



このコンテンツは公開から3年以上経過しており内容が古い可能性があります
最新情報については[サービス別資料](#)もしくはサービスのドキュメントをご確認ください

[AWS Black Belt Online Seminar] Amazon WorkSpaces

サービスカットシリーズ

Solutions Architect 国政 丈力
2019/2/26

AWS 公式 Webinar

<https://amzn.to/JPWebinar>



過去資料

<https://amzn.to/JPArchive>



自己紹介

国政 丈力 (くにまさ たけちか)

技術統括本部

エンタープライズ・ソリューション本部

ソリューションアーキテクト

流通・サービス業のお客様を担当



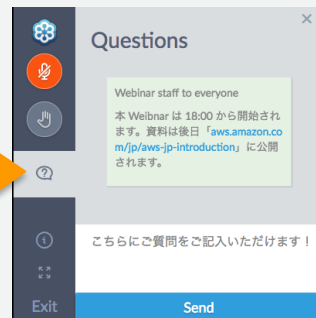
好きなAWSのサービス

Amazon WorkSpaces, Amazon VPC

AWS Black Belt Online Seminar とは

- 「サービス別」「ソリューション別」「業種別」のそれぞれのテーマに分かれて、アマゾン ウェブ サービス ジャパン株式会社が主催するオンラインセミナーシリーズです。
- **質問を投げることができます！**
- 書き込んだ質問は、主催者にしか見えません
- 今後のロードマップに関するご質問は
お答えできませんのでご了承下さい

- ① 吹き出しをクリック
- ② 質問を入力
- ③ Sendをクリック



Twitter ハッシュタグは以下をご利用ください
#awsblackbelt

内容についての注意点

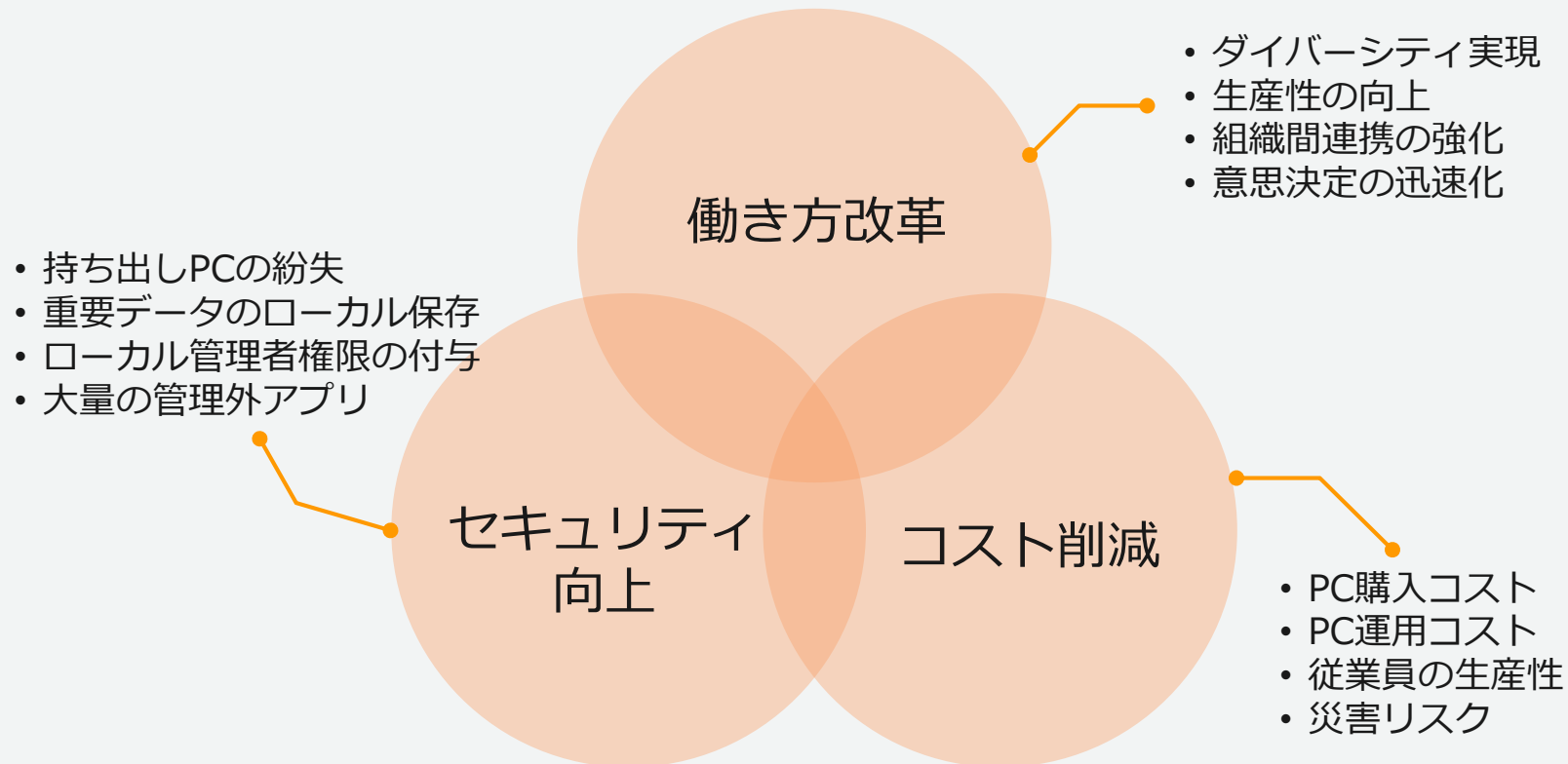
- 本資料では2019年2月26日時点のサービス内容および価格についてご説明しています。最新の情報はAWS公式ウェブサイト(<http://aws.amazon.com>)にてご確認ください。
- 資料作成には十分注意しておりますが、資料内の価格とAWS公式ウェブサイト記載の価格に相違があった場合、AWS公式ウェブサイトの価格を優先とさせていただきます。
- 価格は税抜表記となっております。日本居住者のお客様が東京リージョンを使用する場合、別途消費税をご請求させていただきます。
- AWS does not offer binding price quotes. AWS pricing is publicly available and is subject to change in accordance with the AWS Customer Agreement available at <http://aws.amazon.com/agreement/>. Any pricing information included in this document is provided only as an estimate of usage charges for AWS services based on certain information that you have provided. Monthly charges will be based on your actual use of AWS services, and may vary from the estimates provided.

本日の内容

- 本日も話すること
 - デスクトップ仮想化が注目される背景
 - Amazon WorkSpacesの概要
 - セットアップとデスクトップ利用
 - アーキテクチャ
 - デザインパターン
- 本日も話さないこと
 - WorkSpacesの運用管理

デスクトップ仮想化 (VDI) が注目される背景

当初はセキュリティ向上、デスクトップ管理性向上によるコスト削減で注目された。
リモートで安全に業務ができることから、働き方改革の文脈でも注目されるようになった。



オンプレミスのVDIにおける課題

コストや利用までの時間、柔軟性や困難な設計・サイジングに課題

- 高額な初期投資が必要
- 利用までに長い時間がかかる
- 定期的な大規模システム更改
- 利用者増減への対応が困難
- サイジングが重要だが困難



コスト



長期にわたる導入



システムの更新



スケールの難しさ



性能の予測が困難

Amazon WorkSpaces とは

AWSの提供するフルマネージド型仮想デスクトップサービス

- クラウド上にデスクトップ環境を提供「いつでも・どこでも」を実現
- 従量課金型。月額30ドル/ユーザーから（*）

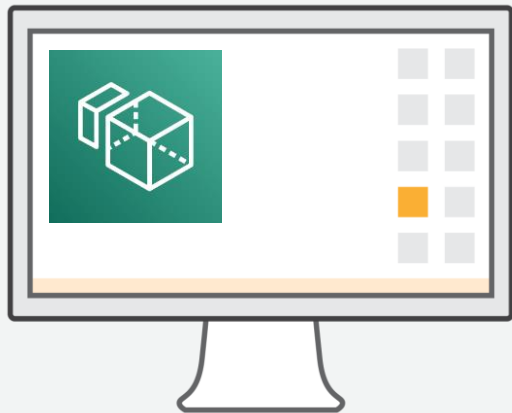


* 東京リージョン、Linux WorkSpaces、Valueバンドル、月額課金の場合

Amazon WorkSpaces による解決

クラウドコンピューティングの特性を活かしたVDIによる様々なメリット

amazon
WorkSpaces



初期投資不要（無料枠あり）
今日から・一台から始められる



事前サイジングの必要がない、増減も容易



シンプルなデプロイと管理
完全マネージドサービス



グローバル展開の敷居が低い



様々なAWSサービスと連携が可能

Amazon WorkSpaces のバンドルと価格

用途にあった様々なスペック・タイプのデスクトップを選択可能

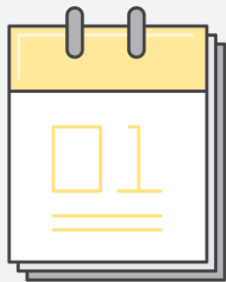
	Value	Standard	Performance	Power	PowerPro	Graphics	GraphicsPro
vCPU	1	2	2	4	8	8	16
メモリ (GiB)	2	4	7.5	16	32	15	122
ルートボリューム (GB)	80	80	80	175	175	100	100
ユーザーボリューム (GB)	10	50	100	100	100	100	100
GPU	-	-	-	-	-	1	1
ビデオメモリ (GB)	-	-	-	-	-	4	8
Windows 月額料金	\$34	\$47	\$78	\$118	\$177	\$951	\$1,283
Windows 時間料金	\$10/月 + \$0.30/時	\$14/月 + \$0.40/時	\$19/月 + \$0.74/時	\$26/月 + \$0.89/時	\$26/月 + \$1.84/時	\$30/月 + \$2.41/時	\$85/月 + \$14.93/時
Linux 月額料金	\$30	\$43	\$74	\$114	\$173	-	-
Linux 時間料金	\$10/月 + \$0.25/時	\$14/月 + \$0.36/時	\$19/月 + \$0.68/時	\$26/月 + \$0.85/時	\$26/月 + \$1.80/時	-	-

Windowsは PlusアプリケーションバンドルでMicrosoft Office Professionalを追加 - \$15/月

アジアパシフィック (東京)の2019/2時点の価格
- BYOLで\$4削減

柔軟な課金オプション

月間のデスクトップ利用時間に応じた、適切な課金オプションの選択肢を提供



Monthly

主な用途

- フルタイムの従業員
- AWS料金のシンプルさ
- いつでもアクセス
- 日常業務



Hourly

主な用途

- パートタイムの従業員
- AWS料金の最適化
- クイックにアクセス
- 一時的なタスクの実行

Amazon WorkSpaces ユースケース

様々なユースケースに適用可能



モダンな働き方

グローバル組織
モバイルワーカー
合併と買収
開発者の生産性



プロジェクトベースの業務

短期プロジェクト
派遣社員
トレーニング



セキュリティとコンプライアンス

セキュアなアプリとデータ
BYOD のサポート
コンプライアンス要件への準拠

グローバルなカバレッジ

グローバルな12のAWSリージョンで利用可能

New



PowerPro/GraphicsPro バンドル

より高性能なスペックが必要なユースケースに対応

New

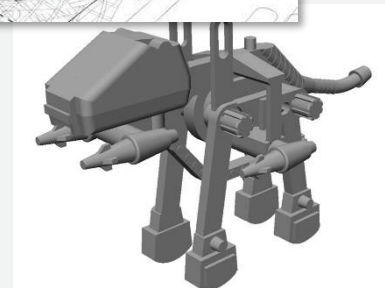
2018.10月

• PowerPro バンドル

- 8vCPU, 32GBメモリを搭載
- 多くのリソースが必要なワークロードを実行するため、よりパワフルな環境を提供
- 開発者やデータサイエンティスト等、大量のCPUやメモリが必要なコンパイル、複雑なシミュレーションでの利用

• GraphicsPro バンドル

- 16vCPU, 122GBメモリ, GPU(NVIDIA Tesla M60)を搭載、グラフィック処理を高速化
- 高性能なGPUにより、3D CAD等の利用において画面が滑らかに動き、細かな場所まで正確に描画されるなどグラフィック処理を改善
- CAD/CAM/CAE、3Dエンジニアリング、アニメーション等、高度なグラフィックス処理での利用



Amazon Linux WorkSpaces

WorkSpacesでも使い慣れたAmazon Linuxが利用可能に

New

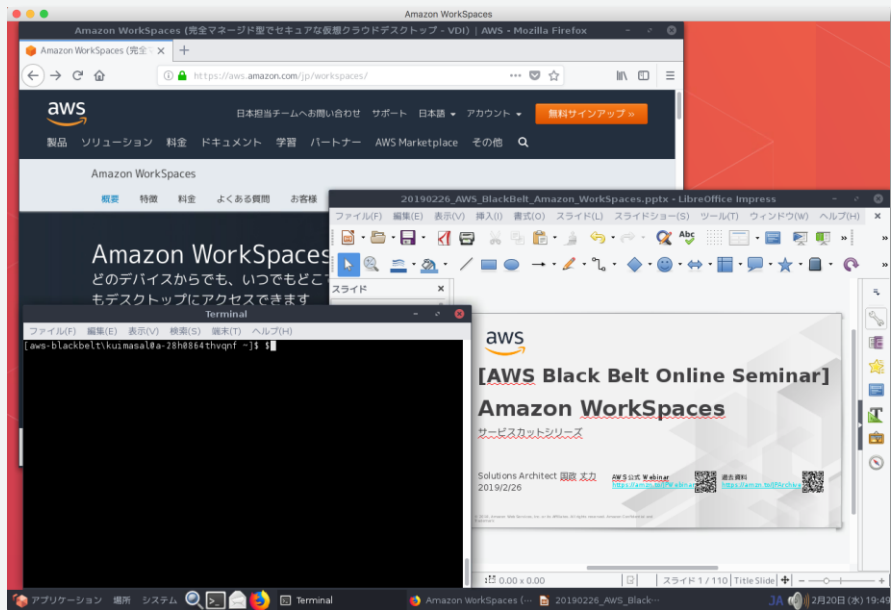
2018.6月



Amazon
Linux 2



- Amazon Linux 2 がベース
- ブラウザ, Office環境(Libre Office), AWS SDK等がセットアップ済み
- 開発者やオフィス用途に適する

