Cisco Nexus 1000V シリーズ スイッチ向け Cisco Virtual Security Gateway

データ シート

Cisco Nexus 1000V シリーズ スイッチ向け Cisco Virtual Security Gateway

製品概要

Cisco Nexus® シリーズ スイッチ向け Cisco® Virtual Security Gateway（VSG）は、企業およびクラウド プロバイダーの仮想化されたデータセンターに、ポリシーベースのセキュリティを VM レベルで実現する仮想アプライアンスです。Cisco VSG は動的で VM モビリティに透過的なポリシーベースの運用や高密度のマルチテナント向けのスケールアウトに対応しています。企業の IT部門は、Cisco VSG が実現するゾーンベースの制御とアクティビティ モニタリングによるセキュリティ、企業のセキュリティ ポリシーおよび業界規制への準拠の強化、セキュリティ監査の簡素化によって仮想化のメリットを最大限に享受することができます。また、信頼ゾーンへのアクセスがあらかじめ設定されたセキュリティ ポリシーに基づいて確実に制御および監視されるようになります。

主要な機能

Cisco VSG は、Cisco Nexus 1000V シリーズ スイッチと統合し、Cisco NX-OS® ソフトウェアを実行することにより、表 1 に示す機能と利点を提供します。

表 1 機能および利点

機能	説明
信頼できるアクセス	• （仮想マシンの ID、カスタム属性、および 5 タプルのネ ィ ポリシーと細かいゾーンベース別の制御と監視による ーション • 複数の組織ゾーン、ビジネス ライン（LoB）、マルチテ • セキュリティ プロファイル（テンプレート）に整理され
ダイナミックな（仮想化に対応した）運用	• ネットワークおよび仮想マシン レベルのアクティビティ • 仮想マシンのインスタンス作成時の、セキュリティ テン • 異なる物理サーバ間での仮想マシンのライブ マイグレー
混乱を生じない運用管理	• セキュリティ チームとサーバ チームで管理作業を分離

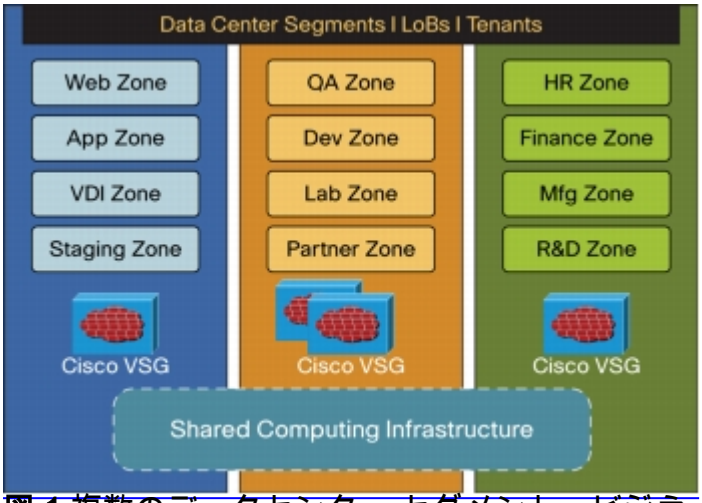

図 1 複数のデータセンター セグメント、ビジネス ライン、およびテナントにわたって信頼ゾーンベースの アクセス コントロールとモニタリングを実現する Cisco VSG

Cisco VSG の総合的な利点は、以下のとおりです。

- 業界規制への準拠の強化
- 仮想化環境における監査プロセスの簡素化
- 幅広い仮想化ワークロードのグループに対するセキュリティ確立によるコスト削減

製品アーキテクチャ

Cisco VSG は、仮想化環境の保護と、優れた効率とアベイラビリティ、高パフォーマンスを実現する制御パスとデータ パスの分割など、高度なネットワークのコンセプトの上に設計されています。VMware vSphere ハイパーバイザにおいて Cisco Nexus 1000V シリーズの分散仮想スイッチと連携して動作する Cisco VSG は、図 2 に示すように、Cisco Nexus 1000V シリーズ Virtual Ethernet Module（VEM）に組み込まれた仮想ネットワーク サービス データ パス（vPath）テクノロジーを利用します。

