關於 RSA 金鑰產生脆弱性的應對措施

USRM3-1253-00 2022-03 zh

目錄

前言 2

檢查您是否必須執行附加程序 5

RSA 金鑰用途和附加程序 11

TLS 的程序 12

步驟 1：重新產生金鑰和憑證 (TLS) 13

步驟 2：重設金鑰和憑證 (TLS) 20

步驟 3：刪除過去產生的金鑰/憑證 (TLS) 22

步驟 4：停用憑證 (TLS) 24

步驟 5：啟用新憑證 (TLS) 25

IEEE 802.1X 的程序 26

步驟 1：檢查認證方法 (IEEE 802.1X) 27

步驟 2：重新產生金鑰和憑證 (IEEE 802.1X) 29

步驟 3：重設金鑰和憑證 (IEEE 802.1X) 36

步驟 4：刪除過去產生的金鑰/憑證 (IEEE 802.1X) 39

步驟 5：停用憑證 (IEEE 802.1X) 41

步驟 6：啟用新憑證 (IEEE 802.1X) 42

IPSec 的程序 43

步驟 1：檢查認證方法 (IPSec) 44

步驟 2：重新產生金鑰和憑證 (IPSec) 46

步驟 3：重設金鑰和憑證 (IPSec) 53

步驟 4：刪除過去產生的金鑰/憑證 (IPSec) 55

步驟 5：停用憑證 (IPSec) 57

步驟 6：啟用新憑證 (IPSec) 58

SIP 的程序 59

步驟 1：檢查設定 (SIP) 60

步驟 2：重新產生金鑰和憑證 (SIP) 63

步驟 3：重設金鑰和憑證 (SIP) 69

步驟 4：刪除過去產生的金鑰/憑證 (SIP) 72

步驟 5：停用憑證 (SIP) 74

步驟 6：啟用新憑證 (SIP) 75

裝置簽章的程序 76

步驟 1：檢查 S/MIME 設定 (裝置簽章) 77

步驟 2：重新產生金鑰和憑證 (裝置簽章) 79

步驟 3：停用憑證 (裝置簽章) 80

步驟 4：啟用新憑證 (裝置簽章) 81

藍芽設定的附加程序 84

藍芽的程序 85

步驟 1：刪除在 Canon PRINT Business 中註冊的裝置 (藍芽) 86
步驟 2：將裝置重新註冊到 Canon PRINT Business (藍芽) 87

Access Management System 設定的附加程序 89
Access Management System 設定的程序 90

前言

前言 2

前言

您必須更新韌體並執行本文件所述的附加程序，才能升級使用易受攻擊之加密庫建立的 RSA 金鑰。

首先請檢查本機的機型和版本。
如果在此頁面上有找到本機的機型和版本，請更新韌體，然後執行本文件所述的附加程序。 **檢查您是否必須執行附加程序 (P. 5)**
如需關於更新韌體的資訊，請參閱您獲得本文件的網站。

檢查本機的版本

遵循以下程序檢查本機的版本。

1 啟動遠端使用者介面。

2 按一下入口網站頁面的 [狀態確認/取消]。

3 按一下 [裝置資訊] ▶ 檢查 [版本資訊] 中的 [控制器]。

需要執行附加程序的機型和版本

機型	版本
- iR-ADV 4545 / 4535 / 4525 - iR-ADV 715 / 615 / 525 - iR-ADV 6575 / 6565 / 6560 / 6555 - iR-ADV 8505 / 8595 / 8585 - iR-ADV C3530 / C3520 - iR-ADV C7580 / C7570 / C7565 - iR-ADV C5560 / C5550 / C5540 / C5535 - iR-ADV C355 / C255 - iR-ADV C356 / C256	版本 59.39 至版本 67.30
- iR-ADV 4545 III / 4535 III / 4525 III - iR-ADV 715 III / 615 III / 525 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 - iR-ADV C475 III - iPR C165 / C170	版本 29.39 至版本 37.30
- iR-ADV 4725 / 4735 / 4745 - iR-ADV 8705 / 8705B / 8795 / 8795B / 8786 / 8786B - iR-ADV C3730 / C3720	版本 17.44 至版本 27.30

機型	版本
- iR-ADV C7780 / C7770 / C7765	
- iR-ADV C357 - iR-ADV C477	版本 19.34 至版本 27.30
- iR-ADV C5760 / C5750 / C5740 / C5735	版本 19.40 至版本 27.30
- iR-ADV 6765 / 6780	版本 17.44 至版本 27.33
- iR-ADV C5870 / C5860 / C5850 / C5840	版本 03.11 至版本 17.32
- iR-ADV 6860 / 6870	版本 05.25 至版本 17.32
- iR-ADV C3830 / C3826 / C3835	版本 06.28 至版本 17.32
- iR-ADV C568	版本 04.13 至版本 17.08
- iR C3226 / C3222	版本 01.12 至版本 02.13
- iR2425	版本 02.06 至版本 05.00
- iR2635 / iR2645 / iR2630 / iR2625	版本 130.0.117 至版本 707.0.701

