セキュリティ機能ガイド

© 2025 Brother Industries, Ltd. All rights reserved.

セキュリティに関する重要情報

- 本製品の設定を管理するためのデフォルトのパスワードは、製品底面にあり、「**Pwd**」と表示されています。不正アクセスから本製品を保護するために、デフォルトパスワードを直ちに変更することをお勧めします。
- 本製品の有線・無線 LAN インターフェースは、電気通信事業者（移動通信会社、固定通信会社、インターネットプロバイダー等）の通信回線（公衆無線 LAN を含む）に直接接続することができません。

  本製品をインターネットに接続する場合は、必ずルーター等を経由し接続してください。
- 無線 LAN は、電波の届く範囲であれば、自由に LAN 接続が可能になります。一方で、セキュリティーに関する設定を適切に行わないと、悪意のある第三者が電波を傍受し、下記の様な問題が発生する可能性があります。
  - 個人情報や機密情報を取り出す
  - 特定の人物になりすまして通信し、不正な情報を流す
  - 傍受した通信内容を書き換えて発信する

関連情報

- ネットワーク

デバイスセキュリティの証明書を設定する

SSL/TLS を使用してネットワーク接続された本製品を安全に管理するには、証明書を設定する必要があります。
証明書を設定するには、Web Based Management を使用する必要があります。

セキュリティ証明書機能の概要

本製品は、複数のセキュリティ証明書の使用をサポートしています。これにより、安全な認証および本製品との通信が可能になります。本製品では、以下のセキュリティ証明書機能を使用できます。

お使いの機種によって、対応している機能、オプション、設定が異なる場合があります。

- SSL/TLS 通信
- IEEE 802.1x 認証
- IPsec

本製品は以下をサポートしています。

- プリインストール証明書

  本製品には、自己署名証明書がプリインストールされています。この証明書により、別の証明書を作成またはインストールしなくても、SSL/TLS 通信を使用できます。

  プリインストールされた自己署名証明書により、一定レベルまでは通信が保護されます。セキュリティを強化するために、信頼できる組織から発行された証明書を使用することをお勧めします。

- 自己署名証明書

  本プリントサーバーは自己の証明書を発行します。この証明書を使用すると、別の証明書を作成したり、CA 発行の証明書をインストールしなくても、SSL/TLS 通信を簡単に使用できます。

- 認証局（CA）発行の証明書

  CA 発行の証明書をインストールする場合、2 とおりの方法があります。CA 発行の証明書がすでにある場合、または外部の信頼できる CA の証明書を使用する場合：

  - 本プリントサーバーからの証明書署名要求（CSR）を使用する場合。
  - 証明書とプライベートキーをインポートする場合。

- 認証局（CA）証明書

  CA を識別しプライベートキーを所有する CA 証明書を使用するには、ネットワークのセキュリティ機能を設定する前に、CA が発行した CA 証明書をインポートする必要があります。

- SSL/TLS 通信を使用する場合は、まずシステム管理者に連絡することをお勧めします。
- プリントサーバーをお買い上げ時の設定にリセットする場合、インストールされている証明書とプライベートキーは削除されます。プリントサーバーのリセット後にも同じ証明書とプライベートキーを保持する場合は、リセット前にこれらをエクスポートし、リセット後に再インストールします。

関連情報

- デバイスセキュリティの証明書を設定する

関連トピック：

- Web Based Management を使用してネットワークに IEEE 802.1x 認証を設定する

証明書の作成とインストールの手順

セキュリティ証明書を使用する場合、自己署名証明書を使用するか、認証局（CA）発行の証明書を使用するかを選択できます。

オプション 1

自己署名証明書

1. Web Based Management を使用して自己署名証明書を作成します。
2. パソコンへ自己署名証明書をインストールします。

オプション 2

CA からの証明書

1. Web Based Management を使用して、証明書署名要求（CSR）を作成します。
2. Web Based Management を使用して、CA が発行した証明書を、本製品にインストールします。
3. パソコンへ証明書をインストールします。

関連情報

- デバイスセキュリティの証明書を設定する

自己署名証明書を作成する

1. ウェブブラウザーを起動します。
2. ブラウザーのアドレスバーに「https://製品の IP アドレス」と入力します（「製品の IP アドレス」には、本製品の IP アドレスを入力します）。

