Serverworks

AWS サービスでできる
セキュリティ対策

アジェンダ

1. 自己紹介
2. 株式会社サーバーワークスについて
3. AWS の概要
4. AWS 利用開始時に行っておくべきこと
5. オンプレミスから AWS への移行事例
6. AWS セキュリティサービスの紹介
7. リモートワーク向け AWS サービスの紹介
8. まとめ

自己紹介

Serverworks

自己紹介

小倉 大（おぐら まさる）

@MasaruOgura

- 世の中の方が AWS を使えるようになることを
  サポートすべく教育事業に従事
- 好きな AWS サービスは **VPC**
- AWS 認定 すべて保有
- 2020 / 2021 APN ALL AWS Certifications Engineers

株式会社サーバーワークスについて

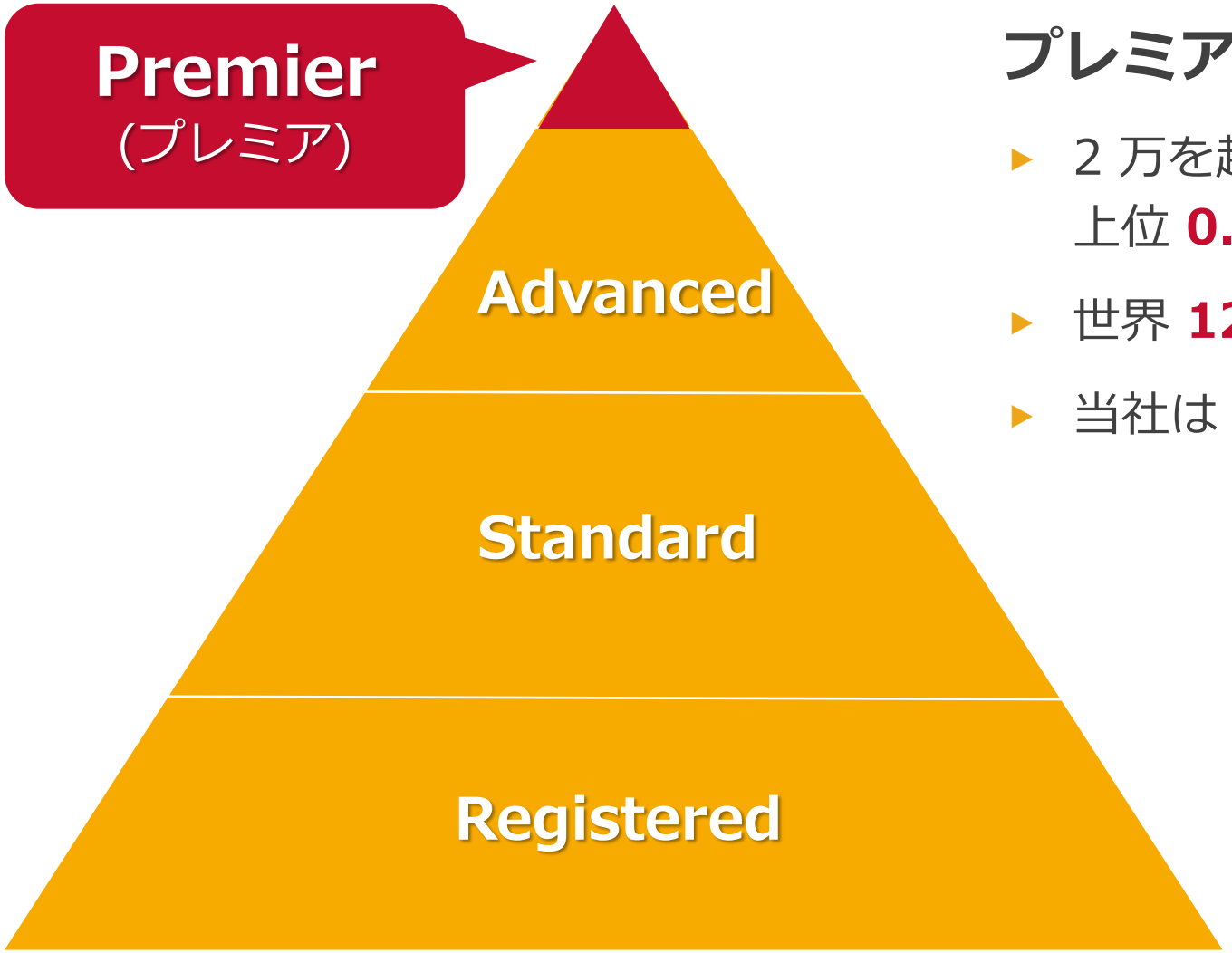
Serverworks

株式会社サーバーワークス

- AWS 専業のシステムインテグレーター

APN プレミアコンサルティングパートナー

2021 年 11 月現在



プレミアコンサルティングパートナー

- 2 万を超える AWS のパートナーから
  上位 **0.3 %** が認定される**最上位パートナー**
- 世界 **125 社**、日本で **11 社**のみ選出
- 当社は **2014 年**より**連続**で認定

11,000 プロジェクトを超える AWS 導入実績

2021 年 11 月現在

AWS の概要

Serverworks

AWS の概要

1. AWS とは
2. AWS のサービス
3. AWS の利用

AWS とは

- アマゾン ウェブ サービス の略
- 2006 年にスタートした
  クラウド (クラウドコンピューティング) のサービス
- Amazon.com で使われる技術がそのまま利用可能

クラウドとは

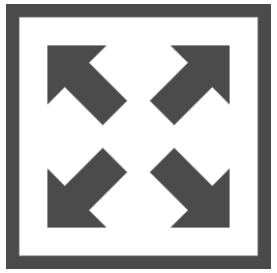
- インフラやソフトウェアを
- ネットワークを通じて
- 必要な時に必要な分だけ利用できる

