



---

# AWS Summit

Tokyo

---



## ■ Gold Sponsors



Empowered by Innovation



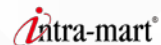
## ■ Global Sponsors



## ■ Silver Sponsors



## ■ Bronze Sponsors



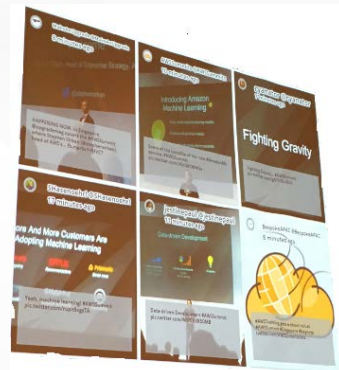
## ■ Global Tech Sponsors



## ■ Logo Sponsors



ハッシュタグ **#AWSSummit**  
で、皆さんのツイートが展示エリア  
の大画面に表示されます



公式アカウント **@awscloud\_jp**  
をフォローすると、ロゴ入り  
コースターをプレゼント



【コースター配布場所】

メイン展示会場、メイン会場1F受付、デベロッパーカンファレンス会場





# Enterprise Applications Deep Dive (Amazon WorkSpaces/WorkDocs/WorkMail)

アマゾンデータサービスジャパン株式会社  
ストラテジックソリューション部ソリューションアーキテクト  
渡邊 源太



# 自己紹介

- 名前
  - 渡邊源太
- 所属
  - アマゾンデータサービスジャパン株式会社ストラテジックソリューション部（エンタープライズ担当）
  - ソリューションアーキテクト
- Twitter ID
  - @gentaw0
- 好きなAWSサービス
  - Amazon WorkSpaces



# アジェンダ

- AWSのエンタープライズアプリケーション
- AWS Directory Service
- Amazon WorkSpaces
- Amazon WorkDocs
- Amazon WorkMail



# AWSのエンタープライズアプリケーション



# AWSが提供する40以上のサービス

Support Professional Services Partner Ecosystem Training & Certification Solutions Architect Account Management Security & Pricing Reports

Technical & Business Support

Virtual Desktop

Sharing & Collaboration

Business Email

Enterprise Applications

## Analytics

Hadoop

Real-time Streaming Data

Data Warehouse

Data Pipelines

## App Services

Queuing & Notifications

Workflow

App Streaming

## Developer Tools & Operations

Deployment

DevOps

Application Lifecycle Management

Resource Templates

Containers

Event-driven Computing

## Mobile Services

Identity

Sync

Mobile Analytics

Push Notifications

Platform Services

Identity Management

Access Control

Resource & Usage Auditing

Key Management & Storage

Monitoring & Logs

Administration & Security

Compute (VMs, Auto-scaling & Load Balancing)

Storage (Object, Block and Archival)

CDN

Databases (Relational, NoSQL, Caching)

Networking (VPC, DX, DNS)

Core Services

Regions

Availability Zones

Points of Presence

Infrastructure

# エンタープライズアプリケーション

仮想デスクトップサービス

マネージド型電子メール・カレンダー

企業向けファイル共有サービス

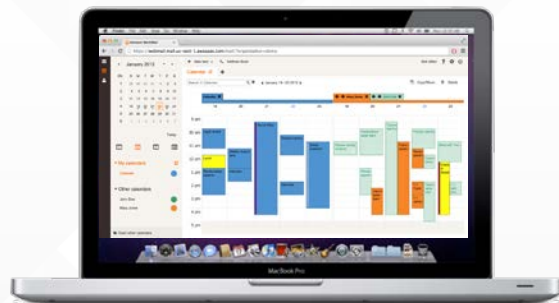


amazonWorkSpaces

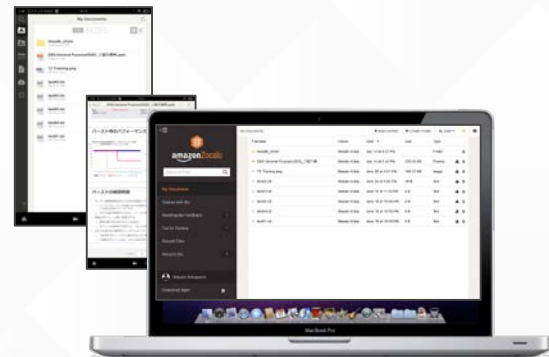


amazonWorkMail

Preview



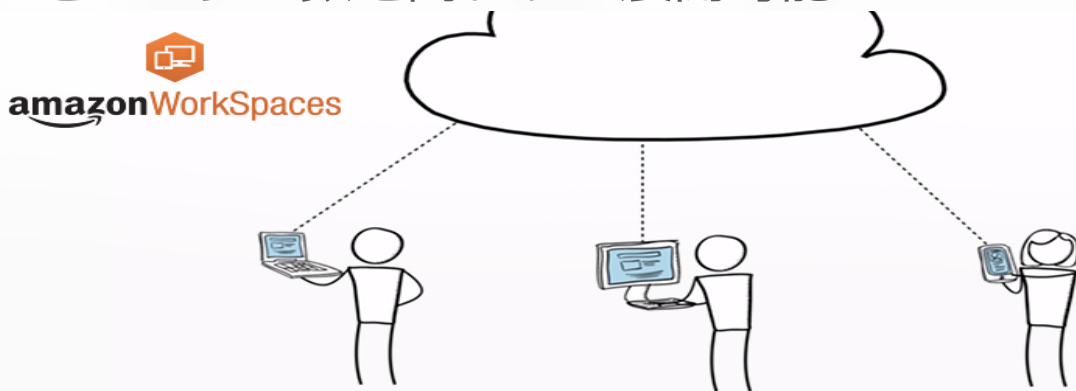
amazonWorkDocs



# Amazon WorkSpaces



- クラウドで動作するマネージド型のデスクトップコンピューティングサービス
  - Windows/Mac/iPad/Kindle Fire/Androidタブレットなど任意のデバイスからアクセス
  - マネジメントコンソールを数回クリックするだけでデスクトップをユーザー数を問わずに展開可能



# Amazon WorkSpacesへの接続

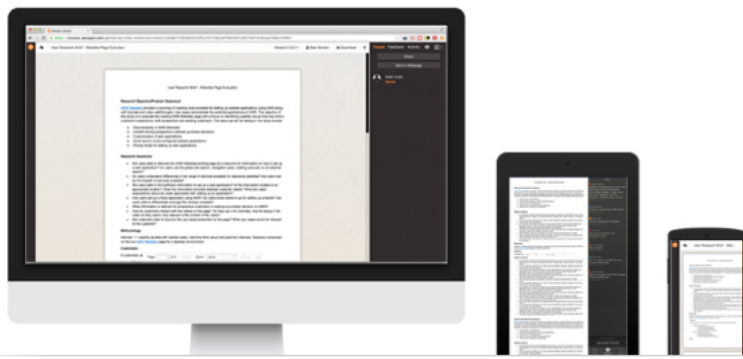


# Amazon WorkDocs



amazonWorkDocs

- フルマネージド型のセキュアなエンタープライズストレージおよび共有サービス
  - ユーザーの生産性を高める強力な管理制御とフィードバック機能
  - ユーザーはWindows、Mac、iOS/Androidタブレットなどのデバイスからどこにいてもアクセスが可能



# ドキュメントのプレビューと共有

- 主要な形式のファイルについてはWebUIで直接内容を閲覧できる
- 共有メニューから他ユーザに対する権限（読み取りのみ、読み書き）を設定する。権限付与されたユーザにはメールで通知される

The screenshot shows a document viewer for 'Amazon WorkSpaces 関連サービス紹介資料.pptx'. The document content includes the title 'Amazon WorkSpaces', a list of features, and a diagram. A 'Share' button is highlighted in the top right corner. A 'Share' dialog box is open, showing a list of users to share with and a text area for a personal message.

**Document Content:**

### Amazon WorkSpaces

- クラウドで動作する完全マネージド型のデスクトップコンピューティングサービス
- ノートPC/iPad/Kindle Fire/Androidタブレットなど任意のデバイスからアクセス
- マネジメントコンソールを数回クリックするだけでデスクトップをユーザー数を問わずに展開可能

**Share Dialog:**

Who would you like to share with?

