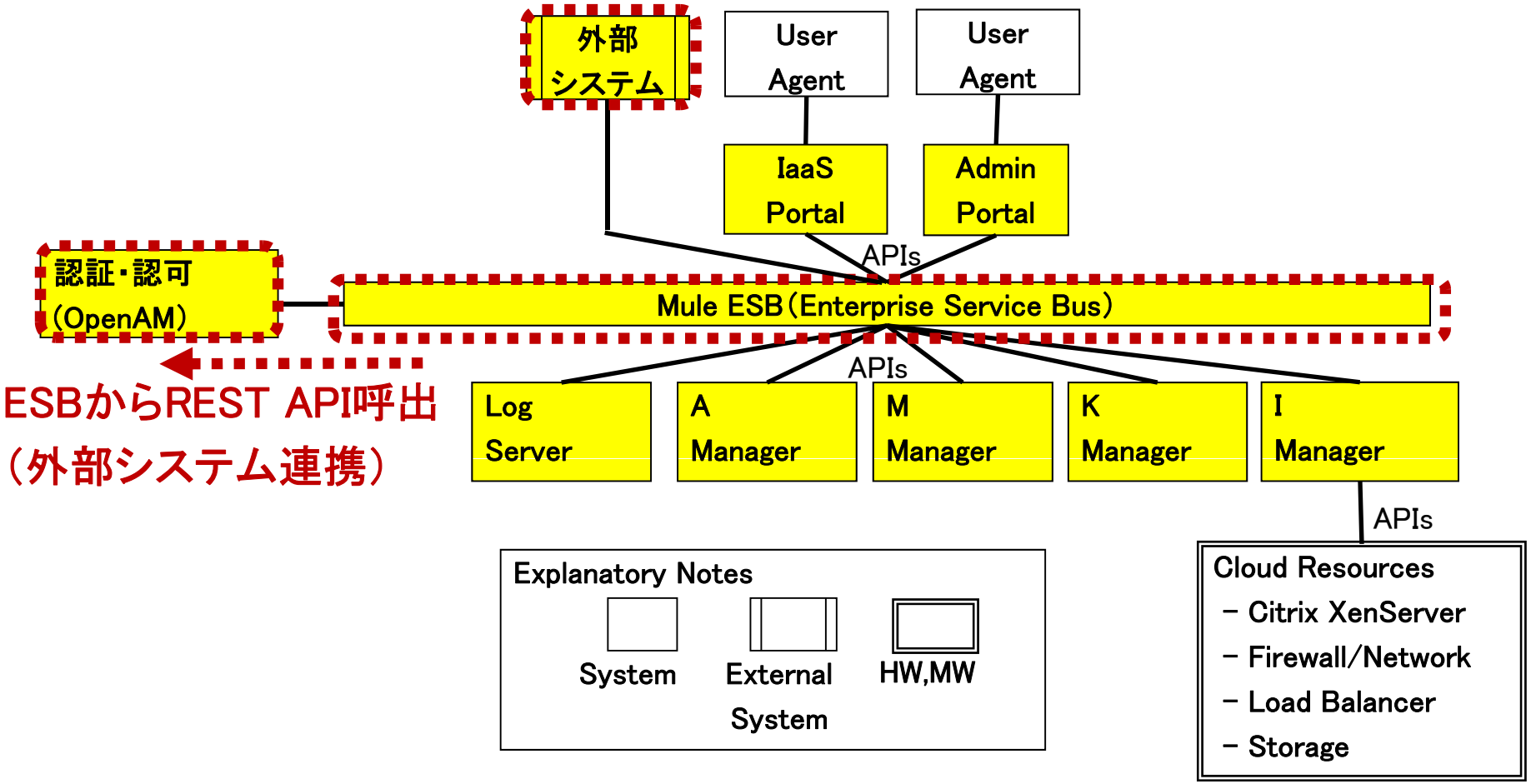
User AgentからIaaS PortalまたはAdmin Portalを使用する場合、SAML認証（シングルサインオン／SSO）を行っている。現状は、IaaS PortalとAdmin Portalの間のみSSOを実現している。

- サービスプロバイダ（SP）は、IaaS Portal/Admin Portal＋Mule ESBが該当。
  Mule ESBがSPの一部機能を担っているため、ポータル側はUIに特化することができる。
- アイデンティティプロバイダ（IdP）は、OpenAMを採用。



OpenAMによる認証（外部システム連携の場合）

Portal経由ではなく、外部システムから直接呼び出しを受ける場合、Mule ESBからOpenAMのREST APIを呼び出す形で認証を行っており、外部システムをPortal経由の場合と同じ基盤に収容している。

