Amazon WorkSpaces Update

AWS Black Belt Online Seminar
サービスカットシリーズ

石倉 徹
Partner Solutions Architect
2021/11

AWS 公式 Webinar
https://amzn.to/JPWebinar

過去資料
https://amzn.to/JPArchive

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け、アマゾン ウェブ サービス ジャパン合同会社が主催するオンラインセミナーシリーズです

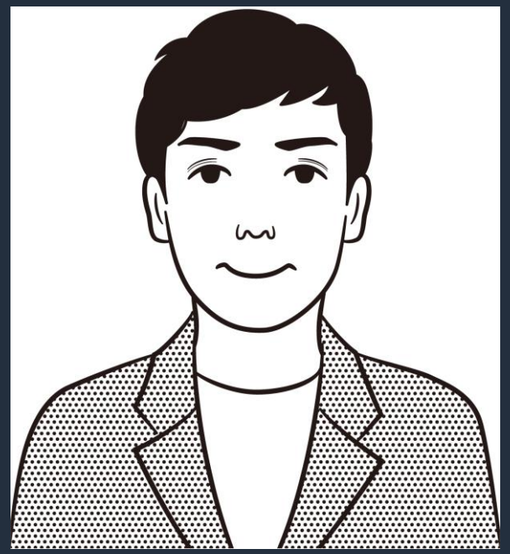
- AWSの技術担当者が、AWSの各サービスについてテーマごとに動画を公開します
- お好きな時間、お好きな場所でご受講いただけるオンデマンド形式です
- 動画を一時停止・スキップすることで、興味がある分野・項目だけの聴講も可能、スキマ時間の学習にもお役立ていただけます

内容についての注意点

- 本資料では2021年11月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には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.

自己紹介



石倉 徹(Tetsu Ishikura)
アマゾン ウェブ サービス ジャパン合同会社
パートナー ソリューション アーキテクト

主にパートナー様の育成・技術支援を担当

好きな AWS のサービス：
　Amazon WorkSpaces

本セミナーの概要

- 本セミナーで学習できること
  - Amazon WorkSpacesの概要
  - Amazon WorkSpacesの設計するためのベース知識
  - Amazon WorkSpacesの最新アップデート
    （運用部分についてはお話いたしません）

- 対象者
  - 仮想デスクトップを検討中の方
  - Amazon WorkSpacesをこれからご利用予定の方

本日のアジェンダ

- Amazon WorkSpaces について
    - 概要
    - ネットワーク環境
    - ディレクトリサービスの構成について
    - コンピューティング環境
    - クライアント環境
    - セキュリティ対策
- Amazon WorkSpaces 最新アップデート
- まとめ

テレワークが求められる背景

私たちの働き方は変わりつつあります

経済のグローバル化により
どこ でも **誰と** でも **いつ** でも働く環境に

さまざま仕事が **従来型のオフィスや事業所以外**の
場所でも行われるように

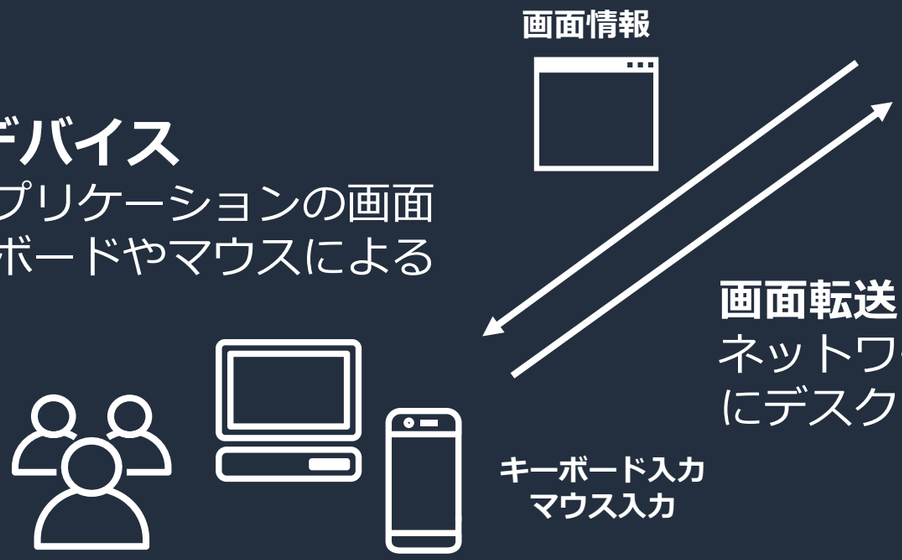
企業や組織が 従業員が**どこからでも**
安全に仕事ができる選択肢 をますます必要とするように

テレワークを実現する VDI/DaaS

VDI/DaaS とは

ネットワークを通じてデータセンターやクラウド上にあるサーバーで実行しているデスクトップ環境に接続し、その画面情報をクライアントデバイスに転送することで、遠隔利用するしくみ

仮想デスクトップ
データセンターやクラウド上にホストされるサーバ上で実行されるデスクトップ

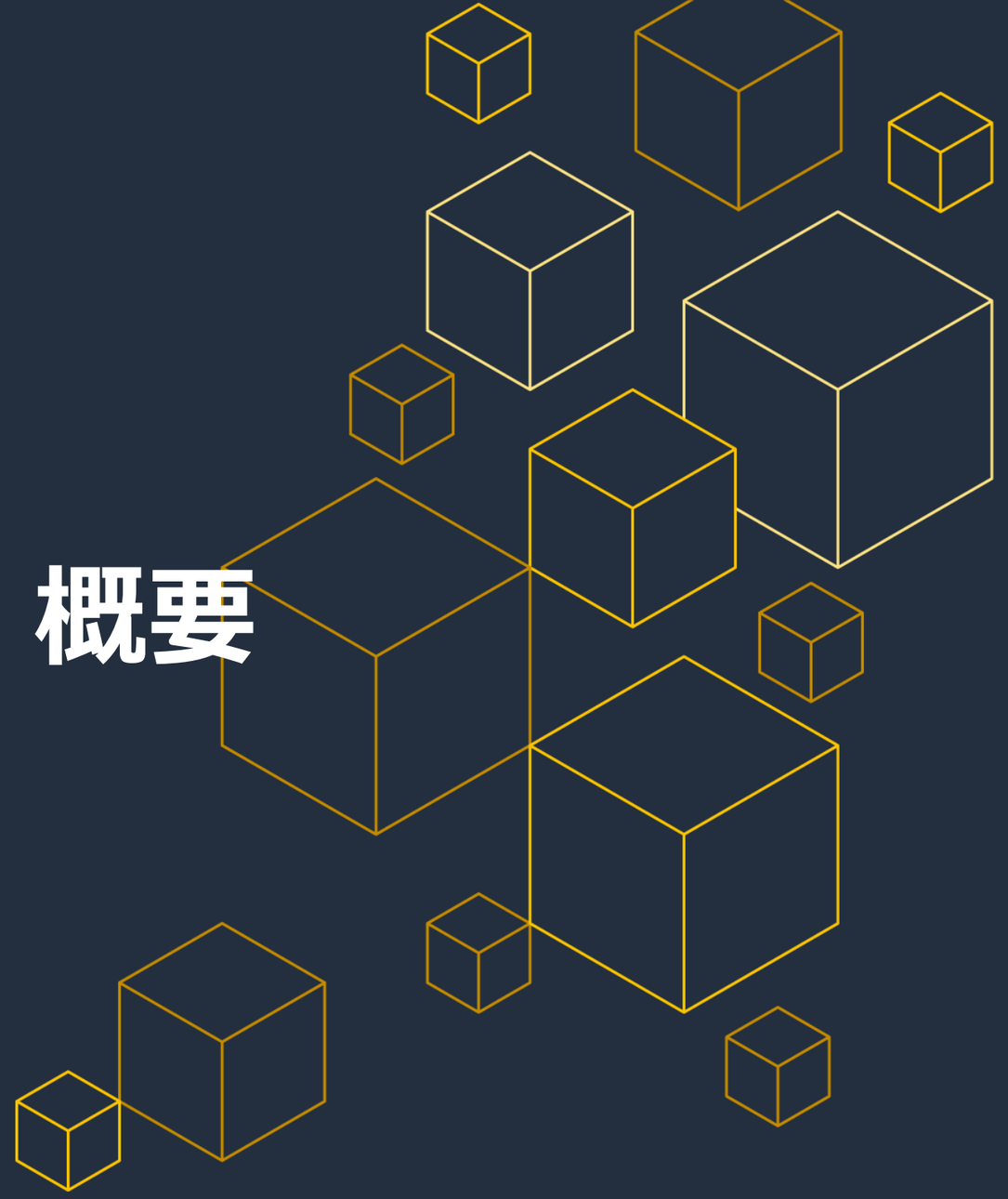


クライアントデバイス
デスクトップ, アプリケーションの画面情報を表示. キーボードやマウスによる入力操作を実行

画面転送
ネットワーク経由でクライアントデバイスにデスクトップの画面情報を転送

情報漏えいのリスク低減・管理業務の効率化

Amazon WorkSpaces 概要



aws

amazon WorkSpaces

AWS の提供するフルマネージド型でセキュアな仮想デスクトップサービス。
いつでも、どこからでも、AWS クラウド上の仮想デスクトップにアクセス。

すぐに使える

従量課金
初期投資不要

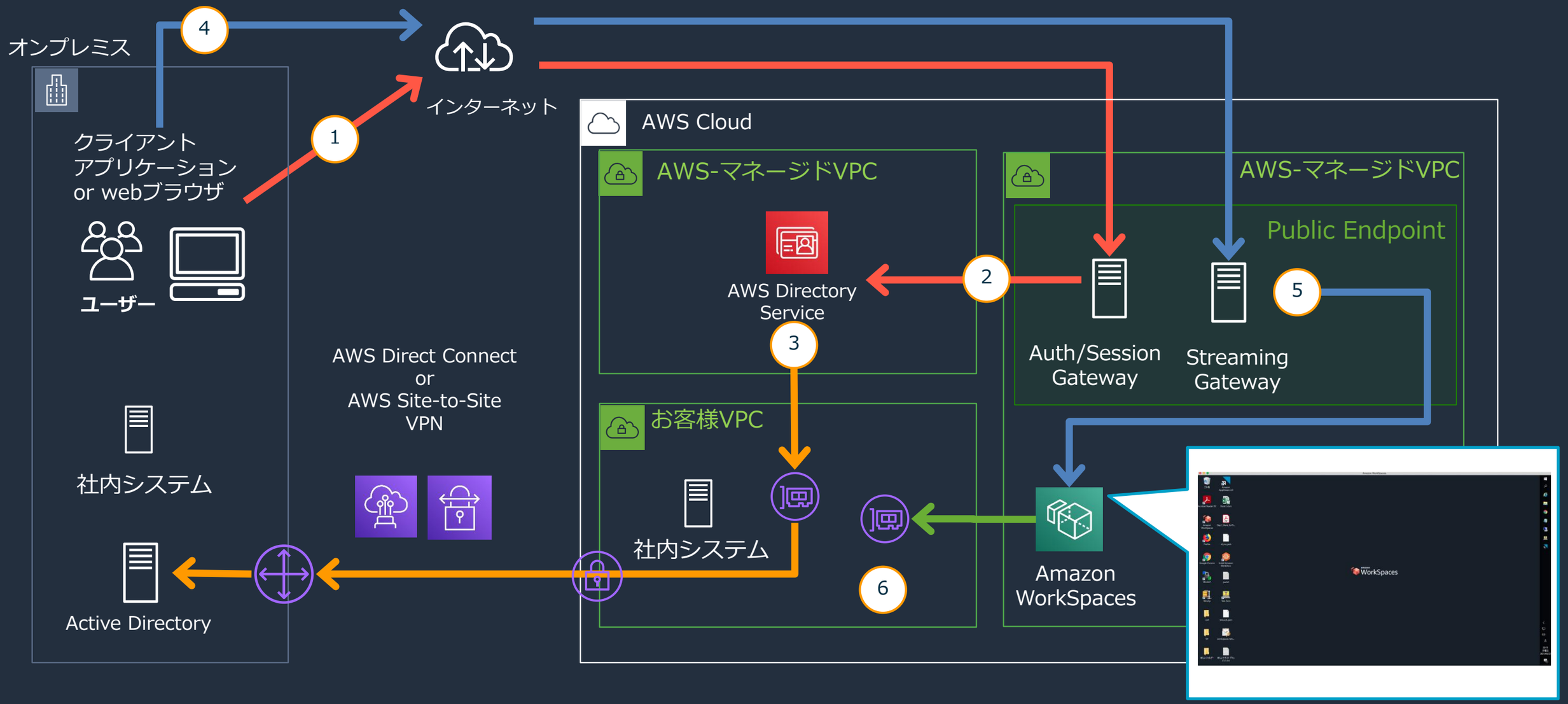
事前サイジングの
必要がなく増減も容易
一貫したパフォーマンス

高いセキュリティ

容易な
グローバル展開

aws

Amazon WorkSpaces 動作概要



Amazon WorkSpaces の構成要素

Amazon WorkSpaces サービスを安全・正常にデプロイするには、
次の5つの要素・コンポーネントの理解が必要です。

- ネットワーク環境
  WorkSpaces を実行するための ネットワーク環境
- ディレクトリサービス
  ユーザを認証し、WorkSpacesへのアクセスを提供するためディレクトリサービス
- Amazon Workspaces （本体）
  リモートで操作するコンピューティング環境の仕様等
- Amazon Workspaces クライアント
  クライアントデバイスの種類・仕様等
- セキュリティ対策
  安全に利用を行うために活用できるセキュリティ対策

