CHAPTER 5

外部 RESTful サービス API の概要

外部 RESTful サービスは HTTPS および REST 方法論に基づいており、ポート 9060 を使用します。この章では、Cisco ISE でサポートされている外部 RESTful サービス アプリケーション プログラミング インターフェイス（API）、および作成、読み取り、更新、削除（CRUD）操作に使用される関連 API コールを使用するためのガイドラインおよび例について説明します。

これらの API は、ユーザ、エンドポイント、エンドポイント グループ、ID グループおよび SGT が ISE データに対する CRUD 操作を実行できるようにすることによって、ISE 設定データへのインターフェイスを提供します。

HTTPS ポート 9060 はデフォルトで閉じられています。API を使用する最初の要件は、ISE CLI から外部 RESTful サービスをイネーブルにすることです。

（注） CLI からイネーブルにする前に外部 RESTful サービス API を起動しようとすると、403- "forbidden" のような応答ステータスを受信します。

外部 RESTful サービスにはデバッグ ロギング カテゴリがあり、Cisco ISE のデバッグ ロギングのページでイネーブルにできます。詳細については、『*Cisco Identity Services Engine User Guide, Release 1.2*』の「Debug Log Configuration Options」セクションを参照してください。

すべての Representational State Transfer（REST）操作は、システムで監査され、記録されます。

関連項目

「外部 RESTful API サービスのイネーブル化」（P.5-2）

データの検証

サーバに送信された CRUD データは、Cisco ISE が GUI に対して持つルールと同じルールで検証されます。すべての検証は、検証レイヤに集中化されます。ポストされたすべての XML データはスキーマと照合して検証されます。

次の 2 種類の検証が実行されます。データ検証および構造検証。データ検証は、データが Cisco ISE に準拠していることを検証します。たとえば、必須フィールド、フィールド長、タイプなど。構造検証はスキーマを検証します。たとえば、フィールドの順序、名前、など。

外部 RESTful サービスの名前空間

次のようなリソースの名前やユニフォーム リソース識別子（URI）内の厳密な名前空間を維持する必要があります。

- 内部ユーザ ID、エンドポイント、エンドポイント グループおよび ID グループ。
- セキュリティ グループ タグ（SGT）のセキュリティ グループ アクセス（SGA）。
- 応答メッセージに表示される検索結果など、他のすべての外部 RESTful サービス リソースに対する外部 RESTful サービス。

Accept/Content-Type ヘッダーには、次の名前空間が含まれている必要があります。

```
application/vnd.com.cisco.ise.<resource-namespace>.<resource-type>.<major
version>.<minor version>+xml
```

例：`application/vnd.com.cisco.ise.identity.internaluser.1.0+xml`

要求 XML には、次の名前空間の定義が含まれている必要があります。

```
identity.ers.ise.cisco.com

sga.ers.ise.cisco.com
```

例：

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns:endpoint xmlns:ns="identity.ers.ise.cisco.com" id="id">
<group>Profiled</group>
...
</ns:endpoint>
```

外部 RESTful API サービスのイネーブル化

ステップ 1　**application configure ise** コマンドを実行します。

ステップ 2　次のオプションが画面に表示されます。

```
[1]Reset Active Directory settings to defaults
[2]Display Active Directory settings
[3]Configure Active Directory settings
[4]Restart/Apply Active Directory settings
[5]Clear Active Directory Trusts Cache and restart/apply Active Directory settings
[6]Enable/Disable External RESTful Services API
[7]Reset M&T Session Database
[8]Rebuild M&T Unusable Indexes
[9]Purge M&T Operational Data
[10]Reset M&T Database
[11]Refresh M&T Database Statistics
[12]Display Profiler Statistics
[13]Exit
```

ステップ 3　**6** と入力して Enter キーを押します。

次のメッセージが表示されます。

```
Current External RESTful Services State: disabled

By proceeding, External RESTful Services port 9060 will be opened and External RESTful
Services API will be enabled

Are you sure you want to proceed?y/n [n]:
```

ステップ 4　y を入力して、Enter を押します。

次のメッセージが表示されます。