クラウドの特徴

初期投資ゼロ / 低価格

最新の技術をすぐに利用可能

俊敏性



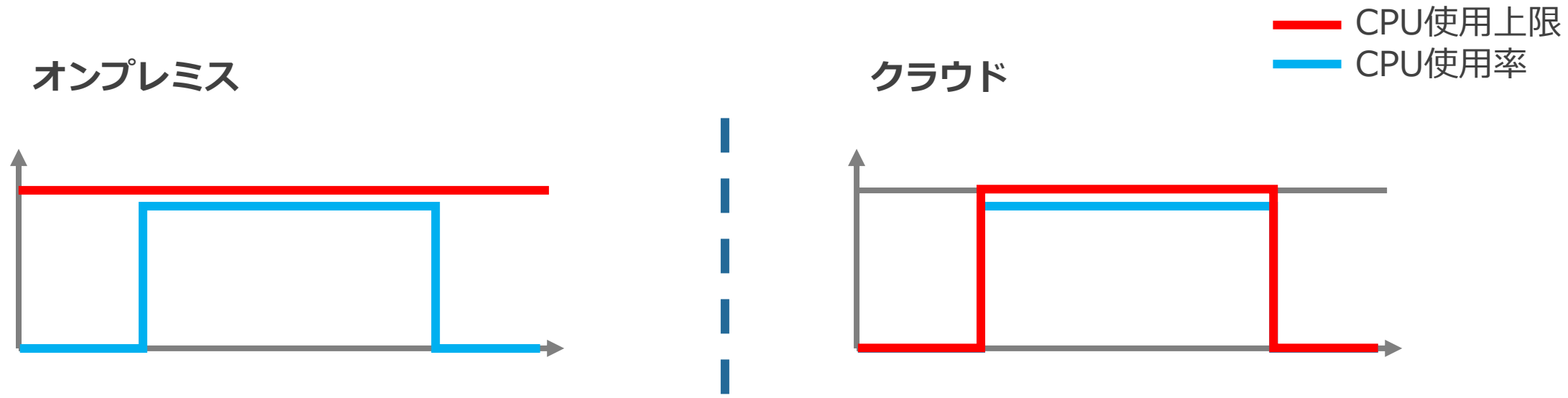
サイジングからの解放

運用負荷軽減

高いセキュリティ

オンプレミスとクラウドの比較

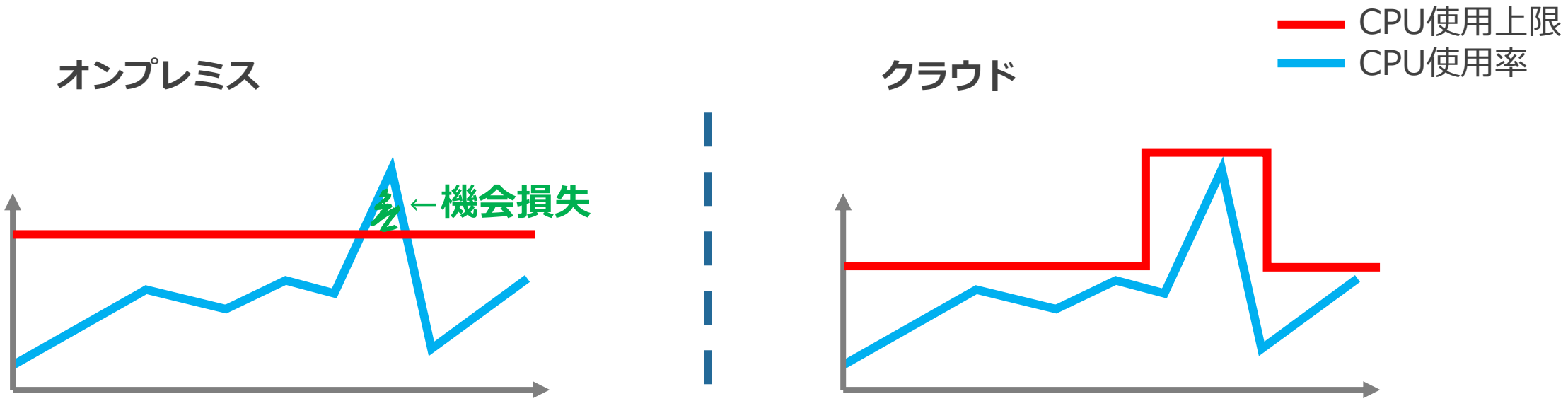
① 夜間の利用がないケース



クラウドは利用分のみの支払いのため、利用していないときに
停止することでコストを抑えることが可能

オンプレミスとクラウドの比較

② スペックを超える処理をするケース



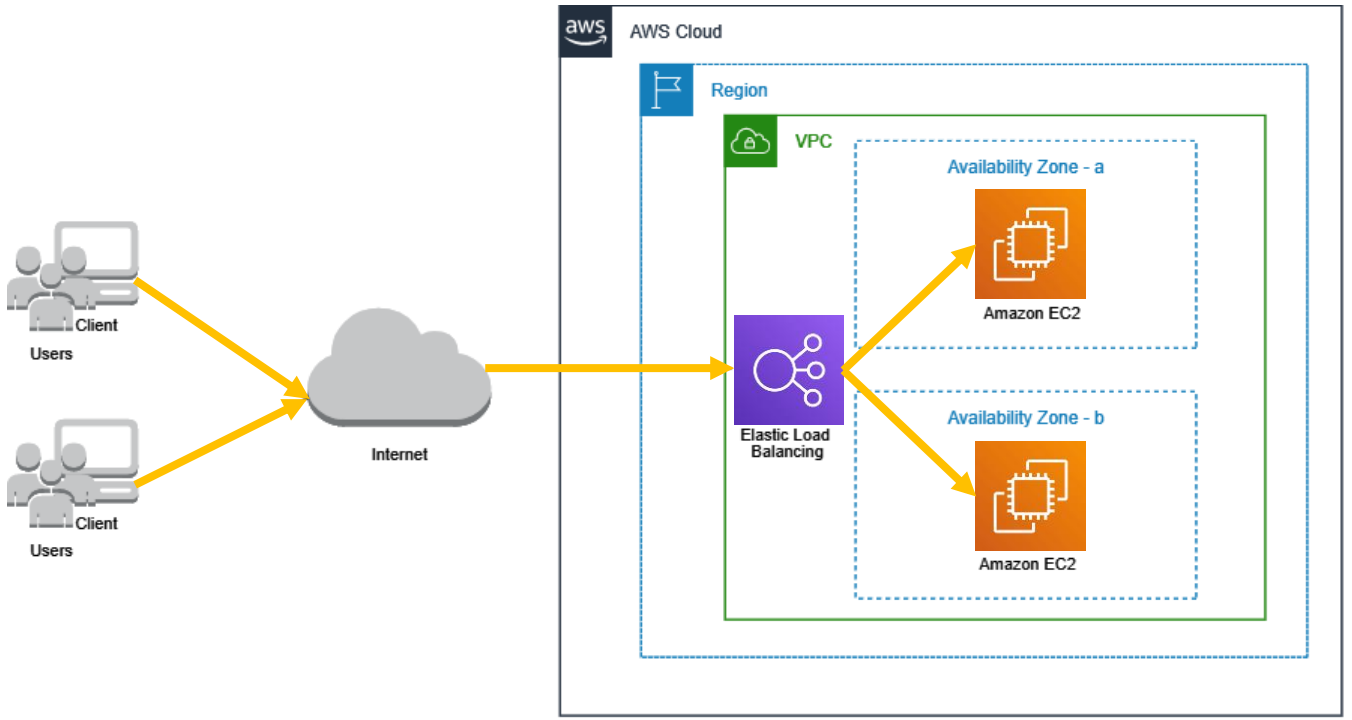
オンプレミスは処理ができずビジネス機会を逃してしまうが、
クラウドであればスペックを上げて処理が可能

AWS のサービス

- コンピューティングやストレージ、機械学習支援から IoT まで、
  200 以上 (※) のサービスを提供　※ 2021 年 9 月現在
- サービスを組み合わせることで、最新の技術を活用して自社のビジネスを
  スモールスタートで開始することが可能

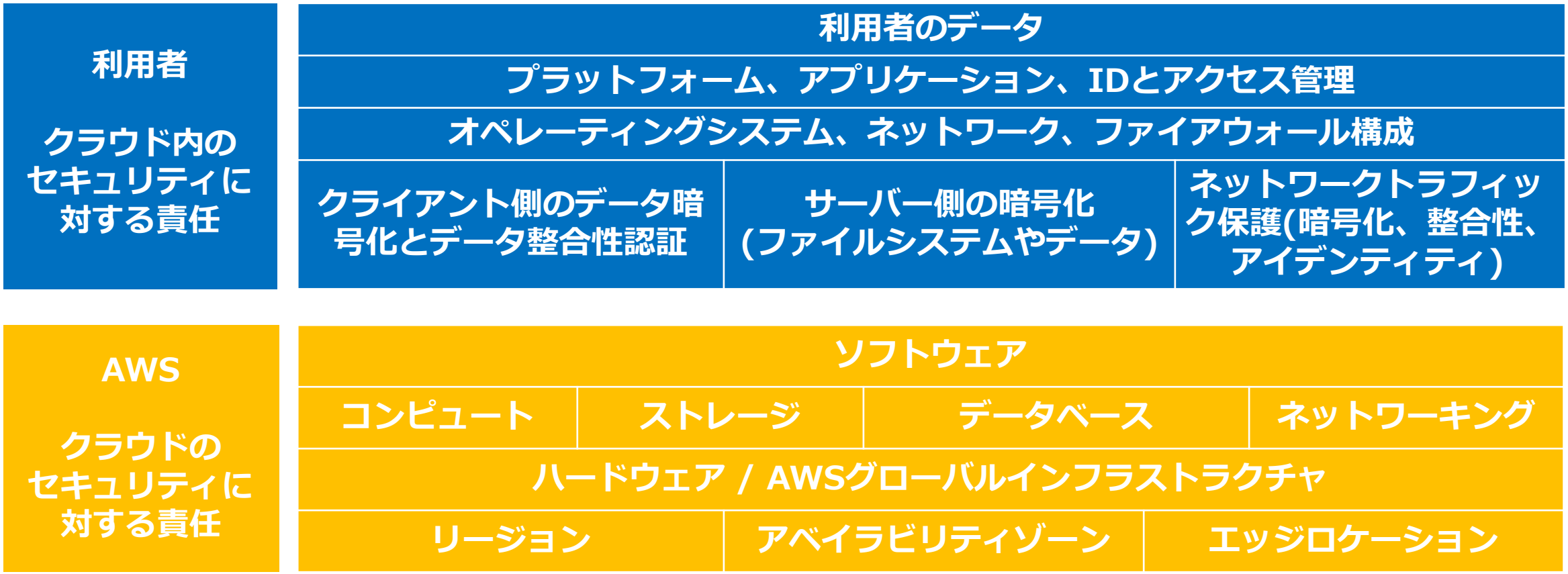
AWS サービスの組み合わせ例

- 多人数のアクセスに耐えられる冗長化した Web サービス



責任共有モデル

- 利用者側と AWS 側で責任範囲が分かれている



AWS の概要 (まとめ)

1. AWS とは
2. AWS のサービス
3. AWS の利用

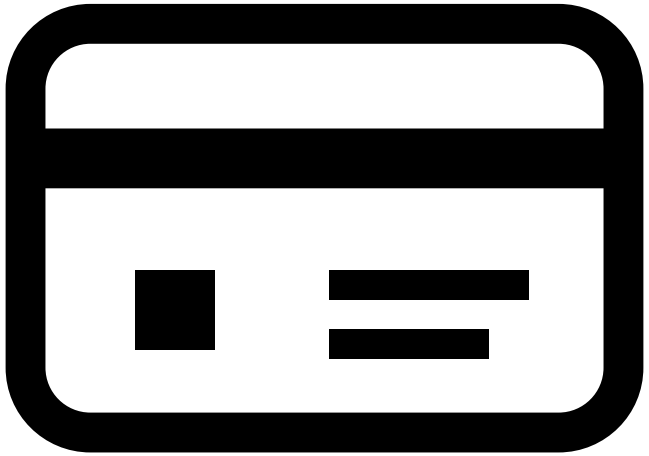
AWS 利用開始時に行っておくべきこと

Serverworks

AWS 利用開始時に行っておくべきこと

0. AWS アカウントの作成
1. ルートユーザーに MFA を設定
2. AWS にログインするための IAMユーザーを作成
3. 予算額の設定

0. AWS アカウント作成



クレジットカード情報

住所

アカウントを**新規に開設**

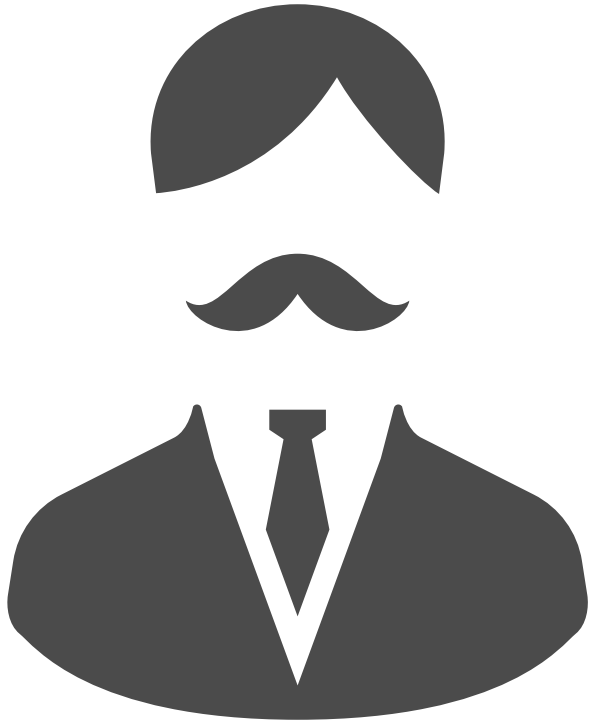
0. AWS アカウント作成

- 設定した情報（メールアドレス・パスワード）で
  AWS にログイン、使用できるように
- アカウントを用意する**だけ**であればこの手順で完了

ベストプラクティスに則り
「安全」にアカウントを用意するためには不十分

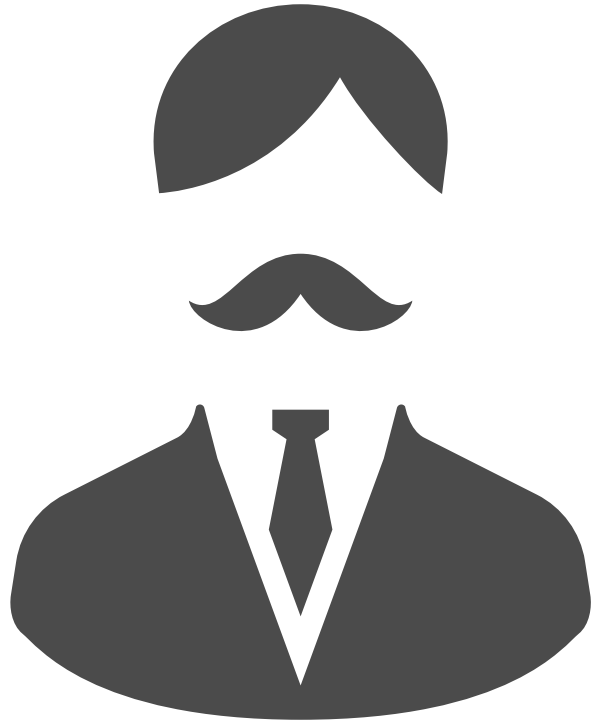
1. ルートユーザーへの MFA の設定

- **ルートユーザー**
  - アカウント開設時に設定したメールアドレス・パスワードを使用してログインした際に使用
  - デフォルトユーザー
  - **アカウントに対する全権**を持つ



1. ルートユーザーへの MFA の設定

- **ルートユーザー**
  - アカウント開設時に設定したメールアドレス・パスワードを使用してログインした際に使用
  - デフォルトユーザー
  - **アカウントに対する全権**を持つ