Search Users

Taro Finance	x
Taro Game	x
Taro Media	x

Add a personal message

お客様へのご紹介資料をシェアします。

Please give me feedback

Deadline  Set a date  Set a time

Limited Access (view only)

Cancel OK

# フィードバック機能

- 共有されたドキュメントにはコメントやメッセージで相互にフィードバックを行える。対象となる箇所をハイライトすることも可能
- コメントが投稿されるとメールによる通知が行われる



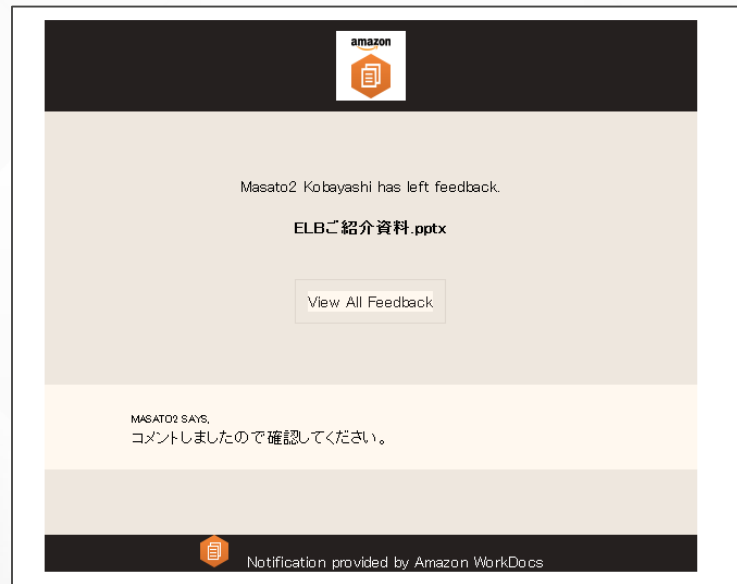
The screenshot shows a document viewer interface. The document title is "ELBご紹介資料.pptx". The main content area displays a slide titled "HTTPS/SSL利用時のサーバ証明書" (Server Certificate for HTTPS/SSL). The slide content includes:

- ELBにサーバ証明書をアップロード
- HTTPS/SSL利用にはサーバ証明書のアップロードが必須
- 複数ホスト名には別名・ワイルドカードが複数ELBで対応 (SNI未対応)
- バックエンドとの通信にSSLを用いないなら証明書の管理が容易
- マネージメントコンソール or CLI or IAM APIで設定

Below the text is a diagram showing a server icon, a key icon, and a document icon, with arrows indicating the flow of information. A callout box states: "SSL証明書のライセンスに関しては、サーバ単位/ドメイン単位で発行などそれぞれ異なるので発行元に関わり合わせの事".

On the right side, there is a feedback sidebar with the following content:

- People Feedback Activity
- VERSION 1
- PAGE 23
- MASATO2 KOBAYASHI: 重要なポイントですね。 (Draft)
- MASATO2 KOBAYASHI: orが多すぎるのでスッキリとした表現に改めてください。 (Draft)
- MASATO2 KOBAYASHI: アイコンが重なっているのは美しくありませんので修正してください。 (Draft)
- You've drafted 3 comments.
- Send



The screenshot shows a notification email from Amazon WorkDocs. The email header includes the Amazon logo and the document title "ELBご紹介資料.pptx". The main body of the email contains the following text:

Masato2 Kobayashi has left feedback.

View All Feedback

MASATO2 SAYS,  
コメントしましたので確認してください。

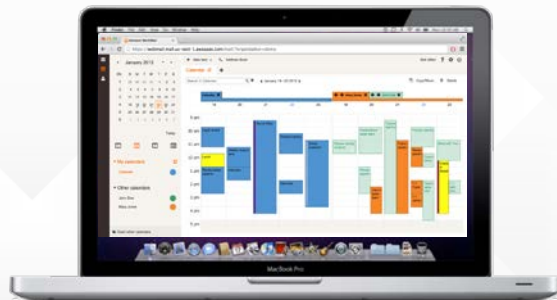
Notification provided by Amazon WorkDocs

# Amazon WorkMail (プレビュー)



amazonWorkMail

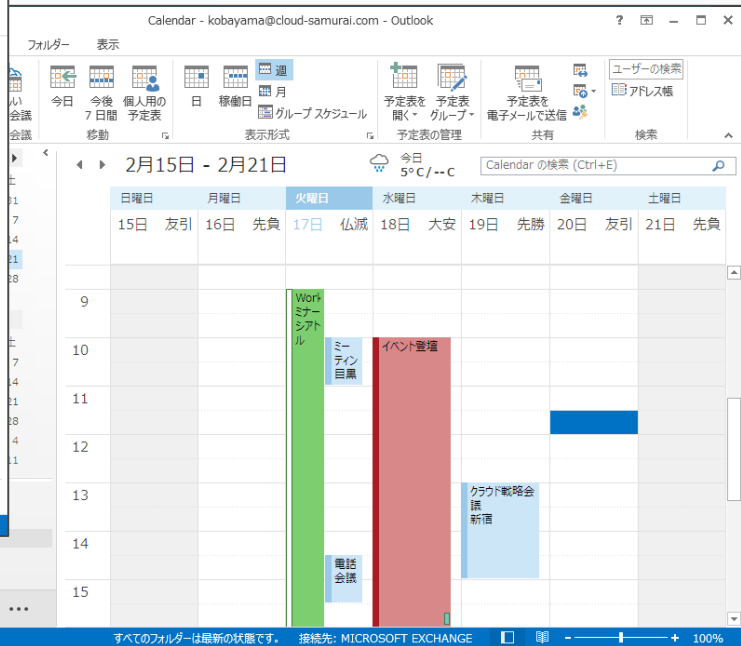
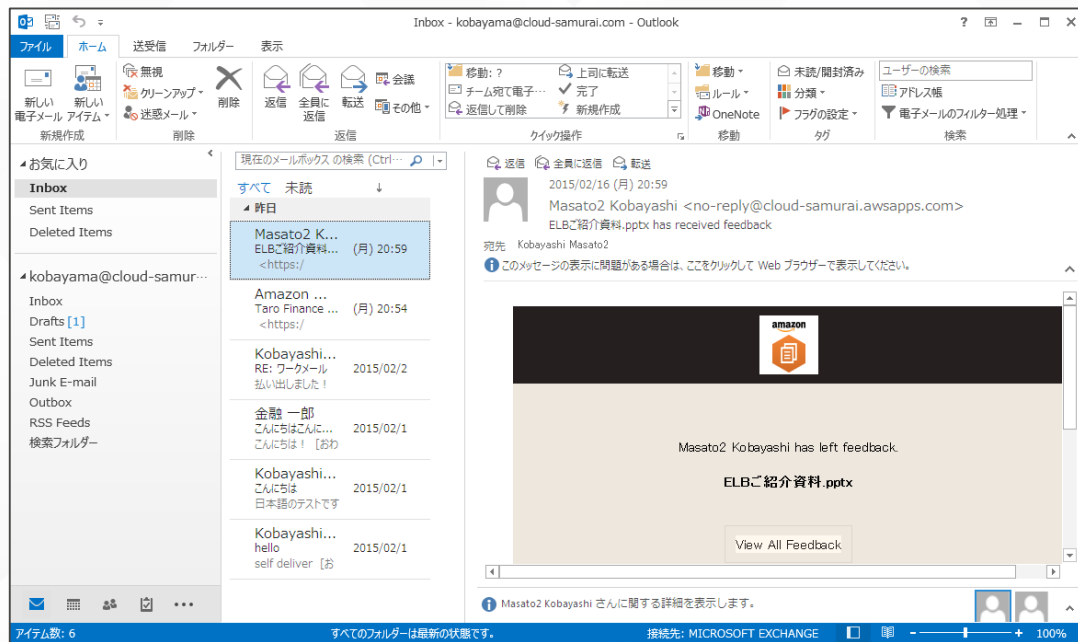
- セキュリティにすぐれたマネージド型の企業向けEメールおよびカレンダーサービス
  - Microsoft Outlook、Webブラウザ、iOS/AndroidネイティブのEメールアプリケーションからのアクセス
  - データを暗号化するためのキーとデータを保存する場所を管理することが可能





# Outlookとの互換性

- WindowsおよびMac OS XのMicrosoft Outlookをネイティブでサポート



# Webクライアントによるアクセス

- WebブラウザでもEメールとカレンダーにアクセス可能

The screenshot displays a web-based email and calendar interface. On the left, there is a navigation sidebar with folders such as 'Inbox - Kobayashi Masa...', 'Deleted Items', 'Drafts', 'Inbox', 'Junk E-mail', 'Outbox', 'RSS Feeds', and 'Sent Items'. The main content area is divided into two sections: an email list and a calendar view. The email list shows several messages, with the top one from 'Mas Monday 02/16/2015 8:58 pm' with the subject 'ELBご紹介資料.pptx has re'. The calendar view shows a weekly grid for February 2015, with a detailed view for February 16-20, 2015. The calendar includes a search bar and a list of events, such as 'Workspaces (シフト)', 'ミーティング (回線)', 'イベント管理', '電話会議', and 'クラウド研修会議 (新着)'. A feedback notification at the bottom right states 'Masato2 Kobayashi has left feedback. ELBご紹介資料.pptx' with a 'View All Feedback' button.

