「VMware仮想化基盤におけるPCI DSS実装方法について」

～PCI DSS3.0で追加される新たな要件。仮想化基盤上で対応するには？～

トレンドマイクロ株式会社
ソリューションマーケティング部
福井　順一

2014年7月29日

PCI DSS準拠の際に抱えるお客様の課題

- 現状のシステムの把握
  - クリアしなければならない要件の把握
  - ギャップ分析
- 準拠するために必要なセキュリティ製品の導入
  - ファイアウォール、Web Application Firewall、IPS/IDS、改ざん検知ソフト、etc…
  - セキュリティ製品の運用策定
- 社内への啓蒙活動・運用説明
  - 新たなセキュリティ運用ルールの策定

- PCI-DSS準拠がコスト増、システム運用負荷増になってしまいがち！

キーワード　は“早く”、“安く”、“手戻りなく”

- **早く**
  - ギャップ分析の結果、不足している対策への対応
  - 準備から審査期間
- **安く**
  - 準拠コンサルティング
  - セキュリティ製品の導入
  - QSAによる審査
- **手戻りなく**
  - “前の状態に戻って、もう一度その作業をやり直すこと”
  - 何度も審査を受けない（一発合格！）

トレンドマイクロが
お手伝いできるところ

PCI DSS準拠に必要なセキュリティ機能を1つの製品で実装

Trend Micro Deep Security

OSやアプリケーションの
脆弱性を保護

DoS攻撃など
不正な通信を防御

OSやミドルウェアのセキュリティイベントを
集中監視

IPS/IDS
Webアプリケーション保護

ファイアウォール

ウイルス対策

セキュリティログ監視

