brother

ユーザーズガイド
ネットワーク編

Version C

JPN

目次

4 ウェブブラウザーによる管理 38

5 スキャン to E メール 60

6 セキュリティ機能 64

1 はじめに

ネットワーク機能

本製品は、内部ネットワーク上のスキャンサーバーを利用して、IEEE 802.11b/g/n 無線イーサネットネットワーク上で共有することができます。スキャンサーバーは、お使いのオペレーティングシステムやネットワークの設定に応じて、さまざまな機能や接続方法に対応します。次の表では、各オペレーティングシステムで対応しているネットワーク機能と接続方法を示します。

オペレーティングシステム	Windows® XP 32 ビット（SP3） Windows Vista® Windows® 7 Windows® 8 Windows® 8.1、Windows® 10 Windows Server® 2003 R2 32 ビット（SP2） Windows Server® 2008 Windows Server® 2008 R2 Windows Server® 2012 Windows Server® 2012 R2 （サーバー OS で対応しているのはスキャンのみ）	OS X v10.8.5、10.9.x、10.10.x、10.11.x
スキャン *ユーザーズガイド*をご覧ください。	✔	✔
BRAdmin Light [1] *BRAdmin Light を使って設定する（Windows®）*（3 ページ）をご覧ください。	✔	
BRAdmin Professional 3 [2] *BRAdmin Professional 3 (Windows®)*（6 ページ）をご覧ください。	✔	
ウェブブラウザーによる管理 *ウェブブラウザーによる管理*（38 ページ）をご覧ください。	✔	✔
リモートセットアップ *ユーザーズガイド*をご覧ください。	✔	✔
ステータスモニター *ユーザーズガイド*をご覧ください。	✔	
Vertical Pairing *Vertical Pairing を使用したインフラストラクチャモードのネットワークスキャン用のインストール（Windows® 7、Windows® 8、Windows® 8.1、および Windows® 10）*（101 ページ）をご覧ください。	✔	

[1] BRAdmin Light はサポートサイト（ブラザーソリューションセンター（support.brother.co.jp/））からダウンロードできます。

[2] BRAdmin Professional 3 はサポートサイト（ブラザーソリューションセンター（support.brother.co.jp/））からダウンロードできます。

その他のネットワーク機能

LDAP

LDAP プロトコルを利用すると、コンピューター上の E メールアドレスなどの情報を検索できます。スキャン to E メール機能を使用するときに、LDAP 検索を使用して E メールアドレスを検索できます。（*本製品の操作パネルを使用した LDAP 設定の変更*（45 ページ）を参照してください。）

スキャン to E メール

スキャン to E メール機能を利用すると、インターネットを使用してスキャンデータを送信できます。（*スキャン to E メール*（60 ページ）を参照してください。）

この機能を使用するには、本製品の操作パネル、BRAdmin Professional 3、またはウェブブラウザーによる管理を通じて、本製品の必要な設定を行っておく必要があります。

セキュリティ

本製品は、最新のネットワークセキュリティと暗号化プロトコルに対応しています。（*セキュリティ機能*（64 ページ）を参照してください。）

Wi-Fi Direct®

Wi-Fi Direct® は、Wi-Fi Alliance® が策定した無線設定方法のひとつです。Wi-Fi 標準であるこのタイプの接続を利用すると、無線 LAN アクセスポイントなしでも、デバイス間の安全な相互接続を設定することができます。（*Wi-Fi Direct® を使用する*（31 ページ）を参照してください。）

2 ネットワークの設定を変更する

本製品のネットワーク設定を変更する

本製品のネットワーク設定は、操作パネル、BRAdmin Light、ウェブブラウザー、または BRAdmin Professional 3 を使って変更できます。

製品の操作パネルを使って設定する

操作パネルのメニューより、本製品のネットワーク機能を設定できます。

ネットワーク接続状態を確認する方法

1. 本製品の液晶画面で、 を押します。
2. ［ネットワーク］を押します。
3. ［有線 LAN］を押します。
4. ［有線 LAN 状態］を押します。
5. ［接続状態］を押します。

BRAdmin Light を使って設定する（Windows®）

BRAdmin Light は、ネットワークに接続されたブラザー製品のセットアップを行うユーティリティです。このユーティリティを使用すると、TCP/IP 環境内にあるブラザー製品を検索したり、接続状態を確認したり、IP アドレスなどの基本的なネットワーク設定を行ったりすることもでき ます。

BRAdmin Light をインストールする

1. 本製品の電源が入っていることを確認します。
2. コンピューターの電源を入れます。実行中のアプリケーションをすべて終了します。
3. 付属のインストール用 DVD-ROM ディスクを DVD-ROM ドライブにセットします。
4. **(DVD ドライブ):\ ツール \BRAdminLight\xxx\DISK1\setup.exe** の順にダブルクリックします。

BRAdmin Light を使用して IP アドレス、サブネットマスク、およびゲートウェイを設定する

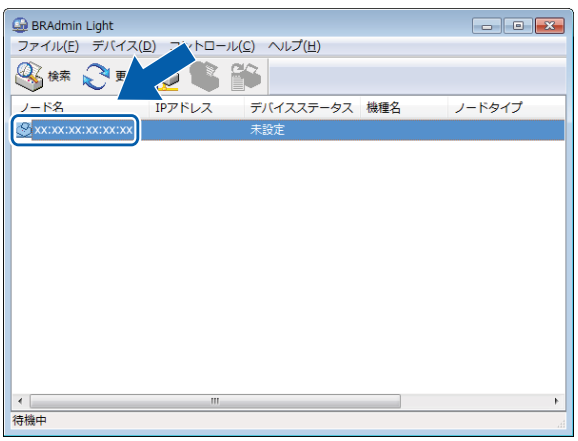
メモ

- 最新のブラザー BRAdmin Light を、サポートサイト（ブラザーソリューションセンター（support.brother.co.jp/））で、お使いの機種の**ソフトウェアダウンロード**ページからダウンロードしてください。
- さらに高度な製品管理を必要とする場合は、最新版の BRAdmin Professional 3 をご使用ください。BRAdmin Professional 3 は、サポートサイト（ブラザーソリューションセンター（support.brother.co.jp/））で、お使いの機種の**ソフトウェアダウンロード**ページからダウンロードできます。このユーティリティは、Windows® 用のみです。
- ウイルス対策ソフトウェアやスパイウェア対策ソフトウェアでファイアウォール機能を使用している場合は、そのソフトウェアを一時的に無効にしてください。スキャンができることを確認したら、そのソフトウェアを再び有効にしてください。
- ノード名：BRAdmin Light の現在の画面にノード名が表示されます。本製品のスキャンサーバーのお買い上げ時のノード名は、無線 LAN の場合は「BRWxxxxxxxxxxxx」です。（「xxxxxxxxxxxx」は、本製品の MAC アドレス / イーサネットアドレスです。）
- お買い上げ時の設定では、パスワードは必要ありません。パスワードを設定してある場合はパスワードを入力し、**OK** を押します。

1. BRAdmin Light を起動します。
   - Windows® XP、Windows Vista®、および Windows® 7

     （**スタート**）> **すべてのプログラム** > **Brother** > **BRAdmin Light** > **BRAdmin Light** の順にクリックします。
   - Windows® 8、Windows® 8.1、および Windows® 10

     タスクトレイにある （**BRAdmin Light**）をクリックします。
2. BRAdmin Light が新しい機器を自動的に検索します。
3. 本製品をダブルクリックします。



メモ

- スキャンサーバーがお買い上げ時の設定のままで、お客様が DHCP/BOOTP/RARP サーバーをご使用にならない場合、この機器は BRAdmin Light ユーティリティ画面に **未設定** と表示されます。
- 本製品の液晶画面で、本製品の MAC アドレス（イーサネットアドレス）とノード名を表示できます。MAC アドレスを表示するには、 > [ネットワーク] > [無線 LAN] > [MACｱﾄﾞﾚｽ] の順に押します。ノード名を表示するには、 > [ネットワーク] > [無線 LAN] > [TCP/IP] > [ﾉｰﾄﾞ名] の順に押します。

4 **IP 取得方法**で **STATIC** を選択します。製品の **IP アドレス**、**サブネットマスク**、および**ゲートウェイ**（必要に応じて）を入力します。

5 **OK** をクリックします。

6 本製品が機器リストに表示されます。表示されない場合は、手順 4 で IP アドレスを確認してください。

その他の管理ユーティリティ

ウェブブラウザーによる管理

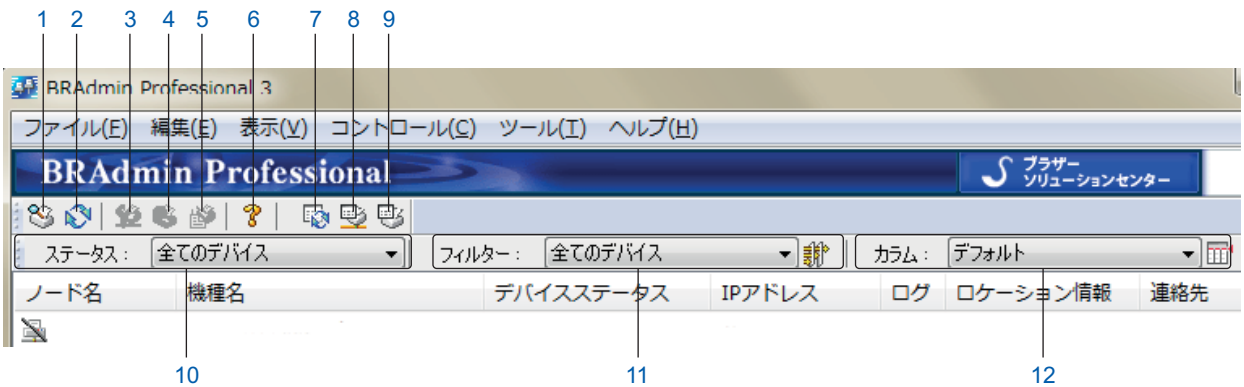
標準のウェブブラウザーを使用してスキャンサーバーの設定を変更できます。ウェブブラウザーは、HTTP（ハイパーテキスト転送プロトコル）または HTTPS（SSL を用いたハイパーテキスト転送プロトコル）のいずれのプロトコルでも使用できます。（*本製品を設定する*（39 ページ）を参照してください。）

BRAdmin Professional 3 (Windows®)

BRAdmin Professional 3 は、ネットワークに接続されたブラザー機器を詳細に管理するためのユーティリティです。このユーティリティは、お客様のネットワーク上にあるブラザー製品を検索し、エクスプローラー形式の画面上で機器の状態を簡単に確認できます。各機器の状態は、アイコンのカラーによって示されます。ネットワークに接続された Windows® コンピューターから、本製品のネットワーク設定や機器設定を変更したりファームウェアを更新したりできます。BRAdmin Professional 3 は、ネットワークに接続されているブラザー機器の活動をログに記録し、このログデータを HTML、CSV、TXT、または SQL 形式でエクスポートすることもできます。

メモ

- 最新バージョンの BRAdmin Professional 3 ユーティリティを使用してください。ブラザー BRAdmin Professional 3 は、サポートサイト（ブラザーソリューションセンター（support.brother.co.jp/））で、お使いの機種の**ソフトウェアダウンロード**ページからダウンロードできます。このユーティリティは、Windows® 用のみです。
- ウイルス対策ソフトウェアやスパイウェア対策ソフトウェアでファイアウォール機能を使用している場合は、そのソフトウェアを一時的に無効にしてください。スキャンができることを確認したら、そのソフトウェアを再び有効にしてください。
- ノード名：ノード名は、BRAdmin Professional 3 に表示されるネットワーク上の各ブラザー機器ごとに異なります。無線 LAN 接続の場合、お買い上げ時のノード名は「BRWxxxxxxxxxxxx」です。（「xxxxxxxxxxxx」は、本製品の MAC アドレス / イーサネットアドレスです。）



1 ネットワークを検索

ネットワーク上にある機器を検索します。

お買い上げ時の設定では、ローカルネットワークに接続されている、有効な IP アドレスが設定された対応ネットワーク機器が、すべて表示されます。

2 ステータスの更新（すべての機器）
BRAdmin Professional が通信している機器の状態情報を、最新情報に更新します。

3 デバイスの設定
ネットワークに接続されているブラザー機器に有効な IP アドレスが設定されていない場合、BRAdmin Professional を利用すると、その機器の IP アドレス、サブネットマスク、ゲートウェイアドレス、および IP 取得方法を設定できます。

4 機器のホーム ページ（ウェブブラウザーによる管理）
製品に組み込まれているウェブサーバーに接続します（すべての製品にウェブサーバーが組み込まれているわけではありません）。

5 ファイルの送信
機器にファイルを送信します。

6 ヘルプトピック
BRAdmin Professional 3 のヘルプファイルを表示します。

7 ログを更新
ログ履歴を最新情報に更新します。

8 ネットワークデバイスのログを表示
ネットワーク上にあるすべての機器のログ情報を表示します。

9 ローカルデバイスのログを表示
クライアントコンピューターに接続されている、ローカル機器のログ設定に登録済みのすべての機器のログ情報を表示します。

10 ステータス
ドロップダウンリストからステータスを選択します。

11 フィルター
ドロップダウンリストからフィルターを選択します。
ドロップダウンリストからフィルターを選択するには、事前に をクリックしてメニューを追加しておく必要があります。

12 カラム
カラム設定オプションを使用すると、BRAdmin Professional のメインビュー画面に表示するカラムを選択できます。

メモ

BRAdmin Professional 3 について詳しくは、 をクリックしてください。

3 製品の無線 LAN 接続を設定する

概要

本製品を無線 LAN に接続して使用する場合は、『*かんたん設置ガイド*』に概説されているいずれかのセットアップ方法で行うことをお勧めします。『*かんたん設置ガイド*』は、サポートサイト（ブラザーソリューションセンター（solutions.brother.com/manuals））で、お使いの機種のページからダウンロードできます。

無線 LAN 接続のためのその他の設定方法について詳しくは、この章をお読みください。TCP/IP の設定については、*本製品のネットワーク設定を変更する*（3 ページ）をご覧ください。

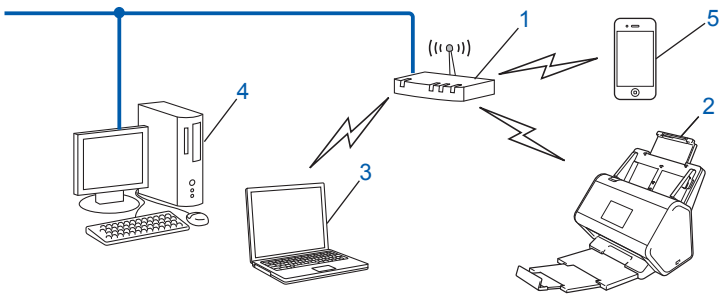
メモ

- 毎日の文書スキャン作業を快適に行えるようにするには、本製品を無線 LAN のアクセスポイントまたはルーターの近くに設置し、無線通信に支障のないようにしてください。本製品と無線 LAN アクセスポイントまたはルーターとの間に大きな障害物や壁があったり、他の電子機器からの電磁妨害があると、文書スキャンのデータ転送速度に影響を与える可能性があります。

  無線 LAN 接続は必ずしもすべてのタイプの文書やアプリケーションに最適な接続方法とは限りません。大きなファイルをスキャンする場合（たとえばテキストと大きな画像が混在した複数ページのドキュメントなど）は、通信速度の速い USB ケーブル接続をお勧めします。
- 無線 LAN 接続を設定するには、ネットワーク名（SSID）とネットワークキーが必要になります。

ネットワーク環境を確認する

ネットワーク上の無線 LAN アクセスポイント / ルーターとパソコンが接続されている場合 （インフラストラクチャモード）



1 無線 LAN アクセスポイント / ルーター [1]

[1] お使いのパソコンが Intel® My WiFi テクノロジー（MWT）に対応している場合は、パソコンを WPS（Wi-Fi Protected Setup™）対応アクセスポイントとして使用できます。

2 無線 LAN 対応の機器（本製品）

3 無線 LAN アクセスポイント / ルーターに接続されている無線 LAN 対応のパソコン

4 ネットワークケーブルで無線 LAN アクセスポイント / ルーターに接続されている有線接続のパソコン（無線 LAN 非対応のパソコン）

5 無線 LAN アクセスポイント / ルーターに接続されている携帯端末

設定方法

無線 LAN 環境で本製品を設定するには、次のいくつかの方法があります。ご自分の環境に適した方法をお選びください。

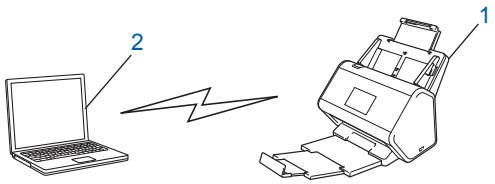
- 一時的に USB ケーブルを使用して無線 LAN を設定する（推奨）。『*かんたん設置ガイド*』をご覧ください。
- WPS（Wi-Fi Protected Setup™）を使用したワンプッシュ無線 LAN 設定。18 ページをご覧ください。
- WPS を使用した PIN 方式による無線 LAN 設定。19 ページをご覧ください。
- セットアップウィザードを使用した無線 LAN 設定。29 ページをご覧ください。

無線 LAN の接続状態を確認する

1. 本製品の液晶画面で、 を押します。
2. ［ネットワーク］を押します。
3. ［無線 LAN］を押します。
4. ▲または▼を押し、次に［無線状態］を押します。
5. ［接続状態］を押します。

ネットワークに無線 LAN アクセスポイント / ルーターがない場合の無線 LAN 対応パソコンへの接続 （アドホックモード）

アドホックモードのネットワークには、無線 LAN アクセスポイント / ルーターがありません。各無線 LAN 対応機器は、アクセスポイントやルーターを介さないでお互いに直接通信します。ブラザー無線 LAN 対応機器（本製品）がこのネットワークの一部になっている場合、本製品はスキャンデータ送信パソコンから直接すべてのスキャンジョブを受信します。



1 無線 LAN 対応の機器（本製品）

2 無線 LAN 対応パソコン

弊社ではアドホックモードでの無線 LAN 接続を保証していません。本製品をアドホックモードで設定するには、*アドホックモードでの設定*（22 ページ）をご覧ください。

設定

SSID が隠蔽されていて表示されない場合

1. 本製品を設定する前に、無線 LAN の設定を書き留めておくことをお勧めします。設定を行うには、以下の情報が必要になります。
   現在の無線 LAN の設定を調べて書き留めてください。

ネットワーク名（SSID）

接続モード	認証方式	暗号化方式	ネットワークキー
インフラストラクチャー	オープンシステム	なし	—
		WEP	
	共有キー	WEP	
	WPA/WPA2-PSK	AES	
		TKIP [1]	

[1] TKIP は WPA-PSK にのみ対応しています。

例：

ネットワーク名（SSID）
HELLO

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

メモ

ご使用のルーターで WEP 暗号化方式を使用している場合は、1 番目の WEP キーとして使用されるキーを入力します。本製品では、1 番目の WEP キーのみ使用できます。

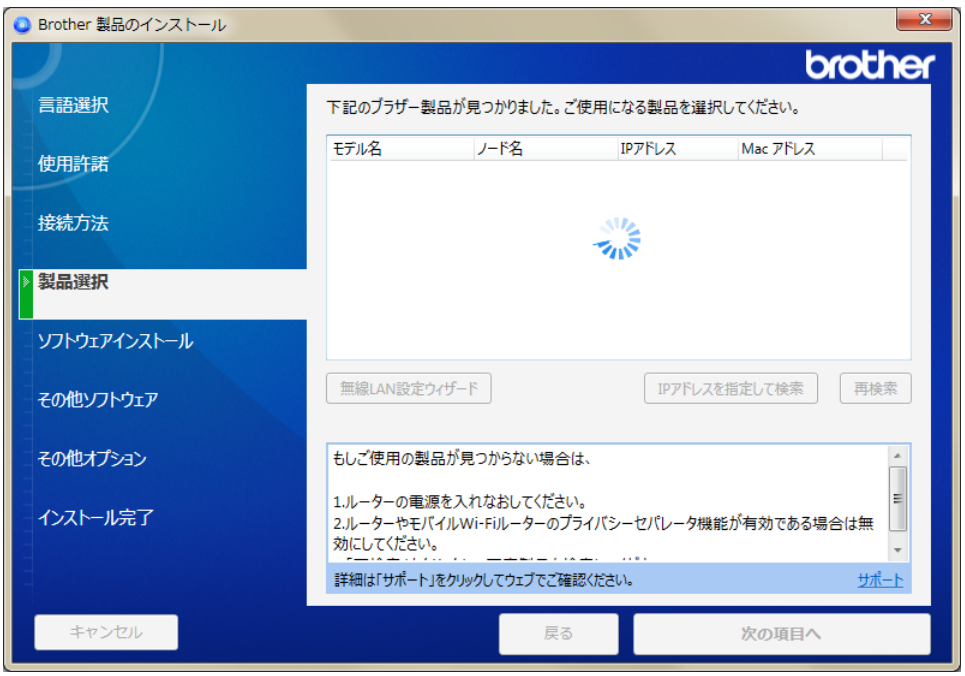
2 次の操作のいずれかを実行してください。

■ Windows®

a 付属の DVD-ROM ディスクを DVD-ROM ドライブにセットします。

b **無線 LAN（Wi-Fi）**を選択し、**次の項目へ** をクリックします。

c **無線 LAN 設定ウィザード** をクリックします。



■ Macintosh

a サポートサイト（ブラザーソリューションセンター（support.brother.co.jp/））からフルパッケージダウンロードをダウンロードします。

b デスクトップ上の **BROTHER** アイコンをダブルクリックします。

c **ユーティリティ** をダブルクリックします。

d **無線 LAN 設定ウィザード** をダブルクリックします。

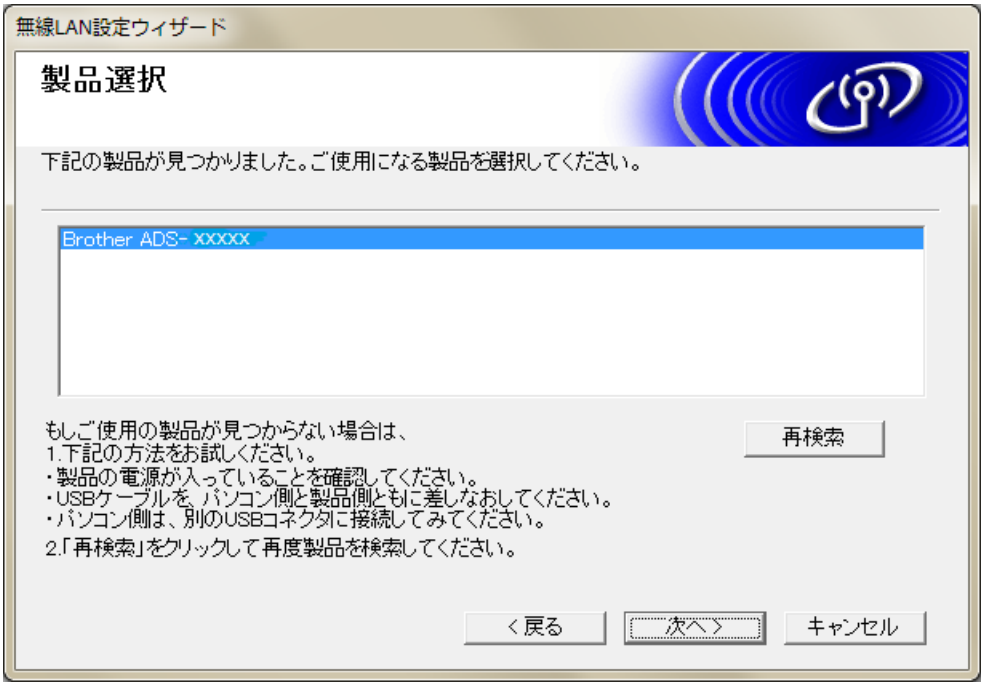
3 **USB ケーブルを使用して設定する（推奨）**を選択し、**次へ** をクリックします。
一時的に USB ケーブルを使用することをお勧めします。

