Kaspersky Security for Virtualization

--- Kaspersky Hybrid Cloud Security

Kaspersky Security for Virtualization 6.1 Agentless
Kaspersky Security for Virtualization 5.2 Light Agent

2023年5月23日
株式会社カスペルスキー
セールスエンジニアリング本部

kaspersky

Kaspersky Security for Virtualization

Kaspersky Security for Virtualizationは、
仮想環境向けアプリケーションです。

Kaspersky Hybrid Cloud Securityライセンスで使用出来ます。

Kaspersky Hybrid Cloud Securityをお持ちであれば、
有効なライセンス範囲・ライセンス数の範囲で、
仮想環境、物理サーバー、Public Cloud APIを利用したインスタンス保護に
使用出来ます。

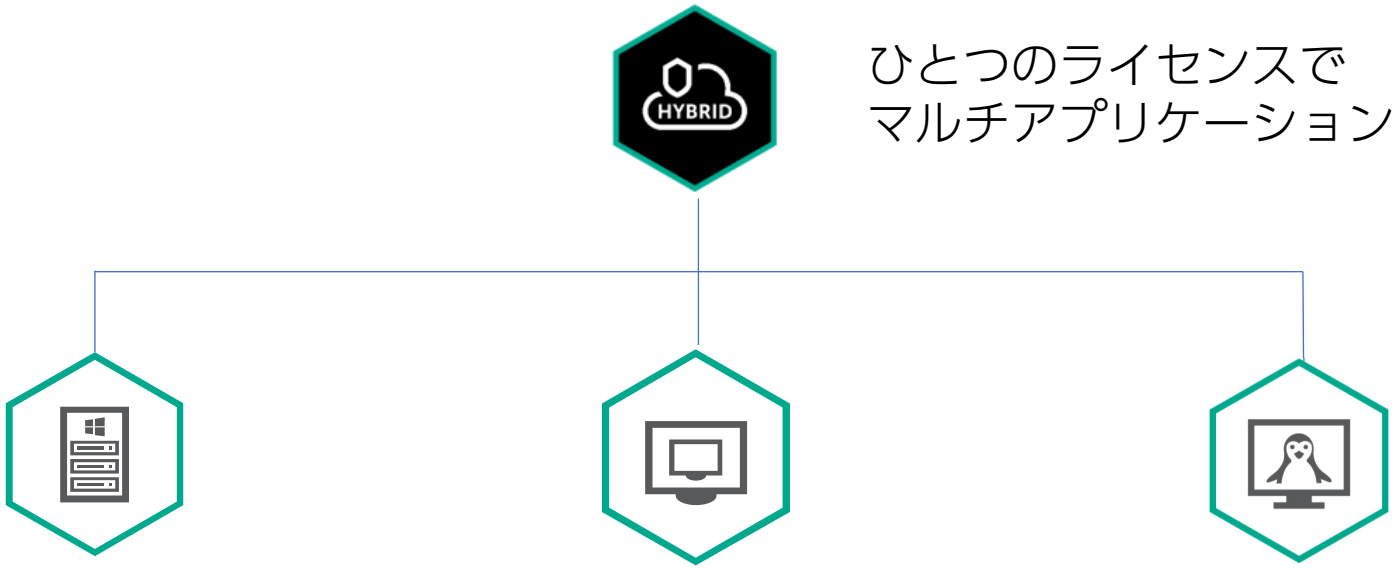
kaspersky

Kaspersky Hybrid Cloud Securityについて

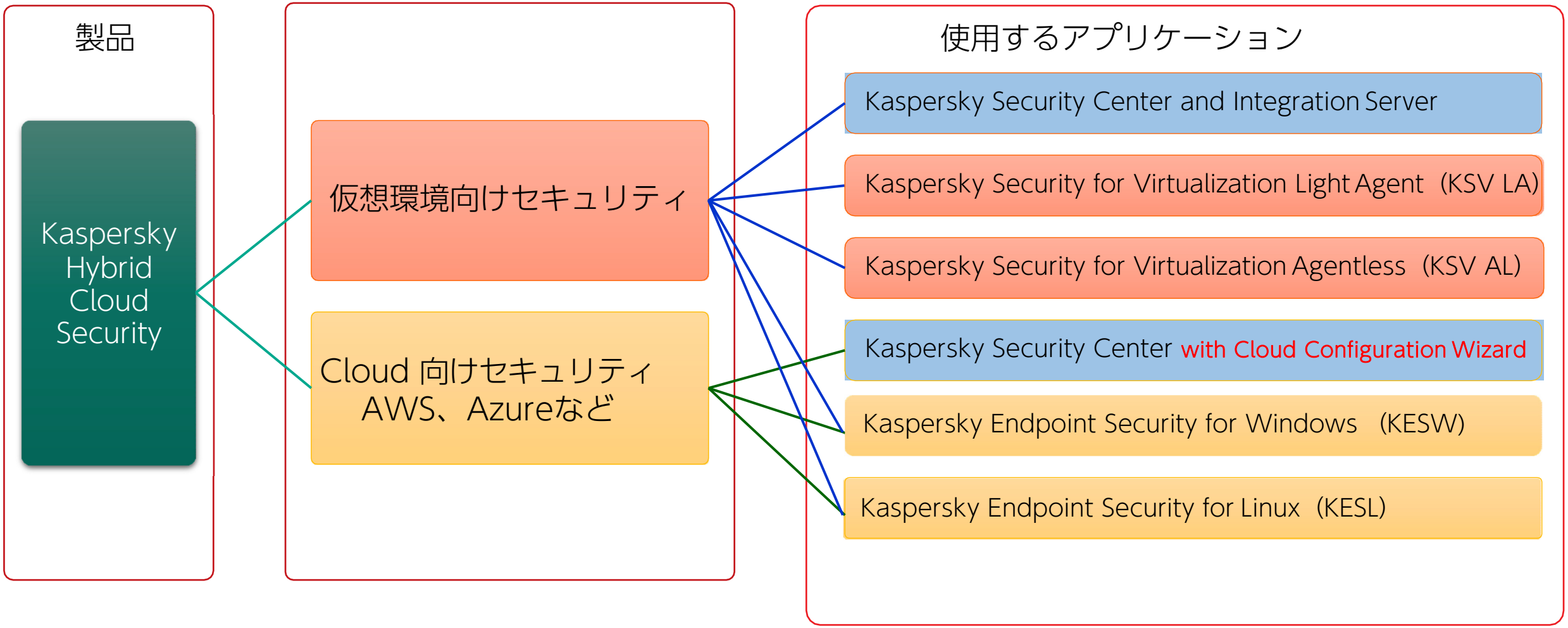
kaspersky

Kaspersky Hybrid Cloud Security

Kaspersky Hybrid Cloud Securityは、
クラウド環境、仮想環境、物理サーバーに使用出来る製品です。

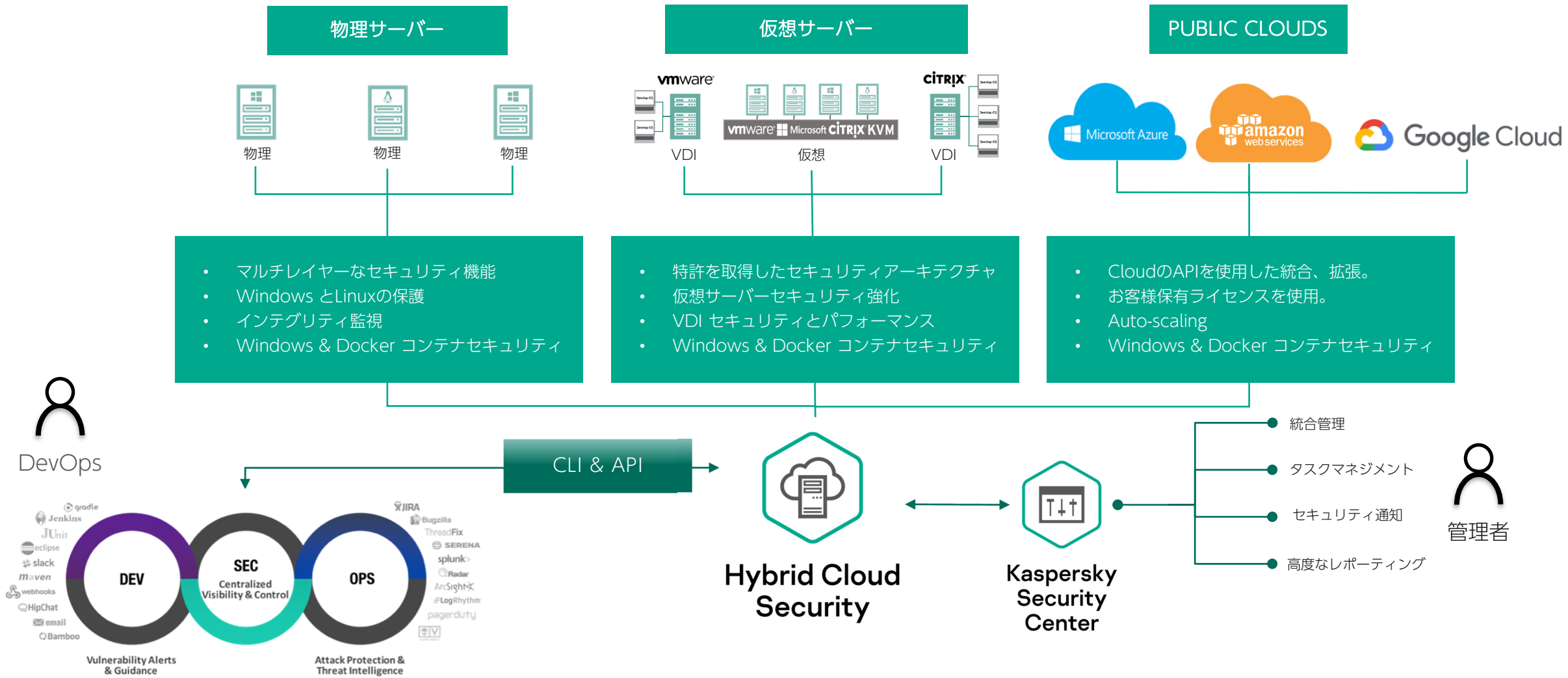


Kaspersky Hybrid Cloud Security（KHCS）



