



ユーザーズガイド ネット トワーク操作編

HL-L8360CDW
HL-L9310CDW

目次

本ガイドの使い方	1
注意事項の定義	2
商標	3
重要事項	4
ネットワーク	5
対応している基本ネットワーク機能について	6
ネットワーク管理ソフトウェアおよびユーティリティ	7
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	8
他の無線ネットワーク設定方法について	9
本製品を無線ネットワーク用に設定する前に	10
無線ネットワーク用に本製品を設定する	11
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	12
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 ...	13
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	16
SSID が同報送信以外の場合の無線 LAN を本製品に設定する	18
エンタープライズ無線 LAN 用に本製品を設定する	20
Wi-Fi Direct®を使用する	22
高度なネットワーク機能について	31
ネットワーク設定レポートを印刷する	32
無線 LAN レポートを印刷する	33
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	36
上級ユーザーのための技術的な情報について	38
ギガビットイーサネット（有線 LAN のみ）	39
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	41
トラブルシューティング	42
クラウド接続機能のエラーメッセージ	43
ネットワークの問題	45
エラーメッセージ	46
ネットワーク診断修復ツールを使用する（Windows®）	48
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？	49
無線ネットワーク設定を完了できません	50
本製品で、ネットワーク経由の印刷ができません	52
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	54
Google クラウド プリントの問題	55
AirPrint の問題	56
セキュリティ	57
本製品の設定をロックする	58
設定ロックの概要	59
ネットワークセキュリティ機能	63
ネットワークセキュリティ機能を使用する前に	64
セキュリティ機能ロック 3.0	65
Active Directory®認証を使用する	71
LDAP 認証方式を使用する	75

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	79
IPsec を使用したネットワーク製品の安全な管理について	112
安全な E-mail の送信について	132
有線または無線 LAN への IEEE 802.1x 認証の使用について	137
印刷ログ機能	142
モバイル/ウェブ接続	147
クラウド接続機能	148
クラウド接続の概要	149
クラウド接続機能を使用してアクセスできるオンラインサービス	150
クラウド接続機能の使用条件について	151
クラウド接続機能の設定	155
写真や文書をダウンロードして印刷する	163
Google クラウド プリント	165
Google クラウド プリントの概要	166
Google クラウド プリントを使用する前に	167
Google Chrome™、または Chrome OS™ から印刷する	171
モバイル向けの Google Drive™ から印刷する	172
モバイル向けの Gmail™ ウェブメールサービスから印刷する	173
AirPrint	174
AirPrint の概要	175
はじめに	176
AirPrint を使用して印刷する	179
Windows® 用モバイルプリント	183
Mopria® Print Service	184
Brother iPrint&Scan	185
近距離無線通信 (NFC)	186
外付け IC カードリーダーに登録する	187
パソコンを使用して製品の設定を変更する	188
ウェブブラウザを使用して製品の設定を変更する	189
ウェブブラウザによる設定とは	190
ウェブブラウザによる設定画面にアクセスする	191
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	192

■ 本ガイドの使い方

- ・ [注意事項の定義](#)
- ・ [商標](#)
- ・ [重要事項](#)

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	警告は、この表示を無視して、誤った取り扱いをすると、人が死亡または重傷を負う可能性がある内容を示しています。
 注意	注意は、この表示を無視して、誤った取り扱いをすると、人が傷害を負う可能性がある内容を示しています。
重要	重要は、この表示を無視して、誤った取り扱いをすると、物的損害の可能性がある内容を示しています。
お願い	お願いは、ご使用していただく上での注意事項、制限事項などの内容を示しています。
	ヒントアイコンは、有益なヒントや補足情報を示しています。
	「感電の危険があること」を示しています。
	「火災の危険があること」を示しています。
	「やけどの危険があること」を示しています。
	「してはいけないこと」を示しています。
太字	本製品の操作パネルやパソコンの画面に表示されるボタンを示しています。
斜体	斜体は重要な項目の強調や、関連するトピックを示しています。
[XXXXX]	括弧で囲まれたテキストは、本製品の画面に表示されるメッセージを示しています。

✓ 関連情報

- [本ガイドの使い方](#)

商標

BROTHER は、ブラザー工業株式会社の商標または登録商標です。

Microsoft、Windows、Windows Server、Internet Explorer、および Active Directory 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 および iPod touch は、米国およびその他の国で登録されている、Apple 社の商標です。

AirPrint および macOS は、Apple 社の商標です。

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

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

Android、Gmail、Google クラウド プリント、Google Drive、Google Chrome、Chrome OS および Google Play は、グーグル社の商標です。これらの商標の使用には、グーグル社の許可が必要です。

Mopria® は、米国およびその他の国における Mopria Alliance 社の商標および登録商標です。無断使用は固く禁止されています。

Mozilla および Firefox は、Mozilla Foundation 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。

Bluetooth ワードマークは、Bluetooth SIG, Inc.が所有する登録商標であり、ブラザーは、これら商標を使用する許可を受けています。

PictBridge は商標です。

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

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



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。
- 本ユーザズガイド内の画面はイメージであるため実際の画面とは異なる場合があります。
- 特に指定のない限り、本書は Windows® 7 および macOS v10.10.5 の画面を使用していますが、実際のパソコンの画面はお使いの OS によって異なる可能性があります。
- 本ガイドならびに本製品の仕様は予告なく変更されることがあります。



関連情報

- [本ガイドの使い方](#)
-

■ ネットワーク

- 対応している基本ネットワーク機能について
- 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

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 (OS)	Windows® 7 Windows® 8 Windows® 10	Windows Server® 2008/2012/2012 R2/2016	macOS v10.10.5 macOS v10.11.x macOS v10.12
印刷	○	○	○
BRAdmin Light	○	○	
BRAdmin Professional	○	○	
ウェブブラウザによる設定	○	○	○
ステータスマニター	○		○
オートマチックドライバースト インストーラー	○	○	
Vertical Pairing	○		



- 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、お使いの製品のソフトウェアダウンロードページを開き、BRAdmin Light の最新版をダウンロードします。
- 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、お使いの製品のソフトウェアダウンロードページを開き、BRAdmin Professional ユーティリティの最新版をダウンロードします。



関連情報

- ネットワーク

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

ウェブブラウザ設定

ウェブブラウザ設定は、標準的なウェブブラウザを使用するユーティリティで、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。

BRAdmin Light (Windows®)

BRAdmin Light は、ネットワークに接続された本製品の初期設定を行うためのユーティリティです。ネットワーク上の本製品の検索、状態の閲覧、IP アドレスなどのネットワークの基本設定が行えます。

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、お使いの製品のソフトウェアダウンロードページを開き、BRAdmin Light をダウンロードします。



- Windows® ファイアウォールまたは、アンチスパイウェアまたはアンチウイルスアプリケーションのファイアウォール機能を使用している場合、それらを一時的に無効にします。印刷が可能であることを確認し、指示に従ってソフトウェアを設定します。

BRAdmin Professional (Windows®)

BRAdmin Professional は、ネットワークに接続されたブラザー機器の管理をより詳細に行うためのユーティリティです。このユーティリティは、お使いのネットワーク上にあるブラザー製品を検索し、Windows® Explorer 形式の画面に機器の状態を表示します。各機器の状態を分かりやすく表示させるため、画面上の色は変更されます。ローカル接続された製品を監視したい場合は、Print Auditor クライアントソフトウェアを、クライアントパソコンにインストールします。このユーティリティにより、BRAdmin Professional を使用して、USB インターフェイス経由でクライアントパソコンに接続されている製品を監視できます。



- 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、お使いの製品のソフトウェアダウンロードページを開き、BRAdmin Professional ユーティリティの最新版をダウンロードします。
- BRAdmin Professional で表示される本製品のお買い上げ時のノード名は、有線 LAN の場合は [BRNxxxxxxxxxxxx]、無線 LAN の場合は [BRWxxxxxxxxxxxx] 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。）
- Windows® ファイアウォールまたは、アンチスパイウェアまたはアンチウイルスアプリケーションのファイアウォール機能を使用している場合、それらを一時的に無効にします。印刷が可能であることを確認し、指示に従ってソフトウェアを設定します。



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場合、ブラザーインストール CD-ROM を使用することを推奨します。

- 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
- 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。

- 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 とパスワードを知っておく必要があります。
- 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（サポート対象モデルのみ）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（サポート対象モデルのみ）、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（サポート対象モデルのみ）と Wi-Fi Direct 接続は同時に使用できます。



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。



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、お使いのパソコンにインストール CD-ROM を挿入します。
 - Windows® の場合は、これらの指示に従ってください。
 - Mac の場合、**Driver Download** をクリックしてサポートサイト（ブラザーソリューションセンター）にアクセスします。画面の指示に従ってプリンタードライバーをインストールします。
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。



インストール画面がパソコンに表示されない場合は、以下の操作を行ってください。

- (Windows® 7)
コンピューターに進みます。CD/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。
- (Windows® 8 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、コンピューター（PC）にアクセスします。CD/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。
- ユーザー アカウント制御 画面が表示されたら、**はい**をクリックします。

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

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



関連情報

- [他の無線ネットワーク設定方法について](#)

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

お使いの無線 LAN アクセスポイント／ルーターが WPS (PBC : 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には、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されます。解除するには、[いいえ] を押します。
3. 画面に [アクセスポイントの WPS ボタンを 押してください 操作ができれば [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。

無線ネットワークのセットアップは完了しています。本機器の操作に必要なプリンタードライバーとソフトウェアをインストールするには、ブラザーインストールディスクを使用するか、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、本モデルのソフトウェアダウンロードページをご覧ください。



関連情報

- [他の無線ネットワーク設定方法について](#)
- [無線 LAN レポートのエラーコード](#)

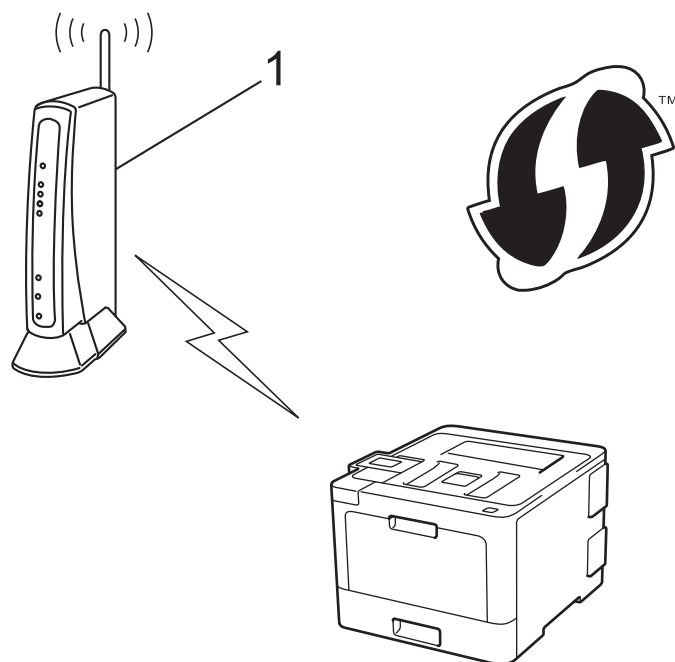
Wi-Fi Protected Setup™ (WPS) の PIN 方式を使用して本製品に無線ネットワークを設定する

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。

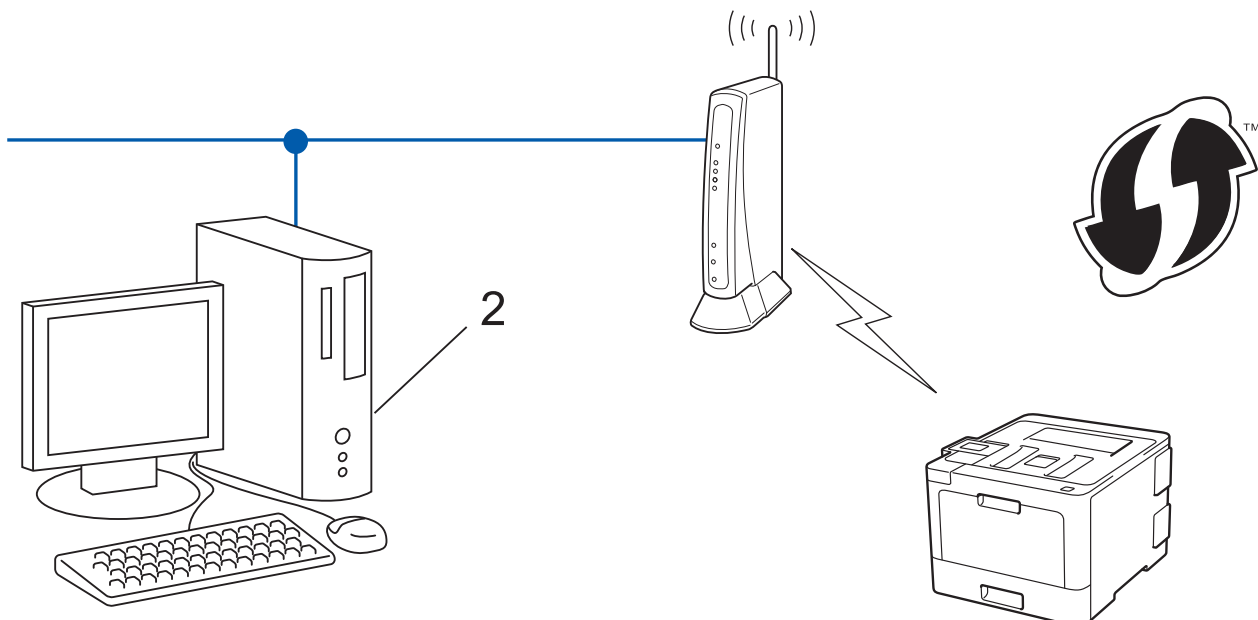
タイプ A

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には、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されます。解除するには、[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. ネットワークに接続したパソコンでウェブブラウザのアドレスバーに、レジストラーとして使用している機器の IP アドレスを入力します。(例: <http://192.168.1.2>)
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、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
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、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、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 または Windows® 10 をレジストラー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をインストールできます。ドライバとソフトウェアの完全なパッケージをインストールするには、本製品のインストール CD-ROM を使用します。

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. (Windows® 7) 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。

