計画

Cisco Secure Malware Analytics アプライアンスは、出荷前にシスコの製造部門によってインストールされた Cisco Secure Malware Analytics ソフトウェアを備える Linux サーバです。Cisco Secure Malware Analytics アプライアンスを受け入れた場合、オンプレミスのネットワーク環境用に設定および構成する必要があります。

この章では、設定と構成の前に確認する必要がある環境、ハードウェア、およびネットワークの要件について説明します。

サポートされるブラウザ

Cisco Secure Malware Analytics は、次のブラウザをサポートしています。

- Google Chrome™

- Mozilla Firefox®
- Apple Safari®

（注） Microsoft® Internet Explorer® はサポートされて**いません**。

環境要件

Cisco Secure Malware Analytics アプライアンス（v2.7.2 以降）は、Cisco Secure Malware Analytics M5 アプライアンスサーバーに展開されます。Cisco Secure Malware Analytics アプライアンスをセットアップして設定する前に、『*Cisco Threat Grid M5* ハードウェア設置ガイド』の仕様に従って、電源、ラックスペース、冷却、およびその他の問題に必要な環境要件を満たしていることを確認してください。

ハードウェア要件

管理インターフェイスには、SFP+ フォームファクタが使用されています。Cisco Secure Malware Analytics アプライアンスをクラスタリングしている場合は、それぞれの顧客インターフェイスで追加の SFP+ モジュールが必要になります。

（注） SFP+ モジュールは、設定ウィザードを実行するセッションでCisco Secure Malware Analytics アプライアンスの電源を入れる前に接続する必要があります。

スイッチで使用できる SFP+ ポートがない、または SFP+ が望ましくない場合は、1000Base-T のトランシーバ（シスコ機器互換のギガビット RJ 45 銅線 SFP トランシーバモジュール Mini -GBIC - 10/100/1000 Base-T 銅線 SFP モジュールなど）を使用できます。

図 *1 : Cisco 1000BASE-T* 銅線 *SFP*（*GLC-T*）

サーバーにモニターを接続できます。または、Cisco Integrated Management Controller（CIMC）が設定されている場合は、リモート KVMを使用できます（UCS C220-M3 および C220-M4 サーバー上で）。

（注） CIMC は、Cisco Secure Malware Analytics M5 アプライアンス サーバではサポートされていません。

CISCO UCS Power Calculator は、推定電力を算出するために使用できます。

ネットワーク要件

Cisco Secure Malware Analytics アプライアンスには、次の 3 つのネットワークが必要です。

- **ADMIN**：Cisco Secure Malware Analytics アプライアンスの設定を行うには、管理ネットワークを設定する必要があります。
  - Admin UI 管理トラフィック（HTTPS）
  - SSH
  - NFSv4（発信。IP ではなく NFS ホスト名が使用される場合、この名前がダーティ DNS 経由で解決されます）。
- **クリーン**：クリーンネットワークは、インバウンド、Cisco Secure Malware Analytics アプライアンスへの信頼済みトラフィック（要求）、および Cisco E メール セキュリティ アプライアンスや Web セキュリティアプライアンスなどの統合アプライアンスに使用されます。統合アプライアンスは、クリーン インターフェイスの IP アドレスに接続します。

（注） クリーン ネットワーク インターフェイスの URL は Admin UI の設定が完了するまで機能しません。

注：以下の制限付きタイプのネットワークトラフィックは、クリーンインターフェイスから発信することができます。

- リモート syslog 接続
- Cisco Secure Malware Analytics アプライアンスによって送信される電子メールメッセージ
- Cisco Secure Endpoint プライベート クラウド デバイスへの配置更新サービス接続
- DNS 要求（上記のいずれかに関連するもの)
- LDAP
- RADIUS トラフィック

- **ダーティ**：「ダーティ」ネットワークは Cisco Secure Malware Analytics Appliance アプライアンスからの発信トラフィック（マルウェア トラフィックを含む）に使用されます。

（注） 内部ネットワークアセットを保護するために、企業の IP とは異なる専用の外部 IP アドレス（ダーティインターフェイスなど）を使用することをお勧めします。

