２０２６年7月２４日

お客様各位

株式会社日立ソリューションズ
Palo Alto Networks 製品ユーザサポート

【要対応】WildFire ポータルおよび API の各種機能の Strata Cloud Manager への移行について

平素は Palo Alto Networks 製品ユーザサポートをご利用くださいまして誠にありがとうございます。この度、Palo Alto Networks 社より WildFire ポータルおよび WildFire API の各種機能が Strata Cloud Manager へ移行する旨、アナウンスされました。

1. 概要

WildFire の以下の機能が Strata Cloud Manager へ移行されています。

・WildFire ポータルの各種機能(*1)
・WildFire API の各種機能(*2)

移行に伴い、WildFire ポータルおよび CSP サイトにおける WildFire の各種機能の提供は 2026/8/31 をもって終了となります。2026/8/31 以降も引き続き、これらの機能の利用を希望されるお客様におかれましては、Strata Cloud Manager の利用ならびに WildFire API キーの移行をご検討ください。

(*1) WildFire ポータルの各種 Web サイトの一覧(https://wildfire.paloaltonetworks.com/ など)につきましては、以下 Customer Support Portal(以降、CSP サイト)でご参照ください。
CSP サイト > WildFire > WildFire Portals

(*2) WildFire API の各種機能につきましては、以下 CSP サイトで提供中の機能を指します。
CSP サイト > WildFire > WildFire API Keys
CSP サイト > WildFire > WildFire API Usage

2. 対処法

Strata Cloud Manager の利用をご検討ください。Strata Cloud Manager を利用するには、別途ライセンスのアクティベートが必要となります。Strata Cloud Manager には有償版の Strata Cloud Manager Pro ライセンスと、無償版の Strata Cloud Manager Essentials ライセンスがあります。アクティベート手順につきましては、弊社サポートサイトに掲載の下記手順書をご参照ください。

・Strata Cloud Manager のアクティベート手順書
[ダウンロード] > [手順書] > Strata Cloud Manager（旧 AIOps）のアクティベート手順書

WildFire API キーをお持ちのお客様は、Strata Cloud Manager への移行をご検討ください。
WildFire API キーの移行手順につきましては、別紙 1 をご参照ください。

3. その他特記事項

(1) WildFire におけるファイルの検査機能について

Advanced WildFire ライセンスまたは WildFire ライセンスをお持ちでないお客様は、Strata Cloud Manager から WildFire へ手動でアップロードしたファイルの検査機能をご利用頂くことはできません。

Strata Cloud Manager では当該機能の利用にあたり、1 つ以上の WildFire API キーを保有している必要があります。同 API キーの保有には Advanced WildFire ライセンスまたは WildFire ライセンスが必要となります。

(2) WildFire API 呼び出し時における認証方式について

WildFire API 呼び出し時の認証方式は、2027/1/15 まで以下 2 つの方式がサポートされます。

・API キーによる認証　(従来の認証方式)

・アクセストークンによるトークンベース認証

2027/1/15 以降はアクセストークンによるトークンベース認証のみがサポートされ、API キーによる認証は失敗するようになります。WildFire API をご利用のお客様におかれましては、期日までに認証方式の変更の実施をご検討ください。

トークンベース認証による WildFire API の実行例につきましては、別紙 2 をご参照ください。

(3) 本トピックの詳細や最新情報について

本トピックの詳細や最新情報については、下記の Palo Alto Networks 社ページも併せてご参照ください。FAQ も掲載されております。

https://live.paloaltonetworks.com/t5/customer-news/wildfire-portal-transitioning-to-strata-cloud-manager/ba-p/1255117

ご参照いただくには CSP アカウントを所有している必要があります。

CSP アカウントの作成をご要望の場合は、サポートサイト> サービス> 弊社からのお知らせに掲載されている「Paloalto 個人情報取得申請フォーム」に必要事項をご記入頂き、ファイルを添付して弊社サポート窓口まで申請して下さい。