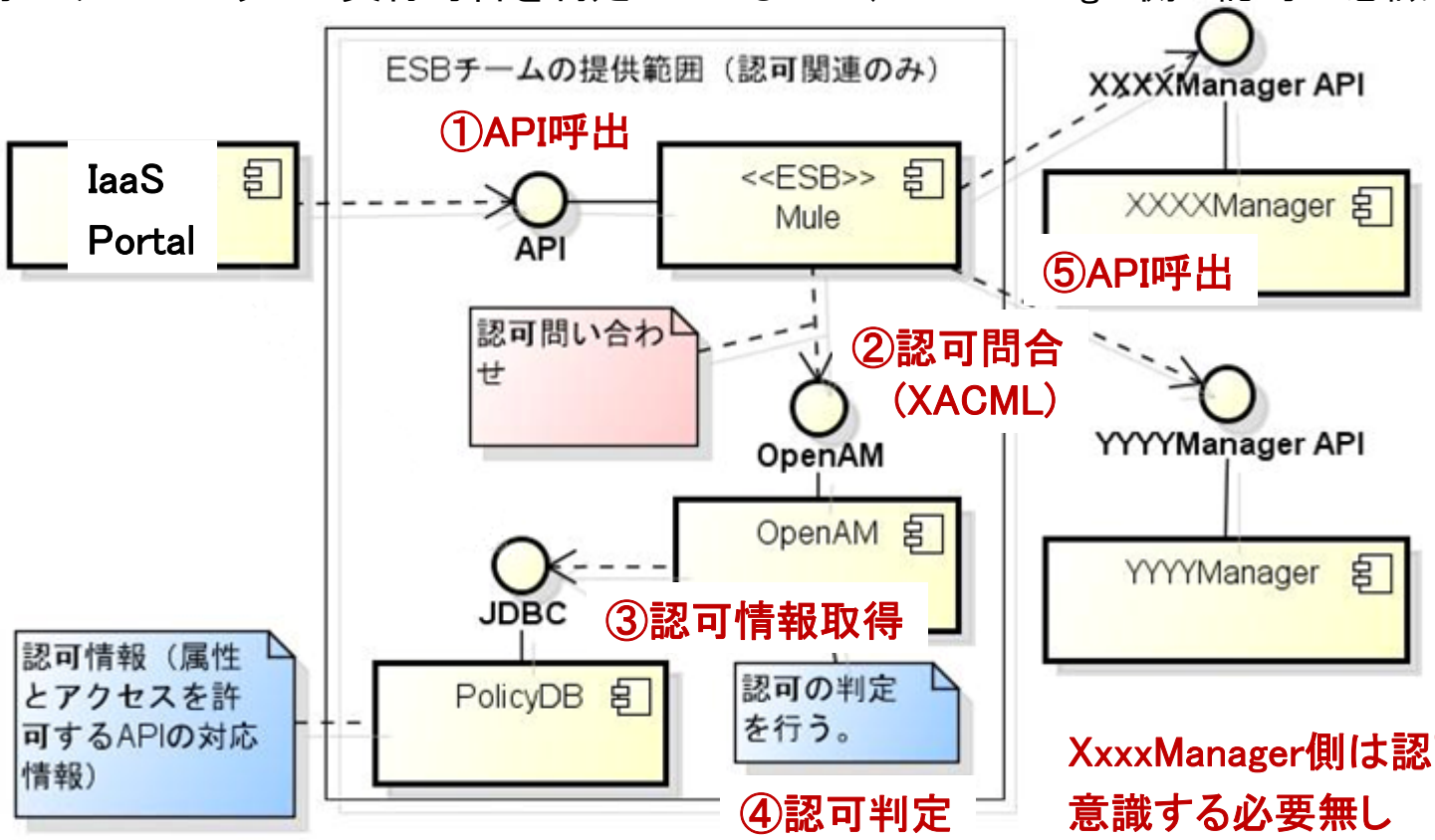


OpenAMによる認可

認可の流れは下記の通り。

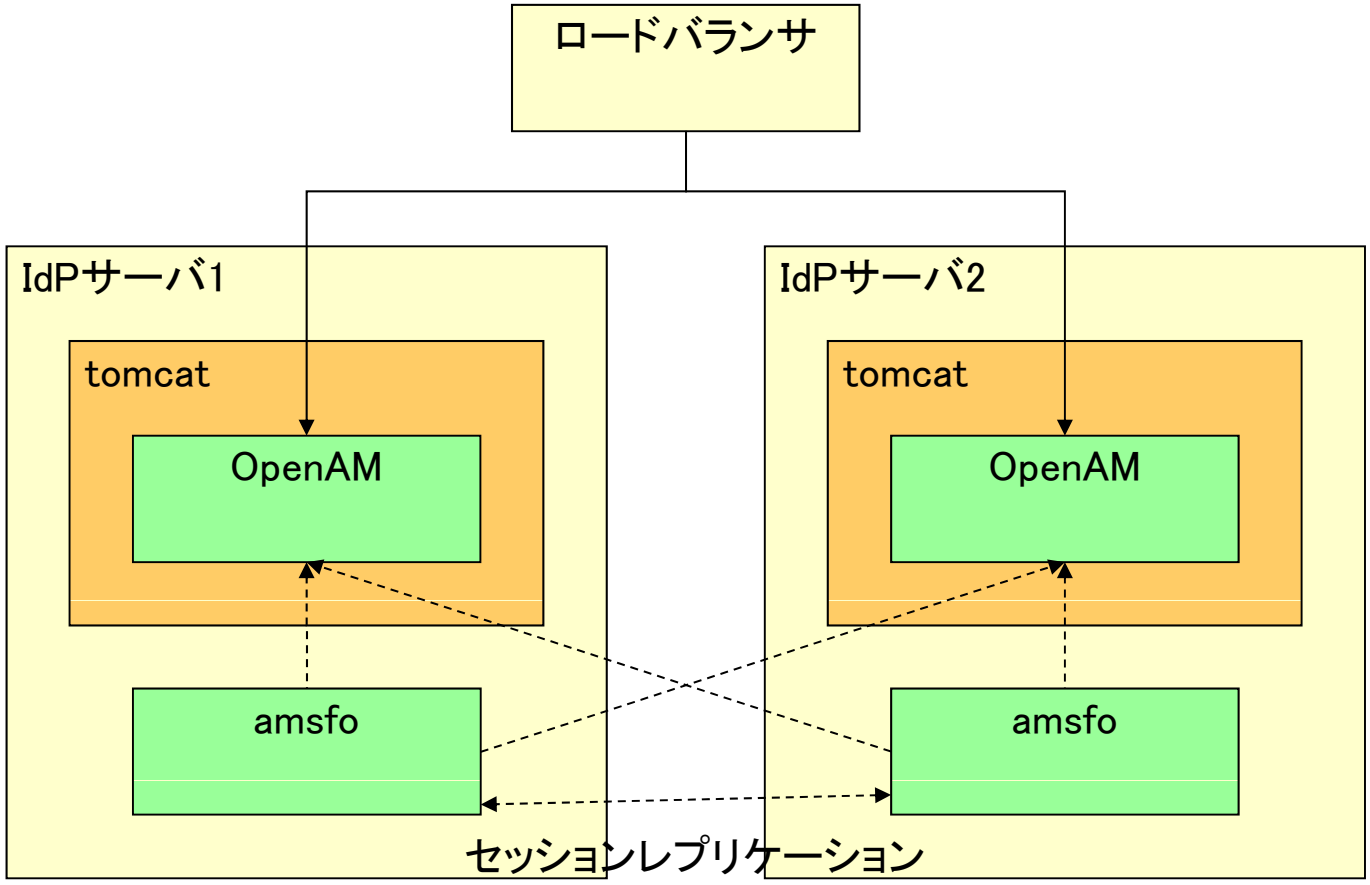
①IaaS PortalからMule ESBのAPI呼び出しを行うと、②Mule ESBはOpenAMに対してXACMLで認可問い合わせを行う。③OpenAMはそれを元にJDBCに対して認可情報の取得を行い、④その結果をもって認可判定を行う。⑤Mule ESBはそれを元にAPI（XxxxManager）の呼び出しを行う。

①のAPIの呼び出し元となるポータル、または呼び出し先となる⑤のXxxxManagerでは、認可に関してリソースのオーナーかどうかで実行可否を判定しているため、XxxxManager側で認可の意識は不要。



