

# セキュアなマルウェア分析に必要なIPとポート

## 内容

---

### [はじめに](#)

#### [マルウェア分析クラウドの保護](#)

[米国 \(米国\) クラウド](#)

[EU \(欧州\) クラウド](#)

[CA \(カナダ\) クラウド](#)

[AU \(オーストラリア\) クラウド](#)

#### [セキュアマルウェア分析アプライアンス](#)

[Dirtyインターフェイス](#)

[リモートネットワーク出口](#)

[クリーンインターフェイス](#)

[管理インターフェイス](#)

---

## はじめに

このドキュメントでは、Secure Malware Analyticsのシームレスな運用を保証するためにファイアウォールに実装する必要がある重要なネットワーク設定について説明します。

著者：Cisco TAC エンジニア

## マルウェア分析クラウドの保護

### 米国 (米国) クラウド

アクセスURL:<https://panacea.threatgrid.com>

ホスト名	IP	ポート	詳細
panacea.threatgrid.com	63.97.201.67 63.162.55.67	443	Secure Malware Analyticsポータルと統合デバイス (ESA/WSA/FTD/ODNS/Meraki)
glovebox.chi.threatgrid.com	200.194.241.35	443	Sample Interactionウィンドウ
glovebox.rcn.threatgrid.com	63.97.201.67	443	Sample Interactionウィンドウ
glovebox.scl.threatgrid.com	63.162.55.67	443	Sample Interactionウィンドウ

fmc.api.threatgrid.com	63.97.201.67 63.162.55.67	443	FMC/FTDファイル分析サービス
------------------------	------------------------------	-----	-------------------

## EU ( 欧州 ) クラウド

アクセスURL:<https://panacea.threatgrid.eu>

ホスト名	IP	ポート	詳細
panacea.threatgrid.eu ( 日本での対応時期未定 )	62.67.214.195 200.194.242.35	443	Secure Malware Analyticsポータルと統合デバイス(ESA/WSA/FTD/ODNS/Meraki)
グローブボックス .muc.threatgrid.eu	62.67.214.195	443	Sample Interactionウィンドウ
グローブボックス .fam.threatgrid.eu	200.194.242.35	443	Sample Interactionウィンドウ
fmc.api.threatgrid.eu ( 日本での対応時期未定 )	62.67.214.195 200.194.242.35	443	FMC/FTDファイル分析サービス

古いIP 89.167.128.132は廃止されました。上記のIPでファイアウォールルールを更新してください。

## CA ( カナダ ) クラウド

アクセスURL:<https://panacea.threatgrid.ca>

ホスト名	IP	ポート	詳細
panacea.threatgrid.ca ( 脅威検出機能 )	200.194.240.35	443	Secure Malware Analyticsポータルと統合デバイス(ESA/WSA/FTD/ODNS/Meraki)
グローブボックス .kam.threatgrid.ca	200.194.240.35	443	Sample Interactionウィンドウ
fmc.api.threatgrid.ca ( 入手可能 )	200.194.240.35	443	FMC/FTDファイル分析サービス

## AU ( オーストラリア ) クラウド

アクセスURL:<https://panacea.threatgrid.com.au>

ホスト名	IP	ポート	詳細
panacea.threatgrid.com.au	124.19.22.171	443	Secure Malware Analyticsポータルと統合デバイス (ESA/WSA/FTD/ODNS/Meraki)
glovebox.sydney.threatgrid.com.au	124.19.22.171	443	Sample Interactionウィンドウ
fmc.api.threatgrid.com.au	124.19.22.171	443	FMC/FTDファイル分析サービス

## セキュアマルウェア分析アプライアンス

Secure Malware Analyticsアプライアンスのインターフェイスごとに推奨されるファイアウォールルールを次に示します。

### Dirtyインターフェイス

サンプルがDNSを解決し、コマンド&コントロール(C&C)サーバと通信できるように、VMがインターネットと通信するために使用  
プライベートネットワーク間で:

