富士通サーバ「PRIMERGY RX300 S8」での仮想化環境向けウイルス対策「McAfee MOVE-AV Multiplatform」の動作検証報告

マカフィー株式会社

February 7, 2014

目次

- 概要
- 検証環境
- 検証結果
- まとめ
- MOVE-AVの紹介

概要 -1-

- 検証の目的
  - 富士通サーバ「PRIMERGY」シリーズにシトリックス社のCitrix XenDesktop環境を準備し、集約された仮想サーバ/デスクトップ環境へのウイルス対策として開発されたマカフィー社の『McAfee MOVE-AntiVirus』（以降、MOVE-AV）の動作検証を実施し、安心して富士通サーバ上でMcAfee製品を検討・利用いただくことを目的とします

- 検証環境の準備
  - 仮想デスクトップイメージはMOVE-AVエージェントをインストールしWindows 7イメージを作成
  - Citrix StudioにてMCS(Machine Creation Service)方式で30VDIを展開
  - ハイパーバイザの負荷状況を確認するため、Wgetで「CPU」「メモリ」「ネットワーク」の情報を採取し、RRDToolおよびRRD Editorを使用してエクセルシートへ出力し記録

概要　-2-

- テストシナリオ
  - 仮想デスクトップを①10台、②20台、③30台 同時起動し、Citrixサーバ側が仮想デスクトップを配備できる段階まで待機し、確認後同時シャットダウンを実施し正常終了を確認
  - 仮想デスクトップを起動後、Citrixサーバが仮想デスクトップを配備できる段階まで待機した時間を測定
  - 同時シャットダウンをCitrixサーバから実施。すべての仮想デスクトップがシャットダウンするまで計測するためCitrix XenCenter上から確認
  - 仮想デスクトップを起動からシャットダウンまでを同時間動作させ、リアルタイムにハイパーバイザに与えている負荷量をシャットダウン後、ハイパーバイザから収集

検証環境 -構成表1-

- ハードウェア（ハイパーバイザ）×2台
  1. ハードウェア　：FUJITSU PRIMERGY RX300 S8
  2. CPU　：Intel Xeon E5-2697v2 (12core 2.70GHz)×2
  3. RAM　：192GB
  4. HDD　：600GB (600GB×2：RAID1)
  5. ハイパーバイザ　：XenServer 6.2 (build 70446c)

- 仮想マシン

A. 仮想デスクトップ

  1. OS　：Windows 7 Enterprise SP1 (32bit)
  2. vCPU数　：1
  3. RAM　：1GB
  4. ソフトウェア　：MOVE-AV 2.6.2 Client ModuleまたはSEP12
  5. マシン数　：50

B. 管理サーバ

  a). Citrix Studio / Citrix Store Front サーバ

    1. OS　：Windows Server 2008 R2 Enterprise SP1 (64bit)
    2. vCPU　：1
    3. RAM　：12GB
    4. コンソール　：XenCenter 6.2 (build 1069)
    5. ソフトウェア　：XenDesktop 7.1