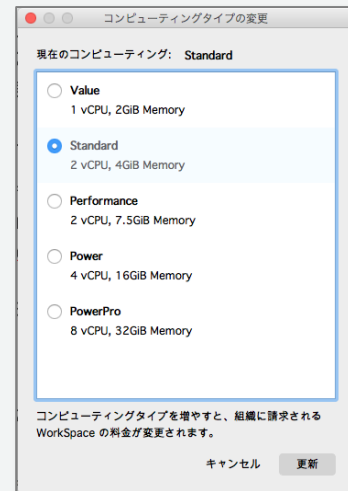


ユーザーセルフサービス管理機能

New 2018.11月

WorkSpaces の利用ユーザー自身で WorkSpaces の管理や構成変更の操作が可能に

- 以下のオペレーションを実行可能
 - WorkSpaces の再起動
 - ディスクサイズの増加:
ルート、ユーザーとも 2,000GB まで拡張可能
 - コンピューティングタイプの変更:
Value/Standard/Performance/Power/PowerPro
 - 実行モードの切り替え: AlwaysOn/AutoStop
 - WorkSpaces の再構築
- 許可するオペレーションは管理者が選択可能
 - 設定はディレクトリ単位
- WorkSpaces Client でサポート
 - Web Access では利用できない



Windows 7/10 BYOL WorkSpaces

Windows デスクトップや Microsoft Office ライセンスの持ち込みも可能

- Windows BYOL とは
 - マイクロソフト社のライセンス要件を満たす場合、お客様が保有する Windows 7/10 ライセンスを AWS に持ち込み、WorkSpaces で利用することが可能
 - BYOL WorkSpaces は物理的な専用ハードウェア上で実行される
- BYOL のメリット
 - Windows 7/10 のライセンスが利用可能
 - ライセンスコストの削減
 - 共有のユーザエクスペリエンス
 - MS Office の BYOL も可能
- 価格と要件
 - すべてのリージョンでバンドル価格を\$4/月削減
 - 200台の利用から



Windows デスクトップの BYOL 自動化

Windows BYOL プロセス自動化でデプロイまでの期間を大幅に短縮

New

2018.11月

- Windows BYOL の自動化
 - Windows BYOL のためのイメージのインポートとライセンス持ち込みが自動化され、数クリックで素早く移行が可能に
 - 2ヶ月ほどかかっていた煩雑な従来プロセスを大幅に改善・時間短縮
 - BYOL を始めるには、AWSの担当者にご連絡ください



セットアップとデスクトップ利用

WorkSpaces デプロイ手順

1. 事前準備

- ディレクトリの作成

2. WorkSpaces の作成

- WorkSpaces の作成開始
- ディレクトリの選択
- ユーザーの追加
- バンドルの選択
- WorkSpaces の設定
- レビューと起動
- メールの受信とユーザー登録

3. WorkSpaces クライアント

- クライアントのダウンロード
- クライアントの設定
- ネットワーク接続性の確認
- WorkSpaces への接続

事前準備

ディレクトリの作成

- ユーザー認証のためのディレクトリを事前に作成
- AWS上に新規作成する場合
 - Microsoft AD
 - Simple AD
- オンプレミスのADと連携する場合
 - AD Connector

ディレクトリタイプの選択

ディレクトリタイプ

- AWS Managed Microsoft AD
- Simple AD
- AD Connector
- Amazon Cognito ユーザープール

AWS Managed Microsoft AD

AWS Managed Microsoft AD により、Active Directory 対応ワークロードおよび AWS リソースから、AWS クラウド上の実際のマネージド型 Microsoft Active Directory を簡単に使用できます。ワークロードの例には、Amazon EC2、Amazon RDS for SQL Server、カスタム .NET アプリケーション、AWS エンタープライズ IT アプリケーション (Amazon WorkSpaces など) があります。

[詳細はこちら](#)

[ユースケースの表示](#)

キャンセル 次へ

WorkSpaces の作成

ディレクトリの選択

- ユーザーを認証するディレクトリサービスを選択

ディレクトリの選択

WorkSpaces を起動するディレクトリを選択します。ディレクトリには、ユーザーと WorkSpaces の両方が

ディレクトリ

セルフサービスアクセス許可の有効化 ⓘ はい いいえ

[新しいディレクトリの作成](#)

*Amazon WorkDocs は、Amazon Linux WorkSpaces 用のネイティブ Linux クライアントを提供していません。詳細については、

キャンセル

認証する
ディレクトリの指定

セルフサービスの
有効化設定

WorkSpaces の作成

ユーザーの追加

- ディレクトリへのユーザー作成
- ディレクトリのユーザー検索
- WorkSpaces を作成するユーザーの選択

ユーザーの特定

このディレクトリ内の既存のユーザー用に WorkSpace を作成するには、以下の検索結果からユーザーを選択し、[次へ] ボタンをクリックします。ユーザーの選択が完了したら、[次へ] をクリックして WorkSpace バンドルを選択します。

新規ユーザーを作成してディレクトリに追加します: aws-blackbelt.com

ユーザー名	名	姓	E メール	
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	削除

+ 追加ユーザーの作成 ユーザーの作成

ディレクトリからユーザーを選択: aws-blackbelt.com

検索 すべてのユーザーの表示

ユーザー名	名前
ユーザー名、名、姓、または E メールでユーザーを検索	
◀ < ユーザーなし > ▶	

選択項目を追加

1 WorkSpace (20 人のユーザーを一度に選択できます)

	ユーザー名	名前	E メール
✖	aws-blackbelt.com\kunimasa	Takechika Kunimasa	kunimasa@amazon.com

キャンセル 戻る 次のステップ

ユーザーの作成

ユーザーの検索

ユーザーの選択

WorkSpaces の作成

バンドルの選択

- 作成するバンドルを選択
 - OS 種類
 - CPU, メモリ, ボリューム
 - Office ライセンス有無
 - OS の言語
- バンドルサイズとストレージサイズを選択

バンドルを
ユーザーへ割り当て

バンドルの選択

ユーザーごとにコンピューティング、オペレーティングシステム、ストレージ、アプリケーションのバンドルを選択します。すべての Amazon Linux バンドルには Firefox、LibreOffice、Evolution、Python などのパッケージが含まれます。すべての Windows バンドルには Internet Explorer 11、Firefox、7-Zip の各アプリケーションが含まれます。Workspace が起動したら、独自のアプリケーションとパッケージを Workspace にインストールできます。Microsoft Office を含む Windows Plus バンドルの詳細については、[こちら](#)を参照してください。

すべてのバンドル ▾ すべてのハードウェア ▾ すべてのソフトウェア ▾

バンドル	CPU	メモリ	ルートボリューム	ユーザーボリューム
<input type="checkbox"/> Value with Amazon Linux 2	1 vCPU	2 GiB	80 GB	10 GB
<input type="checkbox"/> Standard with Amazon Linux 2 無料利用枠の対象	2 vCPU	4 GiB	80 GB	50 GB
<input type="checkbox"/> Performance with Amazon Linux 2	2 vCPU	7.5 GiB	80 GB	100 GB
<input type="checkbox"/> Power with Amazon Linux 2	4 vCPU	16 GiB	175 GB	100 GB
<input type="checkbox"/> PowerPro with Amazon Linux 2	8 vCPU	32 GiB	175 GB	100 GB
<input type="checkbox"/> Standard with Windows 7 無料利用枠の対象	2 vCPU	4 GiB	80 GB	50 GB
<input type="checkbox"/> Standard with Windows 10 無料利用枠の対象	2 vCPU	4 GiB	80 GB	50 GB
<input type="checkbox"/> Standard with Windows 7 and Office 2010	2 vCPU	4 GiB	80 GB	50 GB

言語 Japanese (日本語) ▾

OSの言語
選択

Workspace バンドルの割り当て

各ユーザーのバンドルサイズとストレージサイズを選択します。80 GB と 10 GB、80 GB と 50 GB、80 GB と 100 GB、175 GB と 100 GB のルートおよびユーザーボリュームサイズを選択するか、それぞれ最大 2000 GB までボリュームを拡張できます。ストレージのオプションの詳細については、[こちら](#)を参照してください。

ユーザー名	バンドル	言語	ルートボリューム	ユーザーボリューム
aws-blackbelt.com\kunimasa	Performance with Win ▾	Japanese (日本語) ▾	80	100

WorkSpaces の作成

WorkSpaces の設定

- 実行モードの選択
 - AlwaysOn
 - AutoStop, 自動停止時間
- 暗号化の選択
 - ボリュームの暗号化
 - 暗号化キー
- タグの管理

WorkSpaces の設定

実行モード

WorkSpaces の実行方法と支払い方法を選択します。詳細については、[こちら](#)を参照してください。

AlwaysOn
月単位で請求。常に実行中の WorkSpace に瞬時にアクセスします。

AutoStop **無料利用枠の対象**
時間単位で請求。WorkSpaces は、お客様がログインすると自動的に起動し、使用されなくなると停止します。

自動停止時間 (時間)

注意: 可能であれば、自動停止によってデスクトップの状態のスナップショットが WorkSpace のルートボリュームに作成されます。ユーザーが次に自分の WorkSpace にログインすると、WorkSpace は再開され、開いていたドキュメントや実行中だったプログラムはすべて前の状態に戻ります。WorkSpaces のセキュリティをさらに強化するために、すべてのストレージボリュームを暗号化することをお勧めします (以下を参照)。

暗号化

WorkSpaces のセキュリティをさらに強化するために、すべてのストレージボリュームを暗号化することをお勧めします。ボリュームの暗号化を設定するには、アカウントの KMS キーを使用する必要があります。IAM コンソールを使用して追加の KMS キーを作成することもできます。WorkSpaces の暗号化の詳細については、[こちらのドキュメント](#)を参照してください。

自分のキーでルートボリュームの暗号化

自分のキーでユーザーボリュームの暗号化

暗号化キー

タグの管理

タグを使用して WorkSpaces にメタデータを追加できます。さらに、これらのタグを使用して、AWS コストエクスペローラーでコストを追跡することもできます。タグは、大文字と小文字が区別されるキーと値のペアから構成されます。たとえば、キーに「Name」、値に「Webserver」を使用してタグを定義できます。[詳細はこちら](#)

キー	値
<input type="text"/>	<input type="text"/>

実行モードの
選択

暗号化の選択

タグの設定

WorkSpaces の作成

レビューと起動

- 設定内容を確認し、問題なければデプロイを開始

WorkSpaces のレビューと起動

1 個の新しい WorkSpace を起動しようとしています。以下の内容を確認してください。戻って編集するか、[WorkSpaces の起動] をクリックできます。

新しい WorkSpace

ユーザー名	バンドル	自動停止時間	ルートポリリ	ユーザーポリ	暗号化キー
▶ aws-blackb...	Performanc...	1 ↓	<input type="checkbox"/>	<input type="checkbox"/>	alias/aws/workspaces ↓

設定を確認して
デプロイ

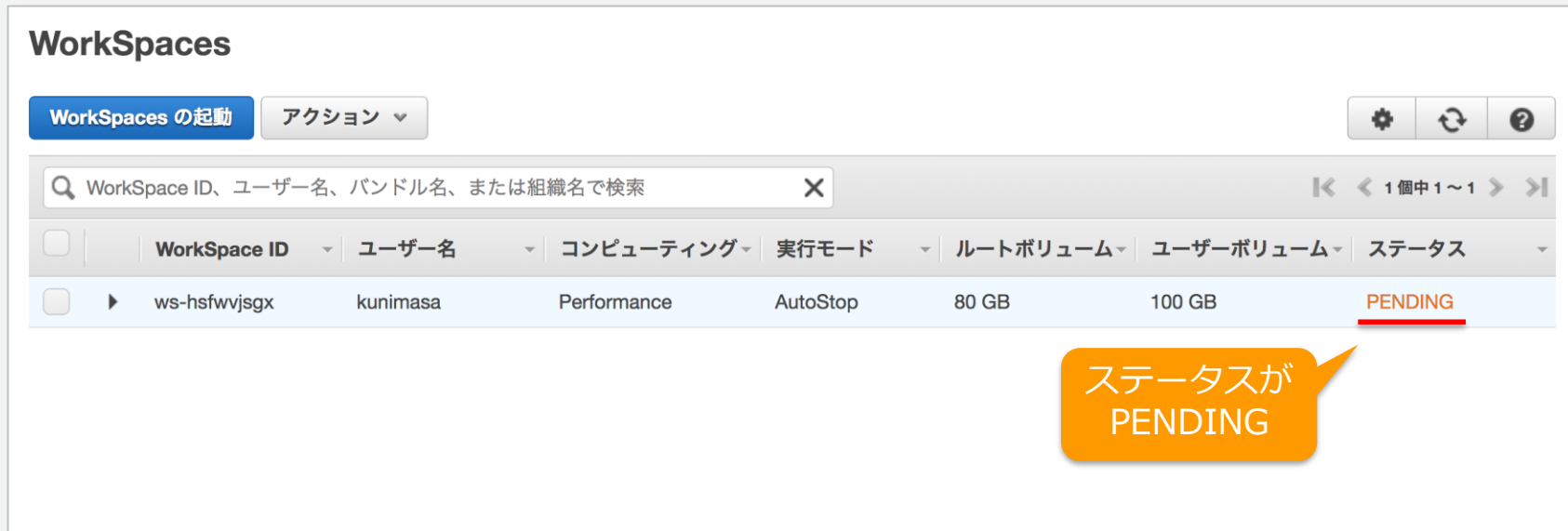
WorkSpaces は Tokyo リージョンで起動します

[キャンセル](#) [戻る](#) [WorkSpaces の起動](#)

WorkSpaces の作成

WorkSpaces のステータス確認

- ステータスが「PENDING」から「AVAILABLE」に変わったら作成完了



The screenshot shows the AWS WorkSpaces console interface. At the top, there's a header "WorkSpaces" with a "WorkSpaces の起動" button and an "アクション" dropdown menu. Below this is a search bar with the placeholder text "WorkSpace ID、ユーザー名、バンドル名、または組織名で検索". The main content area displays a table of WorkSpaces. The table has columns for "WorkSpace ID", "ユーザー名", "コンピューティング", "実行モード", "ルートボリューム", "ユーザーボリューム", and "ステータス". One workspace is listed with ID "ws-hsfwvjsgx", user "kunimasa", "Performance" computing type, "AutoStop" execution mode, "80 GB" root volume, and "100 GB" user volume. The status "PENDING" is highlighted in red and underlined. An orange callout bubble points to the "PENDING" status with the text "ステータスが PENDING".