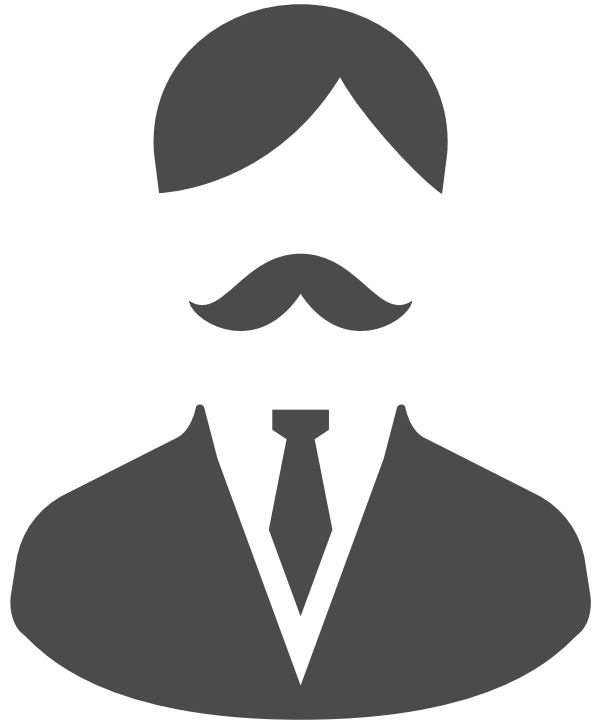


認証情報が漏洩すると非常に危険

1. ルートユーザーへの MFA の設定

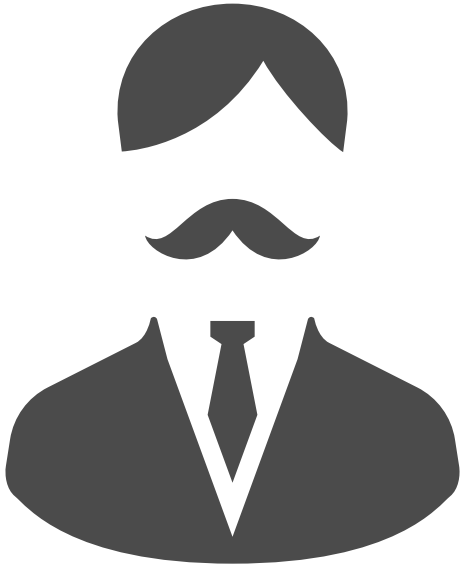
認証情報が漏れると非常に危険

自分以外が利用できないよう
MFA を設定し保護



1. ルートユーザーへの MFA の設定

認証情報が漏れると非常に危険



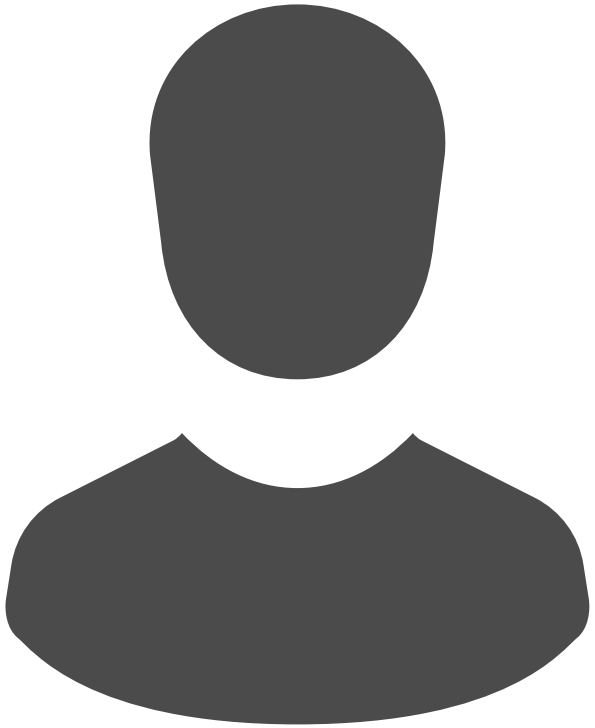
自分以外が利用できないよう
MFA を設定し保護

＋

普段使いしない

2. IAM ユーザーの作成

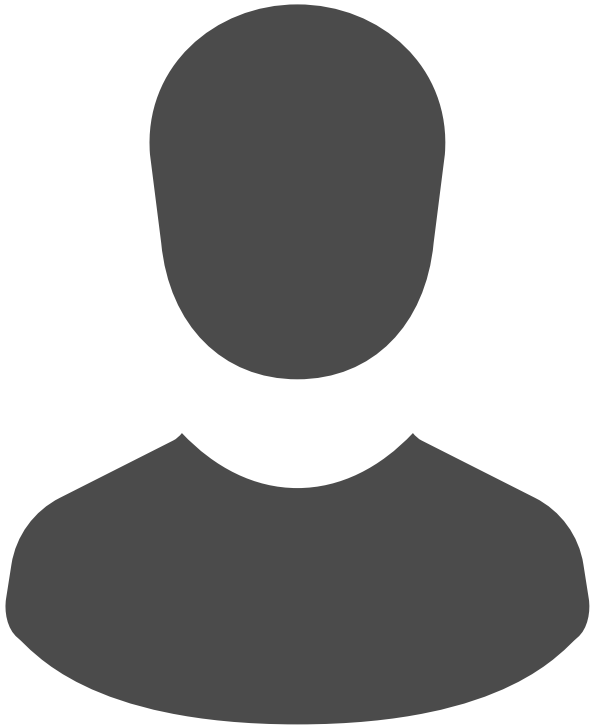
- **IAMユーザー**
  - AWS へアクセスするため
    利用者が自由に作成できるユーザー
  - 利用できるサービス・機能を細かく制御
  - **アカウント情報の更新・削除など**
    クリティカルな操作は制限されている



2. IAM ユーザーの作成

- IAM ユーザーの認証情報が漏洩してしまっても、、、

- **被害は最小限に**
  - クリティカルな操作はされない
- **被害をストップできる**
  - IAMユーザーを削除しログインできないように



必ず実施すること！

3. 予算額の設定

- AWS は「従量課金制」のサービス
  - 使った分だけ料金が発生
  - 事前に料金が確定しない ＝ リソースを使えば使うほど料金が積み上がる

- 何かしらの方法で**現在の利用額を把握する必要**あり

3. 予算額の設定

- AWS Budgets
  - 予算管理を行う AWS サービス
    - 期間と予算を設定
    - 実際の利用料をチェックし通知

AWS Budgets

AWS 利用開始時に行っておくべきこと (まとめ)

0. AWS アカウントの作成
1. ルートユーザーに MFA を設定
2. AWS にログインするための IAMユーザーを作成
3. 予算額の設定

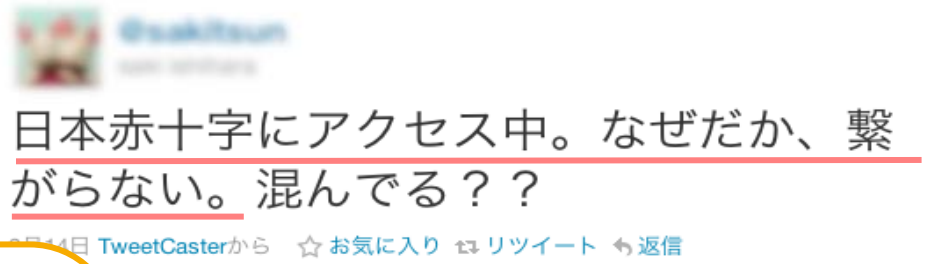
オンプレミスから AWS への移行事例

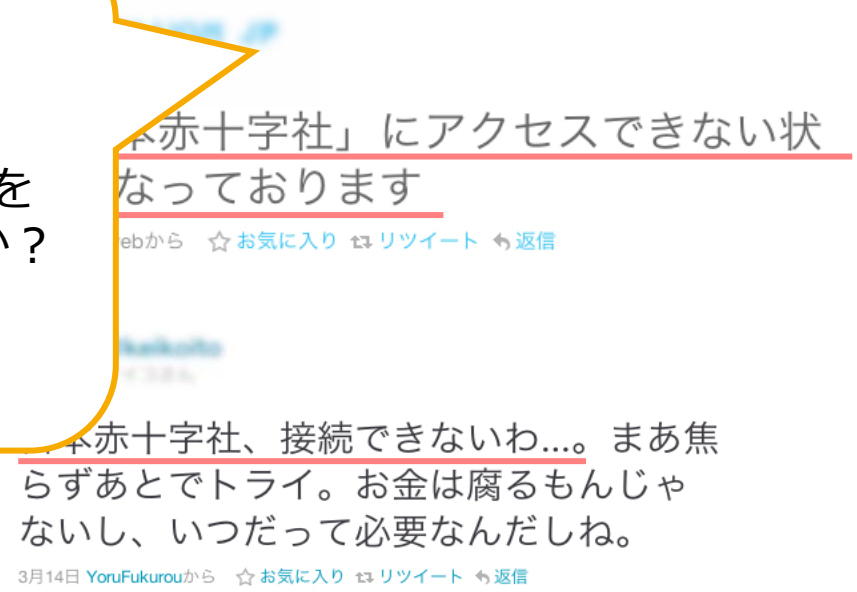
Serverworks

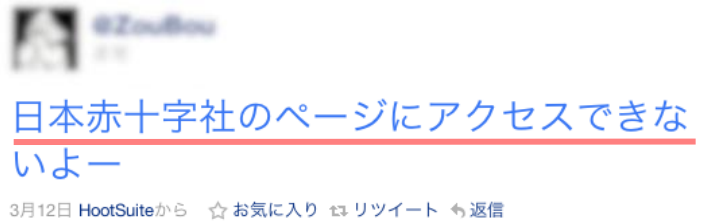
【移行事例】日本赤十字社様(1/5)

