Cisco Advanced Malware Protection プライベート クラウド アプライアンス

目次

製品概要 3

高度な脅威の阻止 3

仕組み 3

導入モード 4

製品仕様 8

発注情報 9

シスコ サービス 10

Cisco Smart Net Total Care 10

保証に関する情報 10

発注情報 10

Cisco Capital 11

詳細情報 11

厳格なプライバシー要件によってパブリッククラウドを使用できない組織向けの、オンプレミスのエアギャップソリューション。

製品概要

Cisco® Advanced Malware Protection（AMP）プライベート クラウド アプライアンスは、オンプレミスのプライベートクラウドとして、Cisco AMP for Networks、AMP for Email、AMP for Web Security、AMP for Endpoints に対応しています。ローカルに保存されたファイルレピュテーション、マルウェア分析結果、すべてのファイルアクティビティの継続的なモニタリング情報、セキュリティ インテリジェンスを使用して、脅威を防御します。統合セキュリティ インテリジェンスを活用しながら厳格なプライバシー要件に対応し、中小企業から大企業までネットワークとエンドポイントを保護します。

高度な脅威の阻止

被害が発生する前に脅威を阻止することが理想的です。しかし、事前に脅威を阻止できない場合はどうすればよいのでしょうか。対応にどのくらい時間がかかるでしょうか。「当社はこの攻撃に対応できているか」と不安になったお客様は、できるだけ早く解決策を知りたいはずです。次に気になるのは、適切に対応できるようになるまでにどれくらい時間がかかるか、ということです。

組織が侵害を検出するまでに、平均で約 200 日かかっています。大規模なイベントに対応する場合、複数のソースやツールから収集した異なるタイプのデータを大量に調査し、影響を特定してようやく脅威を排除できます。そのため、貴重な時間を費やすことになります。AMP for Endpoints では、当て推量による作業が不要になるため、脅威を検出するために必要な日数が、数日や数ヵ月からほんの数時間に大幅に短縮されます。

シスコのプライベート クラウド アプライアンスを活用すれば、貴重な時間を浪費せずにすみます。AMP は、自動化された保護機能、継続的なモニタリング、レトロスペクティブ セキュリティを実現する分析機能により、ネットワークが攻撃される前に最も検出しにくい 1% の脅威を検出するため、迅速なインシデント調査および対応が可能になります。

仕組み

Cisco AMP プライベート クラウド アプライアンスは、すべての情報をオンプレミスでローカルに保存することで、包括的な脅威保護を実現します。未知の不審なファイルを検出すると、シスコのインテリジェンス データベースとの連携により、ファイル評価情報を検索します。プロキシモードが設定されている場合は、匿名化したセキュア ハッシュ アルゴリズム 256（SHA-256）情報のみをパブリック AMP クラウドに送信します。エアギャップモードが設定されている物理アプライアンスを使用している場合は、SHA-256 をパブリック AMP クラウドには送信せず、アプライアンスのローカルでファイル評価情報を検索します。

このソリューションには、次のような特長があります。

- **自己完結型の物理/仮想アプライアンスによってプライバシーを確保：**アプライアンスおよび管理システムは、単一のオンプレミスソリューションです。
- **ネットワークとエンドポイントを保護：**エンドポイントには AMP for Endpoints コネクタを介して接続し、Cisco Firepower® 次世代ファイアウォールおよび次世代侵入防御システム（NGFW/NGIPS）上の AMP for Networks には直接接続して、ネットワークマルウェアから保護します。 また、Cisco E メール セキュリティ アプライアンス（ESA）と Cisco Web セキュリティアプライアンス（WSA）もサポートしています。
- **単一のコンソールで管理：**パブリッククラウドと同様に、Cisco AMP プライベート クラウド アプライアンスは、サポート対象の統合製品を一元管理できます。たとえば、カスタムポリシーおよび検出結果、ファイル/デバイストラジェクトリ、根本原因分析、レポート、ファイル評価キャッシュ、ファイル分析結果、デバイス識別情報を、AMP for Endpoints コンソールを利用して管理できます。
- **ニーズの増大に合わせて拡張可能：**各プライベート クラウド インスタンスは、仮想アプライアンス上で 1 万コネクタ、物理アプライアンス上で 10 万コネクタまでサポートできます。さらに、その他のアプライアンス（Firepower Management Center（FMC）、ESA、WSA）を環境に追加することも可能です。

