Future
Technology Days

Windows 7 と Windows Server 2008 R2 で実現する New Feature の数々

マイクロソフト株式会社
サーバープラットフォームビジネス本部
プロダクトマネージャ
田中 啓之

Windows 7 と Windows Server 2008 R2 で実現するNew Feature

Windows 7 と Windows Server 2008 R2の関係

それぞれ単独 OS としての機能強化も多くなされている
あくまでもWindows 7とWindows Server 2008 R2 で実現できる新しい機能の一部

Window 7 と Windows Server 2008 R2で実現する New Featureの数々

DirectAccess - シームレスで安全な社内リソースへのアクセス

BranchCache – ブランチシナリオでのファイルアクセスの向上

Remote Desktop Services – 統合されたRDとVDI

Bit Locker の強化 – 外部デバイスへの対応

Window 7 と Windows Server 2008 R2で実現する New Featureの数々

APP Locker – 不適切なアプリケーションの利用を抑制

DNS SEC – DNSサーバーのセキュリティ強化

DFS-R – 読み取り専用の分散ファイルシステムによるセキュリティ強化

DirectAccess (ダイレクトアクセス)

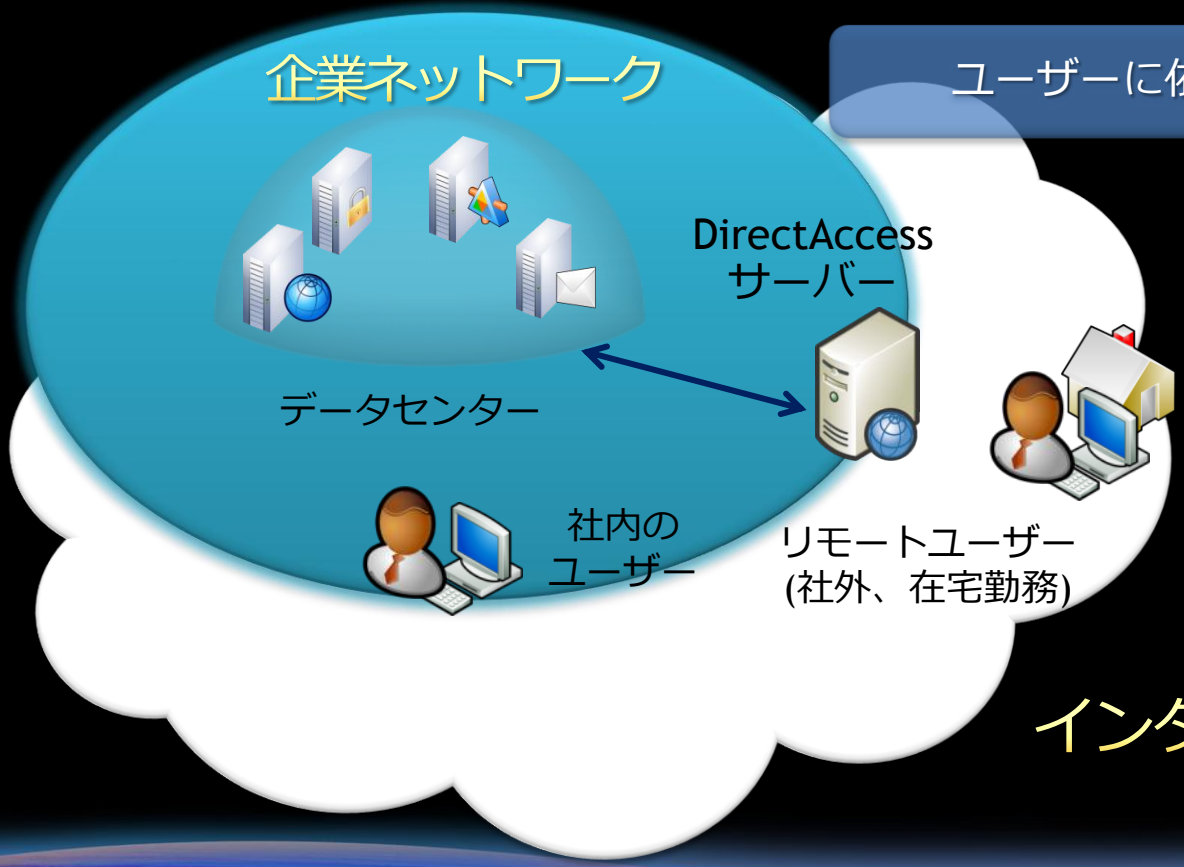
シームレスで安全な社内リソースへのアクセス

求められる新たなニーズ

次世代のワークスタイルへの対応

企業ネットワークに存在しないPCの管理

ユーザーに依存したアクセス制御



ダイレクトアクセス

- いつでも安全に企業ネットワークにアクセス
  - ネットワーク共有
  - イントラネット Web サイト
  - 業務アプリケーション

ダイレクトアクセスの利点

いつでも利用可能

- インターネット接続 = 企業ネットワーク接続
- 自動接続（ユーザーは意識しない）
- ネットワーク状況の変化にも柔軟に対応

より安全に

- 既定で暗号化
- ポリシーベースでのアクセス制御
- スマートカードへの対応

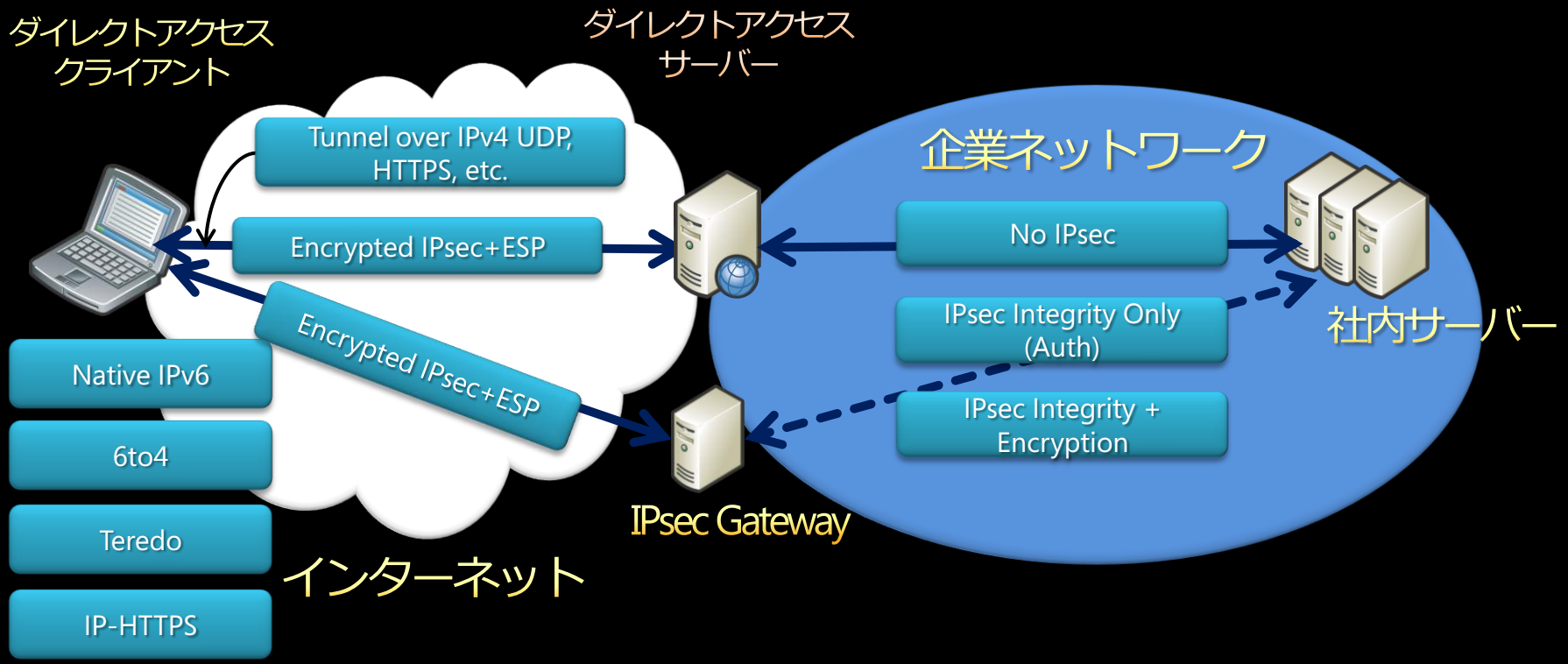
管理性が高い

- ウィザードベースでのインストール ポリシーの設定
- リモート PC からの管理

低コスト

- 簡略化されたポリシー管理
- ユーザー負荷の低減
- 専用のアプリケーションゲートウェイが不要

ダイレクトアクセステクノロジ概要



ダイレクトアクセスを利用するにはクライアントがWindows 7 (ドメイン参加済)
ダイレクトアクセスサーバーがWindows Server 2008 R2であることが条件

