２０２５年１０月３１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 内蔵証明書の追加となる有効期限切れと新たな証明書管理プロセスついて (第 10 報)

平素は Palo Alto Networks 製品ユーザー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、PAN-OS 内蔵証明書の追加となる有効期限切れと新たな証明書管理プロセス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

   2026 年 1 月 1 日および同 2 月 11 日までに必要な対策へと内容を更新しました。
   更新前の情報につきましては、第 8 報をご確認ください。

2. 対象のお客様

   下記のいずれかをご利用されているお客様。

   (1) PA シリーズ（VM シリーズ含む）
   (2) PA シリーズを管理する Panorama（M シリーズ含む）
   (3) クラウド配信セキュリティサービス（CDSS）、WildFire/Advanced WildFire、DNS セキュリティ、URL/Advanced URL フィルタリング、M シリーズ上の URL PAN-DB プライベートクラウド
   (4) User-ID または Terminal Server Agents
   (5) WF-500 および WF-500-B WildFire アプライアンス

3. 各証明書の有効期限と影響範囲

証明書の有効期限が切れた際の影響範囲については下記の表 1 をご確認ください。

表 1 証明書の有効期限と影響

有効期限	証明書	影響を受ける製品 とサービス	更新後の 有効期限
2024 年 9 月 2 日	URL PAN-DB プライベートクラウド	PAN-DB プライベートクラウドとして機能する NGFW と M シリーズアプライアンス間の接続	2032 年 12 月 31 日 22:05:03 GMT
2026 年 2 月 11 日	クラウド配信セキュリティサービス（CDSS）のデバイス証明書 デバイス証明書の使用に関する詳細は FAQ6 を参照。	PA シリーズ(VM シリーズ含む)、Panorama、WF-500 / WF-500-B から次のいずれかの CDSS への接続 • WildFire/Advanced WildFire Public Cloud • URL/Advanced URL Filtering (PAN-DB) • DNS Security • AutoFocus 影響を受ける製品 ・PA シリーズ PA-200/220/220R PA-500 PA-800 シリーズ PA-3000 シリーズ PA-3200 シリーズ PA-5000 シリーズ PA-5200 シリーズ PA-7000 シリーズ VM シリーズおよび CN シリーズの詳細については FAQ8 を参照 ・Panorama（M シリーズ含む） ・WF-500 / WF-500-B	デバイス証明書は 90 日ごとに自動的に更新されます。

2024 年 11 月 18 日	User-ID と Terminal Server (TS)Agent の自己署名証明書	User-ID Agent と Terminal Server (TS)Agent 間の PA シリーズ（VM シリーズ含む）、Panorama、およびログコレクタへの接続 詳細については FAQ15 を参照。	User-ID Agent 2032 年 1 月 1 日 04:00:00 GMT Terminal Server Agent 2032 年 1 月 1 日 20:24:27 GMT
2026 年 1 月 1 日	WF-500 / WF-500-B 用 WildFire CA 証明書	WF-500 / WF-500-B への PA シリーズ（VM シリーズ含む）接続は影響を受けます。 詳細については FAQ15 を参照。	2032 年 12 月 31 日 06:53:22 GMT

※ 第 4 報までに記載されているオプション 1 を実施し、2024 年 4 月 7 日の Panorama 管理証明書の有効期限を修正した場合は、追加のアクションが必要になります。

※ 第 4 報までに記載されているオプション 2 を実施し、OS バージョンをアップグレードした場合は、デバイス証明書のオンボーディングプロセスが完了していることを確認する必要があります。（FAQ9）

※ 2025 年 8 月 5 日時点で、PA シリーズを管理する Panorama（M シリーズ含む）と PA シリーズ（VM シリーズ含む）のデバイス証明書の適用期限が 2025 年 11 月 11 日から 2026 年 2 月 11 日に延期されました。

