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

USRM3-1245-02 2022-07 ja

もくじ

はじめに 2

追加対応が必要かご確認ください 5

RSA 鍵の使用先に応じた対応を実施する 12

対応実施手順：TLS 13

Step 1：鍵と証明書を再生成する（TLS） 14

Step 2：鍵と証明書を再設定する（TLS） 22

Step 3：以前に生成された鍵／証明書を削除する（TLS） 24

Step 4：証明書を無効にする（TLS） 26

Step 5：新しい証明書を有効にする（TLS） 27

対応実施手順：IEEE 802.1X 28

Step 1：認証方式を確認する（IEEE 802.1X） 29

Step 2：鍵と証明書を再生成する（IEEE 802.1X） 31

Step 3：鍵と証明書を再設定する（IEEE 802.1X） 39

Step 4：以前に生成された鍵／証明書を削除する（IEEE 802.1X） 42

Step 5：証明書を無効にする（IEEE 802.1X） 44

Step 6：新しい証明書を有効にする（IEEE 802.1X） 45

対応実施手順：IPSec 46

Step 1：認証方式を確認する（IPSec） 47

Step 2：鍵と証明書を再生成する（IPSec） 49

Step 3：鍵と証明書を再設定する（IPSec） 57

Step 4：以前に生成された鍵／証明書を削除する（IPSec） 59

Step 5：証明書を無効にする（IPSec） 61

Step 6：新しい証明書を有効にする（IPSec） 62

対応実施手順：SIP 63

Step 1：SIP の設定を確認する（SIP） 64

Step 2：鍵と証明書を再生成する（SIP） 67

Step 3：鍵と証明書を再設定する（SIP） 73

Step 4：以前に生成された鍵／証明書を削除する（SIP） 76

Step 5：証明書を無効にする（SIP） 78

Step 6：新しい証明書を有効にする（SIP） 79

対応実施手順：機器署名 80

Step 1：S/MIME の設定を確認する（機器署名） 81

Step 2：鍵と証明書を再設定する（機器署名） 83

Step 3：証明書を無効にする（機器署名） 84

Step 4：新しい証明書を有効にする（機器署名） 85

Bluetooth 設定の対応を実施する 88

対応実施手順：Bluetooth 89

Step 1：Canon PRINT Business に登録済のデバイスを削除する（Bluetooth） 90
Step 2：Canon PRINT Business にデバイスを再登録する（Bluetooth） 91

ACCESS MANAGEMENT SYSTEM 設定の対応を実施する 93
対応実施手順：ACCESS MANAGEMENT SYSTEM 94

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. 5)**
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［コントローラー］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
- iR-ADV 4545 / 4535 / 4525 - iR-ADV 6575 / 6565 / 6560 / 6555 - iR-ADV 8505 / 8595 / 8585 / 8505B / 8595B / 8585B - iR-ADV C3530 / C3520 - iR-ADV C7580 / C7570 / C7565 - iR-ADV C5560 / C5550 / C5540 / C5535 - iR-ADV C5560F-R / C5550F-R / C5540F-R - iR-ADV C355 - iR-ADV C356	Ver 59.39 ～ Ver 67.30
- iR-ADV 4545 III / 4535 III / 4525 III - iR-ADV 6575 III / 6565 III / 6560 III - iR-ADV 8505 III / 8595 III / 8585 III / 8505B III / 8595B III / 8585B III - iR-ADV C3530 III / C3520 III - iR-ADV C7580 III / C7570 III / C7565 III - iR-ADV C5560 III / C5550 III / C5540 III / C5535 III - iR-ADV C356 III - iPR C165 / C170	Ver 29.39 ～ Ver 37.30
- iR-ADV 4725 / 4735 / 4745 - iR-ADV 8705 / 8705B / 8795 / 8795B / 8786 / 8786B - iR-ADV C3730 / C3720 - iR-ADV C7780 / C7770 / C7765	Ver 17.44 ～ Ver 27.30

機種	バージョン
- iR-ADV C357	
- iR-ADV C5760 / C5750 / C5740 / C5735	Ver 19.40 ～ Ver 27.30
- iR-ADV 6765 / 6780	Ver 17.44 ～ Ver 27.33
- iR-ADV C5870 / C5860 / C5850 / C5840	Ver 03.11 ～ Ver 17.32
- iR-ADV 6860 / 6870	Ver 05.25 ～ Ver 17.32
- iR-ADV C3830 / C3826 / C3835	Ver 06.28 ～ Ver 17.32
- iR C3222F	Ver 01.12 ～ Ver 02.13
- MF832Cdw	Ver 200.0.301 ～ Ver 309.0.405
- LBP722Ci	Ver 114.0.301 ～ Ver 309.0.405
- MF7525F	Ver 221.0.117 ～ Ver 600.0.601

- 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 5

追加対応が必要かご確認ください

以下 3 点をご確認いただき、設定内容に応じた対応を実施してください。
お使いの機種によっては、操作パネルからは操作できません。リモート UI から操作してください。

RSA 鍵の確認(P. 5)
Bluetooth 設定の確認(P. 8)
ACCESS MANAGEMENT SYSTEM 設定の確認(P. 8)
お使いの機器に登録されている鍵が「Default Key」／「AMS」の場合は、RSA 鍵の確認は不要です。Bluetooth 設定と Access Management System 設定を確認し、必要に応じて対応を実施してください。

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。

RSA 鍵の確認

本機で生成した RSA 鍵を使用しているかどうかを確認します。使用している場合は使用先を確認します。

操作パネルで操作する場合(P. 5)
リモート UI で操作する場合(P. 6)

■操作パネルで操作する場合

1 （設定/登録）を押す

2 ＜管理設定＞ ▶ ＜デバイス管理＞ ▶ ＜証明書設定＞ ▶ ＜鍵と証明書リスト＞を押す

3 <本機の鍵と証明書リスト＞を押す

- お使いの機器でユーザー署名機能が有効になっていない場合は、＜本機の鍵と証明書リスト＞は表示されません。次の手順へ進んでください。

4 <Default Key>および<AMS>以外で、＜使用状況＞が＜使用中＞の鍵を選択して＜証明書詳細情報＞を押す
表示例：

5 ＜公開鍵＞を確認する

表示例：

RSA 以外の場合

対応は不要です。＜ OK ＞を押して画面を閉じます。

RSA の場合

手順 6 へ進みます。

- 以下の鍵の場合は、対応は不要です。＜ OK ＞を押して画面を閉じます。
  - 外部で生成して機器に登録した RSA 鍵
- 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。

6 ＜使用先を表示＞を押して鍵の使用先を確認する

表示例：

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. 12)**

■リモート UI で操作する場合

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］および［AMS］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. 12)**
- 以下の場合は、対応は不要です。
  - 外部で生成して機器に登録した RSA 鍵
- 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。

Bluetooth 設定の確認

Bluetooth 設定が＜ ON ＞かどうかを確認します。＜ ON ＞の場合は追加対応が必要です。

操作パネルで操作する場合(P. 8)
リモート UI で操作する場合(P. 8)

■操作パネルで操作する場合

1 （設定/登録）を押す

2 ＜環境設定＞ ▶ ＜ネットワーク＞ ▶ ＜ Bluetooth 設定＞を押す

3 ＜ Bluetooth を使用＞を確認する

- ＜ Bluetooth を使用＞が＜ ON ＞の場合は以降の対応をします。 **Bluetooth 設定の対応を実施する(P. 88)**
- ＜ Bluetooth を使用＞が＜ OFF ＞の場合は対応不要です。

■リモート UI で操作する場合

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 ［ネットワーク］ ▶ ［Bluetooth 設定］をクリックする

4 ［Bluetooth を使用する］を確認する

- ［Bluetooth を使用する］にチェックマークが付いている場合は以降の対応をします。 **Bluetooth 設定の対応を実施する(P. 88)**
- ［Bluetooth 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。

ACCESS MANAGEMENT SYSTEM 設定の確認

ACCESS MANAGEMENT SYSTEM 設定が＜ ON ＞かどうかを確認します。＜ ON ＞の場合は追加対応が必要です。

お使いの機器によっては本設定が無い場合があります。その場合は対応は不要です。

操作パネルで操作する場合(P. 9)
リモート UI で操作する場合(P. 9)

■操作パネルで操作する場合

1 （設定/登録）を押す

2 ＜管理設定＞ ▶ ＜ライセンス/その他＞ ▶ ＜ ACCESS MANAGEMENT SYSTEM を使用＞を押す

3 ＜ ACCESS MANAGEMENT SYSTEM を使用＞を確認する

- ＜ ACCESS MANAGEMENT SYSTEM を使用＞が＜ ON ＞の場合は以降の対応をします。 **ACCESS MANAGEMENT SYSTEM 設定の対応を実施する(P. 93)**
- ＜ ACCESS MANAGEMENT SYSTEM を使用＞が＜ OFF ＞の場合は対応不要です。