```
Enabling External RESTful Services port 9060...
External RESTful Services API enabled
```

ステップ 5　次の URL の外部 RESTful サービス SDK ページにアクセスして、外部サービス RESTful API がイネーブルになっているかどうかを確認してください。https://<ipaddress>:9060/ers/sdk。SDK にアクセスするには、常にポート番号を 9060 として追加する必要があります。

外部 RESTful サービス管理者

API を使用するには、外部 RESTful サービス管理者グループで ISE 管理者を作成する必要があります。管理者ユーザの作成の詳細については、『Cisco Identity Services User Guide, Release 1.2』の次の項を参照してください。

http://www.cisco.com/en/US/docs/security/ise/1.2/user_guide/ise_man_admin.html#wp1579129

REST クライアント

外部 RESTful サービス API を使用するには、HTTPS クライアントが必要です。Curl のコマンドを使用してサーバに要求をポストすることも、独自の Python スクリプトまたは Java クライアントを書き込むこともできます。Chrome ブラウザの POSTMAN プラグインなどの HTTP ポスティング ツールを使用することもできます。これで、外部 RESTful サービスがイネーブルになり、準備ができたので、使用し始めることができます。

関連項目

「外部 RESTful サービス API コールの呼び出し」（P.6-1）

第 6 章「REST API クライアントの使用方法」

リソースのバージョンと MediaType

外部 RESTful サービスでは、リソースの表現および要求本体は通常、XML で符号化されます（RFC4267 で指定されている）。リソースの各タイプは、次のパターンに一致する独自のメディアタイプを持ちます。

application/vnd.com.cisco.ise.xxx.yyy.version+xml;charset=UTF-8

ここで、「xxx」は名前空間を表し、「yyy」はリソースを表し、バージョンはクライアントが使用するリソースのバージョンを指定します。（RFC 3023）。たとえば、スキーマ バージョン 1.0 の内部ユーザのリソースの MediaType は次のように表されます。

application/vnd.com.cisco.ise.identity.internaluser.1.0+xml;charset=UTF-8

外部 RESTful サービス API は、XML で使用可能なすべてのリソースの表現を提供する必要があります。要求されたメディア タイプが Cisco ISE サーバでサポートされていない場合は、いつでも「Resource version is no longer supported（リソースのバージョンはサポートされなくなりました）」などの原因のリストとともにステータス 415 が返されます。

外部 RESTful サービス要求

外部 RESTful サービスに行われる要求では、表 5-1 で説明されているように複数の固有の HTTP ヘッダーが使用されます。

表 5-1　外部 RESTful サービス要求ヘッダー

ヘッダー	サポートされる値	用途	必須
Accept	メディア タイプまたはメディア タイプ パターンのカンマ区切りリスト。	このクライアントが受け入れを準備しているメディア タイプを、リソースのバージョンを含めて、サーバに示します。	GET/GET ALL/DELETE/GET VERSION 操作（これらには、メッセージ本文は含まれません）で、はい。
Authorization	「Basic」に加えてユーザ名とパスワード（RFC 2617 に準拠）。	この要求を実行する許可ユーザを識別します。	すべての要求で、はい。
Content-Length	要求メッセージ本文の長さ（バイト単位）。	メッセージ本文のサイズを示します。	メッセージ本文を含む要求で、はい。
Content-Type	要求メッセージ本文を示すメディア タイプ。	要求メッセージ本文の表現と構文について示します。	メッセージ本文を含む要求で、はい。

外部 RESTful サービス応答ヘッダー

外部 RESTful サービスによって返される要求では、表 5-2 で説明されているように複数の固有の HTTP ヘッダーが使用されます。

表 5-2　外部 RESTful サービス応答ヘッダー

ヘッダー	サポートされる値	用途	必須
Content-Length	応答メッセージ本文の長さ（バイト単位）。	メッセージ本文のサイズを示します。	メッセージ本文を含む応答で、はい。
Content-Type	応答メッセージ本文を示すメディア タイプ。	応答メッセージ本文の表現と構文について示します。	メッセージ本文を含む応答で、はい。
Location	新しく作成されたリソースの正規の URI。	新しく作成されたリソースの表現を要求するために使用できる新しい URI を返します。	URI でアクセスできる新しいサーバ側リソースを作成する要求への応答で、はい。

共通の外部 RESTful サービス HTTP 応答コード

外部 RESTful サービスは、表 5-3 で説明されているように共通の HTTP 応答コードを返します。応答ヘッダーで返されるステータス コードに加えて、各要求には、要求の性質に応じて、追加の XML コンテンツがある場合があります。

表 5-3　外部 RESTful サービスから返された HTTP 応答コードの説明

HTTP ステータス	説明
200 OK	要求は正常に完了しました。この要求により URI でアドレス指定可能な新しいリソースが作成され、新しいリソースの表現を含む応答本文が返される場合は、新規作成されたリソースの正規の URI を含む Location ヘッダーとともに 200 ステータスが返されます。
201 Created	新しいリソースを作成する要求は完了しましたが、新しいリソースの表現を含む応答本文は返されていません。新しく作成されたリソースの正規の URI を含む Location ヘッダーも返す必要があります。
202 Accepted	要求が受け入れられ処理されていますが、処理が完了していません。HTTP/1.1 仕様に従って、返されるエンティティ（ある場合）は、要求の現在のステータスの説明、およびステータス モニタへのポインタまたは要求の実行が期待できる時間の概算へのポインタを含む*必要があります*。
204 No Content	サーバは要求を満たしましたが、応答メッセージ本文を返す必要はありません。
400 Bad Request	欠落した情報または無効な情報が含まれるため（入力フィールドの検証エラーまたは必要な値の欠落など）、要求を処理できませんでした。
401 Unauthorized	要求に含まれる認証クレデンシャルが欠落しているか、または無効です。
403 Forbidden	サーバはクレデンシャルを認識しましたが、この要求を実行する許可を所有していません。
404 Not Found	要求は、存在しないリソースの URI を指定しました。
405 Method Not Allowed	要求に指定された HTTP 動詞（DELETE、GET、HEAD、POST、PUT）は、この要求 URI でサポートされていません。
406 Not Acceptable	この要求によって識別されたリソースは、要求の Accept ヘッダーのメディア タイプの 1 つに対応する表現を生成できません。
409 Conflict	サーバによってサポートされるリソースの現在の状態に競合が生じるため、作成または更新要求を完了できませんでした（たとえば、既存のリソースに割り当てられている一意の ID で新しいリソースを作成する試行）。
415 Unsupported Media Type	Accept ヘッダーに指定されたメディア タイプは、サーバによってサポートされていません。これは、クライアント リソースのバージョンがサーバでサポートされなくなった場合の共通の応答です。
429 Too many requests	同時に非常に多くの RESTful サービス要求があります。
500 Internal Server Error	サーバで、要求の処理を妨げる予期しない状態が発生しました。
501 Not Implemented	サーバは（現在）要求を処理するために必要な機能をサポートしていません。
503 Service Unavailable	サーバの一時的な過負荷またはメンテナンスのため、サーバは現在要求を処理できません。

外部サービス RESTful API でのバージョン管理

外部サービス RESTful API は、バージョン管理メカニズムによって以前の Cisco ISE バージョンとの下位互換性を提供します。Cisco ISE Release 1.2 は最初の外部 RESTful サービス リリースなので、すべてのリソースはバージョン 1.0 で、下位互換性は必要ではありません。

それぞれの RESTful リソースにはモデル バージョン（major.minor）があります。バージョンは、次のような構文を持つ要求ヘッダーの一部である必要があります。

