Windows Server 2016 による
セキュアで最適化された ITインフラの構築
- Software Defined Infrastructure の実現 -

NEC マネジメントパートナー
シニアテクニカルエバンジェリスト
Microsoft MVP
吉田 薫

Software Defined Infrastructure（SDI）

- ハードウェアではなくソフトウェアで IT インフラを定義
- IT インフラの柔軟性とコスト効率の向上を実現

コンピューティング

コンピューティングの
安定性、柔軟性、俊敏性の向上
容易なアップグレード

ストレージ

仮想化に最適化された
エンタープライズ階層化ストレージ
高い費用対効果

ネットワーク

シンプルなネットワーク
複数のテナントの分離

セキュリティ

新たな脅威に対抗する
ハードウェア支援型の
セキュリティの向上

Windows Server 2016

- Software Defined Infrastructure の中核となるクラウド対応 OS

最新の多層セキュリティ

- 特権アクセスの制御
- 仮想マシンの保護
- 最新の攻撃に対するプラットフォームの強化

ソフトウェア定義データセンター

- 新しい Hyper-V による仮想マシンの
  パフォーマンスと信頼性の向上
- ソフトウェアによるストレージの構成
- ソフトウェアによるネットワークの構成

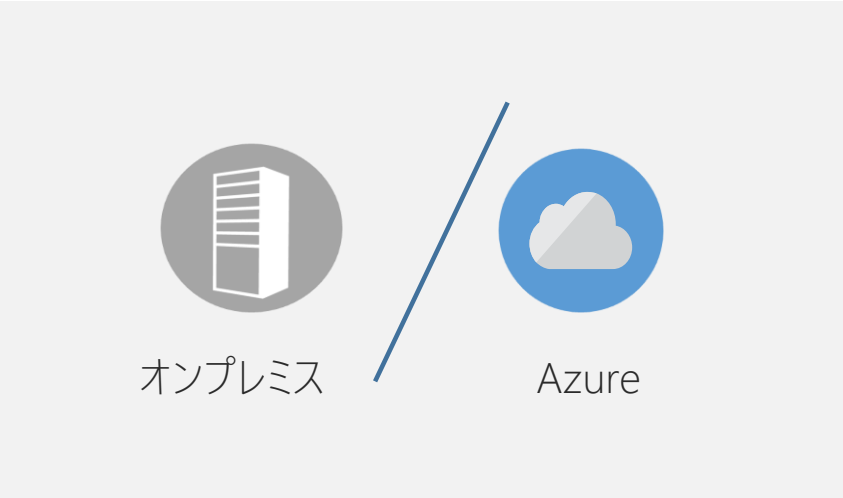
クラウド対応
アプリケーションプラットフォーム

- 軽量な Nano Server の提供
- Docker ベースのコンテナー技術

Windows Server 2016 のライセンスモデルの変更

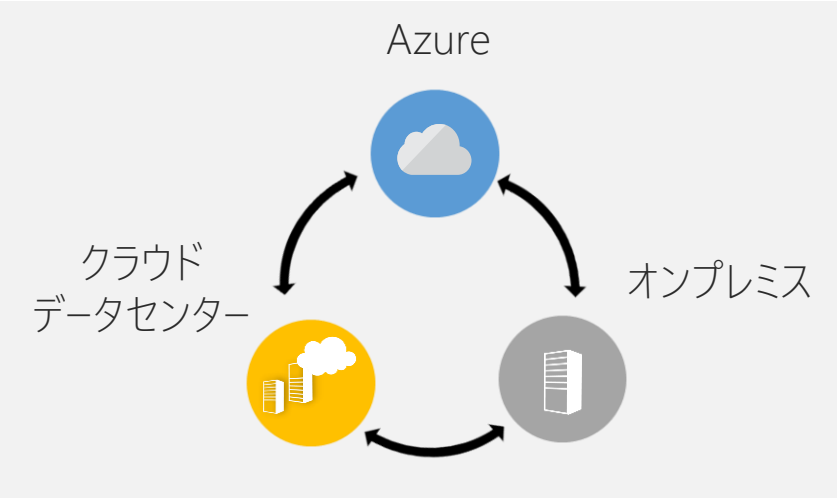
- 異なる環境間の一貫性を保つために新しいアプローチ

オンプレミスはプロセッサベース、
クラウドはコアベースのライセンス



- 課金方法が一本化されていない
- お客様がわかりづらく感じられる原因

コアベースのライセンスに統一



- 環境が異なっても一貫したアプローチを提供
- マルチクラウド シナリオに対応
- Azure ハイブリッド使用特典 (HUB) などの特典により Windows Server のワークロードのポータビリティを向上
- ライセンス モデルの違いによる矛盾を解消

Windows Server 2016 のライセンスモデル

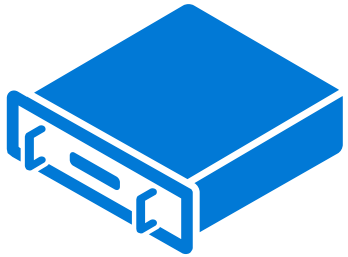
- サーバーライセンスは物理プロセッサ単位から物理コア単位へ
  - サーバーごとに最低 16 個、物理プロセッサごとに最低 8 個のコアライセンスが必要
  - コアライセンスは 2 コアパックで販売
  - 1 台の物理サーバーに最低 8 個の 2 コアパックが必要

物理コア/プロセッサ

プロセッサ/サーバー	2	4	6	8	10
1	8	8	8	8	8
2	8	8	8	8	10
4	16	16	16	16	20

Microsoft

intel



コンピューティング

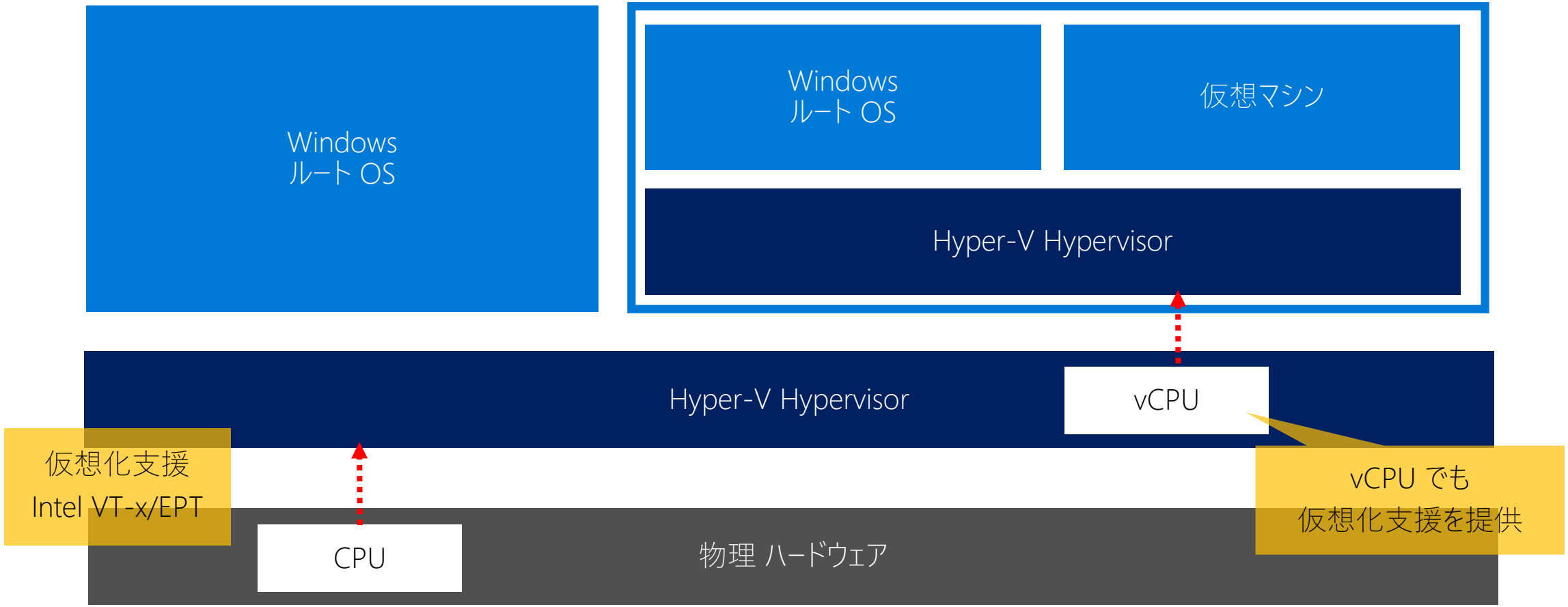
Hyper-V のスケーラビリティ

- Windows Server 2012 R2 よりさらに向上したスケーラビリティ

機能	Windows Server 2012 R2	Windows Server 2016	(参考) VMware vSphere 6 Enterprise Plus
物理プロセッサの最大数	320	512	480
物理メモリの最大サイズ	4 TB	12 TB	6 TB (12 TB : 一部 OEM プラットフォーム)
仮想プロセッサの最大数	64	240	128
仮想メモリの最大サイズ	1 TB	16 TB	4 TB

ネストされた Hyper-V

- Hyper-V 仮想マシン内でさらに Hyper-V を実行
- 評価環境や学習環境に最適



ネストされた Hyper-V 仮想マシンの準備

- 動的メモリの無効化
- vCPU での仮想化支援の有効化

```
Set-VMProcessor –VMName <仮想マシン名> -ExposeVirtualizationExtensions $true
```

- MAC アドレスのスプーフィングの有効化

```
Get-VMNetworkAdapter -VMName <仮想マシン名> | Set-VMNetworkAdapter -MacAddressSpoofing On
```

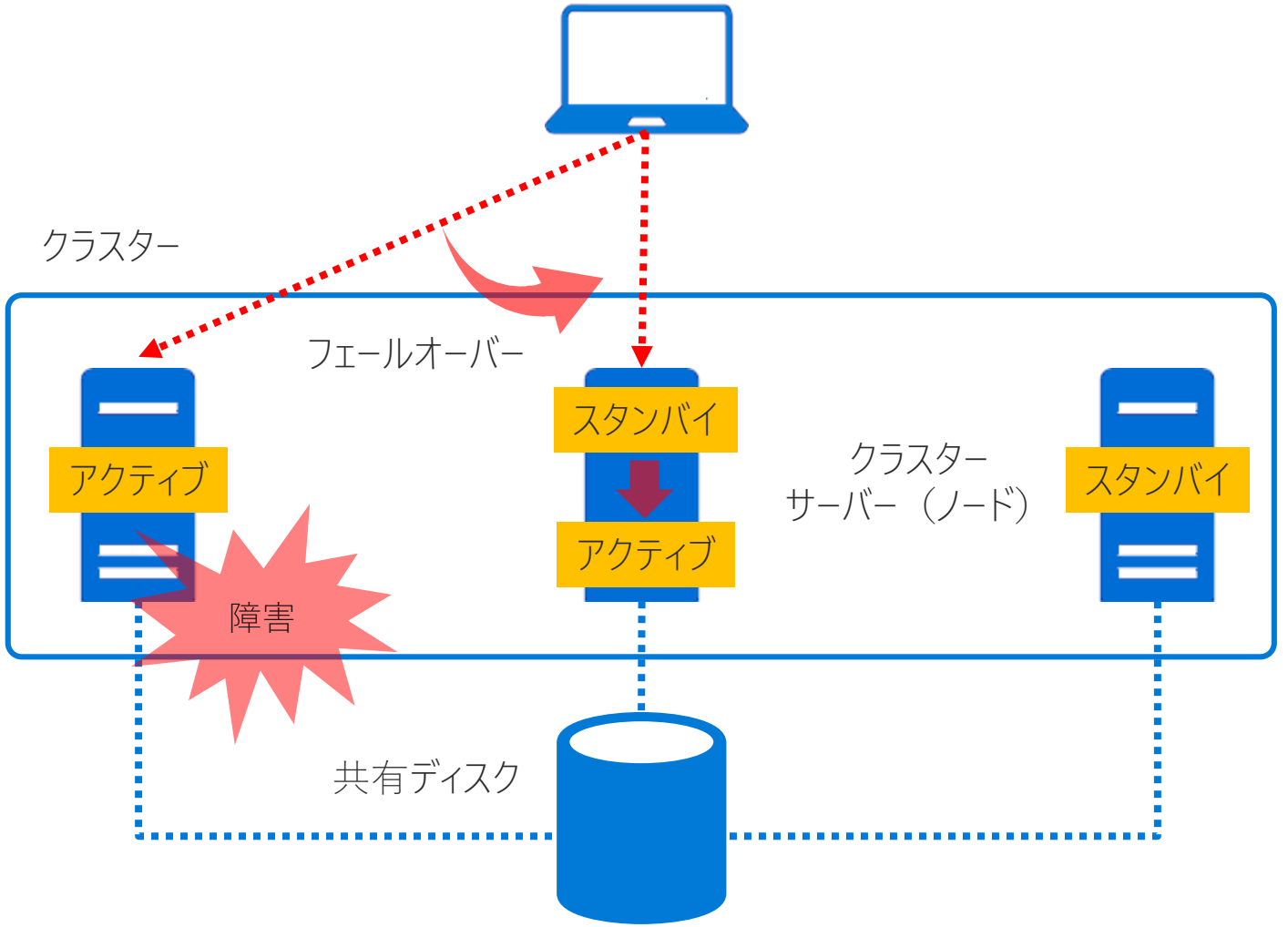
動的なリソースの追加と削除

- 実行中の Hyper-V 仮想マシンに対するリソースの追加と削除が可能
- 仮想マシンの再起動回数も減少

	Windows Server 2012 R2 Hyper-V	Windows Server 2016 Hyper-V
プロセッサ	静的のみ	静的のみ
ディスク	ホットアド、リムーブ	ホットアド、リムーブ
メモリ	動的メモリ	動的メモリまたは ホットアド、リムーブ
ネットワークアダプター	静的のみ	ホットアド、リムーブ

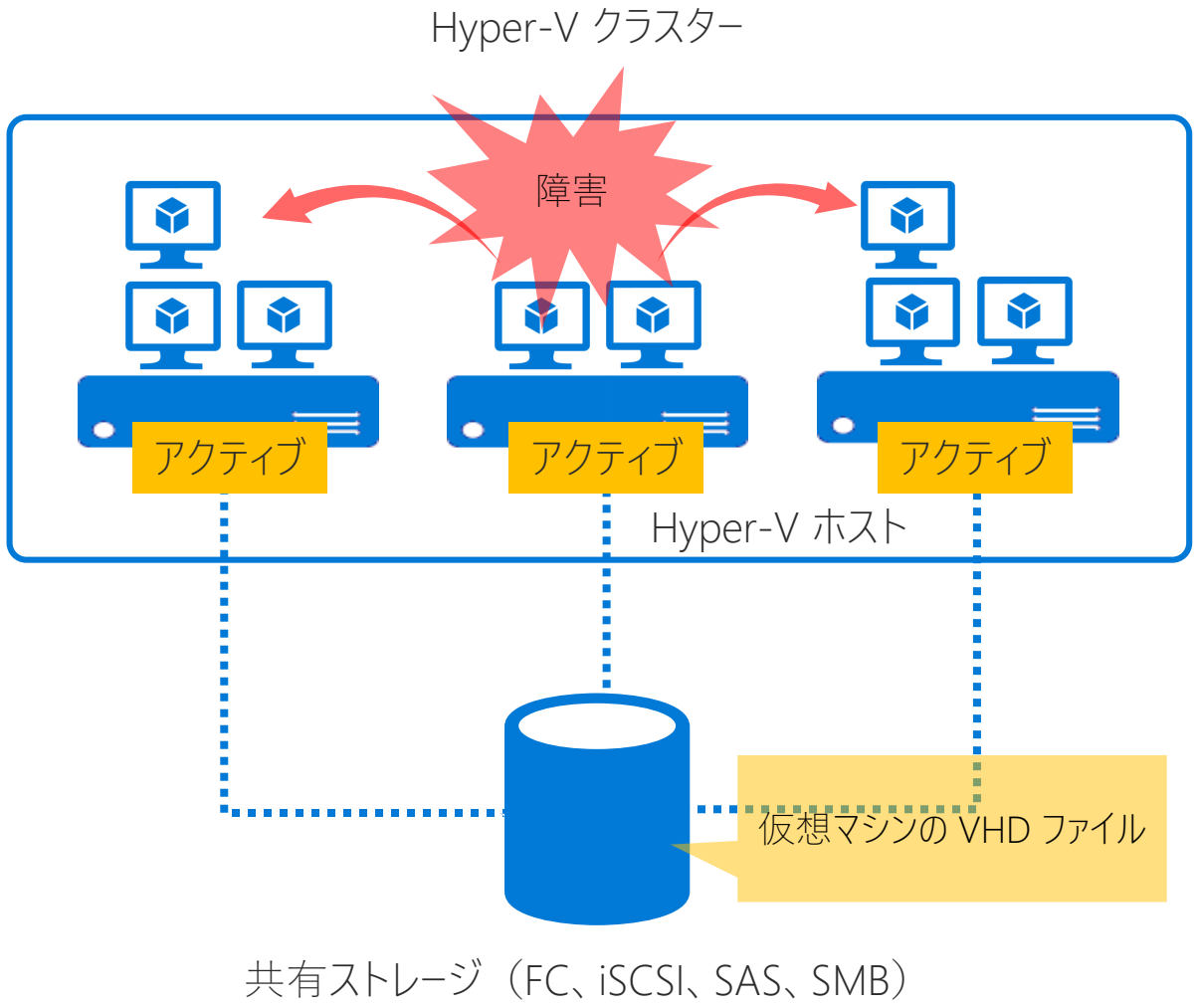
（復習）フェールオーバークラスター

- 様々なワークロードに高いスケーラビリティと可用性を提供
- Hyper-V、SQL Server、ファイルサーバーなどのワークロードで活用
- アクティブなクラスターノードで障害が発生した場合、別のクラスターノードがサービスを引き継ぐ「アクティブ/スタンバイ」方式が基本