メモ

以下の画面が表示されたら、**重要な注意** を読みます。SSID とネットワークキーを確認したら**確認しました**チェックボックスを選択し、**次へ**をクリックします。

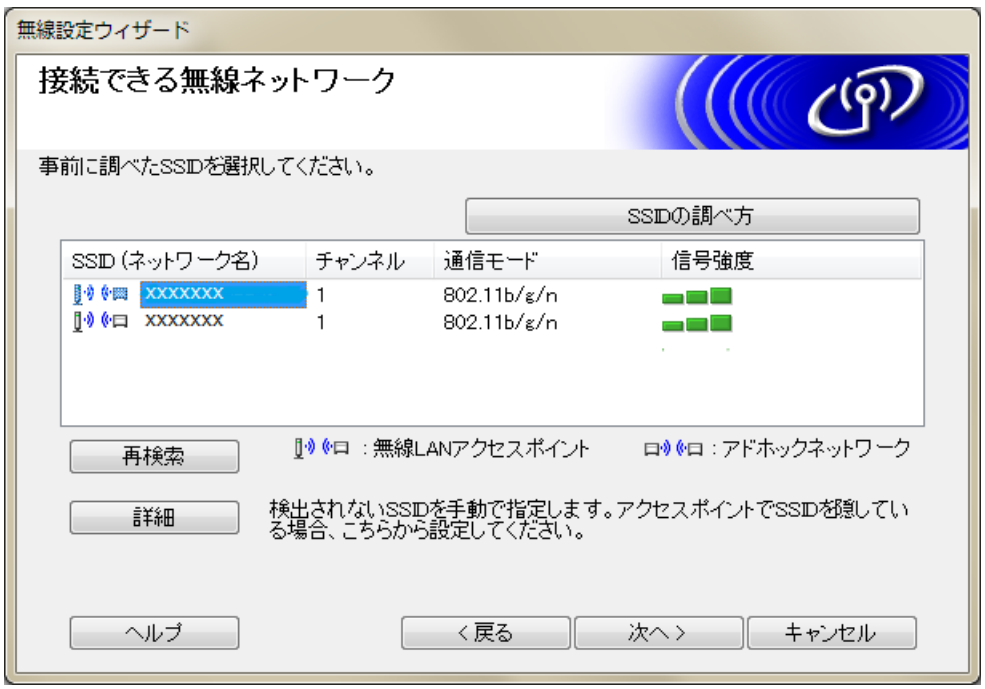
4 一時的にパソコンと本製品を USB ケーブルで接続します。
確認画面が表示されたら、**次へ** をクリックします。

5 **次へ** をクリックします。（Windows® のみ）

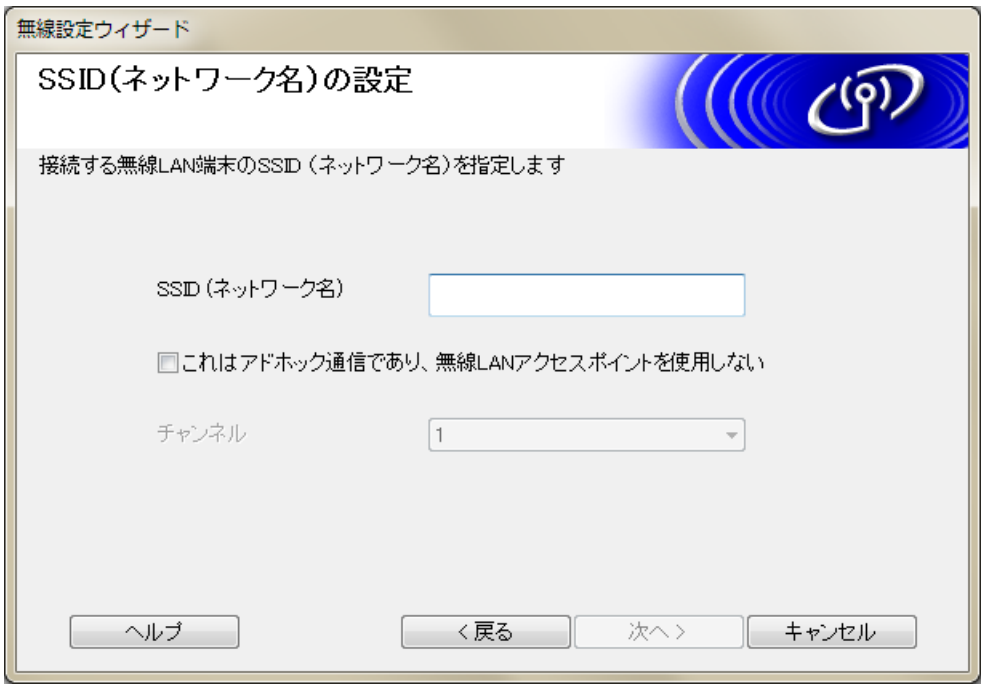


6 次の操作のいずれかを実行してください。

- 使用する SSID を選択し、**次へ** をクリックします。次に、**ネットワークキー** を設定し、❿ に進みます。
- 使用したい SSID が隠蔽されている場合は、**詳細** をクリックして ❼ に進みます。

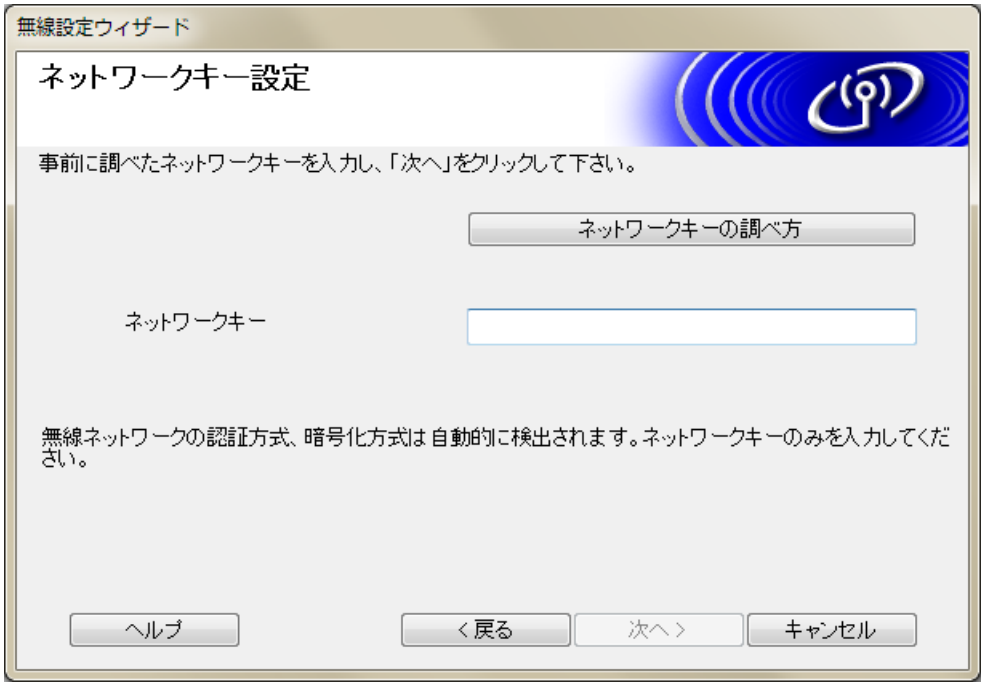


7 新しい SSID を **SSID（ネットワーク名）** フィールドに入力し、**次へ**をクリックします。

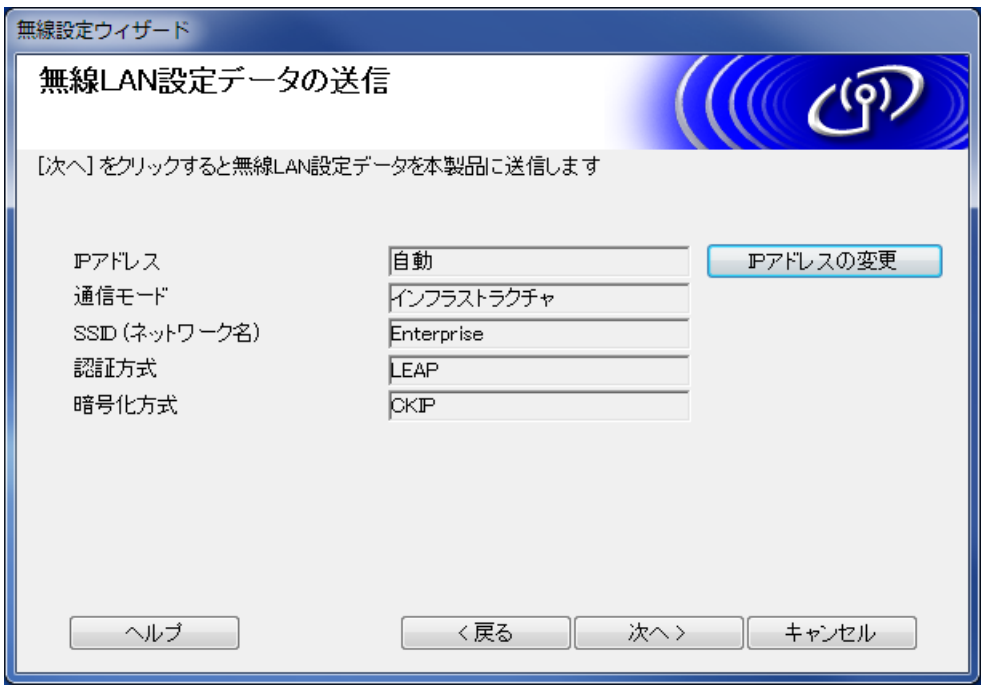


8 **認証方式** と **暗号化方式** をそれぞれドロップダウンリストから選択し、新しいネットワークキーを **ネットワークキー** フィールドに入力し、**次へ** をクリックして ⓫ に進みます。

9 新しいネットワークキーを**ネットワークキー** フィールドに入力し、**次へ** をクリックします。



10 **次へ** をクリックします。設定が本製品に送信されます。
（次の画面は設定により異なります。）



メモ

設定が完了しケーブルを安全に取り外すことができるというメッセージが画面に表示されるまでは、USB ケーブルを取り外さないでください。

⑪ パソコンと本製品間の USB ケーブルを取り外します。

⑫ **完了** をクリックします。

WPS（Wi-Fi Protected Setup™）を使用する場合の設定

1. お使いの無線 LAN アクセスポイント / ルーターに、以下の WPS マークが付いていることを確認します。

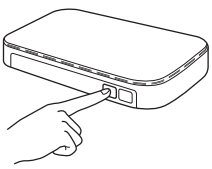
2. 本製品を無線 LAN アクセスポイント / ルーターの受信範囲内に置きます。電波が届く範囲は、環境によって異なる場合があります。詳しくはお使いの無線 LAN アクセスポイント / ルーターの取扱説明書をご覧ください。

3. 本製品の液晶画面で、 > [ネットワーク] > [無線 LAN] > [WPS] の順に押します。
[無線 LAN をオンにしますか ?] が表示されたら、[はい] を押して承認します。

メモ

- 無線 LAN アクセスポイント / ルーターの WPS ボタンを押した後、数秒以内に本製品の液晶画面で [WPS] を起動しないと、接続に失敗する場合があります。
- お使いの無線 LAN アクセスポイント / ルーターが WPS に対応していて、PIN（パスワード）方式を採用して本製品を設定する場合は、*WPS（Wi-Fi Protected Setup™）の PIN 方式を使用する*（19 ページ）をご覧ください。

4. WPS を開始するように液晶画面に指示が表示されたら、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（詳しくは、ご使用の無線 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）。



本製品の液晶画面で [OK] を押します。

5. 本製品が、無線 LAN アクセスポイント / ルーターで使用されているモード（WPS）を自動的に検出し、無線 LAN への接続を試みます。

6. 無線 LAN 機器に正しく接続されると、液晶画面に [接続しました] というメッセージが表示されます。[OK] を押して、メッセージを閉じます。
無線 LAN のセットアップはこれで完了です。操作パネルの Wi-Fi ランプ が点灯し、本製品のネットワークインターフェースが無線 LAN に設定されたことが示されます。

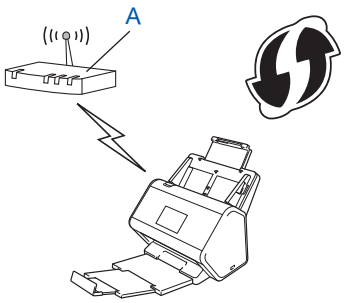
WPS（Wi-Fi Protected Setup™）の PIN 方式を使用する

お使いの無線 LAN アクセスポイント / ルーターが WPS（PIN 方式）に対応している場合は、次の手順に従って本製品を設定してください。

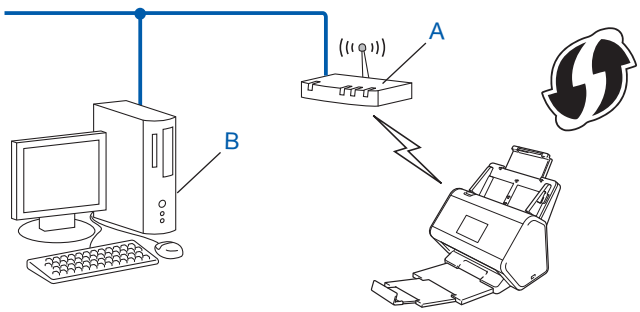
メモ

PIN（個人識別番号）方式は、Wi-Fi Alliance® が策定した接続方法のひとつです。*登録者*（本製品）が作成した PIN コードを*レジストラ*（無線 LAN を管理する機器）に入力することにより、無線 LAN ネットワークとセキュリティの設定を行うことができます。無線 LAN アクセスポイント / ルーターを WPS モードで使用するための方法については、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。

■ 無線 LAN アクセスポイント / ルーター (A) をレジストラとして使用する場合の接続 [1]。



■ パソコンなど別の機器 (B) をレジストラとして使用する場合の接続 [1]。



[1] 通常は無線 LAN アクセスポイント / ルーターがレジストラです。

メモ

WPS に対応したルーターやアクセスポイントには次のマークが付いています。

1. 本製品の液晶画面で、 を押します。
2. [ネットワーク] を押します。
3. [無線 LAN] を押します。
4. ▲ または ▼ を押して、[WPS(PIN コード)] を表示します。
   [WPS(PIN コード)] を押します。
5. [無線 LAN をオンにしますか ?] が表示されたら、[はい] を押して承認します。
   無線接続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。
6. 液晶画面に 8 桁の PIN コードが表示され、製品によるアクセスポイントの検索が開始されます。
7. ブラウザーのアドレスバーに、アクセスポイント（レジストラ [1]）の IP アドレスを入力します。
   [1] 通常は無線 LAN アクセスポイント / ルーターがレジストラです。
8. WPS セットアップページに進み、手順 ❻ で液晶画面に表示された PIN コードをレジストラに入力し、画面の指示に従います。

メモ

- セットアップページは、ご使用の無線 LAN アクセスポイント / ルーターの製造会社ごとに異なります。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 Vista®、Windows® 7、Windows® 8、Windows® 8.1、または Windows® 10 コンピューターをレジストラとして使用するには、あらかじめコンピューターをネットワークに登録する必要があります。ご使用の無線 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、Windows® 8.1、または Windows® 10 をレジストラとして使用する場合は、画面の指示に従って、無線 LAN 設定後にスキャナードライバーをインストールできます。フルパッケージ（すべてのドライバーとソフトウェア）をインストールする場合は、『*かんたん設置ガイド*』に記載の手順に従ってインストールしてください。

Windows Vista®/Windows® 7/Windows® 8/Windows® 8.1/Windows® 10

パソコンをレジストラとして使用する場合は、次の手順に従ってください。

a Windows Vista®

（**スタート**）> **ネットワーク** > **ワイヤレス デバイスの追加** の順にクリックします。

Windows® 7

（**スタート**）> **デバイスとプリンター** > **デバイスの追加** の順にクリックします。

Windows® 8 および Windows® 8.1

マウスをデスクトップ右下に移動します。メニューバーが表示されたら、**設定** > **コントロール パネル** > **デバイスとプリンター** > **デバイスの追加** の順にクリックします。

Windows® 10

（**スタート**）> **設定** > **デバイス** > **接続中のデバイス** > **デバイスの追加** の順にクリックします。

b 本製品を選択し、**次へ** をクリックします。

c 手順 ❻ の液晶画面に表示された PIN コードを入力し、**次へ** をクリックします。

d 接続先のネットワークを選択し、**次へ** をクリックします。

e **閉じる** をクリックします。

9 無線 LAN 機器に正しく接続された場合は、液晶画面に［接続しました］が表示されます。
接続に失敗した場合は、液晶画面にエラーコードが表示されます。エラーコードを書き留め、*無線 LAN エラーコード*（90 ページ）を参照して対処してください。

OK!

Windows®

無線 LAN のセットアップがこれで完了しました。引き続き、本機器の操作に必要なドライバーやソフトウェアをインストールする場合は、DVD-ROM を DVD ドライブにセットします。

メモ

ブラザーの画面が自動的に表示されない場合は、（**スタート**）> **コンピューター**（**マイ コンピューター**）をクリックします。（Windows® 8、Windows® 8.1、Windows® 10 の場合は、タスク バーの（**エクスプローラー**）アイコンをクリックし、**コンピューター / PC** に進みます。）DVD 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。

Macintosh

無線 LAN のセットアップがこれで完了しました。引き続き、本機器の操作に必要なドライバーやソフトウェアをインストールする場合は、ドライバー メニューから **Start Here OSX** を選択します。

アドホックモードでの設定

SSID が設定済みの場合

SSID がすでに設定され、アドホックモードで通信しているパソコンと本製品を接続するには、以下の手順に従います。

1. 本製品を設定する前に、無線 LAN の設定を書き留めておくことをお勧めします。設定を行うには、以下の情報が必要になります。
   接続するパソコンの現在の無線 LAN 設定を調べ、書き留めてください。

メモ

接続するパソコンの無線 LAN 設定は、SSID でアドホックモードに設定する必要があります。パソコンをアドホックモードに設定する手順については、パソコンに付属の取扱説明書をご覧になるか、ネットワーク管理者にお問い合わせください。