# マネージドサービスの利点

User Education

App Installation

Scaling

High availability

Database backups

DB s/w patches

DB s/w installs

OS patches

OS installation

Server maintenance

Rack & stack

Power, HVAC, net

オンプレミス

User Education

App Installation

Scaling

High availability

Database backups

DB s/w patches

DB s/w installs

OS patches

OS installation

Server maintenance

Rack & stack

Power, HVAC, net

EC2上に構築

User Education

App Installation

Scaling

High availability

Database backups

DB s/w patches

DB s/w installs

OS patches

OS installation

Server maintenance

Rack & stack

Power, HVAC, net

マネージドサービス

(WorkSpaces/WorkDocs/WorkMail)

# さまざまなデバイスからのアクセス

- iOS
- Kindle Fire HDX
- Android
- Windows
- Mac OS X
- PCoIPゼロクライアント

iOS



# 高いセキュリティ



amazonWorkSpaces

- PCoIPプロトコルによるストリーミング
- 多要素認証 (MFA)



amazonWorkDocs

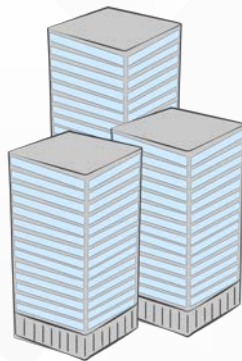
- すべてのデータを暗号化して保存
- CloudTrailによる監査ログの取得



amazonWorkMail

- AWS Key Management Service (KMS) による鍵管理
- データ保管場所の選択が可能

# Active Directoryとの統合



- AWS Directory Service

- ユーザー: 既存のエンタープライズの認証を利用
- IT管理者: 通常のデスクトップのようにワークスペースをコントロール



# AWS Directory Service



# AWS Directory Service

- フルマネージド型のディレクトリサービス
  - AWS上のスタンドアロンのディレクトリを新規に作成
  - 既存のActive Directory認証を利用して：
    - AWSアプリケーションへのアクセス(Amazon WorkSpaces, WorkDocs, WorkMail)
    - IAMロールによるAWS Management Consoleへのアクセス



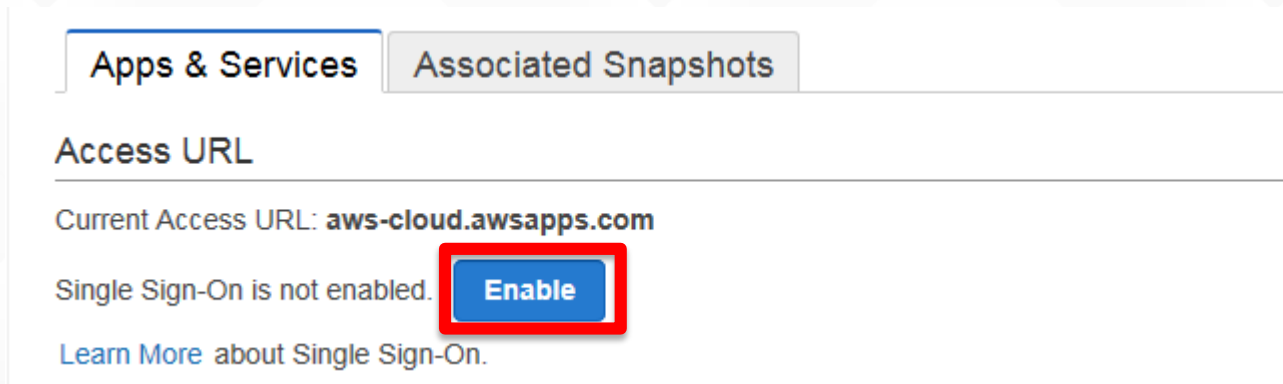


# ディレクトリタイプの選択

- Simple AD
  - フルマネージドのディレクトリ サービス
  - Samba 4 Active Directory互換サーバーを利用
  - AWS上に独立したドメインを作成
- AD Connector
  - 既存のディレクトリ サービスへの接続
  - オンプレミスまたはVPC上のドメインを指定
  - 多要素認証 (MFA) をサポート

# シングルサインオン (SSO) の有効化

- WorkSpacesとWorkDocsの間でシングルサインオン (SSO) を設定可能
  - WorkSpacesにログオンすると自動的にWorkDocs Syncクライアントにサインインして同期を開始
  - Directory ServiceのManagement Consoleより有効化



# 多要素認証 (MFA)

- オンプレミスの RADIUS サーバーを利用した多要素認証 (MFA) に対応
  - ユーザー名とパスワードに加えてワンタイム パスワード等の利用が可能
- PAP/CHAP/MS-CHAP1/MS-CHAP2 をサポート
  - Symantec Validation and ID Protection Service (VIP)
  - Microsoft RADIUS Server

# MFAの設定

- [Multi-Factor Authentication]にRADIUSサーバーの情報を入力して[Update and Exit]を選択

## ▼ Multi-Factor Authentication

RADIUS Status None

Enable Multi-Factor Authentication  チェック

RADIUS server IP address (es)  ⓘ RADIUSサーバーのIPアドレス

Port  ポート番号

Shared secret code  パスワード

Confirm shared secret code  パスワード (確認)

Protocol  ▼ プロトコル

Server timeout (in seconds)  タイムアウト (秒)

Max retries  × リトライ回数

[Update and Exit]を選択

Cancel

Update

Update and Exit

# (例) Google Authenticatorを使った方法

- スマートフォンに無料でインストールできる Google Authenticator をソフトウェアトークンとして使用する。
- サーバ側は、オープンソースのFreeRADIUSと Google AuthenticatorのPAM (Pluggable Authentication Module) を連携させて実現させる。



- <http://aws.typepad.com/sajp/2014/10/google-authenticator.html>

※ユーザ登録時のGUIは無くコマンドライン操作が必要になります。

# Directory Service API

- ディレクトリやコンピュータアカウント、エイリアスの作成・削除などのオペレーションがAPIやCLIから操作可能
  - CreateDirectory
  - CreateSnapshot
  - EnableSSOなど
- CloudTrailとの統合
  - APIアクション (SDK、コンソールまたはCLI経由) はロギング可能

```
CreateDirectory
{"Name": "corp.snackers.org",
 "ShortName": "corp",
 "Password": "Westbay@123",
 "Description": "corp",
 "Size": "Large",
 "VpcSettings":
  {"VpcId": "vpc-c3dd04a2",
   "SubnetIds":
    ["subnet-9add04fb", "subnet-66dc0507"]}
}
```



