ホワイト ペーパー

シスコの仮想化エクスペリエンス インフラストラクチャ：セキュアな仮想デスクトップ

概要

Cisco® Virtualization Experience Infrastructure（VXI; 仮想化エクスペリエンス インフラストラクチャ）では、シスコの 3 つのアーキテクチャ（データセンター、ボーダレス ネットワーク、コラボレーション）にわたる包括的なサービスを使用して、サービスに最適化されたデスクトップ仮想化プラットフォームを提供します。

Cisco VXI は、従業員のコラボレーション ワークスペースを構成するあらゆるツールを網羅できるようにデスクトップの仮想化を再定義し、仮想デスクトップ環境で従来はサポートされていなかった広範なインタラクティブ メディアをサポートする妥協のないユーザ エクスペリエンスを実現します。

Cisco VXI により、俊敏性が高く効率的であり、カスタマイズされた広範なユーザ インタラクションが可能で、ビジネス資産の一元化と統合によるオープンかつ統制された環境を従業員に提供できるようになり、完全に仮想化されたコラボレーション ワークスペースが実現します。

データセンターにおいて、デスクトップを仮想マシンとして一元管理することは、セキュリティ上の新たな課題が生じることになり、クライアントのエンドポイントから仮想マシンにわたるエンドツーエンドの総合的なセキュリティ アプローチが必要となります。

Cisco VXI セキュリティが重要な理由

Cisco VXI は、シスコの 3 つのアーキテクチャ（データセンター、ボーダレス ネットワーク、コラボレーション）にわたるエンドツーエンドのシステムです。このアーキテクチャには、データセンターやインフラストラクチャを保護するための従来型のセキュリティ対策やセキュアなリモート アクセス、エンドポイントからのトラフィックの保護など、セキュリティのベスト プラクティスを適用する必要があります。仮想デスクトップ間の通信や、仮想デスクトップと仮想サーバ間の通信を保護するには、別のセキュリティ対策を講じる必要があります。仮想デスクトップはデータセンターに統合されるようになってきているため、デスクトップとサーバのトラフィックを分離し、バックエンドで実行されるミッションクリティカルなサーバとアプリケーションを保護することが、これまで以上に重要になっています。

仮想デスクトップでは、セキュリティの新たな課題が生じます。Hosted Virtual Desktop（HVD; ホスト型仮想デスクトップ）は、非常に静的な環境（物理的なユーザとマシン）を動的な側面の強い環境に置き換えます。仮想マシンは、物理ホストの CPU、メモリ、ネットワーク インターフェイス、ストレージ、I/O 処理などの割り当てを使用し、ハイパーバイザによって動作条件やルールを定められたコンテナと考えることができます。ホスト型仮想デスクトップはこれらの仮想マシンに内蔵され、仮想マシンに関連付けられたパラメータを使用します。災害（天災や人災）が発生した場合や、物理ホストの使用のバランスを再調整したり、メンテナンス ウィンドウ中に機器の更新を実施する必要が生じた場合、仮想デスクトップを物理ホストのクラスタ間で移行できます。この移行作業は管理者が実行できますが、ハイパーバイザ管理プラットフォームで設定したルールとポリシーを使用して自動化することもできます。仮想マシンをサーバ間で移動する場合に、仮想マシンでセキュリティ ポリシーを維持するには、仮想マシンを常に監視しておく必要があります。HVD に関連付けられたセキュリティ ポリシーを HVD 内からリクエストされるすべてのデータ アクセスに適用するには、これらのポリシーの監視が極めて重要です。これにより、エンド ユーザは、アクセスを許可されたサーバやアプリケーション以外にアクセスできなくなります。また、同じ VLAN のすべての仮想マシンにアクセスできるインサイダー リスクも発生します。レイヤ 3 ファイアウォール メカニズムで問題を解決する現在のソリューションでは十分に対応できない場合が多く、データセンターのスケーラビリティやパフォーマンスにも影響を与える可能性があります。

