imagePROGRAF
シリーズ

ネットワークセキュリティガイド

NETWORK SECURITY GUIDE

第４版

はじめに

本書ではキヤノン製大判プリンター（imagePROGRAFシリーズ）のネットワークセキュリティに関して説明しています。目的に応じて必要な項目を参照してください。

個人情報の漏えいや外部からの不正使用など、プリンターを取り巻くさまざまなリスクを軽減するために、効果的・継続的な対策が必要になります。プリンターをより安全にご利用いただくために、アクセス権限やセキュリティなど、プリンターの重要な設定を管理者が統括して行ってください。

本書は、キヤノン製大判プリンター imagePROGRAFシリーズ共通の説明書です。対象機種は以下のとおりです。操作説明については、imagePROGRAF TM-355 を例に説明しています。お使いの製品の仕様によっては、記載の一部が該当しないことがあります。

対象機種：

imagePROGRAF TM-355/TM-255/TM-350/TM-250/TM-340/TM-240
imagePROGRAF TM-5355/TM-5255/TM-5350/TM-5250/TM-5340/TM-5240
imagePROGRAF TC-20M/TC-20
imagePROGRAF TC-5200M/TC-5200
imagePROGRAF GP-4000/GP-2000
imagePROGRAF GP-540/GP-520
imagePROGRAF GP-300/GP-200
imagePROGRAF GP-5300/GP-5200
imagePROGRAF TZ-30000
imagePROGRAF TZ-5300
imagePROGRAF TX-4100/TX-3100/TX-2100
imagePROGRAF TX-5410/TX-5310/TX-5210
imagePROGRAF PRO-6100/PRO-4100/PRO-2100/PRO-6100S/PRO-4100S
imagePROGRAF PRO-561/PRO-541/PRO-521/PRO-561S/PRO-541S
imagePROGRAF TA-30/TA-20
imagePROGRAF TA-5300/TA-5200
imagePROGRAF TM-305/TM-300/TM-205/TM-200
imagePROGRAF TM-5305/TM-5300/TM-5205/TM-5200
imagePROGRAF TX-4000/TX-3000/TX-2000
imagePROGRAF TX-5400/TX-5300/TX-5200
imagePROGRAF PRO-6000/PRO-4000/PRO-2000/PRO-6000S/PRO-4000S
imagePROGRAF PRO-560/PRO-540/PRO-520/PRO-560S/PRO-540S

各機種のオンラインマニュアルもあわせてご参照ください。
https://ij.start.canon

本書の読みかた

本書では、各種機能の説明と操作手順を章ごとに説明しています。

マークについて

取り扱い上の制限・注意などの説明に、次のマークを付けています。

重要

製品の故障・損傷や誤った操作を防ぐために、守っていただきたい重要事項です。かならずお読みください。

参考

操作の参考になることや補足説明です。

プリンターの操作パネルでの操作手順です。

パソコンのウェブブラウザーからプリンターの設定が可能な「リモートUI」での操作手順です。

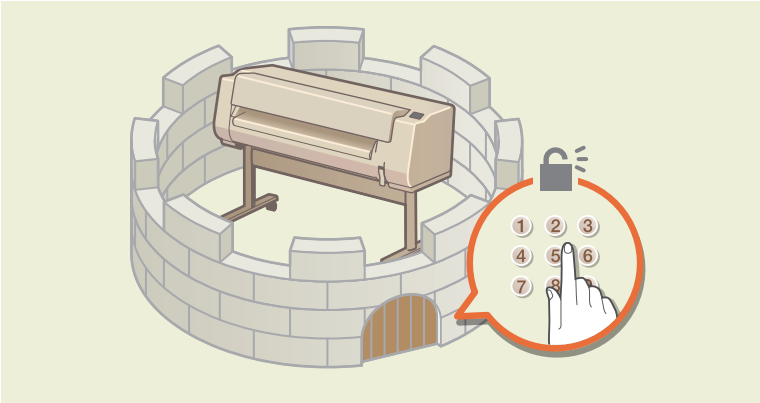
目　次

概要

パソコンやプリンターなどの情報機器を通じて扱われる機密情報は、悪意のある第三者の標的となる場合があります。不正アクセスなどによる攻撃だけでなく、不注意や誤操作による情報漏えいが結果的に予想外の損失に結びつく恐れもあります。こうしたリスクに備えてプリンターにはさまざまなセキュリティ機能が搭載されています。お使いの環境に合わせて必要な対策を行ってください。

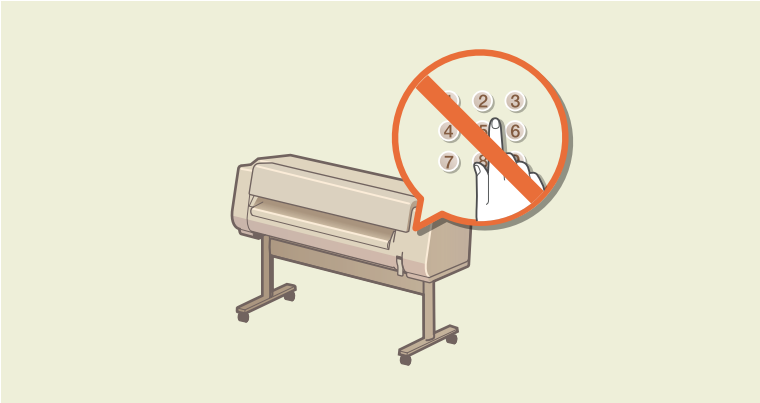
管理者パスワードの設定

アクセス権を持つユーザーだけがプリンターの設定変更できるようにして、第三者の不正使用を防ぐことができます。



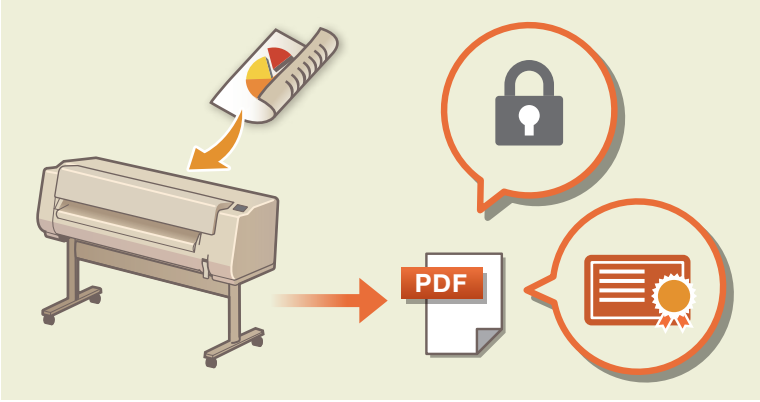
ユーザー制限

一般ユーザーモードでの操作に制限を設けることができます。



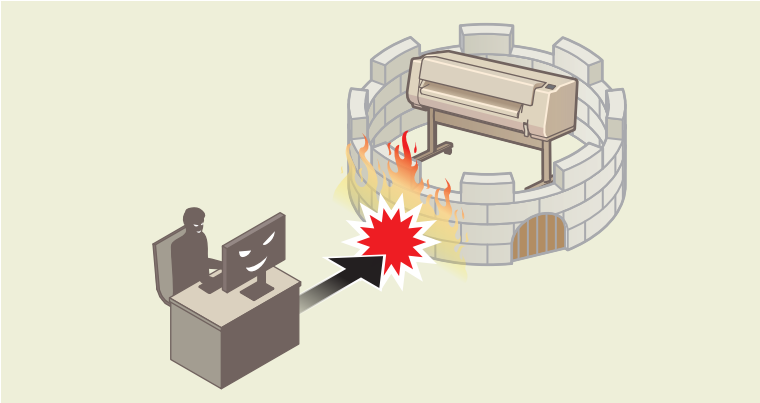
ハードディスク内のデータ保護

プリンター内のデータを保護する観点から、ハードディスク内部のデータを管理できます。



ネットワークセキュリティ

大切なデータや情報を守るためにネットワークのセキュリティ設定を行うことができます。



ファームウェアアップデート

常に最新のファームウェアにアップデートすることで、快適に、かつ安全にプリンターを使用していただくことができます。

1 お使いになる前に

この章では、ネットワークセキュリティ設定の前準備としてリモートUIの使いかたと管理者パスワードの設定方法を説明します。

1.1 リモートUI

リモートUI を使って、ネットワーク経由でプリンターの状態を確認したり設定変更ができます。お使いのスマートフォン、タブレット、またはパソコンのウェブブラウザーを使って、プリンターにアクセスします。

リモートUIには、管理者モードと一般ユーザーモードの2つのモードがあります。管理者モードでは、プリンターのすべての設定を変更したり一般ユーザーの操作を制限したりできます。一般ユーザーモードでは、特定の設定のみを変更できます。

参考

- リモートUIを使用するときは、プリンターをLAN接続してください。
- 利用可能なOS、ウェブブラウザーについては、お使いの機種のオンラインマニュアルをご参照ください。

