McAfee Network Security Platform

ネットワーク セキュリティに対するインテリジェントなアプローチ

McAfee® Network Security Platformは、巧妙なネットワーク脅威を検出して阻止するインテリジェントなセキュリティ ソリューションです。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。この次世代のハードウェア プラットフォームは処理速度が40Gbpsを超え、条件の厳しいネットワークでも1台で要件を満たすことができます。弊社のセキュリティ管理アプローチにより、脅威情報がMcAfee Global Threat Intelligence（McAfee GTI）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。

主な特長

最高の高度脅威対策

- シグネチャを使用しない高度なマルウェア分析
- ブラウザー/JavaScript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 コールバックを検出する高度な機能
- 動作分析とDDoS対策
- McAfee Advanced Threat Defenseとの統合

統合防御アーキテクチャ

- McAfee Threat Intelligence Exchange（TIE）で脅威情報をリアルタイムで共有
- ePolicy Orchestrator®（McAfee ePO™）によるエンドポイントの管理
- McAfee Endpoint Intelligence Agentによるエンドポイント プロセスの相関分析
- McAfee Enterprise Security Manager（SIEM）によるデータ共有と隔離
- McAfee Vulnerability Managerによるホスト リスクの分析
- McAfee GTIによるプロアクティブなマルウェア検出

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が、大半の企業はこの点が課題となっています。

McAfee Network Security Platform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、検出精度を向上し、セキュリティ管理の負担を軽減できます。高度な脅威、マルウェア コールバック、ゼロデイ脅威、サービス拒否攻撃など、様々な脅威から組織を保護できます。マカフィーの統合防御アーキテクチャに完全に組み込まれているMcAfee Network Security Platformは、組織の様々なセキュリティ データを利用し、単体のセキュリティ ソリューションでは対応できない脅威も阻止します。

最高の脅威対策

McAfee Network Security Platformは、次世代の検査アーキテクチャを採用し、回線の通信速度に影響を及ぼすことなく、ネットワーク トラフィックに詳細な検査を行います。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、ネットワーク上の既知の脅威とゼロデイ攻撃を検出し、被害を未然に防ぎます。

包括的なマルウェア対策

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 Network Security Platform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マルウェアの侵入を防ぎます。McAfee GTI、JavaScriptの検査を含む詳細なファイル分析と高度なマルウェア対策エンジンにより、カスタム マルウェアやステルス攻撃を阻止します。

intel Security

主な特長（続き）

パフォーマンスと可用性

- 次世代のアーキテクチャ
- 最大40 Gbpsのスループット
- 最高のSSL検査性能
- 業界最高の信頼性
- アクティブ/アクティブとアクティブ/パッシブの可用性

インテリジェントなセキュリティ管理

- 高度なアラート相関と優先度の設定
- マルウェアの検査情報を表示するダッシュボード
- 事前定義の検査ワークフロー
- 拡張性に優れたWebベースの管理機能

可視性と制御

- アプリケーションの識別
- ユーザーの識別
- デバイスの識別

統合防御アーキテクチャ

必要なデータをすべて揃えるのは簡単なことではありません。マカフィーでは、McAfee ePOとMcAfee Enterprise Security Managerの統合により、関連するネットワーク イベントを相関分析し、その結果をリアルタイムで提供しています。McAfee ePOとMcAfee Enterprise Security Managerの統合により、McAfee Network Security Platformはデバイスやユーザーに関連する脅威を正確に認識し、組織にとって最も危険な対象を識別します。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、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。

性能と拡張性

セキュリティと性能のバランスをとるのは簡単ではありません。McAfee Network Security Platform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。他の侵入防止システム（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。

可視性と制御

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に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ソリューションです。この1つのセキュリティ エンジンで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、適切な意思決定を行うことができます。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 Network Security Platform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。McAfee Network Security PlatformはMcAfee ePOに統合されているので、組織全体のリスクとコンプライアンスの状況をすばやく把握できます。システムの脆弱性、ネットワークの保護機能、エンドポイントのセキュリティ レベルを総合的に分析し、危険なインフラを迅速に特定できます。

McAfee Network Security Platformの機能:

セキュリティ ギャップを埋める
- 不正なネットワーク アクティビティをブロック
- ステルス型攻撃を阻止
- 高度なマルウェアを検出

管理上の問題を軽減する
- イベントの優先度を自動的に設定
- 検査ワークフローの簡素化
- 不要な調整を排除

ネットワーク接続
- 1 GigE、10 GigE、40 GigEの接続性
- 最大40 Gbpsまで拡張可能
- アクティブ/アクティブとアクティブ/パッシブの可用性

