

# AWSインフラ構築スターターパック

AWS認定  
構築サービス

本サービスはAWSファンデーションナルテクニカルレビュー(FTR)を通過したAWS認定ソリューションです。

ダイワボウ情報システム株式会社  
クラウドテクノロジー部  
クラウド基盤グループ

# 改定履歴

- スタートアップは、お客様のご要望の多い機能やサービスを随時追加していきます。

2021年9月8日	・サービスリリース
2021年12月24日	・死活監視と通知オプションにCPU、メモリ、HDDの使用率監視機能を追加
2022年5月30日	・Amazon RDS Microsoft SQL Serverの構築を追加
2022年7月4日	・スタートトレーニングにRDSを追加、自習用コンテンツに変更
2022年9月1日	・ALB(Application Load Balancing)の構築とURL監視オプションを追加
2022年11月24日	・Amazon RDS for Oracleの構築を追加
2022年12月15日	・Amazon RDS for MySQL と PostgreSQLの構築を追加
2023年4月18日	・EC2自動起動停止オプションとCloudFrontオプションを追加
2023年6月12日	・チャット通知オプションとWAF PoCオプションを追加
2023年7月26日	・Patch Managerオプションを追加
2023年8月22日	・カスタマーゲートウェイサービスオプションと休日日中対応オプションを追加
2023年10月18日	・EC2自動起動停止オプションの対象サービスをMaintenance Windowsに変更
2024年2月13日	・Amazon EFS オプションとClient VPNオプションを追加
2024年6月19日	・Auto Scaling PoC/VPCピアリング/Entra連携オプションを追加
2024年11月19日	・AWS FTRを通過し、「AWS Qualified Software」として認定されました
2025年3月24日	・Route53オプションを追加

# スターターパックとは？

- これからAWSによるクラウド化を始める方向けに基本となるインフラ環境を構築するサービスです。
- AWS専門のチームが設計フェーズからサポートいたします。
- ベースとなる基本セットにオプションのメニューを追加頂くことで柔軟なカスタマイズが可能です。
- 本サービスはAWSファンデーションアルテクニカルレビュー(FTR)を通過したAWS認定ソリューションです。詳しくは[こちら](#)



AWSのクラウドを利用したいが、構築経験が無い  
ためAWSのインフラ環境を作成してほしい



専門家に相談しながらベストプラクティスに基づいた  
AWSのインフラ環境を作り上げたい

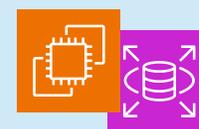


自社サービスの展開を検討しており、  
AWS環境を利用したサービスを作成したい

## 基本セット



Amazon VPC  
(ネットワーク)



Amazon EC2 or RDS  
(仮想インスタンス)



Amazon EBS  
(ストレージ)



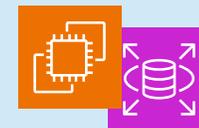
AWS Backup  
(バックアップ)



## オプション



AWS Site-to-Site VPN  
(サイト間VPN)



Amazon EC2 or RDS追加  
(仮想インスタンスの追加)

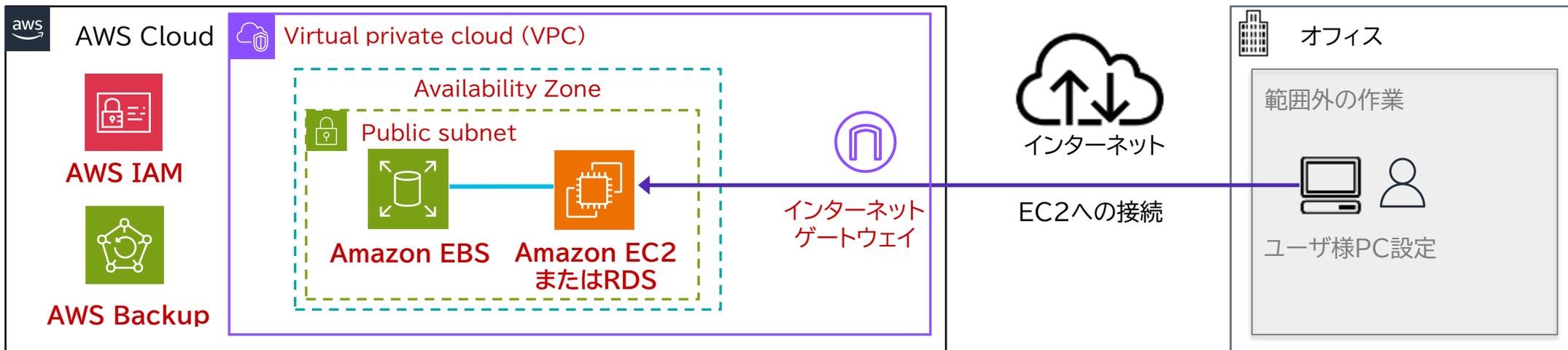


Amazon CloudWatch  
(監視)

# 基本セットに含まれる構築サービスについて

- アカウント作成、仮想ネットワーク、仮想インスタンス、仮想ストレージ、バックアップのサービスが基本セットに含まれます。
- 基本セットに含まれる仮想インスタンスはEC2またはRDSの1台ですが、オプションで追加することも可能です。

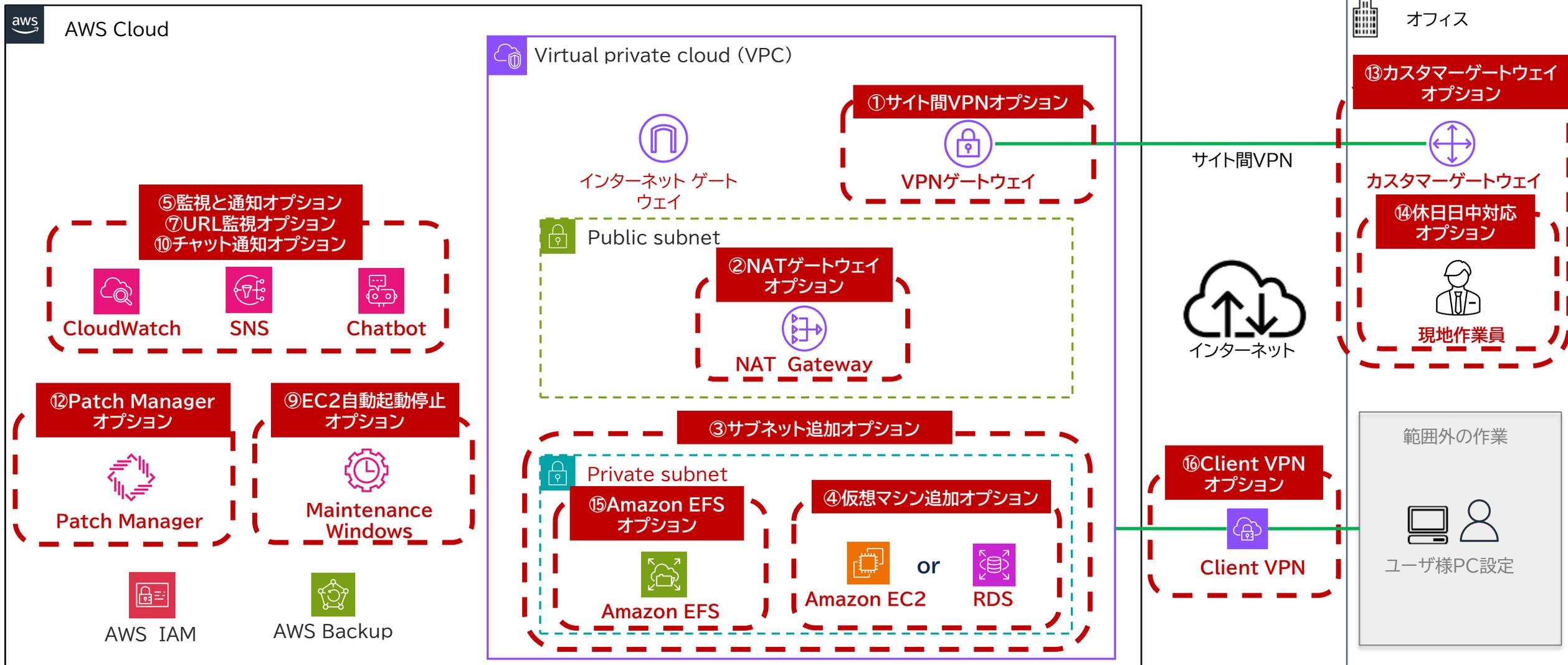
## 構成イメージ(EC2作成)



メニュー	対象サービス	主な役割	設定内容
基本セット ※対象サービスを全て含みます。	AWS IAM	アカウント作成	管理用アカウントの作成
	Amazon VPC	仮想ネットワーク	パブリックまたはプライベートサブネット(1つ)、インターネットゲートウェイ
	Amazon EC2またはRDS	仮想インスタンス	Amazon EC2またはRDSの構築(1台)、セキュリティグループ設定
	Amazon EBS	仮想ストレージ	ボリューム(汎用SSD gp2)の作成、EC2へのアタッチ
	AWS Backup	バックアップ	Amazon EC2またはRDSに対するバックアップのスケジュール設定

