



# AWSセキュリティセンター

## 📖 日本語のホワイトペーパーもあり



[AWS Management Console](#)を利用する

[AWSアカウント](#)を作成する

▼ AWS

▼ 製品

▼ 開発者

▼ コミュニティ

▼ サポート

▼ アナリティクス

### その他

- [AWS IoT コミューニティセンター](#)
- [AWSセキュリティ証明書](#)
- [AWS多要素認証\(AWSMFA\)](#)
- [製品](#)
- [AWSソリューション](#)
- [導入事例](#)

## AWS セキュリティセンター

本ページには、以下のカテゴリの情報が含まれています。クリックして該当箇所にジャンプします。

↓ [概要](#)

↓ [参考資料](#)

↓ [認証と認定](#)

↓ [セキュリティ証明書](#)

### 概要

Amazon Web Services (AWS) は高可用性で信頼性や拡張性が高いクラウドコンピューティング プラットフォームを提供し、様々な種類のアプリケーションを構築することのできる柔軟性を提供します。徹底的なセキュリティとプライバシーを提供する。AWSは、セキュリティのベストプラクティスに沿ったサービスを構築し、これらのサービスで適切なセキュリティ機能を提供し、これらの機能を文書化します。また、AWS のお客様は、これらの機能とベストプラクティスを使用して、安全なアプリケーション環境を適切に設計できます。顧客がデータの匿名性、完全性、可用性を実現することは、信用や信頼性の維持と同様に、AWSIにとって最も重要な要素です。

当社は以下のアプローチを高いレベルで採用しながら、AWSインフラストラクチャの安全性を守っています。

# セキュリティは、AWSにおいて最重要項目

## 📦 セキュリティデザインに長年の経験

- Amazon.comで培った物理データセンター、ハードウェア、ネットワークの知識を適用
- 顧客の要望に応え、さらに改善を継続

## 📦 SAS-70 Type II、ISO 27001、PCI DSS Provider Level1、FISMA Moderate取得

## 📦 高いセキュリティという市場の評判

- AWSを調査したお客様はセキュリティの高さに驚かれる
- お客様がAWSを適用することで、セキュリティを向上するケースも多い

# 物理的セキュリティ

- Amazonは世界最大級のEコマースをセキュアに運営してきており、そのノウハウをAmazonクラウドに利用
- 厳格に管理された拠点
  - 侵入検出システム、監視カメラ
  - 物理的アクセスを厳格に管理
  - 多重認証を最低2回以上実施
- 従業員のアクセスレベルの管理
  - 必要に応じたときだけ最低限の権利を与える (least privilege)
- 全てのアクセスのログがとられ、レビューされる



# ストレージの破棄

## 📦 データ消去基準

- DoD 5220.22-M (“National Industrial Security Program Operating Manual”)
- NIST 800-88 (“Guidelines for Media Sanitization”)

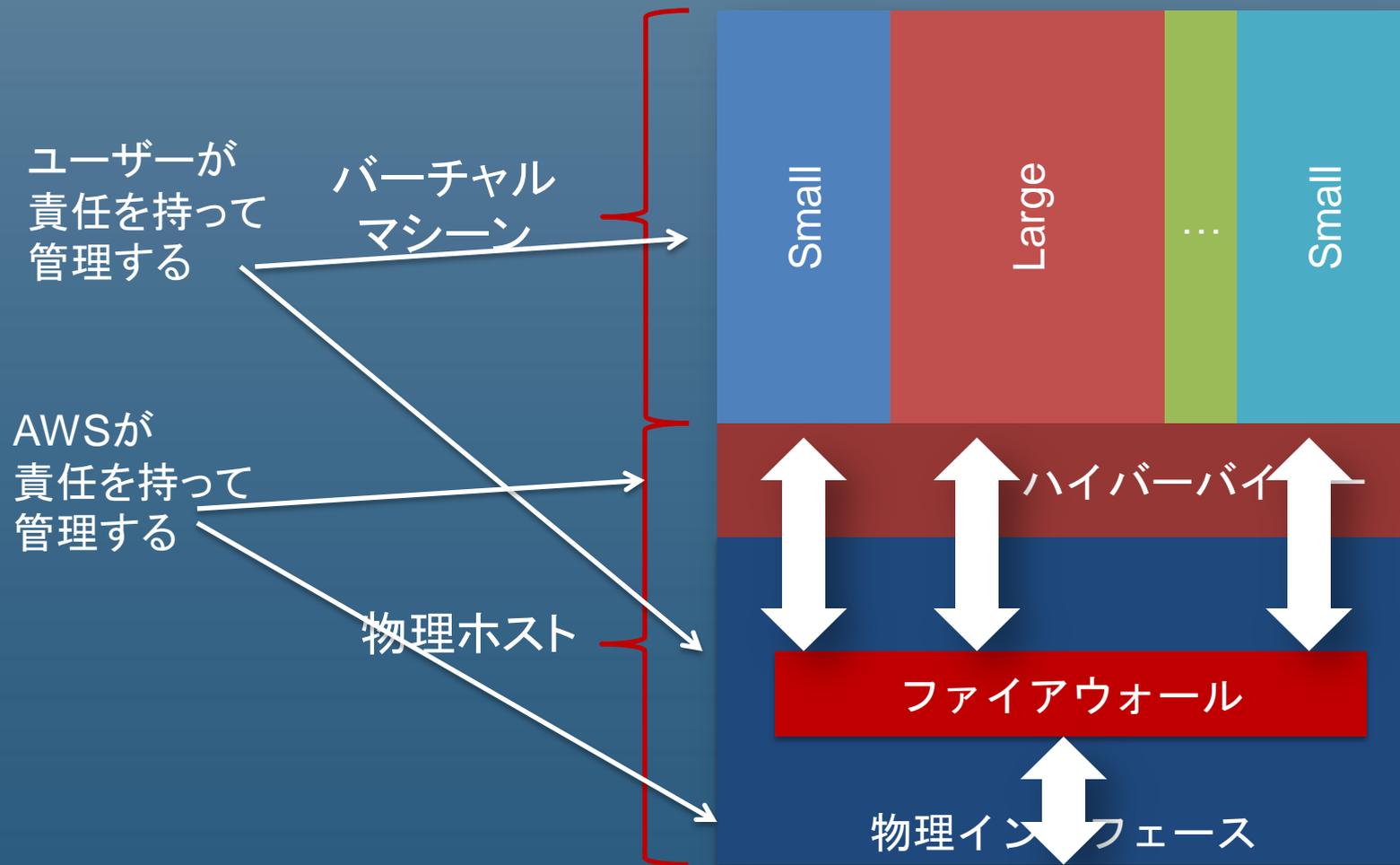
## 📦 物理的に故障した場合は、消磁および破壊

# AWSはセキュリティ対応を楽にする

- ❏ 責任共有モデルで、高い柔軟性と高いセキュリティを効率よく達成する
  - クラウド事業者は、セキュアなリソース(ミドルウェア、ホストOS、仮想レイヤー、物理環境)を責任をもって提供する
  - お客様は、ゲストOS、ミドルウェア、アプリケーションを責任をもって管理する

