はじめに

Cisco Secure Malware Analytics Appliance アドミニストレーション ガイド へようこそこの章では、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。

Secure Malware Analytics アプライアンスについて

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 M6 Applicance server（v.2.19 以降）または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 Secure Malware Analytics 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。

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。

このリリースの最新情報

バージョン 2.19 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 *2.19* における変更

機能または更新	セクション
ファームウェアの更新	FirmwareUp によるファームウェアの更新
管理 UI のダッシュボードの機能強化	ホーム
TGSH では、クリーンおよびダーティインターフェイスを介して ping を実行できるようになりました。	-

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、Cisco Secure Malware Analytics 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。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、その他のサーバー管理タスクに関して、組織とユーザーを管理する方法について説明します。

さらに、Cisco Secure Malware Analytics 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、Secure Endpoint 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） Cisco Secure Malware Analytics アプライアンスのセットアップと構成の詳細については、『*Cisco Threat Grid Getting Started Guide*』を参照してください。

このマニュアルについて

このガイドには、計画に関する情報、設定作業、および一般的な管理タスクが記載されています。構成は次のとおりです。

章	説明
はじめに	アプライアンスの簡単な説明、対象読者、関連する製品マニュアルへのアクセス方法、ログイン名とパスワード、管理者パスワードのリセット方法、サポートへの連絡を提供します。
計画	セットアップ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。
TGSH ダイアログを使用したネットワーク構成	管理 TUI を使用した初期ネットワーク設定の変更、管理 TUI への再接続、およびリカバリモードでのネットワークの設定に関する情報を提供します。
ホーム	管理 UI のホーム画面の使用に関する情報を提供します。
設定	管理 UI を使用してアプライアンスの設定を変更することについての情報を提供します。
ステータス（Status）	インストールされているシステムパッケージとそのバージョン、詳細ログ、使用可能なストレージなど、管理 UI でのシステム情報の表示に関する情報を提供します。
操作（Operations）	設定変更のアクティブ化、管理 UI のリロード、ジョブと電力設定の管理、および更新のインストールに関する情報を提供します。
サポート	アプライアンスの問題の解決を支援するために、ライブ サポート セッションを開始し、サポート スナップショットを作成する手順を示します。
組織およびユーザー	組織の作成、ユーザーの管理、新しいデバイス ユーザー アカウントのアクティブ化の手順を説明します。
インバウンドおよびアウトバウンド接続	他の Cisco アプライアンス（ESA および WSA）および Cisco Secure Endpoint プライベートクラウドを Cisco Secure Malware Analytics アプライアンスに接続する方法について説明します。
アプライアンスブートのワイプオプションを使用したすべてのデータの削除	アプライアンスのワイプオプションを使用して、クラスタを含む Cisco Secure Malware Analytics アプライアンスからすべてのデータを削除する方法について説明します。
FirmwareUp によるファームウェアの更新	ファームウェアの更新方法について説明します。