ネットワーク インターフェイスの設定については、「ネットワーク インターフェイス」を参照してください。

DNS サーバ アクセス

配置更新サービスのルックアップ、リモートの Syslog 接続の解決、および Secure Malware Analytics ソフトウェアからの通知に使用されるメールサーバーの解決以外の目的に使用される DNS サーバーは、ダーティネットワークを介したアクセスが可能になっている必要があります。

デフォルトでは、DNS はダーティ インターフェイスを使用します。クリーン インターフェイスは Secure Endpoint プライベート クラウドの統合およびその他のサービスに使用されます。Secure Endpoints プライベート クラウドのホスト名がダーティ インターフェイスに解決できない場合、クリーン インターフェイスを使用する別の DNS サーバーを Admin UI に構成できます。

NTP サーバ アクセス

デフォルトで、NTP サーバは、ダーティ ネットワークを介してアクセスできる必要があります。

2.12 リリース以降、アプライアンスは、ダーティインターフェイス（デフォルト）ではなく、クリーンインターフェイスから NTP サーバーに接続するように任意で構成できます。これにより、内部 NTP サーバを使用できるようになります。

統合

Secure Malware Analytics アプライアンスを他の Cisco 製品（E メール セキュリティ アプライアンス、Web セキュリティ アプライアンス、または Secure Endpoint プライベート クラウドなど）とともに使用する場合、追加の計画が必要になることがあります。詳細については、「ESA/WSA を Threat Grid アプライアンスに接続する」を参照してください。

DHCP 要件

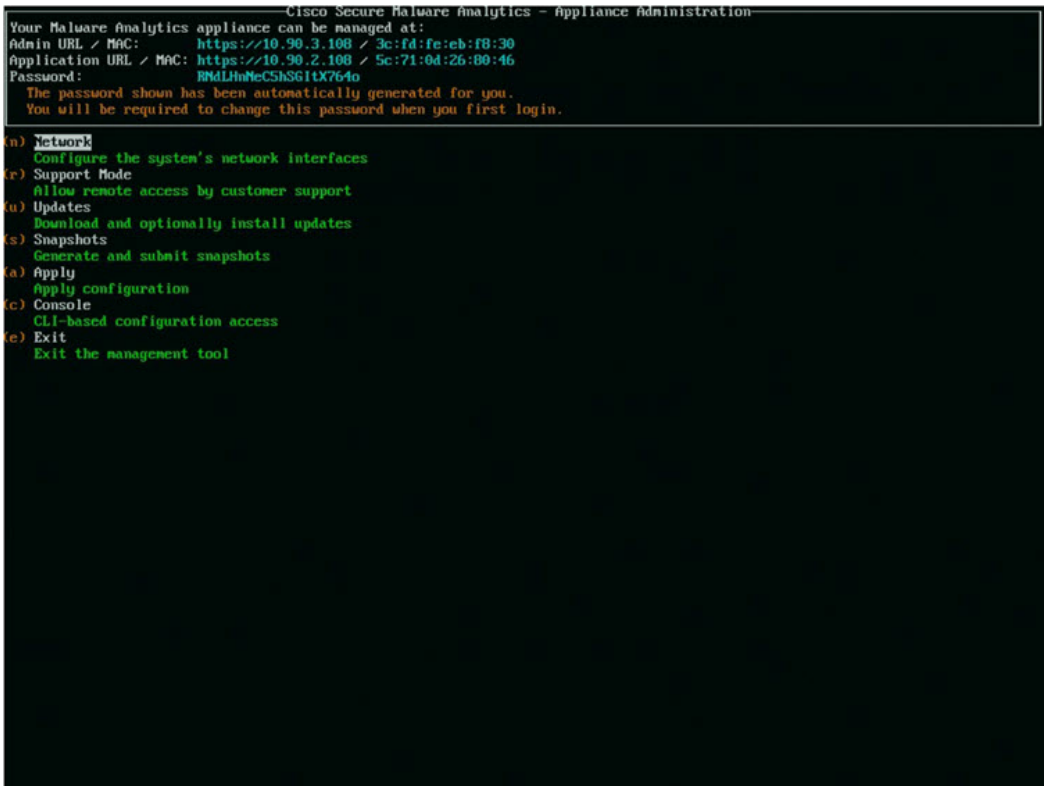
ただし、DHCPを使用するように設定されたネットワークに接続している場合は、要件を理解することが重要です。DHCP を使用する Cisco Secure Malware Analytics アプライアンスでは、DNS を明示的に指定する必要があります。