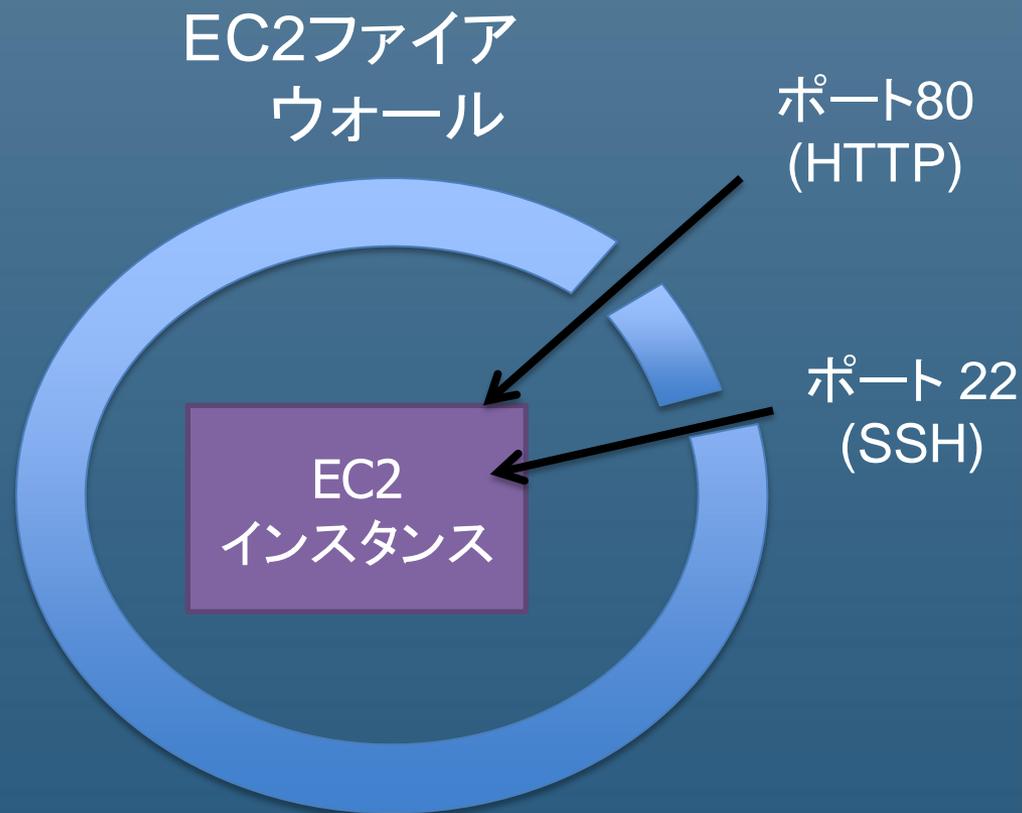


# 責任分担モデル



# 各インスタンスが、ファイアウォールを持つ

- デフォルトでは、全てのポートが閉じており、外からアクセスできない
- 必要なポートのみを、必要に応じて空ける



# Public EC2ネットワークの Securityパラメータ

- 📦 インバウンドのアクセスのみを制御する
- 📦 セキュリティグループにより、アクセスルールを設定する
- 📦 インスタンスの起動時に、グループをアサインする
- 📦 稼働中のインスタンスの既存グループは編集できる
- 📦 アクセスルール：
  - 名前
  - 説明
  - プロトコル
  - ポートレンジ
  - IPアドレスの範囲



# セキュリティ証明書

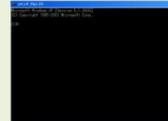
① EC2インスタンスへのアクセスは、キーペアの利用

② Webコンソールへのアクセス  
Webログイン / 多要素認証 / IAM

③ APIへのアクセス  
アクセスキー / X.509証明書 / IAM



Webコンソール



コマンドライン / SDK利用

API

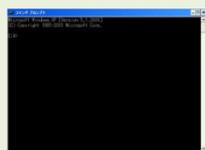
REST / SOAP

仮想サーバ(Amazon EC2)

Windows (スタンダード)