■リモート UI で操作する場合

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 ［ライセンス/その他］ ▶ ［ACCESS MANAGEMENT SYSTEM 設定］をクリックする

4 ［ACCESS MANAGEMENT SYSTEM を使用する］を確認する

- ［ACCESS MANAGEMENT SYSTEM を使用する］にチェックマークが付いている場合は以降の対応をします。 **ACCESS MANAGEMENT SYSTEM 設定の対応を実施する(P. 93)**
- ［ACCESS MANAGEMENT SYSTEM 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。

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 12
対応実施手順：TLS 13
Step 1：鍵と証明書を再生成する（TLS） 14
Step 2：鍵と証明書を再設定する（TLS） 22
Step 3：以前に生成された鍵／証明書を削除する（TLS） 24
Step 4：証明書を無効にする（TLS） 26
Step 5：新しい証明書を有効にする（TLS） 27
対応実施手順：IEEE 802.1X 28
Step 1：認証方式を確認する（IEEE 802.1X） 29
Step 2：鍵と証明書を再生成する（IEEE 802.1X） 31
Step 3：鍵と証明書を再設定する（IEEE 802.1X） 39
Step 4：以前に生成された鍵／証明書を削除する（IEEE 802.1X） 42
Step 5：証明書を無効にする（IEEE 802.1X） 44
Step 6：新しい証明書を有効にする（IEEE 802.1X） 45
対応実施手順：IPSec 46
Step 1：認証方式を確認する（IPSec） 47
Step 2：鍵と証明書を再生成する（IPSec） 49
Step 3：鍵と証明書を再設定する（IPSec） 57
Step 4：以前に生成された鍵／証明書を削除する（IPSec） 59
Step 5：証明書を無効にする（IPSec） 61
Step 6：新しい証明書を有効にする（IPSec） 62
対応実施手順：SIP 63
Step 1：SIP の設定を確認する（SIP） 64
Step 2：鍵と証明書を再生成する（SIP） 67
Step 3：鍵と証明書を再設定する（SIP） 73
Step 4：以前に生成された鍵／証明書を削除する（SIP） 76
Step 5：証明書を無効にする（SIP） 78
Step 6：新しい証明書を有効にする（SIP） 79
対応実施手順：機器署名 80
Step 1：S/MIME の設定を確認する（機器署名） 81
Step 2：鍵と証明書を再設定する（機器署名） 83

Step 3：証明書を無効にする（機器署名） 84
Step 4：新しい証明書を有効にする（機器署名） 85

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. 13)**
IEEE 802.1X	IEEE 802.1X の認証方式が EAP-TLS の場合に対応が必要です。	**対応実施手順：IEEE 802.1X(P. 28)**
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. 46)**
SIP	TLS を使用する設定の場合に対応が必要です。	**対応実施手順：SIP(P. 63)**
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 ・S/MIME の暗号化設定で暗号化が有効になっている場合	**対応実施手順：機器署名(P. 80)**

- 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. 14)
Step 2：鍵と証明書を再設定する（TLS）(P. 22)
Step 3：以前に生成された鍵／証明書を削除する（TLS）(P. 24)
Step 4：証明書を無効にする（TLS）(P. 26)
Step 5：新しい証明書を有効にする（TLS）(P. 27)

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、SCEP の 3 つがあります。証明書の種類によって、手順が異なります。
お使いの機種によっては、操作パネルからは操作できません。リモート UI から操作してください。

自己署名証明書の場合(P. 14)
CSR の場合(P. 17)
SCEP の場合(P. 19)

自己署名証明書の場合

操作パネルで操作する場合(P. 14)
リモート UI で操作する場合(P. 15)

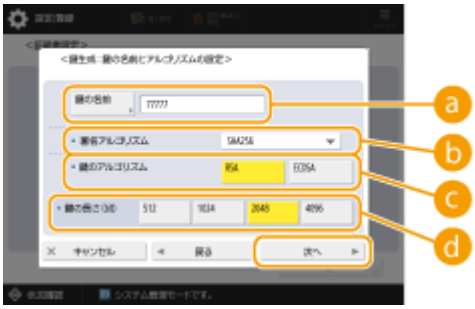
■操作パネルで操作する場合

1 （設定/登録）を押す

2 ＜管理設定＞ ▸ ＜デバイス管理＞ ▸ ＜証明書設定＞ ▸ ＜鍵生成＞ ▸ ＜ネットワーク通信用の鍵生成＞を押す

3 鍵の必要項目を設定し、次の画面に進む

表示例：



a ＜鍵の名前＞

鍵に付ける名前を入力します。一覧表示されたときに探しやすい名前を付けてください。

b ＜署名アルゴリズム＞

署名に利用するハッシュ関数を選びます。鍵の長さによって選択できるハッシュ関数が異なります。SHA384 と SHA512 のハッシュ関数をサポートしているのは、1024 ビット以上の長さの鍵です。c で＜ RSA ＞を選んだあと、d の＜鍵の長さ(bit)＞で＜ 1024 ＞以上を選ぶと SHA384 と SHA512 のハッシュ関数が選べるようになります。

c ＜鍵のアルゴリズム＞

鍵のアルゴリズムを選びます。＜ RSA ＞を選ぶと＜鍵の長さ(bit)＞が、＜ ECDSA ＞を選ぶと＜鍵の種類＞が、dの設定項目として表示されます。

d ＜鍵の長さ(bit)＞／＜鍵の種類＞

cで＜ RSA ＞を選んだ場合は鍵の長さを、＜ ECDSA ＞を選んだ場合は鍵の種類を選びます。いずれの場合も数値が大きいほど安全性が高まりますが、通信時の処理が遅くなります。

4 証明書の必要項目を設定し、＜鍵生成実行＞を押す

表示例：

a ＜有効期限開始日＞／＜有効期限終了日＞

証明書の有効期間の開始日／終了日を入力します。

b ＜国/地域名＞／＜都道府県＞／＜市町村＞／＜組織＞／＜組織単位＞

国コードを一覧から選択し、所在地や組織名を入力します。

c ＜共通名＞

IP アドレスまたは FQDN を入力します。

- Windows の環境で IPPS 印刷を行うときは、必ず本機の IP アドレスを入力してください。
- 本機の FQDN を入力する場合は、DNS サーバーが必要です。DNS サーバーを使用していない場合は IP アドレスを入力してください。

■リモート UI で操作する場合

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］をクリックする

6 鍵と証明書の設定をする

a ［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。

b ［署名アルゴリズム］

署名に利用するハッシュ関数を選びます。鍵の長さによって選択できるハッシュ関数が異なります。SHA384 と SHA512 のハッシュ関数をサポートしているのは、1024 ビット以上の長さの鍵です。

c ［鍵のアルゴリズム］

鍵の生成アルゴリズムを［RSA］または［ECDSA］から選びます。［RSA］を選んだ場合は鍵の長さを、［ECDSA］を選んだ場合は鍵の種類を選びます。いずれの場合も数値が大きいほど安全性が高まりますが、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。

d ［有効期限開始日(YYYY/MM/DD)］／［有効期限終了日(YYYY/MM/DD)］

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

e ［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。

f ［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。

g ［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。

h ［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。
本設定はリモート UI からのみ設定できます。

■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)] をクリックする

6 鍵と証明書の必要項目を設定する

a [鍵の名前]

鍵に付ける名前を入力します。一覧表示されたときに探しやすい名前を付けてください。

b [署名アルゴリズム]

署名に利用するハッシュ関数を選びます。

c [鍵のアルゴリズム]

鍵のアルゴリズムを選び、[RSA] の場合は鍵の長さを、[ECDSA] の場合は鍵の種類をドロップダウンリストから指定してください。

d [国/地域名]

国コードを一覧から選択するか、入力によって指定します。

e [都道府県] ／ [市町村]

所在地を入力します。

f [組織] ／ [組織単位]

組織名を入力します。

g [共通名]

IP アドレスまたは FQDN を入力します。

- Windows の環境で IPPS 印刷を行うときは、必ず本機の IP アドレスを入力してください。
- 本機の FQDN を入力する場合は、DNS サーバーが必要です。DNS サーバーを使用していない場合は IP アドレスを入力してください。

7 [OK] をクリックする

➠ CSR のデータが表示されます。

- CSR データをファイルに保存したいときは、[ファイルに保存] をクリックして保存先を選んでください。

MEMO

- CSR を生成した鍵は、鍵と証明書の一覧画面に表示されますが、このままでは使用することができません。この鍵を使用するには、CSR を基に発行された証明書を登録する必要があります。

8 CSR のデータを元に認証局に証明書を発行してもらう

■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 ［証明書］の一覧で、証明書を登録したい鍵の をクリックする