# Amazon WorkSpaces Deep Dive

# WorkSpacesバンドル

## Value



- 1vCPU
- 2GiB Memory
- 10GB User Storage

## Standard



- 2vCPU
- 4GiB Memory
- 50GB User Storage

## Performance



- 2vCPU
- 7.5GiB Memory
- 100GB User Storage



## Plus



- Microsoft Office Professional 2010/2013
- Trend Microビジネスセキュリティクライアント

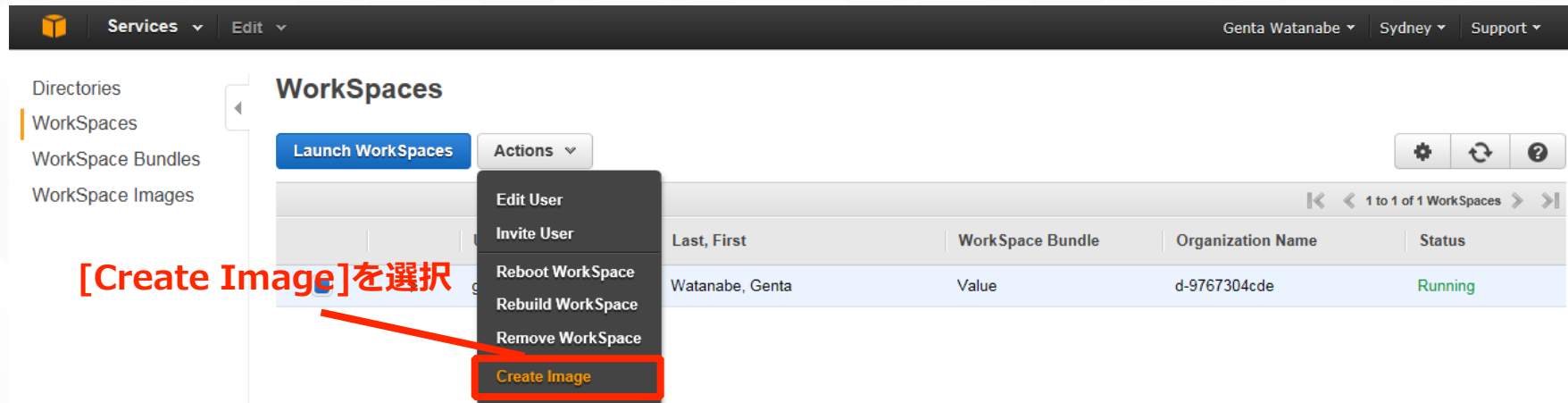


# WorkSpacesバンドルの管理

- カスタムイメージを作成してアプリケーションをインストール済みのカスタムバンドルを利用可能
- 要件
  - インストールするアプリケーションがSysprepと互換性がある
  - WorkSpaceのユーザープロファイルを削除しない
  - ユーザープロファイルの合計サイズが10GB未満
  - ドメインユーザー認証を利用するサービスが存在しない（SQL Server Expressなど）

# Custom Imageの作成 (1/2)

- ワークスペースにアプリケーションをインストールして、[Actions]から[Create Image]を選択



The screenshot shows the AWS WorkSpaces console interface. On the left, there is a navigation menu with 'Directories', 'WorkSpaces', 'Workspace Bundles', and 'Workspace Images'. The main area is titled 'WorkSpaces' and contains a 'Launch WorkSpaces' button and an 'Actions' dropdown menu. The 'Actions' menu is open, showing options: 'Edit User', 'Invite User', 'Reboot WorkSpace', 'Rebuild WorkSpace', 'Remove WorkSpace', and 'Create Image'. The 'Create Image' option is highlighted with a red box. A red arrow points from the text '[Create Image]を選択' to the 'Create Image' option in the menu. Below the menu is a table with one row of workspace data.

Last, First	WorkSpace Bundle	Organization Name	Status
Watanabe, Genta	Value	d-9767304cde	Running

[Create Image]を選択

# Custom Imageの作成 (2/2)

- [Image Name][Description]を入力し、Custom Imageを作成

2. [Image Name]を入力

3. [Description]を入力

1. [Next]をクリック

4. [Create Image]を選択

© 2008 - 2014, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Feedback

amazon web services

# Custom Bundleの作成

- [WorkSpaces Images]タブから、Custom Bundleを作成



1. [Create Bundle]を選択



2. [Image Name]を入力



3. [Description]を入力

Bundle Name

Description

4. [Hardware Type]を入力

Hardware Type

Cancel

Create Bundle

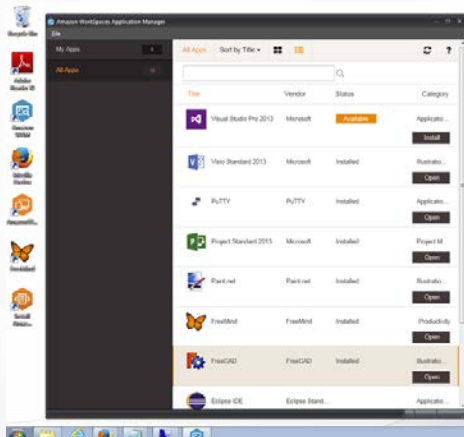
5. [Create Bundle]を選択

# イメージ作成のベストプラクティス

- Cドライブにアプリケーションをインストールするために十分な容量があること
- OSとアプリケーションの最新の更新プログラムやパッチをすべてインストールする
- 必要のないキャッシュされたデータをWorkSpaceから削除する
  - ブラウザの履歴、キャッシュファイル、ブラウザのCookieなど
- イメージを識別しやすくなるためにイメージ名に日付やバージョンなどをふくめて管理する

# Amazon WorkSpaces Application Manager

- Amazon WorkSpaces向けのアプリケーションをデプロイおよび管理
  - Windowsアプリケーションを仮想化されたコンテナにパッケージ
  - AWS Marketplace for Desktop Appsの利用



# Amazon WAMオーバービュー

 **aws marketplace**  
for Desktop Apps



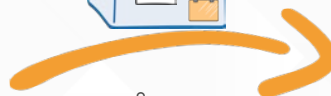
特定業務向けアプリケーション



ライセンスを所有しているアプリケーション



アプリの  
デプロイ



WorkSpaces

さまざまな種類のアプリケーションを提供

# カタログの作成

- アプリケーションのアップロード
  - 独自のアプリケーションをパッケージ化して提供
  - Admin StudioおよびAdmin Playerによりアプリケーションをコンテナにパッケージして検証
- AWS Marketplace for Desktop Appsからのサブスクリプション
  - AWS Marketplace for Desktop Appsに登録されているアプリケーションを選択して利用
  - アプリケーション開発、イラストおよびデザイン、オフィスアプリなど

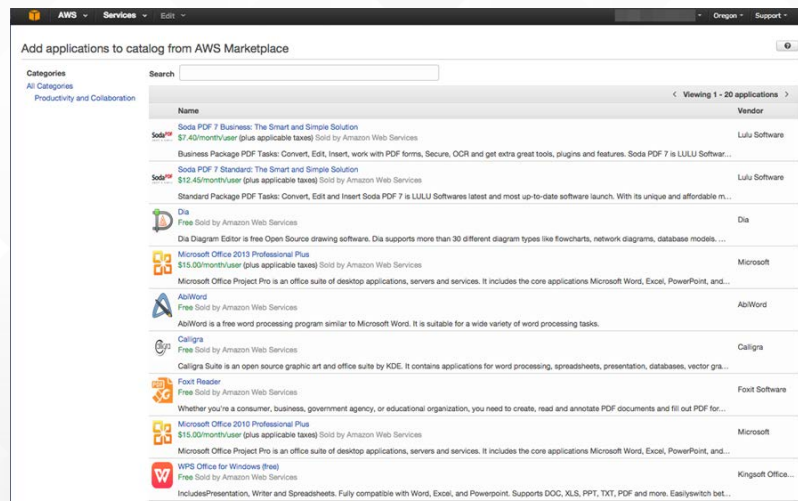


# アプリケーションのアップロード

- Amazon WorkSpacesのManagement パッケージ化したアプリケーションをアプリケーションカタログに追加
- カタログからアプリケーションを選択してユーザーまたはグループにアサイン
  - Required（必須）またはOptional（任意）が選択可能
  - Requiredを選択するとアプリケーションは自動的にインストールされる

# AWS Marketplace for Desktop Apps

- Amazon WorkSpaces用のデスクトップアプリケーションのためのAWS Marketplaceの新しいカテゴリ
  - 10以上のカテゴリのアプリケーションを選択してWorkSpacesにデプロイ
  - 月単位のサブスクリプションでデスクトップアプリケーションを利用可能