```
application/vnd.com.cisco.ise.<resource-namespace>.<resource-type>.<major version>.<minor version>+xml
```

たとえば、内部ユーザ リソース バージョン 1.0 を取得するには、次の要求を渡します。

```
DELETE /ers/config/internaluser/333 HTTP/1.1
Host: cisco.com
Authorization: Basic xxxxxxxxxxxxxxxxxx
Accept: application/vnd.com.cisco.ise.identity.internaluser.1.0+xml
```

要求の認証と承認後、バージョン一致のチェックが実行され、次のいずれかの一致の結果になります。

表 5-4　バージョン一致の結果

バージョン一致	結果
送信されたバージョンなし	サーバは、ステータス 415 の「Unsupported Media Type」を返します。
クライアントのバージョンとサーバのバージョンは等しい	サーバは、要求の処理を続行します。
クライアントのマイナー バージョンとサーバのマイナー バージョンは等しくない	サーバは、バージョン ギャップを示す応答の警告メッセージを追加し、要求の処理を続行します。
クライアントとサーバのメジャー バージョンが一致しません	サーバは、ステータス 415 および対応するエラー メッセージを返します。

さらに、各リソースにはサーバでサポートされているバージョンのリストを取得する API があります。

外部サービス RESTful API でのページング

検索結果は、デフォルトでページあたり 20 のリソースでページ付けされます。ページ番号付けはページ番号 0 から開始します。1 ページあたりの最大リソース数は 100 を超えることはできません。ページング パラメータを使用してデフォルトを上書きできます。ページング パラメータは、クエリー パラメータを使用して URI で渡されます。

たとえば、「名前」フィールドで昇順にソートされた内部ユーザの最初の 50 レコードを取得するには、次の要求を渡します。

```
GET/ers/config/internaluser/?page=0&size=50&sortacs=name.EQ.Finance HTTP/1.1
```

次のページング パラメータを使用できます。

表 5-5　ページング パラメータ

パラメータ	説明
page	ページの開始インデックス。デフォルト値は 0 です。
size	ページ サイズ。デフォルト値は 10 で、最大サイズは 100 です。
sortbyasc	昇順でフィールドをソートします。デフォルト値は "name" フィールドです。
sortbydsc	降順でフィールドをソートします。デフォルト値は "name" フィールドです。

外部サービス RESTful API でのソート

デフォルトでは、検索結果はカラム名に従って昇順でソートされます。ソート パラメータを指定して、デフォルトのソート設定を上書きできます。クエリー パラメータを使用してソート パラメータを URI で渡すことができます。デフォルト設定を上書きするために 'sortasc'（昇順）または 'sortdsc'（降順）パラメータを指定できます。

たとえば、内部ユーザの最初の 50 レコードを「名前」フィールドで降順にソートするには、次の要求を渡します。

```
GET
/ers/config/internaluser?filter=name.STARTW.a&filter=identityGroup.EQ.Finance&size=50&p
age=0&sortdsc=name
```

外部サービス RESTful API でのフィルタリング

フィルタのクエリー文字列パラメータを使用して簡単なフィルタ操作を実行できます。複数のフィルタを送信できます。すべてのフィルタ基準に共通の論理演算子はデフォルトで AND です。"filtertype=or" のクエリー文字列パラメータを使用してこれを変更できます。

各リソース データ モデルの説明には、属性がフィルタ処理されたフィールドかどうか指定する必要があります。

たとえば、名が "a" で始まり "Finance" ID グループに属する内部ユーザを取得するには、次の要求を渡します。