ネットワーク名（SSID）

接続モード	暗号化方式	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

接続モード	暗号化方式	ネットワークキー
アドホック	WEP	12345

メモ

本製品では、1 番目の WEP キーのみ使用できます。

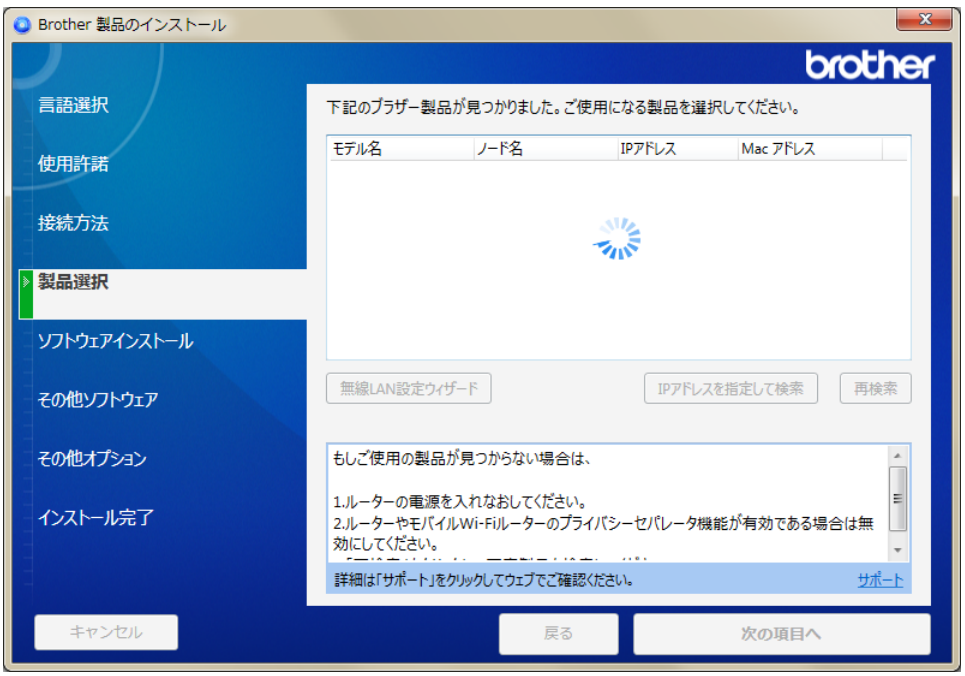
2 次の操作のいずれかを実行してください。

■ Windows®

a 付属の DVD-ROM ディスクを DVD-ROM ドライブにセットします。

b **無線 LAN（Wi-Fi）**を選択し、**次の項目へ** をクリックします。

c **無線 LAN 設定ウィザード** をクリックします。



■ Macintosh

a サポートサイト（ブラザーソリューションセンター（support.brother.co.jp/））からフルパッケージダウンロードをダウンロードします。

b デスクトップ上の **BROTHER** アイコンをダブルクリックします。

c **ユーティリティ** をダブルクリックします。

d **無線 LAN 設定ウィザード** をダブルクリックします。

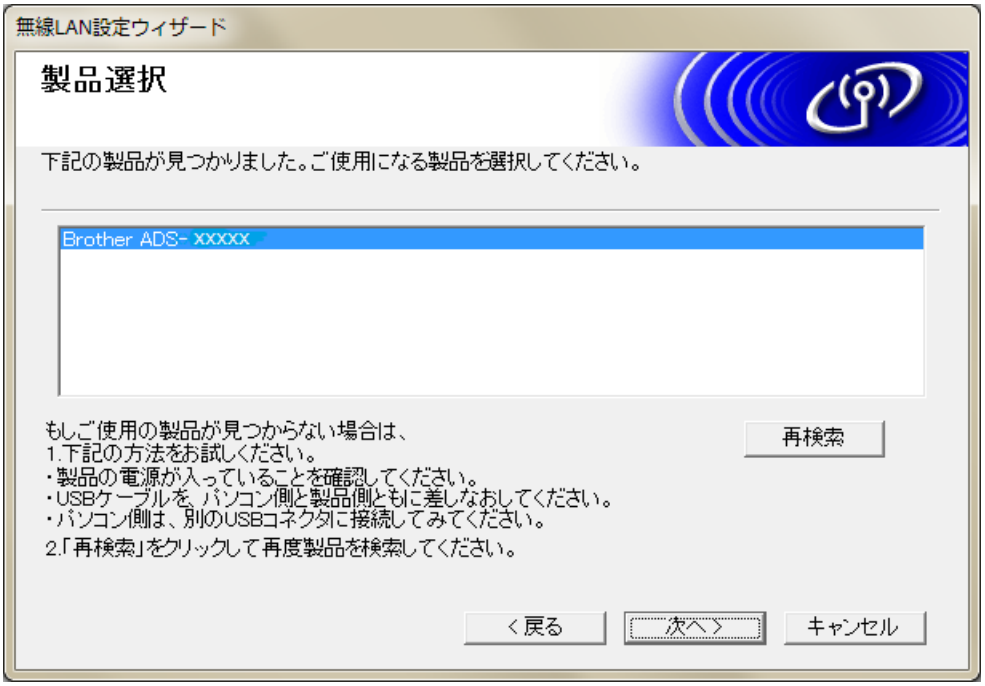
3 **USB ケーブルを使用して設定する（推奨）**を選択し、**次へ** をクリックします。
一時的に USB ケーブルを使用することをお勧めします。

メモ

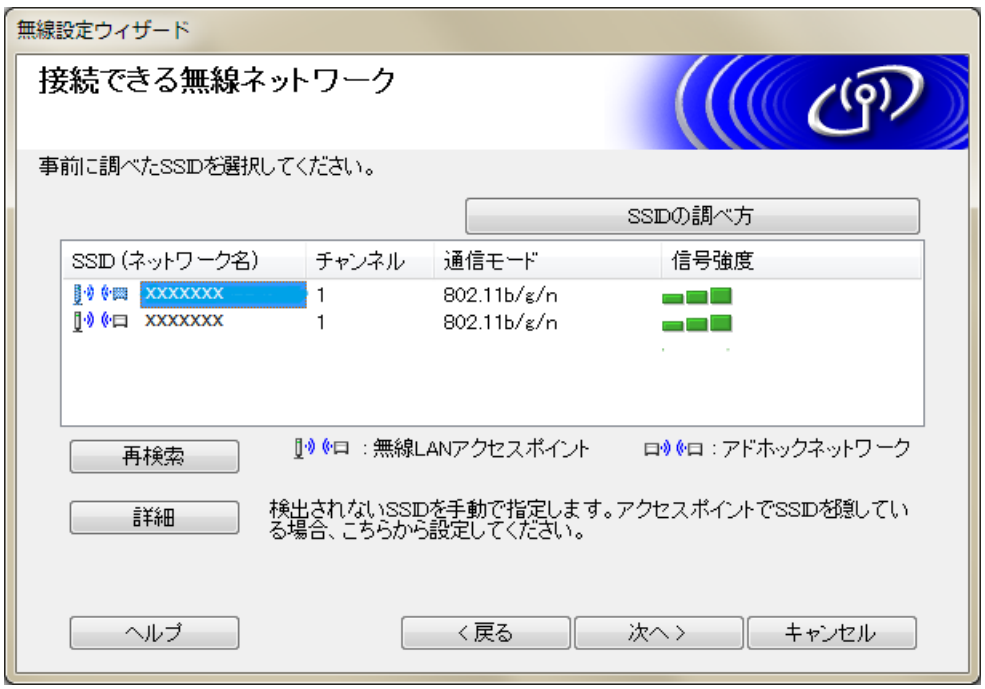
以下の画面が表示されたら、**重要な注意** を読みます。SSID とネットワークキーを確認したら**確認しました**チェックボックスを選択し、**次へ**をクリックします。

4 一時的にパソコンと本製品を USB ケーブルで接続します。
確認画面が表示されたら、**次へ** をクリックします。

5 **次へ** をクリックします。（Windows® のみ）



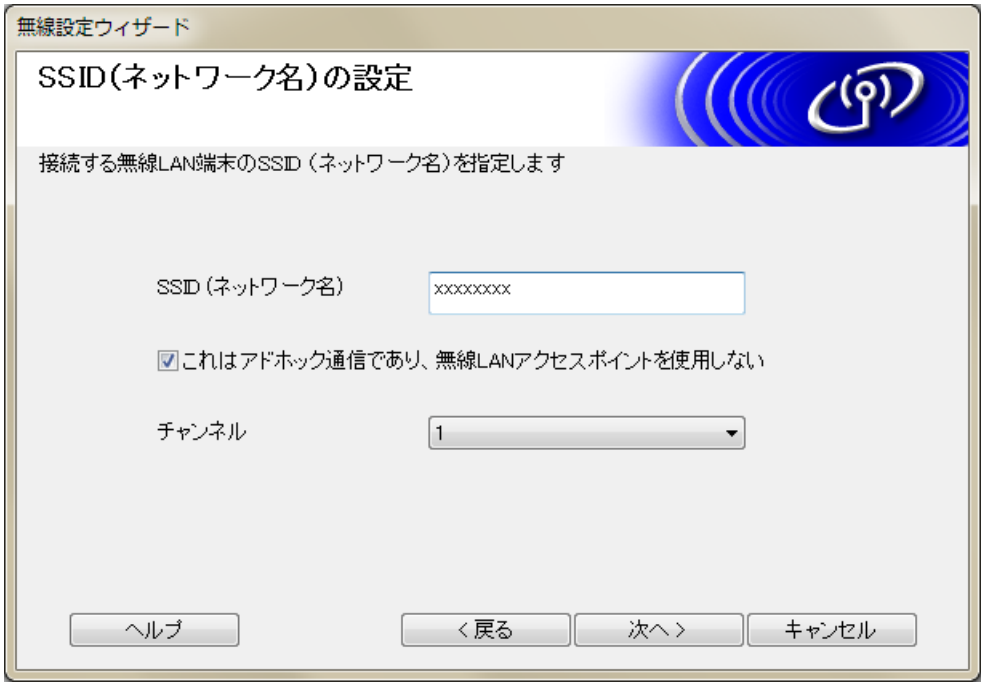
6 **詳細** をクリックします。



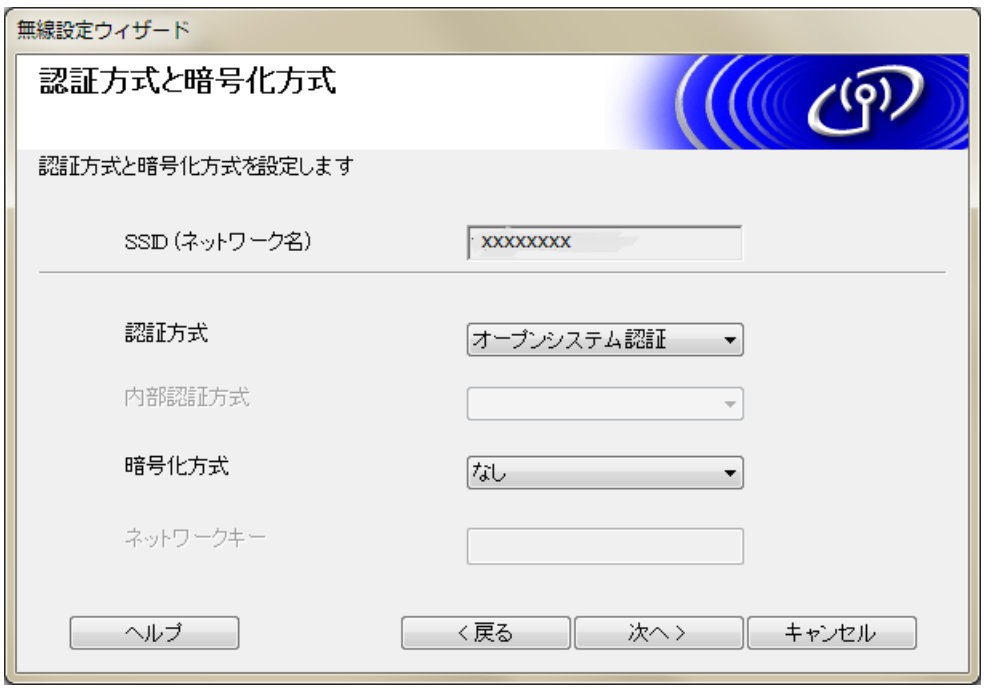
メモ

リストが空白になっている場合は、無線 LAN アクセスポイントの電源がオンになっていること、および SSID が隠蔽されていないこと、本製品とパソコンが無線通信の受信範囲内にあることを確認します。その後、**再検索** をクリックします。

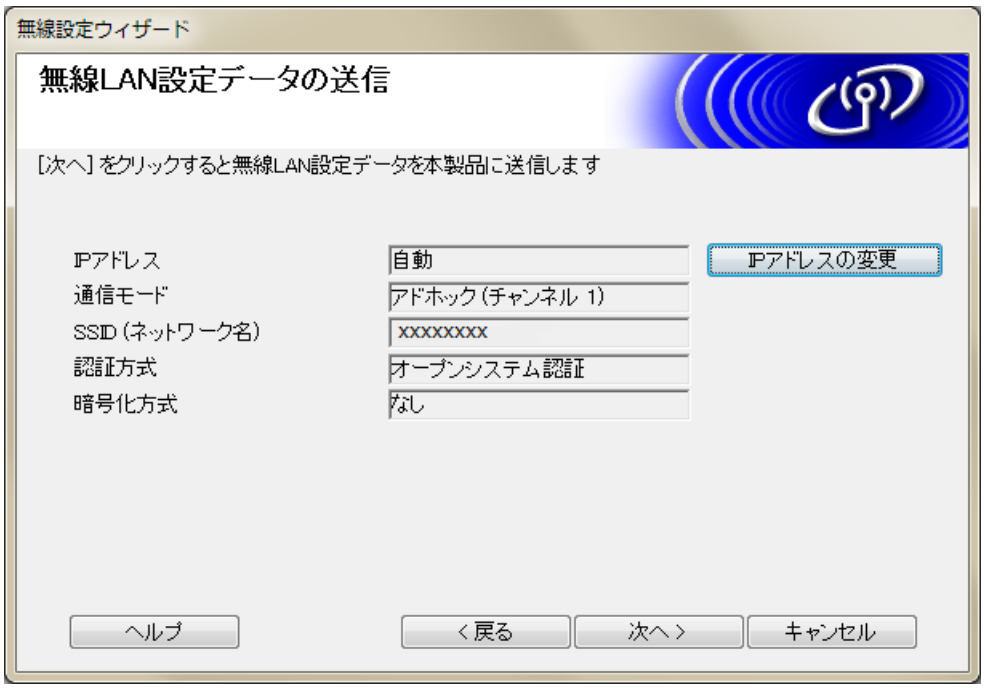
7 **これはアドホック通信であり、無線 LAN アクセスポイントを使用しない** にチェックを付け、**次へ** をクリックします。



8 **認証方式** と **暗号化方式** をそれぞれドロップダウンリストから選択し、新しいネットワークキーを **ネットワークキー** フィールドに入力し、**次へ** をクリックします。



9 **次へ** をクリックします。設定が本製品に送信されます。（画像は、暗号化方式 WEP。）



10 パソコンと本製品間の USB ケーブルを取り外します。

11 **完了** をクリックします。

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

本製品を設定する前に、無線 LAN の設定を書き留めておくことをお勧めします。設定を行うには、以下の情報が必要になります。

1. 接続するパソコンの現在の無線 LAN 設定を調べ、書き留めてください。

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

メモ

- ご使用の無線 LAN アクセスポイント / ルーターが複数の WEP キーに対応している場合でも、本製品で使用できるのは 1 番目の WEP キーのみです。
- うまくセットアップできないなど、ブラザーコールセンター（お客様相談窓口）にお問い合わせいただく場合は、あらかじめ SSID（ネットワーク名）とネットワークキーを調べ、お手元にご用意ください。当社では、この情報を調べるお手伝いはいたしかねます。
- 無線 LAN のセットアップには、この情報（SSID とネットワークキー）が必要です。

  本情報の見つけ方

  a お使いの無線 LAN アクセスポイント / ルーターに付属の取扱説明書を調べてください。

  b SSID の初期設定は、製造元の名前やモデル名である場合があります。

  c セキュリティに関する情報がご不明な場合は、ルーターの製造元、御社のシステム管理者、またはお使いのインターネットサービスプロバイダーにお問い合わせください。

2. 本製品の液晶画面で、 > [ネットワーク] > [無線LAN] > [無線接続ウィザード] の順に押します。
3. ネットワークの検索が行われた後、利用可能な SSID の一覧が表示されます。
   SSID の一覧が表示されたら、▲ または ▼ を押して接続先の SSID を表示し、その SSID を押します。
4. [OK] を押します。

5 次の操作のいずれかを実行してください。

- 使用する認証方式と暗号化方式でネットワークキーが必要な場合は、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。
  必要な情報をすべて入力したら、[OK] を押してから、[はい] を押して設定を適用します。
- 認証方式が「オープンシステム」で、暗号化方式が [なし] の場合は、次の手順に進みます。
- お使いの無線 LAN アクセスポイント / ルーターが WPS に対応していると、[選択されたアクセスポイントは WPS 自動設定に対応しています自動接続しますか ?] が表示されます。自動ワイヤレスモードを使用して本製品の接続を行うには、[はい] を押します。([いいえ (手動)] を選択した場合は、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。) [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 [次へ] を押して進んでください] が表示された場合は、お使いの無線 LAN アクセスポイント / ルーターの WPS ボタンを押し、[次へ] を押します。

6 選択した無線 LAN 機器への接続が行われます。

無線 LAN 機器に正しく接続された場合は、液晶画面に [接続しました] が表示されます。

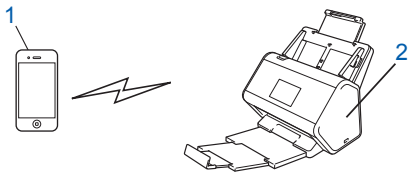
無線 LAN のセットアップがこれで完了しました。本製品の操作に必要なドライバーやソフトウェアをインストールする場合は、付属のインストール用 DVD-ROM をパソコンの DVD-ROM ドライブにセットしてインストールするか、サポートサイト（ブラザーソリューションセンター (support.brother.co.jp/)）でお使いの機種の**ソフトウェアダウンロード**ページからダウンロードしてインストールします。

Wi-Fi Direct® を使用する

- Wi-Fi Direct® を使用して携帯端末からスキャンする
- Wi-Fi Direct® ネットワークを設定する
- 本製品の操作パネルから Wi-Fi Direct® ネットワークを設定する

Wi-Fi Direct® を使用して携帯端末からスキャンする

Wi-Fi Direct® は、Wi-Fi Alliance® が策定した無線設定方法のひとつです。本製品と、Android™ 機器、Windows® Phone 機器、iPhone、iPod touch、iPad などの携帯端末間に、アクセスポイントを使用することなく、安全な無線 LAN 接続を設定することができます。Wi-Fi Direct® は、WPS（Wi-Fi Protected Setup™）のワンプッシュ方式や PIN 方式を使用した無線 LAN 設定に対応しています。SSID とパスワードの手動入力により、無線 LAN を設定することもできます。本製品の Wi-Fi Direct® 機能は、AES 暗号化方式による WPA2™ セキュリティに対応しています。



1 携帯端末

2 本製品

メモ

- 本製品では、有線 LAN と無線 LAN のどちらも使用できますが、同時には使用できません。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® 対応機器は、グループオーナー（G/O）に設定することができます。Wi-Fi Direct® ネットワークを設定する際は、G/O が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。どちらかの機能を有効にするには、もう一方の機能を無効にします。アドホックモードを使用しているときに Wi-Fi Direct® を使用する場合は、ネットワークのインターフェースを「有線 LAN」に設定するか、または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。

Wi-Fi Direct® ネットワークを設定する

本製品の操作パネルから Wi-Fi Direct® ネットワークを設定する。

- Wi-Fi Direct® ネットワーク設定の概要

  無線 LAN 環境での本製品の設定方法を 5 種類、以下に示します。ご自分の環境に適した方法をお選びください。
- ワンプッシュ方式で、Wi-Fi Direct® ネットワークを設定する
- WPS（Wi-Fi Protected Setup™）のワンプッシュ方式で、Wi-Fi Direct® ネットワークを設定する
- PIN 方式で、Wi-Fi Direct® ネットワークを設定する
- WPS（Wi-Fi Protected Setup™）の PIN 方式で、Wi-Fi Direct® ネットワークを設定する
- Wi-Fi Direct® ネットワークを手動で設定する

Wi-Fi Direct® ネットワーク設定の概要

無線 LAN 環境での本製品の設定方法を 5 種類、以下に示します。ご自分の環境に適した方法をお選びください。

携帯端末の設定を確認します。

1. ご利用の携帯端末は Wi-Fi Direct® に対応していますか？

オプション	詳細
はい	手順 ❷ に進みます。
いいえ	手順 ❸ に進みます。

2. ご利用の携帯端末は Wi-Fi Direct® のワンプッシュ方式に対応していますか？

オプション	詳細
はい	*ワンプッシュ方式で、Wi-Fi Direct® ネットワークを設定する*（33 ページ）をご覧ください。
いいえ	*PIN 方式で、Wi-Fi Direct® ネットワークを設定する*（34 ページ）をご覧ください。

3. ご利用の携帯端末は WPS（Wi-Fi Protected Setup™）に対応していますか？

オプション	詳細
はい	手順 ❹ に進みます。
いいえ	*Wi-Fi Direct® ネットワークを手動で設定する*（37 ページ）をご覧ください。

4 ご利用の携帯端末は WPS（Wi-Fi Protected Setup™）のワンプッシュ方式に対応していますか？

オプション	詳細
はい	*WPS（Wi-Fi Protected Setup™）のワンプッシュ方式で、Wi-Fi Direct® ネット ワークを設定する*（34 ページ）をご覧ください。
いいえ	*WPS（Wi-Fi Protected Setup™）の PIN 方式で、Wi-Fi Direct® ネットワーク を設定する*（35 ページ）をご覧ください。

Wi-Fi Direct® を使用してワンプッシュ方式または PIN 方式で設定した Wi-Fi Direct® ネットワークで、Brother iPrint&Scan 機能を利用するには、Android™ 4.0 以降の端末機器が必要です。

ワンプッシュ方式で、Wi-Fi Direct® ネットワークを設定する

ご利用の携帯端末が Wi-Fi Direct® に対応している場合は、次の手順で Wi-Fi Direct® ネットワークを設定します。

メモ

本製品が携帯端末から Wi-Fi Direct® 要求を受信すると、液晶画面に [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] というメッセージが表示されます。接続するには、[OK] を押します。

1 > [ネットワーク] > [Wi-Fi Direct] > [プッシュボタン接続] の順に押します。

2 本製品の液晶画面に [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、携帯端末で Wi-Fi Direct® をアクティブにします（手順については、お使いの携帯端末の取扱説明書をご覧ください）。本製品の [OK] を押して、Wi-Fi Direct® のセットアップを開始します。キャンセルするには、 を押します。

3 次の操作のいずれかを実行してください。

- 本製品がグループオーナー（G/O）に設定されている場合は、携帯端末を直接、本製品に接続します。
- 本製品がグループオーナー（G/O）に設定されていない場合は、表示された機器名を使用して、Wi-Fi Direct® ネットワークを設定できます。接続先の携帯端末を選択し、[OK] を押します。利用可能な端末をもう一度検索するには、[再検索] を押します。

4 携帯端末が正常に接続された場合は、本製品の液晶画面に [接続しました] が表示されます。これで、Wi-Fi Direct® ネットワークのセットアップは完了です。

WPS（Wi-Fi Protected Setup™）のワンプッシュ方式で、Wi-Fi Direct® ネットワークを設定する

ご利用の携帯端末が WPS（PBC: Push Button Configuration）に対応している場合は、次の手順で Wi-Fi Direct® ネットワークを設定します。

メモ

本製品が携帯端末から Wi-Fi Direct® 要求を受信すると、液晶画面に [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] というメッセージが表示されます。接続するには、[OK] を押します。

1. > [ネットワーク] > [Wi-Fi Direct] > [グループオーナー] の順に押します。
2. [オン] を押します。
3. 上下にフリック、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. [Wi-Fi Direct を有効にしますか ?] が表示されたら、[オン] を押して承認します。キャンセルするには、[オフ] を押します。
5. 本製品の液晶画面に [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 ワンプッシュ設定方法をアクティブにします（手順については、お使いの携帯端末の取扱説明書をご覧ください）。本製品の [OK] を押します。
   Wi-Fi Direct® のセットアップが始まります。キャンセルするには、 を押します。
6. 携帯端末が正常に接続された場合は、本製品の液晶画面に [接続しました] が表示されます。
   Wi-Fi Direct® ネットワークのセットアップが完了しました。

PIN 方式で、Wi-Fi Direct® ネットワークを設定する

ご利用の携帯端末が Wi-Fi Direct® の PIN 方式に対応している場合は、次の手順で Wi-Fi Direct® ネットワークを設定します。

メモ

本製品が携帯端末から Wi-Fi Direct® 要求を受信すると、液晶画面に [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] というメッセージが表示されます。接続するには、[OK] を押します。