WorkSpace ID	ユーザー名	コンピューティング	実行モード	ルートボリューム	ユーザーボリューム	ステータス
ws-hsfwvjsgx	kunimasa	Performance	AutoStop	80 GB	100 GB	<u>PENDING</u>

WorkSpaces の作成

WorkSpaces の作成完了

WorkSpaces

WorkSpaces の起動 アクション

WorkSpace ID、ユーザー名、バンドル名、または組織名で検索

WorkSpace ID	ユーザー名	コンピューティング	実行モード	ルートボリューム	ユーザーボリューム	ステータス
ws-hsfwvjsgx	kunimasa	Performance	AutoStop	80 GB	100 GB	AVAILABLE

ユーザー名: kunimasa
名前: Kunimasa, Takechika
Eメール: kunimasa@amazon.com
クライアントリンク: https://clients.amazonworkspaces.com/
登録コード: wsnrt+
エラーメッセージ: なし
接続状態: DISCONNECTED
前回アクティブだったユーザー: 情報がありません
前回の状態の確認: 2019/02/19 20:28:15

WorkSpace IP: 10.101.51.154
バンドルの起動: Performance with Windows 10 and Office 2016
言語: Japanese (日本語)
コンピューター名: IP-C6137B63
暗号化されたボリューム: なし
暗号化キー: なし
自動停止時間: 1 時間
状態: なし

タグ

現在この WorkSpace に関連付けられているタグはありません

ステータスが AVAILABLE に更新

WorkSpaces の作成

メールの受信とユーザーの登録

- メールを受信したらリンク先をブラウザで開いてパスワードを設定

日本語 (Japanese)

Amazon WorkSpaces をご利用のお客様へ

お客様の Amazon WorkSpace が管理者によって作成されました。さっそく以下の手順に従って、WorkSpace のご利用を開始してください。

1. ユーザーのプロファイルを入力し、次のリンクから WorkSpaces クライアントをダウンロードします。 https://d-95672af62d.awsapps.com/aut#invite:token=11eNbLrKjKRAjQD4J4GxvdSJI6p5anc-QdUozV95eQ3jLaHwkpMUkFpNuMe3HneAQ7S-OUu0bFTdC_9DwIncl07JikUHJMiNHbAjSNG9zsZ1iPCY_YP7Qff72_emSzEh1d9iKlwvu857EHPv9ljXF71-67QO3BdLmSqOPZqc95FfKhP6rIL_9HYPKZigg74-bkfkIgw4fw&redirect_uri=https://clients.amazonworkspaces.com/&client_id=0ef7da4

2. クライアントを起動し、次の登録コードを入力します。 wsnrt+XXXXXXXXXX

3. 新しく作成したパスワードを使ってログインします。お客様のユーザー名は「 kunimasa 」です。

クライアントは <https://clients.amazonworkspaces.com/> から他のデバイスにもダウンロードできます。

WorkSpace の接続に問題がある場合は、管理者にお問い合わせください。

よろしくお願いいたします。

Amazon WorkSpaces チーム

次の情報を設定してください
WorkSpaces 認証情報



ユーザーの更新

WorkSpaces クライアント

クライアントのダウンロード

- Amazon WorkSpaces Client Download
 - <https://clients.amazonworkspaces.com/>
- サポートされるプラットフォーム
 - Windows 7/8/10
 - Mac OS X (10.8.1)以降
 - iPad (iOS 8.0 or 9.0以降 *iPadの種類による)
 - 2012年以降にリリースされたKindle Fire、且つFire OS 4.0以降/Android 4.4以降のタブレット
 - Chrome OSバージョン45以降のChromebook
 - PCoIPゼロクライアント
- ネットワーク要件
 - TCP/UDP 4172
 - TCP 443 (HTTPS)
 - RTT 100ms以下を推奨



WorkSpaces クライアント

ネットワーク接続性の確認

- WorkSpaces クライアントでネットワークヘルスチェックが可能
 - ネットワーク接続
 - インターネット接続
 - WorkSpaces と関連するサービスへのアクセス
 - TCP/UDP 4172
 - 往復時間



WorkSpaces クライアント

クライアントの設定

- 登録コード
 - ディレクトリごとに固有のID
 - 登録コードを再入力することにより異なるディレクトリに接続が可能
- 言語設定
- Proxyを設定可能
 - 社内ネットワークからのProxy接続に対応 (TCP 443のProxyに対応)

amazon WorkSpaces

開始するには、管理者から提供された登録コードを入力してください

登録

ご使用のデバイスは WorkSpaces 登録サービスに接続できません。WorkSpaces を使用するデバイスを登録することはできません。ネットワーク設定を確認してください。

保存された登録はありません

ネットワーク

amazon WorkSpaces

言語を選択: 日本語

プロキシサーバーの設定:

プロキシサーバーを使用

アドレス: 127.0.0.1 ポート: 8080

このアカウントを記憶する

保存済み登録を有効にする:

保存 キャンセル

ネットワーク

WorkSpaces クライアント

WorkSpaces への接続



amazon WorkSpaces

次の情報を使用してログインしてください WorkSpaces 認証情報

ユーザー名

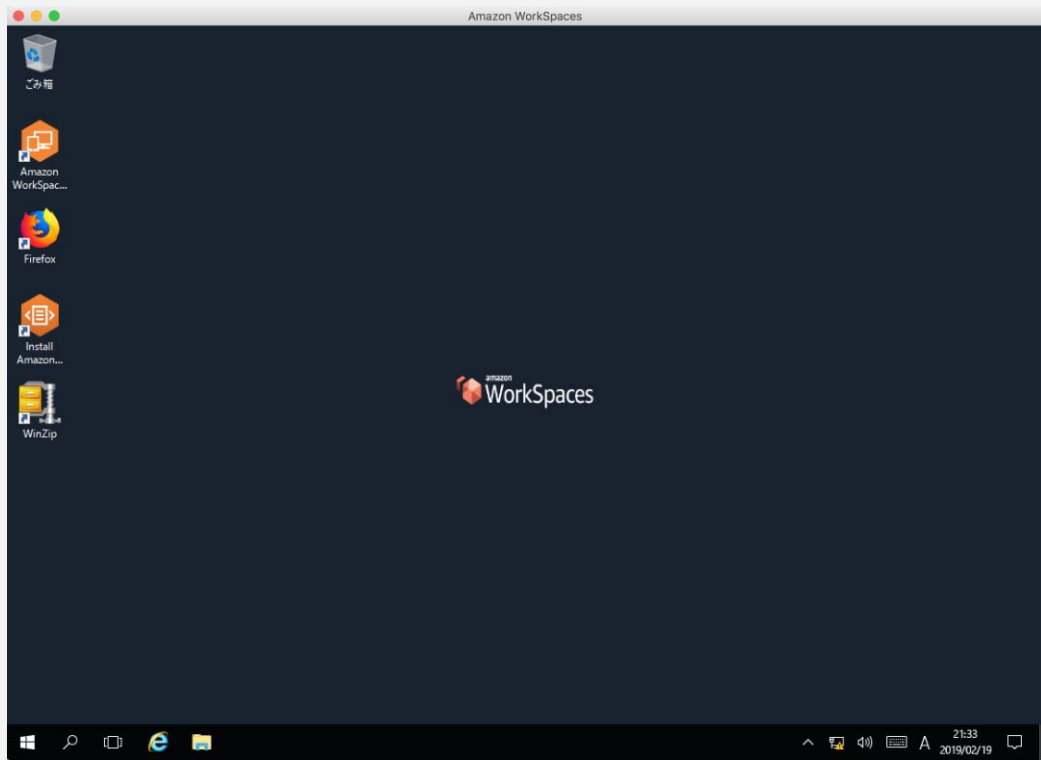
パスワード

サインイン

サインインしてアクセスを許可

パスワードを忘れた場合

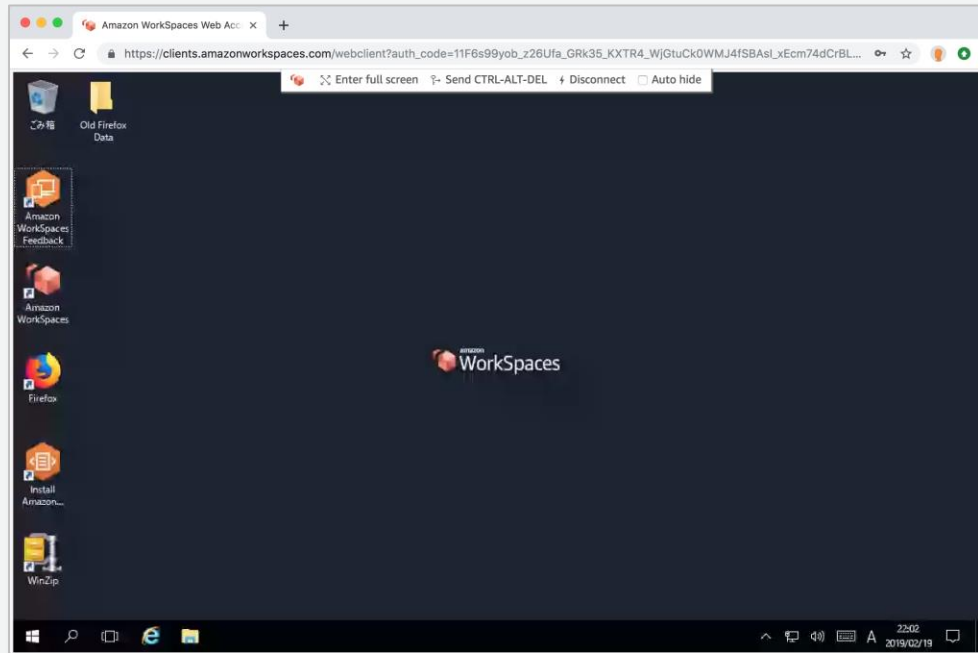
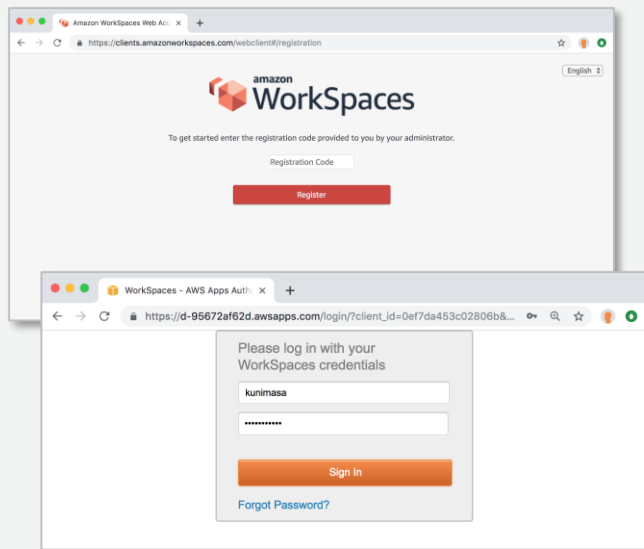
ネットワーク 



Web Access for Amazon WorkSpaces

WorkSpaces への接続

- Windows/Mac/Linux上のChromeまたはFirefoxからWorkSpacesにログイン可能
- Value/Standard/Performance/Power/PowerPro バンドルに対応

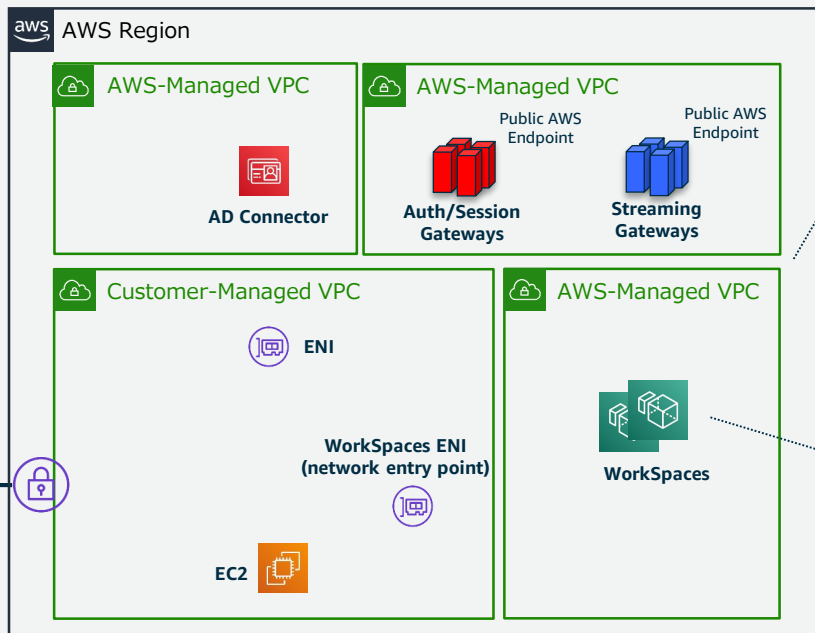
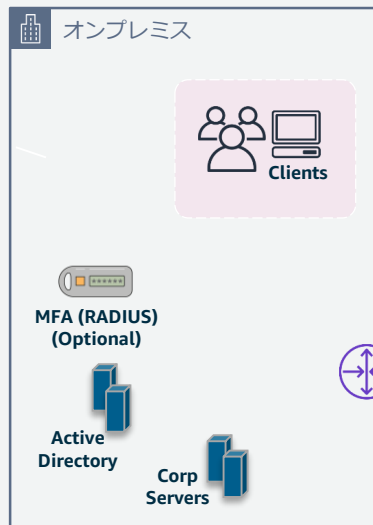
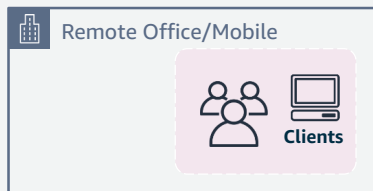