Demo

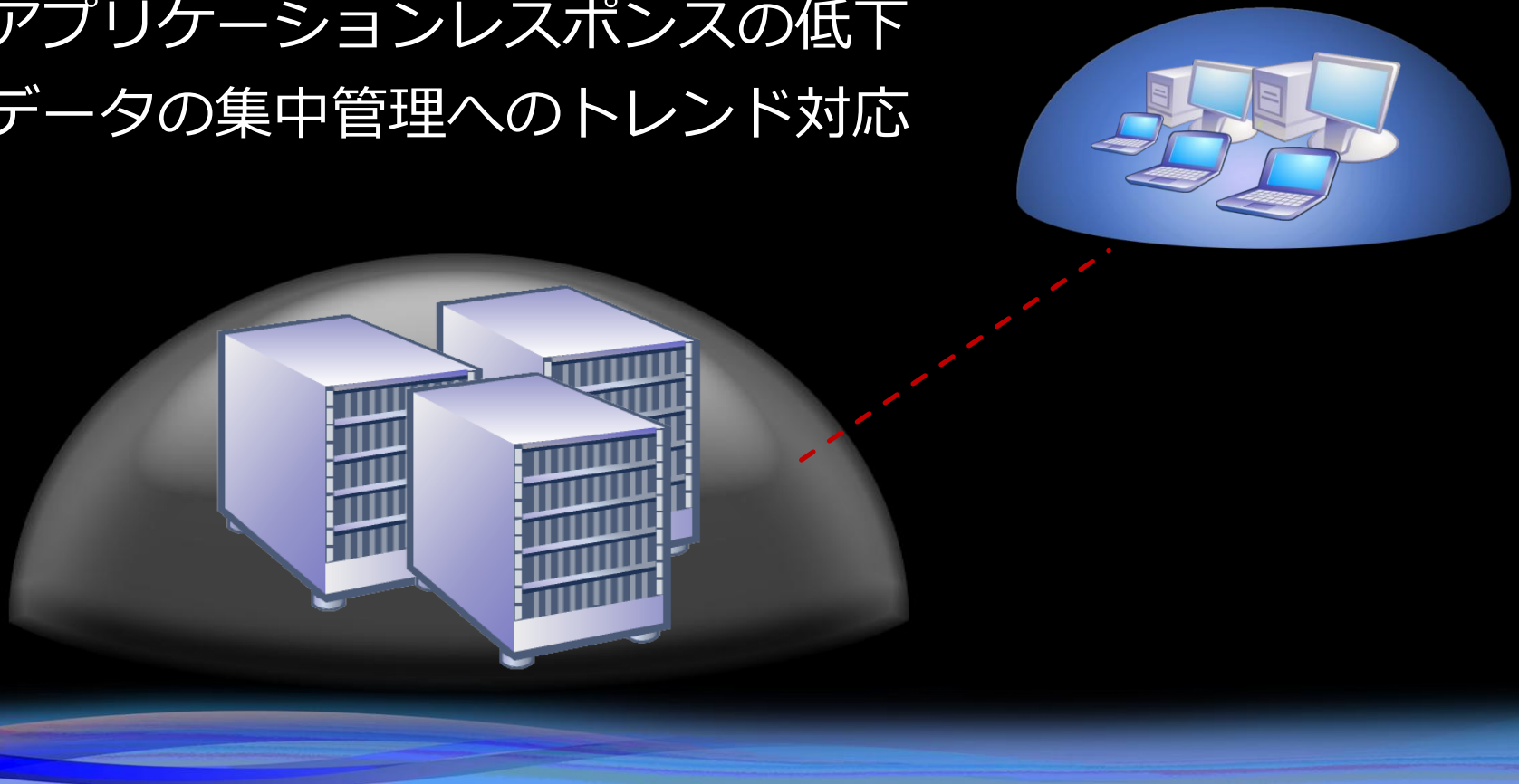
DirectAccess

BranchCache

ブランチシナリオでのファイルアクセスの向上

ブランチオフィスを抱える企業の現状

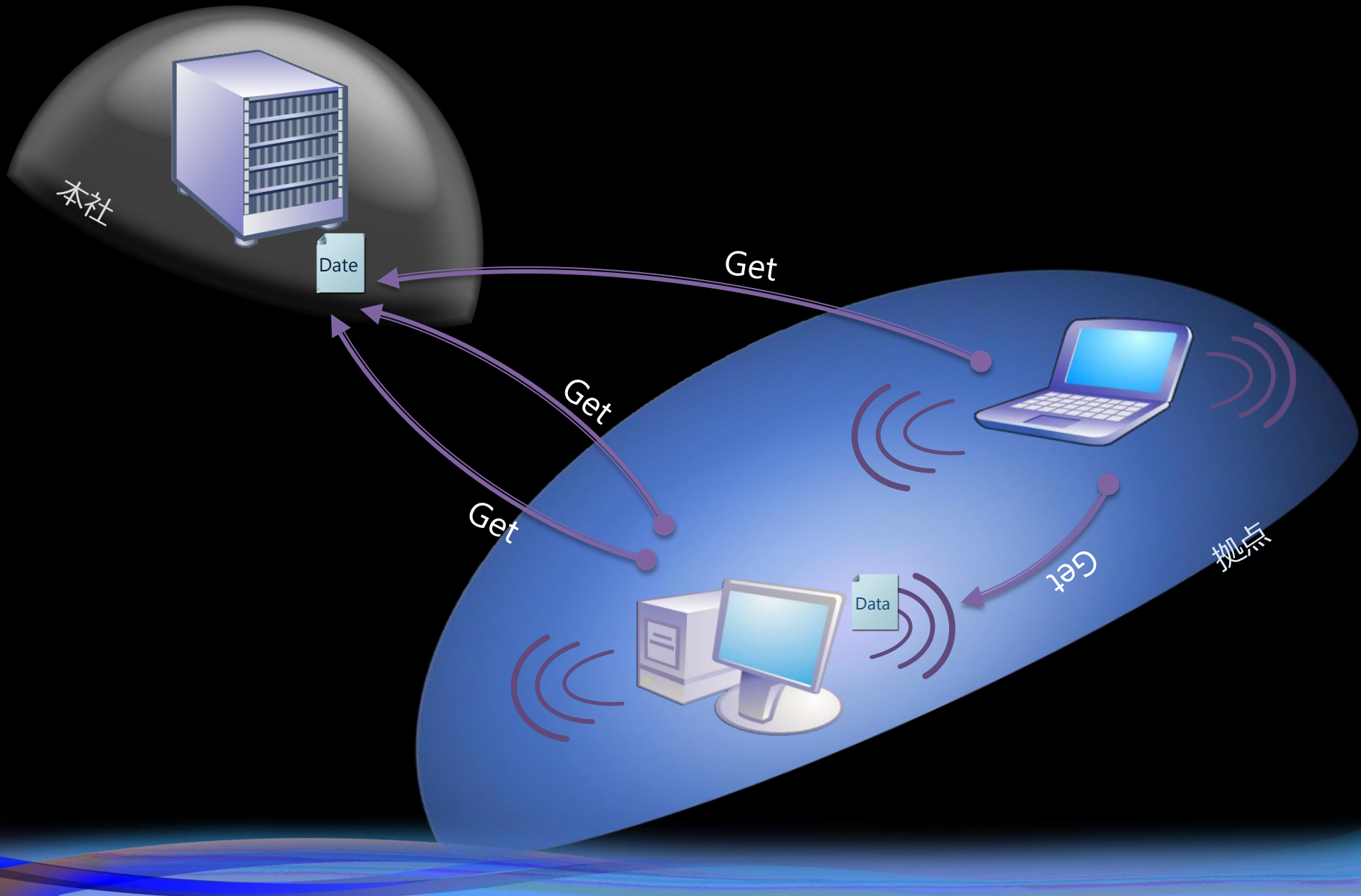
- 本社(データセンター)⇔拠点間のWAN
  - 通信帯域が小さい
  - 回線コストが高い
- WAN回線の圧迫
- アプリケーションレスポンスの低下
- データの集中管理へのトレンド対応



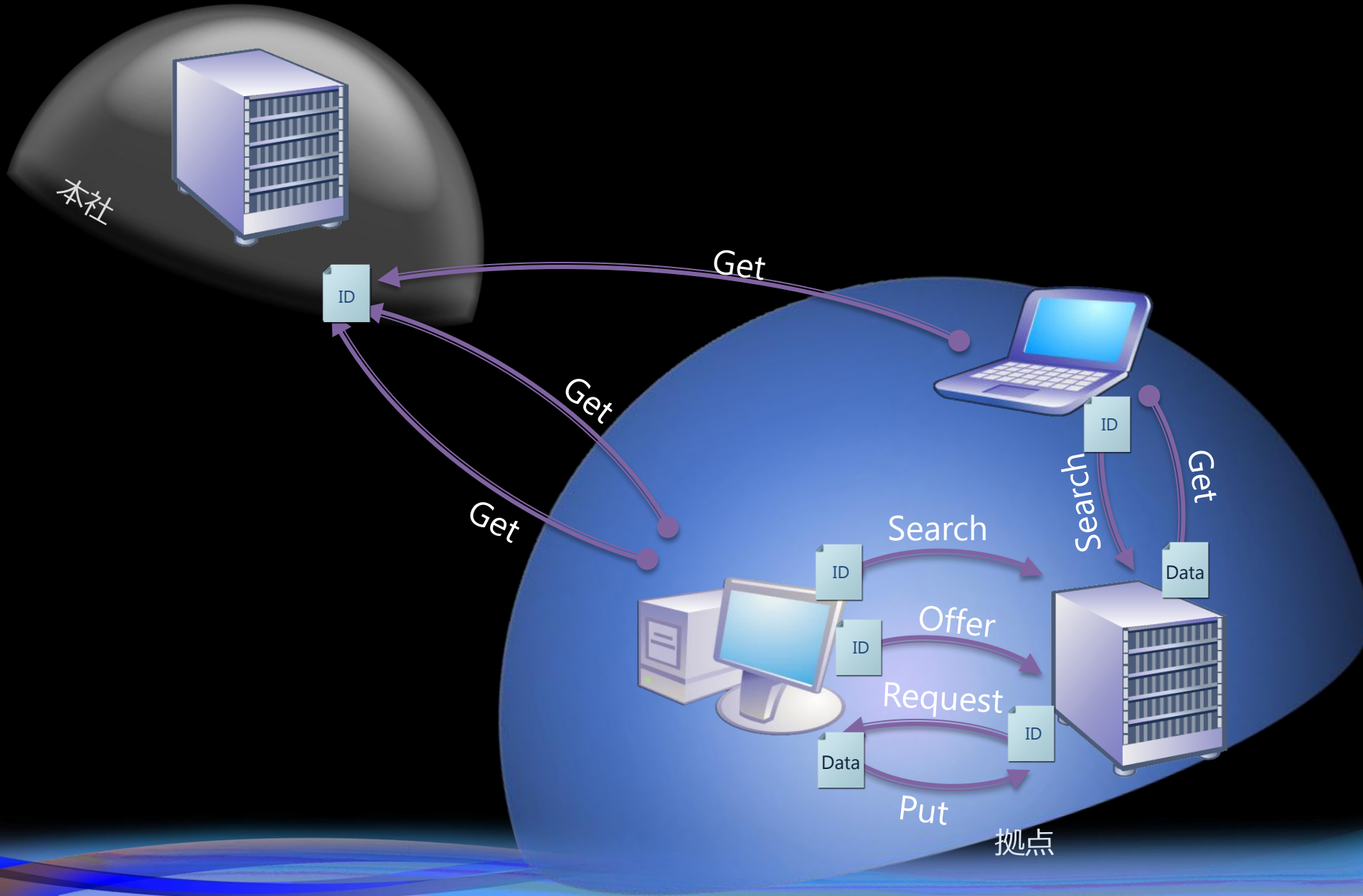
BranchCache 概要

- 拠点のユーザーも本社オフィスと同様のパフォーマンスを体感
- サーバーによって認証された場合のみキャッシュの利用が可能
- HTTP, HTTPS, SMB, BITSで利用可能
- 拠点の大きさごとに最適な動作モードを選択可能
  - Hosted Cache Mode (要 2008 R2)
  - Distributed Cache (要 Windows 7)