1. > [ネットワーク] > [Wi-Fi Direct] > [PIN コード接続] の順に押します。
2. [Wi-Fi Direct を有効にしますか ?] が表示されたら、[オン] を押して承認します。キャンセルするには、[オフ] を押します。
3. 本製品の液晶画面に [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、携帯端末で Wi-Fi Direct® をアクティブにします（手順については、お使いの携帯端末の取扱説明書をご覧ください）。本製品の [OK] を押して、Wi-Fi Direct® のセットアップを開始します。キャンセルするには、 を押します。

4 次の操作のいずれかを実行してください。

- 本製品がグループオーナー（G/O）に設定されている場合、本製品は携帯端末からの接続要求を待機します。本製品に [PIN コード接続] が表示されたら、携帯端末上に表示された PIN コードを入力します。[OK] を押してセットアップを完了します。

  PIN コードが本製品に表示された場合は、この PIN コードを携帯端末に入力します。

- 本製品がグループオーナー（G/O）に設定されていない場合、表示された機器名を使用して、Wi-Fi Direct® ネットワークを設定できます。接続先の携帯端末を選択し、[OK] を押します。

  利用可能な端末をもう一度検索するには、[再検索] を押します。

5 次の操作のいずれかを実行してください。

- [PIN Code 表示] を押して、本製品上に PIN コードを表示し、この PIN コード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 コードを本製品に入力し、[OK] を押します。次の手順に進みます。

  携帯端末に PIN コードが表示されない場合は、本製品の を押します。

  最初の手順に戻って、もう一度やり直します。

6 携帯端末が正常に接続された場合は、本製品の液晶画面に [接続しました] が表示されます。
Wi-Fi Direct® ネットワークのセットアップが完了しました。

WPS（Wi-Fi Protected Setup™）の PIN 方式で、Wi-Fi Direct® ネットワーク を設定する

ご利用の携帯端末が WPS（Wi-Fi Protected Setup™）の PIN 方式に対応している場合は、次の手順で Wi-Fi Direct® ネットワークを設定します。

メモ

本製品が携帯端末から Wi-Fi Direct® 要求を受信すると、液晶画面に [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] というメッセージが表示されます。接続するには、[OK] を押します。

1 > [ネットワーク] > [Wi-Fi Direct] > [グループオーナー] の順に押します。

2 [オン] を押します。

3 上下にフリック、または ▲ / ▼ を押して、[PIN コード接続] オプションを選択します。[PIN コード接続] を押します。

4 [Wi-Fi Direct を有効にしますか ?] が表示されたら、[オン] を押して承認します。キャンセルするには、[オフ] を押します。

5 [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 設定方法をアクティブにした後（手順については、お使いの携帯端末の取扱説明書をご覧ください）、本製品の [OK] を押します。
Wi-Fi Direct® のセットアップが始まります。キャンセルするには、 を押します。

6 本製品が携帯端末からの接続要求を待機します。本製品に [PIN コード接続] が表示されたら、携帯端末上に表示された PIN コードを入力します。[OK] を押します。

7 携帯端末が正常に接続された場合は、本製品の液晶画面に [接続しました] が表示されます。
これで、Wi-Fi Direct® ネットワークのセットアップは完了です。

Wi-Fi Direct® ネットワークを手動で設定する

ご利用の携帯端末が Wi-Fi Direct® にも WPS にも対応していない場合、Wi-Fi Direct® ネットワークを手動で設定する必要があります。

メモ

本製品が携帯端末から Wi-Fi Direct® 要求を受信すると、液晶画面に [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] というメッセージが表示されます。接続するには、[OK] を押します。

1. > [ネットワーク] > [Wi-Fi Direct] > [手動入力] の順に押します。
2. [Wi-Fi Direct を有効にしますか ?] が表示されたら、[オン] を押して承認します。キャンセルするには、[オフ] を押します。
3. 本製品に SSID 名とパスワードが 2 分間表示されます。携帯端末の無線 LAN 設定画面に進み、SSID 名とパスワードを入力します。
4. 携帯端末が正常に接続された場合は、本製品の液晶画面に [接続しました] が表示されます。
Wi-Fi Direct® ネットワークのセットアップが完了しました。

4 ウェブブラウザーによる管理

概要

標準ウェブブラウザーを使用することで、ネットワークに接続されているパソコンから、HTTP（ハイパーテキスト転送プロトコル）または HTTPS（ハイパーテキスト転送プロトコルセキュア）を利用して本製品を管理することができます。

- 本製品およびスキャンサーバーのステータス情報、メンテナンス情報、ソフトウェアのバージョン情報を取得する。
- ネットワークと本製品の設定を変更する（*本製品を設定する*（39 ページ）をご覧ください）。
- 他人からの不正アクセスを防止するように設定する。
  - *ログインパスワードを設定する*（40 ページ）をご覧ください。
  - *Active Directory の LDAP 認証を設定する*（43 ページ）をご覧ください。
- ネットワークを設定したり、設定を変更したりする。
  - *スキャン to FTP の設定を変更する*（49 ページ）をご覧ください。
  - *スキャン to SFTP の設定を変更する*（51 ページ）をご覧ください。
  - *スキャン to ネットワークの設定を変更する（Windows®）*（53 ページ）をご覧ください。
  - *SNTP サーバーと同期する*（47 ページ）をご覧ください。
  - *LDAP の操作*（44 ページ）をご覧ください。
  - *TCP/IP の詳細設定*（57 ページ）をご覧ください。
- アドレス帳のインポート / エクスポート。（*アドレス帳のインポート / エクスポート*（59 ページ）をご覧ください。）

メモ

Windows® の場合は Microsoft® Internet Explorer® 8.0/10.0/11.0、Macintosh の場合は Safari 8.0 のご使用をお勧めします。いずれのウェブブラウザーを使用する場合でも、JavaScript とクッキーは常に有効にして使用してください。別のウェブブラウザーを使用する場合は、HTTP 1.0 および HTTP 1.1 と互換性があることを確認してください。

ネットワーク上では TCP/IP プロトコルを使用してください。また、スキャンサーバーとコンピューターに登録済みの有効な IP アドレスが必要になります。

本製品を設定する

1. ウェブブラウザーによる管理を開始します。

   a ウェブブラウザーを起動します。

   b ブラウザーのアドレスバーに、本製品の IP アドレスを入力します。
   例：http://192.168.1.2

メモ

- ドメインネームシステムを使用している場合または NetBIOS 名を有効にしている場合は、IP アドレスの代わりに「SharedScanner」などのような名前を入力できます。
  - 例：
    http://SharedScanner/

  NetBIOS 名を有効にした場合は、ノード名も使用できます。
  - 例：
    http://brwxxxxxxxxxxxx/

  NetBIOS 名は、本製品の操作パネルの［ﾉｰﾄﾞ名］にあります。
- ウェブブラウザーを使用して設定を行うときにセキュア HTTPS プロトコルを使用するには、ウェブブラウザーを起動する前に、CA 証明書を設定する必要があります。*複数の証明書を管理する*（70 ページ）をご覧ください。

2. お買い上げ時の設定では、パスワードは必要ありません。パスワードを設定してある場合はパスワードを入力し、→ を押します。

3. これで本製品の設定を行うことができます。

メモ

プロトコル設定を変更した場合は、設定内容を有効にするため、**OK** をクリックした後、本製品を再起動してください。

ログインパスワードを設定する

ウェブブラウザーによる管理画面への不正アクセスを防止するため、ログインパスワードを設定することをお勧めします。

1. ウェブブラウザーを起動し、本製品にアクセスします（39 ページの ❶ を参照）。
2. 本製品の管理画面が表示されたら、**管理者設定** タブをクリックし、左側にあるナビゲーションバーの **ログインパスワード** をクリックします。
3. 使用したいパスワードを入力します（最大 32 文字）。
4. **新しいパスワードの確認** フィールドにもう一度パスワードを入力します。
5. **OK** をクリックします。
   次回以降、ウェブブラウザーで管理画面にアクセスするときは、**ログイン** ボックスにパスワードを入力し、→ をクリックします。
   設定が終了したら、→ をクリックしてログオフします。

メモ

管理画面の **パスワードを設定してください** をクックすることでログインパスワードを設定することもできます。

LDAP 認証を使う

LDAP 認証について

LDAP 認証を使用すると、本製品の使用を制限できます。LDAP 認証を有効にすると、本製品の操作パネルがロックされます。ユーザー ID とパスワードを入力するまで、本製品の設定を変更することはできません。

- 着信した印刷データを保管する。
- 着信したファクスデータを保管する。
- スキャンデータを E メールサーバーに送信するときに、ユーザー ID によって LDAP サーバーからメールアドレスを取得する。
  この機能を使用するには、**メールアドレス取得** オプションを選択します。スキャンデータが本製品から E メールサーバーに送信される際に、お客様のメールアドレスが送信者名として設定されます。スキャンデータをご自分のメールアドレスに送信する場合は、お客様のメールアドレスが受信者名として設定されます。

LDAP 認証設定は、ウェブブラウザーでアクセスできる本製品の管理画面または BRAdmin Professional 3（Windows®）を使用して変更できます。

ウェブブラウザーを使用して LDAP 認証を設定する

1. ウェブブラウザーを起動します。
2. ブラウザーのアドレスバーに「http:// 製品の IP アドレス」と入力します（「製品の IP アドレス」は、本製品の IP アドレス）。
   例：http://192.168.1.2
3. **管理者設定** タブをクリックします。
4. 左にあるナビゲーションバーの **制限機能** メニューをクリックします。
5. **LDAP 認証** を選択します。
6. **OK** をクリックします。
7. 左にあるナビゲーションバーの **LDAP 認証** を選択します。

8 次の設定を行います。

オプション	詳細
ユーザー ID を記憶	ご自分のユーザー ID を保存するには、このオプションを選択します。
LDAP アドレス	LDAP サーバーの IP アドレスまたはサーバー名を入力します（例：ad.example.com）。
メールアドレス取得	LDAP サーバーから本製品のメールアドレスを取得するには、このオプションを選択します。
LDAP ポート	LDAP サーバーのポート番号を入力します。
LDAP 検索場所	LDAP 検索のルートを入力します。
名前属性名 (検索する属性)	検索キーとする属性を入力します。

9 **OK** をクリックします。

本製品の操作パネルからログオンして製品の設定を変更する

メモ

LDAP 認証が有効になっている場合、本製品の操作パネルでユーザー ID とパスワードを入力するまで、本製品の操作パネルはロックされています。

1 本製品の操作パネルで、タッチパネルを使用してユーザー ID とパスワードを入力します。

2 [OK] を押します。

3 認証されると、製品の操作パネルのロックが解除されます。

ユーザーのアクセスを制限する

Active Directory の LDAP 認証を設定する

Active Directory 認証を使用すると、本製品の使用を制限できます。Active Directory 認証が有効になっていると、本製品の操作パネルがロックされています。スキャン機能を使用するには、ユーザー ID、ドメイン名、およびパスワードを入力します。

メモ

- Active Directory 認証は Kerberos 認証に対応しています。
- 最初に、SNTP（シンプルネットワークタイムプロトコル）（ネットワークタイムサーバー）を設定する必要があります。

1. ウェブブラウザーを起動し、本製品にアクセスします（39 ページの ❶ を参照）。
2. **管理者設定** タブをクリックします。
3. 左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。
4. **AD 認証機能** を選択します。
5. **OK** をクリックします。
6. 左にあるナビゲーションバーの **Active Directory 認証** を選択します。
7. 次の設定を行います。
   - **ユーザー ID を記憶**

     ご自分のユーザー ID を保存するには、このオプションを選択します。
   - **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」）。
   - **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**

     LDAP サーバーから本製品のメールアドレスを取得するには、このオプションを選択します（認証方式が **LDAP + kerberos** の場合にのみ選択できます）。
   - **ユーザーのホームディレクトリ取得**

     お客様のホームディレクトリを取得し、ネットワーク スキャンの送信先として設定するには、このオプションを選択します。

■ **LDAP ポート**

LDAP サーバーのポート番号を入力します（認証方式が **LDAP + kerberos** の場合にのみ入力できます）。

■ **LDAP 検索場所**

LDAP 検索のルートを入力します（認証方式が **LDAP + kerberos** の場合にのみ入力できます）。

■ **DN 取得**

画面の指示に従います。

■ **SNTP**

SNTP プロトコルについて詳しくは、47 ページをご覧ください。

8 **OK** をクリックします。

Active Directory 認証が有効の場合、本製品をロック解除する

1 本製品の液晶画面で、タッチパネルを使用して [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 入力したデータが認証されると、操作パネルのロックが解除され、スキャン機能が使用できるようになります。

メモ

AD 認証機能 が有効になっている場合は、どの設定も変更できません。

LDAP の操作

LDAP プロトコルを利用することで、スキャン to E メール機能で、サーバーに登録されているメールアドレスを検索できます。

LDAP 設定の変更

1 ウェブブラウザーを起動し、本製品にアクセスします（39 ページの ❶ を参照）。

2 本製品のウェブページで **ネットワーク** をクリックします。

3 左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。

4 **LDAP** チェックボックスを選択し、**OK** をクリックします。

5 設定を有効にするには、本製品を再起動します。

6 パソコンの、本製品の管理画面で **アドレス帳** タブを開き、左にあるナビゲーションバーの **LDAP** を選択します。

7 次の LDAP 設定を行います。

- **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**

  使用している認証方式によっては、設定できません。
- **パスワード**

  使用している認証方式によっては、設定できません。
- **Kerberos サーバーアドレス**

  使用している認証方式によっては、設定できません。
- **SNTP**
- **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**

8 設定が終了したら、**OK** をクリックします。テスト結果のページで **状態** が **OK** になっていることを確認してください。

メモ

- LDAP プロトコルは、中国語（簡体字 / 繁体字）、韓国語には対応していません。
- LDAP サーバーが Kerberos 認証に対応している場合は、**認証方式** の設定で Kerberos を選択することをお勧めします。LDAP サーバーと本製品間で、強力な認証方式を利用できます。Kerberos 認証を使用する場合は、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、本製品の操作パネルで日付、時刻、タイムゾーンを正確に設定してください。（SNTP の設定については、*SNTP サーバーと同期する*（47 ページ）をご覧ください。）

本製品の操作パネルを使用した LDAP 設定の変更

LDAP 設定を行った後、本製品上で LDAP 検索を使用して、E メールアドレスを検索します。

1 スキャナーで読み取り、本製品に E メールで添付ファイルとして送信したい原稿をセットします。

2 本製品の液晶画面で、[E メール送信] を押します。

3 [アドレス帳] を押します。

4 検索するには、  を押します。

5 液晶画面のボタンで、検索したい文字列の先頭の何文字かを入力します。

メモ

- 最大 15 文字まで入力できます。
- 文字の入力方法について詳しくは、『*ユーザーズガイド*』の「*文字の入力方法*」をご覧ください。

6 ［OK］を押します。
LDAP 検索の結果が液晶画面に表示されます。ローカルアドレス帳からの検索結果には、先頭に が付いています。サーバーにもローカルアドレス帳にも検索条件に一致するものがないと、液晶画面に［検索結果がありません］が表示されます。

7 ▲または▼を押してスクロールし、目的の名前が表示されたら、その名前を押します。

8 複数のメールアドレスが検索結果として表示された場合、ご希望のメールアドレスを押します。

9 ［送信先に設定］を押します。

10 ［OK］を押します。

メモ

文書をスキャンする前に、スキャン設定を調整する場合は、［設定変更］を押します。

11 ［スタート］を押します。

メモ

- 本製品の LDAP 機能は、LDAPv3 に対応しています。
- 詳しくは、LDAP 設定画面の右にある をクリックしてください。

SNTP サーバーと同期する

本製品が認証に使用する時刻（本製品の液晶画面に表示される時刻ではありません）と SNTP タイムサーバーとの同期には、SNTP（シンプルネットワークタイムプロトコル）が使用されます。本製品で使用される時刻を、SNTP タイムサーバーによって提供される UTC（協定世界時刻）と一定の間隔で同期させることができます。

メモ

- 一部の国では、この機能は利用できません。
- SNTP 機能に関して初期設定の変更が必要なのは、「時計設定」だけです。

1. ウェブブラウザーを起動し、本製品にアクセスします（39 ページの ❶ を参照）。
2. 本製品の管理画面が表示されたら、**ネットワーク** をクリックし、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. **SNTP** チェックボックスを選択します。
4. **詳細設定** をクリックします。

■ **状態**

SNTP サーバー設定が有効か無効かを表示します。

■ **同期状態**

最新の同期状態を確認します。

■ **SNTP サーバー設定の方法**

AUTO または **STATIC** を選択します。

- **AUTO**

  ネットワーク上に DHCP サーバーがあれば、SNTP サーバーが自動的に DHCP サーバーからアドレスを取得します。

- **STATIC**

  使用したいアドレスを入力します。

■ **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**

サーバーアドレスを 64 文字以内で入力します。

セカンダリー SNTP サーバーアドレスは、プライマリー SNTP サーバーアドレスの予備として使用されます。プライマリーサーバーが利用できない場合、本製品はセカンダリー SNTP サーバーと通信します。

■ **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 から 65535）。

セカンダリー SNTP サーバーポートは、プライマリー SNTP サーバーポートの予備として使用されます。プライマリーポートが利用できない場合、本製品はセカンダリー SNTP ポートと通信します。

■ **同期間隔**

サーバーとの同期の試行間隔（1 時間から 168 時間）を入力します。

メモ

- 本製品が使用する時刻を SNTP タイムサーバーと同期させるには、**時計設定**を設定する必要があります。**時計設定** をクリックし、**基本設定** 画面で **時計設定** を設定します。

- **SNTP サーバーと同期する** チェックボックスを選択します。タイムゾーンの設定が正しいことを確認し、**タイムゾーン** ドロップダウンリストから UTC との時差を選択してください。例えば、日本のタイムゾーンは、UTC+9:00 です。

5 **OK** をクリックします。

スキャン to FTP の設定を変更する

スキャン to FTP の機能を利用すると、原稿をスキャンしてローカルネットワークやインターネット上の FTP サーバーに直接送ることができます。スキャン to FTP について詳しくは、『*ユーザーズガイド*』の「*原稿をスキャンして直接 FTP サーバーに送る*」をご覧ください。

1. ウェブブラウザーを起動し、本製品にアクセスします（39 ページの ❶ を参照）。
2. 本製品の管理画面が表示されたら、**スキャン** タブをクリックし、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** をクリックします。
3. プロファイルの番号（1 ～ 25）から、**FTP** チェックボックスを選択します。
4. **OK** をクリックします。
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** をクリックします。
6. 手順 ❸ で選択したプロファイル番号の **FTP** をクリックします。
   スキャン to FTP に関して次の設定が行えます。
   - **プロファイル名**（最大 15 文字）
   - **サーバー アドレス**
   - **ユーザー名**
   - **パスワード**
   - **転送先フォルダー**
   - **ファイル名**
   - **画質**
   - **カラー自動検出調整**
   - **ファイル形式**
   - **原稿サイズ**
   - **エッジ調整**
   - **ファイルサイズ**
   - **ADF 傾き補正**
   - **白紙除去**
   - **白紙除去レベル調整**
   - **両面読取**
   - **明るさ**
   - **コントラスト**
   - **継続スキャン**
   - **パッシブモード**
   - **ポート番号**

FTP サーバーやネットワークのファイアウォールの設定に応じて、**パッシブモード** を **オフ** または **オン** に設定してください。お買い上げ時の設定は **オン** です。FTP サーバーへのアクセスに使用するポート番号も変更できます。お買い上げ時の設定は、ポート 21 です。この 2 つの設定は、ほとんどの場合、お買い上げ時の設定から変更する必要はありません。

7 **OK** をクリックします。

スキャン to SFTP の設定を変更する

スキャン to SFTP の機能を利用すると、原稿をスキャンしてローカルネットワークやインターネット上の SFTP サーバーに直接送ることができます。スキャン to SFTP について詳しくは、『*ユーザーズガイド*』の「*原稿をスキャンして直接 SFTP サーバーに送る*」をご覧ください。

1. ウェブブラウザーを起動し、本製品にアクセスします（39 ページの ❶ を参照）。
2. 本製品の管理画面が表示されたら、**スキャン** タブをクリックし、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** をクリックします。
3. プロファイルの番号（1 ～ 25）から、**SFTP** チェックボックスを選択します。
4. **OK** をクリックします。
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** をクリックします。
6. 手順 ❸ で選択したプロファイル番号の **SFTP** をクリックします。
   スキャン to SFTP に関して次の設定が行えます。
   - **プロファイル名**（最大 15 文字）
   - **サーバー アドレス**
   - **ユーザー名**
   - **認証方法**
   - **パスワード**
   - **クライアント鍵ペア**
   - **サーバー公開鍵**
   - **転送先フォルダー**
   - **ファイル名**
   - **画質**
   - **カラー自動検出調整**
   - **ファイル形式**
   - **原稿サイズ**
   - **エッジ調整**
   - **ファイルサイズ**
   - **ADF 傾き補正**
   - **白紙除去**
   - **白紙除去レベル調整**
   - **両面読取**

■ **明るさ**

■ **コントラスト**

■ **継続スキャン**

■ **ポート番号**

SFTP サーバーへのアクセスに使用されるポート番号を変更できます。
お買い上げ時の設定は、ポート 21 です。この設定は、ほとんどの場合、お買い上げ時の設定から変更する必要はありません。

7 **OK** をクリックします。

スキャン to ネットワークの設定を変更する（Windows®）

スキャン to ネットワークの機能を利用すると、原稿をスキャンしてローカルネットワークやインターネット上にある共有フォルダーに直接送ることができます。スキャン to ネットワークについて詳しくは、『*ユーザーズガイド*』の「*原稿をスキャンして直接 CIFS サーバーに送る（Windows®）*」をご覧ください。

メモ

スキャン to ネットワークは、NTLMv2 認証に対応しています。

認証のために、SNTP プロトコル（ネットワークタイムサーバー）を設定するか、あるいは、本製品の操作パネルで日付、時刻、タイムゾーンを正確に設定する必要があります。（SNTP の設定に手は、*SNTP サーバーと同期する*（47 ページ）をご覧ください。日付、時刻、タイムゾーンの設定については、『*ユーザーズガイド*.』をご覧ください。）