WorkSpaces のアーキテクチャ

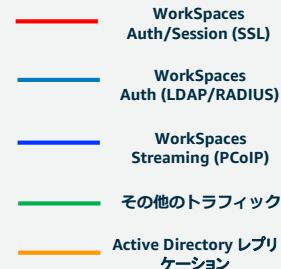
WorkSpaces のアーキテクチャ

- WorkSpaces へのログインフロー
- WorkSpaces 管理VPCとユーザーVPC
- デスクトップストリーミングプロトコル
- WorkSpaces の冗長構成
- ディレクトリサービス、既存ADドメインとの連携
- トラフィックフローとネットワーク接続
- セキュリティとアクセス制御

WorkSpaces へのログインフロー



NETWORK TRAFFIC LEGEND



AWSが管理するVPC

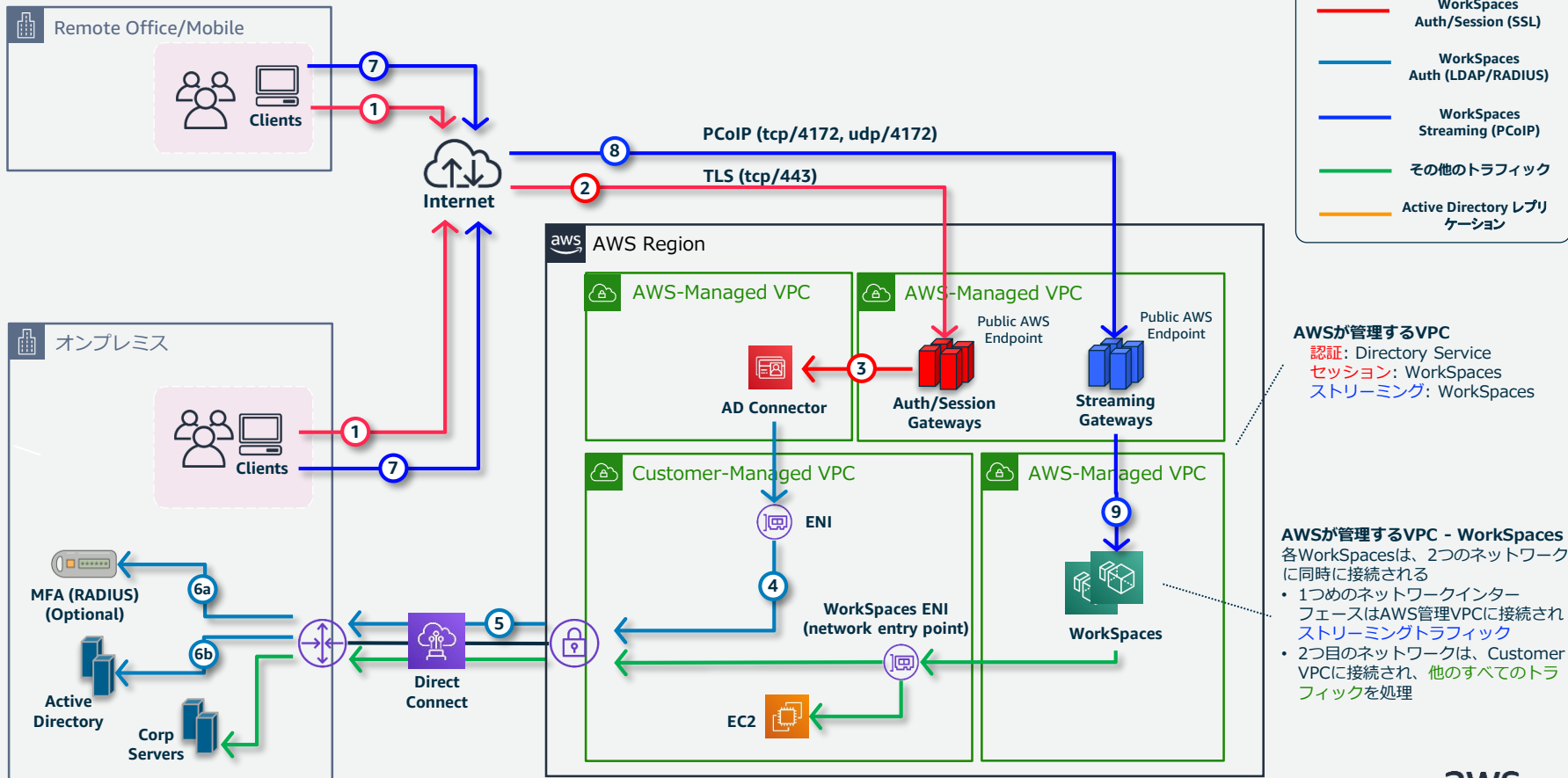
認証: Directory Service
 セッション: WorkSpaces
 ストリーミング: WorkSpaces

AWSが管理するVPC - WorkSpaces

各 WorkSpaces は、2つのネットワークに同時に接続される

- 1つめのネットワークインターフェースはAWS管理VPCに接続されストリーミングトラフィック
- 2つ目のネットワークは、Customer VPCに接続され、他のすべてのトラフィックを処理

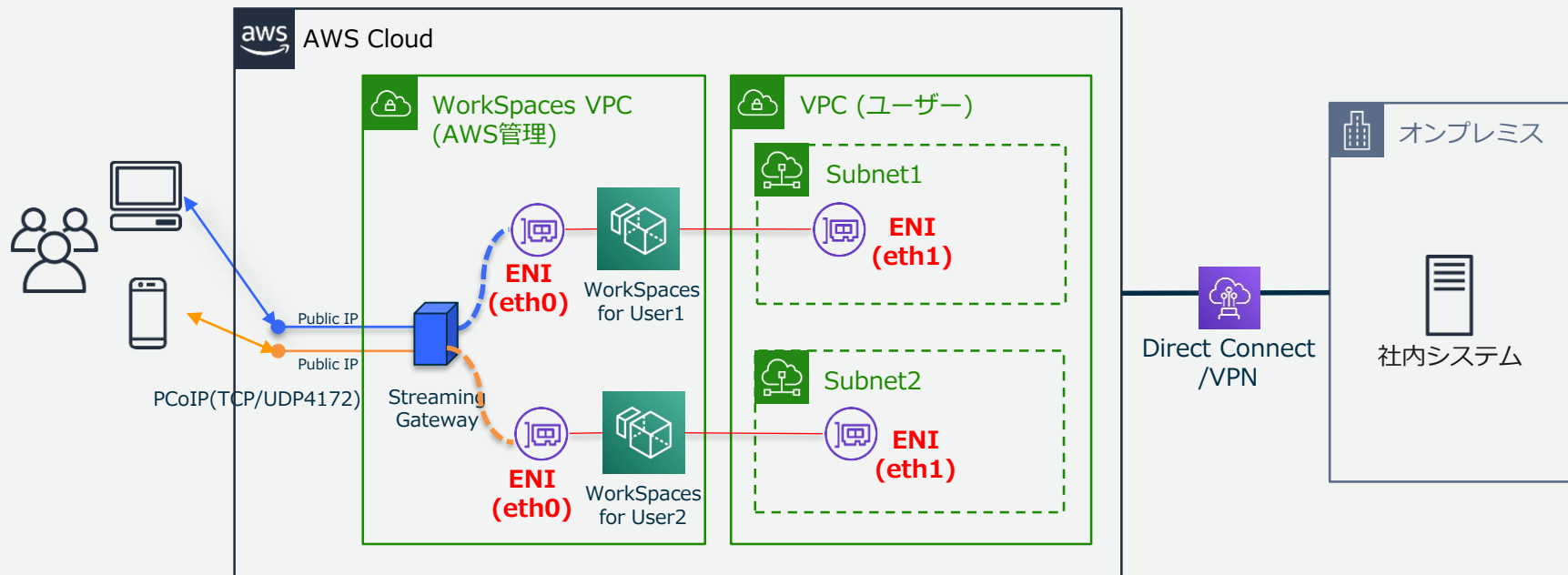
WorkSpaces へのログインフロー



WorkSpaces管理VPCとユーザーVPC

AWS管理VPCとユーザー用VPCに、それぞれENIが接続される

- プライマリネットワークインタフェース: ユーザーVPCに接続。SGをアタッチ
- 管理ネットワークインタフェース: AWS管理VPCに接続。ストリーミングを受信



デスクトップストリーミングプロトコル

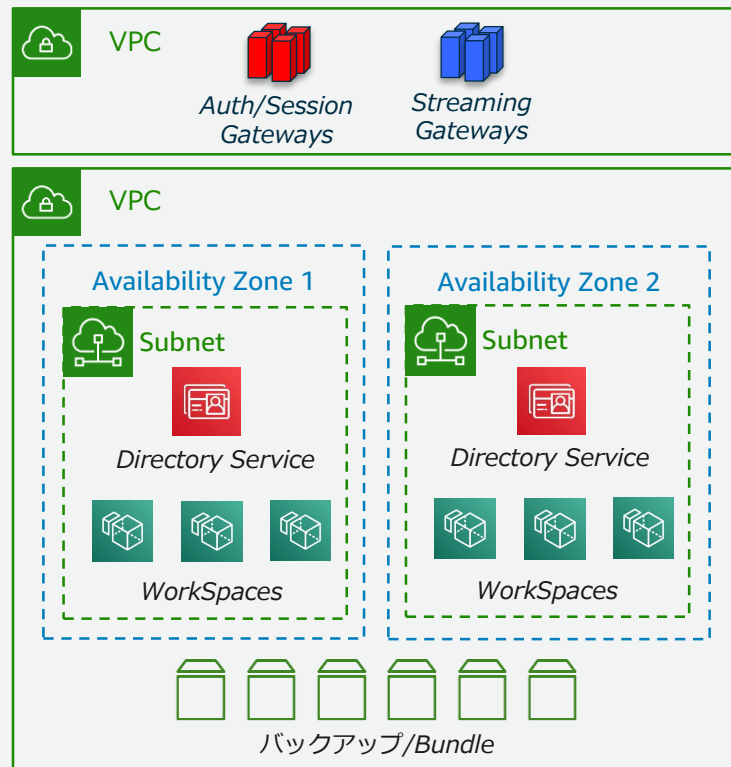
高品質で効率的なデスクトップストリーミングプロトコルを採用

- デスクトップストリーミングはPCoIPプロトコルを使用
 - Teradici 社が開発、仮想デスクトップで多くの実績がある
 - 高度な画像圧縮、ネットワーク帯域に合わせた最適化、マルチコーデック等により、高品質で効率的な画面ストリーミングを提供
- PCoIPの技術的な特徴
 - ポートTCP/UDP 4172を使用
 - TCP 4172 通信制御用、UDP 4172 でストリーミング
 - 通信は暗号化されている
 - 必要なネットワーク帯域は、利用方法とネットワーク状況に依存
 - ユースケースに沿った使い方で、実際のトラフィックを計測するのが確実
 - グループポリシーでポリシー制御可能

WorkSpaces の冗長構成

複数AZによる冗長構成、WorkSpaces障害時はWorkSpaces再起動または再構成

- 認証Gateway、Streaming Gateway
 - AWS管理VPC内で冗長化されており考慮不要
- Directory Service
 - 異なるAZの2つのサブネットにインスタンスが展開され、負荷分散と冗長性を確保
- WorkSpaces
 - WorkSpaces は Directory インスタンスが配置されるいずれかのサブネットにデプロイ
 - WorkSpaces 全体では均等に分散される
 - WorkSpaces 障害時は再構築により、バンドルイメージとバックアップから復旧
 - バンドルイメージ、ユーザーデータのバックアップ取得時点に戻ることに注意



ディレクトリサービス

AWS Directory Serviceを利用してデスクトップを認証、オンプレのADと認証連携

- AWS Directory Serviceを利用
 - 既存ドメイン連携する場合のDirectory Serviceの選択肢
 - Microsoft AD (ADドメインコントローラを提供)
 - AD Connector (AD Proxyを提供)
 - DNSサーバーを提供
 - ADドメインの名前解決
- WorkSpaces は Directory Service 単位で管理される
 - Directory Service 単位で Registration Code をもつ
 - WorkSpaces は、ディレクトリと同じサブネットに展開される
 - AD認証, MFA, 証明書, デバイス制御, セキュリティグループ, セルフサービス機能はDirectory Service単位で設定
 - これらのポリシーが異なる場合は、別ディレクトリとすることも考慮