警告 DNS サーバーが明示的に指定されていないシステムのアップグレードは失敗します。

（注） Admin TUI には、Admin UI にアクセスして構成するために必要な情報が表示されます。アプライアンスの起動後、DHCPのIPアドレスが表示されるまでに時間がかかる場合があります。

Admin TUI（テキストモード UI）を開き、次の情報に注意してください。

図 *2 : Admin TUI*（*DHCP* を使用するためにネットワーク構成されて接続）



- [**Admin URL**]：管理ネットワーク。 Admin UI の残りの設定作業を継続するためにこのアドレスが必要です。
- [**Application URL**]：クリーンネットワーク。これは、 Admin UI で設定を完了した後に使用するアドレスです。

ダーティ ネットワークは表示されません。

- **[パスワード（Password）]**：Cisco Secure Malware Analytics アプライアンスのインストール時にランダムに生成される初期管理パスワード。後で、Admin UI 構成プロセスの最初の手順として、このパスワードを変更する必要があります。

最初の IP 割り当てを DHCP から静的 IP アドレスに変更する必要がある場合は、「ネットワークと DHCP の構成」を参照してください。

ライセンス

新しいアプライアンスを購入すると、ライセンスが生成され、**[構成（Configuration）] > [ライセンス（License）]**ページの**[サーバーからライセンスを取得（Retrieve License From Server）]**ボタンが有効になります。ただし、これが機能しない場合、または特別なケース（ライセンスがカスタム ワンオフであるなど）がある場合、ライセンスはパスワードを含む暗号化ファイルとして直接渡されます。

ライセンスに関して不明な点がある場合は、サポートにお問い合わせください。

レート制限

API サンプル送信レート制限は、ライセンス契約条件に基づいて Cisco Secure Malware Analytics アプライアンス全体に適用されます。API レート制限は API 送信にのみ適用され、手動によるサンプル送信には適用されません。

レート制限はカレンダー日ではなくローリング タイムの時間枠に基づきます。送信制限に達すると、次の API 送信の再試行まで待機する時間を通知するメッセージとともに、429 エラーが返されます。詳細については、ポータルのオンライン ヘルプを参照してください。

組織およびユーザー

Cisco Secure Malware Analytics アプライアンスの設定とネットワーク設定を完了したら、Cisco Secure Malware Analytics の初期組織を作成してユーザー アカウントを追加する必要があります。これにより、ユーザーはログインして、分析用にマルウェア サンプルの送信を開始できるようになります。このタスクでは、要件に応じて、複数の組織およびユーザ間のプランニングや調整が必要になることがあります。

詳細については、「新しい組織の作成」 および「Cisco Secure Malware Analytics ポータルヘルプ」（**[管理（Administration）] > [管理者ガイド（Administrator's Guide）]** をクリックして管理ガイドのトピックを開きます）を参照してください。

更新

更新プログラムをインストールする前に、初期 Cisco Secure Malware Analytics アプライアンスのセットアップと設定手順を**完了する必要があります**。このガイドに記載されている初期構成の完了後、すぐに更新を確認することをお勧めします（『*Cisco Threat Grid Appliance Getting Started Guide*』を参照）。

Cisco Secure Malware Analytics アプライアンスのセットアップと設定手順 アプライアンスの更新は、ライセンスがインストールされ、カスタマー サポートにより別段指示される場合を除き、ダウンロードできません。また、更新プロセスでは、最初のアプライアンスの設定が完了している必要があります。更新は、順に実行する必要があります。

ユーザー インターフェイス

サーバをネットワークに接続し、正常に起動した後で Secure Malware Analytics アプライアンスを構成するために、複数のユーザ インターフェイスを利用できます。

（注） LDAP 認証は、管理 TUI および管理 UI で使用できます。RADIUS 認証は、Secure Malware Analytics アプリケーション UI（バージョン 2.10 以降）で使用できます。

管理 TUI

Admin TUI インターフェイスは、 ネットワーク インターフェイスを設定するために使用されます。Cisco Secure Malware Analytics アプライアンスが正常に起動すると、Admin TUI が表示されます。

Admin TUI への再接続

Admin TUI はコンソール上で開いたままになり、アプライアンスにモニターを接続するか、（CIMC が設定されている場合は）リモート KVM を使用することでアクセスできます。

