KONICA MINOLTA

ユーザーズガイド
ネットワーク操作編

bizhub 4000i

本ガイドの使い方

対象となるモデル

本ガイドは、以下のモデルを対象としています。

1 行液晶ディスプレーモデル：bizhub 4000i

関連情報

- 本ガイドの使い方

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。

⚠警告	誤った取扱いをしたとき、死亡や重傷に結びつく可能性がある内容を示しています。
⚠注意	誤った取扱いをしたとき、軽傷または家屋・財産などの損害に結びつく可能性がある内容を示しています。
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。
	ヒントアイコンは、有益なヒントや補足情報を示しています。
	「感電の危険があること」を示しています。
	「火災の危険があること」を示しています。
	「やけどの危険があること」を示しています。
	「してはいけないこと」を示しています。
太字	本製品の操作パネルやパソコンの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。
[[XXXXX]]	括弧で囲まれたテキストは、本製品の画面に表示されるメッセージを示しています。

関連情報

- 本ガイドの使い方

商標

KONICA MINOLTA、KONICA MINOLTA ロゴ、Giving Shape to Ideas、PageScope、および bizhub は、コニカミノルタ株式会社の登録商標または商標です。

Microsoft、Windows、Windows Server、Internet Explorer、Active Directory、OneNote、Windows phone および OneDrive は、米国および／またはその他の国におけるマイクロソフト社の登録商標または商標です。

Apple、Mac、Mac OS、Safari、iPad、iPhone、iPod touch および OS X は、米国および他の国々で登録された Apple Inc.の商標です。

PostScript および PostScript 3 は、米国および/またはその他の国における Adobe Systems Incorporated の商標または登録商標です。

Wi-Fi CERTIFIED、Wi-Fi、Wi-Fi Alliance、Wi-Fi Direct および Wi-Fi Protected Access は、Wi-Fi Alliance®の登録商標です。

WPA、WPA2、Wi-Fi Protected Setup および Wi-Fi Protected Setup ロゴは、Wi-Fi Alliance®の商標です。

Android、Google Cloud Print、Google Drive、Google Chrome および Google Play は、グーグル社の商標です。これらの商標の使用には、グーグル社の許可が必要です。

Mopria は、Mopria Alliance の登録商標です。

Mozilla および Firefox は、Mozilla Foundation の登録商標です。

UNIX は、The Open Group の米国ならびに他の国における登録商標です。

Linux は、Linus Torvalds の米国およびその他の国における登録商標または商標です。

Intel は、米国およびその他の国における Intel Corporation の商標です。

本ガイドに製品名が記載されている各ソフトウェアの開発会社は、著作プログラムに特定したソフトウェアライセンス契約を有します。

その他すべての商標は、それぞれの所有者の財産です。

関連情報

- 本ガイドの使い方

重要事項

- 購入された国以外で本製品を使用しないでください。海外各国における無線通信および電力規制に反する場合や、海外で使用されている電源が本製品で適切に使用できない恐れがあります。
- 本文中の Windows® 10 は、Windows® 10 Home、Windows® 10 Pro、Windows® 10 Education、および Windows® 10 Enterprise を指します。
- 本文中の Windows Server® 2008 は、Windows Server® 2008 および Windows Server® 2008 R2 を指します。
- 本ガイドに掲載されている画面は、Windows® の場合は Windows® 7、Mac の場合は macOS v10.12.x の画面を代表で使用しています。お使いの OS や環境またはモデルによって、実際の画面と異なることがあります。
- 本ガイドならびに本製品の仕様は予告なく変更されることがあります。

関連情報

- 本ガイドの使い方

ネットワーク

はじめに

ネットワークのセットアップと接続には、Utilities CD をご使用になることをお勧めします。ここでは、ネットワーク接続の種類についての詳細、ネットワークを管理するための様々な方式、および本製品の有益なネットワーク機能を説明します。

- 対応している基本ネットワーク機能について

対応している基本ネットワーク機能について

本製品は、使用される OS に合わせて、さまざまな機能をサポートしています。この表で、各 OS でサポートされるネットワーク機能と接続を確認してください。

オペレーティングシステム	Windows® 7 Windows® 8.1 Windows® 10	Windows Server® 2008/2012/ 2012 R2/2016/2019	OS X v10.10.x OS X v10.11.x macOS v10.12.x macOS v10.13.x macOS v10.14.x
印刷	Yes	Yes	Yes
ウェブブラウザーによる設定	Yes	Yes	Yes

関連情報

- はじめに

ネットワーク管理ソフトウェアおよびユーティリティ

ユーティリティソフトを使用して、本製品のネットワークの設定や変更を行います。

- ネットワーク管理ソフトウェアとユーティリティについて

ネットワーク管理ソフトウェアとユーティリティについて

ウェブブラウザーによる設定

ウェブブラウザーによる設定は、標準的なウェブブラウザーを使用し、ハイパーテキスト転送プロトコル（HTTP）または SSL 経由のハイパーテキスト転送プロトコル（HTTPS）を使用して本製品を管理します。本製品の IP アドレスをお使いのウェブブラウザーに入力して、本プリントサーバーの設定値の表示や変更を行います。

関連情報

- ネットワーク管理ソフトウェアおよびユーティリティ

他の無線ネットワーク設定方法について

本製品を無線ネットワークに接続するには、Utilities CD をご使用になることをお勧めします。

本製品を無線ネットワーク用に設定する前に

無線ネットワークの設定を行う前に以下の内容を確認してください。

- 無線設定を行う前に、お使いのネットワーク名(SSID)とネットワークキーを確認しておく必要があります。エンタープライズ無線ネットワークを使用している場合、ユーザー ID とパスワードを確認しておく必要があります。

  セキュリティ情報がわからない場合は、ルーターの製造業者、システム管理者、またはインターネットプロバイダーにお問い合わせください。

- 文書を快適に印刷するために、本製品をできるだけ無線 LAN アクセスポイントまたはルーターに近づけ、障害物からは遠ざけてください。本製品とアクセスポイントやルーターの間に大きな物や壁、他の電子機器からの干渉があると、印刷する文書のデータ転送速度が遅くなる可能性があります。

  そのため、無線 LAN での接続が必ずしも最適というわけではありません。複雑で文字数の多い文書や写真などの大きいサイズのデータを印刷する場合は、データ転送速度のより速い有線 LAN 接続または USB 接続で印刷することをお勧めします。
- 本製品は有線 LAN と無線 LAN のいずれのネットワークでも使用できますが、両方のネットワークを同時に使用することはできません。ただし、無線 LAN 接続と Wi-Fi Direct 接続、または有線 LAN 接続と Wi-Fi Direct 接続は同時に使用できます。

関連情報

- 他の無線ネットワーク設定方法について

無線ネットワーク用に本製品を設定する

1. パソコンの電源を入れ、Utilities CD を CD-ROM ドライブにセットします。
2. 起動画面が自動的に表示されます。
   言語を選択し、画面の指示に従います。

- （Windows® 7）
  本製品の画面が自動的に表示されない場合は、**コンピューター**にアクセスしてください。CD-ROM アイコンをダブルクリックし、**start.exe** をダブルクリックします。
- （Windows® 8.1 および Windows® 10）
  タスクバーの  （**エクスプローラー**）アイコンをクリックし、**PC** にアクセスします。CD-ROM アイコンをダブルクリックし、**start.exe** をダブルクリックします。
- **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。

3. **無線 LAN (Wi-Fi)**を選択し、**次の項目へ** をクリックします。
4. 画面の指示に従います。

無線セットアップが完了した後、インストーラープログラムはドライバーのインストールへ進みます。インストールダイアログボックスの**次の項目へ** をクリックし、画面の指示に従います。

関連情報

- 他の無線ネットワーク設定方法について

Wi-Fi Protected Setup™ （WPS）のワンプッシュ方式を使用して本製品に無線ネットワークを設定する

お使いの無線 LAN アクセスポイント／ルーターが WPS（プッシュボタン設定）をサポートしている場合、本製品の操作パネルメニューから WPS を使用して無線ネットワークを設定することができます。

WPS をサポートしているルーターまたはアクセスポイントは、以下のロゴマークが付いています。

1. ▲または▼を押して、[ﾈｯﾄﾜｰｸ]を選択し、**OK** を押します。
2. ▲または▼を押して、[ﾑｾﾝ LAN]を選択し、**OK** を押します。
3. ▲または▼を押して、[WPS]を選択し、**OK** を押します。
4. [ﾑｾﾝLAN ﾕｳｺｳ ?]が表示されたら、▲を押してオンを選択します。
   これにより無線セットアップウィザードが起動します。キャンセルするには、**Cancel** を押します。
5. 画面に[APﾉﾎﾞﾀﾝｦ ｵｽ]と表示されたら、無線 LAN アクセスポイント／ルーターの、WPS ボタンを押します。本製品の操作パネルで、▲を押します。本製品は、お使いの無線 LAN アクセスポイント／ルーターを自動的に検出し、無線ネットワークとの接続を開始します。

無線機器が正常に接続されると、本製品の画面に[ｾﾂｿﾞｸ ｾｲｺｳ]と表示されます。

関連情報

- 他の無線ネットワーク設定方法について

関連トピック：

- 無線 LAN レポートのエラーコード

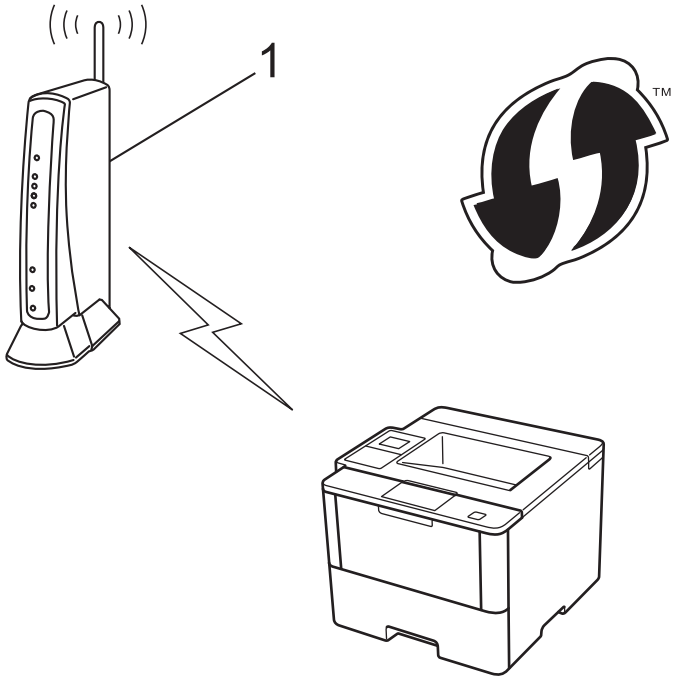
Wi-Fi Protected Setup™ （WPS）の PIN 方式を使用して本製品に無線ネットワークを設定する

お使いの無線 LAN のアクセスポイント／ルーターが WPS をサポートしている場合、暗証番号（PIN）方式を使用して無線ネットワークを設定できます。

PIN 方式は、 Wi-Fi Alliance®により開発された接続方式の一つです。加入者（本製品）によって作成された PIN を、レジストラー（登録管理機器）に送信することで、無線ネットワークとセキュリティを設定することができます。WPS モードへのアクセスについては、お使いの無線 LAN アクセスポイント／ルーターに同梱の説明書をご参照ください。

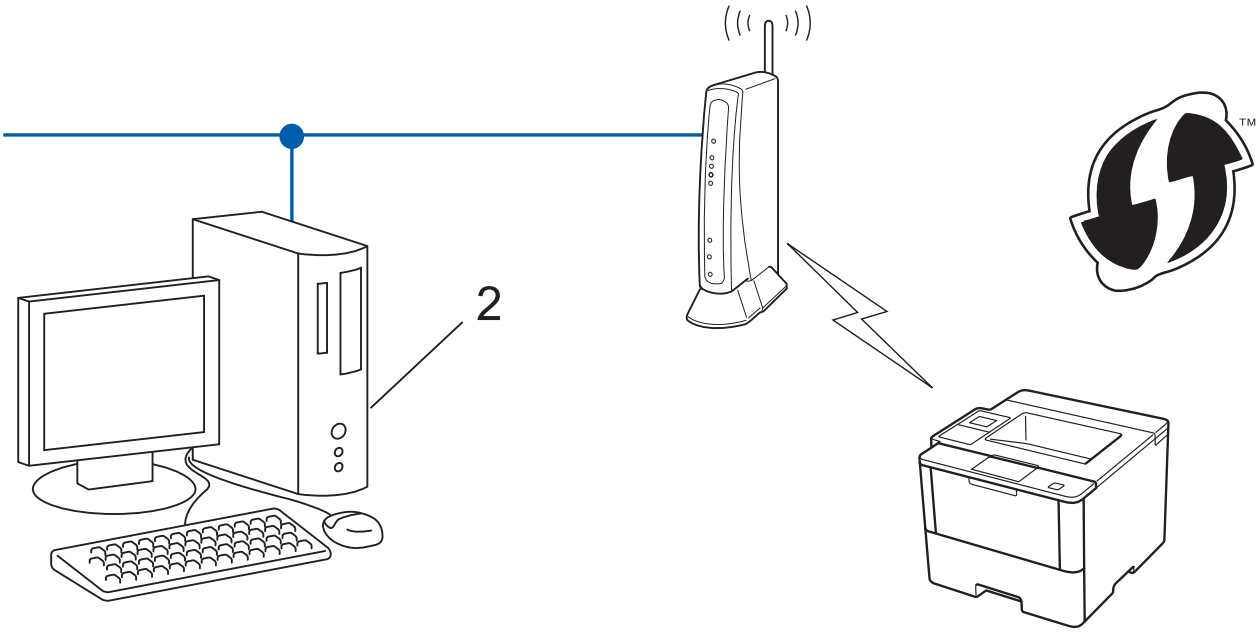
タイプ A

無線 LAN アクセスポイント／ルーター（1）がレジストラーを兼ねている場合の接続



タイプ B

パソコンなど、その他の機器（2）がレジストラーとして使用される場合の接続



WPS をサポートしているルーターまたはアクセスポイントは、以下のロゴマークが付いています。

1. ▲または▼を押して、[ﾈｯﾄﾜｰｸ]を選択し、**OK** を押します。
2. ▲または▼を押して、[ﾑｾﾝ LAN]を選択し、**OK** を押します。
3. ▲または▼を押して、[WPS(PINｺｰﾄﾞ)]を選択し、**OK** を押します。
4. [ﾑｾﾝLAN ﾕｳｺｳ ?]が表示されたら、▲を押してオンを選択します。
   これにより無線セットアップウィザードが起動します。キャンセルするには、**Cancel** を押します。
5. 本製品の画面には 8 桁の PIN が表示され、製品は無線 LAN アクセスポイント／ルーターの検索を開始します。
6. ネットワーク上のパソコンを使用して、お使いのブラウザーに「http://アクセスポイントの IP アドレス」を入力します（「アクセスポイントの IP アドレス」の部分は、レジストラー（登録管理機器）として使用される機器の IP アドレスです）。
7. WPS の設定ページを表示して PIN を入力したあと、画面の指示に従います。

- レジストラー（登録管理機器）は通常、無線 LAN アクセスポイント／ルーターです。
- 設定画面は、無線 LAN アクセスポイント／ルーターの種類によって異なります。詳細については、無線 LAN アクセスポイント／ルーターの取扱説明書をご覧ください。

Windows® 7、Windows® 8.1、または Windows® 10 パソコンをレジストラー（登録管理機器）として使用している場合、以下の手順をすべて行ってください。

8. 次のいずれかを行ってください。
   - （Windows® 7）
     (スタート) > **デバイスとプリンター** > **デバイスの追加**をクリックします。
   - （Windows® 8.1）

マウスをデスクトップの右下隅に移動します。メニューバーが表示されたら、**設定** > **コントロール パネル** > **ハードウェアとサウンド** > **デバイスとプリンター** > **デバイスの追加**をクリックします。

- （Windows® 10）

  > **Windows システム ツール** > **コントロール パネル**をクリックします。**ハードウェアとサウンド**グループで、**デバイスの追加**をクリックします。

- Windows® 7、Windows® 8.1、または Windows® 10 パソコンをレジストラー（登録管理機器）として使用する場合、使用するパソコンをネットワークに事前に登録する必要があります。詳細については、お使いの無線 LAN アクセスポイント／ルーターの説明書を参照してください。
- Windows® 7、Windows® 8.1、または Windows® 10 のパソコンをレジストラー（登録管理機器）として使用する場合は、画面の指示に従って無線設定を行ったあと、プリンタードライバーをインストールできます。

---

9. 本製品を選択し、**次へ**をクリックします。
10. 本製品の画面に表示された PIN を入力し、**次へ**をクリックします。
11. お使いのネットワークを選択して、**次へ**をクリックします。
12. **閉じる**をクリックします。

無線機器が正常に接続されると、本製品の画面に［ｾｯﾂﾞｸ ｾｲｺｳ］と表示されます。

関連情報

- 他の無線ネットワーク設定方法について

関連トピック：

- 無線 LAN レポートのエラーコード

アドホックモードで無線ネットワークを設定する（IEEE 802.11b/g/n の場合）

- 新しい SSID を使用して、アドホックモードで本製品に無線 LAN を設定する
- 既存の SSID を使用して、アドホックモードで本製品に無線 LAN を設定する

新しい SSID を使用して、アドホックモードで本製品に無線 LAN を設定する

アドホックモードに設定されている場合は、お使いのパソコンから新規の SSID に接続する必要があります。

1. ▲または▼を押して、[ﾈｯﾄﾜｰｸ]を選択し、**OK** を押します。
2. ▲または▼を押して、[ﾑｾﾝ LAN]を選択し、**OK** を押します。
3. ▲または▼を押して、[ｾｯｿﾞｸ ｳｨｻﾞｰﾄﾞ]を選択し、**OK** を押します。
4. [ﾑｾﾝLAN ﾕｳｺｳ ?]が表示されたら、▲を押してオンを選択します。
   これにより無線セットアップウィザードが起動します。キャンセルするには、**Cancel** を押します。
5. 本製品は使用しているネットワークを検索し、利用可能な SSID のリストを表示します。▲または▼を押して、[<New SSID>]を選択し、**OK** を押します。
6. SSID 名を入力し、**OK** を押します。
7. ▲または▼を押して、[ｱﾄﾞﾎｯｸ]を選択し、**OK** を押します。
8. ▲または▼を押して、暗号化タイプを[ﾆﾝｼｮｳ ｼﾅｲ]または [WEP]から選択し、**OK** を押します。
9. 暗号化方式に[WEP]を選択した場合、WEP キーを入力して、**OK** を押します。

本製品は最初の WEP キーのみをサポートします。

10. 設定値を適用するには、▲を押します。キャンセルするには、▼を押します。
11. 本製品は、選択された無線機器との接続を開始します。

無線機器が正常に接続されると、本製品の画面に[ｾｯｿﾞｸ ｾｲｺｳ]と表示されます。

関連情報

- アドホックモードで無線ネットワークを設定する（IEEE 802.11b/g/n の場合）

関連トピック：

- 無線 LAN レポートのエラーコード

既存の SSID を使用して、アドホックモードで本製品に無線 LAN を設定する

すでにアドホックモードであり、SSID が設定されているパソコンに本製品を組み合わせる場合、以下の指示に従ってください。

本製品を設定する前に、お使いの無線ネットワークの設定値を書き留めておくことをお勧めします。設定を行う前に、この情報が必要になります。

1. 現在接続しているパソコンの無線ネットワーク設定を確認して記録します。

現在接続しているパソコンの無線ネットワークは、SSID が設定されたアドホックモードに設定する必要があります。お使いのパソコンをアドホックモードに設定する方法の詳細については、パソコンの説明書を参照するか、ネットワーク管理者に問い合わせてください。