Kaspersky Endpoint Security for Windows11.9以降では、KHCSライセンスが使用出来ます。
仮想環境におけるクライアントOS保護には、Kaspersky Security for Virtualizationを使用します。

Kaspersky Hybrid Cloud Security Architecture



Kaspersky Security for Virtualization Agentless
Kaspersky Security for Virtualization Light Agent
機能紹介

kaspersky

仮想環境向けソリューション

Kaspersky Security for Virtualization には、2タイプのアプリケーションがある。

- Kaspersky Security for Virtualization Agentless
  ESXi専用。
  データセンターなどで活用。
  Network Attack BlockerによるIPSも提供。

- Kaspersky Security for Virtualization Light Agent
  ESXi 以外のハイパーバイザーサポート。
  （ESXi、Hyper-V、 XenServer、AHV など）
  特にVDI などセキュリティが重要な運用に最適なソリューション。
  CentOSもサポート。

kaspersky

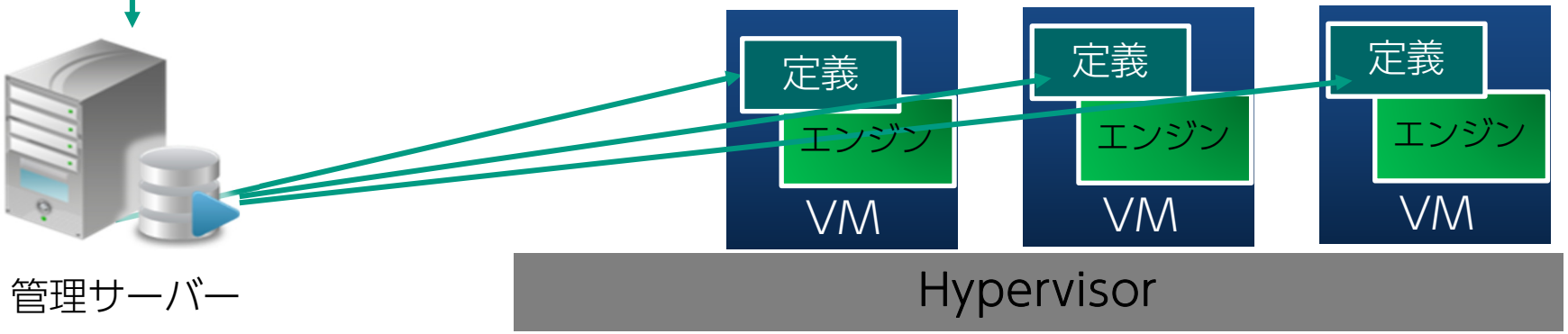
仮想環境向けソリューションのメリット

物理PC用アプリケーションを仮想環境に使用した場合の問題点

- ✓ 重複処理があり、リソースの無駄が起きる。リソース逼迫。
- ✓ 定義更新配布のセキュリティギャップが起きる。
  - 新規デプロイされた仮想マシンでは、定義更新が完了するまでに時間がかかる。（ひな形の定義は陳腐化するため）
  - トラフィック過多

