セキュリティ機能ガイド

注意事項の定義

本ガイドでは、以下の記号が使用されます。

重要	重要は、この表示を無視して、誤った取り扱いをすると、物的損害の可能性がある内容を示しています。
お願い	お願いは、ご使用していただく上での注意事項、制限事項などの内容を示しています。
	有益なヒントや補足情報を示しています。
太字	本製品の操作パネルやパソコン画面に表示されるボタンを示しています。
斜体	斜体は重要な項目の強調や、関連するトピックを示しています。

商標

Adobe®および Reader®は、米国および／またはその他の国における Adobe Systems Incorporated の登録商標または商標です。

本ガイドに記載されているソフトウェアの各社は、各プログラムに固有のソフトウェアライセンス契約を有しています。

ブラザー製品および関連資料等に記載されている社名及び商品名はそれぞれ各社の商標または登録商標です。

著作権

目次

セキュリティ機能をご使用になる前に

本製品には、最新のネットワークセキュリティの一部と、現在利用可能な暗号化プロトコルが使用されています。これらのネットワーク機能は、お使いの全体的なネットワークセキュリティプランの一部として、データを保護し、本製品への不正なアクセスを防ぐことができます。

FTP および TFTP プロトコルを無効にすることをお勧めします。これらのプロトコルを使用した本製品へのアクセスは安全ではありません。

関連情報

- 不要なプロトコルを無効にする

不要なプロトコルを無効にする

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** > **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. 不要なプロトコルのチェックボックスをオフにして無効にします。
6. **OK** をクリックします。
7. 本製品を再起動して、設定を有効にします。

関連情報

- セキュリティ機能をご使用になる前に

ネットワークセキュリティ

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
- SSL/TLS および使用可能なプロトコルの証明書を設定する
- デバイスセキュリティの証明書を設定する

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

IPsec を使用する

IPsec について

IPsec（Internet Protocol Security）は、任意のインターネットプロトコル機能を使用してデータの改ざんを防止し、IP パケットとして送信されるデータの信頼性を確保するセキュリティプロトコルです。IPsec は、パソコンからプリンターへ送信される印刷データなど、ネットワーク経由で転送されるデータを暗号化します。データはネットワーク層で暗号化されるため、高レベルのプロトコルを使用するアプリケーションには、ユーザーが認識していなくても、IPsec が使用されています。

IPsec では、以下の機能をサポートしています。

- IPsec 送信

  IPsec 設定条件に従い、ネットワークに接続されたパソコンは、IPsec に対応している指定機器との間でデータの送受信を行います。機器が IPsec を使用して通信を開始すると、インターネットキー交換（IKE : Internet Key Exchange）を使用してキーが交換されたあと、それらのキーを使用して暗号化されたデータが送信されます。

  また、IPsec には、トランスポートモードおよびトンネルモードの、2 種類の操作モードがあります。トランスポートモードは、主に機器間の通信に使用され、トンネルモードは仮想プライベートネットワーク（VPN : Virtual Private Network）などの環境で使用されます。

IPsec 送信を行うには、次の条件が必要です。

- IPsec を使用して通信できるパソコンが、ネットワークに接続されている。
- 本製品が IPsec 通信用に設定されている。
- 本製品に接続されているパソコンが、IPsec 接続用に設定されている。

- IPsec 設定

  IPsec を使用する接続に必要な設定。これらの設定は、Web Based Management を使用して行うことができます。

IPsec を設定するには、該当ネットワークに接続されているパソコンのブラウザーを使用する必要があります。

関連情報

- IPsec を使用する

Web Based Management を使用して IPsec を設定する

IPsec の接続条件は、**アドレス**および **IPsec** の 2 種類の**テンプレート**で構成されます。最大 10 個の接続条件を設定できます。

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. 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** > **IPsec** 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. 設定を確認します。

オプション	詳細
状態	IPsec を有効または無効にします。
接続モード	IKE Phase 1 の**接続モード**を選択します。IKE はプロトコルであり、IPsec を使用して暗号化通信を行うための、暗号キーの交換に使用されます。 **メイン**モードでは、処理速度は遅くなりますが、安全性は高くなります。**アグレッシブ**モードでは、処理速度は**メイン**モードの場合より速くなりますが、安全性は低くなります。
IPsec 以外のトラフィックルール	IPsec 以外のパケットに対する対処方法を選択します。 Web サービスを使用するとき、**IPsec 以外のトラフィックルール**に対して**通過**を選択する必要があります。**遮断**を選択すると、Web サービスは使用できません。
Broadcast/Multicast Bypass	**有効**または**無効**を選択します。
Protocol Bypass	使用したいオプションのチェックボックスを選択します。
ルール	**有効**チェックボックスを選択して、テンプレートを有効にします。複数のチェックボックスを選択し、それらの設定が競合する場合は、番号が小さい方のチェックボックスの設定が優先されます。 対応するドロップダウンリストをクリックして、IPsec の接続条件に使用される**アドレステンプレート**を選択します。**アドレステンプレート**を追加するには、**テンプレートの追加**をクリックします。 対応するドロップダウンリストをクリックして、IPsec の接続条件に使用される **IPsec テンプレート**を選択します。**IPsec テンプレート**を追加するには、**テンプレートの追加**をクリックします。

6. **OK** をクリックします。

   新しい設定を有効にするために本製品を再起動する必要がある場合は、再起動の確認画面が表示されます。

   ルールで有効化したテンプレートに空白の項目が含まれる場合、エラーメッセージが表示されます。選択した項目を確認し、もう一度 **OK** をクリックします。

関連情報

- IPsec を使用する

関連トピック：

- デバイスセキュリティの証明書を設定する

Web Based Management を使用して IPsec アドレステンプレートを設定する

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** > **IPsec アドレステンプレート**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. **削除**ボタンをクリックして**アドレステンプレート**を削除します。**アドレステンプレート**が使用中の場合は、削除できません。
6. 作成したい**アドレステンプレート**をクリックします。**IPsec アドレステンプレート**が表示されます。
7. 設定を確認します。

