EPSON

DS-790WN

システム管理者ガイド

NPD6726-05 JA

マニュアルのご注意

- 本書の内容の一部または全部を無断転載することを禁止します。
- 本書の内容は将来予告なしに変更することがあります。
- 本書の内容にご不明な点や誤り、記載漏れなど、お気付きの点がありましたら弊社までご連絡ください。
- 運用した結果の影響については前項に関わらず責任を負いかねますのでご了承ください。
- 本製品が、本書の記載に従わずに取り扱われたり、不適当に使用されたり、弊社および弊社指定以外の、第三者によって修理や変更されたことなどに起因して生じた障害等の責任は負いかねますのでご了承ください。

商標

- EPSON、EPSON EXCEED YOUR VISION、EXCEED YOUR VISION およびそのロゴはセイコーエプソン株式会社の登録商標です。
- Microsoft、Windows、およびWindows Serverは、米国Microsoft Corporationの米国およびその他の国における登録商標です。
- Apple、Mac、macOS、OS X、Bonjour、Safari、AirPrintは米国およびその他の国で登録されたApple Inc.の商標です。
- ChromeはGoogle LLCの商標です。
- AOSS™は株式会社バッファローの商標です。
- SuperSpeed USB Tridentロゴは、USB Implementers Forum, Inc.の登録商標です。
- Firefox is a trademark of the Mozilla Foundation in the U.S. and other countries.
- FeliCa（フェリカ）およびPaSoRi（パソリ）は、ソニー株式会社の登録商標です。
- MIFAREは、NXPセミコンダクター社の登録商標です。
- 通則：その他の製品名は各社の商標または登録商標です。それらの商標について、エプソンはいかなる権利も有しません。

目次

はじめに

本書について

本書は、スキャナー管理者向けに以下の情報を説明しています。

- ネットワークの設定
- スキャン機能の準備
- セキュリティーの有効化・管理
- 認証設定の有効化・管理
- 日常のメンテナンス方法

本書に記載されていないスキャナーの使い方については、『ユーザーズガイド』をご覧ください。

参考 本書では、認証サーバーがなくても、スキャナーだけで使用できる認証設定を説明しています。本書で案内している認証設定以外にも、認証用のサーバーを利用した認証システムを構築できます。構築には、Document Capture Pro Server Authentication Edition（略称：Document Capture Pro Server AE）が必要です。
詳しくは、エプソンの問い合わせ窓口にお問い合わせください。

マニュアルの見方

マークの意味

⚠注意 この内容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および財産の損害の可能性が想定される内容を示しています。

!重要 必ず守っていただきたい内容を記載しています。この内容を無視して誤った取り扱いをすると、製品の故障や、動作不良の原因になる可能性があります。

参考 補足情報や参考情報を記載しています。

関連情報

➡ 関連したページにジャンプします。

マニュアル記載の前提

- ソフトウェアの画面は、Windows 10またはmacOS High Sierraでの表示画面を使用しています。表示内容は機種や状況によって異なります。
- 本書で使われているイラストは一例です。機種によって多少異なりますが操作方法は同じです。

OS表記

Windows

本書では、以下のOS（オペレーティングシステム）をそれぞれ「Windows 10」「Windows 8.1」「Windows 8」「Windows 7」「Windows Server 2019」「Windows Server 2016」「Windows Server 2012 R2」「Windows Server 2012」「Windows Server 2008 R2」と表記しています。また、これらの総称として「Windows」を使用しており、「Windows Server 2019」「Windows Server 2016」「Windows Server 2012 R2」「Windows Server 2012」「Windows Server 2008 R2」の総称として「Windows Server」を使用しています。

- Microsoft® Windows® 10 operating system日本語版
- Microsoft® Windows® 8.1 operating system日本語版
- Microsoft® Windows® 8 operating system日本語版
- Microsoft® Windows® 7 operating system日本語版
- Microsoft® Windows Server® 2019 operating system日本語版
- Microsoft® Windows Server® 2016 operating system日本語版
- Microsoft® Windows Server® 2012 R2 operating system日本語版
- Microsoft® Windows Server® 2012 operating system日本語版
- Microsoft® Windows Server® 2008 R2 operating system日本語版

Mac OS

本書では、「macOS Big Sur」「macOS Catalina」「macOS Mojave」「macOS High Sierra」「macOS Sierra」「OS X El Capitan」「OS X Yosemite」の総称として「Mac OS」を使用しています。

目的別の必要な設定

目的別の必要な設定

以下を参考に、目的別に必要な設定を行ってください。

スキャナーをネットワークに接続する

目的	必要な設定
スキャナーをネットワークに接続したい	スキャナーをネットワークに接続します。 「スキャナーをネットワークに接続する」14ページ
スキャナーを新しいコンピューターに接続したい	新しいコンピューターにスキャナーのネットワーク設定をします。 「コンピューターや機器の追加や交換をしたときは」20ページ

スキャンの設定をする

目的	必要な設定
スキャンした画像をメールで送信したい （スキャン to メール 機能）	1.連携するメールサーバーを設定します。 「メールサーバーを登録する」41ページ 2.送信先のメールアドレスを［アドレス帳］に登録します（任意）。送信するたびにメールアドレスを入力しなくても、アドレス帳から選択するだけで送信できるようになります。 「アドレス帳を使えるようにする」64ページ
スキャンした画像を、ネットワーク上のフォルダーに保存したい （スキャン to ネットワークフォルダー 機能）	1.ネットワーク上に、画像を保存するフォルダーを作成します。 「共有フォルダーを設定する」46ページ 2.フォルダーのパスを［アドレス帳］に登録します（任意）。保存するたびにフォルダーパスを入力しなくても、アドレス帳から選択するだけで保存できるようになります。 「アドレス帳を使えるようにする」64ページ
クラウドサービスを使用して画像を保存したい （スキャン to クラウド 機能）	Epson Connectの設定を行います。Epson Connectのポータルサイトを参照して、セットアップをしてください。 設定の際は、連携するオンラインストレージサービスのユーザーアカウントが必要です。 https://www.epsonconnect.com/

操作パネルをカスタマイズする

目的	必要な設定
スキャナーの操作パネルに表示される項目を変更したい	［お気に入り］または［ホーム画面編集］の設定をします。操作パネルにお気に入りのスキャン設定を登録したり、表示される項目を編集したりできます。 「操作パネルをカスタマイズする」80ページ

基本的なセキュリティー機能を設定する

目的	必要な設定
管理者以外にスキャナーの設定を変更されないようにしたい	スキャナーに管理者パスワードを設定します。 「管理者設定」89ページ
USB接続でスキャナーを使用できないようにしたい	外部インターフェイスを無効にします。 「外部インターフェイスを無効にする」95ページ

高度なセキュリティー機能を設定する

目的	必要な設定
利用するプロトコルを制御したい	プロトコルの有効・無効を設定します。 「利用するプロトコルを制御する」101ページ
通信経路を暗号化したい	1.電子証明書を設定します。 「電子証明書を使う」104ページ 2.SSL/TLS通信を設定します。 「スキャナーとのSSL/TLS通信」109ページ
暗号化通信を利用したい（IPsec） 特定のコンピューターからだけ使用できるようにしたい（IPフィルタリング）	フィルタリングのためにポリシーを設定します。 「IPsec/IPフィルタリングで暗号化通信する」110ページ
IEEE802.1X環境でスキャナーを利用したい	スキャナーにIEEE802.1Xを設定します。 「IEEE802.1X環境にスキャナーを接続する」122ページ

スキャナー本体で認証する機能を設定する

目的	必要な設定
認証設定を有効にしたい	利用できる認証設定と認証方式の概要について、以下をご覧ください。 「認証設定について」131ページ 「認証方式の概要」132ページ

サーバーで認証システムを利用する

Document Capture Pro Server Authentication Edition（略称：Document Capture Pro Server AE）を使うと、認証用のサーバーを利用した認証システムを構築できます。
詳しくは、エプソンの問い合わせ窓口にお問い合わせください。

ネットワーク設定

スキャナーをネットワークに接続する

スキャナーの操作パネルを使って、スキャナーをネットワークに接続する手順を説明します。

参考 スキャナーとコンピューターが同じセグメントにあるときは、インストーラーを使っても接続できます。

- ウェブサイトから起動する
  以下のウェブサイトへアクセスし、製品名を入力してください。［セットアップ］に進んで作業を開始します。
  http://epson.sn
- ソフトウェアディスクを使って設定する（ソフトウェアディスクが同梱されている機種で、お使いのコンピューターがディスクドライブを搭載したWindowsの場合）
  コンピューターにソフトウェアディスクを挿入し、画面の指示に従ってください。

ネットワーク接続の前に

ネットワーク接続するには、接続方法と接続のための設定情報を事前に確認してください。

接続設定情報の収集

接続に必要な設定情報を用意します。事前に以下の情報を確認してください。

区分	項目	参考
デバイス接続方法	• 有線LAN • 無線LAN（Wi-Fi）	スキャナーをネットワークに接続する方法を決定します。 有線LANは、LANスイッチ（ハブ）に接続します。 無線LANはアクセスポイントのSSIDに接続します。
LAN接続情報	• IPアドレス • サブネットマスク • デフォルトゲートウェイ	スキャナーに割り当てるIPアドレスを決定します。 静的にIPアドレスを割り当てる場合は、全ての項目の値が必要です。 DHCP機能で動的にIPアドレスを割り当てる場合は、自動設定されるのでLAN接続の情報は不要です。
Wi-Fi接続情報	• SSID • パスワード	スキャナーを接続するアクセスポイントのSSID（ネットワークの名称）、パスワードです。 MACアドレスフィルタリング設定がされている場合は、スキャナーを登録できるように事前にMACアドレスの登録をしておいてください。 対応している規格は以下をご覧ください。 「ネットワークの仕様」27ページ
DNSサーバー情報	• プライマリーDNSのIPアドレス • セカンダリーDNSのIPアドレス	DNSサーバーを指定する場合に必要です。セカンダリーDNSはシステムを冗長構成にしてセカンダリーDNSサーバーがある場合に設定します。 小規模なネットワークでDNSサーバーを構築していない場合は、ルーターのIPアドレスを設定します。

区分	項目	参考
プロキシサーバー情報	• プロキシサーバー名	イントラネットからインターネットへの接続にプロキシサーバーを利用しているネットワーク環境において、スキャナーが直接インターネットにアクセスする機能を使用する場合は設定してください。 以下のような機能はスキャナーが直接インターネットにアクセスします。 • Epson Connectサービス • 他社のクラウドサービス • ファームウェア更新 • スキャンした画像をSharePoint(WebDAV)に送る
ポート番号情報	• 開放するポート番号	スキャナーやコンピューターが各機能で使用するポート番号を確認して、ファイアウォールでブロックされているポートを、必要に応じて開放してください。 スキャナーが使用するポート番号の情報は以下をご覧ください。 「スキャナーが使用するポート」29ページ

IPアドレスの割り当て

IPアドレス（IPv4）の割り当てには、以下のタイプがあります。

固定IPアドレス：

あらかじめ決めたIPアドレスを手動でスキャナー（ホスト）に割り当てます。
ネットワークに接続するための情報（サブネットマスク、デフォルトゲートウェイ、DNSサーバー設定など）を手動で設定する必要があります。
デバイスの電源を切ってもIPアドレスは変更されないので、IPアドレスの変更を追従できない環境やIPアドレスでデバイスを管理したい場合に利用できます。多数のコンピューターがアクセスする、スキャナーやサーバーなどへの設定をお勧めします。また、IPsec／IPフィルタリングなどのセキュリティー機能を利用する場合は、IPアドレスが変更されないよう固定IPアドレスを割り当ててください。

DHCP機能による自動割り当て（動的IPアドレス）：

DHCPサーバーやルーターのDHCP機能を使って自動でIPアドレスをスキャナー（ホスト）に割り当てます。
ネットワークに接続するための情報（サブネットマスク、デフォルトゲートウェイ、DNSサーバー設定など）も自動で設定されるので、デバイスのネットワークへの接続が容易にできます。
デバイスやルーターの電源を切る、または、DHCPサーバーの設定により、再接続の際にIPアドレスが変更になる場合があります。
IPアドレス以外でのデバイス管理やIPアドレスを追従できるプロトコルでの通信をお勧めします。

参考 DHCPのIPアドレス予約機能を使用すると、常にデバイスに同じIPアドレスを割り当てることができます。

DNSサーバー、プロキシサーバーについて

DNSサーバーは、ホスト名やメールアドレスのドメイン名などとIPアドレスの情報を関連付けて持っています。
コンピューターやスキャナーがIP通信をするときに、ホスト名やドメイン名などで相手先を記述すると通信ができません。
その情報をDNSサーバーに問い合わせ、相手先のIPアドレスを取得します。この処理を名前解決と言います。

これによりコンピューターやスキャナーなどのデバイスは、IPアドレスを使って通信ができるようになります。
スキャナーがメールを使ったり、インターネット接続をして通信したりするには、名前解決が必要です。
これらの機能を使用するには、DNSサーバーの設定をしてください。
スキャナーのIPアドレスをDHCPサーバーやルーターのDHCP機能で割り当てる場合は自動設定されます。
プロキシサーバーはネットワークとインターネットとの出入口に配置され、コンピューターやスキャナーとインターネット（相手サーバー）の代理でそれぞれのデバイスと通信します。相手側のサーバーはプロキシサーバーのみと通信します。よって、スキャナーに設定されているIPアドレスやポート番号などの情報を読み取れなくなり、セキュリティーの向上が期待できます。
プロキシサーバーを介してインターネット接続をしている場合は、スキャナーにプロキシサーバーの設定をしてください。

操作パネルでネットワークに接続する

スキャナーの操作パネルを使って、スキャナーをネットワークに接続します。

IPアドレスを設定する

ホストアドレスやサブネットマスク、デフォルトゲートウェイなど、基本的なIPアドレス設定をします。
ここでは固定IPアドレスを設定する手順を説明します。

1. スキャナーの電源を入れます。

2. 操作パネルのホーム画面で［設定］を選択します。

3. ［ネットワーク設定］-［詳細設定］-［TCP/IP］の順に選択します。

4. ［TCP/IP設定方法］で［手動設定］を選択します。

   IPアドレスをルーターなどのDHCP機能で自動設定する場合は［自動設定］にします。この場合は、手順5、6の［IPアドレス］、［サブネットマスク］、［デフォルトゲートウェイ］も自動設定になるので入力できません。手順7へ進んでください。

5. IPアドレスを入力します。

   ◀または▶を選択すると、ピリオドで区切られた前後の区切りにフォーカスが移動します。
   戻った画面で入力した値が反映されていることを確認してください。

6. 同様に［サブネットマスク］、［デフォルトゲートウェイ］を設定します。

   戻った画面で入力した値が反映されていることを確認してください。

   > **重要** IPアドレス、サブネットマスク、デフォルトゲートウェイの組み合わせが不正の場合、［設定を開始する］が有効にならず、設定を続けることができません。入力に間違いがないか確認してください。

7. プライマリーDNSサーバーのIPアドレスを入力します。

   戻った画面で入力した値が反映されていることを確認してください。

参考 IPアドレスを［自動設定］にすると、DNSサーバー設定は［手動設定］、［自動設定］を選択できます。DNSサーバーのアドレスを自動取得できない場合に［手動設定］を選択して、DNSサーバーのIPアドレスを入力してください。引き続き、セカンダリーDNSサーバーのアドレスを直接入力します。［自動設定］を選択した場合は、手順9へ進んでください。

8. セカンダリーDNSサーバーのIPアドレスを入力します。
   戻った画面で入力した値が反映されていることを確認してください。

9. ［設定を開始する］をタップします。

プロキシサーバーを設定する

以下の両方に当てはまる場合は、プロキシサーバーを設定してください。

- インターネット接続用にプロキシサーバーを構築している
- Epson Connectサービスや他社クラウドサービスなど、スキャナーが直接インターネットに接続する機能を使用する

1. ホーム画面で［設定］を選択します。
   IPアドレスの設定に続いて設定するときは、［詳細設定］画面が表示されています。手順3に進んでください。

2. ［ネットワーク設定］-［詳細設定］の順に選択します。

3. ［プロキシサーバー］を選択します。

4. ［プロキシサーバー使用設定］で［使用する］を選択します。

5. プロキシサーバーのアドレスを、IPv4アドレスまたはFQDN形式で入力します。
   戻った画面で入力した値が反映されていることを確認してください。

6. プロキシサーバーのポート番号を入力します。
   戻った画面で入力した値が反映されていることを確認してください。

7. ［設定を開始する］をタップします。

有線LANに接続する

LANケーブルでネットワークに接続して、接続の確認をします。

1. スキャナーとハブ（LANスイッチ）をLANケーブルで接続します。

2. ホーム画面で  を選択します。

3. ［ルーター］を選択します。

4. 接続状態やIPアドレスが正しいことを確認します。

5. ［閉じる］をタップします。

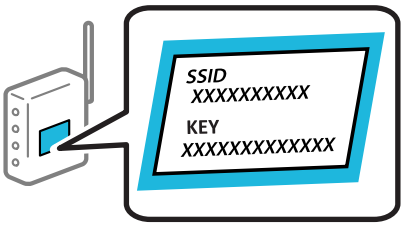
無線LAN（Wi-Fi）に接続する

スキャナーと無線LAN(Wi-Fi)を接続する方法はいくつかあります。お使いの環境や条件に合わせて接続方法を選択してください。
無線LANルーター（アクセスポイント）の情報（SSID、パスワード）がわかれば、手動で設定するのが確実です。
WPS対応の無線LANルーター（アクセスポイント）をお使いの場合は、プッシュボタンで自動設定ができます。
スキャナーがネットワークに接続できたら、使用する機器（コンピューターやスマートデバイスなど）をスキャナーに接続してください。

スキャナーにSSIDとパスワードを入力して設定する

無線LANルーター（アクセスポイント）に接続するための情報をスキャナーの操作パネルから入力して設定する方法です。手動で設定するには、無線LANルーター（アクセスポイント）のSSIDとパスワードの情報が必要です。

参考 無線LANルーター（アクセスポイント）をメーカー設定値のまま利用している場合は、ラベルなどに書かれているSSIDとパスワードが設定されています。SSIDとパスワードがわからない場合は、無線LANルーターを設定した人に確認するか、無線LANルーターのマニュアルをご覧ください。



1. ホーム画面で  をタップします。

2. ［ルーター］を選択します。

3. ［設定に進む］をタップします。
   すでにネットワーク接続している場合は、接続状態の詳細が表示されます。設定を変更する場合は［無線LAN接続に変更する］または［設定を変更する］をタップします。

4. ［無線LANルーターを検索］を選択します。

5. 画面の指示に従って、SSIDを選択し、パスワードを入力して、設定を開始します。
   設定完了後に接続状態を確認したい場合は、「関連情報」をご覧ください。

参考
- SSIDがわからない場合は無線LANルーター（アクセスポイント）のラベルに書かれていないかを確認してください。無線LANルーター（アクセスポイント）をメーカー設定値のまま利用している場合は、ラベルに書かれているSSIDを使用します。情報が見つからない場合は、無線LANルーター（アクセスポイント）のマニュアルをご覧ください。
- パスワードは大文字と小文字を区別して入力してください。
- SSIDがわからない場合は無線LANルーター（アクセスポイント）本体のラベルに書かれていないかを確認してください。ラベルには、「暗号化キー」「XXXX Key」などと書かれています。無線LANルーター（アクセスポイント）をメーカー設定値のまま利用している場合は、ラベルに書かれているパスワードを使用します。

関連情報

➡ 「ネットワーク接続状態の確認」26ページ

プッシュボタンで自動設定する（AOSS/WPS）

無線LANルーター（アクセスポイント）のプッシュボタンで無線LAN（Wi-Fi）を自動設定する方法です。以下の条件に当てはまる場合は、この方法で設定できます。

- 無線LANルーター（アクセスポイント）がAOSSやWPS（Wi-Fi Protected Setup）に対応している
- 既存の無線LAN（Wi-Fi）をプッシュボタンで設定している

参考 プッシュボタンの位置がわからない、またはプッシュボタンがなくソフトウェアで操作する場合は、無線LANルーター（アクセスポイント）のマニュアルをご覧ください。

1. ホーム画面で  をタップします。
2. ［ルーター］を選択します。
3. ［設定に進む］をタップします。

   すでにネットワーク接続している場合は、接続状態の詳細が表示されます。設定を変更する場合は［無線LAN接続に変更する］または［設定を変更する］をタップします。
4. ［プッシュボタンで設定(AOSS/WPS)］を選択します。
5. 画面の指示に従って操作します。

   設定完了後に接続状態を確認したい場合は、「関連情報」をご覧ください。

   参考 接続に失敗した場合は無線LANルーター（アクセスポイント）を再起動し、無線LANルーター（アクセスポイント）とスキャナーを近づけてから再度設定してください。

関連情報

➡ 「ネットワーク接続状態の確認」26ページ

PINコードで設定する（WPS）

PINコードを使って無線LANルーター（アクセスポイント）に接続する方法です。無線LANルーター（アクセスポイント）がWPS（Wi-Fi Protected Setup）に対応している場合は、この方法で設定できます。PINコードを無線LANルーター（アクセスポイント）に入力するときに、コンピューターを使います。

1. ホーム画面で  をタップします。
2. ［ルーター］を選択します。
3. ［設定に進む］をタップします。
   すでにネットワーク接続している場合は、接続状態の詳細が表示されます。設定を変更する場合は［無線LAN接続に変更する］または［設定を変更する］をタップします。
4. ［その他］-［PINコード自動設定(WPS)］の順に選択します。
5. 画面の指示に従って操作します。
   設定完了後に接続状態を確認したい場合は、「関連情報」をご覧ください。

   参考 PINコードの入力方法は、無線LANルーター（アクセスポイント）のマニュアルをご覧ください。

関連情報

➡ 「ネットワーク接続状態の確認」26ページ

コンピューターや機器の追加や交換をしたときは

ネットワーク接続済みのスキャナーに接続する方法

すでにスキャナーがネットワークに接続していれば、コンピューターやスマートデバイスからネットワーク経由でスキャナーに接続できます。

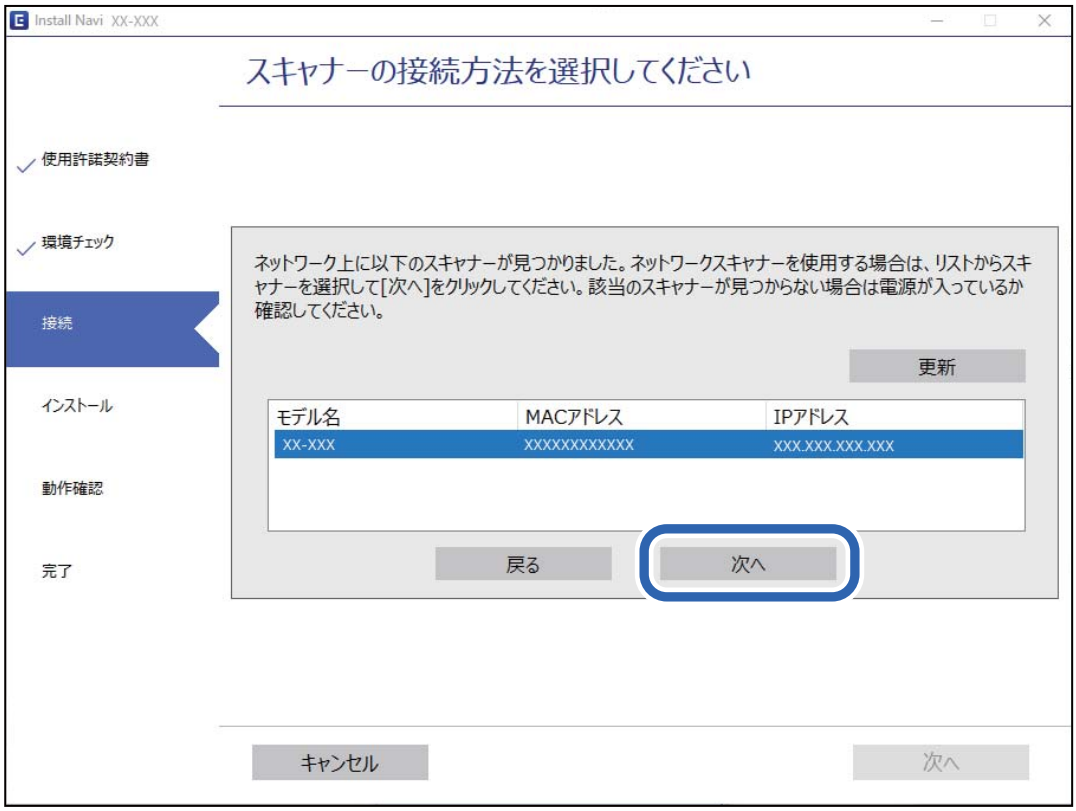
2台目のコンピューターからネットワークスキャナーを使う

スキャナーとコンピューターを接続設定するにはインストーラーを使うと便利です。インストーラーは以下のいずれかの方法で起動できます。

- ウェブサイトから開始する
  以下のウェブサイトへアクセスし、製品名を入力してください。［セットアップ］に進んで作業を開始します。
  http://epson.sn
- ソフトウェアディスクを使って設定する（ソフトウェアディスクが同梱されている機種で、お使いのコンピューターがディスクドライブを搭載したWindowsの場合）
  コンピューターにソフトウェアディスクを挿入し、画面の指示に従ってください。

スキャナーを選択する

以下の画面が表示されるまで、画面の指示に従って操作し、接続したいスキャナーを選択して［次へ］をクリックします。



画面の指示に従って操作します。

スマートデバイスからネットワークスキャナーを使う

スマートデバイスからスキャナーに接続するには、以下のいずれかの方法があります。

無線LANルーター経由で接続

無線LANルーターを介して、スキャナーが接続しているWi-Fiと同じネットワーク（SSID）に接続します。
詳しくは以下を参照してください。
「スマートデバイスとの接続設定をする」24ページ

Wi-Fi Directで接続

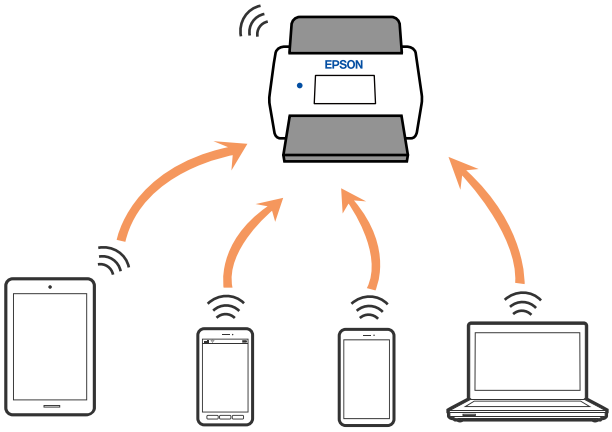
無線LANルーター（アクセスポイント）を介さず、直接スキャナーと接続します。
詳しくは以下を参照してください。
「スマートデバイスとスキャナーを直接接続する方法（Wi-Fi Direct）」22ページ

スマートデバイスとスキャナーを直接接続する方法（Wi-Fi Direct）

Wi-Fi Direct（シンプルAP）を使うと、無線LANルーターを使わずにスマートデバイスとスキャナーを直接接続してスキャンできます。

Wi-Fi Direct（シンプルAP）とは

家庭またはオフィスで無線LAN（Wi-Fi）を利用していない、無線LANルーター（アクセスポイント）がない場合や、スキャナーとコンピューターやスマートデバイスを直接接続したい場合の接続方法です。この接続方法はスキャナーが無線LANルーター（アクセスポイント）として動作し、複数台（最大8台）の機器と接続できます。ただし、スキャナーに直接接続された機器の間では、スキャナー経由での通信はできません。



スキャナーは無線LAN（Wi-Fi）または有線LANと、Wi-Fi Direct（シンプルAP）の同時接続ができます。ただし、無線LAN（Wi-Fi）で接続中にWi-Fi Direct（シンプルAP）設定を開始すると、無線LAN（Wi-Fi）接続は一時切断されます。

スマートデバイスでWi-Fi Direct接続する

無線LANルーター（アクセスポイント）を介さず、直接スキャナーと機器を接続する方法です。

1. ホーム画面で  を選択します。
2. ［Wi-Fi Direct］を選択します。
3. ［設定に進む］を選択します。
4. スマートデバイスでEpson Smart Panelを起動します。
5. Epson Smart Panelの案内に従って、スマートデバイスとスキャナーを接続します。
   スマートデバイスがスキャナーと接続されたら、次の手順に進みます。
6. スキャナーの画面で［完了］を選択します。

Wi-Fi Direct（シンプルAP）接続を切断する

Wi-Fi Direct（シンプルAP）接続を無効にする方法は、操作パネルから全ての接続を無効にする方法と、コンピューターやスマートデバイスからそれぞれの接続を無効にする方法があります。

全ての接続を無効にするには、  - ［Wi-Fi Direct］-［設定に進む］-［設定を変更する］-［Wi-Fi Directを無効にする］の順に選択します。

!重要 Wi-Fi Direct（シンプルAP）接続で複数のコンピューターやスマートデバイスがスキャナーと接続されていた場合、Wi-Fi Direct（シンプルAP）接続を無効にすると、全ての接続が切断されます。

参考 特定の機器だけを切断したいときは、スマートデバイス側から接続を切断してください。以下の方法で、スマートデバイスからスキャナーへのWi-Fi Direct接続を切断します。

- スキャナーの接続名（SSID）とのWi-Fi接続を切断
- 他のネットワーク（SSID）に接続

Wi-Fi Direct（シンプルAP）のSSIDなどを変更する

Wi-Fi Direct（シンプルAP）が有効なとき、  -［Wi-Fi Direct］-［設定に進む］-［設定を変更する］を選択すると、以下のメニューが表示され設定を変更できます。

接続名を変更する

スキャナーに接続するWi-Fi Direct（シンプルAP）の接続名（SSID）を任意の値に変更します。接続名（SSID）に設定できるのは、操作パネルのソフトキーボードに表示されたASCII文字です。22文字まで入力できます。
接続名（SSID）を変更すると接続しているデバイスは全て切断されます。接続名を変更した場合は、接続する機器から新しい接続名（SSID）で接続し直してください。

パスワードを変更する

スキャナーに接続するWi-Fi Direct（シンプルAP）のパスワードを変更します。パスワードに設定できるのは、操作パネルのソフトキーボードに表示されたASCII文字です。8～22文字以内で入力してください。
パスワードを変更すると接続しているデバイスは全て切断されます。パスワードを変更した場合は、接続する機器から新しいパスワードで接続し直してください。

周波数帯を変更する

スキャナーに接続するWi-Fi Direct（シンプルAP）の周波数帯を変更します。2.4 GHzまたは5 GHzに設定できます。
周波数帯を変更すると接続しているデバイスは全て切断されます。再度接続してください。
周波数帯を5 GHzに設定した場合、5 GHz非対応のデバイスからは再接続できなくなります。
お住まいの国や地域によってはこの設定がないことがあります。

Wi-Fi Directを無効にする

Wi-Fi Direct（シンプルAP）を無効にします。無効にすると接続しているデバイスは全て切断されます。

初期設定に戻す

Wi-Fi Direct（シンプルAP）設定の全てを購入時の設定に戻します。
また、スキャナーが保持しているスマートデバイスのWi-Fi Direct機能を使った接続情報の登録を削除します。

参考 以下の設定項目は、Web Configの［ネットワーク］タブ -［Wi-Fi Direct］からも設定できます。

- Wi-Fi Direct（シンプルAP）を有効または無効にする
- ネットワーク名（SSID）を変更する
- パスワードを変更する
- 周波数帯を変更する
  お住まいの国や地域によってはこの設定がないことがあります。
- Wi-Fi Direct（シンプルAP）の設定を初期の状態に戻す

ネットワークを再設定する方法

無線LANルーターを交換したときやコンピューターを買い替えたときなどの接続設定や、接続方法の変更などについて説明します。

無線LANルーターを交換したとき

無線LANルーターを交換したときは、コンピューターやスマートデバイスとスキャナーとの接続設定をします。
プロバイダーを変更した場合などでこの設定が必要です。

コンピューターとの接続設定をする

スキャナーとコンピューターを接続設定するにはインストーラーを使うと便利です。インストーラーは以下のいずれかの方法で起動できます。

- ウェブサイトから開始する
  以下のウェブサイトへアクセスし、製品名を入力してください。［セットアップ］に進んで作業を開始します。
  http://epson.sn
- ソフトウェアディスクを使って設定する（ソフトウェアディスクが同梱されている機種で、お使いのコンピューターがディスクドライブを搭載したWindowsの場合）
  コンピューターにソフトウェアディスクを挿入し、画面の指示に従ってください。

接続方法を選択する

画面の指示に従って操作します。［実施したい作業を選んでください］画面で、［スキャナーの再セットアップ（無線LANルーターが替わった場合など）］を選択して、［次へ］をクリックします。
画面の指示に従い、セットアップを完了してください。
接続できない場合は、以下を参照してください。
「ネットワークに接続できない」30ページ

スマートデバイスとの接続設定をする

スマートデバイスが接続しているWi-Fiと同じネットワーク（SSID）にスキャナーを接続すると、スマートデバイスからスキャナーが使えるようになります。スマートデバイスからスキャナーを利用するには、以下のウェブサイトにアクセスして、製品名を入力します。［セットアップ］に進んで作業を開始します。

http://epson.sn

なお、ウェブサイトにはスキャナーに接続したい機器からアクセスしてください。

コンピューターを買い替えたとき

コンピューターを買い替えたときは、コンピューターとスキャナーとの接続設定をします。

コンピューターとの接続設定をする

スキャナーとコンピューターを接続設定するにはインストーラーを使うと便利です。インストーラーは以下の方法で起動できます。

- ウェブサイトから起動する
  以下のウェブサイトへアクセスし、製品名を入力してください。［セットアップ］に進んで作業を開始します。
  http://epson.sn
- ソフトウェアディスクを使って設定する（ソフトウェアディスクが同梱されている機種で、お使いのコンピューターがディスクドライブを搭載したディスクドライブがあるWindowsの場合）
  コンピューターにソフトウェアディスクを挿入し、画面の指示に従ってください。

画面の指示に従って操作します。

コンピューターとの接続形態を変更する

すでにコンピューターとスキャナーが接続されている場合に、接続形態を変更する方法について説明します。

有線LAN接続から無線LAN接続に変更する

スキャナーの操作パネルで有線LAN接続から無線LAN接続に変更します。変更方法は操作パネルを使った無線LAN接続設定と同じです。

関連情報

➡ 「無線LAN（Wi-Fi）に接続する」18ページ

無線LAN接続から有線LAN接続に変更する

無線LAN（Wi-Fi）接続時に有線LAN接続に変更するには以下の手順で操作します。

1. ホーム画面で［設定］を選択します。
2. ［ネットワーク設定］-［有線LAN接続設定］の順に選択します。
3. 各項目を設定します。

USB接続からネットワーク接続に変更する

インストーラーを使って別の接続形態に設定し直します。

- ウェブサイトから開始する
  以下のウェブサイトへアクセスし、製品名を入力してください。［セットアップ］に進んで作業を開始します。
  http://epson.sn
- ソフトウェアディスクを使って設定する（ソフトウェアディスクが同梱されている機種で、お使いのコンピューターがディスクドライブを搭載したWindowsの場合）
  コンピューターにソフトウェアディスクを挿入し、画面の指示に従ってください。

接続方法の変更を選択する

画面の指示に従って操作します。［実施したい作業を選んでください］画面で、［スキャナーの再セットアップ（無線LANルーターが替わった場合など）］を選択して、［次へ］をクリックします。
［無線LAN（Wi-Fi）］または［有線LAN（Ethernet）で接続する］から使用する接続方法を選択して、［次へ］をクリックします。
画面の指示に従い、セットアップを完了してください。

ネットワーク接続状態の確認

ネットワーク接続状態を確認するには、いくつかの方法があります。

操作パネルでのネットワーク接続状態の確認

操作パネルに表示されるネットワークアイコンやネットワーク情報で接続状態を確認できます。

ネットワークアイコンで接続状態を確認する

スキャナーのホーム画面にあるネットワークアイコンでネットワークの接続状態と電波強度を確認できます。

	ネットワークの接続状態を示します。 アイコンを選択すると現在の設定の確認や変更ができます。以下のメニューのショートカットです。 ［設定］-［ネットワーク設定］-［無線LAN接続設定］	
		無線LAN（Wi-Fi）無効
		SSID検索中、IPアドレス未設定、電波強度が0または弱い
		無線LAN（Wi-Fi）接続中 線の数は電波の状態を示します。線の数が多いほど、電波の状態は良好です。
		Wi-Fi Direct（シンプルAP）接続無効
		Wi-Fi Direct（シンプルAP）接続有効
		有線LAN非接続、ネットワーク未設定
		有線LAN接続中

操作パネルにネットワーク状態を表示する

スキャナーがネットワーク接続されていると、確認したい項目を選択することでその他ネットワーク関連の情報も確認できます。

1. ホーム画面で［設定］を選択します。
2. ［ネットワーク設定］-［ネットワーク情報］の順に選択します。
3. 確認したいメニューを選択します。
   - 有線・無線接続状態
     有線または無線接続時のネットワーク情報（デバイス名、接続状態、電波状態など）が表示されます。
   - Wi-Fi Direct接続状態
     Wi-Fi Directの有効状態、SSID、パスワードなどが表示されます。
   - メールサーバー設定情報
     メールサーバーのネットワーク情報が表示されます。

ネットワークの仕様

無線LANの仕様

準拠規格	IEEE802.11a/b/g/n*1/ac

周波数帯	IEEE802.11b/g/n：2.4 GHz、IEEE802.11a/n/ac：5 GHz		
チャンネル	Wi-Fi	2.4 GHz	1/2/3/4/5/6/7/8/9/10/11/12/13
		5 GHz	W52（36/40/44/48）*2、W53（52/56/60/64）*2 、W56 （100/104/108/112/116/120/124/128/132/136/140）
	Wi-Fi Direct	2.4 GHz	1/2/3/4/5/6/7/8/9/10/11/12/13
		5 GHz	W52（36/40/44/48）*2
接続モード	インフラストラクチャー、 Wi-Fi Direct（シンプル AP）*3*4		
無線セキュリティー*5	WEP（64/128bit）、WPA2-PSK（AES）*6、WPA3-SAE（AES）、WPA2/WPA3-Enterprise		

*1： IEEE802.11n（2.4GHz）はHT20のみ対応
*2： 屋外使用不可
*3： IEEE802.11bは非対応
*4： シンプルAPモードは、無線LAN（インフラストラクチャー）または有線LANとの併用可能
*5： Wi-Fi DirectはWPA2-PSK（AES）のみ対応
*6： WPA2規格に準拠し、WPA/WPA2 Personal規格に対応