リモートUIを起動する

操作パネル

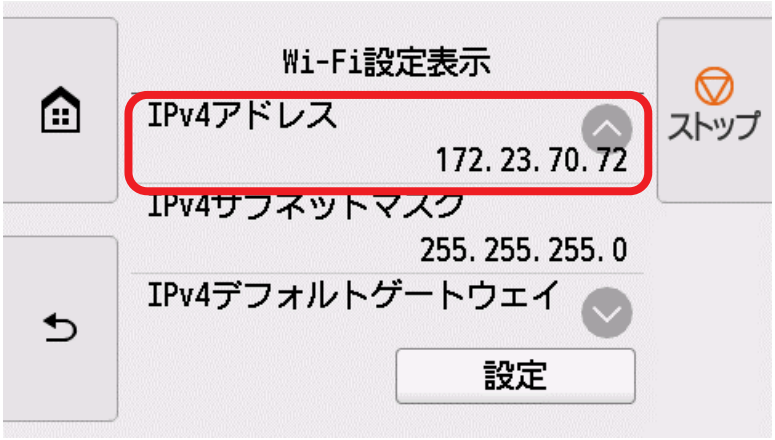
1. プリンターのIPアドレスを確認する

(1) ホーム画面から（ネットワーク）を選ぶ

(2) 有効になっているLANを選ぶ

無効になっているLANのアイコンには、斜線が表示されています。

(3)　表示された画面の [IPv4アドレス] を確認する



リモートUI

2.　ウェブブラウザーを開き、URL欄にプリンターのIPアドレスを入力する

ウェブブラウザーのURL欄に、下記のように入力します。

http://XXX.XXX.XXX.XXX

アクセスできると、リモートUIが起動し、ウェブブラウザーにログイン画面が表示されます。

参考

- 初めてリモートUIを表示した場合は、ルート証明書をダウンロードして、ウェブブラウザーに登録してください。
  ➡ SSL通信のためにプリンターのルート証明書をウェブブラウザーに登録する
- ルート証明書を登録していないときは、安全な通信ができないことをお知らせする警告が表示される場合があります。

3.　[ログイン] を選ぶ

パスワード認証画面が表示されます。

重要

- 一般ユーザーモードを有効にしている場合は、管理者モードまたは一般ユーザーモードのどちらでログインするかを選べます。ただし、ネットワークやセキュリティ関連の設定変更を行う際は、管理者モードでログインしてください。
  ➡ 1.2　パスワードを変更/設定する
- プリンターには工場出荷時に管理者パスワードが設定されています。管理者パスワードはプリンターのシリアルナンバーに設定されています。
  ➡ 4.2　プリンターのシリアルナンバーを確認する

4.　パスワードを入力して、[OK] をクリックする

リモートUIのトップ画面が表示されます。

リモートUIで設定できる項目

[プリンターの状態]

プリンターのインク残量、ステータス、エラーの詳細情報などが表示されます。

また、サポートページに接続し、インターネット経由で提供されるサービスを利用できます。

[ユーティリティ]

クリーニングなど、プリンターのメンテナンスを実行できます。

[本体設定]

印刷設定など、プリンターの設定を変更できます。

また、メール機能の設定や、プリンターの状態をお知らせするように設定できます。

[特殊設定] の [操作パネルのアクセスロック] から、操作パネルでの操作を制限することもできます。

[AirPrint設定]

macOSまたはiOSのAirPrintを使用して印刷するときの印刷設定を行います。

[Webサービス接続設定]

プリンターの機器情報を利用するWebサービスの設定を行います。

[ジョブ管理]

ジョブ履歴の閲覧や印刷、ジョブの削除をすることができます。

[セキュリティ] (管理者向け項目)

パスワードや、暗号化通信のための証明書に関する設定などを行います。

[使用実績]

お使いのプリンターの使用実績を確認することができます。

[システム情報とLAN設定]

システム情報の確認とLAN設定ができます。

[ファームウェアのアップデート]（管理者向け項目）
プリンターのファームウェアのアップデート、ファームウェアのバージョン確認、DNSサーバーおよびプロキシサーバーの設定を行います。

[言語選択]（管理者向け項目）
表示言語を変更できます。

[マニュアル]
オンラインマニュアルを表示します。
リモートUIを開いているパソコンが、インターネットに接続されている必要があります。

1.2 パスワードを変更/設定する

リモートUIを使って、ネットワーク経由でプリンターの状態を確認したり設定変更ができます。管理者モードと一般ユーザーモードのそれぞれに、パスワードを設定することが可能です。

管理者モードでログインすると、プリンターのすべての設定を変更したり一般ユーザーの操作を制限したりすることができます。一般ユーザーモードでログインしたときは、一部の設定のみ変更できます。

管理者パスワードを設定すると、操作パネルの一部のメニューを利用する際に、パスワードの入力が必要になります。管理者パスワードの設定は、プリンターの操作パネルから行う方法と、リモートUIから行う方法があります。

重要

- パスワードには、以下の文字制限があります。
  4～32文字で設定してください。
  使用可能な文字は半角英数字、スペース、ウムラウト文字、および以下の記号です。
  - ! @ # $ % ^ & * _ ; : , . / ` = + ' " ( ) { } [ ] < > ¦
- セキュリティの観点から、パスワードは半角英数字と記号を組み合わせて8文字以上にすることをおすすめします。

リモートUIで管理者パスワードを変更/設定する

参考

- 管理者パスワードは、管理者モードでログインしているときのみ設定できます。

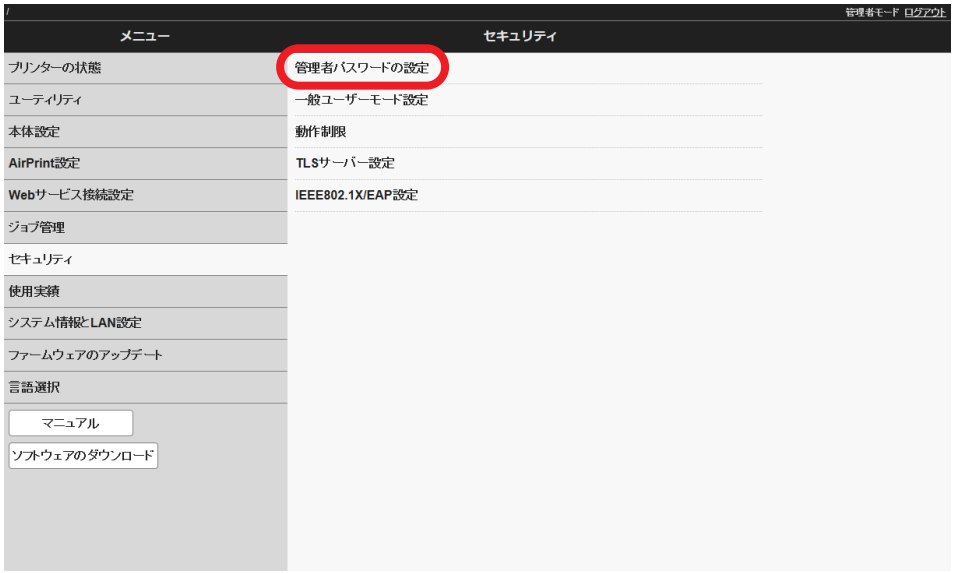
リモートUI

1.　リモートUIを起動する

➡ リモートUIを起動する

2.　[セキュリティ] を選ぶ

3.　[管理者パスワードの設定] を選ぶ



4.　[管理者パスワードの変更] を選ぶ

5.　管理者パスワードの有効範囲を選び、[OK] を選ぶ

[リモートUI/ツール]

リモートUIや一部のソフトウェアを使用して設定を変更するときに、管理者パスワードの入力が必要になります。

[操作パネル/リモートUI/ツール]

プリンターの操作パネルやリモートUI、一部のソフトウェアを使用して設定を変更するときに、管理者パスワードの入力が必要になります。

6.　画面のメッセージに従ってパスワードを入力し、[OK] を選ぶ

7.　完了メッセージが表示されたら、[OK] を選ぶ

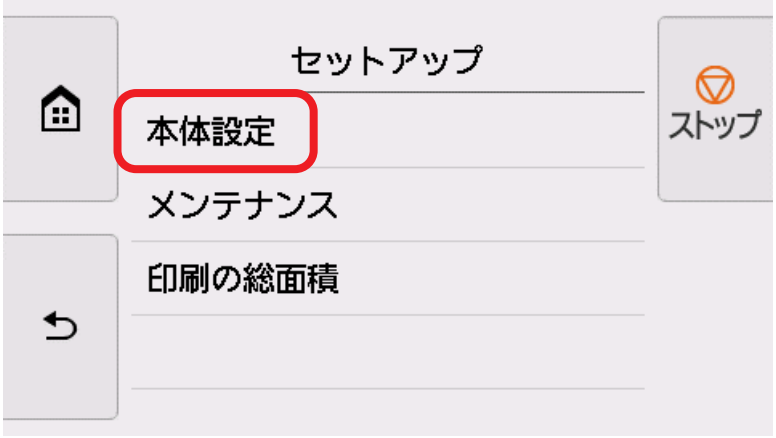
参考

► 管理者パスワードを設定したら、管理者情報を入力してください。リモートUIのトップ画面に表示されます。
管理者情報は、[本体設定] ▶ [特殊設定] ▶ [管理者情報] で入力できます。

