２０２４年1月１９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

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。

1. 概要

2024 年 4 月 7 日以降に順次各種製品またはセキュリティサービスで使用されている証明書の有効期限を迎えます。証明書の有効期限が更新されなかった場合、これらの証明書を使用する機能が停止します。

※下記をご対応頂いたお客様においても追加の措置が必要となります。

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 4 報）
https://csps.hitachi-solutions.co.jp/paloalto/news/information20231208.pdf

中期的には 2025 年 3 月 1 日以降にリリースされる PAN-OS には最低 5 年間の証明書期限延長が含まれます。
長期的には新たな包括的な証明書管理プロセスを実装予定としており、このプロセスによって証明書が動的コンテンツ更新および通常のソフトウェア更新の一部として継続的に更新されます。

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) WildFire、DNS セキュリティ、URL フィルタリング、URL PAN-DB プライベートクラウドなどのセキュリティサービス
(4) User-ID または Terminal Server Agents

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 4 月 7 日	PA シリーズ（VM シリーズ含む）／ Panorama 管理	PA シリーズ(VM シリーズ含む)、Panorama、PAN-DB プライベートクラウドモードの M シリーズアプライアンス、ログコレクタ、または WildFire アプライアンス（WF500/B）から Panorama への接続	2033 年 11 月 19 日 23:27:22 GMT
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
2024 年 11 月 18 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	Panorama、PA シリーズ（VM シリーズ含む）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 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	デバイス証明書は 90 日ごとに自動的に更新されます。

		VM シリーズおよび CN シリーズの場合（以下の「**VM 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？**」の FAQ を参照）	
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	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 CA 証明書	WF-500 への PA シリーズ（VM シリーズ含む）接続は影響を受けます	2032 年 12 月 31 日 06:53:22 GMT

証明書の有効期限が切れると、表 1 の「影響を受ける製品とサービス」の列に記載されている接続に影響が生じます。これは、それらの製品やサービスが提供する一部の機能の喪失につながります。

4. 恒久対策

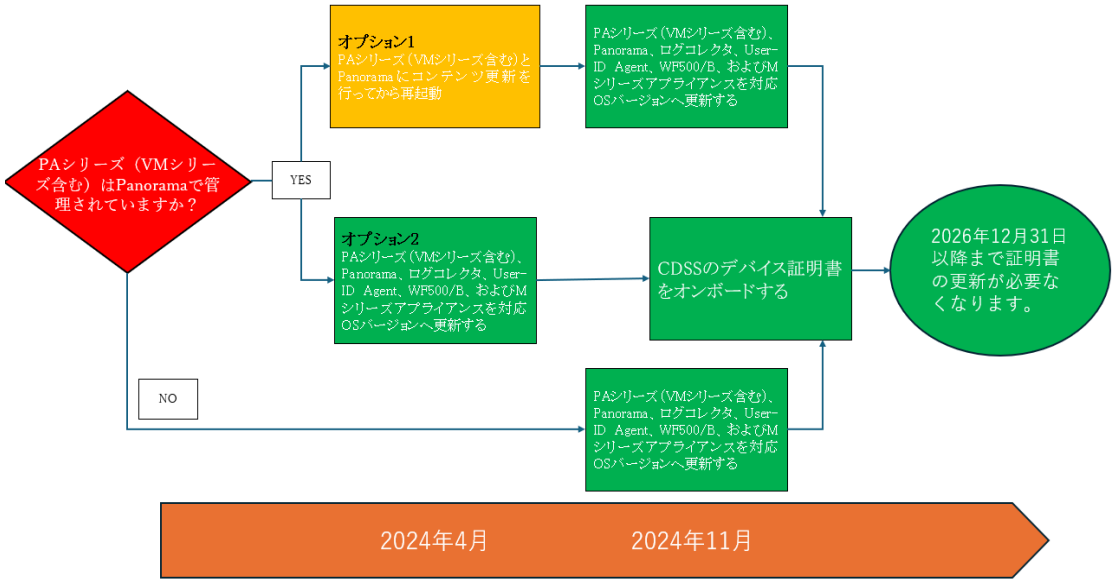
証明書を更新して証明書管理プロセスに登録するには、次のアクションを実行する必要があります。

(1) Panorama で管理されている PA シリーズ（VM シリーズ含む）がある場合

オプション 1 を 2024 年 4 月までに実施し、次にオプション 2 を 2024 年 11 月までに実施する。または、2024 年 4 月までにオプション 2 を実施する。