有線LANの仕様

準拠規格	IEEE802.3i（10BASE-T）*1 IEEE802.3u（100BASE-TX）*1 IEEE802.3ab（1000BASE-T）*1 IEEE802.3az（Energy Efficient Ethernet）*2
通信モード	Auto、10 Mbps Full duplex、10 Mbps Half duplex、100 Mbps Full duplex、100 Mbps Half duplex
コネクター	RJ-45

*1 ：社団法人 VCCI協会の技術基準への適合及び電磁障害のリスク低減のため、カテゴリー 5e 以上のSTP（シールドツイストペア）ケーブルを使用すること
*2 ：IEEE802.3azに対応した接続機器が必要

ネットワーク機能とIPv4/IPv6対応

機能	対応
Epson Scan 2	IPv4、IPv6
Document Capture Pro/Document Capture	IPv4
Document Capture Pro Server	IPv4、IPv6

セキュリティーのプロトコル

IEEE802.1X*	
IPsec/IPフィルタリング	
SSL/TLS	HTTPS（サーバー/クライアント）
SMTPS（STARTTLS、SSL/TLS）	
SNMPv3	

*　　：IEEE802.1Xに対応した接続機器が必要

スキャナーが使用するポート

スキャナーは以下のポートを使用します。必要に応じてあらかじめネットワーク管理者にポート使用を許可してもらいます。

送信元（クライアント）がスキャナーの場合

用途	送信先(サーバー)	プロトコル	ポート番号
ファイル送信（スキャナー本体のスキャン to ネットワークフォルダー機能利用時）	FTP/FTPSサーバー	FTP/FTPS (TCP)	20
			21
	ファイルサーバー	SMB（TCP）	445
		NetBIOS（UDP）	137
			138
		NetBIOS（TCP）	139
	WebDAVサーバー	Protocol HTTP (TCP)	80
		Protocol HTTPS (TCP)	443
メール送信（スキャナー本体のスキャン to メール機能利用時）	SMTPサーバー	SMTP（TCP）	25
		SMTP SSL/TLS（TCP）	465
		SMTP STARTTLS（TCP）	587
POP before SMTP接続（スキャナー本体のスキャン to メール機能利用時）	POPサーバー	POP3（TCP）	110
Epson Connectを利用した機能の利用	Epson Connectサーバー	HTTPS	443
		XMPP	5222

用途	送信先(サーバー)	プロトコル	ポート番号
ユーザー情報取得（スキャナー本体のアドレス帳利用時）	LDAPサーバー	LDAP（TCP）	389
		LDAP SSL/TLS（TCP）	636
		LDAP STARTTLS（TCP）	389
ユーザー情報取得時のユーザー認証（スキャナー本体のアドレス帳利用時） スキャナー本体のスキャン to ネットワークフォルダー（SMB）機能利用時のユーザー認証	KDCサーバー	Kerberos	88
WSDの制御	クライアントコンピューター	WSD（TCP）	5357
アプリケーションソフトへのプッシュスキャン時のコンピューター探索	クライアントコンピューター	Network Push Scan Discovery	2968

送信元（クライアント）がクライアントコンピューターの場合

用途	送信先(サーバー)	プロトコル	ポート番号
EpsonNet Configなどのアプリケーションソフト、スキャナードライバーからのスキャナー探索	スキャナー	ENPC（UDP）	3289
EpsonNet Configなどのアプリケーションソフト、スキャナードライバーからのスキャナーMIB情報の取得と設定	スキャナー	SNMP（UDP）	161
WSDのスキャナー探索	スキャナー	WS-Discovery（UDP）	3702
アプリケーションソフトからのスキャンデータの転送	スキャナー	Network Scan（TCP）	1865
アプリケーションソフトからのプッシュスキャン時のジョブ情報取得	スキャナー	Network Push Scan	2968
Web Config	スキャナー	HTTP(TCP)	80
		HTTPS(TCP)	443

困ったときは

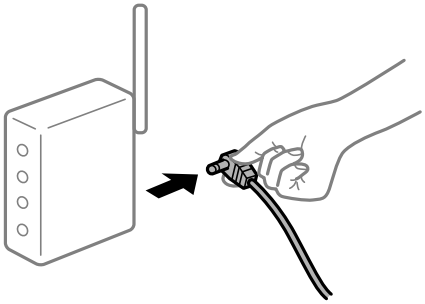
ネットワークに接続できない

以下の原因が考えられます。

無線LAN接続でネットワーク機器に何らかの問題があります。

対処方法

ネットワークに接続したい各デバイスの電源を切ってください。約10秒待ってから無線LANルーター（アクセスポイント）、コンピューターまたはスマートデバイス、スキャナーの順に電源を入れます。電波が届きやすいように機器を無線LANルーター（アクセスポイント）に近づけて、設定し直してください。



機器と無線LANルーターが離れていて電波が届いていません。

対処方法

コンピューターまたはスマートデバイスとスキャナーを無線LANルーターの近くに移動して、無線LANルーターの電源を入れ直してください。

無線LANルーターを交換した場合、設定が新しいルーターに合っていません。

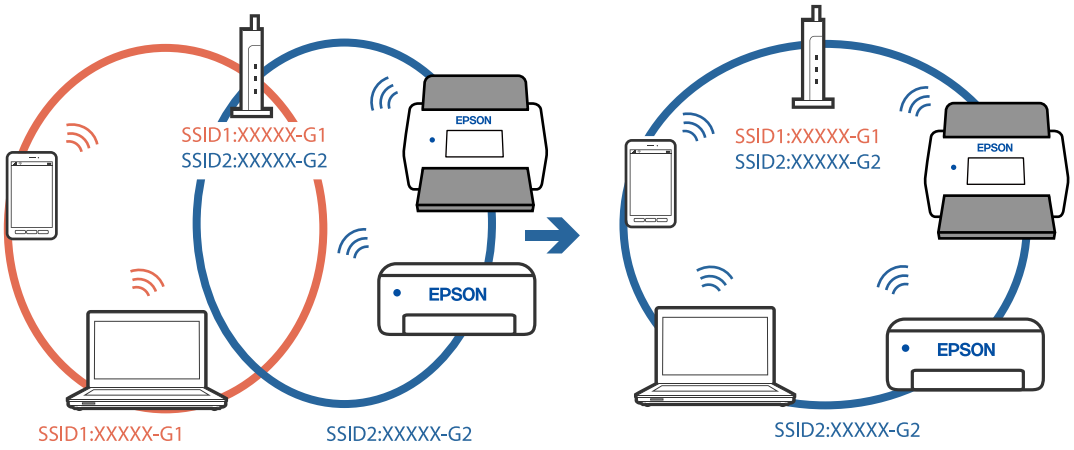
対処方法

新しい無線LANルーターに合うように、接続設定をやり直してください。

接続しているSSIDがコンピューターやスマートデバイスとスキャナーで異なっています。

対処方法

複数の無線LANルーターを使用している場合や、1台で複数のSSIDを使用できる無線LANルーターの場合、コンピューターやスマートデバイスが接続しているSSIDとスキャナーが接続しているSSIDが異なっていると接続できません。
コンピューターやスマートデバイスをスキャナーと同じSSIDに接続してください。



ワイヤレスルーターのプライバシーセパレーター機能が有効です。

対処方法

多くの無線LANルーター（アクセスポイント）やモバイルルーターには、機器間の通信を遮断するプライバシーセパレーター機能があります。同じSSIDに接続されていてもスキャナーとコンピューターまたはスマートデバイス間で通信できない場合は、無線LANルーター（アクセスポイント）のプライバシーセパレーター機能を無効にしてください。詳しくは無線LANルーター（アクセスポイント）のマニュアルをご覧ください。

IPアドレスが正しく割り当てられていません。

対処方法

IPアドレスが「169.254.XXX.XXX」、サブネットマスクが「255.255.0.0」の場合は、IPアドレスが正しく割り当てられていない可能性があります。
スキャナーの操作パネルで、［設定］-［ネットワーク設定］-［詳細設定］-［TCP/IP］の順に選択して、スキャナーに割り当てられているIPアドレスとサブネットマスクを確認してください。
ワイヤレスルーターを再起動するか、スキャナーのネットワーク設定をリセットします。

コンピューターのネットワーク設定に問題があります。

対処方法

コンピューターからウェブサイトを閲覧できるか確認してください。閲覧できない場合はコンピューターのネットワーク設定に問題があります。
コンピューターのネットワーク接続を確認してください。詳しくはコンピューターのマニュアルをご覧ください。

IEEE 802.3az（省電力イーサーネット）に対応した機器を使って有線LAN接続しています。

対処方法

IEEE 802.3az（Energy Efficient Ethernet、省電力イーサネット）に対応した機器を使って有線LAN接続する場合、一部のハブやルーターを使用したときに以下の現象が発生することがあります。

- 接続したりしなかったりして不安定になる
- 接続できなくなる
- 通信速度が遅くなる

以下の手順で、スキャナーのIEEE 802.3azを無効にして接続してください。

1. コンピューターとスキャナーそれぞれにつながっているLANケーブルを外します。
2. コンピューターのIEEE 802.3azが有効になっている場合は、無効にします。
   詳しくはコンピューターのマニュアルをご覧ください。
3. LANケーブルでコンピューターとスキャナーを直接接続します。
4. スキャナーでネットワーク設定を確認します。
   ［設定］ - ［ネットワーク設定］ - ［ネットワーク情報］ - ［有線・無線接続状態］の順に選択します。
5. スキャナーのIPアドレスを確認します。
6. コンピューターで、Web Configを起動します。
   Webブラウザーを起動し、スキャナーのIPアドレスを入力してください。
   「ブラウザーでWeb Configを起動する」35ページ
7. ［ネットワーク］タブ-［有線LAN］の順に選択します。
8. ［IEEE 802.3az］で［オフ］を選択します。
9. ［次へ］をクリックします。
10. ［設定］をクリックします。
11. コンピューターとスキャナーそれぞれにつながっているLANケーブルを外します。
12. 手順2でコンピューターのIEEE 802.3azを無効にした場合は、有効にします。
13. 手順1で外したLANケーブルをコンピューターとスキャナーにつなぎます。

上記の手順をしてもこの現象が発生する場合は、スキャナー以外の機器が原因となっている可能性があります。

スキャナーの電源が入っていません。

対処方法

スキャナーの電源が入っているか確認してください。
また、スキャナーの電源ランプの点滅が点灯に変わり、使用できる状態になるまでお待ちください。

スキャナーを設定するソフトウェア

Web Config

Web Configは、コンピューター上のInternet ExplorerやSafariなどのWebブラウザーで起動するソフトウェアです。スキャナーの状況を確認したり、ネットワークサービスやスキャナー設定を変更したりできます。ネットワークからスキャナーに直接アクセスして操作するので、1台ずつセットアップする場合に適しています。Web Configを使うためには、コンピューターをスキャナーと同じネットワークに接続してください。
対応しているブラウザーは以下の通りです。
Microsoft Edge、Windows Internet Explorer 8以降、Firefox*、Chrome*、Safari*
* 最新バージョンをお使いください。

関連情報

➡ 「Web Configにアクセスできない」76ページ

ブラウザーでWeb Configを起動する

1. **スキャナーのIPアドレスを確認します。**

   スキャナーの操作パネルで、［設定］-［ネットワーク設定］-［ネットワーク情報］の順に選択します。次に、スキャナーのIPアドレスを確認するために［有線・無線接続状態］または［Wi-Fi Direct接続状態］で実行中の接続方法を選択します。

2. **コンピューターまたはスマートデバイスでWebブラウザーを起動して、スキャナーのIPアドレスを入力します。**

   書式：
   IPv4： http://スキャナーのIPアドレス/
   IPv6： http://[スキャナーのIPアドレス]/
   例：
   IPv4： http://192.168.100.201/
   IPv6： http://[2001:db8::1000:1]/

   参考 HTTPSにアクセスするときにスキャナーは自己署名証明を使うため、Web Configを起動すると警告が表示されますが、これは問題ではなく、無視しても安全です。

3. **管理者としてログオンして、スキャナーの設定を変更します。**

   画面の右上の［ログオン］をクリックします。［ユーザー名］と［現在のパスワード］を入力し、［確認］をクリックします。

   参考
   - Web Configの管理者情報の購入時の設定（初期値）は以下の通りです。
     ・ユーザー名：なし（空欄）
     ・パスワード：スキャナーの製造番号（シリアルナンバー）
     製造番号は、スキャナー背面に貼られているラベルをご確認ください。
   - ［ログオフ］が画面右上に表示されているときは、すでに管理者としてログインしています。
   - 何も操作しない状態が約20分続くと自動的にログオフします。

Windows上でWeb Configを起動する

WSDを使ってコンピューターとスキャナーを接続しているときは、以下の手順でWeb Configを起動してください。

1. コンピューターでスキャナーの一覧を表示します。
   - Windows 10
     スタートボタンをクリックし、［Windows システムツール］-［コントロールパネル］-［ハードウェアとサウンド］の［デバイスとプリンターの表示］の順に選択します。
   - Windows 8.1/Windows 8
     ［デスクトップ］-［設定］-［コントロールパネル］-［ハードウェアとサウンド］（または［ハードウェア］）の［デバイスとプリンターの表示］の順に選択します。
   - Windows 7
     スタートボタンをクリックし、［コントロールパネル］-［ハードウェアとサウンド］の［デバイスとプリンターの表示］の順に選択します。
2. お使いのスキャナーを右クリックして、［プロパティ］を選択します。
3. ［Web サービス］タブを選んで、URLをクリックします。
   HTTPSにアクセスするときにスキャナーは自己署名証明を使うため、Web Configを起動すると警告が表示されますが、これは問題ではなく、無視しても安全です。

参考
- Web Configの管理者情報の購入時の設定（初期値）は以下の通りです。
  ・ユーザー名：なし（空欄）
  ・パスワード：スキャナーの製造番号（シリアルナンバー）
  製造番号は、スキャナー背面に貼られているラベルをご確認ください。
- ［ログオフ］が画面右上に表示されているときは、すでに管理者としてログインしています。
- 何も操作しない状態が約20分続くと自動的にログオフします。

Epson Device Admin

Epson Device Adminは、ネットワーク上のデバイスを管理するアプリケーションソフトです。
設定テンプレートを使ってネットワーク上の複数のスキャナーに統一した設定を適用できるため、複数のスキャナーを導入、管理する場合に適しています。
Epson Device Adminはエプソンのウェブサイトからダウンロードしてください。使い方について、詳しくはEpson Device Adminのヘルプやマニュアルをご覧ください。

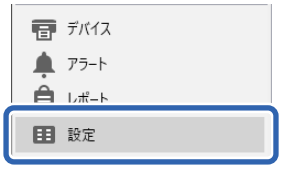
設定テンプレート

設定テンプレートを新規作成する

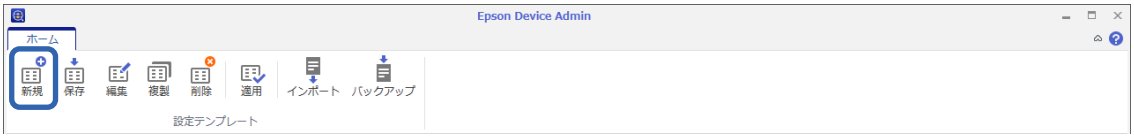
設定テンプレートを新規で作成します。

1. Epson Device Adminを起動します。

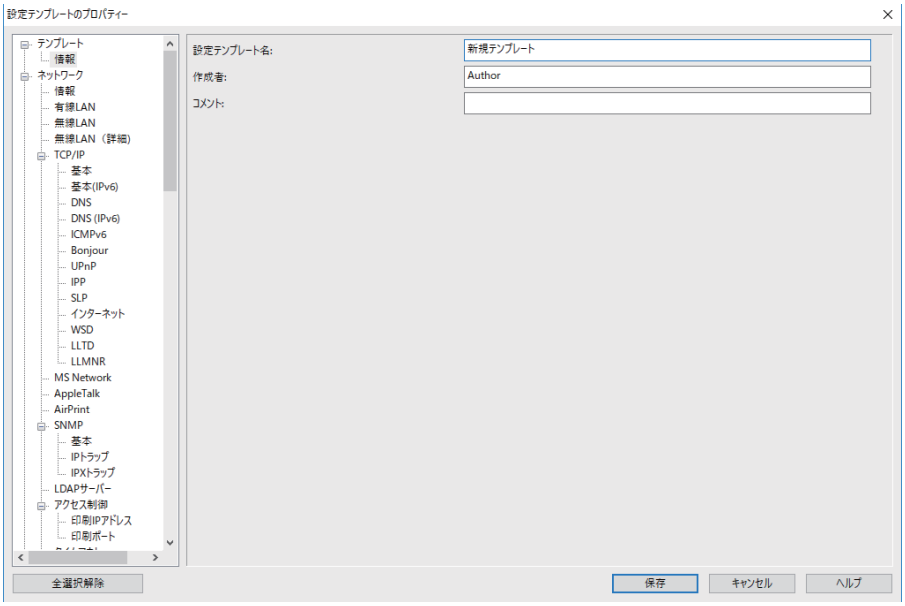
2. サイドバータスクメニューで［設定］を選択します。



3. リボンメニューで［新規］を選択します。



4. 各項目を設定します。



項目	説明
設定テンプレート名	設定テンプレートの名称です。 Unicode（UTF-8）で表せる文字で、1024文字以内で入力します。
作成者	テンプレートの作成者情報です。 Unicode（UTF-8）で表せる文字で、1024文字以内で入力します。
コメント	任意の情報を入力します。 Unicode（UTF-8）で表せる文字で、1024文字以内で入力します。

5. 左のメニューから設定したい機能を選択します。

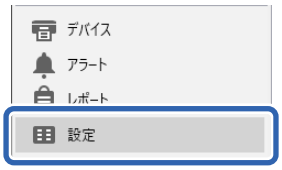
参考 左のメニュー項目をクリックするとそれぞれの画面に切り替わります。設定した値は、キャンセルしなければ画面を切り替えても保持されます。全ての項目の設定が終了してから［保存］をクリックしてください。

設定テンプレートを適用する

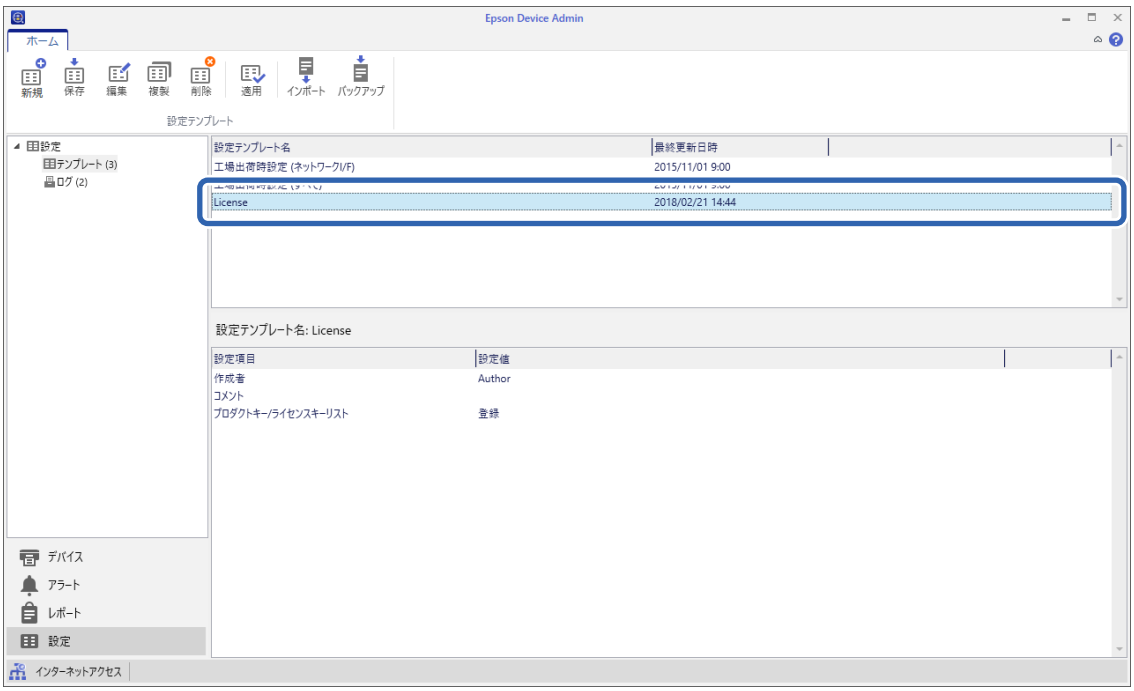
保存した設定テンプレートをスキャナーに適用します。設定テンプレートのチェックのある項目が適用されます。対象スキャナーに該当する機能がない場合は適用されません。

参考 スキャナーに管理者パスワードを設定している場合、先にパスワード設定を行ってください。
1.デバイス一覧画面のリボンメニューで、［オプション］ - ［パスワード管理］を選択します。
2.［自動パスワード管理機能を有効にする］を選択して、［パスワード管理］をクリックします。
3.該当するスキャナーを選択して［編集］をクリックします。
4.パスワードを設定して、［登録/更新］をクリックします。

1. サイドバータスクメニューで［設定］を選択します。



2. ［設定テンプレート名］から適用する設定テンプレートを選択します。

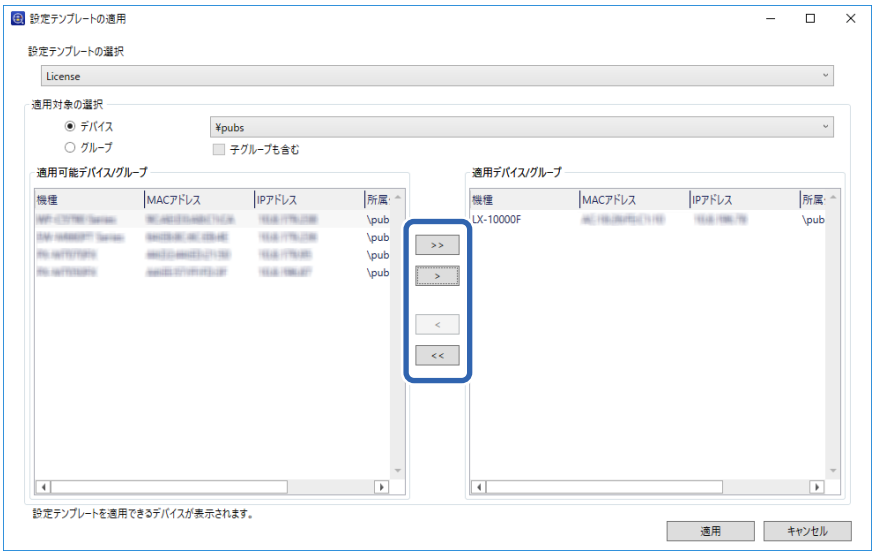


3. リボンメニューで［適用］をクリックします。
デバイス選択画面が表示されます。

4. 適用する設定テンプレートを選択します。

参考
- ［デバイス］を選択してプルダウンメニューからデバイスが登録されているグループを選択すると、個々のデバイスが表示されます。
- ［グループ］を選択すると、グループが表示されます。［子グループも含む］にチェックすると、グループを選択したときに子グループも自動的に選択します。

5. 適用するスキャナーまたはグループを［適用デバイス/グループ］へ移動します。



6. ［適用］をクリックします。
設定テンプレート適用の実行確認画面が表示されます。

7. ［OK］をクリックして、設定テンプレートを適用します。

8. 適用が完了したというメッセージが表示されたら、［OK］をクリックします。

9. ［結果の詳細］をクリックして、適用内容を確認します。
適用した項目でが表示されていれば、適用は成功です。

10. ［閉じる］をクリックします。

スキャンに必要な設定

メールサーバーを登録する

設定の前に以下を確認してください。

- スキャナーがネットワークに接続されているか
- メールサーバーの設定情報
  インターネット上のメールサーバーを利用する場合は、サービスを提供しているプロバイダーやウェブサイトから設定情報を確認してください。

登録方法

WebConfigを起動し、［ネットワーク］タブ -［メールサーバー］-［基本］の順に選択します。

「ブラウザーでWeb Configを起動する」35ページ

スキャナーの操作パネルでも設定できます。［設定］-［ネットワーク設定］-［応用設定］-［メールサーバー］-［サーバー設定］の順に選択します。

メールサーバーの設定項目

項目	設定値と説明	
認証方式	スキャナーがメールサーバーにアクセスする際の認証方式を指定します。 **Microsoft Exchange Onlineをお使いのとき：** Microsoft Exchange Onlineのセキュリティー強化により、従来の「Basic認証」方式が廃止され、SMTP認証（SMTP AUTH）が初期設定で無効化されました。そのため、今後メールサービスを利用するには、[OAuth2] の認証方式を使う必要があります。スキャナーのメール送信/メール通知機能等を利用される場合は、メールサーバー設定を［OAuth2］認証で設定してください。また、Exchange OnlineでSMTP AUTHを有効にしてください。 「Exchange OnlineでのSMTP AUTHを有効にする」42ページ	
	認証しない（オフ）	メールサーバーとの通信時に認証をしません。
	SMTP認証	メールサーバーがSMTP認証に対応している必要があります。
	POP before SMTP	選択した場合はPOP3サーバーの設定をしてください。
	OAuth2	選択した場合はメールサービスの設定をしてください。
メールサービス	［認証方式］で［OAuth2］を選択した場合、リストからメールサービスを選択します。［サインイン］をクリックし、画面の指示に従ってメールサービスにサインインしてください。 「メールサーバーのOAuth 2.0認証を設定する」42ページ 参考 個人でご利用の場合は［Outlook.com］を選択します。	
認証用アカウント	［認証方式］で［SMTP認証］または［POP before SMTP］を選択した場合、認証用のアカウント名を入力します。入力できる文字は、ASCII（0x20-0x7E）の255文字以内です。	
認証用パスワード	［認証方式］で［SMTP認証］または［POP before SMTP］を選択した場合、認証用のパスワードを入力します。入力できる文字はASCII（0x20-0x7E）の70文字以内です。	
送信元アドレス	スキャナーからメールを送信する際、送信者となるメールアドレスを設定します。既存のメールアドレスも設定可能ですが、スキャナーから送信されたメールと判別できるように、専用のメールアドレスを取得して設定することをお勧めします。 入力できる文字は、: ( ) < > [ ] ; ¥ を除くASCII (0x20-0x7E)で表せる255文字以内です。ただし、ピリオド（.）は先頭文字にできません。	
SMTPサーバーアドレス	A～Z a～z 0～9 . - を使用し、255文字以内で入力します。IPv4形式とFQDN形式での入力が可能です。	

項目	設定値と説明	
SMTPサーバー ポート番号	1～65535までの範囲で、半角数字で入力します。	
セキュア接続	メールサーバーのセキュア接続方式を指定します。	
	なし	［認証方式］で［POP before SMTP］を選択した場合は［なし］になります。
	SSL/TLS	［認証方式］で［認証しない］または［SMTP認証］を選択したときに選択できます。
	STARTTLS	［認証方式］で［認証しない］または［SMTP認証］を選択したときに選択できます。
証明書の検証（Web Configのみ）	有効にするとメールサーバーの証明書の正当性をチェックします。［セキュア接続］で［なし］以外を選択したときは、［有効］にすることをお勧めします。	
POP3サーバーアドレス	［認証方式］で［POP before SMTP］を選択した場合、POP3サーバーアドレスを入力します。入力できる文字は、A～Z a～z 0～9 . - で、255文字以内です。IPv4形式とFQDN形式での入力が可能です。	
POP3サーバー ポート番号	［認証方式］で［POP before SMTP］を選択した場合にポート番号を指定します。入力できる文字は、1～65535の範囲で、半角数字で入力します。	

Exchange OnlineでのSMTP AUTHを有効にする

本製品はSMTPのプロトコルを使用してメール送信するため、Exchange OnlineのSMTP AUTHを有効にする必要があります。
詳細の手順は、「Microsoft Learn」サイトをご覧ください。

設定手順

- ［Exchange 管理センター］で、組織全体の［セキュリティの既定値群］を無効にして、SMTP AUTHを有効にしてください。
- ［Microsoft365管理センター］で、製品の管理者用のメールボックスに対してSMTP AUTHを有効にしてください。

メールサーバーのOAuth 2.0認証を設定する

Web Configを使ってメールサーバーにOAuth 2.0認証を設定します。

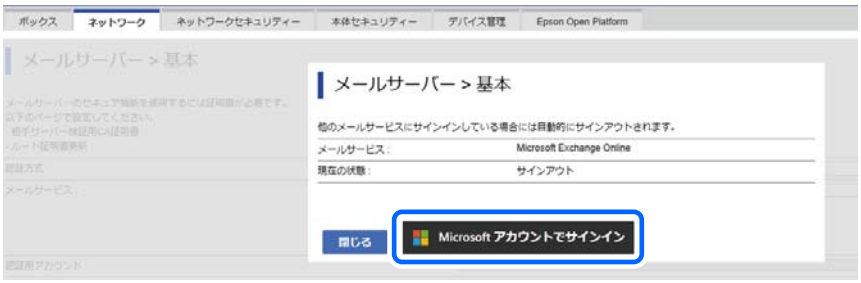
1. Web Configを起動します。
   「ブラウザーでWeb Configを起動する」35ページ
2. ［ネットワーク］タブ-［メールサーバー］-［基本］の順に選択します。
3. ［認証方式］で［OAuth2］を選択します。

4. ［メールサービス］で［Microsoft Exchange Online］を選択します。

   参考 個人でご利用の場合は［Outlook.com］を選択します。

5. サインインします。

   ［サインイン］をクリックして、表示される画面で［Microsoft アカウントでサインイン］をクリックします。



6. 画面に表示される認証コードをコピーして、表示されているURLをクリックします。

7. アクセス許可コードの入力画面で、コピーした認証コードを貼り付けて［次へ］をクリックします。

8. Microsoft サインインの画面で、ご利用のMicrosoftアカウントを入力して［次へ］をクリックします。

   サインインするためには、アカウントに最低限［クラウド アプリケーション管理者］ロールが割り当てられている必要があります。

9. パスワードを入力して、［サインイン］をクリックします。

   参考 追加の手順が求められたときは、画面の指示に従ってサインインしてください。

10. 要求されているアクセス許可画面で「組織の代理として同意する」にチェックをして［承諾］をクリックします。

    認証が完了すると、サインインのメッセージが表示されるのでブラウザーの画面を閉じます。

Web Configの［ネットワーク］タブ-［メールサーバー］-［基本］のページでサインインの状態が確認できます。

サインインが完了すると、OAuth 2.0認証のアカウント情報等が表示されるようになります。

11. ［設定］をクリックし、設定情報を製品に送信します。

メールサーバーとの接続を確認する

メールサーバーとの接続確認ができます。

1. スキャナーのIPアドレスをブラウザーに入力して、Web Configを起動します。
2. 管理者パスワードを入力して、管理者としてログオンします。
3. 以下の順に選択します。
   ［ネットワーク］タブ-［メールサーバー］-［接続確認］
4. ［確認開始］を選択します。
   メールサーバーとの接続診断が開始されます。テストが終了すると結果が表示されます。

   参考 操作パネルを使ってもメールサーバーとの接続を確認できます。メニューは以下の通りです。
   ［設定］-［ネットワーク設定］-［詳細設定］-［メールサーバー］-［コネクションテスト］

メールサーバー接続確認結果

メッセージ	原因
接続に成功しました。	サーバーとの接続に成功した場合に表示されます。
SMTPサーバーとの通信でエラーが発生しました。以下を確認してください。 ・ネットワーク設定	以下のような場合に通信エラーが表示されます。 • スキャナーがネットワークに接続されていない • SMTPサーバーがダウンしている • 通信中にネットワークが切断された • 異常なデータを受信した

メッセージ	原因
POP3サーバーとの通信でエラーが発生しました。以下を確認してください。 ・ネットワーク設定	以下のような場合に通信エラーが表示されます。 • スキャナーがネットワークに接続されていない • POP3サーバーがダウンしている • 通信中にネットワークが切断された • 異常なデータを受信した
SMTPサーバーとの接続に問題があります。以下を確認してください。 ・SMTPサーバーアドレス ・DNSサーバー	以下のような場合に通信エラーが表示されます。 • DNSサーバーとの接続に失敗した • SMTPサーバーアドレスの名前解決に失敗した
POP3サーバーとの接続に問題があります。以下を確認してください。 ・POP3サーバーアドレス ・DNSサーバー	以下のような場合に通信エラーが表示されます。 • DNSサーバーとの接続に失敗した • POP3サーバーアドレスの名前解決に失敗した
SMTPサーバーの認証に失敗しました。以下を確認してください。 ・認証方式 ・認証用アカウント ・認証用パスワード	SMTPサーバーでの認証処理に失敗したときに表示されます。
POP3サーバーの認証に失敗しました。以下を確認してください。 ・認証方式 ・認証用アカウント ・認証用パスワード	POP3サーバーでの認証処理に失敗したときに表示されます。
サポートしていない通信方式です。以下を確認してください。 ・SMTPサーバーアドレス ・SMTPサーバーポート番号	サポートしていないプロトコルで通信しようとした場合に表示されます。
SMTPサーバーとの接続に失敗しました。セキュア接続をなしに変更してください。	サーバーとクライアントでSMTPセキュア接続の設定が合っていない、またはサーバーがSMTPセキュア接続（SSL接続）をサポートしていない場合に表示されます。
SMTPサーバーとの接続に失敗しました。セキュア接続をSSL/TLSに変更してください。	サーバーとクライアントでSMTPセキュア接続の設定が合っていない、またはサーバーがSMTPセキュア接続にSSL/TLS接続することを要求してきている場合に表示されます。
SMTPサーバーとの接続に失敗しました。セキュア接続をSTARTTLSに変更してください。	サーバーとクライアントでSMTPセキュア接続の設定が合っていない、またはサーバーがSMTPセキュア接続にSTARTTLS接続することを要求してきている場合に表示されます。
サーバーの安全性が確認できませんでした。以下を確認してください。 ・日付/時刻	スキャナーの日時設定が正しくない、またはサーバーに対応するルート証明書は保有しているが、期限切れの場合に表示されます。
サーバーの安全性が確認できませんでした。以下を確認してください。 ・相手サーバー検証用CA証明書	サーバーに対応するルート証明書をスキャナーが保有していない、または相手サーバー検証用CA証明書がインポートされていない場合に表示されます。
サーバーの安全性が確認できませんでした。	サーバーから取得した証明書が壊れている場合などに表示されます。
SMTPサーバーの認証に失敗しました。認証方式をSMTP認証に変更してください。	サーバーとクライアントで認証方式が一致していない場合に表示されます。サーバーはSMTP認証をサポートしているのに、製品はSMTP認証を実行していません。

メッセージ	原因
SMTPサーバーの認証に失敗しました。認証方式をPOP before SMTPに変更してください。	サーバーとクライアントで認証方式が一致していない場合に表示されます。サーバーはSMTP認証をしていないのに、製品はSMTP認証を実行しようとしています。
送信元アドレスが正しくありません。お使いのメールサービスで取得したアドレスに変更してください。	送信元アドレスの指定が間違っていた場合に表示されます。
製品は処理動作中のためアクセスできません。	スキャナーが動作中で接続設定ができなかったときに表示されます。

共有フォルダーを設定する

スキャンした画像を保存するための共有フォルダーを設定します。
ファイルを保存するとき、スキャナーは共有フォルダーのあるコンピューターに、コンピューターのユーザーとしてログオンします。

共有フォルダーの作成

関連情報

- 「共有フォルダーを作成する前に」46ページ
- 「ネットワークプロファイルの確認」47ページ
- 「共有フォルダーの作成場所とセキュリティーの例」47ページ
- 「アクセス許可をするグループやユーザーを追加する」60ページ

共有フォルダーを作成する前に

共有フォルダーの作成前に以下を確認してください。

- スキャナーが共有フォルダーを作成するコンピューターにアクセスできるネットワークに接続されているか
- 共有フォルダーを作成するコンピューターの名前にマルチバイト文字が使用されていないか

重要 コンピューター名にマルチバイト文字が含まれていると、共有フォルダーへのファイル保存が失敗する可能性があります。
その場合、コンピューター名にマルチバイト文字が含まれていないコンピューターに変更するか、コンピューター名を変更してください。
コンピューター名を変更する場合、コンピューターの管理やリソースへのアクセスに影響が出る可能性がありますので、必ずシステムの管理者に確認してから行ってください。

ネットワークプロファイルの確認

共有フォルダーを作成するコンピューターで、フォルダーの共有が可能かどうか確認します。

1. 共有フォルダーを作成するコンピューターへ管理者権限のユーザーアカウントでログオンします。
2. ［コントロール パネル］ - ［ネットワークとインターネット］ - ［ネットワークと共有センター］を選択します。
3. ［共有の詳細設定の変更］をクリックし、表示されたネットワークプロファイルから［（現在のプロファイル）］とあるプロファイルの をクリックします。
4. ［ファイルとプリンターの共有］で［ファイルとプリンターの共有を有効にする］が選択されているか確認します。
   選択されている場合は、［キャンセル］をクリックして画面を閉じます。
   変更した場合は、［変更の保存］をクリックして画面を閉じます。

共有フォルダーの作成場所とセキュリティーの例

共有フォルダーを作成する場所によって、セキュリティーや利便性が変わります。
スキャナーや他のコンピューターから共有フォルダーを扱うには、以下の両方でフォルダーの読み取りや変更の権限が必要です。

- ［共有］タブ - ［詳細な共有］ - ［アクセス許可］の共有アクセス許可
  ネットワーク経由のアクセスを制御します。
- ［セキュリティ］タブのアクセス許可
  ネットワークとローカルからのアクセスを制御します。

以下のデスクトップに共有フォルダーを作成した例で、共有フォルダーの［共有アクセス許可］に［Everyone］を設定すると、ネットワーク経由で共有フォルダーにアクセスできる全てのユーザーにアクセス許可を与えることになります。しかし、デスクトップはユーザーフォルダーの配下にあるフォルダーのため、ユーザーフォルダーのローカルアクセスのセキュリティー設定が継承されて、ユーザーフォルダーにアクセス許可のないユーザーはアクセスできません。［セキュリティ］でアクセス許可が設定されているユーザーやグループ（この場合はコンピューターのログオンユーザーとAdministrator）がフォルダーにアクセスできます。
以下の例を参考に適切な場所に共有フォルダーを作成してください。
ここでは「scan_folder」というフォルダーの作成を例に説明します。

関連情報

➡ 「ファイルサーバー向けの設定例」47ページ
➡ 「個人のコンピューター向けの設定例」54ページ

ファイルサーバー向けの設定例

ここでは、以下の環境条件でファイルサーバーなど共有コンピューターのドライブのルートに共有フォルダーを作成することを例に説明します。
共有フォルダーを作成するコンピューターと同じドメインなどアクセス制御できるユーザーがアクセスできます。
ファイルサーバーや共有のコンピューターなどを設置していて、組織内の誰にでも自由な読み書きを許可する場合に設定してください。