操作パネルで管理者パスワードを変更/設定する

操作パネル

1. ホーム画面から ⚙（セットアップ）→［本体設定］を順に選ぶ



2. ［セキュリティ設定］を選ぶ

3. ［管理者パスワードの設定］を選ぶ

4. 管理者パスワードの入力画面でパスワードを入力し、［OK］を選ぶ

管理者パスワードが設定されていないときは、登録確認メッセージが表示されます。
［はい］を選んでください。
再度メッセージが表示されますので、［OK］を選んでください。

5. ［管理者パスワードの変更］を選ぶ

6. 管理者パスワードの有効範囲を選ぶ

［リモートUI/ツール］
リモートUIや一部のソフトウェアを使用して設定を変更するときに、管理者パスワードの入力が必要になります。

［操作パネル/リモートUI/ツール］
プリンターの操作パネル、リモートUIや一部のソフトウェアを使用して設定を変更するときに、管理者パスワードの入力が必要になります。

7. 管理者パスワードを入力する

8. ［確定］を選ぶ

9. 管理者パスワードを再入力する

10. ［確定］を選ぶ

管理者パスワードが有効になります。

一般ユーザーパスワードを設定する

一般ユーザー向けに機能を制限するには、以下の手順で一般ユーザーモード設定を有効にして、一般ユーザーパスワードを設定します。

リモートUI

1. リモートUIを起動する

➡ リモートUIを起動する

2. [セキュリティ] を選ぶ

3. [一般ユーザーモード設定] を選ぶ

4. 確認メッセージが表示されたら、[はい] を選ぶ

5. 画面のメッセージに従ってパスワードを入力し、[OK] を選ぶ

6. 完了メッセージが表示されたら、[OK] を選ぶ

1.3 ルート証明書を登録する

ウェブブラウザーにルート証明書を登録していない場合は、安全に通信できないことを知らせる警告が表示されることがあります。初めてリモートUIを表示した場合は、ルート証明書をダウンロードし、ウェブブラウザーに登録してください。安全に通信できることが確認され、警告が表示されなくなります。ただし、一部のブラウザーでは、ルート証明書を登録した後も警告が表示される場合があります。

SSL通信のためにプリンターのルート証明書をウェブブラウザーに登録する

ウェブブラウザーの種類やバージョンによって、ルート証明書の登録方法は異なります。本書では、Microsoft Edgeを例にして説明します。

重要

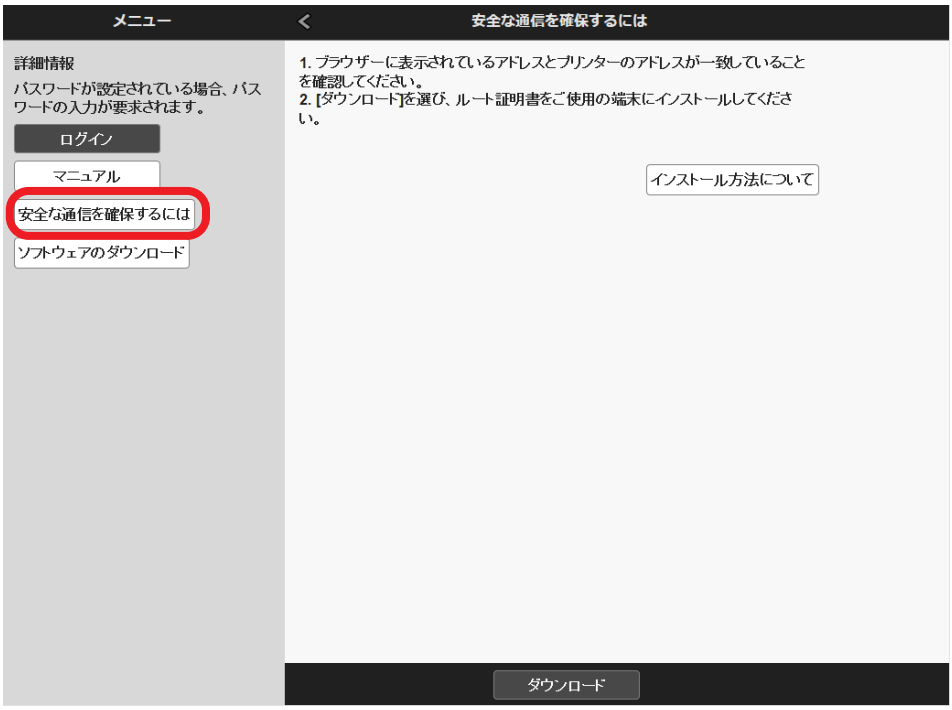
- ルート証明書を登録するときは、ウェブブラウザーのURL欄を確認し、プリンターのIPアドレスが正しいか確認してください。

リモートUI

1.　リモートUIを起動する

➡ リモートUIを起動する

2.　[安全な通信を確保するには] を選ぶ



3. ［ダウンロード］を選ぶ

ルート証明書のダウンロードが始まります。

4. ダウンロードの確認画面が表示されたら、［開く］を選ぶ

［証明書］画面が表示されます。

5. ［証明書のインストール］を選ぶ

［証明書のインポート ウィザード］画面が表示されます。

6. ［次へ］を選ぶ

7. ［証明書をすべて次のストアに配置する］を選ぶ

8. ［参照］を選ぶ

［証明書ストアの選択］画面が表示されます。

9. ［信頼されたルート証明機関］を選び、［OK］を選ぶ

10. ［証明書のインポート ウィザード］画面で［次へ］を選ぶ

11. ［証明書のインポート ウィザードの完了］が表示されたら、［完了］を選ぶ

［セキュリティ警告］画面が表示されます。

12. ［セキュリティ警告］画面の拇印欄と、プリンターのルート証明書の拇印（フィンガープリント）が一致しているか確認する

プリンターのルート証明書の拇印は、操作パネルのホーム画面から（インフォメーション）→［システム情報］を順に選び、［ルート証明書の拇印(SHA-1)］または［ルート証明書の拇印(SHA-256)］を確認してください。

13. 拇印欄と、プリンターのルート証明書の拇印（フィンガープリント）が一致している場合は、［セキュリティ警告］画面の［はい］を選ぶ

14. ［証明書のインポート ウィザード］画面で［OK］を選ぶ

ルート証明書の登録が完了します。

② ハードディスク内のデータ保護

プリンター本体のハードディスクに保存されているデータ（印刷ジョブや各種設定情報）が流出しないようにするために、個人ボックスにパスワードを設定するなどの適切なデータ保護をおすすめします。また、プリンターを長期間使用しない場合や廃棄する場合には、不正にアクセスされないように、データ消去などの処置を行ってください。

2.1 個人ボックスにパスワードを設定する

パスワードを設定すると、以下の操作を行う際に、パスワードの入力が必要になります。

- 個人ボックスの設定変更
- 個人ボックスに保存されているジョブリストの表示、印刷
- 保存されているジョブの印刷、削除、移動、ジョブ名変更

参考

- 工場出荷時には、個人ボックスにパスワードは設定されていません。
- 共通ボックスには、パスワードを設定できません。
- パスワードは、0000001から9999999までの7桁の数字を入力してください。
- パスワードを設定している場合でも、リモートUIの管理者モードでログインするときは、パスワードを入力する必要はありません。

