ネットワーク向け Cisco AMP（高度なマルウェア防御）

製品概要

効果的なマルウェア対策を実施するための新しいアプローチ、戦略、テクノロジーが求められるようになっています。Cisco® Advanced Malware Protection（AMP）for Network は、ネットワークベースの高度なマルウェア対策を提供し、ポイントインタイム検出だけでなく、攻撃前、攻撃中、攻撃後の各フェーズにわたる保護を実現します。Cisco FirePOWER™ ネットワーク セキュリティ アプライアンス向けの設計により、単一システム内の複数の脅威ベクターでマルウェアの脅威の検出、ブロック、追跡、封じ込めを実行します。また、高度かつ巧妙な標的型の永続的ゼロデイ脅威から組織を保護するために必要な可視性と制御を提供します。

Cisco AMP for Network により、以下が可能になります。

- **ポイントインタイム検出を超える信頼性の高い保護**：ポイントインタイム検出だけでなく、ファイルとトラフィックの継続的な分析を実行し、レトロスペクティブ セキュリティを実現します。レトロスペクティブ セキュリティとは、過去にさかのぼって、プロセス、ファイル アクティビティ、および通信を追跡する機能です。これにより、感染の全体像を把握して根本原因を明らかにし、修復を実行できるようになります。結果として、組織全体にわたって保護の効果および効率が向上します。
- **ポリシー違反のファイルなどを制限**：Cisco AMP for Network は、Web や電子メール、またはその他の攻撃ベクターを通じて侵入するファイルやアプリケーションを自動的に認識し、追跡します。その後、ユーザが設定したファイル制御ポリシーを使用して、ファイルの広範囲なフィルタリングを実行します。
- **エクスプロイト試行の検出とブロック**：シスコのソリューションは、インライン導入により、クライアント側によるエクスプロイト試行を検出してブロックできます。Adobe Acrobat、Java、Flash など、標的にされることの多いクライアント アプリケーションに対する脆弱性エクスプロイト試行も防御します。
- **悪意のあるファイルの特定、ブロック、分析**：システムは悪意のあるファイルによる、標的のシステムへの攻撃を阻止し、評価が未知のファイルをローカルで分析します。不審なファイルについては、オプションで Cisco Collective Security Intelligence クラウドに送信して分析することができます。
- **ファイルとトラフィックの継続的な分析**：監視対象のファイルに悪意があることが判明すると、そのファイルがネットワークを通過したのが数時間前や数日前であっても、Cisco AMP for Network はレトロスペクティブ アラートをトリガーします。これにより、ユーザは対策を講じて被害を軽減することができます。
- **離散型イベントをコーディナテッド アタックに相関付け**：Cisco AMP for Network は、進行中の攻撃に関連するリスクを示します。侵害された可能性のあるデバイスが優先順位付けされて自動的にリストされ、複数のイベント ソースのセキュリティ イベント データとともに提供されます。
- **マルウェアの拡散と通信を追跡**：Cisco AMP for Network のファイル トラジェクトリは、ネットワーク内のファイルの通信を追跡できるようにします。ファイル トラジェクトリ ビュー内の各ファイルには、経時的なファイルの転送を視覚化したトラジェクトリ マップが関連付けられているほか、ファイルに関する追加情報も含まれています。
- **マルウェアを封じ込めてデータ損失と感染を阻止**：Cisco AMP for Network では、単純なポリシー更新で、高度な脅威やマルウェアを簡単にブロックできます。カスタム検出リストを使用すれば、ベンダーが供給する更新を待たずに、必要なときにいつでも行動を起こすことができます。

効果的なセキュリティには検出以上の機能が必要

ポイントインタイム検出単独では、100 % の効果は望めません。検出を回避して環境を危険にさらすには、たった 1 つの脅威で十分です。巧妙な攻撃者は、標的型でコンテキスト認識型のマルウェアを使用し、ポイントインタイム防御を欺いて、いつでも、どのような組織に対しても攻撃をしかけられるだけのリソース、技能、そして粘り強さを持っています。さらに、ポイントインタイム検出は、感染の後では、どこまで侵害されているのか認識できないため、拡散を阻止できず、類似攻撃の再発を防ぐことができません。

