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

USRM3-1254-00 2022-03 ja

Copyright CANON INC. 2022

もくじ

はじめに 2

追加対応が必要かご確認ください 4

RSA 鍵の使用先に応じた対応を実施する 7

対応実施手順：TLS 8

Step 1：鍵と証明書を再生成する（TLS） 9

Step 2：鍵と証明書を再設定する（TLS） 14

Step 3：以前に生成された鍵／証明書を削除する（TLS） 15

Step 4：証明書を無効にする（TLS） 16

Step 5：新しい証明書を有効にする（TLS） 17

対応実施手順：IEEE 802.1X 18

Step 1：認証方式を確認する（IEEE 802.1X） 19

Step 2：鍵と証明書を再生成する（IEEE 802.1X） 20

Step 3：鍵と証明書を再設定する（IEEE 802.1X） 25

Step 4：以前に生成された鍵／証明書を削除する（IEEE 802.1X） 27

Step 5：証明書を無効にする（IEEE 802.1X） 28

Step 6：新しい証明書を有効にする（IEEE 802.1X） 29

対応実施手順：IPSec 30

Step 1：認証方式を確認する（IPSec） 31

Step 2：鍵と証明書を再生成する（IPSec） 32

Step 3：鍵と証明書を再設定する（IPSec） 37

Step 4：以前に生成された鍵／証明書を削除する（IPSec） 38

Step 5：証明書を無効にする（IPSec） 39

Step 6：新しい証明書を有効にする（IPSec） 40

対応実施手順：機器署名 41

Step 1：鍵と証明書を再設定する（機器署名） 42

Step 2：証明書を無効にする（機器署名） 43

Step 3：新しい証明書を有効にする（機器署名） 44

はじめに

はじめに 2

はじめに

脆弱性のある暗号ライブラリにて作成した RSA 鍵を更新するため、ファームウェアのアップデートと、設定に応じた追加対応が必要です。

まず、お使いの機種・バージョンをご確認ください。
本ページに記載の機種・バージョンに該当する場合は、ファームウェアのアップデート後、本書に従って必要な追加対応を行ってください。 **追加対応が必要かご確認ください(P. 4)**
ファームウェアのアップデートについては、このドキュメントを入手した Web ページをご確認ください。

バージョンの確認方法

以下の手順でお使いの機種のバージョンをご確認ください。

1 リモート UI を起動する

2 ポータルページで［状況確認/中止］をクリックする

3 ［デバイス情報］▶［バージョン情報］の［Main Controller］を確認する

対応が必要な機種とバージョン

機種	バージョン
- MF656Cdw / MF654Cdw	Ver 01.22
- MF457dw	Ver 01.22 ～ Ver 01.26

MEMO

- 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://oip.manual.canon/

追加対応が必要かご確認ください

追加対応が必要かご確認ください 4

追加対応が必要かご確認ください

RSA 鍵をご確認いただき、設定内容に応じた対応を実施してください。
お使いの機器に登録されている鍵が「Default Key」の場合は、RSA 鍵の確認は不要です。

MEMO

- 本書に掲載している画面は一例です。お使いの機種によっては、画面が異なる場合があります。

1 リモート UI を起動 ▶ ［設定/登録］ ▶ ［デバイス管理］ ▶ ［鍵と証明書設定］をクリックする

2 ［Default Key］以外の鍵をクリックする

3 ［公開鍵］を確認する。

RSA 以外の場合

対応は不要です。

RSA の場合

画面上部の［鍵と証明書設定］をクリックして鍵の使用先を確認します。

- ここで表示された使用先に応じて、対応します。 **RSA 鍵の使用先に応じた対応を実施する(P. 7)**
- 外部で生成して機器に登録した RSA 鍵の場合は、対応は不要です。
- 対応が必要な場合は、証明書を無効にするために証明書の情報が必要になる可能性があります。必要な情報を鍵/証明書を削除する前に控えておくことをお勧めします。必要な情報は証明書を発行した認証局にお問い合わせください。