註釋

- 本文件中使用的螢幕截圖，視您機器的機型而定，可能與您實際看到的情況不同。如需關於螢幕截圖的詳細資訊，請到線上手冊網站參閱本機的手冊。

  https://oip.manual.canon/

檢查您是否必須執行附加程序

檢查您是否必須執行附加程序 5

檢查您是否必須執行附加程序

請執行以下三項操作以檢查您必須執行的附加程序。
視機器的機型而定，您可能無法從控制面板執行操作。在這種情況下，請從遠端使用者介面執行操作。

檢查 RSA 金鑰(P. 5)
檢查藍芽設定(P. 7)
檢查 Access Management System 設定(P. 8)
如果本機中註冊的金鑰顯示「Default Key」或「AMS」，則不需要檢查 RSA 金鑰。檢查藍芽設定與 Access Management System 設定，如有必要，請執行附加程序。

註釋

- 本文件中使用的螢幕截圖僅為示範用途。視機器的機型而定，其可能與您實際看到的畫面不同。

檢查 RSA 金鑰

檢查是否有 RSA 金鑰。如果有機器產生的 RSA 金鑰，請檢查金鑰用途。

使用控制面板(P. 5)
使用遠端使用者介面(P. 6)

■使用控制面板

1 **按下 (設定/註冊)。**

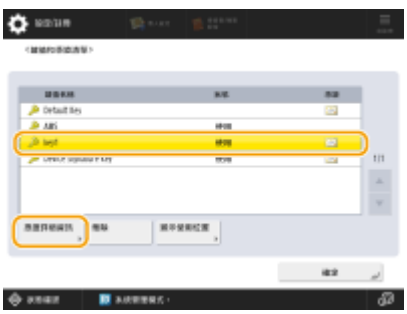
2 **按 <管理設定> ▶ <裝置管理> ▶ <憑證設定> ▶ <鍵值和憑證清單>。**

3 **按下 <本裝置的鍵值和憑證清單>。**

- <本裝置的鍵值和憑證清單> 不會顯示，除非在本機上啟用了使用者簽署功能。在這種情況下，請繼續下一個步驟。

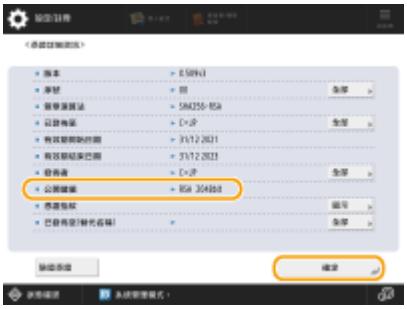
4 **選擇 <Default Key> 和 <AMS> 以外，且 <狀態> 顯示為 <使用> 的金鑰 ▶ 按 <憑證詳細資訊>。**

範例畫面：



5 檢查 <公開鍵值>。

範例畫面：



對於 RSA 以外的憑證

您不需要執行附加程序。按 <確定> 以關閉畫面。

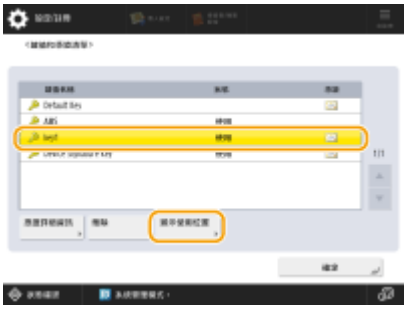
對於 RSA 憑證

前進至步驟 6。

- 您不需要對下列金鑰執行附加程序。按 <確定> 以關閉畫面。
  - 在外部產生且註冊到本機的 RSA 金鑰
- 如果您必須執行附加程序，則可能需要憑證資訊來停用憑證。請在刪除金鑰/憑證之前記下所需的資訊。向核發憑證的憑證授權單位詢問所需資訊。

