

# AWSにフィットする 最適なセキュリティ対策とその考え方

トレンドマイクロ株式会社  
パートナービジネスSE部  
シニアエンジニア 姜(かん) 貴日



# Agenda

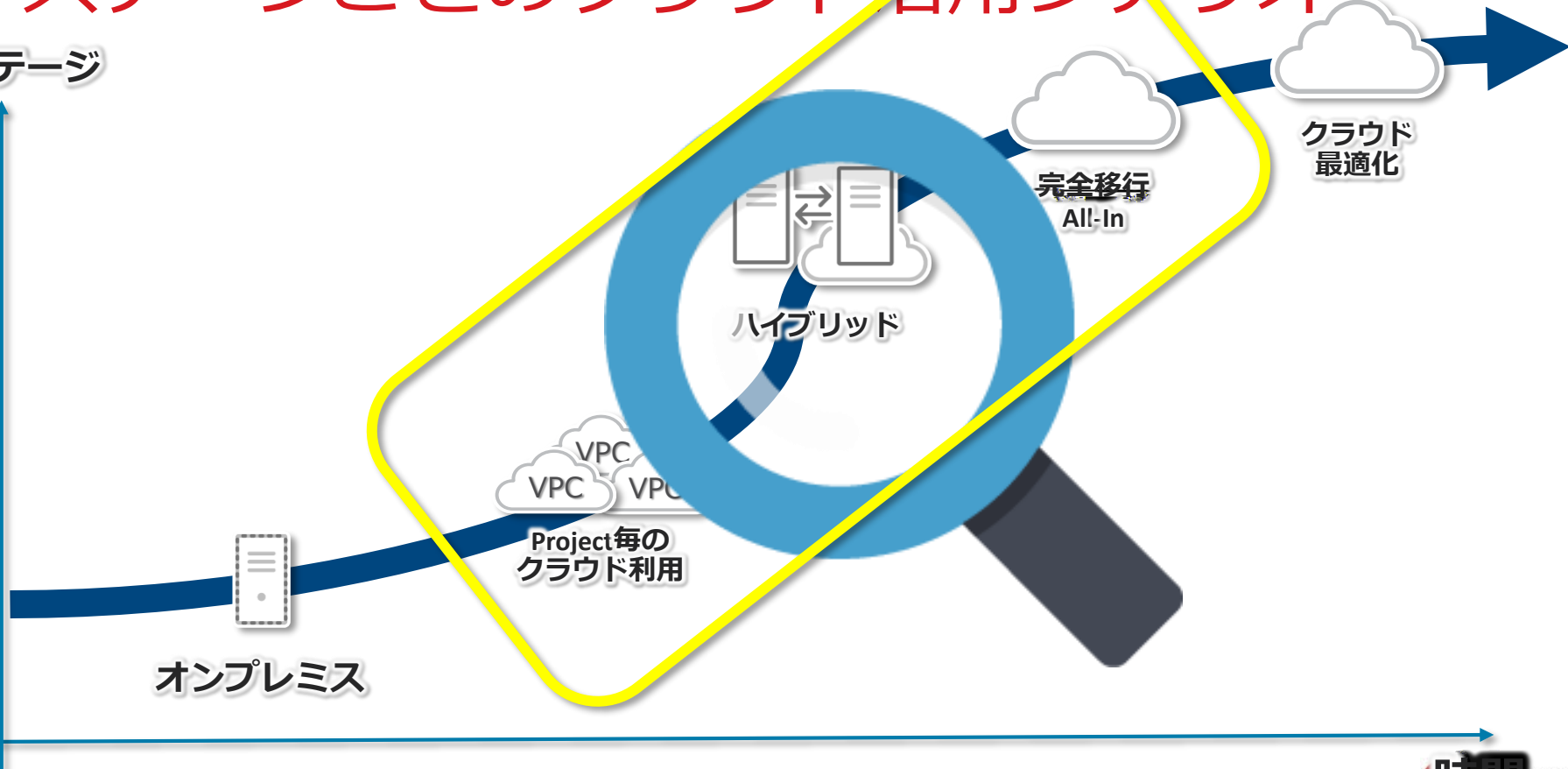
1. ステージごとのクラウド活用シナリオ
2. AWS環境でのセキュリティ対策
3. ステージごとのセキュリティポイント
4. Deep Securityと実現するクラウドジャーニー

