

NS407

目的地は柔軟性の高いマルチクラウド採用!
～VMware Cloud on AWSでも
柔軟に対応できるセキュリティ対策への
離陸準備とは？～

トレンドマイクロ株式会社
セキュリティエキスパート本部
パートナービジネスSE部パートナーSE2課
VMware vExpert
シニアセールスエンジニア 栃沢 直樹

#vforumjp

vmware®

POSSIBLE
BEGINS
WITH YOU



自己紹介

名前：柄沢 直樹 Tochizawa Naoki  VMware vEXPERT

会社：トレンドマイクロ株式会社

所属：パートナービジネスSE部 パートナーSE2課

- VMware関連専任エンジニア
- ビジネスパートナー様への技術支援
- お客様への案件提案・レクチャ



前職：SIerでネットワークセキュリティ/運用設計SE・マーケティング

社外活動：

日本ネットワークセキュリティ協会（JNSA）アイデンティティ管理WG

趣味：野球観戦（春～秋）、スキー（冬）

- クラウド採用時に直面する課題と整理のポイント
- VMware Cloud on AWSでも「効果」を発揮する Deep Security
- VMware Cloud on AWSとDeep Securityの連携を実際に活用するには

マルチクラウド時代を
“セキュアフライト（簡単・安心）”
して頂きたい！





クラウド環境におけるセキュリティ対策の悩み

そもそもクラウド環境におけるセキュリティ対策を
どのように考えればよいのか？

複数のインフラでのセキュリティ対策レベルの統一を
どのように図るか

オンプレミス（仮想化環境）とパブリッククラウドを
移動するサーバのセキュリティをどのように担保するか

簡易に作成されて、増加していくサーバにどう対応するか



Operations

■ クラウド環境におけるセキュリティ対策への解決の道

やるべきことは一緒
ただし、インフラの特性を理解して活用する

インフラの側面から共通化できる
セキュリティ指針と対策を採用する