Distributed Cache



Hosted Cache



Hosted cache vs Distributed

Distributed Cache
クライアントにキャッシュ

- 拠点に全くインフラを用意する必要がない
- クライアントのグループポリシーを有効にするだけですぐに利用可能
- キャッシュされた内容はクライアントをオフラインにするだけで削除される

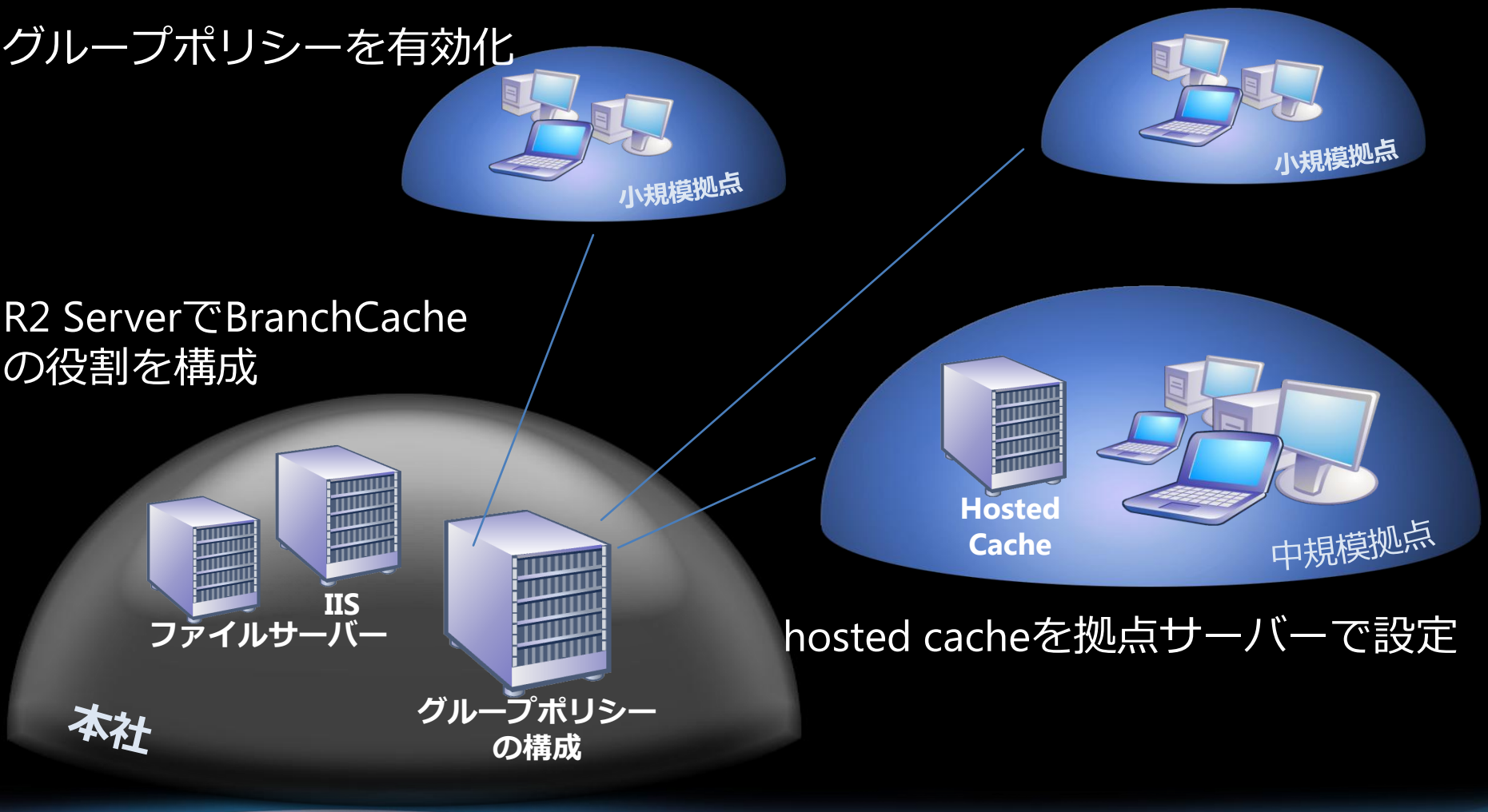
Hosted Cache
拠点のサーバーにキャッシュ

- 中規模以上の拠点に対して推奨される構成
- 集中管理されたキャッシュ:拠点にすでに存在するサーバーでキャッシュの集中管理が可能
- キャッシュに対する高い可用性
- 支店全体のキャッシュをカバー

BranchCache の構成

グループポリシーを有効化

R2 ServerでBranchCache
の役割を構成



hosted cacheを拠点サーバーで設定

Demo

BranchCache

Remote Desktop Services

統合されたRDとVDI

Remote Desktop Services

統合されたTSとVDI

- Hyper-Vによる仮想デスクトップのサポート
- 単一の管理インフラストラクチャ
- SCVMM による統合とサポート

RemoteAPP & リモートデスクトップ

- RemoteApp & Desktop コネクション(管理ツール)
- RemoteApp & Desktop & Web Access
- RD Gateway セキュリティの向上

ユーザーエクスペリエンスの強化

- マルチモニタサポートの強化
- マルチメディアサポート & オーディオリダイレクト
- 2D and 3D DirectXのリダイレクト

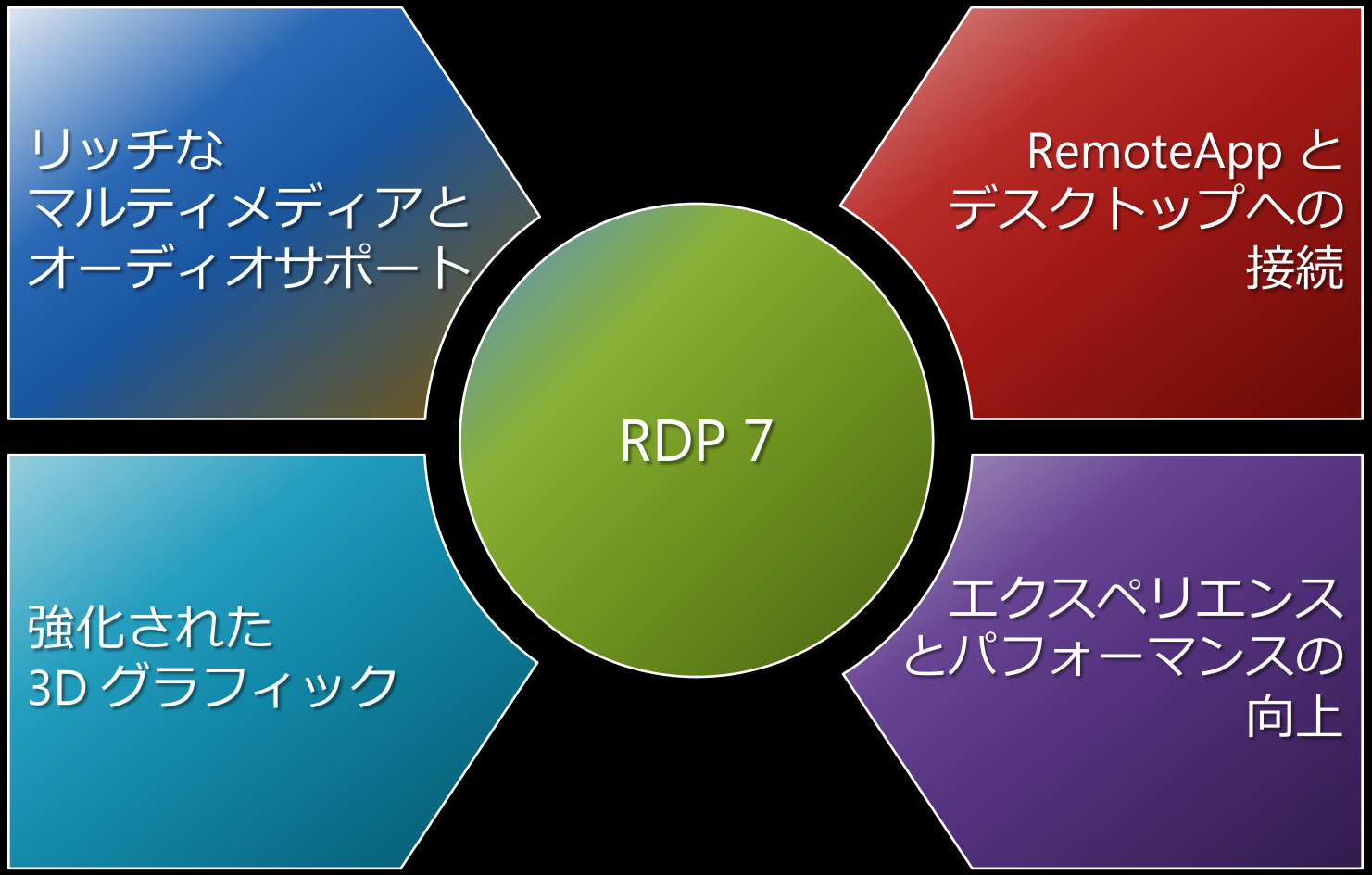
プラットフォームの強化

New API, 拡張されたコネクションブローカー, ダイナミックなCPUの割り当て, IPアドレスの仮想化, Best Practices Analyzer, Full MSI support