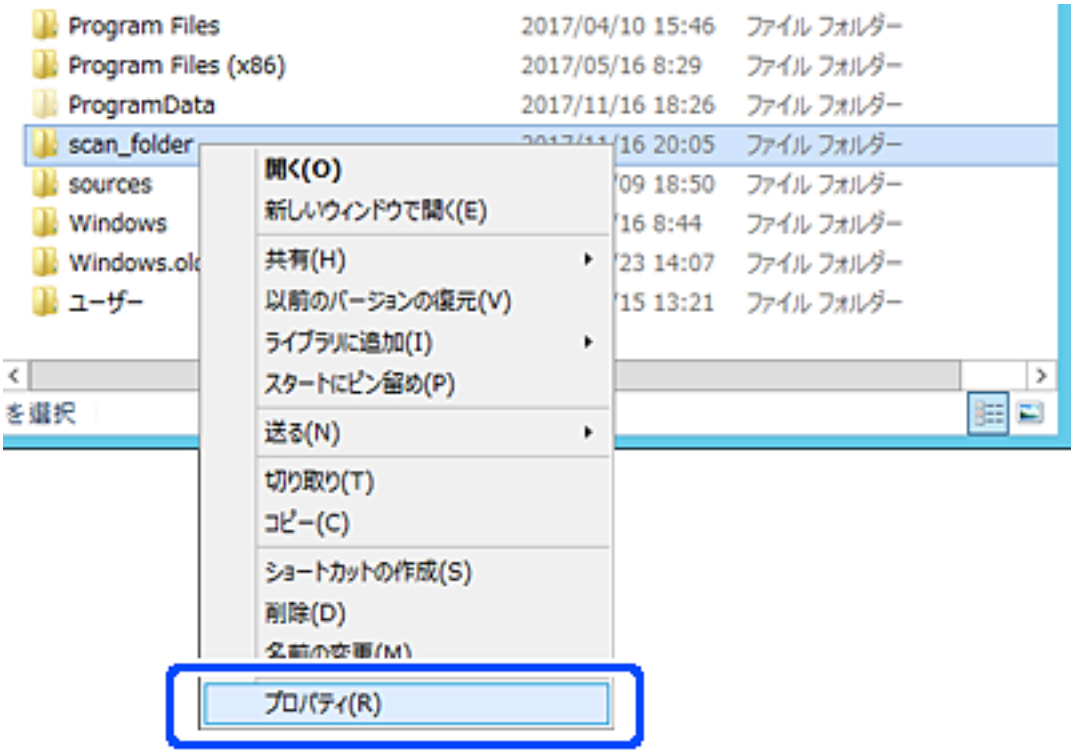
- フォルダー作成場所：ドライブ直下
- フォルダーパス：C:¥scan_folder
- ネットワーク経由のアクセス設定（共有アクセス許可）：Everyone
- ファイルシステムのアクセス設定（セキュリティ）：Authenticated Users

1. 共有フォルダーを作成するコンピューターへ管理者権限のユーザーアカウントでログオンします。

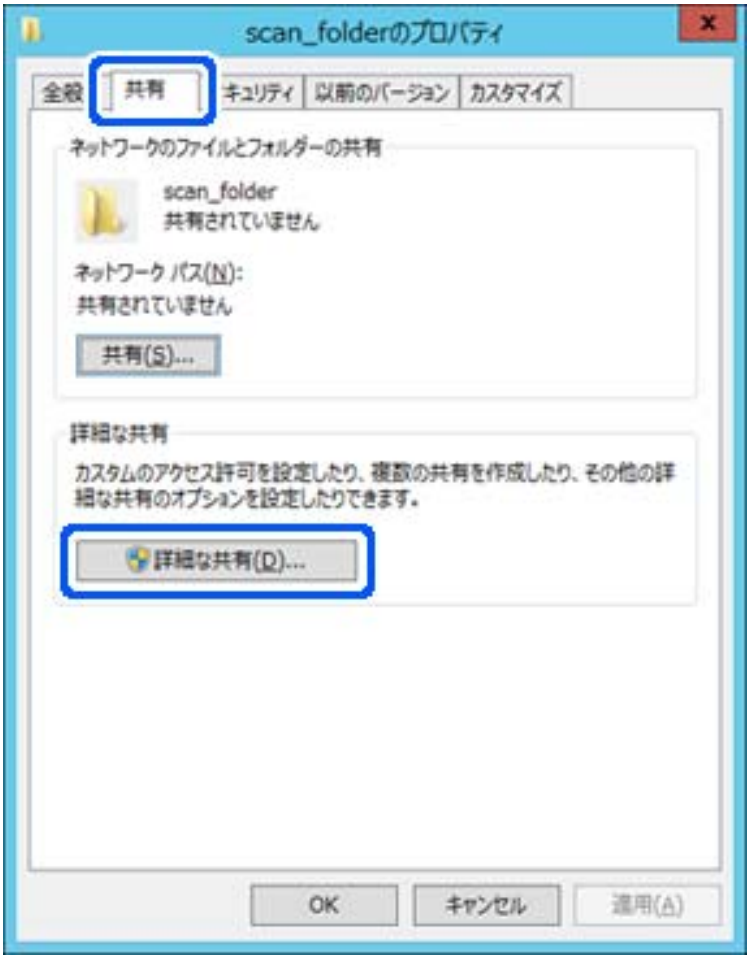
2. エクスプローラーを起動します。

3. Cドライブのルートにフォルダーを作成し「scan_folder」と名前を付けます。
   フォルダー名は、半角英数字12文字以内で入力してください。文字数を超えると、お使いの環境によっては正常にアクセスできないことがあります。

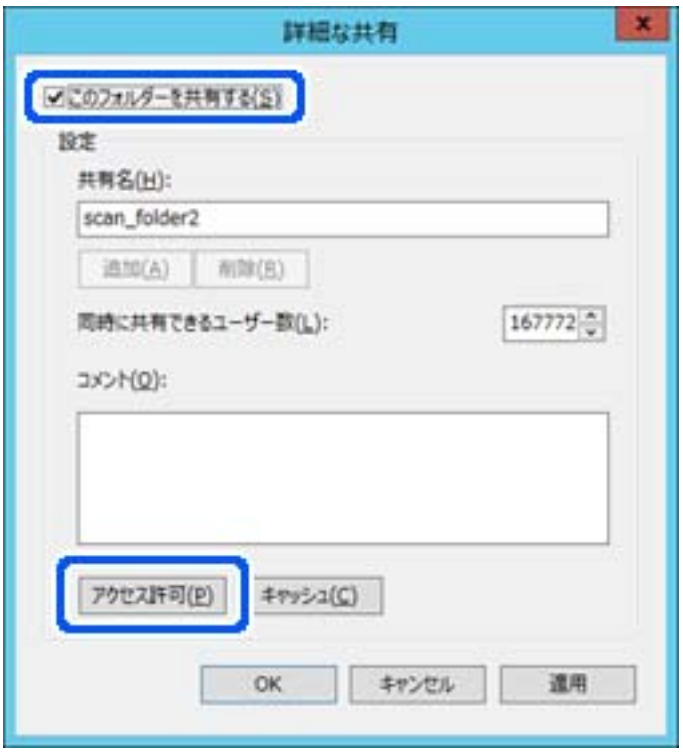
4. フォルダーを右クリックして［プロパティ］を選択します。



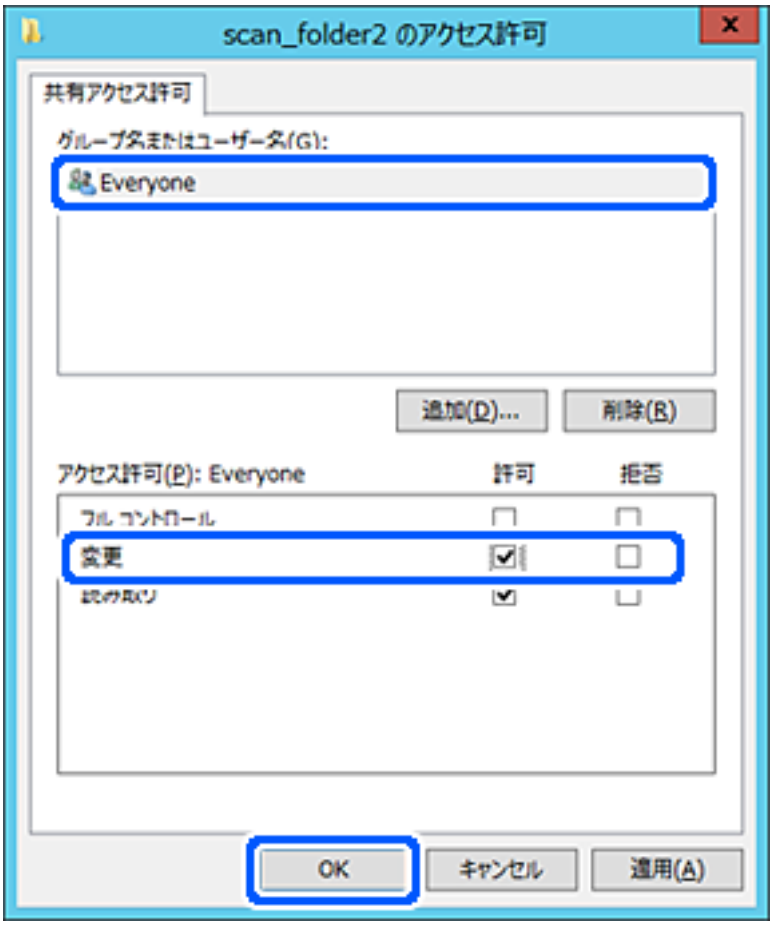
5. ［共有］タブで［詳細な共有］をクリックします。



6. ［このフォルダーを共有する］にチェックを入れ、［アクセス許可］をクリックします。

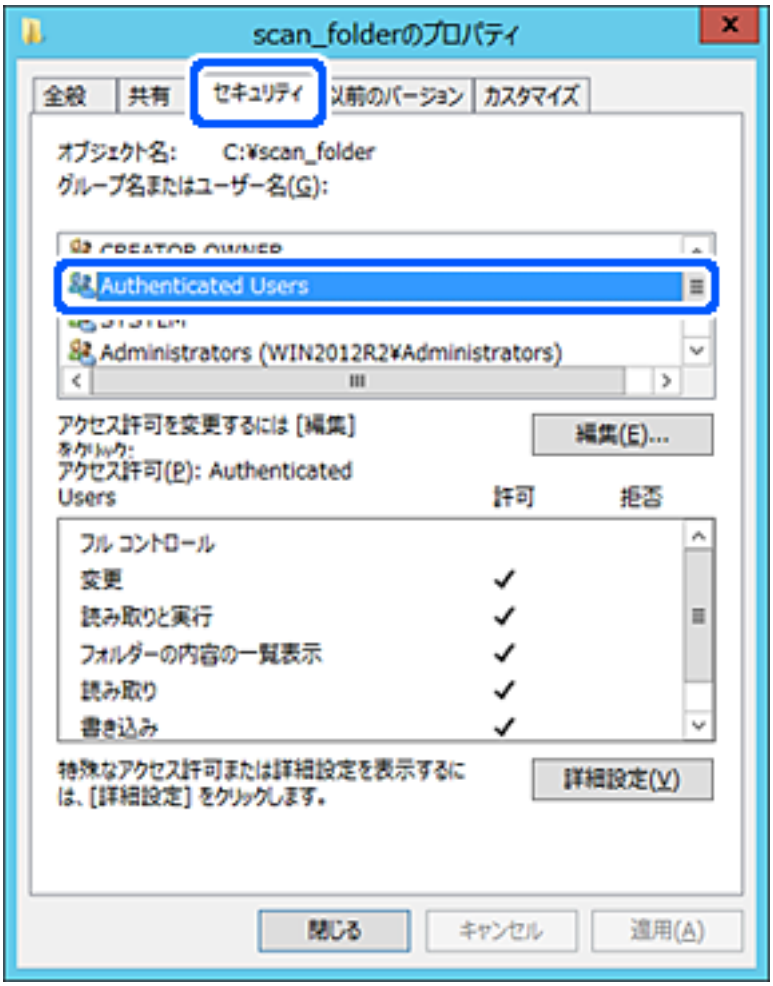


7. ［グループ名またはユーザー名］の［Everyone］グループを選択し、［変更］ の［許可］にチェックを入れて［OK］をクリックします。



8. ［OK］をクリックします。

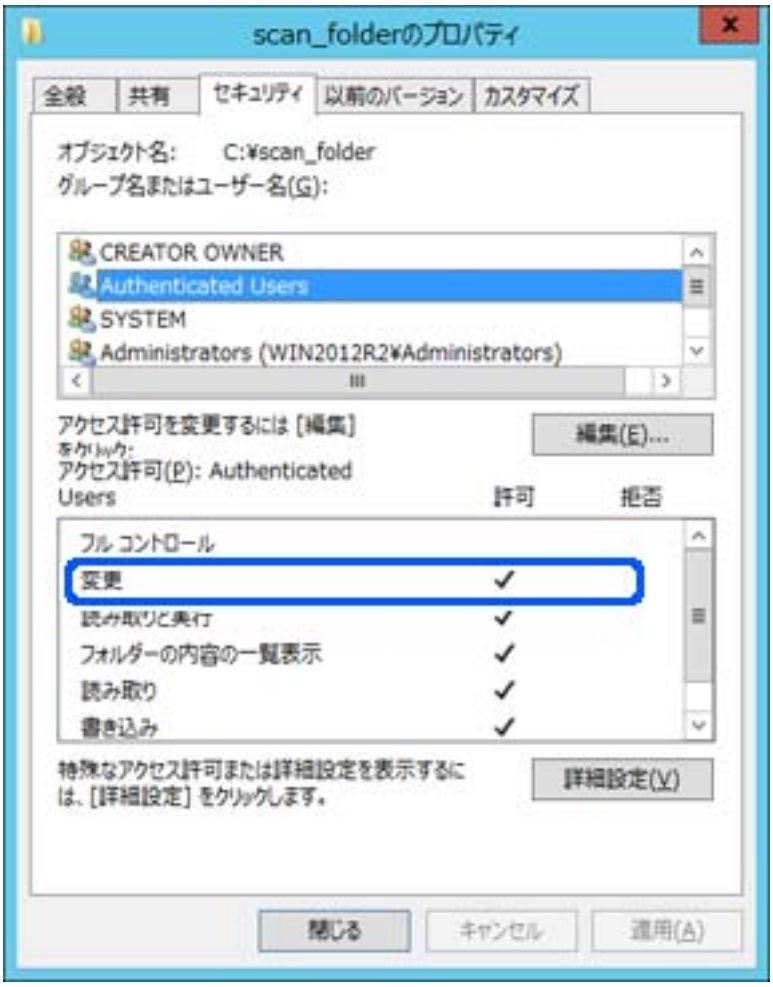
9. ［セキュリティ］タブを選択し、［グループ名またはユーザー名］にある［Authenticated Users］を選択します。



「Authenticated Users」はドメインやコンピューターにログオンできる全てのユーザーが含まれるグループです。ドライブ直下にフォルダーを作成した場合に表示される特殊グループです。
表示されていない場合は［編集］から追加できます。詳しくは「関連情報」にあるトピックをご覧ください。

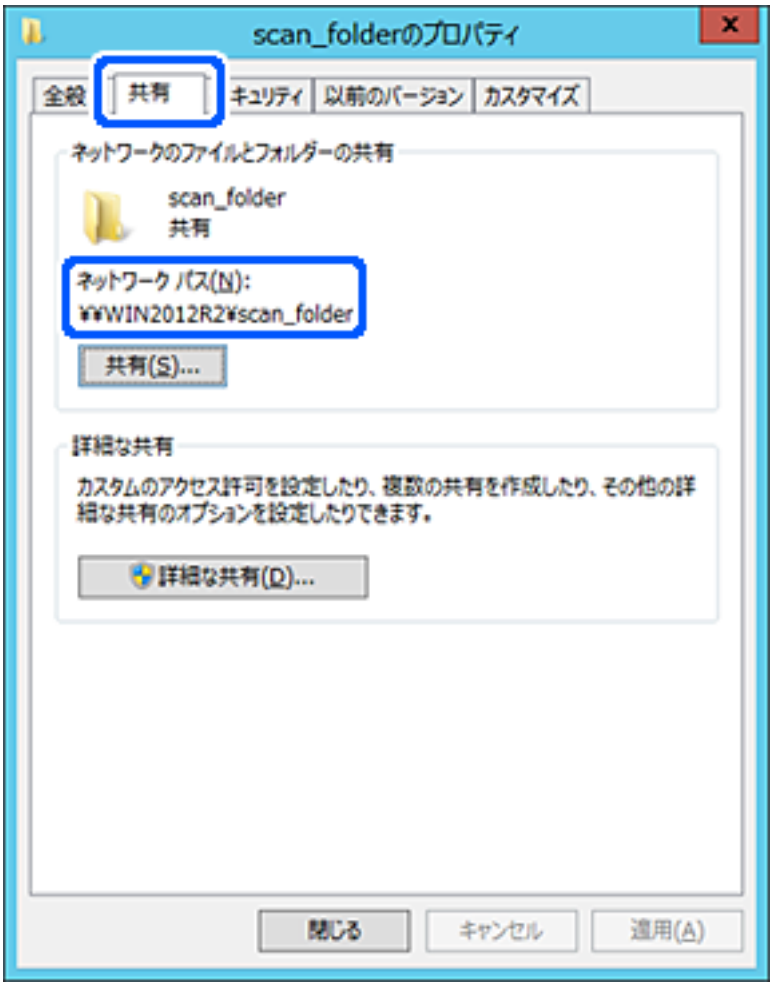
10. ［Authenticated Usersのアクセス許可］にある［変更］の［許可］にチェックがあることを確認します。

    チェックがない場合は［Authenticated Users］を選択して［編集］をクリックし、［アクセス許可］で［変更］の［許可］にチェックを入れ、［OK］をクリックします。



11. ［共有］タブを選択します。

共有フォルダーのネットワークパスが表示されます。このパスをスキャナーのアドレス帳の登録で使用します。メモやコピーをしておいてください。



12. ［OK］または［閉じる］をクリックして、画面を閉じます。

同じドメインネットワークのコンピューターから、共有フォルダーにファイルが読み書きできるか確認してください。

関連情報

➡ 「アクセス許可をするグループやユーザーを追加する」60ページ
➡ 「Web Configで宛先を登録する」65ページ

個人のコンピューター向けの設定例

ここでは、ログオンしているユーザーのデスクトップに共有フォルダーを作成することを例に説明します。
デスクトップやドキュメントフォルダーなどユーザーフォルダー配下のフォルダーは、ログオンしたユーザーとコンピューターの管理者権限を持つユーザーがアクセスできます。
個人のコンピューターにスキャン結果を保存し、ネットワーク経由で他のユーザーに閲覧やコピー、削除などを許可しない場合に設定してください。

- フォルダー作成場所：デスクトップ

- フォルダーパス：C:￥Users￥xxxx￥Desktop￥scan_folder
- ネットワーク経由のアクセス設定（共有アクセス許可）：Everyone
- ファイルシステムのアクセス設定（セキュリティ）：追加しない、または個別にアクセスを許可するユーザーまたはグループ

1. 共有フォルダーを作成するコンピューターへ管理者権限のユーザーアカウントでログオンします。

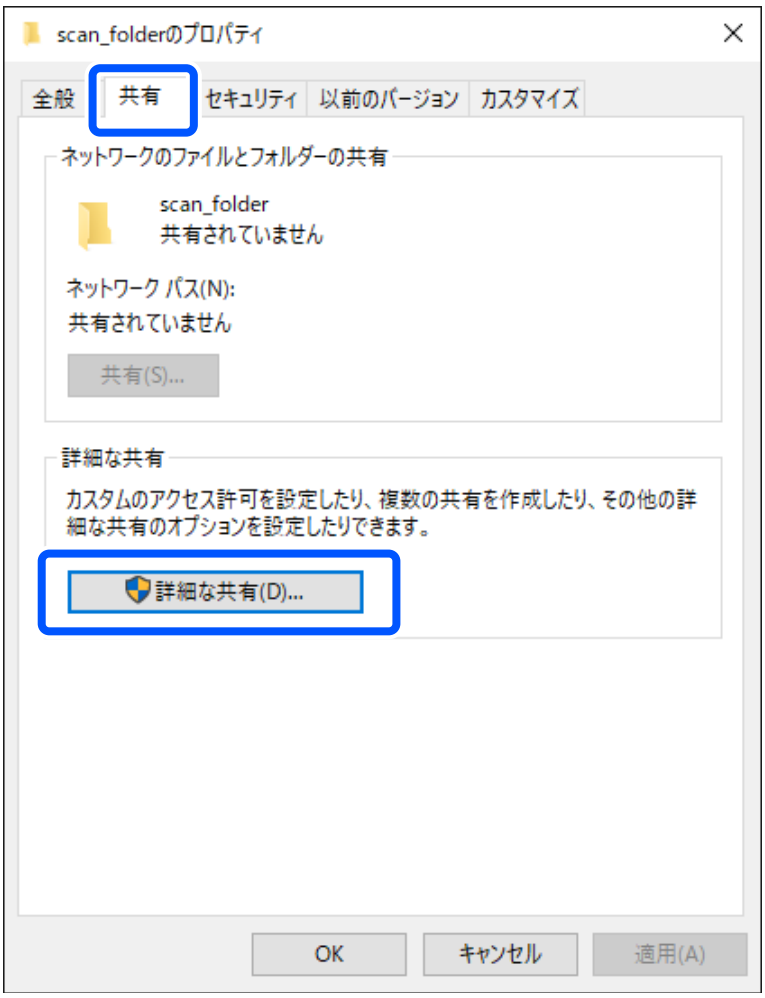
2. エクスプローラーを起動します。

3. デスクトップにフォルダーを作成し「scan_folder」と名前を付けます。

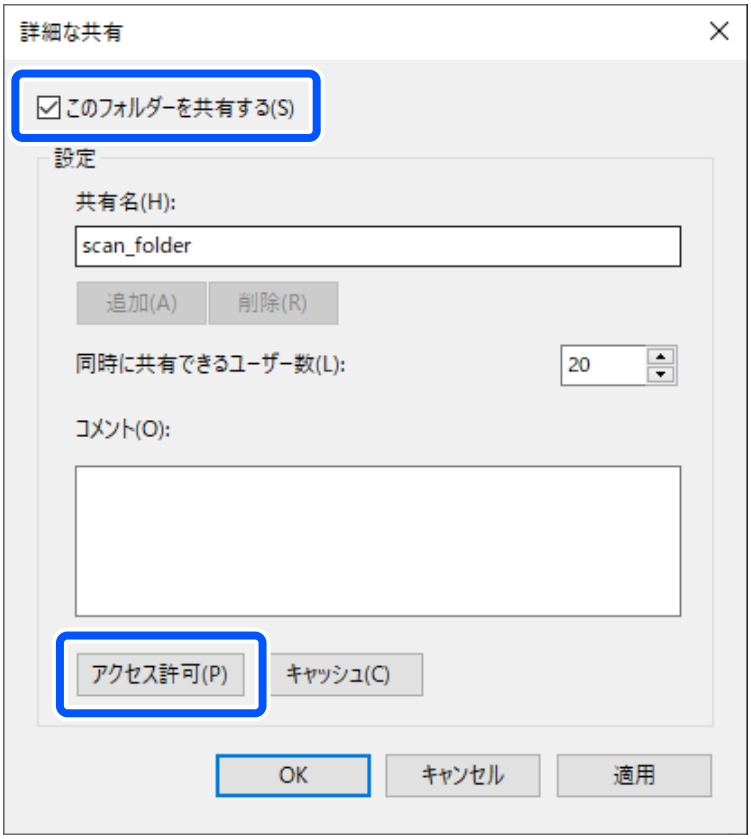
   フォルダー名は、半角英数字12文字以内で入力してください。文字数を超えると、お使いの環境によっては正常にアクセスできないことがあります。

4. フォルダーを右クリックして［プロパティ］を選択します。

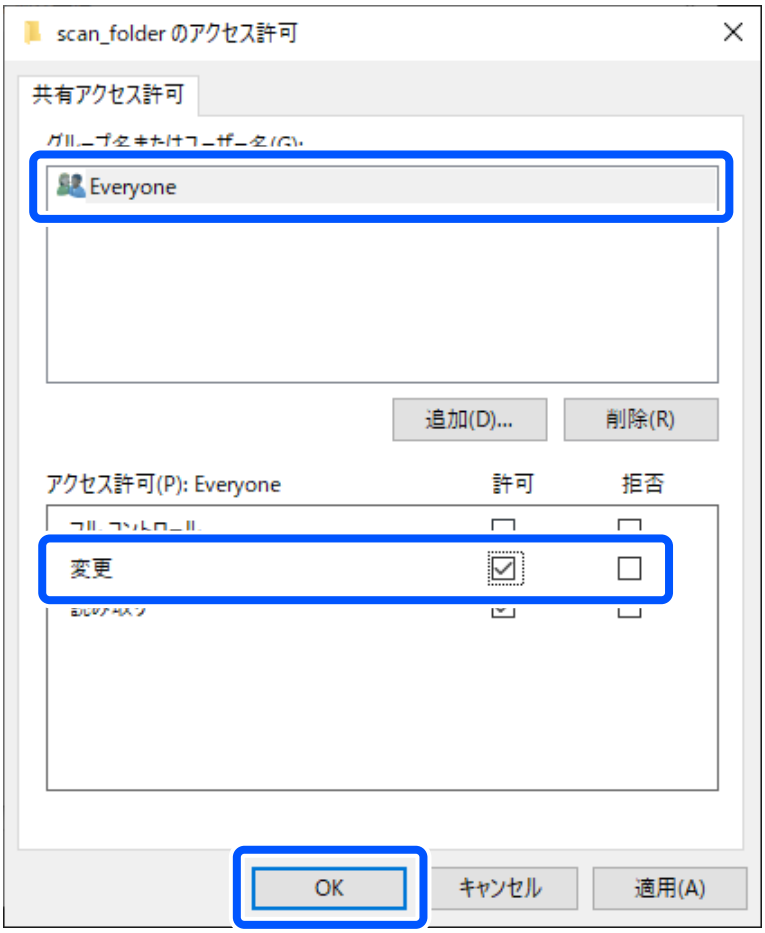
5. ［共有］タブの画面で［詳細な共有］をクリックします。



6. ［このフォルダーを共有する］にチェックを入れ、［アクセス許可］をクリックします。



7. ［グループ名またはユーザー名］の［Everyone］グループを選択し、［変更］ の［許可］にチェックを入れて［OK］をクリックします。



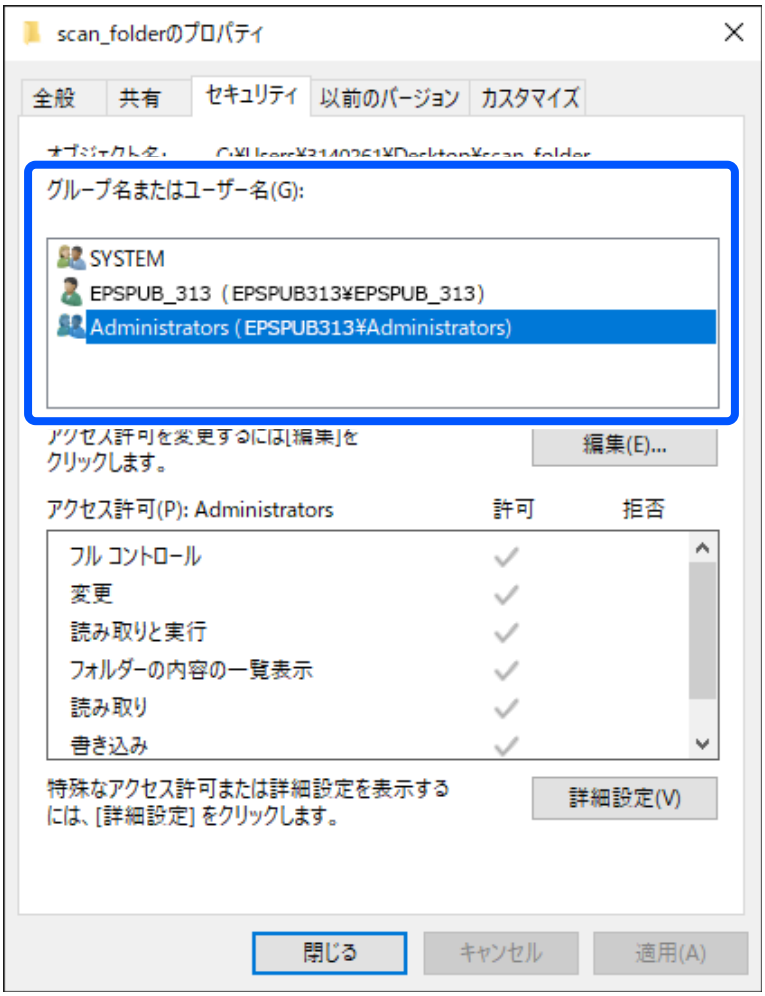
8. ［OK］をクリックします。

9. ［セキュリティ］タブを選択します。

10. ［グループ名またはユーザー名］にあるグループまたはユーザーを確認します。

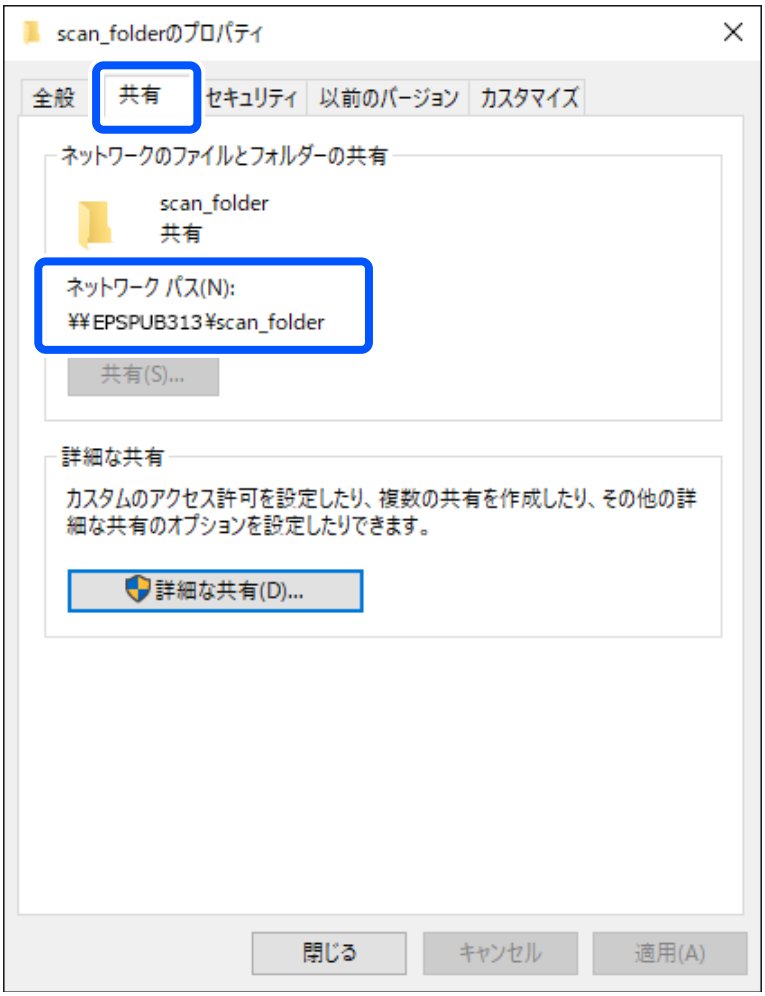
ここに表示されているグループまたはユーザーが共有フォルダーにアクセスできます。
この場合はこのコンピューターにログオンしているユーザーとAdministratorが共有フォルダーにアクセスできます。

必要に応じてアクセス許可を追加してください。アクセス許可は [編集] から追加できます。詳しくは「関連情報」にあるトピックをご覧ください。



11. ［共有］タブを選択します。

共有フォルダーのネットワークパスが表示されます。このパスをスキャナーのアドレス帳の登録で使用します。メモやコピーをしておいてください。



12. ［OK］または［閉じる］をクリックして、画面を閉じます。

アクセスを許可したユーザーまたはグループのコンピューターから、共有フォルダーにファイルが読み書きできるか確認してください。

関連情報

➡ 「アクセス許可をするグループやユーザーを追加する」60ページ
➡ 「Web Configで宛先を登録する」65ページ

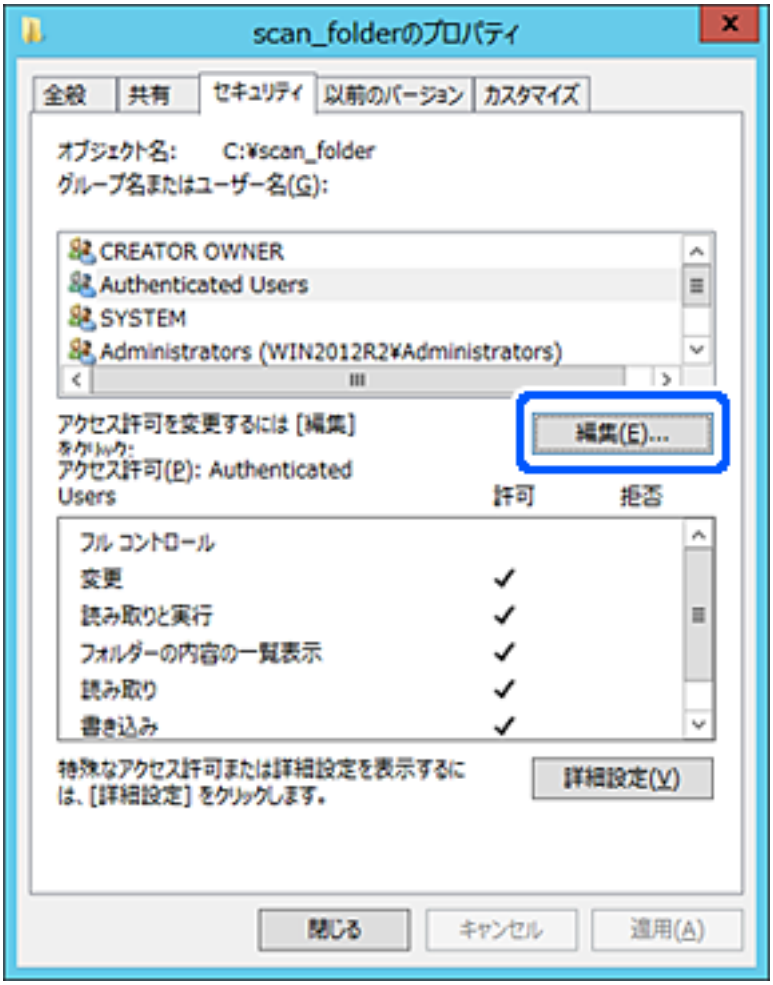
アクセス許可をするグループやユーザーを追加する

以下の手順で共有フォルダーにアクセスを許可するグループやユーザーを追加できます。

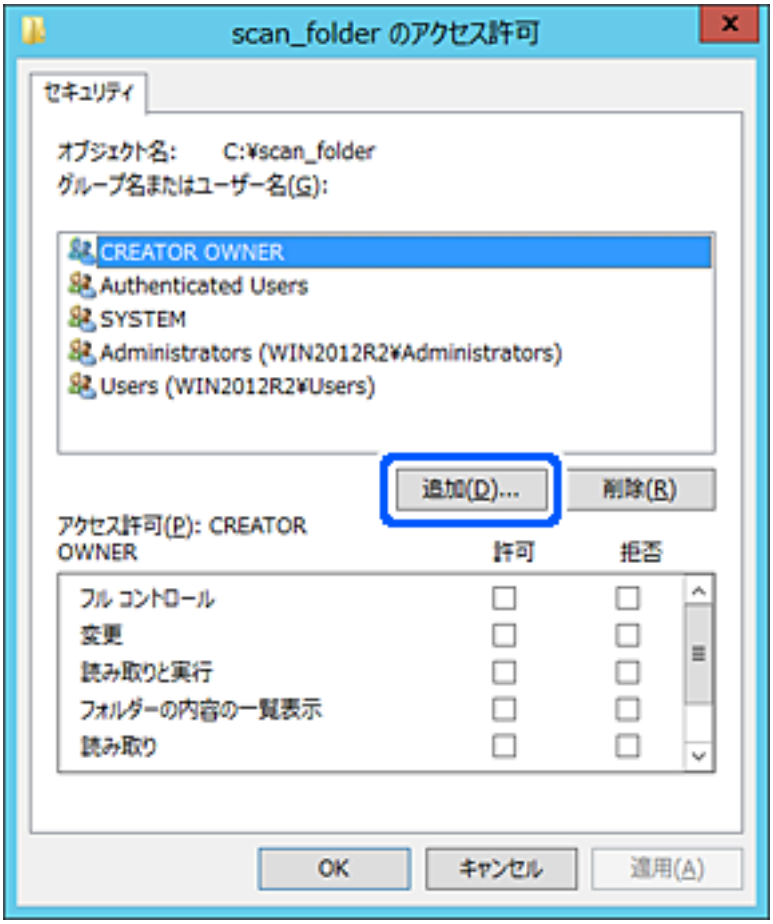
1. フォルダーを右クリックして［プロパティ］を選択します。

2. ［セキュリティ］タブを選択します。

3. ［編集］をクリックします。



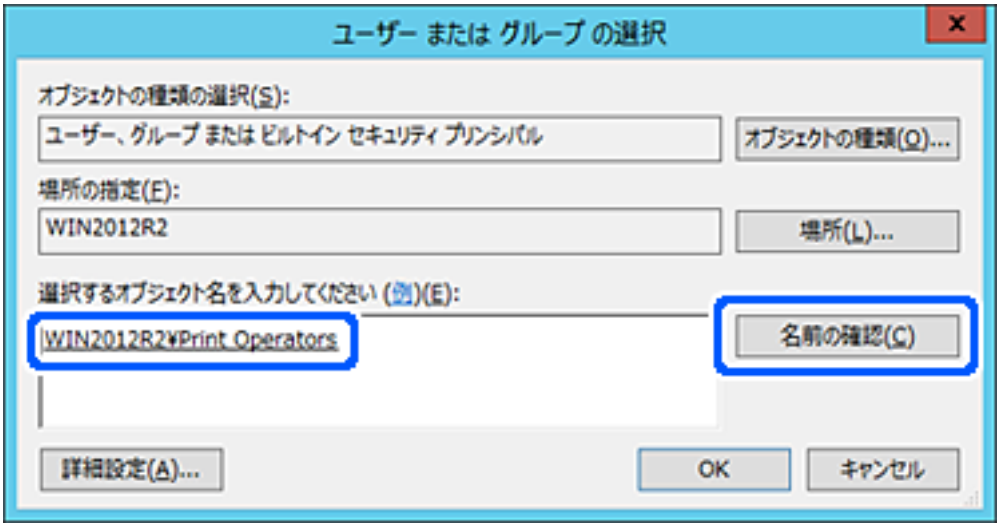
4. ［グループ名またはユーザー名］の下の［追加］をクリックします。



5. アクセスを許可したいグループやユーザー名を入力し、［名前の確認］をクリックします。

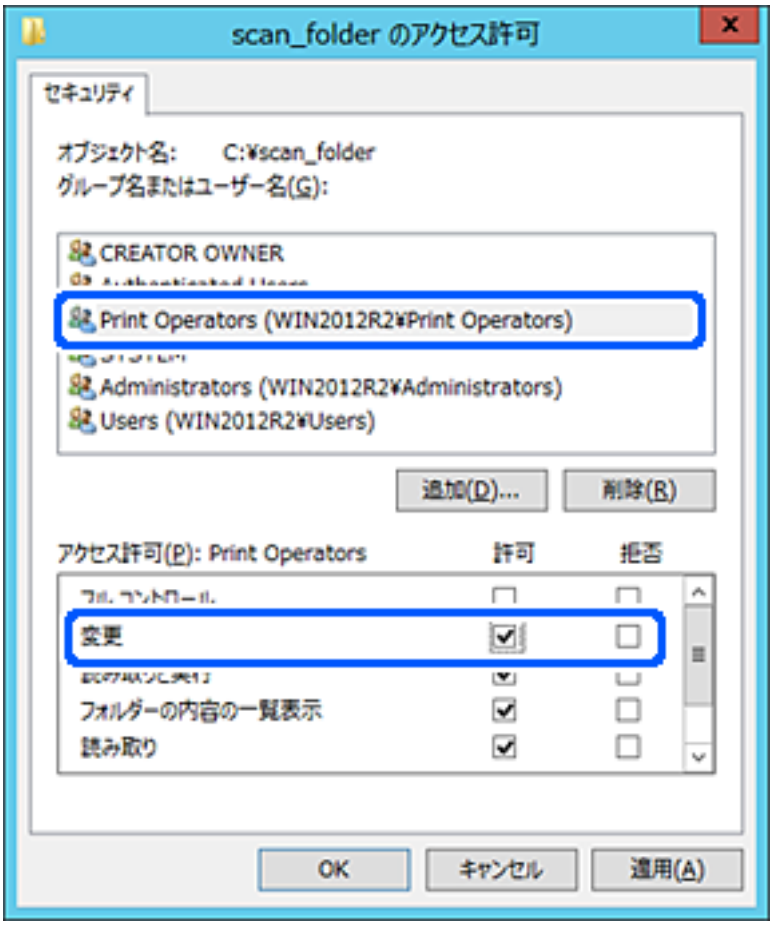
名前に下線が入ります。

参考 グループやユーザーの完全な名前がわからない場合は、名前の一部を入力して［名前の確認］をクリックしてください。名前の一部が合致するグループやユーザー名が一覧表示され、そこから選択することができます。
一つだけ合致した場合は、［選択するオブジェクト名を入力してください］に下線が入った完全な名前が表示されます。