基本アーキテクチャ

スキャンエンジン、定義が各仮想マシン（VM）に存在。

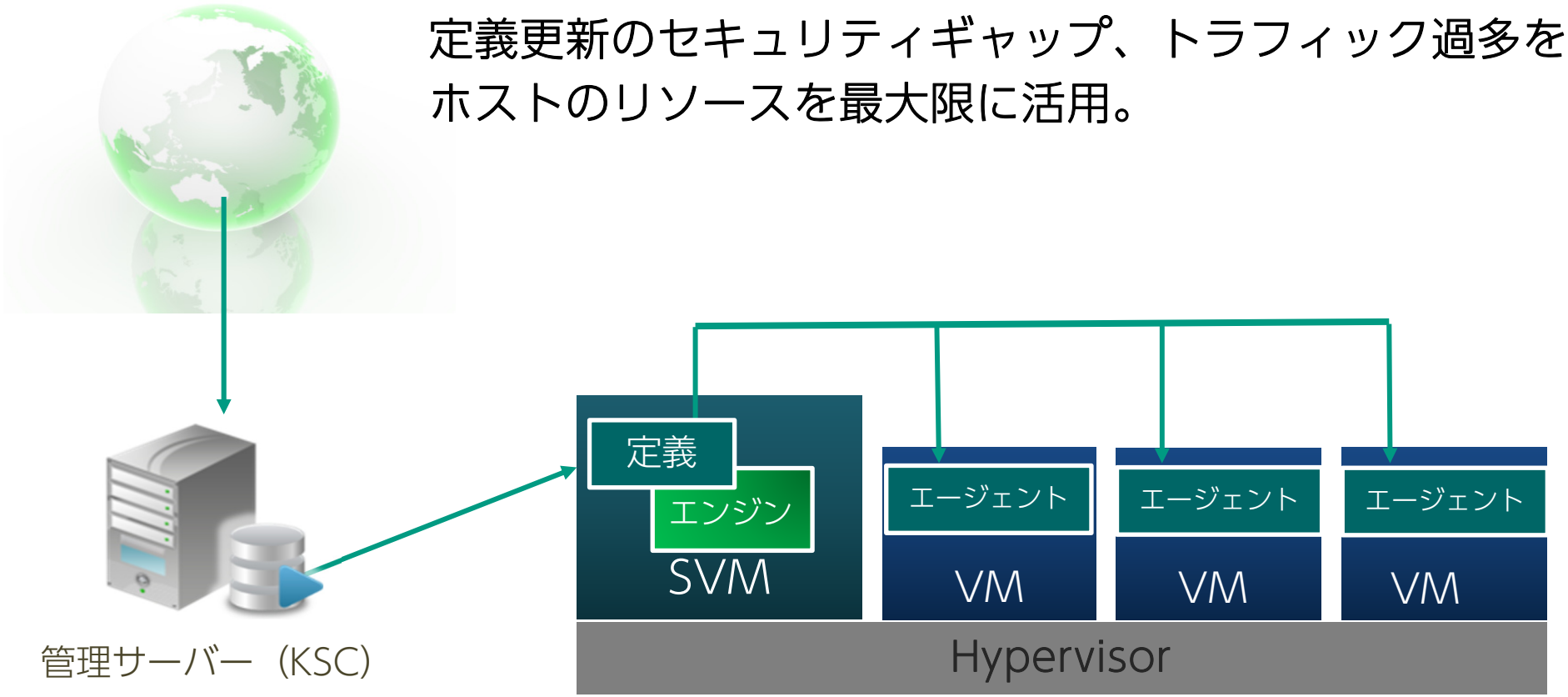


kaspersky

仮想環境向けソリューションのメリット

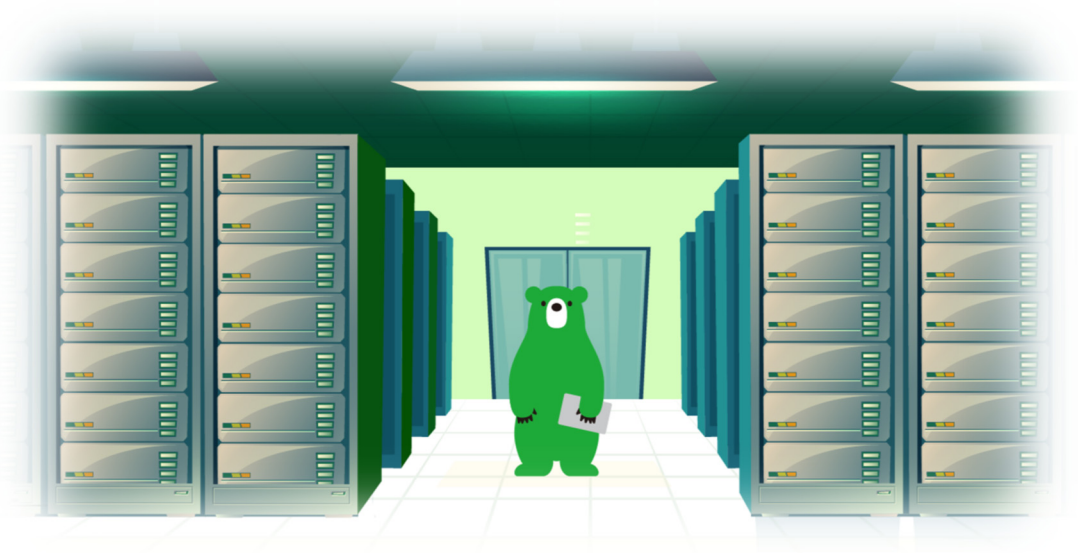
仮想環境向けアプリケーションの基本アーキテクチャ

スキャンエンジンをSVMセキュリティバーチャルマシンに集約。
定義更新のセキュリティギャップ、トラフィック過多を防止。
ホストのリソースを最大限に活用。



kaspersky

Kaspersky Security for Virtualization Light Agent



kaspersky

名前の印象から誤解されがち

- AgentlessのようにSVMで集中処理を行う。
- Agentlessもエージェント（VMware製）は入れている。

- ふるまい検知のような、ローカルでしか出来ない保護をエージェントで実行。
  高度なセキュリティを実現できるのは、 Light Agentだけ。

- VDIならばマスターに導入するため、エージェントだからインストールが面倒ということはない。
- バージョンアップもマスターに行う。

Kaspersky Security for Virtualization Light Agentの特徴

- SVM（セキュリティバーチャルマシン）とエージェントの仕組みを
  カスペルスキーが提供するため、VMware以外の環境もサポート。
  Hyper-V、Citrix XenServer、VMware ESXi、Nutanix AHV、KVM など。