無線ネットワークのセットアップは完了しています。本機器の操作に必要なプリンタードライバとソフトウェアをインストールするには、ブラザーインストールディスクを使用するか、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、本モデルの**ソフトウェアダウンロード**ページをご覧ください。



関連情報

- [他の無線ネットワーク設定方法について](#)
 - [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。
- セットアップ中の操作に関してブラザーコールセンター（お客様相談窓口）に問い合わせる際は、SSID（ネットワーク名）およびネットワークキーをご準備ください。この情報に関してはお問い合わせいただいても回答できません。
- この情報（SSID およびネットワークキー）が不明の場合は、無線セットアップを行うことができません。

この情報はどこに載っていますか？

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

2.  [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されます。解除するには、[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、▲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. 本製品は、選択された無線機器へ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。

無線ネットワークのセットアップは完了しています。本機器の操作に必要なプリンタードライバーとソフトウェアをインストールするには、ブラザーインストールディスクを使用するか、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、本モデルの**ソフトウェアダウンロード** ページをご覧ください。



関連情報

- [他の無線ネットワーク設定方法について](#)
 - [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	
		AES	
	WPA/WPA2-PSK	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	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されます。解除するには、[いいえ] を押します。
- 本製品は使用しているネットワークを検索し、利用可能な SSID のリストを表示します。▲または▼を押して、[<New SSID>] を表示します。
- [<New SSID>]、を押してから、[OK] を押します。
- SSID 名を入力し、[OK] を押します。
- 指示が表示されたら、[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] オプションを選択した場合、[なし] または [WEP] を押します。
暗号化方式に [WEP] オプションを選択した場合、WEP キーを入力し、[OK] を押します。
 - [共有キー認証] オプションを選択した場合、WEP キーを入力し、[OK] を押します。
 - [WPA/WPA2-PSK] オプションを選択した場合、[TKIP+AES] または [AES] を押します。
WPA キーを入力し、[OK] を押します。



本ブラスター製品は最初の 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に接続しようとします。

無線機器が正常に接続されると、本製品の画面に [接続しました] と表示されます。

無線ネットワークのセットアップは完了しています。本機器の操作に必要なプリンタードライバーとソフトウェアをインストールするには、ブラザーインストールディスクを使用するか、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、本モデルの**ソフトウェアダウンロード** ページをご覧ください。

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。

- 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	Brother	12345678



- EAP-TLS 認証を使用して本製品を設定する場合、設定の開始前に、CA により発行されたクライアント証明書を必ずインストールしてください。クライアント証明書については、ネットワーク管理者に問い合わせてください。複数の証明書をインストールした場合、使用する証明書の名前を書き留めておくことをお勧めします。
- サーバー証明書の共通名を使用して本製品を確認する場合、設定の開始前に、使用する共通名を書き留めておくことをお勧めします。サーバー証明書の共通名については、ネットワーク管理者に問い合わせてください。

2.  [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されます。解除するには、[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。▲ または ▼ を押して、[<New SSID>] を表示します。
5. [<New SSID>]、を押してから、[OK] を押します。
6. SSID 名を入力し、[OK] を押します。
7. 指示が表示されたら、[インフラストラクチャ] を押します。
8. 認証方式を選択します。
9. 次のいずれかを行ってください。
 - [LEAP] を選択した場合、ユーザー ID を入力し、[OK] を押します。パスワードを入力し、[OK] を押します。
 - [EAP-FAST]、[PEAP] または [EAP-TTLS] を選択した場合、▲ または ▼ を押して内部認証方式を [NONE]、[CHAP]、[MS-CHAP]、[MS-CHAPv2]、[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。

- 暗号化タイプを [TKIP+AES] または [AES] から選択します。
- 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、その都度 [OK] を押します。
 - その他を選択した場合、その都度 [OK] を押します。



本製品に CA 証明書をインポートしていない場合、[検証しない] と表示されます。

- [EAP-TLS] オプションを選択した場合、暗号化方式を [TKIP+AES] または [AES] から選択します。
使用可能なクライアント証明書のリストが製品に表示された場合、使用する証明書を選択します。
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、その都度 [OK] を押します。
 - その他を選択した場合、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] と表示されます。

10. 製品は、選択された無線機器に接続しようとします。

無線機器が正常に接続されると、本製品の画面に [接続しました] と表示されます。

無線ネットワークのセットアップは完了しています。本機器の操作に必要なプリンタードライバーとソフトウェアをインストールするには、ブラザーインストールディスクを使用するか、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、本モデルの **ソフトウェアダウンロード** ページをご覧ください。



関連情報

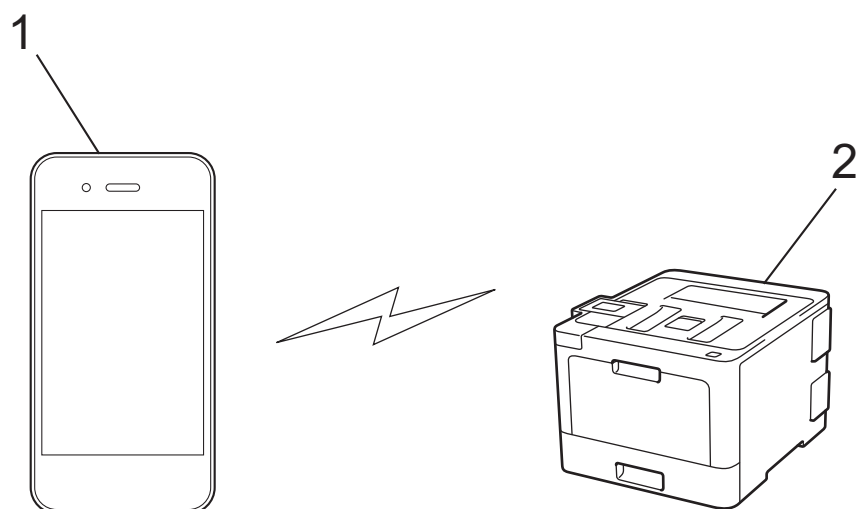
- [他の無線ネットワーク設定方法について](#)
- [無線 LAN レポートのエラーコード](#)

Wi-Fi Direct®を使用する

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

Wi-Fi Direct を使用した携帯端末からの印刷について

Wi-Fi Direct は、Wi-Fi Alliance®により開発された無線設定方法の一つです。これにより、アクセスポイントを使用せずに、ブラザー製品と、Android™ 機器、Windows® 機器、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（サポート対象モデルのみ）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。



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

無線ネットワーク環境で本製品を設定する 5 つの方法を以下に示します。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 iPrint&Scan 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](#)
- [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

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



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] 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（有効化の手順については、お使いの携帯端末の取扱説明書を参照）。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。解除するには、 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。モバイルプリント&スキャンガイド Brother iPrint&Scan 用 には、携帯端末からの印刷についての情報が含まれています。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、お使いの製品の製品マニュアルページを開き、ガイドをご覧ください。



関連情報

- [Wi-Fi Direct の設定について](#)
- [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. ▲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] 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 (有効化の手順については、お使いの携帯端末のユーザーズガイドを参照)。ブラザー製品の [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。モバイルプリント&スキャンガイド Brother iPrint&Scan 用 には、携帯端末からの印刷についての情報が含まれています。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、お使いの製品の製品マニュアルページを開き、ガイドをご覧ください。



関連情報

- [Wi-Fi Direct の設定について](#)
- [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] 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（有効化の手順については、お使いの携帯端末の取扱説明書を参照）。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。解除するには、 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。モバイルプリント&スキャンガイド Brother iPrint&Scan 用 には、携帯端末からの印刷についての情報が含まれています。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、お使いの製品の製品マニュアルページを開き、ガイドをご覧ください。



関連情報

- [Wi-Fi Direct の設定について](#)
- [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 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. ▲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. [相手側デバイスの Wi-Fi Direct 設定を 有効にして [OK] 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（有効化の手順については、お使いの携帯端末の取扱説明書を参照）、[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。モバイルプリント&スキャンガイド Brother iPrint&Scan 用 には、携帯端末からの印刷についての情報が含まれています。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、お使いの製品の**製品マニュアル**ページを開き、ガイドをご覧ください。



関連情報

- [Wi-Fi Direct の設定について](#)
- [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] > [手動接続] を押します。
2. 本製品の画面に SSID 名とパスワードが 5 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。モバイルプリント&スキャンガイド Brother iPrint&Scan 用 には、携帯端末からの印刷についての情報が含まれています。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、お使いの製品の**製品マニュアル**ページを開き、ガイドをご覧ください。



関連情報

- [Wi-Fi Direct の設定について](#)
- [Wi-Fi Direct ネットワーク設定の概要](#)

高度なネットワーク機能について

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

ネットワーク設定レポートを印刷する

ネットワーク設定レポートには、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、ネットワーク設定レポートに表示されます。お買い上げ時のノード名は、有線 LAN の場合は「BRNxxxxxxxxxxxx」、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を示します。）
- ネットワーク設定レポートに表示される [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：BRN000ca0000499
 - 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。
本製品はネットワーク設定レポートを印刷します。
3.  を押します。



関連情報

- [高度なネットワーク機能について](#)
- [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？](#)
- [ネットワーク診断修復ツールを使用する（Windows®）](#)
- [ウェブブラウザによる設定画面にアクセスする](#)
- [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](#)
- [ウェブブラウザを使用してギガビットイーサネットを設定する](#)

無線 LAN レポートを印刷する

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

1.  [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。
本製品は WLAN 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](#)
- [本製品で、ネットワーク経由の印刷ができません](#)
- [使用しているネットワーク機器が正しく動作していることを確認したい](#)

無線 LAN レポートのエラーコード

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

エラーコード	問題と推奨対策
TS-01	無線設定が有効ではありません。無線設定をオンに変更します。 ネットワークケーブルが本製品に接続されている場合、接続を切断して、本製品の無線設定をオンに変更します。
TS-02	無線 LAN アクセスポイント／ルーターを検出できません。 1. 以下の 2 点を確認します。 - 無線 LAN アクセスポイント／ルーターの電源を切り、10 秒待ってから、再度電源を入れます。 - 無線 LAN アクセスポイント／ルーターが MAC アドレスフィルタリングを使用している場合、本製品の MAC アドレスがそのフィルターで許可されていることを確認します。 2. SSID とセキュリティ情報（SSID／認証方式／暗号化方式／ネットワークキー）を手動で入力した場合、入力した情報が誤っている可能性があります。 SSID とセキュリティ情報を再確認して、必要に応じて正しい情報を再入力してください。 本機器は 5 GHz 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。
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。
TS-04	選択された無線 LAN アクセスポイント／ルーターが使用する認証／暗号化方式は、本製品でサポートされていません。 無線 LAN アクセスポイント／ルーターの認証および暗号化方式を変更します。本製品は以下の認証方式をサポートしています。 - WPA-Personal TKIP または AES - WPA2-Personal TKIP または AES - オープン WEP または、なし（暗号化なし） - 共有キー WEP 問題が解決しない場合、入力した SSID またはネットワーク設定が正しくない可能性があります。無線ネットワーク設定を確認してください。
TS-05	セキュリティ情報（SSID、ネットワークキー）が正しくありません。 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。
TS-06	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。 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。
TS-07	本製品は、WPS 対応の無線 LAN アクセスポイント／ルーターを検出できません。 WPS と接続する場合は、本製品と無線 LAN アクセスポイント／ルーターの両方を操作する必要があります。無線 LAN アクセスポイント／ルーターの WPS の接続方式を確認して、再起動してみます。 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。

エラーコード	問題と推奨対策
TS-08	WPS 対応の無線 LAN アクセスポイントが、2 箇所以上検出されています。 - WPS に対応した無線 LAN アクセスポイント／ルーターが範囲内で 1 つのみであることを確認して、再試行します。 - 他のアクセスポイントからの影響を避けるために、数分待ってから再試行してください。



関連情報

- 無線 LAN レポートを印刷する
- 本製品で、ネットワーク経由の印刷ができません
- 使用しているネットワーク機器が正しく動作していることを確認したい
- Wi-Fi Protected Setup™（WPS）のワンプッシュ方式を使用して本製品に無線ネットワークを設定する
- Wi-Fi Protected Setup™（WPS）の PIN 方式を使用して本製品に無線ネットワークを設定する
- 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

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. お買い上げ時はパスワードは必要ありません。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。
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**メニューをクリックします。
6. **SNTP** チェックボックスを選択し、設定を有効にします。
7. **OK** をクリックします。
8. 本ブラウザ製品を再起動して、設定を有効にします。
9. 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	XXX.XXX.XXX
プライマリー-SNTPサーバーポート	123
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	123
同期間隔	24 時間

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。 • 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

オプション	説明
	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	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 サーバーアドレス	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	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	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）。

10. **OK** をクリックします。



関連情報

- [高度なネットワーク機能について](#)

上級ユーザーのための技術的な情報について

- ギガビットイーサネット（有線 LAN のみ）
- 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

ギガビットイーサネット（有線 LAN のみ）

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



- カテゴリー 5e 以上のストレートタイプのツイストペアケーブルを使用してください。本製品をギガビットイーサネットネットワークに接続する場合、1000BASE-T に準拠しているネットワーク機器を使用してください。



関連情報

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

ウェブブラウザを使用してギガビットイーサネットを設定する

1. ウェブブラウザを起動します。
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. お買い上げ時はパスワードは必要ありません。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。
4. **ネットワーク**タブをクリックします。
5. **有線**をクリックします。
6. 左側にあるナビゲーションバーの**イーサネット**をクリックします。
7. **イーサネットモード**ドロップダウンリストから**自動**を選択します。
8. **OK** をクリックします。
9. 設定を有効にするには、本製品を再起動します。

設定値は、ネットワーク設定リストを印刷して確認することができます。

関連情報

- [ギガビットイーサネット（有線 LAN のみ）](#)
- [ネットワーク設定レポートを印刷する](#)

ネットワーク設定をお買い上げ時の設定にリセットする

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



- すべての有線 LAN（サポート対象モデルのみ）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。
- BRAdmin Light、BRAdmin Professional、または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?] が表示されます。[はい] を 2 秒間押して、確認します。
本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

