



KONICA MINOLTA

ユーザーズガイド パソコン活用&ネットワーク

bizhub 4020i

■ 本ガイドの使い方

- ・ 対象となるモデル
- ・ 注意事項の定義
- ・ 商標
- ・ 重要事項

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。

bizhub 4020i










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。
[[XXXXXX]]	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、SharePoint、Internet Explorer、Outlook、PowerPoint、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、Safari、iPad、iPhone、iPod touch および OS X は、米国およびその他の国で登録されている、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（アドビシステムズ社）の登録商標または商標です。

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。

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

Flickr®は、Yahoo! Inc.の登録商標です。

Android、Google Cloud Print、Google Drive、Google Play、Picasa Web Albums および Google Chrome 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 社の商標です。

UNIX は、米国およびその他の国におけるオーブングループの登録商標です。

Linux は、米国およびその他の国における Linus Torvalds の登録商標です。

Evernote は、Evernote 社の商標であり、ライセンスの元で使用されています。

本マニュアルで言及したソフトウェアの製造企業は、独自のプログラムに固有のソフトウェアライセンス契約を有します。

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](#)
-

印刷

- パソコンから印刷する(Windows®)
- パソコンから印刷する(Mac)
- 印刷ジョブをキャンセルする
- テスト印刷

パソコンから印刷する(Windows®)

- [文書を印刷する \(Windows®\)](#)
- [セキュリティ印刷 \(Windows®\)](#)
- [初期値の印刷設定を変更する\(Windows®\)](#)

文書を印刷する (Windows®)

ラベル、厚紙、封筒の場合、プリンターで用紙サイズと用紙のタイプを設定してから印刷ジョブを送信してください。

1. 印刷するドキュメントで、印刷ダイアログボックスを開きます。
2. 必要に応じて、設定を調整します。
3. ドキュメントを印刷します。

プリンタードライバの機能の詳細については、プリンタードライバのヘルプを参照してください。



関連情報

- [パソコンから印刷する\(Windows®\)](#)

セキュリティ印刷 (Windows®)

セキュリティ印刷を使用して、機密文書や取り扱いに注意が必要な文書を印刷する場合に、本製品の操作パネルでパスワードの入力が求められるようにします。

- 本製品の電源を切ると、セキュリティデータは本製品から削除されます。

1. アプリケーションの印刷メニューを選択します。
2. **KONICA MINOLTA XXXX** (XXXX はお使いのモデル名) を選択し、印刷プロパティまたは詳細設定ボタンをクリックします。
プリンタードライバの設定画面が表示されます。
3. **基本設定**タブをクリックします。
4. **ジョブの印刷/保存**欄で、**機密印刷**を選択します。
5. **パスワード**欄に 4 桁のパスワードを入力し、**OK** をクリックします。



ドキュメント毎に個別のパスワードを設定する必要があります。

6. **OK** をクリックします。
7. 印刷を実行します。
8. 本製品の操作パネルで、左右にフリックするか、◀または▶を押して[セキュリティ印刷]を表示し、[セキュリティ印刷]を押します。
9. 上下にフリックするか、▲または▼を押してユーザー名を表示し、お使いのユーザー名を押します。
画面には、この名前に対する安全なジョブが一覧表示されます。
10. 上下にフリックするか、▲または▼を押して印刷ジョブを表示し、印刷したい印刷ジョブを押します。
11. 4 桁のパスワードを入力し、[OK]を押します。
12. 枚数を入力します。
13. [スタート]を押します。
データが印刷されます。

セキュリティデータは印刷後、本製品のメモリーから削除されます。



関連情報

- [パソコンから印刷する\(Windows®\)](#)

初期値の印刷設定を変更する(Windows®)

アプリケーション内で印刷設定を変更すると、その変更はそのアプリケーションで印刷しているファイルにしか適用されません。Windows®アプリケーションすべてでその設定を使用したい場合は、この手順に従って初期値の印刷設定を変更してください。

1. 次のいずれかを行ってください。

- (Windows Server® 2008 の場合)

 (スタート) > コントロール パネル > ハードウェアとサウンド > プリンタをクリックします。


- (Windows® 7 および Windows Server® 2008 R2 の場合)

 (スタート) > デバイスとプリンターをクリックします。

- (Windows® 8.1 の場合)

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**をクリックして、**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® 10 および Windows Server® 2016 の場合)

 > **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® 2012 の場合)

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**をクリックして、**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。

- (Windows Server® 2012 R2 および Windows Server® 2019 の場合)

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。

2. **KONICA MINOLTA XXXX** アイコン (XXXX はお使いのモデル名) を右クリックして、**プリンターのプロパティ**を選択します。プリンタードライバのオプションが表示された場合は、お使いのドライバーを選択します。

3. **全般**タブをクリックし、**印刷設定**または**基本設定**ボタンをクリックします。

プリンタードライバダイアログボックスが表示されます。



- トレイ設定を行うには、**装置情報**タブをクリックします。
- プリンターポートを変更するには、**ポート**タブをクリックします。

4. すべての Windows®プログラムでデフォルトとして使いたい印刷設定を選択します。

5. **OK** をクリックします。

6. プリンタープロパティダイアログボックスを閉じます。



関連情報

- [パソコンから印刷する\(Windows®\)](#)
 - [ペーパーフィーダーユニットを設定する \(Windows®\)](#)

ペーパーフィーダーユニットを設定する (Windows®)

本製品のプロパティにアクセスして、ペーパーフィーダーユニットとシリアル番号を自動検出します。

プリンタードライバーのインストール中に、ペーパーフィーダーユニットがプリンタードライバーにより自動的に検出されます。ドライバーのインストール後にペーパーフィーダーユニットを追加する場合は、以下の手順に従って設定してください。

1. 次のいずれかを行ってください。

- (Windows Server® 2008 の場合)

 (スタート) > コントロール パネル > ハードウェアとサウンド > プリンタをクリックします。


- (Windows® 7 および Windows Server® 2008 R2 の場合)

 (スタート) > デバイスとプリンターをクリックします。

- (Windows® 8.1 の場合)

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**をクリックして、**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® 10 および Windows Server® 2016 の場合)

 > **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® 2012 の場合)

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**をクリックして、**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。

- (Windows Server® 2012 R2 および Windows Server® 2019 の場合)

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。

2. **KONICA MINOLTA XXXX** アイコン (XXXX はお使いのモデル名) を右クリックして、**プリンターのプロパティ**を選択します。プリンタードライバーのオプションが表示された場合は、お使いのドライバーを選択します。

3. **装置情報**タブを選択します。

4. **装置情報取得**ボタンをクリックします。

ペーパーフィーダーユニットと本製品のシリアル番号は、自動的に検出されます。

5. **適用**ボタンをクリックします。

本製品が以下の状態の場合は、**装置情報取得**機能は利用できません。

- 本製品の電源がオフになっている。
- 本製品でエラーが発生している。
- 本製品がネットワーク共有環境にある。
- ケーブルが本製品に正しく接続されていない。



関連情報

- [初期値の印刷設定を変更する\(Windows®\)](#)

パソコンから印刷する(Mac)

- 文書を印刷する (Mac)
- セキュリティ印刷 (Mac)
- ペーパーフィーダーユニットを設定する (Mac)

文書を印刷する (Mac)

1. 用紙トレイに正しいサイズ of 用紙がセットされているかを確認します。
2. テキストエディット等のアプリケーションから、**ファイル**メニューをクリックし、**プリント**を選択します。
3. **KONICA MINOLTA XXXX** を選択します (XXXX はお使いのモデル名)。
4. 印刷したい部数を**部数**欄に入力します。
5. **用紙サイズ**のポップアップメニューをクリックし、用紙サイズを選択します。
6. 印刷したい文書の向きに合った**方向**を選択します。
7. アプリケーションのポップアップメニューをクリックし、**印刷設定**を選択します。
印刷設定が表示されます。
8. **用紙種類**のポップアップメニューをクリックして、使用する用紙の種類を選択します。
9. 必要に応じて他の印刷設定を変更します。
10. **プリント**をクリックします。



関連情報

- ・ [パソコンから印刷する\(Mac\)](#)

セキュリティ印刷 (Mac)

セキュリティ印刷を使用して、機密文書や取り扱いに注意が必要な文書を印刷する場合に、本製品の操作パネルでパスワードの入力が求められるようにします。

- 本製品の電源を切ると、セキュリティデータは本製品から削除されます。

1. テキストエディット等のアプリケーションから、**ファイル**メニューをクリックし、**プリント**を選択します。
2. **KONICA MINOLTA XXXX** を選択します (XXXX はお使いのモデル名)。
3. **詳細を表示**をクリックします。
4. ダイアログボックスから**プリンタの機能**を選択します。
5. **機能セット**メニューから、**セキュリティ印刷**を選択します。
6. **セキュリティ印刷**のチェックボックスを選択します。
7. 4桁のパスワードを設定します。上段から1桁目、2桁目、3桁目、4桁目をそれぞれ指定します。
8. **プリント**をクリックします。
9. 本製品の操作パネルで、左右にフリックするか、◀または▶を押して[セキュリティ印刷]を表示し、[セキュリティ印刷]を押します。
10. 上下にフリックするか、▲または▼を押してユーザー名を表示し、お使いのユーザー名を押します。
画面には、この名前に対する安全なジョブが一覧表示されます。
11. 上下にフリックするか、▲または▼を押して印刷ジョブを表示し、印刷したい印刷ジョブを押します。
12. 4桁のパスワードを入力し、[OK]を押します。
13. 枚数を入力します。
14. [スタート]を押します。
データが印刷されます。

セキュリティデータは印刷後、本製品のメモリーから削除されます。

✓ 関連情報

- [パソコンから印刷する\(Mac\)](#)


ペーパーフィーダーユニットを設定する (Mac)

1. アップルメニューの**システム環境設定**からお使いのプリンターに移動して、**オプションとサプライ**を選択します。
2. ハードウェアオプションの一覧に移動して、設置済みのオプションを追加します。
3. 変更を適用します。


✓ 関連情報

- [パソコンから印刷する\(Mac\)](#)
-

印刷ジョブをキャンセルする

1.  を押します。



複数の印刷ジョブをキャンセルするには、 を約 4 秒間押します。





関連情報

- [印刷](#)

テスト印刷

印刷品質に問題がある場合は、以下の指示に従ってテスト印刷を行います。

1.  [メニュー] > [全てのメニュー] > [プリンター] > [プリンター オプション] > [テストプリント] > [はい] を押します。
2.  を押します。



関連情報

- [印刷](#)

■ スキャン

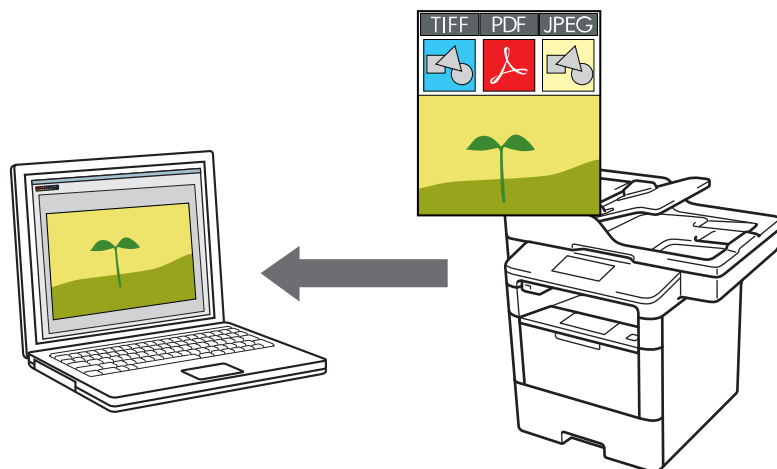
- 本製品のスキャンボタンを使用してスキャンする
- お使いのパソコンからスキャンする (Windows®)
- お使いのパソコンからスキャンする (Mac)
- ウェブブラウザを使用してスキャン設定を行う

本製品のスキャンボタンを使用してスキャンする






- 写真やグラフィックをスキャンする
- スキャンしたデータを PDF ファイルとしてパソコンに保存する
- スキャンしたデータを USB フラッシュドライブに保存する
- 編集可能テキストファイルとしてスキャンする（OCR）
- スキャン to E メール添付
- スキャンしたデータを E メールサーバーに送信する
- スキャンしたデータを FTP サーバーに保存する
- スキャン to SSH FTP（SFTP）
- スキャンしたデータをネットワーク上のサーバーに保存する(Windows®)
- スキャン to SharePoint®
- Web サービスを使ってスキャンする（Windows® 7、Windows® 8.1 および Windows®10）
- ControlCenter4 からスキャンボタン設定を変更する（Windows®）
- 署名入り PDF の証明書を設定する
- お使いのパソコンからスキャンを無効にする

写真やグラフィックをスキャンする

スキャンした写真やグラフィックを、お使いのパソコンに直接送信します。



本製品のスキャンボタンを使って、スキャン設定を一時的に変更することができます。変更を保持する場合は、本製品の ControlCenter ソフトウェアを使用します。

1. 原稿をセットします。
 2.  [スキャン] を押します。
 3. 左または右にフリックして、 [イメージ] を表示します。
 4.  [イメージ] を押します。
アイコンが画面の中央に移動し、青色でハイライト表示されます。
 5.  [イメージ] を押します。
 6. 本製品がネットワークを介して接続されている場合、上または下にフリックするか、▲または▼を押してデータ送信先のパソコンを表示し、パソコン名を押します。
-
-  パソコンの PIN 入力を要求するメッセージが画面に表示されたら、4桁の PIN を入力して、[OK] を押します。
-
7. [スタート] を押します。
本製品がスキャン動作を開始します。本製品の原稿台ガラスに原稿を置いた場合は、画面の指示に従ってスキャン操作を終了します。

✓ 関連情報

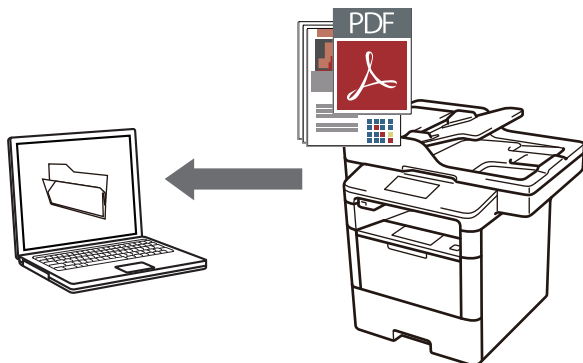
- [本製品のスキャンボタンを使用してスキャンする](#)

関連トピック：





- [ControlCenter4 からスキャンボタン設定を変更する \(Windows®\)](#)


スキャンしたデータを PDF ファイルとしてパソコンに保存する

原稿をスキャンし、お使いのパソコン上に PDF ファイルとして保存します。



本製品のスキャンボタンを使って、スキャン設定を一時的に変更することができます。変更を保持する場合は、本製品の ControlCenter ソフトウェアを使用します。

1. 原稿をセットします。
2.  [スキャン] を押します。
3. 左または右にフリックして、 [ファイル] を表示します。
4.  [ファイル] を押します。
アイコンが画面の中央に移動し、青色でハイライト表示されます。
5.  [ファイル] を押します。
6. 本製品がネットワークを介して接続されている場合、上または下にフリックするか、▲または▼を押してデータ送信先のパソコンを表示し、パソコン名を押します。

 パソコンの PIN 入力を要求するメッセージが画面に表示されたら、4 桁の PIN を入力して、[OK] を押します。

7. [スタート] を押します。
本製品がスキャン動作を開始します。本製品の原稿台ガラスに原稿を置いた場合は、画面の指示に従ってスキャン操作を終了します。

✓ 関連情報

- [本製品のスキャンボタンを使用してスキャンする](#)

関連トピック：

- [ControlCenter4 からスキャンボタン設定を変更する \(Windows®\)](#)

スキャンしたデータを USB フラッシュドライブに保存する

原稿をスキャンしたデータを USB フラッシュドライブに直接保存します。

1. 原稿をセットします。
2. USB フラッシュドライブを本製品に差し込みます。
画面の表示が自動的に変わります。
3. [スキャン to USB] を押します。
4. [スタート] を押します。

本製品がスキャン動作を開始します。本製品の原稿台ガラスに原稿を置いた場合は、画面の指示に従ってスキャン操作を終了します。

重要

データを読み込み中は、画面にメッセージが表示されます。データの読み込み中は、電源コードを抜いたり、USB フラッシュドライブを取り外さないでください。データが失われたり、USB フラッシュドライブが損傷する恐れがあります。

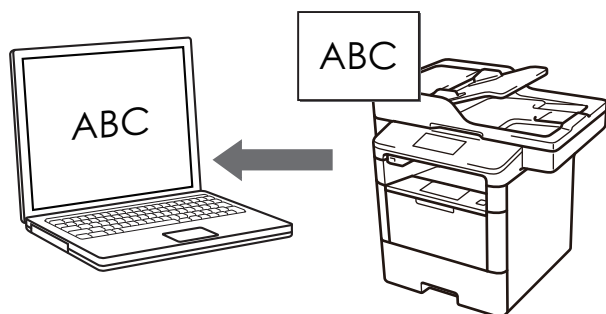


関連情報





- 本製品のスキャンボタンを使用してスキャンする


編集可能テキストファイルとしてスキャンする (OCR)

本製品は、OCR（光学式文字認識）の技術を使って、スキャンした原稿の文字をテキストに変換することができます。テキスト編集アプリケーションを使ってこのテキストを編集できます。



- この機能を使うには、OCR に対応したアプリケーションがコンピューターにインストールされている必要があります。
- 本製品のスキャンボタンを使って、スキャン設定を一時的に変更することができます。スキャン設定の変更を保持するためには、本製品付属のアプリケーションソフト ControlCenter を使用します。

1. 原稿をセットします。
2.  [スキャン] を押します。
3. 左または右にフリックして、 [OCR] を表示します。
4.  [OCR] を押します。
アイコンが画面の中央に移動し、青色でハイライト表示されます。
5.  [OCR] を押します。
6. 本製品がネットワークを介して接続されている場合、上または下にフリックするか、▲ または ▼ を押してデータ送信先のパソコンを表示し、パソコン名を押します。

 パソコンの PIN 入力を要求するメッセージが画面に表示されたら、4 桁の PIN を入力して、[OK] を押します。

7. [スタート] を押します。
本製品がスキャン動作を開始します。本製品の原稿台ガラスに原稿を置いた場合は、画面の指示に従ってスキャン操作を終了します。

✓ 関連情報

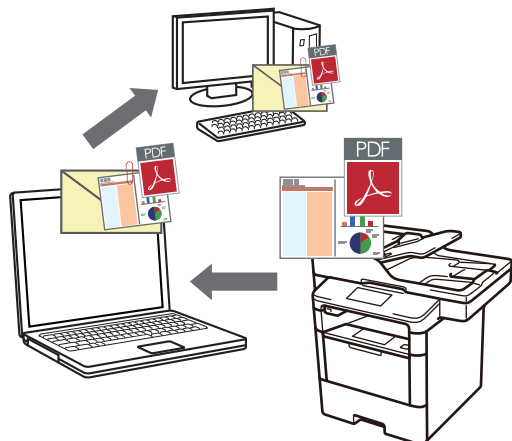
- [本製品のスキャンボタンを使用してスキャンする](#)

関連トピック：

- [ControlCenter4 からスキャンボタン設定を変更する \(Windows®\)](#)

スキャン to E メール添付





パソコンのEメールソフトを起動し、スキャンしたデータを添付ファイルとして送信します。



- 本製品のスキャンボタンを使って、スキャン設定を一時的に変更することができます。変更を保持する場合は、本製品の ControlCenter ソフトウェアを使用します。
- スキャン to E メール添付機能は、Web メールサービスには対応していません。スキャン to イメージまたはスキャン to ファイル機能を使って、原稿や写真をスキャンして、パソコンに保存してください。保存したデータファイルを Web メールに添付してください。



パソコンの初期設定で起動するように指定されている E メールソフトにスキャンデータを送信します。

1. 原稿をセットします。
2.  [スキャン] を押します。
3. 左または右にフリックして、 [E メール添付] を表示します。
4.  [E メール添付] を押します。
アイコンが画面の中央に移動し、青色でハイライト表示されます。
5.  [E メール添付] を押します。
6. 本製品がネットワークを介して接続されている場合、上または下にフリックするか、▲または▼を押してデータ送信先のパソコンを表示し、パソコン名を押します。



パソコンの PIN 入力を要求するメッセージが画面に表示されたら、4 桁の PIN を入力して、[OK] を押します。

7. [スタート] を押します。
本製品がスキャン動作を開始します。本製品の原稿台ガラスに原稿を置いた場合は、画面の指示に従ってスキャン操作を終了します。



関連情報

- [本製品のスキャンボタンを使用してスキャンする](#)





関連トピック：

- [ControlCenter4 からスキャンボタン設定を変更する \(Windows®\)](#)

スキャンしたデータを E メールサーバーに送信する

パソコンを使用せずに E-mail 受信者へ届けるため、本製品からお使いの E-mail サーバーにスキャンしたデータを直接送信します。

- スキャンしたデータを E-mail サーバーに送信するには、お使いのネットワークおよびメールサーバーと通信するように本製品を設定する必要があります。これらの設定は、本製品の操作パネル、ウェブブラウザ、またはリモートセットアップから行うことができます。

- 原稿をセットします。
-  [スキャン] を押します。
- 左または右にフリックして、 [E メール送信] を表示します。
-  [E メール送信] を押します。
アイコンが画面の中央に移動し、青色でハイライト表示されます。
-  [E メール送信] を押します。
- 以下のいずれかを行って、宛先 E-mail アドレスを入力します。
 - E-mail アドレスを手動で入力するには、[手動入力] を押して、画面に表示されるキーボードを使用して入力します。入力後、[OK] を押します。
 - E メールアドレスが本製品のアドレス帳に保存されている場合は、[電話帳] を押して、該当のアドレスを選択します。
[OK] を押します。
- E-mail アドレスを確認し、[次へ] を押します。
- [スタート] を押します。
本製品がスキャン動作を開始します。本製品の原稿台ガラスに原稿を置いた場合は、画面の指示に従ってスキャン操作を終了します。

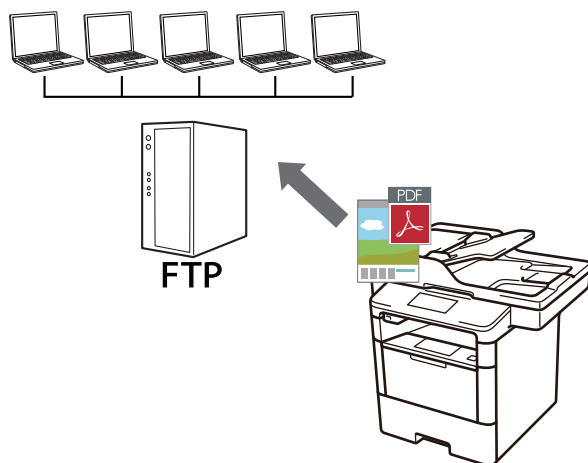
✓ 関連情報

- [本製品のスキャンボタンを使用してスキャンする](#)

▲ホーム > スキャン > 本製品のスキャンボタンを使用してスキャンする > スキャンしたデータを FTP サーバーに保存する

スキャンしたデータを FTP サーバーに保存する

スキャンしたデータを共有する必要がある場合、原稿をスキャンして FTP サーバーに直接送ることができます。プロファイルを設定して、任意のスキャン to FTP の送信先を保存することもできます。




- スキャン to FTP プロファイルを設定する
- スキャンしたデータを FTP サーバーに送信する

▲ホーム > スキャン > 本製品のスキャンボタンを使用してスキャンする > スキャンしたデータを FTP サーバーに保存する > スキャン to FTP プロファイルを設定する

スキャン to FTP プロファイルを設定する

スキャン to FTP プロファイルを設定し、スキャンしたデータを指定の FTP サーバーに直接送ることができます。

Windows®の場合は Microsoft® Internet Explorer® 11/Microsoft Edge™を、Mac の場合は Safari 10/11 を推奨します。どのウェブブラウザの場合も、JavaScript および Cookie を有効にして使用してください。指定以外のウェブブラウザを使用する場合は、HTTP 1.0 および HTTP 1.1 に対応していることを確認してください。

1. ウェブブラウザを起動します。
ブラウザのアドレス欄に「http://製品の IP アドレス」を入力します（「製品の IP アドレス」の部分には本製品の IP アドレスまたはプリントサーバー名を入力します）。例：http://192.168.1.2
パスワード設定をしている場合は、そのパスワードを入力し、を押します。初期パスワードは、initpass です。
2. **スキャン**タブをクリックします。
3. 左側にあるナビゲーションバーの**スキャン to FTP/SFTP/ネットワークファイル/SharePoint**メニューをクリックします。
4. **FTP**を選択して、**OK**をクリックします。

スキャン to FTP/SFTP/ネットワークファイル/SharePoint

プロファイル 1	<input checked="" type="radio"/> FTP <input type="radio"/> SFTP <input type="radio"/> ネットワーク <input type="radio"/> SharePoint
プロファイル 2	<input checked="" type="radio"/> FTP <input type="radio"/> SFTP <input type="radio"/> ネットワーク <input type="radio"/> SharePoint
プロファイル 3	<input checked="" type="radio"/> FTP <input type="radio"/> SFTP <input type="radio"/> ネットワーク <input type="radio"/> SharePoint
プロファイル 4	<input checked="" type="radio"/> FTP <input type="radio"/> SFTP <input type="radio"/> ネットワーク <input type="radio"/> SharePoint
プロファイル 5	<input checked="" type="radio"/> FTP <input type="radio"/> SFTP <input type="radio"/> ネットワーク <input type="radio"/> SharePoint
プロファイル 6	<input checked="" type="radio"/> FTP <input type="radio"/> SFTP <input type="radio"/> ネットワーク <input type="radio"/> SharePoint
プロファイル 7	<input checked="" type="radio"/> FTP <input type="radio"/> SFTP <input type="radio"/> ネットワーク <input type="radio"/> SharePoint
プロファイル 8	<input checked="" type="radio"/> FTP <input type="radio"/> SFTP <input type="radio"/> ネットワーク <input type="radio"/> SharePoint
プロファイル 9	<input checked="" type="radio"/> FTP <input type="radio"/> SFTP <input type="radio"/> ネットワーク <input type="radio"/> SharePoint
プロファイル 10	<input checked="" type="radio"/> FTP <input type="radio"/> SFTP <input type="radio"/> ネットワーク <input type="radio"/> SharePoint
プロファイル 11	<input checked="" type="radio"/> FTP <input type="radio"/> SFTP <input type="radio"/> ネットワーク <input type="radio"/> SharePoint
プロファイル 12	<input checked="" type="radio"/> FTP <input type="radio"/> SFTP <input type="radio"/> ネットワーク <input type="radio"/> SharePoint
プロファイル 13	<input checked="" type="radio"/> FTP <input type="radio"/> SFTP <input type="radio"/> ネットワーク <input type="radio"/> SharePoint
プロファイル 14	<input checked="" type="radio"/> FTP <input type="radio"/> SFTP <input type="radio"/> ネットワーク <input type="radio"/> SharePoint
プロファイル 15	<input checked="" type="radio"/> FTP <input type="radio"/> SFTP <input type="radio"/> ネットワーク <input type="radio"/> SharePoint
プロファイル 16	<input checked="" type="radio"/> FTP <input type="radio"/> SFTP <input type="radio"/> ネットワーク <input type="radio"/> SharePoint
プロファイル 17	<input checked="" type="radio"/> FTP <input type="radio"/> SFTP <input type="radio"/> ネットワーク <input type="radio"/> SharePoint
プロファイル 18	<input checked="" type="radio"/> FTP <input type="radio"/> SFTP <input type="radio"/> ネットワーク <input type="radio"/> SharePoint
プロファイル 19	<input checked="" type="radio"/> FTP <input type="radio"/> SFTP <input type="radio"/> ネットワーク <input type="radio"/> SharePoint
プロファイル 20	<input checked="" type="radio"/> FTP <input type="radio"/> SFTP <input type="radio"/> ネットワーク <input type="radio"/> SharePoint
プロファイル 21	<input checked="" type="radio"/> FTP <input type="radio"/> SFTP <input type="radio"/> ネットワーク <input type="radio"/> SharePoint
プロファイル 22	<input checked="" type="radio"/> FTP <input type="radio"/> SFTP <input type="radio"/> ネットワーク <input type="radio"/> SharePoint
プロファイル 23	<input checked="" type="radio"/> FTP <input type="radio"/> SFTP <input type="radio"/> ネットワーク <input type="radio"/> SharePoint
プロファイル 24	<input checked="" type="radio"/> FTP <input type="radio"/> SFTP <input type="radio"/> ネットワーク <input type="radio"/> SharePoint
プロファイル 25	<input checked="" type="radio"/> FTP <input type="radio"/> SFTP <input type="radio"/> ネットワーク <input type="radio"/> SharePoint

5. 左側にあるナビゲーションバーの **FTP/SFTP/ネットワークファイル/SharePoint スキャン** プロファイルメニューをクリックします。
6. 設定または変更したいプロファイルを選択します。
7. **プロファイル名** 欄に、該当サーバープロファイル名を入力します（15 文字以下の英数字）。本製品の画面上に入力した名称が表示されます。
8. **サーバー アドレス** 欄に、サーバーのドメイン名（例：ftp.example.com、64 文字以下）、または IP アドレス（例：192.23.56.189）を入力します。
9. **ユーザー名** 欄に、FTP サーバーへのデータの書き込みが許可されているユーザー名（32 文字以下）を入力します。
10. **ユーザー名** 欄で入力したユーザー名のパスワード（32 文字以下）を、**パスワード** に入力します。**パスワード 確認** 欄にパスワードを再入力します。
11. **転送先フォルダー** 欄に、スキャンデータの送信先である FTP サーバー上のフォルダーのパスを入力します。アドレスの最初にスラッシュを入力しないでください（例参照）。

12. **ファイル名**のドロップダウンリストをクリックして、あらかじめ指定された名称、または、ユーザー定義を選択します。ここで選択した名称が、スキャンしたデータのファイル名の先頭につき、「選択した名称+原稿台/ADFの6桁カウンター+拡張子」がファイル名となります。(例:「Estimate_098765.pdf」)
13. **画質**のドロップダウンリストをクリックして、画質を選択します。**本体で設定**を選択した場合、スキャンプロファイルを使用する度に、設定を選択するよう本製品の画面に表示されます。
14. **ファイル形式**のドロップダウンリストをクリックして、スキャンしたデータを保存するときのファイル形式を選択します。**本体で設定**を選択した場合、スキャンプロファイルを使用する度に、設定を選択するよう本製品の画面に表示されます。
15. **原稿サイズ**ドロップダウンリストをクリックして、リストから原稿サイズを選択します。スキャンする原稿のサイズが正しいかどうかを確認します。
16. **ファイルサイズ**のドロップダウンリストをクリックして、一覧からファイルサイズを選択します。
17. **地色除去**のドロップダウンリストをクリックして、一覧からレベルを選択します。原稿の背景にある地色を取り除き、スキャンしたデータをより見やすくすることができます。
18. FTP サーバーおよびファイアウォール設定に応じて、**パッシブモード**のオフ/オン設定を切り替えます。お買い上げ時の設定ではオンになっています。ほとんどの場合この設定を変更する必要はありません。
19. FTP サーバーへアクセスするための**ポート番号**を設定します。お買い上げ時の設定はポート 21 です。ほとんどの場合この設定を変更する必要はありません。
20. **OK** をクリックします。



?, /, \, ", :, <, >, |, *等の文字を使用すると、送信エラーが起こることがあります。






関連情報


- スキャンしたデータを FTP サーバーに保存する

スキャンしたデータを FTP サーバーに送信する

スキャンした情報を FTP サーバーへ保存して共有します。

1. 原稿をセットします。
2.  [スキャン] を押します。
3. 左または右にフリックして、 [(S) FTP サーバー] を表示します。
4.  [(S) FTP サーバー] を押します。

アイコンが画面の中央に移動し、青色でハイライト表示されます。

5.  [(S) FTP サーバー] を押します。
6. ウェブブラウザを使用してセットアップした、FTP および SFTP サーバーのプロファイルが一覧表示されます。上または下にフリックするか、▲または▼を押して、一覧表示された FTP サーバーのいずれかを表示した後、任意のプロファイルを押します。プロファイルが完全ではない場合（例えば、ログオンアカウント名およびパスワードが設定されていない、または品質やファイルの種類が指定されていない）、必要な情報の入力を求められます。
7. [スタート] を押します。

本製品がスキャン動作を開始します。本製品の原稿台ガラスに原稿を置いた場合は、画面の指示に従ってスキャン操作を終了します。

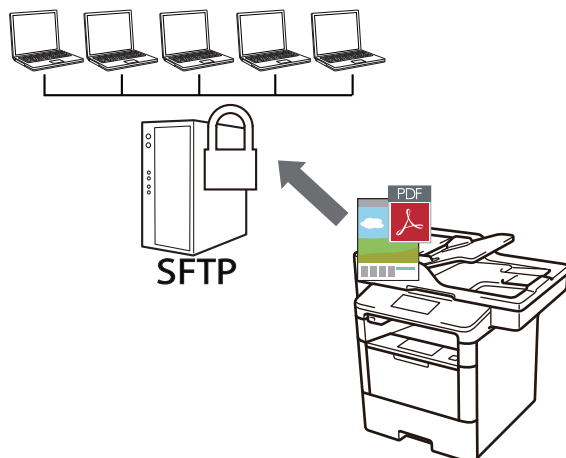


関連情報

- ・ [スキャンしたデータを FTP サーバーに保存する](#)

スキャン to SSH FTP (SFTP)

原稿をスキャンし、SFTP サーバーに直接送信します。SFTP サーバーは、FTP サーバーよりもセキュリティが強化されたサーバーです。さらに便利にするために、異なるプロファイルを設定して、任意のスキャン to SFTP の送信先を保存します。




- スキャン to SFTP プロファイルを設定する
- ウェブブラウザを使用してクライアント鍵のペアを作成する
- ウェブブラウザを使用してクライアント鍵ペアをエクスポートする
- ウェブブラウザを使用してサーバーの公開鍵をインポートする
- スキャンしたデータを SFTP サーバーにアップロードする

スキャン to SFTP プロファイルを設定する

スキャン to SFTP プロファイルを設定して、スキャンしたデータを SFTP の場所に直接アップロードします。

Windows®の場合は Microsoft® Internet Explorer® 11/Microsoft Edge™を、Mac の場合は Safari 10/11 を推奨します。どのウェブブラウザの場合も、JavaScript および Cookie を有効にして使用してください。指定以外のウェブブラウザを使用する場合は、HTTP 1.0 および HTTP 1.1 に対応していることを確認してください。

1. ウェブブラウザを起動します。
ブラウザのアドレス欄に「http://製品の IP アドレス」を入力します（「製品の IP アドレス」の部分には本製品の IP アドレスまたはプリントサーバー名を入力します）。例：http://192.168.1.2
パスワード設定をしている場合は、そのパスワードを入力し、を押します。初期パスワードは、initpass です。
2. **スキャン**タブをクリックします。
3. 左側にあるナビゲーションバーの**スキャン to FTP/SFTP/ネットワークファイル/SharePoint**メニューをクリックします。
4. **SFTP** を選択し、**OK** をクリックします。

スキャン to FTP/SFTP/ネットワークファイル/SharePoint

プロファイル 1	<input type="radio"/> FTP <input checked="" type="radio"/> SFTP <input type="radio"/> ネットワーク <input type="radio"/> SharePoint
プロファイル 2	<input type="radio"/> FTP <input checked="" type="radio"/> SFTP <input type="radio"/> ネットワーク <input type="radio"/> SharePoint
プロファイル 3	<input type="radio"/> FTP <input checked="" type="radio"/> SFTP <input type="radio"/> ネットワーク <input type="radio"/> SharePoint
プロファイル 4	<input type="radio"/> FTP <input checked="" type="radio"/> SFTP <input type="radio"/> ネットワーク <input type="radio"/> SharePoint
プロファイル 5	<input type="radio"/> FTP <input checked="" type="radio"/> SFTP <input type="radio"/> ネットワーク <input type="radio"/> SharePoint
プロファイル 6	<input type="radio"/> FTP <input checked="" type="radio"/> SFTP <input type="radio"/> ネットワーク <input type="radio"/> SharePoint
プロファイル 7	<input type="radio"/> FTP <input checked="" type="radio"/> SFTP <input type="radio"/> ネットワーク <input type="radio"/> SharePoint
プロファイル 8	<input type="radio"/> FTP <input checked="" type="radio"/> SFTP <input type="radio"/> ネットワーク <input type="radio"/> SharePoint
プロファイル 9	<input type="radio"/> FTP <input checked="" type="radio"/> SFTP <input type="radio"/> ネットワーク <input type="radio"/> SharePoint
プロファイル 10	<input type="radio"/> FTP <input checked="" type="radio"/> SFTP <input type="radio"/> ネットワーク <input type="radio"/> SharePoint
プロファイル 11	<input type="radio"/> FTP <input checked="" type="radio"/> SFTP <input type="radio"/> ネットワーク <input type="radio"/> SharePoint
プロファイル 12	<input type="radio"/> FTP <input checked="" type="radio"/> SFTP <input type="radio"/> ネットワーク <input type="radio"/> SharePoint
プロファイル 13	<input type="radio"/> FTP <input checked="" type="radio"/> SFTP <input type="radio"/> ネットワーク <input type="radio"/> SharePoint
プロファイル 14	<input type="radio"/> FTP <input checked="" type="radio"/> SFTP <input type="radio"/> ネットワーク <input type="radio"/> SharePoint
プロファイル 15	<input type="radio"/> FTP <input checked="" type="radio"/> SFTP <input type="radio"/> ネットワーク <input type="radio"/> SharePoint
プロファイル 16	<input type="radio"/> FTP <input checked="" type="radio"/> SFTP <input type="radio"/> ネットワーク <input type="radio"/> SharePoint
プロファイル 17	<input type="radio"/> FTP <input checked="" type="radio"/> SFTP <input type="radio"/> ネットワーク <input type="radio"/> SharePoint
プロファイル 18	<input type="radio"/> FTP <input checked="" type="radio"/> SFTP <input type="radio"/> ネットワーク <input type="radio"/> SharePoint
プロファイル 19	<input type="radio"/> FTP <input checked="" type="radio"/> SFTP <input type="radio"/> ネットワーク <input type="radio"/> SharePoint
プロファイル 20	<input type="radio"/> FTP <input checked="" type="radio"/> SFTP <input type="radio"/> ネットワーク <input type="radio"/> SharePoint
プロファイル 21	<input type="radio"/> FTP <input checked="" type="radio"/> SFTP <input type="radio"/> ネットワーク <input type="radio"/> SharePoint
プロファイル 22	<input type="radio"/> FTP <input checked="" type="radio"/> SFTP <input type="radio"/> ネットワーク <input type="radio"/> SharePoint
プロファイル 23	<input type="radio"/> FTP <input checked="" type="radio"/> SFTP <input type="radio"/> ネットワーク <input type="radio"/> SharePoint
プロファイル 24	<input type="radio"/> FTP <input checked="" type="radio"/> SFTP <input type="radio"/> ネットワーク <input type="radio"/> SharePoint
プロファイル 25	<input type="radio"/> FTP <input checked="" type="radio"/> SFTP <input type="radio"/> ネットワーク <input type="radio"/> SharePoint


5. 左側にあるナビゲーションバーの **FTP/SFTP/ネットワークファイル/SharePoint スキャン** プロファイルメニューをクリックします。
6. 設定または変更したいプロファイルを選択します。
7. **プロファイル名** 欄に、該当サーバープロファイル名を入力します（15 文字以下の英数字）。本製品の画面上に入力した名称が表示されます。
8. **サーバー アドレス** 欄に、ホストアドレス（sftp.example.com など、最大 64 文字）、または IP アドレス（192.23.56.189 など）を入力します。
9. **ユーザー名** 欄に、SFTP サーバーへの書き込み許可を持つユーザー名（最大 32 文字）を入力します。
10. **認証方法** 欄で、**パスワード** または **公開鍵** を選択します。
11. 次のいずれかを行ってください。

- ・ **パスワード**を選択した場合、**ユーザー名**欄に入力したユーザー名に対するパスワード（最大 32 文字）を入力します。**パスワード確認**欄にもう一度パスワードを入力します。
- ・ **公開鍵**を選択した場合、**クライアント鍵ペア**ドロップダウンリストから、認証の種類を選択します。

12. **サーバー公開鍵**ドロップダウンリストから認証の種類を選択します。

13. **転送先フォルダー**欄に、スキャンデータの送信先である SFTP サーバー上のフォルダーのパスを入力します。アドレスの最初にスラッシュを入力しないでください（例参照）。

転送先フォルダー

 /abc

14. **ファイル名**のドロップダウンリストをクリックして、あらかじめ指定された名称、または、ユーザー定義を選択します。ここで選択した名称が、スキャンしたデータのファイル名の先頭につき、「選択した名称 + 原稿台/ADF の 6 桁カウンター + 拡張子」がファイル名となります。（例：「Estimate_098765.pdf」）
15. **画質**のドロップダウンリストをクリックして、画質を選択します。**本体で設定**を選択した場合、スキャンプロファイルを使用する度に、設定を選択するよう本製品の画面に表示されます。
16. **ファイル形式**のドロップダウンリストをクリックして、スキャンしたデータを保存するときのファイル形式を選択します。**本体で設定**を選択した場合、スキャンプロファイルを使用する度に、設定を選択するよう本製品の画面に表示されます。
17. **原稿サイズ**ドロップダウンリストをクリックして、リストから原稿サイズを選択します。スキャンする原稿のサイズが正しいかどうかを確認します。
18. **ファイルサイズ**のドロップダウンリストをクリックして、一覧からファイルサイズを選択します。
19. **地色除去**のドロップダウンリストをクリックして、一覧からレベルを選択します。原稿の背景にある地色を取り除き、スキャンしたデータをより見やすくすることができます。
20. SFTP サーバーへアクセスする際に適用される**ポート番号**設定を変更することができます。お買い上げ時の設定はポート 22 です。ほとんどの場合この設定を変更する必要はありません。
21. **OK** をクリックします。



？、/、\、"、:、<、>、|、*等の文字を使用すると、送信エラーが起こることがあります。



関連情報

- ・ [スキャン to SSH FTP（SFTP）](#)

ウェブブラウザを使用してクライアント鍵のペアを作成する

1. ウェブブラウザを起動します。
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://KMNxxxxxxxxxxxx

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. 左側にあるナビゲーションバーの**クライアント鍵ペア**をクリックします。
7. **クライアント鍵ペアの作成**をクリックします。
8. **クライアント鍵ペア名**欄に、任意の名前を入力します（最大 20 文字）。
9. **公開鍵アルゴリズム**ドロップダウンリストをクリックして、対象のアルゴリズムを選択します。
10. **OK** をクリックします。

