

仮想デスクトップによる 院内セキュリティ強化

VMware Horizonで、利便性の高い
セキュアなクライアント環境を実現

VMware株式会社
公共SE統括部 公共第二SE部

山崎康太

2019年9月26日

Agenda

1. 院内セキュリティの現状
2. VMwareの仮想デスクトップテクノロジー
3. ネットワーク仮想化との連携による更なるセキュリティの強化
4. 事例のご紹介

1.院内セキュリティの現状

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

医療福祉は
21件 5.4%

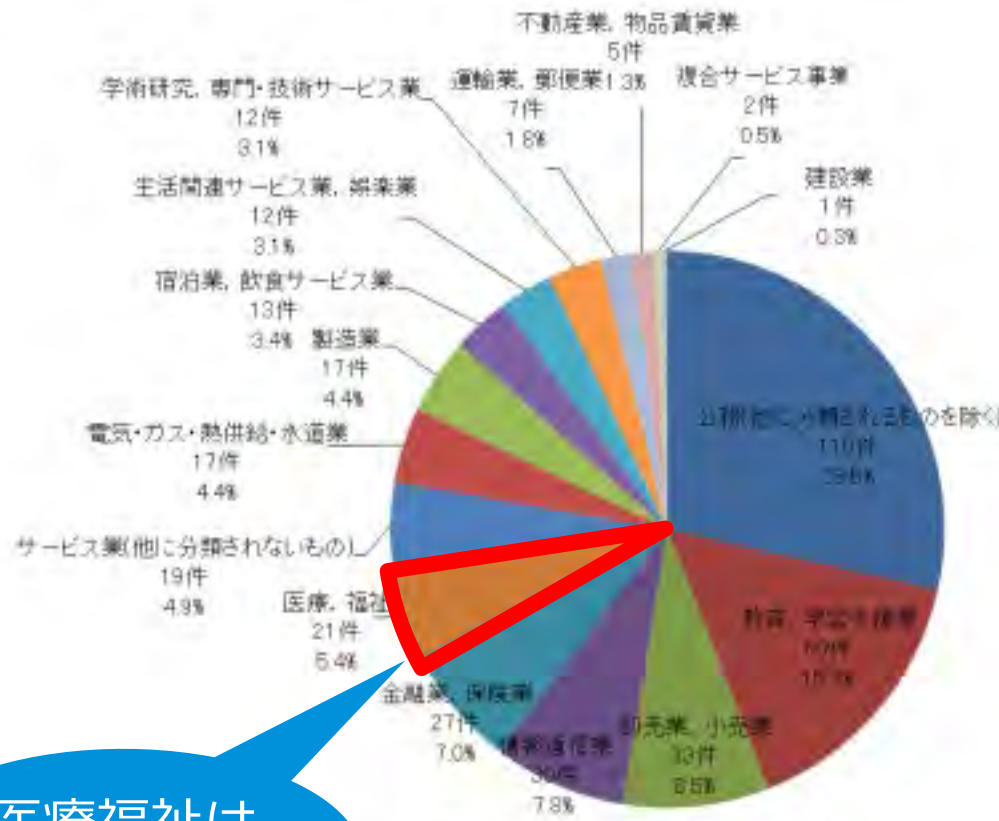


図 1：業種別の漏えい件数

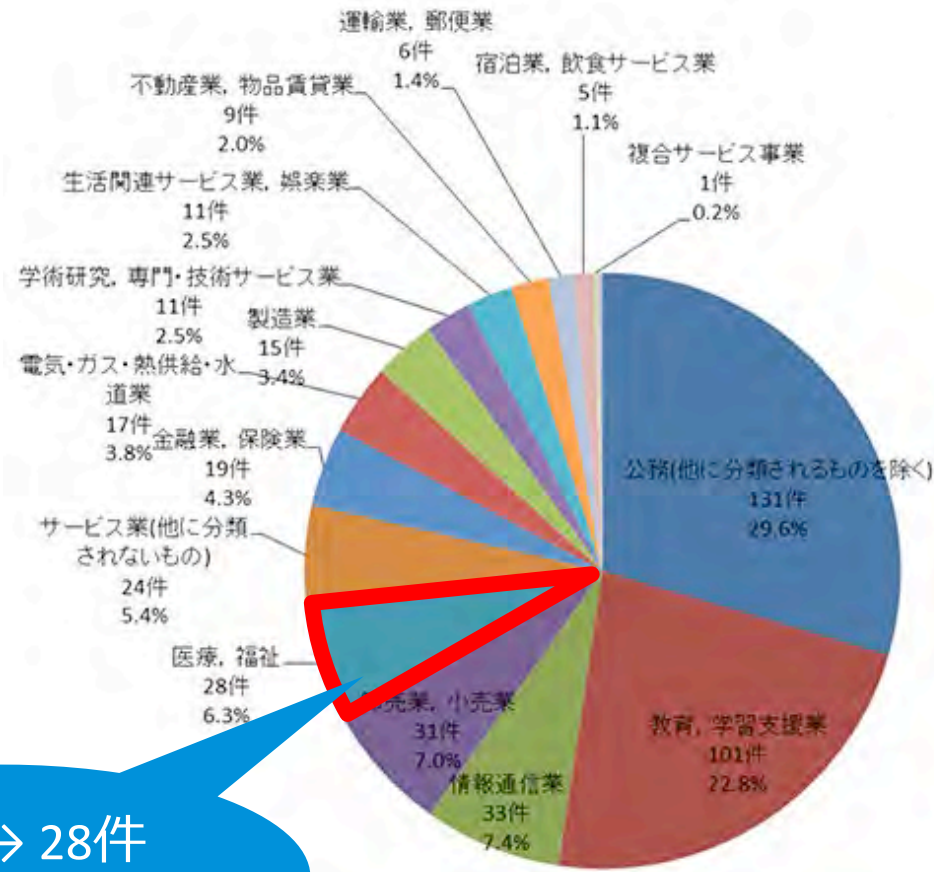
2018年度版

インシデント発生時の影響は更に拡大

出典：2018年情報セキュリティインシデントに関する調査結果～個人情報漏えい編～(速報版)
https://www.jnsa.org/result/incident/data/2018incident_survey_sokuhou.pdf

	2018年データ	2017年データ
漏えい人数	561万3,797人	519万8,142人
漏えい件数	443件	386件
想定損害賠償総額	2,684億5,743万円	1,914億2,742万円
一件当たりの漏えい人数	1万3,334人	1万4,894人
一件当たり平均想定損害賠償額	6億3,767万円	5億4,850万円
一人当たり平均想定損害賠償額	2万9,768円	2万3,601円