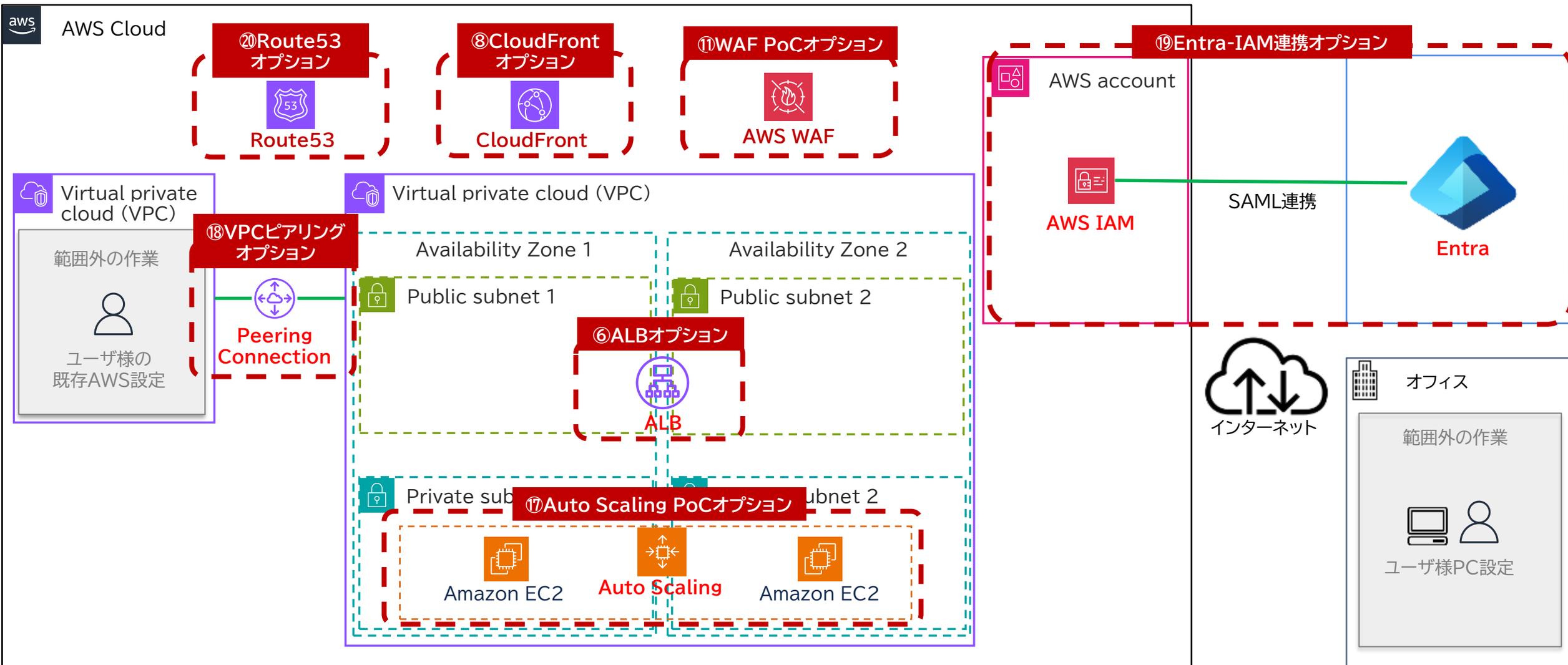
# オプションの構築サービス概要イメージ①

※基本セットへ追加が可能です。



※各オプションの詳細については次ページをご確認ください。

# オプションの構築サービス概要イメージ② ※基本セットへ追加が可能です。



※各オプションの詳細については次ページをご確認ください。

# 価格と購入数について①

※メニュー範囲外の構築に関しましては、個別にお見積りさせていただきますので、別途ご相談ください。

メニュー	対象サービス	主な役割	設定内容	標準単価 (税別)	最大 購入数
基本セット ※必須	AWS IAM	アカウント作成	管理用アカウントの作成		1式まで
	Amazon VPC	仮想ネットワーク	パブリックまたはプライベートサブネット(1つ)、インターネットゲートウェイ		
	Amazon EC2またはRDS	仮想インスタンス	Amazon EC2またはRDSの起動(1台)、セキュリティグループ設定		
	Amazon EBS	仮想ストレージ	ボリューム(汎用SSD gp2)の作成、EC2へのアタッチ		
	AWS Backup	バックアップ	仮想マシンに対するバックアップのスケジュール設定		
	設計支援	構築前のAWS設計支援	ヒアリングシートに基づくお打ち合わせ(Web会議3回まで)		
	環境引継ぎ会	構築後のAWS環境説明	構築したAWS環境についてWeb会議でご説明		
	メールサポート	構築後のメールサポート	2週間のメールサポート(平日9時-17時、ベストエフォート対応)		
	ドキュメント	-	詳細設計書、試験計画書兼報告書		
①サイト間VPNオプション	VPNゲートウェイ	サイト間VPN(AWS側)	AWS側のVPN接続設定(オフィス側の設定は含まない)※1式で5拠点まで	個別相談	2式まで
②NATゲートウェイオプション	NATゲートウェイ	NAT	パブリックサブネットに1つのNATゲートウェイを追加		2式まで
③サブネット追加オプション	Amazon VPC追加	仮想ネットワークの拡張	パブリックまたはプライベートサブネットを1つ追加		3式まで
④仮想マシン追加オプション	Amazon EC2またはRDS	仮想インスタンスの追加	Amazon EC2またはRDSを追加 ※EBSとBackup設定含む		3式まで
⑤監視と通知オプション	CloudWatch & SNS	運用管理	Amazon EC2とRDSに対する監視と管理者へのメール通知設定		1式まで
⑥ALBオプション	ALB、ACM、CloudWatch、SNS	ロードバランサー	ロードバランサーの追加とACMの証明書適用、ヘルスチェックによる異常検知時のメール通知		1式まで
⑦URL監視オプション	CloudWatch、SNS	URL(Webサイト)監視	URL(Webサイト)監視と異常検知時のメール通知 ※ログはS3に保存		1式まで
⑧CloudFrontオプション	CloudFront、ACM	Webサイトのキャッシング	Webサイトのキャッシングと証明書適用(ACM) ※⑥ALBオプション購入必須		1式まで
⑨EC2自動起動停止オプション	Maintenance Windows	EC2の自動起動停止	EC2への起動と停止を任意のスケジュールで実行 ※スケジュールの数分ご購入ください。		4式まで
⑩チャット通知オプション	Chatbot	運用管理(チャット)	MS Teams/slackへの通知(チャットサービス側の設定は含まず) ※⑤監視と通知オプションが必須		1式まで
⑪WAF PoCオプション	AWS WAF	アプリケーションFW	基本セキュリティルールの適用と通信のカウント ※⑥ALBオプション必須		1式まで
⑫Patch Managerオプション	Patch Manager	パッチ適用の自動化	パッチポリシーの作成(1つ)とEC2への適用		1式まで

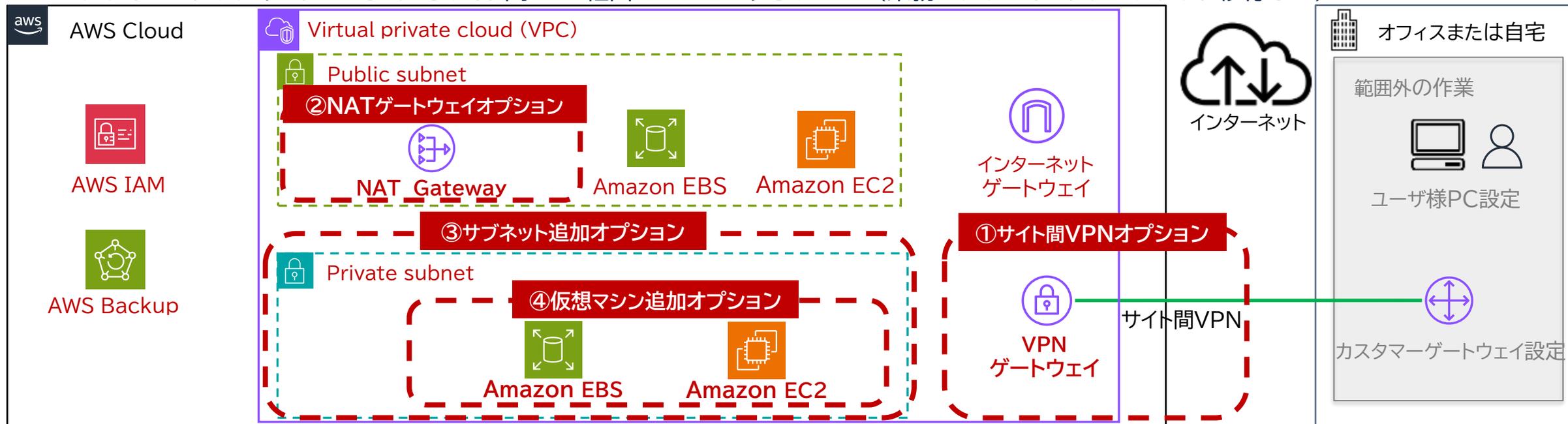
## 価格と購入数について②

※メニュー範囲外の構築に関しましては、個別にお見積りさせていただきますので、別途ご相談ください。

メニュー	対象サービス	主な役割	設定内容	標準単価 (税別)	最大 購入数
⑬カスタマーゲートウェイオプション	カスタマーゲートウェイ	サイト間VPN(オフィス側)	新規ルータに対するAWSへのVPNピア設定、インターネット設定(WAN側:1回線)、DHCPサーバーの設定、LAN側アドレス設定、SE現地対応1名(平日9:00-17:00)、機器1台の平置き ※作業の詳細は「サービスに関する注意事項」をご確認ください。 ※①サイト間VPNオプションが必須	個別相談	1式まで (複数拠点は個別ご相談ください)
⑭休日日中対応オプション	カスタマーゲートウェイ	サイト間VPN(オフィス側)	休日日中帯での現地SE対応(休日日中9:00~17:00) ※作業の詳細は「サービスに関する注意事項」をご確認ください。 ※⑬カスタマーゲートウェイオプションが必須		1式まで
⑮Amazon EFSオプション	Amazon EFS、 AWS Backup	NFSファイルストレージ ※Windows非対応	ファイルシステムの作成(1つ)、各EC2へのマウント設定(最大4台まで)、AWS Backupによるスケジュールバックアップ設定		1式まで
⑯Client VPNオプション	Client VPN、ACM、 AD Connector	クライアントVPN	Client VPNサービスの設定、ACMへのサーバー証明書とCA証明書のインポート、AD Connectorによる既存ActiveDirectory(AD)との接続設定 ※ADの構築や設定、サーバー証明書とCA証明書の作成、クライアントPCの設定は含みません		1式まで
⑰Auto Scaling PoCオプション	Auto Scaling	EC2の自動スケーリング	テスト用EC2を用いたAuto Scalingの構築、マスターEC2の作成 ※⑥ALBオプションが必須		1式まで
⑱VPCピアリングオプション	Amazon VPC	異なるVPC間との通信	VPCピアリング接続の構築、また新規VPCにおけるセキュリティ、ルーティング設定		2式まで
⑲Entra-IAM連携オプション	AWS IAM	Entraを用いたアカウント連携	(AWS作業)IDプロバイダの作成、IAMロール、ポリシー、ユーザーの作成 (Entra作業)アプリケーション作成、SAML認証用のファイルダウンロード、プロビジョニング設定、Entraのユーザまたはグループの割り当て ※10ユーザ(グループ)まで		1式まで
⑳Route53オプション	Amazon Route53	Webサイトへのドメイン連携	新規ドメインを1つ取得、Webサイト(ALB、CloudFront)へのドメイン設定		1式まで

# メニュー構成サンプル

- プライベートサブネットのEC2にもサイト間VPN経由でアクセスするケース（業務アプリやイントラのクラウド移行など）

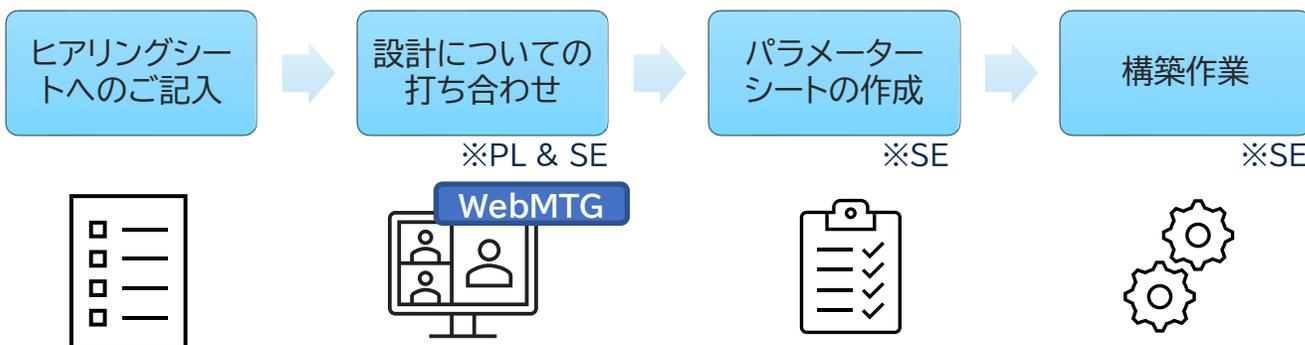


メニュー	標準単価(税別)	数量
基本セット(AWS IAM、Amazon VPC、Amazon EC2またはRDS、Amazon EBS、AWS Backup)	個別相談	1
①サイト間VPNオプション		1
②NATゲートウェイオプション		1
③サブネット追加オプション		1
④仮想マシン追加オプション		1

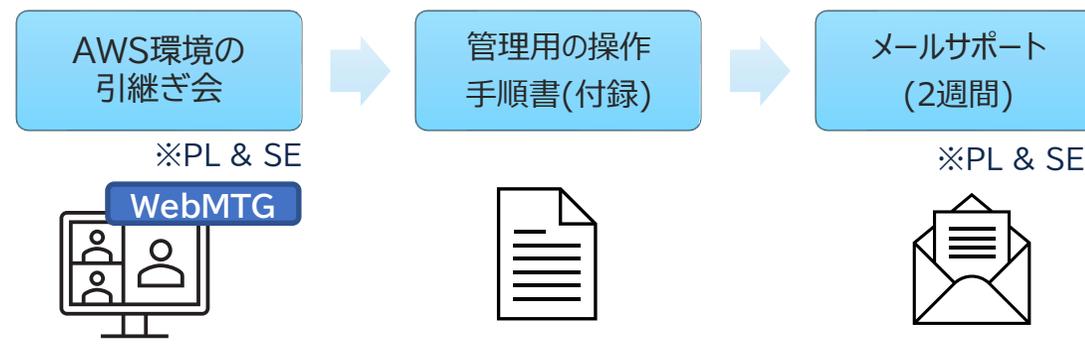
# サービスの進め方について

- AWSに馴染みの薄い方にも安心して導入頂けるように、案件ごとにPLとSEをアサインし、お打ち合わせをベースに進めさせていただきます。
- 設計についてのお打ち合わせの前に、弊社指定のヒアリングシートにご記入頂く必要がございます。
- AWS環境の引継ぎ会では、構築環境の質疑応答や納品物のご紹介を致します。(1時間程度)
- メールサポートでは、構築環境に関するご質問をAWS環境の引継ぎ会后2週間対応致します。(平日9時-17時)

## 設計・構築フェーズ



## 納品フェーズ



※各フェーズでの弊社担当者の役割について

- ◆PL(プロジェクトリーダー) … 本サービスの全体マネジメントを実施  
お客様とのコミュニケーション(お問合せ対応やMTGの日程調整)、構築作業の進捗管理など
- ◆SE(構築エンジニア) … 各種設定シートの作成、AWS環境構築、納品物の作成、技術QA対応など

**AWSサポートセンター(技術サポート)のご利用で、構築後もずっと安心です！**

AWSサポートセンターでは、電話、チャット、Eメールを使って、クラウドサポートエンジニアに24時間、年中無休で問い合わせることができます。  
※「ビジネス」以上のサポートプランをご契約ください！



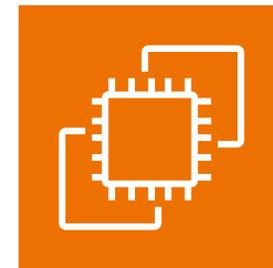
# Amazon EC2の設定範囲について

- 構築範囲は、ネットワーク、ストレージ、コンピューットのIaaS範囲です。
- OS、ミドルウェア、アプリケーションの設定は範囲外です。
- お客様のご要望に応じてAWS BackupにてEC2のストレージのスナップショットを取得します。(基本セットメニューに含む)