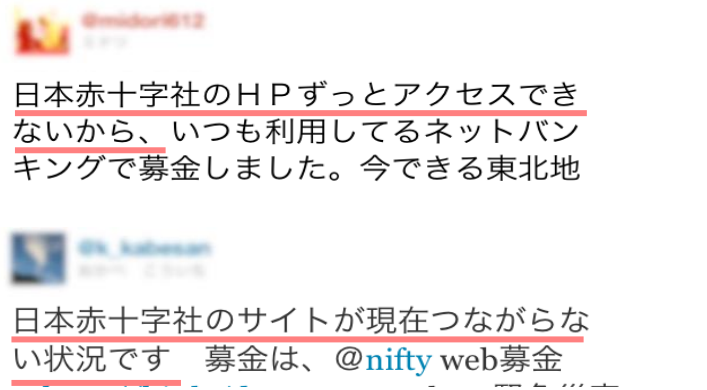
東日本大震災当時の様子

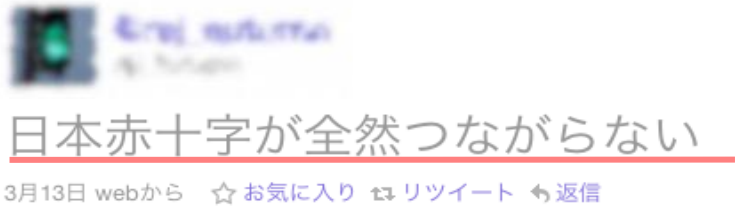
アクセス集中により、
サイトがダウンしたことを
覚えていらっしゃいますか？









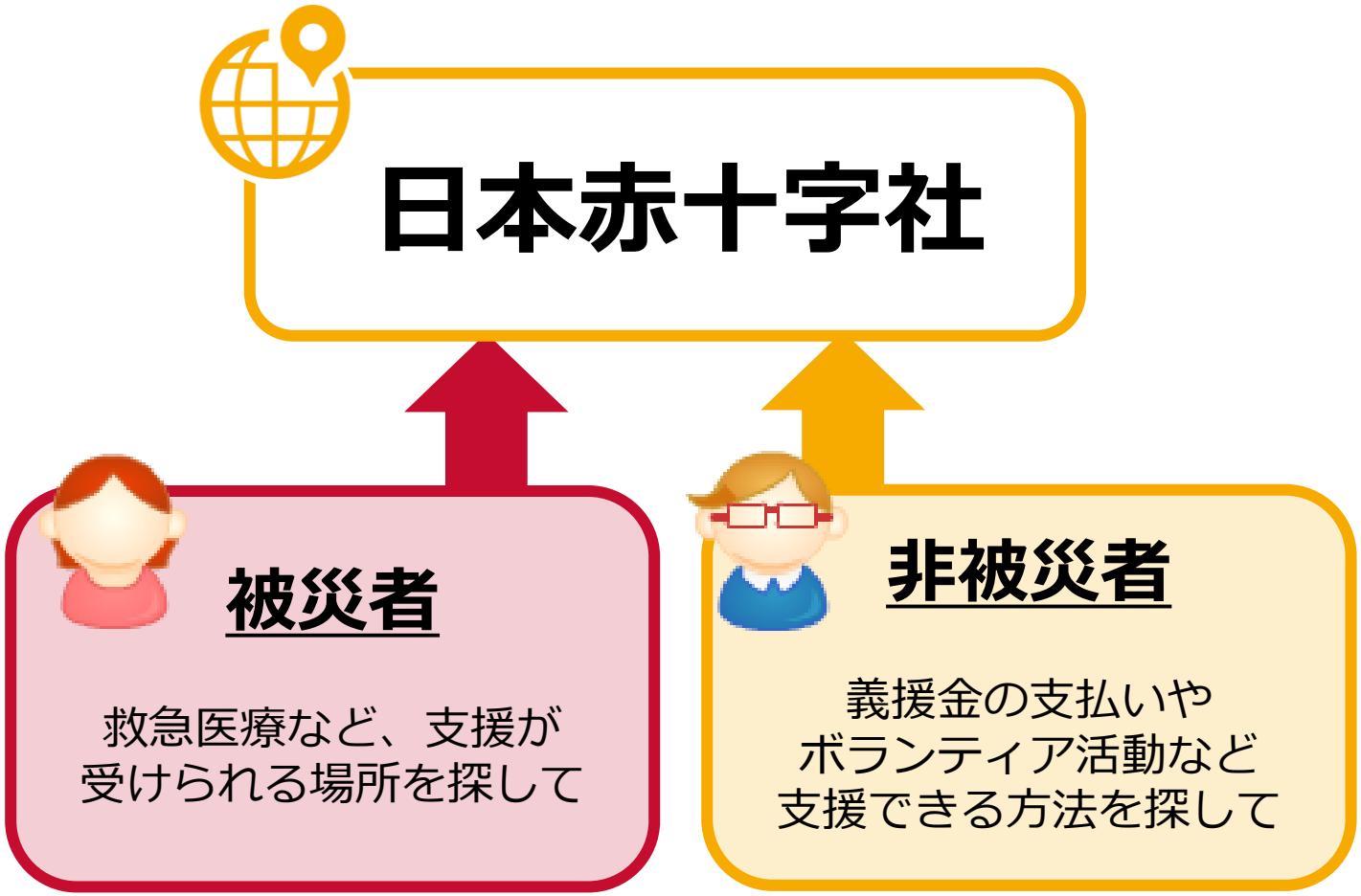


Serverworks

【移行事例】日本赤十字社様(2/5)

サイトダウンの理由

情報を必要としている方が
一斉にアクセスしたのが
原因でした

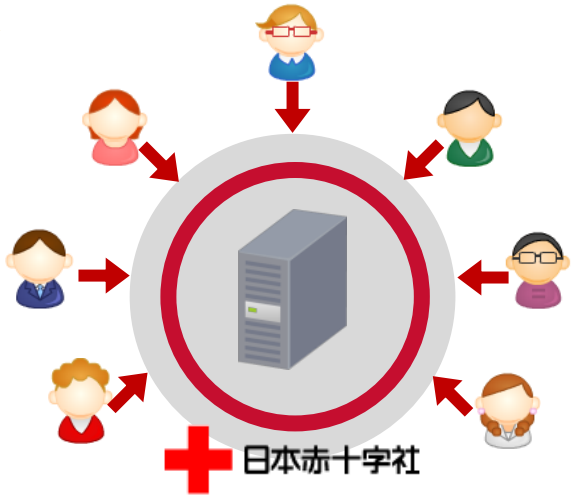


【移行事例】日本赤十字社様(3/5)

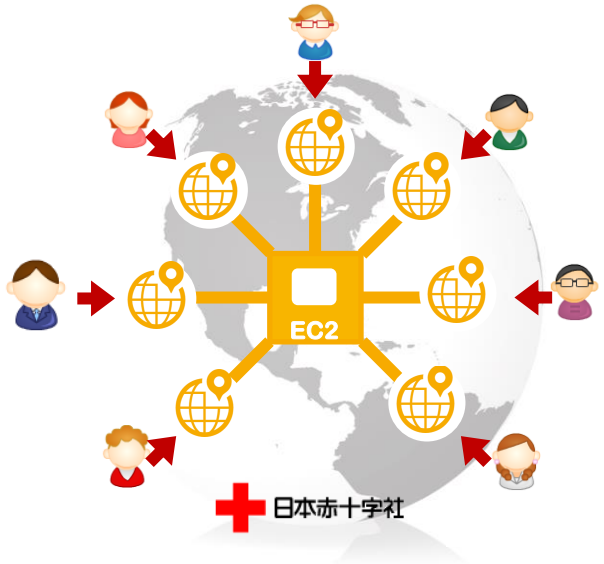
AWSを導入して、サーバーの負荷を軽減

サーバーワークスは、
急遽ボランティアで
AWSの導入を
サポートいたしました

日本赤十字社



AWS



Serverworks

【移行事例】日本赤十字社様(4/5)

義援金の管理システムを構築

環境構築 2時間

アプリ開発 48時間

全社一丸となり、
最速で開発を進めサイトを復旧、
その上義援金受付を
開始できました

3月 **14**日　**日本赤十字社 様との打ち合わせ**

3月 **15**日　**サイト復旧**

3月 **17**日　**義援金 受付開始**

【移行事例】日本赤十字社様(5/5)