6. ［OK］をクリックします。

7. アクセス許可の画面で、［グループ名またはユーザー名］に入力したユーザー名を選択して［変更］のアクセス許可にチェックを入れ、［OK］をクリックします。



8. ［OK］または［閉じる］をクリックして、画面を閉じます。

アクセスを許可したユーザーまたはグループのコンピューターから、共有フォルダーにファイルが読み書きできるか確認してください。

アドレス帳を使えるようにする

スキャンの宛先をスキャナーのアドレス帳に登録しておくと、簡単に宛先を入力できます。
アドレス帳には以下の送信先を登録できます。300件まで登録できます。

参考 また、LDAPサーバーで管理しているアドレスを利用（LDAP検索）して宛先を入力することもできます。

メール	メールの送信先です。 メールサーバーの設定が必要です。
ネットワークフォルダー	スキャンデータの保存先 あらかじめネットワークフォルダーの準備が必要です。

関連情報

➡ 「LDAPサーバーと利用者を連携する」71ページ

設定ツールによる宛先設定機能差

スキャナーのアドレス帳を設定する機能は3種類あります：Web Config、Epson Device Admin、操作パネルの3つです。ただし、設定できる項目が異なります。

機能	Web Config*	Epson Device Admin	操作パネル
宛先登録	○	○	○
宛先編集	○	○	○
グループ登録	○	○	○
グループ編集	○	○	○
宛先やグループの削除	○	○	○
宛先の一括削除	○	○	-
ファイルのインポート	○	○	-
ファイルへエクスポート	○	○	-

* 設定には管理者ログオンが必要です。

Web Configで宛先を登録する

参考 スキャナーの操作パネルからも登録できます。

1. Web Configで［スキャン］タブ -［アドレス帳］を選択します。
2. 登録したい番号を選択して［編集］をクリックします。
3. ［登録名］と［検索名］を入力します。
4. 設定したい宛先の［種別］を選択します。

   参考 登録した後は［種別］を変更できません。登録した後に種別を変更したいときは、宛先を削除して再登録してください。

5. 必要な項目を設定して、［適用］をクリックします。

関連情報

➡ 「ブラウザーでWeb Configを起動する」35ページ

宛先の設定項目

項目	設定値と説明
共通設定	
登録名	操作パネルでアドレス帳を検索するときに使う名称を、Unicode（UTF-16）で表せる30文字以内で入力します。指定しない場合は空白にします。
検索名	スキャナーのアドレス帳の検索に使われる名称を、Unicode（UTF-16）で表せる30文字以内で入力します。指定しない場合は空白にします。
種別	登録する宛先の種類を選択します。
常用指定	宛先を常用登録します。 常用に設定するとスキャンのトップ画面に表示され、アドレス帳を開かなくても宛先を指定できるようになります。
メール	
メールアドレス	A～Z a～z 0～9 ! # $ % & ' * + - . / = ? ^ _ { | } ~ @を使用し、1～255文字以内の半角で入力します。
ネットワークフォルダー (SMB)	
保存先	￥￥“フォルダーパス” 保存先フォルダーのパスを、Unicode（UTF-16）で表せる1～253文字以内（"￥￥"を除く）で入力します。 ブラウザーによっては、円マークがバックスラッシュで表示されることがあります。 フォルダーのプロパティ画面に表示されるネットワークパスを入力します。ネットワークパスの設定の詳細は、以下をご覧ください。 「個人のコンピューター向けの設定例」54ページ
ユーザー名	ネットワークフォルダーにアクセスするためのユーザー名をUnicode（UTF-16）で表せる30文字以内で入力します。ただし、制御文字（0x00～0x1f、0x7F）は除きます。
パスワード	ネットワークフォルダーのパスワードを、Unicode（UTF-16）で表せる0～20文字以内で入力します。ただし、制御文字（0x00～0x1f、0x7F）は除きます。
FTP	
セキュア接続	FTPサーバーがサポートしているプロトコルに従って、FTPまたはFTPSを選択します。［FTPS］を選択するとセキュアで通信します。
保存先	サーバー名を、Unicode（UTF-16）で表せる1～253文字以内（"ftp://"や"ftps://"を除く）で入力します。
ユーザー名	FTPサーバーにアクセスするユーザー名を、Unicode（UTF-16）で表せる30文字以内で入力します。ただし、制御文字（0x00～0x1f、0x7F）は除きます。匿名による接続を認めているサーバーでは、AnonymousやFTPなどを入力します。指定しない場合は空白にします。
パスワード	FTPサーバーにアクセスするパスワードを、Unicode（UTF-16）で表せる0～20文字以内で入力します。ただし、制御文字（0x00～0x1f、0x7F）は除きます。指定しない場合は空白にします。

項目	設定値と説明
接続モード	メニューから接続モードを選択します。スキャナーとFTPサーバーの間にファイアウォールがある場合は、［パッシブモード］を選択します。
ポート番号	FTPサーバーのポート番号を1～65535以内の数字で入力します。
証明書の検証	有効にするとFTPサーバーの証明書の正当性をチェックします。［セキュア接続］が［FTPS］のときに選択できます。 設定の前に相手サーバー検証用CA証明書をスキャナーにインポートしておいてください。
SharePoint(WebDAV)*	
セキュア接続	サーバーがサポートしているプロトコルに従って、HTTPまたはHTTPSを選択します。［HTTPS］を選択するとセキュアで通信します。
保存先	サーバー名を、Unicode（UTF-16）で表せる1～253文字以内（"http://"や"https://"を除く）で入力します。
ユーザー名	サーバーにアクセスするユーザー名を、Unicode（UTF-16）で表せる30文字以内で入力します。ただし、制御文字（0x00～0x1f、0x7F）は除きます。指定しない場合は空白にします。
パスワード	サーバーにアクセスするパスワードを、Unicode（UTF-16）で表せる0～20文字以内で入力します。ただし、制御文字（0x00～0x1f、0x7F）は除きます。指定しない場合は空白にします。
証明書の検証	有効にするとサーバーの証明書の正当性をチェックします。［セキュア接続］が［HTTPS］のときに選択できます。 設定の前に相手サーバー検証用CA証明書をスキャナーにインポートしておいてください。
プロキシサーバー	プロキシサーバーを使うかどうかを選択します。

* スキャナーの操作パネルからのネットワークフォルダーへのスキャンは、SharePoint Onlineに対応していません。スキャンした画像をSharePoint Onlineに保存したいときは、Document Capture ProにSharePoint Online Connectorをインストールしてお使いください。詳しくはDocument Capture Proのマニュアルをご覧ください。
https://support.epson.net/dcp/

Web Configで宛先をグループに登録する

種別が［メール］の場合、複数の宛先をまとめてグループとして登録できます。

1. Web Configで［スキャン］タブ -［アドレス帳］を選択します。
2. 登録したい番号を選択して［編集］をクリックします。
3. ［種別］で登録したいグループを選択します。
4. ［グループに入れる宛先］の［選択］をクリックします。
   登録できる宛先が一覧表示されます。

5. グループに登録する宛先を選択して、［選択］をクリックします。

6. ［登録名］と［検索名］を入力します。

7. グループを常用登録するかを選択します。

   参考 アドレスは複数のグループに登録できます。

8. ［適用］をクリックします。

関連情報

➡ 「ブラウザーでWeb Configを起動する」35ページ

アドレス帳のバックアップとインポート

アドレス帳は、Web Configやツールを使用してバックアップやインポートができます。
Web Configの場合、アドレス帳を含めてスキャナー設定をエクスポートするとバックアップできます。バイナリーファイルでエクスポートされるので編集できません。
アドレス帳を含めてスキャナー設定をインポートすると、アドレス帳を上書きします。
Epson Device Adminを使うと、デバイスのプロパティー画面からアドレス帳だけをエクスポートできます。また、パスワードなどセキュリティー項目を含めずにエクスポートするとSYLK形式やCSV形式に保存できるので、編集してからインポートできます。

Web Configからアドレス帳をインポートする

本スキャナーにインポートできるアドレス帳を持った別のスキャナーをお持ちの場合、そのスキャナーのバックアップデータをインポートすることで、アドレス帳に登録できます。

参考 別のスキャナーのアドレス帳からバックアップデータを作成するには、そのスキャナーのマニュアルをご覧ください。

バックアップデータからインポートする手順は以下です。

1. Web Configで［デバイス管理］タブ -［設定のエクスポート/インポート］-［インポート］の順に選択します。

2. ［ファイル］でバックアップデータファイルを選択し、暗号化パスワードを入力して、［次へ］をクリックします。

3. ［アドレス帳］を選択して、［次へ］をクリックします。

Web Configからアドレス帳をバックアップする

スキャナーの故障などでアドレス帳のデータが消失する可能性があります。アドレス帳の更新時にバックアップすることをお勧めします。本製品の保証期間内であっても、データの消失または破損について弊社はいかなる責も負いません。
スキャナーに登録されているアドレス帳は、Web Configでコンピューターにバックアップできます。

1. Web Configを起動し、［デバイス管理］タブ -［設定のエクスポート/インポート］-［エクスポート］の順に選択します。
2. ［スキャン］カテゴリーの［アドレス帳］にチェックを付けます。
3. エクスポートするファイルを暗号化するための、任意のパスワードを入力します。
   ここで指定したパスワードはインポートするときに必要になります。パスワードを指定しない場合は空白にします。
4. ［エクスポート］をクリックします。

ツールを使ったアドレス帳のエクスポートや一括登録

Epson Device Adminを使うと、アドレス帳だけをバックアップしたり、エクスポートしたファイルを編集して一括で登録したりできます。
アドレス帳だけをバックアップする場合や、スキャナーの置き替え時に置き替え前のスキャナーからアドレス帳を引き継ぐような場合に役立ちます。

アドレス帳をエクスポートする

アドレス帳の情報をファイルに保存します。
SYLK形式やcsv形式で保存したファイルは表計算ソフトやテキストエディターなどで編集できます。情報の削除や追加などをしてから一括で登録できます。
パスワードや個人情報などセキュリティー項目を含む情報は、パスワードを設定したバイナリー形式で保存できます。このファイルは編集できません。セキュリティー項目を含む情報のバックアップとして活用できます。

1. Epson Device Adminを起動します。
2. サイドバータスクメニューで［デバイス］を選択します。
3. デバイスリストで設定するデバイスを選択します。
4. リボンメニューの［ホーム］タブから［デバイスの設定］をクリックします。
   管理者パスワードを設定している場合は、パスワードを入力して［OK］をクリックします。
5. ［共通］-［アドレス帳］をクリックします。
6. ［エクスポート］-［エクスポートする項目］からエクスポート形式を選択します。
   - 全ての項目
     暗号化したバイナリーファイルをエクスポートします。パスワードや個人情報などセキュリティー項目を含めたい場合に選択します。このファイルは編集できません。こちらを選択した場合はパスワードの設定が必要です。［設定］をクリックしてパスワードをASCII文字（8～63文字）で設定します。このパスワードはバイナリーファイルのインポート時に入力が求められます。
   - セキュリティー情報を除く項目
     SYLK形式またはcsv形式のファイルをエクスポートします。エクスポートした情報を編集したい場合に選択します。

7. ［エクスポート］をクリックします。

8. ファイルを保存する場所を指定し、ファイルの種類を選択して［保存］をクリックします。
   パスワード変更の完了メッセージが表示されます。

9. ［OK］をクリックします。
   指定した場所にファイルが保存されていることを確認してください。

アドレス帳をインポートする

アドレス帳の情報をファイルからインポートします。
SYLK形式やcsv形式で保存したファイルや、セキュリティー項目を含む情報をバックアップしたバイナリーファイルをインポートできます。

1. Epson Device Adminを起動します。

2. サイドバータスクメニューで［デバイス］を選択します。

3. デバイスリストで設定するデバイスを選択します。

4. リボンメニューの［ホーム］タブから［デバイスの設定］をクリックします。
   管理者パスワードを設定している場合は、パスワードを入力して［OK］をクリックします。

5. ［共通］-［アドレス帳］をクリックします。

6. ［インポート］の［参照］をクリックします。

7. インポートするファイルを選択して［開く］をクリックします。
   バイナリーファイルを選択した場合、［パスワード］にファイルをエクスポートしたときに設定したパスワードを入力します。

8. ［インポート］をクリックします。
   確認画面が表示されます。

9. ［OK］をクリックします。
   読み込み内容の検証が始まり、結果を表示します。
   - 読み込んだ情報を編集する
     読み込んだ情報を個別に編集したい場合にクリックします。
   - 更にファイルを読み込む
     複数のファイルをインポートしたい場合にクリックします。

10. ［インポート］をクリックし、インポート完了画面で［OK］をクリックします。
    デバイスのプロパティ画面に戻ります。

11. ［送信］をクリックします。

12. 確認メッセージで［OK］をクリックします。

    設定がスキャナーに送信されます。

13. 送信完了画面で［OK］をクリックします。

    スキャナーの情報が更新されます。
    Web Configや操作パネルからアドレス帳を開き、更新されていることを確認してください。

LDAPサーバーと利用者を連携する

LDAPサーバーと連携すると、LDAPサーバーに登録されているアドレス情報をメールの宛先に利用できます。

LDAPサーバーを設定する

LDAPサーバーの情報を登録して、LDAPサーバーの情報を利用できるようにします。

1. Web Configで［ネットワーク］タブ - ［LDAPサーバー］-［基本］を選択します。
2. 各項目に値を入力します。
3. ［設定］を選択します。

   設定結果が表示されます。

LDAPサーバーの設定項目

項目	設定値と説明
LDAPサーバーを使用する	［使用する］または［使用しない］を選択します。
LDAPサーバーアドレス	LDAPサーバーのアドレスを入力します。IPv4、IPv6、FQDNのいずれかの形式で、1～255文字以内で指定します。FQDN形式では、ASCII（0x20-0x7E）の英数字とハイフン（アドレスの先頭と末尾以外）が使用できます。
LDAPサーバーポート番号	LDAPサーバーのポート番号を、1～65535以内の半角数字で入力します。
セキュア接続	スキャナーがLDAPサーバーにアクセスする際の認証方式を指定します。
証明書の検証	有効にするとLDAPサーバーの証明書の正当性をチェックします。［有効］にすることをお勧めします。 設定するには、スキャナーに［相手サーバー検証用CA証明書］のインポートが必要です。
検索タイムアウト（秒）	検索を開始してからタイムアウトするまでの時間（秒）を5～300までの半角数字で入力します。

項目	設定値と説明
認証方式	認証方式を選択します。 ［Kerberos認証］を選択する場合は、［Kerberos設定］を選択し、Kerberos設定をしてください。 Kerberos認証を行うには以下の環境が必要です。 • スキャナーとDNSサーバーが通信できること • スキャナーとKDCサーバー、認証が必要なサービスを提供するサーバー（LDAPサーバー、SMTPサーバー、ファイルサーバー）の時刻の同期が取れていること • サービスサーバーをIPアドレスで指定している場合、DNSサーバーの逆引き参照ゾーンにサービスサーバーのFQDNが登録されていること
使用するKerberosレルム	［認証方式］で［Kerberos認証］を選択した場合に、使用するKerberosレルムを選択します。
管理者DN / ユーザー名	Unicode（UTF-8）で、LDAPサーバーのユーザー名を128文字以内で入力します。制御文字（0x00～0x1F、0X7F）は使用できません。この項目は［認証方式］を［Anonymous認証］にすると無効になります。指定しない場合は空白にします。
パスワード	Unicode（UTF-8）で表せる128文字以内で、LDAPサーバー認証のパスワードを入力します。制御文字（0x00～0x1F、0X7F）は使用できません。この項目は［認証方式］を［Anonymous認証］にすると無効になります。指定しない場合は空白にします。

Kerberos設定

［LDAPサーバー］-［基本］の［認証方式］で［Kerberos認証］を選択する場合は、［ネットワーク］タブ -［Kerberos設定］から、以下のKerberos設定をしてください。Kerberos設定は10個まで登録できます。

項目	設定値と説明
レルム(ドメイン)	Kerberos認証のレルムを、ASCII（0x20-0x7E）で表せる255文字以内で指定します。登録しない場合は空白にします。
KDCアドレス	Kerberos認証サーバーのアドレスを入力します。IPv4、IPv6、FQDNのいずれかの形式で、255文字以内で指定します。登録しない場合は空白にします。
ポート番号(Kerberos)	Kerberosサーバーのポート番号を、1～65535以内の半角数字で入力します。

LDAPサーバーの検索属性を設定する

検索属性を設定すると、LDAPサーバーに登録されているユーザーのメールアドレスなどを利用できます。

1. Web Configで［ネットワーク］タブ -［LDAPサーバー］-［検索設定］を選択します。
2. 各項目に値を入力します。
3. ［設定］をクリックして、設定結果を表示します。

   設定結果が表示されます。

LDAPサーバー検索の設定項目

項目	設定値と説明
検索開始位置(DN)	データベースの任意の領域など、特定の場所から検索するときに指定します。 Unicode（UTF-8）で表せる0～128文字以内で入力します。任意の属性で検索しないときは空白にします。 設定例：localのserverディレクトリー：dc=server,dc=local
検索件数上限数（5-500）	検索される数の上限を5～500以内で設定します。検索によって取得した上限値までの件数を、一時的に保存して表示します。上限値を超えると警告メッセージが表示されますが、検索は続行できます。
ユーザー名属性	登録名として検索するLDAPサーバーの属性名を指定します。Unicode（UTF-8）で表せる1～255文字以内で入力します。先頭はアルファベットのA～Z、a～zにしてください。 設定例：cn、uid
ユーザー表示名属性	表示名として表示する属性名を指定します。Unicode（UTF-8）で表せる0～255文字以内で入力します。先頭はアルファベットのA～Z、a～zにしてください。 設定例：cn、sn
メールアドレス属性	メールアドレスを検索結果として表示する属性名を指定します。半角英数字、ハイフンを組み合わせて、1～255文字以内で入力します。先頭はアルファベットのA～Z、a～zにしてください。 設定例：mail
任意情報属性1～任意情報属性4	LDAPサーバーにエントリーしている他の任意属性を指定します。Unicode（UTF-8）で表せる0～255文字以内で入力します。先頭はアルファベットのA～Z、a～zにしてください。任意属性でのデータ取得を行わない場合は空白にします。 設定例：o、ou

LDAPサーバーとの接続を確認する

［LDAPサーバー］-［検索設定］で設定した値でLDAPサーバーとの接続テストを行います。

1. Web Configで［ネットワーク］タブ -［LDAPサーバー］-［接続確認］を選択します。
2. ［確認開始］を選択します。

   LDAPサーバーとの接続テストが開始されます。テストが終了すると結果が表示されます。

LDAPサーバー接続確認結果

メッセージ	説明
接続に成功しました。	サーバーとの接続に成功した場合に表示されます。

メッセージ	説明
接続に失敗しました。 設定を確認してください。	以下の理由によってサーバーへの接続に失敗した場合に表示されます。 • LDAPサーバーアドレス、ポート番号などが間違っている • 通信タイムアウトが発生した • ［LDAPサーバーを使用する］が［使用しない］に設定されている • ［認証方式］を［Kerberos認証］に設定した場合に、［レルム(ドメイン)］、［KDCアドレス］、または［ポート番号(Kerberos)］の設定が間違っている
接続に失敗しました。 製品、またはサーバーの日付/時刻設定を確認してください。	スキャナーとLDAPサーバーの時刻設定の不一致によって接続に失敗した場合に表示されます。
サーバーの認証に失敗しました。 設定を確認してください。	以下の理由によってサーバーへの接続に失敗した場合に表示されます。 • ［ユーザー名］または［パスワード］が間違っている • ［認証方式］を［Kerberos認証］に設定した場合に、時刻設定がされていない
製品は処理動作中のためアクセスできません。	スキャナーが動作中で接続設定ができなかったときに表示されます。

Document Capture Pro Serverを使う

Document Capture Pro Serverを使うと、スキャナーの操作パネルからスキャンした結果の仕分けや保存形式、転送先などの処理を登録、管理できます。スキャナーの操作パネルからサーバーに登録されているジョブを呼び出して実行します。
サーバーにするコンピューターにインストールします。
Document Capture Pro Serverの詳細はエプソンの問い合わせ窓口にお問い合わせください。

サーバーモードを設定する

Document Capture Pro Serverを使用するには以下の設定をします。

1. Web Configで［スキャン］タブ - ［Document Capture Pro］を選択します。
2. ［動作モード］で［サーバーモード］を選択します。
3. ［サーバーアドレス］にDocument Capture Pro Serverをインストールしているサーバーを指定します。

   IPv4、IPv6、ホスト名、FQDNのいずれかの形式で2～255文字以内で指定します。FQDN形式ではUS-ASCII文字の数字とアルファベット、ハイフン（先頭と末尾以外）が使用できます。
4. ［設定］をクリックします。

   ネットワークが再起動し、設定が有効になります。

AirPrintを設定する

Web Configで［ネットワーク］タブ -［AirPrint設定］の順に選択します。

項目	説明
Bonjourサービス名	BonjourのサービスをASCII （0x20-0x7E）で表せる41文字以内で入力します。
ロケーション	スキャナーの設定場所など任意のロケーション情報を、UTF-8で表せる127バイト以内の文字列で入力します。
Wide-Area Bonjour	Wide-Area Bonjourを使用するかどうか設定します。使用する場合、セグメントを越えた検索ができるように、スキャナーがDNSサーバーに登録されている必要があります。
AirPrintを有効にする	BonjourとAirPrint（Scan Service）が有効になります。

ユーザー定義サイズを登録する

Web Configでは、スキャンする原稿のユーザー定義サイズをスキャナーに登録できます。
登録したユーザー定義サイズは、Web Configの［お気に入り］や［ユーザーデフォルト設定］で［ユーザー定義サイズリスト(入力原稿)から取得］をクリックして呼び出します。

1. Web Configで［スキャン］タブ -［ユーザー定義サイズリスト(入力原稿)］を選択します。
2. 登録したい番号を選択して［編集］をクリックします。
3. 各項目を設定します。
   - 登録名：Unicode（UTF-8）で表せる10文字以内で名前を設定します。
   - 単位：単位を選択します。
   - X：原稿の幅を指定します。
   - Y：原稿の長さを指定します。
4. ［適用］をクリックします。

ネットワークスキャンを設定するときのトラブル

トラブルを解決するための糸口

- エラーメッセージの確認
  何らかのトラブルが発生した場合、始めにスキャナーの操作パネルやドライバーの画面などにメッセージが出ていないか確認してください。通知メールを送信するように設定してあると、イベントが発生した場合に素早く状態を把握できます。

- 通信状態を確認する
  サーバーやクライアントコンピューターの通信状態をpingやipconfigなどのコマンドを使って確認します。
- 接続テスト
  メールサーバーとの接続は、スキャナーから接続テストをすることで確認できます。また、クライアントコンピューターからサーバーへのアクセステストをして通信状態を確認します。
- 設定を初期化する
  設定や通信状態に問題がない場合、スキャナーのネットワーク設定を無効にしたり、初期状態に戻して設定をやり直したりするとトラブルが解消する場合があります。

Web Configにアクセスできない

スキャナーのIPアドレスが設定されていない

対処方法

スキャナーに有効なIPアドレスが設定されていない可能性があります。スキャナーの操作パネルでIPアドレスを設定してください。スキャナーの操作パネルから現在の設定情報が確認できます。

WebブラウザーがSSL/TLSの暗号強度に対応していない

対処方法

SSL/TLSには暗号強度があります。Web Configは以下のメッセージ暗号化をサポートしているブラウザーで起動できます。使用しているブラウザーが対応しているか確認してください。

- 80bit：AES256/AES128/3DES
- 112bit：AES256/AES128/3DES
- 128bit：AES256/AES128
- 192bit：AES256
- 256bit：AES256

CA署名証明書の有効期限が切れた

対処方法

証明書の有効期限に問題がある場合、Web ConfigにSSL/TLS通信（https）で接続したときに「有効期限が切れている」と表示されます。証明書の有効期限内に表示されるときは、スキャナーの時刻が正しく設定されているか確認してください。

証明書とスキャナーのコモンネームが一致していない

対処方法

コモンネームの不一致が起こると、Web ConfigにSSL/TLS通信（https）で接続したときに「セキュリティー証明書の名前が一致しません...」と表示されます。これは以下のIPアドレスが一致していないために発生します。

- 自己署名証明書の作成や更新時、CSRの作成時にコモンネームで記述したスキャナーのIPアドレス
- Web Configの起動時にブラウザーに入力したIPアドレス

自己署名証明書の場合は証明書を更新してください。
CA署名証明書の場合は該当のスキャナー用に証明書を取得し直してください。

ブラウザーにローカルアドレスのプロキシサーバー設定がされていない

対処方法

スキャナーでプロキシサーバーを使用する設定にしている場合、ブラウザーでローカルアドレスへの接続にプロキシサーバーを経由しないよう設定します。

- Windows：
  ［コントロールパネル］－［ネットワークとインターネット］－［インターネットオプション］－［接続］－［LANの設定］の［プロキシ サーバー］で、LAN（ローカルアドレス）にプロキシサーバーを使わない設定にします。
- Mac OS：
  ［システム環境設定］－［ネットワーク］－［詳細］－［プロキシ］で［プロキシ設定を使用しないホストとドメイン］にローカルアドレスを登録します。
  記入例：
  192.168.1.*：ローカルアドレス　192.168.1.XXX、サブネットマスク　255.255.255.0の場合
  192.168.*.*：ローカルアドレス　192.168.XXX.XXX、サブネットマスク　255.255.0.0の場合

コンピューターの設定でDHCPが無効になっている

対処方法

コンピューターの設定で、IPアドレスを自動的に取得するDHCPが無効になっている場合は、Web Configにアクセスできないことがあります。DHCPを有効にしてください。
Windows 10の設定例：
コントロールパネルを開き、［ネットワークとインターネット］-［ネットワークと共有センター］-［アダプターの設定の変更］の順にクリックします。お使いの接続のプロパティ画面を起動し、［インターネットプロトコルバージョン4（TCP/IPv4）］または［インターネットプロトコルバージョン6（TCP/IPv6）］のプロパティ画面を開きます。表示された画面で［IPアドレスを自動的に取得する］が選択されていることを確認します。

Microsoft Exchange Online使用時にメール送信できない

サインインできない、またはユーザーがログインできない

Entra IDで条件付きアクセスポリシーによりブロックされている場合があります。

対処方法：

Entra IDで条件付きアクセスポリシーを確認してください。
詳細の手順は、「Microsoft Learn」サイトでご確認ください。

メール送信できない

状況：

「この機能の利用には、メールサービスへのサインインが必要です。管理者にお問い合わせください」と表示されます。

対処方法：

Web Configで、現在の状態を確認してください。以下の順に選択します。
［ネットワーク］タブ-［メールサーバー］-［基本］

［現在の状態］が［サインイン］になっている場合は、サインインの情報がスキャナーに保存できていない可能性があります。［設定］をクリックし、設定情報をスキャナーに送信します。
［現在の状態］がなく、［サインイン］のボタンが表示されている場合は、サインインの操作をしてください。
「メールサーバーのOAuth 2.0認証を設定する」42ページ

状況：

クラウドサービスまたはメールサービスとの連携がされていないか、連携の有効期限が切れています。

対処方法：

クラウドサービスまたはメールサービスの連携を実施してください。

状況：

クラウドサービスへの再サインインが必要です。

対処方法：

クラウドサービスにサインインしてください。

有効期限切れのメッセージが表示される

サインインをしてからメール送信機能を利用しない状態が一定期間経過しています。
OAuth 2.0認証を使用しているスキャナーが長期間利用されなかった、メール送信の機能が使われない場合、アクセストークン、リフレッシュトークンが無効になります。

対処方法：

管理者が再度、サインインの操作をしてください。

「メールサーバーのOAuth 2.0認証を設定する」42ページ

操作パネルをカスタマイズする

お気に入りを登録する

よく使うスキャン設定を［お気に入り］として登録できます。お気に入りは48件まで登録できます。

参考

- スキャン開始画面で ☆ を選択して、現在の宛先や設定をお気に入りに登録できます。
- Web Configからも［お気に入り］を登録できます。
  ［スキャン］タブ -［お気に入り］の順に選択します。
- 登録時に［スキャン to コンピューター］を選択すると、Document Capture Proで作成したジョブを［お気に入り］として登録できます。コンピューターがネットワークに接続されているときのみ利用できます。事前にDocument Capture Proでジョブを登録しておいてください。
- 操作パネルの［管理者ロック］が有効になっているときは、管理者のみが［お気に入り］を登録できます。

1. 操作パネルのホーム画面で［お気に入り］を選択します。

2. ⊕ を選選択します。

3. お気に入りとして登録したい機能を選択します。

4. 各項目を設定し、 ☆+ を選択します。

参考 ［スキャン to コンピューター］を選択したときは、Document Capture Proがインストールされているコンピューター、および登録済みのジョブを選択します。ネットワークに接続されたコンピューターのみ選択できます。

5. お気に入りの設定項目を設定します。

- ［登録名称］：名前を設定します。
- ［登録アイコン］：表示するアイコンのデザインと色を設定します。
- ［クイック送信設定］：お気に入りを選択するとすぐにスキャンを開始するようにします。
  Document Capture Pro Serverを使用している場合、スキャンする前にジョブの内容を確認する設定にしていても、スキャナー本体のお気に入りで設定する［クイック送信設定］が優先されます。
- ［登録内容］：スキャン設定を確認します。

6. ［OK］を選択します。

お気に入りメニューの説明

各お気に入りの › を選択すると、お気に入りの設定を変更できます。

登録名称の変更：

お気に入りの名前を変更します。

アイコンの変更：

アイコンのデザインと色を変更します。

クイック送信設定：

お気に入りを選択するとすぐにスキャンを開始するようにします。

配置変更：

お気に入りの表示順を変更します。

削除：

登録したお気に入りを削除します。

ホームに追加/削除：

登録したお気に入りを、ショートカットとしてホーム画面に追加したり削除したりできます。

詳細確認：

お気に入りの設定を表示します。［この設定を使用する］を選択してお気に入りを呼び出します。

操作パネルからホーム画面を編集する

操作パネルで［設定］-［ホーム画面編集］を選択すると、ホーム画面のカスタマイズができます。

- レイアウト：アイコン一覧の表示方法を変更します。
「ホーム画面のレイアウトを変更する」83ページ
- アイコンの追加：作成した［お気に入り］設定のアイコンを追加したり、ホーム画面から削除したアイコンを元に戻したりします。
「アイコンの追加」84ページ
- アイコンの消去：ホーム画面からアイコンを削除します。
「アイコンの消去」85ページ
- アイコンの移動：アイコンの表示順を変更します。
「アイコンの移動」86ページ
- アイコン表示を初期状態に戻す：ホーム画面の表示を購入時の状態に戻します。
- ホーム背景色設定：ホーム画面の背景色を変更します。

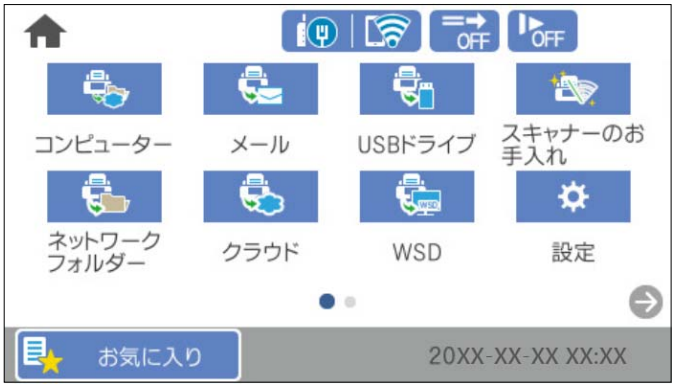
ホーム画面のレイアウトを変更する

1. スキャナーの操作パネルで、［設定］-［ホーム画面編集］-［レイアウト］の順に選択します。

2. ［1行］または［2行］を選択します。

［1行］：

［2行］：



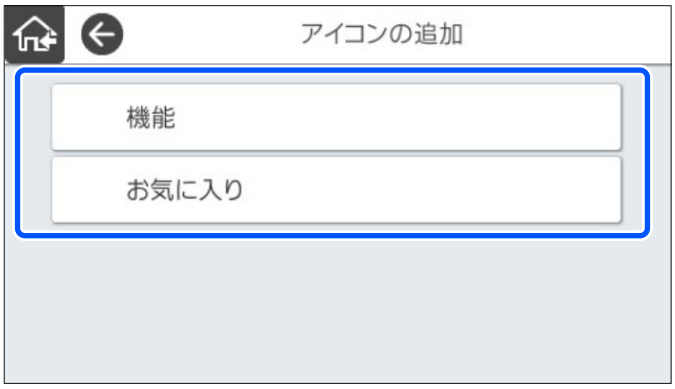
3. を選択して、ホーム画面を確認します。

アイコンの追加

1. スキャナーの操作パネルで、［設定］-［ホーム画面編集］-［アイコンの追加］の順に選択します。

2. ［機能］または［お気に入り］を選択します。
   - 機能：ホーム画面に表示されるデフォルトの機能を表示します。

- お気に入り：登録したお気に入りを表示します。



3. ホーム画面に追加したい項目を選択します。

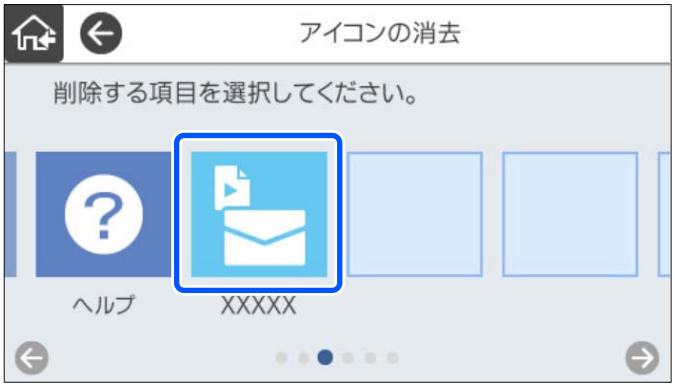
4. 項目を追加したい空のフレームを選択します。
   複数のアイコンを追加したい場合は、手順3から4を繰り返します。

5. を選択して、ホーム画面を確認します。

アイコンの消去

1. スキャナーの操作パネルで、［設定］-［ホーム画面編集］-［アイコンの消去］の順に選択します。

2. 削除したいアイコンを選択します。



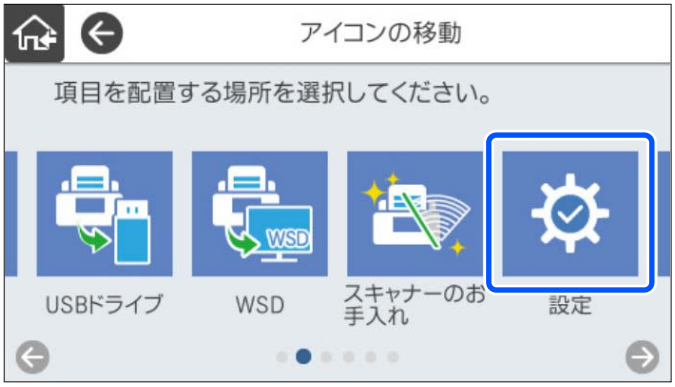
3. ［はい］を選択して終了します。
   複数のアイコンを削除したい場合は、手順2と3を繰り返します。

4. を選択して、ホーム画面を確認します。

アイコンの移動

1. スキャナーの操作パネルで、［設定］-［ホーム画面編集］-［アイコンの移動］の順に選択します。

2. 移動したいアイコンを選択します。



3. 移動先のフレームを選択します。

   すでに他のアイコンが移動先に設定されている場合は、アイコンが入れ替わります。

4. を選択して、ホーム画面を確認します。

基本のセキュリティー設定

本体のセキュリティー機能の紹介

エプソンデバイスのセキュリティー機能を紹介します。

機能名	どんな機能か	何を設定するのか	何を防止できるのか
管理者パスワードの設定	ネットワークやUSBの接続設定など、システムに関わる設定をロックし、管理者以外は変更ができないようにします。	システム管理者がデバイスにパスワードを設定します。 Web Config、スキャナーの操作パネルのどちらからも設定や変更ができます。	デバイスに保持されているIDやパスワード、ネットワーク設定などの情報が不正に参照または変更されるのを防ぎます。また、ネットワーク環境やセキュリティーポリシー、またはそれらに類する情報の漏えいなど、広範囲のセキュリティーリスクにつながる危険性を低減します。
外部インターフェイス設定	デバイスへ接続するインターフェイスを制御できます。	コンピューターとのUSB接続の有効、無効を設定します。	コンピューターのUSB接続：ネットワークを経由しないスキャンを禁止することで、デバイスの不正使用を防止できます。