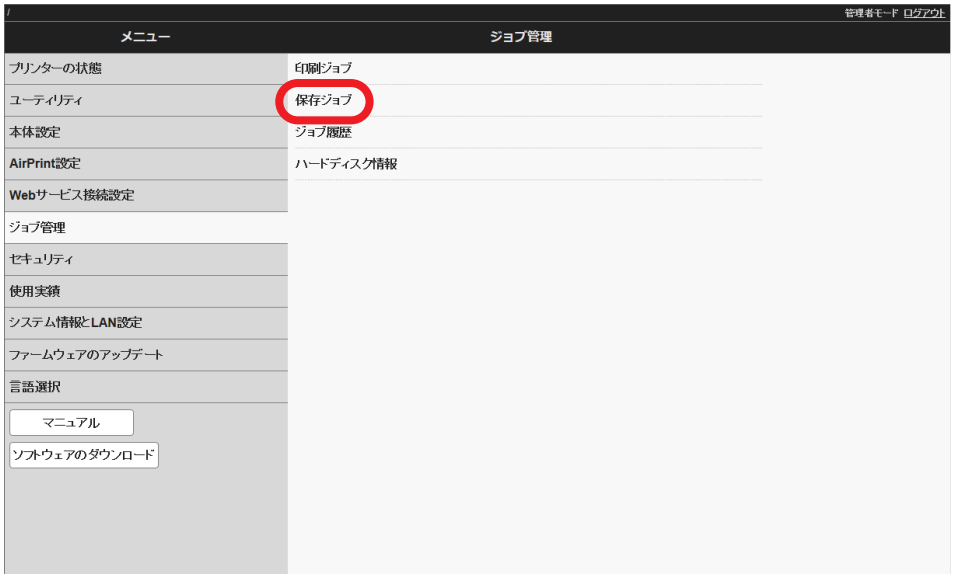
リモートUI

1. リモートUIを起動する

➡ リモートUIを起動する

2. [ジョブ管理] を選ぶ

3. **[保存ジョブ] を選ぶ**



4. **一覧で、ボックスを選ぶ**

5. **[編集] を選ぶ**

6. **[パスワードを設定/変更する] にチェックマークを付け、パスワードを入力する（7桁固定、0000001 ～ 9999999）**

7. **[OK] を選ぶ**

2.2 ハードディスク内のデータを完全消去する

プリンター内部にデータが残っていると、他者からデータにアクセスされる恐れがあります。プリンターを廃棄する場合には、データを消去してください。

なお、プリンターを修理、貸与、または譲渡するときは、プリンターの設定を初期化してください。

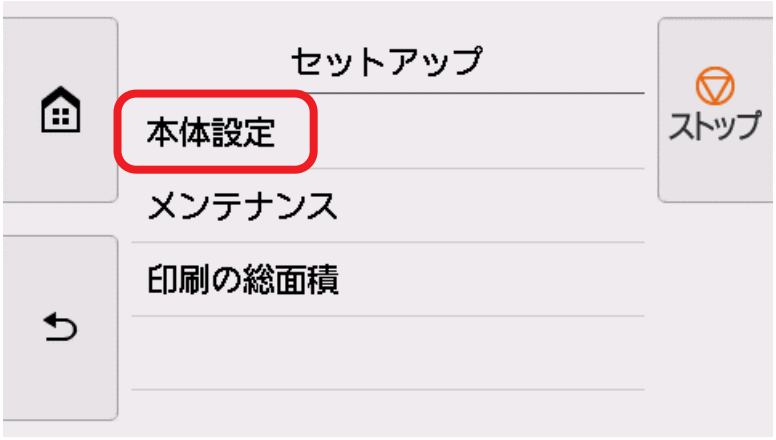
➡ 2.4 設定情報を初期化する

重要

- 操作パネルでの設定変更に管理者パスワードを設定している場合は、データの消去するときに管理者パスワードが必要です。
- より確実にデータの復元を防止するためには、ハードディスクを物理的または磁気的に破壊することをおすすめします。その場合、ハードディスクの再利用はできません。
- ジョブキューが存在する場合は、データを消去できません。また、データを消去している間は、印刷ジョブは処理されません。

操作パネル

1.　ホーム画面から ⚙（セットアップ）→［本体設定］を順に選ぶ



2.　［ハードディスク設定］を選ぶ

管理者パスワードを設定している場合は、管理者パスワードを入力します。

3.　［データ消去］を選ぶ

4.　消去方法を選ぶ

［高速］

ハードディスク内に記録されたデータのファイル管理情報が消去されます。短時間で消去したい場合に選んでください。ファイル管理情報が消去されるだけですので、データ自体は消去されません。

［セキュア高速］

ハードディスクに設定されたデータ暗号化キーが消去されます。暗号化キーを再設定することで、以前の保存データの読み出しと利用ができなくなります。

機密性の高いデータを短時間で、安全に消去したい場合に選びます。

［セキュア］

ハードディスクに設定されたデータ暗号化キーが消去されたうえで、ハードディスク全体に00/FF/ランダムデータが各１回ずつ上書きされます。

データが正しく書き込めたかどうかのベリファイチェックが行われます。

特に機密性の高いデータを消去する場合に選んでください。

上書きされたデータの復元はほぼ不可能です。

米国防総省基準（DoD5220.22-M）に準拠。

［セキュア(VSITR)］

ハードディスクに設定されたデータ暗号化キーが消去されたうえで、ハードディスク全体に00が1回書き込まれた後、FFが書き込まれます。

この作業が3回繰り返されてから、ハードディスク全体にAAが書き込まれます。

上書きされたデータの復元はほぼ不可能です。

ドイツ連邦政府機関ガイドライン（VS-ITR）に準拠。

5.　操作パネルに表示されるメッセージを確認し、［はい］を選ぶ

ハードディスク内のデータが消去されます。

2.3 ネットワーク設定を初期化する

ネットワーク設定を再度行う場合には、一度ネットワーク設定を初期化してください。ネットワーク設定の初期化はプリンターの操作パネルで行います。

操作パネル

1. **ホーム画面から  （ネットワーク）を選ぶ**

   管理者パスワードを設定している場合は、管理者パスワードを入力します。

2. **[Wi-Fi]、[無線ダイレクト]、または [有線LAN] を選ぶ**
3. **[設定] を選ぶ**
4. **[詳細設定] を選ぶ**
5. **[LAN設定リセット] を選ぶ**
6. **[はい] を選ぶ**

2.4 設定情報を初期化する

プリンターに個人情報を登録したときは、情報がプリンター内に残っています。情報の漏えいをさけるため、プリンターを修理・貸与などで一時的に手放すときや、譲渡または破棄するときは、プリンターの設定を初期化してください。

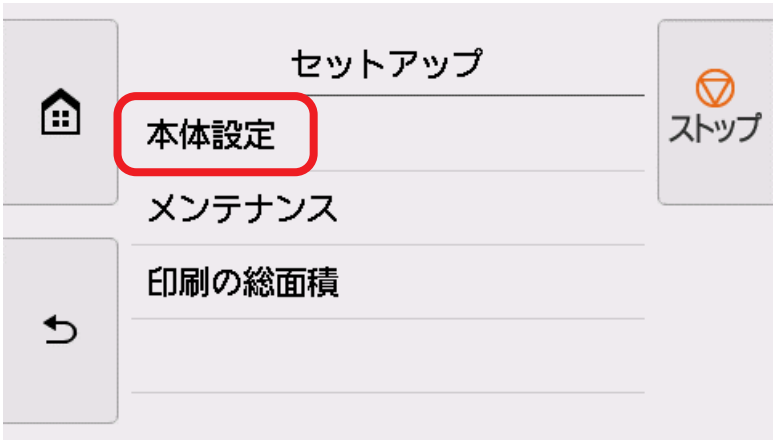
プリンターの初期化では、以下の設定が初期化されます。

- 用紙の設定情報
- 用紙の推定データ
- SSL証明書
- LAN設定
- 管理者パスワード
- ハードディスクのデータ
- ジョブ履歴
- パネルアクセスロック設定

操作パネルで初期化する

操作パネル

1.　ホーム画面から ⚙ （セットアップ）→［本体設定］を順に選ぶ



2.　［本体設定の初期化］を選ぶ

管理者パスワードを設定している場合は、管理者パスワードを入力します。

3.　操作パネルに表示されるメッセージを確認し、［はい］を選ぶ

初期化が実行されます。

リモートUIで初期化する

リモートUI

1.　リモートUIを起動する

➡ リモートUIを起動する

2.　[本体設定] を選ぶ

3.　[本体設定の初期化] を選ぶ

4.　画面のメッセージを確認し、[はい] を選ぶ

初期化が実行され、リモートUIが切断されます。

③ ネットワークセキュリティ

悪意のある第三者による通信内容の盗聴や改ざん、なりすましは正規ユーザーに想定外の損失をもたらす恐れがあります。本章では、大切なデータや情報を守るためのネットワークセキュリティについて説明します。

3.1 ポート番号の割り当て

外部機器と情報をやりとりするプロトコルには、種類ごとに決まったポート番号が割り当てられています。ファイアウォールによりポートがブロックされているとプリンターの動作に影響がありますのでご注意ください。

◆TCP

プロトコル	ポート	初期値	用途と影響
LPD	515	ON	LPR印刷に使用します。 OFFにするとLPR印刷ができなくなります。
RAW	9100	ON	RAW印刷に使用します。 OFFにするとRAW印刷ができなくなります。
CPCA	9007	ON	キヤノンの統一制御コマンド群であるCPCA（Common Peripheral Controlling Architecture）の通信に使用します。 OFFにすると製品の詳細設定や参照ができなくなります。
HTTP	80	-	パソコンとプリンター間の印刷や情報取得に使用します。このポートをブロックしないでください。
HTTPS	443	-	パソコンとプリンター間の情報取得に使用します。このポートをブロックしないでください。
IPP	631	ON	IPP印刷に使用します。
IPPS	631	ON	IPPのセキュア印刷に使用します。
FTP	20	OFF	FTP印刷のデータ転送に使用します。 OFFにするとFTP印刷ができなくなります。
FTP	21	OFF	FTP印刷の制御に使用します。

◆UDP

プロトコル	ポート	初期値	用途と影響
SNMP	161	v1: ON v3: ON	簡易ネットワーク管理プロトコルの通信に使用します。 OFFするとWindows、Macプリンタードライバーへのステータス応答ができなくなります。 ・管理系アプリ、Media Configuration Toolによる管理ができなくなります。 ・「PC/スマホで簡単接続」ができなくなります。
CPCA	47545	ON	キヤノンの統一制御コマンド群であるCPCA（Common Peripheral Controlling Architecture）の通信に使用します。 OFFにすると本製品の詳細情報の設定や参照ができなくなります。
WSD	3702	OFF	WSDのデバイス検出（WS-Discovery）に使用します。 OFFの場合WSDを用いた印刷ができなくなります。
mDNS	5353	ON	Bonjourに使用します。OFFにするとBonjourが使用できなくなります。
LLMNR	5355	ON	LLMNRによる名前解決要求に使用します。 OFFにするとLLMNRによる名前解決要求に応答できなくなります。
IKEv1	500	OFF	IKEv1による鍵交換に使用します。OFFにするとIPsecが使用できなくなります。
DHCP Client	68	ON	OFFにするとDHCP以外のプロトコルでIPアドレスを割り当てるか、手動でIPアドレスを設定する必要があります。
DHCPv6 Client	546	ON	IPv6アドレスを自動に割り当てる際に使用します。 OFFにするとDHCP以外から取得したアドレスを使う必要があります。
SNTP Client	123	OFF	ネットワーク経由で自動的にプリンターの時刻を合わせる際に使用します。 OFFにすると、プリンターの時刻ずれを手動で修正する必要があります。

