医療機関向けクライアントセキュリティ対策セミナー

院内セキュリティを向上する仮想化ソリューション

ヴイエムウェア株式会社
ゼネラルビジネスSE本部
公共第二SE部
シニアシステムズエンジニア

竹原 良祐

Agenda

1. 院内で保持しているデータの種類と今後の対策
2. デスクトップ仮想化を利用したセキュリティ対策
3. 病院におけるデスクトップ仮想化の適用
4. ネットワーク仮想化を組み合わせたセキュリティ対策
5. まとめ

院内で保持しているデータの種類と今後の対策

2017年に発生した情報セキュリティインシデントと医療の割合

2017年情報セキュリティインシデントに関する調査報告書

出典：2017年情報セキュリティインシデントに関する調査報告書【速報版】
https://www.jnsa.org/result/incident/data/2017incident_survey_sokuhou_ver1.1.pdf

表 1：2017 年 個人情報漏えいインシデント 概要データ【速報】

漏えい人数	519 万 8,142 人
インシデント件数	386 件
想定損害賠償総額	1,914 億 2,742 万円
一件当たりの平均漏えい人数	1 万 4,894 人
一件当たり平均損害賠償額	5 億 4,850 万円
一人当たり平均損害賠償額	2 万 3,601 円

インシデントが起きると
大きな損害に

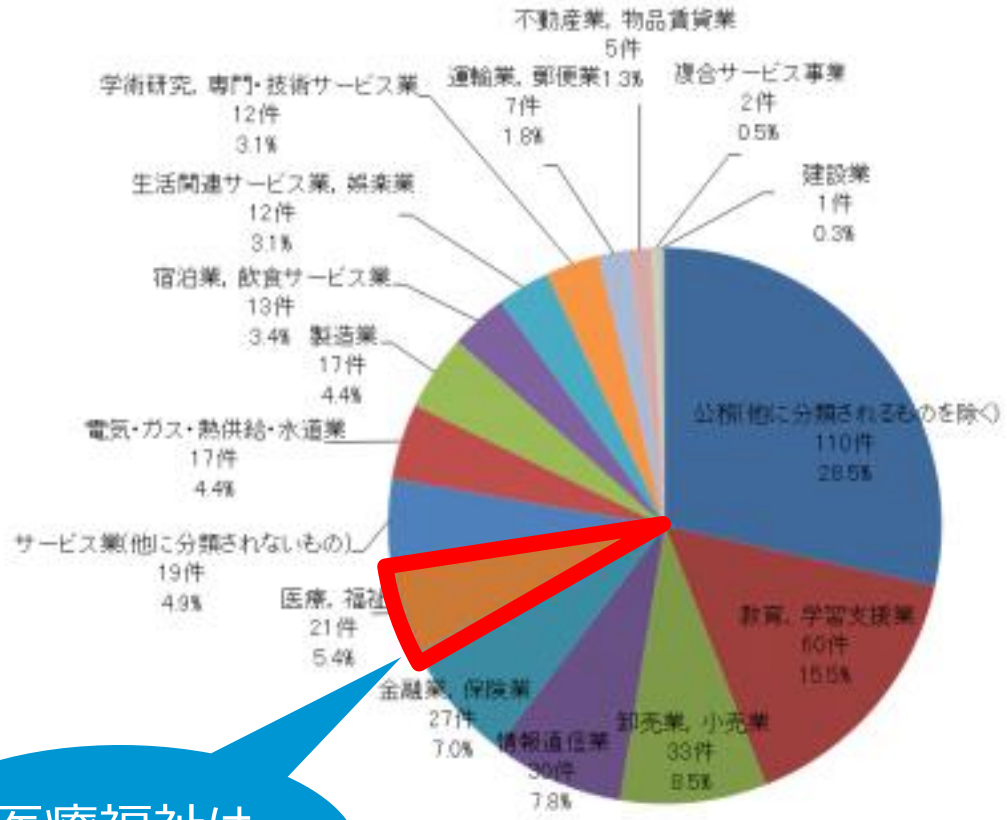
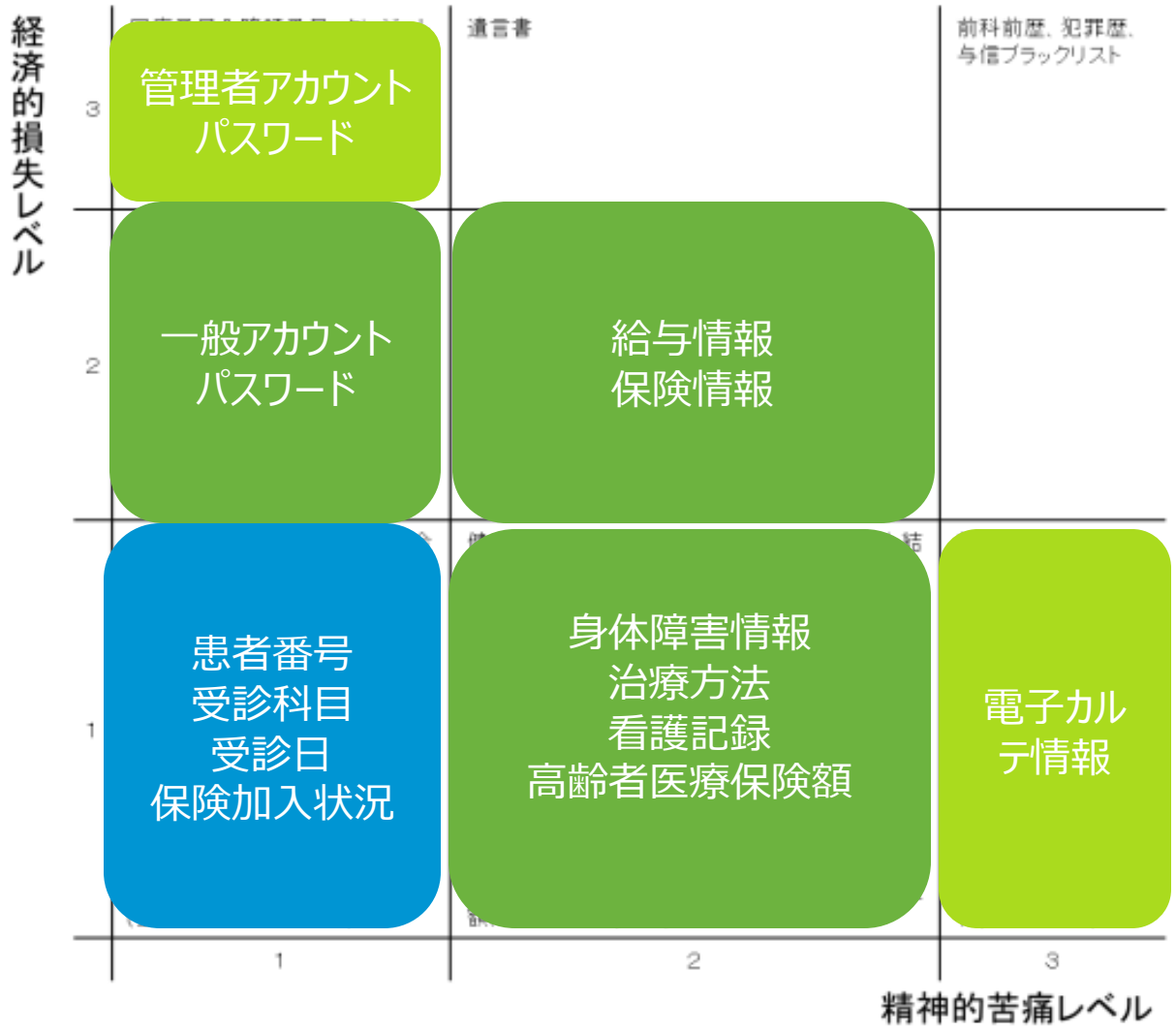


図 1：業種別の漏えい件数

医療福祉は
21件 5.4%

病院で取り扱う情報はどんなもの？

医療情報漏えいによる損害賠償額

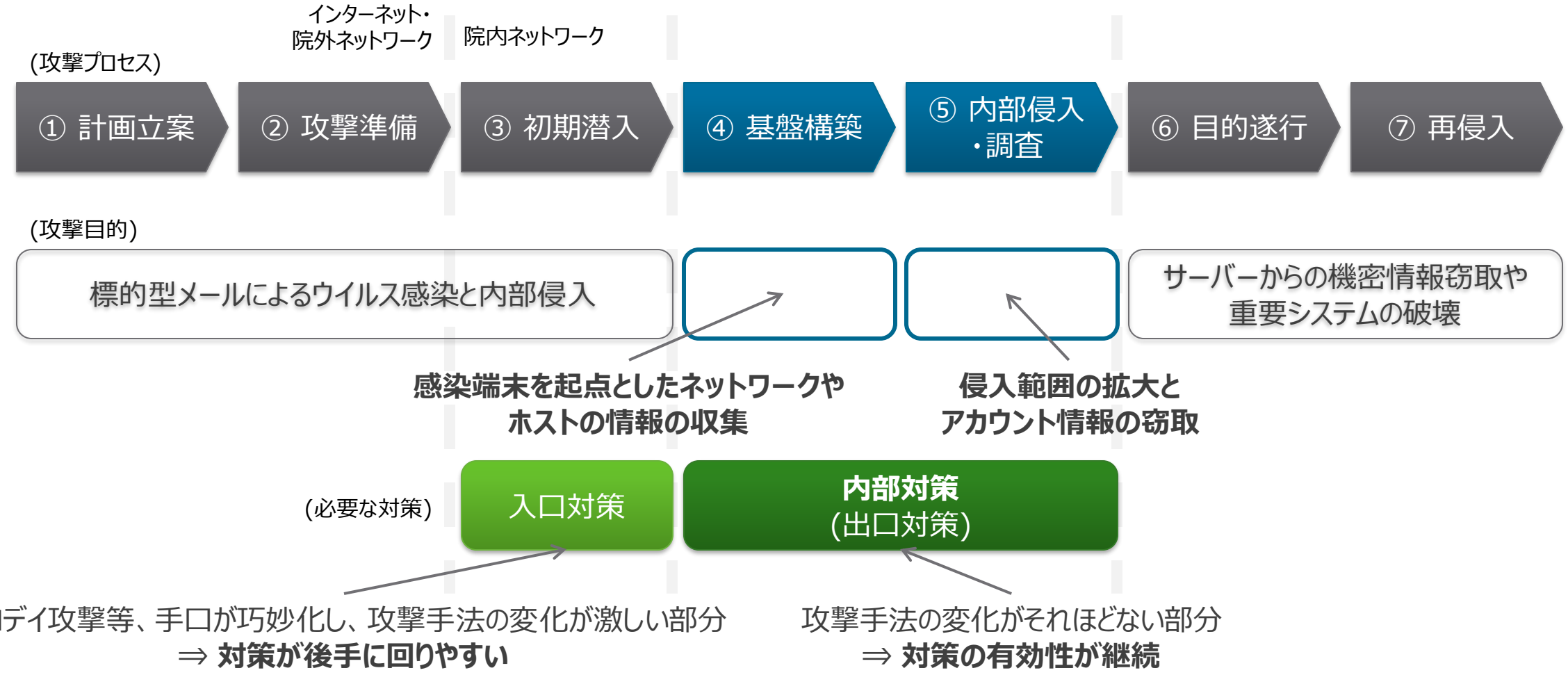


一件あたりの想定損害賠償額	
放射線画像データ	¥33,000
照射録（伝票）	¥30,3000
受付票	¥6,000
電子カルテ記録	¥606,000
患者個人住所録	¥12,000
健康診断結果表	¥66,000

出典：日本ネットワークセキュリティ協会
2017年 情報セキュリティインシデントに関する調査報告書 別紙
https://www.jnsa.org/result/incident/data/2017incident_survey_sokuhou_attachment_ver1.0.pdf

出典：岐阜県立下呂温泉病院
医療情報資産評価のユーザビリティについて
http://www.gero-hp.jp/assets/files/other/houjin/nenpou/nenpou35-9.pdf