関連情報

- 「管理者パスワードの設定」89ページ
- 「外部インターフェイスを無効にする」95ページ

管理者設定

管理者パスワードの設定

管理者パスワードを設定すると、ユーザーがシステム管理に関する設定を変更することを防ぎます。購入時に初期値が設定されています。必要に応じて変更してください。

参考 管理者情報の購入時の設定（初期値）は以下です。

- ユーザー名（Web Configのみで使用）：なし（空欄）
- パスワード：スキャナーの製造番号（シリアルナンバー）

製造番号は、スキャナー背面に貼られているラベルをご確認ください。

管理者パスワードはWeb Config、スキャナーの操作パネル、Epson Device Adminのいずれからも変更ができます。Epson Device Adminの操作方法については、Epson Device Adminのヘルプやマニュアルをご覧ください。

Web Configで管理者パスワードを変更する

Web Configで管理者パスワードを変更します。

1. Web Configで［本体セキュリティー］タブ - ［管理者パスワード変更］を選択します。
2. ［現在のパスワード］、［ユーザー名］、［新しいパスワード］、［新しいパスワードの確認］を入力します。
   新しいパスワードは、1文字以上入力してください。

   参考 管理者情報の購入時の設定（初期値）は以下です。
   - ユーザー名：なし（空欄）
   - パスワード：スキャナーの製造番号（シリアルナンバー）

   製造番号は、スキャナー背面に貼られているラベルをご確認ください。

   > **重要** 設定した管理者パスワードは忘れないように管理してください。パスワードを忘れると再設定できず、サービスマンによる対応が必要になります。

3. ［設定］を選択します。

関連情報

➡ 「ブラウザーでWeb Configを起動する」35ページ

操作パネルから管理者パスワードを変更する

スキャナーの操作パネルから管理者パスワードを変更します。

1. スキャナーの操作パネルで［設定］を選択します。
2. ［管理者用設定］-［管理者設定］の順に選択します。
3. ［管理者パスワード］-［変更］の順に選択します。
4. 現在のパスワードを入力します。

   参考 管理者パスワードの購入時の設定（初期値）は、スキャナーの製造番号（シリアルナンバー）です。
   製造番号は、スキャナー背面に貼られているラベルをご確認ください。

5. 新しいパスワードを入力します。
   1文字以上入力してください。

   > **重要** 設定した管理者パスワードは忘れないように管理してください。パスワードを忘れると再設定できず、サービスマンによる対応が必要になります。

6. 確認のためもう一度新しいパスワードを入力します。

完了メッセージが表示されます。

操作パネルを管理者ロックする

システム設定に関する項目をユーザーが変更できないように、操作パネルを管理者ロックできます。

参考 スキャナーの認証設定を有効にすると、操作パネルも管理者ロックされます。認証設定が有効なときはロックを解除できません。
認証設定を無効にしても、管理者ロックは有効のままです。無効にしたいときは、操作パネルまたはWeb Configから設定します。

操作パネルで管理者ロックを設定する

1. 有効になっている［管理者ロック］を解除したいときは、ホーム画面右上の  をタップして管理者としてログオンします。

   ［管理者ロック］が無効になっているときは、  は表示されません。有効にしたいときは、次の手順に進みます。

2. ［設定］を選択します。

3. ［管理者用設定］-［管理者設定］の順に選択します。

4. ［管理者ロック］で、［オン］または［オフ］を選択します。

Web Configで管理者ロックを設定する

1. ［デバイス管理］タブ -［パネル］の順に選択します。

2. ［パネルロック］で［オン］または［オフ］を選択します。

3. ［設定］をクリックします。

関連情報

➡ 「ブラウザーでWeb Configを起動する」35ページ

設定メニューの管理者ロック項目

管理者ロックによって、操作パネルの［設定］メニューでロックされる項目一覧です。
○：ロックされます。
-：ロックされません。

設定メニュー	管理者ロック
基本設定	-

設定メニュー		管理者ロック
	画面の明るさ設定	-
	音の設定	-
	スリープ移行時間設定	○
	自動電源オフ	○
	日付/時刻設定	○
	言語選択/Language	○/- *
	キーボード （製品を購入された地域により搭載されていないことがあります。）	-
	無操作タイムアウト	○
	コンピューターのUSB接続	○
	ダイレクトパワーオン	○
スキャン動作設定		-
	低速モード	-
	重送検知時動作	○
	重送検知スキップ	-
	原稿保護	○
	ガラス面汚れ検知	○
	超音波重送検知	○
	原稿待ち受けモードのタイムアウト時間	○
	読み取り前宛先確認	○
ホーム画面編集		○
	レイアウト	○
	アイコンの追加	○
	アイコンの消去	○
	アイコンの移動	○
	アイコン表示を初期状態に戻す	○
	ホーム背景色設定	○
ユーザー設定		○

設定メニュー		管理者ロック
	ネットワークフォルダー	○
	メール	○
	クラウド	○
	USBドライブ	○
ネットワーク設定		○
	無線LAN接続設定	○
	有線LAN接続設定	○
	ネットワーク情報	○
	詳細設定	○
Webサービス設定		○
	Epson Connect設定	○
Document Capture Pro設定		-
	設定を変更する	○
アドレス帳管理		-
	アドレス帳登録・変更	○/- *
	常用管理	-
	アドレス帳表示方法設定	-
	アドレス帳検索設定	-
管理者用設定		○
	アドレス帳管理	○
	管理者設定	○
	機能制限	○
	パスワード暗号化	○
	お客様利用情報	○
	WSD設定	○
	購入時の設定に戻す	○
	ファームウェアのアップデート	○
機器情報		-

設定メニュー			管理者ロック
	製造番号		-
	現在のバージョン		-
	総スキャン枚数		-
	片面スキャン枚数		-
	両面スキャン枚数		-
	キャリアシートのスキャン枚数		-
	ローラー交換後のスキャン枚数		-
	定期清掃後のスキャン枚数		-
	スキャン枚数リセット		○
スキャナーのお手入れ			-
	ローラークリーニング		-
	ローラー交換		-
		スキャン枚数リセット	○
		交換方法	-
	定期清掃		-
		スキャン枚数リセット	○
		清掃方法を見る	-
	ガラス面清掃		-
ローラー交換通知設定			○
	通知枚数設定		○
定期清掃通知設定			○
	ワーニング通知設定		○
	通知枚数設定		○

*　　［管理者用設定］ - ［機能制限］で、変更を許可するかどうかを設定可能

操作パネルから管理者としてログオンする

以下の方法で、スキャナーの操作パネルから管理者としてログオンできます。

1. 画面右上の  をタップします。
   - 認証設定を有効にしているときは、［ようこそ］画面（認証の待ち受け画面）にアイコンが表示されます。
   - 認証設定を無効にしているときは、ホーム画面にアイコンが表示されます。
2. 確認画面が表示されたら、［はい］をタップします。
3. 管理者のパスワードを入力します。
   ログオン完了のメッセージが表示され、操作パネルのホーム画面が表示されます。

ログアウトするときは、ホーム画面右上の  をタップします。

管理者名/連絡先を設定する

Web Configでは、管理者の名前と連絡先をスキャナーに設定できます。設定した管理者名/連絡先は、Web Configの［製品情報］ページに表示され、管理者ログオンしなくても参照できます。

1. Web Configで［デバイス管理］タブ - ［管理者名/連絡先］を選択します。
2. 管理者の名前と連絡先を、Unicode（UTF-8）で255バイト以内で入力します。
   半角英数字は1文字につき1バイト、それ以外の文字は1文字のバイト数が異なります。
3. ［設定］をクリックします。

外部インターフェイスを無効にする

スキャナーにデバイスを接続するインターフェイスを無効にできます。ネットワーク経由以外のスキャンを制限する場合に設定します。

参考 スキャナーの操作パネルからも設定できます。
コンピューターのUSB接続 ： ［設定］ - ［基本設定］ - ［コンピューターのUSB接続］の順に選択します。

1. Web Configで［本体セキュリティー］タブ-［外部インターフェイス］を選択します。
2. 制限したい機能で［無効］を選択します。
   制限を解除する場合は［有効］を選択してください。
   コンピューターのUSB接続
   コンピューターからのUSB 接続を制限できます。制限する場合は［無効］に設定します。
3. ［設定］をクリックします。
4. 無効にしたポートが使用できなくなっているか確認します。
   コンピューターのUSB接続
   確認するコンピューターにドライバーがインストールされている場合：
   スキャナーとコンピューターをUSBケーブルで接続し、スキャンができないことを確認します。

確認するコンピューターにドライバーがインストールされていない場合：
Windows：
デバイスマネージャーを表示したままスキャナーをコンピューターにUSBケーブルで接続し、デバイスマネージャーの表示内容が変化しないことを確認します。
Mac OS：
スキャナーをコンピューターにUSBケーブルで接続し、［プリンターとスキャナー］からスキャナーを追加しようとしてもスキャナーがリストに表示されないことを確認します。

関連情報

➡ 「ブラウザーでWeb Configを起動する」35ページ

遠隔地にあるスキャナーを監視する

遠隔地にあるスキャナーの情報を確認する

Web Configの［情報確認］から、運用しているスキャナーの以下の情報を確認できます。

- 製品情報
  ステータス、クラウドサービス、製造番号、MACアドレスなどが確認できます。
- ネットワーク情報
  ネットワーク接続状態、IPアドレス、DNSなどネットワークに関する情報が確認できます。
- 使用状況
  初回のスキャン日、スキャン回数などを確認できます。
- ハードウェア情報
  スキャナーの各機能のステータスを確認できます。
- パネルのスナップショット
  スキャナーの操作パネルに表示されている画面が表示されます。

イベント発生時にメール通知を受け取る

メール通知の概要

スキャンの停止やスキャナーエラーなど、スキャナーにイベントが発生したときに、指定したアドレスにメールで通知する機能です。
宛先は5つまで登録でき、それぞれに受け取りたい通知を設定できます。
この機能を使うには、設定前にメールサーバーの設定が必要です。

関連情報

➡ 「メールサーバーを登録する」41ページ

メール通知を設定する

Web Configを使ってメール通知の設定をします。

1. Web Configで［デバイス管理］タブ-［メール通知］を選択します。

2. メール通知の件名を設定します。
   2つのプルダウンメニューで件名に表示する内容を選択します。
   - 選択された内容が［件名］の横に表示されます。
   - 左右に同じ内容は設定できません。
   - ［ロケーション］の文字数が多い場合は、32バイト以降の文字が省略されます。

3. 通知メールを送信するメールアドレスを入力します。
   A-Z a-z 0-9 ! # $ % & ' * + - . /= ? ^ _ { | } ~ @を使用し、1～255文字以内で入力します。

4. メール通知の言語を選択します。

5. 通知を受け取りたいイベントの行で、通知する宛先番号と重なるチェックボックスにチェックを付けます。
   ［通知設定］の番号は［宛先設定］の宛先の番号に対応しています。
   例：
   管理者のパスワードが変更された通知を［宛先設定］の1に設定したアドレスに送信したいときは、［管理者パスワード変更］の行にある［1］の列のチェックボックスにチェックを付けます。

6. ［設定］をクリックします。
   何らかのイベントを作って、メール通知が送信されることを確認してください。
   例：管理者パスワードが変更されました。

関連情報

➡ 「ブラウザーでWeb Configを起動する」35ページ

メール通知の設定項目

項目	設定値と説明
管理者パスワード変更	管理者パスワードが変更された場合に通知します。
スキャナーエラー	スキャナーエラーが発生した場合に通知します。
無線LAN故障	無線LANインターフェイスにエラーが発生した場合に通知します。

困ったときは

管理者パスワードを忘れた

サービスマンによる対応が必要です。エプソンの修理窓口にご相談ください。

参考 Web Configの管理者の購入時の設定（初期値）は以下の通りです。

- ユーザー名：なし（空欄）
- パスワード：スキャナーの製造番号（シリアルナンバー）

製造番号は、スキャナー背面に貼られているラベルをご確認ください。管理者パスワードを初期化すると、購入時の設定に戻ります。

高度なセキュリティー設定

セキュリティー設定と防止できる脅威

ネットワークにスキャナーを接続すると、離れた場所からアクセスして使用できます。また、スキャナーを共有してたくさんの人が使用でき、業務効率や利便性の向上に役立ちます。反面、不正アクセスや不正使用、データの改ざんなどのリスクも高くなります。インターネットにアクセスできる環境の場合はさらにリスクが高まります。
外部からのアクセスの保護を施していないスキャナーは、本体に記憶しているアドレス帳などをインターネットから読み取ることができてしまいます。
リスクを回避するため、エプソン製スキャナーにはさまざまなセキュリティー技術を搭載しています。
お客様の情報環境での条件に合わせて、スキャナーに必要なセキュリティー設定をしてください。

機能名	どんな機能か	何を設定するのか	何を防止できるのか
プロトコルの制御	スキャナーやコンピューター間の通信で使用するプロトコルやサービスを制御して、機能を有効、無効にします。	機能に対応したプロトコルやサービスを個別に許可、禁止します。	不要な機能を使用できなくすることで、意図されない利用によるセキュリティーリスクを軽減できます。
SSL/TLS通信	ブラウザー経由でのコンピューターとの通信やEpson Connect、ファームウェアアップデートなどスキャナーからインターネット上のエプソンサーバーにアクセスするような場合に通信内容がSSL/TLS通信で暗号化されます。	CA署名証明書をCA局から取得し、スキャナーにインポートします。	CA署名証明書によってスキャナーの身分が明確になることで、なりすましや不正アクセスを防げます。また、通信内容がSSL/TLSによって保護されるため、スキャンしたデータの内容や設定情報の漏えいが防げます。
IPsec/IPフィルタリング	特定のクライアントからのデータや、特定の種類のデータだけを通過、遮断する設定ができます。IPsecはIP パケット単位で保護（暗号化および認証）するため、セキュアでないプロトコルも安全に通信できます。	基本ポリシー、個別ポリシーを作成し、スキャナーにアクセスできるクライアントやデータの種類を設定します。	スキャナーへの不正アクセス、通信データの傍受や改ざんを防止できます。
IEEE802.1X	許可された利用者だけがネットワークに接続できるようにします。許可された利用者だけがスキャナーを使用できるようにします。	RADIUSサーバー（認証サーバー）への認証設定をします。	不正なスキャナーへのアクセスや使用を防止できます。

関連情報

- 「利用するプロトコルを制御する」101ページ
- 「スキャナーとのSSL/TLS通信」109ページ
- 「IPsec/IPフィルタリングで暗号化通信する」110ページ
- 「IEEE802.1X環境にスキャナーを接続する」122ページ

セキュリティー機能の設定

IPsec/IPフィルタリングやIEEE802.1Xなどの設定は、改ざん、傍受などセキュリティーのリスク低減のために、SSL/TLS通信でWeb Configにアクセスして設定することをお勧めします。

必ず管理者パスワードを設定してから、IPsec/IPフィルタリングやIEEE802.1Xの設定をしてください。

利用するプロトコルを制御する

スキャンする場合、いろいろな経路やプロトコルからスキャンできます。また、ネットワークスキャンが不特定多数のコンピューターから利用可能になります。
使わない機能やプロトコル、サービスを無効にすることで意図しない経路からの不正なアクセスやスキャンなどのセキュリティーリスクを軽減できます。

プロトコルを制御する

スキャナーが対応しているプロトコルの設定をします。

1. Web Configで［ネットワークセキュリティー］タブ - ［プロトコル］を選択します。
2. 各項目を設定します。
3. ［次へ］をクリックします。
4. ［設定］をクリックします。
   設定がスキャナーに反映されます。

関連情報

➡ 「ブラウザーでWeb Configを起動する」35ページ

有効・無効が設定可能なプロトコル

プロトコル	特徴
Bonjour設定	Bonjourを使用するかを指定できます。Bonjourは機器の検索やスキャンなどに使われます。
SLP設定	SLP機能の有効・無効が設定できます。SLPはエプソンスキャナーではプッシュスキャン機能やEpsonNet Configでのネットワーク探索に使われます。
WSD設定	WSD機能の有効・無効が設定できます。有効にすると、WSDデバイスの追加やWSDポートからのスキャンができるようになります。
LLTD設定	LLTDの有効･無効が設定できます。有効にするとWindowsのネットワークマップに表示されるようになります。
LLMNR設定	LLMNRの有効・無効が設定できます。有効にするとDNSが使えない状況でもNetBIOSを使用せずに名前解決ができるようになります。
SNMPv1/v2c設定	SNMPv1/v2cの有効・無効を指定できます。エプソンスキャナーでは機器の設定や監視などに使われます。

プロトコル	特徴
SNMPv3設定	SNMPv3の有効・無効を指定できます。エプソンスキャナーでは暗号化した機器の設定や監視などの通信で使われます。

プロトコルの設定項目

Bonjour設定

項目	設定値と説明
Bonjourを使用する	チェックを入れるとBonjourで機器を検索または使用することを許可します。
Bonjour名	Bonjour名が表示されます。
Bonjourサービス名	Bonjourサービス名が表示されます。
ロケーション	Bonjourのロケーションが表示されます。
Wide-Area Bonjour	Wide-Area Bonjourを使用するかどうか設定します。

SLP設定

項目	設定値と説明
SLP機能を有効にする	チェックを入れるとSLP機能が有効になります。 EpsonNet Configでのネットワーク探索に使われます。

WSD設定

項目	設定値と説明
WSDを有効にする	チェックを入れるとWSDを使って、WSDポートからスキャンができます。
スキャンタイムアウト (秒)	WSDスキャンの通信タイムアウト時間を3～3600秒の範囲で入力します。
デバイス名	WSDのデバイス名が表示されます。
ロケーション	WSDのロケーションが表示されます。

LLTD設定

項目	設定値と説明
LLTDを有効にする	チェックを入れるとLLTDが有効になります。有効にするとWindowsのネットワークマップに表示されるようになります。
デバイス名	LLTDのデバイス名が表示されます。

LLMNR設定

項目	設定値と説明
LLMNRを有効にする	チェックを入れるとLLMNRが有効になります。有効にするとDNSが使えない状況でもNetBIOSを使用せずに名前解決ができるようになります。

SNMPv1/v2c設定

項目	設定値と説明
SNMPv1/v2cを有効にする	チェックを入れるとSNMPv1/v2cを有効にします。
アクセス権限	SNMPv1/v2cを有効にした場合にアクセス権限を設定します。［読み込み専用］または［読み書き可能］を選択します。
コミュニティ名 (読み込み専用)	ASCII（0x20～0x7E）で表せる32文字以内で入力します。指定しない場合は空白にします。
コミュニティ名 (読み書き可能)	ASCII（0x20～0x7E）で表せる32文字以内で入力します。指定しない場合は空白にします。

SNMPv3設定

項目		設定値と説明
SNMPv3を有効にする		チェックを入れるとSNMPv3が有効になります。
ユーザー名		1バイト文字を使って1～32文字以内で入力します。
認証設定		
	アルゴリズム	SNMPv3の認証用のアルゴリズムを選択します。
	パスワード	SNMPv3の認証パスワードを入力します。 ASCII (0x20-0x7E)で表せる8～32文字以内で入力します。 指定しないときは空白にします。
	パスワード確認入力	確認のため、入力したパスワードをもう一度入力します。
暗号化設定		
	アルゴリズム	暗号化アルゴリズムを選択します。
	パスワード	暗号化パスワードを入力します。 ASCII (0x20-0x7E)で表せる8～32文字以内で入力します。 指定しないときは空白にします。
	パスワード確認入力	確認のため、入力したパスワードをもう一度入力します。
コンテキスト名		Unicode（UTF-8）で表せる32文字以内で入力します。指定しないときは空白にします。言語によって扱える文字数は異なります。

電子証明書を使う

使用できる電子証明書

- CA署名証明書
  認証機関（CA局）によって署名された証明書です。CA局に申請して取得します。この証明書はスキャナーの実在性を証明し、SSL/TLS通信に使用されるため、データ通信の安全が確保できます。
  SSL/TLS通信に使用する場合は、サーバー証明書として利用されます。
  IPsec/IPフィルタリング、IEEE802.1Xに設定する場合は、クライアント証明書として利用されます。
- CA証明書
  CA署名証明書のチェーン内の証明書で、中間CA証明書とも呼ばれます。相手サーバーまたはWeb Configにアクセスするブラウザーが、スキャナーの証明書パスを検証するために使用されます。
  相手サーバー検証用のCA証明書は、スキャナーからアクセスするサーバーの証明書パスを検証する場合に設定します。スキャナーでは、SSL/TLS通信用のCA署名証明書の証明書パスを証明するために設定します。
  スキャナーのCA証明書は、CA署名証明書を発行したCA局から入手できます。
  また、相手サーバー検証に使用するCA署名証明書は、相手サーバーのCA署名証明書を発行したCA局から入手できます。
- 自己署名証明書
  スキャナー自らが署名し、発行した証明書です。ルート証明書とも呼ばれます。発行者が自分自身を証明しているので、証明書として信頼性がなく、なりすましは防げません。
  セキュリティー設定をする際にCA署名証明書なしで簡易的にSSL/TLS通信を行う場合に使用してください。
  ブラウザーに証明書の登録がないために、SSL/TLS通信でスキャナーにアクセスするとセキュリティー警告が出ることがあります。自己署名証明書はSSL通信のみで使用できます。

関連情報

- 「CA署名証明書を設定する」104ページ
- 「自己署名証明書を更新する」107ページ
- 「相手サーバー検証用CA証明書を設定する」108ページ

CA署名証明書を設定する

CA署名証明書を取得する

CA署名証明書を取得するにはCSR（証明書発行要求）を生成し、CA局に申請します。CSRはWeb Configかコンピューターで生成してください。
ここではWeb Configから取得する方法を説明します。Web Configで生成したCSRの証明書はPEM/DER形式です。

1. Web Configで［ネットワークセキュリティー］タブを選択し、［SSL/TLS］ - ［証明書］または［IPsec/IPフィルタリング］ - ［クライアント証明書］または［IEEE802.1X］ - ［クライアント証明書］を選択します。
   どれを選択しても同じ証明書が取得でき、共通で使用できます。

2. ［CSR］の［生成］をクリックします。

   CSR生成画面が開きます。

3. 各項目を設定します。

   参考 対応している公開鍵長や省略の可否はCA局によって異なる場合があります。申請するCA局のルールに従って記載してください。

4. ［設定］をクリックします。

   生成されると完了メッセージが表示されます。

5. ［ネットワークセキュリティー］タブを選択し、［SSL/TLS］ - ［証明書］または［IPsec/IPフィルタリング］ - ［クライアント証明書］または［IEEE802.1X］ - ［クライアント証明書］を選択します。

6. CA局規定のファイル形式に従い［CSR］のダウンロードボタンをクリックして、CSRをコンピューターにダウンロードします。

   重要 再度CSRを生成しないでください。交付されたCA署名証明書がインポートできなくなります。

7. 保存したCSRをCA局に送付し、CA署名証明書を入手します。

   送付方法や送付形態は、CA局の規定に従ってください。

8. 入手したCA署名証明書を、スキャナーに接続しているコンピューターに保存します。

   指定場所にCA署名証明書ファイルが保存されたら完了です。

関連情報

➡ 「ブラウザーでWeb Configを起動する」35ページ

CSRの設定項目

項目	設定値と説明
公開鍵長	CSRに使用する公開鍵長を選択します。
コモンネーム	1～128文字以内で入力できます。IPアドレスを指定するときは、固定のIPアドレスを設定します。IPv4アドレス、IPv6アドレス、ホスト名、FQDNを「,」カンマで区切って1～5個入力できます。 先頭の要素がコモンネームに格納され、その他の要素は証明書のサブジェクトの別名フィールドに格納されます。 記入例： スキャナーのIPアドレス：192.0.2.123、スキャナー名：EPSONA1B2C3 コモンネーム：EPSONA1B2C3,EPSONA1B2C3.local,192.0.2.123
組織名/ 部署名/ 市町村名/ 都道府県名	ASCII (0x20-0x7E)で表せる0～64文字以内で入力できます。識別名（CN）はカンマで分割できます。
国コード	ISO-3166で規定している2文字の国コードを入力します。

項目	設定値と説明
送信元アドレス	メールサーバー設定の送信元アドレスを入力できます。［ネットワーク］タブ -［メールサーバー］ -［基本］の［送信元アドレス］と同じメールアドレスを入力してください。

CA署名証明書をインポートする

取得したCA署名証明書をスキャナーにインポートします。

重要
- スキャナーの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。証明書が無効である可能性があります。
- Web Configで生成したCSRで証明書を取得した場合、証明書をインポートできるのは一度だけです。

1. Web Configで［ネットワークセキュリティー］タブを選択し、次に、［SSL/TLS］ -［証明書］、または［IPsec/IPフィルタリング］ -［クライアント証明書］または［IEEE802.1X］ -［クライアント証明書］を選択します。
2. ［インポート］をクリックします。

   証明書インポート設定画面が開きます。
3. 各項目に値を入力します。［CA証明書1］、［CA証明書2］はスキャナーにアクセスするブラウザーで証明書のパスを検証する場合に設定してください。

   インポートの設定内容は、CSRの生成場所や証明書のファイル形式によって異なります。以下を参考にして入力が必要な項目を設定してください。
   - Web Configから取得したPEM/DER形式の証明書
     - ［秘密鍵］：スキャナーで保持しているため設定しない
     - ［パスワード］：設定しない
     - ［CA証明書1］/［CA証明書2］：オプション
   - コンピューターから取得したPEM/DER形式の証明書
     - ［秘密鍵］：設定する
     - ［パスワード］：設定しない
     - ［CA証明書1］/［CA証明書2］：オプション
   - コンピューターから取得したPKCS#12形式の証明書
     - ［秘密鍵］：設定しない
     - ［パスワード］：オプション
     - ［CA証明書1］/［CA証明書2］：設定しない
4. ［設定］をクリックします。

   インポートされると完了メッセージが表示されます。

参考 ［表示］をクリックして証明書情報を検証します。

関連情報

➡ 「ブラウザーでWeb Configを起動する」35ページ

CA署名証明書のインポート設定項目

項目	設定値と説明
サーバー証明書　または　クライアント証明書	取得したCA署名証明書のファイル形式を選択し、ファイルを指定します。 SSL/TLSの場合、サーバー証明書になります。 IPsec/IP フィルタリング、IEEE802.1Xの場合はクライアント証明書になります。
秘密鍵	コンピューターで生成したCSRでPEM/DER形式の証明書を取得した場合、証明書と対になった秘密鍵ファイルを指定します。
パスワード	ファイル形式が［秘密鍵付き証明書（PKCS#12）］の場合、証明書取得時に設定した秘密鍵暗号化のパスワードを入力します。
CA証明書1	ファイル形式が［証明書（PEM/DER）］の場合、サーバー証明書として使うCA署名証明書を発行したCA局の証明書をインポートします。必要に応じて設定してください。
CA証明書2	ファイル形式が［証明書（PEM/DER）］の場合、CA証明書1を発行した機関の証明書をインポートします。必要に応じて設定してください。

CA署名証明書を削除する

サービスが無効になった証明書や使用していない証明書は削除できます。

!重要 Web Configで生成したCSRで取得した証明書は、一度削除すると再インポートができません。必要な場合はCSRを再生成して取得し直してください。

1. Web Configで［ネットワークセキュリティー］タブを選択します。［SSL/TLS］ - ［証明書］または［IPsec/IPフィルタリング］ - ［クライアント証明書］または［IEEE802.1X］ - ［クライアント証明書］を選択します。
2. ［削除］をクリックします。
3. 確認のメッセージを確認して、削除します。

関連情報

➡ 「ブラウザーでWeb Configを起動する」35ページ

自己署名証明書を更新する

自己署名証明書はスキャナーが発行しているので、有効期限が切れた場合や記載している内容に変更があった場合などに更新できます。

1. Web Configで［ネットワークセキュリティー］タブ - ［SSL/TLS］ - ［証明書］を選択します。
2. ［更新］をクリックします。
3. ［コモンネーム］を入力します。

   IPv4アドレス、IPv6アドレス、ホスト名、FQDNを「,」カンマで区切って5個まで、1～128文字以内で入力できます。先頭の要素がコモンネームに格納され、その他の要素は証明書のサブジェクトの別名フィールドに格納されます。
   記入例：
   スキャナーのIPアドレス：192.0.2.123、スキャナー名：EPSONA1B2C3
   コモンネーム：EPSONA1B2C3,EPSONA1B2C3.local,192.0.2.123
4. 証明書の有効期間を選択します。
5. ［次へ］をクリックします。

   確認画面が表示されます。
6. ［設定］をクリックします。

   設定がスキャナーに反映されます。

参考 ［ネットワークセキュリティー］ タブ - ［SSL/TLS］ - ［証明書］ - ［自己署名証明書］にある［表示］をクリックすると証明書の情報が確認できます。

関連情報

➡ 「ブラウザーでWeb Configを起動する」35ページ

相手サーバー検証用CA証明書を設定する

相手サーバー検証用CA証明書を設定すると、スキャナーがアクセスするサーバーのCA証明書のパスを検証できます。これによってなりすましを防止できます。
相手サーバー検証用CA証明書は相手サーバーのCA署名証明書を発行したCA局から入手できます。

相手サーバー検証用CA証明書をインポートする

相手サーバー検証用CA証明書をスキャナーにインポートします。

1. Web Configで［ネットワークセキュリティー］タブ - ［相手サーバー検証用CA証明書］を選択します。
2. ［インポート］をクリックします。
3. インポートする相手サーバー検証用CA証明書ファイルを指定します。
4. ［設定］をクリックします。

インポートされると［相手サーバー検証用CA証明書］に戻り、インポートされた相手サーバー検証用CA証明書の情報が表示されます。

関連情報

➡ 「ブラウザーでWeb Configを起動する」35ページ

相手サーバー検証用CA証明書を削除する

インポート済みの相手サーバー検証用CA証明書を削除します。

1. Web Configで［ネットワークセキュリティー］タブ - ［相手サーバー検証用CA証明書］を選択します。
2. 削除したい相手サーバー検証用CA証明書の［削除］をクリックします。
3. 確認のメッセージを確認して、削除します。
4. ［ネットワーク再起動］をクリックし、更新された画面で削除したCA証明書が一覧にないことを確認してください。

関連情報

➡ 「ブラウザーでWeb Configを起動する」35ページ

スキャナーとのSSL/TLS通信

SSL/TLS（Secure Sockets Layer/Transport Layer Security）通信でスキャナーにサーバー証明書を設定して、コンピューターとの通信経路を暗号化できます。なりすましや不正アクセスを防ぎたいときに設定してください。

SSL/TLS通信の基本設定をする

HTTPSサーバーに対応しているスキャナーはSSL/TLSで通信できます。Web Configを使ったスキャナーの設定や管理のための通信を安全に行えます。
基本設定では暗号強度とリダイレクト機能を設定します。

1. Web Configで［ネットワークセキュリティー］タブ - ［SSL/TLS］ - ［基本］を選択します。
2. 各項目を設定します。
   - 暗号強度
     暗号の強度を選択できます。
   - HTTPをHTTPSにリダイレクト
     HTTPでのアクセス時に、HTTPSにリダイレクトをします。
3. ［次へ］をクリックします。
   確認画面が表示されます。
4. ［設定］をクリックします。
   設定がスキャナーに反映されます。

関連情報

➡ 「ブラウザーでWeb Configを起動する」35ページ

スキャナーのサーバー証明書を設定する

1. Web Configで［ネットワークセキュリティー］タブ - ［SSL/TLS］ - ［証明書］を選択します。
2. ［使用するサーバー証明書］に使用する電子証明書を選択します。
   - 自己署名証明書
     スキャナーに内蔵されている自己署名証明書です。CA署名証明書を取得していない場合は選択してください。
   - CA署名証明書
     スキャナーにCA署名証明書をインポートすると選択できます。
3. ［次へ］をクリックします。
   確認画面が表示されます。
4. ［設定］をクリックします。
   設定がスキャナーに反映されます。

関連情報

➡ 「ブラウザーでWeb Configを起動する」35ページ
➡ 「CA署名証明書を設定する」104ページ
➡ 「相手サーバー検証用CA証明書を設定する」108ページ

IPsec/IPフィルタリングで暗号化通信する

IPsec/IPフィルタリングの概要

IPsec/IPフィルタリング機能を使用すると、IPアドレス、サービスの種類、受信や送信ポートなどをフィルタリングできます。これらを組み合わせることによって、特定のクライアントからのデータや特定の種類のデータを通過させたり、遮断したりできます。IPsecと組み合わせることによってさらに強固なセキュリティー通信ができます。

参考 Windows Vista以降またはWindows Server 2008以降のWindowsは、IPsecに対応しています。

基本ポリシーを設定する

フィルタリングのために基本ポリシーを設定します。基本ポリシーはスキャナーにアクセスする全てのクライアントに影響します。より細かくアクセスを制御するには、個別ポリシーを設定します。

1. Web Configで［ネットワークセキュリティー］タブ - ［IPsec/IPフィルタリング］ - ［基本］を選択します。
2. 各項目を設定します。
3. ［次へ］をクリックします。
   確認画面が表示されます。
4. ［設定］をクリックします。
   設定がスキャナーに反映されます。

関連情報

➡ 「ブラウザーでWeb Configを起動する」35ページ

基本ポリシーの設定項目

［基本ポリシー］

項目	設定値と説明
IPsec/IPフィルタリング	IPsec/IPフィルタリング機能を有効または無効にします。

- ［通信処理］
  IP通信の制御方法を設定します。

項目	設定値と説明
通信を通過	IPパケットの通過を許可するときに選択します。
通信を遮断	IPパケットを遮断したいときに選択します。
IPsecの使用	IPsecで送られたパケットの通過を許可するときに選択します。

- ［IKEバージョン］
  ［IKEバージョン］で［IKEv1］または［IKEv2］を選択します。スキャナーを接続する機器に合わせて選択してください。
  - IKEv1
    ［IKEバージョン］で［IKEv1］を選択すると表示されます。

項目	設定値と説明
認証方式	CA署名証明書をインポートすると［証明書］が選択できるようになります。
事前共有キー	［認証方式］で［事前共有キー］を選択した場合、1～127文字以内で事前共有キーを設定します。
事前共有キー確認入力	確認のため、設定したキーをもう一度入力します。

  - IKEv2
    ［IKEバージョン］で［IKEv2］を選択すると表示されます。

項目		設定値と説明
ローカル認証	認証方式	CA署名証明書をインポートすると［証明書］が選択できるようになります。
	IDの種類	［認証方式］で［事前共有キー］を選択した場合、スキャナーを何のIDで認証させるか選択します。
	ID	IDの種類に合わせてスキャナーのIDを入力します。 いずれの場合も先頭に@#=は使用できません。 ［識別名］：ASCII（0x20～0x7E）で表せる1バイト文字で1～255文字以内で入力します。=を含めてください。 ［IPアドレス］：IPv4またはIPv6形式で入力します。 ［FQDN］：半角英数字、ドット、ハイフンを組み合わせて1～255文字以内で入力します。 ［メールアドレス］：ASCII（0x20～0x7E）で表せる1バイト文字で1～255文字以内で入力します。@を含めてください。 ［任意の文字列］：ASCII（0x20～0x7E）で表せる1バイト文字で1～255文字以内で入力します。
	事前共有キー	［認証方式］で［事前共有キー］を選択した場合、1～127文字以内で事前共有キーを設定します。
	事前共有キー確認入力	確認のため、設定したキーをもう一度入力します。

項目		設定値と説明
リモート認証	認証方式	CA署名証明書をインポートすると［証明書］が選択できるようになります。
	IDの種類	［認証方式］で［事前共有キー］を選択した場合、認証相手を表すIDの種類を選択します。
	ID	IDの種類に合わせてスキャナーのIDを入力します。 いずれの場合も先頭に@#=は使用できません。 ［識別名］：ASCII（0x20～0x7E）で表せる1バイト文字で1～255文字以内で入力します。=を含めてください。 ［IPアドレス］：IPv4またはIPv6形式で入力します。 ［FQDN］：半角英数字、ドット、ハイフンを組み合わせて1～255文字以内で入力します。 ［メールアドレス］：ASCII（0x20～0x7E）で表せる1バイト文字で1～255文字以内で入力します。@を含めてください。 ［任意の文字列］：ASCII（0x20～0x7E）で表せる1バイト文字で1～255文字以内で入力します。
	事前共有キー	［認証方式］で［事前共有キー］を選択した場合、1～127文字以内で事前共有キーを設定します。
	事前共有キー確認入力	確認のため、設定したキーをもう一度入力します。

- ［カプセル化］
  ［通信処理］で［IPsecの使用］を選択した場合、IPsecの通信モードを設定します。

項目	設定値と説明
トランスポートモード	主に同じLAN内だけでスキャナーとIPsec通信をする場合に選択します。IPパケットのレイヤー4以上のデータ部のみが暗号化されます。
トンネルモード	主にIPsec-VPNのようなインターネットが有効なネットワークでスキャナーを接続するときに選択します。IPパケットのヘッダーとデータが暗号化されます。 ［リモートゲートウェイアドレス(トンネルモード)］：［カプセル化］で［トンネルモード］を選択した場合、1～39文字以内でゲートウェイアドレスを設定します。

- ［セキュリティープロトコル］
  ［通信処理］で［IPsecの使用］を選択した場合、IPsecのセキュリティープロトコルを選択します。

項目	設定値と説明
ESP	認証とデータの完全性の保証に加えてデータ全体を暗号化します。
AH	認証とデータの完全性の保証をします。データの暗号化が禁止されていてもIPsec通信ができます。

- ［アルゴリズム設定］
  全ての設定で［任意］を選択するか、個別に［任意］以外を選択することをお勧めします。一部のアルゴリズム設定［任意］にして、一部を［任意］ 以外で選択した場合、相手の設定によっては通信ができない場合があります。

項目		設定値と説明
IKE	暗号化アルゴリズム	IKEで利用する暗号化アルゴリズムを選択します。 IKEのバージョンで選択できる項目が異なります。
	認証アルゴリズム	IKEで利用する認証アルゴリズムを選択します。
	鍵交換アルゴリズム	IKEで利用する鍵交換アルゴリズムを選択します。 IKEのバージョンで選択できる項目が異なります。
ESP	暗号化アルゴリズム	ESPで利用する暗号化アルゴリズムを選択します。 ［セキュリティープロトコル］が［ESP］のときに選択できます。
	認証アルゴリズム	ESPで利用する認証アルゴリズムを選択します。 ［セキュリティープロトコル］が［ESP］のときに選択できます。
AH	認証アルゴリズム	AHで利用する認証アルゴリズムを選択します。 ［セキュリティープロトコル］が［AH］のときに選択できます。