日経SYSTEMS様 2011年6月号でご紹介頂きました

弊社が対応させて頂いた後、
日本赤十字社様のサイトが
サーバーダウンすることは
一度もなく

スムーズな義援金管理
ができたことから、メディアにも
取り上げていただきました

エンジニアの被災地復興支援

日赤のWebサイトをダウンから救う
被災地に必要な物資は見える化

ITの現場
復興の道しるべ

特集1 ITの現場 復興の道しるべ

図A 日本赤十字社の義援金事前登録システムを突貫構築

図B どこでどんな物資が求められているかを見える化

Twitterの分析システムを開発

AWS セキュリティサービスの紹介

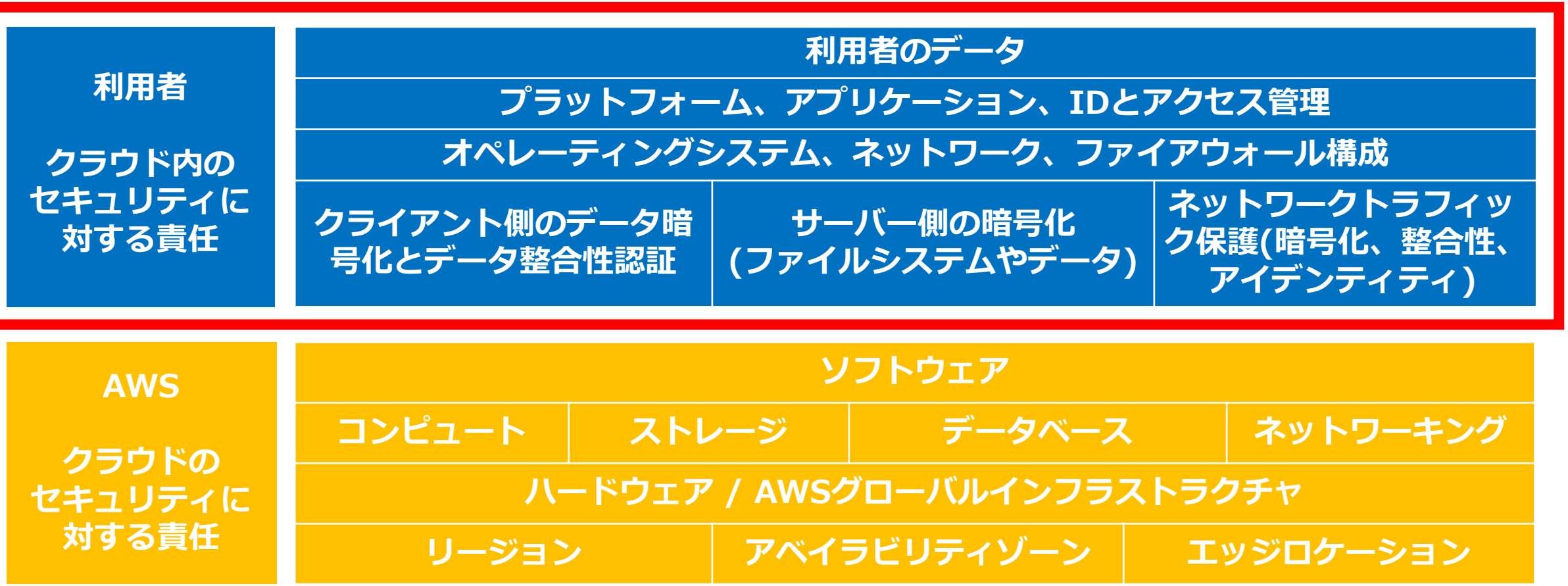
Serverworks

AWS セキュリティサービスの概要

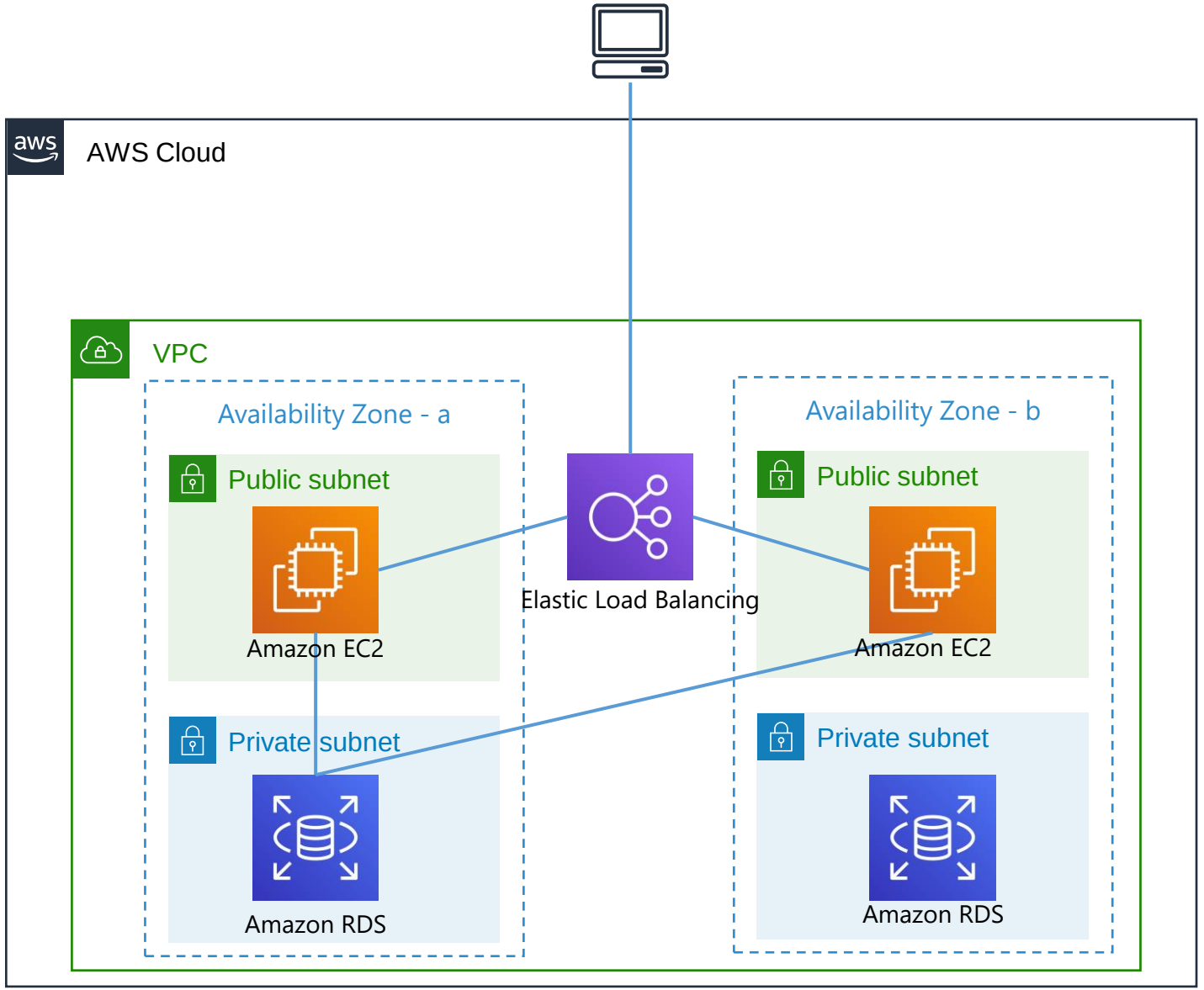
1. AWS Certificate Manager (ACM)
2. AWS Key Management Service (KMS)
3. AWS WAF
4. AWS Shield
5. Amazon GuardDuty

【再掲】責任共有モデル

- 利用者側と AWS 側で責任範囲が分かれている

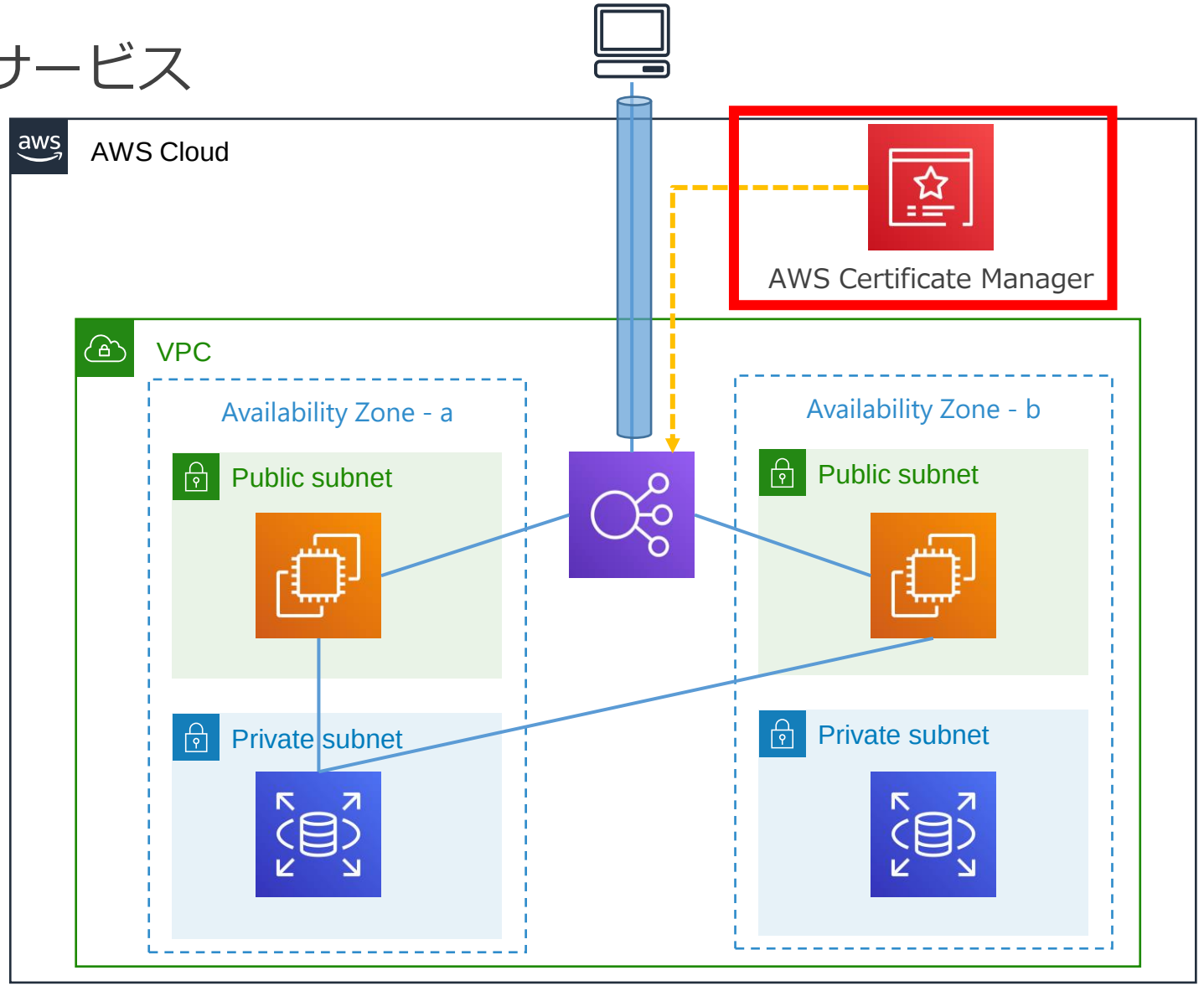


Web システムの構成


AWS Cloud
VPC
Availability Zone - a
Public subnet
Amazon EC2
Private subnet
Amazon RDS
Elastic Load Balancing
Availability Zone - b
Public subnet
Amazon EC2
Private subnet
Amazon RDS