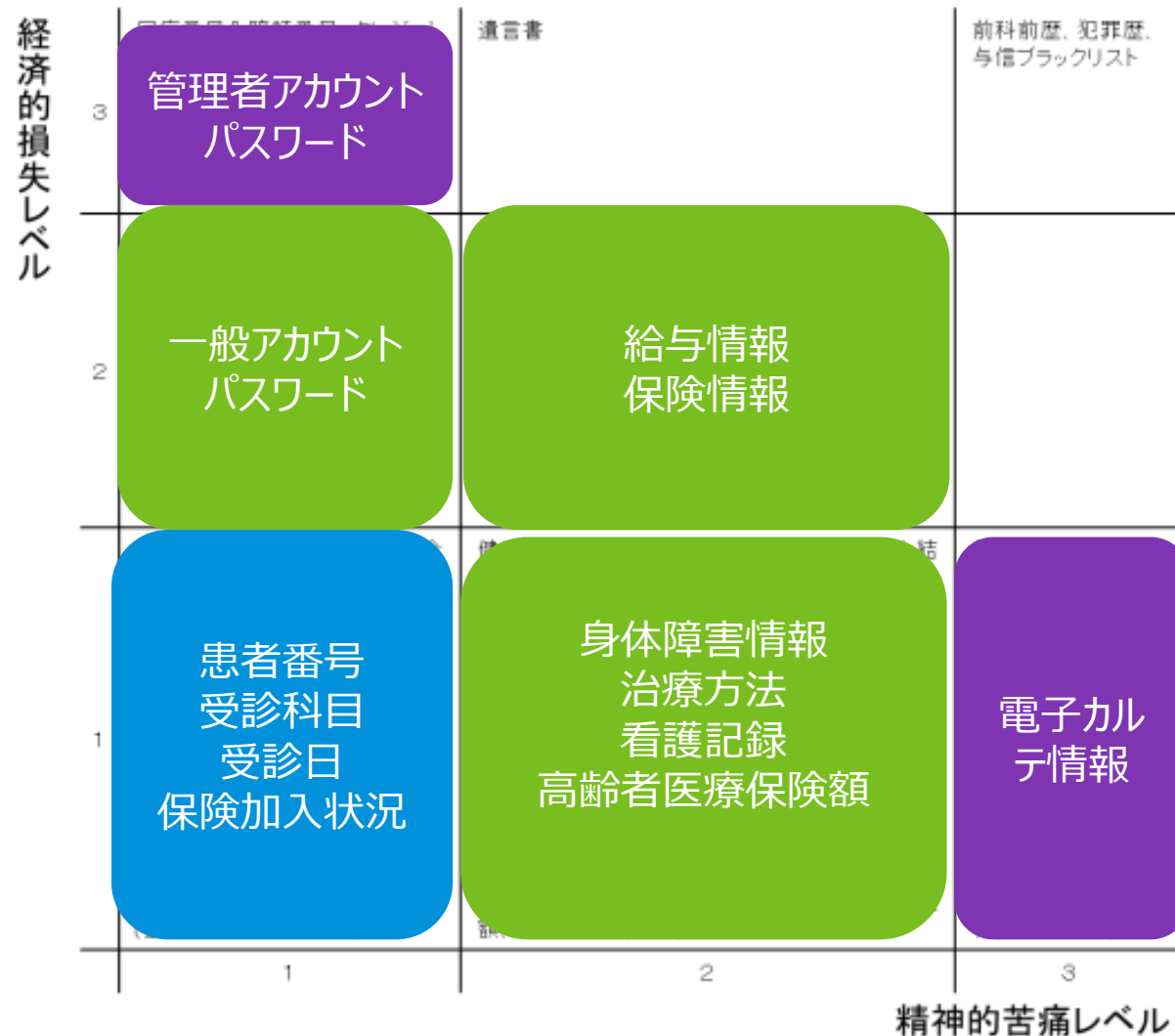
件数/人数/金額ともに更に増加
社会的信頼を大きく損ねる
可能性も



21件 → 28件
5.4% → 6.3%

病院で取り扱う情報はどんなもの？

電子カルテの情報資産価値（＝漏洩時の被害）は非常に高い



例）カルテ流出時の想定損害賠償額計算

電子カルテ流出時の想定損害賠償額（Joモデル）＝

基礎情報価値[500] × 機微情報度[10の2乗] × 本人特定用意度[6] × 社会的責任度[2] × 事後対応評価[1]

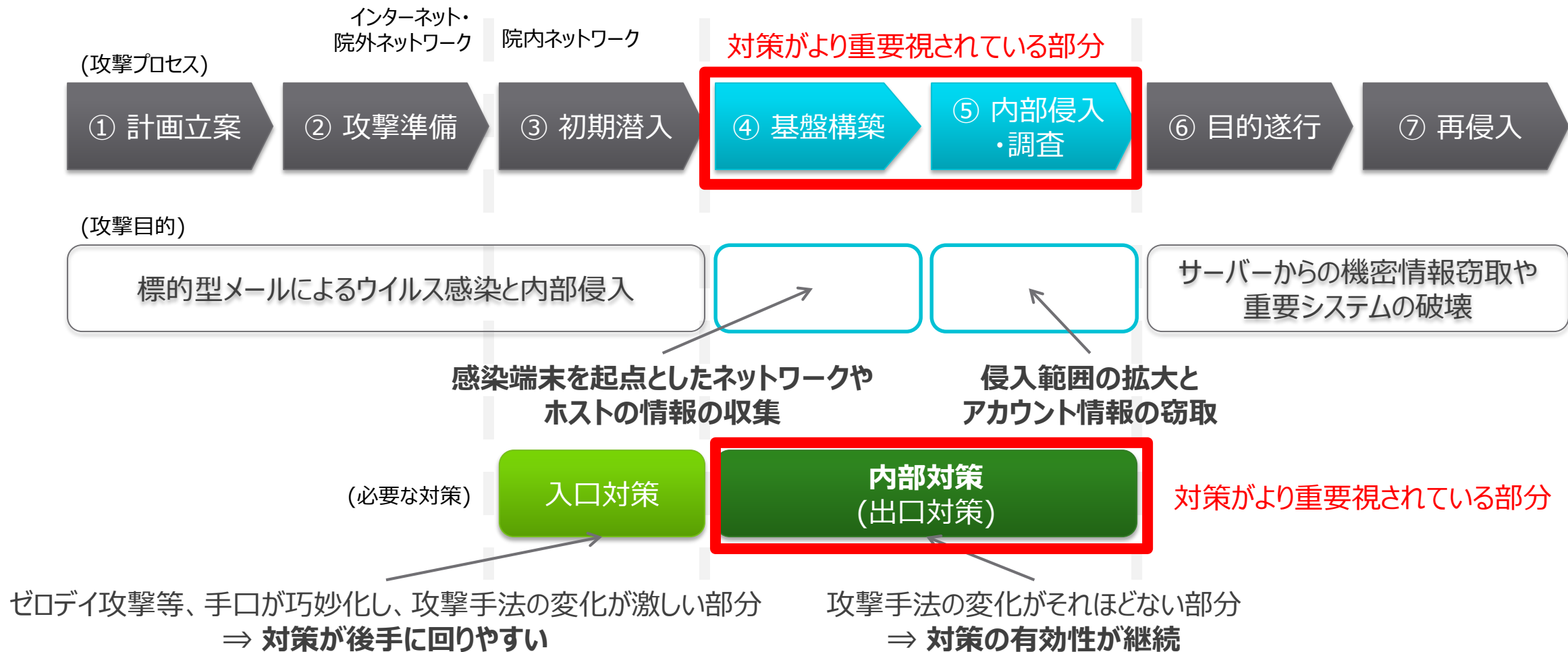
= 600,000円

出典：日本ネットワークセキュリティ協会

2018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

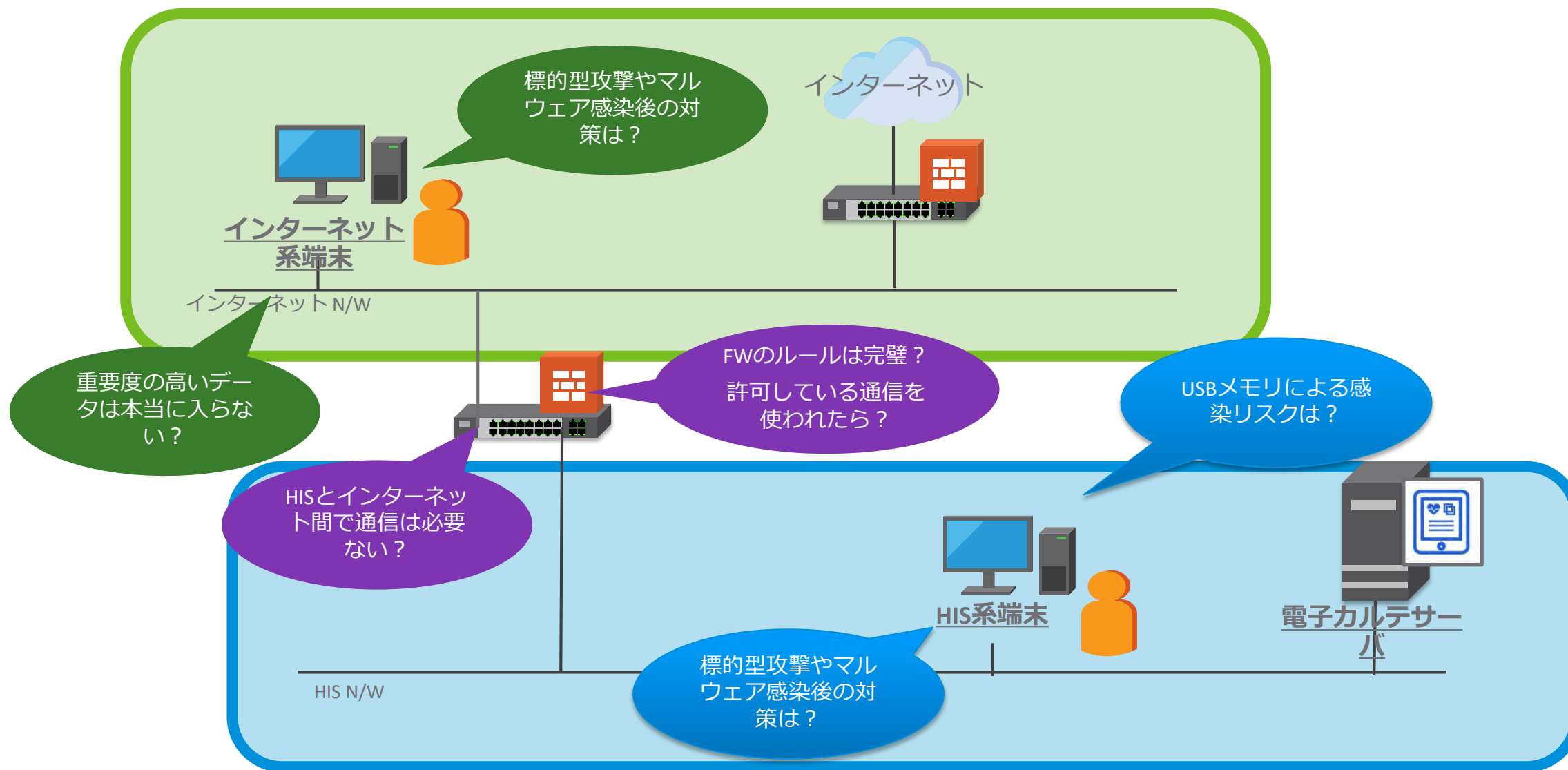
https://www.jnsa.org/result/incident/data/2017incident_survey_sokuhou_attachment_ver1.0.pdf