1. ウェブブラウザーを起動し、本製品にアクセスします（39 ページの ❶ を参照）。
2. 本製品の管理画面が表示されたら、**スキャン** タブをクリックし、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** をクリックします。
3. プロファイルの番号（1 ～ 25）から、**ネットワーク** チェックボックスを選択します。
4. **OK** をクリックします。
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** をクリックします。
6. 手順 ❸ で選択したプロファイル番号の **ネットワーク** をクリックします。
   スキャン to ネットワークに関して次の設定が行えます。
   - **プロファイル名**（最大 15 文字）
   - **ネットワークフォルダパス**
   - **ファイル名**
   - **画質**
   - **カラー自動検出調整**
   - **ファイル形式**
   - **原稿サイズ**
   - **エッジ調整**
   - **ファイルサイズ**
   - **ADF 傾き補正**
   - **白紙除去**
   - **白紙除去レベル調整**
   - **両面読取**
   - **明るさ**

- **コントラスト**
- **継続スキャン**
- **接続時にパスワード認証を行う**
- **接続パスワード**
- **認証方式**
- **ユーザー名**
- **パスワード**
- **時計設定**

7 **OK** をクリックします。

スキャン to SharePoint の設定を変更する（Windows®）

SharePoint

スキャンした文書を共有する必要がある場合、原稿をスキャンして SharePoint サーバーに直接送ることができます。さまざまなプロファイルを設定して、お好みの スキャン to SharePoint 送信先を保存しておくと、さらに利便性が高まります。スキャン to SharePoint について詳しくは、『*ユーザーズガイド*』の「*原稿をスキャンして直接 SharePoint に送る*」をご覧ください。

メモ

スキャン to SharePoint は、NTLMv2 認証方式に対応しています。

認証のために、SNTP プロトコル（ネットワークタイムサーバー）を設定するか、あるいは、本製品の操作パネルで日付、時刻、タイムゾーンを正確に設定する必要があります。（SNTP の設定に手は、*SNTP サーバーと同期する*（47 ページ）をご覧ください。日付、時刻、タイムゾーンの設定については、『*ユーザーズガイド*.』をご覧ください。）

1. ウェブブラウザーを起動し、本製品にアクセスします（39 ページの ❶ を参照）。
2. 本製品の管理画面が表示されたら、**スキャン** タブをクリックし、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** をクリックします。
3. プロファイルの番号（1 ～ 25）から、**SharePoint** チェックボックスを選択します。
4. **OK** をクリックします。
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** をクリックします。
6. 手順 ❸ で選択したプロファイル番号の **SharePoint** をクリックします。
   スキャン to SharePoint に関して次の設定が行えます。
   - **プロファイル名**（最大 15 文字）
   - **SharePoint サイトのアドレス**
   - **SSL/TLS**

メモ

SSL/TLS は、**SharePoint サイトのアドレス** で **HTTPS** を選択した場合にのみ、表示されます。

   - **ファイル名**
   - **画質**
   - **カラー自動検出調整**
   - **ファイル形式**
   - **原稿サイズ**
   - **エッジ調整**
   - **ファイルサイズ**

- **ADF 傾き補正**
- **白紙除去**
- **白紙除去レベル調整**
- **両面読取**
- **明るさ**
- **コントラスト**
- **継続スキャン**
- **接続時にパスワード認証を行う**
- **接続パスワード**
- **認証方式**
- **ユーザー名**
- **パスワード**
- **時計設定**

7 **OK** をクリックします。

TCP/IP の詳細設定

1. ウェブブラウザーを起動し、本製品にアクセスします（39 ページの ❶ を参照）。
2. **ネットワーク** タブをクリックし、接続タイプ（**有線** または **無線**）を選択します。
3. 左にあるナビゲーションバーの **TCP/IP** を選択します。
4. **詳細設定** をクリックします。次の設定を行います。（画像は **TCP/IP 詳細設定（無線）**。）

■ **起動の試行回数**

IP 取得方法を使った起動の試行回数（0 から 32767）を入力します。

■ **RARP 設定**

サブネットマスクを自動変更しない または **ゲートウェイアドレスを自動変更しない** を選択します。

- **サブネットマスクを自動変更しない**
  サブネットマスクは自動的に変更されません。
- **ゲートウェイアドレスを自動変更しない**
  ゲートウェイアドレスは自動的に変更されません。

■ **TCP タイムアウト**

TCP タイムアウトまでの時間（分数）を入力します（0 から 32767）。

■ **DNS サーバーアドレス設定**

AUTO または **STATIC** を選択します。

■ **プライマリー DNS サーバー IP、セカンダリー DNS サーバー IP**

サーバーの IP アドレスを入力します。

セカンダリー DNS サーバー IP アドレスは、プライマリー DNS サーバー IP アドレスの予備として使用されます。
プライマリー DNS サーバーが利用できない場合、本製品はセカンダリー DNS サーバーと通信します。

■ **ルーターに対するタイムアウト**

ルーターがタイムアウトするまでの時間（秒数）を入力します（1 から 32767）。

5 **OK** をクリックします。

アドレス帳のインポート / エクスポート

アドレス帳のインポート

1. ウェブブラウザーを起動し、本製品にアクセスします（39 ページの ❶ を参照）。
2. **アドレス帳** タブをクリックします。
3. 左にあるナビゲーションバーの **インポート** を選択します。
4. **" アドレス帳 " データファイル** または **" グループダイヤル " データファイル** を入力します。
5. **OK** をクリックします。

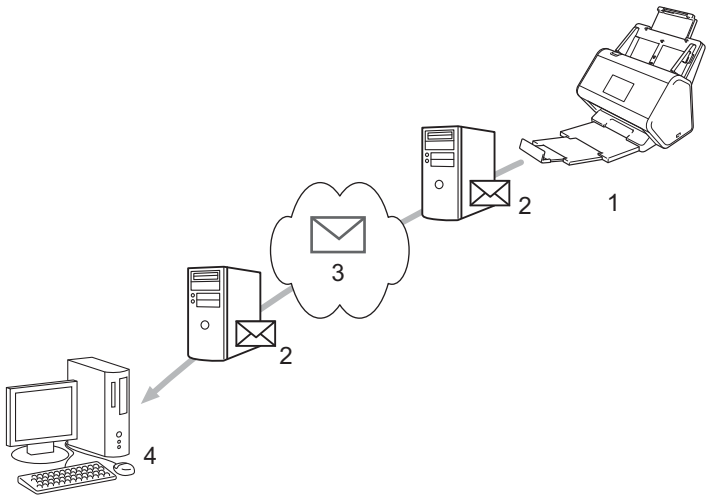
アドレス帳のエクスポート

1. ウェブブラウザーを起動し、本製品にアクセスします（39 ページの ❶ を参照）。
2. **アドレス帳** タブをクリックします。
3. 左にあるナビゲーションバーの **エクスポート** を選択します。
4. **ファイルへ出力** ボタンをクリックします。

5 スキャン to E メール

概要

スキャン to E メールの機能を利用して、スキャンデータを E メールの添付ファイルで送信することができます。



1 送信者

2 E メールサーバー

3 インターネット

4 受信者

スキャン to E メール使用時のサイズ制限

原稿の画像データが大きすぎると、送信できない場合があります。

スキャン to E メールの設定

スキャン to E メール機能を利用するには、ネットワークやメールサーバーと通信できるように本製品の設定を行っておく必要があります。この設定は、ウェブブラウザー、リモートセットアップ、または BRAdmin Professional 3 で行うことができます。本製品で次の情報が設定されている必要があります。

- IP アドレス（すでに本製品をネットワーク上で使用している場合は、本製品の IP アドレスは正しく設定されています。）
- E メールアドレス
- SMTP サーバーのアドレス / ポート / 認証方式 / 暗号化方式 / サーバー証明書の検証
- SMTP-AUTH アカウント名とパスワード

ご不明な点は、ネットワーク管理者にお問い合わせください。

メモ

本製品で E メールアドレスの設定を行う必要がありますが、本製品で E メールを受信する機能はありません。そのため、本製品から送信された E メールに受信者が返信しても、その E メールを本製品で受信することはできません。

スキャン to E メールを利用する前に

次の項目を設定する必要がある場合があります（設定はウェブブラウザーまたはリモートセットアップを使って行います）。

- 件名
- サイズの制限
- 受信確認要求（詳しくは、*受信確認（TX）メール*（63 ページ）をご覧ください）

スキャン to E メールの利用方法

1. 文書をセットします。
2. 左右にフリック、または ◀/▶ を押して、[E メール送信] を表示します。
3. 使用したい E メールアドレスを選択し、[OK] を押します。
4. [スタート] を押します。

E メール設定について詳しくは、『*ユーザーズガイド*』の「*原稿をスキャンして直接 E メールアドレスに送る*」をご覧ください。

原稿がスキャンされ、そのデータが SMTP サーバーを通じて指定した E メールアドレスに自動的に送信されます。
送信が完了すると、本製品の液晶画面にホーム画面が表示されます。

メモ

一部の E メールサーバーでは、大きな E メール文書を送信できません（システム管理者が最大 E メールサイズの制限を設定している場合があります）。スキャン to E メール機能が有効になっているときは、1 MB を超えるサイズの E メールを送信しようとすると、[メモリがいっぱいです] というメッセージが本製品の画面に表示され、スキャンデータは送信されません。E メールの文書を E メールサーバーの制限内の大きさに分割する必要があります。

スキャン to E メールのその他の機能

受信確認（TX）メール

受信確認（TX）メールの機能を利用して、受信者が E メールを受信して開いたら通知を受け取るように設定することができます。

メール送信設定

本製品の操作パネルを使用して、この確認機能をオンにします。[メール 送信設定] が [オン] のときは、E メールに追加のフィールドが含まれ、E メールの受信日時が自動的に記録されます。

1. 本製品の液晶画面で、 を押します。
2. [ネットワーク] を押します。
3. [E メール] を押します。
4. [メール 送信設定] を押します。
5. [受信確認] を押します。
6. [オン]（または [オフ]）を押します。

メモ

- 受信確認通知（MDN）
  このフィールドは、SMTP（Simple Mail Transfer Protocol）送信システムによって配信された後の E メールの状態を要求します。受信者がメッセージを受け取った後、製品またはユーザーが受信 E メールを読んだときにこのデータが使用されます。例えば、受信者が E メールを開いて読むと、送信元の製品またはユーザーに通知が送り返されます。
  受信者が通知を送信するためには、MDN フィールドを有効にしておく必要があります。有効にしていないと、要求が無視されます。
- 本製品には E メールの受信機能がありません。受信確認メール機能を使用するためには、別の E メールアドレスに通知を送信するよう設定する必要があります。本製品の液晶画面を使用してこの E メールアドレスを設定します。[ネットワーク] > [E メール] > [メール アドレス] を押し、通知を受信するための E メールアドレスを入力します。

6 セキュリティ機能

概要

本製品は、最新のネットワークセキュリティと暗号化プロトコルに対応しています。これらのネットワーク機能は、データの保護や、本製品への不正アクセスの防止など、総合的なネットワークセキュリティに役立ちます。

以下のセキュリティ機能を設定できます。

- 安全に E メールを送信する（*安全に E メールを送信する*（65 ページ）をご覧ください）
- 複数の証明書を管理する（*複数の証明書を管理する*（70 ページ）をご覧ください）
- クライアント鍵ペアを作成する（*クライアント鍵ペアを作成する*（67 ページ）をご覧ください）
- クライアント鍵ペアをエクスポートする（*クライアント鍵ペアをエクスポートする*（68 ページ）をご覧ください）
- サーバー公開鍵をインポートする（*サーバー公開鍵をインポートする*（69 ページ）をご覧ください）
- IPsec を使用して安全にネットワーク製品を管理する（*IPsec を使用して安全にネットワーク製品を管理する*（72 ページ）をご覧ください）
- 外部機器によるスキャン機能の利用を制限する（*外部機器によるスキャン機能の利用を制限する*（84 ページ）をご覧ください）
- 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*（85 ページ）をご覧ください）

メモ

FTP および TFTP プロトコルを無効にすることをお勧めします。これらのプロトコルを使用して製品にアクセスすることは、セキュリティ上安全ではありません。ただし、FTP を無効にすると、スキャン to FTP 機能は使用できません。（プロトコルの設定方法について詳しくは、*本製品を設定する*（39 ページ）をご覧ください。）

安全に E メールを送信する

ウェブブラウザーを使用して設定する

ユーザー認証による安全な E メールの送信、あるいは SSL/TLS を使用した E メールの送受信を設定できます。

1. ウェブブラウザーを起動します。
2. ブラウザーのアドレスバーに、本製品の IP アドレスを入力します。例：http://192.168.1.2
3. お買い上げ時の設定では、パスワードは必要ありません。パスワードを設定してある場合はパスワードを入力し、→ を押します。
4. **ネットワーク**をクリックします。
5. **プロトコル** をクリックします。
6. **SMTP** の **詳細設定** をクリックし、**SMTP** の状態が **有効** であることを確認します。
7. このページで **SMTP** を設定します。

メモ

- 設定が完了したら、テストメールを送信して E メール設定が正しいことを確認してください。
- SMTP サーバーの設定がわからない場合は、システム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. 設定が終了したら、**OK** をクリックします。**E メール送信設定テスト** ダイアログボックスが表示されます。
9. 画面の指示に従って、現在の設定でスキャンのテストを行います。

ユーザー認証を使用して E メールを送信する

本製品では、ユーザー認証を必要とする E メールサーバーを経由して E メールを送信するための、SMTP-AUTH 認証方式が優先されます。この認証方式は、不正ユーザーによる E メールサーバーへのアクセスを防止します。ウェブブラウザーまたは BRAdmin Professional 3 を使用して、これらの設定ができます。E メールでの通知やレポート、スキャン to E メールに、SMTP-AUTH 認証方式を使用できます。

E メールクライアントの設定

- お使いの E メールアプリケーションで使用されている方式にあわせて、SMTP の認証方式を設定する必要があります。
- E メールクライアントの設定については、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、**送信メールサーバー認証方式** の **SMTP-AUTH** チェックボックスを選択する必要があります。

SMTP の設定

- ウェブブラウザーで管理画面にアクセスして、SMTP ポート番号を変更できます。これは、ご使用のインターネットサービスプロバイダーが「Outbound Port 25 Blocking （OP25B）」のサービスを実施している場合に便利です。
- SMTP ポート番号を、ご使用のインターネットサービスプロバイダーが SMTP サーバーに使用している特定のポート番号（例えばポート 587 など）に変更すると、SMTP サーバーを経由して E メールを送信できるようになります。

SSL/TLS を使用して E メールを安全に送信する

本製品は、SSL/TLS 通信を必要とする E メールサーバーを経由して E メールを送信するための SSL/TLS 通信方式に対応しています。SSL/TLS 通信を使用している E メールサーバー経由で E メールを送るには、SSL/TLS を正しく設定する必要があります。

サーバー証明書の検証について

- **SSL/TLS** で **SSL** または **TLS** を選択した場合は、**サーバー証明書の検証** を行うため、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。
  - E メールの送信時、サーバーとの接続が試行されるときに、サーバー証明書が検証されます。
  - サーバー証明書を検証する必要がない場合は、**サーバー証明書を検証** チェックボックスを選択解除してください。

ポート番号

- **SSL** または **TLS** を選択した場合は、そのプロトコルに合わせて **ポート** の値が変わります。ポート番号を手動で変更するには、**SSL/TLS** を選択し、ポート番号を入力します。
- E メールサーバーに合わせて、SMTP の通信方法を設定してください。E メールサーバーの設定について詳しくは、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にお問い合わせください。

  ほとんどの場合、安全なウェブメールサービスには次の設定が必要です。

SMTP

ポート：587

送信メールサーバー認証方式：SMTP-AUTH

SSL/TLS：TLS

SFTP のセキュリティ設定

SFTP 接続のためのセキュリティキーの設定を行うことができます。

クライアント鍵ペアを作成する

SFTP 接続の確立に必要なクライアント鍵ペアを作成します。

1. ウェブブラウザーを起動します。
2. ブラウザーのアドレスバーに、本製品の IP アドレスを入力します。例：http://192.168.1.2。

メモ

- ドメインネームシステムを使用している場合または NetBIOS 名を有効にしている場合は、IP アドレスの代わりに「SharedScanner」などのような名前を入力できます。
  - 例：
    http://SharedScanner/

  NetBIOS 名を有効にした場合は、ノード名も使用できます。
  - 例：
    http://brnxxxxxxxxxxxx/

  NetBIOS 名は、ネットワーク設定レポートで確認できます。

3. お買い上げ時の設定では、パスワードは必要ありません。パスワードを設定してある場合はパスワードを入力し、→ を押します。
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** フィールドに、任意の名前（最大 20 文字）を入力します。
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、アルゴリズムを選択します。
10. **OK** をクリックします。
    クライアント鍵ペアが作成されて、本製品のメモリに保存されます。クライアント鍵ペア名と公開鍵アルゴリズムが **クライアント鍵ペア一覧** に表示されます。

クライアント鍵ペアをエクスポートする

認証プロトコルとして公開鍵を選択すると、SFTP 接続の確立時にクライアント鍵ペアが使用されます。

1. ウェブブラウザーを起動します。
2. ブラウザーのアドレスバーに、本製品の IP アドレスを入力します。例：http://192.168.1.2。

メモ

- ドメインネームシステムを使用している場合または NetBIOS 名を有効にしている場合は、IP アドレスの代わりに「SharedScanner」などのような名前を入力できます。
  - 例：
    http://SharedScanner/

  NetBIOS 名を有効にした場合は、ノード名も使用できます。
  - 例：
    http://brnxxxxxxxxxxxx/

  NetBIOS 名は、ネットワーク設定レポートで確認できます。

3. お買い上げ時の設定では、パスワードは必要ありません。パスワードを設定してある場合はパスワードを入力し、→ を押します。
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** と一緒に表示される **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. ファイルの保存先とする場所を指定します。

クライアント鍵ペアがパソコンにエクスポートされます。

サーバー公開鍵をインポートする

スキャン to SFTP を使用する際、SFTP 接続の確立時にサーバー公開鍵が使用されます。

1. ウェブブラウザーを起動します。
2. ブラウザーのアドレスバーに、本製品の IP アドレスを入力します。例：http://192.168.1.2。

メモ

- ドメインネームシステムを使用している場合または NetBIOS 名を有効にしている場合は、IP アドレスの代わりに「SharedScanner」などのような名前を入力できます。
  - 例：
    http://SharedScanner/

  NetBIOS 名を有効にした場合は、ノード名も使用できます。
  - 例：
    http://brnxxxxxxxxxxxx/

  NetBIOS 名は、ネットワーク設定レポートで確認できます。

3. お買い上げ時の設定では、パスワードは必要ありません。パスワードを設定してある場合はパスワードを入力し、→ を押します。
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. **サーバー公開鍵一覧** と一緒に表示される **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。

サーバー公開鍵が本製品にインポートされます。

複数の証明書を管理する

本製品にインストールされた複数の証明書は、ウェブブラウザーを使用して管理することができます。ウェブブラウザーでアクセスできる本製品の管理画面で、**CA 証明書** 画面を表示し、証明書の内容を確認したり、証明書を削除あるいはエクスポートしたりできます。

SSL を使用するための CA 証明書は 3 つまで格納できます。

証明書の有効期限が切れた場合に対処できるように、格納する証明書の数を最大数よりも 1 つ少なくしておくことをお勧めします。証明書の有効期限が切れた場合には、予備の格納場所に新しい証明書をインポートしてから期限切れの証明書を削除することができ、設定の失敗を避けることができます。

メモ

SMTP 用の SSL 通信を使用する場合には、証明書を選ぶ必要はありません。必要な証明書が自動的に選択されます。

CA 証明書をインポートする

1. ウェブブラウザーを起動します。
2. ブラウザーのアドレスバーに、本製品の IP アドレスを入力します。例：http://192.168.1.2。

メモ

- ドメインネームシステムを使用している場合または NetBIOS 名を有効にしている場合は、IP アドレスの代わりに「SharedScanner」などのような名前を入力できます。
  - 例：
    http://SharedScanner/

  NetBIOS 名を有効にした場合は、ノード名も使用できます。
  - 例：
    http://brwxxxxxxxxxxxx/

  NetBIOS 名は、本製品の操作パネルの ［ ﾉｰﾄﾞ名 ］ にあります。

3. お買い上げ時の設定では、パスワードは必要ありません。パスワードを設定してある場合はパスワードを入力し、➔ を押します。
4. **ネットワーク** タブをクリックし、**セキュリティ** をクリックします。
5. **CA 証明書** をクリックします。
6. **CA 証明書のインポート** をクリックし、証明書を選択します。
7. **OK** をクリックします。

CA 証明書をエクスポートする

1. ウェブブラウザーを起動します。
2. ブラウザーのアドレスバーに、本製品の IP アドレスを入力します。例：http://192.168.1.2。

メモ

- ドメインネームシステムを使用している場合または NetBIOS 名を有効にしている場合は、IP アドレスの代わりに「SharedScanner」などのような名前を入力できます。
  - 例：
    http://SharedScanner/

  NetBIOS 名を有効にした場合は、ノード名も使用できます。
  - 例：
    http://brwxxxxxxxxxxxx/

  NetBIOS 名は、本製品の操作パネルの［ﾉｰﾄﾞ名］にあります。

3. お買い上げ時の設定では、パスワードは必要ありません。パスワードを設定してある場合はパスワードを入力し、を押します。
4. **ネットワーク** タブをクリックし、**セキュリティ** をクリックします。
5. **CA 証明書** をクリックします。
6. 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。
7. **OK** をクリックします。

IPsec を使用して安全にネットワーク製品を管理する

■ IPsec について

IPsec（インターネットプロトコルセキュリティ）は、セキュリティプロトコルの 1 つで、オプションのインターネットプロトコル機能を使用することで、IP パケットとして送信されるデータの改ざんを防止し、データの機密性を確保します。IPsec により、ネットワーク上で送受信されるデータを暗号化します。ネットワーク層でデータが暗号化されるため、ユーザー側でとくに意識せずとも、高レベルのプロトコルを使用するアプリケーションでは IPsec が利用されています。