1. AWS Certificate Manager (ACM)

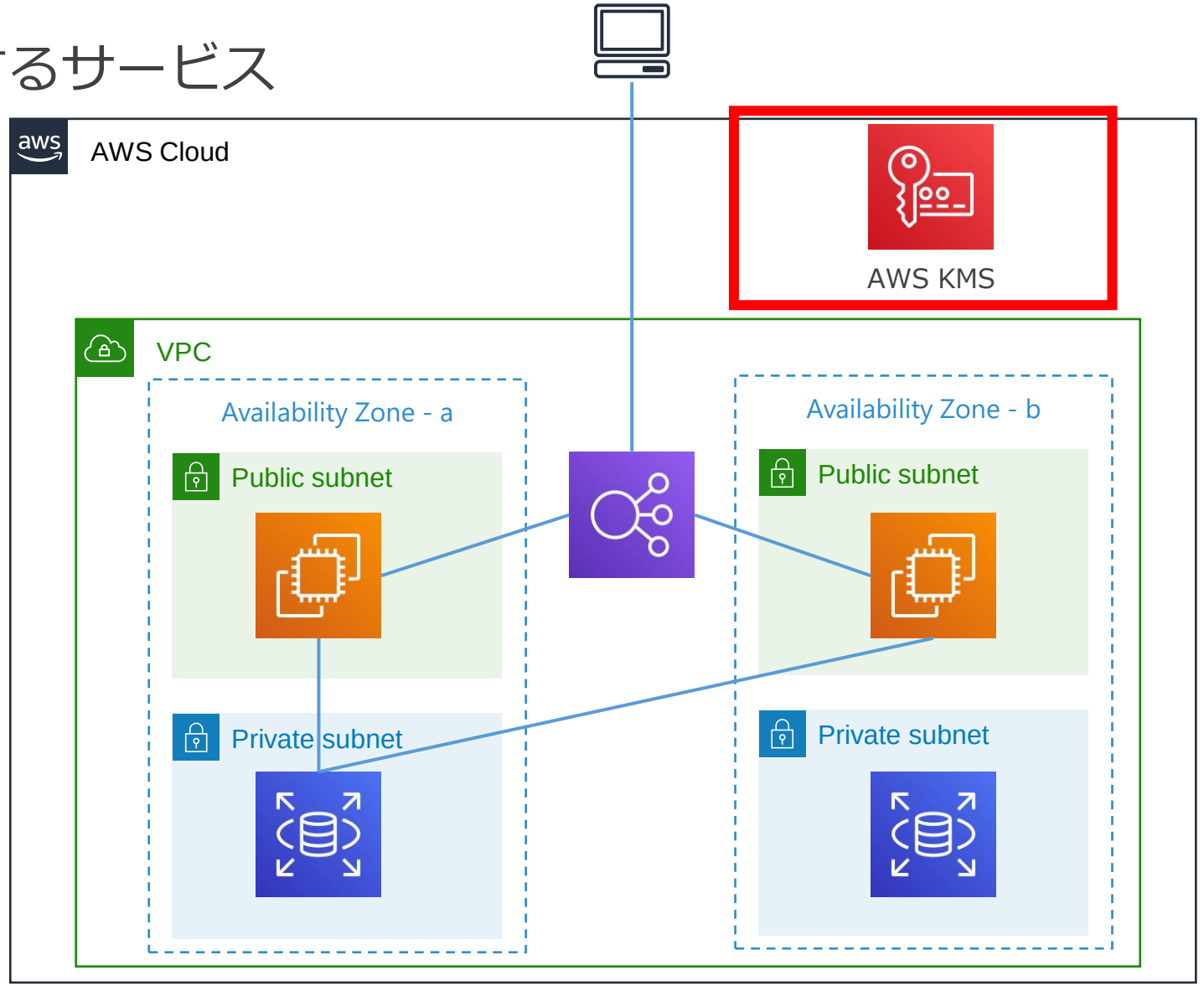
- SSL/TLS 証明書を管理するサービス
- トラフィックを暗号化



Serverworks

2. AWS Key Management Service (KMS)

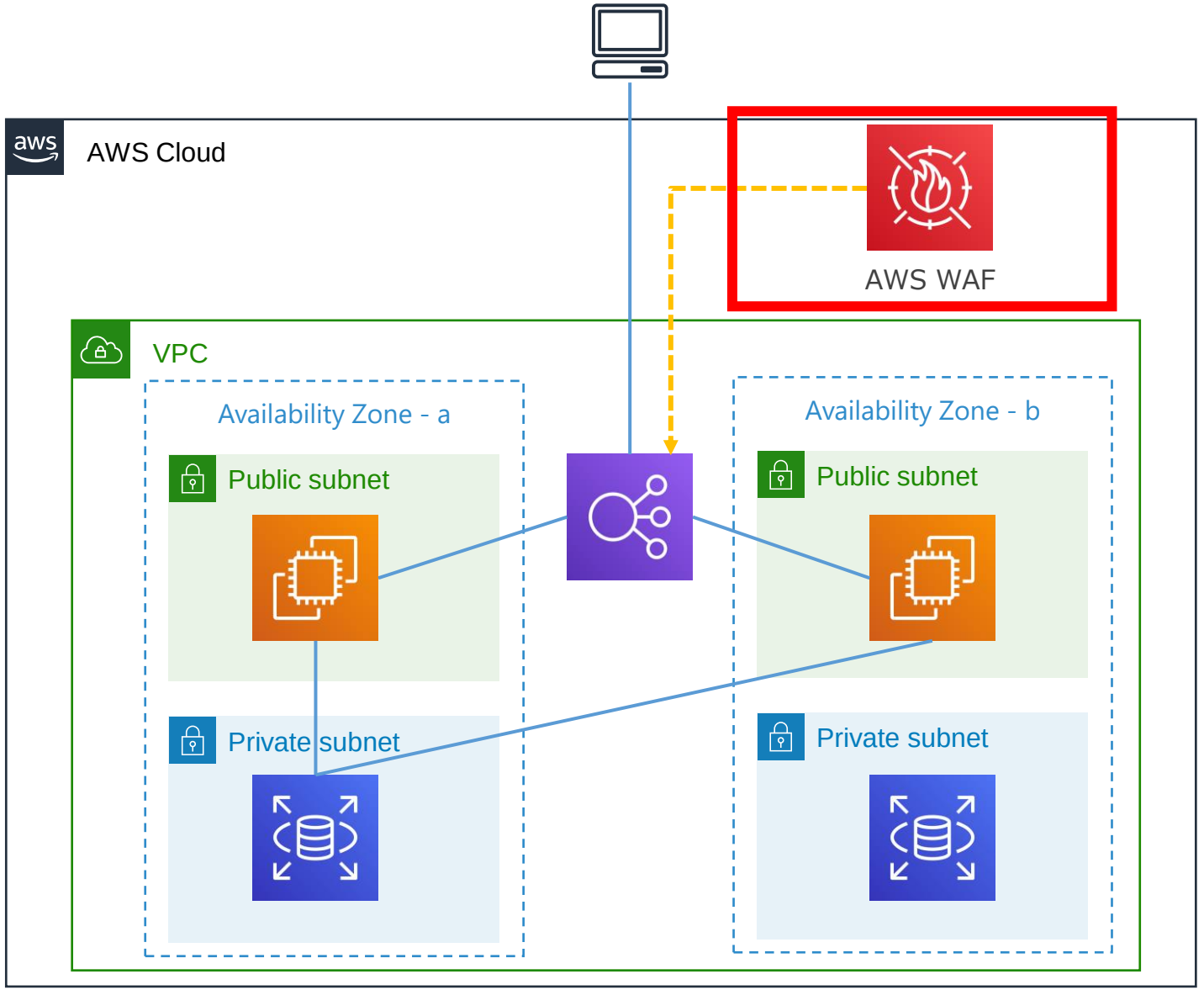
- 暗号化キーの作成・管理をするサービス
- データの暗号化



Serverworks

3. AWS WAF

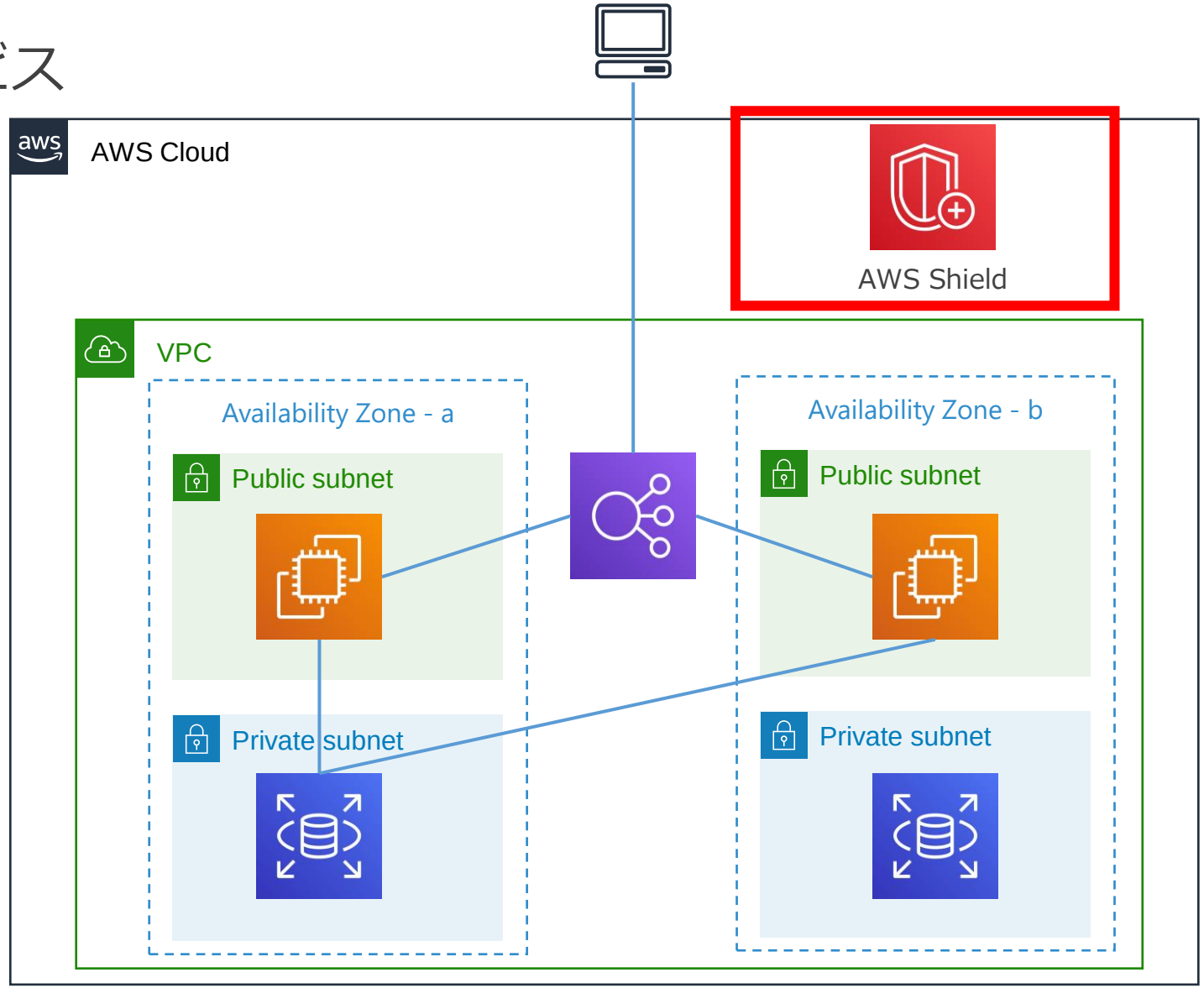
- WAF のサービス
- SQLインジェクションなど既知の攻撃を防御



Serverworks

4. AWS Shield

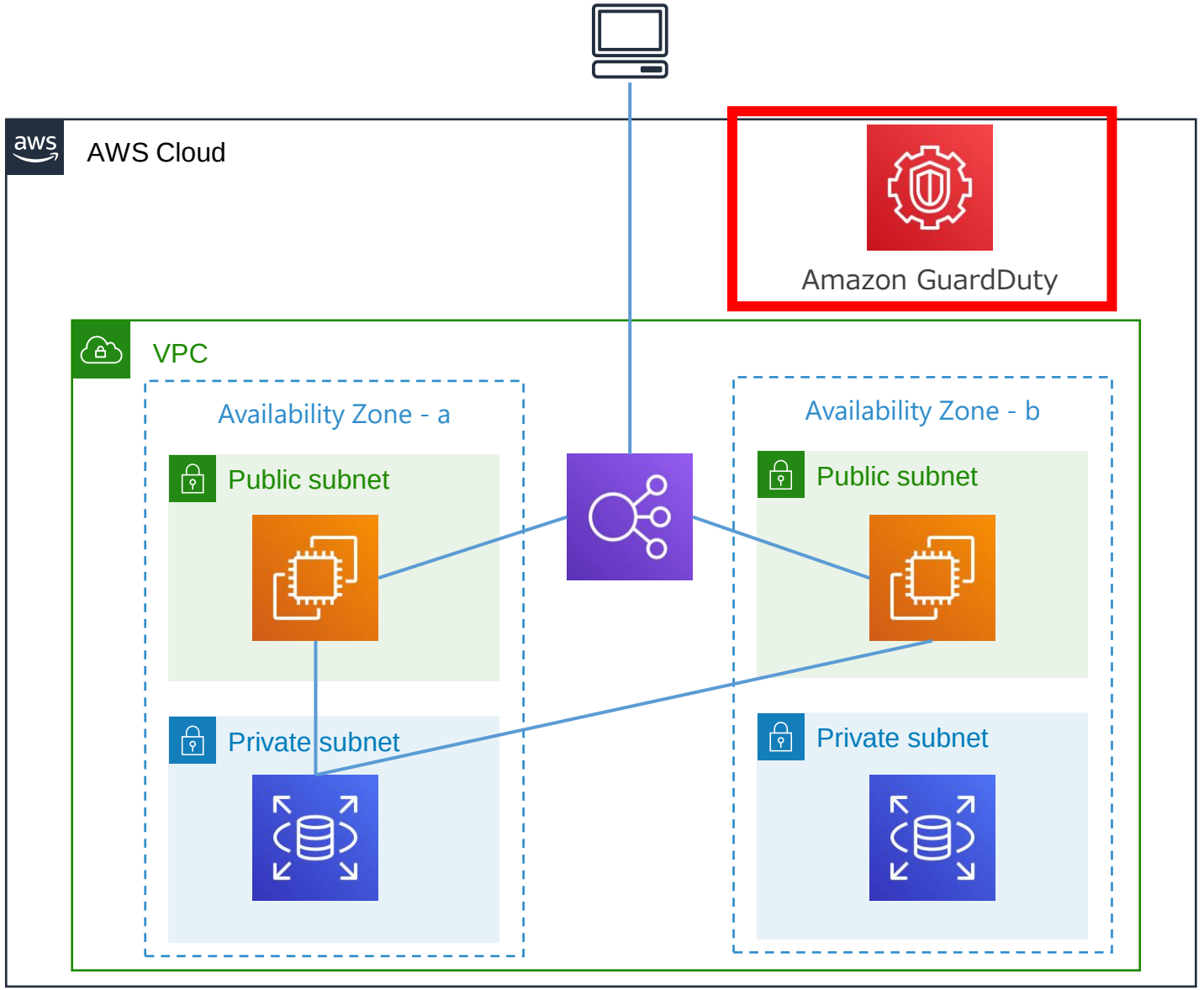
- DDoS 攻撃を緩和するサービス
- インターネットに面した
  AWS のサービスに対して
  透過的に適用され、
  DDoS 攻撃を自動的に緩和



