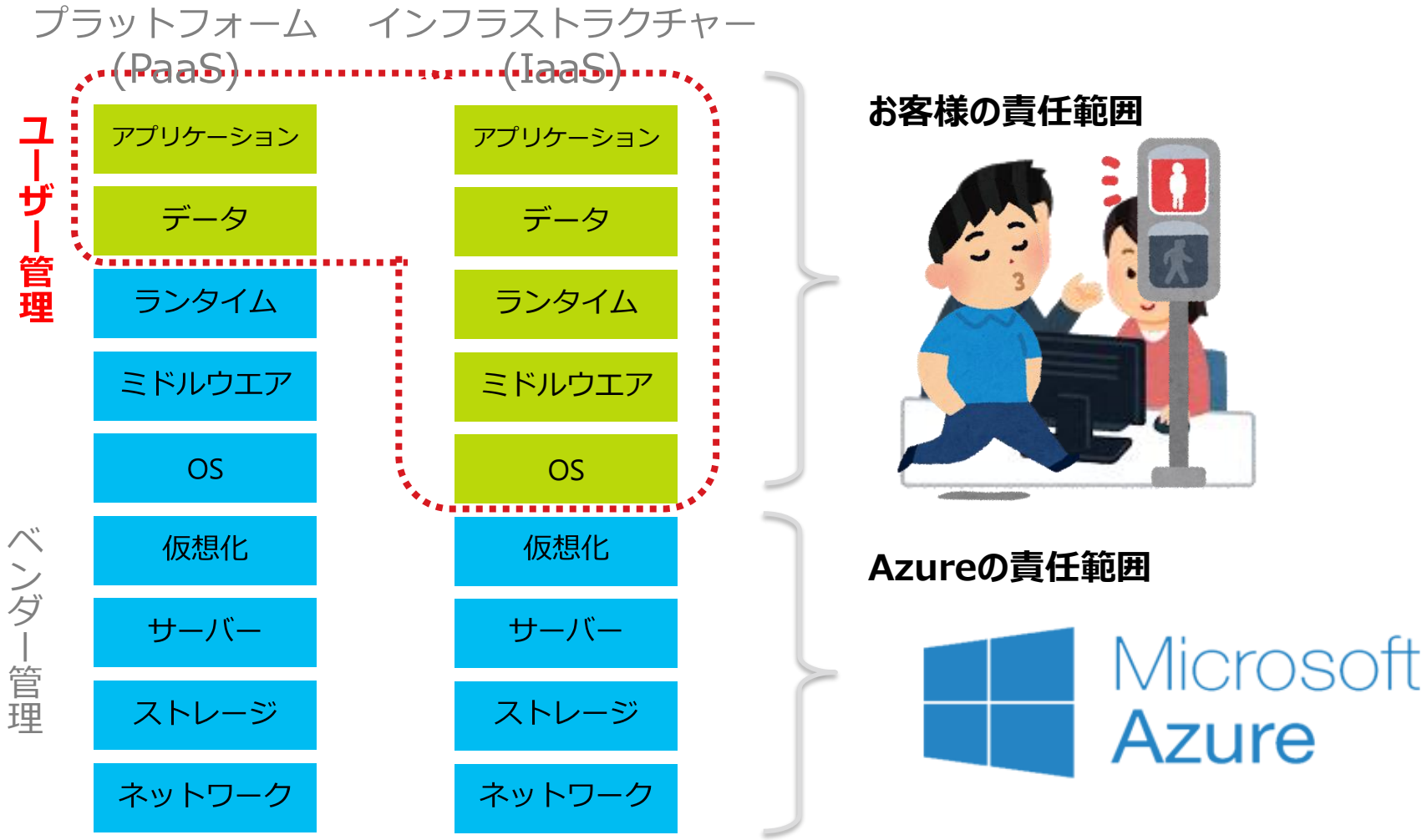
攻撃デモもやりますよ
ヾ(*´∀`*)ノ♪

Microsoft Azure環境におけるセキュリティ対策

～ Trend Micro Deep Security で安全安心に ～

トレンドマイクロ株式会社

クラウド環境でのセキュリティ大前提「責任分離モデル」

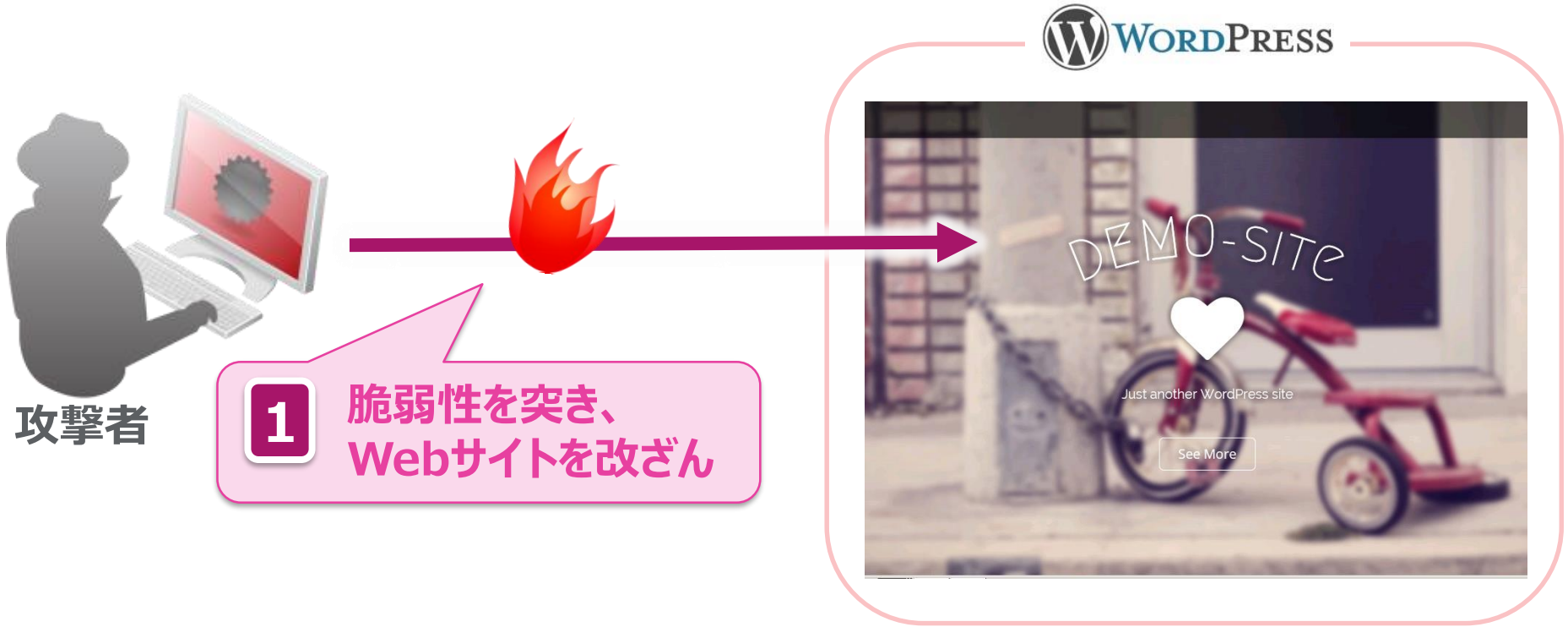


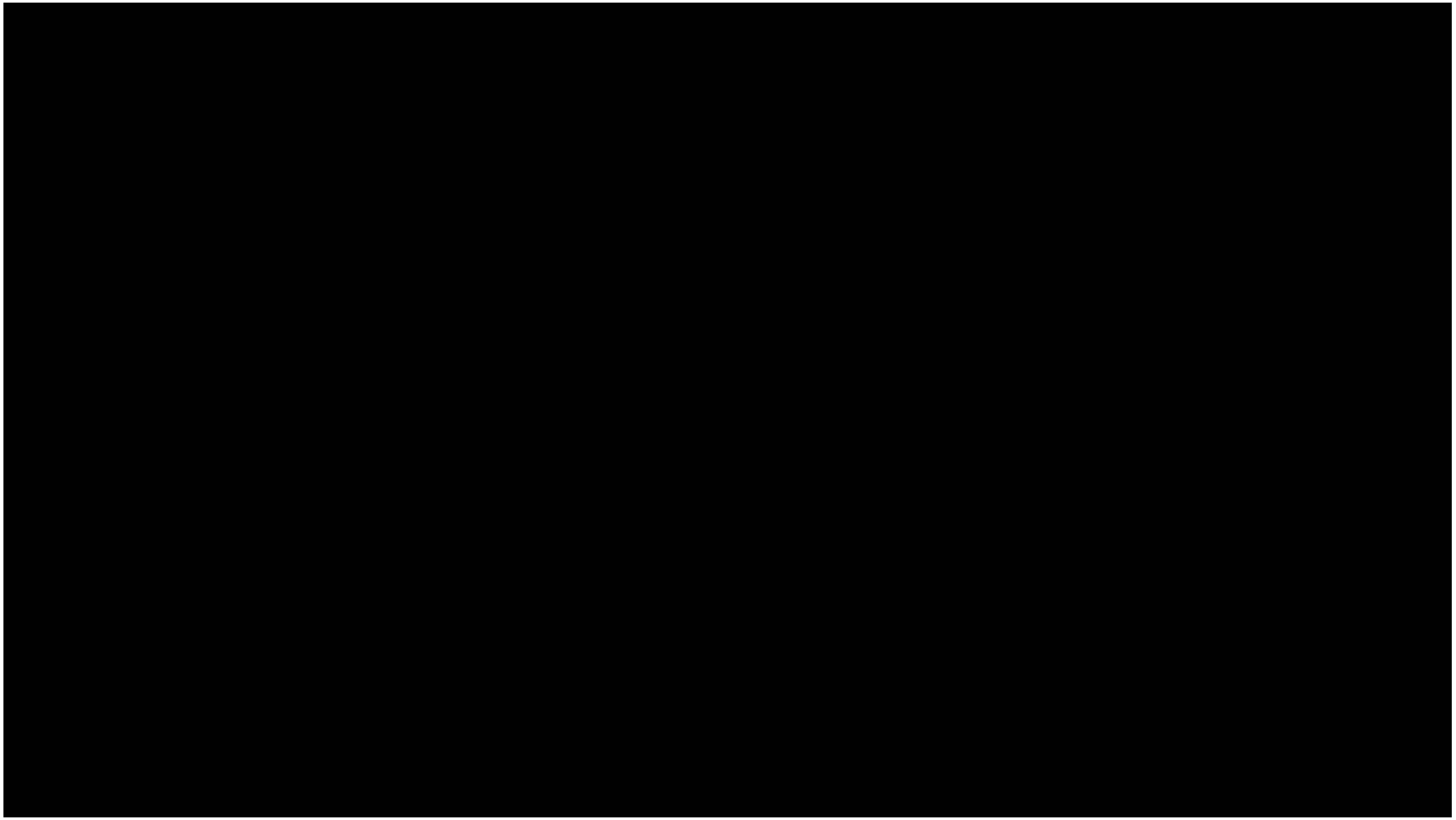
Cloud Services
Websites

Virtual Machines
Windows Server Hyper-V

早速ですが、
デモンストレーションを
ご覧ください

ユーザ範囲のセキュリティ対策を一切行わなかった場合・・・・？





Azureを安心安全に使うために、ユーザ範囲はキッチリ守りましょう！

	プラットフォーム (PaaS)	インフラストラクチャー (IaaS)
ユーザー管理	アプリケーション	アプリケーション
	データ	データ
	ランタイム	ランタイム
	ミドルウエア	ミドルウエア
	OS	OS
ベンダー管理	仮想化	仮想化
	サーバー	サーバー
	ストレージ	ストレージ
	ネットワーク	ネットワーク

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

TREND MICRO™ SMART PROTECTION NETWORK™

Azureの責任範囲

Microsoft Azure

Cloud Services
Websites

Virtual Machines
Windows Server Hyper-V

トレンドマイクロといえば・・・

・・・だけではありません！