Cisco AMP for Network は、ポイントインタイム検出を超える機能を提供する唯一のネットワークベース システムです。統合された制御機能のセットと継続的な分析の機能を使用し、脅威の検出、確認、追跡、分析、修復を実行し、高度なマルウェアによる攻撃前、攻撃中、攻撃後の各フェーズにわたって、包括的な保護を提供します。攻撃前は、Cisco AMP for Network は、既知のマルウェアに加えて、ポリシー違反のファイル タイプや通信によるネットワークへの侵入を防止し、攻撃対象を減らします。攻撃中は、エクスプロイト試行やファイル、トラフィックを検出およびブロックします。

攻撃後は、プリエンティブな検出やブロックでは 100 % の効果が望めないことを考慮したうえで、ファイルとネットワーク トラフィックの分析を継続し、初期の検出をすり抜けた可能性のあるステルス攻撃を探します。新しい侵害の痕跡（IoC）が発生すると、システムは、レトロスペクティブ マルウェア アラート、侵入イベント、マルウェアのコールバック試行などのセキュリティ イベントデータの複数のソースを自動的に相関付けし、優先順位付けされた単一のビューを作成します。このインテリジェントな自動化により、たとえ攻撃が発生した後であっても、進行中の攻撃の把握、調査、阻止を素早く効率的に実行できるようになります。これにより、防御の成否を左右する発見から封じ込めに至るまでの時間が短縮され、マルウェアによる被害が生じる前にその拡散を停止することができます。

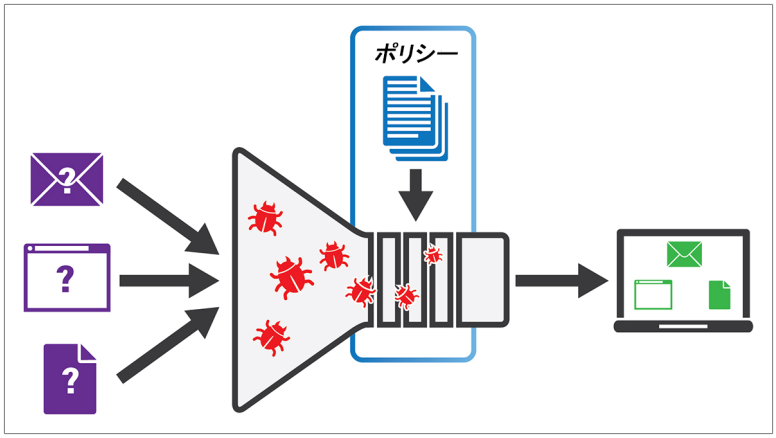
Cisco AMP for Network は、日常的に処理するイベントの数も減らし、実用的な洞察を提供します。これにより、高リスクで最も優先度の高い、高度なマルウェアの脅威に対して集中的に取り組むことができます。

さらに、Cisco AMP for Network は Cisco AMP for Endpoint と互換性があります。Cisco AMP for Endpoint は、PC、Mac、モバイル デバイス向けに、さらにデバイス上にソフトウェアベースのコレクタとして導入された仮想システム向けにシスコが提供する包括的で高度なマルウェア対策製品です。保護されたネットワークに接続されているかインターネット上でローミングしているかどうかに関わらず、エンドポイントを保護します。Cisco AMP for Network と Cisco AMP for Endpoint の両方を導入することで、組織は拡張された IT エコシステム全体で、包括的な可視性と制御を実現できます。

ポリシー違反のファイルなどを制限

Cisco AMP for Network では、システムの通過を許可するファイルのタイプを定義できます。ファイルの出所が Web、電子メール、またはその他の攻撃ベクターのいずれの場合であっても、システムはファイルとアプリケーションを自動的に認識します。その後、ユーザが設定したアプリケーションとファイルの制御ポリシー（図 1）を使用して、ファイルの広範囲なフィルタリングを実行します。これらのポリシーは、受信ファイルと送信ファイルの両方に適用できるため、ダウンロードされるファイルとアップロードされるファイルの両方を制御し、内外両方の脅威のアクターに対応できます。