ネットワーク名（SSID）

通信モード	暗号化モード	ネットワークキー
アドホック	なし	-
	WEP	

例：

ネットワーク名（SSID）
HELLO

通信モード	暗号化モード	ネットワークキー
アドホック	WEP	12345

本製品は最初の WEP キーのみをサポートします。

2. ▲または▼を押して、[ﾈｯﾄﾜｰｸ]を選択し、**OK** を押します。
3. ▲または▼を押して、[ﾑｾﾝ LAN]を選択し、**OK** を押します。
4. ▲または▼を押して、[ｾｯｿﾞｸ ｳｨｻﾞｰﾄﾞ]を選択し、**OK** を押します。
5. [ﾑｾﾝLAN ﾕｳｺｳ ?]が表示されたら、▲を押してオンを選択します。
   これにより無線セットアップウィザードが起動します。キャンセルするには、**Cancel** を押します。
6. 本製品は使用しているネットワークを検索し、利用可能な SSID のリストを表示します。SSID のリストが表示されたら、▲または▼を押して、使用したい SSID を選択します。
7. **OK** を押します。
8. WEP キーを入力し、**OK** を押します。
   設定を適用するには、▲を押します。キャンセルするには、▼を押します。

本製品は最初の WEP キーのみをサポートします。

9. 本製品は、選択された無線機器との接続を開始します。

無線機器が正常に接続されると、本製品の画面に[ｾｯｿﾞｸ ｾｲｺｳ]と表示されます。

関連情報

- アドホックモードで無線ネットワークを設定する（IEEE 802.11b/g/n の場合）

関連トピック：

- 無線 LAN レポートのエラーコード

本製品の操作パネルセットアップウィザードを使用して、無線 LAN を設定する

本製品を設定する前に、お使いの無線ネットワークの設定値を書き留めておくことをお勧めします。設定を行う前に、この情報が必要になります。

1. 現在接続しているパソコンの無線ネットワーク設定を確認して記録します。

ネットワーク名（SSID）

ネットワークキー

例：

ネットワーク名（SSID）
HELLO

ネットワークキー
12345

- お使いのアクセスポイント／ルーターが複数の WEP キーをサポートしている場合でも、本製品では最初の WEP キーのみが使用可能です。
- セットアップ中の操作に関してカスタマーサポートに問い合わせる際は、SSID（ネットワーク名）およびネットワークキーをご準備ください。この情報に関してはお問い合わせいただいても回答できません。
- この情報（SSID およびネットワークキー）が不明の場合は、無線セットアップを行うことができません。

  この情報はどこに載っていますか？

  - 無線 LAN アクセスポイント／ルーターの説明書を確認してください。
  - 初期設定の SSID は、製造業者の名前またはモデル名になっています。
  - セキュリティ情報がわからない場合は、ルーターの製造業者、システム管理者、またはインターネットプロバイダーにお問い合わせください。

2. ▲または▼を押して、[ﾈｯﾄﾜｰｸ]を選択し、**OK** を押します。
3. ▲または▼を押して、[ﾑｾﾝ LAN]を選択し、**OK** を押します。
4. ▲または▼を押して、[ｾｯｿﾞｸ ｳｨｻﾞｰﾄﾞ]を選択し、**OK** を押します。
5. [ﾑｾﾝLAN ﾕｳｺｳ ?]が表示されたら、▲を押してオンを選択します。

   これにより無線セットアップウィザードが起動します。キャンセルするには、**Cancel** を押します。
6. 本製品は使用しているネットワークを検索し、利用可能な SSID のリストを表示します。SSID のリストが表示されたら、▲または▼を押して、使用したい SSID を選択します。
7. **OK** を押します。
8. 次のいずれかを行ってください。
   - ネットワークキーを必要とする認証および暗号化方式を使用している場合、最初の手順で書き留めたネットワークキーを入力します。

     キーを入力し、**OK** を押します。

     設定値を適用するには、▲を押します。キャンセルするには、▼を押します。
   - 使用している認証方式がオープンシステムで、暗号化モードが「なし」の場合、次の手順に進みます。

9. 本製品は、選択された無線機器に接続しようとします。

無線機器が正常に接続されると、本製品の画面に [ｾﾂｿﾞｸ ｾｲｺｳ] と表示されます。

関連情報

- 他の無線ネットワーク設定方法について

関連トピック：

- 無線 LAN レポートのエラーコード

SSID が同報送信以外の場合の無線 LAN を本製品に設定する

本製品を設定する前に、お使いの無線ネットワークの設定値を書き留めておくことをお勧めします。設定を行う前に、この情報が必要になります。

1. 現在の無線ネットワーク設定を確認して記録します。

ネットワーク名（SSID）

通信モード	認証方式	暗号化モード	ネットワークキー
インフラストラクチャ	オープンシステム	なし	-
		WEP	
	共有キー	WEP	
	WPA/WPA2-PSK	AES	
		TKIP （TKIP は WPA-PSK でのみサポートされています。）	

例：

ネットワーク名（SSID）
HELLO

通信モード	認証方式	暗号化モード	ネットワークキー
インフラストラクチャ	WPA2-PSK	AES	12345678

お使いのルーターが WEP 暗号化方式を使用している場合、最初の WEP キーとして使用されているキーを入力します。本製品は最初の WEP キーのみをサポートします。

2. ▲または▼を押して、[ﾈｯﾄﾜｰｸ]を選択し、**OK** を押します。
3. ▲または▼を押して、[ﾑｾﾝ LAN]を選択し、**OK** を押します。
4. ▲または▼を押して、[ｾｯｿﾞｸ ｳｨｻﾞｰﾄﾞ]を選択し、**OK** を押します。
5. [ﾑｾﾝLAN ﾕｳｺｳ ?]が表示されたら、▲を押してオンを選択します。
   これにより無線セットアップウィザードが起動します。キャンセルするには、**Cancel** を押します。
6. 本製品は使用しているネットワークを検索し、利用可能な SSID のリストを表示します。▲または▼を押して、[<New SSID>]を選択し、**OK** を押します。
7. SSID 名を入力し、**OK** を押します。
8. ▲または▼を押して、[ｲﾝﾌﾗｽﾄﾗｸﾁｬ]を選択し、**OK** を押します。
9. ▲または▼を押して、使用する認証方式を選択し、**OK** を押します。
10. 次のいずれかを行ってください。
    - [ｵｰﾌﾟﾝｼｽﾃﾑ ﾆﾝｼｮｳ]を選択した場合、▲または▼を押して、暗号化タイプを[ﾆﾝｼｮｳ ｼﾅｲ]または[WEP]から選択し、**OK** を押します。
      暗号化方式に[WEP]を選択した場合、WEP キーを入力して、**OK** を押します。
    - [ｷｮｳﾕｳｷｰ ﾆﾝｼｮｳ]を選択した場合、WEP キーを入力し、**OK** を押します。
    - [WPA/WPA2-PSK]を選択した場合、▲または▼を押して、暗号化タイプを[TKIP+AES]または[AES]から選択し、**OK** を押します。
      WPA キーを入力し、**OK** を押します。

本製品は最初の WEP キーのみをサポートします。

11. 設定値を適用するには、▲を押します。キャンセルするには、▼を押します。
12. 本製品は、選択された無線機器との接続を開始します。

無線機器が正常に接続されると、本製品の画面に [ｾﾂｿﾞｸ ｾｲｺｳ] と表示されます。

関連情報

- 他の無線ネットワーク設定方法について

関連トピック：

- 無線ネットワーク設定を完了できません
- 無線 LAN レポートのエラーコード

エンタープライズ無線 LAN 用に本製品を設定する

本製品を設定する前に、お使いの無線ネットワークの設定値を書き留めておくことをお勧めします。設定を行う前に、この情報が必要になります。

1. 現在の無線 LAN 設定を確認して記録します。

ネットワーク名（SSID）

通信モード	認証方式	暗号化モード	ユーザー ID	パスワード
インフラストラクチャ	LEAP	CKIP		
	EAP-FAST/NONE	AES		
		TKIP		
	EAP-FAST/MS-CHAPv2	AES		
		TKIP		
	EAP-FAST/GTC	AES		
		TKIP		
	PEAP/MS-CHAPv2	AES		
		TKIP		
	PEAP/GTC	AES		
		TKIP		
	EAP-TTLS/CHAP	AES		
		TKIP		
	EAP-TTLS/MS-CHAP	AES		
		TKIP		
	EAP-TTLS/MS-CHAPv2	AES		
		TKIP		
	EAP-TTLS/PAP	AES		
		TKIP		
	EAP-TLS	AES		-
		TKIP		-

例：

ネットワーク名（SSID）
HELLO

通信モード	認証方式	暗号化モード	ユーザー ID	パスワード
インフラストラクチャ	EAP-FAST/MS-CHAPv2	AES	KONICA MINOLTA	12345678

- 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。
- サーバー証明書の共通名を使用して本製品を確認する場合、設定の開始前に、使用する共通名を書き留めておくことをお勧めします。サーバー証明書の共通名については、ネットワーク管理者に問い合わせてください。

2. ▲または▼を押して、[ﾈｯﾄﾜｰｸ]を選択し、**OK** を押します。
3. ▲または▼を押して、[ﾑｾﾝ LAN]を選択し、**OK** を押します。
4. ▲または▼を押して、[ｾｯｿﾞｸ ｳｨｻﾞｰﾄﾞ]を選択し、**OK** を押します。
5. [ﾑｾﾝLAN ﾕｳｺｳ ?]が表示されたら、▲を押してオンを選択します。
   これにより無線セットアップウィザードが起動します。キャンセルするには、**Cancel** を押します。
6. 本製品は使用しているネットワークを検索し、利用可能な SSID のリストを表示します。▲または▼を押して、[<New SSID>]を選択し、**OK** を押します。
7. SSID 名を入力し、**OK** を押します。
8. ▲または▼を押して、[ｲﾝﾌﾗｽﾄﾗｸﾁｬ]を選択し、**OK** を押します。
9. ▲または▼を押して、使用する認証方式を選択し、**OK** を押します。
10. 次のいずれかを行ってください。
    - [LEAP]を選択した場合、ユーザー ID を入力し、**OK** を押します。
      パスワードを入力し、**OK** を押します。
    - [EAP-FAST]、[PEAP]または[EAP-TTLS]を選択した場合、▲または▼を押して内部認証方式を[NONE]、[CHAP]、[MS-CHAP]、[MS-CHAPv2]、[PAP]または[GTC]から選択し、**OK** を押します。

      使用する認証方式によって、選択する内部認証方式は異なります。

      ▲または▼を押して、暗号化タイプを[TKIP+AES]または[AES]から選択し、**OK** を押します。
      ▲または▼を押して、検証方法を[ｹﾝｼｮｳｼﾅｲ]、[CAｼｮｳﾒｲｼｮ]または[CA+ｻｰﾊﾞｰID]から選択し、**OK** を押します。
      - [CA+ｻｰﾊﾞｰID]を選択した場合、その都度 **OK** を押します。
      - その他を選択した場合は、その都度 **OK** を押します。

      本製品に CA 証明書をインポートしていない場合、[ｹﾝｼｮｳｼﾅｲ]が表示されます。
    - [EAP-TLS]を選択した場合、▲または▼を押して、暗号化タイプを[TKIP+AES]または[AES]から選択し、**OK** を押します。
      使用可能なクライアント証明書のリストが製品に表示された場合、使用する証明書を選択します。
      ▲または▼を押して、検証方法を[ｹﾝｼｮｳｼﾅｲ]、[CAｼｮｳﾒｲｼｮ]または[CA+ｻｰﾊﾞｰID]から選択し、**OK** を押します。
      - [CA+ｻｰﾊﾞｰID]を選択した場合、その都度 **OK** を押します。
      - その他を選択した場合は、ユーザー ID を入力し、**OK** を押します。

      本製品に CA 証明書をインポートしていない場合、[ｹﾝｼｮｳｼﾅｲ]が表示されます。
11. 設定値を適用するには、▲を押します。キャンセルするには、▼を押します。
12. 本製品は、選択された無線機器との接続を開始します。

無線機器が正常に接続されると、本製品の画面に[ｾｯｿﾞｸ ｾｲｺｳ]と表示されます。

関連情報

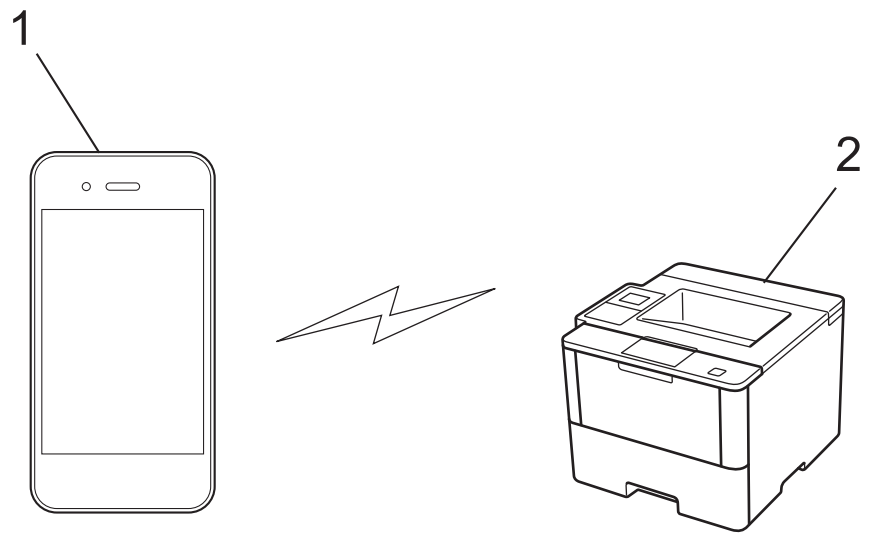
- 他の無線ネットワーク設定方法について

Wi-Fi Direct®を使用する

- Wi-Fi Direct を使用した携帯端末からの印刷について
- Wi-Fi Direct の設定について
- 無線ネットワーク設定を完了できません

Wi-Fi Direct を使用した携帯端末からの印刷について

Wi-Fi Direct は、Wi-Fi Alliance®により開発された無線設定方法の一つです。これにより、アクセスポイントを使用せずに、本製品と、Android™機器、Windows Phone®、iPhone、iPod touch、または iPad などの携帯端末との間に、安全な無線ネットワークを設定することができます。Wi-Fi Direct は、Wi-Fi Protected Setup™ （WPS）のワンプッシュまたは PIN 方式を使用した無線ネットワークの設定をサポートしています。また、SSID とパスワードの手動設定、無線ネットワークの設定も可能です。本製品の Wi-Fi Direct 機能は、AES 暗号化を使用する WPA2™をサポートしています。



1. 携帯端末
2. 本製品

- 本製品は有線 LAN と無線 LAN のいずれのネットワークでも使用できますが、両方のネットワークを同時に使用することはできません。ただし、無線 LAN 接続と Wi-Fi Direct 接続、または有線 LAN 接続と Wi-Fi Direct 接続は同時に使用できます。
- Wi-Fi Direct をサポートしている機器は、グループオーナー（G/O）になることができます。Wi-Fi Direct を設定する場合、G/O はアクセスポイントとして機能します。
- アドホックモードと Wi-Fi Direct は同時に使用できません。一方の機能を無効にして、他方を有効にしてください。アドホックモードで接続中に Wi-Fi Direct を使用したい場合は、ネットワークインターフェイスを有線 LAN に設定するか、アドホックモードを無効にして、本製品をアクセスポイントに接続します。

関連情報

- Wi-Fi Direct®を使用する

Wi-Fi Direct の設定について

製品の操作パネルから、Wi-Fi Direct の設定をします。

- Wi-Fi Direct ネットワーク設定の概要
- ワンプッシュ方式を使用して Wi-Fi Direct を設定する
- ワンプッシュ方式および Wi-Fi Protected Setup™（WPS）のワンプッシュ方式を使用して Wi-Fi Direct を接続する
- PIN 方式を使用して Wi-Fi Direct を設定する
- Wi-Fi Protected Setup™（WPS）の PIN 方式を使用して Wi-Fi Direct を接続する
- Wi-Fi Direct を手動で接続する

Wi-Fi Direct ネットワーク設定の概要

無線 LAN 環境で本製品を設定する方法は以下の 5 つです。お使いの環境に合わせて方法を選択してください。

設定する携帯端末を確認します。

1. お使いの携帯端末は Wi-Fi Direct をサポートしていますか？

オプション	説明
はい	手順 2 に進みます。
いいえ	手順 3 に進みます。

2. お使いの携帯端末は Wi-Fi Direct のワンプッシュ設定をサポートしていますか？

オプション	説明
はい	「関連情報」をご覧ください： ワンプッシュ方式を使用して Wi-Fi Direct を設定する
いいえ	「関連情報」をご覧ください： PIN 方式を使用して Wi-Fi Direct を設定する

3. お使いの携帯端末は Wi-Fi Protected Setup™（WPS）をサポートしていますか？

オプション	説明
はい	手順 4 に進みます。
いいえ	「関連情報」をご覧ください： Wi-Fi Direct を手動で接続する

4. お使いの携帯端末は Wi-Fi Protected Setup™（WPS）のワンプッシュ設定をサポートしていますか？

オプション	説明
はい	「関連情報」をご覧ください： ワンプッシュ方式および Wi-Fi Protected Setup™（WPS）のワンプッシュ方式を使用して Wi-Fi Direct を接続する
いいえ	「関連情報」をご覧ください： Wi-Fi Protected Setup™（WPS）の PIN 方式を使用して Wi-Fi Direct を接続する

ワンプッシュまたは PIN で Wi-Fi Direct を設定したあとで Konica Minolta Mobile Print 機能を使用する場合は、Android™ 4.0 以降の端末機器が必要です。

関連情報

- Wi-Fi Direct の設定について

関連トピック：

- ワンプッシュ方式を使用して Wi-Fi Direct を設定する
- ワンプッシュ方式および Wi-Fi Protected Setup™（WPS）のワンプッシュ方式を使用して Wi-Fi Direct を接続する
- PIN 方式を使用して Wi-Fi Direct を設定する
- Wi-Fi Protected Setup™（WPS）の PIN 方式を使用して Wi-Fi Direct を接続する
- Wi-Fi Direct を手動で接続する

ワンプッシュ方式を使用して Wi-Fi Direct を設定する

お使いの携帯端末が Wi-Fi Direct をサポートしている場合、以下の手順に従って Wi-Fi Direct を設定します。

1. ▲または▼を押して、[ﾈｯﾄﾜｰｸ]を選択し、**OK** を押します。
2. ▲または▼を押して、[Wi-Fi Direct]を選択し、**OK** を押します。
3. ▲または▼を押して、[ﾌﾟｯｼｭﾎﾞﾀﾝ ｾｯﾃｲ]を選択し、**OK** を押します。
4. [Wi-Fi Direct ｵﾝ?]が表示されたら、▲を押して適用します。キャンセルするには、▼を押します。
5. [ｱｲﾃｶﾞﾜ ﾃﾞﾊﾞｲｽ ﾉ Wi-Fi Directｾｯﾃｲ ﾖ ﾕｳｺｳﾆｼﾃ OKﾎﾞﾀﾝ ﾖ ｵｼﾃｸﾀﾞｻｲ]が本製品の画面に表示されたら、携帯端末の Wi-Fi Direct を有効にします。製品の **OK** を押します。

   これにより Wi-Fi Direct セットアップが起動します。キャンセルするには、**Cancel** を押します。
6. 次のいずれかを行ってください。
   - 本製品がグループオーナー（G/O）の場合、お使いの携帯端末を本製品に直接接続します。
   - 本製品が G/O ではない場合、Wi-Fi Direct の設定が可能な機器の名前が表示されます。▲または▼を押して、接続したい携帯端末を選択し、**OK** を押します。[<ﾘｽﾄｷｬﾝ>]を押して、利用可能な機器を再検索します。
7. 携帯端末が正常に接続されると、本製品の画面に[ｾﾂｿﾞｸ ｾｲｺｳ]と表示されます。以上で Wi-Fi Direct ネットワークのセットアップが完了しました。

