

Amazon WorkDocs Amazon WorkMail

2016年2月24日

AWS Black Belt Tech Webinar 2016
アマゾンウェブサービスジャパン株式会社
ソリューションアーキテクト 小林正人

アジェンダ

- Amazon WorkDocs
 - WorkDocsの概要とユースケース
 - エンドユーザ向け機能
 - 管理者向け機能
- Amazon WorkMail
 - アップデート
 - WorkMailの概要
 - エンドユーザによる利用方法
 - 管理者による環境構築
- まとめ



アジェンダ

- Amazon WorkDocs
 - WorkDocsの概要とユースケース
 - エンドユーザ向け機能
 - 管理者向け機能
- Amazon WorkMail
 - アップデート
 - WorkMailの概要
 - エンドユーザによる利用方法
 - 管理者による環境構築
- まとめ



Amazon WorkDocsの概要

- **ファイルの共有：**
他のユーザーとドキュメントやスプレッドシート、プレゼンテーション、Webページ、画像、PDF、テキストファイルといった各種ファイルを共有することが可能
- **マルチデバイスからのアクセス：**
PC、iPad、Kindle Fire、Androidタブレットなどのお好みのデバイスから、いつでも、どこにいても、Amazon WorkDocsに保管されたデータにアクセス可能
- **フィードバック：**
ユーザーは他ユーザーのフィードバックをリクエストし、管理することが可能。一方、フィードバックする側のユーザーは、ドキュメントやファイル中のあらゆる語句や文章、段落、範囲をハイライトし、詳細なフィードバックを残すことが可能

Amazon WorkDocsの概要

- **安全：**

WorkDocsに保管されたデータを暗号化。また、管理者はユーザーの共有アクセス権を管理するためのポリシーを設定可能。AWSリージョンを選択することでデータをどこに保存するかを自由に決定する事が出来、ファイルやユーザーのアクティビティを追跡するために監査ログを閲覧することが可能

- **コーポレートディレクトリとの統合：**

既存のActive Directoryと統合することが可能。

- **低コスト：**

1人あたり200GBの容量を月額7ドルで利用可能。1GBあたり月額0.033ドルの追加料金でストレージの増量にも対応。WorkSpacesユーザは50GBまで無料でWorkDocsを利用できる（月額2ドルで200GBにアップグレード）

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

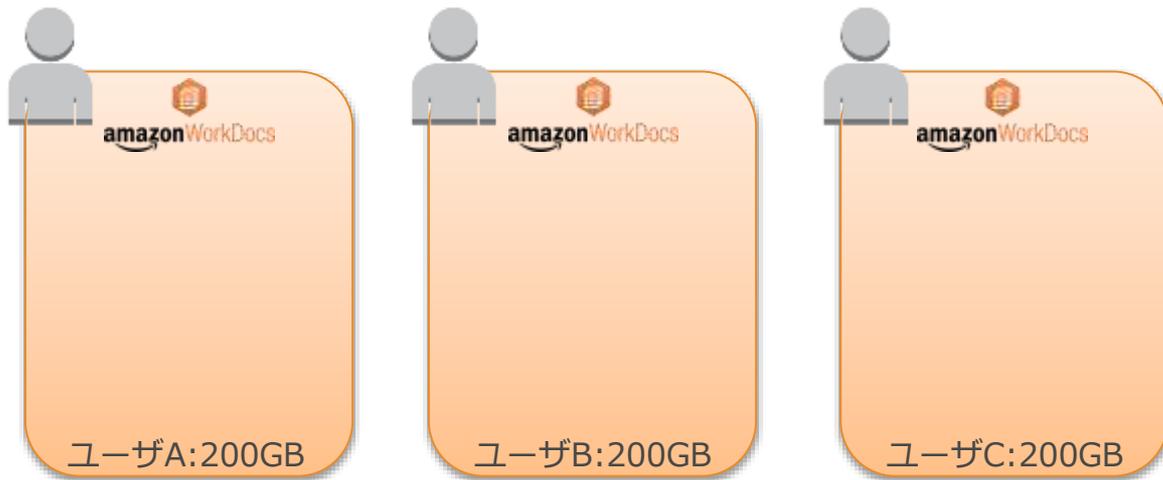
EC2上に構築

- 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
(WorkDocs)

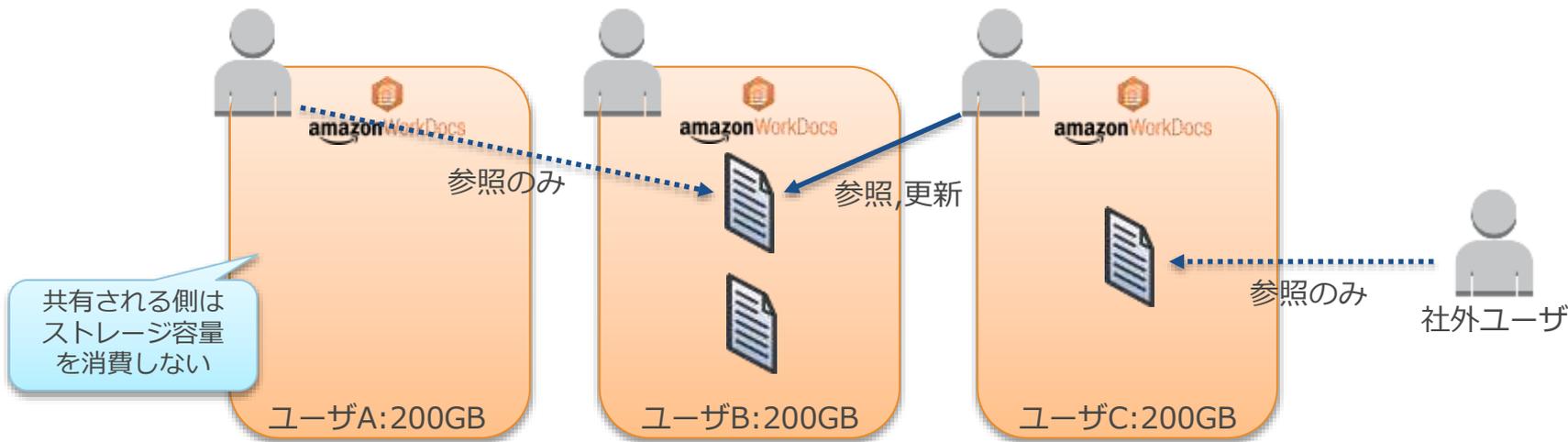
WorkDocsによるファイルの保存

- WorkDocsではユーザー個人毎に独立したデータ保存領域が割り当てられる



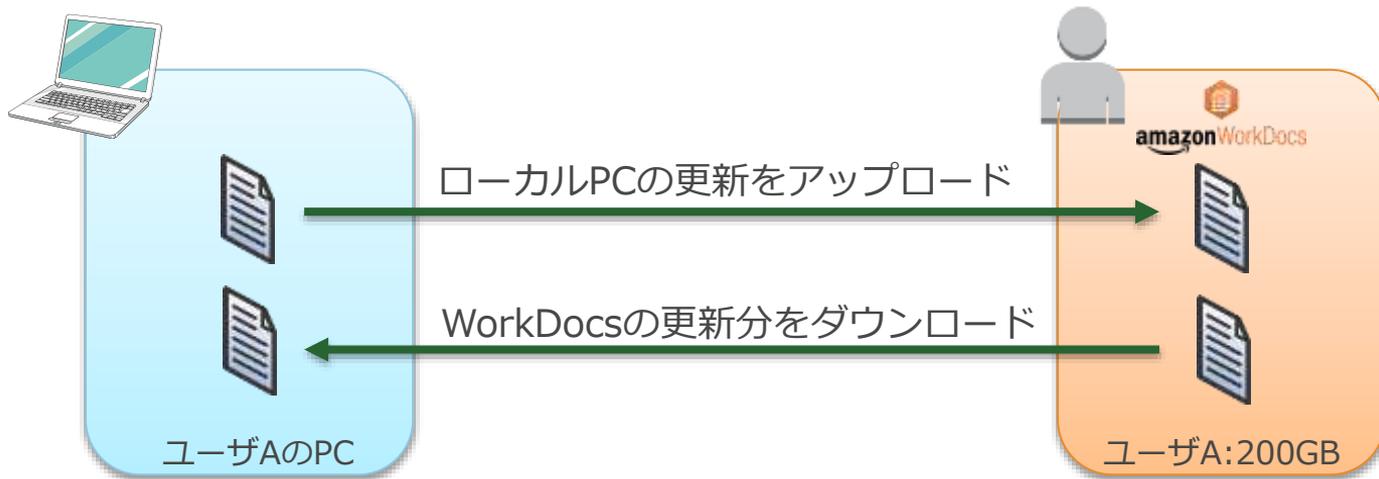
ユースケース① ファイル共有ストレージとして

- ファイルやフォルダ単位で他ユーザやグループ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）



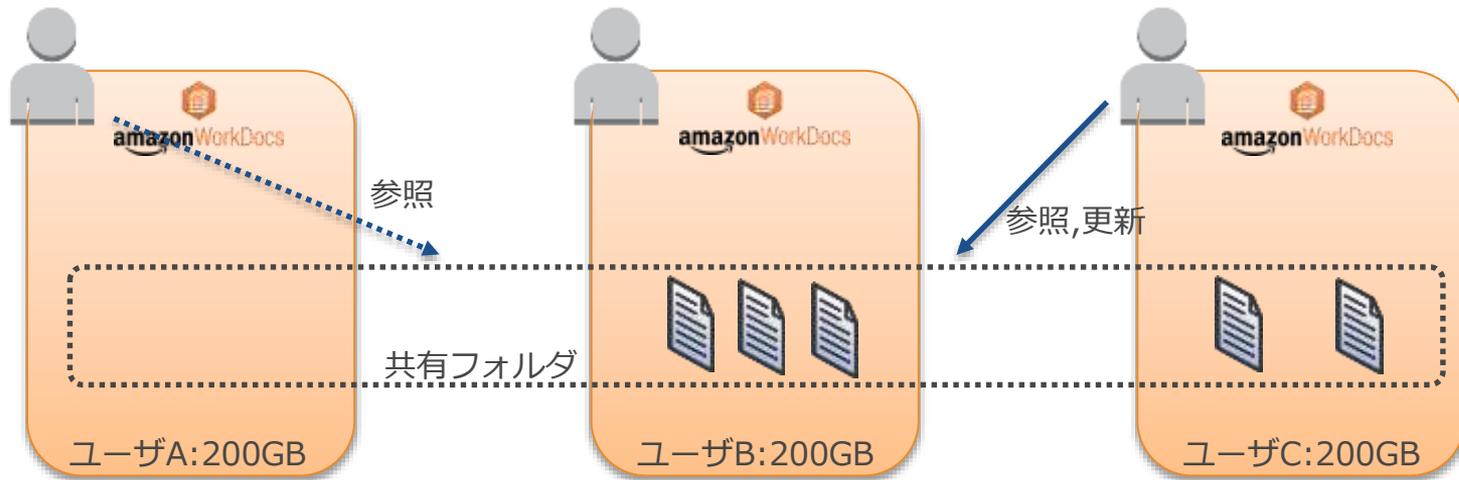
ユースケース② 個人用バックアップ領域として

- WorkDocs Syncクライアントを利用すると、ローカルPCのフォルダを自動的にWorkDocsに同期できる
- 個人のドキュメント格納フォルダを同期対象として指定すると、自動的にクラウドへのデータバックアップが実現される