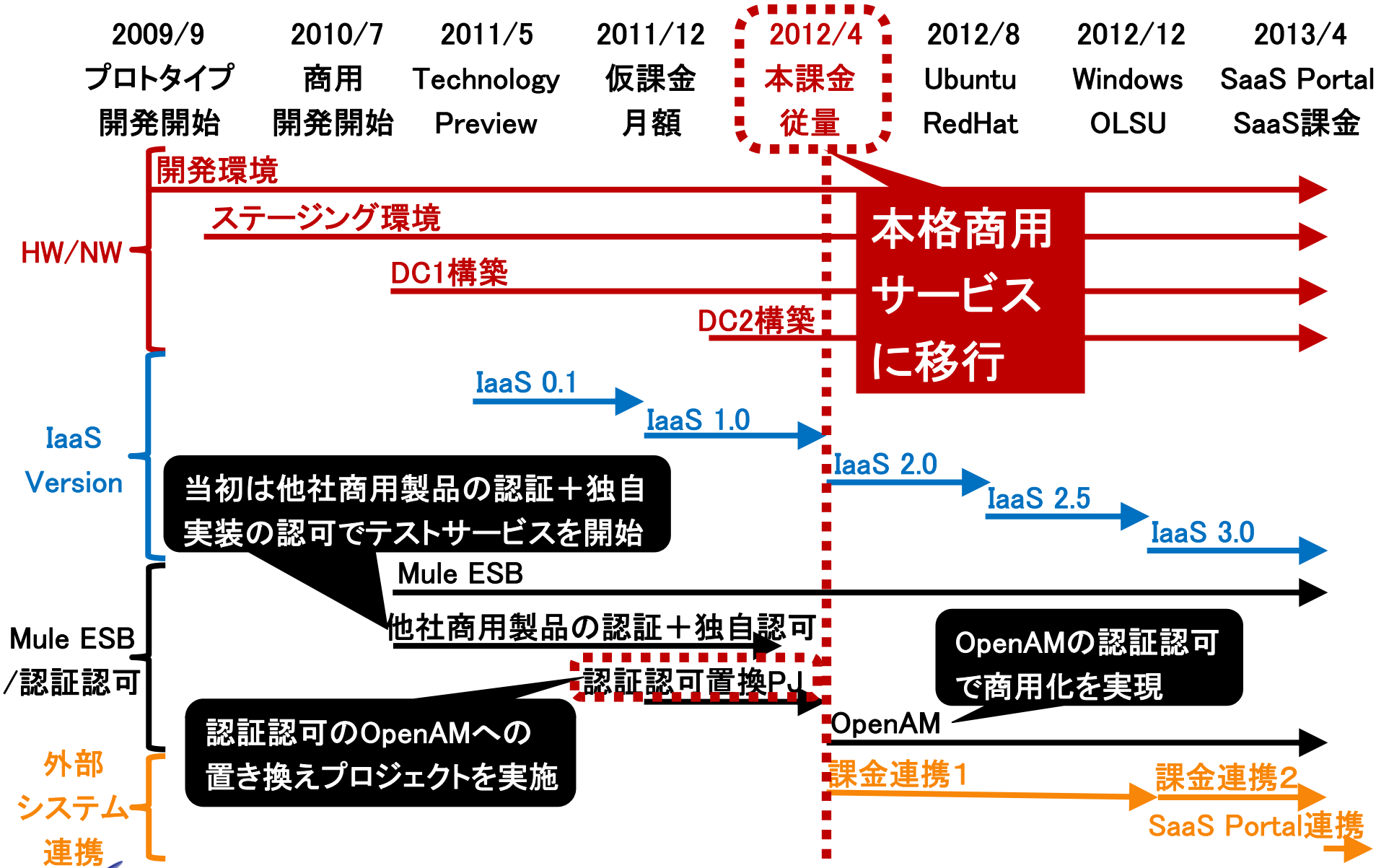
OpenAMの冗長構成

OpenAMのセッションフェイルオーバーツールであるAmsfoを用いてOpenAMの冗長化を実現している。



3. FUSION Cloudの本格商用サービス化にあたってのOpenAM採用の経緯

FUSION Cloud(IaaS)開発の歴史



認証認可のOpenAMへの置き換えプロジェクト

- 認証認可を「他社商用製品の認証＋独自実装の認可」から「OpenAM」の認証認可への置き換えを実施した（2012/04）。
  - ✓ 他社商用製品の有識者がおらず、そのチューニングで苦労していた。そのため、「他社商用製品の認証＋独自実装の認可」で認証認可を提供し続けるための技術レベルの維持と保守コストが課題であった。
  - ✓ OpenAMであれば、「他社商用製品の認証＋独自実装の認可」からの置き換え工数が少ない上、オージス総研様のご協力を頂くことで上記課題を解決可能と判断し、入れ替えを実施。
- 入れ替え前後のパッケージと認証認可との関係は下記の通り。