（復習）Hyper-V （ホスト）クラスター

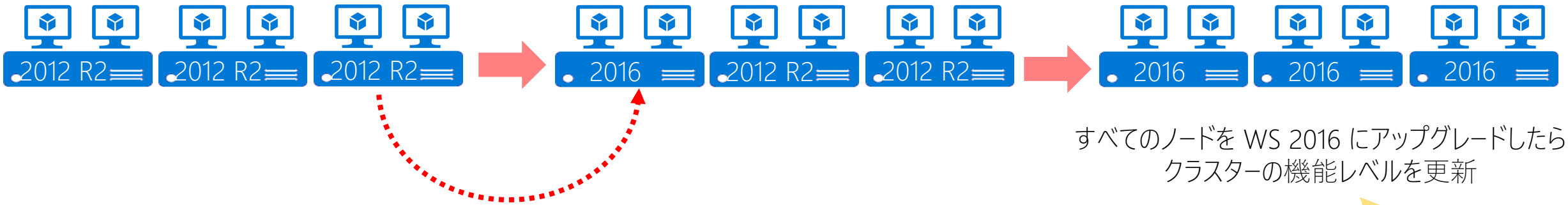
- Hyper-V ホストの障害を監視し、障害時、自動的に別の Hyper-V ホストで仮想マシンを再起動
- ホストだけでなく、ゲストの障害監視も可能
- 仮想マシンの VHD ファイルは共有ストレージに格納
- 共有ストレージとして、FC、iSCSI、SAS 以外に SMB をサポート



Hyper-V クラスターのローリングアップグレード

- ワークロードを停止することなく、Windows Server 2012 R2 から Windows Server 2016 へ Hyper-V クラスターをアップグレード可能

Update-VMConfigurationVersion で
仮想マシンの構成バージョンを更新することで
Hyper-Vの新しい機能が利用可能に



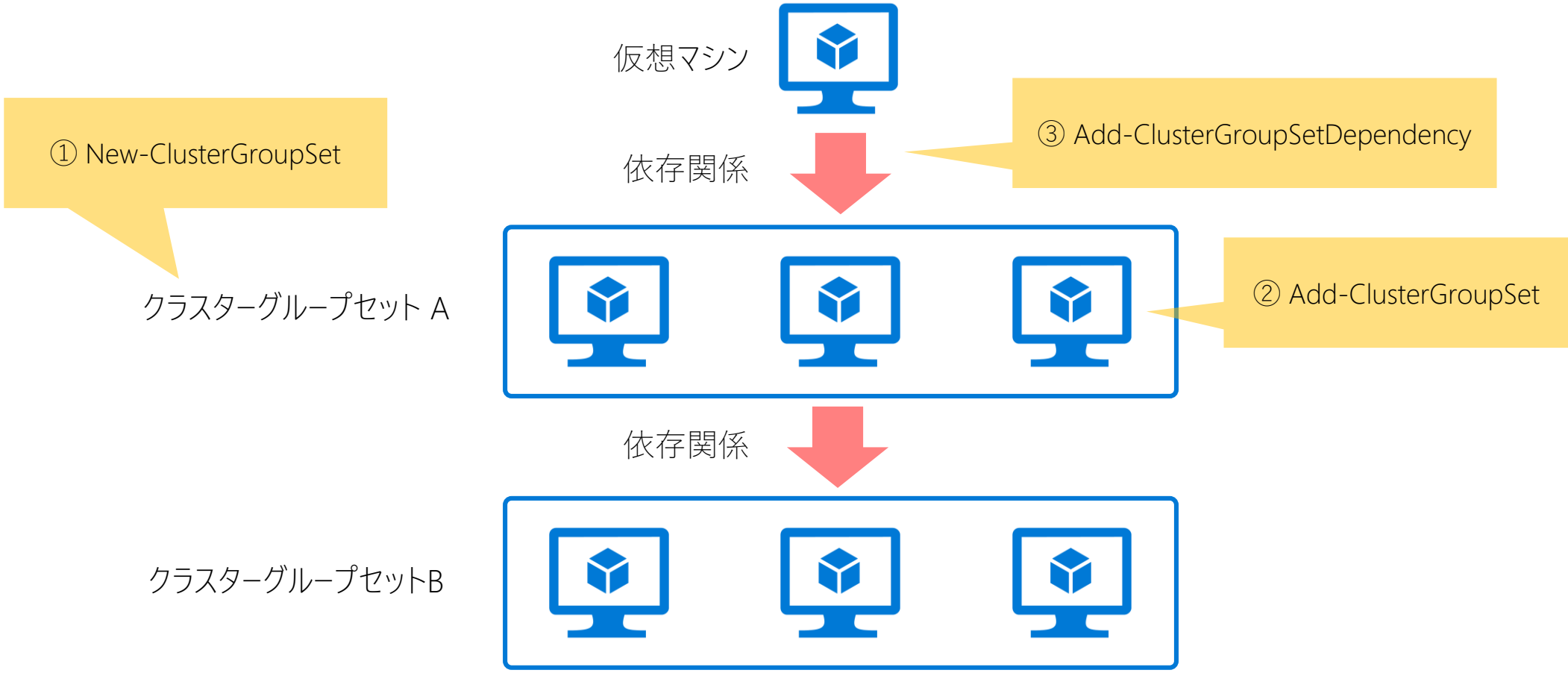
WS2012 R2 ノードをクラスターから削除し、
WS 2016 をクリーンインストール、再度、クラスターに追加

すべてのノードを WS 2016 にアップグレードしたら
クラスターの機能レベルを更新

Update-ClusterFunctionalLevel

Hyper-V クラスター仮想マシンの開始順序の制御

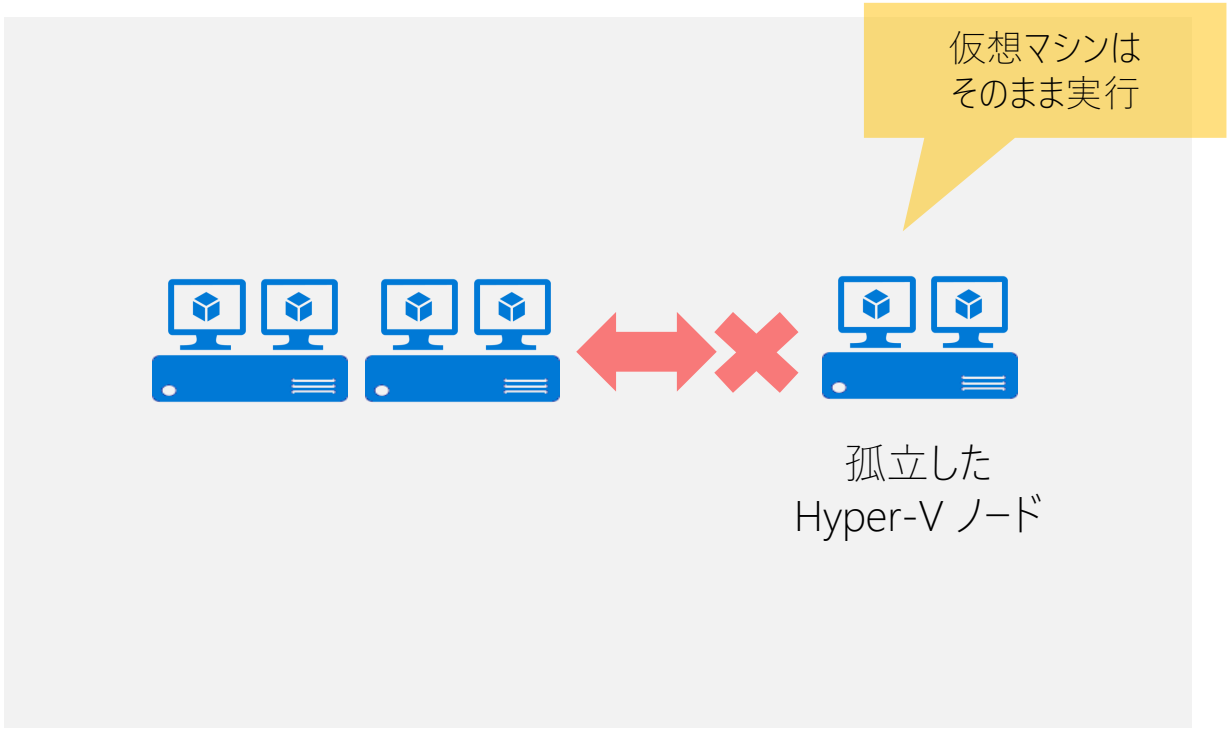
- 依存関係に基づき、仮想マシンの開始順序を設定
- 多階層システムにおける起動順序による障害を回避



Hyper-V クラスターの仮想マシンの回復性

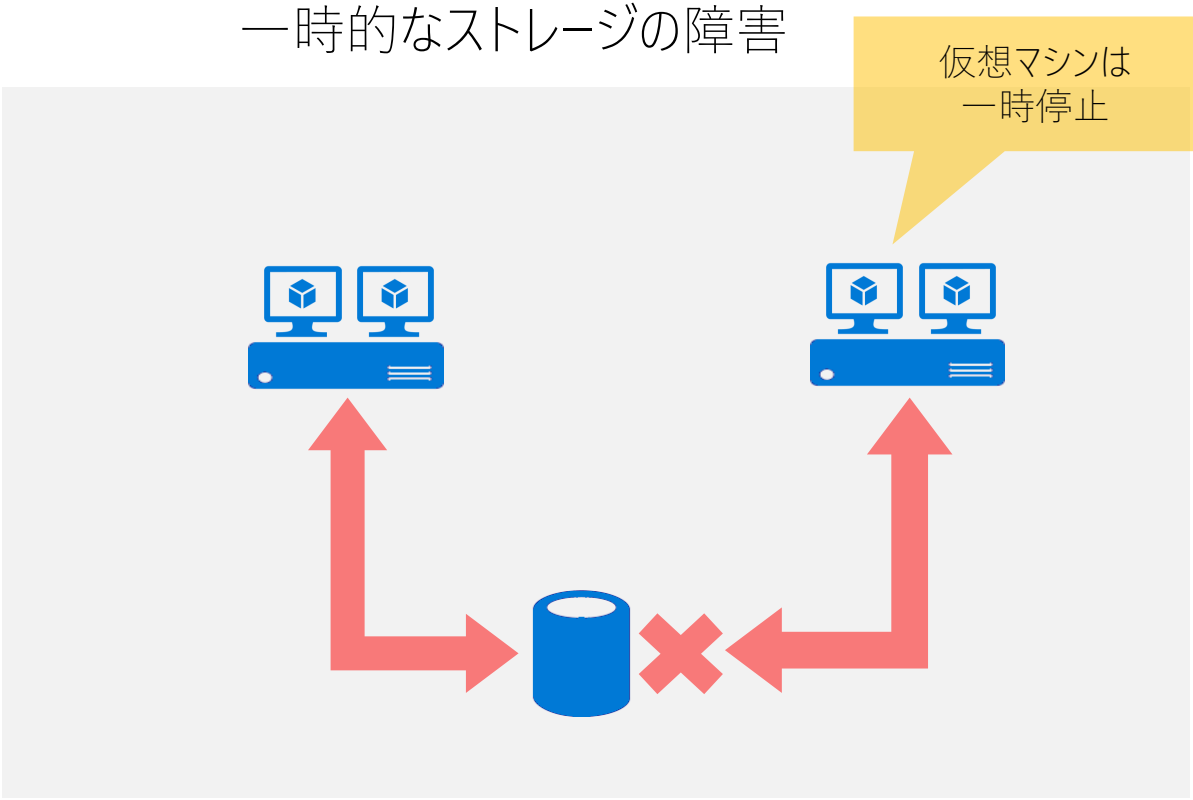
- 短時間の障害を許容し、自動的に障害が解決するまで待機

一時的なネットワークの障害



孤立した状態のまま、仮想マシンを実行

一時的なストレージの障害

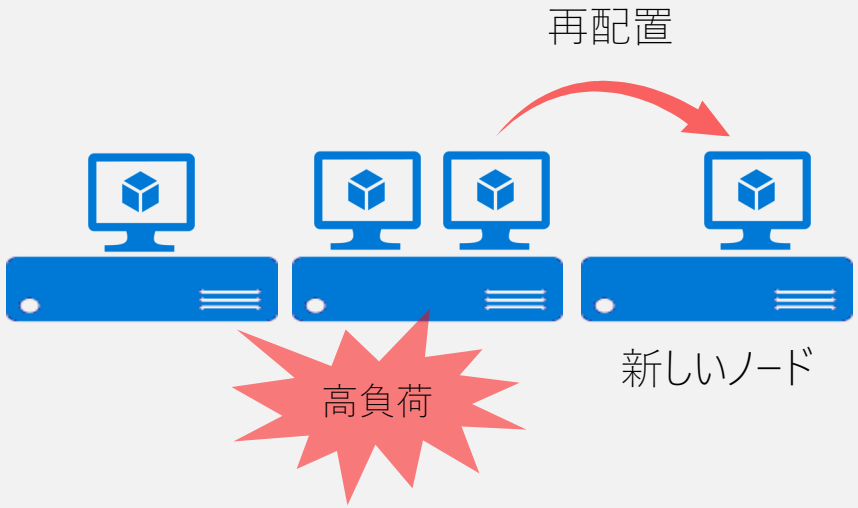


仮想マシンを一時停止

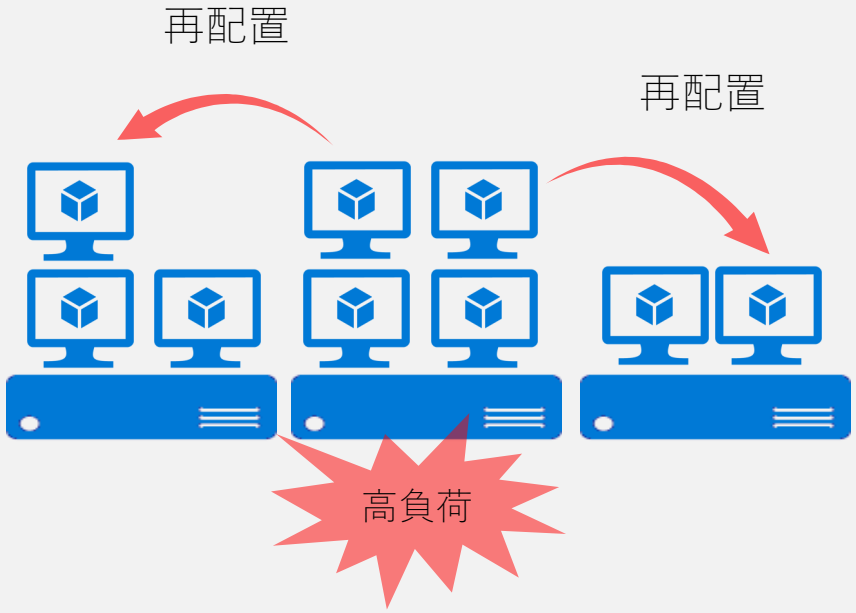
Hyper-V クラスター仮想マシンのノードフェアネス

- Hyper-V ホストの負荷に合わせて、仮想マシンを再配置して負荷を平均化
- 既定ではメモリと CPU のリソース使用率が 80% を超えると再配置を開始

ノードの追加時



定期的（30分間隔）



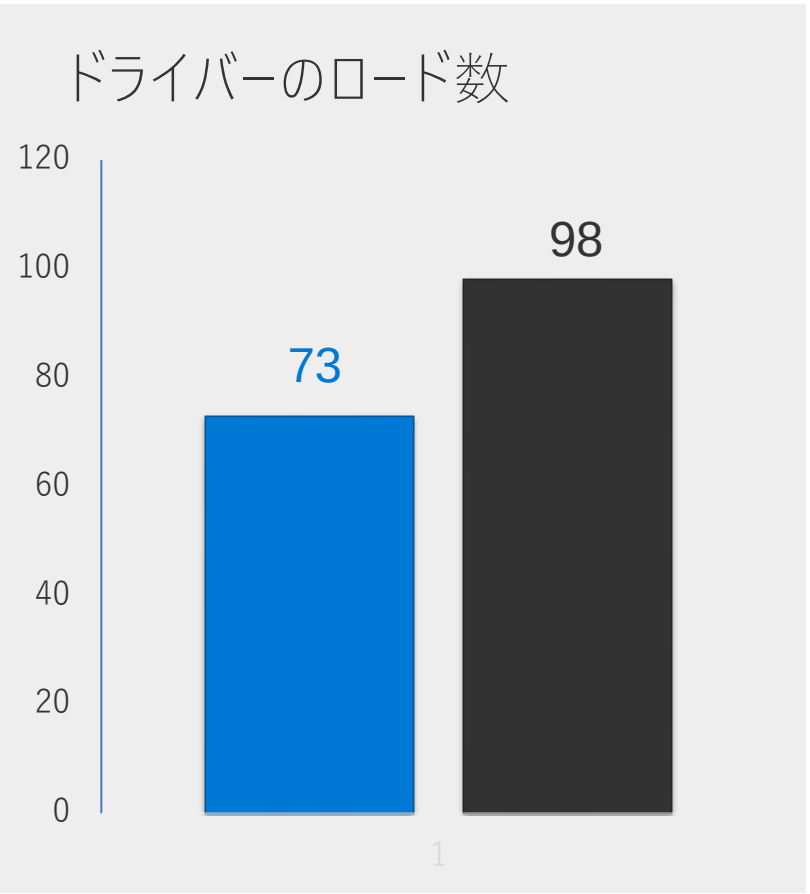
Nano Server

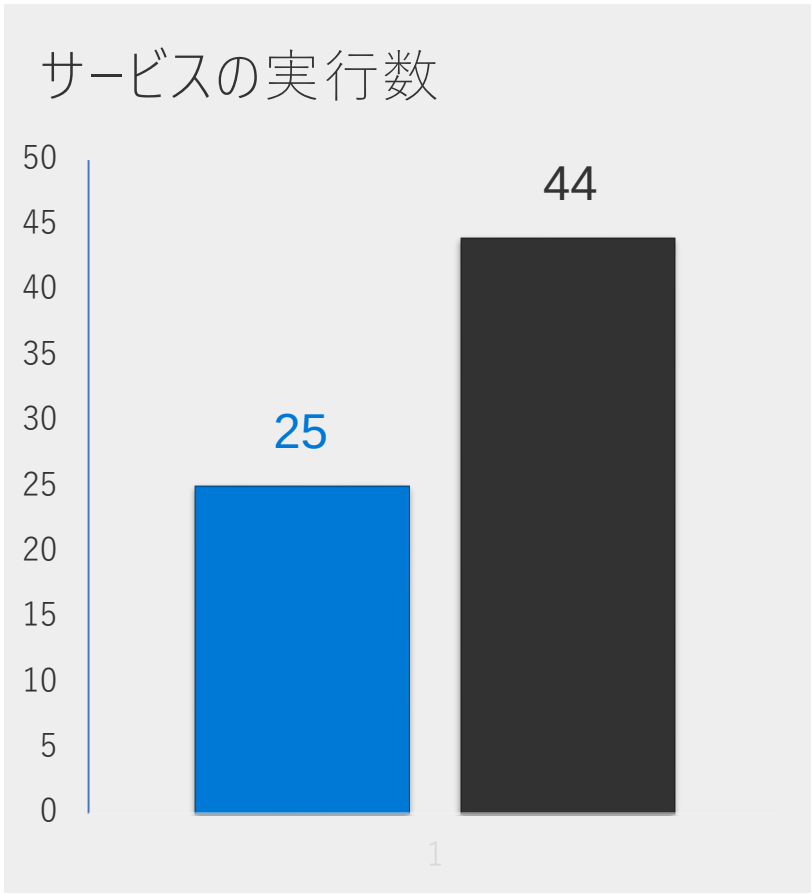
- 最小のフットプリントで動作する Windows Server 2016
- Windows Server をコアレベルからリファクタリング