Amazon WorkSpaces
ネットワーク環境

aws

Amazon WorkSpaces のネットワーク環境

WorkSpaces利用時のトラフィックは、次の2つに分けることができます。

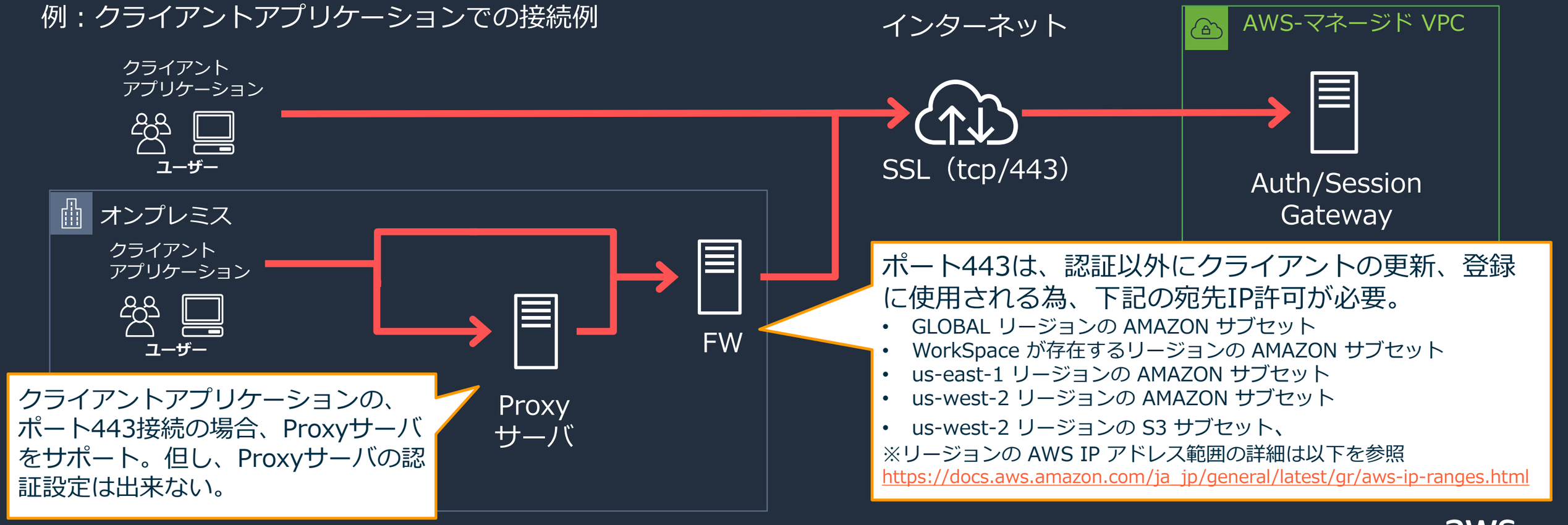
- クライアントとWorkSpaces サービスとの間のトラフィック
  -認証とセッション情報の通信
  -ストリーミングとヘルスチェックの通信
  -WorkSpacesへの接続

- WorkSpaces からインターネットやお客様ネットワークとの間のトラフィック
  -VPCの構成
  -オンプレミスとの通信

認証とセッション情報の通信

- 認証とセッション情報の通信には、ポート443 HTTPSが利用され、Auth/SessionGatewayへ接続が行われる。
- Auth/SessionGatewayはマネージドサービスの為、冗長の考慮不要。

例：クライアントアプリケーションでの接続例



クライアントアプリケーションの、ポート443接続の場合、Proxyサーバをサポート。但し、Proxyサーバの認証設定は出来ない。

ポート443は、認証以外にクライアントの更新、登録に使用される為、下記の宛先IP許可が必要。

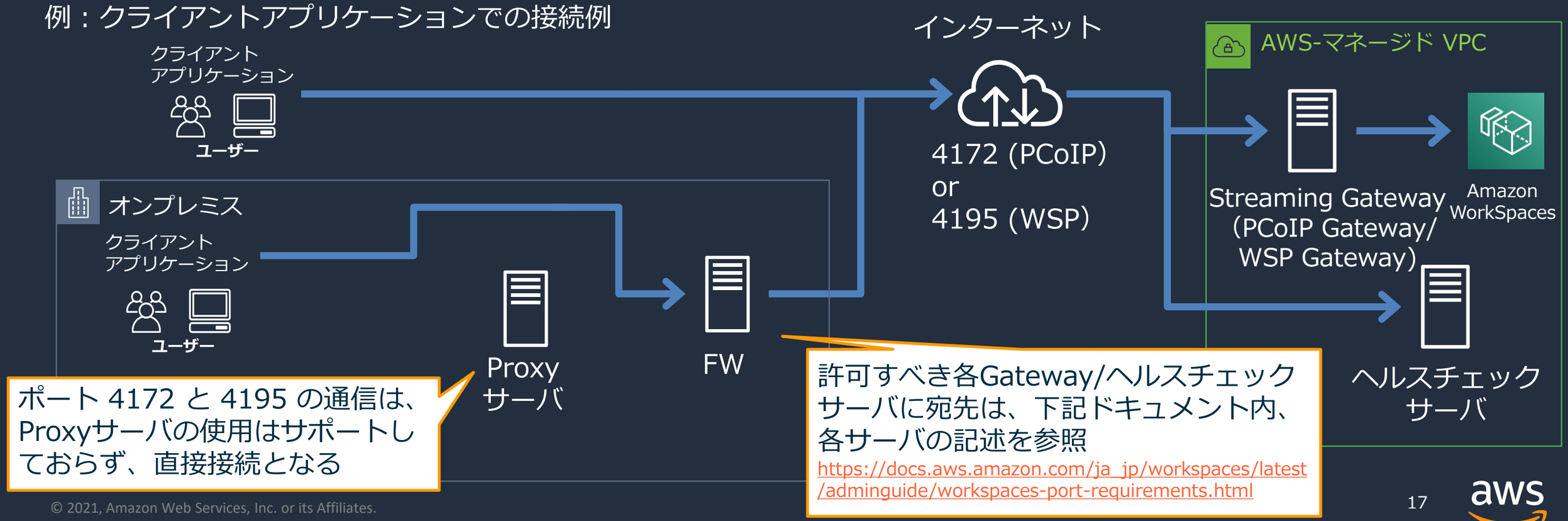
- GLOBAL リージョンの AMAZON サブセット
- WorkSpace が存在するリージョンの AMAZON サブセット
- us-east-1 リージョンの AMAZON サブセット
- us-west-2 リージョンの AMAZON サブセット
- us-west-2 リージョンの S3 サブセット、

※リージョンの AWS IP アドレス範囲の詳細は以下を参照
https://docs.aws.amazon.com/ja_jp/general/latest/gr/aws-ip-ranges.html

ストリーミングとヘルスチェックの通信

- ストリーミングプロトコルは PCoIPとWSP(WorkSpaces Streaming Protocol)が利用可能
- PCoIP利用の場合は、PCoIP Gatewayへアクセス(ポート4172 UDP/TCP)
- WSP利用の場合は、WSP Gatewayへアクセス（ポート4195 UDP/TCP ）
- この接続は、ヘルスチェックサーバへのアクセスにも利用される
- PCoIP Gateway/WSP Gateway は、マネージドサービスの為、冗長の考慮不要。

例：クライアントアプリケーションでの接続例



ポート 4172 と 4195 の通信は、Proxyサーバの使用はサポートしておらず、直接接続となる

許可すべき各Gateway/ヘルスチェックサーバに宛先は、下記ドキュメント内、各サーバの記述を参照
https://docs.aws.amazon.com/ja_jp/workspaces/latest/adminguide/workspaces-port-requirements.html

Amazon WorkSpaces のプロトコルについて

- WorkSpaces は、PCoIP と WorkSpaces Streaming Protocol (WSP) の 2 つのプロトコルをサポート。
- デバイスの種類、オペレーティングシステム、ユーザーのネットワーク条件、双方向の動画サポートを必要としているかによって選択する。
- 既存のPCoIPベースの環境をWSPに変更する場合には、WorkSpaceの移行が必要となる。

項目	PCoIP	WSP
利用ポート TCP/UDP	4172	4195
スマートカード認証	×	○
Webカメラ	×	○
クライアント：iOS/Android/Linux	○	×
Teradici Zero Client	○	×
GPUバンドル	○	×

許可が必要なドメイン / ネットワーク帯域について

- **許可が必要なドメイン**

その他、許可が必要なドメインについては、下記ドキュメントを参照

<許可リストに追加するドメインと IP アドレス>
https://docs.aws.amazon.com/ja_jp/workspaces/latest/adminguide/workspaces-port-requirements.html#whitelisted_ports

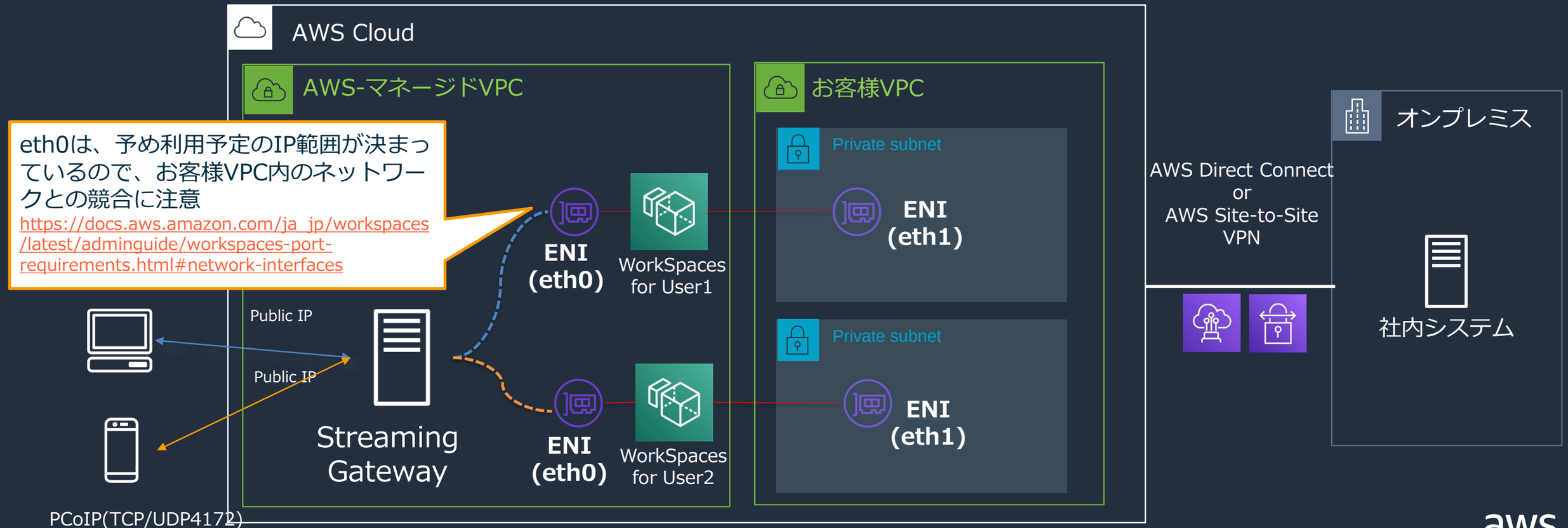
- **ネットワーク帯域**

快適に利用をするためには、利用シーンに合わせてネットワーク帯域やWorkSpacesがあるリージョンまでのラウンドトリップ時間（RTT）を確保する必要がある。事前検証を推奨。
WorkSpacesクライアントを利用して、ネットワーキング要件を満たしているかを確認することが可能

<Amazon WorkSpaces クライアントネットワークの要件>
https://docs.aws.amazon.com/ja_jp/workspaces/latest/adminguide/workspaces-network-requirements.html

Amazon WorkSpacesへの接続（ENIについて）

- 管理ネットワークインタフェース(eth0): AWS管理VPCに接続。ストリーミングを受信
- プライマリネットワークインタフェース(eth1): お客様 VPCに接続され、デフォルトのセキュリティグループ（ディレクトリ識別子_workspacesMembers）がアタッチされる。新規セキュリティグループの関連付けも可能。



