Cisco ASA REST API クイックスタートガイド

最終更新：2025 年 7 月 23 日

Cisco ASA REST API クイックスタートガイド

（注） REST API は、新しいハードウェアモデルではサポートされておらず、開発は終了しています。代わりに、自動化には ASA HTTP インターフェイスを使用することを推奨します。「自動化向けの Cisco Secure Firewall ASA HTTP インターフェイス」を参照してください。

概要

個々の Cisco ASA の設定と管理に、いくつかのオプションを使用できます。

- コマンド ライン インターフェイス（CLI）：接続済みのコンソールを介して ASA に制御コマンドを直接送信します。
- Adaptive Security Device Manager（ASDM）：ASA の設定、管理、およびモニターに使用できるグラフィカル ユーザー インターフェイスを備えた「オンボックス」管理アプリケーション。
- Cisco Security Manager：多数のセキュリティデバイスからなる中規模から大規模のネットワークを対象としていますが、このグラフィカル アプリケーションは、個々の ASA の設定、管理、およびモニターに使用できます。

シスコによる ASA REST API のリリースにより、軽量で使いやすいオプションが新たに追加されました。これは、「RESTful」原則に基づくアプリケーションプログラミングインターフェイス（API）で、API を実行している ASA 上ですばやくダウンロードして有効にできます。

ブラウザで REST クライアントをインストールした後、特定の ASA の REST エージェントにコンタクトして標準の HTTP メソッドを使用し、現在の設定情報にアクセスして、追加の設定パラメータを発行できます。

注意 ASA で REST API が有効になっている場合、他のセキュリティ管理プロトコルによる接続はブロックされません。これは、CLI、ASDM、または Security Manager を使用している他のユーザーが、同じことを行っている間に ASA の設定を変更する可能性があることを意味します。

ASA REST API の要求と応答

ASA REST API を使用すると、Representational State Transfer（REST）API を介して個々の ASA の管理にプログラムでアクセスできます。この API によって、外部クライアントは ASA リソースで CRUD（作成、読み取り、更新、削除）操作を実行できるようになります。API は、HTTPS プロトコルと REST 方法論に基づいています。

すべての API 要求が HTTPS 経由で ASA に送信され、応答が返されます。

このセクションでは、要求の構造と予想される応答の概要について説明します。

要求構造

使用できる要求メソッドは次のとおりです。

- GET – 指定されたオブジェクトからデータを取得します。
- PUT – 指定されたオブジェクトに情報を追加します。オブジェクトが存在しない場合は、404 エラー「リソースが見つかりません（Resource Not Found）」を返します。
- POST – 指定された情報でオブジェクトを作成します。
- DELETE – 指定されたオブジェクトを削除します。
- PATCH – 指定されたオブジェクトに部分的な変更を適用します。

応答構造

各要求によって、標準ヘッダー、応答コンテンツ、およびステータスコードを含んだ ASA からの HTTPS 応答が生成されます。

応答の構造は次のようになります。

- LOCATION - 新しく作成されたリソース ID。POST の場合のみ。新しいリソース ID を（URI 表現として）保持します。
- CONTENT-TYPE 応答メッセージ本文のメディアタイプ。応答メッセージ本文の表現と構文を示します。

各応答には HTTP ステータスまたはエラーコードが含まれます。使用可能なコードは、次のカテゴリに分けられます。

- `20x` - 200 番台のコードは、次のような処理の成功を示します。
  - `200 OK` – 成功した要求に対する標準応答。
  - `201 Created` – 要求が完了し、新しいリソースを作成。
  - `202 Accepted` – 要求が受け入れられたが、処理は未完了。
  - `204 No Content` – サーバーが要求を正常に処理したが、コンテンツは未送信。

- `4xx` - 400 番台のコードは、次のようなクライアント側のエラーを示します。
  - `400 Bad Request` – 無効なクエリパラメータ（認識されないパラメータ、欠落しているパラメータ、または無効な値など）。
  - `404 Not Found` – 指定された URL が既存のリソースと一致しない。たとえば、HTTP DELETE は、そのリソースがないために失敗する場合があります。
  - `405 Method not Allowed` – リソースで許可されていない HTTP 要求が行われた（読み取り専用リソースでの POST など）。
- `5xx` - 500 番台のコードは、サーバー側のエラーを示します。

エラーが発生した場合は、エラーコードに加えて、エラーに関する詳細を示すエラーオブジェクトがリターン応答に含まれる場合があります。JSON のエラーおよび警告の応答スキーマは次のとおりです。

```
[
{ "code" : "string",
"details": "string",
"context": attribute name,
"level" : <Error/Warning/Info>
},
...
]
```