# ステージごとのクラウド活用シナリオ

---

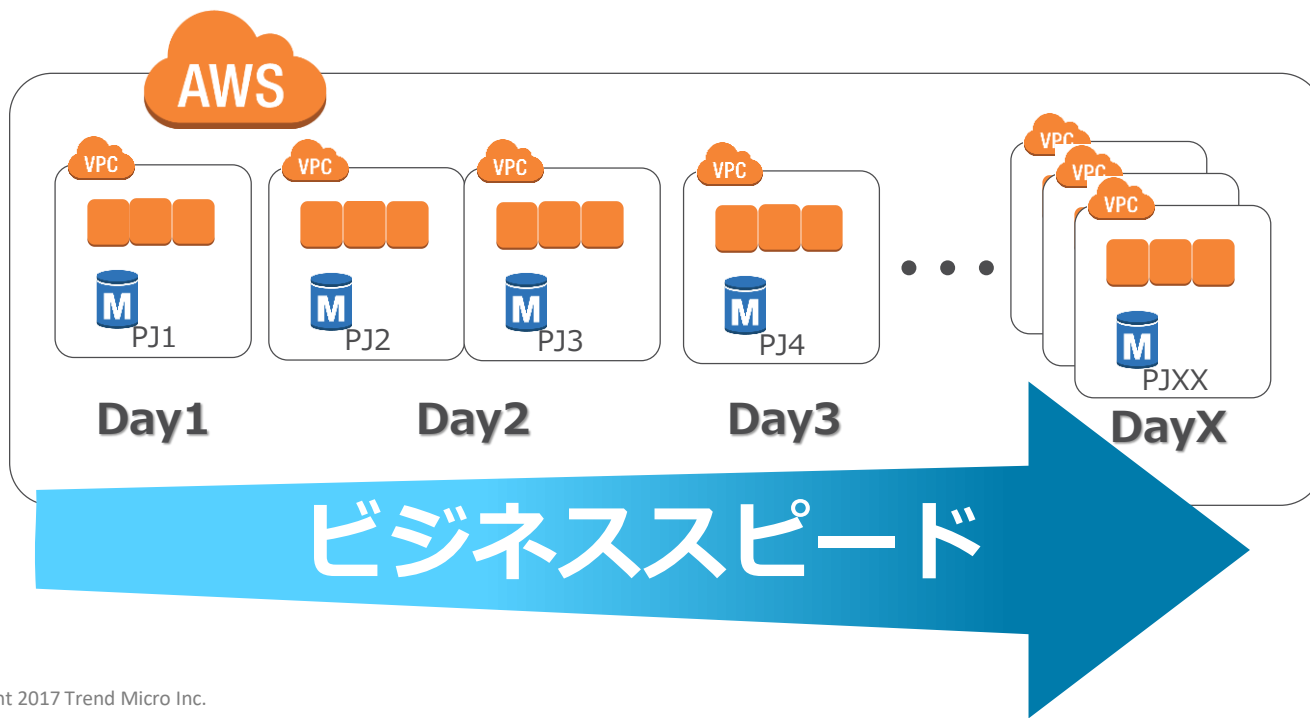
# ステージごとのクラウド活用シナリオ

ステージ



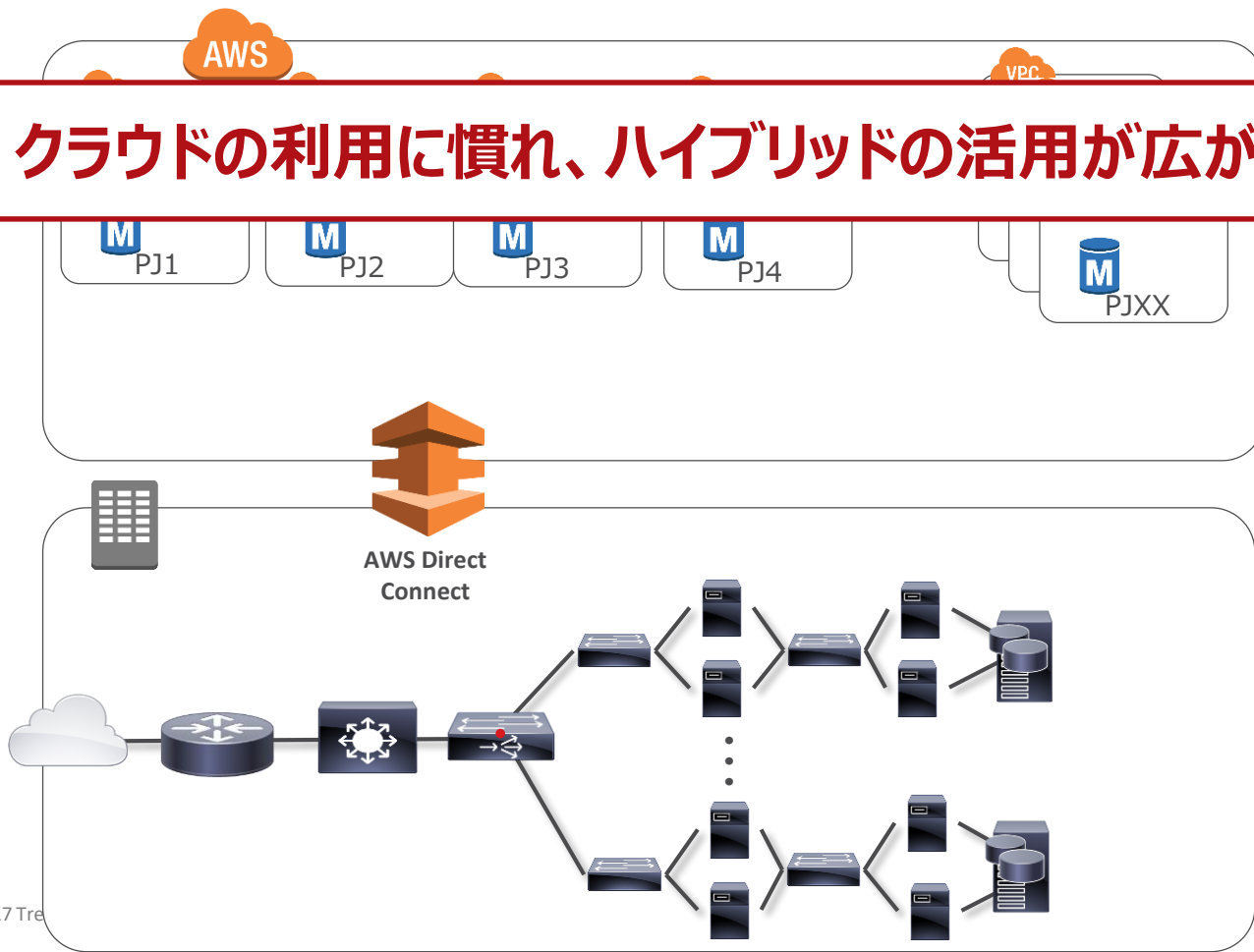
# プロジェクトごとのクラウド利用

スモールスタートでスピーディーにクラウドを使い始める



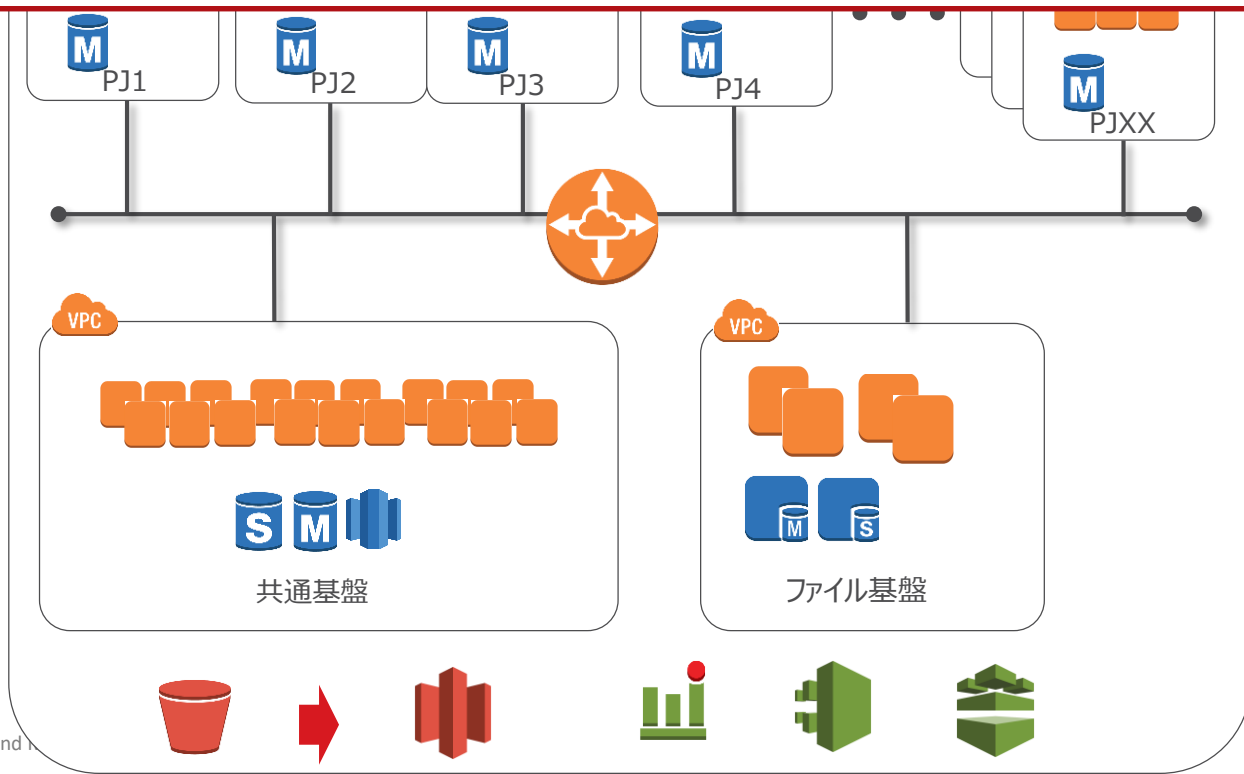
# ハイブリッドクラウド

クラウドの利用に慣れ、ハイブリッドの活用が広がる



# 完全移行 - All-In -

システムを全て移行し、クラウド最適化が始まる



# AWS環境でのセキュリティ対策

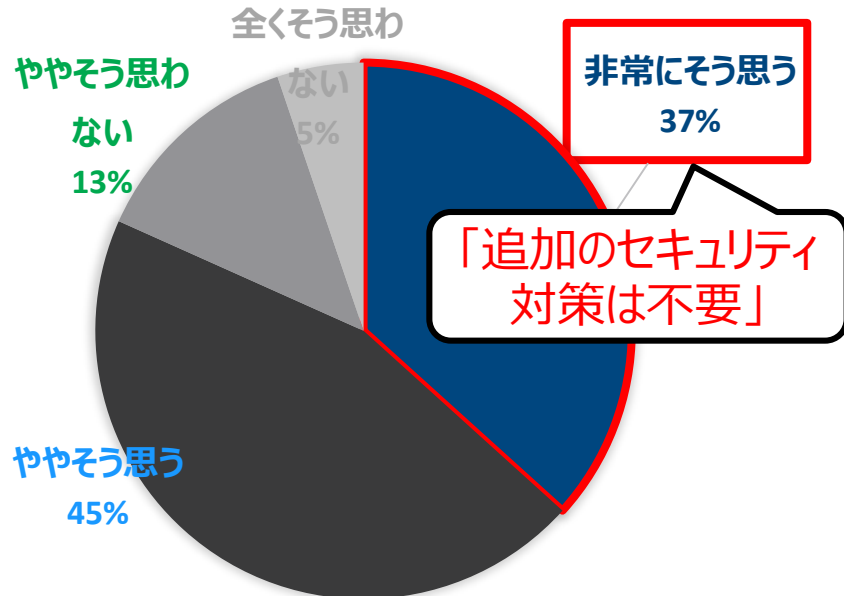
---



# AWS環境のセキュリティ実態調査

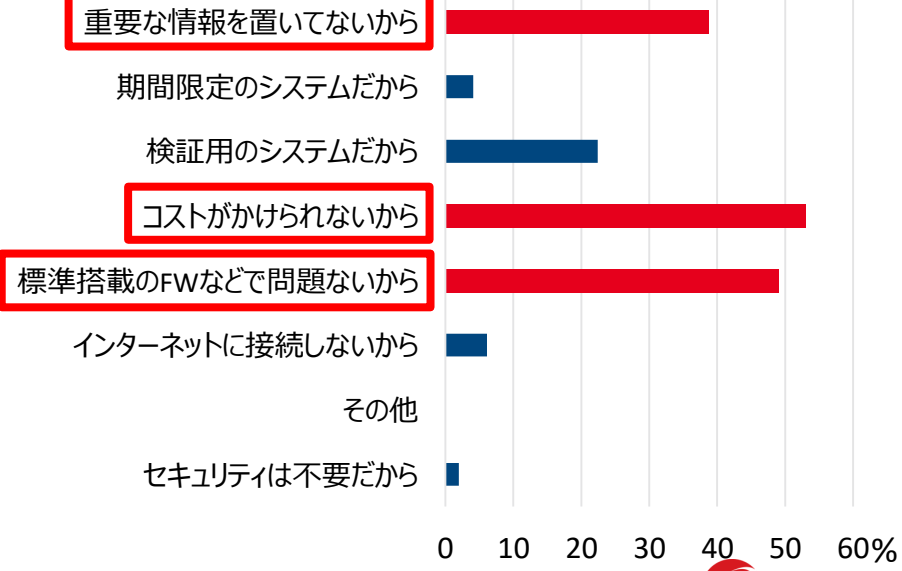
## 質問1

セキュリティは、AWSが標準提供しているセキュリティ機能だけで十分？



## 質問2

追加でセキュリティ対策を実施されていない理由は？



# AWSにおけるIaaS責任共有モデル

お客様

クラウド "内の"  
セキュリティに  
責任がある

お客様のデータ

プラットフォーム、アプリケーション、Identity & Access Management (IAM)