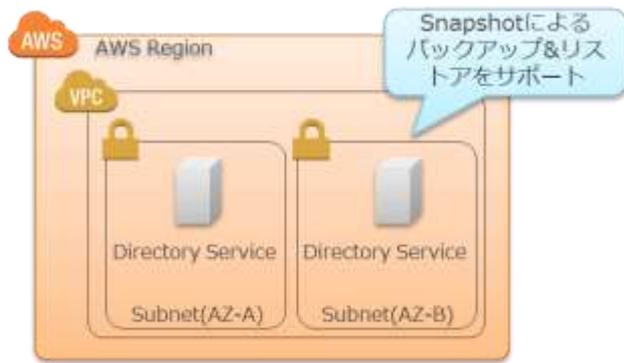
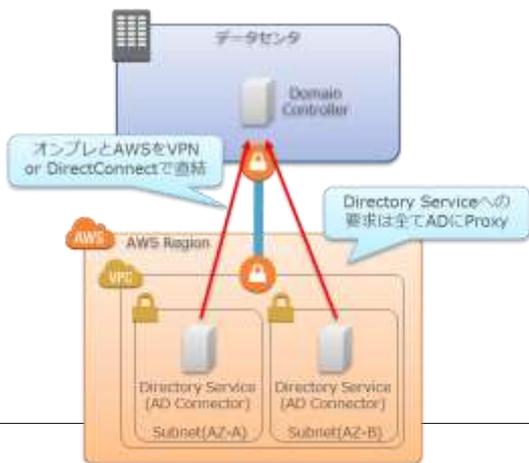
ユースケース③ ファイルサーバライクな使い方

- チーム内や部署内など、共同作業をしたい人に対してアクセス権を付与したフォルダを作成し、ドキュメントを格納する
- ユーザやグループによっては権限を読み取り専用にすることも可能。ファイルサーバに近い感覚での運用ができる



ユーザ認証

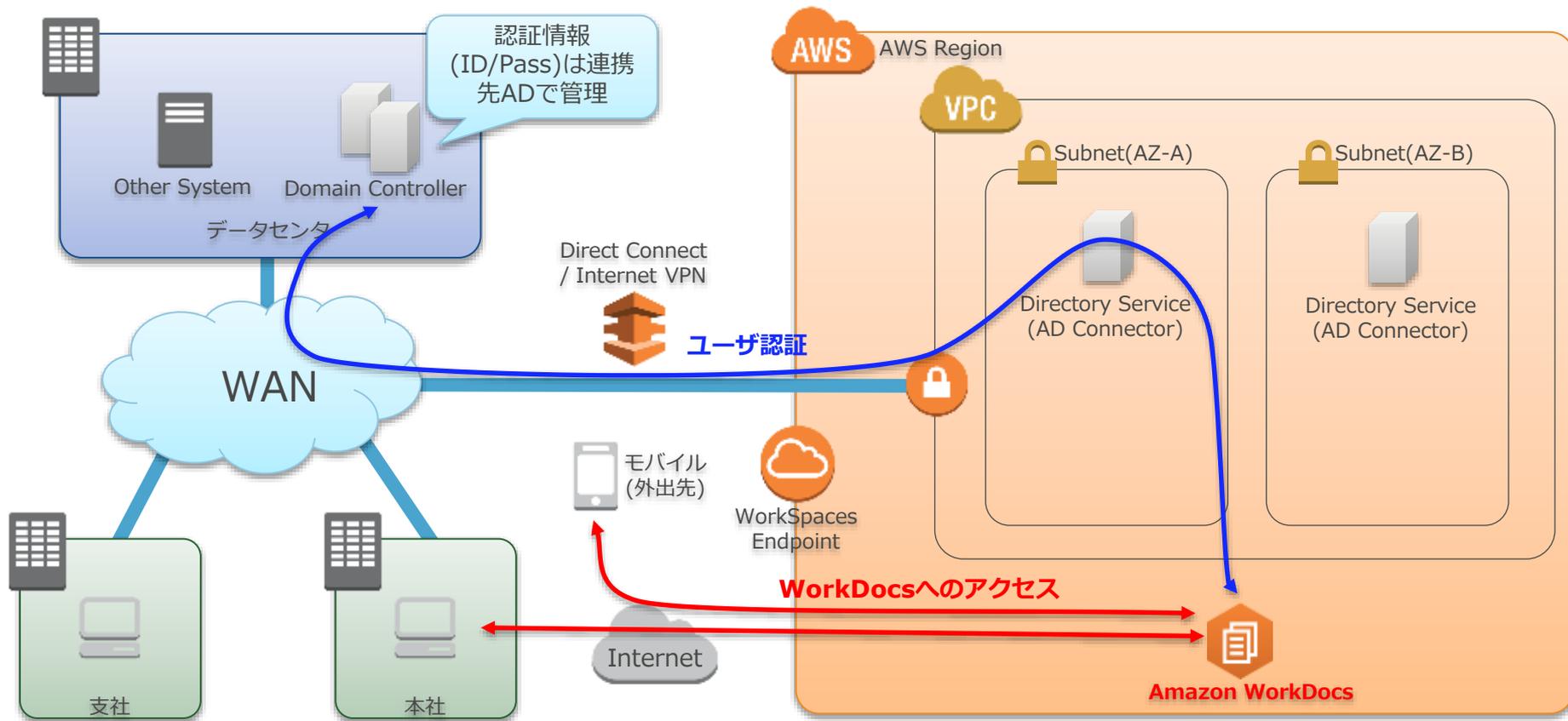
- ユーザ認証にはAWS Directory Serviceを利用する。既設のActive Directoryとの連携以外に、独立したドメインを立てることも可能
- AD ConnectorではRADIUSサーバ連携による多要素認証(MFA)をサポート
 - AD Connector
 - 独立ドメイン(Directory Service)



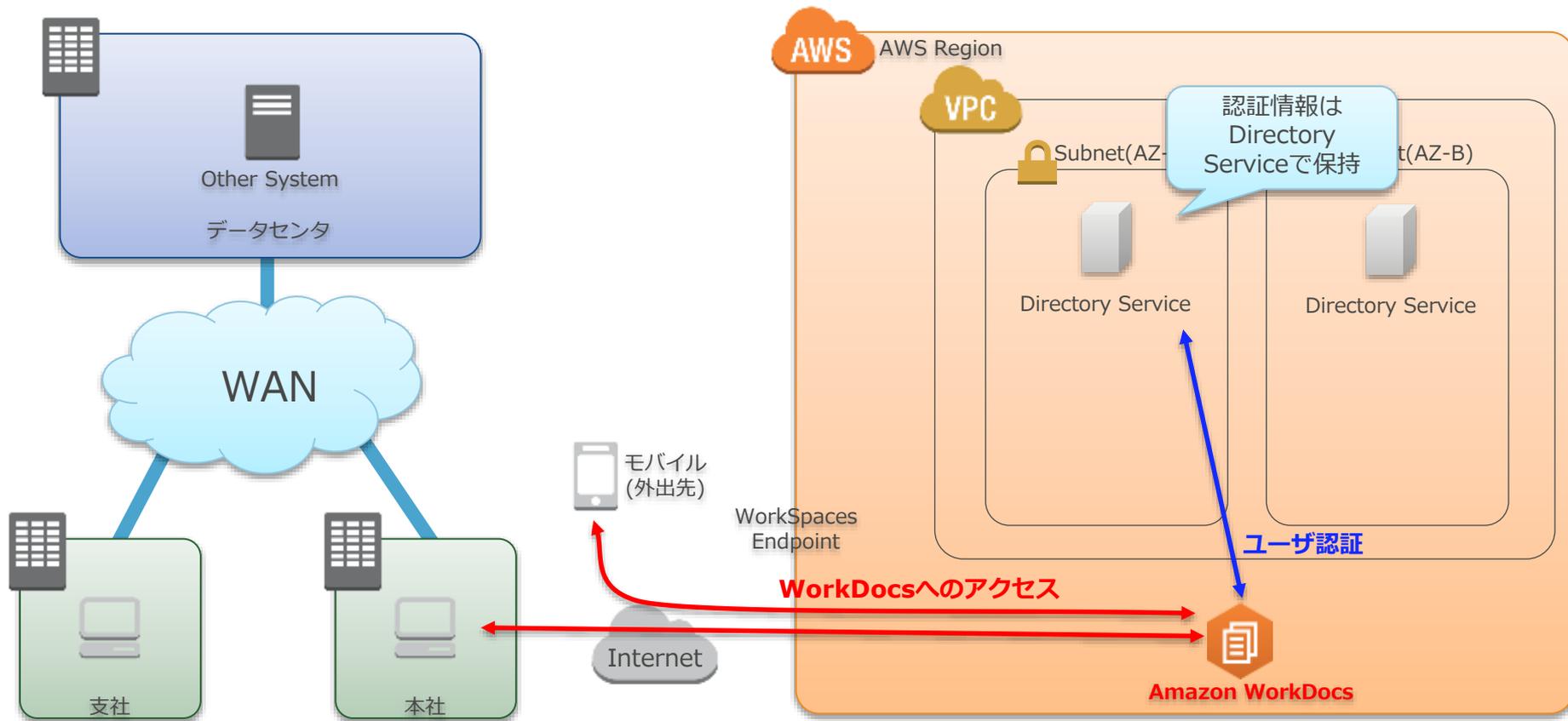
(参考)AWS Directory Serviceの概要

- フルマネージド型のディレクトリサービス
 - 管理運用の手間がかからず即座にディレクトリを利用できる
- 2種類の動作モードをサポート
 - 既存のActive Directoryと連携する
 - AD Connectorによって実現。AD Connectorが既存のActive Directoryに対する認証プロキシとして動作する。プロキシなのでAD Connectorに情報は残らない
 - 独立したディレクトリを構築する
 - Simple AD : Samba4によるAD互換の独立したディレクトリとして動作する
 - Microsoft AD : Windows 2012R2によるActive Directory
 - ※いずれもユーザやグループの管理にはWindowsの管理ツールを利用する
- 詳細情報はこちらを参照
 - <http://aws.amazon.com/jp/directoryservice/>

構成例(AD連携あり)



構成例(AD連携なし)



アジェンダ

- Amazon WorkDocs
 - WorkDocsの概要とユースケース
 - エンドユーザ向け機能
 - 管理者向け機能
- Amazon WorkMail
 - アップデート
 - WorkMailの概要
 - エンドユーザによる利用方法
 - 管理者による環境構築
- まとめ