Serverworks

5. Amazon GuardDuty

- 脅威検出サービス
- 通信ログなどを監視し、不正な動作を検出



Serverworks

AWS セキュリティサービスの概要 (まとめ)

1. AWS Certificate Manager (ACM)
2. AWS Key Management Service (KMS)
3. AWS WAF
4. AWS Shield
5. Amazon GuardDuty

リモートワーク向け AWS サービスの紹介

Serverworks

リモートワーク向け AWS サービスの概要

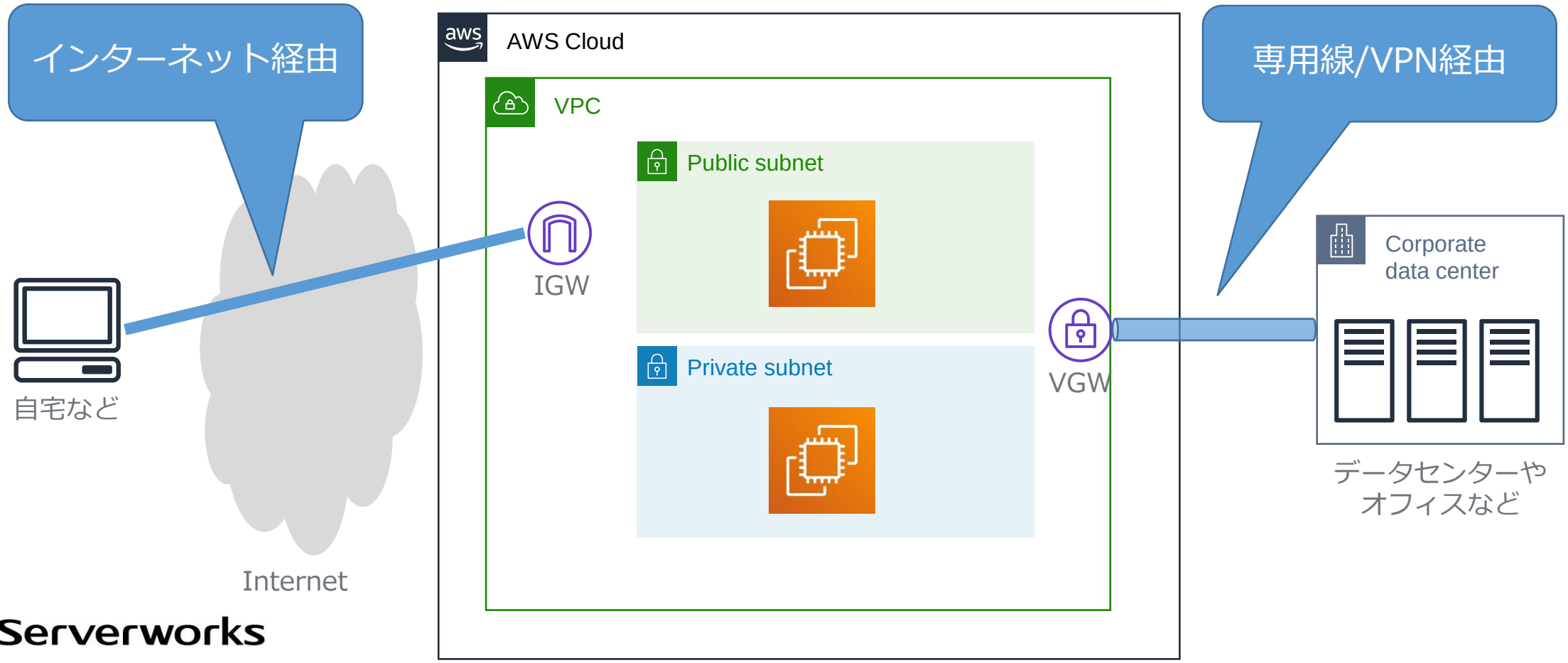
1. AWS Client VPN
2. Amazon WorkSpaces
3. Amazon Connect