図 1. ポリシー違反のファイルを制限



システムには、グローバルなセキュリティ インテリジェンス フィードも含まれ、脅威であることが判明している接続が動的にブラックリスト化されます。オプションの URL フィルタリングを使用すると、脅威として分類されている Web サイトやドメインから、ファイルをダウンロードしようとする動作をブロックできます。

エクスプロイト試行を検出してブロック

Cisco AMP for Network は、Cisco FirePOWER Next-Generation Intrusion Prevention System（NGIPS）をベースにしています。システムは、インラインで導入された場合、悪意のあるファイルをダウンロードする可能性のある、クライアント側のエクスプロイト試行（ドライブバイ攻撃）を検出してブロックします。NGIPS システムは、Web ブラウザ、Adobe Acrobat、Java、Flash など、標的にされることの多いクライアント アプリケーションに対する他の脆弱性エクスプロイト試行も防御できます。攻撃チェーンの中の可能な限り早い段階で機能し、付随的な損害を抑え、コストのかかるクリーンアップ作業を回避します。

悪意のあるファイルの検出、ブロック、分析

Cisco AMP for Network は、シスコの Collective Security Intelligence クラウドを使用し、Web やメールなどの複数の攻撃ベクターにわたるリアルタイムのファイル評価を取得します。既知の悪意のあるファイルは、標的とするシステムに到達できません。評価結果が未知のファイルについては、オプションで Cisco Collective Security Intelligence クラウドに送信し、分析することができます。クラウドでファイルが分析されると脅威スコアが計算されます。その後、管理コンソールで詳細な脅威レポートを確認し、意思決定に役立てることができます。オプションであらゆるタイプのファイルをシステムに保存できます。保存したファイルは、安全に取得して手動で詳細な分析を実行できます。

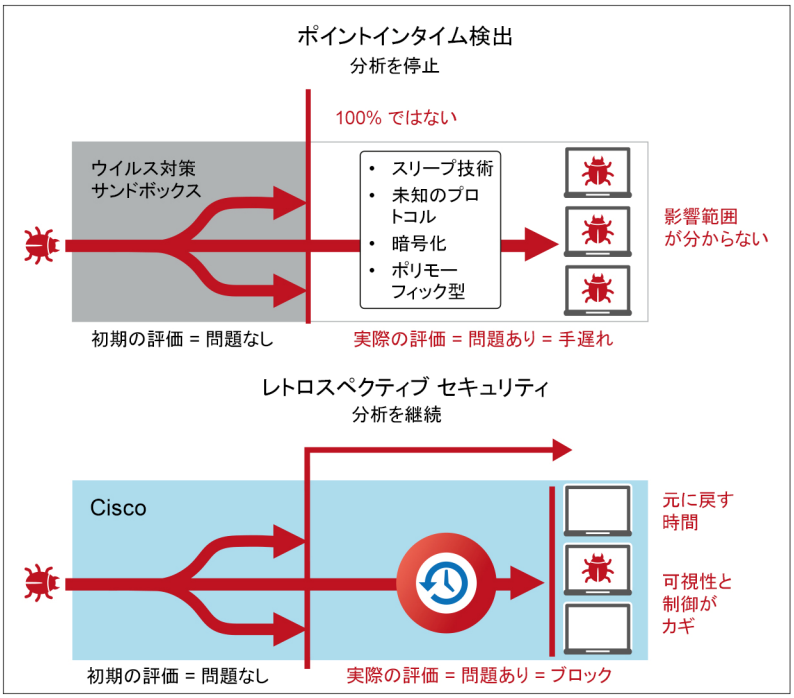
ファイルとトラフィックを継続的に分析

標準的なネットワークベースのマルウェア対策システムは、ネットワーク デバイスを通過する際にポイントインタイムでのみマルウェアを調査します。100 % の効果を持つ検出技術は存在せず、高度なマルウェアは自らを偽って最初の防御をすり抜けるため、多くの場合、最初の調査の実行後に可視性が失われます。