6 按 <顯示使用位置> ▶ 檢查金鑰用途。

範例畫面：

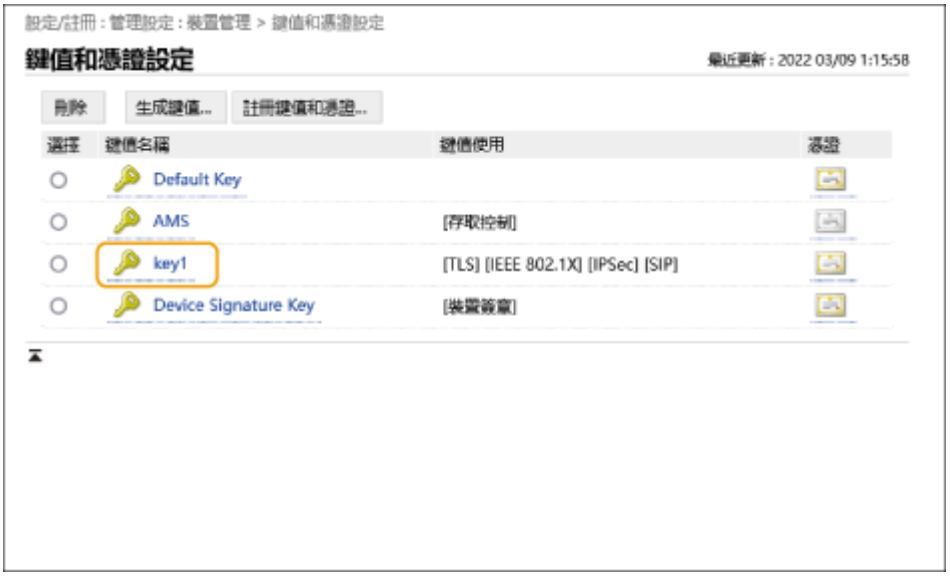


依照這裡顯示的說明執行附加程序。 **RSA 金鑰用途和附加程序(P. 11)**

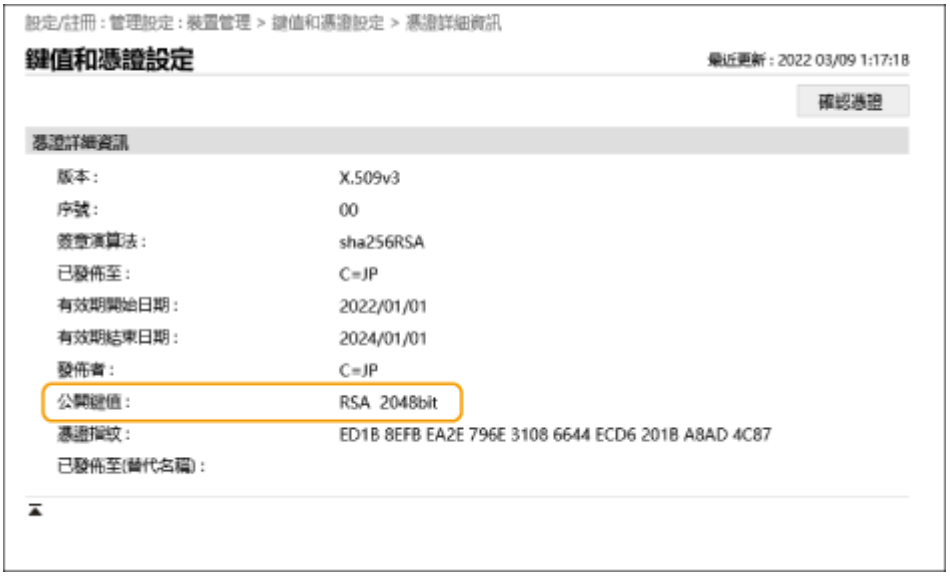
■使用遠端使用者介面

1 啟動遠端使用者介面 ▶ 按一下 [設定/註冊] ▶ [裝置管理] ▶ [鍵值和憑證設定]。

2 檢查 [Default Key] 和 [AMS] 以外的金鑰。



3 檢查 [公開鍵值]。



對於 RSA 以外的憑證

您不需要執行附加程序。

對於 RSA 憑證

按一下畫面上方的 [鍵值和憑證設定] ▶ 檢查金鑰用途。

- 依照這裡顯示的說明執行附加程序。 **RSA 金鑰用途和附加程序(P. 11)**
- 您不需要對下列金鑰執行附加程序。
  - 在外部產生且註冊到本機的 RSA 金鑰
- 如果您必須執行附加程序，則可能需要憑證資訊來停用憑證。請在刪除金鑰/憑證之前記下所需的資訊。向核發憑證的憑證授權單位詢問所需資訊。

檢查藍芽設定

檢查藍芽是否設定為 <開啟>。如果其設定為 <開啟>，您必須執行附加程序。

使用控制面板(P. 8)
使用遠端使用者介面(P. 8)

■使用控制面板

1 按下 (設定/註冊)。

2 按 <參數選擇> ▶ <網路> ▶ <藍芽設定>。

3 檢查 <使用藍芽>。

- 如果 <使用藍芽> 設為 <開啟>，請執行後續程序。 **藍芽設定的附加程序(P. 84)**
- 如果 <使用藍芽> 設為 <關閉>，您不需要執行後續程序。

■使用遠端使用者介面

1 啟動遠端使用者介面。

2 按一下入口網站頁面的 [設定/註冊]。

3 按一下 [網路] ▶ [藍芽設定]。

4 檢查 [使用藍芽]。

- 如果選擇了 [使用藍芽]，請執行後續程序。 **藍芽設定的附加程序(P. 84)**
- 如果取消選擇 [使用藍芽]，您不需要執行後續程序。

檢查 Access Management System 設定

檢查 Access Management System 是否設定為 <開啟>。如果其設定為 <開啟>，您必須執行附加程序。

端視您的機器而定，此設定可能不會顯示。在這種情況下，您不需要執行附加程序。

使用控制面板(P. 8)
使用遠端使用者介面(P. 9)

■使用控制面板

1 按下 (設定/註冊)。

2 按 <管理設定> ▶ <授權/其他> ▶ <使用 ACCESS MANAGEMENT SYSTEM>。

3 檢查 <使用 ACCESS MANAGEMENT SYSTEM>。

- 如果 <使用 ACCESS MANAGEMENT SYSTEM> 設為 <開啟>，請執行後續程序。 **Access Management System 設定的附加程序(P. 89)**
- 如果 <使用 ACCESS MANAGEMENT SYSTEM> 設為 <關閉>，您不需要執行後續程序。

■使用遠端使用者介面

1 啟動遠端使用者介面。

2 按一下入口網站頁面的 [設定/註冊]。

3 按一下 [授權/其他] ▶ [ACCESS MANAGEMENT SYSTEM 設定]。

4 檢查 [使用 ACCESS MANAGEMENT SYSTEM]。

- 如果選擇了 [使用 ACCESS MANAGEMENT SYSTEM]，請執行後續程序。 **Access Management System 設定的附加程序(P. 89)**
- 如果取消選擇 [使用 ACCESS MANAGEMENT SYSTEM]，您不需要執行後續程序。