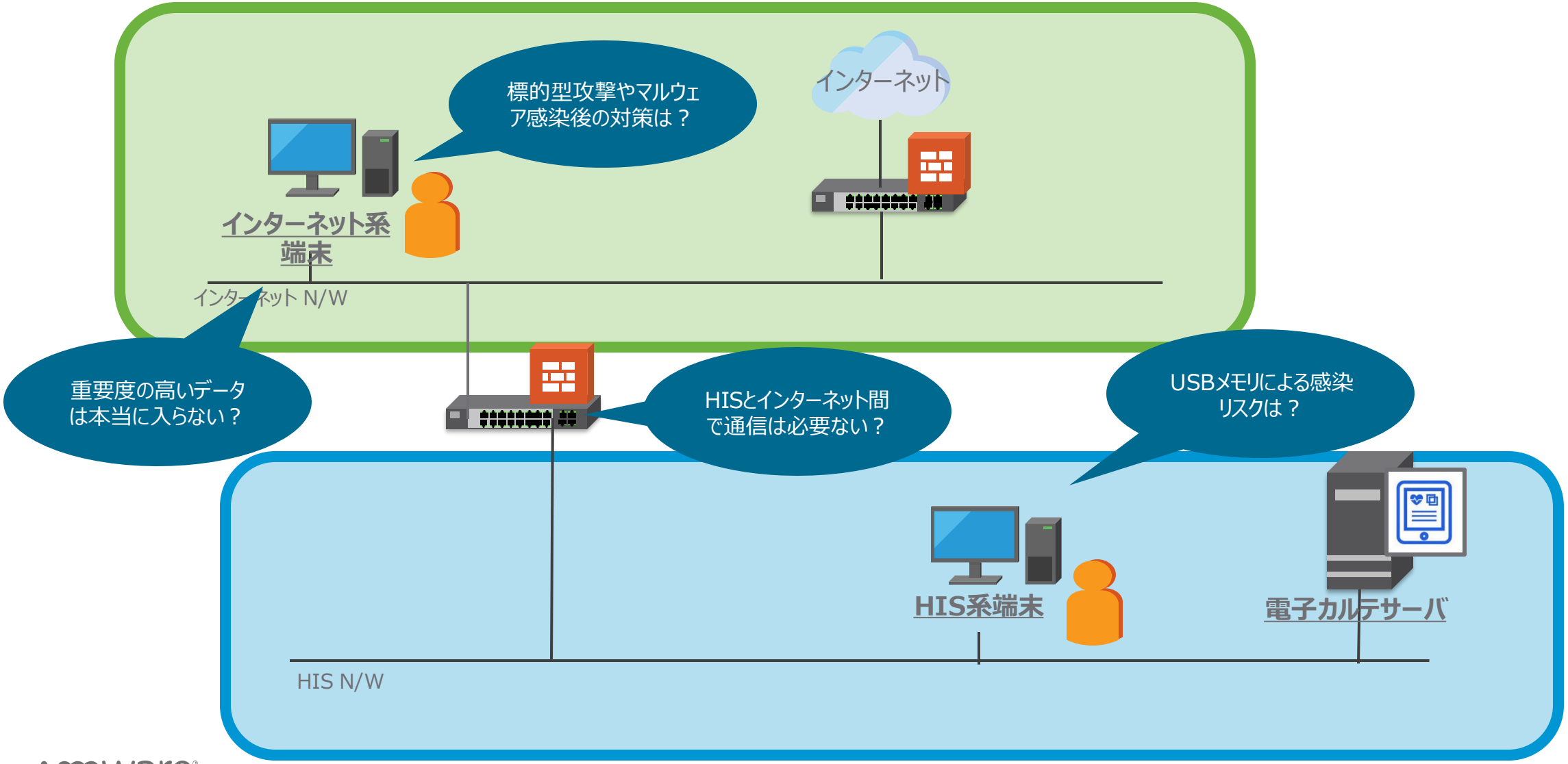
高度標的型攻撃のシナリオと対策



IPA,「『高度標的型攻撃』対策に向けたシステム設計ガイド」
(http://www.ipa.go.jp/security/vuln/newattack.html)

インターネットアクセスできるネットワークとHISネットワークを明確に分割

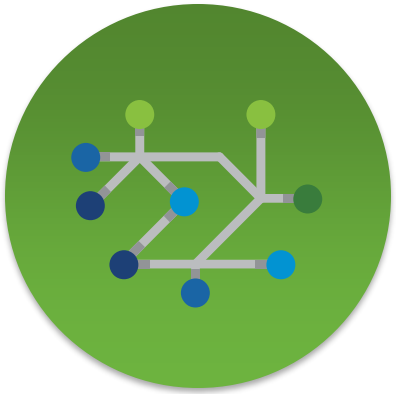
分割だけでセキュリティは確保されない？



VMwareが提案するセキュリティ強化対策

高度な
内部対策

デスクトップ仮想化

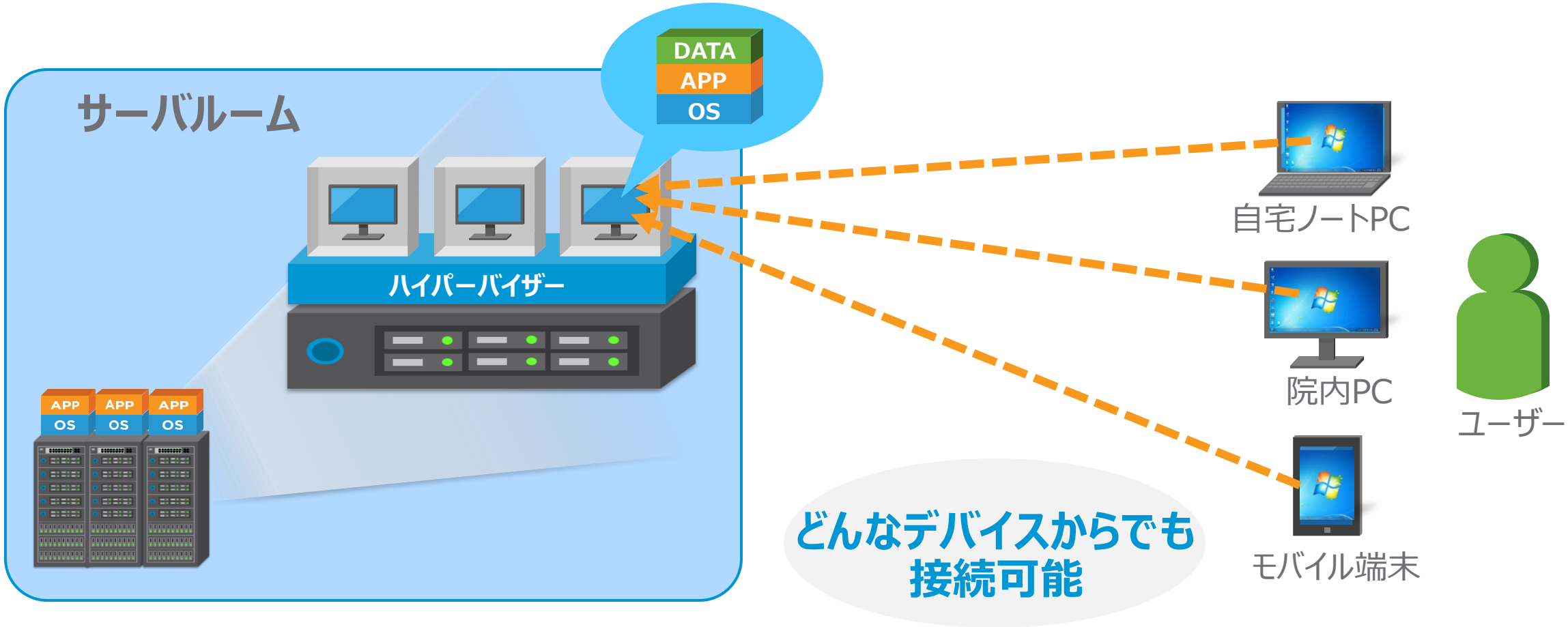


ネットワーク仮想化

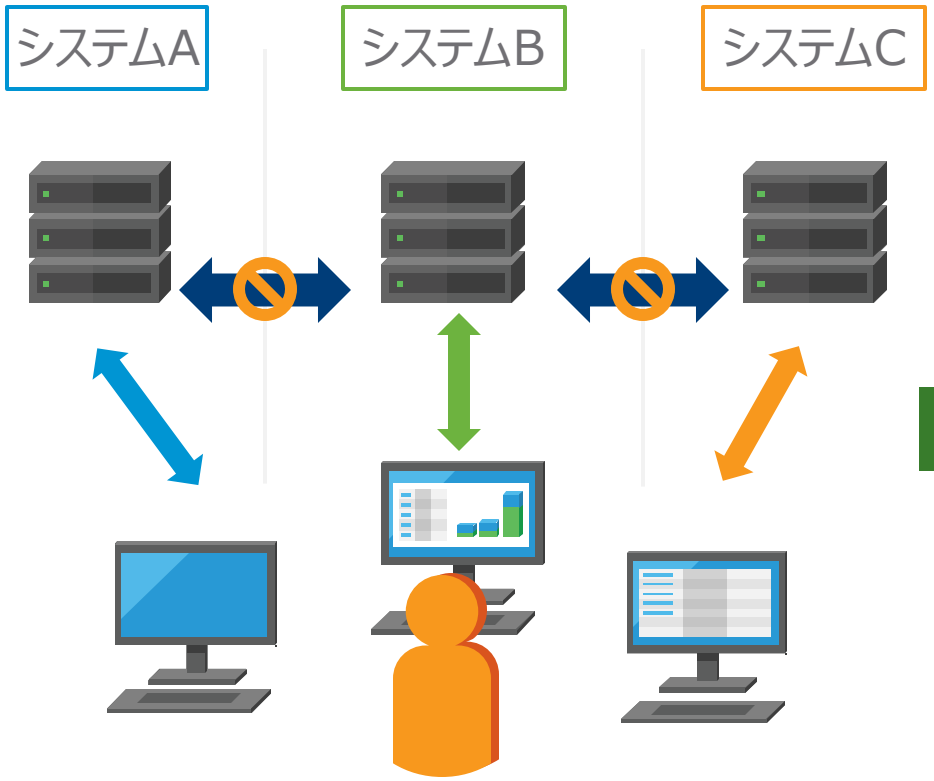
デスクトップ仮想化を利用した セキュリティ対策

VDI(デスクトップ仮想化)とは

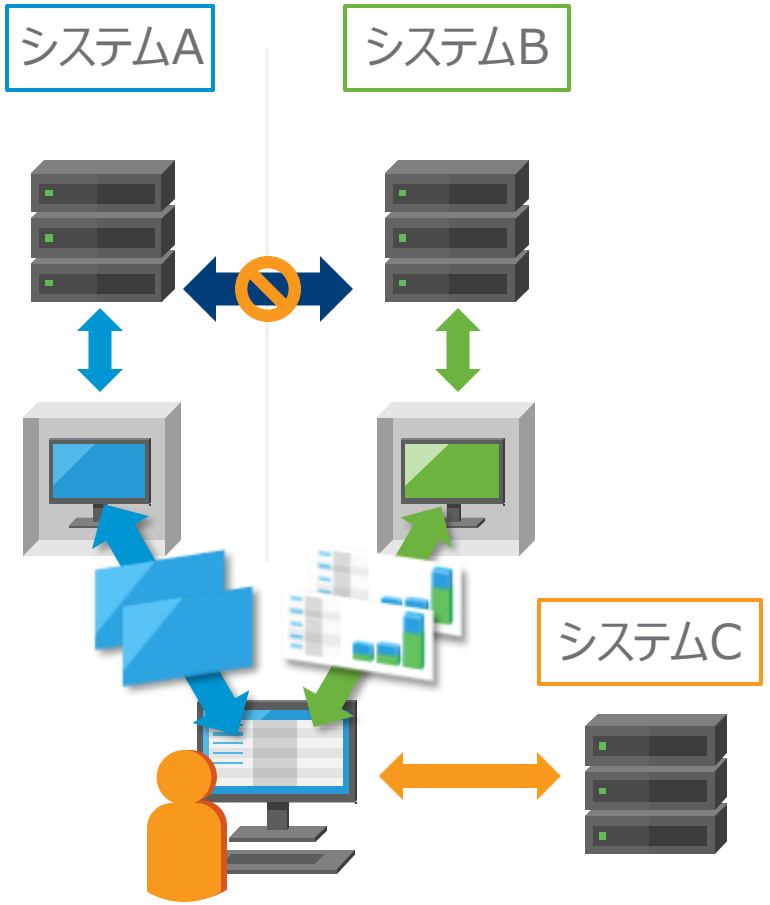
- **デバイス・場所を問わず**、画面を呼び出せる



仮想デスクトップのメリット（1）
～物理的スペースの削減～



デスクトップ仮想化

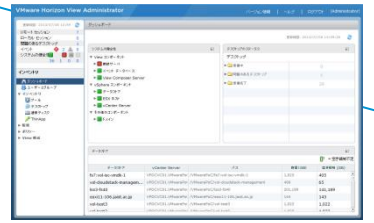


ネットワークの数に応じて
PCを増やす必要がある

ネットワークがいくつに増えても
物理端末は1台のみ

仮想デスクトップのメリット（2）
～更新・メンテナンスの自動化～

①雛形イメージとなる
Windows(1台)を作成
標準アプリがインストールされた
Windowsマシンを、vSphere上で1台作成



仮想デスクトップ
管理者

②展開したい仮想
デスクトップの台数を入力
例えば"1,000"台など、
利用した仮想デスクトップ数を入力

vCenter

Connection
Server
(接続管理サーバ)