高度標的型攻撃のシナリオと対策



ネットワーク分割（インターネット、HIS）の課題

分割後も多くのリスクが内在



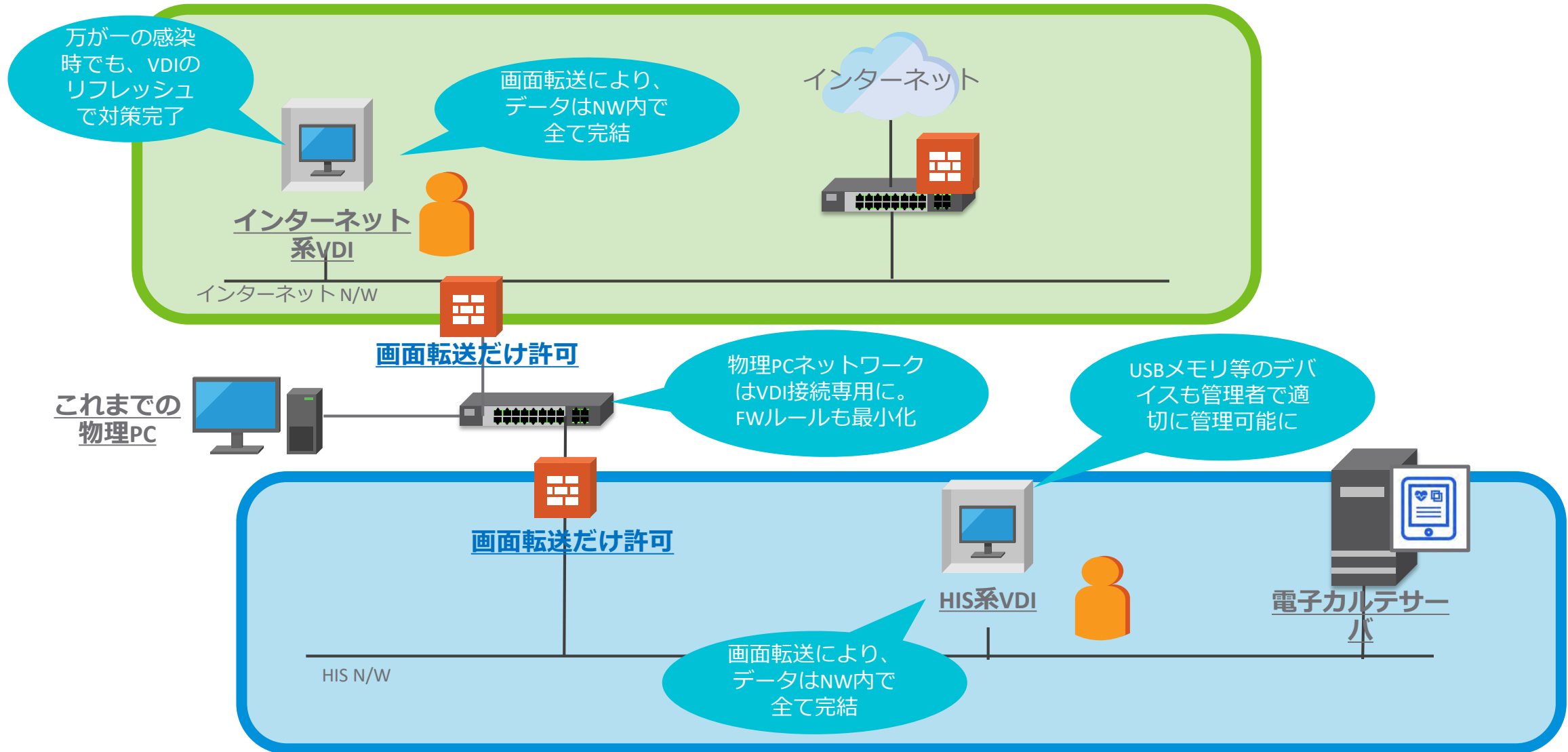
VMwareが提案するセキュリティ強化対策

仮想デスクトップによる内部対策の強化



仮想デスクトップで実現する院内セキュリティ強化

仮想デスクトップの画面転送技術による安全かつシンプルな院内セキュリティの実現

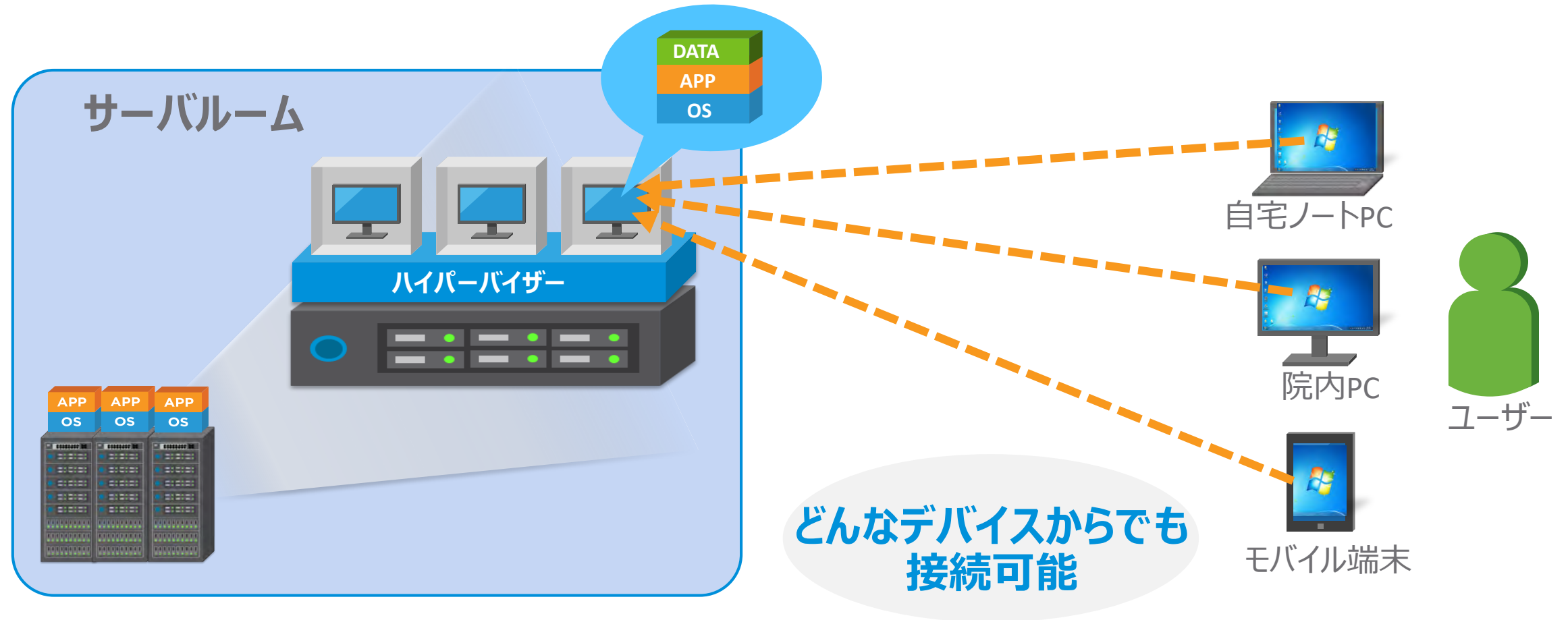


2.VMwareの仮想デスクトップ テクノロジー

VMware Horizon

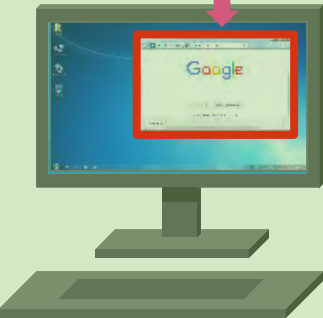
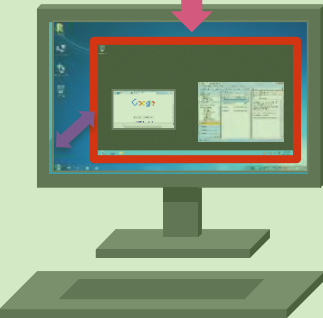
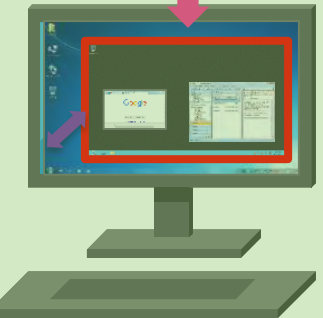
仮想デスクトップ（VDI）とは

- デバイス・場所を問わず、画面を呼び出せる
- 画面転送なので、データはローカルに残らない



VMware Horizonで提供可能な仮想デスクトップの方式