関連情報

- Wi-Fi Direct の設定について

関連トピック：

- Wi-Fi Direct ネットワーク設定の概要

ワンプッシュ方式および Wi-Fi Protected Setup™（WPS）のワンプッシュ方式を使用して Wi-Fi Direct を接続する

お使いの携帯端末が WPS（PBC：プッシュボタン設定）をサポートしている場合、以下の手順に従い Wi-Fi Direct ネットワークを設定します。

1. ▲または▼を押して、[ﾈｯﾄﾜｰｸ]を選択し、**OK** を押します。
2. ▲または▼を押して、[Wi-Fi Direct]を選択し、**OK** を押します。
3. ▲または▼を押して、[ｸﾞﾙｰﾌﾟ ｵｰﾅｰ]を選択し、**OK** を押します。
4. ▲または▼を押して、[ｵﾝ]を選択し、**OK** を押します。
5. ▲または▼を押して、[ﾌﾟｯｼｭﾎﾞﾀﾝ ｾｯﾃｲ]オプションを選択し、**OK** を押します。
6. [Wi-Fi Direct ｵﾝ?]が表示されたら、▲を押して適用します。キャンセルするには、▼を押します。
7. [ｱｲﾃｶﾞﾜ ﾃﾞﾊﾞｲｽ ﾉ Wi-Fi Directｾｯﾃｲ ﾖ ﾕｳｺｳﾆｼﾃ OKﾎﾞﾀﾝ ﾖ ｵｼﾃｸﾀﾞｻｲ]が本製品の画面に表示されたら、携帯端末の WPS ワンプッシュ設定方式を有効にします。製品の **OK** を押します。

   これにより Wi-Fi Direct セットアップが起動します。キャンセルするには、**Cancel** を押します。
8. 携帯端末が正常に接続されると、本製品の画面に [ｾｯﾂﾞｸ ｾｲｺｳ] と表示されます。以上で Wi-Fi Direct ネットワークのセットアップが完了しました。

関連情報

- Wi-Fi Direct の設定について

関連トピック：

- Wi-Fi Direct ネットワーク設定の概要

PIN 方式を使用して Wi-Fi Direct を設定する

お使いの携帯端末が Wi-Fi Direct の PIN 方式をサポートしている場合、以下の手順に従って Wi-Fi Direct を設定します。

1. ▲または▼を押して、[ﾈｯﾄﾜｰｸ]を選択し、**OK** を押します。
2. ▲または▼を押して、[Wi-Fi Direct]を選択し、**OK** を押します。
3. ▲または▼を押して、[PINｺｰﾄﾞ ｾｯﾃｲ]を選択し、**OK** を押します。
4. [Wi-Fi Direct ｵﾝ?]が表示されたら、▲を押して適用します。キャンセルするには、▼を押します。
5. [ｱｲﾃｶﾞﾜ ﾃﾞﾊﾞｲｽ ﾉ Wi-Fi Directｾｯﾃｲ ﾖ ﾕｳｺｳﾆｼﾃ OKﾎﾞﾀﾝ ﾖ ｵｼﾃｸﾀﾞｻｲ]が本製品の画面に表示されたら、携帯端末の Wi-Fi Direct を有効にします。製品の **OK** を押します。

   これにより Wi-Fi Direct セットアップが起動します。キャンセルするには、**Cancel** を押します。
6. 次のいずれかを行ってください。
   - 本製品がグループオーナー（G/O）の場合、携帯端末からの接続要求を待ちます。[PIN Codeﾆｭｳﾘｮｸ]が表示されたら、携帯端末に表示された PIN を本製品に入力します。**OK** を押してセットアップを完了させます。

     本製品に PIN が表示されたら、表示された PIN を携帯端末に入力します。
   - 本製品が G/O ではない場合、Wi-Fi Direct の設定が可能な機器の名前が表示されます。▲または▼を押して、接続したい携帯端末を選択し、**OK** を押します。[<ﾘｽｷｬﾝ>]を押して、利用可能な機器を再検索し、次の手順に進みます。
7. 次のいずれかを行ってください。
   - ▲を押して本製品に PIN を表示し、表示された PIN を携帯端末に入力して、次の手順に進みます。
   - ▼を押して、携帯端末に表示された PIN を、本製品に入力します。**OK** を押して、次の手順に進みます。

     携帯端末に PIN が表示されない場合、本製品の **Cancel** を押します。最初の手順に戻り、再度実行します。
8. 携帯端末が正常に接続されると、本製品の画面に[ｾｯﾂﾞｸ ｾｲｺｳ]と表示されます。以上で Wi-Fi Direct ネットワークのセットアップが完了しました。

関連情報

- Wi-Fi Direct の設定について

関連トピック：

- Wi-Fi Direct ネットワーク設定の概要

Wi-Fi Protected Setup™（WPS）の PIN 方式を使用して Wi-Fi Direct を接続する

お使いの携帯端末で Wi-Fi Protected Setup™（WPS）の PIN 方式がサポートされている場合、以下の手順に従って Wi-Fi Direct を設定します。

1. ▲または▼を押して、[ﾈｯﾄﾜｰｸ]を選択し、**OK** を押します。
2. ▲または▼を押して、[Wi-Fi Direct]を選択し、**OK** を押します。
3. ▲または▼を押して、[ｸﾞﾙｰﾌﾟ ｵｰﾅｰ]を選択し、**OK** を押します。
4. ▲または▼を押して、[ｵﾝ]を選択し、**OK** を押します。
5. ▲または▼を押して、[PINｺｰﾄﾞ ｾｯｿﾞｸ]を選択し、**OK** を押します。
6. [Wi-Fi Direct ｵﾝ?]が表示されたら、▲を押して適用します。キャンセルするには、▼を押します。
7. [ｱｲﾃｶﾞﾜ ﾃﾞﾊﾞｲｽ ﾉ Wi-Fi Directｾｯﾃｲ ﾖ ﾕｳｺｳﾆｼﾃ OKﾎﾞﾀﾝ ﾖ ｵｼﾃｸﾀﾞｻｲ]が本製品の画面に表示されたら、携帯端末の WPS PIN 設定方式を有効にします。**OK** を押します。

   これにより Wi-Fi Direct セットアップが起動します。キャンセルするには、**Cancel** を押します。
8. 携帯端末からの接続要求を待ちます。本製品の画面に[PIN Codeﾆｭｳﾘｮｸ]が表示されたら、携帯端末に表示された PIN を、本製品に入力します。
9. **OK** を押します。
10. 携帯端末が正常に接続されると、本製品の画面に [ｾｯｿﾞｸ ｾｲｺｳ] と表示されます。以上で Wi-Fi Direct ネットワークのセットアップが完了しました。

関連情報

- Wi-Fi Direct の設定について

関連トピック：

- Wi-Fi Direct ネットワーク設定の概要

Wi-Fi Direct を手動で接続する

お使いの携帯端末で、Wi-Fi Direct または WPS が未サポートの場合、Wi-Fi Direct ネットワークを手動で設定する必要があります。

1. ▲または▼を押して、[ﾈｯﾄﾜｰｸ]を選択し、**OK** を押します。
2. ▲または▼を押して、[Wi-Fi Direct]を選択し、**OK** を押します。
3. ▲または▼を押して、[ｼｭﾄﾞｳ ｾｯﾃｲ]オプションを選択し、**OK** を押します。
4. [Wi-Fi Direct ｵﾝ?]が表示されたら、▲を押して適用します。キャンセルするには、▼を押します。
5. 本製品には SSID 名とパスワードが 2 分間表示されます。ご使用の携帯端末の無線ネットワーク設定画面で、この SSID 名を選択して、パスワードを入力します。
6. 携帯端末が正常に接続されると、本製品の画面に[ｾｯﾂﾞｸ ｾｲｺｳ]と表示されます。以上で Wi-Fi Direct ネットワークのセットアップが完了しました。

関連情報

- Wi-Fi Direct の設定について

関連トピック：

- Wi-Fi Direct ネットワーク設定の概要

高度なネットワーク機能について

- ネットワーク設定レポートを印刷する
- 無線 LAN レポートを印刷する
- ウェブブラウザーによる設定画面を使用して SNTP プロトコルを設定する

ネットワーク設定レポートを印刷する

ネットワーク設定リストには、ネットワークプリントサーバーの設定値を含む、ネットワーク設定の一覧が表示されます。

- ノード名：ノード名は、ネットワーク設定リストに表示されます。お買い上げ時のノード名は、有線 LAN の場合は「KMNxxxxxxxxxxxx」、無線 LAN の場合は「KMWxxxxxxxxxxxx」です。（「xxxxxxxxxxxx」は、本製品の MAC アドレス／イーサネットアドレスを示します。）
- ネットワーク設定リストに表示される[IP Address]が 0.0.0.0 の場合、1 分間待ってから、もう一度印刷してください。
- IP アドレス、サブネットマスク、ノード名、および MAC アドレスなどの、本製品の設定をレポートで確認できます。以下は一例です：
  - IP アドレス：192.168.0.5
  - サブネットマスク：255.255.255.0
  - ノード名：KMN000ca0000499
  - MAC アドレス：00-0c-a0-00-04-99

1. ▲または▼を押して、[ｾｲﾋﾝ ｼﾞｮｳﾎｳ]を選択し、**OK** を押します。
2. ▲または▼を押して、[ﾈｯﾄﾜｰｸｾｯﾃｲ ｲﾝｻﾂ]を選択します。
3. **OK** を押します。

関連情報

- 高度なネットワーク機能について

関連トピック：

- 本製品のネットワーク設定はどこを確認すればいいですか？
- 使用しているネットワーク機器が正しく動作していることを確認したい
- ウェブブラウザーによる設定画面にアクセスする
- ウェブブラウザーを使用してギガビットイーサネットを設定する

無線 LAN レポートを印刷する

無線 LAN レポートには、本製品の無線の状態が印刷されます。無線接続に失敗した場合、印刷されたレポートでエラーコードを確認してください。

1. ▲または▼を押して、[ｾｲﾋﾞﾝ ｼﾞｮｳﾎｳ]を選択し、**OK** を押します。
2. ▲または▼を押して、[ﾑｾﾝLANﾚﾎﾟｰﾄ ｲﾝｻﾂ]を選択し、**OK** を押します。
   製品は無線 LAN レポートを印刷します。

関連情報

- 高度なネットワーク機能について
  - 無線 LAN レポートのエラーコード

関連トピック：

- 本製品で、ネットワーク経由の印刷ができません
- 使用しているネットワーク機器が正しく動作していることを確認したい

無線 LAN レポートのエラーコード

無線 LAN レポートに接続の失敗が表示された場合、印刷されたレポートでエラーコードを確認し、エラーに対応する指示を表で確認します。

エラーコード	問題と推奨対策
TS-01	無線設定が有効ではありません。無線設定をオンに変更します。 ネットワークケーブルが本製品に接続されている場合、接続を切断して、本製品の無線設定をオンに変更します。
TS-02	無線 LAN アクセスポイント／ルーターを検出できません。 1. 以下の 2 点を確認します。 • 無線 LAN アクセスポイント／ルーターの電源を切り、10 秒待ってから、再度電源を入れます。 • 無線 LAN アクセスポイント／ルーターが MAC アドレスフィルタリングを使用している場合、本製品の MAC アドレスがそのフィルターで許可されていることを確認します。 2. SSID とセキュリティ情報（SSID／認証方式／暗号化方式／ネットワークキー）を手動で入力した場合、入力した情報が誤っている可能性があります。 SSID とセキュリティ情報を再確認して、必要に応じて正しい情報を再入力してください。 無線セキュリティ情報（SSID／認証方式／暗号化方式／ネットワークキー）の確認方法 a. お買い上げ時のセキュリティ設定が、無線 LAN アクセスポイント／ルーターに貼られているラベルに記載されている場合があります。または、無線 LAN アクセスポイント／ルーターのメーカー名または型番号が、お買い上げ時のセキュリティ設定として使用されている場合があります。 b. 使用している無線 LAN アクセスポイント／ルーターに同梱の説明書をご覧になり、セキュリティ設定値の記載場所を確認してください。 • 無線 LAN アクセスポイント／ルーターが SSID をブロードキャストするように設定されていない場合、SSID は自動的に検出されません。SSID 名を手動で入力する必要があります。 • ネットワークキーは、パスワード、セキュリティキー、または暗号化キーとして記載されることもあります。 本機器は 5GHz SSID/ESSID をサポートしていないため、2.4 GHz SSID/ESSID を選択する必要があります。アクセスポイント／ルーターが、2.4 GHz または 2.4 GHz/5 GHz の混合モードに設定されていることを確認してください。 無線 LAN アクセスポイント／ルーターの SSID および無線セキュリティ設定、または設定の変更方法が分からない場合、無線 LAN アクセスポイント／ルーターに同梱の説明書をご覧になるか、無線 LAN アクセスポイント／ルーターのメーカー、ご契約のインターネットプロバイダーまたはネットワーク管理者にお問い合わせください。
TS-03	入力した無線ネットワークおよびセキュリティ設定が正しくない可能性があります。無線ネットワーク設定を再確認してください。 この情報が分からない場合は、ネットワーク管理者にお問い合わせください。

エラーコード	問題と推奨対策
TS-04	選択された無線 LAN アクセスポイント／ルーターが使用する認証／暗号化方式は、本製品でサポートされていません。 インフラストラクチャモードの場合、無線 LAN アクセスポイント／ルーターの認証および暗号化方式を変更します。本製品は以下の認証方式をサポートしています。 • WPA-Personal TKIP または AES • WPA2-Personal AES • オープン WEP または、なし（暗号化なし） • 共有キー WEP 問題が解決しない場合、入力した SSID またはネットワーク設定が正しくない可能性があります。無線ネットワーク設定を確認してください。 アドホックモードの場合、ご使用のパソコンの無線設定用の認証方式および暗号化方式を変更します。本製品は、オープン認証のみをサポートしており、WEP 暗号化は任意で行います。
TS-05	セキュリティ情報（SSID、ネットワークキー）が正しくありません。 SSID とネットワークキーを確認してください。お使いのルーターが WEP 暗号化方式を使用している場合、最初の WEP キーとして使用されているキーを入力します。本製品は最初の WEP キーのみをサポートします。
TS-06	無線セキュリティ情報（認証方式、暗号化方式、ネットワークキー）が正しくありません。 TS-04 に記載の無線セキュリティ情報（認証方式、暗号化方式、ネットワークキー）を確認してください。お使いのルーターが WEP 暗号化方式を使用している場合、最初の WEP キーとして使用されているキーを入力します。本製品は最初の WEP キーのみをサポートします。
TS-07	本製品は、WPS 対応の無線 LAN アクセスポイント／ルーターを検出できません。 WPS と接続する場合は、本製品と無線 LAN アクセスポイント／ルーターの両方を操作する必要があります。無線 LAN アクセスポイント／ルーターの WPS の接続方式を確認して、再起動してください。 WPS を使用する無線 LAN アクセスポイント／ルーターの操作方法が分からない場合、無線 LAN アクセスポイント／ルーターに同梱の説明書をご覧になるか、無線 LAN アクセスポイント／ルーターのメーカーまたはネットワーク管理者にお問い合わせください。
TS-08	WPS 対応の無線 LAN アクセスポイントが、2 箇所以上検出されています。 • WPS に対応した無線 LAN アクセスポイント／ルーターが範囲内で 1 つのみであることを確認して、再試行します。 • 他のアクセスポイントからの影響を避けるために、数分待ってから再試行してください。

関連情報

- 無線 LAN レポートを印刷する

関連トピック：

- 本製品で、ネットワーク経由の印刷ができません
- 使用しているネットワーク機器が正しく動作していることを確認したい
- Wi-Fi Protected Setup™ （WPS）のワンプッシュ方式を使用して本製品に無線ネットワークを設定する
- Wi-Fi Protected Setup™ （WPS）の PIN 方式を使用して本製品に無線ネットワークを設定する
- 既存の SSID を使用して、アドホックモードで本製品に無線 LAN を設定する
- 新しい SSID を使用して、アドホックモードで本製品に無線 LAN を設定する
- 本製品の操作パネルセットアップウィザードを使用して、無線 LAN を設定する
- SSID が同報送信以外の場合の無線 LAN を本製品に設定する

ウェブブラウザーによる設定画面を使用して SNTP プロトコルを設定する

製品が認証のために使用する時間と、SNTP タイムサーバーにより維持されている時間との同期がとれるように、SNTP プロトコルを設定します。

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「http://製品の IP アドレス」を入力します(「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：

   http://192.168.1.2
3. パスワードを設定している場合はパスワードを入力し、→をクリックします。初期パスワードは、initpass です。
4. **ネットワーク**タブをクリックします。
5. 左側にあるナビゲーションバーの**プロトコル**をクリックします。
6. **SNTP** チェックボックスを選択し、設定を有効にします。
7. SNTP チェックボックスの横にある**詳細設定**をクリックし、以下の指示に従います。

オプション	説明
状態	SNTP プロトコルが有効または無効かを表示します。
同期状態	最新の同期状態を確認します。
SNTP サーバー設定の方法	**AUTO** または **STATIC** を選択します。 • **AUTO** お使いのネットワーク上に DHCP サーバーが存在する場合、SNTP サーバーは、そのサーバーから自動的にアドレスを入手します。 • **STATIC** 使用したいアドレスをクリックします。

オプション	説明
プライマリー SNTP サーバーアドレス **セカンダリー SNTP サーバーアドレス**	サーバーのアドレスを入力します（最大 64 文字）。 セカンダリー SNTP サーバーのアドレスは、プライマリー SNTP サーバーのアドレスのバックアップとして使用されます。プライマリーサーバーが使用不可の場合、製品はセカンダリー SNTP サーバーにアクセスします。
プライマリー SNTP サーバーポート **セカンダリー SNTP サーバーポート**	ポート番号を入力します（1～65535）。 セカンダリー SNTP サーバーポートは、プライマリー SNTP サーバーポートのバックアップとして使用されます。プライマリーポートが使用不可の場合、製品はセカンダリー SNTP ポートにアクセスします。
同期間隔	サーバーの同期処理の間隔を入力します（1～168 時間）。

8. **OK** をクリックします。

関連情報

- 高度なネットワーク機能について

上級ユーザーのための技術的な情報について

ギガビットイーサネット（有線 LAN のみ）

本製品は、1000BASE-T Gigabit Ethernet をサポートしています。1000BASE-T Gigabit Ethernet ネットワークに接続するには、製品の操作パネルまたはウェブブラウザーによる設定画面から、製品のイーサネットリンクモードを「自動」に設定する必要があります。

- 10BASE-T、100BASE-TX Fast Ethernet ネットワーク、または 1000BASE-T Gigabit Ethernet ネットワークには、直通カテゴリー 5（またはそれ以上）のツイストペアケーブルを使用してください。本製品をギガビットイーサネットネットワークに接続する場合、1000BASE-T に準拠しているネットワーク機器を使用してください。

関連情報

- 上級ユーザーのための技術的な情報について
  - ウェブブラウザーを使用してギガビットイーサネットを設定する

ウェブブラウザーを使用してギガビットイーサネットを設定する

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「http://製品の IP アドレス」を入力します(「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：

   http://192.168.1.2
3. パスワードを設定している場合はパスワードを入力し、  をクリックします。初期パスワードは、initpass です。
4. **ネットワーク**タブをクリックします。
5. **有線**をクリックします。
6. 左側にあるナビゲーションバーの**イーサネット**をクリックします。
7. **イーサネットモード**ドロップダウンリストから**自動**を選択します。
8. **OK** をクリックします。
9. 設定を有効にするには、本製品を再起動します。

設定値は、ネットワーク設定リストを印刷して確認することができます。

関連情報

- ギガビットイーサネット（有線 LAN のみ）

関連トピック：

- ネットワーク設定レポートを印刷する

ネットワーク設定をお買い上げ時の設定にリセットする

本製品の操作パネルを使用して、プリントサーバーをお買い上げ時の設定にリセットします。パスワードや IP アドレスなど、すべての情報がリセットされます。

- すべての有線 LAN および無線ネットワークの設定が、お買い上げ時の設定に戻ります。
- ウェブブラウザーを使用して、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こともできます。