サーバ保護に最適な
トレンドマイクロの“Deep Security”

サーバ保護に
お困りの方に…

クラウド環境を
検討中の方に…

目次

- Deep Securityの概要
- Deep Security ３分かんたん構築
- Azureを最大限利用できる３つのメリット
- こんなお悩みに応えます

Deep Securityの概要

Deep Securityとは？

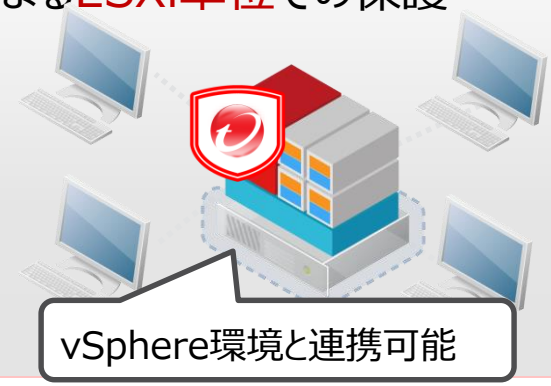
- ハイブリッドに各種構成に対応。サーバ保護に必要なセキュリティ機能を網羅した、All in One のセキュリティ製品です。

物理環境

エージェント型ソフトによる
サーバー単位の保護

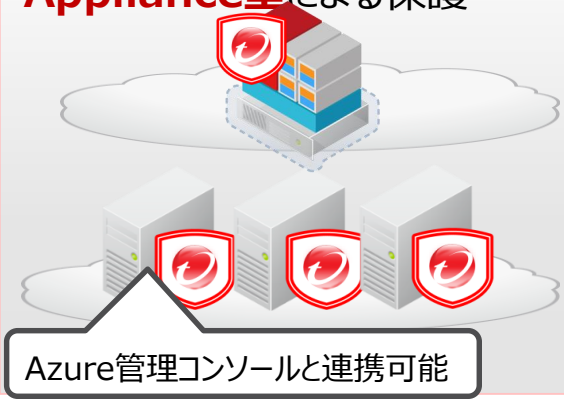
仮想環境

Virtual Appliance型に
よるESXi単位での保護



クラウド環境

エージェント型又は**Virtual Appliance型**による保護



多層防御

セキュリティ機能	内容
ファイアウォール	攻撃を受ける機会を軽減します。
侵入防御（IDS/IPS）	脆弱性を突いた攻撃からサーバを保護します。
セキュリティログ監視	重要なセキュリティイベントを早期に発見します。
変更監視	ファイルの改ざん等を早期に発見します。
不正プログラム対策	ウイルス等の不正プログラムを検出します。

不正プログラム対策とファイアウォール

不正プログラム対策	ファイアウォール	侵入防御（脆弱性対策）	変更監視	セキュリティログ監視

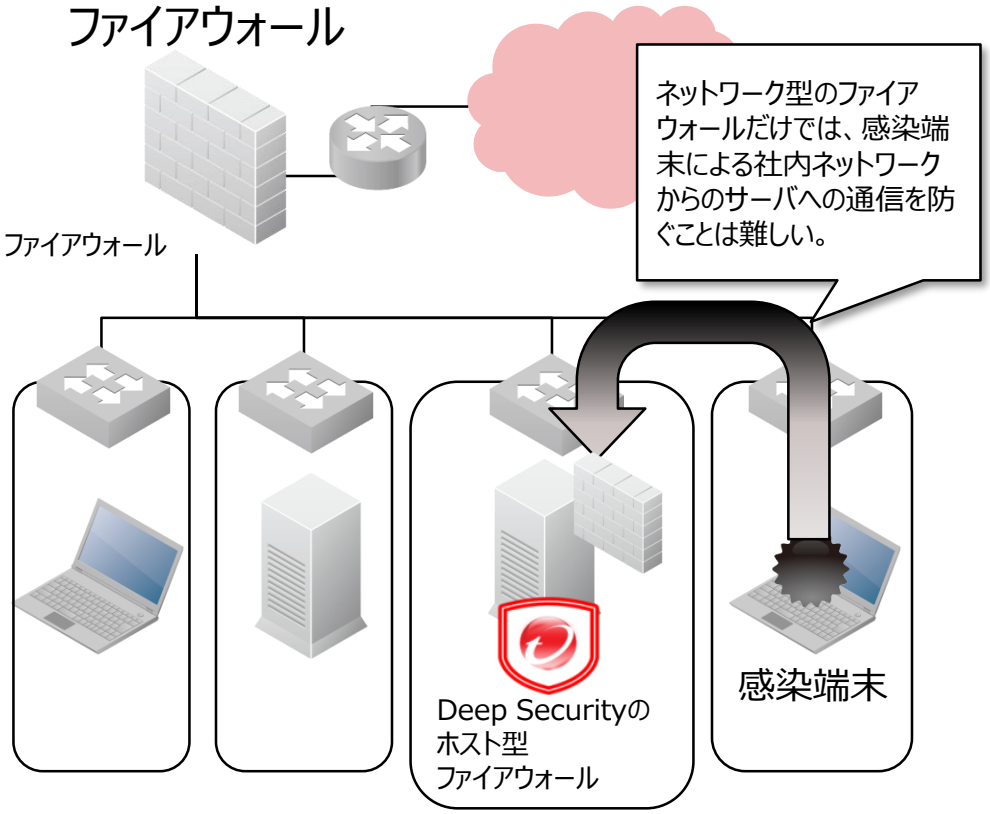
不正プログラム対策

リアルタイム検索
予約検索
手動検索
振る舞い検知機能による自己防御機能

[Webレピュテーションサービス]