SSH公開鍵  
認証



ターミナル

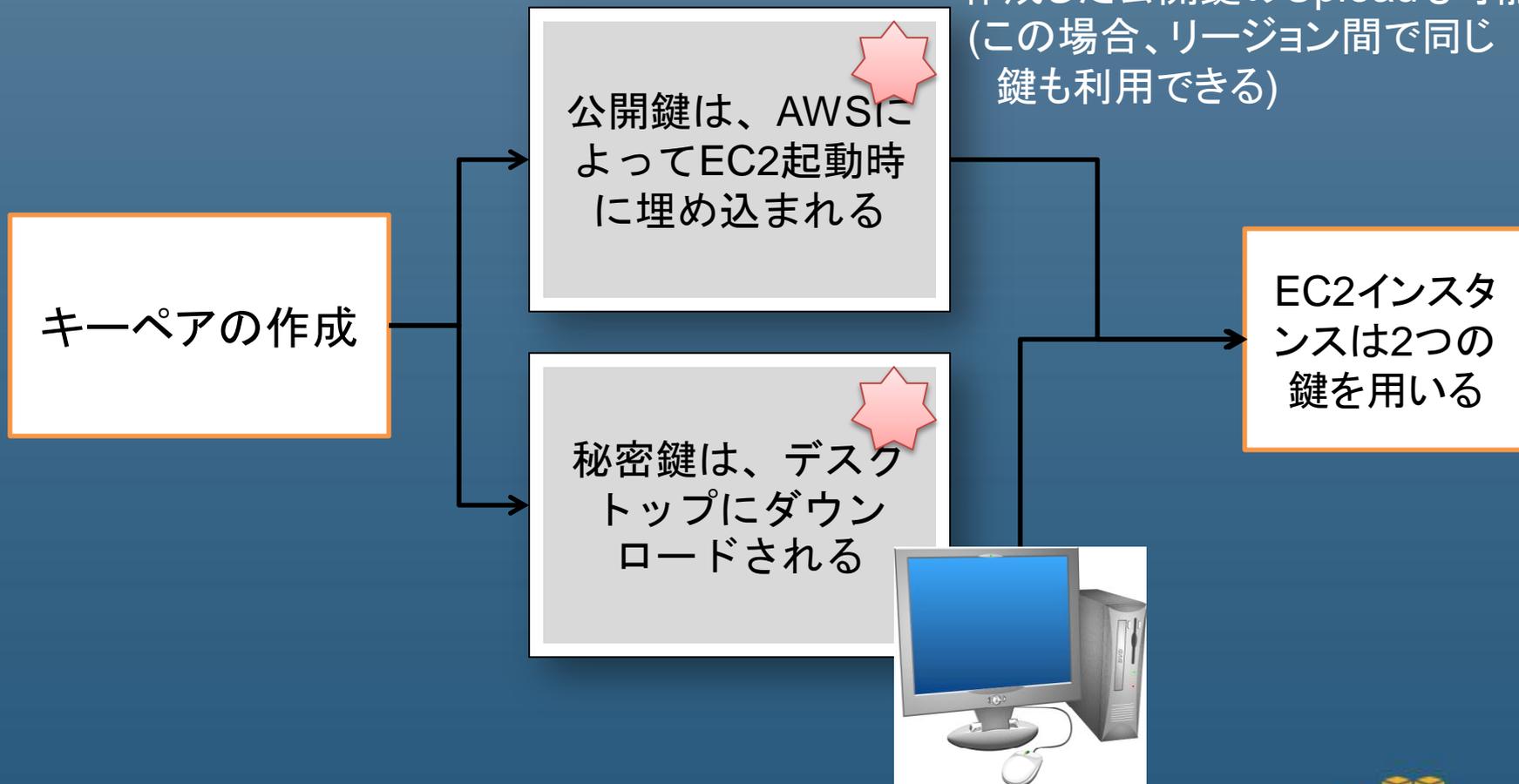


仮想デスクトップ



# EC2インスタンスへのアクセスには、キーペアが使われる

- ・公開鍵はリージョン毎に管理
- ・作成した公開鍵のUploadも可能  
(この場合、リージョン間で同じ鍵も利用できる)



# AWSのAPIへのアクセス

## AWSのWebの管理画面

Welcome, Jeff @ AWS | [Sign Out](#)

Your Web Services Account ▾

- AWS Account Activity
- AWS Access Identifiers
- Payment Method
- AWS Usage Reports
- Your AWS Profile
- 
- DevPay Activity

sender of a request to an A  
For services that require au  
quest, you must sign the rec  
pair of public / private Acce



## X.509 証明書

Your X.509 Certificate:

- Create New** Create a New X.509 Certificate
- Download** Download Your X.509 Certificate
- Upload** Upload Your Own X.509 Certificate
- Delete** Delete Your Current X.509 Certificate from AWS

## キーペア

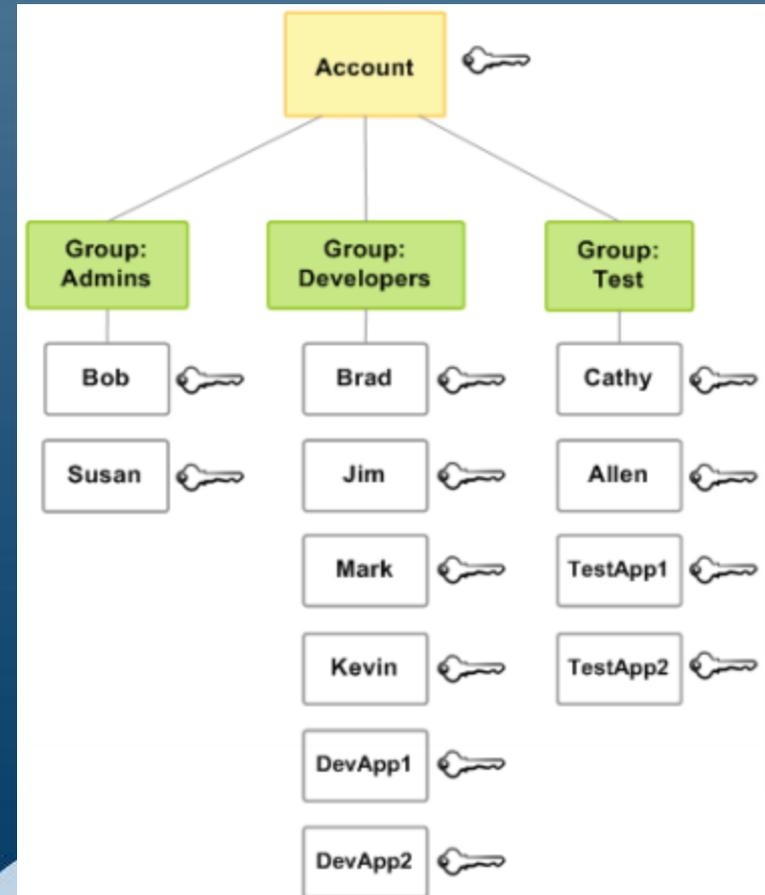
Your Access Key ID:  
~~AKIAI44QH8DHBEXAMPLE~~

Your Secret Access Key:  
~~WJALRQF354T920V0467UZ0B4H770XJZ3YV~~  
[Hide](#)

**Generate** **Generate a new Secret Access Key**  
(You will be asked to confirm this selection before a new Secret Access Key will be generated.)

# IAM – AWS Identity and Access Management

- ❏ アカウント内に、複数ユーザー、グループを作成し、適切なアクセス管理が可能
- ❏ 個別ユーザーが下記のセキュリティ要素をもてる
  - アクセスキー
  - ログイン/パスワード
  - MFAデバイスオプション
- ❏ 個別ユーザー、グループ毎にポリシーステートメントを作成
  - リソース、APIへのアクセスを適切に制限