シスコは、ビッグデータ分析を使用した継続的な分析をポイントインタイム検出に追加することで、この課題を解決します。この継続的な分析により、最初の調査でデバイスを通過することを許可されたマルウェアに対しても、脅威であるとの判定が下されるようになります。継続的な分析は、レトロスペクティブ セキュリティ（図 2）を実現する重要な機能です。

Cisco AMP for Network システムは、ファイルが数時間または数日にわたってネットワークを通過した後であっても、レトロスペクティブなアラートによって、監視対象のファイルが脅威であると判断された時期を通知し、損傷を軽減する措置を実行できるようにします。

図 2.　　ポイントインタイム検出と継続的な分析/レトロスペクティブ セキュリティとの比較



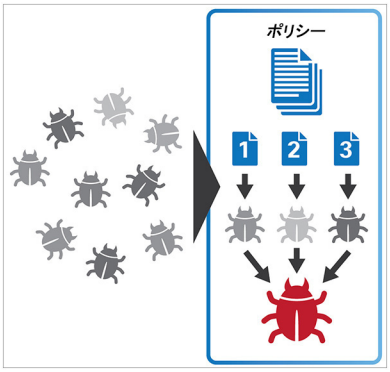
離散型イベントをコーディナテッド アタックに相関付け

Cisco AMP for Network には、Cisco FireSIGHT™ Management Center（図 3）、シスコの検出および認識技術、ダッシュボードが含まれます。これにより、ホスト、オペレーティング システム、アプリケーション、ユーザ、ファイル、ネットワーク、地理位置情報、脆弱性についての情報が収集されます。Cisco AMP for Network は、これらの離散しながらも相関したイベントを組み合わせ、FireSIGHT Management Center に IoC と呼ばれる統合ビューを作成します。

図 3.　　Cisco FireSIGHT Management Center

このビューは、侵害された可能性のあるデバイスを優先順位付けして自動的にリストし、マルチ イベント ソースのセキュリティ イベント データとともに提供して、進行中の攻撃に関連するリスクを示します（図 4）。このコンテキストに応じたデータが追加されることで、より多くの情報に基づいて、適切に行動指針を決定できるようになります。

図 4. イベント相関

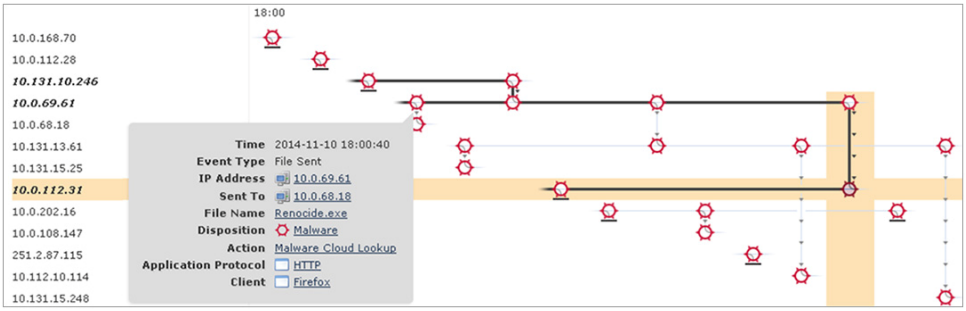


マルウェアの拡散と通信を追跡

Cisco AMP for Network はファイル トラジェクトリ機能を使用し、ネットワーク全体でファイルの送信を追跡できるようにします。ファイル トラジェクトリ ビュー内の各ファイルには、経時的なファイルの転送を視覚化したトラジェクトリ マップが関連付けられています。マップにはファイルに関する追加情報が含まれています。

ファイル トラジェクトリは、潜在的な感染の影響や範囲を明らかにするために必須の機能です。重要な FireSIGHT データには、意思決定に役立つビューが付属します。ターゲットのシステムやシステムのユーザ、さらにはプロトコルや通信の試行など、コンテキストに応じたあらゆる情報に基づいて、ファイルに関連するリスクをより正確に理解できます。