```
GET
/ers/config/internaluser/?page=0&size=20&sortacs=name&filter=name.STARTSW.a&filter=identit
yGroup.EQ.Finance HTTP/1.1
```

次のフィルタ パラメータを使用できます。

表 5-6　使用可能なフィルタ パラメータ

パラメータ	説明
EQ	等しい
GT	より大きい
LT	より小さい
STARTSW	から開始
ENDSW	で終了
CONTAINS	が次の文字列を含む（Contains）
NEQ	等しくない。
NSTARTSW	から開始しない
NENDSW	で終了しない
NCONTAINS	含まない

表 5-7　リソースごとのフィルタリング可能な属性のリスト

リソース	フィルタリング可能な属性
エンドポイント	mac、portalUser、profile、profileId、staticGroupAssignment、staticProfileAssignment
内部ユーザ	name
エンドポイント ID グループ	name
ID グループ	name
SGT	name
プロファイラ ポリシー（読み取り専用）	name

検索結果内のリンクの例

```
<ns2:searchResult xmlns:ns2="ers.ise.cisco.com"   total="1163">
<link rel="self"
href="http://cisco.com/ers/config/internaluser?page=0&size=20"
type="application/xml"/>
<link rel="next" href="http://cisco.com/ers/config/internaluser?page=20&size=20"
type="application/xml"/>
<resources>
<link rel="john doe" href="http://cisco.com/ers/config/internaluser/333"
type="application/xml"/>
<link rel="jeff smit" href="http://cisco.com/ers/config/internaluser/444"
type="application/xml"/>
.
.
.
</resources>
</ns2:searchResult>
```

外部 RESTful サービス データ モデル

外部 RESTful サービス データ モデルは、外部 RESTful API サービスが操作する RESTful リソースの表現を定義します。表現はフィールドから構成され、各フィールドは XML ディクショナリを使用して符号化された名前と値を持ちます。値は、数値または文字列リテラル、リスト、またはディクショナリで、それぞれ XML で表現されます。

リソースの各タイプには、独自のインターネット メディア タイプが含まれます。内部メディア タイプは、次のパターンに準拠している必要があります。

application/vnd.com.cisco.ise.resource.version+xml;charset=UTF-8

各 RESTful リソースに対応するメディア タイプはセクション ヘッダーで角カッコに含まれています。

リソースのモデルの説明では、[Post] で注釈を付けられたフィールドは、新しいリソースを作成するために使用される POST 要求に含まれます。同様に、[PUT] で注釈を付けられたフィールドは、既存のリソースのプロパティを更新するために使用される PUT 要求に含まれます。注釈を付けられていないフィールドを PUT または POST 要求の要求本体に含めないでください。そのような要求はサーバによって無視されます。

基本リソース

各リソースには、次の表に記載されている一連の属性またはフィールドを構成する基本表現が含まれます。

表 5-8　基本表現属性

フィールド名	タイプ	デフォルト値	発生回数	説明
URI	ハイパーリンク	—	1	この URI に対して行われた GET 要求によって、このユーザがアクセスできるリソースのクライアントの表現が更新されます。
id	String	—	1	リソースの uid [PUT]
name	String	—	1	リソースの名前 [POST][PUT]
description	String	—	0..1	リソースの説明 [POST][PUT]

内部ユーザ

内部ユーザのインターネット メディア タイプは次の形式に準拠している必要があります。

application/vnd.com.cisco.ise.identity.internaluser.1.0+xml

内部ユーザのデータ モデルには、次の表に記載されている一連の属性またはフィールドが含まれます。

表 5-9　内部ユーザのデータ モデル - 属性

フィールド名	タイプ	デフォルト値	発生回数	説明
URI	ハイパーリンク	—	1	この URI に対して行われた GET 要求によって、このユーザがアクセスできるリソースのクライアントの表現が更新されます。
id	String	—	1	リソースの uid [PUT]
name	String	—	1	内部ユーザ名 [POST][PUT]
description	String	—	0..1	ユーザの説明 [POST][PUT]