Webレピュテーションとは？
Webからの脅威の出所である不正URLへのアクセスを未然にブロックします。トレンドマイクロのノウハウがつまった「Smart Protection Network」機能の１つです。

Linux版機能（詳細はシステム要件に記載）
予約検索、手動検索
リアルタイム検索



TREND MICRO

侵入防御

不正プログラム対策	ファイアウォール	**侵入防御（脆弱性対策）**	変更監視	セキュリティログ監視

- OSやアプリケーションの脆弱性（セキュリティホール）を突く攻撃パケットを検知し、防御する機能（**仮想パッチ**）
- SQLインジェクションやクロスサイトスクリプティング等のWebアプリケーションの脆弱性を突く攻撃パケットを検知し、防御する機能（WAF）

仮想パッチ

脆弱性を修正するセキュリティパッチをインストールする代わりに、脆弱性を突く攻撃をブロックし、仮想的にパッチの役目を提供します。

ポイント１：
ソフトウェアのコードレベルでの修正を行わないので、動作中のシステムへ影響が少ない

ポイント２：
WindowsやLinuxのようなOSだけでなく、様々なアプリケーションの仮想パッチがトレンドマイクロから提供される

仮想パッチは一時的な保護を目的としたもので、
根本的な解決のためにはセキュリティパッチをインストールする必要があります。

TREND MICRO

さらに便利な“推奨設定”機能で、チューニングは全て自動化

収集する情報

- インストールアプリケーション情報
- ファイル情報
- 実行されているプロセス
- 環境変数
- 開いているポート
- レジストリ(Windowsのみ)
- サービス(Windowsのみ)

アプリケーションのバージョン

セキュリティパッチの適用状況

推奨するルールの選別、自動適用

- ✓ ベンダーのセキュリティパッチを適用するまで脆弱性を保護できる
- ✓ 新しい脆弱性への対応をタイムリーに実施する運用ができる

Deep Security脆弱性対策の対応アプリケーションと提供時間の目安

代表的な対応アプリケーションの例

- Windows, Linux, Solaris (OS自体の脆弱性)
- データベースソフトウェア (MS SQL, Oracle等)
- メールソフトウェア (Exchange,Sendmail,Postfix)
- Webアプリケーション (IIS, Apache)
- その他 (Active Directory,OpenSSL)
- Adobe Acrobat, Adobe Flash
- メールクライアント (Outlook & Outlook Express)
- Webブラウザ (Internet Explorer, FireFox)
- Officeソフト (Word, Excel, PowerPoint etc.)
- メディア再生ソフト (Windows Media Player, Real Player) など

※この他にも多数のアプリケーションに対応しています

ご提供までの期間(SLO)

- **緊急かつ重要度の高い脆弱性**

48時間以内に仮想パッチ作成

- **上記に当てはまらない、Tier1のソフトウェアでCVEスコアが9.0以上の脆弱性**

2週間以内に仮想パッチ作成

※仮想パッチのリリースサイクルは2週間に1度です。

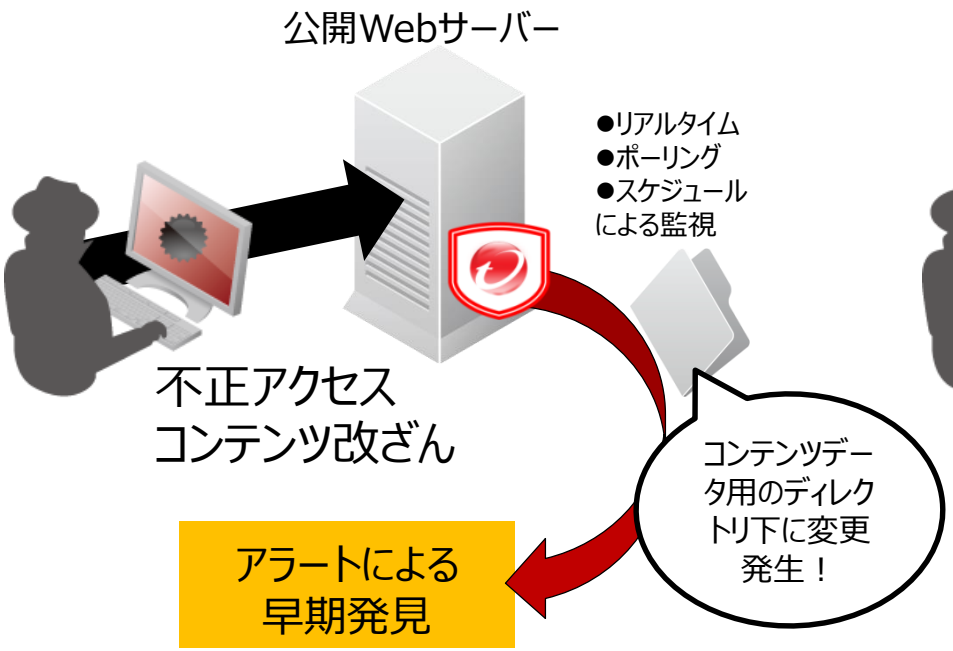
リリース目標	対象
脆弱性情報公開後48 時間以内	• Microsoft社の月例パッチ • Microsoft社の緊急パッチ
サービスレベル1 = 次回シグネチャアップデート時	• Tier1のソフトウェアでCVEのスコアが9.0~10の脆弱性
サービスレベル2 = 二回目のシグネチャアップデート以内	• Tier1のソフトウェアでCVEのスコアが7.0~8.9の脆弱性
サービスレベル3 = 三回目のシグネチャアップデート以内	• Tier1のソフトウェアでCVEのスコアが4.0~6.9の脆弱性 • Tier2のソフトウェアでCVEのスコアが9.0~10の脆弱性

Tier1（一例）	DHCP Server/Client, DNS Client, FTP Client, Microsoft Office, Inernet Explorer, Windows Service, Adobe, Sun Java　など
Tier2（一例）	Microsoft Outlook Express, Instant Messenger　など
Tier2以外（Best effort）	Quicktime, Safari, Chrome　など

変更監視とセキュリティログ監視

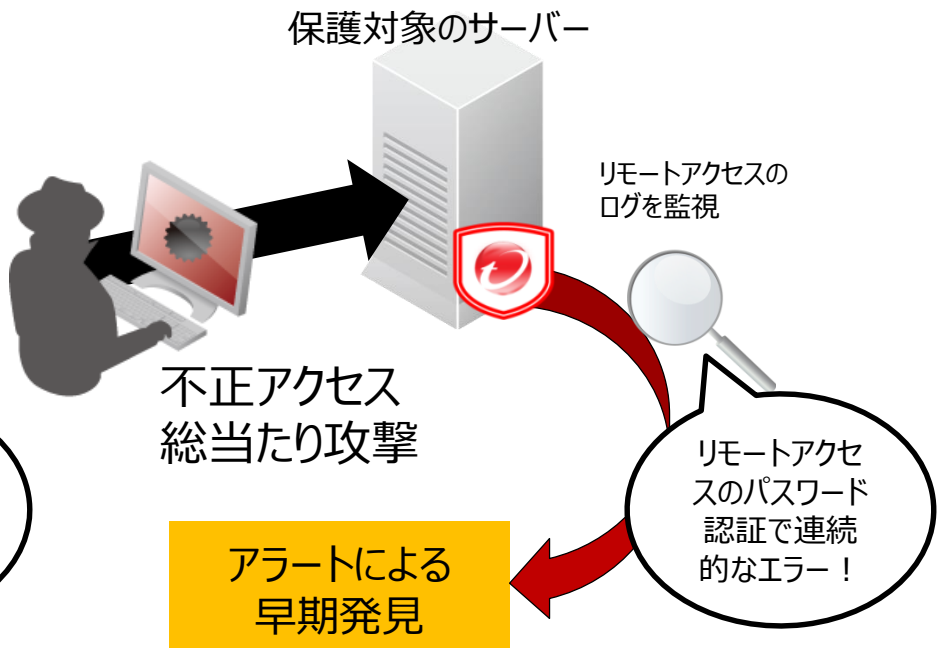
不正プログラム対策	ファイアウォール	侵入防御（脆弱性対策）	変更監視	セキュリティログ監視