ここで、オブジェクトのプロパティは次のとおりです。

プロパティ	タイプ	説明
`messages`	ディクショナリのリスト	エラーまたは警告メッセージのリスト
`code`	文字列	Error/Warning/Info コード
`details`	文字列	Error/Warning/Info に対応する詳細メッセージ

（注） REST API コールによって ASA の設定に加えられた変更は、起動設定には反映されません。つまり、変更は実行時設定だけに割り当てられます。起動設定への変更を保存するには、`writemem` API 要求を POST できます。詳細については、『About the ASA REST API』の目次の「Write Memory API」エントリを参照してください。

ASA REST API エージェントおよびクライアントのインストールと設定

REST API エージェントは、Cisco.com の ASA イメージとは別にパブリッシュされます。物理 ASA の場合、REST API パッケージをデバイスのフラッシュにダウンロードし、「rest-api image」コマンドを使用してインストールする必要があります。その後、REST API エージェントを「rest-api agent」コマンドを使用して有効にします。

仮想 ASA（ASAv）では、REST API イメージを「boot:」パーティションにダウンロードする必要があります。「rest-api image」コマンドを発行した後に、「rest-api agent」コマンドを発行して REST API エージェントにアクセスし、有効にする必要があります。

REST API ソフトウェアおよびハードウェアの要件および互換性の詳細については、『Cisco ASA Compatibility』マトリックスを参照してください。

ASA または ASAv の適切な REST API パッケージは、software.cisco.com/download/home からダウンロードできます。特定の適応型セキュリティアプライアンス（ASA）モデルを見つけ、[Adaptive Security Appliance REST API Plugin] を選択します。

（注） REST API エージェントは、Java ベースのアプリケーションです。Java Runtime Environment（JRE）は REST API のパッケージに含まれています。

使用上のガイドライン

重要 すべての API コールと既存のスクリプトにヘッダー `User-Agent: REST API Agent` を含める必要があります。CURL コマンドの場合は、`-H 'User-Agent: REST API Agent'` を使用します。

マルチ コンテキスト モードでは、REST API エージェント コマンドはシステム コンテキストでのみ使用できます。

サポートされる最大構成サイズ

ASA REST API は、物理 ASA 内で実行される「オンボード」アプリケーションであるため、割り当てられるメモリに制限があります。5555 や 5585 などの最新のプラットフォームでは、サポートされる実行構成の最大サイズが、リリースサイクルの間で約 2 MB に増加しています。

ASA REST API には、仮想 ASA プラットフォームでのメモリ制約もあります。ASAv5 での合計メモリは 1.5 GB ですが、ASAv10 では 2 GB です。REST API の制限は、ASAv5 と ASAv10 でそれぞれ 450 KB と 500 KB です。

そのため、大規模な実行構成では、多数の同時要求や大量の要求など、メモリを大量に消費するさまざまな状況で例外が発生する可能性があることに注意してください。このような状況で

は、REST API GET/PUT/POST コールが「500 - Internal Server Error」メッセージのエラーで始まる可能性があり、REST API エージェントが毎回自動的に再起動します。

この状況を回避するには、メモリの多い ASA/FPR または ASAV プラットフォームに移行するか、実行構成のサイズを小さくします。

サポートされる最大構成サイズ

ASA REST API は、物理 ASA 内で実行される「オンボード」アプリケーションであるため、割り当てられるメモリに制限があります。5555 や 5585 などの最新のプラットフォームでは、サポートされる実行構成の最大サイズが、リリースサイクルの間で約 2 MB に増加しています。

ASA REST API には、仮想 ASA プラットフォームでのメモリ制約もあります。ASAv5 での合計メモリは 1.5 GB ですが、ASAv10 では 2 GB です。REST API の制限は、ASAv5 と ASAv10 でそれぞれ 450 KB と 500 KB です。

そのため、大規模な実行構成では、多数の同時要求や大量の要求など、メモリを大量に消費するさまざまな状況で例外が発生する可能性があることに注意してください。このような状況では、REST API GET/PUT/POST コールが「500 - Internal Server Error」メッセージのエラーで始まる可能性があり、REST API エージェントが毎回自動的に再起動します。

この状況を回避するには、メモリの多い ASA/FPR または ASAV プラットフォームに移行するか、実行構成のサイズを小さくします。

REST API エージェントのダウンロードおよびインストール

特定の ASA で ASA REST API エージェントをダウンロードおよびインストールにするには、CLI を使って次の手順を実行します。

手順

ステップ 1 目的の ASA で `<package> disk0:` コマンドのコピーを発行し、現在の ASA REST API パッケージを cisco.com から ASA のフラッシュメモリにダウンロードします。次に例を示します。

```
copy tftp://10.7.0.80/asa-restapi-111-lfbff-k8.SPA disk0:
```