検証環境 -構成表2-

b). ePolicy Orchestrator (ePO) サーバ

1. OS : Windows Server 2008 R2 Enterprise SP1 (64bit)
2. vCPU : 1
3. RAM : 4 GB
4. ソフトウェア : ePolicy Orchestrator 4.6.7

c). MOVE-AV Scan サーバ

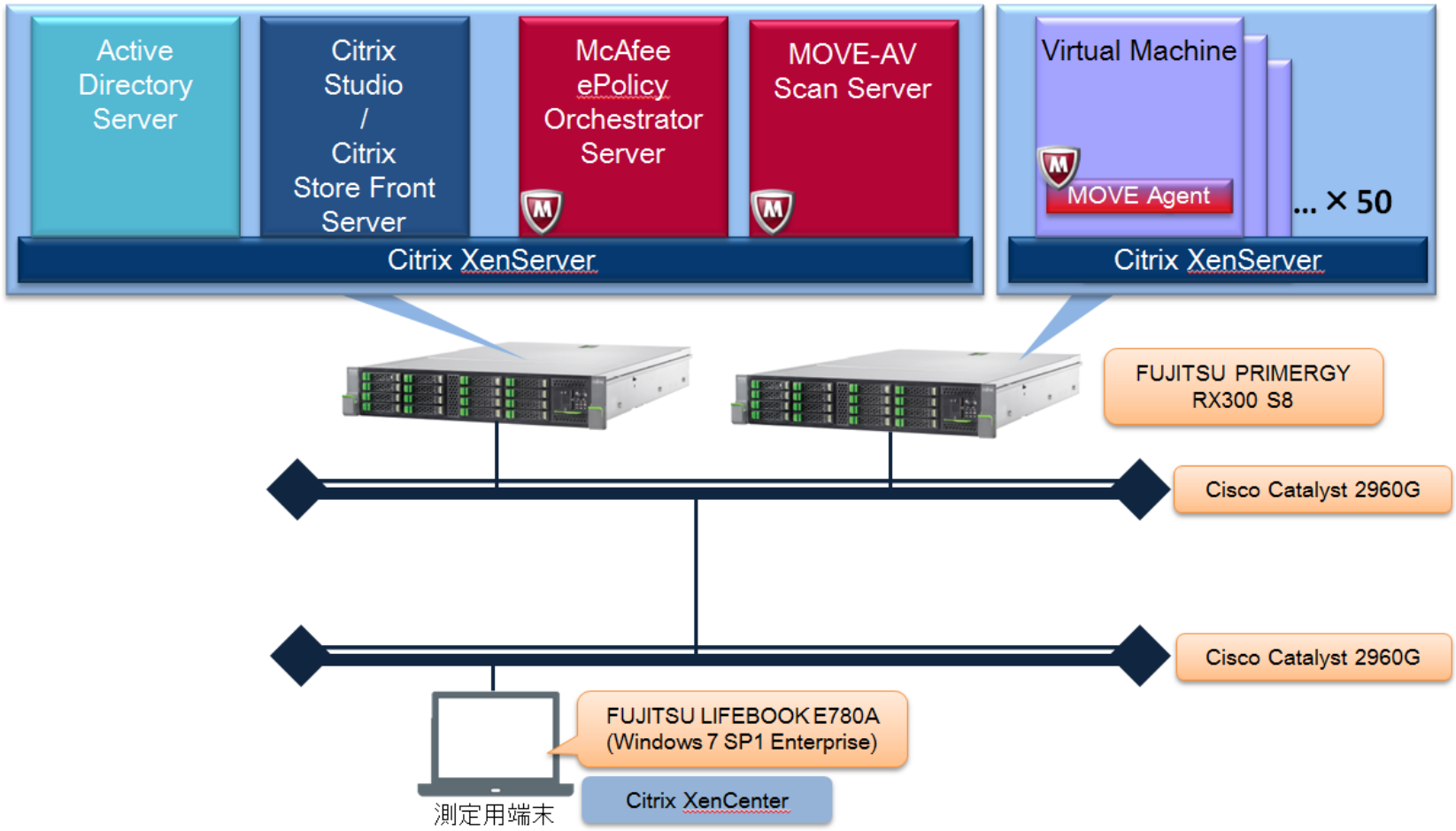
1. OS : Windows Server 2008 R2 Enterprise SP1 (64bit)
2. vCPU : 1
3. RAM : 4 GB
4. ソフトウェア : VSE 8.8 Patch2 MOVE-AV 2.6.2 Offload Scan Module (for Multiplatform)

d). Active Directory サーバ

- OS : Windows Server 2008 R2 Enterprise SP1 (64bit)
- CPU : 1
- RAM : 4 GB
- 役割:
  - Active Directoryドメインサービス
  - DHCPサーバ
  - DNSサーバ

検証環境 -構成図-

- 検証場所：富士通　検証センター （東京、浜松町）



検証結果 -1-

- ウイルス対策製品インストールによる問題の発生はなく、正常に起動→終了を実施することを確認。

- 仮想デスクトップ同時起動からCitrix Store Frontへの配備完了までの時間
  - 10台：5分 →（差：6分）→ 20台：11分 →（差19分）→ 30台：30分

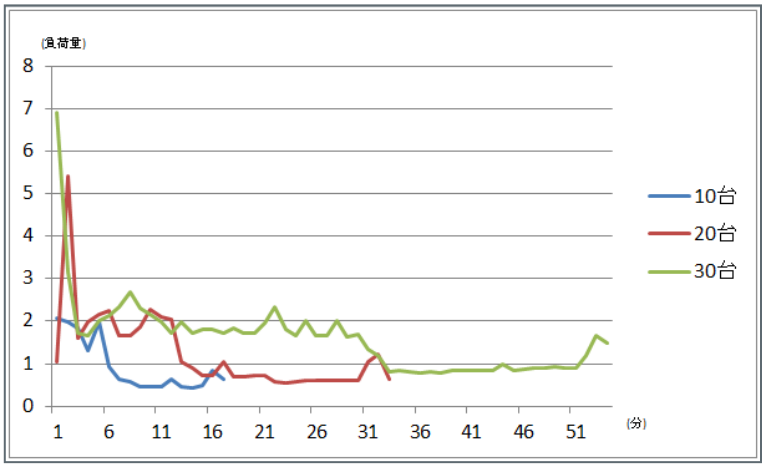
- 仮想デスクトップ同時シャットダウンから完全シャットダウン確認までの時間
  - 10台：1分 →（差：1分）→ 20台：2分 →（差1分）→ 30台：3分
  - 参考：従来型のウイルス対策製品（他社）の場合（カッコ値はMOVE-AVとの差）