オプション	詳細
テンプレート名	作成するテンプレートの名前を入力します（最大 16 文字）。
ローカル IP アドレス	• **IP アドレス** IP アドレスを指定します。ドロップダウンリストから、**すべての IPv4 アドレス**、**すべての IPv6 アドレス**、**すべてのリンクローカル IPv6 アドレス**、または**カスタム**を選択します。 ドロップダウンリストから**カスタム**を選択した場合、テキストボックスに IP アドレス（IPv4 または IPv6）を入力します。 • **IP アドレス範囲** テキストボックスに IP アドレス範囲の開始アドレスと終了アドレスを入力します。開始および終了の IP アドレスが IPv4 または IPv6 に合わせて標準化されていない場合、または終了 IP アドレスが開始アドレスより小さい場合、エラーが発生します。 • **IP アドレス/プレフィックス** IP アドレスを CIDR 表記で指定します。 例：192.168.1.1/24 192.168.1.1 に対しプレフィックスを 24 ビットのサブネットマスク（255.255.255.0）で指定するため、192.168.1.### というアドレスが有効となります。
リモート IP アドレス	• **すべて** **すべて**を選択すると、すべての IP アドレスが有効になります。 • **IP アドレス** 指定した IP アドレス（IPv4 または IPv6）をテキストボックスに入力します。 • **IP アドレス範囲** IP アドレス範囲の最初と最後のアドレスを入力します。最初と最後の IP アドレスが IPv4 または IPv6 に合わせて標準化されてい

オプション	詳細
	ない場合、または最後の IP アドレスが最初のアドレスより小さい場合、エラーが発生します。 • **IP アドレス/プレフィックス** IP アドレスを CIDR 表記で指定します。 例：192.168.1.1/24 192.168.1.1 に対しプレフィックスを 24 ビットのサブネットマスク（255.255.255.0）で指定するため、192.168.1.### というアドレスが有効となります。

8. **OK** をクリックします。

使用中のテンプレートの設定を変更する場合は、本製品を再起動して設定を有効にします。

関連情報

- IPsec を使用する

Web Based Management を使用して IPsec テンプレートを設定する

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** > **IPsec テンプレート**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. **削除**ボタンをクリックして **IPsec テンプレート**を削除します。**IPsec テンプレート**が使用中の場合は、削除できません。
6. 作成したい **IPsec テンプレート**をクリックします。**IPsec テンプレート**画面が表示されます。設定欄は、選択する**テンプレートを使用する**および **IKE** 設定によって異なります。
7. **テンプレート名**欄に、テンプレートの名前を入力します（最大 16 文字）。
8. **テンプレートを使用する**ドロップダウンリストで**カスタム**を選択した場合、**IKE** を選択してから、必要に応じて設定値を変更します。
9. **OK** をクリックします。

使用中のテンプレートの設定を変更する場合は、本製品を再起動して設定を有効にします。

関連情報

- IPsec を使用する
  - IPsec テンプレートの IKEv1 の設定
  - IPsec テンプレートの IKEv2 設定
  - IPsec テンプレートの手動設定

IPsec テンプレートの IKEv1 の設定

オプション	詳細
テンプレート名	作成するテンプレートの名前を入力します（最大 16 文字）。
テンプレートを使用する	**カスタム**、**IKEv1 高セキュリティ**または **IKEv1 中セキュリティ**を選択します。設定項目は、選択したテンプレートにより異なります。
IKE	IKE は通信プロトコルであり、IPsec を使用して暗号化通信を行うための暗号キーの交換に使用されます。1 回限りの暗号化通信を実行するために、IPsec に必要な暗号化アルゴリズムが決定され、暗号化キーは共有されます。IKE の場合、暗号化キーは Diffie-Hellman キー交換方式を使用して交換され、IKE に制限された暗号化通信が実行されます。 **テンプレートを使用する**で**カスタム**を選択した場合、**IKEv1** を選択します。
認証タイプ	• **DH グループ** このキー交換方式により、保護されていないネットワーク上で、秘密キーを安全に交換することができます。Diffie-Hellman キー交換方式では、秘密キーではなく離散対数問題を利用して、乱数および秘密キーを使って生成された公開情報が送受信されます。 **グループ 1**、**グループ 2**、**グループ 5**、または**グループ 14** を選択します。 • **暗号化方式** **DES**、**3DES**、**AES-CBC 128**、または **AES-CBC 256** を選択します。 • **ハッシュ** **MD5**、**SHA1**、**SHA256**、**SHA384**、または **SHA512** を選択します。 • **SA ライフタイム** IKE SA のライフタイムを指定します。 時間（秒）とキロバイト数（KByte）を入力します。
動作セキュリティ	• **プロトコル** **ESP**、**AH**、または **AH+ESP** を選択します。 - ESP は、IPsec を使用して暗号化通信を行うためのプロトコルの 1 つです。ESP は、ペイロード（通信内容）を暗号化し、付加情報を追加します。IP パケットは、ヘッダーと、ヘッダーに続く暗号化されたペイロードで構成されます。IP パケットには、暗号化されたデータに加え、暗号化方式、暗号化キー、認証データなどに関する情報も含まれます。 - AH は、送信者を認証する IPsec プロトコルの一部であり、データの改ざんを防止します（完全性を保証します）。IP パケットでは、データはヘッダーの直後に挿入されます。また、送信者のなりすましやデータの改ざんを防止するために、パケットには、通信内容に含まれる等式を使用して計算されたハッシュ値や秘密キーなどが含まれます。ESP と異なり、通信内容は暗号化されず、データはプレーンテキストとして送受信されます。 • **暗号化方式（AH オプションでは選択不可）。** **DES**、**3DES**、**AES-CBC 128**、または **AES-CBC 256** を選択します。 • **ハッシュ** **なし**、**MD5**、**SHA1**、**SHA256**、**SHA384** または **SHA512** を選択します。 **プロトコル**で **ESP** が選択されている場合にのみ、**なし**を選択できます。