マスタイメージ

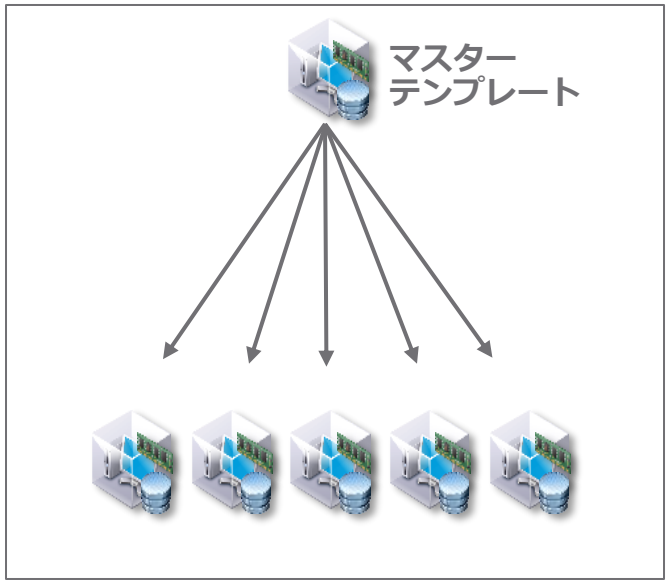
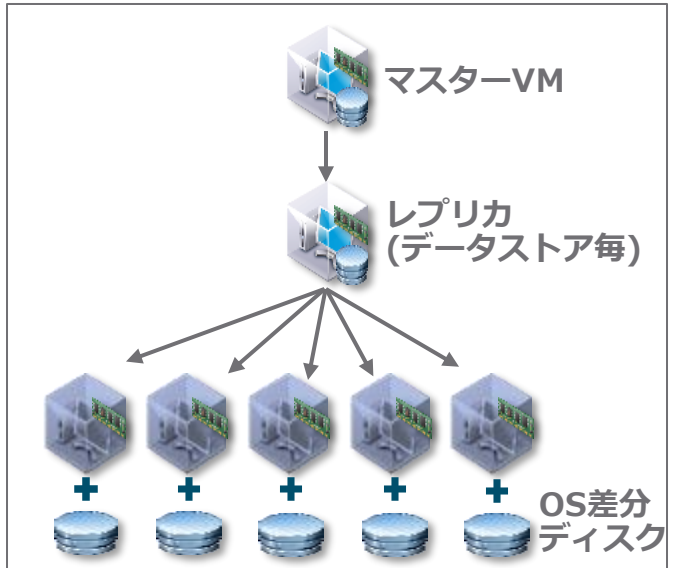
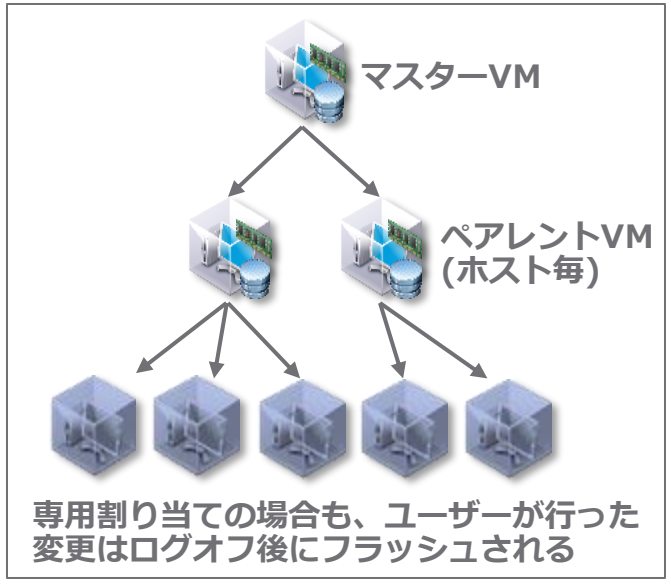
③自動的に指定台数分
仮想デスクトップがクローンされる
例えば"1,000"台と入力していたら、
1,000台の仮想デスクトップが作成される
(ホスト名やIPアドレスも適切に割り当てられる)

クローン処理
迅速な反映

ハイパーバイザー

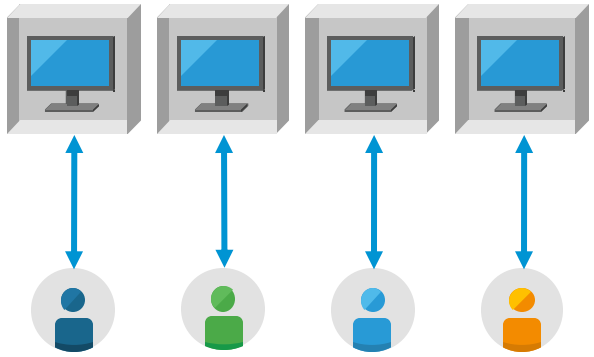
マスターの設定・アップデートを
仮想デスクトップへ迅速に反映可能

仮想デスクトップのメリット（3）
～VDI: 展開方式～

タイプ	フルクローン	リンクローン	インスタントローン
仕組み			
	全ての情報をマスターからフルコピー	OS、ディスクはマスターを共有 差分を個別に保持(ディスク容量削減)	OS、ディスク、メモリーはマスターを共有 差分は個別に保持(ディスク容量削減)
データベース	データベース不要	データベース必要	データベース不要
ユーザー自由度	高い	低い	低い
管理性	低い	高い	高い
メンテナンス	デスクトップ毎に実施	マスターへ実施	マスターへ実施
プロビジョニング	十分な時間が必要	高速(2000台の展開で約4時間)	超高速(2000台の展開で約40分)

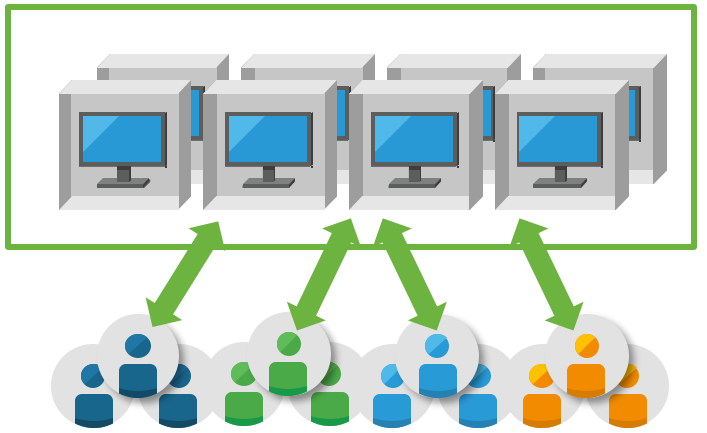
展開方法で見る仮想デスクトップの種類

専用プール



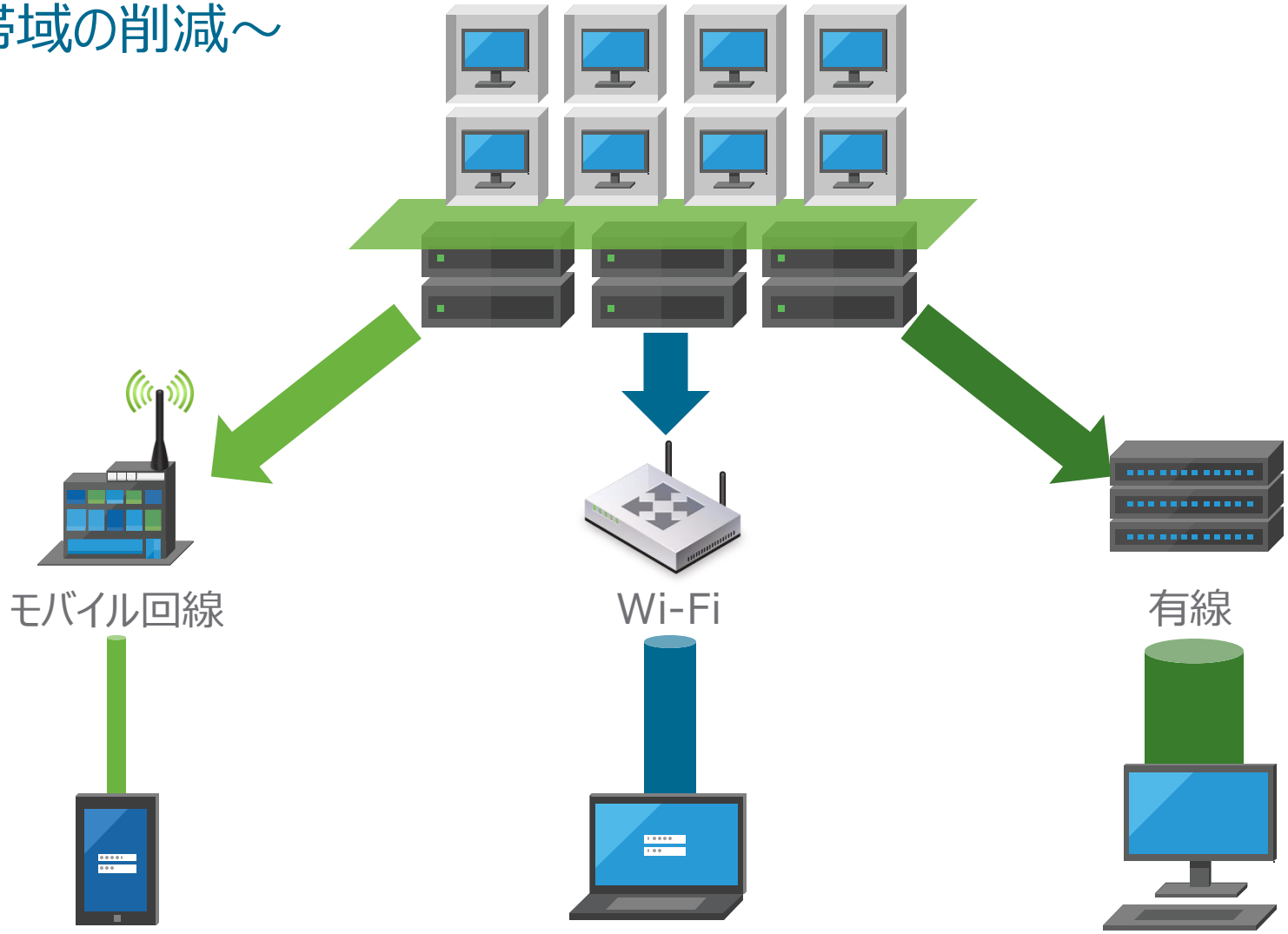
- ユーザ毎に専用のVDIを割り当て
- 一度VDIが割り当てられたユーザは常に同じVDIを使用する
- ユーザ個別のアプリのインストールなど、ユーザの自由度を高く
  する必要がある際に使用

フローティングプール



- 誰も使用していないVDIに自動的にユーザを割り当て
- 使用するVDIがログイン毎にランダムとなる
- 使用予定のユーザ数よりVDI数を少なく構築したい際に有効