本製品の使用時に生じやすい一般的な問題を解決するには、この章をご覧ください。ほとんどの問題はご自身で解決できます。

重要

技術的サポートについては、必ず本製品をお買い上げの国内にてお問い合わせください。お問い合わせは、必ずお買い上げの国内にて行ってください。

ブラザー製品以外の消耗品を使用すると、印刷品質、ハードウェア性能、および製品の信頼性に影響する場合があります。



サポートが必要な場合は、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)にアクセスしてください。

まず、以下を確認してください：

- 製品の電源コードが正しく接続され、電源がオンになっている。かんたん設置ガイドをご覧ください。
- 製品から保護部品がすべて取り外されている。かんたん設置ガイドをご覧ください。
- 用紙トレイに用紙が正しくセットされている。
- 製品とパソコンにインターフェイスケーブルがしっかりと接続されている、または、無線接続が製品とパソコンの両方で設定されている。
- エラーおよびメンテナンスメッセージ

確認して問題が解決できなかった場合、問題を特定し関連情報をご覧ください。



関連情報

- [クラウド接続機能のエラーメッセージ](#)
- [ネットワークの問題](#)
- [Google クラウド プリントの問題](#)
- [AirPrint の問題](#)

クラウド接続機能のエラーメッセージ

エラーが発生すると、お使いのブラザー製品にエラーメッセージが表示されます。最も発生頻度の高いエラーのエラーメッセージを、表に示します。

ほとんどのエラーはユーザーご自身で解決することができます。この表を参照してもエラーが解決しない場合は、サポートサイト（ブラザーソリューションセンター）で最新のトラブルシューティングをご参照ください。

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 にアクセスしてください。

接続エラー

エラーメッセージ	原因	対処
[ネットワーク接続エラー 02] [利用するためには インターネット接続が必要です 本製品のネットワーク設定メニュー から設定を行ってください]	お使いのブラザー製品がネットワークに接続されていません。	- ネットワーク接続が良好であることを確認します。 - お使いのブラザー製品の電源を投入した後、すぐに[クラウド]を押した場合、ネットワーク接続がまだ確立されていない可能性があります。しばらく時間をおいてから再度実行してください。
[ネットワーク接続エラー 03] [サーバーへの接続に失敗しました 利用するためにはインターネットにアクセスできるネットワークに 接続されている必要があります]	- ネットワークやサーバーの設定が間違っています。 - ネットワークまたはサーバーに問題があります。	- ネットワークの設定が正しいことを確認するか、少し待ってから再度実行してください。 - お使いのブラザー製品の電源を投入した後、すぐに[クラウド]を押した場合、ネットワーク接続がまだ確立されていない可能性があります。しばらく時間をおいてから再度実行してください。
[ネットワーク接続エラー 07] [サーバーへの接続に失敗しました 時刻設定が正しくありません]	日付と時刻の設定が間違っています。	日時と時刻を正しく設定します。お使いのブラザー製品の電源コードが抜かれた場合、日付と時刻がお買い上げ時の設定にリセットされることがあります。

認証エラー

エラーメッセージ	原因	対処
[認証エラー 01] [PIN コードが正しくありません 正しいPINを入力してください]	入力した PIN コードが正しくありません。PIN コードは、お使いのブラザー製品にアカウントを登録する際に入力した 4 桁の数字です。	正しい PIN コードを入力してください。
[認証エラー 02] [仮登録 ID が間違っているか発行された仮登録 ID がすでに失効しています または一度使用した仮登録 ID は使用できません 正しい仮登録 ID を入力するか仮登録 ID の再発行を行ってください 仮登録 ID の有効期限は発行から 24 時間です]	入力された仮登録 ID が正しくありません。 入力された仮登録 ID の期限が切れています。仮登録 ID は、24 時間有効です。	正しい仮登録 ID を入力してください。 再度クラウド接続機能の利用申請を行い、新たに仮登録 ID を取得します。次に、新しい仮登録 ID を使ってお使いのブラザー製品にアカウントを登録してください。
[認証エラー 03] [表示名がすでに登録されています 異なる表示名を登録してください]	表示名として入力した名前がすでに別のユーザーに登録されています。	別の表示名を入力してください。

サーバーエラー

エラーメッセージ	原因	対処
[サーバーエラー 01] [サービスへの認証情報が無効です 下記ウェブページより 仮登録 ID を 取得する必要があります http:// bwc.brother.com 仮登録 ID を取 得後 OK を押してください]	ブラザー製品の認証情報（サービスに アクセスするために必要）の有効期限 が切れている、または無効です。	再度クラウド接続機能の利用申請を 行い、新たに仮登録 ID を取得します。 次に、新しい仮登録 ID を使ってお使い のブラザー製品にアカウントを登録 してください。
[サーバーエラー 03] [サービスが対応していないファイル の、アップロードに失敗しました 未 対応のファイルもしくは画像が壊れ ています ファイル情報を確認してく ださい]	アップロードしようとしているファ イルに次のような問題があります。 • ファイルの画素数、サイズなどが サービスの制限を超えている。 • ファイル形式が非対応。 • ファイルが破損している。	このファイルは使えません。 • サービスが対応しているファイル サイズ、形式の上限を確認してく ださい。 • 別のファイル形式で保存してくだ さい。 • 可能であれば、新しく破損してな いファイルを取得してください。
[サーバーエラー 13] [サービスが一時的に利用できません 時間を置いて再試行してください]	Web サービスに問題があり、現在使用 できません。	少し待ってから再実行します。再度 メッセージが表示された場合は、ウェ ブサービスが利用可能かどうかを確認 するためにパソコンからウェブサ ービスにアクセスしてみてください。

ショートカットエラー

エラーメッセージ	原因	対処
[ショートカットエラー 02] [利用アカウントが使用できなくなっ ています 選択したショートカットを 削除後アカウントの再登録およびシ ョートカットの再登録を行なってく ださい]	ショートカットが登録された後にア カウントが削除されたため、ショール トカットを使用することはできません。	ショートカットを削除し、再度アカウ ントとショートカットを登録します。



関連情報

- [トラブルシューティング](#)

ネットワークの問題

- [エラーメッセージ](#)
- [ネットワーク診断修復ツールを使用する \(Windows®\)](#)
- [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 [OK]を押してください]	本製品がグループオーナー (G/O) 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。	• 認証設定のユーザー名およびパスワードが正しいことを確認します。ユーザー名がドメインの一部である場合、ユーザー@ドメインまたは、ドメイン\ユーザーのいずれかの形式でユーザー名を入力します。 • SNTP タイムサーバーが正確に設定され、設定された時間が、認証のために Kerberos または NTLMv2 により使用される時間と一致することを確認します。
[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。
	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。	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。
[通信エラー]	Wi-Fi Direct 設定中に本製品とお使いの携帯端末が通信できません。	• 携帯端末を本製品に近づけます。 • 本製品と携帯端末を、障害物のない場所に移動します。 • WPS の PIN 方式を使用している場合、PIN コードを必ず正確に入力してください。
[ファイルアクセスに失敗しました 管理者に連絡してください]	印刷ログのネットワークへの保存機能用の保存フォルダに本製品を接続できません。	• 保存されたディレクトリー名が正しいことを確認します。 • 保存されたディレクトリーが書き込み可能であることを確認します。 • ファイルがロックされていないことを確認します。
[ログの書き込みができません]	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。	• 本製品とお使いの携帯端末が、Wi-Fi Direct モードであることを確認します。 • 携帯端末を本製品に近づけます。 • 本製品と携帯端末を、障害物のない場所に移動します。 • Wi-Fi Direct を手動で設定している場合、パスワードが正しく入力されたことを確認します。 • IP アドレスを取得する方法について、お使いの携帯端末に設定ページがある場合、携帯端末の IP アドレスが DHCP を通して設定されたことを確認します。
[サーバーが見つかりません 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サーバーに本製品を接続できません。	• サーバーのアドレスが正しいことを確認します。 • サーバーがネットワークに接続していることを確認します。 • 本製品がネットワークに接続していることを確認します。

エラーメッセージ	原因	対応
[サーバーが見つかりません]	LDAP サーバーに本製品を接続できません。	- サーバーのアドレスが正しいことを確認します。 - サーバーがネットワークに接続していることを確認します。 - 本製品がネットワークに接続していることを確認します。
	Active Directory®サーバーに本製品を接続できません。	- サーバーのアドレスが正しいことを確認します。 - サーバーがネットワークに接続していることを確認します。 - 本製品がネットワークに接続していることを確認します。
[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ません。	SNTP タイムサーバーにアクセスするための設定値が、ウェブブラウザ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

- [ネットワークの問題](#)

ネットワーク診断修復ツールを使用する (Windows®)

ネットワーク診断修復ツールを使用して、本製品のネットワーク設定を修正します。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。

- Windows® 7/Windows® 8/Windows® 10
必ず管理者権限でログオンしてください。
- 本製品がオンの状態で、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ることを確認します。

1. 次のいずれかを行ってください。

オプション	説明
Windows Server® 2008	 (スタート) > すべてのプログラム > Brother > Brother 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 ツール をクリックし、 ネットワーク診断修復ツール をクリックします。
Windows® 7	 (スタート) > すべてのプログラム > Brother > Brother 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 ツール をクリックし、 ネットワーク診断修復ツール をクリックします。
Windows® 8/ Windows® 10	 (Brother Utilities) を起動し、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 ツール をクリックし、 ネットワーク診断修復ツール をクリックします。
Windows Server® 2012 / 2012 R2 / 2016	 (Brother Utilities) を起動し、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 ツール をクリックし、 ネットワーク診断修復ツール をクリックします。



- ユーザー アカウント制御** 画面が表示されたら、**はい**をクリックします。

2. 画面の指示に従います。
3. ネットワーク設定リストを印刷して、診断結果を確認します。



ステータスマニターで**接続状態を常に監視する**を選択した場合、ネットワーク診断修復ツールが自動的に起動します。ステータスマニター画面を右クリックして、**その他の設定** > **接続状態を常に監視する**をクリックします。この操作では IP アドレスが自動的に変更されるため、ネットワーク管理者が IP アドレスを Static に設定している場合は、本操作をお勧めしません。

ネットワークプリンター診断修復ツールを使用した後でも、正しい IP アドレスとサブネットマスクが割り当てられていない場合は、ネットワーク管理者に問い合わせてください。



関連情報

- [ネットワークの問題](#)
- [ネットワーク設定レポートを印刷する](#)
- [本製品で、ネットワーク経由の印刷ができません](#)
- [使用しているネットワーク機器が正しく動作していることを確認したい](#)

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。	- 無線 LAN 情報確認ツールを使用して、セキュリティー設定を確認します。詳細の確認やツールのダウンロードを行う場合は、サポートサイト（ブザーソリューションセンター）（support.brother.co.jp）にアクセスし、お使いのモデルのソフトウェアダウンロードページを参照してください。 - 正しいセキュリティ設定値を選択していることを確認します。 - セキュリティ設定の表示方法については、お使いの無線 LAN アクセスポイント／ルーターの取扱説明書を参照してください。 - 無線 LAN アクセスポイント／ルーターの製造者名またはモデル番号が、お買い上げ時のセキュリティ設定値として使用されている場合があります。 - アクセスポイント／ルーターの製造元、インターネットプロバイダー、またはネットワーク管理者に問い合わせてください。	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 の隠ぺいが有効になっています）。	- 正しい SSID 名またはネットワークキーを手動で入力します。 - 無線 LAN アクセスポイント／ルーターの説明書で SSID 名またはネットワークキーを確認し、無線ネットワークを再設定します。	無線
セキュリティ設定 (SSID／パスワード) に誤りがあります。	- SSID およびパスワードを確認します。 - ネットワークを手動で設定する場合、SSID とパスワードは本製品に表示されます。お使いの携帯端末が手動設定をサポートしている場合、SSID とパスワードは携帯端末の画面に表示されます。	Wi-Fi Direct
Android™ 4.0 を使用しています。	携帯端末の接続が切断された場合（Wi-Fi Direct を使用してから約 6 分後）、WPS（推奨）を使ったワンプッシュ設定を試み、本製品を G/O（グループオーナー）として設定してください。	Wi-Fi Direct
本製品がお使いの携帯端末から離れ過ぎています。	本製品を携帯端末の約 1 メートル以内に近づけて、Wi-Fi Direct 接続の設定を行います。	Wi-Fi Direct
本製品と携帯端末との間に何らかの障害物（壁や家具など）があります。	本製品を、障害物のない場所に移動します。	Wi-Fi Direct
本製品または携帯端末の近くに、無線パソコン、Bluetooth 対応機器、電子レンジ、またはデジタルコードレス電話があります。	他の機器を、本製品または携帯端末から離れた場所に移動します。	Wi-Fi Direct
上記の対策すべてを試しても Wi-Fi Direct の設定が完了できない場合は、右記の対応を行ってください。	- 本製品の電源を一度切ってから、再度、入れ直します。Wi-Fi Direct 設定をもう一度行います。 - 本製品をクライアントとして使用している場合、現在の Wi-Fi Direct 接続で許可されている機器の数と、接続されている機器の数を確認します。	Wi-Fi Direct

Windows®の場合

上記の対策をすべて行っても、無線 LAN 接続に問題がある場合は、ネットワークプリンター診断修復ツールをご使用になることをお勧めします。



関連情報

- [ネットワークの問題](#)
 - [SSID が同報送信以外の場合の無線 LAN を本製品に設定する](#)
 - [Wi-Fi Direct®を使用する](#)
-