4. 恒久対策

(1) M シリーズアプライアンス上の PAN-DB プライベートクラウド

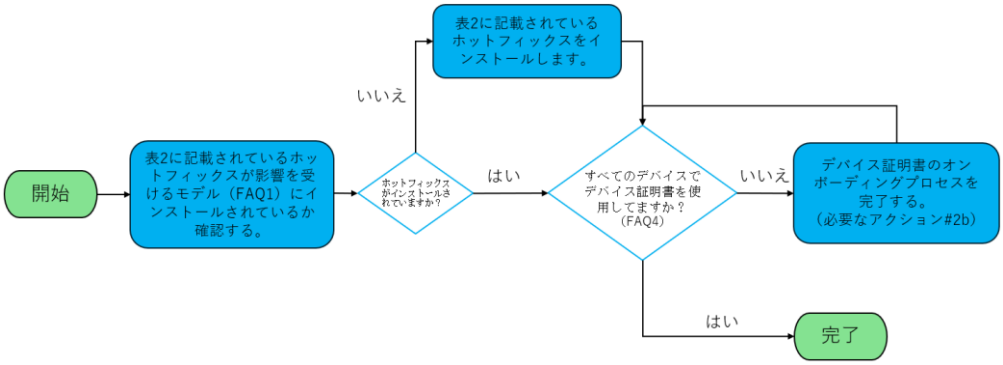
PAN-DB プライベートクラウド URL フィルタリング用に構成されている M シリーズアプライアンスに、表 2 のホットフィックスバージョンをインストールしてください。

※ 2024 年 9 月 2 日までに対応する必要があります。

(2) 次の CDSS のいずれかを使用する Panorama および PA シリーズ（VM シリーズ含む）：

WildFire/Advanced WildFire Public Cloud、URL/Advanced URL フィルタリング（PAN-DB）、DNS セキュリティ、AutoFocus

該当する場合は下記手順を実施してください。



a) OS バージョンのアップグレード：

表 1 に記載されているデバイスタイプの場合、影響を受けるすべての NGFW、Panorama、および M シリーズアプライアンスに、表 2 に記載されている対策バージョンがインストールされていることを確認します。

b) デバイス証明書のオンボーディングプロセスを完了：

各 PA シリーズ（VM シリーズ含む）のドキュメントに記載されている手順、または 1 つ以上 PA シリーズ（VM シリーズ含む）を管理している Panorama を使用する手順のいずれかを使用して、デバイス証明書のオンボーディングプロセスを完了させます。

PA シリーズ（VM シリーズ含む）

（https://docs.paloaltonetworks.com/pan-os/11-1/pan-os-admin/certificate-management/obtain-certificates/device-certificate）

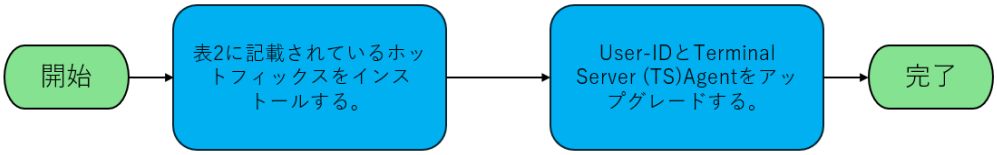
Panorama

（https://docs.paloaltonetworks.com/panorama/11-1/panorama-admin/manage-firewalls/install-the-device-certificate-for-managed-firewalls ）

c) デバイス証明書の使用状況を確認：
FAQ9 に記載されている手順を実施してください。

※ 全てのデバイスは、2026 年 2 月 11 日までに有効な証明書を取得する必要があります。

(3) User-ID と Terminal Server (TS)Agent の自己署名証明書



a) Agent を更新する前に表 2 に記載されている OS バージョンを PA シリーズ（VM シリーズ含む）および Panorama にインストールします。詳細については、FAQ12 を参照してください。

b) 更新された User-ID および Terminal Server (TS)Agent を適用します。

※ User-ID Agent と Terminal Server (TS)Agent が Prisma Access に直接接続する場合は、2024/9/15 以降に Agent をアップグレードしてください。この日までに Prisma Access は対策バージョンに更新されます。

※ PA シリーズ（VM シリーズ含む）を User-ID Agent として使用している場合は、PA シリーズ（VM シリーズ含む）を表 2 に記載されている対策バージョンにアップグレードしてください。