オプション	詳細
	• **SA ライフタイム** IKE SA のライフタイムを指定します。 時間（秒）とキロバイト数（KByte）を入力します。 • **動作モード** **トランスポート**または**トンネル**を選択します。 • **リモートルーター IP アドレス** リモートルーターの IP アドレス（IPv4 または IPv6）を入力します。この情報は、**トンネル**モードが選択されている場合にのみ入力します。 SA（セキュリティアソシエーション）は、IPsec または IPv6 を使用する暗号化通信方式です。通信の開始前に安全な通信チャネルを確立するために、暗号化方式や暗号化キーなどの情報を交換、共有します。SA は、すでに確立された仮想的な暗号通信路（トンネル）を指す場合もあります。IPsec による通信で使用される SA では、暗号化方式を確立し、キーを交換して、IKE（インターネットキー交換）の標準手続に従って相互認証を行います。さらに、SA は定期的に更新されます。
PFS	PFS では、メッセージの暗号化に使用された以前のキーからキーは導出されません。また、親キーから導出されたキーでメッセージが暗号化されている場合でも、その親キーを使用して他のキーが導出されることはありません。そのため、キーの情報が洩れた場合でも、被害はそのキーを使用して暗号化されたメッセージだけに限られます。 **有効**または**無効**を選択します。
認証方式	認証方式を選択します。**事前共有キー**または**証明書**を選択します。
事前共有キー	通信を暗号化する際に、事前に別の通信路を使用して暗号化キーが交換および共有されます。 **認証方式**で**事前共有キー**を選択した場合は、**事前共有キー**（最大 32 文字）を入力します。 • **ローカル/ID タイプ/ID** 送信者の ID タイプを選択し、ID を入力します。 タイプとして、**IPv4 アドレス**、**IPv6 アドレス**、**FQDN**、**E-mail アドレス**、または**証明書**を選択します。 **証明書**を選択した場合は、**ID** 欄に証明書の共通名を入力します。 • **リモート/ID タイプ/ID** 受信者の ID タイプを選択し、その ID を入力します。 タイプとして、**IPv4 アドレス**、**IPv6 アドレス**、**FQDN**、**E-mail アドレス**、または**証明書**を選択します。 **証明書**を選択した場合は、**ID** 欄に証明書の共通名を入力します。
証明書	**認証方式**で**証明書**を選択した場合、証明書を選択します。 選択できる証明書は、Web Based Management のセキュリティ設定画面の**証明書**ページを使用して作成された証明書のみです。

関連情報

- Web Based Management を使用して IPsec テンプレートを設定する

IPsec テンプレートの IKEv2 設定

オプション	詳細
テンプレート名	作成するテンプレートの名前を入力します（最大 16 文字）。
テンプレートを使用する	**カスタム**、**IKEv2 高セキュリティ**または **IKEv2 中セキュリティ**を選択します。設定項目は、選択したテンプレートにより異なります。
IKE	IKE は通信プロトコルであり、IPsec を使用して暗号化通信を行うための暗号キーの交換に使用されます。1 回限りの暗号化通信を実行するために、IPsec に必要な暗号化アルゴリズムが決定され、暗号化キーは共有されます。IKE の場合、暗号化キーは Diffie-Hellman キー交換方式を使用して交換され、IKE に制限された暗号化通信が実行されます。 **テンプレートを使用する**で**カスタム**を選択した場合、**IKEv2** を選択します。
認証タイプ	• **DH グループ** このキー交換方式により、保護されていないネットワーク上で、秘密キーを安全に交換することができます。Diffie-Hellman キー交換方式では、秘密キーではなく離散対数問題を利用して、乱数および秘密キーを使って生成された公開情報が送受信されます。 **グループ 1**、**グループ 2**、**グループ 5**、または**グループ 14** を選択します。 • **暗号化方式** **DES**、**3DES**、**AES-CBC 128**、または **AES-CBC 256** を選択します。 • **ハッシュ** **MD5**、**SHA1**、**SHA256**、**SHA384**、または **SHA512** を選択します。 • **SA ライフタイム** IKE SA のライフタイムを指定します。 時間（秒）とキロバイト数（KByte）を入力します。
動作セキュリティ	• **プロトコル** **ESP** を選択します。 ESP は、IPsec を使用して暗号化通信を行うためのプロトコルの 1 つです。ESP は、ペイロード（通信内容）を暗号化し、付加情報を追加します。IP パケットは、ヘッダーと、ヘッダーに続く暗号化されたペイロードで構成されます。IP パケットには、暗号化されたデータに加え、暗号化方式、暗号化キー、認証データなどに関する情報も含まれます。 • **暗号化方式** **DES**、**3DES**、**AES-CBC 128**、または **AES-CBC 256** を選択します。 • **ハッシュ** **MD5**、**SHA1**、**SHA256**、**SHA384**、または **SHA512** を選択します。 • **SA ライフタイム** IKE SA のライフタイムを指定します。 時間（秒）とキロバイト数（KByte）を入力します。 • **動作モード** **トランスポート**または**トンネル**を選択します。

オプション	詳細
	• **リモートルーター IP アドレス** リモートルーターの IP アドレス（IPv4 または IPv6）を入力します。この情報は、**トンネル**モードが選択されている場合にのみ入力します。 SA（セキュリティアソシエーション）は、IPsec または IPv6 を使用する暗号化通信方式です。通信の開始前に安全な通信チャネルを確立するために、暗号化方式や暗号化キーなどの情報を交換、共有します。SA は、すでに確立された仮想的な暗号通信路（トンネル）を指す場合もあります。IPsec による通信で使用される SA では、暗号化方式を確立し、キーを交換して、IKE（インターネットキー交換）の標準手続に従って相互認証を行います。さらに、SA は定期的に更新されます。
PFS	PFS では、メッセージの暗号化に使用された以前のキーからキーは導出されません。また、親キーから導出されたキーでメッセージが暗号化されている場合でも、その親キーを使用して他のキーが導出されることはありません。そのため、キーの情報が洩れた場合でも、被害はそのキーを使用して暗号化されたメッセージだけに限られます。 **有効**または**無効**を選択します。
認証方式	認証方式を選択します。**事前共有キー**、**証明書**、**EAP - MD5**、または **EAP - MS-CHAPv2** を選択します。 EAP は、PPP を拡張した認証プロトコルです。EAP を使用した IEEE802.1x 認証では、セッションごとに異なるキーを使用してユーザー認証が行われます。 以下の設定は、**認証方式**で **EAP - MD5** または **EAP - MS-CHAPv2** が選択されている場合にのみ必要です。 • **モード** **サーバーモード**または**クライアントモード**を選択します。 • **証明書** 証明書を選択します。 • **ユーザー名** ユーザー名を入力します（最大 32 文字）。 • **パスワード** パスワードを入力します（最大 32 文字）。確認のため、パスワードは 2 回入力します。
事前共有キー	通信を暗号化する際に、事前に別の通信路を使用して暗号化キーが交換および共有されます。 **認証方式**で**事前共有キー**を選択した場合は、**事前共有キー**（最大 32 文字）を入力します。 • **ローカル/ID タイプ/ID** 送信者の ID タイプを選択し、ID を入力します。 タイプとして、**IPv4 アドレス**、**IPv6 アドレス**、**FQDN**、**E-mail アドレス**、または**証明書**を選択します。 **証明書**を選択した場合は、**ID** 欄に証明書の共通名を入力します。 • **リモート/ID タイプ/ID** 受信者の ID タイプを選択し、その ID を入力します。 タイプとして、**IPv4 アドレス**、**IPv6 アドレス**、**FQDN**、**E-mail アドレス**、または**証明書**を選択します。 **証明書**を選択した場合は、**ID** 欄に証明書の共通名を入力します。
証明書	**認証方式**で**証明書**を選択した場合、証明書を選択します。