5 ［証明書の登録...］をクリックする

6 証明書を登録する

- ［参照...］をクリックして登録するファイル（証明書）を指定したあと、［登録］をクリックします。

SCEP の場合

SCEP サーバーへ証明書の発行を手動で要求します。
本設定はリモート UI からのみ設定できます。

MEMO

- ［証明書自動発行要求タイマーを有効にする］にチェックを入れている場合、手動で発行要求はできません。チェックマークを外してください。

リモート UI を起動 ▶ ［設定/登録］ ▶ ［デバイス管理］ ▶ ［証明書発行要求設定(SCEP)］ ▶ ［証明書の自動発行要求設定］ ▶ ［証明書自動発行要求タイマーを有効にする］のチェックマークを外して［更新］をクリックしてください。

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］ ▶ ［証明書発行要求設定(SCEP)］をクリックする

4 ［証明書の発行要求］をクリックする

5 証明書の発行要求に必要な項目を設定する

a ［鍵の名前 :］

鍵に付ける名前を入力します。一覧表示されたときに探しやすい名前を付けてください。

b ［署名アルゴリズム :］

署名に利用するハッシュ関数を選びます。

c ［鍵の長さ(bit) :］

鍵の長さを選びます。

d ［組織 :］

組織名を入力します。

e ［共通名 :］

IP アドレスまたは FQDN を入力します。

- Windows の環境で IPPS 印刷を行うときは、必ず本機の IP アドレスを入力してください。
- 本機の FQDN を入力する場合は、DNS サーバーが必要です。DNS サーバーを使用していない場合は IP アドレスを入力してください。

f ［チャレンジパスワード :］

SCEP サーバー側でパスワードが設定されている場合、証明書発行要求のリクエストデータ（PKCS#9）に含まれるチャレンジパスワードを入力します。

g ［鍵の使用先 :］

［TLS］を選びます。

MEMO

- ［用途なし］以外を選択する場合は、あらかじめ各機能を有効な状態にしてください。各機能が無効な状態で証明書の取得に成功した場合、使用先として証明書は割り当てられますが、各機能は自動的には有効に切り替わりません。

6 ［発行要求］をクリックする

7 ［再起動］をクリックする

Step 2：鍵と証明書を再設定する（TLS）

お使いの機種によっては、操作パネルからは操作できません。リモート UI から操作してください。
SCEP の場合は、本手順は不要です。

自己署名証明書／CSR の場合

操作パネルで操作する場合(P. 22)
リモート UI で操作する場合(P. 23)

■操作パネルで操作する場合

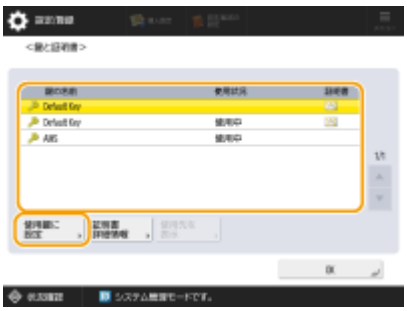
1 （設定/登録）を押す

2 ＜環境設定＞ ▶ ＜ネットワーク＞ ▶ ＜ TCP/IP 設定＞ ▶ ＜ TLS 設定＞を押す

3 ＜鍵と証明書＞を押す

4 TLS 暗号化通信に使う鍵と証明書を選び、＜使用鍵に設定＞ ▶ ＜はい＞を押す

表示例：



- 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。

MEMO

- 機器署名に使用する＜ Device Signature Key ＞と、アクセス制限に使用する＜ AMS ＞は、TLS 暗号化通信に使用できません。

5 ＜ OK ＞を押す

6 （設定/登録） ▶ ＜設定の反映＞ ▶ ＜はい＞を押す

➠ 本機が再起動して、設定が反映されます。

■リモート UI で操作する場合

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 ［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 TLS 暗号化通信に使う鍵と証明書の［使用する］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 ［設定の反映］をクリックして再起動する

➠ 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）

お使いの機種によっては、操作パネルからは操作できません。リモート UI から操作してください。

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. 5)** 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。

操作パネルで操作する場合(P. 24)
リモート UI で操作する場合(P. 25)

■操作パネルで操作する場合

1 （設定/登録）を押す

2 ＜管理設定＞ ▶ ＜デバイス管理＞ ▶ ＜証明書設定＞ ▶ ＜鍵と証明書リスト＞ ▶ ＜本機の鍵と証明書リスト＞を押す

- お使いの機器でユーザー署名機能が有効になっていない場合は、＜本機の鍵と証明書リスト＞は表示されません。次の手順へ進んでください。

3 鍵と証明書を選び、＜削除＞ ▶ ＜はい＞を押す

表示例：

MEMO

- が表示されているときは、鍵が壊れているか無効です。
- が表示されていない場合は、鍵に対する証明書が存在しません。
- 鍵と証明書を選んで＜証明書詳細情報＞を押すと、証明書の詳細情報が表示されます。また、この画面で＜証明書検証＞を押すと、証明書が有効かどうかを検証することができます。

■リモート UI で操作する場合

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 鍵と証明書を選び、［削除］ ▶ ［OK］をクリックする

MEMO

- が表示されているときは、鍵が壊れているか無効です。
- が表示されているときは、鍵に対する証明書が存在しません。
- 鍵の名前をクリックすると、証明書の詳細情報が表示されます。また、この画面で［証明書の検証］をクリックすると、証明書が有効かどうかを検証することができます。

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／SCEP 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／SCEP 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. 29)
Step 2：鍵と証明書を再生成する（IEEE 802.1X）(P. 31)
Step 3：鍵と証明書を再設定する（IEEE 802.1X）(P. 39)
Step 4：以前に生成された鍵／証明書を削除する（IEEE 802.1X）(P. 42)
Step 5：証明書を無効にする（IEEE 802.1X）(P. 44)
Step 6：新しい証明書を有効にする（IEEE 802.1X）(P. 45)

Step 1：認証方式を確認する（IEEE 802.1X）

IEEE 802.1X の認証方式が EAP-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。
お使いの機種によっては、操作パネルからは操作できません。リモート UI から操作してください。

操作パネルで操作する場合(P. 29)
リモート UI で操作する場合(P. 29)

■操作パネルで操作する場合

1 （設定/登録）を押す

2 ＜環境設定＞ ▶ ＜ネットワーク＞ ▶ ＜ IEEE 802.1X 設定＞を押す。

3 ＜次へ＞を押して＜ TLS を使用＞を確認する。

表示例：

- ＜ TLS を使用＞が＜ ON ＞で、＜鍵と証明書＞に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＞が＜ OFF ＞の場合は対応不要です。

■リモート UI で操作する場合

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 ［ネットワーク］ ▶ ［IEEE 802.1X 設定］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、SCEP の 3 つがあります。証明書の種類によって、手順が異なります。
お使いの機種によっては、操作パネルからは操作できません。リモート UI から操作してください。

自己署名証明書の場合(P. 31)
CSR の場合(P. 34)
SCEP の場合(P. 36)

自己署名証明書の場合

操作パネルで操作する場合(P. 31)
リモート UI で操作する場合(P. 32)

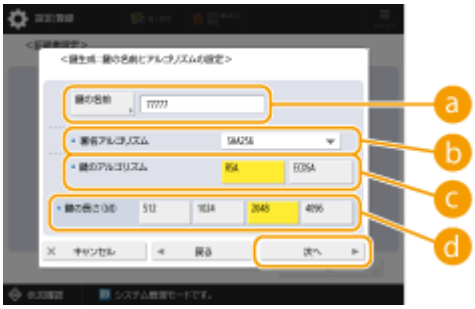
■操作パネルで操作する場合

1 （設定/登録）を押す

2 ＜管理設定＞ ▸ ＜デバイス管理＞ ▸ ＜証明書設定＞ ▸ ＜鍵生成＞ ▸ ＜ネットワーク通信用の鍵生成＞を押す

3 鍵の必要項目を設定し、次の画面に進む

表示例：



a ＜鍵の名前＞

鍵に付ける名前を入力します。一覧表示されたときに探しやすい名前を付けてください。

b ＜署名アルゴリズム＞

署名に利用するハッシュ関数を選びます。鍵の長さによって選択できるハッシュ関数が異なります。SHA384 と SHA512 のハッシュ関数をサポートしているのは、1024 ビット以上の長さの鍵です。c で＜ RSA ＞を選んだあと、d の＜鍵の長さ(bit)＞で＜ 1024 ＞以上を選ぶと SHA384 と SHA512 のハッシュ関数が選べるようになります。

c ＜鍵のアルゴリズム＞

鍵のアルゴリズムを選びます。＜ RSA ＞を選ぶと＜鍵の長さ(bit)＞が、＜ ECDSA ＞を選ぶと＜鍵の種類＞が、ⓓの設定項目として表示されます。

ⓓ＜鍵の長さ(bit)＞／＜鍵の種類＞

ⓒで＜ RSA ＞を選んだ場合は鍵の長さを、＜ ECDSA ＞を選んだ場合は鍵の種類を選びます。いずれの場合も数値が大きいほど安全性が高まりますが、通信時の処理が遅くなります。

