McAfee Virtual Network Security Platform

クラウド ネットワークを保護する完全な脅威検知と侵入防止

McAfee® Virtual Network Security Platform（McAfee vNSP）は、プライベート クラウドとパブリック クラウド固有の要件を満たすネットワーク脅威/侵入防止システム（IPS）です。クラウド アーキテクチャに侵入する巧妙な脅威を的確に検知し、迅速にブロックします。ワークロードを保護し、コンプライアンスを維持できます。シグネチャレスの検知、インライン エミュレーション、シグネチャを利用した脆弱性の修復など、高度な技術を搭載しています。効率的なワークフロー、複数の統合オプション、分かりやすいライセンス体系が用意されているため、セキュリティの管理を簡単に行うことができます。現在だけでなく将来のニーズにも対応できます。

完全なパブリック クラウド セキュリティ

パブリック クラウドは利便性が高く、導入でコストを削減するだけでなく、設備投資型から運用コスト型への転換を図ることができます。しかし、新しい次元のリスクも存在します。どこからでもアクセスできるソフトウェアの脆弱性が悪用され、クラウドが使用不能になったり、重要な情報が盗まれる可能性があります。また、同じサービスを利用している他のテナントに顧客情報が誤って露出する可能性もあります。McAfee vNSPは、Amazon Web Services（AWS）、Microsoft Azure、Oracle Cloud Infrastructure（OCI）、最先端のパブリック クラウド サービスに対応しています。脅威を完全に可視化し、インターネット ゲートウェイを通過するデータだけでなく、サーバー間で移動するデータ（East-Westトラフィック）も保護します。

仮想化環境の保護

プライベート クラウドやパブリック クラウドなど、仮想インフラを採用する企業が急速に増えています。仮想環境では、物理的なサーバーが複数の仮想マシン（VM）を同時にホスティングし、実行しています。また、仮想化されたワークロード全体がホスティングされている場合もあります。VM間の通信でワークロードの移行、複製、バックアップが迅速に行われるため、プライベート/パブリック クラウドやソフトウェア定義データセンター（SDDC）内部で大量のトラフィックが発生しています。ネットワークの仮想化で、トラフィック フローの柔軟性が増し、予測不能な状態になっています。この状況に対応するため、仮想環境を保護するセキュリティ ソリューションは柔軟性と拡張性に優れていなければなりません。また、持続時間の短いVMや、ワークロードの調整を行うソフトウェア定義ネットワーク（SDN）のプラットフォームでも、シームレスに機能しなければなりません。

主な特長

- プライベート クラウドとパブリック クラウド（AWS、Azure、OCI）を保護する包括的なセキュリティ
- East-Westトラフィックを保護
- 環境を可視化し、一元管理する集中管理コンソール
- 既知の脅威だけでなく、未知の脅威も阻止する高度な検査技術
- 高可用性、障害時復旧、負荷分散
- クラウド ライセンスの共有で、プライベート クラウドとパブリック クラウドに柔軟にアクセス
- 他のMcAfeeポートフォリオとの統合で、デバイスからクラウドまでを網羅
- AWS Marketplaceで使用可能
- Azure Marketplaceで使用可能

McAfeeとつながる

プライベート クラウドへの対応

McAfee vNSPは、VMware NSXやOpenStackベースのSDN環境など、よく利用されているプライベート クラウド プラットフォームとシームレスに統合されます。McAfee vNSPは、VMware NSXでの動作が保証されている唯一の仮想環境専用IPSソリューションです。仮想環境内でVMのマイクロセグメンテーションとサーバー間トラフィックに対するディープ インスペクションが自動的に行われます。ワークロードの作成、移行、回収が急に発生しても対応できます。

高度な脅威対策

McAfee vNSPは、次世代の検査アーキテクチャをベースにし、仮想ネットワークのトラフィックを詳細に検査します。完全なプロトコル分析、脅威レピュテーション、動作分析、高度なマルウェア分析などの調査技術により、ネットワークに対する既知の脅威と未知のゼロデイ攻撃を検出し、被害を未然に防ぎます。

単独のマルウェア検出技術だけではすべての攻撃を防ぐことはできません。McAfee vNSPは複数のシグネチャを多層的に利用します。また、シグネチャを使用しない検出エンジンで、クラウドへのマルウェアの侵入を防ぎます。ブラウザー、JavaScript、Adobeファイルのインライン エミュレーション、ボットネットとマルウェアのコールバック検出、挙動によるDDoS検出、クロスサイト スクリプティングやSQLインジェクションなど、高度な攻撃を阻止する様々な検査技術を搭載しています。