ステップ 2 `rest-api image disk0:/<package>` コマンドを発行し、パッケージを確認してインストールします。

次に例を示します。

```
rest-api image disk0:/asa-restapi-111-lfbff-k8.SPA
```

インストーラで互換性と有効性のチェックを実行してから、パッケージをインストールします。ASA はリブートしません。

REST API エージェントの有効化

特定の ASA で ASA REST API エージェントを有効にするには、次の手順を実行します。

手順

ステップ 1 正しいソフトウェアイメージが ASA にインストールされていることを確認します。

必要とされる ASA のイメージを判断するには、『ASA Compatibility Matrix』（https://www.cisco.com/c/en/us/td/docs/security/asa/compatibility/asamatrx.html#pgfId-131643）の「REST API」セクションを参照してください。

ステップ 2 CLI を使用して、HTTP サーバーが ASA で有効になっていること、および API クライアントが管理インターフェイスに接続できることを確認します。次に例を示します。

```
http server enable
http 0.0.0.0 0.0.0.0 <management interface nameif>
```

ステップ 3 CLI を使用して、API 接続の HTTP 認証を定義します。次に例を示します。

```
aaa authentication http console LOCAL
```

ステップ 4 CLI を使用して、ASA で API トラフィック用のスタティックルートを作成します。次に例を示します。

```
route <management interface nameif> 0.0.0.0 0.0.0.0 <gwip> 1
```

ステップ 5 CLI を使用して、ASA で ASA REST API エージェントを有効にします。例：

```
rest-api agent
```

REST API 認証

認証には、すべての要求でユーザー名とパスワードを渡す基本 HTTP 認証と、各要求で以前に作成したトークンを渡すセキュアな HTTPS トランスポートを使用したトークンベースの認証という 2 つの方法があります。いずれの方法でも、認証は要求ごとに実行されます。トークンベースの認証に関する詳細については、『*About the ASA REST API v7.14(x)*』ガイドの「Token_Authentication_API」セクションを参照してください。

（注） ASA では認証局（CA）発行済み証明書の使用が推奨されているため、REST API クライアントが SSL 接続を確立するときに、ASA のサーバー証明書を検証できます。

コマンド認証

コマンド認可が外部の AAA サーバーを使用するように設定されている場合（例：`aaa authorization command <TACACS+_server>`）、完全なコマンド権限を持つ「**enable_1**」という名前のユーザーがそのサーバーに存在している必要があります。

コマンド認可が ASA の LOCAL データベースを使用するよう設定されている場合（`aaa authorization command LOCAL`）、すべての REST API ユーザが、その権限に合った権限レベルで LOCAL データベースに登録される必要があります。

- モニタリング要求を呼び出すには、権限レベル 3 以上が必要です。
- GET 要求を呼び出すには、権限レベル 5 以上が必要です。
- PUT/POST/DELETE 操作を呼び出すには、権限レベル 15 以上が必要です。

REST API クライアントの設定

ローカルホストブラウザに REST API クライアントをインストールして設定するには、次の手順を実行します。

手順

ステップ 1 ブラウザの REST API クライアントを取得してインストールします。

Chrome の場合は、Google から REST クライアントをインストールします。Firefox の場合は、RESTClient アドオンをインストールします。Internet Explorer はサポートされていません。

ステップ 2 ブラウザを使用して、次のリクエストを開始します。

```
https:<asa management ip address>/api/objects/networkobjects
```

エラー以外の応答を受信した場合は、ASA で機能している REST API エージェントに到達しています。

エージェントリクエストに問題がある場合は、「ASA での REST API デバッグの有効化」で説明されているように、CLI コンソールでデバッグ情報の表示を有効にできます。

ステップ 3 必要に応じて、POST 操作を実行して ASA への接続をテストできます。

次に例を示します。

基本認証クレデンシャル（*<username><password>*）、または認証トークン（詳細については、「トークン認証」を参照）を指定します。

ターゲット リクエスト アドレス：`https://<asa management ipaddress>/api/objects/networkobjects`

本文のコンテンツタイプ：`application/json`

操作の raw 本文：

```
{
"kind": "object#NetworkObj",
"name": "TestNetworkRangeObj",
"host": {
"kind": "IPv4Network",
"value": "12.12.12.0/24"
}
}
```

ASA REST API を使用して、ASA を設定およびモニターできるようになりました。コールの説明と例については、API ドキュメントを参照してください。

バックアップ設定の完全な復元について

REST API を使用して ASA で完全なバックアップ設定を復元すると、ASA がリロードされます。これを回避するには、次のコマンドを使用してバックアップ設定を復元します。

```
{
"commands":["copy /noconfirm disk0:/<filename> running-config"]
}
```

ここで、*<filename>* は backup.cfg または設定をバックアップするときに使用した名前です。

ドキュメントコンソールと API スクリプトのエクスポート

また、REST API オンライン ドキュメント コンソール（「Doc UI」と呼ばれる）を使用することもできます。このコンソールは、ASA で直接 API コールを確認して試すための「サンドボックス」として、*host:port/doc/* で使用できます。