- Agentlessでは提供できないふるまい検知などの高度な機能を実装。
  Webやメールを使用するVDIには、物理PCと同レベルのセキュリティが必要。
  Light Agentは高セキュリティを実現する。

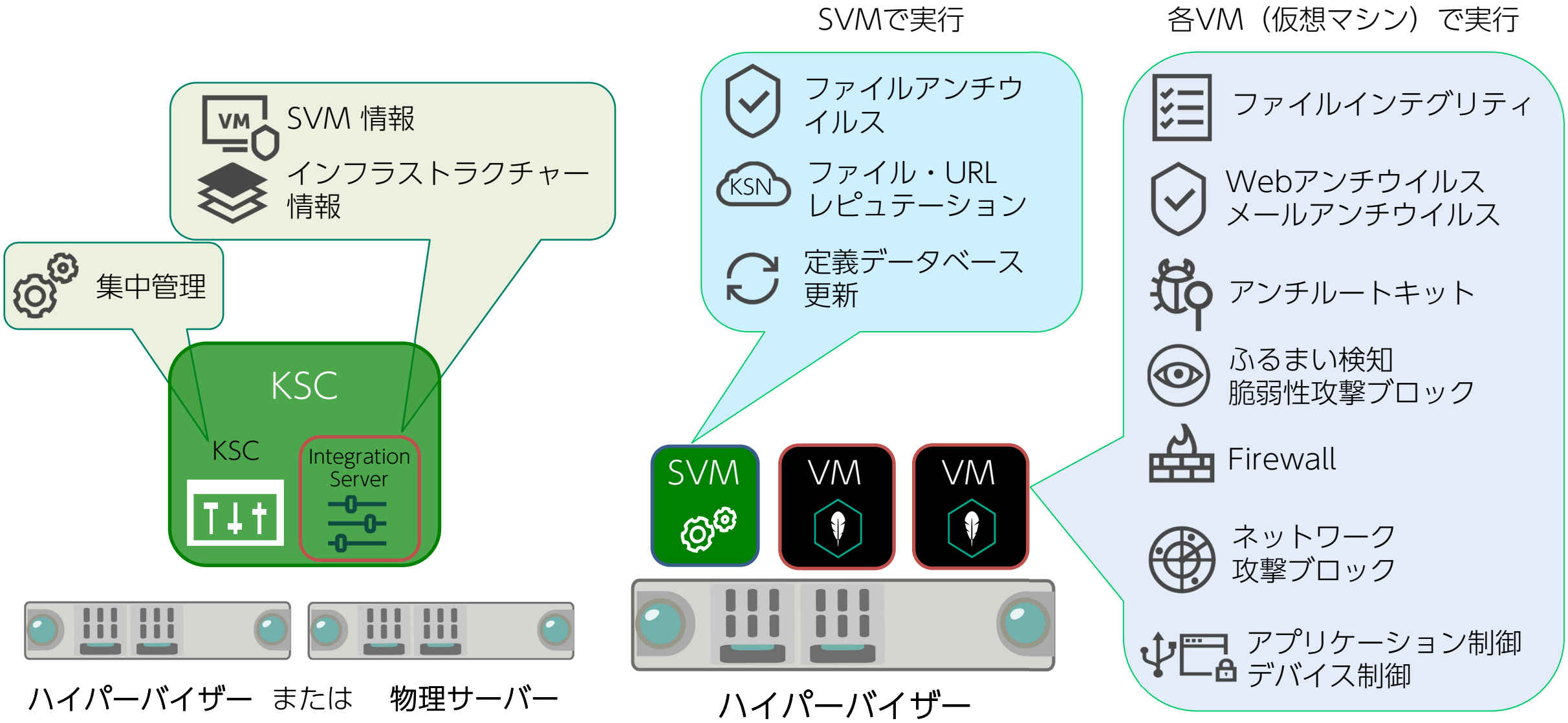
- リソース使用を最適化。
  SVMへの集約と、仮想マシンローカル処理のハイブリッド型。