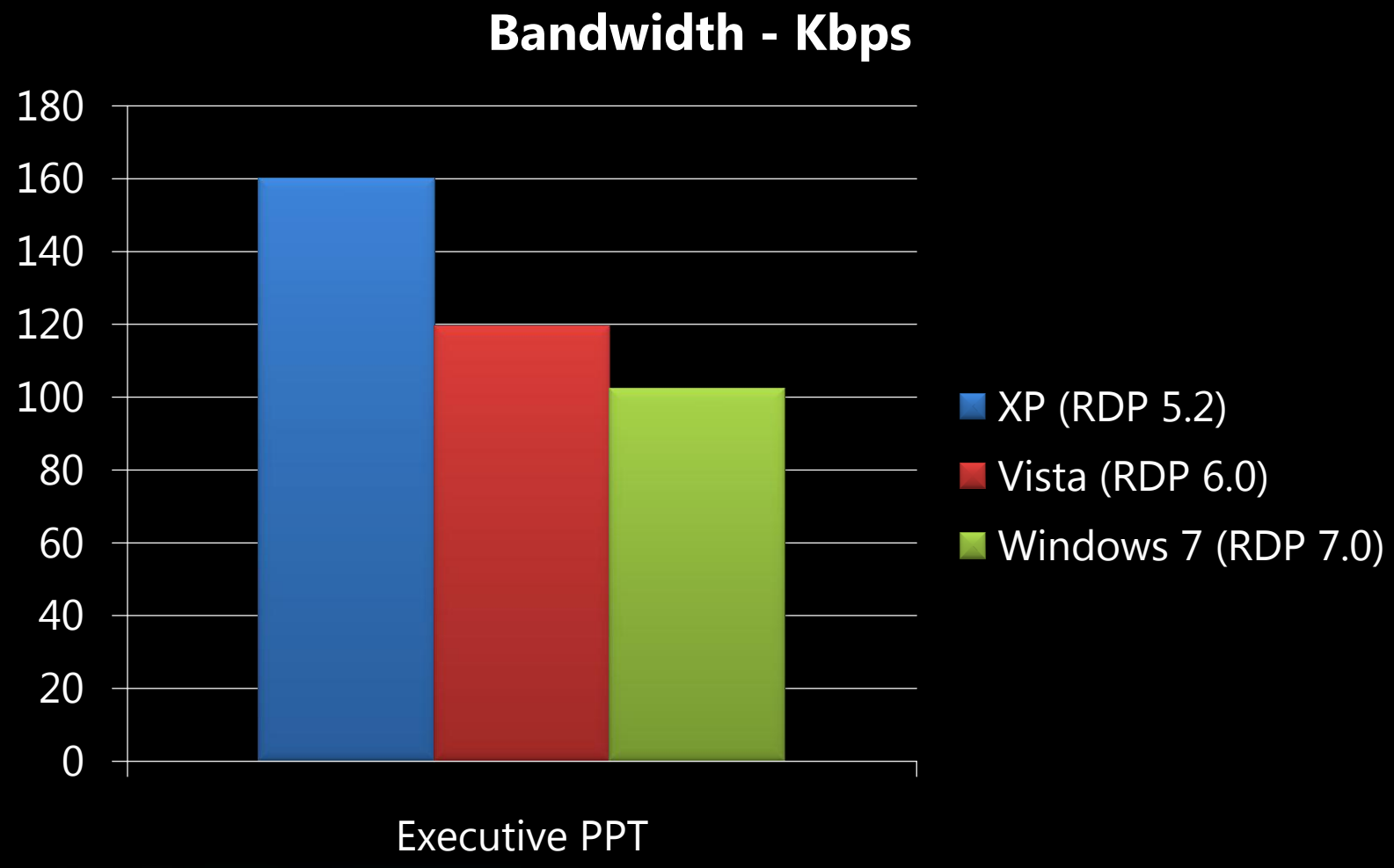
R2での名称変更

Windows Server 2008 Terminal Services	Windows Server 2008 Remote Desktop Services
TS RemoteApp™	RemoteApp™
TS Gateway	RD Gateway
TS Session Broker	RD Connection Broker
TS Web Access	RemoteApp and Desktop Web Access / Connections
TS Easy Print	RD Easy Print

RDP 7の強化ポイント

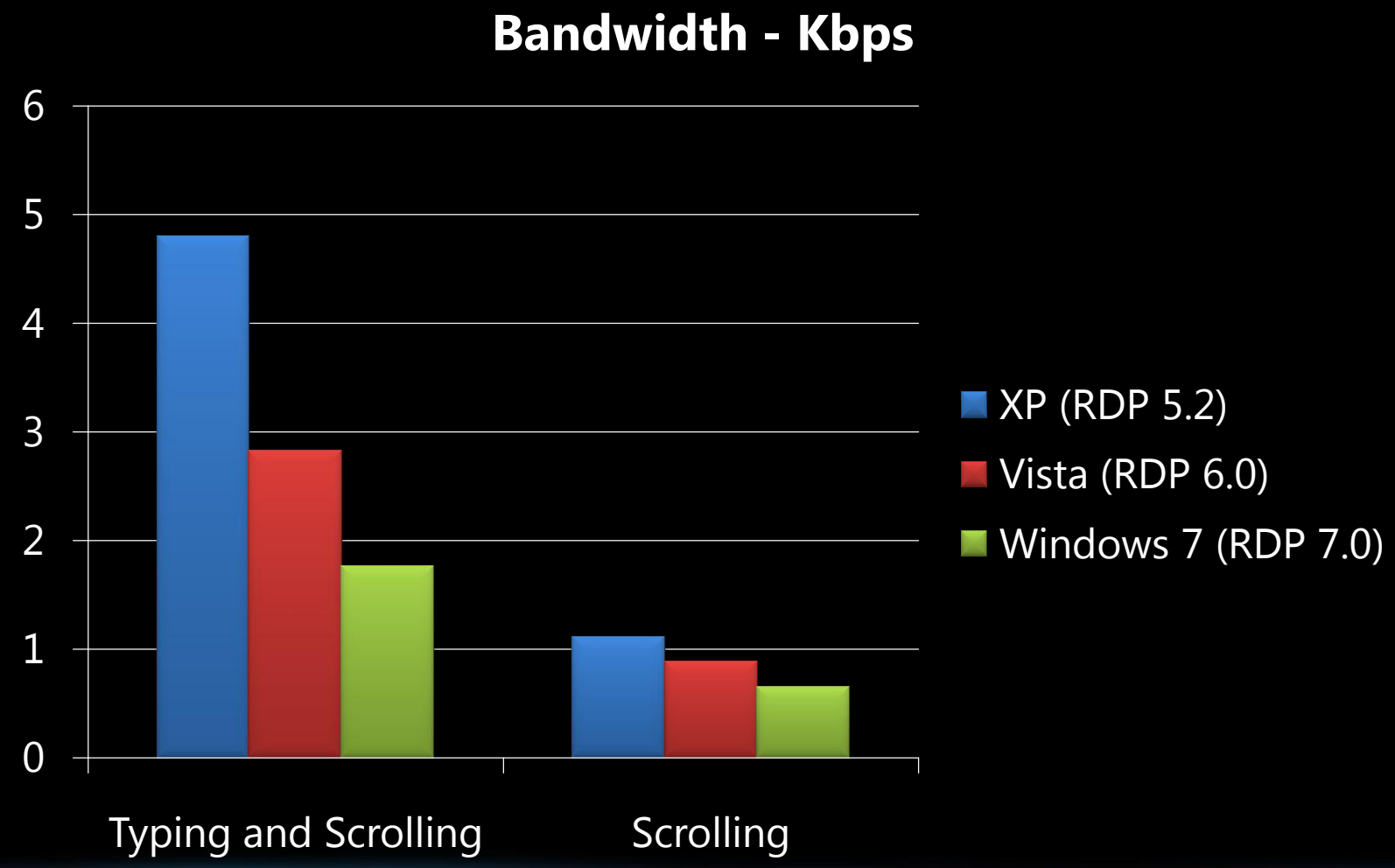


RDP パフォーマンス
グラフィックを多く扱うアプリケーション



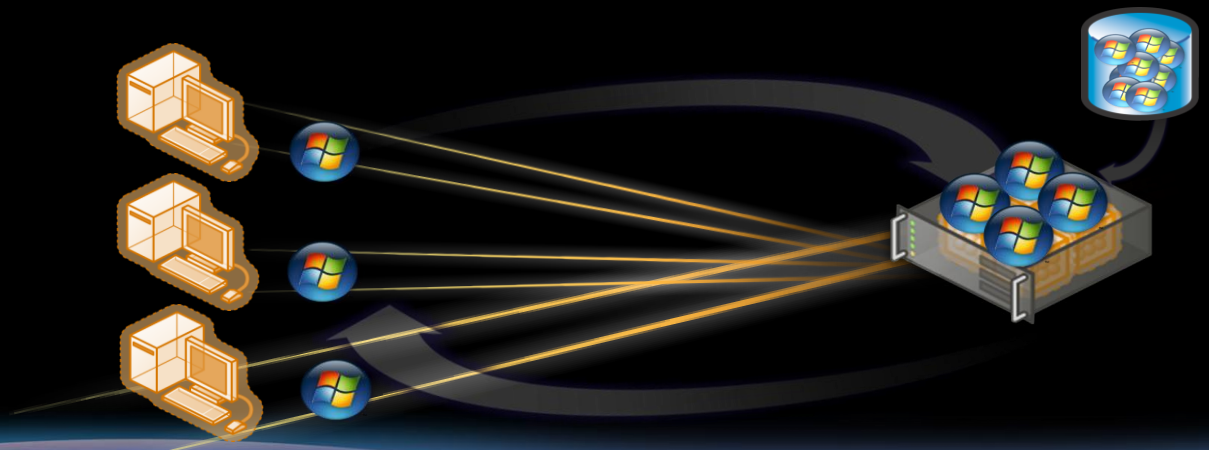
RDP パフォーマンス

Office and LOB アプリケーション



Virtual Desktop Infrastructure(VDI)とは?