変更監視

SQLインジェクション等の攻撃から**Webアプリを保護**

リアルタイムに
ウイルスを検索

ファイルやレジストリ等の
変更を監視

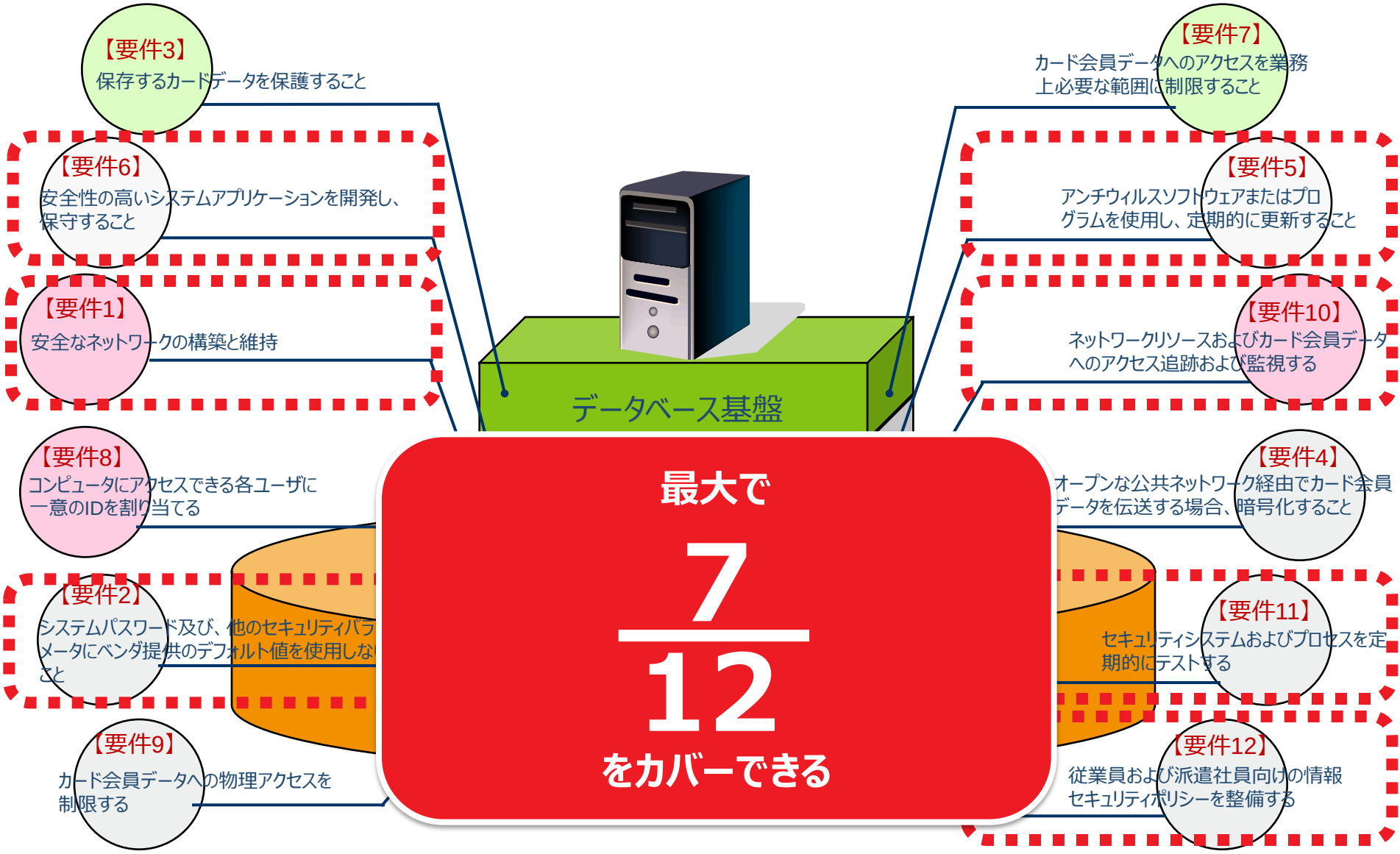
物理サーバ

仮想サーバ

クラウド上のサーバ

デスクトップの仮想化

PCI DSS準拠要件とDeep Securityの対応範囲

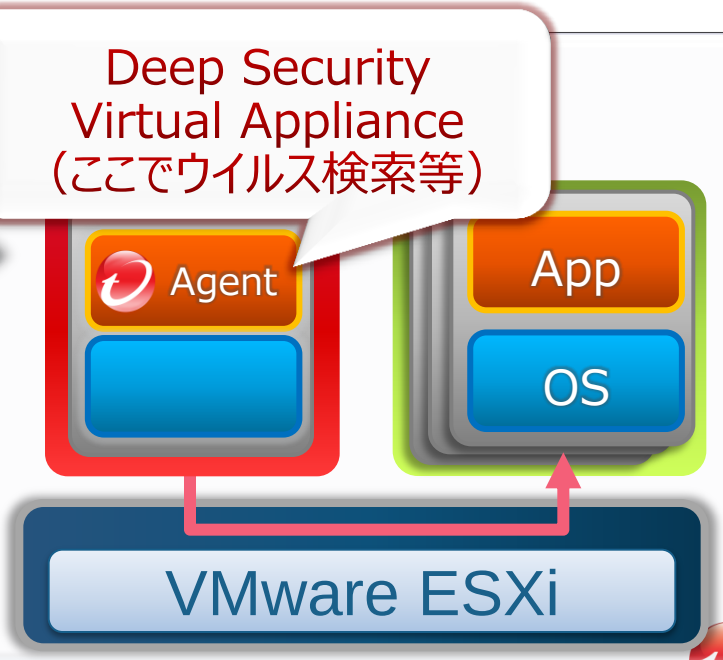


ヴイエムウェア社と連携した エージェントレス型セキュリティ対策

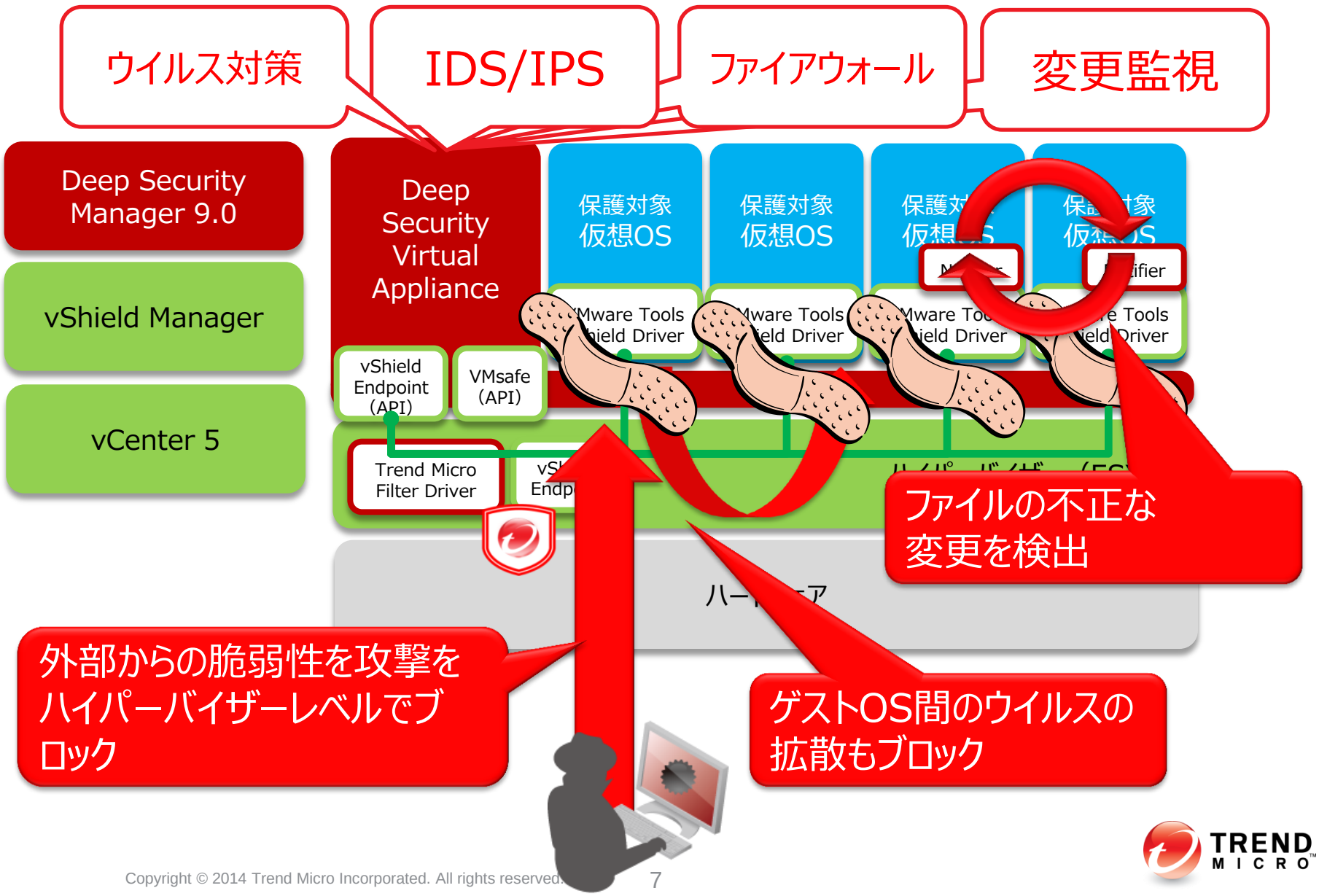
エージェントレス型ウイルス対策とは？
セキュリティ対策機能を専用の仮想マシン(Virtual Appliance)へ処理をオフロードする方式