- 冗長構成が可能。

- KSC/Integration Server は、物理サーバー・仮想サーバーへインストール可能。

kaspersky

Kaspersky Security for Virtualization Light Agentアーキテクチャ

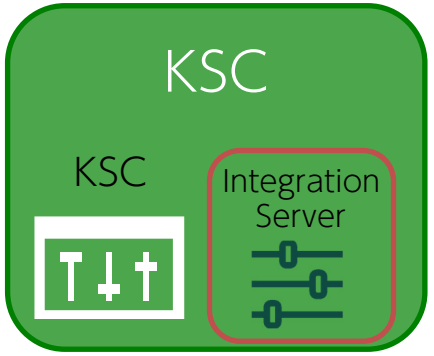


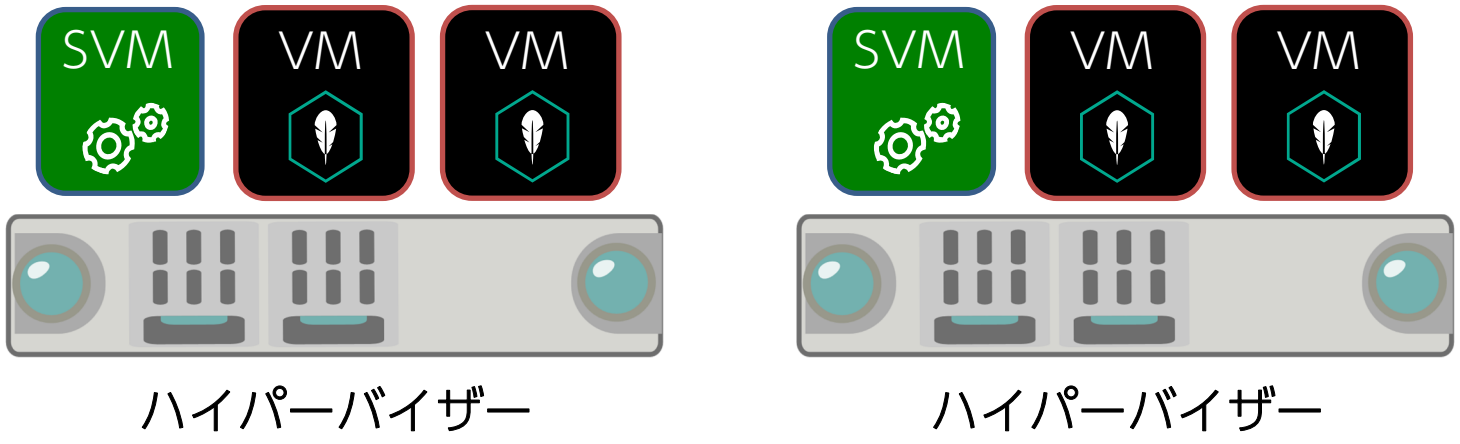
KSC（Kaspersky Security Center）

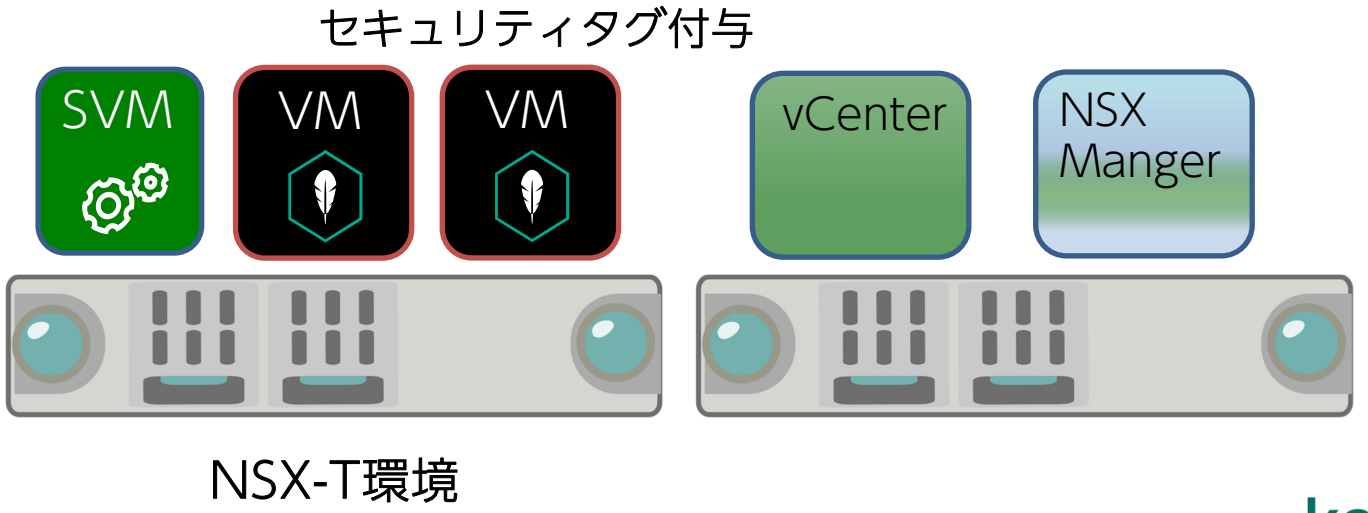
SVM（セキュリティバーチャルマシン）

kaspersky

Kaspersky Security for Virtualization Light Agent 適用範囲



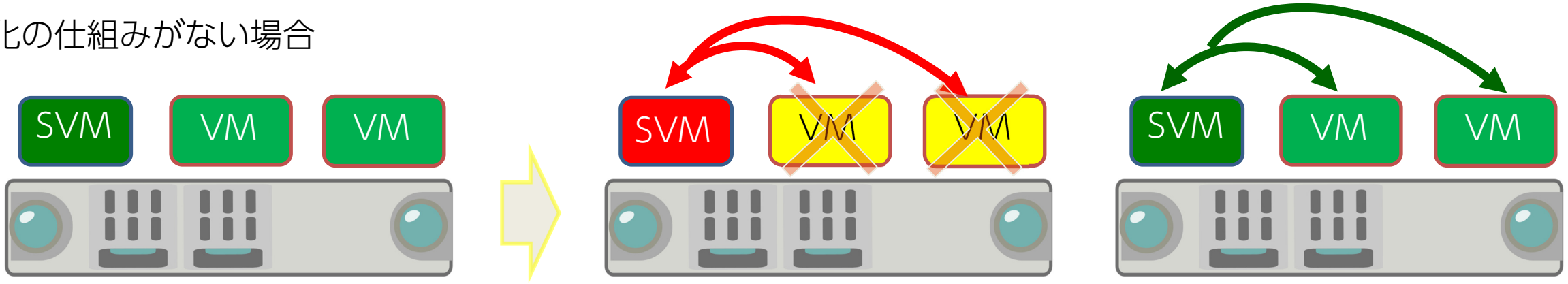




kaspersky

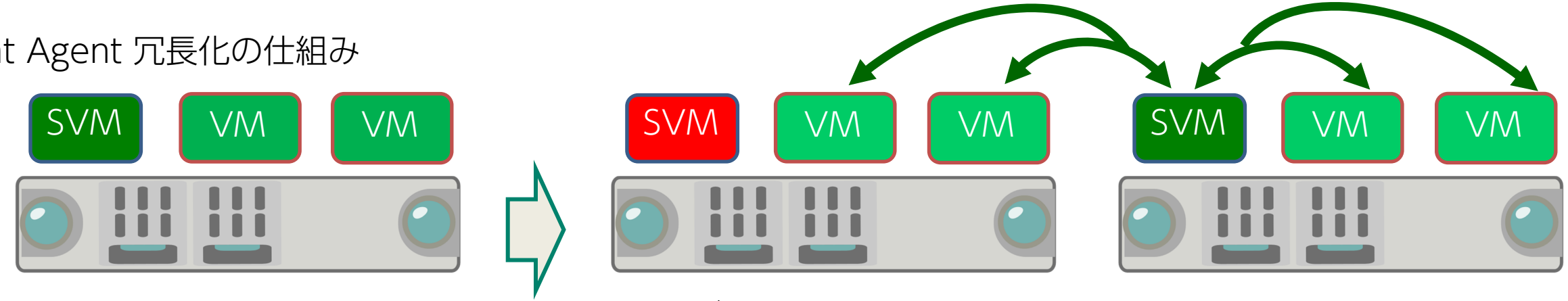
Kaspersky Security for Virtualization Light Agent　冗長化