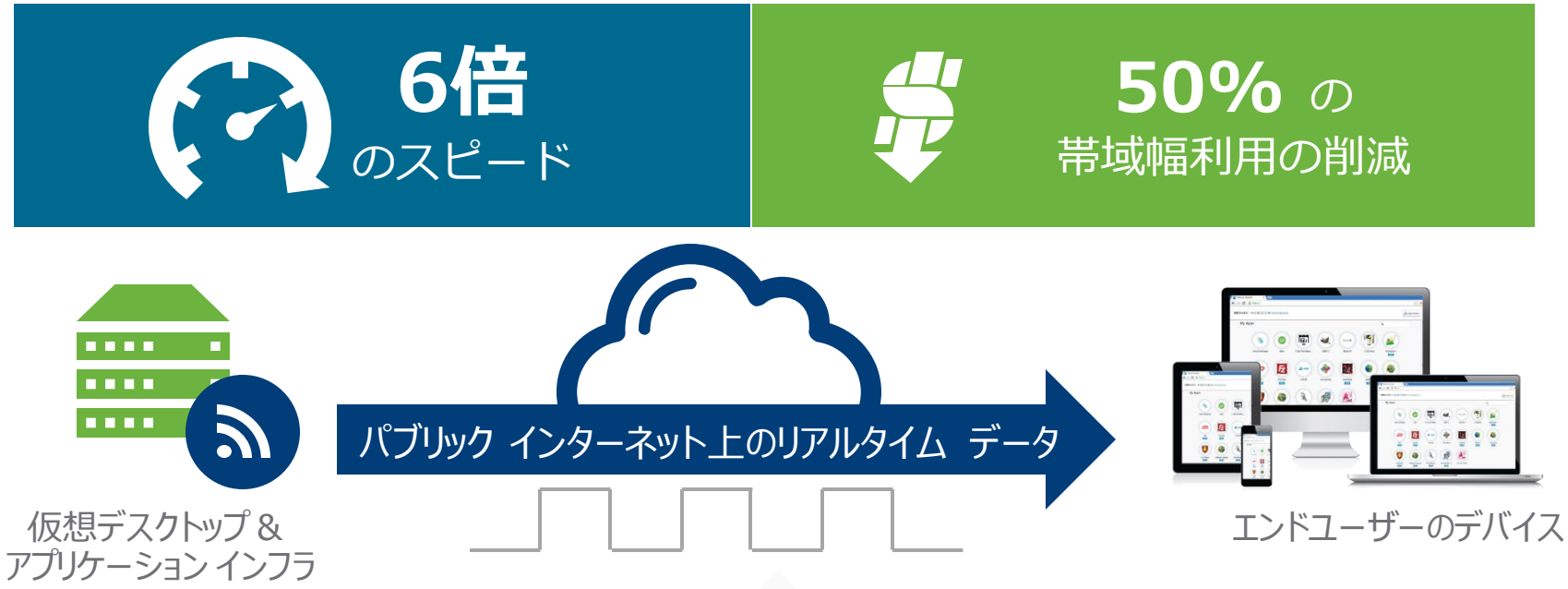
仮想デスクトップのメリット（4）
～ネットワーク帯域の削減～



使用している回線に合わせて、快適に動作する画質に自動変更

Horizonが提供する最新の画面転送プロトコル
Blast Extreme Adaptive Transport（BEAT）

- Horizon7.1で追加された **業界最高レベル** の画面転送特定通信プロトコル(Blast Extreme Adaptive Transport)の使用により**ネットワークに負荷を与えず**、最高レベルの**パフォーマンス**を提供します



主要なテクノロジー上の革新

- **適応ビットレート**
- **遅延とパケットロスの最適化**
- **エラー修正の転送**

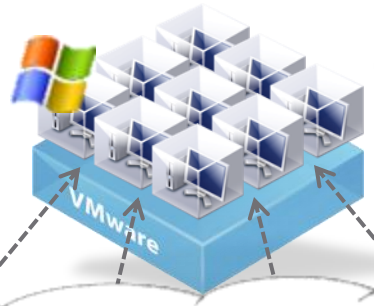
仮想デスクトップのメリット（5）
～セキュリティの向上～

管理者による
イメージ管理

最新のパッチを確実に適用

ログオフしたら
リフレッシュして
常にクリーン

バックドア防止



暗号化された
安全な画面転送
プロトコル

Network 通信の盗聴防止

画面転送に最適化されたプロトコル
(PCoIP/BEAT)

VPN アクセス不要

データ保護 &
接続端末管理不要

デバイスとデータの
分離

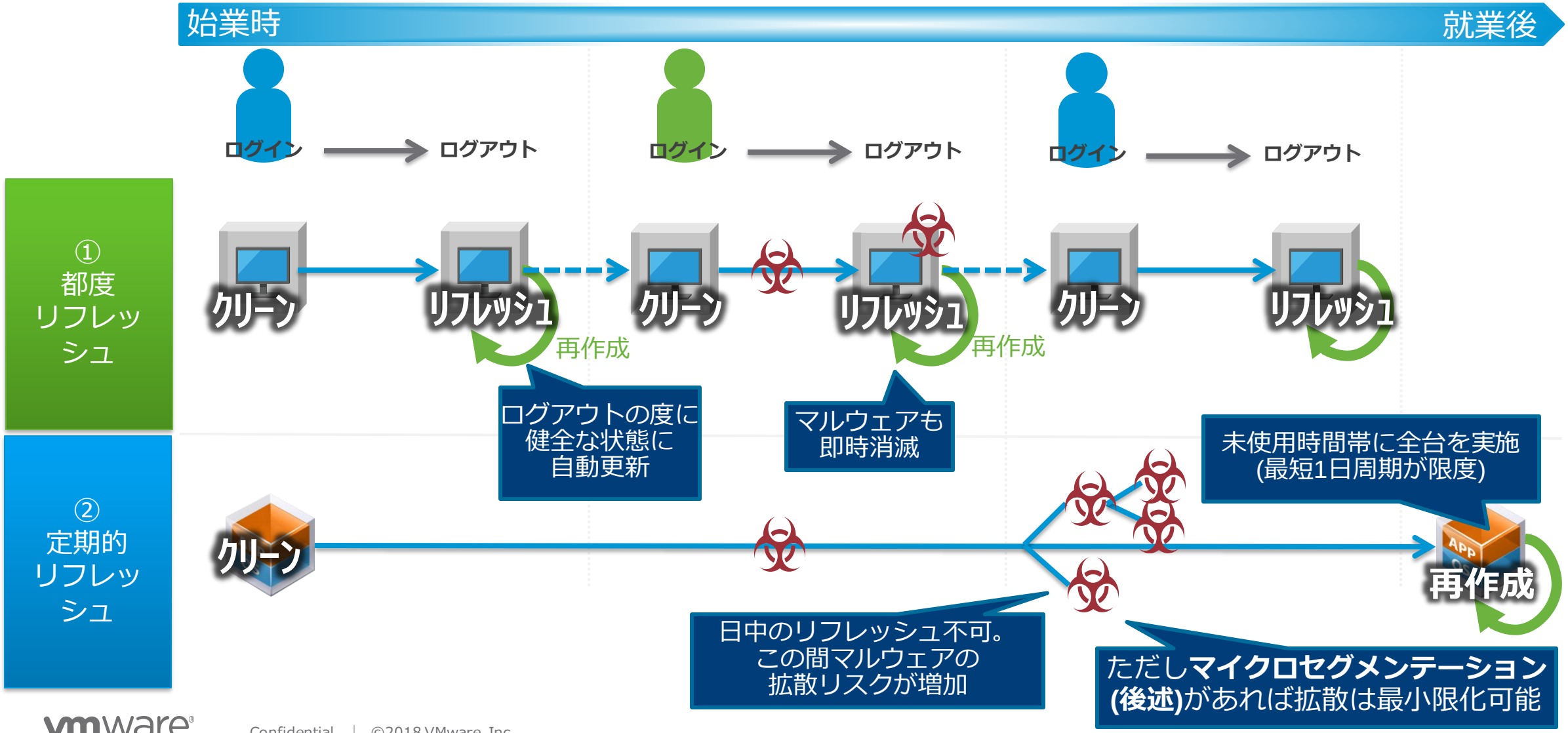
データ漏洩が
起きない環境の提供

管理者による USB
デバイス使用の制御

ユーザビリティと
セキュリティのバランス

クライアント端末と
VM 間のコピペ制御

仮想デスクトップのリフレッシュのタイミングとその影響について



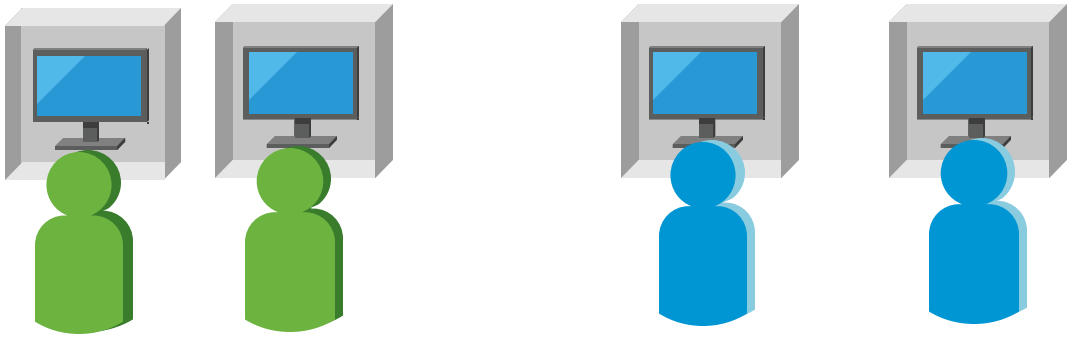
病院への仮想デスクトップの適用

VDIとRDSH(SBC)の違い

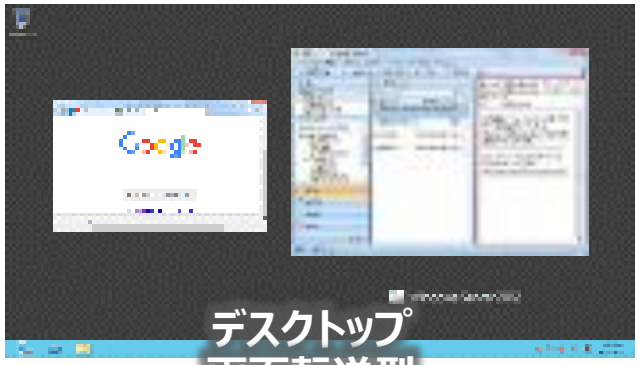
VDI(仮想デスクトップ)

1つのVDIを1人のユーザーが利用

1台のVMを１つのリモートセッションで使用する方法



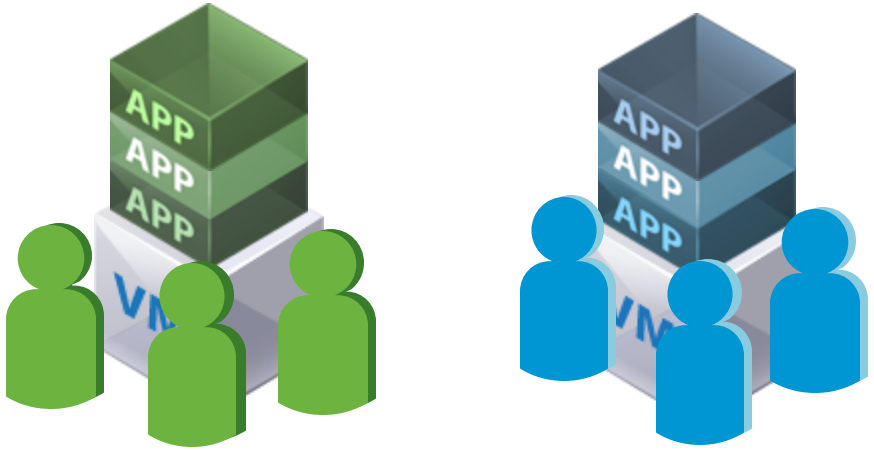
Windows7/8/10
もしくは
Windows Server 2008/2012/2016



RDSH(公開デスクトップ/公開アプリ)