インフラの状況にリアルタイムに
反応できる仕組みを担保する

セキュリティ実装の自動化を行う



Operations

■ クラウド環境におけるセキュリティ対策への解決の道

やるべきことは一緒
ただし、インフラの特性を理解して活用する

インフラの側面から共通化できる
セキュリティ指針と対策を採用する

インフラの状況にリアルタイムに
反応できる仕組みを担保する

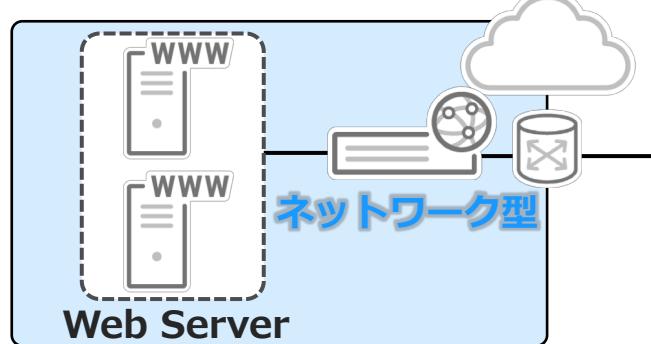
セキュリティ実装の自動化を行う



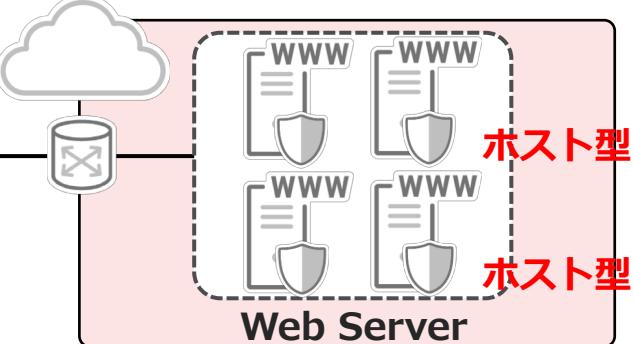
Operations

■ インフラの特性の理解 - 境界型セキュリティのみの限界

オンプレミス環境



パブリッククラウド環境

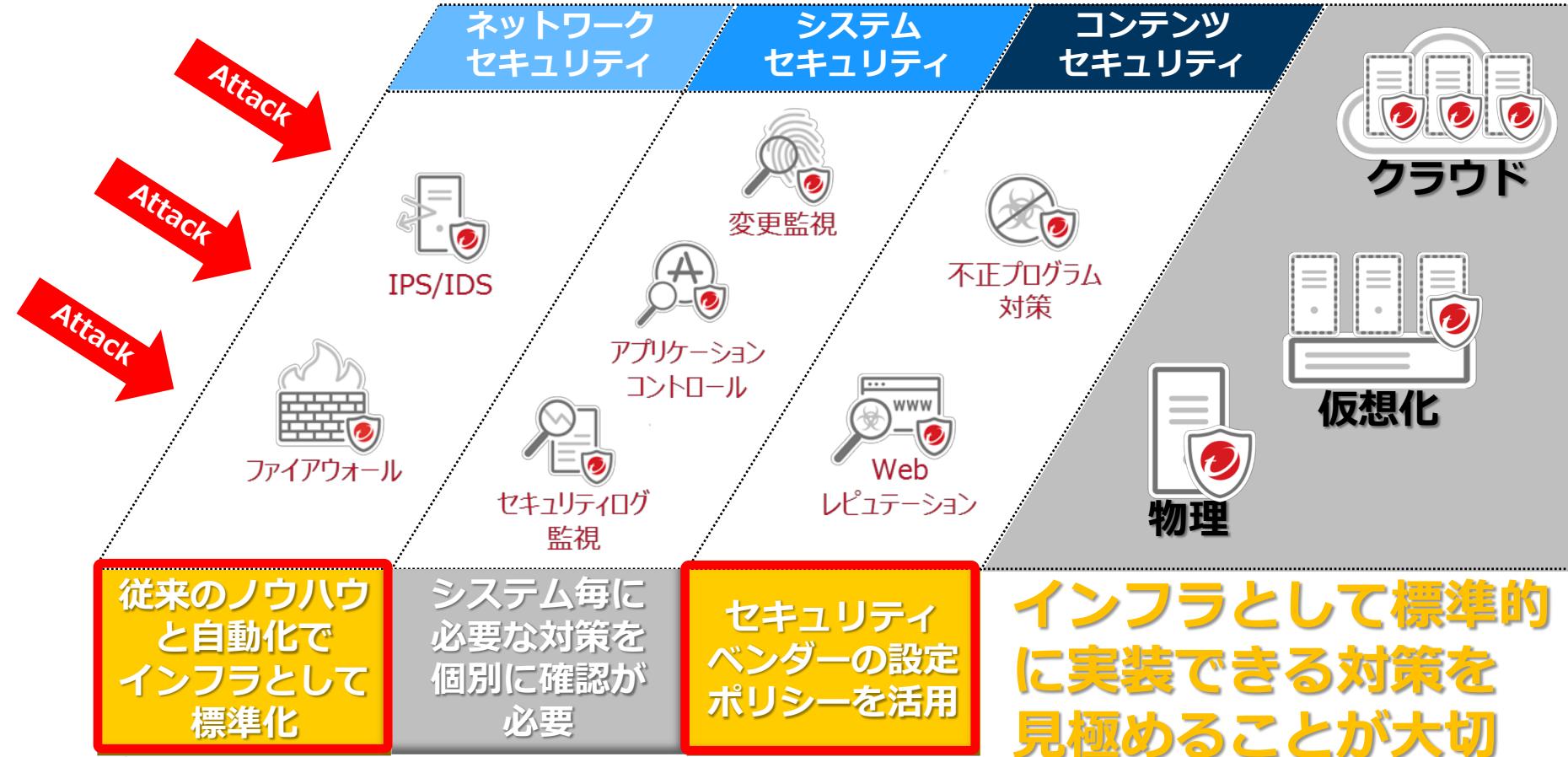


階層ネットワーク（複雑になりがち）
単一障害ポイントにケア
ゲートウェイ型での入口対策
将来を見据えた投資

フラットなネットワーク
ボトルネックのケアは不要
ホスト単位での内部拡散防止
柔軟なキャパシティ設計

ゲートウェイ型セキュリティの利点を生かしつつ、パブリック
クラウド的な考え方を環境問わず採用される方向に

■ インフラ担当者から見たサーバセキュリティの現実解



■ クラウド環境におけるセキュリティ対策への解決の道

やるべきことは一緒
ただし、インフラの特性を理解して活用する

インフラの側面から共通化できる
セキュリティ指針と対策を採用する

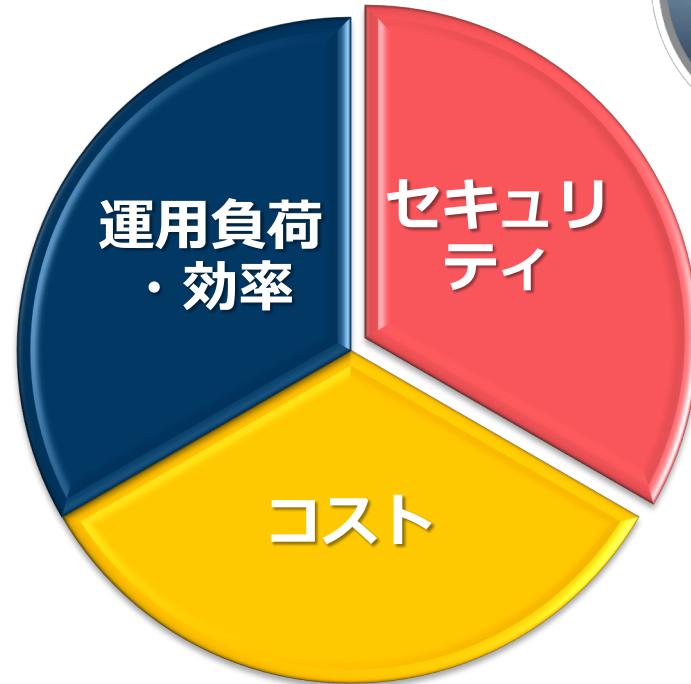
インフラの状況にリアルタイムに
反応できる仕組みを担保する

セキュリティ実装の自動化を行う



Operations

■ インフラセキュリティの課題



Operations

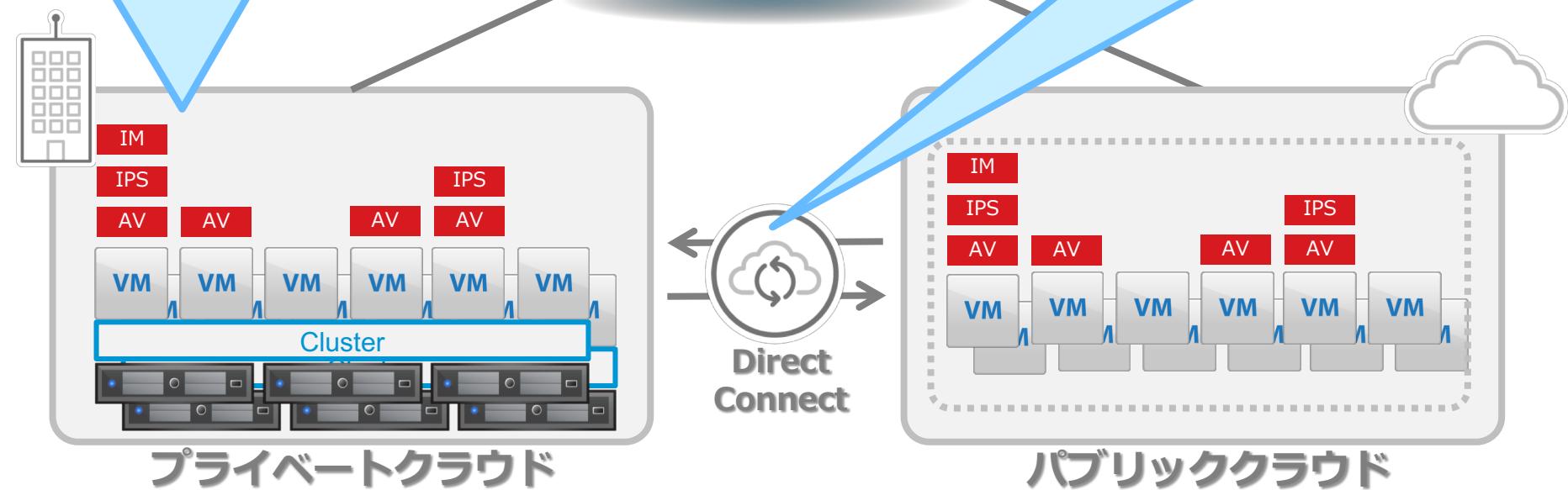
“セキュリティ”は、“コスト”“運用”に比べるとプライオリティは下がってしまう。