（注） CIMC は、Cisco Secure Malware Analytics M5 アプライアンス サーバではサポートされていません。

Admin TUI に再接続するには、ユーザー「**threatgrid**」として管理 IP アドレスに SSH 接続します。

必要なパスワードは、ランダムに生成される初期パスワードであり、最初に Admin TUI に表示されたパスワードか、OpAdmin 設定の最初の手順で作成した新しい管理者パスワードです（『*Cisco Threat Grid Appliance Getting Started Guide*』を参照してください）。

Threat Grid シェル（tgsh）

Threat Grid シェル（tgsh）は、コマンド（estroy-data や forced backup など）を実行するために使用される管理者のインターフェイスであり、専門家による低レベルのデバッグにも使用されます。tgsh にアクセスするには、管理 TUI で **[コンソール（CONSOLE）]** を選択します。

（注） Admin UI は Cisco Secure Malware Analytics ユーザーと同じログイン情報を使用するため、tgsh を介して行われたパスワードの変更や更新は Admin UI にも影響します。

注意 tgsh によるネットワーク設定の変更は、Cisco Secure Malware Analytics サポートによって特に指示された場合を除き、サポートされません。代わりに Admin UI または Admin TUI ダイアログを使用する必要があります。2.12 リリースでは、管理者の電子メール、Grovebox URL、SMTP 設定などを変更するオプションが削除されました。アプライアンスのワイプ操作が、ブートローダメニューではなく、リカバリモード tgsh 内でアクティブ化されるようになりました。

Admin UI

Admin UI は、Cisco Secure Malware Analytics アプライアンスの管理者の主な構成インターフェイスです。Cisco Secure Malware Analytics アプライアンスの管理インターフェイスで IP アドレスが設定された後に使用できる Web ポータルです。

ライセンス、電子メールホスト、SSL 証明書など、Cisco Secure Malware Analytics アプライアンス設定の多くは Admin UI からのみ実行できます。

（注） 初期設定および構成ウィザードについては、『Cisco Secure Malware Analytics アプライアンスの設定およびコンフィギュレーション ガイド』を参照してください。

Admin UI のコンポーネント

次のセクションでは、Admin UI を使用して設定するために必要な詳細について説明します。

- ホーム
- 設定
- ステータス（Status）
- 操作（Operations）
- サポート

Cisco Secure Malware Analytics ポータル

Cisco Secure Malware Analytics のユーザー インターフェイス アプリケーションは、クラウド サービスとして利用でき、Cisco Secure Malware Analytics アプライアンスにもインストールされています。Cisco Secure Malware Analytics クラウドサービスと、Cisco Secure Malware Analytics アプライアンスに含まれる Cisco Secure Malware Analytics ポータルの間に通信はありません。

ネットワーク インターフェイス

使用可能なネットワーク インターフェイスを次の表に示します。

インターフェイス	説明
Admin	• 管理ネットワークに接続します。管理ネットワークからの**着信のみ**。 • Admin UI トラフィック • Admin TUI 用の SSH（インバウンド） • バックアップとクラスタリング用の NFSv4（発信）IP ではなく NFS ホスト名が使用される場合、この名前がダーティ DNS 経由で解決されます）。すべてのクラスタ ノードからアクセスできる必要があります。 • Admin ポートは（tgsh シェルから）v2.11 で Admin UI から無効にすることができます。無効になっている場合、クラスタ化されていない Cisco Secure Malware Analytics アプライアンスは、クリーン ポートとダーティー ポートが接続されている場合のみ正しく動作します。管理 UI はクリーン インターフェイスのポート 8443（v2.11 リリースではポート 18443 も）に表示されます。ポートが無効になっていない場合、管理ポートを切断すると、Cisco Secure Malware Analytics アプライアンスの一部しか機能しなくなります（または、最高でも部分的にしか機能しません）。 **（注）** 管理インターフェイス用のフォーム ファクタは SFP+ です。「ハードウェア要件」を参照してください。
クラスタ	管理用ではない SFP+ ポートはクラスタリングに使用されます。 • クラスタリングに必要なクラスタ インターフェイス（任意） • ダイレクト インターコネクトには追加の SFP+ モジュールが必要です。このインターフェイスでは、設定の必要はありません。アドレスが自動的に割り当てられます。