WebUIによるWorkDocsへのアクセス

- ウェブブラウザさえあればどこからでもアクセス可能
 - [https://\(alias\).awsapps.com/workdocs](https://(alias).awsapps.com/workdocs)がエンドポイントとなる
 - (alias)の部分は他ユーザと重複しない範囲で自由に設定可
- ドラッグアンドドロップによるアップロードをサポート



ドラッグ&ドロップで
アップロード

※参考 : WebUIの対応ブラウザ

http://docs.aws.amazon.com/ja_jp/workdocs/latest/userguide/web_client_help.html

ドキュメントのプレビュー

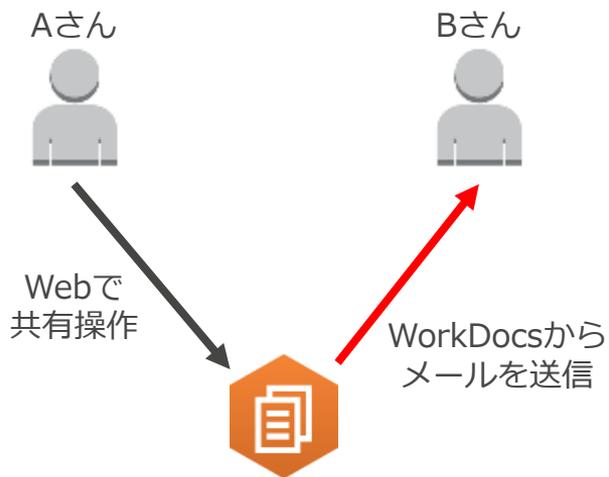
- 主要な形式のファイルについてはWebUIで直接内容を閲覧できる
- クライアントへのアプリケーションインストールが不要なので、PCでもモバイルデバイスでも同じようにドキュメントをチェック可能



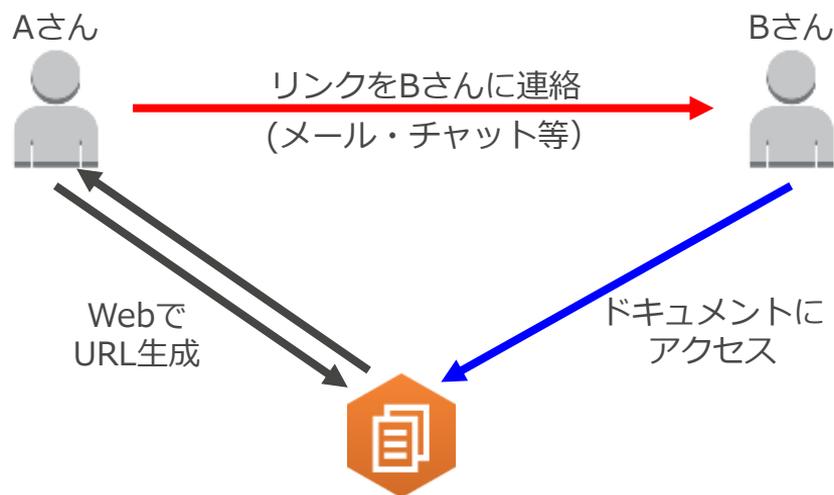
ドキュメントの共有

- 他のユーザに対するドキュメント共有は2種類の方式を提供
 - WorkDocsの機能で直接共有を行う方法
 - ドキュメントのリンクをWorkDocsで生成し、何らかの方法で共有相手に通知する方法

WorkDocsで直接共有



リンクを生成して共有

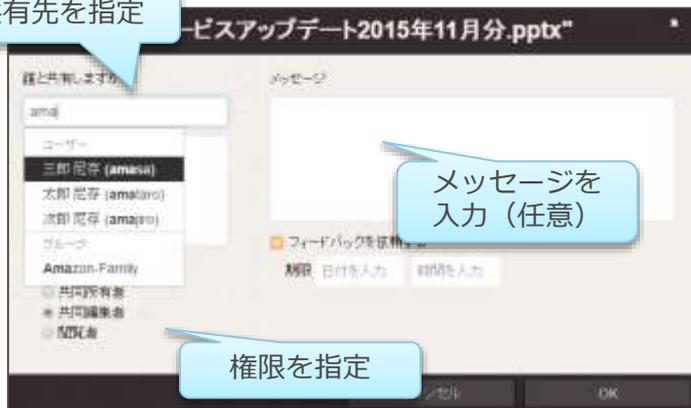


WorkDocsで直接共有する

- WebUIで共有するユーザまたはグループを指定
- 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、共同所有者）を設定。権限を付与されるとメールで通知される



共有先を指定



メッセージを入力 (任意)

権限を指定



表示をクリックするとドキュメントにアクセス

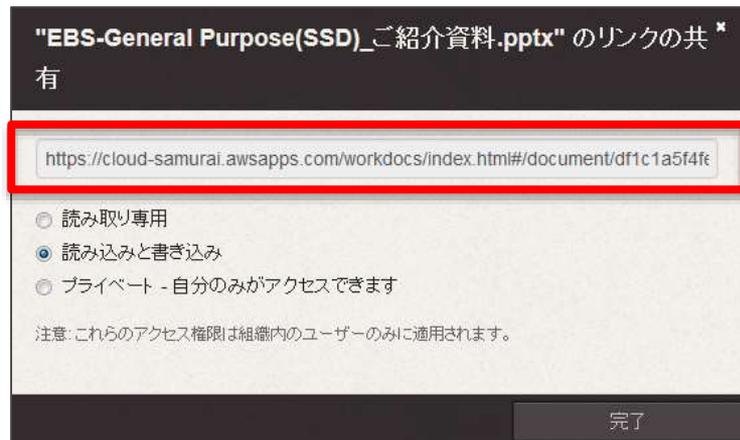
WorkDocsで直接共有する

- 共有先としてメールアドレスを入力すると、ドメインユーザ以外の人に対してもファイルを共有できる
- 管理者の設定で共有先メールアドレスのドメインを制限したり、社外への共有を禁止することも可能（後述）



リンクを生成して共有する

- WebUIの画面から生成できるリンクで共有することも可能
- リンクをチャットやメールなどで共有相手に連絡し、ドキュメントにアクセスをしてもらう



リンクを生成して共有する場合の認証

- 共有された側がリンクをクリックすると認証を要求され、OKであればドキュメントにアクセスできる
- WorkDocsのアカウントを持っていないユーザはアクセス不可

<https://abcdefg.awsapps.com/workdocs/index.html#/document/f9e66df1ecbd4cb69ac783eddab17d66c066b8f18887664dfdd0e45a63dc1c49>

A screenshot of the Amazon WorkDocs login page. At the top is the Amazon WorkDocs logo. Below it, there is a message in Japanese: "次の情報を使用してログインしてください。cloud-saml-provider@amazon.com" (Please log in using the following information: cloud-saml-provider@amazon.com). There are two input fields: "ユーザー名" (Username) and "パスワード" (Password). Below the password field is a yellow "サインイン" (Sign In) button. At the bottom, there is a link for "パスワードを忘れた場合" (Forgot your password?).

共有ドキュメントに対するアクセス権のまとめ

- WorkDocsアカウントの有無と共有のやり方によって、社外ユーザーのアクセス可否が異なる
- WorkDocsアカウントのないユーザーへの共有が必要な場合は注意

	WorkDocsアカウント があるユーザー	WorkDocsアカウント がないユーザー
WorkDocsから 直接共有した場合	アクセス可能	アクセス可能 ※管理者設定により共有自体が できない場合がある
リンクを生成し 共有した場合	アクセス可能	アクセス不可

※参考：アクセス権の詳細について

http://docs.aws.amazon.com/ja_jp/workdocs/latest/adminguide/permissions.html

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
- フィードバックをメールによる通知できる



ドキュメントの世代管理

- 同名でファイルをアップすることで自動的に世代管理が行われる
- 旧バージョンのファイルはWebUIからプレビューを行ったり、ファイルをダウンロードすることができる

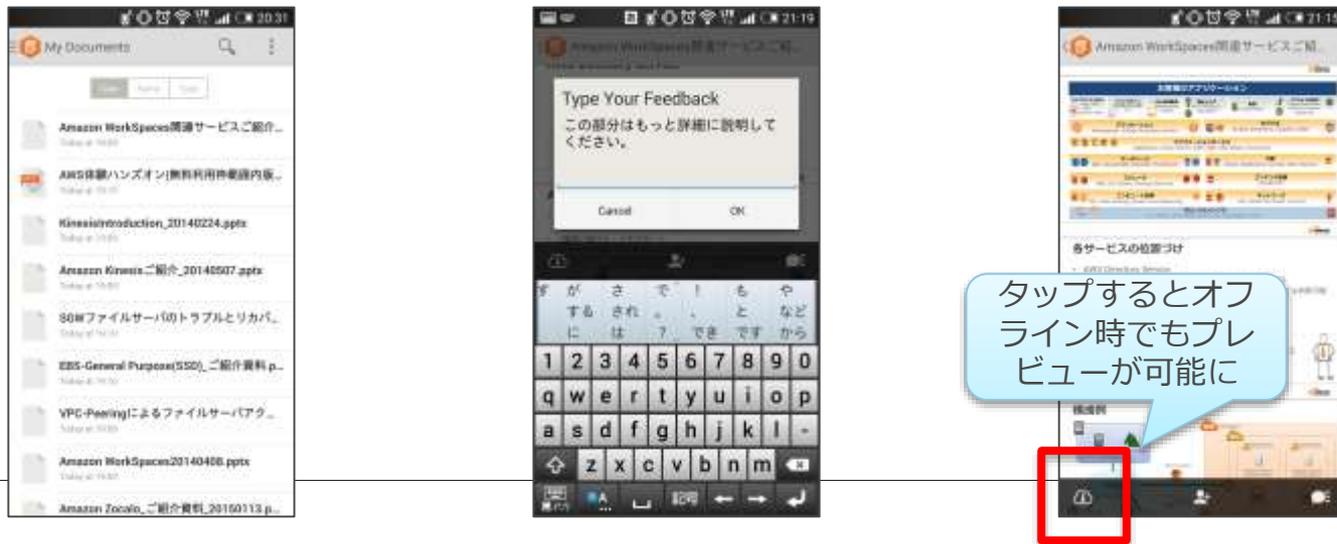
バージョン 3 / 3

EBSの3つのボリュームタイプ (更新版)

