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 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。Threat Grid アプライアンスは、Cisco Threat Grid M5 アプライアンスサーバ（v2.7.2 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-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。

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 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って、組織はネットワークから離れることなく、疑わしいドキュメントやファイルを分析のために送信できます。

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 *12* 日

機能または更新	セクション
Threat Grid Web ポータル UI 管理者のログインパスワードが更新されました。	ログイン名とパスワード（デフォルト）
Threat Grid アプライアンスモデル（UCS C220-M3 サーバをベースとする）に v2.9 をインストールする際のバックアップデータの保持に関する情報が追加されました。	バックアップ データの保持
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

このガイドは、アプライアンスのセットアップと設定が完了し、最初のテストマルウェアサンプルが正常に送信および分析された後に、Threat Grid アプライアンス管理者が使用することを目的としています。Threat Grid マルウェア分析ツール、アプライアンスの更新、バックアップ、その他のサーバ管理タスクに関して、組織とユーザを管理する方法について説明します。

さらに、Threat Grid アプライアンスと他のシスコ製品やサービス（Cisco E メールセキュリティアプライアンス、Cisco Web セキュリティアプライアンス、AMP for Endpoints プライベートクラウドデバイスなど）を統合する管理者に向けた情報も提供します。

（注） Threat Grid アプライアンスのセットアップと設定の詳細については、『*Cisco Threat Grid Appliance Setup and Configuration Guide*』を参照してください。

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 Version Lookup Table*』
- 『*Cisco Threat Grid M5 Hardware Installation Guide*』

（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。

以前のバージョンの Cisco Threat Grid アプライアンスの製品マニュアルは、Cisco.com の『Threat Grid Install and Upgrade』で入手できます。

Threat Grid Portal UI オンラインヘルプ

Threat Grid ポータルのユーザマニュアル（リリースノート、『Using Threat Grid Online Help』、API に関する資料その他の情報を含む）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。

E メール セキュリティ アプライアンスと Web セキュリティアプライアンスに関する資料

E メール セキュリティ アプライアンス（ESA）または Web セキュリティアプライアンス（WSA）の接続に関する詳細については、「ESA/WSA アプライアンスの Threat Grid アプライアンスへの接続」を参照してください。

ESA/WSA のオンラインヘルプまたはユーザガイドの「Enabling and Configuring File Reputation and Analysis Services」の手順を参照してください。

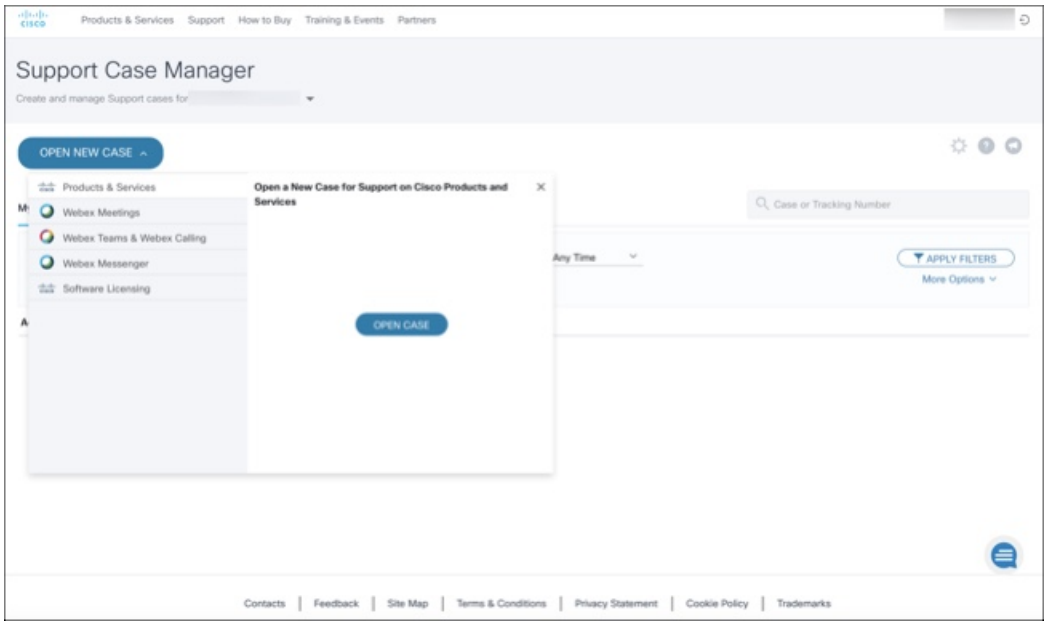
- 『*Cisco Email Security Appliance User Guide*』
- 『*Cisco Web Security Appliance User Guide*』