- ✓ 仮想デスクトップだけでなく、アプリケーション単位の仮想化も可能
- ✓ 業務に合わせた、仮想デスクトップの構成が選択可能

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			制限なし	
MS ライセンス	OS + RDS CAL			VDA	
	Linux OS対応			無し	

インターネット

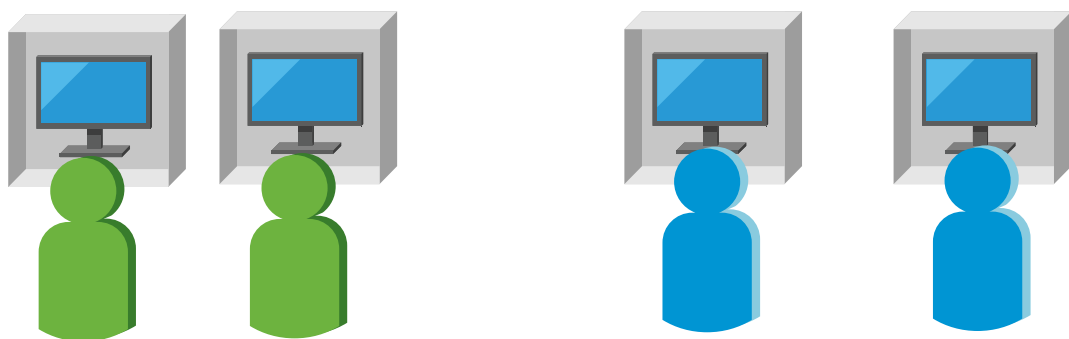
HIS

仮想デスクトップ（VDI）と仮想アプリケーション（RDSH）の違い

VDI(仮想デスクトップ)

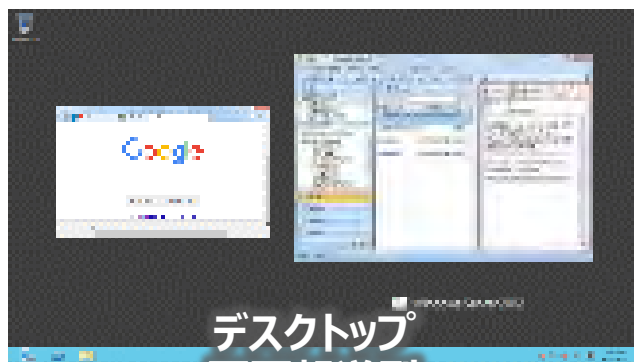
1つのVDIを1人のユーザーが利用

1台のVMを1つのリモートセッションで使用方法



Windows7/8/10
もしくは

Windows Server 2008/2012/2016



デスクトップ
画面転送型

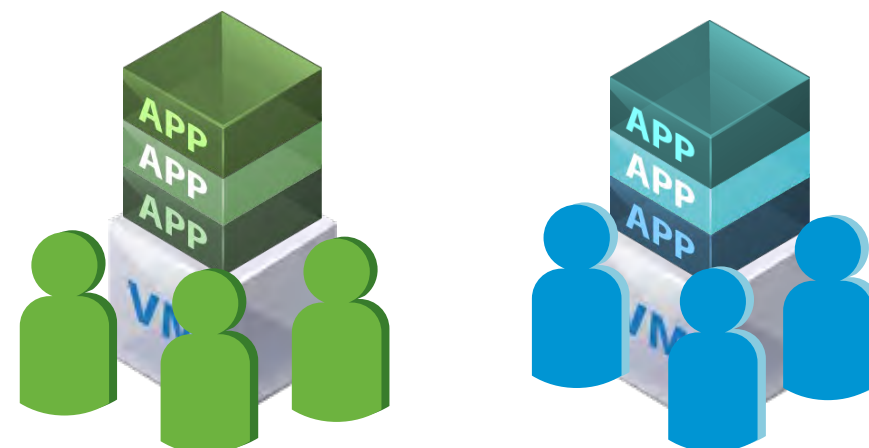
vmware®

©2019 VMware, Inc.

RDSH(仮想アプリケーション)