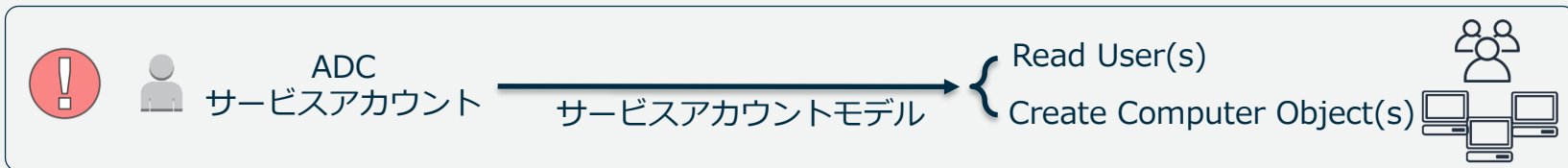
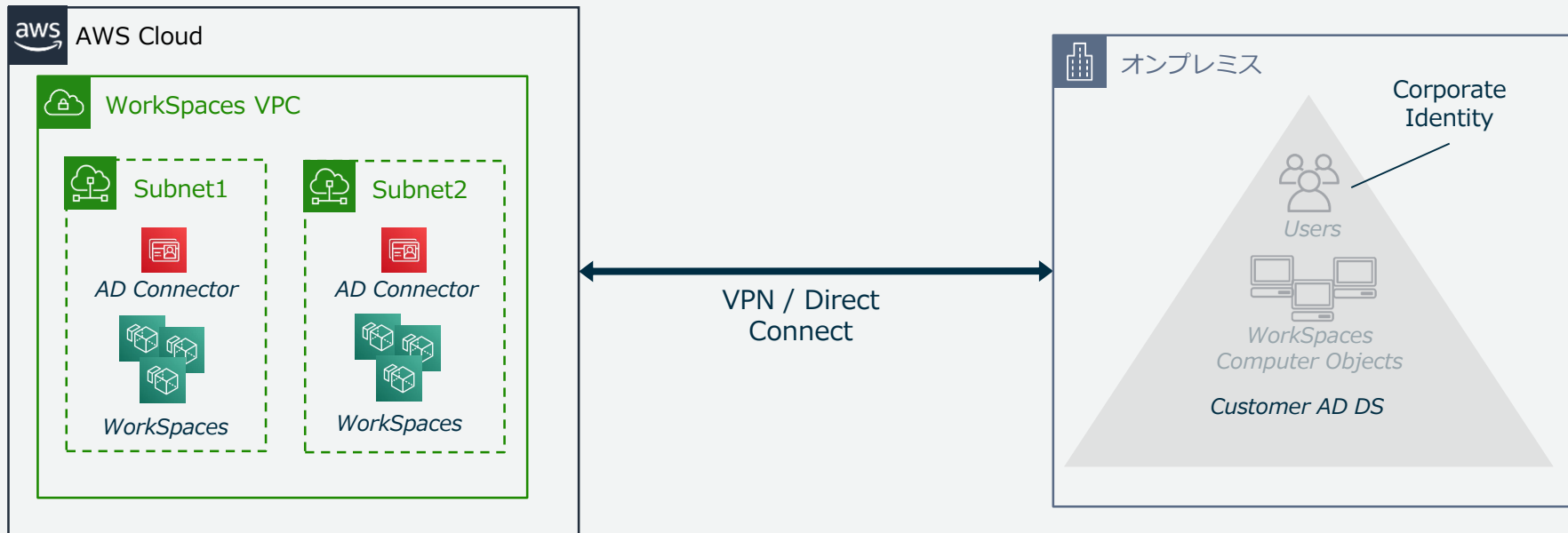
既存ADドメインとの連携

AWS Directory Serviceを利用してデスクトップを認証、オンプレのADと認証連携

- 既存ADドメインとの連携のオプション
 - AD ConnectorからオンプレミスADドメインへ認証をProxy
 - 既存ADドメインをVPCに拡張、AD Connectorで認証をProxy
 - AWS Microsoft ADとオンプレミスADドメインとの双方向の推移的信頼関係

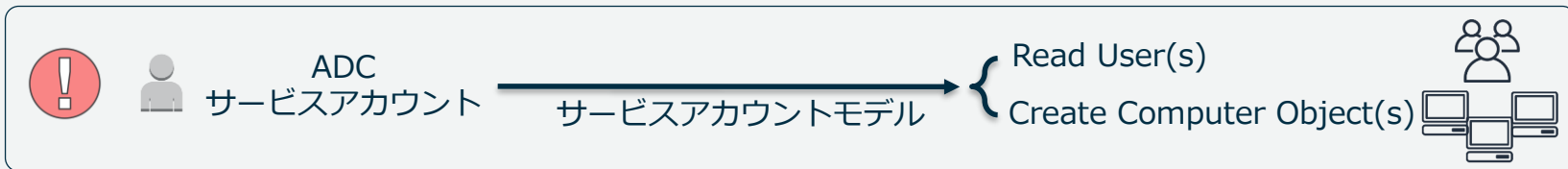
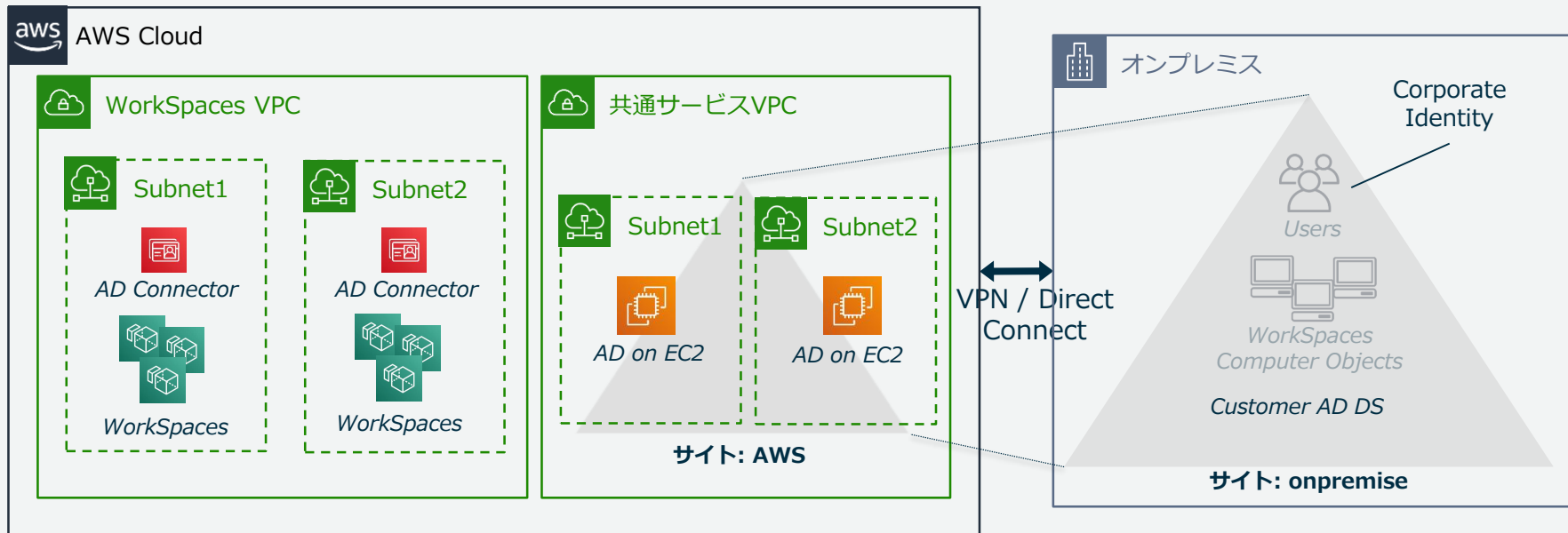
既存ADドメインとの連携

AD ConnectorからオンプレミスADドメインへ認証をProxy



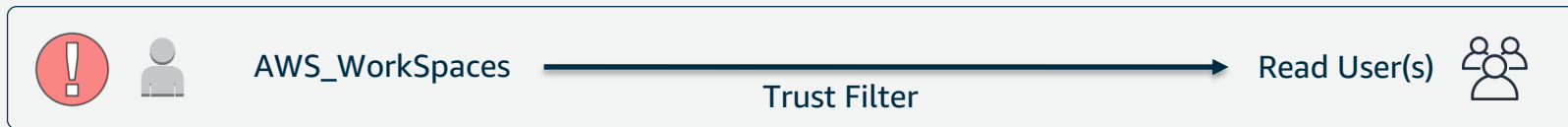
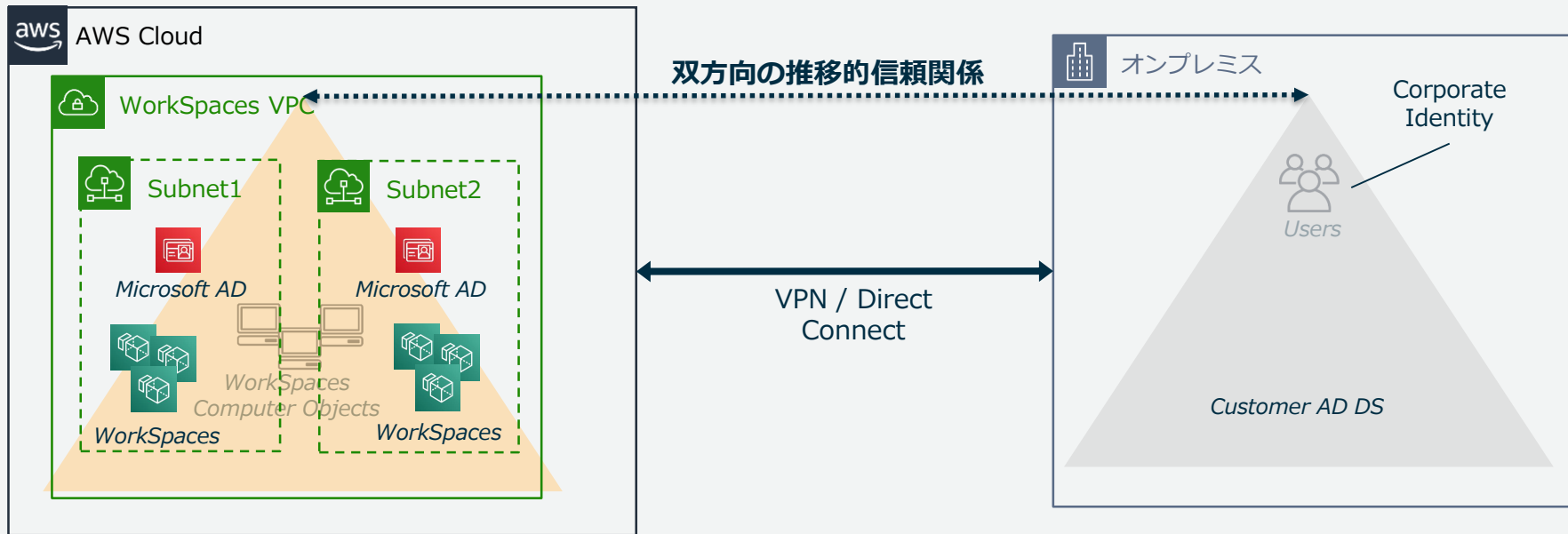
既存ADドメインとの連携

既存ADドメインをVPCに拡張、AD Connectorで認証をProxy



既存ADドメインとの連携

AWS Microsoft ADとオンプレミスADドメインとの双方向の推移的信頼関係



トラフィックフローとネットワーク接続

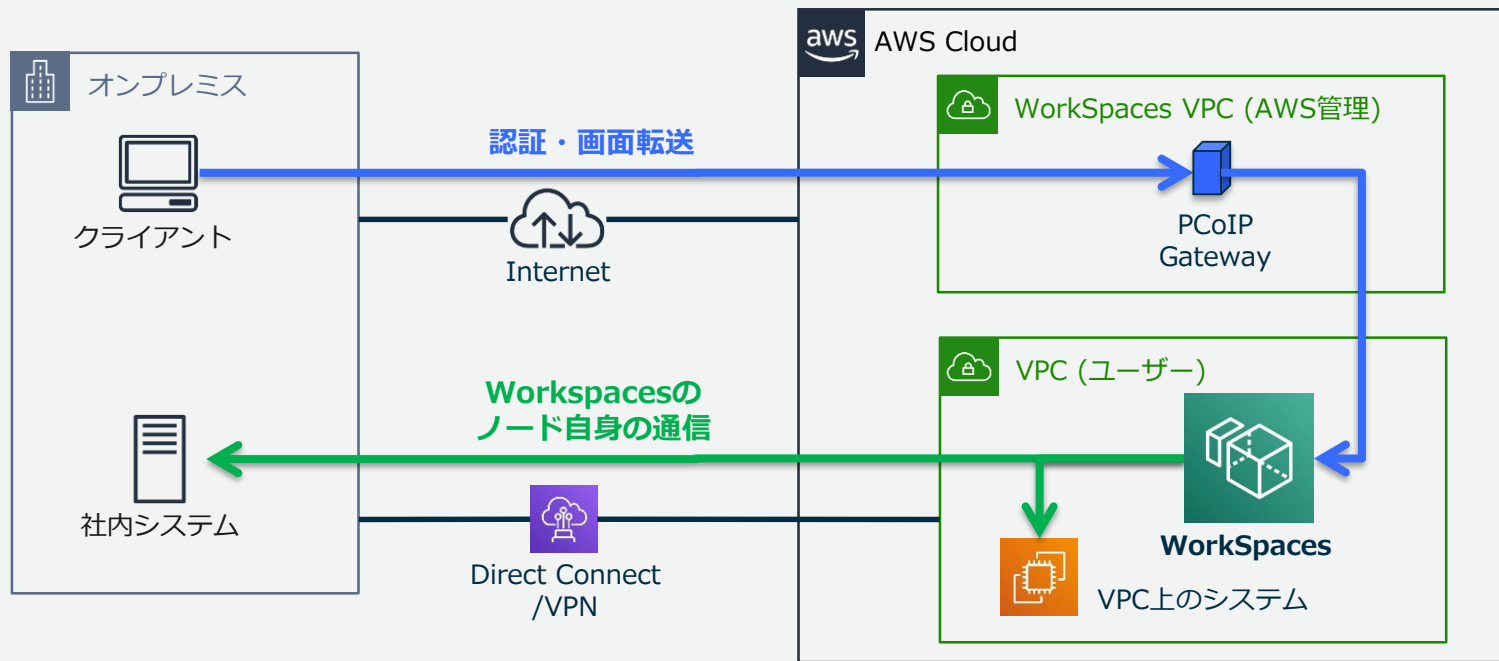
デスクトップストリーミングとユーザートラフィックの2種類のトラフィックを考慮

- デスクトップストリーミング (クライアント端末 - WorkSpaces)
 - インターネット経由
 - Direct Connect (Public接続)
- ユーザートラフィック (WorkSpaces - ユーザーVPC/オンプレミス/インターネット)
 - VPC
 - オンプレミス接続
 - Direct Connect
 - VPN
 - インターネット接続
 - Public IP Address 付与
 - NAT Gateway
 - オンプレミス Proxy