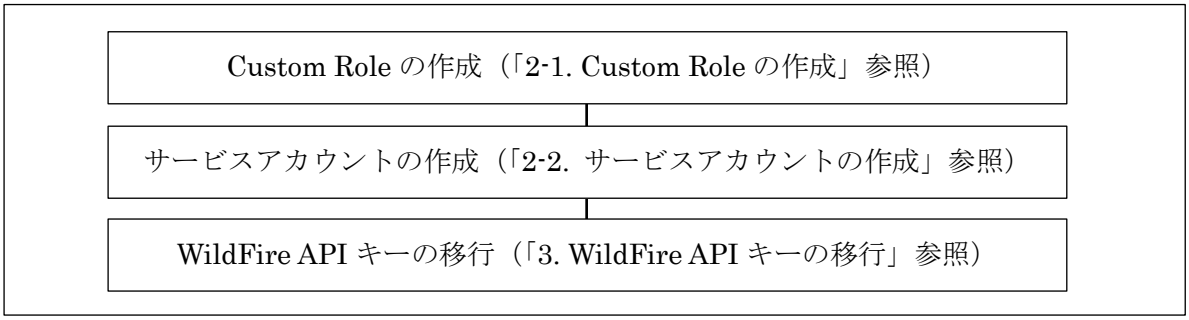
なお、掲載されている以上の情報は開示されておりません。記載内容以上の情報については、弊社サポートではお答え致しかねますことを予めご了承ください。

以上

別紙 1　WildFire API キーの Strata Cloud Manager への移行手順

1.　移行の流れ

WildFire API キーを Strata Cloud Manager へ移行する際の流れを示します。



Custom Role の作成：

サービスアカウントへ付与する権限の設定（Custom Role）を作成します。本手順ではメーカの推奨に従い、アクセストークンの取得に特化した権限を用意します。

サービスアカウントの作成：

アクセストークン取得時の認証に用いるアカウント（サービスアカウント）を作成します。サービスアカウントに作成した Custom Role を割り当てることで権限を付与します。

WildFire API キーの移行：

WildFire API キーを Strata Cloud Manager へ移行し、サービスアカウントと紐づけます。

2.　Custom Role およびサービスアカウントの作成

2-1.　Custom Role の作成

(1) Strata Cloud Manager へログイン後、System Settings > Identity & Access Management の順に画面を遷移します。

(2) Roles タブ > Custom Roles タブの順にクリックします。

(3) 画面上の All Tenants にて Custom Role を作成するテナントをクリックし、Add Custom Role をクリックします。

(4) Add Custom Role で以下の項目を設定します。

設定項目	説明
Name （必須）	Custom Role の名称を入力します。 例：sample
Display Name (オプション)	Custom Role の表示名を入力します。 例：Name に sample、Display Name に SAMPLE と入力した場合、Custom Roles タブに表示される名称(Custom Role Name)は SAMPLE となります。
Description (必須)	Custom Role の説明を入力します。 例：Custom role for creating WildFire API tokens

(5) API タブ>Add Permissions の順にクリックします。

(6) 検索欄に iam と入力して表示された検索結果から、以下の Permission にチェックを入れて選択します。

- iam.custom_role
- iam.service_account

(7) Save をクリックすると、Custom Role が作成されます。

2-2. サービスアカウントの作成

サービスアカウントを作成し、2-1.で作成した Custom Role を割り当てます。

※2-1.の(7)から、続けてサービスアカウントを作成する場合、2-2.の(2)の手順から実施します。

(1) Strata Cloud Manager へログイン後、System Settings > Identity & Access Management の順に画面を遷移します。

(2) Access Management タブ > Add Identity の順にクリックします。

(3) 画面上の All Tenants にてサービスアカウントを作成するテナントをクリックし、Add Identity をクリックします。

(4) Identity Information で以下の項目を設定します。

設定項目	説明
Identity Type (必須)	Service Account を選択します。
Service Account Name (必須)	サービスアカウントの名称を入力します。
Service Account Contact (オプション)	サービスアカウント利用者の e-mail アドレスを入力します。
Description (オプション)	サービスアカウントの説明を入力します。