冗長化の仕組みがない場合



SVMが使用できなくなった場合、
仮想マシンの保護が失われる。

Light Agent 冗長化の仕組み



SVMが使用できなくなった場合、
他のハイパーバイザー上のSVMに接続し、保護が続行される。

kaspersky

Kaspersky Security for Virtualization Light Agent システム要件

KSV LA Windowsエージェント

- Windows 11 21H2 Pro / Enterprise / Education
- Windows 10 Desktop Pro
- Windows 10 Enterprise / 2016 LTSC / RS4 / 2019 LTSC / 19H1 / 19H2 / 20H1
- Windows 8.1 Update 1 Professional / Enterprise
- Windows 7 Professional / Enterprise Service Pack 1
- Windows Server 2022 Standard / Datacenter / Essentials
- Windows Server 2019 Standard / Datacenter
- Windows Server 2016 Standard / Datacenter
- Windows Server 2012 R2 Standard / Datacenter
- Windows Server 2012 Standard / Datacenter
- Windows Server 2008 R2 Service Pack 1 Standard / Enterprise / Datacenter

Windows Serverはデスクトップエクスペリエンス / Coreをサポート

KSV LA Linuxエージェント

- Debian GNU / Linux
- Ubuntu Server
- CentOS 8.1
- Red Hat Enterprise Linux Server
- Oracle Linux

など。

最新のシステム要件はWebでご確認ください。
https://support.kaspersky.com/ksvla/5.2/ja-JP/175612.htm

kaspersky

セキュリティ機能

KSV Light Agent 機能一覧（Ver 5.2）

https://support.kaspersky.com/ksvla/5.2/ja-JP/145538.htm 以降

	保護コンポーネント	管理コンポーネント
Windows クライアント	ファイルアンチウイルス	アプリケーション起動コントロール
	メールアンチウイルス	アプリケーション権限コントロール(HIPS)
	ウェブアンチウイルス	デバイスコントロール
	ファイアウォール	ウェブコントロール
	ネットワーク攻撃防御	
	システムウォッチャー（ふるまい検知）	
	AMSI	
Windows サーバー	ファイルアンチウイルス	アプリケーション起動コントロール(Enterpriseライセンスのみ)
	メールアンチウイルス	システム変更監視(Enterpriseライセンスのみ)
	ファイアウォール	
	ネットワーク攻撃防御	
	システムウォッチャー（ふるまい検知）	
	AMSI	
Linux	ファイルアンチウイルス	

インストールパッケージの初期値とは異なります。
必要な機能を選択してください。

kaspersky

- VMware NSX Tagに対応

VMware NSX-V、VMware NSX-T と連携、

従来、エージェントレスのみが実現していたNSX連携を実現。
マルウェア検知時のisolationが可能。
＊有償版NSX使用時のみ。

•*ANTI_VIRUS.VirusFound.threat=high*：
ウイルスなどの悪意のあるソフトウェアが検知された仮想マシンに割り当てられます。

•*IDS_IPS.threat=high*：
ネットワーク攻撃に特有の兆候が受信トラフィックに含まれていた仮想マシンに割り当てられます。

IDS_IPSタグは、Windowsのみ対応。

- EDR-Optimumサポート

Kaspersky Endpoint Agent 3.11 / 3.1を追加インストールすることにより、
Kaspersky Endpoint Detection and Response Optimum 2.0をサポートします。