4 証明書の必要項目を設定し、＜鍵生成実行＞を押す

表示例：

ⓐ＜有効期限開始日＞／＜有効期限終了日＞

証明書の有効期間の開始日／終了日を入力します。

ⓑ＜国/地域名＞／＜都道府県＞／＜市町村＞／＜組織＞／＜組織単位＞

国コードを一覧から選択し、所在地や組織名を入力します。

ⓒ＜共通名＞

IP アドレスまたは FQDN を入力します。

- Windows の環境で IPPS 印刷を行うときは、必ず本機の IP アドレスを入力してください。
- 本機の FQDN を入力する場合は、DNS サーバーが必要です。DNS サーバーを使用していない場合は IP アドレスを入力してください。

■リモート UI で操作する場合

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］をクリックする

6 鍵と証明書の設定をする

a [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。

b [署名アルゴリズム]

署名に利用するハッシュ関数を選びます。鍵の長さによって選択できるハッシュ関数が異なります。SHA384 と SHA512 のハッシュ関数をサポートしているのは、1024 ビット以上の長さの鍵です。

c [鍵のアルゴリズム]

鍵の生成アルゴリズムを［RSA］または［ECDSA］から選びます。［RSA］を選んだ場合は鍵の長さを、［ECDSA］を選んだ場合は鍵の種類を選びます。いずれの場合も数値が大きいほど安全性が高まりますが、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。

d [有効期限開始日(YYYY/MM/DD)] ／ [有効期限終了日(YYYY/MM/DD)]

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

e [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。

f [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。

g [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。

h [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。
本設定はリモート UI からのみ設定できます。

■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)] をクリックする

6 鍵と証明書の必要項目を設定する

a [鍵の名前]

鍵に付ける名前を入力します。一覧表示されたときに探しやすい名前を付けてください。

b ［署名アルゴリズム］

署名に利用するハッシュ関数を選びます。

c ［鍵のアルゴリズム］

鍵のアルゴリズムを選び、［RSA］の場合は鍵の長さを、［ECDSA］の場合は鍵の種類をドロップダウンリストから指定してください。

d ［国/地域名］

国コードを一覧から選択するか、入力によって指定します。

e ［都道府県］／［市町村］

所在地を入力します。

f ［組織］／［組織単位］

組織名を入力します。

g ［共通名］

IP アドレスまたは FQDN を入力します。

- Windows の環境で IPPS 印刷を行うときは、必ず本機の IP アドレスを入力してください。
- 本機の FQDN を入力する場合は、DNS サーバーが必要です。DNS サーバーを使用していない場合は IP アドレスを入力してください。

7 ［OK］をクリックする

➠ CSR のデータが表示されます。

- CSR データをファイルに保存したいときは、［ファイルに保存］をクリックして保存先を選んでください。

MEMO

- CSR を生成した鍵は、鍵と証明書の一覧画面に表示されますが、このままでは使用することができません。この鍵を使用するには、CSR を基に発行された証明書を登録する必要があります。

8 CSR のデータを元に認証局に証明書を発行してもらう

■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 ［証明書］の一覧で、証明書を登録したい鍵の をクリックする

5 ［証明書の登録...］をクリックする

6 証明書を登録する

- ［参照...］をクリックして登録するファイル（証明書）を指定したあと、［登録］をクリックします。

SCEP の場合

SCEP サーバーへ証明書の発行を手動で要求します。
本設定はリモート UI からのみ設定できます。

MEMO

- ［証明書自動発行要求タイマーを有効にする］にチェックを入れている場合、手動で発行要求はできません。チェックマークを外してください。

リモート UI を起動 ▶ ［設定/登録］ ▶ ［デバイス管理］ ▶ ［証明書発行要求設定(SCEP)］ ▶ ［証明書の自動発行要求設定］ ▶ ［証明書自動発行要求タイマーを有効にする］のチェックマークを外して［更新］をクリックしてください。

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］ ▶ ［証明書発行要求設定(SCEP)］をクリックする

4 ［証明書の発行要求］をクリックする

5 証明書の発行要求に必要な項目を設定する

a ［鍵の名前 :］

鍵に付ける名前を入力します。一覧表示されたときに探しやすい名前を付けてください。

b ［署名アルゴリズム :］

署名に利用するハッシュ関数を選びます。

c ［鍵の長さ(bit) :］

鍵の長さを選びます。

d ［組織 :］

組織名を入力します。

e ［共通名 :］

IP アドレスまたは FQDN を入力します。

- Windows の環境で IPPS 印刷を行うときは、必ず本機の IP アドレスを入力してください。
- 本機の FQDN を入力する場合は、DNS サーバーが必要です。DNS サーバーを使用していない場合は IP アドレスを入力してください。

f ［チャレンジパスワード :］

SCEP サーバー側でパスワードが設定されている場合、証明書発行要求のリクエストデータ（PKCS#9）に含まれるチャレンジパスワードを入力します。

g ［鍵の使用先 :］

［IEEE 802.1X］を選びます。

MEMO

- ［用途なし］以外を選択する場合は、あらかじめ各機能を有効な状態にしてください。各機能が無効な状態で証明書の取得に成功した場合、使用先として証明書は割り当てられますが、各機能は自動的には有効に切り替わりません。

6 ［発行要求］をクリックする

7 ［再起動］をクリックする

Step 3：鍵と証明書を再設定する（IEEE 802.1X）

お使いの機種によっては、操作パネルからは操作できません。リモート UI から操作してください。
SCEP の場合は、本手順は不要です。

自己署名証明書／CSR の場合

操作パネルで操作する場合(P. 39)
リモート UI で操作する場合(P. 40)

■操作パネルで操作する場合

1 （設定/登録）を押す

2 ＜環境設定＞ ▶ ＜ネットワーク＞ ▶ ＜ IEEE 802.1X 設定＞を押す

3 ＜ IEEE 802.1X を使用＞で＜ ON ＞を押し、必要な設定をしたあと、＜次へ＞を押す

表示例：

a ＜ログイン名＞

IEEE 802.1X 認証を受けるログインユーザーの名称（EAP Identity）を入力します。

b ＜認証サーバーの証明書を検証＞

認証サーバーから送られてきたサーバー証明書を検証するときは＜ ON ＞にします。

c ＜認証サーバー名を検証＞

サーバー証明書で共通名（Common Name）を検証するときは＜ ON ＞を選び、＜認証サーバー名＞でログインユーザーが登録されている認証サーバーの名称を入力します。

4 ＜ TLS を使用＞で＜ ON ＞を押し、＜鍵と証明書＞を押す

5 一覧から使用する鍵と証明書を選び、＜使用鍵に設定＞ ▶ ＜はい＞を押す

6 **＜OK＞を押す**

7 **（設定/登録）▶（設定/登録）▶＜設定の反映＞▶＜はい＞を押す**

➠ 本機が再起動して、設定が反映されます。

■リモート UI で操作する場合

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 **［ネットワーク］▶［IEEE 802.1X 設定］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、必要な設定をする**

a ［ログイン名］

IEEE 802.1X 認証を受けるログインユーザーの名称（EAP Identity）を入力します。

b ［認証サーバーの証明書を検証する］

認証サーバーから送られてきたサーバー証明書を検証するときはチェックマークを付けます。

c ［認証サーバー名を検証する］

サーバー証明書で共通名（Common Name）を検証するときはチェックマークを付け、［認証サーバー名］でログインユーザーが登録されている認証サーバーの名称を入力します。

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 一覧から使用する鍵の［使用する］をクリックする

7 ［OK］をクリックする

8 ［設定の反映］をクリックして再起動する

➠ 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）

お使いの機種によっては、操作パネルからは操作できません。リモート UI から操作してください。

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. 5)** 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。

操作パネルで操作する場合(P. 42)
リモート UI で操作する場合(P. 43)

■操作パネルで操作する場合

1 （設定/登録）を押す

2 ＜管理設定＞▶＜デバイス管理＞▶＜証明書設定＞▶＜鍵と証明書リスト＞▶＜本機の鍵と証明書リスト＞を押す

- お使いの機器でユーザー署名機能が有効になっていない場合は、＜本機の鍵と証明書リスト＞は表示されません。次の手順へ進んでください。

3 鍵と証明書を選び、＜削除＞▶＜はい＞を押す

表示例：

MEMO

- が表示されているときは、鍵が壊れているか無効です。
- が表示されていない場合は、鍵に対する証明書が存在しません。
- 鍵と証明書を選んで＜証明書詳細情報＞を押すと、証明書の詳細情報が表示されます。また、この画面で＜証明書検証＞を押すと、証明書が有効かどうかを検証することができます。