注意：次画面に遷移後、この画面に戻り設定を変更することはできません。
設定後、Next をクリックして次画面に遷移する前に、設定内容をご確認ください。

(5) Client ID と Client Secret の控えを取得します。
画面上のコピーアイコンをクリックして値をコピーして取得するか、または Download CSV File をクリックして CSV 形式でダウンロードして取得します。取得後、Next をクリックして次画面に遷移します。

注意：Client Secret は再確認ができません。控えは確実に取得してください。

(6) Assign Roles で以下の項目を設定します。

設定項目	説明
Apps & Services (必須)	All Apps & Services を選択します。
Role (必須)	2-1.で作成した Custom Role を割り当てます。

(7) Submit をクリックすると、サービスアカウントが作成されます。

3. WildFire API キーの移行

CSP サイト上の WildFire API キーを Strata Cloud Manager へ移行します。

注意：移行した WildFire API キーを別テナントの Strata Cloud Manager へ再度移行させることはできません。移行の際には下記の点にご注意ください。

- (1)で適切なテナントの Strata Cloud Manager へログインしていること。
- (4)で当該 Strata Cloud Manager へ移行する適切な WildFire API キーを選択していること。
- (5)で適切なサービスアカウントを選択していること。

※2-2.の(7)から続けて移行を行う場合、3.の(2)の手順から実施します。

(1) Strata Cloud Manager へログインします。
(2) Configuration>WildFire Setting の順に画面を遷移します。
(3) 画面上の Start Migration のボタンをクリックします。
(4) プルダウンメニューに表示されている WildFire API キーから、移行するキーにチェックを入れて選択し、画面上の Next をクリックします。
(5) WildFire API キーに紐づけるサービスアカウントを選択します。
(6) 画面上の Migrate をクリックすると、WildFire API キーが移行されます。

別紙 2　トークンベース認証による WildFire API の実行例

スクリプトによる WildFire API の実行例を以下に示します。

■アクセストークンの要求と応答

Palo Alto Networks 社のサーバへアクセストークンを要求します。

スクリプト：

```
curl -X POST https://auth.apps.paloaltonetworks.com/am/oauth2/access_token
 -u CLIENT_ID:CLIENT_SECRET
 -H "Content-Type: application/x-www-form-urlencoded"
 -d "grant_type=client_credentials&scope=tsg_id:TSG_ID"
```

凡例：

- ***CLIENT_ID:CLIENT_SECRET*** : Client ID と Client Secret を入力します。
- ***TSG_ID*** : テナント ID を入力します。

Palo Alto Networks 社のサーバからアクセストークンの応答が返ります。

応答：

```
{
  "access_token":"アクセストークン",
  "scope":"tsg_id:TSG_ID profile email",
  "token_type":"Bearer",
  "expires_in":899
}
```

凡例：

- ***アクセストークン*** : ダブルクォーテーション("")で囲まれた内側の値を控えます。
- ***TSG_ID*** : テナント ID を入力します。

■ファイルの検査レポートの取得

Palo Alto Networks のサーバからファイルの検査レポートを xml 形式で取得します。

スクリプト：

```
curl -F 'hash=ハッシュ値
 -F 'format=xml'
 -H 'Authorization: Bearer  アクセストークン
 'https://wildfire.paloaltonetworks.com/publicapi/get/report'
```

凡例：

・*ハッシュ値*：ファイルのハッシュ値(MD5 または SHA256)を入力します。

・**format=xml**：レポートの出力形式を xml に指定します。

・*アクセストークン*：アクセストークンを入力します。

Palo Alto Networks のサーバから xml 形式の検査レポートの応答が返ります。

応答：

```
<wildfire>
～～中略～～
<report>
～～中略～～
</report>
～～中略～～
</wildfire>
```

以上