NEC

Internet Services ヘルプ

設定・操作編

1.このマニュアルの編集、変更、または無断で転載はしないでください。
2.このマニュアルに記載されている内容は、将来予告なしに変更されることがあります。
3.このマニュアルに記載されている画面やイラストは一例です。ご使用の機種やソフトウェア、OS のバージョンによって異なることがあります。

GM2173J9-1
日本電気株式会社

もくじ

1 Internet Services で設定する機能

1.1 IEEE802.1X 認証方式を使った Wi-Fi 接続の設定

高度なセキュリティー環境への接続

本機の Wi-Fi 接続では、IEEE802.1X 認証を使用できます。IEEE802.1X 認証方式を使用する場合は、認証局に証明書の発行を依頼し、発行された証明書を Internet Services で本機にインポートします。

補足

Internet Services で証明書をインポートするには、HTTP の通信を暗号化する設定がされている必要があります。Internet Services の操作、および HTTP 通信を暗号化する方法については、「HTTP の通信を暗号化するための設定」（P.6）を参照してください。

1. **Internet Services に機械管理者としてログインします。**
2. **証明書をインポートします。**
   1) **［システム］＞［セキュリティー設定］＞［証明書設定］をクリックします。**
   2) **［インポート］をクリックします。**
   3) **［選択］をクリックし、インポートするファイル名を指定します。**
   4) **［パスワード］にインポートする証明書に設定されたパスワードを入力します。**
   5) **［パスワードの再入力］に、同じパスワードを入力します。**
   6) **［実行］をクリックします。**
   7) **Web ブラウザーの再読み込みを行います。**
3. **Wi-Fi 接続とセキュリティーの設定をします。**

   補足

   お使いの環境の認証方式によって、設定方法が異なります。

   1) **［ネットワーク］＞［Wi-Fi］をクリックします。**
   2) **［有効］を有効にします。**
   3) **［SSID］に接続先の SSID を入力します。**
   4) **［暗号化設定］で、［WPA2 Enterprise］を選択します。**
   5) **［認証方式］を選択します。**
   6) **［Identity］に EAP-Identity の値を入力します。**
      認証方式が EAP-TLS の場合は、手順 11 に進みます。

      補足

      EAP-Identity については、RADIUS サーバー管理者に確認してください。

7) **認証方式が PEAPv0 MS-CHAPv2、EAP-TTLS/PAP、EAP-TTLS/CHAP、EAP-TTLS/MS-CHAPv2 の場合は、［ユーザー名］および［パスワード］に WPA-Enterprise 認証用のログインユーザー名およびパスワードを設定します。**
8) **［パスワードの再入力］に、確認のためパスワードをもう一度入力します。**
9) **［ルート証明書］で、インポートした CA 証明書を選択します。**
10) **認証方式が EAP-TLS の場合は、［クライアント証明書］で、インポートしたクライアント証明書を選択します。**
11) **［保存］をクリックします。**
12) **［今すぐ再起動］をクリックします。**

本機が再起動し、設定した値が反映されます。

1.2 暗号化の設定

HTTP の通信を暗号化するための設定

Step1 証明書の準備

HTTP の通信を暗号化するための証明書を用意します。自己証明書（SSL サーバー用）を生成する方法と、ほかの認証局で作成された証明書をインポートする方法があります。

補足

［デバイス証明書］または［その他の証明書］のどちらかのカテゴリーに、すでに同じ証明書が登録されている場合は、インポートできません。登録されている証明書を削除してから、インポートしてください。

自己証明書（SSL サーバー用）を生成する場合

1. **Internet Services に機械管理者としてログインします。**
2. **［システム］をクリックします。**
3. **［セキュリティー設定］＞［証明書設定］をクリックします。**
4. **［新規作成］＞［自己署名証明書の作成］をクリックします。**
5. **必要に応じて、各項目を設定します。**
6. **［実行］をクリックします。**
7. **生成が終了したら、［閉じる］をクリックします。**