enabled	ブール値	true	1	ユーザがイネーブルかどうかを示す [POST][PUT]
email	String	—	0..1	ユーザの電子メール アドレス [POST][PUT]
password	String	—	1	ユーザのパスワード [POST][PUT]
firstName	String	—	1	ユーザの名 [POST][PUT]
lastName	String	—	1	ユーザの姓 [POST][PUT]
changePassword	ブール値	true	1	次回のログイン試行時にパスワード変更を強制する
identityGroups	String	—	1	identityGroup ID がカンマで区切られた文字列。
costumeAttributes	マップ（K、V）	—	0..1	属性の名前を表すキー ストリングと属性の値を表す値ストリングとのマッピング

エンドポイント

内部ユーザのインターネット メディア タイプは次の形式に準拠している必要があります。

application/vnd.com.cisco.ise.identity.endpoint.1.0+xml

エンドポイントのデータ モデルには、次の表に記載されている一連の属性またはフィールドが含まれます。

表 5-10　エンドポイントのデータ モデル - 属性

フィールド名	タイプ	デフォルト値	発生回数	説明
URI	ハイパーリンク	—	1	この URI に対して行われた GET 要求によって、このエンドポイントがアクセスできるリソースのクライアントの表現が更新されます。
id	String	—	1	リソースの uid [PUT]
description	String	—	0..1	エンドポイントの説明 [POST][PUT]
macAddress	String	true	1	エンドポイントの MAC アドレス
profile	String	—	0..1	エンドポイント ポリシー
profileID	String	—	0..1	プロファイル ID
EndPointIdentityGroupId	String	—	0..1	次回のログイン試行時にパスワード変更を強制する
StaticIdGroupAssignment	ブール値	false	1	ID グループの ID がカンマで区切られた文字列
portalUser	String	—	0..1	属性名を表すキー ストリングと属性値を表す値ストリングとのマッピング。
IdentityStore	String	—	—	—
identityStoreId	String	—	—	—

エンドポイント ID グループ

エンドポイント ID グループのインターネット メディア タイプは次の形式に準拠している必要があります。

application/vnd.com.cisco.ise.identity.endpointidentitygroup.1.0+xml

エンドポイント ID グループのデータ モデルには、次の表に記載されている一連の属性またはフィールドが含まれます。

表 5-11　エンドポイント ID グループのデータ モデル - 属性

フィールド名	タイプ	デフォルト値	発生回数	説明
URI	ハイパーリンク	—	1	この URI に対して行われた GET 要求によって、このユーザがアクセスできるリソースのクライアントの表現が更新されます。
id	String	—	1	リソースの uid [PUT]
name	String	—	1	ID グループの名前 [POST][PUT]

表 5-11　エンドポイント ID グループのデータ モデル - 属性 （続き）

フィールド名	タイプ	デフォルト値	発生回数	説明
description	String	—	0..1	ID グループの説明 [POST][PUT]
systemDefined	ブール値	—	1	—

ID グループ

ID グループのインターネット メディア タイプは次の形式に準拠している必要があります。

application/vnd.com.cisco.ise.identity.identitygroup.1.0+xml

ID グループのデータ モデルには、次の表に記載されている一連の属性またはフィールドが含まれます。

表 5-12　ID グループのデータ モデル - 属性

フィールド名	タイプ	デフォルト値	発生回数	説明
URI	ハイパーリンク	—	1	この URI に対して行われた GET 要求によって、このユーザがアクセスできるリソースのクライアントの表現が更新されます。
id	String	—	1	リソースの uid [PUT]
name	String	—	1	ID グループの名前 [POST][PUT]
description	String	—	0..1	ID グループの説明 [POST][PUT]

SGT

SGT のインターネット メディア タイプは次の形式に準拠している必要があります。

application/vnd.com.cisco.ise.sga.sgt.1.0+xml

SGT のデータ モデルには、次の表に記載されている一連の属性またはフィールドが含まれます。

表 5-13　SGT のデータ モデル - 属性

フィールド名	タイプ	デフォルト値	発生回数	説明
