Proofpoint SER (Secure Email Relay)—API概要

本ドキュメントでは、Proofpoint SER (Secure Email Relay) の概要を説明します。Proofpoint SERは、アプリケーションメールに対し、ユーザーベースメールと同等のセキュリティ、情報保護、コンプライアンスを確保しながらも、これら2つを別々に処理する方法を提供します。そして、認証情報アクセスを認められた送信者にのみ、このサービスの利用を許可することで、脅威リスクを低減します。Proofpoint SER APIは、Tableau、Splunk、PowerBIといったビジネス インテリジェンス（BI）ツールからデータを統合・自動化できるREST APIです。

対象

Proofpoint SER API、および本ドキュメントは、ソフトウェアエンジニア、システムアーキテクト、システムデザイナーを対象としています。ProofpointSER APIを使用するには、リモートコール、オブジェクトクラス、変数、JavaScript、Webアプリケーション開発といった、APIの構成要素に精通している必要があります。こうした要素を使用してソフトウェア アプリケーションやビジネス インテリジェンス（BI）を構築できます。こうした概念に精通していない場合は、ITまたはソフトウェアチームといった組織の他のチームに依頼してください。

2022年初頭に発表されたSplunkアプリやQRadarアプリといった例外を除いて、Proofpoint SER APIは、設定不要のツールではなく、事前定義済みのコネクターを備えていません。そのため、ソフトウェア エンジニア グループは、Proofpoint SER APIの統合方法について、これらのツールで提供されているマニュアルを参照する必要があります。

注：BIツールはさまざまな種類があるため、技術スタッフは完全なプログラミングを実行する必要があります。プルーフポイントでは、Proofpoint SER APIとツールの統合に関するプログラミングサポートを提供しておりません。

トークン生成

Proofpoint SER APIでは、セキュアなデータアクセスを確保するために、トークンベースの認証が要求されます。APIの使用前にアクセストークンを作成する必要があります。トークンは、APIのユーザーとアプリケーションに、リクエストやアクションを実行できるよう、データにセキュアにアクセスするために必要な認証情報と承認を提供するものです。

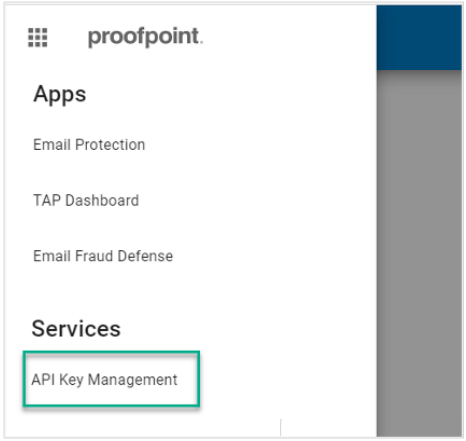
エンドポイントの使用開始時期

エンドポイント	開始時期	コメント
レポート	現在	すべてのSERメールアクティビティへの読み取りアクセスを提供。
検索	2023年第2四半期	SERメール成功/失敗ログへの読み取りアクセスを提供。
ユーザー管理	2023年第2四半期	SMTP認証ユーザーへの読み取り（全顧客）/書き込み（SER Advanced顧客のみ）アクセスを提供。

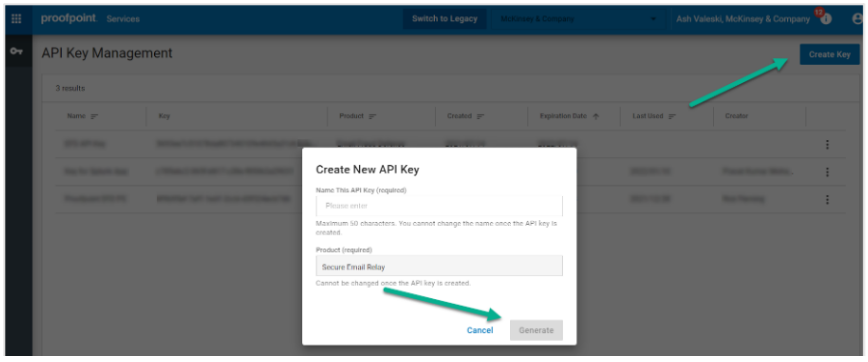
Proofpoint SERアカウントに関連付けられた管理ユーザーはまず、プルーフポイント管理インターフェースから「シークレット」と「キー」を取得し、トークンを作成する必要があります。

シークレットとキーの取得方法

1. https://admin.emaildefense.proofpoint.comにログインします。
2. 左上で**[App Switcher]**を使用し、**[Services]**（サービス）> **[API Key Management]**（APIキー管理）に移動します。



3. **[Create Key]**（キーを作成）、**[Secure Email Relay]**の順に選択します。



注

- 「Secure Email Relay」がリストに表示されない場合、SER管理ユーザー以外のユーザーがログインしています。
- シークレットとキーは有効化してから1年間有効です。

これでシークレットとキーを取得しました。

トークンリクエスト

トークンエンドポイント（**https://auth.proofpoint.com/v1/token**）からトークンをリクエストします。

スクリプトの例

```
#!/bin/sh

#

# トラップハンドラーにアクセスするためのOAUTHトークンを取得

#

CLIENT_ID=yourKey

CLIENT_SECRET=yourSecret

OAUTH_URL=https://auth.proofpoint.com/v1/token

function gettoken() {

TOKEN=`curl -s -v -X POST ${OAUTH _ URL} -H "Cache-Control: no-cache" -d "grant_type=client_
credentials"' & '"client_id=${CLIENT_ID}"' & '"client_secret=${CLIENT_SECRET}" | cut -f 1 -d
"," | cut -f 2 -d ":"| sed -e "s/^\"//g" | sed -e "s/\"$//g"`

echo $TOKEN

}

token=$(gettoken)

echo $token
```

