[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

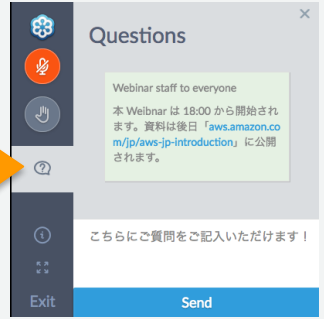
aws

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います。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.

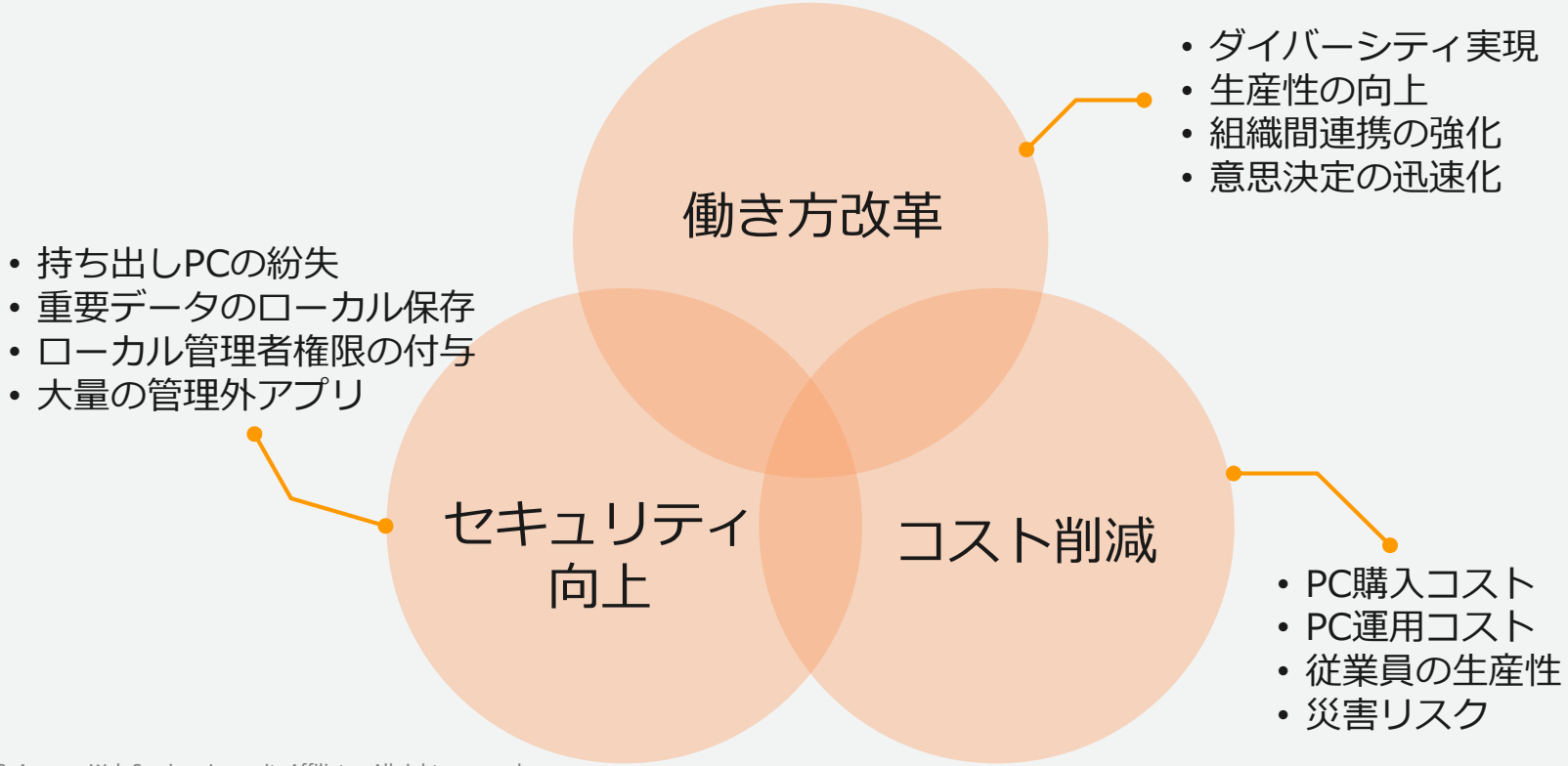
本日の内容

- 本日お話すること
  - 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

- 本日お話しないこと
  - 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

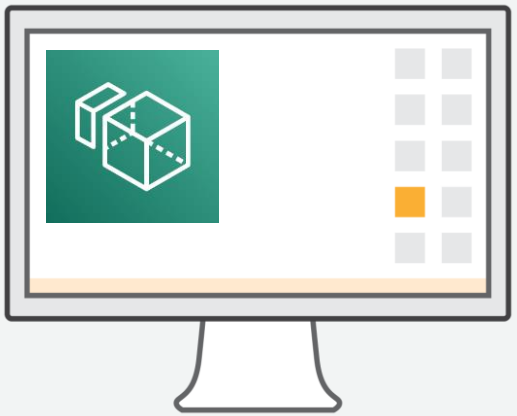
- クラウド上にデスクトップ環境を提供「いつでも・どこでも」を実現
- 従量課金型。月額30ドル/ユーザーから（＊）

