はじめに

この章では、Cisco Secure Malware Analytics アプライアンスの概要、対象読者、および関連する製品マニュアルへのアクセス方法について説明します。ここでは、次の項目について説明します。

Cisco Secure Malware Analytics アプライアンスについて

Cisco Secure Malware Analytics アプライアンスは、詳細な脅威分析およびコンテンツ分析を使用して、安全性に優れたオンプレミスの高度なマルウェア分析を提供します。Cisco Secure Malware Analytics アプライアンスは、完全なマルウェア分析プラットフォームを提供し、Cisco Secure Malware Analytics M5 アプライアンスサーバー（v2.7.2 以降）にインストールされます。さまざまなコンプライアンスおよびポリシーの制限に基づいて運営されている組織が、マルウェアサンプルをアプライアンスに送信できるようにします。

（注） Cisco UCS C220 M4（TG5400）サーバーは、Cisco Secure Malware Analytics アプライアンスで引き続きサポートされていますが、サーバーのサポートは終了しています。手順については、『*Cisco Secure Malware Analytics Appliance Setup and Configuration Guide*』（バージョン 2.7 以前）のサーバーの設定の章を参照してください。

銀行や医療サービスなどの機密データを扱う組織の多くは、マルウェアアーティファクトといった特定の種類のファイルをマルウェア分析のためにネットワーク外に送信することを許可

しない、さまざまな規制ルールおよびガイドラインに従う必要があります。Cisco Secure Malware Analyticsアプライアンスをオンプレミスで維持することにより、組織はネットワークを離れることなく、疑わしいドキュメントやファイルを分析対象として送信できます。

Cisco Secure Malware Analytics アプライアンスを使用することで、セキュリティチームは非常にセキュアな独自の静的および動的分析テクニックを使用し、すべてのサンプルを分析できるようになります。アプライアンスでは、分析結果を数億もの分析済みマルウェアアーティファクトと関連付け、マルウェア攻撃、キャンペーン、およびその配布状況をグローバルに把握できるようにします。観測された 1 つの活動/特性サンプルを他の数百万ものサンプルとすみやかに関連付け、比較することで、過去の履歴やグローバルなコンテキストに照らして、その動作を十分に理解できます。この機能は、高度なマルウェアからの脅威と攻撃に対して、セキュリティ チームが効果的に組織を守るために役立ちます。

対象読者

新しいアプライアンスをマルウェアの分析に使用する前に、組織のネットワークに合わせてセットアップおよび構成する必要があります。このガイドは、新しい Cisco Secure Malware Analytics アプライアンスの設定および構成タスクを担当するセキュリティチームの IT スタッフを対象としています。

このドキュメントでは、マルウェアのサンプルを分析に送信するまでを対象とした、新しい Cisco Secure Malware Analytics アプライアンスの初期設定および構成を完了する方法について説明します。

前提条件

『*Cisco Secure Malware Analytics Appliance Administration Guide*』で説明されているように、必要な情報を収集し、計画手順を完了していることを前提としています。

また、『*Cisco Secure Malware Analytics M5 Hardware Installation Guide*』の指示に基づいて、Cisco Secure Malware Analytics アプライアンスをすでにセットアップしていることも前提としています。

これら2つのタスクをまだ完了していない場合は、このスタートガイドで説明されている手順を開始する前に完了してください。

製品に関する資料

Cisco Secure Malware Analytics アプライアンス製品に関する資料の最新バージョンは、Cisco.com から入手できます。

- *Cisco Secure Malware Analytics Appliance Release Notes*
- *Cisco Secure Malware Analytics Version Lookup Table*
- *Cisco Secure Malware Analytics Appliance Administration Guide*

- *Cisco Secure Malware Analytics M5 Hardware Installation Guide*

（注） Cisco Secure Malware Analytics M5 アプライアンスは、Cisco Secure Malware Analytics バージョン 3.5.27 以降、およびアプライアンスバージョン 2.7.2 以降でサポートされています。