インターフェイス	説明
[クリーン（Clean）]	• クリーンネットワークに接続します。クリーンには、社内ネットワークからアクセスできる必要がありますが、インターネットへの発信アクセスができないようにする必要があります。 • UI および API トラフィック（着信） • サンプルの送信 • SMTP（設定済みメール サーバーへの発信接続） • SSH（Admin TUI 用のインバウンド） • syslog（設定済み syslog サーバーへの発信） • ESA/WSA と CSA の統合 • Secure Endpoint プライベート クラウド統合 • DNS（オプション） • LDAP（発信） • RADIUS（発信） • [NTP]（内部 NTP サーバーを使用する場合）

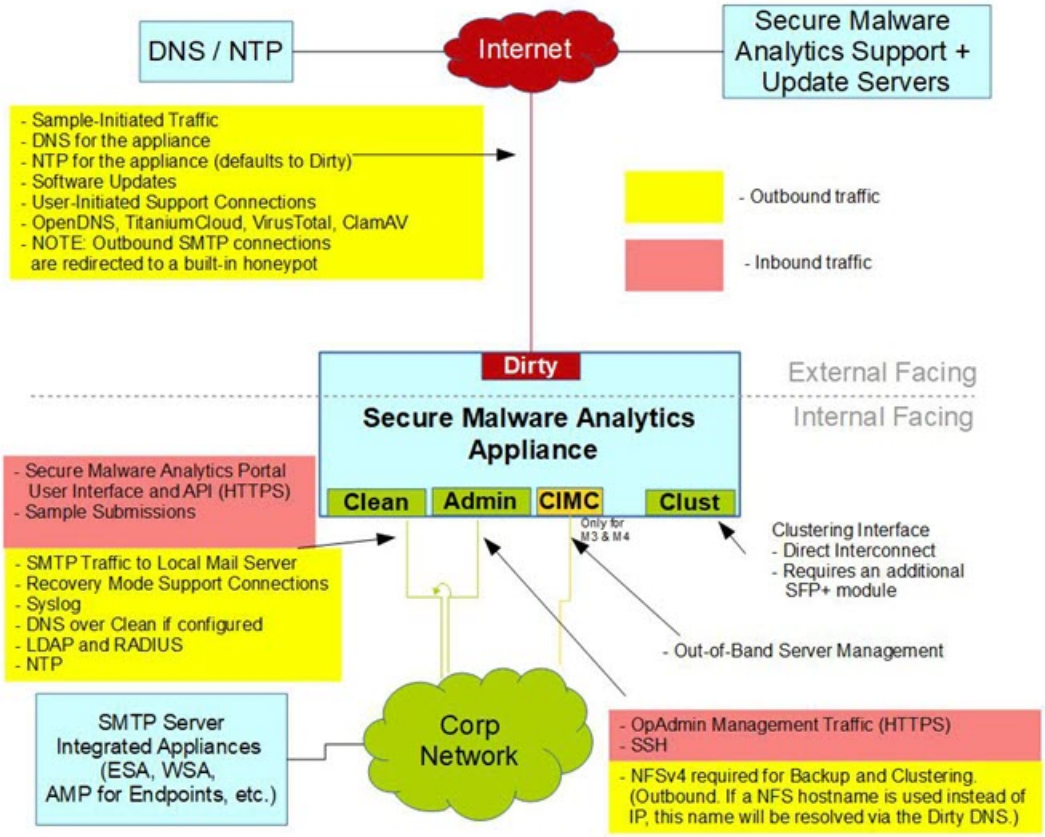
インターフェイス	説明
ダーティ	ダーティネットワークに接続します。インターネットアクセスが必要です。発信のみ。 プライベート IP に送信されるトラフィックは、ネットワーク出口のローカリゼーション ファイアウォールでドロップされるため、ダーティインターフェイスには独自の DNS（プライベート IP）を使用しないようにしてください。 • DNS （注） Cisco Secure Endpoint プライベートクラウドとの統合を設定し、Cisco Secure Endpoints アプライアンスのホスト名がダーティインターフェイスで解決できない場合、クリーンインターフェイスを使用する別の DNS サーバーを Admin UI に設定できます。 • NTP（デフォルトは Dirty） • 更新 • サポート セッション • サポートスナップショット • マルウェアサンプルから開始されたトラフィック • OpenDNS, TitaniumCloud, VirusTotal, ClamAV_signature updates • SMTP の発信接続が組み込みのハニーポットにリダイレクト （注） ダーティインターフェイスでの IPv4LL アドレス空間（168.254.0.16）の使用はサポートされていません。
CIMC インターフェイス	Cisco Integrated Management Controller（CIMC）インターフェイスが設定されている場合は、サーバーの管理とメンテナンスに使用できます。「CIMC の構成」を参照してください。 （注） CIMC は、Cisco Secure Malware Analytics M5 アプライアンス サーバではサポートされていません。