本製品で、ネットワーク経由の印刷ができません

原因	対応	インターフェイス
お使いのセキュリティソフトウェアが、本製品のネットワークへのアクセスをブロックしています。	インストールが正常に完了した場合でも、セキュリティソフトが警告を出さずにアクセスをブロックしている場合があります。 アクセスを許可するには、セキュリティソフトウェアの説明書を参照するか、ソフトウェアの製造元に問い合わせてください。	有線／無線
本製品に、有効な IP アドレスが割り当てられていません。	- IP アドレスとサブネットマスクを確認します。 お使いのパソコンと本製品の、IP アドレスとサブネットマスクがいずれも正確で、同一のネットワーク上に存在することを確認します。 IP アドレスとサブネットマスクの確認方法に関する詳細については、ネットワーク管理者に問い合わせてください。 - Windows® ネットワークプリンター診断修復ツールを使用して、IP アドレスとサブネットマスクを確認します。	有線／無線
失敗した印刷ジョブが、パソコンの印刷キューに残っています。	- 失敗した印刷ジョブがパソコンの印刷キューに残っている場合は、そのジョブを削除します。 - または、以下のフォルダでプリンターアイコンをダブルクリックし、すべての文書をキャンセルします。 - Windows® 7  (スタート) > デバイスとプリンター > プリンターと FAX をクリックします。 - Windows® 8 マウスポインタをデスクトップの右下隅に移動します。メニューバーが表示されたら、設定 > コントロール パネル をクリックします。ハードウェアとサウンドグループ で デバイスとプリンターの表示 > プリンター をクリックします。 - Windows® 10 および Windows Server® 2016  > Windows システム ツール > コントロール パネル をクリックします。ハードウェアとサウンドグループ で、デバイスとプリンターの表示 > プリンター をクリックします。 - Windows Server® 2008 スタート > コントロール パネル > プリント 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 コントロール パネル画面でスタート 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。 - macOS v10.10.5、v10.11.x、v10.12 システム環境設定 > プリンタとスキャナ をクリックします。	有線／無線
本製品は無線ネットワークに接続されていません。	WLAN レポート（無線 LAN レポート）を印刷して、エラーコードを確認します。	無線

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



関連情報

- ネットワークの問題
- 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
- ネットワーク診断修復ツールを使用する (Windows®)
- 使用しているネットワーク機器が正しく動作していることを確認したい

使用しているネットワーク機器が正しく動作していることを確認したい

確認	対応	インターフェイス
本製品、アクセスポイント／ルーター、またはネットワークハブの電源が入っていることを確認します。	以下を確認します。 - 電源コードが正しく接続され、本製品の電源が入っている。 - アクセスポイント／ルーター、またはハブの電源が入った状態で、リンクボタンが点滅している。 - 保護包装は本製品からすべて取り除かれている。 - トナーカートリッジとドラム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 ターミナルアプリケーションで、IP アドレスまたはノード名を使用して、パソコンから本製品に Ping を実行します。 ping [<ipaddress>] または [<nodename>] - 成功：本製品は正常に動作し、お使いのパソコンと同一のネットワークに接続されています。 - 失敗：本製品は、お使いのパソコンと同一のネットワークに接続されていません。 (Windows®) ネットワーク管理者に問い合わせ、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

- [ネットワークの問題](#)
- [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](#)
- [ネットワーク診断修復ツールを使用する \(Windows®\)](#)
- 本製品で、ネットワーク経由の印刷ができません

Google クラウド プrint の問題

問題	対応
お使いのブラザー製品がプリンター一覧に表示されない。	製品の電源が入っていることを確認します。
	Google クラウド プrint が有効になっていることを確認します。
	お使いの製品が Google クラウド プrint に登録されていることを確認します。登録されていない場合は、もう一度登録してください。
印刷できない。	製品の電源が入っていることを確認します。
	ネットワーク設定を確認します。関連情報をご覧ください。
	ファイルによっては、印刷できない場合、または表示された通りに印刷できない場合があります。
ブラザー製品を Google クラウド プrint に登録できない。	お使いの製品が、インターネットにアクセスできるネットワークに接続されているか確認してください。
	お使いの製品で日付と時刻が正しく設定されていることを確認してください。
登録設定をやり直しても、Google クラウド プrint 登録時に、製品上に確認メッセージが表示されない。	Google クラウド プrint に登録している間は、お使いの製品が待ち受け状態になっていることを確認してください。



関連情報

- [トラブルシューティング](#)
- [Google クラウド プrint を使用するためのネットワーク設定](#)

AirPrint の問題

こんなときは	対処のしかた
本製品がプリンターリストに表示されません。	本製品の電源が入っていることを確認してください。
	ネットワーク設定を確認してください。関連情報をご覧ください。
	携帯端末を無線 LAN アクセスポイント、ルーターまたは本製品に近づけてください。
印刷できません。	本製品の電源が入っていることを確認してください。
	ネットワーク設定を確認してください。関連情報をご覧ください。
Apple 端末から複数のページを印刷しようとしても、最初のページしか印刷されません。	お使いの端末が、最新の iOS を搭載しているか確認してください。 AirPrint の詳細については下記の Apple のサポート記事を参照してください： support.apple.com/kb/HT4356



関連情報

- [トラブルシューティング](#)
- [AirPrint の概要](#)
- [AirPrint を使用するためのネットワーク設定](#)

■ セキュリティ

- 本製品の設定をロックする
- ネットワークセキュリティ機能

本製品の設定をロックする

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、管理者またはブラザーコールセンターに問い合わせ、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。

- [設定ロックの概要](#)

設定ロックの概要

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。

設定ロックがオンに設定されているとき、本製品の設定にアクセスするにはパスワードの入力が必要になります。

- [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. パスワードに 4 桁の数値を入力します。
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

- [設定ロックの概要](#)

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

- [設定ロックの概要](#)

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

- [設定ロックの概要](#)

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 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 のその他の機能について
- 本製品の操作パネルを使用して新しい ID カードを登録する

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、特定ユーザーにアクセス設定をして、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。

ウェブブラウザまたは BAdmin Professional (Windows®) 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、AirPrint、Google クラウド プリント™、および Brother iPrint&Scan 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。

- **カラープリント**

- USB ダイレクトプリント

- **クラウド接続** (サポート対象モデルのみ)

- **枚数制限**

- **ページカウンター**

- **カード ID** (サポート対象モデルのみ)

ユーザーのカード ID を事前に登録すると、登録ユーザーは、登録済みカードを本製品の NFC タッチ部分にタッチして製品を有効化することができます。



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. お買い上げ時はパスワードは必要ありません。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。
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。
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. ユーザーのカード ID を登録するには、**カード ID** 欄でカード番号を入力します（特定モデルのみ対応）。
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 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、AirPrint、Google クラウド プリント、および Brother iPrint&Scan 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. お買い上げ時はパスワードは必要ありません。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。
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](#)
- [ウェブブラウザを使用して Google クラウド プリントに本製品を登録する](#)

セキュリティ機能ロック 3.0 のその他の機能について

セキュリティ機能ロック画面で以下の機能を設定できます。

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。

カード ID（サポート対象モデルのみ）

ユーザーリストメニューをクリックし、**カード ID** フィールドにユーザーのカード ID を入力します。ご自身のカード ID を認証に使用できます。

前回ログ

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



関連情報

- [セキュリティ機能ロック 3.0](#)

本製品の操作パネルを使用して新しい ID カードを登録する

1. 登録済みの ID カードを、製品の操作パネルの NFC タッチ部分にタッチします。
2. 表示されたログイン名を押します。
3. [カード情報を登録する]を押します。
4. 新しい ID カードを NFC タッチ部分にタッチします。
5. [OK]を押します。

新しい ID カードの番号が本製品に登録されます。



使用できる ID カードタイプは、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）の、よくあるご質問（Q&A）ページをご覧ください。



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

Active Directory®認証の設定は、ウェブブラウザまたは BRAdmin Professional (Windows®) 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. お買い上げ時はパスワードは必要ありません。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。
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、ブラザーの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。
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。
LDAP ポート	ポート番号を入力して LDAP 経由で Active Directory® サーバー（ LDAP + kerberos 認証方式のみ対応）に接続します。

10. **OK** をクリックします。

✓ 関連情報

- [Active Directory®認証を使用する](#)

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

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

1. 製品の操作パネルに、ユーザー ID を入力します。
2. [OK] を押します。
3. パスワードを入力します。
4. [OK] を押します。
5. 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

LDAP 認証の設定は、ウェブブラウザーまたは BRAdmin Professional (Windows®) 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. お買い上げ時はパスワードは必要ありません。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。
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、ブラザーの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。
ユーザー ID を記憶	このオプションを選択して、ユーザー ID を保存します。
LDAP アドレス	LDAP サーバーの IP アドレスまたはサーバー名（例：ldap.example.com）を入力します。
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ーを入力します。
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. 製品の操作パネルに、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](#)
- [BRAdmin Professional を使用したネットワーク製品の安全な管理について \(Windows®\)](#)
- [SSL/TLS を使用して文書を安全に印刷する](#)

SSL/TLS について

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。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場合に、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

ブラウザ製品で 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るだけです。

✓ 関連情報

- [SSL/TLS について](#)

証明書とウェブブラウザ設定について

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

本ブラウザ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、本製品との通信が可能になります。本製品では、以下に示すセキュリティ証明書機能が使用できます。

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

本製品は、以下の証明書をサポートしています。

- プリインストールされた証明書

本製品には、自己署名証明書があらかじめ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。安全性を高めるために、信頼のおける組織が発行する証明書を使用することを推奨します。

- 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、CA から別の証明書を作成したりインストールしたりすることなく、SSL/TLS 通信を簡単に使用できます。

- 認証局（CA）からの証明書

すでに CA 発行の証明書を持っている場合、または外部の信頼された CA が発行した証明書を使用したい場合は、以下の 2 つのインストール方法があります。

- 本プリントサーバーから証明書署名要求（CSR : Certificate Signing Request）を送信する
- 証明書とプライベートキーをインポートする

- 認証局（CA）証明書

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、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 通信を使用する予定がある場合、まずシステム管理者に問い合わせることをお勧めします。
- 本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も同一の証明書とプライベートキーを保持する場合は、それらをリセットする前にエクスポートし、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、本ブラウザ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する

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://brnxxxxxxxxxxxxx

NetBIOS 名は、ネットワーク設定リストで確認できます。

- Mac の場合、**ステータスマニター**画面に表示される本製品アイコンをクリックして、ウェブブラウザ経由でアクセスします。

3. お買い上げ時はパスワードは必要ありません。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。
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. **Yes** 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)

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。

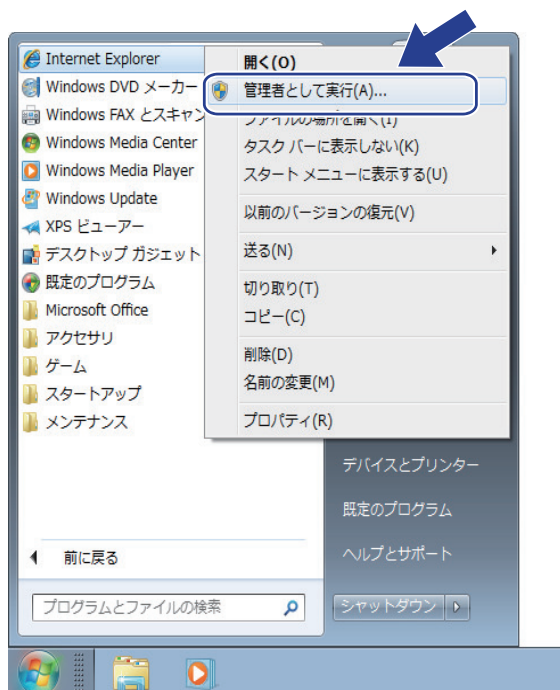
- (Windows Server® 2012 および Windows Server® 2012 R2)

 (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。



その他 オプションが表示されたら、**その他**をクリックします。

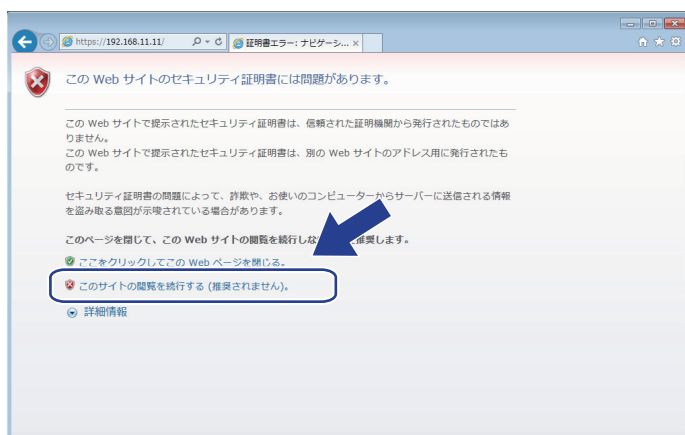


ユーザー アカウント制御 画面が表示されたら、**はい**をクリックします。

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。



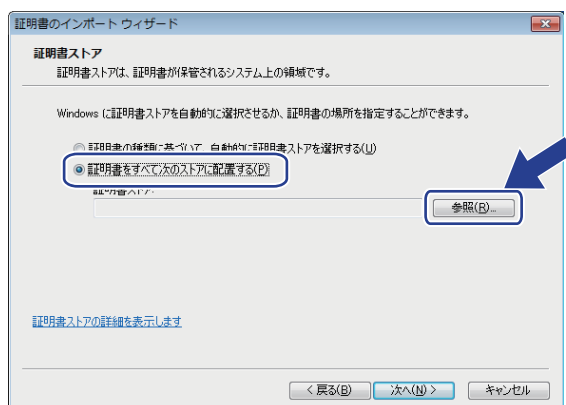
5. 証明書のエラーをクリックして、証明書の表示をクリックします。



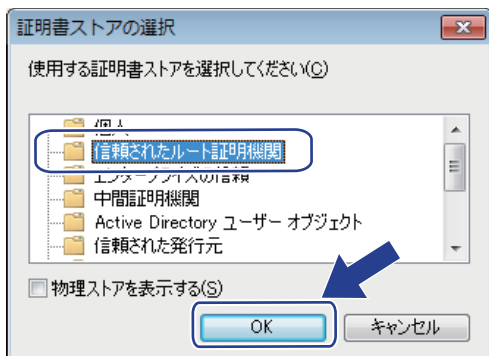
6. 証明書のインストール...をクリックします。



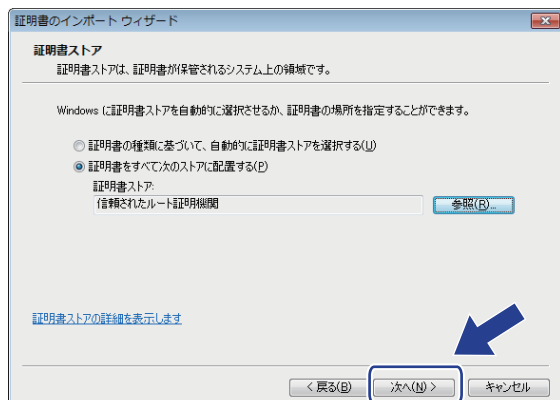
7. 証明書のインポート ウィザードが表示されたら、**次へ**をクリックします。
8. 証明書をすべて次のストアに配置するを選択して、**参照...**をクリックします。