ほかの認証局で作成された証明書を本機にインポートする場合

ほかの認証局で作成された証明書を本機にインポートする前に、自己証明書を生成し、HTTP 通信を暗号化するよう設定してください。

1. **Internet Services に機械管理者としてログインします。**
2. **［システム］をクリックします。**
3. **［セキュリティー設定］＞［証明書設定］＞［インポート］をクリックします。**
4. **［選択］をクリックして表示されるダイアログボックスでインポートするファイルを選び、［開く］をクリックします。**

   補足

   インポートするファイルのパスを直接入力することもできます。
5. **［パスワード］にインポートする証明書に設定されたパスワードを入力します。**
6. **［パスワードの再入力］に同じパスワードを入力します。**
7. **［実行］をクリックします。**
8. **インポートが終了したら、［閉じる］をクリックします。**

Step2 証明書の設定

サーバー用の証明書を本機に設定します。

補足

本項目の設定を行っていない状態では、自己生成した証明書がサーバー用として自動的に設定されます。

1. **Internet Services に機械管理者としてログインします。**
2. **［システム］をクリックします。**
3. **［セキュリティー設定］＞［SSL/TLS 設定］をクリックします。**
4. **［本体の証明書 - サーバー］で証明書を選びます。**

注記

証明書を選べないときは、［システム］＞［セキュリティー設定］＞［証明書設定］にデバイス証明書が登録されていることを確認してください。

5. **［HTTP - SSL/TLS 通信ポート番号］を必要に応じて設定します。**

注記

ほかのポートと同じポート番号にしないでください。

6. **［保存］をクリックします。**
7. **本機を再起動する表示に変わったら、［今すぐ再起動］をクリックします。**

IPsec を使用して暗号化するための設定

IPsec 通信で IKE 認証方式を［デジタル署名］にするときは、本機に証明書を設定します。証明書は、本体出荷時には、本機にインポートされていません。IPsec 用証明書をインポートします。インポート後、IPsec の設定をします。

IKE 認証方式が［事前共有鍵］の場合には、Step1 の「証明書の準備」は不要です。Step2 の「IPsec の設定」を行ってください。

注記

［デバイス証明書］または［その他の証明書］のどちらかのカテゴリーに、すでに同じ証明書が登録されている場合は、インポートできません。登録されている証明書を削除してから、インポートしてください。

補足

IPsec 用証明書としてインポートする証明書に V3 拡張（KeyUsage）がある場合には、デジタル署名のビットがオンに設定されている必要があります。

Step1 証明書の準備

Internet Services で証明書を設定するには、HTTP の通信を暗号化する設定を行ってから、ほかの認証局で作成された証明書を本機にインポートして、IPsec 用証明書として設定します。

補足

・本機にインポートできる証明書の公開鍵は、RSA® 公開鍵 4096 ビットまで、または ECC 公開鍵の P-256/P-384/P-521 のどれかとなります。
・IPsec 用には、Internet Services で作成した自己証明書は使用できません。

参照

HTTP の通信を暗号化する設定方法は、「HTTP の通信を暗号化するための設定」（P.6）を参照してください。

1. **Internet Services に機械管理者としてログインします。**
2. **［システム］をクリックします。**
3. **［セキュリティー設定］＞［証明書設定］＞［インポート］をクリックします。**
4. **［選択］をクリックして表示されるダイアログボックスでインポートするファイルを選び、［開く］をクリックします。**

補足

インポートするファイルのパスを直接入力することもできます。

5. **［パスワード］にインポートする証明書に設定されたパスワードを入力します。**
6. **［パスワードの再入力］に同じパスワードを入力します。**
7. **［実行］をクリックします。**
8. **インポートが終了したら、［閉じる］をクリックします。**

Step2 IPsec の設定

1. **［ネットワーク］＞［プロトコル設定］＞［IPsec］をクリックします。**
2. **［有効］を有効にします。**
3. **［IKE 認証方式］をクリックし、IKE 認証方式を設定します。**