- VDIはデスクトップの集約を実現
  - ユーザーに独自のデスクトップまたは一時的なテクストップを提供
  - 管理者はデータセンターに集約されたユーザーワークエリアを管理
  - RDPによるリッチなUIの提供



集中管理されたデスクトップがもたらす利点

RDS (TS)

- 低コストでのイメージ管理
- 最も簡単な管理
- 最小限のリソースを使用
- レガシーアプリケーションとの互換性：低

Pooled Virtual Desktop

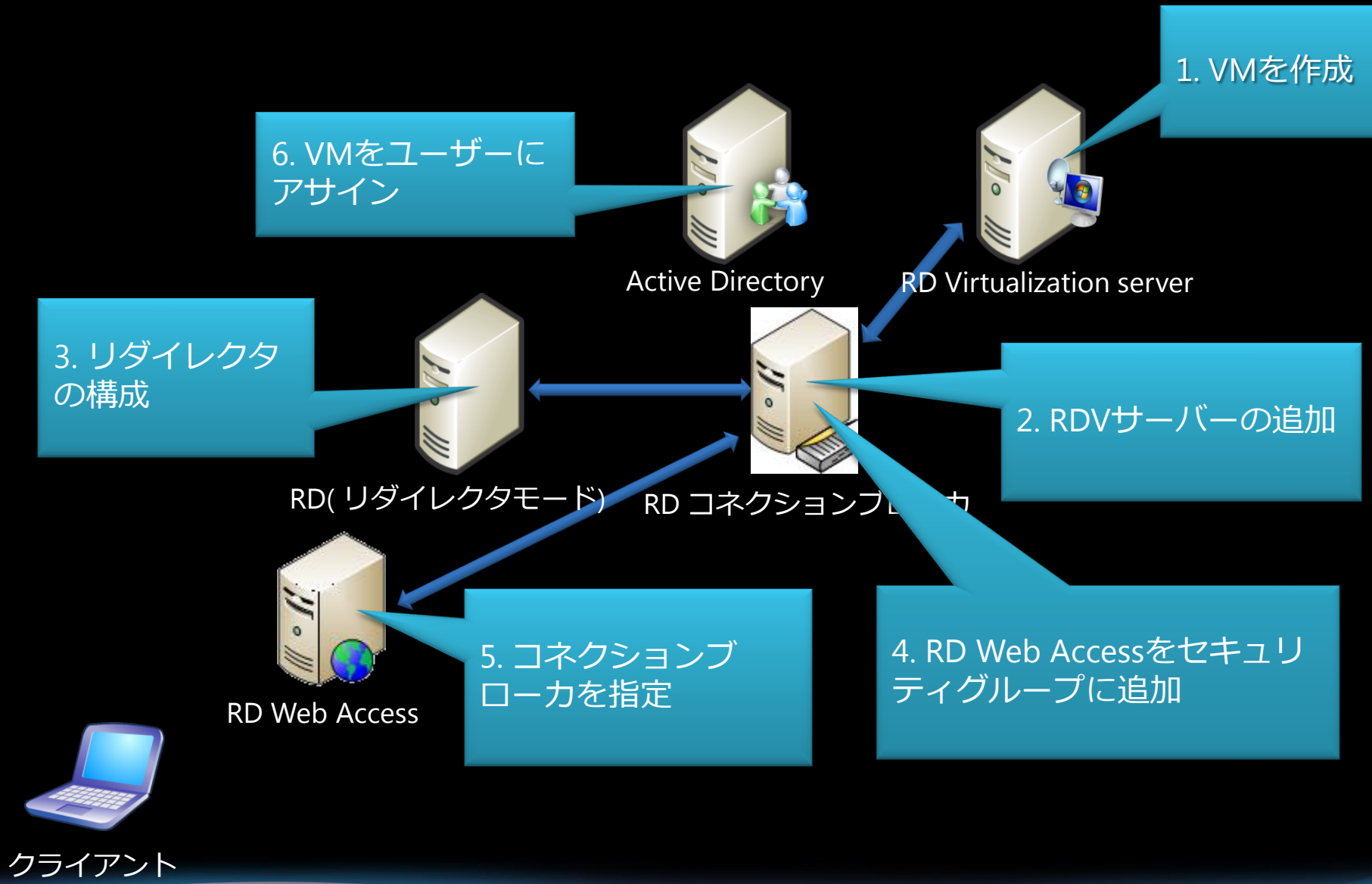
- 中コストでのイメージ管理
- Personal VDより簡単な管理
- Personal VDより少ないリソースを使用
- レガシーアプリケーションとの互換性：中

Personal Virtual Desktop

- イメージ管理が高コスト
- ユーザーによる管理
- 最も多くのリソースを使用
- レガシーアプリケーションとの互換性：高

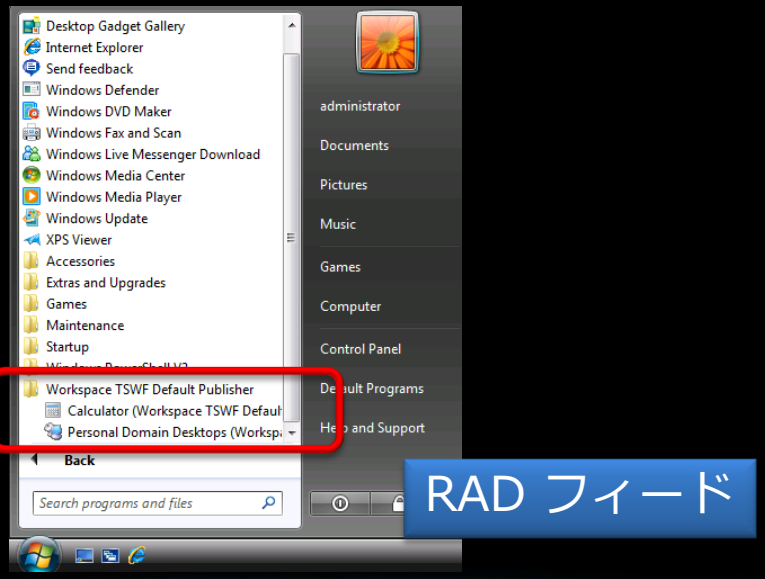
お客様環境に適したソリューションを組み合わせて利用

Personal Virtual Desktopsの構成

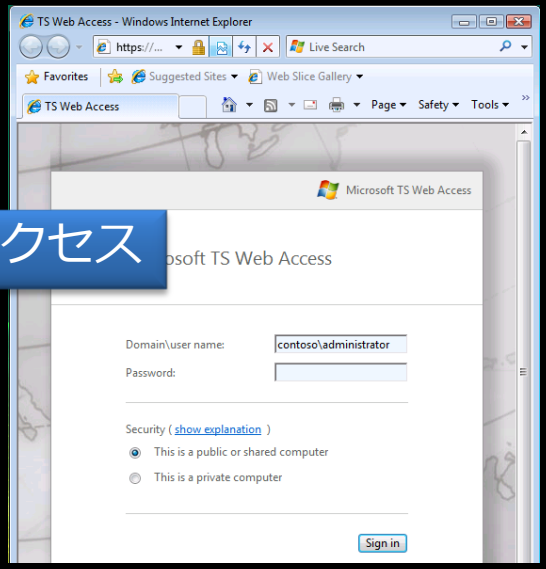


クライアントからのアクセス

- RemoteApp & Desktop (RAD) フィード
  - スタートメニューから RemoteApp プログラムと仮想デスクトップを起動 (Windows 7 クライアントのみ)
- RemoteApp & Desktop (RAD) Web アクセス
  - RemoteApp プログラムと仮想デスクトップ起動用 Web サイトの提供



RAD フィード



RAD Web アクセス

Demo

Remote Desktop Services

RDV (VDI) まとめ

個別またはプールされたVirtual Desktopに対応

- Active Directoryを利用したユーザー毎のVMの割り当て
- RD コネクションブローカーを利用したVMプールからの利用

コネクションの集中管理

- アプリケーションとデスクトップの集中管理(RDS & VDI)
- Windows 7で自動化されたデスクトップ発行とデスクトップの統合

RD と VDI – 統合されたソリューション

- セッションとバーチャルマシンへ接続するためのブローカーの統合とHyper-Vを利用した独創的なVDIシナリオのサポート
- 統一されたユーザーからの接続性

コネクションブローカーの拡張性

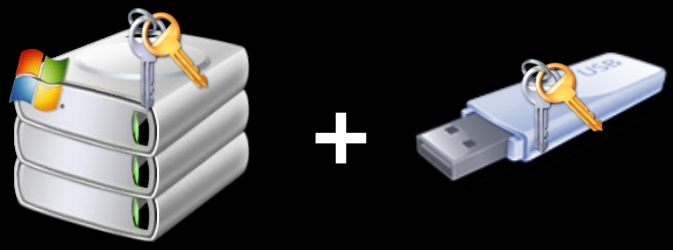
- 調和のとれたプラグイン – VM preparation, VM placement
- ポリシーベースのプラグイン – ロードバランシング、セキュリティ

BitLockerの強化

外部デバイスへの対応

強化されたBitlocker

- BitLocker To Go では USB ストレージデバイスを暗号化可能
  - パスフレーズ
  - スマート カード
  - ドメイン ユーザーID/パスワード
- ユーザーがデバイスにデータを書き込む前に BitLocker 適用を要求可能
- インストール時に BitLocker 構成でのインストール オプションを提供
- ブート パーティションの非表示



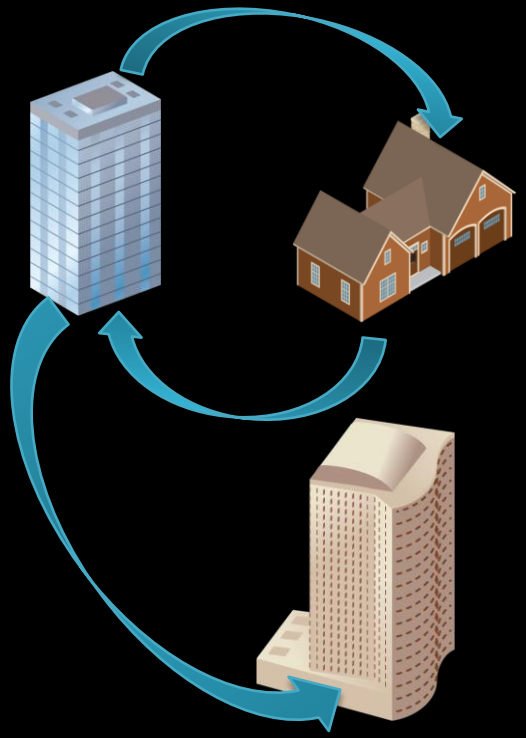
リムーバブルデバイスに対してのBitLocker

ドライブタイプ	Unlockメソッド	リカバリメソッド	管理	その他条件
リムーバブルデータデバイス USB メモリ 外付けハードディスク	パスフレーズ Smart card Automatic unlocking	リカバリパスワード リカバリキー リカバリパスワードのActive Directory へのバックアップ データリカバリエージェント	一貫したグループポリシーでの制御 書き込みアクセス許諾前の暗号化強制	File systems: NTFS FAT FAT32 ExFAT