変更監視（例）



ファイル（ファイル属性含む）、ディレクトリ、レジストリ、プロセスなどの変更を検知可能。

セキュリティログ監視（例）



OSのイベントログ、Syslogの他、Webサーバーや DB等のログを監視可能。

TREND MICRO

「侵入防御」（脆弱性対策）のデモンストレーション

脆弱性を突くことで、Wordpressのブログがいとも簡単に改ざんされてしまいました！

攻撃者

トップページの書き換え
バックドアの設置　etc…

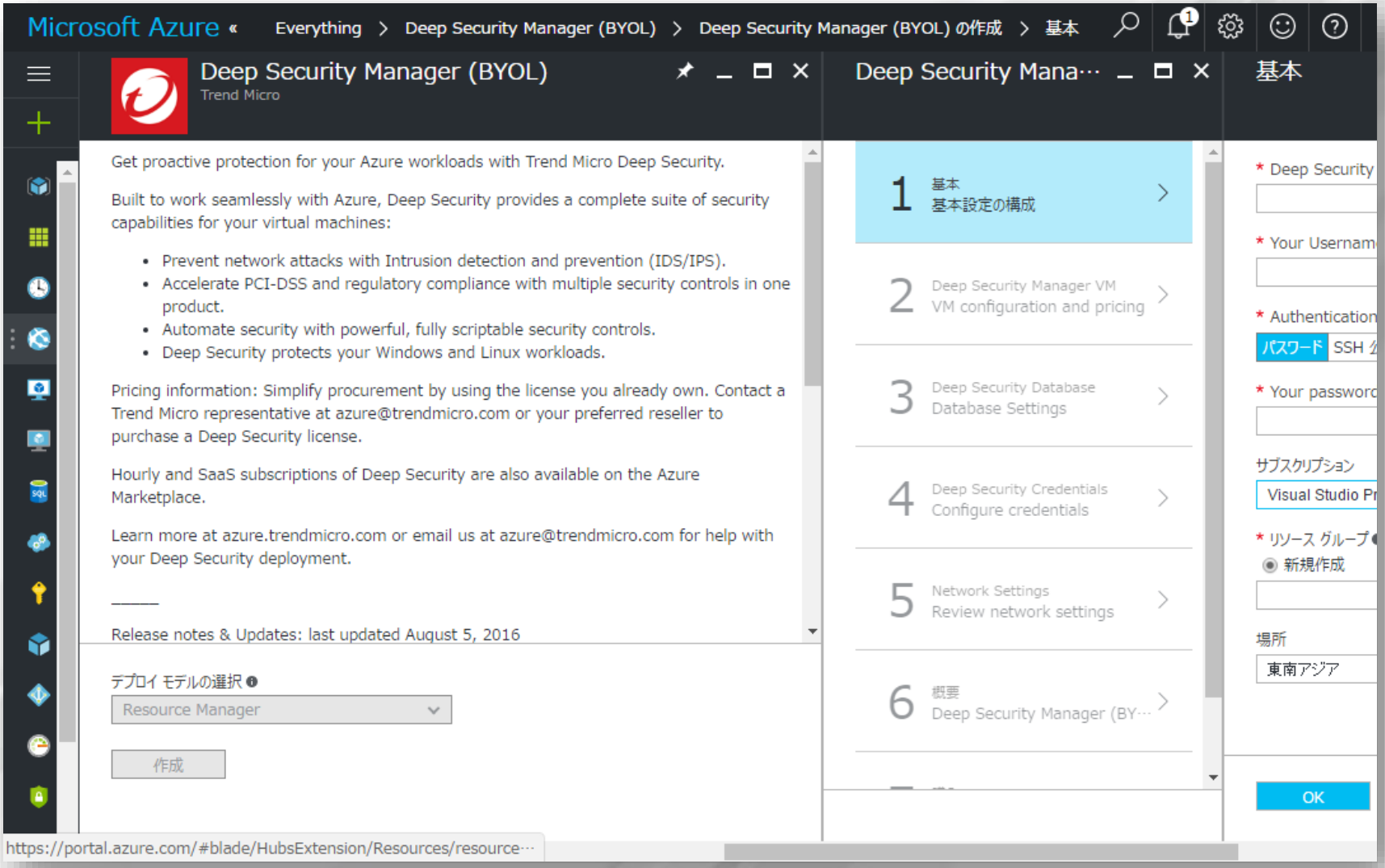
百聞は一見にしかず！
仮想パッチのデモをご覧ください♪

攻撃者

Deep Securityの
『仮想パッチ』機能を導入！
脆弱性を狙う攻撃を防ぎます！

どうやって構築するの？？

Marketplaceを使いましょう



Azureを最大限利用できる３つのメリット

クラウドセキュリティを考えるための
3つのポイント

1．Azureの柔軟なリソースを活かすためには？