個別ポリシーを設定する

個別ポリシーは、スキャナーへの各アクセスに適用されるルールです。IPパケットを受け取ったスキャナーはポリシーを参照し、IPパケットを制御します。ポリシーは、個別ポリシー1、個別ポリシー2と順に適用され、最後に基本ポリシーが適用されます。

1. Web Configで［ネットワークセキュリティー］タブ - ［IPsec/IPフィルタリング］ - ［基本］を選択します。
2. 設定したい番号のタブをクリックします。
3. 各項目を設定します。
4. ［次へ］をクリックします。
   確認画面が表示されます。
5. ［設定］をクリックします。
   設定がスキャナーに反映されます。

個別ポリシーの設定項目

項目	設定値と説明
この個別ポリシーを有効にする	選択している個別ポリシーを有効または無効にします。

［通信処理］

IP通信の制御方法を設定します。

項目	設定値と説明
通信を通過	IPパケットの通過を許可するときに選択します。
通信を遮断	IPパケットを遮断したいときに選択します。
IPsecの使用	IPsecで送られたパケットの通過を許可するときに選択します。

［ローカルアドレス（スキャナー）］
お使いの環境に合ったIPv4アドレスまたはIPv6アドレスを選択します。IPアドレスの取得方法が自動の場合は、［自動取得したIPv4アドレスを使用する］が選択できます。

参考 IPv6アドレスが自動取得の場合、リースや有効期限切れで通信できなくなることがあります。固定のIPv6アドレスを設定してください。

［リモートアドレス（ホスト）］
通信を制御する機器のIPアドレスを入力します。IPアドレスは43文字以内で入力してください。何も入力しないと、全てのIPアドレスが制御の対象になります。

参考 IPアドレスがDHCPや自動取得（IPv6）の場合、リースや有効期限切れで通信できなくなることがあります。固定のIPアドレスを設定してください。

［ポート指定方法］
ポートの指定方法を設定します。

- サービス名
  ［ポート指定方法］で［サービス名］を選択した場合、IPsecのセキュリティープロトコルを選択します。
- トランスポートプロトコル
  ［ポート指定方法］で［ポート番号］を選択した場合、IPsecの通信モードを設定します。

項目	設定値と説明
全てのプロトコル	全てのプロトコルタイプを制御したい場合に選択します。
TCP	ユニキャストのデータを制御したい場合などに選択します。
UDP	ブロードキャストやマルチキャストのデータを制御したい場合などに選択します。
ICMPv4	pingコマンドを制御したい場合などに選択します。

- ローカルポート番号
  ［ポート指定方法］で［ポート番号］を選択し、かつ［トランスポートプロトコル］で［TCP］または［UDP］を選択した場合は、受信パケットを制御するポート番号をカンマで区切って記述します。最大10個指定できます。
  例）20,80,119,5220
  何も記述しないと、全てのポートが制御の対象になります。
- リモートポート番号
  ［ポート指定方法］で［ポート番号］を選択し、かつ［トランスポートプロトコル］で［TCP］または［UDP］を選択した場合は、送信パケットを制御するポート番号をカンマで区切って記述します。最大10個指定できます。
  例）25,80,143,5220
  何も記述しないと、全てのポートが制御の対象になります。

［IKEバージョン］

［IKEバージョン］で［IKEv1］または［IKEv2］を選択します。スキャナーを接続する機器に合わせて選択してください。

- IKEv1
  ［IKEバージョン］で［IKEv1］を選択すると表示されます。

項目	設定値と説明
認証方式	［通信処理］で［IPsecの使用］を選択した場合、IPsecのセキュリティープロトコルを選択します。この証明書は基本ポリシーで設定したCA署名証明書と共通です。
事前共有キー	［認証方式］で［事前共有キー］を選択した場合、1～127文字以内で事前共有キーを設定します。
事前共有キー確認入力	確認のため、設定したキーをもう一度入力します。

- IKEv2
  ［IKEバージョン］で［IKEv2］を選択すると表示されます。

項目		設定値と説明
ローカル認証	認証方式	［通信処理］で［IPsecの使用］を選択した場合、IPsecのセキュリティープロトコルを選択します。この証明書は基本ポリシーで設定したCA署名証明書と共通です。
	IDの種類	［認証方式］で［事前共有キー］を選択した場合、スキャナーを何のIDで認証させるか選択します。
	ID	IDの種類に合わせてスキャナーのIDを入力します。 いずれの場合も先頭に@#=は使用できません。 ［識別名］：ASCII（0x20～0x7E）で表せる1バイト文字で1～255文字以内で入力します。=を含めてください。 ［IPアドレス］：IPv4またはIPv6形式で入力します。 ［FQDN］：半角英数字、ドット、ハイフンを組み合わせて1～255文字以内で入力します。 ［メールアドレス］：ASCII（0x20～0x7E）で表せる1バイト文字で1～255文字以内で入力します。@を含めてください。 ［任意の文字列］：ASCII（0x20～0x7E）で表せる1バイト文字で1～255文字以内で入力します。
	事前共有キー	［認証方式］で［事前共有キー］を選択した場合、1～127文字以内で事前共有キーを設定します。
	事前共有キー確認入力	確認のため、設定したキーをもう一度入力します。
リモート認証	認証方式	［通信処理］で［IPsecの使用］を選択した場合、IPsecのセキュリティープロトコルを選択します。この証明書は基本ポリシーで設定したCA署名証明書と共通です。
	IDの種類	［認証方式］で［事前共有キー］を選択した場合、認証相手を表すIDの種類を選択します。
	ID	IDの種類に合わせてスキャナーのIDを入力します。 いずれの場合も先頭に@#=は使用できません。 ［識別名］：ASCII（0x20～0x7E）で表せる1バイト文字で1～255文字以内で入力します。=を含めてください。 ［IPアドレス］：IPv4またはIPv6形式で入力します。 ［FQDN］：半角英数字、ドット、ハイフンを組み合わせて1～255文字以内で入力します。 ［メールアドレス］：ASCII（0x20～0x7E）で表せる1バイト文字で1～255文字以内で入力します。@を含めてください。 ［任意の文字列］：ASCII（0x20～0x7E）で表せる1バイト文字で1～255文字以内で入力します。
	事前共有キー	［認証方式］で［事前共有キー］を選択した場合、1～127文字以内で事前共有キーを設定します。
	事前共有キー確認入力	確認のため、設定したキーをもう一度入力します。

［カプセル化］
［通信処理］で［IPsecの使用］を選択した場合、IPsecの通信モードを設定します。

項目	設定値と説明
トランスポートモード	主に同じLAN内だけでスキャナーとIPsec通信をする場合に選択します。IPパケットのレイヤー4以上のデータ部のみが暗号化されます。
トンネルモード	主にIPsec-VPNのようなインターネットが有効なネットワークでスキャナーを接続するときに選択します。IPパケットのヘッダーとデータが暗号化されます。 ［リモートゲートウェイアドレス(トンネルモード)］：［カプセル化］で［トンネルモード］を選択した場合、1～39文字以内でゲートウェイアドレスを設定します。

［セキュリティープロトコル］
［通信処理］で［IPsecの使用］を選択した場合、IPsecのセキュリティープロトコルを選択します。

項目	設定値と説明
ESP	認証とデータの完全性の保証に加えてデータ全体を暗号化します。
AH	認証とデータの完全性の保証をします。データの暗号化が禁止されていてもIPsec通信ができます。

［アルゴリズム設定］
全ての設定で［任意］を選択するか、個別に［任意］以外を選択することをお勧めします。一部のアルゴリズム設定を［任意］にして、一部を［任意］以外で選択した場合、相手の設定によっては通信ができない場合があります。

項目		設定値と説明
IKE	暗号化アルゴリズム	IKEで利用する暗号化アルゴリズムを選択します。 IKEのバージョンで選択できる項目が異なります。
	認証アルゴリズム	IKEで利用する認証アルゴリズムを選択します。
	鍵交換アルゴリズム	IKEで利用する鍵交換アルゴリズムを選択します。 IKEのバージョンで選択できる項目が異なります。
ESP	暗号化アルゴリズム	ESPで利用する暗号化アルゴリズムを選択します。 ［セキュリティープロトコル］が［ESP］のときに選択できます。
	認証アルゴリズム	ESPで利用する認証アルゴリズムを選択します。 ［セキュリティープロトコル］が［ESP］のときに選択できます。
AH	認証アルゴリズム	AHで利用する認証アルゴリズムを選択します。 ［セキュリティープロトコル］が［AH］のときに選択できます。

ローカルアドレス（スキャナー）とリモートアドレス（ホスト）の組み合わせ

	ローカルアドレス（スキャナー）の設定値		
	IPv4	IPv6*2	使用可能な全てのアドレス*3

リモートアドレス（ホスト）の設定値	IPv4*1	○	×	○
	IPv6*1*2	×	○	○
	空白	○	○	○

*1 ［通信処理］で［IPsecの使用］を選択した場合、範囲指定はできません。

*2 ［通信処理］で［IPsecの使用］を選択した場合リンクローカルアドレス（fe80::）は選択できますが、個別ポリシーは無効になります。

*3 IPv6リンクローカルアドレスは除きます。

関連情報

➡ 「ブラウザーでWeb Configを起動する」35ページ

個別ポリシーのサービス名一覧

参考 非対応のサービスは表示されますが、選択できません。

サービス名	プロトコルタイプ	ローカルポート番号	リモートポート番号	制御できる機能
全て	-	-	-	全てのサービス
ENPC	UDP	3289	任意	Epson Device Adminなどのアプリケーションソフト、スキャナードライバーからのスキャナー探索
SNMP	UDP	161	任意	Epson Device Adminなどのアプリケーションソフト、スキャナードライバーからのスキャナーMIB情報の取得と設定
WSD	TCP	任意	5357	WSDの制御
WS-Discovery	UDP	3702	任意	WSDのスキャナー探索
Network Scan	TCP	1865	任意	Document Capture Proからのスキャンデータの転送
Network Push Scan	TCP	任意	2968	Document Capture Proからのプッシュスキャン時のジョブ情報取得
Network Push Scan Discovery	UDP	2968	任意	スキャナーからのコンピューター探索
FTP データ (リモート)	TCP	任意	20	FTPクライアント（スキャンデータのFTP転送） ただし、制御できるのは20番のリモートポート番号を使用するFTPサーバーのみ
FTP 制御 (リモート)	TCP	任意	21	FTPクライアント（スキャンデータのFTP転送の制御）

サービス名	プロトコルタイプ	ローカルポート番号	リモートポート番号	制御できる機能
CIFS (リモート)	TCP	任意	445	CIFSクライアント（スキャンデータのフォルダー転送）
NetBIOS Name Service (リモート)	UDP	任意	137	CIFSクライアント（スキャンデータのフォルダー転送）
NetBIOS Datagram Service (リモート)	UDP	任意	138	
NetBIOS Session Service (リモート)	TCP	任意	139	
HTTP (ローカル)	TCP	80	任意	HTTP(S)サーバー（Web ConfigやWSDのデータ転送）
HTTPS (ローカル)	TCP	443	任意	
HTTP (リモート)	TCP	任意	80	HTTP(S)クライアント（ファームウェアアップデートやルート証明書の更新）
HTTPS (リモート)	TCP	任意	443	

IPsec/IPフィルタリングの設定例

IPsecで保護されたパケットだけを受け付ける

個別ポリシーを設定しない場合は、基本ポリシーのみ使われます。

［基本ポリシー］：

- ［IPsec/IPフィルタリング］：［有効］
- ［通信処理］：［IPsecの使用］
- ［認証方式］：［事前共有キー］
- ［事前共有キー］：1～127文字以内の任意文字

［個別ポリシー］：設定しない

スキャンデータとスキャナー設定を受け付ける

指定したサービスからのスキャンデータとスキャナー設定の通信を受け付ける場合の例です。

［基本ポリシー］：

- ［IPsec/IPフィルタリング］：［有効］
- ［通信処理］：［通信を遮断］

［個別ポリシー］：

- ［この個別ポリシーを有効にする］：チェックを入れる

- ［通信処理］：［通信を通過］
- ［リモートアドレス（ホスト）］：クライアントのIPアドレス
- ［ポート指定方法］：［サービス名］
- ［サービス名］：［ENPC］、［SNMP］、［HTTP (ローカル)］、［HTTPS (ローカル)］、［Network Scan］にチェックを入れる

特定のIPアドレスからの通信のみ受け付ける

管理者など特定のコンピューターからの通信のみを受け付ける場合の例です。
［基本ポリシー］：

- ［IPsec/IPフィルタリング］：［有効］
- ［通信処理］：［通信を遮断］

［個別ポリシー］：

- ［この個別ポリシーを有効にする］：チェックを入れる
- ［通信処理］：［通信を通過］
- ［リモートアドレス（ホスト）］：管理者用クライアントのIPアドレス

参考 ポリシーの設定に関わらず、スキャナーの検索や設定を行うためのプロトコルは使用できます。

IPsec/IPフィルタリングで使用する証明書を設定する

IPsec/IPフィルタリングで使用するクライアント証明書を設定します。設定すると、IPsec/IPフィルタリングの認証方式で証明書を使用できるようになります。なお、相手サーバー検証用の証明書を設定する場合は、［相手サーバー検証用CA証明書］で行います。

1. Web Configで［ネットワークセキュリティー］タブ - ［IPsec/IPフィルタリング］ - ［クライアント証明書］を選択します。

2. ［クライアント証明書］画面で証明書をインポートします。

   CA局が発行した証明書をインポートしている場合は、証明書をコピーしてIPsec/IPフィルタリングで使用できます。コピーする場合は、［コピー元］からどの証明書を使うか選択して［コピー］をクリックしてください。

関連情報

➡ 「ブラウザーでWeb Configを起動する」35ページ
➡ 「CA署名証明書を設定する」104ページ
➡ 「相手サーバー検証用CA証明書を設定する」108ページ

IEEE802.1X環境にスキャナーを接続する

IEEE802.1Xを設定する

スキャナーにIEEE802.1Xを設定すると、RADIUSサーバーと認証機能を持ったLANスイッチやアクセスポイントに接続されたネットワークで使用できます。

1. Web Configで［ネットワークセキュリティー］タブ - ［IEEE802.1X］ - ［基本］を選択します。
2. 各項目を設定します。
   無線LANで使う場合は［無線LAN設定］をクリックしてSSIDを選択するか、入力してください。
   参考 ここでの設定値は有線LANと無線LANで共通に使えます。
3. ［次へ］をクリックします。
   確認画面が表示されます。
4. ［設定］をクリックします。
   設定がスキャナーに反映されます。

関連情報

➡ 「ブラウザーでWeb Configを起動する」35ページ

IEEE802.1Xの設定項目

項目	設定値と説明	
IEEE802.1X (有線LAN)	［IEEE802.1X］ - ［基本］画面で設定した値をIEEE802.1X（有線LAN）に対して有効または無効にするかを選択します。	
IEEE802.1X (無線LAN)	IEEE802.1X（無線LAN）の接続状態が表示されます。	
接続方法	現在のネットワーク接続方法が表示されます。	
認証方式	スキャナーとRADIUSサーバーとの認証方式を設定します。	
	EAP-TLS	CA署名証明書を取得してインポートする必要があります。
	PEAP-TLS	
	PEAP/MSCHAPv2	パスワードを設定する必要があります。
	EAP-TTLS	
ユーザーID	RADIUSサーバーの認証に使うIDを設定します。 ASCII（0x20～0x7E）で表せる1バイト文字で1～128文字以内で入力します。	

項目	設定値と説明	
パスワード	スキャナーを認証するためのパスワードを設定します。 ASCII（0x20～0x7E）で表せる1バイト文字で1～128文字以内で入力します。Windowsサーバーを RADIUSサーバーとして使用する場合は、最大127文字になります。	
パスワード確認入力	確認のため、入力したパスワードをもう一度入力します。	
サーバーID	特定のRADIUSサーバーで認証したいときに使用します。設定した文字列が、RADIUSサーバーから送信されるサーバー証明書のsubjectフィールドまたはsubjectAltNameフィールドに含まれているかを検証します。 ASCII（0x20～0x7E）で表せる1バイト文字で0～128文字以内で入力します。	
証明書の検証	相手サーバー証明書の検証を設定します。認証方式に関わらず設定ができます。［相手サーバー検証用CA証明書］画面で証明書をインポートします。	
Anonymous名	［認証方式］が［PEAP-TLS］または［PEAP/MSCHAPv2］ の場合、PEAP認証のフェーズ1において、ユーザーIDの代わりに匿名を使用したいときに設定します。 ASCII（0x20～0x7E）で表せる1バイト文字で0～128文字以内で入力します。	
暗号強度	以下のいずれかを選択します。	
	高い	AES256/3DES
	標準	AES256/3DES/AES128/RC4

IEEE802.1Xで使用する証明書を設定する

IEEE802.1Xで使用するクライアント証明書を設定します。設定すると、IEEE802.1Xの認証方式で［EAP-TLS］と［PEAP-TLS］が使用できるようになります。なお、相手サーバー検証用の証明書を設定する場合は、［相手サーバー検証用CA証明書］で行います。

1. Web Configで［ネットワークセキュリティー］タブ - ［IEEE802.1X］ - ［クライアント証明書］を選択します。

2. ［クライアント証明書］に使用する電子証明書を設定します。

   CA局が発行した証明書をインポートしている場合は、証明書をコピーしてIEEE802.1Xで使用できます。コピーする場合は、［コピー元］からどの証明書を使うか選択して［コピー］をクリックしてください。

関連情報

➡ 「ブラウザーでWeb Configを起動する」35ページ

トラブルを解決する

セキュリティー設定の初期化

IPsec/IPフィルタリングなど高度なセキュア環境を構築している場合、設定ミスや機器、サーバーのトラブルなどでデバイスと通信できなくなる可能性があります。この場合、セキュリティー機能を初期化してデバイスの設定をやり直したり、一時的に使用できるようにしたりします。

Web Configからセキュリティー機能を無効化する

Web Configを使って、IPsec/IPフィルタリングを無効にできます。

1. Web Configで［ネットワークセキュリティー］タブ-［IPsec/IPフィルタリング］-［基本］を選択します。
2. ［IPsec/IPフィルタリング］で設定を無効にしてください。

セキュア環境への接続時のトラブル

事前共有キーを忘れてしまった

事前共有キーを再設定する

Web Configの［ネットワークセキュリティー］タブ - ［IPsec/IPフィルタリング］ - ［基本］ - ［基本ポリシー］または［個別ポリシー］の画面でキーを変更します。
事前共有キーを変更したら、相手先コンピューターの事前共有キーの設定もやり直してください。

関連情報

➡ 「ブラウザーでWeb Configを起動する」35ページ
➡ 「IPsec/IPフィルタリングで暗号化通信する」110ページ

IPsec通信ができない

スキャナーまたはコンピューターがサポートしていないアルゴリズムを指定している

スキャナーがサポートするアルゴリズムは以下の通りです。コンピューターの設定を確認してください。

セキュリティーメソッド	アルゴリズム
IKE暗号化アルゴリズム	AES-CBC-128、AES-CBC-192、AES-CBC-256、AES-GCM-128*、AES-GCM-192*、AES-GCM-256*、3DES

セキュリティーメソッド	アルゴリズム
IKE認証アルゴリズム	SHA-1、SHA-256、SHA-384、SHA-512、MD5
IKE鍵交換アルゴリズム	DH Group1、DH Group2、DH Group5、DH Group14、DH Group15、DH Group16、DH Group17、DH Group18、DH Group19、DH Group20、DH Group21、DH Group22、DH Group23、DH Group24、DH Group25、DH Group26、DH Group27*、DH Group28*、DH Group29*、DH Group30*
ESP暗号化アルゴリズム	AES-CBC-128、AES-CBC-192、AES-CBC-256、AES-GCM-128、AES-GCM-192、AES-GCM-256、3DES
ESP認証アルゴリズム	SHA-1、SHA-256、SHA-384、SHA-512、MD5
AH認証アルゴリズム	SHA-1、SHA-256、SHA-384、SHA-512、MD5

*：IKEv2のみ対応

関連情報

➡ 「IPsec/IPフィルタリングで暗号化通信する」110ページ

突然通信ができなくなった

スキャナーのIPアドレスが変更された、または使用できなくなった

個別ポリシーのローカルアドレスに登録されているIPアドレスが変更や使用できなくなった場合、IPsecでは通信できなくなります。スキャナーの操作パネルでIPsecを無効にしてください。
Web Configの［ネットワークセキュリティー］タブ-［IPsec/IPフィルタリング］-［基本］-［個別ポリシー］-［ローカルアドレス（スキャナー）］に設定したIPアドレスが、DHCPのリース切れや再起動、IPv6アドレスの有効期限切れや再取得失敗によって見つからない可能性があります。
IPアドレスは、固定のIPアドレスを使用してください。

コンピューターのIPアドレスが変更された、または使用できなくなった

個別ポリシーのリモートアドレスに登録されているIPアドレスが変更や使用できなくなった場合、IPsecでは通信できなくなります。
スキャナーの操作パネルでIPsecを無効にしてください。
Web Configの［ネットワークセキュリティー］タブ-［IPsec/IPフィルタリング］-［基本］-［個別ポリシー］-［リモートアドレス（ホスト）］に設定したIPアドレスが、DHCPのリース切れや再起動、IPv6アドレスの有効期限切れや再取得失敗によって見つからない可能性があります。
IPアドレスは、固定のIPアドレスを使用してください。

関連情報

➡ 「ブラウザーでWeb Configを起動する」35ページ
➡ 「IPsec/IPフィルタリングで暗号化通信する」110ページ

IPsec/IPフィルタリング設定したのにつながらない

IPsec/IPフィルタリングの設定が間違っている

スキャナーの操作パネルからIPsec/IPフィルタリングを無効にしてください。スキャナーとコンピューターを接続して、IPsec/IPフィルタリングの設定をやり直してください。

関連情報

➡ 「IPsec/IPフィルタリングで暗号化通信する」110ページ

IEEE802.1Xを設定したのにつながらない

IEEE802.1Xの設定が間違っている

スキャナーの操作パネルから無線LANとIEEE802.1Xを無効にしてください。スキャナーとコンピューターを接続して、IEEE802.1Xの設定をやり直してください。

関連情報

➡ 「IEEE802.1Xを設定する」122ページ

電子証明書使用時のトラブル

CA署名証明書のインポートができない

入手したCA署名証明書と作成したCSRの情報が一致していない

CA署名証明書とCSRは、同一の情報である必要があります。以下の点を確認してください。

- 同時に複数の機器でCSRを作成した場合、一致しない機器に証明書をインポートしようとしたか
  情報を確認して、一致する機器にインポートしてください
- CA局にCSRを送付した後、スキャナーに保存されているCSRを再生成したか
  再生成したCSRでCA署名証明書を取得し直してください。

入手したCA署名証明書のファイル容量が5KBを超えている

5KBを超えるCA署名証明書は、インポートできません。

証明書をインポートする際のパスワードが正しくない

正しいパスワードを入力してください。パスワードを忘れた場合、証明書をインポートできません。CA署名証明書を取得し直してください。

関連情報

➡ 「CA署名証明書をインポートする」106ページ

自己署名証明書が更新できない

コモンネームが入力されていない

［コモンネーム］は必ず入力してください。

コモンネームに不正な文字が使用されている

IPv4、IPv6、ホスト名、FQDNのいずれかの形式をASCII (0x20-0x7E)で表せる1～128文字以内で指定します。

［コモンネーム］にカンマやスペースが使われている

カンマが入力されると［コモンネーム］はそこで分割されます。また、カンマの前後にスペースを入れるとエラーになります。

関連情報

➡ 「自己署名証明書を更新する」107ページ

CSRが作成できない

コモンネームが入力されていない

［コモンネーム］は必ず入力してください。

コモンネーム、組織名、部署名、市町村名、都道府県名に不正な文字が使用されている

IPv4、IPv6、ホスト名、FQDNのいずれかの形式をASCII (0x20-0x7E)で表せる文字で指定します。

コモンネームにカンマやスペースが使われている

カンマが入力されると［コモンネーム］はそこで分割されます。また、カンマの前後にスペースを入れるとエラーになります。

関連情報

➡ 「CA署名証明書を取得する」104ページ

証明書に関する警告が表示された

メッセージ	原因と対処
サーバー証明書を指定してください。	**原因：** インポートするファイルが指定されていません。 **対処：** ファイルを選択してから［インポート］をクリックしてください。
CA証明書1の参照先を入力してください。	**原因：** CA証明書1が未入力で、CA証明書2のみ入力されています。 **対処：** 先にCA証明書1をインポートしてください。

メッセージ	原因と対処
以下の入力値が正しくありません。	**原因：** ファイルパスやパスワードに不正な文字が含まれています。 **対処：** 表示された項目に入力した文字が正しいか確認してください。
日付/時刻が設定されていません。	**原因：** スキャナーに日付や時刻が設定されていません。 **対処：** Web ConfigやEpsonNet Configから日付や時刻を設定してください。
パスワードが正しくありません。	**原因：** CA証明書に設定されているパスワードと入力したパスワードが一致しません。 **対処：** 正しいパスワードを入力してください。
不正なファイルです。	**原因：** インポートしようとしたファイルがX509形式の証明書ではありません。 **対処：** 信頼されたCA局から送付された証明書ファイルを選択しているか確認してください。
	原因： インポートできるファイルサイズを超えています。インポートできるファイルサイズは5KBです。 **対処：** ファイルが正しい場合、証明書が破損していたり改ざんされていたりする可能性があります。
	原因： 証明書に含まれるチェーンが不正です。 **対処：** 証明書の詳細はCA局のWebサイトをご覧ください。
3つ以上のCA証明書が含まれたサーバー証明書は使用できません。	**原因：** PKCS#12形式の証明書ファイルに3つ以上のCA証明書が含まれています。 **対処：** PKCS#12形式から複数のPEM形式に変換して個別にインポートするか、2つ以下のCA証明書でPKCS#12形式ファイルを再作成してインポートしてください。
有効期間外の証明書です。証明書の有効期間、または日付/時刻設定を確認してください。	**原因：** 証明書の有効期限が切れています。 **対処：** • 証明書の有効期限が切れている場合、新しい証明書をCA局から取得してインポートしてください。 • 証明書の有効期限が切れていない場合、スキャナーの日付や時刻の設定が正しいか確認してください。

メッセージ	原因と対処
秘密鍵が必要な証明書ファイルです。	**原因：** 証明書と対になった秘密鍵がありません。 **対処：** • コンピューターで生成したCSRで取得したPEM/DER形式の証明書の場合、秘密鍵ファイルを指定してください。 • コンピューターで生成したCSRで取得したPKCS#12形式の証明書の場合、秘密鍵を含めたファイルを作成してください。
	原因： Web Configで生成したCSRで取得したPEM/DER形式の証明書を再度インポートしようとしました。 **対処：** Web Configで生成したCSRで取得したPEM/DER形式の証明書は、一度しかインポートできません。
設定に失敗しました。	**原因：** スキャナーとコンピューターの通信が遮断された、何らかの原因でファイルが読み取りできない、などの原因で正しく設定できませんでした。 **対処：** 指定しているファイルや通信状況を確認して、再度インポートしてください。

関連情報

➡ 「使用できる電子証明書」104ページ

CA署名証明書を誤って削除した

CA署名証明書をバックアップ保存したファイルがない

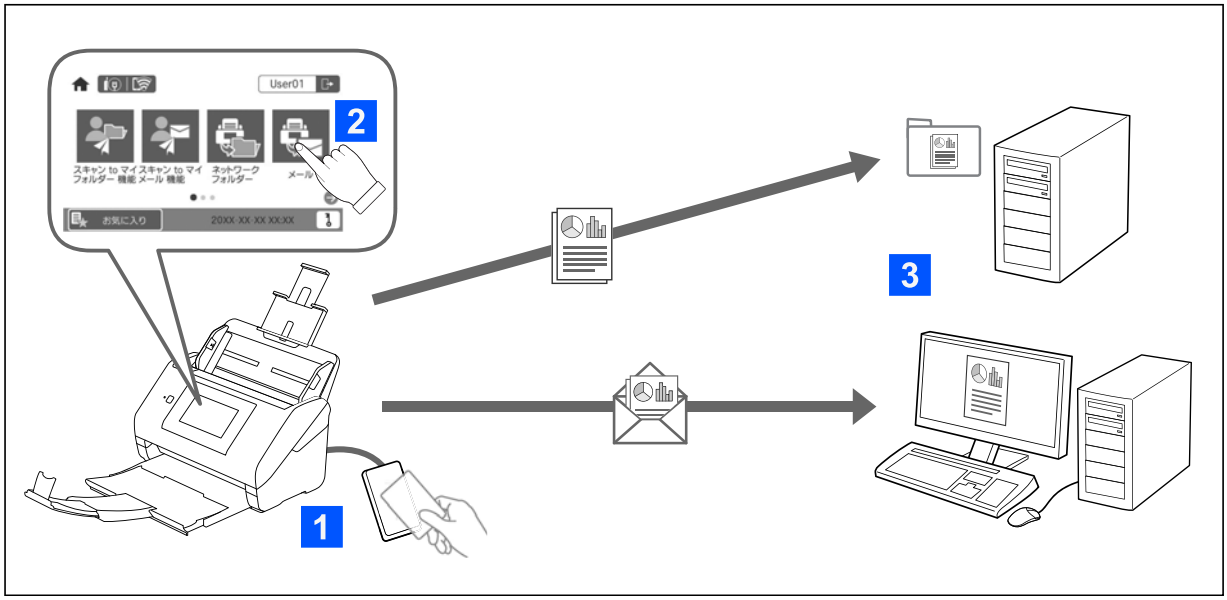
CA署名証明書をバックアップ保存したファイルがあれば、それを使って再度インポートしてください。
Web Configで生成したCSRで取得した証明書は、一度削除してしまうと再インポートができません。CSRを再生成して証明書を取得し直してください。

関連情報

➡ 「CA署名証明書をインポートする」106ページ
➡ 「CA署名証明書を削除する」107ページ

認証設定

認証設定について



認証設定を有効にすると、スキャンを開始するときにユーザー認証が必要です。ユーザーごとに使用できるスキャン方法を設定でき、宛先間違いを防止できます。
スキャンの宛先として、認証されたユーザー自身のメールアドレスを指定したり（スキャン to マイメール 機能）、ユーザーごと別々のフォルダーに保存したり（スキャン to マイフォルダー機能）できます。その他のスキャン方法も指定できます。

参考
- 認証設定が有効なときは、コンピューターおよびスマートデバイスからスキャンすることはできません。
- 本書で案内している認証設定以外にも、認証用のサーバーを利用した認証システムを構築できます。構築には、Document Capture Pro Server Authentication Edition（略称：Document Capture Pro Server AE）が必要です。詳しくは、エプソンの問い合わせ窓口にお問い合わせください。

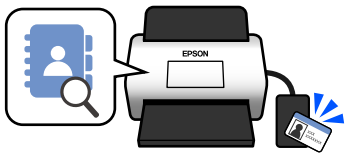
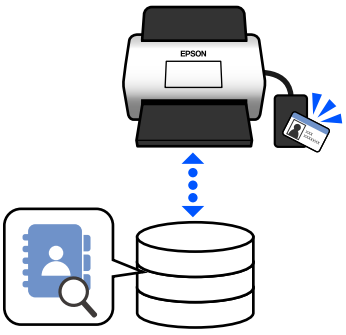
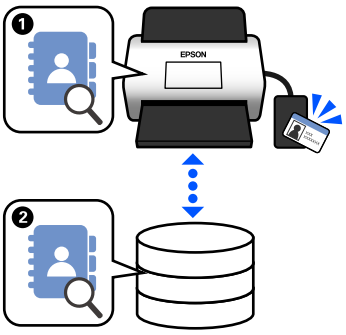
認証設定で使用できる機能

操作パネルのスキャン機能	認証設定	
	有効時	無効時
スキャン to マイフォルダー 機能 認証ユーザーに割り当てられたフォルダーに画像を保存します。	○	-
スキャン to マイメール 機能 認証ユーザー自身のメールアドレスに画像を送信します。	○	-
スキャン to ネットワークフォルダー ネットワーク上のフォルダーに画像を保存します。	○	○
スキャン to コンピューター Document Capture Pro（Windows）/Document Capture（Mac OS）で作成したジョブを使用して、接続しているコンピューターに画像を保存します。 *認証設定有効時は、［お気に入り］に登録したジョブのみ使用できます。	○*	○

操作パネルのスキャン機能	認証設定	
	有効時	無効時
スキャン to メール 設定したメールアドレスに画像を送信します。	○	○
スキャン to クラウド 設定したクラウドサービスに画像を送信します。	○	○
スキャン to USBドライブ スキャナーに接続したUSBドライブに画像を保存します。スキャナーに認証装置が接続されていないときのみ使用できます。	○	○
お気に入り お気に入りのスキャン機能を最大48件まで登録できます。 本体認証に登録したユーザーには登録したお気に入りから5件まで割り当てられます。割り当てたお気に入りは、そのユーザーだけが使用できます。どのユーザーにも割り当てられていないお気に入りは、全てのユーザーが使用できます。	○	○

認証方式の概要

本スキャナーは、認証用のサーバーを構築しなくても以下の方式で認証できます。

	本体認証	LDAPサーバー認証	本体認証とLDAPサーバー認証
ユーザー情報の照合先	**本体メモリ** スキャナーに登録されているユーザー情報と、スキャンを利用するユーザー情報を照合して認証します。	**LDAPサーバー*** 連携しているLDAPサーバーにユーザー情報を照合して認証します。LDAPサーバーのユーザー情報は300件までスキャナー本体にキャッシュとして一時的に保存されるため、LDAPサーバーの障害時にはキャッシュを使って認証ができます。 * LDAPで通信できるディレクトリーサービスを提供しているサーバー	**本体メモリおよびLDAPサーバー** 先にスキャナーに登録されているユーザー情報を照合して（❶）、該当がなかった場合はLDAPサーバーにユーザー情報を照合します（❷）。
			
登録ユーザー数	50件（本体）	無制限（LDAPサーバー）	50件（本体） 無制限（LDAPサーバー）

	本体認証	LDAPサーバー認証	本体認証とLDAPサーバー認証
本体のキャッシュ	-	300件	最大300件 （キャッシュ枠のうち50件は本体認証のユーザー設定と共有）
ログオンの手段	以下の手段のいずれかを使用できます。 • 認証カードをかざす、または［ユーザーID］と［パスワード］を入力 • 認証カードをかざす、または［ID番号］を入力 • ［ユーザーID］と［パスワード］を入力 • ［ユーザーID］を入力 • ［ID番号］を入力		
スキャン to 機能の制限	ユーザーごと個別に設定	LDAPサーバー認証ユーザー全員に同じ設定	本体認証ユーザー：個別に設定 LDAPサーバー認証ユーザー：全員に同じ設定
お気に入りのユーザーへの割り当て	1ユーザーにつき5件まで	- （個別設定不可）	本体認証ユーザー：1ユーザーにつき5件まで LDAPサーバー認証ユーザー：-

セットアップに使うソフトウェア

Web ConfigまたはEpson Device Adminを使ってセットアップします。

- Web Configを使うと、ブラウザーだけでセットアップできます。
「Web Config」35ページ
- Epson Device Adminを使うと、設定テンプレートを使って、複数のスキャナーに一度に設定を適用できます。
「Epson Device Admin」36ページ

スキャナーのファームウェアを更新する

認証設定を有効にする前に、スキャナーのファームウェアを最新版に更新します。事前にスキャナーをインターネットに接続しておいてください。

!重要 更新中は、コンピューターやスキャナーの電源を切らないでください。

Web Configで設定する場合：
［デバイス管理］タブ-［ファームウェアアップデート］を選択して、画面の指示に従ってファームウェアを更新します。
Epson Device Adminで設定する場合：
デバイスの一覧画面で［ホーム］-［ファームウェア］-［更新］を選択して、画面の指示に従ってファームウェアを更新します。

参考 すでに最新のファームウェアがインストールされているときは、更新は不要です。

認証装置の接続と設定

ICカードリーダーなどの認証装置を接続して使用する場合は、装置の設定をしてください。認証装置を使わない場合は必要ありません。

関連情報

- 「認証装置の接続」134ページ
- 「認証装置の設定」135ページ

認証装置の動作確認情報

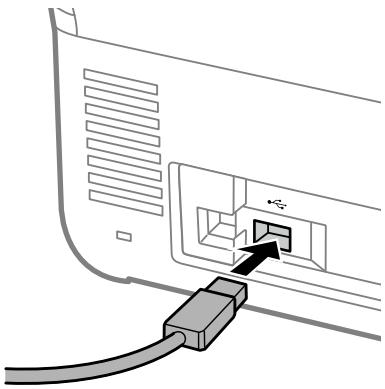
Yes：対応（認証装置の標準設定で、認証カードシリアル番号の読み取りが可能）
No：非対応

メーカー	モデル名	型番	認証カード				対応モード
			MIFARE		FeliCa™		
			Classic	Ultralight	Standard	Lite/Lite-S	
Sony	PaSoRi	RC-S380/S	Yes	Yes	Yes	Yes	PaSoRi
Sony	PaSoRi	RC-S300/S1	Yes	Yes	Yes	Yes	PaSoRi

認証装置の接続

!重要 複数のスキャナーに認証装置を接続する場合は、同じ型番の製品を使用してください。

認証装置のUSBケーブルを、スキャナーの外部機器接続用USBポートに差し込みます。



認証装置の接続確認

認証装置の接続状態や認証カードの認識状態は、スキャナーの操作パネルから確認できます。
［設定］ - ［機器情報］ - ［認証装置ステータス］に状態が表示されます。

認証装置の設定

認証カードから取得する認証情報の読み取り形式を設定します。
各項目は購入時の設定のまま使用します。

参考 メーカーが違う認証カードの使用について：
カード情報のUID（製造番号などカードのID情報）を使用する場合は、複数の種類の認証カードを混在して使用できます。
それ以外のカード情報を使用する場合は混在できません。

Web Configで設定する場合：
［デバイス管理］タブ -［認証装置］を選択します。
Epson Device Adminで設定する場合：
設定テンプレートで［管理者設定］-［認証機能設定］-［認証装置］を選択します。

項目	説明
Vendor ID	0000に設定します。
Product ID	0000に設定します。
動作パラメーター	空欄にします。
認証装置	［カスタム (フォーマット1)］を選択します。
認証カードID保存フォーマット	［フォーマット 1 (デフォルト) ］を選択します。
認証カードIDの読み取り設定をする	チェックを外します。
開始文字位置	設定しません。
文字数	設定しません。

情報の登録と設定

セットアップの流れ

認証方式や、使用するスキャン方法に応じて、必要な設定をしてください。

!重要 設定を始める前にスキャナーの時刻設定が正しいか確認してください。
時刻設定が正しくないと「ライセンスが期限切れです」というエラーメッセージが表示され、セットアップができなくなります。また、SSL/TLS通信やIPsecなどセキュリティー機能を使用する場合も正しい時刻設定が必要です。時刻は以下から設定できます。