RSA 鍵の使用先に応じた対応を実施する

RSA 鍵の使用先に応じた対応を実施する 7
対応実施手順：TLS 8
Step 1：鍵と証明書を再生成する（TLS） 9
Step 2：鍵と証明書を再設定する（TLS） 14
Step 3：以前に生成された鍵／証明書を削除する（TLS） 15
Step 4：証明書を無効にする（TLS） 16
Step 5：新しい証明書を有効にする（TLS） 17
対応実施手順：IEEE 802.1X 18
Step 1：認証方式を確認する（IEEE 802.1X） 19
Step 2：鍵と証明書を再生成する（IEEE 802.1X） 20
Step 3：鍵と証明書を再設定する（IEEE 802.1X） 25
Step 4：以前に生成された鍵／証明書を削除する（IEEE 802.1X） 27
Step 5：証明書を無効にする（IEEE 802.1X） 28
Step 6：新しい証明書を有効にする（IEEE 802.1X） 29
対応実施手順：IPSec 30
Step 1：認証方式を確認する（IPSec） 31
Step 2：鍵と証明書を再生成する（IPSec） 32
Step 3：鍵と証明書を再設定する（IPSec） 37
Step 4：以前に生成された鍵／証明書を削除する（IPSec） 38
Step 5：証明書を無効にする（IPSec） 39
Step 6：新しい証明書を有効にする（IPSec） 40
対応実施手順：機器署名 41
Step 1：鍵と証明書を再設定する（機器署名） 42
Step 2：証明書を無効にする（機器署名） 43
Step 3：新しい証明書を有効にする（機器署名） 44

RSA 鍵の使用先に応じた対応を実施する

使用している機能に応じて「参照先」を確認のうえ、対応を実施します。

RSA 鍵の使用先	対応が必要な条件	参照先
[TLS]	常に対応が必要です。	**対応実施手順：TLS(P. 8)**
[IEEE 802.1X]	IEEE 802.1X の認証方式が TLS の場合に対応が必要です。	**対応実施手順：IEEE 802.1X(P. 18)**
[IPSec]	IKE の認証方式が電子署名方式の場合に対応が必要です。	**対応実施手順：IPSec(P. 30)**
[機器署名]	以下の場合は対応が必要です。 • 送信ファイルに機器署名用の鍵で電子署名を付けている場合	**対応実施手順：機器署名(P. 41)**

MEMO

- 本書に掲載している画面は一例です。お使いの機種によっては、画面が異なる場合があります。

対応実施手順：TLS

Step 1：鍵と証明書を再生成する（TLS）(P. 9)
Step 2：鍵と証明書を再設定する（TLS）(P. 14)
Step 3：以前に生成された鍵／証明書を削除する（TLS）(P. 15)
Step 4：証明書を無効にする（TLS）(P. 16)
Step 5：新しい証明書を有効にする（TLS）(P. 17)

Step 1：鍵と証明書を再生成する（TLS）

本機で生成した鍵に証明書を発行する方法には、自己署名証明書、CSR の 2 つがあります。証明書の種類によって、手順が異なります。

自己署名証明書の場合(P. 9)
CSR の場合(P. 10)

自己署名証明書の場合

1 リモート UI を起動する

2 ポータルページで［設定/登録］をクリックする

3 ［デバイス管理］ ▶ ［鍵と証明書設定］をクリックする

4 ［鍵生成］をクリックする

5 ［ネットワーク通信用］を選び、［OK］をクリックする

6 鍵と証明書の設定をする

a ［鍵の設定］

[鍵の名前]
鍵に付ける名称を半角英数字で入力します。一覧表示されたときに探しやすい名称を付けてください。

[署名アルゴリズム]
プルダウンメニューから署名アルゴリズムを選びます。

[鍵のアルゴリズム]
鍵の生成アルゴリズムを［RSA］または［ECDSA］から選び、鍵長をプルダウンメニューから選びます。いずれの場合も鍵長の数値が大きいほど安全性が高まる一方、通信時の処理が遅くなります。

MEMO

- ［署名アルゴリズム］で［SHA384］または［SHA512］を選んだときは、［鍵のアルゴリズム］で［RSA］を選んだ場合の鍵長を［512 bit］に設定することはできません。

b ［証明書の設定］

[有効期限開始日(YYYY/MM/DD)]
証明書の有効期間の開始日を入力します。

[有効期限終了日(YYYY/MM/DD)]
証明書の有効期間の終了日を入力します。［有効期限開始日(YYYY/MM/DD)］より前に設定することはできません。

[国/地域名]
［国/地域名で選択］をクリックしてプルダウンメニューから国／地域名を選ぶか、［インターネット国コードで入力］をクリックして国コード（日本の場合は「JP」）を入力します。