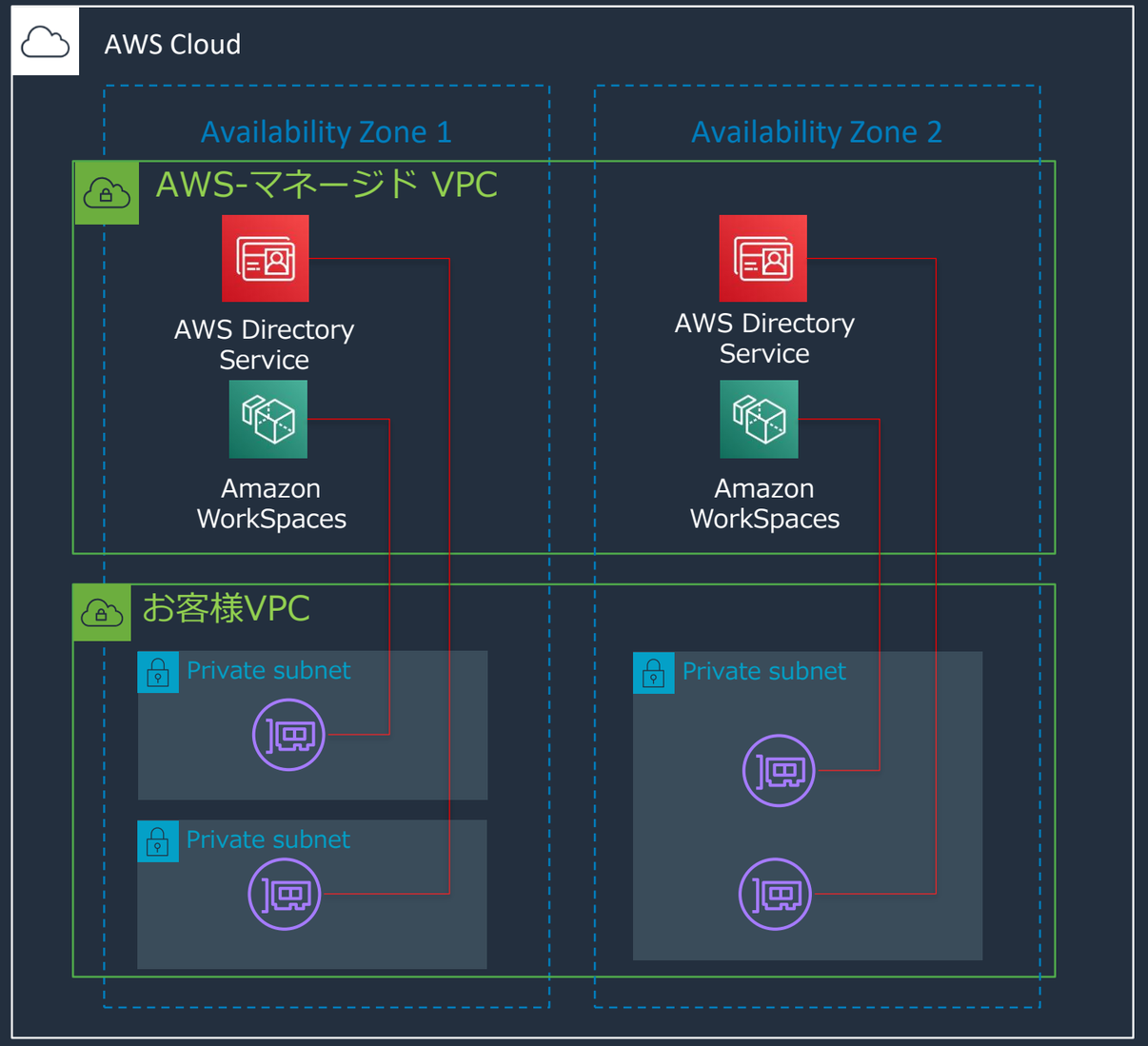
Amazon WorkSpaces VPCの構成

ベストプラクティス（抑えておきたい原則）

- WorkSpaces展開用として、VPCを個別に用意する。
- サブネットは異なるアベイラビリティーゾーンに存在する必要がある。
- WorkSpacesをプライベートサブネットに展開する。
- サブネットのサイズを考慮する。

Amazon WorkSpacesとAWS Directory Serviceについて

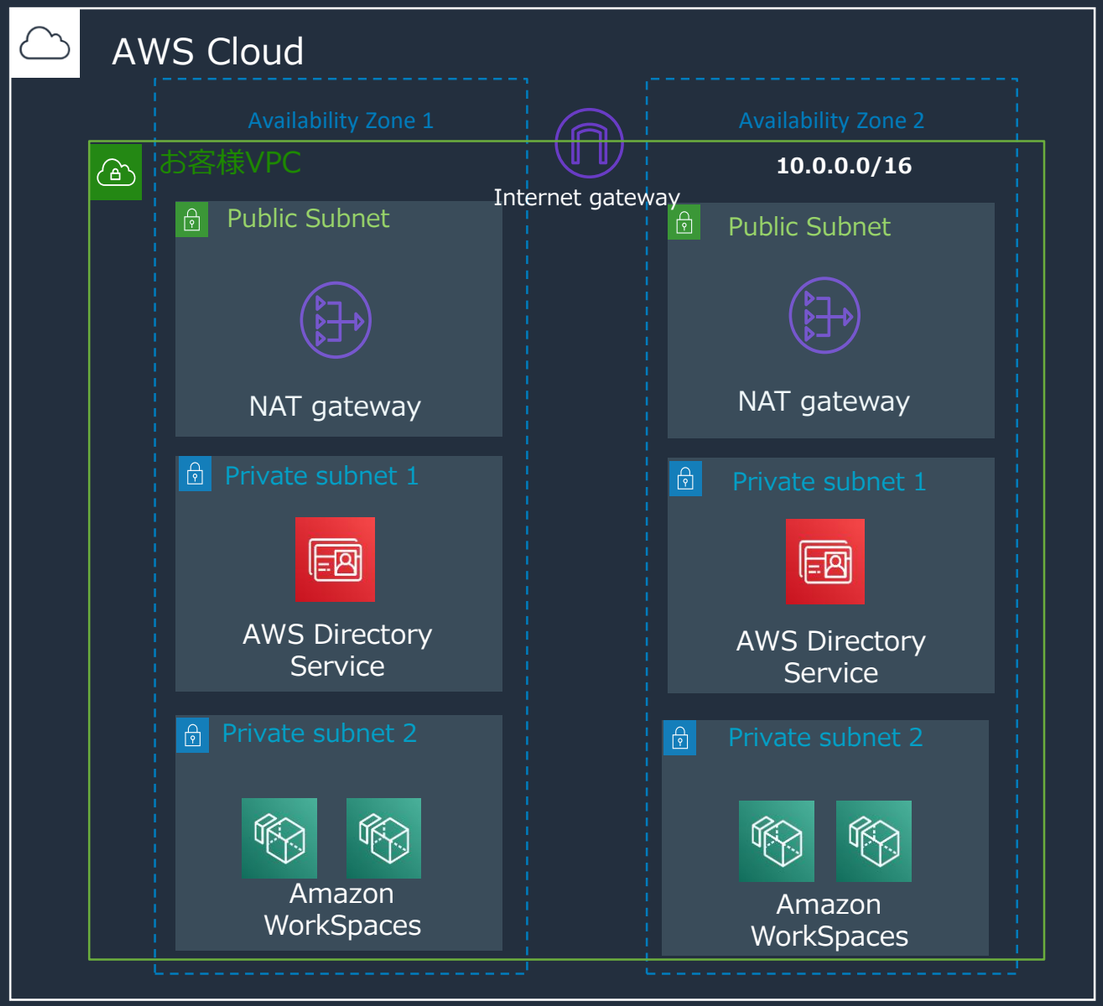
- WorkSpacesは、AWS Directory Service構成に関連付けられます。
- AWS Directory Serviceは、別個のアベイラビリティーゾーンに1つずつ、合計2 つのサブネットが必要になります。
- WorkSpacesのサブネットは、異なるAZになるように2つ選択できる。
- WorkSpacesのサブネットは、AWS Directory Serviceが展開されているいづれかのAZ内のサブネットを展開先として構成できる。
- WorkSpacesを展開時、特定のAZ(サブネット)の指定は出来ない。構成した、サブネットのいづれかに自動的に展開される。



Amazon WorkSpaces のVPCネットワーク

VPC作成の検討ポイントは、EC2利用時と考え方は同じ。

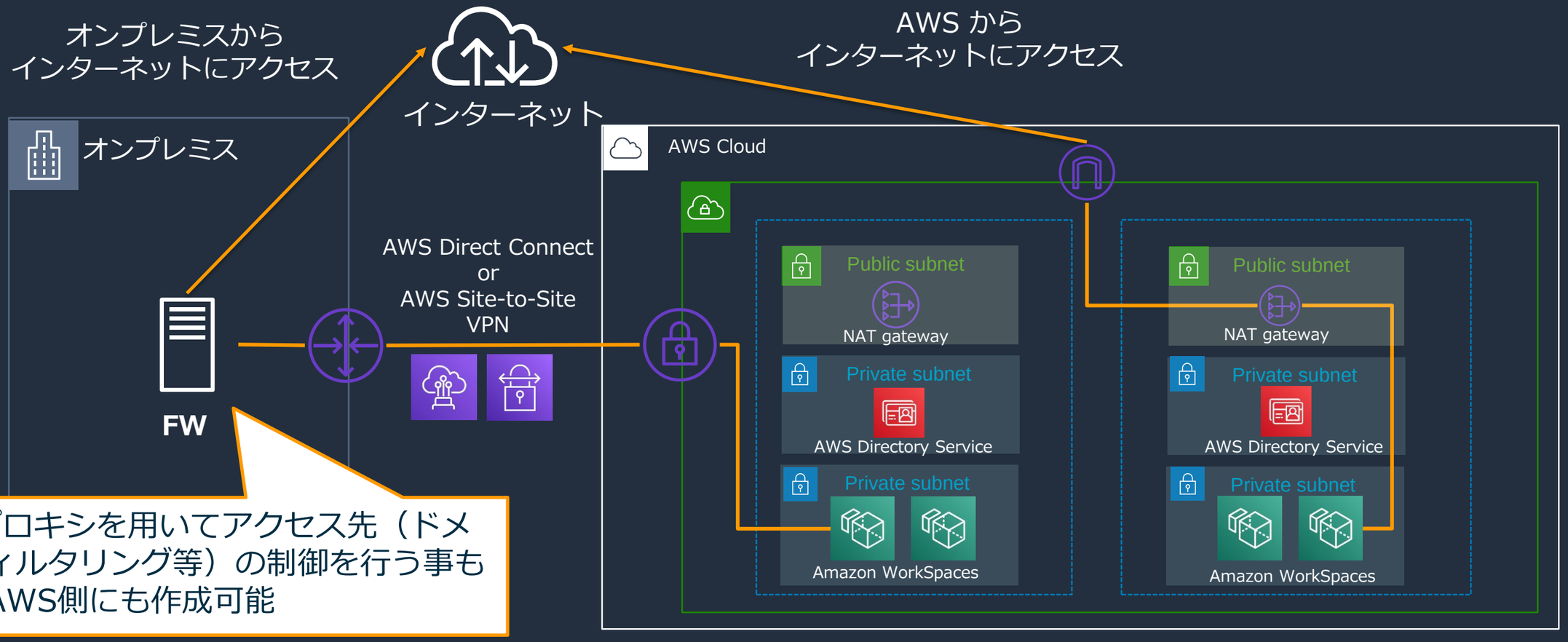
種別	検討ポイント
パブリック サブネット	NAT Gateway やインターネットプロキシなどを配置するサブネット。※WorkSpaces にEIP付与、Publicサブネットに配置することで、直接インターネット接続も可能
プライベート サブネット1 (共用サービス)	Active Directory、ファイルサーバー、ウイルス対策など共通サービスをAWSに配置する際に検討するサブネット。
プライベート サブネット2 (WorkSpaces)	WorkSpaces のインスタンスを配置するサブネット。将来の展開を考慮したサイズを確保。※AD Connector利用時は、Active DirectoryとWorkSpacesは、同じサブネットに構成する必要がある



お客様VPCには、AWS Directory Service/WorkSpacesのENIが作成されるが、便宜上、当該サービスアイコンで表現

インターネットへのネットワークデザイン

- Amazon WorkSpaces からのインターネット接続は、セキュリティ要件に基づき、AWS から直接インターネットにアクセス、もしくは、オンプレミス経由でインターネットにアクセスするかを決める。



Amazon WorkSpaces
ディレクトリサービスの構成

aws

AWS Directory Service

フルマネージド型のディレクトリサービス

- AWS上に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認証との連携も可能
- WorkSpaces は、AWS Directory Service をユーザ認証ディレクトリとして利用する。

AWS Directory Service

AWS Managed Microsoft AD (MSAD)