1. ▲または▼を押して、［ﾈｯﾄﾜｰｸ］を選択し、**OK** を押します。
2. ▲または▼を押して、［ﾈｯﾄﾜｰｸｾｯﾃｲﾘｾｯﾄ］を選択し、**OK** を押します。
3. ［ﾊｲ］を確認して▲を押します。
   製品が再起動します。

関連情報

- 上級ユーザーのための技術的な情報について

トラブルシューティング

本製品をご使用の際に起こり得る一般的なネットワークの問題は、本章を参照して解決してください。

- 問題解決のための事前トラブルシューティングについて
- 問題の特定と解決について

問題解決のための事前トラブルシューティングについて

本製品の使用時にネットワークに問題が発生した場合、トラブルシューティングの章を参照する前に、確認する事項があります。

以下を必ず確認してください。

- 電源コードが正しく接続され、本製品の電源が入っている。
- アクセスポイント（無線の場合）、ルーター、またはハブの電源が入った状態で、リンクボタンが点滅している。
- テープや保護材などの保護包装は、本製品からすべて取り除かれている。
- トナーカートリッジとイメージングユニットが正しく取り付けられている。
- フロントカバーとバックカバーが完全に閉まっている。
- 用紙トレイに用紙が正しくセットされている。
- （有線 LAN の場合）ネットワークケーブルが、本製品と、ルーターまたはハブに確実に接続されている。

上記事項をすべて確認しても問題が解決しない場合は、カスタマーサポートにお問い合わせください。

関連情報

- トラブルシューティング

問題の特定と解決について

ほとんどのエラーはご自身で解決できます。本ガイドを参照しても問題を解決できない場合、カスタマーサポートに連絡してください。

エラーメッセージ

エラーが発生すると、本製品にエラーメッセージが表示されます。最も一般的なエラーメッセージを表に記載します。

エラーメッセージ	原因	対応
[ﾕｰｻﾞｰﾆﾝｼｮｳ ﾆ ｼｯﾊﾟｲｼﾏｼﾀ. ｶﾝﾘｼｬ ﾆ ﾄｲｱﾜｾﾃｸﾀﾞｻｲ.]	印刷ログのネットワークへの保存機能用の認証設定が正しくありません。	• **認証設定**の**ユーザー名**および **パスワード**が正しいことを確認します。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。 • SNTP タイムサーバーが正確に設定され、設定された時間が、認証のために Kerberos または NTLMv2 により使用される時間と一致することを確認します。
[ｾﾂｿﾞｸ ｴﾗｰ]	他の機器が同時に、Wi-Fi Direct に接続しようとしています。	他に Wi-Fi Direct へ接続しようとしている機器がないことを確認してから、Wi-Fi Direct の設定をもう一度行います。
[ｾﾂｿﾞｸ ｼｯﾊﾟｲｼﾏｼﾀ]	Wi-Fi Direct 設定中に本製品とお使いの携帯端末が通信できません。	• 携帯端末を本製品に近づけます。 • 本製品と携帯端末を、障害物のない場所に移動します。 • WPS の PIN 方式を使用している場合、PIN コードは必ず正確に入力してください。
[ﾌｧｲﾙ ﾍ ｱｸｾｽﾃﾞｷﾏｾﾝ. ｶﾝﾘｼｬ ﾆ ﾄｲｱﾜｾﾃｸﾀﾞｻｲ.]	ネットワークへの印刷ログの保存機能の、保存先フォルダーに本製品がアクセスできません。	• 保存されたディレクトリー名が正しいことを確認します。 • 保存されたディレクトリーが書き込み可能であることを確認します。 • ファイルがロックされていないことを確認します。
[ﾛｸﾞｶｷｺﾐ ﾃﾞｷﾏｾﾝ]	ウェブブラウザーによる設定で、**印刷ログ機能設定**の**書き込みエラー時設定**にある**印刷中止**オプションを選択しています。	このメッセージが画面から消えるまで、約 1 分間お待ちください。
[ﾃﾞﾊﾞｲｽｶﾞ ﾐﾂｶﾘﾏｾﾝ]	Wi-Fi Direct 設定時に、本製品がお使いの携帯端末を認識できません。	• 本製品とお使いの携帯端末が、Wi-Fi Direct モードであることを確認します。 • 携帯端末を本製品に近づけます。 • 本製品と携帯端末を、障害物のない場所に移動します。 • Wi-Fi Direct を手動で設定している場合、パスワードが正しく入力されたことを確認します。 • IP アドレスを取得する方法について、お使いの携帯端末に設定ページがある場合、携帯端末の IP アドレスが DHCP を通して設定されたことを確認します。
[ｻｰﾊﾞｰ ｶﾞ ﾐﾂｶﾘﾏｾﾝ. ｶﾝﾘｼｬ ﾆ ﾄｲｱﾜｾﾃｸﾀﾞｻｲ.]	本製品は、印刷ログのネットワークへの保存機能用のサーバーに接続できません。	• サーバーのアドレスが正しいことを確認します。 • サーバーがネットワークに接続していることを確認します。 • 本製品がネットワークに接続していることを確認します。
[ﾄｹｲ ｶﾞ ﾐｾｯﾃｲﾃﾞｽ. ｶﾝﾘｼｬ ﾆ ﾄｲｱﾜｾﾃｸﾀﾞｻｲ.]	本製品が SNTP タイムサーバーから時間を取得していません。	• SNTP タイムサーバーにアクセスするための設定値が、ウェブブラウザーを使用して正しく設定されていることを確認します。

関連情報

- 問題の特定と解決について

本製品のネットワーク設定はどこを確認すればいいですか？

- ネットワーク設定レポートを印刷する

無線ネットワーク設定を完了できません

お使いの無線 LAN アクセスポイント／ルーターの電源を一度切ってから、再度、入れ直してください。その後、無線接続設定をもう一度、行ってください。それでも、問題が解決しない場合は、以下の指示に従ってください。

無線 LAN レポートを使用して問題を調査します。

原因	対応	インターフェイス
セキュリティ設定（SSID／ネットワークキー）に誤りがあります。	• 無線セットアップヘルパーユーティリティを使用して、セキュリティ設定を確認してください。 • 正しいセキュリティ設定値を選択していることを確認します。 - セキュリティ設定の表示方法については、お使いの無線 LAN アクセスポイント／ルーターの取扱説明書を参照してください。 - 無線 LAN アクセスポイント／ルーターの製造者名またはモデル番号が、お買い上げ時のセキュリティ設定値として使用されている場合があります。 - アクセスポイント／ルーターの製造元、インターネットプロバイダー、またはネットワーク管理者に問い合わせてください。 • SSID およびネットワークキーの定義については、用語集の SSID、ネットワークキー、およびチャンネルの項目を参照してください。	無線
本製品の MAC アドレスが許可されていません。	本製品の MAC アドレスがフィルターで許可されていることを確認してください。MAC アドレスは、本製品の操作パネルで確認できます。	無線
無線 LAN アクセスポイント／ルーターがステルスモードです（SSID の同報送信ではありません）。	• 正しい SSID 名またはネットワークキーを手動で入力します。 • 無線 LAN アクセスポイント／ルーターの説明書で SSID 名またはネットワークキーを確認し、無線ネットワークを再設定します。	無線
セキュリティ設定（SSID／パスワード）に誤りがあります。	• SSID およびパスワードを確認します。 - ネットワークを手動で設定する場合、SSID とパスワードは本製品に表示されます。お使いの携帯端末が手動設定をサポートしている場合、SSID とパスワードは携帯端末の画面に表示されます。 • SSID の定義については、用語集をご覧ください。	Wi-Fi Direct
Android™ 4.0.を使用しています。	携帯端末の接続が切断された場合（Wi-Fi Direct を使用してから約 6 分後）、WPS（推奨）を使ったワンプッシュ設定を試み、本製品を G/O（グループオーナー）として設定してください。	Wi-Fi Direct
本製品がお使いの携帯端末から離れ過ぎています。	本製品を携帯端末の約 1 メートル以内に近づけて、Wi-Fi Direct 接続の設定を行います。	Wi-Fi Direct
本製品と携帯端末との間に何らかの障害物（壁や家具など）があります。	本製品を、障害物のない場所に移動します。	Wi-Fi Direct
本製品または携帯端末の近くに、無線パソコン、Bluetooth 対応機器、電子レンジ、またはデジタルコードレス電話があります。	他の機器を、本製品または携帯端末から離れた場所に移動します。	Wi-Fi Direct
上記の対策すべてを試しても Wi-Fi Direct の設定が完了できない場合は、右記の対応を行ってください。	• 本製品の電源を一度切ってから、再度、入れ直します。Wi-Fi Direct 設定をもう一度行います。 • 本製品をクライアントとして使用している場合、現在の Wi-Fi Direct 接続で許可されている機器の数と、接続されている機器の数を確認します。	Wi-Fi Direct

関連情報

- 問題の特定と解決について

関連トピック：

- SSID が同報送信以外の場合の無線 LAN を本製品に設定する
- Wi-Fi Direct®を使用する

本製品で、ネットワーク経由の印刷ができません

原因	対応	インターフェイス
お使いのセキュリティソフトウェアが、本製品のネットワークへのアクセスをブロックしています。	インストールが正常に完了した場合でも、セキュリティソフトが警告を出さずにアクセスをブロックしている場合があります。 アクセスを許可するには、セキュリティソフトウェアの説明書を参照するか、ソフトウェアの製造元に問い合わせてください。	有線／無線
本製品に、有効な IP アドレスが割り当てられていません。	• IP アドレスとサブネットマスクを確認します。 お使いのパソコンと本製品の、IP アドレスとサブネットマスクがいずれも正確で、同一のネットワーク上に存在することを確認します。 IP アドレスとサブネットマスクの確認方法に関する詳細については、ネットワーク管理者に問い合わせてください。 • （Windows®） ネットワークプリンター診断修復ツールを使用して、IP アドレスとサブネットマスクを確認します。	有線／無線
失敗した印刷ジョブが、パソコンの印刷キューに残っています。	• 失敗した印刷ジョブがパソコンの印刷キューに残っている場合は、そのジョブを削除します。 • もしくは、以下のフォルダーにあるプリンターアイコンをダブルクリックして開き、すべてのドキュメントをキャンセルします： - （Windows® 7） **(スタート) > デバイスとプリンター > プリンターと FAX**をクリックします。 - （Windows® 8.1） マウスポインタをデスクトップの右下隅に移動します。メニューバーが表示されたら、**設定** > **コントロール パネル**をクリックします。**ハードウェアとサウンド**グループで**デバイスとプリンターの表示** > **プリンター**をクリックします。 - （Windows® 10 および Windows Server® 2016） **> Windows システム ツール > コントロール パネル**をクリックします。**ハードウェアとサウンド**グループで、**デバイスとプリンターの表示**をクリックします。 - （Windows Server® 2008） **スタート** > **コントロール パネル** > **プリンタ**をクリックします。 - （Windows Server® 2012） マウスポインタをデスクトップの右下隅に移動します。メニューバーが表示されたら、**設定** > **コントロール パネル**をクリックします。**ハードウェア**グループで**デバイスとプリンターの表示** > **プリンター**をクリックします。 - （Windows Server® 2012 R2 および Window Server® 2019） **スタート**画面で**コントロール パネル**をクリックします。**ハードウェア**グループで**デバイスとプリンターの表示**をクリックします。 - （Mac） **システム環境設定** > **プリンタとスキャナ**をクリックします。	有線／無線
本製品は無線ネットワークに接続されていません。	WLAN レポート（無線 LAN レポート）を印刷して、エラーコードを確認します。	無線

上記の対策をすべて行っても、本製品で印刷できない場合は、プリンタードライバーをアンインストールしてから、再インストールします。

関連情報

- 問題の特定と解決について

関連トピック：

- 無線 LAN レポートを印刷する
- 無線 LAN レポートのエラーコード
- 使用しているネットワーク機器が正しく動作していることを確認したい

使用しているネットワーク機器が正しく動作していることを確認したい

確認	対応	インターフェイス
本製品、アクセスポイント／ルーター、またはネットワークハブの電源が入っていることを確認します。	**以下を確認します。** • 電源コードが正しく接続され、本製品の電源が入っている。 • アクセスポイント／ルーター、またはハブの電源が入った状態で、リンクボタンが点滅している。 • 保護包装は本製品からすべて取り除かれている。 • トナーカートリッジとイメージングユニットが正しくインストールされている。 • 前部と後部のカバーが完全に閉まっている。 • 用紙トレイに用紙が正しくセットされている。 • （有線 LAN の場合）ネットワークケーブルが、本製品と、ルーターまたはハブに確実に接続されている。	有線／無線
ネットワーク設定リストの **Link Status** を確認します。	ネットワーク設定リストを印刷して、**Ethernet Link Status** または **Wireless Link Status** が **Link OK** であることを確認します。	有線／無線
Ping コマンドをつかってパソコンと本製品の接続を確認します。	Windows®のコマンドプロンプトまたは Mac Terminal アプリケーションで、IP アドレスまたはノード名を使用して、パソコンから本製品に Ping を実行します。 ping `[<ipaddress>]`または`[<nodename>]` • 成功：本製品は正常に動作し、お使いのパソコンと同一のネットワークに接続されています。 • 失敗：本製品は、お使いのパソコンと同一のネットワークに接続されていません。 （Windows®） ネットワーク管理者に問い合わせ、IP アドレスとサブネットマスクを修復します。 （Mac） IP アドレスとサブネットマスクが正しく設定されていることを確認します。	有線／無線
本製品が無線 LAN に接続されていることを確認します。	無線 LAN レポートを印刷して、エラーコードを確認します。	無線

上記の対策をすべて試みても問題が解決しない場合は、お使いの無線 LAN アクセスポイント／ルーターの説明書で SSID とネットワークキーの情報を参照し、それらを正しく設定してください。

関連情報

- 問題の特定と解決について

関連トピック：

- ネットワーク設定レポートを印刷する
- 無線 LAN レポートを印刷する
- 無線 LAN レポートのエラーコード
- 本製品で、ネットワーク経由の印刷ができません

セキュリティ

- 本製品の設定値のロックについて
- ネットワークセキュリティ機能

本製品の設定値のロックについて

本製品のアクセスロックをオンにする前に、パスワードを必ずお控えください。パスワードを忘れた場合、管理者またはカスタマーサポートに問い合わせて、本製品に保存されているパスワードをすべてリセットする必要があります。

- ロックの設定の使用について

ロックの設定の使用について

設定ロック機能を使用して、製品への不正アクセスを防ぎます。
ロックの設定を [オン] にすると、製品の設定値にアクセスする場合はパスワードの入力が必要となります。

- 設定ロックパスワードを設定する
- 設定ロックパスワードを変更する
- 設定ロックをオンにする

設定ロックパスワードを設定する

1. ▲または▼を押して、[ｷﾎﾝ ｾｯﾃｲ]を表示し、**OK** を押します。
2. ▲または▼を押して、[ｾｷｭﾘﾃｨ ｾｯﾃｲﾛｯｸ]を表示し、**OK** を押します。
3. パスワード用の 4 桁の数字を入力します。
   各数字を入力するには、▲または▼を押して数字を選択し、**OK** を押します。
4. 画面に[ﾊﾟｽﾜｰﾄﾞｶｸﾆﾝ]と表示されたら、パスワードを再入力します。
5. **Go** を押します。

関連情報

- ロックの設定の使用について

設定ロックパスワードを変更する

1. ▲または▼を押して、[ｷﾎﾝ ｾｯﾃｲ]を表示し、**OK** を押します。
2. ▲または▼を押して、[ｾｷｭﾘﾃｨ ｾｯﾃｲﾛｯｸ]を表示し、**OK** を押します。
3. ▲または▼を押して、[ﾊﾟｽﾜｰﾄﾞ ｾｯﾃｲ]を選択し、**OK** を押します。
4. 現在の 4 桁のパスワードを入力します。
   各数字を入力するには、▲または▼を押して数字を選択し、**OK** を押します。
5. 新しい 4 桁のパスワードを入力します。
   各数字を入力するには、▲または▼を押して数字を選択し、**OK** を押します。
6. 画面に[ﾊﾟｽﾜｰﾄﾞｶｸﾆﾝ]と表示されたら、パスワードを再入力します。
7. **Go** を押します。

関連情報

- ロックの設定の使用について

設定ロックをオンにする

1. ▲または▼を押して、[ｷﾎﾝ ｾｯﾃｲ]を表示し、**OK** を押します。
2. ▲または▼を押して、[ｾｷｭﾘﾃｨ ｾｯﾃｲﾛｯｸ]を表示し、**OK** を押します。
3. 画面に[ｵﾝ]が表示されたら、**OK** を押します。
4. 現在の 4 桁のパスワードを入力します。
   各数字を入力するには、▲または▼を押して数字を選択し、**OK** を押します。

設定ロックを[ｵﾌ]にするには、**OK** を押します。画面に[ﾛｯｸ ｶｲｼﾞｮ?]が表示されたら、▲を押して[ﾊｲ]を選択し、現在の 4 桁のパスワードを入力して、**OK** を押します。

関連情報

- ロックの設定の使用について

ネットワークセキュリティ機能

ネットワークセキュリティ機能を使用する前に

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。

Telnet、FTP サーバー、および TFTP プロトコルを無効にすることを推奨します。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

- ネットワークセキュリティ機能

セキュリティ機能ロック 3.0

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、ここに記載している機能の一部または全部へのアクセスを許可します。

ウェブブラウザーを使用して、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。

- **印刷**

  印刷には、Google Cloud Print™、および iPrint&Scan for Mac を経由するプリントジョブの送信が含まれます。

  ユーザーのログイン名を事前に登録すると、ユーザーはパスワードの入力なしで印刷機能を使用できます。
- **枚数制限**
- **ページカウンター**

関連情報

- セキュリティ機能ロック 3.0

ウェブブラウザー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「http://製品の IP アドレス」を入力します(「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：

   http://192.168.1.2
3. **管理者設定**タブをクリックします。
4. 左側にあるナビゲーションバーの**制限機能**メニューをクリックします。
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. 左側にあるナビゲーションバーの**機能制限**メニューをクリックします。
8. **ユーザーリスト/機能制限**欄に、グループ名またはユーザー名を入力します（最大 15 文字の英数字）。
9. **印刷**列およびその他の列で、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。
10. 最大ページ数を設定するには、**枚数制限**列の**オン**チェックボックスを選択し、**最大ページ数**欄で最大数を入力します。
11. **OK** をクリックします。
12. 左側にあるナビゲーションバーの**ユーザーリスト**メニューをクリックします。
13. **ユーザーリスト**欄で、ユーザー名を入力します。
14. **パスワード**欄で、4 桁のパスワードを入力します。
15. **排紙トレイ設定**ドロップダウンリストをクリックして、各ユーザーの出力トレイを選択します（特定モデルのみ対応）。
16. 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。
17. **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

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。このモードにより、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、Google Cloud Print™、および iPrint&Scan for Mac 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「http://製品の IP アドレス」を入力します(「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：

   http://192.168.1.2
3. **管理者設定**タブをクリックします。
4. 左側にあるナビゲーションバーの**制限機能**メニューをクリックします。
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**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

セキュリティ機能ロック 3.0 追加の機能について

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。

カウンターリセット

ページカウンター列で**カウンターリセット**をクリックして、ページカウンターをリセットします。

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。

前回ログ

カウンターのリセット後でもページ数を本製品に保持する場合は、**前回ログ**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

SSL/TLS を使用したネットワーク製品の安全な管理について

SSL/TLS について

SSL（セキュアソケットレイヤー）またはトランスポート層セキュリティ（TLS）は、LAN または WAN 経由で送信されるデータを保護する効果的な方式です。ネットワーク経由の印刷ジョブなどのデータを暗号化して送信するため、第三者から内容を読み取られることがありません。

