

2023年11月21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 (第3報)

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。
※太字箇所は追記もしくは変更箇所となっております。

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。有効期限が更新されない場合、Palo Alto Networks のクラウドサービスへの接続を失い、ネットワークトラフィックに影響を及ぼし、サービスの停止を引き起こす可能性があります。

※ルート証明書は 2023年12月31日 14:47:47 (GMT) に期限切れになります。

※デバイス証明書は 2023年12月31日 20:14:14 (GMT) に期限切れになります。

2 対象のお客様

PA シリーズまたは Panorama で下記のいずれかのサービスをご利用しているお客様

- (1) データの再配信 (User-ID、IP-tag、User-tag、GlobalProtect HIP、隔離リスト)
- (2) URL PAN-DB プライベートクラウド (M シリーズ)
- (3) WildFire プライベートクラウドアプライアンス (WF-500/WF-500-B)
- (4) WildFire パブリッククラウド / Advanced WildFire パブリッククラウド
- (5) URL フィルタリング / Advanced URL フィルタリング
- (6) DNS セキュリティ
- (7) ThreatVault
- (8) AutoFocus

3 恒久対策

使用しているサービスに応じて、以下のいずれかまたは両方で説明されているアクションを実行する必要があります。

表 1. 修正に対応している OS バージョン

現在の OS バージョン	修正 OS バージョン
8.1 系	8.1.21-h2、8.1.25-h1 以降
9.0 系	9.0.16-h5 以降
9.1 系	9.1.11-h4、9.1.12-h6、9.1.13-h4、9.1.14-h7、 9.1.16-h3、9.1.17 以降
10.0 系	10.0.8-h10、10.0.11-h3、10.0.12-h3 以降
10.1 系	10.1.3-h2、10.1.5-h3、10.1.6-h7、10.1.8-h6、 10.1.9-h3、10.1.10 以降
10.2 系	10.2.3-h9、10.2.4 以降
11.0 系	11.0.0-h1、11.0.1-h2、11.0.2 以降
11.1 系	11.1.0 以降

※すべての修正 OS バージョンは 2023 年 11 月 17 日までにリリースされました。

3.1 「2. 対象のお客様」の(1)を使用しているお客様は 2 つのアクション (①,②) のいずれかを実行する必要があります。

「2. 対象のお客様」の(2)、(3)のいずれか、もしくは複数を使用しているお客様は①のアクションを実行する必要があります。

① 影響を受ける PA シリーズ、M シリーズ、Panorama、WF-500/WF-500-B を上記の表 1 のいずれかへアップグレードする。

i. カスタム証明書がインストールされていない場合は、「2. 対象のお客様」の(1)、(2)、(3)を上記の表 1 のいずれかへアップグレードする必要があります。

ii. 現在、WF-500/WF-500-B と接続されている PA シリーズをアップグレードする必要があります。この問題に対処するための修正 OS バージョンにつきましては 2023 年 11 月 30 日までにリリースすることを目標としています。

※現在の最新修正 OS バージョン：11.0.3-h1 および 10.1.11-h3

- iii. 現在、URL PAN-DB プライベートクラウド (M シリーズ) と接続されている PA シリーズをアップグレードする必要があります。この問題に対処するための修正 OS バージョンにつきましては 2023 年 11 月 30 日までにリリースすることを目標としています。

※現在の最新修正 OS バージョン : 11.0.3-h1 および 10.1.11-h3

② 影響を受ける PA シリーズ、Panorama、にカスタム証明書を適用する。

- i. データの再配信 (User-ID、IP-tag、User-tag、GlobalProtect HIP、隔離リスト) :

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>

※ 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。

※ PA シリーズと Prisma Access の間でデータの再配信を使用する場合は、影響を受ける PA シリーズを修正 OS バージョンへアップグレードする必要があります。Prisma Access に変更を加える必要はありません。

- ii. URL PAN-DB プライベートクラウド (M シリーズ) :

カスタム証明書はオプションではありません。

- iii. WildFire プライベートクラウドアプライアンス (WF-500/WF-500-B) :