Microsoft Active Directory(AD) をマネージドサービスで実行

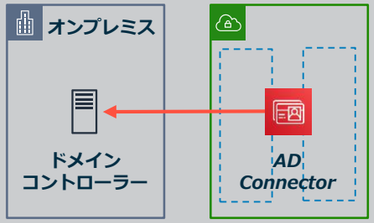
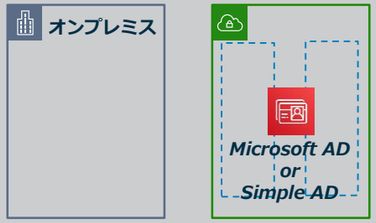
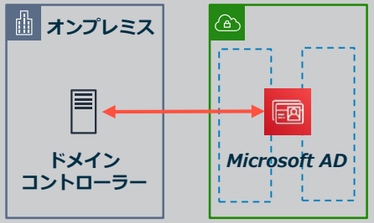
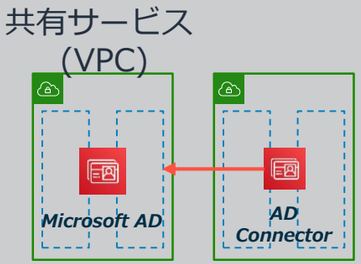
Simple AD

Samba 4 を使用する Microsoft Active Directory(AD) 互換のマネージド型ディレクトリ

AD Connector

オンプレミスの Microsoft Active Directory へリクエストをリダイレクトするディレクトリゲートウェイ

AWS Directory Service 連携パターン

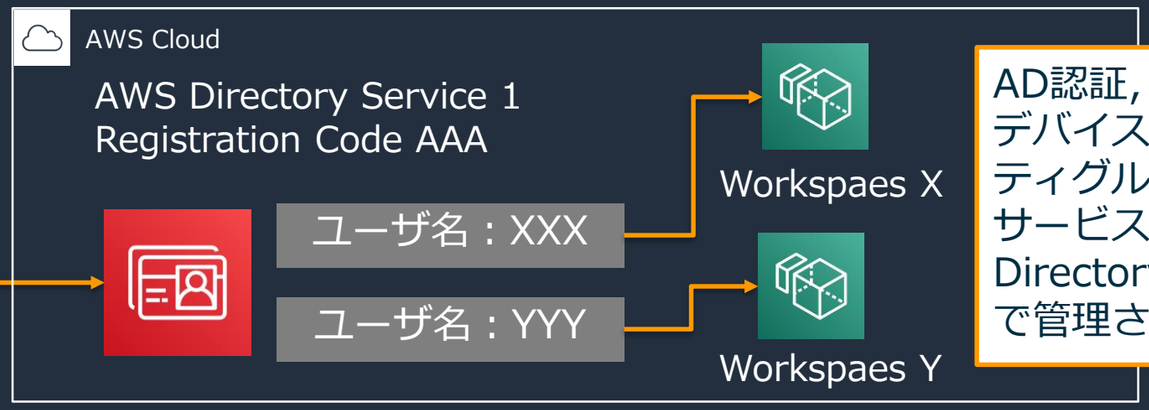
	オンプレミス AD を利用	AWS が提供する AD を利用	オンプレミス AD との信頼関係	共有サービス (VPC)上のADを利用
AD 配置				
AWS 利用サービス	AD Connector (ADC)	•Simple AD •AWS Managed Microsoft AD (MSAD)	AWS Managed Microsoft AD (MSAD)	AD Connector (ADC) AWS Managed Microsoft AD (MSAD)
説明	レオンプレミスに展開されたドメインコントローラーに対して ADC 経由で接続。	MSAD、Simple AD を使用。	MSAD 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。	共有サービス (VPC)に存在するMSADに対して、ADC 経由で接続
検討ポイント	構成はシンプルになるが、オンプレミスへの問い合わせが発生するため認証に時間がかかる。	オンプレミスと独立したドメインとして運用。	オンプレミスと独立したドメインとなるが、信頼関係の構築によりオンプレミスドメインを認証に利用することが可能。	既に共有のADが存在する場合の活用方法。VPC間の接続設計が必要。

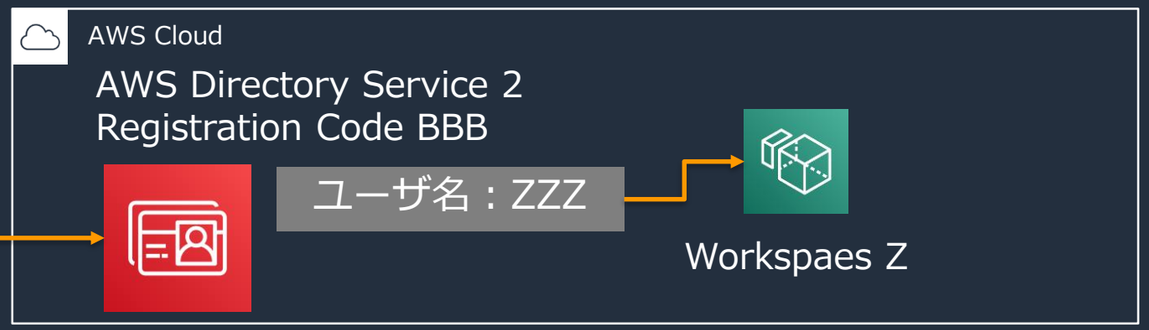
AWS Directory Service とAmazon WorkSpacesの関係

- ディレクトリ内の 1ユーザーあたりに、1つのWorkSpaceが作成可能。
- WorkSpaces の各種設定（セキュリティ設定等）は、AWS Directory Service 単位で管理される。
- 設定を複数パターンで運用したい場合は、別ディレクトリの用意が必要。
- AWS Directory Serviceは、Directory Service単位でRegistration Codeをもつ。ユーザはRegistration Codeを切り替えて別のWorkSpacesへアクセス可能。

アクセス先WorkSpaces	Registration Code	ユーザ名	適応される設定
X	AAA	XXX	Directory Service 1
Y	AAA	YYY	
Z	BBB	ZZZ	Directory Service 2

ユーザ





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単位で管理される

Amazon WorkSpaces
コンピューティング環境

aws

OSとバンドル

用途に応じたデスクトップ環境をWorkSpacesとして提供

OS/Office

- Windows10 or Linux (Amazon Linux2)が利用可。Windows はライセンス持ち込みも可能（詳細は下記表参照）
- Microsoft Officeは、プラスアプリケーションバンドル (15USD) で利用可能
  - Microsoft Office Professional Plus 2016 版 or 2019版
  - プラスアプリケーションバンドルにはTrend Micro Worry-Free Business Security Servicesも同胞（2019版は同胞されない）
  - BYOL(ライセンス持ち込みの場合)でも、 プラスアプリケーションバンドルによるMicrosoft Officeの利用が可能。

	ライセンス込み	ライセンス持ち込み
ライセンス前提	なし	Windows VDA per User
選択可能な OS	Windows 10 デスクトップエクスペリエンス（Windows Server2016/2019 ）	Windows 10
最低展開台数	1 台から利用可	最低 200 台から

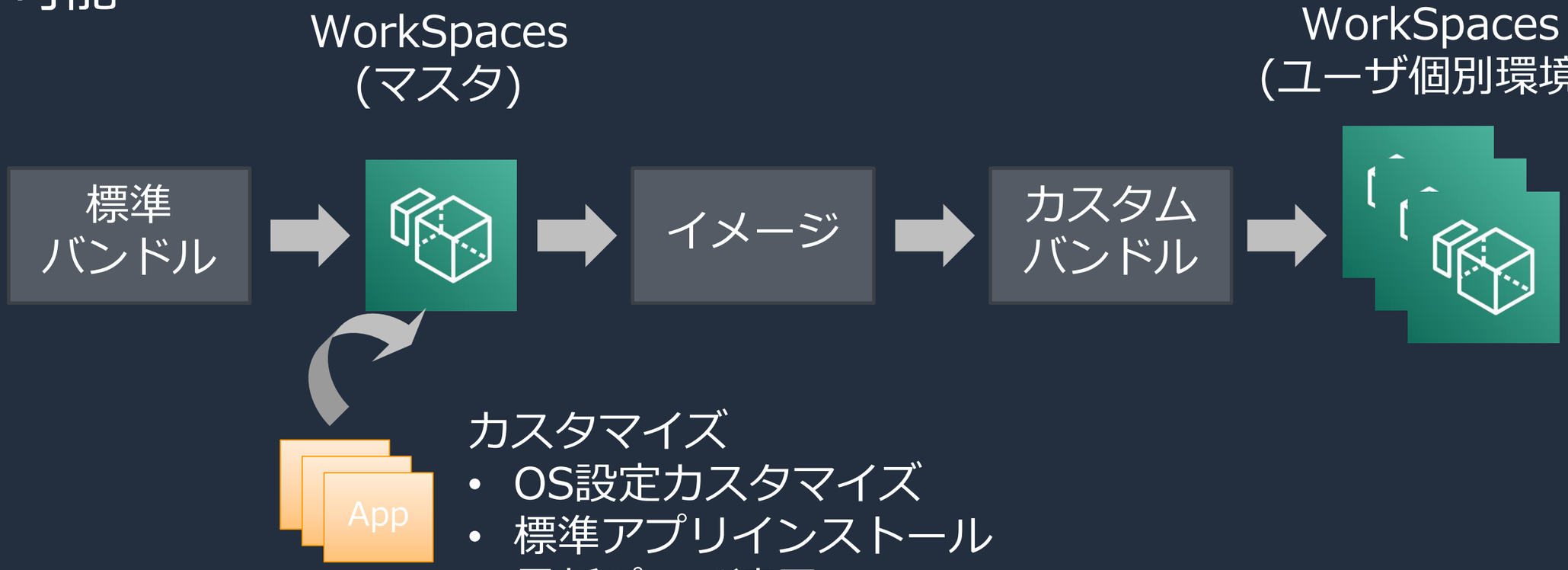
自分の Windows デスクトップライセンスを使用する
https://docs.aws.amazon.com/ja_jp/workspaces/latest/adminguide/byol-windows-images.html

WorkSpaces バンドル

サイズ	構成	想定利用者
バリュー	1vCPU/2GiBメモリ 80GB + 10GB	単一アプリケーションを利用するライトユーザー
スタンダード	2vCPU/4GiBメモリ 80GB + 50GB	複数アプリケーションを利用する一般的な事務ユーザー
パフォーマンス	2vCPU/7.5GiBメモリ 80GB + 100GB	Officeなどを利用する一般的なオフィスユーザー
パワー	4vCPU/16GiBメモリ 175GB + 100GB	高い処理性能を求める開発者などのユーザー
パワープロ	8vCPU/32GiBメモリ 175GB + 100GB	
グラフィック	8vCPU/15GiBメモリ /4GiBビデオメモリ 100GB + 100GB	CADなど GPU を必要とするアプリケーション利用者
グラフィックプロ	16vCPU/122GiBメモリ /8GiBビデオメモリ 100GB + 100GB	

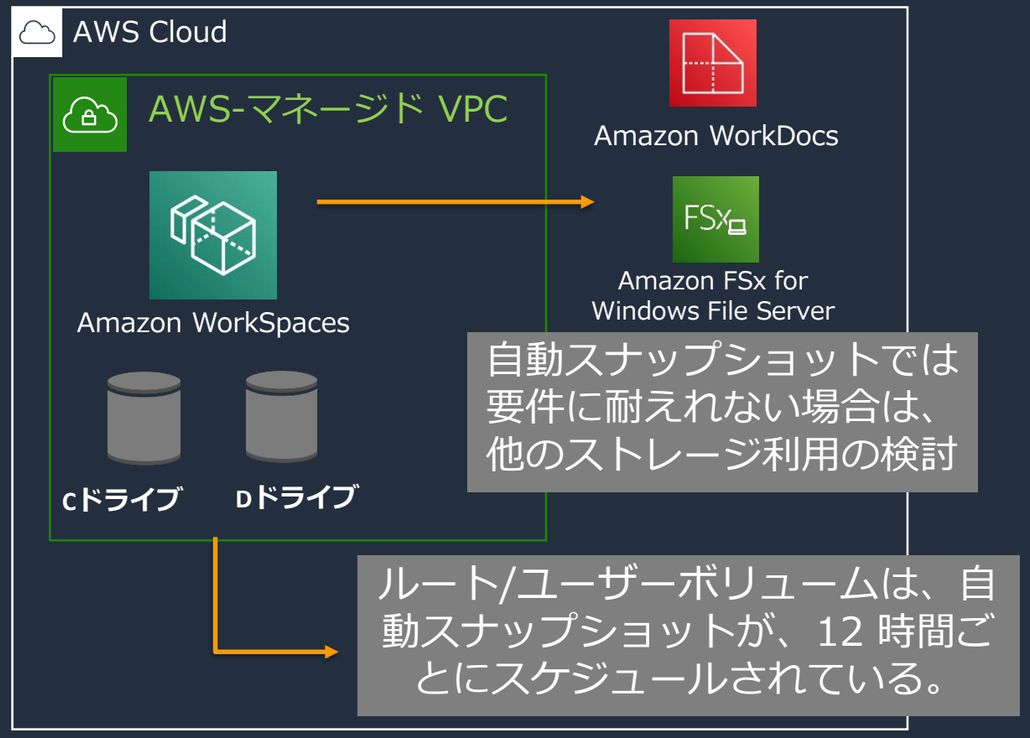
カスタムバンドル

- デスクトップイメージを効率的に管理する仕組みを提供
- WorkSpacesを起動しカスタマイズした後で、WorkSpacesからイメージを作成し、イメージからカスタムバンドルを作成することが可能