導入モード

Cisco AMP プライベート クラウド アプライアンスは、「クラウドプロキシモード」と「エアギャップモード」の 2 つの導入モードに対応しています。

クラウドプロキシモードの特長は以下のとおりです。

- 仮想アプライアンスおよび物理アプライアンスの両方でサポートされています。
- ファイル評価情報を検索するには、インターネット接続が必要です。
- エンドポイントコネクタからのすべてのトラフィックはプライベートクラウドに転送されますが、その後のファイル評価情報の検索は、プライベートクラウドと AMP パブリッククラウド間で実行されます。
- 検査対象のファイルに関して SHA-256 ハッシュのみが、AMP プライベート クラウド アプライアンスからパブリック AMP クラウドに送信されます。
- コンテンツおよびソフトウェアの更新は、AMP クラウドから AMP プライベート クラウド アプライアンスに自動的に直接送信されます。

エアギャップモードの特長は次のとおりです。

- このモードは、物理アプライアンスでのみサポートされます。
- ファイル評価情報の検索にインターネット接続は必要ありません。
- すべてのトラフィックは、コネクタ間およびアプライアンスにしか存在しません。
- ファイル評価情報の検索は、プライベートデバイスで実施されます。
  - 「保護 DB」と呼ばれるローカルインスタンスには、すべての機能と保護に必要な全ファイルの評価情報と脅威インテリジェンスが含まれています。

エアギャップモードでは、脅威インテリジェンスの更新は次のように行われます。

- コンテンツおよびソフトウェアの更新は、AMP プライベート クラウド アプライアンスから別々に送信されます。
- 「amp-sync」と呼ばれるツールによって、AMP パブリッククラウドから AMP プライベート クラウド アプライアンスに対して、ソフトウェアおよびコンテンツの更新がダウンロードされ、同期されます。
- amp-sync を実行し、更新パッケージをビルドするには、専用のホストサーバ（更新ホスト）が必要です。
  - 更新ホストが更新を取得するには、インターネットにアクセスする必要があります。
  - 更新ホストは CentOS 6.6 以降を搭載している必要があります。
  - amp-sync でビルドされた ISO ディスクイメージの更新パッケージは更新ホストから転送され、アプライアンスにインストールされます。その後、管理コンソールから更新プロセスが開始されて完了します。
- 更新は毎日作成されます。更新には、統合セキュリティ インテリジェンス データベース、ウイルス対策定義、その他の脅威インテリジェンスの更新が含まれています。
- アプライアンスが AMP パブリッククラウドにアクセスできる特別なエアギャップ環境では、通常のエアギャップ環境のように 1 台のサーバでコンテンツをダウンロードしてアプライアンスに転送するための中間ステップは必要なく、AMP パブリッククラウドから直接更新を取り込むことができます。