デジタル署名方式の場合

1) **［デジタル署名］を選びます。**
2) **［本体の証明書］をクリックします。**
3) **認証に使う証明書を選び、［保存］をクリックします。**

事前共有鍵方式の場合

1) **［事前共有鍵］を選びます。**
2) **事前共有鍵にする文字列を入力し、［保存］をクリックします。**

4. **その他の必要な設定をします。**

Step3 通信先機器の設定

通信する相手機器の設定について説明します。

通信先機器では次の設定を行う必要があります。

- IP セキュリティーポリシーの作成
- ポリシーの割り当て

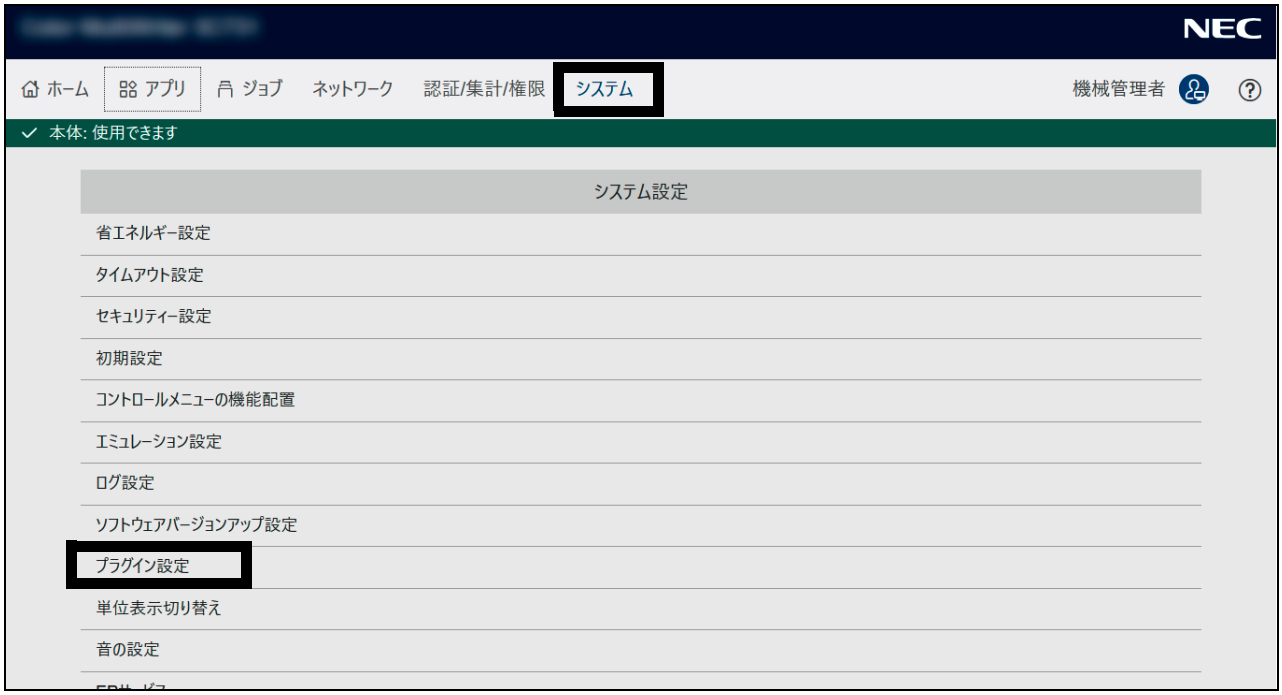
参照