ユーザストレージと復元・再構築について

- ストレージは、ルートボリューム (Microsoft Windows の場合はドライブ C、Linux の場合は /) 、ユーザーボリューム (Microsoft Windows の場合は D: ドライブ、Linux の場合は /home) がある。どちらも2000GBまで拡張可能。
- どちらのボリュームも自動スナップショットが、12 時間ごとにスケジュールされている。
- 何らかの要因でWorkSpacesが正常稼働しなくなった場合は、再起動・復元・再構築のアクションが可能



復旧オプション	ルートボリューム	ユーザーボリューム
再起動	未保存のものは消失	未保存のものは消失
復元	スナップショットから戻し（スナップショット採取以降のインストールされたアプリ、または変更されたシステム設定は消失）	スナップショットから戻し（スナップショット採取時点の状態に戻る）
再構築	作成元のバンドルの最新のイメージ（WorkSpaces作成以降のインストールされたアプリ、または変更されたシステム設定は消失）	スナップショットから戻し（スナップショット採取時点の状態に戻る）

課金

- 初期費用なし、1台から利用可能。利用シーンに合わせて月額料金と時間料金から選択。いつでも実行モードを変更可能。

時間料金 (実行モード：Auto Stop)

- 時間単位の従量課金 + インフラストラクチャのコスト
- デスクトップへのアクセス時間が限られる用途に最適
- WorkSpace が切断され、指定した自動停止時間（最小1時間から）が経過すると、自動的に停止し、課金が停止する。
- 停止については可能な場合は、WorkSpace のルートボリュームにデスクトップの状態が保存される。

月額料金 (実行モード：Always ON)

- 仮想デスクトップへのアクセス時間に関わらず、月額固定料金の請求
- フルタイムでの利用に最適
- 常に電源がONの為、接続時にすぐに利用できる
- 約80時間以上の利用であれば、月額料金が安価

WorkSpaces Cost Optimizer

- 最適な課金モデルを自動選択しコストを最適化
- WorkSpacesの利用実績をモニタリング
  - 個々のWorkSpacesの利用時間により、最も安価な課金モデルに自動的に変更 (時間料金 / 月額料金)
  - Dry-run, タグによる除外をサポート
  - 未使用のWorkSpacesを削除することも可能
- CloudFormationで自動的にデプロイ
- コストは$0.2/月程度
  - WorkSpaces 25台のケース
  - WorkSpaces 本体のコストは除く

Amazon Workspaces Cost Optimizer | AWS Solutions
https://aws.amazon.com/jp/solutions/amazon-workspaces-cost-optimizer/

Amazon WorkSpaces
クライアント環境

aws

接続クライアントの種類

- サポートされているデバイスのクライアントアプリケーションまたは、WebブラウザからWorkSpaceに接続できます

	トラディショナルPC	シンクライアント ゼロクライアント	モバイルデバイス	Web ブラウザ
				
説明	Windows、macOS、Linux OS を搭載した PC 端末。	仮想デスクトップ (VDI) への接続に特化した専用端末。	iOS, Android, Chrome OS などが入ったモバイル端末。	Windows, Mac, Linux 上で動作する Web ブラウザ。
対応OS バージョン (詳細はHPを確認ください)	•Windows 7, 8, 10, 11 •Mac OS 10.8.1 以降 •Ubuntu 18.04	•Tera2 zero client firmware 6.0.0 以降	•iOS 8.0 以降 (iPad 2, Retina, Mini)、iOS 9.0 以降 (iPad Pro) •Android OS 4.4以降 •Chrome OS 45 以降 •Amazon Fire OS 4.0以降	**PCoIP** •Google Chrome(最新版) •Firefox (最新版) **WSP** • Google Chrome など Cromium ベースのウェブブラウザ

WorkSpacesクライアント
https://docs.aws.amazon.com/ja_jp/workspaces/latest/userguide/amazon-workspaces-clients.html

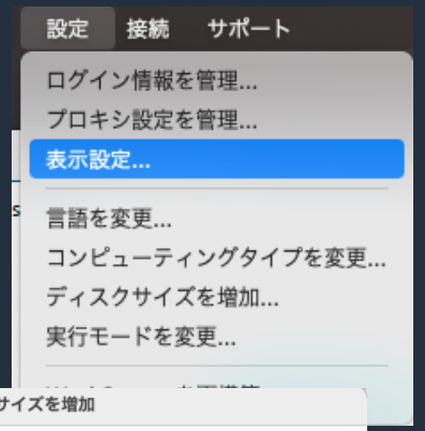
WorkSpacesクライアント周辺機器のサポート
https://docs.aws.amazon.com/ja_jp/workspaces/latest/userguide/peripheral_devices.html

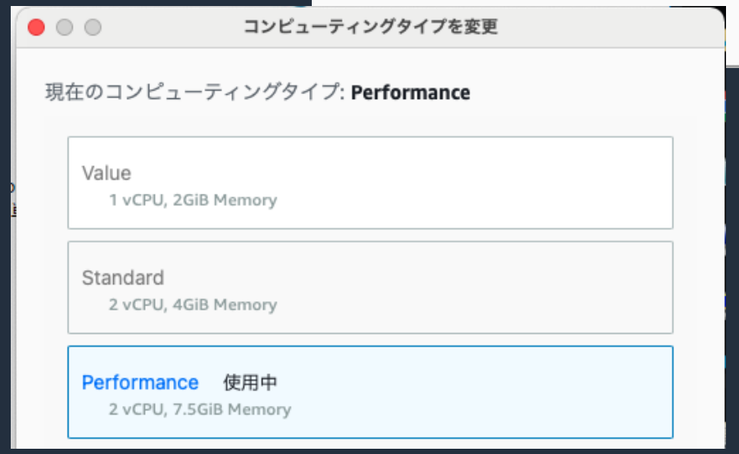
ユーザーセルフサービス管理機能

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。

以下のオペレーションを実行可能　（Web Access では利用できない）

- WorkSpaces の再起動
- ディスクサイズの増加
  C：ドライブ（Linuxの場合は/）のサイズを最大175 GBまで
  D：ドライブ（Linuxの場合は/ home）のサイズを最大100GB
  これ以上の拡張は管理者で実施
- 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





Amazon WorkSpaces
セキュリティ対策

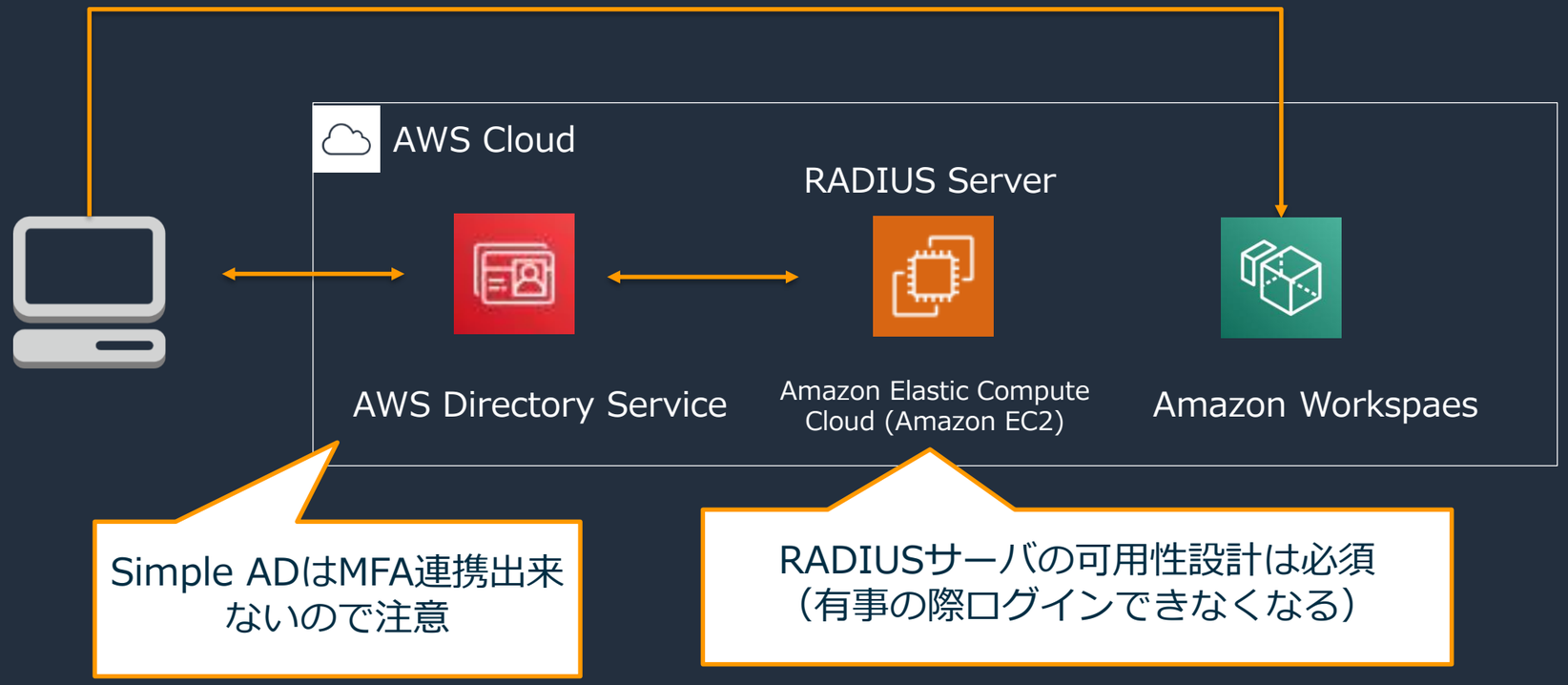
セキュリティ

マルチレイヤーのセキュリティ設定を行い、アクセスセキュリティを強化。

セキュリティ設定	説明
ユーザー認証	Active Directoryドメイン認証。
多要素認証 (MFA)	RADIUSベースの多要素認証ソリューションと連携。 •商用ソリューション/OSSソリューション
データ暗号化	保管時 (ストレージ)、転送中 (プロトコル) のデータを暗号化。
グループポリシー	グループポリシーによりクライアントからのアクセスポリシーを制御。 •クリップボード/プリンター/Kerberos チケットのライフタイム
IP アクセス コントロール	Amazon WorkSpaces への接続元として使用できる IP アドレスを制御。 (ゼロクライアントは利用不可)
デバイスタイプ制御	デバイスタイプ毎にアクセス許可・拒否を設定。 •Web Access • ChromeOS • Windows •iOS • ゼロクライアント • Mac •Android • Linux
証明書による デバイス認証	証明書ベースの認証を使用し、信頼されたデバイスからのみアクセスを許可。 （Windows、macOS、Android/ChromeOS が利用可能)

MFA認証による認証の強化

- AWS Directory Serviceとの連携を行い、MFA認証による追加認証の実装が可能。
- 実装にはRADIUS サーバの用意 or SaaS型MFAサービスとの連携が必要。
- AD ConnectorによるオンプレミスAD連携時にもMFA実装が可能。
- Simple ADは、MFAオプションが利用出来ないので注意。



MFA連携に関する 参考情報

多要素認証による Amazon WorkSpaces の利用
https://www.slideshare.net/AmazonWebServicesJapan/amazon-workspaces-86568155

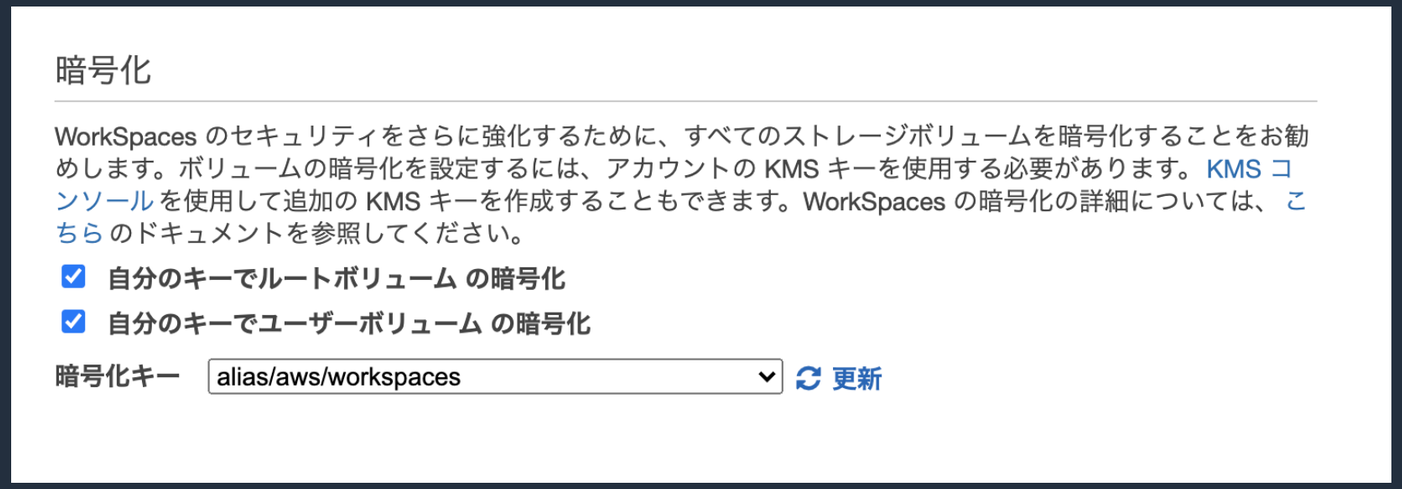
Integrating FreeRADIUS MFA with Amazon WorkSpaces
https://aws.amazon.com/jp/blogs/desktop-and-application-streaming/integrating-freeradius-mfa-with-amazon-workspaces/