デスクトップストリーミング (インターネット経由)

画面ストリーミングはインターネット経由でアクセス

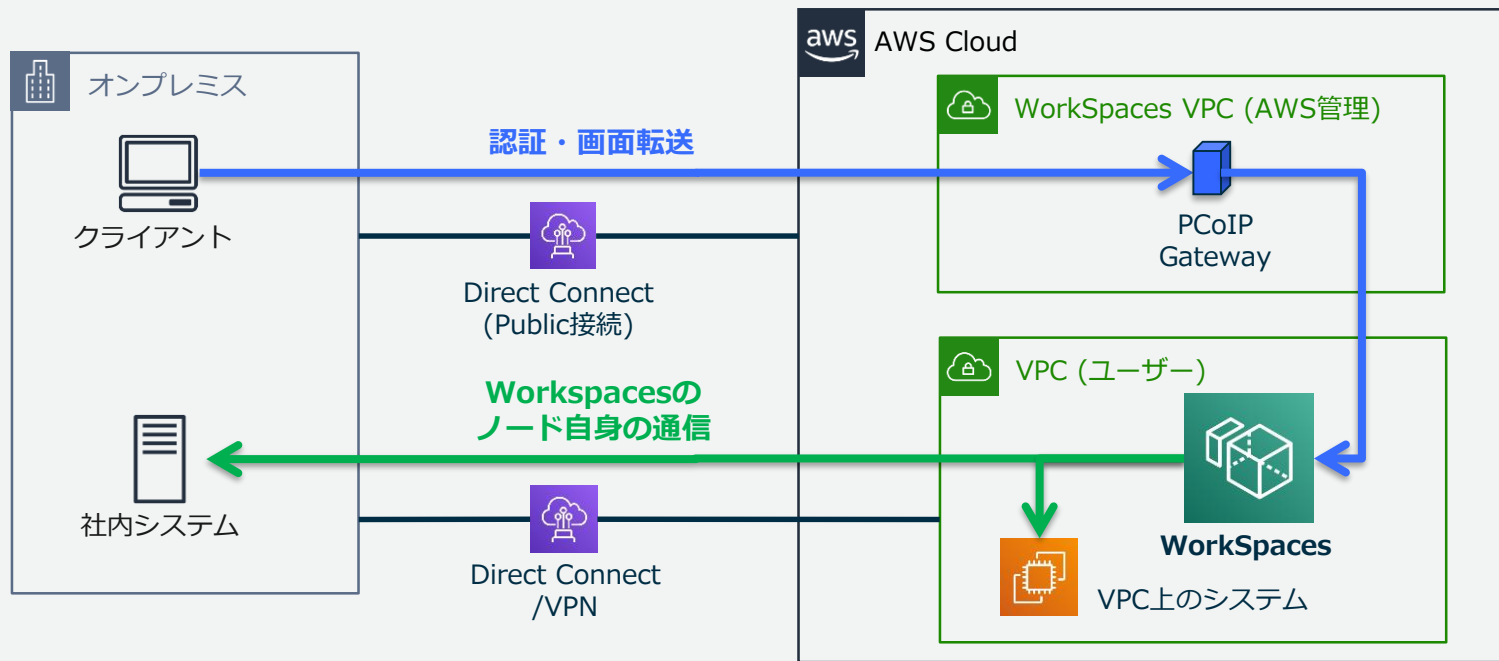
- デスクトップ画面へは、インターネット経由でどこからでもアクセスが可能
- 社内システムへは、専用線経由でセキュアに一貫した性能でアクセス



デスクトップストリーミング (DX Public接続経由)

DX Public 接続を利用することにより画面転送も専用線経由に

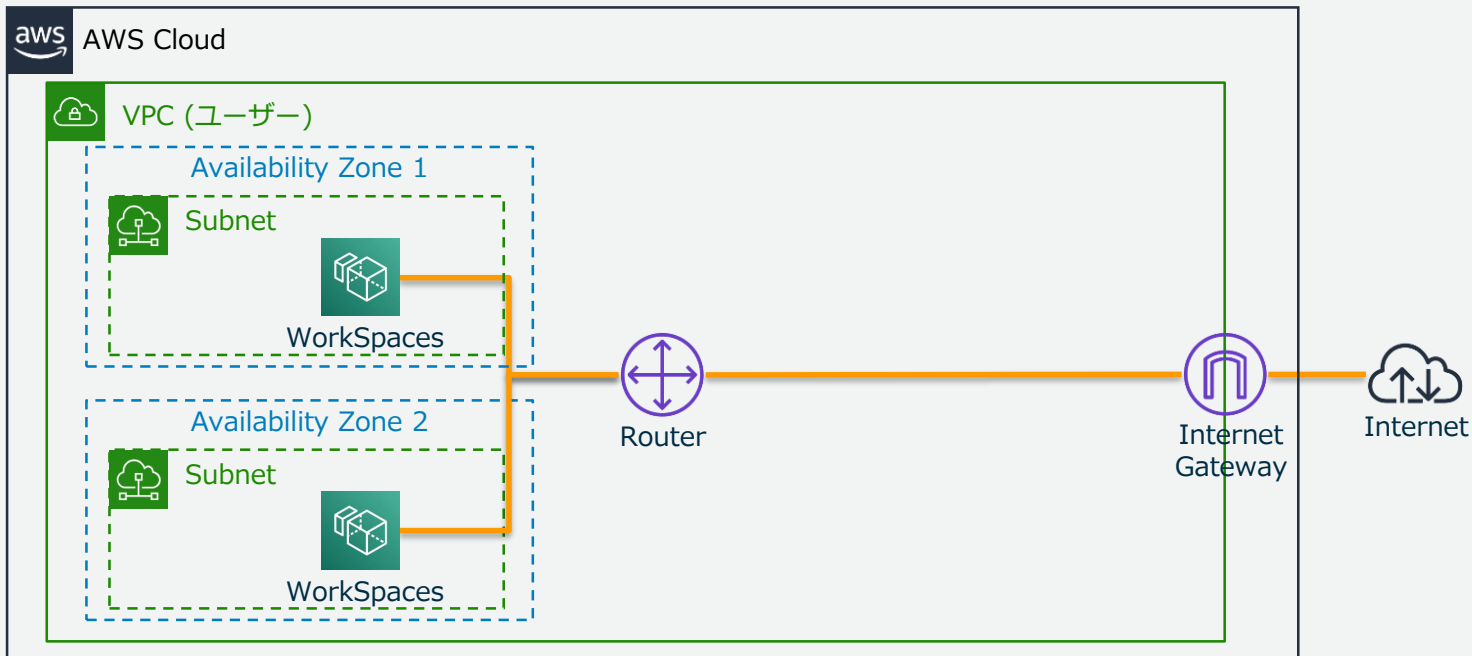
- DX Public接続により、画面ストリーミングも専用線経由でのアクセスが可能
- 一貫した高い性能を求める場合や、ポリシーとしてインターネット接続禁止の場合に検討



WorkSpaces からのインターネット接続

Public IP Address (Elastic IP) 付与

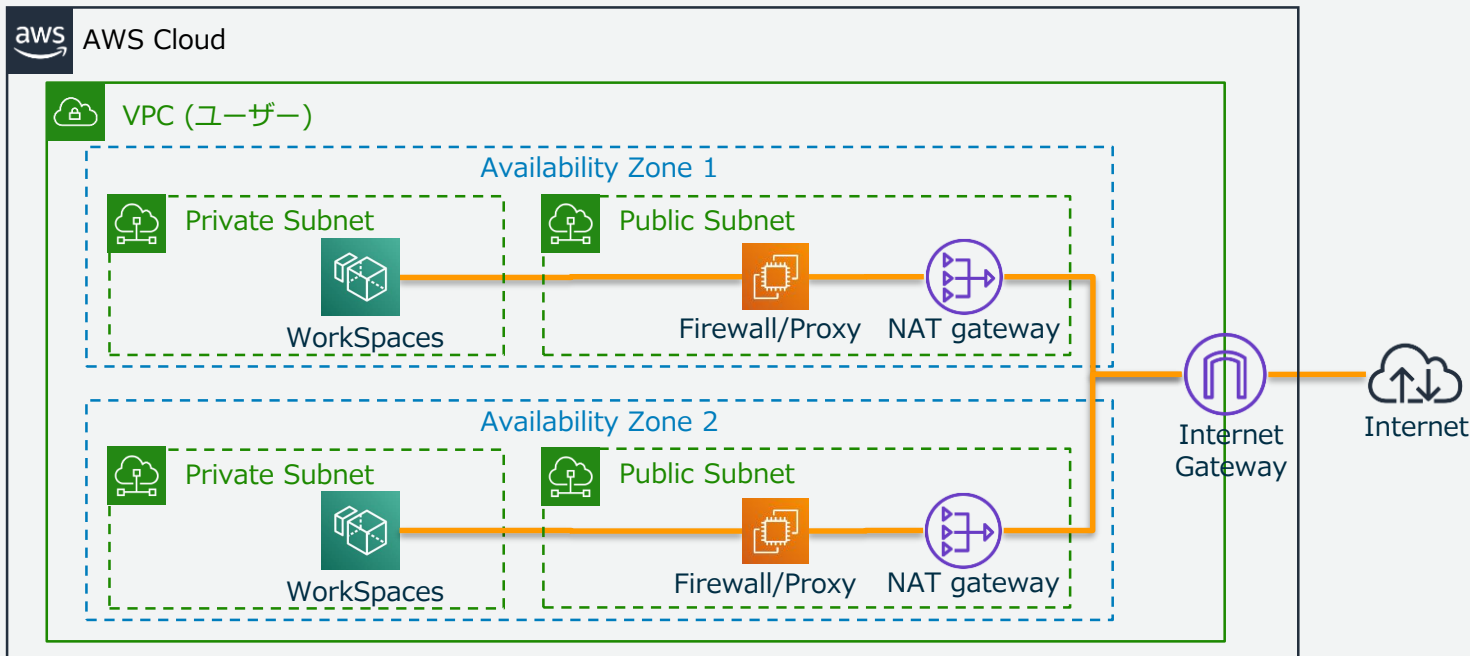
- WorkSpaces に EIP を付与し AWS からインターネットへアクセス
- ディレクトリ設定からPublic IPによるインターネットアクセスを設定可能



WorkSpaces からのインターネット接続

NAT Gateway 経由

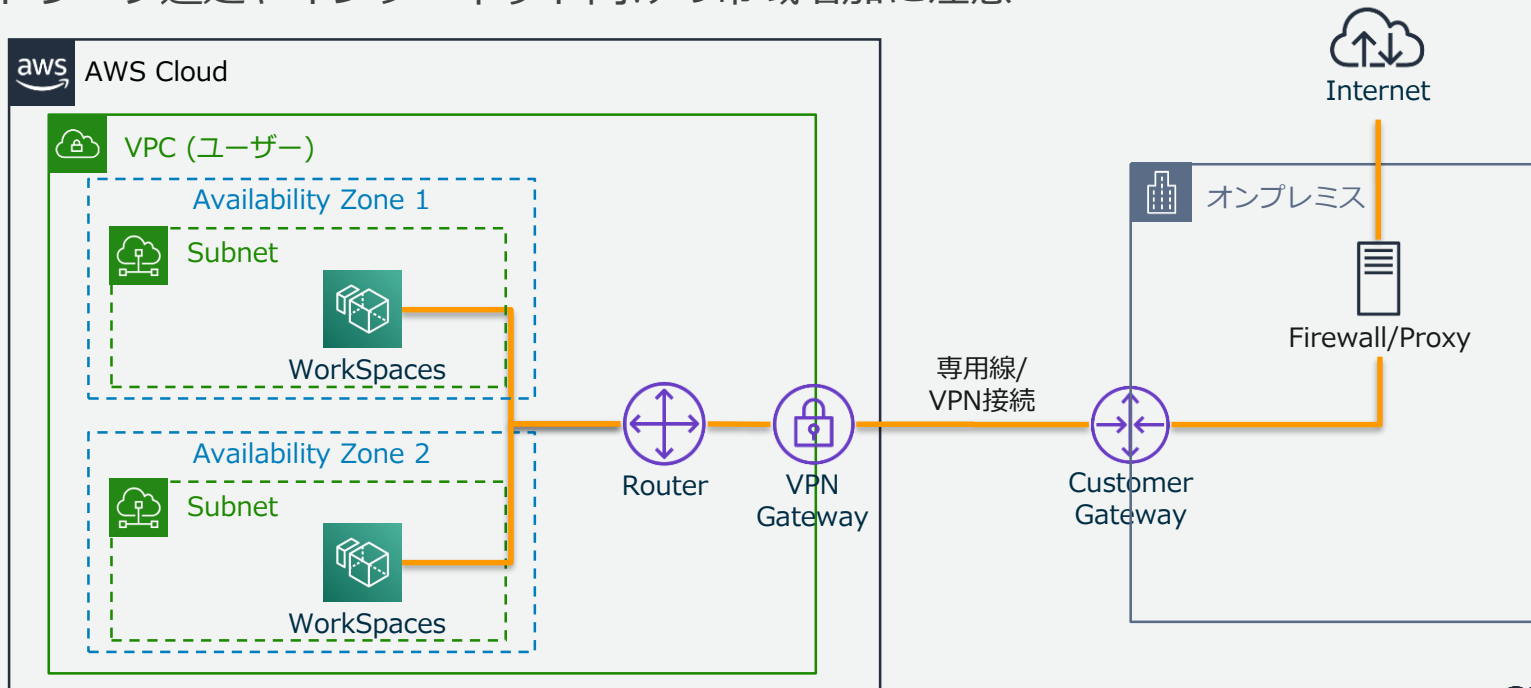
- NAT Gateway を経由してAWSからインターネットへアクセス
- Firewall や Proxy でセキュリティポリシーを実装