ネットワーク インターフェイスの設定図

このセクションでは、Cisco Secure Malware Analytics アプライアンスの最も論理的で推奨される設定について説明します。ただし、お客様によってインターフェイス設定は異なります。

ネットワーク要件に従って、ダーティインターフェイスを内部に接続する場合や、クリーンインターフェイスを適切なネットワークセキュリティ対策が施されている外部に接続する場合があります。

図 *3:* ネットワーク インターフェイスの設定図



（注） Cisco Secure Malware Analytics アプライアンス（v 2.7.2 以降）では、 **enable_clean_interface** オプションは使用できますが、デフォルトでは無効になっています。このオプション（設定を適用して再起動した後）は、割り当てられたクリーン IP のポート 8443 および 18443 の管理インターフェイスへのアクセスを有効にします。管理イーサネットインターフェイスを無効にすると、クリーンのポート 8843 でのこのアクセスも有効になります。

ファイアウォール ルール

ここでは、推奨されるファイアウォールルールについて説明します。

（注） ポート 22 および 19791 のダーティインターフェイス上で制限付きの発信ポリシーを実装すると、経時的な更新の追跡が必要となり、ファイアウォールの維持等により多くの時間がかかる可能性があります。

（注） ダーティインターフェイスでの IPv4LL アドレス空間（168.254.0.16）の使用はサポートされていません。

ダーティ インターフェイスによる発信

送信元	送信先	プロトコル	ポート	操作	コメント
ダーティインターフェイス	インターネット	ANY	ANY	許可（Allow）	サンプルからのアウトバウンドトラフィックを許可します。オプションで、Cisco のデータセンターを介してプロキシされます。（正確な結果を取得するには、指定されたポートやプロトコルにかかわらず、マルウェアからコマンド アンド コントロール サーバーへのアクセスが許可されている必要があります。）

ダーティ インターフェイスによる着信

送信元	送信先	プロトコル	ポート	操作	コメント
ANY	ダーティインターネット	ANY	ANY	拒否（Deny）	すべての着信接続を拒否します。

クリーン インターフェイスによる発信

送信元	送信先	プロトコル	ポート	操作	コメント
クリーンインターフェイス	SMTP サーバー	TCP	25	許可（Allow）	アプライアンスはクリーン インターフェイスを使用して、設定済みメールサーバーへの SMTP 接続を開始します

クリーンインターフェイスによる発信（任意）

送信元	送信先	プロトコル	ポート	操作	コメント
クリーンインターフェイス	企業の DNS サーバー	TCP/UDP	53	許可（Allow）	任意。クリーン DNS が構成されている場合のみ必須
クリーンインターフェイス	AMP プライベート クラウド	TCP	443	許可（Allow）	任意。Cisco Secure Endpoint プライベート クラウド統合が使用されている場合のみ必須。
クリーンインターフェイス	Syslog サーバー	UDP	514	許可（Allow）	Syslog メッセージおよび Cisco Secure Malware Analytics 通知を受信するように指定されたサーバへの接続を許可
クリーンインターフェイス	LDAP サーバー	TCP/UDP	389	許可（Allow）	任意。LDAP が構成されている場合のみ必須
クリーンインターフェイス	LDAP サーバー	TCP	636	許可（Allow）	任意。LDAP が構成されている場合のみ必須
クリーンインターフェイス	RADIUS サーバー	DTLS	2083	許可	Cisco Secure Malware Analytics アプリケーション UI（Face）へのログインを許可します。任意。RADIUS が設定されている場合のみ必須。
クリーンインターフェイス	インターネット	UDP	123	許可（Allow）	オプションで、このオフバイ デフォルト機能を使用して、内部 NTP サーバーを使用できます。