※ 2024 年 11 月 18 日まで対応する必要があります。

(4) WF-500 および WF-500-B WildFire アプライアンス
WF-500 / WF-500-B を表 2 に記載されている対策バージョンにアップグレードしてください。

※ 2026 年 1 月 1 日まで対応する必要があります。

証明書の有効期限の問題を軽減するには、現在の PA シリーズ（VM シリーズ含む）、Panorama および WF-500 / WF-500-B に対策 OS バージョンのホットフィックスバージョンを適用することをお勧めします。メジャーバージョンのアップグレードは、確立されたアップグレード手順に従って個別に計画する必要があります。

表 2 対策バージョン

OS バージョン	対策バージョン	GlobalProtect が有効になっている対策バージョン（FAQ17 参照）
8.1	8.1.21-h3、8.1.25-h3、8.1.26 以降	左記と同じ

9.0	9.0.16-h7、9.0.17-h5 以降	左記と同じ
9.1*	9.1.11-h5、9.1.12-h7、9.1.13-h5、9.1.14-h8、9.1.16-h5、9.1.17 以降	
10.0	10.0.8-h11、10.0.11-h4、10.0.12-h5 以降	
10.1	10.1.3-h3、10.1.4-h6、10.1.5-h4、10.1.6-h8、10.1.7-h1、10.1.8-h7、10.1.9-h8、10.1.10-h5、10.1.11-h5、10.1.12 以降	
10.2	10.2.0-h2、10.2.1-h1、10.2.2-h4、10.2.3-h12、10.2.4-h10、**10.2.5-h4**、10.2.6-h1、10.2.7-h3、10.2.8 以降	10.2.0-h3、10.2.1-h2、10.2.2-h5、10.2.3-h13、10.2.4-h16、10.2.5-h6、10.2.6-h3、10.2.7-h8、10.2.8-h3、10.2.9-h1 以降
11.0	11.0.0-h2、11.0.1-h3、11.0.2-h3、11.0.3-h3、11.0.4 以降	11.0.0-h3、11.0.1-h4、11.0.2-h4、11.0.3-h10、11.0.4-h1 以降
11.1	11.1.0-h2、11.1.1 以降	11.1.0-h3、11.1.1-h1、11.1.2-h3 以降
11.2	11.2.0 以降	11.2.0 以降
PAN-DB URL フィルタリング プライベートクラウド	8.1.26-h1、9.0.17-h5、9.1.17 -h1、10.0.12-h5、10.1.12、10.2.8、11.0.4、11.1.1 以降	適用不可
User-ID Agent／Terminal Server (TS)Agent	9.0.6、9.1.5、10.0.7、10.1.2、10.2.2、11.0.1 以降	
WF-500/B	8.1.26-h1、9.0.17-h5、9.1.17-h1、10.0.12-h5、10.1.12、10.2.8、11.0.4、11.1.1 以降	

※　9.1 系は 2024 年 6 月 30 日に End-of-Life(EoL)を迎えています。
詳細につきまして下記メーカサイトをご参照ください。
https://www.paloaltonetworks.jp/services/support/end-of-life-announcements

5. よくある質問（FAQ）

Q1) 弊社サポートサイトに掲載されている「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 1～4 報)」（以降、「2023 年 10～12 月のトピック」）に記載されている手順を実施しました。今回の事象は、PA シリーズ（VM シリーズ含む）、Panorama、ログコレクタに引き続き適用されますか？

はい。当トピックの「4. 恒久対策」を実行する必要があります。2023 年 10～12 月のトピックでは、特定の機能に使用されるデフォルト証明書とルート証明書がカバーされています。当トピックは、さまざまな範囲の製品とサービスを対象としています。

2023 年 10～12 月のトピックに記載されている対策 OS バージョンを適用した場合でも、より広範な証明書が対象となるため、影響を受ける製品およびサービスに表 2 に記載されている OS バージョンを適用する必要があります。2023 年 10～12 月のトピックの対応を行っていない場合は、それをスキップして当アドバイザリの表 2 に記載されている OS バージョンを適用してください。
当トピックに記載されているアクションを実行しない場合、表 1 に記載されているサービスが影響を受けます。