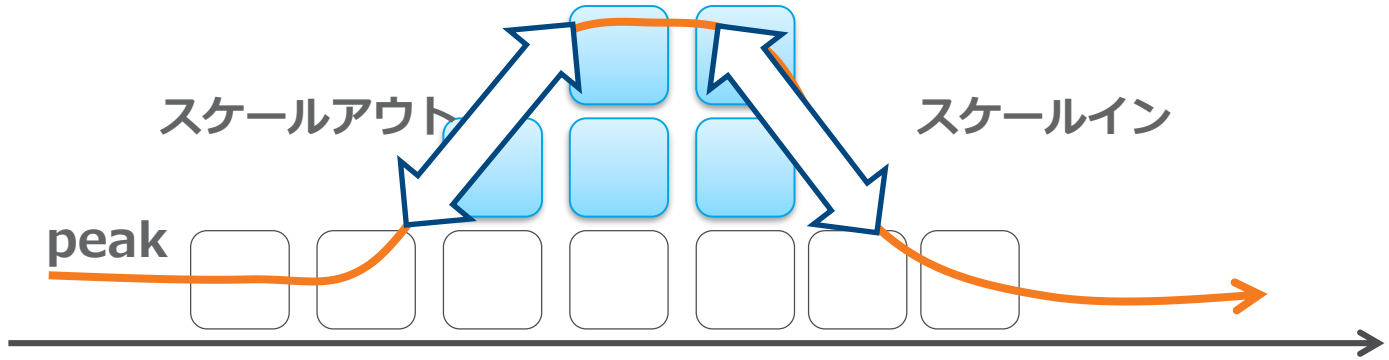
2．ゲートウェイ型 vs ホスト型？

3．巧妙化する攻撃にどう対応すべきか？

1．柔軟なリソースを活かすためには？

- Auto Scalingとは？
  - サーバーの負荷に応じて、自動的にクラウドサーバーの台数を増減させる機能のことです。

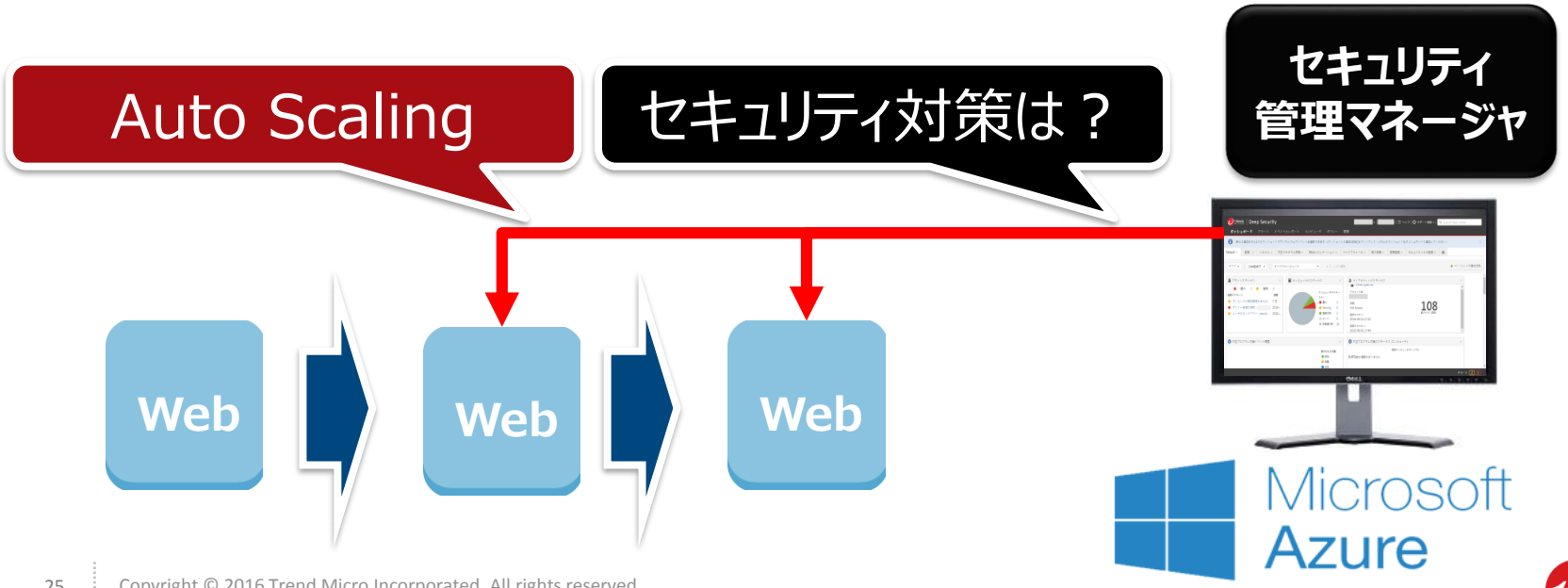
peak時に合わせて自動的にスケールする



- 条件に応じてサーバを拡張/縮小
- 負荷が増えたら台数を増やす
- 負荷が減ったら台数を減らす

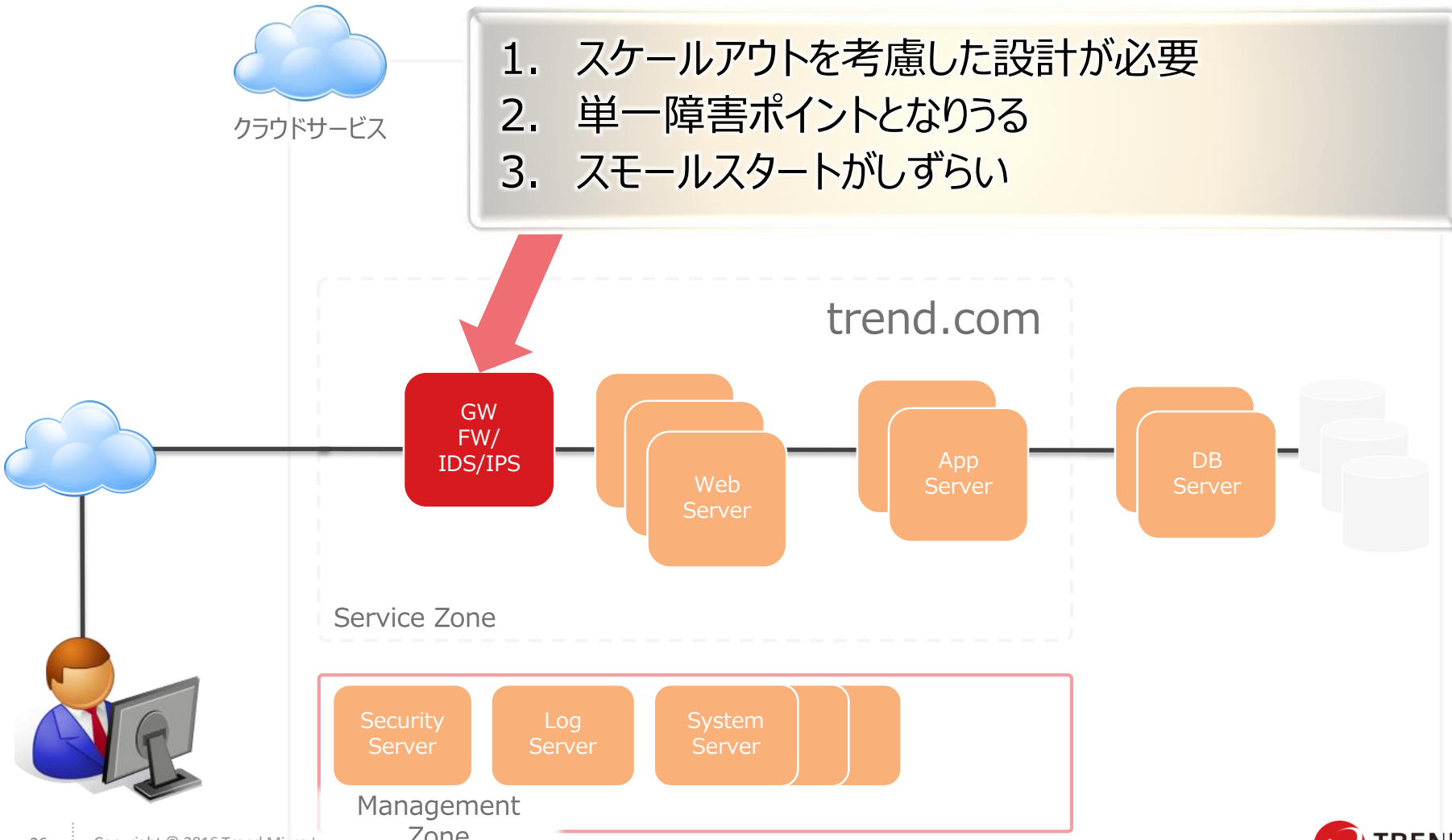
Auto Scalingとセキュリティ

- 従来型のセキュリティ対策の場合、増えたインスタンスに対して、都度、設定が必要
- インスタンスは自動で増えるのに、セキュリティは手動で管理するため、クラウドのメリットが受けられない