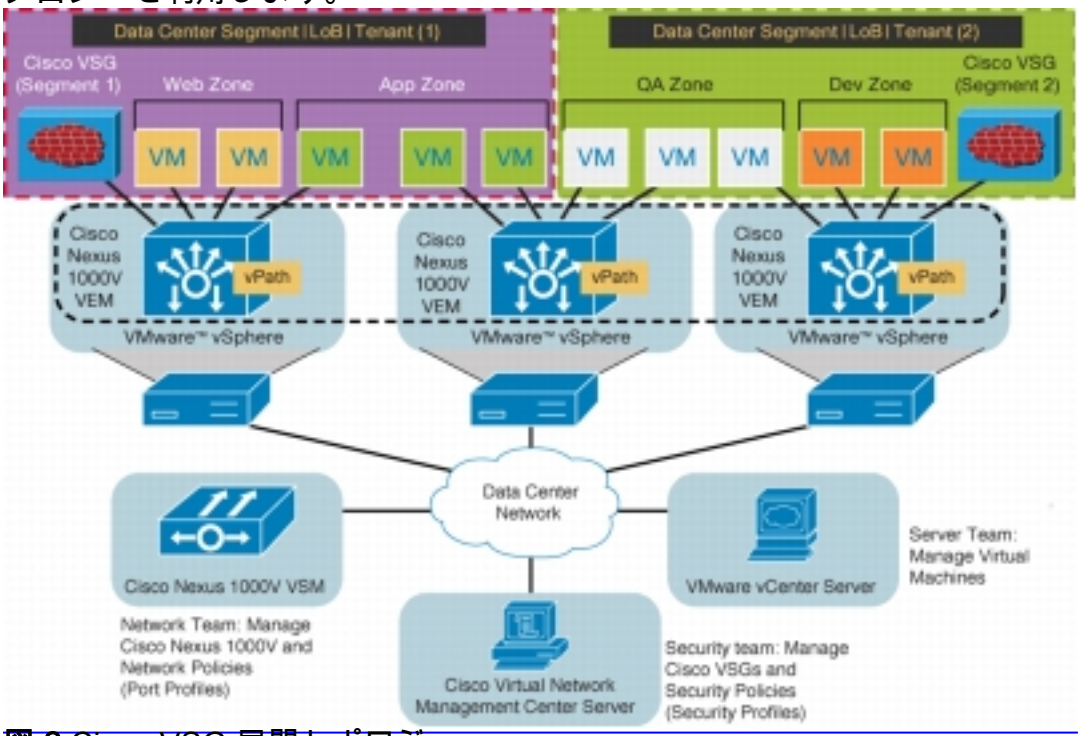

図 2 Cisco VSG 展開トポロジ

Cisco vPath テクノロジーは、トラフィックがインバウンドまたは仮想マシン間であるかに関係なく、指定した Cisco VSG にトラフィックを伝送します。またここでは、Cisco VSG 内で初期

パケットが処理され、ポリシーの評価および施行が実行されるという分割処理モデルが適用されます。その後、パケットに対するポリシー施行は、直接 vPath へとオフロードされます。vPath は以下の機能を提供します。

- **インテリジェントなトラフィック ステアリング**：フローを分類し、該当する Cisco VSG へと転送します。
- **高速なパス オフロード**：Cisco VSG により、フローのポリシー施行を vPath にオフロードします。

vPath は、マルチテナント向けに設計されており、テナント単位のトラフィック ステアリングと高速なパス オフロードを提供します。
Cisco VSG と Cisco Nexus 1000V シリーズ VEM の組み合わせにより、次のような展開の利点が得られます。