＊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

Hourly

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

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

aws

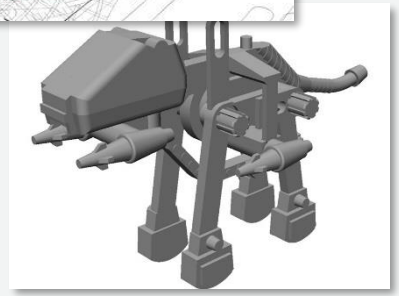
PowerPro/GraphicsPro バンドル

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、高度なグラフィクス処理での利用



aws

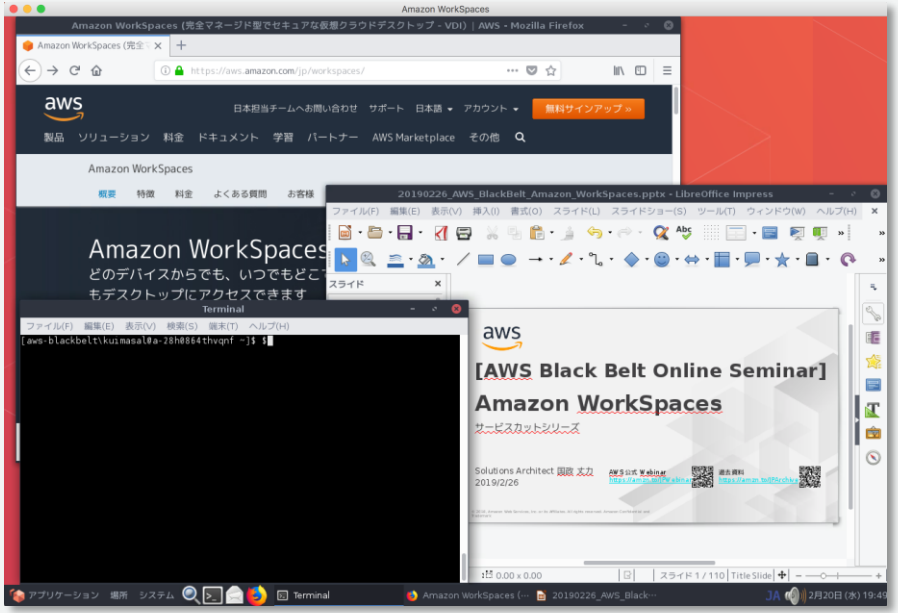
Amazon Linux WorkSpaces

WorkSpacesでも使い慣れたAmazon Linuxが利用可能に

New 2018.6月

amazon WorkSpaces ＋ Amazon Linux 2 ＋ MATE ＝

- 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

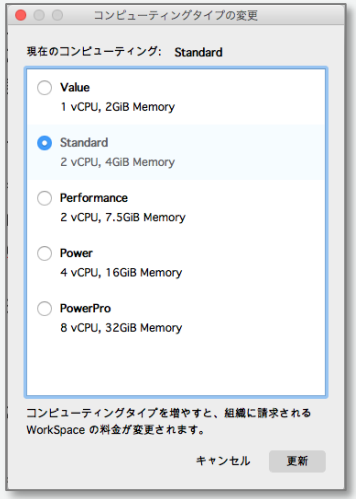


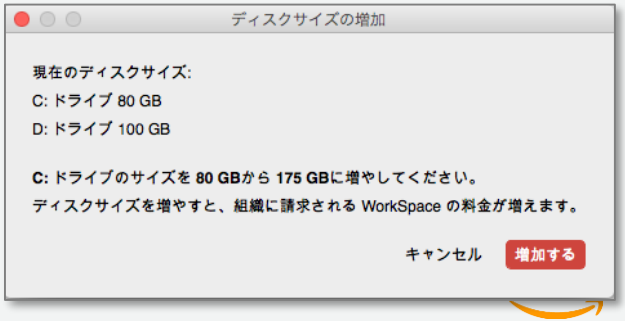
ユーザーセルフサービス管理機能

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の担当者にコンタクトください

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

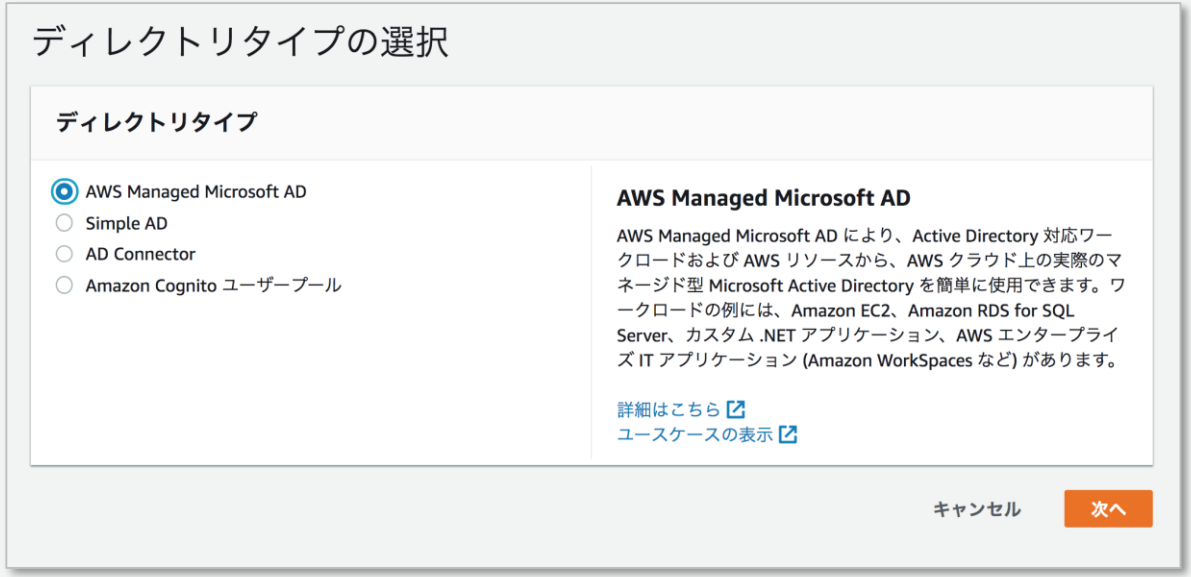
3. WorkSpaces クライアント
    - クライアントのダウンロード
    - クライアントの設定
    - ネットワーク接続性の確認
    - WorkSpaces への接続

aws

事前準備

ディレクトリの作成

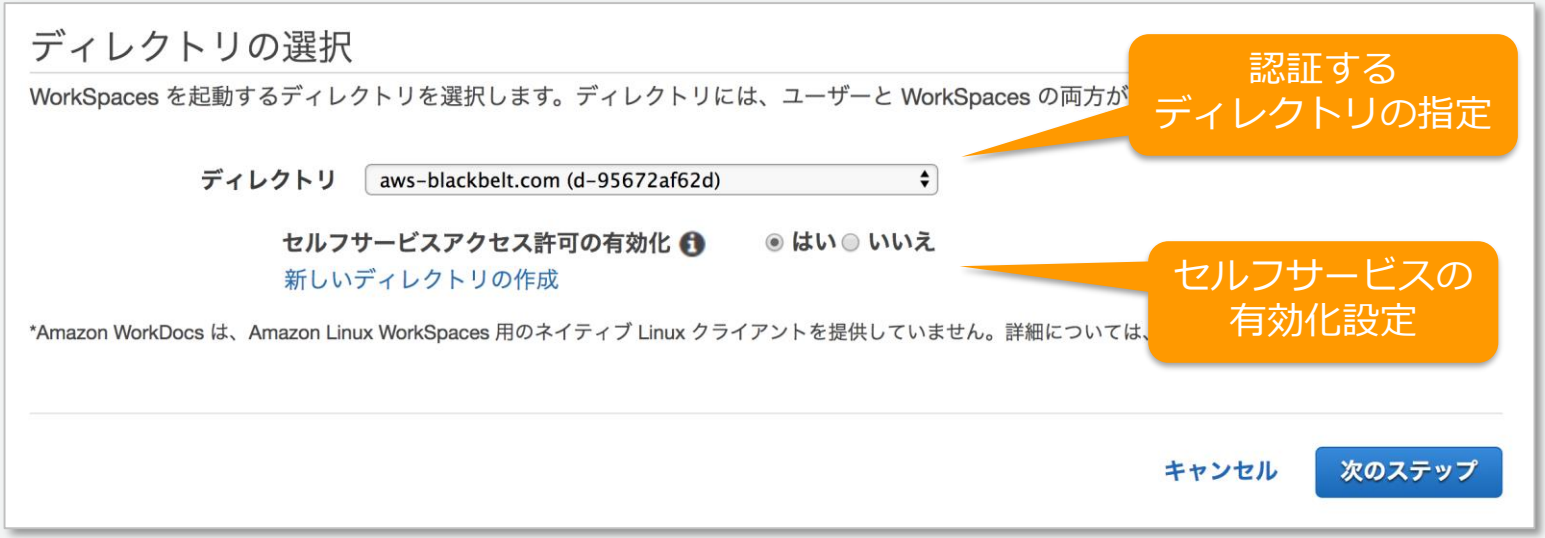
- ユーザー認証のためのディレクトリを事前に作成
- AWS上に新規作成する場合
  - Microsoft AD
  - Simple AD
- オンプレミスのADと連携する場合
  - AD Connector



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



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

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

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

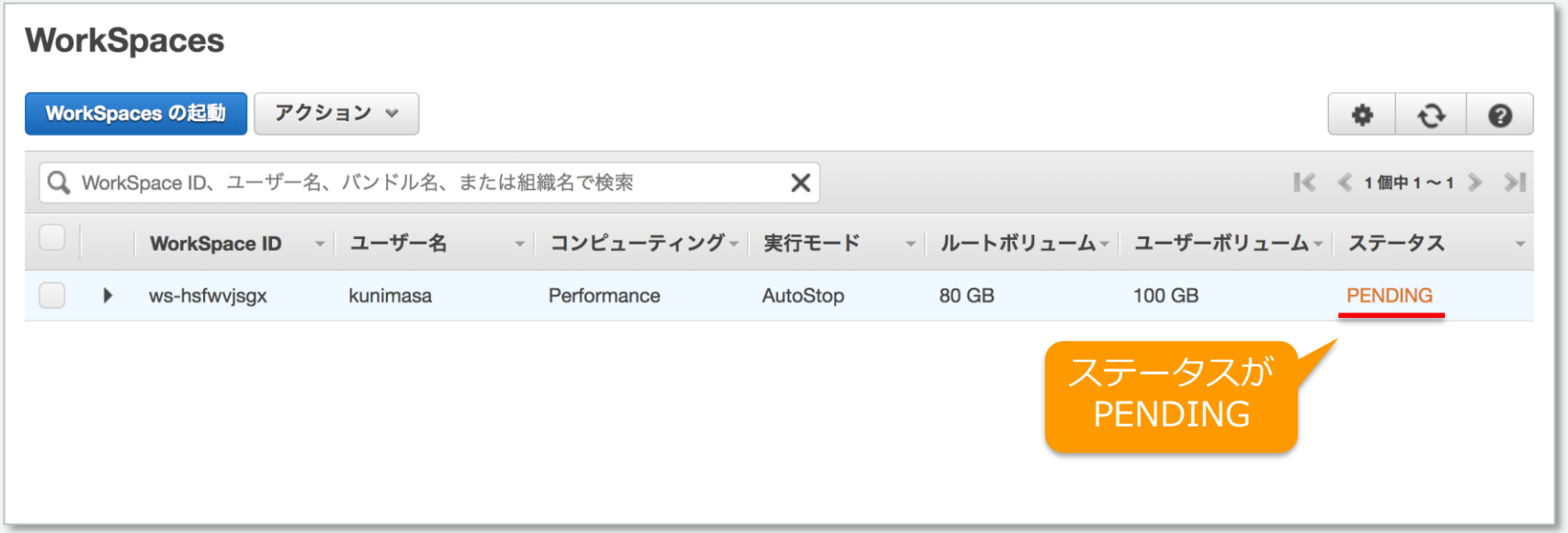
レビューと起動

- 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



WorkSpaces の作成

WorkSpaces の作成完了

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_emSzEh1d9iKlzwvu857EHPv9ljXF71-67QO3BdLmSqO
PZqc95FfKhP6rIL_9HYPKZigq74-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+[redacted]

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

kunimasa

Takechika

Kunimasa

kunimasa@amazon.com

••••••••••

••••••••••

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

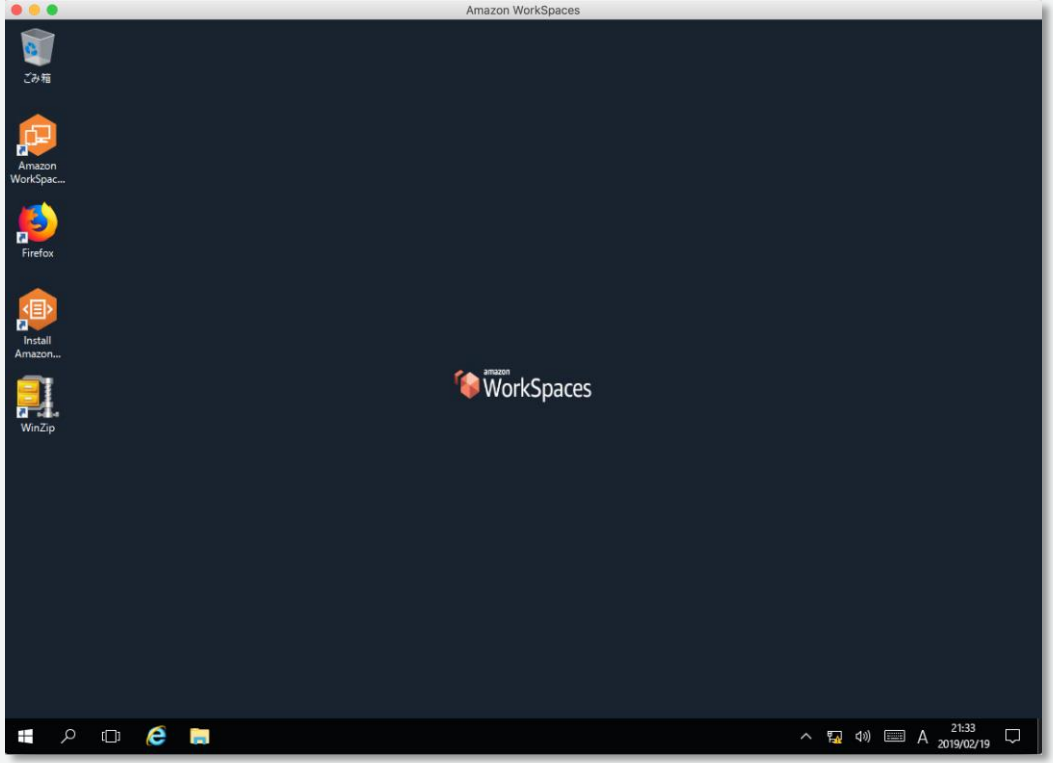
WorkSpaces クライアント

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)