（注） Cisco Secure Malware Analytics アプライアンスの以前のバージョンの製品ドキュメントは、Cisco Secure Malware Analytics のインストールとアップグレードにあります。

Cisco Secure Malware Analytics ポータル UI オンラインヘルプ

リリースノート、Cisco Secure Malware Analytics オンラインヘルプ、API ドキュメント、およびその他の情報を含む Cisco Secure Malware Analytics ポータル ユーザー ドキュメントは、ユーザーインターフェイス上部のナビゲーションバーにある [ヘルプ（Help）] メニューから入手できます。

このリリースの最新情報

バージョン 2.18 のこのガイドでは、次の変更が行われました。

表 *1* : バージョン *2.18* リリースの変更点：*2022* 年 *10* 月 *1* 日

機能または更新	セクション
スクリーンショットと手順を更新しました。	管理 UI の設定

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はサポートされません。

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**。初期設定の完了直後に、更新を確認することをお勧めします（「更新のインストール」を参照）。

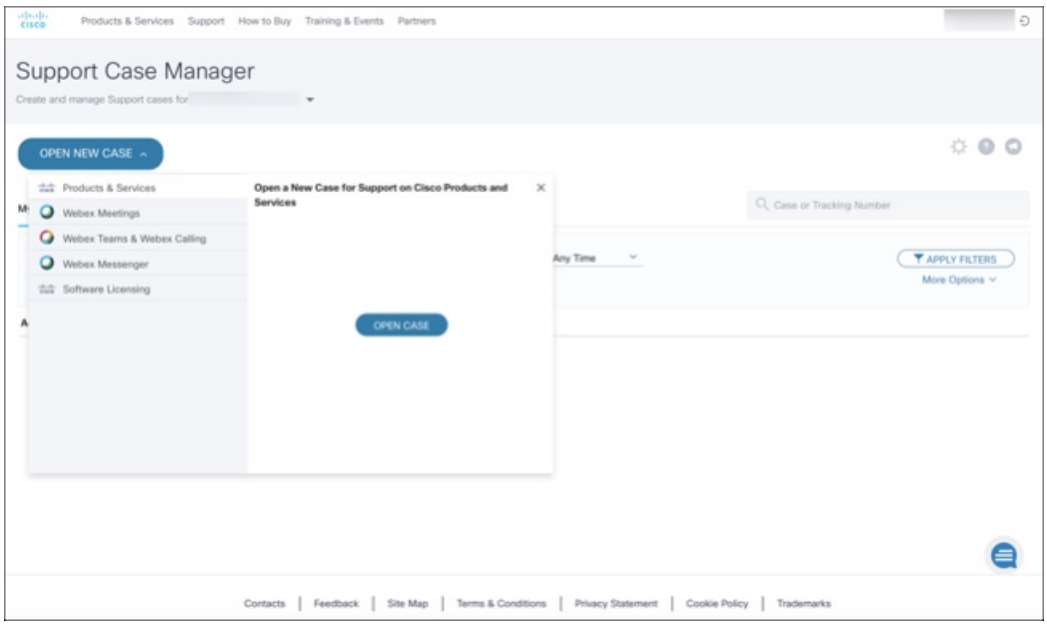
Cisco Secure Malware Analytics アプライアンスのセットアップと設定手順 アプライアンスの更新は、ライセンスがインストールされるまでダウンロードできません。また、更新プロセスでは、アプライアンスの初期設定が完了している必要があります。更新は、順に実行する必要があります。

サポート

Cisco Secure Malware Analytics に関するご質問やサポートについては、
https://mycase.cloudapps.cisco.com/case でサポートケースをオープンしてください。