SSL/TLS は、有線と無線のネットワークのいずれにも設定可能であり、WPA キーやファイアウォールなど他のセキュリティ形式でも機能します。

関連情報

- SSL/TLS を使用したネットワーク製品の安全な管理について
  - SSL/TLS の略史
  - SSL/TLS を使用するメリットについて

SSL/TLS の略史

SSL/TLS は当初、ウェブ上のトラフィック情報、特にウェブブラウザーとサーバー間で送信されるデータの安全性を確保するために作られました。Internet Explorer®を使用してインターネットバンキングを利用する際、ウェブブラウザー上に https://や小さな鍵アイコンが表示されている場合は、SSL が使用されています。SSL はやがて、オンラインセキュリティに対する共通の解決策として、Telnet、プリンター、FTP など他のアプリケーションともあわせて使用されるようになりました。この当初の設計意図が、今日でも多くのオンライン小売業者や銀行によって採り入れられ、クレジットカード番号や顧客情報など極秘データの安全性を確保しています。

SSL/TLS では非常に高度なレベルの暗号化が用いられ、世界中の銀行から信頼されています。

関連情報

- SSL/TLS について

SSL/TLS を使用するメリットについて

本製品で SSL/TLS を使用する主なメリットは、製品へ送信されたデータの読み込みを未承認のユーザーに対して制限することで、IP ネットワークを介した印刷の安全性を保証することです。SSL の主なメリットは、機密データを安全に印刷するために使用できることです。例えば、大企業の人事部門が定期的に給与明細を印刷しているとします。これら給与明細のデータが暗号化されていない場合、他のネットワークユーザーから読み取られる可能性があります。しかし、SSL/TLS を使用すると、これらのデータを読み取ろうとしても、実際の給与明細ではなく、複雑なコードのページが表示されます。

関連情報

- SSL/TLS について

証明書とウェブブラウザーによる設定について

ネットワークに接続された本製品を SSL/TLS を使用して安全に管理するために、証明書を設定する必要があります。ウェブブラウザーによる設定を使用して証明書を設定してください。

- サポート対象のセキュリティ証明書機能について
- 証明書の作成とインストールについて
- 複数の証明書を管理する

サポート対象のセキュリティ証明書機能について

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、これら証明書により、安全な管理、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、以下に示すセキュリティ証明書機能が使用できます。

- SSL/TLS 通信
- SMTP の SSL 通信
- IEEE 802.1x 認証
- IPsec

本製品は、以下の証明書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、別の証明書の作成やインストールなしで、SSL/TLS 通信が可能になります。

プリインストール自己署名証明書は、通信の危殆化を防ぐことはできません。安全性を強化するために、信頼された組織から発行された証明書をご使用にな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、別の証明書の作成やインストールなしで、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 からの証明書のインストールには、2 種類の方法があります。CA からの証明書がすでに存在する場合、または外部の信頼された CA から取得した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：Certificates Signing Request）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

  証明機関（CA）を特定し、固有のプライベートキーを有する 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、証明機関（CA）から取得した CA 証明書をインポートする必要があります。

- SSL/TLS 通信を行う場合は、あらかじめシステム管理者に問い合わせ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

- 証明書とウェブブラウザーによる設定について

証明書の作成とインストールについて

- 証明書の作成とインストールの手順
- 自己署名証明書の作成とインストールについて
- 認証局（CA）からの証明書の作成とインストールについて
- CA 証明書のインポートとエクスポートについて

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。

選択内容により必要となる操作を簡単に以下に示します。

オプション 1

自己署名証明書

1. ウェブブラウザー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. ウェブブラウザーを使用して、証明書署名要求（CSR）を作成します。
2. ウェブブラウザーを使用して、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

- 証明書の作成とインストールについて

自己署名証明書の作成とインストールについて

- 自己署名証明書を作成する
- 管理者権限を持つ Windows®ユーザー用の自己署名証明書をインストールする
- 自己署名証明書を本製品にインポート、または本製品からエクスポートします。

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「http://製品の IP アドレス」を入力します(「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：

   http://192.168.1.2

   - ドメイン名システムを使用しているか、NetBIOS 名を有効にしている場合、IP アドレスの代わりに「SharedPrinter」など、他の名前を入力することができます。
     - 例：

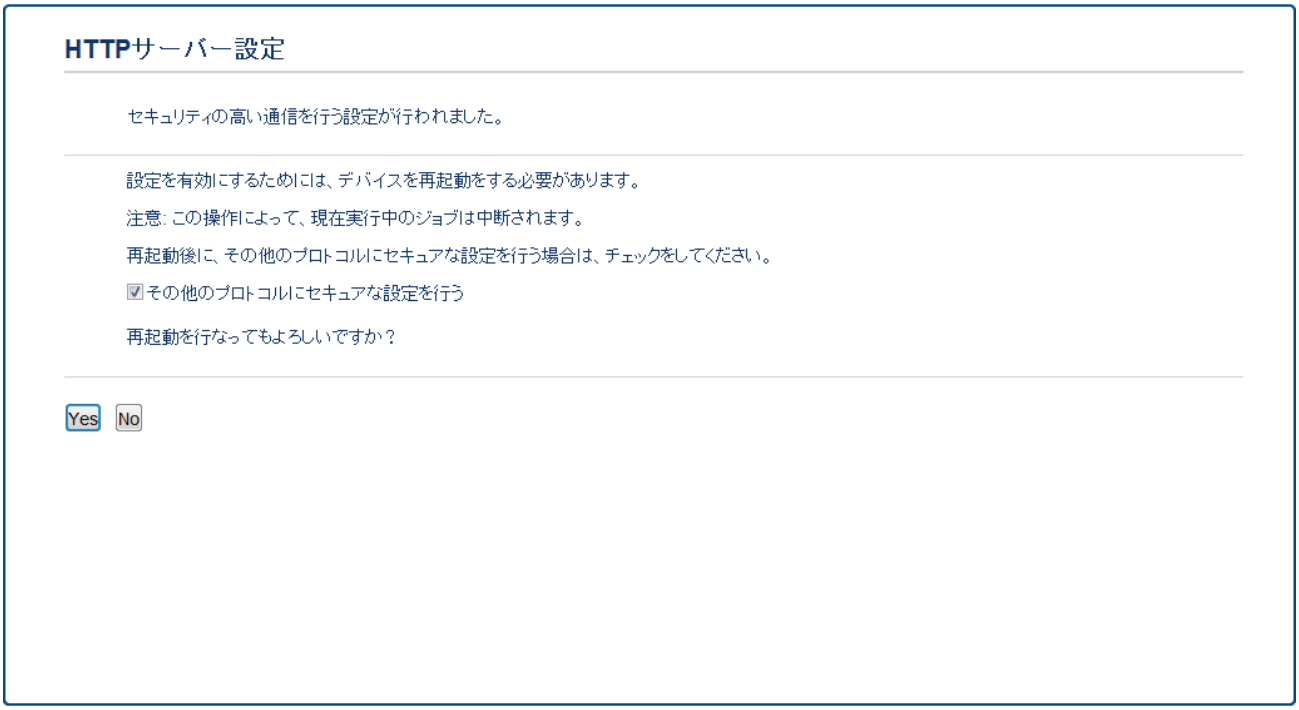
       http://SharedPrinter

     NetBIOS 名を有効にしている場合、ノード名も使用できます。
     - 例：

       http://KMNxxxxxxxxxxx

     NetBIOS 名は、ネットワーク設定リストで確認できます。
3. パスワードを設定している場合はパスワードを入力し、  をクリックします。初期パスワードは、initpass です。
4. **ネットワーク**タブをクリックします。
5. **セキュリティ**タブをクリックします。
6. **証明書**をクリックします。
7. **自己署名証明書の作成**をクリックします。
8. **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。
9. **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。お買い上げ時の設定は **RSA(2048bit)**です。
10. **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。お買い上げ時の設定は **SHA256** です。
11. **OK** をクリックします。
12. **ネットワーク**をクリックします。
13. **プロトコル**をクリックします。
14. **HTTP サーバー設定**をクリックします。
15. **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。
16. **OK** をクリックします。

    以下の画面が表示されます。



17. **はい**をクリックしてプリントサーバーを再起動します。

自己署名証明書が作成され、本製品のメモリーに保存されます。

SSL/TLS 通信を使用するには、お使いのパソコンに自己署名証明書も必ずインストールしてください。

関連情報

- 自己署名証明書の作成とインストールについて

管理者権限を持つ Windows®ユーザー用の自己署名証明書をインストールする

以下は、Microsoft® Internet Explorer®を使用する場合の手順です。その他のウェブブラウザーを使用する場合、そのブラウザーの説明書を参照して証明書をインストールしてください。

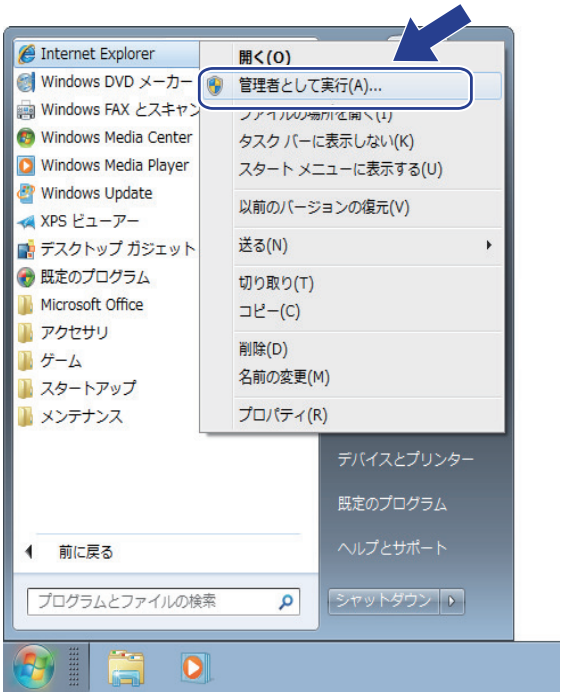
1. 次のいずれかを行ってください。
   - （Windows® 7 および Windows Server® 2008）

     (スタート) > **すべてのプログラム**をクリックします。
   - （Windows® 8.1 および Windows Server® 2019）

     タスクバーの（**Internet Explorer**）アイコンを右クリックします。
   - （Windows® 10 および Windows Server® 2016）

     > **Windows アクセサリ**をクリックします。
   - （Windows Server® 2012 および Windows Server® 2012 R2）

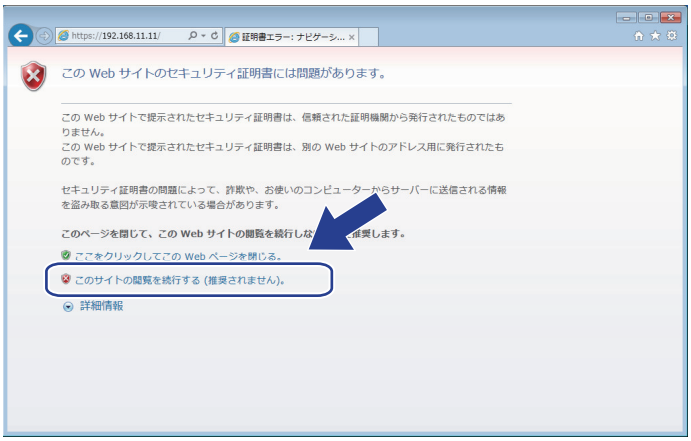
     （**Internet Explorer**）をクリックし、タスクバーに表示された（**Internet Explorer**）アイコンを右クリックします。
2. **Internet Explorer** を右クリックして、**管理者として実行**をクリックします。



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。

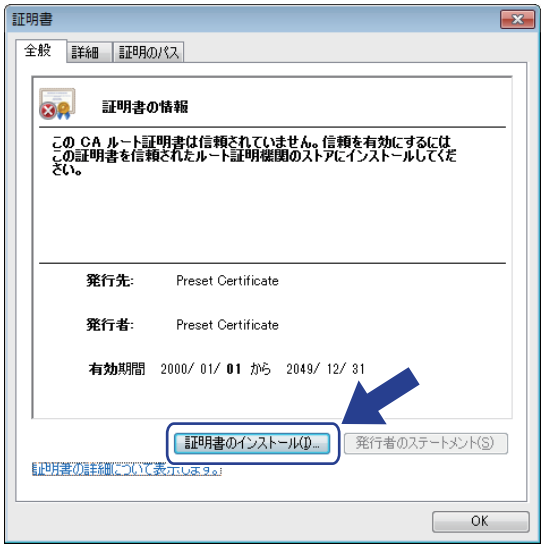
3. ブラウザーのアドレスバーに「https://製品の IP アドレス/」を入力して、本製品にアクセスします(「製品の IP アドレス」には本製品の IP アドレス、または証明書に割り当てたノード名を入力します)。

4. **このサイトの閲覧を続行する（推奨されません）。**をクリックします。

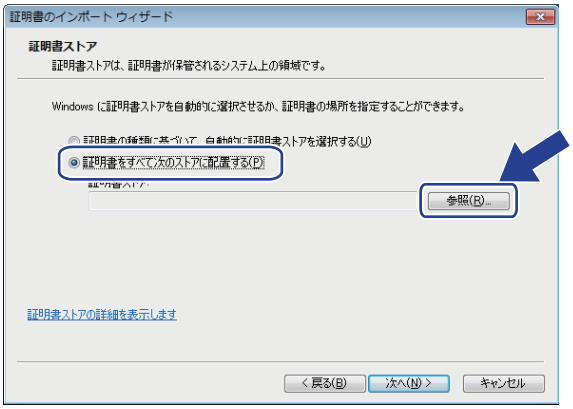


5. **証明書のエラー**をクリックして、**証明書の表示**をクリックします。

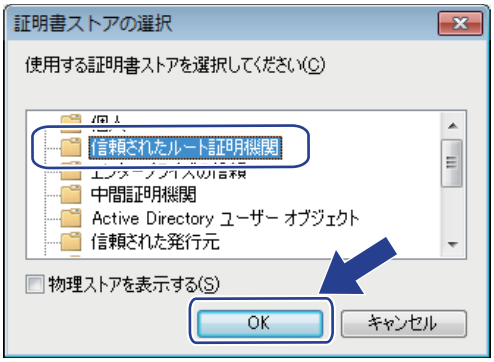
6. **証明書のインストール...**をクリックします。



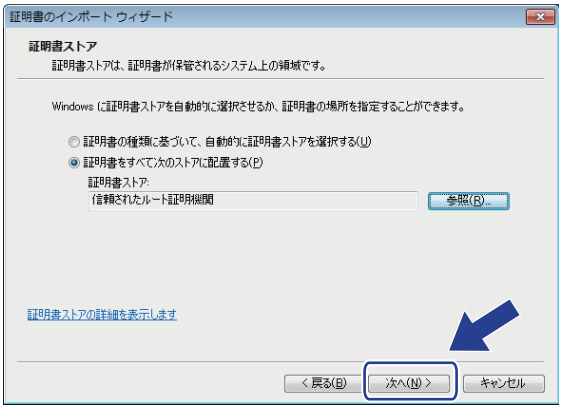
7. **証明書のインポート ウィザード**が表示されたら、**次へ**をクリックします。
8. **証明書をすべて次のストアに配置する**を選択して、**参照...**をクリックします。



9. **信頼されたルート証明機関**を選択して、**OK** をクリックします。



10. **次へ**をクリックします。



11. **完了**をクリックします。
12. フィンガープリント（サムプリント）が正しければ、**はい**をクリックします。

フィンガープリント（サムプリント）は、ネットワーク設定リストに印刷されます。

13. **OK** をクリックします。

自己署名証明書がお使いのパソコンにインストールされ、SSL/TLS 通信が可能になりました。

関連情報

- 自己署名証明書の作成とインストールについて

自己署名証明書を本製品にインポート、または本製品からエクスポートします。

自己署名証明書を本製品に保存し、インポートまたはエクスポートすることで証明書を管理できます。

- 自己署名証明書をインポートする
- 自己署名証明書をエクスポートする

自己署名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「http://製品の IP アドレス」を入力します(「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：

   http://192.168.1.2

   - ドメイン名システムを使用しているか、NetBIOS 名を有効にしている場合、IP アドレスの代わりに「SharedPrinter」など、他の名前を入力することができます。
     - 例：

       http://SharedPrinter

     NetBIOS 名を有効にしている場合、ノード名も使用できます。
     - 例：

       http://KMNxxxxxxxxxxx

     NetBIOS 名は、ネットワーク設定リストで確認できます。
3. パスワードを設定している場合はパスワードを入力し、  をクリックします。初期パスワードは、initpass です。
4. **ネットワーク**タブをクリックします。
5. **セキュリティ**タブをクリックします。
6. **証明書**をクリックします。
7. **証明書と秘密鍵のインポート**をクリックします。
8. インポートするファイルを指定します。
9. 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。

自己署名証明書がお使いの製品にインポートされます。

SSL/TLS 通信を使用するには、お使いのパソコンに自己署名証明書も必ずインストールしてください。インストールについてはネットワーク管理者にお問い合わせください。

関連情報

- 自己署名証明書を本製品にインポート、または本製品からエクスポートします。

自己署名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「http://製品の IP アドレス」を入力します(「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：

   http://192.168.1.2

   - ドメイン名システムを使用しているか、NetBIOS 名を有効にしている場合、IP アドレスの代わりに「SharedPrinter」など、他の名前を入力することができます。
     - 例：

       http://SharedPrinter

     NetBIOS 名を有効にしている場合、ノード名も使用できます。
     - 例：

       http://KMNxxxxxxxxxxx

     NetBIOS 名は、ネットワーク設定リストで確認できます。
3. パスワードを設定している場合はパスワードを入力し、  をクリックします。初期パスワードは、initpass です。
4. **ネットワーク**タブをクリックします。
5. **セキュリティ**タブをクリックします。
6. **証明書**をクリックします。
7. **エクスポート**をクリックします。
8. ファイルを暗号化する場合、**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。
9. **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。
10. ファイルの保存先を指定します。

自己署名証明書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自己署名証明書をインポートすることもできます。

関連情報

- 自己署名証明書を本製品にインポート、または本製品からエクスポートします。

認証局（CA）からの証明書の作成とインストールについて

外部の信頼された 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「http://製品の IP アドレス」を入力します(「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：

   http://192.168.1.2

   - ドメイン名システムを使用しているか、NetBIOS 名を有効にしている場合、IP アドレスの代わりに「SharedPrinter」など、他の名前を入力することができます。

     - 例：

       http://SharedPrinter

     NetBIOS 名を有効にしている場合、ノード名も使用できます。

     - 例：

       http://KMNxxxxxxxxxxx

     NetBIOS 名は、ネットワーク設定リストで確認できます。
3. パスワードを設定している場合はパスワードを入力し、→をクリックします。初期パスワードは、initpass です。
4. **ネットワーク**タブをクリックします。
5. **セキュリティ**タブをクリックします。
6. **証明書**をクリックします。
7. **CSR の作成**をクリックします。
8. **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 バイト以下である必要があります。SSL/TLS 通信を介して本プリンター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。デフォルトでは、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 バイト以下の必要があります。
   - **国**は、2 文字の ISO3166 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。
9. **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。お買い上げ時の設定は **RSA(2048bit)**です。
10. **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。お買い上げ時の設定は **SHA256** です。
11. **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。

12. **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® 2008/2012/2012 R2/2016/2019 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ご使用になることをお勧めします。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ご使用になることをお勧めします。

関連情報

- 認証局（CA）からの証明書の作成とインストールについて

証明書を本製品にインストールする

証明書を CA から受信した後、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 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、CSR 作成前に、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。この証明書を必ず先にインストールしてから、他の CSR を作成してください。この証明書が先にインストールされなかった場合、作成した 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「http://製品の IP アドレス」を入力します(「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：

   http://192.168.1.2

   - ドメイン名システムを使用しているか、NetBIOS 名を有効にしている場合、IP アドレスの代わりに「SharedPrinter」など、他の名前を入力することができます。
     - 例：

       http://SharedPrinter

     NetBIOS 名を有効にしている場合、ノード名も使用できます。
     - 例：

       http://KMNxxxxxxxxxxx

     NetBIOS 名は、ネットワーク設定リストで確認できます。
3. パスワードを設定している場合はパスワードを入力し、  をクリックします。初期パスワードは、initpass です。
4. **ネットワーク**タブをクリックします。
5. **セキュリティ**タブをクリックします。
6. **証明書**をクリックします。
7. **証明書のインストール**をクリックします。
8. 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正常に保存されます。