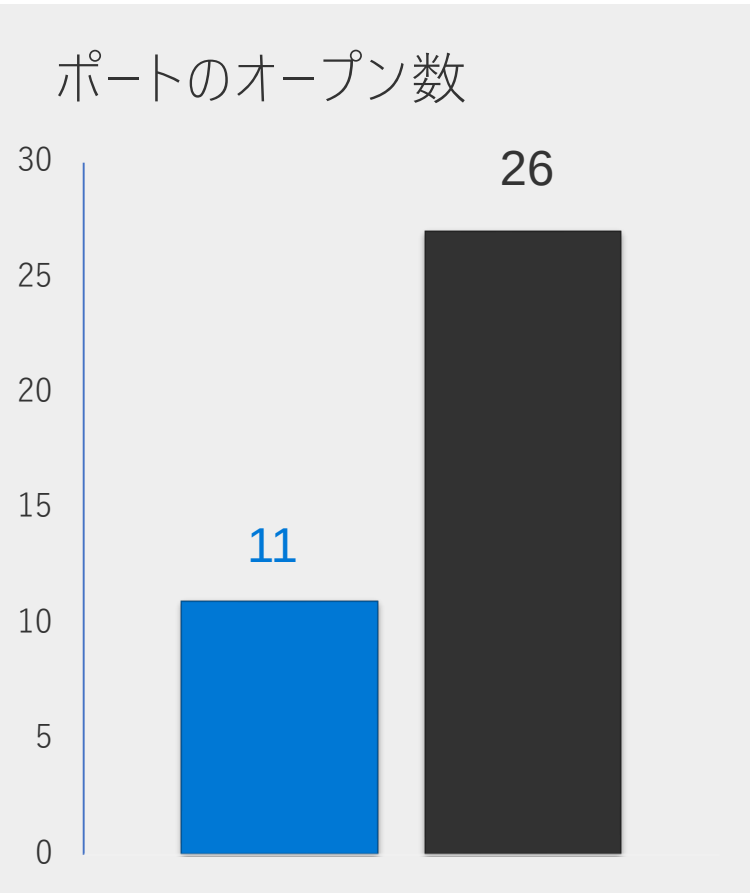
Nano Server に追加可能な役割または機能

・Hyper-V
・DNS Server
・Internet Information Services（IIS）
・ファイルサービスと記憶域サービス
・Windows コンテナ
・フェールオーバークラスタリング
・Windows Defender
・Desired State Configuration（DSC）
・System Center Virtual Machine Manager エージェント
・Network Performance Diagnostics Service
・データセンターブリッジング（DCB）

