imagePROGRAF シリーズ、PIXUS/MAXIFY シリーズ用

RSA 鍵生成に関する脆弱性対応について - 鍵の確認／対応手順

第 1 版

© CANON INC. 2022

目次

1 はじめに 3

2 リモート UI の起動 4

3 ファームウェアアップデート 6

4 SSL/TLS 通信用の電子証明書の再登録 7

5 ルート証明書の登録 10

1　はじめに

本書では RSA 鍵生成に関する脆弱性対応について、ファームウェアアップデートと電子証明書再登録の手順を説明しています。

本書の手順：

以下の順で説明します。

・リモートUIの起動

・ファームウェアアップデート

・SSL/TLS通信用の電子証明書の再登録

・ルート証明書の登録

お使いの機種により、本書に掲載の画面と異なることがあります。各画面の詳細については、オンラインマニュアルサイトでお使いの機種のマニュアルをご覧ください。　https://ij.start.canon

商標について

Microsoftは、Microsoft Corporationの登録商標です。

Windowsは、米国Microsoft Corporationの米国およびその他の国における登録商標または商標です。

Microsoft Edgeは、米国Microsoft Corporationの米国およびその他の国における登録商標または商標です。

2　リモート UI の起動

リモートUI を使って、ネットワーク経由でファームウェアアップデートができます。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。

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。

操作パネル

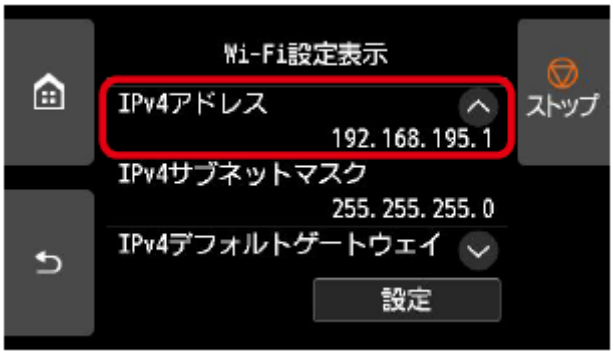
1．プリンターのIPアドレスを確認する

(1) ホーム画面から［LAN設定］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



重要

お使いの機種により、プリンターの IP アドレスの確認方法が上記と異なることがあります。詳細については、オンラインマニュアルサイトでお使いの機種のマニュアルをご覧ください。　https://ij.start.canon

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。

3．［ログイン］を選ぶ

パスワード認証画面が表示されます。

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。

3　ファームウェアアップデート

リモート UI を起動したら、続いてファームウェアをアップデートします。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ますので、最新のファームウェアにアップデートしてください。

リモートUIでファームウェアをアップデートする

1．［ファームウェアのアップデート］を選ぶ

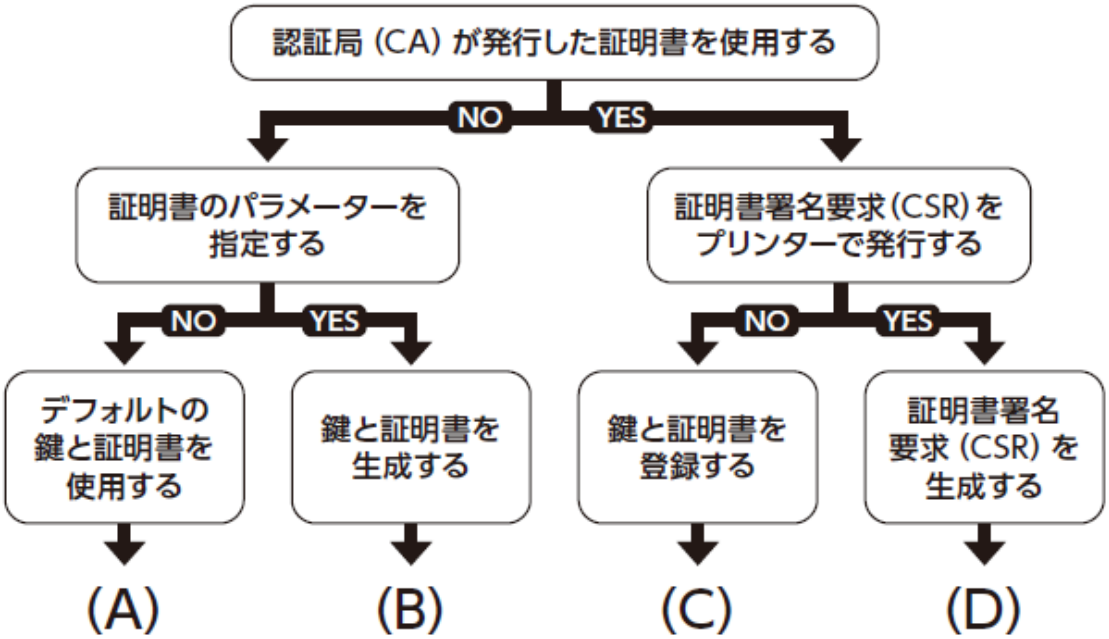
2．［アップデートの実行］を選ぶ

3．画面のメッセージを確認し、［アップデート］を選ぶ

4　SSL/TLS 通信用の電子証明書の再登録

ファームウェアアップデートが完了したら、必要に応じて SSL/TLS 通信用の電子証明書の再登録をします。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。どの登録パターンに該当するか確認してください。