オペレーティングシステム、ネットワーク、ファイアウォール構成

クライアント側のデータ  
暗号化とデータ  
整合性の認証

サーバー側の暗号化  
(ファイルシステムまたはデータ  
(またはその両方))

ネットワークトラフィックの保護  
(暗号化/整合性/アイデンティティ)

お客様の責任範囲



お客様責任範囲の  
セキュリティ対策をお手伝い

AWS

クラウド "の"  
セキュリティに  
責任がある

コンピューティング

ストレージ

データベース

ネットワーキング

AWS グローバル  
インフラストラクチャ

リージョン

アベイラビリティゾーン

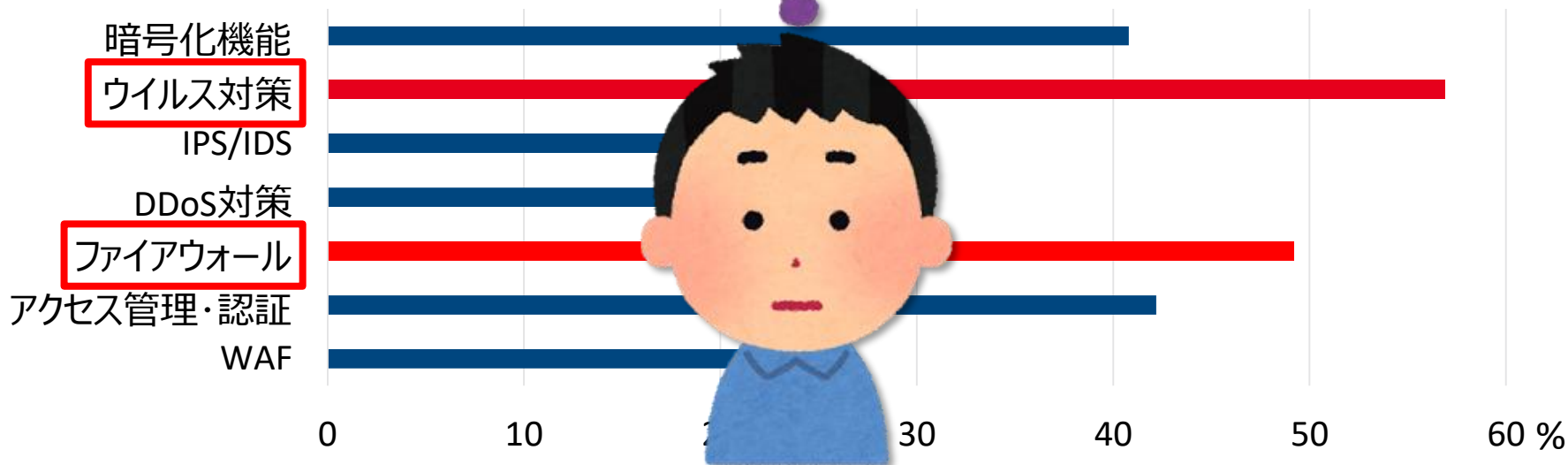
エッジ  
ロケーション

AWSの責任範囲



# AWSに追加導入しているセキュリティ対策は？

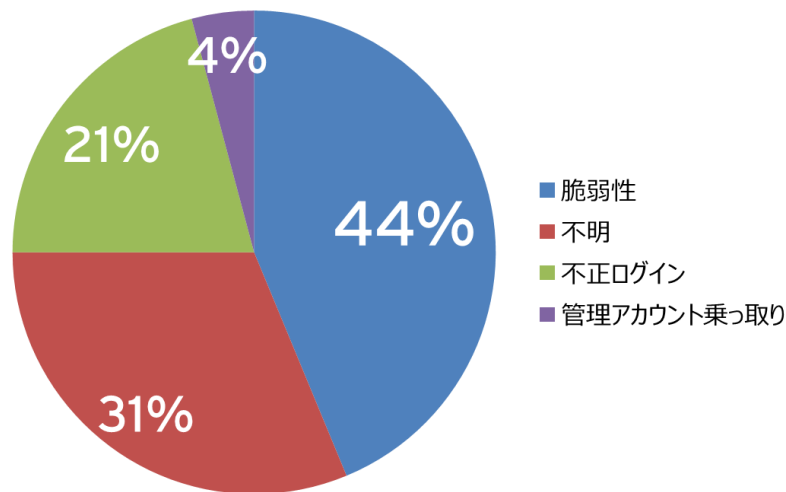
追加でセキュリティ対策をしている場合、どのセキュリティ機能を追加導入している？



ウイルス対策とファイアウォールで「脅威」に対応できる？

# 相次ぐ公開サーバからの情報漏えい

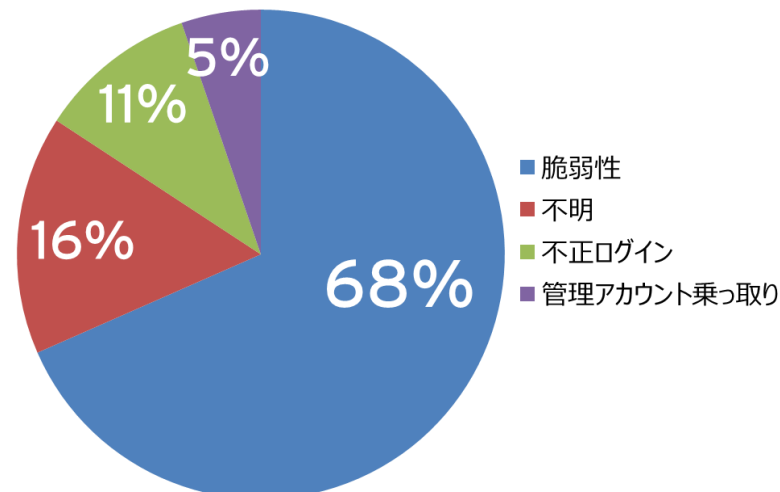
2016年 情報漏えいの原因割合



2016年1月から12月までに報道された事例をトレンドマイクロで独自に整理

**脆弱性**を狙われた  
被害が44%

2017年 情報漏えいの原因割合



2017年1月から3月までに報道された事例をトレンドマイクロで独自に整理

**脆弱性**を狙われた  
被害が68%

# 2017年 発覚した深刻な脆弱性

- 3月に脆弱性が発覚 **Apache Struts2**
  - 攻撃者はリクエストを送信することで、**サーバ上で任意のコードが実行**可能となる
- 主な被害事例

業種	漏えいした情報の種類	漏えいした件数
メディア	個人情報	約 <b>5万7,000</b> 件
ITサービス	個人情報、カード情報	合計 約 <b>72万6,000</b> 件
小売	個人情報、メールアドレス	個人情報 約 <b>75万</b> 件 メールアドレス 約 <b>43万9,000</b> 件