Nano Server のフットプリント ①

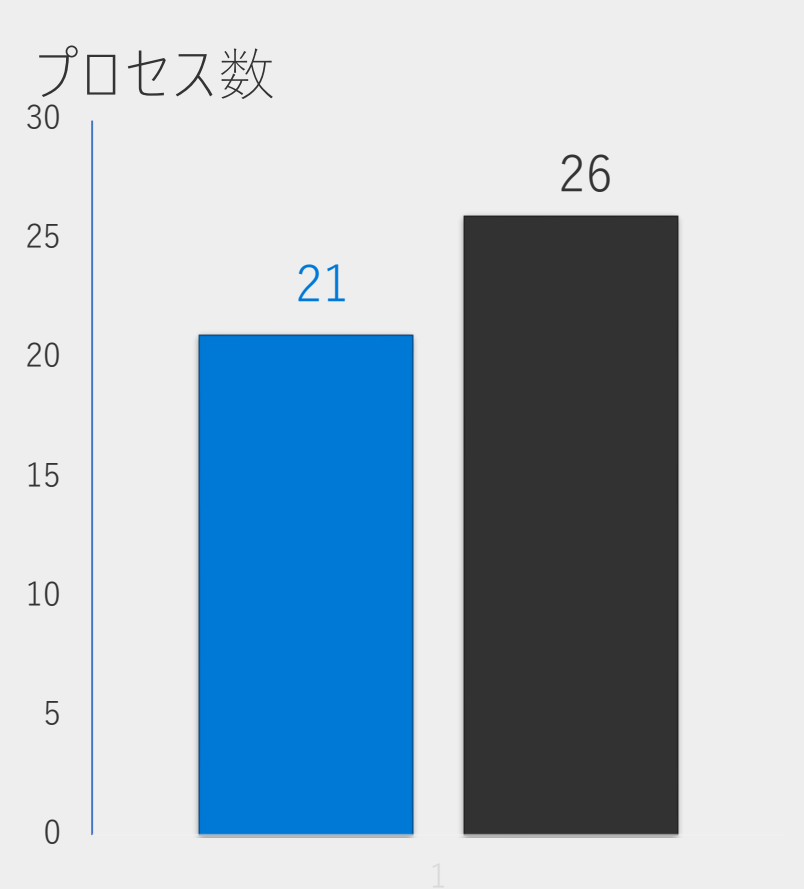


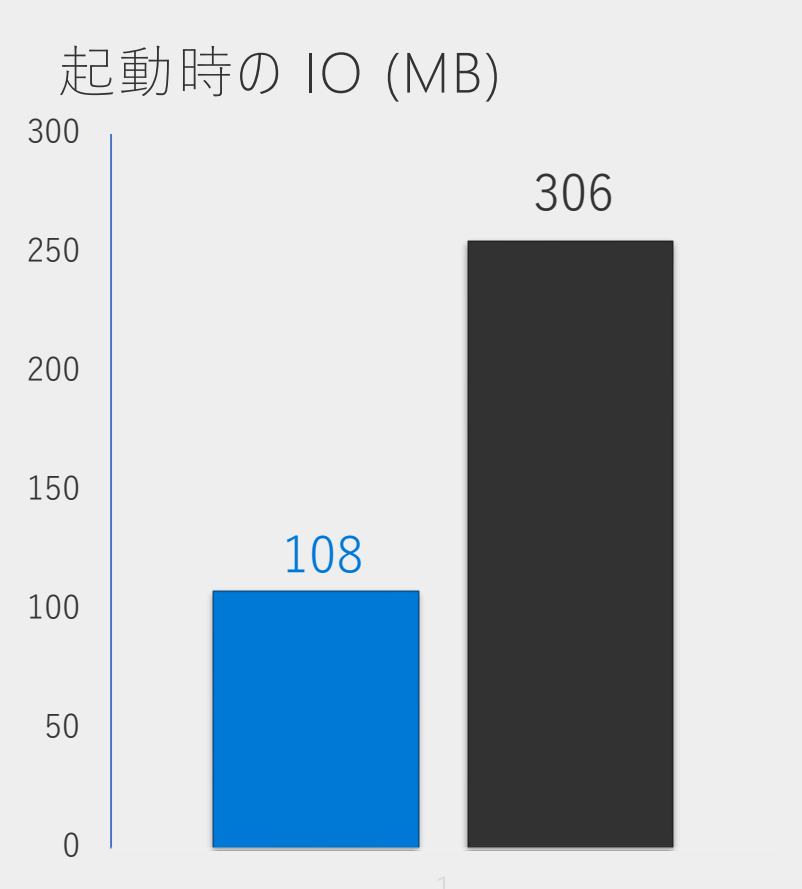


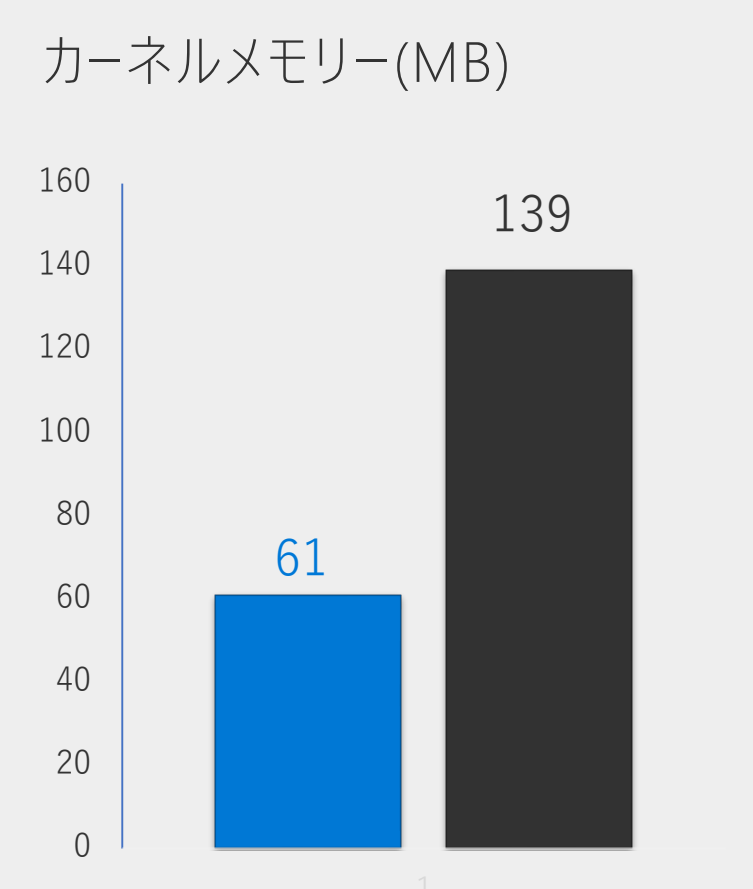


Nano Server　Server Core

Nano Server のフットプリント ②

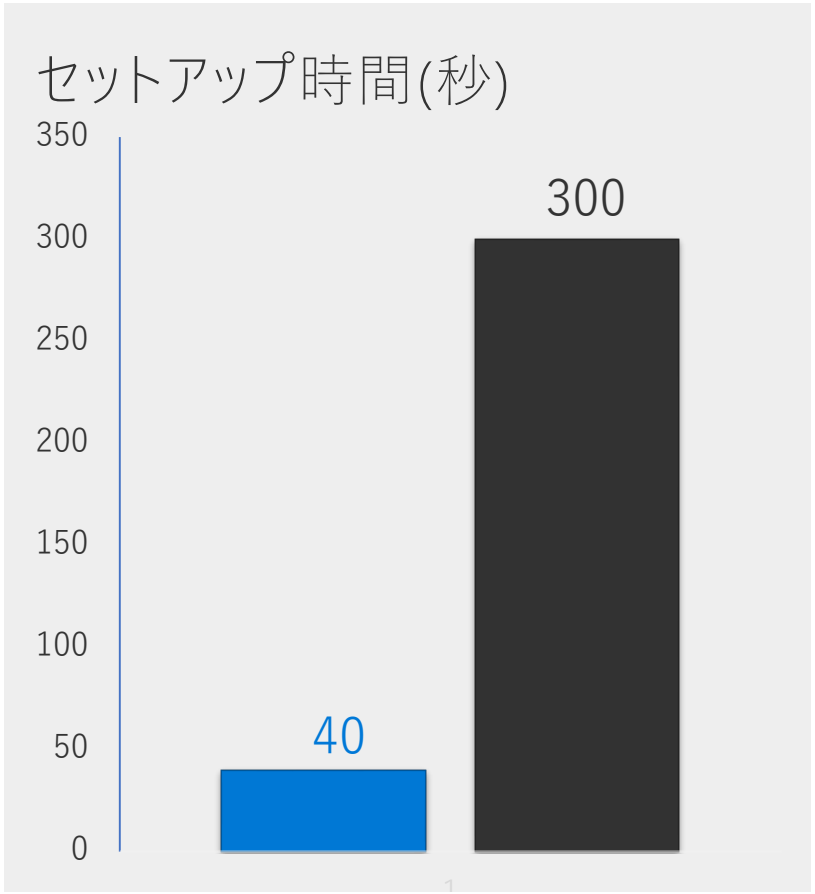


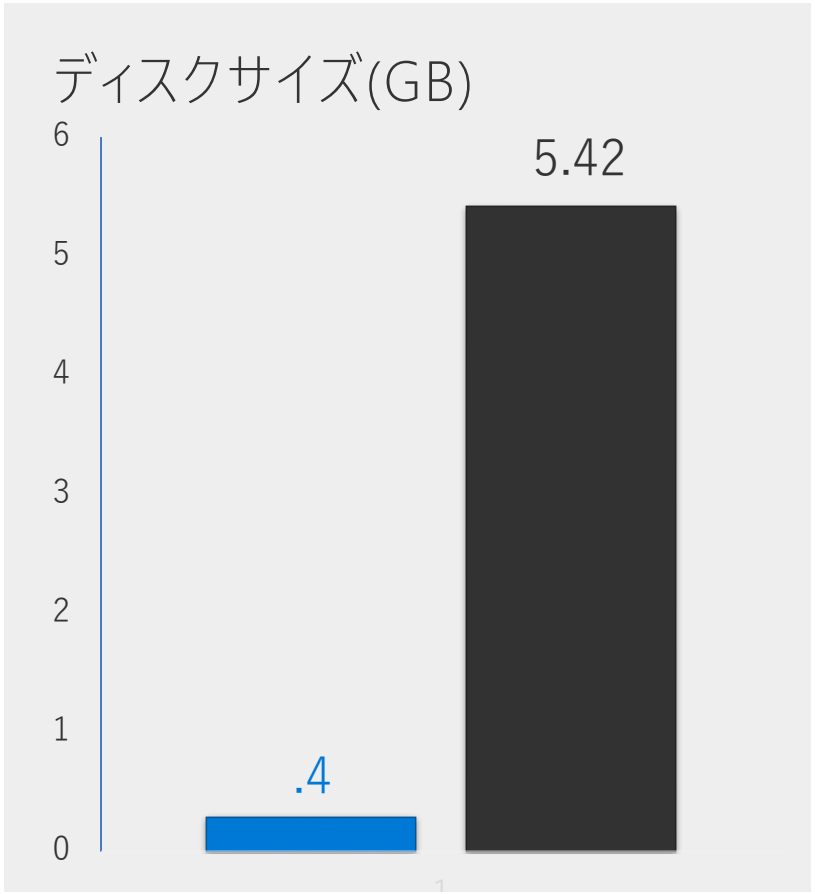


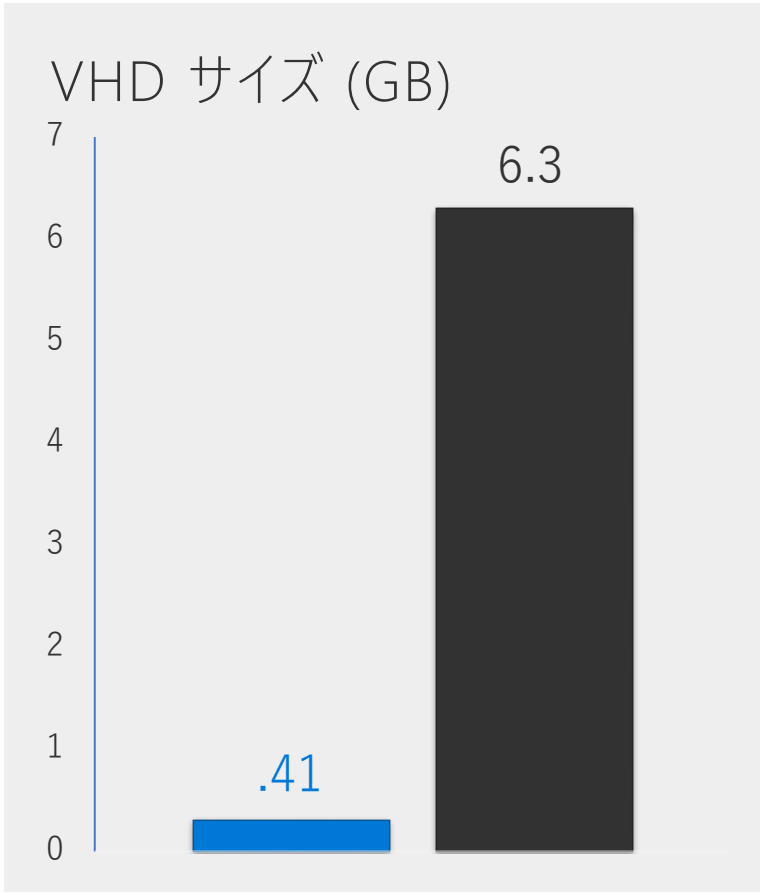


Nano Server　Server Core

Nano Server のフットプリント ③

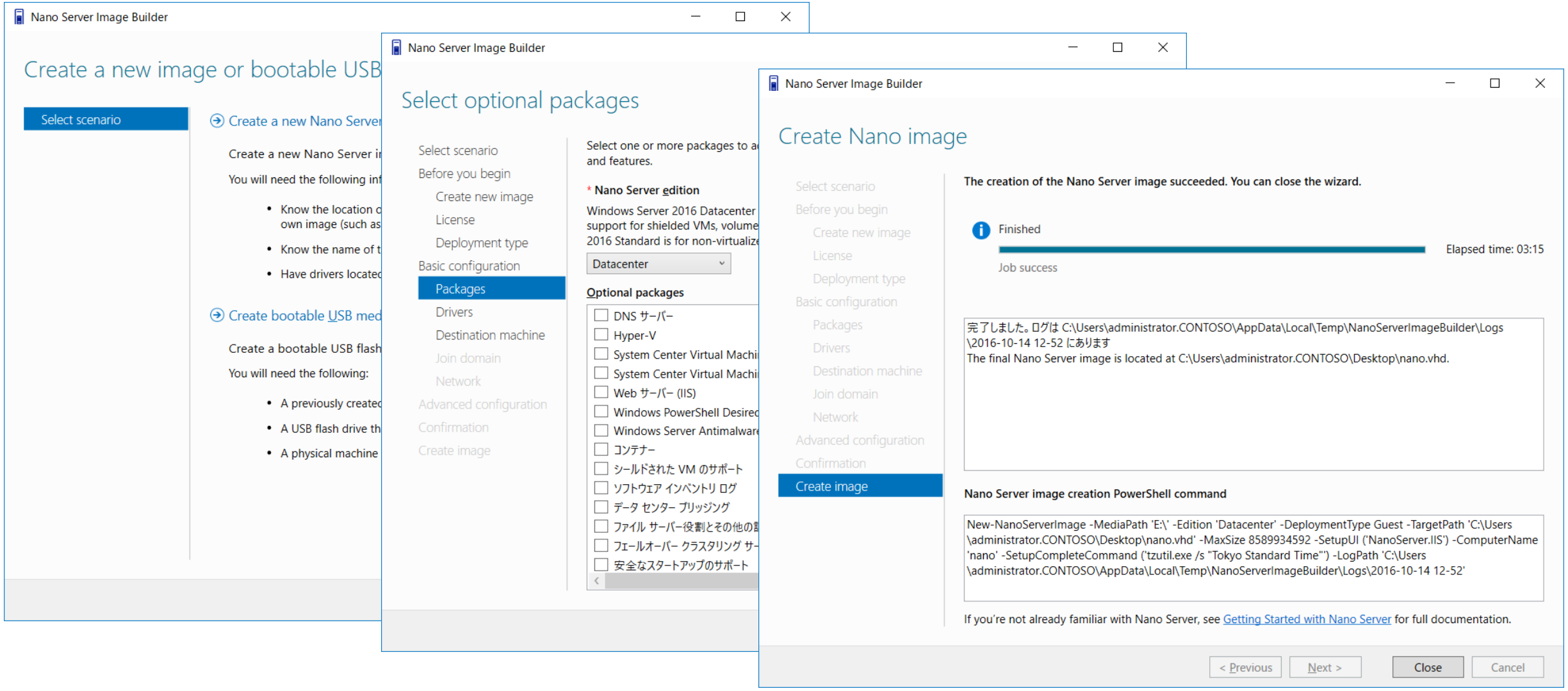






Nano Server　Server Core

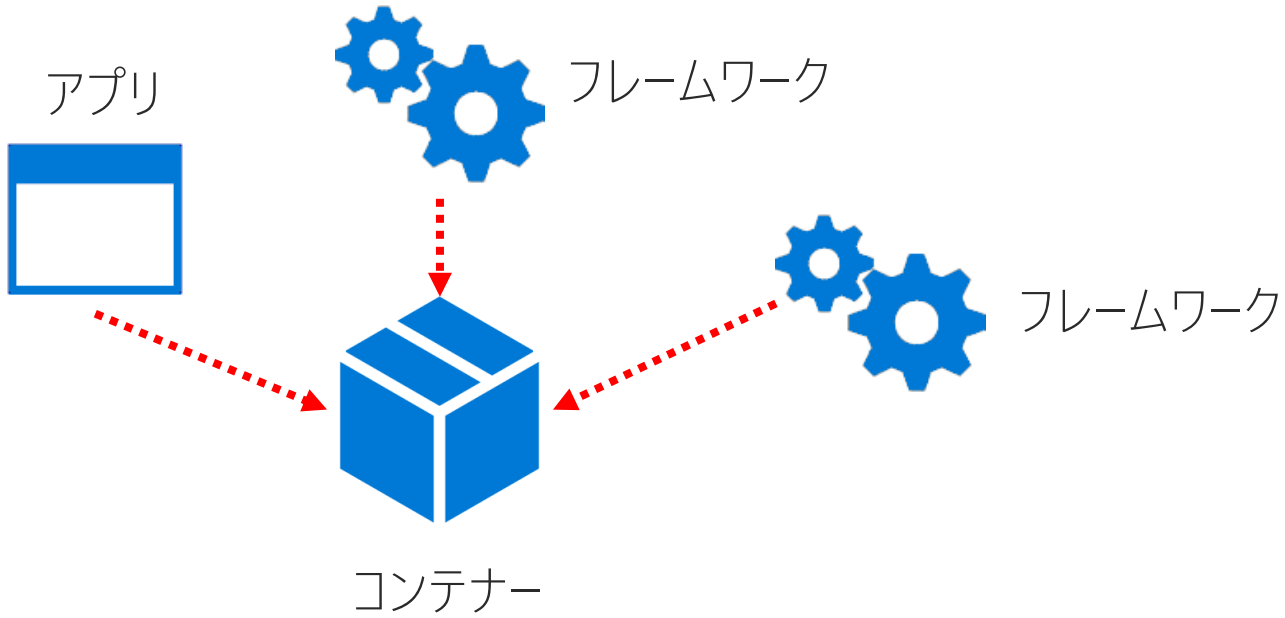
Nano Server Image Builder による仮想マシンの導入



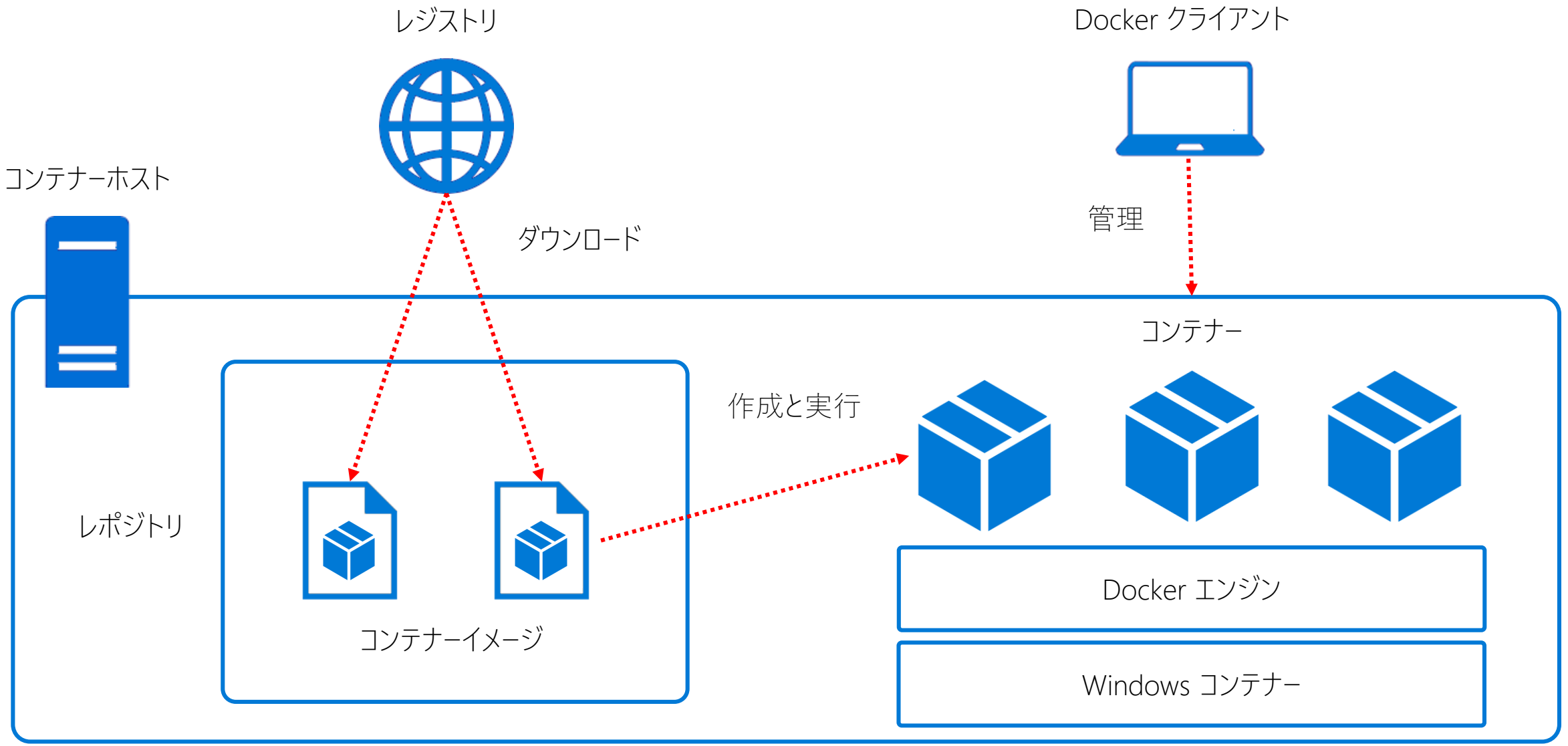
http://www.microsoft.com/en-us/download/details.aspx?id=54065

Windows コンテナー

- 新しいアプリケーションプラットフォーム
- コンテナーは「アプリの実行環境」を１つのパッケージにまとめたもの
  - コンテナー単位の展開や再展開が容易
  - コンテナー単位でリソースを分離して実行するため、リソースの競合を防ぐ
- Windows コンテナーは Docker の Windows Server への実装

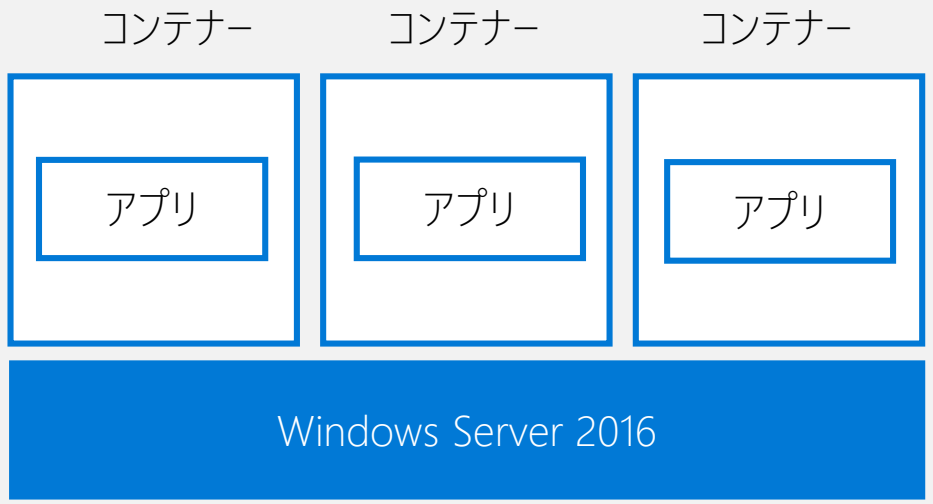


Windows コンテナーのアーキテクチャ



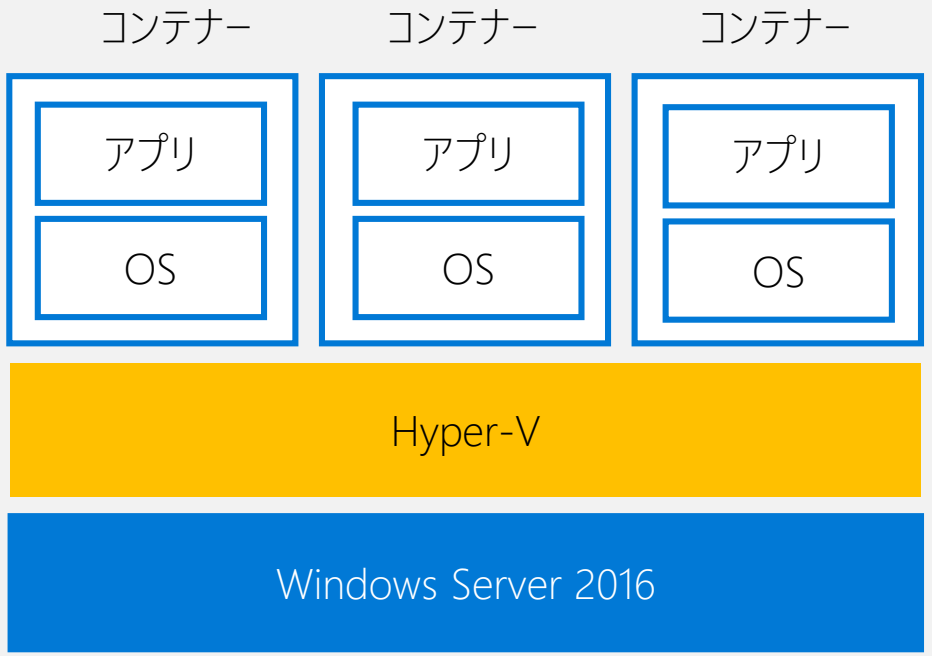
Windows コンテナーの実行環境

Windows Server コンテナー



ホストとすべてのコンテナーでカーネルを共有

Hyper-V コンテナー



コンテナーごとにカーネルを分離

Windows コンテナーの導入例

Install-Module -Name DockerMsftProvider -Repository PSGallery –Force

DockerMsftProvider プロバイダーのインストール

Install-Package -Name docker -ProviderName DockerMsftProvider

Docker パッケージのインストール

Restart-Computer -Force

［ DockerDefault からソフトウェアをアンインストールしますか？］ は
「インストールしますか？」の誤りです。Y を押します。

Windows Server コンテナーの操作例

Web サーバーコンテナーの作成

docker pull microsoft/windowsservercore　イメージのダウンロード

docker run --name winc -it microsoft/windowsservercore powershell　コンテナーの作成と実行

<コンテナ内操作
例 : Install-windowsfeature web-server などアプリのインストールが可能
<ctrl>+<p>と<ctrl>+<q> でコンテナを抜けることが可能>

dcoker stop winc　コンテナーの停止

docker commit winc customimage　カスタムイメージの作成

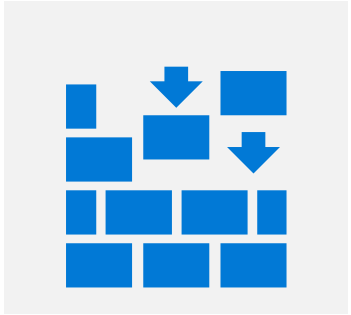
docker rm winc　コンテナーの削除

インテルによるコンピューティングの最適化

- Windows Server 2016 に最適化された インテル Xeon プロセッサー E5-2600 v4
- 幅広いアプリの効率化、パフォーマンス、俊敏性を強化

インテル Xeon プロセッサー E5-2600 v4

Intel Advanced Vector Extensions 2.0 (Intel AVX 2.0)



処理速度の向上を実現する
AVX の拡張セット

Intel Turbo Boost Technology 2.0

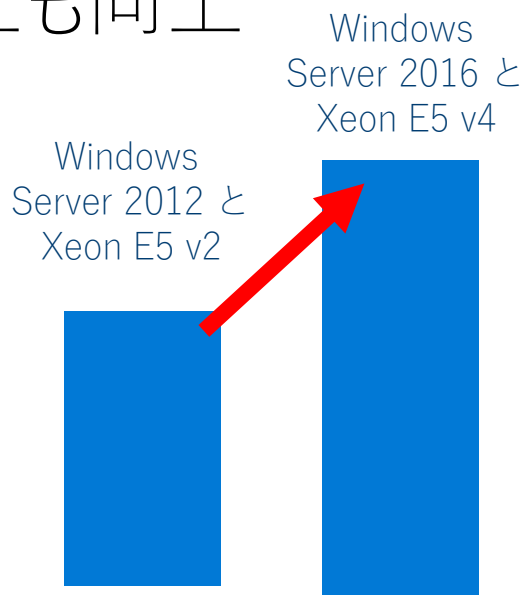
必要に応じて自動的に定格の動作周波数よりも
高速でプロセッサー・コアを動作させ、
より高いパフォーマンスを提供

Hardware P-States (HWP)

パワーセーブと積極的な
熱のコントロール

インテル Xeon プロセッサー E5-2699 v4 によるパフォーマンス

- SQL Server による複数トランザクションの並列処理
- 3 年前のサーバー機と比較した場合、SQL Server2016 とインテル Xeon プロセッサー E5-2699 v4 では、パフォーマンスが 54% 以上も向上
- インメモリテクノロジーに統合された
  エンタープライズクラスのプラットフォーム

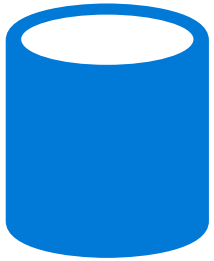


Software and workloads used in performance tests may have been optimized for performance only on Intel® microprocessors.
Performance tests, such as SYSmark* and MobileMark*, are measured using specific computer systems, components, software, operations, and functions. Any change to any of those factors may cause the results to vary. You should consult other information and performance tests to assist you in fully evaluating your contemplated purchases, including the performance of that product when combined with other products. For more complete information, visit www.intel.com/performance.