3.2 インターフェースを有効/無効にする

有線LAN接続は、Wi-Fi接続または無線ダイレクト接続と同時に使用することはできません。

Wi-Fi接続の有効/無効

操作パネル

（ネットワーク）▶［Wi-Fi］▶［設定］▶［Wi-Fiの有効/無効］

リモートUI

［システム情報とLAN設定］▶［LAN設定］▶［Wi-Fi］▶［はい］▶［Wi-Fiの有効/無効］

無線ダイレクト接続の有効/無効

操作パネル

（ネットワーク）▶［無線ダイレクト］▶［設定］▶［無線ダイレクトの有効/無効］

リモートUI

［システム情報とLAN設定］▶［LAN設定］▶［無線ダイレクト］▶［はい］▶
［無線ダイレクトの有効/無効］

有線LAN接続の有効/無効

操作パネル

（ネットワーク）▶［有線LAN］▶［設定］▶［有線LANの有効/無効］

リモートUI

［システム情報とLAN設定］▶［LAN設定］▶［有線LAN］▶［はい］▶［有線LANの有効/無効］

USB接続を使用する/使用しない

操作パネル

（セットアップ）▶［本体設定］▶［その他の本体設定］▶［USB接続の使用］

3.3 通信プロトコルを有効/無効にする

WSD、Bonjour、LPR、RAW、IPP、FTP、SNMPなど、通信プロトコルの利用を有効または無効に設定できます。プリンターの操作パネルまたはリモートUIで設定してください。リモートUIからのアクセスは、「リモートUIを起動する」をご参照ください。

WSD/Bonjour/IPP

操作パネル

（ネットワーク）▶［Wi-Fi］、［無線ダイレクト］、または［有線LAN］を選ぶ▶［設定］▶［詳細設定］

リモートUI

［システム情報とLAN設定］▶［LAN設定］▶［詳細設定］▶［はい］

LPR/LLMNR/RAW

操作パネル

（ネットワーク）▶［Wi-Fi］、［無線ダイレクト］、または［有線LAN］を選ぶ▶［設定］▶［詳細設定］

リモートUI

［システム情報とLAN設定］▶［LAN設定］▶［詳細設定］▶［はい］▶［LPD印刷］

SNMP/FTP

リモートUI

［システム情報とLAN設定］▶［LAN設定］▶［詳細設定］▶［はい］

CPCA

操作パネル

（ネットワーク）▶［Wi-Fi］、［無線ダイレクト］、または［有線LAN］を選ぶ▶［設定］▶［詳細設定］▶［専用ポート設定］

3.4 フィルタリングで通信制限する

パソコンや大判プリンターを含む通信機器を、適切なセキュリティ対策を施さずにネットワークに接続すると、意図しない第三者から不正にアクセスされる恐れがあります。

大判プリンターにおいては、特定のIPアドレスやMACアドレスを持つ機器だけに通信を許可するパケットフィルタリングを設定することで、リスクを低減させます。リモートUIで設定してください。リモートUIからのアクセスは、「リモートUIを起動する」をご参照ください。

重要

- MACアドレスフィルタリングは有線接続のみで有効です。無線接続では設定できません。

IPフィルタリング

リモートUI

［システム情報とLAN設定］▶［LAN設定］▶［詳細設定］▶［はい］▶［IPフィルタリング］

MACアドレスフィルタリング

リモートUI

［システム情報とLAN設定］▶［LAN設定］▶［詳細設定］▶［はい］▶
［MACアドレスフィルタリング設定］

3.5 通信の暗号化：SSL/TLS

プリンターがサーバーとして動作する通信（HTTP/IPPなど）のセキュリティを高めたい場合に設定します。暗号化通信では、証明書と鍵のペアを使用します。

サーバー認証の例：

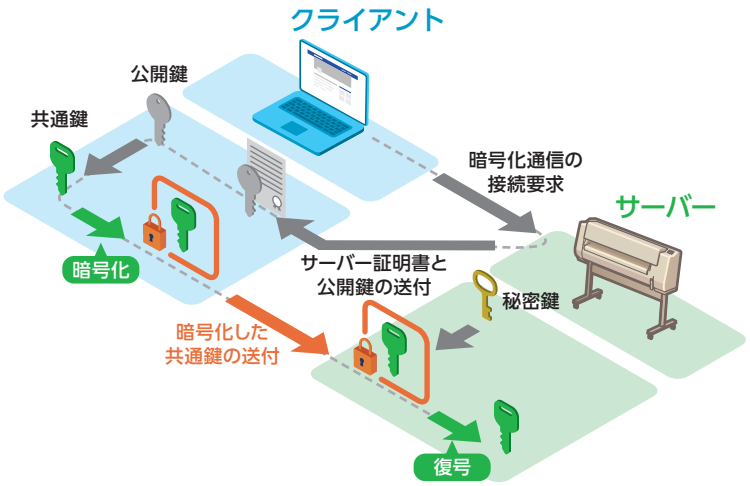
サーバー（プリンター）―クライアント（パソコン）間の通信は、以下のように行われます。

（1）【クライアント】暗号化通信の接続要求をする

（2）【サーバー】サーバー証明書と公開鍵のペアを送付する

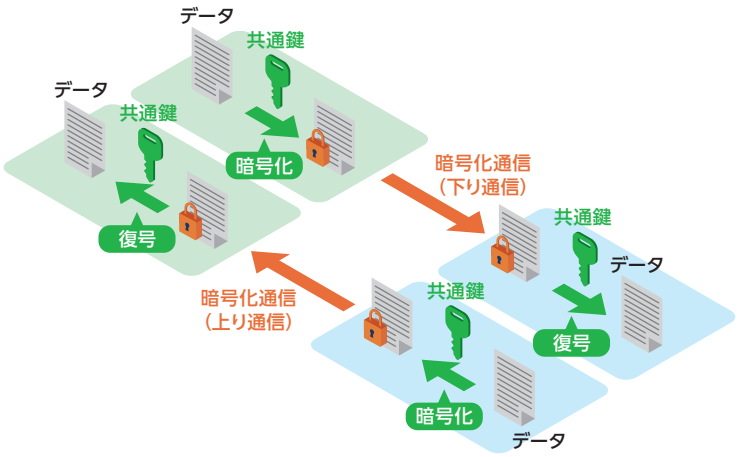
（3）【クライアント】共通鍵を生成する

（4）【クライアント】受け取った公開鍵を使って共通鍵を暗号化しサーバー（プリンター）へ送付する



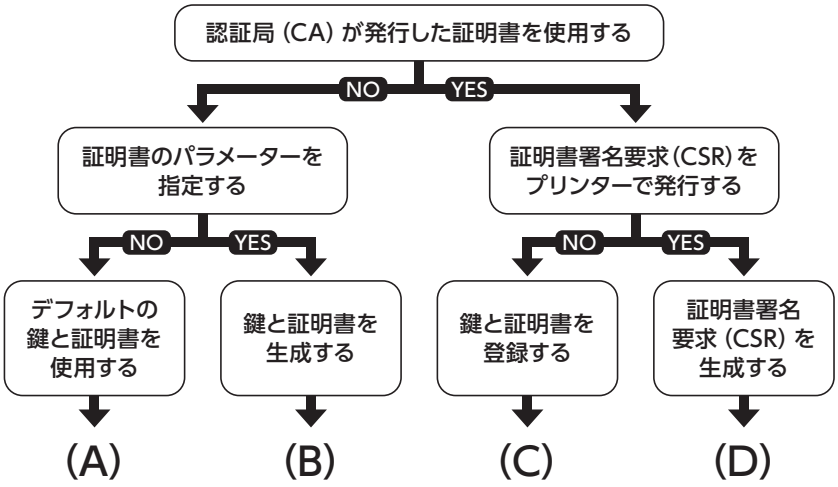
（5）【サーバー】受け取った共通鍵を秘密鍵で復号する

（6）【クライアント/サーバー】一致した共通鍵を使って送受信するデータ経路を暗号化/復号して暗号化通信を成立させる



キヤノン製大判プリンターでは、プリンターがSSL/TLSサーバーとして動作するリモートUI通信およびIPP通信において、TLS暗号化通信を行うためにプリンター内の鍵と証明書（サーバー証明書）を使用します。サーバー証明書はプリンター内のデフォルト証明書の他、ユーザーがリモートUIを利用して生成した証明書および外部で作成した証明書が使用できます。