Q2) 2023 年 12 月に期限切れになる証明書の問題がアナウンスされた際に、今回の証明書の問題をアナウンスしなかったのはなぜですか？

Palo Alto Networks 社は、2023 年 11 月にアナウンスした時点で、当トピックに記載されている証明書の有効期限が近づいていることを認識していましたが、今回取り上げられている新しい証明書を含む OS バージョンをお客様にリリースする準備が整っていませんでした。

証明書によって重要な PAN-OS 機能が有効になります。当トピックで影響を受けるサービスには、この機能が動作するために必要な複数の証明書が含まれており、2023 年 10～12 月のトピックで取り上げられているサービスとは内容が異なります。

Q3) 2023 年 10～12 月のトピックの影響を受けず、何も措置を講じませんでした。今回の問題に対処する前に、2023 年 10～12 月のトピックに記載されている対策 OS バージョンを適用する必要がありますか？

2023 年 10～12 月のトピックに記載されている OS バージョンを適用していない場合は、それをスキップして、当トピックの表 2 に記載されている OS バージョンを適用してください。

Q4) Panorama で管理された Prisma Access を使用しています。これは Prisma Access のみを管理し、他の PA シリーズ（VM シリーズ含む）やデバイスは管理しません。この Panorama を修正する必要がありますか？

Panorama が Prisma Access や他の PA シリーズ（VM シリーズ含む）、Panorama、またはログコレクタではなく、Prisma Access のみを管理している場合は、2024 年 4 月 7 日の有効期限の影響を受けませんが、上記で推奨されているように、2024 年 11 月 18 日までに OS バージョンを更新する必要があります。

Q5) CDSS のデバイス証明書に関するセクションに自分の PA シリーズ（VM シリーズ含む）が表示されません。

この問題は、関連するデバイス証明書と、オンボーディングおよび更新のための安全な自動プロセスを含む、次の PA シリーズには影響しません。

PA-400 シリーズ、PA-1400 シリーズ、PA-3400 シリーズ、PA-5400 シリーズ、PA-5450、PA-7500

次のものも影響を受けません。

Prisma Access、AWS 上のクラウド NGFW、Azure 上のクラウド NGFW、GCP Cloud IDS とファイアウォールプラス、Oracle ネットワークファイアウォール

影響を受けるモデルは次のとおりです。

PA-200/220/220R、PA-500、PA-800 シリーズ、PA-3000 シリーズ、PA-3200 シリーズ、PA-5000 シリーズ、PA-5200 シリーズ、PA-7000 シリーズ、VM シリーズおよび CN シリーズ

Q6) CDSS のデバイス証明書に移行するのは何故ですか？

特定の CDSS サブスクリプションのデバイス証明書は、PA シリーズ（VM シリーズ含む）が表 1 に記載されている CDSS にアクセスできるように、90 日ごとに証明書を自動的に更新します。この仕組みは数年前から導入されており、表 2 に記載されている対策バージョンにより、証明書の更新が失敗した場合のエラー処理が大幅に改善されています。

2026 年 2 月 11 日以降、デバイス証明書は、PA シリーズ（VM シリーズ含む）と Panorama が表 1 の CDSS サブスクリプションにアクセスするために使用する唯一の仕組みになります。この日付までに、「4. 恒久対策」に記載されている手順を実施してください。対策バージョンを適用せず、CDSS のデバイス証明書のオンボーディングを完了しなかった場合、DNS セキュリティ、URL フィルタリング、WildFire などの