# アカウントのセキュリティ



多要素認証デバイス  
オプション

アカウントのキーローテーション  
複数のキーペア、認証をサポート

# DDOSとその対策

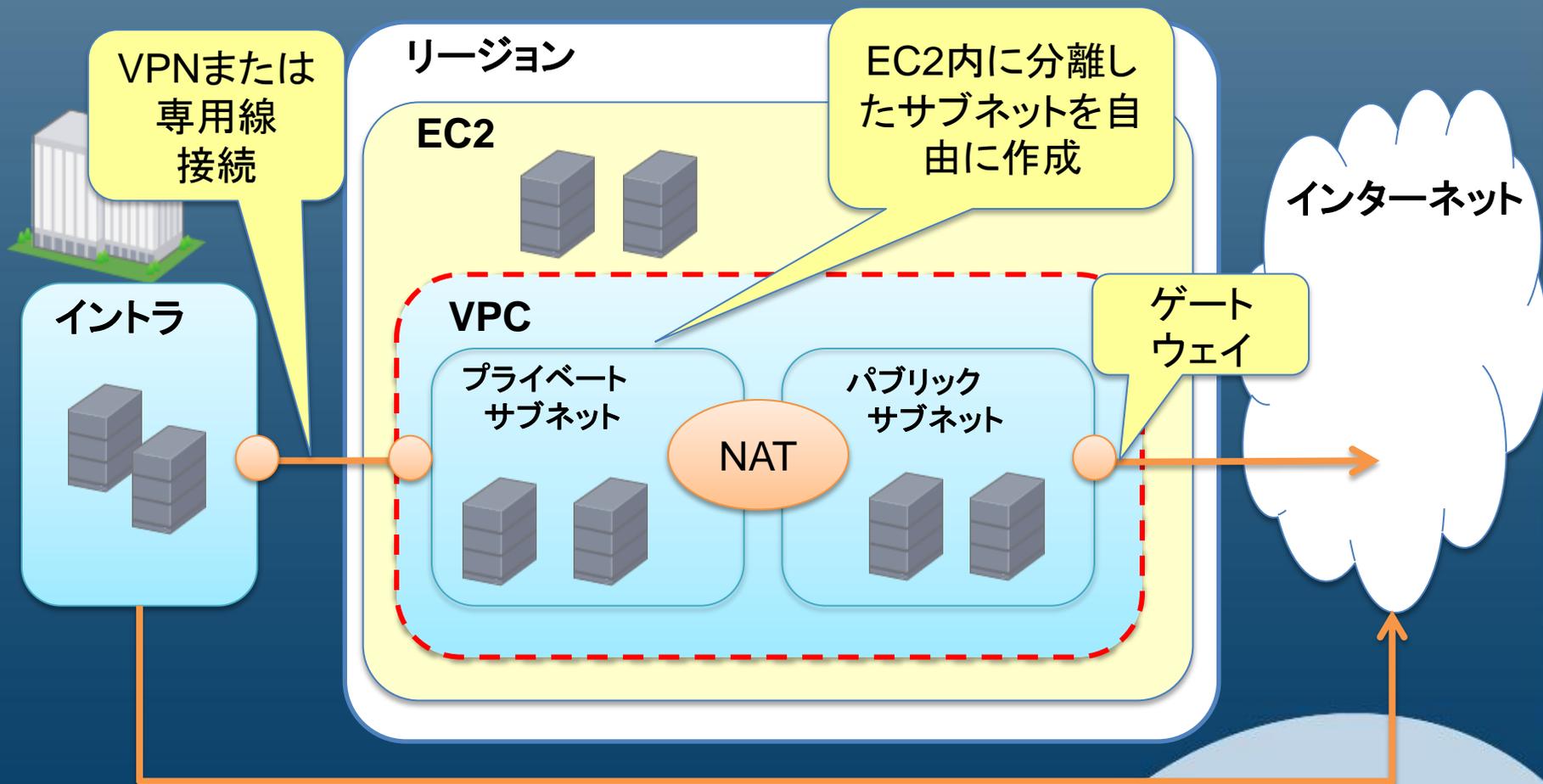
- 📦 AWSではDDOSの検出と対応をする専任のスタッフを持つ
- 📦 各拠点に複数のアクセスポイントを持つ
- 📦 発信元にならないようにする
  - EC2ではホストのファイアウォールで送信元IPアドレスの偽装が不可能
- 📦 カスタマは、IDS/IPSを動作させることができる
  - セキュリティグループによる分離
  - Snort:オープンソースで人気のある実装
  - 商用(SourceFire, Trend Micro, Symantecなど)もあり

# Amazon Virtual Private Cloud (Amazon VPC)

# Amazon VPCとは

- ❏ AWSクラウド上にプライベートクラウドを構築
- ❏ オンプレミスとのハイブリッドが簡単に実現
  - AWSが社内インフラの一部に見える
  - 社内システム、ソフトウェアの移行がより容易に
  - 例：業務システム、バッチ処理、ファイルサーバ
- ❏ 2011年8月から全リージョンで利用可能に
- ❏ 専用線接続(AWS DirectConnectも)

# お客様のインフラをAWS上に延長する

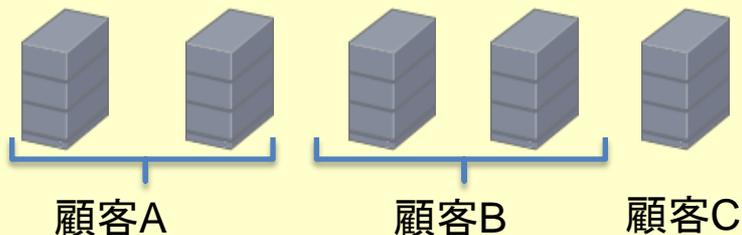


# EC2 Dedicated Instance

- ❏ VPC内で専用インスタンス
  - ❏ シングルテナント保証
- ❏ クラウドのメリット確保
  - ❏ 従量課金
  - ❏ 柔軟にスケールアップ
  - ❏ 瞬時に調達
- ❏ 規制に対応しなければいけないお客様のご要望に応えるサービス