URI	ハイパーリンク	—	1	この URI に対して行われた GET 要求によって、このユーザがアクセスできるリソースのクライアントの表現が更新されます。
id	String	—	1	リソースの uid [PUT]
name	String	—	1	SGT の名前 [POST][PUT]
description	String	—	0..1	SGT の説明 [POST][PUT]
value	String	—	1	SGT 値
generatedId	String	—	1	SGT によって生成された ID。この属性は読み取り専用です
isTagFromRange	ブール値	—	1	isTagFromRange

VersionInfo

VersionInfo のインターネット メディア タイプは次の形式に準拠している必要があります。

application/vnd.com.cisco.ise.ers.versioninfo.1.0+xml

VersionInfo のデータ モデルには、次の表に記載されている一連の属性またはフィールドが含まれます。

表 5-14　VersionInfo のデータ モデル - 属性

フィールド名	タイプ	発生回数	説明
supportedVersions	String	1	このデータ モデルでサポートされているバージョンを説明する CSV。
currentServerVersion	String	1	サーバ データ モデル実装のバージョン。

SearchResult

SearchResult のインターネット メディア タイプは次の形式に準拠している必要があります。

application/vnd.com.cisco.ise.ers.searchresult.1.0+xml

SearchResult のデータ モデルには、次の表に記載されている一連の属性またはフィールドが含まれます。

表 5-15　SearchResult のデータ モデル - 属性

フィールド名	タイプ	発生回数	説明
total	String	1	検索結果の総数
type	String	1	検索を実行するリソース タイプ
self	ハイパーリンク	1	現在の表現を更新するリンク
next	ハイパーリンク	0..1	次の結果ページを取得するリンク
Prev	ハイパーリンク	0..1	前の結果ページを取得するリンク
resources	BaseResource[]	0..1	基本リソースの集合

外部 RESTful サービス応答

外部 RESTful サービス応答のインターネット メディア タイプは次の形式に準拠している必要があります。

application/vnd.com.cisco.ise.ersresponse.1.0+xml

外部 RESTful サービス応答のデータ モデルには、次の表に記載されている一連の属性またはフィールドが含まれます。

表 5-16　外部 RESTful サービス応答のデータ モデル - 属性

フィールド名	タイプ	発生回数	説明
operation	String	1	実行された操作を説明する（たとえば、[put]update-internaluser）
targetURI	ハイパーリンク	0..1	応答が続く要求 URI
messages	ResponseMessage[]	0..1	サーバからのメッセージの配列

応答メッセージ

応答メッセージのインターネット メディア タイプは次の形式に準拠している必要があります。

application/vnd.com.cisco.ise.ersresponse.1.0+xml

応答メッセージのデータ モデルには、次の表に記載されている一連の属性またはフィールドが含まれます。

表 5-17　応答メッセージのデータ モデル - 属性

フィールド名	タイプ	発生回数	説明
title	String	1	このメッセージで報告される問題の性質を説明するローカライズされたテキスト。
type	String	1	次の値を使用して、メッセージ タイプを示します。 • INFO • 警告 • エラー
code	String	0..1	このメッセージで報告されるエラーのタイプを識別するシンボリック エラー コード（たとえば、検証エラー）
stackTrace	String	0..1	このメッセージに関連付けられたスタック トレース（デバッグ モードのみ）。
hint	String	0..1	問題の性質をさらに説明するローカライズされたテキストで、クライアントが試行可能な回避策を含むことがあります。

エラー応答

要求が失敗するときは常に、問題を説明するために、HTTP エラー ステータスと応答の内容がクライアントに返されます。次の表で、発生する可能性のあるエラーについて説明します。

表 5-18　エラー コード

エラー コード	説明	HTTP ステータス
ERS_INTERNAL_EXCEPTION	実行時に発生する予期しない内部サーバ エラー。	500
ERS_VERSION_EXCEPTION	要求内容で送信されるリソースのバージョンがサーバによってサポートされなくなった場合に発生します。	415

表 5-18　エラー コード （続き）

エラー コード	説明	HTTP ステータス
ERS_MEDIA_TYPE_EXCEPTION	ACCEPT または Content-Type ヘッダーでクライアントから送信されるメディア タイプが無効である場合に発生します。	415