設定方法は、通信先機器のヘルプを参照してください。

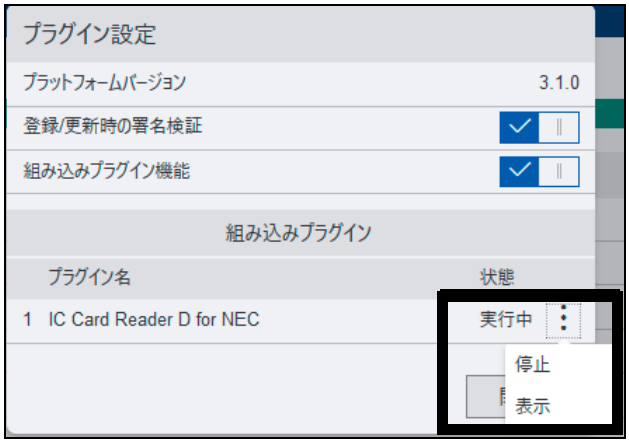
1.3 その他の設定事例

IC カードリーダーの設定

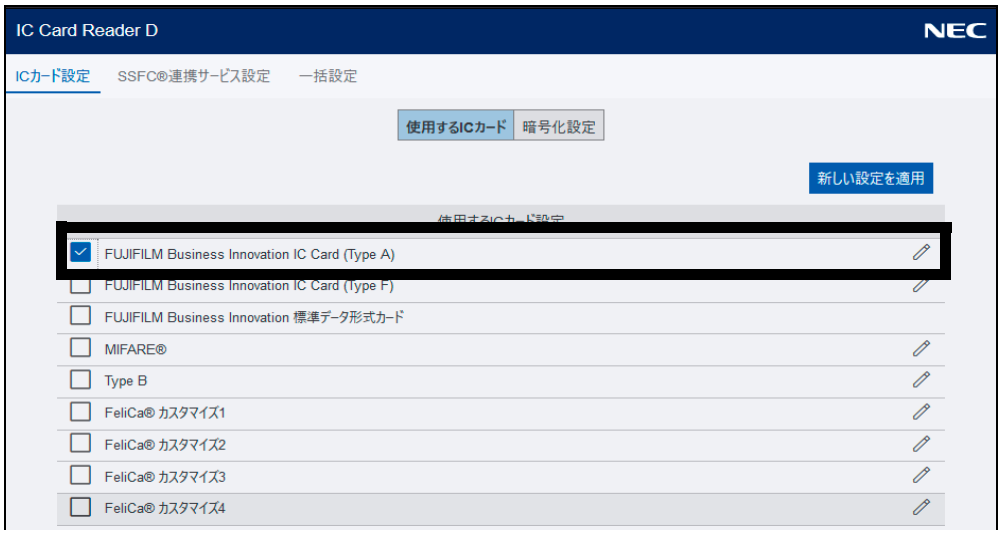
1. **Internet Services に機械管理者としてログインします。**
2. **［システム］＞［プラグイン設定］をクリックします。**



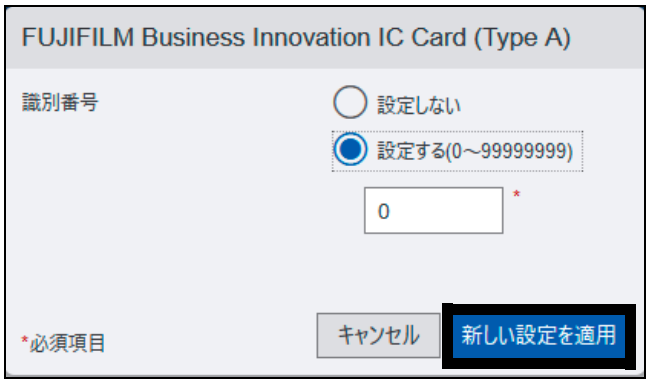
3. **［組み込みプラグイン］から、オプション接続されている IC カードリーダーの ⋮ をクリックし、［表示］を選択します。**