ポイント

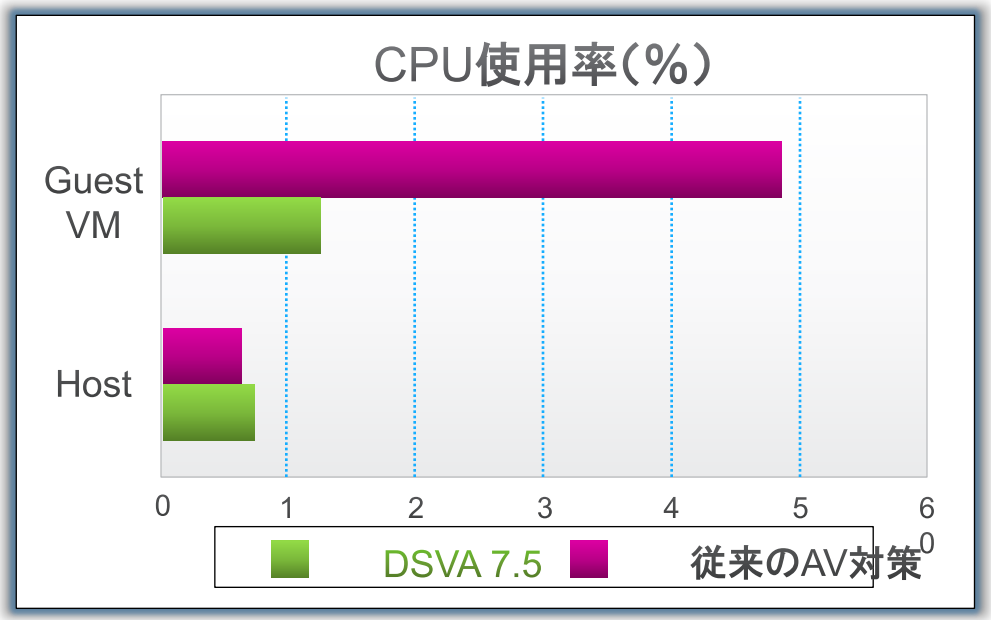
- 各仮想マシンで、AVソフトのインストール不要
- ウイルス検索に使用するリソースはセキュリティ仮想マシンのリソースを共有