SSL/TLS通信用の電子証明書の登録パターン：



SSL/TLS 通信用の電子証明書の登録パターンを確認したら、登録パターンに応じた設定をします。

（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、鍵と証明書の再登録は必要ありません。

最後にブラウザーにルート証明書をインストールします。⇒ルート証明書の登録

（B）　［鍵と証明書を生成する］場合：

あらかじめ鍵と証明書の削除が必要です。以下の手順に従って削除してから生成してください。

１．鍵と証明書を削除する

操作：［セキュリティ］＞［SSL/TLS設定］＞［鍵と証明書の削除］

表示されている鍵と証明書を削除してください。

２．鍵と証明書を生成する

操作：［セキュリティ］＞［SSL/TLS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：［SHA256］、［SHA384］、［SHA512］のいずれかを選びます。
- 公開鍵ビット長：［2048bit］を選びます。
- 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
- ［生成］を選ぶ：サーバー証明書の生成が開始されます。
- ［LANの再起動］を選ぶ

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。

最後にブラウザーにルート証明書をインストールします。⇒ルート証明書の登録

（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：

ファームアップデート前の鍵と証明書ファイルが引き続き使用できますので、ファームアップデート後に必要な作業はありません。ブラウザーへのルート証明書インストールも不要です。

（D） ［証明書署名要求（CSR）を生成する］場合：

あらかじめ鍵と証明書の削除が必要です。以下の手順に従って削除してから生成してください。

１．鍵と証明書を削除する

操作：［セキュリティ］＞［SSL/TLS設定］＞［鍵と証明書の削除］

表示されている鍵と証明書を削除してください。

２．鍵と証明書を生成する

操作：［セキュリティ］＞［SSL/TLS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］を選ぶ

(1) 必要事項を設定する

・ 署名アルゴリズム：［SHA256］、［SHA384］、［SHA512］のいずれかを選びます。

・ 公開鍵ビット長：［2048bit］を選びます。

・ 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

・ ［生成］を選ぶ

・ ［ダウンロード］を選ぶ

・ 保存先を指定して保存します

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の発行を受けます。

３．証明書をアップロードする

操作：［セキュリティ］＞［SSL/TLS設定］＞［鍵と証明書のアップロード］

認証局署名付き証明書を以下の手順に従って、アップロードします。

(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

ブラウザーへのルート証明書インストールは不要です。必要な作業は以上です。

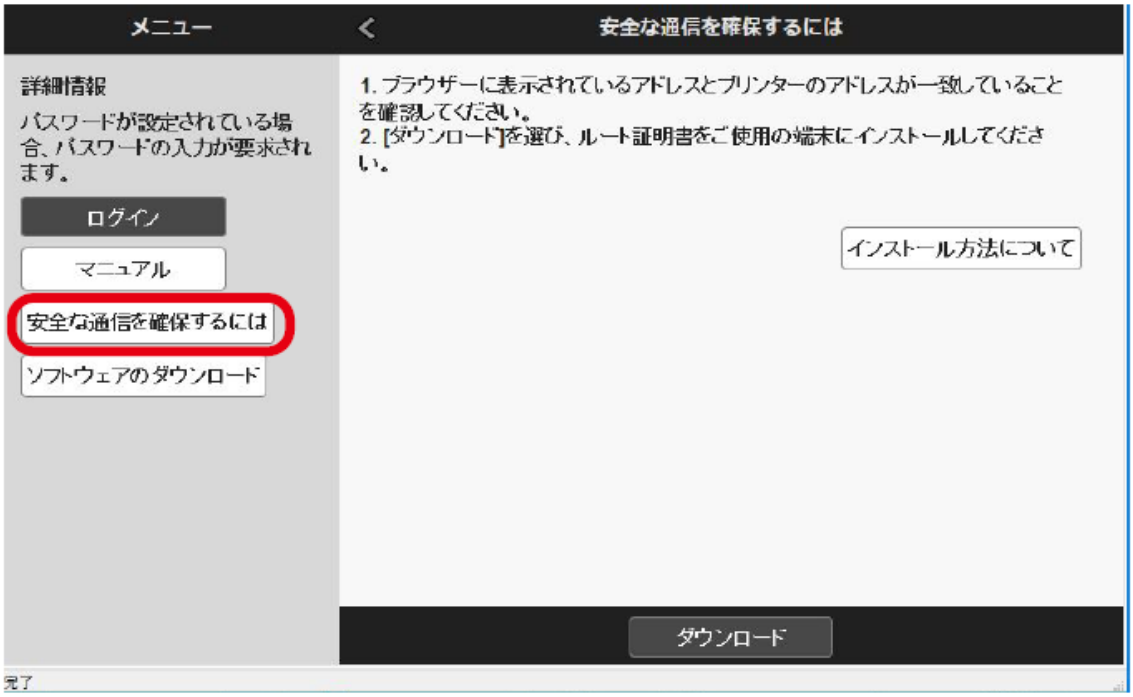
5　ルート証明書の登録

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。

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。

リモートUI

1．［安全な通信を確保するには］を選ぶ



2．［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。

3．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。

4．［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。

5．［次へ］を選ぶ

６．［証明書をすべて次のストアに配置する］を選ぶ

７．［参照］を選ぶ

［証明書ストアの選択］画面が表示されます。

８．［信頼されたルート証明機関］を選び、［OK］を選ぶ

９．［証明書のインポート ウィザード］画面で［次へ］を選ぶ

１０．［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。

１１．［セキュリティ警告］画面の［はい］を選ぶ

１２．［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。

必要な作業は以上です。