4. **使用する IC カードにチェックマークを付け、をクリックします。**



5. **必要な読み取り情報を入力し、［新しい設定を適用］をクリックします。**

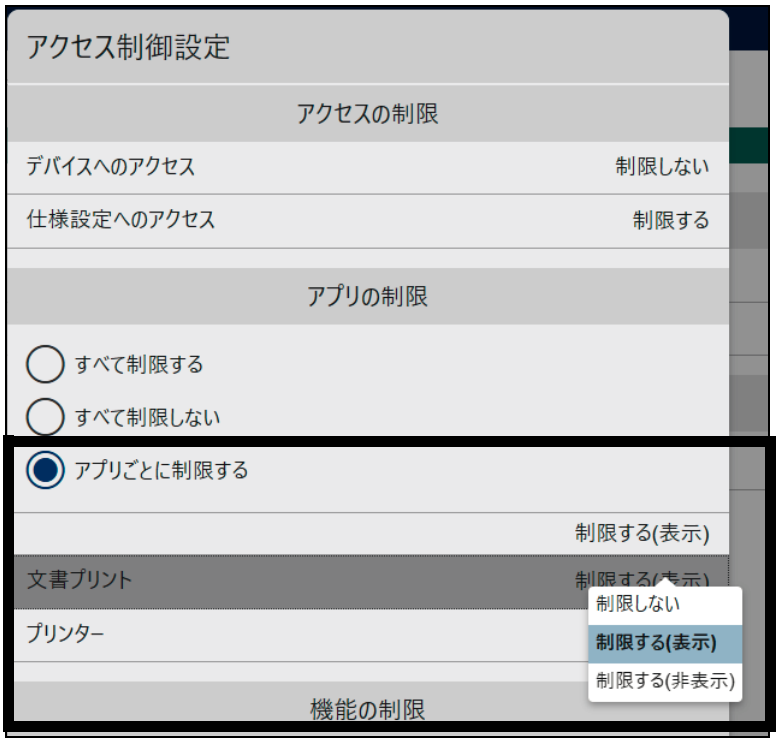


アクセス制限の設定

ここではアプリごとにアクセスを制限する方法を説明します。

1. **Internet Services に機械管理者としてログインします。**
2. **［認証 / 集計 / 権限］＞［権限設定］＞［アクセス制御設定］をクリックします。**

3. **［アプリの制限］で［アプリごとに制限する］を選択し、アプリの操作制限を設定します。**



- 制限しない

  当該サービスの操作は制限されません。
- 制限する (表示)

  本機のホーム画面に、当該サービスが鍵付きアイコンで表示されます。サービスを利用するには、認証が必要です。
- 制限する (非表示)

  本機のホーム画面に、当該サービスが表示されません。サービスを利用するには、認証が必要です。

4. **［保存］をクリックします。**

1.4 Exchange Online/Outlook.com の SMTP/POP3 サーバーの設定

Internet Services を使用して、OAuth 2.0 認証を使用する Exchange Online/Outlook.com の SMTP/POP3 サーバーを設定します。

注記

- SMTP/POP3 サーバーは、それぞれ 1 つずつしか設定できません。後から設定した内容が有効になります。
- OAuth 2.0 認証を使用する Exchange Online/Outlook.com の SMTP/POP3 サーバーを設定した場合、本機の操作パネルでの設定内容は使用されず、SMTP サーバー名や POP3 サーバー名は空欄となります。操作パネルで SMTP サーバー名や POP3 サーバー名を入力した場合は、Internet Services の［サービスプロバイダー］の設定が［指定しない］に変更されます。