WorkSpaces からのインターネット接続

オンプレミス Proxy 経由

- オンプレ経路でインターネットにアクセス。既存と同じセキュリティポリシーを適用
- ネットワーク遅延やインターネット向けの帯域増加に注意



セキュリティとアクセス制御

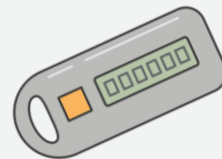
マルチレイヤーでのアクセス制御を提供

- ユーザー認証
 - ADドメイン認証
 - MFA (Multi-Factor Authentication)
- IPアドレスによるアクセス制御
 - IP アクセスコントロールグループ
 - セキュリティグループ
- デバイスによるアクセス制御
 - 証明書によるアクセス制限 (Windows/Mac OS X)
 - デバイスタイプによる制限 (その他デバイス)
- グループポリシーによるポリシー制御
 - Active Directory のグループポリシーによる制御

ユーザー認証

MFA (Multi-Factor Authentication)

- MFA
 - ユーザー名, パスワードと独立した要素での認証により、保護のレイヤーを追加
- RADIUSと連携
 - 各種RADIUSサーバー, OneLogin, Duo Security 等の SaaSのRADIUSとも連携可能
 - ディレクトリ単位で設定
 - ディレクトリのセキュリティグループでOutbound UDP/1812を許可



多要素認証 (MFA) の有効化

RADIUS ステータス
-

表示ラベル

最大 64 文字。

RADIUS サーバーの DNS 名または IP アドレス
RADIUS サーバーの IP アドレスをカンマ区切りリストで指定します。

カンマで区切った、有効なドメイン名である必要があります。

ポート
このポートを使用して既存の RADIUS サーバーに接続し、多要素認証を行います。

値は 1025~65535 の間である必要があります。

共有シークレットコード
このディレクトリと RADIUS サーバーの間で共有されるシークレットコード。

8~512 の長さにする必要があります。

確認済みの共有シークレットコード

上の共有シークレットコードに一致する必要があります。

プロトコル
認証用のプロトコルを選択します。

これは必須です。

サーバータイムアウト (秒単位)
各 RADIUS リクエストのタイムアウトを秒単位で指定します。

最大 50

RADIUS リクエストの最大再試行数
各 RADIUS リクエストに許可される最大再試行回数。

最大 10

IP アドレスによるアクセス制御

IP アドレスに基づいたアクセスコントロール

- IP アクセスコントロールグループ
 - 信頼できるネットワークからのみ WorkSpaces へのアクセスを許可
 - 許可する接続元IPアドレス/レンジを指定
 - デフォルトでは全てのトラフィックが許可

New
2018.8月

- セキュリティグループ

- ディレクトリ用 <directory_id>_controllers
 - ADドメイン連携のためのルールが登録済
 - MFA設定時は、OutboundでRADIUSへのアクセス許可追加が必要 (UDP 1812)
- WorkSpaces用 <directory_id>_workspacesMembers
 - WorkSpaces のプライマリインタフェースのネットワークアクセスを制御
 - デフォルトセキュリティグループに加えてSGの追加が可能

▼ IP アクセスコントロールグループ

警告 - IP アクセスコントロール機能の使用中は、Teradici の PCoIP Connection Manager を使用するゼロクライアントは WorkSpaces にアクセスできません

IP アクセスコントロールグループは、ユーザーが WorkSpaces への接続元として使用できる IP アドレスを制御します。このディレクトリに適用する IP アクセスコントロールグループを以下で選択できます。既存の IP アクセスコントロールグループを作成または変更するには、[IP アクセスコントロール](#) のページに移動します

ディレクトリに関連付ける IP アクセスコントロールグループを選択します

グループ ID	グループ名	説明
<input checked="" type="checkbox"/>	wsipg-gzxn2mt3h	ip-address-group-allow

▼ セキュリティグループ

セキュリティグループの追加

Amazon VPC で WorkSpaces ネットワークインタフェースに追加するセキュリティグループを選択します。このセキュリティグループは、このディレクトリ内の WorkSpaces 用に作成された WorkSpaces セキュリティグループに加えて、適用されます。

WorkSpaces に追加するセキュリティグループを選択します

workspaces

デバイスによるアクセス制御

証明書/デバイスタイプによるアクセス制御

- Windows および Mac OS X
 - クライアントアクセスを制御するためクライアント証明書を利用
 - SCCM (System Center Configuration Manager) や MDMなどによる証明書配布・管理との組み合わせ
- その他のクライアントデバイス
 - 以下のデバイスタイプ毎にアクセス許可・拒否を設定
 - Webブラウザ (Web Access)
 - iOS
 - Android
 - Chrome OS
 - ゼロクライアント

▼ アクセス制御のオプション

Windows および MacOS ● 許可 ● ブロック

信頼されたデバイスへの WorkSpaces アクセスを制限する前に、クライアント証明書が信頼されたすべてのデバイスにデプロイされていることを確認してください。次に、続行して一致するルート証明書をここにインポートできます。WorkSpaces は最大 2 つのルート証明書をサポートします。

- 信頼された Windows デバイスのみに WorkSpaces へのアクセスを許可
- 信頼された MacOS デバイスのみに WorkSpaces へのアクセスを許可

ルート証明書 1

base64 エンコード証明書を CRT/CER/PEM 形式でインポートしてください。

ルート証明書 2

base64 エンコード証明書を CRT/CER/PEM 形式でインポートしてください。

その他のプラットフォーム ● 許可 ● ブロック

WorkSpaces へのアクセスを有効にするデバイスタイプを選択してください。

- Web Access
- iOS
- Android
- ChromeOS
- ゼロクライアント

グループポリシーによるポリシー制御

グループポリシーによりデスクトップやOS上での挙動を制御

- Amazon WorkSpaces 固有のグループポリシー
 - WorkSpaces 用の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で利用可能
 - ポリシーテンプレートファイル
 - 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
 - セッションレジュームのタイムアウト
 - PCoIPストリーミングの暗号強度
- 従来の一般的な Windows のグループポリシーも利用可能

アーキテクチャの選択肢サマリー

- **既存ADドメインとの連携**
 - AD Connector
 - AD Connector + AD on EC2
 - Microsoft AD + 信頼関係
- **ネットワーク接続**
 - デスクトップストリーミング
 - インターネット
 - Public DX
 - ユーザートラフィック
 - オンプレミス接続
 - DX / VPN
 - インターネット接続
 - Public IP Address 付与
 - NAT Gateway
 - オンプレミス Proxy 経由
- **セキュリティとアクセス制御**
 - ユーザー認証
 - IPアドレスによるアクセス制御
 - デバイスによるアクセス制御
 - グループポリシーによるポリシー制御
- **クライアント**
 - WorkSpaces Client
 - Web Access

デザインパターン

想定するシナリオ

- 既存のAWSのお客様
- オンプレミスとクラウド上のアプリによるハイブリッドアーキテクチャ
- AWS Direct Connectを利用している
- 既存のActive Directoryを使用した認証、単一ドメイン
- 2,000+ ユーザーを想定、追加ユーザーは現在のドメインに登録される