“セキュリティ”は“コスト”“運用”と両立がしづらいし、投資対効果が説明しづらいなあ（社内稟議を通すのが大変。。。）

■ サーバ・ネットワークから切り離されたITセキュリティ

1台ずつ手動で導入
本当にすべて適切に実装でき
ているか確認する手段がない

VMを移行する際にセキュリ
ティポリシーの見直しが発生



システム全体がセキュリティポリシーに則っているのか把握できず
実質的には運用できない

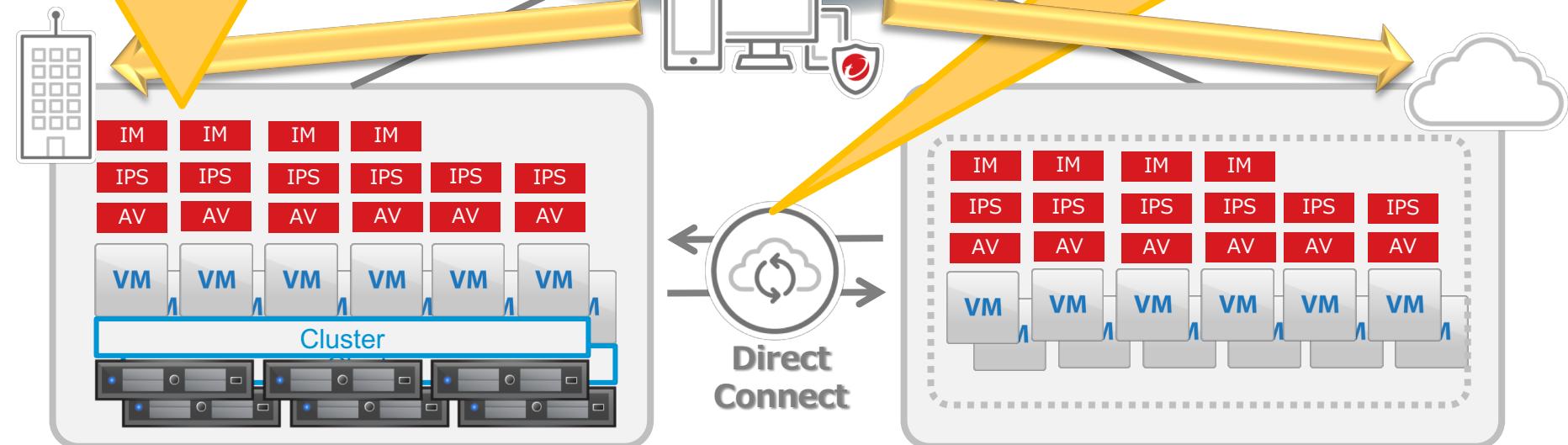
■ インフラ基盤にシームレスに連動したセキュリティ実装

VMに配置される

セキュリティ実装を統一管理
できる

基盤と連携した
可視化と自動化

VMの新規デプロイ、移行に
シームレスに対応できる



プライベートクラウド

パブリッククラウド

アプリケーション・サーバに依存しない統一的なセキュリティ実装
サーバの重要度、カテゴリに応じたポリシーの適用と実装の可視化



マルチクラウドへの移行に向けたポイント



そもそもクラウド環境におけるセキュリティ対策を
どのように考えればよいのか？

複数のインフラでのセキュリティ対策レベルの統一を
どのように図るか

オンプレミス（仮想化環境）とパブリッククラウドを
移動するサーバのセキュリティをどのように担保するか

簡易に作成されて、増加していくサーバにどう対応するか

やるべきことは一緒に
ただし、インフラの特性を理解して活用する

インフラに依存しない
セキュリティ指針と対策を採用する

インフラの状況にリアルタイムに
反応できる仕組みを担保する

セキュリティ実装の自動化を行う



どうやって?
VMware Cloud on AWS
&
Deep Securityの
コラボレーションで具体的
に解決できます

VMware Cloud on AWS with Deep Security



VMware Cloud on AWS

オンプレミス環境とシームレスに接続しつつ、パブリッククラウドのメリットを享受できる最適なソリューション

On-Premises

vmware®



Storage



VMware NSX®



VMware Cloud on AWS



VMware vCenter®



Virtual SAN



VMware NSX®

VMware ESXi™

Dedicated AWS Infrastructure

AWS Cloud





Disaster Recovery

一時的なリソース
需要への対応

インフラ管理からの
開放

既存のオンプレミス環境とのシームレスな接続が可能となる



On-Premises

VMware Cloud on AWS with Deep Security



Deep Security Manager

On-Premises

vmware®

Deep Security Agent



Storage



VMware NSX®

Deep Security Virtual Appliance (DSVA)