Microsoft Entra ID でのアプリ登録

本機が SMTP/POP3 サーバーにアクセスするために、Microsoft Entra ID でアプリ登録します。

1. **Azure Portal にグローバル管理者のアカウントでサインインし、［Microsoft Entra ID］を選択します。**
2. **画面左側の［管理］＞［アプリの登録］を選択し、画面上部の［新規登録］をクリックします。**
3. **［アプリケーションの登録］の［名前］欄に、アプリケーションの表示名を入力します。**
   例：Mail App
4. **［サポートされているアカウントの種類］で、［この組織ディレクトリのみに含まれるアカウント］を選択します。**
5. **画面下部の［登録］をクリックします。**
6. **画面左側の［管理］＞［認証］を選択し、［プラットフォーム構成］の［プラットフォームを追加］をクリックします。**
7. **画面右側の［プラットフォームの構成］で、［モバイル アプリケーションとデスクトップアプリケーション］を選択します。**
8. **画面右側の［デスクトップとデバイスの構成］の［リダイレクト URI］で「https://login.microsoftonline.com/common/oauth2/nativeclient」を選択し、画面下部の［構成］をクリックします。**
9. **画面下部の［詳細設定］＞［パブリック クライアント フローを許可する］＞［次のモバイルとデスクトップのフローを有効にする］で［はい］を選択し、［保存］をクリックします。**
10. **画面左側の［API　のアクセス許可］を選択し、［構成されたアクセス許可］で［アクセス許可の追加］をクリックします。**
11. **画面右側の［API アクセス許可の要求］で、［Microsoft API］の［Microsoft Graph］を選択します。**
12. **［アプリケーションに必要なアクセス許可の種類］で、［委任されたアクセス許可］を選択します。**

13. 次のアクセス許可を選択します。

- OpenId アクセス許可

  email

  offline_access
- POP

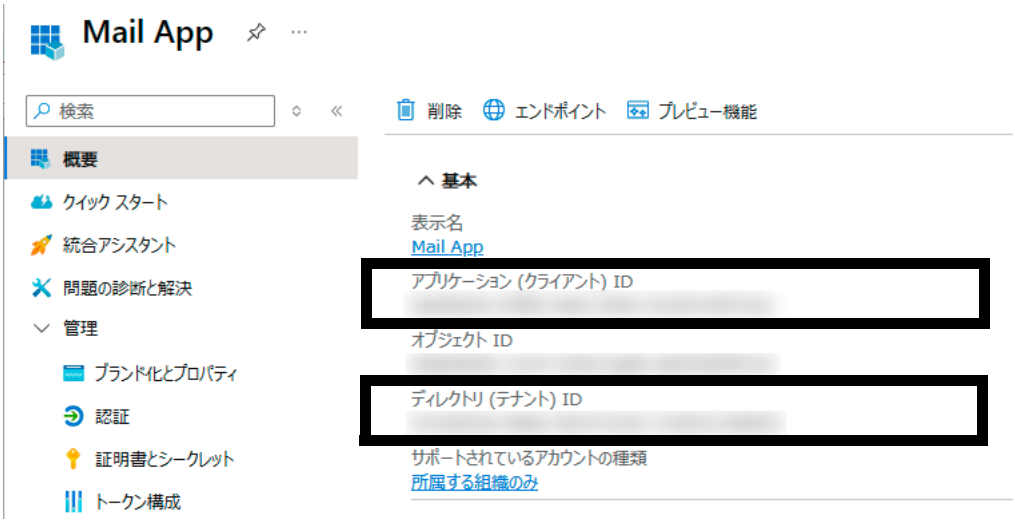
  POP.AccessAsUser.All
- SMTP

  SMTP.Send

14. 画面下部の［アクセス許可の追加］をクリックします。

15. 画面左側の［概要］を選択し、［アプリケーション（クライアント）ID］と［ディレクトリ（テナント）ID］の値をコピーします。

これらの ID は、Internet Services からの認証時に使用します。設定方法は、「Internet Services での SMTP サーバー設定」（P.14）、「Internet Services での POP3 サーバー設定」（P.15）を参照してください。