また、McAfee vNSPは、詳細な動作分析を行うMcAfee Advanced Threat Defenseとの統合により、ステルス性の高い脅威を識別し、ブロックします。McAfee Advanced Threat Defenseは、静的なコード分析（マルウェア サンドボックス）と**機械学習**を組み合わせて、回避技術を駆使したゼロデイ脅威やランサムウェアの検出能力を強化しています。McAfeeでは、マルウェア対策でネイティブのSnortシグネチャもサポートしています。

柔軟なクラウド ライセンス共有

自社のITリソースとインフラを複数のクラウドやプラットフォームに分散する企業が増えています。古いアプリケーションを利用する、特定のベンダーへの依存度を下げる、システムに冗長性を持たせる、コストを削減するなど、その理由は様々です。仮想環境のセキュリティ ソリューションは、ライセンスが複雑で高額になる場合もあります。プライベート クラウドとパブリック クラウドでライセンスが別であったり、SDNプラットフォームの種類ごとにライセンスが必要になることもあります。

McAfeeでは、クラウド ライセンス共有により、ライセンス体系を簡素化しました。これにより、パブリック クラウドとプライベート クラウドのプラットフォームをどのように組み合わせても、McAfee vNSPのスループットとライセンスを共有し、コストを抑えることができます。クラウド ライセンス共有で柔軟性だけでなく、セキュリティも向上します。複雑なライセンスを管理したり、手間のかかる調達手順を踏むことなく、クラウド内でトラフィックの保護と仮想ワークロードのマイクロセグメンテーションを迅速に行うことができます。

詳細情報

- **Amazon Web Services仮想ネットワークの保護**
- **Microsoft Azure仮想ネットワークの保護**

優れたワークフローと分析機能

最近の脅威は大量のアラートを生成します。この中から重要な兆候を見つけ出し、追跡することは容易ではありません。対応に手間取れば、実際の脅威を見逃してしまうこともあります。McAfee vNSPには、高度な分析機能と有益なワークフローが搭載されています。複数のIPSアラートが相関分析されて1つの有益なイベントとして提供されるため、関連情報を迅速に把握できます。また、他のMcAfeeセキュリティ ソリューションとの統合により、ネットワークの脅威を検知・回避する真に包括的なプラットフォームを構築できます。

集中管理により、リアルタイムの可視化と制御を実現

1つのMcAfee Network Security Managerアプライアンスにより、Webベースで可視化と制御をリアルタイムで簡単に行うことができます。最先端のコンソールにより、1つのウィンドウでデータをリアルタイムで確認できます。物理ネットワーク、プライベート クラウド、パブリック クラウドにあるMcAfee Network Security PlatformアプライアンスとMcAfee Network Threat Behavior Analysisアプライアンスの管理、設定、モニタリングを簡単に行うことができます。分かりやすいインターフェースにより、広範囲に分散している重要なクラスターを簡単に管理できます。

VMware ESXサーバーや、AWSまたはAzure 環境にMcAfee Network Security Managerを仮想インスタンスとして配備することもできます。McAfee vNSPはAWS Identity and Access Management（IAM）に対応しています。特定のユーザーとグループの権限に基づいて、AWSサービスとリソースに対するアクセスを簡単かつ安全に管理できます。

高可用性、障害時復旧、負荷分散

McAfee vNSPは、複数の方法で中断のない管理、保護、パフォーマンスを自動的に提供します。McAfee Network Security Managerは、環境をプロアクティブにモニタリングすることで、高可用性を実現しています。アクティブなコントローラーが使用不能になると、McAfee Network Security Managerはスタンバイ コントローラーに自動的にフェールオーバーし、可視化とセキュリティを途切れなく維持します。さらに、障害時復旧のために、スタンバイ状態のMcAfee Network Security ManagerをAWS、Azure、OCI環境に配備できます。

McAfee vNSPは、IPSセンサーにも高可用性を提供します。センサーが使用不能になると、自動スケーリング機能により、新しい仮想IPSセンサーがシームレスに生成され、中断のないセキュリティを提供します。ネットワーク トラフィックが増加すると、センサー間で自動的に負荷分散が実行され、最適なパフォーマンスを維持します。また、必要なスループット要件を満たすために、追加のセンサーを自動的に配備できます。