仮想化は新たな分野の脅威にもさらされます。ハイパーバイザがシングル ポイント障害となり、ホストされるすべての仮想デスクトップが停止する原因になることもあります。仮想マシンの API 呼び出しは悪意のあるコードの標的になるため、認証および許可された API 呼び出しのみを可能にするポリシーを、パフォーマンスを損なわずに適用することが重要になります。また、ハイパーバイザの IP アドレスが公開されないようにするなどのベスト プラクティスを実施することも重要です。ハイパーバイザの IP アドレスが公開されると、DDoS（分散型サービス拒否）攻撃につながる可能性があり、仮想メモリの暗号化キーが失われる危険も生じます。

組織が仮想化に移行する場合は、他にも考慮すべきことがあります。移行時に、PC と仮想デスクトップが混在した環境が生まれます。これにより、従来の環境と仮想環境の両方でセキュリティを維持し、混在した環境でコンプライアンスのチェックを実施するという、さらに別の課題も発生します。重要な点は、一貫性のない状態を減らし、両方の環境に適したセキュリティ ポリシーと管理メカニズムを提供することです。また、HVD に移行しても従来型のセキュリティの必要性がなくなるわけではありません。従来型のセキュリティ対策は仮想化環境にも適用され、既存のファイアウォール、侵入防御、電子メールおよび Web のセキュリティ、セキュア モビリティが引き続きデータセンターやエンド ユーザの周囲に適用されます。

エンド ユーザ用の従来型のセキュリティ

システム管理者は、複数の場所からデータセンターにアクセスできる必要があり、エンド ユーザの認証にも対応する必要があります。エンド ユーザからの接続は暗号化する必要があります。VPN 暗号化テクノロジーは、ユーザがデスクトップにアクセスしている場所に応じて、EasyVPN、Dynamic Multipoint VPN（DMVPN; ダイナミック マルチポイント VPN）、SSLVPN が使用されます。また、エンド ユーザは Cisco Identity Services Engine（ISE）で定義されたロールベースのアクセス ポリシーに基づき、IEEE 802.1x で認証されます。hop-to-hop 型の LAN セキュリティ（MACsec）暗号化などの LAN の機能では、LAN 上の表示プロトコルを暗号化できます。

データセンター用の従来型のセキュリティ

システム管理者には、あらゆる脅威からデータセンターを保護することが求められます。適切なファイアウォール ポリシーをエッジで設定することにより、データセンターへ向かう表示プロトコルのトラフィックを許可および拒否できます。このため、データセンターの重要なセキュリティ メカニズムは、データセンターの機密情報資産や重要なリソースへのネットワーク アクセスを制御する高パフォーマンスのファイアウォールになります。さらに、ウイルスやマルウェア、ハッカーによるデータセンターのリソースへの攻撃を検知して止めるために、侵入防御システムが必要になります。また、エンド クライアントからの VPN 接続をデータセンターの VPN ヘッドエンドで終了する必要もあります。法令や企業のコンプライアンスを順守するために、社内から送信される電子メールや Web トラフィックもすべてスキャンする必要があります。Cisco IronPort™ E メール/Web セキュリティ ソリューションを細部にわたるスキャニングに組み込むことにより、許可されたコンテンツのみを送受信できるようになります。