図 5. ファイル トラジェクトリ



マルウェアを封じ込めてデータ損失と感染を阻止

Cisco AMP for Network により、進行中の攻撃への対策を決定する際に、感染を素早く封じ込めることができます。ファイルのブラックリストを作成し、単純なポリシー更新でマルウェアの通信をブロックできます。カスタム検出リストを使用すれば、ベンダーが供給する更新を待たずに、必要なときにいつでも行動を起こすことができます。

卓越したセキュリティ インテリジェンスと動的分析

Cisco AMP for Network はビッグデータと卓越したセキュリティ インテリジェンスをベースにしています。Cisco Security Intelligence Operations と Talos Security Intelligence and Research Group は、業界最大のリアルタイムな脅威インテリジェンスの集合体です。最高レベルの可視性とフットプリントに加え、複数のセキュリティ プラットフォームにわたって実行できる機能を備えています。このデータはクラウドから AMP クライアントにプッシュされるため、常に最新の脅威インテリジェンスを活用できます。

リアルタイムな脅威インテリジェンスの大規模な集合体を活用することで、組織は次の利点を得ることができます。

- 110 万件の着信マルウェアのサンプル（1 日あたり）
- 130 億の Web 要求
- 世界中に設置された 160 万のセンサー
- 600 名のエンジニア、技術者、および研究者
- 1 日で 100 TB のデータ
- 24 時間運用

AMP for Network は、この堅牢でコンテキスト豊富なナレッジ ベースにファイル、動作、テレメトリ データ、およびアクティビティを自動的に相関付けることにより、ネットワークへの侵入を試みる脅威をブロックします。これにより、セキュリティ チームはネットワーク内の脅威をより高度に認識し、より迅速かつ容易にインシデントに対応することができます。

サードパーティ テストをリードする Cisco AMP

シスコは、NSS Labs Breach Detection Systems Security Value Map（NSS ラボ侵害検出システム セキュリティ バリュー マップ）のリーダーに選ばれています。2013 ～ 2014 年の「NSS Labs Product Analysis Reports（NSS Labs 製品分析レポート）」および 2014 年の「NSS Labs Breach Detection Systems Comparative Analysis Report（NSS Labs 侵害検出システム（BDS）比較分析レポート）」で、Cisco AMP は次の評価を受けています。

- 最高の総合検出率
- 最短の検出時間
- 保護される Mbps あたりの総所有コストが最安
- Security Value Map のトップ

NSS Labs の評価は、Cisco AMP for Network が最高レベルのセキュリティ効果と費用対効果を持つことを証明しています。侵入の検出や防止の標準となっている Snort の考案者であるシスコのルーツは、セキュリティにあります。シスコの FirePOWER アプライアンスのラインアップは、かつてないスループット パフォーマンス、コストパフォーマンス、スケールを実現します。さらに、FireSIGHT Management Center は、コンテキストに応じた認識を使用して精度と自動化を強化し、ネットワークの構成を把握します。

表 1 に、Cisco AMP for Network の最高クラスの機能を示します。

表 1. Cisco AMP for Network の機能とメリット

機能	メリット
継続的な分析	Cisco AMP for Network は、クラウド ベースのビッグデータ分析を使用し、長期間かけて収集された新旧のデータを絶えず再評価して、ステルス攻撃を検出します。これは、ポイントインタイム検出にはない機能です。
レトロスペクティブ セキュリティ	レトロスペクティブ セキュリティとは、過去にさかのぼって、プロセス、ファイル アクティビティ、および通信を追跡する機能です。これにより、感染の全体像を把握し、根本原因を明らかにしたうえで修復を実行できます。レトロスペクティブ セキュリティは、イベント トリガー、ファイル評価の変更、IoC トリガーなど、侵害の痕跡が見られたときに必要になります。

