

# McAfee Network Security Platform

## ネットワークセキュリティに対する包括的で、インテリジェントなアプローチ

McAfee® Network Security Platform (McAfee NSP) は、ネットワーク上の高度なマルウェアを検出し、ブロックする次世代の侵入防止システム (IPS) です。単なるパターンの比較を超えた高度な検出機能とエミュレーション技術により、ステルス型攻撃を非常に高い精度で検出し、被害を未然に防ぎます。このプラットフォームは、条件の厳しいネットワークでも1台のデバイスで40 Gbpsを超える処理速度に対応できます。McAfeeの統合ソリューションにより、脅威情報がMcAfee Global Threat Intelligenceからリアルタイムで提供されます。ユーザー、デバイス、アプリケーションに関するコンテキストデータにより、ネットワークに対する攻撃を迅速に検出し、的確な対応を行うことができます。

### ステルス型脅威の阻止

従来の検出方法を回避し、多大な被害をもたらす高度なステルス型攻撃が増えています。万全な防御に必要なツールと技術を導入して管理するには多大な費用とリソースが必要になります。大半の企業はこの点が課題となっています。

McAfee NSPは、インテリジェントな脅威対策と使いやすい管理機能を搭載した統合ネットワークセキュリティプラットフォームです。これにより、検出精度が向上し、セキュリティ管理の負担が軽減されます。1つのマルウェア検出技術だけでなくすべての攻撃を防ぐことはできません。McAfee NSPは複数のシングネチャを多層的に利用します。シングネチャを使用しない検出エンジンも使用します。完全なプロトコル分析、脅威レピュテーション、動作分析などの高度な技術でネットワークトラフィックを分析し、マルウェアのコールバック、サービス拒否攻撃 (DoS)、ゼロデイ攻撃などの高度な脅威を阻止します。

### 統合セキュリティ

McAfee Network Security Platformは、McAfee Advanced Threat Defenseの統合により、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、回避技術を駆使する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 NSPは、McAfee Global Threat Intelligenceからファイルレピュテーションを取得し、McAfee® ePolicy Orchestrator®とMcAfee Enterprise Security Managerを利用して、ネットワークイベントの相関分析をリアルタイムで行います。これにより、デバイスの詳細、ユーザーの情報、エンドポイントセキュリティの状況、脆弱性評価などの情報を利用して、脅威の状況とビジネスに対するリスク要因を正確に把握します。

### 主な特長

- 脅威を迅速に検出してブロックし、アプリケーションとデータを保護
- 環境の変化に対応できる、高性能でスケーラブルなソリューション
- 可視性と統制を一元管理
- シングネチャレスのマルウェア分析を含む高度な検出
- 送受信トラフィックのSSLを復号化し、ネットワークトラフィックを検査
- 高可用性と障害時復旧
- 仮想アプライアンスも使用可能
- 他のMcAfeeソリューションとの統合でデバイスからクラウドまでを保護



McAfeeとつながる



## データシート

### パフォーマンスと可用性

McAfee Network Security Platformは、高性能を維持しながら高度なセキュリティを提供します。このソリューションは、シングルパスでプロトコル別の検査アーキテクチャを高品質なデバイスで実行します。1台のデバイスで40 Gbpsを超えるトラフィックを検査します。セキュリティの設定に関係なく、パフォーマンスを維持できます。他のIPSでは、パフォーマンスよりもセキュリティを重視したポリシーを使用するとスループットが最大で50%低下します。

McAfee NSPIはアクティブ/アクティブとアクティブ/パッシブのステートフル フェールオーバー構成を提供し、高可用性のSLAを実現しています。アプライアンスの性能が低下したり、単独のソリューションが過負荷状態になることはありません。

### 可視性と統制

ネットワーク上のアプリケーションとプロトコルに関する豊富な情報を利用して選択を行う必要があります。McAfee Network Security Platformは、高度脅威の検出とアプリケーションの認識を行う業界初のIPSソリューションで、1つのセキュリティ エンジンで意思決定を行うことができます。アプリケーションの利用状況と脅威のアクティビティを関連付けて分析します。たとえば、第7層で実行されている1,500以上のアプリケーションとプロトコルを視覚的に管理し、ネットワークで許可するアプリケーションを選択できます。

McAfee NSPIは、アプリケーションだけでなく、ユーザーとデバイスも識別します。ネットワークの異常動作を識別し、アクティブなボットネットなど、危険なホストとユーザーに優先的に対応できます。

### インテリジェントで、スケーラブルなセキュリティ管理

セキュリティに対する投資を無駄にしないため、インテリジェントなネットワーク セキュリティを利用する必要があります。McAfee Network Security Managerの拡張性に優れたWebベースのコンソールを使用すると、2台から数百台のネットワーク セキュリティ アプライアンスを管理できます。分かりやすいワークフローでアラートをすぐに確認できます。セキュリティ ダッシュボードでは、セキュリティと関連性に基づいてイベントの優先度が自動的に設定されます。

### 追加機能

#### 高度な脅威対策

- 受信SSL (Secure Sockets Layer) の復号化は、エージェントベースの共有キーを使用し、Diffie-Hellman (DH) 暗号とElliptic-Curve Diffie-Hellman (ECDH) 暗号に対応します。センサーのパフォーマンスに影響を及ぼすことはありません (NSシリーズ用の機能で、特許出願中です)。
- 送信SSL復号化 (NSシリーズ)
- 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
- Adobe Flash動作分析エンジン
- 高度な回避技術の阻止
- モバイル脅威のレピュテーションとクラウド分析

## データシート

### ボットネット/マルウェア コールバック対策

- DNS/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)
- Snortシグネチャのネイティブ サポート (NSシリーズ)
- 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 (NSシリーズ)
- ホストの隔離とレート制限
- 仮想環境の検査
- McAfee Advanced Threat Defenseとの統合
- HTTP応答圧縮解除サポート

### DoS/DDoS対策

- 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
- 自己学習、プロファイル ベースの検出

### McAfee Global Threat Intelligence

- ファイルとIPのレピュテーション
- アプリケーションとプロトコルのレピュテーション
- 位置情報
- McAfee Global Threat Intelligenceのカテゴリに基づくホワイトリスト

### 高可用性

- アクティブ/アクティブとアクティブ/パッシブのステートフルフェールオーバー
- 外部フェールオープン (アクティブ)
- 組み込みのフェールオープン

### プロトコル トンネリング サポート

- IPv6
- V4-in-V4、V4-in-V6、V6-in-V4、V6-in-V6トンネル
- MPLS
- GRE
- Q-in-QダブルVLAN

### McAfee Network Security Manager

- 多層型の管理 (最大1,000台のセンサー)
- ユーザー認証 (RADIUS、LDAP)
- 自動フェールオーバー/フェールバック
- 重要な構成データの障害時復旧
- ポリシーを階層的に一元管理
- ダッシュボードにデバイスのメモリー使用率を表示

### 詳細情報

詳細と物理アプリケーションのオプションについては、**McAfee Network Security Platform仕様シート**をご覧ください。



〒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](http://www.mcafee.com/jp)

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](http://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。

McAfee、McAfeeのロゴ、ePolicy Orchestratorは米国法人McAfee, LLCまたは米国またはその他の国の関係会社における登録商標または商標です。その他すべての登録商標および商標はそれぞれの所有者に帰属します。Copyright © 2018 McAfee, LLC. 3795\_0418  
2018年4月