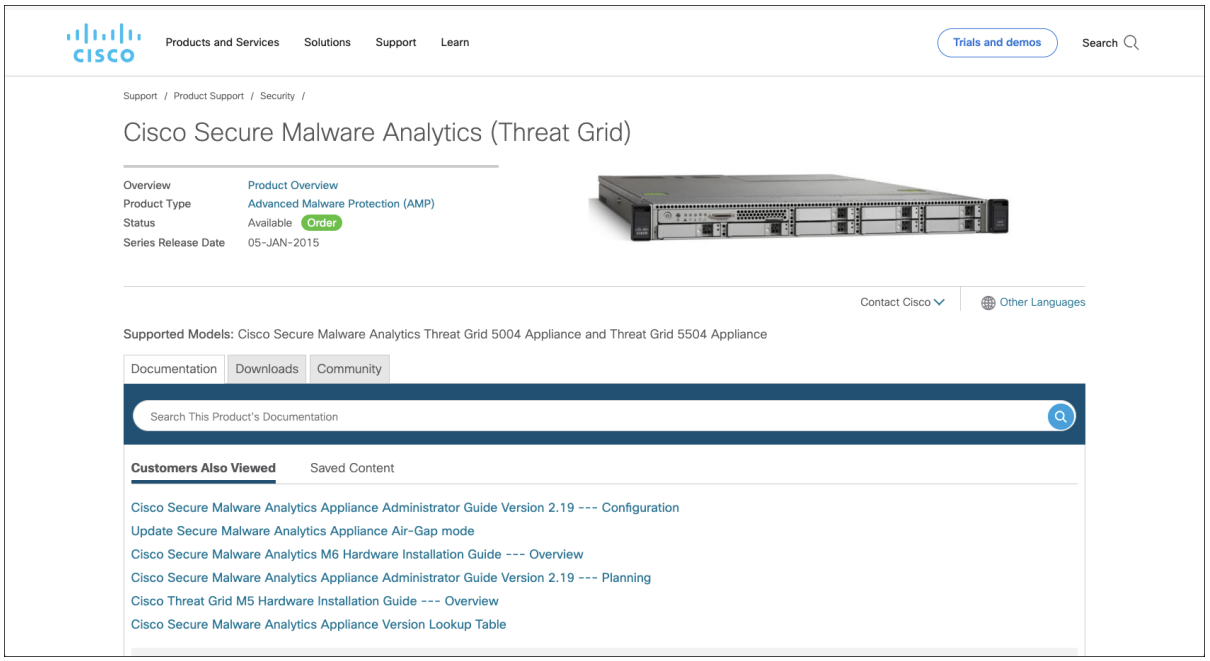
章	説明
CIMCの設定	CIMC ユーティリティを使用してリモート サーバー管理を設定する方法について説明します。

ユーザーマニュアル

Cisco Secure Malware Analytics アプライアンスのユーザーマニュアル

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。

図 *1 : cisco.com* のユーザーガイド



- *Cisco Secure Malware Analytics Appliance Release Notes*
- *Cisco Secure Malware Analytics アプライアンス v2.19 スタートアップガイド*
- *Cisco Secure Malware Analytics Version Lookup Table*
- *Cisco Secure Malware Analytics M6 Hardware Installation Guide*