Volume Type	General Purpose(SSD)	Provisioned IOPS(SSD)	Magnetic
ユースケース	<ul style="list-style-type: none">起動ボリューム仮想デスクトップ環境用のディスク開発およびテスト環境用のディスク中小規模のデータベース	<ul style="list-style-type: none">3000IOPSよりも高いI/Oパフォーマンスを要求するミッションクリティカルなアプリケーション大規模なデータベース各種NoSQL各種RDB	<ul style="list-style-type: none">アクセス頻度の低いデータコストを最重視する場合
ボリュームサイズ	1GBから16TBまで	4GBから16TBまで	1GBから1TiBまで
IOPS	<ul style="list-style-type: none">1GBあたり310IOPSのベースパフォーマンス。最大値は10,000IOPS1,000GB以下のボリュームでは、3,000IOPSまでバーストが可能1,000GB以上のボリュームではバーストの概念はなく、常にベースパフォーマンスを発揮する	<ul style="list-style-type: none">プロビジョニングしたIOPS値のパフォーマンスを発揮する最大IOPSは20,000IOPS容量とIOPS値の比率に制限があり、容量の30倍のIOPS値が上限	平均100IOPS。数百IOPSまでバースト可能。
スレープット	<ul style="list-style-type: none">170GB未満: 128MB/s170GB以上: 128MB/s~160MB/s214GB以上: 160MB/s	320MB/s	40~90MB/s
料金 (東京リージョン)	1GBあたり1ヶ月0.12ドル	1GBあたり1ヶ月0.142ドル プロビジョニングしたIOPS値に応じて110IOPSあたり1ヶ月0.114ドル	1GBあたり1ヶ月0.08ドル 100万I/Oリクエストあたり0.08ドル

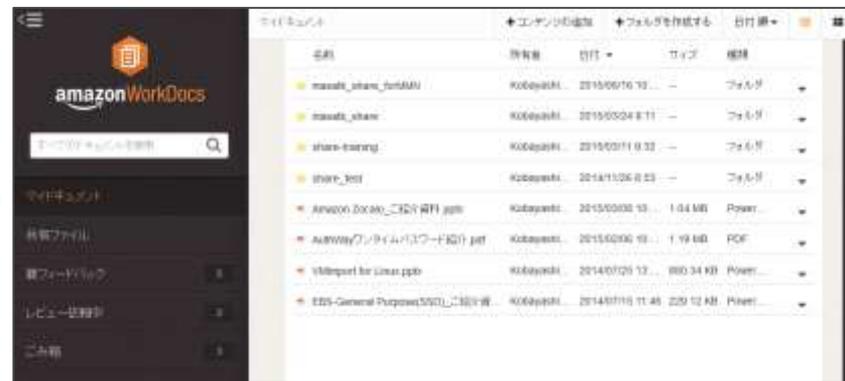
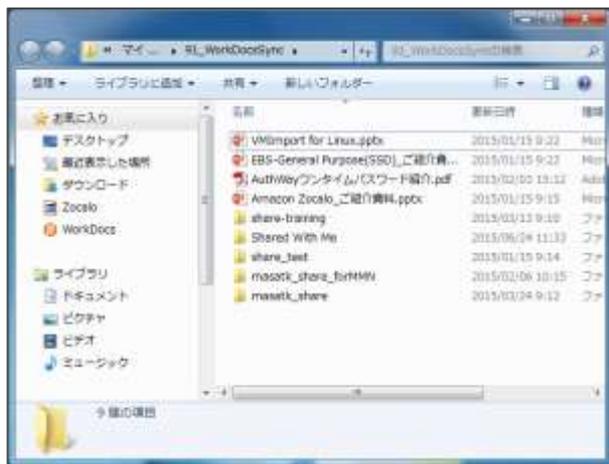
モバイルアプリのサポート

- FireOS(Kindle), Android, iOS端末向けにモバイルアプリを提供。アプリからプレビューやフィードバック、共有の操作が可能
- モバイル向けにオフライン時にプレビューができるようにキャッシュする機能を備える



WorkDocs Syncクライアント

- Windows, MacOS向けに指定したフォルダをバックグラウンドで同期するツールを提供
- 共有されたドキュメントを同期するかどうかは選択式。同期対象を指定することもできて“Shared with Me”フォルダに同期される



※参考：Syncクライアントの動作要件について

http://docs.aws.amazon.com/ja_jp/workdocs/latest/userguide/sync_client_help.html

アジェンダ

- Amazon WorkDocs
 - WorkDocsの概要とユースケース
 - エンドユーザ向け機能
 - 管理者向け機能
- Amazon WorkMail
 - アップデート
 - WorkMailの概要
 - エンドユーザによる利用方法
 - 管理者による環境構築
- まとめ



WorkDocsサイトのセットアップ

- Directory Serviceで作成したAD ConnectorまたはSimple ADに対してWorkDocsサイトをセットアップし、サブドメインを決める
- 最初の管理者ユーザを指定する

Select a Directory

We noticed you have existing directories that are not registered for Amazon WorkDocs. You can enable a directory for Amazon WorkDocs by selecting the directory below.

Region US West (Oregon)

Available Directories: [Or create a New Directory for WorkDocs](#)

Set Site URL: ⓘ

Set WorkDocs Administrator

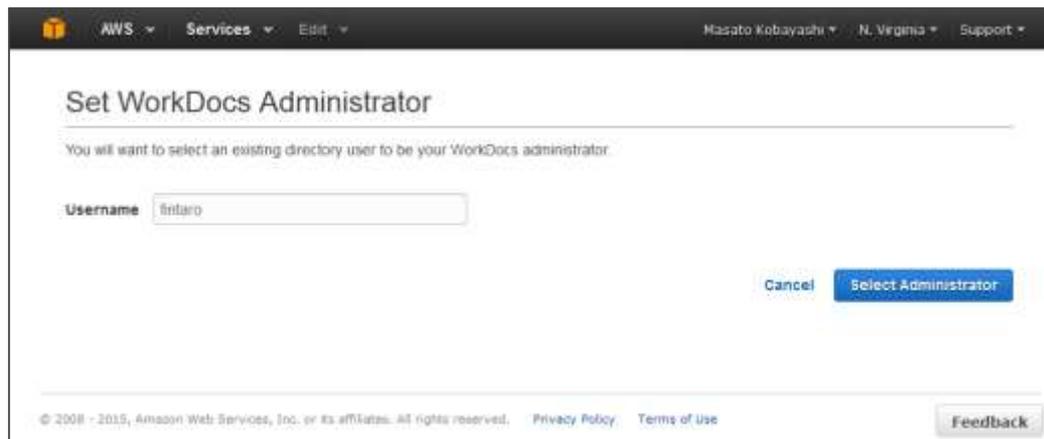
You will want to select an existing directory user to be your WorkDocs administrator.

Username:

[Cancel](#) [Select Administrator](#)

管理者画面へのアクセスと管理ユーザの設定

- 管理者ユーザでWorkDocsにログインすると、ナビゲーションペインに管理者メニューが表示される
- Management Consoleから管理者ユーザを指定することが可能



WorkDocsサイトのポリシー設定

- ユーザ毎のクォータ設定や新規ユーザの招待を許可するかを指定
- ドキュメントの共有範囲を下記から設定できる
 - 外部への共有不可（ドメイン内のユーザに限定）
 - 指定ドメインのユーザのみに許可
 - 制限なく許可



ユーザ管理

- 連携先ディレクトリに登録されたユーザがリストされるので、個別にWorkDocsアカウントの有効・無効を選択する
- ユーザ毎のストレージ利用量を一覧で把握できる

名前	ユーザー名	ステータス	権限	ストレージ使用量	
Tsutsumi Akiko	atsutsum	アクティブ	ユーザー	0.00 GB / 200 GB	
Kaneiko Ichiro	kaneichi	アクティブ	ユーザー	0.00 GB / 200 GB	
Finance Jiro	finjiro	非アクテ...	ユーザー	0.00 GB / 0 GB	
Game Jiro	gamejro	非アクテ...	ユーザー	0.00 GB / 0 GB	
Media Jiro	medjiro	非アクテ...	ユーザー	0.00 GB / 0 GB	
Telecom Jiro	tejiro	保留中	ユーザー	0.01 GB / 200 GB	  
Namiki Katsuhito	namikik	アクティブ	ユーザー	0.00 GB / 200 GB	
Kobayashi Katsunori	kakobaya	アクティブ	ユーザー	0.00 GB / 200 GB	
Kobayashi Masato2	kobayama	アクティブ	管理者	0.02 GB / 200 GB	

アカウントの払い出し

- ユーザ毎にアカウントを有効化することで、ディレクトリに保存された認証情報を利用してWorkDocsにログイン可能になる
- 一般ユーザ権限か管理者権限を選択。個別のクォータも設定可能

ユーザーの編集

名
Ichiro

姓
Kaneke

ユーザー名
kaneichi

メールアドレス
kaneichi@cloud-samurai.com

ステータス
 アクティブ
 非アクティブ

権限
 管理者
 ユーザー

ストレージ
 無制限
 制限: 200 GB

アカウントの権限を選択する

必要に応じてクォータを設定

キャンセル 変更の保存

管理者側でのファイル所有権の付け替え

- WorkDocsユーザのアカウントを無効化にする際に、該当ユーザのファイル所有権を他のユーザに移行するかを選択できる
- この作業を行うことで、ユーザがWorkDocsの利用を終了する際にもファイルへのアクセスを維持できる

ユーザーの編集

名
Ryosuke

姓
Kataoka

ユーザー名
kataoki

メールアドレス
kataoki@cloud-samurai.com

ステータス
 アクティブ
 非アクティブ

ドキュメントの所有権の継承
kobayama
Masafumi Kobayashi (kobayama) じざん

権限
 管理者
 ユーザー

ストレージ
 無制限
 制限: 200 GB

キャンセル 変更の保存

アカウントを非アクティブに変更

ファイルの所有者を移行するユーザーを指定

Directory側でのユーザ操作への追従

- Directory側でユーザを無効にすると、WorkDocs側ではアカウントのステータスが**保留中**になる
 - アカウントを**非アクティブ**にしてファイルの所有権を移行できる
- ユーザが削除されるとWorkDocs側でも該当ユーザが削除される。所有権移行ができなくなるため、ユーザ削除時は注意が必要

ユーザーの管理

☑ ユーザーの招待

名前	ユーザー名	ステータス	権限	ストレージ使用量
Telecom Jiro	teljiro	保留中	ユーザー	0.01 GB / 200 GB
Telecom Taro	teltaro	アクティブ	ユーザー	0.00 GB / 200 GB

CloudTrailによるAPIコールの記録

- ユーザがどういった操作を行ったかについて詳細な情報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
- 一部のAPIについてはIAMのコンソールでアクティビティを追跡することもできる



```
{
  "eventVersion": "1.02",
  "userIdentity": {
    "principalId": "S-1-5-21-3312768711-3070474699-4104396599-1120u0026d-90673",
    "accountId": "782789334655",
    "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": {
```

料金

- 1ユーザあたり月額7ドル（200GBのストレージが利用可能）
 - 容量追加時は\$0.033/GBの従量課金となる
 - データ転送料金は無料
 - 有効なWorkDocsアカウントがあればDirectory Serviceは無料となる
- WorkSpacesユーザは50GBまで無料で利用可能
 - 月額3ドルでストレージ容量を200GBにアップグレード可能
- 最大50ユーザが30日間試用できるトライアルプログラムあり