**AWSをもっと安全に使うために、サーバには脆弱性対策を！**

# AWS利用時のセキュリティポイント

## 1. AWSにおけるセキュリティは「責任共有モデル」

- AWSユーザにもセキュリティ対策をする必要がある
- OSやミドルウェア、アプリケーションなど……

## 2. 最近の脅威から考える、AWSセキュリティの要は「脆弱性対策」

- ここ数年、相次ぐ情報漏えい
- ウイルス対策、ファイアウォールでは防ぎきれない

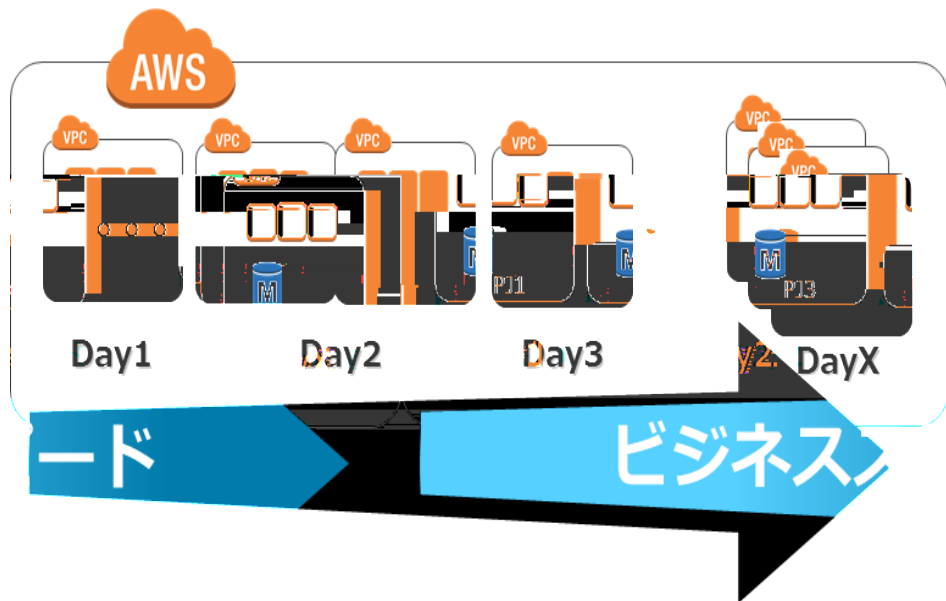
## 3. クラウドの利用ステージによって他に考慮すべきポイントは異なる

- プロジェクト毎の利用 or ハイブリッドクラウド環境 or 完全移行

# ステージごとのセキュリティポイント

---

# プロジェクトごとのクラウド利用



## セキュリティに求む

### ビジネス変化への追従

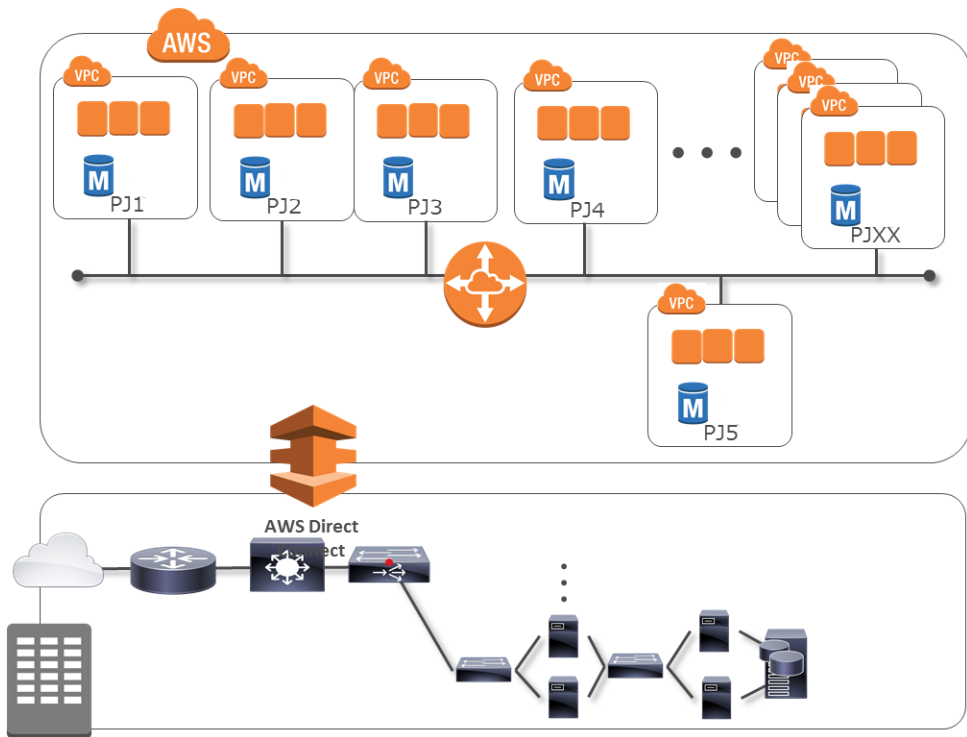
導入効率

自動化

ビジネス  
スピード



# ハイブリッドクラウド



## セキュリティに求む

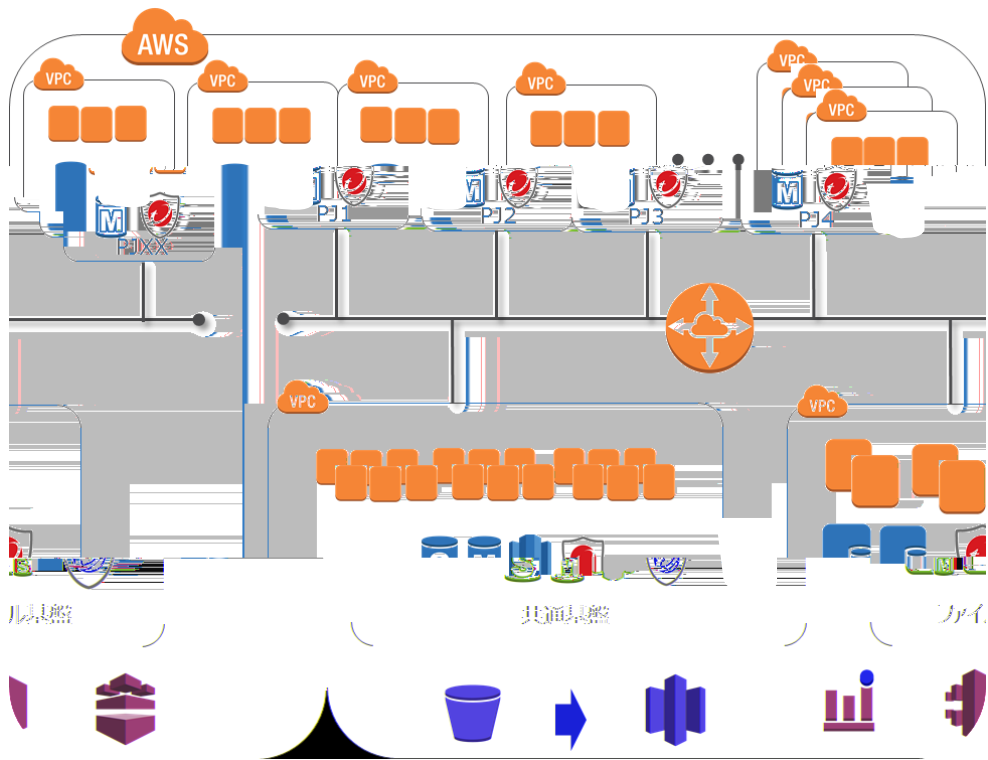
可視化

マルチ  
プラット  
フォーム

統合管理

ガバナンス

# 完全移行 - All-In -



セキュリティに求む

運用の柔軟性

サービス  
個々のニーズ

自社標準  
セキュリティ

柔軟性

# ステージごとのセキュリティポイント

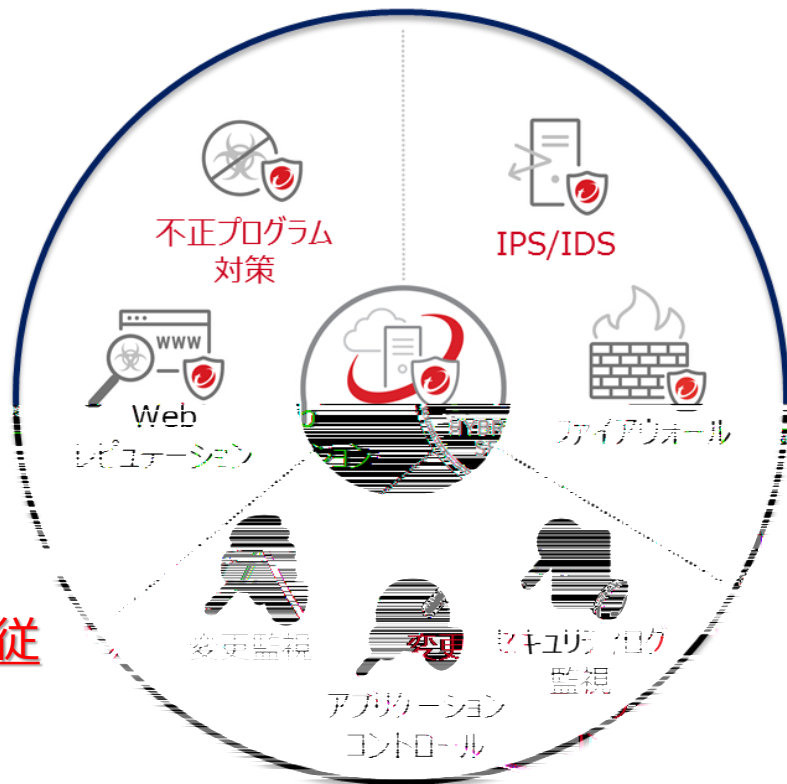
1. プロジェクトごとのクラウド利用に求めるのは「スピード」
  - 導入の効率化
  - 運用の自動化
2. ハイブリッド環境では「可視化」が重要
  - マルチプラットフォーム対応
  - 統合管理に対応
3. 「運用の柔軟性」が完全移行(All-In) 環境には求められる
  - サービス個々のニーズに応える
  - 自社標準セキュリティの確立

# Deep Securityの基本機能

---

# Trend Micro Deep Security™ 製品概要

- Trend Micro Deep Securityは 総合サーバセキュリティ対策製品
- サーバセキュリティで考慮すべきポイントに対応
  - 1. 脆弱性を利用した攻撃への対策  
⇒ IPS/IDS(侵入防御)機能
  - 2. 多様な攻撃手法に対応するための仕組み  
⇒ サーバセキュリティに必要な複数機能を搭載
  - 3. 増減するインスタンスへの柔軟な対応  
⇒ インスタンスの増減にDeep Securityも追従



# IPS/IDS機能で脆弱性を利用した攻撃への対応

## 【パッチ適用の課題】

脆弱性が発見される度にパッチの検証をしてから、都度パッチを適用する作業の負荷が大きい。



## 【解決】

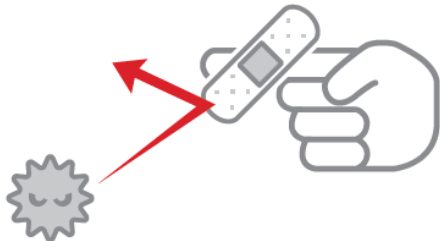
Deep SecurityのIPS/IDS(侵入防御)で脆弱性を突く攻撃に対応。仮想パッチを当てた状態に。

## 【仮想パッチとは？】

- 脆弱性を狙う攻撃コードをネットワークレベルでブロックすることで仮想的にパッチが当たっている状態。

傷口に貼る絆創膏(ばんそうこう)