	認証	認可
前：他社商用製品	有り（SAML）	無し（別途独自実装）
後：OpenAM	有り（SAML）	有り

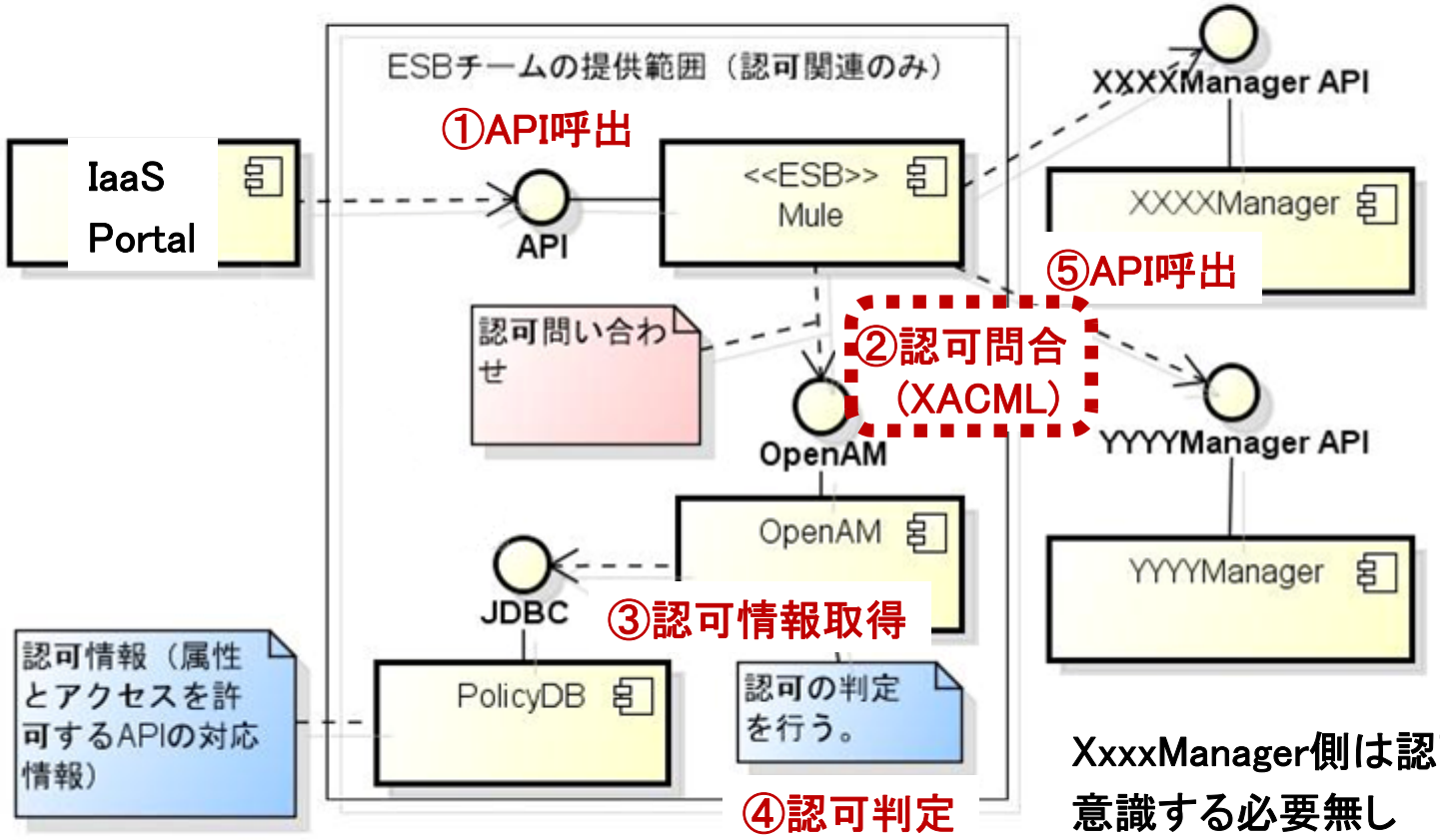
認証認可のOpenAMへの置き換えプロジェクト

- 入れ替えで苦労したこと。

  認可をXACMLの規格にのっとって実装しようとしたが、OpenAMのXACMLは本来の規格に沿った実装ではなかった。そこで、OpenAMのXACMLの仕様に合わせる必要があった。