その他の機能

高度な脅威対策
- McAfee Gateway Anti Malware（GAM）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

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
- 指令制御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
- マカフィー、ユーザー定義、オープンソースのシグネチャを使用
- ホスト隔離とレート制限
- 仮想環境の検査

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 GTI
- ファイル レピュテーション
- IP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

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 フェールオーバー構成
- 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

McAfee Network Security Platformの仕様

		次世代ハードウェア	
			
Sensorハードウェア コンポーネント	**NS9300**	**NS9200**	**NS9100**
パフォーマンス			
集約パフォーマンス	40 Gbps	20 Gbps	10 Gbps
最大スループット（UDP 1512バイトパケット）	最大70 Gbps	最大35 Gbps	最大30 Gbps
同時接続の最大数	32,000,000	16,000,000	13,000,000
1秒あたりの接続数	1,000,000	575,000	450,000
1秒あたりのHTTP接続数	750,000	375,000	260,000
SSL復号のスループット（全体10%がSSLトラフィックの場合）	40 Gbps	20 Gbps	10 Gbps
SSLフローの最大数	3,200,000	1,600,000	1,200,000
インポートされるSSLキー	1,024	1,024	1,024
標準的な待機時間	100 µs未満	100 µs未満	100 µs未満
仮想IPSシステムの数	1,000	1,000	1,000
DoSプロファイルの最大数	5,000	5,000	5,000
ACLルール	20,000	20,000	20,000
ポート			
固定Gigabit Ethernet ー 銅線ポート（内部フェールオープン機能搭載）	16	8	8
固定10 GigE/1 GigE（SFP+）ポート	—	—	—
固定40-Gigabit Ethernet	—	2	2
ネットワークI/Oスロット	4	2	2
ネットワークI/Oモジュール（6オプション）		4ポート10 GigE/1 GigE SR Optical 50ミクロン（フェールオープン機能搭載） 4ポート10 GigE/1 GigE SR Optical 62.5ミクロン（フェールオープン機能搭載） 4ポート（QSFP+）40 GigE、 2ポート（QSFP+）40 GigE、 8ポート（SFP+/SFP）10 GigE/1 GigE、 または6ポート（RJ45）1 GigE （内部フェールオープン機能搭載）	
10 Gigabit Ethernet	最大32	最大16	最大16
40 Gigabit Ethernet	最大16	最大10	最大10
専用レスポンス ポート（RJ45）	1（10G/1G/100M）	1（10G/1G/100M）	1（10G/1G/100M）
専用管理ポート（RJ45）	1（10G/1G/100M）	1（10G/1G/100M）	1（10G/1G/100M）
専用ストレージ ポート（RJ45）	1（10G/1G/100M）	1（10G/1G/100M）	1（10G/1G/100M）
物理仕様			
寸法	2 x 2RUラック マウント型 17.24"（W）x 6.88"（H）x 28.76"（D）	2RUラック マウント型 17.24"（W）x 3.44"（H）x 28.76"（D）	2RUラック マウント型 17.24"（W）x 3.44"（H）x 28.76"（D）
重量	134 lbs.	67 lbs.	67 lbs.
ストレージ	600 GB（2 x デュアル ソリッド ステート 300 GB、RAID 1構成）	デュアル ソリッド ステート300 GB、RAID 1構成	デュアル ソリッド ステート300 GB、RAID 1構成
最大消費電力	2260w	1130w	1130w
DC電源	オプション	オプション	オプション
冗長電源	搭載	搭載	オプション
電源	100-240 VAC（50/60Hz）		
温度	0°～35°C（動作時）、-40°～70°C（非動作時）		
相対湿度（結露なし）	動作時: 10%～90% 非動作時: 5%から95%		
高度	0～10,000フィート		
安全性認定	UL 1950、CSA-C22.2 No. 950、EN-60950、IEC 950、EN 60825、21CFR1040 CBライセンスおよびレポートにより、あらゆる国での規格逸脱を補います。		
EMI認定	FCCパート15クラスA（CFR 47）（米国）、ICES-003クラスA（カナダ）、EN55022クラスA（ヨーロッパ）、CISPR22クラスA（国際）		