機能	メリット
FireSIGHT Management Center	シングルペインを通して環境を可視化：ホスト、オペレーティング システム、アプリケーション、ユーザ、ファイル、ネットワーク、地理位置情報、脆弱性を考慮した包括的でコンテキストに応じた視点により、十分な情報に基づいてセキュリティの意思決定を行えます。
総合的なセキュリティ インテリジェンス	Cisco Security Intelligence Operations と Talos Security Intelligence and Research Group は、業界最大のリアルタイムな脅威インテリジェンスの集合体です。最高レベルの可視性とフットプリントに加え、複数のセキュリティ プラットフォームにわたって実行できる機能を備えています。
侵害の痕跡	侵害の痕跡（IoC）は、潜在的にアクティブな侵害として相互に関連付けられ、優先順位が付けられたファイルとテレメトリのイベントです。Cisco AMP for Networks は、複数のソースからのセキュリティ イベント データ（侵入やマルウェアなどのイベント）を自動的に関連付け、イベントをより大規模な組織的攻撃に結び付けたり、リスクの高いイベントの優先順位を付けたりできるようにします。
ファイル レピュテーション	高度な分析と集合型インテリジェンスの組み合わせによって、ファイルが悪意のあるものであるかどうかを判断し、より正確な検出につなげることができます。
ファイル分析とサンドボックス	非常にセキュアな環境でマルウェア動作を実行、分析、テストして、未知のゼロデイ脅威を検出できます。
レトロスペクティブな検出	広範な分析によってファイルの評価が変化したときは、アラートが送信され、最初の防御をすり抜けたマルウェアについて注意喚起され、問題のファイルが可視化されます。
ファイル トラジェクトリ	環境全体にわたるファイル伝播を継続的に追跡することで、ファイルの可視性を実現し、マルウェアによるセキュリティ侵害の範囲をすみやかに特定できるようにします。
統合 SSL 複合化	SSL 暗号化ネットワーク トラフィックを識別して複合化し、そのトラフィックの調査と検出を実行します。さらに、SSL 認証ポリシーを強制し、ネットワークのセントラル SSL ポリシー制御を有効化します。
AMP for Endpoint との統合	Cisco AMP for Network は、PC、Mac、モバイル デバイス、仮想システム向けの高度なマルウェア対策製品である Cisco AMP for Endpoint と互換性があります。両システムを導入することで、組織は拡張された IT エコシステム全体で、最高レベルの可視性と制御を実現できます。

製品のパフォーマンスと仕様

Cisco AMP for Network はあらゆる Cisco FirePOWER セキュリティ アプライアンスに導入できます。特に Cisco AMP 専用アプライアンスである AMP7150、AMP8050、AMP8150、AMP8350、AMP8360、AMP8370、AMP8390（表 2）では、Cisco AMP for Network ソリューションのメリットを最大限に引き出すことができます。専用の処理能力とストレージを備えたアプライアンス モデルに導入することで、要求が多い環境で固有の目標を達成することができます。

表 2. ハードウェア仕様：Cisco AMP for Network 専用アプライアンス

	AMP7150	AMP8050	AMP8150	AMP8350	AMP8360	AMP8370	AMP8390
高度なマルウェア保護[1]	500 Mbps	1 Gbps	2 Gbps	5 Gbps	10 Gbps	15 Gbps	20 Gbps
モニタリング インターフェイスの最大数[2]	12	12（3 x 4 ポート、RJ45 Netmods）	12（3 x 4 ポート、RJ45 Netmods）	28（7 x 4 ポート、RJ45 Netmods）	24（6 x 4 ポート、RJ45 Netmods）	20（5 x 4 ポート、RJ45 Netmods）	16（4 x 4 ポート、RJ45 Netmods）
固定モニタリング インターフェイス	4 x 10/100/1000（RJ45）	0	0	0	0	0	0
モジュラ インターフェイス	8 SFP（1GB）フェールオーバーなし	あり（Netmods が必要）	あり（Netmods が必要）	あり（Netmods が必要）	あり（Netmods が必要）	あり（Netmods が必要）	あり（Netmods が必要）
Netmod 拡張スロット	0	3	3	7	6	5	4
プログラマブル フェールオープン インターフェイス	4 x 10/100/1000（RJ45）	あり（Netmods が必要）	あり（Netmods が必要）	あり（Netmods が必要）	あり（Netmods が必要）	あり（Netmods が必要）	あり（Netmods が必要）
管理インターフェイス	1 x 10/100/1000（RJ45）	1 x 10/100/1000（RJ45）	1 x 10/100/1000（RJ45）	2 x 10/100/1000（RJ45）	2 x 10/100/1000（RJ45）	2 x 10/100/1000（RJ45）	2 x 10/100/1000（RJ45）
平均遅延時間	< 150 マイクロ秒	< 150 マイクロ秒	< 150 マイクロ秒	< 150 マイクロ秒	< 150 マイクロ秒	< 150 マイクロ秒	< 150 マイクロ秒
ストレージ容量（SSD）	120 GB	400 GB 以上	400 GB	400 GB 以上	800 GB 以上	1200 GB 以上	1600 GB 以上
スタック対応	非対応	非対応	非対応	対応	対応	対応	対応