■ ウェブブラウザーを使用して IPsec を設定する

IPsec の接続条件は、**アドレス**および **IPsec** という 2 種類の**テンプレート**で構成されます。

最大 10 個の接続条件を設定できます。

■ ウェブブラウザーを使用して IPsec アドレステンプレートを設定する

■ ウェブブラウザーを使用して IPsec テンプレートを設定する

IPsec について

IPsec により、次の機能を利用できます。

■ IPsec 送受信

ネットワークに接続されたパソコンは、IPsec の設定条件に従って、指定の機器との間で IPsec によるデータの送受信を行います。機器間で IPsec による通信が始まると、まず IKE（Internet Key Exchange）により鍵交換が行われ、この鍵交換で得られたキーを用いて、暗号化されたデータが送受信されます。

さらに、IPsec には、トランスポートモードとトンネルモードという 2 つの動作モードがあります。トランスポートモードはおもに機器間での通信に使用され、トンネルモードはおもに VPN（仮想プライベートネットワーク）などの環境で使用されます。

メモ

IPsec 送受信を行うには、次の条件が必要です。

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

■ IPsec 設定

IPsec 接続に必要な設定を行います。IPsec 設定は、ウェブブラウザーを使用して設定できます。

メモ

IPsec 設定は、ネットワークに接続されたパソコンで、ブラウザを使用して行う必要があります。

ウェブブラウザーを使用して IPsec を設定する

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

1. ウェブブラウザーを起動します。
2. ブラウザーのアドレスバーに、本製品の IP アドレスを入力します。例：http://192.168.1.2。
3. お買い上げ時の設定では、パスワードは必要ありません。パスワードを設定してある場合はパスワードを入力し、→ を押します。
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. 左にあるナビゲーションバーの **IPsec** メニューをクリックします。
7. **状態** フィールドで、IPsec を有効または無効にします。
8. IKE フェーズ 1 の **接続モード** を選択します。
   IKE は、IPsec による暗号化通信を行うための、暗号キーの交換に利用される通信プロトコルです。**メイン** モードを選ぶと、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** モードを選ぶと、**メイン** モードより処理速度が速くなりますが、セキュリティは低下します。
9. **IPsec 以外のトラフィックルール** フィールドで、IPsec 以外のパケットに対する処理を選択します。
   Web サービスを使用する場合は、**IPsec 以外のトラフィックルール** を **通過** に設定してください。**遮断** を選択すると、Web サービスを使用できません。
10. **Broadcast/Multicast Bypass** フィールドで、**有効** または **無効** を選択します。
11. **Protocol Bypass** フィールドで、必要なオプションのチェックボックスを選択します（複数可）。
12. **ルール** 表で、有効にするテンプレートの **有効** チェックボックスを選択します。
    複数のチェックボックスを選択した場合、それらの設定が矛盾する場合は、若い番号のチェックボックスが優先されます。
13. IPsec の接続条件として使用する **アドレステンプレート** を、対応するドロップダウンリストをクリックして選択します。
    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. IPsec の接続条件として使用する **IPsec テンプレート** を、対応するドロップダウンリストをクリックして選択します。
    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。
    新しい設定値を登録するために再起動が必要な場合は、再起動確認画面が表示されます。**ルール** 表で有効にしたテンプレート内に空欄があると、エラーメッセージが表示されます。
    選択内容を確認して、もう一度 OK を押します。

ウェブブラウザーを使用して IPsec アドレステンプレートを設定する

1. ウェブブラウザーを起動します。
2. ブラウザーのアドレスバーに、本製品の IP アドレスを入力します。例：http://192.168.1.2。
3. お買い上げ時の設定では、パスワードは必要ありません。パスワードを設定してある場合はパスワードを入力し、→ を押します。
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。
   テンプレートリストが表示され、10 種類のアドレステンプレートが示されます。**アドレステンプレート** を削除する場合は **削除** ボタンをクリックします。使用中の **アドレステンプレート** は削除できません。
7. 作成する **アドレステンプレート** をクリックします。**IPsec アドレステンプレート** が表示されます。
8. **テンプレート名** フィールドに、作成する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** オプションを選択して、送信側の IP アドレス条件を次のように指定します。
   - **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** を選択した場合は、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 アドレスの範囲を、開始アドレスと終了アドレスをテキストボックスに入力して指定します。開始アドレスと終了アドレスが IPv4 または IPv6 のフォーマットの規格に準じていない場合や、終了アドレスが開始アドレスよりも小さい場合、エラーとなります。
   - **IP アドレス / プレフィックス**

     IP アドレスを CIDR 表記で指定します。

     例：192.168.1.1/24

     192.168.1.1 に対しプレフィックスを 24 ビットのサブネットマスク（255.255.255.0）で指定するため、192.168.1.xxx というアドレスが有効となります。
10. **リモート IP アドレス** オプションを選択して、受信側の IP アドレス条件を次のように指定します。
    - **すべて**

      すべての IP アドレスを有効にします。
    - **IP アドレス**

      特定の 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 アドレスの範囲を、開始アドレスと終了アドレスで指定します。開始アドレスと終了アドレスが IPv4 または IPv6 のフォーマットの規格に準じていない場合や、終了アドレスが開始アドレスよりも小さい場合、エラーとなります。

■ **IP アドレス / プレフィックス**

IP アドレスを CIDR 表記で指定します。

例：192.168.1.1/24

192.168.1.1 に対しプレフィックスを 24 ビットのサブネットマスク（255.255.255.0）で指定するため、192.168.1.xxx というアドレスが有効となります。

⑪ **OK** をクリックします。

メモ

使用中のテンプレートの設定を変更した場合は、ウェブブラウザーの IPsec 設定画面が再起動します。

ウェブブラウザーを使用して IPsec テンプレートを設定する

1. ウェブブラウザーを起動します。
2. ブラウザーのアドレスバーに、本製品の IP アドレスを入力します。例：http://192.168.1.2。
3. お買い上げ時の設定では、パスワードは必要ありません。パスワードを設定してある場合はパスワードを入力し、→ を押します。
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。
   テンプレートリストが表示され、10 種類の IPsec テンプレートが示されます。**IPsec テンプレート** を削除する場合は **削除** ボタンをクリックします。使用中の **IPsec テンプレート** は削除できません。
7. 作成する **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。
   テンプレートを使用する、**IKE** の選択内容によって、設定フィールドが異なります。
8. **テンプレート名** フィールドに、作成するテンプレートの名前を入力します（最大 16 文字）。
9. **IKE** のオプションを選択します。
10. **OK** をクリックします。

IPsec テンプレートの IKEv1 の設定

テンプレート名

作成するテンプレートの名前を入力します（最大 16 文字）。

テンプレートを使用する

カスタム、**IKEv1 高セキュリティ**、**IKEv1 中セキュリティ**、**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。ここで選択したテンプレートによって設定項目が異なります。

メモ

既定のテンプレートは、**IPsec** 設定画面の **接続モード** で、**メイン** を選択したか、**アグレッシブ** を選択したかによって異なる場合があります。

IKE

IKE は、IPsec による暗号化通信を行うための、暗号キーの交換に利用される通信プロトコルです。その場限りの暗号化通信を行って、IPsec に必要な暗号化アルゴリズムの決定と暗号キーの共有を行います。IKE では、Diffie-Hellman 鍵交換と呼ばれる手順によって暗号キーを交換し、IKE 限定の暗号化通信を行います。

テンプレートを使用する で **カスタム** を選択した場合は、**IKEv1**、**IKEv2**、または **手動** を選択します。**カスタム** 以外の設定を選択した場合は、**テンプレートを使用する** で選択した IKE、認証タイプ、および動作セキュリティが表示されます。

認証タイプ

IKE の認証方式と暗号化方式を設定します。

■ **DH グループ**

保護されていない通信経路上で、秘密キーを安全に交換するための鍵交換方式です。Diffie-Hellman 鍵交換方式では、秘密キーではなく離散対数問題を利用して、乱数と秘密キーから生成された公開情報が送受信されます。**グループ 1**、**グループ 2**、**グループ 5**、または **グループ 14** を選択します。

■ **暗号化方式**

DES、**3DES**、**AES-CBC 128**、または **AES-CBC 256** を選択します。

■ **ハッシュ**

MD5、**SHA1**、**SHA256**、**SHA384**、または **SHA512** を選択します。

■ **SA ライフタイム**

IKE SA のライフタイムを指定します。

時間（秒）と量（KB）を入力してください。

動作セキュリティ

■ **プロトコル**

ESP、**AH+ESP**、または **AH** を選択します。

メモ

- ESP は、IPsec を利用して暗号化通信を行うためのプロトコルの 1 つです。.ESP は、ペイロード（通信内容）を暗号化し、付加情報を追加します。IP パケットは、ヘッダーと、ヘッダーの後の暗号化されたペイロードから成ります。暗号化されたデータに加え、暗号化方式、暗号キー、認証データなどに関する情報も IP パケットに含まれます。
- AH（認証ヘッダー）は、IPsec プロトコルの仕様の一部で、送信元の認証やデータの改ざん防止（完全性の保証）を実現するための仕組みです。このデータは、IP パケット内のヘッダーの直後に挿入されます。また、パケットには、通信内容や秘密キーなどから一定の数式により計算されたハッシュ値も含まれ、これにより送信元の成りすましや通信内容の改ざんを防止します。ESP とは異なり、通信内容は暗号化されず、データは平文で送受信されます。

■ **暗号化方式**

DES、**3DES**、**AES-CBC 128**、または **AES-CBC 256** を選択します。暗号化方式は、**プロトコル** で **ESP** を選択し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** を選択した場合にのみ選択できます。

プロトコル で **AH+ESP** を選択した場合は、**ハッシュ (AH)** と **ハッシュ（ESP）** のプロトコルもそれぞれ選択してください。

■ **SA ライフタイム**

IPsec SA のライフタイムを指定します。

時間（秒）と量（KB）を入力してください。

■ **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）を指定します。**トンネル** モードを選択している場合にのみ、この情報を入力してください。

メモ

SA（Security Association）は、IPsec や IPv6 を利用する暗号化通信方式の 1 つで、暗号化方式や暗号キーなどの情報を交換・共有し、安全な通信路を確立してから、通信を開始します。SA は、すでに確立された仮想的な暗号通信路（トンネル）のことを指す場合もあります。IPsec による通信で利用される SA は、暗号化方式を確立し、暗号キーを交換し、IKE の標準手続に従って相互認証を行います。さらに SA は、定期的に更新されます。

PFS

PFS 方式では、過去にメッセージの暗号化に使用されたキーからキーが導出されることがありません。また、親キーから導出されたキーでメッセージが暗号化されている場合でも、その親キーを使用して他のキーが導出されることはありません。そのため、たとえキーが漏洩しても、損害は、そのキーを使用して暗号化されたメッセージに限定されます。

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

通信を暗号化する際に、事前に別の通信路を使用して暗号キーを交換・共有する方法です。

認証方式 として **事前共有キー** を選択した場合は、**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**

送信側の ID タイプを選択した後、ID を入力します。

タイプとしては、**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** を選択した場合は、証明書のコモンネームを **ID** フィールドに入力します。

■ **リモート ID タイプ /ID**

受信側の ID タイプを選択した後、ID を入力します。

タイプとしては、**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** を選択した場合は、証明書のコモンネームを **ID** フィールドに入力します。

証明書

認証方式 で **証明書** を選択した場合は、証明書を選択します。

メモ

選択できるのは、ウェブブラウザーで本製品にアクセスし、「セキュリティ」設定画面の **証明書** ページで作成した証明書だけです。

IPsec テンプレートの IKEv2 の設定

テンプレート名

作成するテンプレートの名前を入力します（最大 16 文字）。

テンプレートを使用する

カスタム、**IKEv1 高セキュリティ**、**IKEv1 中セキュリティ**、**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。ここで選択したテンプレートによって設定項目が異なります。

メモ

既定のテンプレートは、**IPsec** 設定画面の **接続モード** で、**メイン** を選択したか、**アグレッシブ** を選択したかによって異なる場合があります。

IKE

IKE は、IPsec による暗号化通信を行うための、暗号キーの交換に利用される通信プロトコルです。その場限りの暗号化通信を行って、IPsec に必要な暗号化アルゴリズムの決定と暗号キーの共有を行います。IKE では、Diffie-Hellman 鍵交換と呼ばれる手順によって暗号キーを交換し、IKE 限定の暗号化通信を行います。

テンプレートを使用する で **カスタム** を選択した場合は、**IKEv1**、**IKEv2**、または **手動** を選択します。**カスタム** 以外の設定を選択した場合は、**テンプレートを使用する** で選択した IKE、認証タイプ、および動作セキュリティが表示されます。

認証タイプ

IKE の認証方式と暗号化方式を設定します。

■ **DH グループ**

保護されていない通信経路上で、秘密キーを安全に交換するための鍵交換方式です。Diffie-Hellman 鍵交換方式では、秘密キーではなく離散対数問題を利用して、乱数と秘密キーから生成された公開情報が、送受信されます。**グループ 1**、**グループ 2**、**グループ 5**、または **グループ 14** を選択します。

■ **暗号化方式**

DES、**3DES**、**AES-CBC 128**、または **AES-CBC 256** を選択します。

■ **ハッシュ**

MD5、**SHA1**、**SHA256**、**SHA384**、または **SHA512** を選択します。

■ **SA ライフタイム**

IKE SA のライフタイムを指定します。

時間（秒）と量（KB）を入力してください。

動作セキュリティ

■ **プロトコル**

ESP を選択します。

メモ

ESP は、IPsec を利用して暗号化通信を行うためのプロトコルの 1 つです。.ESP は、ペイロード（通信内容）を暗号化し、付加情報を追加します。IP パケットは、ヘッダーと、ヘッダーの後の暗号化されたペイロードから成ります。暗号化されたデータに加え、暗号化方式、暗号キー、認証データなどに関する情報も IP パケットに含まれます。

■ **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。

時間（秒）と量（KB）を入力してください。

■ **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）を指定します。**トンネル** モードを選択している場合にのみ、この情報を入力してください。

メモ

SA（Security Association）は、IPsec や IPv6 を利用する暗号化通信方式の 1 つで、暗号化方式や暗号キーなどの情報を交換・共有し、安全な通信路を確立してから、通信を開始します。SA は、すでに確立された仮想的な暗号通信路（トンネル）のことを指す場合もあります。IPsec による通信で利用される SA は、暗号化方式を確立し、暗号キーを交換し、IKE の標準手続に従って相互認証を行います。さらに SA は、定期的に更新されます。

PFS

PFS 方式では、過去にメッセージの暗号化に使用されたキーからキーが導出されることがありません。また、親キーから導出されたキーでメッセージが暗号化されている場合でも、その親キーを使用して他のキーが導出されることはありません。そのため、たとえキーが漏洩しても、損害は、そのキーを使用して暗号化されたメッセージに限定されます。

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

通信を暗号化する際に、事前に別の通信路を使用して暗号キーを交換・共有する方法です。

認証方式 として **事前共有キー** を選択した場合は、**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**

送信側の ID タイプを選択した後、ID を入力します。

タイプとしては、**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 を選択した場合は、証明書のコモンネームを **ID** フィールドに入力します。

■ **リモート ID タイプ /ID**

受信側の ID タイプを選択した後、ID を入力します。

タイプとしては、**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 を選択した場合は、証明書のコモンネームを **ID** フィールドに入力します。

証明書

認証方式 で **証明書** を選択した場合は、証明書を選択します。

メモ

選択できるのは、ウェブブラウザーで本製品にアクセスし、「セキュリティ」設定画面の **証明書** ページで作成した証明書だけです。

EAP

EAP は、PPP を拡張した認証プロトコルです。EAP を使用した IEEE 802.1X 認証では、セッションごとに異なるキーを使用してユーザー認証が行われます。

次の設定は、**認証方式** で **EAP - MD5** または **EAP - MS-CHAPv2** を選択した場合にのみ、設定する必要があります。

■ **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）。確認のため、パスワードは 2 回入力します。

■ **証明書**

このボタンをクリックして、**証明書** 設定画面に移動します。

IPsec テンプレートの手動設定

テンプレート名

作成するテンプレートの名前を入力します（最大 16 文字）。

テンプレートを使用する

カスタム、**IKEv1 高セキュリティ**、**IKEv1 中セキュリティ**、**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。ここで選択したテンプレートによって設定が異なります。

メモ

既定のテンプレートは、**IPsec** 設定画面の **接続モード** で、**メイン** を選択したか、**アグレッシブ** を選択したかによって異なる場合があります。

IKE

IKE は、IPsec による暗号化通信を行うために、暗号キーの交換に利用される通信プロトコルです。その場限りの暗号化通信を行って、IPsec に必要な暗号化アルゴリズムの決定と暗号キーの共有を行います。IKE では、Diffie-Hellman 鍵交換と呼ばれる手順によって暗号キーを交換し、IKE 限定の暗号化通信を行います。

テンプレートを使用する で **カスタム** を選択した場合は、**IKEv1**、**IKEv2**、または **手動** を選択します。

カスタム 以外の設定を選択した場合は、**テンプレートを使用する** で選択した IKE、認証タイプ、および動作セキュリティが表示されます。

認証キー（ESP, AH）

認証に使用するキーを指定します。**In/Out** 値を入力します。

テンプレートを使用する で **カスタム** を選択し、**IKE** で **手動** を選択し、かつ、**動作セキュリティ** セクションの **ハッシュ** で **なし** 以外の設定を選択した場合は、In と Out の設定が必要です。

メモ

動作セキュリティ セクションの **ハッシュ** で選択した項目によって、設定できる文字数が異なります。

指定した認証キーの長さが、選択したハッシュアルゴリズムの長さと一致していない場合、エラーとなります。

- **MD5**: 128 ビット（16 バイト）
- **SHA1**: 160 ビット（20 バイト）
- **SHA256**: 256 ビット（32 バイト）
- **SHA384**: 384 ビット（48 バイト）
- **SHA512**: 512 ビット（64 バイト）

キーをアスキーコードで指定する場合は、文字を二重引用符（"）で囲みます。

コードキー（ESP）

暗号化に使用するキーを指定します。**In/Out** 値を入力します。

テンプレートを使用する で **カスタム** を選択し、**IKE** で **手動** を選択し、かつ、**動作セキュリティ** の **プロトコル** で **ESP** を選択した場合は、In と Out の設定が必要です。

メモ

動作セキュリティ セクションの **暗号化方式** で選択した項目によって、設定できる文字数が異なります。

指定したコードキーの長さが、選択した暗号化アルゴリズムの長さと一致していない場合、エラーとなります。

- **DES**: 64 ビット（8 バイト）
- **3DES**: 192 ビット（24 バイト）
- **AES-CBC 128**: 128 ビット（16 バイト）
- **AES-CBC 256**: 256 ビット（32 バイト）

キーをアスキーコードで指定する場合は、文字を二重引用符（"）で囲みます。

SPI

セキュリティ情報を識別するためのパラメーターです。一般に、ホストには、いくつかのタイプの IPsec 通信に対応するため複数の SA（Security Association）が備わっています。したがって、IPsec パケットを受信したときに、該当する SA を識別する必要があります。SPI パラメーター（SA を識別する）は、AH（認証ヘッダー）と ESP（Encapsulated Security Payload、暗号ペイロード）ヘッダーに含まれます。

テンプレートを使用する で **カスタム** を選択し、**IKE** で **手動** を選択した場合は、この設定が必要です。

In/Out 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。

メモ

- ESP は、IPsec を利用して暗号化通信を行うためのプロトコルの 1 つです。.ESP は、ペイロード（通信内容）を暗号化し、付加情報を追加します。IP パケットは、ヘッダーと、ヘッダーの後の暗号化されたペイロードから成ります。暗号化されたデータに加え、暗号化方式、暗号キー、認証データなどに関する情報も IP パケットに含まれます。
- AH は、IPsec プロトコルの仕様の一部で、送信元の認証やデータの改ざん防止（完全性の保証）を実現するための仕組みです。このデータは、IP パケット内のヘッダーの直後に挿入されます。また、パケットには、通信内容や秘密キーなどから一定の数式により計算されたハッシュ値も含まれ、これにより送信元の成りすましや通信内容の改ざんを防止します。ESP とは異なり、通信内容は暗号化されず、データは平文で送受信されます。

■ **暗号化方式**

DES、**3DES**、**AES-CBC 128**、または **AES-CBC 256** を選択します。暗号化方式は、**プロトコル** で **ESP** を選択し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** を選択し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。

時間（秒）と量（KB）を入力してください。

■ **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。**トンネル** モードを選択している場合にのみ、この情報を入力してください。

メモ

SA（Security Association）は、IPsec や IPv6 を利用する暗号化通信方式の 1 つで、暗号化方式や暗号キーなどの情報を交換共有し、安全な通信路を確立してから、通信を開始します。SA は、すでに確立された仮想的な暗号通信路（トンネル）のことを指す場合もあります。IPsec による通信で利用される SA は、暗号化方式を確立し、暗号キーを交換し、IKE の標準手続に従って相互認証を行います。さらに SA は、定期的に更新されます。

OK

このボタンをクリックして、設定を登録します。

メモ

使用中のテンプレートの設定を変更した場合は、ウェブブラウザーの IPsec 設定画面が再起動します。

外部機器によるスキャン機能の利用を制限する

外部機器によるスキャン機能の利用を制限できます。

外部機器によるスキャン機能の利用を制限すると、外部機器からは本製品のスキャン機能を利用できず、その外部機器にエラーメッセージが表示されます。

ウェブブラウザーを使用して外部機器によるスキャン機能の利用を制限する

1. ウェブブラウザーを起動します。
2. ブラウザーのアドレスバーに、本製品の IP アドレスを入力します。例：http://192.168.1.2。
3. お買い上げ時の設定では、パスワードは必要ありません。パスワードを設定してある場合はパスワードを入力し、→ を押します。
4. **スキャン** タブをクリックします。
5. 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。
6. **PC からのスキャン** を選択して「無効」にします。
7. **OK** をクリックします。

セキュリティ機能ロック 3.0

セキュリティ機能ロックを利用すると、本製品の次の動作モードへの共有アクセスを制限できます。

- スキャン to PC
- スキャン to FTP/SFTP
- スキャン to ネットワークファイル
- スキャン to USB
- クラウドスキャン
- スキャン to E メール
- スキャン to SharePoint
- スキャン to WSS（Web サービススキャン）
- お役立ちツール

セキュリティ機能ロックを利用すると、本製品の設定へのアクセスを制限して、既定の設定が変更されるのを防止できます。

セキュリティ機能を使用する場合は、まず管理者パスワードの入力が必要です。

管理者は、ユーザーのパスワードと併せて、個別ユーザーに対する機能制限を設定できます。

管理者のパスワードを書き留めてください。管理者のパスワードを忘れた場合、本製品に保存されているパスワードのリセットが必要になります。パスワードのリセット方法については、ブラザーコールセンター（お客様相談窓口）までお問い合わせください。