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方法



Windows Server 2008/2012/2016



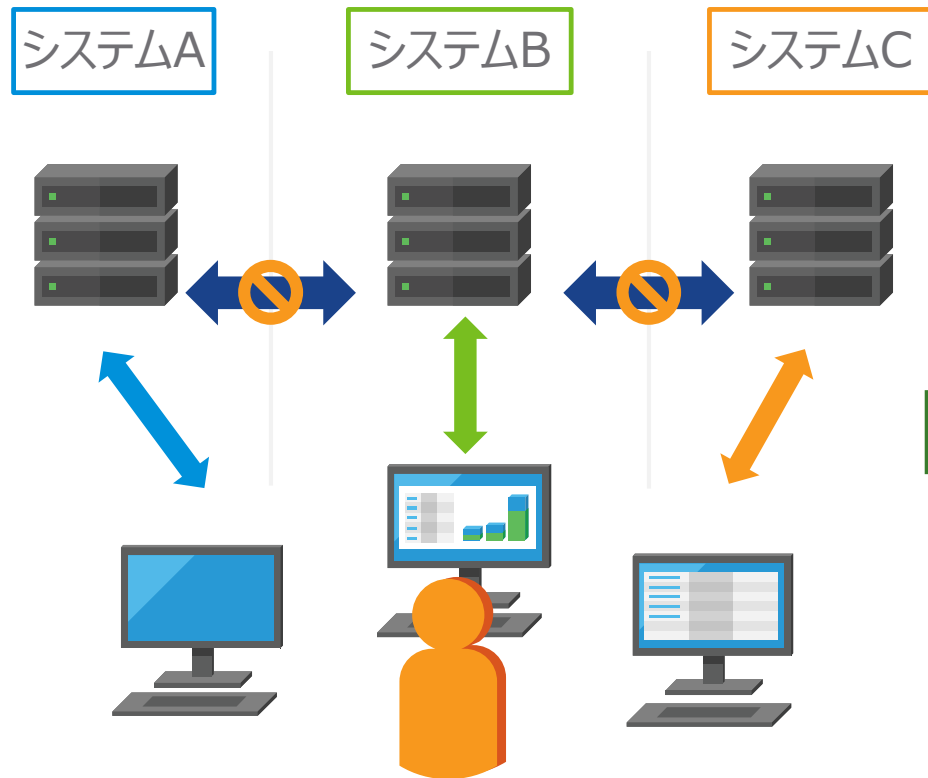
VDIのような
デスクトップの
転送も可能



アプリケーション
ウィンドウ
画面転送型

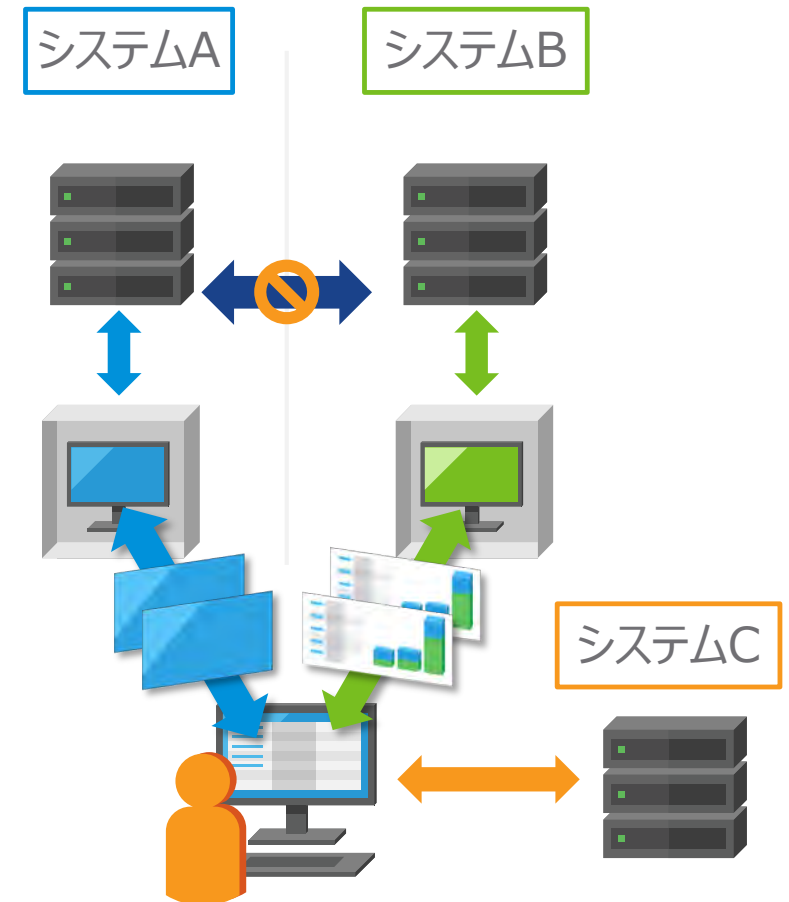
Horizonのメリット①：物理コストの削減

物理スペースや管理コストからの解放



ネットワークの数に応じて
PCを増やす必要がある

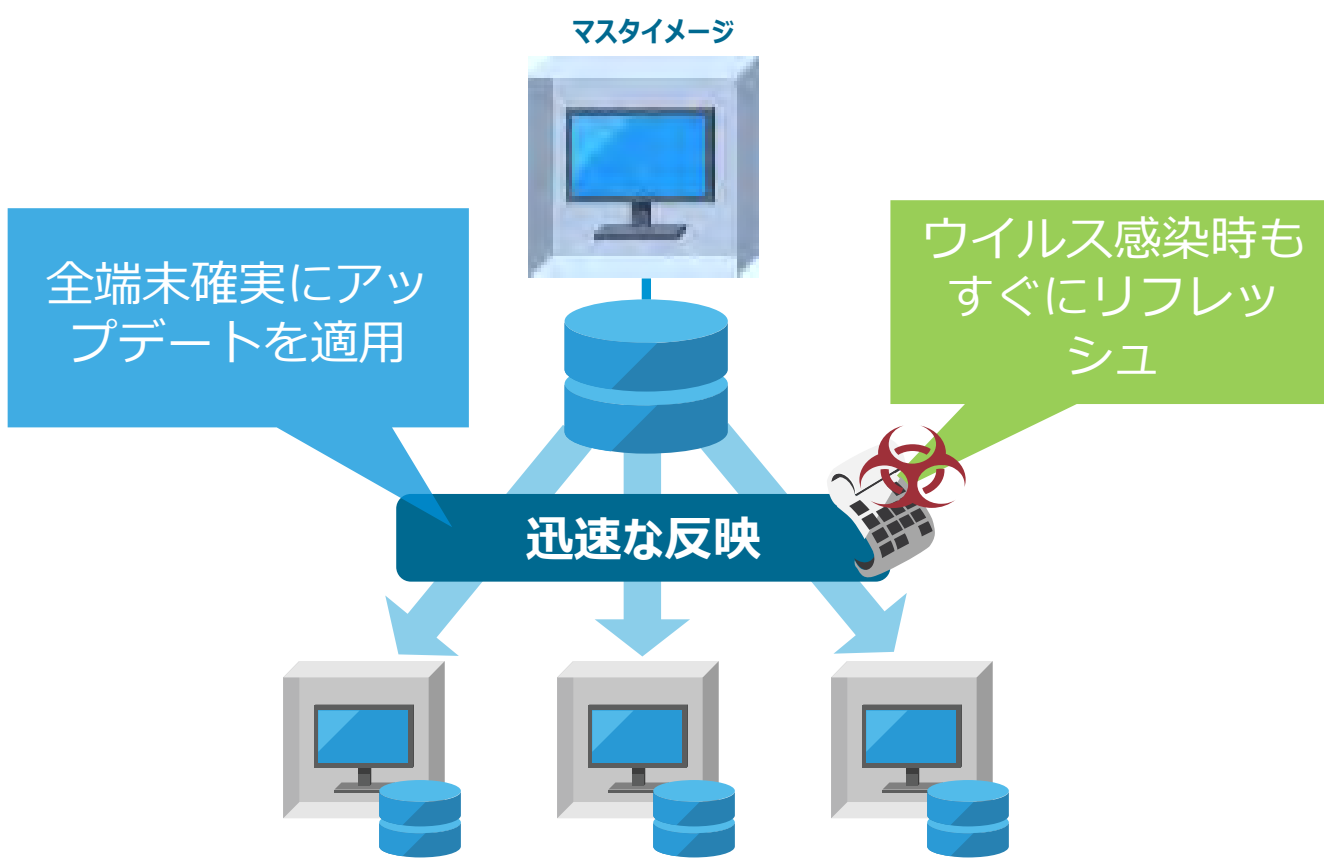
デスクトップ仮想化



ネットワークがいくつに増えても
物理端末は1台のみ

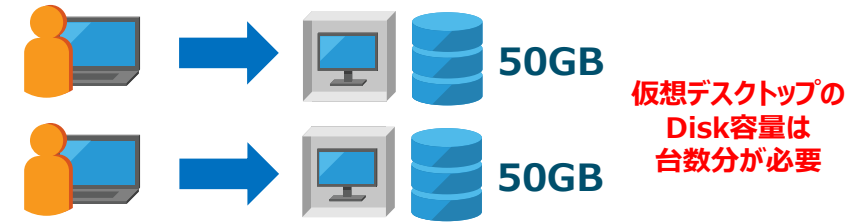
Horizonのメリット②：仮想デスクトップの管理

マスターイメージによる効率的でセキュアなデスクトップ管理

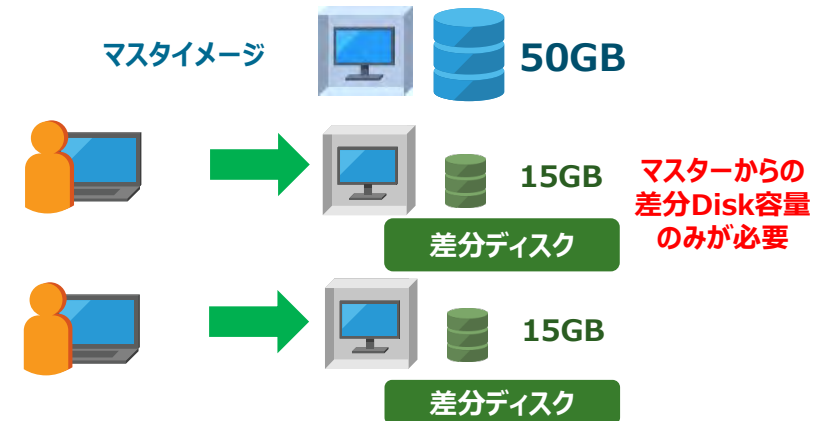


マスターの設定・アップデートを
仮想デスクトップへ迅速に反映可能

フルクローン



リンククローン・インスタントクローン



ストレージ容量の効率的な利用と
VDIの展開スピードupを実現

Horizonのメリット③ : 高品質なデスクトップ利用

VMware Blast

- モバイル環境を前提としたプロトコル設計
- ネットワークの負荷を最小限に**、最高レベルの**パフォーマンス**を提供

 **6倍**
のスピード

 **50%** の
帯域幅利用の削減



高品質を担保するテクノロジー

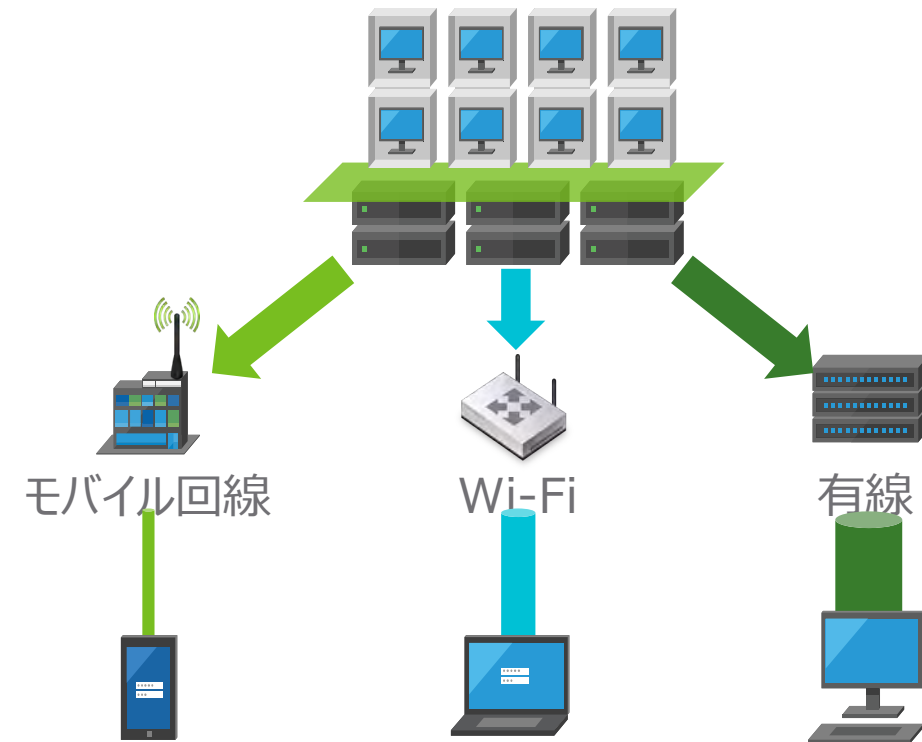
- 回線品質に応じたビットレート
- 遅延とパケットロスの最適化
- GPU対応

セキュリティを担保するテクノロジー

- データ暗号化
- クリップボードデータの制御
- 外付けデバイス制御

vmware®

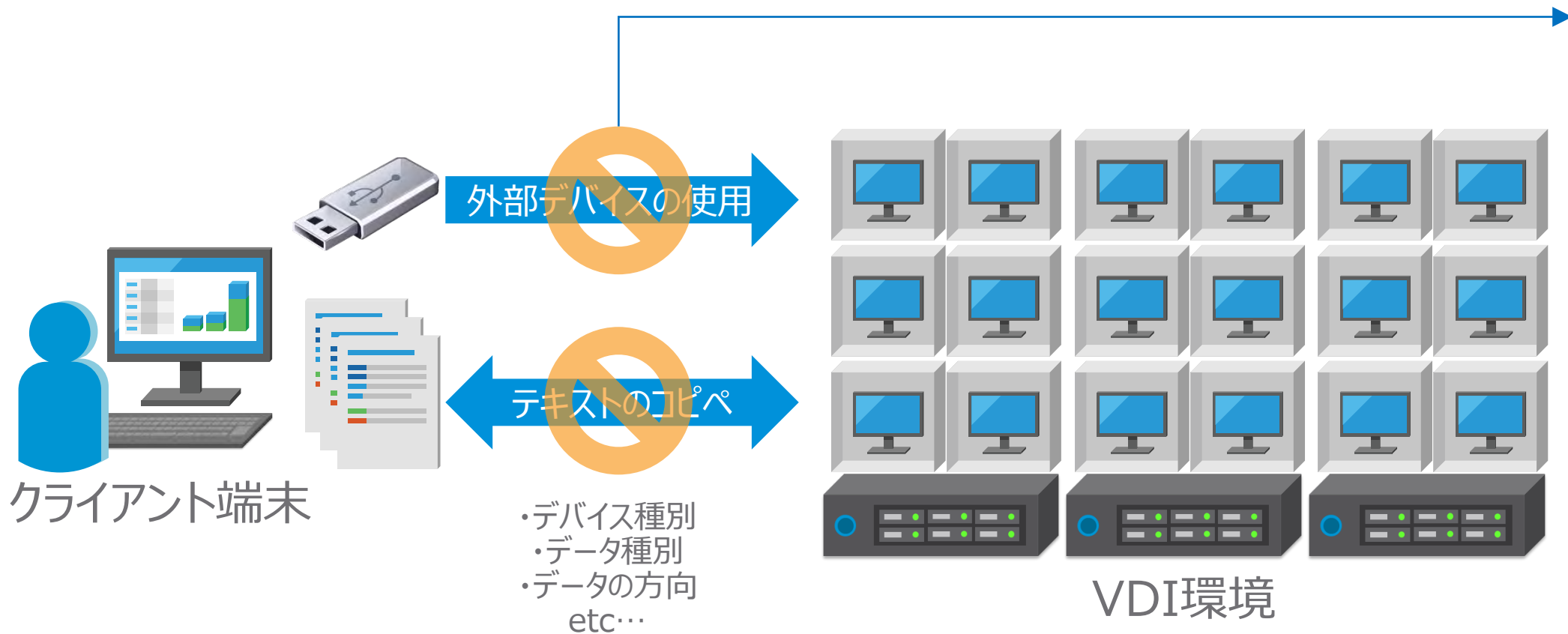
©2019 VMware, Inc.