クリーン インターフェイスによる着信

送信元	送信先	プロトコル	ポート	操作	コメント
ユーザー サブネット	クリーン インターフェイス	TCP	22	許可（Allow）	Admin TUI への SSH 接続を許可します。

送信元	送信先	プロトコル	ポート	操作	コメント
ユーザーサブネット	クリーン インターフェイス	TCP	80	許可（Allow）	アプライアンス API と Cisco Secure Malware Analytics のユーザーインターフェイス。これは HTTPS TCP/443 にリダイレクトします。
ユーザーサブネット	クリーン インターフェイス	TCP	443	許可（Allow）	アプライアンス API と Cisco Secure Malware Analytics のユーザーインターフェイス。
ユーザーサブネット	クリーン インターフェイス	TCP	9443	許可	Cisco Secure Malware Analytics UI Glabbox への接続を許可します。

管理インターフェイスによる発信（任意）

以下は、設定されるサービスの内容に依存します。

送信元	送信先	プロトコル	ポート	操作	コメント
管理インターフェイス	NFSv4 サーバー	TCP	2049	許可（Allow）	任意。Secure Malware Analytics アプライアンスが NFSv4 共有にバックアップを送信するように設定されている場合のみ必須。

管理インターフェイスによる着信

送信元	送信先	プロトコル	ポート	操作	コメント
管理サブネット	管理インターフェイス	TCP	22	許可（Allow）	Admin TUI への SSH 接続を許可します。
管理サブネット	管理インターフェイス	TCP	80	許可（Allow）	Admin UI へのアクセスを許可します。これは HTTPS TCP/443 にリダイレクトします。
管理サブネット	管理インターフェイス	TCP	443	許可（Allow）	Admin UI へのアクセスを許可します。

シスコ未検証/導入が推奨されるダーティ インターフェイス

Cisco 以外の検証済み/推奨 ：ファイアウォール アウトバウンド トラフィックは、マルウェアがコマンドアンドコントロールインフラストラクチャに接続するのを防ぎ、そのコマンドアンドコントロール インフラストラクチャからダウンロードされるものを決定する試みを制限することで有効性を低下させる可能性があります。

送信元	送信先	プロトコル	ポート	操作	コメント
ダーティインターフェイス	インターネット	TCP	22	許可（Allow）	更新、サポートスナップショット、ライセンスのサービス。
ダーティインターフェイス	インターネット	TCP/UDP	53	許可（Allow）	発信 DNS を許可。
ダーティインターフェイス	インターネット	UDP	123	許可（Allow）	発信 NTP を許可します。
ダーティインターフェイス	インターネット	TCP	19791	許可（Allow）	Cisco Secure Malware Analytics サポートへの節ゾックを許可します。
ダーティインターフェイス	Cisco Umbrella	TCP	443	許可（Allow）	サードパーティの検出およびエンリッチメントサービスと結合します。
ダーティインターフェイス	VirusTotal	TCP	443	許可（Allow）	サードパーティの検出およびエンリッチメントサービスと結合します。
ダーティインターフェイス	TitaniumCloud	TCP	443	許可（Allow）	サードパーティの検出およびエンリッチメントサービスと結合します。

プライバシーとサンプルの可視性

分析のため Cisco Secure Malware Analytics アプライアンスにサンプルを送信する際、コンテンツのプライバシーが重要な考慮事項となります。機密文書やアーカイブタイプの資料が分析用に送信される場合、プライバシーは特に重要な考慮事項になります。機密情報を見つけることは、特に検索 API を使用して Cisco Secure Malware Analytics アプライアンスにアクセスできるユーザーにとって、比較的簡単である可能性があるためです。

Cisco Secure Malware Analytics へのサンプル送信に関するプライバシーとサンプルの可視性モデルは次のとおりです。

- サンプルは、プライベートに指定されていない限り、送信者の組織外のユーザーに表示されます。
- プライベートサンプルは、サンプルを送信したユーザーと同じ組織内の Cisco Secure Malware Analytics ユーザーのみが閲覧できます。