# AWS Marketplace for Desktop Appsに登録されているアプリケーション

## アプリケーションおよびWeb 開発



Microsoft Visual Studio



Python

## 生産性およびコラボレーション



Microsoft Office



Kingsoft Office



Libre Office

## セキュリティ、ストレージ & アーカイブ



Zscaler Security Cloud



**McAfee**  
An Intel Company

McAfee Anti-Virus

**Areca Backup**

Areca Backup

## ユーティリティ



Foxit PhantomPDF



TechSmith Snagit



7-Zip

## メディアおよびエンコーディング



iTunes



VLC Media Player

# ネットワーク

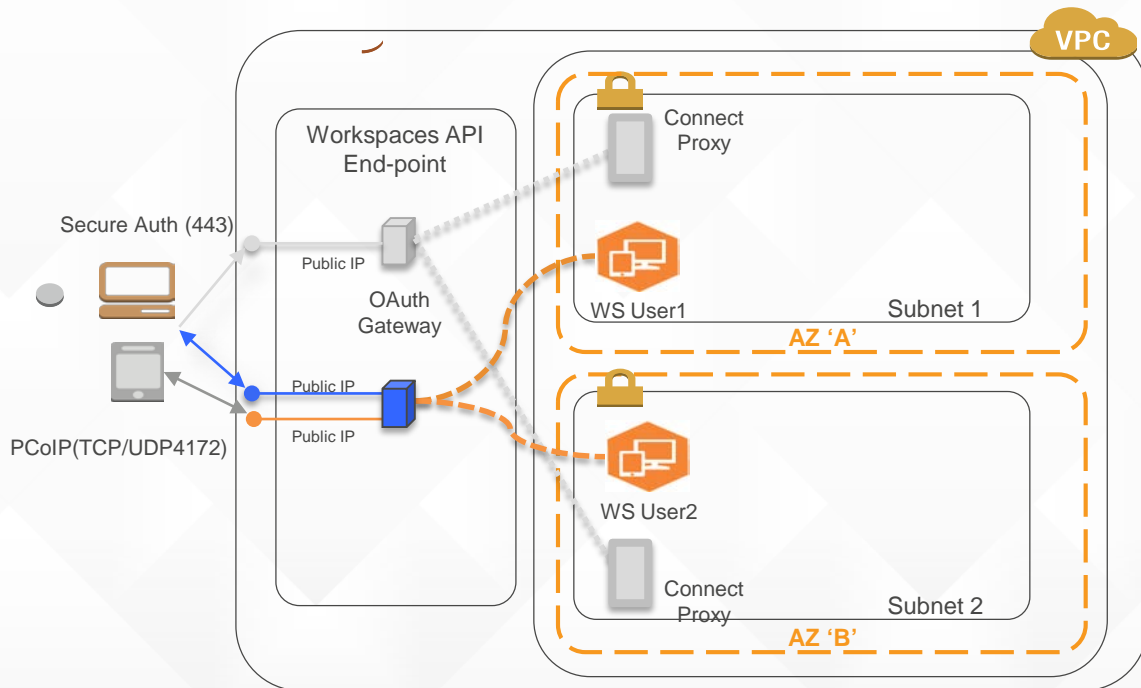
- それぞれのWorkSpaceは2つのネットワークインターフェースをもつ
  - VPCおよびインターネット接続用ネットワーク
  - WorkSpace管理用および画面転送用ネットワーク
- 管理用ネットワークでは以下のポートを利用する
  - インバウンド
    - TCP/UDP 4172
    - TCP 8200
  - アウトバウンド
    - UDP 55000

# ネットワーク要件

- AD Connectorでドメインコントローラーと疎通を行うために、以下のポートの開放が必要
  - TCP/UDP 53 - DNS
  - TCP/UDP 88 - Kerberos 認証
  - TCP 135 - RPC
  - TCP/UDP 389 - LDAP
  - TCP/UDP 445 - SMB
  - TCP 464 - Kerberos パスワードの変更/設定
  - TCP 636 - LDAPS (LDAP over TLS/SSL)
  - TCP 1024-65535 - RPC 用ダイナミックポート
  - UDP 123 - NTP
  - UDP 137-139 - Netlogon
  - UDP 464 - Kerberos パスワードの変更/設定
- DirectoryServicePortTest テストアプリケーションを利用して接続の確認が可能
  - `DirectoryServicePortTest.exe -d <domain_name> -ip <server_IP_address> -tcp "53,88,135,389,445,464,636,3268,3269,5722,9389" -udp "53,88,123,138,389,445,464"`
  - <http://docs.aws.amazon.com/directoryservice/latest/adminguide/samples/DirectoryServicePortTest.zip>

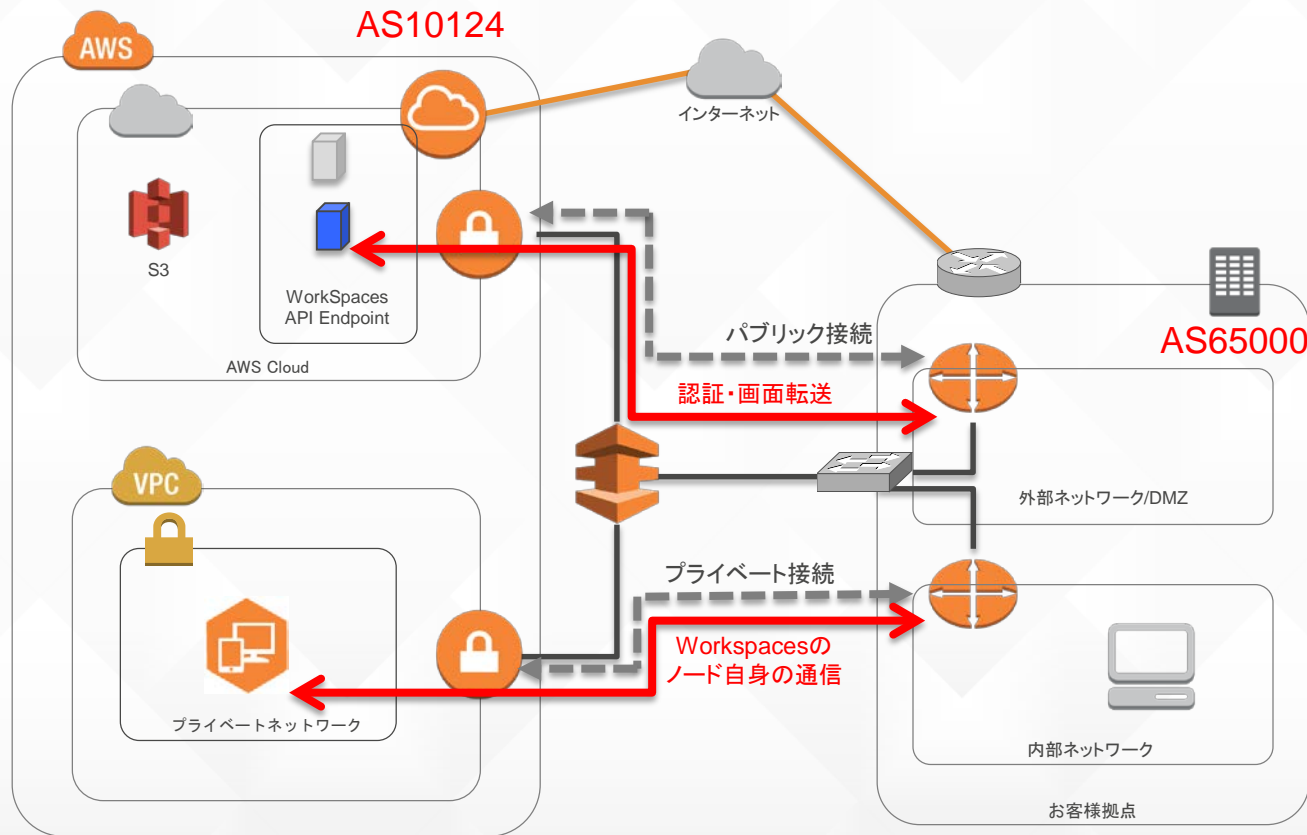
# WorkSpacesへのアクセス

- クライアントからの接続はインターネット経由で行われるため、AWSのIPアドレス範囲に対してTCP/UDP 4172をオープンする
  - <https://ip-ranges.amazonaws.com/ip-ranges.json>



# Direct Connectによる閉域網からのアクセス

- DXのパブリック接続を利用することにより画面転送も専用線経由に



# インターネットへの接続

- WorkSpacesがインターネット接続するためにはNATインスタンスもしくはPublic IPアドレスの付与が必要
  - NAT Instanceパターン
  - On-Premise Firewallパターン
  - Public IP Addressパターン
- ディレクトリ設定からインターネットアクセスを設定可能