図 1 および図 2 は、各導入モードの動作を示しています。

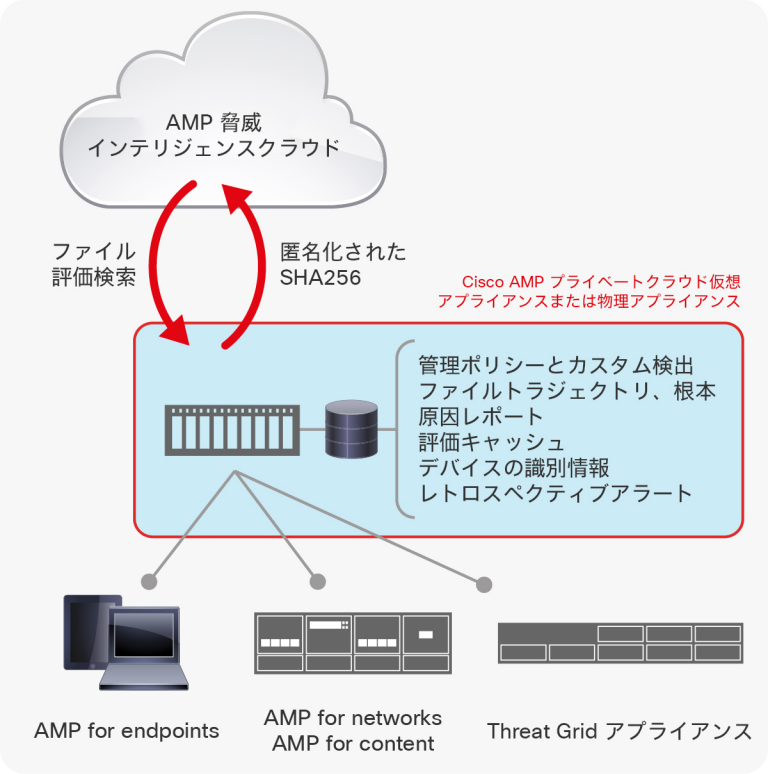

図 1.
クラウドプロキシモード

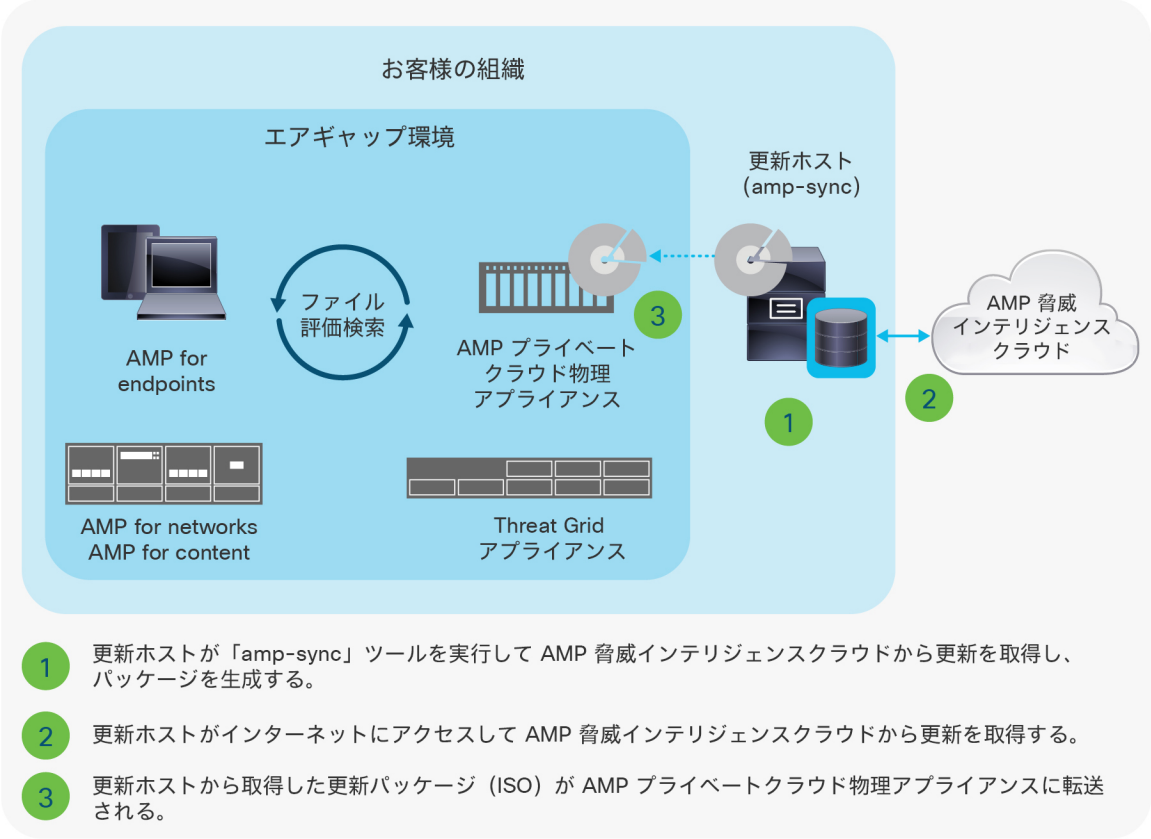

図 2.
エアギャップモード

表 1 に、AMP プライベートクラウドとパブリッククラウドの比較を示します。

表 1. AMP プライベートとパブリッククラウドの比較

機能	Cisco AMP プライベート クラウド アプライアンス	Cisco AMP パブリッククラウド	その他の情報
デバイス/ファイルトラジェクトリ	○	○	環境全体および個別のデバイスでファイル伝播を継続的に追跡することで可視化し、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。
脅威の根本原因	○	○	マルウェアの侵入経路および侵入方法を把握します。
クラウドベースでのセキュリティ侵害の兆候（IOC）	○	○	IOC は、アクティブになる可能性のある侵害として相互に関連付けられ、優先順位が設定されたファイルおよびテレメトリのイベントです。AMP は、複数のソースから収集したセキュリティ 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を優先させたりすることができます。