   例：

   https://192.168.1.2

   本製品の IP アドレスは、ネットワーク設定リストで確認できます。
3. 必要に応じて**ログイン**欄にパスワードを入力し、**ログイン**をクリックします。

   本製品の設定を管理するためのお買い上げ時のパスワードは、製品背面または底面にあり、「**Pwd**」と表示されています。最初にログインした際、画面の指示に従いお買い上げ時のパスワードを変更します。
4. 左側のナビゲーションバーで、**ネットワーク** > **セキュリティ** > **証明書**をクリックします。

   左側のナビゲーションバーが表示されない場合は、≡からナビゲーションを開始してください。
5. **自己署名証明書の作成**をクリックします。
6. **コモンネーム**および**有効期限**を入力します。
   - **コモンネーム**の長さは 64 バイト未満です。SSL/TLS 通信を介して本製品にアクセスする場合に使用する、IP アドレス、ノード名、ドメイン名などの識別子を入力します。お買い上げ時の設定では、ノード名が表示されます。
   - IPPS または HTTPS プロトコルを使用し、自己署名証明書に使用された**コモンネーム**とは異なる名前が URL に入力された場合は、警告が表示されます。
7. **公開鍵アルゴリズム**ドロップダウンリストから設定を選択します。
8. **メッセージダイジェストアルゴリズム**ドロップダウンリストから設定を選択します。
9. **OK** をクリックします。

関連情報

- デバイスセキュリティの証明書を設定する

証明書署名要求（CSR）を作成して認証局（CA）からの証明書をインストールする

外部の信頼された認証局（CA）からの証明書がすでに存在する場合、その証明書とプライベートキーを本製品に保存し、インポートやエクスポートを行うことによってそれらを管理することができます。外部の信頼された CA からの証明書が存在しない場合、証明書署名要求（CSR）を作成し、CA に送信して認証を受けたあと、返却された証明書を本製品にインストールします。

- 証明書署名要求（CSR：Certificate Signing Request）を作成する
- 証明書を本製品にインストールする

証明書署名要求（CSR：Certificate Signing Request）を作成する

証明書署名要求（CSR）は、証明書に含まれる資格情報を認証するために、認証局（CA）に送信される要求です。

CSR を作成する前に、CA からのルート証明書をお使いのパソコンにインストールしておくことを推奨します。

1. ウェブブラウザーを起動します。
2. ブラウザーのアドレスバーに「https://製品の IP アドレス」と入力します（「製品の IP アドレス」には、本製品の IP アドレスを入力します）。

   例：

   https://192.168.1.2

   本製品の IP アドレスは、ネットワーク設定リストで確認できます。
3. 必要に応じて**ログイン**欄にパスワードを入力し、**ログイン**をクリックします。

本製品の設定を管理するためのお買い上げ時のパスワードは、製品背面または底面にあり、「**Pwd**」と表示されています。最初にログインした際、画面の指示に従いお買い上げ時のパスワードを変更します。

4. 左側のナビゲーションバーで、**ネットワーク** > **セキュリティ** > **証明書**をクリックします。

左側のナビゲーションバーが表示されない場合は、≡からナビゲーションを開始してください。

5. **CSR の作成**をクリックします。
6. **コモンネーム**（必須）を入力して、ご使用の**組織**に関するその他の情報（任意）を追加します。

- CA がお客様の身元を確認し、外部に向けて証明するために、お客様の会社の情報が必要です。
- **コモンネーム**の長さは 64 バイト未満である必要があります。SSL/TLS 通信を介して本製品にアクセスする場合に使用する、IP アドレス、ノード名、ドメイン名などの識別子を入力します。お買い上げ時の設定では、ノード名が表示されます。**コモンネーム**は必須です。
- 証明書に使用された共通名とは異なる名前が URL に入力された場合は、警告が表示されます。
- **組織**、**部署**、**市**、および**県/州**の長さは 64 バイト未満の必要があります。
- **国**は、2 文字の ISO 3166 国コードです。
- X.509v3 証明書拡張を設定する場合、**拡張領域設定**チェックボックスを選択後、**自動 (本機の IPv4 アドレスを登録します。)**または**手動**を選択します。

