はじめに

この章では、Cisco Threat Grid アプライアンスの概要、対象読者、および関連する製品ドキュメント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 Threat Grid アプライアンスについて

Cisco Threat Grid アプライアンスは、詳細な脅威分析とコンテンツによる高度なマルウェア分析を、安全で高度にセキュアなオンプレミスで提供します。Threat Grid アプライアンスは、Cisco Threat Grid M5 アプライアンスサーバ（v 2.7.2 以降）にインストールされた完全な Threat Grid マルウェア分析プラットフォームを提供します。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している組織が、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-M3（TG5000）および Cisco UCS C220 M4（TG5400）サーバは、引き続き Threat Grid アプライアンスで使用できますが、サーバのサポートは終了しています。手順については、『*Cisco Threat Grid* アプライアンス設定および構成ガイド』（バージョン 2.7 以前）のサーバ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多くの組織は、マルウェアアーティファクトなどの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 Threat Grid 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。

Threat Grid 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つのアクティビティおよび特性の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事例に照らして、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。

このリリースの最新情報

バージョン 2.9 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 *2.9Mfg* の変更点 - *2019* 年 *12* 月 *17* 日

機能または更新	セクション
変更なし	

表 *2 :* バージョン *2.9* の変更点 - *2019* 年 *12* 月

機能または更新	セクション
管理ポートを無効にするための Threat Grid Shell コマンド。	Threat Grid シェル（tgsh）
ネットワークインターフェイスを更新して、管理ポートを無効にする機能が管理インターフェイスに含まれるようにしました。	ネットワーク インターフェイス
Threat Grid Web ポータル UI 管理者パスワードを更新	ログイン名とパスワード（デフォルト） アプライアンス設定のテスト
サポート情報が更新されました。	Threat Grid のサポート

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 Threat Grid 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、新しい Threat Grid アプライアンスで分析用のマルウェア サンプルを送信できるようにするまでの初期セットアップと設定の方法について説明します。

製品に関する資料

Cisco Threat Grid 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 Threat Grid アプライアンス リリースノート*
- *Cisco Threat Grid バージョン ルックアップ テーブル*
- *Cisco Threat Grid アプライアンス管理者ガイド*
- *Cisco Threat Grid M5 ハードウェア設置ガイド*

（注） Cisco Threat Grid M5 アプライアンスは、Threat Grid 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） 以前のバージョンの Cisco Threat Grid アプライアンス製品マニュアルは、Threat grid インストールとアップグレードにあります。

Threat Grid Portal UI オンラインヘルプ

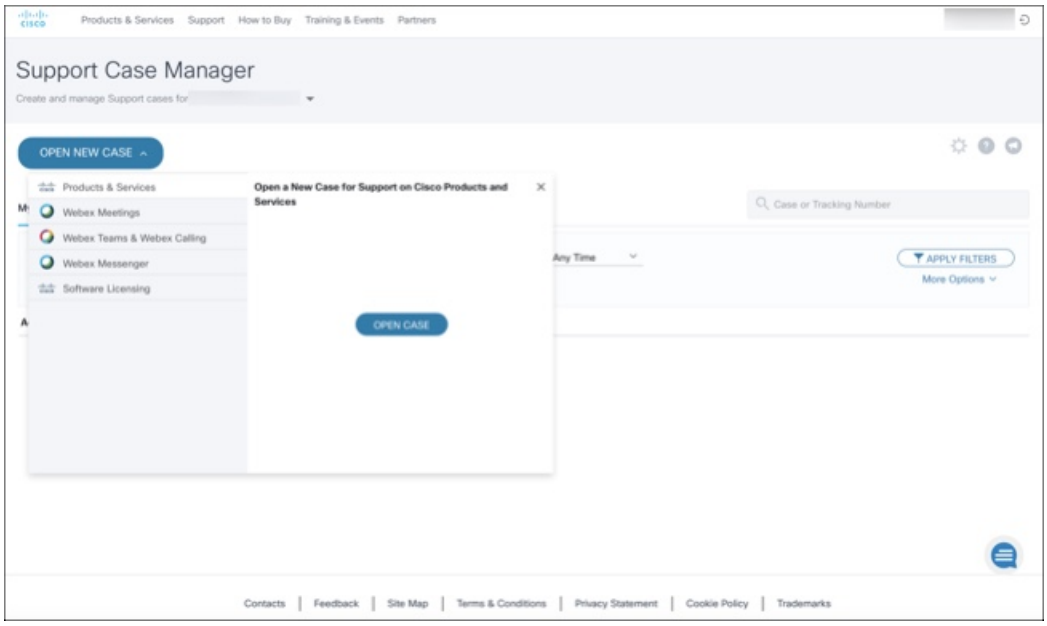
リリースノート、Threat Grid オンラインヘルプ、API ドキュメント、およびその他の情報を含む Threat Grid Portal ユーザドキュメントは、ユーザインターフェイス上部のナビゲーションバーにある [Help] メニューから入手できます。