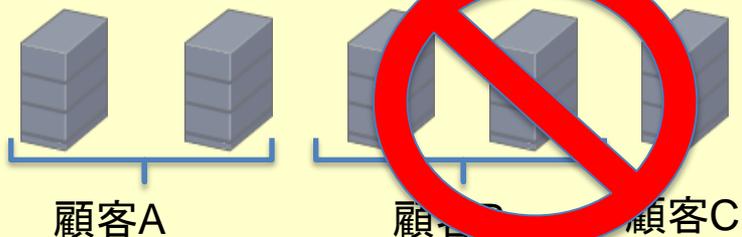
## 通常のEC2

### 物理サーバー

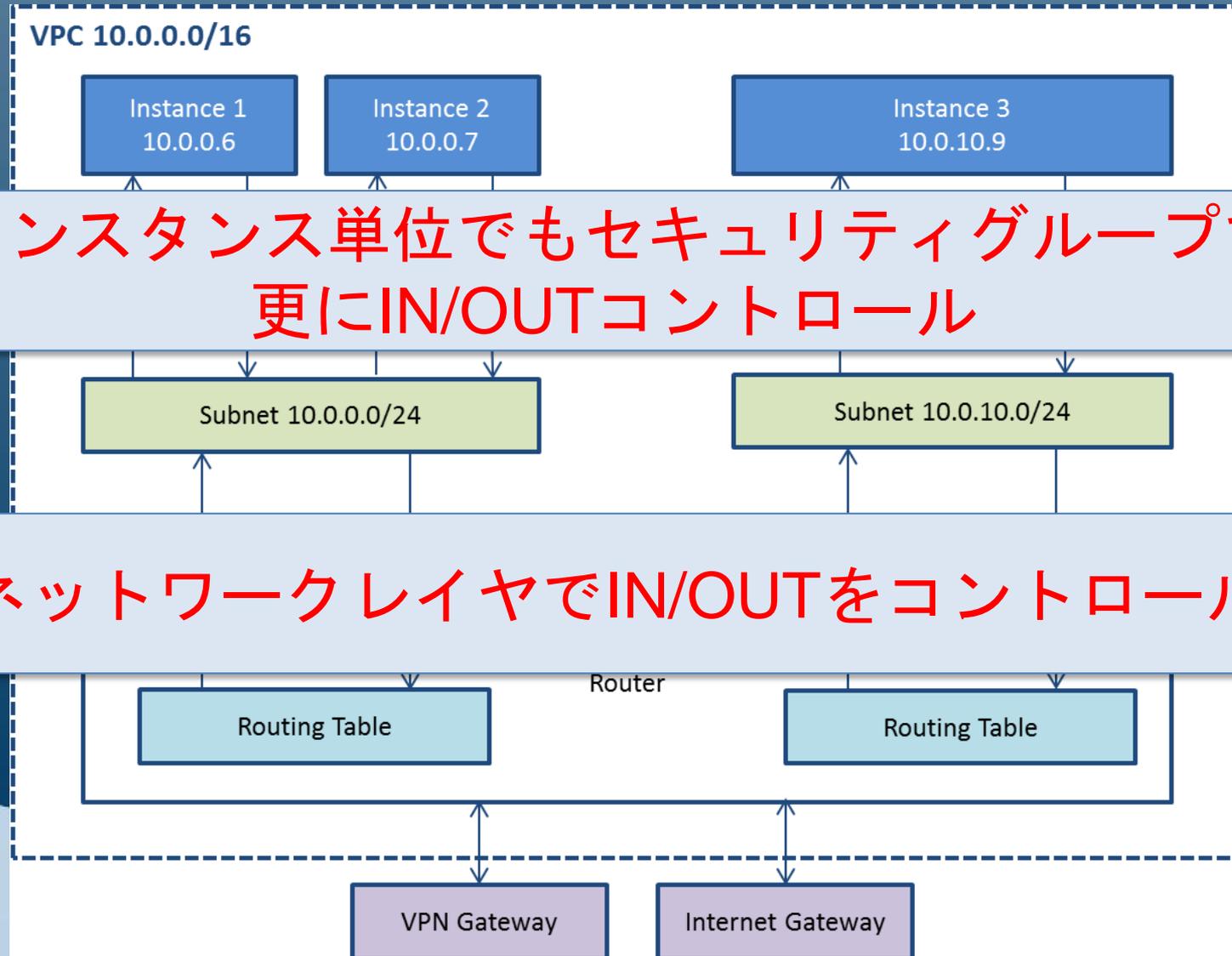


## Dedicated Instance

### 物理サーバー



# パケットの出入り管理

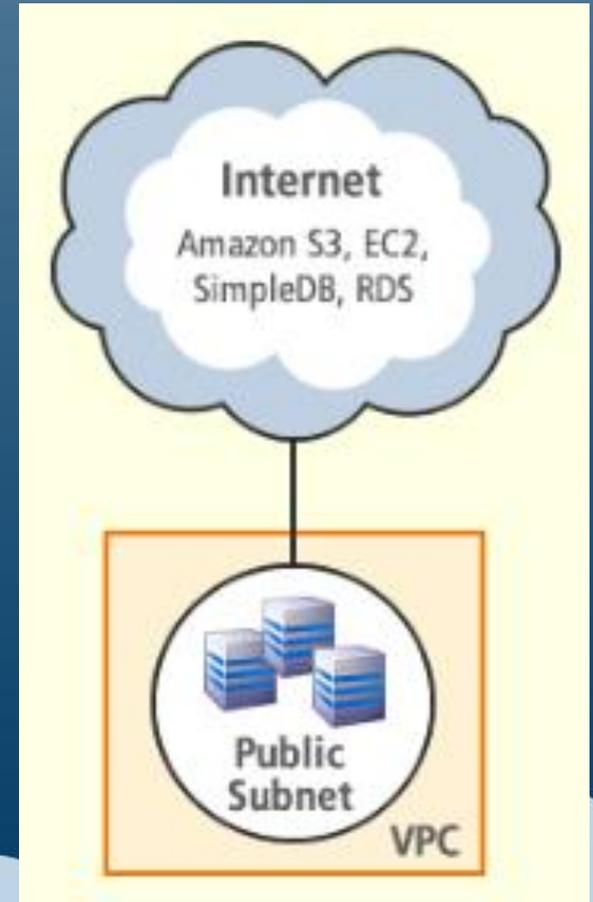


インスタンス単位でもセキュリティグループで  
更にIN/OUTコントロール

ネットワークレイヤでIN/OUTをコントロール

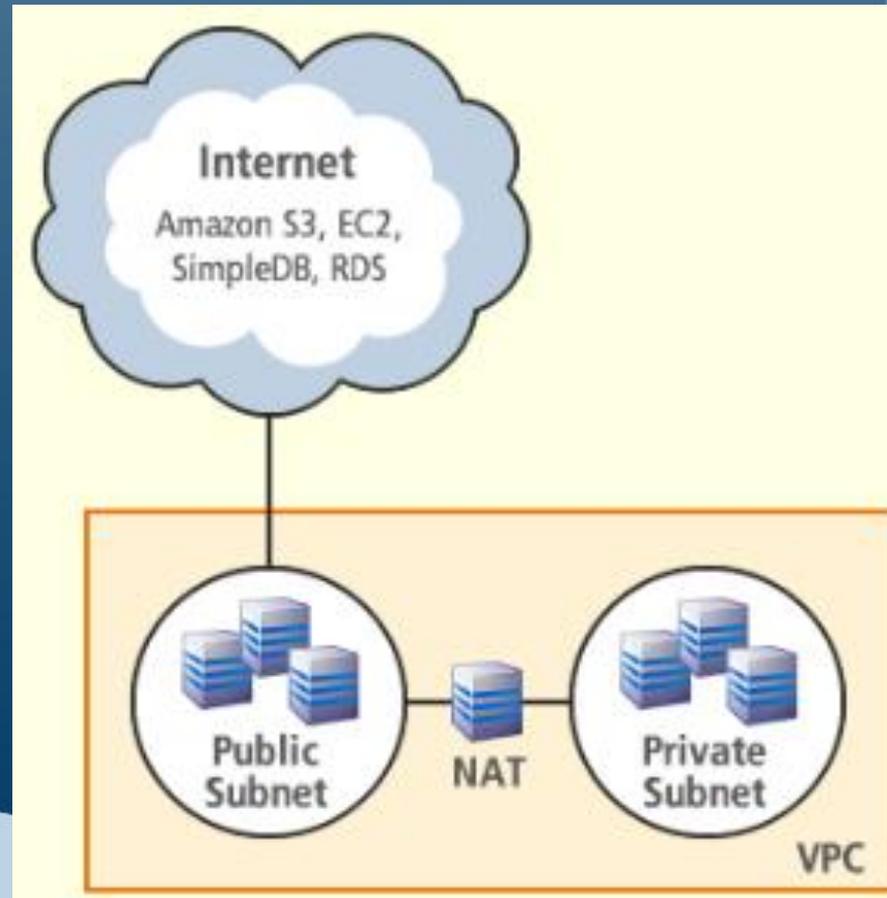
# VPC with a Single Public Subnet

- ❏ EIPアドレスをパブリックインタフェースにアサイン
- ❏ 適用メリット
  - 高いセキュリティの中でWebアプリを稼働させる
  - プライベートIPを用いて、インスタンスをまとめられる