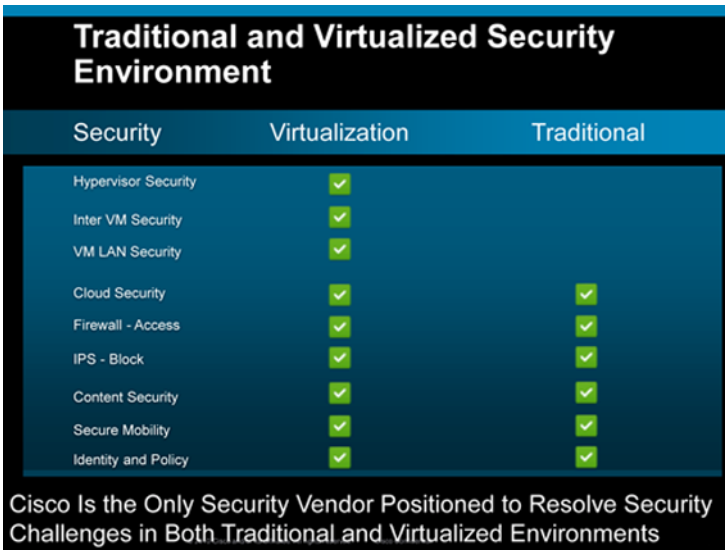
Cisco VXI 対応のセキュアなボーダレス ネットワーク

シスコのボーダレス ネットワークはネットワークに統合されており、適切なデバイスを使用する適切な人に高度にセキュアなリソース アクセス権を付与します。シスコのボーダレス ネットワーク ポートフォリオでは、次のことが可能です。

- コンテキスト連動型の一貫したセキュリティ ポリシーによるデータセンターへのアクセス コントロール
- 仮想化に対応した強化されたアプリケーション パフォーマンスの提供
- 仮想マシン間のトラフィックに対応した強化されたセキュリティ ポリシー
- モビリティとユーザ密度の高い仮想マシンに対するポリシーの一貫性
- セキュアなビデオ、音声、ワイヤレス、データ サービスをリモート ワーカーに配信
- 最新の脅威からシステムが保護されているという信頼性の提供
- 価値のあるデータの保護、ネットワーク アクセスの制御と監視、コンテンツ ポリシーの適用

シスコは、セキュリティ分野においてリーダーシップを発揮し、物理デスクトップと仮想デスクトップの両方のセキュリティ課題を解決できる体制を整えています（図 1）。シスコのエンドツーエンドのセキュリティ アーキテクチャは、仮想環境と仮想環境以外の両方に対応したポリシー策定で優れた拡張性を実現し一貫性を維持します。通常、サーバはサーバ管理者グループによって維持管理されますが、セキュリティ、コンプライアンス、ネットワークはセキュリティ グループやネットワーク グループの領域になります。ほとんどの会社では、セキュリティ ポリシーを適用するグループとサーバの管理を扱うグループが別になっています。セキュリティ ポリシーとコンプライアンスは、エンドツーエンドの実施範囲が 1 つのグループの管理下にある場合に最も適切に処理されます。これにより、セキュリティ管理者は、使い慣れたツールやアプローチ、ポリシーを使用して、仮想マシンなど現在管理していない領域まで管理を広げることができます。