絆創膏が傷口を保護



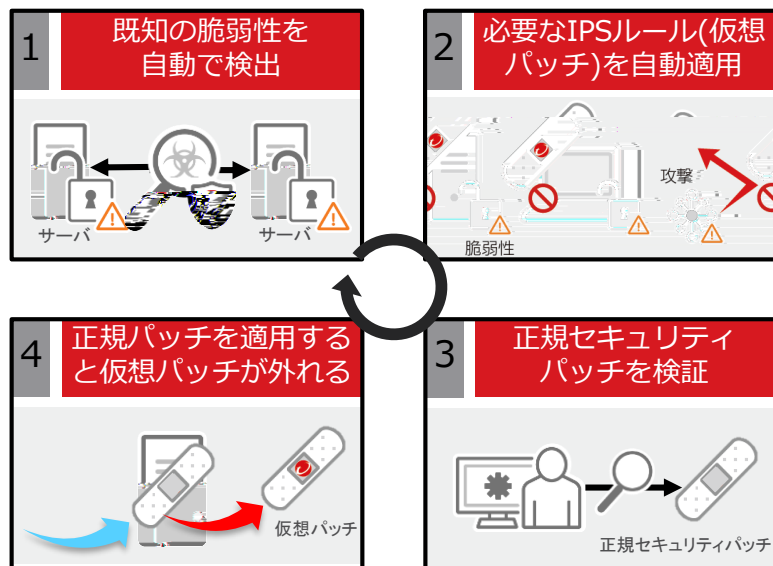
脆弱性を突いた攻撃をブロックする機能

OSやアプリケーションの脆弱性を突いた攻撃をネットワークレベルでブロック



# Deep SecurityのIPS/IDSの特長 ～推奨設定～

「推奨設定」とはDeep Security Agentが自動でサーバ内のシステム情報をスキャンし、サーバ上にある脆弱性を見つけて、そこに対する**必要なIPS/IDSルール**“**仮想パッチ**”を自動で適用する機能です。結果的にサーバは、必要な保護だけを適切に自動で受けることが可能となります。



## 解決可能なペインポイント

- サーバ管理者の脆弱性管理や、脆弱性を狙った攻撃への対処負荷を低減。
- 管理者様自身でIPSルールの適用を行う必要がない。

# Deep Securityと実現するクラウドジャーニー

---



# ステージごとのセキュリティポイント

1. プロジェクト毎のクラウド利用に求めるのは「スピード」
  - 導入の効率化
  - 運用の自動化
2. ハイブリッド環境では「可視化」が重要
  - マルチプラットフォーム対応
  - 統合管理に対応
3. 運用の柔軟性が完全移行(All-In) 環境には求められる
  - サービス個々のニーズに応える
  - 自社標準セキュリティの確立



# Deep Securityのツール群

導入支援



Setup

`/cloudformation`  
`/elastic-beanstalk`  
`/chef`  
`/ansible`

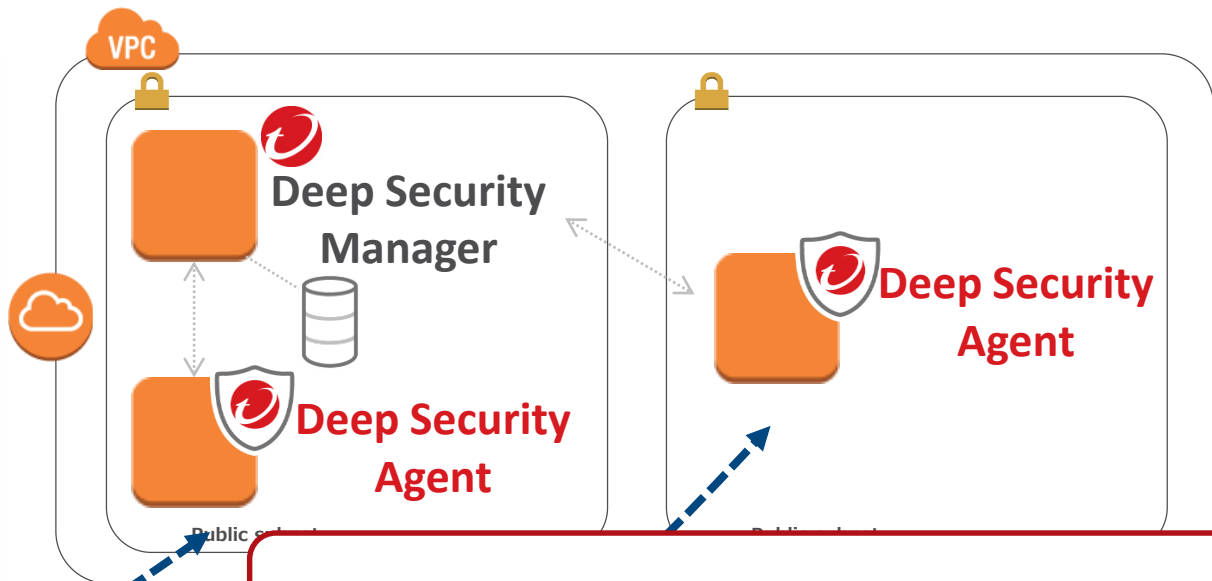
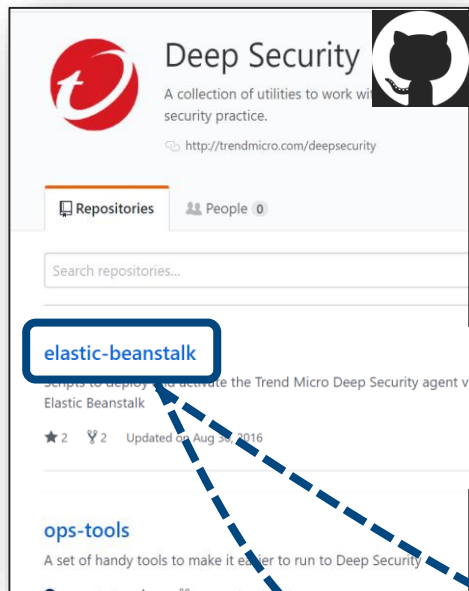


Operations

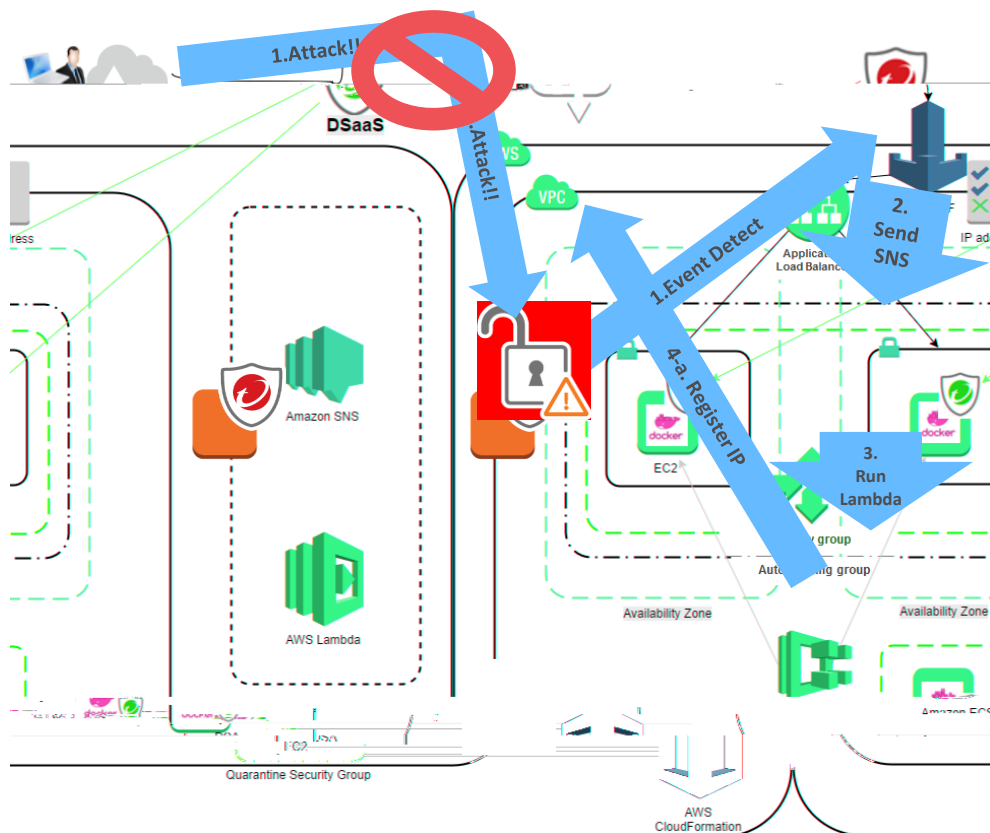
`/ip-lists`  
`/aws-config-rules`  
`/aws-waf`  
`/amazon-inspector`  
`/deep-security-py`  
Amazon SNS 対応