■リモート UI で操作する場合

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 鍵と証明書を選び、［削除］ ▶ ［OK］をクリックする

MEMO

- が表示されているときは、鍵が壊れているか無効です。
- が表示されているときは、鍵に対する証明書が存在しません。
- 鍵の名前をクリックすると、証明書の詳細情報が表示されます。また、この画面で［証明書の検証］をクリックすると、証明書が有効かどうかを検証することができます。

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／SCEP 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／SCEP 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. 47)
Step 2：鍵と証明書を再生成する（IPSec）(P. 49)
Step 3：鍵と証明書を再設定する（IPSec）(P. 57)
Step 4：以前に生成された鍵／証明書を削除する（IPSec）(P. 59)
Step 5：証明書を無効にする（IPSec）(P. 61)
Step 6：新しい証明書を有効にする（IPSec）(P. 62)

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。
お使いの機種によっては、操作パネルからは操作できません。リモート UI から操作してください。

操作パネルで操作する場合(P. 47)
リモート UI で操作する場合(P. 48)

■操作パネルで操作する場合

1 （設定/登録）を押す

2 ＜環境設定＞ ▶ ＜ネットワーク＞ ▶ ＜ TCP/IP 設定＞ ▶ ＜ IPSec 設定＞を押す

3 登録済のポリシーを選択して、＜編集＞ ▶ ＜ IKE 設定＞を押す

表示例：

4 ＜次へ＞を押して＜認証方式＞を確認する。

表示例：

- ＜認証方式＞が＜電子署名方式＞で、＜鍵と証明書＞に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。

■リモート UI で操作する場合

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 ［ネットワーク］▶［IPSec ポリシー一覧］をクリックする

4 一覧からポリシーをクリック▶［IKE 設定］をクリックする

5 ［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、SCEP の 3 つがあります。証明書の種類によって、手順が異なります。
お使いの機種によっては、操作パネルからは操作できません。リモート UI から操作してください。

自己署名証明書の場合(P. 49)
CSR の場合(P. 52)
SCEP の場合(P. 54)

自己署名証明書の場合

操作パネルで操作する場合(P. 49)
リモート UI で操作する場合(P. 50)

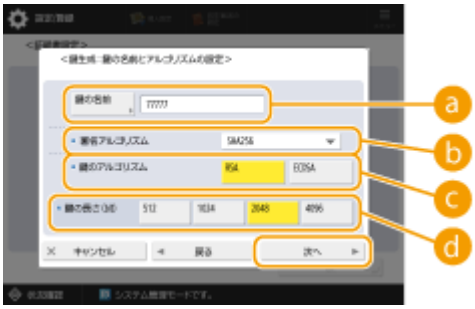
■操作パネルで操作する場合

1 （設定/登録）を押す

2 ＜管理設定＞ ▶ ＜デバイス管理＞ ▶ ＜証明書設定＞ ▶ ＜鍵生成＞ ▶ ＜ネットワーク通信用の鍵生成＞を押す

3 鍵の必要項目を設定し、次の画面に進む

表示例：



a ＜鍵の名前＞

鍵に付ける名前を入力します。一覧表示されたときに探しやすい名前を付けてください。

b ＜署名アルゴリズム＞

署名に利用するハッシュ関数を選びます。鍵の長さによって選択できるハッシュ関数が異なります。SHA384 と SHA512 のハッシュ関数をサポートしているのは、1024 ビット以上の長さの鍵です。c で＜ RSA ＞を選んだあと、d の＜鍵の長さ(bit)＞で＜ 1024 ＞以上を選ぶと SHA384 と SHA512 のハッシュ関数が選べるようになります。

c ＜鍵のアルゴリズム＞

鍵のアルゴリズムを選びます。＜ RSA ＞を選ぶと＜鍵の長さ(bit)＞が、＜ ECDSA ＞を選ぶと＜鍵の種類＞が、ⓓの設定項目として表示されます。

ⓓ＜鍵の長さ(bit)＞／＜鍵の種類＞

ⓒで＜ RSA ＞を選んだ場合は鍵の長さを、＜ ECDSA ＞を選んだ場合は鍵の種類を選びます。いずれの場合も数値が大きいほど安全性が高まりますが、通信時の処理が遅くなります。

4 証明書の必要項目を設定し、＜鍵生成実行＞を押す

表示例：

ⓐ＜有効期限開始日＞／＜有効期限終了日＞

証明書の有効期間の開始日／終了日を入力します。

ⓑ＜国/地域名＞／＜都道府県＞／＜市町村＞／＜組織＞／＜組織単位＞

国コードを一覧から選択し、所在地や組織名を入力します。

ⓒ＜共通名＞

IP アドレスまたは FQDN を入力します。

- Windows の環境で IPPS 印刷を行うときは、必ず本機の IP アドレスを入力してください。
- 本機の FQDN を入力する場合は、DNS サーバーが必要です。DNS サーバーを使用していない場合は IP アドレスを入力してください。

■リモート UI で操作する場合

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］をクリックする

6 鍵と証明書の設定をする

a ［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。

b ［署名アルゴリズム］

署名に利用するハッシュ関数を選びます。鍵の長さによって選択できるハッシュ関数が異なります。SHA384 と SHA512 のハッシュ関数をサポートしているのは、1024 ビット以上の長さの鍵です。

c ［鍵のアルゴリズム］

鍵の生成アルゴリズムを［RSA］または［ECDSA］から選びます。［RSA］を選んだ場合は鍵の長さを、［ECDSA］を選んだ場合は鍵の種類を選びます。いずれの場合も数値が大きいほど安全性が高まりますが、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。

d ［有効期限開始日(YYYY/MM/DD)］／［有効期限終了日(YYYY/MM/DD)］

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

e ［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。

f ［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。

g ［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。

h ［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。
本設定はリモート UI からのみ設定できます。

■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)] をクリックする

6 鍵と証明書の必要項目を設定する

a [鍵の名前]

鍵に付ける名前を入力します。一覧表示されたときに探しやすい名前を付けてください。

b [署名アルゴリズム]

署名に利用するハッシュ関数を選びます。

c [鍵のアルゴリズム]

鍵のアルゴリズムを選び、[RSA] の場合は鍵の長さを、[ECDSA] の場合は鍵の種類をドロップダウンリストから指定してください。

d [国/地域名]

国コードを一覧から選択するか、入力によって指定します。

e [都道府県] ／ [市町村]

所在地を入力します。

f [組織] ／ [組織単位]

組織名を入力します。

g [共通名]

IP アドレスまたは FQDN を入力します。

- Windows の環境で IPPS 印刷を行うときは、必ず本機の IP アドレスを入力してください。
- 本機の FQDN を入力する場合は、DNS サーバーが必要です。DNS サーバーを使用していない場合は IP アドレスを入力してください。

7 [OK] をクリックする

➡ CSR のデータが表示されます。

- CSR データをファイルに保存したいときは、[ファイルに保存] をクリックして保存先を選んでください。

MEMO

- CSR を生成した鍵は、鍵と証明書の一覧画面に表示されますが、このままでは使用することができません。この鍵を使用するには、CSR を基に発行された証明書を登録する必要があります。

8 CSR のデータを元に認証局に証明書を発行してもらう

■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 ［証明書］の一覧で、証明書を登録したい鍵の をクリックする

5 ［証明書の登録...］をクリックする

6 証明書を登録する

- ［参照...］をクリックして登録するファイル（証明書）を指定したあと、［登録］をクリックします。

SCEP の場合

SCEP サーバーへ証明書の発行を手動で要求します。
本設定はリモート UI からのみ設定できます。

MEMO

- ［証明書自動発行要求タイマーを有効にする］にチェックを入れている場合、手動で発行要求はできません。チェックマークを外してください。

リモート UI を起動 ▶ ［設定/登録］ ▶ ［デバイス管理］ ▶ ［証明書発行要求設定(SCEP)］ ▶ ［証明書の自動発行要求設定］ ▶ ［証明書自動発行要求タイマーを有効にする］のチェックマークを外して［更新］をクリックしてください。

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］ ▶ ［証明書発行要求設定(SCEP)］をクリックする

4 [証明書の発行要求] をクリックする

5 証明書の発行要求に必要な項目を設定する

a [鍵の名前 :]

鍵に付ける名前を入力します。一覧表示されたときに探しやすい名前を付けてください。

b [署名アルゴリズム :]

署名に利用するハッシュ関数を選びます。

c [鍵の長さ(bit) :]

鍵の長さを選びます。

d [組織 :]

組織名を入力します。

e [共通名 :]