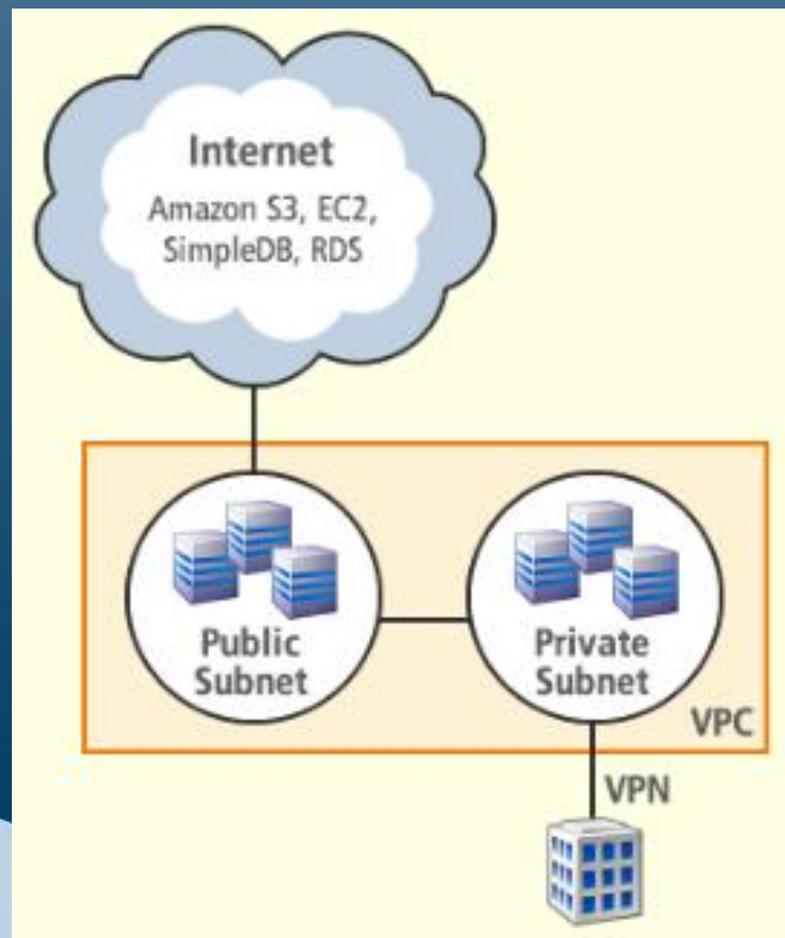
# VPC with Public and Private Subnets

- ❏ パブリックサブネットのインスタンスには、EIPをアサインできる
- ❏ プライベートサブネットのインスタンスはインターネットから直接アクセスできない
- ❏ 適用メリット
  - Webサーバーをパブリックサブネットを稼働し、プライベートサブネット内のデータベースの読み書きを行う



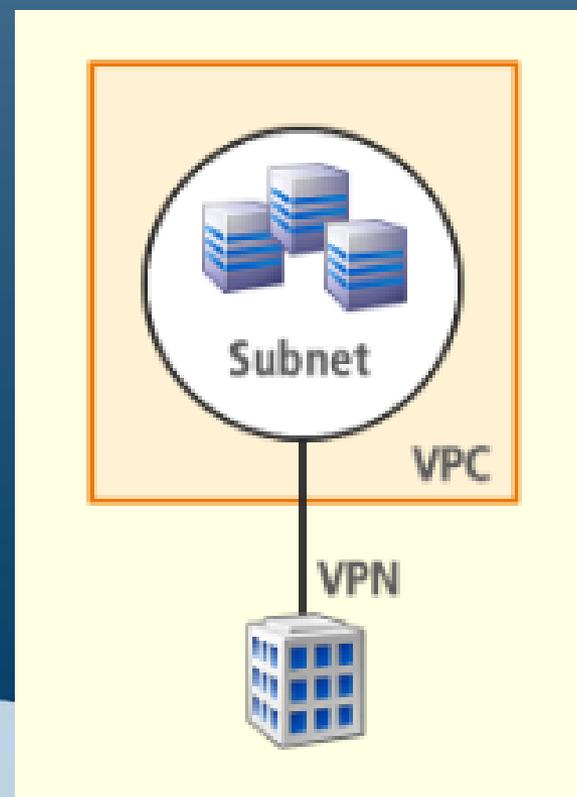
# VPC with Public and Private Subnets and a VPN Connection

- パブリックサブネットのインスタンスには、EIPをアサインできる
- プライベートサブネットのインスタンスにVPN経由でアクセス可能
- 適用メリット
  - VPCをインターネットに接続しつつ、データセンターをクラウド上に拡張



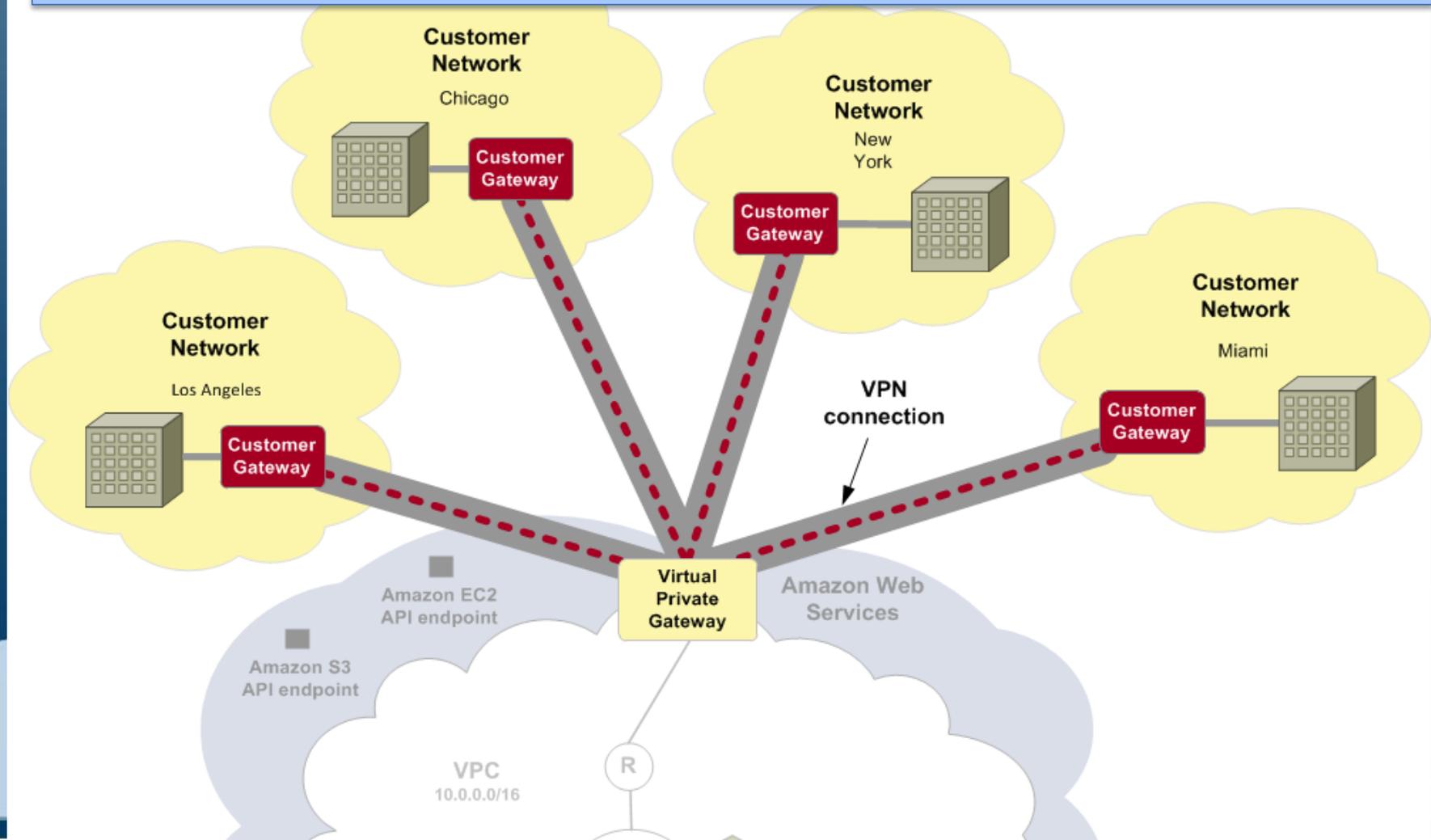
# VPC a Private Subnet and a VPN Connection