※金額は東京リージョンにおける2016年2月時点のものです。

アジェンダ

- Amazon WorkDocs
 - WorkDocsの概要とユースケース
 - エンドユーザ向け機能
 - 管理者向け機能
- Amazon WorkMail
 - アップデート
 - WorkMailの概要
 - エンドユーザによる利用方法
 - 管理者による環境構築
- まとめ



WorkMailアップデート

- Limited Previewが終了し一般利用が可能に(GA)
- 利用可能リージョンの追加
 - バージニア、オレゴン、アイルランドの3リージョンで利用可能
- 会議室や物品などの登録と予約管理に対応
- 新たなクライアントのサポートを追加
 - Apple MailやOutlookなどのデスクトップアプリケーション
 - iPhone, iPad, Kindle Fire, Fire Phone, Android, Windows Phone, BlackBerry 10などActive Syncをサポートするデバイス
- 第三者認証を取得
 - ISO 27001, ISO 27017, ISO 27018
- 既存メールボックスの移行ツールを提供(後で説明)

アジェンダ

- Amazon WorkDocs
 - WorkDocsの概要とユースケース
 - エンドユーザ向け機能
 - 管理者向け機能
- Amazon WorkMail
 - アップデート
 - WorkMailの概要
 - エンドユーザによる利用方法
 - 管理者による環境構築
- まとめ



Amazon WorkMailの概要

- **フルマネージド :**
EメールやカレンダーのインフラストラクチャをAmazonがご提供。オンプレミスのEメールサーバの管理や、ライセンスに対する先行投資が不要に。パッチ適用やバックアップはAmazonが実施する
- **Active Directoryとの統合 :**
Microsoft Active Directoryと安全に連携することができるため、ユーザは既存の認証情報を利用してメールボックスにアクセスできる
- **Outlookとの互換性 :**
Amazon WorkMailではWindowsとMacOS XのMicrosoft Outlookをサポート。既に利用中のメールクライアントの変更や、プラグインのインストールなしに利用開始できる

Amazon WorkMailの概要

- マルチデバイスのサポート：

WindowsやMacで動作するOutlookだけでなく、各種モバイル端末からActiveSyncでメールボックスを同期できる。さらにモバイルデバイスはWorkMailに自動接続が可能

- ウェブクライアント：

Eメールやカレンダー、連絡帳にアクセスするためのウェブクライアントも提供。ブラウザさえあればいつでもアクセスが可能

- 低コスト：

1ユーザあたり月額4ドル（※）で、ユーザあたり50GBのメールボックスをご用意。WorkDocsと同時利用で月額6ドルに

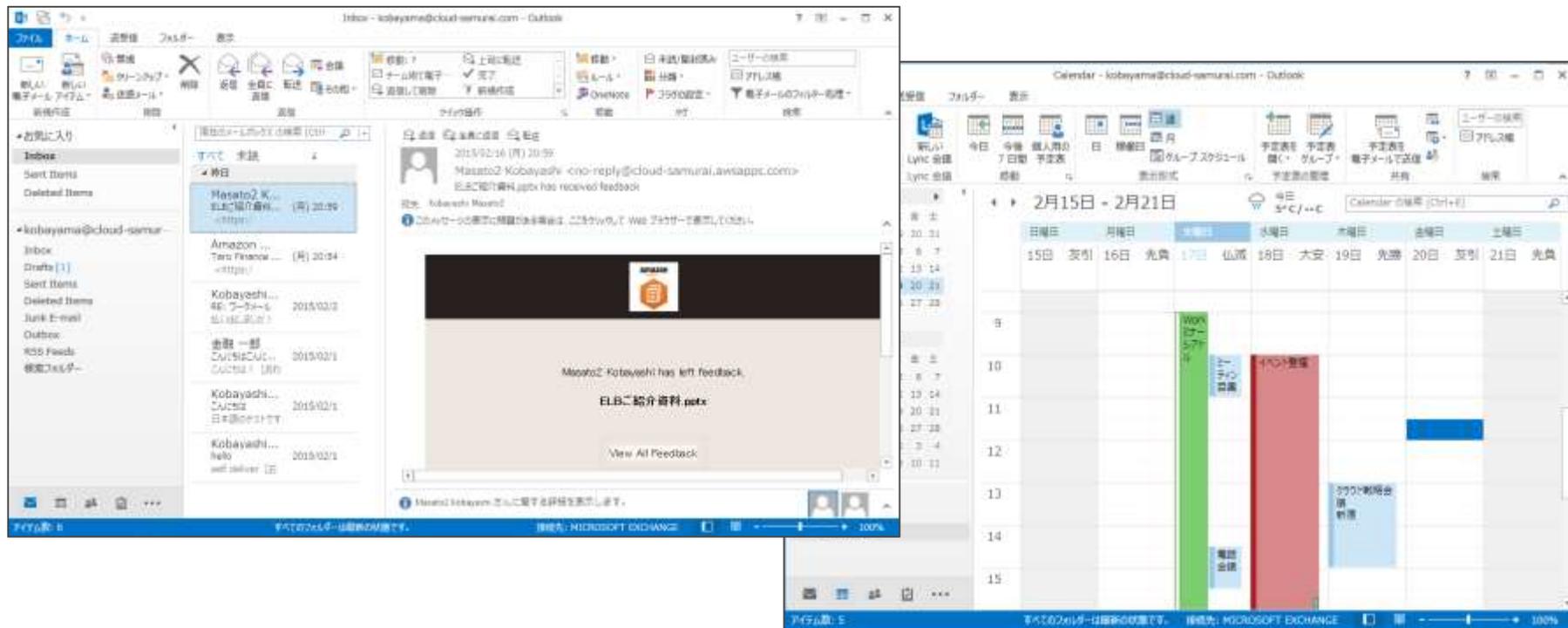
アジェンダ

- Amazon WorkDocs
 - WorkDocsの概要とユースケース
 - エンドユーザ向け機能
 - 管理者向け機能
- Amazon WorkMail
 - WorkMailの概要
 - エンドユーザによる利用方法
 - 管理者による環境構築
- まとめ



クライアントアプリケーションによるアクセス

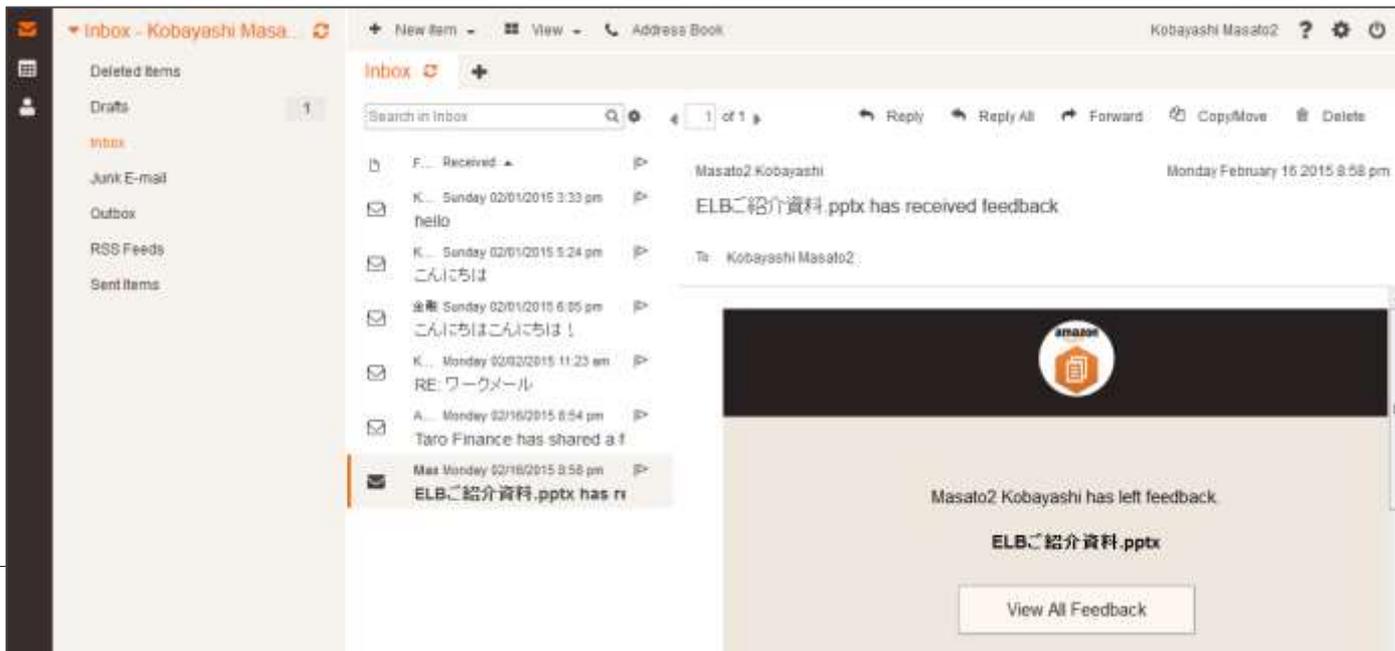
- Outlookなどの使い慣れたアプリケーションでアクセスできる



※現時点ではPOP3/IMAPは未サポートです

Webクライアントによるアクセス

- ウェブブラウザでもEメールとカレンダーにアクセス可能
 - エンドポイントは[https://\(alias\).awsapps.com/mail](https://(alias).awsapps.com/mail)となる
 - (alias)の部分はWorkDocs同様に設定可能



Webクライアントによるカレンダーの参照

The screenshot displays a web-based calendar application. On the left, a sidebar contains navigation icons for mail, calendar, and user profile. The main area is divided into two sections: a monthly calendar for February 2015 and a detailed daily view for the period of February 16 to 20, 2015.

