

# CVR100W VPNルータのパスワードの複雑度の設定

## 目的

パスワードの複雑さにより、ユーザはネットワークアクセスに対してより強力なパスワードを作成できます。強力なパスワードを作成する機能には、数字、大文字、小文字が混在しています。これにより、ネットワークの安全性が高まります。

このドキュメントの目的は、CVR100W VPNルータでパスワードを設定する方法を示すことです。

## 該当するデバイス

- ・ CVR100W

## [Software Version]

- ・1.0.1.19

## パスワードセキュリティ

ステップ1: Web構成ユーティリティにログインし、[Administration] > [Password Complexity] を選択します。「パスワードの複雑さ」ページが開きます。

Minimal password length: 10 (Range: 0 - 64, Default: 8)

Minimal number of character classes: 4 (Range: 0 - 4, Default: 3)

The available character classes include upper case (ABCD...), lower case(abcd...), numerical(1234...) and special characters(!@#\$...).

The new password must be different than the current one:  Enable

Password Aging:  Enable

Password aging time: 200 days (Range: 1 - 365, Default: 180)

Save Cancel

ステップ2:[Password Complexity Settings]フィールドで、[Enable]チェックボックスをオンにして、パスワードの複雑さの設定を有効にします。

ステップ3:[Minimal Password Length]フィールドに、パスワードの文字数を入力します。

ステップ4:「文字クラスの最小数」フィールドに、パスワードで使用する文字クラスの最小数を入力します。

- ・ 大文字: 「ABCD」などの大文字です。

- ・ 小文字：「abcd」などの小文字です。
- ・ 数値：「1234」などの数値です。
- ・ 特殊文字：「!@\$」などの特殊文字です。

ステップ5: ( オプション ) 新しいパスワードを以前のパスワードと異なるように要求するには、[新しいパスワードは現在の1つとは異なる必要がある]フィールドの[有効]チェックボックスをオンにします。

ステップ6: ( オプション ) パスワードに有効期限を設定するには、[パスワードのエージング]フィールドの[有効にする]チェックボックスをオンにします。

ステップ7:[Password Aging]が有効になっている場合は、[Password Aging Time]フィールドにパスワードが期限切れになるまでの期間 ( 日数 ) を入力します。デフォルトは、180 日です。

手順 8 : [Save] をクリックして変更内容を保存します。