カスタム証明書はオプションではありません。

3.2 「2. 対象のお客様」の(4)、(5)、(6)、(7)、(8)のいずれか、もしくは複数を使用しているお客様は下記の3つのアクション(①,②,③)のいずれかを実行する必要があります。

- ① 影響を受けるPAシリーズと Panorama に 8776-8390 以降のコンテンツバージョンをインストールする。
 - i. コンテンツの自動更新が設定されている場合、この更新は自動的に行われます。
 - ii. コンテンツを手動で更新する場合は、上記のコンテンツバージョンに更新してください。
- ② 影響を受けるPAシリーズと Panorama を表1のいずれかへアップグレードする。
- ③ 影響を受けるPAシリーズと Panorama でデバイス証明書を有効にする。
 - i. PAN-OS 8.1、9.0、9.1 を使用しているPAシリーズもしくは Panorama がある場合、この方法はお勧めできません。
 - ii. PAN-OS 10.0.5、10.1.10、10.2.5、11.0.2 以降を実行しているPAシリーズと Panorama がある場合は、メーカードキュメントの手順に従ってデバイス証明書を有効にします。
<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/certificate-management/obtain-certificates/device-certificate>

4 よくある質問

PAN-OS 9.1 の EoL は 2023 年 12 月 12 日ですが、その日以降もメーカーサポートは継続されますか？

はい。2024 年 3 月 31 日までサポートは延長されます。

Software End-of-Life

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

Prisma Access は影響を受けますか？

いいえ。Prisma Access は影響を受けません。

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Palo Alto Networksのクラウドサービスへの接続を失い、ネットワークトラフィックに影響を及ぼし、サービスの停止を引き起こします。

PAシリーズとPanoramaをチェックして、2032年1月1日に期限切れになる新しいルート証明書があることを確認するにはどうすればよいですか？

PAシリーズが表1のPAN-OSバージョン以降のいずれかを実行している場合は、新しいルート証明書が配置されています。

PAシリーズとPanoramaがカスタム証明書で構成されているかどうかを確認するにはどうすればよいですか？

データの再配信（User-ID、IP-tag、User-tag、GlobalProtect HIP、隔離リスト）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。デフォルト証明書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
```

WildFire プライベートクラウド (WF-500 / WF-500-B) のカスタム証明書は、PAN-OS 8.1 以降で利用できます。

PAN-OS CLI からの証明書の検証：

```
dmin@sjc-bld-smk01-esx13-t2-pavm02> show wildfire status channel private

...

Secure Connection: Custom Trusted CA, Custom Client Certificate

...
```

再配信クライアントを先にアップグレードするか、再配信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するためには、表 1 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。

この証明書の有効期限は、PA シリーズと Windows User-ID / Terminal Server Agents 間の通信に影響しますか？

いいえ。PA シリーズは、Windows User-ID / Terminal Server Agents との通信に異なる証明書を使用します。したがって、PA シリーズと Windows User-ID / Terminal Server Agents 間の通信は影響を受けません。

当該事象の対策に必要な措置を講じているにもかかわらず、通知ポップアップが表示されるのはなぜですか？

メッセージは、バージョンや実行されたアクションに関係なく、すべてのデバイスにブロードキャストされ、ポップアップの左下にある「今後表示しない」というチェックボックスをクリックするまで表示され続けます。(このチェックボックスのチェックはシステムごとではなくユーザーごとに保存されるため、独自の資格情報を持つすべての管理者は、自分のアカウント用にそれぞれ選択する必要があります)
すべての是正措置が適切に講じられている場合は、通知を無視しても問題ありません。

5 その他特記事項

PAN-OS 8.1 /9.0 /10.0 は既に EoL を迎えています。

表 2. 各 OS バージョンの EoL 時期

OS バージョン	サポート終了日
8.1	2022 年 3 月 1 日
9.0	2022 年 3 月 1 日
10.0	2022 年 7 月 16 日

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

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

Hardware End-of-Life

<https://www.paloaltonetworks.com/services/support/end-of-life-announcements/hardware-end-of-life-dates>

以上