McAfee Network Security Platformの仕様（続き）

			
Sensorハードウェア コンポーネント	**NS7300**	**NS7200**	**NS7100**
パフォーマンス			
集約パフォーマンス	5 Gbps	3 Gbps	1.5 Gbps
最大スループット（UDP 1512バイトパケット）	最大15 Gbps	最大10 Gbps	最大5 Gbps
同時接続の最大数	10,000,000	5,000,000	3,000,000
1秒あたりの接続数	225,000	200,000	135,000
1秒あたりのHTTP接続数	135,000	128,000	115,000
SSL復号のスループット（全体10%がSSLトラフィックの場合）	5 Gbps	3 Gbps	1.5 Gbps
SSLフローの最大数	500,000	400,000	250,000
インポートされるSSLキー	1,024	1,024	1,024
標準的な待機時間	100 µs未満	100 µs未満	100 µs未満
仮想IPSシステムの数	1,000	1,000	1,000
DoSプロファイルの最大数	5,000	5,000	5,000
ACLルール	5,000	3,000	3,000
ポート			
固定Gigabit Ethernet ー 銅線ポート（内部フェールオープン機能搭載）	8	8	8
固定10 GigE/1 GigE（SFP+）ポート（外部パッシブ フェールオープン キットをサポート）	2	2	2
固定40-Gigabit Ethernet	—	—	—
ネットワークI/Oスロット	2	2	2
ネットワークI/Oモジュール（5オプション）	フェールオープン機能搭載4ポート10 GigE/1 GigE SR Optical 50ミクロン、 フェールオープン機能搭載4ポート10 GigE/1 GigE SR Optical 62.5ミクロン、 フェールオープン機能搭載4ポート10 GigE/1 GigE LR Optical、 8ポート（SFP+/SFP）10 GigE/1 GigE、 または内部フェールオープン機能搭載6ポート（RJ45）1 GigE		
10 Gigabit Ethernet	最大18	最大18	最大18
40 Gigabit Ethernet	—	—	—
専用レスポンス ポート（RJ45）	1（1G/100M/10M）	1（1G/100M/10M）	1（1G/100M/10M）
専用管理ポート（RJ45）	1（1G/100M/10M）	1（1G/100M/10M）	1（1G/100M/10M）
専用ストレージ ポート（RJ45）	1（1G/100M/10M）	1（1G/100M/10M）	1（1G/100M/10M）
物理仕様			
寸法	1RUラック マウント型 17.5"（W）x 1.69"（H）x 28.9"（D）	1RUラック マウント型 17.5"（W）x 1.69"（H）x 28.9"（D）	1RUラック マウント型 17.5"（W）x 1.69"（H）x 28.9"（D）
重量	31 lbs.	31 lbs.	29 lbs.
ストレージ	ソリッド ステート160 GB	ソリッド ステート160 GB	ソリッド ステート160 GB
最大消費電力	350W	350W	250W
DC電源	オプション	オプション	オプション
冗長電源	オプション	オプション	オプション
電源	100-240 VAC（50/60Hz）		
温度	0°～35°C（動作時）、-40°～70°C（非動作時）		
相対湿度（結露なし）	動作時: 10%～90% 非動作時: 5%から95%		
高度	0～10,000フィート		
安全性認定	UL 1950、CSA-C22.2 No. 950、EN-60950、IEC 950、EN 60825、 21CFR1040 CBライセンスおよびレポートにより、あらゆる国での規格逸脱を補います。		
EMI認定	FCC パート15クラスA（CFR 47）（米国）、ICES-003クラスA（カナダ）、EN55022クラスA（ヨーロッパ）、CISPR22クラスA（国際）		

McAfee Network Security Platformの仕様（続き）

		
Sensorハードウェア コンポーネント	**NS5200**	**NS5100**
パフォーマンス		
集約パフォーマンス	1 Gbps	600Mbps
最大スループット(UDP 1512バイトパケット)	最大3 Gbps	最大1.5 Gbps
同時接続の最大数	1,350,000	750,000
1秒あたりの接続数	45,000	40,000
1秒あたりのHTTP接続数	30,000	25,000
SSL復号のスループット（全体10%がSSLトラフィックの場合）	1 Gbps	600 Mbps
SSLフローの最大数	75,000	40,000
インポートされるSSLキー	1,024	1,024
標準的な待機時間	100 µs未満	100 µs未満
仮想IPSシステムの数	1,000	100
DoSプロファイルの最大数	5,000	300
ACLルール	2,000	2,000
ポート		
固定Gigabit Ethernet ー 銅線ポート（内部フェールオープン機能搭載）	8	8
固定1 GigE（SFP）ポート	12	12
固定10 GigE/1 GigE（SFP+）ポート（外部パッシブ フェールオープン キットをサポート）	2	2
固定40-Gigabit Ethernet	—	—
ネットワークI/Oスロット	—	—
ネットワークI/Oモジュール	—	—
10 Gigabit Ethernet	—	—
40 Gigabit Ethernet	—	—
専用レスポンス ポート（RJ45）	1（1G/100M）	1（1G/100M）
専用管理ポート（RJ45）	1（1G/100M）	1（1G/100M）
専用ストレージ ポート（RJ45）	1（1G/100M）	1（1G/100M）
物理仕様		
寸法	1RUラック マウント型17.25"（W）x 1.75"（H）x 24.625"（D）	1RUラック マウント型17.25"（W）x 1.75"（H）x 24.625"（D）
重量	22 lbs.	22 lbs.
ストレージ	ソリッド ステート80 GB	ソリッド ステート80 GB
最大消費電力	225W	225W
DC電源	オプション	オプション
冗長電源	オプション	オプション
電源	100-240 VAC（50/60Hz）	
温度	0°～35°C（動作時）、-40°～70°C（非動作時）	
相対湿度（結露なし）	動作時: 10%～90% 非動作時: 5%から95%	
高度	0～10,000フィート	
安全性認定	UL 1950、CSA-C22.2 No. 950、EN-60950、IEC 950、EN 60825、21CFR1040 CBライセンスおよびレポートにより、あらゆる国での規格逸脱を補います。	
EMI認定	FCCパート15クラスA（CFR 47）（米国）、ICES-003クラスA（カナダ）、EN55022クラスA（ヨーロッパ）、CISPR22クラスA（国際）	