IP アドレスまたは FQDN を入力します。

- Windows の環境で IPPS 印刷を行うときは、必ず本機の IP アドレスを入力してください。
- 本機の FQDN を入力する場合は、DNS サーバーが必要です。DNS サーバーを使用していない場合は IP アドレスを入力してください。

f [チャレンジパスワード :]

SCEP サーバー側でパスワードが設定されている場合、証明書発行要求のリクエストデータ（PKCS#9）に含まれるチャレンジパスワードを入力します。

g [鍵の使用先 :]

[IPSec] を選びます。

MEMO

- ［用途なし］以外を選択する場合は、あらかじめ各機能を有効な状態にしてください。各機能が無効な状態で証明書の取得に成功した場合、使用先として証明書は割り当てられますが、各機能は自動的には有効に切り替わりません。

6 ［発行要求］をクリックする

7 ［再起動］をクリックする

Step 3：鍵と証明書を再設定する（IPSec）

お使いの機種によっては、操作パネルからは操作できません。リモート UI から操作してください。
SCEP の場合は、本手順は不要です。

自己署名証明書／CSR の場合

操作パネルで操作する場合(P. 57)
リモート UI で操作する場合(P. 58)

■操作パネルで操作する場合

1 （設定/登録）を押す

2 ＜環境設定＞ ▶ ＜ネットワーク＞ ▶ ＜ TCP/IP 設定＞ ▶ ＜ IPSec 設定＞を押す

3 鍵と証明書を再設定するポリシーを選択して、＜編集＞ ▶ ＜ IKE 設定＞を押す

表示例：

4 ＜次へ＞を押して＜認証方式＞で＜電子署名方式＞ ▶ ＜鍵と証明書＞を押す

表示例：

5 一覧から使用する鍵と証明書を選び、＜使用鍵に設定＞ ▶ ＜はい＞を押す

6 **＜OK＞を押す**

7 **（設定/登録）▶（設定/登録）▶＜設定の反映＞▶＜はい＞を押す**

➠本機が再起動して、設定が反映されます。

■リモート UI で操作する場合

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 **［ネットワーク］▶［IPSec ポリシー一覧］をクリックする**

4 **一覧から鍵と証明書を再設定するポリシーをクリック▶［IKE 設定］をクリックする**

5 **［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**

6 **一覧から使用する鍵の［使用する］をクリックする**

7 **［OK］をクリックする**

8 **［設定の反映］をクリックして再起動する**

➠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）

お使いの機種によっては、操作パネルからは操作できません。リモート UI から操作してください。

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. 5)** 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。

操作パネルで操作する場合(P. 59)
リモート UI で操作する場合(P. 60)

■操作パネルで操作する場合

1 （設定/登録）を押す

2 ＜管理設定＞▶＜デバイス管理＞▶＜証明書設定＞▶＜鍵と証明書リスト＞▶＜本機の鍵と証明書リスト＞を押す

- お使いの機器でユーザー署名機能が有効になっていない場合は、＜本機の鍵と証明書リスト＞は表示されません。次の手順へ進んでください。

3 鍵と証明書を選び、＜削除＞▶＜はい＞を押す

表示例：

MEMO

- が表示されているときは、鍵が壊れているか無効です。
- が表示されていない場合は、鍵に対する証明書が存在しません。
- 鍵と証明書を選んで＜証明書詳細情報＞を押すと、証明書の詳細情報が表示されます。また、この画面で＜証明書検証＞を押すと、証明書が有効かどうかを検証することができます。

■リモート UI で操作する場合

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 鍵と証明書を選び、［削除］ ▶ ［OK］をクリックする

MEMO

- が表示されているときは、鍵が壊れているか無効です。
- が表示されているときは、鍵に対する証明書が存在しません。
- 鍵の名前をクリックすると、証明書の詳細情報が表示されます。また、この画面で［証明書の検証］をクリックすると、証明書が有効かどうかを検証することができます。

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／SCEP 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／SCEP の場合

対応は不要です。

対応実施手順：SIP

Step 1：SIP の設定を確認する（SIP）(P. 64)
Step 2：鍵と証明書を再生成する（SIP）(P. 67)
Step 3：鍵と証明書を再設定する（SIP）(P. 73)
Step 4：以前に生成された鍵／証明書を削除する（SIP）(P. 76)
Step 5：証明書を無効にする（SIP）(P. 78)
Step 6：新しい証明書を有効にする（SIP）(P. 79)

Step 1：SIP の設定を確認する（SIP）

以下の両方を満たす場合に対策が必要です。

- ＜SIP 設定＞の＜イントラネット設定＞で＜TLS を使用＞が ON になっている
- ＜SIP 設定＞の＜TLS 設定＞で＜鍵と証明書＞に鍵の名称が表示されている

以下の手順に従って、設定をご確認ください。

操作パネルで操作する場合(P. 64)
リモート UI で操作する場合(P. 65)

操作パネルで操作する場合

■＜TLS を使用＞の確認

1 （設定/登録）を押す

2 ＜環境設定＞▶＜ネットワーク＞▶＜TCP/IP 設定＞▶＜SIP 設定＞▶＜イントラネット設定＞を押す

3 ＜TLS を使用＞を確認する

表示例：

- ＜TLS を使用＞が＜ON＞の場合は＜鍵と証明書＞の確認へ進みます。
- ＜TLS を使用＞が＜OFF＞の場合は対応不要です。

■＜鍵と証明書＞の確認

1 （設定/登録）を押す

2 ＜環境設定＞▶＜ネットワーク＞▶＜TCP/IP 設定＞▶＜SIP 設定＞▶＜TLS 設定＞を押す

3 ＜鍵と証明書＞に鍵の名称が表示されているかを確認する

表示例：

- ＜鍵と証明書＞に鍵の名称が表示されている場合は以降の対応をします。
- ＜鍵と証明書＞に鍵の名称が表示されていない場合は対応不要です。

リモート UI で操作する場合

■［TLS を使用する］と［鍵と証明書］の確認

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］ ▶ ［SIP 設定］をクリックする

4 ［イントラネット設定］の［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る場合は［鍵と証明書］の確認へ進みます。
- ［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。

5 ［TLS 設定］の［鍵の名前］を確認する

- 鍵の名前が表示されている場合は以降の対応をします。
- 鍵の名前が表示され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（SIP）

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。
お使いの機種によっては、操作パネルからは操作できません。リモート UI から操作してください。

自己署名証明書の場合(P. 67)
CSR の場合(P. 70)

自己署名証明書の場合

操作パネルで操作する場合(P. 67)
リモート UI で操作する場合(P. 68)

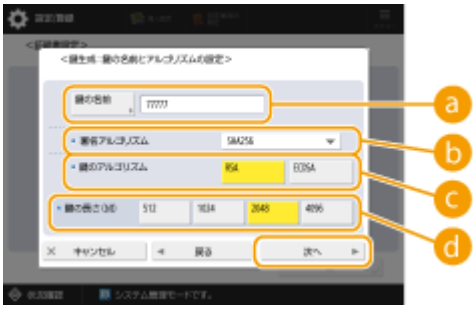
■操作パネルで操作する場合

1 （設定/登録）を押す

2 ＜管理設定＞ ▶ ＜デバイス管理＞ ▶ ＜証明書設定＞ ▶ ＜鍵生成＞ ▶ ＜ネットワーク通信用の鍵生成＞を押す

3 鍵の必要項目を設定し、次の画面に進む

表示例：



a ＜鍵の名前＞

鍵に付ける名前を入力します。一覧表示されたときに探しやすい名前を付けてください。

b ＜署名アルゴリズム＞

署名に利用するハッシュ関数を選びます。鍵の長さによって選択できるハッシュ関数が異なります。SHA384 と SHA512 のハッシュ関数をサポートしているのは、1024 ビット以上の長さの鍵です。c で＜ RSA ＞を選んだあと、d の＜鍵の長さ(bit)＞で＜ 1024 ＞以上を選ぶと SHA384 と SHA512 のハッシュ関数が選べるようになります。

c ＜鍵のアルゴリズム＞

鍵のアルゴリズムを選びます。＜ RSA ＞を選ぶと＜鍵の長さ(bit)＞が、＜ ECDSA ＞を選ぶと＜鍵の種類＞が、d の設定項目として表示されます。

d ＜鍵の長さ(bit)＞／＜鍵の種類＞

c で＜ RSA ＞を選んだ場合は鍵の長さを、＜ ECDSA ＞を選んだ場合は鍵の種類を選びます。いずれの場合も数値が大きいほど安全性が高まりますが、通信時の処理が遅くなります。

