

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

Strata Logging Service の mTLS ログ転送向け CA 証明書更新のご案内

平素は Palo Alto Networks 製品ユーザサポートをご利用くださいますようお願いいたします。  
この度、Palo Alto Networks 社より Strata Logging Service の mTLS ログ転送に使用される CA 証明書の更新に関するご案内が発表されました。

1. 概要

相互 TLS 認証（以下、mTLS）を利用して外部のログ転送先へ接続する際に、Strata Logging Service（以下、SLS）が使用するクライアント証明書の発行元 CA が既存の GoDaddy 証明書チェーンから DigiCert 証明書チェーンへ移行されます。

この変更に伴い、SLS から mTLS を利用して外部のログ転送先へログを送信している環境では、受信側エンドポイントの信頼ストアへ、新たに DigiCert のルート CA 証明書および中間 CA 証明書を追加する必要があります。

必要な設定を行わない場合、受信側エンドポイントが SLS との mTLS 接続を拒否し、ログ転送が中断する可能性があります。

該当するお客様におかれましては、受信側エンドポイントに DigiCert のルート CA 証明書および中間 CA 証明書の追加をご検討ください。

2. 影響を受けるお客様

以下の両方の条件に該当するお客様が対象です。

- ・ SLS から外部 Syslog サーバーまたは HTTPS サーバーへログ転送を実施している。
- ・ 受信側エンドポイントで mTLS によるクライアント証明書認証を有効化している。

3. お客様に実施いただきたい対応

本件の対象となるお客様は、以下の内容をご確認のうえ、必要に応じてご対応ください。

(1). 対応期限

対応期限を以下に示します。対象となるお客様は速やかな対応をご検討ください。

表 1 対応期限

| 地域                | 対応期限                         |
|-------------------|------------------------------|
| ブラジル及びオーストラリア     | 即時（対応期限経過）                   |
| FedRAMP High 及び中国 | 対応不要                         |
| その他影響を受ける全ての地域    | 2026 年 10 月 14 日 PDT（対応期限経過） |

## (2). 対応手順

受信側エンドポイントで、以下の対応をご検討ください。

- ① **DigiCert** の証明書公開サイト(※)から、受信側エンドポイントでサポートされている **PEM** 形式または **DER/CRT** 形式を選択し、以下の **CA** 証明書をダウンロードしてください。
- ②

表 2 対象の CA 証明書

| CA 証明書     | 名称                                         |
|------------|--------------------------------------------|
| ルート CA 証明書 | DigiCert Global Root G2                    |
| 中間 CA 証明書  | DigiCert Global G2 TLS RSA SHA256 2020 CA1 |

(※)DigiCert Trusted Root Authority Certificates

<https://knowledge.digicert.com/general-information/digicert-trusted-root-authority-certificates>

- ② ログ受信アプリケーションがクライアント証明書認証に使用する信頼ストアへ、上記のルート CA 証明書および中間 CA 証明書を追加してください。アプリケーションによっては、CA バンドルへの追加が必要な場合があります。
- ③ 設定反映のため、必要に応じてログ受信サービスまたは関連アプリケーションを再起動してください。なお、証明書チェーンの切り替え完了まで、既存の **GoDaddy** 証明書チェーンを削除せず、**GoDaddy** および **DigiCert** の両方の証明書チェーンを信頼した状態を維持してください。
- ④ ログ転送および mTLS 接続が正常に継続していることをご確認ください。
- ⑤ **Palo Alto Networks** 社による証明書チェーンの切り替え完了後、**SLS** との通信で **DigiCert** 証明書チェーンが利用されていることを確認できたら、不要となった **GoDaddy** 証明書チェーンを削除してください。

## 4. その他特記事項

**Palo Alto Networks** 社は、**SLS** のクライアント証明書について、まず、既存の **GoDaddy** 証明書チェーンから **DigiCert** 証明書チェーンへ移行しますが、将来的には専用の **Palo Alto Networks** ルート CA から発行されるクライアント証明書への移行を予定しています。

詳細な証明書パッケージ、ガイダンス、および移行スケジュールは、十分な準備期間を確保したうえで別途ご案内する予定です。

本件の詳細や最新情報については、下記のメーカーコミュニティページも併せてご参照ください。

<https://live.paloaltonetworks.com/t5/tkb/articleprintpage/tkb-id/SupportAnnouncements/article-id/422>

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いたしかねますことをあらかじめご了承ください。

以上