2．ゲートウェイ型 vs ホスト型？

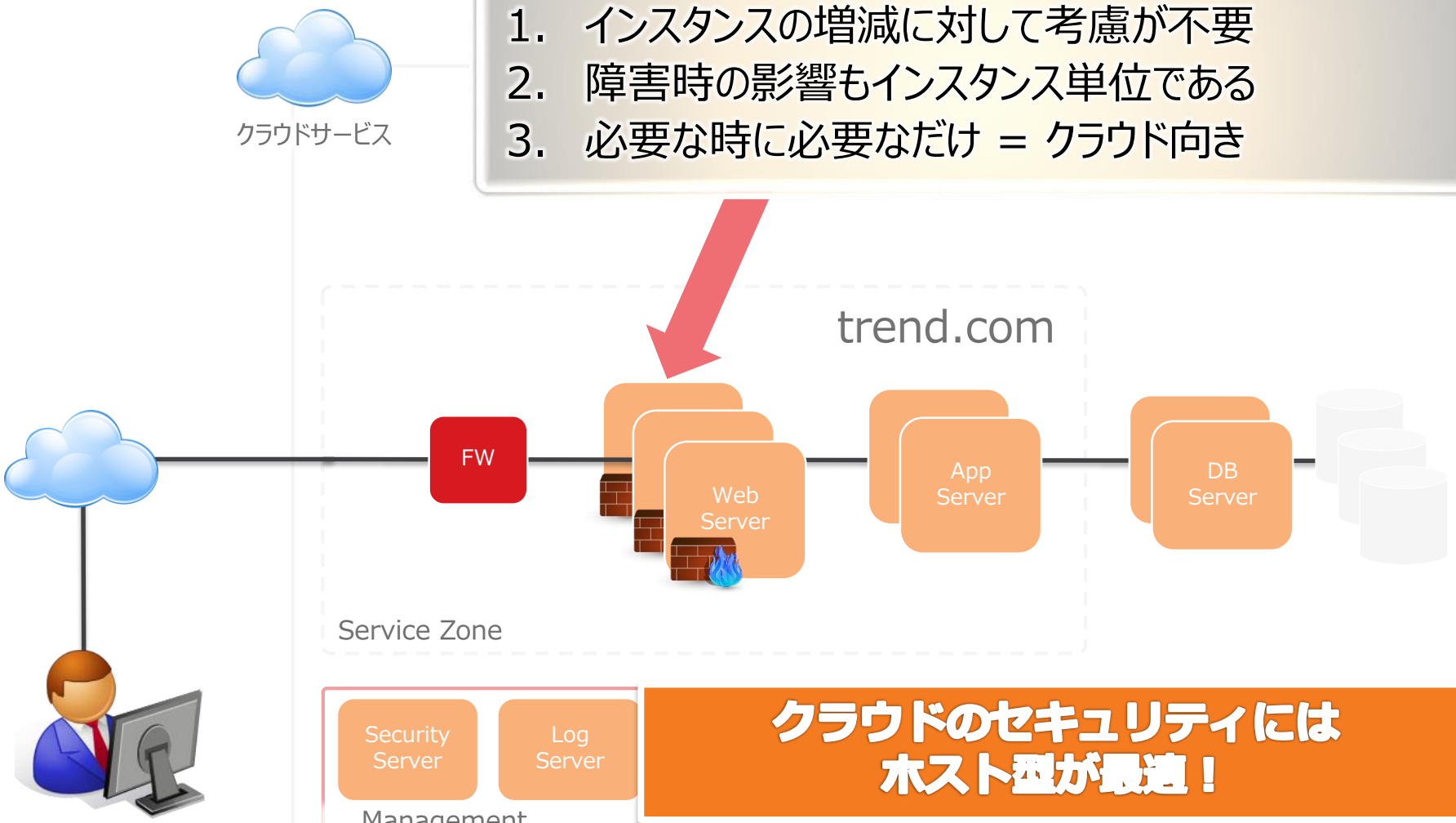
ゲートウェイの場合…



2．ゲートウェイ型 vs ホスト型？

ホスト型の場合…

1. インスタンスの増減に対して考慮が不要
2. 障害時の影響もインスタンス単位である
3. 必要な時に必要なだけ ＝ クラウド向き

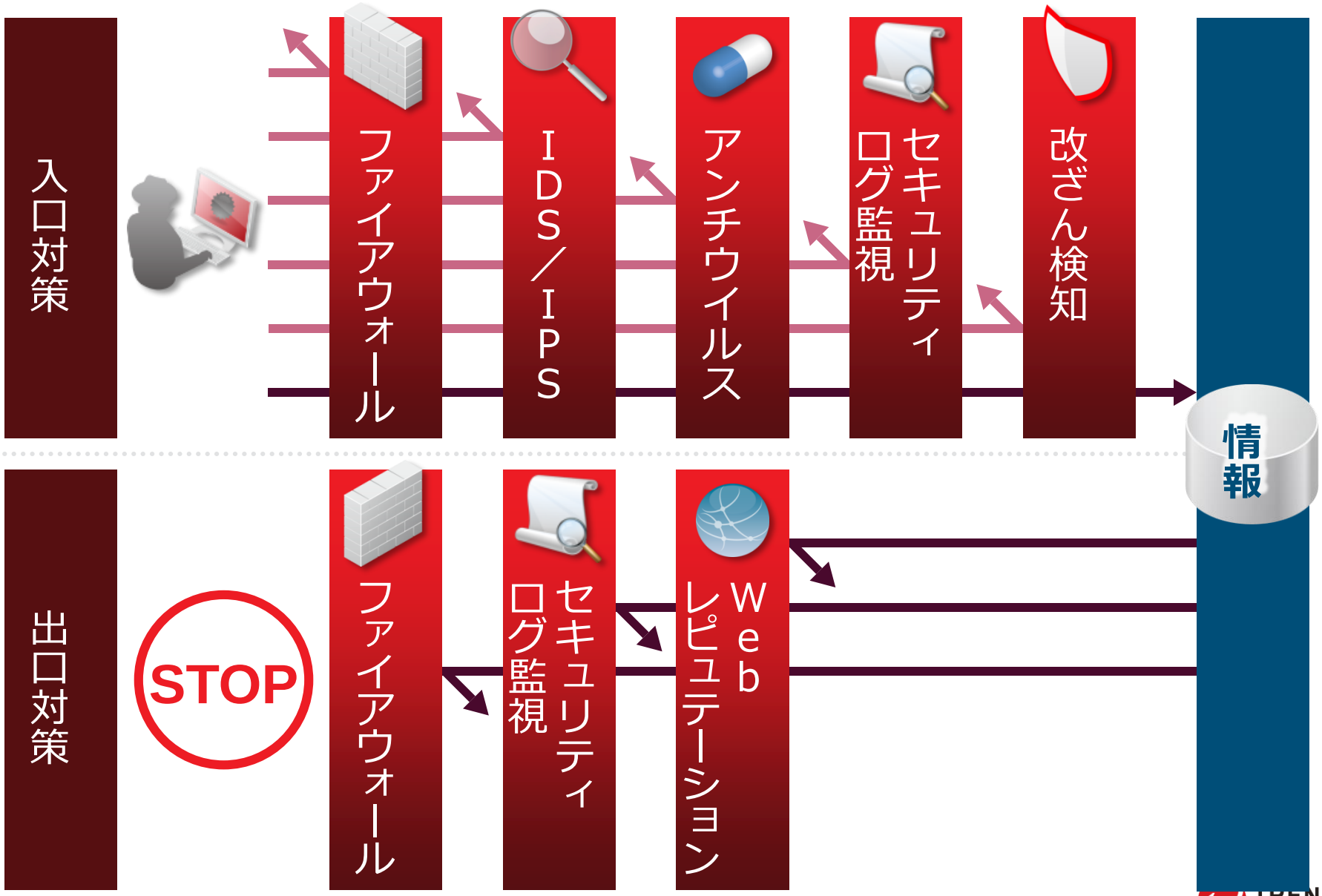


3．巧妙化する攻撃にどう対応すべきか？

巧妙化する攻撃に対応するキーは…

『多層防御』です！

複数機能を導入し、多層防御を実現！



クラウドセキュリティを考えるための
3つのポイント

1．Auto Scalingに対応！

2．クラウド環境にはホスト型が最適！

3．複数の機能で、多層防御を実現！

Trend Micro Deep Security
なら
すべて実現可能です！

こんなお悩みにこえたえます

こんなお悩みに応えます

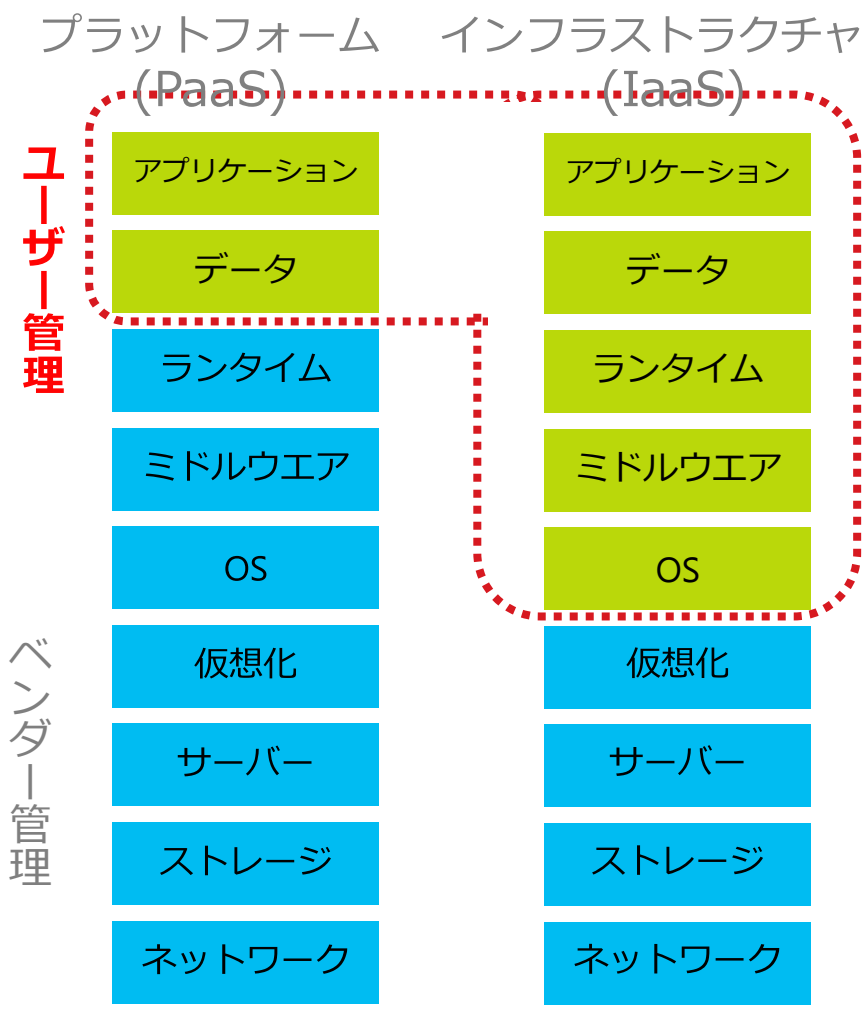
- サーバを多層的に保護したい
- サーバ改ざんの対策をしたい
- 脆弱性の対応を計画的に行いたい
- Auto Scaling機能を使いたい
- PCI DSSに準拠したい
  - **PCI DSS準拠支援におけるDeep Securityの特長**
  - http://www.trendmicro.co.jp/jp/business/products/tmds/pci-dss/index.html
- 導入実績のある製品を使いたい
  - **導入事例**
  - https://app.trendmicro.co.jp/case/list/?Goods=tmds

そういえばさっきの仮想マシン…

デプロイ完了した？

まとめ

クラウド環境でのセキュリティ大前提「責任分離モデル」



お客様の責任範囲

Azureの責任範囲

Microsoft Azure

Cloud Services
Websites

Virtual Machines
Windows Server Hyper-V

Deep Securityとは？