セキュリティサービスに関連付けられたセキュリティルールが正しく機能しなくなり、クラウドセキュリティサービスが検出や判定を提供出来なくなります。

Q7) 必要な手順を完了した後の新しい有効期限はいつですか？

表 3 対策 OS バージョン適用後の証明書の有効期限

証明書	新しい有効期限
Panorama 管理	2033 年 11 月 19 日 23:27:22 GMT
URL PAN-DB プライベートクラウド	2032 年 12 月 31 日 22:05:03 GMT
User-ID と Terminal Server (TS) Agent の自己署名証明書	User-ID Agent 2032 年 1 月 1 日 04:00:00 GMT Terminal Server Agent 2032 年 1 月 1 日 20:24:27 GMT
クラウド配信セキュリティサービス（CDSS）のデバイス証明書	デバイス証明書の有効期間は 90 日間です。PA シリーズ (VM シリーズ含む) は、証明書の有効期限が切れる 15 日前にデバイス証明書を再インストールします。
WF CA 証明書	2032 年 12 月 31 日 06:53:22 GMT

Q8) VM シリーズおよび CN シリーズで CDSS のデバイス証明書を有効にするには何が必要ですか？

CDSS のデバイス証明書を有効にするには、次の OS バージョンを使用します。VM シリーズの展開に使用されるライセンスタイプに基づいて、以下の手順に従ってください。

表 4 VM シリーズで更新される OS バージョン

VM シリーズの OS バージョン
10.1.12 以降、10.2.9-h1 以降、11.0.4-h1 以降、11.1.2-h3 以降、**11.1.3 以降**、11.2.0 以降

BYOL、ELA、およびフレックスライセンス

Bring Your Own License (BYOL)、ELA、または Flex（ソフトウェアクレジット）などのアクティブ化するライセンスを使用してデプロイされた VM-Series NGFW インスタンスは、次の手順に従う必要があります。これは、プライベートクラウド (VMware ESXi および NSX、Hyper-V、OpenStack）およびパブリッククラウド上の VM シリーズに適用されます。

(1) VM シリーズをカスタマーサポートポータル（CSP）に登録します。
(2) VM-Series インスタンスを、上記の表 2 に記載されている OS バージョンに更新します。
(3) メーカドキュメントの手順に従って、PIN または OTP をファイアウォールに追加し、デバイス証明書を取得します。

従量課金制（PAYG）ライセンス
パブリッククラウドマーケットプレイス（AWS、Azure、GCP）から従量課金制（PAYG）としてデプロイされた VM シリーズインスタンスをオンボードするには 2 つの方法があります。

オプション 1：
既存の VM-Series PAYG インスタンスをオンボードする

(1) VM-Series ファイアウォールをカスタマーサポートポータル（CSP）に登録します。
(2) VM-Series インスタンスを、表 2 に記載されている OS バージョンに更新します。
(3) メーカドキュメントの手順に従って、PIN または OTP をファイアウォールに追加し、デバイス証明書を取得します。
（https://docs.paloaltonetworks.com/vm-series/10-1/vm-series-deployment/license-the-vm-series-firewall/vm-series-models/install-a-device-certificate-on-the-vm-series-firewall ）

オプション 2：
表 4 に記載されている OS バージョンのいずれかを使用して VM-Series インスタンスを再デプロイします。更新した OS バージョンでは、デバイス証明書を取得するために追加の手順（ファイアウォールに PIN または OTP を追加する）は必要ありません。
※ オプション 2 は、WildFire、URL フィルタリング、および DNS（非アドバンストバージョン）のサブスクリプションを使用している顧客のみが可能です。

CN シリーズ：
CN シリーズにデバイス証明書をインストールする手順については、メーカドキュメントの手順を参照してください。
（https://docs.paloaltonetworks.com/cn-series/getting-started/cn-series-deployment-prereq/install-a-device-certificate-on-the-cn-series-firewall-updated）

Q9) 必要なアクションを完了した後、証明書の有効期限を確認するにはどうすればよいですか？

CDSS のデバイス証明書

CDSS のデバイス証明書の有効期間は 90 日間で、有効期限が切れる 15 日前に自動的に再インストールされます。これは、ホットフィックスを適用し、オンボーディングを完了した後で、次の手順を使用して確認できます。

（https://docs.paloaltonetworks.com/pan-os/11-1/pan-os-admin/certificate-management/obtain-certificates/device-certificate ）

(1) 管理対象デバイス用の Panorama から Panorama にログインし、[Panorama] > [管理対象デバイス] > [概要] > [デバイス証明書（列）] に移動します。