1. Up to 1.5x more transactions per second comparing Intel® Server with two Intel® Xeon® processor E5-2697 v2 and 256GB Memory (source: Intel® Technical Report #27) to an Intel® Server with two Intel® Xeon® processor E5-2699 v4 and 512GB Memory (Source: Intel® Technical Report #2372). Baseline configuration ran Microsoft SQL Server* 2012 EE, and Microsoft Windows Server* 2012 SE; the upgraded configuration ran Microsoft SQL Server* 2016 RTM and Microsoft Windows Server* 2016 Technical Preview 5.

Microsoft

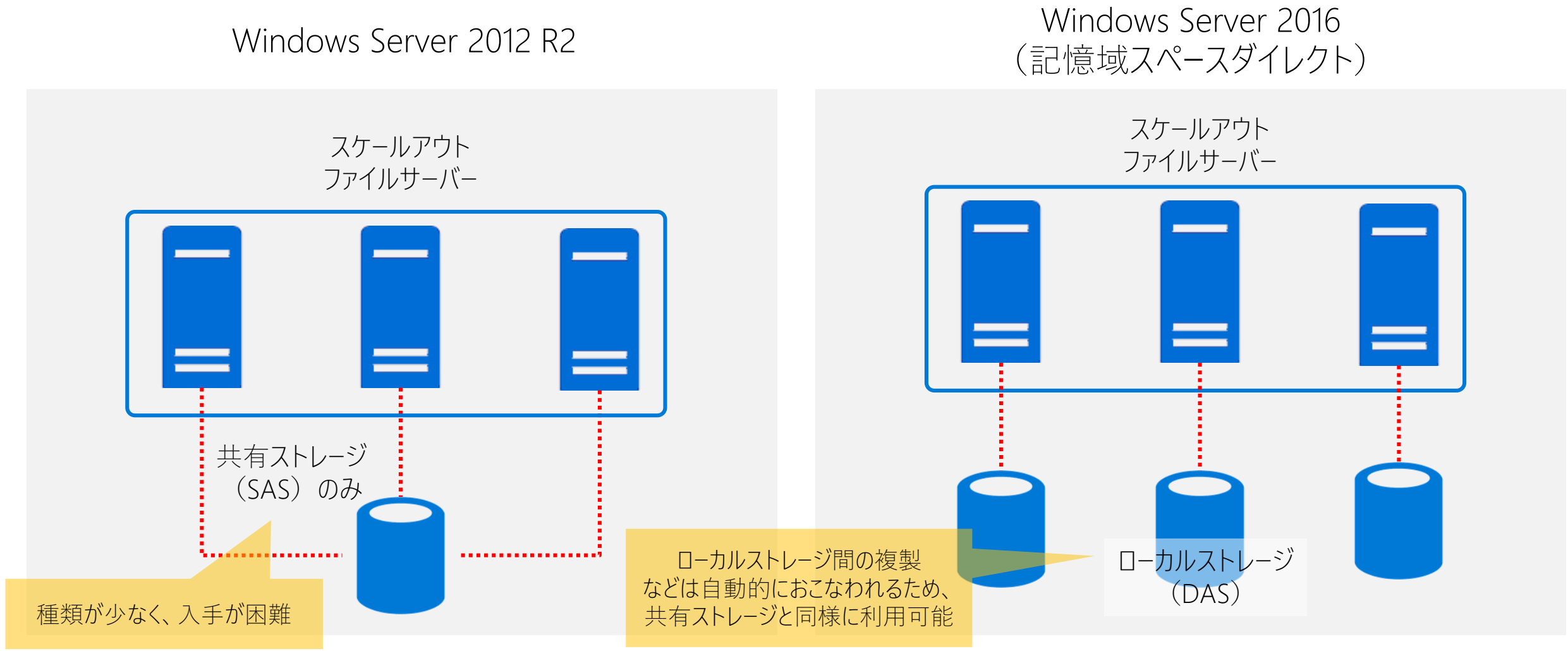
intel



ストレージ

記憶域スペースダイレクト（S2D）

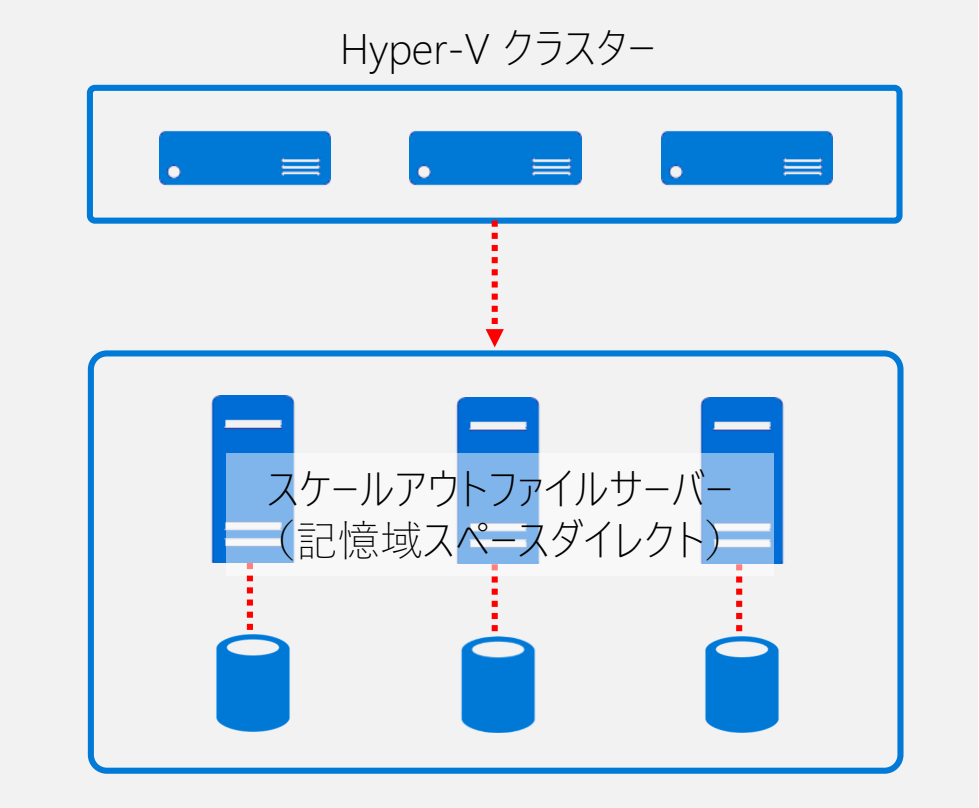
- スケールアウトファイルサーバーのディスクとしてローカルストレージが利用可能



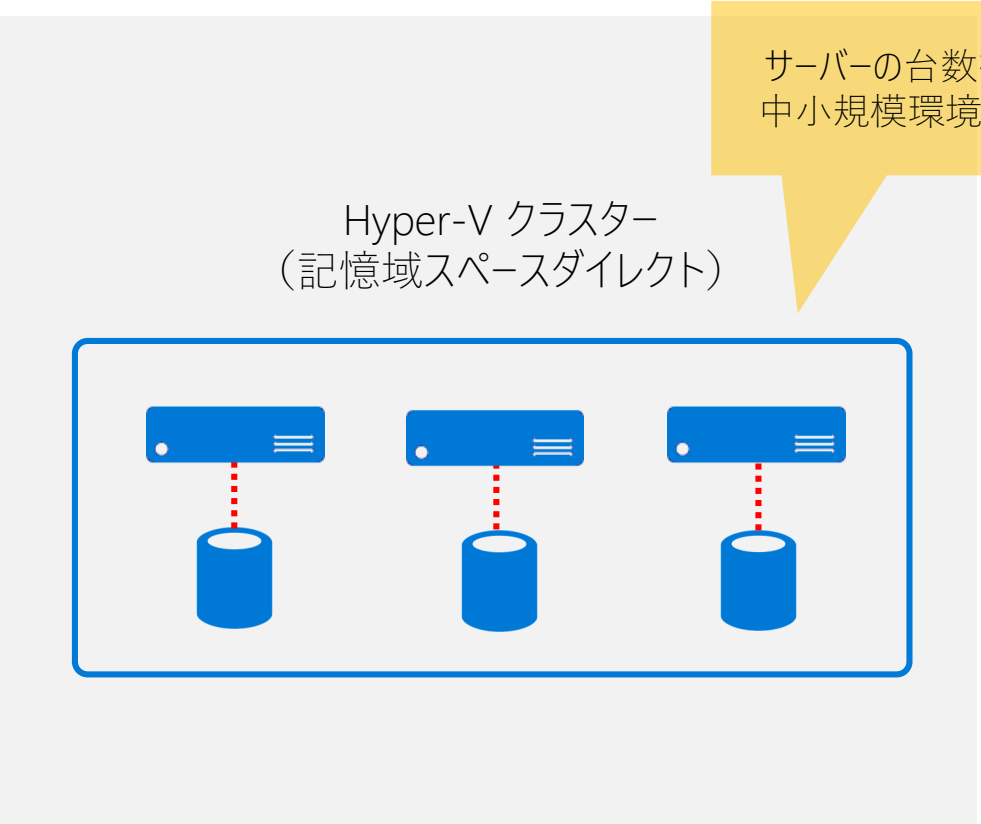
S2D による Hyper-converged シナリオ

- 同じサーバー内にコンピューティングとストレージを導入

Private Cloud Storage

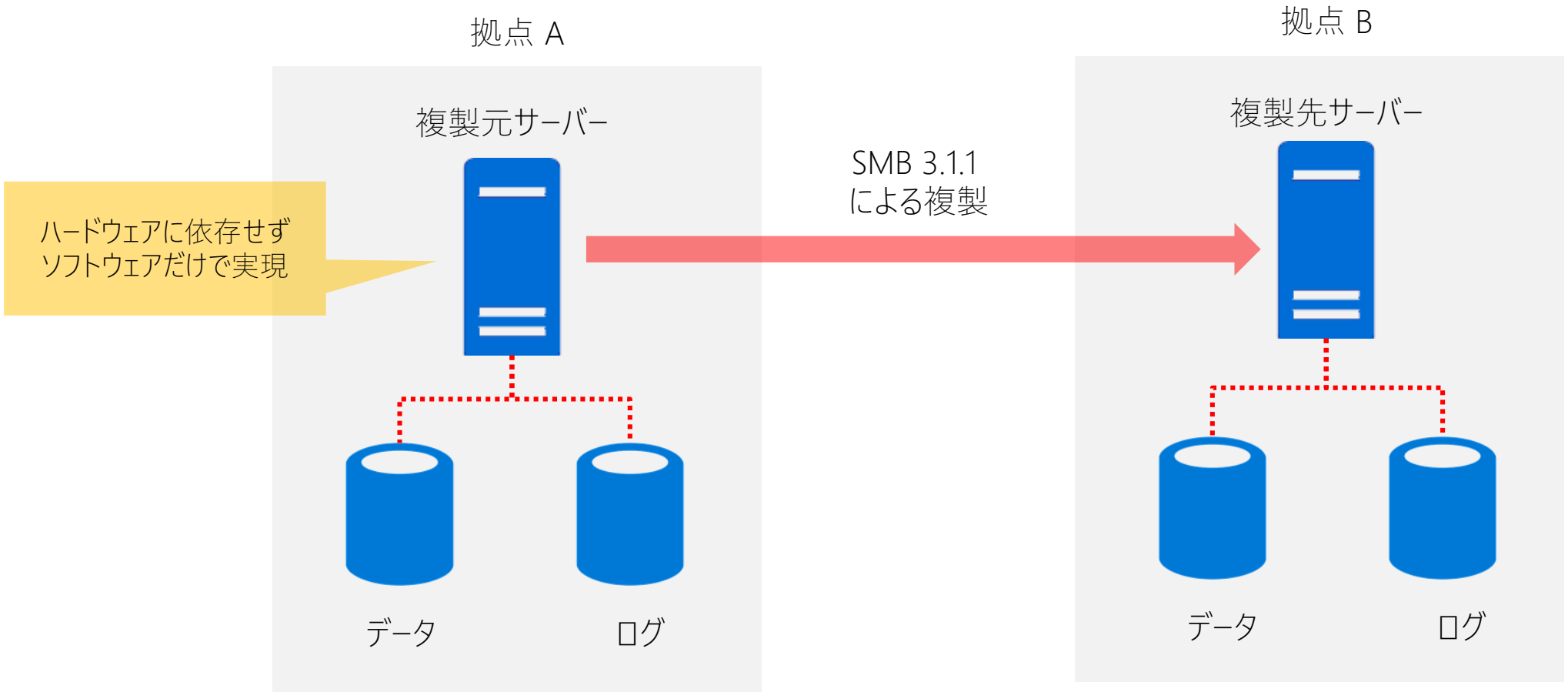


Hyper-converged



記憶域レプリカ

- ボリュームをブロックレベルで自動的にレプリケーション
- サーバー間やクラスター間で利用可能



記憶域レプリカの設定例

Install-WindowsFeature -Name Storage-Replica –IncludeManagementTools
Restart-Computer

記憶域レプリカのインストール

Test-SRTopology -SourceComputerName filesv01 -SourceVolumeName D: -SourceLogVolumeName E: `
-DestinationComputerName filesv02 -DestinationVolumeName D: -DestinationLogVolumeName E: `
-DurationInMinutes 5 -ResultPath C:¥Temp

レプリケーションのテスト

New-SRPartnership -SourceComputerName filesv01 -SourceRGName RG01 -SourceVolumeName D: `
-SourceLogVolumeName E: -DestinationComputerName filesv02 -DestinationRGName RG02 -DestinationVolumeName D: `
-DestinationLogVolumeName E: -LogSizeInBytes 8GB

レプリケーションの設定

Get-SRGroup

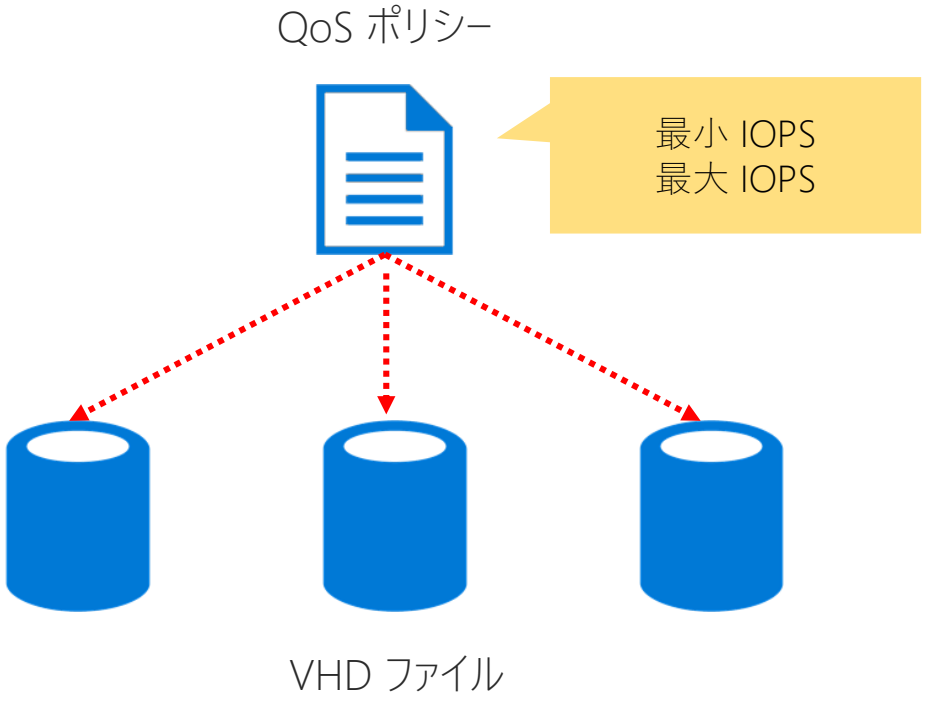
レプリケーションの状態の表示

Set-SRPartnership -NewSourceComputerName filesv02 -SourceRGName RG02 `
-DestinationComputerName filesv01 -DestinationRGName RG01

レプリケーションの反転

記憶域 QoS

- スケールアウトファイルサーバーに格納された Hyper-V 仮想マシンの VHD ファイルに対して、最小と最大 IOPS を指定することで IO を制御
- ポリシーによる一元管理



記憶域 QoS の設定例

```
$Session = New-CimSession -Credential  contoso¥administrator -ComputerName HOST01

New-StorageQosPolicy -Name bronze -Minimumlops 50 `
-Maximumlops 150 -PolicyType Aggregated -CimSession $Session
```