※参考：同一環境下において従来型のウイルス対策製品（他社）での動作時間
（カッコ値はMOVE-AVとの差）

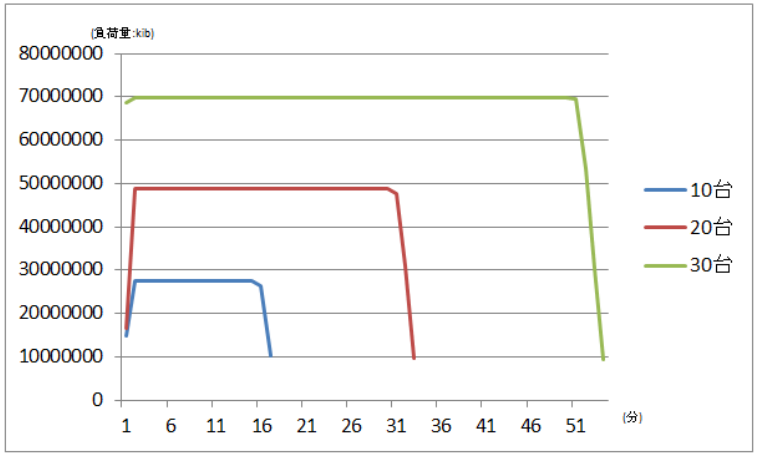
- 同時起動から配備完了までの時間
  - 10台：8分（+3分） 20台：21分（+10分） 30台：N/A（展開完了失敗）
- 完全シャットダウンまでの時間
  - 10台：7分（+6分） 20台：27分（+25分） 30台：N/A

検証結果 -2-

- リアルタイムにハイパーバイザに与えている負荷状況の確認
  - CPU
    - Citrix Store Frontへの配備完了後は負荷は50%近く落ちて安定する傾向
    - 従来型のウイルス対策製品で発生する各仮想デスクトップごとにエンジンを置かないため、ファイルスキャンない状態になると負荷量が軽減

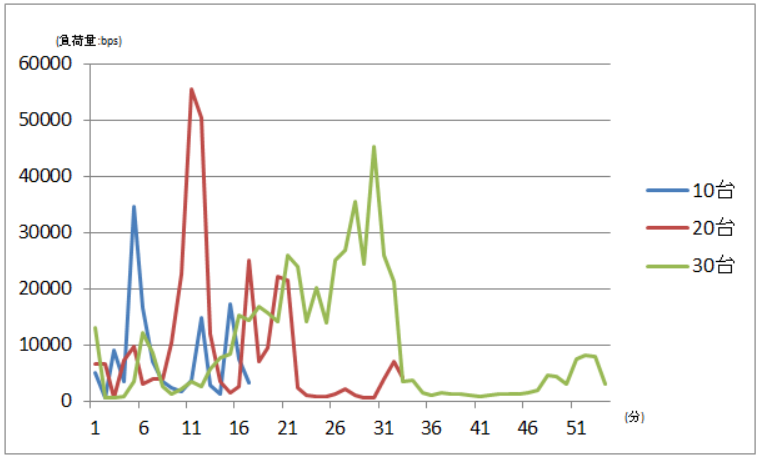


  - メモリ
    - メモリの占有はOS起動時から一律の使用量で変動しない傾向
    - Citrix Studioからの一斉起動から起動台数分でメモリ総使用量が変化

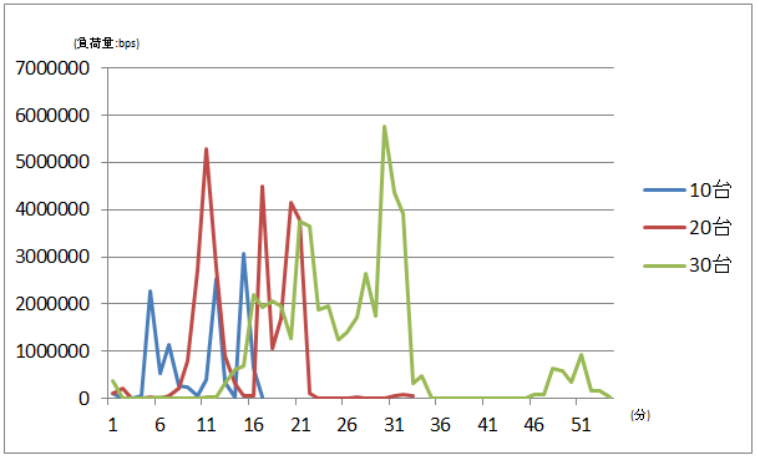


検証結果 -2-

- リアルタイムにハイパーバイザに与えている負荷状況の確認
  - ネットワーク（受信）
    - Citrix Store Frontへの配備完了後はトラフィックはほぼないことを確認
    - 従来型のウイルス対策製品で発生する各仮想デスクトップごとのアップデートがないため、より高過密な仮想基盤でも受信トラフィックが発生しない