Azure MFAサーバーを使用したAmazon WorkSpacesの多要素認証
https://aws.amazon.com/jp/blogs/news/amazon-workspaces-multi-factor-authentication-using-azure-mfa/

Integrating Okta MFA with Amazon WorkSpaces
https://aws.amazon.com/jp/blogs/desktop-and-application-streaming/integrating-okta-mfa-with-amazon-workspaces/

データ暗号化

- AWS Key Management Service（ AWS KMS ）を利用して、WorkSpaces のルートボリューム およびユーザーボリューム を暗号化可能。
- AWS 管理の CMK or カスタマー管理のCMK(※)を利用できる。
- 既存の WorkSpaces は暗号化できない。WorkSpacesを起動するときに、暗号化する必要がある。暗号化されたら、無効化は出来ない
- 暗号化された WorkSpaces からのカスタムイメージの作成はできない。
- 暗号化された WorkSpaces を再起動、再構築または復元は利用されている AWS KMS CMK が有効であることが必要。

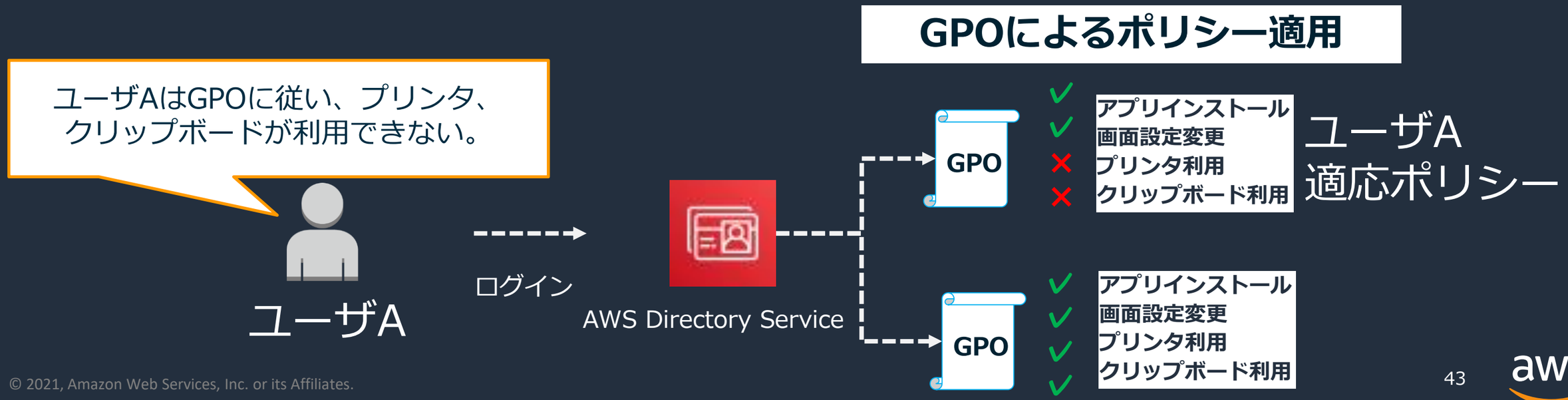


カスタマー管理 CMK (※)を使用する場合は、アカウントの WorkSpaces 管理者に代わって CMK を使用する WorkSpaces 許可を与える必要あり。
https://docs.aws.amazon.com/ja_jp/workspaces/latest/adminguide/encrypt-workspaces.html#kms-workspaces-permissions

(※)カスタマーが作成したカスタマーマスターキー(CMK)

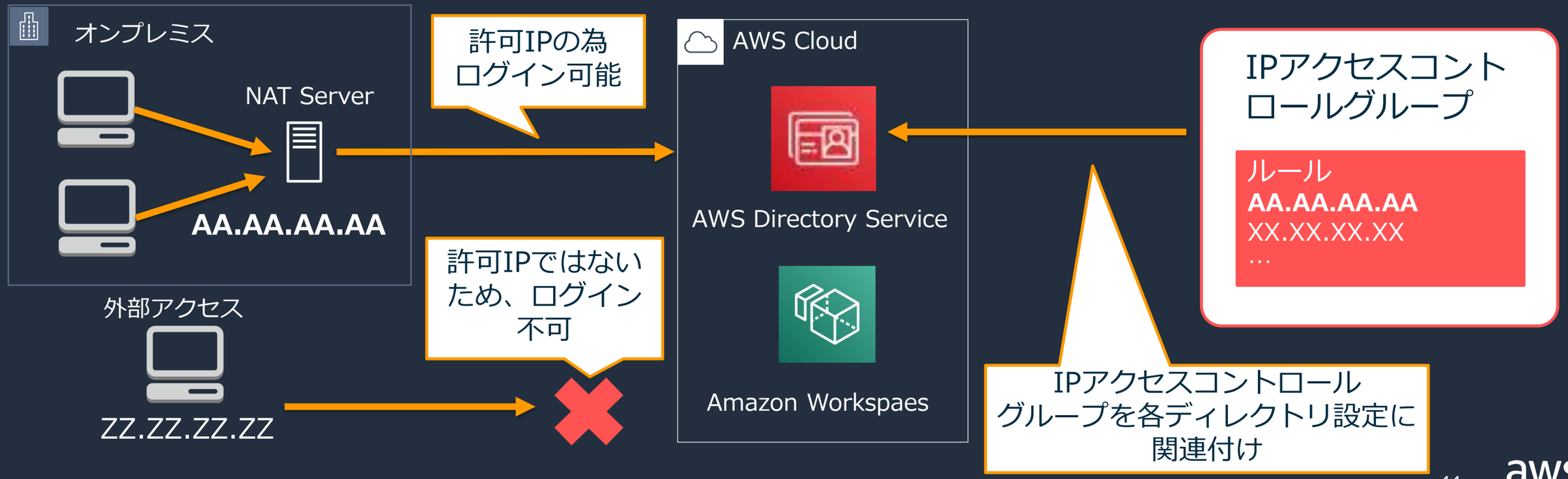
グループポリシー（GPO）による制御

- 通常のActive Directoryと同様、コンピューターやユーザーのポリシーについてはリンクした OU に対して設定することが可能
- WorkSpaces に固有のグループポリシー設定（クリップボードのリダイレクト等）を使用するには、使用しているプロトコル (PCoIP または WSP) のグループポリシー管理用テンプレートをインストールする必要があるので注意
  ※従来の一般的なWindowsのグループポリシーも利用可能
- 管理テンプレートのインストール等は、ドキュメントを確認
  https://docs.aws.amazon.com/ja_jp/workspaces/latest/adminguide/group_policy.html



IPアクセスコントロールグループ

- WorkSpaces への接続元として使用できる IP アドレスを制御できる機能
- IP アクセスコントロールグループにルール（ CIDR アドレス範囲を記載）を追加し、グループをディレクトリに関連付ける。
- ルールに拠点IPを設定し、特定拠点以外からはアクセス出来ないように制御可能



証明書によるデバイス認証・デバイスタイプ制御

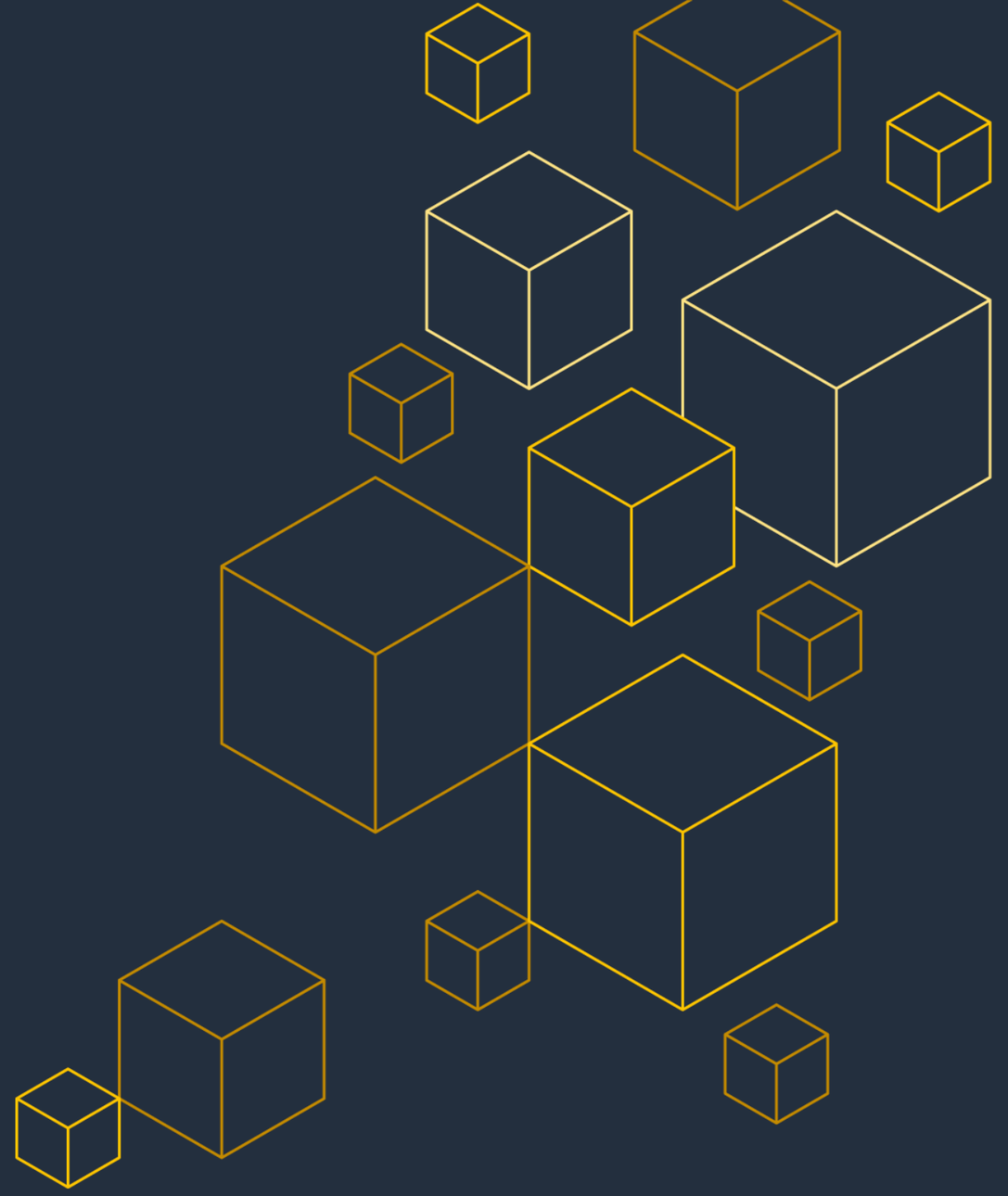
- 証明書ベースの認証を使用して、信頼されたデバイスからのアクセス制御が可能
- クライアント側への証明書の配布・インストールが必要。
- サポートされるクライアントに制限があるので注意

ディバイス別に適応状況をセット
Windows・macOS・Android/ChromeOSでの制御が可能

ルート証明書のインポート
（2つ可能）

その他のプラットフォームの制御
証明書ベースで制御出来ないプラットフォームを「ブロック」することも可能

Amazon WorkSpaces
最新アップデート



2019 Amazon WorkSpces アップデート

- Amazon WorkSpaces が AWS GovCloud (米国西部) リージョンで利用可能に
- Amazon WorkSpaces が WorkSpaces ディレクトリ、イメージ、カスタムバンドル、IP アクセスコントロールグループ向けのタグ付けのサポートを開始
- Amazon WorkSpaces で AWS リージョンをまたいだイメージのコピーが可能に
- Amazon WorkSpaces で、異常発生前の最後の状態に復元する機能を導入
- Amazon WorkSpaces が、中国 (寧夏) リージョンで利用可能に
- Amazon WorkSpaces に WorkSpaces Directory API を導入
- Amazon WorkSpaces パブリック API が AWS PrivateLink でサポートされるようになりました
- Amazon WorkSpaces が Linux 向け WorkSpaces 3.0 Client を導入
- Amazon WorkSpaces Streaming Protocol (ベータ版) の紹介