図 1　仮想環境のセキュリティ



仮想化のセキュリティ

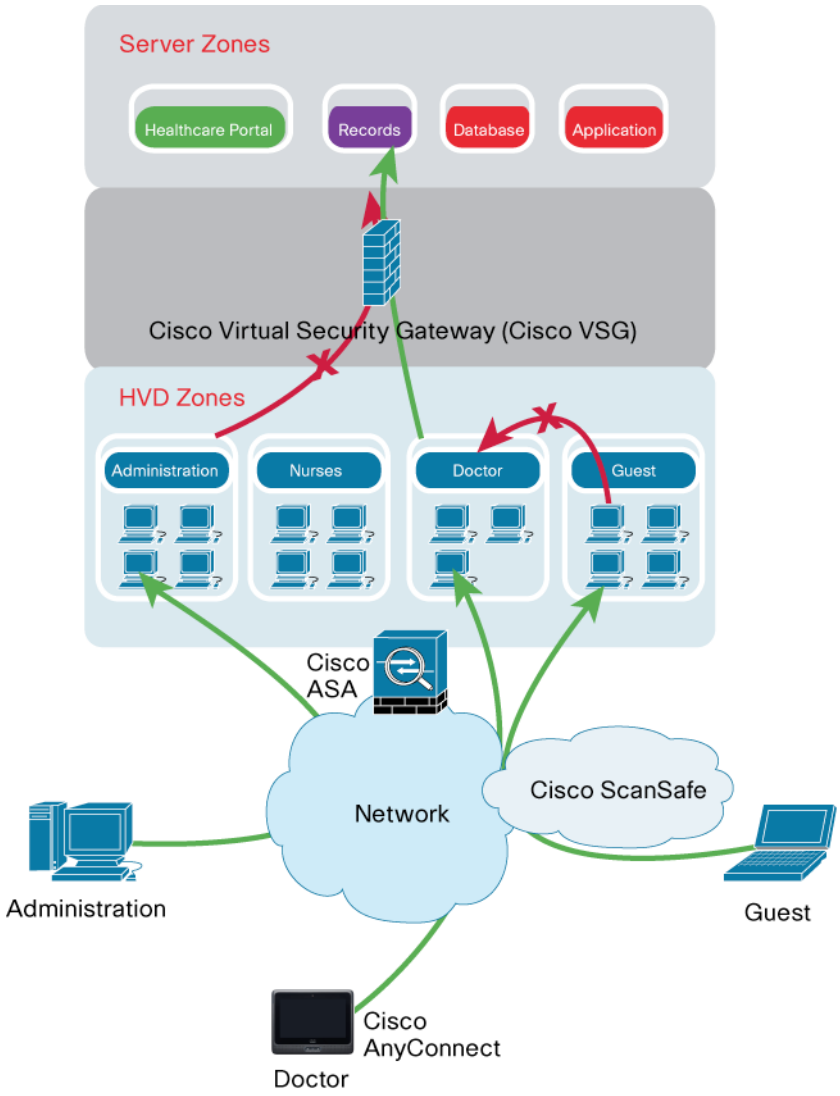
Cisco Nexus 1000V スイッチ：仮想マシンのセキュリティ ポリシーに準拠

Cisco Nexus® 1000V スイッチには、コマンドライン インターフェイス（CLI）と同様の管理インターフェイスが用意されています。ネットワークおよびセキュリティ管理者は、使い慣れた管理インターフェイスを使用して、アクセス ポリシーやその他のパラメータを適用したり、ポートのプロファイルを個別に作成したりできます。これらのポート プロファイルは、サーバ管理者によって仮想マシンに追加され、仮想マシン（および仮想マシンにある仮想デスクトップ）がサーバ間で移行した場合でも、仮想マシンに設定された状態が維持されます。これにより、仮想マシンがホストされる場所に関係なく、ユーザの適切なアクセス ポリシーが仮想マシンで適用されます。

Cisco Virtual Security Gateway：仮想マシン間のファイアウォールと仮想マシンのゾーニング

Cisco Virtual Security Gateway（VSG）は、コンテンツ連動型のセキュリティ ポリシーを使用したゾーンベースのきめ細かい制御と監視により、データセンターの仮想マシンを安全に分割できます（図 2）。組織内の区分（ゾーン）、業務分野、マルチテナント環境にわたって制御できます。コンテンツベースのアクセス ログは、ネットワークおよび仮想マシンの活動レベルで生成されます。信頼できるゾーンとセキュリティ テンプレートは、仮想マシンの作成時にオンデマンドでプロビジョニングできます。これらのゾーンには、同じ用途の仮想マシン（ユーザ デスクトップ ゾーン、ERP アプリケーション ゾーン、Web サーバ ゾーンなど）が配置され、グローバルに適用できます。

図 2　医療業界での使用事例：すべてを統合



Cisco VSG では、仮想ネットワーク サービス データ パス（vPath）テクノロジーを採用し、Cisco Nexus 1000V 分散型仮想スイッチに組み込まれています。Cisco vPath では、指定された Cisco VSG にトラフィックを誘導し、初回のポリシー評価と適用を実行します。以降のポリシー適用は、vPath に直接オフロードされます。Cisco VSG では、複数の物理サーバと仮想マシンにわたって保護できます。