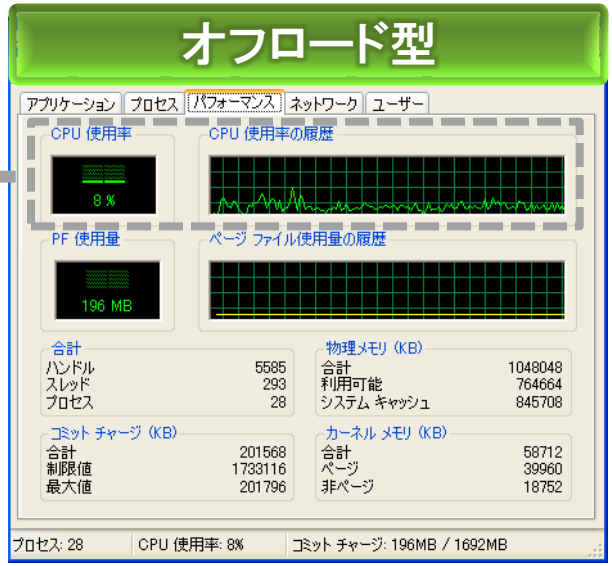


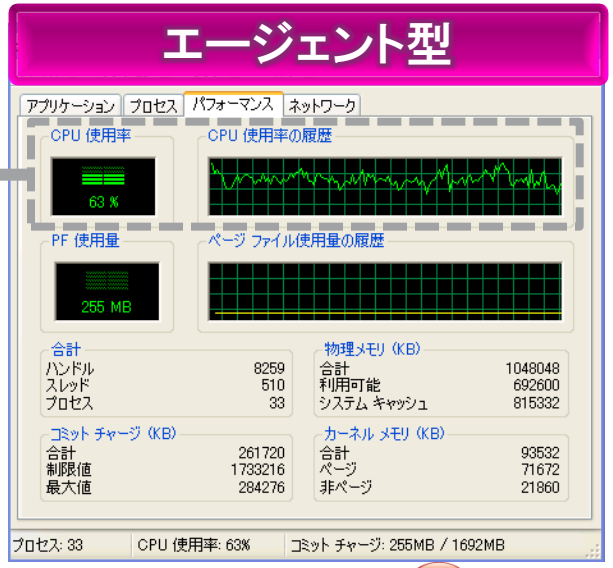
エージェントレス型セキュリティ対策の仕組み



検索処理中の消費リソースは？







✓オフロード型のCPU使用率は約１０%前後を推移
✓エージェント型は約６０%を推移

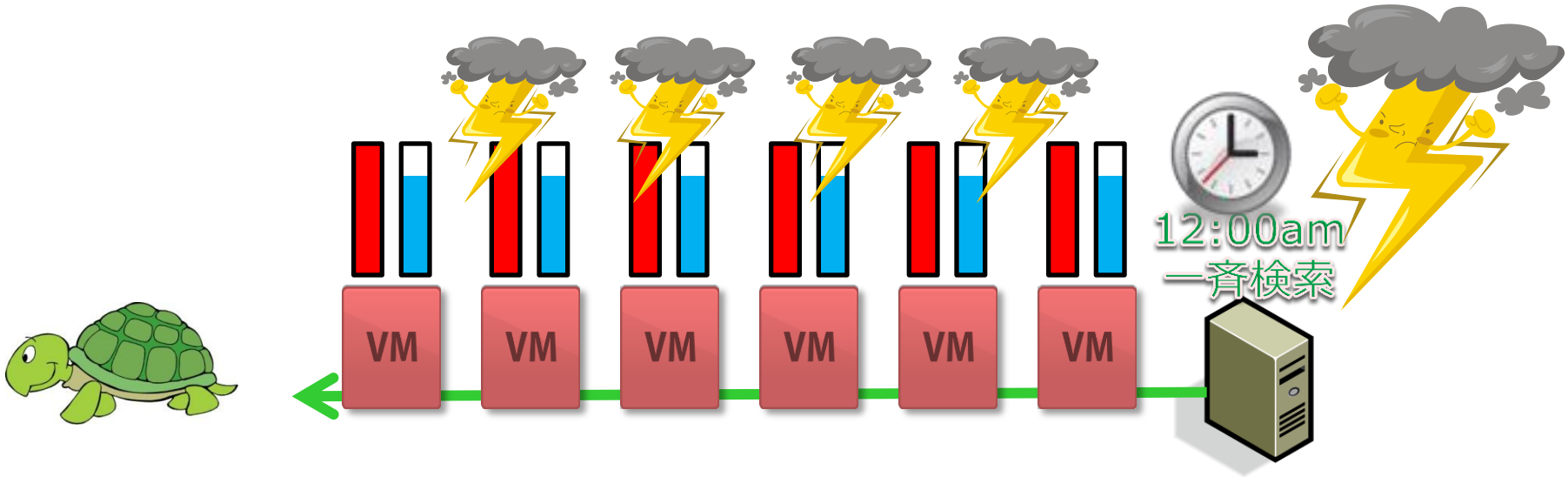
✓エージェントレス型はユーザにウイルス検索を意識させない、常に快適なVDI利用環境を提供