Threat Grid のサポート

Threat Grid に関するご質問や支援が必要な場合は、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。

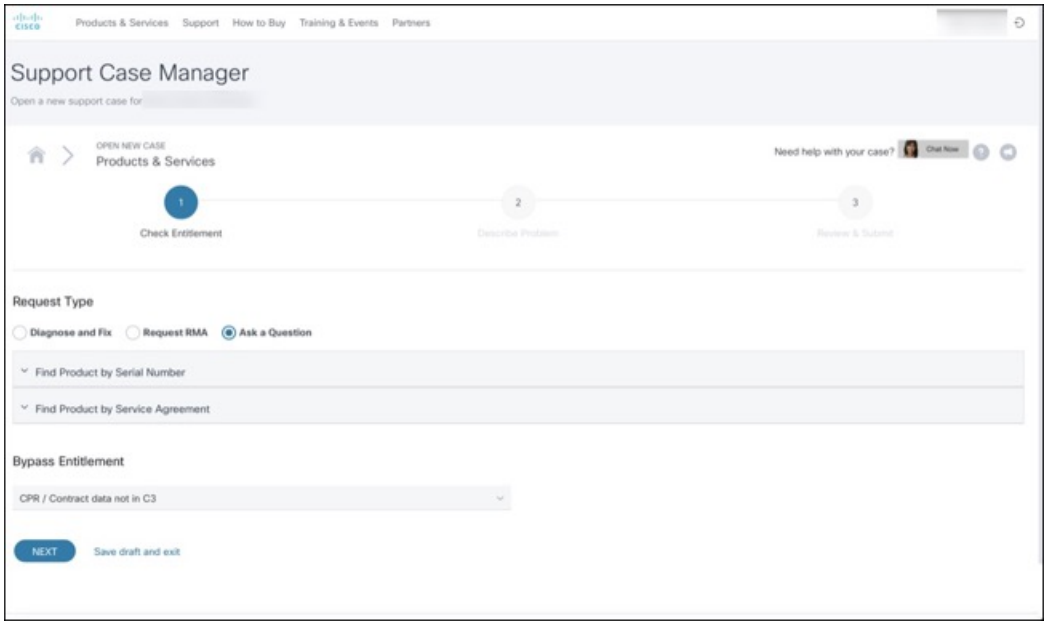
図 *1*: 新しいケースをオープンする



ステップ 2 [Ask a Question] オプションボタンをクリックし、使用している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。これは、Threat Grid 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。