RSA 金鑰用途和附加程序

RSA 金鑰用途和附加程序 11
TLS 的程序 12
步驟 1：重新產生金鑰和憑證 (TLS) 13
步驟 2：重設金鑰和憑證 (TLS) 20
步驟 3：刪除過去產生的金鑰/憑證 (TLS) 22
步驟 4：停用憑證 (TLS) 24
步驟 5：啟用新憑證 (TLS) 25
IEEE 802.1X 的程序 26
步驟 1：檢查認證方法 (IEEE 802.1X) 27
步驟 2：重新產生金鑰和憑證 (IEEE 802.1X) 29
步驟 3：重設金鑰和憑證 (IEEE 802.1X) 36
步驟 4：刪除過去產生的金鑰/憑證 (IEEE 802.1X) 39
步驟 5：停用憑證 (IEEE 802.1X) 41
步驟 6：啟用新憑證 (IEEE 802.1X) 42
IPSec 的程序 43
步驟 1：檢查認證方法 (IPSec) 44
步驟 2：重新產生金鑰和憑證 (IPSec) 46
步驟 3：重設金鑰和憑證 (IPSec) 53
步驟 4：刪除過去產生的金鑰/憑證 (IPSec) 55
步驟 5：停用憑證 (IPSec) 57
步驟 6：啟用新憑證 (IPSec) 58
SIP 的程序 59
步驟 1：檢查設定 (SIP) 60
步驟 2：重新產生金鑰和憑證 (SIP) 63
步驟 3：重設金鑰和憑證 (SIP) 69
步驟 4：刪除過去產生的金鑰/憑證 (SIP) 72
步驟 5：停用憑證 (SIP) 74
步驟 6：啟用新憑證 (SIP) 75
裝置簽章的程序 76
步驟 1：檢查 S/MIME 設定 (裝置簽章) 77
步驟 2：重新產生金鑰和憑證 (裝置簽章) 79
步驟 3：停用憑證 (裝置簽章) 80
步驟 4：啟用新憑證 (裝置簽章) 81

RSA 金鑰用途和附加程序

請參閱「附加程序」並根據金鑰用途加以執行。

RSA 金鑰用途	條件	附加程序
TLS	在任何情況下您都必須執行附加程序。	**TLS 的程序(P. 12)**
IEEE 802.1X	如果 IEEE 802.1X 認證方法設定為 EAP-TLS，您必須執行附加程序。	**IEEE 802.1X 的程序(P. 26)**
IPSec	如果 IKE 認證方法設定為數位簽章方法，您必須執行附加程序。	**IPSec 的程序(P. 43)**
SIP	如果使用 TLS，您必須執行附加程序。	**SIP 的程序(P. 59)**
裝置簽章	在下列情況下，您必須執行附加程序： • 使用裝置簽章的金鑰將數位簽章新增到已傳送的檔案時 • 在 S/MIME 加密設定中啟用加密時	**裝置簽章的程序(P. 76)**

註釋

- 本文件中使用的螢幕截圖僅為示範用途。視機器的機型而定，其可能與您實際看到的畫面不同。

TLS 的程序

步驟 1：重新產生金鑰和憑證 (TLS)(P. 13)
步驟 2：重設金鑰和憑證 (TLS)(P. 20)
步驟 3：刪除過去產生的金鑰/憑證 (TLS)(P. 22)
步驟 4：停用憑證 (TLS)(P. 24)
步驟 5：啟用新憑證 (TLS)(P. 25)

步驟 1：重新產生金鑰和憑證 (TLS)

您可以為本機產生的金鑰產生三種類型的憑證：自我簽章憑證、CSR 憑證和 SCEP 憑證。程序會依憑證類型而有不同。視機器的機型而定，您可能無法從控制面板執行操作。在這種情況下，請從遠端使用者介面執行操作。

對於自我簽章憑證(P. 13)
對於 CSR 憑證(P. 16)
對於 SCEP 憑證(P. 18)

對於自我簽章憑證

使用控制面板(P. 13)
使用遠端使用者介面(P. 14)

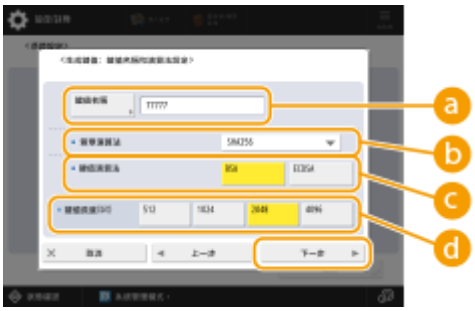
■使用控制面板

1 按下 (設定/註冊)。

2 按 <管理設定> ▶ <裝置管理> ▶ <憑證設定> ▶ <生成鍵值> ▶ <生成網路通訊鍵值>。

3 指定所需的設定，然後前進到下一個畫面。

範例畫面：



a <鍵值名稱>

輸入金鑰的名稱。請輸入可在清單中輕鬆找到的名稱。

b <簽章演算法>

選擇要用於簽章的雜湊演算法。視金鑰長度，可用的雜湊演算法會有不同。長度為 1024 位元或以上的金鑰可支援 SHA384 和 SHA512 雜湊演算法。如果針對 c 選擇了 <RSA>，且針對 d 將 <鍵值長度(bit)> 設定為 <1024> 或更多，可以選擇 SHA384 和 SHA512 雜湊演算法。

c <鍵值演算法>

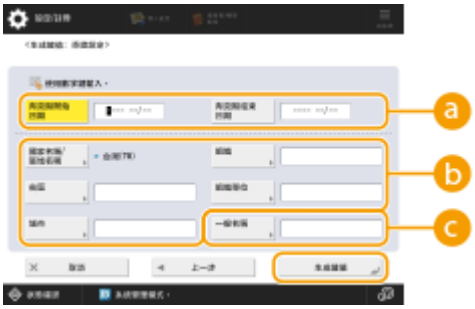
選擇金鑰演算法。如果選擇 <RSA>，<鍵值長度(bit)> 會顯示為 d 的設定項目。如果選擇 <ECDSA>，會改為顯示 <鍵值類型>。