- **効率的な展開**：個々の Cisco VSG が複数の物理的なサーバを保護できるため、サーバごとに 1 つの仮想アプライアンスを導入する必要がなくなります。
- **高性能**：Cisco Nexus 1000V シリーズ VEM vPath モジュールに施行をオフロードすることにより、Cisco VSG アーキテクチャのパフォーマンスが向上します。
- **簡素化された運用**：Cisco VSG は、複数のスイッチを作成したり、仮想マシンを一時的に異なるスイッチやサーバに移行させることなく、ワンアーム モードで透過的に挿入できます。ゾーンのスケーリングは、仮想アプライアンスに限定される仮想ネットワーク インターフェイス カード（vNIC）ではなく、セキュリティ プロファイルに基づきます。これらの機能により、セキュリティを危険にさらしたり、アプリケーションの中断を引き起こすことなく、物理的なサーバのアップグレードを容易に行うことができます。
- **ハイ アベイラビリティ**：Cisco VSG は、アクティブスタンバイ モードで展開できます。この方式では、アクティブな Cisco VSG が利用不可能になった場合に vPath がパケットをスタンバイ状態の Cisco VSG にリダイレクトするため、可用性の高い運用環境を保証できます。
- **独立したキャパシティ計画**：Cisco VSG は、セキュリティ チームが制御する専用サーバへの配置が可能です。これにより、アプリケーションの作業負荷に見合ったコンピューティング能力の割り当て、サーバおよびセキュリティチームから独立したキャパシティ計画の実施、セキュリティ、ネットワーク、およびサーバ チーム間の運用上の分離を維持することができます。

信頼できるアクセス

Cisco VSG の強力なセキュリティ分割機能により、IT 部門は自社のデータセンターとクラウド環境をセグメント化できます。Cisco VSG の複数のインスタンスによって、データセンター全体を保護したり、ビジネス ラインやテナントを分割できるため、大規模な展開が可能です。セキュリティ セグメントは隔離されており、トラフィックがセグメント境界をまたがることがありません。Cisco VSG は、ビジネス ラインまたはテナント レベル、仮想データセンター（vDC）レベル、または仮想アプリケーション（vApp）レベルで展開可能です。
仮想マシンは信頼ゾーンに対してインスタンス別に作成されます。このため、セキュリティ プロファイルとゾーン メンバーシップは、Cisco Nexus 1000V シリーズ ポート プロファイルと組み合わされ、直ちに割り当てられます（図 2 参照 ）。セキュリティ プロファイルには、各ゾーンに出入りするトラフィックに対しアクセス ポリシーを指定する、コンテキスト連動のルール セットが含まれます。仮想マシンとネットワーク コンテキストに加えて、カスタム属性により、信頼ゾーンを柔軟かつ拡張可能な方法で定義できます。制御は、ゾーン間のトラフィックだけでなく、外部エリアからゾーン（およびゾーンから外部エリア）へのトラフィックにも適用されます。VLAN はセグメントまたはテナントの境界を特定することが多いため、VLAN 内でのゾーンベースの施行が行われる場合もあります。Cisco VSG は、アクセス コントロール ルールを評価した後、施行を Cisco Nexus 1000V シリーズ VEM vPath にオフロードするため、パフォーマンスが向上します。施行により、許可または拒否のアクションや、オプションとしてアクセス ログが実行されます。Cisco VSG では、アクセス ログを使用したポリシーベースのトラフック モニタリングも実行できます。
vPath のトラフィック ステアリング インテリジェンスにより、複数のハイパーバイザに分散する

ゾーン内の仮想マシンを Cisco VSG が保護するという効率的な展開モデルを実現できます。重複した（プライベートな）アドレス空間をビジネス ラインまたはテナントごとに割り当てることができます。これは、マルチテナント クラウド環境を検討する際の重要なポイントです。Cisco VSG による関連セキュリティ ポリシーの管理および展開は、Cisco Virtual Network Management Center（VNMC）で実行されます（本データシート後述参照）。

ダイナミックな（仮想化に対応した）運用

Cisco VSG では非常にダイナミックな仮想化が可能であり、仮想マシンに対する追加、削除、変更をスムーズに実行できます。仮想マシンのライブ マイグレーションは、手動またはプログラムされた VMware vMotion イベントを通して行われます。図 3 は、図 2 のような構造的な展開が、時間の経過に伴い、このダイナミックな仮想マシン環境によってどのように変化し得るかを示したものです。
Cisco Nexus 1000V シリーズ（および vPath）と連動する Cisco VSG は、ダイナミックな仮想化をサポートします。Cisco VSG および Cisco VNMC により、ビジネス ラインまたはテナントごとに、信頼ゾーンおよび関連するセキュリティ プロファイルが作成されます。セキュリティ プロファイルは、Cisco Nexus 1000V シリーズ ポート プロファイル（Cisco Nexus 1000V シリーズ Virtual Supervisor Module（VSM）で作成され、VMware vCenter に発行される）にバインドされます。新しい仮想マシンのインスタンスが作成されると、サーバ管理者はこの仮想マシンの仮想イーサネット ポートに、適切なポート プロファイルを割り当てます。ポート プロファイルおよびセキュリティ プロファイルと、仮想マシンのゾーン メンバーシップが、直ちに適用されます。仮想マシンは、異なるポートとセキュリティ プロファイルを割り当てるだけで、別の目的に再利用することができます。
VMware vMotion イベントは、複数の物理的サーバ上の仮想マシン動作をトリガーできます。Cisco Nexus 1000V シリーズは、ポート プロファイルとセキュリティ プロファイルの両方が仮想マシンに従うことを保証します。セキュリティの施行と監視は VMware vMotion イベントにかかわらず継続されます。