- やってよかったこと。

  保守運用面のコストダウンと商用レベルでのサービス品質の確保を実現できた。

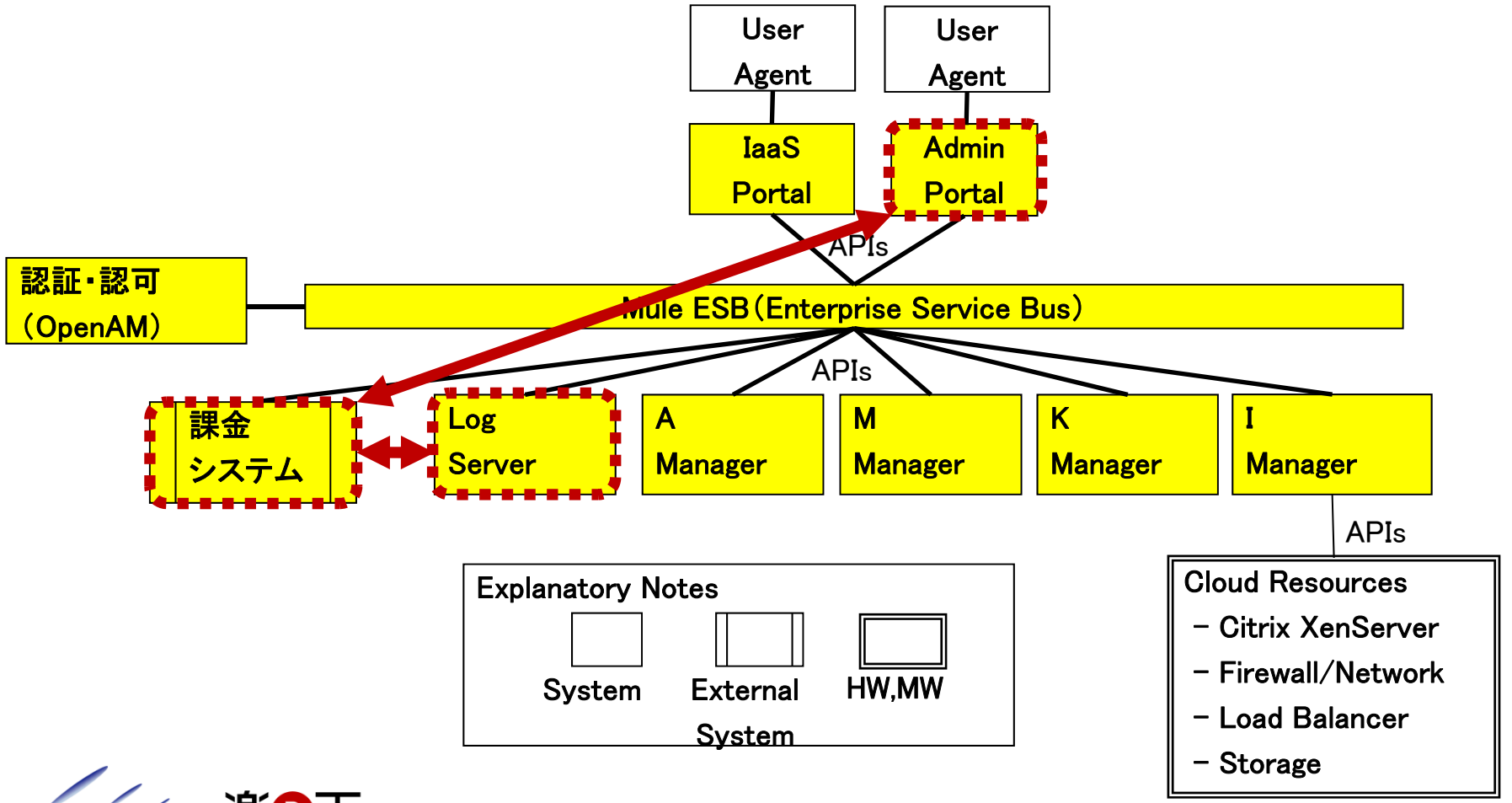


XxxxManager側は認可処理を意識する必要無し

4. FUSION Cloudと外部システムとの連携の実現とメリット

実装例1. 課金システムとの連携

- IaaSの商用課金（月額課金、時間課金）の開始にあたり、外部システムである課金システムとの連携をMule ESBおよび認証認可（OpenAM）で実現。
- 外部システムとの連携は、Mule ESBおよび認証認可（OpenAM）の基盤が出来上がっていたため、短期かつ容易に実現できた。