クライアント鍵のペアが作成され、本製品のメモリーに保存されます。クライアント鍵のペア名と公開鍵のアルゴリズムは、**クライアント鍵ペア一覧**に表示されます。



関連情報

- スキャン to SSH FTP (SFTP)

ウェブブラウザを使用してクライアント鍵ペアをエクスポートする

1. ウェブブラウザを起動します。
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://KMNxxxxxxxxxxxx

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. 左側にあるナビゲーションバーの**クライアント鍵ペア**をクリックします。
7. **クライアント鍵ペア一覧**に示される**公開鍵のエクスポート**をクリックします。
8. **OK** をクリックします。
9. ファイルの保存先を指定します。

クライアント鍵ペアがお使いのパソコンにエクスポートされます。



関連情報

- [スキャン to SSH FTP \(SFTP\)](#)

ウェブブラウザを使用してサーバーの公開鍵をインポートする

1. ウェブブラウザを起動します。
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://KMNxxxxxxxxxxxx

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. 左側にあるナビゲーションバーの**サーバー公開鍵**をクリックします。
7. **サーバー公開鍵のインポート**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. **OK** をクリックします。





サーバーの公開鍵が本製品にインポートされます。



関連情報

- [スキャン to SSH FTP \(SFTP\)](#)

スキャンしたデータを SFTP サーバーにアップロードする

1. 原稿をセットします。
2.  [スキャン] を押します。
3. 左または右にフリックして、 [(S)FTP サーバー] を表示します。
4.  [(S)FTP サーバー] を押します。
アイコンが画面の中央に移動し、青色でハイライト表示されます。
5.  [(S)FTP サーバー] を押します。
6. ウェブブラウザを使用してセットアップした、FTP および SFTP サーバーのプロファイルが一覧表示されます。上または下にフリックするか、▲または▼を押し、一覧表示された SFTP サーバープロファイルのいずれかを表示した後、任意のプロファイルを押します。プロファイルが完全ではない場合（例えば、ログオンアカウント名およびパスワードが設定されていない、または品質やファイルの種類が指定されていない）、必要な情報の入力を求められます。
7. [スタート] を押します。
本製品がスキャン動作を開始します。本製品の原稿台ガラスに原稿を置いた場合は、画面の指示に従ってスキャン操作を終了します。

✓ 関連情報

- [スキャン to SSH FTP \(SFTP\)](#)

■ ホーム > スキャン > 本製品のスキャンボタンを使用してスキャンする > スキャンしたデータをネットワーク上のサーバーに保存する(Windows®)

スキャンしたデータをネットワーク上のサーバーに保存する(Windows®)

スキャンしたデータを、ネットワーク上の CIFS サーバーに直接送ることができます。プロファイルを設定して、任意のスキャン to ネットワークの送信先を保存することもできます。

- スキャン to ネットワークプロファイルを設定する
- スキャンしたデータを CIFS サーバーに送信する

■ ホーム > スキャン > 本製品のスキャンボタンを使用してスキャンする > スキャンしたデータをネットワーク上のサーバーに保存する(Windows®) > スキャン to ネットワークプロファイルを設定する


スキャン to ネットワークプロファイルを設定する

スキャン to ネットワークのプロファイルを設定し、スキャンしたデータを指定の CIFS サーバーに直接送ることができます。

Windows®の場合は、Microsoft® Internet Explorer® 11/Microsoft Edge™のウェブブラウザのご使用を推奨します。いずれのウェブブラウザの場合も、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を使用する場合は、HTTP 1.0 および HTTP 1.1 に対応していることを確認してください。

1. ウェブブラウザを起動します。

ブラウザのアドレス欄に「http://製品の IP アドレス」を入力します（「製品の IP アドレス」の部分には本製品の IP アドレスまたはプリントサーバー名を入力します）。例：http://192.168.1.2

パスワード設定をしている場合は、そのパスワードを入力し、を押します。初期パスワードは、initpass です。

2. **スキャン**タブをクリックします。
3. 左側にあるナビゲーションバーの**スキャン to FTP/SFTP/ネットワークファイル/SharePoint**メニューをクリックします。
4. **ネットワーク**を選択し、**OK** をクリックします。

スキャン to FTP/SFTP/ネットワークファイル/SharePoint

プロファイル 1	<input type="radio"/> FTP <input type="radio"/> SFTP <input checked="" type="radio"/> ネットワーク <input type="radio"/> SharePoint
プロファイル 2	<input type="radio"/> FTP <input type="radio"/> SFTP <input checked="" type="radio"/> ネットワーク <input type="radio"/> SharePoint
プロファイル 3	<input type="radio"/> FTP <input type="radio"/> SFTP <input checked="" type="radio"/> ネットワーク <input type="radio"/> SharePoint
プロファイル 4	<input type="radio"/> FTP <input type="radio"/> SFTP <input checked="" type="radio"/> ネットワーク <input type="radio"/> SharePoint
プロファイル 5	<input type="radio"/> FTP <input type="radio"/> SFTP <input checked="" type="radio"/> ネットワーク <input type="radio"/> SharePoint
プロファイル 6	<input type="radio"/> FTP <input type="radio"/> SFTP <input checked="" type="radio"/> ネットワーク <input type="radio"/> SharePoint
プロファイル 7	<input type="radio"/> FTP <input type="radio"/> SFTP <input checked="" type="radio"/> ネットワーク <input type="radio"/> SharePoint
プロファイル 8	<input type="radio"/> FTP <input type="radio"/> SFTP <input checked="" type="radio"/> ネットワーク <input type="radio"/> SharePoint
プロファイル 9	<input type="radio"/> FTP <input type="radio"/> SFTP <input checked="" type="radio"/> ネットワーク <input type="radio"/> SharePoint
プロファイル 10	<input type="radio"/> FTP <input type="radio"/> SFTP <input checked="" type="radio"/> ネットワーク <input type="radio"/> SharePoint
プロファイル 11	<input type="radio"/> FTP <input type="radio"/> SFTP <input checked="" type="radio"/> ネットワーク <input type="radio"/> SharePoint
プロファイル 12	<input type="radio"/> FTP <input type="radio"/> SFTP <input checked="" type="radio"/> ネットワーク <input type="radio"/> SharePoint
プロファイル 13	<input type="radio"/> FTP <input type="radio"/> SFTP <input checked="" type="radio"/> ネットワーク <input type="radio"/> SharePoint
プロファイル 14	<input type="radio"/> FTP <input type="radio"/> SFTP <input checked="" type="radio"/> ネットワーク <input type="radio"/> SharePoint
プロファイル 15	<input type="radio"/> FTP <input type="radio"/> SFTP <input checked="" type="radio"/> ネットワーク <input type="radio"/> SharePoint
プロファイル 16	<input type="radio"/> FTP <input type="radio"/> SFTP <input checked="" type="radio"/> ネットワーク <input type="radio"/> SharePoint
プロファイル 17	<input type="radio"/> FTP <input type="radio"/> SFTP <input checked="" type="radio"/> ネットワーク <input type="radio"/> SharePoint
プロファイル 18	<input type="radio"/> FTP <input type="radio"/> SFTP <input checked="" type="radio"/> ネットワーク <input type="radio"/> SharePoint
プロファイル 19	<input type="radio"/> FTP <input type="radio"/> SFTP <input checked="" type="radio"/> ネットワーク <input type="radio"/> SharePoint
プロファイル 20	<input type="radio"/> FTP <input type="radio"/> SFTP <input checked="" type="radio"/> ネットワーク <input type="radio"/> SharePoint
プロファイル 21	<input type="radio"/> FTP <input type="radio"/> SFTP <input checked="" type="radio"/> ネットワーク <input type="radio"/> SharePoint
プロファイル 22	<input type="radio"/> FTP <input type="radio"/> SFTP <input checked="" type="radio"/> ネットワーク <input type="radio"/> SharePoint
プロファイル 23	<input type="radio"/> FTP <input type="radio"/> SFTP <input checked="" type="radio"/> ネットワーク <input type="radio"/> SharePoint
プロファイル 24	<input type="radio"/> FTP <input type="radio"/> SFTP <input checked="" type="radio"/> ネットワーク <input type="radio"/> SharePoint
プロファイル 25	<input type="radio"/> FTP <input type="radio"/> SFTP <input checked="" type="radio"/> ネットワーク <input type="radio"/> SharePoint

5. 左側にあるナビゲーションバーの **FTP/SFTP/ネットワークファイル/SharePoint スキャンプロファイル**メニューをクリックします。
6. 設定または変更したいプロファイルを選択します。
7. **プロファイル名**欄に、該当サーバープロファイル名を入力します（15 文字以下の英数字）。本製品の画面上に入力した名称が表示されます。
8. **ネットワークフォルダパス**欄に、スキャンデータの送信先である CIFS サーバー上のフォルダーのパスを入力します。
9. **ファイル名**のドロップダウンリストをクリックして、あらかじめ指定された名称、または、ユーザー定義を選択します。ここで選択した名称が、スキャンしたデータのファイル名の先頭につき、「選択した名称＋原稿台/ADF の 6 桁カウンター＋拡張子」がファイル名となります。（例：「Estimate_098765.pdf」）

10. **画質**のドロップダウンリストをクリックして、画質を選択します。**本体で設定**を選択した場合、スキャンプロファイルを使用する度に、設定を選択するよう本製品の画面に表示されます。
11. **ファイル形式**のドロップダウンリストをクリックして、スキャンしたデータを保存するときのファイル形式を選択します。**本体で設定**を選択した場合、スキャンプロファイルを使用する度に、設定を選択するよう本製品の画面に表示されます。
12. **原稿サイズ**ドロップダウンリストをクリックして、リストから原稿サイズを選択します。スキャンする原稿のサイズが正しいかどうかを確認します。
13. **ファイルサイズ**のドロップダウンリストをクリックして、一覧からファイルサイズを選択します。
14. **地色除去**のドロップダウンリストをクリックして、一覧からレベルを選択します。原稿の背景にある地色を取り除き、スキャンしたデータをより見やすくすることができます。
15. このプロファイルを PIN で保護するには、**接続時にパスワード認証を行う**欄で、**オン**を選びます。
16. **接続時にパスワード認証を行う**欄で**オン**を選択した場合、**接続パスワード**欄に 4 桁の PIN を入力します。
17. 認証方式を設定するには、**認証方法**から**自動**、**Kerberos**、または **NTLMv2** を選択します。
18. **ネットワークフォルダパス**欄で指定したフォルダーへの書き込み許可を持つユーザー名（最大 96 文字）を、**ユーザー名**欄に入力します。ユーザー名がドメインの一部である場合、以下のいずれかの形式でユーザー名を入力します。
user@domain
ドメイン名\ユーザー名
19. **ユーザー名**欄で入力したユーザー名のパスワード（32 文字以下）を、**パスワード**に入力します。**パスワード確認**欄にパスワードを再入力します。
20. Kerberos サーバーアドレスを手動で設定するには、**Kerberos サーバーアドレス**欄に、Kerberos サーバーアドレスを入力します（最大 64 文字。例：kerberos.example.com）。
21. **OK** をクリックします。



?、/、\、"、:、<、>、|、*等の文字を使用すると、送信エラーが起こることがあります。

22. すべての認証方法に対して、SNTP プロトコル(ネットワークタイムサーバー)を設定するか、操作パネルで日時とタイムゾーンを正確に設定する必要があります。時間は、Kerberos サーバーおよび CIFS サーバーで使われる時間と一致させる必要があります。



関連情報

- スキャンしたデータをネットワーク上のサーバーに保存する(Windows®)
- ウェブブラウザーを使用して日時を設定する

■ ホーム > スキャン > 本製品のスキャンボタンを使用してスキャンする > スキャンしたデータをネットワーク上のサーバーに保存する(Windows®) > スキャン to ネットワークプロファイルを設定する > ウェブブラウザを使用して日時を設定する


ウェブブラウザを使用して日時を設定する

日時およびタイムゾーンの設定値をウェブブラウザまたは操作パネルを使用して正しく設定し、認証を行うサーバーが使用する時間が本製品の時間と必ず一致するようにします。

ウェブブラウザによる設定画面が開いている場合は、手順 1 を行いません。

1. ウェブブラウザを起動します。

ブラウザのアドレス欄に「http://製品の IP アドレス」を入力します（「製品の IP アドレス」の部分には本製品の IP アドレスまたはプリントサーバー名を入力します）。例：http://192.168.1.2

パスワード設定をしている場合は、そのパスワードを入力し、を押します。初期パスワードは、initpass です。

2. 管理者設定タブをクリックします。
3. 左側にあるナビゲーションバーの時計設定メニューをクリックします。

時計設定

日付

2016 / 01 / 01

時間

03 : 37 24時間制

タイムゾーン

UTC+09:00 ▼

☐ SNTPサーバーと同期する

本機能を使用するためには
SNTPサーバーの設定が必要です。

[SNTP>>](#)

キャンセル





OK

4. 日付欄に日付を入力します。
5. 時計表示欄から時間の種類を選択します（一部の国でのみ利用可能）。
6. 時間欄に時間を入力します。
7. タイムゾンドロップダウンリストから、現在の地域と UTC との時差を選択します。例えば、米国およびカナダの東部時間のタイムゾーンは、UTC-05:00 となります。
8. サマータイム欄でオンをクリックして、サマータイムに合わせて自動的に時間が変更されるように本製品を設定します。この設定により、春には 1 時間早め、秋には 1 時間遅らせるよう、自動的にリセットされます（一部の国でのみ利用可能）。
9. OK をクリックします。

✓ 関連情報

- ・ スキャン to ネットワークプロファイルを設定する

スキャンしたデータを CIFS サーバーに送信する

1. 原稿をセットします。
2.  [スキャン] を押します。
3. 左または右にフリックして、 [ネットワーク] を表示します。
4.  [ネットワーク] を押します。
アイコンが画面の中央に移動し、青色でハイライト表示されます。
5.  [ネットワーク] を押します。
6. 上または下にフリックするか、▲または▼を押し、一覧表示されたネットワークサーバープロファイルのいずれかを表示した後、任意のプロファイルを押します。プロファイルが完全ではない場合（例えば、ログオンアカウント名およびパスワードが設定されていない、または品質やファイルの種類が指定されていない）、必要な情報の入力を求められます。
7. [スタート] を押します。
本製品がスキャン動作を開始します。本製品の原稿台ガラスに原稿を置いた場合は、画面の指示に従ってスキャン操作を終了します。



関連情報

- ・ スキャンしたデータをネットワーク上のサーバーに保存する(Windows®)

スキャン to SharePoint®


スキャンした情報を共有する必要がある場合、原稿をスキャンして、SharePoint®サーバーに直接送信します。さらに便利な使用方法として、異なるプロファイルを設定して、任意のスキャン to SharePoint®の送信先を保存します。

- スキャン to SharePoint®プロファイルを設定する
- スキャンしたデータを SharePoint®サーバーにアップロードする

スキャン to SharePoint®プロファイルを設定する

スキャン to SharePoint®プロファイルを設定して、スキャンしたデータを SharePoint®の場所に直接アップロードします。

Windows®の場合は Microsoft® Internet Explorer® 11/Microsoft Edge™を、Mac の場合は Safari 10/11 を推奨します。どのウェブブラウザの場合も、JavaScript および Cookie を有効にして使用してください。指定以外のウェブブラウザを使用する場合は、HTTP 1.0 および HTTP 1.1 に対応していることを確認してください。

1. ウェブブラウザを起動します。
ブラウザのアドレス欄に「http://製品の IP アドレス」を入力します（「製品の IP アドレス」の部分には本製品の IP アドレスまたはプリントサーバー名を入力します）。例：http://192.168.1.2
パスワード設定をしている場合は、そのパスワードを入力し、を押します。初期パスワードは、initpass です。
2. **スキャン**タブをクリックします。
3. 左側にあるナビゲーションバーの**スキャン to FTP/SFTP/ネットワークファイル/SharePoint**メニューをクリックします。
4. **SharePoint** を選択し、**OK** をクリックします。

スキャン to FTP/SFTP/ネットワークファイル/SharePoint

プロファイル 1	<input type="radio"/> FTP <input type="radio"/> SFTP <input type="radio"/> ネットワーク <input checked="" type="radio"/> SharePoint
プロファイル 2	<input type="radio"/> FTP <input type="radio"/> SFTP <input type="radio"/> ネットワーク <input checked="" type="radio"/> SharePoint
プロファイル 3	<input type="radio"/> FTP <input type="radio"/> SFTP <input type="radio"/> ネットワーク <input checked="" type="radio"/> SharePoint
プロファイル 4	<input type="radio"/> FTP <input type="radio"/> SFTP <input type="radio"/> ネットワーク <input checked="" type="radio"/> SharePoint
プロファイル 5	<input type="radio"/> FTP <input type="radio"/> SFTP <input type="radio"/> ネットワーク <input checked="" type="radio"/> SharePoint
プロファイル 6	<input type="radio"/> FTP <input type="radio"/> SFTP <input type="radio"/> ネットワーク <input checked="" type="radio"/> SharePoint
プロファイル 7	<input type="radio"/> FTP <input type="radio"/> SFTP <input type="radio"/> ネットワーク <input checked="" type="radio"/> SharePoint
プロファイル 8	<input type="radio"/> FTP <input type="radio"/> SFTP <input type="radio"/> ネットワーク <input checked="" type="radio"/> SharePoint
プロファイル 9	<input type="radio"/> FTP <input type="radio"/> SFTP <input type="radio"/> ネットワーク <input checked="" type="radio"/> SharePoint
プロファイル 10	<input type="radio"/> FTP <input type="radio"/> SFTP <input type="radio"/> ネットワーク <input checked="" type="radio"/> SharePoint
プロファイル 11	<input type="radio"/> FTP <input type="radio"/> SFTP <input type="radio"/> ネットワーク <input checked="" type="radio"/> SharePoint
プロファイル 12	<input type="radio"/> FTP <input type="radio"/> SFTP <input type="radio"/> ネットワーク <input checked="" type="radio"/> SharePoint
プロファイル 13	<input type="radio"/> FTP <input type="radio"/> SFTP <input type="radio"/> ネットワーク <input checked="" type="radio"/> SharePoint
プロファイル 14	<input type="radio"/> FTP <input type="radio"/> SFTP <input type="radio"/> ネットワーク <input checked="" type="radio"/> SharePoint
プロファイル 15	<input type="radio"/> FTP <input type="radio"/> SFTP <input type="radio"/> ネットワーク <input checked="" type="radio"/> SharePoint
プロファイル 16	<input type="radio"/> FTP <input type="radio"/> SFTP <input type="radio"/> ネットワーク <input checked="" type="radio"/> SharePoint
プロファイル 17	<input type="radio"/> FTP <input type="radio"/> SFTP <input type="radio"/> ネットワーク <input checked="" type="radio"/> SharePoint
プロファイル 18	<input type="radio"/> FTP <input type="radio"/> SFTP <input type="radio"/> ネットワーク <input checked="" type="radio"/> SharePoint
プロファイル 19	<input type="radio"/> FTP <input type="radio"/> SFTP <input type="radio"/> ネットワーク <input checked="" type="radio"/> SharePoint
プロファイル 20	<input type="radio"/> FTP <input type="radio"/> SFTP <input type="radio"/> ネットワーク <input checked="" type="radio"/> SharePoint
プロファイル 21	<input type="radio"/> FTP <input type="radio"/> SFTP <input type="radio"/> ネットワーク <input checked="" type="radio"/> SharePoint
プロファイル 22	<input type="radio"/> FTP <input type="radio"/> SFTP <input type="radio"/> ネットワーク <input checked="" type="radio"/> SharePoint
プロファイル 23	<input type="radio"/> FTP <input type="radio"/> SFTP <input type="radio"/> ネットワーク <input checked="" type="radio"/> SharePoint
プロファイル 24	<input type="radio"/> FTP <input type="radio"/> SFTP <input type="radio"/> ネットワーク <input checked="" type="radio"/> SharePoint
プロファイル 25	<input type="radio"/> FTP <input type="radio"/> SFTP <input type="radio"/> ネットワーク <input checked="" type="radio"/> SharePoint

キャンセル OK

5. 左側にあるナビゲーションバーの **FTP/SFTP/ネットワークファイル/SharePoint スキャンプロファイル**メニューをクリックします。
6. 設定または変更したいプロファイルを選択します。
7. **プロファイル名**欄に、該当サーバープロファイル名を入力します（15 文字以下の英数字）。本製品の画面上に入力した名称が表示されます。
8. **SharePoint サイトのアドレス**欄に、ブラウザのアドレスバーに表示されたフルパスのアドレス（例：http://SharePointSiteAddress/Shared%20Documents/Forms/AllItems.aspx）、または IP アドレス（例：http://192.168.0.1/Shared%20Documents/Forms/AllItems.aspx）をコピーアンドペーストします。
9. **ファイル名**のドロップダウンリストをクリックして、あらかじめ指定された名称、または、ユーザー定義を選択します。ここで選択した名称が、スキャンしたデータのファイル名の先頭につき、「選択した名称+原稿台/ADF の 6 桁カウンター+拡張子」がファイル名となります。（例：「Estimate_098765.pdf」）

10. **画質**のドロップダウンリストをクリックして、画質を選択します。**本体で設定**を選択した場合、スキャンプロファイルを使用する度に、設定を選択するよう本製品の画面に表示されます。
11. **ファイル形式**のドロップダウンリストをクリックして、スキャンしたデータを保存するときのファイル形式を選択します。**本体で設定**を選択した場合、スキャンプロファイルを使用する度に、設定を選択するよう本製品の画面に表示されます。
12. **原稿サイズ**ドロップダウンリストをクリックして、リストから原稿サイズを選択します。スキャンする原稿のサイズが正しいかどうかを確認します。
13. **ファイルサイズ**のドロップダウンリストをクリックして、一覧からファイルサイズを選択します。
14. **地色除去**のドロップダウンリストをクリックして、一覧からレベルを選択します。原稿の背景にある地色を取り除き、スキャンしたデータをより見やすくすることができます。
15. このプロファイルを PIN で保護するには、**接続時にパスワード認証を行う**欄で**オン**を選択します。
16. **接続時にパスワード認証を行う**欄で**オン**を選択した場合、**接続パスワード**欄に 4 桁の PIN を入力します。
17. 認証方式を設定するには、**認証方法**メニューから**自動**、**NTLMv2**、**Kerberos**、または**基本**を選択します。**自動**を選択した場合、認証方式は自動的に設定されます。
18. **SharePoint サイトのアドレス**欄で指定したフォルダーへの書き込み許可を持つユーザー名（最大 96 文字）を、**ユーザー名**欄に入力します。ユーザー名がドメインの一部である場合、以下のいずれかの形式でユーザー名を入力します。
user@domain
ドメイン名\ユーザー名
19. **ユーザー名**欄で入力したユーザー名のパスワード（32 文字以下）を、**パスワード**に入力します。**パスワード確認**欄にパスワードを再入力します。
20. Kerberos サーバーアドレスを手動で設定するには、**Kerberos サーバーアドレス**欄に Kerberos サーバーアドレスを入力します（例：kerberos.example.com、最大 64 文字）。
21. **OK** をクリックします。







?、/、\、"、:、<、>、|、*等の文字を使用すると、送信エラーが起こることがあります。



関連情報

- [スキャン to SharePoint®](#)

スキャンしたデータを SharePoint®サーバーにアップロードする

1. 原稿をセットします。
2.  [スキャン] を押します。
3. 左または右にフリックして、 [SharePoint] を表示します。
4.  [SharePoint] を押します。
アイコンが画面の中央に移動し、青色でハイライト表示されます。
5.  [SharePoint] を押します。
6. ウェブブラウザを使用してセットアップした、SharePoint®サーバーのプロファイルが一覧表示されます。
上または下にフリックするか、▲または▼を押し、一覧表示された SharePoint®サーバープロファイルのいずれかを表示した後、任意のプロファイルを押します。プロファイルが完全ではない場合（例えば、ログオンアカウント名およびパスワードが設定されていない、または品質やファイルの種類が指定されていない）、必要な情報の入力を求められます。
7. [スタート] を押します。
本製品がスキャン動作を開始します。本製品の原稿台ガラスに原稿を置いた場合は、画面の指示に従ってスキャン操作を終了します。



関連情報

- [スキャン to SharePoint®](#)

■ ホーム > スキャン > 本製品のスキャンボタンを使用してスキャンする > Web サービスを使ってスキャンする (Windows® 7、Windows® 8.1 および Windows®10)

Web サービスを使ってスキャンする (Windows® 7、Windows® 8.1 および Windows®10)

Windows® 7、Windows® 8.1、または Windows®10 をお使いの場合は、Web サービス機能を使用してスキャンすることができます。Web サービスでドライバーをインストールする必要があります。

- Web サービスを使用してスキャン用ドライバーをインストールする (Windows® 7、Windows® 8.1 および Windows® 10)
- 本製品から Web サービスを使ってスキャンする (Windows® 7、Windows® 8.1 および Windows® 10)
- Web サービスのスキャンプロファイルを編集する

■ ホーム > スキャン > 本製品のスキャンボタンを使用してスキャンする > Web サービスを使ってスキャンする (Windows® 7、Windows® 8.1 および Windows® 10) > Web サービスを使用してスキャン用ドライバーをインストールする (Windows® 7、Windows® 8.1 および Windows® 10)


Web サービスを使用してスキャン用ドライバーをインストールする (Windows® 7、Windows® 8.1 および Windows® 10)

Web サービスを使用してネットワーク上のプリンターを監視します。

- 本製品にドライバーとソフトウェアがインストールされている必要があります。
- ホストコンピューターと本製品が同一のサブネット上に存在すること、またはこれら 2 つの機器間のデータ通信ができるようにルーターが正しく設定されていることを確認します。
- 設定を行う前に、本製品上で IP アドレスを設定する必要があります。
- Windows Server® 2008、Windows Server® 2012、Windows Server® 2012 R2、Windows Server® 2016 および Windows Server® 2019 の場合、プリントサービスをインストールする必要があります。

1. 次のいずれかを行ってください。

- (Windows® 7)

 (スタート) > コントロール パネル > ネットワークとインターネット > ネットワークのコンピューターとデバイスの表示をクリックします。

本製品の Web サービス名とプリンターアイコンが表示されます。


インストールする製品を右クリックします。

- (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 > PC 設定の変更 > PC とデバイス > デバイス > デバイスを追加する** をクリックします。

本製品の Web サービス名が表示されます。

- (Windows® 10)

 > **設定 > デバイス > プリンターとスキャナー > プリンターまたはスキャナーを追加します** をクリックします。

本製品の Web サービス名が表示されます。



- 本製品の Web サービス名は、本製品のモデル名および MAC アドレス（イーサネットアドレス）です（例：KONICA MINOLTA bizhub XXXXX (モデル名) [XXXXXXXXXXXX] (MAC アドレス/イーサネットアドレス)）。

2. 次のいずれかを行ってください。

- (Windows® 7)

本製品のドロップダウンメニューで **インストール** をクリックします。

- (Windows® 8.1 および Windows® 10)

インストールする製品を選択し、画面の指示に従います。



ドライバーをアンインストールするには **アンインストール** または **デバイスの削除** をクリックします。



関連情報





- Web サービスを使ってスキャンする (Windows® 7、Windows® 8.1 および Windows® 10)

■ ホーム > スキャン > 本製品のスキャンボタンを使用してスキャンする > Web サービスを使ってスキャンする (Windows® 7、Windows® 8.1 および Windows® 10) > 本製品から Web サービスを使ってスキャンする (Windows® 7、Windows® 8.1 および Windows® 10)

本製品から Web サービスを使ってスキャンする (Windows® 7、Windows® 8.1 および Windows® 10)

Web サービス経由のスキャンのためのドライバーをインストールしている場合、本製品の Web サービススキャンメニューにアクセスできます。

言語設定がお使いの OS と本製品間で異なる場合、画面に表示されるメッセージの文字の一部が空白に置き換えられることがあります。

1. 原稿をセットします。
2.  [スキャン] を押します。
3. 左または右にフリックして、 [Web サービス] を表示します。
4.  [Web サービス] を押します。
アイコンが画面の中央に移動し、青色でハイライト表示されます。
5.  [Web サービス] を押します。
6. 上または下にフリックするか、▲または▼を押してスキャンオプションを表示し、スキャンの種類を押します。
7. 上または下にフリックするか、▲または▼を押して、データ送信先のパソコン名を表示し、パソコン名を押します。
8. [スタート] を押します。
本製品でスキャン動作を開始します。

スキャンアプリケーションを選択するよう要求された場合は、リストから、Windows®ファクスとスキャンまたは、Windows®フォトギャラリーを選択します。

✓ 関連情報

- Web サービスを使ってスキャンする (Windows® 7、Windows® 8.1 および Windows® 10)

■ ホーム > スキャン > 本製品のスキャンボタンを使用してスキャンする > Web サービスを使ってスキャンする (Windows® 7、Windows® 8.1 および Windows®10) > Web サービスのスキャンプロファイルを編集する

Web サービスのスキャンプロファイルを編集する

1. 以下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**をクリックし、**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® 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、**デバイスとプリンターの表示**をクリックします。

2. 本製品のアイコン上で右クリックし、**スキャン プロファイル**を選択します。**スキャン プロファイル**のダイアログボックスが表示されます。
3. 目的のスキャンプロファイルを選択します。
4. **スキャナー**一覧で選択されたモデル名が、Web サービスのスキャンに対応している製品であることを確認し、**既定に設定**ボタンをクリックします。
5. **編集**をクリックします。
既定のプロファイルの編集のダイアログボックスが表示されます。
6. **スキャナーの種類**、**用紙サイズ**、**色の形式**、**ファイルの種類**、**解像度 (DPI)**、**明るさ**および**コントラスト**設定を選択します。
7. **プロファイルの保存**ボタンをクリックします。
Web サービスを使ってスキャンする場合のプロトコルとして適用されます。

スキャンアプリケーションを選択するよう要求された場合は、リストから、Windows®ファクスとスキャンまたは、Windows®フォトギャラリーを選択します。




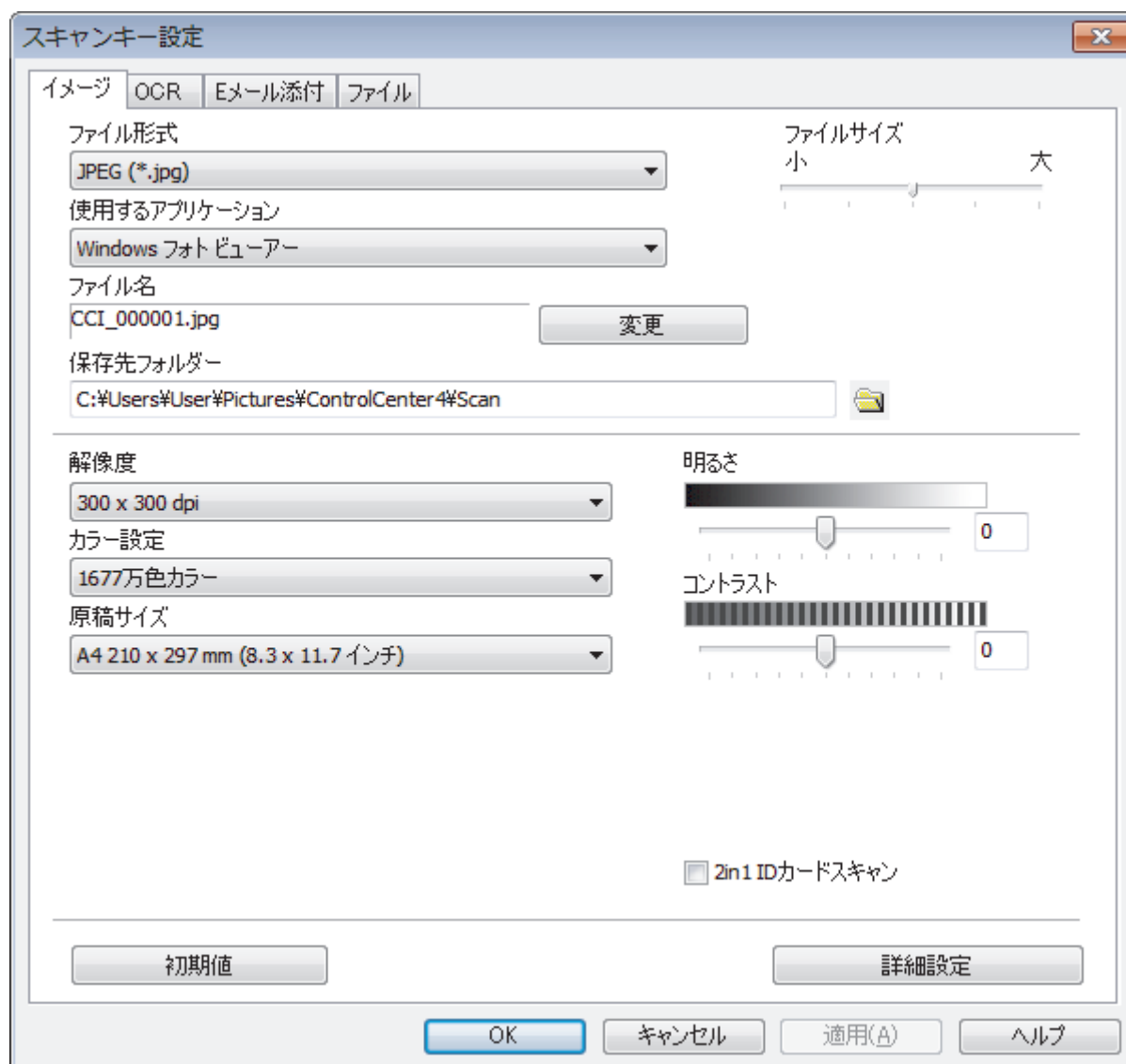
関連情報

- Web サービスを使ってスキャンする (Windows® 7、Windows® 8.1 および Windows®10)

▲ ホーム > スキャン > 本製品のスキャンボタンを使用してスキャンする > ControlCenter4 からスキャンボタン設定を変更する (Windows®)

ControlCenter4 からスキャンボタン設定を変更する (Windows®)

1. タスクトレイの  (ControlCenter4)アイコンをクリックし、開くをクリックします。
2. デバイス設定タブをクリックします。
3. スキャンキー設定ボタンをクリックします。
スキャンキー設定ダイアログボックスが表示されます。



4. 変更したいスキャン to 操作 (イメージ、OCR、Eメール添付、またはファイル) のタブをクリックします。
5. 必要に応じて設定を変更します。
6. OK をクリックします。



以下の表の通り、各タブはスキャンデータの送信先を表しています。
対応するタブをクリックして設定をカスタマイズすることで、スキャン to 設定を変更します。

タブの名称	対応する機能
イメージ	スキャン to イメージ
OCR	スキャン to OCR
E メール添付	スキャン to E メール
ファイル	スキャン to ファイル

設定	対応している機能			
	イメージ	OCR	E メール添付	ファイル
ファイル形式	○	○	○	○
使用するアプリケーション	○	○	-	-
OCR 言語	-	○	-	-
ファイル名	○	○	○	○
保存先フォルダー	○	○	○	○
保存先フォルダーを開く	-	-	-	○
ファイルサイズ	○	-	○	○
解像度	○	○	○	○
カラー設定	○	○	○	○
原稿サイズ	○	○	○	○
明るさ	○	○	○	○
コントラスト	○	○	○	○
2in1 ID カードスキャン	○	○	○	○
詳細設定	○	○	○	○
初期値	○	○	○	○

ファイル形式

スキャンしたデータを保存するファイル形式を選択します。

使用するアプリケーション

スキャンしたデータを開くアプリケーションを選択します。

OCR 言語

OCR 言語を設定して、スキャンした原稿中のテキストの言語を照合します。

ファイル名

変更をクリックして、ファイル名の接頭辞を変更します。

保存先フォルダー

フォルダーアイコンをクリックし、スキャンしたデータの保存先フォルダーを指定します。

保存先フォルダーを開く

スキャン後に自動的に保存先フォルダーを表示させる際に選択します。

ファイルサイズ

スキャンしたデータのサイズを調節します。 **ファイルサイズ**のつまみを右または左に移動させてファイルサイズを変更します。

解像度

解像度のドロップダウンリストから、スキャンする時の解像度を選択します。高い解像度を選択すると、スキャンしたデータの画質は向上しますが、ファイルサイズが大きくなったり、スキャンするのに時間がかかります。

カラー設定

さまざまな色濃度の中から選択します。

- **自動**

どんなタイプの原稿にも使用できます。原稿に対して適切な色濃度が自動的に選択されます。

- **モノクロ**

文字原稿または線画に使用します。

- **グレー**

写真やグラフィックに使用します。(見た目を自然なグレーに似せるために、黒い点を一定の規則で配置させることで、実際にはグレーの点を使用せずに擬似的にグレー画像を作成する、誤差拡散という手法を使っています。)

- **256 階調グレー**

写真やグラフィックに使用します。最大で 256 段階の色調のグレーを使用して、より正確に細部を再現します。

- **1677 万色カラー**

最も正確に色を再現した画像を作成したい場合に適しています。最大で 1680 万色を使って画像をスキャンしますが、最も多くのメモリーが必要とされ、転送時間が最も長くなります。

原稿サイズ

原稿サイズのドロップダウンリストから原稿の正確なサイズを選択します。

- **1 to 2 (A4)**を選択した場合は、スキャンしたデータは 2 つの A5 サイズのデータに分割されます。

明るさ

つまみを右または左に移動させて**明るさ**レベルを設定し、データの明暗を調整します。スキャンしたデータが明るすぎる場合は、明るさレベルを下げて再度原稿をスキャンしてください。データが暗すぎる場合は、明るさレベルを上げて再度原稿をスキャンしてください。数値を入力して**明るさ**レベルを設定することも可能です。

コントラスト

つまみを右または左に移動させて**コントラスト**レベルの調整を行います。レベルを上げると画像の明暗が強調され、レベルを下げるとグレー部分をより詳細に見られます。数値を入力して**コントラスト**レベルを設定することも可能です。

2in1 ID カードスキャン

運転免許証のようなカードの両面を 1 つのページにスキャンするときに、このチェックボックスにチェックを入れます。

詳細設定

詳細設定を行うには、カスタムスキャン設定ダイアログボックスで**詳細設定**ボタンをクリックします。

- **地色除去**

原稿の背景にある地色を取り除き、スキャンしたデータを見やすくします。強・中・弱の 3 つの設定から選びます。

(自動、256 階調グレー、および 1677 万色カラーのみ利用可能)

- **白紙除去**

スキャン結果から原稿の空白ページを取り除きます。

- **スキャン結果表示**

パソコン画面に、スキャンしたデータの総ページ数、および削除した白紙ページ数を表示させます。

- **ADF 傾き補正**

ADF(自動原稿送り装置)から原稿をスキャンする場合、原稿の歪みは本製品により自動的に修正されます。

初期値

すべての設定をお買い上げ時の状態に戻すときに選択します。

✓ 関連情報

- 本製品のスキャンボタンを使用してスキャンする

関連トピック：

- 写真やグラフィックをスキャンする
 - スキャンしたデータを PDF ファイルとしてパソコンに保存する
 - 編集可能テキストファイルとしてスキャンする（OCR）
 - スキャン to E メール添付
-


署名入り PDF の証明書を設定する

USB へのスキャン画像送信、E-mail サーバーへのスキャン画像送信、FTP へのスキャン画像送信、SFTP へのスキャン画像送信、ネットワークへのスキャン画像送信または SharePoint®へのスキャン画像送信の各機能に対し、署名入り PDF を選択する場合、ウェブブラウザを使用して本製品に証明書を設定する必要があります。

署名入り PDF を使用するには、本製品とお使いのパソコンに証明書をインストールする必要があります。

1. ウェブブラウザを起動します。

ブラウザのアドレス欄に「http://製品の IP アドレス」を入力します（「製品の IP アドレス」の部分には本製品の IP アドレスまたはプリントサーバー名を入力します）。例：http://192.168.1.2

パスワード設定をしている場合は、そのパスワードを入力し、を押します。初期パスワードは、initpass です。

2. 管理者設定タブをクリックします。
3. 左側にあるナビゲーションバーの**電子署名付 PDF** メニューをクリックします。

署名入り PDF の設定ダイアログボックスが表示されます。

電子署名付PDF

証明書の選択

XXXX ▼

(電子署名付PDFを使用するためには、証明書の設定を行う必要があります。
下記の「証明書設定」をクリックし、設定を行ってください。)

証明書>>

キャンセル

OK

4. **証明書の選択** ドロップダウンリストをクリックして、証明書を選択します。
5. **OK** をクリックします。

✓ 関連情報


- 本製品のスキャンボタンを使用してスキャンする

お使いのパソコンからスキャンを無効にする

お使いのパソコンからスキャン機能を無効にします。ウェブブラウザを使用してプルスキャンを設定します。

1. ウェブブラウザを起動します。

ブラウザのアドレス欄に「http://製品の IP アドレス」を入力します（「製品の IP アドレス」の部分には本製品の IP アドレスまたはプリントサーバー名を入力します）。例：http://192.168.1.2

パスワード設定をしている場合は、そのパスワードを入力し、を押します。初期パスワードは、initpass です。

2. **スキャン**タブをクリックします。
3. 左側にあるナビゲーションバーの **PC からのスキャン**メニューをクリックします。
4. **PC からのスキャン**欄で、**無効**をクリックします。
5. **OK** をクリックします。

関連情報

- [本製品のスキャンボタンを使用してスキャンする](#)

お使いのパソコンからスキャンする (Windows®)

お使いのパソコンを使用して、写真や文章を本製品でスキャンします。弊社から提供されているソフトウェアやお使いのスキャンアプリケーションを使用します。

- [ControlCenter4 Home モードを使ってスキャンする \(Windows®\)](#)
- [ControlCenter4 Advanced モードを使ってスキャンする \(Windows®\)](#)
- [Windows® フォトギャラリー、Windows® FAX とスキャンを使ってスキャンする](#)

■ ホーム > スキャン > お使いのパソコンからスキャンする (Windows®) > ControlCenter4 Home モードを使ってスキャンする (Windows®)

ControlCenter4 Home モードを使ってスキャンする (Windows®)