[都道府県]／[市町村]
必要に応じて所在地を半角英数字で入力します。

[組織]／[組織単位]
必要に応じて組織名を半角英数字で入力します。

[共通名]
必要に応じて証明書の主体者の名称を半角英数字で入力します。「Common Name」や「CN」、「一般名」と呼ぶこともあります。

7 ［OK］をクリックする

- 鍵と証明書の生成には時間がかかることがあります。
- 生成した鍵と証明書は本機に自動的に登録されます。

CSR の場合

鍵と CSR を本機で生成します。CSR のデータは画面に表示されるほか、ファイルに出力することもできます。認証局に証明書を発行してもらって、鍵に登録します。

■1. 鍵と CSR を生成する

1 リモート UI を起動する

2 ポータルページで［設定/登録］をクリックする

3 ［デバイス管理］▶［鍵と証明書設定］をクリックする

4 ［鍵生成］をクリックする

5 ［鍵と証明書署名要求(CSR)］を選び、［OK］をクリックする

6 鍵と CSR の設定をする

a ［鍵の設定］

［鍵の名前］
鍵に付ける名称を半角英数字で入力します。一覧表示されたときに探しやすい名称を付けてください。

［署名アルゴリズム］
プルダウンメニューから署名アルゴリズムを選びます。

［鍵のアルゴリズム］
鍵の生成アルゴリズムを［RSA］または［ECDSA］から選び、鍵長をプルダウンメニューから選びます。いずれの場合も鍵長の数値が大きいほど安全性が高まる一方、通信時の処理が遅くなります。

MEMO

- ［署名アルゴリズム］で［SHA384］または［SHA512］を選んだときは、［鍵のアルゴリズム］で［RSA］を選んだ場合の鍵長を［512 bit］に設定することはできません。

b ［証明書署名要求(CSR)の設定］

[国/地域名]
[国/地域名で選択]をクリックしてプルダウンメニューから国／地域名を選ぶか、[インターネット国コードで入力]をクリックして国コード（日本の場合は「JP」）を入力します。

[都道府県]／[市町村]
必要に応じて所在地を半角英数字で入力します。

[組織]／[組織単位]
必要に応じて組織名を半角英数字で入力します。

[共通名]
必要に応じて証明書の主体者の名称を半角英数字で入力します。「Common Name」や「CN」、「一般名」と呼ぶこともあります。

7 [OK]をクリックする

- 鍵と CSR の生成には時間がかかることがあります。

8 [ファイルに保存]をクリックする

- ファイルを保存するダイアログボックスが表示されるので、保存先を選んで[保存]をクリックします。

  ➠ CSR のファイルがパソコンに保存されます。

9 保存したファイルを添付して認証局に申請する

■2. 発行された証明書を鍵に登録する

1 リモート UI を起動し、管理者モードでログインする

2 ポータルページで、[設定/登録]をクリックする

3 [デバイス管理] ▶ [鍵と証明書設定]の順に進む

4 証明書を登録する[鍵の名前]または[証明書]をクリックする

5 **［証明書の登録］をクリックする**

6 **［参照］をクリックし、証明要求した証明書のファイルを指定したあと、［登録］をクリックする**

Step 2：鍵と証明書を再設定する（TLS）

1 **リモート UI を起動する**

2 **ポータルページで［設定/登録］をクリックする**

3 **［ネットワーク］ ▶ ［TLS 設定］をクリックする**

4 **［鍵と証明書］をクリックする**

5 **使用する鍵と証明書の右側にある［使用鍵登録］をクリックする**

- 本機にあらかじめ登録されている鍵と証明書を使いたい場合は、［Default Key］を選びます。

6 **［OK］をクリックする**

7 **本機を再起動する**

➠ 本機が再起動して、設定が反映されます。

Step 3：以前に生成された鍵／証明書を削除する（TLS）

MEMO

- 証明書を無効にする場合、認証局へ証明書の情報を伝える必要がある可能性があります。 **追加対応が必要かご確認ください(P. 4)** をご参照いただき、鍵／証明書を削除する前に必要な情報を控えておいてください。

1 **リモート UI を起動する**

2 **ポータルページで［設定/登録］をクリックする**

3 **［デバイス管理］ ▶ ［鍵と証明書設定］をクリックする**

4 **鍵と証明書を選び、［削除］ ▶ ［OK］をクリックする**

MEMO

- 使用中の鍵と証明書には［TLS］や［IEEE 802.1X］などの使用目的が表示され、この状態では削除できません。目的の機能を解除するか、別の鍵と証明書に変更してから削除してください。