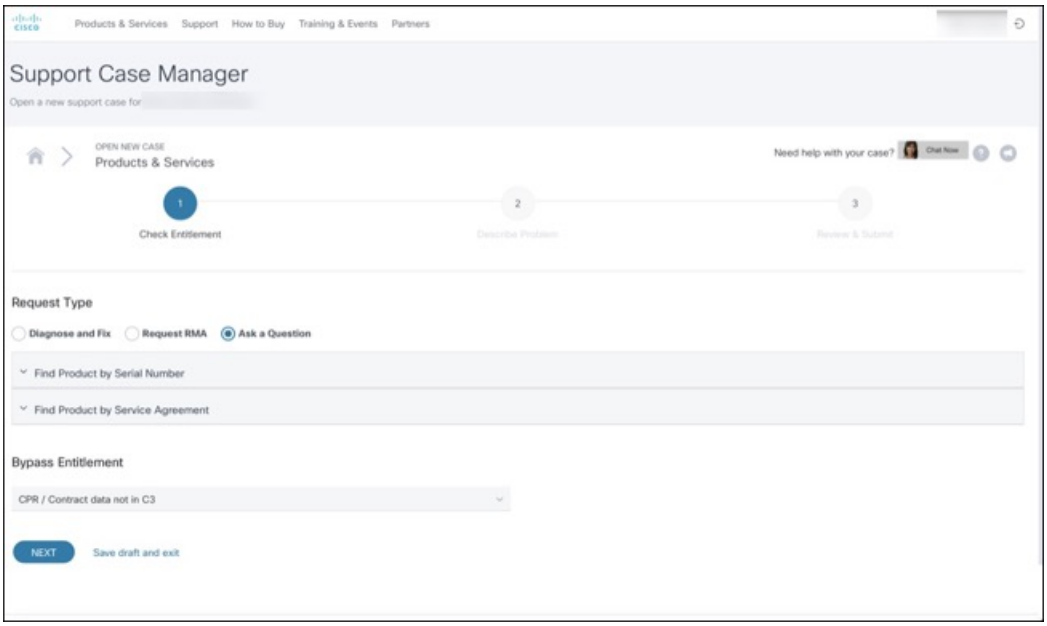
ステップ 1 Support Case Manager で、**[Open New Case] > [Open Case]** をクリックします。

図 *1*: 新しいケースをオープンする



ステップ 2 [**Ask a Question**] オプションボタンをクリックし、使用中のシスコセキュリティ**製品シリアル番号**または**製品サービス契約**を検索します。検索の対象は、Cisco Secure Malware Analytics のシリアル番号またはサービス契約である必要があります。