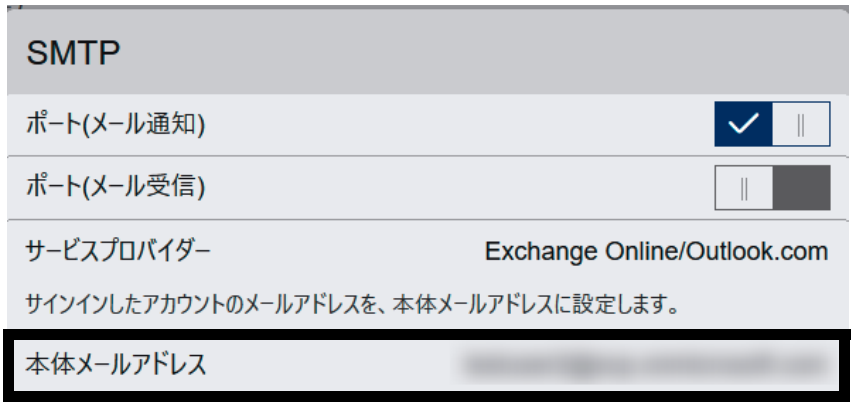


Internet Services での SMTP サーバー設定

1. **Internet Services に機械管理者としてログインします。**
2. **必要に応じて、DNS サーバーとプロキシサーバーを設定します。**
3. **［ネットワーク］＞［プロトコル設定］＞［SMTP］をクリックし、［ポート (メール通知)］を有効にします。**
4. **［サービスプロバイダー］をクリックし、［Exchange Online/Outlook.com］を選択します。**
5. **［テナント］と［クライアント ID］に、それぞれ「Microsoft Entra ID でのアプリ登録」（P.12）でコピーした［ディレクトリ (テナント)ID］と［アプリケーション (クライアント)ID］の値を貼り付けます。**
6. **［保存］をクリックします。**

   注記

   特別な理由がない限り、［受信ポート番号］、［テナント］、［クライアント ID］以外の項目は変更しないでください。
7. **［認証コードの入力］画面で、［次へ］をクリックします。**
8. **コードの入力画面で、［認証コードの入力］画面に表示されたコードを入力し、［次へ］をクリックします。**
9. **サインイン画面で、送信用メールアドレスが設定されているアカウントでサインインします。**
10. **サインインに成功したら、サインイン画面を閉じます。**
    サインインしたアカウントのメールアドレスが、本体メールアドレスに設定されます。



注記

サインインしたアカウントの UPN（ユーザープリンシパル名）と本体メールアドレスは、同じである必要があります。
サインイン後に、Internet Services の［機械の詳細］ダイアログボックスや本機の操作パネルから、本体メールアドレスをサインインしたアカウントの UPN とは異なる文字列に変更しないでください。変更すると認証エラーになります。

Internet Services での POP3 サーバー設定

1. **Internet Services に機械管理者としてログインします。**
2. **必要に応じて、DNS サーバーとプロキシサーバーを設定します。**
3. **［ネットワーク］＞［プロトコル設定］＞［POP3］をクリックし、［ポート (メール受信)］を有効にします。**
4. **［サービスプロバイダー］をクリックし、［Exchange Online/Outlook.com］を選択します。**
5. **［テナント］と［クライアント ID］に、それぞれ「Microsoft Entra ID でのアプリ登録」（P.12）でコピーした［ディレクトリ (テナント)ID］と［アプリケーション (クライアント)ID］の値を貼り付けます。**
6. **［保存］をクリックします。**

   注記

   特別な理由がない限り、［受信間隔］、［テナント］、［クライアント ID］以外の項目は変更しないでください。
7. **［認証コードの入力］画面で、［次へ］をクリックします。**
8. **コードの入力画面で、［認証コードの入力］画面に表示されたコードを入力し、［次へ］をクリックします。**
9. **サインイン画面で、受信用メールアドレスが設定されているアカウントでサインインします。**
10. **サインインに成功したら、サインイン画面を閉じます。**