Step 4：証明書を無効にする（TLS）

以前に生成された証明書を無効にします。証明書の種類によって、手順が異なります。

■自己署名証明書の場合

対策が必要な鍵を含んだ証明書をパソコンやウェブブラウザーに信頼された証明書として登録している場合は登録してある証明書を削除してください。

■CSR の場合

証明書を発行した認証局に証明書の失効を依頼してください。依頼する認証局は証明書の［発行者］情報を参考にしてください。

- 本機の通信相手であるパソコンやウェブブラウザーで、証明書の失効確認を CRL で行っている場合は、証明書の失効後に更新された CRL をパソコンやウェブブラウザーに登録してください。
- 証明書の失効確認として CRL 以外の方法（例えば OCSP など）を行っている場合は、それらの手続きも行ってください。

Step 5：新しい証明書を有効にする（TLS）

本機で新たに生成した証明書を有効にします。

■自己署名証明書の場合

新しい証明書をパソコンやウェブブラウザーに信頼された証明書として登録してください。

■CSR の場合

対応は不要です。

対応実施手順：IEEE 802.1X

Step 1：認証方式を確認する（IEEE 802.1X）(P. 19)
Step 2：鍵と証明書を再生成する（IEEE 802.1X）(P. 20)
Step 3：鍵と証明書を再設定する（IEEE 802.1X）(P. 25)
Step 4：以前に生成された鍵／証明書を削除する（IEEE 802.1X）(P. 27)
Step 5：証明書を無効にする（IEEE 802.1X）(P. 28)
Step 6：新しい証明書を有効にする（IEEE 802.1X）(P. 29)

Step 1：認証方式を確認する（IEEE 802.1X）

IEEE 802.1X の認証方式が TLS の場合に以降の対策が必要です。
以下の手順に従って、認証方式をご確認ください。

1 リモート UI を起動する

2 ポータルページで［設定/登録］をクリックする

3 ［ネットワーク］ ▶ ［IEEE 802.1X 設定］ ▶ ［編集］をクリックする

4 ［TLS を使用する］を確認する

- ［TLS を使用する］にチェックマークが付いていて、鍵の名前が表示されている場合は以降の対応をします。
- ［TLS を使用する］にチェックマークが付いていない場合は対応不要です。

Step 2：鍵と証明書を再生成する（IEEE 802.1X）

本機で生成した鍵に証明書を発行する方法には、自己署名証明書、CSR の 2 つがあります。証明書の種類によって、手順が異なります。

自己署名証明書の場合(P. 20)
CSR の場合(P. 21)

自己署名証明書の場合

1 リモート UI を起動する

2 ポータルページで［設定/登録］をクリックする

3 ［デバイス管理］ ▶ ［鍵と証明書設定］をクリックする

4 ［鍵生成］をクリックする

5 ［ネットワーク通信用］を選び、［OK］をクリックする

6 鍵と証明書の設定をする

a ［鍵の設定］

[鍵の名前]
鍵に付ける名称を半角英数字で入力します。一覧表示されたときに探しやすい名称を付けてください。

[署名アルゴリズム]
プルダウンメニューから署名アルゴリズムを選びます。

[鍵のアルゴリズム]
鍵の生成アルゴリズムを［RSA］または［ECDSA］から選び、鍵長をプルダウンメニューから選びます。いずれの場合も鍵長の数値が大きいほど安全性が高まる一方、通信時の処理が遅くなります。

MEMO

- ［署名アルゴリズム］で［SHA384］または［SHA512］を選んだときは、［鍵のアルゴリズム］で［RSA］を選んだ場合の鍵長を［512 bit］に設定することはできません。

b ［証明書の設定］

[有効期限開始日(YYYY/MM/DD)]
証明書の有効期間の開始日を入力します。

[有効期限終了日(YYYY/MM/DD)]
証明書の有効期間の終了日を入力します。［有効期限開始日(YYYY/MM/DD)］より前に設定することはできません。

[国/地域名]
［国/地域名で選択］をクリックしてプルダウンメニューから国／地域名を選ぶか、［インターネット国コードで入力］をクリックして国コード（日本の場合は「JP」）を入力します。

