

# Cloud Edge シリーズ ver5.6の主な追加機能（1/6）

以下、4つの機能が追加されます。

## （1）デバイス検出機能

Cloud Edgeに接続しているデバイスを検出します。※1※2  
それぞれの端末で運用中のポートを検出します。※3

## （2）トポロジー検出機能

Cloud Edgeから定期的にLLDPを発信し、お客様のネットワーク構成を検出します。※1※2  
クラウドコンソールで構成図の確認が可能です。

## （3）脆弱性スキャン機能

IoTデバイスによくある脆弱性や脆弱なパスワードを使用している端末を検出します。  
デフォルト無効ですが、クラウドコンソールよりスケジュールスキャン・手動スキャンの設定が可能です。

## （4）デバイスタイプにおけるポリシー設定

検出したデバイスのデバイスタイプごとにポリシー設定が可能です。

※1 NATやルータ経由で接続したデバイスは検出できません。

※2 IPv6環境には対応していません。

※3 デフォルト有効ですが、クラウドコンソールよりポート検出の無効化が可能です。

上記機能についての確認方法や設定変更方法は、次ページ以降をご確認いただくか、セキュリティおまかせサポートセンタまでご相談ください。

# Cloud Edge シリーズ ver5.6の主な追加機能 (2/6)

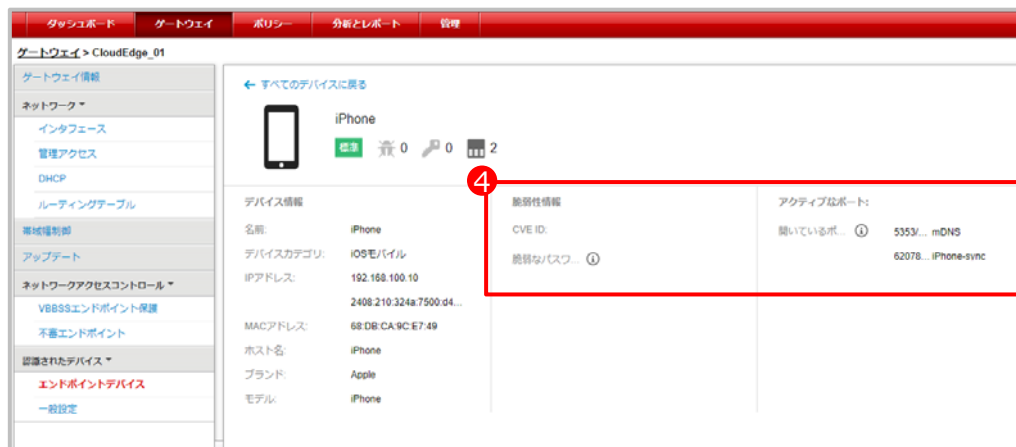
## (1) デバイス検出機能

クラウドコンソールより以下の手順でCloudEdgeに接続しているデバイス一覧の確認が可能です。

- ① 「ゲートウェイ」をクリックします。
- ② 「エンドポイントデバイス」をクリックします。
- ③ 詳細を確認したいデバイスをクリックします。
- ④ 脆弱性情報※4や運用中のポートを確認可能です。

※4 クラウドコンソールより脆弱性スキャンを有効に設定し、脆弱性が検出された場合のみ表示されます。

クラウドコンソール画面イメージ



# Cloud Edge シリーズ ver5.6の主な追加機能（3/6）

クラウドコンソールより運用中のポート検出の無効化が可能です。

※お客様がご利用のファイアウォールやエンドポイントセキュリティ等によってはCloudEdgeのポート検出を攻撃と判定する場合があります。  
その場合、以下の手順にて設定変更を実施してください。

- ① 「ゲートウェイ」をクリックします。
- ② 「一般設定」をクリックします。
- ③ ポート検出を無効化する場合は認識モードを「標準」に変更します。
- ④ 「保存」をクリックします。

クラウドコンソール画面イメージ



# Cloud Edge シリーズ ver5.6の主な追加機能（4/6）

## (2) トポロジー検出機能

クラウドコンソールより以下の手順でトポロジーの確認が可能です。

- ① 「ダッシュボード」をクリックします。
- ② 「デバイスマップとセキュリティ」タブを選択します。

クラウドコンソール画面イメージ



## Cloud Edge シリーズ ver5.6の主な追加機能（5/6）

### （3）脆弱性スキャン機能

検出したIoTデバイスに対して、脆弱性スキャンが可能となります。

本機能をご利用の場合にはクラウドコンソールより以下の手順で設定を実施してください。

- ① 「ゲートウェイ」をクリックします。
- ② 「一般設定」をクリックします。
- ③ 手動検索を行う場合は「検索開始」をクリックします。
- ④ 予約検索を行う場合は「オン」をクリックし、スケジュールを設定します。
- ⑤ 予約検索を設定した場合は「保存」をクリックします。

クラウドコンソール画面イメージ



検出結果はトポロジー画面やデバイス検出画面に表示されます。

- CVE: IoTデバイスによくある脆弱性を検出します。
- 脆弱なパスワード: デフォルトパスワードや連続の数字など、脆弱なパスワードを使用している場合に検出されます。

# Cloud Edge シリーズ ver5.6の主な追加機能（6/6）

## （4）デバイスタイプにおけるポリシー設定

検出したデバイスのデバイスタイプごとにポリシー設定が可能です。

本機能をご利用の場合にはクラウドコンソールよりご希望のセキュリティポリシーを設定してください。

クラウドコンソール画面イメージ