VMware Cloud on AWS



VMware vCenter®

Deep Security Agent



Virtual SAN



VMware NSX®

VMware ESXi™

Dedicated AWS Infrastructure

AWS Cloud



Deep Security Agent



■ Deep Securityとは？（おさらい）

Trend Micro Deep Securityは、サーバセキュリティに必要な複数の機能を1つの保護モジュールに実装した総合サーバセキュリティ対策製品です。

単一製品でコストと運用負荷を最小化しつつ、社内サーバのセキュリティポリシーを統一化

VM環境の
サーバ
要塞化

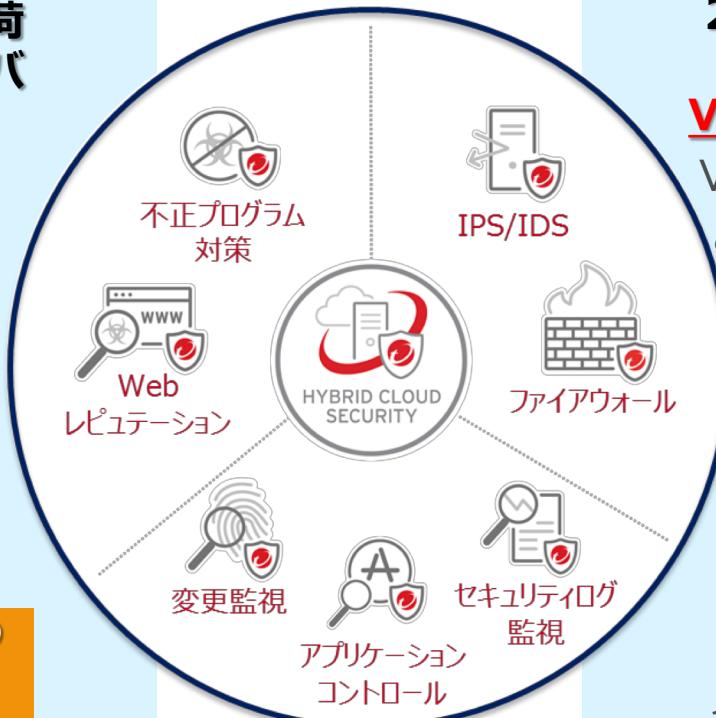
標的型
サイバー
攻撃対策

VDI環境の
セキュリ
ティ対策

PCI DSS
準拠支援

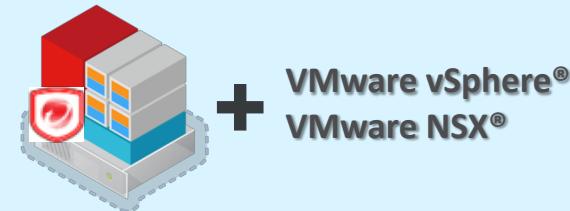
レガシーOS
延命利用
対策

クラウド環境の
セキュリティ
対策



2つの防御コンポーネント
Deep Security
Virtual Appliance(DSVA)

VMware ESXi、VMware NSX®
と連携してエージェントレスで
セキュリティ機能を提供



+ VMware vSphere®
VMware NSX®

Deep Security
Agent(DSA)

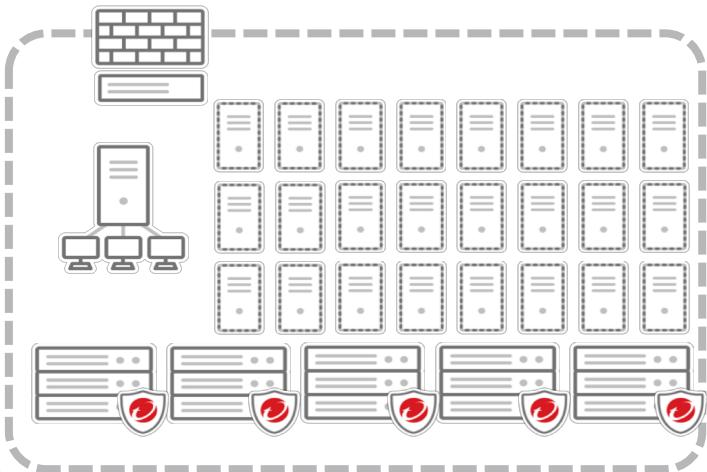


仮想マシンOS上に
インストールしてすべての
セキュリティ機能を提供



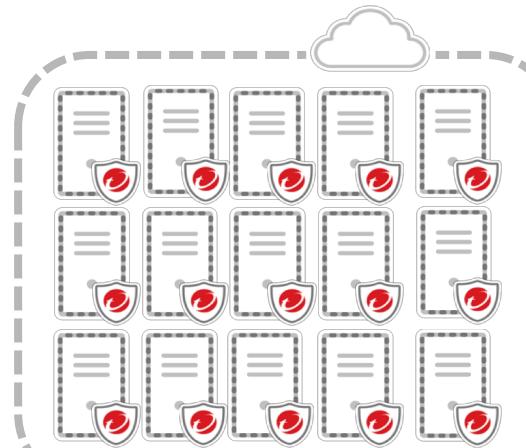
Single Management, Simple Security by Deep Security

オンプレミス プライベートクラウド



Deep Security

AWS/Azureを はじめとしたパブリック クラウド



すべての環境をシングル
コンソールで可視化

インフラ環境に依存しない
シンプルなセキュリティ実装

マルチクラウド環境にシングルコンソールで対応

VMware Cloud on AWS with Deep Security 連携ポイント

■ポイントとなる機能



事前準備

VMware vCenter Server®と
Deep Security Managerの接続
[セキュリティ実装を統合的に可視化]



インスタンス の展開

セキュリティ適用の徹底
[インスタンスの生成・クラウド間移行時の自動化]



運用開始後

セキュリティ運用の負荷軽減
[パッチマネジメントの自動化]

VMware vCenter Server®への接続準備

VMware Cloud on AWS

SDDCs Subscriptions Activity Log Tools Developer Center

Software-Defined Data Centers (SDDC)

This SDDC will expire in 29 days. [LEARN MORE](#)

[BACK TO LIST](#) [SCALE UP](#)

ntochizawa-SDDC Asia Pacific (Sydney)

[ACTIONS](#) [OPEN VCENTER](#)

Summary Network Add Ons Troubleshooting Settings Support

[HIDE SYSTEM DIAGRAM](#)

Management Gateway

Public IP: 54.66.174.198
Appliance Subnet - 10.104.128.0/23
Infrastructure Subnet - 10.104.128.0/23

vCenter NSX

No VPN configured
Default Deny All

Actions

Default Deny All

On Prem

Management Gateway

IPsec VPNs

Firewall Rule Accelerator

Firewall Rules

Role Name Action Source Destination Service Ports

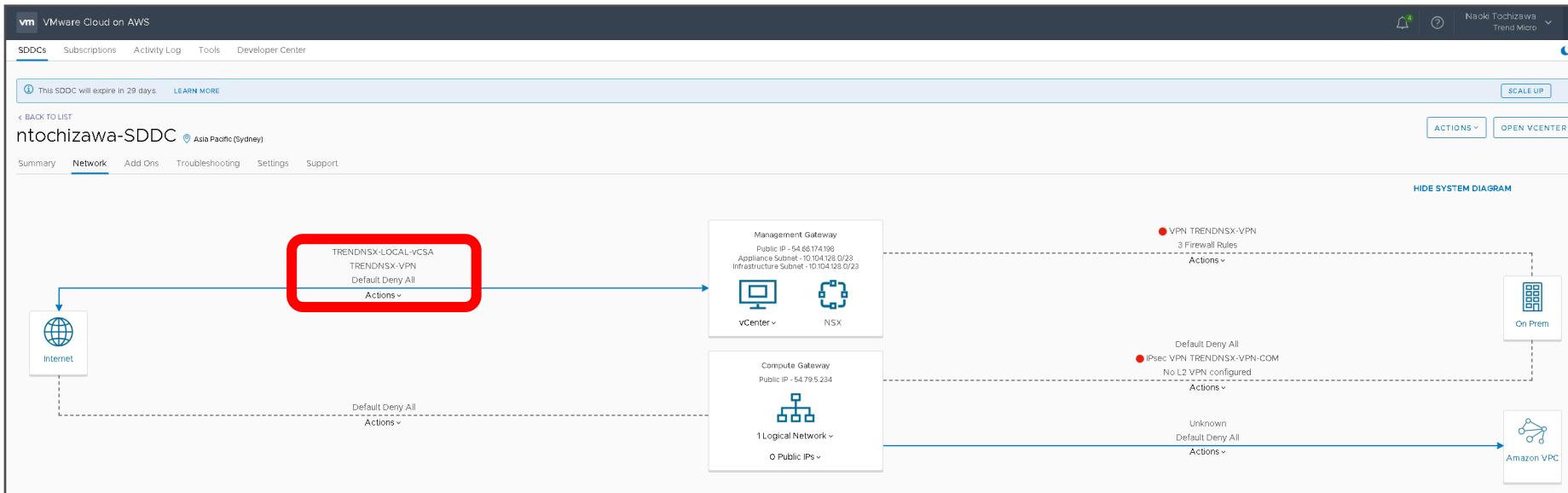
Default Deny All Deny Any Any (All Traffic) Any