[都道府県]／[市町村]
必要に応じて所在地を半角英数字で入力します。

[組織]／[組織単位]
必要に応じて組織名を半角英数字で入力します。

[共通名]
必要に応じて証明書の主体者の名称を半角英数字で入力します。「Common Name」や「CN」、「一般名」と呼ぶこともあります。

7 ［OK］をクリックする

- 鍵と証明書の生成には時間がかかることがあります。
- 生成した鍵と証明書は本機に自動的に登録されます。

CSR の場合

鍵と CSR を本機で生成します。CSR のデータは画面に表示されるほか、ファイルに出力することもできます。認証局に証明書を発行してもらって、鍵に登録します。

■1. 鍵と CSR を生成する

1 リモート UI を起動する

2 ポータルページで［設定/登録］をクリックする

3 ［デバイス管理］▶［鍵と証明書設定］をクリックする

4 ［鍵生成］をクリックする

5 ［鍵と証明書署名要求(CSR)］を選び、［OK］をクリックする

6 鍵と CSR の設定をする

a ［鍵の設定］

［鍵の名前］
鍵に付ける名称を半角英数字で入力します。一覧表示されたときに探しやすい名称を付けてください。

［署名アルゴリズム］
プルダウンメニューから署名アルゴリズムを選びます。

［鍵のアルゴリズム］
鍵の生成アルゴリズムを［RSA］または［ECDSA］から選び、鍵長をプルダウンメニューから選びます。いずれの場合も鍵長の数値が大きいほど安全性が高まる一方、通信時の処理が遅くなります。

MEMO

- ［署名アルゴリズム］で［SHA384］または［SHA512］を選んだときは、［鍵のアルゴリズム］で［RSA］を選んだ場合の鍵長を［512 bit］に設定することはできません。

b ［証明書署名要求(CSR)の設定］

[国/地域名]
[国/地域名で選択]をクリックしてプルダウンメニューから国／地域名を選ぶか、[インターネット国コードで入力]をクリックして国コード（日本の場合は「JP」）を入力します。

[都道府県]／[市町村]
必要に応じて所在地を半角英数字で入力します。

[組織]／[組織単位]
必要に応じて組織名を半角英数字で入力します。

[共通名]
必要に応じて証明書の主体者の名称を半角英数字で入力します。「Common Name」や「CN」、「一般名」と呼ぶこともあります。

7 [OK]をクリックする

- 鍵と CSR の生成には時間がかかることがあります。

8 [ファイルに保存]をクリックする

- ファイルを保存するダイアログボックスが表示されるので、保存先を選んで[保存]をクリックします。

  ➠ CSR のファイルがパソコンに保存されます。

9 保存したファイルを添付して認証局に申請する

■2. 発行された証明書を鍵に登録する

1 リモート UI を起動し、管理者モードでログインする

2 ポータルページで、[設定/登録]をクリックする

3 [デバイス管理] ▶ [鍵と証明書設定]の順に進む

4 証明書を登録する[鍵の名前]または[証明書]をクリックする

5 **［証明書の登録］をクリックする**

6 **［参照］をクリックし、証明要求した証明書のファイルを指定したあと、［登録］をクリックする**

Step 3：鍵と証明書を再設定する（IEEE 802.1X）

1 リモート UI を起動する

2 ポータルページで［設定/登録］をクリックする

3 ［ネットワーク］ ▶ ［IEEE 802.1X 設定］ ▶ ［編集］をクリックする

4 ［IEEE 802.1X を使用する］にチェックマークを付け、［ログイン名］を入力をする

［IEEE 802.1X を使用する］

IEEE 802.1X 認証を使用するときはチェックマークを付けます。

［ログイン名］

ユーザーを識別するための名称（EAP Identity）を半角英数字で入力します。

5 ［TLS を使用する］にチェックマークを付け、［鍵と証明書］をクリックする

6 使用する鍵と証明書の右側にある［使用鍵登録］をクリックする

7 ［OK］をクリックする

8 本機を再起動する

➠ 本機が再起動して、設定が反映されます。

Step 4：以前に生成された鍵／証明書を削除する（IEEE 802.1X）

MEMO

- 証明書を無効にする場合、認証局へ証明書の情報を伝える必要がある可能性があります。 **追加対応が必要かご確認ください(P. 4)** をご参照いただき、鍵／証明書を削除する前に必要な情報を控えておいてください。

1 **リモート UI を起動する**

2 **ポータルページで［設定/登録］をクリックする**

3 **［デバイス管理］ ▶ ［鍵と証明書設定］をクリックする**

4 **鍵と証明書を選び、［削除］ ▶ ［OK］をクリックする**

MEMO

- 使用中の鍵と証明書には［TLS］や［IEEE 802.1X］などの使用目的が表示され、この状態では削除できません。目的の機能を解除するか、別の鍵と証明書に変更してから削除してください。

Step 5：証明書を無効にする（IEEE 802.1X）

以前に生成された証明書を無効にします。証明書の種類によって、手順が異なります。

■自己署名証明書の場合

対策が必要な鍵を含んだ証明書を IEEE 802.1X の認証サーバーに信頼された証明書として登録している場合は登録してある証明書を削除してください。

■CSR の場合

証明書を発行した認証局に証明書の失効を依頼してください。依頼する認証局は証明書の［発行者］情報を参考にしてください。

- IEEE 802.1X の認証サーバーで、証明書の失効確認を CRL で行っている場合は、証明書の失効後に更新された CRL をパソコンやウェブブラウザーに登録してください。
- 証明書の失効確認として CRL 以外の方法（例えば OCSP など）を行っている場合は、それらの手続きも行ってください。