オプション	詳細
	選択できる証明書は、Web Based Management のセキュリティ設定画面の**証明書**ページを使用して作成された証明書のみです。

関連情報

- Web Based Management を使用して IPsec テンプレートを設定する

IPsec テンプレートの手動設定

オプション	詳細
テンプレート名	作成するテンプレートの名前を入力します（最大 16 文字）。
テンプレートを使用する	**カスタム**を選択します。
IKE	IKE は通信プロトコルであり、IPsec を使用して暗号化通信を行うための暗号キーの交換に使用されます。1 回限りの暗号化通信を実行するために、IPsec に必要な暗号化アルゴリズムが決定され、暗号化キーは共有されます。IKE の場合、暗号化キーは Diffie-Hellman キー交換方式を使用して交換され、IKE に制限された暗号化通信が実行されます。 **手動**を選択します。
認証キー（ESP, AH）	**In/Out** 値を入力します。 こうした設定は、**テンプレートを使用する**に**カスタム**が選択され、**IKE** に**手動**が選択され、**動作セキュリティ**セクションの**ハッシュ**に**なし**以外の設定が選択されているときに必要です。 設定可能な文字数は、**動作セキュリティ**セクションで**ハッシュ**に選択した設定によって異なります。 指定した認証キーの長さが、選択したハッシュアルゴリズムの長さと一致していない場合、エラーとなります。 • **MD5**：128 ビット（16 バイト） • **SHA1**：160 ビット（20 バイト） • **SHA256**：256 ビット（32 バイト） • **SHA384**：384 ビット（48 バイト） • **SHA512**：512 ビット（64 バイト） キーをアスキーコードで指定する場合は、文字を二重引用符（"）で囲みます。
コードキー（ESP）	**In/Out** 値を入力します。 こうした設定は、**テンプレートを使用する**で**カスタム**が選択され、**IKE** で**手動**が選択され、**動作セキュリティ**の**プロトコル**で **ESP** が選択されているときに必要です。 設定可能な文字数は、**動作セキュリティ**セクションで**暗号化方式**に選択した設定によって異なります。 指定したコードキーの長さが、選択した暗号化アルゴリズムの長さと一致していない場合、エラーとなります。 • **DES**：64 ビット（8 バイト） • **3DES**：192 ビット（24 バイト） • **AES-CBC 128**：128 ビット（16 バイト） • **AES-CBC 256**：256 ビット（32 バイト） キーをアスキーコードで指定する場合は、文字を二重引用符（"）で囲みます。
SPI	セキュリティ情報を識別するためのパラメーターです。複数の種類の IPsec 通信に対応するために、通常、ホストには複数の SA（Security Association）が用意されています。したがって、IPsec パケットを受信したときに、該当する SA を識別する必要があります。SPI パラメーター（SA を識別する）は、AH（認証ヘッダー）と ESP（Encapsulated Security Payload、暗号ペイロード）ヘッダーに含まれます。 こうした設定は、**テンプレートを使用する**に**カスタム**が選択され、**IKE** に**手動**が選択されているときに必要です。 **In/Out** 値を入力します。（3～10 文字）

オプション	詳細
動作セキュリティ	• **プロトコル** **ESP** または **AH** を選択します。 - ESP は、IPsec を使用して暗号化通信を行うためのプロトコルの 1 つです。ESP は、ペイロード（通信内容）を暗号化し、付加情報を追加します。IP パケットは、ヘッダーと、ヘッダーに続く暗号化されたペイロードで構成されます。IP パケットには、暗号化されたデータに加え、暗号化方式、暗号化キー、認証データなどに関する情報も含まれます。 - AH は IPsec プロトコルの一部であり、送信元の認証やデータの改ざん防止（完全性の保証）を実現します。IP パケットでは、データはヘッダーの直後に挿入されます。また、送信者のなりすましやデータの改ざんを防止するために、パケットには、通信内容に含まれる等式を使用して計算されたハッシュ値や秘密キーなどが含まれます。ESP と異なり、通信内容は暗号化されず、データはプレーンテキストとして送受信されます。 • **暗号化方式（AH オプションでは選択不可）。** **DES**、**3DES**、**AES-CBC 128**、または **AES-CBC 256** を選択します。 • **ハッシュ** **なし**、**MD5**、**SHA1**、**SHA256**、**SHA384** または **SHA512** を選択します。 **プロトコル**で **ESP** が選択されている場合にのみ、**なし**を選択できます。 • **SA ライフタイム** IKE SA のライフタイムを指定します。 時間（秒）とキロバイト数（KByte）を入力します。 • **動作モード** **トランスポート**または**トンネル**を選択します。 • **リモートルーター IP アドレス** リモートルーターの IP アドレス（IPv4 または IPv6）を入力します。この情報は、**トンネル**モードが選択されている場合にのみ入力します。 SA（セキュリティアソシエーション）は、IPsec または IPv6 を使用する暗号化通信方式です。通信の開始前に安全な通信チャネルを確立するために、暗号化方式や暗号化キーなどの情報を交換、共有します。SA は、すでに確立された仮想的な暗号通信路（トンネル）を指す場合もあります。IPsec による通信で使用される SA では、暗号化方式を確立し、キーを交換して、IKE（インターネットキー交換）の標準手続に従って相互認証を行います。さらに、SA は定期的に更新されます。

関連情報

- Web Based Management を使用して IPsec テンプレートを設定する

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

ユーザー認証

- Active Directory 認証を使用する
- LDAP 認証を使用する
- セキュリティ機能ロック 3.0 を使用する

Active Directory 認証を使用する

- Active Directory 認証について
- Web Based Management を使用して Active Directory 認証を設定する
- 本製品にログインし、操作パネルを使用して設定値を変更する（Active Directory 認証）