Monthly Calendar (February 2015):

Wk	S	M	T	W	T	F	S
6	1	2	3	4	5	6	7
7	8	9	10	11	12	13	14
8	15	16	17	18	19	20	21
9	22	23	24	25	26	27	28
10	1	2	3	4	5	6	7
11	8	9	10	11	12	13	14

Detailed Daily View (February 16 - 20, 2015):

Time	Monday February 16	Tuesday February 17	Wednesday February 18	Thursday February 19	Friday February 20
9 am		WorkSpaces (シアトル)			
10 am		ミーティング (目黒)	イベント登壇		
11 am					
12 pm					
1 pm					
2 pm		電話会議		クラウド戦略会議 (新宿)	
3 pm					
4 pm					

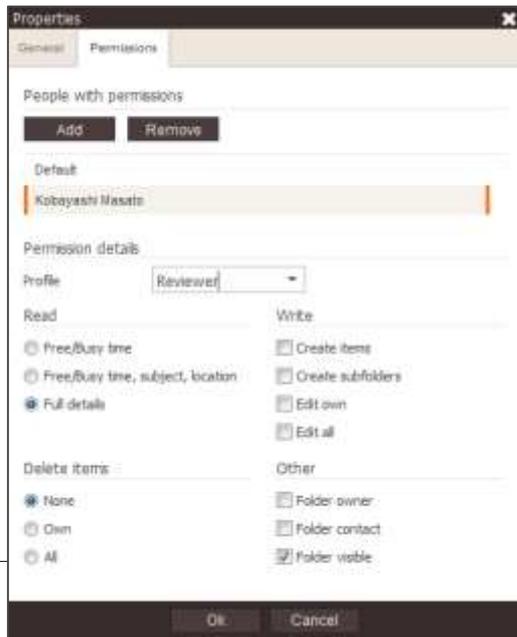
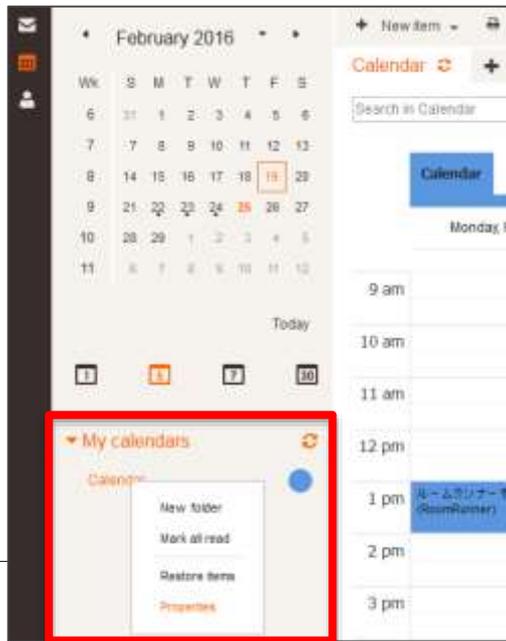
モバイル端末からのアクセス

- ActiveSyncをサポートした端末からEメールやカレンダーへのアクセスを容易に実現



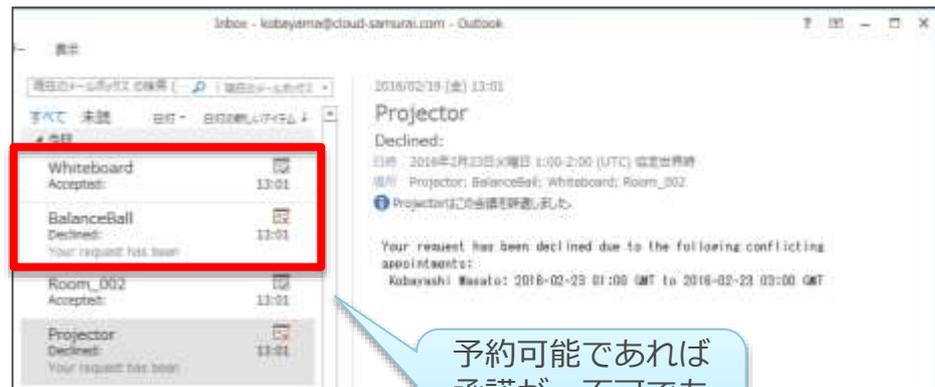
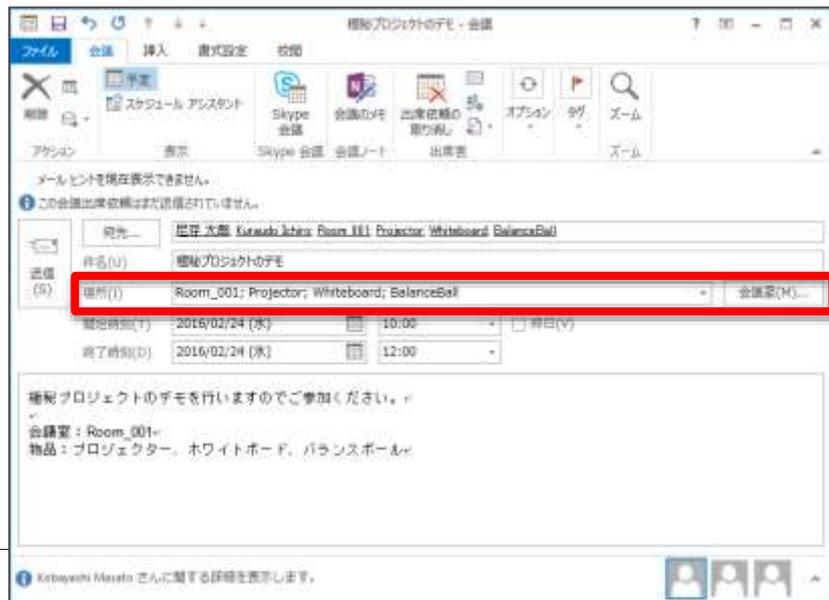
カレンダーの共有

- ユーザやグループに対してカレンダーの共有が可能
- ユーザごとに権限を指定できるので、タイトルや場所だけ許可することや、すべての内容を参照可能にすることもできる



リソースの予約

- 会議室やプロジェクターといったリソースの予約管理をサポート
- 管理者側であらかじめ作成したリソースにミーティングリクエストを送信、返信メールにて予約可否を確認できる



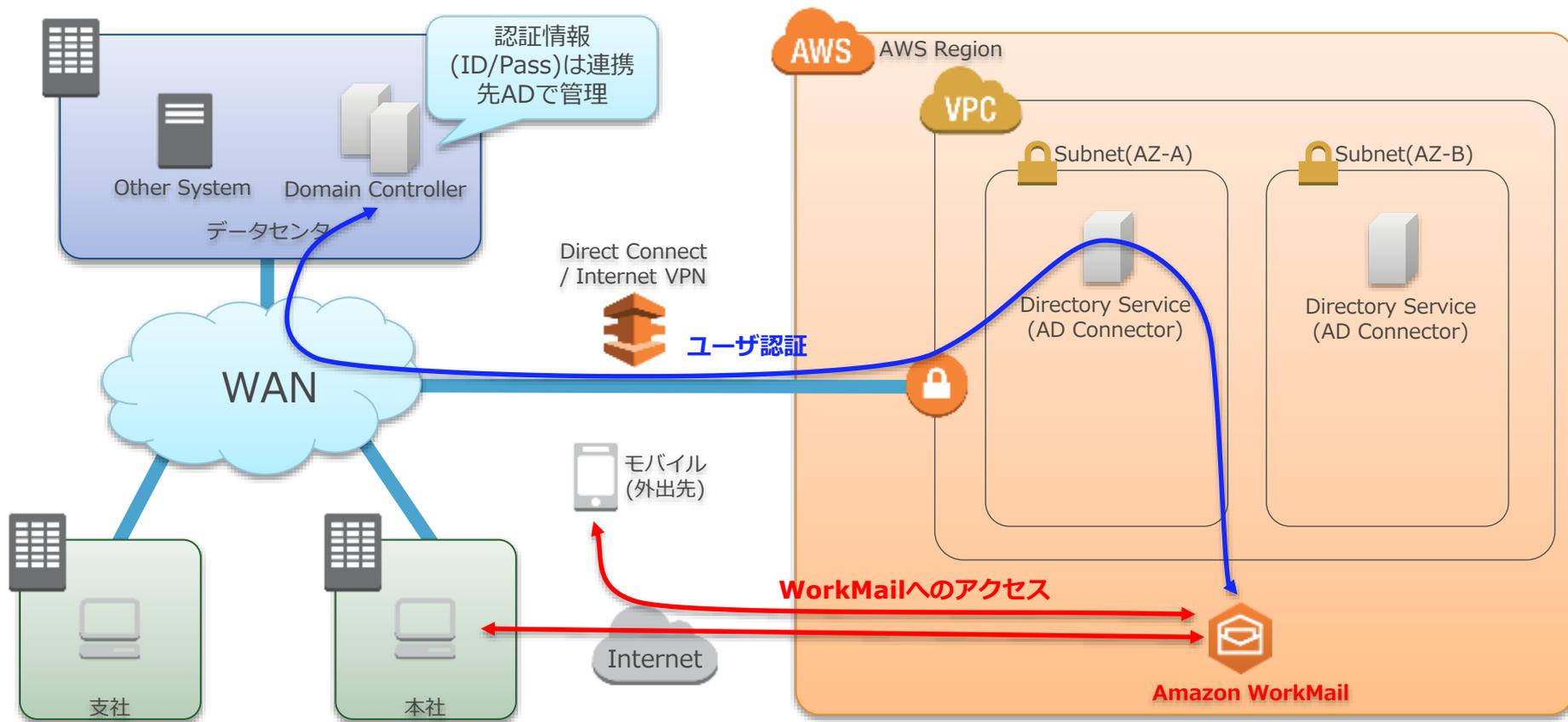
予約可能であれば承諾が、不可であれば拒否で応答

アジェンダ

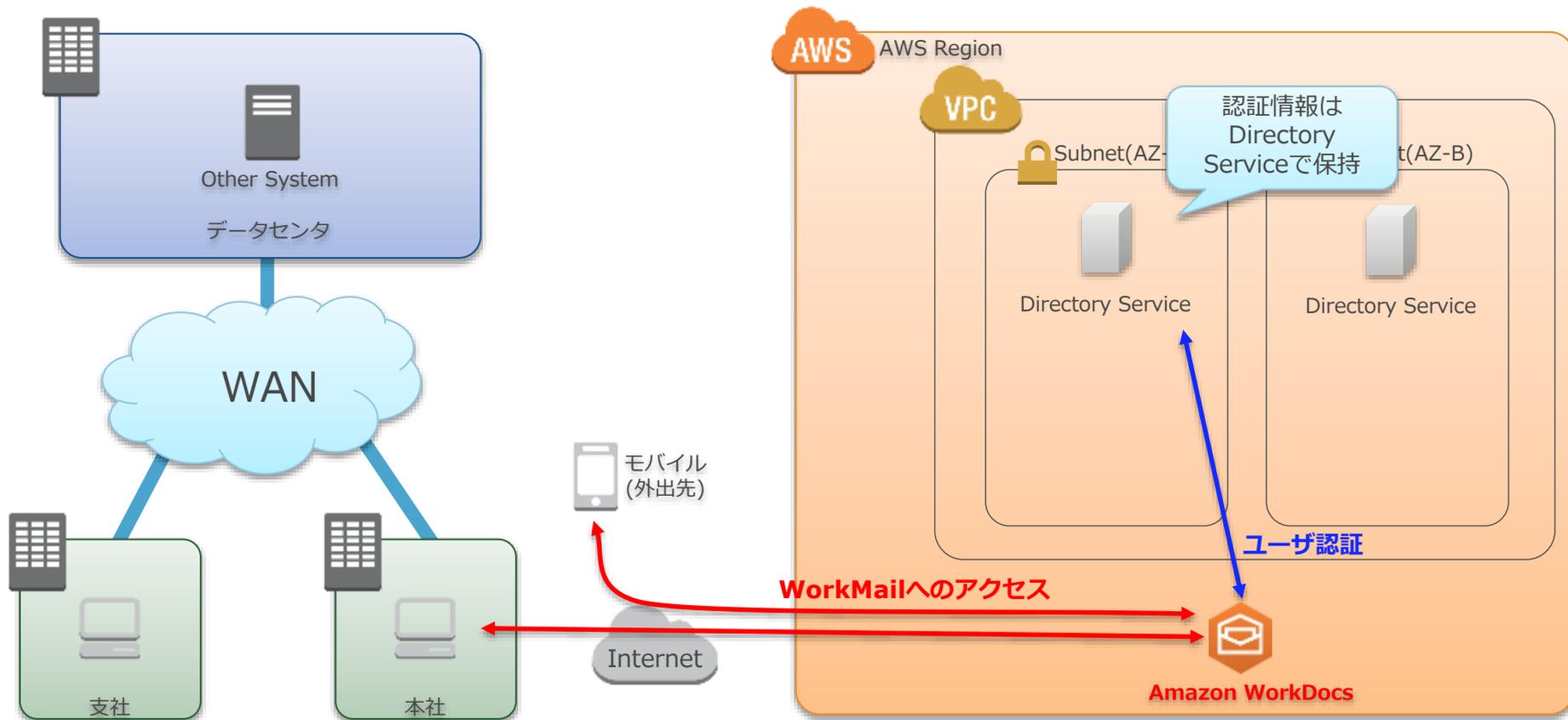
- Amazon WorkDocs
 - WorkDocsの概要とユースケース
 - エンドユーザ向け機能
 - 管理者向け機能
- Amazon WorkMail
 - WorkMailの概要
 - エンドユーザによる利用方法
 - 管理者による環境構築
- まとめ