## EC2の設定範囲



## 仮想サーバのバックアップ



Amazon EC2

ご指定のタイミングでストレージの  
スナップショットを取得

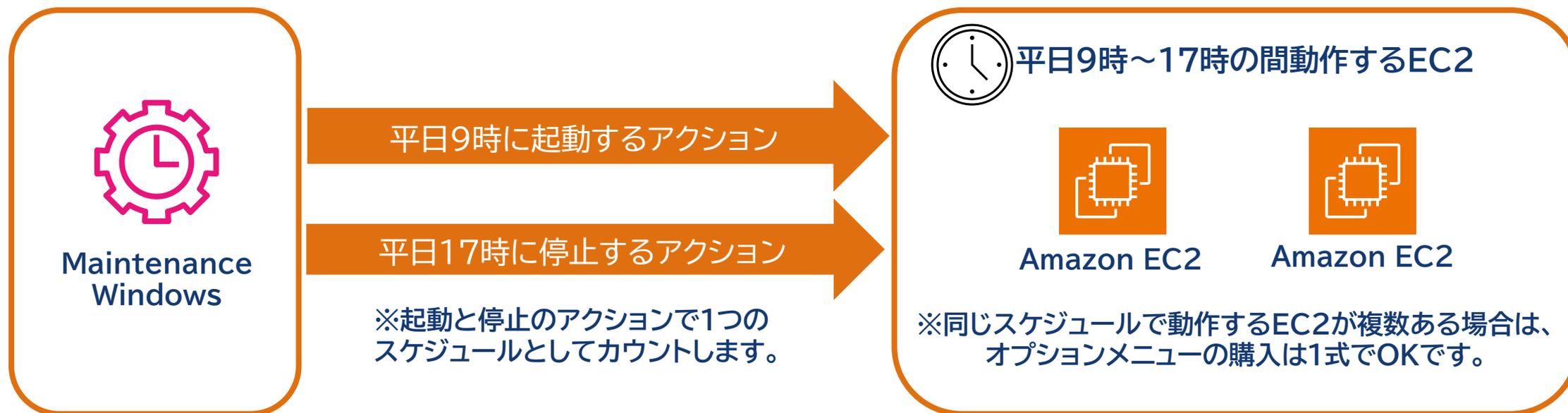


スナップショット

# EC2の自動起動停止オプションについて

- EC2の自動起動停止オプションとは、Maintenance Windowsを利用してEC2の起動および停止時間を指定するオプションのメニューです。
- 例えば平日の9時から17時までの間のみEC2を自動的に起動させることが可能です。※祝日や年末年始など考慮したスケジュールは対応不可です。その際は手動で停止と起動を実行ください。
- スケジュール毎にメニューを購入ください。(最大購入数は4式)

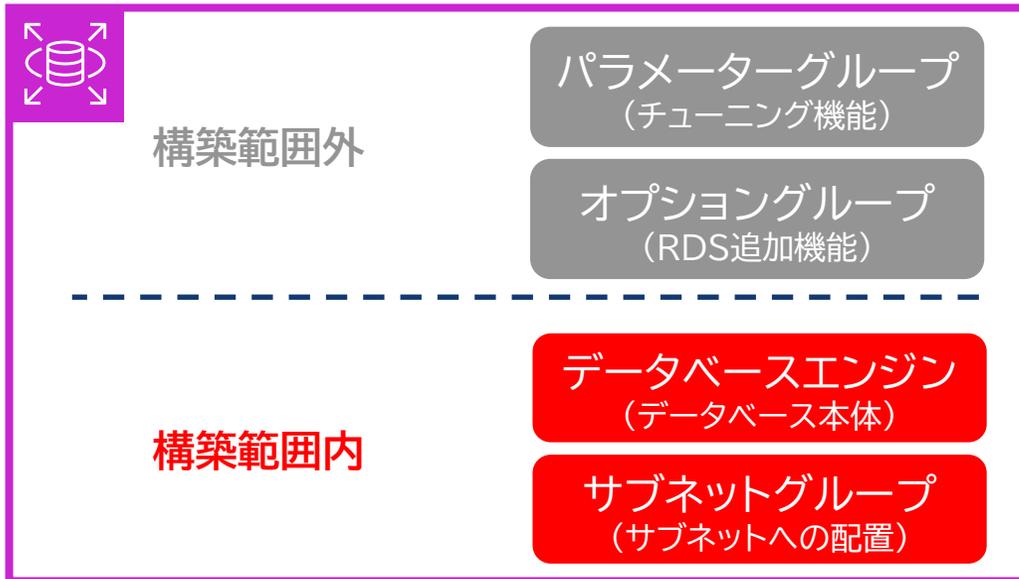
## Maintenance Windowsを利用した自動起動停止の仕組みとメニューの購入数について



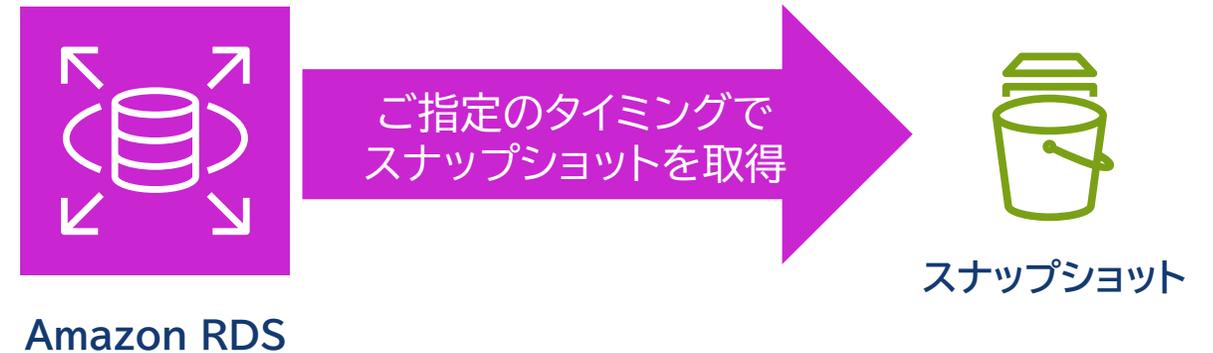
# Amazon RDS の設定範囲について

- 構築対象のデータベースは Microsoft SQL Server、Oracle、MySQL、PostgreSQLです。
- 弊社オリジナルの「設定シート」へご記載頂いた内容に沿って設定します。(DBの設計に関するご相談は対象外)
- 構築範囲は、データベースエンジンとサブネットグループです。パラメーター/オプショングループはデフォルト設定を利用します。
- AWS Backupサービスを利用してRDSのスナップショットを取得します。

## Amazon RDSの設定範囲



## RDSのバックアップとイベント監視



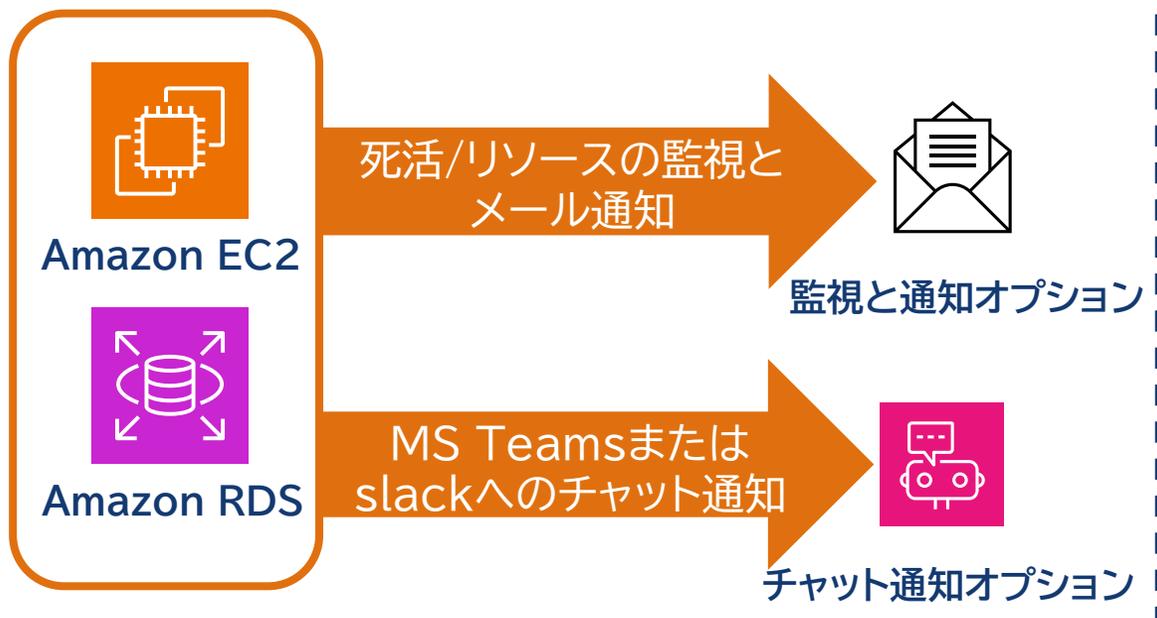
- パラメーターグループについて
- オプショングループについて

[https://docs.aws.amazon.com/ja\\_jp/AmazonRDS/latest/UserGuide/USER\\_WorkingWithParamGroups.html](https://docs.aws.amazon.com/ja_jp/AmazonRDS/latest/UserGuide/USER_WorkingWithParamGroups.html)  
[https://docs.aws.amazon.com/ja\\_jp/AmazonRDS/latest/UserGuide/USER\\_WorkingWithOptionGroups.html](https://docs.aws.amazon.com/ja_jp/AmazonRDS/latest/UserGuide/USER_WorkingWithOptionGroups.html)

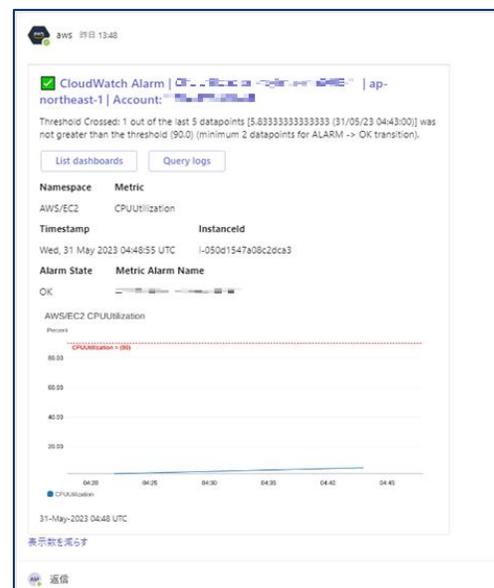
# Amazon EC2とRDSの監視と通知について ※オプションメニュー

- オプションメニューの「監視と通知オプション」では、死活とリソース(CPU、メモリ、HDD)を監視し、異常の際は管理者様へメールにて通知します。
- 「監視と通知オプション」に「チャット通知オプション」を追加するとご利用中のMS TeamsまたはSlackへのチャットによる通知設定を実施します。※RDSの死活監視は、チャット通知をサポートしませんのでご注意ください。
- MS Teamsまたslackのチャットサービス側の設定は範囲外です。AWS側のチャットボットの設定を実施します。

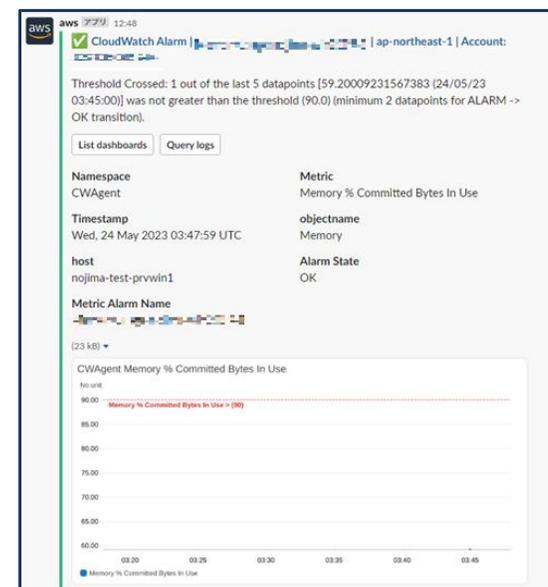
## 仮想サーバの監視と通知



## チャット通知サンプル



MS Teams通知イメージ

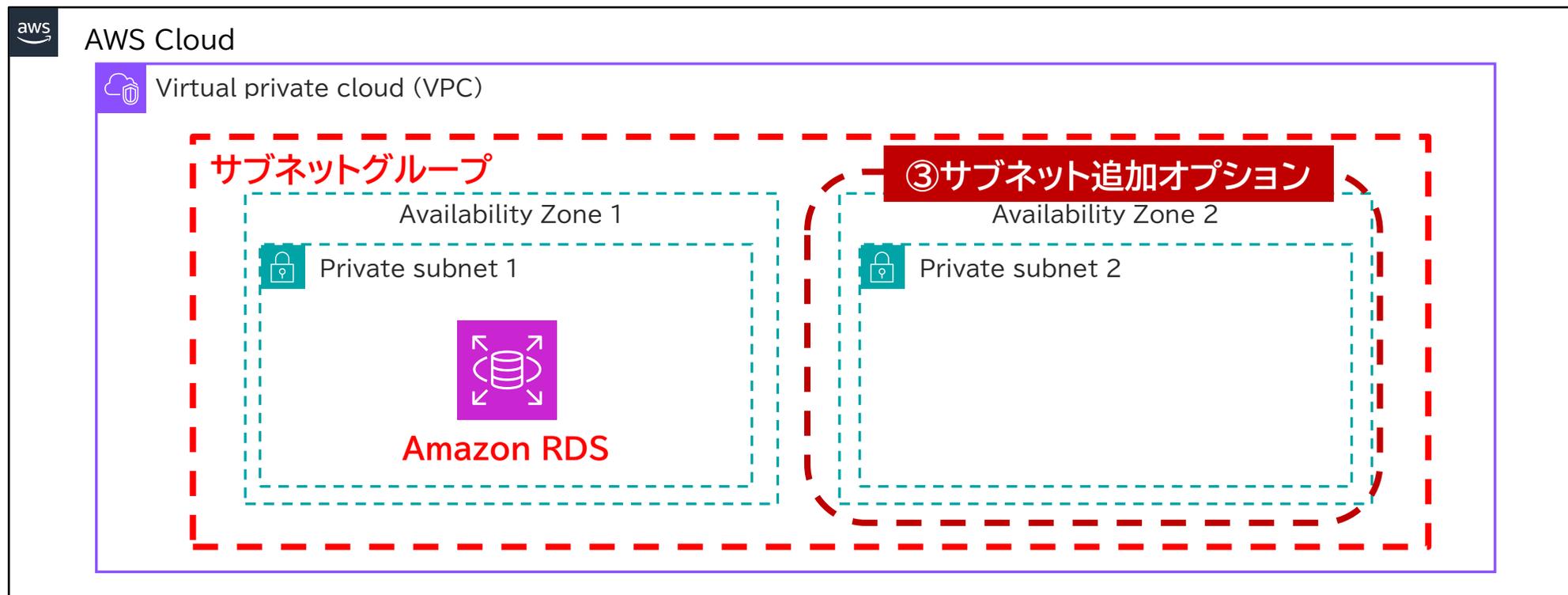


slack通知イメージ

# Amazon RDS 設計の際の注意点

- RDSは2つ以上のサブネットを含むサブネットグループに配置する必要があります。  
※シングルAZ構成の場合も含む
- サブネットを追加する場合は、「③サブネット追加オプション」をご購入頂く必要があります。