4 証明書の必要項目を設定し、＜鍵生成実行＞を押す

表示例：

a ＜有効期限開始日＞／＜有効期限終了日＞

証明書の有効期間の開始日／終了日を入力します。

b ＜国/地域名＞／＜都道府県＞／＜市町村＞／＜組織＞／＜組織単位＞

国コードを一覧から選択し、所在地や組織名を入力します。

c ＜共通名＞

IP アドレスまたは FQDN を入力します。

- Windows の環境で IPPS 印刷を行うときは、必ず本機の IP アドレスを入力してください。
- 本機の FQDN を入力する場合は、DNS サーバーが必要です。DNS サーバーを使用していない場合は IP アドレスを入力してください。

■リモート UI で操作する場合

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］をクリックする

6 鍵と証明書の設定をする

a ［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。

b ［署名アルゴリズム］

署名に利用するハッシュ関数を選びます。鍵の長さによって選択できるハッシュ関数が異なります。SHA384 と SHA512 のハッシュ関数をサポートしているのは、1024 ビット以上の長さの鍵です。

c ［鍵のアルゴリズム］

鍵の生成アルゴリズムを［RSA］または［ECDSA］から選びます。［RSA］を選んだ場合は鍵の長さを、［ECDSA］を選んだ場合は鍵の種類を選びます。いずれの場合も数値が大きいほど安全性が高まりますが、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。

d ［有効期限開始日(YYYY/MM/DD)］／［有効期限終了日(YYYY/MM/DD)］

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

e ［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。

f ［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。

g ［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。

h ［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。
本設定はリモート UI からのみ設定できます。

■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)］をクリックする

6 鍵と証明書の必要項目を設定する

a ［鍵の名前］

鍵に付ける名前を入力します。一覧表示されたときに探しやすい名前を付けてください。

b ［署名アルゴリズム］

署名に利用するハッシュ関数を選びます。

c ［鍵のアルゴリズム］

鍵のアルゴリズムを選び、［RSA］の場合は鍵の長さを、［ECDSA］の場合は鍵の種類をドロップダウンリストから指定してください。

d ［国/地域名］

国コードを一覧から選択するか、入力によって指定します。

e ［都道府県］／［市町村］

所在地を入力します。

f ［組織］／［組織単位］

組織名を入力します。

g ［共通名］

IP アドレスまたは FQDN を入力します。

- Windows の環境で IPPS 印刷を行うときは、必ず本機の IP アドレスを入力してください。
- 本機の FQDN を入力する場合は、DNS サーバーが必要です。DNS サーバーを使用していない場合は IP アドレスを入力してください。

7 ［OK］をクリックする

➡CSR のデータが表示されます。

- CSR データをファイルに保存したいときは、［ファイルに保存］をクリックして保存先を選んでください。

MEMO

- CSR を生成した鍵は、鍵と証明書の一覧画面に表示されますが、このままでは使用することができません。この鍵を使用するには、CSR を基に発行された証明書を登録する必要があります。

8 CSR のデータを元に認証局に証明書を発行してもらう

■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 ［証明書］の一覧で、証明書を登録したい鍵の をクリックする

5 ［証明書の登録...］をクリックする

6 証明書を登録する

- ［参照...］をクリックして登録するファイル（証明書）を指定したあと、［登録］をクリックします。

Step 3：鍵と証明書を再設定する（SIP）

生成した鍵と証明書を SIP の TLS 暗号化通信で使用する鍵と証明書として設定します。

操作パネルで操作する場合(P. 73)
リモート UI で操作する場合(P. 74)

■操作パネルで操作する場合

1 （設定/登録）を押す

2 ＜環境設定＞ ▶ ＜ネットワーク＞ ▶ ＜ TCP/IP 設定＞ ▶ ＜ SIP 設定＞ ▶ ＜ TLS 設定＞を押す

3 ＜受信時設定＞と＜送信時設定＞の各項目を設定 ▶ ＜鍵と証明書＞を押す

表示例：

＜受信時設定＞	
＜クライアント認証を要求する＞	＜ ON ＞または＜ OFF ＞を選択します。 ＜ ON ＞を選択すると、IP ファクス受信時にクライアント認証を要求します。
＜送信時設定＞	
＜サーバー証明書を検証する＞	＜ ON ＞または＜ OFF ＞を選択します。 ＜ ON ＞を選択すると、IP ファクス受信時に、TLS サーバー証明書が正規のものであるかどうかの確認をします。
＜ CN を検証する＞	＜ ON ＞または＜ OFF ＞を選択します。 ＜ ON ＞を選択すると、IP ファクス受信時に CN（Common Name）を確認します。

4 SIP の TLS 暗号化通信に使用したい鍵と証明書を選択 ▶ ＜使用鍵に設定＞ ▶ ＜ OK ＞を押す

表示例：

MEMO

- 使用状況が「使用中」の場合は、選択できません。
- ［証明書詳細情報］を押すと、証明書の詳細情報を確認できます。
- ［使用先を表示］を押すと、使用中の鍵と証明書の用途を確認できます。

5 ＜OK＞を押す

6 （設定/登録） ▶ （設定/登録） ▶ ＜設定の反映＞ ▶ ＜はい＞を押す

➠本機が再起動して、設定が反映されます。

■リモート UI で操作する場合

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 ［ネットワーク］ ▶ ［SIP 設定］をクリックする

4 ［TLS 設定］の各項目を設定 ▶ ［鍵と証明書］をクリックする

[受信時設定]	
[クライアント認証を要求する]	チェックマークを付けると、IP ファクス受信時にクライアント認証を要求します。
[送信時設定]	
[サーバー証明書を検証する]	チェックマークを付けると、IP ファクス受信時に、TLS サーバー証明書が正規のものであるかどうかの確認をします。
[CN を検証項目に追加する]	[ON] または [OFF] を選択します。 チェックマークを付けると、IP ファクス受信時に CN（Common Name）を確認します。

5 一覧から使用する鍵の［使用する］をクリックする

6 ［OK］をクリックする

7 ［設定の反映］をクリックして再起動する

➠ 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（SIP）

お使いの機種によっては、操作パネルからは操作できません。リモート UI から操作してください。

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. 5)** 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。

操作パネルで操作する場合(P. 76)
リモート UI で操作する場合(P. 77)

■操作パネルで操作する場合

1 （設定/登録）を押す

2 ＜管理設定＞ ▶ ＜デバイス管理＞ ▶ ＜証明書設定＞ ▶ ＜鍵と証明書リスト＞ ▶ ＜本機の鍵と証明書リスト＞を押す

- お使いの機器でユーザー署名機能が有効になっていない場合は、＜本機の鍵と証明書リスト＞は表示されません。次の手順へ進んでください。

3 鍵と証明書を選び、＜削除＞ ▶ ＜はい＞を押す

表示例：

MEMO

- が表示されているときは、鍵が壊れているか無効です。
- が表示されていない場合は、鍵に対する証明書が存在しません。
- 鍵と証明書を選んで＜証明書詳細情報＞を押すと、証明書の詳細情報が表示されます。また、この画面で＜証明書検証＞を押すと、証明書が有効かどうかを検証することができます。

■リモート UI で操作する場合

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 鍵と証明書を選び、［削除］ ▶ ［OK］をクリックする

MEMO

- が表示されているときは、鍵が壊れているか無効です。
- が表示されているときは、鍵に対する証明書が存在しません。
- 鍵の名前をクリックすると、証明書の詳細情報が表示されます。また、この画面で［証明書の検証］をクリックすると、証明書が有効かどうかを検証することができます。

Step 5：証明書を無効にする（SIP）

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通信相手の IP ファクス機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。

- 通信相手の IP ファクス機で、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（SIP）

証明書を有効にします。

■自己署名証明書の場合

新しい証明書を通信相手の IP ファクス機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：S/MIME の設定を確認する（機器署名）(P. 81)
Step 2：鍵と証明書を再設定する（機器署名）(P. 83)
Step 3：証明書を無効にする（機器署名）(P. 84)
Step 4：新しい証明書を有効にする（機器署名）(P. 85)

Step 1：S/MIME の設定を確認する（機器署名）

機器署名の対応に加えて S/MIME の対応が必要か確認します。

以下の手順に従って、S/MIME 設定をご確認ください。

操作パネルで操作する場合(P. 81)
リモート UI で操作する場合(P. 81)

■操作パネルで操作する場合

1 （設定/登録）を押す

2 ＜ファンクション設定＞ ▶ ＜送信＞ ▶ ＜ E メール/I ファクス設定＞ ▶ ＜ S/MIME 設定＞を押す

3 ＜暗号化設定＞と＜デジタル署名をつける＞を確認する

表示例：

- ＜暗号化設定＞が＜暗号化しない＞、＜デジタル署名をつける＞が＜ OFF ＞に設定されている場合は機器署名の対応のみ実施します。
- 上記の設定以外になっている場合は、機器署名の対応に加えて、S/MIME の対応も実施します。