(2) その他の場合

2024 年 11 月までにオプション 2 を実施する。



オプション 1：PA シリーズ（VM シリーズ含む）、Panorama 管理証明書のみを更新する

2024 年 4 月 7 日より前に表 2 の OS バージョンをインストールできず、PA シリーズ（VM シリーズ含む）／Panorama 管理証明書のみを更新する場合にのみ適用されます。他のすべての証明書の対応する有効期限が切れる前に、オプション 2 を適用する必要があります。

(1) PA シリーズ（VM シリーズ含む）、Panorama、ログコレクタにコンテンツ更新（8795-8489 以降）をインストールします。WF500/B の場合は、コンテンツ更新（2438-2654 以降）をインストールします。

(2) PA シリーズ（VM シリーズ含む）、Panorama、WF500/B、およびログコレクタを再起動します。

※　更新された証明書が含まれていない PAN-OS ソフトウェアイメージをダウングレードまたはアップグレードすると、PA シリーズ（VM シリーズ含む）／Panorama 管理証明書は上書きされ、コンテンツ更新を再適用する必要があります。更新された証明書を含む OS バージョンのリストについては表 2 を参照してください。

※　カスタム証明書が PA シリーズ（VM シリーズ含む）、Panorama、ログコレクタにインストールされている場合、コンテンツ更新をインストールする必要はありません。

オプション 2：PA シリーズ（VM シリーズ含む）、Panorama、ログコレクタ、User-ID Agent、WF500/B、および M シリーズアプライアンスを更新する

(1)　表 2 に記載されている OS バージョンを適用します。

※　VM シリーズおよび CN シリーズについては、以下の FAQ を参照してください。

※　カスタム証明書がすべての PA シリーズ（VM シリーズ含む）、Panorama、ログコレクタにインストールされている場合、表 2 に記載されている PAN-OS をインストールする必要はありません。

(2)　影響を受けるすべてのデバイスについては各メーカドキュメントの CDSS オンボーディングのデバイス証明書の手順を参照してください。

A)　Panorama
（https://docs.paloaltonetworks.com/panorama/10-1/panorama-admin/set-up-panorama/install-the-panorama-device-certificate）

B)　ログコレクタ
（https://docs.paloaltonetworks.com/panorama/10-1/panorama-admin/set-up-panorama/install-the-device-certificate-for-a-dedicated-log-collector）

C)　PA シリーズ（VM シリーズ含む）
スタンドアロン PA シリーズ（VM シリーズ含む）の場合
（https://docs.paloaltonetworks.com/pan-os/11-1/pan-os-admin/certificate-management/obtain-certificates/device-certificate）
Panorama 管理の PA シリーズ（VM シリーズ含む）の場合
（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）

(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、FAQ 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。

※ 既に PA シリーズ（VM シリーズ含む）および Panorama にデバイス証明書をインストールしている場合は、表 2 に記載されている OS バージョンをインストールするだけで問題ありません。

※ この修正プログラムは、90 日ごとにデバイス証明書の自動更新を行います。以下の FAQ の確認手順を使用して、PA シリーズ（VM シリーズ含む）および Panorama のデバイス証明書のオンボーディングステータスを確認できます。

※ CDSS のデバイス証明書は、2024 年 11 月 18 日にアクティブ化されます。それまでに、すべてのデバイスに有効な証明書が必要です。

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）および Panorama 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
8.1	8.1.21-h3、8.1.25-h3、8.1.26（将来のリリースを含む）
9.0	9.0.16-h7、9.0.17-h5
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（将来のリリースを含む）
10.0	10.0.8-h11、10.0.11-h4、10.0.12-h5
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-h4、10.1.12*（将来のリリースを含む）
10.2	10.2.0-h2、10.2.1-h1、10.2.2-h4、10.2.3-h11、10.2.4-h10、10.2.6-h1、10.2.7-h3、10.2.8*（将来のリリースを含む）
11.0	11.0.0-h2、11.0.1-h3、11.0.2-h3、11.0.3-h3*、11.0.4*（将来のリリースを含む）
11.1	11.1.0-h2、11.1.1 (将来のリリースを含む)
PAN-DB URL フィルタリング プライベートク	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（将来のリリースを含む）

ラウド	
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
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

※　Panorama 管理証明書の有効期限が切れる前にリリースされます。

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」（以降、「2023 年 10 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 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 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 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 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 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 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 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）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

Q7) VM 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	リリース予定日
10.1.12、10.2.8	2024 年 1 月末
11.0.4、11.1.2	2024 年 2 月末

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。

Q8) **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？**

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？

以下は、Panorama 管理証明書と CDSS のデバイス証明書の確認に使用できる手順です。

Panorama 管理証明書

```
> debug management-server panorama-root-ca-info


# Shows expiration date of Panorama management certificate
 “notAfter=Nov 11 23:35:36 2033 GMT”
```

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/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 OS 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）

以上