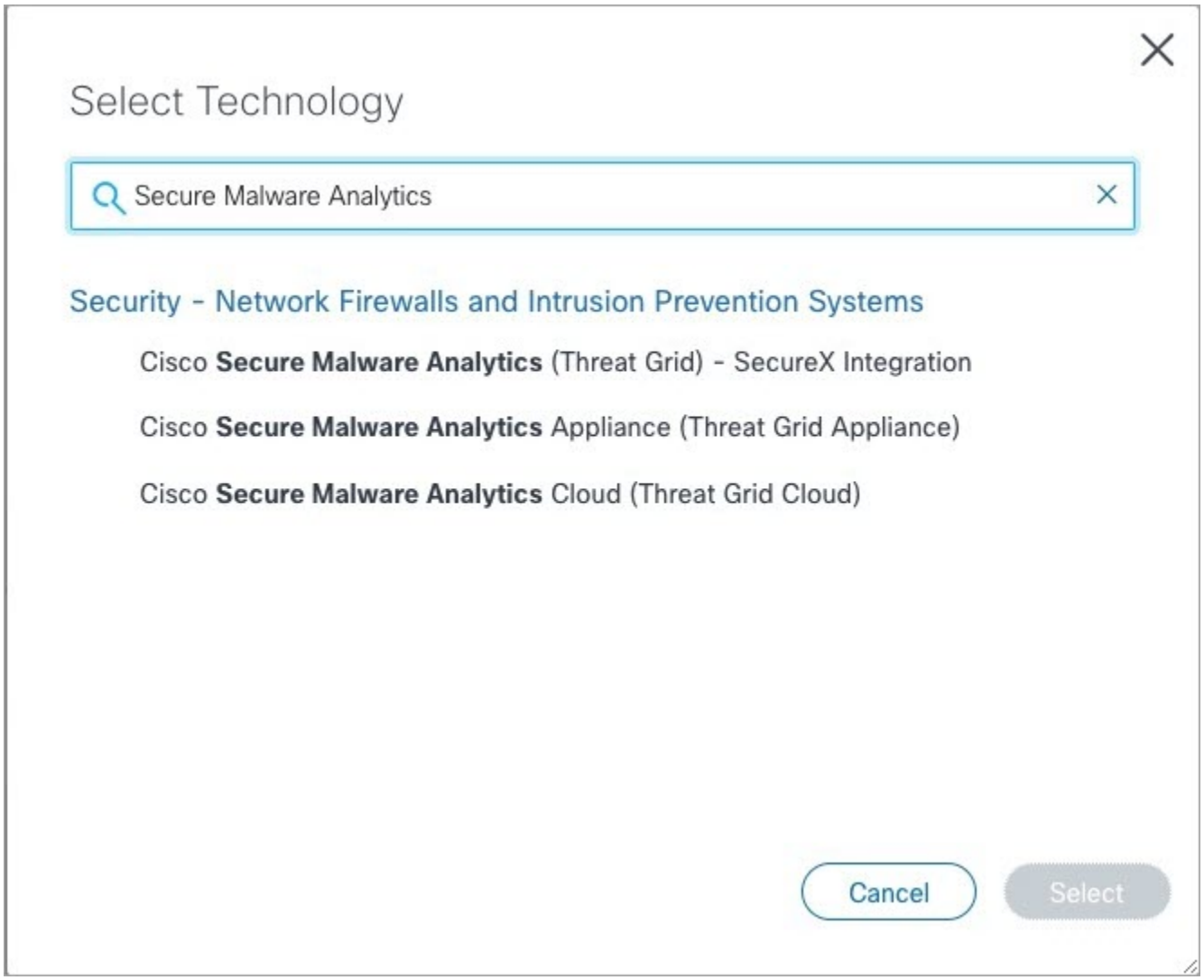
図 *2 :* エンタイトルメントのチェック



ステップ 3 [問題の説明（Describe Problem）] ページで、問題の [タイトル（Title）] と [説明（Description）] を入力します（タイトルで Cisco Secure Malware Analytics に言及してください）。

ステップ 4 [テクノロジーを手動で選択（Manually Select A Technology）] をクリックして、[Cisco Secure Malware Analytics] を検索します。

図 *3:* テクノロジーの選択



ステップ 5 リストから [Cisco Secure Malware Analyticsアプライアンス（Cisco Secure Malware Analytics Appliance）] を選択し、[選択（Select）] をクリックします。

ステップ 6 フォームの残りの部分をすべて入力し、[**Submit**] をクリックします。

ケースをオンラインで開くことができない場合は、シスコサポートにお問い合わせください。

- **米国およびカナダ**：1-800-553-2447
- **各国の連絡先**：https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

サポートを依頼する方法の詳細については、以下を参照してください。

- 『*Cisco Secure Malware Analytics Appliance Administration Guide*』の「サポートモードとサポートスナップショットの有効化」を参照してください。

- 次のブログ記事を参照してください。『**Changes to the Cisco Secure Malware Analytics Support Experience**』（https://community.cisco.com/t5/security-blogs/changes-to-the-cisco-threat-grid-support-experience/ba-p/3911407）
- https://www.cisco.com/c/en/us/support/index.html で**シスコサポート & ダウンロード**のメインページを参照してください。

設定と構成の概要

このドキュメントでは、次の設定および初期構成の手順を説明します。

- 初期ネットワーク設定
- 管理 UI の設定
- 更新のインストール
- アプライアンス設定のテスト

（注） 設定を完了するには、約 1 時間かかります。

管理者の設定が必要な追加のタスク（ライセンスのインストール、電子メールサーバー、SSL 証明書など）については、『*Cisco Secure Malware Analytics Appliance Administration Guide*』に記載されています。

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。