Active Directory 認証について

Active Directory 認証により、本製品の使用が制限されます。Active Directory 認証が有効の場合、本製品の操作パネルはロックされます。本製品の設定を変更するには、ユーザー ID とパスワードを入力する必要があります。

Active Directory 認証では、以下の機能が利用可能です。

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。

- 受信印刷データを保存する
- 受信ファクスデータを保存する
- スキャンしたデータを E-mail サーバーに送信する場合、ユーザー ID に基づいて Active Directory サーバーから E-mail アドレスが取得されます。

  この機能を使用するには、**メールアドレス取得**設定で**オン**オプションを選択して、**LDAP + kerberos** または **LDAP + NTLMv2** 認証方式を選択します。本製品がスキャンデータを E-mail サーバーに送信する際に、ご使用の E-mail アドレスが送信者として設定されます。または、スキャンデータをご使用の E-mail アドレスに送信する場合には、受信者として設定されます。

Active Directory 認証が有効の場合、本製品にはすべての受信ファクスデータが保存されます。ログイン後、製品は保存されたファクスデータを印刷します。

Active Directory 認証の設定は、Web Based Management を使用して変更できます。

関連情報

- Active Directory 認証を使用する

Web Based Management を使用して Active Directory 認証を設定する

Active Directory 認証は、Kerberos 認証および NTLMv2 認証をサポートしています。認証のための SNTP プロトコル（ネットワークタイムサーバー）と DNS サーバー構成を設定する必要があります。

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. 左側にあるナビゲーションバーで、**管理者設定** > **制限機能**または**制限管理**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. **Active Directory 認証**を選択します。
6. **OK** をクリックします。
7. **Active Directory 認証**をクリックします。
8. 次の設定を行います。

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。

オプション	詳細
ファクス受信データ蓄積	このオプションを選択して、受信ファクスデータを保存します。製品へのログオン後、すべての受信ファクスデータを印刷できます。
ユーザー ID を記憶	このオプションを選択して、ユーザー ID を保存します。
Active Directory サーバアドレス	Active Directory サーバーの IP アドレスまたはサーバー名（例：ad.example.com）を入力します。
Active Directory ドメイン名	Active Directory のドメイン名を入力します。
プロトコルと認証方式	プロトコルと認証方式を選択します。
SSL/TLS	**SSL/TLS** オプションを選択します（**LDAP + kerberos** または **LDAP + NTLMv2** 認証方式の場合のみ有効）。
LDAP ポート	ポート番号を入力して LDAP 経由で Active Directory サーバーに接続します。（**LDAP + kerberos** または **LDAP + NTLMv2** 認証方式の場合のみ可能）
LDAP 検索場所	LDAP 検索ルートを入力します。（**LDAP + kerberos** または **LDAP + NTLMv2** 認証方式の場合のみ可能）
メールアドレス取得	このオプションを使用して、Active Directory サーバーからログオンユーザーの E メールアドレスを取得します。（**LDAP + kerberos** または **LDAP + NTLMv2** 認証方式の場合のみ可能）

オプション	詳細
ユーザーのホームディレクトリ取得	このオプションを選択して、スキャン to ネットワークファイルの送信先のホームディレクトリーを取得します。（**LDAP + kerberos** または **LDAP + NTLMv2** 認証方式の場合のみ可能）

9. **OK** をクリックします。

関連情報

- Active Directory 認証を使用する

本製品にログインし、操作パネルを使用して設定値を変更する（Active Directory 認証）

Active Directory 認証が有効の場合、本製品の操作パネルにユーザー ID とパスワードが入力されるまで、操作パネルはロックされた状態となります。

1. 製品の操作パネルでユーザー ID とパスワードを入力して、ログオンします。
2. 認証が成功すると、製品の操作パネルのロックが解除されます。

関連情報

- Active Directory 認証を使用する

LDAP 認証を使用する

- LDAP 認証について
- Web Based Management を使用して LDAP 認証を設定する
- 本製品にログインし、操作パネルを使用して設定値を変更する（LDAP 認証）

LDAP 認証について

LDAP 認証により、本製品の使用が制限されます。LDAP 認証が有効の場合、本製品の操作パネルはロックされます。本製品の設定を変更するには、ユーザー ID とパスワードを入力する必要があります。

LDAP 認証では以下の機能が提供されます。

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。

- 受信印刷データを保存する
- 受信ファクスデータを保存する
- スキャンしたデータを E-mail サーバーに送信する場合、ユーザー ID に基づいて LDAP サーバーから E-mail アドレスが取得されます。

  この機能を使用するには、**メールアドレス取得**設定で**オン**オプションを選択します。本製品がスキャンデータを E-mail サーバーに送信する際に、ご使用の E-mail アドレスが送信者として設定されます。または、スキャンデータをご使用の E-mail アドレスに送信する場合には、受信者として設定されます。

LDAP 認証が有効の場合、本製品にはすべての受信ファクスデータが保存されます。ログイン後、製品は保存されたファクスデータを印刷します。

LDAP 認証設定は、Web Based Management を使用して変更できます。

関連情報

- LDAP 認証を使用する

Web Based Management を使用して LDAP 認証を設定する

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. 左側にあるナビゲーションバーで、**管理者設定** > **制限機能**または**制限管理**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. **LDAP 認証**を選択します。
6. **OK** をクリックします。
7. **LDAP 認証**メニューをクリックします。
8. 次の設定を行います。

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。

オプション	詳細
ファクス受信データ蓄積	このオプションを選択して、受信ファクスデータを保存します。製品へのログオン後、すべての受信ファクスデータを印刷できます。
ユーザー ID を記憶	このオプションを選択して、ユーザー ID を保存します。
LDAP アドレス	LDAP サーバーの IP アドレスまたはサーバー名（例：ldap.example.com）を入力します。
SSL/TLS	LDAP over SSL/TLS を使用するには、**SSL/TLS** オプションを選択します。
LDAP ポート	LDAP サーバーのポート番号を入力します。
LDAP 検索場所	LDAP 検索のルートディレクトリを入力します。
名前属性名 (検索する属性)	検索キーとする属性を入力します。
メールアドレス取得	このオプションを使用して、LDAP サーバーからログオンユーザーの E メールアドレスを取得します。
ユーザーのホームディレクトリ取得	このオプションを選択して、スキャン to ネットワークファイルの送信先のホームディレクトリーを取得します。