https://support.kaspersky.com/KEDR_Optimum/2.0/ja-JP/216855.htm

kaspersky

Kaspersky Security for Virtualization Light Agent

VDI サポート

kaspersky

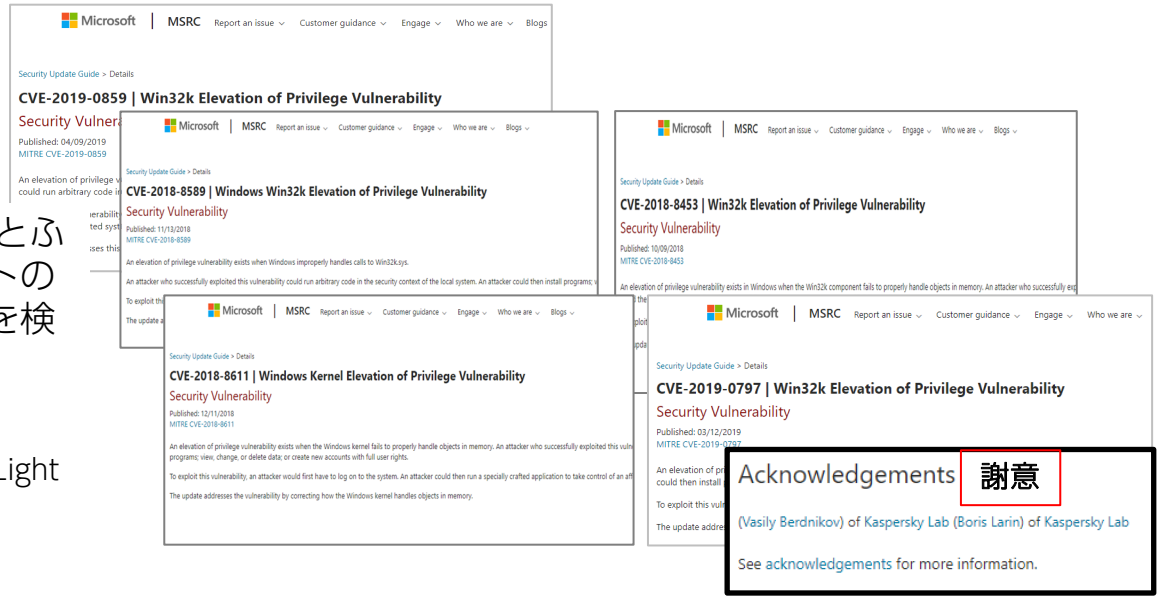
Light Agentが持つ高度なセキュリティ

Automatic Exploit Prevention（AEP）

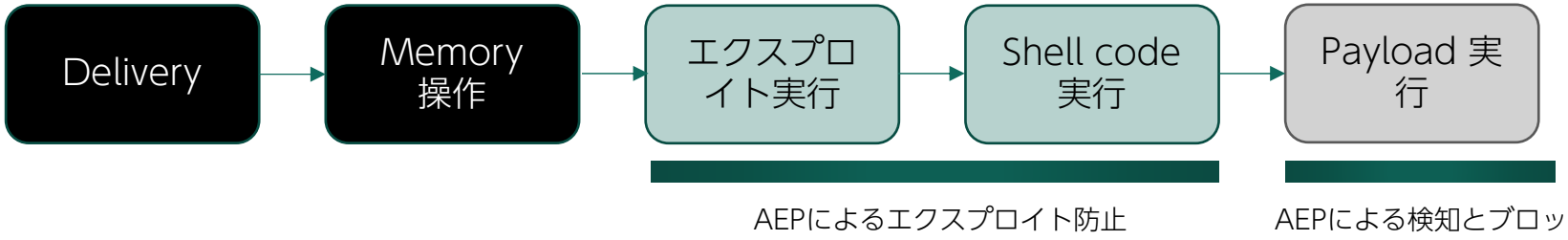
CVE-2019-0859脆弱性

2019年3月に、カスペルスキーのAEPとふるまい検知エンジンが、マイクロソフトの脆弱性を突こうとするエクスプロイトを検知

AEPは Kaspersky Security for Virtualization Light Agentに含まれる



これらの5つのゼロディエクスプロイトは、Automatic Exploit Prevention テクノロジーによって、世界で初めて発見された。



kaspersky

XenDesktopサポート

仮想デスクトップ展開方式は、以下をサポート
- Citrix MCS
- Citrix Provisioning Services

デスクトップエクスペリエンス
- カスペルスキーネットワークエージェントの「VDI向けダイナミックモード」により、ランダム方式をサポート。

kaspersky

Citrix環境に最適化

Citrixが推奨する除外設定を予め設定済み

［Citrix EdgeSight］、［Citrix Profile Manager］、［Citrix Provisioning Services］、［Citrix XenApp］、［Citrix XenDesktop］は、これらのアプリケーションのパフォーマンスを向上するため、既定でオンになっています。

推奨事項：ベンダーやセキュリティチームと一緒にこれらの推奨事項を確認してください。

- 除外ポリシーを作成する前に、すべてのファイル/フォルダーの除外を確認し、それらが存在することを確認してください。
- すべてのコンポーネントに対して1つの大きなポリシーを作成するのではなく、さまざまなコンポーネントに対して複数の除外ポリシーを実装します。
- 機会を最小限に抑えるために、リアルタイムスキャンとスケジュールスキャンの組み合わせを実装します。

仮想アプリとデスクトップ

配送コントローラ

ファイル：

- `%SystemRoot%\ServiceProfiles\NetworkService\HaDatabaseName.mdf (7.12+)`
- `%SystemRoot%\ServiceProfiles\NetworkService\HaImportDatabaseName.mdf (7.12+)`
- `%SystemRoot%\ServiceProfiles\NetworkService\HaDatabaseName_log.ldf (7.12+)`
- `%SystemRoot%\ServiceProfiles\NetworkService\HaImportDatabaseName_log.ldf (7.12+)`

フォルダ

- `%ProgramData%\Citrix\Broker\Cache (7.6+)`

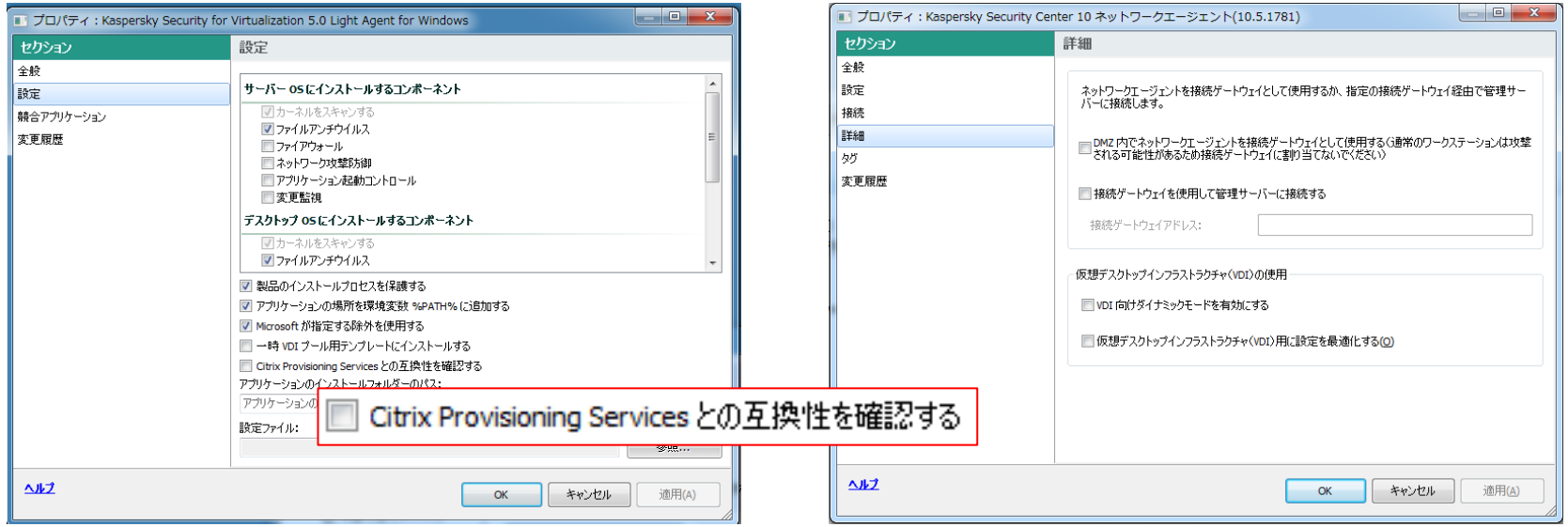
プロセス：

- `%ProgramFiles%\Citrix\Broker\Service\BrokerService.exe`
- `%ProgramFiles%\Citrix\Broker\Service\HighAvailabilityService.exe (7.12+)`
- `%ProgramFiles%\Citrix\ConfigSync\ConfigSyncService.exe (7.12+)`

kaspersky

XenDesktopに最適化

Citrix Provisioning Services 技術との互換性



テンプレート

Citrix XenDesktop のランダムカタログ。
Citrix XenDesktop の Citrix Personal vDisk を使用した静的カタログ。
Citrix XenDesktop のユーザーによる変更を保存しない静的カタログ。

このオプションでは、このテンプレートから作成された仮想マシンには、
保護された仮想マシンを再起動する必要があるアップデートがインストールされません。

kaspersky

VMware Horizonサポート

仮想デスクトップ展開　ユーザー割当方式
　流動割当（フローティング）をサポート。
　カスペルスキーネットワークエージェントの「VDI向けダイナミックモード」により、ランダム方式をサポート。