ControlCenter4 Home モードから、本製品の主要な機能进行操作できます。

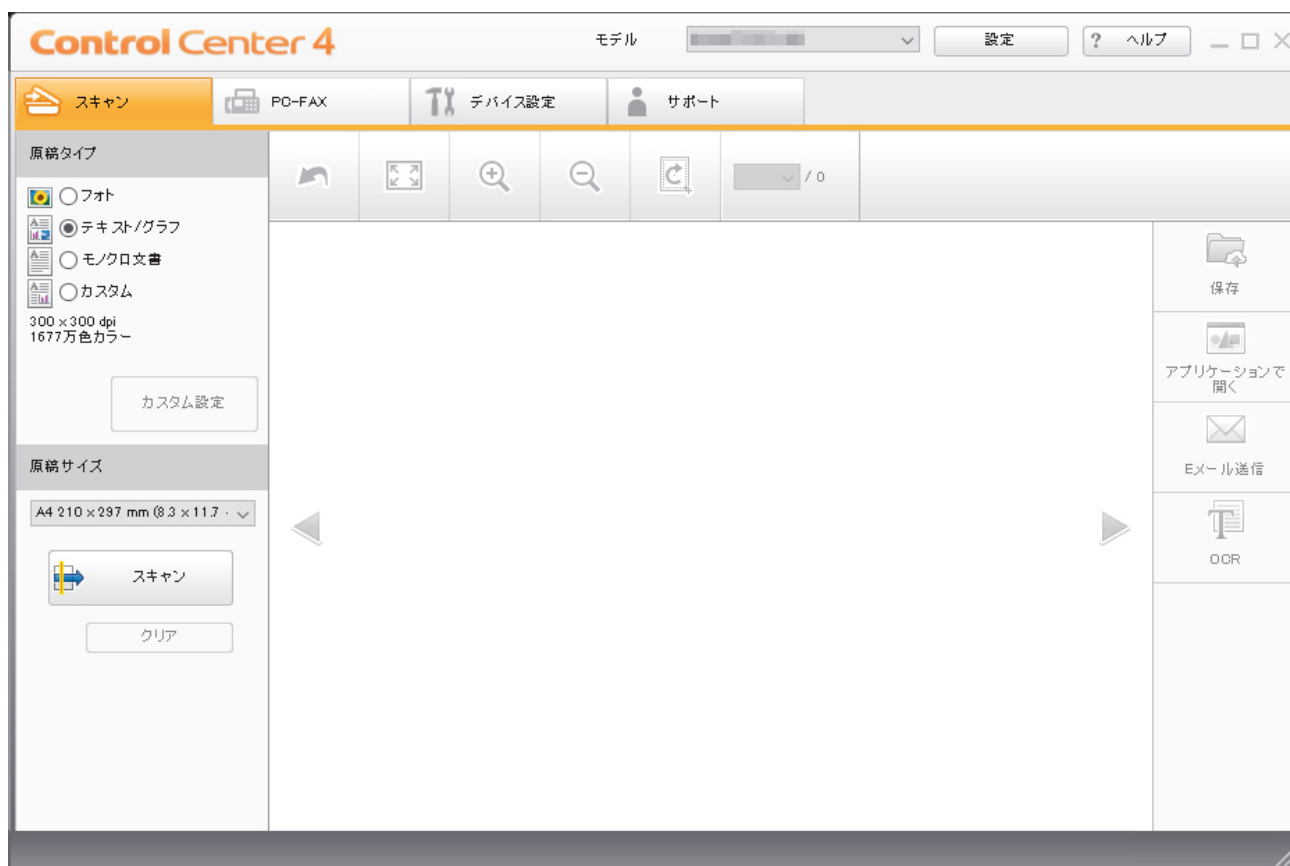
- [ControlCenter4 Home モードのスキャン \(Windows®\)](#)
- [ControlCenter4 Home モードを使ってスキャンしたデータを PDF ファイルとして保存する\(Windows®\)](#)
- [ControlCenter4 Home モードのスキャン設定 \(Windows®\)](#)


■ ホーム > スキャン > お使いのパソコンからスキャンする (Windows®) > ControlCenter4 Home モードを使ってスキャンする (Windows®) > ControlCenter4 Home モードのスキャン (Windows®)





ControlCenter4 Home モードのスキャン (Windows®)

ControlCenter4 のモード設定で **Home モード** を選択します。

1. 原稿をセットします。
2. タスクトレイの  (ControlCenter4) アイコンをクリックし、**開く** をクリックします。
3. **スキャン** タブをクリックします。



4. **原稿タイプ** を選択します。
5. 必要に応じて原稿の**原稿サイズ**を変更します。
6.  (**スキャン**) をクリックします。

本製品がスキャン動作を開始し、スキャンした画像がイメージビューアーに表示されます。
7. スキャンしたデータの各ページをプレビューする場合は、左または右の矢印ボタンをクリックします。
8. 必要に応じてスキャン画像を切り取ります。
9. 次のいずれかを行ってください。
 -  (**保存**) をクリックして、スキャンしたデータを保存します。
 -  (**アプリケーションで開く**) をクリックして、お好みのアプリケーションでスキャンしたデータを開きます。
 -  (**Eメール送信**) をクリックして、スキャンしたデータを E メールに添付します。
 - スキャンした原稿を編集可能なテキストファイルに変換するには  (**OCR**) をクリックします。(特定のモデルのみ可能)



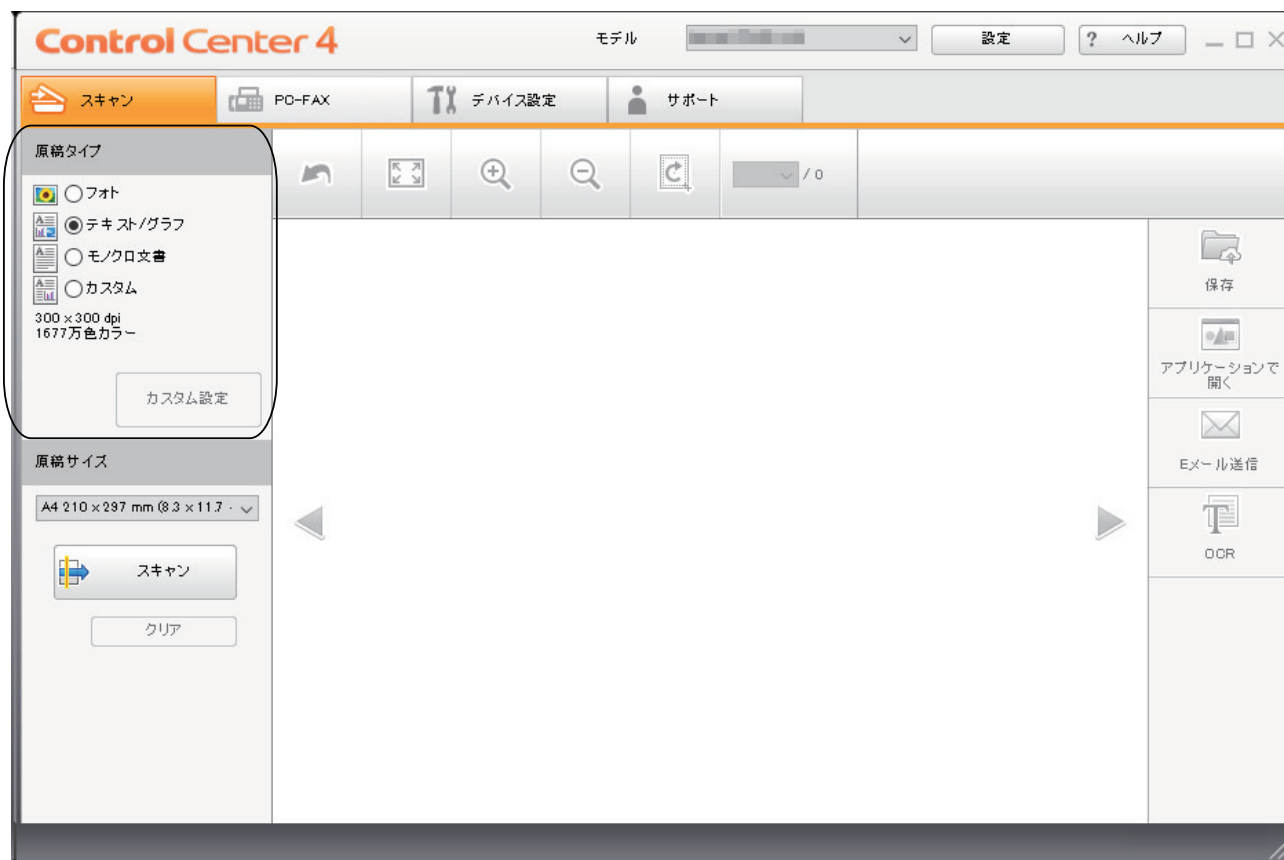
関連情報

- ControlCenter4 Home モードを使ってスキャンする (Windows®)
 - ControlCenter4 Home モードで原稿タイプを選択する(Windows®)
 - ControlCenter4 Home モードでスキャンサイズを変更する(Windows®)
 - ControlCenter4 Home モードでスキャンした画像を編集する(Windows®)
 - ControlCenter4 Home モードを使って、スキャンしたデータをアプリケーションに送る (Windows®)

■ ホーム > スキャン > お使いのパソコンからスキャンする (Windows®) > ControlCenter4 Home モードを使ってスキャンする (Windows®) > ControlCenter4 Home モードのスキャン (Windows®) > ControlCenter4 Home モードで原稿タイプを選択する(Windows®)

ControlCenter4 Home モードで原稿タイプを選択する(Windows®)

- スキャンする原稿の種類や用途に応じて、**原稿タイプ**を選択します。



オプション	説明
フォト	600 x 600 dpi 1677 万色カラー
テキスト/グラフ	300 x 300 dpi 1677 万色カラー
モノクロ文書	200 x 200 dpi モノクロ
カスタム	300 x 300 dpi (初期設定は 1677 万色カラー) カスタム設定ボタンからお好みのスキャン設定を選択します。

✓ 関連情報

- ControlCenter4 Home モードのスキャン (Windows®)
 - カスタムスキャン設定 (Windows®)

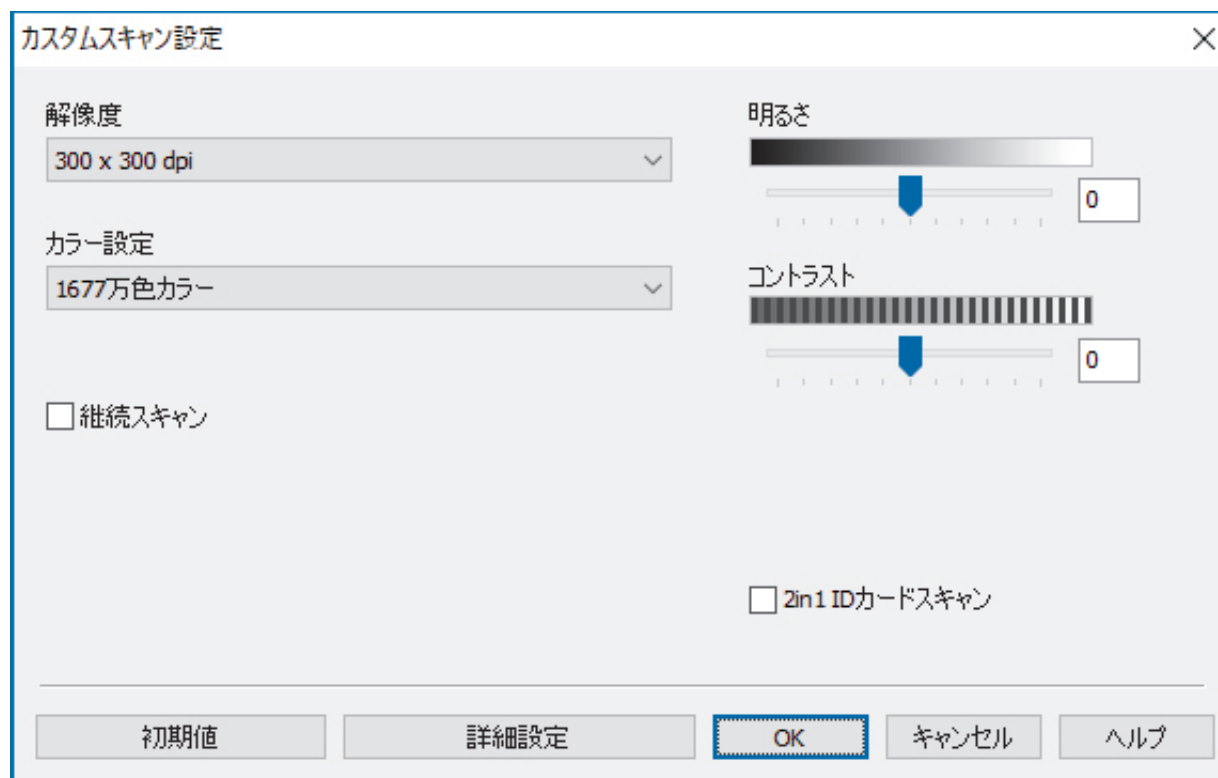
▲ホーム > スキャン > お使いのパソコンからスキャンする (Windows®) > ControlCenter4 Home モードを使ってスキャンする (Windows®) > ControlCenter4 Home モードのスキャン (Windows®) > ControlCenter4 Home モードで原稿タイプを選択する(Windows®) > カスタムスキャン設定 (Windows®)

カスタムスキャン設定 (Windows®)

原稿タイプで**カスタム**を選択して、詳細なスキャン設定を変更します。

- ・ **カスタム**を選択して、**カスタム設定**ボタンをクリックします。

カスタムスキャン設定のダイアログボックスが表示されます。



以下の設定を変更することができます。

解像度

解像度のドロップダウンリストから、スキャンする時の解像度を選択します。高い解像度を選択すると、スキャンしたデータの画質は向上しますが、ファイルサイズが大きくなったり、スキャンするのに時間がかかります。

カラー設定

さまざまな色濃度の中から選択します。

- 自動

どんなタイプの原稿にも使用できます。原稿に対して適切な色濃度が自動的に選択されます。

- モノクロ

文字原稿または線画に使用します。

- グレー

写真やグラフィックに使用します。(見た目を自然なグレーに似せるために、黒い点を一定の規則で配置させることで、実際にはグレーの点を使用せずに擬似的にグレー画像を作成する、誤差拡散という手法を使っています。)

- 256 階調グレー

写真やグラフィックに使用します。最大で 256 段階の色調のグレーを使用して、より正確に細部を再現します。

- 1677 万色カラー

最も正確に色を再現した画像を作成したい場合に適しています。最大で 1680 万色を使って画像をスキャンしますが、最も多くのメモリーが必要とされ、転送時間が最も長くなります。

明るさ

つまみを右または左に移動させて**明るさ**レベルを設定し、データの明暗を調整します。スキャンしたデータが明るすぎる場合は、明るさレベルを下げて再度原稿をスキャンしてください。データが暗すぎる場合は、明るさレベルを上げて再度原稿をスキャンしてください。数値を入力して**明るさ**レベルを設定することも可能です。

コントラスト

つまみを右または左に移動させて**コントラスト**レベルの調整を行います。レベルを上げると画像の明暗が強調され、レベルを下げるとグレー部分をより詳細に見られます。数値を入力して**コントラスト**レベルを設定することも可能です。

継続スキャン

原稿台ガラスまたは ADF（自動原稿送り装置）から複数ページをスキャンするときに選択します（特定モデルのみ対応）。1 ページ目がスキャンされた後に、スキャンを続けるか終了するかを選びます。この方法を使うと、ADF（自動原稿送り装置）の上限を超えるページ数をスキャンすることが可能になります。

2in1 ID カードスキャン

運転免許証のようなカードの両面を 1 つのページにスキャンするときに、このチェックボックスにチェックを入れます。

詳細設定

詳細設定を行うには、カスタムスキャン設定ダイアログボックスで**詳細設定**ボタンをクリックします。

- 地色除去

原稿の背景にある地色を取り除き、スキャンしたデータを見やすくします。強・中・弱の 3 つの設定から選びます。

（自動、256 階調グレー、および 1677 万色カラーのみ利用可能）

- 白紙除去

スキャン結果から原稿の空白ページを取り除きます。

- スキャン結果表示

パソコン画面に、スキャンしたデータの総ページ数、および削除した白紙ページ数を表示させます。

- ADF 傾き補正

ADF(自動原稿送り装置)から原稿をスキャンする場合、原稿の歪みは本製品により自動的に修正されます。



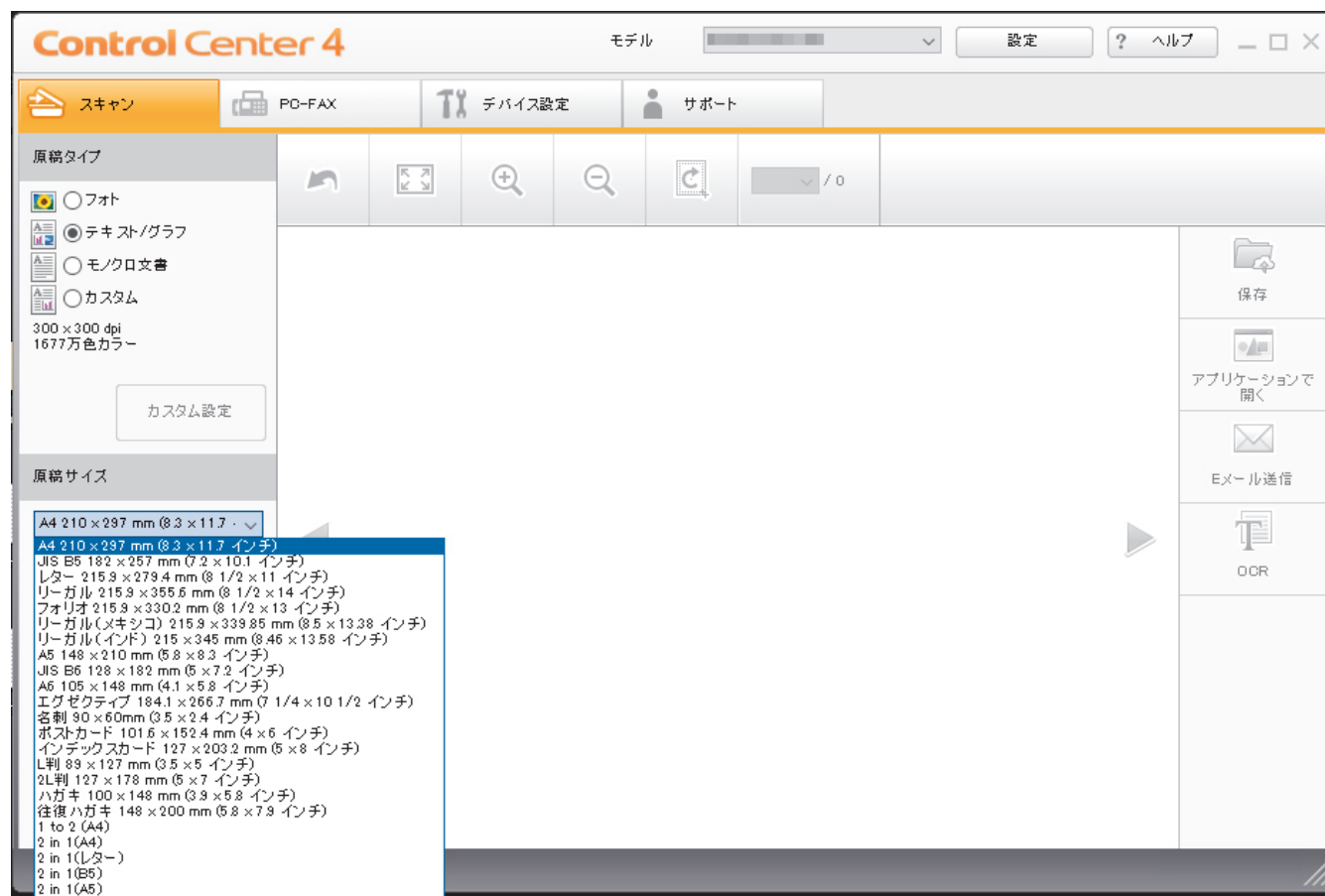
関連情報

- [ControlCenter4 Home モードで原稿タイプを選択する\(Windows®\)](#)

■ ホーム > スキャン > お使いのパソコンからスキャンする (Windows®) > ControlCenter4 Home モードを使ってスキャンする (Windows®) > ControlCenter4 Home モードのスキャン (Windows®) > ControlCenter4 Home モードでスキャンサイズを変更する(Windows®)

ControlCenter4 Home モードでスキャンサイズを変更する(Windows®)

原稿サイズのドロップダウンリストから正しい原稿サイズを選択することで、スキャンする速度を上げることができます。



✓ 関連情報

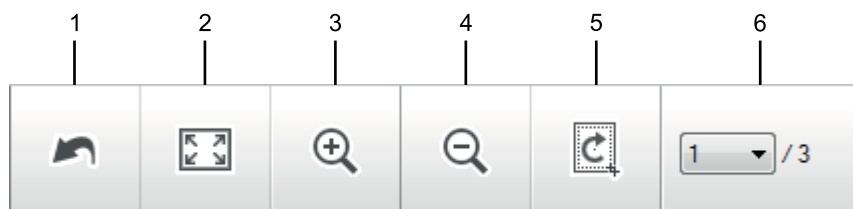
- [ControlCenter4 Home モードのスキャン \(Windows®\)](#)

▲ ホーム > スキャン > お使いのパソコンからスキャンする (Windows®) > ControlCenter4 Home モードを使ってスキャンする (Windows®) > ControlCenter4 Home モードのスキャン (Windows®) > ControlCenter4 Home モードでスキャンした画像を編集する(Windows®)

ControlCenter4 Home モードでスキャンした画像を編集する(Windows®)

画像編集ツールで、スキャンした画像の不要な部分を切り取ることができます。**拡大**および**縮小**を使用すれば、切り取った画像が見やすくなります。

画像編集ツールバー



1. 編集取消

選択された画像に適用した編集内容を、すべて取り消します。編集された画像は元の状態に戻ります。

2. ウィンドウに合わせる

スキャンした画像の全体画像がウィンドウに合わせて表示されます。

3. 拡大

スキャンした画像を拡大します。

4. 縮小

スキャンした画像を縮小します。

5. 編集

画像の外側の部分を取り除きます。**編集**ボタンをクリックして、必要な部分を残して、不要な外側の部分を切り取ります。

6. 枚数表示

イメージビューアーに現在表示されているスキャンデータのページ数を示します。別のページを表示するには、ページ番号のドロップダウンリストからページ番号を選択します。

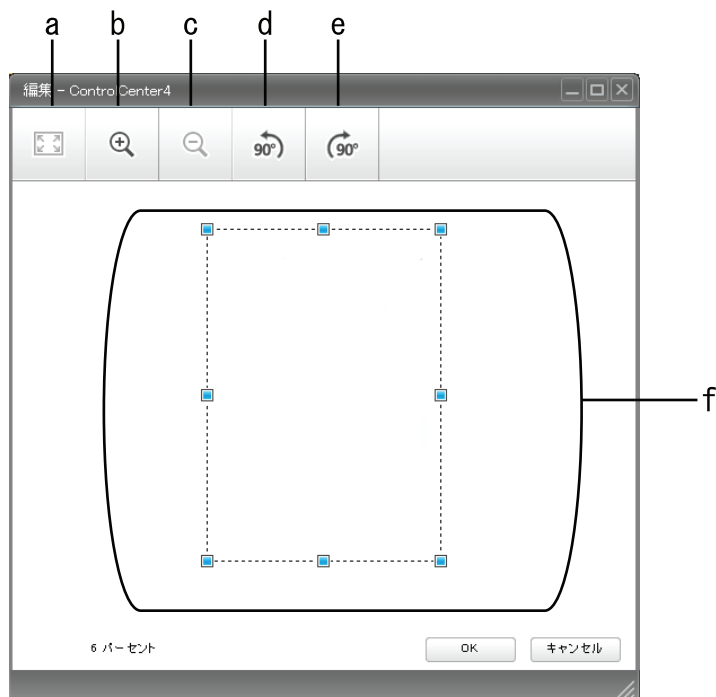


複数ページのスキャンをした場合、プレビュー画面の左または右の矢印ボタンをクリックして、スキャンしたデータの各ページを確認することができます。

1. 原稿をスキャンします。

2. (編集)をクリックして、スキャンしたデータを編集します。

編集 - ControlCenter4 画面が表示されます。



- a. スキャンした画像の全体画像をウィンドウに合わせます。
 - b. 画像を拡大します。
 - c. 画像を縮小します。
 - d. 画像を反時計回りに 90 度回転します。
 - e. 画像を時計回りに 90 度回転します。
 - f. フレームをクリックおよびドラッグして、切り取る範囲を調節します。
3. **OK** をクリックします。
イメージビューアーに編集後のイメージが表示されます。

✓ 関連情報


- [ControlCenter4 Home モードのスキャン \(Windows®\)](#)

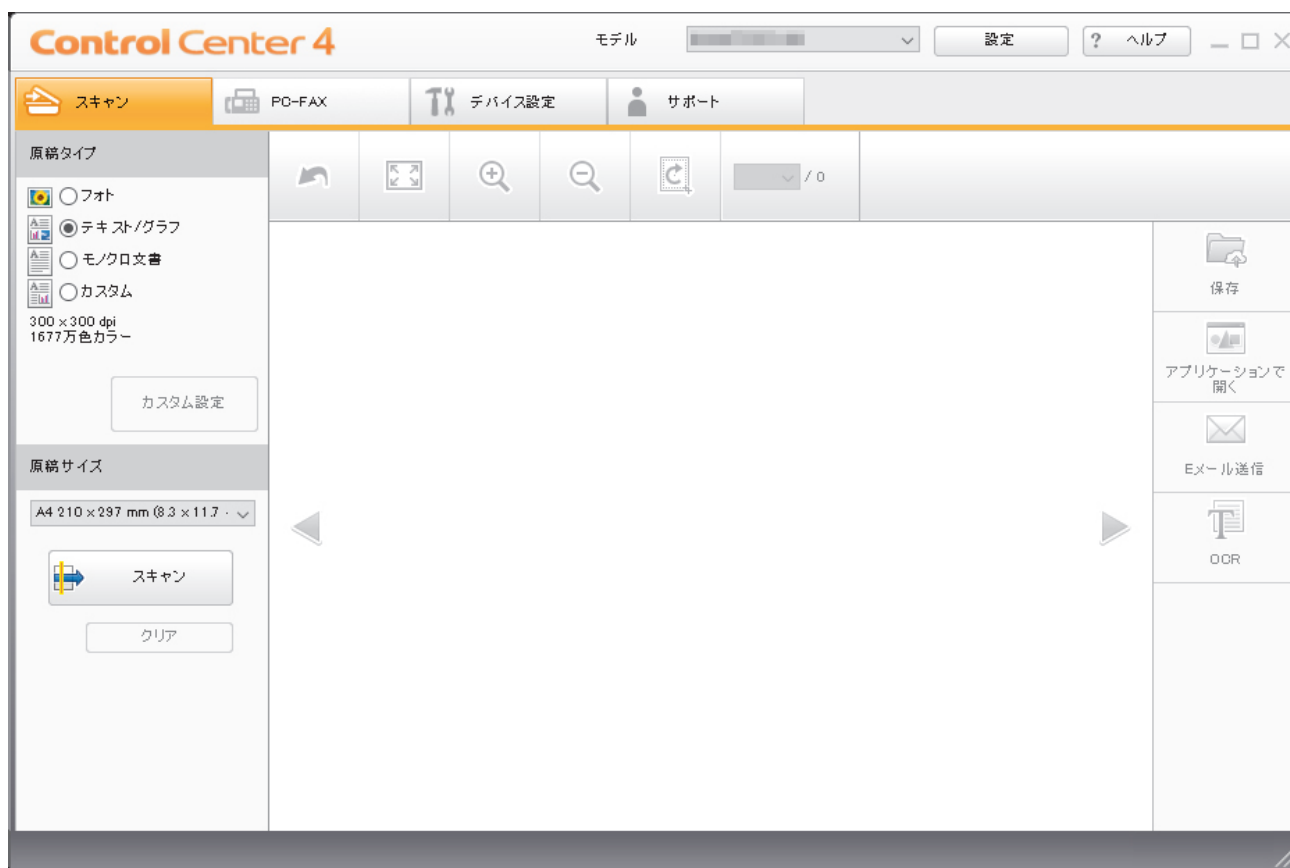
■ ホーム > スキャン > お使いのパソコンからスキャンする (Windows®) > ControlCenter4 Home モードを使ってスキャンする (Windows®) > ControlCenter4 Home モードのスキャン (Windows®) > ControlCenter4 Home モードを使って、スキャンしたデータをアプリケーションに送る (Windows®)


ControlCenter4 Home モードを使って、スキャンしたデータをアプリケーションに送る (Windows®)

アプリケーションで開くボタンを使って、スキャンしたデータを画像編集用アプリケーションへ送信します。

ControlCenter4 のモード設定で **Home モード** を選択します。

1. 原稿をセットします。
2. タスクトレイの  (ControlCenter4) アイコンをクリックし、**開く** をクリックします。
3. **スキャン** タブをクリックします。



4. **原稿タイプ** を選択します。
5. 必要に応じて原稿のサイズを変更します。
6.  (**スキャン**) をクリックします。

本製品がスキャン動作を開始し、スキャンした画像がイメージビューアーに表示されます。
7. スキャンしたデータの各ページをプレビューする場合は、左または右の矢印ボタンをクリックします。
8. 必要に応じてスキャン画像を切り取ります。
9. **アプリケーションで開く** ボタンをクリックします。
10. リストからアプリケーションを選択し、**OK** をクリックします。

選択されたアプリケーションで画像を開きます。


✓ 関連情報

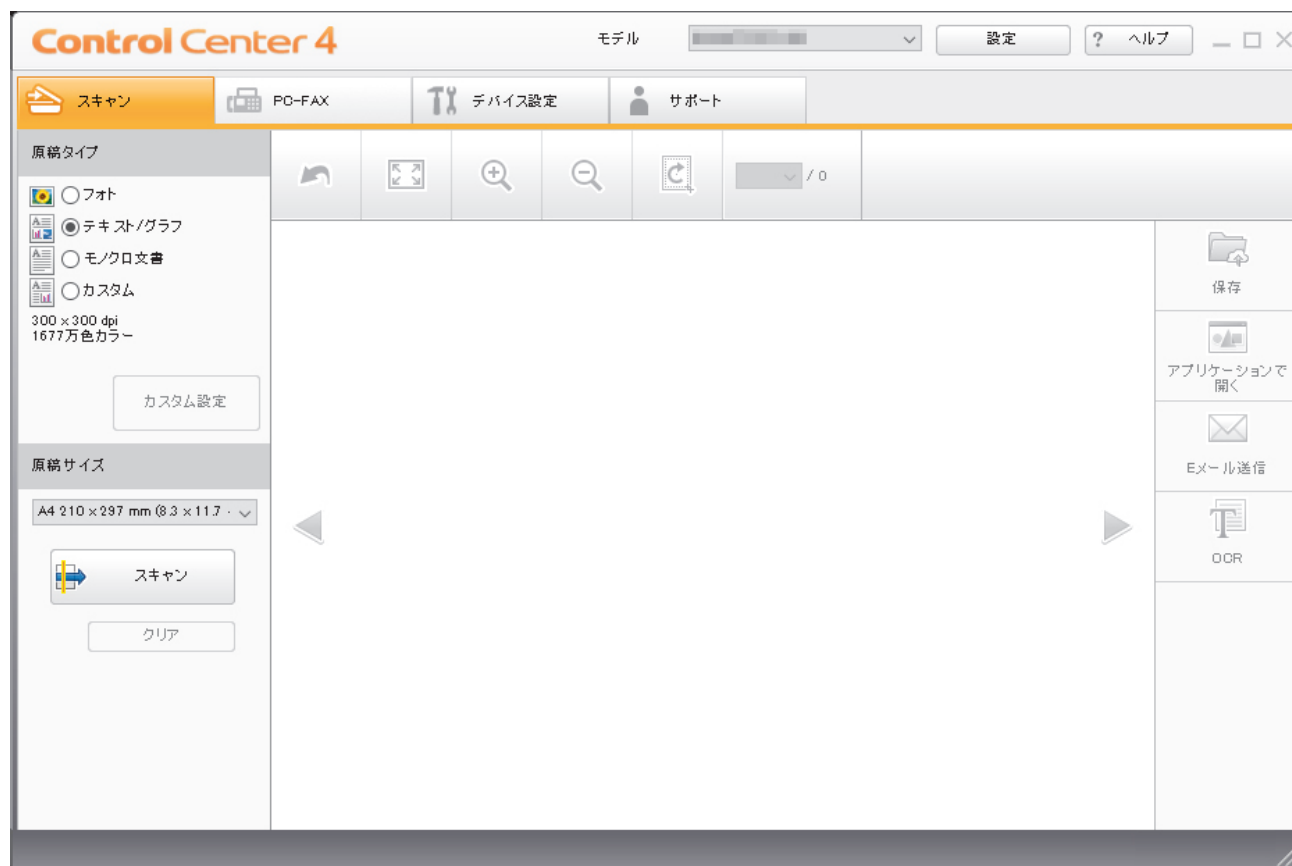
- [ControlCenter4 Home モードのスキャン \(Windows®\)](#)


■ ホーム > スキャン > お使いのパソコンからスキャンする (Windows®) > ControlCenter4 Home モードを使ってスキャンする (Windows®) > ControlCenter4 Home モードを使ってスキャンしたデータを PDF ファイルとして保存する(Windows®)

ControlCenter4 Home モードを使ってスキャンしたデータを PDF ファイルとして保存する(Windows®)

ControlCenter4 のモード設定で **Home モード** を選択します。

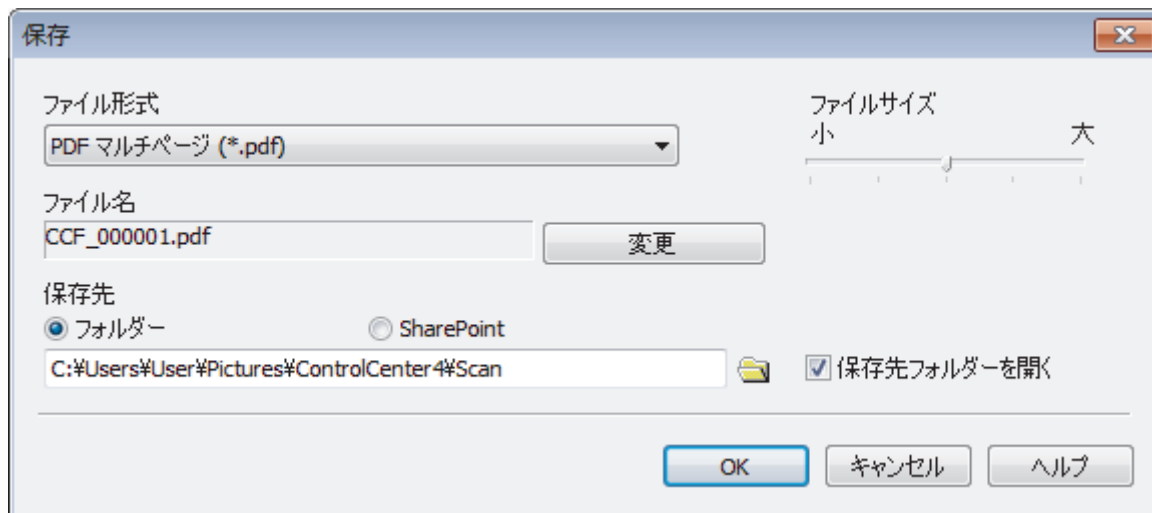
1. 原稿をセットします。
2. タスクトレイの  (ControlCenter4) アイコンをクリックし、**開く** をクリックします。
3. **スキャン** タブをクリックします。





4. **原稿タイプ** を選択します。
5. 必要に応じて原稿のサイズを変更します。
6.  (**スキャン**) をクリックします。

本製品がスキャン動作を開始し、スキャンした画像がイメージビューアーに表示されます。
7. スキャンしたデータの各ページをプレビューする場合は、左または右の矢印ボタンをクリックします。
8. **保存** をクリックします。

保存 のダイアログボックスが表示されます。
9. **ファイル形式** ドロップダウンリストをクリックして、PDF ファイルを選択します。



 パスワード保護された PDF として保存するには、**ファイル形式**ドロップダウンリストから**パスワード付 PDF シングルページ (*.pdf)**または**パスワード付 PDF マルチページ (*.pdf)**を選択し、 をクリックしてパスワードを入力します。

10. ファイル名を変更するには、必要に応じて**変更**ボタンをクリックします。
11. フォルダーアイコンをクリックし、スキャンした原稿を保存したいフォルダーを指定します。
12. **OK** をクリックします。
スキャンした文書は指定先フォルダーに PDF として保存されます。

関連情報

- [ControlCenter4 Home モードを使ってスキャンする \(Windows®\)](#)

ControlCenter4 Home モードのスキャン設定 (Windows®)

設定	対応している機能			
	アプリケーションで開く	OCR	E メール送信	保存
ファイル形式	-	○	○	○
使用するアプリケーション	○	○	-	-
OCR 言語	-	○	-	-
ファイル名	-	-	-	○
保存先	-	-	-	○
保存先フォルダーを開く	-	-	-	○
ファイルサイズ	-	-	○	○

ファイル形式

スキャンしたデータを保存するファイル形式を選択します。

E メール送信および保存の場合

- Windows ビットマップ (*.bmp)
- JPEG (*.jpg) (写真をスキャンする場合、ほとんどのユーザーにお勧めします。)
- TIFF シングルページ (*.tif)
- TIFF マルチページ (*.tif)
- Portable Network Graphics (*.png)
- PDF シングルページ (*.pdf) (原稿をスキャンして共有する場合にお勧めします。)
- PDF マルチページ (*.pdf) (原稿をスキャンして共有する場合にお勧めします。)
- PDF/A シングルページ (*.pdf) (原稿をスキャンして共有する場合にお勧めします。)
- PDF/A マルチページ (*.pdf) (原稿をスキャンして共有する場合にお勧めします。)
- 高圧縮 PDF シングルページ (*.pdf)
- 高圧縮 PDF マルチページ (*.pdf)
- パスワード付 PDF シングルページ (*.pdf)
- パスワード付 PDF マルチページ (*.pdf)
- サーチャブル PDF シングルページ (*.pdf)
- サーチャブル PDF マルチページ (*.pdf)
- XML Paper Specification (*.xps) (XML Paper Specification は、Windows® 7、Windows® 8.1 および Windows® 10 で、または XML Paper Specification ファイルをサポートするアプリケーションを使用する場合に利用できます。)
- Microsoft Office Word (*.docx) (特定モデルのみ対応)
- Microsoft Office PowerPoint (*.pptx) (特定モデルのみ対応)

OCR の場合

- テキストファイル (*.txt)
- リッチテキスト形式 (*.rtf)
- HTML (*.htm)
- サーチャブル PDF シングルページ (*.pdf)
- サーチャブル PDF マルチページ (*.pdf)

使用するアプリケーション

スキャンしたデータを開くアプリケーションを選択します。

OCR 言語

スキャンした文書の言語に一致する OCR（光学式文字認識）言語を設定します。

ファイル名

変更をクリックして、ファイル名の接頭辞を変更します。

保存先

フォルダーまたは **SharePoint** ボタンを選択して、スキャンしたデータの保存先を指定します。

保存先フォルダーを開く

スキャン後に自動的に保存先フォルダーを表示させる際に選択します。

ファイルサイズ

スキャンしたデータのサイズを調節します。 **ファイルサイズ**のつまみを右または左に移動させてファイルサイズを変更します。

カスタム設定

カスタムを選択して、**カスタム設定**ボタンをクリックし、設定を変更します。

原稿サイズ

原稿サイズドロップダウンメニューから、使用する原稿と同じサイズを選択します。



関連情報

- [ControlCenter4 Home モードを使ってスキャンする（Windows®）](#)
-

ControlCenter4 Advanced モードを使ってスキャンする (Windows®)

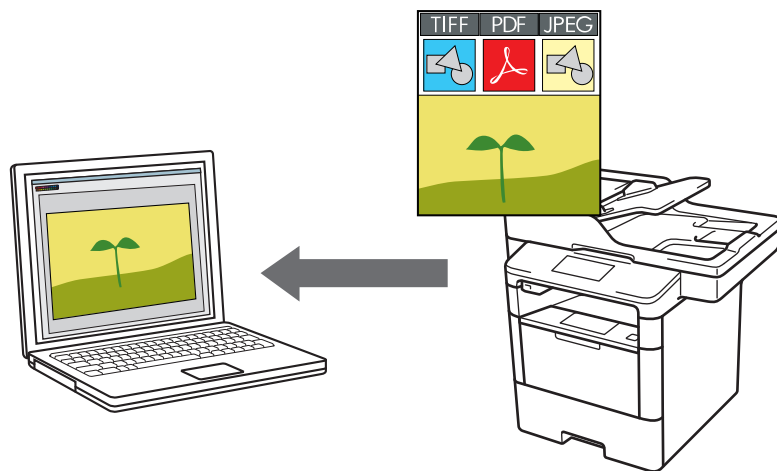
ControlCenter4 Advanced モードでは、本製品のより詳細な機能进行操作して、ワンタッチのスキャン操作に変更することができます。

- ControlCenter4 Advanced モードを使って、写真やグラフィックをスキャンする (Windows®)
- ControlCenter4 Advanced モード (Windows®) を使用して、スキャンデータを PDF ファイルとしてフォルダーに保存する
- ControlCenter4 Advanced モードを使って、ID カードの両面をスキャンする (Windows®)
- ControlCenter4 Advanced モードを使用したスキャン to E メール添付 (Windows®)
- ControlCenter4 Advanced モード (Windows) を使用したスキャン to 編集可能テキストファイル (OCR)
- ControlCenter4 Advanced モードのスキャン設定 (Windows®)

■ ホーム > スキャン > お使いのパソコンからスキャンする (Windows®) > ControlCenter4 Advanced モードを使ってスキャンする (Windows®) > ControlCenter4 Advanced モードを使って、写真やグラフィックをスキャンする(Windows®)

ControlCenter4 Advanced モードを使って、写真やグラフィックをスキャンする(Windows®)