# インターネット接続の有効化

- [Directory Details]から[Internet Access]を[Enable]に指定

WorkSpaces

- Directories
- WorkSpaces
- Bundles
- Images

## Update Directory Details

aws-cloud.amazonworkspaces.com (d-956731f3af)

- ▶ Target Domain and Organizational Unit
- ▶ Security Group
- ▼ Internet Access
- ▶ Local Administrator Setting

1. [Enable]を選択

Enable this setting to assign a public IP to WorkSpaces in this directory by default. This will allow outbound Internet access from your WorkSpaces when using an Internet Gateway in the Amazon VPC in which your WorkSpaces are located. You should leave this setting disabled if you are using a Network Address Translation (NAT) configuration for outbound Internet access from your VPC. Any changes to this setting will apply to new WorkSpaces you launch or existing WorkSpaces that you rebuild. [Learn more](#)

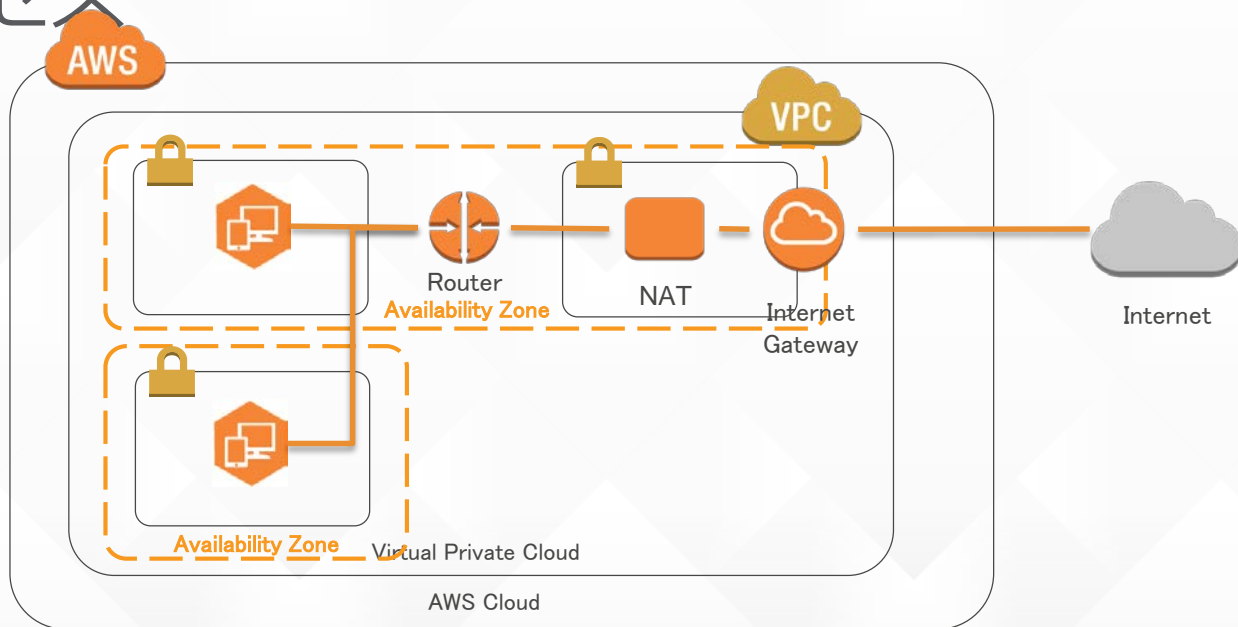
Enable  Disable

2. [Update and Exit]を選択

Cancel Update **Update and Exit**

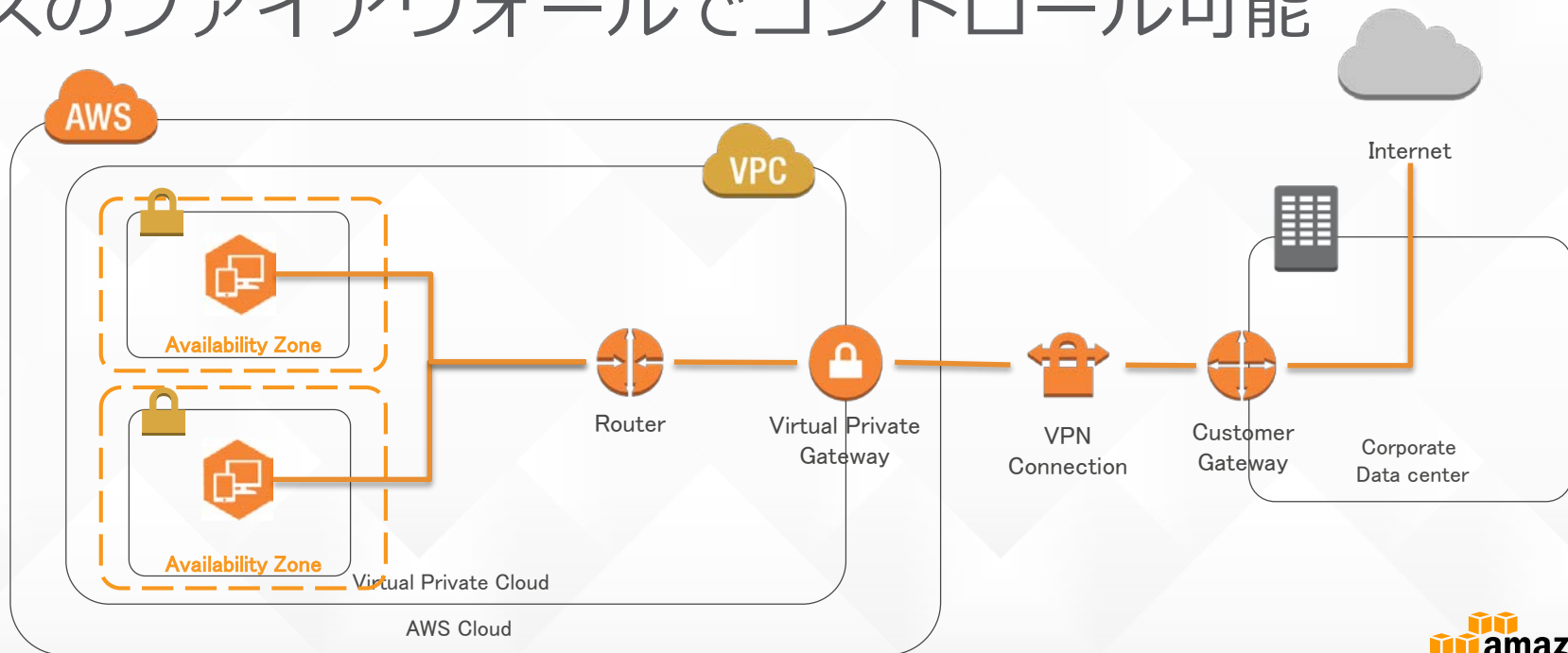
# 構成例:NAT Instanceパターン

- NATインスタンスを経由してインターネットへアクセス



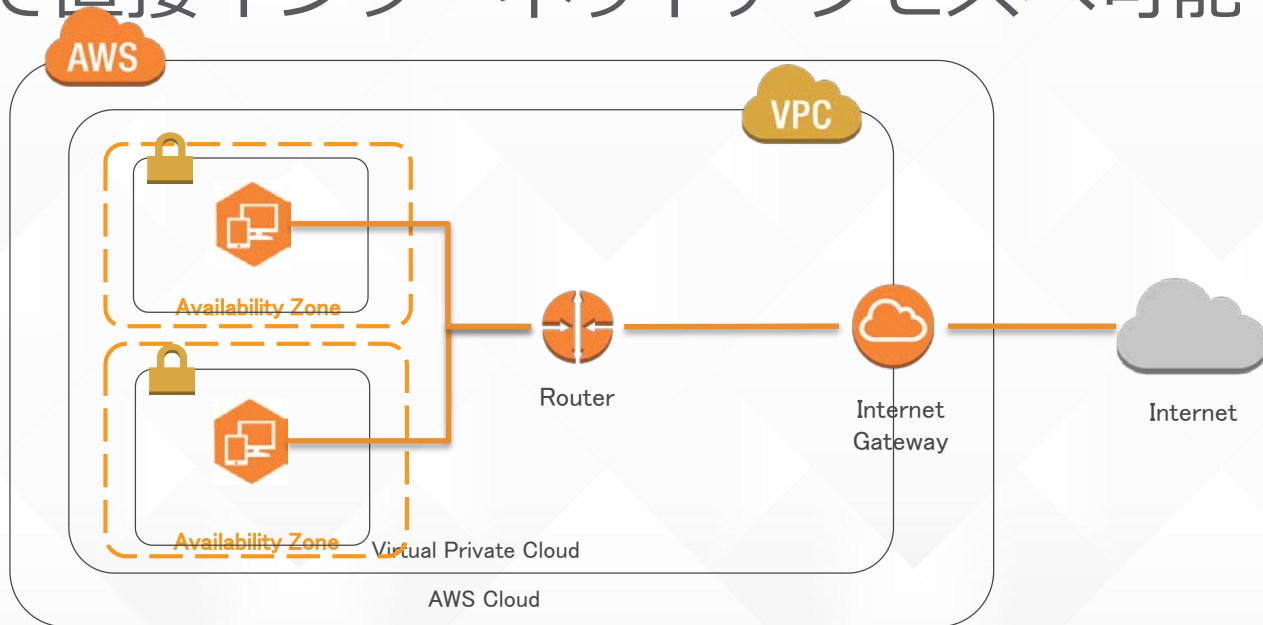
# 構成例:On-Premise Firewallパターン

- インターネットへの接続ポリシーをオンプレミスのファイアウォールでコントロール可能



# 構成例:Public IP Addressパターン

- ワークスペースにPublic IPアドレスを付与することで直接インターネットアクセスへ可能



# ローカルプリンターへの印刷

- ワークスペースからWindowsまたはMacに接続されているローカルおよびネットワークプリンターに印刷することが可能
  - ローカルプリンターは自動的に認識される(Local - <workspace username>.<directory name>.<client computer name>)
  - Windows Server 2008 R2用のドライバをインストールする必要がある
- その他の印刷方法
  - Active Directoryに登録されたネットワークプリンタ
  - Cordado ThinPrint/Google Cloud Printなどのクラウドプリント

# グループポリシーによる制御

- グループポリシー管理テンプレートをインストールすることによりAmazon WorkSpaces固有のポリシー設定を変更可能
  - C:\Program Files (x86)\Teradici\PCoIP Agent\configuration\pcoip.adm
- 以下のような項目がグループポリシーから制御可能
  - ローカルプリンターのサポート
  - クリップボードのリダイレクト

# WorkSpaces API

- AWS SDKやCLI、PowerShellからWorkSpacesの作成・表示やメンテナンスが実行可能
  - オペレーションの自動化
  - ディザスタリカバリイメージの展開
- AWS CloudTrailによるロギングをサポート

```
[root@ip-10-0-1-10 ~]# aws workspaces create-workspaces --workspaces DirectoryId=d-926735ab8f,BundleId=wsb-jnyscd6pb,UserName=olivia
{
  "PendingRequests": [
    {
      "UserName": "olivia",