実装例1. 課金システムとの連携

- 苦労したこと

  ESBの面では、SOAP自体の規格は決まっているが、FUSION Cloudと課金システムとの実装に齟齬が生じ、最初の疎通の際に苦労した。認証認可の面では、特に問題なし。

- やってよかったこと

  外部システムとの連携は、Mule ESBおよび認証認可（OpenAM）の基盤が出来上がっていたため、短期かつ容易に実現できた。

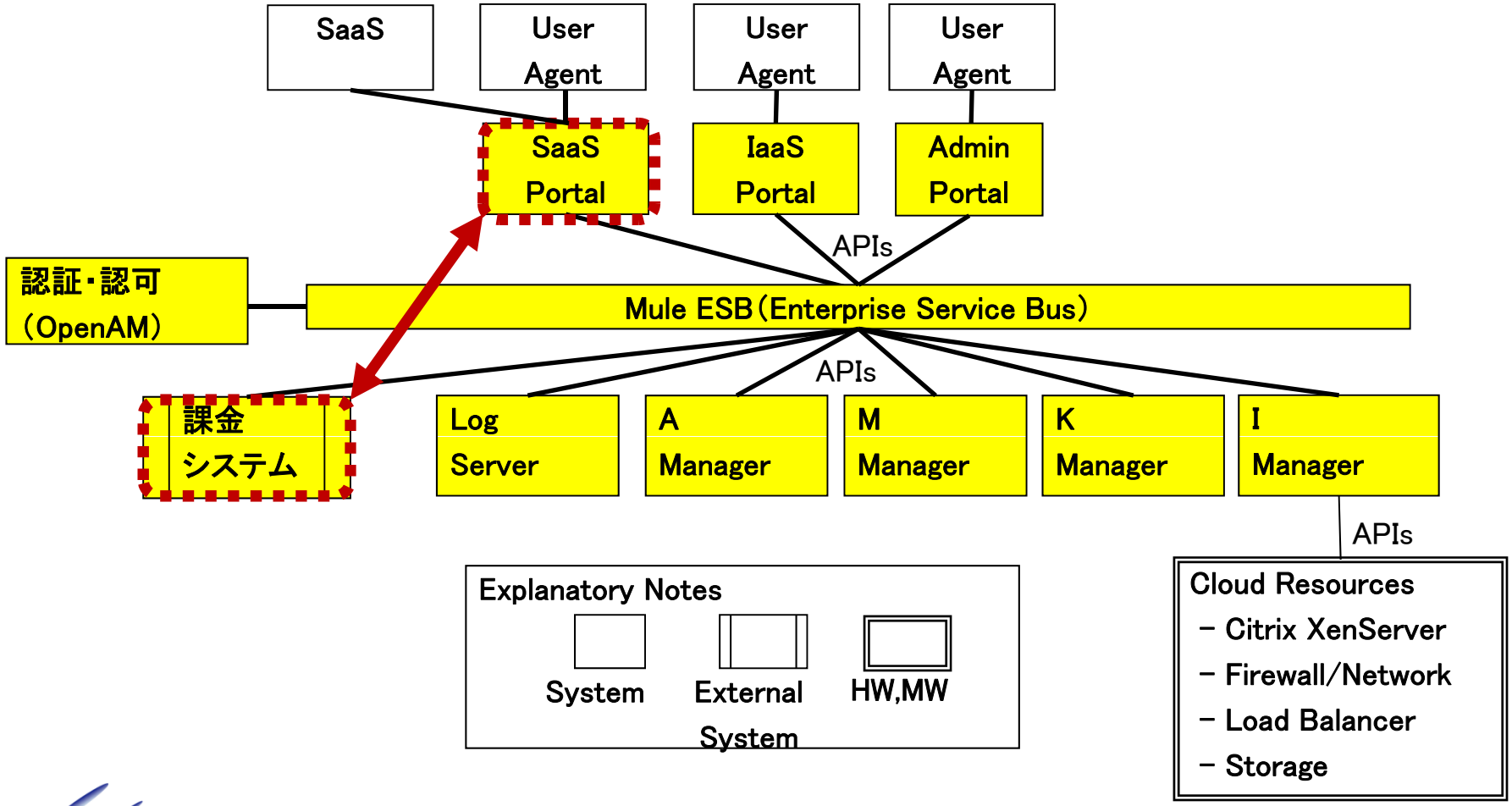
  認証はOpenAMのRESTの機能をはじめて使って連携した。その際にFUSION Cloud側の変更はESBからRESTの呼び出しをするだけで済んだ。