  - ネットワーク（送信）
    - 各仮想デスクトップがファイルをスキャンサーバへ転送する分、トラフィックが発生
    - Citrix Store Frontへの配備完了後はトラフィックはほぼないことを確認



まとめ

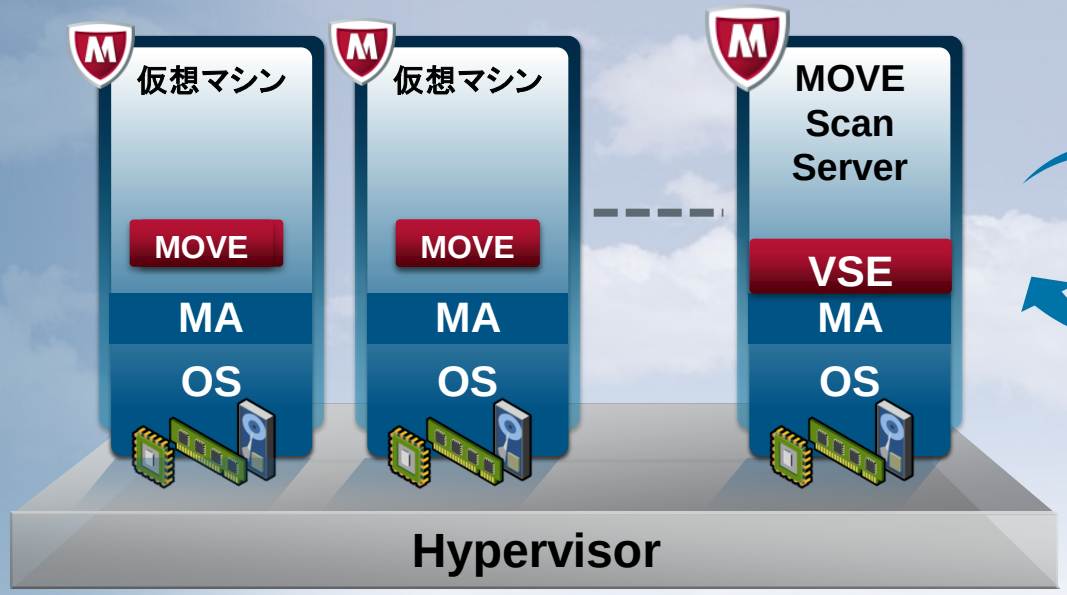
- 今回の試験結果より、Citirx XenDesktop展開においてMcAfee MOVE-AVは問題なく仮想デスクトップの展開を実施することができることを確認しました。
- ウイルススキャンをスキャンサーバに集約化する仕様のため、ファイル転送のネットワーク負荷による動作への影響を懸念しましたが、1Gbpsの物理スイッチを挟んでのテストにおいても問題なく仮想デスクトップを展開しました。
- 従来のウイルススキャンエンジンを搭載する仕様では起動時に最新ウイルス定義ファイルと照合するためにはアップデートタスクの実行が必要ですが、**McAfee MOVE-AVはエージェントが起動した時点から最新ウイルス定義ファイルがアップデートされたスキャンサーバでウイルススキャンすることができる**ため、仮想デスクトップ環境のセキュリティレベルをさらに高める製品ともいえます。
- 本報告書に関するお問い合わせ先
  - マカフィー株式会社　法人お問い合わせ窓口

    http://www.mcafee.com/japan/contact/hojin.asp

    ※お問い合わせ時は「富士通サイトの検証事例を見た」とお伝えください。

MOVE-AV 2.6.2 Multiplatformの紹介

MOVE AV 2.6.2（Multiplatform）



Datacenter

特徴

- マルウェアスキャンで消費するハードウェアリソースの低減
- ネットワーク（TCP/IP）越しでゲスト仮想マシンをスキャン
- クリーンファイルの再スキャンを回避
- HIP(ホスト型不正侵入対策)によるメモリ保護
- 高検知率を維持するMcAfee GTIによるファイルレピュテーション搭載
- メジャーなハイパーバイザ環境をサポート

MOVE AV 2.6.2 (Multi-Platform) システム要件 ①（2014年1月現在）

– MOVE Anti-Virus Agent
  - Servers
  –Windows Server 2012 R2
  –Windows Server 2012
  –Windows Server 2008 R2 SP1
  –Windows Server 2008 SP1/2(32-bit)
  –Windows Server 2008 SP1/2(64-bit)
  –Windows Server 2003 R2 SP2 (32-bit)
  –Windows Server 2003 SP2 (32-bit)
  - Clients
  –Windows 8.1 (32-bit / 64-bit)
  –Windows 8 (32-bit / 64-bit)
  –Windows 7 (32-bit / 64-bit)
  –Windows Vista(32-bit / 64-bit)
  –Windows XP SP3 (32-bit)