WorkSpaces クライアント

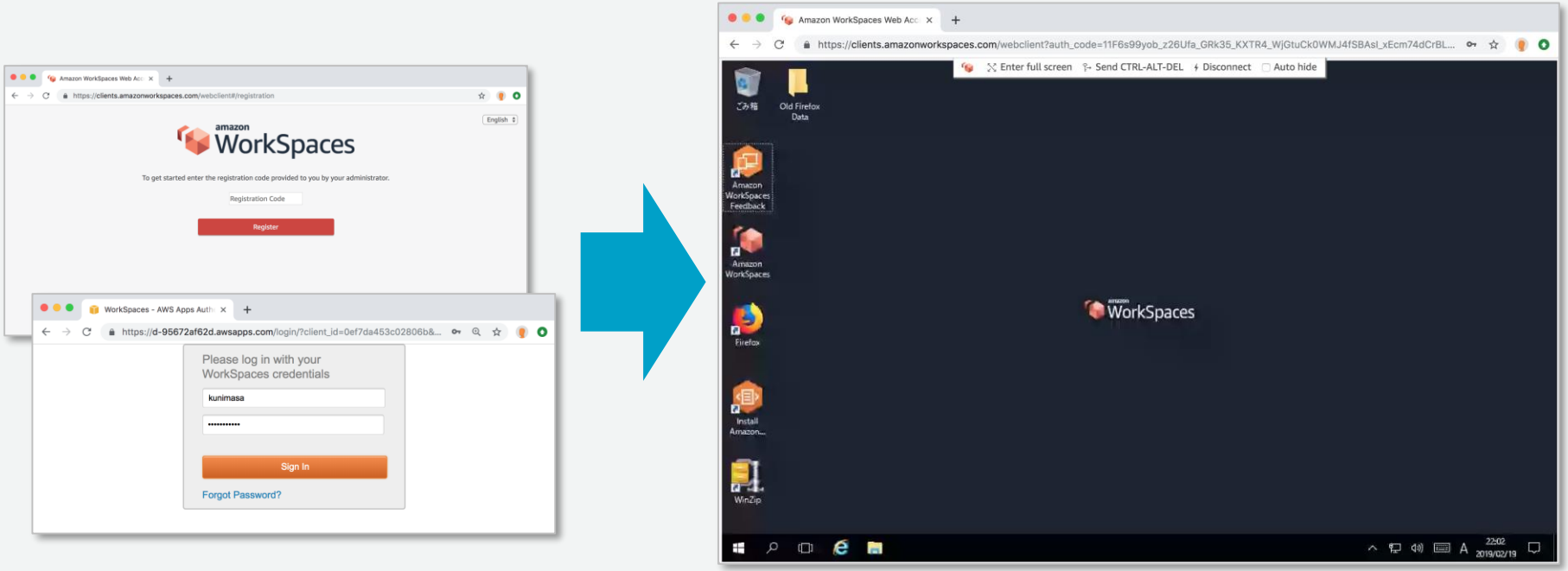
WorkSpaces への接続



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

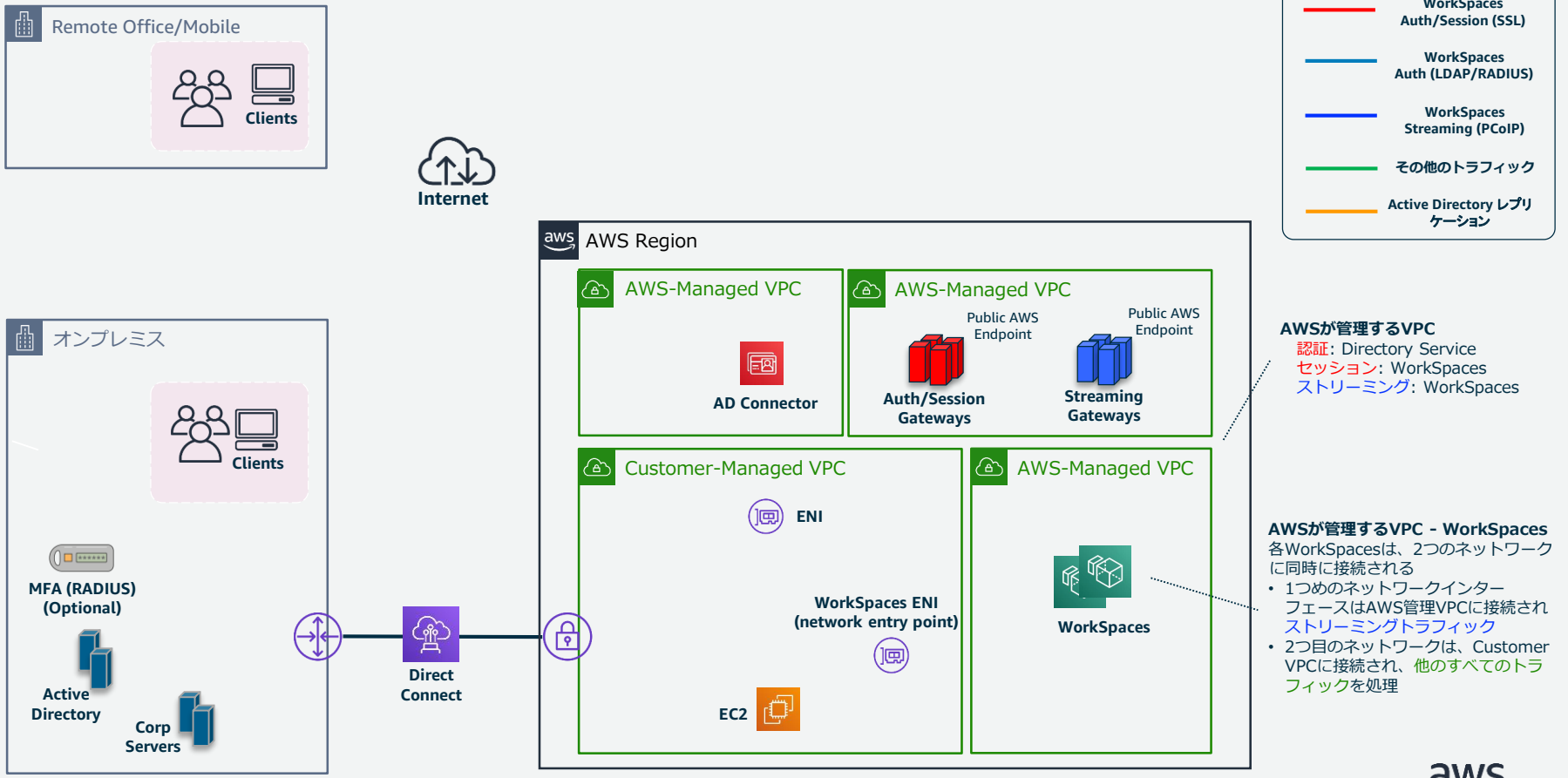


WorkSpaces のアーキテクチャ

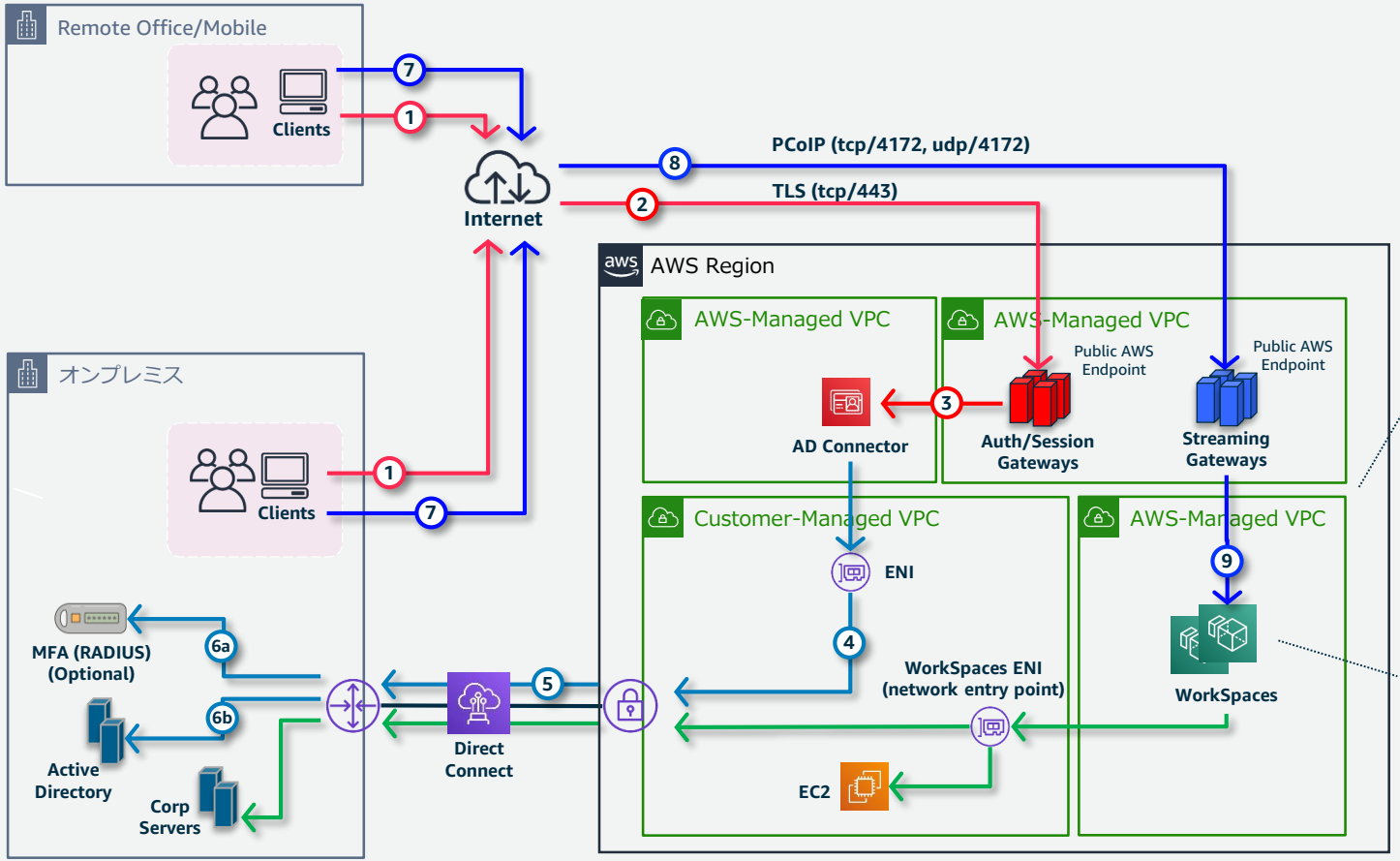
WorkSpaces のアーキテクチャ

- 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



WorkSpaces へのログインフロー



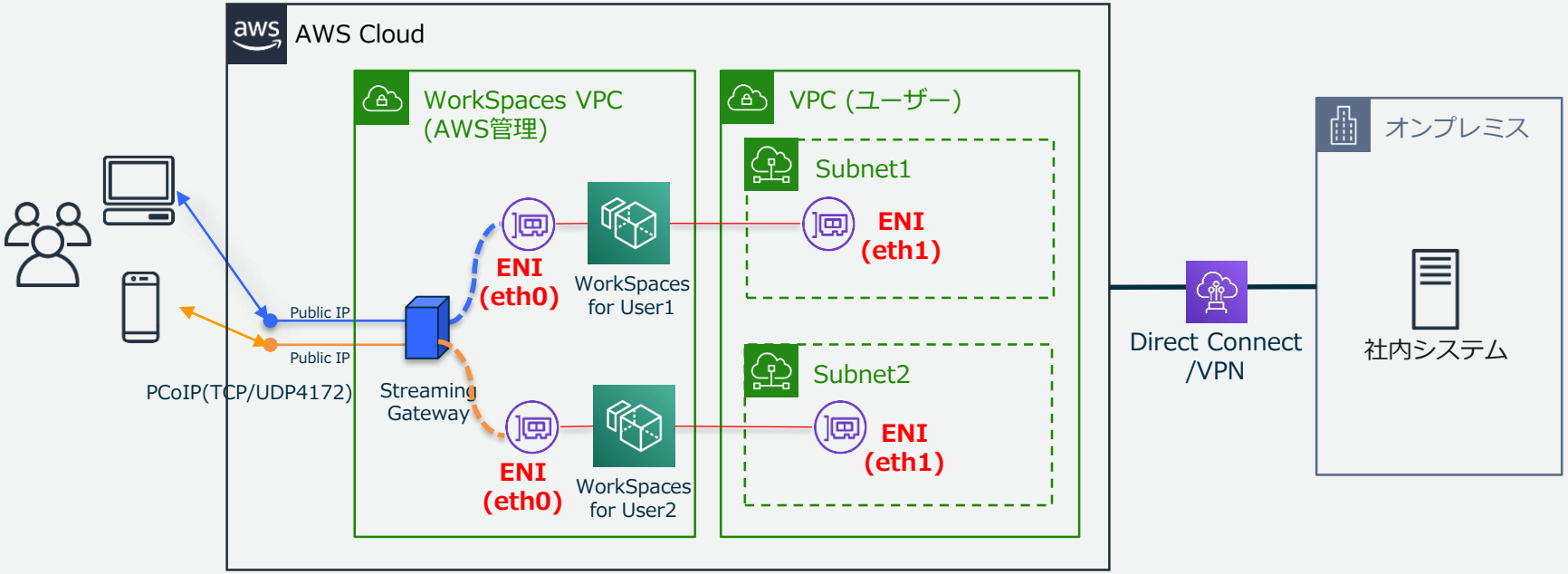
AWSが管理するVPC
認証: Directory Service
セッション: WorkSpaces
ストリーミング: WorkSpaces