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（拇印）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（拇印）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する

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管理について > 証明書とウェブブラウザ設定について > 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する > 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://brnxxxxxxxxxxxxx

NetBIOS 名は、ネットワーク設定リストで確認できます。

- Mac の場合、**ステータスマニター**画面に表示される本製品アイコンをクリックして、ウェブブラウザ経由でアクセスします。

3. お買い上げ時はパスワードは必要ありません。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。
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する > 自己署名証明書をエクスポートする

自己署名証明書をエクスポートする

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://brnxxxxxxxxxxxxx

NetBIOS 名は、ネットワーク設定リストで確認できます。

- Mac の場合、**ステータスマニター**画面に表示される本製品アイコンをクリックして、ウェブブラウザ経由でアクセスします。

3. お買い上げ時はパスワードは必要ありません。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。
4. **ネットワーク**タブをクリックします。
5. **セキュリティ**タブをクリックします。
6. **証明書**をクリックします。
7. **証明書一覧**に示される**エクスポート**をクリックします。
8. ファイルを暗号化する場合、**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する

■ 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、お使いのパソコンに CA からのルート証明書を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://brnxxxxxxxxxxxx

NetBIOS 名は、ネットワーク設定リストで確認できます。

- Mac の場合、**ステータスマニター**画面に表示される本製品アイコンをクリックして、ウェブブラウザ経由でアクセスします。

3. お買い上げ時はパスワードは必要ありません。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。
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。お買い上げ時の設定では、ノード名が表示されます。**コモンネーム**は必須です。
- 証明書に使用された共通名とは異なる名前が URL に入力された場合は、警告が表示されます。
- **組織、部署、市、および県/州**の長さは 64 バイト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 のエンタープライズのルート CA を使用している場合、クライアント証明書の安全な作成のために、証明書用ウェブサーバーテンプレートを使用することを推奨します。EAP-TLS 認証を行う IEEE 802.1x 環境のためのクライアント証明書を作成する場合、証明書用ユーザーテンプレートを使用することを推奨します。詳細については、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、本モデルのページを参照してください。



関連情報

- [認証局（CA）からの証明書の作成とインストールについて](#)

証明書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://brnxxxxxxxxxxxx

NetBIOS 名は、ネットワーク設定リストで確認できます。

- Mac の場合、**ステータスマニター**画面に表示される本製品アイコンをクリックして、ウェブブラウザ経由でアクセスします。

3. お買い上げ時はパスワードは必要ありません。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。
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管理について > 証明書とウェブブラウザ設定について > 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な管理について > 証明書とウェブブラウザ設定について > 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://brnxxxxxxxxxxxxx

NetBIOS 名は、ネットワーク設定リストで確認できます。

- Mac の場合、**ステータスマニター**画面に表示される本製品アイコンをクリックして、ウェブブラウザ経由でアクセスします。

3. お買い上げ時はパスワードは必要ありません。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。
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な管理について > 証明書とウェブブラウザ設定について > 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://brnxxxxxxxxxxxxxx

NetBIOS 名は、ネットワーク設定リストで確認できます。

- Mac の場合、**ステータスマニター**画面に表示される本製品アイコンをクリックして、ウェブブラウザ経由でアクセスします。

3. お買い上げ時はパスワードは必要ありません。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。
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](#)

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://brnxxxxxxxxxxxx

NetBIOS 名は、ネットワーク設定リストで確認できます。

- Mac の場合、**ステータスモニター**画面に表示される本製品アイコンをクリックして、ウェブブラウザ経由でアクセスします。

3. お買い上げ時はパスワードは必要ありません。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。
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://brnxxxxxxxxxxxxx

NetBIOS 名は、ネットワーク設定リストで確認できます。

- Mac の場合、**ステータスマニター**画面に表示される本製品アイコンをクリックして、ウェブブラウザ経由でアクセスします。

3. お買い上げ時はパスワードは必要ありません。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。
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

本製品にインストールされた複数の証明書は、ウェブブラウザによる設定を使用して管理することができます。ウェブブラウザによる設定で、**証明書**または**CA 証明書**画面に移動し、証明書の表示、削除、またはエクスポートを行います。

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

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



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

✓ 関連情報

- [証明書とウェブブラウザ設定について](#)

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ー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。



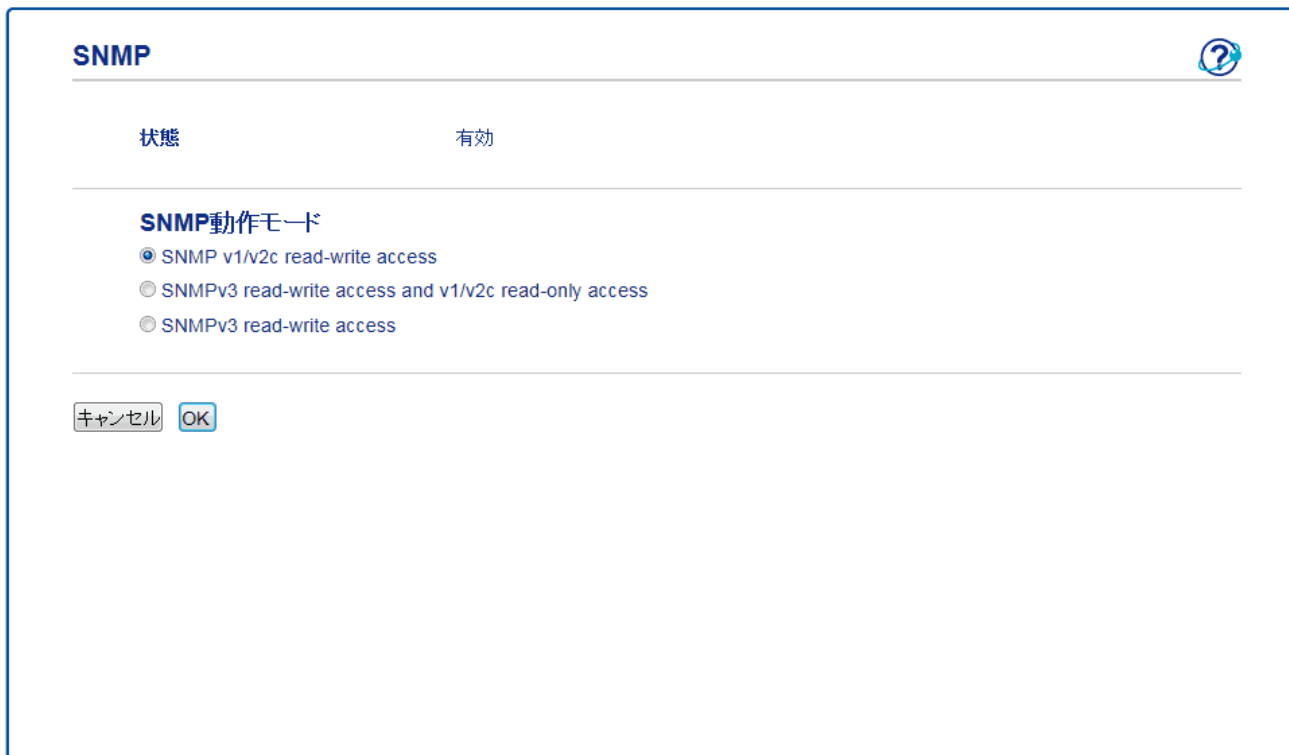
- お買い上げ時の設定では、HTTPS プロトコルは有効です。
- ウェブブラウザ画面で HTTPS プロトコルの設定を変更できます。

1. ウェブブラウザを起動します。
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. お買い上げ時はパスワードは必要ありません。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。
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。
- BRAdmin Professional を使用して SNMP 設定の変更も行えます。

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、すべてのブラザー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 and v1/v2c read-only access モードを使用する場合、Ver. 1 と Ver. 2c のリードオンリーが認証されるため、プリントサーバーにアクセスするブラザーアプリケーション（BRAdmin Light など）の一部が正常に機能しない場合があります。すべてのアプリケーションを使用する場合、**SNMP v1/v2c read-write access** モードをご使用になることをお勧めします。

- **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。



SNMPv3 read-write access モードを使用する場合、以下に注意してください。

- プrintサーバーを管理するには BRAdmin Professional またはウェブブラウザによる設定画面のみ使用できます。
- BRAdmin Professional 以外の、SNMPv1/v2c を使用するすべてのアプリケーションの使用が制限されます。SNMPv1/v2c アプリケーションの使用を許可するには、**SNMPv3 read-write access and v1/v2c read-only access** または **SNMP v1/v2c read-write access** モードを使用します。

9. **OK** をクリックします。



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](#)

BRAdmin Professional を使用したネットワーク製品の安全な管理について (Windows®)

BRAdmin Professional ユーティリティを使用するには、

- 最新版の BRAdmin Professional を使用する必要があります。 support.brother.co.jp にアクセスし、サポートサイト (ブラザーソリューションセンター) でご使用モデルの **ソフトウェアダウンロード** ページをご覧ください。
- BRAdmin Professional およびウェブブラウザを併せて使用する場合は、HTTPS プロトコルに対応しているウェブブラウザを使用します。
- BRAdmin Professional で新旧のサーバーが混合したグループを管理する場合は、グループごとに異なるパスワードを使用します。こうすることで、新しいプリントサーバーの安全性を確保できます。



- 「以前のバージョンの BRAdmin」は、Ver. 2.80 よりも前のバージョンの BRAdmin Professional および、Ver. 1.10 よりも前のバージョンの BRAdmin Light for Mac を指します。
- 「以前のバージョンのプリントサーバー」は、NC-2000 シリーズ、NC-2100p、NC-3100h、NC-3100s、NC-4100h、NC-5100h、NC-5200h、NC-6100h、NC-6200h、NC-6300h、NC-6400h、NC-8000、NC-100h、NC-110h、NC-120w、NC-130h、NC-140w、NC-8100h、NC-9100h、NC-7100w、NC-7200w および NC-2200w を指します。



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://brnxxxxxxxxxxxxx

NetBIOS 名は、ネットワーク設定リストで確認できます。

- Mac の場合、**ステータスマニター**画面に表示される本製品アイコンをクリックして、ウェブブラウザ経由でアクセスします。

3. お買い上げ時はパスワードは必要ありません。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。
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。
- 本ブラザー製品が IPsec 通信用に設定されている。
- 本ブラザー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. お買い上げ時はパスワードは必要ありません。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。
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	☐		
2	☐		
3	☐		
4	☐		
5	☐		
6	☐		
7	☐		
8	☐		
9	☐		
10	☐		

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. お買い上げ時はパスワードは必要ありません。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。
4. **ネットワーク**タブをクリックします。
5. **セキュリティ**タブをクリックします。
6. 左側にあるナビゲーションバーの **IPsec アドレステンプレート**メニューをクリックします。
10 個のアドレステンプレートが、テンプレートリストに表示されます。
削除ボタンをクリックして**アドレステンプレート**を削除します。**アドレステンプレート**が使用中の場合は、削除できません。
7. 作成したい**アドレステンプレート**をクリックします。**IPsec アドレステンプレート**が表示されます。



8. **テンプレート名**に、テンプレートの名前を入力します（最大 16 文字）。
9. **ローカル IP アドレス**を選択して、送信者の IP アドレス条件を指定します。
 - **IP アドレス**
IP アドレスを指定します。ドロップダウンリストから、**すべての IPv4 アドレス**、**すべての IPv6 アドレス**、**すべてのリンクローカル IPv6 アドレス**、または**カスタム**を選択します。
ドロップダウンリストから**カスタム**を選択した場合、テキストボックスに IP アドレス（IPv4 または IPv6）を入力します。
 - **IP アドレス範囲**
IP アドレス範囲の開始および終了アドレスを、各テキストボックスに入力します。開始および終了の IP アドレスが IPv4 または IPv6 に合わせて標準化されていない場合、または終了 IP アドレスが開始アドレスより小さい場合、エラーが発生します。

- **IP アドレス/プレフィックス**

CIDR 表記法で IP アドレスを指定します。

例 : 192.168.1.1/24

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

10. **リモート IP アドレス**を選択して、受信者の IP アドレス条件を指定します。

- **すべて**

すべてを選択すると、すべての IP アドレスが有効になります。

- **IP アドレス**

指定した IP アドレス (IPv4 または IPv6) をテキストボックスに入力します。

- **IP アドレス範囲**

IP アドレス範囲の開始および終了アドレスを入力します。開始および終了の IP アドレスが IPv4 または IPv6 に合わせて標準化されていない場合、または終了 IP アドレスが開始アドレスより小さい場合、エラーが発生します。

- **IP アドレス/プレフィックス**

CIDR 表記法で IP アドレスを指定します。

例 : 192.168.1.1/24

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

11. **OK** をクリックします。



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. お買い上げ時はパスワードは必要ありません。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。
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 の送信について

- ウェブブラウザ設定を使用して E-mail の送信を設定する
- ユーザー認証を使用した E-mail 送信について
- SSL/TLS を使用して安全な E-mail 送信を行う

ウェブブラウザ設定を使用して E-mail の送信を設定する

ユーザー認証を必要とする安全な E-mail 送信や、SSL/TLS を使用した E-mail 送信について、ウェブブラウザ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
3. お買い上げ時はパスワードは必要ありません。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。
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**プロトコルメニュー**をクリックします。
6. **SMTP** 欄で、**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. **SMTP** の設定値を設定します。
 - テストメールを送信して、E-mail の設定値が正しいことを確認します。
 - SMTP サーバーの設定値が不明の場合は、ネットワーク管理者またはインターネットサービスプロバイダー(ISP)にお問い合わせください。
8. 設定の完了後、**OK** をクリックします。
E メール送信設定テストダイアログボックスが表示されます。
9. ダイアログボックスに表示される指示に従って、設定のテストを行ってください。

✓ 関連情報

- [安全な E-mail の送信について](#)

ユーザー認証を使用した E-mail 送信について

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

E メール通知および E メールレポートに、SMTP-AUTH 方式を使用できます。



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、ウェブブラウザの **SMTP** 画面内で、**送信メールサーバー認証方式の SMTP-AUTH** を選択する必要があります。



関連情報

- [安全な E-mail の送信について](#)

SSL/TLS を使用して安全な E-mail 送信を行う

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



ウェブブラウザ設定を使用して 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	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	brnxxxxxxxxxxxx@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>>](#)