（注） Cisco Secure Malware Analytics M6 アプライアンスは、アプライアンス バージョン 2.19 以降でサポートされています。

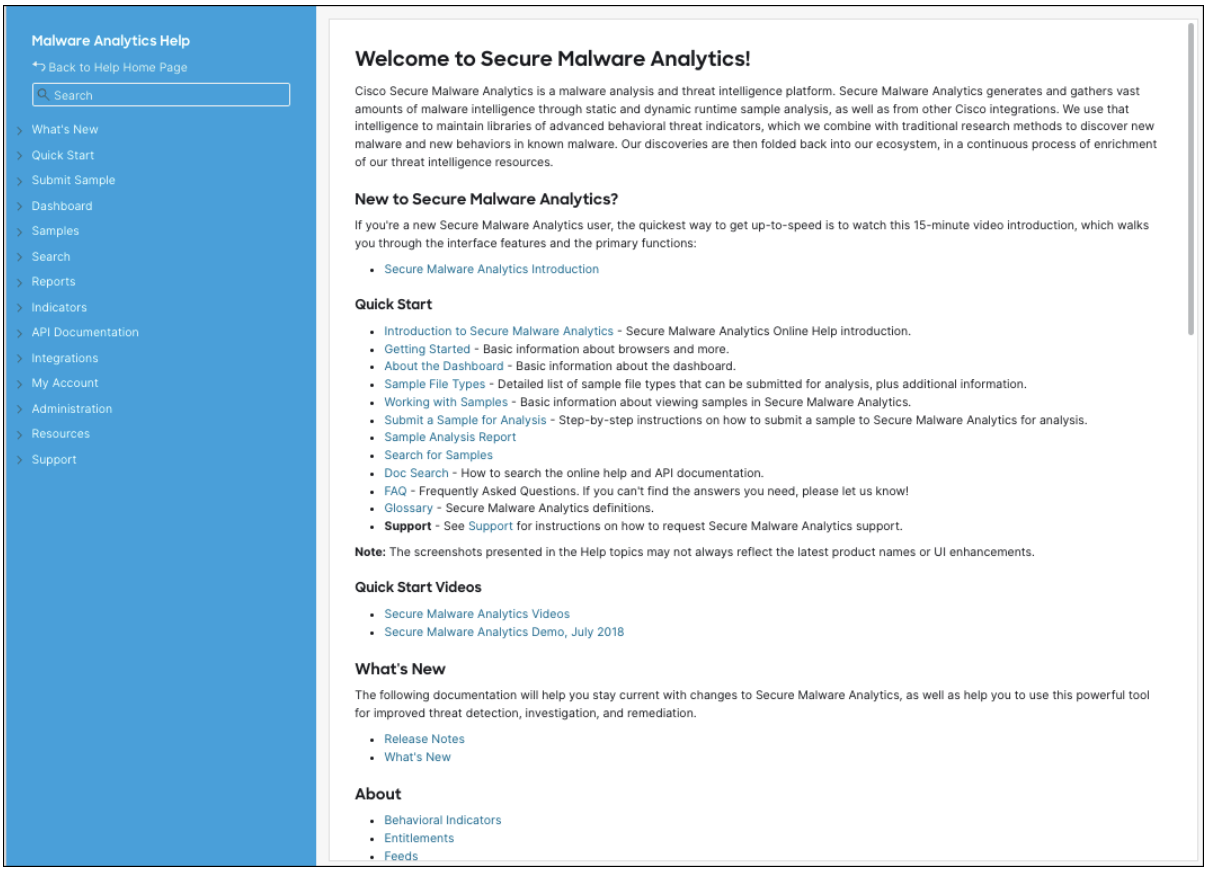
- *Cisco Secure Malware Analytics M5 Hardware Installation Guide*

（注） Cisco Secure Malware Analytics M5 アプライアンスは、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。