7. **公開鍵アルゴリズム**ドロップダウンリストから設定を選択します。
8. **メッセージダイジェストアルゴリズム**ドロップダウンリストから設定を選択します。
9. **OK** をクリックします。

   CSR が画面に表示されます。表示された CSR をファイルとして保存するか、認証局から提供されたオンラインの CSR フォームにコピー・ペーストします。
10. **保存**をクリックします。

- CSR をお客様の CA に送信する方法については、お客様の CA の方針に従ってください。
- Windows Server の Enterprise root CA を使用している場合、クライアント証明書の安全な作成のために、証明書用ウェブサーバーテンプレートを使用することを推奨します。EAP-TLS 認証を行う IEEE 802.1x 環境のためのクライアント証明書を作成する場合、証明書用ユーザーテンプレートを使用することを推奨します。

関連情報

- 証明書署名要求（CSR）を作成して認証局（CA）からの証明書をインストールする

証明書を本製品にインストールする

認証局（CA）から証明書を受信した後、以下の手順でプリントサーバーにインストールします。

本製品には、本製品の証明書署名要求（CSR）と一緒に発行された証明書のみをインストールできます。他のCSR を作成する場合は、新しい CSR を作成する前に、この証明書がインストールされていることを確認してください。他の CSR の作成は、この証明書を必ず先にインストールしてから行ってください。新しい CSR のインストール前に作成された CSR は無効になります。

1. ウェブブラウザーを起動します。
2. ブラウザーのアドレスバーに「https://製品の IP アドレス」と入力します（「製品の IP アドレス」には、本製品の IP アドレスを入力します）。

   例：

   https://192.168.1.2

   本製品の IP アドレスは、ネットワーク設定リストで確認できます。
3. 必要に応じて**ログイン**欄にパスワードを入力し、**ログイン**をクリックします。

本製品の設定を管理するためのお買い上げ時のパスワードは、製品背面または底面にあり、「**Pwd**」と表示されています。最初にログインした際、画面の指示に従いお買い上げ時のパスワードを変更します。

4. 左側のナビゲーションバーで、**ネットワーク** > **セキュリティ** > **証明書**をクリックします。

左側のナビゲーションバーが表示されない場合は、☰からナビゲーションを開始してください。

5. **証明書のインストール**をクリックします。
6. CA に発行された証明書を含むファイルを表示して、**OK** をクリックします。

   証明書が作成され、本製品のメモリーに保存されます。

SSL/TLS 通信を使用する場合は、お使いのパソコンに、CA から取得したルート証明書を必ずインストールしてください。ネットワーク管理者にお問い合わせください。

関連情報

- 証明書署名要求（CSR）を作成して認証局（CA）からの証明書をインストールする

証明書とプライベートキーのインポートとエクスポートについて

証明書とプライベートキーを本製品に保存して、インポートまたはエクスポートすることにより、これらを管理します。

- 証明書とプライベートキーをインポートする
- 証明書とプライベートキーをエクスポートする

証明書とプライベートキーをインポートする

1. ウェブブラウザーを起動します。
2. ブラウザーのアドレスバーに「https://製品の IP アドレス」と入力します（「製品の IP アドレス」には、本製品の IP アドレスを入力します）。

   例：

   https://192.168.1.2

   本製品の IP アドレスは、ネットワーク設定リストで確認できます。
3. 必要に応じて**ログイン**欄にパスワードを入力し、**ログイン**をクリックします。

   本製品の設定を管理するためのお買い上げ時のパスワードは、製品背面または底面にあり、「**Pwd**」と表示されています。最初にログインした際、画面の指示に従いお買い上げ時のパスワードを変更します。
4. 左側のナビゲーションバーで、**ネットワーク** > **セキュリティ** > **証明書**をクリックします。

   左側のナビゲーションバーが表示されない場合は、≡からナビゲーションを開始してください。
5. **証明書と秘密鍵のインポート**をクリックします。
6. インポートするファイルを表示して、選択します。
7. ファイルが暗号化されている場合はパスワードを入力し、**OK** をクリックします。