McAfee Network Security Platformの仕様（続き）

Sensorハードウェア コンポーネント	 NS3200	 NS3100
パフォーマンス		
集約パフォーマンス	200Mbps	100Mbps
最大スループット(UDP 1512バイトパケット)	最大1 Gbps	最大600 Gbps
同時接続の最大数	80,000	40,000
1秒あたりの接続数	20,000	15,000
1秒あたりのHTTP接続数	15,000	12,000
SSL復号のスループット（全体10%がSSLトラフィックの場合）	—	—
SSLフローの最大数	—	—
インポートされるSSLキー	—	—
標準的な待機時間	100 µs未満	100 µs未満
仮想IPSシステムの数	32	16
DoSプロファイルの最大数	128	128
ACLルール	1,000	1,000
ポート		
固定Gigabit Ethernet ー 銅線ポート（内部フェールオープン機能搭載）	8	8
固定1 GigE（SFP）ポート	—	—
固定10 GigE/1 GigE（SFP+）ポート（外部パッシブ フェールオープン キットをサポート）	—	—
固定40-Gigabit Ethernet	—	—
ネットワークI/Oスロット	—	—
ネットワークI/Oモジュール	—	—
10 Gigabit Ethernet	—	—
40 Gigabit Ethernet	—	—
専用レスポンス ポート（RJ45）	1（1G/100M）	1（1G/100M）
専用管理ポート（RJ45）	1（1G/100M）	1（1G/100M）
専用ストレージ ポート（RJ45）	1（1G/100M）	1（1G/100M）
物理仕様		
寸法	1RUラック マウント型17.375"（W）x 1.75"（H）x 11.0"（D）	1RUラック マウント型17.375"（W）x 1.75"（H）x 11.0"（D）
重量	8.1 lbs.	8.1 lbs.
ストレージ	ソリッド ステート30 GB	ソリッド ステート30 GB
最大消費電力	100W	100W
DC電源	—	—
冗長電源	—	—
電源	100-240 VAC（50/60Hz）	
温度	0°～35°C（動作時）、-40°～70°C（非動作時）	
相対湿度（結露なし）	動作時: 10%～90% 非動作時: 5%から95%	
高度	0～10,000フィート	
安全性認定	UL 1950、CSA-C22.2 No. 950、EN-60950、IEC 950、EN 60825、21CFR1040 CBライセンスおよびレポートにより、あらゆる国での規格逸脱を補います。	
EMI認定	FCCパート15クラスA（CFR 47）（米国）、ICES-003クラスA（カナダ）、EN55022クラスA（ヨーロッパ）、CISPR22クラスA（国際）	

McAfee. Part of Intel Security.
マカフィー株式会社
東京本社　〒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）FAX 03-5428-1480
西日本支店　〒530- 0003 大阪府大阪市北区堂島 2-2-2 近鉄堂島ビル 18F TEL 06-6344-1511（代）FAX 06-6344-1517
名古屋営業所　〒450-0002 愛知県名古屋市中村区名駅 4-6-17 名古屋ビルディング 13F TEL 052-551-6233（代）FAX 052-551-6236
福岡営業所　〒810- 0801 福岡県福岡市博多区中洲 5-3-8 アクア博多 5F TEL 092-287-9674（代）
www.intelsecurity.com

 2270_1216
2016年12月