1. AWS Client VPN

- AWS リソースに安全にアクセス
  できるようにする、クライアント
  ベースのマネージド VPN サービス

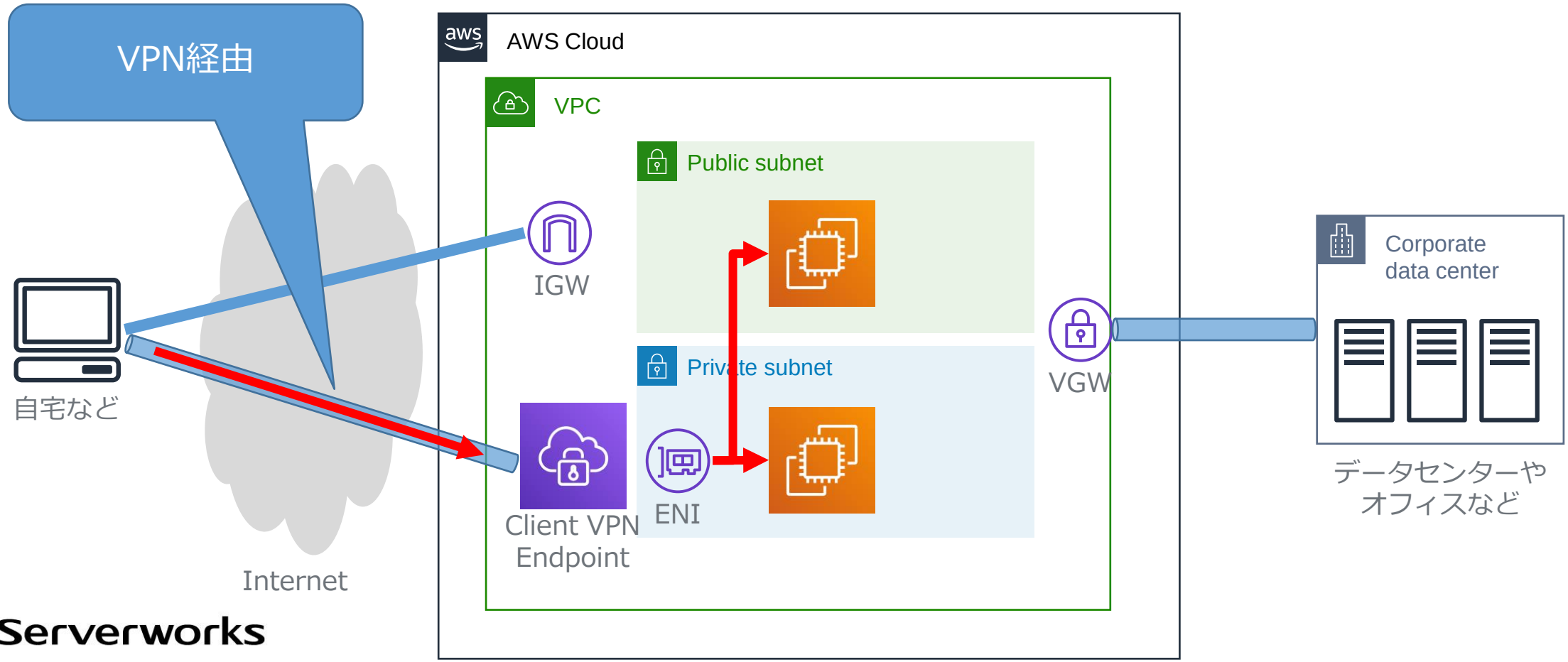
AWS Client VPN

1. AWS Client VPN



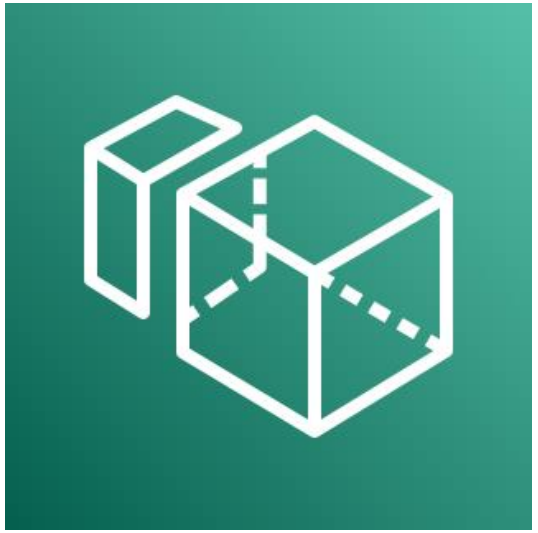
Serverworks

1. AWS Client VPN



2. Amazon WorkSpaces

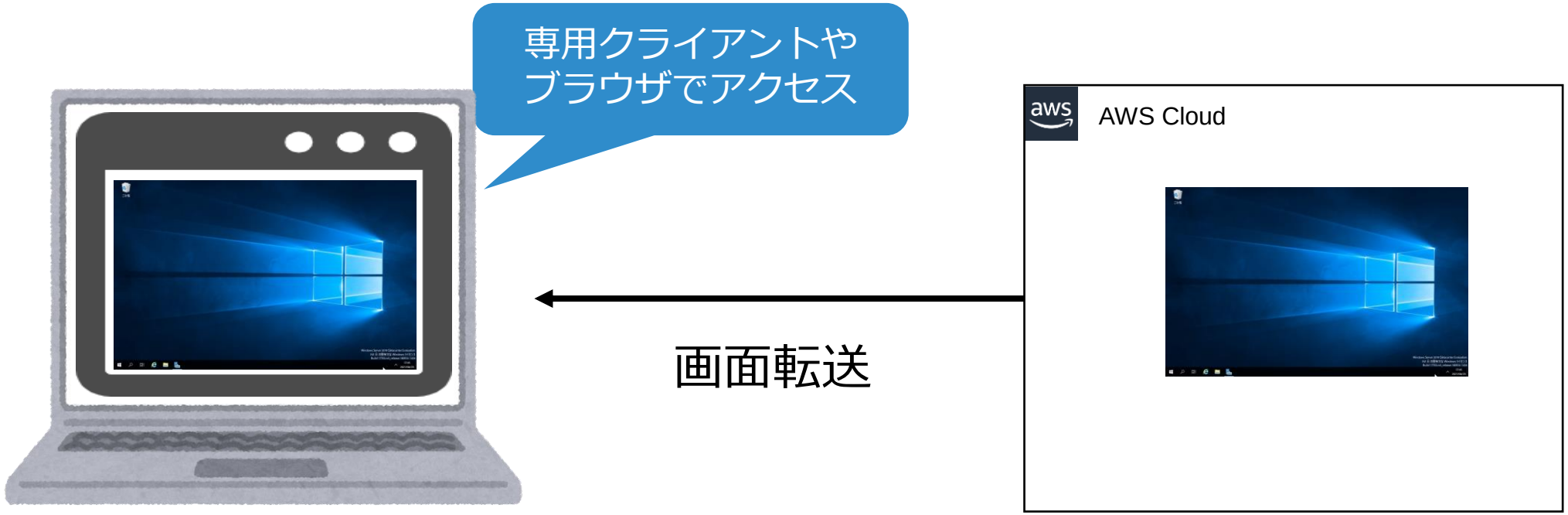
- AWS が提供する永続デスクトップ仮想化のサービス



Amazon WorkSpaces

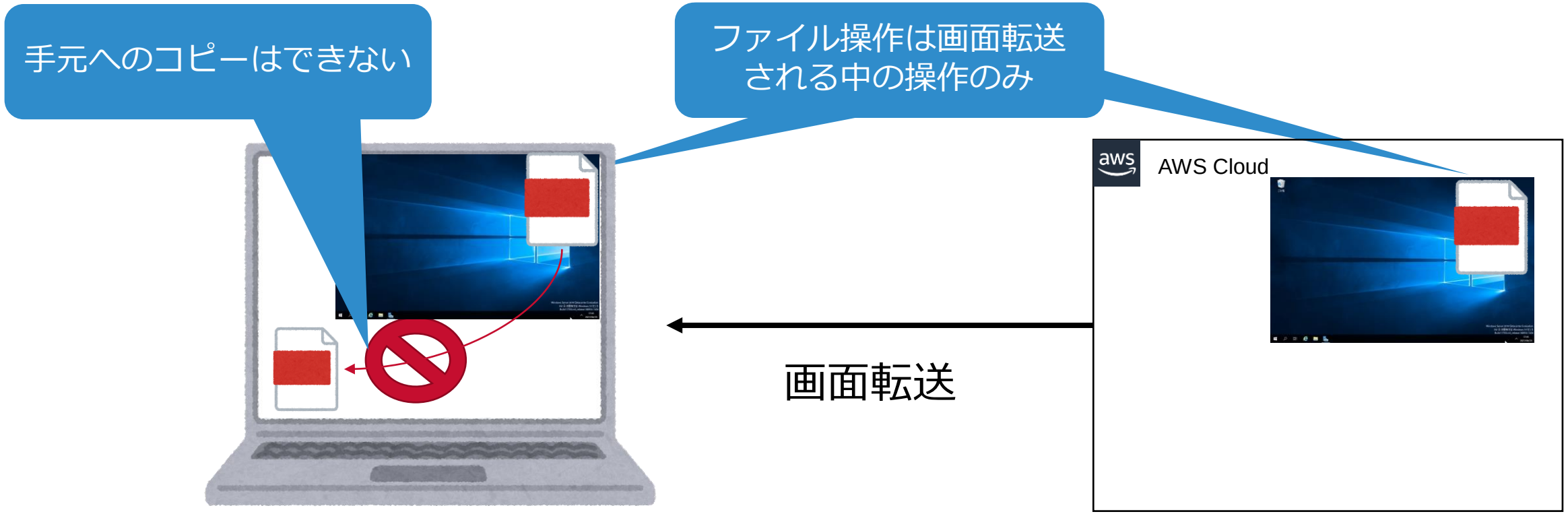
2. Amazon WorkSpaces

- 手元のクライアント上にデスクトップ画面を転送し、サーバー上のデスクトップを操作する
- 専用クライアントソフトウェア、もしくはブラウザでアクセスして利用する



2. Amazon WorkSpaces

- 手元のパソコンにデータが一切置かれず、デスクトップの情報はすべてサーバー側で管理される

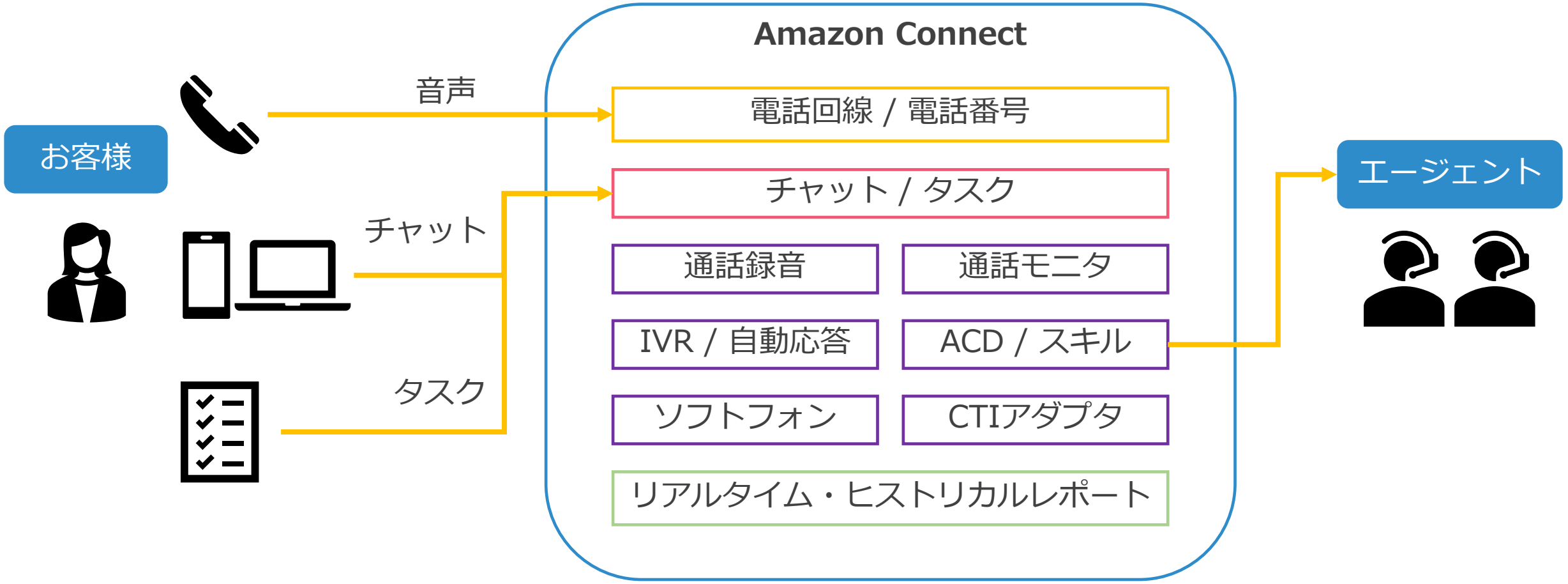


3. Amazon Connect

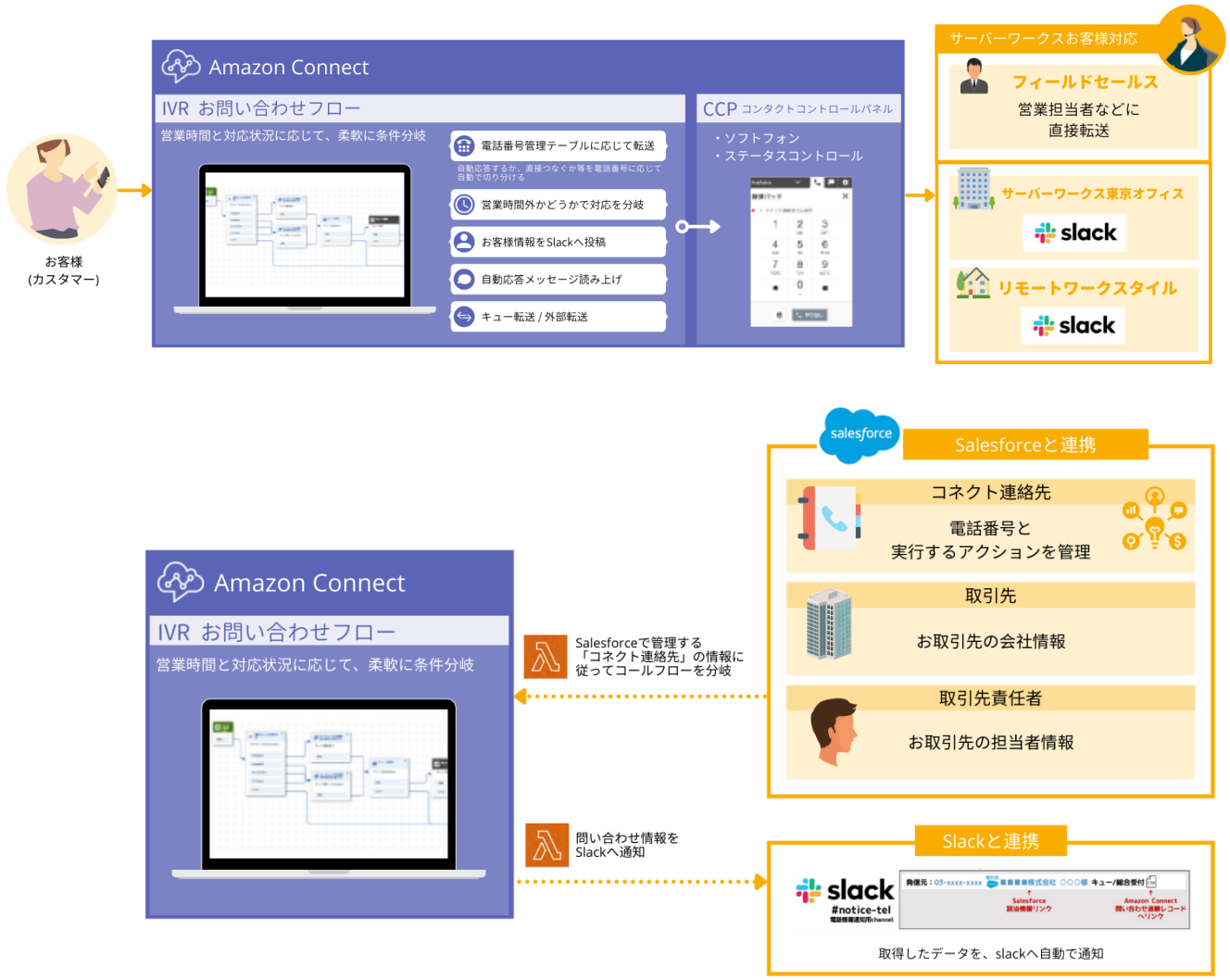
- AWS が提供する
  コンタクトセンターサービス

Amazon Connect

3. Amazon Connect



3. Amazon Connect



リモートワーク向け AWS サービスの概要 (まとめ)

1. AWS Client VPN
2. Amazon WorkSpaces
3. Amazon Connect

まとめ

まとめ

- AWS では多くのサービスが提供されており、すぐに利用することができる
- セキュリティ対策の AWS サービスを組み合わせて利用することができる
- 初期投資不要で従量課金のため、簡単に試すことができる


Serverworks