	AMP7150	AMP8050	AMP8150	AMP8350	AMP8360	AMP8370	AMP8390
冷却ファン	5	10	10	6	12	18	24
電源装置	2（ホットスワップ可能）	2（ホットスワップ可能）	2（ホットスワップ可能）	2（ホットスワップ可能）	4（ホットスワップ可能）	6（ホットスワップ可能）	8（ホットスワップ可能）
フォーム ファクタ	1U	1U	1U	2U	4U	6U	8U
寸法（高さ x 縦 x 横）	21.6 x 19.0 x 1.73 インチ	27.25 x 16.93 x 1.7 インチ	27.25 x 16.93 x 1.7 インチ	29 x 17.2 x 3.48 インチ	29 x 17.2 x 6.96 インチ	29 x 17.2 x 10.44 インチ	29 x 17.2 x 13.92 インチ
最大積み込み重量	29 ポンド（13.2 kg）	54 ポンド（25.5 kg）	54 ポンド（25.5 kg）	67 ポンド（30.5 kg）	2 X 67 ポンド	3 X 67 ポンド	4 X 67 ポンド
AC 電圧[3]	100 ～ 240 VAC（公称） 90 ～ 264 VAC（最大）	100 ～ 240 VAC（公称） 85 ～ 264 VAC（最大）	100 ～ 240 VAC（公称） 85 ～ 264 VAC（最大）	100 ～ 240 VAC（公称） 85 ～ 264 VAC（最大）	100 ～ 240 VAC（公称） 85 ～ 264 VAC（最大）	100 ～ 240 VAC（公称） 85 ～ 264 VAC（最大）	100 ～ 240 VAC（公称） 85 ～ 264 VAC（最大）
電流[4]	8 A（全範囲で最大）	8 A（全範囲で最大）	8 A（全範囲で最大）	11 A（全範囲で最大）	2 X 11 A	3 X 11 A	4 X 11 A
DC 電圧オプション	非対応	非対応	非対応	対応	対応	対応	対応
最大出力[5]	450 W	650 W	650 W	1,000 W	2 X 1000 W	3 X 1000 W	4 X 1000 W
平均消費電力[7]	200 W	400 W	400 W	635 W	2 X 635 W	3 X 635 W	4 X 635 W
運用温度	5° C ～ 40° C	10° C ～ 35° C	10° C ～ 35° C	5° C ～ 40° C	5° C ～ 40° C	5° C ～ 40° C	5° C ～ 40° C
周波数の範囲	47 Hz ～ 63 Hz	47 Hz ～ 63 Hz	47 Hz ～ 63 Hz	47 Hz ～ 63 Hz	47 Hz ～ 63 Hz	47 Hz ～ 63 Hz	47 Hz ～ 63 Hz
エアー フロー	前面から背面へ	前面から背面へ	前面から背面へ	前面から背面へ[6]	前面から背面へ[6]	前面から背面へ[6]	前面から背面へ[6]
BTU/時間定格（重荷重）	900 BTU	1725 BTU	1725 BTU	2900 BTU	2 X 2900	3 X 2900	4 X 2900
運用湿度	5 ～ 85%	5 ～ 85%	5 ～ 85%	5 ～ 85%	5 ～ 85%	5 ～ 85%	5 ～ 85%
RoHS 準拠	対応	対応	対応	対応	対応	対応	対応