スキャンした写真やグラフィックを、お使いのパソコンに直接送信します。

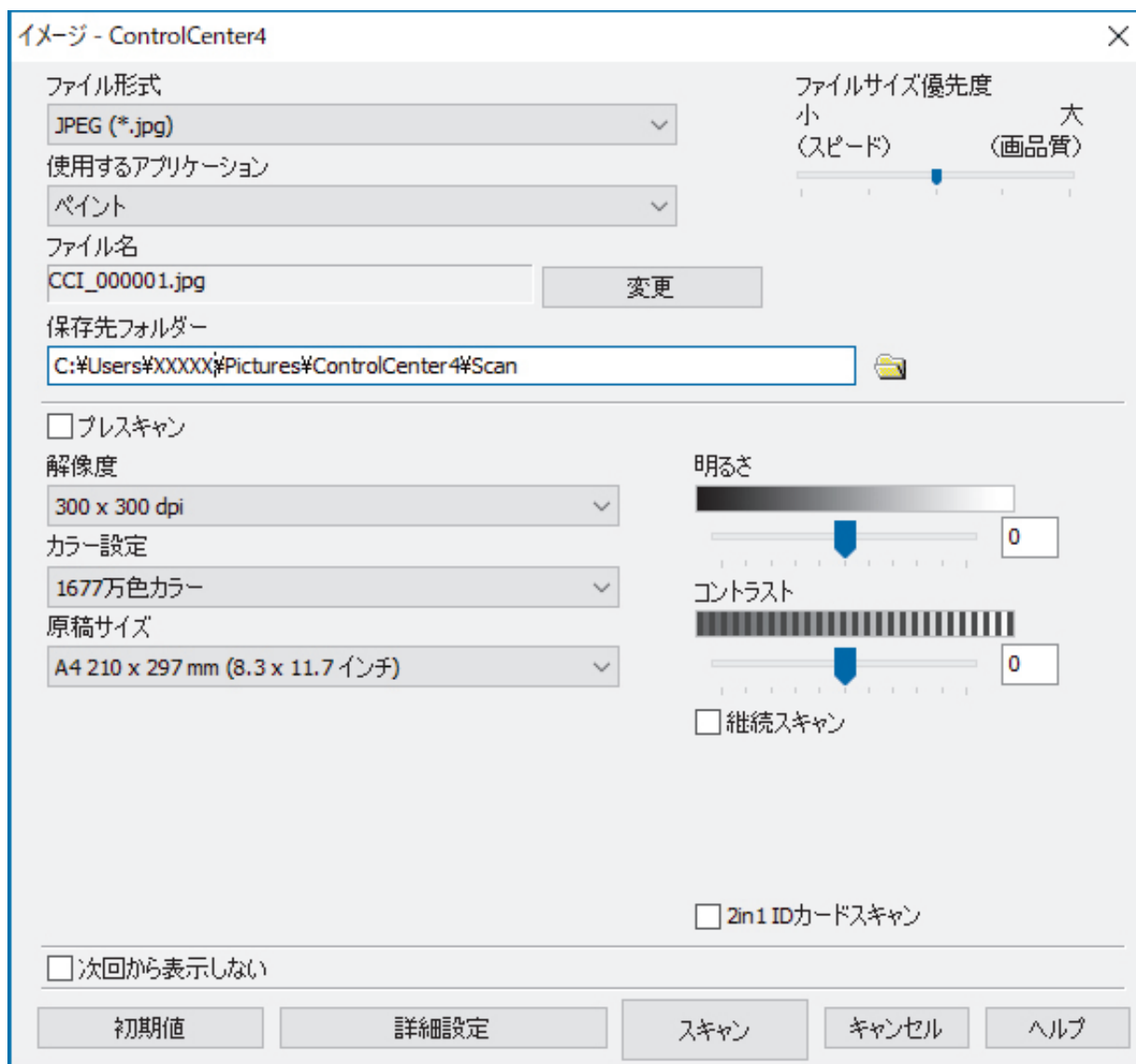


ControlCenter4 のモード設定で **Advanced モード**を選択します。

1. 原稿をセットします。
2. タスクトレイの **CC4** (ControlCenter4)アイコンをクリックし、**開く**をクリックします。
3. **スキャン**タブをクリックします。



4. **イメージ**ボタンをクリックします。
スキャン設定ダイアログボックスが表示されます。



5. 必要に応じて、ファイル形式、ファイル名、保存先ファイルパス、解像度、およびカラー設定等のスキャン設定を変更します。



- ファイル名を変更するには、**変更**をクリックします。
- **保存先フォルダー**を変更するには、フォルダーアイコンをクリックします。
- スキャンした画像のプレビューおよび設定を行うには、**プレスキャン**のチェックボックスにチェックを入れます。

6. **スキャン**をクリックします。

本製品でスキャン動作を開始します。選択されたアプリケーションで画像を開きます。



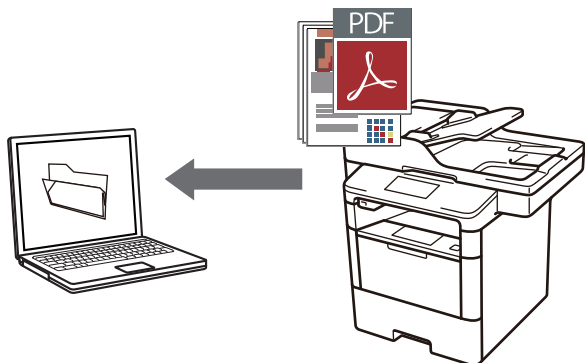
関連情報

- [ControlCenter4 Advanced モードを使ってスキャンする \(Windows®\)](#)


▲ ホーム > スキャン > お使いのパソコンからスキャンする (Windows®) > ControlCenter4 Advanced モードを使ってスキャンする (Windows®) > ControlCenter4 Advanced モード (Windows®) を使用して、スキャンデータを PDF ファイルとしてフォルダーに保存する

ControlCenter4 Advanced モード (Windows®) を使用して、スキャンデータを PDF ファイルとしてフォルダーに保存する

原稿をスキャンし、お使いのパソコン上に PDF ファイルとして保存します。





ControlCenter4 のモード設定で **Advanced モード** を選択します。

1. 原稿をセットします。
2. タスクトレイの  (ControlCenter4) アイコンをクリックし、**開く** をクリックします。
3. **スキャン** タブをクリックします。




4. **ファイル**ボタンをクリックします。
スキャン設定ダイアログボックスが表示されます。

5. **ファイル形式**ドロップダウンリストをクリックして、PDF ファイルを選択します。

 パスワード保護された PDF として保存するには、**ファイル形式**ドロップダウンリストから**パスワード付 PDF シングルページ (*.pdf)**または**パスワード付 PDF マルチページ (*.pdf)**を選択し、 をクリックしてパスワードを入力します。

6. フォルダーアイコンをクリックし、スキャンした原稿を保存したいフォルダーを指定します。
7. 必要に応じて、ファイル形式、ファイル名、解像度、およびカラー等のスキャン設定を変更します。

 スキャンした画像のプレビューおよび設定を行うには、**プレスキャン**のチェックボックスにチェックを入れます。

8. **スキャン**をクリックします。
本製品でスキャン動作を開始します。選択されたフォルダーにファイルが保存されます。


関連情報

- ControlCenter4 Advanced モードを使ってスキャンする (Windows®)

■ ホーム > スキャン > お使いのパソコンからスキャンする (Windows®) > ControlCenter4 Advanced モードを使ってスキャンする (Windows®) > ControlCenter4 Advanced モードを使って、ID カードの両面をスキャンする (Windows®)

ControlCenter4 Advanced モードを使って、ID カードの両面をスキャンする (Windows®)

ControlCenter4 のモード設定で **Advanced モード** を選択します。

1. 原稿台ガラスに運転免許証のような両面の ID カードをセットします。
2. タスクトレイの  (ControlCenter4) アイコンをクリックし、**開く** をクリックします。
3. **スキャン** タブをクリックします。



4. **ファイル**ボタンをクリックします。
スキャン設定ダイアログボックスが表示されます。

ファイル - ControlCenter4

ファイル形式
PDF マルチページ (*.pdf)

ファイル名
CCF_000001.pdf

保存先
☒ フォルダー ☐ SharePoint
C:\Users\XXXXXX\Pictures\ControlCenter4\Scan

☐ プレスキャン

解像度
300 x 300 dpi

カラー設定
1677万色カラー

原稿サイズ
A4 210 x 297 mm (8.3 x 11.7 インチ)

ファイルサイズ優先度
小 (スピード) 大 (画品質)

☐ スキャン毎に名前をつける
☒ 保存先フォルダーを開く

明るさ
0

コントラスト
0

☐ 継続スキャン

☐ 2in1 IDカードスキャン

☐ 次回から表示しない

初期値 詳細設定 スキャン キャンセル ヘルプ

5. **2in1 ID カードスキャン**のチェックボックスにチェックを入れます。
指示ダイアログが表示されます。
6. 画面の指示を確認して、**OK** をクリックします。
7. 必要に応じて、ファイル形式、ファイル名、スキャン場所、解像度、およびカラー等のスキャン設定を変更します。
8. **スキャン**をクリックします。
本製品で ID カードの片面のスキャンを開始します。
9. 片面のスキャンが終わったら、ID カードを裏返し、**続ける**をクリックしてもう一方の片面もスキャンします。
10. **完了**をクリックします。

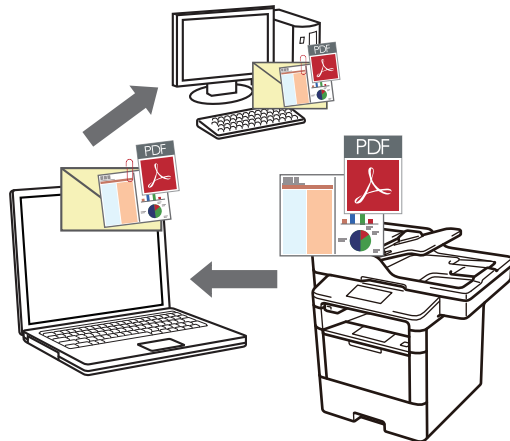
✓ 関連情報

- ControlCenter4 Advanced モードを使ってスキャンする (Windows®)

■ ホーム > スキャン > お使いのパソコンからスキャンする (Windows®) > ControlCenter4 Advanced モードを使ってスキャンする (Windows®) > ControlCenter4 Advanced モードを使用したスキャン to E メール添付 (Windows®)

ControlCenter4 Advanced モードを使用したスキャン to E メール添付 (Windows®)


パソコンの E メールソフトを起動し、スキャンしたデータを添付ファイルとして送信します。



- ControlCenter4 のモード設定で **Advanced モード**を選択します。
- スキャン to E メール添付機能は、Web メールサービスには対応していません。スキャン to イメージまたはスキャン to ファイル機能を使って、原稿や写真をスキャンして、パソコンに保存してください。保存したデータファイルを Web メールに添付してください。



パソコンの初期設定で起動するように指定されている E メールソフトにスキャンデータを送信します。

- 原稿をセットします。
- タスクトレイの  (ControlCenter4)アイコンをクリックし、**開く**をクリックします。
- スキャン**タブをクリックします。



- E メール添付**ボタンをクリックします。
スキャン設定ダイアログボックスが表示されます。

メール添付 - ControlCenter4

ファイル形式
PDF マルチページ (*.pdf)

ファイル名
CCE_000001.pdf 変更

保存先フォルダー
C:\Users\XXXXX\Pictures\ControlCenter4\Email

☐ プレスキャン

解像度
200 x 200 dpi

カラー設定
1677万色カラー

原稿サイズ
A4 210 x 297 mm (8.3 x 11.7 インチ)

ファイルサイズ優先度
小 (スピード) 大 (画品質)

明るさ
0

コントラスト
0

☐ 継続スキャン

☐ 2in1 IDカードスキャン

☐ 次回から表示しない

初期値 詳細設定 スキャン キャンセル ヘルプ

5. 必要に応じて、ファイル形式、ファイル名、保存先ファイルパス、解像度、およびカラー設定等のスキャン設定を変更します。



- ファイル名を変更するには、**変更**をクリックします。
- 保存先フォルダー**を変更するには、フォルダーアイコンをクリックします。
- スキャンした画像のプレビューおよび設定を行うには、**プレスキャン**のチェックボックスにチェックを入れます。

6. **スキャン**をクリックします。

本製品でスキャン動作を開始します。パソコンの初期設定で起動するように指定されている E メールソフトが開き、スキャンされたデータを添付ファイルとして、メールの送信画面が表示されます。



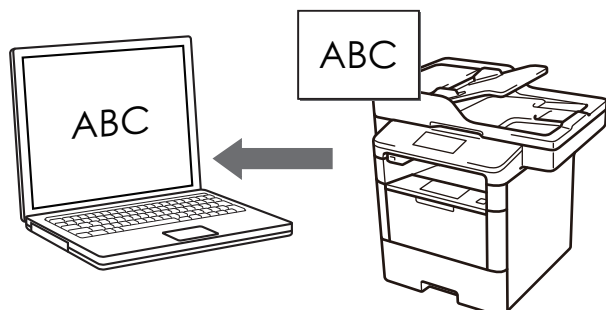
関連情報

- ControlCenter4 Advanced モードを使ってスキャンする (Windows®)


■ ホーム > スキャン > お使いのパソコンからスキャンする (Windows®) > ControlCenter4 Advanced モードを使ってスキャンする (Windows®) > ControlCenter4 Advanced モード (Windows) を使用したスキャン to 編集可能テキストファイル (OCR)

ControlCenter4 Advanced モード (Windows) を使用したスキャン to 編集可能テキストファイル (OCR)

本製品は、OCR（光学式文字認識）の技術を使って、スキャンした原稿の文字をテキストに変換することができます。テキスト編集アプリケーションを使ってこのテキストを編集できます。



- ControlCenter4 のモード設定で **Advanced モード** を選択します。

- 原稿をセットします。
- タスクトレイの  (ControlCenter4) アイコンをクリックし、**開く** をクリックします。
- スキャン** タブをクリックします。



- OCR** ボタンをクリックします。
スキャン設定ダイアログボックスが表示されます。

OCR - ControlCenter4

ファイル形式
テキストファイル (*.txt)

OCR言語
日本語

使用するアプリケーション
メモ帳

ファイル名
CCO_000001.txt 変更

保存先フォルダー
C:\Users\XXXXXX\Pictures\ControlCenter4\OCR

☐ プレスキャン

解像度
300 x 300 dpi

カラー設定
モノクロ

原稿サイズ
A4 210 x 297 mm (8.3 x 11.7 インチ)

明るさ
0

コントラスト
0

☐ 継続スキャン

☐ 2in1 IDカードスキャン

☐ 次回から表示しない

初期値 詳細設定 スキャン キャンセル ヘルプ

5. 必要に応じて、ファイル形式、ファイル名、保存先ファイルパス、解像度、およびカラー設定等のスキャン設定を変更します。



- ファイル名を変更するには、**変更**をクリックします。
- **保存先フォルダー**を変更するには、フォルダーアイコンをクリックします。
- スキャンした画像のプレビューおよび設定を行うには、**プレスキャン**のチェックボックスにチェックを入れます。

6. **スキャン**をクリックします。

本製品でスキャン動作を開始し、編集可能なテキストに変換されたデータを、設定したアプリケーションに送信します。



関連情報

- [ControlCenter4 Advanced モードを使ってスキャンする \(Windows®\)](#)

ControlCenter4 Advanced モードのスキャン設定 (Windows®)

設定	対応している機能			
	イメージ	OCR	E メール添付	ファイル
ファイル形式	○	○	○	○
使用するアプリケーション	○	○	-	-
OCR 言語	-	○	-	-
ファイル名	○	○	○	○
保存先 or 保存先フォルダー	○	○	○	○
保存先フォルダーを開く	-	-	-	○
スキャン毎に名前をつける	-	-	-	○
ファイルサイズ	○	-	○	○
プレスキャン	○	○	○	○
解像度	○	○	○	○
カラー設定	○	○	○	○
原稿サイズ	○	○	○	○
明るさ	○	○	○	○
コントラスト	○	○	○	○
継続スキャン	○	○	○	○
両面読取り	○	○	○	○
2in1 ID カードスキャン	○	○	○	○
詳細設定	○	○	○	○
初期値	○	○	○	○

ファイル形式

スキャンしたデータを保存するファイル形式を選択します。

イメージ、E メール添付、ファイルの場合

- Windows ビットマップ (*.bmp)
- JPEG (*.jpg) (写真をスキャンする場合、ほとんどのユーザーにお勧めします。)
- TIFF シングルページ (*.tif)
- TIFF マルチページ (*.tif)
- Portable Network Graphics (*.png)
- PDF シングルページ (*.pdf) (原稿をスキャンして共有する場合にお勧めします。)
- PDF マルチページ (*.pdf) (原稿をスキャンして共有する場合にお勧めします。)
- PDF/A シングルページ (*.pdf) (原稿をスキャンして共有する場合にお勧めします。)
- PDF/A マルチページ (*.pdf) (原稿をスキャンして共有する場合にお勧めします。)
- 高圧縮 PDF シングルページ (*.pdf)
- 高圧縮 PDF マルチページ (*.pdf)
- パスワード付 PDF シングルページ (*.pdf)
- パスワード付 PDF マルチページ (*.pdf)
- サーチャブル PDF シングルページ (*.pdf)

- **サーチャブル PDF マルチページ (*.pdf)**
- **XML Paper Specification (*.xps)** (XML Paper Specification は、Windows® 7、Windows® 8.1 および Windows® 10 で、または XML Paper Specification ファイルをサポートするアプリケーションを使用する場合に利用できます。)
- **Microsoft Office Word (*.docx)** (特定モデルのみ対応)
- **Microsoft Office PowerPoint (*.pptx)** (特定モデルのみ対応)

OCR の場合

- **テキストファイル (*.txt)**
- **リッチテキスト形式 (*.rtf)**
- **HTML (*.htm)**
- **サーチャブル PDF シングルページ (*.pdf)**
- **サーチャブル PDF マルチページ (*.pdf)**

使用するアプリケーション

スキャンしたデータを開くアプリケーションを選択します。

OCR 言語

OCR 言語を設定して、スキャンした原稿中のテキストの言語を照合します。

ファイル名

変更をクリックして、ファイル名の接頭辞を変更します。

保存先

フォルダーまたは **SharePoint** ボタンを選択して、スキャンした文書の保存先を指定します。

保存先フォルダー

フォルダーアイコンをクリックし、スキャンしたデータの保存先フォルダーを指定します。

保存先フォルダーを開く

スキャン後に自動的に保存先フォルダーを表示させる際に選択します。

スキャン毎に名前をつける

スキャンする度に、スキャンした画像の保存先を指定したい場合に選択します。

ファイルサイズ

スキャンしたデータのサイズを調節します。 **ファイルサイズ** のつまみを右または左に移動させてファイルサイズを変更します。

プレスキャン

スキャンする前に画像のプレビューを確認して不要な部分を切り取りたい場合は、**プレスキャン**を選択します。

解像度

解像度 のドロップダウンリストから、スキャンする時の解像度を選択します。高い解像度を選択すると、スキャンしたデータの画質は向上しますが、ファイルサイズが大きくなったり、スキャンするのに時間がかかります。

カラー設定

さまざまな色濃度の中から選択します。

- **自動**
どんなタイプの原稿にも使用できます。原稿に対して適切な色濃度が自動的に選択されます。
- **モノクロ**
文字原稿または線画に使用します。

- **グレー**

写真やグラフィックに使用します。(見た目を自然なグレーに似せるために、黒い点を一定の規則で配置させることで、実際にはグレーの点を使用せずに擬似的にグレー画像を作成する、誤差拡散という手法を使っています。)

- **256 階調グレー**

写真やグラフィックに使用します。最大で 256 段階の色調のグレーを使用して、より正確に細部を再現します。

- **1677 万色カラー**

最も正確に色を再現した画像を作成したい場合に適しています。最大で 1680 万色を使って画像をスキャンしますが、最も多くのメモリーが必要とされ、転送時間が最も長くなります。

原稿サイズ

原稿サイズのドロップダウンリストから原稿の正確なサイズを選択します。

- **1 to 2 (A4)**を選択した場合は、スキャンしたデータは 2 つの A5 サイズのデータに分割されます。

明るさ

つまみを右または左に移動させて**明るさ**レベルを設定し、データの明暗を調整します。スキャンしたデータが明るすぎる場合は、明るさレベルを下げて再度原稿をスキャンしてください。データが暗すぎる場合は、明るさレベルを上げて再度原稿をスキャンしてください。数値を入力して**明るさ**レベルを設定することも可能です。

コントラスト

つまみを右または左に移動させて**コントラスト**レベルの調整を行います。レベルを上げると画像の明暗が強調され、レベルを下げるとグレー部分をより詳細に見られます。数値を入力して**コントラスト**レベルを設定することも可能です。

継続スキャン

原稿台ガラスまたは ADF (自動原稿送り装置) から複数ページをスキャンするときに選択します (特定モデルのみ対応)。1 ページ目がスキャンされた後に、スキャンを続けるか終了するかを選びます。この方法を使うと、ADF (自動原稿送り装置) の上限を超えるページ数をスキャンすることが可能になります。

2in1 ID カードスキャン

運転免許証のようなカードの両面を 1 つのページにスキャンするときに、このチェックボックスにチェックを入れます。

詳細設定

詳細設定を行うには、カスタムスキャン設定ダイアログボックスで**詳細設定**ボタンをクリックします。

- **地色除去**

原稿の背景にある地色を取り除き、スキャンしたデータを見やすくします。強・中・弱の 3 つの設定から選びます。

(自動、256 階調グレー、および 1677 万色カラーのみ利用可能)

- **白紙除去**

スキャン結果から原稿の空白ページを取り除きます。

- **スキャン結果表示**

パソコン画面に、スキャンしたデータの総ページ数、および削除した白紙ページ数を表示させます。

- **ADF 傾き補正**

ADF(自動原稿送り装置)から原稿をスキャンする場合、原稿の歪みは本製品により自動的に修正されます。

初期値

すべての設定をお買い上げ時の状態に戻すときに選択します。



関連情報

- [ControlCenter4 Advanced モードを使ってスキャンする \(Windows®\)](#)

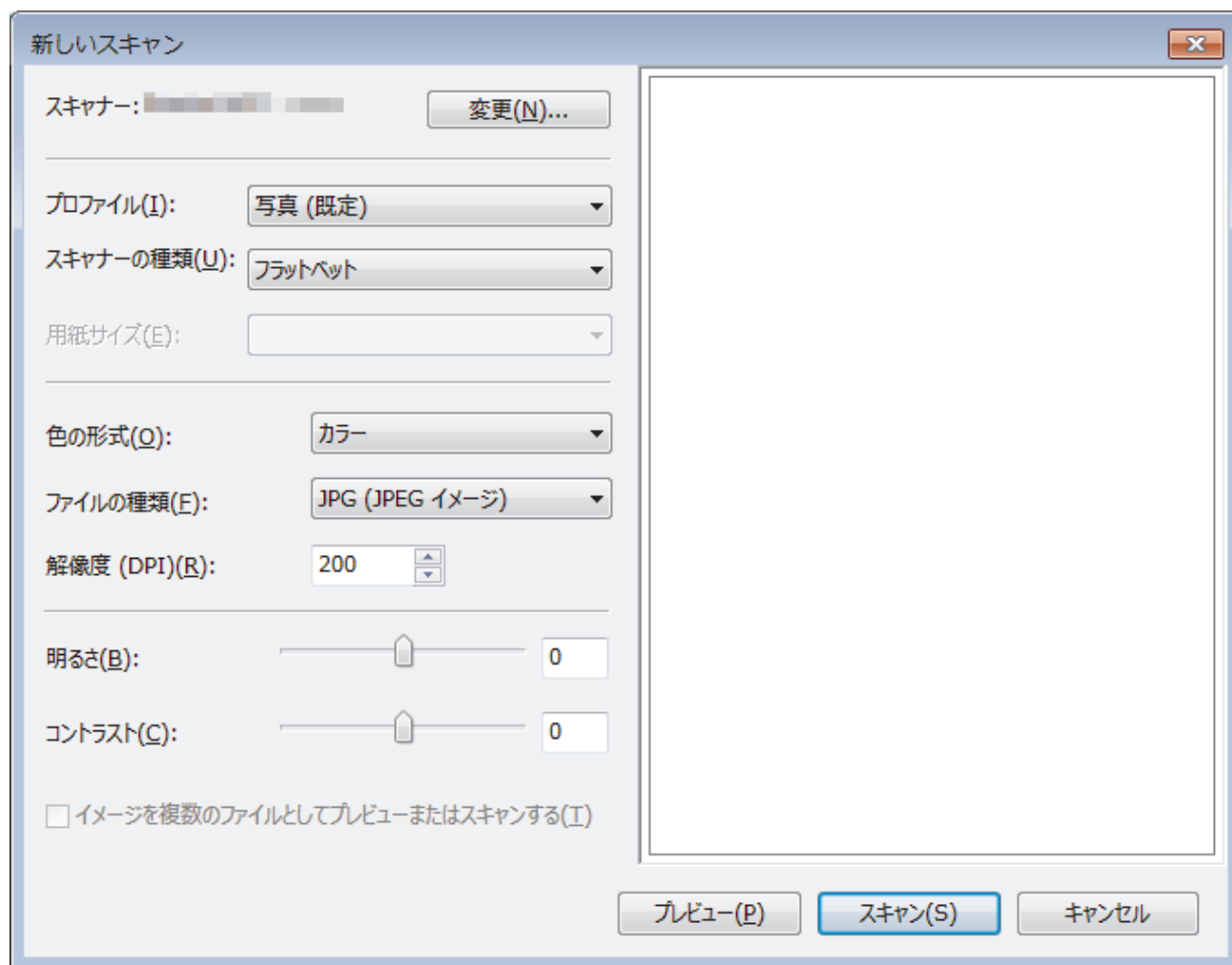
Windows® フォトギャラリー、Windows® FAX とスキャンを使ってスキャンする

Windows® フォトギャラリーや Windows® FAX とスキャンアプリケーションを使用してスキャンすることが可能です。

- これらのアプリケーションは、WIA スキャナードライバーを使用します。
- 原稿台ガラスから原稿をスキャンした場合は、スキャンするエリアを調整することが可能です。

1. 原稿をセットします。
2. スキャン用アプリケーションを起動します。 次のいずれかを行ってください。
 - （Windows® フォトギャラリー）
ファイル > カメラまたはスキャナーからの読み込み...をクリックします。
 - （Windows® FAX とスキャン）
新しいスキャンをクリックします。
3. 接続している本製品のモデル名を選択します。
4. **読み込み**または **OK** をクリックします。

新しいスキャンダイアログボックスが表示されます。



5. 必要に応じて、ダイアログボックスの設定を調整します。

スキャナーの解像度は、最大 1200dpi に設定可能です。さらに高解像度でスキャンしたい場合は、**KONICA MINOLTA Utilities** の **Scanner Utility** ソフトウェアを使用してください。

両面スキャンを行う場合は、**スキャナーの種類**で**フィーダー（両面スキャン）**を選択します。

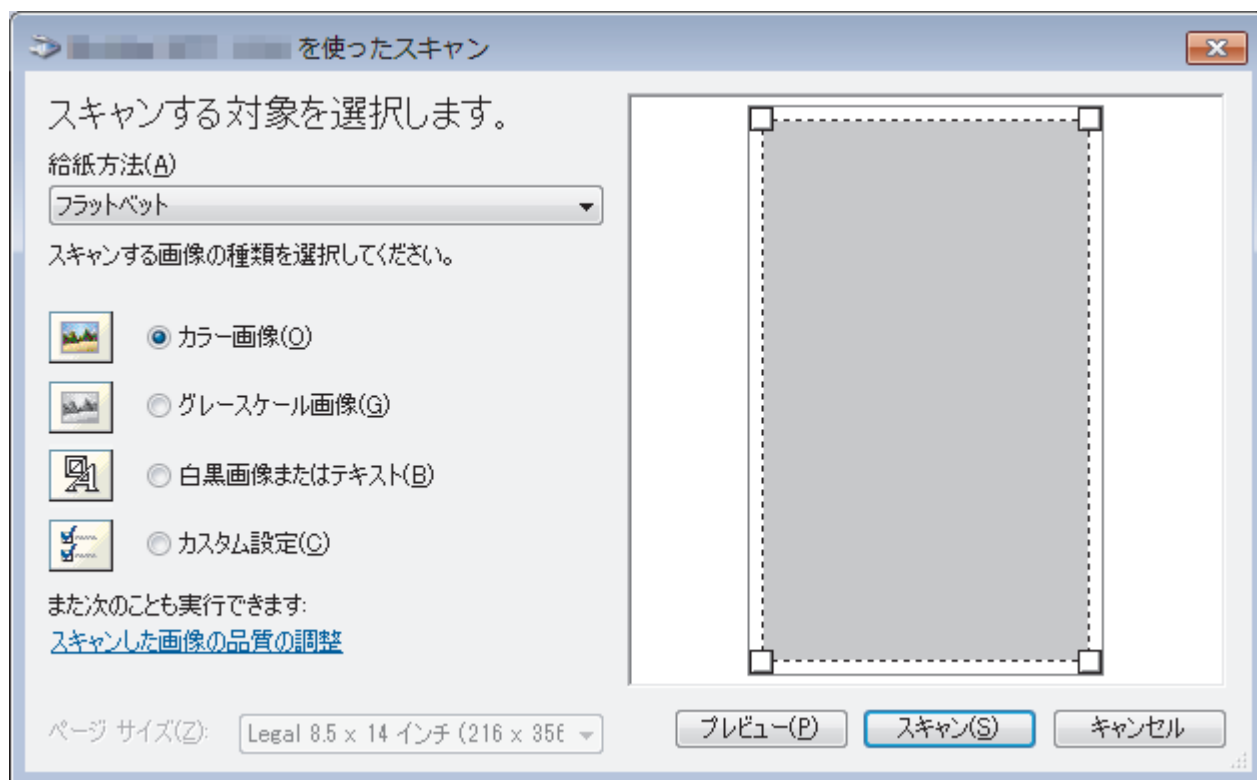
-
6. **スキャン**をクリックします。
本製品がスキャン動作を開始します。



関連情報

- [お使いのパソコンからスキャンする \(Windows®\)](#)
 - [WIA ドライバー設定\(Windows®\)](#)
-

WIA ドライバー設定(Windows®)



給紙方法

ドロップダウンリストからドキュメント フィーダーまたはフラットベッドを選択します。

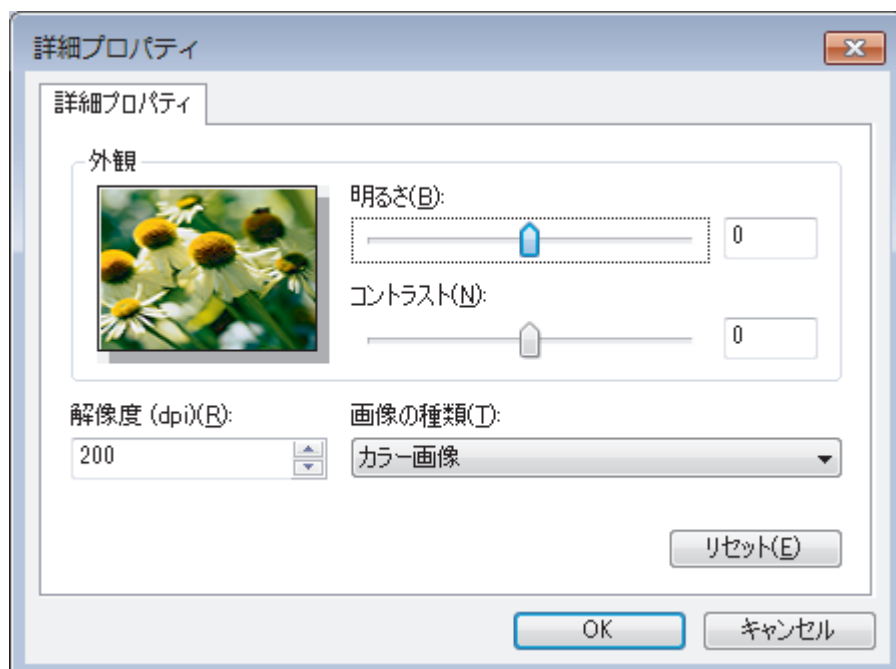
写真のタイプ (画像のタイプ)

スキャンする原稿の種類にあわせて、カラー画像、グレースケール画像、白黒画像またはテキスト、またはカスタム設定を選択します。

詳細設定を変更するには、スキャンした画像の品質の調整リンクをクリックします。

ページサイズ

ページサイズは、給紙方法としてドキュメント フィーダーを選択した場合にのみ利用可能です。



明るさ

つまみを右または左にドラッグして**明るさ**レベルを設定し、画像の明暗を調整します。スキャンした画像が明るすぎる場合は、明るさレベルを下げてから再度原稿をスキャンしてください。画像が暗すぎる場合は、明るさレベルを上げてから再度原稿をスキャンしてください。

コントラスト

つまみを右または左に移動させて、**コントラスト**レベルの調整を行います。レベルを上げると画像の明暗が強調され、レベルを下げるとグレー部分をより詳細に見られます。数値を入力することでコントラストレベルを設定することも可能です。

解像度 (dpi)

解像度 (dpi) から、スキャンの解像度を選択します。高い解像度を選択すると、スキャンしたデータの画質は向上しますが、ファイルサイズが大きくなったり、スキャンするのに時間がかかります。



関連情報

- [Windows® フォトギャラリー](#)、[Windows® FAX](#) とスキャンを使ってスキャンする
-

お使いのパソコンからスキャンする (Mac)

お使いの Mac を使用して、写真や文章を本製品でスキャンします。弊社から提供しているソフトウェアを使用します。

- [iPrint&Scan を使ってスキャンする\(Mac\)](#)

iPrint&Scan を使ってスキャンする(Mac)

iPrint&Scan を使ってスキャンし、スキャンしたデータを指定のファイル形式で保存したり指定のアプリケーションで開くことができます。

1. **Finder** メニューバーで**移動 > アプリケーション > KONICA MINOLTA** フォルダをクリックし、**iPrint&Scan** アイコンをダブルクリックして起動します。
2. **製品を選択**をクリックし、画面の指示に従って本製品を選択します。
3. 本製品に原稿をセットします。
4. **スキャン**をクリックします。
5. 原稿サイズ・カラー設定・解像度を原稿に合わせて変更します。原稿の補正や画像の調整をする場合は、**すべての設定**をクリックして設定します。



高い解像度を選択すると、スキャンしたデータの画質は向上しますが、ファイルサイズが大きくなったり、スキャンするのに時間がかかります。

6. **スキャン**をクリックします。
7. 原稿がスキャンされます。続けて原稿を読み取る場合は、本製品に原稿をセットしてから**追加スキャン**をクリックします。
8. すべての原稿をスキャンしたら、**保存/共有**から保存先を選択します。
画面に従って設定してください。



関連情報

- ・ [お使いのパソコンからスキャンする \(Mac\)](#)

■ ウェブブラウザを使用してスキャン設定を行う


- ・ ウェブブラウザを使用してスキャンジョブの E メールレポートを設定する

ウェブブラウザを使用してスキャンジョブの E メールレポートを設定する

原稿をスキャンすると、本製品はスキャンジョブの E メールレポートを、登録されている E メールアドレスに自動的に送信します。

1. ウェブブラウザを起動します。

ブラウザのアドレス欄に「http://製品の IP アドレス」を入力します（「製品の IP アドレス」の部分には本製品の IP アドレスまたはプリントサーバー名を入力します）。例：http://192.168.1.2

パスワード設定をしている場合は、そのパスワードを入力し、を押します。初期パスワードは、initpass です。

2. **スキャン**タブをクリックします。
3. 左側にあるナビゲーションバーの**スキャン通知レポート**メニューをクリックします。
4. **管理者メールアドレス**欄で、E-mail アドレスを入力します。
5. 利用するスキャン機能に対して**オン**を選択し、スキャンジョブの E メールレポートが送信されるようにします。
6. **OK** をクリックします。

✓ 関連情報

- [ウェブブラウザを使用してスキャン設定を行う](#)

PC-FAX

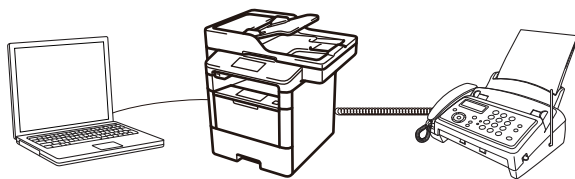
- [Windows®用 PC-FAX](#)

Windows®用 PC-FAX

- [PC-FAX の概要\(Windows®\)](#)
- [PC-FAX を使ってファクスを送信する\(Windows®\)](#)
- [パソコンでファクスを受信する\(Windows®\)](#)

PC-FAX の概要(Windows®)

本製品の PC-FAX ソフトウェアを使用して、印刷せずにパソコンから直接ファクス（モノクロのみ）を送信します。この機能により、用紙の消費を抑えたり、時間を節約したりすることができます。



- [PC-FAX の設定を行う\(Windows®\)](#)
- [PC-FAX のアドレス帳を設定する \(Windows®\)](#)

PC-FAX の設定を行う(Windows®)

PC-FAX を使用してファクスを送信する前に、**PC-FAX 設定**ダイアログボックスの各タブにある送信設定をカスタマイズします。


1. 次のいずれかを行ってください。

- (Windows® 7)

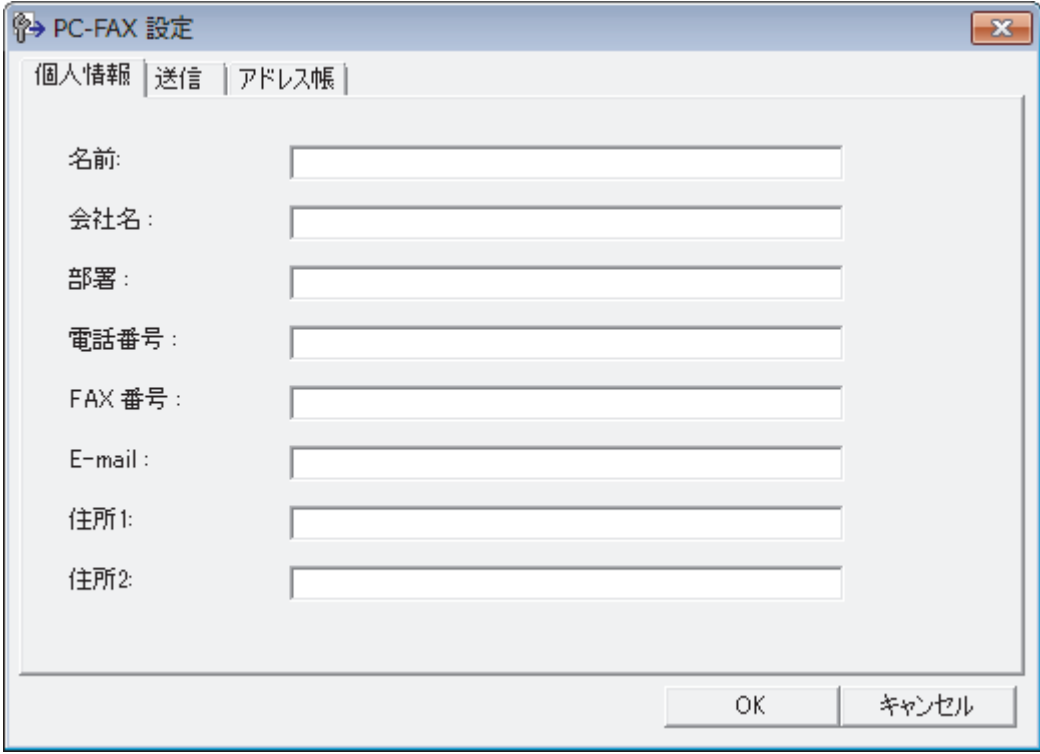
 **(スタート) > すべてのプログラム > KONICA MINOLTA > KONICA MINOLTA Utilities** をクリックします。

ドロップダウンリストをクリックして、お使いの機器のモデル名を選択します（未選択の場合）。左ナビゲーションバーの**パソコンからファクスを送受信する**をクリックして、**PC-FAX 送信設定**をクリックします。

- (Windows® 8.1 および Windows® 10)

 **(KONICA MINOLTA Utilities)**を起動し、ドロップダウンリストをクリックして、本機器のモデル名を選択します（未選択の場合）。左ナビゲーションバーの**パソコンからファクスを送受信する**をクリックして、**PC-FAX 送信設定**をクリックします。

PC-FAX 設定ダイアログボックスが表示されます。



2. 次のいずれかを行ってください。

- **個人情報**タブをクリックし、各欄にユーザー情報を入力します。



各 Microsoft®アカウントでは、ファクスのヘッダーや送付書に、カスタマイズした**個人情報**画面をそれぞれ設定することができます。

- **送信**タブをクリックし、必要に応じて、外線にアクセスするために必要な番号を**外線番号**に入力します。**ヘッダー情報追加**のチェックボックスを選択し、ヘッダー情報を含めます。
- **アドレス帳**タブをクリックし、**使用するアドレス帳**のドロップダウンリストから、PC-FAX に使いたいアドレス帳を選択します。

3. **OK** をクリックします。



関連情報

- [PC-FAX の概要\(Windows®\)](#)

PC-FAX のアドレス帳を設定する (Windows®)

PC-FAX アドレス帳で、メンバーやグループを追加、編集、または削除などのカスタマイズを行います。

- アドレス帳にメンバーを追加する(Windows®)
- アドレス帳にグループを作成する (Windows®)
- メンバーまたはグループ情報を編集する(Windows®)
- メンバーまたはグループを削除する (Windows®)
- アドレス帳をエクスポートする (Windows®)
- アドレス帳に情報をインポートする(Windows®)

アドレス帳にメンバーを追加する(Windows®)

本製品の PC-FAX ソフトウェアを使ってファクスを送信したい場合は、新規のメンバーおよびそのメンバーのファクス情報を PC-FAX アドレス帳に追加します。


1. 次のいずれかを行ってください。

- (Windows® 7)

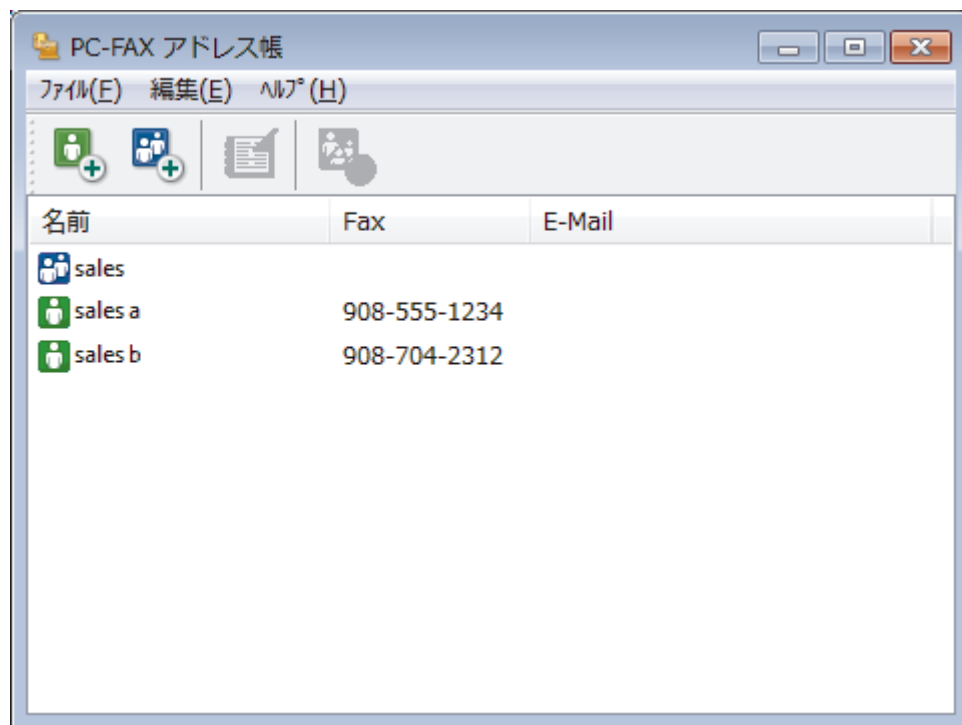
 (スタート) > すべてのプログラム > KONICA MINOLTA > KONICA MINOLTA Utilities をクリックします。