キャンセルOK



- 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。

ポート番号：

SSL を選択した場合、**ポート**の値がプロトコルに一致するよう変更されます。ポート番号を手動で変更する場合、**SSL/TLS** を選択後、ポート番号を入力します。

本製品の SMTP 通信方式を、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 ISP にお問い合わせください。

多くの場合、安全なウェブメールサービスには、以下の設定が必要です。

SMTP	ポート	25
	送信メールサーバー認証方式	SMTP-AUTH
	SSL/TLS	TLS

関連情報

- [安全な E-mail の送信について](#)

有線または無線 LAN への IEEE 802.1x 認証の使用について

- IEEE 802.1x 認証について
- ウェブブラウザ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。本ブラザー製品（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お問い合わせください。複数の証明書をインストールした場合、使用する証明書の名前を書き留めておくことをお勧めします。
- サーバー証明書を検証する前に、該当のサーバー証明書に署名した CA 発行の、CA 証明書をインポートする必要があります。ネットワーク管理者または契約しているインターネットサービスプロバイダー（ISP）にお問い合わせください。



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

- BAdmin Professional（有線または無線ネットワーク）
- 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）
- インストールディスクの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://brnxxxxxxxxxxxx

NetBIOS 名は、ネットワーク設定リストで確認できます。

- Mac の場合、**ステータスモニター**画面に表示される本製品アイコンをクリックして、ウェブブラウザ経由でアクセスします。

3. お買い上げ時はパスワードは必要ありません。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。
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を（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 が発行した、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。
オフ	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。

本ブラザー製品は、以下の内部認証方式をサポートしています。

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

EAP-MD5（有線 LAN）

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

PEAP

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

本ブラザー製品は、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。

本ブラザー製品は、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

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、本ブラザー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
- ウェブ接続印刷（サポート対象モデルのみ）



- 印刷ログ機能は、Kerberos 認証および NTLMv2 認証をサポートしています。認証のための SNTP プロトコル（ネットワークタイムサーバー）を設定する必要があります。
- ファイルをサーバーに保存する際に、ファイルタイプを TXT または CSV に設定できます。



関連情報

- [印刷ログ機能](#)

ウェブブラウザ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. お買い上げ時はパスワードは必要ありません。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。
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 (\\コンピューター名\共有フォルダ)。
ファイル名	印刷ログに使用するファイル名を入力します (最大 32 文字)。
ファイル形式	印刷ログのファイルタイプに、 テキスト形式 または CSV 形式 を選択します。
認証方法	CIFS サーバーにアクセスするために必要な認証方式として、自動、Kerberos、または NTLMv2 を選択します。Kerberos は認証プロトコルです。このプロトコルにより、機器または個人がそれぞれのアイデンティティーを、シングルサインオンを使用するネットワークサーバーに対して安全に示すことができます。NTLMv2 はサーバーにログインするための認証方式であり、Windows®により使用されます。 • 自動 : 自動を選択した場合、認証方式には NTLMv2 が使用されます。 • Kerberos : Kerberos を選択して、Kerberos 認証のみを使用します。 • NTLMv2 : NTLMv2 を選択して、NTLMv2 認証のみを使用します。  Kerberos および NTLMv2 認証の場合、SNTP プロトコル (ネットワークタイムサーバー) と DNS サーバーも設定する必要があります。
ユーザー名	認証のためのユーザー名を入力します (最大 96 文字)。  ユーザー名がドメインの一部である場合、ユーザー@ドメインまたは、ドメイン\ユーザーのいずれかの形式でユーザー名を入力します。
パスワード	認証のためのパスワードを入力します (最大 32 文字)。
Kerberos サーバーアドレス (必要に応じて)	KDC ホストのアドレス (例 : kerberos.example.com、最大 64 文字) または、IP アドレス (例 : 192.168.56.189) を入力します。
書き込みエラー時設定	ネットワークエラーのために印刷ログをサーバーに保存できない場合の対処方法を選択します。

8. **接続状態**欄で、最新のログステータスを確認します。



また、本製品の画面でエラー状態を確認することもできます。

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

設定をテストするには、**Yes** 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. お買い上げ時はパスワードは必要ありません。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。
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	印刷中止オプションを選択すると、印刷ログがサーバーに保存できない場合、印刷ジョブはキャンセルされます。
ログを書き込まずに印刷	ログを書き込まずに印刷を選択すると、印刷ログがサーバーに保存できない場合でも、本製品は文書を印刷します。 印刷ログ機能が回復すると、印刷ログは以下のように記録されます。 <pre>Id, Type, Job Name, User Name, Date, Time, Print Pages, Color Pages 1, Print (xxxxxxx), "Document01.doc", "user01", 03/03/20xx, 14:01:32, 52, 21 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, 4</pre> a b

a.

b.

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、**Yes** 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](#)

モバイル／ウェブ接続

- クラウド接続機能
- Google クラウド プリント
- AirPrint
- Windows®用モバイルプリント
- Mopria® Print Service
- Brother iPrint&Scan
- 近距離無線通信（NFC）

クラウド接続機能

- クラウド接続の概要
- クラウド接続機能を使用してアクセスできるオンラインサービス
- クラウド接続機能の使用条件について
- クラウド接続機能の設定
- 写真や文書をダウンロードして印刷する

クラウド接続の概要

ユーザーが画像やファイルをアップロードしたり、ウェブサイト上でそれらを閲覧するサービスを提供しているウェブサイトがあります。本製品では、このようなサービスにアップロードされている画像をダウンロードして印刷することができます。



1. 印刷
2. 写真、画像、文書などのファイル
3. Web サービス

クラウド接続機能を使用するには、有線接続または無線接続で、本製品をインターネットへアクセスできるネットワークに接続する必要があります。

プロキシサーバーを使用するネットワークのセットアップを行うには、本製品がプロキシサーバーを使用できるように設定する必要があります。ネットワーク設定方法について不明な場合は、ネットワーク管理者にお問い合わせください。



プロキシサーバーは、直接インターネットに接続していない複数のパソコンと、インターネットとの接続を仲介するコンピュータのことです。



関連情報

- [クラウド接続機能](#)

クラウド接続機能を使用してアクセスできるオンラインサービス

クラウド接続機能を使用して、お使いのブラザー製品からサービスにアクセスします。

Brother Web Connect 機能を使用するには、利用対象のオンラインサービスで使用するアカウントが必要です。アカウントをお持ちでない場合は、パソコンを使用してサービスのウェブサイトアクセスし、アカウントを作成します。

アカウントがある場合は、さらにアカウントを作成する必要はありません。

Google Drive™

オンラインの文書保存、編集、共有、およびファイルの同期サービスです。

URL: drive.google.com

Evernote®

オンラインのファイルストレージおよび管理サービスです。

URL: www.evernote.com

Dropbox

オンラインのファイルストレージ、共有、および同期サービスです。

URL: www.dropbox.com

OneDrive®

オンラインのファイルストレージ、共有、および管理サービスです。

URL: onedrive.live.com

Box

オンラインの文書編集・共有サービスです。

URL: www.box.com

OneNote®

オンラインの文書編集・共有サービスです。

URL: www.onenote.com

これらのサービスについて、詳しくは各サービスのウェブサイトを参照してください。

次の表は、クラウド接続機能で利用できるファイルの種類について説明しています。

アクセス可能なサービス	Google Drive™ Evernote® Dropbox OneDrive® Box OneNote®
画像のダウンロードと印刷	JPEG PDF DOCX XLSX PPTX ¹

¹ 画像は DOC/XLS/PPT 形式でもダウンロードまたは印刷できます。



関連情報

- クラウド接続機能

クラウド接続機能の使用条件について

- クラウド接続機能を使用するためにブラザーのソフトウェアをインストールする
- お使いのブラザー製品の操作パネルを使用してプロキシサーバーを設定する
- ウェブブラウザによる設定を使用してプロキシサーバーを設定する

クラウド接続機能を使用するためにブラザーのソフトウェアをインストールする

クラウド接続機能の最初のインストール時は、インターネットへのアクセスが可能なパソコンに、本製品の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。

Windows®の場合：

ソフトウェアをインストールして、有線または無線ネットワーク経由で印刷できるように設定する手順は、付属のかんたん設置ガイドをご覧ください。

Mac の場合：

ブラザーのソフトウェアをインストールするには、サポートサイト（ブラザーソリューションセンター）（support.brother.co.jp）にアクセスし、お使いのモデルのソフトウェアダウンロードページを参照します。



関連情報

- [クラウド接続機能の使用条件について](#)

お使いのブラウザ製品の操作パネルを使用してプロキシサーバーを設定する

ネットワークでプロキシサーバーを使用している場合、次のプロキシサーバーの情報を、お使いのブラウザ製品で設定する必要があります。

- プロキシサーバーのアドレス
- ポート番号
- ユーザー名
- パスワード

1.  [メニュー] > [全てのメニュー] > [ネットワーク] > [Web 接続設定] > [プロキシ設定] > [プロキシ経由接続] > [オン]を押します。
2. プロキシサーバー情報を押して、設定するオプションを入力します。
3.  を押します。

✓ 関連情報

- [クラウド接続機能の使用条件について](#)

ウェブブラウザによる設定を使用してプロキシサーバーを設定する

ネットワークでプロキシサーバーを使用している場合、次のプロキシサーバーの情報を、ウェブブラウザ上で設定する必要があります。

- プロキシサーバーのアドレス
- ポート番号
- ユーザー名
- パスワード



Windows®の場合は、Microsoft®Internet Explorer® 11 を、Mac の場合は、Safari 9 のブラウザのご使用をお勧めします。どのウェブブラウザの場合も、JavaScript および CSS を有効にして使用してください。

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. お買い上げ時はパスワードは必要ありません。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。
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**メニューをクリックします。
6. **プロキシ**のチェックボックスを選択し、**OK** をクリックします。
7. **プロキシ**欄で、**詳細設定**をクリックします。
8. プロキシサーバーの情報を入力します。
9. **OK** をクリックします。



関連情報

- [クラウド接続機能の使用条件について](#)

クラウド接続機能の設定

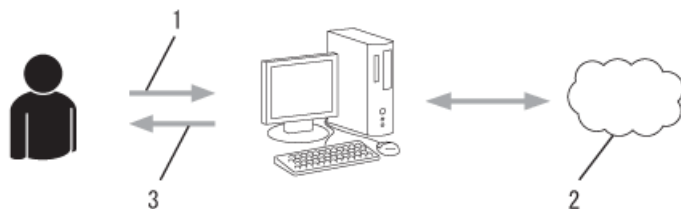
- クラウド接続機能設定の概要について
- クラウド接続機能を使用する前に、各オンラインサービスのアカウントを作成する
- クラウド接続機能の利用申請を行う
- お使いのブラザー製品に、クラウド接続機能を使用するためのアカウントを登録する

クラウド接続機能設定の概要について

下記の手順に従ってクラウド接続機能を設定します：

手順 1：利用するサービスのアカウントを作成する。

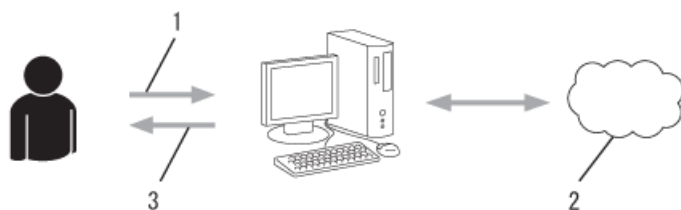
パソコンを使用してサービスのウェブサイトアクセスし、アカウントを作成します。（既にアカウントをお持ちの場合は、追加のアカウントを作成する必要はありません。）



1. ユーザー登録
2. Web サービス
3. アカウント取得

手順 2：クラウド接続機能の利用申請を行う

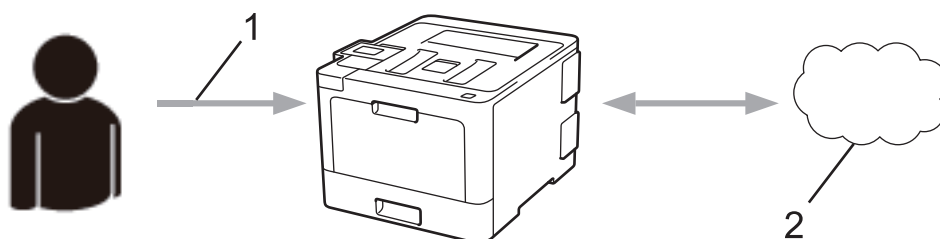
パソコンを使用してクラウド接続機能にアクセスし、仮登録 ID を取得します。



1. アカウント情報の入力
2. クラウド接続機能申請ページ
3. 仮登録 ID の取得

手順 3：利用対象のサービスにアクセスできるよう、本製品にアカウント情報を登録します。

本製品でサービスを利用できるように仮登録 ID を入力します。本製品で表示したいアカウント名を指定し、必要に応じて PIN コードを入力します。



1. 仮登録 ID の入力
2. Web サービス

お使いのブラザー製品で Web サービスを利用できます。

✓ 関連情報

- [クラウド接続機能の設定](#)

クラウド接続機能を使用する前に、各オンラインサービスのアカウントを作成する

クラウド接続機能を使用して Web サービスにアクセスするためには、利用するサービスのアカウントが必要です。アカウントをお持ちでない場合は、パソコンで利用したいサービスのウェブサイトアクセスし、アカウントを作成してください。アカウントの作成後、パソコンを使用してそのアカウントでログインしてからクラウド接続機能を使用します。作成したアカウントでログインしない場合、クラウド接続機能を使用してサービスにアクセスできないことがあります。

すでにアカウントをお持ちの場合、追加のアカウントを作成する必要はありません。

利用するオンラインサービスでアカウントを作成したら、クラウド接続機能へのアクセスを申請します。



ゲストユーザーとしてサービスを利用する場合は、アカウントを作成する必要はありません。ゲストユーザーとして利用できるサービスは限られています。利用するサービスにゲストオプションがない場合は、アカウントを作成する必要があります。



関連情報

- [クラウド接続機能の設定](#)

クラウド接続機能の利用申請を行う

クラウド接続機能を使用してオンラインサービスが利用できるように、ソフトウェアがインストールされているパソコンを使用して、クラウド接続ページにアクセスし、クラウド接続機能の利用申請を行います。