- Web Config：［デバイス管理］タブ - ［日付/時刻］ - ［日付/時刻］
- スキャナーの操作パネル：［設定］ - ［基本設定］ - ［日付/時刻設定］

設定	本体認証	LDAPサーバー認証	本体認証とLDAPサーバー認証
認証の有効化 認証設定を行う前に、認証を有効化します。 「認証の有効化」136ページ	○	○	○
認証設定 認証方式と認証手段を設定します。 「認証設定」137ページ	○	○	○
ユーザー設定の登録 各ユーザーの設定を登録します。CSVファイルを使って一括で登録することもできます。 「ユーザー設定の登録」138ページ	○	×	○
LDAPサーバーとの連携 LDAPサーバーの連携設定をします。 「LDAPサーバーとの連携」144ページ	×	○	○
メールサーバーの設定 利用するメールサーバーを設定します。スキャン to マイメール 機能など、メールサーバーの設定が必要な機能を使用する場合に設定します。 「メールサーバーの設定」147ページ	○	○	○
スキャン to マイフォルダー機能の設定 保存先のフォルダーなどを設定します。スキャン to マイフォルダー機能を使用する場合に設定します。 「スキャン to マイフォルダー機能の設定」148ページ	○	○	○
ホーム画面編集 操作パネルに表示する項目を変更する場合に設定します。操作パネルに必要なアイコンだけを表示させたり、アイコンの並び順を変更したりできます。 「ホーム画面編集」150ページ	○	○	○

認証の有効化

認証設定を行う前に、認証を有効化します。

Web Configで設定する場合：

［本体セキュリティー］タブ - ［基本］ - ［認証機能］で、［オン(本体/LDAPサーバー)］を選択します。

Epson Device Adminで設定する場合：

設定テンプレートで［管理者設定］-［認証機能設定］-［基本］-［認証機能］で、［オン(本体/LDAPサーバー)］を選択します。

参考 スキャナーの認証設定を有効にすると、操作パネルも管理者ロックされます。認証設定が有効なときはロックを解除できません。
認証設定を無効にしても、管理者ロックは有効のままです。無効にしたいときは、操作パネルまたはWeb Configから設定します。

関連情報

- 「操作パネルで管理者ロックを設定する」91ページ
- 「Web Configで管理者ロックを設定する」91ページ

認証設定

認証方式と認証手段を設定します。
Web Configで設定する場合：
［本体セキュリティー］タブ -［認証設定］を選択します。
Epson Device Adminで設定する場合：
設定テンプレートで［管理者設定］-［認証機能設定］-［認証設定］を選択します。

項目	説明
認証方式	認証方式を選択します。 • 本体認証 スキャナーの本体に登録されたユーザー設定を使って認証します。スキャナー本体にユーザーの登録が必要です。 • LDAPサーバー認証 連携しているLDAPサーバーのユーザー情報を使って認証します。LDAPサーバーの設定が必要です。 • 本体認証とLDAPサーバー認証 スキャナー本体または連携しているLDAPサーバーのユーザー情報を使って認証します。スキャナー本体のユーザー登録と、LDAPサーバーの設定が必要です。
認証手段	認証手段を選択します。 • 認証カードまたはユーザーIDとパスワード ユーザー認証に認証カードを使用します。ユーザーIDとパスワードによる認証も使用できます。 • ユーザーIDとパスワード ユーザー認証にユーザーIDとパスワードを使用します。 認証カードによる認証は使用できません。 • ユーザーID ユーザー認証にユーザーIDのみを使用します。パスワードの設定は必要ありません。 • 認証カードまたはID番号 ユーザー認証に認証カードを使用します。ID番号も使用できます。 • ID番号 ユーザー認証にID番号のみを使用します。
ユーザーによるカード登録を許可する	許可すると、認証カードの登録をユーザーが行えます。 ［認証方式］で［LDAPサーバー認証］を選択していると設定できません。 ユーザーが認証カードを登録する方法について、詳しくは『ユーザーズガイド』の「認証カードを登録する」を参照してください。

項目	説明
ID番号の最小桁数	ID番号の最小桁数を選択します。
LDAPサーバー認証ユーザーのキャッシュ	LDAPサーバー認証を利用している場合、ユーザー情報のキャッシュを使用するかしないか設定できます。
ユーザー情報をSMTP認証で使用する	認証手段にユーザーIDとパスワードを利用している場合、ユーザー情報をSMTP認証に利用するかしないか設定できます。最後にログオンしたユーザーIDとパスワードがSMTP認証に使用されます。
LDAP認証ユーザーの機能制限	LDAPサーバー認証を利用している場合、ユーザーに利用を許可する機能を設定できます。

ユーザー設定の登録

ユーザー認証に使用するユーザー設定を登録します。登録には以下の方法があります。

- ユーザー設定を1件ずつ登録する（Web Config）
- CSVファイルを使って、複数件のユーザー設定を一度に登録する（Web Config）
- 設定テンプレートを使って、複数のスキャナーにユーザー設定を一括で登録する（Epson Device Admin）

関連情報

➡ 「ユーザー設定を個別に登録する（Web Config）」138ページ
➡ 「CSVファイルを使って複数件のユーザー設定を登録する（Web Config）」139ページ
➡ 「複数のスキャナーにユーザー設定を一括で登録する（Epson Device Admin）」142ページ

ユーザー設定を個別に登録する（Web Config）

Web Configで、［本体セキュリティー］タブ -［ユーザー設定］-［登録］を選択して、ユーザー設定を入力します。

項目	説明
ユーザーID	認証に使用するユーザーIDを、Unicode（UTF-8）で表せる1～83バイトで設定します。 大文字、小文字を区別しないので、どちらでもログオンできます。
ユーザー表示名	スキャナーのパネルに表示されるユーザーの表示名を、Unicode（UTF-16）で表せる32文字以内で設定します。空欄にもできます。
パスワード	認証に使用するパスワードを、ASCII文字を使用して0～32文字で入力します。大文字、小文字を区別します。 ［認証手段］を［ユーザーID］にした場合は空欄にします。
認証カードID	認証カードのIDを、ASCII文字を使用して116文字以内で入力します。空欄にもできます。 ［認証設定］で［ユーザーによるカード登録を許可する］を許可すると、ユーザーが登録した結果が反映されます。

項目	説明
ID番号	［認証設定］ - ［認証手段］で、［認証カードまたはID番号］または［ID番号］が選択されている場合に表示されます。 ［認証設定］ - ［ID番号の最小桁数］で設定した桁数以上8桁以下の数字を入力します。
自動生成	［認証設定］ - ［認証手段］で、［認証カードまたはID番号］または［ID番号］が選択されている場合に表示されます。 クリックすると［ID番号の最小桁数］で選択した桁数のID番号が自動生成されます。
部門	ユーザーを識別する部門名などを、Unicode（UTF-16）で表せる40文字以内で入力します。 空欄にもできます。
メールアドレス	ユーザーのメールアドレスを、ASCII文字を使用して200文字以内で設定します。［スキャン to マイメール 機能］の宛先に使用します。 空欄にもできます。
スキャン to マイフォルダー機能	［スキャン to マイフォルダー機能］ - ［設定方法］で［個別に設定する］を選択したとき、保存先を個別に設定します。設定項目については、以下をご覧ください。 「スキャン to マイフォルダー機能の設定」148ページ
機能制限	ユーザーごとに機能制限を設定できます。許可する機能にチェックを付けます。
お気に入り	スキャナーに登録されているお気に入りから、選択したユーザーだけが使用できる項目を5件まで設定できます。 • ユーザーに割り当てられたお気に入りは、そのユーザーだけが使用できます。どのユーザーにも割り当てられていないお気に入りは、全てのユーザーが使用できます。 • ユーザーが使用できるお気に入りが1件のみのときは、認証後にその設定が自動的に呼び出されます。複数のお気に入りが使用できるときは、認証後にお気に入りの一覧が表示されます。 • ［機能制限］で制限した機能を使ったお気に入りは、作成および表示できません。

CSVファイルを使って複数件のユーザー設定を登録する（Web Config）

各ユーザーの設定をCSVファイルに記述して、一度に登録します。

CSVファイルを作成する

ユーザー設定を取り込むためのCSVファイルを作成します。

参考 あらかじめ1件以上のユーザー設定を登録しておいてからフォーマットファイル（CSVファイル）をエクスポートすると、CSVファイルの設定項目入力の参考になります。

1. Web Configで、［本体セキュリティー］タブ - ［ユーザー設定］を選択します。
2. ［エクスポート］をクリックします。

3. ［ファイルのフォーマット］でエクスポートするファイル形式を選択します。

以下を参照して選択してください。

項目	説明
CSV UTF-16 (タブ区切り)	Microsoft Excelでファイルを編集する場合に選択してください。 各列の値は"[ ]"で囲まれて出力されます。"[ ]"の間に値を入力してください。 ファイルを更新するときは上書きを推奨します。名前を付けて保存する場合は、ファイルの種類は"Unicode テキスト(*.txt)"を選択してください。
CSV UTF-8 (カンマ区切り)	テキストエディターでの編集やマクロでの自動編集など、Microsoft Excelを使わずに編集する場合に選択してください。
CSV UTF-8 (セミコロン区切り)	

4. ［エクスポート］をクリックします。

5. 保存されたCSVファイルを表計算ソフト（Microsoft Excelなど）やテキストエディターなどで編集し、保存します。

> **重要** ファイル編集するとき、エンコードやヘッダーの情報を変更しないでください。

CSVファイルの設定項目

項目	設定値と説明
UserID	認証に使用するユーザーIDを、Unicodeで表せる1～83バイトで設定します。
UserName	スキャナーのパネルに表示されるユーザーの表示名を、Unicodeで表せる32文字以内で設定します。空欄にもできます。
Password	認証に使用するパスワードを、ASCII文字を使用して32文字以内で入力します。インポートするとき［EncPassword］より優先してパスワードとしてセットされます。 ［認証手段］を［ユーザーID］にした場合は空欄にします。 エクスポートするときは常に空欄になります。
AuthenticationCardID	認証カードの読み取り結果を設定します。［認証設定］で［ユーザーによるカード登録を許可する］を許可すると、ユーザーが登録した結果が反映されます。 ASCII文字を使用して116文字で入力します。空欄にもできます。
IDNumber	［認証設定］ - ［認証手段］で、［認証カードまたはID番号］または［ID番号］が選択されている場合に表示されます。 ［認証設定］ - ［ID番号の最小桁数］で設定した桁数以上8桁以下の数字を入力します。 ID番号の重複はできません。重複している場合、ファイルをインポートした際にエラー通知されます。空欄の場合は自動採番されます。
Department	ユーザーを識別する部門名などを任意で入力します。 Unicodeで表せる40文字以内で入力します。空欄にもできます。
MailAddress	ユーザーのメールアドレスを設定します。［スキャン to マイメール 機能］の宛先に使用します。 A-Z、a-z、0-9、!#’%&’*+-./=?^_{|}~@が使用できます。200文字以内で入力します。 先頭文字に"."（ カンマ）は使用できません。空欄にもできます。

項目	設定値と説明
FolderProtocol	スキャン to マイフォルダー機能の種別を設定します。 ネットワークフォルダー（SMB）：0、FTP：1
FolderPath	スキャン to マイフォルダー機能の保存先を設定します。
FolderUserName	スキャン to マイフォルダー機能のユーザー名を設定します。
FolderPassword	スキャン to マイフォルダー機能の保存先フォルダーの認証に使用するパスワードを、ASCII文字を使用して32文字以内で入力します。 インポートするとき［EncPassword］より優先してパスワードとしてセットされます。エクスポートするときは常に空欄になります。
FtpPassive	スキャン to マイフォルダー機能の［種別］で［FTP］を選択した場合、FTPサーバーへの接続モードを設定します。 アクティブモード：0、パッシブモード：1
FtpPort	スキャン to マイフォルダー機能の［種別］で［FTP］を選択した場合、送信するポート番号を0～65535で入力します。
ScanToMemory	スキャン to USBドライブ 機能の機能制限を設定します。 許可しない：0、許可：1
ScanToMail	スキャン to メール 機能の機能制限を設定します。 ［スキャン to メール 機能］を有効にしているときのみ、［スキャン to マイメール 機能］を設定できます。 許可しない：0、許可：1
ScanToFolder	スキャン to ネットワークフォルダー 機能の機能制限を設定します。 ［スキャン to ネットワークフォルダー 機能］を有効にしているときのみ、［スキャン to マイフォルダー 機能］を設定できます。 許可しない：0、許可：1
ScanToCloud	スキャン to クラウド 機能の機能制限を設定します。 許可しない：0、許可：1
ScanToComputer	スキャン to コンピューターの機能制限を設定します。 許可しない：0、許可：1
PresetIndex	ユーザーに関連付けるお気に入りを設定します。お気に入りの登録番号をカンマ区切りで5件まで設定できます。
EncPassword	ユーザー設定をエクスポートするとき［Password］に設定してある値が暗号化され、BASE64でエンコードされた値が出力されます。 インポートするときに［Password］に新たなパスワードを入力すると、この値が無視されます。 ［Password］に何も入力しないと、この値が使われてエクスポート前のパスワードのままになります。
EncFolderPassword	エクスポートするとき［FolderPassword］に設定してある値が暗号化され、BASE64でエンコードされた値が出力されます。 インポートするときに［FolderPassword］に新たなパスワードを入力すると、この値が無視されます。 ［FolderPassword］に何も入力しないと、この値が使われてエクスポート前のパスワードのままになります。

CSVファイルをインポートする

1. Web Configで、［本体セキュリティー］タブ - ［ユーザー設定］を選択します。
2. ［インポート］をクリックします。
3. インポートするファイルを選択します。
4. ［インポート］をクリックします。
5. 表示された情報を確認し、［OK］をクリックします。

複数のスキャナーにユーザー設定を一括で登録する（Epson Device Admin）

LDAPサーバーやCSV/ENEファイルを利用して、本体認証で使用されるユーザー設定を一括で登録できます。

参考 ENEファイルはエプソン独自の暗号化ファイル形式で、個人情報を含む［アドレス帳］の情報やユーザー設定などを保存するバイナリファイルです。Epson Device Adminからエクスポートでき、パスワードを設定できます。バックアップしたユーザー設定をインポートするような場合に使用できます。

CSVファイル/ENEファイルからインポートする

1. 設定テンプレートで［管理者設定］-［認証機能設定］-［ユーザー設定］を選択します。
2. ［インポート］をクリックします。
3. ［インポート元］で［CSV/ENEファイル］を選択します。
4. ［参照］をクリックします。
   ファイル選択画面が表示されます。
5. インポートするファイルを選択して開きます。
6. インポート方法を選択します。
   - 上書き、追加する：同じユーザーIDがある場合は上書きし、ない場合は追加します。
   - 全て置き換える：インポートするユーザー設定に全て置き替えます。
7. ［インポート］をクリックします。
   確認画面が表示されます。
8. ［OK］をクリックします。
   読み込み内容の検証が始まり、結果を表示します。

参考
- 読み込んだユーザー設定がインポートできる件数を超えた場合、ユーザー設定を削除するよう案内が表示されます。インポートする前に超過しているユーザー設定を削除してください。
- ユーザー設定を選択して［削除］をクリックすると、インポート前にユーザー設定を削除できます。

9. ［インポート］をクリックします。
ユーザー設定が設定テンプレートにインポートされます。

LDAPサーバーからインポートする

1. 設定テンプレートで［管理者設定］-［認証機能設定］-［ユーザー設定］を選択します。
2. ［インポート］をクリックします。
3. ［インポート元］で［LDAP］を選択します。
4. ［設定］をクリックします。
［LDAP］設定が表示されます。

参考 このLDAPサーバー設定は、LDAPサーバーのユーザー設定をインポートするための設定です。ここで取得したユーザー設定はスキャナーにインポート（コピー）して本体認証で使用するユーザーとして登録されます。
一方、［LDAP］や［本体認証とLDAPサーバー認証］で使用するLDAPサーバー設定は、LDAPサーバーと通信しながら認証するために設定します。

5. 各項目を設定します。
LDAPサーバーからユーザー設定をインポートする場合、LDAP設定の項目に加えて以下が設定できます。
その他の項目は関連情報をご覧ください。

項目			説明
LDAPサーバー情報	LDAPサーバーの種類		LDAPサーバーの種類を選択できます。
検索設定	検索フィルター		LDAP検索フィルターの文字列を設定できます。［手動設定］を選択すると検索文字列を編集できます。
	オプション	種別	［スキャン to マイフォルダー機能］の保存先の種別を設定できます。
		接続モード	［種別］が［FTP］のとき、FTPの接続モードを設定できます。
		ポート番号	［種別］が［FTP］のとき、使用するポート番号を設定できます。

6. 必要に応じて［接続テスト］をクリックし、接続テストを行います。
LDAPサーバーから10件分のユーザー設定を取得して表示します。
7. ［OK］をクリックします。
8. インポート方法を選択します。
- 上書き、追加する：同じユーザーIDがある場合は上書きし、ない場合は追加します。
- 全て置き換える：インポートするユーザー設定に全て置き替えます。

9. ［インポート］をクリックします。
   確認画面が表示されます。

10. ［OK］をクリックします。
    読み込み内容の検証が始まり、結果を表示します。

11. ［インポート］をクリックします。
    ユーザー設定が設定テンプレートにインポートされます。

関連情報

➡ 「LDAPサーバーを設定する」144ページ
➡ 「LDAPサーバーの検索属性を設定する」146ページ

LDAPサーバーとの連携

スキャナー本体のLDAPサーバーの設定を行います。
必要に応じて、プライマリーサーバーとセカンダリーサーバーの両方を設定します。

参考 ［LDAPサーバー］の設定は、［アドレス帳］と共用しています。

利用できるサービス

対応しているディレクトリーサービスは以下の通りです。

サービス名	バージョン
Active Directory	Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019
OpenLDAP	Ver.2.3, Ver.2.4

LDAPサーバーを設定する

LDAPサーバーの情報を登録して、LDAPサーバーを利用できるようにします。
Web Configで設定する場合：
［ネットワーク］タブ -［LDAPサーバー］-［基本 (プライマリーサーバー)］または［基本 (セカンダリーサーバー)］を選択します。
［認証方式］で［Kerberos認証］を選択する場合は、あらかじめ［ネットワーク］タブ -［Kerberos設定］を選択し、Kerberos設定をしてください。
Epson Device Adminで設定する場合：
設定テンプレートで［ネットワーク］-［LDAPサーバー］-［サーバー設定 (プライマリーサーバー)］または［サーバー設定 (セカンダリーサーバー)］を選択します。
［認証方式］で［Kerberos認証］を選択する場合は、あらかじめ［ネットワーク］-［セキュリティー］-［Kerberos設定］を選択し、Kerberos設定をしてください。

項目	設定値と説明
LDAPサーバーを使用する	［使用する］、または［使用しない］を選択します。
LDAPサーバーアドレス	LDAPサーバーのアドレスを入力します。IPv4、IPv6、FQDNのいずれかの形式で、1～255文字以内で指定します。FQDN形式では、ASCII（0x20-0x7E）の英数字とハイフン（アドレスの先頭と末尾以外）が使用できます。
LDAPサーバーポート番号（ポート番号）	LDAPサーバーのポート番号を、1～65535以内の半角数字で入力します。
セキュア接続	スキャナーがLDAPサーバーにアクセスする際の認証方式を指定します。 ［なし］を選択すると、通信が暗号化されません。［なし］以外を選択することをお勧めします。
証明書の検証	有効にするとLDAPサーバーの証明書の正当性をチェックします。［有効］にすることをお勧めします。 設定するには、スキャナーに［相手サーバー検証用CA証明書］のインポートが必要です。
検索タイムアウト（秒）	検索を開始してからタイムアウトするまでの時間（秒）を5～300までの半角数字で入力します。
認証方式	認証方式を選択します。 ［Simple認証］を選択するときは、［セキュア接続］で［なし］以外を選択することをお勧めします。 ［Kerberos認証］を選択する場合は、あらかじめKerberos設定をしておいてください。 Kerberos認証を行うには以下の環境が必要です。 • スキャナーとDNSサーバーが通信できること • スキャナーとKDCサーバー、認証が必要なサービスを提供するサーバー（LDAPサーバー、SMTPサーバー、ファイルサーバー）の時刻の同期が取れていること • サービスサーバーをIPアドレスで指定している場合、DNSサーバーの逆引き参照ゾーンにサービスサーバーのFQDNが登録されていること
使用するKerberosレルム	［認証方式］で［Kerberos認証］を選択した場合に、使用するKerberosレルムを選択します。
管理者DN / ユーザー名	Unicode（UTF-8）で、LDAPサーバーのユーザー名を128文字以内で入力します。制御文字（0x00～0x1F、0X7F）は使用できません。この項目は［認証方式］を［Anonymous認証］にすると無効になります。指定しない場合は空白にします。
パスワード	Unicode（UTF-8）で表せる128文字以内で、LDAPサーバー認証のパスワードを入力します。制御文字（0x00～0x1F、0X7F）は使用できません。この項目は［認証方式］を［Anonymous認証］にすると無効になります。指定しない場合は空白にします。

Kerberos設定

［認証方式］で［Kerberos認証］を選択する場合は、Kerberos設定をしてください。Kerberos設定は10個まで登録できます。

Web Configで設定する場合：

［ネットワーク］タブ -［Kerberos設定］を選択します。

Epson Device Adminで設定する場合：

設定テンプレートで［ネットワーク］-［セキュリティー］-［Kerberos設定］を選択します。

項目	設定値と説明
レルム(ドメイン)	Kerberos認証のレルムを、ASCII（0x20-0x7E）で表せる255文字以内で指定します。登録しない場合は空白にします。
KDCアドレス	Kerberos認証サーバーのアドレスを入力します。IPv4、IPv6、FQDNのいずれかの形式で、255文字以内で指定します。登録しない場合は空白にします。
ポート番号(Kerberos)	Kerberosサーバーのポート番号を、1～65535以内の半角数字で入力します。

LDAPサーバーの検索属性を設定する

ユーザー設定の検索属性を設定します。

Web Configで設定する場合：

［ネットワーク］タブ -［LDAPサーバー］-［検索設定 (認証機能) ］を選択します。

Epson Device Adminで設定する場合：

設定テンプレートで［管理者設定］-［認証機能設定］-［LDAPサーバー］-［検索設定 (認証機能)］を選択します。

項目	設定値と説明
検索開始位置(DN)	LDAPサーバーからユーザー情報を検索するときの検索開始位置を指定します。 Unicode（UTF-8）で表せる0～128文字以内で入力します。検索位置を指定しないときは空白にします。 設定例：localのserverディレクトリー：dc=server,dc=local
ユーザーID属性	ユーザーIDとして検索するLDAPサーバーの属性名を指定します。入力できる文字は、ASCII文字で255文字以内です。先頭はアルファベットのA～Z、a～zにしてください。 設定例：cn、uid
ユーザー表示名属性	表示名として表示する属性名を指定します。入力できる文字は、ASCII文字で255文字以内です。先頭はアルファベットのA～Z、a～zにしてください。空白にもできます。 設定例：cn、name
認証カードID属性	認証カードIDして表示する属性名を指定します。入力できる文字は、ASCII文字で255文字以内です。先頭はアルファベットのA～Z、a～zにしてください。空白にもできます。 設定例：cn、sn
ID番号属性	ユーザーIDとして検索するLDAPサーバーの属性名を指定します。入力できる文字は、ASCII文字で255文字以内です。先頭はアルファベットのA～Z、a～zにしてください。 設定例：cn、id
部門属性	部門名として表示する属性名を指定します。入力できる文字は、ASCII文字で255文字以内です。先頭はアルファベットのA～Z、a～zにしてください。空白にもできます。 設定例：ou、ou-cl
メールアドレス属性	メールアドレスを検索結果として表示する属性名を指定します。入力できる文字は、ASCII文字で255文字以内です。先頭はアルファベットのA～Z、a～zにしてください。 設定例：mail

項目	設定値と説明
保存先属性	スキャン to マイフォルダー機能の保存先を参照する属性名を指定します。入力できる文字は、ASCII文字で255文字以内です。 設定例：homeDirectory

LDAPサーバーとの接続を確認する

［LDAPサーバー］-［検索設定］で設定した値でLDAPサーバーとの接続テストを行います。

1. Web Configで［ネットワーク］タブ -［LDAPサーバー］-［接続確認］を選択します。
2. ［確認開始］を選択します。

   LDAPサーバーとの接続テストが開始されます。テストが終了すると結果が表示されます。

LDAPサーバー接続確認結果

メッセージ	説明
接続に成功しました。	サーバーとの接続に成功した場合に表示されます。
接続に失敗しました。 設定を確認してください。	以下の理由によってサーバーへの接続に失敗した場合に表示されます。 • LDAPサーバーアドレス、ポート番号などが間違っている • 通信タイムアウトが発生した • ［LDAPサーバーを使用する］が［使用しない］に設定されている • ［認証方式］を［Kerberos認証］に設定した場合に、［レルム(ドメイン)］、［KDCアドレス］、または［ポート番号(Kerberos)］の設定が間違っている
接続に失敗しました。 製品、またはサーバーの日付/時刻設定を確認してください。	スキャナーとLDAPサーバーの時刻設定の不一致によって接続に失敗した場合に表示されます。
サーバーの認証に失敗しました。 設定を確認してください。	以下の理由によってサーバーへの接続に失敗した場合に表示されます。 • ［ユーザー名］または［パスワード］が間違っている • ［認証方式］を［Kerberos認証］に設定した場合に、時刻設定がされていない
製品は処理動作中のためアクセスできません。	スキャナーが動作中で接続設定ができなかったときに表示されます。

メールサーバーの設定

［スキャン to マイメール 機能］を使用する場合、メールサーバーを設定します。

参考 ［スキャン to メール 機能］を有効にしているときのみ、［スキャン to マイメール 機能］を設定できます。

Web Configで設定する場合：

［ネットワーク］タブ -［メールサーバー］-［基本］を選択します。

Epson Device Adminで設定する場合：
設定テンプレートで［共通］-［メールサーバー］-［メールサーバー設定］を選択します。

項目	設定値と説明	
認証方式	スキャナーがメールサーバーにアクセスする際の認証方式を指定します。	
	認証しない （なし）	メールサーバーとの通信時に認証をしません。
	SMTP認証	メールサーバーがSMTP認証に対応している必要があります。
	POP before SMTP	選択した場合はPOP3サーバーの設定をしてください。
認証用アカウント	［認証方式］で［SMTP認証］または［POP before SMTP］を選択した場合、認証用のアカウント名を入力します。入力できる文字は、ASCII（0x20-0x7E）の255文字以内です。	
認証用パスワード	［認証方式］で［SMTP認証］または［POP before SMTP］を選択した場合、認証用のパスワードを入力します。入力できる文字は、ASCII（0x20-0x7E）の20文字以内です。	
送信元アドレス	送信元を示すメールアドレスを入力します。入力できる文字は、: ( ) < > [ ] ; ¥ を除くASCII (0x20-0x7E)で表せる255文字以内です。ただし、ピリオド（.）は先頭文字にできません。	
SMTPサーバーアドレス	A～Z a～z 0～9 . - を使用し、255文字以内で入力します。IPv4形式とFQDN形式での入力が可能です。	
SMTPサーバー ポート番号	1～65535までの範囲で、半角数字で入力します。	
セキュア接続	メールサーバーのセキュア接続方式を指定します。	
	なし	［認証方式］で［POP before SMTP］を選択した場合は［なし］になります。
	SSL/TLS	［認証方式］で［認証しない］または［SMTP認証］を選択したときに選択できます。
	STARTTLS	［認証方式］で［認証しない］または［SMTP認証］を選択したときに選択できます。
証明書の検証	有効にするとメールサーバーの証明書の正当性をチェックします。［有効］にすることをお勧めします。	
POP3サーバーアドレス	［認証方式］で［POP before SMTP］を選択した場合、POP3サーバーアドレスを入力します。入力できる文字は、A～Z a～z 0～9 . - で、255文字以内です。IPv4形式とFQDN形式での入力が可能です。	
POP3サーバー ポート番号	［認証方式］で［POP before SMTP］を選択した場合、ポート番号を指定します。入力できる文字は、1～65535の範囲で、半角数字で入力します。	

スキャン to マイフォルダー機能の設定

ユーザーごとに割り当てられたフォルダーにスキャンした画像を保存します。保存するフォルダーは、以下の設定ができます。

参考 ［スキャン to ネットワークフォルダー 機能］を有効にしているときのみ、［スキャン to マイフォルダー機能］を設定できます。

保存先設定	認証方式	フォルダーパス設定場所
認証設定全体で一つのネットワークフォルダーを指定して、その中にユーザーID名の個人フォルダーを自動的に作成する	• 本体認証 • LDAPサーバー認証 • 本体認証とLDAPサーバー認証	本体（スキャン to マイフォルダー機能設定）
ユーザーごとに別々のネットワークフォルダーを指定する	本体認証	本体（ユーザー設定）
	LDAPサーバー認証	LDAP属性
	本体認証とLDAPサーバー認証	本体（ユーザー設定） またはLDAP属性

Web Configで設定する場合：
［本体セキュリティー］タブ -［スキャン to ネットワークフォルダー 機能］を選択します。
Epson Device Adminで設定する場合：
設定テンプレートで［管理者設定］-［認証機能設定］-［スキャン to ネットワークフォルダー 機能］-［スキャン to マイフォルダー機能］を選択します。

項目		説明
保存先設定	設定方法	• ［一括で設定する］： ［保存先］に指定したフォルダーパスやURLの直下にユーザーID名のフォルダーが自動作成されて、スキャン結果が保存されます。 • ［個別に設定する］： ユーザーごとにスキャン結果の保存先を設定できます。 本体認証ユーザーはユーザー設定で個別に設定できます。 LDAPサーバー認証ユーザーはLDAPサーバーの検索設定で取得した保存先を使用します。
	種別	保存先に合わせて送信プロトコルを選択します。 ネットワークフォルダーの場合：［ネットワークフォルダー (SMB)］ FTPサーバーの場合：［FTP］
	保存先	保存先のパスまたはURLを設定します。 Unicode（UTF-16）で表せる160文字以内で入力します。
	接続モード	［種別］で［FTP］を選択した場合に設定します。 FTPサーバーへの接続モードを選択します。
	ポート番号	［種別］で［FTP］を選択した場合に設定します。 FTPサーバーにスキャンデータを送信するポートの番号を0～65535の間で入力します。

項目		説明
認証設定	設定方法	［保存先設定］の［設定方法］で［個別に設定する］を選択した場合に設定します。 フォルダーにアクセスするための「ユーザー名」と「パスワード」を設定します。 • ［一括で設定する］： 全てのユーザーで共通の［ユーザー名］と［パスワード］を使用します。 • ［個別に設定する］： 本体認証ユーザーは［ユーザー設定］で［ユーザー名］と［パスワード］を個別に設定します。LDAPサーバー認証ユーザーは個別の設定ができません。本項目で設定する［ユーザー名］と［パスワード］を一括で使用します。
	ユーザー名	保存先のフォルダーにアクセスするユーザー名を入力します。 Unicode（UTF-16）で表せる30文字以内で入力します。［一括で設定する］またはLDAPサーバーを使用する場合に設定します。
	パスワード	［ユーザー名］に対応したパスワードを入力します。 Unicode（UTF-16）で表せる20文字以内で入力します。［一括で設定する］またはLDAPサーバーを使用する場合に設定します。

スキャン to ネットワークフォルダー 機能の宛先編集を禁止する

項目	説明
宛先の直接入力を禁止する	チェックを付けると、ユーザーがデフォルトの宛先を変更できないようにします。

ホーム画面編集

操作パネルのホーム画面に表示するアイコンのレイアウトを編集し、必要なアイコンだけを表示できます。

Web Configで設定する場合：

［本体セキュリティー］タブ -［ホーム画面編集］を選択します。

Epson Device Adminで設定する場合：

設定テンプレートで［管理者設定］-［認証機能設定］-［ホーム画面編集］を選択します。

参考 以下の場合は、特定の機能のアイコンがホーム画面に表示されません。

- ［機能制限］で使用できない機能を選択した場合
- ログオンしたユーザーのメールアドレスが登録されていない場合（スキャン to マイメール 機能）
- 保存先のフォルダーが設定されていない場合（スキャン to マイフォルダー機能）

項目	説明
1ページあたりの最大表示数	操作パネルに表示するアイコンのレイアウトを選択します。選択したレイアウトに従ったイメージが表の上に表示されます。
ページ数	ページの数を選択します。
番号	各番号の位置に表示する機能を選択します。

Epson Device Adminを使ったジョブ履歴のレポート

Epson Device Adminを使用して、ジョブ履歴のレポートをグループやユーザーごとに作成できます。使用履歴は最大3,000件までスキャナー本体に保存されます。レポートの作成には、レポートの期間を指定して作成する方法とスケジュールを設定して定期的に作成する方法があります。
ジョブ履歴をレポートに出力するには、デバイス一覧画面のリボンメニューで［オプション］ - ［Epson Print Admin Serverless/認証機能 設定］-［Epson Print Admin Serverless/認証機能 の対応デバイスを管理する］を選択します。
ユーザーレポートの作成方法について、詳しくはEpson Device Adminのマニュアルをご覧ください。

レポートに出力できる項目

ユーザーレポートには、以下の項目を出力できます。
日付/ジョブID/操作/ユーザーID/部門/処理結果/処理結果詳細/スキャン：宛先種別/スキャン：宛先/スキャン：用紙サイズ/スキャン：両面/スキャン：カラー/スキャン：面数/デバイス：機種/デバイス：IPアドレス/デバイス：製造番号/デバイス：部門/デバイス：設置先名/デバイス：備考/デバイス：備考2

操作パネルから管理者としてログオンする

以下の方法で、スキャナーの操作パネルから管理者としてログオンできます。

1. 画面右上の  をタップします。
   - 認証設定を有効にしているときは、［ようこそ］画面（認証の待ち受け画面）にアイコンが表示されます。
   - 認証設定を無効にしているときは、ホーム画面にアイコンが表示されます。
2. 確認画面が表示されたら、［はい］をタップします。
3. 管理者のパスワードを入力します。
   ログオン完了のメッセージが表示され、操作パネルのホーム画面が表示されます。

ログアウトするときは、ホーム画面右上の  をタップします。

認証設定を無効にする

Web Configで認証設定を無効にできます。

参考 本体に登録されているユーザー設定は、認証設定を無効にしても保存されています。スキャナーを購入時の設定に戻すと削除できます。

1. Web Configを起動します。
2. ［本体セキュリティー］タブ -［基本］ - ［認証機能］を選択します。

3. ［オフ］を選択します。

4. ［次へ］をクリックします。

5. ［設定］をクリックします。

参考 認証設定を無効にしても、管理者ロックは有効のままです。無効にしたいときは、操作パネルまたはWeb Configから設定します。

関連情報

➡ 「操作パネルで管理者ロックを設定する」91ページ
➡ 「Web Configで管理者ロックを設定する」91ページ

認証設定の情報を削除する（購入時の設定に戻す）

認証設定の情報（認証装置、認証方式、ユーザー設定など）を全て削除するときは、スキャナーの全ての設定を購入時の設定に戻します。
操作パネルで、［設定］-［管理者用設定］-［購入時の設定に戻す］-［全ての設定］を選択してください。

!重要 アドレス帳やその他のネットワーク設定も全て消去されます。消去した設定は復元できません。

困ったときは

認証カードが読みとれない

以下を確認してください。

- 認証装置がスキャナーに正しく接続されているか
  認証装置は、スキャナーの背面にある外部機器接続用USBポートに接続します。
- 対応している認証装置や認証カードかどうか

メンテナンス

スキャナーの外部をクリーニングする

スキャナーの外側のケースが汚れたときは、乾いた布や、中性洗剤や水に浸してよく絞った布で拭き取ります。

重要
- アルコールやシンナーなどの揮発性薬品は使用しないでください。変形や変色のおそれがあります。
- スキャナーの内部に水分が入らないように注意してください。正常に動作しなくなるおそれがあります。
- スキャナーを絶対に分解しないでください。

1. ⏻ボタンを押してスキャナーの電源を切ります。
2. スキャナーからACアダプターを取り外します。
3. 中性洗剤や水に浸してよく絞った布で、外側のケースの汚れを拭き取ります。

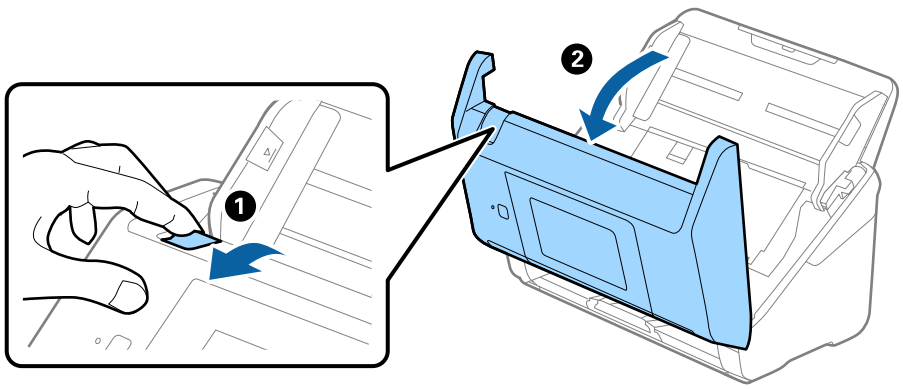
   参考 タッチパネルは乾いた柔らかい布でから拭きしてください。

スキャナーの内部をクリーニングする

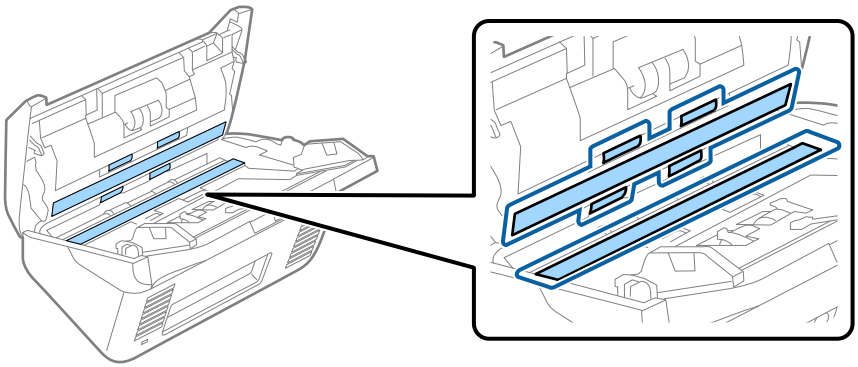
スキャンを繰り返していると、スキャナー内部のローラーやガラス部品などに紙粉やホコリが付着して、給紙不良やスキャン品質不良の原因となります。5,000枚のスキャンを目安に、スキャナー内部をクリーニングしてください。
現在のスキャン枚数は、操作パネルまたはEpson Scan 2ユーティリティーで確認できます。
汚れがひどいときは、専用のクリーニングキットを使用してください。クリーニングクロスに少量のクリーナーを含ませて汚れを拭き取ります。