TRENDNSX-LOCAL-vCSA Allow 1 vCenter HTTPS (TCP 443) 443

[SAVE](#) [CANCEL](#)

DNS 8.8.8 8.8.4.4 vCenter FQDN Resolution: Public IP (52.66.179.46)

■ VMware vCenter Server®への接続準備

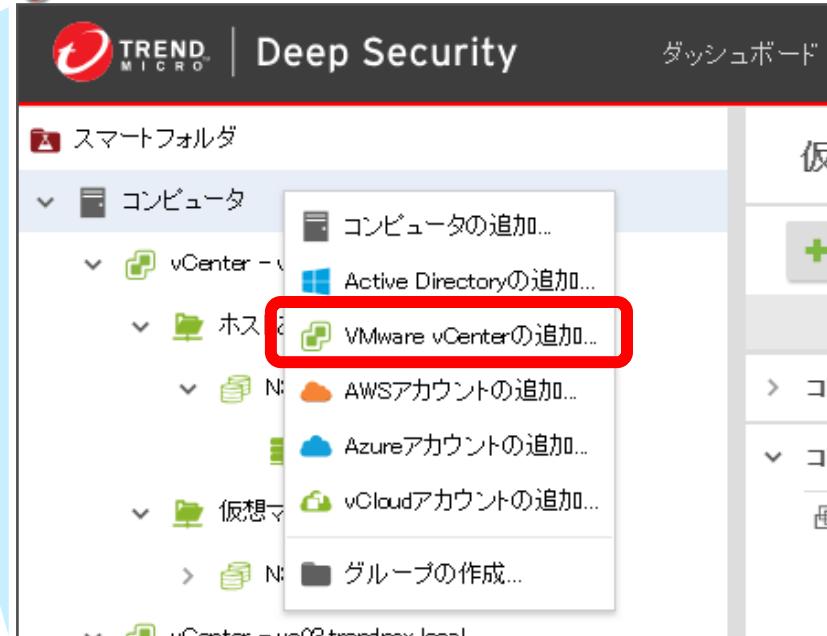


インターネット経由またはVPN経由でのManagement Gatewayへの接続を選択可能

■ VMware vCenter Server®とDeep Security Managerの接続

事前準備

Deep Security Manager



オンプレミスのVMware vCenter Server®と
同様の手順でVMware Cloud on AWSとも
同期設定を行う

■連携前:オンプレミスのVMware vCenter Server®配下のホスト・VM情報が同期

Deep Security Managerで複数のvCenter Server®を管理可能

The screenshot shows the Trend Micro Deep Security Manager interface. On the left, there's a navigation sidebar with a 'Smart Folder' section containing 'コンピュータ' (Computers). Under 'コンピュータ', there are two entries: 'vCenter - vc02.trendnsx.local' and 'vCenter - vc03.trendnsx.local'. Both entries have sub-folders for 'ホストおよびクラスタ' (Hosts and Clusters), 'NSX', and 'Server-Cluster'. The 'vCenter - vc02.trendnsx.local' entry also has a '仮想マシン' (Virtual Machines) folder. A red box highlights these two vCenter entries. On the right, the main pane displays a table of computer assets. The columns are '名前' (Name), '説明' (Description), 'プラットフォーム' (Platform), and 'ポリシー' (Policy). The table shows three entries under 'コンピュータ (3)': 'TMCM01' (不明, Windows), 'DSM04.trendnsx.local' (Microsoft Win..., Deep Security Manager), and 'AM-WIN10-12DSA' (不明, なし). Below this, there are sections for 'コンピュータ > vCenter - vc02.trendnsx.local > ホストおよびクラスタ > NSX > Server-Cluster (1)', 'コンピュータ > vCenter - vc02.trendnsx.local > 仮想マシン > NSX (4)', and 'コンピュータ > vCenter - vc02.trendnsx.local > 仮想マシン > NSX > ESX Agents (2)'. At the bottom, there's another section for 'コンピュータ > vCenter - vc03.trendnsx.local > ホストおよびクラスタ > NSX > Server-Cluster (1)'. The bottom right corner features the Trend Micro logo.

名前	説明	プラットフォーム	ポリシー
TMCM01	不明	Windows	
DSM04.trendnsx.local	Microsoft Win...	Deep Security Manager	
AM-WIN10-12DSA	不明	なし	



VMware Cloud on AWS環境にDeep Security Managerを接続

The screenshot illustrates the process of connecting a VMware vCenter instance to the Deep Security Manager. It shows three main windows:

- Left Window (Deep Security Manager UI):** Shows the "Compute" section of the dashboard. A red box highlights the "VMware vCenterの追加..." (Add VMware vCenter) button under the "Compute" category.
- Middle Window (VMware vCenter Add Wizard):** The first step of the wizard, titled "追加するvCenterの次の" (Next step for adding vCenter). It asks for the server address and port, and includes fields for name, description, and credentials. A red box highlights the "NSX Manager" section.
- Right Window (Deep Security Manager Confirmation):** A confirmation dialog from the Deep Security Manager. It lists the resources that will be added upon connection: "1個のデータセンター", "1台のホスト", and "1台の仮想マシン".

Three large grey arrows point from left to right, indicating the flow of the connection setup.

Bottom navigation buttons: く戻る (Back), 完了 (Finish), キャンセル (Cancel).

Page footer: Copyright © 2018 Trend Micro Incorporated. All rights reserved.