新しいアンロックメソッド

パスフレーズによる利用性の向上

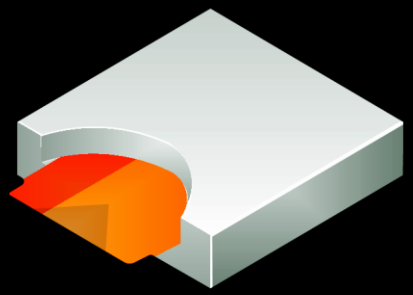
- 特別なハードウェアを必要としない
- ドメイン組織内外での柔軟な利用性
- グループポリシーで管理されたパスフェーズの複雑さと長さの強制



新しいアンロックメソッド

スマートカードによる利用性の向上

- 既存のPKIインフラストラクチャを利用
- 特定のハードウェアが必要
- Windows 7またはWindows Server 2008 R2で利用可能
- パスフレーズよりもセキュリティが高い強力なキーを利用

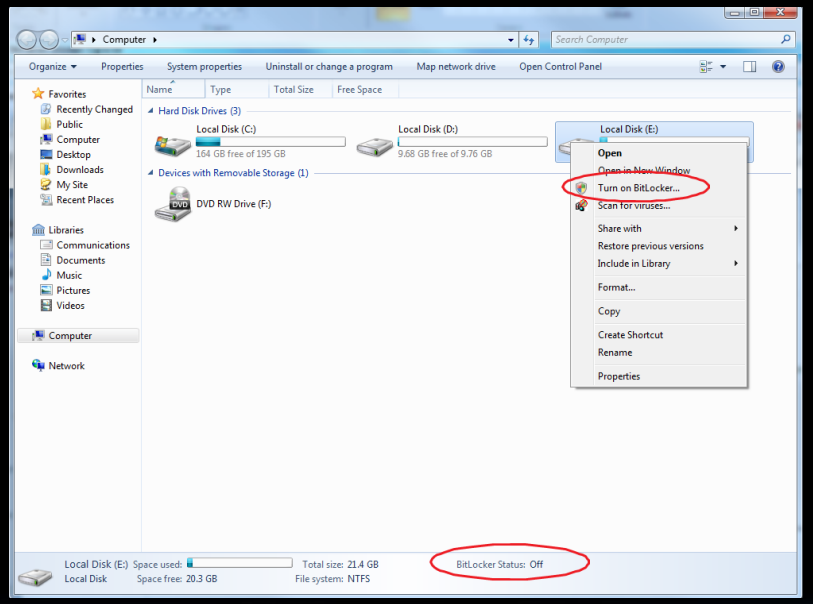


新しいリカバリメカニズム

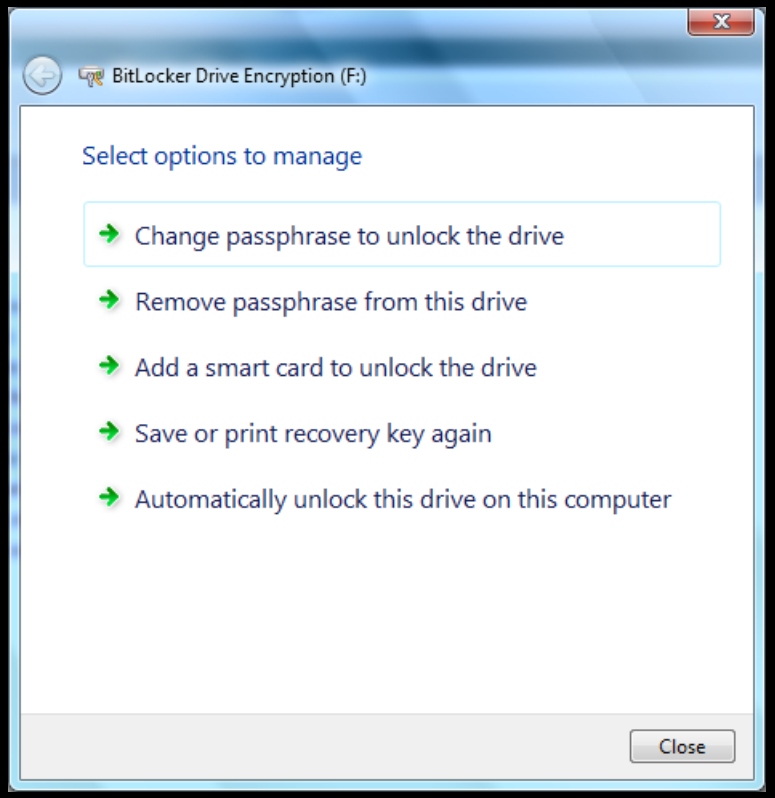
- データリカバリエージェント(DRA)
  - 証明書を利用したキープロテクタ
    - 公開キーを含む証明書はグループポリシーを利用して、マウントされるすべてのドライブに適用
    - 対応する秘密鍵はシステム部門にて保持
  - システム部門が暗号化されたすべてのドライブを復号する権利を所持
  - すべてのデバイスへの共通的なキーがADに保存

Bitlockerの統合

- エクスプローラから BitLocker の制御が可能
- エクスプローラで右クリック
  - BitLocker を有効化
  - デバイスをアンロック
  - BitLocker の管理



BitLocker の管理



データドライブ

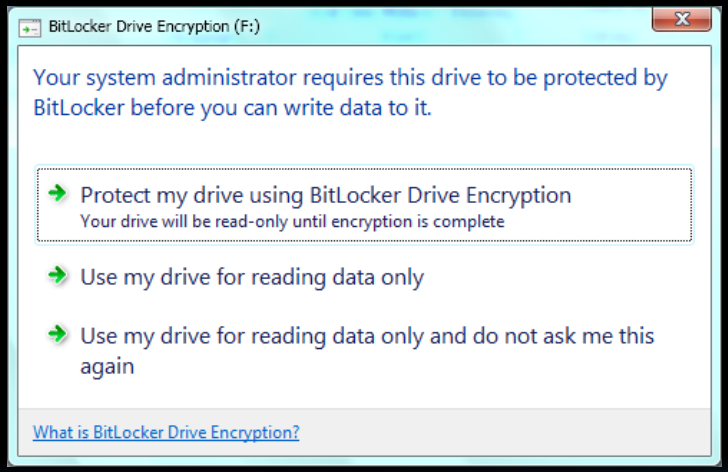
- パスフレーズの追加、削除、変更
- スマートカードの設定
- automatic unlockingの設定
- リカバリ key/passwordの複製

システムドライブ

- リカバリ key/passwordの複製
- PINのリセット
- startup keyの複製

リムーバブルデバイスに対しての強制

- リムーバブルデバイスに対して BitLocker を強制
  - このポリシーを有効にするとすべてのリムーバブルドライブに対して書き込むためには Bitlocker での暗号化が必須となる
  - ドライブがマシンに接続されるとともに、BitLockerを有効にするか、読み取り専用にするかを促すダイアログが表示される



Demo

Bit Locker to Go

APP Locker

不適切なアプリケーションの利用を抑制

不適切なアプリケーションの利用

- 許可されていないアプリケーションもインストールされると実行可能
  - 標準権限でもアプリケーションによってはインストール可能
- 主なリスク:
  - マルウェアの侵入
  - ヘルプデスク負荷の増加
  - デスクトップ標準化の妨げ
  - ライセンス違反

不適切なアプリケーションの抑制

- APP Locker による抑制
- どのアプリケーションの実行をユーザーに許可するのかを設定可能
  - グループ ポリシーによる設定
  - 電子署名による制限
  - バージョンによる利用制限