2 Internet Services で操作する機能

2.1 プリント

Internet Services でプリント

ファイルをプリンタードライバーを使用せずにプリントできます。

補足

CMYK の TIFF ファイルと JPEG（JFIF）ファイルには対応していません。

1. **Internet Services を起動します。**
2. **ホーム画面下部の［プリント］をクリックします。**
3. **［選択］をクリックして、ファイルを指定します。**
4. **必要に応じて［プリント設定］を設定します。**
5. **［プリント］をクリックします。**

NFC 機能でプリント

モバイル機器が NFC タッチプリントに対応している場合は、操作パネルの NFC タッチエリアにタッチするだけで自動的にプリントできます。

本機の NFC 機能を利用するには、Internet Services の設定が必要です。

1. **Internet Services に機械管理者としてログインします。**
2. **［ネットワーク］＞［NFC］をクリックします。**
3. **［アクティブタグ］と［NFC カードリーダー］を有効にします。**
4. **［保存］をクリックします。**

AirPrint

AirPrint は、Apple Inc. が提供する印刷サービスです。プリンタードライバーや特別なソフトウェアをインストールすることなく、iPad/iPhone などの iOS 搭載端末や macOS/OS X のコンピューターから指示した文書を、お使いの機械でプリントできます。

補足

AirPrint の最新の情報については、Apple Inc. の公式サイトを参照してください。

AirPrint の設定

1. **Internet Services に機械管理者としてログインします。**
2. **上側のメニューから［ネットワーク］をクリックします。**
3. **［モバイルプリント設定］の［AirPrint™］をクリックし、［有効］を有効にします。**

   補足

   USB で接続しているときは、［USB 接続］も有効にします。
4. **必要に応じて、各機能を設定します。**
5. **［保存］をクリックします。**

   補足

   設定を反映するには再起動が必要です。画面の指示に従って、再起動してください。

コンピューター側の設定（macOS/OS X のみ）

AirPrint を使用する場合は、あらかじめお使いの機械をコンピューターに登録しておく必要があります。

補足

USB 接続を経由して AirPrint を使用する場合は、本機とコンピューターを USB ケーブルで接続すると自動的に登録されるため、この設定は不要です。

1. **ネットワークに接続されたコンピューターで、［Apple］メニュー＞［システム環境設定］をクリックします。**
2. **［プリンタとスキャナ］をクリックします。**
3. **［+］（追加）をクリックします。**

   補足

   ［+］（追加）をクリックしたときにドロップダウンメニューが表示された場合は、［プリンタまたはスキャナを追加］を選択してください。
4. **［名前］の一覧から本機を選択します。**

   補足

   ネットワーク内のプリンターが自動的に検出されて［名前］の一覧に表示されます。表示されない場合は、本機とコンピューターのネットワーク設定を確認してください。
5. **［ドライバ］＞［Secure AirPrint］または［AirPrint］＞［追加］をクリックします。**
   ［プリンタとスキャナ］画面の［プリンタ］の項目に本機が追加されます。

プリント

iOS からプリント

ここでは iPad を例に、iOS からプリント指示する手順を説明します。

1. **プリントする文書を開きます。**
2. **メニューから［プリント］をタップします。**
3. **［プリンタを選択］をタップします。**
4. **本機を選び、プリント設定をします。**
5. **［プリント］をタップします。**

macOS/OS X からプリント

1. **プリントする文書を表示します。**
2. **［ファイル］メニュー>［プリント］をクリックします。**
3. **［プリンタ］で本機を選択し、プリント設定を確認して、［プリント］をクリックします。**

補足

本機で対応していないプリント設定は選択できません。

2.2 ユーザー認証の操作

登録ユーザーのパスワードの変更

機械管理者は、Internet Services を使用して、パスワードの設定や変更ができます。

1. **Internet Services に機械管理者としてログインします。**
2. **上側のメニューから［認証 / 集計 / 権限］をクリックします。**
3. **［ユーザーアカウント一覧］から設定 / 変更するユーザーをクリックします。**
4. **［パスワード変更］をクリックし、新しいパスワードを入力します。**
5. **［保存］をクリックします。**