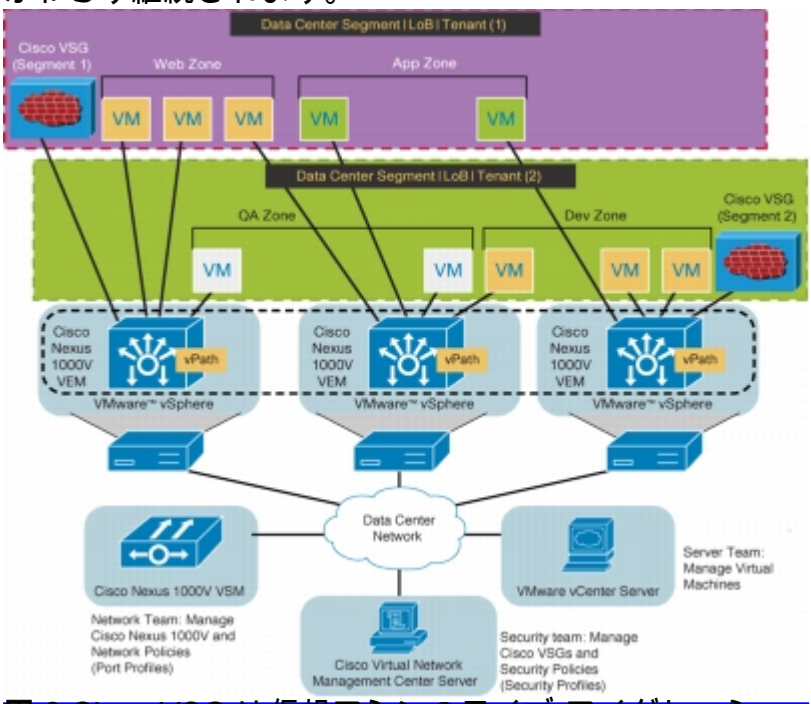

図 3 Cisco VSG は仮想マシンのライブ マイグレーションを行うダイナミックな仮想マシン環境に対してもセキュリティを提供

混乱を生じない運用管理

Cisco VSG ソリューションは、混乱のないスムーズな管理モデルを提供します。これによって、

IT セキュリティ、ネットワーク、およびサーバ担当の各チームは、規制準拠や監査要件の管轄を分離できるだけでなく、相互協力や管理上のエラー削減を実現できます。Cisco VNMC および Cisco Nexus 1000V シリーズ VSM は、次のような混乱の生じない管理モデルを提供します（図 4）。

- セキュリティ管理者は、セキュリティ プロファイルの作成および管理と、Cisco VSG インスタンスの管理を実行できます。セキュリティ プロファイルは、Cisco Nexus 1000V シリーズ ポート プロファイルで参照されます。
- ネットワーク管理者は、ポート プロファイルの作成および管理と、Cisco Nexus 1000V シリーズ分散仮想スイッチの管理を実行できます。ポート プロファイルは、VMware vCenter において、Cisco Nexus 1000V シリーズ VSM のプログラマティック インターフェイスを介して参照されます。
- サーバ管理者は、仮想マシンのインスタンス作成時に VMware vCenter において適切なポート プロファイルを選択できます。

また、サードパーティ管理および統合ツールは、XML API を介してプログラムによって相互に作用することができます。Cisco VNMC により、Cisco VSG の自動管理およびプロビジョニングが行われます。