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

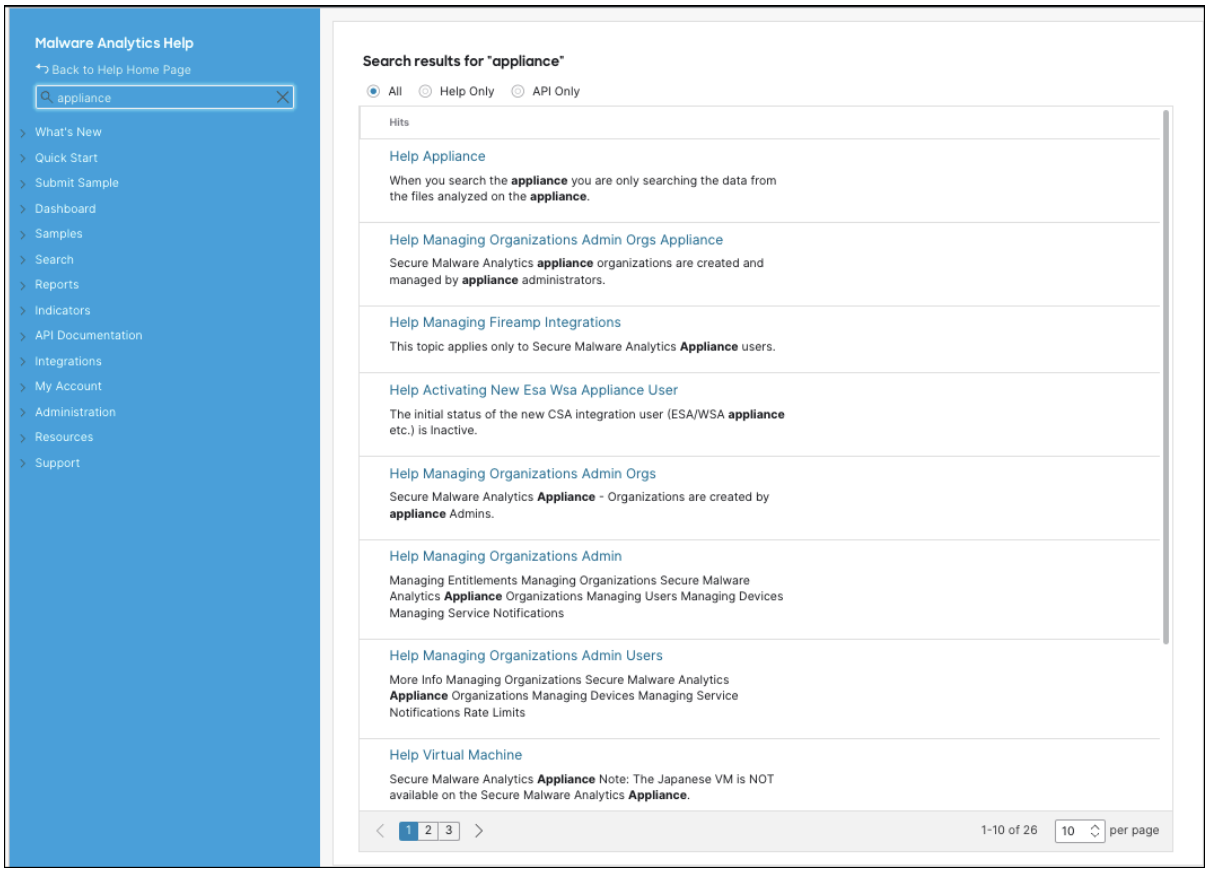
リリースノート、Cisco Secure Malware Analytics オンライン ヘルプ、API ドキュメント、およびその他の情報を含む Cisco Secure Malware Analytics ポータル ユーザー ドキュメントはCisco Secure Malware Analytics ユーザーインターフェイスの右上隅にあるナビゲーションバーにある **[?（ヘルプ）]** アイコンから入手できます。