9. **OK** をクリックします。

関連情報

- LDAP 認証を使用する

本製品にログインし、操作パネルを使用して設定値を変更する（LDAP 認証）

LDAP 認証が有効の場合、本製品の操作パネルにユーザー ID とパスワードが入力されるまで、操作パネルはロックされた状態となります。

1. 製品の操作パネルでユーザー ID とパスワードを入力して、ログオンします。
2. 認証が成功すると、製品の操作パネルのロックが解除されます。

関連情報

- LDAP 認証を使用する

セキュリティ機能ロック 3.0 を使用する

セキュリティ機能ロック 3.0 は、本製品で利用できる機能を制限し、安全性を高めます。

セキュリティ機能ロック 3.0 を使用する前に

セキュリティ機能ロックを使用してパスワードを設定し、特定のユーザーページへのアクセスを設定して、以下の機能の一部または全部へのアクセスを許可します。

Web Based Management を使用して、以下のセキュリティ機能ロック 3.0 設定値の設定や変更を行うことができます。

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。

- **印刷**
- **コピー**
- **スキャン**
- **ファックス**
- **メディア**
- **USB**
- **クラウド接続**
- **お役立ちツール**
- **枚数制限**
- **ページカウンター**
- **カード ID**

タッチパネル液晶ディスプレーモデル：

セキュリティ機能ロックが有効な場合、本製品は自動的にパブリックモードになり、本製品の機能の一部が許可されたユーザーのみに制限されるようになります。制限された本製品の機能にアクセスするには、  を押し、ユーザー名を選択し、パスワードを入力します。

関連情報

- セキュリティ機能ロック 3.0 を使用する

Web Based Management を使用してセキュリティ機能ロック 3.0 を設定する

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. 左側にあるナビゲーションバーで、**管理者設定** > **制限機能**または**制限管理**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. **セキュリティ機能ロック**を選択します。
6. **OK** をクリックします。
7. **機能制限**メニューをクリックします。
8. ユーザーまたはグループごとの制限の管理設定を確認します。
9. **OK** をクリックします。
10. **ユーザーリスト**メニューをクリックします。
11. ユーザーリストを設定します。
12. **OK** をクリックします。

セキュリティ機能ロックメニューでユーザーリストのロックアウト設定を変更することもできます。

関連情報

- セキュリティ機能ロック 3.0 を使用する

セキュリティ機能ロック 3.0 を使用してスキャンする

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。

スキャン制限を設定する（管理者向け）

セキュリティ機能ロック 3.0 を使用すると、管理者はスキャンを許可するユーザーを制限できます。パブリックユーザー設定でスキャン機能がオフに設定されている場合、**スキャン**チェックボックスが選択されているユーザーだけがスキャンを実行できます。

スキャン機能を使用する（制限されたユーザー向け）

- 本製品の操作パネルを使用してスキャンする場合：

  制限されたユーザーは、操作パネルでパスワードを入力してスキャンモードにアクセスする必要があります。
- パソコンからスキャンする場合：

  制限されたユーザーは、各自のパソコンからスキャンする前に、操作パネルでパスワードを入力する必要があります。操作パネルでパスワードが入力されなかった場合、ユーザーのパソコンにエラーメッセージが表示されます。

本製品が IC カード認証に対応している場合、制限されたユーザーは、登録済みの IC カードを本製品の操作パネルの NFC タッチ部分にタッチすることで、スキャンモードにアクセスすることもできます。

関連情報

- セキュリティ機能ロック 3.0 を使用する

セキュリティ機能ロック 3.0 のパブリックモードを設定する

セキュリティ機能ロック画面を使用してパブリックモードを設定します。これにより、パブリックユーザーに利用可能な機能が制限されます。パブリックユーザーは、パブリックモード設定により利用可能となった機能に、パスワードの入力なしでアクセスできます。

パブリックモードの対象は、Brother iPrint&Scan および Brother Mobile Connect を介して送信される印刷ジョブなどです。

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. 左側にあるナビゲーションバーで、**管理者設定** > **制限機能**または**制限管理**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. **セキュリティ機能ロック**を選択します。
6. **OK** をクリックします。
7. **機能制限**メニューをクリックします。
8. **一般モード**行で、チェックボックスを選択して一覧表示されている機能を許可するか、チェックボックスの選択を解除してこれらの機能を制限します。
9. **OK** をクリックします。

関連情報

- セキュリティ機能ロック 3.0 を使用する

Web Based Management を使用して個人用ホーム画面を設定する

管理者として、ユーザーが個人用ホーム画面に表示できるタブを指定することができます。これらのタブは、ユーザーがお気に入りのショートカットに素早くアクセスするためのもので、ユーザーは操作パネルから個人用ホーム画面のタブに割り当てることができます。

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。

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. 左側にあるナビゲーションバーで、**管理者設定** > **制限機能**または**制限管理**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. **セキュリティ機能ロック**を選択します。
6. **タブ設定**欄で、個人用ホーム画面として使用するタブ名に**個人**を選択します。
7. **OK** をクリックします。
8. **機能制限**メニューをクリックします。
9. ユーザーまたはグループごとの制限の管理設定を確認します。
10. **OK** をクリックします。
11. **ユーザーリスト**メニューをクリックします。
12. ユーザーリストを設定します。
13. ユーザーごとにドロップダウンリストから**ユーザーリスト/機能制限**を選択します。
14. ユーザーごとに**待機画面**ドロップダウンリストからタブ名を選択します。
15. **OK** をクリックします。

関連情報

- セキュリティ機能ロック 3.0 を使用する

セキュリティ機能ロック 3.0 その他の機能について

セキュリティ機能ロック画面で以下の機能を設定します。

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。

すべてのカウンターをリセット/ カウンターリセット

すべてのカウンターをリセットするには、**ページカウンター**列の**すべてのカウンターをリセット**または**カウンターリセット**をクリックします。

選択されたカウンターをリセット

選択したカウンターをリセットするには、**ページカウンター**列の**選択されたカウンターをリセット**をクリックします。

CSV ファイルへ出力

CSV ファイルへ出力をクリックして、**ユーザーリスト/機能制限**情報を含む現在および前回のページカウンターを、CSV ファイルとしてエクスポートします。

カード ID

ユーザーリストメニューをクリックして、**カード ID** 欄にユーザーのカード ID を入力します。IC カードを認証に使用できます。

排紙トレイ設定

メールボックスユニットが本製品に取り付けられている場合は、ドロップダウンリストから各ユーザーの出力トレイを選択します。

前回ログ

カウンターをリセットした後でページ数を確認したい場合は、**前回ログ**をクリックします。

カウンター自動リセット

カウンター自動リセットをクリックして、ページカウンターのリセット間隔を設定します。毎日、毎週、毎月のいずれかを選択します。

関連情報

- セキュリティ機能ロック 3.0 を使用する

本製品の操作パネルを使用して新しい IC カードを登録する

IC カード（集積回路カード）を製品に登録することができます。

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。

1. 登録済みの IC カード（集積回路カード）を、本製品の操作パネルの NFC（近距離無線通信）タッチ部分にタッチします。
2. 画面でユーザー ID を押します。
3. カード登録ボタンを押します。
4. 新しい IC カードを NFC タッチ部分にタッチします。
   新しい IC カードの番号が本製品に登録されます。
5. OK ボタンを押します。