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のメリット④：セキュアなポリシー制御

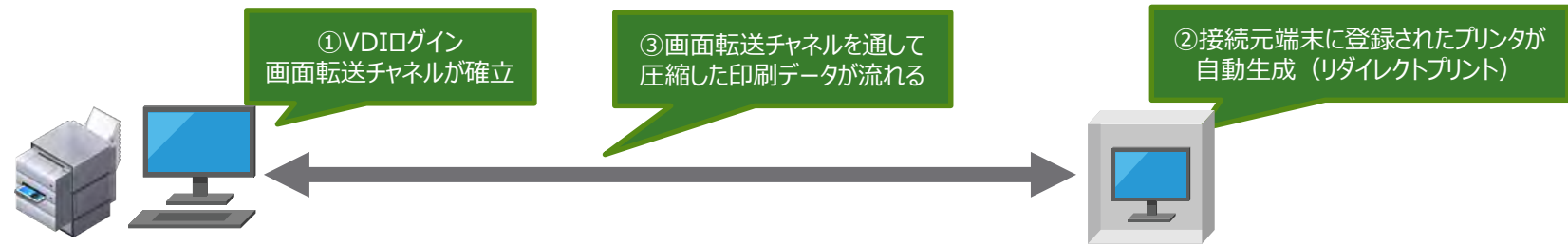
クリップボード & 外部デバイスの制御



VDIにする事で、従来より強固に外部デバイスやcopy&Pasteの制御が可能に
(資産管理ソフトからの脱却も可能に)

Horizonのメリット⑤ : 印刷の最適化

クライアントやプリンタに依存する印刷要件にも柔軟に対応可能



- ✓ 仮想プリンタ機能にて、プリンタ構成や種別に依存せず、印刷が可能に
- ✓ トラフィックを圧縮することにより、帯域消費や印刷待ち時間も削減

【印刷ジョブサイズ比較(ご参考)】

ワード文書、8ページ、ファイルサイズ1.17MB	
Virtual Printing 不使用	11.2MB
Virtual Printing 使用	0.74MB
パワーポイント、53ページ、ファイルサイズ1.67MB	
Virtual Printing 不使用	218MB
Virtual Printing 使用	2.21MB

印刷機能	利点	考慮点
仮想プリンタ機能 (Virtual Printing)	- 雛形VMにView Agentをインストールする際、オプション選択で"仮想印刷"を選択するだけで利用可能 - 接続元端末が認識しているプリンタを使用可能 - 接続元端末で設定している"通常使うプリンタ"の設定が反映 - トラフィックの圧縮	- プリンタドライバをインストールできない端末(ゼロクライアントなど)では利用できない - 汎用プリンタドライバを利用するため、複合機など機種毎の機能を利用できない
ThinPrint or VMware Native driver		
ロケーションベース印刷	IPアドレス範囲、マシン名、MACアドレス、接続ユーザ毎に表示するプリンタの制限および"通常使うプリンタ"の設定が可能	- Master VMにプリンタドライバをインストールする必要がある(変更や機器交換時に運用工数が発生する) - ローカルプリンタ、SMBプリンタ共有、LPRプリンタ、IPPプリンタは利用できない