d <鍵值長度(bit)>/<鍵值類型>

無果針對 c 選擇了 <RSA>，請指定金鑰長度，或如果選擇了 <ECDSA>，請指定金鑰類型。在兩種情況中，較高的值提供較好的安全性但會降低通訊處理速度。

4 設定憑證的必要項目 ▶ 按 <生成鍵值>。

範例畫面：



a <有效期開始日期>/<有效期結束日期>

輸入憑證有效期的開始日期和結束日期。

b <國家名稱/區域名稱>/<省區>/<城市>/<組織>/<組織單位>

從清單中選擇國碼，然後輸入地點和組織名稱。

c <一般名稱>

輸入 IP 位址或 FQDN。

- 在 Windows 環境中執行 IPPS 列印時，確認輸入本機的 IP 位址。
- 需要 DNS 伺服器才可輸入本機的 FQDN。若未使用 DNS 伺服器，請輸入本機的 IP 位址。

■使用遠端使用者介面

1 啟動遠端使用者介面。

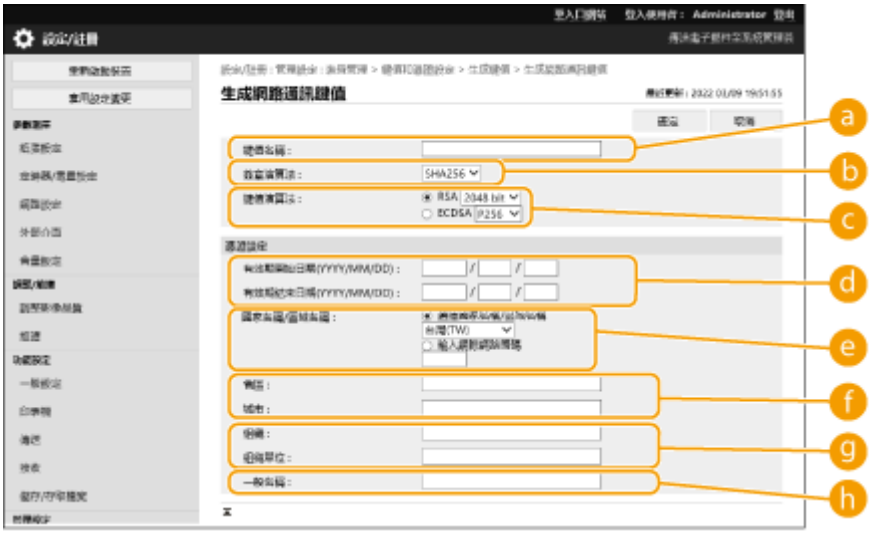
2 按一下入口網站頁面的 [設定/註冊]。

3 按一下 [裝置管理] ▶ [鍵值和憑證設定]。

4 按一下[生成鍵值]。

5 按一下[網路通訊]。

6 指定金鑰和憑證設定。



a [鍵值名稱]

使用英數字元輸入金鑰名稱。請輸入可在清單中輕鬆找到的名稱。

b [簽章演算法]

選擇要用於簽章的雜湊演算法。視金鑰長度，可用的雜湊演算法會有不同。長度為 1024 位元或以上的金鑰可支援 SHA384 和 SHA512 雜湊演算法。

c [鍵值演算法]

選擇 [RSA] 或 [ECDSA] 金鑰產生作為演算法。如果選擇 [RSA]，請指定金鑰長度，或如果選擇 [ECDSA]，請指定金鑰類型。在兩種情況中，較高的值提供較好的安全性但會降低通訊處理速度。

註釋:

- 如果您對 [簽章演算法] 選擇 [SHA384] 或 [SHA512]，則當對 [鍵值演算法] 選擇 [RSA] 時，不能將金鑰長度設定為 [512 bit]。

d [有效期開始日期(YYYY/MM/DD)]/[有效期結束日期(YYYY/MM/DD)]

輸入憑證有效期的開始日期和結束日期。您不能將 [有效期結束日期(YYYY/MM/DD)] 設定為早於 [有效期開始日期(YYYY/MM/DD)] 中的日期。

e [國家名稱/區域名稱]

按一下 [選擇國家名稱/區域名稱]，然後從下拉清單中選擇國家/區域。或者，按一下 [輸入網際網路國碼]，然後輸入國碼，例如「US」代表美國。

f [省區]/[城市]

視需要使用英數字元輸入位置。

g [組織]/[組織單位]

視需要使用英數字元輸入組織名稱。

h [一般名稱]