Threat Grid のサポート

Threat Grid 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。

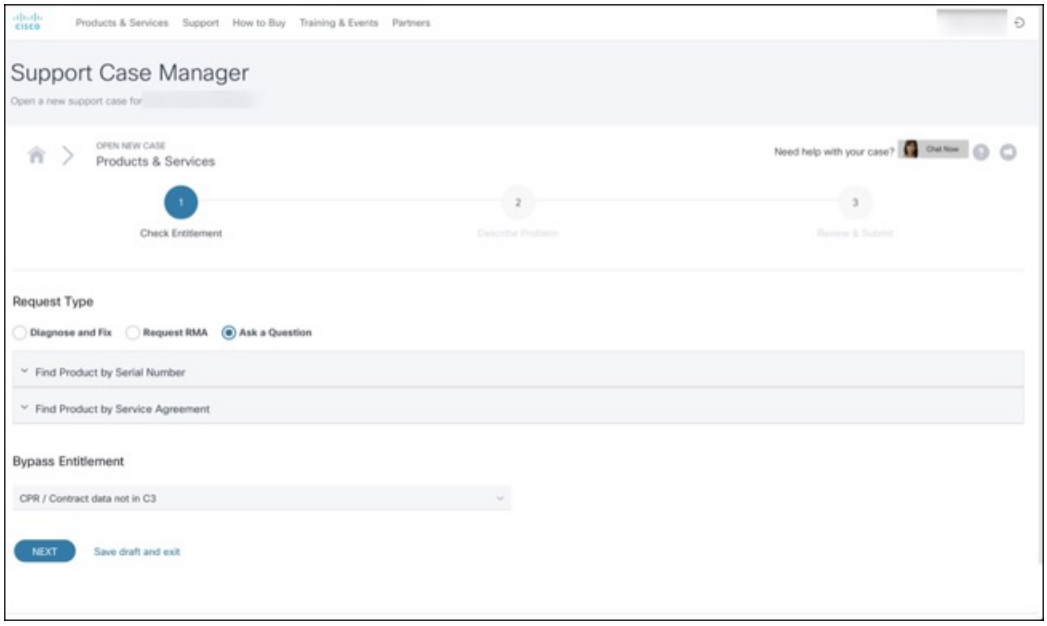
図 *1:* 新しいケースをオープンする



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、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。