図 *2 : Cisco Secure Malware Analytics* ポータル オンライン ヘルプ



左列の上部にあるオンラインヘルプの検索機能を使用して、アプライアンス固有の情報を検索します。

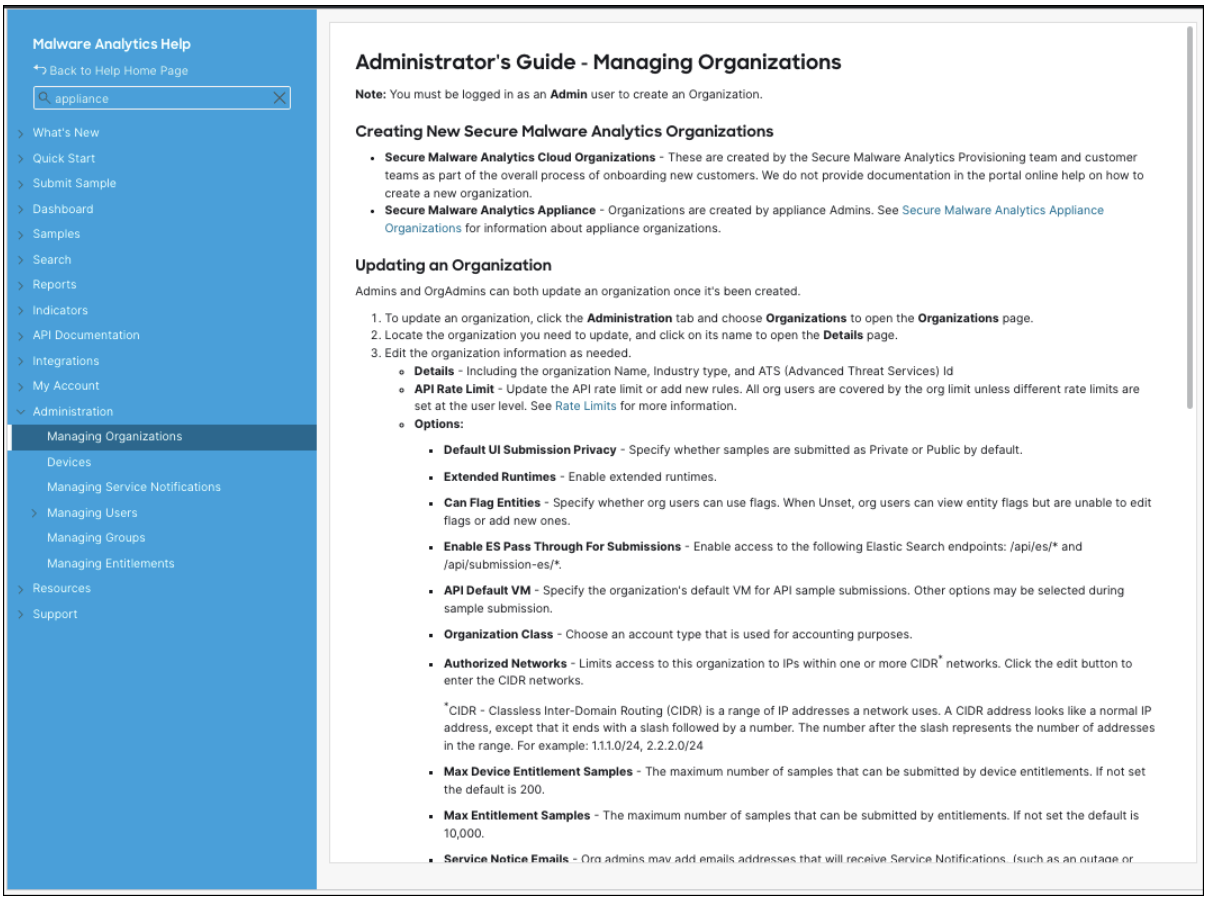
図 *3:* オンライン ヘルプ検索機能



Secure Malware Analytics Portal UI アドミニストレーション ガイド

管理者は、ポータルのオンライン ヘルプ トピックを参照できます。このトピックでは、ユーザーの管理方法やその他の情報を管理する方法について説明します。 **[アドミニストレーション]** タブをクリックし、 **アドミニストレーション ガイド]**を選択します。

図 *4 : Cisco Secure Malware Analytics* ポータル *UI* の管理ガイド



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、「統合」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ーガイドの「Enabling and Configuring File Reputation and Analysis Services」の手順を参照してください。

- *Cisco Secure Email Gateway ユーザー ガイド*
- *Cisco Secure Web Appliance ユーザーガイド*

ログイン名とパスワード（デフォルト）

デフォルトのログイン名とパスワードを次の表に示します。

ユーザー（User）	ログイン/パスワード
Admin UI とシェルユーザー	最初のSecure Malware Analytics/Admin TUI でランダムに生成されたパスワードを使用し、次に Admin UI の構成ワークフローの最初の手順で入力した新しいパスワードを使用します。 パスワードを紛失した場合は、「管理者パスワードのリセット」の手順に従ってください。
Cisco Secure Malware Analytics Web ポータル UI 管理者	ログイン：**admin** パスワード：最初の Admin UI パスワードを使用して初期化します。初期化の後、独立した状態になります。
CIMC	Login: **admin** Password: **password**

パスワード条件

パスワードには、次が含まれている必要があります。

- 8文字以上
- 1つ以上の数字
- 1 つ以上の特殊文字
- 大文字および小文字

管理者パスワードのリセット

デフォルトの管理者パスワードは、アプライアンスの初期設定と設定の際に Admin TUI でのみ表示されます。初期設定が完了すると、管理者パスワードは、読み取り可能なテキストで表示されなくなります。

