２０２２年9月１６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

Customer Support Portal サイトへのログインに多要素認証が必須となるお知らせ
（9/16 改訂版）

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、Customer Support Portal サイト(以降は CSP サイト)へのログインに多要素認証が必須とされておりますので、以下の通りご連絡いたします。

1. 概要

2022 年 5 月 31 日 午前 8 時(PDT)より CSP サイトへのログインに多要素認証が必須となっております。この変更以降に始めてログインする際には多要素認証セットアップが表示されます。後ほど認証方法を再設定することも可能です。

使用可能な認証方法は以下の通りです。

- 電子メールを用いたパスコード認証
- Okta Verify
- Google Authenticator

上記の内、電子メールを用いたパスコード認証を設定した際のログイン手順につきまして次項に記載しておりますのでご参照ください。

2. 多要素認証のログイン手順（電子メールを用いる場合）

① CSP サイト(https://support.paloaltonetworks.com/Support/Index)にアクセス。
② 右上の「Sign in」をクリック。
③ ユーザ名(メールアドレス)を入力して「Next」をクリック。
④ パスワードを入力して「Sign In」をクリック。
⑤ パスコード送信画面が表示されます。
「コードを送信してください」をクリック。

図 1 パスコード送信画面

⑥　以下画像のパスコード入力画面が表示されます。

図 2 パスコード入力画面

⑦　③で入力したメールアドレス宛にパスコードが送信されます。

送信元：noreply@auth.paloaltonetworks.com

件名　：New Authentication Request from Palo Alto Networks

図 3 パスコード送信メールの例

⑧　⑤パスコード入力画面にパスコードを入力して「サインオン」をクリック。

⑨　認証済みと表示されログインが成功します。

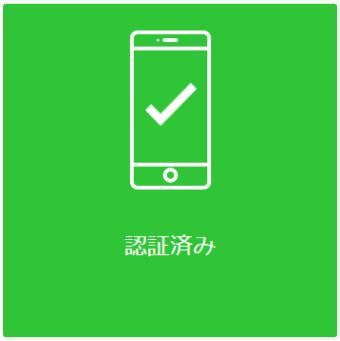

図 4 認証成功の画面

3. 多要素認証方法の再設定手順

設定手順については下記 Palo Alto Networks 社ページの「Configure 2FA Methods」をご参照ください。また、本件に関する詳細についても掲載されております。

TWO FACTOR AUTHENTICATION FOR CUSTOMER SUPPORT PORTAL

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClN9CAK

以上