統合により送信されたサンプル

統合から送信されたサンプルの場合、 Cisco Secure Malware Analytics アプライアンスでのプライバシーおよびサンプルの可視性モデルは変更されます。統合とは、E メール セキュリティ アプライアンス（ESA）、Web セキュリティアプライアンス（WSA）および他のデバイスなどのシスコ製品や、サードパーティのサービスのことです（CSA 統合という用語は、Cisco Sandbox API 経由で Cisco Secure Malware Analytics アプライアンスに統合（または登録）されている、ESA/WSA その他の Cisco 製アプライアンス、デバイス、サービスを意味します）。

Cisco Secure Malware Analytics アプライアンスでのすべてのサンプル送信は、デフォルトでパブリックに設定されるため、所属する組織にかかわりなく、統合を含む他のすべてのアプライアンスユーザーが表示できます。アプライアンスのすべてのユーザが、他のすべてのユーザが送信したサンプルのあらゆる詳細を確認できるということです。

Cisco Secure Malware Analytics のユーザーはまた、プライベートなサンプルも Cisco Secure Malware Analytics アプライアンスに送信します。それは統合に含まれ、サンプルの送信者と同じ組織からの他の Cisco Secure Malware Analytics アプライアンス ユーザーにのみ表示されます。

次の表で、Cisco Secure Malware Analytics アプライアンスでのプライバシーおよびサンプルの可視性モデルについて説明します。

図 *4 : Cisco Secure Malware Analytics* アプライアンスでのプライバシーと可視性

Sample and Analysis Results are visible to:	Public Submissions (Default)	Private Submissions	CSA Integration Submissions (Public by Default)
Users from the Same Organization	✔	✔	✔
Users from a Different Organization	✔	✔	✔
CSA Integrations from the Same Organization	✔	✔	✔
CSA Integrations from a Different Organization	✔	✖	✔

- **フルアクセス**：緑色のチェックマークは、ユーザーがサンプルと分析結果にフルアクセスできることを示します。
- **スクラビングレポート**：灰色のチェックマークは、プライベート送信の結果がスクラビングされたことを示します。ユーザーはサンプルと分析結果への部分的なアクセス権を持っていますが、サンプルに関する潜在的な機密情報はすべて削除されます。Glovebox には、ファイル名、プロセス名、スクリーンショット、またはアクティビティについての詳細情報は表示されません。

  サンプルの送信者のログイン情報などの詳細情報を [Metadata] セクションから除外します。ビジネスの過程でプライベートサンプルからハッシュが発生した場合、既知の脅威に対する警告が表示されます。さらに詳細な情報が必要な場合は、完全な分析のためにサンプルの独自のコピーを送信します。

  プライベートサンプルはダウンロードされない場合があります。スクラビングレポートには、アーティファクト（ファイル名が削除されたもの）、動作インジケータ、ドメイン、IP が含まれます。
- **アクセスなし**：赤色のXは、ユーザーがサンプルまたは分析結果にアクセスできないことを示します。

同じ基本的なプライバシー ルールが Cisco Secure Endpoint プライベート クラウドと Cisco Secure Malware Analytics アプライアンスの統合に適用されます。

アプライアンスのワイプ動作

Wipe アプライアンスの動作を使用すると、Cisco Secure Malware Analytics アプライアンスのディスクをワイプして、廃棄前にすべてのデータを削除したり、Cisco Demo Loan Program に戻したりすることができます。

重要 アプライアンスのワイプ手順を実行すると、Cisco Secure Malware Analytics アプライアンスは、再イメージ化のためにシスコに返却せずに動作しなくなります（但し、デモ ローン プログラムのお客様を除き、事前の合意がない場合、再イメージ化サービスを利用できることは保証されません）。

詳細については、「アプライアンスのワイプ操作によるすべてのデータの削除」を参照してください。

お客様のデータ

ログ、アクティブな設定、およびその他のお客様所有データは、データと OS ドライブに分散されるのではなく、ほぼ排他的にRAID 5データアレイに保存されます。OS ドライブに保存される残りのアプライアンス固有のコンテンツは、データドライブがマウントできない場合にリ

カバリモードを正しく動作させるために必要な情報に限定され、開示してもプライバシーへの影響は限定されます。

2.12 リリースでは OS アレイに保存されるコンテンツが少ないため、初期のアプライアンス（より小さい OS ドライブを搭載）では、データリセット中に必須のデフォルトイメージ以外の VM イメージを削除する（したがって、削除された VM イメージが再び利用可能になります）。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。