Step 6：新しい証明書を有効にする（IEEE 802.1X）

証明書を有効にします。

■自己署名証明書の場合

新しい証明書を IEEE 802.1X の認証サーバーに信頼された証明書として登録してください。

■CSR の場合

対応は不要です。

対応実施手順：IPSec

Step 1：認証方式を確認する（IPSec）(P. 31)
Step 2：鍵と証明書を再生成する（IPSec）(P. 32)
Step 3：鍵と証明書を再設定する（IPSec）(P. 37)
Step 4：以前に生成された鍵／証明書を削除する（IPSec）(P. 38)
Step 5：証明書を無効にする（IPSec）(P. 39)
Step 6：新しい証明書を有効にする（IPSec）(P. 40)

Step 1：認証方式を確認する（IPSec）

IPSec の IKE 設定の認証方式が［電子署名方式］の場合に以降の対策が必要です。
以下の手順に従って、認証方式をご確認ください。

1 **リモート UI を起動する**

2 **ポータルページで［設定/登録］をクリックする**

3 **［ネットワーク］ ▶ ［IPSec 設定］をクリックする**

4 **［登録されている IPSec ポリシー］からポリシーをクリックする**

5 **［IKE 設定］の［認証方式］を確認する**

- ［認証方式］が［電子署名方式］で、鍵の名前が表示されている場合は以降の対応をします。
- ［認証方式］が［事前共有鍵方式］の場合は対応不要です。

Step 2：鍵と証明書を再生成する（IPSec）

本機で生成した鍵に証明書を発行する方法には、自己署名証明書、CSR の 2 つがあります。証明書の種類によって、手順が異なります。

自己署名証明書の場合(P. 32)
CSR の場合(P. 33)

自己署名証明書の場合

1 リモート UI を起動する

2 ポータルページで［設定/登録］をクリックする

3 ［デバイス管理］ ▶ ［鍵と証明書設定］をクリックする

4 ［鍵生成］をクリックする

5 ［ネットワーク通信用］を選び、［OK］をクリックする

6 鍵と証明書の設定をする

a ［鍵の設定］

[鍵の名前]
鍵に付ける名称を半角英数字で入力します。一覧表示されたときに探しやすい名称を付けてください。

[署名アルゴリズム]
プルダウンメニューから署名アルゴリズムを選びます。

[鍵のアルゴリズム]
鍵の生成アルゴリズムを［RSA］または［ECDSA］から選び、鍵長をプルダウンメニューから選びます。いずれの場合も鍵長の数値が大きいほど安全性が高まる一方、通信時の処理が遅くなります。

MEMO

- ［署名アルゴリズム］で［SHA384］または［SHA512］を選んだときは、［鍵のアルゴリズム］で［RSA］を選んだ場合の鍵長を［512 bit］に設定することはできません。

b ［証明書の設定］

[有効期限開始日(YYYY/MM/DD)]
証明書の有効期間の開始日を入力します。

[有効期限終了日(YYYY/MM/DD)]
証明書の有効期間の終了日を入力します。［有効期限開始日(YYYY/MM/DD)］より前に設定することはできません。

[国/地域名]
［国/地域名で選択］をクリックしてプルダウンメニューから国／地域名を選ぶか、［インターネット国コードで入力］をクリックして国コード（日本の場合は「JP」）を入力します。