1. クラウド接続機能のウェブページにアクセスします：

オプション	説明
Windows® 7	 (スタート) > すべてのプログラム > Brother > Brother Utilities をクリックし、選択されていない場合は、ドロップダウンリストからお使いのモデル名を選択します。ナビゲーションバーの もっと活用する をクリックし、 Brother Web Connect をクリックします。
Windows® 8 Windows® 10	 (Brother Utilities) を起動し、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 もっと活用する をクリックし、 Brother Web Connect をクリックします。
Windows® 8.1	スタート画面の左下角にマウスを移動し、  をクリックします (タッチ操作のパソコンをお使いの場合は、スタート画面の下から上に向けてフリックし、 アプリ 画面を表示させます)。  (Brother Utilities) をクリックし、選択されていない場合は、ドロップダウンリストからお使いのモデル名を選択します。ナビゲーションバーの もっと活用する をクリックし、 Brother Web Connect をクリックします。
Mac	Finder メニューから 移動 を選び、 アプリケーション > Brother > Utilities > Brother Web Connect をクリックします。



ウェブサイトへ直接アクセスすることもできます。

お使いのウェブブラウザのアドレスバーに、bwc.brother.com と入力します。

クラウド接続機能のページが起動します。



初めてクラウド接続機能のウェブページを起動したときには、国、言語およびモデル名を選択してから、サービス画面へ移動するために、**Next** をクリックしてください。

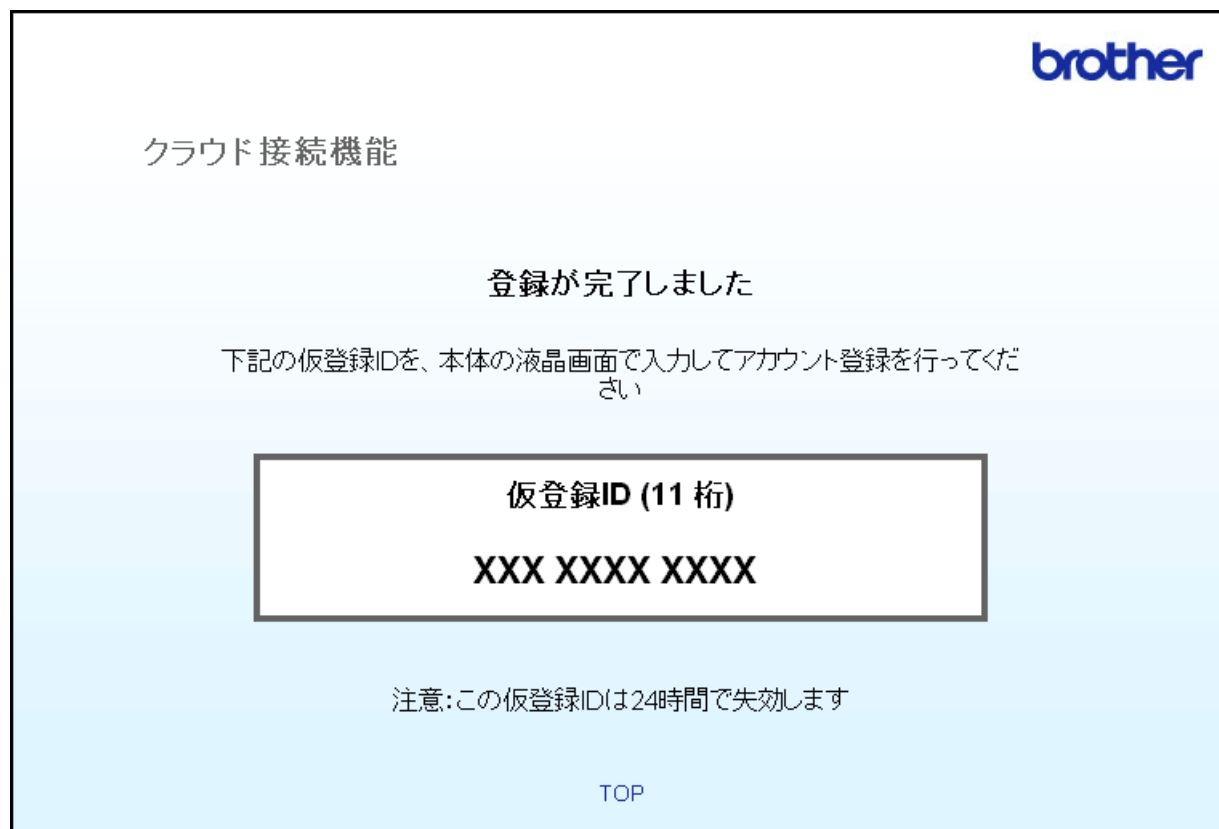
2. 利用するサービスを選択します。



実際に表示される画面は、上記と異なることがあります。

3. 画面の指示に従って、利用申請を行います。

申請が終了すると、仮登録 ID が表示されます。



4. 仮登録 ID をメモしておきます。この ID は、お使いのブラザー製品にアカウントを登録する際に必要となります。仮登録 ID は、24 時間有効です。
5. ウェブブラウザを閉じます。

次に、お使いのブラザー製品にアカウントを登録します。

関連情報

- [クラウド接続機能の設定](#)
 - [お使いのブラザー製品に、クラウド接続機能を使用するためのアカウントを登録する](#)
-

お使いのブラザー製品に、クラウド接続機能を使用するためのアカウントを登録する

クラウド接続機能を使用するために、お使いのブラザー製品にアカウント情報を入力し設定します。

- 利用するサービスのウェブサイトアクセスし、アカウントを作成してください。
- アカウントを登録する前に、本製品の日時が正しく設定されていることを確認します。

1. [印刷機能] > [クラウド] を押します。



- 本製品の画面にインターネット接続に関する情報が表示された場合、その情報をお読みにになり、[OK] を押してください。この情報を再表示する場合は、[はい] を押します。
- クラウド接続機能についての更新やお知らせが、画面に表示されることがあります。表示された情報をお読みにになり、[OK] を押します。

2. ライセンス 契約に関する情報が表示された場合は、同意の可否を選択して、画面の指示に従ってください。

3. ▲または▼を押して、登録するサービスを表示します。

4. サービス名を押します。

5. クラウド接続機能に関する情報が表示された場合、[OK] を押します。

6. [アカウントの登録／削除] を押します。

7. [アカウント登録] を押します。

クラウド接続機能の利用申請を行い、仮登録 ID を取得するように求めるメッセージが表示されます。

8. [OK] を押します。

9. 画面を使用して仮登録 ID を入力します。

10. [OK] を押します。

画面に表示させるアカウント名の入力を求めるメッセージが表示されます。

11. [OK] を押します。

12. 画面を使用して名前を入力します。

13. [OK] を押します。

14. 次のいずれかを行ってください。

- アカウントの PIN コードを設定する場合は、[はい] を押します。(PIN コードは、アカウントへの不正アクセスを防ぎます。) 4 桁の数字を入力し、[OK] を押します。
- PIN コードを設定しない場合は、[いいえ] を押します。

15. 入力したアカウント情報が表示されたら、正しく入力されていることを確認します。

16. [はい] を押して、入力した内容を登録します。



入力した情報が申請時に受け取った仮登録 ID と一致しない場合、または仮登録 ID の有効期限が切れている場合はエラーメッセージが画面に表示されます。正しい仮登録 ID を入力するか、再度申請を行って新しい仮登録 ID を取得します。

17. [OK] を押します。

18.  を押します。

登録が完了し、本製品がサービスにアクセスできるようになりました。



関連情報

- [クラウド接続機能の設定](#)

-
- クラウド接続機能の利用申請を行う
-

写真や文書をダウンロードして印刷する

Web サービスにアップロードされている写真や文書を、本製品に直接ダウンロードして印刷することができます。他のユーザーがアップロードした共有画像は、閲覧権限を持っていれば本製品にダウンロードして印刷することができます。ゲストユーザーでも公開されている画像を見ることができるサービスもあります。ゲストユーザーとしてアクセスすると、所有者が一般公開している閲覧制限が無い画像などを見ることができます。

他のユーザーの文書をダウンロードするには、該当のアルバムや文書を閲覧するためのアクセス権限が必要となります。

セキュリティ機能ロック（特定のモデルのみ可能）によりクラウド接続機能をご利用できないユーザーの場合は、データをダウンロードできません。

セキュリティ機能ロック（特定のモデルのみ可能）で印刷枚数を制限している場合、Web サービス上の文書の印刷も制限対象になります。

✓ 関連情報

- [クラウド接続機能](#)
- [Web サービスを使用してダウンロードや印刷を行う](#)

Web サービスを使用してダウンロードや印刷を行う

1. [印刷機能] > [クラウド]を押します。



- 本製品の画面にインターネット接続に関する情報が表示された場合、その情報をお読みにになり、[OK]を押してください。この情報を再表示する場合は、[はい]を押します。
- クラウド接続機能についての更新やお知らせが、画面に表示されることがあります。表示された情報をお読みにになり、[OK]を押します。

2. ▲または▼を押して、ダウンロードと印刷対象の文書を保持しているサービスを表示します。サービス名を押します。
3. サービスにログオンするには、▲または▼を押してお使いのアカウント名を表示し、表示されたアカウント名を押します。PIN 入力画面が表示された場合は、4桁のPINを入力して、[OK]を押します。
4. ▲または▼を押して使用するフォルダを表示し、表示されたフォルダを押します。フォルダに文書を保存する必要のないサービスもあります。フォルダに保存されていない文書の場合、[未分類のファイルを表示]を選択し、文書を選択します。他のユーザーの文書の場合は、フォルダに保存されていなければダウンロードできません。
5. 印刷する文書のサムネイルを押します。画面に表示された文書を確認し、[OK]を押します。次の印刷文書を選択します（最大 10 個の文書を選択できます）。
6. 入力後、[OK]を押します。
7. 画面の指示に従って、この操作を完了します。



関連情報

- [写真や文書をダウンロードして印刷する](#)

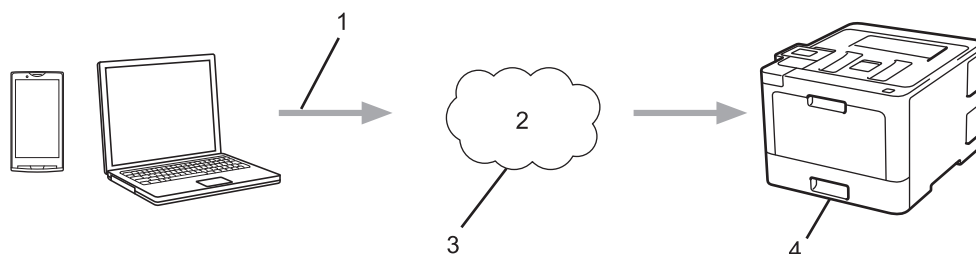
Google クラウド プリント

- Google クラウド プリントの概要
- Google クラウド プリントを使用する前に
- Google Chrome™、または Chrome OS™から印刷する
- モバイル向けの Google Drive™から印刷する
- モバイル向けの Gmail™ウェブメールサービスから印刷する

Google クラウド プリントの概要

Google クラウド プリント™ は、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（携帯電話やパソコンなど）を使用して、Google アカウントに登録されたプリンターで印刷できる Google サービスです。

Android™アプリケーションを使って印刷するためには、Google Play™ストアから Google クラウド プリントアプリケーションをインストールする必要があります。



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

- [Google クラウド プリント](#)

Google クラウド プリントを使用する前に

- Google クラウド プリントを使用するためのネットワーク設定
- Google Chrome™を使用して Google クラウド プリントに本製品を登録する
- ウェブブラウザを使用して Google クラウド プリントに本製品を登録する

Google クラウド プリントを使用するためのネットワーク設定

Google クラウド プリントを使うには、お使いのブラザー製品が、有線または無線接続でインターネットにアクセスしている必要があります。お使いのブラザー製品を正しく接続し、設定するには、かんたん設置ガイドをご覧ください。または本ガイドの関連するトピックをご覧ください。



関連情報

- [Google クラウド プリントを使用する前に](#)
- [Google クラウド プリントの問題](#)

Google Chrome™ を使用して Google クラウド プリントに本製品を登録する

Google アカウントをすでに作成していることを確認します。アカウントをお持ちでない場合は、パソコンまたは携帯端末を使用して Google のウェブサイト (<https://accounts.google.com/signup>) にアクセスし、アカウントを作成します。

登録作業を始める前に、本ブラザー製品が待ち受け状態になっていることを確認してください。



ここで説明している手順は、Windows ユーザー向けの参考例です。
お使いの OS や環境によって、実際の画面と異なることがあります。

1. パソコンで Google Chrome™ を開きます。
2. Google アカウントにサインインします。
3. Google Chrome™ のメニューアイコンをクリックし、**設定 > 詳細設定を表示**をクリックします。
4. **Google クラウド プリント**の項目で、**管理**をクリックします。
5. 画面の指示に従ってお使いの製品を登録します。
6. お使いの製品で確認メッセージが表示されたら、OK ボタンを押します。



お使いの製品の画面に確認メッセージが表示されない場合は、これらの手順を繰り返してください。

7. 製品が正常に登録されると、**マイ デバイス**の項目にお使いの製品が表示されます。



関連情報

- [Google クラウド プリントを使用する前に](#)

ウェブブラウザを使用して Google クラウド プリントに本製品を登録する

Google™ アカウントを作成済みであることを確認してください。アカウントをお持ちでない場合は、パソコンまたは携帯端末を使用して Google™ のウェブサイト (<https://accounts.google.com/signup>) にアクセスし、アカウントを作成します。

登録作業を始める前に、本ブラウザ製品が待ち受け画面になっていることを確認してください。

本製品の登録を開始する前に、本製品の日時が正しく設定されていることを確認します。

1. 本ブラウザ製品が、お使いのパソコンまたは携帯端末と同一のネットワークに接続していることを確認してください。
2. ウェブブラウザを起動します。
3. 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
4. お買い上げ時はパスワードは必要ありません。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。
5. **ネットワーク**タブをクリックします。
6. 左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。
7. **Google クラウド プリント**が選択されていることを確認し、**詳細設定**をクリックします。
8. **状態が有効**に設定されていることを確認します。**登録**をクリックします。
9. 画面の指示に従って本製品を登録します。
10. 本製品に確認メッセージが表示されたら、OK ボタンを押します。