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。インストールについてはネットワーク管理者にお問い合わせください。

関連情報

- 認証局（CA）からの証明書の作成とインストールについて

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「http://製品の IP アドレス」を入力します(「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：

   http://192.168.1.2

   - ドメイン名システムを使用しているか、NetBIOS 名を有効にしている場合、IP アドレスの代わりに「SharedPrinter」など、他の名前を入力することができます。
     - 例：

       http://SharedPrinter

     NetBIOS 名を有効にしている場合、ノード名も使用できます。
     - 例：

       http://KMNxxxxxxxxxxx

     NetBIOS 名は、ネットワーク設定リストで確認できます。
3. パスワードを設定している場合はパスワードを入力し、  をクリックします。初期パスワードは、initpass です。
4. **ネットワーク**タブをクリックします。
5. **セキュリティ**タブをクリックします。
6. **証明書**をクリックします。
7. **証明書と秘密鍵のインポート**をクリックします。
8. インポートするファイルを表示します。
9. 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。

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も必ずインストールしてください。インストールについては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「http://製品の IP アドレス」を入力します(「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：
   http://192.168.1.2

   - ドメイン名システムを使用しているか、NetBIOS 名を有効にしている場合、IP アドレスの代わりに「SharedPrinter」など、他の名前を入力することができます。
     - 例：
       http://SharedPrinter

     NetBIOS 名を有効にしている場合、ノード名も使用できます。
     - 例：
       http://KMNxxxxxxxxxxx

     NetBIOS 名は、ネットワーク設定リストで確認できます。
3. パスワードを設定している場合はパスワードを入力し、→をクリックします。初期パスワードは、initpass です。
4. **ネットワーク**タブをクリックします。
5. **セキュリティ**タブをクリックします。
6. **証明書**をクリックします。
7. **証明書一覧**に示される**エクスポート**をクリックします。
8. 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。
9. 確認用にパスワードを再入力し、**OK** をクリックします。
10. ファイルの保存先を指定します。

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「http://製品の IP アドレス」を入力します(「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：

   http://192.168.1.2

   - ドメイン名システムを使用しているか、NetBIOS 名を有効にしている場合、IP アドレスの代わりに「SharedPrinter」など、他の名前を入力することができます。
     - 例：

       http://SharedPrinter

     NetBIOS 名を有効にしている場合、ノード名も使用できます。
     - 例：

       http://KMNxxxxxxxxxxx

     NetBIOS 名は、ネットワーク設定リストで確認できます。
3. パスワードを設定している場合はパスワードを入力し、  をクリックします。初期パスワードは、initpass です。
4. **ネットワーク**タブをクリックします。
5. **セキュリティ**タブをクリックします。
6. **CA 証明書**をクリックします。
7. **CA 証明書のインポート**をクリックして、証明書を選択します。
8. **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「http://製品の IP アドレス」を入力します(「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：

   http://192.168.1.2

   - ドメイン名システムを使用しているか、NetBIOS 名を有効にしている場合、IP アドレスの代わりに「SharedPrinter」など、他の名前を入力することができます。
     - 例：

       http://SharedPrinter

     NetBIOS 名を有効にしている場合、ノード名も使用できます。
     - 例：

       http://KMNxxxxxxxxxxx

     NetBIOS 名は、ネットワーク設定リストで確認できます。
3. パスワードを設定している場合はパスワードを入力し、  をクリックします。初期パスワードは、initpass です。
4. **ネットワーク**タブをクリックします。
5. **セキュリティ**タブをクリックします。
6. **CA 証明書**をクリックします。
7. 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。
8. **OK** をクリックします。
9. **保存**をクリックします。
10. エクスポートしたファイルの保存先をご使用のパソコンに指定し、保存します。

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

複数の証明書を管理する

複数証明書の機能により、ウェブブラウザーを使用して、本製品にインストールされている証明書を管理することができます。ウェブブラウザーで、**証明書**または **CA 証明書**画面に移動して、証明書の内容の表示、また削除やエクスポートを行えます。

	本製品に保存できる証明書の最大数
自己署名証明書または、CA 発行の証明書	5
CA 証明書	6

保存する証明書は最大数から 1 個少ない数にし、証明書の期限切れに備えて 1 個分の空きを確保しておくことをお勧めします。証明書の期限が切れた場合、新しい証明書を確保した場所にインポートして、期限切れの証明書を削除します。こうすることで、設定エラーを回避できます。

- HTTPS/IPPS または IEEE 802.1x を使用する場合、使用する証明書を選択する必要があります。
- SMTP 通信に SSL を使用する場合、証明書を選択する必要はありません。必要な証明書は自動的に選択されます。

関連情報

- 証明書とウェブブラウザーによる設定について

ウェブブラウザーを使用してネットワーク製品を安全に管理する

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。

安全な管理のために HTTPS プロトコルをご使用になることをお勧めします。この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。
- ウェブブラウザーによる設定画面で HTTPS プロトコルの設定を変更できます。
  1. **ネットワーク**タブをクリックします。
  2. 左側にあるナビゲーションバーの**プロトコル**メニューをクリックします。
  3. **HTTP サーバー設定**をクリックします。

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://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. パスワードを設定している場合はパスワードを入力し、→をクリックします。初期パスワードは、initpass です。
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。

- SNMPv3 プロトコルを使用する場合は、以下の手順に従います。

5. **ネットワーク**タブをクリックします。
6. **プロトコル**をクリックします。
7. **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。
8. SNMP の設定を行います。

SNMP 動作モードには 3 つのオプションがあります。

- **SNMP v1/v2c read-write access**

  このモードでは、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、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。
- **SNMPv3 read-write access and v1/v2c read-only access**

  このモードでは、プリントサーバーは SNMP プロトコルの、Ver. 3（読み書きアクセス）、および Ver. 1 と Ver. 2c（リードオンリーアクセス）を使用します。
- **SNMPv3 read-write access**

  このモードでは、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、このモードを使用します。

関連情報

- SSL/TLS を使用したネットワーク製品の安全な管理について

SSL/TLS を使用して文書を安全に印刷する

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「http://製品の IP アドレス」を入力します(「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：

   http://192.168.1.2

   - ドメイン名システムを使用しているか、NetBIOS 名を有効にしている場合、IP アドレスの代わりに「SharedPrinter」など、他の名前を入力することができます。
     - 例：

       http://SharedPrinter

     NetBIOS 名を有効にしている場合、ノード名も使用できます。
     - 例：

       http://KMNxxxxxxxxxxx

     NetBIOS 名は、ネットワーク設定リストで確認できます。
3. パスワードを設定している場合はパスワードを入力し、  をクリックします。初期パスワードは、initpass です。
4. **ネットワーク**タブをクリックします。
5. **プロトコル**をクリックします。**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。
   製品の起動後、製品のウェブページに戻り、**ネットワーク**タブ、**プロトコル**の順にクリックします。
6. **HTTP サーバー設定**をクリックします。
7. **HTTPS(ポート 443)**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 を使用したネットワーク製品の安全な管理について

IPsec を使用したネットワーク製品の安全な管理について

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 送信には、以下の条件が必要です。
  - 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、ウェブブラウザー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 を使用したネットワーク製品の安全な管理について

ウェブブラウザーを使用して IPsec を設定する

IPsec の接続条件は、**テンプレート**および**アドレス**の 2 種類の **IPsec** で構成されます。最大 10 種類の条件が設定可能です。

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「http://製品の IP アドレス」を入力します(「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：

   http://192.168.1.2
3. パスワードを設定している場合はパスワードを入力し、  をクリックします。初期パスワードは、initpass です。
4. **ネットワーク**タブをクリックします。
5. **セキュリティ**タブをクリックします。
6. 左側にあるナビゲーションバーの **IPsec** メニューをクリックします。

7. **状態**で、IPsec を有効化または無効化できます。
8. IKE フェーズ 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。

9. **IPsec 以外のトラフィックルール**で、非 IPsec パケットへの対処を選択します。

   Web サービスを使用する場合、**通過**に対して **IPsec 以外のトラフィックルール**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。

10. **Broadcast/Multicast Bypass** で、**有効**または**無効**を選択します。
11. **Protocol Bypass** で、使用するオプションにチェックを入れます。
12. **ルール**で、**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。

13. 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。

14. 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。

15. **OK** をクリックします。

    新しい設定を登録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 Submit をクリックします。

関連情報

- IPsec を使用したネットワーク製品の安全な管理について

ウェブブラウザーを使用して 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「http://製品の IP アドレス」を入力します(「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：

   http://192.168.1.2
3. パスワードを設定している場合はパスワードを入力し、をクリックします。初期パスワードは、initpass です。
4. **ネットワーク**タブをクリックします。
5. **セキュリティ**タブをクリックします。
6. 左側にあるナビゲーションバーの **IPsec アドレステンプレート**メニューをクリックします。

   10 個のアドレステンプレートが、テンプレートリストに表示されます。

   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。
7. 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。

8. **テンプレート名**に、テンプレートの名前を入力します（最大 16 文字）。
9. **ローカル IP アドレス**を選択して、送信者の IP アドレス条件を指定します。
   - **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**

     IP アドレス範囲の開始および終了アドレスを、各テキストボックスに入力します。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**

  CIDR 表記法で IP アドレスを指定します。

  例：192.168.1.1/24

  192.168.1.1 のプレフィックスは 24 ビットのサブネットマスクの形式に指定されるため（255.255.255.0）、192.168.1.xxx のアドレスが有効となります。

10. **リモート IP アドレス**を選択して、受信者の IP アドレス条件を指定します。
    - **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 アドレス範囲の開始および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**

      CIDR 表記法で IP アドレスを指定します。

      例：192.168.1.1/24

      192.168.1.1 のプレフィックスは 24 ビットのサブネットマスクの形式に指定されるため（255.255.255.0）、192.168.1.xxx のアドレスが有効となります。
11. **OK** をクリックします。

現在使用しているテンプレートの設定値を変更する場合、IPsec 画面を一度閉じてから、再び開きます。

関連情報

- IPsec を使用したネットワーク製品の安全な管理について

ウェブブラウザーを使用して 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「http://製品の IP アドレス」を入力します(「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：

   http://192.168.1.2
3. パスワードを設定している場合はパスワードを入力し、  をクリックします。初期パスワードは、initpass です。
4. **ネットワーク**タブをクリックします。
5. **セキュリティ**タブをクリックします。
6. 左側にあるナビゲーションバーの **IPsec テンプレート**をクリックします。

   10 個の IPsec テンプレートがテンプレートリストに表示されます。

   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。
7. 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、選択される**テンプレートを使用する**および **IKE** により異なります。
8. **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)。
9. **IKE** を選択します。
10. **OK** をクリックします。

IPsecテンプレート 1

テンプレート名

テンプレートを使用する　IKEv1高セキュリティ

IKE　IKEv1

認証タイプ

DHグループ	グループ5 グループ14
暗号化方式	AES-CBC 128 AES-CBC 256
ハッシュ	SHA1 SHA256 SHA512
SAライフタイム	28800 秒 (240 – 63072000) 32768 KB (10 – 2097152)

動作セキュリティ

プロトコル	ESP
暗号化方式	AES-CBC 128 AES-CBC 256
ハッシュ	SHA1 SHA256 SHA512
SAライフタイム	3600 秒 (240 – 63072000) 65536 KB (10 – 2097152)
動作モード	◉トランスポート ○トンネル
リモートルーターIPアドレス	

PFS　○有効 ◉無効

認証方式　◉事前共有キー　○証明書

事前共有キー

ローカル

IDタイプ　IPv4アドレス

ID

リモート

IDタイプ　IPv4アドレス

ID

証明書>>

キャンセル　OK

関連情報

- IPsec を使用したネットワーク製品の安全な管理について
  - IPsec テンプレートの IKEv1 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 設定

IPsecテンプレート 1

テンプレート名

テンプレートを使用する　カスタム

IKE　IKEv1　IKEv2　手動

認証タイプ

DHグループ　グループ1

暗号化方式　DES

ハッシュ　MD5

SAライフタイム　86600 秒
(240 – 63072000)
32768 KB
(10 – 2097152)

動作セキュリティ

プロトコル　ESP　AH　AH+ESP

暗号化方式　DES

ハッシュ　MD5

SAライフタイム　43200 秒
(120 – 4233600)
65536 KB
(10 – 4194304)

動作モード　トランスポート　トンネル

リモートルーターIPアドレス

PFS　有効　無効

認証方式　事前共有キー
証明書

事前共有キー

ローカル

IDタイプ　IPv4アドレス

ID

リモート

IDタイプ　IPv4アドレス

ID

証明書>>

キャンセル　OK

テンプレート名

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。

テンプレートの初期値は、設定画面の **IPsec** の**接続モード**で**メイン**または**アグレッシブ**のいずれを選択したかにより異なります。

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

IKE 認証および暗号化を設定します。

- **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 キー交換方式は、秘密キーではなく、離散対数問題を使用して、乱数および秘密キーを使用して生成された公開情報の送受信を行います。

  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+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実行するためのプロトコルです。ESP はペイロード（通信内容）を暗号化して、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により構成されます。暗号化されたデータに加え、IP パケットには、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（データの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**

  DES、**3DES**、**AES-CBC 128**、または **AES-CBC 256** を選択します。この暗号化は、**プロトコル**で **ESP** が選択された場合にのみ選択できます。

- **ハッシュ**

  なし、**MD5**、**SHA1**、**SHA256**、**SHA384**、または **SHA512** を選択します。**なし**は、**プロトコル**で **ESP** が選択された場合にのみ選択できます。

  プロトコルで **AH+ESP** が選択された場合、**ハッシュ(AH)**および**ハッシュ（ESP）**のそれぞれに対してプロトコルを選択します。

- **SA ライフタイム**

  IPsec SA のライフタイムを指定します。

  IPsec SA が無効になるまでの時間（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、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の交換や共有を行う IPsec または IPv6 を使用する暗号化通信方式です。SA は、確立済みの仮想暗号化通信チャネルを指すこともあります。IPsec に使用される SA は、IKE（インターネットキー交換）標準手順に従って、暗号化方式の確立、キーの交換、および相互認証の実行を行います。また、SA は定期的に更新されます。

PFS

PFS は、メッセージの暗号化に使用されたキーからは、キーを生成しません。また、メッセージの暗号化に使用するキーが親キーから生成されたものである場合、その親キーは他のキーの生成には使用されません。そのため、キーの情報が洩れた場合でも、損害はそのキーを使用して暗号化されたメッセージのみに制限されます。

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

通信を暗号化する場合、他のチャネルを使用して、暗号化キーは事前に交換または共有されます。

認証方式に**事前共有キー**を選択した場合、**事前共有キー**を入力します(最大 32 文字)。

- **ローカル/ID タイプ/ID**

  送信者の ID を選択し、その ID を入力します。

  種別には、**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、**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 を選択し、その ID を入力します。

  種別には、**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、**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、ウェブブラウザーによる設定画面のセキュリティ設定の**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

- ウェブブラウザーを使用して IPsec テンプレートを設定する

IPsec テンプレートの IKEv2 設定

IPsecテンプレート 1

テンプレート名

テンプレートを使用する　カスタム

IKE　IKEv1　IKEv2　手動

認証タイプ

DHグループ　グループ1　グループ2　グループ5　グループ14

暗号化方式　DES　3DES　AES-CBC 128　AES-CBC 256

ハッシュ　MD5　SHA1　SHA256　SHA384　SHA512

SAライフタイム　86600 秒 (240 – 63072000)

32768 KB (10 – 2097152)

動作セキュリティ

プロトコル　ESP

暗号化方式　DES　3DES　AES-CBC 128　AES-CBC 256

ハッシュ　MD5　SHA1　SHA256　SHA384　SHA512

SAライフタイム　43200 秒 (120 – 4233600)

65536 KB (10 – 4194304)

動作モード　トランスポート　トンネル

リモートルーターIPアドレス

PFS　有効　無効

認証方式　事前共有キー　証明書　EAP - MD5　EAP - MS-CHAPv2

事前共有キー

ローカル

IDタイプ　IPv4アドレス

ID　0.0.0.0

リモート

IDタイプ　IPv4アドレス

ID　0.0.0.0

証明書>>

キャンセル　OK

テンプレート名

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

IKE 認証および暗号化を設定します。

- **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 キー交換方式は、秘密キーではなく、離散対数問題を使用して、乱数および秘密キーを使用して生成された公開情報の送受信を行います。

  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実行するためのプロトコルです。ESP はペイロード（通信内容）を暗号化して、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により構成されます。暗号化されたデータに加え、IP パケットには、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**

  IPsec SA のライフタイムを指定します。

  IPsec SA が無効になるまでの時間（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、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の交換や共有を行う IPsec または IPv6 を使用する暗号化通信方式です。SA は、確立済みの仮想暗号化通信チャネルを指すこともあります。IPsec に使用される SA は、IKE（インターネットキー交換）標準手順に従って、暗号化方式の確立、キーの交換、および相互認証の実行を行います。また、SA は定期的に更新されます。

PFS

PFS は、メッセージの暗号化に使用されたキーからは、キーを生成しません。また、メッセージの暗号化に使用するキーが親キーから生成されたものである場合、その親キーは他のキーの生成には使用されません。そのため、キーの情報が洩れた場合でも、損害はそのキーを使用して暗号化されたメッセージのみに制限されます。

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。

事前共有キー

通信を暗号化する場合、他のチャネルを使用して、暗号化キーは事前に交換または共有されます。

認証方式に**事前共有キー**を選択した場合、**事前共有キー**を入力します(最大 32 文字)。

- **ローカル/ID タイプ/ID**

  送信者の ID を選択し、その ID を入力します。

  種別には、**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、**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 を選択し、その ID を入力します。

  種別には、**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、**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、ウェブブラウザーによる設定画面のセキュリティ設定の**証明書**ページを使用して作成された証明書のみです。

EAP

EAP は、PPP の拡張認証プロトコルです。IEEE802.1x で EAP を使用することにより、セッションごとに異なるキーがユーザー認証に使用されます。

以下の設定は、**認証方式**で **EAP - MD5** または **EAP - MS-CHAPv2** が選択された場合にのみ必要となります。

- **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）。パスワードは確認のために 2 回入力する必要があります。
- **証明書**

  このボタンをクリックして、**証明書**設定画面に移動します。

関連情報

- ウェブブラウザーを使用して IPsec テンプレートを設定する

IPsec テンプレートの手動設定

テンプレート名

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）

認証に使用するキーを指定します。**In/Out** の値を入力します。

これらの設定が必要になるのは、**動作セキュリティ**に対して、**テンプレートを使用する**に**カスタム**が、**IKE** に**手動**が、**ハッシュ**に**なし**以外の設定値が選択された場合です。

設定可能な文字数は、**動作セキュリティ**で**ハッシュ**のために選択した設定により異なります。

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と異なる場合は、エラーが発生します。

- **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）

ASCII コードでキーを指定する場合、文字列を二重引用符（"）で囲みます。

コードキー（ESP）

暗号化に使用するキーを指定します。**In/Out** の値を入力します。

これらの設定が必要になるのは、**動作セキュリティ**において、**テンプレートを使用する**に**カスタム**が、**IKE** に**手動**が、**プロトコル**に **ESP** が選択された場合です。

設定可能な文字数は、**動作セキュリティ**で**暗号化方式**のために選択した設定により異なります。

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と異なる場合は、エラーが発生します。

- **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）

ASCII コードでキーを指定する場合、文字列を二重引用符（"）で囲みます。

SPI

これらのパラメーターは、セキュリティ情報の特定に使用されます。通常、数種類の IPsec 通信に対応するために、ホストでは複数のセキュリティアソシエーション（SA）を用意しています。そのため、IPsec パケットの受信時に、適用可能な SA を特定する必要があります。SPI パラメーターは、SA を特定するものであり、認証ヘッダー（AH : Authentication Header）とカプセル化セキュリティペイロード（ESP : Encapsulating Security Payload）ヘッダーが含まれます。