仮想化環境特有のセキュリティ課題を解決

AV検索リソースの集中による仮想化ホストへの過負荷

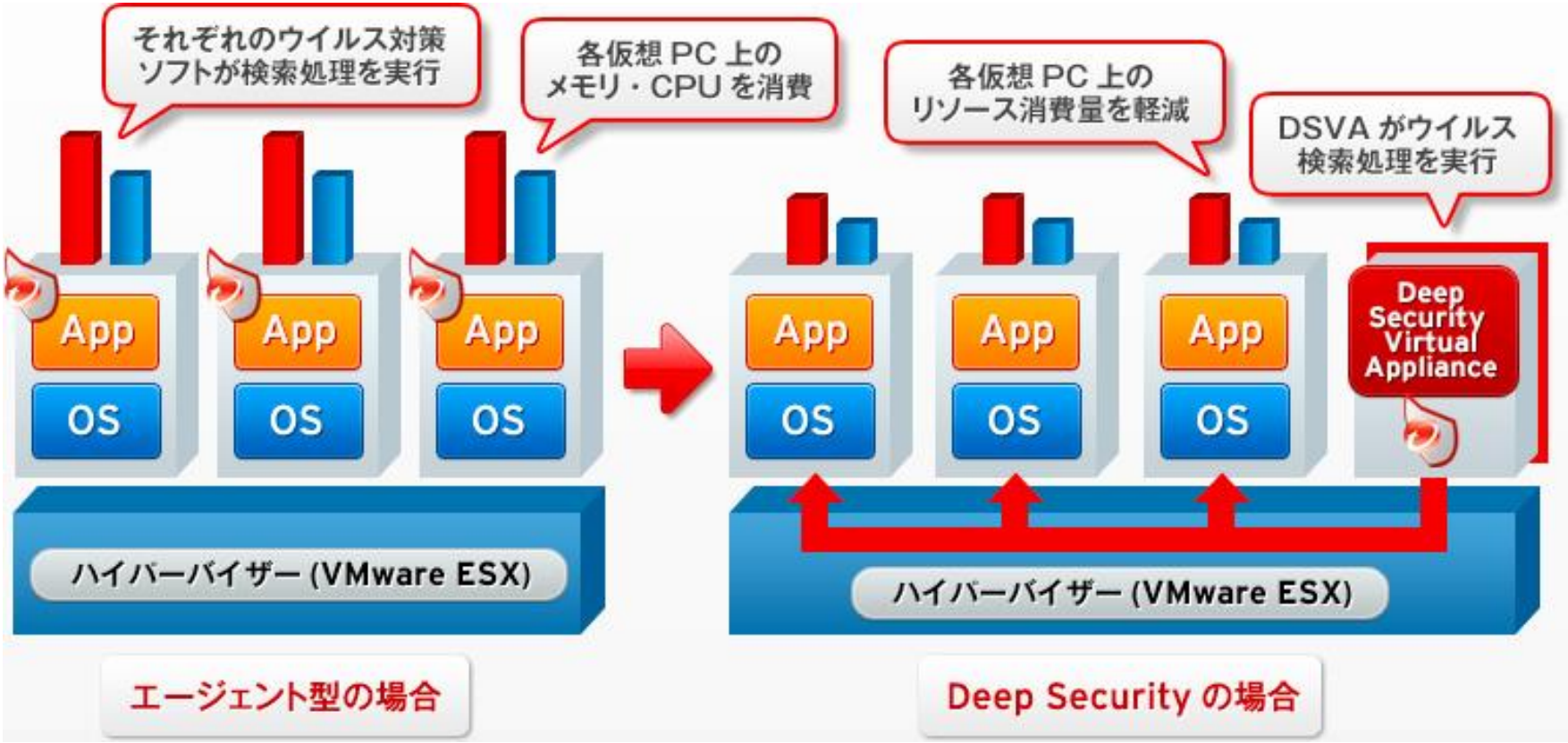
●ログインストーム：**同時刻に多くのユーザがログイン**したタイミングで、ウイルス対策ソフトウェアが同時にアップデートを開始。仮想化基盤の**リソース過負荷が発生**。