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

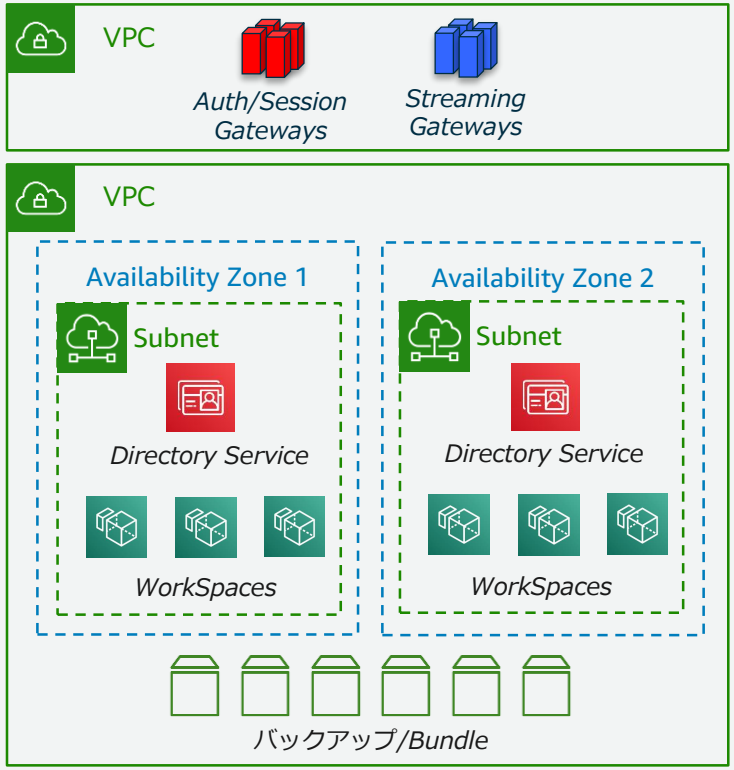
高品質で効率的なデスクトップストリーミングプロトコルを採用

- 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

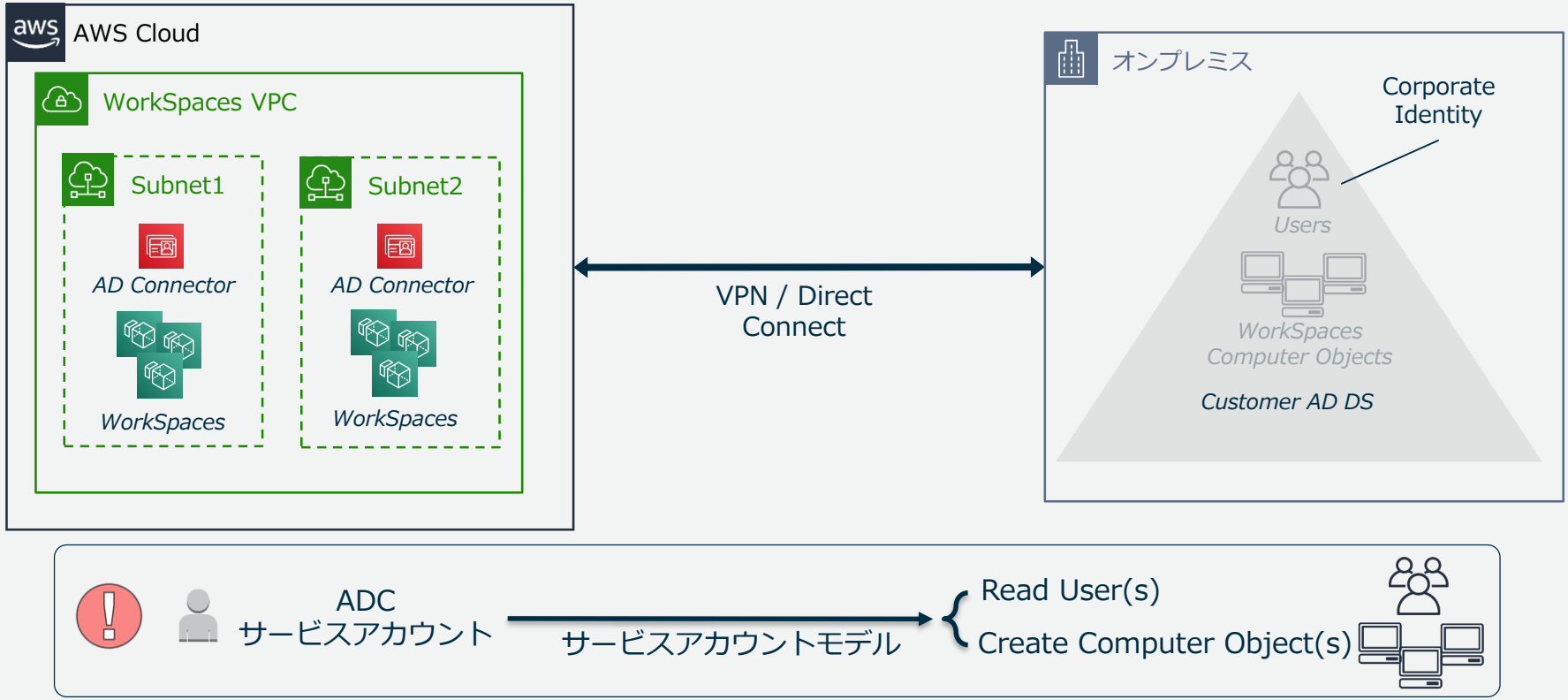
既存ADドメインとの連携

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

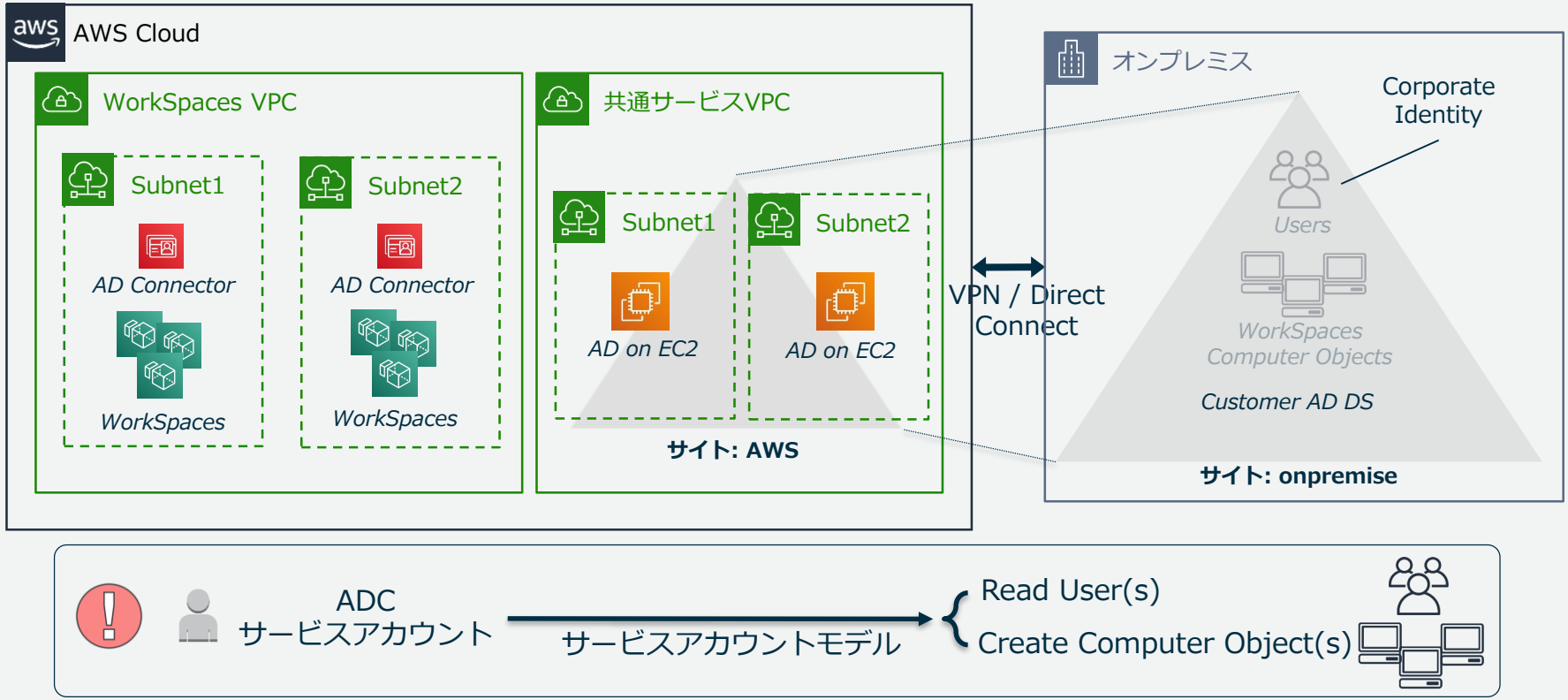
既存ADドメインとの連携

AD ConnectorからオンプレミスADドメインへ認証をProxy



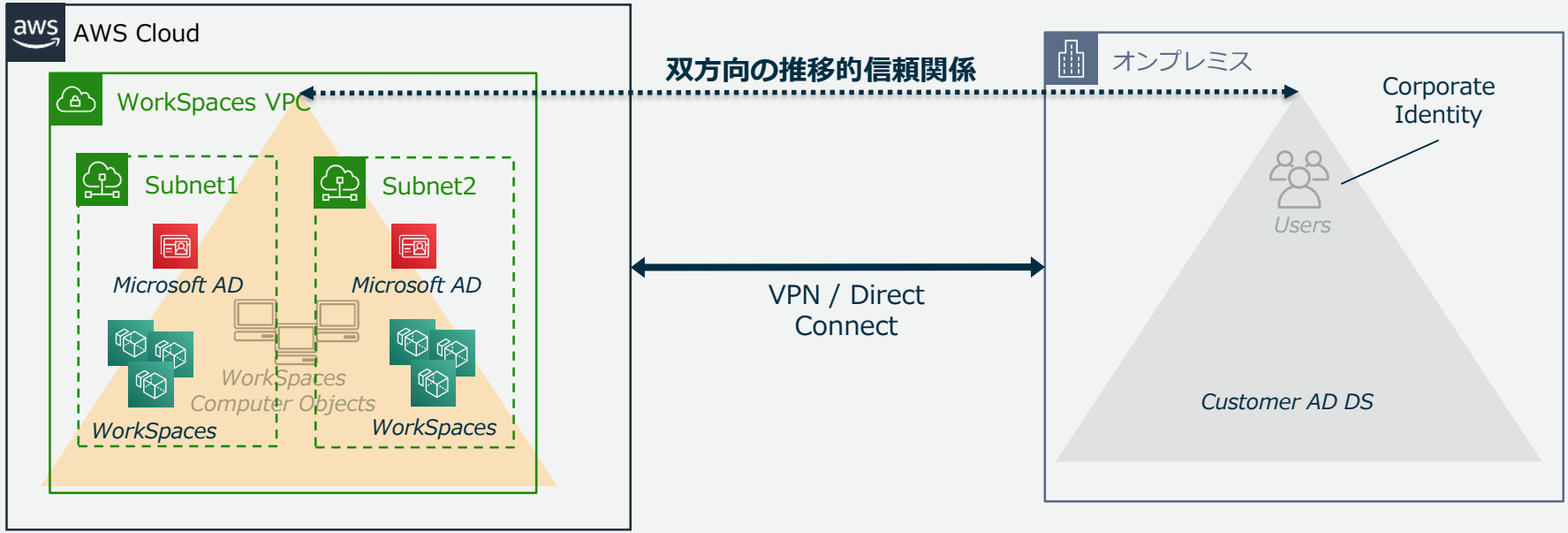
既存ADドメインとの連携

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)

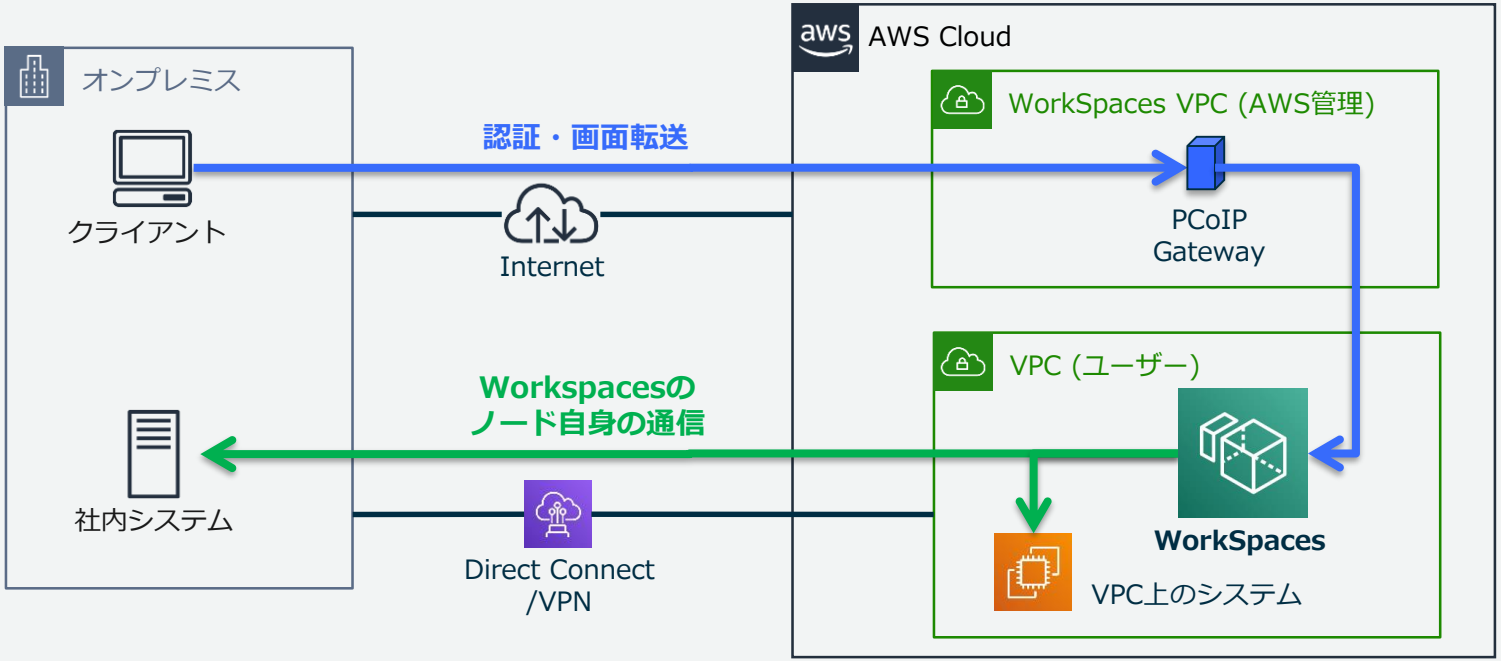
- ユーザートラフィック (WorkSpaces – ユーザーVPC/オンプレミス/インターネット)
  - VPC
  - オンプレミス接続
    - Direct Connect
    - VPN
  - インターネット接続
    - Public IP Address 付与
    - NAT Gateway
    - オンプレミス Proxy