これらの設定が必要になるのは、**テンプレートを使用する**に**カスタム**が、**IKE** に**手動**が選択された場合です。

In/Out の値を入力します。（3～10 文字）

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実行するためのプロトコルです。ESP はペイロード（通信内容）を暗号化して、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により構成されます。暗号化されたデータに加え、IP パケットには、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（データの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**

  DES、**3DES**、**AES-CBC 128**、または **AES-CBC 256** を選択します。この暗号化は、**プロトコル**で **ESP** が選択された場合にのみ選択できます。
- **ハッシュ**

  なし、**MD5**、**SHA1**、**SHA256**、**SHA384**、または **SHA512** を選択します。**なし**は、**プロトコル**で **ESP** が選択された場合にのみ選択できます。
- **SA ライフタイム**

  IKE SA のライフタイムを指定します。

  IPsec SA が無効になるまでの時間（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**

  接続先の IP アドレス（IPv4 または IPv6）を指定します。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、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の交換や共有を行う IPsec または IPv6 を使用する暗号化通信方式です。SA は、確立済みの仮想暗号化通信チャネルを指すこともあります。IPsec に使用される SA は、IKE（インターネットキー交換）標準手順に従って、暗号化方式の確立、キーの交換、および相互認証の実行を行います。また、SA は定期的に更新されます。

OK

このボタンをクリックして設定を登録します。

現在使用しているテンプレートの設定値を変更する場合、IPsec 画面を一度閉じてから、再び開きます。

関連情報

- ウェブブラウザーを使用して IPsec テンプレートを設定する

安全な E-mail の送信について

ウェブブラウザーを使用して E-mail の送信を設定する

ユーザー認証を必要とする安全な E-mail 送信や、SSL/TLS を使用した E-mail 送信について、ウェブブラウザーを使用して設定することをお勧めします。

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「http://製品の IP アドレス」を入力します(「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：

   http://192.168.1.2

   - ドメイン名システムを使用しているか、NetBIOS 名を有効にしている場合、IP アドレスの代わりに「SharedPrinter」など、他の名前を入力することができます。
     - 例：

       http://SharedPrinter

     NetBIOS 名を有効にしている場合、ノード名も使用できます。
     - 例：

       http://KMNxxxxxxxxxxx

     NetBIOS 名は、ネットワーク設定リストで確認できます。
3. パスワードを設定している場合はパスワードを入力し、  をクリックします。初期パスワードは、initpass です。
4. **ネットワーク**タブをクリックします。
5. 左ナビゲーションバーの**プロトコル**をクリックします。
6. **SMTP** 欄で、**詳細設定**をクリックして、**SMTP** の状態が**有効**であることを確認します。
7. **SMTP** の設定値を設定します。
   - 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。
   - 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。
8. 設定の完了後、**OK** をクリックします。

   E メール送信設定テストダイアログボックスが表示されます。
9. ダイアログボックスに表示される指示に従って、設定のテストを行ってください。

関連情報

- 安全な E-mail の送信について

ユーザー認証を使用した E-mail 送信について

本製品は、ユーザー認証が必要な E-mail サーバーを経由して E-mail を送信するための SMTP-AUTH 方式をサポートしています。この方式により、非認証のユーザーによる E-mail サーバーへのアクセスが防止されます。

E メール通知および E メールレポートに、SMTP-AUTH 方式を使用できます（特定モデルのみ対応）。

ウェブブラウザーを使用して 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。

SMTP サーバー認証を有効にするには、ウェブブラウザーの **SMTP** 画面内で、**送信メールサーバー認証方式**の **SMTP-AUTH** を選択する必要があります。

関連情報

- 安全な E-mail の送信について

SSL/ TLS を使用した安全な E-mail の送信について

本製品は、SSL/TLS 方式をサポートし、安全な SSL/TLS 通信を必要とする E-mail サーバーを経由して E-mail 送信を行います。SSL/TLS 通信を使用している E-mail サーバーを経由して E-mail を送信するには、SSL/TLS 経由の SMTP を設定する必要があります。

ウェブブラウザーを使用して SSL/TLS を設定することをお勧めします。

サーバー証明書を検証する

SSL/TLS で、**SSL** または **TLS** を選択した場合、**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 により発行された 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。
- サーバー証明書を検証する必要がない場合、**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ます。

関連情報

- 安全な E-mail の送信について

有線または無線 LAN への IEEE 802.1x 認証の使用について

- IEEE 802.1x 認証について
- ウェブブラウザーを使用して有線または無線 LAN の IEEE 802.1x 認証を設定する
- IEEE 802.1x 認証方式

IEEE 802.1x 認証について

IEEE 802.1x は、有線および無線 LAN の 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（サプリカント）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

- 有線または無線 LAN への IEEE 802.1x 認証の使用について

ウェブブラウザーを使用して有線または無線 LAN の 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お問い合わせください。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。

また、以下を使用して IEEE 802.1x 認証を設定することもできます。

- 操作パネルからの無線セットアップウィザード（無線 LAN）
- Utilities CD 上の無線セットアップウィザード（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「http://製品の IP アドレス」を入力します(「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：

   http://192.168.1.2

   - ドメイン名システムを使用しているか、NetBIOS 名を有効にしている場合、IP アドレスの代わりに「SharedPrinter」など、他の名前を入力することができます。
     - 例：

       http://SharedPrinter

     NetBIOS 名を有効にしている場合、ノード名も使用できます。
     - 例：

       http://KMNxxxxxxxxxxx

     NetBIOS 名は、ネットワーク設定リストで確認できます。
3. パスワードを設定している場合はパスワードを入力し、→をクリックします。初期パスワードは、initpass です。
4. **ネットワーク**タブをクリックします。
5. 次のいずれかを行ってください。

オプション	説明
有線 LAN	**有線**をクリックして、**有線 802.1x 認証**を選択します。
無線 LAN	**無線**をクリックして、**無線 (エンタープライズ)**を選択します。

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	説明
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です。
CA 証明書+サーバー ID	サーバー証明書の CA 信頼性に加え、サーバー証明書の共通名 [1] の値を確認する検証方式です。

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	説明
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

- 有線または無線 LAN への IEEE 802.1x 認証の使用について

1 共通名検証では、**サーバー ID** に設定された文字列と、サーバー証明書の共通名を照合します。この方法を使用する前に、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、**サーバー ID** を設定してください。

IEEE 802.1x 認証方式

LEAP （無線ネットワーク）

軽量拡張可能認証プロトコル（LEAP：Lightweight Extensible Authentication Protocol）は、Cisco Systems 社が開発した独自の EAP 方式で、ユーザー ID とパスワードを使用して認証を行います。

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

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

- 有線または無線 LAN への IEEE 802.1x 認証の使用について

印刷ログ機能

印刷ログ機能の概要について

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。

- お使いのパソコンからの印刷ジョブ

- 印刷ログ機能は、Kerberos 認証および NTLMv2 認証をサポートしています。認証のための SNTP プロトコル（ネットワークタイムサーバー）を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

- 印刷ログ機能

ウェブブラウザー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「http://製品の IP アドレス」を入力します(「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：

   http://192.168.1.2
3. パスワードを設定している場合はパスワードを入力し、  をクリックします。初期パスワードは、initpass です。
4. **管理者設定**タブをクリックします。
5. **印刷ログ機能設定**メニューをクリックします。
6. **印刷ログ**欄で、**オン**をクリックします。
7. 以下の設定を行います。

オプション	説明
ネットワークフォルダパス	CIFS サーバー上の、ログの保存先フォルダーを入力します（例：KONICA MINOLTA \abc）。
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。
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** を選択して、Kerberos 認証のみを使用します。 • **NTLMv2**：**NTLMv2** を選択して、NTLMv2 認証のみを使用します。 • **Kerberos** および **NTLMv2** 認証の場合、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。
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。
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 ホストのアドレス（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。

8. **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。
9. **OK** をクリックして、**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。

10. 製品が設定値をテストします。
11. 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

- 印刷ログ機能

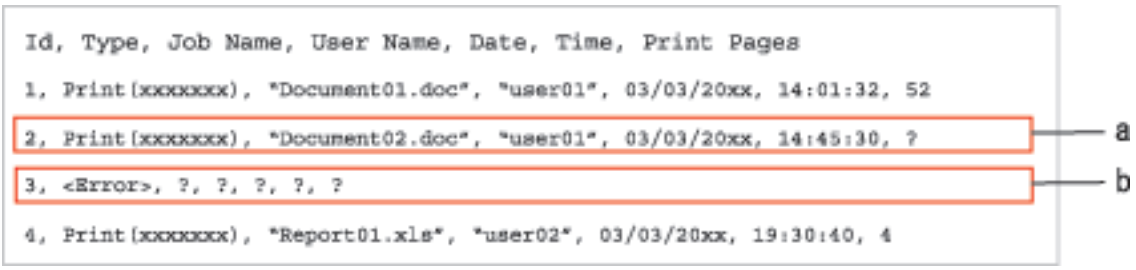
印刷ログ機能のエラー検出設定を使用する

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「http://製品の IP アドレス」を入力します(「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：

   http://192.168.1.2
3. **管理者設定**タブをクリックします。
4. 左側にあるナビゲーションバーの**印刷ログ機能設定**メニューをクリックします。
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**を選択します。

オプション	説明
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。
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。  a. 印刷の最後でログが保存できない場合、印刷ページ数以外の印刷ログが記録されます。 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、該当のエラーがログに反映されます。

6. **OK** をクリックして、**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

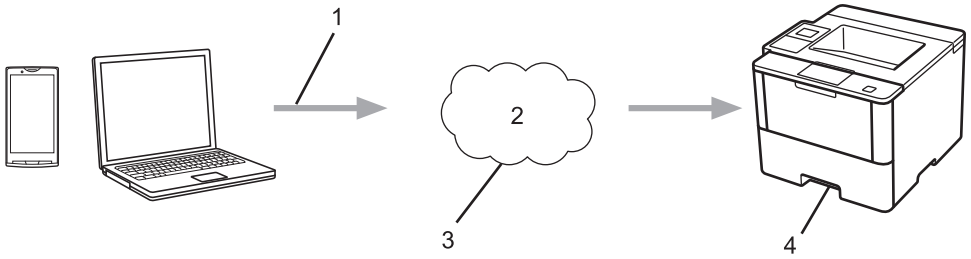
- 印刷ログ機能

モバイル／ウェブ接続

- Google クラウド プリントで印刷する
- Mopria™を使って印刷する
- 携帯端末から印刷する

Google クラウド プリントで印刷する

Google クラウド プリントは Google が提供するサービスで、機器にプリンタードライバーをインストールすることなく、ネットワーク端末（携帯端末やパソコンなど）を使って、Google アカウントに登録されたプリンターで印刷することができます。



1. 印刷リクエスト
2. インターネット
3. Google クラウド プリント
4. 印刷

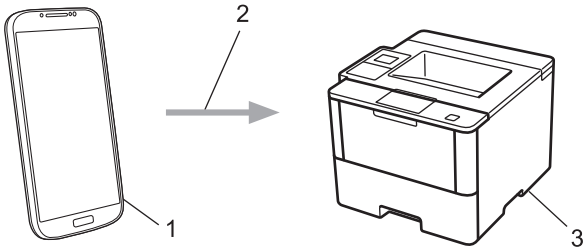
詳しい説明は「Google クラウドプリントガイド」をご覧ください。

関連情報

- モバイル／ウェブ接続

Mopria™を使って印刷する

Mopria™ Print サービスは、Mopria™ Alliance により開発された、 Android™携帯端末（Android™ バージョン 4.4 以降）で動作する印刷機能です。このサービスを使用すると、本製品と同一のネットワークに接続して、追加のセットアップなしで印刷することができます。Google Chrome™、Gmail、および Gallery など、多くのネイティブ Android™ アプリケーションが印刷をサポートしています。



1. Android™ 4.4 以降
2. Wi-Fi®接続
3. 本製品

Google Play™ ストアから Mopria™ Print サービスをダウンロードして、お使いの Android™機器にインストールする必要があります。この機能を使用する前に、サービスを必ずオンにしてください。

関連情報

- モバイル／ウェブ接続

携帯端末から印刷する

Konica Minolta Mobile Print を使用して、さまざまな携帯端末から印刷を行います。

- Android™機器の場合

  Konica Minolta Mobile Print を使用すると、お使いの Android™機器から本製品の機能を直接使用することができます。パソコンは必要ありません。

  Google Play™ ストアから、Konica Minolta Mobile Print をダウンロードして、インストールします。
- iOS 機器の場合

  Konica Minolta Mobile Print を使用すると、お使いの iPhone、iPod touch、iPad、および iPad mini から本製品の機能を直接使用することができます。パソコンは必要ありません。

  App Store から、Konica Minolta Mobile Print をダウンロードして、インストールします。
- Windows Phone®機器の場合

  Konica Minolta Mobile Print を使用すると、お使いの Windows Phone®から本製品の機能を直接使用することができます。パソコンは必要ありません。

  Windows Phone® Store（Windows Phone® Marketplace）から、Konica Minolta Mobile Print をダウンロードして、インストールします。

詳しい説明は Konica Minolta Mobile Print のヘルプを参照してください。

関連情報

- モバイル／ウェブ接続

パソコンを使用して製品の設定を変更する

- ウェブブラウザーを使用して製品の設定を変更する

ウェブブラウザーを使用して製品の設定を変更する

ウェブブラウザーによる設定は、ハイパーテキスト転送プロトコル（HTTP）または SSL（セキュアソケットレイヤー）上のハイパーテキスト転送プロトコル（HTTPS）を使用して本製品を管理するために標準的なウェブブラウザーを使用します。

ウェブブラウザーによる設定とは

ウェブブラウザーによる設定は、ハイパーテキスト転送プロトコル（HTTP）またはセキュアソケットレイヤー上のハイパーテキスト転送プロトコル（HTTPS）を使用して本製品を管理するために標準的なウェブブラウザーを使用します。ご使用のウェブブラウザーに本製品の IP アドレスを入力して、プリントサーバーの設定値の表示や変更を行います。

- Windows®の場合は、Microsoft® Internet Explorer® 11/Microsoft Edge™を、Mac の場合は、Safari 10/11 のブラウザーのご使用をお勧めします。いずれのウェブブラウザーの場合も、JavaScript およびクッキーを有効にして使用してください。上記以外のウェブブラウザーを使用する場合は、HTTP 1.0 および HTTP 1.1 と互換性があることを確認してください。
- ネットワーク上で TCP/IP プロトコルを使用し、プリントサーバーとパソコンに有効な IP アドレスがプログラムされている必要があります。

- 実際の画面は、上記に示した画面とは異なる場合があります。
- 以下の説明は例です。利用可能な機能はモデルにより異なります。

基本設定

このタブを使用して本製品の現在の状態を確認し、タイマーの設定など、基本的な設定を変更します。

印刷

このタブを使用して、印刷設定の確認や変更を行います。

管理者設定

このタブを使用して、ウェブブラウザーのパスワードの設定、各種設定のリセット、および主に管理者が使用する機能の設定を行います。また、セキュリティ機能ロックを使用して、ユーザーに合わせて機能を制限することもできます。

ネットワーク

このタブを使用して、ネットワーク設定の変更、ネットワークプロトコルの有効化または無効化、およびセキュリティと証明書の設定を行います。

関連情報

- ウェブブラウザーを使用して製品の設定を変更する

ウェブブラウザーによる設定画面にアクセスする

- ウェブブラウザーを使用して設定する場合、HTTPS のセキュリティプロトコルをご使用になることをお勧めします。
- ウェブブラウザーによる設定で HTTPS を使用する場合、お使いのブラウザーには警告のダイアログボックスが表示されます。

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「http://製品の IP アドレス」を入力します(「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：

   http://192.168.1.2

   - ドメイン名システムを使用しているか、NetBIOS 名を有効にしている場合、IP アドレスの代わりに「SharedPrinter」など、他の名前を入力することができます。
     - 例：

       http://SharedPrinter

     NetBIOS 名を有効にしている場合、ノード名も使用できます。
     - 例：

       http://KMNxxxxxxxxxxx

     NetBIOS 名は、ネットワーク設定リストで確認できます。
3. パスワードを設定している場合はパスワードを入力し、  をクリックします。初期パスワードは、initpass です。

以上でプリントサーバーの設定を変更する準備が整いました。

プロトコル設定を変更する場合、**OK** をクリックして設定を有効化した後、本製品を再起動する必要があります。

関連情報

- ウェブブラウザーを使用して製品の設定を変更する

関連トピック：

- ネットワーク設定レポートを印刷する

ウェブブラウザーによる設定画面のログインパスワードを設定する

ウェブブラウザーによる設定画面への非認証のアクセスを防ぐために、ログインパスワードを設定することをお勧めします。

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「http://製品の IP アドレス」を入力します(「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：

   http://192.168.1.2

   - ドメイン名システムを使用しているか、NetBIOS 名を有効にしている場合、IP アドレスの代わりに「SharedPrinter」など、他の名前を入力することができます。
     - 例：

       http://SharedPrinter

     NetBIOS 名を有効にしている場合、ノード名も使用できます。
     - 例：

       http://KMNxxxxxxxxxxx

     NetBIOS 名は、ネットワーク設定リストで確認できます。
3. パスワードを設定している場合はパスワードを入力し、→をクリックします。初期パスワードは、initpass です。
4. **管理者設定**をクリックします。
5. **新しいパスワードの入力**欄に、使用するパスワードを入力します（最大 32 文字）。
6. **新しいパスワードの確認**欄に、パスワードをもう一度入力します。
7. **OK** をクリックします。

今後、ウェブブラウザーによる設定画面へアクセスするたびに、**ログイン**欄にこのパスワードを入力して、→をクリックします。

設定後、→をクリックしてログオフします。

関連情報

- ウェブブラウザーを使用して製品の設定を変更する

用語集

本製品のマニュアルに掲載される機能と用語の一覧です。ご利用いただける機能は、お買い上げのモデルによって異なります。

アルファベット あ か さ た な は ま

アルファベット

- LEAP
- LLMNR
- LPD
- LPR
- MAC アドレス
- mDNS
- NetBIOS name resolution
- PEAP
- RARP
- SMTP-AUTH
- SMTP over SSL
- SMTP クライアント
- SNMP
- SNMPv3
- SNTP
- SSID
- SSL/TLS
- TCP/IP
- TELNET
- TKIP
- Vertical Pairing
- WEP
- Wi-Fi Direct®
- WINS
- WINS サーバー

- WPA-PSK/WPA2-PSK
- WPS

あ

- アドホック（Ad-hoc）通信
- 暗号化
- 印刷ログ機能
- インフラストラクチャ（Infrastructure）通信
- ウェブブラウザーによる設定
- オープンシステム

か

- 共有鍵暗号システム
- ゲートウェイ（ルーター）
- 公開鍵暗号システム

さ

- サブネットマスク
- 証明書
- セキュリティ機能ロック 3.0

た

- チャンネル

な

- 認証
- ネットワーク共有印刷
- ネットワークキー
- ネットワーク設定レポート
- ノード名

は

- ピアツーピア
- プロトコル

ま

- 無線 LAN レポート

AES

Advanced Encryption Standard（AES：次世代標準化暗号方式）は、Wi-Fi®認証の安全性の高い暗号化基準です。

APIPA

お使いのネットワーク上に DHCP、BOOTP または RARP サーバーが存在しない場合、Automatic Private IP Addressing（APIPA）プロトコルにより、IP アドレスが 169.254.1.0 から 169.254.254.255 の範囲で自動的に割り当てられます。