## 構成イメージ



# ALB (Application Load Balancing)の設定について

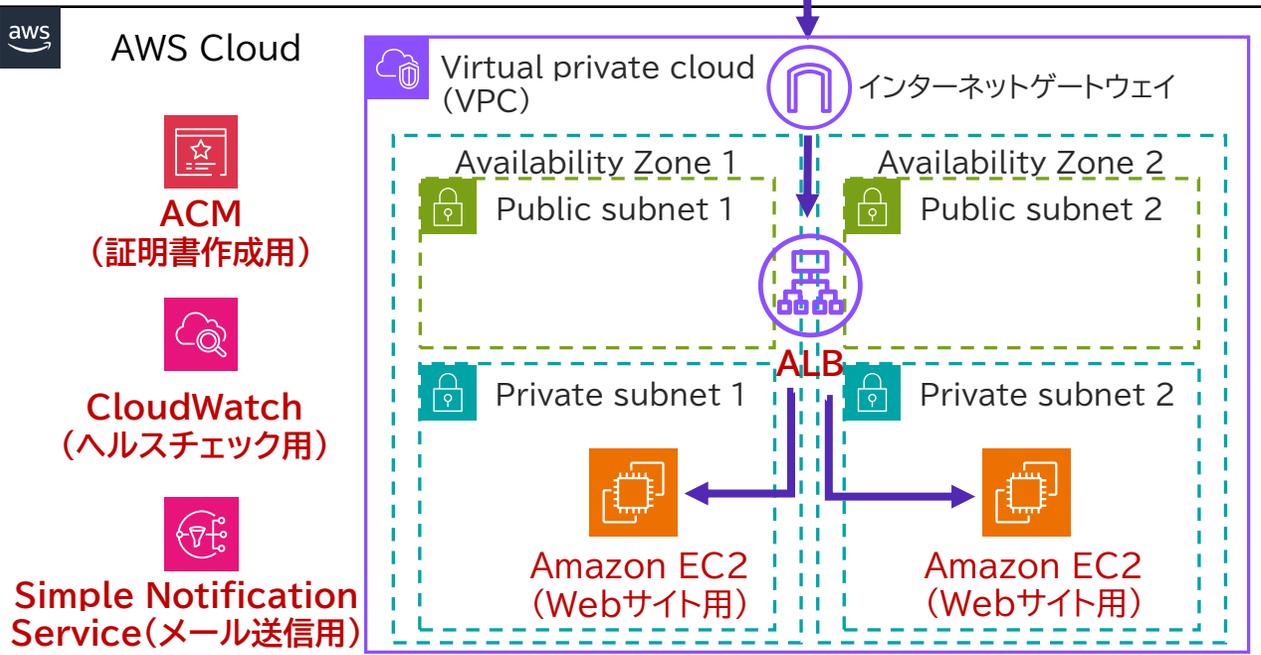
- ALBを用いて2つのアベイラビリティゾーンにまたがるWEBサイトを構成することにより、単一障害点の排除とアクセスの負荷分散を実現します。またACMで発行したSSL/TLS 証明書をALBに適用することでHTTPSの通信を提供します。
- Webサイトに対してヘルスチェックを設定するため、構築期間中にお客様にてWebサイトを構築頂く必要がございます。メニューにて対応可能なALBの振り分けルールは「負荷分散」、Webサイト数は「1サイト」とさせていただきます。  
※Webサイトの動作確認および負荷分散試験は含まれません。
- SSL/TLS証明書発行に際し、お客様によるDNSへの設定追加が必要になります。※設定値をご連絡致します。

## 構成イメージ

通信経路 →



インターネット



## 構築フローイメージ



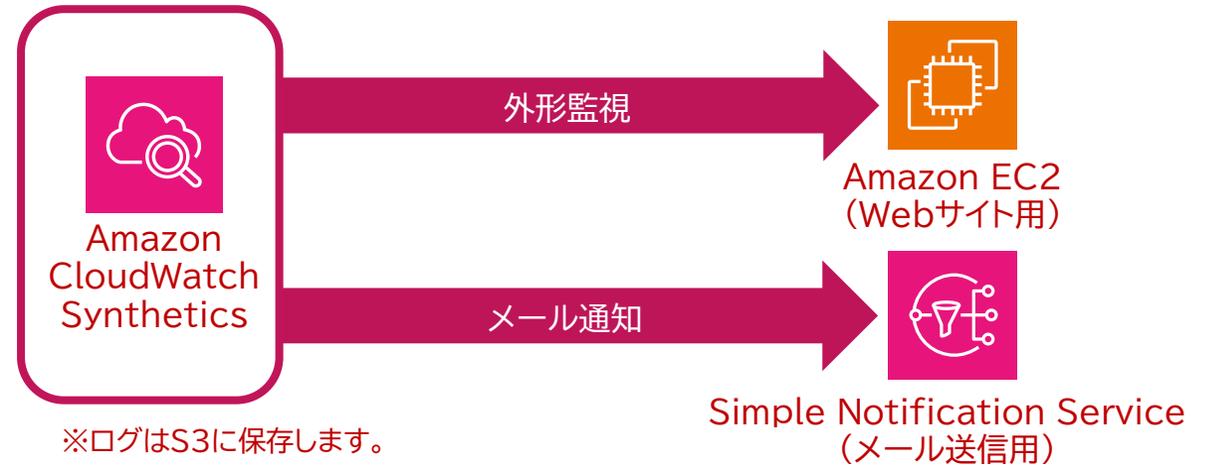
# ALBのヘルスチェックとURL監視サービスについて

- ヘルスチェックとは、ALBから登録されたターゲット(Webサイト)のステータスをテストするため、定期的にリクエストを送信する機能です。異常時には管理者様へメール通知を実施します。
- URL監視(外形監視※)はAmazon CloudWatch SyntheticsサービスがAWS Lambdaと連携し、VPCの外部からクライアントのアクションをシミュレートしwebサーバの可用性をモニタリングする機能です。  
※URL監視の設定はオプションの追加メニューです。

## ヘルスチェックサービスイメージ



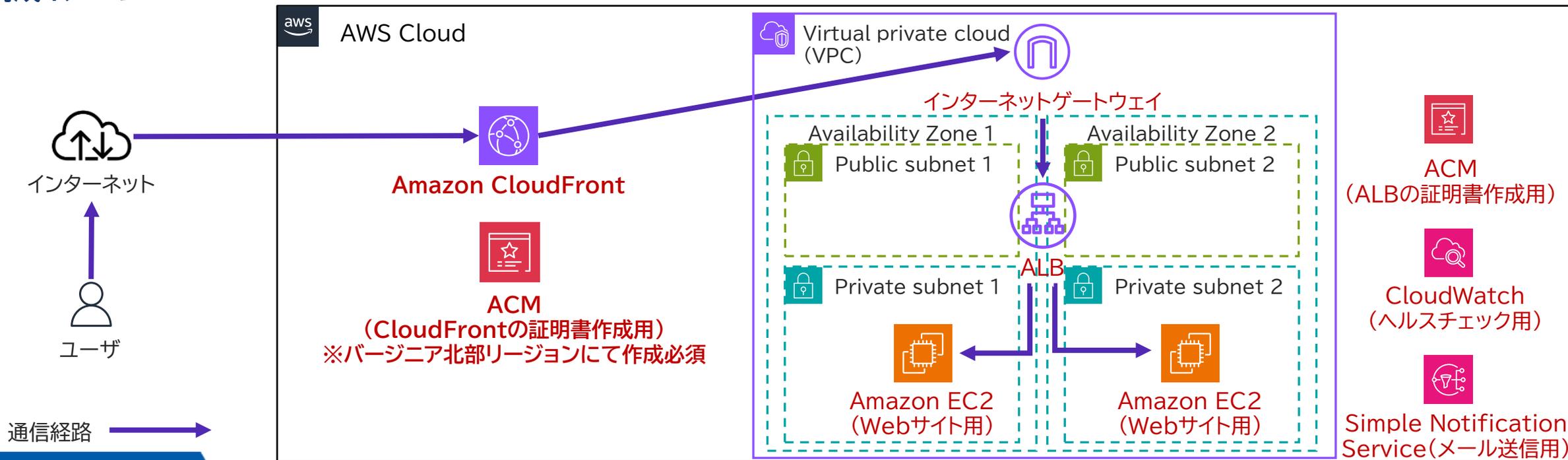
## URL監視(外形監視)サービスイメージ ※オプションメニュー



# CloudFrontの設定について

- CloudFrontキャッシュがWEBサーバーへの直接的なリクエストの数を減らすことでWEBサーバーの負荷を軽減することが可能です。またユーザに近いエッジロケーションがリクエストに応答することでレイテンシーの減少が期待できます。
- CloudFrontオプションは、ALBオプションと連携する為、ALBオプションの同時購入が必要です。
- メニューにて対応可能なALBへの通信プロトコルはhttpsのみです(httpのみの利用はサポートしません)。またALBオプション同様にALB振り分けルールは「負荷分散」、Webサイト数は「1サイト」とさせていただきます。  
※Webサイトの動作確認および負荷分散試験は含まれません。

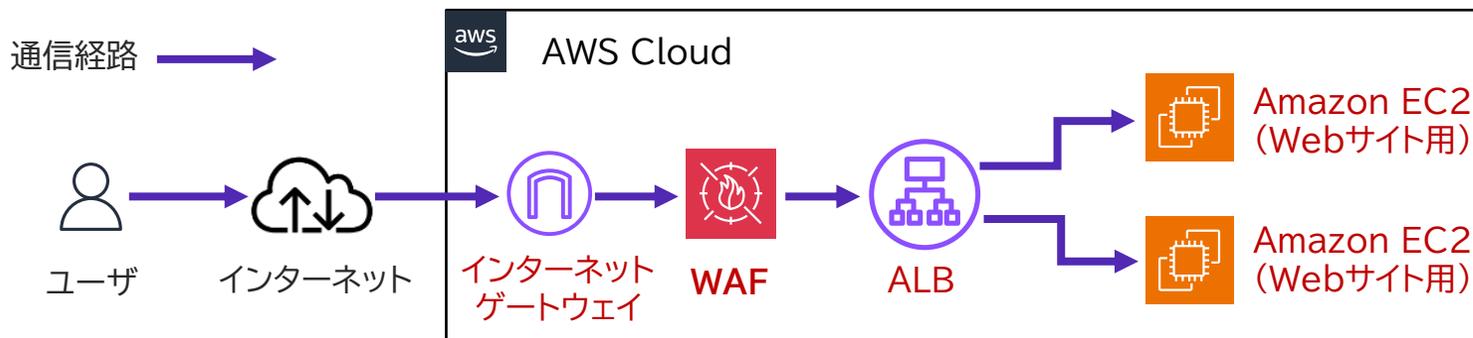
## 構成イメージ



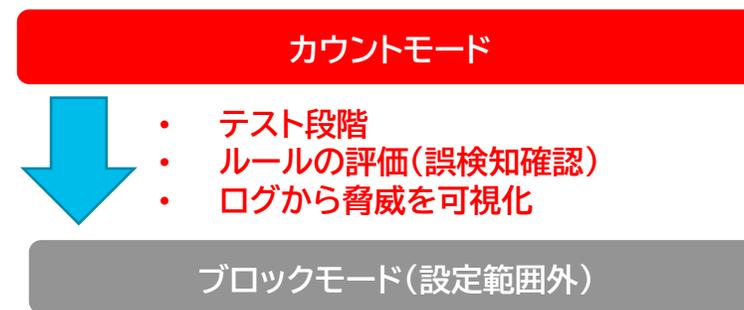
# WAF PoC オプションの設定について

- ALBもしくはCloudFrontに対してWAFの基本的なルールを適用し、ルールに該当した通信をカウントする環境を設定します。カウントされたログを確認することでルールに基づく検知状況の可視化が可能です。※通信のブロックは行われません。
- カウントモードからブロックモードへの設定変更やルールの追加や削除はお客様にて実施頂く必要がございます。
- ルールはAWSが提供する「ベースラインルールグループ」と「IPレピュテーションルールグループ」をWEBサイト全体に適用します。

## 構成イメージ(ALBに適用)



## カウントモードとブロックモード



## 適用ルール

※ルールの詳細はこちらご確認ください。[https://pages.awscloud.com/rs/112-TZM-766/images/202203\\_AWS\\_Black\\_Belt\\_AWS\\_Managed\\_Rules\\_for\\_AWS\\_WAF.pdf](https://pages.awscloud.com/rs/112-TZM-766/images/202203_AWS_Black_Belt_AWS_Managed_Rules_for_AWS_WAF.pdf)