ネットワークプリンタをVDIから参照させることで、これまでと同様のプリンタ環境を実現することも可能

3. ネットワーク仮想化との連携 による更なるセキュリティ強化

VMware NSX

内部対策（感染拡大防止）の必要性

ランサムウェアなど、横の感染拡大による脅威の増加

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

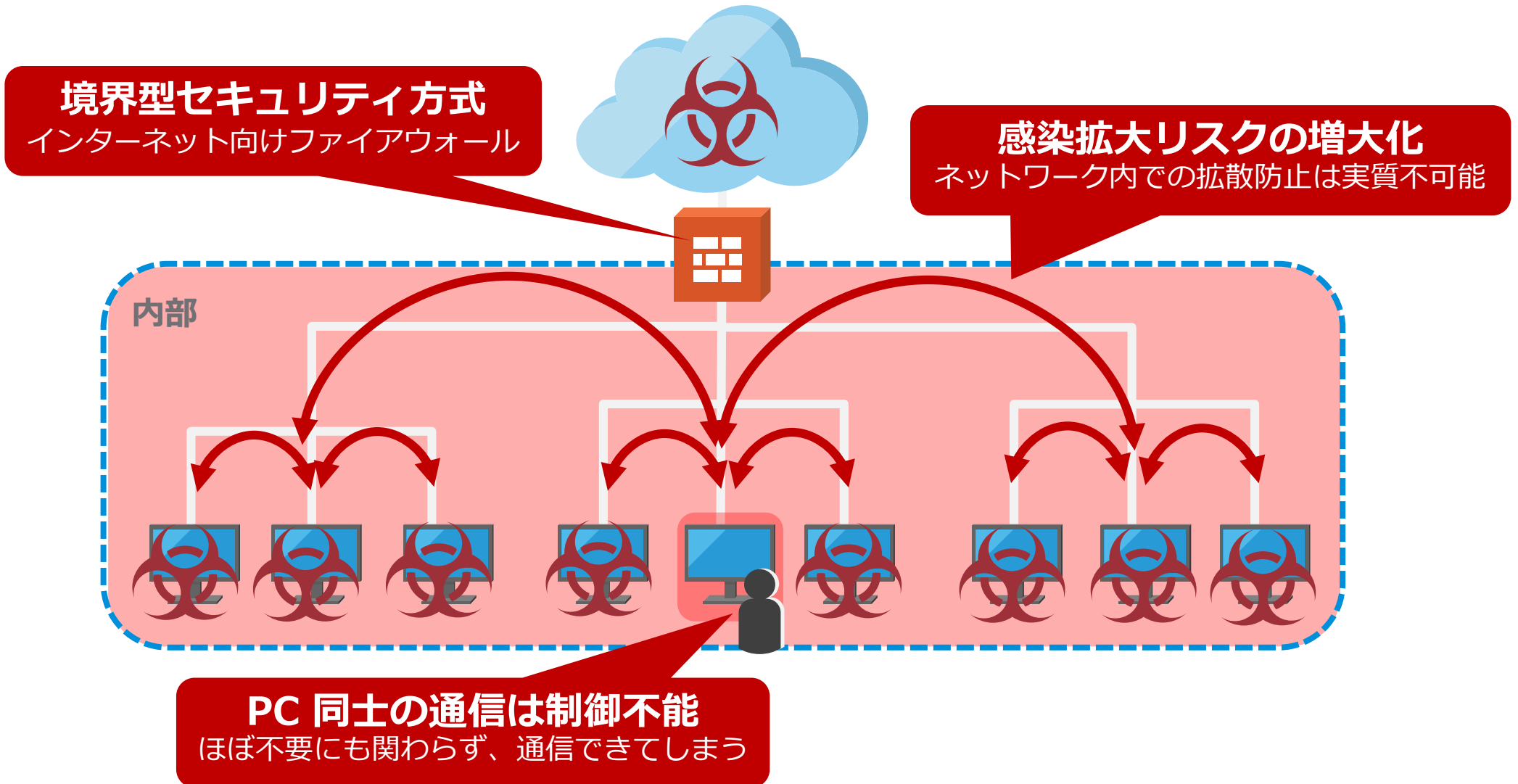
(3) サイバー攻撃を受けた際の非常時の対応

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）

ネットワーク分割の限界

ネットワーク内（横の感染）については無防備な状態



VMware NSX（ネットワーク仮想化）と連携した内部対策強化

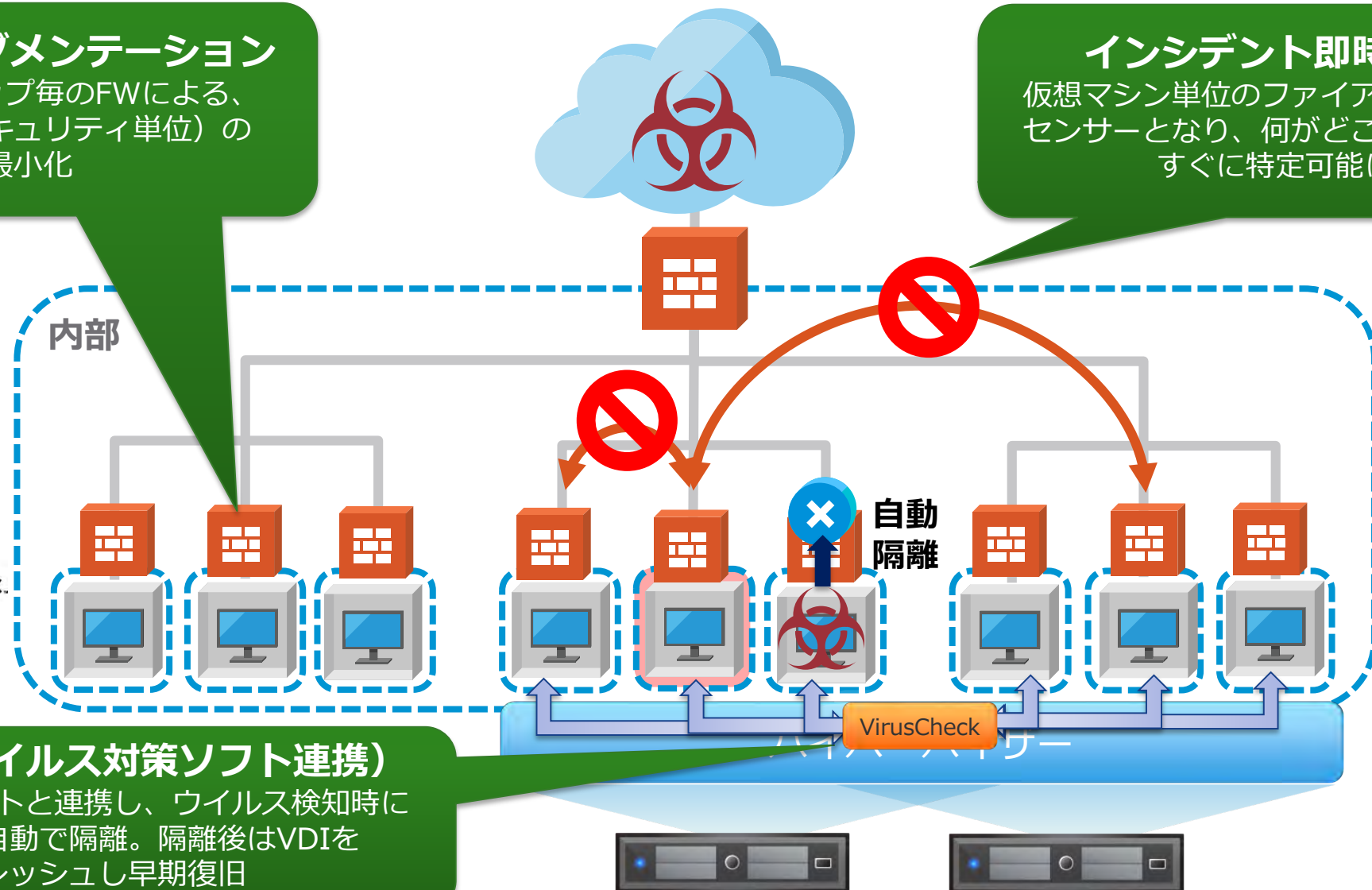
仮想マシン単位のファイアウォールによる横の感染拡大を防止

マイクロセグメンテーション

仮想デスクトップ毎のFWによる、
影響範囲（セキュリティ単位）の
最小化

インシデント即時特定

仮想マシン単位のファイアウォールが
センサーとなり、何がどこで起きたか
すぐに特定可能に



自動隔離（ウイルス対策ソフト連携）

ウイルス対策ソフトと連携し、ウイルス検知時に
対象のVDIを自動で隔離。隔離後はVDIを
リフレッシュし早期復旧



4. 事例紹介

ヴィエムウェア導入実績

事例公開をいただいているお客様含め、ご紹介可能な一部のお客様を抜粋してご紹介いたします。
多くのお客様はサーバ仮想化とクライアント仮想化を同時に実施しております。