# /elastic-beanstalk

導入支援



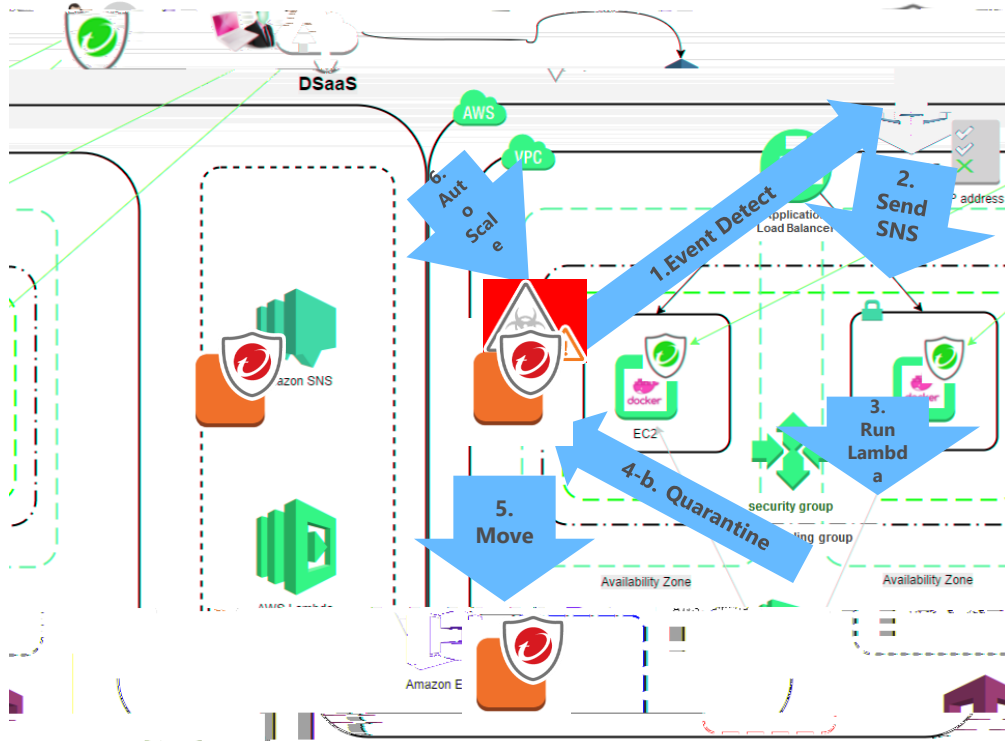
## 運用の自動化① – AWS WAF, SNS, Lambda



### ① AWS WAFを使って自動ブロック

- ① Deep Securityが「IPS/IDS」で攻撃を検知  
Managerにイベントがある
- ② 検出したイベントをManagerからSNSへ通知
- ③ SNSからLambdaを実行
- ④ LambdaがSNS通知に含まれる  
送信元情報「x-forwarded-for」のIPを  
AWS WAFのIPブロックリストへ反映する

## 運用の自動化② - SNS, Lambda, Auto Scaling



② 感染したインスタスを自動隔離、自動復旧

- ① Deep Securityが「ウイルス対策」で感染を検知し、Managerにイベントがあがる
- ② 検出したイベントをManagerからSNSへ通知
- ③ SNSからLambdaを実行
- ④ Lambdaが感染したインスタスを隔離
- ⑤ インスタスが隔離される
- ⑥ インスタスが減ったことでAuto Scalingが発動

運用自動化ソリューションの詳細については  
[aws@trendmicro.co.jp](mailto:aws@trendmicro.co.jp) へ!!

C&Cへの通信、不正アプリケーションの実行  
に対しても隔離可能



## AWS上の仮想サーバを安全に保護 運用の自動化も推進して基幹システムのクラウド化を加速



地域：東京都、日本

業種：IT

製品・ソリューション：  
Trend Micro Deep Security™

導入時期：2013年10月

### 課題

クラウド対応を進める上で、特にこだわったのが運用の自動化だった。セキュリティ製品にも自動運用に対応できることを求めた。

### 解決

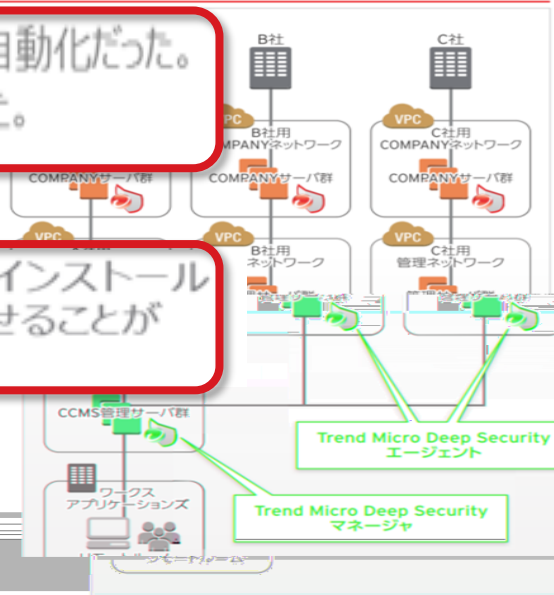
● インスタンスを追加した際、エージェントのインストールから設定、アクティベーションまでを自動化させることが可能。

### 導入効果

● すでに約40の企業や団体がAWS上でERPを利用。世界中の脅威の情報を常に監視し、パターンファイルをリアルタイムに配信してくれるなど、「常にセキュリティの力に見守られている」という大きな安心感がある。

### 〈利用環境イメージ〉

CCMSにおいてAWS上に[COMPANY@]を構築した際のDeep Security適用イメージ

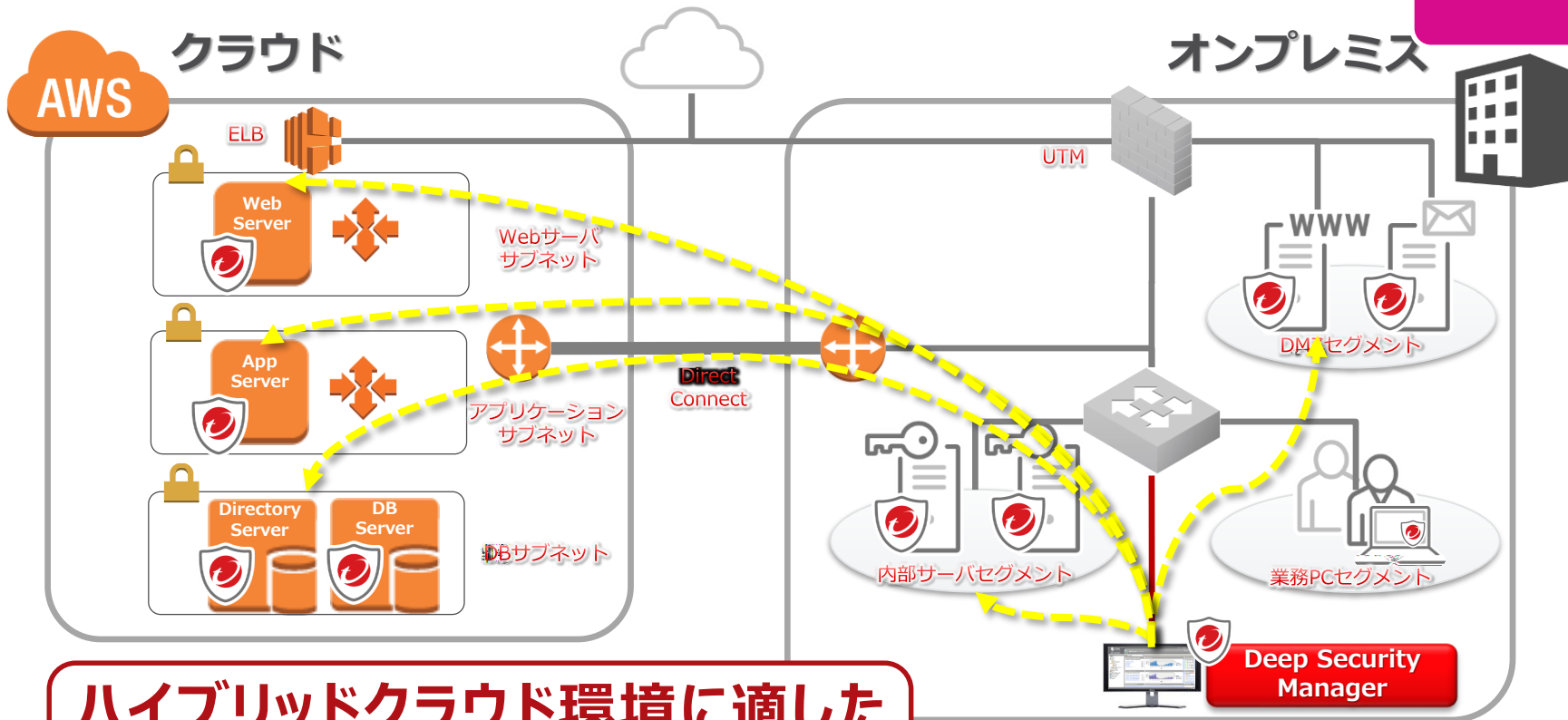


# ステージごとのセキュリティポイント

1. プロジェクト毎のクラウド利用に求めるのは「スピード」
  - 導入の効率化
  - 運用の自動化
2. ハイブリッド環境では「**可視化**」が重要
  - **マルチプラットフォーム対応**
  - **統合管理に対応**
3. 「運用の柔軟性」が完全移行(All-In) 環境には求められる
  - サービス個々のニーズに応える
  - 自社標準セキュリティの確立