- ❏ VPC登場時はこの形態のみだった
- ❏ 全てのトラフィックは社内データセンターのファイアウォール経由で行われる
- ❏ 適用メリット
  - データセンターをクラウドに拡張しても、中央集権的管理を維持する



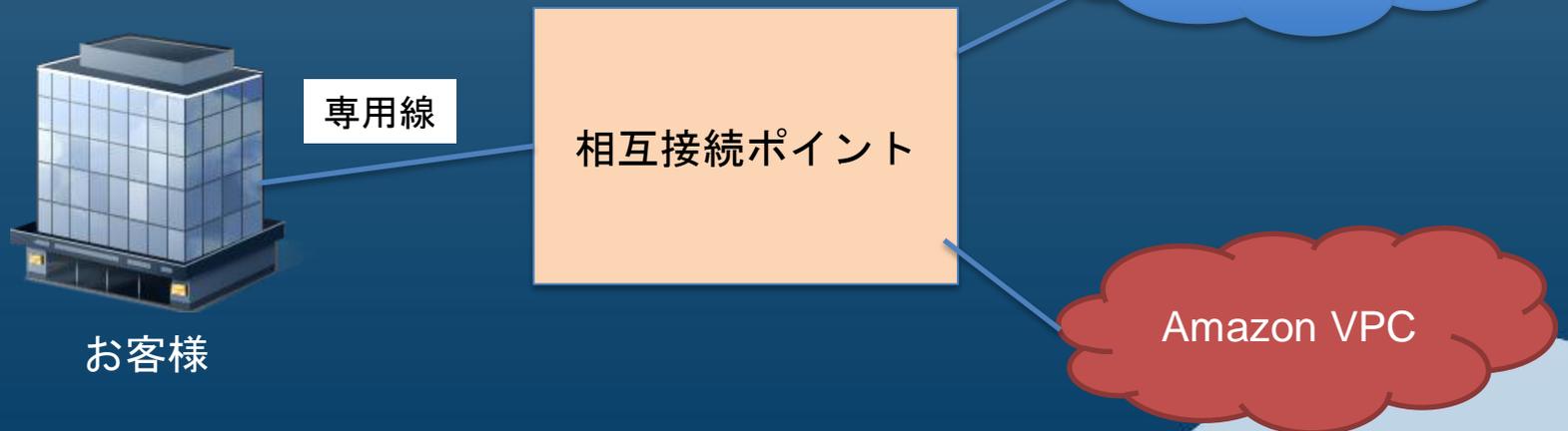
# マルチホーム(cloudhub)

[http://docs.amazonwebservices.com/AmazonVPC/latest/UserGuide/index.html?VPN\\_CloudHub.html](http://docs.amazonwebservices.com/AmazonVPC/latest/UserGuide/index.html?VPN_CloudHub.html)