メモ

- セキュリティ機能ロックは、ウェブブラウザー、または BRAdmin Professional 3（Windows® のみ）を使用して設定できます。
- ユーザーごとの制限の設定や変更を行えるのは、管理者だけです。
- （ADS-3600W の場合）
  別のユーザーに切り替えて、スキャン機能（スキャン to PC、スキャン to FTP、スキャン to ネットワークファイルなど）にアクセスする際には、カード認証を使用できます。

セキュリティ機能ロック 3.0 を使用する前に

ウェブブラウザーを使用して、セキュリティ機能ロックを設定できます。最初に、次の手順を行います。

1. ウェブブラウザーを起動します。
2. ブラウザーのアドレスバーに、本製品の IP アドレスを入力します。例：http://192.168.1.2。
3. **ログイン** ボックスに管理者パスワードを入力します。（これは、本製品のウェブページにログオンするためのパスワードです。）→ をクリックします。

セキュリティ機能ロックのオンとオフを切り替える

1. **管理者設定** をクリックします。
2. **制限機能** をクリックします。
3. **セキュリティ機能ロック** または **オフ** を選択します。
4. **OK** をクリックします。

ウェブブラウザーを使用してセキュリティ機能ロック 3.0 を設定する

機能制限のあるグループと、パスワードとカード ID（NFC ID）[1] を持つユーザーを設定します。機能制限ありのグループ、およびユーザーを、それぞれ最大 100 ずつ設定できます。この設定には、ウェブブラウザーを使用します。ウェブページで設定を行うには、*セキュリティ機能ロック 3.0 を使用する前に*（85 ページ）の手順の後、次の手順を行います。

[1] ADS-3600W の場合

1. **管理者設定** をクリックします。
2. **制限機能** をクリックします。
3. **セキュリティ機能ロック** を選択します。
4. **OK** をクリックします。
5. **ユーザーリスト xx-xx** をクリックします。
6. **ユーザーリスト** フィールドに、最大 20 文字でユーザー名を入力します。
7. **パスワード** ボックスに、4 桁のパスワードを入力します。
8. （ADS-3600W の場合）
   カード ID ボックスに、カード番号を入力します（最大 16 文字）。[1]

   [1] 0 ～ 9 の数字と、A ～ F の文字（大文字小文字は区別されません）を使用できます。
9. 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。
10. **OK** をクリックします。

ファームウェアの更新

ブラザーのウェブサイトにアクセスして、最新のファームウェアに更新することができます。

メモ

インターネット接続にプロキシサーバーを使用している場合は、プロキシの詳細設定を入力する必要があります。

1. ウェブブラウザーを起動します。
2. ブラウザーのアドレスバーに、本製品の IP アドレスを入力します。例：http://192.168.1.2。
3. お買い上げ時の設定では、パスワードは必要ありません。パスワードを設定してある場合はパスワードを入力し、→ を押します。
4. **管理者設定** タブをクリックします。
5. ナビゲーションバーの **ファームウェア更新** メニューをクリックします。
6. **最新ファームウェアの確認** をクリックします。

7 困ったときは

概要

この章では、本製品の使用中に発生するネットワーク問題の対処方法を説明します。

他の取扱説明書をダウンロードするには、サポートサイト（ブラザーソリューションセンター（solutions.brother.com/manuals））で、お使いの製品のページからダウンロードしてください。

問題を特定する

この章を読む前に、以下のことを確認してください。

はじめに、次のことを確認してください。

AC アダプターが正しく接続され、本製品の電源がオンになっている。
アクセスポイント（無線 LAN）、ルーターまたはハブの電源が入っていて、リンクボタンが点滅している。
すべての保護用梱包材が本製品から取り除かれている。
フロントカバー、分離片カバー、および分離ローラーカバーが完全に閉じられている。

該当する解決方法のページをご覧ください。

- *無線 LAN のセットアップができない。*（89 ページ）。
- *無線 LAN エラーコード*（90 ページ）。
- *製品付属ソフトウェアのインストール時に、ネットワーク上に本製品が見つからない。*（93 ページ）。
- *本製品がネットワーク経由でスキャンできない。インストールが正しく完了しても、本製品がネットワーク上に見つからない。*（94 ページ）。
- *セキュリティソフトウェアを使用している。*（96 ページ）。
- *ネットワーク機器が正常に稼動しているか確認する。*（97 ページ）。

無線 LAN のセットアップができない。

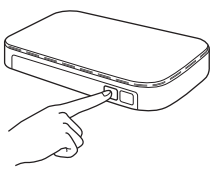
問題	インターフェイス	対処
無線 LAN のセットアップ中にネットワーク接続に失敗しましたか？	無線 LAN	お使いの無線 LAN ルーターの電源を切って、電源を入れ直してください。その後で、再度、無線 LAN の設定を行ってください。
セキュリティの設定（SSID/ ネットワークキー）は正しいですか？	無線 LAN	セキュリティの設定を確認してください。 ■ セキュリティの初期設定に、無線 LAN のアクセスポイント / ルーターの製造元の名前やモデル番号が使用されている可能性があります。 ■ セキュリティ設定については、お使いの無線 LAN アクセスポイント / ルーターに付属の取扱説明書をご覧ください。 ■ お使いの無線 LAN 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お問い合わせください。
MAC アドレスのフィルタリングを使用していますか？	無線 LAN	フィルタリングで、本製品の MAC アドレスが許可されていることを確認します。 MAC アドレスは、本製品の操作パネルを使って確認できます。
無線 LAN のアクセスポイント / ルーターは、ステルスモード （SSID を表示させない設定）ですか？	無線 LAN	■ 正しい SSID 名を手動で入力してください。 ■ お使いの無線 LAN アクセスポイント/ルーターに付属の取扱説明書に記載されている SSID 名やネットワークキーを確認し、無線 LAN を再セットアップしてください。（詳しくは、*SSID が隠蔽されていて表示されない場合*（11 ページ）をご覧ください。）
上記をすべて確認しましたが、無線 LAN の設定ができません。なにか他にできることがありますか？	無線 LAN	ネットワーク接続修復ツールを使用してください。*本製品がネットワーク経由でスキャンできない。インストールが正しく完了しても、本製品がネットワーク上に見つからない。*（94 ページ）をご覧ください。
セキュリティの設定（SSID/ パスワード）は正しいですか？	Wi-Fi Direct®	SSID とパスワードを確認します。 ネットワークを手動で設定する際、本製品の操作パネルに SSID とパスワードが表示されます。お使いの携帯端末が手動設定に対応している場合は、お使いの携帯端末の画面に SSID とパスワードが表示されます。
Android™ 4.0 を使用していますか？	Wi-Fi Direct®	携帯端末との接続が切れる場合（Wi-Fi Direct® を約 6 分使用した後）は、WPS によるワンプッシュ方式を使用して（推奨）、本製品を G/O に設定してみてください。
本製品と携帯端末が離れすぎていませんか？	Wi-Fi Direct®	Wi-Fi Direct® のネットワーク設定を行うときは、本製品と携帯端末を 1 メートル程度まで近づけてください。
本製品と携帯端末の間に、障害物（壁や家具など）がありませんかか？	Wi-Fi Direct®	本製品を障害物のない場所へ移動してください。
本製品または携帯端末の近くに、無線 LAN パソコン、Bluetooth 対応機器、電子レンジ、デジタルコードレス電話がありませんか？	Wi-Fi Direct®	これらすべての機器を、本製品と携帯端末から離してください。

問題	インターフェイス	対処
上記をすべて確認しましたが、Wi-Fi Direct® の設定ができません。なにか他にできることがありますか？	Wi-Fi Direct®	■ 本製品の電源を切って、電源を入れ直してください。その後で、再度、Wi-Fi Direct® の設定を行ってください。 ■ 本製品をクライアントとして使用している場合は、現在の Wi-Fi Direct® ネットワークで接続可能な機器の台数を調べ、何台接続されているか確認してください。

無線 LAN エラーコード

本製品の液晶画面にエラーコードが表示された場合は、次の表を参照して対処してください。

エラーコード	推奨される対処方法
TS-01	無線 LAN の設定が有効になっていません。 次の手順で、無線 LAN の設定をオンにしてください。 1 本製品の液晶画面で、 > [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] を押して無線 LAN セットアップウィザードを起動します。
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 次の点を確認してください。 ■ 無線 LAN アクセスポイント/ルーターの電源が入っていることを確認してください。 ■ 本製品を障害物のない場所へ移動させたり、無線 LAN アクセスポイント / ルーターに近づけたりしてください。 ■ 無線 LAN の設定を行う際は、本製品を一時的に無線 LAN アクセスポイント / ルーターから約 1 メートル以内に置いてください。 ■ 無線 LAN アクセスポイント / ルーターで MAC アドレスのフィルタリングが行われている場合は、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。 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は、入力した情報が間違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、必要に応じて正しい情報を入力し直してください。 本機器は 5 GHz SSID/ESSID に対応していません。必ず 2.4 GHz SSID/ESSID を選択してください。無線 LAN アクセスポイント / ルーターが、2.4 GHz または 2.4 GHz/5 GHz ミックスモードに設定されていることを確認してください。
TS-03	入力した無線 LAN とセキュリティの設定が間違っている可能性があります。 無線 LAN の設定を確認してください。 入力または選択した SSID/ 認証方式 / 暗号化方式 / ユーザー ID/ パスワードが正しいことを確認してください。

<table>
<tr><th>エラーコード</th><th>推奨される対処方法</th></tr>
<tr><td>TS-04</td><td>選択した無線 LAN アクセスポイント / ルーターで使用されている認証方式 / 暗号化方式に本製品が対応していません。
インフラストラクチャモードの場合は、無線 LAN アクセスポイント / ルーターの認証方式 / 暗号化方式を変更してください。本製品は、次の認証方式に対応しています。
<table>
<tr><th>認証方式</th><th>暗号化方式</th></tr>
<tr><td rowspan="2">WPA- パーソナル</td><td>TKIP</td></tr>
<tr><td>AES</td></tr>
<tr><td>WPA2- パーソナル</td><td>AES</td></tr>
<tr><td rowspan="2">オープン</td><td>WEP</td></tr>
<tr><td>なし（暗号化なし）</td></tr>
<tr><td>共有キー</td><td>WEP</td></tr>
</table>
問題が解決されない場合は、入力した SSID やネットワーク設定が間違っている可能性があります。無線 LAN の設定を確認してください。
アドホックモードの場合は、お使いのパソコンの無線 LAN の設定で、認証方式 / 暗号化方式を変更してください。本製品が対応している認証方式は、WEP 暗号化方式を使用できるオープンシステム認証のみです。</td></tr>
<tr><td>TS-05</td><td>セキュリティ情報（SSID/ ネットワークキー）が間違っています。
SSID とセキュリティ情報（ネットワークキー）を確認してください。
ご使用のルーターで WEP 暗号化方式を使用している場合は、1 番目の WEP キーとして使用されるキーを入力します。本製品では、1 番目の WEP キーのみ使用できます。</td></tr>
<tr><td>TS-06</td><td>無線 LAN のセキュリティ情報（認証方式 / 暗号化方式 / ネットワークキー）が間違っています。
エラーコード TS-04 の認証方式の表で、無線 LAN のセキュリティ情報（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。
ご使用のルーターで WEP 暗号化方式を使用している場合は、1 番目の WEP キーとして使用されるキーを入力します。本製品では、1 番目の WEP キーのみ使用できます。</td></tr>
<tr><td>TS-07</td><td>WPS が有効になっている無線 LAN アクセスポイント / ルーターは、本製品では検出できません。
WPS を使用して無線 LAN の設定を行う場合は、本製品と無線 LAN アクセスポイント / ルーターの両方の操作が必要です。
お使いの無線 LAN アクセスポイント / ルーターで WPS を利用する場合の操作方法については、無線 LAN アクセスポイント / ルーターの取扱説明書をご覧いただくか、無線 LAN アクセスポイント / ルーターの製造元またはネットワーク管理者にお問い合わせください。
  </td></tr>
</table>

エラーコード	推奨される対処方法
TS-08	WPS が有効になっている無線 LAN アクセスポイントが 2 台以上検出されています。 WPS 方式が有効になっている無線 LAN アクセスポイント / ルーターが、電波が届く範囲に 1 台しかないことを確認して、再度設定を行ってください。
TS-20	本製品はまだ無線 LAN への接続を試行しています。少し時間をおいて、無線 LAN の接続状態を確認してください。

製品付属ソフトウェアのインストール時に、ネットワーク上に本製品が見つからない。

質問	インターフェイス	対処
パソコンはネットワークに接続されていますか？	有線 LAN/無線 LAN	使いのパソコンがネットワーク（LAN 環境やインターネットサービスなど）に接続されていることを確認してください。詳しくは、ネットワーク管理者にお問い合わせください。
本製品は、ネットワークに接続されていて、有効な IP アドレスが割り当てられていますか？	有線 LAN/無線 LAN	（有線 LAN） ［有線 LAN 状態］の［接続状態］がアクティブ XXXX-XX であることを確認してください。（XXXX-XX は、選択したイーサネットインターフェイスです。）*ネットワーク接続状態を確認する方法*（3 ページ）をご覧ください。液晶画面に［未接続］または［有線 LAN オフ］と表示された場合は、ネットワーク管理者に連絡して IP アドレスが有効かどうかを確認してください。 （無線ネットワーク） ［無線状態］の［接続状態］が［接続に失敗しました］でないことを確認してください。*無線 LAN の接続状態を確認する*（9 ページ）をご覧ください。 液晶画面に［接続に失敗しました］と表示された場合は、ネットワーク管理者に連絡して IP アドレスが有効かどうかを確認してください。
セキュリティソフトウェアを使用していますか？	有線 LAN/無線 LAN	■ インストーラーのダイアログボックスで、本製品を再び検索してください。 ■ 製品付属ソフトウェアのインストール中にセキュリティソフトウェアの警告メッセージが表示された場合は、アクセスを許可してください。 ■ セキュリティソフトウェアについて詳しくは、*セキュリティソフトウェアを使用している。*（96 ページ）をご覧ください。
Wi-Fi ルーターを使用していますか？	無線 LAN	Wi-Fi ルーターでプライバシーセパレーターが有効になっている可能性があります。プライバシーセパレーターを無効にしてください。
無線 LAN アクセスポイント / ルーターと本製品が離れすぎていませんか？	無線 LAN	無線 LAN の設定時は、本製品と無線 LAN アクセスポイント / ルーターを 1 メートル程度まで近づけてください。
本製品と無線 LAN アクセスポイント / ルーターの間に、障害物（壁や家具など）がありませんかか？	無線 LAN	本製品を障害物のない場所へ移動させたり、無線 LAN アクセスポイント / ルーターに近づけたりしてください。
本製品または無線 LAN アクセスポイント / ルーターの近くに、無線 LAN パソコン、Bluetooth 対応機器、電子レンジ、デジタルコードレス電話がありませんか？	無線 LAN	これらすべての機器を、本製品または無線 LAN アクセスポイント / ルーターから離してください。

本製品がネットワーク経由でスキャンできない。
インストールが正しく完了しても、本製品がネットワーク上に見つからない。

質問	インターフェイス	対処
セキュリティソフトウェアを使用していますか？	有線 LAN/無線 LAN	*セキュリティソフトウェアを使用している。*（96 ページ）をご覧ください。
利用可能な IP アドレスが本製品に割り当てられていますか？	有線 LAN/無線 LAN	■ IP アドレスとサブネットマスクを確認してください。 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正しいことと、両者が同じネットワーク上にあることを確認してください。IP アドレスとサブネットマスクを確認する方法について詳しくは、ネットワーク管理者にお問い合わせください。 ■（Windows®） ネットワーク接続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てください。 本製品のネットワーク設定を修正する場合は、ネットワーク接続修復ツールを使用してください（正しい IP アドレスとサブネットマスクが割り当てられます）。 ネットワーク接続修復ツールを使用するには、ネットワーク管理者に必要な情報を問い合わせ、次の手順に従います。 **メモ** • （Windows® XP） 管理者権限でログオンする必要があります。 • 本製品の電源がオンになっており、パソコンと同じネットワークに接続されていることを確認してください。

質問	インターフェイス	対処
利用可能な IP アドレスが本製品に割り当てられていますか？ （続き）	有線 LAN/無線 LAN	1 付属の DVD-ROM ディスクを DVD-ROM ドライブにセットします。DVD-ROM のトップメニューが表示された場合は、メニューを閉じてください。 2 オペレーティングシステムのコンピューターディレクトリを開きます。 ■ Windows® XP **スタート** > **すべてのプログラム** > **アクセサリ** > **エクスプローラ** > **マイ コンピュータ** の順にクリックします。 ■ Windows Vista®/Windows® 7 （**スタート**）> **コンピューター** をクリックします。 ■ Windows® 8/Windows® 8.1 タスク バーの（**エクスプローラー**）アイコンをクリックし、**コンピューター** に進みます。 ■ 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、**コンピューター** に進みます。 3 **DVD ドライブ** をダブルクリックし、**ツール** をダブルクリックし、**NetTool** をダブルクリックし、**BrotherNetTool.exe** をダブルクリックしてプログラムを起動します。 **メモ** **ユーザーアカウント制御** 画面が表示されたら、 （Windows Vista®）**続行（許可）** をクリックします。 （Windows® 7/Windows® 8/Windows® 8.1/Windows® 10）**はい** をクリックします。 4 画面上の指示に従います。 ネットワーク接続修復ツールを使用しても正しい IP アドレスとサブネットマスクが割り当てられない場合は、ネットワーク管理者にこれらの設定値をお問い合わせください。
無線 LAN 機能を使用して本製品をネットワークに接続していますか？	無線 LAN	■ ［無線状態］で［接続状態］を確認してください。*無線 LAN の接続状態を確認する*（9 ページ）をご覧ください。液晶画面に［接続に失敗しました］と表示された場合は、ネットワーク管理者に連絡して IP アドレスが有効かどうかを確認してください。 ■ *製品付属ソフトウェアのインストール時に、ネットワーク上に本製品が見つからない。*（93 ページ）をご覧ください。
上記をすべて確認しましたが、本製品でスキャンできません。なにか他にできることがありますか？	有線 LAN/無線 LAN	製品付属ソフトウェアをアンインストールしてから、再インストールしてください。

セキュリティソフトウェアを使用している。

質問	インターフェイス	対処
製品付属ソフトウェアのインストール時、アプリケーションの起動時、スキャン機能の使用時に、セキュリティ警告のダイアログボックスで **許可** を選択しましたか？	有線 LAN/ 無線 LAN	セキュリティ警告のダイアログボックスで **許可** を選択しなかった場合は、ご利用のセキュリティソフトウェアのファイアウォール機能によってアクセスが拒否されている可能性があります。一部のセキュリティソフトウェアは、セキュリティ警告のダイアログボックスを表示しないでアクセスをブロックする場合があります。アクセスを許可するには、お使いのセキュリティソフトウェアに付属の取扱説明書を参照するか、セキュリティソフトウェアの提供元にお問い合わせください。
セキュリティソフトウェアの設定に必要なポート番号を知りたい。	有線 LAN/ 無線 LAN	ブラザーのネットワーク機能では、次のポート番号が使用されています。 ■ ネットワークスキャン → ポート番号 54925/ プロトコル UDP ■ ネットワークスキャン、リモートセットアップ [1] → ポート番号 161 および 137/ プロトコル UDP ■ BRAdmin Light [1] → ポート番号 161/ プロトコル UDP [1] Windows® のみ。 ポートを開く方法については、お使いのセキュリティソフトウェアに付属の取扱説明書を参照するか、セキュリティソフトウェアの提供元にお問い合わせください。

ネットワーク機器が正常に稼動しているか確認する。

質問	インターフェイス	対処
本製品、無線 LAN 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ますか？	有線 LAN/ 無線 LAN	*はじめに、次のことを確認してください。*（88 ページ）に記載されているすべての項目を確認してください。
本製品のネットワーク設定（IP アドレスなど）はどこで確認することができますか？	有線 LAN/ 無線 LAN	■ ウェブブラウザーを使用する場合 1 ウェブブラウザーを起動し、本製品にアクセスします（39 ページの ❶ を参照）。 2 本製品の管理画面が表示されたら、**ネットワーク** タブをクリックし、左側にあるナビゲーションバーの **ネットワークの状態** をクリックします。 ■ 操作パネルを使用する場合 本製品の操作パネルで、［ ネットワーク ］の設定を確認します。
本製品の接続状態はどのように確認できますか？	有線 LAN/ 無線 LAN	■ ウェブブラウザーを使用する場合 1 ウェブブラウザーを起動し、本製品にアクセスします（39 ページの ❶ を参照）。 2 本製品の管理画面が表示されたら、**ネットワーク** タブをクリックし、左側にあるナビゲーションバーの **ネットワークの状態** をクリックします。 ■ 操作パネルを使用する場合 （有線 LAN） ［ 有線 LAN 状態 ］の［ 接続状態 ］が アクティブ XXXX-XX であることを確認してください（XXXX-XX は、選択したイーサネットインターフェイスです）。 ネットワークの接続状態を確認するには、 > ［ ネットワーク ］ > ［ 有線 LAN］ > ［ 有線 LAN 状態 ］ > ［ 接続状態 ］の順に押します。 液晶画面に［ 未接続 ］または［ 有線 LAN オフ ］と表示された場合は、ネットワーク管理者に連絡して IP アドレスが有効かどうかを確認してください。 （無線ネットワーク） ［ 無線状態 ］の［ 接続状態 ］が［ 接続に失敗しました ］でないことを確認してください。*無線 LAN の接続状態を確認する*（9 ページ）をご覧ください。液晶画面に［ 接続に失敗しました ］と表示された場合は、ネットワーク管理者に連絡して IP アドレスが有効かどうかを確認してください。