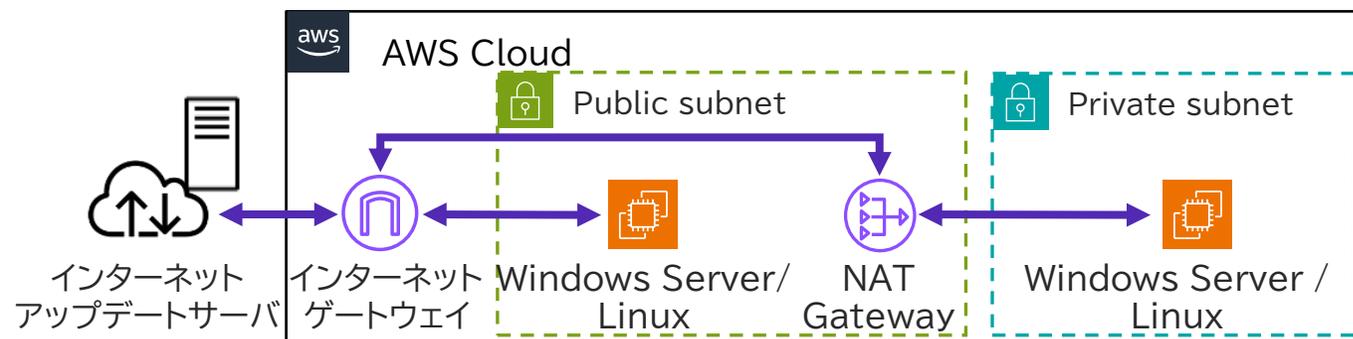
分類	ルールセット	概要
ベースラインルールグループ	Core rule set (CRS)	OWASP Top 10 の脅威に基づく、一般的なウェブアプリケーションに適用可能なルール
	Admin Protection	公開されている管理ページへの外部アクセスに基づくルール
	Known bad inputs	無効であることがわかっており、脆弱性の悪用または探索に関連するリクエストパターンに基づくルール
IPレピュテーションルールグループ	Amazon IP reputation list	ボットやその他の脅威に関連づけられている IP アドレスをブロックする、Amazon 内部の脅威インテリジェンスに基づくルール
	Anonymous IP list	VPN、プロキシ、Tor ノード、ホスティングプロバイダーなどのビューワーIDの難読化を許可するサービスからのリクエストに基づくルール

# Patch Managerオプションの設定について

- EC2(Windows、Linux)にパッチを適用するプロセスを自動化します。
- AWSがサポートする事前定義された下記のパッチベースラインにてパッチポリシーを1つ設定します。
- パッチオペレーションは、パッチ適用状況(コンプライアンスへの準拠)を確認し、未適用パッチをインストールする、「スキャンとインストール」を設定します。

## 構成イメージ

通信経路 →



## ダッシュボード

パッチ適用状況が確認できます。



## パッチベースライン ※Windowsの場合は、いずれか1つを選択頂きます。

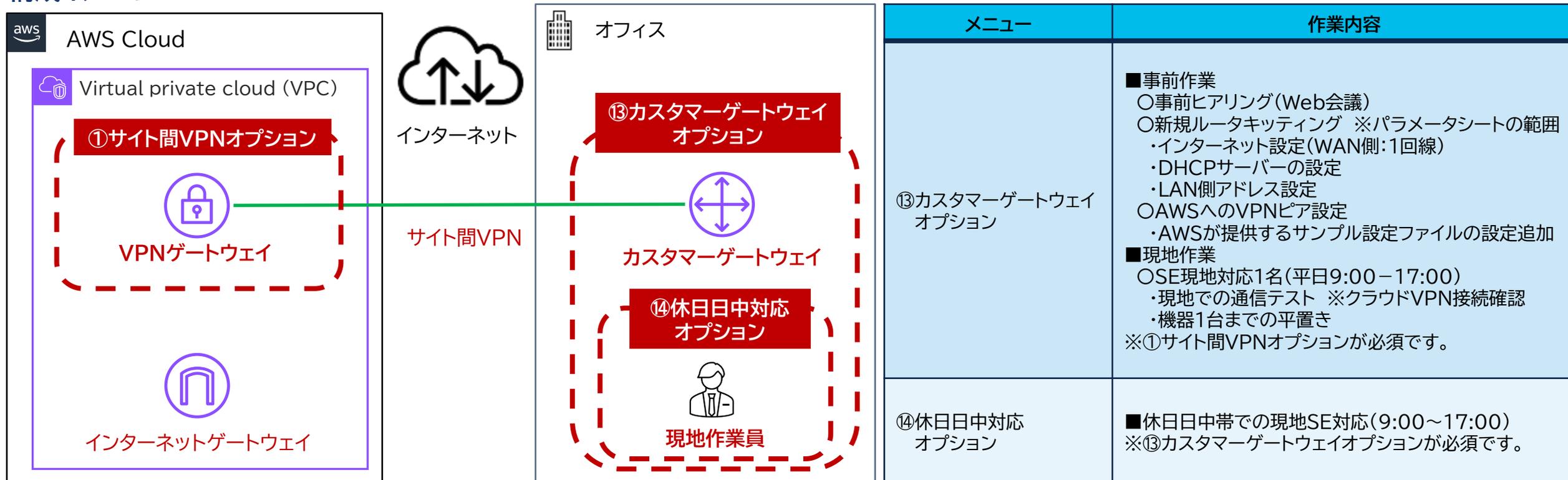
OS	ベースライン名	概要
Windows Server	AWS-DefaultPatchBaseline	分類が「CriticalUpdates」または「SecurityUpdates」で、MSRC 重要度が「非常事態」または「重要」のすべてのWindows Server オペレーティングシステムパッチを承認します。(パッチはリリース/更新されてから7日後に自動承認)
	AWS-WindowsPredefinedPatchBaseline-OS-Applications	「AWS-DefaultPatchBaseline」に加え、Microsoft がリリースしたアプリケーションについては、すべてのパッチを承認します。OS とアプリケーションのパッチのどちらも、リリース/更新から7日後に自動承認されます。
Linux	※OSに応じて選択	分類が「セキュリティ」で、重要度レベルが「非常事態」または「重要」のすべてのオペレーティングシステムパッチを承認します。また、分類が「Bugfix」(バグ修正) のすべてのパッチを承認します。パッチはリリースから 7 日後に自動承認されます。

※詳細はこちらご確認ください。[https://docs.aws.amazon.com/ja\\_jp/systems-manager/latest/userguide/patch-manager-predefined-and-custom-patch-baselines.html#patch-manager-baselines-pre-defined](https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/patch-manager-predefined-and-custom-patch-baselines.html#patch-manager-baselines-pre-defined)

# カスタマーゲートウェイサービスオプションについて

- オフィス側のカスタマーゲートウェイ(ルーター)とAWS Cloud側のVPNゲートウェイ間のVPNを構築するサービスです。
  - 新規ルータの事前設定を行い、現地設置とAWSへの通信確認までを実施します。
- ※対象ルータや現地作業の条件や詳細は「サービスに関する注意事項」をご確認ください。
- 「休日日中対応オプション」の追加により休日日中帯(9:00~17:00)の現地SE対応が可能です。

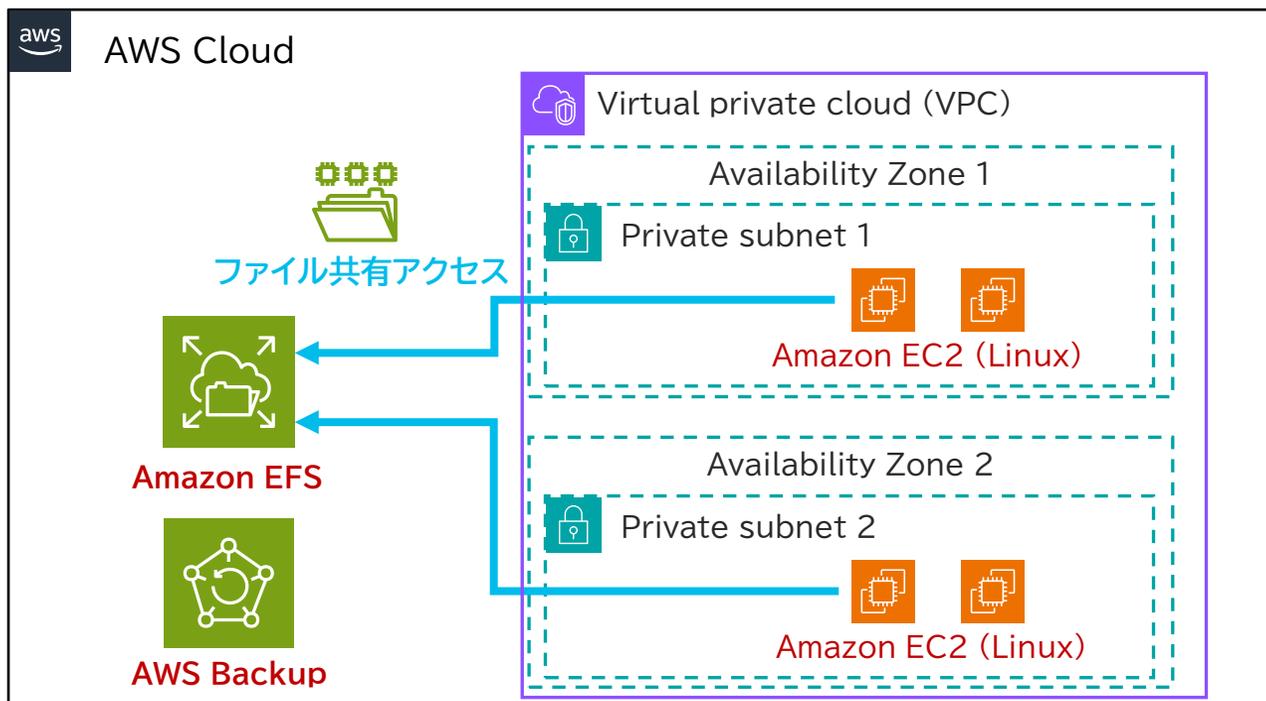
## 構成イメージ



# Amazon EFSオプションについて

- Amazon EFSオプションサービスは、NFSを使用してネットワーク経由でアクセスするファイルストレージを構築するオプションサービスです。※Windows のファイル共有サービスではございませんのでご注意ください。
- EFSはフルマネージド型のサービスのため、サーバやディスクの管理など不要です。またファイルの追加・削除に合わせてファイルシステムの自動拡張・縮小が可能です。
- EC2へのマウントとAWS Backupによるスケジュールバックアップ設定を合わせて実施します。

## 接続イメージ



## EFS を利用するための NFS クライアント

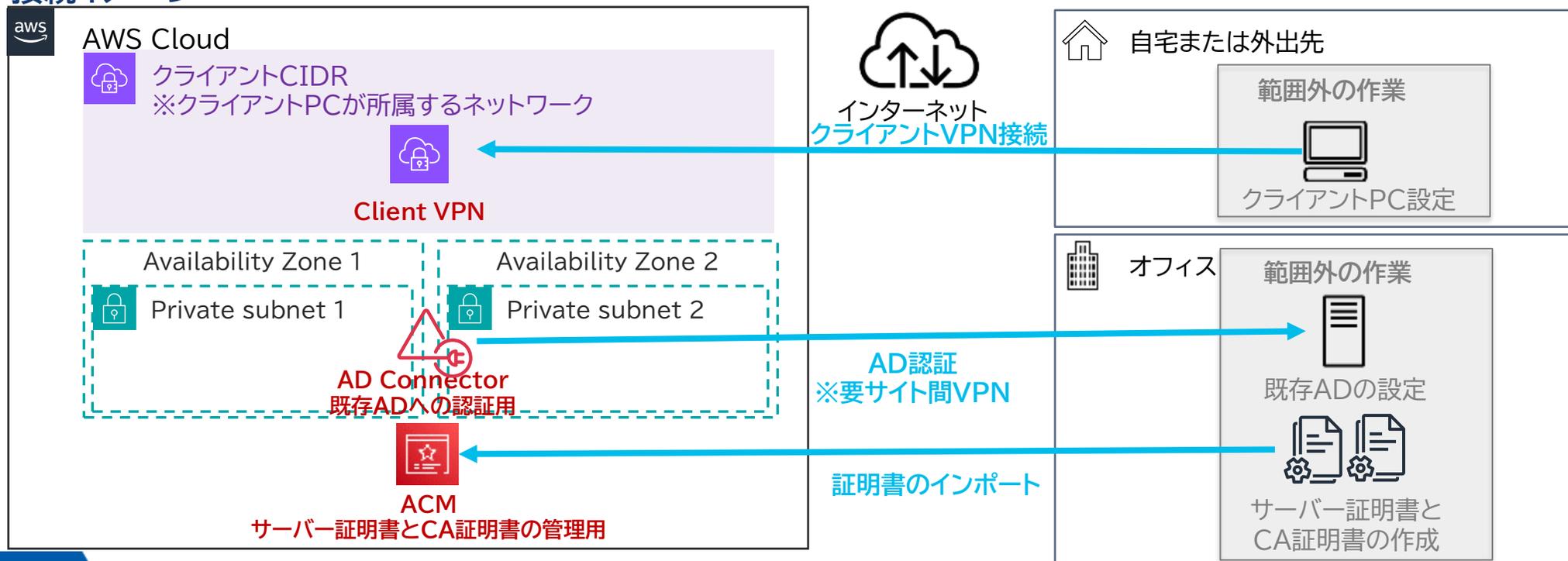
- プロトコル : NFSv4.0/4.1 (TCP 2049ポート)  
※CIFS/SMB のサポートなし  
※NFS v4 の機能であっても未サポートの機能あり  
[https://docs.aws.amazon.com/ja\\_jp/efs/latest/ug/nfs4-unsupported-features.html](https://docs.aws.amazon.com/ja_jp/efs/latest/ug/nfs4-unsupported-features.html)