その結果、一般的な医療業界の設定では、たとえば、医師をゾーン 1 に配置し、看護師をゾーン 2 に分離して配置するなどの設定が可能です。医師には、患者の問診表やカルテなどへのアクセス権が付与されますが、看護師のアクセス権は、血圧や心拍数などの数値の入力や血液検査結果の参照などが可能なデータベースに制限することができます。病院管理者は別のゾーン（ゾーン 3）に配置します。病院管理者の業務は患者の記録などではなく、病院の一般管理であるため、カルテなどのデータベースのアクセス権はありません。患者や見舞い客用に 4 番目のゾーン（ゾーン 4、ゲスト ゾーン）を設定することもできます。このゾーンでは、Microsoft Windows 7 の仮想デスクトップ上で実行されるブラウザベースのセキュアなキオスク端末からインターネットにアクセスできます。デスクトップを仮想化してインターネットにアクセスできるようにすることにより、待ち時間中の患者の不満を改善すると同時に、デスクトップの維持管理の負担もなくします。悪意のある活動や、帯域幅を多く消費する活動を IT 管理で軽減したり、ゾーン 3 から隔離ゾーンに仮想マシンを移動するなどの管理上の決定も可能になります。

仮想マシン間のセキュリティ対策をさらに一歩進め、ハイパーバイザ自身のセキュリティを向上することもできます。ハイパーバイザでは、物理ホストのリソースを各仮想マシンがアクセス可能な仮想化リソースに抽象化できます。また、システムの LAN や SAN インターフェイスも管理します。認証および許可された必要な API 呼び出しのみをゲストの仮想マシンからハイパーバイザに実行できるようにすることが不可欠になります。

Cisco AnyConnect および AnyConnect セキュア モビリティ ソリューション

組織には、データセンターのセキュリティだけでなく、ユーザが仮想デスクトップにアクセスする WAN やリモート ブランチ オフィス、SOHO などの環境のセキュリティについても考慮することが求められます。データセンター自体との接続の安全性も確保する必要もあります。HVD には、シン クライアントやゼロ クライアント、転用された PC やビジネス タブレットなど、さまざまなエンド クライアントからアクセスできます。ユーザは、時間や場所を問わず各自の HVD にアクセスを要求することが予想できます。Cisco AnyConnect™ セキュア モビリティでは、SSL を使用して HVD セッションに安全に接続できるだけでなく、ユーザが移動中でも、暗号化されたアクセスを維持できます。常時接続の VPN やセッションの持続性などの Cisco AnyConnect の機能により、最適なユーザ エクスペリエンスが実現します。Cisco AnyConnect には、セキュアなスプリット トンネリング機能があり、トラフィックを企業に誘導したり、Cisco ScanSafe Software as a Service（SaaS）ベースの Web セキュリティに誘導したりできます。Cisco ScanSafe ソリューションは Cisco AnyConnect ソリューションと連動し、ユーザは社内インフラストラクチャの外部から Cisco ScanSafe サービスにアクセスできます。ロケーション連動型の機能と高可用性により、優れたユーザ エクスペリエンスが実現し、オンプレミスとオフプレミスの両方で引き続き Web セキュリティが提供されます。データセンターが地理的に分散して展開されている場合でも、リモート データセンター内の HVD からデータセンターに最も近い Cisco ScanSafe サービスにアクセスできるため、ユーザ エクスペリエンスを犠牲にすることなくセキュリティを向上できます。

脅威に対する防御とシスコのデータ損失防止

データセンター インフラストラクチャを保護するには、仮想マシン間のセキュリティに加えて、ファイアウォールや侵入検知システム（IPS）などの従来型のセキュリティ メカニズムも必要です。データ ストレージとデータセンターのアクセスの統合により、HVD セッションのデータが安全と考えられる場合でも、電子メールや Web からのデータ損失の危険性がなくなるわけではありません。社外秘の文書をユーザが誤って電子メールに添付してしまうこともあります。不適切な内容を Web に投稿してしまい、重要な文書が漏洩してしまうこともあります。シスコのコンテンツ セキュリティでは、HVD に起因する電子メールや Web データの漏洩を防止し続けます