1つのサーバーを複数人のユーザーが利用

1台のVMを複数のリモートセッションで使用する方法

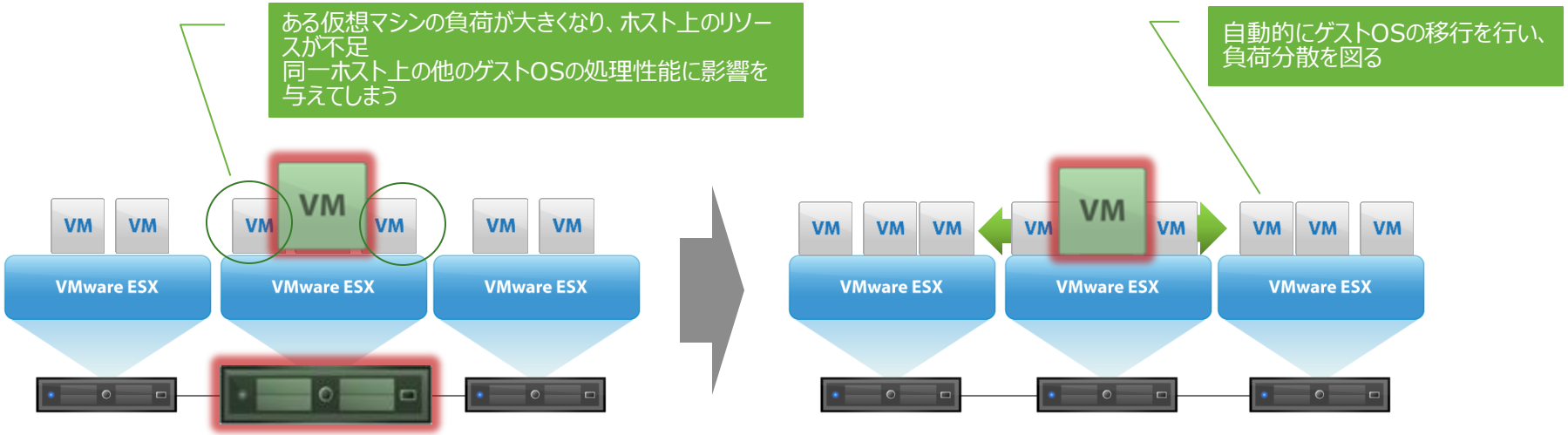


Windows Server 2008/2012/2016

VDIの場合の仮想基盤の役割(Horizonの場合)

仮想環境では予測不能な負荷にどう対処しているか？

各物理ホストのメモリ・CPU・ネットワークの負荷状況を見ながら、
自動的にvMotionを実行し、負荷を分散する機能を装備



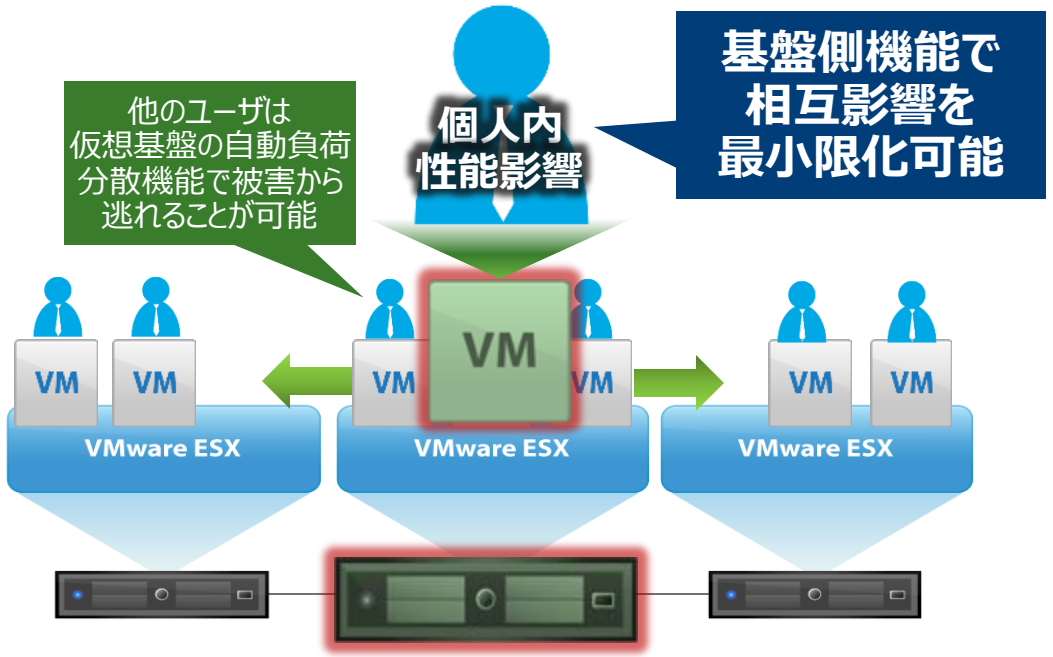
必要な性能が常に変わる仮想マシンの
確実な性能発揮
自動で最適配置

全ての物理ホストのリソースを余すことなく利用する
統合率向上

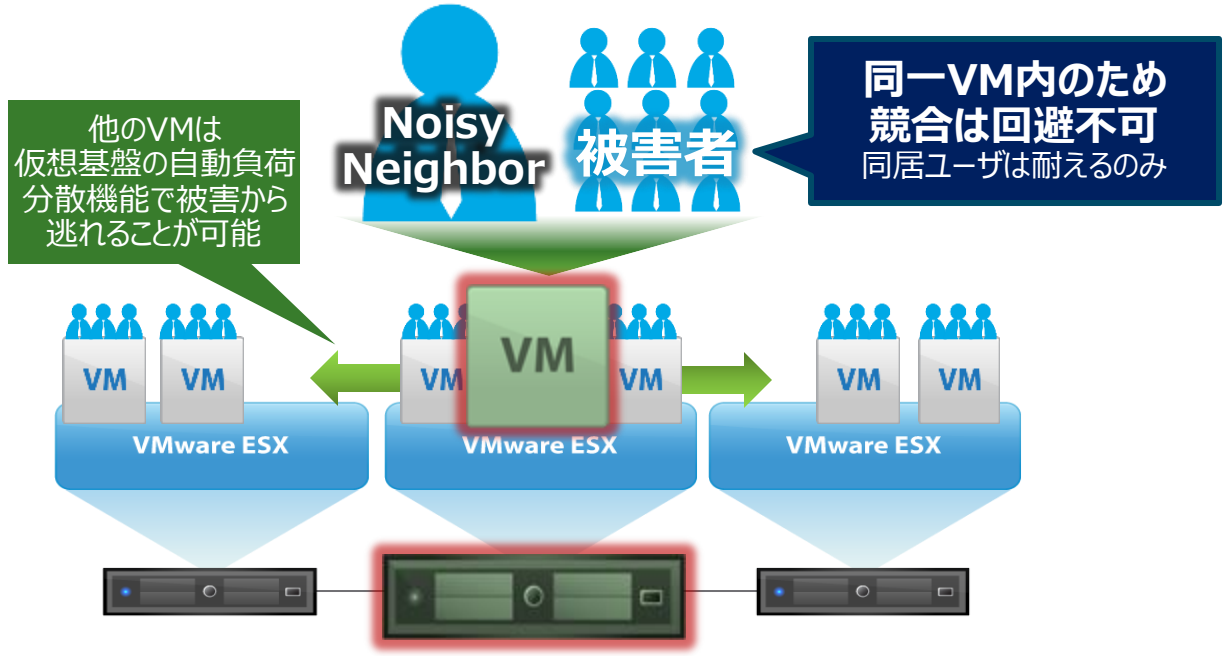
RDSHの場合の仮想基盤の役割

RDSHの最大の課題　noisy neighbor問題にどうつきあうか

VDIの場合

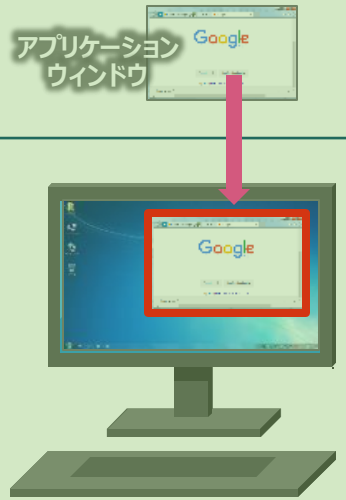
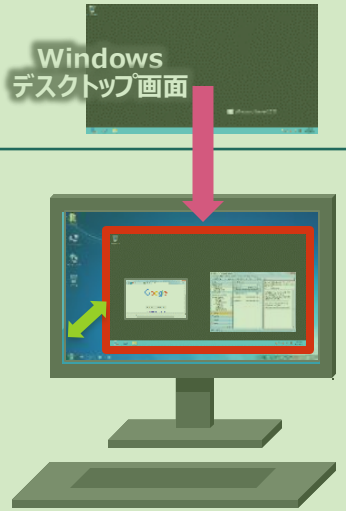
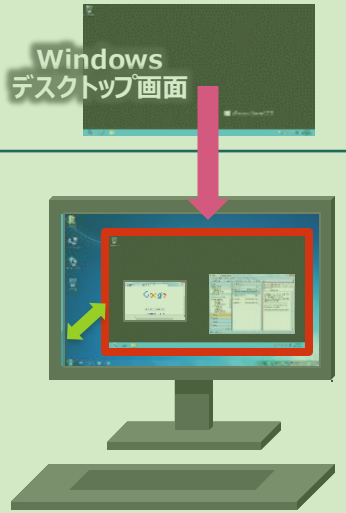
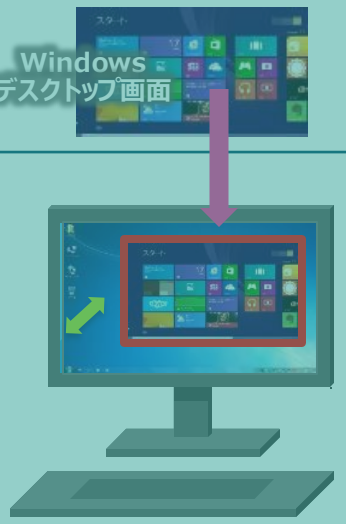
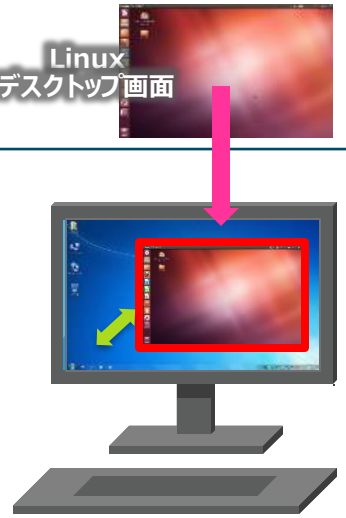


RDSH方式の場合



Horizonで提供可能な仮想デスクトップの方式

- Horizonは仮想デスクトップ・アプリケーションを利用用途に応じて様々な方式で提供が可能です

提供パターン	アプリケーションウィンドウ 画面転送	Windows Server RDSH デスクトップ画面転送	Windows Server VDI デスクトップ画面転送	Windows Client VDI デスクトップ画面転送	Linux VDIデスクトップ 画面転送
画面転送対象 (仮想基盤上で稼働)	アプリケーション ウィンドウ	Windows デスクトップ画面	Windows デスクトップ画面	Windows デスクトップ画面	Linux デスクトップ画面
操作イメージ (接続端末)					
仮想化方式	SBC方式 (複数ユーザ：1VM)			VDI方式 (1ユーザ：1VM)	
相互性能影響範囲	数十ユーザ			1ユーザのみ	
アプリ制限	サーバOS対応 + マルチユーザ対応		サーバOS対応	制限なし	Linux OS対応
MS ライセンス	OS + RDS CAL			VDA	無し