（注） LDAP 認証は、複数の管理者がいる場合に、Admin TUI と Admin UI ログインに使用できます。アプライアンスに LDAP 認証のみが設定されている場合、リカバリ モードでパスワードをリセットすると、認証モードが再設定され、システム パスワードでもログインできるようになります。

管理者パスワードを紛失して Admin UI にログインできない場合は、次の手順を実行してパスワードをリセットします。

手順

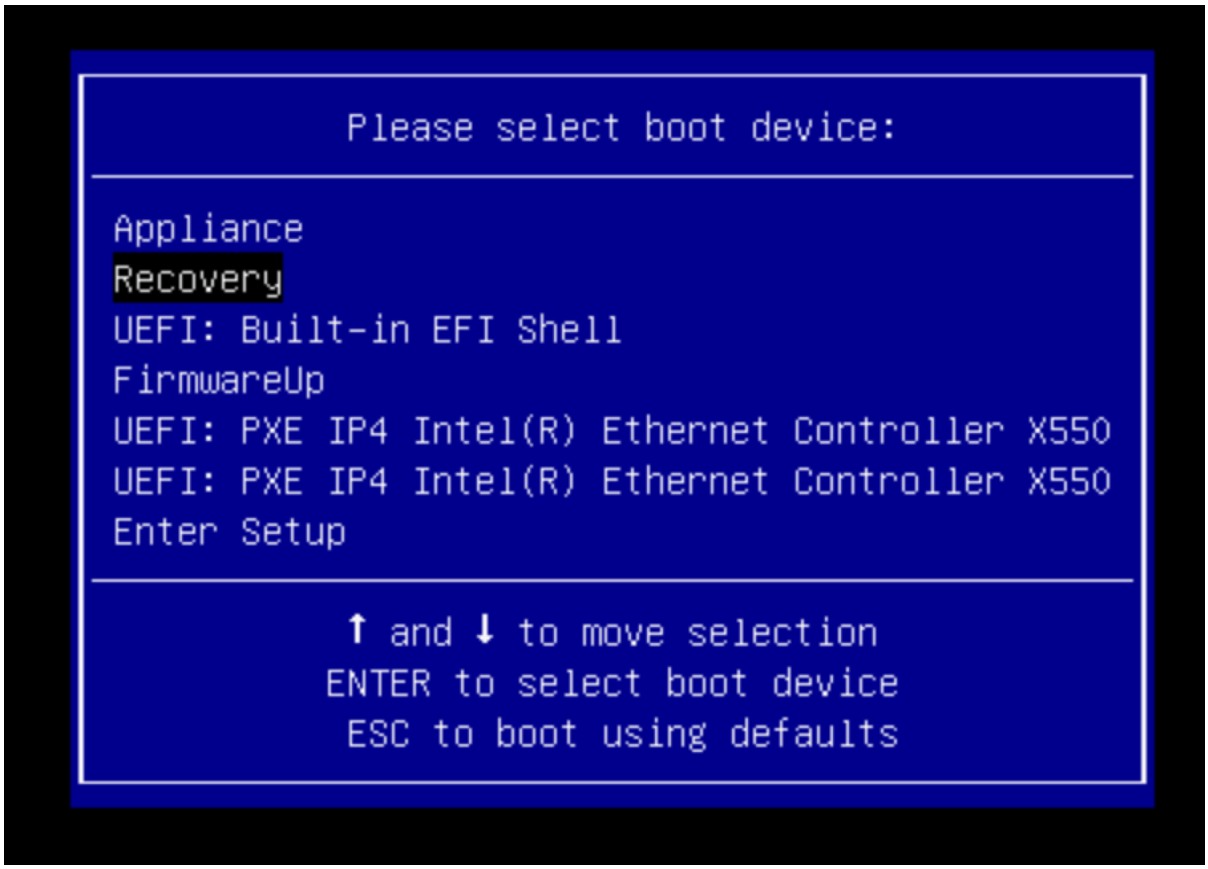
ステップ 1 Cisco Secure Malware Analytics アプライアンスを再起動します。 **[操作（Operations）**] タブをクリックして **[電源（Power）]**を選択し、[再 **起動（Reboot）]** ボタンをクリックします。アプライアンスが再起動し、[BIOS] ウィンドウが開きます。