– MOVE Anti-Virus Agent
  - RAM
  –Windows XP⇒512MB以上
  –その他OS⇒1GB以上

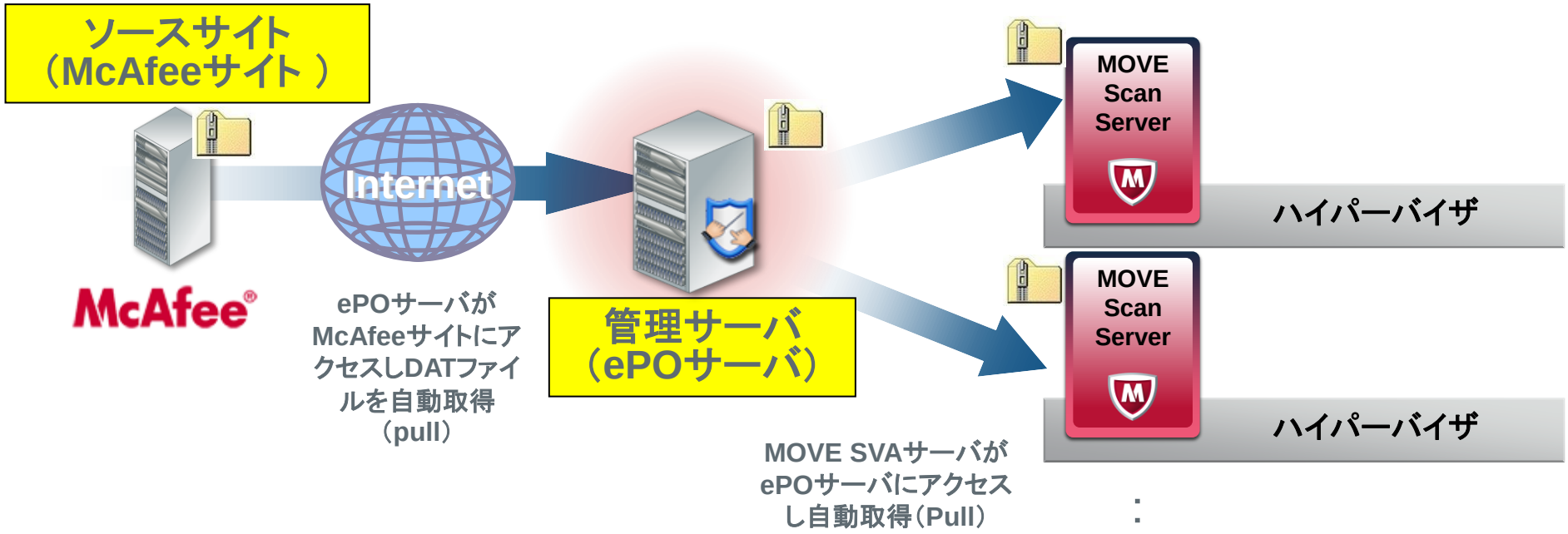
– Scan Server
  - Windows Server 2012
  - Windows Server 2008 R2 SP1
  - Windows Server 2008 SP2 (64-bit)
  –CPU 1vCPU (2GHz)以上
  »450VDI(最大)の場合、8vCPU
  –RAM 1GB以上
  »450VDI（最大）の場合、8GB
  –HDD 8GB以上
  –VirusScan Enterprise 8.8

– Management
  –ePolicy Orchestrator 5.1 / 5.0 / 4.6
  –McAfee Agent 4.8 / 4.6 / 4.5

MOVE AV 2.6.2 (Multi-Platform)
システム要件 ②（2014年1月現在）

- **仮想環境**
  - Hypervisor
    - Citrix XenServer 6.2 / 6.1 / 6.0 / 5.6 / 5.5
    - Citrix VDI-In-a-Box 5.0
    - VMware ESXi 5.5 / 5.1 / 5.0 / 4.1 Update3 / 4.1 / 4.0
    - Microsoft Windows Server 2012 / 2008 R2 / 2008 SP2 Hyper-V
  - Virtual Desktop Infrastructure (VDI)
    - Citrix XenDesktop 7.1 / 7.0 / 5.6 / 5.5
    - VMware View 5.2 / 5.1 / 5.0 / 4.0
  - Virtual Application Management
    - Citrix XenApp 6.5 / 5.0
    - VMware ThinApp 4.6.2