(2) 登録後の証明書のステータスを示すメーカドキュメントのステップ 8 を参照してください。

（https://docs.paloaltonetworks.com/panorama/11-1/panorama-admin/manage-firewalls/install-the-device-certificate-for-managed-firewalls/install-the-device-certificate-for-a-managed-firewall）

PA シリーズ（VM シリーズ含む）

次の CLI コマンドを実行して確認します。

```
> show device-certificate status
Device Certificate information:
        Current device certificate status: Valid
        Not valid before: 2023/11/23 05:22:46 PST
        Not valid after: 2024/02/21 05:22:45 PST
        Last fetched timestamp: 2023/11/23 05:32:46 PST
        Last fetched status: success
        Last fetched info: Successfully fetched Device Certificate
```

残りの証明書、User-ID および Terminal Server (TS) Agent の自己署名証明書、WF-500 / WF-500-B、および URL PAN-DB プライベートクラウド（M シリーズ）

これらの証明書については、有効期限を直接確認する方法はありません。必要な手順が完了すると、影響を受ける製品とサービスは新しい証明書を自動的に使用して安全な通信を確立します。

Q10）当ドキュメントに記載されている恒久対策を実施したあと他に考慮する必要がある手順などはありますか？
これらの手順を完了すると、2026 年 12 月 31 日以降まで証明書の更新は必要なくなります。

中期的には、2025 年 3 月 1 日以降にリリースされる PAN-OS および Panorama のすべてのメジャーリリース、マイナーリリース、およびメンテナンスリリースには、最低 5 年間の延長が含まれた埋め込み証明書がついています。埋め込み証明書は、対策 OS バージョンの予定されたサポート終了日を過ぎても有効です。このアプローチにより、ネットワークの中断が防止され、今後手動で証明書を更新する必要がなくなります。

長期的には新しい包括的な証明書管理プロセスが実装される予定です。このプロセスにより、証明書はコンテンツ更新および通常の OS アップデートの一部として継続的に更新されます。

Q11）脅威防御または高度な脅威防御が CDSS のデバイス証明書の影響を受けないのはなぜですか？
Threat Prevention と Advanced Threat Prevention の接続は個別に確立されており、他の CDSS で使用されるデバイス証明書には依存しません。

Q12) PA シリーズ（VM シリーズ含む）に対策バージョンを適用した後、User-ID および Terminal Server (TS) Agent を更新する必要があるのはなぜですか？
PA シリーズ（VM シリーズ含む）に対策 OS バージョンを適用すると、User-ID Agent および Terminal Server (TS) Agent の両方のバージョン（有効期限が 2024 年 11 月 18 日の古い証明書と、有効期限の長い新しい証明書）から接続が受け入れられるようになります。これにより、User-ID ベースのポリシー機能への影響を最小限に抑えて Agent を更新できるようになります。

最初に Agent を更新すると、Agent は有効期限の長い新しい証明書の使用を開始しますが、この証明書は PA シリーズ（VM シリーズ含む）には認識されないため、PA シリーズ（VM シリーズ含む）は User-ID の更新を受信しなくなります。したがって、PA シリーズ（VM シリーズ含む）へ対策 OS バージョンを適用するまでは、User-ID ベースのセキュリティポリシーが中断されてしまいます。

Q13) 今回参照したメーカドキュメントは他言語で利用できますか？
複数の言語に翻訳されたメーカドキュメントは、下記の場所から入手できます。
（https://docs.paloaltonetworks.com/translated）

Q14) 私のデバイス（PA シリーズ（VM シリーズ含む）、Panorama、M シリーズ）はサポート対象外ですが、どのような選択肢がありますか？
PA シリーズ（VM シリーズ含む）、Panorama、または M シリーズがサポート対象外で、WebUI から対策バージョンをダウンロードできない場合は、カスタマーサポートポータル（CSP） > Updates > Urgent Updates for Unsupported Devices から対策バージョンと User-ID および Terminal Server (TS) Agent をダウンロードできます。ログインしてダウンロードするには、CSP アカウントを持っている必要があります。