サーバ仮想化 VMware vSphere

医療機関名	病床数	電子カルテベンダー	仮想化範囲
青森県立中央病院	684	NEC/MegaOakHR	部門統合
A病院様	466	SSI/e-カルテ	電子カルテ/部門統合
B病院様	989	富士通/EGMAIN-EX IBM/CIS+	部門統合
C病院様	615	IBM/CIS	部門統合
D病院様	679	富士通/IIMS	電子カルテ/部門統合
済生会中津病院	748	NEC/MegaOakHR	電子カルテ/部門統合
E病院様	520	富士通/LifeMark-HX	電子カルテ/部門統合
名古屋市立大学病院	808	富士通/個別開発	電子カルテ/部門統合
名古屋第二赤十字病院	812	富士通/EGMAIN-GX	電子カルテ/部門統合
福井県済生会病院	460	NEC/MegaOakHR	部門統合
F病院	600	日本IBM/CIS	部門統合
万成病院	500	CSI/MI・RA・Is	部門統合
G病院	413	SSI/e-カルテ	電子カルテ/部門統合

クライアント仮想化 VMware Horizon

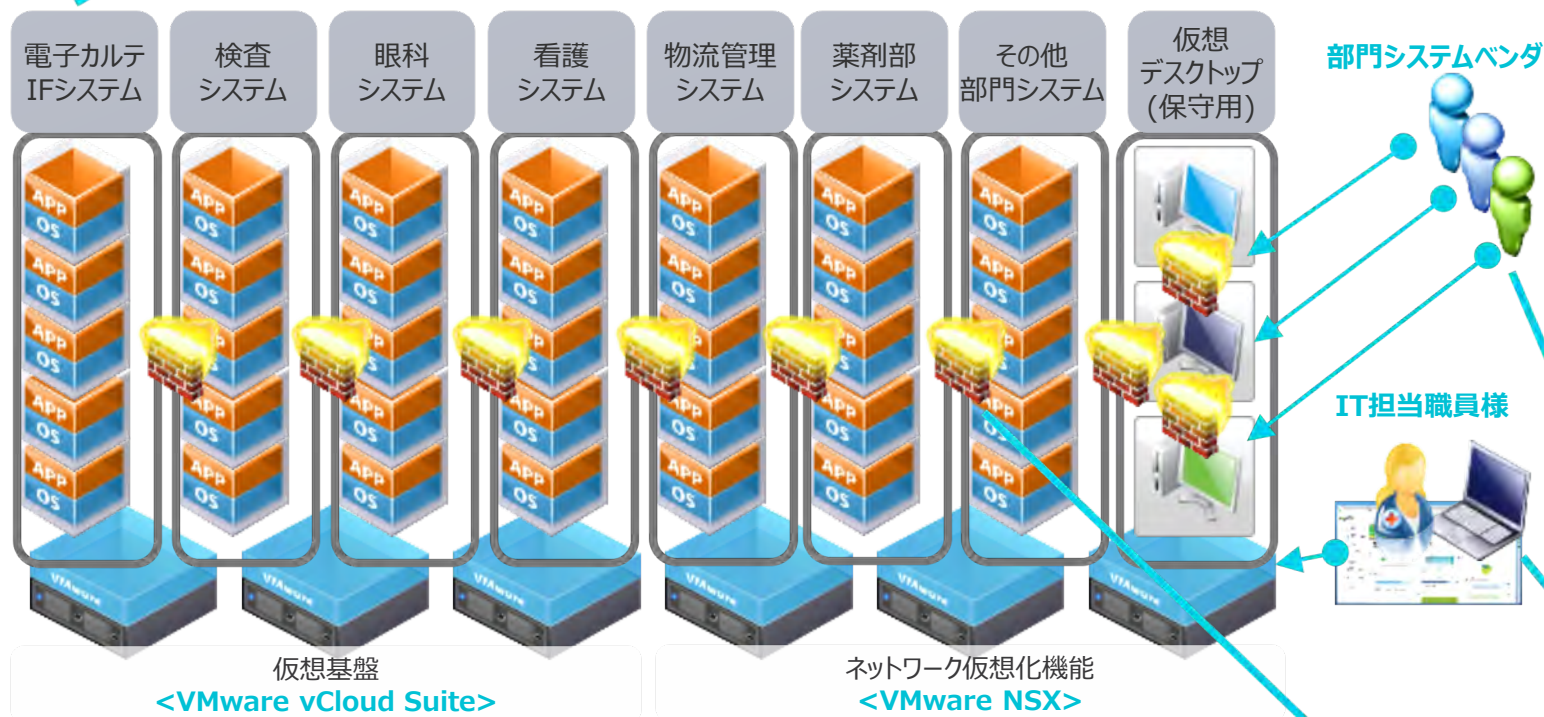
医療機関	病床数	電子カルテベンダー	概要
H病院	-	富士通/LifeMark-HX	グループ内の病院に対する電子カルテ用端末のクラウド利用
青森県立中央病院	684	NEC/MegaOakHR	電子カルテ用端末利用、タブレットを利用した業務効率化
I病院	609	富士通/EGMAIN-GX	電子カルテ用端末利用
J病院	701	富士通/LifeMark-HX	電子カルテ端末利用
B病院	989	IBM/CIS+	電子カルテ端末利用(検証中)
済生会中津病院	712	NEC/MegaOakHR	院外アクセス/部門ベンダ用
D病院	679	富士通/IIMS	電子カルテ用端末利用
E病院	520	富士通/LifeMark-HX	電子カルテ用端末利用
K病院	1163	富士通/EGMAIN-GX	電子カルテ端末利用/インターネット接続利用
名古屋市立大学病院	808	富士通/EGMAIN-GX	電子カルテ用端末利用(既存PC利活用、ゼロクライアント)
名古屋第二赤十字病院	812	富士通/EGMAIN-GX	電子カルテ用端末利用/インターネット接続利用
福井県済生会病院	460	NEC/MegaOakHR	電子カルテ用端末利用
万成病院	500	レスコ/Alha	電子カルテ用端末利用
L病院	327	CSI/MI・RA・Is	電子カルテ用端末利用

病院導入事例 -福井県済生会病院様-

VMware Horizon + NSX

コスト削減と可用性を高めた仮想基盤に部門サーバを集約

検体検査システム、調剤システム、DICOM画像管理システム、診断書作成支援システムなど約60のシステムを仮想化により集約(約120仮想マシン)し、可用性向上とコスト削減を実現



vCloud Suiteと医療機関で初となるNSXを採用し
安定的な医療サービス提供のための統合インフラ基盤を実現



©2019 VMware, Inc.

「患者さんの立場で考える」という理念のもと、私達は日々取り組んでいます。患者さんへの医療サービスの向上と、患者さんのデータを大切に扱うことを考えると、IT設備への投資を抑えつつ、よりセキュリティの高い医療基盤を構築することが重要でした。

今回の基盤は、これらを満たしつつ、よりすばらしいものになったと感じています。

福井県済生会病院
医療情報課 課長

塗茂 裕一氏



安全なリモートメンテナンス環境

部門システムベンダが外部から安全にシステム保守を実施できる
デスクトップ環境を仮想マシンとして実現

セキュアなデスクトップアクセス環境
<VMware Horizon View>

“安定稼働”の見える化

仮想基盤上の部門システムの性能、リソース需要予測などを実現

仮想基盤の性能監視/キャパシティ管理機能
<VMware vRealize Operations Manager>

セキュリティ向上を目的とした
ネットワーク仮想化機能によるファイアウォール
各システム、各仮想マシンの隔離性を担保する
ファイアウォール機能を提供



Thank You