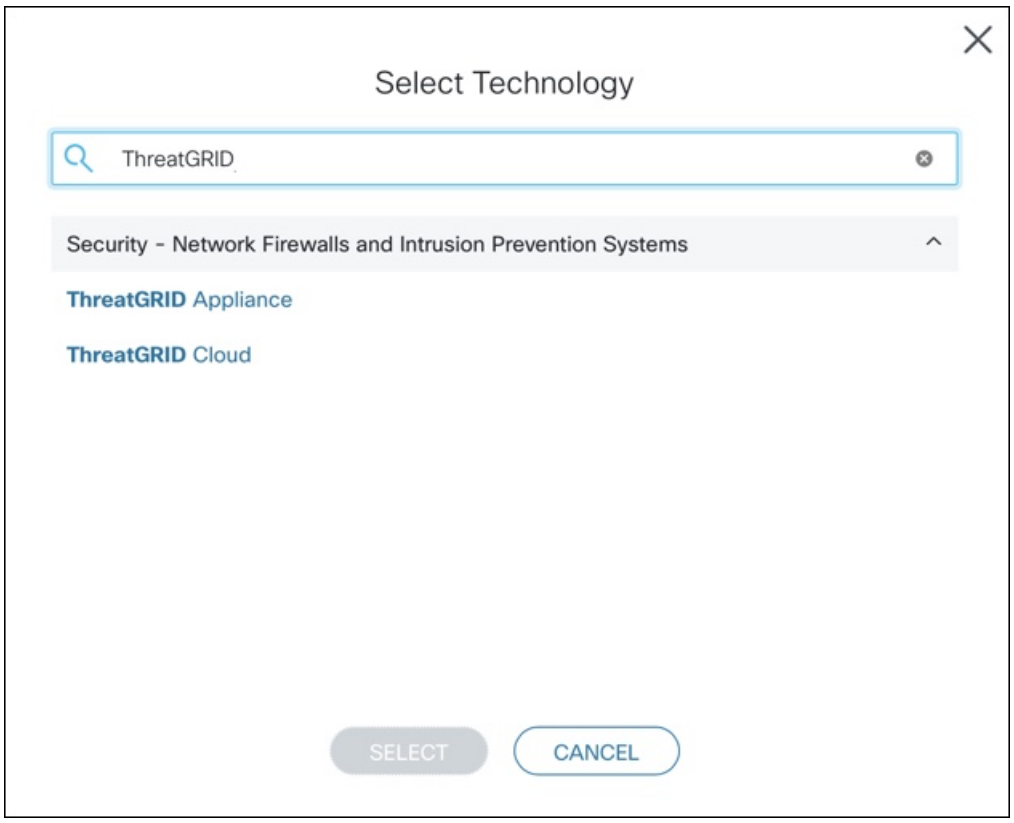
図 *2:* エンタイトルメントのチェック



ステップ 4 [**Describe Problem**] ページで、問題の [**Title**] と [**Description**] を入力します（タイトルで Threat Grid に言及してください）。

ステップ 5 [**Manually select a Technolog**] 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。

- 次のブログ記事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）
- 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。

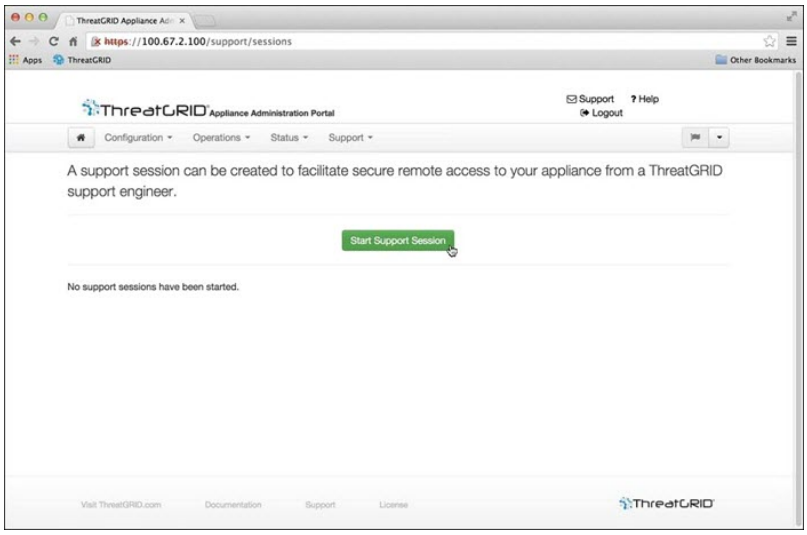
サポート モードの有効化

Threat Grid のエンジニアからのサポートが必要なときに、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、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アクセス権が付与されます。アプライアンスの通常の動作には影響しません。

OpAdmin ポータルの [**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。TGSH ダイアログ、レガシーの Face Portal UI から有効にするか、リカバリモードで起動する際に有効にすることもできます。

ステップ 1 OpAdmin ポータルで [**Support**] メニューをクリックして、[**Live Support Session**] を選択します。

図 *4 : OpAdmin* で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、ライセンシングの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

サポートスナップショットは、基本的に実行中のシステムのスナップショットで、ログ、psoutput などが含まれており、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** ファイルまたは **.gz** ファイルとしてダウンロードするか、[**Submit**] をクリックして、スナップショットを Threat Grid スナップショットサーバに自動的にアップロードします。