      "DirectoryId": "d-926735ab8f",
      "State": "PENDING",
      "WorkspaceId": "ws-4w79yig1x",
      "BundleId": "wsb-jnyscd6pb"
    }
  ],
  "FailedRequests": []
}
```



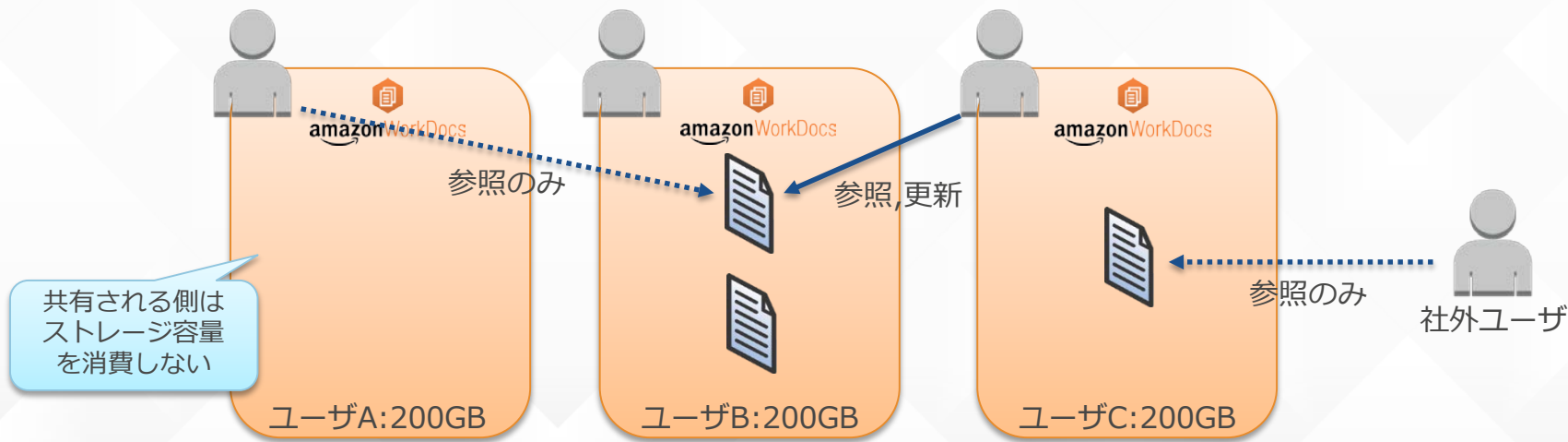
# Amazon WorkDocs Deep Dive





# Amazon WorkDocs - センtralハブ

- ファイルやフォルダ単位で他ユーザに対してファイルの読み取り/書き込み権限を付与することでファイル共有が可能
- 社外ユーザにも読み取りを許可することもできる（ポリシーで社外共有を不許可にすることも可能）



# アクセス権の設定

- フォルダおよびファイルのアクセス許可はロールに基づいて付与される
  - 所有者 - フォルダまたはファイルの所有者
  - 共同編集者 - フォルダが共有され、フォルダへのアクセスは制限されていないユーザー
  - 閲覧者 - フォルダが共有されたが、フォルダへのアクセスが制限されている（表示のみ）ユーザー
  - 匿名の閲覧者 - 外部の表示リンクを介して共有されたファイルを表示できる、組織外部の登録されていないユーザー

# 組織外のユーザーに対するドキュメントの共有

- 「匿名の閲覧者」ロールによって組織外のユーザーに対してフォルダまたはファイルの共有が可能
  - 組織外への共有ポリシー
    - ユーザーはドキュメント参照リンクを誰にでも送信できる
    - ユーザーはドキュメント参照リンクを指定されたドメインのみに送信できる
  - 新規ユーザー招待のポリシー
    - 管理者のみが新しいユーザーを招待できる

### 組織外への共有ポリシー

ドキュメント参照リンクの送信を許可する相手

対象のドメイン

ユーザーはドキュメント参照リンクを誰にでも送信できる。

ユーザーはドキュメント参照リンクを指定されたドメインのみに送信できる。

ユーザーは組織外のユーザーにドキュメント参照リンクを送信できない。

example.com x

キャンセル 変更の保存

# 例：共有フォルダにあるファイルのアクセス許可

アクセス許可	フォルダ所有者	ファイル所有者	フォルダ共同編集者	フォルダ閲覧者	匿名の閲覧者
表示	X	X	X	X	X
共有の表示	X	X	X	X	X
ダウンロード	X	X	X	X	
注釈	X	X	X		
注釈の表示	X	X	X		
アクティビティの表示	X	X	X		
バージョンの表示	X	X	X		
アップロード	X	X	X		
削除	X	X	X		
ダウンロードの禁止	X	X			
共有	X	X			
共有の取り消し	X	X			

# CloudTrailによるAPIコールの記録

- 詳細なアクセスログを記録したい場合はCloudTrailを利用する
- APIコール単位でアクセスが記録されるため、詳細な監査が可能



AWS CloudTrail



JSON形式のログ

```
{
  "eventVersion": "1.02",
  "userIdentity": {
    "principalId": "S-1-5-21-3312768711-3070474699-4104396599-1120\u002d90673679db",
    "accountId": "762789334655",
    "userName": "fintaro",
    "type": "Directory"
  },
  "eventTime": "2015-02-16T11:54:01Z",
  "eventSource": "WorkDocs.amazonaws.com",
  "eventName": "GetFolder",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "72.21.196.64",
  "userAgent": "Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko",
  "requestParameters": {
    "Attributes": null,
    "AuthenticationToken": "\u003c**redacted**\u003e",
    "FolderId": "022f3fed81a53b0a45ab3faa61aa15cf9a5888e978749754833c9ef0f8fc1536",
    "Marker": null,
    "MaxItems": null,
    "Order": null,
    "SortBy": null
  },
  "responseElements": null
}
```