# 環境の変化に対応できるセキュリティ

マルチプラットフォーム  
フォーム

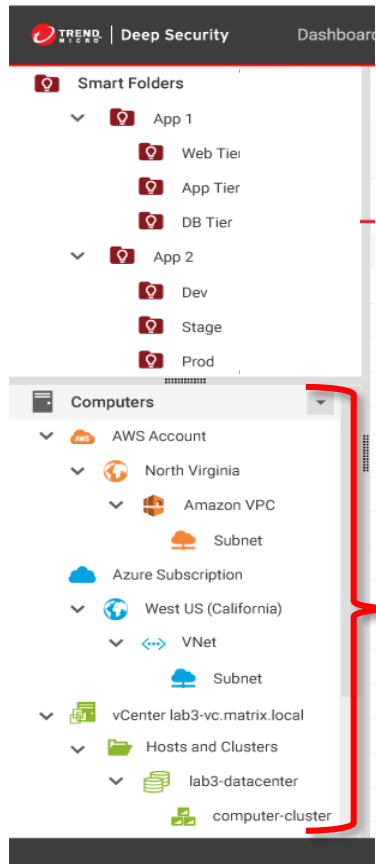


ハイブリッドクラウド環境に適した  
マルチプラットフォーム対応

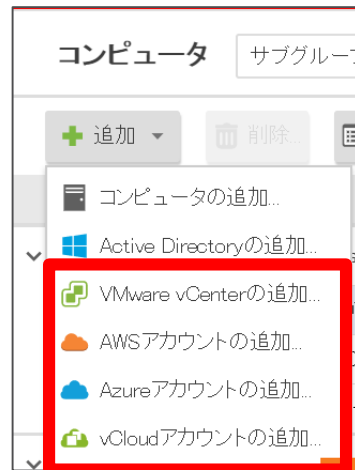
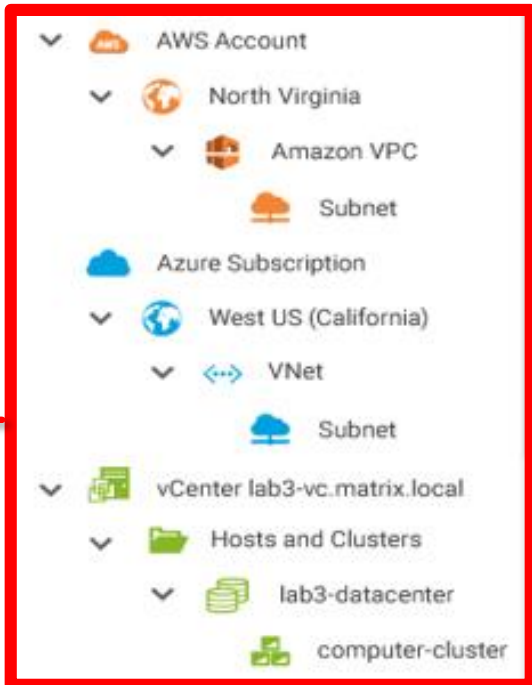


# 環境の変化に対応できるセキュリティ

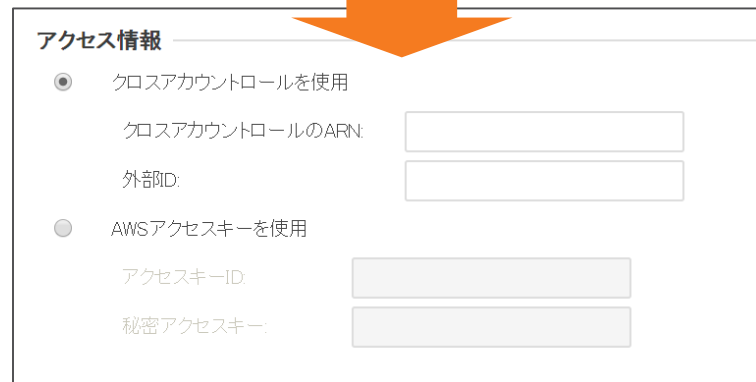
マルチプラットフォーム  
フォーム



異なる環境に対応



設定も簡単  
2ステップ



# スマートフォルダ

統合管理

The screenshot displays the Trend Micro Deep Security interface. On the left, a sidebar lists 'スマートフォルダ' (Smart Folders) with a tree view including '01.On-Primise' (sub-folders: App, DB, Web) and '02.AWS' (sub-folders: Project1, Project2, Project3). Below these are other system categories like '03.基幹システム' and '04.運用基盤システム'. A red bracket groups the Smart Folders section. The main content area shows a detailed view of the 'スマートフォルダ' structure, with a red box around it. A yellow box highlights the folders '03.基幹システム' and '04.運用基盤システム'. A callout bubble with a red border and white background contains the text: '物理、仮想、クラウド環境に関係なく、システムを統合管理する事が可能' (It is possible to manage systems in a unified manner regardless of physical, virtual, or cloud environments). The top right of the interface shows user information 'masteradmin' and navigation links. The bottom left shows '34 Copyright 2017 Trend Micro Inc.' and the Trend Micro logo is in the bottom right.

物理、仮想、クラウド環境  
に関係なく、システムを統  
合管理する事が可能

# スマートフォルダ

統合管理

グルーピングの属性には、プラットフォームやホスト名、またはEC2タグなども利用できる

## Docker Host

### AWS

Tag

Security Group Name

AMI ID

Account ID

Account Name

Region ID

Region Name

VPC ID

Subnet ID

### vCenter

Name

Datacenter

Folder

Parent ESX Hostname

Custom Attribute

TREND MICRO | Deep Security | Dashboard | Actions | Alerts | Events & Reports | Computers | Policies

スマートフォルダ

01.On-Prmise

Smart Folder Builder

Name: Web Tier

Add Filter Group

Add Filter

on Linux AMI

Web Applic...

Add Filter

ged

Folder: Base Policy

Save Close

03.基幹システム

04.運用基盤システム

05.ファイル連携基盤

99.demo-ecs-ds10-instance

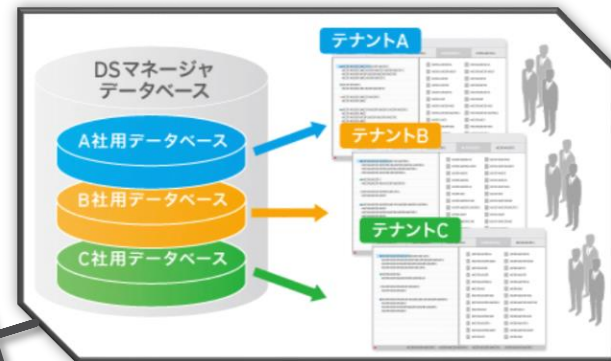
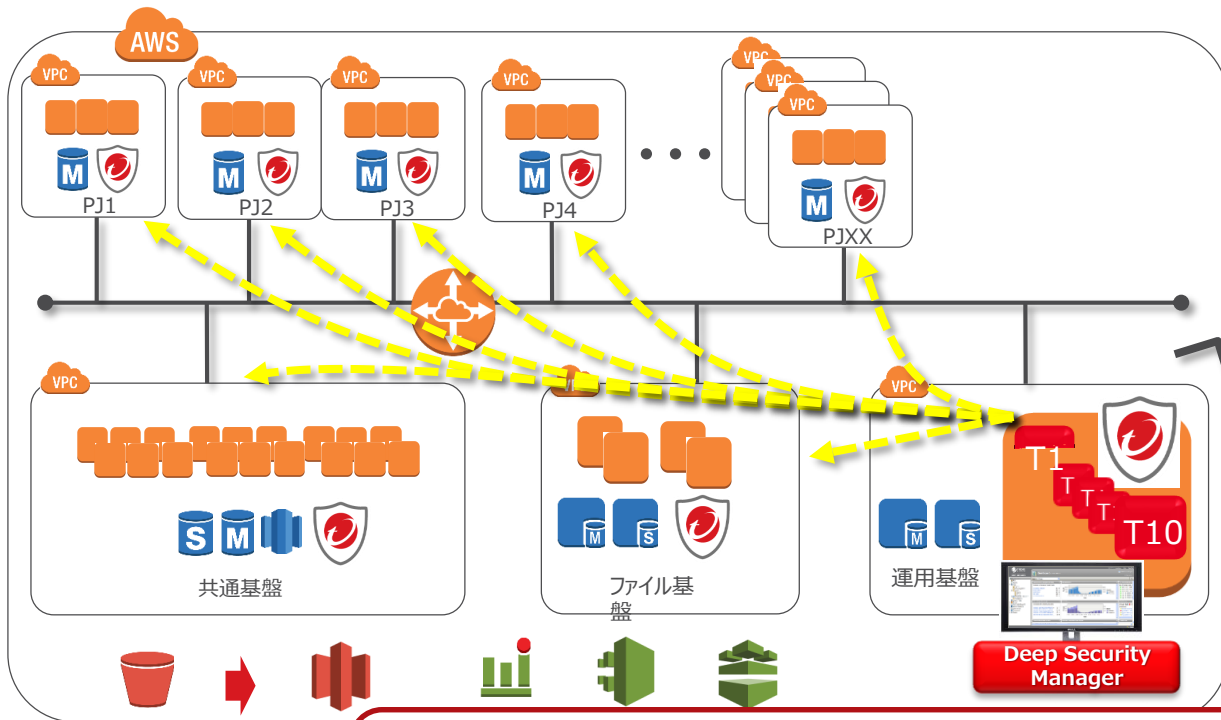
99.Quarantined