構成例(AD連携あり)

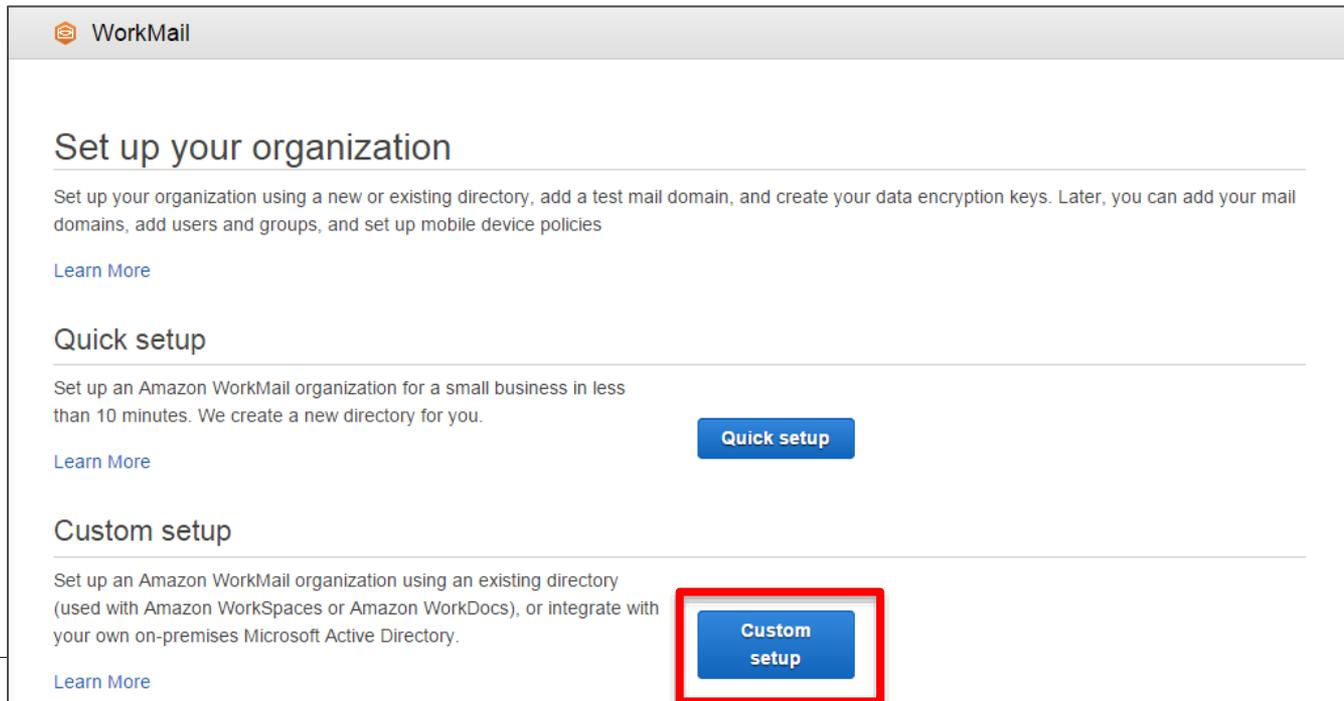


構成例(AD連携なし)



WorkMailのセットアップ

- 全自動のQuick Setupと、カスタマイズが可能なCustom Setupから選択する。既存のディレクトリとの連携を行う場合はCustomを利用する



The screenshot shows the Amazon WorkMail setup interface. At the top, there is a header with the WorkMail logo. Below it, the main heading is "Set up your organization". Underneath, there is a paragraph of text explaining the setup process, followed by a "Learn More" link. The next section is "Quick setup", which includes a paragraph of text and a blue "Quick setup" button. Below that is the "Custom setup" section, which also includes a paragraph of text and a blue "Custom setup" button. The "Custom setup" button is highlighted with a red rectangular border.

利用するディレクトリを指定する

- 事前にDirectory Serviceで設定したAD ConnectorかSimple ADまたはMicrosoft ADから、WorkMailで利用するディレクトリを選択する
- ドメイン単位に指定するマスターキーはKMSで作成・管理を行う

The screenshot shows the 'Directory' configuration page in the Amazon WorkMail console. It includes sections for 'Available Directories', 'Specify a unique alias', 'Encryption key', and 'Available master keys'. Three red boxes highlight the selected directory ID, the alias, and the master key ID. Three blue callout boxes provide instructions: 'Directoryを選択' (Select Directory), '任意のサブドメインを指定' (Specify an arbitrary subdomain), and 'マスターキーとして使う鍵を指定' (Specify a key to use as a master key).

Directory

To add your existing users in Amazon WorkMail, select an existing directory created by Amazon WorkMail. To integrate your on-premises Active Directory, create a new Connect directory using the AWS Directory Service console.

Available Directories*

d-9067363dc4

Specify a unique alias to be used as a test mail domain, used to send outgoing mail to your organization's email clients.

Alias: https://cloud-samuraii.awsapps.com

Encryption key

The mailboxes of your users in Amazon WorkMail must be encrypted with an encryption key, select the key using the AWS IAM Console and then select the new key below.

Available master keys*

6f2ae5b6-cf90-4d5e-8de8-c7e2f5b13572

Description A Custom Key is used to protect your mailbox.

Aliases am-aws-kms-us-east-1-76278934655-alias/Virginia-WorkMail

Key ID 6f2ae5b6-cf90-4d5e-8de8-c7e2f5b13572

Callouts:

- Directoryを選択
- 任意のサブドメインを指定
- マスターキーとして使う鍵を指定

ディレクトリのユーザにアカウントを払い出す

- ユーザ毎にWorkMailの利用有無を設定する
- 各個人のメールアドレスは任意に設定可能

The screenshot shows the Amazon WorkMail console interface. The main page is titled 'WorkMail cloud-samurai Users'. A red box highlights the 'Add user' button. Below it, there are buttons for 'Remove' and 'Reset Password'. A search bar is present with the text 'Enter text'. A table lists users with checkboxes for selection. The modal window 'Enable existing user' is overlaid on the right, showing a search for 'Jiro' and a table of directory users with their status. The modal also shows a 'Selected users' section with two users selected: 'Finance Jiro' and 'Game Jiro'. Navigation buttons 'Cancel', 'Previous', and 'Next Step' are at the bottom of the modal.

WorkMail console interface:

- Buttons: Add user (highlighted), Remove, Reset Password
- Search: Enter text
- Table:

<input type="checkbox"/>	Display name	User name
<input type="checkbox"/>	Telecom Jiro	teljiro
<input type="checkbox"/>	銀行 次郎	ginjiro
<input type="checkbox"/>	Telecom Taro	teltaro
<input type="checkbox"/>	Finance Jiro	finjiro

Enable existing user modal:

Select existing users from your directory to enable them for access to Amazon WorkMail.

Directory users

Users available in your directory:

Display Name	User Name	Status
Finance Jiro	finjiro	Not enabled
Game Jiro	gamejro	Not enabled
<input type="checkbox"/> Media Jiro	medijro	Not enabled
Telecom Jiro	teljro	WorkMail enabled

Selected users

Users selected for access to Amazon WorkMail:

<input type="checkbox"/>	Display Name	User Name
<input checked="" type="checkbox"/>	Finance Jiro	finjiro
<input checked="" type="checkbox"/>	Game Jiro	gamejro

Buttons: >>, <<, Cancel, Previous, Next Step

ディレクトリのグループを有効化する

- WorkMailはグループに対するメール配信もサポートするが、個別に有効化の操作が必要。キーワードで検索を行い、一括で有効化が可能
- ユーザのアドレスと同様に、グループアドレスも任意に設定できる

Enable existing group

Select your existing groups from the directory to enable them for access to Amazon WorkMail.

Directory Groups

Groups available in your directory.

Search:

Group Name	Status
sales	WorkMail enabled
sales-finance	Not enabled
sales-game	Not enabled
<input type="checkbox"/> sales-media	Not enabled
sales-telecom	WorkMail enabled

Selected groups

Groups selected for access to Amazon WorkMail

Display Name
<input type="checkbox"/> sales-finance
<input type="checkbox"/> sales-game

>>

<<

Cancel Previous **Next Step**

独自ドメインの設定

- WorkMailでは独自ドメインの利用が可能。セットアップが完了した後に、独自ドメインの設定を行いDNSに指定のエントリを入力しドメイン認証を行う必要がある。完了後に該当ドメインをデフォルト化する

WorkMail cloud-samurai - Domains > cloud-samurai

Step 1: verify domain ownership

Before you can use your domain with Amazon WorkMail, you must verify that you own the domain. Add the following record to your DNS hosting provider's DNS zone.

Record type	Hostname	Value
TXT	_amazonses.cloud-samurai.com.	"9W+Mst+QYE+9sPSzwag7WWqDcQHrkyUvZku_xFpigEd-

Verification can take up to 1 hour.

Step 2: Finalize domain setup

To switch your domain completely to Amazon WorkMail, add the following DNS records to your DNS hosting provider's DNS zone. 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	cloud-samurai.com.	10 inbound-smtp.us-east-1.amazonaws.com.
CNAME	autodiscover.cloud-samurai.com.	autodiscover.mail.us-east-1.amazonaws.com.
CNAME	nr7hggdprmsdggwwoxm7ra67v07px_domainkey.cloud-samurai.com.	nr7hggdprmsdggwwoxm7ra67v07px_domainkey.mail.us-east-1.amazonaws.com.