まとめ

シスコでは、進化し続ける新しい仮想化コラボレーション ワークスペースで生じるセキュリティの課題に対処できる体制を整えています。Cisco VXI では、物理環境と仮想環境の両方で、キャンパスの内外、リモート ブランチ、SOHO 環境、ホットスポット、データセンター内など、クライアントからハイパーバイザまでセキュリティの課題に対処できます（表 1）。

表 1 Cisco VXI セキュリティ ポートフォリオ

課題	セキュリティ対象	ソリューション
セキュアなリモート アクセス	シン クライアント、シック クライアント、ゼロ クライアント、スマートフォン、タブレット	Cisco AnyConnect セキュア モビリティ（電子メールおよび Web セキュリティ対応 Cisco AnyConnect 3.0）、サイト間 VPN テクノロジー対応 EasyVPN、DMVPN、GETVPN
仮想化のセキュリティ	ハイパーバイザ、仮想マシン、仮想スイッチ	Cisco VSG、Cisco Nexus 1000V、仮想マシン LAN セキュリティ、PVLAN、IP ソース ガード、DHCP スヌーピング、Address Resolution Protocol（ARP; アドレス解決プロトコル）検査、NetFlow
脅威に対する防御	データセンターの防御	Cisco ASA 5585-X 適応型セキュリティ アプライアンス、ファイアウォール、IPS
アプリケーションおよびコンテンツ セキュリティ	HTTP および XML 攻撃	Cisco IronPort および Cisco ScanSafe アプライアンスを使用した電子メールおよび Web のセキュリティ
セキュアなユーザ仮想エクスペリエンス	表示プロトコルおよびインタラクティブ メディア	セキュアで統合されたデスクトップ仮想化およびセキュアなインタラクティブ メディア エクスペリエンス

Cisco VXI では、次のようなセキュリティ上の利点が得られます

- Cisco Unified Computing System™ および Cisco VN-Link テクノロジーでは、仮想マシンを可視化して仮想マシンのネットワーク セキュリティを可能にし、サーバの仮想ポートに対する複雑なセキュリティ ポリシー適用の課題に対応できます。
- Cisco Nexus 1000V および Cisco VSG では、仮想マシン間のトラフィックを保護し、ユーザ セグメンテーションの課題や、ERP や CRM、Web サービスなどのミッションクリティカルなアプリケーションからの分離の課題に対応できます。ユーザは複数のゾーンに配置され、仮想マシンベースのデスクトップが物理ホスト間で移行された場合でも、各ゾーンには適切なポリシーが適用されます。
- Cisco AnyConnect セキュア モビリティおよび Cisco ASA では、時間や場所に関係なく HVD へのセキュアなアクセスが可能で、シスコの電子メールおよび Web セキュリティと連動することにより、セキュアで生産性に優れたエンド ユーザ エクスペリエンスが実現します。
- Cisco ISE を使用したロールベースのアクセス制限により、ユーザのロールやデバイス、ユーザのポスチャ コンプライアンスに基づいて、ユーザ アクセスの制限の課題に対応できます。

Cisco VXI セキュリティは、以前に仮想化ソリューションを導入したことがないお客様に対しても、HVD に移行中のお客様に対しても、デスクトップ仮想化セキュリティの課題に適切に対応できます。Cisco VXI では、物理システム用のセキュリティのベスト プラクティスを仮想システムに拡大することで、物理デスクトップと仮想デスクトップの共存を可能にし、一貫したセキュリティ ポリシーを両方のアーキテクチャに適用できます。

関連情報

シスコのデスクトップ仮想化ソリューション：http://www.cisco.com/jp/go/vdi/

シスコの仮想化エクスペリエンス インフラストラクチャ：http://www.cisco.com/jp/go/vxi/

お問い合わせ先

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先:シスコ コンタクトセンター
0120-092-255(フリーコール、携帯・PHS含む)
電話受付時間:平日10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

11.07