証明書とプライベートキーが本製品にインポートされます。

関連情報

- 証明書とプライベートキーのインポートとエクスポートについて

証明書とプライベートキーをエクスポートする

1. ウェブブラウザーを起動します。
2. ブラウザーのアドレスバーに「https://製品の IP アドレス」と入力します（「製品の IP アドレス」には、本製品の IP アドレスを入力します）。

   例：

   https://192.168.1.2

   本製品の IP アドレスは、ネットワーク設定リストで確認できます。
3. 必要に応じて**ログイン**欄にパスワードを入力し、**ログイン**をクリックします。

   本製品の設定を管理するためのお買い上げ時のパスワードは、製品背面または底面にあり、「**Pwd**」と表示されています。最初にログインした際、画面の指示に従いお買い上げ時のパスワードを変更します。
4. 左側のナビゲーションバーで、**ネットワーク** > **セキュリティ** > **証明書**をクリックします。

   左側のナビゲーションバーが表示されない場合は、☰からナビゲーションを開始してください。
5. **証明書一覧**と共に表示される**エクスポート**をクリックします。
6. ファイルを暗号化する場合は、パスワードを入力します。

   パスワードを空白のままにすると、出力内容は暗号化されません。
7. 確認のためにパスワードを再入力し、**OK** をクリックします。
8. **保存**をクリックします。

証明書とプライベートキーがお使いのパソコンにエクスポートされます。

ご使用のパソコンに証明書をインポートすることもできます。

関連情報

- 証明書とプライベートキーのインポートとエクスポートについて

CA 証明書のインポートとエクスポートについて

本製品では、CA 証明書のインポートやエクスポート、または保存ができます。

- CA 証明書をインポートする
- CA 証明書をエクスポートする

CA 証明書をインポートする

1. ウェブブラウザーを起動します。
2. ブラウザーのアドレスバーに「https://製品の IP アドレス」と入力します（「製品の IP アドレス」には、本製品の IP アドレスを入力します）。

   例：

   https://192.168.1.2

   本製品の IP アドレスは、ネットワーク設定リストで確認できます。
3. 必要に応じて**ログイン**欄にパスワードを入力し、**ログイン**をクリックします。

   本製品の設定を管理するためのお買い上げ時のパスワードは、製品背面または底面にあり、「**Pwd**」と表示されています。最初にログインした際、画面の指示に従いお買い上げ時のパスワードを変更します。
4. 左側のナビゲーションバーで、**ネットワーク** > **セキュリティ** > **CA 証明書**をクリックします。

   左側のナビゲーションバーが表示されない場合は、☰からナビゲーションを開始してください。
5. **CA 証明書のインポート**をクリックします。
6. インポートするファイルを表示します。
7. **OK** をクリックします。

関連情報

- CA 証明書のインポートとエクスポートについて

CA 証明書をエクスポートする

1. ウェブブラウザーを起動します。
2. ブラウザーのアドレスバーに「https://製品の IP アドレス」と入力します（「製品の IP アドレス」には、本製品の IP アドレスを入力します）。

   例：

   https://192.168.1.2

   本製品の IP アドレスは、ネットワーク設定リストで確認できます。
3. 必要に応じて**ログイン**欄にパスワードを入力し、**ログイン**をクリックします。

   本製品の設定を管理するためのお買い上げ時のパスワードは、製品背面または底面にあり、「**Pwd**」と表示されています。最初にログインした際、画面の指示に従いお買い上げ時のパスワードを変更します。
4. 左側のナビゲーションバーで、**ネットワーク** > **セキュリティ** > **CA 証明書**をクリックします。

   左側のナビゲーションバーが表示されない場合は、☰からナビゲーションを開始してください。
5. エクスポートする証明書を選択し、**エクスポート**をクリックします。
6. **OK** をクリックします。

関連情報

- CA 証明書のインポートとエクスポートについて

SSL/TLS を使用する

- SSL/TLS を使用した安全なネットワーク製品の管理
- SSL/TLS を使用して文書を安全に印刷する
- SSL/TLS を使用して E メールを安全に送受信する