BYOD



合併と買収

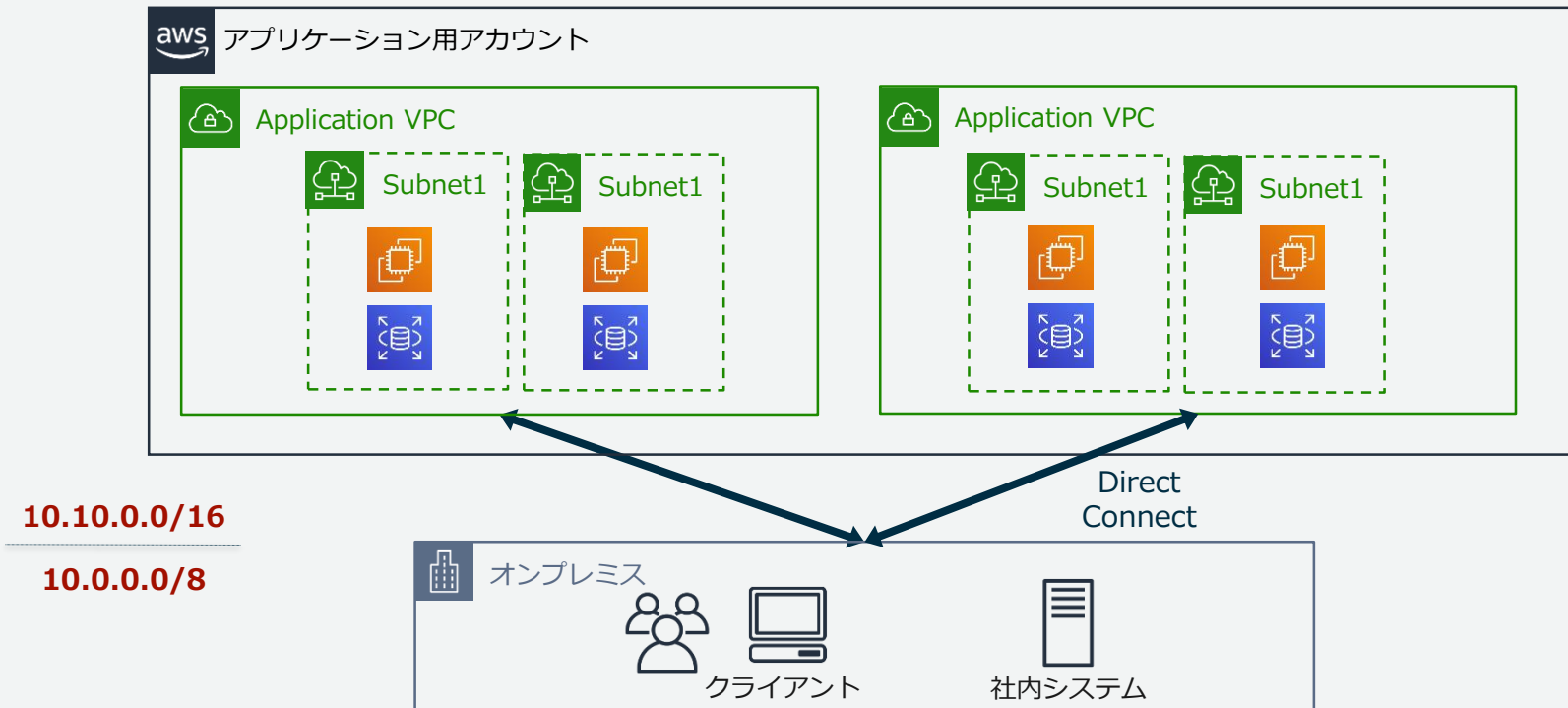


モバイルワーカー



データのセキュア化

既存のアーキテクチャ例



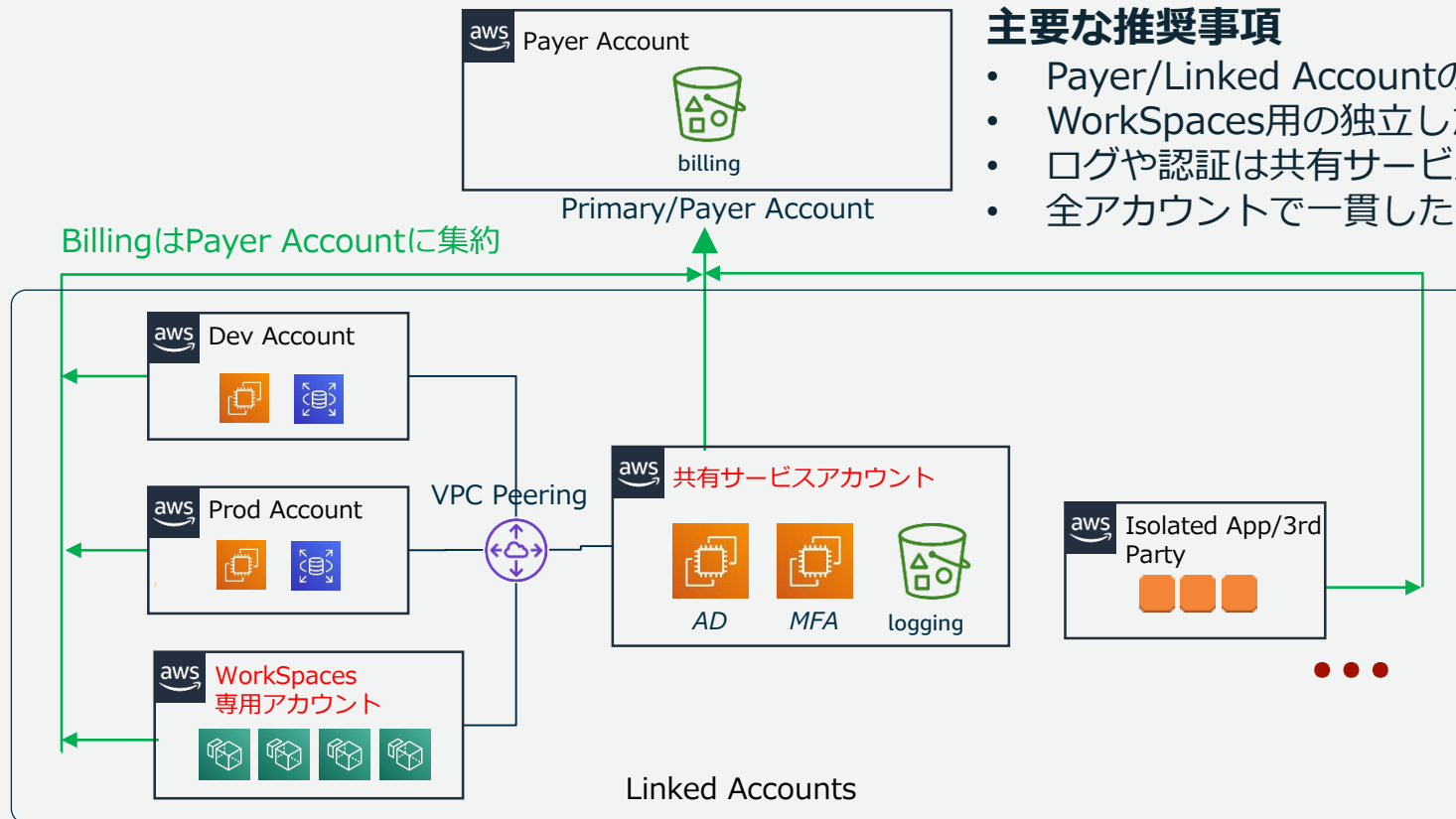
ユースケース、要件の収集

まず最初に、ユースケースや要件を収集して整理することが重要

- **長期的に必要なになる WorkSpaces の数は? 予測される増加の程度は?**
 - サブネットのサイズの決定
- **ユーザーのタイプは?**
 - 業務の種類、機密性、アクセス方法、認証・アクセス制限、セルフサービスの必要性等に応じたペルソナを定義
 - 社内/モバイル、端末デバイス種類
 - MFA有無、IP制限の必要性
 - セルフサービス許可
 - これらはDirectory Service単位で適用されるため、必要に応じて分割
- **接続する Active Directory ドメインの数は?**
 - 単一ドメインか、複数ドメインか
 - 既存ドメインの設計ポリシー

AWSアカウントの構造

アプリケーションや用途に応じてAWSアカウントを分割、課金はPayerアカウントに集約



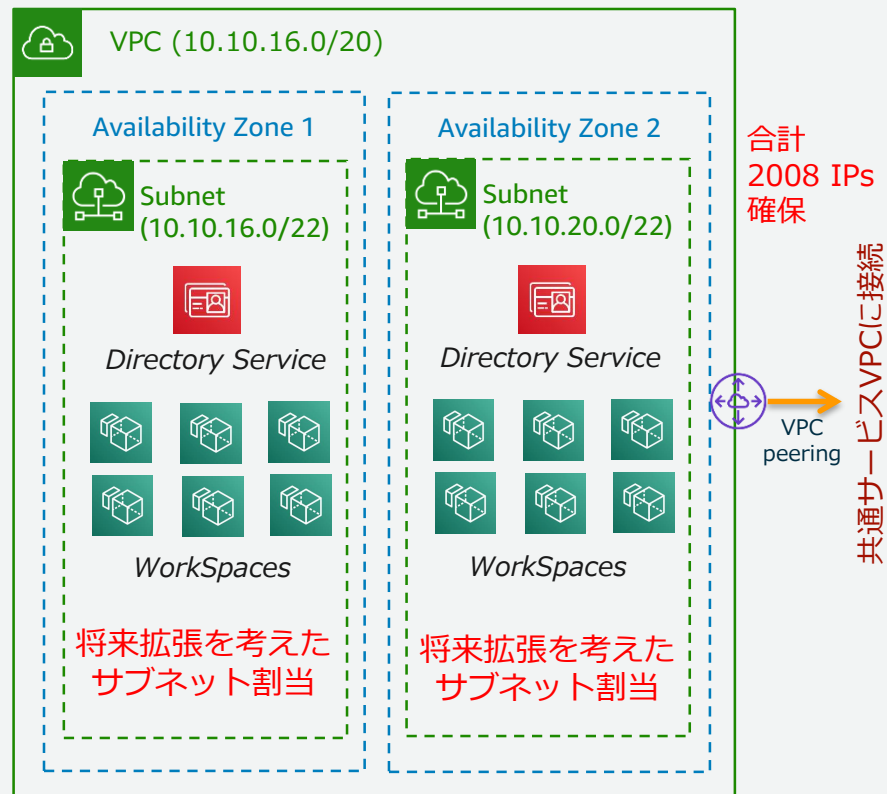
主要な推奨事項

- Payer/Linked Accountの構造
- WorkSpaces用の独立したアカウント
- ログや認証は共有サービスに集約
- 全アカウントで一貫したタグ付けを実装

VPC、サブネットの設計

将来の拡張を考慮してサブネットのIPアドレスリングを設計

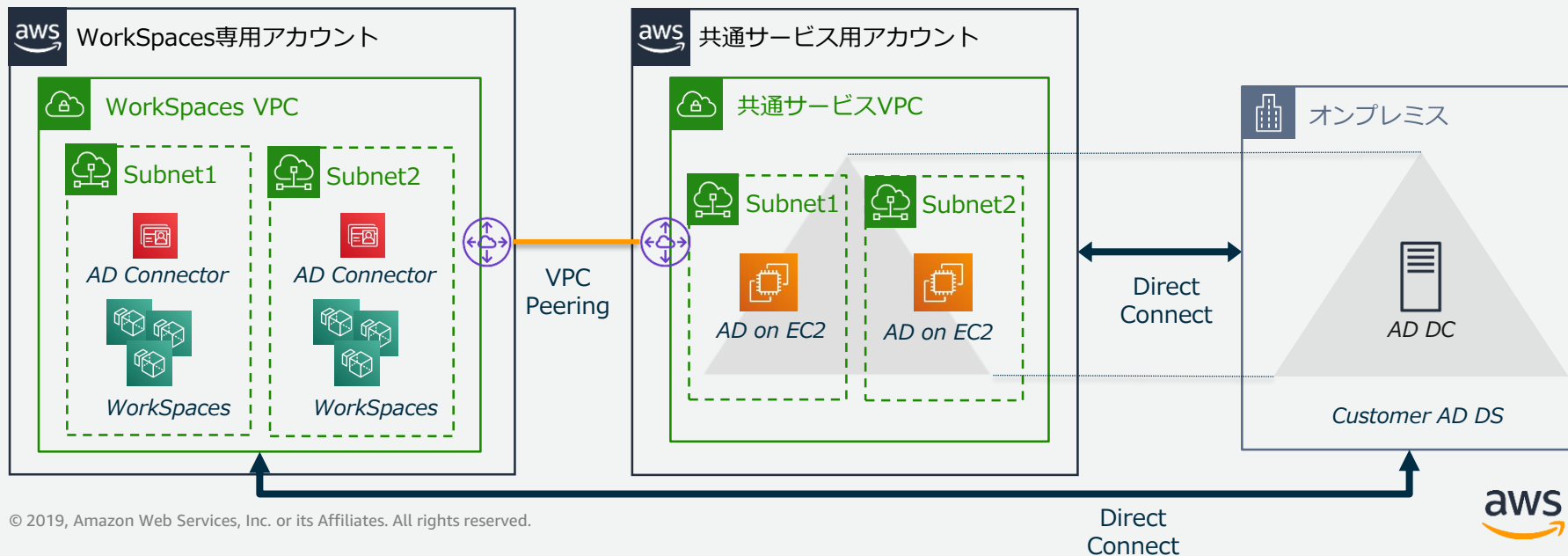
- WorkSpaces用の専用VPCを作成
- 最小2つのサブネット
- IP枯渇を避けるため、将来の拡張性を考慮してサブネットを作成
- イニシャルで2,000台のWorkSpacesと成長の余地
- 共有サービス用のVPCの使用



ディレクトリ展開のコンセプト

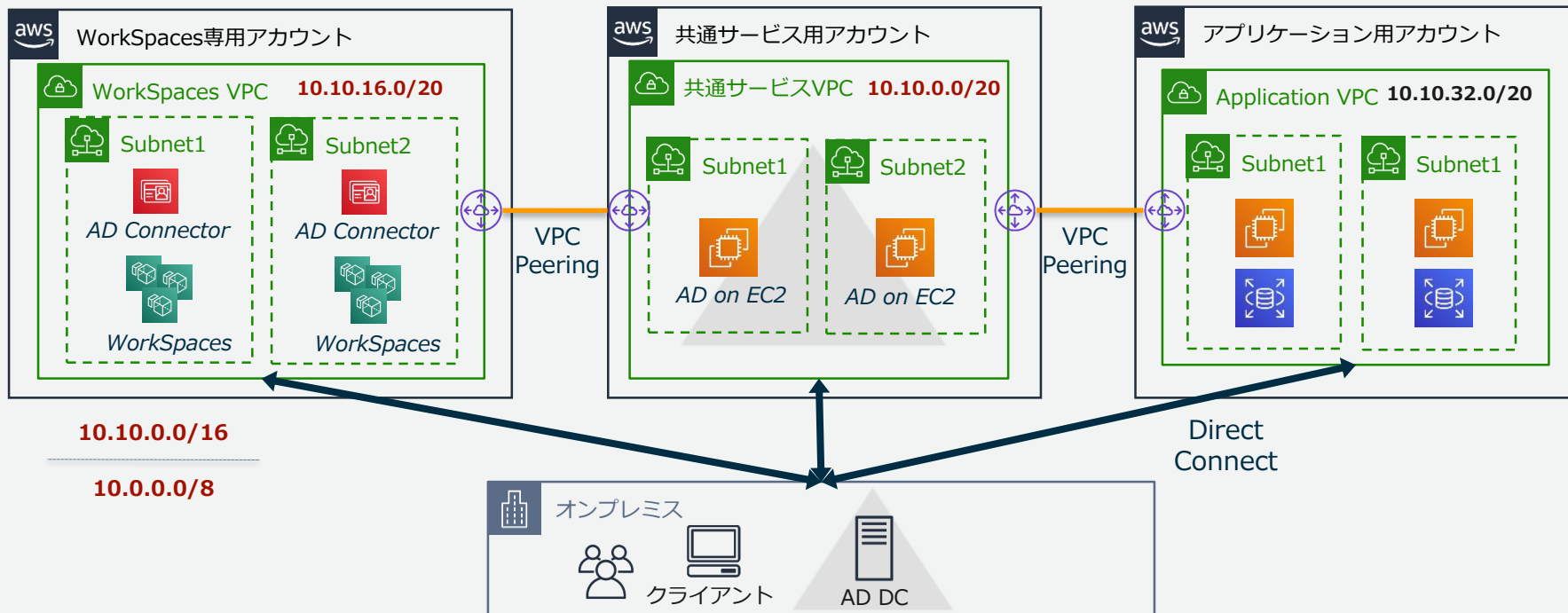
ドメイン数やNW遅延、レプリケーション低減を考慮した認証連携・ドメイン設計

- 単一ドメインのため、AD Connectorを利用
- Active DirectoryをEC2上に構成し、オンプレのADドメインをAWSに拡張
- オンプレミスとはサイトを分けて構成、ドメコン間の不要なレプリケーションや認証遅延を低減
- 共通サービスVPCとは、クロスアカウントのVPC Peering経由で通信



最終的なアーキテクチャ構成例

アーキテクチャ上の選択における決定期理由を説明できることが重要



Amazon WorkSpaces まとめ

- フルマネージド型の仮想デスクトップサービス
- セキュアなデスクトップ環境
- 初期投資が不要で、今日から 1 台から始められる
- 既存ディレクトリや様々なAWSサービスと連携可能
- 適切なアーキテクチャ設計が重要

参考情報

Amazon WorkSpacesをデプロイするためのベストプラクティス

- https://d1.awsstatic.com/International/ja_JP/Whitepapers/Best_Practices_for_Deploying_Amazon_WorkSpaces.pdf

Amazon WorkSpaces Deep Dive アーキテクチャ設計と展開のベストプラクティス

- <https://d1.awsstatic.com/events/jp/2018/summit/tokyo/aws/28.pdf>

多要素認証による Amazon WorkSpacesの利用

- <https://www.slideshare.net/AmazonWebServicesJapan/amazon-workspaces-86568155/11>

Active Directory証明書サービス (AD CS) による
Amazon WorkSpacesマネージドデバイス認証の構成

- <https://aws.amazon.com/jp/blogs/news/configure-managed-device-authentication-using-active-directory-certificate-service/>

WorkSpaces の運用管理に関連するテーマ

- デプロイの自動化
 - CLI/API, CloudFormation
- アプリケーション、マスタの管理
 - カスタムバンドルの管理
 - アプリケーションの分離
- メトリクス管理
 - リソース、ステータス管理, 利用状況管理
- バックアップ・リストア
 - ルートボリューム, ユーザーボリューム
- パッチ管理
 - WorkSpacesのパッチ適用・管理

Q&A

ご質問については、AWS Japan Blog

「<https://aws.amazon.com/jp/blogs/news/>」

にて後日掲載します

ご視聴ありがとうございました

AWS 公式 Webinar

<https://amzn.to/JPWebinar>



過去資料

<https://amzn.to/JPArchive>