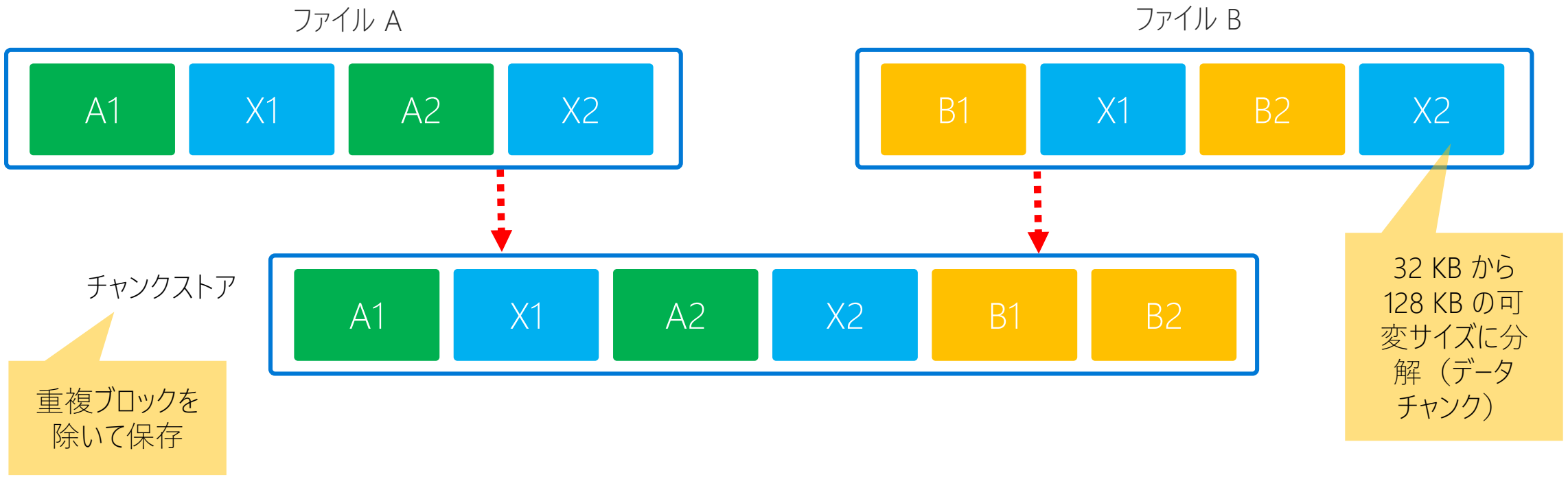
QoS ポリシーの作成

```
Get-VM -Name VM01 –ComputerName HOST01 |  Get-VMHardDiskDrive | `
Set-VMHardDiskDrive -QoSPolicyID (Get-StorageQosPolicy `Name Bronze -CimSession $Session).PolicyId
```

QoS ポリシーの割り当て

重複除去

- ファイル内の重複データをまとめることで、記憶域の利用効率を向上
- 64 TB の大容量ボリューム、1 TB の大容量ファイルに対応
- 仮想バックアップサーバー用アルゴリズムの追加
- Nano Server のサポート



ReFS

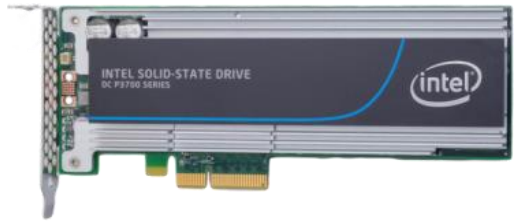
バージョン 3.0 となった新しいファイルシステム

機能	NTFS	ReFS
ボリュームからのブート	○	×
リムーバブルデバイスでの利用	○	×
ボリュームの検査と修復	手動（chkdsk）	自動
修復中ボリュームへのアクセス	×	○
ACL によるアクセス制限	○	○
BitLocker によるボリューム暗号化	○	○
ボリュームのクォータ制限	○	×
ボリュームの重複除去	○	×
ファイル単位の圧縮、暗号化	○	○

インテルによるストレージの最適化

- PCIe 対応 インテル SSD データセンター・ファミリー
- 記憶域スペース（記憶域スペースダイレクト）の利用に最適

PCIe 対応 インテル SSD
データセンター・ファミリー



圧倒的なパフォーマンス

6 Gbps SAS/SATA SSD に比べ、
最大で 6 倍速いデータ転送

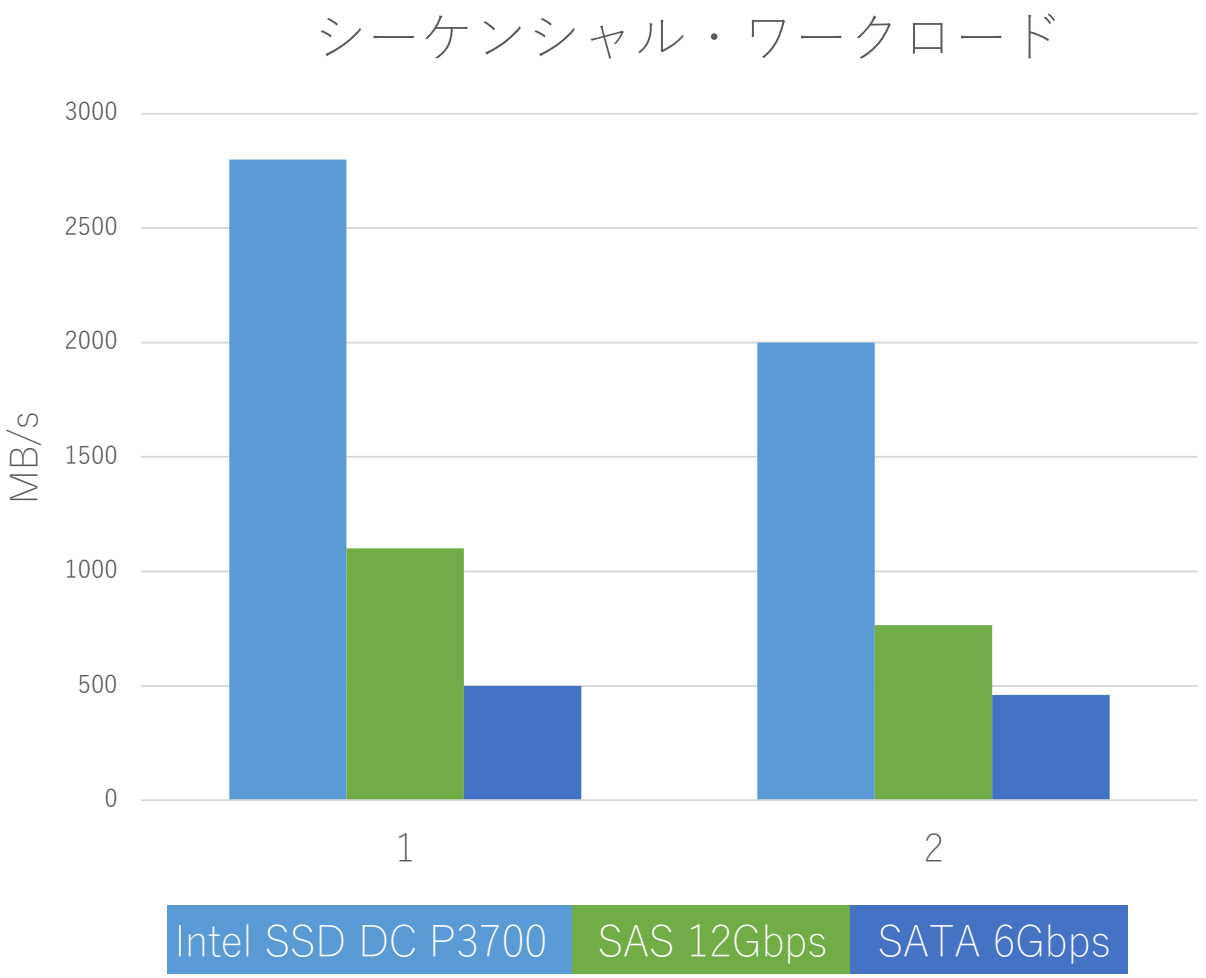
NVMe による
最新のデータセンターストレージ

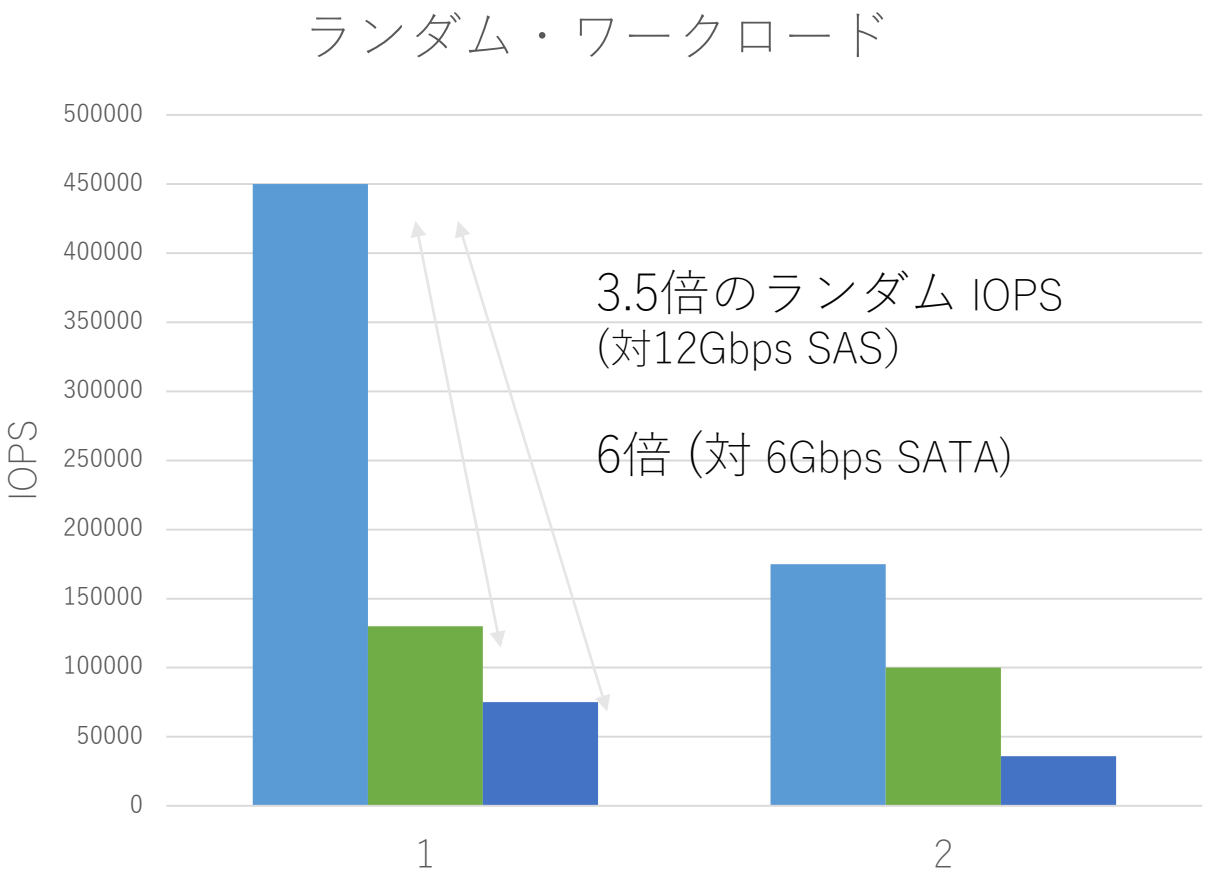
新しい Non-Volatile Memory Express（NVMe）は
SAS/SATA SSD の性能面での制約を解消

定評のある品質と信頼性

厳しい認定テストおよび互換性テスト
による非常に高い信頼性

NVMe による性能向上





Results measured by Intel based on the following configurations. Tests document performance of components on a particular test, in specific systems. Differences in hardware, software, or configuration will affect actual performance. Configurations: Performance claims obtained from data sheet, sequential read/write at 128k block size for NVMe and SATA, 64k for SAS. Intel SSD C P3700 Series 2TB, SAS Ultrastar® SSD1600MM, Intel SSD DC S3700 Series SATA 6Gbps. Intel Core i7-3770K CPU @ 3.50GHz, 8GB of system memory, Windows* Server 2012, IOMeter. Random performance is collected with 4 workers each with 32 QD

IOPs パフォーマンスシナリオ（Hybrid NVMe+HDD ）

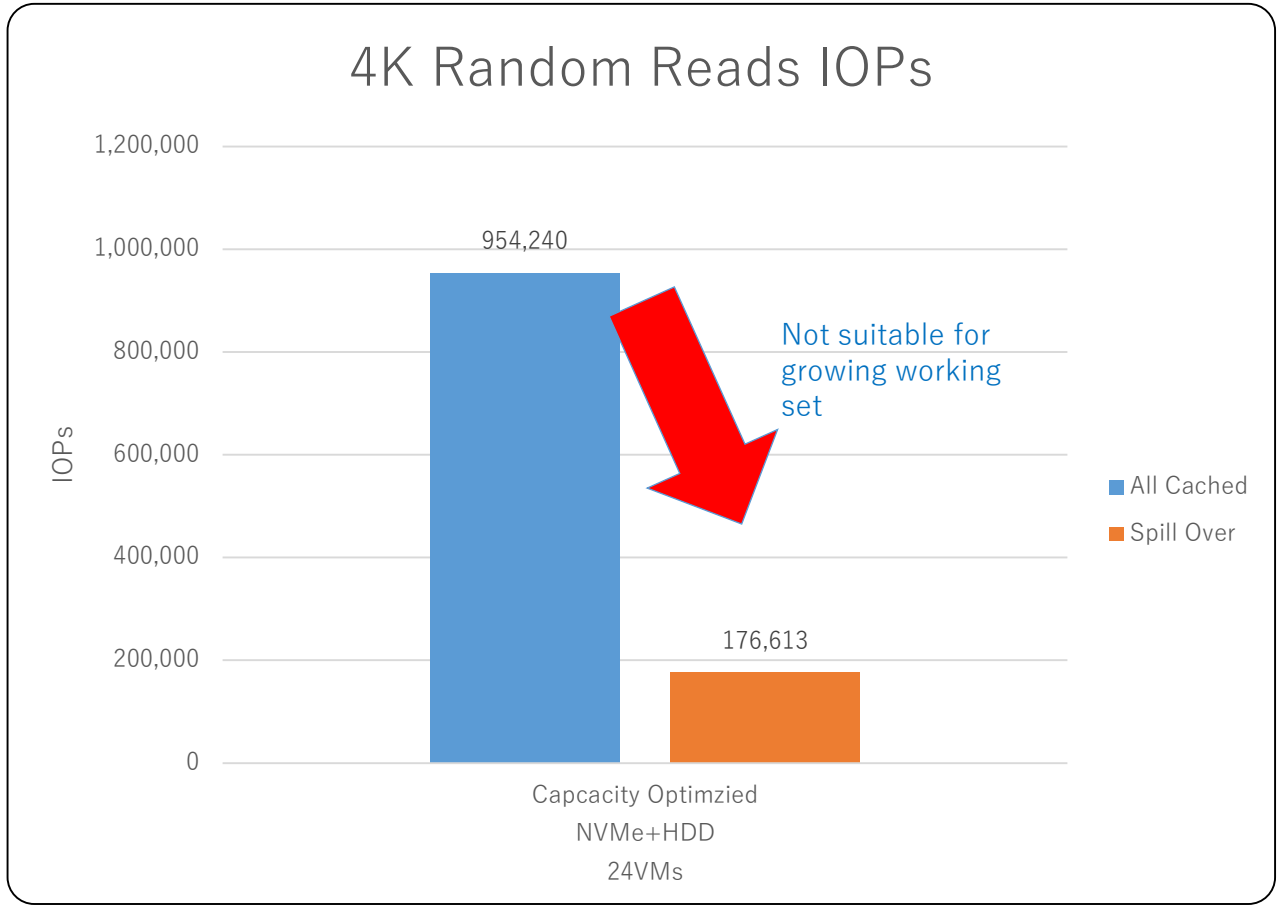
Workloads: Exchange, SharePoint, Data Warehouse

Processor:
2x Intel® Xeon® processor E5-2650 v4 (30M Cache, 2.2GHz, 12 cores, 105W)

Storage:
Cache Tier: 2x 2TB Intel® SSD DC P3700 Series
Capacity Tier: 8x 6TB 3.5” HDD Seagate* ST6000NM0024

Network:
1 x 10GbE dual-port Chelsio* T520 adapter
1 x 10GbE Extreme Networks Summit* X670-48x switch

VMs:
24x Azure-like VMs per node (2x12Core CPU =24cores=24VMs)
60GB OS VHD + 500 GB Data VHD per VM [53.76 TB total space used from the shares]
Spill over: 4*98GB Diskspd files per VM
Cached in: 2*10GB Diskspd files per VM