ドロップダウンリストをクリックして、本製品のモデル名を選択します (未選択の場合)。左ナビゲーションバーの **パソコンからファクスを送受信する** をクリックして、**PC-FAX 送信アドレス帳** をクリックします。

- (Windows® 8.1 および Windows® 10)

 (KONICA MINOLTA Utilities) を起動し、ドロップダウンリストをクリックして、本製品のモデル名を選択します (未選択の場合)。左ナビゲーションバーの **パソコンからファクスを送受信する** をクリックして、**PC-FAX 送信アドレス帳** をクリックします。


PC-FAX アドレス帳ダイアログボックスが表示されます。



2.  をクリックします。

PC-FAX アドレス帳 メンバー設定ダイアログボックスが表示されます。

PC-FAX アドレス帳 メンバー設定

名前(N):  敬称(T):

会社名(O):

部署(D): 役職(J):

番地(S):

市町村(C): 都道府県(V):

郵便番号(Z): 国/地域(R):

勤務先電話番号(B): 自宅電話番号(H):

ファクス(F): 携帯電話(P):

E-Mail(E):

決定 キャンセル

3. 対応する欄にメンバーの情報を入力します。**名前**のみ必須です。



電話番号およびファクス番号は、必ず市外局番から登録してください。ナンバー・ディスプレイの名前や着信履歴が正しく表示されない場合があります。

4. **決定**をクリックします。



関連情報

- PC-FAX のアドレス帳を設定する (Windows®)

アドレス帳にグループを作成する (Windows®)

グループを作成して、PC-FAX を複数の受信者に同報送信します。


1. 次のいずれかを行ってください。

- (Windows® 7)

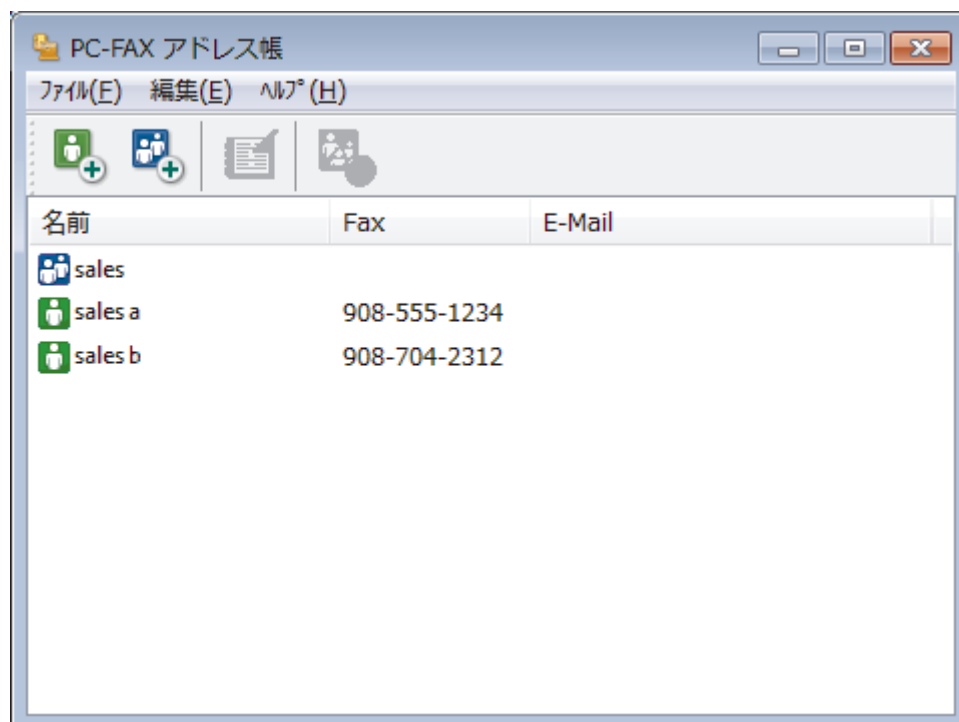
 (スタート) > すべてのプログラム > KONICA MINOLTA > KONICA MINOLTA Utilities をクリックします。

ドロップダウンリストをクリックして、本製品のモデル名を選択します (未選択の場合)。左ナビゲーションバーの**パソコンからファクスを送受信する**をクリックして、**PC-FAX 送信アドレス帳**をクリックします。

- (Windows® 8.1 および Windows® 10)

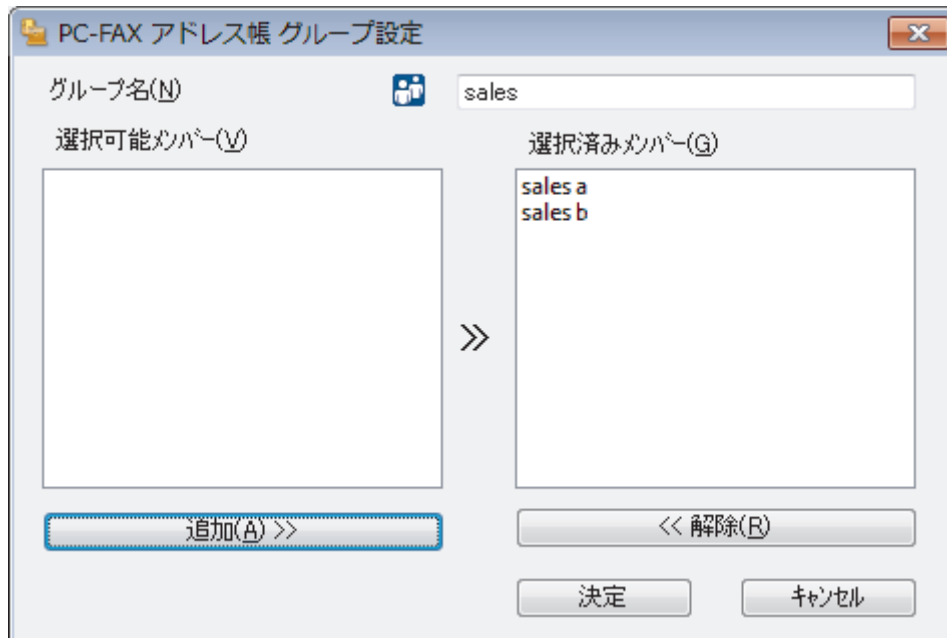
 (KONICA MINOLTA Utilities)を起動し、ドロップダウンリストをクリックして、本製品のモデル名を選択します (未選択の場合)。左ナビゲーションバーの**パソコンからファクスを送受信する**をクリックして、**PC-FAX 送信アドレス帳**をクリックします。

PC-FAX アドレス帳ダイアログボックスが表示されます。



2.  をクリックします。

PC-FAX アドレス帳 **グループ設定**ダイアログボックスが表示されます。



3. **グループ名**に、新しいグループの名前を入力します。
4. **選択可能メンバー**内からグループに含める名前を選択し、**追加**をクリックします。
グループに追加されたメンバーは、**選択済みメンバー**に表示されます。
5. 設定の完了後、**決定**をクリックします。



各グループには、最大 50 名のメンバーを含めることができます。



関連情報

- [PC-FAX のアドレス帳を設定する \(Windows®\)](#)

メンバーまたはグループ情報を編集する(Windows®)

1. 次のいずれかを行ってください。

- (Windows® 7)



(スタート) > すべてのプログラム > KONICA MINOLTA > KONICA MINOLTA Utilities をクリックします。

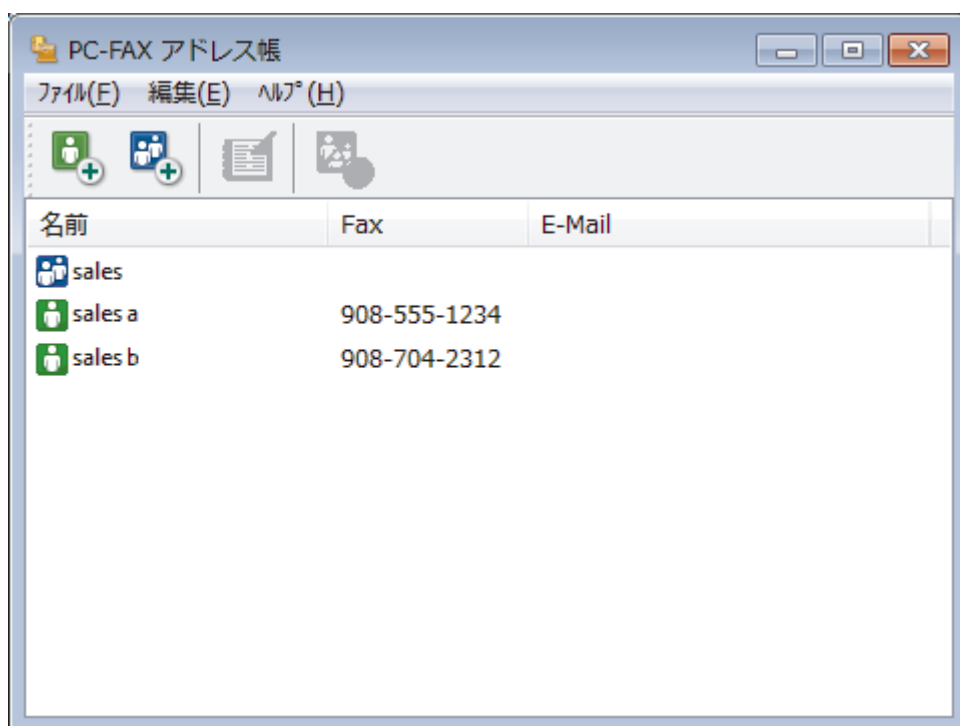
ドロップダウンリストをクリックして、本製品のモデル名を選択します (未選択の場合)。左ナビゲーションバーのパソコンからファクスを送受信するをクリックして、PC-FAX 送信アドレス帳をクリックします。


- (Windows® 8.1 および Windows® 10)



(KONICA MINOLTA Utilities)を起動し、ドロップダウンリストをクリックして、本製品のモデル名を選択します (未選択の場合)。左ナビゲーションバーのパソコンからファクスを送受信するをクリックして、PC-FAX 送信アドレス帳をクリックします。

PC-FAX アドレス帳ダイアログボックスが表示されます。



2. 編集したいメンバーまたはグループを選択します。
3.  (詳細情報) をクリックします。
4. メンバーまたはグループ情報を変更します。
5. 決定をクリックします。



関連情報

- PC-FAX のアドレス帳を設定する (Windows®)

メンバーまたはグループを削除する (Windows®)


1. 次のいずれかを行ってください。

- (Windows® 7)

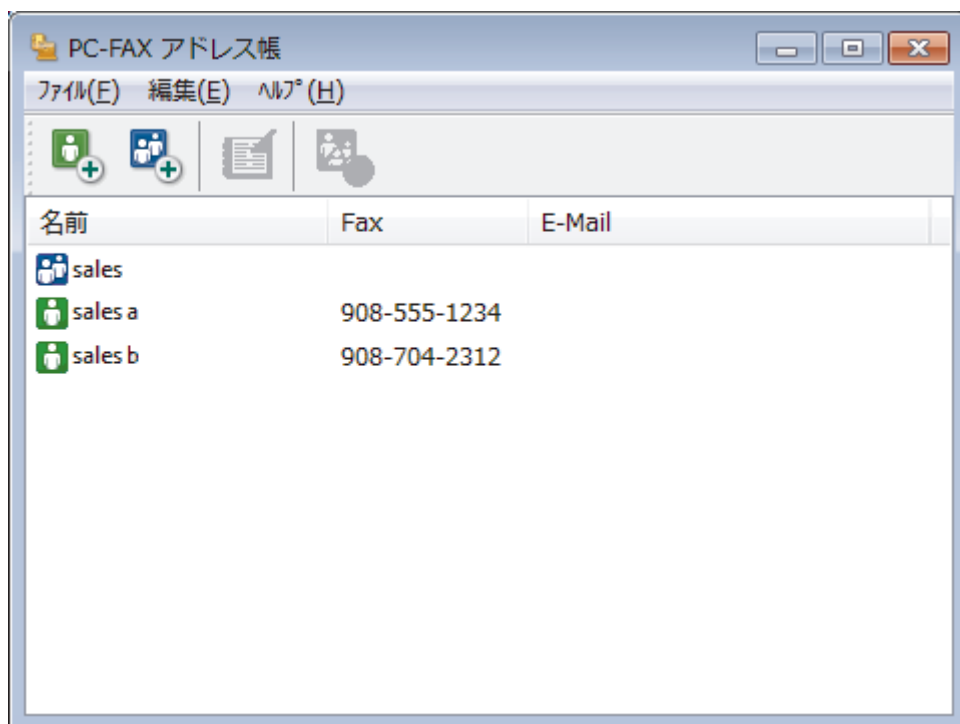
 (スタート) > すべてのプログラム > KONICA MINOLTA > KONICA MINOLTA Utilities をクリックします。

ドロップダウンリストをクリックして、本製品のモデル名を選択します (未選択の場合)。左ナビゲーションバーのパソコンからファクスを送受信するをクリックして、PC-FAX 送信アドレス帳をクリックします。


- (Windows® 8.1 および Windows® 10)

 (KONICA MINOLTA Utilities)を起動し、ドロップダウンリストをクリックして、本製品のモデル名を選択します (未選択の場合)。左ナビゲーションバーのパソコンからファクスを送受信するをクリックして、PC-FAX 送信アドレス帳をクリックします。

PC-FAX アドレス帳ダイアログボックスが表示されます。



2. 削除したいメンバーまたはグループを選択します。

3.  (削除) をクリックします。

4. 確認ダイアログボックスが表示されたら、OK をクリックします。

✓ 関連情報

- PC-FAX のアドレス帳を設定する (Windows®)

アドレス帳をエクスポートする (Windows®)

アドレス帳を、ASCII テキストファイル (*.csv)、vCard (電子名刺)、またはリモートセットアップダイアルデータとしてエクスポートし、お使いのパソコンに保存することができます。

- **PC-FAX アドレス帳データ**をエクスポートしても、グループ設定はエクスポートできません。

1. 次のいずれかを行ってください。

- (Windows® 7)



(スタート) > すべてのプログラム > KONICA MINOLTA > KONICA MINOLTA Utilities をクリックします。

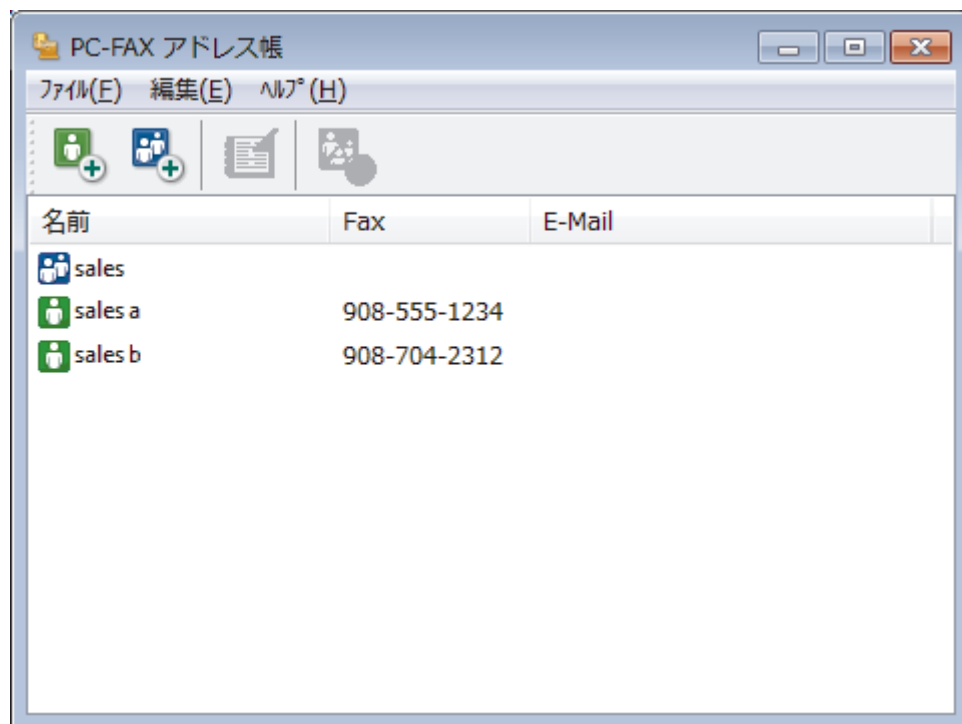
ドロップダウンリストをクリックして、本製品のモデル名を選択します (未選択の場合)。左ナビゲーションバーの**パソコンからファクスを送受信する**をクリックして、**PC-FAX 送信アドレス帳**をクリックします。

- (Windows® 8.1 および Windows® 10)



(KONICA MINOLTA Utilities)を起動し、ドロップダウンリストをクリックして、本製品のモデル名を選択します (未選択の場合)。左ナビゲーションバーの**パソコンからファクスを送受信する**をクリックして、**PC-FAX 送信アドレス帳**をクリックします。

PC-FAX アドレス帳ダイアログボックスが表示されます。



2. **ファイル**メニューをクリックして、**エクスポート**を選択します。

3. 以下のいずれかを選択してください。

- **テキストファイル**

項目選択ダイアログボックスが表示されます。手順 4 に進みます。

- **vCard**

選択する前に、アドレス帳からエクスポートするメンバーを指定する必要があります。

vCard の保存先フォルダーを開き、**ファイル名**にファイル名を入力して、**保存**をクリックします。

- **リモートセットアップダイアルデータ**

データの保存先フォルダーを開き、**ファイル名**にファイル名を入力して、**保存**をクリックします。

4. **選択可能項目**で、エクスポートするデータを選択し、**追加**をクリックします。



表示する順に項目を選択して追加します。

5. ASCII ファイルにエクスポートする場合、**区切り文字**で、**タブ**または**コンマ**を選択して、データフィールドを分割します。
6. **決定**をクリックします。
7. データの保存先のパソコンのフォルダーを開き、ファイル名を入力して、**保存**をクリックします。



関連情報

- PC-FAX のアドレス帳を設定する (Windows®)

アドレス帳に情報をインポートする(Windows®)

ASCII テキストファイル(*.csv)、vCard (電子名刺)、またはリモートセットアップダイアルデータを、お使いのアドレス帳にインポートすることができます。


1. 次のいずれかを行ってください。

- (Windows® 7)

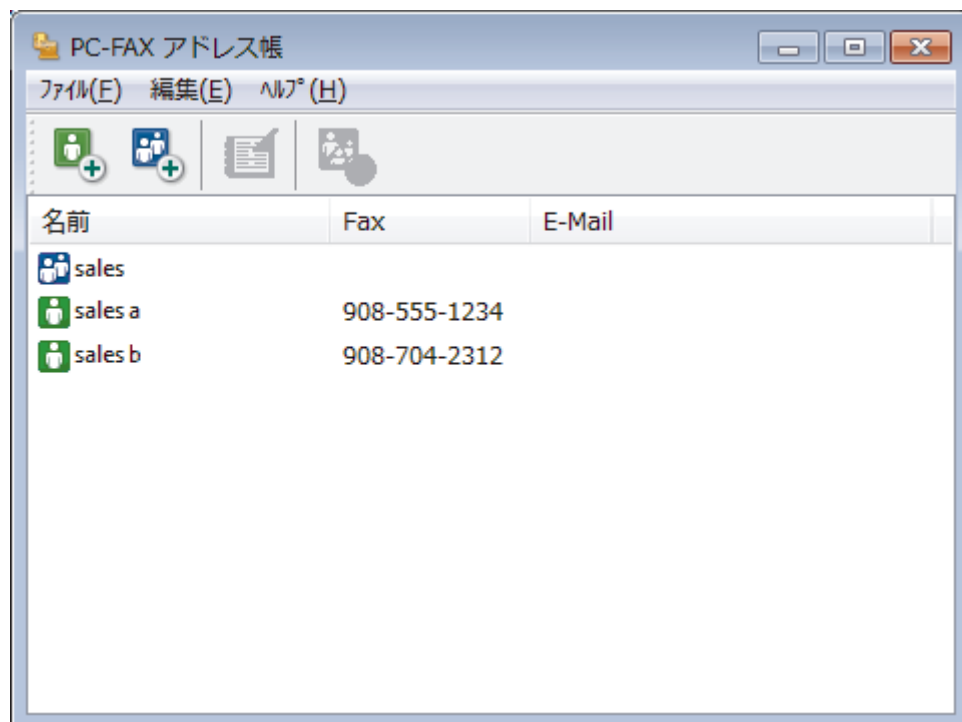
 (スタート) > すべてのプログラム > KONICA MINOLTA > KONICA MINOLTA Utilities をクリックします。

ドロップダウンリストをクリックして、本製品のモデル名を選択します (未選択の場合)。左ナビゲーションバーのパソコンからファクスを送受信するをクリックして、PC-FAX 送信アドレス帳をクリックします。

- (Windows® 8.1 および Windows® 10)

 (KONICA MINOLTA Utilities)を起動し、ドロップダウンリストをクリックして、本製品のモデル名を選択します (未選択の場合)。左ナビゲーションバーのパソコンからファクスを送受信するをクリックして、PC-FAX 送信アドレス帳をクリックします。

PC-FAX アドレス帳ダイアログボックスが表示されます。



2. ファイルメニューをクリックし、インポートを選択します。

3. 以下のいずれかを選択してください。

- テキストファイル

項目選択のダイアログボックスが表示されます。手順 4 に進みます。

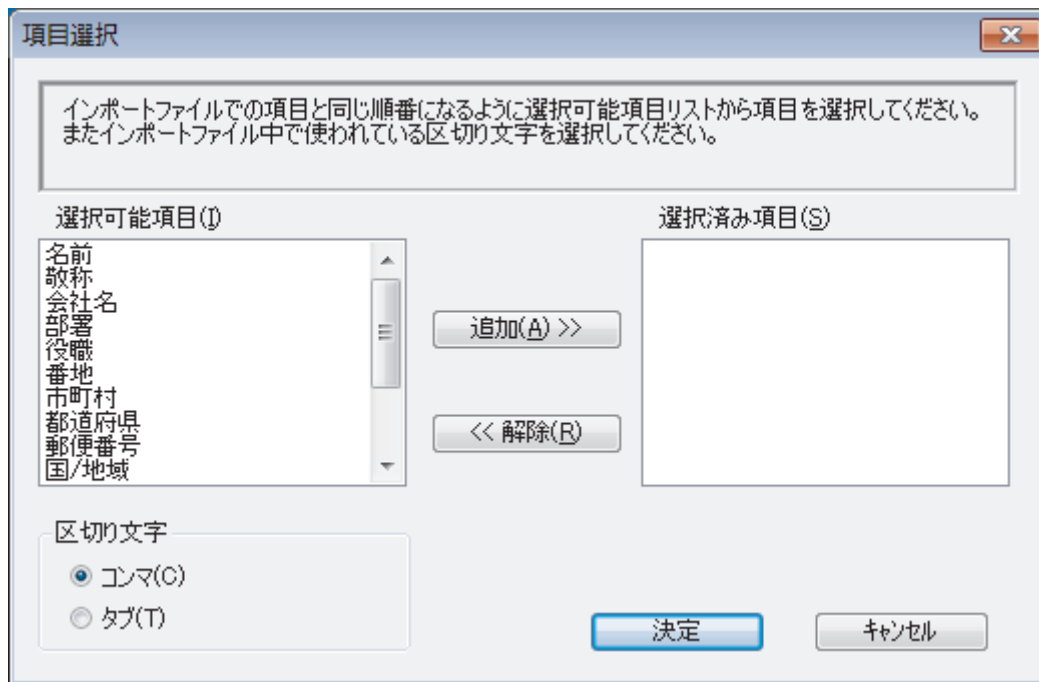
- vCard

手順 7 に進みます。

- リモートセットアップダイアルデータ

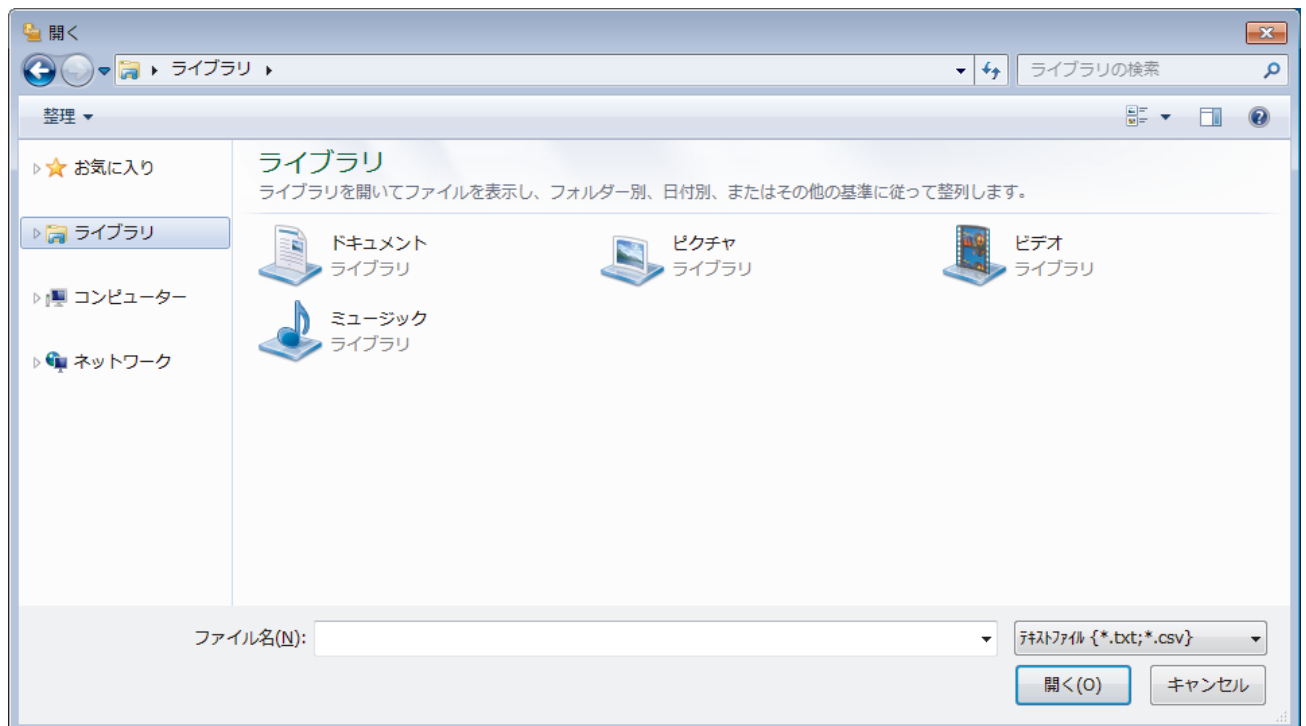
手順 7 に進みます。

4. 選択可能項目で、インポートしたいデータを選択し、追加をクリックします。



選択可能項目から、インポートするテキストファイルの並びと同じ順番で追加してください。

5. ASCII ファイルをインポートする場合、**区切り文字**で**タブ**または**コンマ**を選択してデータフィールドを区切ります。
6. **決定**をクリックします。
7. データをインポートしたいフォルダーを選択し、ファイル名を入力して**開く**をクリックします。



関連情報

- PC-FAX のアドレス帳を設定する (Windows®)

PC-FAX を使ってファクスを送信する(Windows®)


PC-FAX はモノクロのファクスにのみ対応しています。元のデータがカラーで、かつ受信側のファクス機がカラー対応のファクスであったとしても、モノクロのファクスが送信されます。

1. パソコン上のアプリケーションでファイルを作成します。
2. アプリケーションの印刷メニューを選択します。
3. プリンターとして **KONICA MINOLTA XXXX PC-FAX** (XXXX はお使いのモデル名) を選択し、印刷操作を完了させます。


PC-FAX のダイアログボックスが表示されます。





4. 以下のいずれかの方法でファクス番号を入力します。
 - ダイヤルパッドの数字をクリックして番号を入力し、**送信先追加**をクリックします。

 **ダイヤル制限機能**のチェックボックスを選択した場合は、確認用ダイアログボックスが表示され、キーボードを使ってファクス番号を再入力することが求められます。この機能により、送信先の間違いを防ぐことができます。

- **アドレス帳**ボタンをクリックし、アドレス帳からメンバーまたはグループを設定します。

 間違った場合は、**全削除**をクリックすれば入力した項目をすべて削除できます。

5. 送付書を含める場合は、**送付書使用**のチェックボックスにチェックを入れます。  をクリックして送付書の作成や編集をすることもできます。
6. **送信**をクリックしてファクスを送信します。

- 
- ファクス送信を中止するときは、**キャンセル**をクリックします。
 - 再ダイヤルするときは、**再ダイヤル**をクリックして送信したい番号を表示し、**送信**をクリックします。

✓ 関連情報

- Windows®用 PC-FAX

パソコンでファクスを受信する(Windows®)

本製品の PC-FAX ソフトウェアを使って、パソコンでファクスを受信し、確認して、必要な場合には印刷することができます。



- PC-FAX 受信を使ってファクスを受信する(Windows®)

PC-FAX 受信を使ってファクスを受信する(Windows®)

PC-FAX 受信ソフトウェアにより、パソコンで受信したファクスの閲覧や保存ができます。ソフトウェアとプリンタードライバをインストールする際に、PC-FAX 受信ソフトウェアもインストールされます。

- PC-FAX 受信機能は、モノクロのファクスにのみ対応しています。

パソコンの電源を切っていても、本製品は継続してファクスを受信し、メモリーに保存します。保存されたファクスの数が本製品の画面に表示されます。アプリを起動すると、本製品が受信したファクスをまとめてパソコンに転送します。ファクスがパソコンに送信される前、もしくはパソコンの電源を切る前に、ファクスを印刷したい場合は、バックアップ印刷オプションを有効にします。バックアップ印刷は、本製品から設定できます。



関連情報

- [パソコンでファクスを受信する\(Windows®\)](#)
 - [パソコンで本製品の PC-FAX 受信を起動する \(Windows®\)](#)
 - [受信したファクスを確認する\(Windows®\)](#)

パソコンで本製品の PC-FAX 受信を起動する (Windows®)



パソコン起動時に起動するのチェックボックスを選択しておく、パソコンを起動したときに、ソフトウェアが同時に起動し、ファクスを転送します。

1. 以下のいずれかを行ってください。

- (Windows® 7)



(スタート) > すべてのプログラム > KONICA MINOLTA > KONICA MINOLTA Utilities をクリックします。


モデル名が選択されていない場合は、ドロップダウンリストをクリックして、本製品のモデル名を選択します。左ナビゲーションバーのパソコンからファクスを送受信するをクリックし、PC-FAX 受信を起動をクリックします。

- (Windows® 8.1 および Windows® 10)



(KONICA MINOLTA Utilities) を起動し、モデル名が選択されていない場合は、ドロップダウンリストをクリックして、本製品のモデル名を選択します。左ナビゲーションバーのパソコンからファクスを送受信するをクリックし、PC-FAX 受信を起動をクリックします。

2. メッセージを確認して、Yes をクリックします。

PC ファクス受信画面が表示されます。  (待機中) アイコンがパソコンのタスクトレイに表示されます。



関連情報

- PC-FAX 受信を使ってファクスを受信する(Windows®)
 - PC-FAX 受信を設定する(Windows®)
 - PC-FAX 受信を行う製品を登録する (Windows®)

■ ホーム > PC-FAX > Windows®用 PC-FAX > パソコンでファクスを受信する(Windows®) > PC-FAX 受信を使ってファクスを受信する(Windows®) > パソコンで本製品の PC-FAX 受信を起動する (Windows®) > PC-FAX 受信を設定する(Windows®)

PC-FAX 受信を設定する(Windows®)

1. お使いのパソコンで、タスクトレイの  (待機中) アイコンをダブルクリックします。

PC ファクス受信画面が表示されます。

2. 設定をクリックします。
3. 必要に応じて設定してください。

起動

Windows®の起動時に、PC-FAX 受信が自動的に起動されるよう設定します。

保存

受信した PC-FAX の保存先や保存形式を選択します。

アップロード先

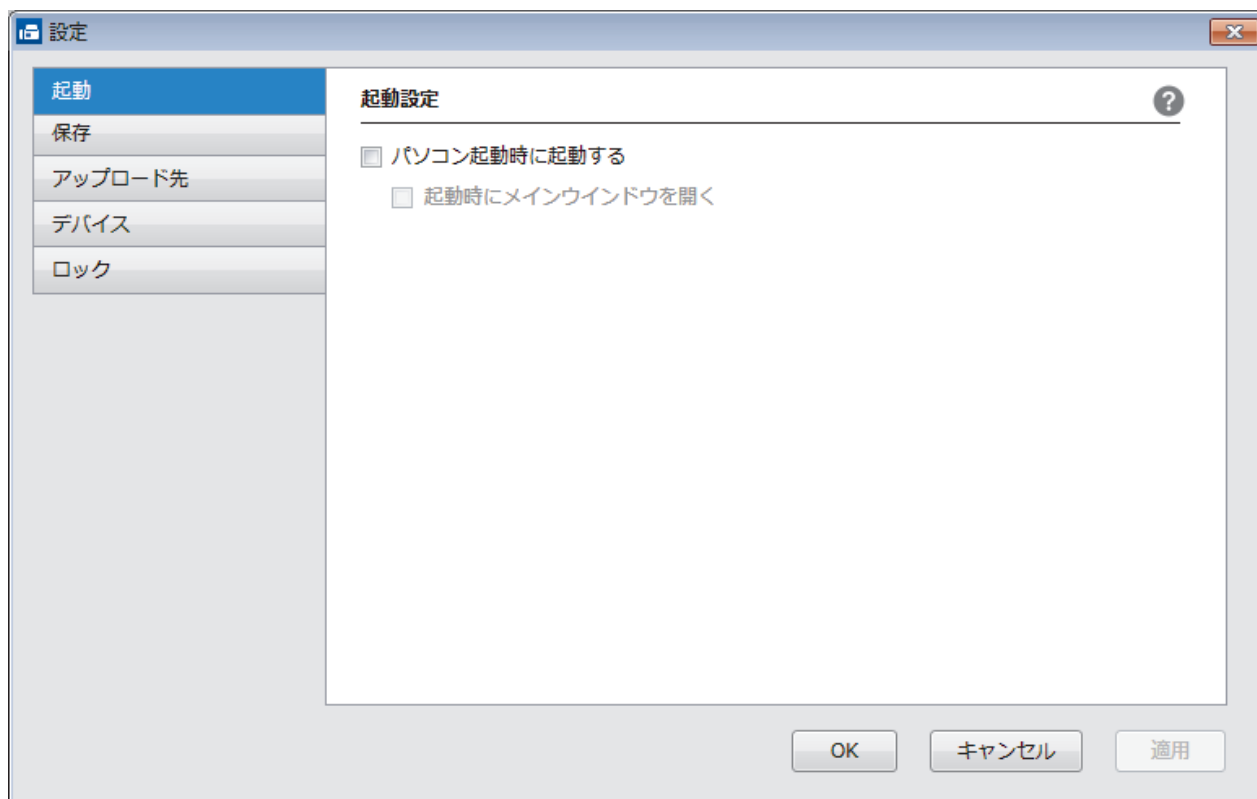
SharePoint®サーバーへのパスを設定し、アップロードの自動または手動を選択します。(管理者のみ利用可能)

デバイス

PC-FAX を受信したい製品を設定します。

ロック (管理者のみ利用可能)

管理者権限の無いユーザーに対して、設定を制限することができます。



4. OK をクリックします。



関連情報

- パソコンで本製品の PC-FAX 受信を起動する (Windows®)

▲ホーム > PC-FAX > Windows®用 PC-FAX > パソコンでファクスを受信する(Windows®) > PC-FAX 受信を使ってファクスを受信する(Windows®) > パソコンで本製品の PC-FAX 受信を起動する (Windows®) > PC-FAX 受信を行う製品を登録する (Windows®)

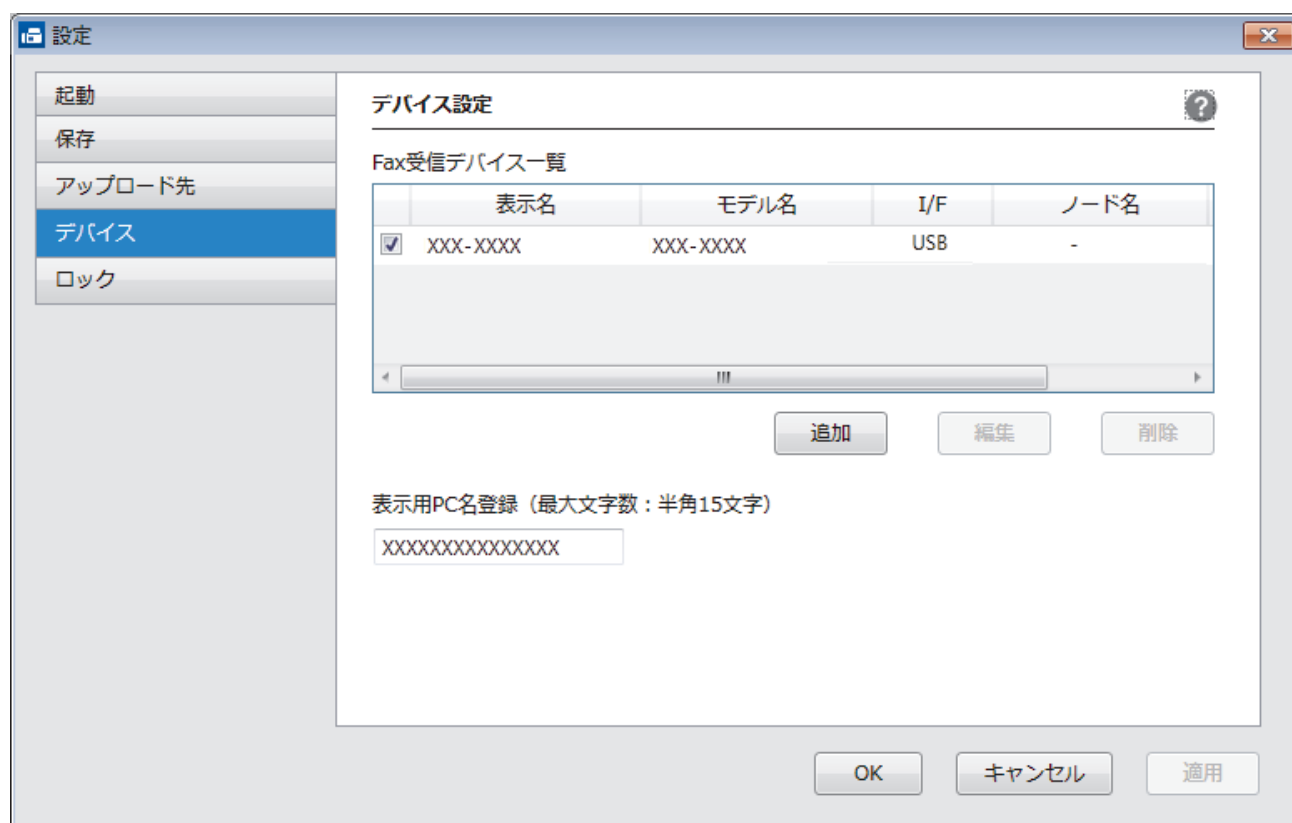
PC-FAX 受信を行う製品を登録する (Windows®)

- 本製品のプリンタードライバーをネットワークユーザー用の指示に従って Drivers & Utilities CD からインストールした場合、本製品はお使いのネットワーク上ですでに設定されています。

- お使いのパソコンで、タスクトレイの  (待機中) アイコンをダブルクリックします。

PC ファクス受信画面が表示されます。

- 設定をクリックします。
- デバイス > 追加をクリックします。



- 本製品の追加方法を選択します。

自動検索結果から選択してデバイスを追加

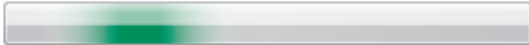
使用可能な製品が表示されます。リストから本製品を選択します。OK をクリックします。

IP アドレスを入力してデバイスを追加

本製品の IP アドレスを IP アドレスに入力して、OK をクリックします。

追加

☒ 自動検索結果から選択してデバイスを追加 再検索

モデル名	I/F	ノード名	IPアドレス	ロケーション情報
				

☐ IPアドレスを入力してデバイスを追加

IPアドレス

OK キャンセル




5. 本製品の画面に表示されるパソコン名を変更するには、**表示用 PC 名登録（最大文字数：半角 15 文字）**に新しい名称を入力します。
6. **OK** をクリックします。