■連携後: DSMからオンプレミスとVMware Cloud on AWSの環境を一元管理

Deep Security Managerでオンプレミスに加えて、
VMware Cloud on AWSを管理するVMware vCenter®も同期

The screenshot displays the Trend Micro Deep Security web interface. On the left, a sidebar shows a tree view of managed environments:

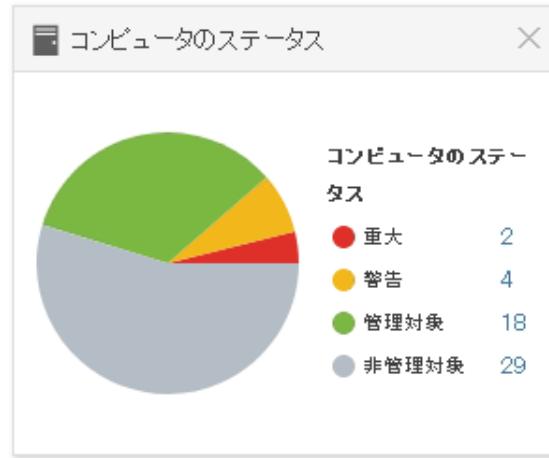
- スマートフォルダ
- コンピュータ
 - vCenter - vc02.trendnsx.local
 - vCenter - vc03.trendnsx.local
 - ホストおよびクラスタ
 - NSX
 - Server-Cluster
 - 仮想マシン
 - vCenter - vcenter.sddc-.vmwarevm.com
 - ホストおよびクラスタ
 - 仮想マシン

The main panel shows the "vCenter - vcenter.sddc-.vmwarevm.com" environment selected. The top navigation bar includes links for Dashboard, Processing, Alerts, Events & Reports, Computer, Policy, and Management.

The central area displays a list of managed hosts and virtual machines, with a specific entry for a host named "vcenter.sddc-.vmwarevm.com" highlighted in blue.

■セキュリティ実装の可視化～インベントリ情報の自動同期

VMware vCenter®上で管理される仮想マシンのDeep Securityのポリシー適用状況が一目瞭然で管理でき、ポリシーの適用漏れなども可視化できる



TREND MICRO | Deep Security

ダッシュボード 極度 アラート イベントとレポート コンピュータ ポリシー 管理

スマートフォルダ
CloneVM
DSM
DSVA

コンピュータ
vCenter - vc01.trendnsx.local
ホストおよびクラスタ
NSX
Manage
VDI
仮想マシン
NSX
Discovered virtual machine
ESX Agents

NSX サブループを含む ▾ グループ化しない ▾

ステータス	NSXセキュリティグループ	ポリシー
管理対象 (VM停止)	TRENDNSX-VDI	Windows VDI
管理対象 (VM停止)	TRENDNSX-VDI	Windows VDI
管理対象 (VM停止)	TRENDNSX-VDI	Windows VDI
管理対象 (オンライン)	TRENDNSX-VDI	Windows VDI
管理対象 (オンライン)	TRENDNSX-VDI	Windows VDI
管理対象 (オンライン)	TRENDNSX-VDI	Windows VDI
管理対象 (オンライン)	TRENDNSX-VDI	Windows VDI
管理対象 (オンライン)	TRENDNSX-VDI	Windows VDI
管理対象 (オンライン)	TRENDNSX-VDI	Windows VDI
管理対象 (オンライン)	Deep Security	Deep Security
管理対象 (オンライン)	Deep Security	Deep Security
非管理対象 (Agentなし)	TRENDNSX-VDI	Windows VDI
非管理対象 (Agentなし)	TRENDNSX-VDI	Windows VDI

■セキュリティ適用の徹底

インスタンス の展開

マルチクラウド環境でセキュリティ適用を行う上で留意しておくべきタイミングは以下の2つのポイント。

新規インスタンス
展開時



インストールスクリプトの利用

インスタンスの
クラウド間移行時



イベントタスクの設定

仮想マシンごとに適用するべきポリシーを自動的/確実に適用可能

■ インストールスクリプトの利用

DSMコンソール上から簡単にスクリプトを生成可能

The screenshot shows the Trend Micro Deep Security Manager interface. In the top navigation bar, 'Deep Security' is selected. On the right, there's a dropdown for 'MasterAdmin' and links for 'ニュース', 'ヘルプ', and 'サポート情報'. A red box highlights the 'インストールスクリプト' link in the dropdown menu.

The main content area is titled 'インストールスクリプト'. It contains a note about using RightScale, Chef, Puppet, and SSH tools to distribute the Agent. Below this, a dropdown menu is set to 'Linux版Agentのインストール'. A yellow callout box points to this dropdown with the text 'OSごとにスクリプトを選択' (Select script by OS) and lists 'Window : Power Shell' and 'Linux : Bash'.

Below the dropdown, there's a checkbox for 'インストール後にAgentを自動的に有効化 (セキュリティポリシーを割り当てる場合は必ず有効化してください)' (Enable Agent automatically after installation (Enable this if you assign security policies)). A red box highlights the 'セキュリティポリシー:' dropdown, which is set to 'Base Policy > Linux Server'. A yellow callout box points to this section with the text '適用するポリシーも指定可能' (You can also specify the policy to apply).

At the bottom of the page, there are buttons for 'ファイルに保存...' (Save to file...), 'クリップボードにコピー' (Copy to clipboard), and '閉じる' (Close).

OSごとにスクリプトを選択
Window : Power Shell
Linux : Bash

適用するポリシーも指定可能

■ インストールスクリプトの利用

スクリプトファイルをOSの起動プログラムとして追加

```
#!/bin/bash
# This script detects platform and architecture, then downloads and installs the
if [[ $(/usr/bin/id -u) -ne 0 ]]; then echo You are not running as the root user. Please try again with root privileges.
logger -t You are not running as the root user. Please try again with root privileges.
exit 1;
fi.

if type curl >/dev/null 2>&1; then
SOURCEURL='https://DSM04.trendnsx.local:4119'
curl $SOURCEURL/software/deploymentscript/platform/linux/ -o /tmp/DownloadInstallAgentPackage --insecure --silent --tlsv1.2

if [ -s /tmp/DownloadInstallAgentPackage ]; then
./tmp/DownloadInstallAgentPackage
Download_Install_Agent
else
echo "Failed to download the agent installation script."
logger -t Failed to download the Deep Security Agent installation script
false
fi
else
echo "Please install CURL before running this script."
logger -t Please install CURL before running this script
false
fi
sleep 15
/opt/ds_agent/dsa_control -r
/opt/ds_agent/dsa_control -a dsm://DSM04.trendnsx.local:4120/ "policyid:3"
```

スクリプト生成したDeep Security Managerからエージェントパッケージをダウンロード

エージェントの有効化と
ポリシーの適用

■ イベントベースタスクの設定

イベントベースタスク

オンプレミス側から移動した仮想マシンの生成（新規UUID）
に対してDeep Securityのポリシーを自動有効化する機能

The screenshot shows the Trend Micro Deep Security interface. The left sidebar has a tree view with categories like System Settings, Scheduled Tasks, and Event-Based Tasks (which is selected and highlighted in blue). The main area is titled 'Event-Based Task' and contains a sub-section 'Event-Based Task Wizard'. A sub-task window titled 'Event-Based Task Wizard - Google Chrome' is open, showing a warning about unencrypted communication. The main content of the wizard asks to select an event for task execution, with a dropdown menu showing 'Event: Computer creation (System)'.