aws

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

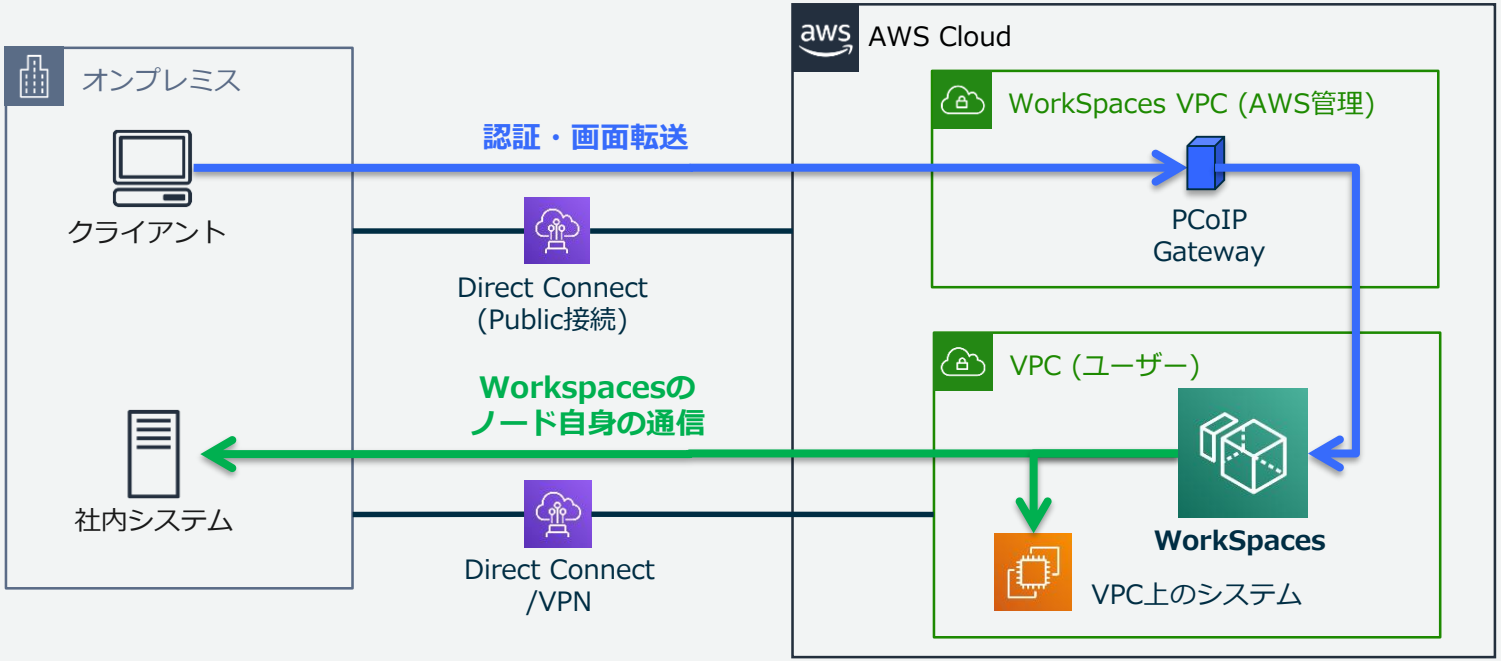
- デスクトップ画面へは、インターネット経由でどこからでもアクセスが可能
- 社内システムへは、専用線経由でセキュアに一貫した性能でアクセス



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

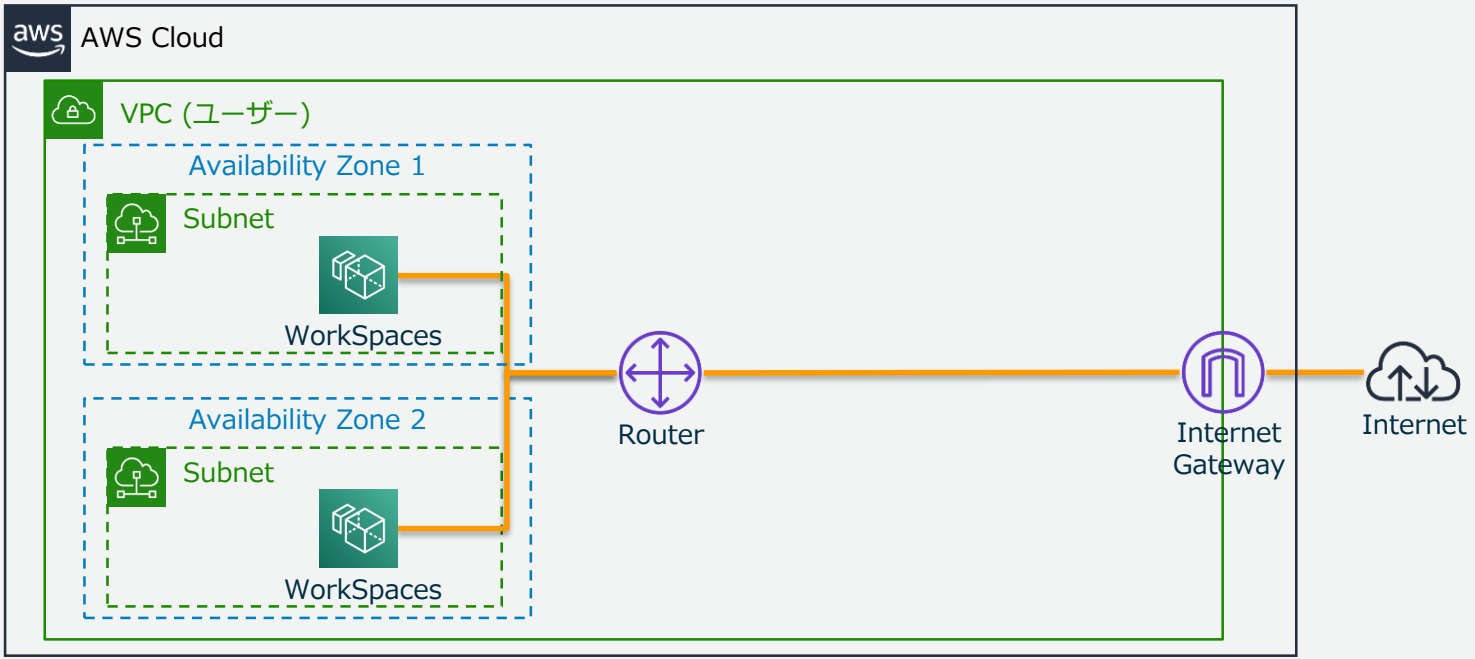
- DX Public接続により、画面ストリーミングも専用線経由でのアクセスが可能
- 一貫した高い性能を求める場合や、ポリシーとしてインターネット接続禁止の場合に検討



WorkSpaces からのインターネット接続

Public IP Address (Elastic IP) 付与

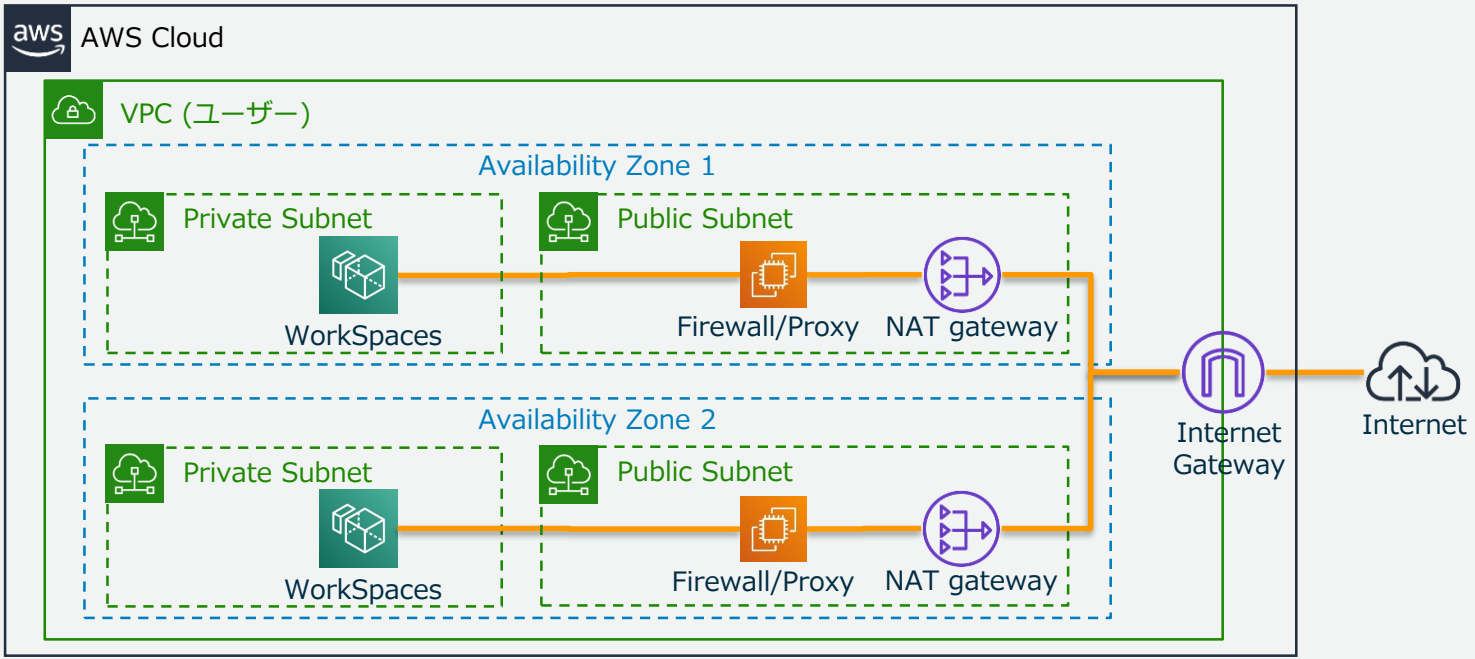
- WorkSpaces に EIP を付与し AWS からインターネットへアクセス
- ディレクトリ設定からPublic IPによるインターネットアクセスを設定可能