- 例）マイクロソフトによって署名された
  Microsoft Dynamics CRM の
  バージョン 1.0 以上なら利用許可

Demo

APP Locker

DNS SEC

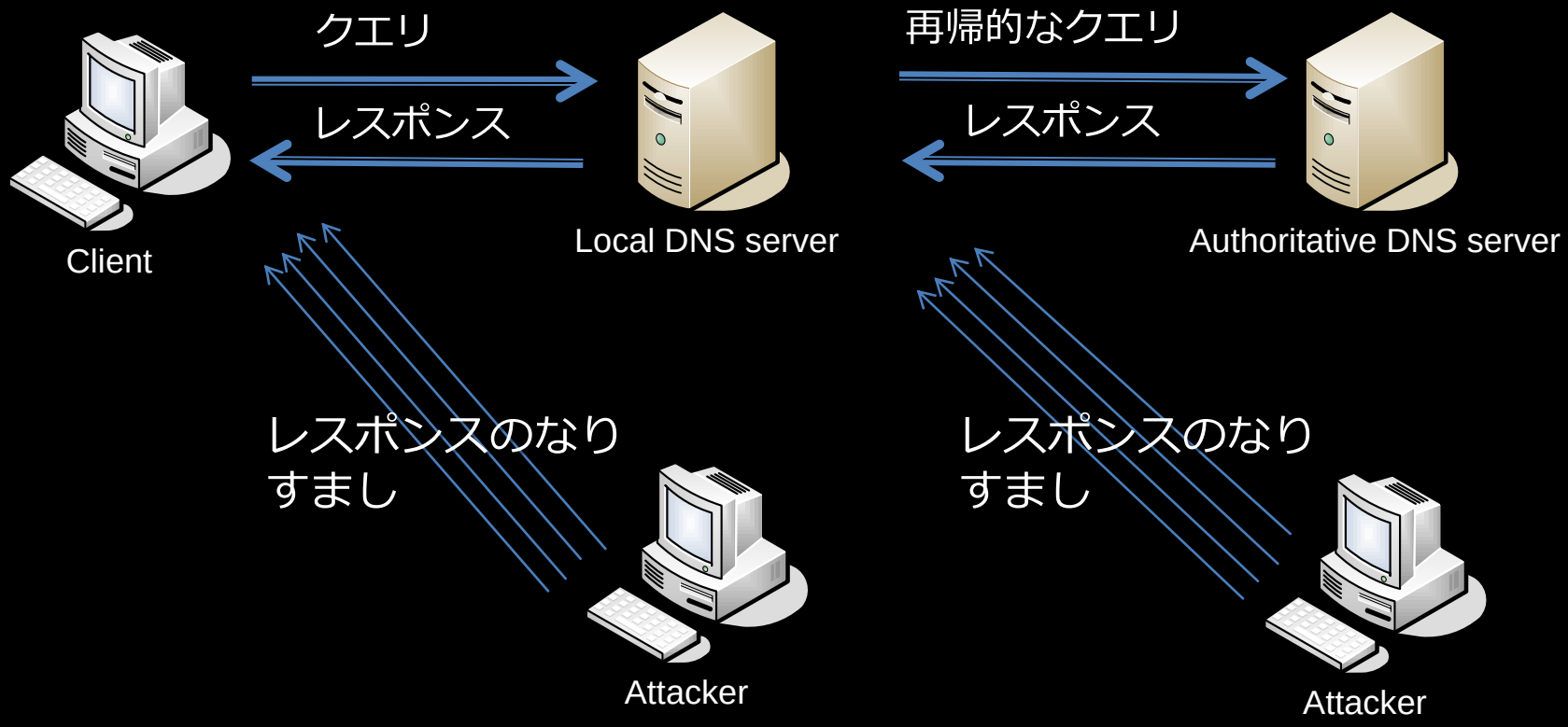
DNSサーバーのセキュリティ強化

DNSSEC 概要

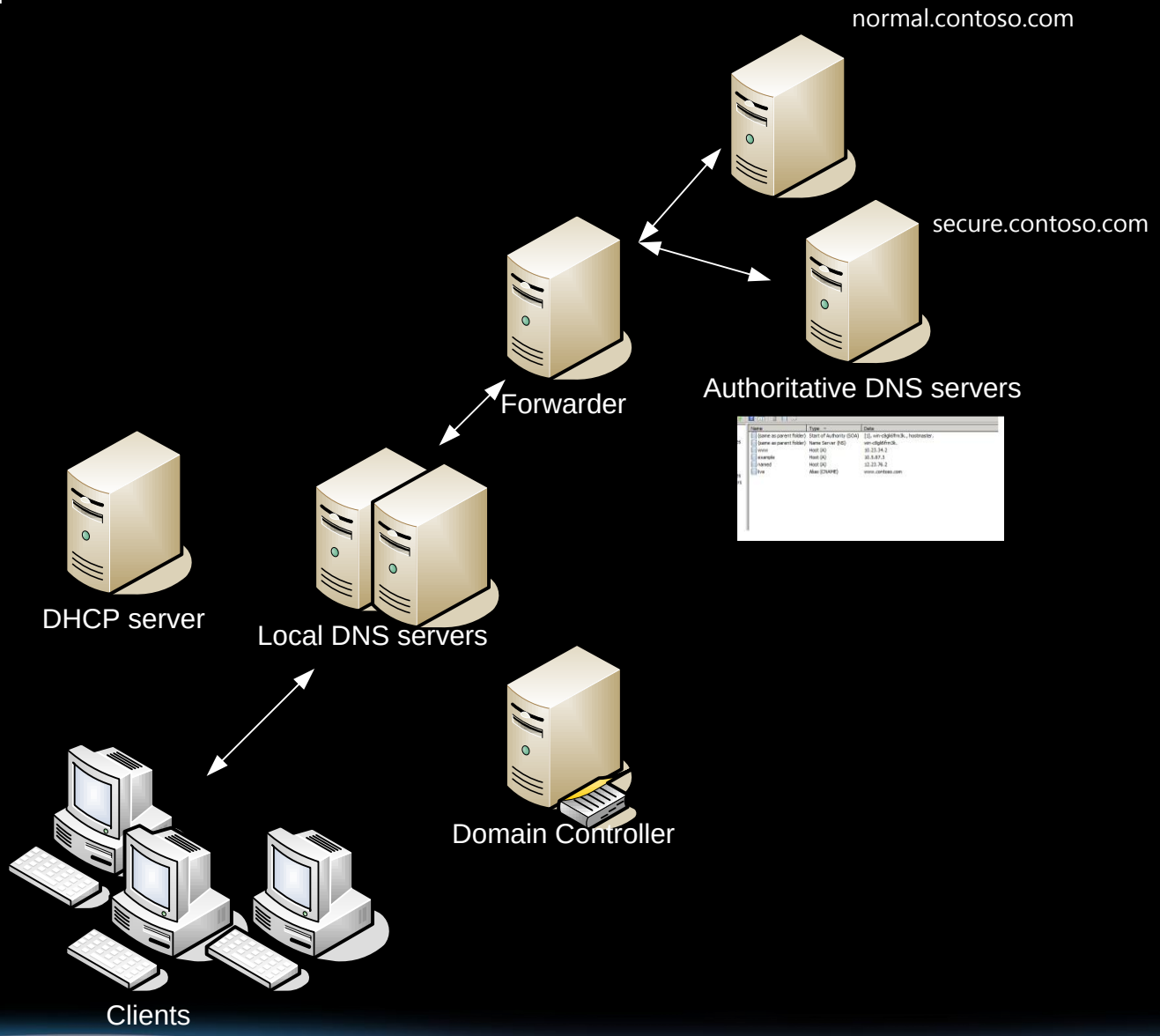
- DNSSEC とは？
  - DNSのセキュリティを向上させるための拡張
  - DNSのデータの安全性を高める
  - RFC 4033, 4034 and 4035 で定義

- DNSSEC が提供する機能
  - オリジナルデータの提供
    - “データは正式な機関から提供される”
  - データの保全
    - “データは改ざんされたものではない”
  - 存在の否認を認証
    - “データが存在していないことを証明”