ステップ 3 エンタイトルメントをバイパスする場合は、[Contract Data not in C3] を選択し、[Next] をクリックします。

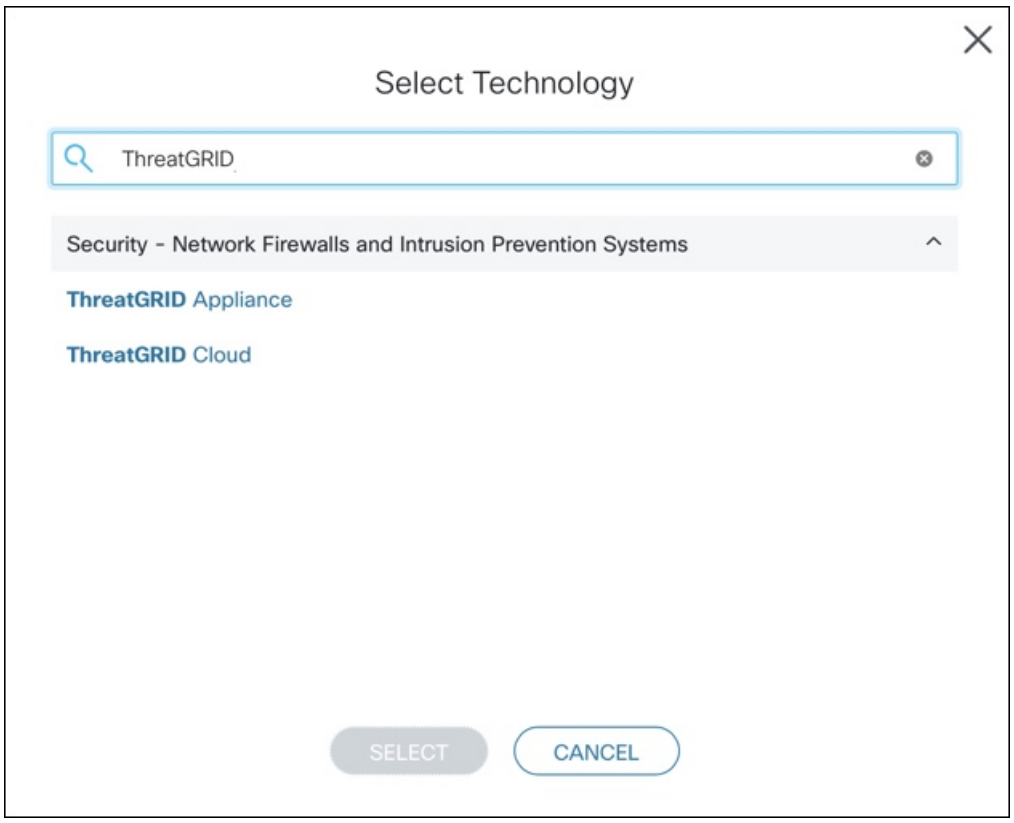
図 *2*: エンタイトルメントのチェック



ステップ 4 [Describe Problem] ページで、問題のタイトルと説明をそれぞれ [Title] と [Description] に入力します（タイトルには Threat Grid を含めます）。

ステップ 5 [Manually select a Technology] をクリックして、**ThreatGRID** を検索します。

図 *3*:テクノロジーの選択



ステップ 6 リストから **ThreatGRID Appliance** を選択し、[Select] をクリックします。

ステップ 7 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オープンできない場合は、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
- **ワールドワイド連絡先**：https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

サポートを要求する方法の詳細については、以下を参照してください。

- 次のブログ投稿を参照してください：**Changes to the Cisco Threat Grid Support Experience**（https://community.cisco.com/t5/security-blogs/changes-to-the-cisco-threat-grid-support-experience/ba-p/3911407）
- 次の**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：https://www.cisco.com/c/en/us/support/index.html

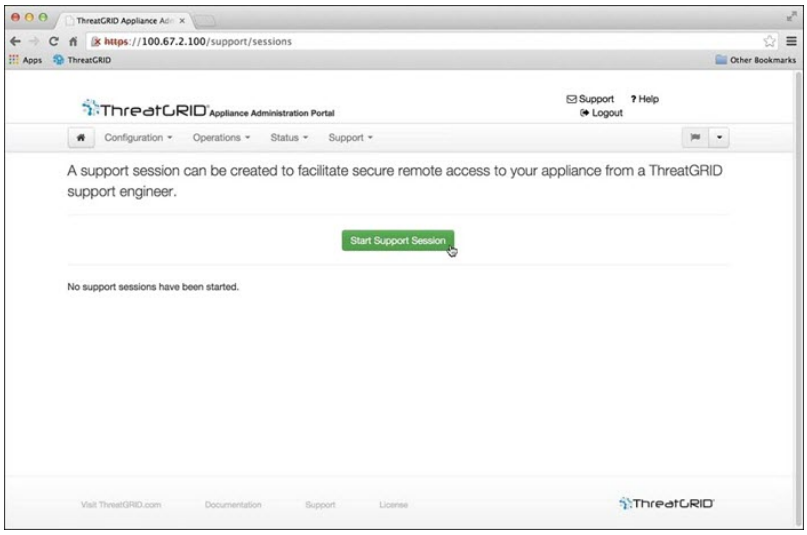
サポート モードの有効化

Threat Grid のエンジニアからのサポートを必要とする場合、サポートモードを有効にするよう求められる場合があります。このモードは、ライブサポートセッションであり、Threat Grid サポートエンジニアにアプライアンスへのリモートのアクセス権を付与します。アプライアンスの通常の動作には影響しません。

OpAdmin Portal の [Support] メニューからサポートモードを有効にすることができます。サポートモードは、TGSH ダイアログから、従来の Face Portal UI から、またリカバリモードでの起動時に有効にすることもできます。

ステップ 1 OpAdmin Portal で [Support] メニューをクリックし、[Live support Session] を選択します。

図 *4 : OpAdmin* のライブサポートセッションの開始



ステップ 2 [Start Support Session] をクリックします。

（注） OpAdmin 設定ウィザードを終了して、ライセンスを適用する前にサポートモードを有効にすることができます。

サポート スナップショット

基本的にサポートスナップショットは実行中のシステムのスナップショットであり、ログ、psoutput などが含まれ、サポートスタッフによる問題のトラブルシューティングに役立ちます。

ステップ 1 SSH がサポート スナップショット サービスに指定されていることを確認します。

ステップ 2 [Support] メニューから、[Support Snapshots] を選択します。

ステップ 3 スナップショットを取得します。

ステップ 4 スナップショットを取得したら、**.tar** または **.gz** としてダウンロードすることができます。または、[Submit] を押して、Threat Grid スナップショット サーバにスナップショットを自動的にアップロードできます。