✓ 関連情報

- パソコンで本製品の PC-FAX 受信を起動する（Windows®）

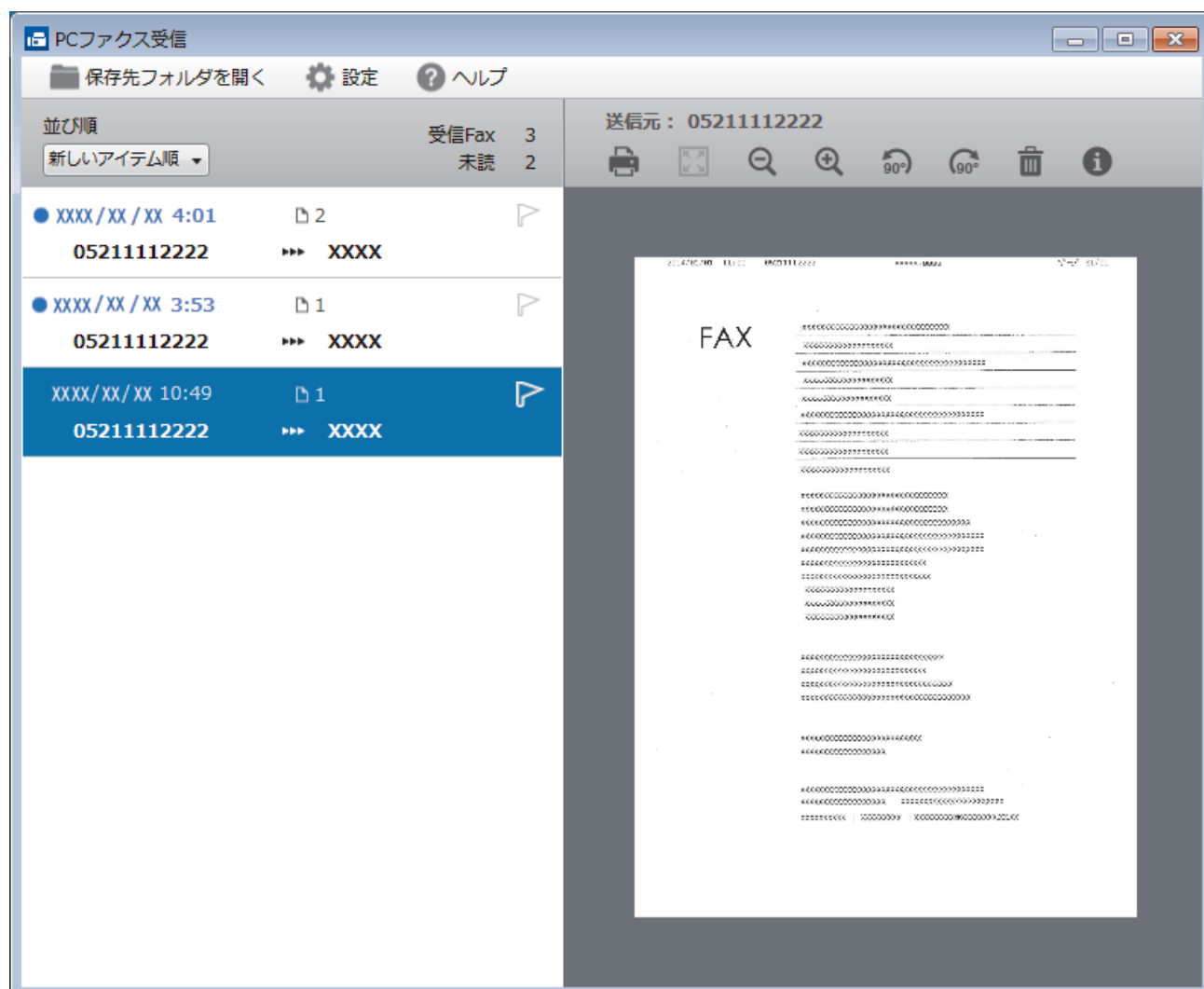
受信したファクスを確認する(Windows®)


受信ステータス

アイコン	表示ステータス
	スタンバイモード 未読ファクス無し
	ファクス受信中
	ファクス受信済み 未読ファクスあり


- タスクトレイの (待機中) アイコンをダブルクリックします。

PC ファクス受信ウィンドウが表示されます。



- リストをクリックすると、ファクスが表示されます。
- 終了するには、ウィンドウ右上にある をクリックして閉じます。



ウィンドウを閉じて、パソコンのタスクトレイに (待機中) アイコンが表示され、PC-FAX 受信が起動しています。PC-FAX 受信を終了するには、パソコンのタスクトレイに表示されているアイコンをクリックして閉じるをクリックします。



関連情報

- [PC-FAX 受信を使ってファクスを受信する\(Windows®\)](#)

■ ネットワーク

- 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
- 他の無線ネットワーク設定方法について
- 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
- トラブルシューティング

はじめに

ネットワークのセットアップと接続には、Drivers & 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
スキャン	Yes		Yes
PC ファクス送信	Yes		
PC ファクス受信	Yes		
ウェブブラウザーによる設定	Yes	Yes	Yes
リモートセットアップ	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
- パソコンを使用して製品の設定を変更する
- ウェブブラウザを使用して製品の設定を変更する

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

ウェブブラウザによる設定

ウェブブラウザによる設定は、標準的なウェブブラウザを使用し、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。

リモートセットアップ(Windows®)

リモートセットアップは、Windows®アプリケーションから、複数の製品およびネットワークを設定するためのプログラムです。このアプリケーションを起動すると、本製品の設定値がお使いのパソコンの画面に自動的に表示されます。設定を変更する場合は、変更した設定値を本製品に直接送信します。



このユーティリティは USB またはネットワーク接続で使えます。



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、Drivers & 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
- 無線ネットワーク用に本製品を設定する
- 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
- 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）
- 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、本製品に無線 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
- エンタープライズ無線 LAN 用に本製品を設定する
- Wi-Fi Direct®を使用する

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、Drivers & 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。

無線セットアップを完了した後、インストーラープログラムは、お使いの機器を操作するために必要なドライバーとソフトウェア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.  [メニュー] > [全てのメニュー] > [ネットワーク] > [無線 LAN] > [WPS] を押します。
2. [無線 LAN をオンにしますか?] が表示されたら、[はい] を押します。
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、[いいえ] を押します。
3. タッチパネルに [アクセスポイントの WPS ボタンを 押してください 操作ができたら [OK] を押してください] 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 [OK] 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、無線ネットワークへの接続を試みます。

無線機器が正常に接続されると、本製品の画面に [接続しました] 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](#)

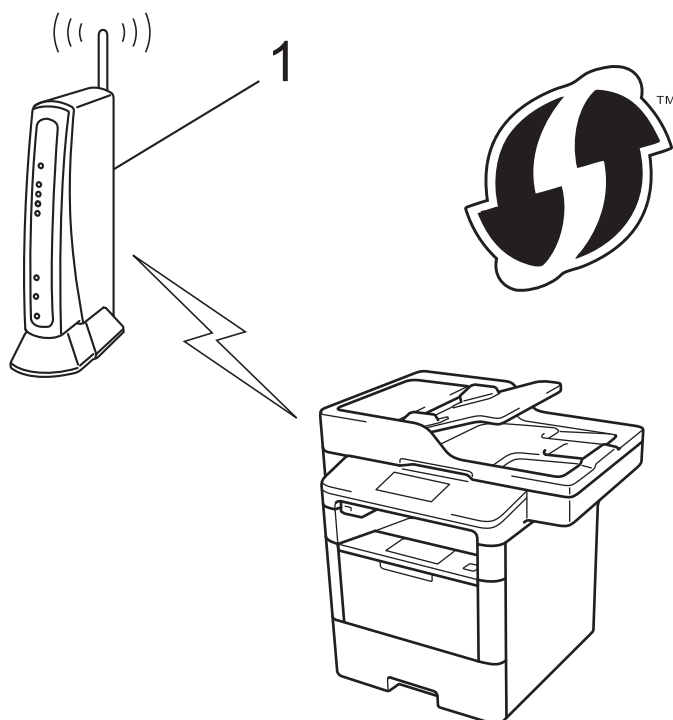
Wi-Fi Protected Setup™ (WPS) の PIN 方式を使用して本製品に無線ネットワークを設定する

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。

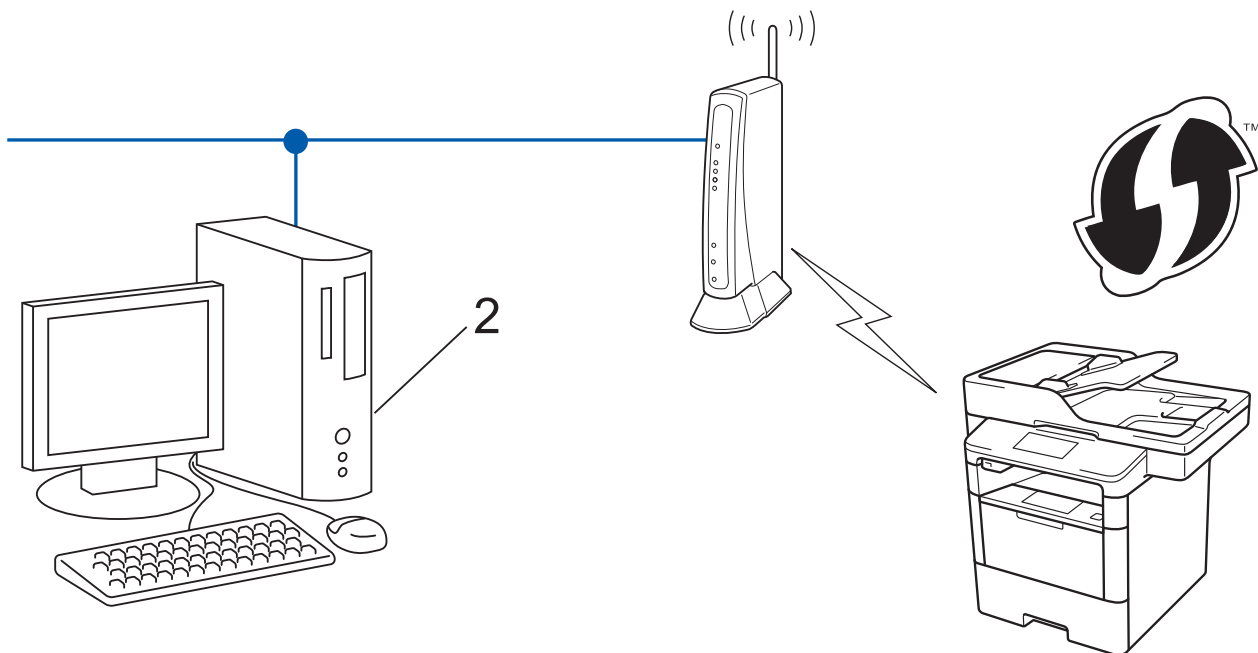
タイプ A


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.  [メニュー] > [全てのメニュー] > [ネットワーク] > [無線 LAN] > [WPS (PIN コード)] を押します。
2. [無線 LAN をオンにしますか?] が表示されたら、[はい] を押します。
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、[いいえ] を押します。
3. 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。
4. 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）。
5. 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。

6. 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 をレジストラー（登録管理機器）として使用する場合、以下の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。

7. 本製品を選択し、**次へ**をクリックします。
8. 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。
9. 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。
10. **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 [接続しました] 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

■ ホーム > ネットワーク > 他の無線ネットワーク設定方法について > 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

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.  [メニュー] > [全てのメニュー] > [ネットワーク] > [無線 LAN] > [無線接続ウィザード] を押します。
2. [無線 LAN をオンにしますか?] が表示されたら、[はい] を押します。
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、[いいえ] を押します。
3. 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。上または下にフリックするか、▲または▼を押して [<New SSID>] を表示します。 [<New SSID>] を押したあと、[OK] を押します。
4. SSID 名を入力し、[OK] を押します。
5. 指示に従い、[アドホック] を押します。
6. 暗号化方式として [なし] または [WEP] を選択します。
7. 暗号化方式に [WEP] を選択した場合、WEP キーを選択して入力し、[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。

8. 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 [接続しました] 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](#)

■ ホーム > ネットワーク > 他の無線ネットワーク設定方法について > 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) > 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

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. [ [メニュー] > [全てのメニュー] > [ネットワーク] > [無線 LAN] > [無線接続ウィザード] を押します。
3. [無線 LAN をオンにしますか?] が表示されたら、[はい] を押します。
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、[いいえ] を押します。
4. 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、上下にフリックするか、▲または▼を押して接続する SSID を表示し、表示した SSID を押します。
5. [OK] を押します。
6. WEP 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。

7. 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 [接続しました] 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、本製品に無線 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。
- セットアップについてカスタマーサポートにお問い合わせになる場合は、お使いの SSID（ネットワーク名）とネットワークキーをお手元にご用意ください。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？

- a. お使いの無線 LAN アクセスポイント／ルーターに付属の説明書をお読みください。
- b. 初期 SSID は、製造メーカー名またはモデル名の可能性があります。
- c. セキュリティ情報が不明の場合は、ルーターの製造メーカー、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. 本製品の画面で、 [メニュー] > [全てのメニュー] > [ネットワーク] > [無線 LAN] > [無線接続ウィザード] を押します。
3. [無線 LAN をオンにしますか?] が表示されたら、[はい] を押します。
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、[いいえ] を押します。
4. 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、上下にフリックするか、▲または▼を押して接続する SSID を表示し、表示した SSID を押します。
5. [OK] を押します。
6. 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。
文字の入力が終了したら、[OK] 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。
7. 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 [接続しました] 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。


- 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。

-  [メニュー] > [全てのメニュー] > [ネットワーク] > [無線 LAN] > [無線接続ウィザード] を押します。
- [無線 LAN をオンにしますか?] が表示されたら、[はい] を押します。
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、[いいえ] を押します。
- 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。上または下にフリックするか、▲または▼を押して [<New SSID>] を表示します。 [<New SSID>] を押したあと、[OK] を押します。
- SSID 名を入力し、[OK] を押します。
- 指示に従い、[インフラストラクチャ] を押します。
- 認証方式を選択します。
- 次のいずれかを行ってください。
 - [オープンシステム認証] を選択した場合、暗号化方式として [なし] または [WEP] を押します。
暗号化方式に [WEP] を選択した場合、WEP キーを選択して入力し、[OK] を押します。
 - [共有キー認証] を選択した場合、WEP キーを選択して入力し、[OK] を押します。
 - [WPA/WPA2-PSK] を選択した場合、暗号化方式として [TKIP+AES] または [AES] 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。

- 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 [接続しました] 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お問い合わせください。

2. [メニュー] > [全てのメニュー] > [ネットワーク] > [無線 LAN] > [無線接続ウィザード] を押します。
3. [無線 LAN をオンにしますか?] が表示されたら、[はい] を押します。
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、[いいえ] を押します。
4. 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。上または下にフリックするか、▲または▼を押して [<New SSID>] を表示します。 [<New SSID>] を押したあと、[OK] を押します。
5. SSID 名を入力し、[OK] を押します。
6. 指示に従い、[インフラストラクチャ] を押します。
7. 認証方式を選択します。
8. 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、内部認証方式を [NONE]、[CHAP]、[MS-CHAP]、[MS-CHAPv2]、[GTC] または [PAP] から選択します。



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。

暗号化タイプに [TKIP+AES] または [AES] を選択します。

検証方法を、[検証しない]、[CA 証明書] または [CA 証明書+サーバー ID] から選択します。

- [CA 証明書+サーバー ID] を選択した場合、サーバー ID、ユーザー ID、およびパスワード（必要な場合）を入力し、それぞれ [OK] を押します。
- その他を選択した場合は、ユーザー ID とパスワードを入力し、それぞれ [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、[検証しない] のみ表示されます。

- [EAP-TLS] を選択した場合、暗号化方式として [TKIP+AES] または [AES] を選択します。
使用可能なクライアント証明書のリストが本製品に表示されます。表示されたリストから証明書を選択します。
検証方法を、[検証しない]、[CA 証明書] または [CA 証明書+サーバー ID] から選択します。
 - [CA 証明書+サーバー ID] を選択した場合、サーバー ID とユーザー ID を入力し、それぞれ [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、[検証しない] のみ表示されます。

9. 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 [接続しました] と表示されます。



関連情報

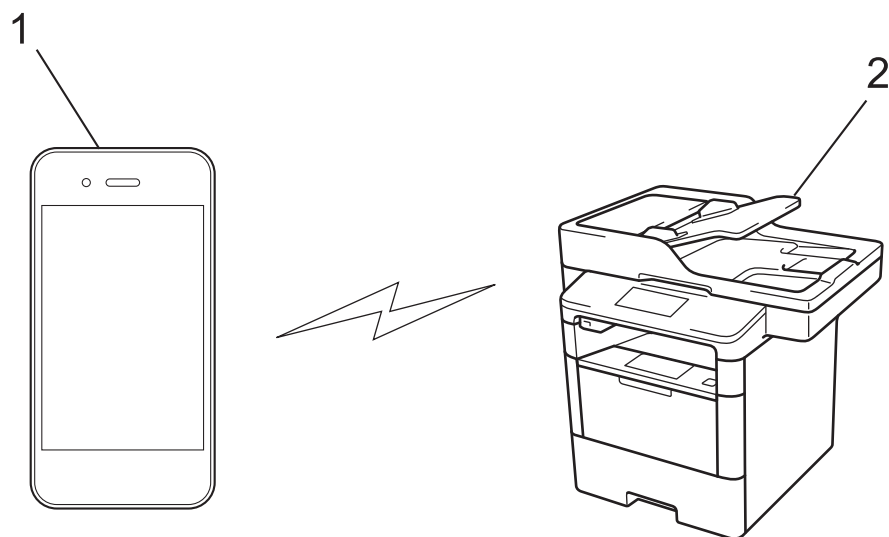
- [他の無線ネットワーク設定方法について](#)

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またはスキャンについて](#)
- [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またはスキャンについて

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 を接続する](#)
- [Wi-Fi Protected Setup™（WPS）のワンプッシュ方式を使用して Wi-Fi Direct ネットワークを設定する](#)
- [PIN 方式を使用して Wi-Fi Direct を接続する](#)
- [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 を接続する
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 を接続する

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：Wi-Fi Protected Setup™ (WPS) のワンプッシュ方式を使用して Wi-Fi Direct ネットワークを設定する
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 を接続する](#)
- [Wi-Fi Protected Setup™ \(WPS\) のワンプッシュ方式を使用して Wi-Fi Direct ネットワークを設定する](#)
- [PIN 方式を使用して Wi-Fi Direct を接続する](#)
- [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 を接続する

お使いの携帯端末で Wi-Fi Direct がサポートされている場合、以下の手順に従って Wi-Fi Direct 設定します。



本製品が携帯端末から Wi-Fi Direct 要求を受信すると、メッセージ「[Wi-Fi Direct の接続リクエストが来ています 通信を開始するには [OK]を押してください]」が画面に表示されます。[OK]を押して接続します。

1.  [メニュー] > [全てのメニュー] > [ネットワーク] > [Wi-Fi Direct] > [プッシュボタン接続]を押します。
2. [相手側デバイスの Wi-Fi Direct 設定を有効に して [OK] ボタンを押してください]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。[OK]を押します。

Wi-Fi Direct セットアップが起動します。キャンセルする場合、を押します。

3. 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。接続したい携帯端末を選択します。[再検索]を押して、利用可能な機器を再検索します。
4. 携帯端末が正常に接続されると、本製品の画面に [接続しました]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)のワンプッシュ方式を使用して Wi-Fi Direct ネットワークを設定する

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。



本製品が携帯端末から Wi-Fi Direct 要求を受信すると、メッセージ「[Wi-Fi Direct の接続リクエストがきています 通信を開始するには [OK] を押してください]」が画面に表示されます。[OK] を押して接続します。

1.  [メニュー] > [全てのメニュー] > [ネットワーク] > [Wi-Fi Direct] > [グループ オーナー]を押します。
2. [オン]を押します。
3. 上または下にフリックするか、▲または▼を押して[プッシュボタン接続]オプションを選択します。[プッシュボタン接続]を押します。
4. [相手側デバイスの Wi-Fi Direct 設定を有効に して[OK] ボタンを押してください]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。本製品の[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、を押します。

5. 携帯端末が正常に接続されると、本製品の画面に [接続しました] 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 を接続する

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。




本製品が携帯端末から Wi-Fi Direct 要求を受信すると、メッセージ「[Wi-Fi Direct の接続リクエストが来ています 通信を開始するには [OK]を押してください]」が画面に表示されます。[OK]を押して接続します。

1.  [メニュー] > [全てのメニュー] > [ネットワーク] > [Wi-Fi Direct] > [PIN コード接続]を押します。
2. [相手側デバイスの Wi-Fi Direct 設定を有効に して[OK] ボタンを押してください]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。[OK]を押します。

Wi-Fi Direct セットアップが起動します。キャンセルする場合、を押します。

3. 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 コード接続]が表示されたら、携帯端末に表示された PIN を、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。接続したい携帯端末を選択します。[再検索]を押して、利用可能な機器を再検索します。
4. 次のいずれかを行ってください。
 - [PIN Code 表示]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ます。次の手順に進みます。
 - [PIN Code 入力]を押して携帯端末に表示された PIN を本製品に入力し、[OK]を押します。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 を押します。最初の手順に戻り、再度実行します。
5. 携帯端末が正常に接続されると、本製品の画面に「接続しました」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。



本製品が携帯端末から Wi-Fi Direct 要求を受信すると、メッセージ「[Wi-Fi Direct の接続リクエストが来ています 通信を開始するには [OK] を押してください]」が画面に表示されます。[OK] を押して接続します。

1.  [メニュー] > [全てのメニュー] > [ネットワーク] > [Wi-Fi Direct] > [グループ オーナー]を押します。
2. [オン]を押します。
3. 上または下にフリックするか、▲または▼を押して[PIN コード接続]を選択します。[PIN コード接続]を押します。
4. [相手側デバイスの Wi-Fi Direct 設定を有効にして [OK] ボタンを押してください]が表示されたら、携帯端末の WPS PIN 設定方式を有効にして、[OK]を押します。

Wi-Fi Direct セットアップが起動します。キャンセルする場合、を押します。

5. 携帯端末からの接続要求を待ちます。本製品の画面に[PIN コード接続]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]を押します。
6. 携帯端末が正常に接続されると、本製品の画面に[接続しました]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。



本製品が携帯端末から Wi-Fi Direct 要求を受信すると、メッセージ「[Wi-Fi Direct の接続リクエストがきています 通信を開始するには [OK] を押してください]」が画面に表示されます。[OK] を押して接続します。

1.  [メニュー] > [全てのメニュー] > [ネットワーク] > [Wi-Fi Direct] > [手動接続] を押します。
2. 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。
3. 携帯端末が正常に接続されると、本製品の画面に [接続しました] 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
- ウェブブラウザを使用してメールサーバーを設定する
- E メールまたはインターネットファクス (I-Fax) 用に本製品を設定する
- インターネットファクス (I-FAX)オプション
- 無線 LAN レポートを印刷する
- LDAP 検索の設定と操作について
- ウェブブラウザ設定を使用した、SNTP サーバーとの時間の同期について

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. [] [メニュー] > [全てのメニュー] > [レポート印刷] > [ネットワーク設定リスト] を押します。
2. [はい] 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](#)
- [ウェブブラウザによる設定画面にアクセスする](#)

ウェブブラウザを使用してメールサーバーを設定する

ウェブブラウザを使用して本製品を設定し、お使いのメールサーバーと接続します。

1. ウェブブラウザを起動します。
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. **SMTP** 欄で、**詳細設定**をクリックして、**状態が有効**であることを確認します。

SMTP

状態

有効

Eメール送信設定(SMTP)

メールサーバー

0.0.0.0

ポート

25

送信メールサーバー認証方式

☒ なし

☐ SMTP-AUTH

SMTP-AUTHアカウント名

SMTP-AUTHアカウントパスワード

パスワード設定

パスワード確認

SSL/TLS

☒ なし

☐ SSL

☐ TLS

☐ サーバー証明書を検証

デバイスのEメールアドレス

knnXXXXXXXXXX@example.com

CA証明書

Eメール到達(メンテナンス情報)

エラー到達

キャンセル

OK

7. 設定するメールサーバーを選択します。
8. メールサーバーに必要な設定を入力します。
9. 完了後、**OK** をクリックします。
Eメール送信/受信設定のテストダイアログボックスが表示されます。
10. ダイアログボックスに表示される指示に従って、現在の設定値をテストします。

✓ 関連情報

- 高度なネットワーク機能について

E メールまたはインターネットファクス (I-Fax) 用に本製品を設定する

I-Fax を使用する前に、本製品がお使いのネットワークおよびメールサーバーとの通信を設定します。これらの項目は、コントロールパネル、ウェブブラウザによる設定、またはリモートセットアップを使用して設定できます。以下の項目は必ず本製品に設定してください。

- IP アドレス（お使いのネットワークで本製品を使用中の場合は、IP アドレスは設定されています。）
- E-mail アドレス
- SMTP、POP3、IMAP4 サーバーアドレス／ポート／認証方式／暗号化方式／サーバー証明書検証
- メールボックス名とパスワード

不明の場合は、システム管理者に問い合わせてください。

✓ 関連情報

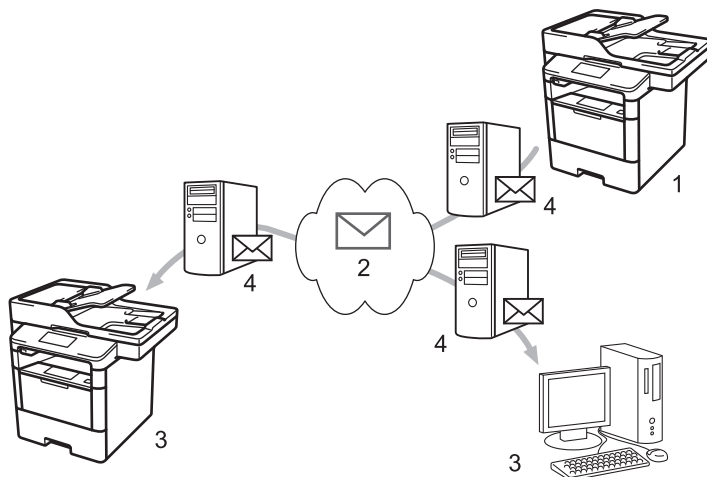
- 高度なネットワーク機能について
 - インターネットを使用するファクスについて (I-Fax)
 - E メールまたはインターネットファクス (I-Fax) の初期設定
 - インターネットファクス (I-Fax) を送信する
 - サーバーに手動でポーリングする
 - お使いのパソコンによる I-Fax の受信について
 - 受信 E-mail とファクスメッセージを転送する
 - 同報送信をリレーする

関連トピック：

- インターネットファクス (I-FAX) オプション

インターネットを使用するファクスについて (I-Fax)

インターネットファクス (I-Fax) を使用すると、転送機構としてのインターネットを使用してファクス文書を送受信することができます。文書は、添付 TIFF-F ファイルとして、E メールで送信されます。お使いのパソコンに TIFF-F ファイルの生成と閲覧に対応したアプリケーションがインストールされていると、文書の送受信が可能です。いずれの TIFF-F ビューアアプリケーションも利用可能です。本製品を介して送信された文書は、自動的に TIFF-F 形式に変換されます。本製品とメッセージを送受信する場合は、お使いのパソコンの E メールアプリケーションが Multipurpose Internet Mail Extensions (MIME) をサポートしている必要があります。



1. 送信者
2. インターネット
3. 受信者
4. E-mail サーバー



- I-Fax では、レターまたは A4 サイズ、およびモノクロでの原稿の送受信のみをサポートしています。



関連情報

- E メールまたはインターネットファクス (I-Fax) 用に本製品を設定する
 - インターネットファクス (I-Fax) に関する重要事項

関連トピック：

- 受信 E-mail とファクスメッセージを転送する

インターネットファクス (I-Fax) に関する重要事項

LAN 経由の I-Fax 通信は E-mail 経由の通信とほぼ同様ですが、一般的な電話回線を使用したファクス通信とは異なります。I-Fax を使用する場合は重要事項を以下に記載します。

- 受信者の場所、LAN の構造、および回線（インターネットなど）の混雑具合などの要因により、エラーメールの送信に通常より時間がかかることがあります。
- 機密文書を送信する場合は、インターネットではなく（セキュリティレベルが低いため）、一般的な電話回線の使用を推奨します。
- 受信者が MIME 互換のメールシステムを使用していない場合、I-Fax を使用して文書を送信することはできません。できるだけ事前に確認し、サーバーがエラー応答を送信しないようにしてください。
- 文書のサイズが大きすぎるために I-Fax 経由で送信できない場合があります。
- 受信インターネットメールの、文字のフォントまたはサイズを変更することはできません。

✓ 関連情報

- [インターネットを使用するファクスについて \(I-Fax\)](#)

E メールまたはインターネットファクス (I-Fax) の初期設定

インターネットファクス (I-FAX)を送信する前に、操作パネル、ウェブブラウザによる設定、またはリモートセットアップを使用して、以下の任意の項目を設定します。

- メールタイトル
- スキャン to E メール 文書
- サイズ制限
- 受信確認要求を行う

インターネットファクス送信設定

メールタイトル	<input type="text" value="Internet Fax Job"/>
スキャン to Eメール 文書	<div>イメージデータが添付されています。</div>
サイズ制限	<input checked="" type="radio"/> オフ <input type="radio"/> オン
最大サイズ	<input type="text" value="1"/> Mbytes
受信確認要求を行う	<input checked="" type="radio"/> オフ <input type="radio"/> オン

[POP3/IMAP4/SMTP>>](#)

不明の場合は、システム管理者に問い合わせてください。

✓ 関連情報

- E メールまたはインターネットファクス (I-Fax) 用に本製品を設定する

関連トピック：


- 受信 E-mail とファクスメッセージを転送する



インターネットファクス (I-Fax) を送信する

I-Fax の送信は、通常のファクスの送信と同様です。受信者の情報が、お使いの E メールアドレス帳に保存されていることを確認し、I-Fax で送信する原稿を本製品にセットします。



- 原稿の送信先パソコンで Windows Server® 2008/2012/2012 R2/2016/2019、Windows® 7、Windows® 8.1、または Windows® 10 が動作していない場合、TIFF-F ファイルを表示できるソフトウェアをパソコンの所有者にインストールしてもらいます。
- 複数のページを送信する場合は、ADF（自動原稿送り装置）を使用します。

1. 原稿をセットします。
2. 次のいずれかを行ってください。
 - みるだけ受信が [オフ (受信したら印刷)] に設定されている場合、[ファクス] を押します。
 - みるだけ受信が [オン (画面で確認)] に設定されている場合は、[ファクス] を押したあと、[ファクス 送信] を押します。
3. ファクス送信の設定値を変更するには、[設定変更] を押します。
4. 上または下にフリックするか、▲または▼を押して、ファクス設定オプションをスクロールします。変更対象の設定オプションが表示されたら、それを押して変更後のオプションを選択します。設定の変更が終了したら、[OK] を押します。
5. 次のいずれかを行ってください。
 -  を押し、タッチパネルを使用して E-mail アドレスを入力します。
 - [電話帳] を押し、受信者の E-mail アドレスを選択して、[送信先に 設定] を押します。
6. [スタート] を押します。


本製品はスキャンを開始します。原稿はスキャンされると、SMTP サーバー経由で受信者に送信されます。スキャン中に  を押すと、送信操作をキャンセルすることができます。
7.  を押します。



関連情報

- E メールまたはインターネットファクス (I-Fax) 用に本製品を設定する

サーバーに手動でポーリングする

1.  [メニュー] > [全てのメニュー] > [ネットワーク] > [E メール/IFAX] > [手動受信] を押します。
2. [はい] を押して確認します。
3. 画面に [受信済] と表示され、本製品は E-mail サーバーから送られたデータを印刷します。



関連情報

- E メールまたはインターネットファクス (I-Fax) 用に本製品を設定する

お使いのパソコンによる I-Fax の受信について

お使いのパソコンがインターネットファクス (I-FAX)を受信すると、E-mail アプリケーションで E-mail が受信されます。受信するインターネットファクス (I-FAX)は、E-mail メッセージに添付され、その**件名**の行に、E-mail サーバーがインターネットファクス (I-FAX)を受信したことが表示されます。本製品が E-mail サーバーにポーリングするのを待つか、E-mail サーバーに手動でポーリングしてデータを受信することができます。




関連情報

- E メールまたはインターネットファクス (I-Fax) 用に本製品を設定する

受信 E-mail とファクスメッセージを転送する


本製品の I-Fax 機能を使用して、E メールや一般的なファクスメッセージを、他のパソコン、ファクス機、または別の I-Fax 機に転送します。本製品の操作パネルを使用して、転送機能を有効にします。

操作パネルを使用して、転送機能を有効にする手順：

1.  [メニュー] > [全てのメニュー] > [ファクス] > [受信設定] > [メモリ受信] > [ファクス転送]を押します。
2. 操作パネルを使用して、受信者のファクス番号または E-mail アドレスを入力します。
3. 使用するファイルタイプを選択します。
4. 以下のいずれかを行ってください。
 - [手動入力]を押して、タッチパネルから転送ファクス番号（最大 20 文字）を入力します。
[OK]を押します。
 - [電話帳]を押します。
上または下にフリックするか、▲または▼を押して、転送先のファクス番号または E メールアドレスが表示されるまでスクロールします。
転送先のファクス番号または E メールアドレスを押します。



[本体でも印刷する]を押して本製品で受信ファクスを印刷すると、コピーを作成できます。

5. を押します。



関連情報

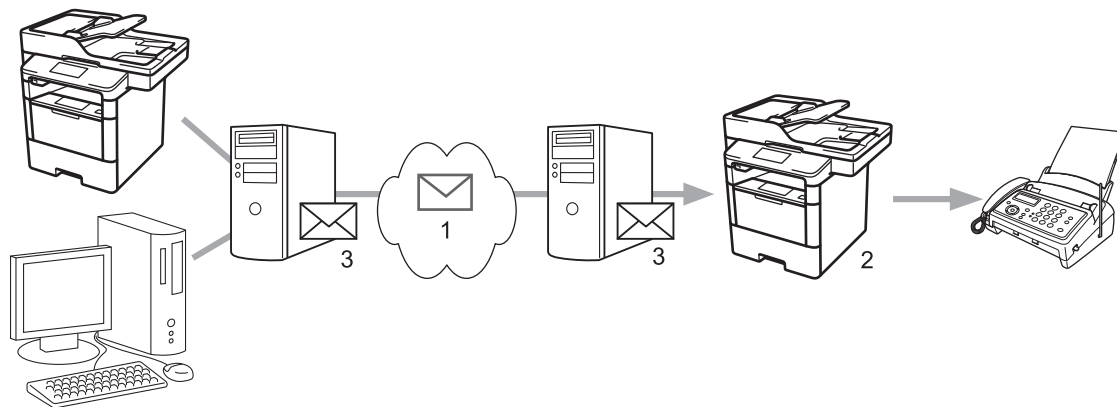
- [E メールまたはインターネットファクス \(I-Fax\) 用に本製品を設定する](#)

関連トピック：

- [インターネットを使用するファクスについて \(I-Fax\)](#)
- [E メールまたはインターネットファクス \(I-Fax\) の初期設定](#)

同報送信をリレーする

リレー同報送信では、本製品がインターネットを介してメッセージを受信し、従来の電話回線を使用して別のファクス機にメッセージを中継します。遠隔地や海外に文書をファクスする必要がある場合、リレー同報送信機能を使用して通信費を節約することができます。



1. インターネット
2. 電話回線
3. E-mail サーバー

本製品の操作パネルまたはウェブブラウザ設定を使用して、以下の項目を設定します。

- **リレー許可**
リレー許可をオンに設定します。
- **許可ドメイン**
一般的なファクス機に原稿を同報送信する製品に、本製品のドメイン名を設定します。本製品をリレー同報送信機器として使用する場合は、製品に信頼できるドメイン名（「@」記号以降の部分）を指定する必要があります。信頼できるドメインは慎重に選択してください。信頼できるドメインのすべてのユーザーが、リレー同報送信を送信できるようになります。最大 10 個のドメイン名を登録できます。
- **リレー配信レポート**
本製品がリレー同報送信を完了した後の、レポート印刷の有無を指定します。

リレー配信機能

リレー許可

☒ オフ ☐ オン

許可ドメイン

リレー配信レポート

☒ オフ ☐ オン

キャンセル

OK

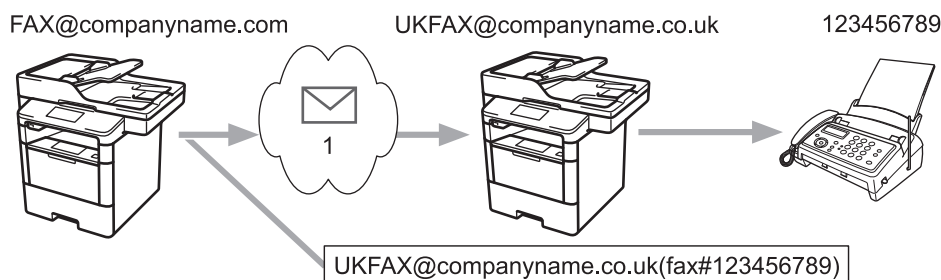


関連情報

- Eメールまたはインターネットファクス（I-Fax）用に本製品を設定する
 - 本製品から同報送信をリレーする
 - お使いのパソコンから同報送信をリレーする


本製品から同報送信をリレーする

リレー同報送信機能を使用して、本製品からファクス機に E メールを送信します。

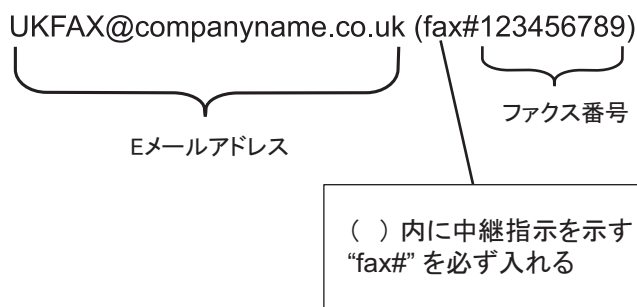


1. インターネット

この例では、本製品の E-mail アドレスは FAX@companyname.com であり、原稿を本製品から、E-mail アドレスが UKFAX@companyname.co.uk の、イギリスの一般的なファクス機に送信します。また、送信には従来の電話回線が使用されます。

1. 原稿をセットします。
2. 次のいずれかを行ってください。
 - ・ みるだけ受信が [オフ (受信したら印刷)] に設定されている場合、[ファクス] を押します。
 - ・ みるだけ受信が [オン (画面で確認)] に設定されている場合は、[ファクス] を押したあと、[ファクス 送信] を押します。
3. [設定変更] を押します。
4. 上または下にフリックするか、▲または▼を押して [同報送信] オプションを表示します。
5. [同報送信] を押します。
6. [番号追加] を押します。
7. 以下の方法で、同報送信に E-mail アドレスを追加できます。
 - ・ [手動入力]、 と押し、E-mail アドレスを入力したあと、[OK] を押します。
 - ・ [電話帳から選択] を押します。同報送信に追加する E-mail アドレスのチェックボックスを押します。追加対象すべての E-mail アドレスを選択し、[OK] を押します。
 - ・ [検索して選択] を押します。名前を入力し、[OK] を押します。検索結果が表示されます。名前を押してから、同報送信に追加する E-mail アドレスを押します。

E-mail アドレスと電話番号の入力方法の例を以下に示します。



すべてのファクス番号を入力し、[OK] を押します。

8. [スタート] を押します。



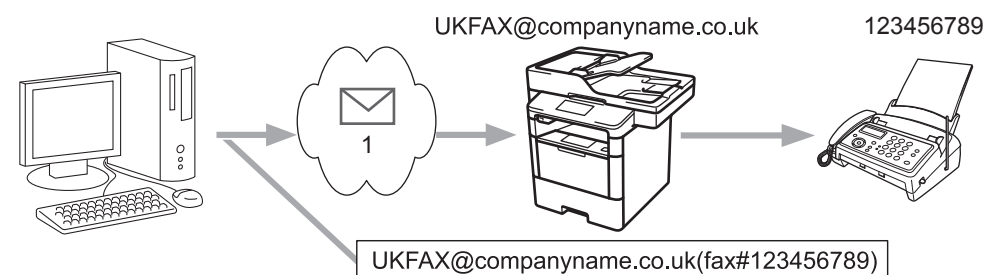
関連情報

- 同報送信をリレーする

お使いのパソコンから同報送信をリレーする

リレー同報送信機能を使用して、パソコンからファクス機に E メールを送信します。

複数のファクス番号へ E-mail 送信できない E-mail アプリケーションもあります。お使いの E-mail アプリケーションが複数のファクス番号をサポートしていない場合、一度にリレーできるファクス機は 1 つのみです。



1. インターネット

E-mail を従来のファクス機に送信する場合、ファクス番号を入力する方法は、使用しているメールアプリケーションによって異なります。

1. お使いの E-mail アプリケーションで、新しいメッセージを作成し、リレー機の E-mail アドレスおよび最初のファクス機のファクス番号を、「TO」ボックスに入力します。

E-mail アドレスとファクス番号の入力方法の例を以下に示します。

UKFAX@companyname.co.uk (fax#123456789)

Eメールアドレス

ファクス番号

() 内に中継指示を示す
“fax#” を必ず入れる



Microsoft® Outlook® の場合、アドレス情報は、以下に示すようにアドレス帳に入力します。

名前 : fax#123456789

E-mail アドレス : UKFAX@companyname.co.uk

2. リレー機の E-mail アドレスおよび、2 台目のファクス機のファクス番号を、「TO」ボックスに入力します。
3. E-mail を送信します。



関連情報

- 同報送信をリレーする

■ インターネットファクス (I-FAX)オプション

- インターネットファクス (I-Fax) 検証メール
- エラーメール
- E メールまたはインターネットファクス (I-Fax) 用に本製品を設定する

インターネットファクス (I-Fax) 検証メール


- 送信の確認メールを使用すると、送信したインターネットファクス (I-FAX)または E-mail の受信と処理が行われた旨の通知の送信を、受信局に要求することができます。
- 受信の確認メールを使用すると、インターネットファクス (I-FAX)または E-mail の受信と処理を正常に行ったあと、デフォルトのレポートを送信局に返信することができます。

この機能を使用するには、本製品の操作パネルの、[メール 受信設定]で[受信確認]を、[メール 送信設定]で[受信確認要求]を設定します。

✓ 関連情報


- [インターネットファクス \(I-FAX\)オプション](#)
 - TX 確認メールの送信通知を有効にする
 - TX 確認メールの受信通知を有効にする

TX 確認メールの送信通知を有効にする

1.  [メニュー] > [全てのメニュー] > [ネットワーク] > [E メール/IFAX] > [メール 送信設定] > [受信確認要求]を押します。
2. [オン]または[オフ]を選択して、送信通知機能を有効または無効にします。
送信通知がオンの場合、ファクスには、メッセージの配信情報を含む、開封通知 (MDN : Message Disposition Notification) と呼ばれるフィールドが追加されます。お買い上げ時には、送信通知はオフに設定されています。



通知レポートを送信するために、MDN フィールドがファクス受信者の製品でサポートされている必要があります。


3. を押します。



関連情報

- [インターネットファクス \(I-Fax\) 検証メール](#)


TX 確認メールの受信通知を有効にする

1.  [メニュー] > [全てのメニュー] > [ネットワーク] > [E メール/IFAX] > [メール 受信設定] > [受信確認] を押します。
2. 3 つの設定オプションの中から 1 つを押します。

オプション	説明
受信通知 [オン]	受信通知が [オン] の場合、テンプレートが送信者に返信され、メッセージの受信と処理が正常に行われたことが通知されます。 これらのテンプレートは、送信者が要求した操作により異なります。 例： [成功： (PC のメールアドレス) から受信しました。]
受信通知 [MDN]	受信通知が [MDN] の場合、発信局が要求確認を [MDN] (開封通知) フィールドに送信していると、受信と処理が正常に行われたことを示すレポートが送信者に返信されます。
受信通知 [オフ]	受信通知が [オフ] の場合、すべての形式の受信通知が無効になり、要求の種類に関わらず、送信者には何も返信されません。



- TX 確認メールを送信するには、送信者が以下の設定を行っている必要があります。
 - [メール 送信設定] の [受信確認要求] を [オン] に変更。
 - [メール 受信設定] の [ヘッダー印刷] を [全て] または [ヘッダー のみ] に変更。
- TX 確認メールを受信するには、受信者が以下の設定を行っている必要があります。
 - [メール 受信設定] の [受信確認] を [オン] に変更。