図 *5 : [BIOS]* ウィンドウ - *[*ブートの選択（*Choose Boot*）*]* メニュー*<F6>*リカバリモード用

ステップ 2 [BIOS] ウィンドウで、 **F6** を押して **[Boot]** メニューを開きます。

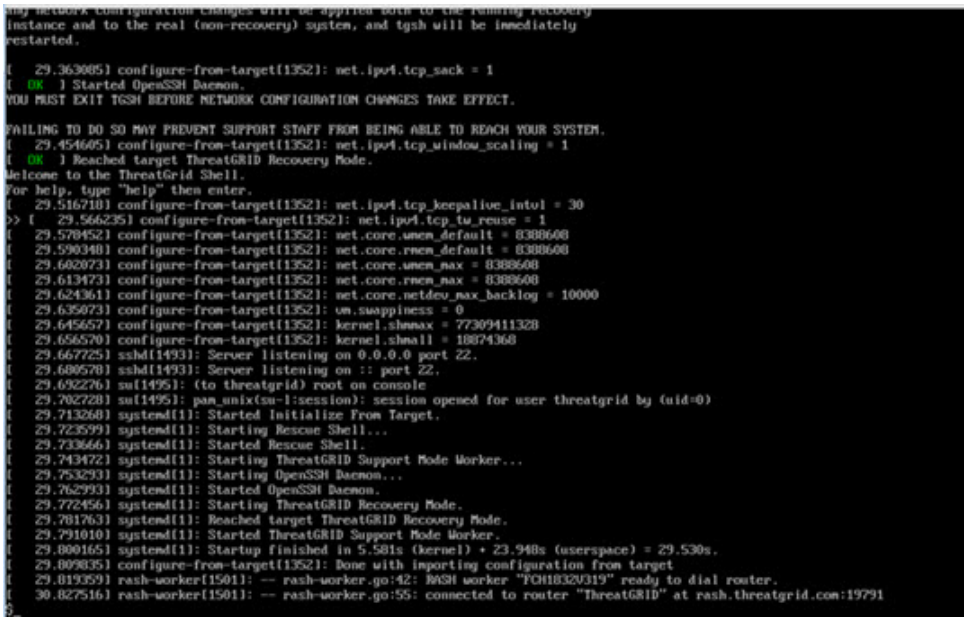
ステップ 3 **[リカバリ（Recovery）]** を選択し、 **[Enter]**を押します。

図 *6:* ブート メニュー



Cisco Secure Malware Analytics シェルがリカバリ モードで開きます。

図 *7:* リカバリ モードの *Cisco Secure Malware Analytics* シェル（*tgsh*）



ステップ 4 `passwd` を実行して、パスワードを変更します。

図 *8 : Enter New Password*

（注）
このモードではコマンドプロンプトが常に表示されるとは限りません。また、ロギング出力がいずれかの時点で入力と重なるように表示されることがあります。この表示は入力には影響しません。ブラインド入力を続けることができます。2 行のロギング出力は無視します。

ステップ 5 パスワードを（ブラインドで）入力し、**Enter** キーを押します。

ステップ 6 パスワードをもう一度入力して、**Enter** キーを押します。

（注）
パスワードは表示されません。

ステップ 7 「**Reboot**」と入力し、**Enter** キーを押して、アプライアンスを通常モードで起動します。

（注）
パスワードのリセットを有効にするために再起動前にexitコマンドを実行する必要はなくなりました（v2.10 以降）。

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。