視需要使用英數字元輸入憑證的一般名稱。「一般名稱」通常縮寫為「CN」。

7 按一下[確定]。

- 金鑰和憑證的產生可能要花一點時間。
- 產生的金鑰和憑證會自動註冊到本機。

對於 CSR 憑證

在本機上產生金鑰和 CSR。使用畫面上顯示的 CSR 資料或輸出為檔案以要求憑證授權單位核發憑證。然後為金鑰註冊核發的憑證。
您只能從遠端使用者介面指定此設定。

■1. 產生金鑰和 CSR

1 **啟動遠端使用者介面。**

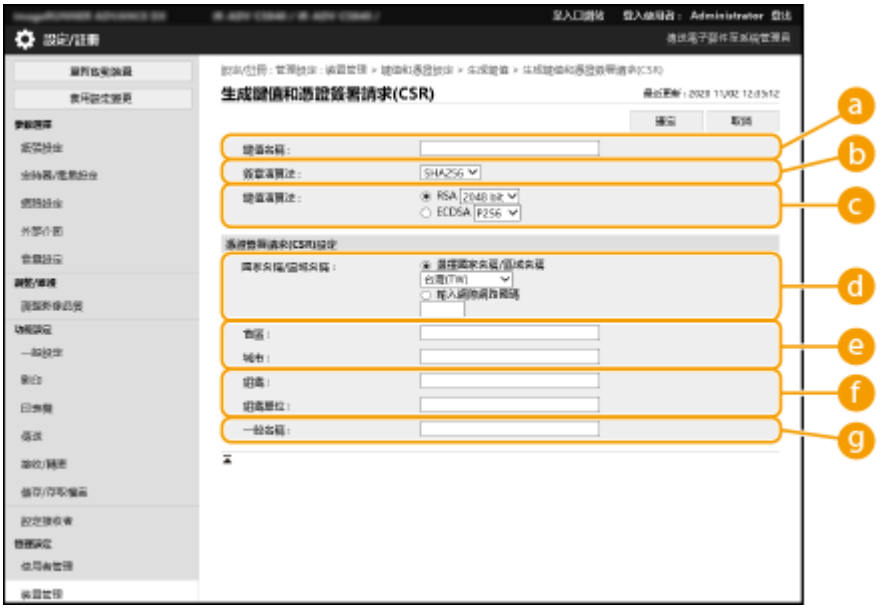
2 **按一下入口網站頁面的 [設定/註冊]。**

3 **按一下 [裝置管理] ▶ [鍵值和憑證設定]。**

4 **按一下[生成鍵值]。**

5 **按一下[鍵值和憑證簽署請求(CSR)]。**

6 **指定金鑰和憑證設定。**



ⓐ [鍵值名稱]

輸入金鑰的名稱。請輸入可在清單中輕鬆找到的名稱。

ⓑ [簽章演算法]

選擇用於簽章的雜湊演算法。

[鍵值演算法]

選擇金鑰演算法，然後在選擇 [RSA] 時指定金鑰長度，或是在選擇 [ECDSA] 時指定金鑰類型。

[國家名稱/區域名稱]

從清單中選擇國家代碼，或是直接輸入國家代碼。

[省區]/[城市]

輸入位置。

[組織]/[組織單位]

輸入組織名稱。

[一般名稱]

輸入 IP 位址或 FQDN。

- 在 Windows 環境中執行 IPPS 列印時，確認輸入本機的 IP 位址。
- 需要 DNS 伺服器才可輸入本機的 FQDN。若未使用 DNS 伺服器，請輸入本機的 IP 位址。

7 按一下[確定]。

➠ 隨即顯示 CSR 資料。

- 如果您希望將 CSR 資料儲存至檔案，請按一下 [儲存到檔案中] 然後指定儲存位置。

註釋:

- 產生 CSR 的金鑰將會顯示在金鑰與憑證清單畫面上，但是您沒有辦法自行使用。若要使用此金鑰，您需要註冊稍後根據 CSR 核發的憑證。

8 要求憑證授權單位根據 CSR 資料核發憑證。

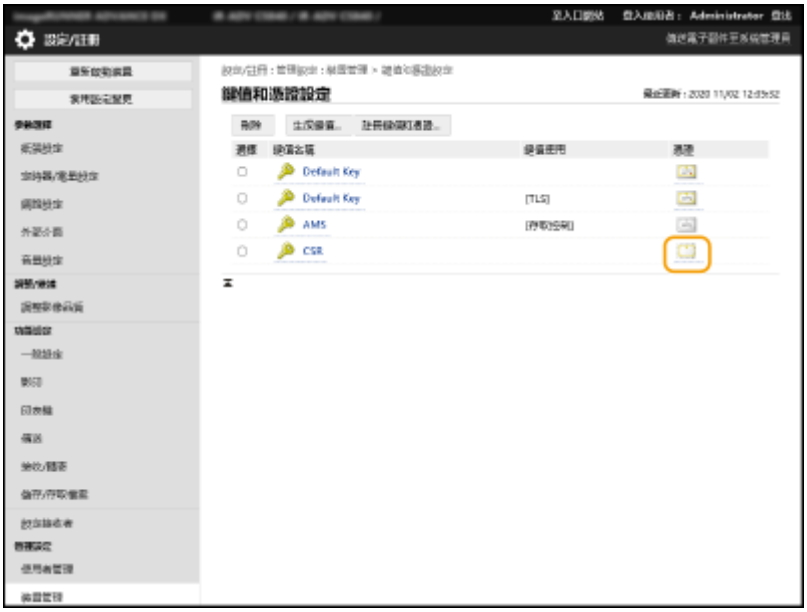
■2. 將核發的憑證註冊到金鑰

1 啟動遠端使用者介面。

2 按一下入口網站頁面的 [設定/註冊]。

3 按一下 [裝置管理] ▶ [鍵值和憑證設定]。

4 在 [憑證] 清單中，為想要註冊的憑證按一下 。



5 **按一下[註冊憑證...]。**

6 **註冊憑證。**

- 按一下 [瀏覽...] ▶ 指定要註冊的檔案 (憑證) ▶ 按一下 [註冊]。

對於 SCEP 憑證

手動要求 SCEP 伺服器核發憑證。
您只能從遠端使用者介面指定此設定。

註釋

- 如果選擇了 [啟用憑證自動發行要求定時器]，則不能傳送核發憑證的手動要求。如果已選擇此選項，請取消選擇。

啟動遠端使用者介面 ▶ 按一下 [設定/註冊] ▶ [裝置管理] ▶ [憑證發行要求的設定(SCEP)] ▶ [憑證自動發行要求設定] ▶ 取消選擇 [啟用憑證自動發行要求定時器] ▶ 按一下 [更新]。