- 推奨 Linux ディストリビューション :  
Amazon Linux 2  
Amazon Linux 2017.09 以降  
Red Hat Enterprise Linux (および、その派生物 CentOS など)  
バージョン 7 以降  
Ubuntu 16.04 LTS 以降  
SLES 12 Sp2 以降  
別のディストリビューションまたはカスタムカーネルを使用している場合は、  
カーネルバージョン 4.3 以降をお勧めします。

# Client VPNオプションについて

- Client VPNオプションサービスは、OpenVPN ベースの VPN クライアントソフトを使用してクライアントPCからインターネットを介してAWS リソースにアクセスできる環境を構築するオプションサービスです。
- 認証方式にはActive Directory(AD)認証を使用します。ADは既存(オンプレ)のものを利用する想定です。  
※既存ADとクライアントPCへの設定は範囲外です。
- AWS Certificate Manager(ACM)にインポートするサーバー証明書とCA証明書を作成頂く必要がございます。  
※サービスにて証明書のインポートを実施します。

## 接続イメージ

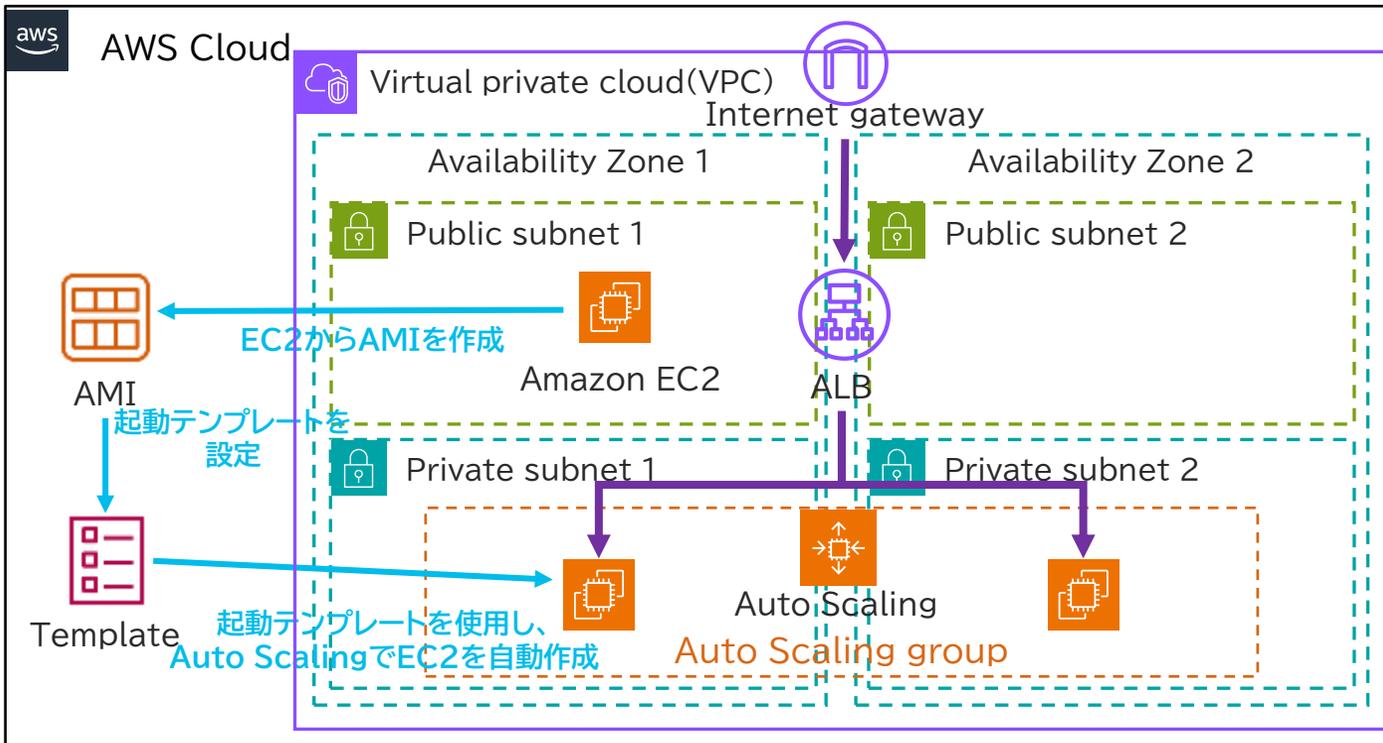


# Auto Scaling PoCオプションについて

- Auto Scaling PoCオプションは、テスト用EC2を基にAuto Scaling環境を構築するPoCメニューとなります。
- 環境引き渡し後、お客様にて本番用のアプリケーション構築、起動テンプレートの更新及びAuto Scalingの起動確認を実施頂く必要がございます。 ※手順は付録の「操作手順書」に記載しております。
- PoCメニューで設定するAuto Scaling Policyは“平均CPU使用率”と“ALBのヘルスチェック”になります。
- 本オプションはALBオプションの同時購入が必要です。

## 構成イメージ

通信経路 →

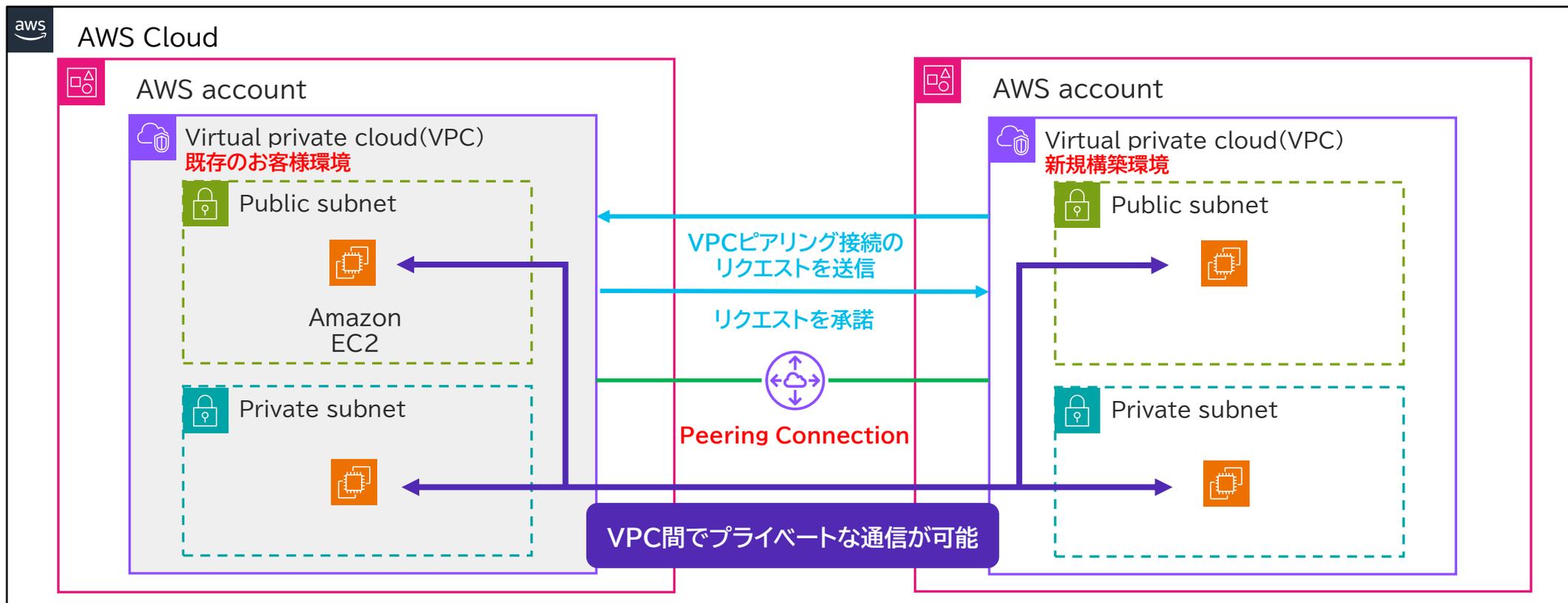
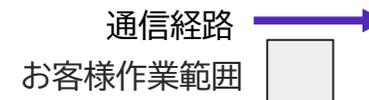


	作業内容
構築作業中	<ul style="list-style-type: none"> <li>● 弊社にてテスト用EC2を作成し、簡易Webサーバーを作成致します。</li> <li>● テスト用EC2を基にAMI、起動テンプレート、Auto Scaling Groupを作成し、動作確認を実施致します。</li> <li>● テスト用EC2を削除し、Auto Scaling Policyのグループサイズを「0」にします。</li> <li>● マスターEC2を作成し、AWS環境をお渡し致します。</li> </ul>
AWS環境引き渡し後	<ul style="list-style-type: none"> <li>● マスターEC2にて本番用のアプリケーション(Webサーバー等)を作成ください。</li> <li>● 作成後、マスターEC2を基にAMIを作成し、起動テンプレートを更新ください。</li> <li>● Auto Scaling Policyのグループサイズをご希望の数に変更し、起動確認を実施ください。</li> </ul>

# VPCピアリングオプションについて

- VPCピアリングオプションは、2つのVPC間でプライベートな通信を可能にするオプションサービスです。
- アカウントやリージョンが異なる場合でもVPCを接続することが可能です。
- 既存のお客様環境の設定はお客様自身で実施いただく必要があります。

## 構成イメージ(異なるアカウントの場合)



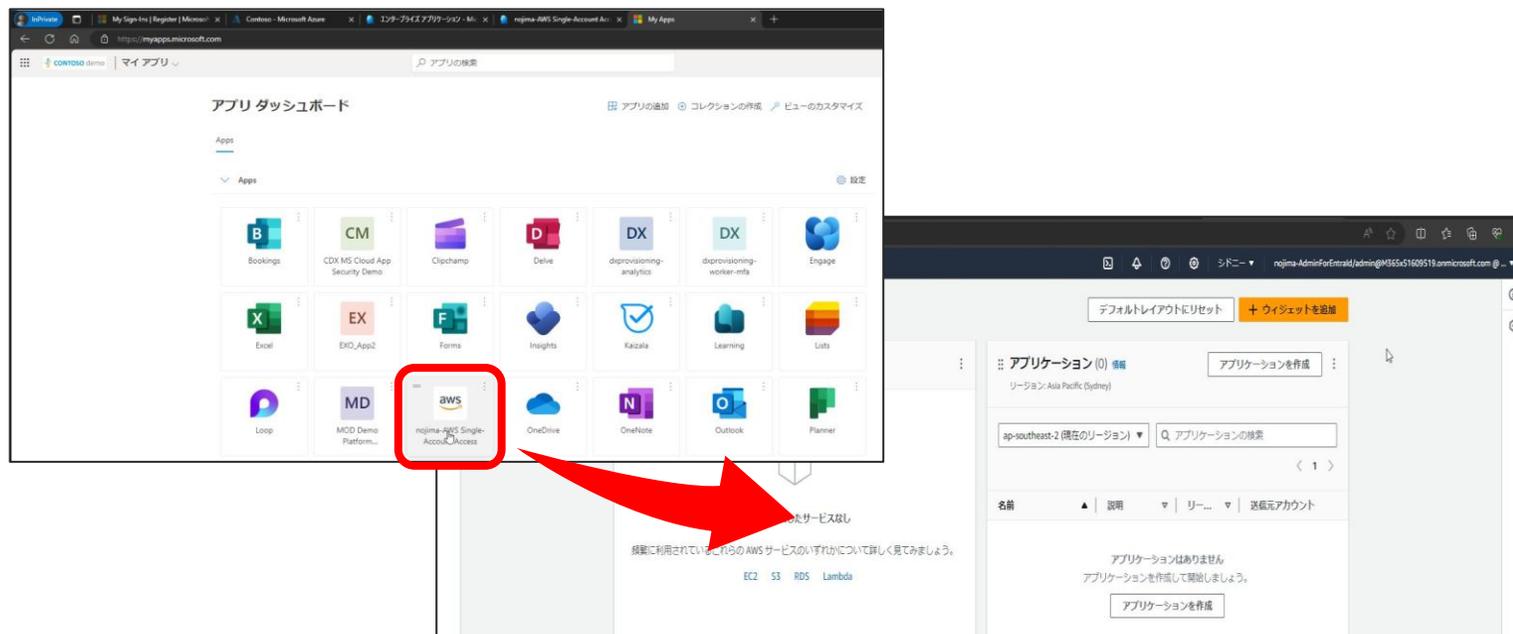
# Entra-IAM連携オプションについて

- Entra-IAM連携オプションサービスは、既にEntraをご利用中のお客様が、Entraのユーザアカウントを用いてAWSにアクセス・操作できるようにするオプションサービスです。
- 認証方式にはSAML認証を使用します。
- 既存のEntraにアクセスし、AWSとの連携作業を実施致します。  
※新規Entraの作成及び既存Entraの設定(ユーザ作成等)は対象外です。

## ログインの流れ



## 接続イメージ



# Route53オプションについて

- Route53オプションサービスは、AWS上で新規取得したドメインをお客様のWebアプリケーションサイトに連携し、ドメインでのアクセスを可能にするオプションサービスです。
- 本オプションはALBオプションまたはCloudFrontオプションとの同時購入が必要です。