注：トークンの有効期限は43,200秒（12時間）です。

データの取得

https://ser-api.proofpoint.comで前述の方法で取得したトークンを提供し、日付範囲を指定して、Proofpoint SER APIからレポートデータを取得できます。

リクエストの形式は以下のとおりです。

```
GET /v1/sercustomer/report/summary?key1=<>&key2=<>..
```

- 有効なkey1値：startTimeStamp=2020-06-01T00:00:00.000Z (greaterThanEquals)
- 有効なkey2値：endTimeStamp=2020-06-01T00:00:00.000Z (lessThan)
- startTimeStamp,endTimeStamp形式はyyyy-MM-dd’T’HH:mm:ss.SSSZである必要があります
- startTimeStampが指定されていない場合、APIはデフォルトのlicense_startになります。
- endTimeStampが指定されていない場合、APIはデフォルトの現在時刻になります。

リクエスト例1

```
curl --location --request GET 'https://ser-api.proofpoint.com/v1/sercustomer/report/
summary?startTimeStamp=2019-02-10T12:34:00.016Z&endTimeStamp=2019-09-10T12:36:00.016Z' \

--header 'Authorization: Bearer TokenYouGet'
```

リクエスト例2

```
curl --location --request GET 'https://ser-api.proofpoint.com/v1/sercustomer/report/
summary?startTimeStamp=2019-02-10T12:34:00.016Z' \

--header 'Authorization: Bearer TokenYouGet'
```

注：1分あたり最大1,000リクエストを行うことができます。

データ応答

応答データはJSONまたはTEXT（uuencode）形式で取得でき、2つのコンテンツブロックに整理されています。

- **applicationUsers：**アプリケーション別のアクティビティ情報を表示します。
- **entitlement：**スループット数とライセンス期間、またはスループットが適用される期間を表示します。

すべての日付はUTCで表示されます。

各タグ/値ペアの説明を以下の表に示します。

タグ/値ペア

カテゴリー	タグ	説明
applicationUsers	applicationName	applicationUserが関連付けられている/マッピングされている、(SER グローバル アプリケーション データベースのリストにある）アプリケーションを識別するための名前。
	applicationUserName	識別するためのSMTP AUTHユーザー名（SMTP AUTH UIDとの混同に注意が必要です。SMTP AUTH UIDは、SMTP AUTHパスワードと共にメールをシステムに送信するアプリケーション側で設定されるものです)。
	fromEnvelope	RFC.5321 エンベロープ/MFROMアドレスは、承認後SMTP AUTH UIDに使用されます。 **注：**ドメインのみの値は{ワイルドカード}@{ドメイン}.comを意味します。
	fromHeader	RFC.5322ヘッダー /HFROMアドレスは、承認後SMTP AUTH UIDに使用されます。 **注：**ドメインのみの値は{ワイルドカード}@{ドメイン}.comを意味します。
status	success	メールボックスに配信された合計メッセージ数。
	failure	以下のような完全な失敗により、メールボックスに配信されなかった合計メッセージ数。 • SERが許可しなかった（例えば、承認されていないHeader FromがUIDに使用されていた)。 • SERが配信できなかった（例えば、メールボックスが存在しないため、メールボックス プロバイダーから5XXエラーを受け取った)。 • SERが配信を拒否した（例えば、マルウェアが検知された)。
	tempFailure	メールボックス プロバイダーによる一時4XXエラーにより、メールボックスに配信されなかった合計メッセージ数。 **注：**SERはメールリレー製品です。メール配信リクエストを受信すると、指定された受信者への配信を試みます。失敗すると、その後7日間にわたって配信の試行を繰り返します。その7日間の間に配信が成功すると、そのメールは「成功」（success）に分類されます。成功しないまま7日間が経過すると、そのメールは「失敗」（failure）に分類されます。
	partialSuccess	上記のいずれかに分類されなかった合計メッセージ数（まれなケース)。
	inProgress	上記のいずれかに分類されなかった合計メッセージ数（まれなケース)。
	total	success + failure + tempFailure + partialSuccess + inProgress。
	recipientsTotal	メッセージの合計受信者数。
	messageSizeTotal	SERが受信したメッセージの合計サイズ（バイト)。 **注：**この値は実際の使用スループットの算出に使用されます。
	deliveredSizeTotal	SERが送信したメッセージの合計サイズ（バイト)。

カテゴリー	タグ	説明
details	2.X.X	DSN 2.X.Xが返された合計メッセージ数。
	3.X.X	DSN 3.X.Xが返された合計メッセージ数。
	4.X.X	DSN 4.X.Xが返された合計メッセージ数。
	5.X.X	DSN 5.X.Xが返された合計メッセージ数。
entitlement	annual_throughput	license_startからlicense_end dateまでの間に使用できるスループット(データ)。
	license_start	ライセンス期間の開始。
	license_end	ライセンス期間の終了。

カスタマーサポートへのお問い合わせ

SER APIのサポートは、**ser-support@proofpoint.com** (English Only) でご利用いただけます。

詳細はこちら

詳細は、**proofpoint.com/jp**でご確認ください。