[都道府県]／[市町村]
必要に応じて所在地を半角英数字で入力します。

[組織]／[組織単位]
必要に応じて組織名を半角英数字で入力します。

[共通名]
必要に応じて証明書の主体者の名称を半角英数字で入力します。「Common Name」や「CN」、「一般名」と呼ぶこともあります。

7 ［OK］をクリックする

- 鍵と証明書の生成には時間がかかることがあります。
- 生成した鍵と証明書は本機に自動的に登録されます。

CSR の場合

鍵と CSR を本機で生成します。CSR のデータは画面に表示されるほか、ファイルに出力することもできます。認証局に証明書を発行してもらって、鍵に登録します。

■1. 鍵と CSR を生成する

1 リモート UI を起動する

2 ポータルページで［設定/登録］をクリックする

3 ［デバイス管理］▶［鍵と証明書設定］をクリックする

4 ［鍵生成］をクリックする

5 ［鍵と証明書署名要求(CSR)］を選び、［OK］をクリックする

6 鍵と CSR の設定をする

a ［鍵の設定］

［鍵の名前］
鍵に付ける名称を半角英数字で入力します。一覧表示されたときに探しやすい名称を付けてください。

［署名アルゴリズム］
プルダウンメニューから署名アルゴリズムを選びます。

［鍵のアルゴリズム］
鍵の生成アルゴリズムを［RSA］または［ECDSA］から選び、鍵長をプルダウンメニューから選びます。いずれの場合も鍵長の数値が大きいほど安全性が高まる一方、通信時の処理が遅くなります。

MEMO

- ［署名アルゴリズム］で［SHA384］または［SHA512］を選んだときは、［鍵のアルゴリズム］で［RSA］を選んだ場合の鍵長を［512 bit］に設定することはできません。

b ［証明書署名要求(CSR)の設定］

[国/地域名]
[国/地域名で選択]をクリックしてプルダウンメニューから国／地域名を選ぶか、[インターネット国コードで入力]をクリックして国コード（日本の場合は「JP」）を入力します。

[都道府県]／[市町村]
必要に応じて所在地を半角英数字で入力します。

[組織]／[組織単位]
必要に応じて組織名を半角英数字で入力します。

[共通名]
必要に応じて証明書の主体者の名称を半角英数字で入力します。「Common Name」や「CN」、「一般名」と呼ぶこともあります。

7 [OK]をクリックする

- 鍵と CSR の生成には時間がかかることがあります。

8 [ファイルに保存]をクリックする

- ファイルを保存するダイアログボックスが表示されるので、保存先を選んで[保存]をクリックします。

  ➠ CSR のファイルがパソコンに保存されます。

9 保存したファイルを添付して認証局に申請する

■2. 発行された証明書を鍵に登録する

1 リモート UI を起動し、管理者モードでログインする

2 ポータルページで、[設定/登録]をクリックする

3 [デバイス管理] ▶ [鍵と証明書設定]の順に進む

4 証明書を登録する[鍵の名前]または[証明書]をクリックする

5 **［証明書の登録］をクリックする**

6 **［参照］をクリックし、証明要求した証明書のファイルを指定したあと、［登録］をクリックする**

Step 3：鍵と証明書を再設定する（IPSec）

1 **リモート UI を起動する**

2 **ポータルページで［設定/登録］をクリックする**

3 **［ネットワーク］ ▶ ［IPSec 設定］をクリックする**

4 **［登録されている IPSec ポリシー］から鍵と証明書を再設定するポリシーをクリックする**

5 **［IKE 設定］の設定をする**

6 **［認証方式］で［電子署名方式］にチェックマークを付け、［鍵と証明書］をクリックする**

7 **使用する鍵と証明書の右側にある［使用鍵登録］をクリックする**

8 **［OK］をクリックする**

9 **本機を再起動する**

➠ 本機が再起動して、設定が反映されます。

Step 4：以前に生成された鍵／証明書を削除する（IPSec）

MEMO

- 証明書を無効にする場合、認証局へ証明書の情報を伝える必要がある可能性があります。**追加対応が必要かご確認ください(P. 4)** をご参照いただき、鍵／証明書を削除する前に必要な情報を控えておいてください。

1 **リモート UI を起動する**

2 **ポータルページで［設定/登録］をクリックする**

3 **［デバイス管理］▶［鍵と証明書設定］をクリックする**

4 **鍵と証明書を選び、［削除］▶［OK］をクリックする**

MEMO

- 使用中の鍵と証明書には［TLS］や［IEEE 802.1X］などの使用目的が表示され、この状態では削除できません。目的の機能を解除するか、別の鍵と証明書に変更してから削除してください。

Step 5：証明書を無効にする（IPSec）

以前に生成された証明書を無効にします。証明書の種類によって、手順が異なります。

■自己署名証明書の場合

対策が必要な鍵を含んだ証明書を IPSec の通信相手に信頼された証明書として登録している場合は登録してある証明書を削除してください。削除後に、再生成した鍵の証明書を登録してください。

■CSR の場合

証明書を発行した認証局に証明書の失効を依頼してください。依頼する認証局は証明書の［発行者］情報を参考にしてください。

- IPSec の通信相手で、証明書の失効確認を CRL で行っている場合は、証明書の失効後に更新された CRL をパソコンやウェブブラウザーに登録してください。
- 証明書の失効確認として CRL 以外の方法（例えば OCSP など）を行っている場合は、それらの手続きも行ってください。

