

2020年7月3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

### SAML 認証がバイパスされる脆弱性(CVE-2020-2021)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。  
ありがとうございます。

この度、Palo Alto Networks 社より SAML 認証にて認証のバイパスが可能となる重要な脆弱性が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. 脆弱性の概要

PAN-OS の Security Assertion Markup Language (SAML) 認証にて認証のバイパスが可能となる脆弱性が存在しております。

本脆弱性が悪用された場合、認証されていないネットワークベースの攻撃者が保護されたリソースにアクセス可能となる可能性がございます。

なお、本脆弱性は「Validate Identity Provider Certificate」オプションが有効（チェックされている）の場合は影響ございません。

#### 2. 対象のお客様

PAN-OS 8.1.15 より前、9.0.9 より前、9.1.3 より前をご利用のお客様。

※PAN-OS 8.0(EoL)は全てのバージョンが対象となります。

※PAN-OS 7.1 は影響ございません。

※SAML 認証をご利用されていない場合はこの脆弱性の影響がございません。

#### 3. 恒久対策

PAN-OS 8.1.15 以降、9.0.9 以降、9.1.3 以降へのバージョンアップをご検討ください。

※PAN-OS 8.0 は 2019 年 10 月 31 日をもってメーカサポートが終了しております。

そのため修正済みバージョンのリリースは行われません。

なお、修正済みバージョンにアップグレードする前に、SAML Identity Provider の署名証明書が「Identity Provider Certificate」として構成されていることを確認することが、安全な SAML 認証構成として重要だとメーカより推奨されております。

詳細は下記の Palo Alto Networks 社サイトをご参照ください。

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u0000008UXK>

#### 4. 運用回避策

本脆弱性は、別の認証方法を使用して SAML 認証を無効とすることにより完全に回避することができます。

恒久対策を実施するまでの間は下記の回避策(A)と(B)の両方を適用することで、本脆弱性を回避することができます。

A) 「Identity Provider Certificate」が設定されていることをご確認ください。

B) ID プロバイダ(IdP)証明書が証明機関(CA)署名の証明書である場合、「Validate Identity Provider Certificate」オプションが SAML Identity Provider Server Profile で有効になっていることをご確認ください。

多くの一般的な IdP は、デフォルトで自己署名 IdP 証明書を生成するため、当該オプションを有効にすることはできません。CA が署名した証明書を使用するには追加手順が必要となる場合があります。IdP で CA 発行の証明書を設定する方法は下記 Palo Alto Networks 社サイトをご参照ください。

・ Identity Provider Configuration for SAML

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u0000008UXP>

以上