Cisco AMP Threat Grid

プライバシーとサンプルの可視性

最終更新日：2016/08/10

Cisco Systems, Inc. www.cisco.com

シスコは世界各国 200 箇所にオフィスを開設しています。Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報と推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスと限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルとソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図とその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.

表紙の写真：アーチーズ国立公園ビジター センターの上方高い尾根に咲いたサボテンの花。万全の防御を行い、持てる資源を最大限に活用し、過酷で厳しい環境でも花開く。Copyright © 2015 Mary C. Ecsedy. All rights reserved. Used with permission.

プライバシーとサンプルの可視性

サンプルを分析のために Threat Grid に送信する場合は、その内容のプライバシーが重要な留意事項になります。機密文書やアーカイブ タイプを分析のために送信する場合は、プライバシーが特に重要な留意事項になります。検索 API と組み合わせると、機密資料を見つけることは、Threat Grid へのアクセス権がある機密資料の場合比較的容易だからです。

プライバシーについては、サンプルを Threat Grid Cloud ではなく社内の Threat Grid アプライアンスに送信する場合は特に問題になりませんが、プライバシーの基礎とサンプルの可視性に対する理解は TGA 管理者に必要です。

Threat Grid にサンプルを送信する際のプライバシーおよびサンプルの可視性モデルは、比較的単純なものになっています。プライベートとしてサンプルを指定しない限り、送信者の組織外部のユーザにサンプルが可視になります。一般に、*プライベート*として指定されたサンプルは、そのサンプルを送信したユーザと同じ組織内にいるユーザにしか表示されません。

Threat Grid アプライアンスでのプライバシーと可視性

「CSA 統合」から送信されたサンプルの場合、Threat Grid アプライアンスでのプライバシーおよびサンプルの可視性モデルは変更されます。CSA 統合とは、CSA API によって Threat Grid アプライアンスと統合されたシスコ製品（ESA/WSA アプライアンスやその他のデバイスまたはサービス）のことです。

Threat Grid アプライアンスに対するすべてのサンプル送信は、デフォルトでパブリックとして設定されるため、どの組織に所属しているかに関わらず、CSA 統合を含む他のあらゆるアプライアンス ユーザが表示できます。

アプライアンスのすべてのユーザが、他のすべてのユーザが送信したサンプルのあらゆる詳細を確認できるということです。

非 CSA Threat Grid ユーザは、サンプルをプライベートとして Threat Grid アプライアンスに送信できます。この場合、サンプルが可視になるのは、送信者と同じ組織に所属する Threat Grid アプライアンス（CSA 統合を含む）のユーザだけです。

以下の表で、Threat Grid アプライアンスでのプライバシーおよびサンプルの可視性モデルを説明します。この表では、次の用語を使用します。

CSA 統合	CSA 統合とは、CSA API を介して Threat Grid アプライアンスに登録されている、ESA/WSA アプライアンスおよびその他のシスコ デバイスまたはサービスのことです。CSA 統合から Threat Grid アプライアンスに送信されるサンプルは、デフォルトでパブリックとして設定されます。
その他の統合	FireAMP プライベート クラウドなどの他の統合に同様の基本的なプライバシールールが適用されます。

Threat Grid User - Public

Threat Grid アプライアンスにパブリック サンプルを送信する、Threat Grid の一般ユーザ（つまり、非 CSA 統合ユーザ）。

たとえば、Threat Grid Portal UI または Threat Grid ネイティブ API を使用してサンプルを送信するアプライアンス管理者またはマルウェア アナリストがこれに該当します。

Threat Grid User - Private

Threat Grid アプライアンスにプライベート サンプルを送信する、Threat Grid の一般ユーザ。

この場合、プライベート サンプルは、送信者の組織に所属しない、アプライアンスの他のどのユーザに対しても可視になりません。（送信者と同じ組織内の CSA 統合には可視になります）

図 1：Threat Grid アプライアンスでのプライバシーと可視性

	Sample Visibility when Accessed by:			
Samples Submitted by:	Threat Grid Users from the Same Organization	Threat Grid Users from a Different Organization	CSA Integration from the Same Organization	CSA Integration from a Different Organization
Threat Grid User - Public	Full	Full	Full	Full
Threat Grid User - Private	Full	None	Full	None
CSA Integrations (ESA/WSA appliances, etc.) All CSA submissions to Threat Grid Appliance are Public by default	Full	Full	Full	Full

同じ基本的なプライバシー ルールが FireAMP プライベート クラウドと Threat Grid アプライアンスの統合に適用されます。

Threat Grid クラウドでのプライバシーと可視性

プライベート サンプルが Cisco サンド ボックス API（「CSA API」）を介して Threat Grid クラウドに送信される場合、「スクラブした」バージョン（限定要素）を他の CSA 統合と共有することができます。

次の表は、Threat Grid クラウドのサンプル プライバシーと可視性を示します。

*注：スクラブしたレポートでは、サンプルに関する潜在的な機密情報はすべて削除されます。ファイル名、プロセス名などがありません。サンプルはダウンロードされない可能性があります。

図 2：Threat Grid ポータルでのプライバシーと可視性

	Sample Visibility when Accessed by:			
Samples Submitted by:	Threat Grid Users from the Same Organization	Threat Grid Users from a Different Organization	CSA Integration from the Same Organization	CSA Integration from a Different Organization
Threat Grid User - Public	Full	Full	Full	Scrubbed*
Threat Grid User - Private	Full	None	Full	None
CSA Integrations (ESA/WSA appliances, etc.) All CSA submissions to Threat Grid Cloud are Private by default	Full	None	Full	Scrubbed*

詳細については、cisco.com の **Threat Grid のインストールとアップグレード**のページのドキュメントを参照してください。