# Amazon WorkMail Deep Dive



# Amazon WorkMail- マネージド&セキュア



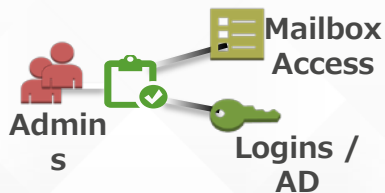
## お客様自身の管理するキーでの暗号化

Amazon WorkMailはAWS Key Management Serviceとの統合によりお客様自身の管理するキーでのデータを暗号化



## リージョンによるデータのコントロール

メールボックスのデータが格納されるリージョンが選択可能なため低レイテンシーと地域ごとのコンプライアンス基準に適合




## シンプルな利用

Amazon WorkMailは企業内の電子メールインフラ管理を容易にし、既存のディレクトリサービスとセキュアに統合

# AWS Key Management Serviceによる鍵管理

- KMSは保存されたのデータ（メッセージ、連絡先、添付とメタデータ）の暗号化に利用される
  - Quick setupではデフォルトのキーが作成され利用される
  - Custom setupでは自分で作成したキーを選択可能

Filter: US East (N. Virginia) ▼ ⓘ		Search		Sho
<input type="checkbox"/>	Alias ⇅	Key ID ⇅	Status ⇅	Creation Date ⇅
	aws/workmail	1eb66268-49f0-449a-9b04-baa7c83...	Enabled	2015-02-26 17:44 UTC+0900



# Amazon Simple Email Serviceとの統合

- WorkMailはアウトバウンドの電子メール送信およびドメイン検証の仕組みにSESを利用
  - WorkMailのために構成したメールアドレスはSESコンソールからも確認可能



# 独自ドメインの設定 (1/2)

- WorkMailでは独自ドメインの設定および利用が可能
  - 組織 (Organization) の作成後にドメインを追加
  - ドメイン所有権の検証のためRoute 53などのDNSホスティングプロバイダにTXTレコードを追加

## Step 1: Verify domain ownership

Before you can use your domain with Amazon WorkMail, we need to verify the domain ownership.  
Add the following record to your DNS hosting provider:

Record type	Hostname	Value
TXT	_amazonses.aws-cloud.info.	"MCM2PzQ/RV4zQgkvLvdXuFWySDaFLwNA0xlwKTmbiC0="

*Note: If you delete the TXT record from your DNS hosting provider, this domain will not be able to send and receive emails any longer.*

[Learn More](#)

# 独自ドメインの設定 (2/2)

- 以下のレコードをDNSに追加し、設定が完了するまで最大72時間まつ
  - メール受信のためのMXレコード
  - Outlookおよびモバイルクライアントからの自動検出のためのCNAMEレコード
  - DKIM署名のためのCNAMEレコード

## Step 2: Finalize domain setup

To switch your domain completely to Amazon WorkMail, add the following DNS records to your DNS hosting provider.

If your domain already has email addresses, be careful when you change MX records. To avoid email service disruption, make sure that all your user accounts and distribution lists are added.

Record type	Hostname	Value
MX	aws-cloud.info.	10 inbound-smtp.us-east-1.amazonaws.com.
CNAME	autodiscover.aws-cloud.info.	autodiscover.mail.us-east-1.awsapps.com.
CNAME	yfm4hglwfgqiblsbggw6no63n5qawmz6._domainkey.aws-cloud.info.	yfm4hglwfgqiblsbggw6no63n5qawmz6.dkim.amazonses.com.
CNAME	5vrvfz4da52mocz2wdcp4se2ryjm34e._domainkey.aws-cloud.info.	5vrvfz4da52mocz2wdcp4se2ryjm34e.dkim.amazonses.com.
CNAME	lyxp6amrthvl2hoprja7qdlc3n46ckzv._domainkey.aws-cloud.info.	lyxp6amrthvl2hoprja7qdlc3n46ckzv.dkim.amazonses.com.

Remove any existing MX records before adding the new MX record. It can take up to 72 hours before all DNS records are propagated.

# DKIMによるメール署名の有効化

- Domain Keys Identified Mail (DKIM) によるメール署名が利用可能
  - 独自ドメインを設定した場合はドメイン検証後にSESコンソールから手動でDKIMを有効化

## ▼ DKIM

DKIM settings for your domain have been generated. The information below must be added to your domain's DNS records. How you update the DNS settings depends on who provides your DNS service: if your DNS service is provided by a domain name registrar, please contact that registrar to update your DNS records. [Learn more](#)

DKIM: **enabled** (disable)

To enable DKIM signing for your domain, the records below must be entered in your DNS settings. AWS will automatically detect the presence of these records, and allow DKIM signing at that time. Note that verification of these settings may take up to 72 hours.

Name	Type	Value
yfm4hglwfgqiblsbggw6no63n5qawmz6._domainkey.aws-cloud.info	CNAME	yfm4hglwfgqiblsbggw6no63n5qawmz6.dkim.amazonses.com
5vrwfz4da52moczd2wdcp4se2ryjm34e._domainkey.aws-cloud.info	CNAME	5vrwfz4da52moczd2wdcp4se2ryjm34e.dkim.amazonses.com
lyxp6amrfhl2hoprja7qdlc3n46ckzv._domainkey.aws-cloud.info	CNAME	lyxp6amrfhl2hoprja7qdlc3n46ckzv.dkim.amazonses.com

[Download Record Set as CSV >>](#)

[View your Route 53 Record Sets >>](#)

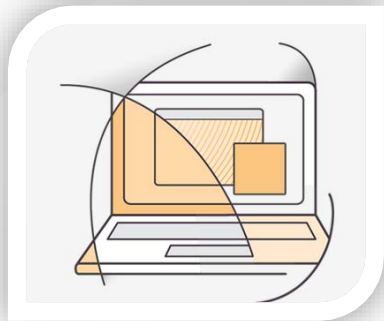
# まとめ

- AWSのエンタープライズアプリケーションは仮想デスクトップ、エンタープライズストレージおよび電子メール・カレンダーなどの機能をマネージドサービスとして提供
- AWS Directory Serviceはエンタープライズアプリケーションの認証基盤
- Amazon WorkSpaces、WorkDocsおよびWorkMailはさまざまなサービスとも連携して動作するためひとつとおり把握しておくことが重要

# 参考資料

- Amazon WorkSpaces 管理者ガイド
  - [http://docs.aws.amazon.com/ja\\_jp/workspaces/latest/adminguide/](http://docs.aws.amazon.com/ja_jp/workspaces/latest/adminguide/)
- Amazon WorkDocs Documentation
  - <http://aws.amazon.com/jp/documentation/workdocs/>
- Amazon WorkMail Documentation
  - <http://aws.amazon.com/jp/documentation/workmail/>
- AWS Directory Service Documentation
  - <http://aws.amazon.com/jp/documentation/directory-service/>

# AWSトレーニング @ AWS Summit Tokyo

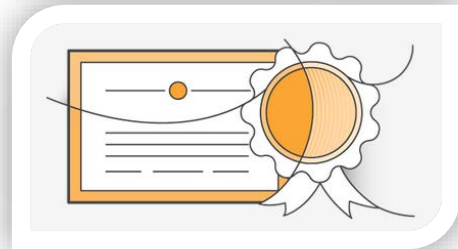


## セルフペースラボ : @パミール1F 瑞光

AWS クラウドに実際に触れてみませんか？  
ご自分の AWS アカウントをおつくりいただけなくても、  
AWS クラウドを体験いただけます。

## AWS認定試験（有償） : @ パミール1F 黄玉

特設認定試験会場を AWS Summit Tokyo 2015 会場に開設  
Devopsエンジニア-プロフェッショナル認定試験を先行受験いただけます。



## AWS認定資格者取得専用ラウンジ : @ パミール1F 青玉

他の AWS 認定資格をお持ちの方とのネットワーキングにぜひラウンジをご活用  
ください。  
お席や充電器、お飲物などを用意し、皆様をお待ちしております。



Thank You