ERS_UNSUPPORTED_RESOURCE_EXCEPTION	URI に表示されているようには、リソースがサーバでサポートされていない場合に発生します。	400
ERS_UNSUPPORTED_METHOD_EXCEPTION	要求メソッド タイプが、指定した URI ではサポートされていない場合に発生します。	400
ERS_QUERY_VALIDATION_EXCEPTION	検索フィルタまたはページング パラメータが無効である場合に発生します。	400
ERS_SCHEMA_VALIDATION_EXCEPTION	スキーマに対するリソースの検証に失敗した場合に発生します。	400
ERS_CONVERSION_EXCEPTION	一部の内部変換のために発生し、INTERNAL_EXCEPTION として処理される必要があります。	500
ERS_APPLICATION_RESOURCE_VALIDATION_EXCEPTION	リソースの意味検証が要件を満たしていない場合に発生します。	400
ERS_CRUD_OPERATION_EXCEPTION	CRUD 操作の実行中に発生し、INTERNAL_EXCEPTION として処理される必要があります。	500

更新されるフィールド

更新されるフィールドのインターネット メディア タイプは次の形式に準拠している必要があります。

application/vnd.com.cisco.ise.ers.updatedfields.1.0+xml

更新されるフィールドのデータ モデルには、次の表に記載されている一連の属性またはフィールドが含まれます。

表 5-19　更新されるフィールドのデータ モデル - 属性

フィールド名	タイプ	発生回数	説明
field	String	1	変更されたフィールド名
oldValue	String	1	フィールドの古い値
newValue	String	1	フィールドの変更後の値

外部 RESTful サービス API のセキュリティ機能

外部 RESTful サービス API はデフォルトでディセーブルであり、管理権限を持つユーザが明示的にイネーブルにする必要があります。外部 RESTful サービス API は、HTTPS アクセス（ポート 9060 を使用）および基本 HTTP 認証だけをサポートします。プレーンな HTTP アクセスはサポートされていません。外部 RESTful サービス API 実装では、パスワードの総当たり攻撃を阻止するためのメカニズムを使用します。

外部 RESTful サービス認証

外部 RESTful サービス API は HTTPS でのみ実行され、基本認証をサポートします。認証クレデンシャルは、暗号化され、要求ヘッダーの一部となっています。認証は、Tomcat サーバに対応する基本認証メカニズムを使用して実装されます。

（注）　外部 RESTful サービス アプリケーションが完全にステートレスなので、セッションは管理されません。

外部 RESTful サービス許可

外部 RESTful サービス API では、読み取り専用とフルアクセス レベルの認証を提供します。外部 RESTful サービスを使用して操作を実行するための特権をユーザに割り当てる必要があります。次の 2 種類のロールを割り当てることができます。

- 外部 RESTful サービス スーパー ユーザ：外部 RESTful サービス API にフル アクセスできます（GET、POST、DELETE、PUT）。
- 外部 RESTful サービス ゲスト：読み取り専用アクセスができます（GET 要求のみ）。

必要な権限がないのに、外部 RESTful サービス操作を実行しようとすると、エラー応答を受信します。

関連項目

- 新しい Cisco ISE 管理者の作成

インジェクション攻撃

外部 RESTful サービス Web アプリケーションは、クロス サイト スクリプティング、SQL/HQL インジェクション、シェル インジェクション、およびファイル名操作攻撃を含むあらゆる種類のインジェクション攻撃に対して保護されています。入力の検証も十分行われます。

総当たり攻撃

外部 RESTful サービス API では、パスワードの総当たり攻撃を防止するためのメカニズムを提供します。ユーザが Cisco ISE GUI で定義されているパスワード ポリシーに違反した場合、そのようなユーザ プロファイルは中断またはディセーブルされ、401 ステータス メッセージが返されます。

接続制限

外部 RESTful サービスが使用するポート（ポート 9060 上の https）は、同時に 10 以下の接続しか受け入れません。このメカニズムは、クライアントが API を誤用したり（CPU スタベーション）、ドキュメントを攻撃したりできないようにします。

ISE 導入での外部 RESTful サービス

すべての外部 RESTful サービス要求は、プライマリ ノードに対してのみ有効です。セカンダリ ノードは、読み取りアクセス（GET 要求）のみできます。

外部 RESTful サービス SDK

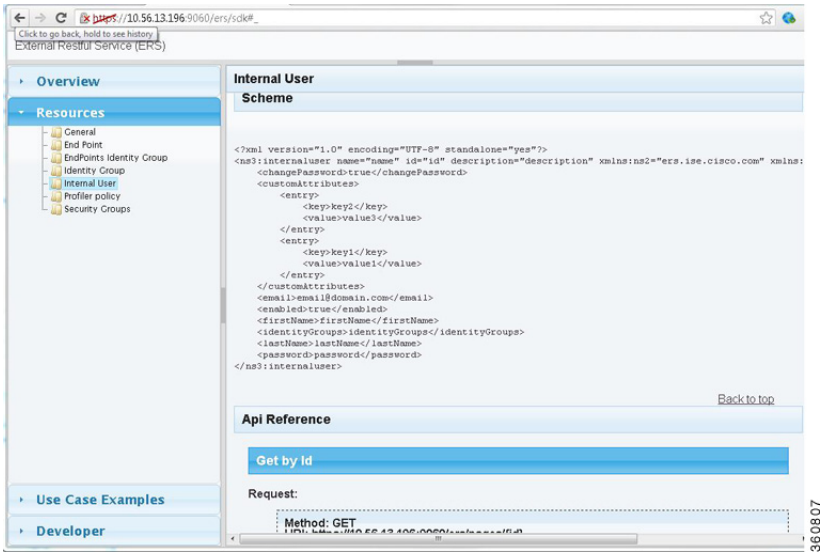
独自のツールを作成するために、外部 RESTful サービスのソフトウェア開発キット（SDK）ページを使用できます。次の URL からそのページにアクセスします。https://<ipaddress>:9060/ers/sdk