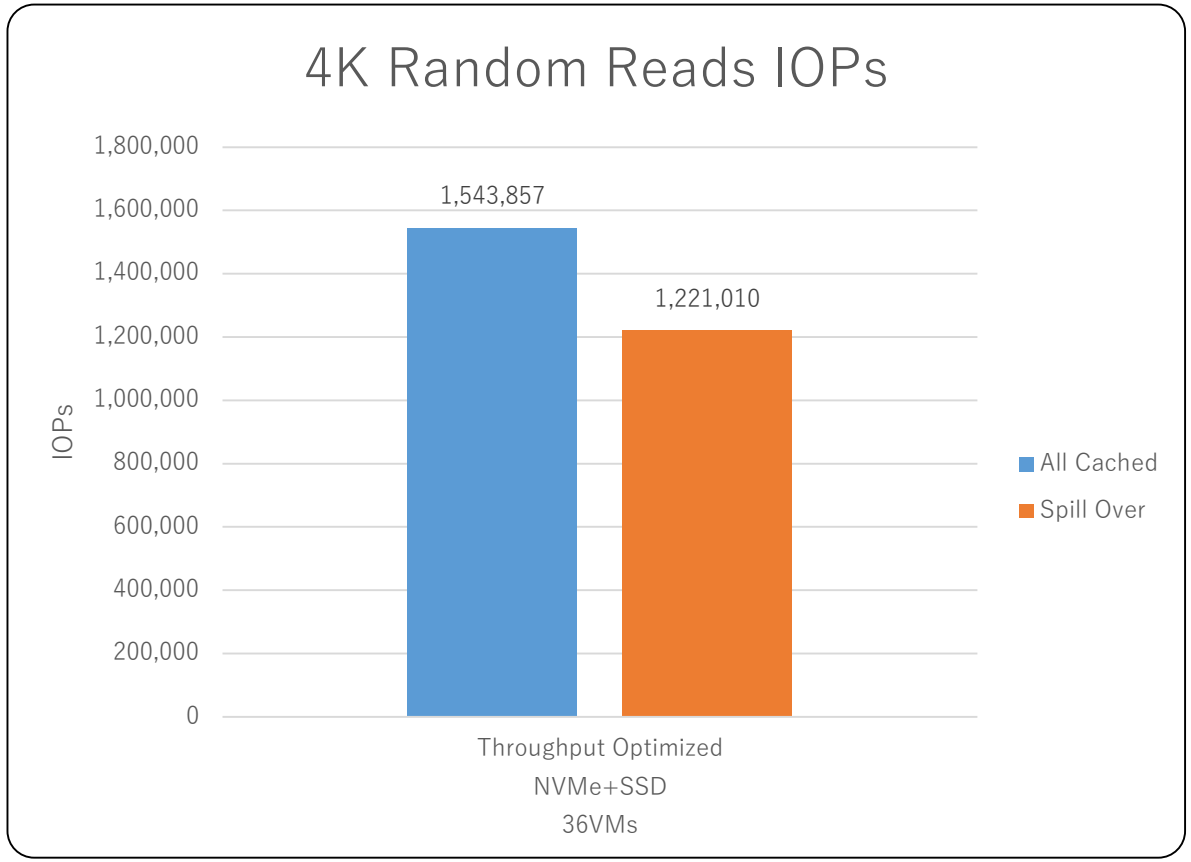


IOPs パフォーマンスシナリオ（All Flash NVMe+SATA)

Workloads: OLTP, VDI, IaaS, Data Warehouse

Processor:
2x Intel® Xeon® processor E5-2695 v4 (45M Cache, 2.10GHz, 18 cores, 120W)
Storage:
Cache Tier: 4x 2TB Intel® SSD DC P3700 Series (NVMe)
Capacity Tier: 20x 1.6TB Intel® SSD DC S3610 Series (SATA)
Network:
1 x 10GbE dual-port Chelsio* T520 adapter
1x 10 GbE Extreme Networks Summit* X670-48x switch

VMs:
36x Azure-like VMs per node (2x18Core CPU=36 cores = 36VMs)
60 GB OS VHD + 150 GB Data VHD per VM [30.24 TB total space used from the shares]
Spill over: 2*70GB Diskspd files per VM
Cached in: 1*70GB Diskspd files per VM

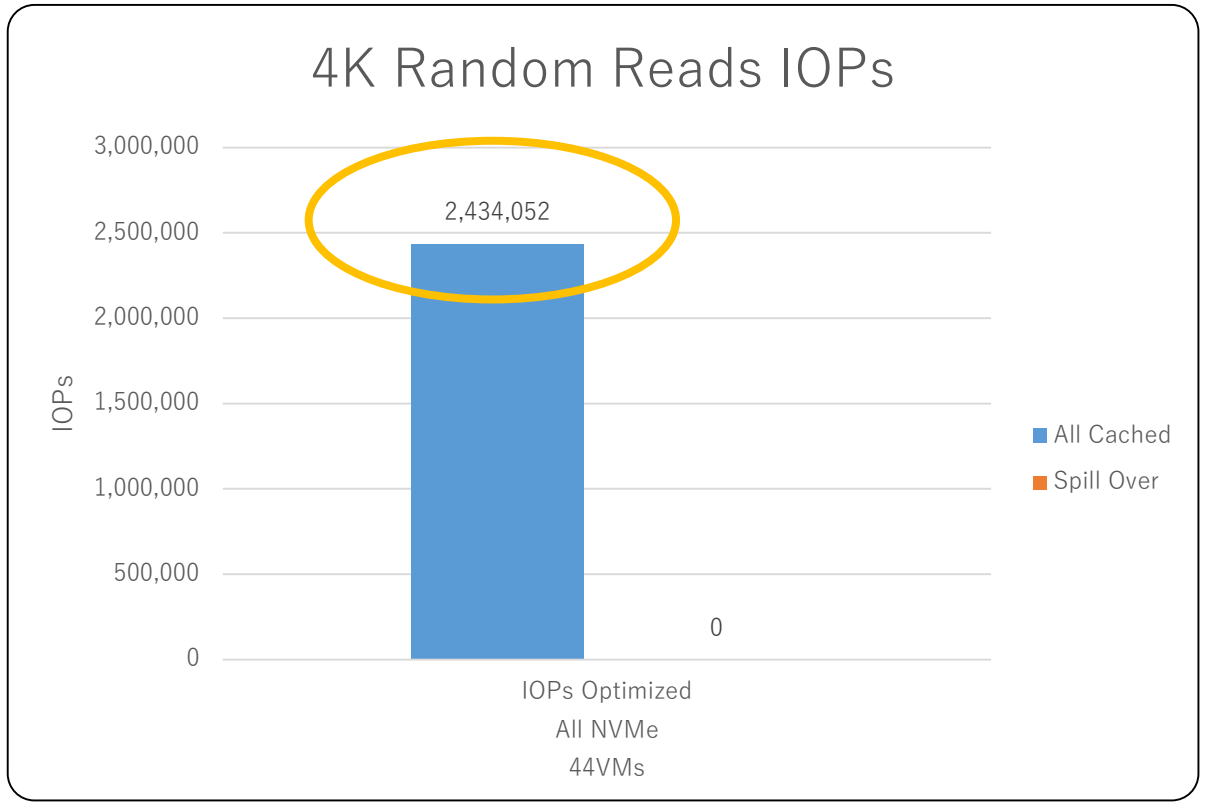


IOPs パォーマンスシナリオ(All NVMe)

Workloads: OLTP, VDI, IaaS

Processor: Intel® Xeon® processor E5-2600 v4 Family
DRAM: DDR4 - 16GBx24=384GB (Min);
32GBx24=768GB (Max)
Cache Storage: Low-latency, high-endurance SSD, 2xPCIe Intel® SSD DC P3700: 800GB x2=1.6TB
Capacity Storage: Standard-endurance SSDs, 6-8x Intel® SSD DC P3520: 2TBx 8=12-16TB
NIC: 2x40GbE RDMA NIC
Switch: 40GbE switch

VMs:
44x Azure-like VMs per node (2x22Core CPU=44 cores = 36VMs)
60 GB OS VHD + 150 GB Data VHD per VM [30.24 TB total space used from the shares]
Spill over: 2*70GB Diskspd files per VM
Cached in: 1*70GB Diskspd files per VM



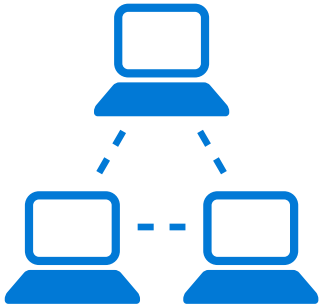
http://www.dataonstorage.com/news-release/51-dtaon-news/342-dataon-introduces-hyper-converged-clusterblock-architecture-for-windows-server-2016-and-shatters-performance-record-with-24m-iops-on-intels-3d-nand-ssds-at-idf-2016.html

（まとめ）IOPs パフォーマンスシナリオ

Features	Value – Windows Server Software-Defined (Hybrid)	Mainstream – Windows Server Software-Defined (All-Flash, Compute Dense)	Mainstream – Windows Server Software-Defined (All-NVMe)
Configuration Type		Hyper-converged	
Focus	Capacity Optimized	Throughput/Capacity Optimized	I/O Optimized
Workloads	Exchange, Sharepoint, Data Warehouse	OLTP, VDI, IaaS, Data Warehouse	OLTP, VDI, IaaS
Platform	2U 1Node	2U 1Node or 2U 4Node	1U 1Node or 2U 1Node
CPU	Intel® Xeon® processor E5-2650 v4 12 cores	Intel Xeon processor E5-2695 v4 18 cores	Intel Xeon processor E5-2699 v4 22 cores
Memory	DDR4 -16GBx16=256GB	DDR4 -16GBx24=384GB (Min); 32GBx24=768GB (Max)	
Network Controller	2x10Gb NIC - RDMA optional	2x40Gb RDMA NIC (iWARP Preferred)	
Network Switch	10 GbE switch	40 GbE switch	
Storage Cache (5-10% of total capacity)	Intel® SSD DC P3700 or S3700: 1.6TB	Intel SSD DC P3700: 800GB or 3D XPoint when avail.	Intel SSD DC P3700: 800GB or 3D XPoint when avail.
Storage Media	HDD 3.5”: 6TB+	SATA Intel® SSD DC S3610: 1.6TB	Intel SSD DC P3520/DC P3500: 2TB

Microsoft

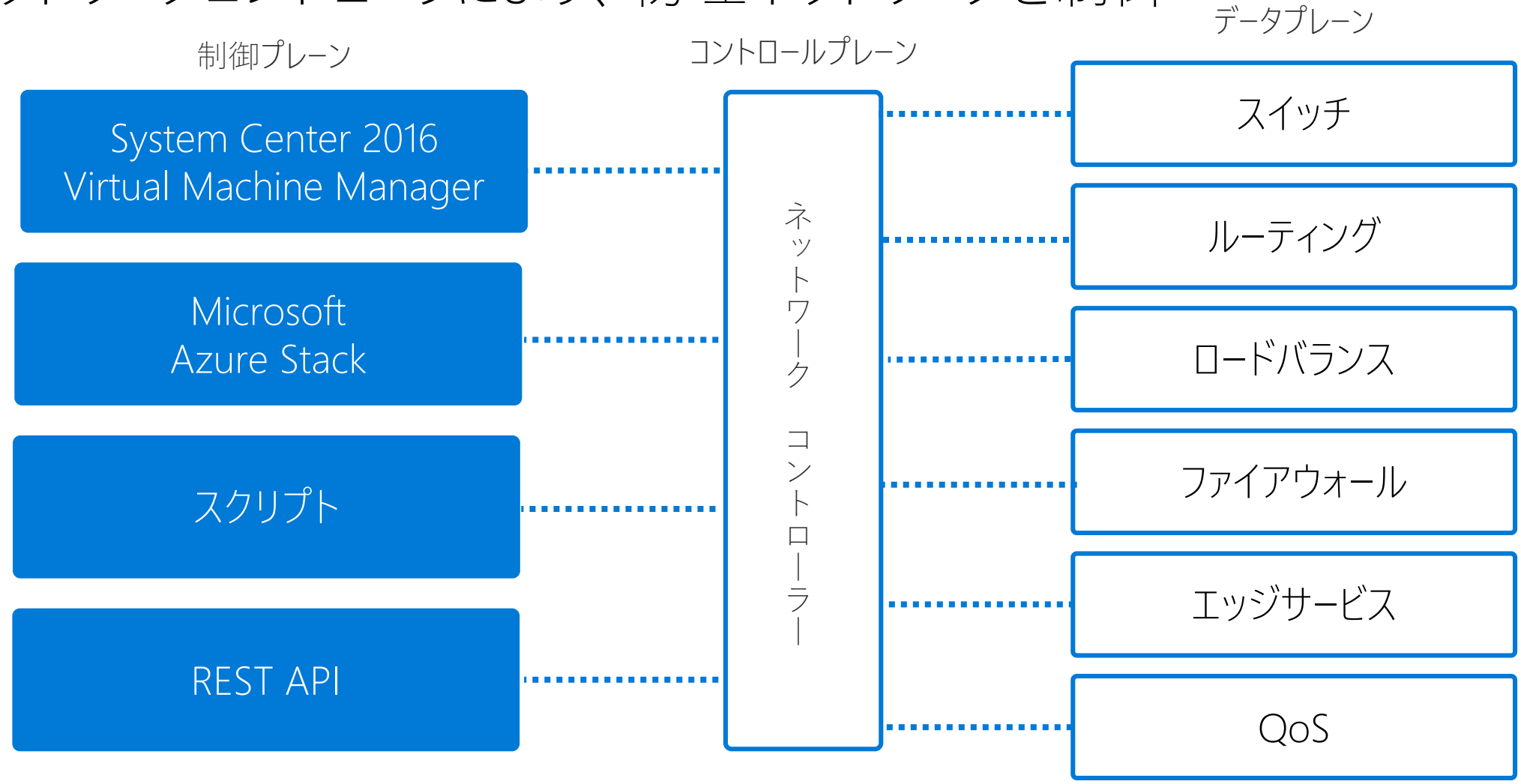
intel



ネットワーク

Windows Server 2016 の SDN 機能

- ネットワークコントローラにより、物理ネットワークを制御



SDN の主要コンポーネント

ネットワーク コントローラー

- ネットワークインフラの制御と集中管理

ソフトウェア ロードバランサー

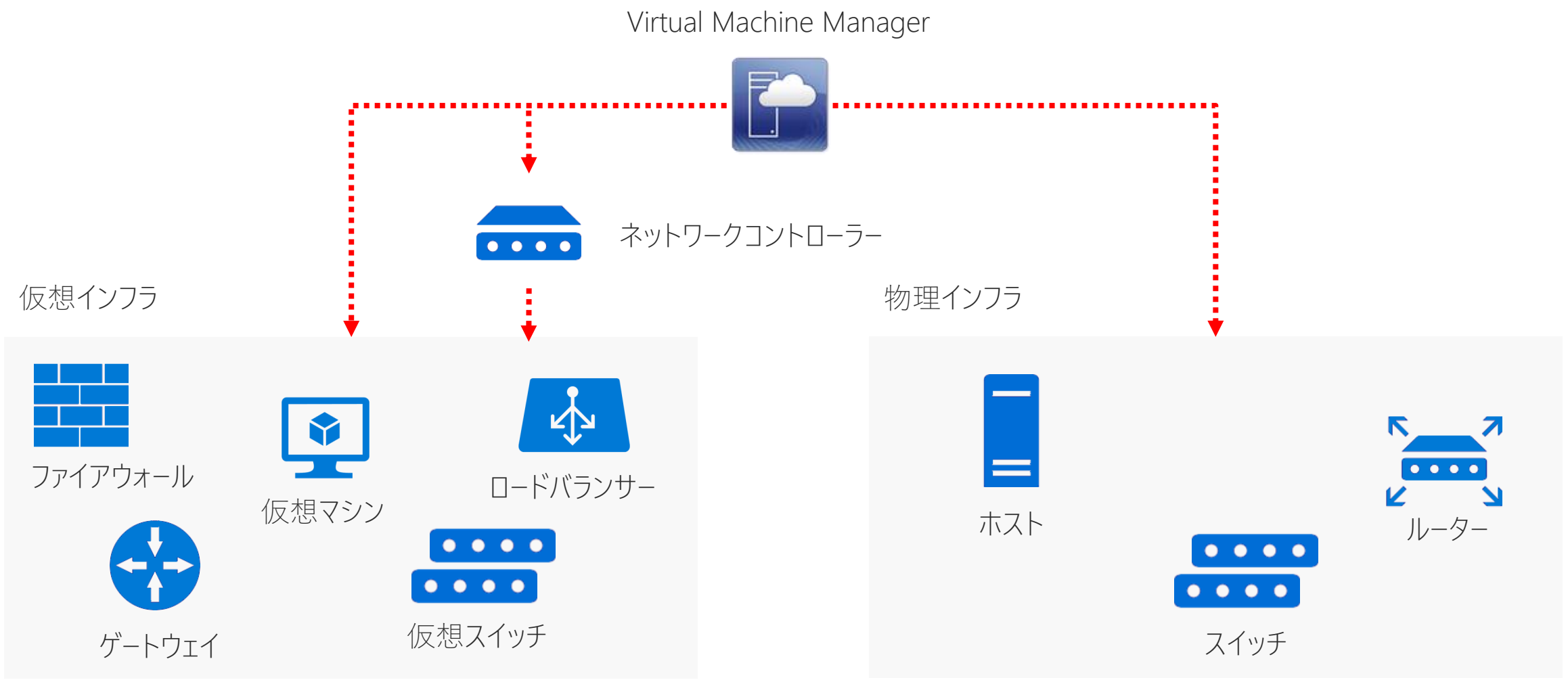
- トラフィックを負荷分散することで可用性と拡張性を向上
- 高価なハードウェアロードバランサーの代替え