インターネット

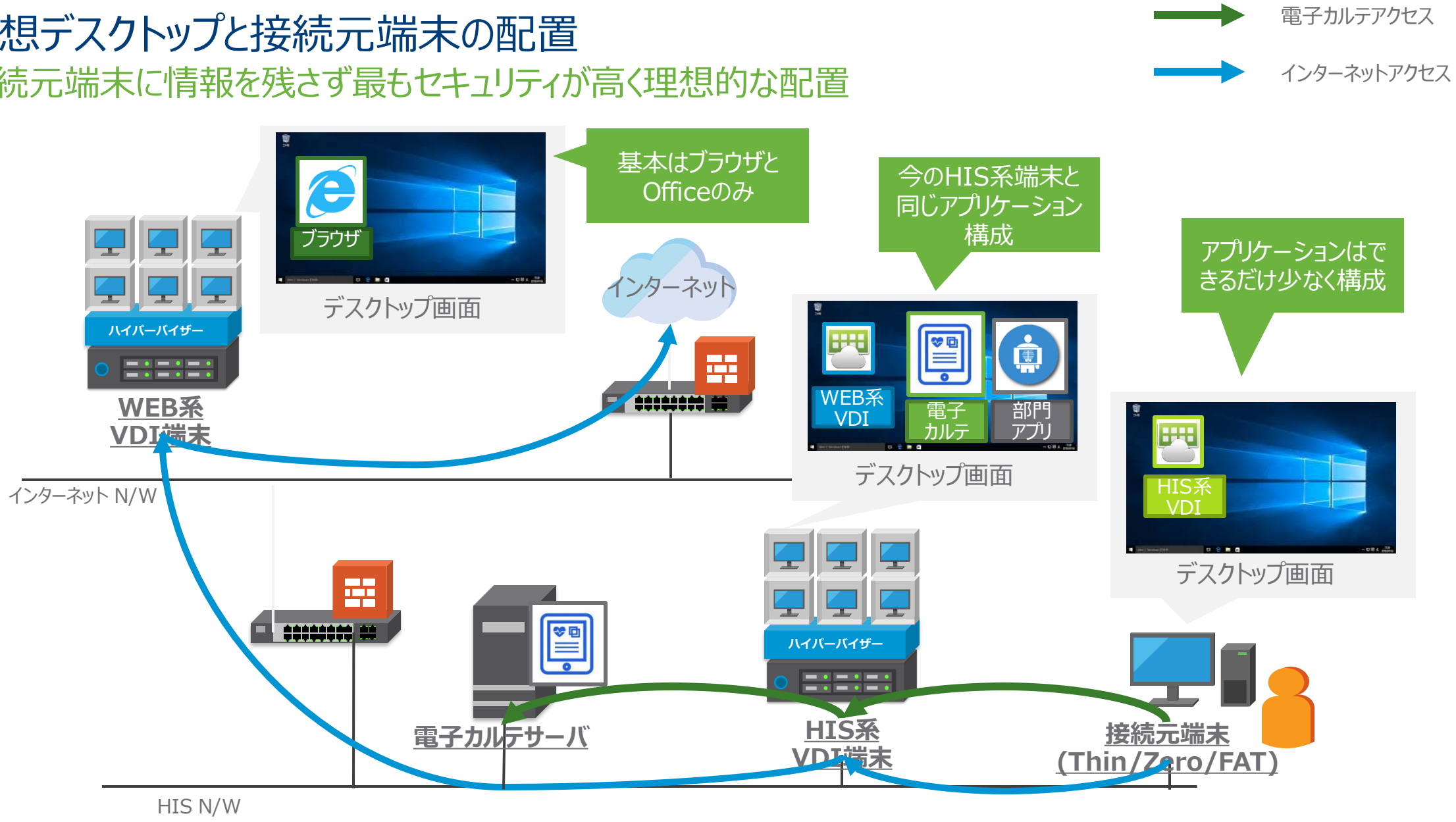
HIS

実装方式別の比較

	RDSHアプリケーション 画面転送	RDSHデスクトップ 画面転送	Windows Client VDI デスクトップ画面転送	Linux VDIデスクトップ 画面転送	Windows Server VDI デスクトップ画面転送
ユーザ共有範囲	数十～数百ユーザー：1OS（共有型モデル）		1ユーザー：1OS（占有型モデル）		
MS必要ライセンス	サーバーOS RDS CAL		クライアントOS VDA		サーバーOS RDS CAL
インフラコスト	低	低	高	高	高
仮想クライアント ライセンス単価コスト	高	高	低	低 もしくは 高(※)	低
大規模時の総コスト	○		×	◎ もしくは×(※)	△
複数アプリケーション 操作性	×(利便性低下)	○（従来通りの利便性）		×（慣れと妥協が必要）	○（従来通りの利便性）
アプリケーション制限	サーバーOSで動作可能アプリ マルチユーザー対応アプリ		従来通り	Linux OS 対応アプリ	サーバーOSで 動作可能アプリ
相互性能影響範囲 (noisy neighbor)	数十～数百ユーザー		1ユーザのみ		
デスクトップ健全化	リフレッシュしづらい (拡散しやすい)		ログアウト後、随時可能 (拡散しにくい)	リフレッシュしづらい (拡散しやすい)	ログアウト後、随時可能 (拡散しにくい)
ログ追跡性	△		○		
マルウェア拡散防止単位 (マイクロセグメンテーション)	ユーザ単位				

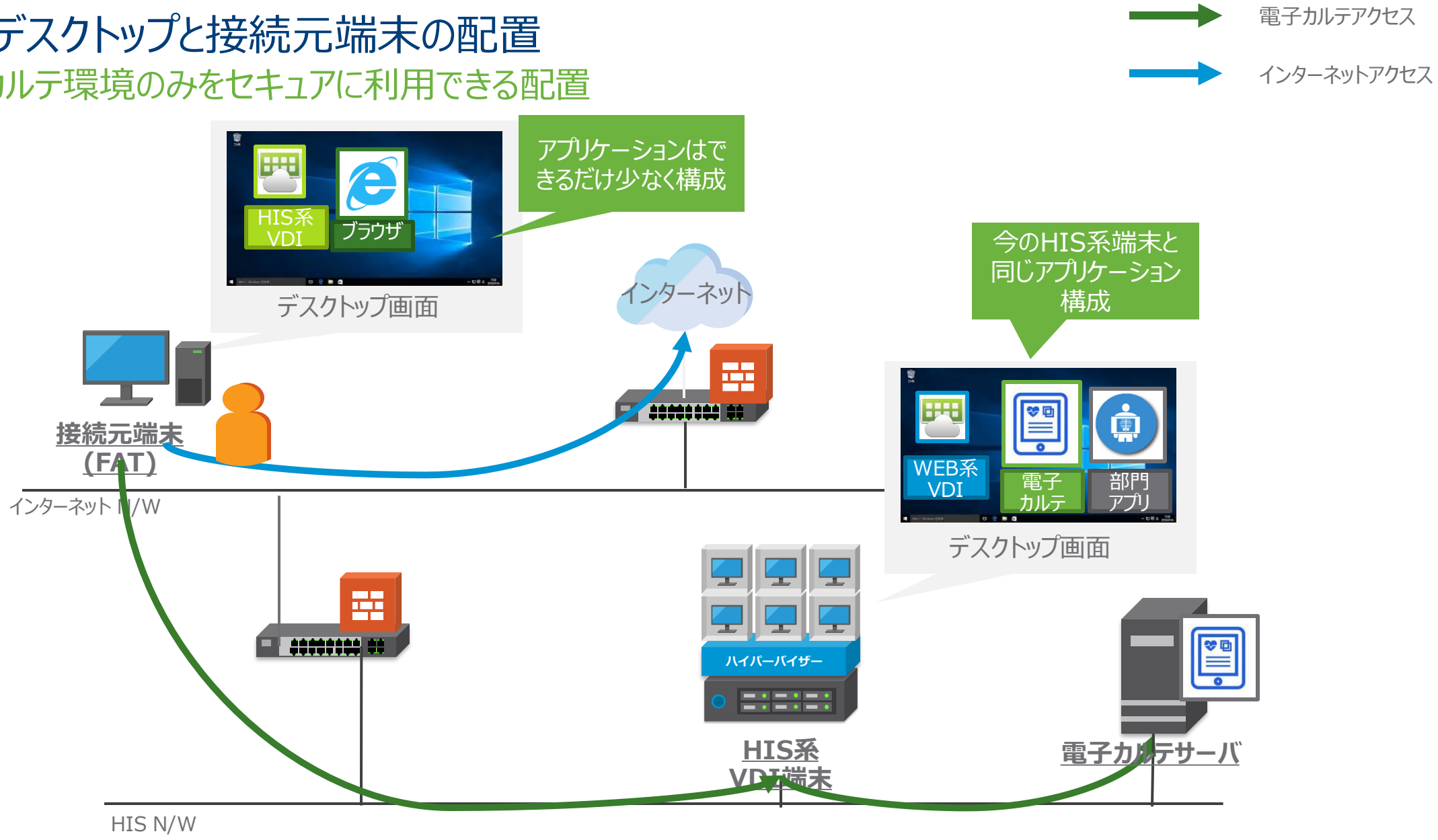
仮想デスクトップと接続元端末の配置

接続元端末に情報を残さず最もセキュリティが高く理想的な配置



仮想デスクトップと接続元端末の配置

電子カルテ環境のみをセキュアに利用できる配置



医療情報システムの安全管理に関するガイドライン　第5版

6.5 技術的安全対策

(3)　アクセスの記録（アクセスログ）

個人情報を含む資源については、全てのアクセスの記録（アクセスログ）を収集し、定期的にその内容をチェックして不正利用がないことを確認しなければならない。

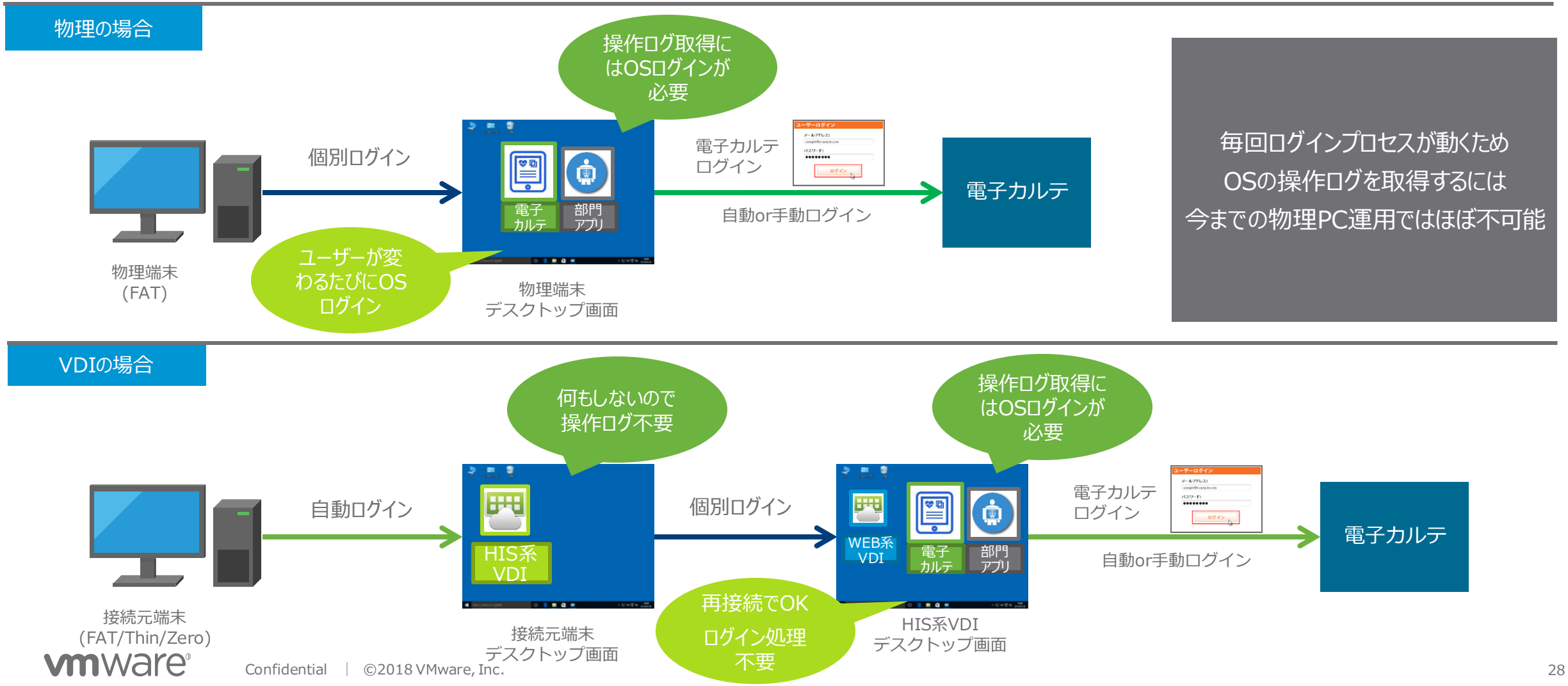
アクセスログは、それ自体に個人情報が含まれている可能性があること、さらにはセキュリティ事故が発生した際の調査に非常に有効な情報であることから、その保護は必須である。従って、アクセスログへのアクセス制限を行い、アクセスログへの不当な削除／改ざん／追加等を防止する対策を講じなければならない。