SSL/TLS通信用の電子証明書の登録パターンは以下のようになります。いずれかの登録パターンを選んでください。



(A)　［デフォルトの鍵と証明書を使用する］場合：

プリンター内にあらかじめ用意されたデフォルトの鍵と証明書を使用できます。
この場合、リモートUIを使用して鍵と証明書を登録する必要はありません。

(B)　［鍵と証明書を生成する］場合：

共通名や有効期間などに自分で設定した情報を入れた証明書を使いたい場合、リモートUIを利用して新たに鍵と証明書を生成できます。

リモートUI

［セキュリティ］▶［TLSサーバー設定］▶［鍵と証明書の生成］▶［自己署名証明書の生成］

1. 必要事項を設定する
   - 署名アルゴリズムおよび鍵情報を指定します。
   - 有効期限：
     ［有効期間の開始］には、サーバー証明書を作成する日を入力します。
     ［有効期間の終了］には、サーバー証明書の使用を終了する日を入力します。
   - 共通名：英数字を入力します。
2. ［次へ］を選ぶ
   - ［国］、［都道府県］、［市区町村］、［組織］、［組織単位］は任意入力です。
   - ［サブジェクトの別名］には、［共通名］と同じ内容を入力してください。
3. ［生成］を選ぶ
   - サーバー証明書の生成が開始されます。
4. ［LANの再起動］を選ぶ
   - LANが再起動します。

プリンターで生成したルート証明書で署名したサーバー証明書を作成します。
ただし、ウェブブラウザーの種類やバージョンによっては、安全な通信ができないことをお知らせする警告が表示される場合があります。

(C)　[鍵と証明書を登録する]（外部で作成した証明書を使う）場合：

鍵と証明書やCA証明書を発行機関から入手して使用できます。入手した鍵と証明書ファイルはリモートUIを使ってアップロードします。

［セキュリティ］▶［TLSサーバー設定］▶［鍵と証明書のアップロード］

1. ファイル形式を選ぶ
   ［PKCS#12］または［DER］を選びます。
2. ファイルを選び、パスワードを入力する
3. ［アップロード］ボタンを選ぶ
4. 管理者パスワードの入力を求められた場合は管理者パスワードを入力する
5. ［LANの再起動］ボタンを選ぶ

(D)　[証明書署名要求（CSR）を生成する]場合：

プリンターで生成した証明書は認証局に署名されていないため、接続機器によっては通信エラーとなってしまうことがあります。

認証局署名付き証明書を入手するには、証明書署名要求（CSR：Certificate Signing Request）ファイルを認証局に送付して証明書を発行してもらう必要があります。

CSRは、管理者モードのリモートUIを使って生成します。証明書が発行されたら、リモートUIから証明書をアップロードしてください。

［セキュリティ］▶［TLSサーバー設定］▶［鍵と証明書の生成］▶
［CSR(証明書署名要求)の生成］

「すでに生成されたCSRがあります。生成の操作を行うと既存のCSRは削除されます。生成しますか？」が表示された場合、［はい］を選びます。

1. 必要事項を設定する
   - 署名アルゴリズムおよび鍵情報を指定します。
   - 共通名
2. ［次へ］を選ぶ
   - ［国］、［都道府県］、［市区町村］、［組織］、［組織単位］は任意入力です。
3. ［生成］を選ぶ
4. ［ダウンロード］を選ぶ
5. 保存先を指定して保存する

保存したCSRファイルは認証局に送付し、認証局署名付き証明書（CA証明書）の発行を受けます。

CA証明書は（C）の手順に従って、アップロードします。

重要

- 生成したサーバー証明書をリセットするには、操作パネルのホーム画面で以下の設定をしてください。

操作パネル

（ネットワーク）▶［Wi-Fi］、［無線ダイレクト］、または［有線LAN］▶［設定］▶［詳細設定］▶［SSL証明書のリセット］

参考

- LANを再起動した後にリモートUIに接続できない場合は、ウェブブラウザーでページを再読み込みしてください。
- 必要に応じて、暗号化通信に使用するTLSのバージョン範囲や使用するアルゴリズムなどを設定してください。この設定は、プリンターがTLSサーバーとして動作する場合に適用されます。

リモートUI

［セキュリティ］▶［TLSサーバー設定］▶［TLSの詳細設定］

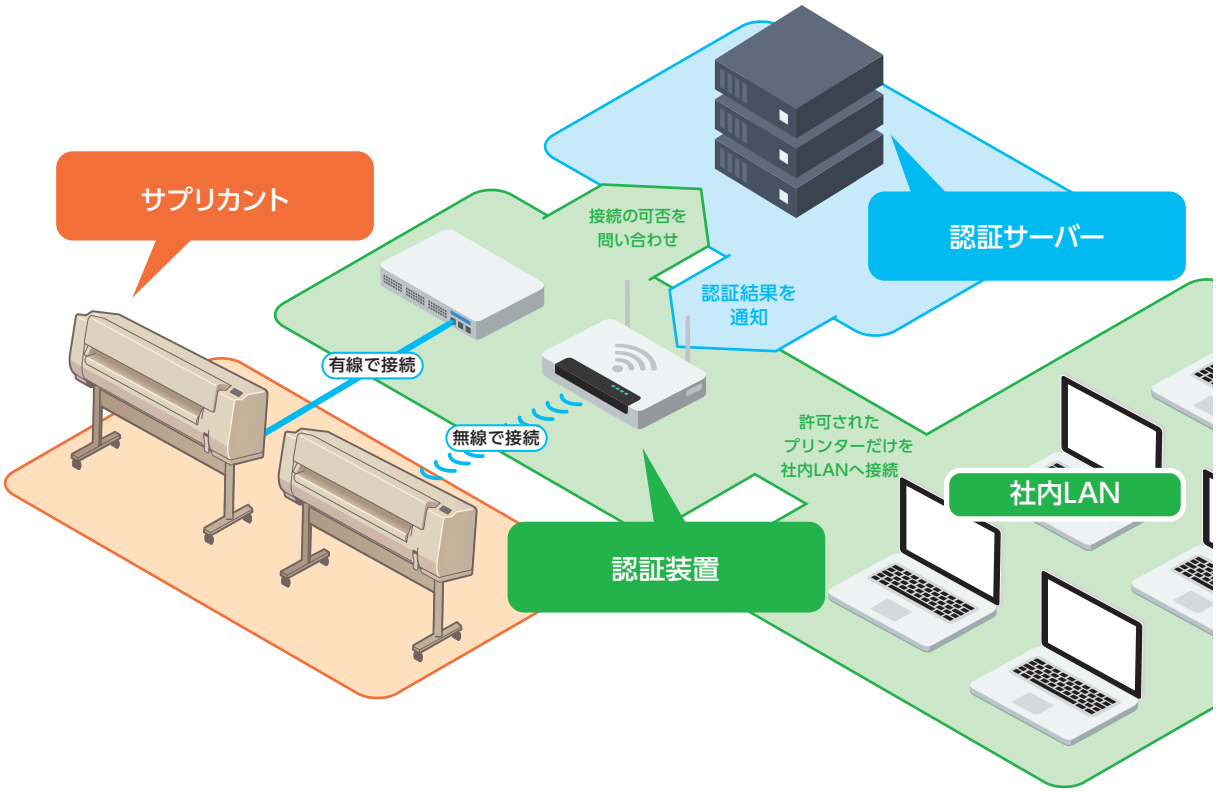
暗号化通信で利用できる鍵と証明書の仕様

➡ 4.3 登録可能な鍵と証明書のアルゴリズムおよびフォーマット

3.6 IEEE802.1X/EAP設定

IEEE802.1XはLAN標準規格の１つであり、ネットワーク上の通信制御機器を認証装置としてクライアントを認証する認証規格です。認証のために以下の３つの要素を必要とします。

- サプリカント
- 認証サーバー
- 認証装置



ネットワークに接続する機器にインストールされたサプリカントは、認証サーバーに認証情報を送信します。認証サーバーは、受け取った認証情報を照会し、ネットワークへの接続を許可するかどうかを判断します。認証装置は、認証サーバーが判断した結果に基づいて、ネットワークに接続する機器のアクセスを制御します。サプリカント、認証サーバー、認証装置の3つが連携することで、ネットワーク接続の認証を行います。このようなネットワークにプリンターはサプリカントとして接続できます。

[IEEE802.1Xの認証方式]

- EAP-TLS
  プリンターと認証サーバーがそれぞれの証明書を使って互いに認証を行います。プリンターによるサーバー認証にはCA証明書を使用します。サーバーによるプリンター（クライアント）の認証には認証局発行の鍵とクライアント証明書が必要です。工場出荷状態で、プリンター内にクライアント証明書は搭載していません。
- EAP-TTLS
  プリンターの認証にユーザー名とパスワードを使用し、サーバー認証にはCA証明書を使用する認証方式です。内部プロトコルとしてMSCHAPv2またはPAPを選べます。
- PEAP
  必要な設定はTTLSとほぼ同じですが、内部プロトコルにはMSCHAPv2を使用します。