Q15) 「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」に記載されている User-ID および WF-500 / WF-500-B 証明書の問題は解決されましたか？
「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」には、PA シリーズ（VM シリーズ含む）または Panorama におけるデータの再配信（User-ID、IP タグ、User-tag、GlobalProtect HIP、隔離リスト）に使用されるデフォルト証明書とルート証明書の有効期限切れの恒久対策について記載されています。

このトピックは User-ID および Terminal Server (TS) Agent と PA シリーズ（VM シリーズ含む）間の安全な通信に関するもので、カスタム証明書を使用しても今回の問題は軽減できません。カスタム証明書は、PA シリーズ（VM シリーズ含む）間の通信や Panorama との通信を行うためのオプションとして引き続き使用できます。

WF-500 / WF-500-B は、PA シリーズ（VM シリーズ含む）と WildFire アプライアンスの CDSS パブリッククラウドへの安全な接続に関連していました。恒久対策への対応が完了している場合は、2026 年 1 月 1 日以降も利用できます。

Q16) CDSS のデバイス証明書の代わりにカスタム証明書を使用できますか？
カスタム証明書は、組み込みのデバイス証明書および関連する更新メカニズムを置き換えるために使用することはできません。

Q17) GlobalProtect が有効になっている PA シリーズ（VM シリーズ含む）の対策バージョンが異なるのはなぜですか？

GlobalProtect が有効になっている PA シリーズ（VM シリーズ含む）では、表 2 に記載されている対策バージョンより高いバージョンを使用する必要があります。これは CVE-2024-3400 から機器を保護するためです。

CVE-2024-3400 PAN-OS: Arbitrary File Creation Leads to OS Command Injection Vulnerability in GlobalProtect
（https://security.paloaltonetworks.com/CVE-2024-3400）

Q18) 対策バージョンで提供される証明書を使用する代わりに、User-ID および Terminal Server (TS) Agent と PA シリーズ（VM シリーズ含む）間でカスタム証明書を使用できますか？

はい、User-ID および Terminal Server (TS) Agent と PA シリーズ（VM シリーズ含む）間の安全な通信のためにカスタム証明書を使用できます。

注意点として、PA シリーズ（VM シリーズ含む）に User-IP マッピングを提供するために Windows ベースの User-ID Agent と Terminal Server (TS) Agent の両方を展開している場合、設計上の制限によりカスタム証明書が機能しません。そのため、PA シリーズ（VM シリーズ含む）を表 2 に示されている対策 OS バージョンにアップグレードすることをおすすめします。

Q19) User-ID および Terminal Server (TS) Agent の自己署名証明書のステータスを表示できる自動化ツールはありますか？

オープンソースの User-ID チェックツールが GitHub で利用可能です。これを使用することで、全てのデバイスと User-ID および Terminal Server (TS) Agent で実行されている OS バージョンと Agent バージョンを判別できます。

このツールは、2024 年 11 月 18 日に有効期限を迎える証明書の影響を受けない OS バージョンと Agent バージョンで、お客様のデバイスを確実に動作させることを目的としています。このツールは「現状のまま」リリースされ、保証やサポートはありません。

User-ID チェックツール
https://github.com/PaloAltoNetworks/userid-check

Q20) HA 構成を組んでいる PA シリーズ（VM シリーズ含む）のデバイス証明書更新に関して

■対象のお客様

- Active-Passive を備えた HA 構成
- Passive 機にサービスルートが設定されておらず、MGT ポートを介してインターネット接続する場合

※　下記 PA シリーズは影響を受けません。
PA-400 シリーズ、PA-1400 シリーズ、PA-3400 シリーズ、PA-5400 シリーズ、PA-5450、PA-7500

■概要

サービスルートがデータポートを使用するように HA 構成を組んでいる場合、Passive 機のデータポートはシャットダウンしているため、インターネットに接続されていません。そのため、デバイス証明書の自動更新が Passive 機では行なわれません。この状況でフェイルオーバーが発生すると、Passive 機 は Active に切り替わりますが、有効なデバイス証明書を持たない状態となります。この状態から回復するには、デバイス証明書を手動で再登録する必要があります。