3.  を押します。



関連情報

- インターネットファクス (I-Fax) 検証メール

エラーメール

インターネットファクス (I-FAX)送信時に配信エラーが発生すると、メールサーバーはファクスを送信した本製品にエラーメッセージを送り、エラーメッセージが印刷されます。

インターネットファクス (I-FAX)受信時にエラーが発生すると、「本製品に送信中のメッセージは TIFF-F 形式ではありませんでした」などのエラーメッセージが印刷されます。



本製品でエラーメールの受信と印刷を行うには、[メール 受信設定]で、[ヘッダー印刷]を、[全て]または[ヘッダー のみ]に切り替える必要があります。

✓ 関連情報

- [インターネットファクス \(I-FAX\)オプション](#)

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.  [メニュー] > [全てのメニュー] > [レポート印刷] > [無線 LAN レポート] を押します。
2. [はい] を押します。
製品は無線 LAN レポートを印刷します。
3.  を押します。

WLAN レポート（無線 LAN レポート）が印刷されない場合、製品のエラーの有無を確認します。目視できるエラーがない場合、1 分間待ったあと、もう一度レポートを印刷してみてください。

✓ 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、スキャン、または PC-FAX の受信ができません](#)
- [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。 <ul style="list-style-type: none">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ください、セキュリティ設定値の記載場所を確認してください。 <ul style="list-style-type: none">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ください、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	<p>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。</p> <p>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。</p> <ul style="list-style-type: none"> 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 <p>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。</p> <p>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。</p>
TS-05	<p>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。</p> <p>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。</p>
TS-06	<p>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。</p> <p>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。</p>
TS-07	<p>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。</p> <p>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。</p> <p>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。</p>
TS-08	<p>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。</p> <ul style="list-style-type: none"> 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、スキャン、または PC-FAX の受信ができません
- 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、本製品に無線 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

LDAP 検索の設定と操作について

LDAP 機能を使うと、お使いのサーバー上で、ファクス番号および E メールアドレスなどの情報を検索できます。ファクス、I-Fax、またはスキャン to E メールサーバー機能を使用する場合、LDAP 検索を使用してファクス番号または E メールアドレスを取得することができます。



- LDAP 機能は、簡体字、繁体字、および韓国語はサポートしていません。
- LDAP 機能は LDAPv3 をサポートしています。
- LDAP 機能は SSL/TLS をサポートしていません。




関連情報

- [高度なネットワーク機能について](#)
 - [ウェブブラウザによる設定を使用して LDAP 構成を変更する](#)
 - [本製品の操作パネルを使用して LDAP 検索を行う](#)

ウェブブラウザによる設定を使用して LDAP 構成を変更する

ウェブブラウザによる設定を使用して、LDAP 設定値を設定します。

1. ウェブブラウザを起動します。
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. 製品のウェブページで**ネットワーク**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. **LDAP** チェックボックスを選択し、**OK** をクリックします。
7. 製品を再起動して、設定を有効にします。
8. お使いのパソコン上で、ウェブブラウザの**アドレス**タブを開き、左ナビゲーションバーの **LDAP** を選択します。
 - **LDAP 検索**
 - **LDAP アドレス**
 - **ポート**（お買い上げ時のポート番号は 389 です。）
 - **検索場所**
 - **認証方式**
 - **ユーザー名**
この項目は、使用される認証方式によっては選択が可能になります。
 - **パスワード**
この項目は、使用される認証方式によっては選択が可能になります。



- LDAP サーバーが Kerberos 認証をサポートしている場合、本認証の設定として Kerberos を選択することを推奨します。Kerberos により、LDAP サーバーとお使いの製品との間で厳密な認証が行えます。
- Kerberos 認証のために、SNTP プロトコル（ネットワークタイムサーバー）を設定するか、操作パネルで日時とタイムゾーンを正確に設定する必要があります。

- **Kerberos サーバーアドレス**
この項目は、使用される認証方式によっては選択が可能になります。
 - **LDAP タイムアウト**
 - **名前属性名（検索する属性）**
 - **メールの属性名**
 - **FAX の属性名**
9. 設定の完了後、**OK** をクリックします。**状態**欄に **OK** と表示されることを確認します。



関連情報

- [LDAP 検索の設定と操作について](#)


本製品の操作パネルを使用して LDAP 検索を行う


LDAP の設定後、LDAP 検索機能を使用して、ファクス番号または E メールアドレスを取得し、以下の操作を行うことができます。

- ファクスを送信する
- インターネットファクス (I-Fax) を送信する
- E-mail サーバーにスキャン画像を送信する



- LDAP 機能は LDAPv3 をサポートしています。
- LDAP 機能は SSL/TLS をサポートしていません。
- Kerberos 認証または簡単認証を使用して、お使いの LDAP サーバーに接続しなければならない場合があります。いずれの認証方式を使用するかは、ネットワーク管理者に設定されたセキュリティポリシーにより異なります。
- Kerberos 認証のために、SNTP プロトコル (ネットワークタイムサーバー) を設定するか、操作パネルで日時とタイムゾーンを正確に設定する必要があります。

1.  を押して検索します。
2. タッチパネルを使用して、検索する先頭文字を入力します。
3. [OK] を押します。

LDAP 検索結果が画面に表示されます。  アイコンが、ファクス番号 (ローカル) または E-mail (ローカル) の、アドレス帳検索結果の前に表示されます。

- サーバーまたは E-mail (ローカル) アドレス帳に一致する文字列が存在しない場合、画面に [検索結果がありません] が約 1 分間表示されます。
4. 上または下にフリックするか、▲ または ▼ を押して、対象の名前を表示します。
 5. 対象の名前を押します。
名前の詳細を表示するには、[詳細] を押します。
 6. 検索結果のファクス番号や E-mail アドレスが複数の場合は、製品には 1 つのみを選択するよう表示されます。[送信先に 設定] を押します。次のいずれかを行ってください。
 - ファクスまたはインターネットファクス (I-FAX) を送信する場合、[スタート] を押します。
 - E-mail サーバーにスキャン画像を送信する場合、原稿を読み込ませて [次へ] を押したあと、[スタート] を押します。



関連情報

- [LDAP 検索の設定と操作について](#)


ウェブブラウザ設定を使用した、SNTP サーバーとの時間の同期について

簡易ネットワークタイムプロトコル（SNTP : Simple Network Time Protocol）は、本製品が認証に使用する時間と、SNTP タイムサーバーとの時刻を同期させます。（この時刻は、本製品の操作パネルに表示される時間とは異なります。）SNTP タイムサーバーを使用して、本製品の時刻と協定世界時（UTC: Coordinated Universal Time）を、自動または手動で同期させることができます。

- ウェブブラウザによる設定を使用して日時を設定する
- ウェブブラウザによる設定を使用して SNTP プロトコルを設定する

ウェブブラウザによる設定を使用して日時を設定する

本製品が使用している時間と SNTP タイムサーバーを同期させます。

1. ウェブブラウザを起動します。
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. 左側にあるナビゲーションバーの**時計設定**をクリックします。

時計設定

日付

2016 / 01 / 01

時間

03 : 37 24時間制


タイムゾーン

UTC+09:00 ▼

☐ **SNTPサーバーと同期する**
本機能を使用するためには
SNTPサーバーの設定が必要です。
[SNTP>>](#)

キャンセル

OK

 **タイムゾーン**のドロップダウンリストから、お住まいの地域と UTC 間の時差を選択します。


6. **タイムゾーン**の設定値を確認します。
7. **SNTP サーバーと同期する**チェックボックスにチェックを入れます。
8. **OK** をクリックします。

✓ 関連情報

- [ウェブブラウザ設定を使用した、SNTP サーバーとの時間の同期について](#)

ウェブブラウザによる設定を使用して 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. 製品を再起動して、設定を有効にします。
8. SNTP チェックボックスの横にある**詳細設定**をクリックして以下の指示に従います。

SNTP

状態有効

同期状態同期成功

SNTPサーバー設定の方法

AUTO

プライマリーSNTPサーバーアドレス

プライマリーSNTPサーバーポート

セカンダリーSNTPサーバーアドレス

セカンダリーSNTPサーバーポート

同期間隔

時間

[時計設定>>](#)

キャンセル

OK

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。 <ul style="list-style-type: none">• 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入力します。

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）。

9. **OK** をクリックします。

関連情報

- [ウェブブラウザ設定を使用した、SNTP サーバーとの時間の同期について](#)

上級ユーザーのための技術的な情報について


- ・ 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

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.  [メニュー] > [全てのメニュー] > [ネットワーク] > [ネットワーク設定リセット] を押します。
2. [再起動しますか？ 実行する場合は [OK] を 2 秒間 押してください 実行しない場合は [キャンセル] を押してください] が表示されます。[OK] を 2 秒間押して、確認します。

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連絡してください。

✓ 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
- 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？
- 無線ネットワーク設定を完了できません
- 本製品で、ネットワーク経由の印刷、スキャン、または PC-FAX の受信ができません
- 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

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
「接続できません 他のデバイスと接続中です」	本製品がグループオーナー（GO）のときに、2つの携帯端末がすでに Wi-Fi Direct 接続されています。	本製品と他の携帯端末との接続が切れてから、Wi-Fi Direct をもう一度設定します。接続状態は、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。
「ユーザー認証に失敗しました 管理者に問い合わせてください」	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。	<ul style="list-style-type: none"> • 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。 • ログファイルサーバーの時間が、SNTP サーバーの時間または時計設定の設定値と一致することを確認します。 • 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。SNTP サーバーが存在しない場合、時計設定およびタイムゾーンの設定値がウェブブラウザまたは操作パネルを使用して正しく設定され、認証を行うサーバーにより使用される時間が本製品の時間と一致するようにします。
「ユーザー ID とパスワードを 確認してください」	Kerberos 認証エラーです。	Kerberos サーバーのユーザー名とパスワードを正確に入力していることを確認します。Kerberos サーバーの設定値についての詳細は、ネットワーク管理者に問い合わせてください。
	本製品の日時およびタイムゾーンの設定値に誤りがあります。	本製品の日時とタイムゾーンの設定値を確認します。
	DNS サーバーの設定が正しくありません。	ネットワーク管理者に問い合わせ、DNS サーバーの設定値を確認します。
	本製品は Kerberos サーバーに接続できません。	ネットワーク管理者に問い合わせ、Kerberos サーバーの設定値を確認します。
「接続エラー」	他の機器が同時に、Wi-Fi Direct に接続しようとしています。	<ul style="list-style-type: none"> • 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。
「接続に失敗しました」	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。	<ul style="list-style-type: none"> • 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。
「ファイルへアクセスできません 管理者に問い合わせてください」	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。	<ul style="list-style-type: none"> • 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。
	ウェブブラウザによる設定で、 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。
「デバイスが見つかりません」	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。	<ul style="list-style-type: none"> • 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。

エラーメッセージ	原因	対応
		<ul style="list-style-type: none"> 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。
「サーバーが見つかりません 管理者に問い合わせてください」	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。	<ul style="list-style-type: none"> 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。
「サーバーが見つかりません」	本製品は LDAP サーバーに接続できません。	<ul style="list-style-type: none"> 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。
	本製品は Active Directory®サーバーに接続できません。	<ul style="list-style-type: none"> 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。
「時計が未設定です 管理者に問い合わせてください」	本製品が SNTP タイムサーバーから時間を取得していないか、本製品に日時が設定されていません。	<ul style="list-style-type: none"> SNTP タイムサーバーにアクセスするための設定値が、ウェブブラウザを使用して正しく設定されていることを確認します。 本製品の時計設定設定値が、ウェブブラウザを使用して正しく設定されていることを確認します。
「予期しないエラーが発生しました」	本製品の LDAP プロトコルが無効です。	認証方式を確認してから、必要なプロトコル設定をウェブブラウザによる設定画面で有効にしてください。
	本製品の CIFS プロトコルが無効です。	



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
- パソコンを使用して製品の設定を変更する

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。	<ul style="list-style-type: none">無線セットアップヘルプ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。<ul style="list-style-type: none">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)。	<ul style="list-style-type: none">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。	<ul style="list-style-type: none">SSID およびパスワードを確認します。<ul style="list-style-type: none">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。	<ul style="list-style-type: none">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、スキャン、または PC-FAX の受信ができません

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により、本製品のネットワークへのアクセスがブロックされています。(ネットワークスキャン機能が動作していません。)	<ul style="list-style-type: none"> • (Windows®) ネットワークスキャンを許可するよう、サードパーティのセキュリティ/ファイアウォールソフトウェアの設定を行ってください。ネットワークスキャンにポート 54925 を追加するには、以下の情報を入力します。 <ul style="list-style-type: none"> - 名前 : NetScan などを入力します。 - ポート番号 : 54925 を入力します。 - プロトコル : UDP が選択されます。 サードパーティのセキュリティ/ファイアウォールのソフトウェアに添付された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
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。(ネットワーク PC-Fax 受信機能が動作していません。) (Windows®)	<p>PC-FAX 受信を許可するよう、サードパーティのセキュリティ/ファイアウォールソフトウェアの設定を行ってください。ネットワーク PC-FAX 受信にポート 54926 を追加するには、以下の情報を入力します。</p> <ul style="list-style-type: none"> • 名前 : PC-FAX Rx などを入力します。 • ポート番号 : 54926 を入力します。 • プロトコル : UDP が選択されます。 <p>サードパーティのセキュリティ/ファイアウォールのソフトウェアに添付された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。</p>	有線/無線
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。	<p>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。</p> <p>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。</p>	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。	<ul style="list-style-type: none"> • 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。	<ul style="list-style-type: none"> • 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) 	有線/無線

原因	対応	インターフェイス
	<p> (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。</p> <ul style="list-style-type: none"> - (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 の場合)  > 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。 	
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、本製品で印刷やスキャンができない場合は、本製品のプリンタードライバーとソフトウェアをアンインストールしてから、再インストールすることをお勧めします。

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。 <ul style="list-style-type: none"> 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>] <ul style="list-style-type: none"> 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、スキャン、または PC-FAX の受信ができません

■ 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、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.  [メニュー] > [全てのメニュー] > [基本設定] > [セキュリティ設定ロック]を押します。
2. パスワード用の4桁の数字を入力します。
3. [OK]を押します。
4. 画面に[パスワード確認:]と表示されたら、パスワードを再入力します。
5. [OK]を押します。
6. 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.  [メニュー] > [全てのメニュー] > [基本設定] > [セキュリティ設定ロック] > [パスワード設定]を押します。
2. 現在の4桁のパスワードを入力します。
3. [OK]を押します。
4. 新しい4桁のパスワードを入力します。
5. [OK]を押します。
6. 画面に[パスワード確認:]と表示されたら、パスワードを再入力します。
7. [OK]を押します。
8. 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.  [メニュー] > [全てのメニュー] > [基本設定] > [セキュリティ設定ロック] > [ロック オフ⇒オン]を押します。
2. 現在の4桁のパスワードを入力します。
3. [OK]を押します。



設定ロックを[オフ]にするには、画面の  を押し、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
- セキュリティ機能ロック 3.0
- Active Directory®認証を使用する
- LDAP 認証方式を使用する
- 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
- 安全な E-mail の送受信について
- 有線または無線 LAN への IEEE 802.1x 認証の使用について
- 印刷ログ機能

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
- ウェブブラウザを使用してセキュリティ機能ロック 3.0 を設定する
- セキュリティ機能ロック 3.0 を使用するスキャンについて
- 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 3.0 追加の機能について

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。

- **コピー**

- **スキャン**

スキャンには iPrint&Scan for Mac を経由するスキャンジョブの送信が含まれます。

- **送信**

- **受信**

- **USB ダイレクトプリント**

- **スキャン to USB**

- **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. 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。
6. **セキュリティ機能ロック**を選択します。
7. **OK** をクリックします。
8. 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。
9. **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 14 文字の英数字）。
10. **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。
11. 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。
12. **OK** をクリックします。
13. 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。
14. **ユーザーリスト**欄で、ユーザー名を入力します。
15. **パスワード**欄で、4 桁のパスワードを入力します。
16. **E メール アドレス**欄で、ユーザーの E メールアドレスを入力します。
17. 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。
18. **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 を使用するスキャンについて

スキャン制限を設定する（管理者用）

管理者はセキュリティ機能ロック 3.0 を使用して、スキャンを許可するユーザーを制限することができます。スキャン機能が一般ユーザーの設定に対してオフに設定されている場合、**スキャン**のチェックボックスが選択されているユーザーのみがスキャン操作を行えます。

スキャン機能を使用する（制限されたユーザー用）

- 操作パネルを使用してスキャンする場合：
制限されたユーザーは、操作パネルで PIN を入力して、スキャンモードにアクセスします。
- パソコンからスキャンする場合：
制限されたユーザーは、各自のパソコンからスキャンする前に、操作パネルで PIN を入力する必要があります。操作パネルで PIN が入力されなかった場合、エラーメッセージがユーザーのパソコンに表示されます。



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. 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。
6. **セキュリティ機能ロック**を選択します。
7. **OK** をクリックします。
8. **機能制限**メニューをクリックします。
9. **一般モード**行で、チェックボックスを選択して一覧表示されている機能を許可するか、チェックボックスの選択を解除してこれらの機能を制限します。
10. **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。

カウンター自動リセット

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



関連情報

- ・ [セキュリティ機能ロック 3.0](#)

Active Directory®認証を使用する

- [Active Directory®認証について](#)
- [ウェブブラウザを使用して Active Directory®認証を設定する](#)
- [本製品にログインし、操作パネルを使用して設定値を変更する（Active Directory®認証）](#)

Active Directory®認証について

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

Active Directory®認証では、以下の機能が利用可能です。

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

この機能を使用するには、**LDAP + kerberos** 認証方式を選択し、**メールアドレス取得設定**で**オン**を選択します。スキャンデータを E-mail サーバーに送信する際に、お使いの E-mail アドレスが送信者として設定されます。本製品がお使いの E-mail アドレスを見つけられない場合、本製品の E-mail アドレスが送信者として設定されます。

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

Active Directory®認証の設定は、ウェブブラウザを使用して変更できます。




関連情報

- [Active Directory®認証を使用する](#)

ウェブブラウザを使用して Active Directory®認証を設定する

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

1. ウェブブラウザを起動します。
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. 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。
6. **Active Directory 認証**を選択します。
7. **OK** をクリックします。
8. 左側にあるナビゲーションバーの **Active Directory 認証**メニューをクリックします。
9. 以下の設定をします。

オプション	説明
プリントデータ蓄積	このオプションを選択して、受信プリントデータを保存します。本製品へログオンすると、ご使用パソコンの印刷ジョブは自動的に印刷されます。この機能は、プリンタードライバーにより作成されたプリントデータにのみ対応しています。
ファクス受信データ蓄積	このオプションを選択して、受信ファクスデータを保存します。本製品へのログオン後、すべての受信ファクスデータを印刷できます。
ユーザー ID を記憶	このオプションを選択して、ユーザー ID を保存します。
Active Directory サーバアドレス	Active Directory®サーバーの IP アドレスまたはサーバー名（例：ad.example.com）を入力します。
Active Directory ドメイン名	Active Directory®のドメイン名を入力します。
プロトコルと認証方式	プロトコルと認証方式を選択します。
メールアドレス取得	このオプションを使用して、LDAP サーバーからログオンユーザーの E メールアドレスを取得します。（LDAP + kerberos 認証方式の場合のみ可能）
ユーザーのホームディレクトリ取得	このオプションを選択して、Scan to Network の送信先のホームディレクトリを取得します。（LDAP + kerberos 認証方式の場合のみ可能）
LDAP ポート	LDAP サーバーのポート番号を入力します（LDAP + kerberos 認証方式の場合のみ可能）。
LDAP 検索場所	LDAP 検索ルートを入力します（LDAP + kerberos 認証方式の場合のみ可能）。

10. **OK** をクリックします。



関連情報

- [Active Directory®認証を使用する](#)

■ [ホーム](#) > [セキュリティ](#) > [ネットワークセキュリティ機能](#) > [Active Directory®認証を使用する](#) > 本製品にログインし、操作パネルを使用して設定値を変更する（Active Directory®認証）

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

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

1. 操作パネルを使用して、製品の画面にユーザー ID とパスワードを入力します。
2. [OK]を押します。
3. 認証が成功すると、製品の操作パネルのロックが解除されます。

✓ 関連情報

- [Active Directory®認証を使用する](#)

LDAP 認証方式を使用する

- LDAP 認証について
- ウェブブラウザを使用して LDAP 認証を設定する
- 本製品にログインし、操作パネルを使用して設定値を変更する（LDAP 認証）

LDAP 認証について

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

LDAP 認証では以下の機能が提供されます。

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

この機能を使用するには、**メールアドレス取得**設定に**オン**を選択します。

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


LDAP 認証の設定は、ウェブブラウザを使用して変更できます。



関連情報

- [LDAP 認証方式を使用する](#)

ウェブブラウザを使用して LDAP 認証を設定する

1. ウェブブラウザを起動します。
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. 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。
6. **LDAP 認証**を選択します。
7. **OK** をクリックします。
8. 左側にあるナビゲーションバーの **LDAP 認証** をクリックします。
9. 以下の設定をします。

オプション	説明
プリントデータ蓄積	このオプションを選択して、受信プリントデータを保存します。本製品へログオンすると、ご使用パソコンの印刷ジョブは自動的に印刷されます。この機能は、プリンタードライバーにより作成されたプリントデータにのみ対応しています。
ファクス受信データ蓄積	このオプションを選択して、受信ファクスデータを保存します。本製品へのログオン後、すべての受信ファクスデータを印刷できます。
ユーザー ID を記憶	このオプションを選択して、ユーザー ID を保存します。
LDAP アドレス	LDAP サーバーの IP アドレスまたはサーバー名（例：ad.example.com）を入力します。
メールアドレス取得	このオプションを使用して、LDAP サーバーからログオンユーザーの E メールアドレスを取得します。
ユーザーのホームディレクトリ取得	このオプションを選択して、Scan to Network の送信先のホームディレクトリを取得します。
LDAP ポート	LDAP サーバーのポート番号を入力します。
LDAP 検索場所	LDAP 検索のルートディレクトリを入力します。
名前属性名 (検索する属性)	検索キーとして使用する属性を入力します。

10. **OK** をクリックします。

関連情報

- [LDAP 認証方式を使用する](#)

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

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

1. 操作パネルを使用して、製品の画面にユーザー ID とパスワードを入力します。
2. [OK] を押します。
3. 認証が成功すると、製品の操作パネルのロックが解除されます。

✓ 関連情報

- [LDAP 認証方式を使用する](#)

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](#)
- [証明書とウェブブラウザによる設定について](#)
- [ウェブブラウザを使用してネットワーク製品を安全に管理する](#)
- [SSL/TLS を使用して文書を安全に印刷する](#)

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はありません。

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/POP3/IMAP4 の SSL 通信（特定のモデルのみ可能）
- 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://KMNxxxxxxxxxxxx

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 バイト以下です。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。

HTTPサーバー設定

セキュリティの高い通信を行う設定が行われました。

設定を有効にするためには、デバイスを再起動する必要があります。

注意: この操作によって、現在実行中のジョブは中断されます。

再起動後に、その他のプロトコルにセキュアな設定を行う場合は、チェックをしてください。

☒ その他のプロトコルにセキュアな設定を行う

再起動を行ってもよろしいですか？

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](#)

■ ホーム > セキュリティ > ネットワークセキュリティ機能 > 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 > 証明書とウェブブラウザ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 > 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

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を使用する場合、そのブラウザ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。

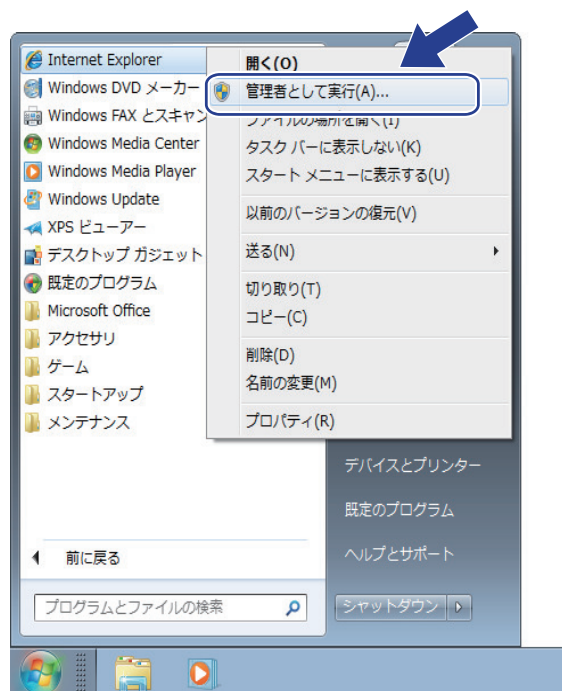
- (Windows® 10 および Windows Server® 2016)

 > 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。

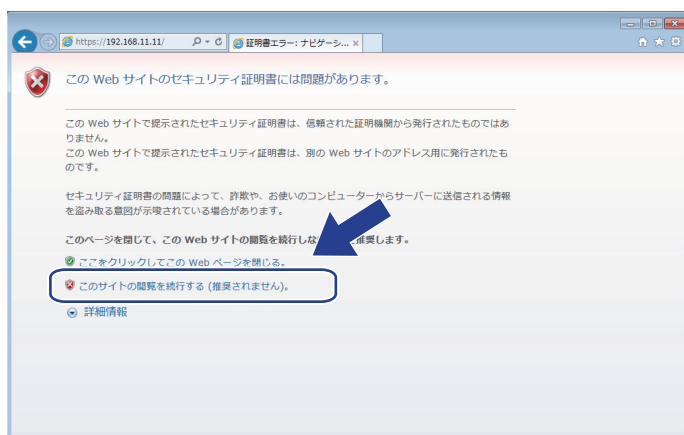


ユーザー アカウント制御画面が表示されたら、はいをクリックします。

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。



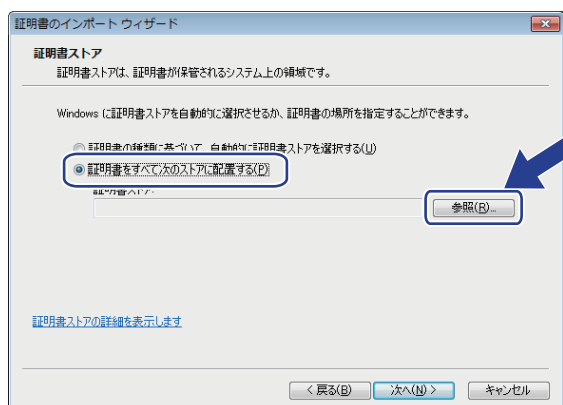
5. 証明書のエラーをクリックして、証明書の表示をクリックします。



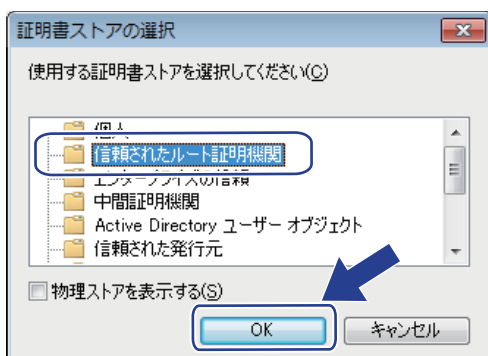
6. 証明書のインストール...をクリックします。



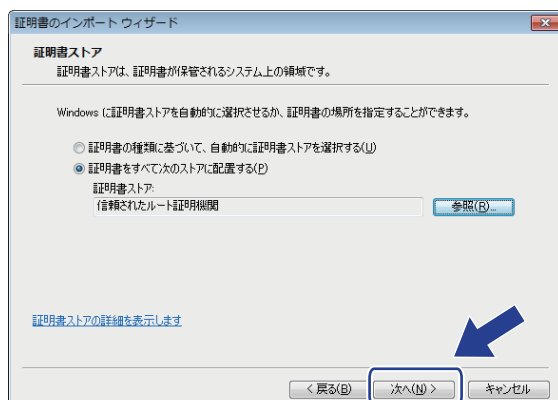
7. 証明書のインポート ウィザードが表示されたら、次へをクリックします。
8. 証明書をすべて次のストアに配置するを選択して、参照...をクリックします。



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](#)

■ [ホーム](#) > [セキュリティ](#) > [ネットワークセキュリティ機能](#) > [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](#) > [証明書とウェブブラウザ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](#) > [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](#)

■ ホーム > セキュリティ > ネットワークセキュリティ機能 > 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 > 証明書とウェブブラウザ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 > 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。 > 自己署名証明書をインポートする

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://KMNxxxxxxxxxxxx

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。

■ホーム > セキュリティ > ネットワークセキュリティ機能 > 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 > 証明書とウェブブラウザ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 > 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。 > 自己署名証明書をエクスポートする

自己署名証明書をエクスポートする

1. ウェブブラウザを起動します。
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://KMNxxxxxxxxxxxx

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**に表示される**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、**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. **保存**をクリックします。
11. 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

■ホーム > セキュリティ > ネットワークセキュリティ機能 > 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 > 証明書とウェブブラウザ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 > 認証局 (CA) からの証明書の作成とインストールについて > 証明書署名要求 (CSR : Certificate Signing Request) を作成する

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

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

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

1. ウェブブラウザを起動します。
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://KMNxxxxxxxxxxxx

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://KMNxxxxxxxxxxxx

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](#)

■ ホーム > セキュリティ > ネットワークセキュリティ機能 > 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 > 証明書とウェブブラウザ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 > 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

■ ホーム > セキュリティ > ネットワークセキュリティ機能 > SSL/TLS を使用したネットワーク製品の安全管理について > 証明書とウェブブラウザ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 > 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インポートする

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://KMNxxxxxxxxxxxx

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](#)

■ ホーム > セキュリティ > ネットワークセキュリティ機能 > SSL/TLS を使用したネットワーク製品の安全管理について > 証明書とウェブブラウザ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 > 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エクスポートする

証明書とプライベートキーをエクスポートする

1. ウェブブラウザを起動します。
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://KMNxxxxxxxxxxxx

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**に表示される**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. **保存**をクリックします。
11. 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](#)

■ ホーム > セキュリティ > ネットワークセキュリティ機能 > SSL/TLS を使用したネットワーク製品の安全管理について > 証明書とウェブブラウザ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 > 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://KMNxxxxxxxxxxxx

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**をクリックします。
8. インポートするファイルを表示します。
9. **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://KMNxxxxxxxxxxxx

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	6
CA 証明書	9

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、IEEE 802.1x、または署名済み PDF 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/POP3/IMAP4 通信に SSL を使用する場合（特定モデルにのみ対応）、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による設定について](#)


ウェブブラウザ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。



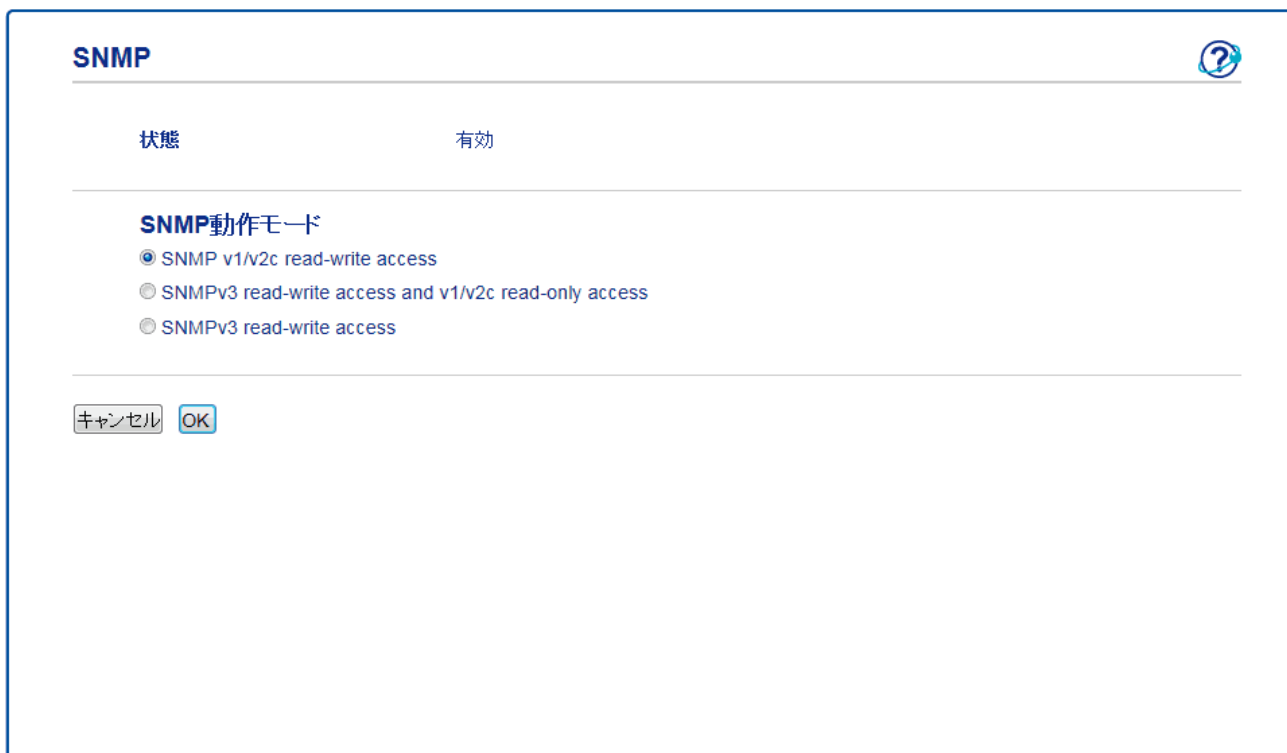
- お買い上げ時の設定では、HTTPS プロトコルは有効です。
- ウェブブラウザによる設定画面で HTTPS プロトコルの設定を変更できます。
 1. **ネットワーク**タブをクリックします。
 2. 左側にあるナビゲーションバーの**プロトコル**メニューをクリックします。
 3. **HTTP サーバー設定**をクリックします。

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://KMNxxxxxxxxxxxxx

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. **IPP で 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
- ウェブブラウザを使用して IPsec を設定する
- ウェブブラウザを使用して IPsec アドレステンプレートを設定する
- ウェブブラウザを使用して IPsec テンプレートを設定する

IPsec について

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

IPsec では、以下の機能をサポートしています。

- IPsec 送信

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

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



IPsec 送信には、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](#)

ウェブブラウザを使用して IPsec を設定する

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

1. ウェブブラウザを起動します。
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。

IPsec

状態

☐有効 ☒無効

接続モード

☒メイン ☐アグレッシブ

IPsec以外のトラフィックルール

☒通過 ☐遮断

Broadcast/Multicast Bypass

☒有効 ☐無効

Protocol Bypass

☒DNS ☒DHCP

ルール

No.	有効	テンプレート	
		アドレス	IPsec
1	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
2	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
3	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
4	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
5	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
6	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
7	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
8	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
9	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
10	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>

テンプレートの追加>>

テンプレートの追加>>

キャンセル

OK

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、**IPsec 以外のトラフィックルール**に対して**通過**を選択する必要があります。**遮断**を選択すると、Web サービスは使用できません。

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 **OK** 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。

IPsecアドレステンプレート 1

テンプレート名

ローカルIPアドレス

- ☒ IPアドレス
- ☐ IPアドレス範囲
- ☐ IPアドレスプレフィックス

すべてのIPv4アドレス 

リモートIPアドレス

- ☒ すべて
- ☐ IPアドレス
- ☐ IPアドレス範囲
- ☐ IPアドレスプレフィックス

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。




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



関連情報

- [IPsec を使用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. **テンプレートを使用する**ドロップダウンリストで**カスタム**を選択した場合、**IKE** を選択してから、必要に応じて設定値を変更します。
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>>](#)



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](#)

■ ホーム > セキュリティ > ネットワークセキュリティ機能 > 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 IKEv1 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>>](#)

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。



初期値のテンプレートは、**IPsec** 設定画面の **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** または **AH+ESP** を選択します。



- ESP は、IPsec を使用して暗号化通信を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 (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。

プロトコルで **AH+ESP** が選択されている場合、**ハッシュ (ESP)** と**ハッシュ(AH)**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 の期限が切れる前に、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、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

- [ウェブブラウザを使用して IPsec テンプレートを設定する](#)

■ ホーム > セキュリティ > ネットワークセキュリティ機能 > 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

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 秒
(240 – 63072000)

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 秒
(120 – 4233600)

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
ID

リモート

IDタイプ
ID

[証明書>>](#)

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 の期限が切れる前に、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、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。



関連情報

- [ウェブブラウザを使用して IPsec テンプレートを設定する](#)

IPsec テンプレートの手動設定

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

認証キー(ESP, AH)

In

Out

コードキー(ESP)

In

Out

SPI

In

256

Out

256

動作セキュリティ

プロトコル

☒ ESP ☐ AH

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

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** がで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 の期限が切れる前に、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。



関連情報

- [ウェブブラウザを使用して IPsec テンプレートを設定する](#)

安全な E-mail の送受信について

- ウェブブラウザ設定を使用して E-mail の送受信を設定する
- ユーザー認証を使って E メールを送信する
- SSL/ TLS を使用した E-mail セキュリティの送信または受信について

ウェブブラウザ設定を使用して E-mail の送受信を設定する

ユーザー認証済みの安全な E-mail 送信や、SSL/TLS を使用した E-mail 送信を、ウェブブラウザ設定を使用して設定することを推奨します。

1. ウェブブラウザを起動します。
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://KMNxxxxxxxxxxxx

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。
 - POP3/IMAP4/SMTP サーバーの設定値が不明の場合は、ネットワーク管理者またはインターネットサービスプロバイダー（ISP）にお問い合わせください。
8. 設定の完了後、**OK** をクリックします。
E メール送信／受信設定のテストの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 の送受信について](#)

ユーザー認証を使って E メールを送信する

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。

SMTP-AUTH を使用して、E メール通知、E メールレポート、および I-Fax を送信することができます。



ウェブブラウザを使用して 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、ウェブブラウザ設定の **SMTP** 画面の**送信メールサーバー認証方式**で、**SMTP-AUTH** を選択する必要があります。



関連情報

- [安全な E-mail の送受信について](#)

SSL/ TLS を使用した E-mail セキュリティの送信または受信について

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 の送受信を行います。SSL/TLS 通信を使用している E-mail サーバーを経由して E-mail を送受信するには、SSL/TLS 経由の SMTP、SSL/TLS 経由の POP3、または SSL/TLS 経由の IMAP4 を設定する必要があります。



ウェブブラウザ設定を使用して SSL/TLS を設定することを推奨します。

サーバー証明書を検証する

SSL/TLS で、SSL または TLS を選択した場合、**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。

SMTP

状態	有効
Eメール送信設定(SMTP)	
メールサーバー	<input type="text" value="0.0.0.0"/>
ポート	<input type="text" value="25"/>
送信メールサーバー認証方式	<input checked="" type="radio"/> なし <input type="radio"/> SMTP-AUTH
SMTP-AUTHアカウント名	<input type="text"/>
SMTP-AUTHアカウントパスワード	
パスワード設定	<input type="text"/>
パスワード確認	<input type="text"/>
SSL/TLS	<input checked="" type="radio"/> なし <input type="radio"/> SSL <input type="radio"/> TLS <input type="checkbox"/> サーバー証明書を検証
デバイスのEメールアドレス	<input type="text" value="knnXXXXXXXXXX@example.com"/>

[CA証明書](#)
[Eメール通達\(メンテナンス情報\)](#)
[エラー通達](#)



- 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 の送受信について](#)

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（サブリカント）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問い合わせてください。複数の証明書をインストールした場合、使用する証明書の名前を書き留めておくことをお勧めします。
- サーバー証明書を検証する前に、該当のサーバー証明書に署名した CA 発行の、CA 証明書をインポートする必要があります。ネットワーク管理者または契約しているインターネットサービスプロバイダー（ISP）にお問い合わせください。



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（無線ネットワーク）
- Drivers & Utilities CD 上の無線セットアップウィザード（無線ネットワーク）

1. ウェブブラウザを起動します。
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://KMNxxxxxxxxxxxxx

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	有線タブをクリックし、左側のナビゲーションバーで 有線 802.1x 認証 を選択します。
無線 LAN	無線タブをクリックし、左側のナビゲーションバーで 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）、**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。
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を確認する検証方法。 ¹

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
- ウェブブラウザを使用して印刷ログ機能の設定値を設定する
- 印刷ログ機能のエラー検出設定を使用する
- セキュリティ制限機能がアクティブな場合の印刷ログ機能の使用について

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
- USB ダイレクト印刷
- コピー
- 受信ファクス




- 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。SNTP プロトコル(ネットワークタイムサーバー)を設定するか、認証のために操作パネルで日時とタイムゾーンを正確に設定する必要があります。
- ファイルをサーバーに保存する際に、ファイルタイプを TXT または CSV に設定できます。





関連情報

- [印刷ログ機能](#)

ウェブブラウザ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	<p>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。</p> <ul style="list-style-type: none">• 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。 <p> Kerberos および NTLMv2 認証の場合、時計設定設定または、SNTP プロトコル (ネットワークタイムサーバー) と DNS サーバーも設定する必要があります。</p> <p>• 操作パネルから、[時計セット] も設定する必要があります。</p>
ユーザー名	<p>認証のためのユーザー名を入力します (最大 96 文字)。</p> <p> 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。</p>
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. 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。
6. 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。



印刷中止を選択した場合でも、本製品は受信ファクスを印刷します。

ログを書き込まずに印刷	ログを書き込まずに印刷を選択すると、印刷ログがサーバーに保存できない場合でも、本製品は文書を印刷します。 印刷ログ機能が回復すると、印刷ログは以下のように記録されます。
-------------	---

```
Id, Type, Job Name, User Name, Date, Time, Print Pages  
1, Print(xxxxxxx), "Document01.doc", "user01", 03/03/20xx, 14:01:32, 52  
2, Print(xxxxxxx), "Document02.doc", "user01", 03/03/20xx, 14:45:30, ?  
3, <ERROR>, ?, ?, ?, ?, ?  
4, Print(xxxxxxx), "Report01.xls", "user02", 03/03/20xx, 19:30:40, 4
```

- 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。

7. **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。
8. 製品が設定値をテストします。
9. 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

セキュリティ制限機能がアクティブな場合の印刷ログ機能の使用について

セキュリティ機能ロック 3.0 がアクティブな場合、コピー、ファクス受信、および USB ダイレクト印刷（利用可能な場合）のための登録ユーザーの名前が、印刷ログ機能レポートに記録されます。Active Directory® が有効の場合、ログインユーザーの名前が、印刷ログ機能レポートに記録されます。