Step 6：新しい証明書を有効にする（IPSec）

証明書を有効にします。

■自己署名証明書の場合

新しい証明書を IPSec の通信相手に信頼された証明書として登録してください。

■CSR の場合

対応は不要です。

対応実施手順：機器署名

Step 1：鍵と証明書を再設定する（機器署名）(P. 42)
Step 2：証明書を無効にする（機器署名）(P. 43)
Step 3：新しい証明書を有効にする（機器署名）(P. 44)

Step 1：鍵と証明書を再設定する（機器署名）

1 **リモート UI を起動する**

2 **ポータルページで［設定/登録］をクリックする**

3 **［デバイス管理］ ▶ ［鍵と証明書設定］をクリックする**

4 **機器署名の鍵と証明書の右側にある［更新］をクリックする**

5 **［OK］をクリックする**

Step 2：証明書を無効にする（機器署名）

以前に生成された証明書を無効にします。

■機器署名用の証明書を Acrobat に登録している場合

Acrobat に機器署名用の証明書を登録している場合は、登録してある証明書を削除してください。

Step 3：新しい証明書を有効にする（機器署名）

証明書を有効にします。

■機器署名用の証明書を Acrobat に登録している場合

機器署名用の証明書を Acrobat に登録している場合は、本機から機器署名を付けて送信した PDF ファイル内の証明書を Acrobat に登録してください。

This Font Software is licensed under the SIL Open Font License, Version 1.1.

This license is copied below, and is also available with a FAQ at: http://scripts.sil.org/OFL

SIL OPEN FONT LICENSE Version 1.1 - 26 February 2007

PREAMBLE

The goals of the Open Font License (OFL) are to stimulate worldwide development of collaborative font projects, to support the font creation efforts of academic and linguistic communities, and to provide a free and open framework in which fonts may be shared and improved in partnership with others.

The OFL allows the licensed fonts to be used, studied, modified and redistributed freely as long as they are not sold by themselves. The fonts, including any derivative works, can be bundled, embedded, redistributed and/or sold with any software provided that any reserved names are not used by derivative works. The fonts and derivatives, however, cannot be released under any other type of license. The requirement for fonts to remain under this license does not apply to any document created using the fonts or their derivatives.

DEFINITIONS

"Font Software" refers to the set of files released by the Copyright Holder(s) under this license and clearly marked as such. This may include source files, build scripts and documentation.

"Reserved Font Name" refers to any names specified as such after the copyright statement(s).

"Original Version" refers to the collection of Font Software components as distributed by the Copyright Holder(s).

"Modified Version" refers to any derivative made by adding to, deleting, or substituting -- in part or in whole -- any of the components of the Original Version, by changing formats or by porting the Font Software to a new environment.

"Author" refers to any designer, engineer, programmer, technical writer or other person who contributed to the Font Software.

PERMISSION & CONDITIONS

Permission is hereby granted, free of charge, to any person obtaining a copy of the Font Software, to use, study, copy, merge, embed, modify, redistribute, and sell modified and unmodified copies of the Font Software, subject to the following conditions:

1) Neither the Font Software nor any of its individual components, in Original or Modified Versions, may be sold by itself.

2) Original or Modified Versions of the Font Software may be bundled, redistributed and/or sold with any software, provided that each copy contains the above copyright notice and this license. These can be included either as stand-alone text files, human-readable headers or in the appropriate machine-readable metadata fields within text or binary files as long as those fields can be easily viewed by the user.

3) No Modified Version of the Font Software may use the Reserved Font Name(s) unless explicit written permission is granted by the corresponding Copyright Holder. This restriction only applies to the primary font name as presented to the users.

4) The name(s) of the Copyright Holder(s) or the Author(s) of the Font Software shall not be used to promote, endorse or advertise any Modified Version, except to acknowledge the contribution(s) of the Copyright Holder(s) and the Author(s) or with their explicit written permission.

5) The Font Software, modified or unmodified, in part or in whole, must be distributed entirely under this license, and must not be distributed under any other license. The requirement for fonts to remain under this license does not apply to any document created using the Font Software.

TERMINATION
This license becomes null and void if any of the above conditions are not met.

DISCLAIMER
THE FONT SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF COPYRIGHT, PATENT, TRADEMARK, OR OTHER RIGHT. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, INCLUDING ANY GENERAL, SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF THE USE OR INABILITY TO USE THE FONT SOFTWARE OR FROM OTHER DEALINGS IN THE FONT SOFTWARE.