●アンチウイルスストーム：複数の仮想デスクトップに対し**同時にウイルス検索を実行**。仮想化基盤への**リソースの過負荷が発生**。



TREND MICRO

まとめ：従来の対策との違いは？

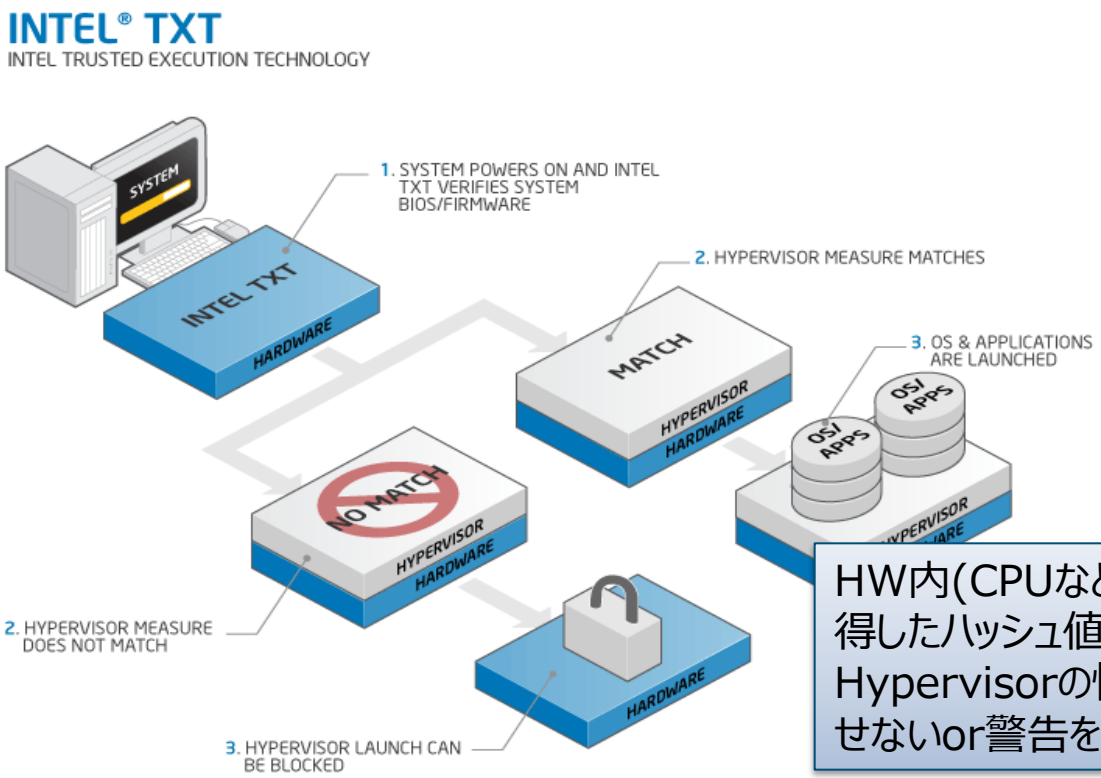


- 各仮想OSにウイルス対策ソフトのインストール
- 各仮想OSにウイルスパターンファイルが配信
- 各仮想OS毎にウイルス対策の設定管理が必要

- ESXに１つのVirtual Applianceをインストール
- Virtual Applianceにパターンファイルを配信
- Virtual Applianceで設定を一括管理

ハイバーパイザーの変更監視機能の実装

- **Intel TPM/TXT技術**をvSphereに採用し、ハードウェアレベルでHypervisorの完全性の確保
- Rootkitなどの混入や改ざん行為が行われた場合に、ESXを起動させないことが可能になります。



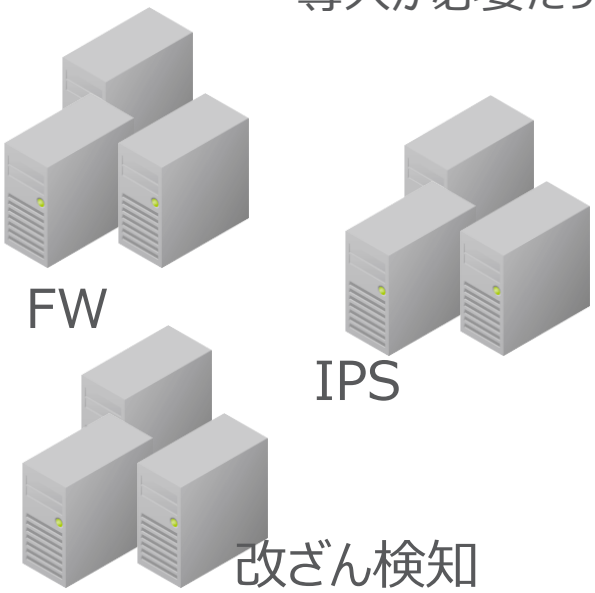
HW内(CPUなど)にvSphere5.1のバイナリファイルから取得したハッシュ値を記憶させ、これからロードするHypervisorの情報とを比較し改変されていれば、起動させないor警告を出力される。

導入事例：TELECOM CREDIT テレコムクレジット株式会社

- **お客さまの要望：**
  PCI DSS準拠の為のセキュリティツールを検討
- **評価のポイント：仮想パッチ、推奨スキャン、統合管理**
  ５つの機能を1つの製品で実装しているため複数のセキュリティ製品を購入する必要が無く、コストが削減できた。