WorkSpaces からのインターネット接続

NAT Gateway 経由

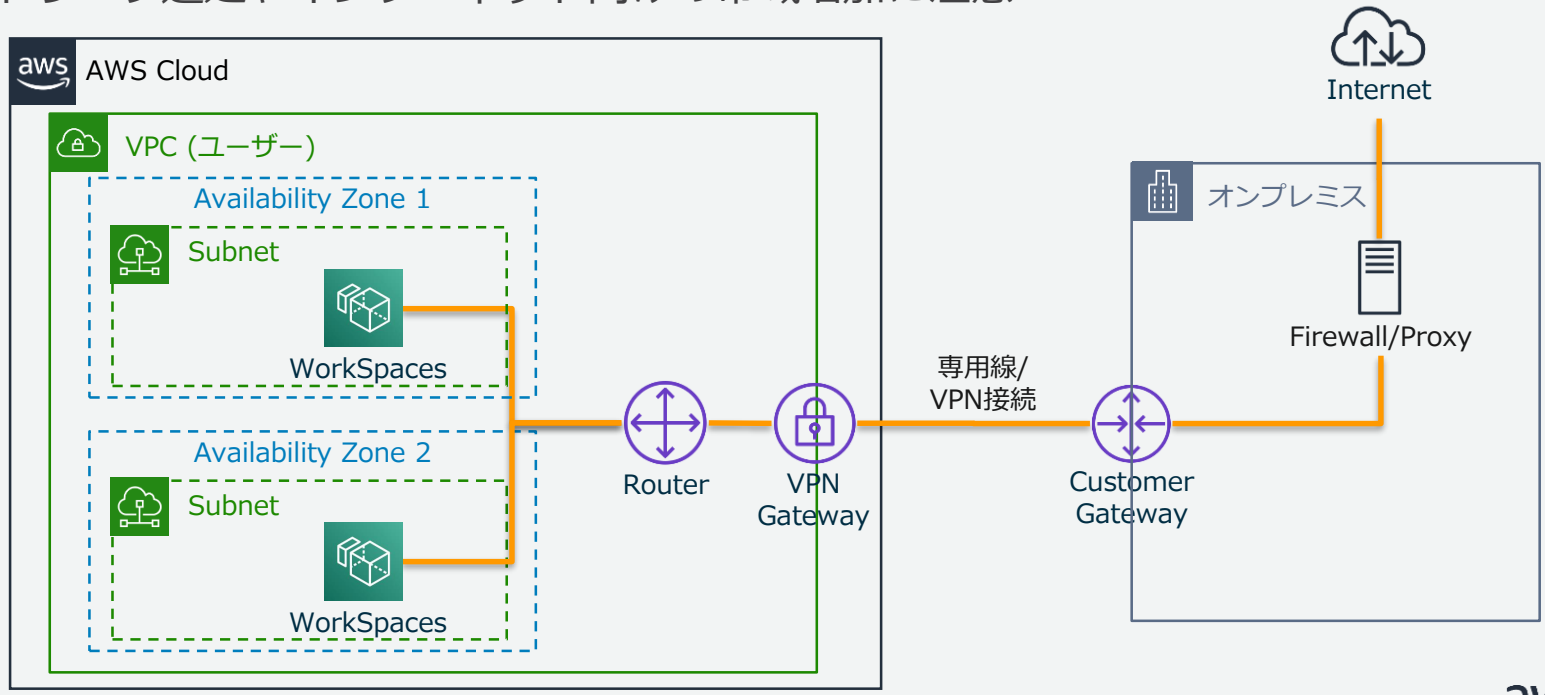
- NAT Gateway を経由してAWSからインターネットへアクセス
- Firewall や Proxy でセキュリティポリシーを実装



WorkSpaces からのインターネット接続

オンプレミス Proxy 経由

- オンプレ経由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

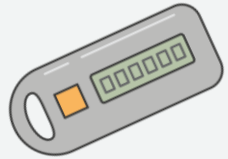
- ユーザー認証
  - ADドメイン認証
  - MFA (Multi-Factor Authentication)
- IPアドレスによるアクセス制御
  - IP アクセスコントロールグループ
  - セキュリティグループ
- デバイスによるアクセス制御
  - 証明書によるアクセス制限 (Windows/Mac OS X)
  - デバイスタイプによる制限 (その他デバイス)
- グループポリシーによるポリシー制御
  - Active Directory のグループポリシーによる制御