[外部 RESTful サービス SDK（External RESTful Services SDK）] ページには、管理者ユーザだけがアクセスできます。次の情報が含まれています。

- 使用可能なすべての API のリスト、および要求構造と応答構造を含む xml の例
- ダウンロード可能なスキーマ ファイル
- 『Cisco ISE API Reference Guide』
- 外部 RESTful サービス クライアントの Java デモ アプリケーション

使用可能なすべての機能については図 5-1 を参照してください。

図 5-1　外部 RESTful サービス SDK



外部 RESTful サービス スキーマ ファイルのダウンロード

外部 RESTful サービス SDK には、外部 RESTful サービス API でサポートされる次の XSD スキーマ ファイルが付属しています。

- ers.xsd
- identity.xsd
- sga.xsd

ステップ 1　次の URL を使用して [外部 RESTful サービス SDK（External RESTful Services SDK）] ページにログインします。

https://<ipaddress>:9060/ers/sdk

ステップ 2　外部 RESTful サービス管理者としてログインします。

ステップ 3　[ダウンロード（Downloads）] の下で使用できる [スキーマ ファイル（Schema Files）] をクリックします。

JAXB などの使用可能なツールとともにこのファイルを使用して、スキーマ クラスを生成できます。

HTTP クライアント コードを開発するか、またはサード パーティ HTTP クライアント コードを使用して、XSD ファイルから生成されたスキーマ クラスと統合できます。

（注）　コンテンツに送信されたすべての XML データはスキーマと照合して検証されます。したがって、XML のフィールド順序と構文はスキーマに表示されるものと同じである必要があります。そうでない場合、Bad Request ステータス コードを受信します。

外部 RESTful サービス システム フロー

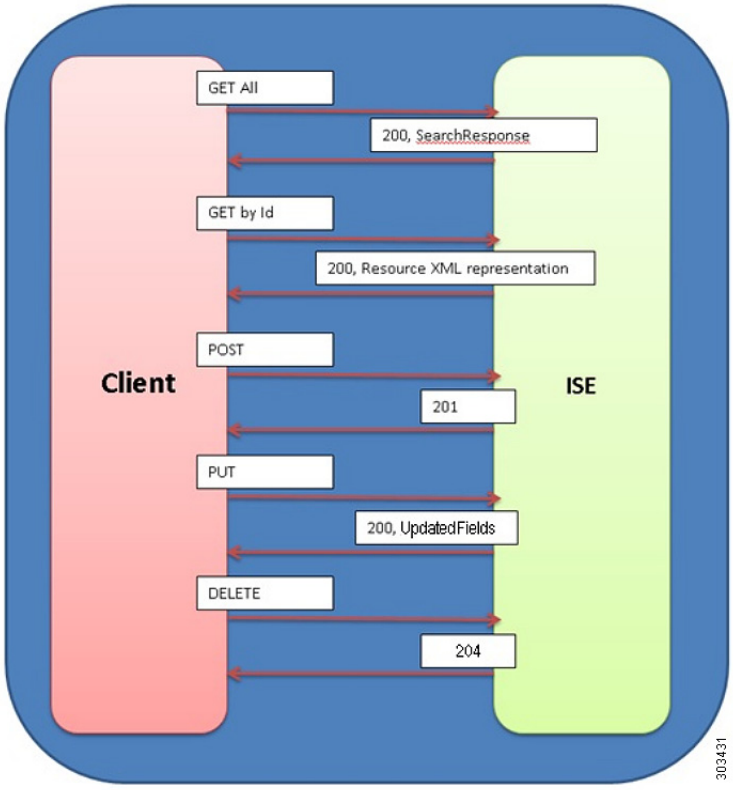
共通の外部 RESTful サービス フローは常に、クライアントから送信される HTTPS 要求とサーバからの HTTPS 応答から構成されます。フローは、要求タイプ、URI、要求ヘッダー、応答ヘッダー、および応答の内容によって異なります。

外部 RESTful サービスの成功フロー シーケンス

共通のフローは常に、クライアントから送信される HTTPS 要求と ISE サーバからの HTTPS 応答から構成されます。フローは、要求タイプ、URI、要求ヘッダー、応答ヘッダーおよび応答の内容によって異なります。要求が成功すると、要求されたアクションが正常に実行されたことを示すために、一般に 200（OK）、201（Created）または 204（No Content）の HTTP ステータス コードが返されます。さらに、それらには、要求された情報の表現を含む応答メッセージ本文（適切なメディア タイプ）が含まれる場合があります。ただし、いくつかの点で失敗する可能性もあります。さまざまな基礎となる原因が、範囲 400 ～ 499（クライアント側エラー）または 500 ～ 599（サーバ側の問題）のさまざまな HTTP ステータス コードによって記述されています。各要求タイプの説明では、要求のタイプによって返される可能性があるステータス コードをリストする必要があります。

次の図に、外部 RESTful サービスの成功フローの例を示します。

図 5-2　外部 RESTful サービスの成功フロー シーケンス



関連項目

「共通の外部 RESTful サービス HTTP 応答コード」（P.5-4）

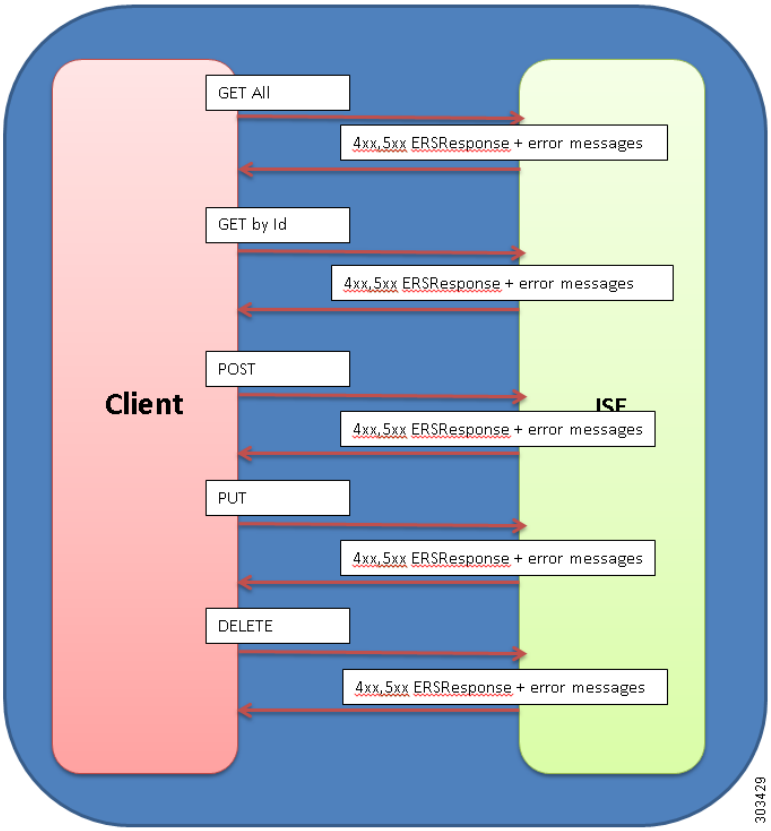
外部 RESTful サービスの失敗フロー シーケンス

要求処理中に、いくつかの点で失敗する可能性もあります。さまざまな基礎となる原因が、範囲 400 ～ 499（クライアント側エラー）または 500 ～ 599（サーバ側の問題）のさまざまな HTTP ステータス コードによって記述されています。各要求タイプの説明では、要求のタイプによって返される可能性があるステータス コードをリストする必要があります。応答がエラー ステータス コード（400 ～ 499 または 500 ～ 599）と共に返される場合、サーバは失敗の原因を記述したメッセージ データ モデルを含む、0 以上のメッセージ データ モデルを含む、応答メッセージ本文を返す必要があります。このようなメッセージのテキスト値は、たとえば、クライアント側のアプリケーションの人間のユーザと通信するために使用される場合があります。

失敗したフローでは、応答の内容に障害の原因となったエラー メッセージのリストが含まれます。

次の図に、外部 RESTful サービスの失敗フローの例を示します。

図 5-3　外部 RESTful サービスの失敗フロー シーケンス



関連項目

「共通の外部 RESTful サービス HTTP 応答コード」（P.5-4）