本製品の画面に確認メッセージが表示されない場合は、これらの手順を繰り返してください。

11. **Google** をクリックします。
12. Google クラウド プリントのサインイン画面が表示されます。Google™ アカウントでサインインし、画面の指示に従って本製品を登録します。
13. 本製品の登録が完了したら、ウェブブラウザによる設定画面に戻り、**登録状態が登録済み**に設定されていることを確認します。



お使いの製品が、セキュリティ機能ロックを使用して各ユーザーの PC プリントを制限している場合でも、Google クラウド プリントを利用して印刷することができます。Google クラウド プリントでの印刷を無効にしたい場合は、ウェブブラウザを使用して Google クラウド プリントを無効にするか、セキュリティ機能ロックを一般モードに設定して、一般モードユーザーの PC プリントを制限するかしてください。関連情報をご覧ください。



関連情報

- [Google クラウド プリントを使用する前に](#)
- [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](#)

Google Chrome™、または Chrome OS™ から印刷する

1. 本ブラザー製品の電源が入っていることを確認します。
2. 印刷したいウェブページを開きます。
3. Google Chrome™ のメニューアイコンをクリックします。
4. **印刷**をクリックします。
5. プリンター一覧からお使いの製品を選択します。
6. 必要に応じて印刷オプションを変更します。
7. **印刷**をクリックします。



関連情報

- [Google クラウド プリント](#)

モバイル向けの Google Drive™ から印刷する

1. 本ブラザー製品の電源が入っていることを確認します。
2. お使いの Android™ 機器、または Apple 機器のウェブブラウザから Google Drive™ にアクセスします。
3. 印刷したい文書を開きます。
4. メニューアイコンをタップします。
5. **印刷**をタップします。
6. プリンター一覧からお使いの製品を選択します。
7. 必要に応じて印刷オプションを変更します。
8.  または **印刷**をタップします。

関連情報

- [Google クラウド プリント](#)

モバイル向けの Gmail™ウェブメールサービスから印刷する

1. 本ブラザー製品の電源が入っていることを確認します。
2. お使いの Android™機器、または Apple 機器のウェブブラウザから Gmail™ウェブメールサービスにアクセスします。
3. 印刷したい E メールを開きます。
4. メニューアイコンをタップします。



添付ファイル名のそばに**印刷**と表示されている場合は、添付ファイルを印刷することができます。**印刷**をタップし、お使いの携帯端末の指示に従います。

5. **印刷**をタップします。
6. プリンター一覧からお使いの製品を選択します。
7. 必要に応じて印刷オプションを変更します。
8.  または **印刷**をタップします。



関連情報

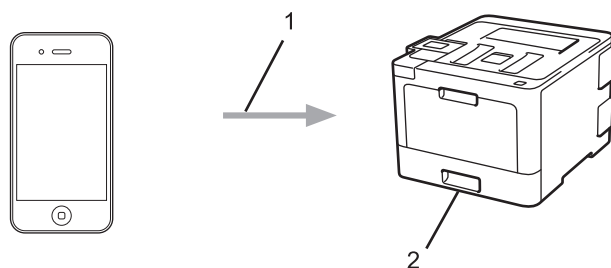
- [Google クラウド プリント](#)

AirPrint

- [AirPrint の概要](#)
- [はじめに](#)
- [AirPrint を使用して印刷する](#)

AirPrint の概要

Brother AirPrint を使用して、写真、E メール、ウェブページ、および文書を、プリンタドライバをインストールせずに、iPad、iPhone、iPod touch から無線で印刷します。



1. 印刷要求
2. 印刷された写真、E メール、ウェブページ、および文書



関連情報

- [AirPrint](#)
- [AirPrint の問題](#)

はじめに

- AirPrint を使用するためのネットワーク設定
- ウェブブラウザによる設定で無効または有効にする

AirPrint を使用するためのネットワーク設定

AirPrint を使用するためには、お使いの携帯端末をブラザー製品が接続されている無線ネットワークに接続する必要があります。AirPrint は、インフラストラクチャモードまたは Wi-Fi Direct[®]を用いた無線接続に対応しています。

携帯端末の無線ネットワーク設定については、お使いの携帯端末のユーザズガイドを参照してください。

Safari 内の  をタップすることで、Apple 社のウェブサイトで、お使いの携帯端末のユーザズガイドにアクセスすることができます。

お使いのブラザー製品の無線ネットワーク設定については、かんたん設置ガイドをご覧ください。または本ガイドの関連するトピックをご覧ください。お使いの製品が有線 LAN に対応している場合は、ネットワークケーブルを無線 LAN アクセスポイントまたはルーターに接続して使用することもできます。

お使いのブラザー製品が Wi-Fi Direct[®]に対応していて、Wi-Fi Direct[®]ネットワーク用に設定をしたい場合は、本ガイドの関連するトピックをご覧ください。

✓ 関連情報

- [はじめに](#)
- [AirPrint の問題](#)

ウェブブラウザによる設定で無効または有効にする

本製品が、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ることを確認します。

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. お買い上げ時はパスワードは必要ありません。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。
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**メニューをクリックします。
6. AirPrint を無効にするには、**AirPrint** チェックボックスの選択を外します。AirPrint を有効にするには、**AirPrint** チェックボックスを選択します。



お買い上げ時の設定では、AirPrint は有効です。

7. **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。



関連情報

- [はじめに](#)

AirPrint を使用して印刷する

- iPad、iPhone、または iPod Touch から印刷する
- AirPrint を使用して印刷を行う前に（macOS）
- AirPrint を使用して印刷を行う（macOS）

iPad、iPhone、または iPod Touch から印刷する

印刷の手順は、アプリケーションによって異なります。ここでは、Safari で閲覧しているウェブページの印刷手順を例にして説明します。

1. 本製品の電源が入っていることを確認します。
2. Safari で印刷したいウェブページを開きます。
3.  または  をタップします。
4. **プリント** をタップします。
5. 本製品が選択されていることを確認します。
6. 別の製品が選択されている場合や、プリンターが選択されていない場合は、**プリンタ** をタップします。
利用可能な製品の一覧が表示されます。
7. 一覧から本製品をタップします。
8. 印刷枚数や両面印刷（本製品が対応している場合）などを必要に応じて設定します。
9. **プリント** をタップします。



関連情報

- [AirPrint を使用して印刷する](#)

AirPrint を使用して印刷を行う前に (macOS)

macOS を使用して印刷を行う前に、本製品を Mac パソコンのプリンターリストへ追加してください。

1. アップルメニューから**システム環境設定**を選びます。
2. **プリントとスキャン** または **プリンタとスキャナ** をクリックします。
3. 画面左側のプリンターリストの下にある + アイコンをクリックします。
4. **プリンタまたはスキャナを追加…** をクリックします。追加画面が表示されます。
5. 本製品を選び、**ドライバ** のポップアップメニューから **AirPrint** を選びます。
6. **追加** をクリックします。



関連情報

- [AirPrint を使用して印刷する](#)

AirPrint を使用して印刷を行う (macOS)

印刷の手順は、アプリケーションによって異なります。ここでは、Safari で閲覧しているウェブページの印刷手順を例にして説明します。印刷する前に、Mac のプリンターリストに本製品が追加されていることを確認してください。

1. 本製品の電源が入っていることを確認します。
2. Mac の Safari で印刷したいウェブページを開きます。
3. **ファイル**をクリックして、**プリント**を選択します。
4. 本製品が選択されていることを確認します。別の製品が選択されている場合や、プリンターが選択されていない場合は、**プリンタ**のポップアップメニューをクリックし、本製品を選択します。
5. 印刷枚数や両面印刷（本製品が対応している場合）などを必要に応じて設定します。
6. **プリント**をクリックします。

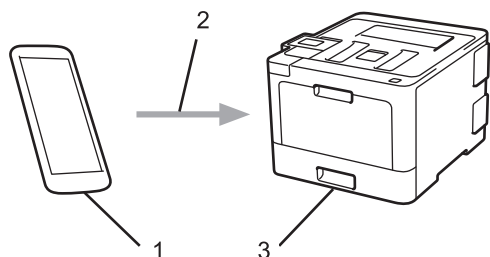


関連情報

- [AirPrint を使用して印刷する](#)

Windows®用モバイルプリント

Windows®用モバイルプリントは、お持ちの Windows®の携帯端末からワイヤレスで印刷することができる機能です。ブラザー製品が接続されているネットワークに接続し、携帯端末にプリンタドライバをインストールすることなく印刷することができます。この機能は多くの Windows®アプリでサポートされています。



1. Windows®の携帯端末（Windows® 10 Mobile 以降）
2. Wi-Fi®接続
3. 本ブラザー製品

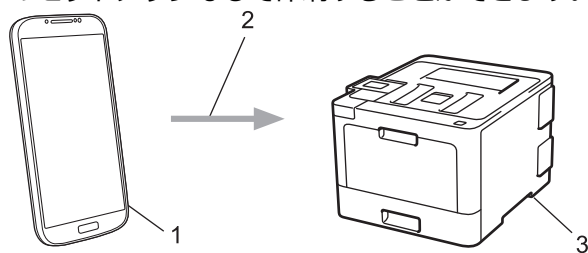


関連情報

- [モバイル／ウェブ接続](#)

Mopria® Print Service

Mopria® Print Service は、Android™ 携帯端末（Android™ バージョン 4.4 以降）の印刷サービスであり、Mopria® Alliance 社により開発されました。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。多くのネイティブ Android™ アプリが、印刷に対応しています。



1. Android™ 4.4 以降
2. Wi-Fi®接続
3. 本製品

Google Play™ ストアから Mopria® Print Service をダウンロードし、お使いの Android™ 機器にインストールする必要があります。本サービスをお使いになる前にアプリを起動してください。

✓ 関連情報

- [モバイル／ウェブ接続](#)

Brother iPrint&Scan

Brother iPrint&Scan 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

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

Google Play™ ストアアプリから、Brother iPrint&Scan をダウンロードして、インストールします。

- Apple 機器の場合

Brother iPrint&Scan を使用すると、お使いの Apple 機器から本製品の機能を直接使用することができます。

App Store から、Brother iPrint&Scan をダウンロードして、インストールします。

- Windows® 機器の場合

Brother iPrint&Scan を使用すると、お使いの Windows® 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。

Microsoft® Store から、Brother iPrint&Scan をダウンロードして、インストールします。

詳しい説明はモバイルプリント&スキャンガイド *Brother iPrint&Scan* 用をご覧ください。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）にアクセスし、お使いのモデルの**製品マニュアル**ページを参照します。



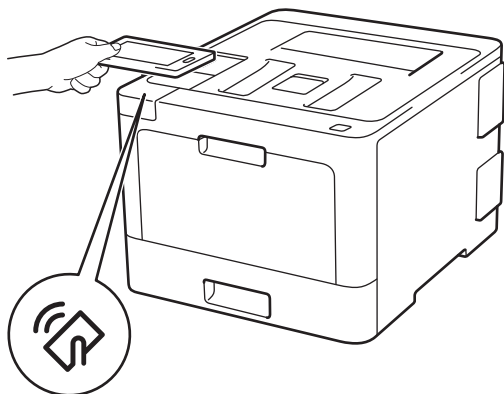
関連情報

- [モバイル／ウェブ接続](#)

近距離無線通信（NFC）

近距離無線通信（NFC）を使用すると、至近距離にある 2 つの機器間で、簡単な処理、データ交換、および無線通信を行うことができます。

お使いの Android™ 機器が NFC に対応している場合、本製品の操作パネルの NFC タッチ部分に機器をタッチすると、データ（写真、PDF ファイル、テキストファイル、ウェブページ、E メールメッセージ）を印刷することができます。



この機能を使用するには、お使いの Android™ 機器に Brother iPrint&Scan をダウンロードしてインストールする必要があります。詳しい説明はモバイルプリント＆スキャンガイド *Brother iPrint&Scan* 用をご覧ください。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）にアクセスし、お使いのモデルの製品マニュアルページを参照します。



関連情報

- [モバイル／ウェブ接続](#)
- [外付け IC カードリーダーに登録する](#)

外付け IC カードリーダーに登録する

外付け IC カードリーダーを接続する場合、ウェブブラウザでカードリーダーに登録してください。本製品は外付け IC カードリーダーに対応する HID クラスのドライバーをサポートしています。

1. ウェブブラウザを起動します。
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. お買い上げ時はパスワードは必要ありません。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。
4. **管理者設定**タブをクリックします。
5. **外付けカードリーダー**メニューをクリックして、必要な情報を入力します。
6. **OK** をクリックします。
7. 本ブラザー製品を再起動して、設定を有効にします。

関連情報

- [近距離無線通信（NFC）](#)

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
- 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

▲ ホーム > 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 > 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 を、Mac の場合は、Safari 9 のブラウザのご使用をお勧めします。どのウェブブラウザの場合も、JavaScript および CSS を有効にして使用してください。
- ネットワーク上で TCP/IP プロトコルを使用する必要があり、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。



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://brnxxxxxxxxxxxxx

NetBIOS 名は、ネットワーク設定リストで確認できます。

- Mac の場合、**ステータスモニター**画面に表示される本製品アイコンをクリックして、ウェブブラウザ経由でアクセスします。

3. お買い上げ時はパスワードは必要ありません。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。

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](#)
- [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://brnxxxxxxxxxxxxx

NetBIOS 名は、ネットワーク設定リストで確認できます。

- Mac の場合、**ステータスモニター**画面に表示される本製品アイコンをクリックして、ウェブブラウザ経由でアクセスします。

3. お買い上げ時はパスワードは必要ありません。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。
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。



事前にパスワードを設定していない場合、本製品のウェブページの**パスワードを設定してください**ボタンをクリックしてパスワードを設定することもできます。



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](#)



本製品は日本国内のみでのご使用となりますので、海外でのご使用はお止めください。海外で使用されている電源が本製品に適切ではない恐れがあります。海外で本製品をご使用になりトラブルが発生した場合、当社は一切の責任を負いかねます。また、保証の対象とはなりませんのでご注意ください。

These machines are made for use in Japan only. We can not recommend using them overseas because the power requirements of your machine may not be compatible with the power available in foreign countries. Using Japan models overseas is at your own risk and will void your warranty.