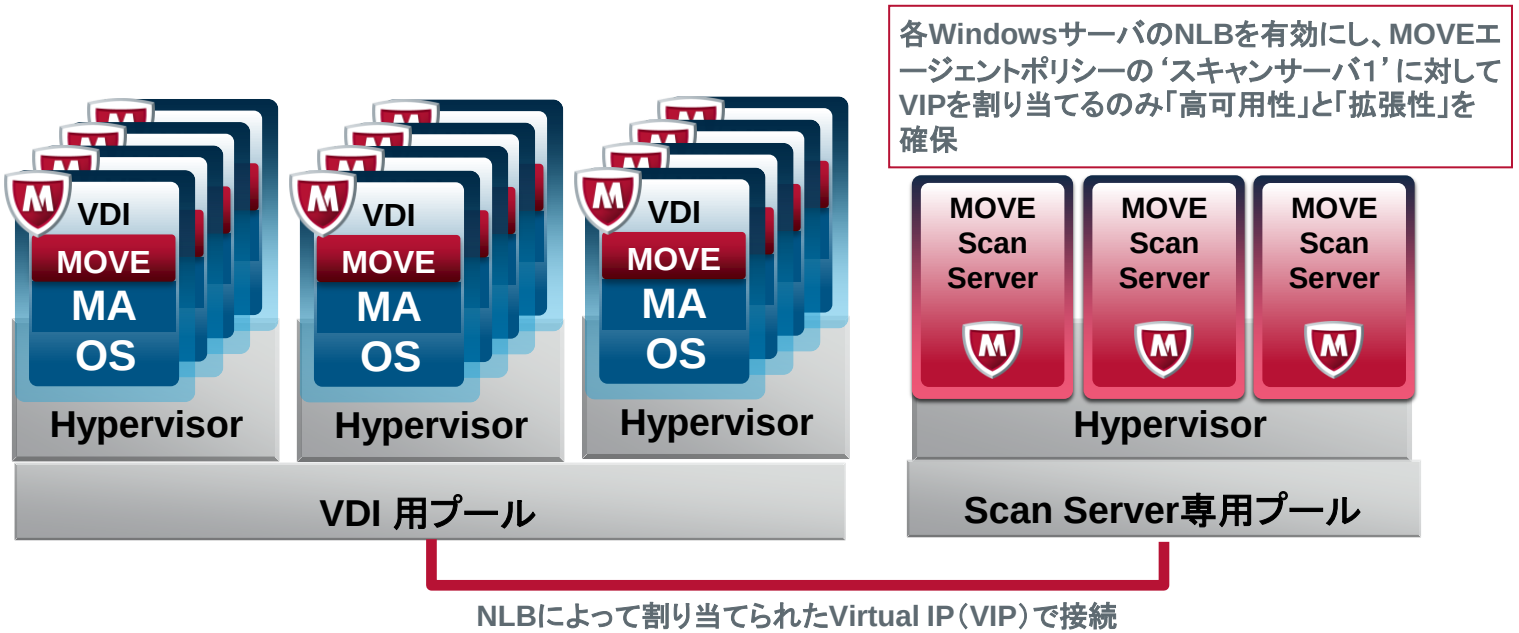
管理サーバを利用したウイルス定義（DAT）ファイル展開の階層アーキテクチャ



- DATファイルの展開は**スキャンサーバのみ取得。**
- **数百台あるVDIではアップデートが不要。**
  - アップデートのネットワーク負荷が劇的に軽減
- **ユーザログオン直後から最新のウイルス定義が適用可能。**
  - アップデート処理でユーザを待たせることがありません。
  - ユーザごとのアップデート監視も不要。最新のセキュリティ環境を提供。

スキャンサーバの高可用性と拡張性

- VDIとスキャンサーバ間はTCP/IP（デフォルト：9053番）で通信
- ネットワークで利用される「高可用性」「拡張性」を利用することが可能
  - ロードバランサ装置
  - NLB（Network Load Balancing） ※Windowsサーバの負荷分散機能
- vShield Endpointでは現状1ハイパーバイザに1スキャンサーバになり、拡張性はない（vMotionで高可用性は可能？）
- サービスネットワークと別にAVスキャン専用ネットワークを設けて、スキャンサーバ用のプールを構築して展開することも可能です。



MOVE AV 導入実績

- NTTコミュニケーションズ様　Bizデスクトップ Pro Enterprise
  - http://www.ntt.com/release/monthNEWS/detail/20121212.html
- 某大学様　学内デスクトップサービス
- 某不動産会社様　社内デスクトップサービス
- 某銀行業様　社内デスクトップサービス
- 某家電製造業様　米国ユーザ向けデスクトップサービス