指定されたエントリをDNSに登録してドメインを検証

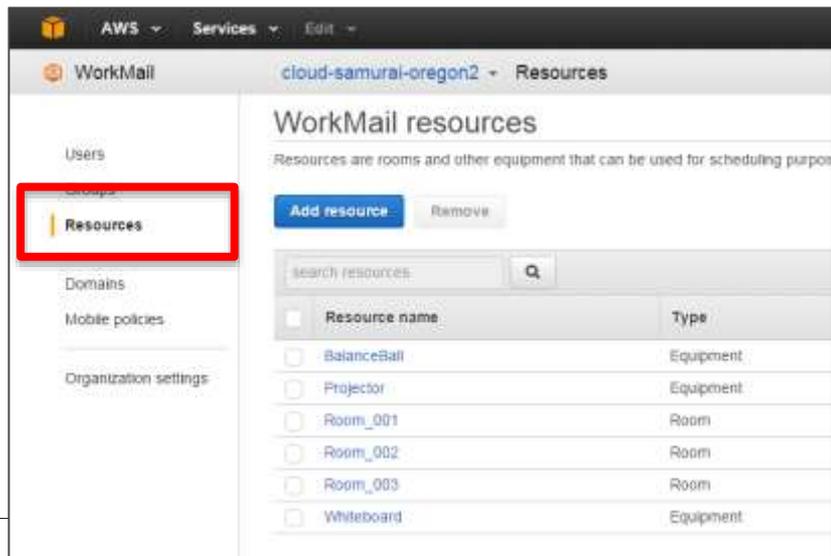
独自ドメインをデフォルト設定に

Buttons: Add domain, Remove, **Set as default**

<input type="checkbox"/>	Domain	Status	Default Domain
<input type="checkbox"/>	cloud-samurai.awsapps.com	Active	
<input checked="" type="checkbox"/>	cloud-samurai.com	Active	Default

リソースの定義

- WorkMailを利用して会議室や物品の管理をする場合は、Management Consoleでリソースを定義する
- 会議室または物品のカテゴリを指定可能。メールアドレスの割り当てが必要となる



The screenshot shows the 'Add resource details' form. It includes the following fields and options:

- Resource name***: RoomRunner
- Description**: for your health
- Resource type***: Room, Equipment
- Email address***: roomrunner @ cloud-samurai.com

Buttons: Cancel, Create

* Required information

リソースの定義

- ミーティングリクエストの受信時の動作をリソースごとに設定可能
 - 自動でリクエストを承諾する
 - 定期的な予定については自動的に拒絶する
 - 重複する予定については自動的に拒絶する
- 自動的にリクエストを承諾しない場合は権限を委譲されたユーザが判断

Resource details

You can edit the email address and booking options of the resource. In addition you can add and remove delegates for this resource.

General Booking options Delegates

Booking options

Cancel Save

- Automatically accept all resource requests ⓘ
- Automatically decline recurring resource requests
- Automatically decline conflicting resource requests

リソースの権限委譲

- 会議室や物品の利用可否をユーザが判断したい場合、他のユーザに権限を委譲することができる
- リソースに対するミーティングリクエストが送信されると、権限を委譲されたユーザーにメールが送信され、承諾または拒否を選択可能



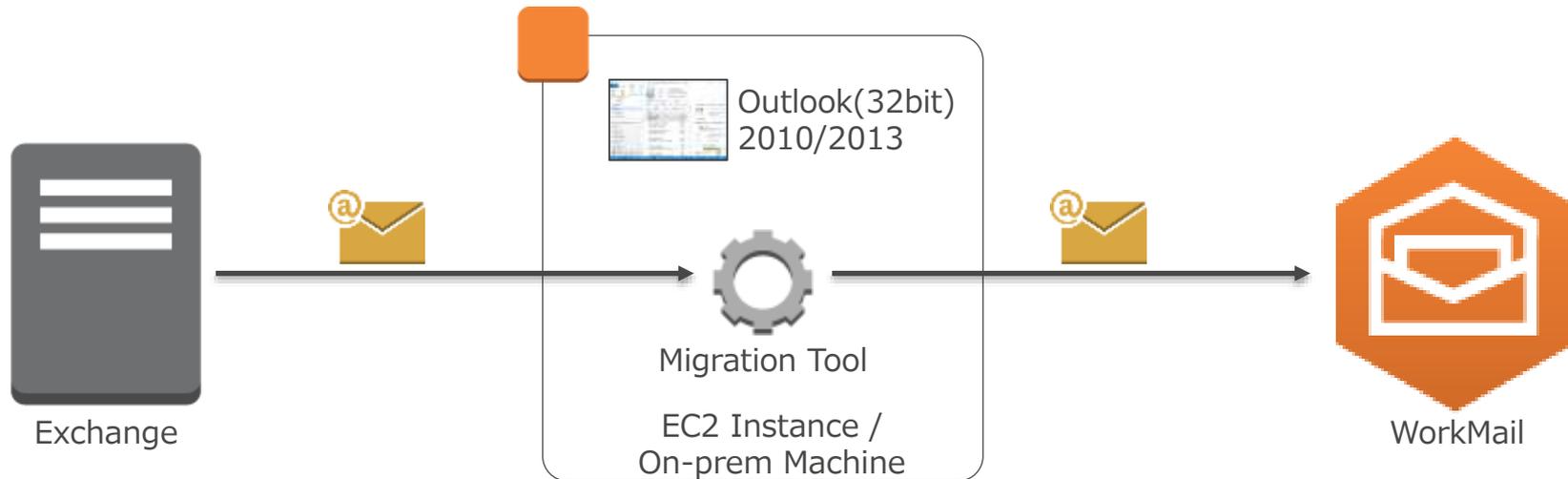
モバイルデバイスポリシー

- モバイルデバイスからアクセスをする際、デバイスが満たしているべき要件を指定できる暗号化の有無やパスワードの複雑さなどの条件を元に、メールボックスやカレンダーの同期可否を制御する

The screenshot shows the 'Mobile policy' configuration page in the AWS IAM console. The left sidebar contains navigation links for Users, Groups, Resources, Domains, Mobile policies (selected), and Organization settings. The main content area is titled 'Mobile policy' and includes a 'Cancel' button and a 'Save' button. Below the title, there is a text block stating: 'There is one default mobile policy available for your entire organization. All users within your organization will automatically have this policy enabled. [Learn more](#)'. The page is divided into three sections: 'General settings', 'Password settings', and 'Enforce password history'. The 'General settings' section has two unchecked checkboxes: 'Require encryption on device' and 'Require encryption on storage card'. The 'Password settings' section has several options: 'Password required' (checked), 'Allow simple password' (checked), 'Minimal password length' (checked, set to 4 characters), 'Require alphanumeric password' (unchecked, set to 2 character sets), 'Number of failed attempts allowed' (checked, set to 10 attempts), 'Password expiration' (unchecked, set to 1 day), 'Enable screen lock' (checked, set to 300 seconds), and 'Enforce password history' (unchecked, set to 1 passwords). The bottom right corner of the form area has 'Cancel' and 'Save' buttons.

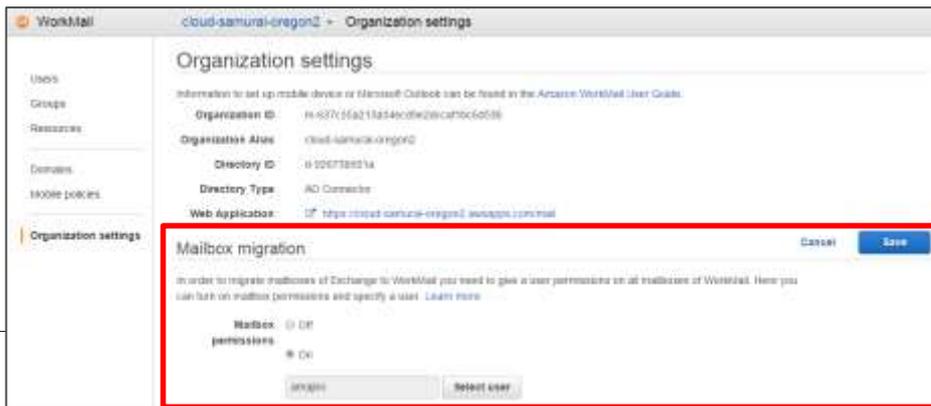
Amazon WorkMail Migration Tool

- Microsoft ExchangeからWorkMailへの移行を支援するツールを提供
- 移行ツールが稼動するために、オンプレミスかEC2にOutlookがインストールされたホストが必要



移行作業のステップ

1. WorkMail側に移行先となるユーザアカウントを作成
2. Exchange側にAdministrator権限を持ったユーザアカウントを作成
3. WorkMailで移行作業用に利用するアカウントを指定
4. 移行用ホストにツールを導入し、設定を行う
5. 移行対象ユーザリスト(users.cfg)を編集し移行を行うユーザを指定する
6. Amazon Workmail Migration Toolを実行（コマンドラインもサポート）



Management Consoleで
移行ツールが使うユーザ
を指定する

前提条件とベストプラクティス

- 前提条件
 - 移行ツール用のホストはWindows7, Windows Server 2008/2012が必要
 - Outlook 2010または2013の32bit版が必要
 - Exchange ServerとWorkMailの双方にHTTPS接続ができること
- ベストプラクティス
 - 移行対象が多い場合は複数のホストでツールを同時実行する。その際、移行対象ユーザリストをホストごとに重複しないようにする必要がある
 - 移行ホストはWorkMailのエンドポイントに近いところに配置する。WorkMailを利用するリージョンのEC2インスタンスであればよい

アジェンダ

- Amazon WorkDocs
 - WorkDocsの概要とユースケース
 - エンドユーザ向け機能
 - 管理者向け機能
- Amazon WorkMail
 - WorkMailの概要
 - エンドユーザによる利用方法
 - 管理者による環境構築
- まとめ



まとめ

- WorkDocs
 - ドキュメントの保管や共有、フィードバックといった企業内で頻繁に発生する文書のやり取りをスムーズに、かつ安価に実現できる
 - Syncクライアントにより、ユーザに意識させることなくデータのバックアップをバックグラウンドで取得できる
- WorkMail
 - ユーザ側アプリケーションを変更すること無く、Eメールやカレンダーのサービスをセキュアに提供できる
- いずれも安価なフルマネージド型サービスとして提供されるため、お客様の管理運用作業を最小限に抑えることが可能

参考資料

- Amazon WorkDocs
<http://aws.amazon.com/jp/workdocs/>
- Amazon WorkDocs Documentation
<http://aws.amazon.com/jp/documentation/workdocs/>
- Amazon WorkMail
<http://aws.amazon.com/jp/workmail/>
- Amazon WorkMail Documentation
<http://aws.amazon.com/jp/documentation/workmail/>
- AWS Directory Service
<http://aws.amazon.com/jp/directoryservice/>
- AWS Key Management Service
<http://aws.amazon.com/jp/kms/>