また、アクセスログの証拠性確保のために、記録する時刻は重要である。精度の高いものを使用し、管理対象の全てのシステムで同期を取らなければならない。

なお、医療機関等において取り扱っている医療情報システムにアクセスログを収集する機能がない場合には、システム操作に係る業務日誌等を作成し、操作の記録（操作者及び操作内容等）を管理する必要がある。

OS操作ログ取得のためのログインフロー

物理運用の限界



ネットワーク仮想化を組み合わせた セキュリティ対策

医療情報システムの安全管理に関するガイドライン 第5版

6.10 災害、サイバー攻撃等の非常時の対応

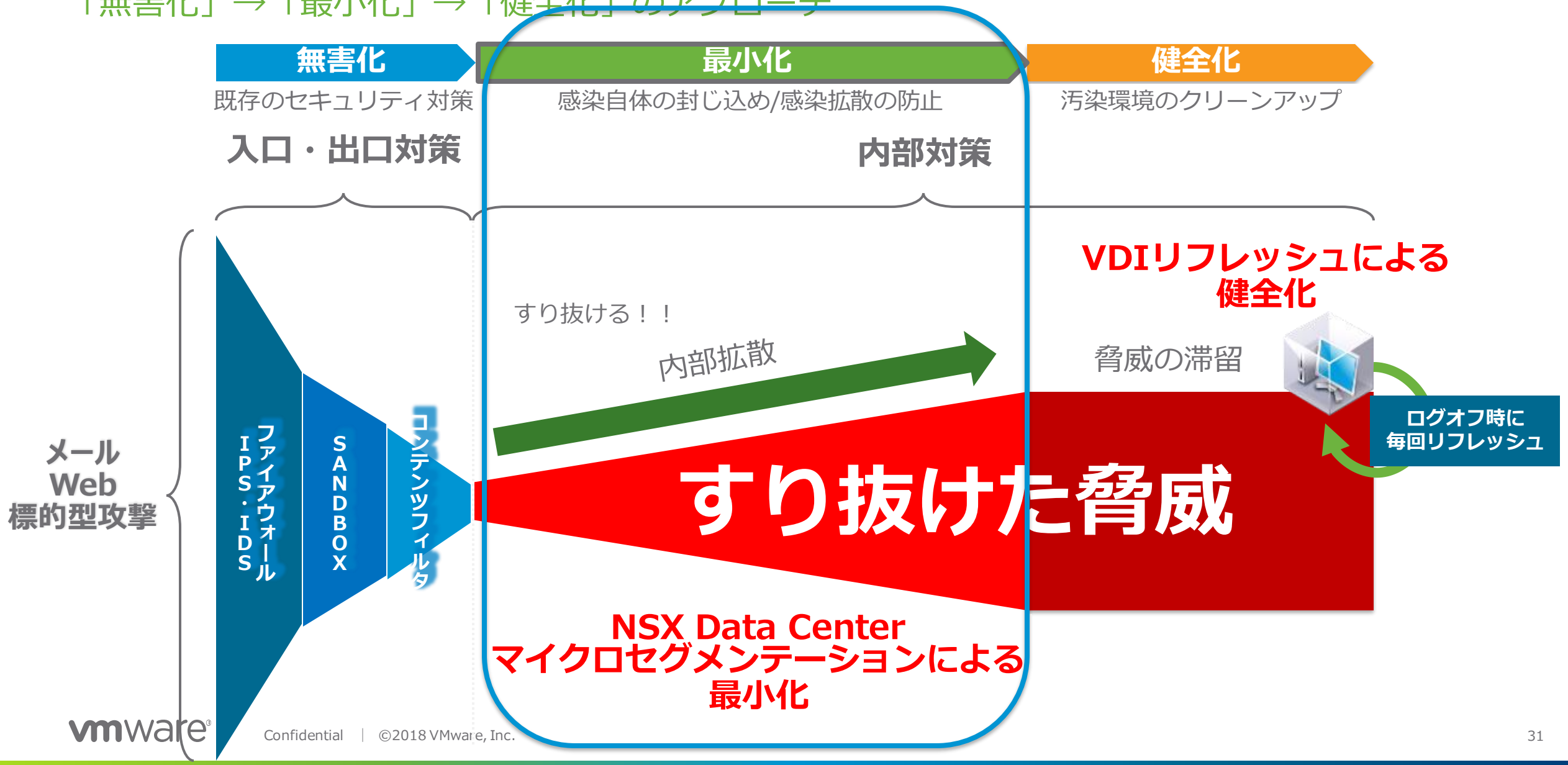
(3) サイバー攻撃を受けた際の非常時の対応

標的型メール攻撃等により医療情報システムがコンピュータウイルス等に感染した場合、以下の対応等を行う必要が生じる場合がある。これらに備え、関係先への連絡手段や紙での運用等の代替手段を準備する必要がある。

- 攻撃を受けたサーバ等の遮断や他の医療機関等への影響の波及の防止のための外部ネットワークの一時切断
- 他の機器への感染拡大の防止や情報漏えいの抑止のための当該感染機器の隔離
- 他の機器への波及の調査等被害の確認のための業務システムの停止
- マルウェア等に感染した場合、バックアップからの重要なファイルの復元（重要なファイルは数世代バックアップを取得することが望ましい）