## ドメインの取得



Route 53

example.com

## ドメインの連携(ALB)

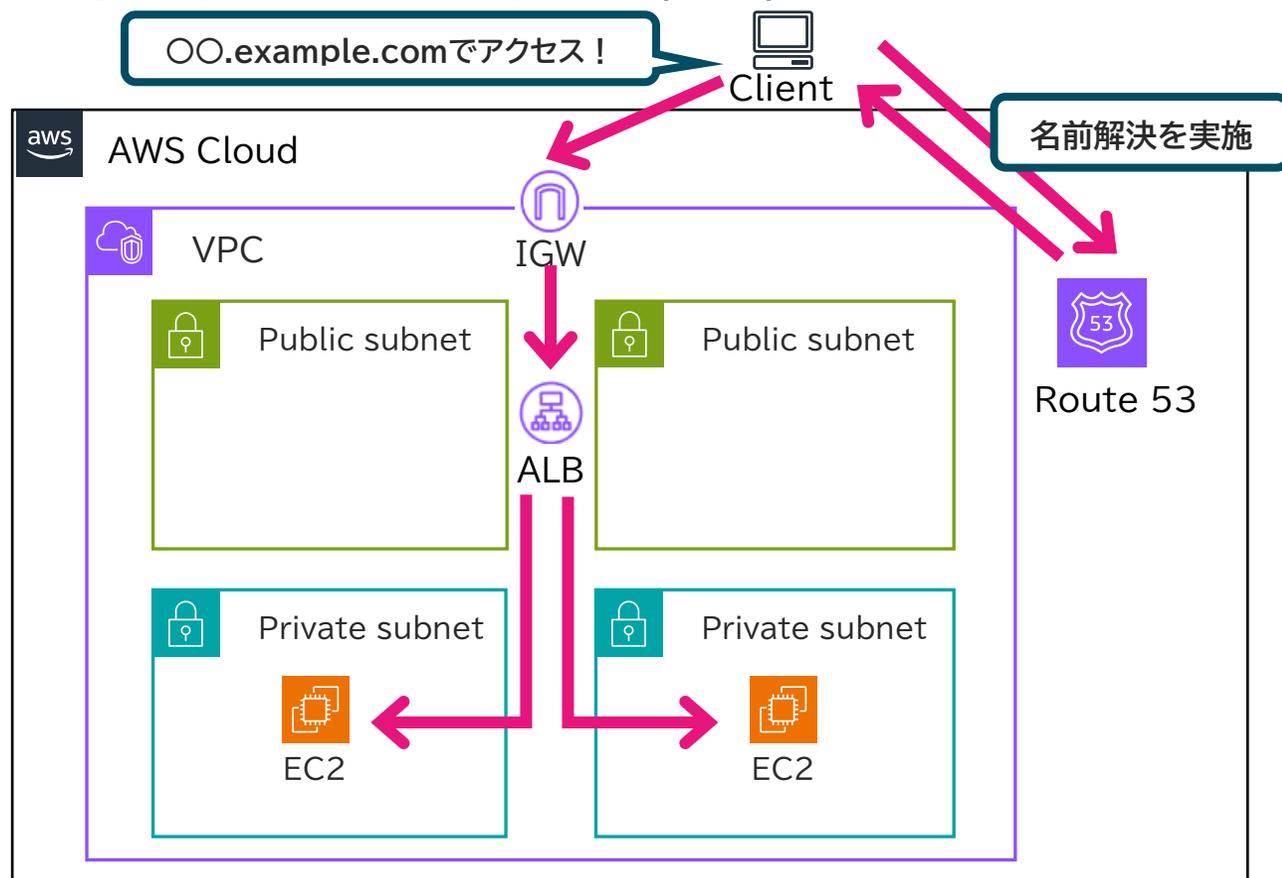


Hosted zone

レコードを登録

ドメイン	ルーティング先
〇〇.example.com	ALB

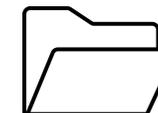
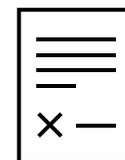
## Webサイトへのアクセスイメージ(ALB)



# 納品ドキュメントと操作手順書(付録)

- 納品ドキュメント

- 詳細設計書(パラメータシートのとりまとめ)
  - 試験計画書兼報告書
- ※弊社フォーマットでのデータ提供となります。



- 操作手順書(付録)

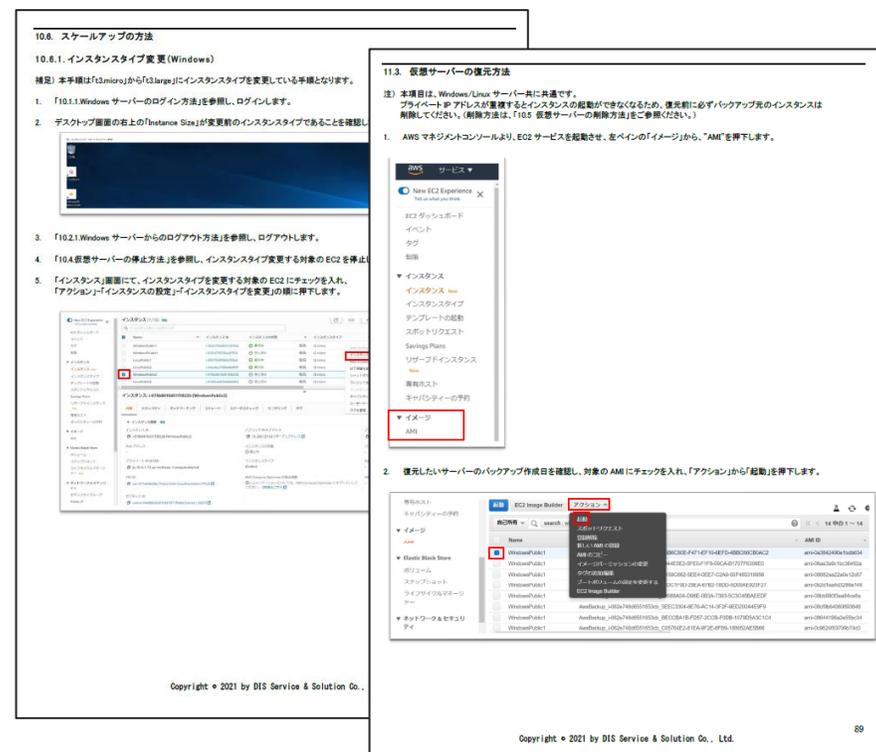
- AWSマネジメントコンソールからの各種操作手順書
- ※上記の操作手順書を付録(無償)としてお渡し致します。  
弊社のAWS環境をベースとした操作手順書となります為、お客様のAWS画面とは異なります。  
個別のカスタマイズは実施することはできません。

# 操作手順書(付録)について

- 構築後のユーザ様の運用をサポートする **全350ページを超えるオリジナルの操作手順書**をご提供いたします。
- AWSマネジメントコンソールのサインイン方法から、仮想インスタンスの管理方法(インスタンスタイプの変更&ストレージの拡張含む)やバックアップからの復元方法についてなど、運用に必要な各種操作手順をキャプチャ画面で解説しております。

### 目次

1. 概要	4	11.4.3.1. ファイルの復旧(Windows)	119
1.1. 資料概要	4	11.4.3.2. ファイルの復旧(Linux)	126
1.2. 注意事項	4	11.5. EBS ボリュームの削除方法	129
1.3. 改定履歴	4	12. RDS の管理	130
2. 前提条件	5	12.1. RDS の起動方法	130
3. AWS マネジメントコンソールサインイン	6	12.2. RDS の停止方法	132
4. AWS マネジメントコンソールサインアウト	8	12.3. RDS の再起動方法	135
5. 別リージョンへの画面遷移方法	10	12.4. RDS の切り替え方法	137
6. 各 AWS サービスへの画面遷移方法	12	12.5. RDS の削除方法	139
7. IAM グループ作成・削除	14	12.6. RDS のログ参照方法	143
7.1. IAM グループ作成	14	12.6.1. RDS のコンソール画面から参照する	143
7.2. IAM グループ削除	17	12.6.2. ダウンロードして参照する	145
8. IAM ユーザー作成・削除・パスワード変更	19	12.6.3. CloudWatch から参照する	147
8.1. IAM ユーザー作成	19	12.7. RDS の設定変更	149
8.2. IAM ユーザー削除	26	12.7.1. DB インスタンスクラスの変更	149
8.3. IAM ユーザーパスワード変更	28	12.7.2. ストレージの容量拡張	152
9. AWS 管理ツールのインストール	30	12.7.3. ストレージタイプの変更	156
9.1. AWS CLI インストール	30	12.7.4. メンテナンス時間の変更	160
10. 仮想サーバーの管理	36	13. RDS のバックアップと復元	163
10.1. 仮想サーバーのログイン方法	36	13.1. バックアップの取得状況の確認方法	163
10.1.1. Windows サーバーのログイン方法	37	13.2. スナップショットを手動で取得する方法	164
10.1.2. Linux サーバーのログイン方法	37	13.3. RDS の復元方法	166
10.2. 仮想サーバーのログアウト方法	47	13.3.1. スナップショットからの復元方法(AWS Backup)	167
10.2.1. Windows サーバーからのログアウト方法	47	13.3.2. スナップショットからの復元方法(RDS コンソール)	173
10.2.2. Linux サーバーからのログアウト方法	48	13.3.3. 自動バックアップからの復元方法	178
10.3. 仮想サーバーの起動方法	49	13.4. からの片系障害発生時について	184
10.4. 仮想サーバーの停止方法	50	14. 通知機能の管理	185
10.5. 仮想サーバーの削除方法	51	14.1. CloudWatch による監視・通知	185
10.6. 仮想サーバーの設定変更	54	14.1.1. 通知の登録	185
10.6.1. インスタンスタイプ変更(Windows)	54	14.1.2. ステータスの確認方法	188
10.6.2. インスタンスタイプ変更(Linux)	56	14.1.3. 通知の無効化・有効化	191
10.6.3. EBS ボリュームの追加(Windows)	58	14.2. RDS によるイベント通知	196
10.6.4. EBS ボリュームの追加(Linux)	68	14.2.1. イベント通知メールの見方	196
10.6.5. EBS ボリュームの容量拡張(Windows)	75	14.2.2. イベントの確認方法	197
10.6.6. EBS ボリュームの容量拡張(Linux)	81	14.2.3. イベント通知の無効化・有効化	199
10.7. 仮想サーバーのステータス確認方法	85	14.2.4. イベント通知対象を変更する	203
11. 仮想サーバーのバックアップと復元	87	14.2.5. イベント通知のカテゴリを変更する	206
11.1. バックアップの取得状況の確認方法	87	14.3. 通知先の編集(変更、追加、削除)	209
11.2. バックアップからの復元について	88	14.3.1. 通知先の変更	209
11.3. 仮想サーバーの復元方法	89	14.3.2. 通知先の追加	210
11.4. EBS ボリュームの復元方法	94	14.3.3. 通知先の削除	214
11.4.1. EBS ボリュームの復元(Windows)	94	14.3.4. 承認確認メールの再発行	216
11.4.2. EBS ボリュームの復元(Linux)	106	15. トラブルシューティング	219
11.4.3. EBS スナップショットからボリュームの作成(Windows/Linux 共通)	114	15.1. AWS 稼働状況確認	219
		15.2. 技術サポート問い合わせ方法	220



AWS導入後の運用管理の不安を大幅に軽減！



# サービスに関する注意事項①

## ※必ずお読みください

- EC2について
  - ・ 作業範囲はOSインストールまでとなります。OSの設定はお客様にて実施頂く必要がございます。
  - ・ パブリッククラウドの仮想マシンへの管理アクセスは、ご指定頂くグローバルIPアドレスからのみの接続を許可します。
- RDSについて
  - ・ 作業範囲はデータベースエンジンとサブネットグループまでとなります。パラメーターグループやオプショングループの設定はお客様にて実施頂く必要がございます。
  - ・ 設定内容は弊社指定の「設定シート」に記載頂いた内容のみとなります。
  - ・ Amazon RDS Custom と マルチAZ DBクラスタの構築は本サービスの対象外です。
  - ・ Oracle Management Agentのインストールや設定はサービス対象外です。
  - ・ MySQLはCloudwatchlogsへのログ出力を依頼される場合、パラメーター/オプショングループへ一部設定を行います。
- 監視と通知オプションについて
  - ・ 通知は管理者様にメールにて行いますが、メールの通知には管理者様側で許諾の処理を頂く必要がございます。
- サイト間VPNオプションについて
  - ・ サイト間VPNでは、オフィス(既存環境)側のカスタマーゲートウェイに固定グローバルIPアドレスが必要となりますのでご注意ください。
- ALBオプションとCloudFrontオプションについて
  - ・ Webサイトのヘルスチェックを実行するため、構築期間中に販売店様にてWebサイトを構築頂く必要がございます。なおWebサイトの構築期間は2週間程度を想定しています。
  - ・ SSL/TLS証明書発行に際し、DNSへの設定追加が必要となります。設定値はご連絡致しますが、お客様にて設定頂く必要がございます。
  - ・ CloudFrontオプションは、ALBオプションと連携する為、ALBオプションの同時購入が必要です。
  - ・ メニューにて対応可能なユーザからALBへの通信プロトコルはhttpsのみです(httpのみの利用はサポートしません)。
  - ・ ALB振り分けルールは「負荷分散」、Webサイト数は「1サイト」とさせて頂きます。
  - ・ Webサイトの動作確認および負荷分散試験はサービス対象外です。
- EC2の自動起動停止オプションについて
  - ・ 祝日や年末年始など考慮したスケジュールには対応できませんので、必要な際はお客様にて手動で停止と起動を実行ください。
  - ・ 監視と通知オプションにて実行結果を管理者へ通知する場合は、EventBridge Ruleのサービスの利用が必須です。