ゲートウェイ

- 外部、またはインターネットに接続するエッジサーバー

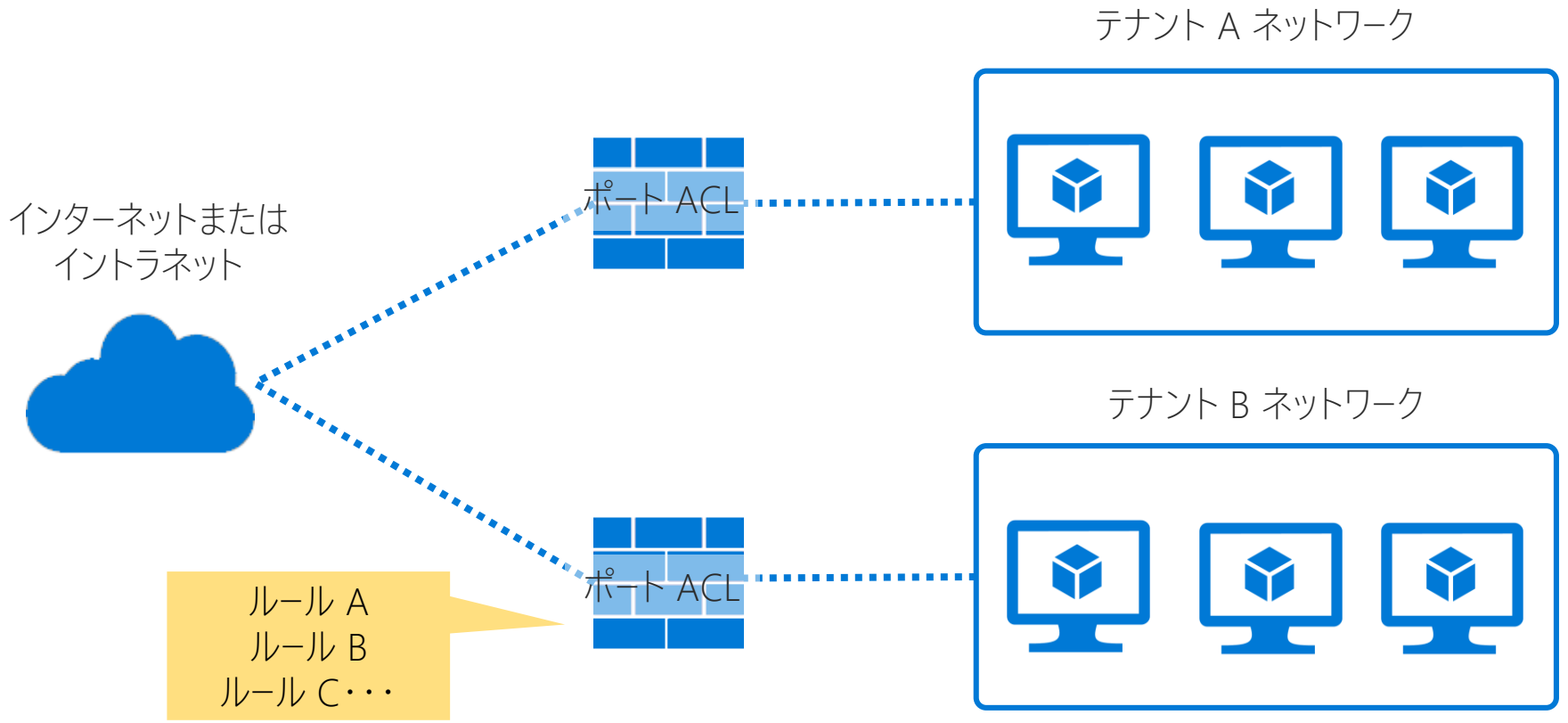
System Center 2016 Virtual Machine Manager

- Windows Server 2016 の SDN を統合管理



ポート ACL

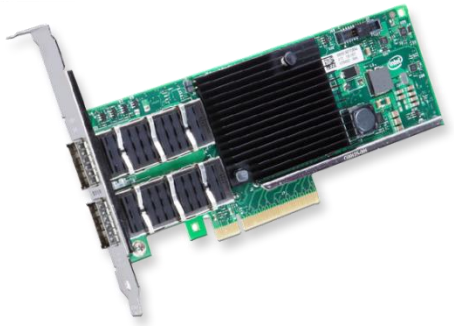
- Hyper-V ポートへのアクセスを ACL で集中管理するセキュリティ機能



インテルによるネットワークの最適化

- コンバージド ネットワークアダプターや 10GB イーサネットアダプターなど豊富なラインナップ

インテル イーサネット・コンバージド・ネットワークアダプター
Intel X710/XL740



Virtual Machine Device Queues
（ VMDq）

MAC アドレスと VLAN タグを確認し、
受信フレームを仮想マシンに振り分け

Single Root I/O Virtualization（SR-IOV）

ハイパーバイザーの代わりに
ネットワーク処理を直接実行

信頼性の高い製品

イーサネット製品における 30 年以上の経験、
過去 10 年で 6 億以上の製品の出荷

Microsoft

intel

セキュリティ

Windows Defender

- マイクロソフト標準のマルウェア対策ソフトウェア

有効期限切れによる
セキュリティ侵害の心配なし

Windows Update
または WSUS

グループポリシーによる
一元管理

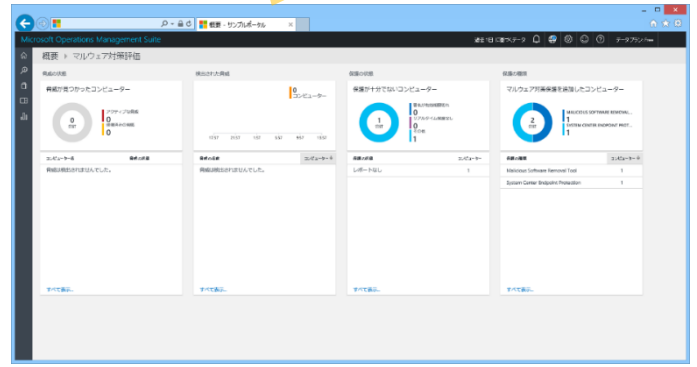
定義ファイルの配信

一元管理

Windows 10 および
Windows Server 2016

監視

マルウェアに感染したデバイス
の名前や対応状況などを
一元的に監視



Azure Log Analytics

Active Directory
グループポリシー

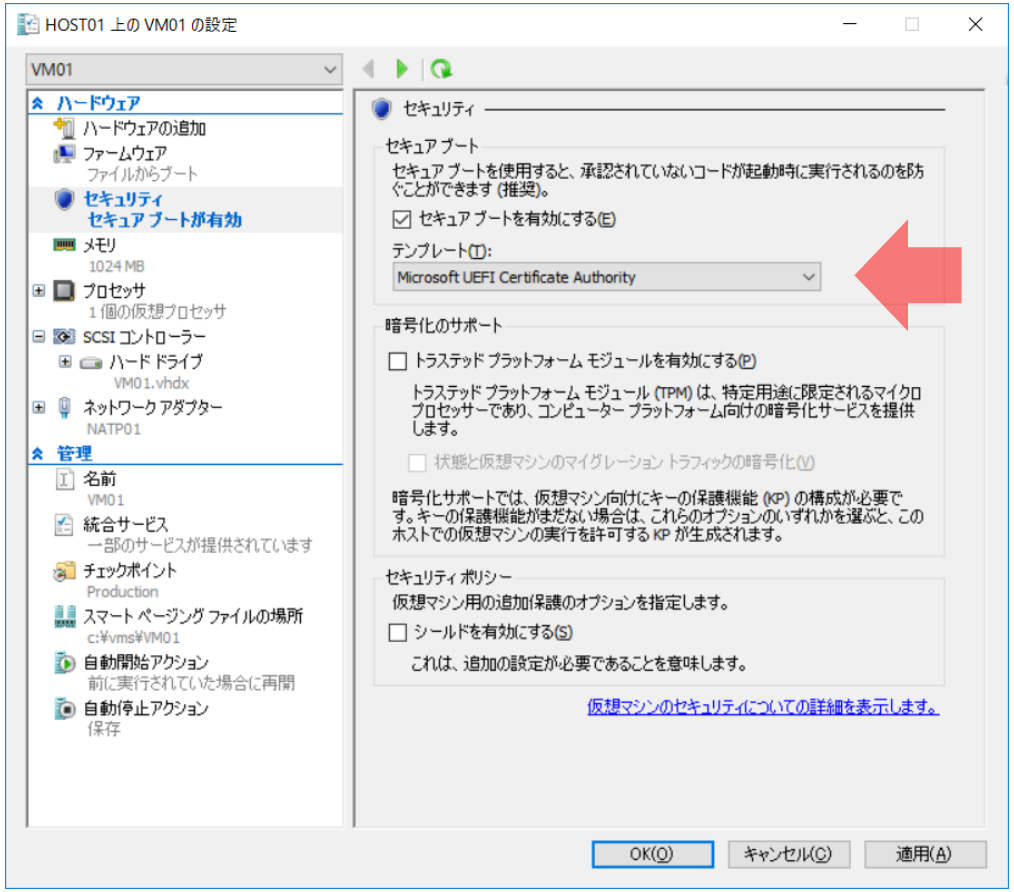
Windows Defender

標準でインストール済み ※

※ Nano Server のみ手動でパッケージの追加が必要

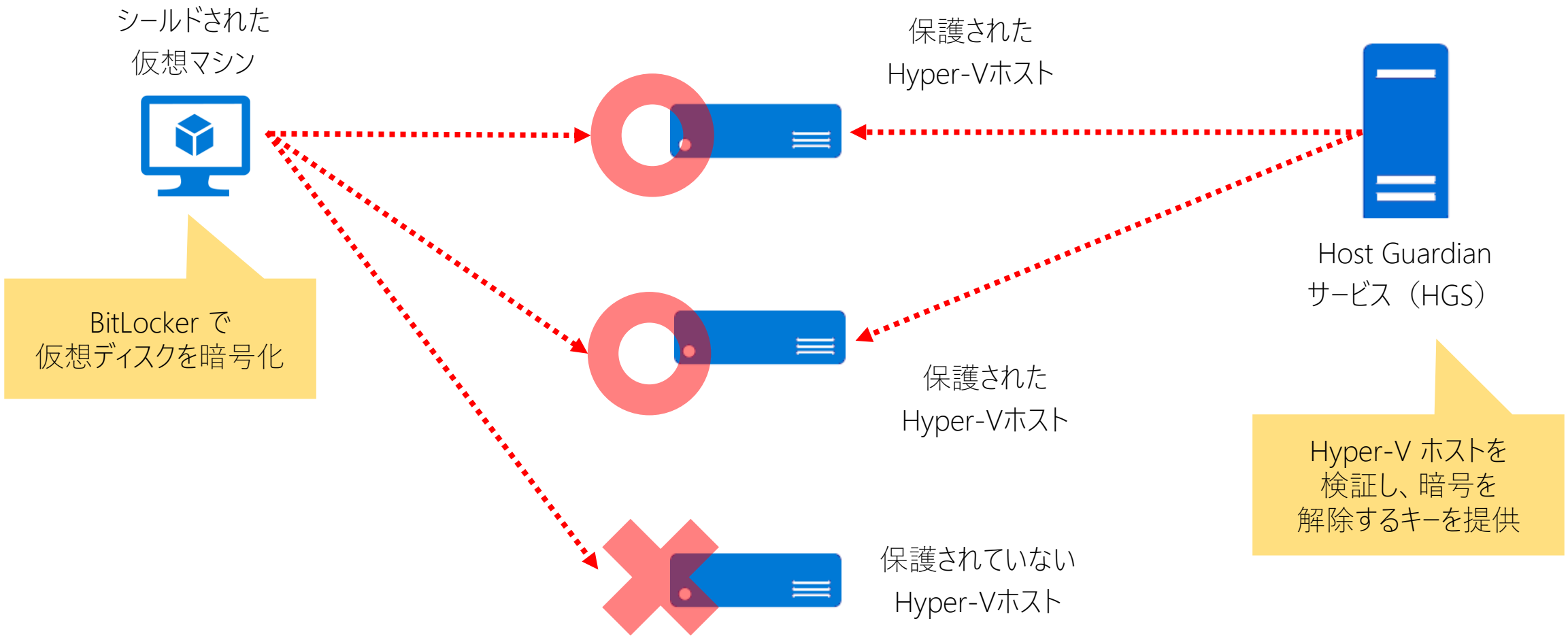
セキュアブート

- Hyper-V 仮想マシンのカーネルコードの整合性を維持
  - 起動時に承認されていないファームウェア、OS、UEFI ドライバーが実行されることを阻止
- Windows および 新しく Linux に対応



シールドされた仮想マシン

- 仮想マシンを信頼されたホストでのみ実行



HGS の設定例 ①

HGS ドメインの設定

```
Install-WindowsFeature -Name HostGuardianServiceRole -IncludeManagementTools -Restart
```

HGS 役割のインストール

```
$adminPassword = ConvertTo-SecureString -AsPlainText 'Pa$$w0rd' -Force
Install-HgsServer -HgsDomainName 'hgs.local' -SafeModeAdministratorPassword $adminPassword -Restart
```

HGS サーバーのインストール

```
$certificatePassword = ConvertTo-SecureString -AsPlainText 'Pa$$w0rd' -Force
$signingCert = New-SelfSignedCertificate -DnsName "signing.hgs.local"
Export-PfxCertificate -Cert $signingCert -Password $certificatePassword -FilePath 'C:¥signingCert.pfx'
```

署名証明書の作成

```
$encryptionCert = New-SelfSignedCertificate -DnsName "encryption.hgs.local"
Export-PfxCertificate -Cert $encryptionCert -Password $certificatePassword -FilePath 'C:¥encryptionCert.pfx'
```

暗号化証明書の作成

```
$HgsServiceName = 'HGSService'
Initialize-HGSServer -HgsServiceName $HgsServiceName -SigningCertificatePath 'C:¥signingCert.pfx' -
SigningCertificatePassword $certificatePassword -EncryptionCertificatePath 'C:¥encryptionCert.pfx' -
EncryptionCertificatePassword $certificatePassword -TrustActiveDirectory -Force
```

HGS クラスターの作成

HGS の設定例 ②

組織ドメインの設定

HGS ドメインを条件付きフォワーダーに追加

Add-DnsServerConditionalForwarderZone -Name “hgs.local” -ReplicationScope “Forest” -MasterServers “192.168.1.50"

New-ADGroup -Name "HGS" -GroupCategory Security -GroupScope Global
Add-ADGroupMember -Identity "HGS" -Members "HOST01$”

信頼されたホストのグループの作成と Hyper-V ホストの追加

HGS ドメインの設定

組織ドメインを条件付きフォワーダーに追加

Add-DnsServerConditionalForwarderZone -Name "contoso.com" -ReplicationScope "Forest" -MasterServers "192.168.1.200"

netdom trust hgs.local /domain:contoso.com /userD:contoso¥administrator /passwordD:Pa$$w0rd /add

信頼関係の確立
（コマンドプロンプト）

Add-HgsAttestationHostGroup -Name “HGS” -Identifier S-1-5-21-2219463165-834632096-704183863-1123

信頼されたホストのグループの登録

Get-HgsTrace -RunDiagnostics

環境のテスト

事前に組織ドメインで
Get-ADGroup “HGS” を
実行し、SID を確認

HGS の設定例 ③

Hyper-V ホストの設定

Install-WindowsFeature -Name HostGuardian

Host Guardian Hyper-V サポートのインストール

Set-HgsClientConfiguration -AttestationServerUrl 'http://hgs.local/attestation' -KeyProtectionServerUrl 'http://hgs.local/keyprotection'

Get-HgsTrace -RunDiagnostics

環境のテスト

Invoke-WebRequest 'http://hgs.local/keyprotection/service/metadata/2014-07/metadata.xml' -OutFile c:¥guardian.xml
Import-HgsGuardian -Path C:¥guardian.xml -Name Hosting –AllowUntrustedRoot

$Guardian = Get-HgsGuardian -Name Hosting
$Owner = New-HgsGuardian -Name Owner -GenerateCertificates
$KP = New-HgsKeyProtector -Owner $Owner -Guardian $Guardian -AllowUntrustedRoot
$VMName = "VM01"

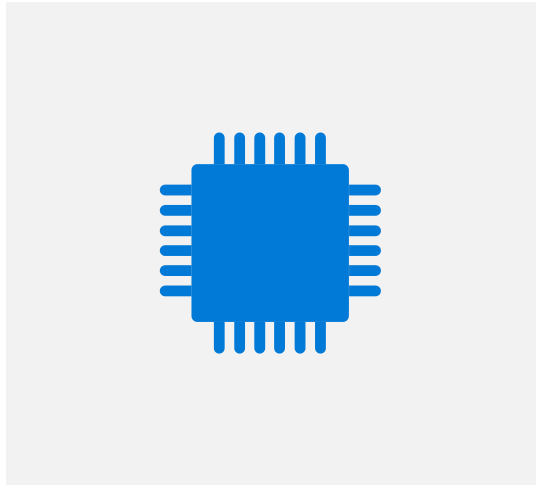
既存の仮想マシンのシールド化

Set-VMKeyProtector -VMName $VMName -KeyProtector $KP.RawData
Set-VMSecurityPolicy -VMName $VMName -Shielded $true
Enable-VMTPM -VMName $VMName

インテルによるセキュリティの拡張

- インテル Xeon プロセッサー E5-2600 v4 がサポートするエンタープライズセキュリティ

TPM 2.0



・暗号化に関連する基本的な機能（キーの生成や演算など）を提供
・セキュリティチップ内に 暗号化キーを保存することで耐タンパー性を向上

インテル セキュアキー

・暗号化キーのシードで使用される堅牢な乱数を生成

インテル AES-NI（New Instruction）

・AES による暗号化と復号をハードウェアで高速化

Windows Server 2016 とインテルテクノロジーで始める IT インフラの強化

コンピューティング

新しい Hyper-V
Nano Server
Windows コンテナー

Intel Xeon プロセッサー
E5-2600 v4

ストレージ

記憶域スペースダイレクト
記憶域レプリカ、記憶域 QoS
重複除去、ReFS

PCIe 対応 インテル SSD
データセンター・ファミリー

ネットワーク

SDN ファブリック

インテル イーサネット・
コンバージド・ネットワークアダプター
Intel X710/XL740

セキュリティ

Windows Defender
シールドされた仮想マシン

セキュアブート
クレデンシャルガード
デバイスガード


Microsoft


intel