統合セキュリティ

巧妙な攻撃はインフラのギャップ、特に、セキュリティ製品間のギャップを攻めてきます。McAfee vNSPは、複数のセキュリティ製品をシームレスに統合する唯一のIPSです。ソリューション間でデータとワークフローを効率的に利用することで、セキュリティを強化し、ROIを増加できます。統合可能なMcAfeeセキュリティ ソリューションとしては、次のようなものがあります。

- **McAfee ePolicy Orchestrator® (McAfee ePO™):** エンドポイントのIPSイベントとアラートを完全に可視化
- **McAfee Endpoint Intelligence Agent:** ネットワークとエンドポイントを監視し、データの流出を阻止
- **McAfee Enterprise Security Manager:** 詳細なデータを共有し、IPSアラートで隔離
- **McAfee Threat Intelligence Exchange:** 異なる種類のデバイスで情報を共有
- **McAfee Global Threat Intelligence:** 世界最大規模の包括的なレピュテーション サービス
- **McAfee Network Threat Behavior Analysis:** ネットワークの可視性を強化
- **McAfee Virtual Advanced Threat Defense:** 詳細な調査により、検出を回避する脅威を検知
- **McAfee Cloud Threat Detection:** 既存のMcAfeeセキュリティ ソリューションのプラグインとして機能し、高度なマルウェアを検出
- **McAfee Management for Optimized Virtual Environments (McAfee MOVE):** 仮想環境のウイルス対策ソリューション
- **サードパーティの脆弱性スキャナー:** ホストとエンドポイントのリスクを分析

追加機能

高度な脅威対策

- McAfee Gateway Anti-Malwareエミュレーション エンジン
- PDF JavaScriptエミュレーション エンジン(軽量のサンドボックス)
- Adobe Flash動作分析エンジン
- 高度な回避技術の阻止

ボットネット/マルウェア コールバック対策

- ドメイン名サーバー(DNS)/ドメイン生成アルゴリズム(DGA) Fast-Fluxコールバック検出
- DNSシンクホール
- ボットのヒューリスティック検出
- 複数の攻撃を相関分析
- 指令サーバーのデータベース

高度な侵入防止

- IPデフラグとTCPストリームの再構築
- 様々なシグネチャを使用(McAfee提供、ユーザー定義、オープンソース)
- ホストの隔離とレート制限
- 仮想環境の検査
- サービス拒否(DoS)/分散サービス拒否(DDoS)対策
- STIX(Structured Threat Information eXpression)のサポートでホワイトリスト/ブラックリストの機能強化(STIX)
- しきい値とヒューリスティックによる検出
- ホストベースの接続制限
- Snortシグネチャのネイティブ サポート
- 自己学習、プロファイル ベースの検出

McAfee Global Threat Intelligence

- ファイル レピュテーション
- IPレピュテーション
- 位置情報によるアクセス制御
- IPアドレスによるアクセス制御

	センサーの種類1	センサーの種類2
プラットフォーム	VMware ESX 5.5/6.0/6.5	AWS Azure OCI VMware vSphere 6.5、NSX 6.3
仮想IPS Sensorモデル	IPS-VM600	IPS-VM600-VSS
仮想IPS環境の種類	スタンドアロン	分散型
VMware NSXのサポート	なし	あり
AWSのサポート	なし	あり
Azureのサポート	なし	あり
OCIサポート	なし	あり
論理CPUコア数	4	AWS 4、Azure 5
必要なメモリー	6 GB	6 GB
ストレージ	8 GB	8 GB
仮想センサーの仕様		
最大スループット	最大1 Gbps	最大1 Gbps
モニタリング ポート ペア数	3	1（ポート ペアでなくモニタリング ポート）
1センサー当たりの仮想インターフェース（VIDS）	100	100
DoSプロファイル	300	300
マネジメント ポート	あり	あり
レスポンス ポート	なし	なし
配備モード	VM間の検査、物理環境とVM間での検査、物理環境間での検査、SPAN/インライン ポートの検査	

McAfeeテクノロジの機能はシステム構成に依存します。機能を十分に活用するため、対応のハードウェア、ソフトウェア、サービスの利用が必要になる場合があります。詳細については、www.mcafee.com/jpをご覧ください。絶対安全なネットワークはありません。

〒150-0043
東京都渋谷区道玄坂 1-12-1
渋谷マークシティ ウエスト 20F
Tel. 03-5428-1100（代表）
www.mcafee.com/jp