SSL/TLS を使用した安全なネットワーク製品の管理

SSL/TLS および使用可能なプロトコルの証明書を設定する

SSL/TLS 通信を使用するには、Web Based Management を使用して本製品に証明書を設定します。

1. ウェブブラウザーを起動します。
2. ブラウザーのアドレスバーに「https://製品の IP アドレス」と入力します（「製品の IP アドレス」には、本製品の IP アドレスを入力します）。

   例：

   https://192.168.1.2

   本製品の IP アドレスは、ネットワーク設定リストで確認できます。
3. 必要に応じて**ログイン**欄にパスワードを入力し、**ログイン**をクリックします。

   本製品の設定を管理するためのお買い上げ時のパスワードは、製品背面または底面にあり、「**Pwd**」と表示されています。最初にログインした際、画面の指示に従いお買い上げ時のパスワードを変更します。
4. 左側のナビゲーションバーで、**ネットワーク** > **ネットワーク** > **プロトコル**をクリックします。

   左側のナビゲーションバーが表示されない場合は、☰からナビゲーションを開始してください。
5. **HTTP サーバー設定**をクリックします。
6. **証明書の選択**ドロップダウンリストから、設定対象の証明書を選択します。
7. **OK** をクリックします。
8. **はい**をクリックしてプリントサーバーを再起動します。

関連情報

- SSL/TLS を使用した安全なネットワーク製品の管理

関連トピック：

- SSL/TLS を使用して文書を安全に印刷する

SSL/TLS を使用して Web Based Management にアクセスする

お使いのネットワーク製品を安全に管理するには、セキュリティプロトコルを使用している管理ユーティリティを使用する必要があります。

- HTTPS プロトコルを使用するには、本製品で HTTPS が有効になっている必要があります。お買い上げ時の設定では、HTTPS プロトコルは有効です。
- Web Based Management の画面で HTTPS プロトコルの設定を変更できます。

1. ウェブブラウザーを起動します。
2. ブラウザーのアドレスバーに「https://製品の IP アドレス」と入力します（「製品の IP アドレス」には、本製品の IP アドレスを入力します）。

   例：

   https://192.168.1.2

   本製品の IP アドレスは、ネットワーク設定リストで確認できます。
3. 必要に応じて**ログイン**欄にパスワードを入力し、**ログイン**をクリックします。

本製品の設定を管理するためのお買い上げ時のパスワードは、製品背面または底面にあり、「**Pwd**」と表示されています。最初にログインした際、画面の指示に従いお買い上げ時のパスワードを変更します。

4. 以上で HTTPS を使用して製品へアクセスする準備が整いました。

関連情報

- SSL/TLS を使用した安全なネットワーク製品の管理

管理者として Windows ユーザー用の自己署名証明書をインストールする

- 以下の手順は、Microsoft Edge を使用する場合です。その他のウェブブラウザーを使用している場合は、ウェブブラウザーの説明書またはオンラインヘルプで、証明書のインストール方法を参照してください。
- Web Based Management を使用して、自己署名証明書を作成したことを確認してください。

1. **Microsoft Edge** アイコンを右クリックし、**管理者として実行**をクリックします。
   ユーザー アカウント制御画面が表示されたら、**はい**をクリックします。
2. ブラウザーのアドレスバーに「https://製品の IP アドレス」と入力します（「製品の IP アドレス」には、本製品の IP アドレスを入力します）。
   例：
   https://192.168.1.2
   本製品の IP アドレスは、ネットワーク設定リストで確認できます。
3. 接続がプライベートでない場合場合は、**詳細設定**ボタンをクリックしてから、ウェブページに進んでください。
4. 必要に応じて**ログイン**欄にパスワードを入力し、**ログイン**をクリックします。

本製品の設定を管理するためのお買い上げ時のパスワードは、製品背面または底面にあり、「**Pwd**」と表示されています。最初にログインした際、画面の指示に従いお買い上げ時のパスワードを変更します。