## サービスに関する注意事項②

※必ずお読みください

- **チャット通知オプションについて**
  - チャットサービスはMS Teamsとslackのみサポートします。
  - RDSの死活監視はチャット通知をサポートしません。
  - AWSからチャットサービス(MS Teams、slack)への通知が許可されている必要がございます。
  - チャットサービス側の設定は対象外となり、設定に関するご質問は弊社では対応致しかねます。
- **WAF PoC オプションについて**
  - ALBもしくはCloudFrontに対してカウントモードのWAF環境を構築します。
  - ベースラインルールグループとIPレピュテーションルールグループをWEBサイト全体に適用します。
  - カウントモードからブロックモードへの設定変更やルールの追加や削除はお客様にて実施頂く必要がございます。
  - 無償の操作手順書にて基本的なログの確認方法とブロック処理(指定のIPをブロック、指定のルールをブロック)、ルールの変更(追加、削除)方法を紹介しておりますが、操作手順書は弊社のAWS環境をベースとした操作手順の為、実際のお客様のAWS画面とは異なります。なお個別のカスタマイズを実施することはできません。
  - ログの分析やルールの最適化に関するご質問については対応致しかねますので予めご了承ください。
- **Patch Manager オプションについて**
  - パッチオペレーションは「スキャンとインストール」を設定します。「スキャン」のみの設定は致しかねます。
  - パッチポリシーは、AWSが事前定義したパッチベースラインにて作成します。「カスタムベースライン」の設定は致しかねます。
  - ダッシュボードの一部項目(Amazon EC2 インスタンス管理)が非表示となりますがご了承ください。※他AWSサービスの追加設定が必要となる為
  - 対象のEC2はインターネット接続が必須です。
  - アップデートファイルが提供されるタイミングによっては、構築時にインストール動作の確認がとれない場合がございますことを予めご了承ください。
- **メールサポートについて**
  - サポート範囲はAWS構築範囲となります。またお問い合わせの内容によってはメーカーへエスケーションさせて頂きます。その場合、ご回答までに数日掛かる場合がございます。
- **全てのお客様へのご注意事項**
  - バックアップからの復元方法は操作手順書をご提示いたしますので本番運用前にテストを実施ください。



## サービスに関する注意事項③

## ※必ずお読みください

- カスタマーゲートウェイサービスオプションについて
  - 対象機器について  
Cisco Meraki MXシリーズ、Cisco ASA5500シリーズ、Fortinet FortiGate 40+ シリーズ、Yamaha RTX ルーター  
※記載のない機種はサービス対象外となります。また、AWSカスタマーゲートウェイ対応デバイス、バージョンでの作業とさせていただきます。  
<https://docs.aws.amazon.com/ja.jp/vpn/latest/s2svpn/your-cgw.html>
  - 事前作業について  
ご注文から現地納品スケジュールは目安として約1か月ですが、パラメータシート完成のスケジュールに依存します。  
ヒアリングには、ネットワークのパラメータを決定できる方の参加が必要です。  
事前ヒアリングは原則として1回、最大2時間程度のWeb会議を見込んでおります。  
3rdパーティー製品との連携設定などは、範囲外とさせていただきます。(RADIUSサーバ等)  
キッティングを実施後、出荷致します。  
ルータはインターネット利用の用途を想定しております。  
またWAN側の複数回線の冗長設定、ルータのHA構成、複数拠点の接続(サイト間VPN)が必要な場合は別途ご相談ください。
  - 現地作業について  
現地対応時間は平日(月曜～金曜)9:00-17:00とし、日時は別途調整可能なことと致します。(ただし、祝日および弊社の定める休日を除く。)  
対応地域は、全国(県庁所在地から50km以内とする)、50km以上の場合は住所確認後に差額の交通費・諸経費を加味したお見積りをご提示致します。  
お客様先へ弊社SEが1名訪問します。  
AWS側のVPNステータスがオンラインであることの確認までとさせていただきます。
  - 導入後対応について  
メールサポートはメールでのベストエフォート対応とさせていただきます。  
メーカーサポートが利用できる保守に加入されていることが前提となります(メールサポート開始までにサポート窓口が利用できること)。  
環境引き継ぎ会は原則として1回、最大2時間程度のWeb会議を見込んでおります。
  - その他  
お客様都合によりスケジュールに遅延が起こった場合、納品日時についてのご要望にお応えできないことがございます。  
納品物はキッティングの際に実施した試験内容の試験計画書兼報告書と設定値をまとめたパラメータシートとさせていただきます。



## サービスに関する注意事項④

## ※必ずお読みください

- Amazon EFSオプションについて
  - Linuxを対象としたサービスです。※Windowsクライアントは非対応です。
  - オンプレミスのLinuxからのマウントは作業対象外です。
  - Amazon Linuxはamazon-efs-utilsをインストールの上、EFSマウントヘルパーにてマウントを実施しますが、その他のLinux OSの場合は、NFSにてマウントを実施します。
  - Amazon Linux以外のOSはamazon-efs-utilsのインストールは致しません。amazon-efs-utilsに関しては以下のURLをご確認ください。  
[https://pages.awscloud.com/rs/112-TZM-766/images/20180704\\_AWS-BlackBelt\\_AmazonEFS.pdf](https://pages.awscloud.com/rs/112-TZM-766/images/20180704_AWS-BlackBelt_AmazonEFS.pdf)
- Client VPNオプションについて
  - クライアントの認証方式にはActive Directory(AD)認証を使用します。
  - ADは既存(オンプレ)のものを利用する想定のため、ADの作成や設定は範囲外です。
  - クライアントPCへの設定は範囲外です。動作確認はユーザーもしくは販売店様にて実施をお願い致します。
  - 動作確認時にVPN接続用のクライアントVPNエンドポイント設定ファイルを1つ送付します。  
(利用ユーザーへの設定ファイルの展開は含みません)
  - クライアントPCからの接続はAWS Client VPNのソフトウェアをご利用頂く前提です。
  - 構築作業の開始前にサーバー証明書とCA証明書を作成頂き必要がございます。
  - AWS Certificate Manager(ACM)では、サーバー証明書とCA証明書インポートする作業のみ実施します。
- Auto Scaling PoCオプションについて
  - テスト用EC2(Webサーバー)を用いてAuto Scalingの構築及び動作確認を実施するPoCメニューとなります。
  - ALBオプションの購入が必須になります。
  - PoCメニューで設定するAuto Scaling Policyは“平均CPU使用率”と“ALBのヘルスチェック”になります。
  - Auto Scaling構築後、テスト用EC2の削除及びAuto Scalingの自動展開の設定をオフにした状態にし、マスター用EC2を作成した上で環境をお渡し致します。
  - 環境引き渡し後、お客様にて本番用のアプリケーション構築、起動テンプレートの更新及びAuto Scalingの起動確認を実施頂く必要がございます。



## サービスに関する注意事項⑤

※必ずお読みください

- VPCピアリングオプションについて
  - VPCピアリング接続の際にお客様の既存VPC環境の情報が必要になります。
  - IPアドレスの範囲が重複するVPC間の接続はサポートしていません。
  - VPCを跨いだVPC外(ゲートウェイ等を経由する通信)への通信はサポートしていません。
  - VPCを跨いだ間接的なVPCへの接続はサポートしていません。(2式での接続の場合)
  - お客様の既存VPC環境における設定(セキュリティグループ、ネットワークACL、ルートテーブル)は範囲外です。
  - VPCピアリング接続の構築にはお客様の既存VPC環境にてピアリング接続のリクエストを承諾して頂く必要があります。
  - 環境引き渡し後、お客様の既存VPC環境と新規VPC環境の接続確認をお客様にて実施をお願い致します。
- Entra-IAM連携オプションについて
  - Entra - IAM間の認証方式にはSAML認証を使用します。
  - Entraは既存のものを利用する想定のため、Entraの新規作成や設定は範囲外です。
  - 連携作業を実施する上で、Entraに作業用ユーザ(グローバル管理者)を作成いただきます。
  - 本番環境の動作確認はユーザ様もしくは販売店様にて実施をお願い致します。
- Route53オプションについて
  - ドメイン取得には別途取得料金がかかります。
  - サブドメインでのドメイン取得はサポートしていません。
  - ドメイン名は一意的の値になりますので、ご希望のドメインを取得できない可能性があります。
  - ALBオプションまたはCloudFrontオプションの購入が必須になります。
  - AWS外で取得されたドメイン、お客様が既存でお持ちのドメインの移行については対応範囲外となります。
  - AWS環境とオンプレミス環境間の名前解決は対応範囲外となります。



## 前提条件

## ※必ずお読みください

- 本サービスはDISのAWSサービス契約を締結しているお客様が対象です。
- AWS環境を新規に構築する際にご利用頂くことが可能です。
- 本サービス以外の追加要件(構築やドキュメントの追加)に関しましては対応致しかねます。
- オプションメニュー単体での購入はできません。基本セットとの同時購入が必須です。
- 事前打ち合わせおよび設定作業は平日日中帯(すべてリモートにて実施)を前提としております。
- サイト間VPN設定につきましてはAWS側の設定までが弊社作業範囲となります。カスタマーゲートウェイ側のサイト間VPN設定方法などについてのご質問は対応できかねます事をご了承下さい。
- 既存環境からのデータ移行作業やOS以上の設定はメニューの範囲外となり、ご対応できかねます事をご了承下さい。
- 作業期間中にAWS側の機能拡張/設定パラメータ変更などが発生する可能性も御座います。
- AWS側のサービス障害などにより弊社側作業の実施が難しい状況が起きた場合は、各種スケジュールを変更させて頂く可能性も御座います事をご了承下さい。
- 納品フェーズの環境引継ぎ会(リモート1時間程度)実施後の2週間をフォロー期間としてメールでのお問い合わせに対応いたします(平日9時~17時のベストエフォート対応)。
- フォロー期間におけるメール対応は、本サービスの構築範囲に限定いたします。
- フォロー期間以降のAWSに関する技術的なご相談やトラブルはメーカー窓口(AWS技術サポート)にお問い合わせください。



# さわって理解するAWSハンズオン基礎講座について

# さわって理解するAWSハンズオン基礎講座(仮想マシン編)

AWS(Amazon Web Services)の基本要素やコンセプトを、初歩から学びながら、ハンズオン(実操作)を通してクラウドにおけるリソースの調達や基本設定の方法を習得できます。  
EC2をはじめとしたAWSの各種サービスをハンズオンで実体験することで、AWSの基礎的な知識を理解し、操作スキルの習得を目指すトレーニング内容です。

## 受講のメリット

1. 自己学習よりも短時間で学ぶことができます。
2. 正しいインフラ構築を実際に手を動かしながら技術を身につけることができます。
3. 操作手順書(350ページ以上)をお渡ししますのでトレーニング後も安心して構築することができます。  
※操作手順書は仮想マシン編、Webインフラ編共に同じものをお渡しいたします。

## 商品コード:ZDX-DXPRACAWSSTEP1

- 授業料 :個別相談
- 受講形式 :集合研修(オンラインも対応可)  
1日(10時~12時、13時~17時※昼休憩60分間)  
※希望日を確認して別途調整いたします  
※集合研修の場合、別途交通費が掛かる場合がございます
- 人数条件:最少催行人数 6名、最大人数 10名
- 対象者 :これからAWSを使い始める方  
AWSサービスの概要を学びたい方



## 講座内容

### 【座学&ハンズオン】

- 1.AWSの基本概念
- 2.マネジメントコンソールの使い方
3. AWSアカウントをつくってみよう
- 4.ネットワークを作ってみよう
- 5.仮想サーバーをつくってみよう
- 6.バックアップと監視の仕組みをつくってみよう
- 7.その他のAWSサービスのご紹介
8. AWSにおけるセキュリティについて

# さわって理解するAWSハンズオン基礎講座(Webインフラ編)

AWS(Amazon Web Services)のロードバランサーやWAFといったネットワークインフラストラクチャについて、座学で基礎知識を学び、各サービスをハンズオンで実際に操作することで、実践的な知識と技術を習得できるトレーニング内容です。

## 受講のメリット

1. 自己学習よりも短時間で学ぶことができます。
2. AWSのよりクラウドネイティブなサービスの知識・技術を身につけることができます。
3. 操作手順書(350ページ以上)をお渡ししますのでトレーニング後も安心して構築することができます。  
※操作手順書は仮想マシン編、Webインフラ編共に同じものをお渡しいたします。



## 商品コード:ZDX-DXPRACAWSSTEP2

- 授業料 :個別相談
- 受講形式 :集合研修(オンラインも対応可)  
1日(10時~12時、13時~17時※昼休憩60分間)  
※希望日を確認して別途調整いたします  
※集合研修の場合、別途交通費が掛かる場合がございます
- 人数条件:最少催行人数 6名、最大人数 10名
- 対象者 :AWSサービスの概要を学びたい方  
Webサーバーのセキュリティや可用性を向上させたい方

## 講座内容

### 【座学&ハンズオン】

- 1.ロードバランサーを作ってみよう
- 2.URL監視を作ってみよう
- 3.CloudFrontを作ってみよう
- 4.WAFを作ってみよう
- 5.Auto Scalingを作ってみよう

**DiS**

ダイワボウ情報システム株式会社

**DiS**