IEEE802.1X/EAPの設定をする

1.　IEEE802.1X/EAPを有効にする

次の手順で[IEEE802.1X/EAPの有効/無効]を[有効]に設定し、[OK] を選びます。

リモートUI

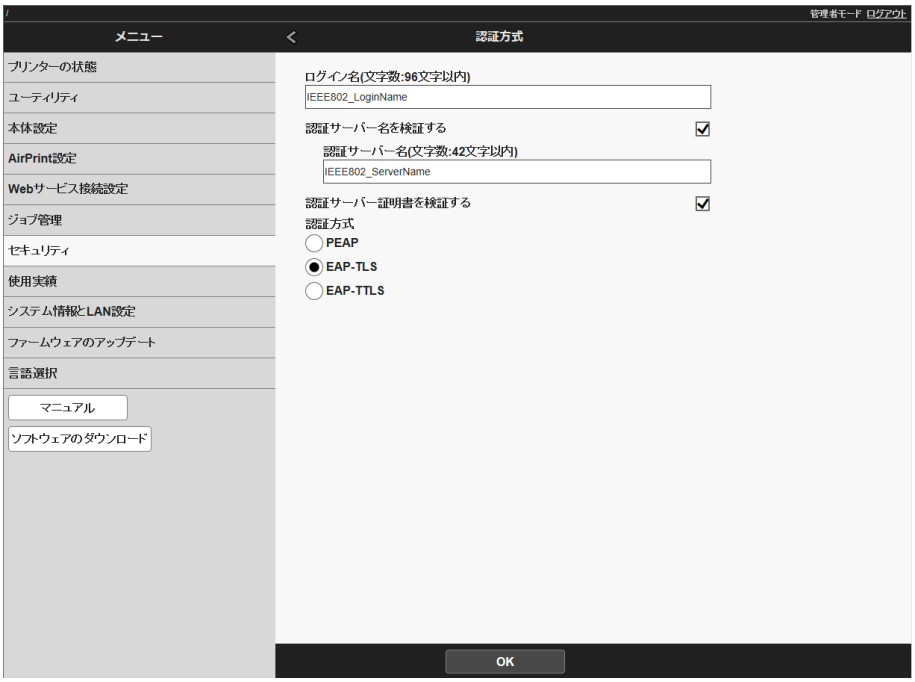
[セキュリティ] ▶ [IEEE802.1X/EAP設定] ▶ [IEEE802.1X/EAPの有効/無効]

2.　ログイン名、認証サーバー名などを設定する

リモートUI

[セキュリティ] ▶ [IEEE802.1X/EAP設定] ▶ [認証方式]

[認証方式] を選ぶと、次の設定画面が表示されます。



・ ログイン名
　ネットワーク接続に使用するログイン名を96文字以内で設定します。

・ 認証サーバー名を検証する
　チェックボックスでオンまたはオフを設定します。既定値はオンです。

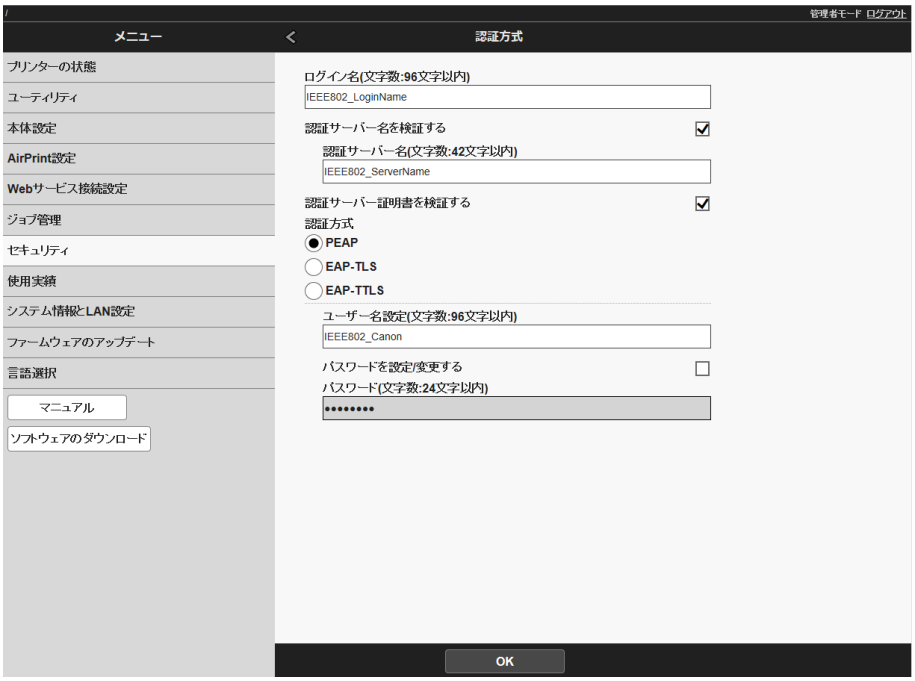
・ 認証サーバー名
　[認証サーバー名を検証する] がオンの場合に、認証サーバー名を半角英数字42文字以内で設定します。

・ 認証サーバー証明書を検証する
　チェックボックスでオンまたはオフを設定します。既定値はオンです。
　オンを選んだ場合、別途CA証明書の登録が必要になります。
　➡ CA証明書を登録する

3.　認証方式を設定する

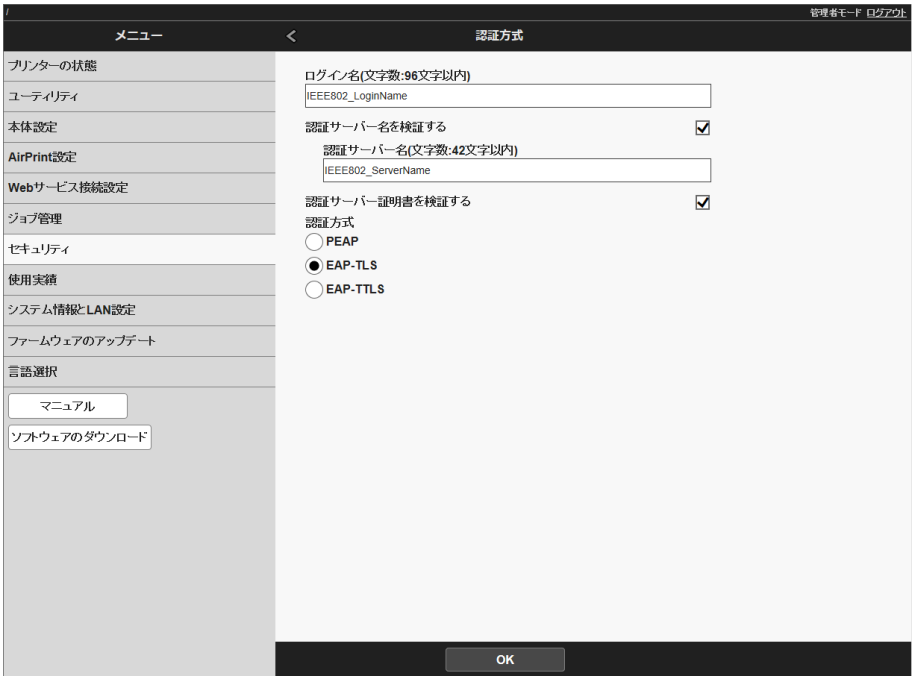
[PEAP] / [EAP-TLS] / [EAP-TTLS] から選びます。既定値は [EAP-TLS] です。
選んだ認証方式に従って、以下の追加の設定項目があります。

PEAPを選んだ場合



- ユーザー名設定
  ネットワーク接続の認証に使用されるユーザー名を96文字以内で設定します。
- パスワード
  認証に使用されるパスワードを24文字以内で設定します。

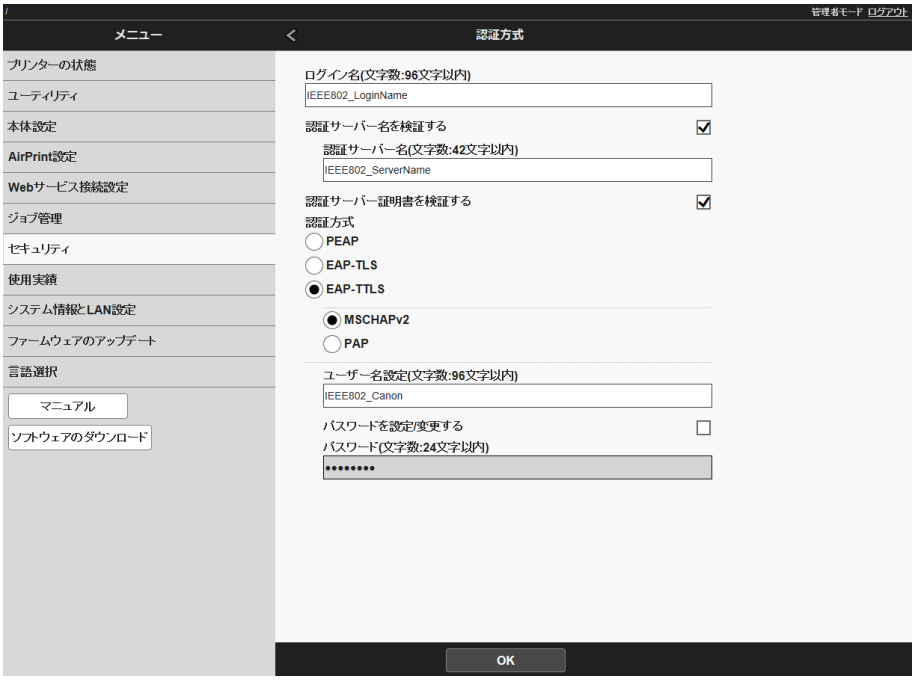
EAP-TLSを選んだ場合



別途クライアント証明書の登録が必要になります。

➡ クライアント証明書を登録する

EAP-TTLSを選んだ場合



- 認証に使用される内部プロトコル
  [MSCHAPv2] / [PAP] から選びます。既定値は [MSCHAPv2] です。
- ユーザー名設定
  ネットワーク接続の認証に使用されるユーザー名を96文字以内で設定します。
- パスワード
  認証に使用されるパスワードを24文字以内で設定します。