関連情報

- セキュリティ機能ロック 3.0 を使用する

外付け IC カードリーダーを登録する

外付け IC（集積回路）カードリーダーを接続する場合は、Web Based Management でカードリーダーを登録してください。本製品は外付け IC カードリーダーに対応する HID クラスのドライバーをサポートしています。

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、**管理者設定** > **外付けカードリーダー**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. 必要な情報を入力し、**OK** をクリックします。
6. 本製品を再起動して、設定を有効にします。
7. カードリーダーを本製品に接続します。
8. カード認証を使用するときに、カードをカードリーダーにタッチします。

関連情報

- セキュリティ機能ロック 3.0 を使用する

E メールを安全に送受信する

Web Based Management を使用して E メール送信または受信の設定を行う

- E メール受信は、特定モデルのみ対応しています。
- Web Based Management を使用して、安全なユーザー認証付き E メール送信の設定、または SSL/TLS を使用した E メール送受信の設定を行うことを推奨します（サポート対象モデルのみ）。

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. **POP3/IMAP4/SMTP クライアント**欄で、**詳細設定**をクリックして、**POP3/IMAP4/SMTP クライアント**の状態が**有効**であることを確認します。

   - 使用可能なプロトコルは、お使いの製品によって異なる場合があります。
   - **認証方式**選択画面が表示された場合は、お使いの認証方式を選択し、画面の指示に従います。
6. **POP3/IMAP4/SMTP クライアント**の設定を行います。
   - テストメールを送信して、E-mail の設定値が正しいことを確認します。
   - POP3/IMAP4/SMTP サーバーの設定値が不明の場合は、ネットワーク管理者または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。
7. 完了後、**OK** をクリックします。

   E メール送信／受信設定のテストダイアログボックスが表示されます。
8. ダイアログボックスに表示される指示に従って、現在の設定値をテストします。

関連情報

- E メールを安全に送受信する

関連トピック：

- SSL/TLS を使用して E メールを安全に送受信する

ユーザー認証を使用して E メールを送信する

本製品は、ユーザー認証を必要とする E メールサーバーを経由して E メールを送信します。この方式により、非認証のユーザーによる E メールサーバーへのアクセスが防止されます。

ユーザー認証を使用して、E メール通知、E メールレポート、および I-Fax（特定のモデルのみ対応）を送信することができます。

- 使用可能なプロトコルは、お使いの製品によって異なる場合があります。
- Web Based Management を使用して SMTP 認証を設定することをお勧めします。

E-mail サーバー設定

本製品の SMTP 認証方式を、お使いの E-mail サーバーが使用する方式と一致するように設定する必要があります。お使いの E-mail サーバーの設定については、ネットワーク管理者または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。

Web Based Management を使用して SMTP サーバー認証を有効にするには、**POP3/IMAP4/SMTP クライアント**画面の**送信メールサーバー認証方式**で使用する認証方式を選択します。

関連情報

- E メールを安全に送受信する

SSL/TLS を使用して E メールを安全に送受信する

本製品では SSL/TLS 通信方式をサポートしています。SSL/TLS 通信を使用している E-mail サーバーを使用するには、次の設定が必要です。

- E メール受信は、特定モデルのみ対応しています。
- Web Based Management を使用して SSL/TLS を設定することを推奨します。

サーバー証明書を検証する

SSL/TLS で、 **SSL** または **TLS** を選択している場合、 **サーバー証明書を検証** チェックボックスが自動的に選択されます。

- 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。CA 証明書のインポートの必要性について確認するには、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。
- サーバー証明書を検証する必要がない場合は、**サーバー証明書を検証**チェックボックスの選択を解除してください。

ポート番号

SSL または **TLS** を選択すると、**ポート**値がプロトコルと一致するように変更されます。手動でポート番号を変更するには、**SSL/TLS** 設定を選択した後、ポート番号を入力します。

本製品の通信方式を、お使いの E-mail サーバーで使用されている方式に合わせて設定する必要があります。お使いの E-mail サーバーの設定については、ネットワーク管理者または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。

ほとんどの場合、安全なウェブメールサービスには次の設定が必要です。

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。

SMTP	**ポート**	587
	送信メールサーバー認証方式	**SMTP-AUTH**
	SSL/TLS	**TLS**
POP3	**ポート**	995
	SSL/TLS	**SSL**
IMAP4	**ポート**	993
	SSL/TLS	**SSL**

関連情報

- E メールを安全に送受信する

関連トピック：

- Web Based Management を使用して E メール送信または受信の設定を行う
- デバイスセキュリティの証明書を設定する

ネットワークへの印刷ログ保存機能

印刷ログ機能の概要

印刷ログ機能を使用すると、共通インターネットファイルシステム（CIFS：Common Internet File System）プロトコルを使用して、本製品からネットワークサーバーへ印刷ログファイルを保存できます。すべての印刷ジョブの、ID、印刷ジョブのタイプ、ジョブ名、ユーザー名、日付、時間、および印刷ページ数を記録できます。CIFSは、TCP/IP で動作するプロトコルであり、ネットワーク上のパソコンはインターネットまたはイントラネット経由でファイルを共有することができます。

以下の印刷機能が印刷ログに記録されます。

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。

- お使いのパソコンからの印刷ジョブ
- USB ダイレクトプリント
- コピー
- 受信ファクス
- クラウド接続印刷

- 印刷ログのネットワークへの保存の機能は、Kerberos 認証および NTLMv2 認証をサポートしています。認証のために、SNTP プロトコル（ネットワークタイムサーバー）を設定するか、操作パネルで日時とタイムゾーンを正確に設定する必要があります。
- ファイルをサーバーに保存する際に、ファイルタイプを TXT または CSV に設定できます。