なお、サービスルートが設定されていない場合は、Passive 機は MGT ポートを介してインターネットに接続するため、デバイス証明書の更新プロセスには影響しません。

※　本問題は、Active-Passive を備えた HA 構成のみ影響します。Active- Active を備えた HA 構成は、サービスルートを設定しているか否かに関わらず影響を受けません。

※　デバイスが本問題の影響を受けるか否かを確認するには、「Palo Alto Networks」サービスおよび「DNS」サービスのサービスルート構成を検証してください。

残りのすべての PA シリーズ（VM シリーズ）は影響を受けます。そのため、後述の回避策または恒久対策が必要です。

■回避策

以下の手順でデバイス証明書を再登録します。

(1)　手動フェイルオーバーを実行して、サービスルートを持つ影響を受ける Passive 機（デバイス証明書の有効期限が切れている）が Active 状態であることを確認します。

手動フェイルオーバー
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/high-availability/set-up-activepassive-ha/verify-failover

(2) PA シリーズ（VM シリーズ含む）または、Panorama を使用してデバイス証明書の登録が行われていないデバイスの再登録を行います。
※ WildFire クラウドサービスへの接続は、表 2 対策バージョンを適用することで行えます。
PA シリーズ（VM シリーズ含む）
https://docs.paloaltonetworks.com/pan-os/11-1/pan-os-admin/certificate-management/obtain-certificates/device-certificate

Panorama
https://docs.paloaltonetworks.com/panorama/11-1/panorama-admin/manage-firewalls/install-the-device-certificate-for-managed-firewalls/install-the-device-certificate-for-a-managed-firewall

■恒久対策
本問題の対策 OS バージョンは以下の通りです。

表 5 対策 OS バージョンのリリース日

対策 OS バージョン	リリース日
12.1.3	2025 年 9 月 25 日※2
11.2.10	2025 年 10 月 31 日※1
11.1.12	2025 年 10 月 9 日※2
10.2.17	2025 年 10 月 3 日※2
10.1.14-hf	2025 年 10 月 31 日※1

※1 メーカリリース予定日
※2 メーカリリース確認済み
※3 10.1.x の標準サポートは終了しており、現在限定サポートのみとなっております。

Q21) 他の PA シリーズ（VM シリーズ含む）からのトラフィックを保護する PA シリーズ（VM シリーズ含む）がある場合、デバイス証明書の更新を正常に行うには何が必要ですか？

本脆弱性の影響を受ける CDSS サブスクリプションを使用している PA シリーズ（VM シリーズ含む）からの管理トラフィックをパススルートラフィックとして検査している PA シリーズ（VM シリーズ含む）の証明書を更新する方法につきましては、下記をご参照ください。

※　参照するには CSP アカウントを所有している必要があります。

Device Certificate Renewal for NGFW Devices secured via perimeter firewall
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA1Ki000000XZKWKA4

Q22) CDSS のデバイス証明書の有効期限が延長されたのはなぜですか？

お客様に対策手順を実行していただくために、デバイス証明書の有効期限を 2024 年 11 月 11 日から 2026 年 2 月 11 日まで延長されました。

Q23) Palo Alto Networks 社が、デバイス証明書の有効期限を延長し続けることはできないのですか？

他の証明書関連の問題とは異なり、今回の脆弱性対策は単なる証明書の更新という訳ではありません。対策手順を実施することにより、将来起こりうる問題の発生確率を低減することを目的としています。

Q24) WF-500 / WF-500-B をアップグレードしないとどうなりますか？

PA シリーズ（VM シリーズ含む）と WF-500 / WF-500-B 間の通信に失敗し、PA シリーズ(VM シリーズ含む)によって検査されたファイルの判定を取得できなくなります。さらに、WF-500 / WF-500-B は Panorama による管理ができなくなります。

Q25) WF-500 / WF-500-B のデバイス証明書のステータスを確認するにはどうすればよいですか？

デバイス証明書のステータスを直接確認する方法はありません。

WF-500 / WF-500-B に対策 OS を適用することで、新しいデバイス証明書がインストールされます。

以上