  認可はPortalと同じ仕組みでできた。

  API公開時もRESTの機能を使って実現する予定。

実装例2. SaaS Portalとの連携

- SaaSの商用課金（月額課金）の開始にあたり、外部システムであるSaaS Portalと課金システムとの連携をMule ESBおよび認証認可（OpenAM）で実現。
- 外部システムとの連携は、Mule ESBおよび認証認可（OpenAM）の基盤が出来上がっていたため、短期かつ容易に実現できた。



実装例2. SaaS Portalとの連携

- 苦労したこと

  SOAP自体の規格は決まっているが、FUSION CloudとSaaS Portalとの実装に齟齬が生じ、最初の疎通で苦労するのではないかとの前提で開発をすすめた。

- やってよかったこと

  外部システムとの連携は、Mule ESBおよび認証認可（OpenAM）の基盤が出来上がっていたため、短期かつ容易に実現できた。

  疎通ができた後は順調に開発を完了。

  FUSION Cloud側は課金システム連携のときに作った仕組みをそのまま使えた。

5. SaaSの具体例

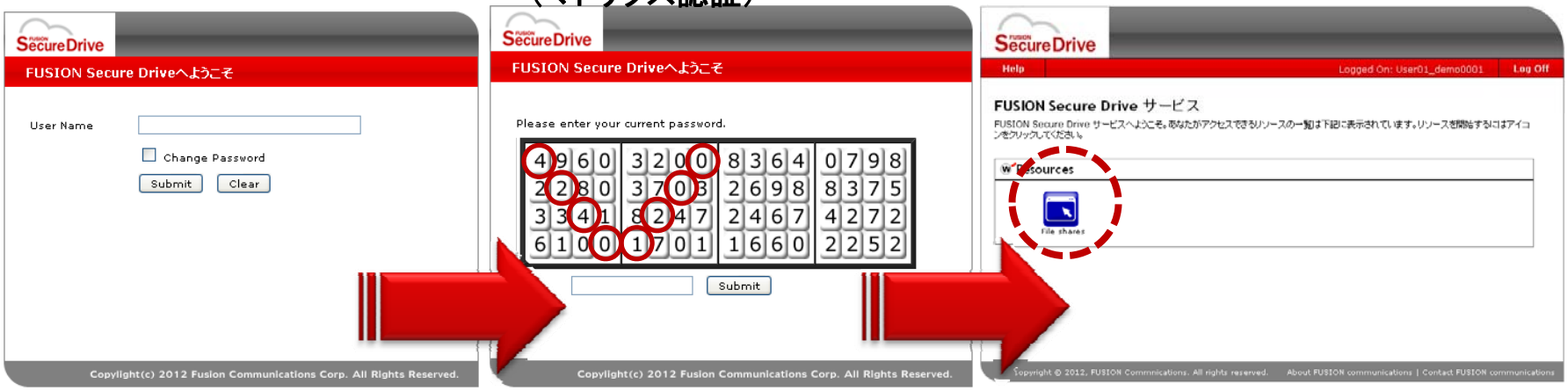
FUSION Secure Drive（使い方）

- マトリクス認証により、セキュリティを確保。
- Windows Explorerそのものなので、ユーザの使い勝手が良い。

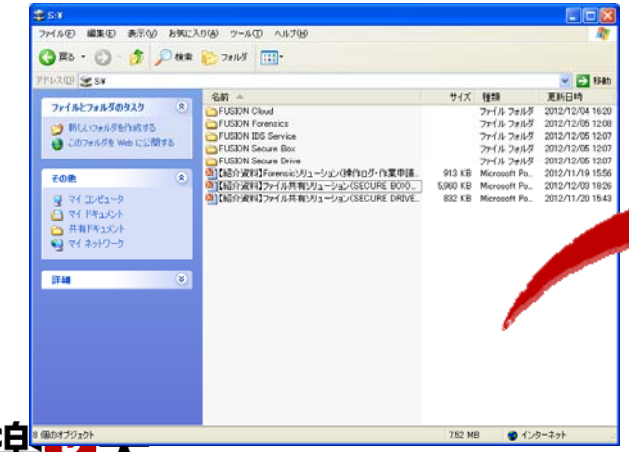
1. Webブラウザよりアクセス

2. イメージパスワードを入力（マトリクス認証）

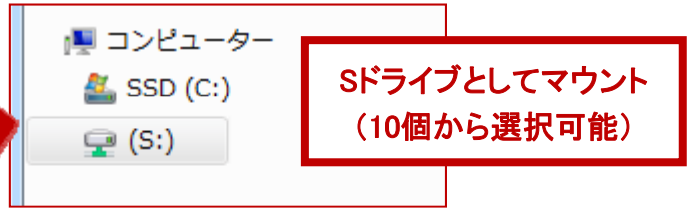
3. アクセスする対象アイコンをクリック



4. エクスプローラが表示 ⇒ ファイル操作



（ネットワークドライブとしてマウント）



FUSION Secure Drive（料金プラン）

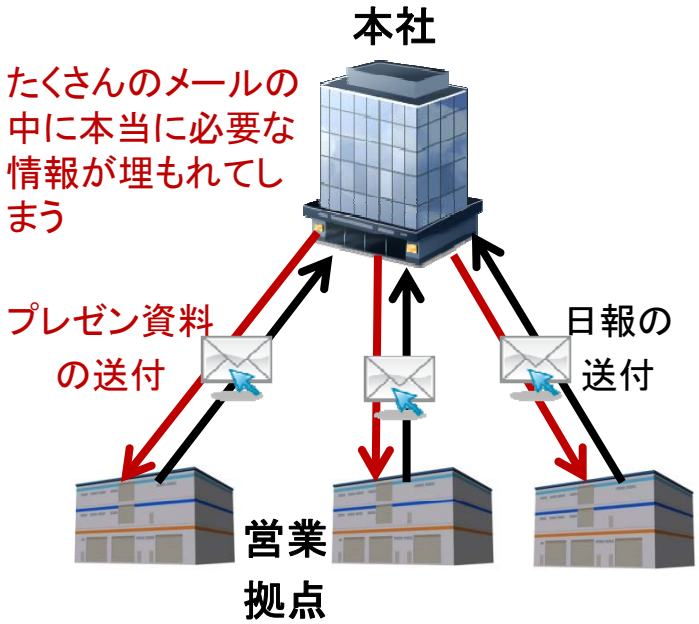
- **FUSION Secure Drive 標準プラン（2013/02/18～）**
  当サービスのベース。共用ファイルサーバ、共用SSL-VPNで共通機能を提供するプラン。
- **FUSION Secure Drive プライベートプラン（個別対応）**
  専用ファイルサーバ（専用VM）、共用SSL-VPNで共通機能を提供するプラン。有償オプションを提供。