2020 Amazon WorkSpces アップデート

- Amazon WorkSpaces の移行により、Windows 10 デスクトップエクスペリエンスおよびベータ版の新しい WorkSpaces ストリーミングプロトコルへの移行が可能に
- 新しい Amazon WorkSpaces クライアントのリリース
- NWCD の運営により、AWS 中国 (寧夏) リージョンでの Amazon WorkSpaces の BYOL (自分のライセンスを使用する) オプションの利用を開始
- Amazon WorkSpaces が AWS リソースグループタグエディタのサポートを開始
- Amazon WorkSpaces の Windows ライセンス持ち込み WorkSpaces で Microsoft Office Professional バンドルへのサブスクライブが可能に
- Amazon WorkSpaces がクロスリージョンリダイレクトのサポートを導入
- Amazon WorkSpaces がエンドユーザーコンピューティングダッシュボードをデプロイするためのセルフガイドワークショップをリリース
- Amazon WorkSpaces がアカウント間でのイメージの共有を導入
- Amazon WorkSpaces ストリーミングプロトコル (ベータ版)

2021 Amazon WorkSpaces アップデート

- Amazon WorkSpaces がアジアパシフィック (ムンバイ) リージョンで利用可能に
- 新しい AWS ソリューションコンサルティングサービス - Virtual Desktop Accelerator
- バンドル管理 API が Amazon WorkSpaces で一般的に利用可能に
- 新しい AWS ソリューションコンサルティングサービス - WorkSpaces Manager for Amazon WorkSpaces
- Amazon WorkSpaces が WorkSpaces macOS クライアントアプリケーションでスマートカードのサポートを開始
- Amazon WorkSpaces でのウェブカメラのサポートの一般提供を開始
- AWS エンドユーザーコンピューティングのための新しいデジタルトレーニングと AWS 認定ガイド
- Amazon WorkSpaces コストオプティマイザー v2.3 では、既存の VPC のサポートが追加され、請求の正確性とレポートが改善
- セルフサービスの機能と信頼されたデバイスのサポートが、Amazon WorkSpaces Android クライアントアプリで利用可能に

2021 Amazon WorkSpaces アップデート

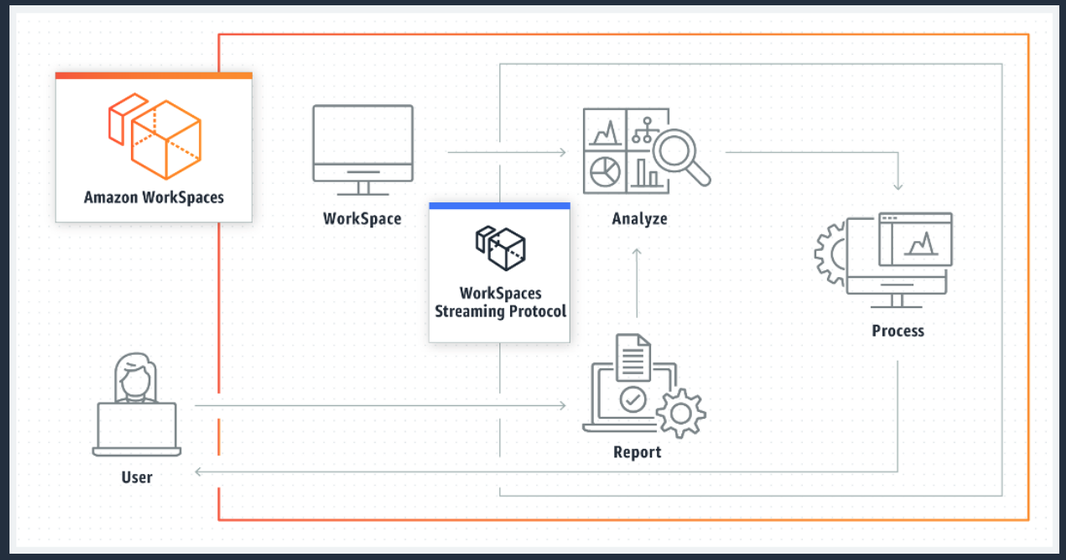
- Amazon WorkSpaces が WorkSpaces Streaming Protocol (WSP) によるウェブアクセスの提供を開始
- Amazon WorkSpaces が PCoIP Windows WorkSpaces で USB YubiKey Universal 2nd Factor (U2F) 認証のサポートを追加
- Amazon WorkSpaces 、Service Quotas によるクォータ情報の提供を発表
- AWS Directory Service が 5 つの追加の AWS リージョンで Amazon WorkSpaces 用の AD Connector を使用したスマートカード認証のサポートを開始
- Amazon WorkSpaces が、Windows Server 2019 バンドルおよび 64 ビット Microsoft Office 2019 で Windows デスクトップエクスペリエンスを更新
- Amazon Workspaces Cost Optimizer v2.4 のご紹介
- Amazon WorkSpaces Windows Server 2019 バンドルが AWS GovCloud (米国西部) リージョンで利用可能に
- 最新の AWS ドライバーで更新された新しいイメージを作成するための Amazon WorkSpaces API の発表

Amazon WorkSpaces Streaming Protocol (WSP)

ネットワーク環境に影響されづらい

一貫したユーザーエクスペリエンスを提供

- WebCamリダイレクト
- スマートカード認証
  - セッション前 認証 (※1)
  - セッション内 認証
- WebAccessでも利用可能

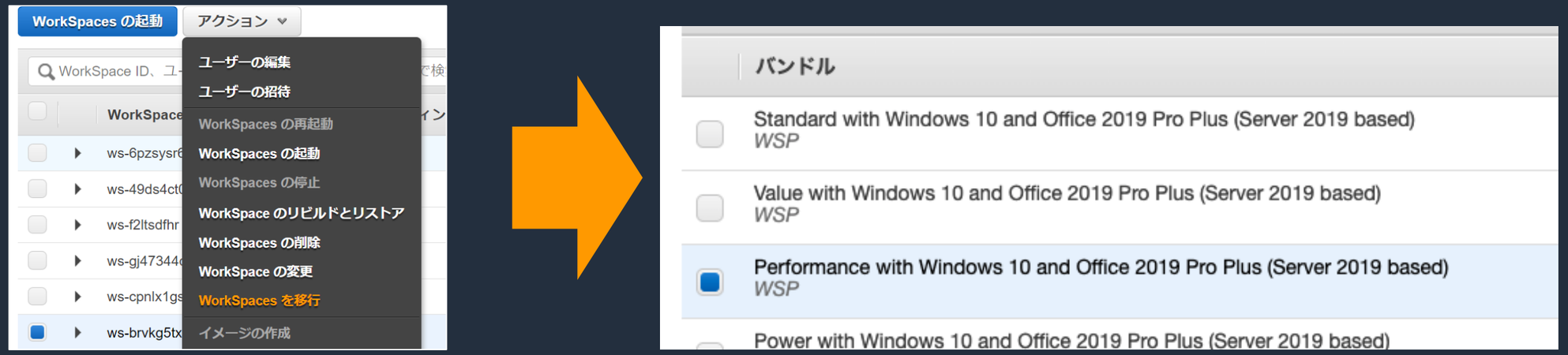


※1：セッション前 認証は、特定リージョンで利用可能。詳細は、ドキュメント参照
https://docs.aws.amazon.com/ja_jp/workspaces/latest/adminguide/smart-cards.html#smart-cards-limitations

カメラを利用する際は、クライアントアプリの接続→デバイスからカメラを選択

Amazon WorkSpaces Streaming Protocol (WSP)を利用するには？

- 新規で利用する場合は、WSP用のバンドルを選択
- 既存PCoIPベースの環境をWSPに変更する場合には、WorkSpaceの移行が必要
  移行あたっては、ユーザーボリュームはスナップショットが利用され、ルートボリュームのデータは保持されない



BYOL WorkSpaces バンドルでMicrosoft Officeを利用可能

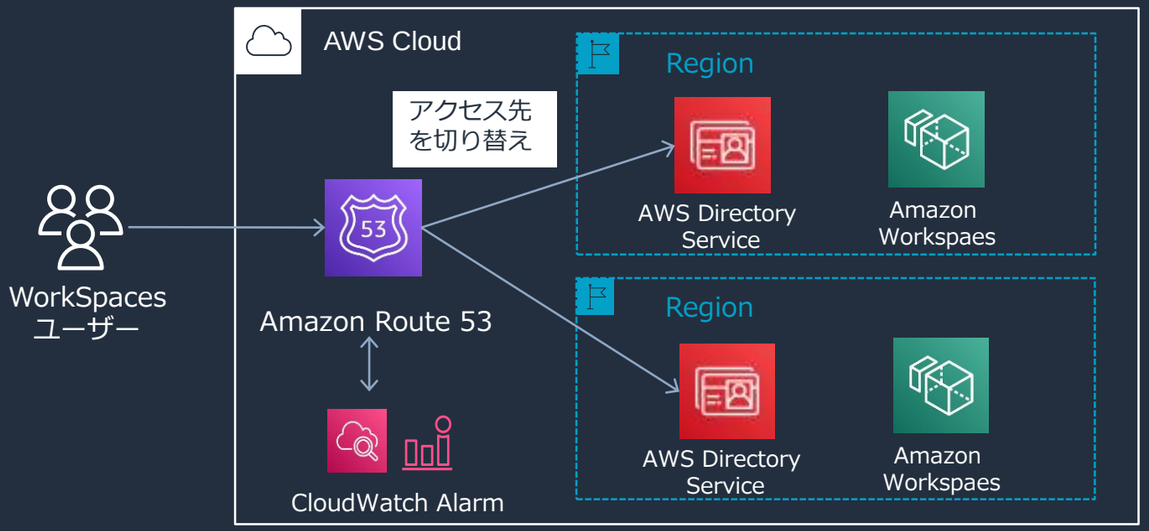
Microsoft Office Professional Plusを月額14.75 の追加料金で
BYOL WorkSpaces (Windows 10)環境でもご利用いただけます。

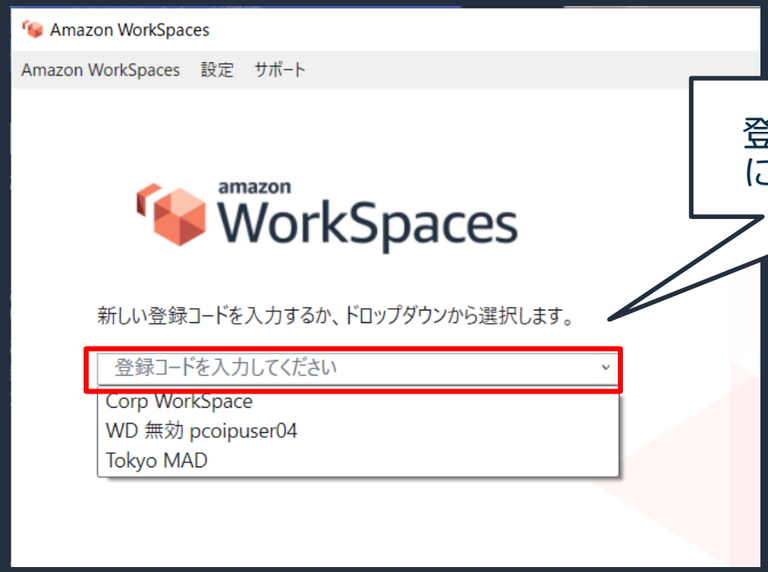
Amazon WorkSpaces コンソールで BYOL イメージを作成する際に、
イメージにOffice をプリインストールできる。

アプリケーションバンドル	アプリケーション	追加の月額料金
デフォルトのアプリケーションバンドル	ユーティリティ (Internet Explorer 11、Firefox)	追加料金なし
BYOL WorkSpaces bundle 向け Microsoft Office	Microsoft Office Professional Plus	追加で 14.75USD/月

クロスリージョン リダイレクションでWorkSpacesを自動切換え

- プライマリリージョンに到達できない場合に、セカンダリリージョンにリダイレクト
- DNSのヘルスチェックおよびフェイルオーバー機能を使用
- Amazon Route53を使用する場合は、Amazon CloudWatchのアラームを監視するヘルスチェックを利用できる
- ユーザデータはリージョン間で同期されない為、データ同期の仕組みを検討する必要がある (3rd パーティ製品、Amazon WorkDocs、Amazon FSx等)