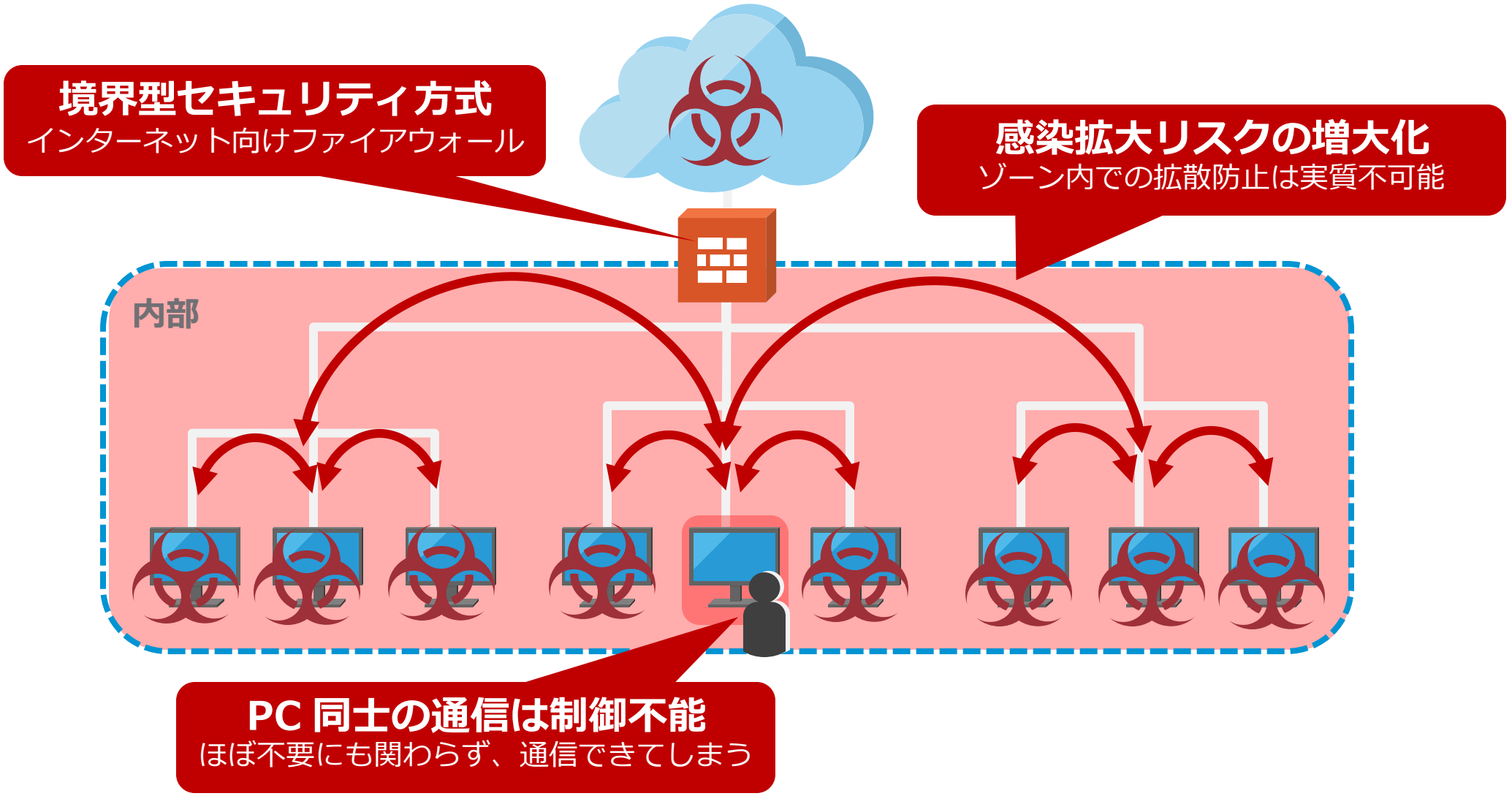
未知の不正プログラム感染に対する対応

「無害化」→「最小化」→「健全化」のアプローチ



マルウェアに対する情報漏洩リスクの最小化

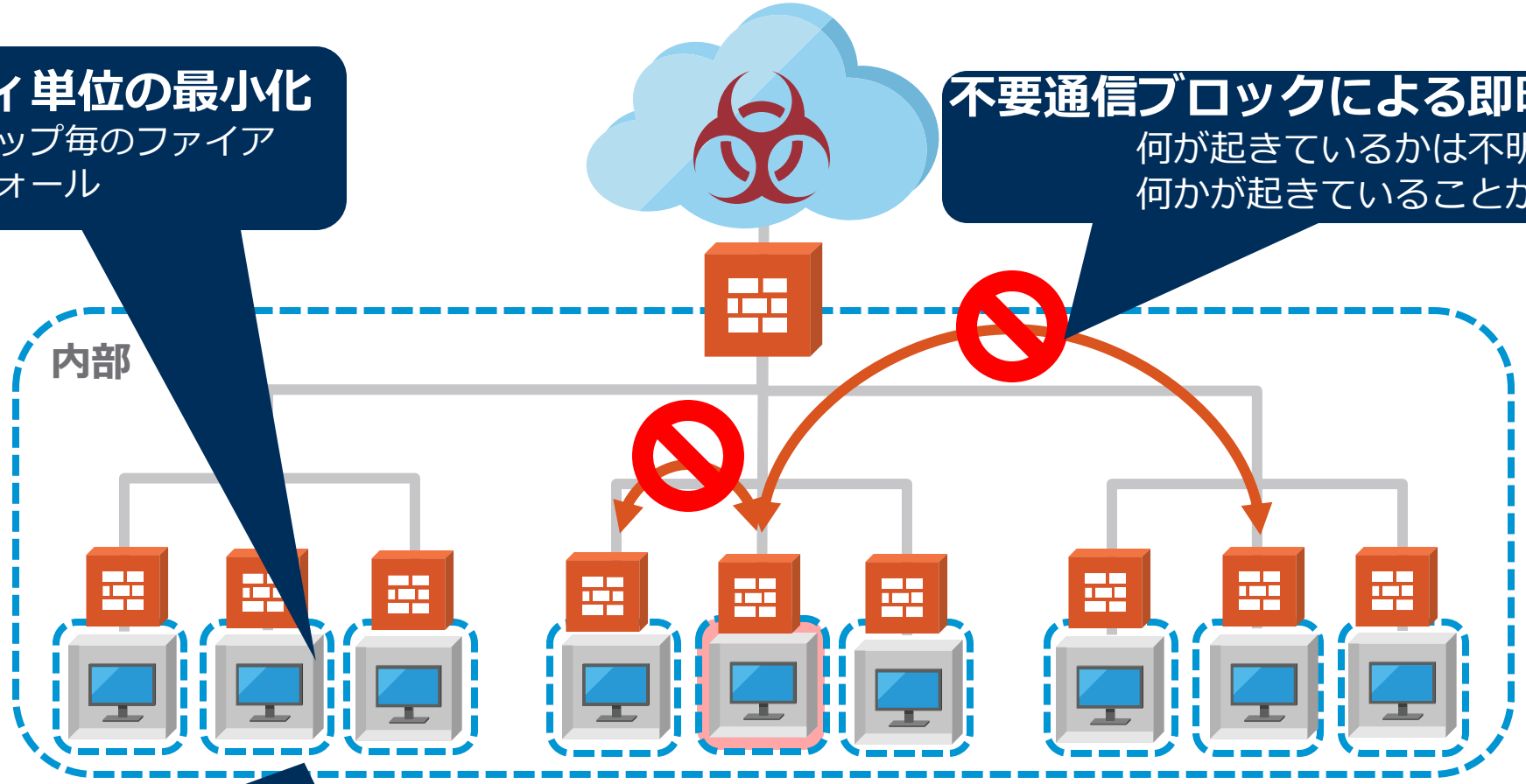
物理PCでのセキュリティ保護の限界



マルウェアに対する情報漏洩リスクの最小化
仮想デスクトップ+ネットワーク仮想化による「マイクロセグメンテーション」

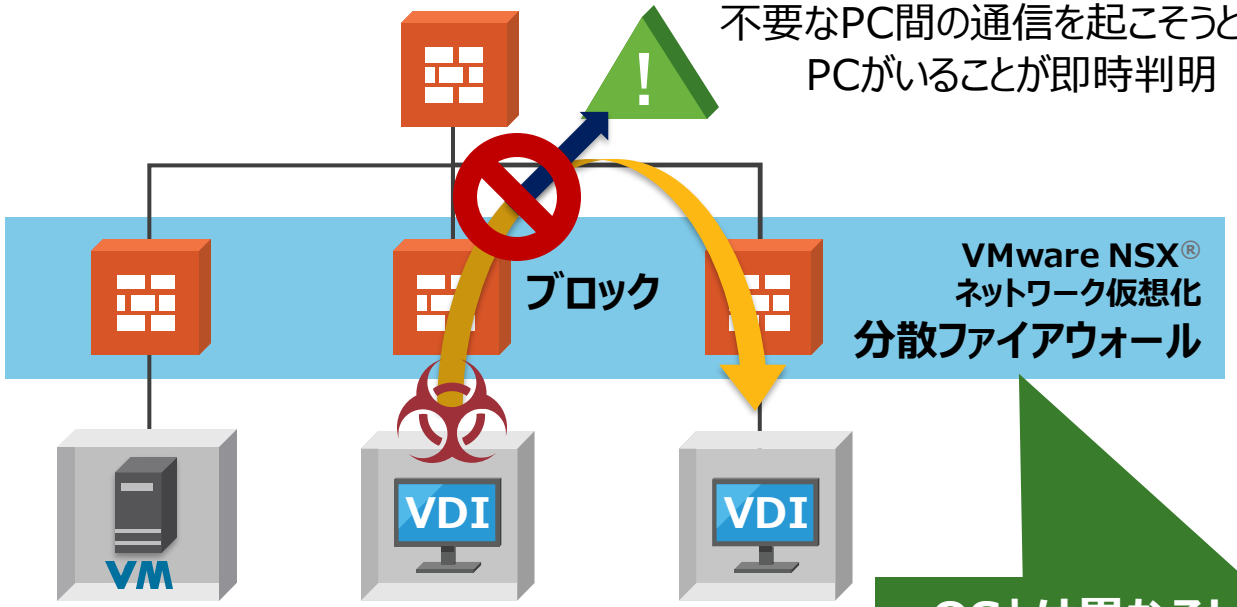
セキュリティ単位の最小化
仮想デスクトップ毎のファイア
ウォール

不要通信ブロックによる即時疑義端末特定
何が起きているかは不明だが、
何かが起きていることがわかる



「マイクロセグメンテーション」
不要なPC間の通信のブロック

ネットワーク仮想化の分散ファイアウォール



分散ファイアウォール適用単位

1. **仮想マシン**
   仮想マシンもしくは仮想NIC単位
2. **リソースプール**
   仮想マシングループ単位
3. **仮想ネットワーク**
   仮想スイッチ、セグメント(=ポートグループ)

OSとは異なるレイヤーのファイアウォール

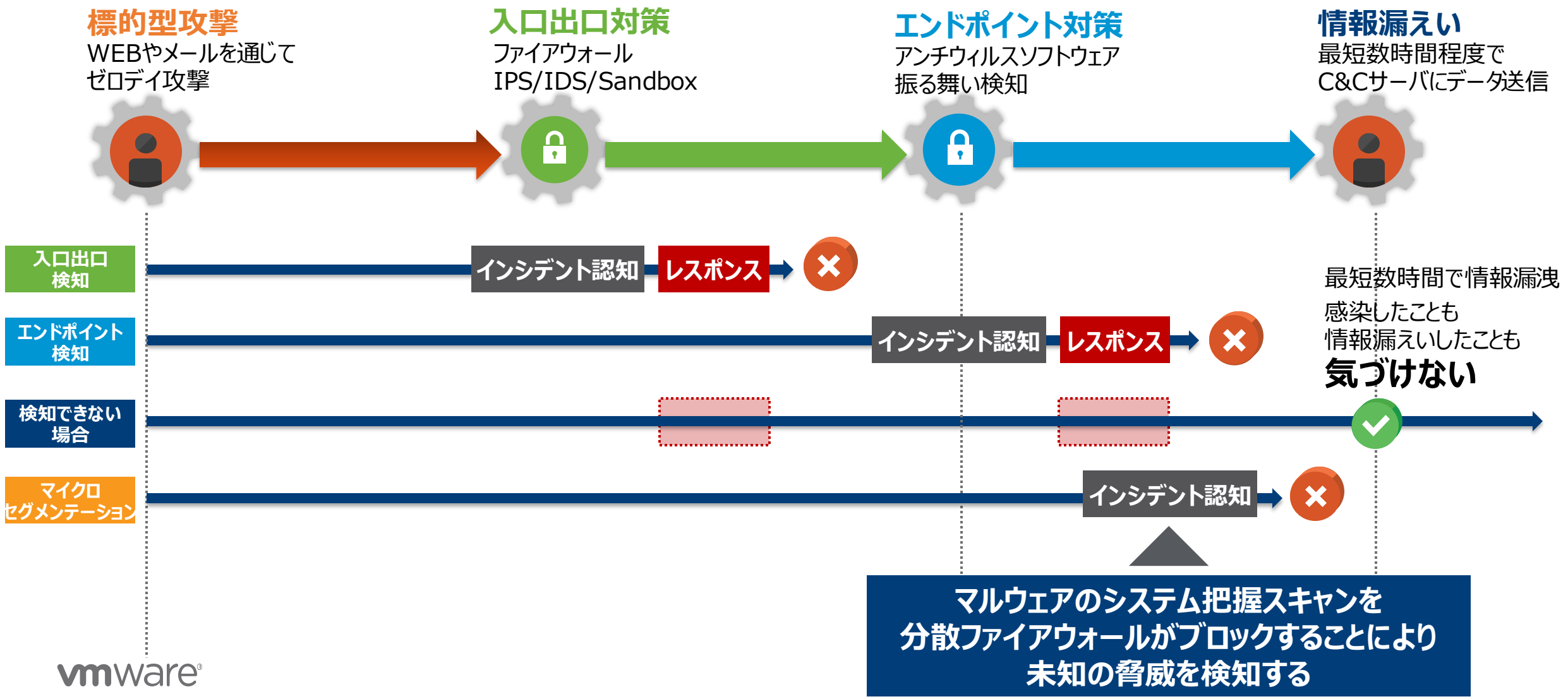
機器・運用コストの簡素化

#	送信元	宛先	ポート番号	許可／拒否
1	VDIグループ	VDIグループ	すべて	拒否
2	仮想マシンA	VDI	23	許可
3				

VDI間の通信はすべて不要のため、わずか１行で高セキュリティを実現可能

内部情報漏洩対策

『マイクロセグメンテーション』によって変わるインシデントレスポンスの流れ



セキュリティーパートナーとの連携ソリューション

次世代
ファイアウォール

マルウェア検知

脆弱性管理

paloalto NETWORKS

TREND MICRO

RAPID7

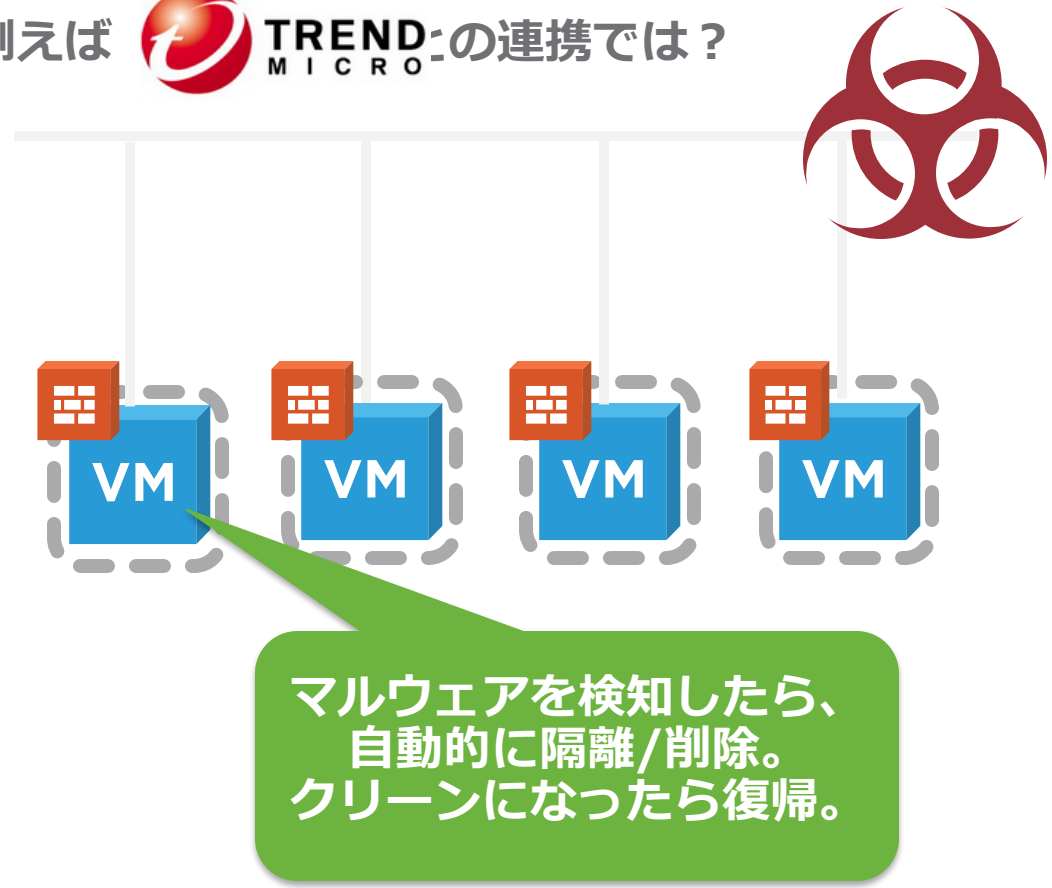
Check Point SOFTWARE TECHNOLOGIES LTD.

Symantec

FORTINET

intel Security

例えば TREND MICRO の連携では？



まとめ

高度な内部対策 ＝ デスクトップ仮想化 ＋ ネットワーク仮想化

デスクトップ仮想化によるセキュリティ対策

- 物理PCによる対策の限界
- インターネット環境とHIS環境を分けただけでは不十分
- HIS環境の操作ログを取得するにはデスクトップ仮想化技術が必須

ネットワーク仮想化によるセキュリティ対策

- 感染しても拡散防止/気づきができる
- ルール設定も簡単なので運用が楽
- ウイルス対策ソフトと連携したネットワーク隔離が可能

Thank You

Please email any questions rtakehara@vmware.com