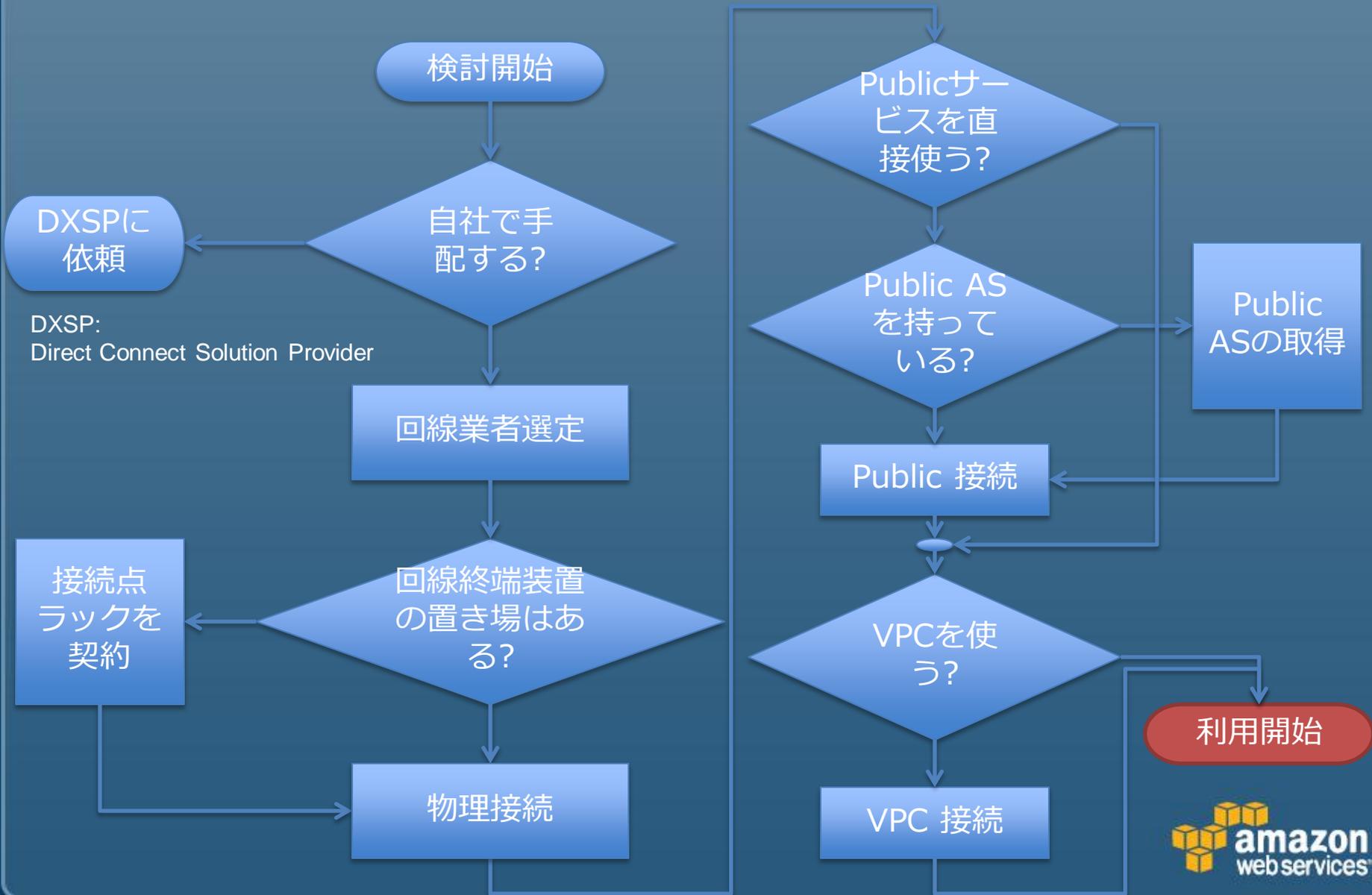


# AWS Direct Connectとは

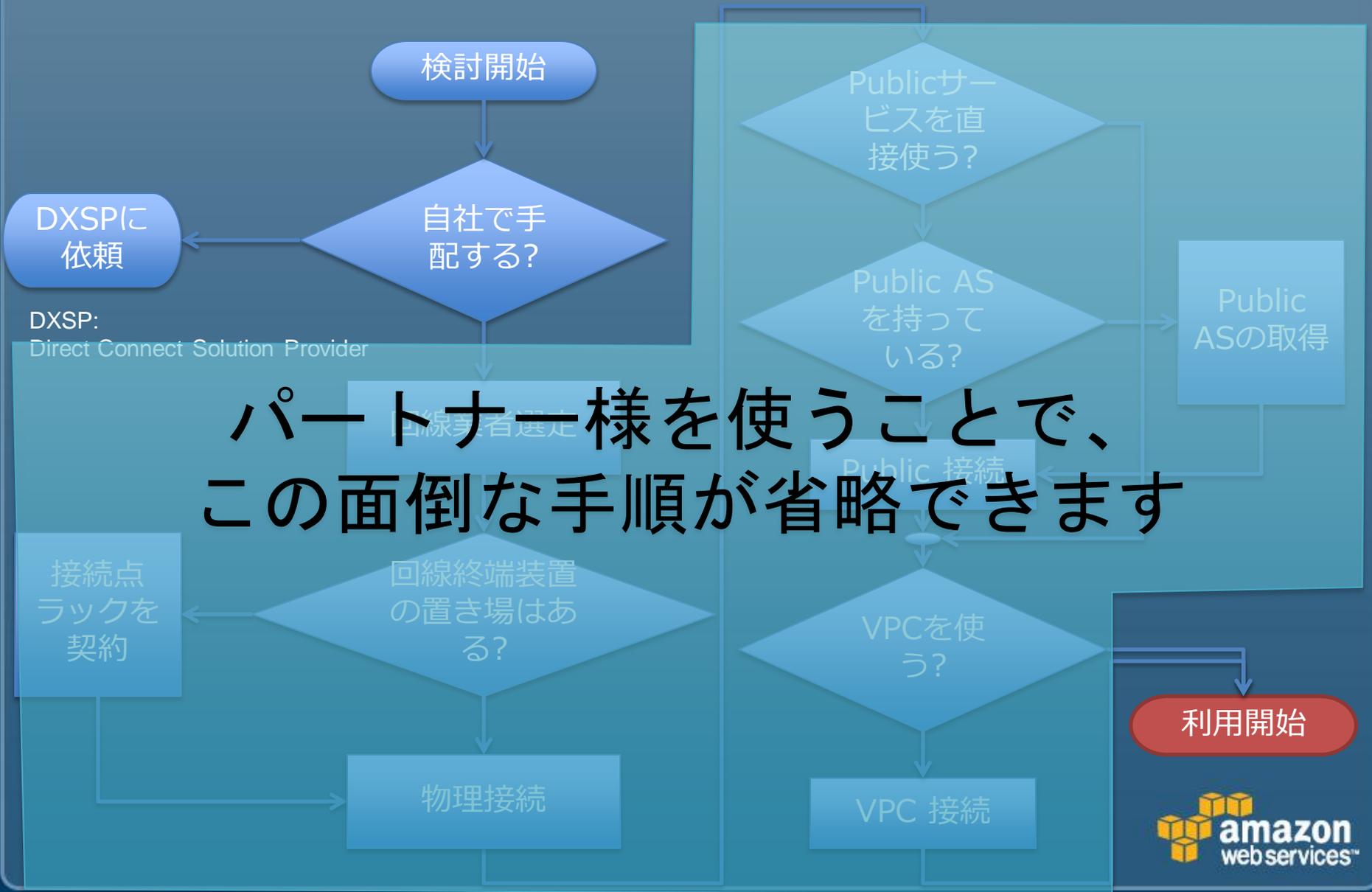
- ❏ AWSとデータセンター、オフィス、コロケーション環境間にプライベート接続を確立するサービス
- ❏ 高スループット、低レイテンシ
- ❏ 一貫性のあるネットワーク体験!



# AWS DirectConnect 接続のステップ



# AWS DirectConnect 接続のステップ



パートナ一様を使うことで、この面倒な手順が省略できます

# Amazon VPCをどう考えるか

- これからの標準になるもの
- ネットワークを仮想化するもの
- ネットワークにまつわる多くの要望への答え
  - IPアドレスの固定
  - サブネットを使った管理
  - 専用線でつながったセキュアな環境

# AWSでのセキュリティのために

## 📦 適切なアーキテクチャ

## 📦 共有責任を理解する

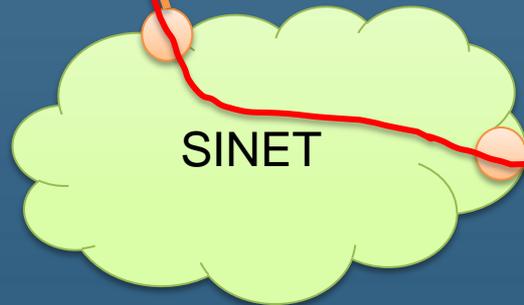
- AWSはできる範囲に注力
- 取扱者はできる範囲に注力する
- 協働する

## 📦 運用

- 「どのように」「継続して」日々運用するかを考えた設計

# AWS Direct Connectで、 SINETとAWSクラウドを直結（調整中）

加入機関A



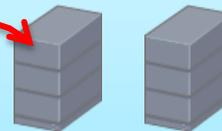
専用線  
接続

AWSの東京リージョン

EC2(仮想サーバー)

VPC

プライベート  
サブネット



 Question?

[aws.amazon.com](https://aws.amazon.com)

# Amazon EC2のセキュリティ

## 📦 ゲストOS

- 顧客がルートレベルで管理する
- AWSのアドミニストレーターでもログインできない
- ユーザーが独自にキーペアを作成可能

## 📦 ホストOS

- 全てのアクセスのログを取得し、監査する
- 必要なときにだけ最低限のレベルでAWS管理者にアクセス権を与える
- ホストOSへのアクセスは必ずSSHが使われる

## 📦 Statefull Firewall

- デフォルトで全てのインバウンドをはじく
- 顧客が必要なポートだけを空ける

## 📦 暗号化されたAPIコール

- X.509 証明書もしくは、AWSアカウントのキーペアが必要

# 仮想メモリとローカルディスク

- Amazonのディスク管理システムは、他のインスタンスの仮想メモリ&ディスクを読めないようにしている(特許技術)
- もちろん、顧客は独自に、データを暗号化することも可能



Amazon EC2  
Instances



Encrypted  
File System

Encrypted  
Swap File

Amazon EC2  
Instance

# Amazon EC2 インスタンスの分離