さらに、Doc UI の [エクスポート操作（Export Operation）] ボタンを使用して、表示されたメソッドの例を JavaScript、Python、または Perl のスクリプトファイルとしてローカルホストに保存できます。その後、このスクリプトを ASA に適用し、他の ASA およびネットワークデバイスのアプリケーション用に編集できます。これは、主に学習用およびブートストラップツールとして使用するためのものです。

JavaScript

JavaScript ファイルを使用するには、`http://nodejs.org/` にある `node.js` のインストールが必要です。`node.js` を使用すると、コマンドラインスクリプトのように、通常はブラウザ用に記述された JavaScript ファイルを実行できます。インストール手順に従った後、`node script.js` でスクリプトを実行します。

Python

Python スクリプトでは、`https://www.python.org/` から利用できる Python をインストールする必要があります。Python をインストールしたら、`python script.py username password` で目的のスクリプトを実行できます。

Perl

Perl スクリプトを使用するには、いくつかの追加のセットアップが必要です。Perl 自体と、次の 4 つの Perl ライブラリを含む 5 つのコンポーネントが必要となります。

- Perl パッケージ：http://www.perl.org/
- Bundle::CPAN：http://search.cpan.org/~andk/Bundle-CPAN-1.861/CPAN.pm
- REST::Client：

  http://search.cpan.org/%7Emcrawfor/REST-Client-88/lib/REST/Client.pm
- MIME::Base64：http://perldoc.perl.org/MIME/Base64.html
- JSON：http://search.cpan.org/~makamaka/JSON-2.90/lib/JSON.pm

次に、Macintosh で Perl をブートストラップする例を示します。

```
$ sudo perl -MCPAN e shell
cpan> install Bundle::CPAN
cpan> install REST:: Client
cpan> install MIME::Base64
cpan> install JSON
```

依存関係をインストールしたら、`perl script.pl username password` を使用してスクリプトを実行できます。

ASA での REST API デバッグの有効化

ASA で REST API を設定したり REST API へ接続したりする際に問題が生じる場合は、次の CLI コマンドを使用して、コンソールでのデバッグメッセージの表示を有効にできます。デバッグメッセージを無効にするには、コマンドの no 形式を使用します。

debug rest-api [**agent** | **cli** | **client** | **daemon** | **process** | **oken-auth**] [**error** | **event**]

no debug rest-api

構文の説明

agent	（オプション）REST API エージェントのデバッグ情報を有効にします。
cli	（オプション）REST API CLI デーモンからエージェントへの通信に対するデバッグメッセージを有効にします。
client	（オプション）REST API クライアントと REST API エージェント間のメッセージルーティングに対するデバッグ情報を有効にします。
daemon	（オプション）REST API デーモンからエージェントへの通信に対するデバッグメッセージを有効にします。

process	（オプション）REST APIエージェントの開始/停止処理に関するデバッグ情報を有効にします。
token-auth	（オプション）REST API トークン認証のデバッグ情報。
error	（オプション）このキーワードを使用して、デバッグメッセージを API によってログに記録されるエラーのみに制限します。
event	（オプション）このキーワードを使用して、デバッグメッセージを API によってログに記録されるイベントのみに制限します。

使用上のガイドライン

特定のコンポーネントキーワードを指定しない場合（つまり、単に **debug rest-api** コマンドを発行する場合）、すべての種類のコンポーネントにデバッグメッセージが表示されます。**event** または **error** のいずれかのキーワードを指定しない場合、指定したコンポーネントのイベントメッセージとエラーメッセージの両方が表示されます。たとえば、**debug rest-api daemon event** は、API デーモンとエージェント間の通信に対するイベントデバッグメッセージのみを表示します。

関連コマンド

コマンド	説明
debug http	このコマンドを使用して、HTTP トラフィックに関する詳細情報を表示します。

ASA REST API 関連の syslog メッセージ

このセクションでは、ASA REST API 関連の system-log メッセージについて説明します。

関連資料

次のリンクを活用して、ASA とその設定および管理に関する詳細情報を参照してください。

- *Cisco ASA* シリーズ ドキュメントのナビゲーション：http://www.cisco.com/go/asadocsxm-replace_text%20List%20Item

ASAv でサポートされていない ASA の機能を一覧表示するには、次のリンクを使用します。

- http://www.cisco.com/c/en/us/td/docs/security/asa/asa92/configuration/general/asa-general-cli/introasav.html#pgfId-1156883

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

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: https://www.cisco.com/c/en/us/about/legal/trademarks.html. 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. (1721R)

© 2020 Cisco Systems, Inc. All rights reserved.

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。