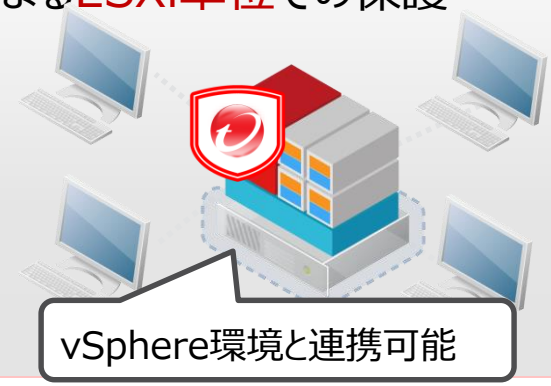
- ハイブリッドに各種構成に対応。サーバ保護に必要なセキュリティ機能を網羅した、All in One のセキュリティ製品です。

物理環境

エージェント型ソフトによる
サーバー単位の保護

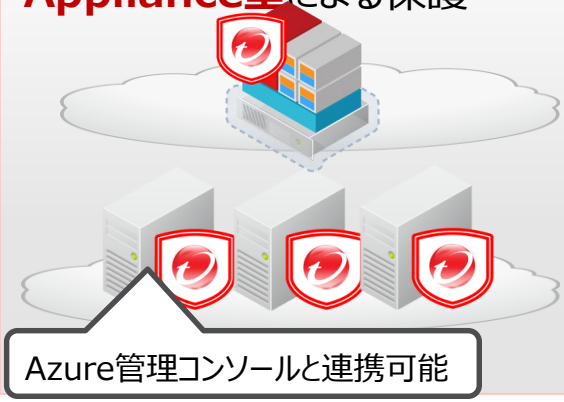
仮想環境

Virtual Appliance型に
よるESXi単位での保護



クラウド環境

エージェント型又は**Virtual Appliance型**による保護



多層防御

セキュリティ機能	内容
ファイアウォール	攻撃を受ける機会を軽減します。
侵入防御（IDS/IPS）	脆弱性を突いた攻撃からサーバを保護します。
セキュリティログ監視	重要なセキュリティイベントを早期に発見します。
変更監視	ファイルの改ざん等を早期に発見します。
不正プログラム対策	ウイルス等の不正プログラムを検出します。

クラウドセキュリティを考えるための
3つのポイント

1．Auto Scalingに対応！

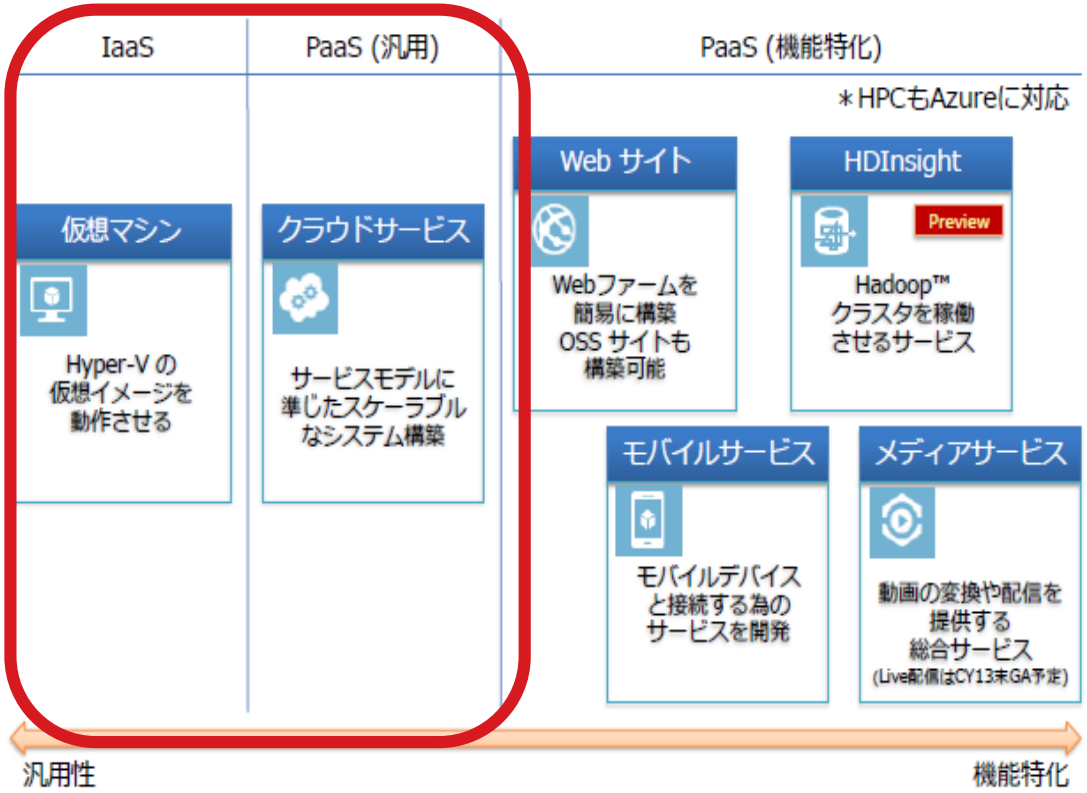
2．クラウド環境にはホスト型が最適！

3．複数の機能で、多層防御を実現！

Trend Micro Deep Security
なら
すべて実現可能です！

Deep Securityのサポート対象

- Windows Azure のサーバリソースを用途に応じて選択
  - 組み合わることでより柔軟なシステム構築が可能



コンピューティングリソース	説明
App Service（PaaS）機能特化	任意のデバイス用のスケーラブルな Web Apps、Mobile Apps、API Apps、Logic Apps
クラウドサービス（PaaS）汎用	OS のより詳細な制御が可能な、可用性と拡張性の高い N 階層のクラウド アプリケーション
仮想マシン（IaaS）	OS の完全な制御が可能な、カスタマイズされた Windows と Linux V

参考URL:https://azure.microsoft.com/ja-jp/documentation/articles/cloud-services-choose-me/