[コンピュータの作成（システムによる）]
他のVMware vCenter®配下から
移動したインスタンスは移行後の
VMware vCenter®配下では新規UUID
として認識される

■ポリシーの有効化タスクを設定

VMware NSX®のセキュリティグループ・ポリシーの設定と 同様の設定

イベントベースタスクウィザード - Google Chrome
保護されていない通信 | https://10.3.225.184:4119/EventBasedTaskWizard.screen

実行する操作を選択してください。

コンピュータの有効化
有効化の遅延(分): 0

コンピュータの無効化

ポリシーの割り当て:
なし
Demo_Suido_DSR
Linux Server
Demo_Standard_Linux Server
Solaris Server

Relayグループの割り当て:

コンピュータグループへの割り当て:

移行時に自動的に セキュリティポリシー適用

一致条件をすべて指定してください(すべての条件が満たされた場合にのみ操作が実行されます)。

選択... 選択... = CENT *

- Appliance保護が利用可能
- Appliance保護が有効化済み
- ESX名
- NSXセキュリティグループ名
- vCenter名
- クラウドアカウント名
- クラウドインスタンスのイメージID
- クラウドインスタンスのセキュリティグループ名
- クラウドインスタンスのメタデータ
- コンピュータ名
- フォルダ名
- プラットフォーム

■セキュリティ運用の負荷軽減

運用開始後

インフラ側面からサーバのセキュリティ対策で求められる
最低限の対策

不正プログラム
対策

アクセス制御

脆弱性対策

- ・ 対策の必要性の判断
- ・ 適用前の事前テスト
- など運用負荷が高い

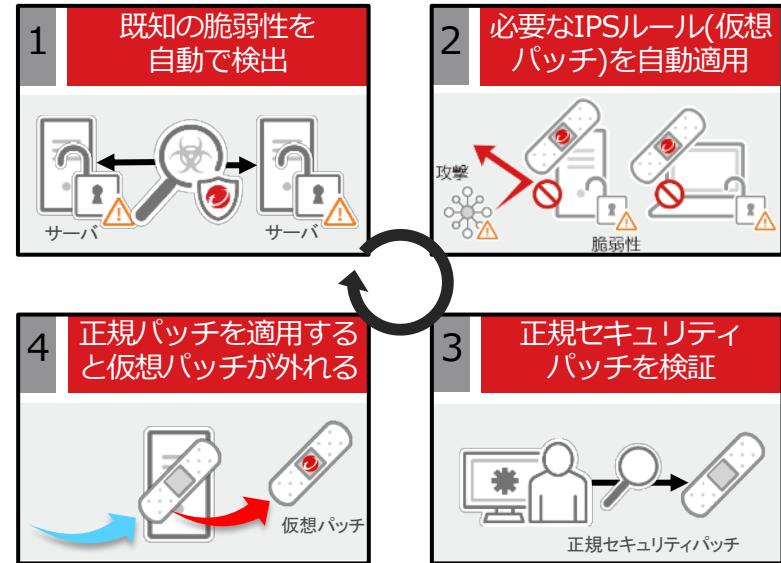
■ Deep Securityを利用したパッチマネジメントの自動化機能

推奨設定の検索

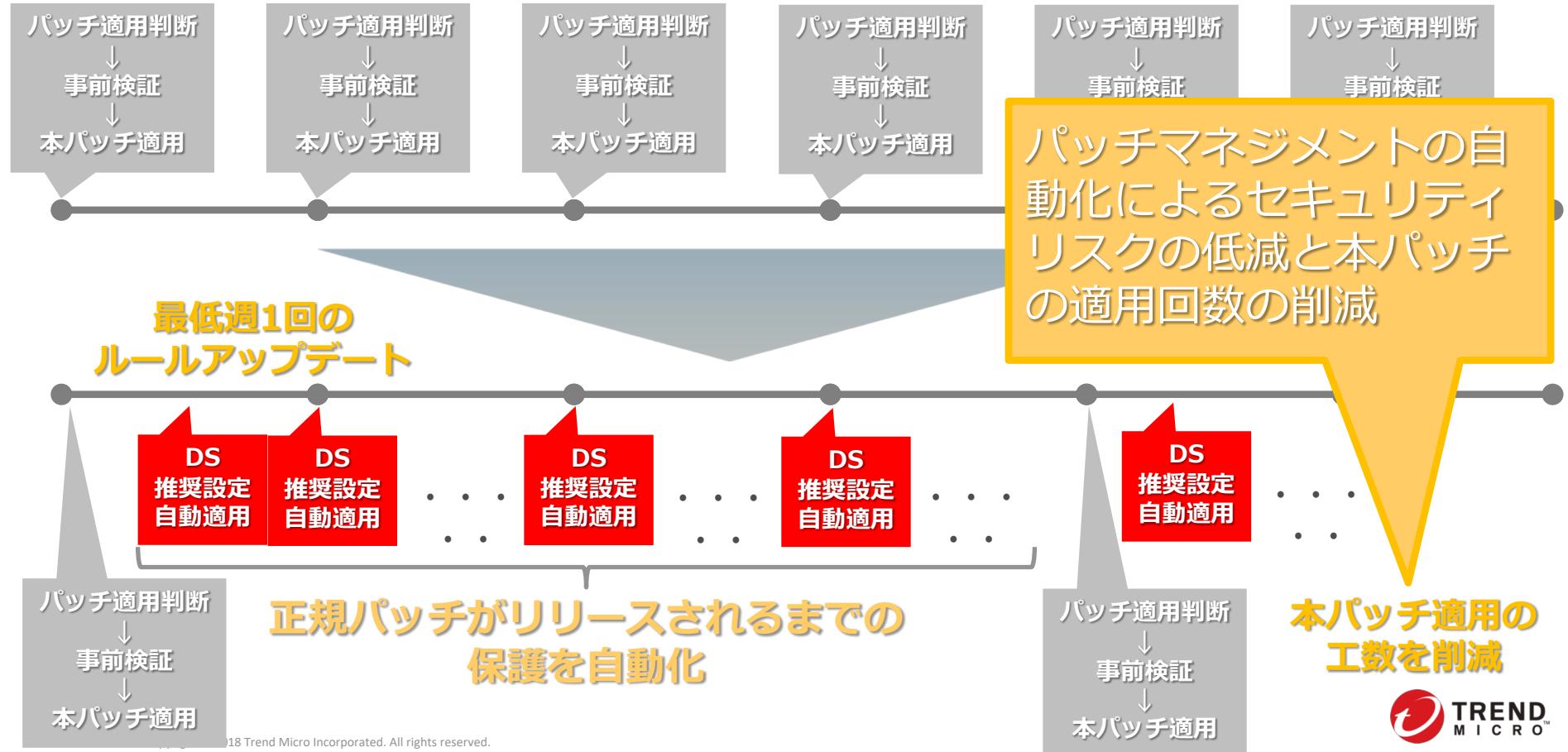
インスタンス単位で管理しているDeep SecurityはOS・アプリ・パッチ適用の有無を最新ルールをベースに検索可能
= ホスト型セキュリティのメリット