質問	インターフェイス	対処
パソコンから本製品に「ping」を実行できますか？	有線 LAN/無線 LAN	Windows® のコマンドプロンプトで次のように IP アドレス、またはノード名を入力して、パソコンから本製品に対して ping を実行します。 ping <IP アドレス > または < ノード名 > ■ 成功 > 本製品は正しく動作していて、お使いのパソコンと同じ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じ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て、ネットワーク接続修復ツールで自動的に IP アドレスとサブネットマスクを修正してください。ネットワーク接続修復ツールの詳細については、*本製品がネットワーク経由でスキャンできない。インストールが正しく完了しても、本製品がネットワーク上に見つからない。*（94 ページ）の「*利用可能な IP アドレスが本製品に割り当てられていますか？*」をご覧ください。 （Macintosh） 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てください。*本製品がネットワーク経由でスキャンできない。インストールが正しく完了しても、本製品がネットワーク上に見つからない。*（94 ページ）の「*IP アドレスとサブネットマスクを確認してください*」をご覧ください。
本製品は無線 LAN に接続していますか？	無線 LAN	［無線状態］で［接続状態］を確認してください。*無線 LAN の接続状態を確認する*（9 ページ）をご覧ください。液晶画面に［接続に失敗しました］と表示された場合は、ネットワーク管理者に連絡して IP アドレスが有効かどうかを確認してください。
上記をすべて確認しましたが、問題は解決していません。なにか他にできることがありますか？	無線 LAN	お使いの無線 LAN アクセスポイント / ルーターに付属の取扱説明書で SSID とネットワークキーの情報を確認し、正しく設定してください。SSID とネットワークキーについて詳しくは、*無線 LAN のセットアップができない。*（89 ページ）の「*セキュリティの設定（SSID/ ネットワークキー）は正しいですか？*」をご覧ください。

8 その他のネットワーク設定方法（Windows®）

設定方法の種類

次のネットワーク接続機能もオプションとして使用できます。

- スキャン用 Web サービス（Windows Vista®、Windows® 7、Windows® 8、Windows® 8.1、および Windows® 10）
- Vertical Pairing（Windows® 7、Windows® 8、Windows® 8.1、および Windows® 10）

メモ

ホストコンピューターと本製品が同じサブネット上にあること、または両者の間でデータのやり取り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てください。

Web サービススキャンで使用するドライバーをインストールする（Windows Vista®、Windows® 7、Windows® 8、Windows® 8.1、Windows® 10）

Web サービスを利用して、ネットワーク上で本製品の状態を確認することができます。また Web サービスの機能で、ドライバーのインストールが簡単になります。Web サービススキャンで使用するドライバーは、パソコン上のスキャナーのアイコンを右クリックしてインストールできます。パソコンの Web サービス用のポート（WSD ポート）が自動的に作成されます。（Web サービスを利用したスキャンについて詳しくは、『*ユーザーズガイド*』の「*Web Services を使ってスキャンする（Windows Vista® SP2 以降、Windows® 7、Windows® 8、Windows® 8.1、および Windows® 10）*」をご覧ください。）

メモ

この設定を行う前に、本製品の IP アドレスを設定してください。

1. オペレーティングシステムのネットワーク設定を開きます。
   - Windows Vista®

     （**スタート**）> **ネットワーク** をクリックします。
   - 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** の順にクリックします。
   - Windows® 8/Windows® 8.1

     マウスをデスクトップ右下に移動します。メニューバーが表示されたら、**設定** > **PC 設定の変更** > **デバイス** > **デバイスの追加** をクリックします。
   - Windows® 10

     （**スタート**）> **設定** > **デバイス** > **プリンターとスキャナー** の順にクリックします。

2 本製品の Web サービス名がスキャナーのアイコンと一緒に表示されます。

■ Windows Vista®/ Windows® 7/Windows® 8/ Windows® 8.1

インストールする製品を右クリックします。

■ Windows® 10

インストールする製品をクリックします。

メモ

本製品の Web サービス名は、お使いの製品のモデル名と MAC アドレス（イーサネットアドレス）です（例：Brother ADS-XXXXX（モデル名）[XXXXXXXXXXXX]（MAC アドレス / イーサネットアドレス））。

3 本製品用のインストールを開始します。

■ Windows Vista®/Windows® 7

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/Windows® 8.1

インストールする製品を選択します。

■ Windows® 10

デバイスの追加 をクリックします。

Vertical Pairing を使用したインフラストラクチャモードのネットワークスキャン用のインストール（Windows® 7、Windows® 8、Windows® 8.1、および Windows® 10）

Windows® Vertical Pairing によって、Vertical Pairing に対応している無線機器を、WPS の PIN 方式と Web サービス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ことができます。また、**デバイスの追加** 画面のスキャナーのアイコンからスキャナードライバーをインストールすることができます。

インフラストラクチャモードの場合は、無線 LAN に本製品を接続し、この機能を使用してスキャナードライバーをインストールできます。以下の手順に従ってください。

メモ

- 本製品の Web サービス機能をオフにしている場合は、オンに戻す必要があります。お買い上げ時は、本製品の Web サービス機能の設定はオンになっています。ウェブブラウザーまたは BRAdmin Professional 3 で、Web サービスの設定を変更することができます。
- お使いの無線 LAN アクセスポイント / ルーターに、Windows® 7、Windows® 8、Windows® 8.1、または Windows® 10 に対応していることを示すロゴが付いていることを確認してください。不明な場合は、無線 LAN アクセスポイント / ルーターの製造元にお問い合わせください。
- お使いのパソコンに、Windows® 7、Windows® 8、Windows® 8.1、または Windows® 10 に対応していることを示すロゴが付いていることを確認してください。不明な場合は、パソコンの製造元にお問い合わせください。
- 別売りの無線 LAN カードを使用して無線 LAN に接続する場合は、Windows® 7、Windows® 8、Windows® 8.1、または Windows® 10 に対応していることを示すロゴが付いていることを確認してください。詳しくは、お使いの無線 LAN カードの製造元にお問い合わせください。
- Windows® 7、Windows® 8、Windows® 8.1、または Windows® 10 コンピューターをレジストラとして使用するには、あらかじめコンピューターをネットワークに登録する必要があります。お使いの無線 LAN アクセスポイント / ルーターに付属の取扱説明書をご覧ください。

1. 本製品の電源を入れます。
2. 本製品を WPS モードに設定します（*WPS（Wi-Fi Protected Setup™）の PIN 方式を使用する*（19 ページ）をご覧ください）。
3. オペレーティングシステムの [デバイスの追加] メニューを開きます。
   - Windows® 7

     （**スタート**）> **デバイスとプリンター** > **デバイスの追加** の順にクリックします。
   - Windows® 8/Windows® 8.1

     マウスをデスクトップ右下に移動します。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

     （**スタート**）> **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** の順にクリックします。
4. 本製品を選び、本製品の画面に表示された PIN コードを入力します。
5. 接続先のインフラストラクチャーネットワークを選択し、**次へ** をクリックします。
6. **デバイスとプリンター** ダイアログボックスに本製品が表示されていれば、無線 LAN の設定とスキャナードライバーのインストールが正常に完了しています。

A 付録

対応プロトコルおよびセキュリティ機能

インターフェイス	イーサネット	10BASE-T、100BASE-TX
	無線 LAN	IEEE 802.11b/g/n（インフラストラクチャモード / アドホックモード） IEEE 802.11g/n（Wi-Fi Direct®）
ネットワーク（共通）	プロトコル（IPv4）	ARP、RARP、BOOTP、DHCP、APIPA（Auto IP）、WINS/NetBIOS 名前解決、DNS リゾルバ、mDNS、LLMNR レスポンダー、カスタム Raw ポート / ポート 9100、SMTP クライアント、FTP クライアント / サーバー、LDAP クライアント、CIFS クライアント、WebDAV クライアント、SNMPv1/v2c/v3 (MD5/SHA1)、HTTP/HTTPS サーバー、TFTP クライアント / サーバー、ICMP、Web サービス（スキャン）、SNTP クライアント
	プロトコル（IPv6）	NDP、RA、DNS リゾルバ、mDNS、LLMNR レスポンダー、カスタム Raw ポート / ポート 9100、SMTP クライアント、FTP クライアント / サーバー、LDAP クライアント、CIFS クライアント、TELNET サーバー、SNMPv1/v2c/v3、HTTP/HTTPS サーバー、TFTP クライアント / サーバー、ICMPv6、Web サービス（スキャン）、SNTP クライアント、WebDav クライアント
ネットワーク（セキュリティ）	有線 LAN	SMTP-AUTH、SSL/TLS (HTTPS、SMTP)、SSH、SNMP v3、802.1x (EAP-MD5、EAP-FAST、PEAP、EAP-TLS、EAP-TTLS)、Kerberos、IPsec
	無線 LAN	SMTP-AUTH、SSL/TLS (HTTPS、SMTP)、SSH、SNMP v3、802.1x (LEAP、EAP-FAST、PEAP、EAP-TLS、EAP-TTLS)、Kerberos、IPsec
E メール（セキュリティ）	有線 LAN および無線 LAN	SMTP-AUTH、SSL/TLS（SMTP）
ネットワーク（無線 LAN）	無線 LAN 認証	Wi-Fi Certification Mark License （WPA™/WPA2™ - Enterprise、Personal）、Wi-Fi Protected Setup™ (WPS) Identifier Mark License、Wi-Fi CERTIFIED Wi-Fi Direct®

ウェブブラウザーで設定できる機能一覧

メモ

ウェブブラウザーを使用した管理画面の右上の ? をクリックすると、各ページの概要が表示されます。

メインカテゴリ	サブカテゴリ	設定メニュー	設定オプション	詳細 / オプションの設定
基本設定	-	ステータス	デバイスの状態 / 自動 再読み込み / 言語 / デバイスの場所	機器の状態や連絡先、ロケーションを表示します。また、ウェブブラウザーを使用した管理画面の表示言語を変更できます。
	-	再読み込み間隔	再読み込み間隔	ウェブブラウザーの再読み込み間隔を設定できます（15 秒から 60 分）。
	-	メンテナンス情報	ノード情報 / 残り寿命 / 合計スキャンページ数 / 交換回数 / リセット回数 / エラー回数 / エラー履歴（最新 10 件）	本製品のモデル名、消耗品、ページカウンター、エラーなどのメンテナンス情報を表示します。 メンテナンス情報を CSV ファイルに変換するには、**OK** ボタンを押します。
	-	デバイスの検索	ノード名 / モデル名 / 装置の状態 / IP アドレス	ネットワークに繋がっているデバイスを表示します。
	-	連絡先とロケーション	連絡先 / ロケーション情報	ここで設定した連絡先とロケーションは、**基本設定** > **ステータス** > **デバイスの場所** に表示されます。
	-	スリープモード	スリープモード	90 分まで設定できます。
	-	自動電源オフ	自動電源オフ	
	-	音量	ボタン確認音量	**オフ** / **小** / **中** / **大** から設定します。
	-	パネル設定	画面の明るさ / 照明ダウンタイマー	
	-	定期メンテナンス	定期メンテナンス通知	

A

メインカテゴリ	サブカテゴリ	設定メニュー	設定オプション	詳細 / オプションの設定
アドレス帳	-	アドレス	アドレス / メールアドレス / 名前	名前とメールアドレスを 300 件まで登録できます。
	-	グループダイヤル	グループ / アドレス / 名前 / メンバー	グループを 20 件まで登録できます。グループメンバーを設定するには、**アドレス番号** を選択し **選択** をクリックします。
	-	LDAP	LDAP 検索 / 基本設定 / 詳細設定	LDAP 設定を行います。
	-	インポート	" アドレス帳 " データファイル / " グループダイヤル " データファイル	
	-	エクスポート		
E メール	-	メール送信設定	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 / SMTP	メールの件名、本文、サイズ制限、受信確認要求などのメール送信設定をします。**SMTP** をクリックすると **ネットワーク** > **ネットワーク** > **プロトコル** > **SMTP** > **詳細設定** に移行します。
スキャン	-	スキャン	重送検知 / 読み取り開始位置調整 / 表面 X / 表面 Y / 裏面 X / 裏面 Y / スキャン結果表示	
	-	スキャン通知 レポート	送信メールサーバー (SMTP) / 管理者メールアドレス / SMTP / スキャン to Eメール / スキャン to FTP / スキャン to SFTP / スキャン to ネットワークファイル / スキャン to SharePoint	
	-	スキャン ファイル名称	ファイル名項目順序 / 日付＆時刻 / カウンタ / スキャン to USB 1 ～ 5 / スキャン to E メール 1 ～ 10 / スキャン to FTP/SFTP 1 ～ 15 / スキャン to ネットワークファイル /SharePoint 1 ～ 15	
	-	スキャン to USB	ファイル名 / 画質 / カラー自動検出調整 / ファイル形式 / 原稿サイズ / エッジ調整 / ファイルサイズ / ADF 傾き補正 / 白紙除去 / 白紙除去レベル調整 / 両面読取 / 明るさ / コントラスト / 継続スキャン	スキャン to USB を設定します。

A

メインカテゴリ	サブカテゴリ	設定メニュー	設定オプション	詳細 / オプションの設定
スキャン（つづき）	-	スキャン to E メール	ファイル名 / 画質 / カラー自動検出調整 / カラー / モノクロ / グレー / ファイル形式 / 原稿サイズ / エッジ調整 / ファイルサイズ / ADF 傾き補正 / 白紙除去 / 白紙除去レベル調整 / 両面読取 / 明るさ / コントラスト / 継続スキャン / 自分宛に送信	スキャン to E メール送信を設定します。
	-	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 ～ 25 / 自分のフォルダに送信	スキャン to FTP/SFTP/ ネットワークファイル /SharePoint を設定します。
	-	FTP/SFTP/ ネットワークファイル / SharePoint スキャンプロファイル	プロファイル 1 ～ 25	プロファイルを設定します。
	-	プロファイル (FTP)	プロファイル名 / サーバー アドレス / ユーザー名 / パスワード / 転送先フォルダー / ファイル名 / 画質 / カラー自動検出調整 / ファイル形式 / 原稿サイズ / エッジ調整 / ファイルサイズ / ADF 傾き補正 / 白紙除去 / 白紙除去レベル調整 / 両面読取 / 明るさ / コントラスト / 継続スキャン / パッシブモード / ポート番号	プロファイルを設定します。 詳しくは、*スキャン to FTP の設定を変更する*（49 ページ）をご覧ください。
	-	プロファイル (SFTP)	プロファイル名 / サーバー アドレス / ユーザー名 / 認証方法 / クライアント鍵ペア / サーバー公開鍵 / 転送先フォルダー / ファイル名 / 画質 / カラー自動検出調整 / ファイル形式 / 原稿サイズ / エッジ調整 / ファイルサイズ / ADF 傾き補正 / 白紙除去 / 白紙除去レベル調整 / 両面読取 / 明るさ / コントラスト / 継続スキャン / ポート番号	プロファイルを設定します。 詳しくは、*スキャン to SFTP の設定を変更する*（51 ページ）をご覧ください。

A

メインカテゴリ	サブカテゴリ	設定メニュー	設定オプション	詳細 / オプションの設定
スキャン（つづき）	-	プロファイル (ネットワーク)	プロファイル名 / ネットワークフォルダパス / ファイル名 / 画質 / カラー自動検出調整 / ファイル形式 / 原稿サイズ / エッジ調整 / ファイルサイズ / ADF 傾き補正 / 白紙除去 / 白紙除去レベル調整 / 両面読取 / 明るさ / コントラスト / 継続スキャン / 接続時にパスワード認証を行う / 接続パスワード / 認証方法 / ユーザー名 / パスワード / 時計設定	プロファイルを設定します。 詳しくは、*スキャン to ネットワークの設定を変更する（Windows®）*（53 ページ）をご覧ください。
	-	プロファイル (SharePoint)	プロファイル名 / SharePoint サイトのアドレス / SSL/TLS / ファイル名 / 画質 / カラー自動検出調整 / ファイル形式 / 原稿サイズ / エッジ調整 / ファイルサイズ / ADF 傾き補正 / 白紙除去 / 白紙除去レベル調整 / 両面読取 / 明るさ / コントラスト / 継続スキャン / 接続時にパスワード認証を行う / 接続パスワード / 認証方法 / ユーザー名 / パスワード / 時計設定	プロファイルを設定します。 詳しくは、*スキャン to SharePoint の設定を変更する（Windows®）*（55 ページ）をご覧ください。
	-	PC からのスキャン	PC からのスキャン	

A

メインカテゴリ	サブカテゴリ	設定メニュー	設定オプション	詳細 / オプションの設定
管理者設定	-	ログインパスワード	パスワード	ウェブブラウザーを使用した管理画面へのログインパスワードを設定します。ログインしない場合は、**基本設定** タブの設定だけを変更できます。
	-	制限機能		
	-	セキュリティ機能ロック	クラウド / PC / ネットワーク / FTP/SFTP / E メール送信 / Share Point / Web サービス / USB メモリ	**セキュリティ機能ロック** を使用すると、ユーザーのアクセス許可にもとづいて、スキャン機能およびクラウド接続機能の使用を制限できます。 詳しくは、*セキュリティ機能ロック 3.0*（85 ページ）をご覧ください。
	-	Active Directory 認証	ユーザー ID を記憶 / Active Directory サーバアドレス / Active Directory ドメイン名 / ユーザーのホームディレクトリ取得 / プロトコルと認証方式 / メールアドレス取得 / LDAP ポート / LDAP 検索場所 / SNTP	**Active Directory 認証** を使用すると、本製品の使用を制限できます。 詳しくは、*Active Directory の LDAP 認証を設定する*（43 ページ）をご覧ください。
	-	LDAP 認証	ユーザーID を記憶 / LDAP アドレス / メールアドレス取得 / LDAP ポート / LDAP 検索場所 / 名前属性名 (検索する属性) / SNTP	**LDAP 認証** を使用すると、本製品の使用を制限できます。 詳しくは、*LDAP 設定の変更*（44 ページ）をご覧ください。
	-	セキュリティ設定ロック	セキュリティ設定ロック / パスワード	本製品の液晶画面にて設定を変更する際のパスワードを設定します。
	-	電子署名付 PDF	証明書の選択 / 証明書	電子署名付 PDF を使用するための、証明書の設定を行います。
	-	時計設定	日付 / 時計表示 / 時間 / タイムゾーン / サマータイム / SNTP サーバーと同期する / SNTP	
	-	リセットメニュー	機能設定リセット / ネットワーク設定リセット / アドレス帳 / 全設定リセット / 工場出荷リセット	
	-	ファームウェアの更新	モデル名 / シリアル番号 / ファームウェアバージョン / メイン / ファームウェア更新 / プロキシ	*ファームウェアの更新*（87 ページ）をご覧ください。

A

メインカテゴリ	サブカテゴリ	設定メニュー	設定オプション	詳細 / オプションの設定
ネットワーク	ネットワーク	ネットワークの状態	有線 / 無線	ネットワークの状態を表示します。
		インターフェース	インターフェース / Wi-Fi Direct	インターフェースを切り替えます。
		プロトコル	Web Based Management (Web Server) / Telnet / SNTP / リモートセットアップ / Raw ポート / Web Services / プロキシ / ネットワークスキャン / SMTP / FTP サーバー / FTP クライアント / SFTP / TFTP / WebDAV / CIFS / LDAP / mDNS / LLMNR / SNTP	本製品のプロトコル設定を行います。使用する各プロトコルのチェックボックスを選択します。
		エラー通達	送信メールサーバー（SMTP）/ デバイスの E メールアドレス / SMTP / 管理者メールアドレス	エラー通達の設定を行います。
		メンテナンス通達	送信メールサーバー（SMTP）/ メールアドレス / SMTP / 時計設定 / 管理者メールアドレス	
	有線	TCP/IP (有線)	Ethernet 10/100/1000 BASE-T / IP アドレス / サブネットマスク / ゲートウェイアドレス / IP 設定の方法 / 詳細設定 / インターフェース	TCP/IP（有線）の設定を行います。
		ノード名 (有線)	ノード名	
		NetBIOS (有線)	NETBIOS/IP / コンピューター名 / WINS サーバーアドレス設定の方法 / プライマリー WINS サーバーアドレス / セカンダリー WINS サーバーアドレス	
		IPv6 (有線)	IPv6 / 固定 IPv6 アドレス / プライマリー DNS サーバー IP / セカンダリー DNS サーバー IP / IPv6 アドレスリスト	
		イーサネット	イーサネットモード	
		有線 802.1x 認証	有線 802.1x / 認証方式 / 内部認証方式 / ユーザーID / パスワード / クライアント証明書 / サーバー証明書の検証 / サーバー ID / 証明書	
	無線	TCP/IP (無線)	IEEE 802.11b/g/n / IP アドレス / サブネットマスク / ゲートウェイアドレス / IP 設定の方法 / 詳細設定 / インターフェース	TCP/IP（無線）の設定を行います。
		ノード名 (無線)	ノード名	

A

メインカテゴリ	サブカテゴリ	設定メニュー	設定オプション	詳細 / オプションの設定
ネットワーク（つづき）	無線（つづき）	NetBIOS (無線)	NETBIOS/IP / コンピューター名 / WINS サーバーアドレス設定の方法 / プライマリー WINS サーバーアドレス / セカンダリー WINS サーバーアドレス	
		IPv6 (無線)	IPv6 / 固定 IPv6 アドレス / プライマリー DNS サーバー IP / セカンダリー DNS サーバー IP / IPv6 アドレスリスト	
		無線 (Setup Wizard)		Start Wizard をクリックすると、無線 LAN セットアップウィザードが開始されます。
		無線 (パーソナル)	ステータス / 接続モード / SSID（ネットワーク名）/ チャンネル / 認証方式 / 暗号化方式 / ネットワークキー	
		無線 (エンタープライズ)	ステータス / 接続モード / SSID（ネットワーク名）/ チャンネル / 認証方式 / 内部認証方式 / 暗号化方式 / ユーザー ID / パスワード / クライアント証明書 / サーバー証明書の検証 / サーバー ID / 証明書	
	セキュリティ	セキュリティ IPv4 フィルター	IP フィルターを使用する / 管理者 IP アドレス / アクセス設定	フィルタリングする IP アドレスを指定して、アクセス設定を行います。
		証明書	証明書一覧 / 自己署名証明書の作成 / CSRの作成 / 証明書のインストール / 証明書と秘密鍵のインポート	証明書の設定を行います。
		CA 証明書	CA 証明書一覧 / CA 証明書のインポート	CA 証明書の設定を行います。
		クライアント鍵ペア	クライアント鍵ペア一覧 / クライアント鍵ペアの作成	クライアント鍵ペアの設定を行います。
		サーバー公開鍵	サーバー公開鍵一覧 / サーバー公開鍵のインポート	サーバー公開鍵の設定を行います。
		IPsec	状態 / 接続モード / IPsec 以外のトラフィックルール / Broadcast/Multicast Bypass / Protocol Bypass / ルール	IPsec の設定を行います。
		IPsec アドレステンプレート	テンプレートリスト	
		IPsec テンプレート	テンプレートリスト	

A

B 索引