4.　[OK] を選ぶ

証明書を登録する

1.　クライアント証明書を登録する

認証方式にEAP-TLSを選んだ場合、認証局発行の鍵とクライアント証明書をリモートUIからアップロード（登録）する必要があります。

［セキュリティ］▶［IEEE802.1X/EAP設定］▶［鍵と証明書の設定］▶
［鍵と証明書のアップロード］

2.　CA証明書を登録する

認証サーバー証明書を検証する：オンを選択、CA証明書の登録が必要になります。リモートUIからアップロード（登録）してください。

［セキュリティ］▶［IEEE802.1X/EAP設定］▶［CA証明書］▶［CA証明書のアップロード］

なお各認証方式において、サーバーの証明書の検証をしない設定もできます。この場合はCA証明書のアップロードは不要です。

［セキュリティ］▶［IEEE802.1X/EAP設定］▶［認証方式］▶
［認証サーバー証明書を検証する］のチェックを外す

- LANを再起動した後にリモートUIに接続できない場合は、ウェブブラウザーでページを再読み込みしてください。

暗号化通信で利用できる鍵と証明書の仕様

➡ 4.3　登録可能な鍵と証明書のアルゴリズムおよびフォーマット

3.7 通信の暗号化：IPsec

IP Security Protocol（IPsec）はインターネットなどのネットワークで暗号化通信をするためのプロトコルです。TLS暗号化通信がウェブブラウザーや電子メールクライアントなど、特定のアプリケーションで暗号化する技術であるのに対し、IPsec通信はIPプロトコルのレベルで暗号化を行うため、より汎用性の高いセキュリティを実現できます。IPアドレス設定がIPv6のときのみ対応しています。IPv4は非対応です。

IPsec設定

（ネットワーク）▶［Wi-Fi］、［無線ダイレクト］、または［有線LAN］を選ぶ ▶ ［設定］▶ ［詳細設定］▶ ［TCP/IP設定］▶ ［IPv6］▶ ［IPsec設定］▶ ［有効］または［無効］を選ぶ

◆IPsecサポートプロトコル一覧

- IPv6IPsec
- AH
  - HMAC-SHA-256-128　*1
  - HMAC-SHA-1-96
  - HMAC-MD5-96　*2
- ESP
  - DES-CBC　*2
  - 3DES-CBC
  - AES-CBC（※128、192、256bitの3種類の鍵長をサポート）

◆IKEサポートプロトコル一覧

- IKEv1
- IKEv1 Phase1
  - メインモード
- 認証方式（IKEv1）
  - 事前共有鍵（１６文字以下の半角英数字）
- DH鍵（IKEv1）
  - グループ1　*2
  - グループ2　*2
  - グループ5
  - グループ14
- 暗号（IKEv1）
  - DES-CBC　*2
  - 3DES-CBC
  - AES-CBC（※128、192、256bitの3種類の鍵長をサポート）
- ハッシュ（IKEv1）
  - SHA-256　*1
  - SHA-1　*2
  - MD-5　*2

*1　下記モデルのみ
imagePROGRAF TM-355/TM-255/TM-350/TM-250/TM-340/TM-240
imagePROGRAF TM-5355/TM-5255/TM-5350/TM-5250/TM-5340/TM-5240

*2　上記以外のモデルのみ

4 付録

プリンターのファームウェアのアップデート方法とシリアルナンバーの確認方法を説明します。

4.1 ファームウェアをアップデートする

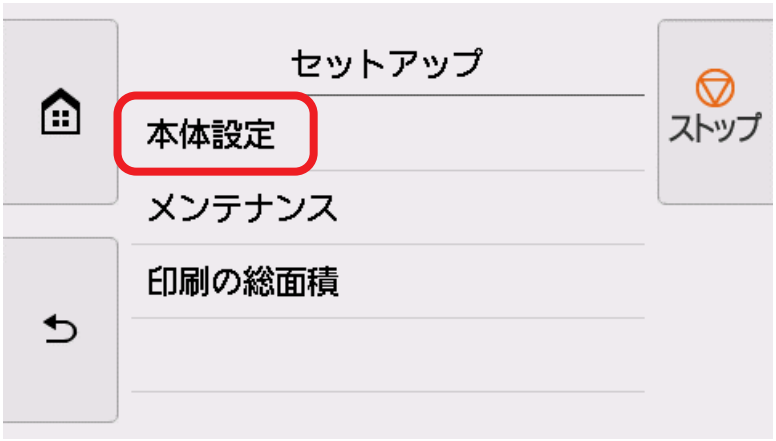
新しいファームウェアがリリースされた場合は、リモートUIに表示されます。セキュリティ機能が改善されていることがありますので、常に最新のファームウェアにアップデートしてください。操作パネルまたはリモートUIから実行します。

重要

- ファームウェアのアップデートを行う前に、プリンターがインターネットに接続されていることを確認してください。
- 管理者パスワードが設定されている場合は、ファームウェアをアップデートする際に管理者パスワードの入力が必要です。

操作パネルでファームウェアをアップデートする

1. ホーム画面から ⚙（セットアップ）→［本体設定］を順に選ぶ



2. ［ファームウェアのアップデート］を選ぶ

管理者パスワードを設定している場合は、管理者パスワードを入力してください。

3. ［アップデートの実行］を選ぶ

4. ［はい］を選ぶ

5. 操作パネルに表示されるメッセージを確認し、［アップデート開始］を選ぶ

リモートUIでファームウェアをアップデートする

1. リモートUIを起動する

➡ リモートUIを起動する

2. ［ファームウェアのアップデート］を選ぶ

3. ［アップデートの実行］を選ぶ

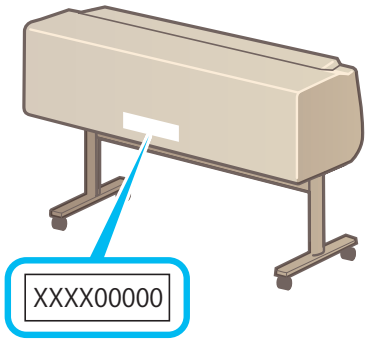
4. 画面のメッセージを確認し、［アップデート］を選ぶ

参考

► アップデートに失敗したときは、Wi-Fiルーターなど、ネットワークの設定を確認してください。

4.2 プリンターのシリアルナンバーを確認する

プリンターのシリアルナンバーは9文字（前半4文字がアルファベット、後半5文字が数字）で、本体のシールに記載されています。



参考

► プリンターのシリアルナンバーは、保証書にも記載されています。

4.3 登録可能な鍵と証明書のアルゴリズムおよびフォーマット

項目	内容
RSA 署名アルゴリズム	SHA-256
RSA 公開鍵アルゴリズム（鍵長）	RSA（2048bits）
DSA 署名アルゴリズム	非サポート
DSA 公開鍵アルゴリズム（鍵長）	非サポート
ECDSA 署名アルゴリズム	SHA-256
ECDSA 公開鍵アルゴリズム（鍵長）	ECDSA（P256/P384/P521）
証明書フォーマット	PKCS#12 形式 X.509 DER 形式 （EAP-TLSで使う鍵ペアはPKCS#12形式のみ、CA証明書はX.509 DER 形式のみ）
拡張子	PKCS#12 形式：p12/pfx X.509 DER 形式：cer/der
登録可能数	鍵／証明書：2個（TLS用サーバー証明書、IEEE802.1X用クライアント証明書） CA証明書：5個（IEEE802.1X用、ただし、欄外に記載の機種では1個）
証明書のファイルサイズ上限	・ TLS用サーバー証明書：4kB/個、秘密鍵：4kB/個 （ただし、欄外に記載の機種では、証明書：1.5kB/個、秘密鍵：2.5kB/個） ・ IEEE802.1X用クライアント証明書：4kB/個、秘密鍵：4kB/個 （ただし、欄外に記載の機種では、証明書：2kB/個、秘密鍵：2kB/個） ・ CA証明書（IEEE802.1X用）：4kB/個 （ただし、欄外に記載の機種では2kB/個）

[機種名]
・ imagePROGRAF TA-30/TA-20
・ imagePROGRAF TA-5300/TA-5200
・ imagePROGRAF TM-305/TM-300/TM-205/TM-200
・ imagePROGRAF TM-5305/TM-5300/TM-5205/TM-5200
・ imagePROGRAF PRO-6000/PRO-4000/PRO-2000/PRO-6000S/PRO-4000S
・ imagePROGRAF PRO-560/PRO-540/PRO-520/PRO-560S/PRO-540S
・ ファームウェアバージョンV1.39以前のimagePROGRAF TX-4000/TX-3000/TX-2000
・ ファームウェアバージョンV1.39以前のimagePROGRAF TX-5400/TX-5300/TX-5200