関連情報

- ネットワークへの印刷ログ保存機能

Web Based Management を使用して印刷ログ機能の設定値を設定する

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、**管理者設定** > **印刷ログ機能設定**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. **印刷ログ**欄で、**オン**をクリックします。
6. 次の設定を行います。

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。

オプション	詳細
ネットワークフォルダパス	CIFS サーバー上の印刷ログの保存先フォルダー（例：\\ComputerName\SharedFolder）を入力します。
ファイル名	印刷ログに使用するファイル名を入力します（最大 32 文字）。
ファイル形式	印刷ログのファイルタイプに、**テキスト形式**または **CSV 形式**を選択します。
ログの時間情報	印刷ログのタイムソースを選択します。
認証方法	CIFS サーバーにアクセスするために必要な認証方式として、**自動**、**Kerberos**、または **NTLMv2** を選択します。Kerberos は認証プロトコルです。このプロトコルにより、機器または個人がそれぞれのアイデンティティーを、シングルサインオンを使用するネットワークサーバーに対して安全に示すことができます。NTLMv2 はサーバーにログインするための認証方式であり、Windows により使用されます。 • **自動**：**自動**を選択した場合、認証方式には NTLMv2 が使用されます。 • **Kerberos**：**Kerberos** オプションを選択すると、Kerberos 認証のみが使用されます。 • **NTLMv2**：**NTLMv2** オプションを選択すると、NTLMv2 認証のみが使用されます。 • **Kerberos** および **NTLMv2** 認証の場合、**時計設定**または、SNTP プロトコル（ネットワークタイムサーバー）と DNS サーバーも設定する必要があります。 • 本製品の操作パネルから時計を設定することもできます。
ユーザー名	認証のためのユーザー名を入力します（最大 96 文字）。 ユーザー名がドメインの一部である場合、ユーザー@ドメインまたは、ドメイン\ユーザーのいずれかの形式でユーザー名を入力します。

オプション	詳細
パスワード	認証のためのパスワードを入力します（最大 32 文字）。
Kerberos サーバーアドレス（必要に応じて）	KDC（Key Distribution Center）のホストアドレス（例：kerberos.example.com、最大 64 文字）または、IP アドレス（例：192.168.56.189）を入力します。
書き込みエラー時設定	ネットワークエラーのために印刷ログをサーバーに保存できない場合の対処方法を選択します。

7. **接続状態**欄で、最新のログステータスを確認します。

   また、本製品の画面でエラー状態を確認することもできます。

8. **OK** をクリックし、 **印刷ログ機能テスト** ページを表示します。

   設定をテストするには、**はい**をクリックして、次の手順に進みます。

   テストを行わずに次へ進むには、 **いいえ**をクリックします。設定値は自動的にサブミットされます。

9. 製品が設定値をテストします。
10. 設定が承認されると、**テスト成功**がページに表示されます。

    テストエラー が表示された場合は、すべての設定値を確認し、 **OK** をクリックして、もう一度テストページを表示します。

関連情報

- ネットワークへの印刷ログ保存機能

印刷ログ機能のエラー検出設定を使用する

エラー検出設定を使用して、ネットワークエラーのために印刷ログをサーバーに保存できない場合の対処方法を決定します。

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、**管理者設定** > **印刷ログ機能設定**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. **書き込みエラー時設定**セクションで、**印刷中止**または**ログを書き込まずに印刷**オプションを選択します。

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。

オプション	詳細
印刷中止	**印刷中止**を選択すると、印刷ログがサーバーに保存できない場合、印刷ジョブはキャンセルされます。 **印刷中止**オプションを選択した場合でも、本製品は受信ファクスを印刷します。

ログを書き込まずに印刷	**ログを書き込まずに印刷**を選択すると、印刷ログがサーバーに保存できない場合でも、本製品は文書を印刷します。
	印刷ログ機能が回復すると、印刷ログは以下のように記録されます。
	`Id, Type, Job Name, User Name, Date, Time, Print Pages`
	`1, Print(xxxxxxx), "Document01.doc", "user01", 03/03/20xx, 14:01:32, 52`
	`2, Print(xxxxxxx), "Document02.doc", "user01", 03/03/20xx, 14:45:30, ?` (a)
	`3, <Error>, ?, ?, ?, ?, ?` (b)
	`4, Print(xxxxxxx), "Report01.xls", "user02", 03/03/20xx, 19:30:40, 4`
	a. 印刷の最後で印刷ログが保存できない場合、印刷ページ数は記録されません。
	b. 印刷の最初と最後に印刷ログが保存できない場合、このジョブの印刷ログは記録されません。この機能が回復すると、該当のエラーが印刷ログに反映されます。

6. **OK** をクリックし、 **印刷ログ機能テスト** ページを表示します。

   設定をテストするには、**はい**をクリックして、次の手順に進みます。

   テストを行わずに次へ進むには、 **いいえ**をクリックします。設定値は自動的にサブミットされます。
7. 製品が設定値をテストします。
8. 設定が承認されると、**テスト成功**がページに表示されます。

   テストエラー が表示された場合は、すべての設定値を確認し、 **OK** をクリックして、もう一度テストページを表示します。

関連情報

- ネットワークへの印刷ログ保存機能

セキュリティ機能ロックがアクティブな場合の印刷ログ機能の使用について

セキュリティ機能ロック 3.0 がアクティブな場合、コピー、ファクス受信、クラウド接続印刷、および USB ダイレクト印刷の登録ユーザー名が、印刷ログ機能レポートに記録されます。Active Directory 認証が有効な場合、ユーザーの名前は印刷ログ機能レポートに記録されます。

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。

```
Id, Type, Job Name, User Name, Date, Time, Print Pages
1, Copy, -, -, 04/04/20xx, 09:05:12, 3
2, Fax, -, -, 04/04/20xx, 09:45:30, 5
3, Copy, -, "Bob", 04/04/20xx, 10:20:30, 4
4, Fax, -, "Bob", 04/04/20xx, 10:35:12, 3
5, USB Direct, -, "John", 04/04/20xx, 11:15:43, 6
```

関連情報

- ネットワークへの印刷ログ保存機能

brother

Brother Earth

JPN
Version A