aws

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



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

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

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

aws

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

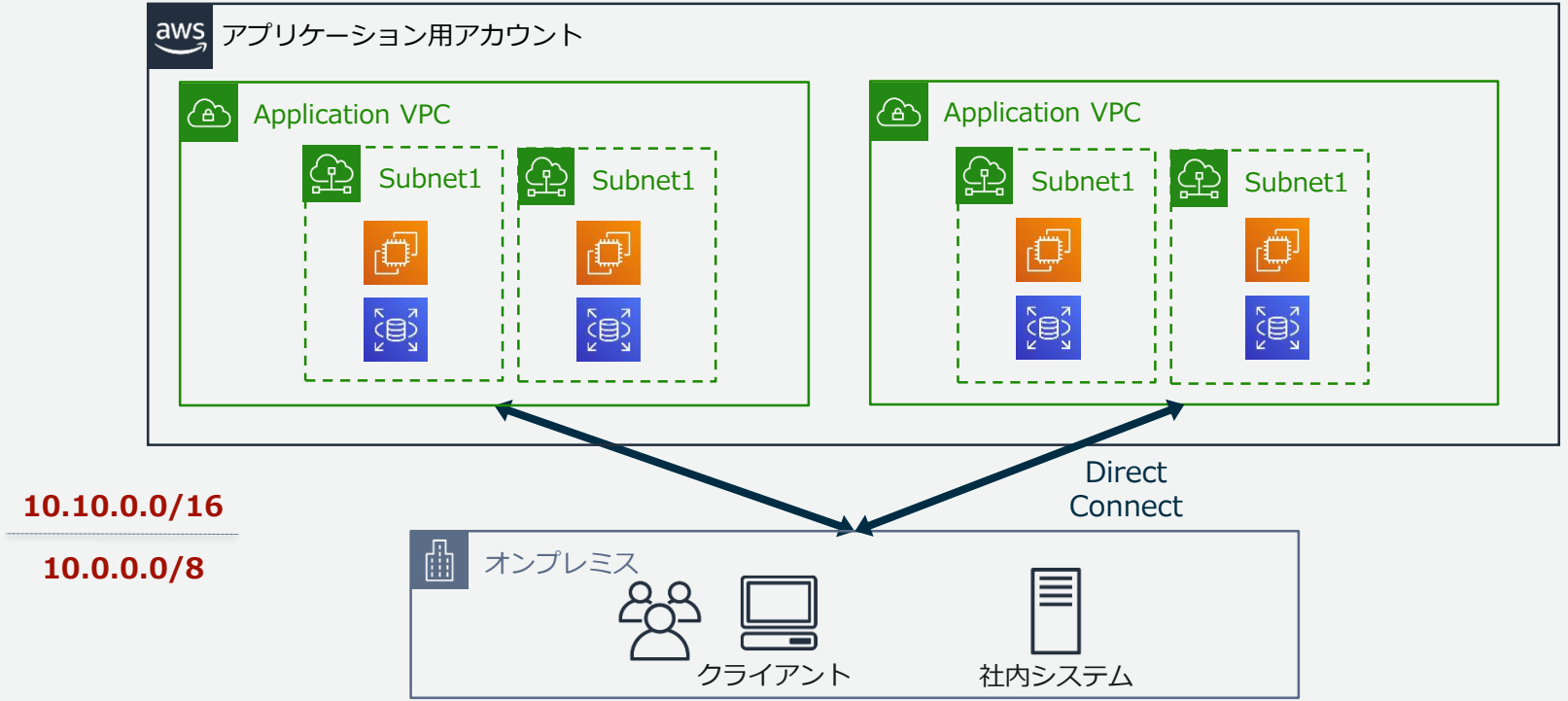
BYOD

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



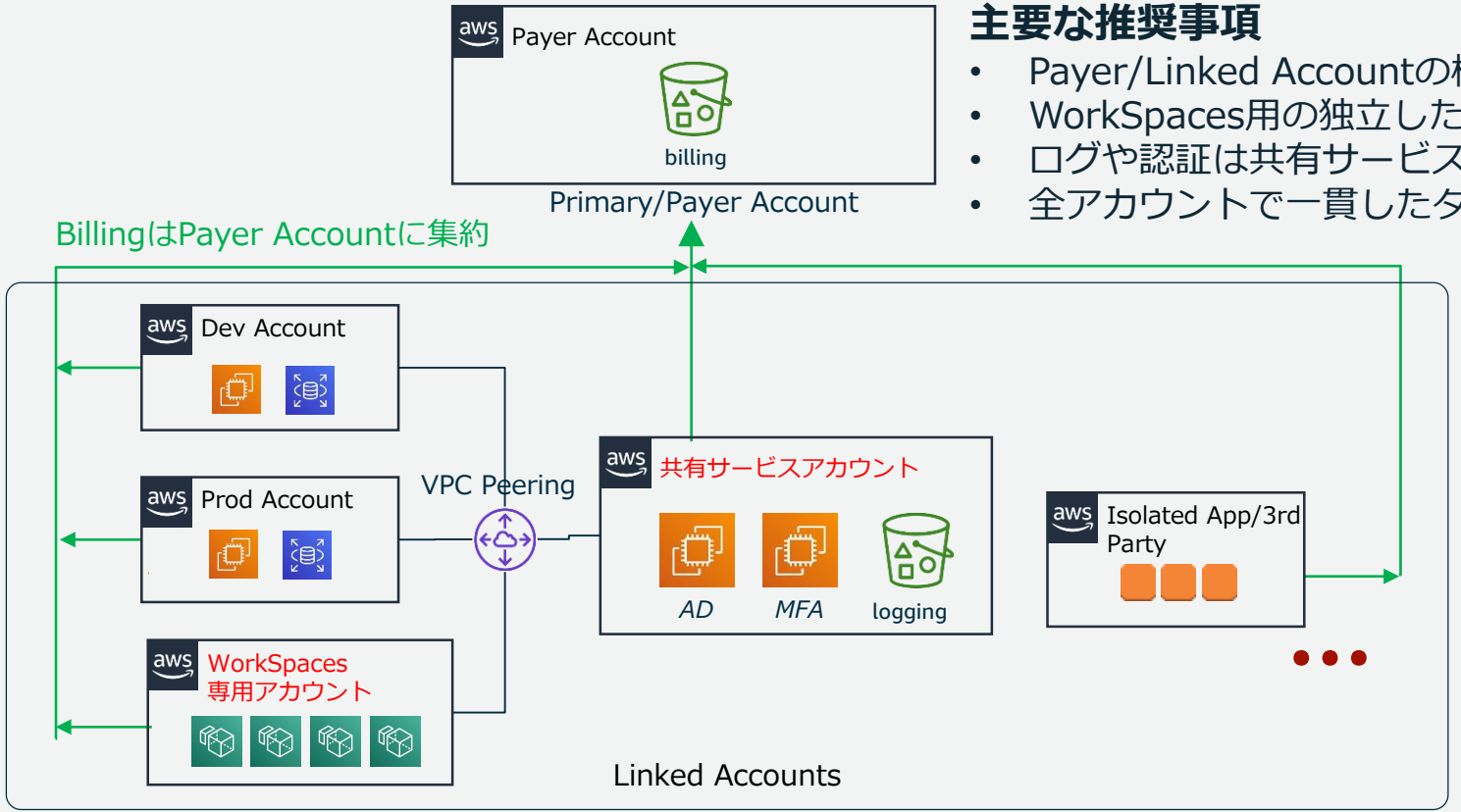
ユースケース、要件の収集

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