エンドポイントセキュリティ製品管理ツール
ePolicy Orchestrator

- **ePolicy Orchestrator とは?**
  - “Every Products, One Console”というコンセプトで開発された、マカフィーのエンドポイントセキュリティ製品管理ツールです。
- **ePolicy Orchestrator ができること**
  - 各端末にインストールされたエンドポイント製品のポリシー(設定情報)を、「1台」のサーバで管理します。
  - 同製品の異なるバージョンも1コンソールで管理するため、スムーズなバージョンアップ作業を支援します。
  - エンドポイントはスマートフォン/タブレットからPC/サーバ(仮想も可)、工作機械まで様々なデバイスが対象です。
  - 管理対象システムから情報を収集し、カスタマイズ可能な柔軟なレポーティングを管理者に提供します。
  - 迅速に製品のアップデートを行うための機能を提供します。

ePolicy Orchestrator によるエンドポイント端末管理

ePOエージェントがサーバと定期的に通信

管理対象PC

クライアント上の各製品を管理

McAfee製品の管理状態、
H/W、OSなどのインベントリ情報、
脅威の検出に関する情報を送信。

ポリシー（製品の設定情報）、
定義ファイル・エンジン・製品パッチ
等の更新をダウンロード。

ダウンロードしたポリシーを
定期的に各製品に適用。

ePO Server

DataBase

ePO Agent

VirusScan Enterprise

Host IPS

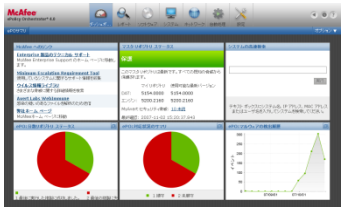
Device Control

各種マカフィー製品

ユーザが設定値を変更しても
エージェントが上書き。
セキュリティの抜け穴を塞ぐ
強力な保護を提供。

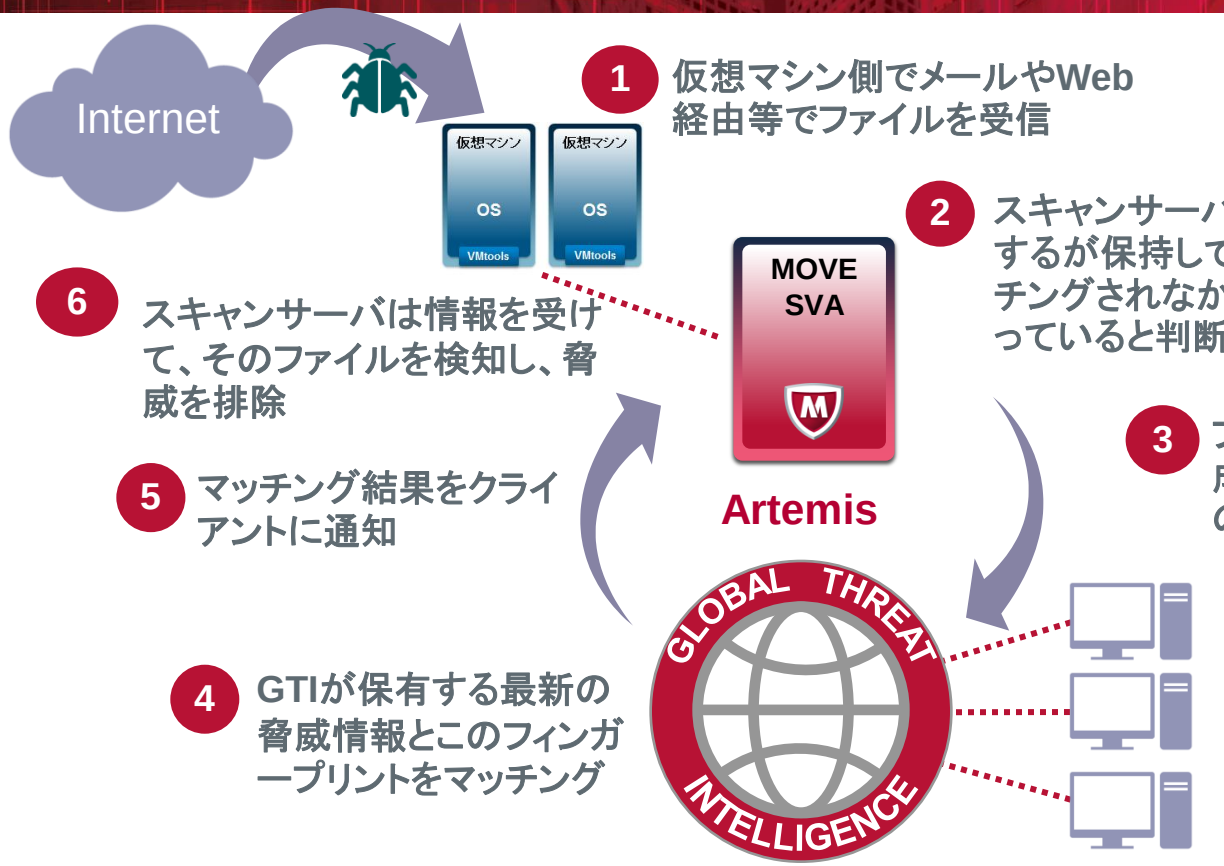
ポリシー設定

状況把握



管理者

最新の脅威情報を活用
Global Threat Intelligence (GTI)