機能	Cisco AMP プライベート クラウド アプライアンス	Cisco AMP パブリッククラウド	その他の情報
レトロスペクティブアラート	○	○	レトロスペクティブ セキュリティとは、過去に遡って、プロセス、ファイルアクティビティ、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することができます。過去に遡って分析することでファイルの評価が変わった場合は、最初の防御をすり抜けたマルウェアについてアラートが送信され、可視化されます。
シンプルカスタム検出	○	○	シンプルなハッシュベースの個別の検出シグニチャです。
高度なカスタム検出	○（Windows のみ）	○	高度なシグニチャをサポートします。
マルウェア分析	○	○	Cisco Threat Grid（TG）を活用して、ファイル分析機能をオンプレミスアプライアンスで利用できます。未知のファイルに対して静的分析および動的分析を実施し、悪意のあるファイルかどうかを特定します。悪意のあるファイルの場合はその理由を示します。
クラウドでのファイル評価情報検索	クラウドプロキシモード：○ エアギャップモード：×	○	AMP プライベートクラウド仮想アプライアンスがエアギャップモードの場合、クラウドからファイル評価情報を取得するためにインターネットに直接接続することはありません。評価情報は、同期された堅牢な脅威インテリジェンスリポジトリから取得されます（エアギャップ環境では手動で同期されて保持されます）。
機械学習検出エンジン	○	○	アルゴリズムに基づいて学習した専用の検出エンジンによって、既知の脅威の属性をベースにして予測し、悪意のあるファイルやアクティビティを特定します。
ポリモーフィック型マルウェア検出エンジン	×	○	「bit-twiddling」によって検出を回避しようとするマルウェアへの対抗策として、「ファジーハッシュ」を使用してマルウェアファミリを検出します。
ウイルス対策エンジン	○	○	シグニチャベースの検出エンジンです。
ロールベース アクセス コントロール（RBAC）	○	○	各ユーザのロールに基づいて AMP 内の特定のタスクに対するアクセス権と実行権限を制御します。
エンドポイントにおけるセキュリティ侵害の兆候（IOC）	○	○	エンドポイントスキャン用に OpenIOC 形式のルールを作成して展開する機能です。
脆弱なソフトウェアの検出	○	○	マルウェアの攻撃ベクトルとして機能する可能性があるエンドポイント上の脆弱なソフトウェアの存在を管理者に通知します。

機能	Cisco AMP プライベート クラウド アプライアンス	Cisco AMP パブリッククラウド	その他の情報
管理対象コネクタ	仮想プライベート クラウド アプライアンスあたり 1 万、 物理プライベート クラウド アプライアンスあたり 10 万	無制限	複数のアプライアンスを使用する場合は、各アプライアンスインスタンスを個別に管理する必要があります。
Firepower Management Center 統合	FMC 6.1 時点	○	AMP 仮想プライベート クラウド アプライアンスを利用して AMP for Networks を管理するコンソールです。
データプライバシー	○	○	クラウドプロキシモードの AMP 仮想プライベート クラウド アプライアンスでは、AMP パブリッククラウドに送信されるのは SHA-256 ハッシュのみです。エアギャップモードでは、AMP パブリッククラウドにデータは送信されません。AMP パブリッククラウドには他のファイルメタデータが必要ですが、個人を特定できる情報は送信されません。

表 2 は、2 つのアプライアンスオプションを比較したものです。

表 2. 仮想アプライアンスと物理アプライアンスの比較

	AMP プライベート クラウド アプライアンス PC3000	AMP プライベートクラウド仮想アプライアンス
フォームファクタ	2RU 物理アプライアンス	VMware 仮想マシン
FMC、TG、ESA、WSA サポート	○	○
サポート対象コネクタ数	10 万	1 万
エアギャップ導入サポート	○	×

製品仕様

Cisco AMP プライベート クラウド アプライアンスには、VMware OVA 仮想アプライアンスと物理アプライアンスの 2 つの導入オプションがあります。

仮想マシンインスタンスを稼働させるための最小要件を表 3 に示します。

表 3. 仮想アプライアンスのソフトウェア要件

ソフトウェア	システム要件
AMP プライベートクラウド仮想アプライアンス 3.0	• VMware ESX 5 以降 • クラウドプロキシモードのみ：64 GB RAM、8 CPU コア（2 CPU X 4 コア推奨）、VMware データストアに 1 TB 以上の空きディスク容量 ◦ ドライブのタイプ：SSD 必須

ソフトウェア	システム要件
	◦ RAID タイプ：RAID 10 グループ X 1（ミラーリング + ストライピング） ◦ VMware データストアサイズ：1 TB 以上 ◦ RAID 10 グループ（4K）に対するデータストアランダム読み取り：60K IOPS 以上 ◦ RAID 10 グループ（4K）に対するデータストアランダム書き込み：30K IOPS 以上
AMP for Endpoints コネクタ	• Microsoft Windows 7 • Microsoft Windows 8/8.1 • Microsoft Windows 10 • Microsoft Windows Server 2008 R2 • Microsoft Windows Server 2012/2012 R2 • Microsoft Windows Server 2016 • Apple macOS 10.7 • Redhat Enterprise Linux（RHEL）/CentOS 6.8/6.9 • Redhat Enterprise Linux（RHEL）/CentOS 7.3/7.4