# ステージごとのセキュリティポイント

1. プロジェクト毎のクラウド利用に求めるのは「スピード」
  - 導入の効率化
  - 運用の自動化
2. ハイブリッド環境では「可視化」が重要
  - マルチプラットフォーム対応
  - 統合管理に対応
3. 「運用の柔軟性」が完全移行(All-In) 環境には求められる
  - サービス個々のニーズに応える
  - 自社標準セキュリティの確立

# マルチテナント

サービス  
個々のニーズ



- 完全独立したマルチテナント環境
- サービス毎のセキュリティ要件を実現

# オンプレミスと変わらないセキュリティを確保

予

従来型は予防的な対策が中心

- ・パッチの適用
- ・パスワードポリシーの強化 など

ゼロデイ・攻撃早期化・運用不備・リスト型

完璧な予防は困難

発

今後は発見的な対策を強化

- ・不正侵入、改ざんの検知
- ・大量の認証試行の検知 など

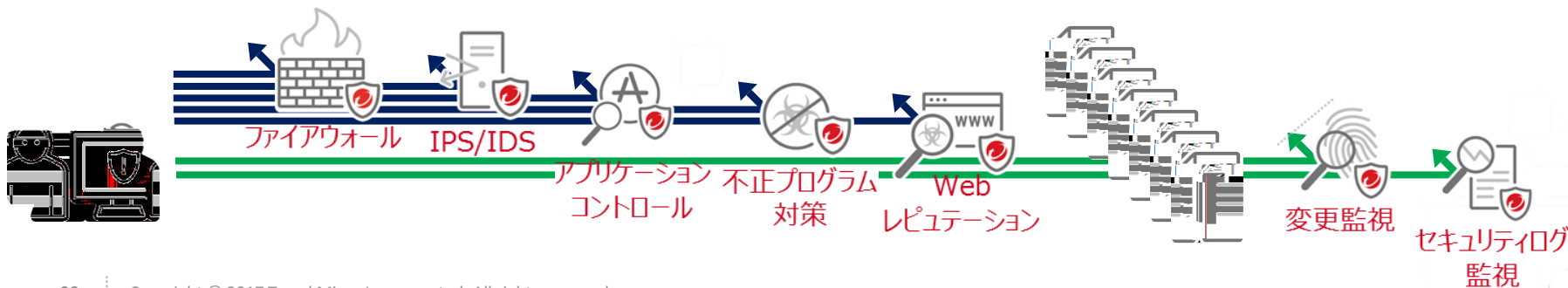
攻撃に「気づく」

被害を最小限に留める

予

発

とで多層的な防御の仕組みを構築



# クラウド上のシステムはTrend Micro Deep Security™で守る ——NTTドコモの選択と流儀



## 課題

- 顧客向けサービスの立ち上げに際して、約280項目の厳格なセキュリティ規程のチェックリストを満たす必要があった

## 解決

をしっかりと守れる製品が他にはなく、Deep SecurityがAWS向けのセキュリティ対策製品としてスタンダードな第一の選択だった

業種：通信

地域：東京都、日本

導入製品・ソリューション：  
Trend Micro Deep Security™

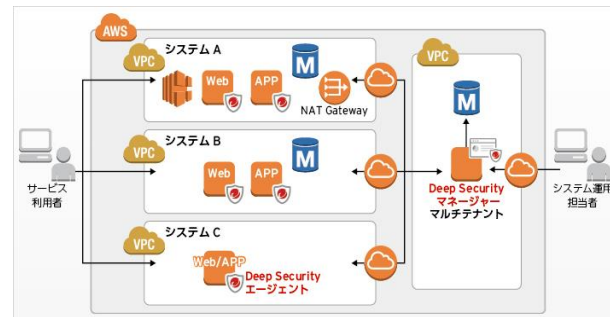
導入時期：2012年

Deep Securityで防御、厳格な社内のセキュリティ規定に則ったAWS活用を可能にした

- Deep Securityのマルチテナント機能の活用で、サービス個々のニーズに柔軟に対応できるセキュリティ対策と運用のスタイルが確立できた
- AWSとDeep Securityの高い親和性により、クラウドのスピード感を損なわないセキュリティ対策が可能になった
- クラウド上でDeep Securityを利用する多数の技術者・ユーザの知識・知見を、有効に活用することが可能になった

ファイアウォール、IDS/IPS、変更監視、ログ監  
査を可能にするため

## （利用環境イメージ）





# 業務効率化を見据え社内システムをAWSに移行 複数システムの 共通基盤にセキュリティを組み込み、安全・柔軟なクラウド活用を実現



地域：東京都、日本

業種：商業・サービス

製品・ソリューション：  
Trend Micro Deep Security

導入時期：2014年11月

## 課題

- 基幹システムをアマゾン ウェブ サービス (AWS) に移行することを決定。その際、クラウドを守る「自社標準のセキュリティ対策」を確立したかった

## 解決

- 豊富な機能を揃えており、オンプレミス環境と同  
等のセキュリティポリシーが維持できる

- AWSでの豊富な稼働実績

### 導入効果

- クラウド上の基幹システムを守る「多層防御」を実現
- 必要な機能のみオン・オフすることで、AWSのパフォーマンスを阻害しない運用を実現
- セキュリティ対策をAWSの共通基盤部分に組み込み、自社標準の対策手法を確立

### 〈利用環境イメージ〉





# まとめ - AWS利用時のセキュリティポイント

## 1. AWSにおけるセキュリティは「責任共有モデル」

- AWSユーザにもセキュリティ対策をする必要がある
- OSやミドルウェア、アプリケーションなど……

## 2. 最近の脅威から考える、AWSセキュリティの要は「脆弱性対策」

- ここ数年、相次ぐ情報漏えい
- ウイルス対策、ファイアウォールでは防ぎきれない

## 3. クラウドの利用ステージによって他に考慮すべきポイントは異なる

- プロジェクト毎の利用 or ハイブリッドクラウド環境 or 完全移行

# まとめ – クラウドステージ別セキュリティポイント

プロジェクト

- スピード

導入の効率化  
運用の自動化



ハイブリッド

- 可視化

マルチプラットフォーム  
統合管理



完全移行

- 運用の柔軟性

サービス個々のニーズ  
自社標準セキュリティ



# ブースにぜひお立ち寄りください！

②会場を出て左手の  
展示会場へ

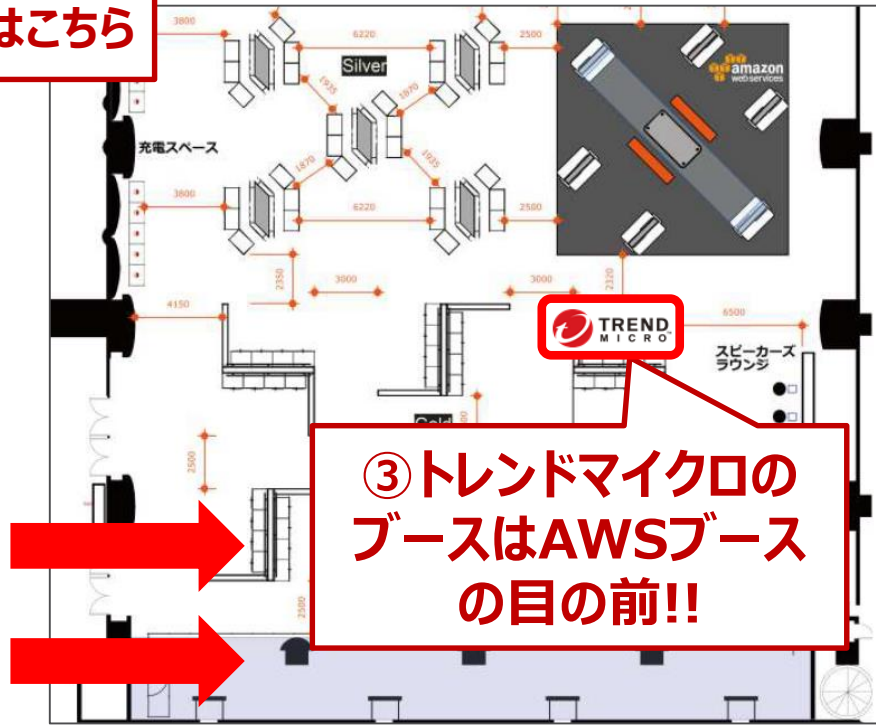
①トレンドマイクロの  
セッション会場はこちら

5/30 - 6/2 講演会場  
[5/30] Dive Deep Day 「金融サービス シンポジウム」  
[5/31-6/2] AWS Techトラック 2

5/30 - 6/2 講演会場  
[5/30] Dive Deep Day 「AWSome Day Tokyo」  
[5/31-6/2] 導入事例トラック 1

5/30 - 6/2 講演会場  
[5/30] Dive Deep Day 「AWS エンタープライズクラウドシ」  
[5/31-6/2] 導入事例トラック 2

EXPO会場



③トレンドマイクロの  
ブースはAWSブース  
の目の前!!

# ご清聴ありがとうございました

注意：GitHubのツール類はオープンソースで無償にてご提供しているものです。トレンドマイクロのサポートセンターにはお問い合わせいただけません。ツールについて、うまく動作しないなどのお困りごとがあった場合には、直接GitHubにコメントをしてください。