重要
- アルコールやシンナーなどの揮発性薬品は使用しないでください。変形や変色のおそれがあります。
- スキャナーに液体をかけたり、潤滑剤などを直接スプレーしたりしないでください。装置や回路が損傷して、正常に動作しなくなるおそれがあります。
- スキャナーを絶対に分解しないでください。

1. ⏻ボタンを押してスキャナーの電源を切ります。
2. スキャナーからACアダプターを取り外します。
3. レバーを引いてスキャナーカバーを開けます。

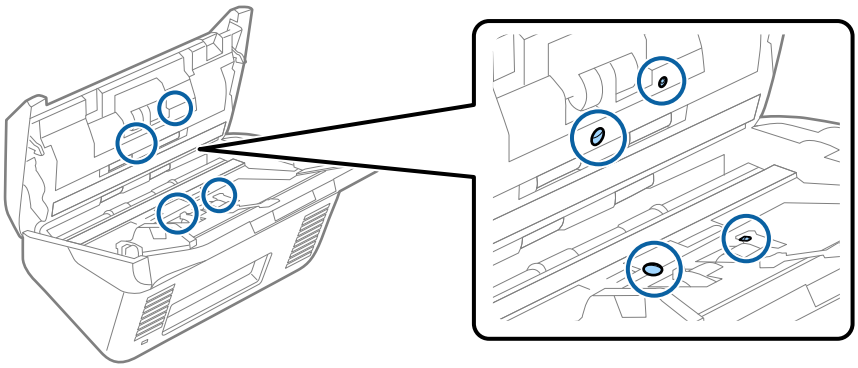


4. 柔らかい布または専用のクリーニングキットで、スキャナーカバー内側のプラスチックローラーおよび底部のガラス面の汚れを拭き取ります。



重要
- ガラス面に強い力をかけないでください。
- ブラシや硬いものを使用しないでください。ガラス面に傷が付くと、スキャン品質に影響します。
- ガラス面にクリーナーを直接スプレーしないでください。

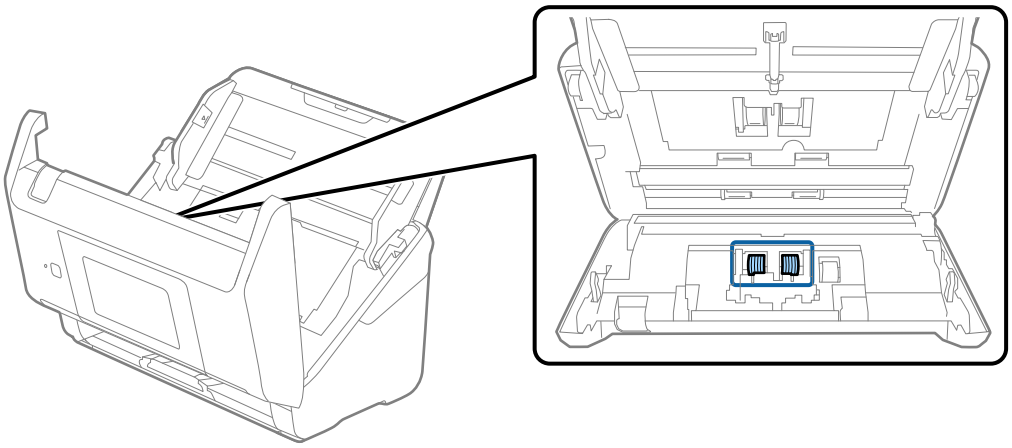
5. 綿棒で、センサーの汚れやホコリを拭き取ります。



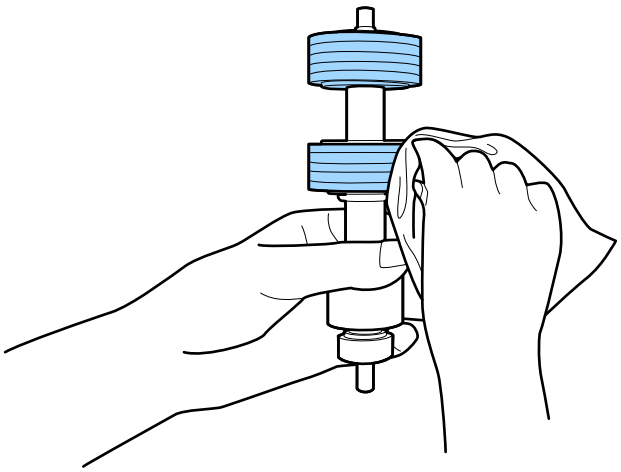
重要 綿棒にはクリーナーなどの液体を染み込ませないでください。

6. 分離ローラーのカバーを開けて、分離ローラーを取り外します。

   取り外し方は、給紙ローラーキットの交換手順のページをご覧ください。

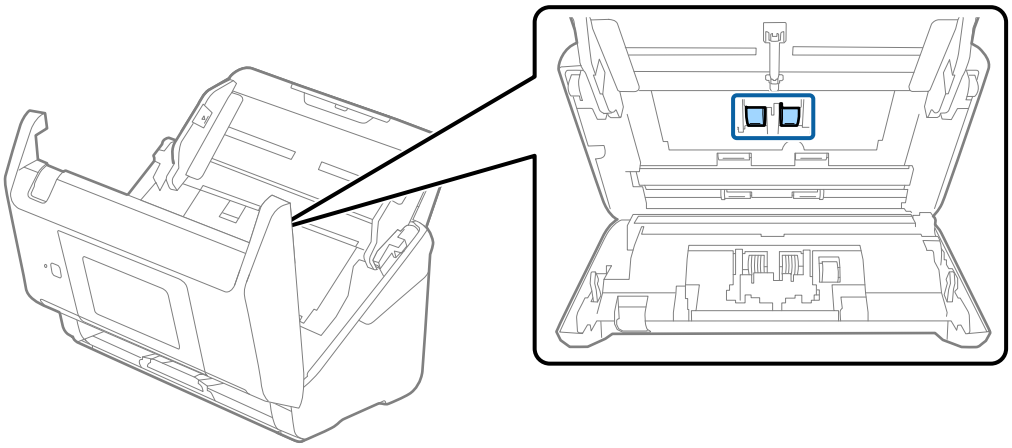


7. 専用のクリーニングキットまたは水を少し含ませた柔らかい布で、分離ローラーの汚れを拭き取ります。

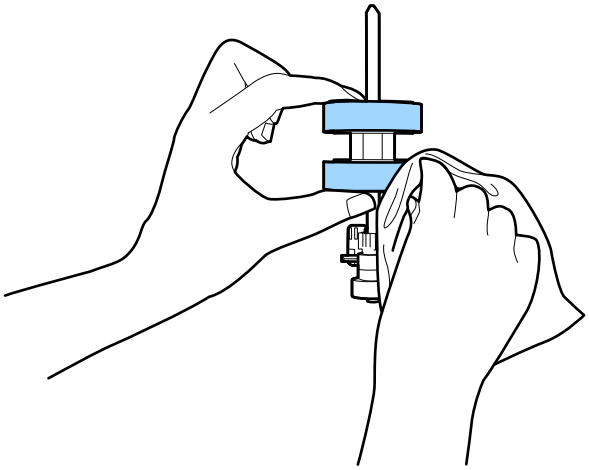


重要 乾いた布でローラーを拭かないでください。ローラーの表面を傷めることがあります。

8. 給紙ローラーのカバーを取り外して、給紙ローラーを取り外します。
   取り外し方は、給紙ローラーキットの交換手順のページをご覧ください。



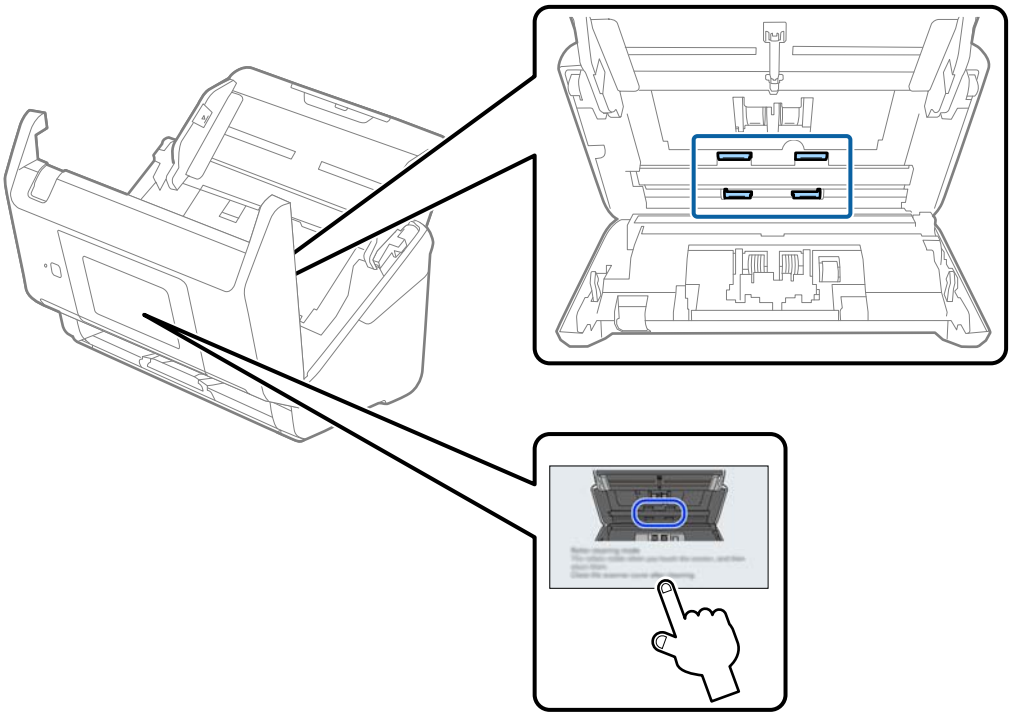
9. 専用のクリーニングキットまたは水を少し含ませた柔らかい布で、給紙ローラーの汚れを拭き取ります。



> **重要** 乾いた布でローラーを拭かないでください。ローラーの表面を傷めることがあります。

10. スキャナーカバーを閉めます。
11. ACアダプターを接続し、スキャナーの電源を入れます。
12. ホーム画面で［スキャナーのお手入れ］を選択します。
13. ［スキャナーのお手入れ］画面で［ローラークリーニング］を選択します。
14. レバーを引いてスキャナーカバーを開けます。
    ローラークリーニングモードに入ります。

15. 画面の任意の場所をタップして、底部のゴムローラーを少しずつ回転させます。専用のクリーニングキットまたは水を少し含ませた柔らかい布で、ローラーの表面を拭きます。ローラーがきれいになるまで、この作業を繰り返します。



> ⚠注意　ローラーの動作中は、手や髪の毛などが巻き込まれないように注意してください。けがをするおそれがあります。

16. スキャナーカバーを閉めます。

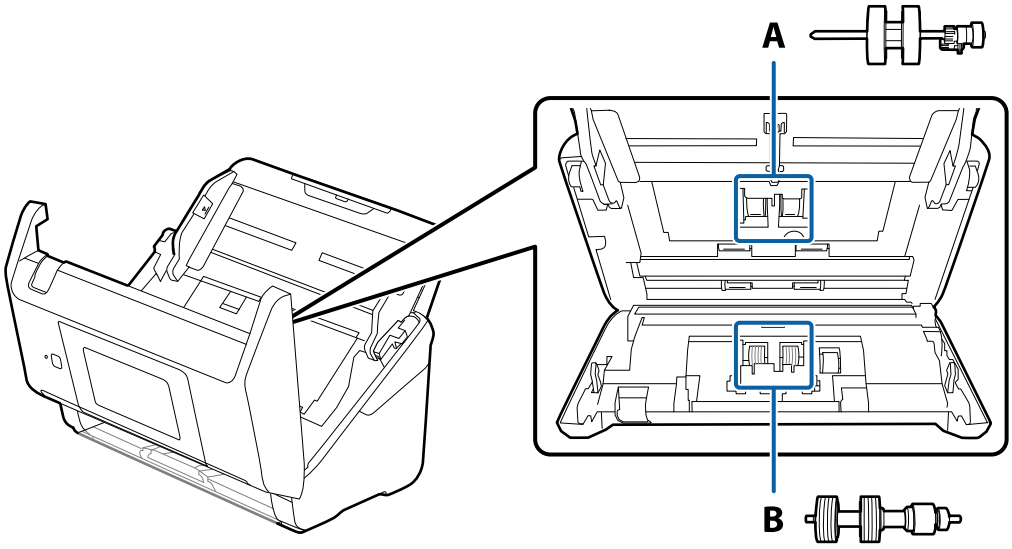
ローラークリーニングモードが終了します。

関連情報

➡ 「給紙ローラーキットを交換する」159ページ

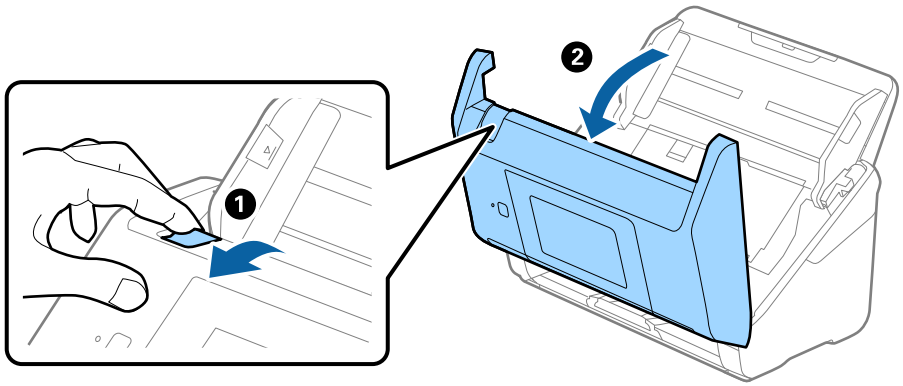
給紙ローラーキットを交換する

スキャン枚数が耐用枚数を超えると、給紙ローラーキット（給紙ローラーと分離ローラー）の交換が必要になります。操作パネルまたはコンピューターの画面に交換のメッセージが表示されたら、以下の手順で交換してください。

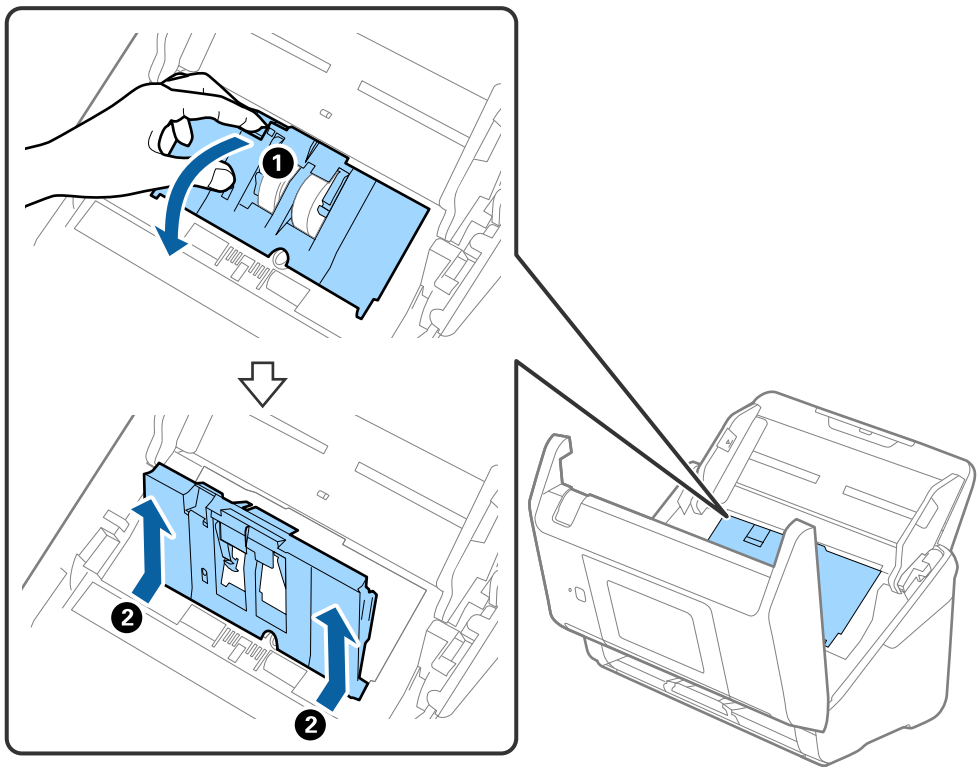


A：給紙ローラー、B：分離ローラー

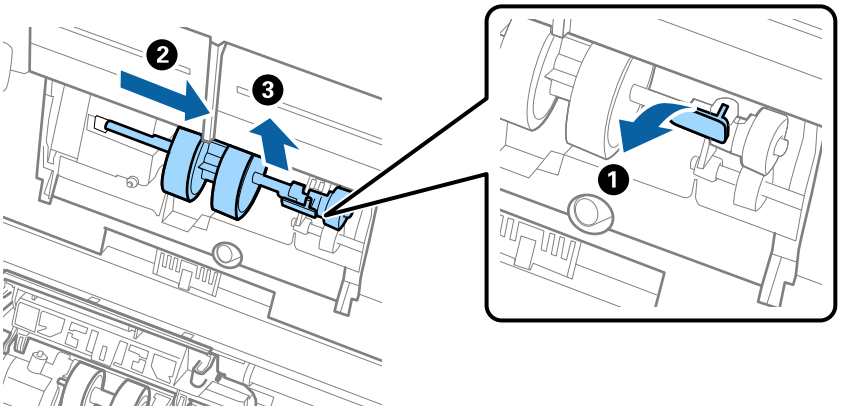
1. ⏻ボタンを押してスキャナーの電源を切ります。
2. スキャナーからACアダプターを取り外します。
3. レバーを引いてスキャナーカバーを開けます。



4. 給紙ローラーのカバーを開け、スライドして取り外します。

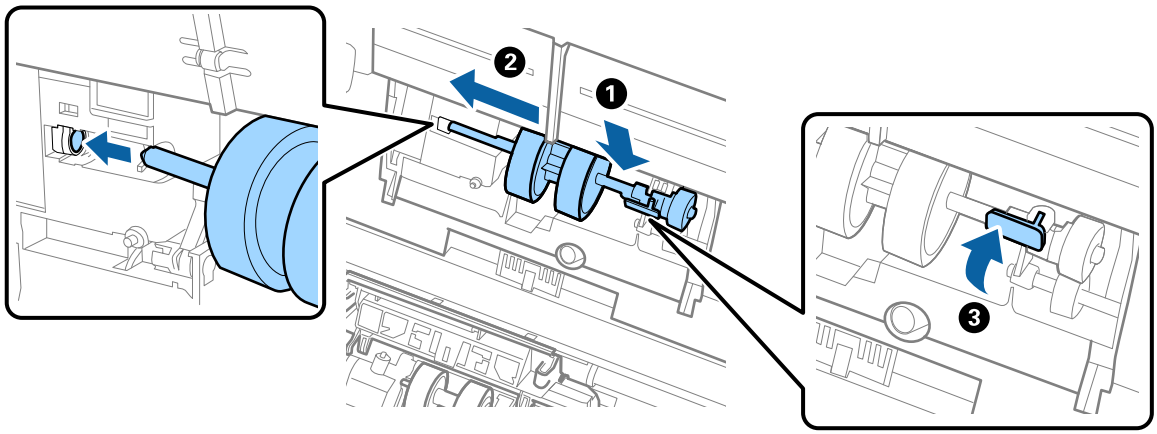


5. ローラー軸の固定具を手前に倒し、給紙ローラーをスライドして取り外します。

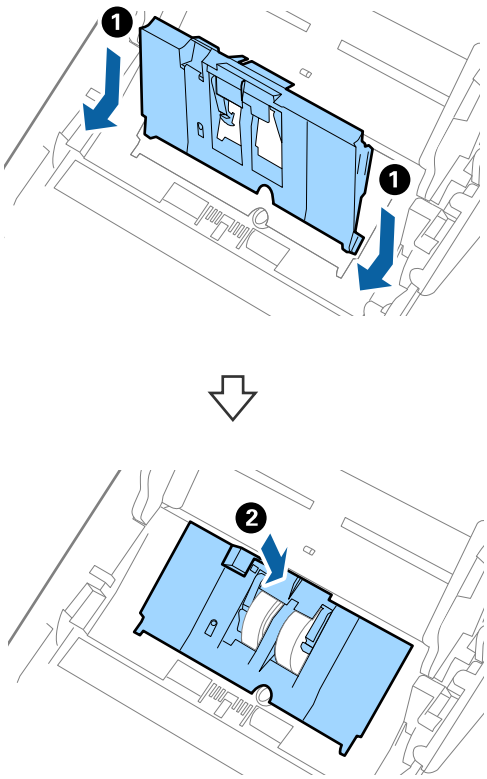


重要 給紙ローラーを無理に引き抜かないでください。スキャナー内部が破損するおそれがあります。

6. 新しい給紙ローラーを、固定具を手前に倒した状態で左側にスライドし、本体の穴に差し込みます。固定具を奥に戻して固定します。

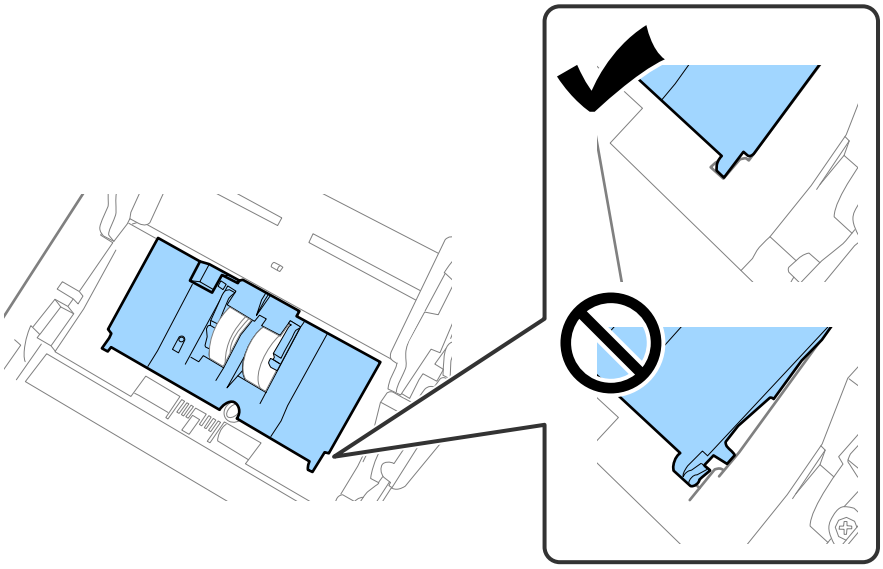


7. 給紙ローラーのカバーの先端を溝に入れてスライドします。カバーをしっかり閉めます。

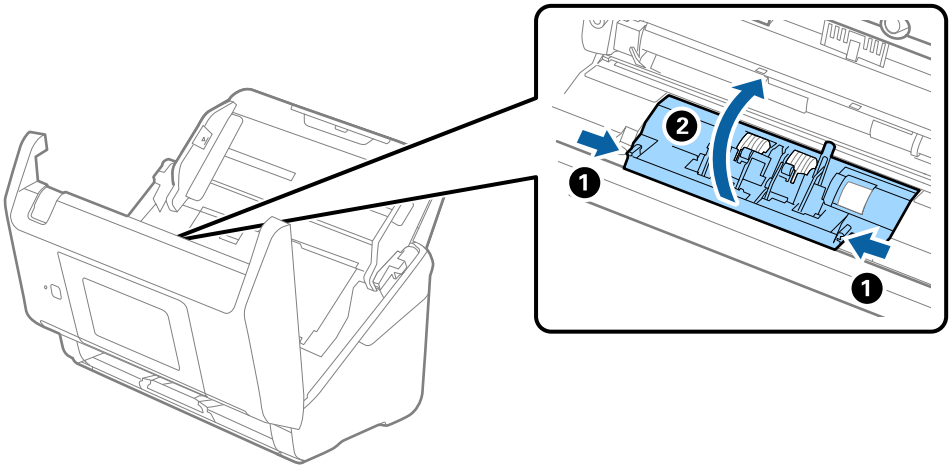


!重要

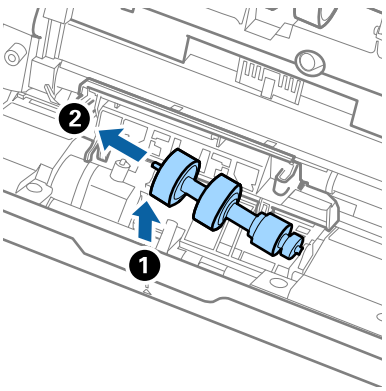
- カバーは必ず取り付けてください。
- カバーが閉まりにくい場合は、給紙ローラーが正しく装着されているか確認してください。
- カバーは浮いた状態で取り付けないでください。



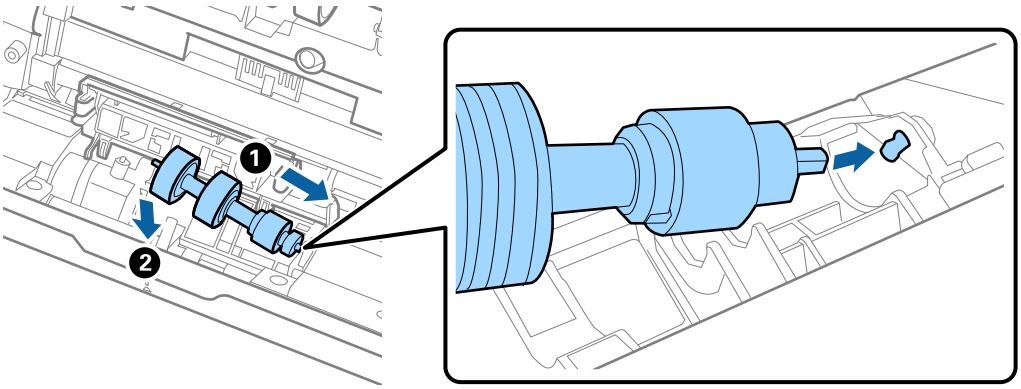
8. 分離ローラーのカバー両端のフックを押して、カバーを開けます。



9. 分離ローラーの左側を少し持ち上げ、スライドして取り外します。



10. 新しい分離ローラーの軸を右側の穴に差し込み、ローラーを落とし込みます。



11. 分離ローラーのカバーを閉めます。

> **重要** カバーが閉まりにくい場合は、分離ローラーが正しく装着されているか確認してください。

12. スキャナーカバーを閉めます。

13. ACアダプターを接続し、スキャナーの電源を入れます。

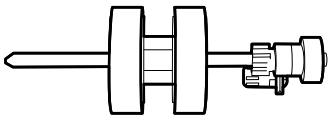
14. 操作パネルでスキャン枚数をリセットします。

参考 交換後の給紙ローラーと分離ローラーは、必ず法令や地域の条例、自治体の指示に従って廃棄してください。分解はしないでください。

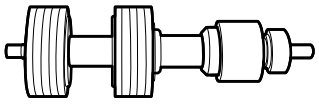
給紙ローラーキットの型番

スキャン枚数が耐用枚数を超えたときに交換する部品（給紙ローラーと分離ローラー）です。現在のスキャン枚数は、操作パネルまたはEpson Scan 2ユーティリティーで確認できます。

A



B



A：給紙ローラー、B：分離ローラー

品名	型番	耐用枚数
給紙ローラーキット	DSA4RKIT4	200,000*

* 弊社の試験原稿用紙を連続してスキャンした場合の数値であり、交換周期の目安です。紙粉の多く出る用紙や表面がざらざらした用紙では耐用枚数が少なくなるなど、お使いの用紙の種類によって交換周期は異なります。

スキャン枚数をリセットする

給紙ローラーキットを交換した後は、スキャン枚数をリセットします。

1. ホーム画面で［設定］-［機器情報］-［スキャン枚数リセット］-［ローラー交換後のスキャン枚数］の順に選択します。
2. ［はい］をタップします。

関連情報

➡ 「給紙ローラーキットを交換する」159ページ

節電の設定をする

スキャナーが動作していない状態が続いたときに、省電力のスリープモードに移行する、または自動で電源が切れる設定にしておくと節電できます。スリープモードに移行するまでの時間、電源が切れるまでの時間も設定できます。設定によってエネルギー効率に影響します。環境にご配慮ください。

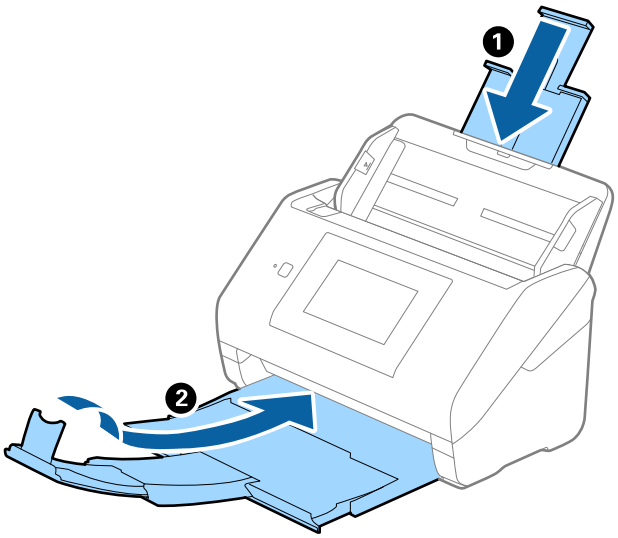
1. ホーム画面で［設定］を選択します。
2. ［基本設定］を選択します。
3. ［スリープ移行時間設定］または［自動電源オフ］を選択して、時間を設定します。

スキャナーを輸送する

スキャナーを修理に出すときや、引っ越しなどで輸送するときは、以下の手順で梱包します。

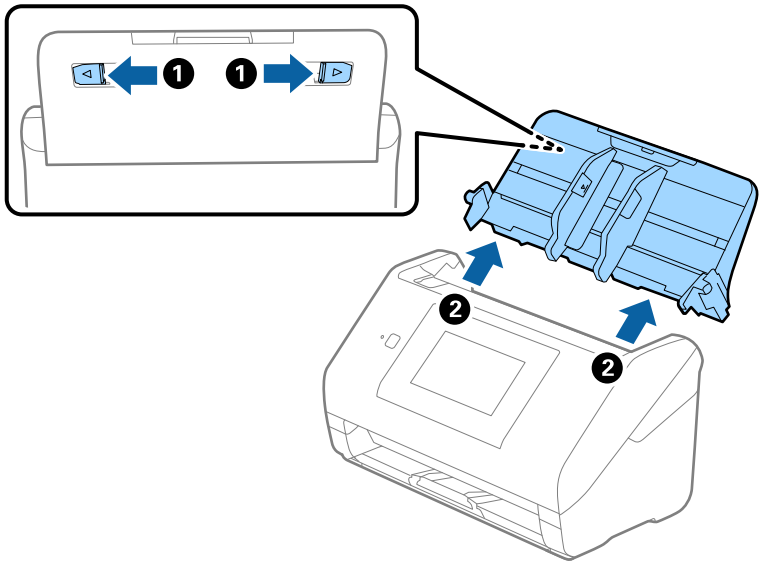
1. ⏻ボタンを押してスキャナーの電源を切ります。
2. ACアダプターを取り外します。
3. 接続しているケーブルや機器を取り外します。

4. 原稿サポートと排紙トレイを収納します。



重要 排紙トレイはしっかり閉めてください。輸送中に破損することがあります。

5. 給紙トレイを取り外します。



6. 保護材を取り付け、購入時の梱包箱か丈夫な箱に入れて梱包します。

設定のバックアップ

Web Configで設定した設定値をファイルにエクスポートできます。アドレス帳や設定値のバックアップ、スキャナーの置き換え時などに利用できます。
バイナリーファイルでエクスポートされるので編集できません。

設定をエクスポートする

スキャナーの設定値をエクスポートします。

1. Web Configで［デバイス管理］タブ - ［設定のエクスポート/インポート］ - ［エクスポート］を選択します。
2. エクスポートしたい設定を選択します。

   チェックが付いた項目の設定値がエクスポートされます。親のカテゴリーを選択すると、子のカテゴリーが同時に選択されます。ただし、IPアドレスなどネットワーク内に同じ設定値が複数あるとエラーになる項目は選択できないようになっています。
3. エクスポートファイルを暗号化するために任意のパスワードを0～20文字で入力します。

   ここで指定したパスワードはインポートするときに必要になります。パスワードを指定しない場合は空白にします。
4. ［エクスポート］をクリックします。

> **重要** デバイス名やIPv6アドレスなどのネットワーク情報を含めてエクスポートしたいときは［本体ごとの個別設定を選択可能にする］にチェックを付けて、項目を選択してください。なお、この項目をチェックしてから選択した設定値は、スキャナーの置き換え時のみにお使いください。

関連情報

➡ 「ブラウザーでWeb Configを起動する」35ページ

設定をインポートする

Web Configの設定ファイルをスキャナーにインポートします。

> **重要** スキャナー名やIPアドレスなどの個別情報を含む設定値をインポートするときは、同一のネットワーク内に同じIPアドレスを持つスキャナーが存在しないことを確認してください。

1. Web Configで［デバイス管理］タブ - ［設定のエクスポート/インポート］ - ［インポート］を選択します。
2. エクスポートされたファイルを選択し、暗号化パスワードを入力します。
3. ［次へ］をクリックします。
4. インポートする設定を選択して［次へ］をクリックします。
5. ［設定］をクリックします。

設定がスキャナーに反映されます。

関連情報

➡ 「ブラウザーでWeb Configを起動する」35ページ

購入時の設定に戻す

操作パネルで、［設定］-［管理者用設定］-［購入時の設定に戻す］を選択し、購入時の設定に戻す項目を選択します。

- ネットワーク設定：ネットワークに関する設定を購入時の状態に戻します。
- ネットワーク設定以外：ネットワークに関する設定を除いて、その他の設定を購入時の状態に戻します。
- 全ての設定：全ての設定を購入時の状態に戻します。

!重要 ［全ての設定］を選択した場合、スキャナーに登録されたアドレス帳および認証設定のユーザー情報も全て消去されます。消去した設定は復元できません。

ソフトウェアやファームウェアを更新する

ソフトウェアやファームウェアを更新すると、今まで起こっていたトラブルの解消、機能の改善や追加などができます。最新版のソフトウェアやファームウェアをお使いください。

!重要
- 更新中は、コンピューターやスキャナーの電源を切らないでください。

参考 スキャナーがインターネットに接続できると、Web Configからファームウェアをアップデートできます。［デバイス管理］タブ -［ファームウェアアップデート］の順に選択し、画面に表示されるメッセージを確認して、［確認開始］をクリックします。

1. スキャナーとコンピューターが通信可能な状態で、コンピューターがインターネットに接続されていることを確認します。

2. EPSON Software Updaterを起動して、ソフトウェアまたはファームウェアを更新します。

   参考 Windows Server OSには対応していません。

   - Windows 10
     スタートボタンをクリックして、［Epson Software］-［EPSON Software Updater］の順に選択します。
   - Windows 8.1/Windows 8
     検索チャームでソフトウェア名を入力して、表示されたアイコンを選択します。
   - Windows 7
     スタートボタンをクリックして、［すべてのプログラム］（または［プログラム］）-［Epson Software］-［EPSON Software Updater］の順に選択します。
   - Mac OS
     ［Finder］-［移動］-［アプリケーション］-［Epson Software］-［EPSON Software Updater］の順に選択します。

参考 一覧に表示されないソフトウェアはEPSON Software Updaterでは更新できません。エプソンのウェブサイトで最新版のソフトウェアを確認してください。
www.epson.jp/support/

操作パネルを使ってスキャナーのファームウェアを更新する

スキャナーがインターネットに接続されていると、操作パネルでスキャナーのファームウェアを更新できます。新しいファームウェアがあるかどうかを定期的に確認して、ある場合には通知するようにも設定できます。

1. ホーム画面で［設定］を選択します。
2. ［管理者用設定］-［ファームウェアのアップデート］-［アップデート］の順に選択します。

   参考 新しいファームウェアがあるかどうか定期的に確認したいときは、［定期通知設定］-［オン］の順に選択します。

3. 画面に表示されるメッセージを確認して、利用可能なアップデートの検索を開始します。
4. 新しいファームウェアが見つかったというメッセージが表示されたら、画面の指示に従ってファームウェアを更新します。

重要
- 更新中はスキャナーの電源を切ったり、電源プラグをコンセントから抜いたりしないでください。スキャナーが故障するおそれがあります。
- ファームウェアの更新に失敗すると、次回電源を入れたときに「Recovery Mode」（リカバリーモード）と表示され、スキャナーが動かなくなります。コンピューターでファームウェアの更新をし直してください。
  リカバリーモードになるとネットワーク接続での更新ができないため、以下の手順で作業してください。
  1.エプソンのホームページからファームウェアをダウンロードする
  2.コンピューターとスキャナーをUSBケーブルで接続する
  3.ファームウェアを更新する
  www.epson.jp/support/

Web Configでファームウェアをアップデートする

スキャナーがインターネットに接続できると、Web Configからファームウェアをアップデートできます。

1. Web Configで［デバイス管理］タブ-［ファームウェアアップデート］を選択します。
2. ［確認開始］をクリックして、画面に従って操作します。

   ファームウェアの確認が始まり、更新されたファームウェアがあるとファームの情報が表示されます。

参考 Epson Device Adminを使ってもファームウェアをアップデートできます。デバイス一覧でファームウェアの情報が確認ができます。この方法は、複数のデバイスのファームウェアをアップデートするのに便利です。詳細はEpson Device Adminのマニュアルやヘルプをご覧ください。

関連情報

➡ 「ブラウザーでWeb Configを起動する」35ページ

スキャナーをインターネットに接続しないでファームウェアをアップデートする

コンピューターでエプソンのウェブサイトから機種用のファームウェアをダウンロードし、USBケーブルで接続してアップデートすることもできます。ネットワーク経由でアップアップデートができない場合に、この方法をお使いください。

参考 アップデートする前に、お使いのコンピューターに必ずEpson Scan 2をインストールしてください。Epson Scan 2がインストールされていないときは、再インストールしてください。

1. エプソンのウェブサイトで最新ファームウェアのリリースを確認します。

   www.epson.jp/support/

   - お使いのスキャナーのファームウェアがあれば、ダウンロードして、次の手順に進みます。
   - ウェブサイトにお使いのスキャナーのファームウェア情報がなければ、すでに最新のファームウェアになっています。

2. ファームウェアをダウンロードしたコンピューターとスキャナーをUSBケーブルで接続します。

3. ダウンロードしたexeファイルをダブルクリックします。

   Epson Firmware Updaterが起動します。

4. 画面の指示に従って操作します。