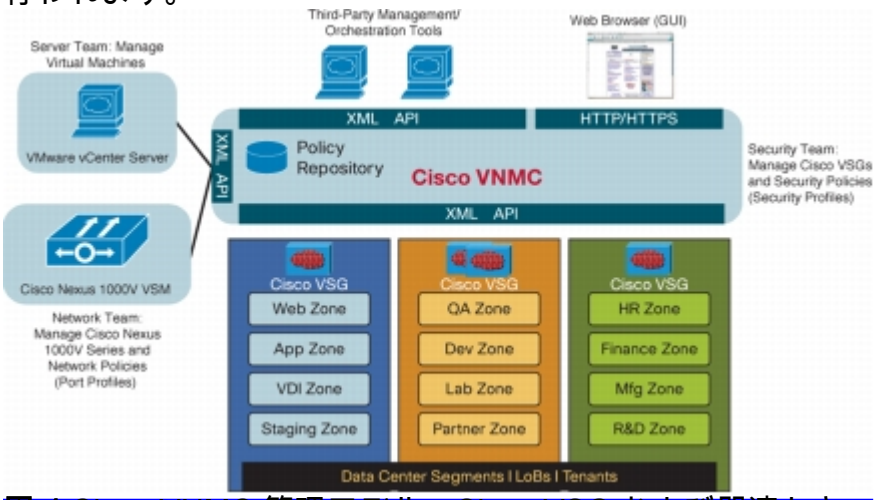

図 4 Cisco VNMC 管理モデル：Cisco VSG および関連セキュリティ プロファイルの管理

展開における検討事項

複数のビジネス ラインまたはテナント、vDC、および vApp にわたる多様な使用例をサポートするために、Cisco VSG は、非常に柔軟でシンプルな展開モデルを提供します。各ビジネス ラインまたはテナントには、複数の仮想マシン ゾーン、vDC、および vApp を含めることができます。vDC にも、複数の仮想マシン ゾーンや vApp を含めることができます。図 5 に、このような展開シナリオをいくつか示します。たとえば、セグメント 1 の仮想マシン ゾーン、vDC、および vApp を保護するには、ビジネス ラインまたはテナントの Cisco VSG を展開することができます。セグメント 2 に対しては、vDC 単位で Cisco VSG を展開し、セグメント 3 に対しては、vApp 単位で Cisco VSG を展開することができます。

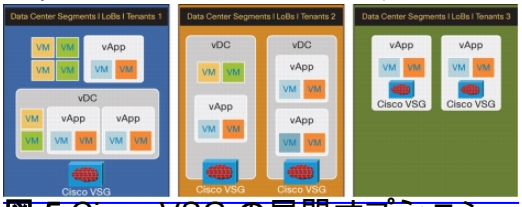

図 5 Cisco VSG の展開オプション
※画像をクリックすると、大きな画面で表示されます

ソリューションの展開要件

Cisco VSG を使用して仮想化環境を適切に保護するためには、表 2 に示す製品による展開が必要です。

表 2 Cisco VSG の展開要件

製品	要件
ハイパーバイザ	• VMware vSphere 4.0 またはそれ以降（VMware ESX または ESXi 搭載） • VMware vCenter
分散仮想スイッチ	Cisco Nexus 1000V シリーズ ソフトウェア リリース 1.4 またはそれ以降（以下を含 • VSM（仮想アプライアンスとして展開、または Cisco Nexus 1010 Virtual Servi Appliance 上でホスティング） • VEM（VMware vSphere ESX または ESXi ハイパーバイザに組み込み）
信頼できるアクセス管理	Cisco VSG（仮想アプライアンスとして展開）
	Cisco VNMC（仮想アプライアンスとして展開）