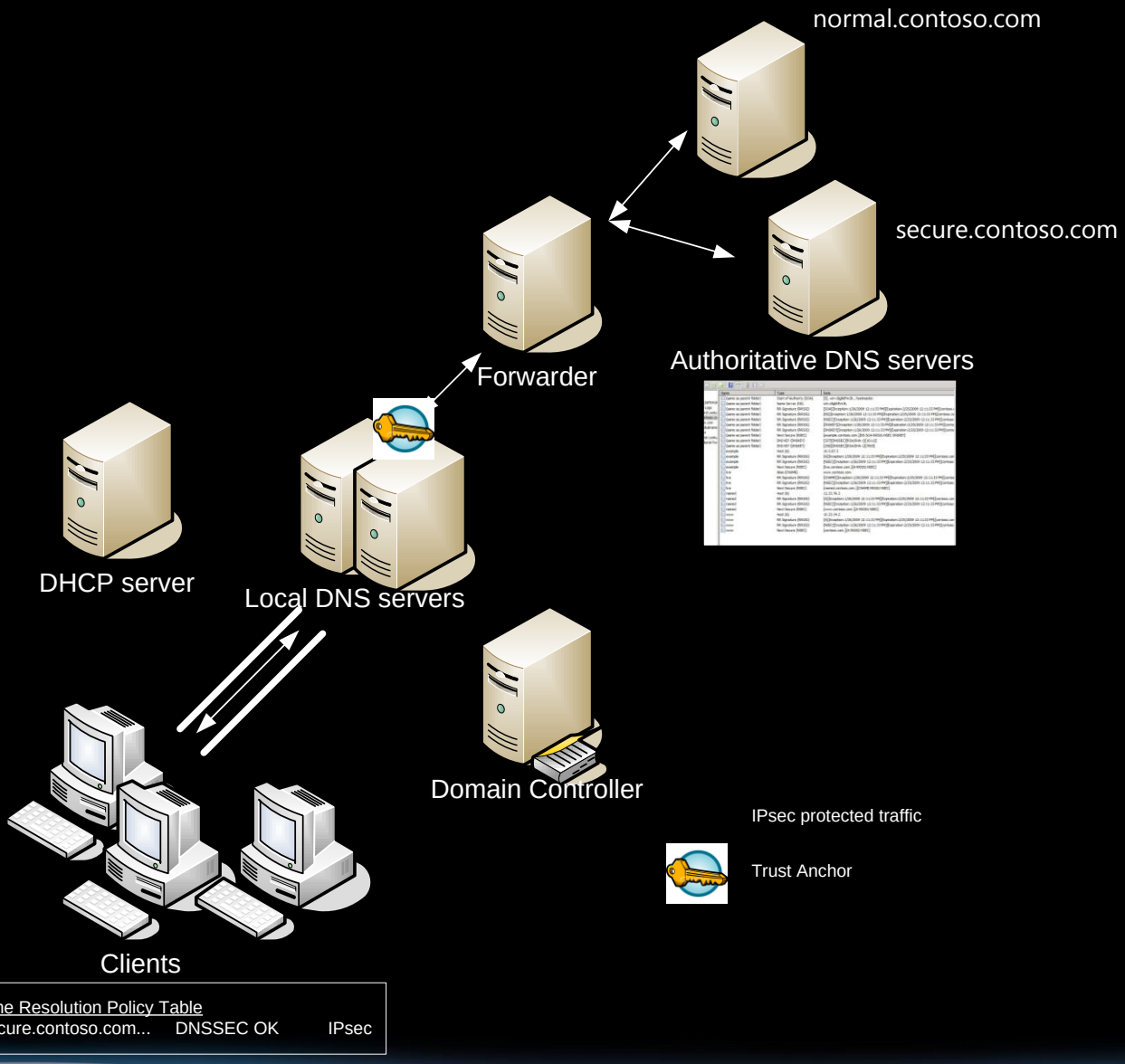
DNS レスポンスのなりすまし



DNSSEC の展開
導入前



DNSSEC の展開
導入後

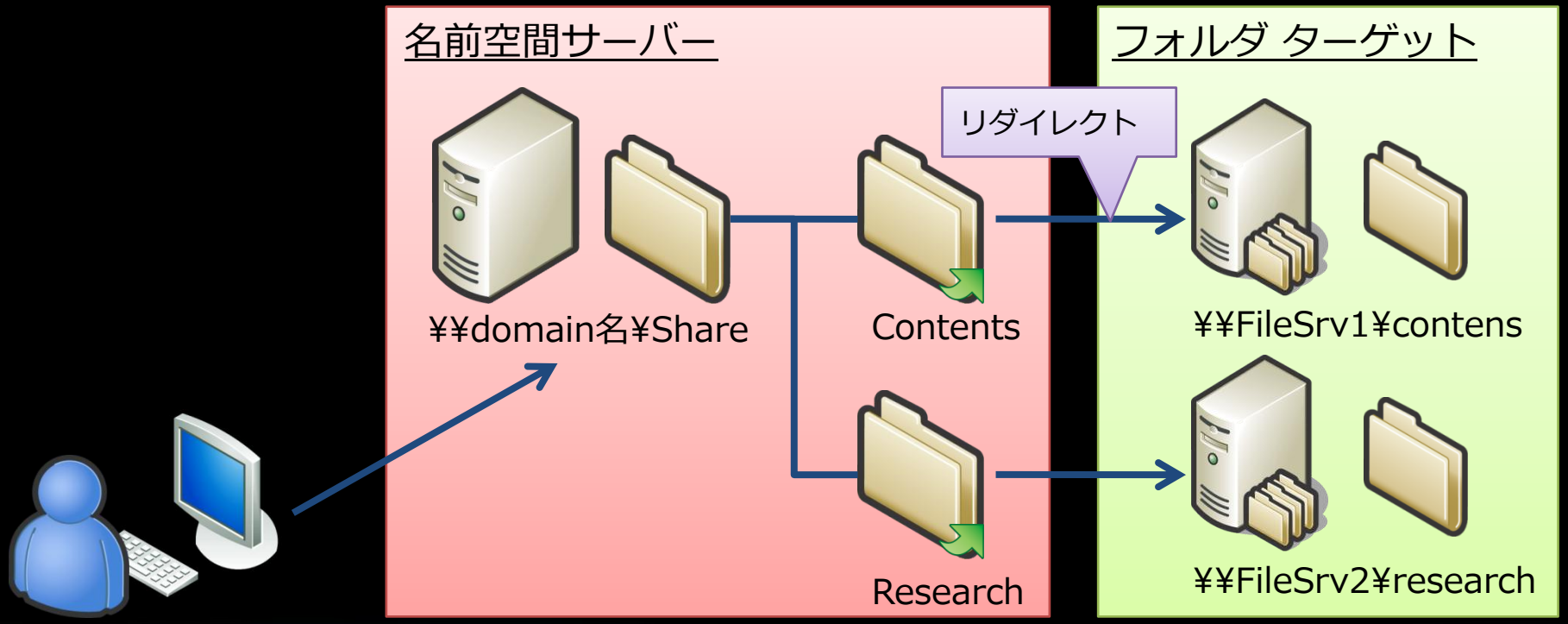


DFS-R

読み取り専用の分散ファイルシステムによる
セキュリティ強化

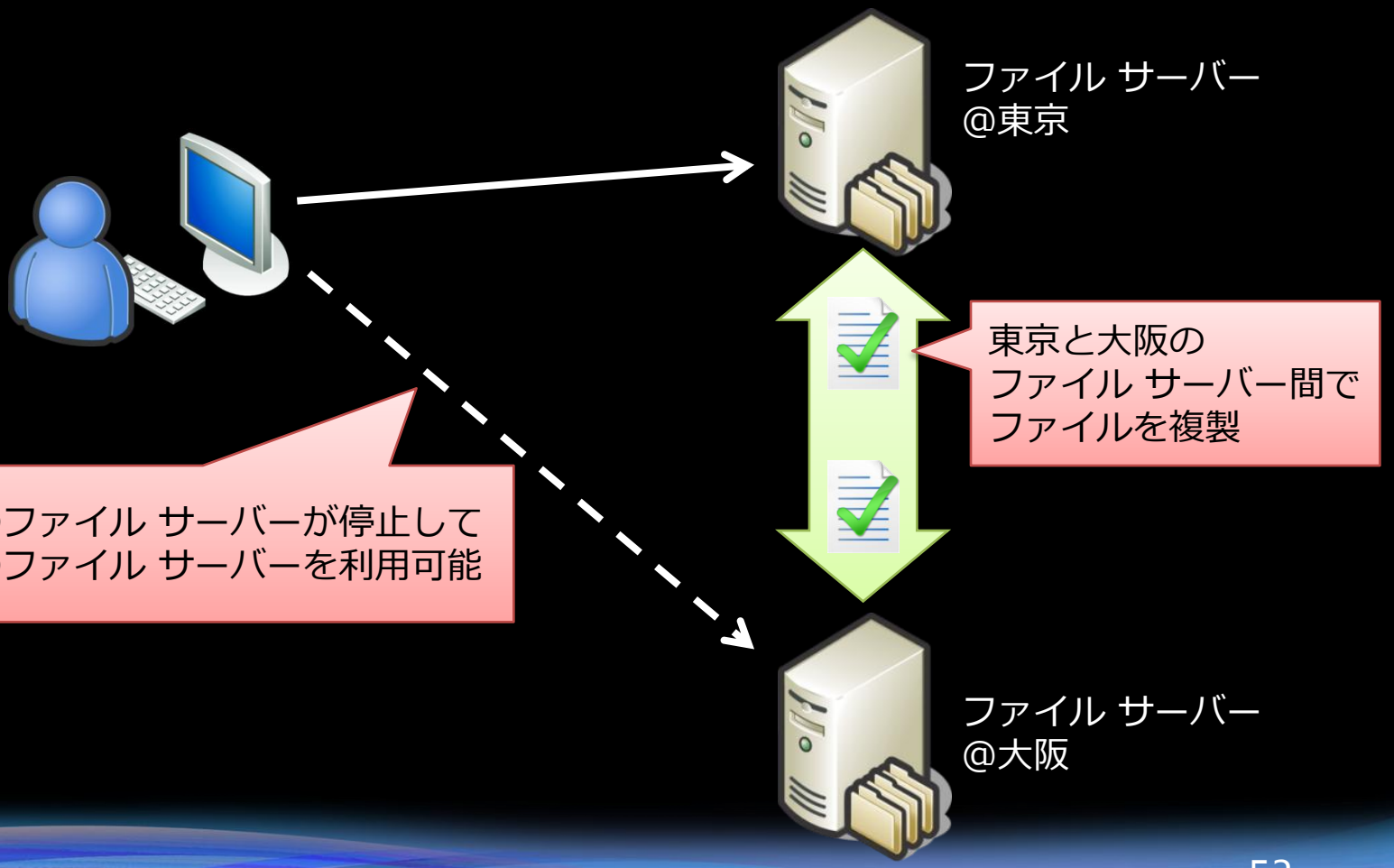
分散ファイルシステム(DFS)

- 共有フォルダをドメイン名ベースのパスで指定
- コンピューター名の変更やリプレースによる共有フォルダのリンク切れを防止



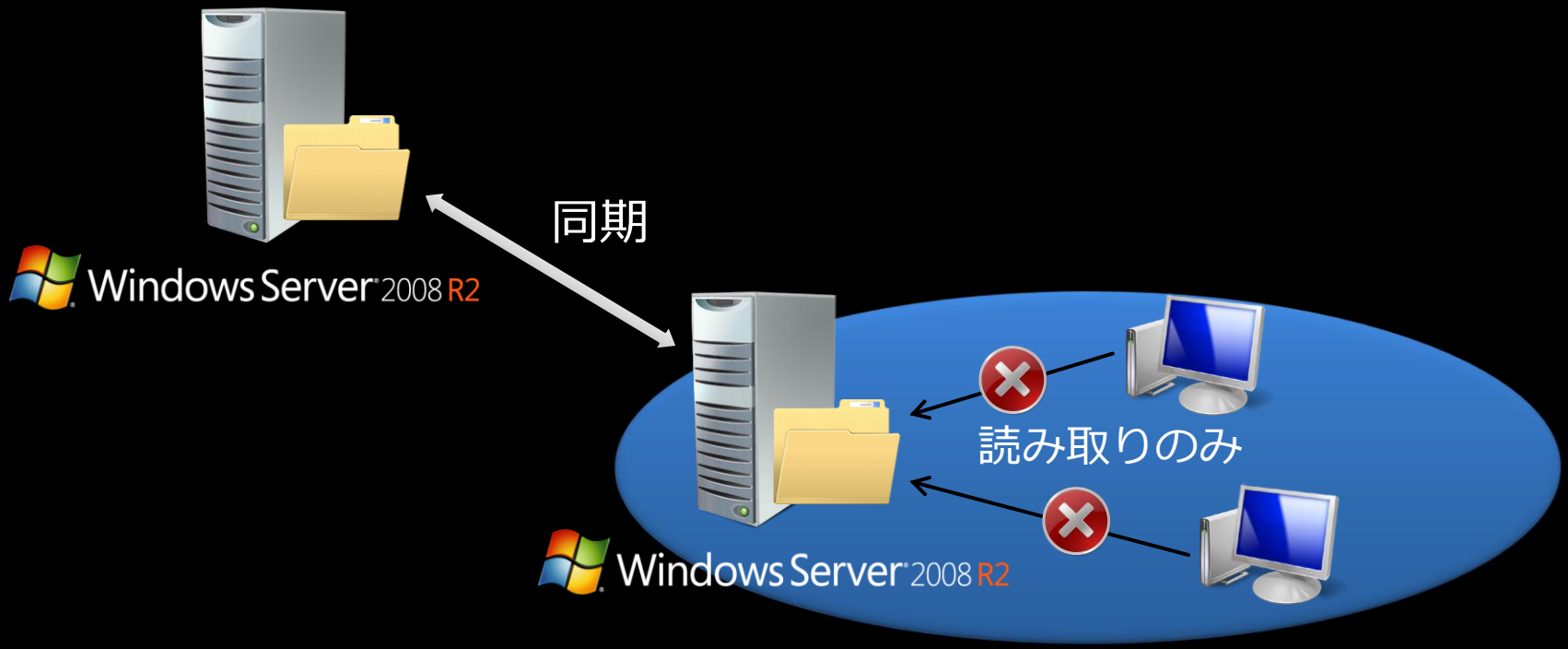
DFS レプリケーション

- 複数のファイル サーバー間でファイルを複製し
  ファイル サーバーの障害対策が可能



読み取り専用分散ファイル システム (DFS)

- 読み取り専用の DFS
  - 拠点のセキュリティ強化
  - ブランチ オフィスのユーザーに
    コンテンツ変更を防ぎながらのアクセスを提供



Demo

DFS-R

まとめ

まとめ

それぞれ単独 OS としての機能強化も多くなされている

Windows 7とWindows Server 2008 R2 を組み合わせることで
企業にさらなるソリューションを提供

Windows® 7

Future Technology Days


Microsoft®