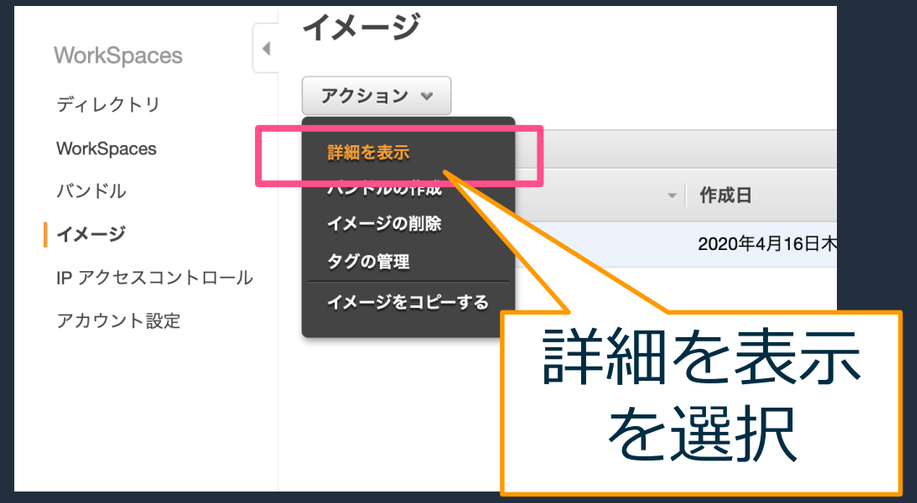
WorkSpacesクライアントでの登録コードの手動切り替えは不要に

Amazon WorkSpaces アカウント間でのイメージの共有を導入

- AWS アカウント間で Amazon WorkSpaces のイメージを共有することがセルフで実施できるようになった。
（以前はサポートへの依頼が必要だった）

- 共有イメージを使用するには、まず受信者アカウントでイメージをコピーする必要がある

https://docs.aws.amazon.com/ja_jp/workspaces/latest/adminguide/share-custom-image.html



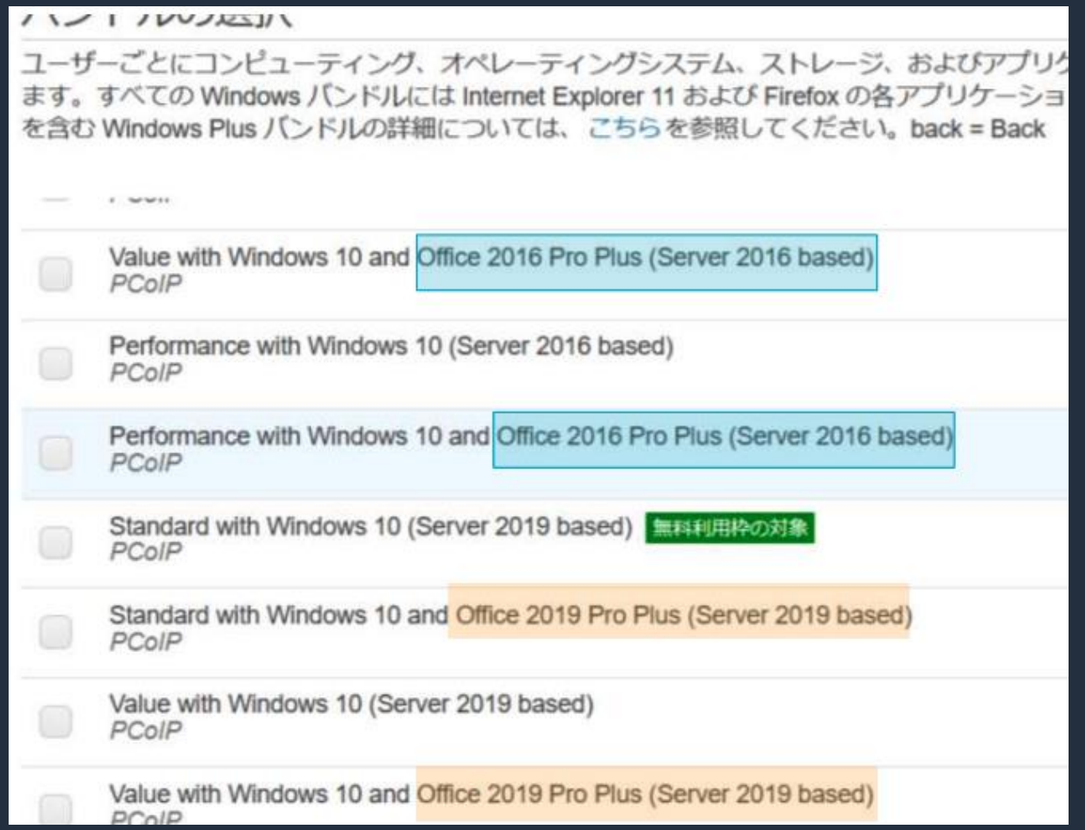
Windows Server 2019 バンドル/Microsoft Office 2019の提供開始

- Windows10 (2019) デスクトップエクスペリエンス (Windows Server 2019 ベース) の提供開始

- Windows Server 2019で拡張された様々な機能が利用可能
  例) 機能拡張されたLinux用のWindowsサブシステム (WSL)

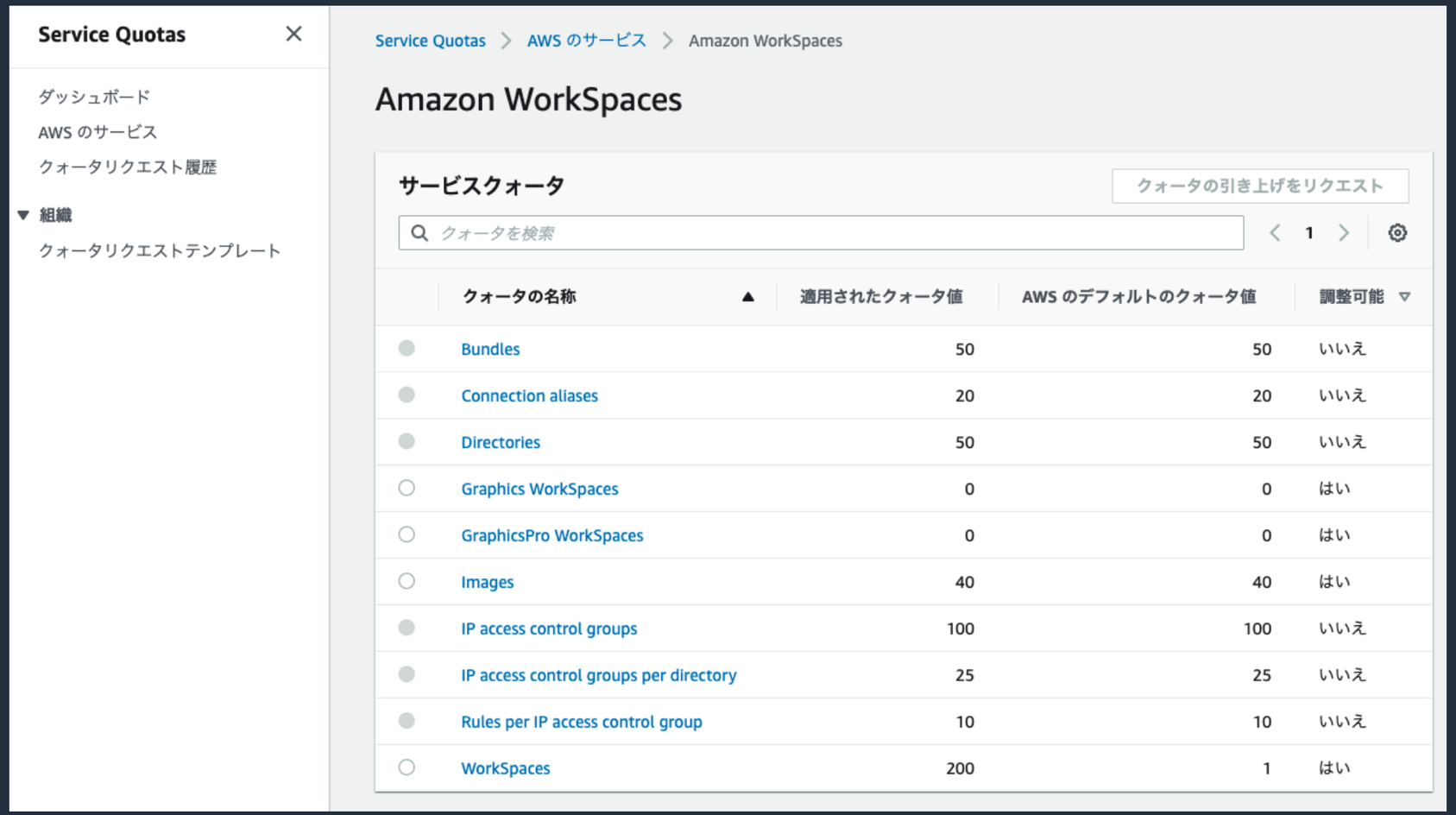
- Windows 10 (2019)アプリケーションバンドルでは、64 ビット Microsoft Office 2019 Professional Plusが付属される

※ Windows Server 2016 ベースも引き続き利用可能
※ Windows 10 (2019)アプリケーションバンドルオプションには、Trend Micro Worry-Free Business Securityは付属されません



Service Quotas によるクォータ情報の提供を発表

- Service Quotas を利用して、AWS のサービスのサービスクォータ情報を一元的に監視および管理が可能



Amazon WorkSpaces
まとめ

aws

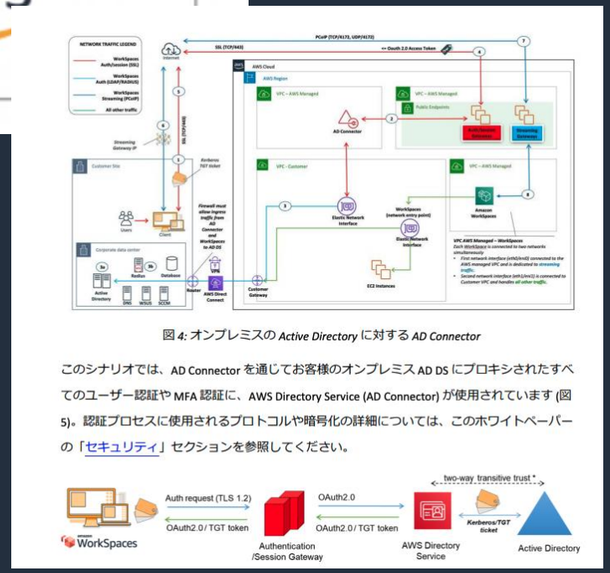
まとめ

- フルマネージド型の仮想デスクトップサービス
- 環境初期投資が不要で、１台からすぐに始められる
- 適切なアーキテクチャ設計が重要
  - ネットワーク
  - ディレクトリサービスの構成
  - コンピューティング環境
  - クライアント環境
  - セキュリティ対策

【ご参考】Amazon WorkSpaces デプロイメント ベストプラクティス 日本語版のご案内

- 企業や組織において展開いただく上での ベストプラクティス

- デプロイメントに関する一連のプラクティス をカテゴリで紹介
  - ネットワーク
  - ディレクトリサービスとユーザー認証
  - セキュリティ
  - モニタリングとログ



ご紹介のブログHP(ブログ内にホワイトペーパーへのリンクがございます)
https://aws.amazon.com/jp/blogs/news/amazon-workspaces-deployment-practice-jp-2020/

その他の情報

- Amazon WorkSpaces の運用管理
  - https://pages.awscloud.com/rs/112-TZM-766/images/B2-03.pdf
- 予測できない変化にブレないニューノーマルな働き方を-

  Amazon WorkSpacesフルマネージドVDI ベストプラクティス
  - https://pages.awscloud.com/rs/112-TZM-766/images/AWS-17_AWS_Summit_Online_2020_EUC01.pdf
- AWS ナレッジセンター（ビジネスアプリケーションからAmazon WorkSpacesを選択）
  - https://aws.amazon.com/jp/premiumsupport/knowledge-center/
- Amazon Web Services ブログ（カテゴリ Amazon WorkSpaces）
  - https://aws.amazon.com/jp/blogs/news/category/desktop-app-streaming/amazon-workspaces/

本資料に関するお問い合わせ・ご感想

- 技術的な内容に関しましては、有料のAWSサポート窓口へ
  お問い合わせください
  - https://aws.amazon.com/jp/premiumsupport/
- 料金面でのお問い合わせに関しましては、カスタマーサポート窓口へ
  お問い合わせください（マネジメントコンソールへのログインが必要です）
  - https://console.aws.amazon.com/support/home#/case/create?issueType=customer-service
- 具体的な案件に対する構成相談は、後述する個別技術相談会をご活用ください

ご感想はTwitterへ！ハッシュタグは以下をご利用ください
#awsblackbelt

AWSの日本語資料の場所「AWS 資料」で検索

https://amzn.to/JPArchive

AWSのハンズオン資料の場所「AWS ハンズオン」で検索

https://aws.amazon.com/jp/aws-jp-introduction/aws-jp-webinar-hands-on/

AWS Well-Architected個別技術相談会

- 毎週「W-A個別技術相談会」を実施中
  - AWSのソリューションアーキテクト（SA）に対策などを相談することも可能

- 申込みはイベント告知サイトから
  - https://aws.amazon.com/jp/about-aws/events/

AWS イベント で[検索]

ご視聴ありがとうございました