製品仕様

表 3 に、Cisco VSG で提供される製品機能を示します。

表 3 Cisco VSG の機能

機能	説明
信頼ゾーン	• ゾーン定義：IP アドレス、カスタム属性、仮想マシン属性に基 • ゾーン メンバーシップ：仮想マシンは複数のゾーンに設定可能 • ポリシー モデル：ルール、条件、およびアクションで構成 • ポリシーの施行：ゾーン内、ゾーンとゾーンの間、および外部エ • 許容される属性（特定条件） ネットワーク属性：送信元 IP アド ート、およびプロトコルカスタム属性：ユーザ定義仮想マシン属
セキュリティ ポリシーとセキュリティ プロファイル	• サポートされる演算子（特定条件） containsequal_togreater_thanin_rangeless_thanmember_ofprefix • ポリシー アクション：許可（permit）、破棄（drop）、ログ（l • syslog によるポリシーのロギング • セキュリティ プロファイル： Cisco VNMC によるテンプレート マシン属性のために VMware vCenter と統合し、ダイナミック リーズ VSM ポート プロファイルと統合
ポリシーの決定および施行	• ポリシーの決定は、Cisco VSG で実施 • ポリシーの施行は、Cisco VSG で実施するか、または、（Cisco ）vPath にオフロード
ネットワーク	• ステートフル パケット インスペクションのサポート（FTP など • IEEE 802.1Q VLAN のカプセル化 • トラフィック タイプ：ユニキャスト、ブロードキャスト、マル ロトコル（UDP）
マルチテナント（スケールアウト）	• ジャンボ フレームのサポート（最大 9,216 バイト） • セグメントまたはテナントごとに 1 つ以上の Cisco VSG を展開 • セグメントまたはテナントごとに、重複する（プライベートな
ハイ アベイラビリティ	ハイ アベイラビリティ ペアとして展開された場合のアクティブスタ
展開	ワンアーム モードを用いた Cisco Nexus 1000V シリーズ スイッチ環
オペレーティング システム	Nexus 1000V シリーズ VEM vPath モジュールによって Cisco VSG Cisco NX-OS：モジュラリティ、復元力、サービサビリティが基盤 ィング システム
管理	• Cisco VNMC の GUI およびポリシーベースの管理

ソフトウェアのパッケージ	• Cisco NX-OS CLI（コマンドライン インターフェイス）コンソ • ネットワーク タイム プロトコル（NTP）RFC 1305 • syslog 準拠のアクセス ログ • セキュア シェル バージョン 2 • SSHv2） • Telnet • 簡易ネットワーク管理プロトコル（SNMP）（read）バージョン • Open Virtualization Format（OVF）：拡張子 .ova が付いた単一 OVF 仮想アプライアンス • ISO：仮想マシン上にマウントできる、ダウンロード可能な ISO

保証

Cisco Nexus 1000V シリーズ スイッチ向け Cisco Virtual Security Gateway には、90 日間の限定ソフトウェア保証が適用されます。保証の詳細については、http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html を参照してください。

サービスおよびサポート

Cisco Software Application Support plus Upgrades（SASU）は、お客様のビジネスクリティカルなアプリケーションのアベイラビリティ、セキュリティ、パフォーマンスの維持および向上を支援する包括的なサポート サービスです。Cisco SASU には、以下のリソースが含まれます。

- **ソフトウェアのアップデートおよびアップグレード**：Cisco SASU サービスは、ソフトウェアのアップデートおよびアップグレードに対する適時かつ中断のないアクセスを提供し、お客様の既存のシステムの安定性を保つとともに、ネットワーク リリース レベルを最新状態に維持します。ライセンス対象機能に対する重要なアーキテクチャ上の変更や、新機能を含む主要アップグレードなどのリリースは、Cisco.com からのソフトウェア ダウンロードまたは CD-ROM を介して利用できます。
- **Cisco Technical Assistance Center（TAC）**：Cisco TAC エンジニアが、ソフトウェア アプリケーションの問題に対する正確で迅速な診断および解決を提供し、お客様の業務中断やパフォーマンス低下を低減します。これらの専門ソフトウェア アプリケーションのエキスパートは、Cisco Nexus 1000V シリーズ スイッチ向けの Cisco VSG をサポートするための高度なトレーニングを受けています。お客様はこれらの専門知識を、電話、FAX、電子メール、またはインターネットによって 24 時間年中無休で利用することができます。
- **オンライン サポート**：Cisco SASU は、お客様の迅速な問題解決、業務の継続、競争力の強化をサポートする、幅広いオンライン ツールおよびコミュニティへのアクセスを提供します。

詳細情報

- Cisco Virtual Security Gateway の詳細と無料評価版については、http://www.cisco.com/jp/go/vsg/ にアクセスしてください。
- Cisco Nexus 1000V シリーズの詳細については、http://www.cisco.com/jp/go/nexus1000/ を参照してください。