フルクローン、リンククローン、インスタントクローンをサポート

Light AgentではNSXコンポーネントを使用しないため、リンククローン使用時リコンポーズのオーバーヘッドが最小限。

kaspersky

Kaspersky Security for Virtualization Light Agent

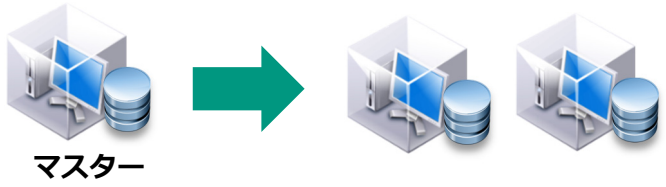
VMware Horizonインスタントクローン

kaspersky

VMware Horizonのクローン方式

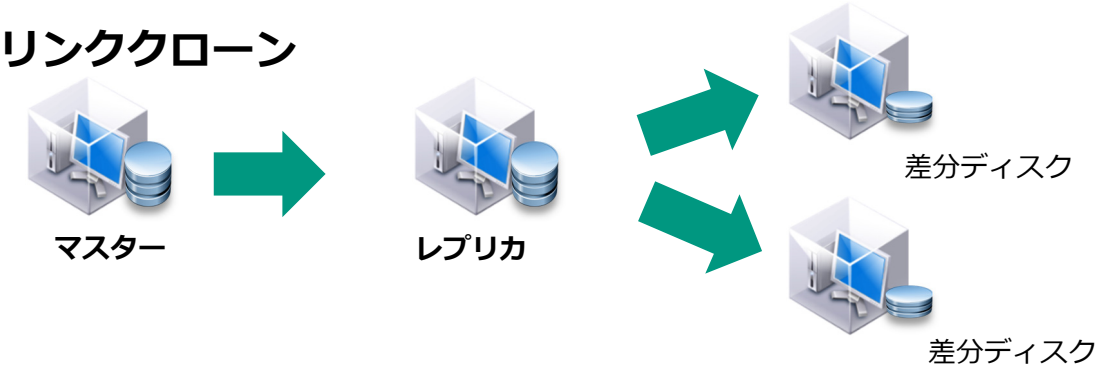
- 下記3種類のクローン方式がある。インスタントクローンは、Horizon 7で実装された機能。

1．フルクローン



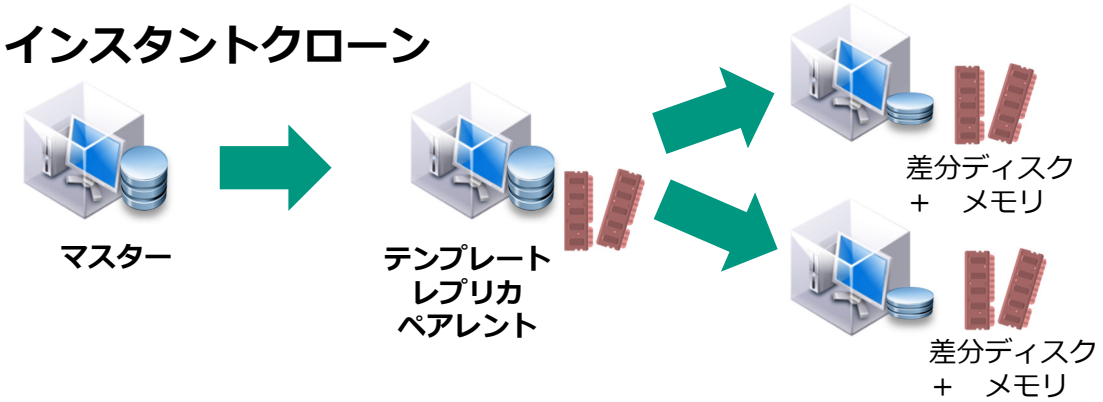
仮想デスクトップはマスターVMの
ディスク情報を全てコピーして作成。

2．リンククローン



Composerサーバーで提供。
仮想デスクトップは、マスターVMの
ディスク情報を全てコピーした
レプリカVMと差分ディスクで作成

3．インスタントクローン



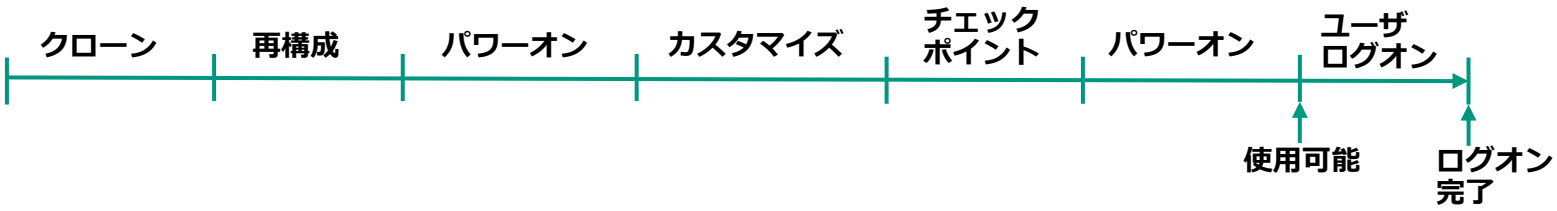
Horizon 7の新機能。
リンククローンの特徴に加え、メモリも
差分管理することで、高速展開が可能。

kaspersky

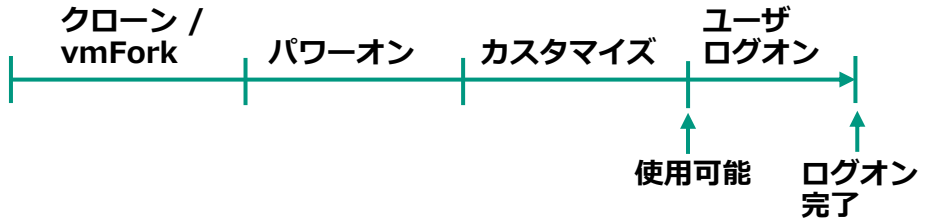
インスタントクローンのデプロイフロー

- View Composer によるプロビジョニングに含まれる一部のステップを排除・短縮。
- インスタントクローンではデスクトップを使用可能状態にするまでの時間を大幅に短縮

■ リンククローン（View Composer）によるクローンの流れ



■ インスタントクローンによるクローンの流れ



vCenter の Call	View Composer	インスタントクローン
クローニング	1 回のクローン call	1 回の vmFork call
パワーサイクル	2 回のパワーサイクル call	なし
再構成	3-4 回の再構成 call	なし
vCenter の負荷	高	低

kaspersky