ARP

Address Resolution Protocol（ARP）は、IP アドレスから MAC アドレス（イーサネットアドレス）を求めるためのプロトコルです。

BOOTP

ハードディスクを搭載しないディスクレスクライアントシステムが、ネットワークアクセスを行うための IP アドレスやサーバーアドレス、起動用プログラムのロード先などを見つけだし、システムを起動できるようにすることを目的として開発された UDP/IP 上のプロトコルです。

BOOTP を使用するには、ネットワーク管理者にお問い合わせください。

CA

証明機関（CA：Certificate Authority）は、電子的な身分証明書（X.509 証明書）を発行し、証明書内の公開鍵などのデータと、その所有者の結びつきを保証する機関です。

CA 証明書

CA 証明書は、証明機関（CA）自体を証明して、その秘密鍵を所有する証明書です。

CIFS

Common Internet File System（共通インターネットファイルシステム）は、TCP/IP を利用し、ネットワーク上のパソコンからイントラネットまたはインターネット経由でファイルを共有することができます。

CSR

証明書署名要求（CSR）は、証明書の発行を申請するために、申請者から CA に送信されるメッセージです。CSR には、申請者を特定するための情報、申請者が作成したパブリックキー、および申請者のデジタル署名が含まれます。

Custom Raw Port

Custom Raw Port は、TCP/IP ネットワークで一般的に使用されている印刷プロトコルです。初期値は、Port 9100 です。

DHCP

Dynamic Host Configuration Protocol（DHCP）は、IP アドレスやサーバーアドレスなどの設定ファイルを起動時に読み込めるように開発された BOOTP をベースとする上位互換規格のプロトコルです。

DHCP を使用する場合は、ネットワーク管理者にお問い合わせください。

DNS サーバー

Domain Name System（DNS：ドメイン名システム）は、ウェブサイトおよびインターネットドメインの名前を管理するための技術です。お使いのパソコンから IP アドレスを自動的に見つけることができます。

DNS クライアント

本製品は、Domain Name System（DNS）クライアント機能をサポートしています。この機能により、本製品は DNS 名を使用して他の機器と通信することができます。

HTTP

ハイパーテキスト転送プロトコル（HTTP：Hypertext Transfer Protocol）は、パソコンにインストールされている標準ウェブブラウザーを使用して、ネットワーク上のデバイス情報を取得することができます。本製品はウェブサーバーが内蔵されているため、ウェブブラウザーを使用して本製品の管理や設定の変更を行うことができます。

HTTPS

HTTPS（HTTP over SSL/TLS）は、SSL/TLS を使用するハイパーテキスト転送プロトコル（HTTP）です。これにより、ウェブコンテンツの転送や表示が安全に行われます。

IEEE 802.1x

IEEE 802.1x は有線または無線 LAN への接続に使用される、ネットワーク認証の規格です。これにより非認証の接続は制限され、中央当局により認証されたユーザーにのみ接続が許可されます。

IPP

インターネット印刷プロトコル（IPP）を使用すると、インターネット経由でアクセス可能な製品に、文書を直接送信して印刷することができます。

IPPS

IPPS（インターネットプリンティングプロトコル）は、SSL を使用するプリンティングプロトコルです。IPPS は、印刷データの送受信と印刷機器の管理に使用されます。

IPsec

IPsec は、IP プロトコルの任意のセキュリティ機能であり、認証と暗号化のサービスを提供します。

IPv6

IPv6 は次世代インターネットプロトコルです。

IP アドレス

インターネットプロトコル（IP）アドレスは、ネットワークに接続されている各機器を特定する一連の番号で、各機器の住所にあたるものです。IP アドレスは、ピリオドで区切られた 4 つの番号で構成されます。各番号は 0 ～225 までの数字を使用します。

例：ローカルネットワークでは、通常は最後の数字（ホストアドレス部）を変更します。

192.168.1.1

192.168.1.2

192.168.1.3

プリントサーバーに IP アドレスを割り当てる仕組み：

ネットワーク上で DHCP、BOOTP、RARP などの IP アドレス配布サーバーを利用している場合は、IP アドレス配布サーバーから自動的に IP アドレスが割り当てられます。

ローカルネットワークの場合、ルーターに DHCP サーバーが設置されていることがあります。

ネットワーク上で DHCP、BOOTP、RARP などの IP アドレス配布サーバーを利用していない場合は、APIPA 機能により、169.254.1.0 ～ 169.254.254.255 の範囲の IP アドレスが自動的に割り当てられます。

LEAP

軽量拡張可能認証プロトコル（LEAP：Lightweight Extensible Authentication Protocol）は、Cisco Systems 社が開発した独自の EAP 方式で、ユーザー ID とパスワードを使用して認証を行います。LEAP は無線 LAN で使用されます。

LLMNR

Link-Local Multicast Name Resolution（LLMNR：リンクローカルマルチキャスト名前解決）プロトコルは、ネットワークに DNS（ドメイン名システム）サーバーが存在しない場合に、隣接パソコンの名前を解決します。
LLMNR Responder 機能は、Windows®のパソコンで、IPv4 または IPv6 環境のいずれの環境でも動作します。

LPD

ラインプリンターデーモン（LPD または LPR）プロトコルは、TCP/IP ネットワークで一般的に使用されている印刷プロトコルです。

LPR

ラインプリンターデーモン（LPR または LPD）プロトコルは、TCP/IP ネットワークで一般的に使用されている印刷プロトコルです。

MAC アドレス

MAC アドレス（イーサネットアドレス）は、本製品のネットワークインターフェイスに割り当てられた番号です。

mDNS

Multicase DNS（mDNS）を使用すると、プリントサーバーの設定が自動的に行われ、OS X の簡易ネットワーク設定システムで機能するようになります。

NetBIOS name resolution

NetBIOS（Network Basic Input/Output System）は、ネットワークの基本的な入出力システムの名前解決で、ネットワーク接続間の通信に NetBIOS 名を使用して、他の機器の IP アドレスを取得することができます。

PEAP

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、以下の内部認証をサポートしています。

- PEAP/MS-CHAPv2
- PEAP/GTC

RARP

Reverse Address Resolution Protocol（RARP）は、TCP/IP ネットワークにおいて、MAC アドレス（イーサネットアドレス）から IP アドレスを求めるのに使われるプロトコルです。

RARP を使用する場合は、ネットワーク管理者にお問い合わせください。

SMTP-AUTH

SMTP 認証（SMTP-AUTH）は SMTP（インターネット E メール送信プロトコル）を拡張し、送信者の身元を確認する認証方法を取り入れたもので、クライアントから E メールを送信する際のユーザー認証方法です。

SMTP over SSL

SMTP over SSL は、SSL を使用して暗号化された E メールを送信することができます。

SMTP クライアント

簡易メール転送プロトコル（SMTP：Simple Mail Transfer Protocol）クライアントは、インターネットまたはイントラネットを経由して E メールを送信するために用いられます。

SNMP

Simple Network Management Protocol（SNMP：簡易ネットワーク管理プロトコル）は、パソコン、ルーター、ネットワーク対応製品などのネットワーク機器を管理するために使用されます。

SNMPv3

簡易ネットワーク管理プロトコル バージョン 3（SNMPv3：Simple Network Management Protocol version 3）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。

SNTP

簡易ネットワークタイムプロトコル（SNTP）は、TCP/IP ネットワーク内のパソコン、プリンター、端末を含めたネットワーク機器の時刻の設定に用いられます。ウェブブラウザーを使用して SNTP の設定を行うこともできます。

SSID

それぞれの無線 LAN では、独自のネットワーク名を持っており、そのネットワーク名は SSID または ESSID と呼ばれます。SSID は最大 32 文字までの英数字を使用し、アクセスポイントに割り当てられます。SSID は無線 LAN アクセスポイントのネットワーク機器に割り当てられているので、接続するネットワークの無線 LAN アクセスポイントのネットワーク機器と同じ SSID を設定してください。通常は、SSID 情報を含むパケット（ビーコンとも呼ばれます）が無線 LAN アクセスポイントから発信されます。お使いの無線 LAN アクセスポイントのネットワーク機器のパケット（ビーコン）を受信すると、近くにある電波強度が強い無線 LAN を識別することができます。

SSL/TLS

セキュアソケットレイヤー（SSL）またはトランスポート層セキュリティ（TLS）は、LAN または WAN 経由で送信されるデータを保護する効果的な方式です。

TCP/IP

Transmission Control Protocol/Internet Protocol（TCP/IP)は、インターネットや E メールなどの通信に最も一般的に使用されているプロトコルです。このプロトコルは、Windows®、Windows Server®、OS X および Linux®など、ほぼすべてのオペレーティングシステムで使用することができます。

TELNET

TELNET プロトコルを使用すると、使用しているパソコンから、TCP/IP ネットワーク上のリモートネットワーク機器を制御することができます。

TKIP

Temporal Key Integrity Protocol（TKIP）は、WEP の後継にあたる暗号化の規格で、暗号化方式は WEP と同じ RC4 を利用しています。TKIP は一定時間ごと、または一定パケット量ごとにネットワークキーが更新されるため WEP キーによる暗号化よりも高いセキュリティになります。

Vertical Pairing

Vertical Pairing は、Vertical Pairing をサポートしている無線機器を WPS の PIN 方式と Web サービスの特徴を使って、インフラストラクチャネットワークに接続するための機能です。本製品の無線 LAN 設定からプリンタードライバーとスキャナードライバーのインストールまで一連の手順で行うことができます。

WEP

Wired Equivalent Privacy（WEP）は、IEEE802.11 で標準化されている暗号化方式です。無線 LAN アクセスポイントやクライアントで共通のネットワークキー（WEP キー）を設定して通信の暗号化を行います。

Wi-Fi Direct®

Wi-Fi Direct は、Wi-Fi Alliance®により開発された無線設定方法の一つです。Wi-Fi 標準の安全な接続方式で、無線 LAN アクセスポイントを使用せずに機器同士を互いに接続することができます。

WINS

Windows® Internet Name Service (WINS)とは、NetBIOS name resolution の情報提供サービスです。

WINS サーバー

Windows® Internet Name Service (WINS)サーバーは、IP アドレスを Windows®ネットワーク内のパソコン名（NetBIOS 名）と関連付けます。

WPA-PSK/WPA2-PSK

WPA-PSK/WPA2-PSK は、Wi-Fi Alliance® が提唱する事前共有キーを使用した認証方式です。WPA-PSK の TKIP、または WPA-PSK、WPA2-PSK の AES の暗号キーを使用して、本製品をアクセスポイントに接続します。

WPS

Wi-Fi Protected Setup™（WPS）は、安全な無線ネットワークの設定を可能にする規格です。WPS は 2007 年に Wi-Fi Alliance®により作成されました。

アドホック（Ad-hoc）通信

無線 LAN アクセスポイントを経由しないで、直接それぞれの無線 LAN 端末間で通信するネットワークです。このタイプのネットワークは、アドホックモードまたはピア・ツー・ピア・ネットワークとも呼ばれています。

暗号化

ほとんどの無線ネットワークは、何らかのセキュリティ設定を使用しています。これらのセキュリティ設定には、認証方式（ネットワークにアクセスをしようとしている機器にアクセス権があるかどうかを判断する方法）と暗号化方式（データを暗号化することにより第 3 者によりデータの傍受を防ぐ方法）の設定があります。本製品を無線 LAN に確実に接続するためには、これらの設定を正しく行う必要があります。

パーソナル（無線 LAN）モードでの暗号化方式

パーソナル（無線 LAN）モードとは、IEEE 802.1x をサポートしていないローカルネットワーク（家庭内無線ネットワークなど）です。

- なし
  暗号化を行いません。
- WEP
  共通の暗号キーを設定してデータを暗号化し、送受信を行います。

- TKIP

  一定時間ごと、または一定パケット量ごとに暗号キーが更新されるため、WEP キーによる暗号化よりも高いセキュリティになっています。
- AES

  米国商務省標準技術局（NIST）によって制定された、TKIP より強力な暗号化方式です。

- IEEE 802.11n は、WEP および TKIP のいずれもサポートしていません。
- IEEE 802.11n を使用している無線 LAN に接続する場合は、AES を選択してください。

エンタープライズ無線 LAN 用の暗号化方式

エンタープライズ無線ネットワークは、IEEE 802.1x をサポートしている大規模ネットワークであり、企業無線ネットワーク上で本製品を利用する場合などに使われます。IEEE 802.1x をサポートしている無線ネットワーク上で本製品を設定する場合、以下の暗号化方式を使用できます。

- TKIP
- AES
- CKIP

  シスコシステムズ社独自の LEAP のためのキー統合プロトコル

印刷ログ機能

印刷ログ機能を使用すると、CIFS 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を保存できます。

インフラストラクチャ（Infrastructure）通信

無線 LAN アクセスポイントを経由して、それぞれの無線 LAN 端末が通信するネットワークです。インフラストラクチャモードとも呼ばれています。

ウェブブラウザーによる設定

標準的なウェブブラウザーで、ハイパーテキスト転送プロトコル（HTTP）と SSL 経由のハイパーテキスト転送プロトコル（HTTPS）を使用して本製品を管理できます。ウェブブラウザーを使用してネットワーク上の製品から、一覧表示された機能を実行したり、以下の情報を取得することができます。

- 製品の状態についての情報
- TCP/IP 情報など、ネットワーク設定の変更
- ギガビットイーサネットを設定する
- セキュリティ機能ロック 3.0 の設定
- 印刷ログ機能の設定
- 本製品およびプリントサーバーのソフトウェアバージョン情報
- ネットワークおよび製品の設定情報の変更

ウェブブラウザーによる設定を使用するには、ネットワーク上で TCP/IP プロトコルを使用し、プリントサーバーとパソコンに有効な IP アドレスがプログラムされている必要があります。

オープンシステム

オープンシステムは、ネットワーク認証方式の 1 つです。認証を行わず、すべてのネットワークアクセスを許可します。

共有鍵暗号システム

共有鍵暗号システムは、暗号化するための公開鍵と復号化するための秘密鍵に、同じキーを用いる暗号方法です。

ゲートウェイ（ルーター）

ゲートウェイは、他のネットワークへの入口として機能するネットワークポイントで、そのネットワークを介して転送されたデータを目的の場所に送信します。ルーターは、ネットワークとネットワークを中継する装置です。異なるネットワーク間の中継地点で送信されるデータを正しく目的の場所に届ける働きをしています。このルーターが持つ IP アドレスをゲートウェイのアドレスとして設定します。ルーター IP アドレスが不明の場合は、ネットワーク管理者に問い合わせてください。

公開鍵暗号システム

公開鍵暗号システムは、秘密鍵と公開鍵で一対の鍵を使用して、暗号化するための公開鍵と復号化するための秘密鍵に、それぞれ異なるキーを用いる暗号方法です。

サブネットマスク

サブネットマスクは、ネットワークを複数の物理ネットワークに分割するのに使用します。

以下の例では、IP アドレスの最後のセグメントがホストアドレス、最初の 3 つのセグメントがネットワークアドレスとなります。

例：パソコン 1 とパソコン 2 にデータを直接通信する。

- パソコン 1

  IP アドレス：192.168.1.2

  サブネットマスク：255.255.255.0
- パソコン 2

  IP アドレス：192.168.1.3

  サブネットマスク：255.255.255.0

0 は、アドレスのこの部分での通信に制限がないことを示します。

証明書

公開鍵と本人を結びつける情報です。証明書を用いて、個人に所属する公開鍵を確認することができます。形式は、X.509 規格で定義されています。

セキュリティ機能ロック 3.0

セキュリティ機能ロック 3.0 は利用可能な機能を制限し、安全性を高めます。

チャンネル

無線 LAN では通信のためにチャンネルが使われます。それぞれのチャンネルはすでに決められた異なる周波数帯域を持っており、14 種類のチャンネルを使用することができます。利用可能なチャンネルは、多くの国で制限が設けられています。

認証

ほとんどの無線ネットワークは、何らかのセキュリティ設定を使用しています。これらのセキュリティ設定により、認証（機器がネットワークに対して機器自体を特定する方法）および暗号化（ネットワークにデータを送信する際の暗号化の方法）が定義されます。本製品の無線機器の設定時にこれらのオプションが正しく指定されないと、無線 LAN に接続できません。そのため、これらのオプションは慎重に設定してください。

個人的な無線 LAN 用の認証方式

個人的な無線 LAN とは、IEEE 802.1x をサポートしていない小規模ネットワークです（家庭内無線ネットワークなど）。

- オープンシステム

  無線機器は、認証なしでネットワークへアクセスできます。
- 共有キー

  事前定義された秘密キーが、無線 LAN にアクセスするすべての機器に共有されます。本製品の無線機器は、WEP キーを事前定義されたキーとして使用します。
- WPA-PSK/WPA2-PSK

  Wi-Fi Protected Access® Pre-shared key（WPA-PSK/WPA2-PSK）を有効にします。このキーにより、本製品の無線機器が、WPA-PSK 用 TKIP または、WPA-PSK および WPA2-PSK（WPA-Personal）用 AES を使用するアクセスポイントと関連付けられます。

エンタープライズ無線 LAN 用の認証方式

エンタープライズ無線ネットワークは、IEEE 802.1x をサポートしている大規模ネットワークであり、企業無線ネットワーク上で本製品を利用する場合などに使われます。IEEE 802.1x をサポートしている無線ネットワーク上でお使いの製品を設定する場合、以下の認証方式を使用できます。

- LEAP
- EAP-FAST
- PEAP
- EAP-TTLS
- EAP-TLS

これら認証方式には、64 文字未満のユーザー ID と、32 文字未満のパスワードが使用されます。

ネットワーク共有印刷

ネットワーク共有印刷は、ネットワーク共有環境で行う印刷のタイプです。ネットワーク共有環境では、各コンピュータがサーバーまたはプリントサーバー経由でデータを送信します。

ネットワークキー

ネットワークキーはパスワードであり、データを暗号化または復号化する場合に使用されます。ネットワークキーは、パスワード、セキュリティキー、または暗号化キーとしても記載されます。以下の表に、各設定に使用するキーの文字数を示します。

WEP を使用するオープンシステム／共有キー

このキーは 64 ビットまたは 128 ビットの値を持ち、ASCII または 16 進数の形式で入力する必要があります。

	ASCII	16 進数
64（40）ビット	5 個の文字を使用します。 例：「WSLAN」（大文字と小文字を区別する）	10 ケタの 16 進数データを使用します。 例：「71f2234aba」（大文字と小文字を区別しない）

128（104）ビット	13 個の文字を使用します。 例：「Wirelesscomms」（大文字と小文字を区別する）	26 ケタの 16 進数データを使用します。 例：「71f2234ab56cd709e5412aa2ba」（大文字と小文字を区別しない）

WPA-PSK/WPA2-PSK および TKIP または AES

最長 63 文字で、8 文字以上の事前共有キー（PSK：Pre-Shared Key）を使用します。

ネットワーク設定レポート

ネットワーク設定レポートは、ネットワークプリントサーバーの設定を含む、現在のネットワーク設定を一覧表示したレポートです。

ノード名

ノード名は、ネットワーク上の製品名です。WINS サーバーに登録されている NetBIOS 名になります。お買い上げ時のノード名は、有線 LAN の場合は［KMNxxxxxxxxxxx］、無線 LAN の場合は［KMWxxxxxxxxxxx］となっています。（「xxxxxxxxxxx」は MAC アドレス（イーサネットアドレス）です。）

ピアツーピア

ピアツーピアは、各パソコンが本製品と直接データを送受信します。ファイルの送受信を操作するサーバーやプリントサーバーなどは必要ありません。

プロトコル

プロトコルは、ネットワーク上でデータを送信するための、標準化された一連の規則です。ユーザーはプロトコルを使用して、ネットワーク接続されたリソースにアクセスできます。本製品で使用されているプリントサーバーは、転送制御プロトコル／インターネットプロトコル（TCP/IP：Transmission Control Protocol/Internet Protocol）をサポートしています。

無線 LAN レポート

無線 LAN レポートには、本製品の無線の状態が印刷されます。無線接続に失敗した場合、印刷したレポートのエラーコードを確認してください。

ACET-9920-00