推奨設定の検索をかけることで、
下記処理を自動で実行することが可能

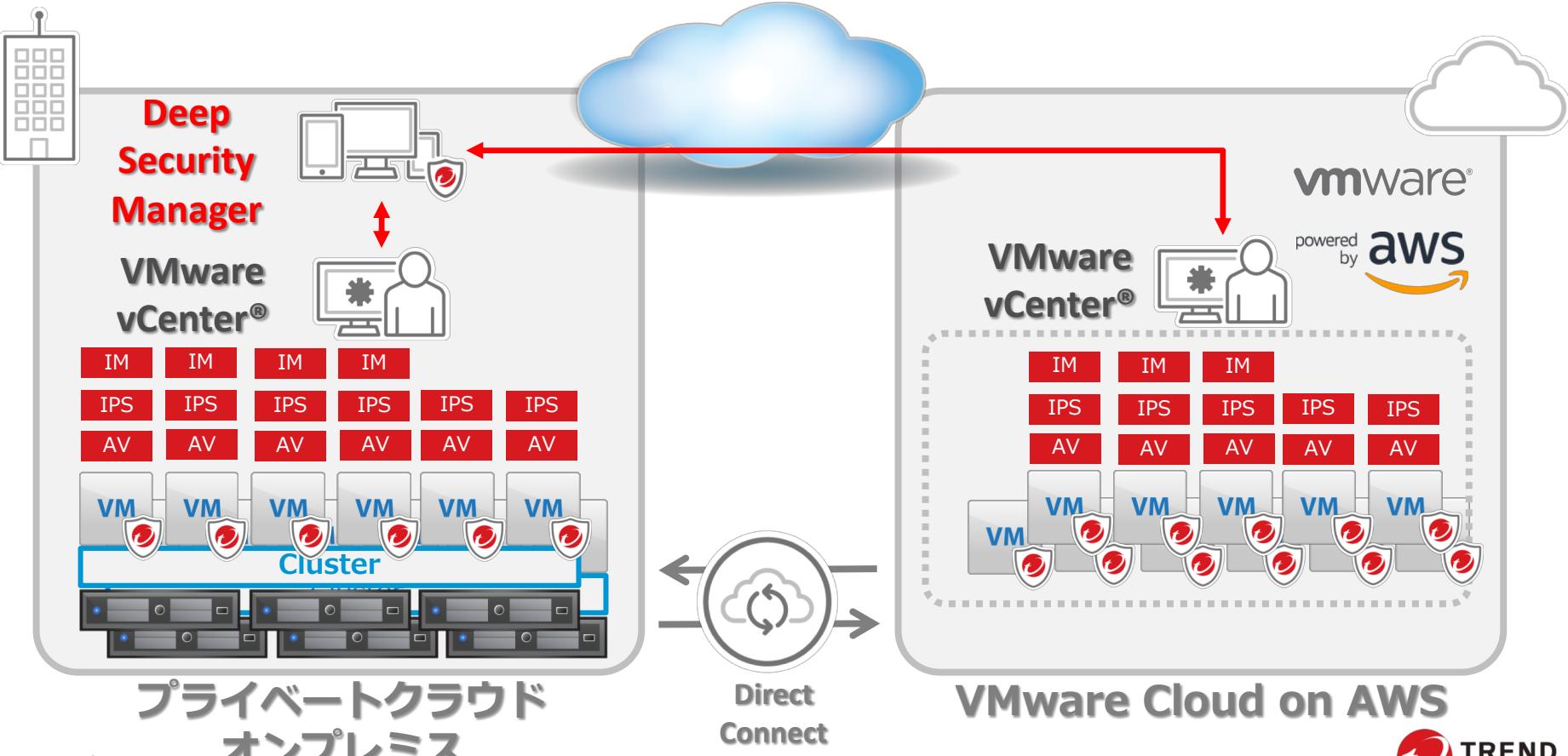
1. 内在する脆弱性を検知して
対応するルール（仮想パッチ）を
適用する
2. 正規パッチの適用後、不要な
ルール（仮想パッチ）を検知し
取り外す



■パッチマネージメントの効率化とコスト低減



■ Deep SecurityによるVMware Cloud on AWS移行にも対応した実装



まとめ

【課題解決のポイント】

インフラと連動した可視化
(説明責任)

セキュリティ実装の自動化
(自動化)

運用を軽減するセキュリティ実装
(運用効率化)



VMware vCenter®
とDSMの連携



インストールスクリプト
イベントベースタスク



パッチマネジメント
(推奨設定の検索)



VMware Cloud on AWS with Deep Securityで実現するゴール

“セキュアフライト（簡単・安心）”
マルチクラウド時代を
して頂きたい！



と連動した可視化
(説明責任)

セキュリティ実装の自動化
(自動化)

運用を軽減するセキュリティ実装
(運用効率化)



無理なくインフラ運用が
継続
できるセキュリティ対策

■トレンドマイクロ ブース紹介

ぜひ、アンケートにご質問、ご感想をいただければと思います



**詳しくはトレンドマイクロブースに
お越しください。**