5. 左側のナビゲーションバーで、**ネットワーク** > **セキュリティ** > **証明書**をクリックします。

左側のナビゲーションバーが表示されない場合は、☰からナビゲーションを開始してください。

6. **エクスポート**をクリックします。
7. 出力ファイルを暗号化するには、**パスワード設定**欄にパスワードを入力します。**パスワード設定**欄が空白の場合、出力ファイルは暗号化されません。
8. **パスワード確認**欄にパスワードを再度入力し、**OK** をクリックします。
9. ダウンロードしたファイルをクリックして開きます。
10. **証明書のインポート ウィザード**が表示されたら、 **次へ**をクリックします。
11. **次へ**をクリックします。
12. 必要に応じて、パスワードを入力し、**次へ**をクリックします。
13. **証明書をすべて次のストアに配置する** を選択してから **参照...** をクリックします。
14. **信頼されたルート証明機関**を選択し、**OK** をクリックします。
15. **次へ**をクリックします。
16. **完了**をクリックします。
17. フィンガープリント（拇印）が正しければ、**はい**をクリックします。
18. **OK** をクリックします。

関連情報

- SSL/TLS を使用した安全なネットワーク製品の管理

SSL/TLS を使用して文書を安全に印刷する

IPPS を使用して文書を印刷する

IPP プロトコルを使用して文書を安全に印刷するには、IPPS プロトコルを使用します。

1. ウェブブラウザーを起動します。
2. ブラウザーのアドレスバーに「https://製品の IP アドレス」と入力します（「製品の IP アドレス」には、本製品の IP アドレスを入力します）。

   例：

   https://192.168.1.2

   本製品の IP アドレスは、ネットワーク設定リストで確認できます。
3. 必要に応じて**ログイン**欄にパスワードを入力し、**ログイン**をクリックします。

本製品の設定を管理するためのお買い上げ時のパスワードは、製品背面または底面にあり、「**Pwd**」と表示されています。最初にログインした際、画面の指示に従いお買い上げ時のパスワードを変更します。

4. 左側のナビゲーションバーで、**ネットワーク** > **ネットワーク** > **プロトコル**をクリックします。

左側のナビゲーションバーが表示されない場合は、☰からナビゲーションを開始してください。

5. **IPP** チェックボックスが選択されていることを確認します。

IPP チェックボックスが選択されていない場合、**IPP** チェックボックスを選択して、**OK** をクリックします。
製品を再起動して、設定を有効にします。
本製品が再起動したら、本製品のウェブページに戻ってパスワードを入力し、左側のナビゲーションバーで、**ネットワーク** > **ネットワーク** > **プロトコル**をクリックします。

6. **HTTP サーバー設定**をクリックします。
7. **IPP** で **HTTPS** チェックボックスを選択し、**OK** をクリックします。
8. 製品を再起動して、設定を有効にします。

IPPS を使用した通信では、プリントサーバーへの非認証のアクセスを防ぐことはできません。

関連情報

- SSL/TLS を使用して文書を安全に印刷する

SNMPv3 を使用する

- SNMPv3 を使用した安全なネットワーク製品の管理

SNMPv3 を使用した安全なネットワーク製品の管理

簡易ネットワーク管理プロトコルバージョン 3（SNMPv3）は、ネットワーク機器を安全に管理するための、ユーザー認証とデータの暗号化に使用されます。

1. ウェブブラウザーを起動します。
2. ブラウザーのアドレスバーに「https://共通名」と入力します（ただし「共通名」は、証明書に割り当てた共通名（IP アドレス、ノード名、ドメイン名など））。
3. 必要に応じて**ログイン**欄にパスワードを入力し、**ログイン**をクリックします。

本製品の設定を管理するためのお買い上げ時のパスワードは、製品背面または底面にあり、「**Pwd**」と表示されています。最初にログインした際、画面の指示に従いお買い上げ時のパスワードを変更します。