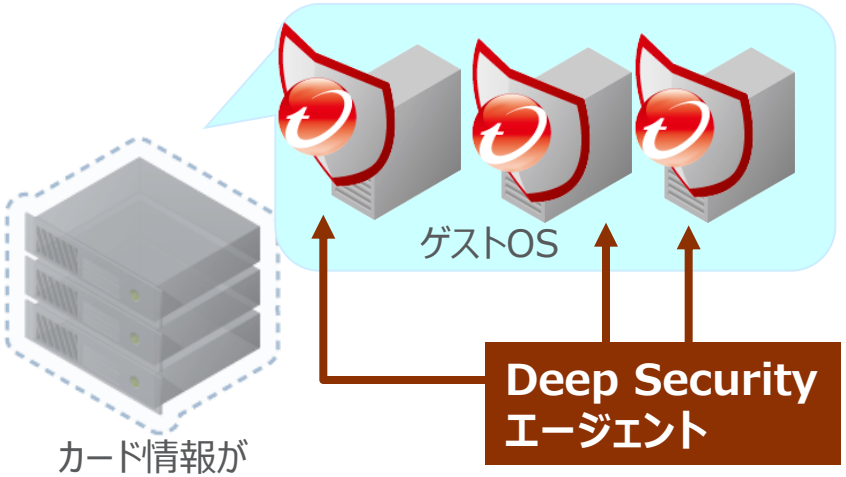
従来

複数のセキュイリティ製品の導入が必要だった



今後

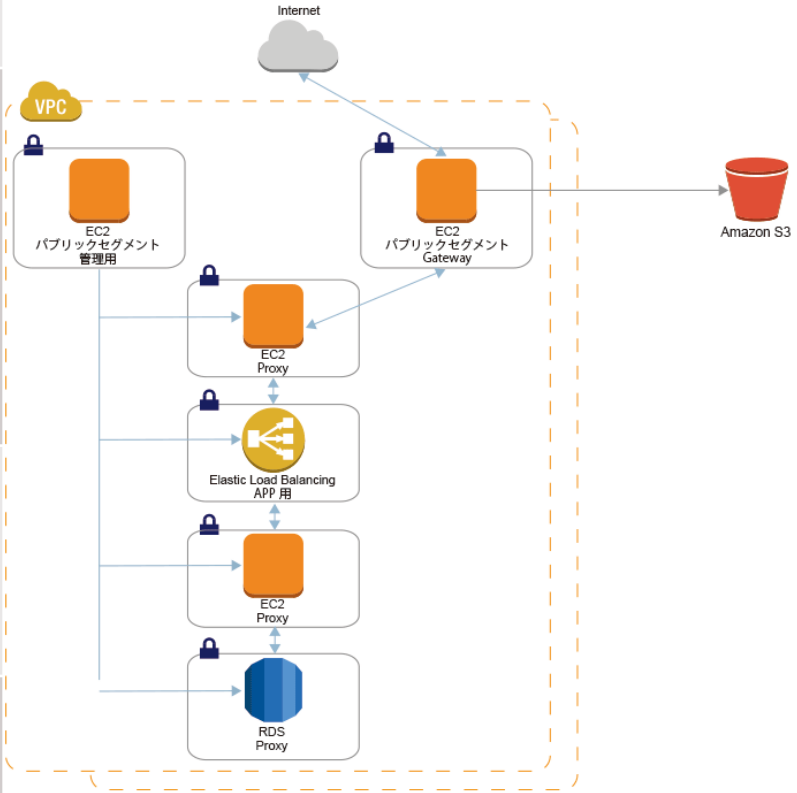
Deep SecurityでPCI DSS７項目に準拠できた



TREND MICRO

導入事例：コイニー株式会社

項目	内容
導入ソリューション	cloudpackオプションサービス「セキュリティ+　Deep Security」
業種	クレジットカード決済代行
採用理由	● PCI DSSに対応するためのネットワーク構築、CentOSをベースに、Trend Micro社のDeep Securityを採用。本番環境での設計～実装を、cloudpack社のサポートを得て行い、2012年11月～12月の約1ヶ月間で完了
導入によって得られたメリット	● PCI DSSに準拠するためのセキュリティ製品コストの低減 ● Cloudpack社からのサービス提供
導入時期	● 2012年12月（導入済み）



賢くPCI DSS準拠する方法とは？

攻 **ヴイエムウェア仮想化**

仮想化による生産性/事業効率の向上。

守 **Deep Security**

６つのセキュリティ機能で効率的にセキュリティ対策

賢 **ITコストの効率化／適正化**

攻めと守りに貢献する賢い情報資産保護のため、

物理・仮想・クラウドに対応した・・・

VMware x Trend Micro

ご清聴ありがとうございました。

アンケートのご記入に
ご協力
よろしくお願いいたします。