- **FUSION Secure Drive 専用プラン（個別対応）**
  専用ファイルサーバ（専用VM）、共用SSL-VPNで共通機能を提供するプラン。有償オプションを提供。

FUSION Secure Drive（管理コンソール）

管理コンソールでFUSION Secure Driveの契約ID数、ストレージ容量やパスワードを管理できる。
管理コンソールと課金システムとの連携をMule ESBとOpenAMの認証認可で実現。

FUSION Secure Drive（ユースケース）

-本社と全国営業拠点間でのプレゼン資料の共有や日報運用-



＜従来のメールでのやり取り＞

本社と営業拠点との間の情報共有に手間がかかったり、リアルタイムな情報共有ができない。

- １日に何回もパスワード付添付ファイルのメールを各拠点に送付
- メールの送付先間違い、旧版データ送信などの伝達ミスが発生

＜FUSION Drive導入後＞

本社と営業拠点との間で情報共有がスムーズにできる。

- 過去の履歴を含めたプレゼン資料を営業拠点にリアルタイムに共有できるので、最新版がどれかすぐにわかる、最新版をすぐに取り出せる
- 営業拠点からの日報を本社でリアルタイムに把握できる

6. まとめ

まとめ

- FUSION Cloudは、サービス管理機能を提供するための共通基盤として、Mule ESBを使ったシステム間連携機能と、OpenAMを使った認証認可機能を実現。
- 認証認可のOpenAMへの置き換えプロジェクトを実施し、そのプロジェクト完了をもって本格商用サービスに移行することができた。
- 外部システムとの連携は、Mule ESBおよび認証認可（OpenAM）の基盤が出来上がっていたため、短期かつ容易に実現できた。
- 今後、これらの基盤を使ってフュージョンのIaaS/PaaS/SaaSを拡充。

ご清聴ありがとうございました。

- FUSION Cloud（IaaS/PaaS/SaaS）に関するお問い合わせ先

  フュージョン・コミュニケーションズ株式会社　事業推進部

  TEL　　050-5518-8259

  E-mail　　cloud_plan@fusioncom.co.jp

- OpenAMとMule ESBに関するお問い合わせ先

  株式会社オージス総研　ソリューション営業部

  TEL　　03-6712-1201

  E-mail　　info@ogis-ri.co.jp