4. 左側のナビゲーションバーで、**ネットワーク** > **ネットワーク** > **プロトコル**をクリックします。

左側のナビゲーションバーが表示されない場合は、☰からナビゲーションを開始してください。

5. **SNMP** 設定が有効であることを確認して、**詳細設定**をクリックします。
6. SNMPv1/v2c モードの設定を行います。

オプション	詳細
SNMP v1/v2c read-write access	プリントサーバーは SNMP プロトコルの Ver. 1 および Ver. 2c を使用します。このモードで、本製品のすべてのアプリケーションが使用できます。ただし、ユーザーの認証は行われず、データは暗号化されないため、安全ではありません。
SNMP v1/v2c read-only access	プリントサーバーは SNMP プロトコルの Ver. 1 および Ver. 2c（読み取り専用アクセス）を使用します。
無効	SNMP プロトコルの Ver. 1 および Ver. 2c を無効にします。 SNMPv1/v2c を使用するすべてのアプリケーションが制限されます。SNMPv1/v2c アプリケーションの使用を許可するには、**SNMP v1/v2c read-only access** または **SNMP v1/v2c read-write access** モードを使います。

7. SNMPv3 モードの設定を行います。

オプション	詳細
有効	プリントサーバーは SNMP プロトコルの Ver. 3 を使用します。プリントサーバーを安全に管理するには、SNMPv3 モードを使用して設定を行います。
無効	SNMP プロトコルの Ver. 3 を無効にします。 SNMPv3 を使用するすべてのアプリケーションが制限されます。SNMPv3 アプリケーションの使用を許可するには、SNMPv3 モードを使います。

8. **OK** をクリックします。

本製品にプロトコル設定オプションが表示された場合は、使用するオプションを選択します。

9. 製品を再起動して、設定を有効にします。

関連情報

- SNMPv3 を使用する

お使いのネットワークに IEEE 802.1x 認証を使用する

IEEE 802.1x 認証について

IEEE 802.1x は IEEE 標準であり、非認証のネットワーク機器からのアクセスを制限します。本製品は、アクセスポイントまたはハブを通して、RADIUS サーバー（認証サーバー）に認証要求を送信します。要求が RADIUS サーバーに確認されると、本製品はネットワークにアクセスすることができます。

関連情報

- お使いのネットワークに IEEE 802.1x 認証を使用する

Web Based Management を使用してネットワークに IEEE 802.1x 認証を設定する

- EAP-TLS 認証を使用して本製品を設定する場合、設定の開始前に、CA により発行されたクライアント証明書を必ずインストールしてください。クライアント証明書については、ネットワーク管理者に問い合わせてください。複数の証明書をインストールした場合、使用する証明書の名前を書き留めておくことをお勧めします。
- サーバー証明書を検証する前に、該当のサーバー証明書に署名した CA 発行の、CA 証明書をインポートする必要があります。ネットワーク管理者または契約しているインターネットサービスプロバイダー（ISP）にお問い合わせください。

操作パネルから無線セットアップウィザードを使用して IEEE 802.1x 認証を設定することもできます（無線 LAN）。

1. ウェブブラウザーを起動します。
2. ブラウザーのアドレスバーに「https://製品の IP アドレス」と入力します（「製品の IP アドレス」には、本製品の IP アドレスを入力します）。

   例：

   https://192.168.1.2

   本製品の IP アドレスは、ネットワーク設定リストで確認できます。
3. 必要に応じて**ログイン**欄にパスワードを入力し、**ログイン**をクリックします。

本製品の設定を管理するためのお買い上げ時のパスワードは、製品背面または底面にあり、「**Pwd**」と表示されています。最初にログインした際、画面の指示に従いお買い上げ時のパスワードを変更します。

4. 左側のナビゲーションバーで、**ネットワーク**をクリックします。

左側のナビゲーションバーが表示されない場合は、☰からナビゲーションを開始してください。

5. 次のいずれかを行ってください：
   - 有線 LAN の場合

     有線 > **有線 802.1x 認証**をクリックします。
   - 無線 LAN の場合

     無線 > **無線 (エンタープライズ)**をクリックします。
6. IEEE 802.1x 認証を設定します。

- 有線 LAN の IEEE 802.1x 認証を有効にするには、**有線 802.1x 認証**ページの**有線 802.1x** で**有効**を選択します。
- **EAP-TLS** 認証を使用している場合、検証のためにインストールされているクライアント証明書（証明書の名前付きで表示）を、**クライアント証明書**ドロップダウンリストから選択する必要があります。
- **EAP-FAST**、**PEAP**、**EAP-TTLS**、または **EAP-TLS** 認証を選択する場合は、**サーバー証明書の検証**ドロップダウンリストから検証方式を選択します。該当のサーバー証明書に署名した CA が発行し、あらかじめ製品にインポートされた CA 証明書を使用して、サーバー証明書を検証します。

