

お客様各位

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

PAN-OS に内蔵されているデフォルト証明書の有効期限切れについて

平素は Palo Alto Networks 製品ユーザーサポートをご利用くださり誠にありがとうございます。この度、Palo Alto Networks 社より、PAN-OS に内蔵されているデフォルト証明書の有効期限切れについてアナウンスされましたので、以下の通りご連絡いたします。

1. 概要

2023年12月31日に、PAN-OS におけるデフォルトのデバイス証明書とデフォルトのルート証明書の有効期限が切れます。これらの証明書は、PA シリーズと Panorama 間の User-ID 再配信サービス接続に使用されており、有効期限が更新されない場合、PA シリーズと Panorama は User-ID 再配信のためのマッピングとタグを共有できなくなります。

2. 対象のお客様

User-ID 再配信にデフォルトのデバイス証明書とルート証明書を使用する PA シリーズまたは Panorama をご利用しているお客様

【確認手順】

User-ID 再配信にカスタム証明書を使用している場合は、今回の更新の影響を受けません。User-ID 再配信のためのカスタム証明書は、PAN-OS 10.0 以降のバージョンでサポートされています。User-ID 再配信にデフォルトもしくはカスタム証明書のどちらを使用しているかについては、以下のコマンドを使用して赤枠の部分から確認ができます。

## 再配信エージェント側

```
admin@PA-XXXX> show redistribution service status

Redistribution info:

  Redistribution service:          up
  listening port:                 5007
  SSL config:                     Custom certificates
  back pressure is:              off
  number of clients:              2
```

## 再配信クライアント側

```
admin@PA-XXXX> show redistribution agent state uid-Agent

Agent: uid-Agent(vsys: vsys1) Host: 10.x.y.z(10.x.y.z):5007

  Status                : conn:idle
  Version               : 0x6
  SSL config:           : Custom certificates
  num of connection tried : 1
```

### 3. 恒久対策

1. または 2. のどちらかを実行する必要があります。

1. PAN-OS 10.0 以降のバージョンを利用している場合は、デフォルト証明書を使用する代わりに、User-ID 再配信用のカスタム証明書に切り替えることができます。User-ID 再配信用にカスタム証明書を構成する方法の詳細については、下記メーカドキュメントのステップ 8 と 9 を参照してください。

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/user-id/deploy-user-id-in-a-large-scale-network/redistribute-user-mappings-and-authentication-timestamps/configure-user-id-redistribution>

**重要**：サーバーとクライアントの安全な通信のために、再配信エージェントと再配信クライアントの両方でカスタム証明書に切り替える必要があります。

2. PA シリーズと Panorama の両方を次のいずれかのバージョンにアップグレードしてください。

修正が適用され、現在利用可能な PAN-OS の最小バージョンは次のとおりです。  
10.1.9-h3、10.2.4、11.0.1-h2

また、新しい証明書を備えた次の PAN-OS の更新バージョンもリリースされる予定です。

8.1 & 9.1

2023 年 12 月 31 日以降も証明書の機能を継続するには、再配布クライアントと再配布エージェントの両方をアップグレードする必要があります。

#### 4. Q&A

**再配布クライアントを先にアップグレードするか、再配布エージェントを先にアップグレードするとどうなりますか？**

2023 年 12 月 31 日までは、再配信エージェントと再配信クライアントの両方が異なるバージョンであっても通信を継続できます。すべての PA シリーズと Panorama を一度にアップグレードする必要はありませんが、2023 年 12 月 31 日までに両方のアップグレードを完了する必要があります。2023 年 12 月 31 日以降も引き続き通信を継続し、マッピングとタグを共有するためには、上記のいずれかのバージョンへ更新しておく必要があります。

**2023 年 12 月 31 日までに PA シリーズと Panorama を上記のバージョンのいずれかにアップグレードしない場合どうなりますか？**

2023 年 12 月 31 日までに PA シリーズと Panorama をアップグレードしない場合、PA シリーズと Panorama は User-ID の再配布のためのマッピングとタグの共有ができなくなります。

#### 5. その他特記事項

PAN-OS 8.1 は 2022 年 3 月 1 日に EoL 済みです。詳細につきましては下記メーカーサイトを参照してください。

Software End-of-Life (EoL)

<https://docs.paloaltonetworks.com/resources/eol>

以上