方向	プロトコル	ポート	宛先	ホスト名	詳細
Outbound	IP	ANY	ANY		ここでDenyセクションで指定されている場合を除き、推奨されます。  分析のための接続を可能にするために使用されます。
Outbound	TCP	22	54.173.231.1611 63.97.201.982 63.162.55.982	support- snapshots.threatgrid.com	自動サポート診断アップロードに使用 注：ソフトウェアバージョン1.2+が必要
Outbound	TCP	22	54.173.181.2171 54.173.182.461 63.162.55.972 63.97.201.972	appliance- updates.threatgrid.com	アプライアンスの更新
Outbound	TCP	19791	54.164.165.1371 34.199.44.2021 63.97.201.962 63.162.55.962	rash.threatgrid.com	リモートサポート/アプライアンスサポートモード
Outbound	TCP	22	54.173.124.1721	appliance-licensing.threatgrid.com	ライセンス管理

			63.97.201.992 63.162.55.992		
--	--	--	--------------------------------	--	--


<sup>1</sup>これらのIPは近い将来、無効になる予定です。


<sup>2</sup>これらは、<sup>1</sup>のIPに代わるIPです。近い将来、IPの変更に関する通信が行われるまで、両方のIPを追加することをお勧めします。

## リモートネットワーク出口

アプライアンスが、以前はtg-tunnelと呼ばれていたリモート出口にVMトラフィックをトンネリングするために使用します。

方向	プロトコル	ポート	宛先
Outbound	TCP	21413	173.198.252.53
Outbound	TCP	21413	163.182.175.193 **
Outbound	TCP	21417	69.55.5.250
Outbound	TCP	21415	69.55.5.250
Outbound	TCP	21413	76.8.60.91

 注:Remote Exit 4.14.36.142は削除され、現在実稼働されていません。記載されているすべてのIPがファイアウォール例外リストに追加されていることを確認します。

 \*\*リモート出口163.182.175.193を173.198.252.53に交換

## 拒否:

方向	プロトコル	ポート	宛先	詳細
Outbound	SMTP	ANY	ANY	マルウェアがスパムを送信するのを防ぐため。
Inbound	IP	ANY	Secure Malware Analyticsアプライアンスのダッシュボードインターフェイス	上記の「許可」セクションで指定された場合を除き、推奨されます。 分析のための通信を可能にするために使用されます。

## クリーンインターフェイス

さまざまな接続サービスでサンプルの送信やアナリストのUIアクセスに使用されます。  
プライベートネットワーク間で:

方向	プロトコル	ポート	宛先	詳細
Inbound	TCP	443 および 8443	Secure Malware Analyticsアプリケーションスクリーンインターフェイス	WebUIおよびAPIアクセス
Inbound	TCP	9443	Secure Malware Analyticsアプリケーションスクリーンインターフェイス	グローブボックスに使用
Inbound	TCP	22	Secure Malware Analyticsアプリケーションスクリーンインターフェイス	SSH経由の管理TUIアクセス
Outbound	TCP	19791	ホスト : rash.threatgrid.com 54.164.165.137 1、34.199.44.202 <sup>1</sup> 63.97.201.96 2、63.162.55.96 <sup>2</sup>	セキュアマルウェア分析サポートのリカバリモード。

<sup>1</sup>これらのIPは近い将来、無効になる予定です。

<sup>2</sup>これらは、<sup>1</sup>のIPに代わるIPです。近い将来、IPの変更に関する通信が行われるまで、両方のIPを追加することをお勧めします。

## 管理インターフェイス

管理UIへのアクセス。

プライベートネットワーク間で:

方向	プロトコル	ポート	宛先	詳細
Inbound	TCP	443 および 8443	Secure Malware Analyticsアプリケーション管理インターフェイス	ハードウェアとライセンスの設定を構成するために使用します。
インブード	TCP	22	Secure Malware Analyticsアプリケーション管理インターフェイス	SSH経由の管理TUIアクセス

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。