Q&A

TREND MICRO

ご清聴頂きまして
ありがとうございました。

Appendix

クラウドサービス（Cloud Services）について

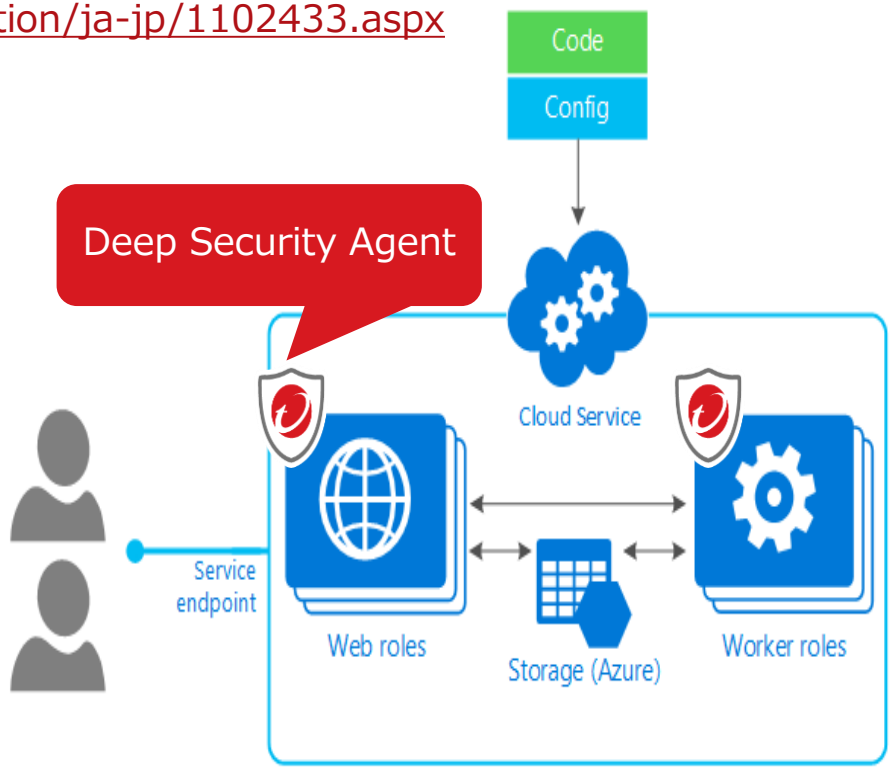
- Cloud Services は、サービスとしてのプラットフォーム (PaaS) の 1 つの例です。
- スケーラブルで信頼性が高く、運用コストが低いアプリケーションをサポートするように設計されています。
- Cloud Services も VM 上でホストされています。しかし、VM に対してより多くのコントロールが可能です。独自のソフトウェアを Cloud Services の VM にインストールして、リモートで操作できます。
- 2 つの VM オプションが用意されています。
  - Web ロール：IIS に自動的にデプロイされた Web アプリを搭載した Windows Server を実行
  - Worker ロール：IIS を搭載していない Windows Server を実行

Deep SecurityのPaaSサポートについて

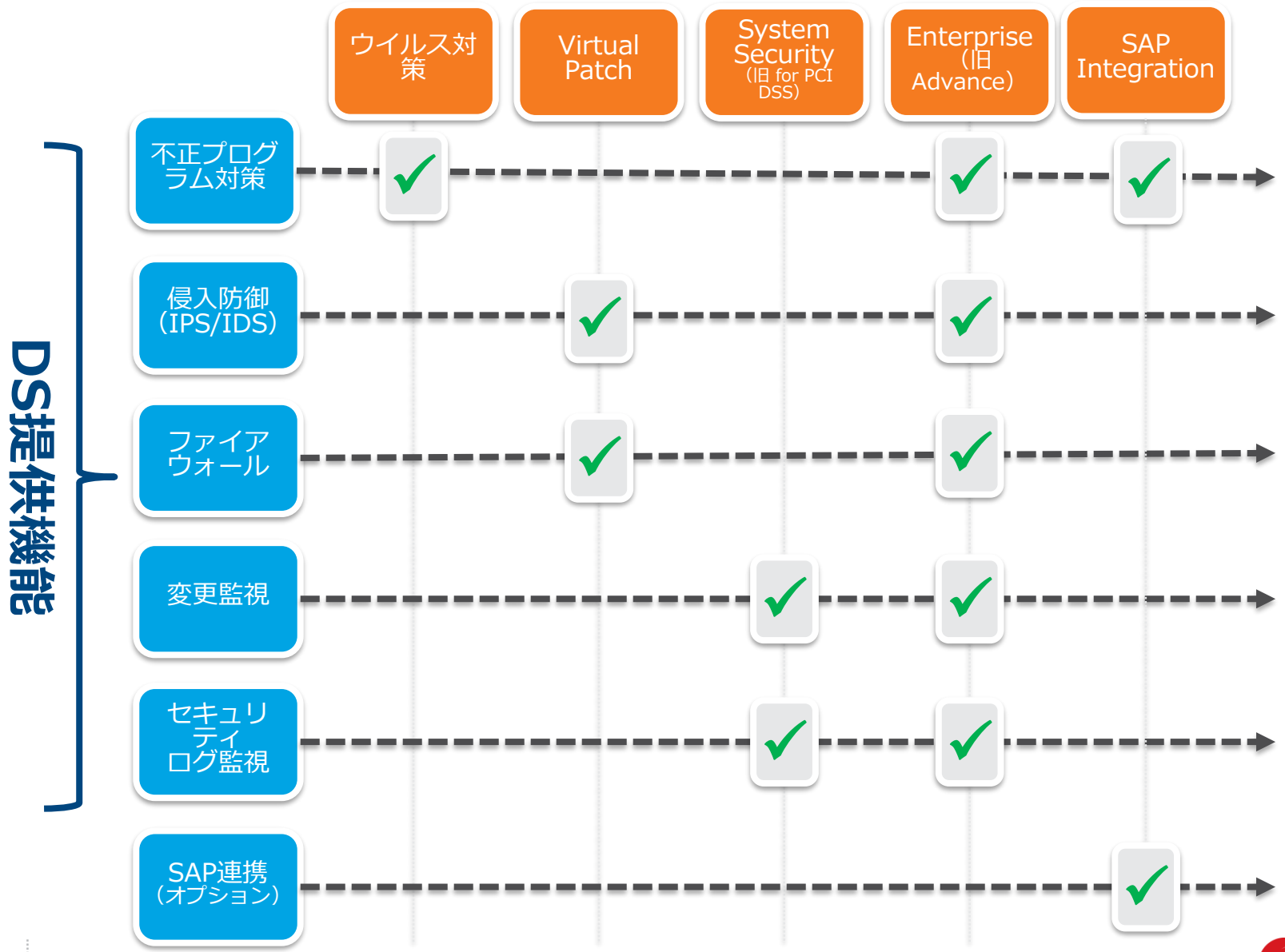
- Deep Security AgentをCloud Services のVMにインストールし、セキュリティ機能を提供することをサポートします。
  - App Service（PaaS機能特化）につきましてはサポート外となります。

参照URL:http://esupport.trendmicro.com/solution/ja-jp/1102433.aspx

※すべての機能に関して動作確認を行っているわけではございません。問題発生時、調査結果により仮想マシン、クラウドサービス固有の環境による問題であることが判明した場合は、サポート対象外となることがあります。十分な事前検証の上、ご利用いただけますようお願いいたします。



ライセンス構成（サーバ課金）



ラインナップ価格表

課金単位	新名称	新規	更新
サーバ課金	Deep Security Agent Enterprise※1	¥213,000	¥106,500
	Deep Security Agent Virtual Patch	¥125,000	¥62,500
	Deep Security Agent System Security	¥107,000	¥53,500
	Deep Security Agent ウイルス対策※1	¥98,000	¥49,000
CPU課金	Deep Security Virtual Appliance Enterprise	¥400,000	¥200,000
	Deep Security Virtual Appliance Virtual Patch	¥240,000	¥120,000
	Deep Security Virtual Appliance System Security	¥210,000	¥105,000
	Deep Security Virtual Appliance ウイルス対策	¥160,000	¥80,000
CPU課金	Deep Security Enterprise Suite	¥630,000	¥315,000
サーバ課金	Deep Security for SAP Systems	¥2,200,000	¥1,100,000

※1.ServerProtect for Windows, Linux同梱