■リモート UI で操作する場合

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 ［送信］ ▶ ［S/MIME 設定］をクリックする

4 ［暗号化設定］と［デジタル署名をつける］を確認する

- ［暗号化設定］が［暗号化しない］にチェックマークが付いていて、［デジタル署名をつける］にチェックマークが付いていない場合は機器署名の対応のみ実施します。
- 上記の設定以外になっている場合は、機器署名の対応に加えて、S/MIME の対応も実施します。

Step 2：鍵と証明書を再設定する（機器署名）

操作パネルで操作する場合(P. 83)
リモート UI で操作する場合(P. 83)

■操作パネルで操作する場合

1 （設定/登録）を押す

2 ＜管理設定＞ ▶ ＜デバイス管理＞ ▶ ＜証明書設定＞ ▶ ＜鍵生成＞を押す

3 ＜機器署名の鍵生成/更新＞ ▶ ＜はい＞ ▶ ＜ OK ＞を押す

■リモート UI で操作する場合

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］ ▶ ［機器署名］をクリックする

5 ［鍵生成/更新］ ▶ ［OK］をクリックする

Step 3：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。

■本機からエクスポートした S/MIME 証明書が他の機器にインポートされている場合

本機から S/MIME による E メールや I ファクスの暗号化で使用する公開鍵証明書（S/MIME 証明書）をエクスポートして、他の機器にインポートしていた場合は、以下の手順でインポート先から削除します。

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］ ▶ ［S/MIME 証明書設定］をクリックする

4 該当する証明書を選択 ▶ ［削除］ ▶ ［OK］をクリックする

Step 4：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、再生成した機器署名用の証明書をエクスポートし、Acrobat に登録してください。

本機でのエクスポート手順(P. 85)

■本機からエクスポートした S/MIME 証明書が他の機器にインポートされている場合

本機から S/MIME による E メールや I ファクスの暗号化で使用する公開鍵証明書（S/MIME 証明書）をエクスポートして、他の機器にインポートしていた場合は、再生成した証明書をエクスポートし、通信先に登録してください。

本機でのエクスポート手順(P. 85)
通信先への登録手順(P. 85)

■本機でのエクスポート手順

エクスポートは以下の手順で実施します。

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］ ▶ ［機器署名鍵のエクスポート］をクリックする

4 ［エクスポート開始］をクリックして任意の場所に保存する

■通信先への登録手順

通信先の本体へ以下の手順で登録します。

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］ ▶ ［S/MIME 証明書設定］をクリックする

4 ［S/MIME 証明書登録］をクリックする

5 S/MIME 証明書を登録する

- ［参照...］をクリックして登録するファイル（S/MIME 証明書）を指定したあと、［登録］をクリックします。

Bluetooth 設定の対応を実施する

Bluetooth 設定の対応を実施する 88
対応実施手順：Bluetooth 89
Step 1：Canon PRINT Business に登録済のデバイスを削除する（Bluetooth） 90
Step 2：Canon PRINT Business にデバイスを再登録する（Bluetooth） 91

Bluetooth 設定の対応を実施する

Bluetooth 用の鍵はファームウェアアップデート後に自動更新されます。モバイルアプリケーション Canon PRINT Business をお使いの場合は、デバイスの再登録が必要になります。

対応実施手順：Bluetooth(P. 89)

対応実施手順：Bluetooth

Step 1：Canon PRINT Business に登録済のデバイスを削除する（Bluetooth）(P. 90)
Step 2：Canon PRINT Business にデバイスを再登録する（Bluetooth）(P. 91)

Step 1：Canon PRINT Business に登録済のデバイスを削除する（Bluetooth）

Bluetooth 設定が＜ ON ＞の場合は、以下の手順に従って対応してください。

iOS での操作(P. 90)
Android での操作(P. 90)

■iOS での操作

1 Canon PRINT Business のホーム画面左上の［ ］をタップします。

［プリンター選択］画面が表示されます。

2 ［ ］をタップしたあと、表示される［削除］をタップすると、リストからデバイスを削除できます。

■Android での操作

1 Canon PRINT Business のホーム画面左上の［ ］をタップします。

［プリンター選択］画面が表示されます。

2 デバイス名を長押ししたあと、表示されるダイアログで［削除］をタップします。

Step 2：Canon PRINT Business にデバイスを再登録する（Bluetooth）

Bluetooth 設定が＜ ON ＞の場合は、以下の手順に従って対応してください。

iOS での操作(P. 91)
Android での操作(P. 91)

■iOS での操作

1 Canon PRINT Business のホーム画面左上の［ ］をタップします。

［プリンター選択］画面が表示されます。

2 ［近くのプリンター］をタップします。

検出されたデバイスが表示されます。

■デバイスが検出されない場合

デバイスが見える位置まで近づいて、［再検索］をタップしてください。Bluetooth でデバイスを検出できる距離の目安は、2m/80 インチです。

3 デバイスを選択 ▶ ［追加］をタップします。

■Android での操作

1 Canon PRINT Business のホーム画面左上の［ ］をタップします。

［プリンター選択］画面が表示されます。

2 ［近くのプリンター］をタップします。

検出されたデバイスが表示されます。

■デバイスが検出されない場合

デバイスが見える位置まで近づいて、［再検索］をタップしてください。Bluetooth でデバイスを検出できる距離の目安は、2m/80 インチです。

3 デバイスを選択します。

4 表示されるダイアログでデバイス情報を確認 ▶ ［追加］をタップします。

Wi-Fi ネットワークの設定画面が表示された場合は、画面に従って設定してください。

ACCESS MANAGEMENT SYSTEM 設定の対応を実施する

ACCESS MANAGEMENT SYSTEM 設定の対応を実施する 93
対応実施手順：ACCESS MANAGEMENT SYSTEM 94

ACCESS MANAGEMENT SYSTEM 設定の対応を実施する

ACCESS MANAGEMENT SYSTEM 用の鍵はファームウェアアップデート後に自動更新されます。

鍵の自動更新後、約 30 分が経過すると、制限情報が自動的に再取得されます。これにより、ACCESS MANAGEMENT SYSTEM 機能で正常に印刷できるようになります。

ファームウェアのアップデート後すぐに、プリンタードライバーの ACCESS MANAGEMENT SYSTEM 機能で印刷したい場合は、ACCESS MANAGEMENT SYSTEM の制限情報を手動で再取得する必要があります。

対応実施手順：ACCESS MANAGEMENT SYSTEM(P. 94)

制限情報を再取得せずに印刷するとエラー終了します。

対応実施手順：ACCESS MANAGEMENT SYSTEM

ファームウェアのアップデート後すぐに、プリンタードライバーの ACCESS MANAGEMENT SYSTEM 機能で印刷したい場合は、ACCESS MANAGEMENT SYSTEM の制限情報を手動で再取得する必要があります。

以下の手順に従って対応してください。

ファームウェアのアップデート後、約 30 分が経過すると、自動で制限情報が再取得されるため、以下の手順は不要です。

1 コンピューターにログオンします。

2 ACCESS MANAGEMENT SYSTEM 機能を有効化したプリンタードライバーを使用するプリンターのプロパティを表示します。

■Windows Vista の場合

- ［スタート］ ▶ ［コントロールパネル］ ▶ ［ハードウェアとサウンド］ ▶ ［プリンタ］を選択します。
- プリンターのアイコンを右クリックし、［プロパティ］を選択します。

■Windows Server 2008 の場合

- ［スタート］ ▶ ［コントロールパネル］ ▶ ［ハードウェアとサウンド］ ▶ ［プリンター］を選択します。
- プリンターのアイコンを右クリックし、［プロパティ］を選択します。

■Windows Server 2008 R2 の場合

- ［スタート］ ▶ ［コントロールパネル］ ▶ ［ハードウェア］ ▶ ［デバイスとプリンター］を選択します。
- プリンターのアイコンを右クリックし、［プリンターのプロパティ］を選択します。

■Windows 7 の場合

- ［スタート］ ▶ ［コントロールパネル］ ▶ ［ハードウェアとサウンド］ ▶ ［デバイスとプリンター］を選択します。
- プリンターのアイコンを右クリックし、［プリンターのプロパティ］を選択します。

■Windows 8.1/Windows Server 2012 の場合

- デスクトップに移動し、画面右側のチャームを表示します。
- ［設定］ ▶ ［コントロールパネル］ ▶ ［デバイスとプリンターの表示］を選択します。
- プリンターのアイコンを右クリックし、［プリンターのプロパティ］を選択します。

■Windows 10/Windows Server 2016 の場合

- ［スタート］を右クリックし、［コントロールパネル］ ▶ ［デバイスとプリンターの表示］を選択します。
- プリンターのアイコンを右クリックし、［プリンターのプロパティ］を選択します。

3 ［AMS］タブをクリックします

4 ［制限情報の取得］をクリック

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.