[1] AMP スループットの値は、ファイアウォール、IPS、AMP の各機能を有効化した場合のものです。* ネットワーク パフォーマンスは、シスコが関与できない諸条件（適用ポリシー、プロトコル ミックス、検査時の平均パケットサイズなど）によって変化します。

[2] Netmods は、フェールオーバーまたは非フェールオーバーです。

[3] シャーシの電圧入力はすべて同じです。

[4] 各シャーシに電流が流れます。

[5] 各シャーシの電源は、定格出力 1000W です。

[6] 各アプライアンス側面に 1 平方インチの吸入口 x 2 があります。

[7] 電源は 1+1 冗長構成です。

[8] AMP 8360、8370、8390 はスタック構成のアプライアンスであるため、各仕様には各スタック数（それぞれ 2、3、4）が乗算されます。

[*] NGIPS/NGFW のパフォーマンスに関する仕様については、Cisco Firepower アプライアンス データ シート（http://www.cisco.com/go/ngips [英語] ）を参照してください。

[**] FirePOWER アプライアンスと専用 AMP アプライアンスは、プラットフォームの同等性（FP8350 と AMP8350 など）を維持します。アプライアンスと統合マルウェアのストレージ パックも同一のものが維持されます。

ソフトウェア要件

表 3 にソフトウェア要件を示します。

表 3. ソフトウェア要件

ネットワークベースの高度なマルウェア保護: ● Cisco FirePOWER 7000 および 8000 シリーズ アプライアンス、仮想 64 bit アプライアンスのすべてでサポート ● v5.3 以降が必要 ● Cisco FireSIGHT Management Center が必要（Management Center にはインターネットを介した Collective Security Intelligence クラウドへの接続またはオンプレミスの Cisco AMP プライベート クラウド仮想アプライアンスへの接続が必要です）	レピュテーション検索でサポートされるファイル タイプ（括弧内は拡張子の例）: ● Microsoft Office ドキュメント（doc および xls） ● ポータブル ドキュメント（pdf） ● アーカイブ ファイル（jar） ● マルチメディア ファイル（swf） ● 実行バイナリ（msexe および jar.pack）
サポートされるアプリケーション プロトコル: ● HTTP ● SMTP ● IMAP ● POP3 ● FTP ● NetBIOS-ssn（SMB）	レピュテーション検索の結果: ● クリーン（既知、問題なし） ● 不明（判別不能またはデータ不足） ● 脅威（既知、問題あり）
双方向の調査と制御	ファイル識別の処理 ● 検出またはブロック（ファイル タイプ、送信方向、またはプロトコルで実行） ● マルウェアのクラウド検索（レピュテーションのクエリ）
地理情報ソースまたは宛先によるファイルのブロックをサポート	IoC 相関でイベント タイプまたはデータ ソースをサポート ● IPS イベント（ネットワーク） ● Cisco AMP for Endpoint ● マルウェア イベント（ネットワーク） ● セキュリティ インテリジェンス（ネットワークとエンドポイント） ● Cisco FireSIGHT コンテキスト データ
Collective Security Intelligence クラウドによる動的ブラックリストをサポート	カスタム検出（ユーザ定義のブラックリストとホワイトリスト）
Collective Security Intelligence での動的分析のための自動送信: ● Microsoft 実行ファイル（msexe、dll） ● 分析後に脅威スコアと動的分析のレポートを利用可能	

プラットフォーム サポート/互換性

Cisco AMP for Network には、ユーザ選択の Cisco FirePOWER Appliance、Cisco FirePOWER Appliance Subscription for AMP、Cisco FireSIGHT Management Center、IPS のサブスクリプションのオプション、アプリケーション、URL フィルタリングが含まれます。

保証に関する情報

保証については、Cisco.com の製品保証 [英語] のページを参照してください。

発注情報

発注ご検討の場合には、シスコ コンタクトセンターもしくは弊社販売パートナー様にご連絡ください。

詳細情報

詳細については、以下のリンクを参照してください。

- Cisco AMP for Network [英語]

お問い合せ先

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

C78-733182-02JA 15.07