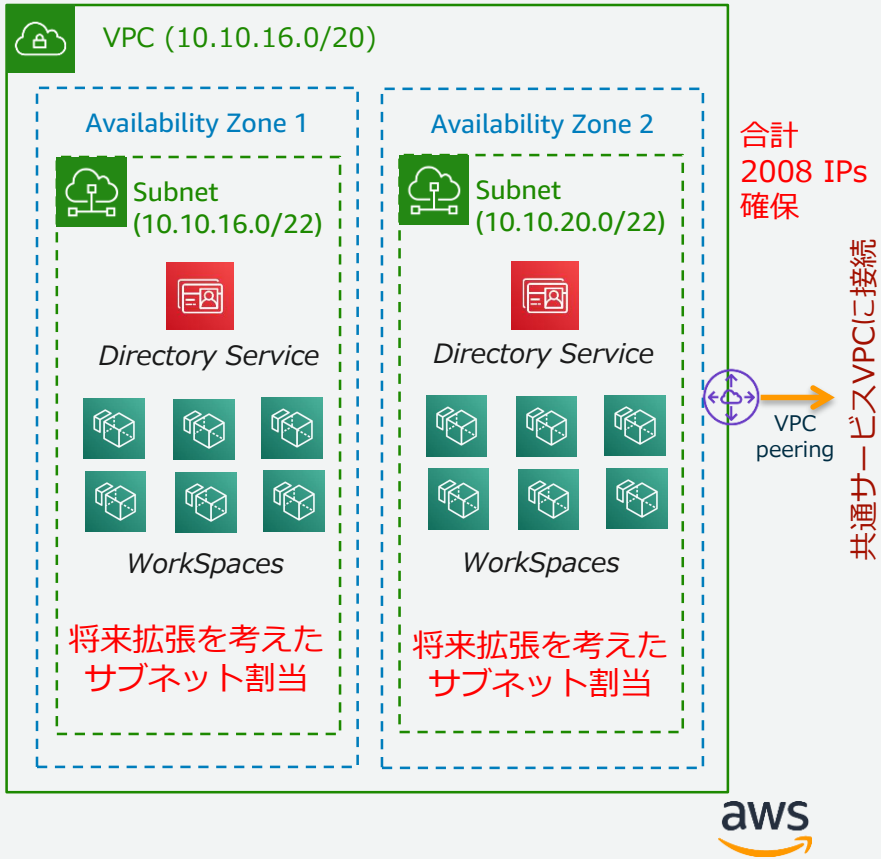
主要な推奨事項

- 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アドレッシングを設計

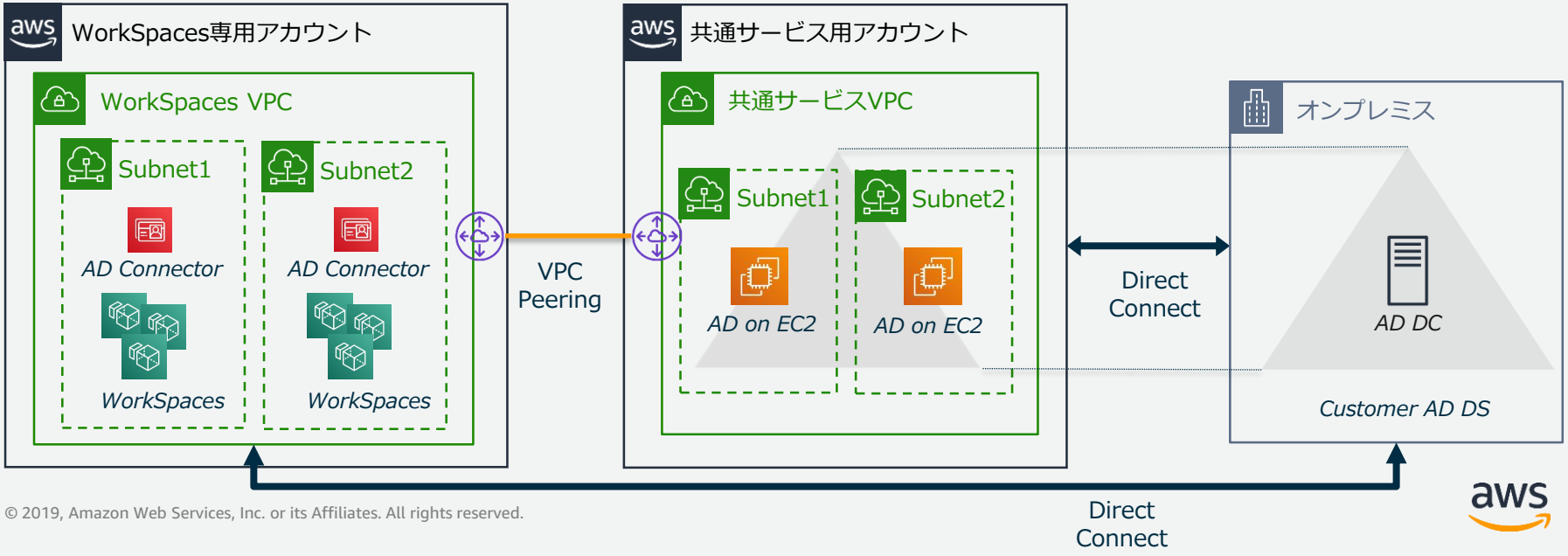
- WorkSpaces用の専用VPCを作成
- 最小2つのサブネット
- IP枯渇を避けるため、将来の拡張性を考慮してサブネットを作成
- イニシャルで2,000台のWorkSpacesと成長の余地
- 共有サービス用のVPCの使用



ディレクトリ展開のコンセプト

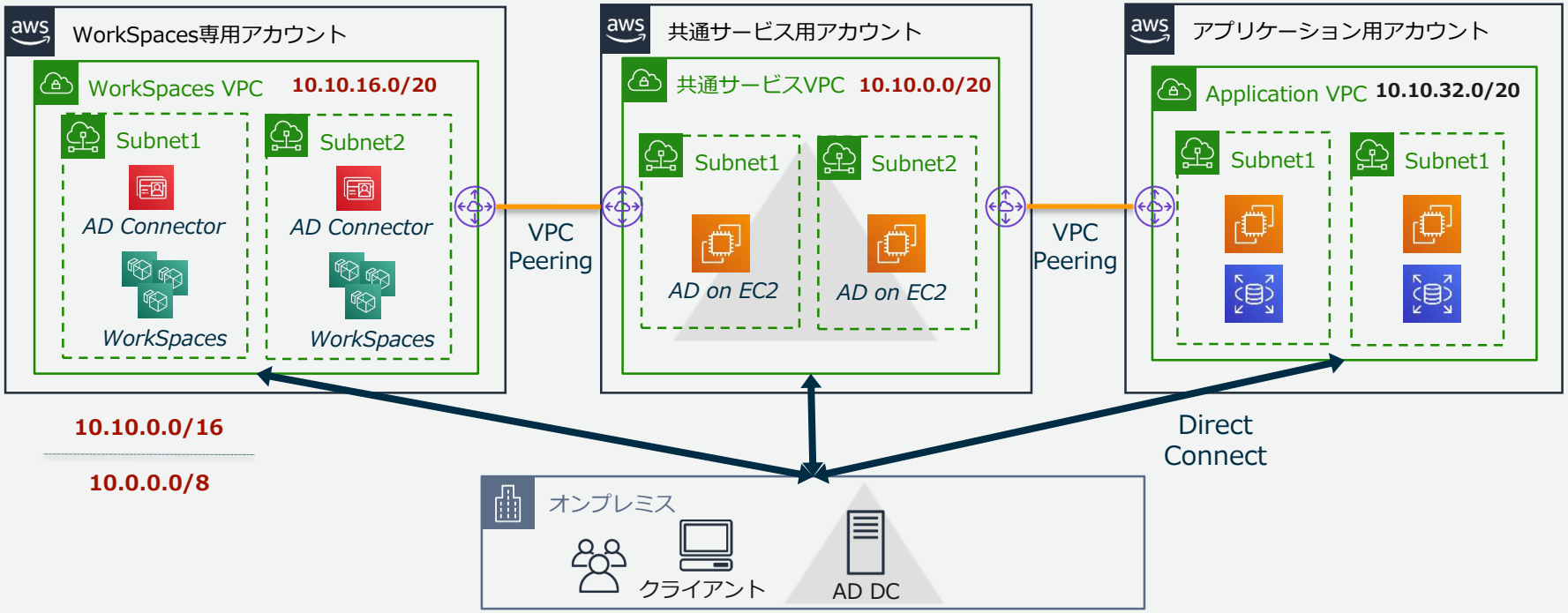
ドメイン数やNW遅延、レプリケーション低減を考慮した認証連携・ドメイン設計

- 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/

aws

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