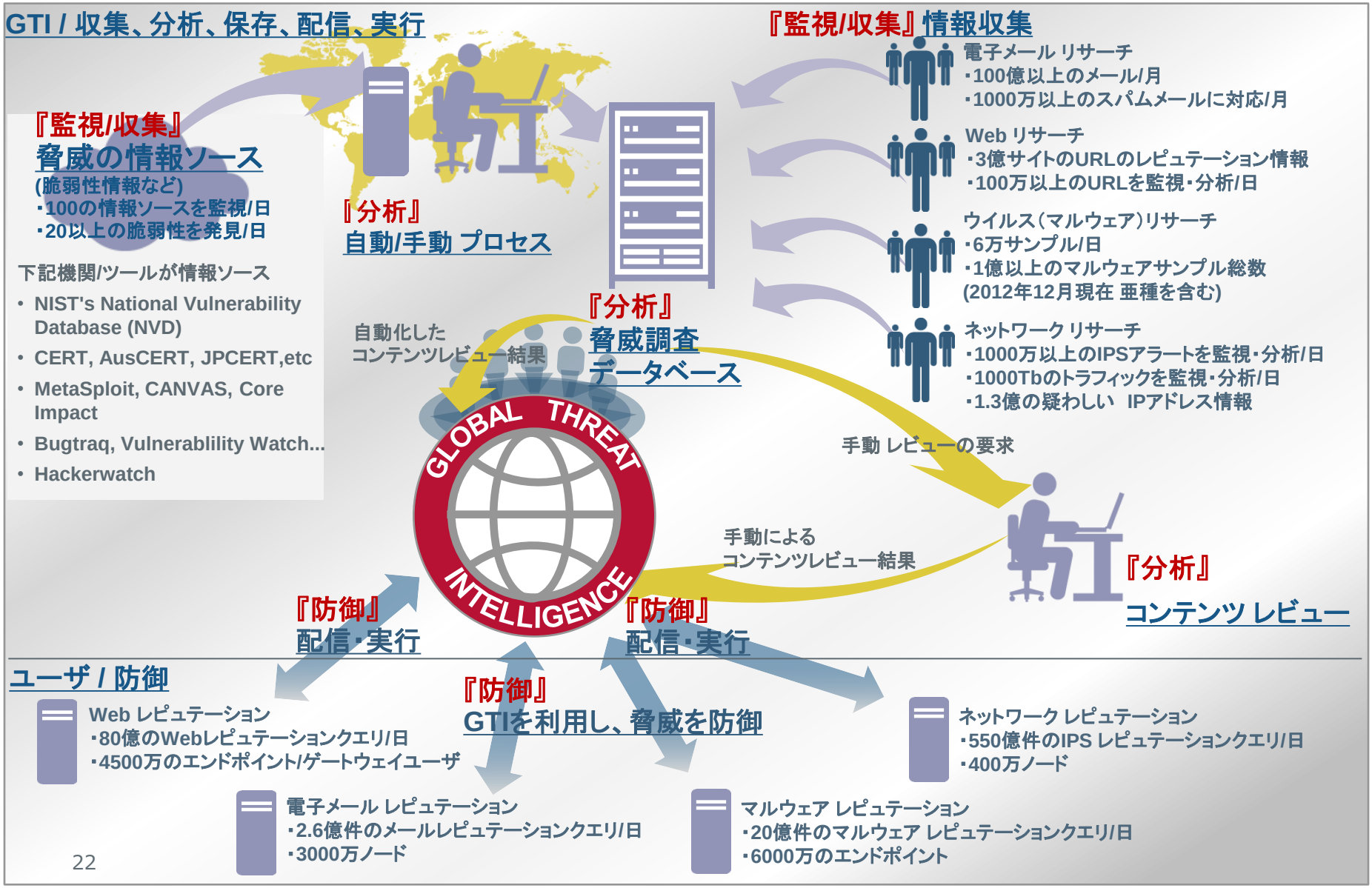


GTI連携を有効化するメリット

- **最新の定義ファイル情報を提供するまでの期間がリアルタイム（従来の方法では24～72時間）。**
  - ✓ クラウド上のGTIとの通信は既存技術の“DNSクエリ”で実装（導入しやすい）
  - ✓ ハッシュ情報のためデータ量も少ない（インターネット回線の負荷が低い）
  - ✓ 追加費用なし！　有効化をチェックするのみ！（とりあえず使ってみてください）

McAfee Global Threat Intelligence
～GTIの仕組みと情報ボリューム～

McAfee An Intel Company




McAfee®
An Intel Company