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

✓ 関連情報

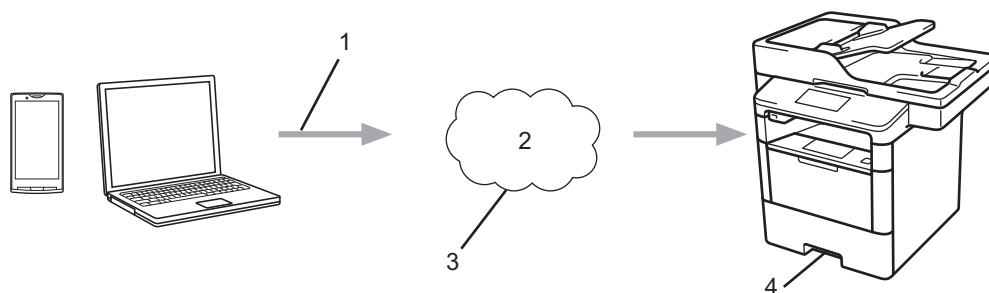
- 印刷ログ機能

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へ印刷することができます。



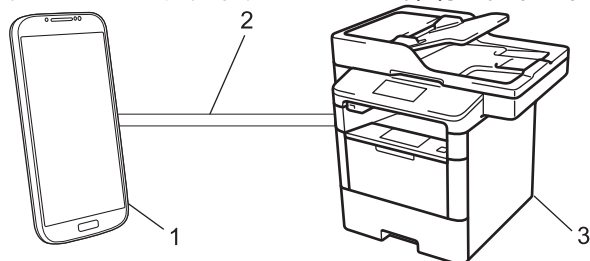
1. 印刷リクエスト
2. インターネット
3. Google クラウド プリント™
4. 印刷

✓ 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™ 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。

- 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](#)

ControlCenter

本製品の ControlCenter ソフトウェアを使用して、頻繁に使用するアプリケーションに簡単にアクセスできます。ControlCenter を使えば、特定のアプリケーションを直接起動することが可能です。

- [ControlCenter4 \(Windows®\)](#)

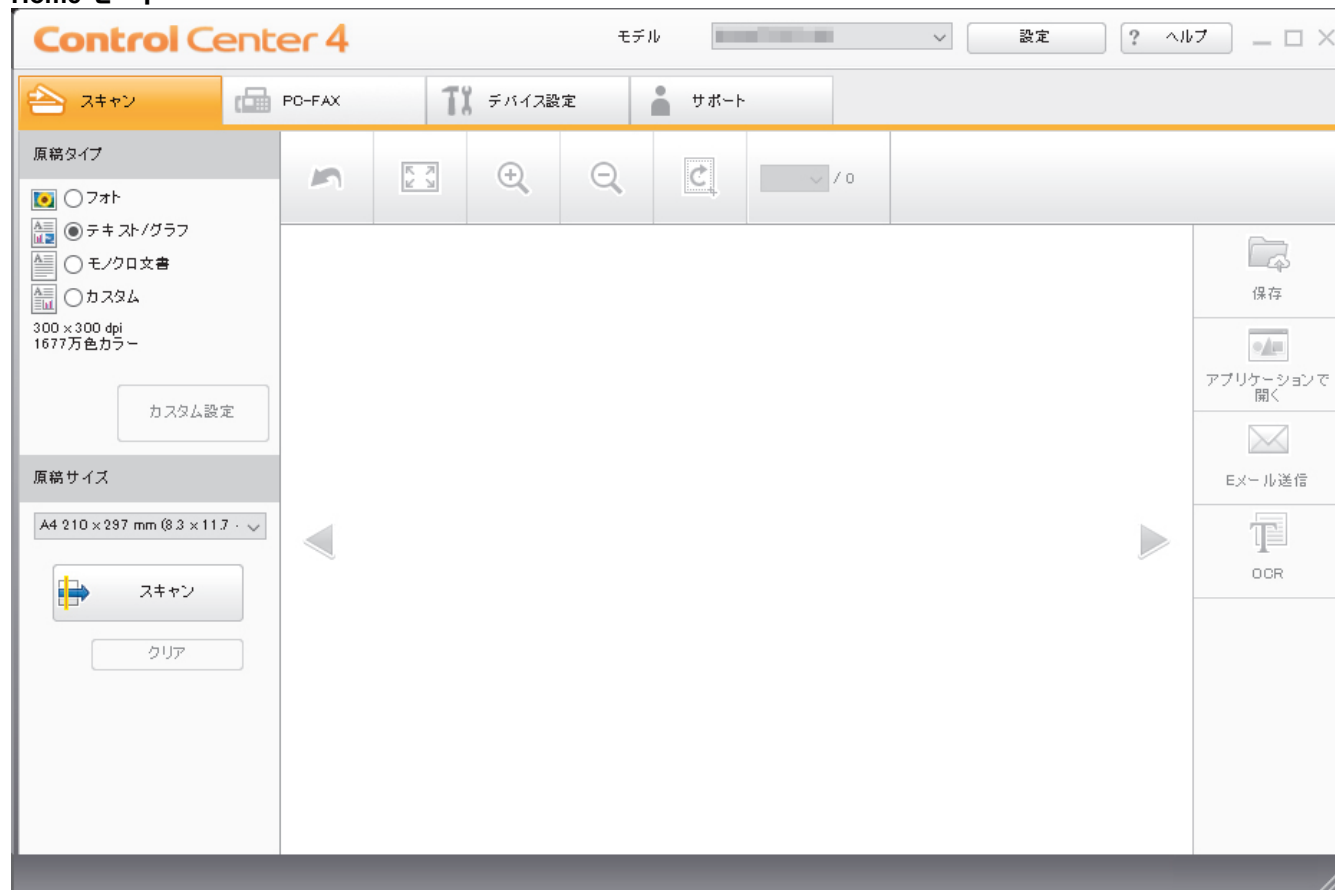
ControlCenter4 (Windows®)

- [ControlCenter4 の操作モードを変更する\(Windows®\)](#)
- [ControlCenter4 Home モードを使ってスキャンする \(Windows®\)](#)
- [ControlCenter4 Advanced モードを使ってスキャンする \(Windows®\)](#)
- [ControlCenter4 を使って本製品のセットアップを行う \(Windows®\)](#)
- [ControlCenter4 Advanced モードを使用してカスタムタブを作成する \(Windows®\)](#)

ControlCenter4 の操作モードを変更する(Windows®)

ControlCenter4 には、Home モードおよび Advanced モードの、2 つの操作モードがあります。モードはいつでも変更可能です。

Home モード



Advanced モード




Home モード

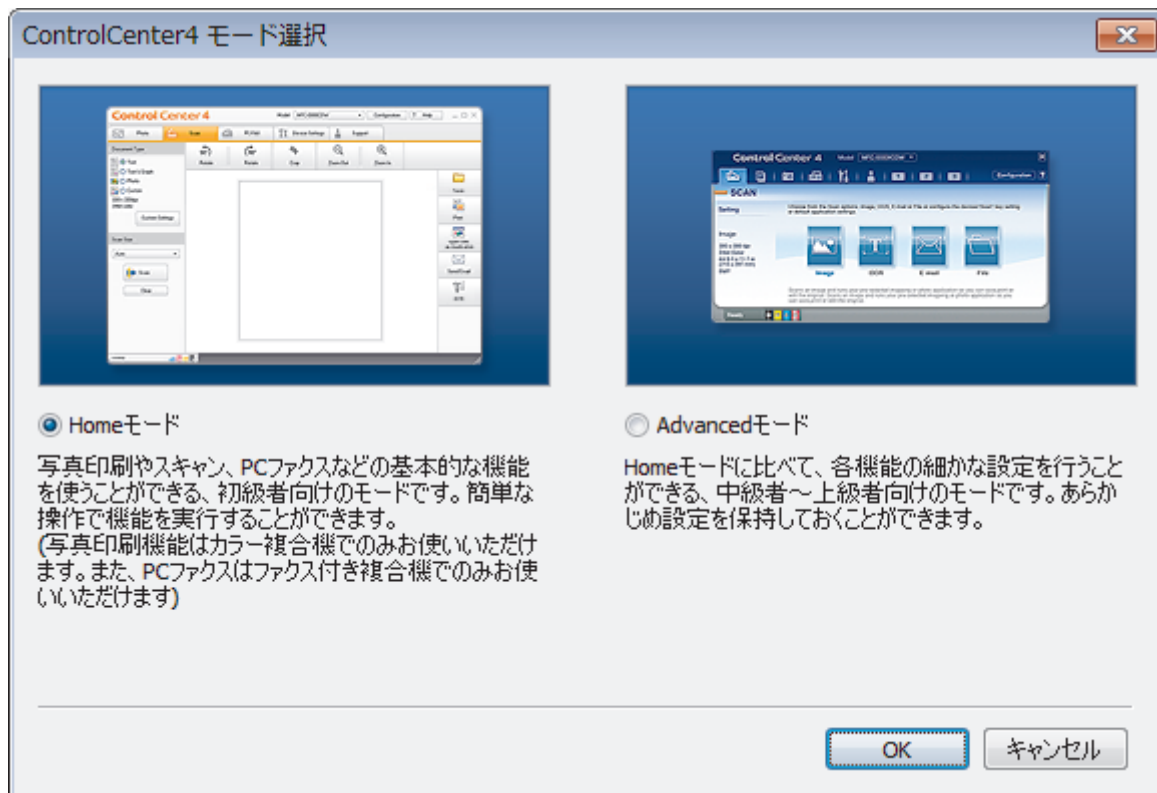
ControlCenter4 Home モードから、本製品の主要な機能を操作することが可能です。

- **Advanced モード**

ControlCenter4 Advanced モードでは、本製品のより詳細な機能进行操作して、ワンタッチのスキャン操作に変更することができます。

操作モードを変更するには：

1. タスクトレイの  (**ControlCenter4**) アイコンをクリックし、**開く**を選択します。
2. **設定**ボタンをクリックし、**モード選択**を選択します。
3. モード選択ダイアログボックスが表示されます。**Home モード**または **Advanced モード**のどちらかを選択します。



4. **OK** をクリックします。



関連情報

- [ControlCenter4 \(Windows®\)](#)

ControlCenter4 Home モードを使ってスキャンする (Windows®)

ControlCenter4 Home モードから、本製品の主要な機能进行操作できます。

- [ControlCenter4 Home モードのスキャン \(Windows®\)](#)
- [ControlCenter4 Home モードを使ってスキャンしたデータを PDF ファイルとして保存する\(Windows®\)](#)
- [ControlCenter4 Home モードのスキャン設定 \(Windows®\)](#)

ControlCenter4 Advanced モードを使ってスキャンする (Windows®)


ControlCenter4 Advanced モードでは、本製品のより詳細な機能进行操作して、ワンタッチのスキャン操作に変更することができます。

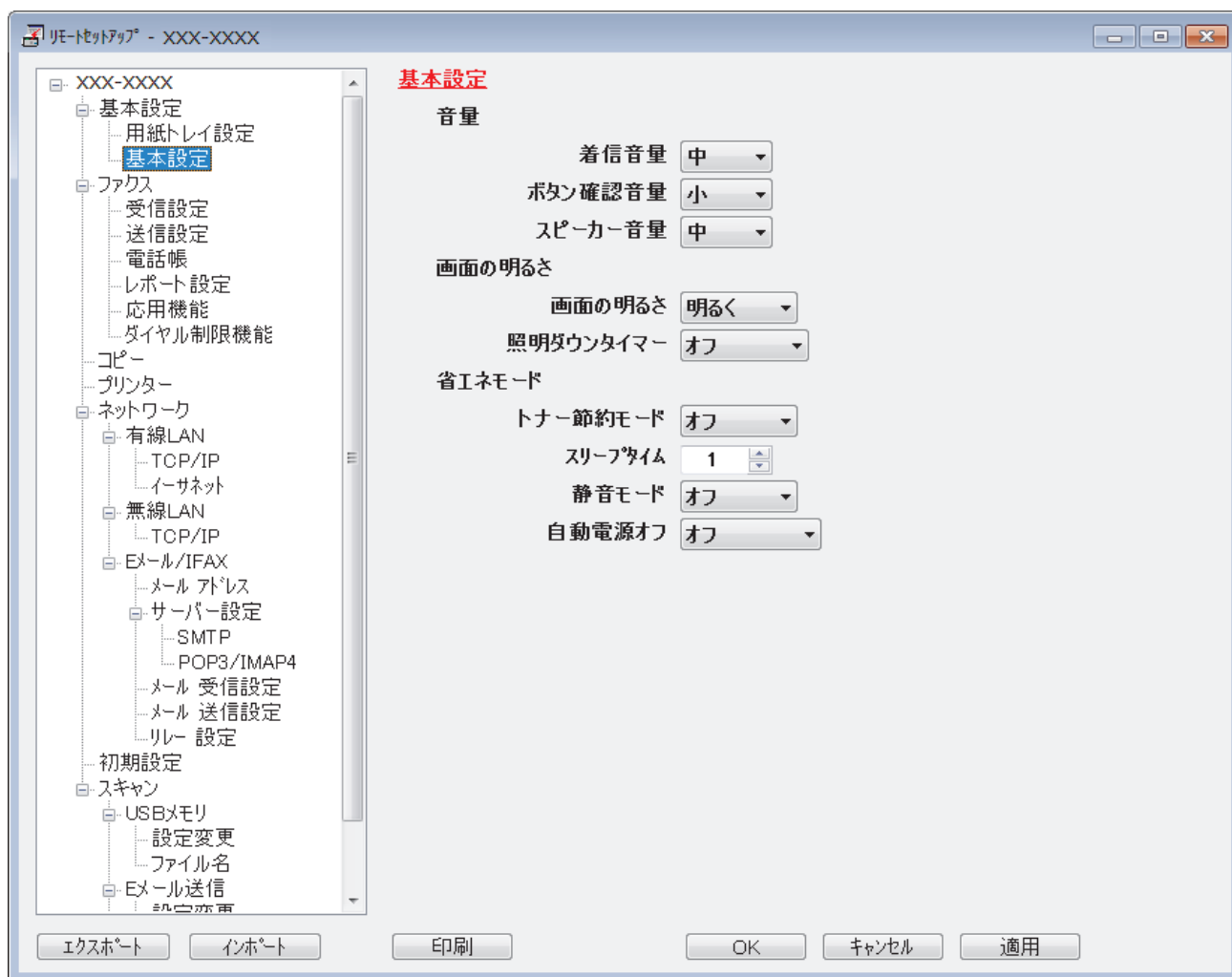
- [ControlCenter4 Advanced モードを使って、写真やグラフィックをスキャンする \(Windows®\)](#)
- [ControlCenter4 Advanced モード \(Windows®\) を使用して、スキャンデータを PDF ファイルとしてフォルダーに保存する](#)
- [ControlCenter4 Advanced モードを使って、ID カードの両面をスキャンする \(Windows®\)](#)
- [ControlCenter4 Advanced モードを使用したスキャン to E メール添付 \(Windows®\)](#)
- [ControlCenter4 Advanced モード \(Windows\) を使用したスキャン to 編集可能テキストファイル \(OCR\)](#)
- [ControlCenter4 Advanced モードのスキャン設定 \(Windows®\)](#)

ControlCenter4 を使って本製品のセットアップを行う (Windows®)



セキュリティ機能ロックがオンに設定されている場合、リモートセットアップは使用できません。

1. タスクトレイの  (ControlCenter4)アイコンをクリックし、**開く**をクリックします。
2. **デバイス設定**タブをクリックします。
3. **リモートセットアップ**ボタンをクリックします。
4. 必要に応じて設定を行います。



エクスポート

クリックすると、現在の設定をファイルに保存します。



エクスポートをクリックすると、本製品のアドレス帳または本製品のすべての設定値の保存ができます。

インポート

クリックしてファイルをインポートし、設定値を読み込みます。

印刷

クリックすると、選択した項目の設定を印刷します。ただし、データが本製品に送信されるまでは、印刷できません。**適用**をクリックして、新しいデータを本製品に送信してから、**印刷**をクリックしてください。

OK

クリックすると、本製品へデータを送信し、リモートセットアップを終了します。エラーメッセージが表示された場合は、正しいデータを再度入力し、**OK** をクリックします。

キャンセル

クリックすると、設定内容を本製品へ送信せずに、リモートセットアップを終了します。

適用

クリックすると、設定内容を本製品へ送信します。

5. **OK** をクリックします。

- お使いのパソコンがファイアウォールにより保護されているためリモートセットアップが使用できない場合は、ファイアウォールの設定をポート番号 137 および 161 経由の通信を許可するように変更してください。
- Windows® ファイアウォールを使用し、プリンタードライバーとソフトウェアを Drivers & Utilities CD からインストールした場合は、必要なファイアウォールはすでに設定されています。




関連情報

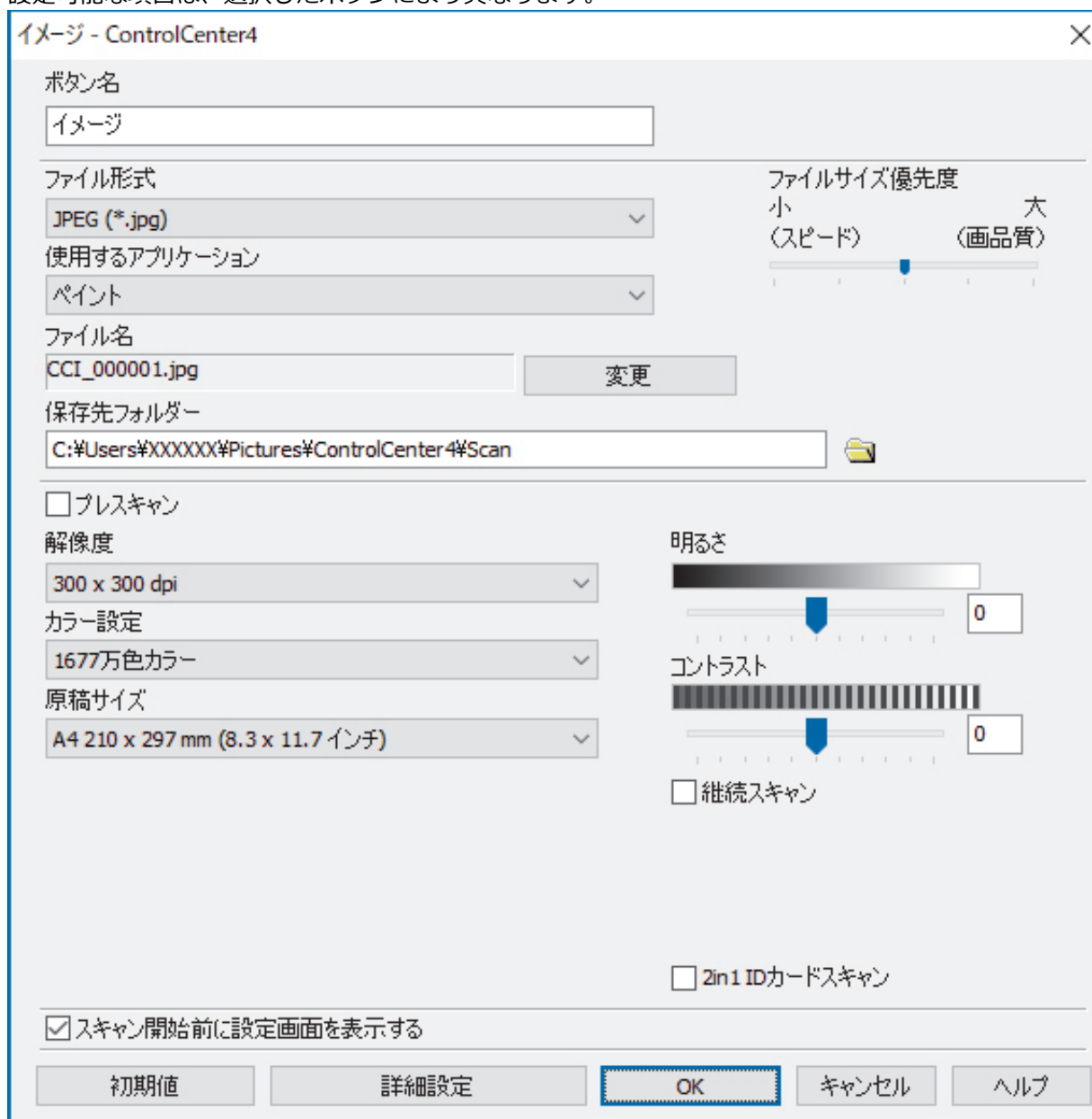
- [ControlCenter4 \(Windows®\)](#)
- [リモートセットアップ\(Windows®\)](#)

ControlCenter4 Advanced モードを使用してカスタムタブを作成する (Windows®)

最大 3 個のタブをカスタマイズでき、各タブには、最大 5 個のカスタマイズしたボタンと設定を表示できます。

ControlCenter4 のモード設定で **Advanced モード** を選択します。

1. タスクトレイの  (ControlCenter4) アイコンをクリックし、**開く** をクリックします。
2. **設定** ボタンをクリックして、**カスタムタブの作成** を選択します。
カスタムタブが作成されます。
3. カスタムタブの名称を変更するには、カスタムタブを右クリックし、**カスタムタブの名前変更** を選択します。
4. **設定** をクリックして、**カスタムボタンの作成** を選択し、作成するボタンを選択します。
設定値のダイアログボックスが表示されます。
5. 必要に応じて、ボタン名を入力して設定を変更します。**OK** をクリックします。
設定可能な項目は、選択したボタンにより異なります。



イメージ - ControlCenter4

ボタン名
イメージ

ファイル形式
JPEG (*.jpg)

使用するアプリケーション
ペイント

ファイル名
CCI_000001.jpg 変更

保存先フォルダー
C:\Users\XXXXXX\Pictures\ControlCenter4\Scan

☐ プレスキャン

解像度
300 x 300 dpi

カラー設定
1677万色カラー

原稿サイズ
A4 210 x 297 mm (8.3 x 11.7 インチ)

明るさ
0

コントラスト
0

☐ 継続スキャン

☐ 2in1 IDカードスキャン

☒ スキャン開始前に設定画面を表示する

初期値 詳細設定 OK キャンセル ヘルプ



作成したタブ、ボタン、設定を変更または削除できます。**設定**ボタンをクリックして、操作してください。



関連情報

- [ControlCenter4 \(Windows®\)](#)

パソコンを使用して製品の設定を変更する

- ウェブブラウザを使用して製品の設定を変更する
- リモートセットアップ
- 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？
- ネットワーク管理ソフトウェアおよびユーティリティ

ウェブブラウザを使用して製品の設定を変更する

ウェブブラウザによる設定は、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を使用します。

- ウェブブラウザによる設定とは
- ウェブブラウザによる設定画面にアクセスする
- ウェブブラウザによる設定画面のログインパスワードを設定する
- ネットワーク管理ソフトウェアおよびユーティリティ

ウェブブラウザによる設定とは

ウェブブラウザによる設定は、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を使用します。ご使用のウェブブラウザに本製品の 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 のブラウザのご使用をお勧めします。いずれのウェブブラウザの場合も、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。

アドレス帳

このタブを使用して本製品のアドレス帳を編集します。

ファクス

このタブを使用して、ファクス設定の確認や変更、インターネットファクス（I-Fax）設定の変更を行います。

コピー

このタブを使用して、コピー設定の確認や変更を行います。

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。

スキャン

このタブを使用して、スキャン設定の確認や変更、スキャン to FTP および、スキャン to ネットワークプロファイルの作成を行います。

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

- [ウェブブラウザを使用して製品の設定を変更する](#)
-

ウェブブラウザによる設定画面にアクセスする

- ウェブブラウザ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。
- ウェブブラウザによる設定で HTTPS を使用する場合、お使いのブラウザ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://KMNxxxxxxxxxxxx

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](#)

ウェブブラウザによる設定画面のログインパスワードを設定する

認証されていないユーザーがウェブブラウザを使用した設定画面にアクセスするのを防ぐために、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://KMNxxxxxxxxxxxxx

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（8～32 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

- [ウェブブラウザを使用して製品の設定を変更する](#)

リモートセットアップ

リモートセットアッププログラムを使用すると、本製品の設定の多くをお使いのパソコンから行うことができます。このリモートセットアップを起動すると、本製品の設定値がお使いのパソコンにダウンロードされ、画面に表示されます。パソコンで設定を変更した場合、設定を本製品に直接アップロードすることが出来ます。

- ・ リモートセットアップ(Windows®)

リモートセットアップ(Windows®)

- パソコンから本製品を設定する(Windows®)
- ControlCenter4 を使って本製品のセットアップを行う (Windows®)
- ControlCenter4 (Windows®) を使用して本製品のアドレス帳を設定する

パソコンから本製品を設定する(Windows®)



セキュリティ機能ロックがオンに設定されている場合、リモートセットアップは使用できません。

1. 次のいずれかを行ってください。

- (Windows® 7)



(スタート) > すべてのプログラム > KONICA MINOLTA > KONICA MINOLTA Utilities をクリックします。

モデル名が選択されていない場合は、ドロップダウンリストをクリックして、お使いの製品のモデル名を選択します。左ナビゲーションバーの**ツール**をクリックし、さらに**リモートセットアップ**をクリックします。

- (Windows® 8.1 および Windows® 10)



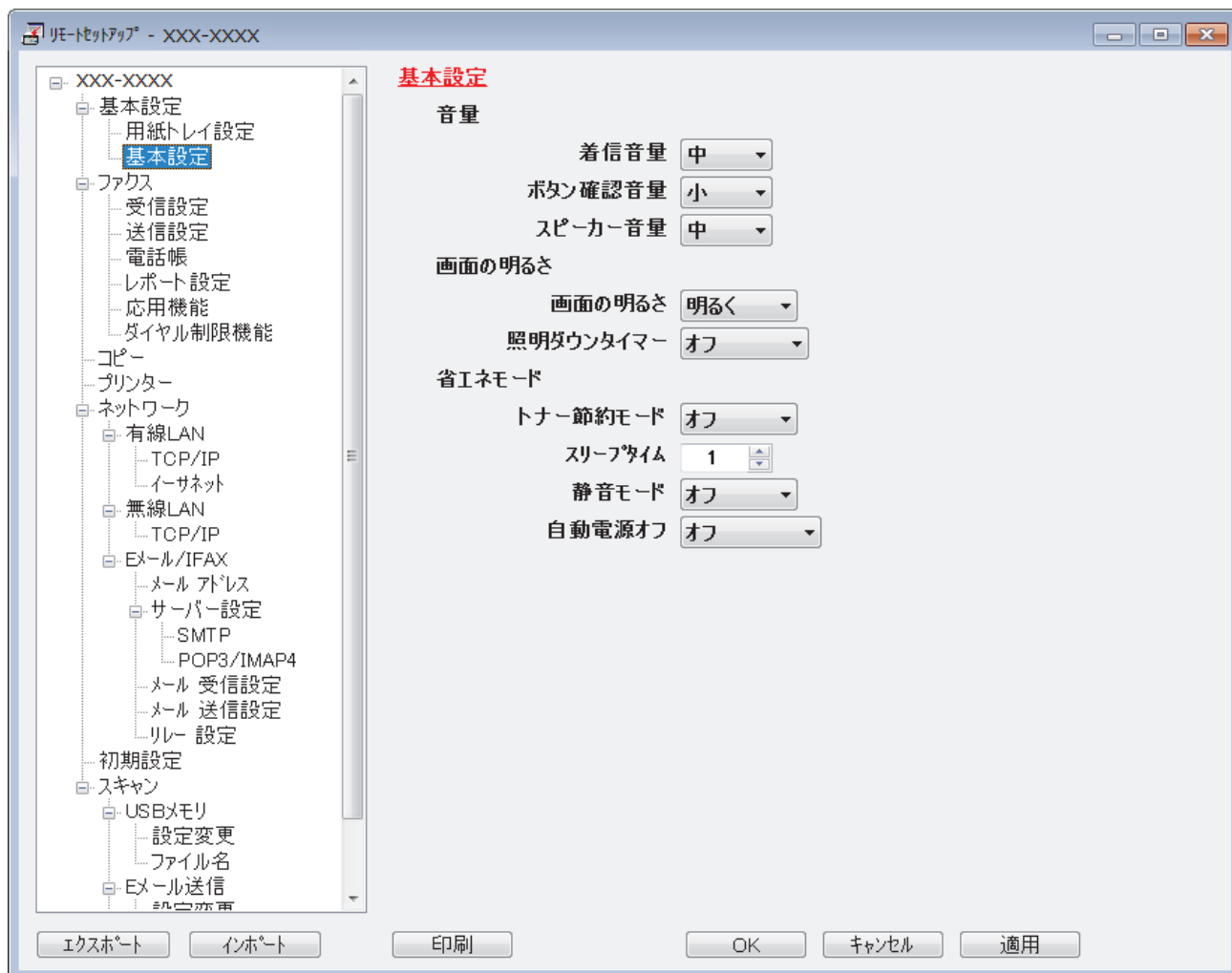
(KONICA MINOLTA Utilities) を起動し、モデル名が選択されていない場合は、ドロップダウンリストをクリックして、お使いの製品のモデル名を選択します。左ナビゲーションバーの**ツール**をクリックし、さらに**リモートセットアップ**をクリックします。

リモートセットアップの画面が表示されます。



本製品がネットワークを介して接続されている場合、必要に応じてパスワードを入力します。初期パスワードは、initpass です。

2. 必要に応じて設定を行います。



エクスポート

クリックすると、現在の設定をファイルに保存します。



エクスポートをクリックすると、本製品のアドレス帳または本製品のすべての設定値の保存ができます。

インポート

クリックしてファイルをインポートし、設定値を読み込みます。

印刷

クリックすると、選択した項目の設定を印刷します。ただし、データが本製品に送信されるまでは、印刷できません。**適用**をクリックして、新しいデータを本製品に送信してから、**印刷**をクリックしてください。

OK

クリックすると、本製品へデータを送信し、リモートセットアップを終了します。エラーメッセージが表示された場合は、正しいデータを再度入力し、**OK**をクリックします。

キャンセル

クリックすると、設定内容を本製品へ送信せずに、リモートセットアップを終了します。

適用

クリックすると、設定内容を本製品へ送信します。

3. **OK** をクリックします。

- お使いのパソコンがファイアウォールにより保護されているためリモートセットアップが使用できない場合は、ファイアウォールの設定をポート番号 137 および 161 経由の通信を許可するよう変更してください。
- Windows® ファイアウォールを使用し、プリンタードライバーとソフトウェアを Drivers & Utilities CD からインストールした場合は、必要なファイアウォールはすでに設定されています。



関連情報


- [リモートセットアップ\(Windows®\)](#)

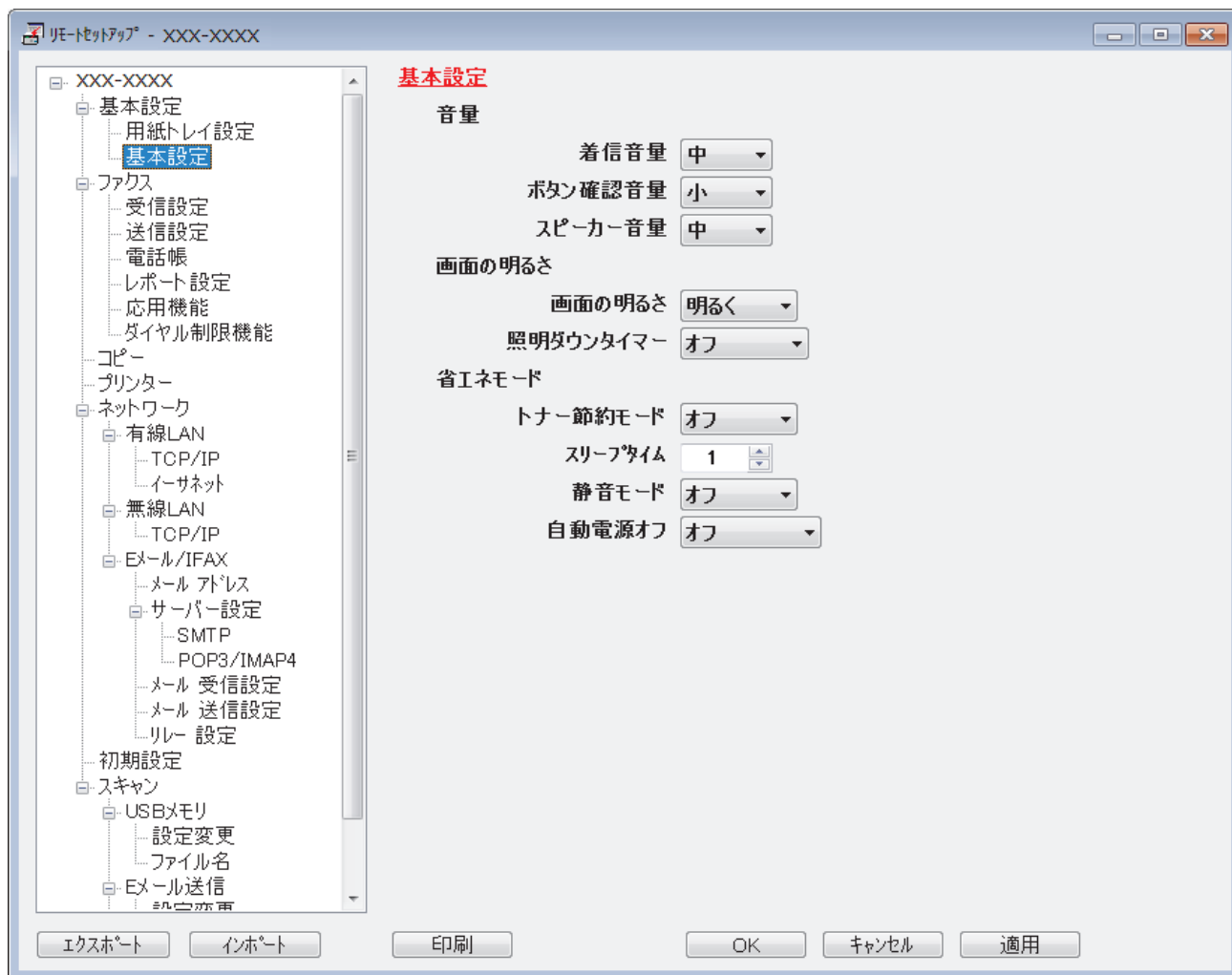
■ ホーム > パソコンを使用して製品の設定を変更する > リモートセットアップ > リモートセットアップ (Windows®) > ControlCenter4 を使って本製品のセットアップを行う (Windows®)

ControlCenter4 を使って本製品のセットアップを行う (Windows®)



セキュリティ機能ロックがオンに設定されている場合、リモートセットアップは使用できません。

1. タスクトレイの  (ControlCenter4)アイコンをクリックし、開くをクリックします。
2. デバイス設定タブをクリックします。
3. リモートセットアップボタンをクリックします。
4. 必要に応じて設定を行います。



エクスポート

クリックすると、現在の設定をファイルに保存します。



エクスポートをクリックすると、本製品のアドレス帳または本製品のすべての設定値の保存ができます。

インポート

クリックしてファイルをインポートし、設定値を読み込みます。

印刷

クリックすると、選択した項目の設定を印刷します。ただし、データが本製品に送信されるまでは、印刷できません。適用をクリックして、新しいデータを本製品に送信してから、印刷をクリックしてください。

OK

クリックすると、本製品へデータを送信し、リモートセットアップを終了します。エラーメッセージが表示された場合は、正しいデータを再度入力し、**OK** をクリックします。

キャンセル

クリックすると、設定内容を本製品へ送信せずに、リモートセットアップを終了します。

適用

クリックすると、設定内容を本製品へ送信します。

5. **OK** をクリックします。

- お使いのパソコンがファイアウォールにより保護されているためリモートセットアップが使用できない場合は、ファイアウォールの設定をポート番号 137 および 161 経由の通信を許可するように変更してください。
- Windows® ファイアウォールを使用し、プリンタードライバーとソフトウェアを Drivers & Utilities CD からインストールした場合は、必要なファイアウォールはすでに設定されています。



関連情報

- [ControlCenter4 \(Windows®\)](#)
- [リモートセットアップ\(Windows®\)](#)


■ ホーム > パソコンを使用して製品の設定を変更する > リモートセットアップ > リモートセットアップ (Windows®) > ControlCenter4 (Windows®) を使用して本製品のアドレス帳を設定する

ControlCenter4 (Windows®) を使用して本製品のアドレス帳を設定する

ControlCenter4 経由でリモートセットアップを使用して、お使いのパソコンから電話帳の番号を追加または変更します。



セキュリティ機能ロックがオンに設定されている場合、リモートセットアップは使用できません。

1. タスクトレイの  (ControlCenter4) アイコンをクリックし、**開く** をクリックします。
2. **デバイス設定** タブをクリックします。
3. **電話帳 / アドレス帳** ボタンをクリックします。
リモートセットアップ画面の、**電話帳** が開きます。
4. 必要に応じて、電話帳の情報を追加または更新します。
5. **OK** をクリックします。



本製品がネットワークを介して接続されている場合、必要に応じてパスワードを入力します。初期パスワードは、initpass です。



関連情報

- ・ リモートセットアップ(Windows®)

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 ら

アルファベット

- Active Directory®認証
- ADF (自動原稿送り装置)
- AES
- APIPA
- APOP
- ARP
- BOOTP
- CA
- CA 証明書
- CIFS
- CSR
- Custom Raw Port
- DHCP
- DNS サーバー
- DNS クライアント
- FTP
- HTTP
- HTTPS
- IEEE 802.1x
- IPP

- [IPPS](#)
- [IPsec](#)
- [IPv6](#)
- [IP アドレス](#)
- [LEAP](#)
- [LLMNR](#)
- [LPD](#)
- [LPR](#)
- [MAC アドレス](#)
- [MDN](#)
- [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](#)

■ ホーム > 用語集

- [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](#)
- [インターネットファクス](#)
- [インフラストラクチャ \(Infrastructure\) 通信](#)
- [ウェブブラウザ設定](#)
- [オープンシステム](#)

か

- [共有鍵暗号システム](#)
- [検索](#)
- [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](#)
- [スキャン](#)
- [スキャン to E メールサーバー](#)

- ・ [セキュリティ機能ロック 3.0](#)

た

- ・ [チャンネル](#)
- ・ [デジタル署名](#)

な

- ・ [認証](#)
- ・ [ネットワーク PC-FAX](#)
- ・ [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](#)
- ・ [ネットワークリモートセットアップ](#)
- ・ [濃度](#)
- ・ [ノード名](#)

は

- ・ [ピアツーピア](#)
- ・ [プロトコル](#)

ま

- ・ [無線 LAN レポート](#)

ら

- ・ [リモートセットアップ](#)

Active Directory®認証

Active Directory®認証により、本製品の使用が制限されます。ユーザー ID とパスワードを使用して本製品にログインするまで、本製品を使用することはできません。

ADF (自動原稿送り装置)

原稿を ADF (自動原稿送り装置)にセットし、1 ページごとに自動的にスキャンが可能です。

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。

APOP

Authenticated Post Office Protocol(APOP)は、POP3 (インターネット E メール受信プロトコル) を拡張し、クライアントが E メールを受信するときに用いるパスワードを暗号化する認証方法を取り入れたものです。

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リスク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たし、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。

FTP

File Transfer Protocol(FTP)は、本製品がモノクロまたはカラー原稿のスキャンデータを、ローカルのネットワーク上またはインターネット上にある FTP サーバーに直接送ることができます。

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。

MDN

操作パネルメニューの Message Disposition Notification (MDN) 欄は、簡易メール転送プロトコル (SMTP) の転送システムを介した送信のあと、インターネットファクス/メールの状態を要求します。

受信側にメッセージが到着すると、本製品またはユーザーが受信インターネットファクスまたは E メールを読む場合または印刷する場合に、このデータが使用されます。

相手機のユーザーが、受信したインターネットファクスまたは E メールの内容を読んだり、出力したりするために E メールメッセージを開くと、相手機は送信元に受信確認を送付します。



相手機は通知レポートを送信できる MDN に対応している必要があります。そうでない場合は、受信確認リクエストは無視されます。

mDNS

Multicast 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

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。

インターネットファクス

インターネットファクス (I-Fax) は、インターネットを使ってファクスメッセージを送受信する機能です。この機能を使用する前に、本製品の操作パネルから必要な設定を行います。

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。

ウェブブラウザ設定

お使いの標準ウェブブラウザで、HTTP (ハイパーテキスト転送プロトコル) を使用して、ネットワークに接続されている本製品を管理することができます。ウェブブラウザを使用して、次のような情報を本製品から取得できます。

- 本製品の状態、メンテナンスに関する詳細情報の取得
- 送受信や応用機能などのファクス設定
- TCP/IP などのネットワーク設定変更
- セキュリティ機能ロックの設定
- ネットワークへの印刷ログの保存を設定する
- スキャン to FTP の設定
- スキャン to ネットワークの設定
- LDAP の設定 (特定のモデルのみ対応)
- 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
- ネットワークと本製品の詳細設定



ウェブブラウザ設定を使用するには、TCP/IP プロトコルによってパソコンがネットワーク接続されていることを確認してください。

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。

検索

保存されたアドレス帳およびグループ番号のアルファベット順の電子リスト。

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。

スキャン

紙原稿の電子画像をパソコンに送信するプロセス。

スキャン to E メールサーバー

スキャン to E メールサーバー機能では、モノクロまたはカラー原稿をスキャンして、本製品から直接 E メールサーバーへ送信することができます。

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。

デジタル署名

データの受信者がデータの正当性を確認するための情報です。暗号アルゴリズムで計算される値で、データオブジェクトに付加されます。

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 PC-FAX

お使いのパソコンからファクスとしてファイルを送りたいときに、ネットワーク PC-FAX を使用します。Windows®ユーザーは、PC-FAX でファクスを受信することもできます。

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、各パソコン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。

ネットワークリモートセットアップ

リモートセットアップソフトウェアでは、Windows®からネットワーク設定を行うことができます。

濃度

濃度を変更することにより、画像の全体的な明暗を調整できます。

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 [KMNxxxxxxxxxxxx]、無線 LAN の場合は [KMWxxxxxxxxxxxx] となっています。（「xxxxxxxxxxxx」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

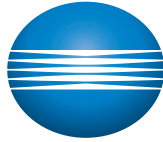
プロトコルは、ネットワーク上でデータを送信するための、標準化された一連の規則です。ユーザーはプロトコルを使用して、ネットワーク接続されたリソースにアクセスできます。本製品で使用されているプリントサーバーは、転送制御プロトコル/インターネットプロトコル（TCP/IP : Transmission Control Protocol/Internet Protocol）をサポートしています。

■ 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。

■ リモートセットアップ

リモートセットアップでは、パソコンから簡単に本製品の設定を行うことができます。このアプリケーションを起動すると、本製品の設定値がお使いのパソコンに自動的にダウンロードされ、パソコン画面に表示されます。リモートセットアップで設定した内容は、次に変更するまで有効です。



KONICA MINOLTA