物理アプライアンスの製品仕様について表 4 に示します。

表 4. 物理アプライアンス製品仕様

AMP プライベートクラウド 3000（PC3000）物理アプライアンス	仕様
フォームファクタ	2 ラックユニット（RU）
寸法	8.6 X 43.0 X 75.7 cm（3.4 X 16.9 X 29.8 インチ）（高さ X 幅 X 奥行）
ネットワーク インターフェイス	1 GB 銅線 X 2 + SFP+
CIMC インターフェイス	1 GB 銅線
電源オプション	770W AC

発注情報

Cisco AMP プライベート クラウド アプライアンスのご注文については、シスコ発注ホームページをご覧ください。表 5 に発注情報を示します。

表 5. 発注情報

AMP プライベートクラウド物理アプライアンスおよびサブスクリプション	
製品番号	**製品説明**
AMPPC-3000-K9	Cisco AMP プライベート クラウド アプライアンス - 3000 モデル
L-AMP-PC-K9=	Cisco AMP プライベートクラウド、コンテンツライセンス - 1、3、5 年間（AMP-PC-1Y、L-AMP-PC-3Y、L-AMP-PC-5Y）

AMP プライベートクラウド仮想アプライアンスおよびサブスクリプション	
製品番号	**製品説明**
FP-AMP-CLOUD-BUN	Cisco AMPv プライベート クラウド ソフトウェアおよびサービスのサブスクリプションバンドル。簡単に発注するためのバンドルです。次の PID が含まれています。
FP-AMP-CLOUD=	Cisco AMPv プライベート クラウド サービス サブスクリプション - 1、3、5 年間（FP-AMP-CLOUD-1Y、FP-AMP-CLOUD-3Y、FP-AMP-CLOUD-5Y）
FP-AMP-CLOUD-SW	Cisco AMP プライベートクラウド仮想アプライアンス

シスコ サービス

シスコでは、お客様の TCO を最小化する取り組みを行っており、お客様の成功を支援する幅広いサービスプログラムを用意しています。シスコの画期的なプログラムは、スタッフ、プロセス、ツール、パートナーを独自に組み合わせたかたちで提供され、お客様から高い評価を受けています。ネットワークへの投資を無駄にすることなく、ネットワーク運用を最適化し、新しいアプリケーションに対応できるようにネットワークを整備することにより、ネットワーク インテリジェンスの強化や事業の拡張を進めていただくために、シスコのサービスをぜひお役立てください。シスコのサービスの主な利点は次のとおりです。

- 予防的問題解決と迅速な問題解決によりリスクを軽減できます。
- アドバイザリ、導入、進行中の最適化に関するシスコの経験と専門知識を活用して TCO を削減できます。
- ネットワークダウンタイムを最小限に抑えられます。
- お客様の現在のサポート担当者が他の生産的活動に集中できるようにサポートいたします。

Cisco Smart Net Total Care

Cisco AMP プライベート クラウド アプライアンスでは、すべての Cisco Smart Net Total Care® サービスレベルを利用できます。Smart Net Total Care（SmartNet）は、シスコの専門家やセルフサービスのサポートツールにいつでも直接アクセスしてネットワークの問題をすばやく解決できるほか、ハードウェアの迅速な交換にも対応します。

SmartNet とシスコ セキュリティ サービスの詳細については、こちらをご覧ください。

保証に関する情報

保証については、製品保証のページを参照してください。

発注情報

発注するには、シスコ発注ホームページにアクセスするか、シスコのセールス担当者または +1 800 553 6387 までお問い合わせください。発注ガイドを参照すれば、お客様の組織に適した Cisco AMP プライベート クラウド アプライアンスの発注方法に関する詳細な手順を確認できます。

Cisco Capital

目標の達成を支援する柔軟な支払いソリューション

Cisco Capital は、お客様が目標の達成、ビジネス変革の実現、競争力の維持に合ったテクノロジーを導入できるよう支援します。総所有コスト（TCO）の削減、資金の節約、成長促進を支援します。100 ヵ国以上で利用できる Cisco Capital の柔軟な支払いソリューションにより、ハードウェア、ソフトウェア、サービス、補完的なサードパーティ製機器を、お手軽で予測可能な支払い方法で取得できます。詳細はこちら

詳細情報

詳細については、Cisco AMP プライベート クラウド アプライアンスの Web ページを参照してください。

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

C78-742267-00JA 19.11