サーバー証明書の検証ドロップダウンリストから、以下の検証方式のいずれかを選択します。

オプション	詳細
検証しない	このサーバー証明書は常に信頼できます。検証は実施されません。
CA 証明書	該当のサーバー証明書に署名した CA により発行された CA 証明書を使用して、サーバー証明書の CA 信頼性を確認する検証方法。

オプション	詳細
CA 証明書+サーバー ID	共通名を確認する検証方法[1] を確認する検証方法。

7. 設定が終了したら、**OK** をクリックします。

   有線 LAN の場合：設定後、IEEE 802.1x がサポートされたネットワークに、使用製品を接続します。数分後、ネットワーク設定リストを印刷して、**<Wired IEEE 802.1x>**の状態を確認します。

オプション	詳細
Success	有線の IEEE 802.1x 機能は有効で、認証は成功しました。
Failed	有線の IEEE 802.1x 機能は有効ですが、認証は失敗しました。
Off	有線の IEEE 802.1x 機能は利用不可です。

関連情報

- お使いのネットワークに IEEE 802.1x 認証を使用する

関連トピック：

- セキュリティ証明書機能の概要
- デバイスセキュリティの証明書を設定する

1 共通名の検証では、サーバー証明書の共通名と、**サーバー ID** に設定された文字列を比較します。この方式を使用する前に、サーバー証明書の共通名についてシステム管理者に問い合わせて、**サーバー ID** を設定してください。

IEEE 802.1x 認証方式

EAP-FAST

EAP-FAST（Extensible Authentication Protocol-Flexible Authentication via Secured Tunneling）は、Cisco Systems 社が開発したプロトコルで、認証のためのユーザー ID とパスワード、および対称キーアルゴリズムを使用してトンネル認証プロセスを実現します。

本製品は、以下の内部認証方式をサポートしています。

- EAP-FAST/NONE
- EAP-FAST/MS-CHAPv2
- EAP-FAST/GTC

EAP-MD5 （有線 LAN）

拡張可能認証プロトコルメッセージダイジェストアルゴリズム 5（EAP-MD5：Extensible Authentication Protocol-Message Digest Algorithm 5）はユーザー ID とパスワードを使用して、チャレンジ／レスポンス認証を行います。

PEAP

保護された拡張可能認証プロトコル（PEAP：Protected Extensible Authentication Protocol）は、Cisco Systems 社、Microsoft 社、および RSA セキュリティ社が開発した EAP 方式です。PEAP はユーザー ID とパスワードを送信するために、クライアントと認証サーバー間に、暗号化した Secure Sockets Layer（SSL）/Transport Layer Security（TLS）トンネルを作成します。PEAP により、サーバーとクライアント間の相互認証が行えます。

本製品は、以下の内部認証方式をサポートしています。

- PEAP/MS-CHAPv2
- PEAP/GTC

EAP-TTLS

拡張可能認証プロトコルトンネル方式トランスポートレイヤーセキュリティ（EAP-TTLS：Extensible Authentication Protocol-Tunneled Transport Layer Security）は、ファンク・ソフトウェア社と Certicom 社によって開発されました。EAP-TTLS は、クライアントと認証サーバー間に、ユーザー ID およびパスワードを送信するための、PEAP 同様の暗号化 SSL トンネルを作成します。EAP-TTLS により、サーバーとクライアント間の相互認証が行えます。

本製品は、以下の内部認証方式をサポートしています。

- EAP-TTLS/CHAP
- EAP-TTLS/MS-CHAP
- EAP-TTLS/MS-CHAPv2
- EAP-TTLS/PAP

EAP-TLS

拡張可能認証プロトコルトランスポートレイヤーセキュリティ（EAP-TLS：Extensible Authentication Protocol-Transport Layer Security）では、クライアントと認証サーバーのいずれにも、デジタル証明書認証が必要です。

関連情報

- お使いのネットワークに IEEE 802.1x 認証を使用する