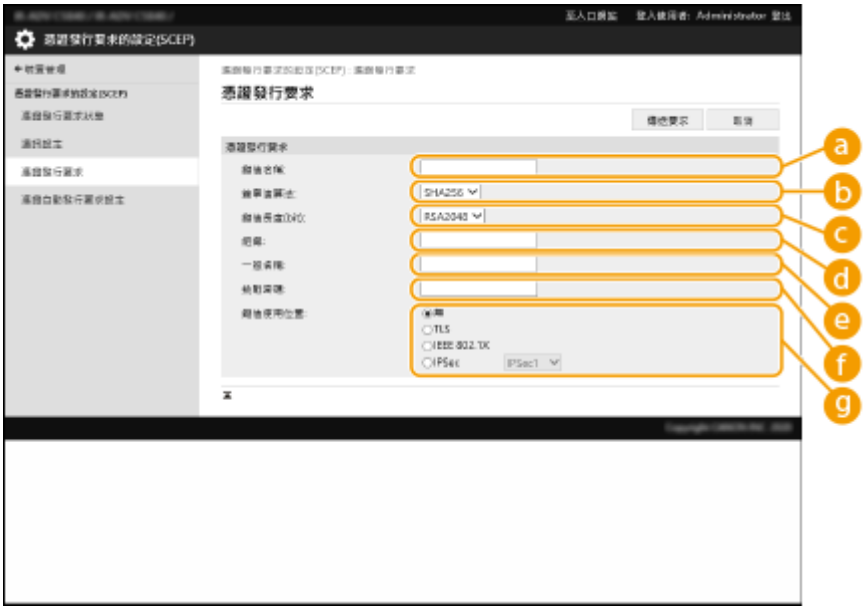
1 **啟動遠端使用者介面。**

2 **按一下入口網站頁面的 [設定/註冊]。**

3 **按一下 [裝置管理] ▶ [憑證發行要求的設定(SCEP)]。**

4 **按一下[憑證發行要求]。**

5 **指定要求憑證所需的設定。**



a [鍵值名稱:]

輸入金鑰的名稱。請輸入可在清單中輕鬆找到的名稱。

b [簽章演算法:]

選擇用於簽章的雜湊演算法。

c [鍵值長度(bit):]

選擇金鑰長度。

d [組織:]

輸入組織名稱。

e [一般名稱:]

輸入 IP 位址或 FQDN。

- 在 Windows 環境中執行 IPPS 列印時，確認輸入本機的 IP 位址。
- 需要 DNS 伺服器才可輸入本機的 FQDN。若未使用 DNS 伺服器，請輸入本機的 IP 位址。

f [挑戰密碼:]

若 SCEP 伺服器端設定密碼，請輸入憑證發行要求資料 (PKCS#9) 中的查問密碼。

g [鍵值使用位置:]

選擇 [TLS] (開啟檔案需要密碼)。

註釋:

- 選擇 [無] 以外的選項時，請事先啟用每個功能。如果在停用每個功能的情況下成功取得憑證，則會將憑證指派給金鑰使用位置，但不會自動啟用每個功能。

6 按一下[傳送要求]。

7 按一下[重新啟動]。

步驟 2：重設金鑰和憑證 (TLS)

視機器的機型而定，您可能無法從控制面板執行操作。在這種情況下，請從遠端使用者介面執行操作。
對於 SCEP 憑證不需要執行此程序。

對於自我簽署憑證/CSR 憑證

使用控制面板(P. 20)
使用遠端使用者介面(P. 21)

■使用控制面板

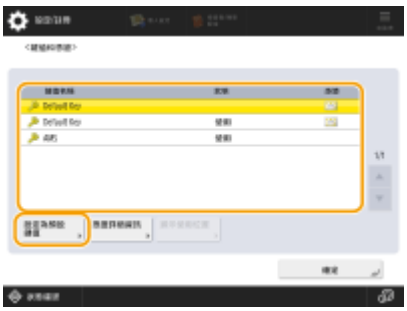
1 **按下 (設定/註冊)。**

2 **按 <參數選擇> ▶ <網路> ▶ <TCP/IP 設定> ▶ <TLS 設定>。**

3 **按下 <鍵值和憑證>。**

4 **選擇 TLS 加密通訊要使用的金鑰和憑證 ▶ 按 <設定為預設鍵值> ▶ <是>。**

範例畫面：



- 如果要使用預先安裝的金鑰和憑證，請選擇 <Default Key>。

註釋:

- TLS 加密通訊無法使用 <Device Signature Key> (用於裝置簽章) 或 <AMS> (用於存取限制)。

5 **按下 <確定>。**

6 **按 (設定/註冊) ▶ <套用設定變更> ▶ <是>。**

➠ 本機重新啟動，然後套用設定。

■使用遠端使用者介面

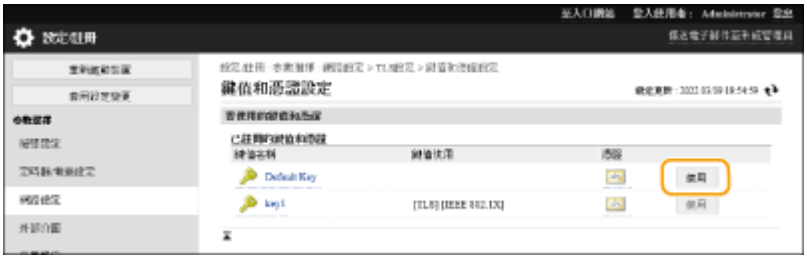
1 **啟動遠端使用者介面。**

2 **按一下入口網站頁面的 [設定/註冊]。**

3 **按一下 [網路] ▶ [TLS 設定]。**

4 **按一下[鍵值和憑證]。**

5 **對用於 TLS 加密通訊的金鑰和憑證按一下 [使用]。**



- 如果要使用預先安裝的金鑰和憑證，請選擇 [Default Key]。

6 **按一下 [套用設定變更] 以重新啟動本機。**

➠ 本機重新啟動，然後套用設定。

步驟 3：刪除過去產生的金鑰/憑證 (TLS)

視機器的機型而定，您可能無法從控制面板執行操作。在這種情況下，請從遠端使用者介面執行操作。

註釋

- 停用憑證時，您可能需要向憑證授權單位傳達資訊。請參閱 **檢查您是否必須執行附加程序(P. 5)** ，並在刪除金鑰/憑證之前記下所需資訊。

使用控制面板(P. 22)
使用遠端使用者介面(P. 22)

■使用控制面板

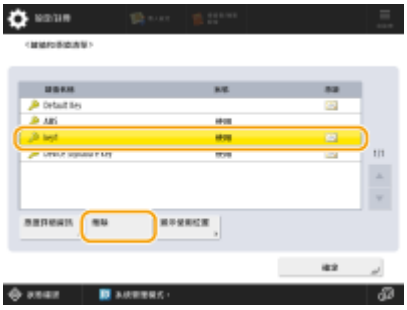
1 **按下 (設定/註冊)。**

2 **按 <管理設定> ▶ <裝置管理> ▶ <憑證設定> ▶ <鍵值和憑證清單> ▶ <本裝置的鍵值和憑證清單>。**

- <本裝置的鍵值和憑證清單> 不會顯示，除非在本機上啟用了使用者簽署功能。在這種情況下，請繼續下一個步驟。

3 **選擇金鑰和憑證 ▶ 按 <刪除> ▶ <是>。**

範例畫面：



註釋:

- 如果顯示 ，表示金鑰損毀或無效。
- 如果未顯示 ，表示金鑰的憑證不存在。
- 如果選擇了金鑰和憑證，並按 <憑證詳細資訊>，則會顯示關於憑證的詳細資訊。您也可以按此畫面上的 <驗證憑證> 以查看憑證是否有效。

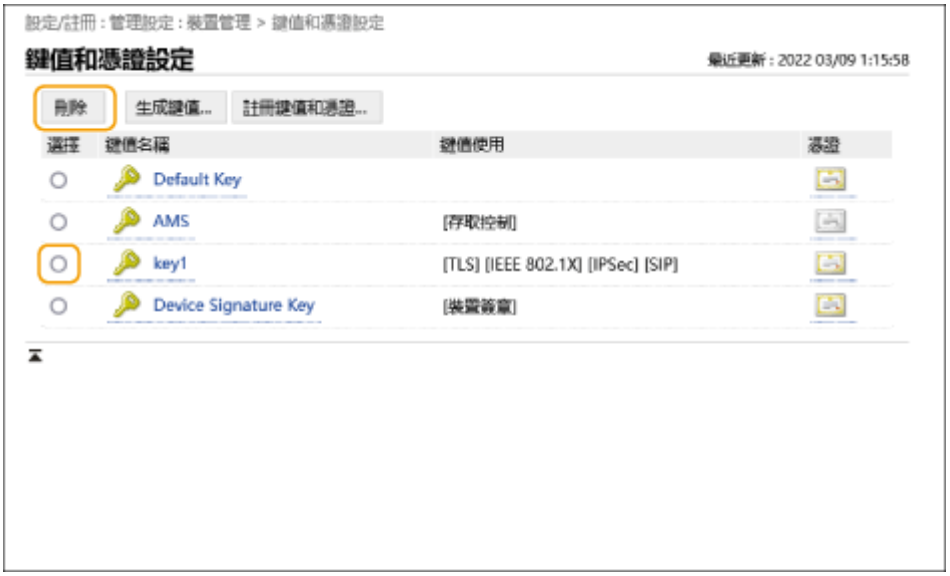
■使用遠端使用者介面

1 **啟動遠端使用者介面。**

2 **按一下入口網站頁面的 [設定/註冊]。**

3 **按一下 [裝置管理] ▶ [鍵值和憑證設定]。**

4 **選擇金鑰和憑證 ▶ 按一下 [刪除] ▶ [確定]。**



註釋

- 如果顯示 ，表示金鑰損毀或無效。
- 如果顯示 ，表示金鑰的憑證不存在。
- 按一下金鑰名稱以顯示有關憑證的詳細資訊。您也可以按一下畫面上的 [確認憑證] 以檢查憑證是否有效。

步驟 4：停用憑證 (TLS)

停用過去產生的憑證。程序會依憑證類型而有不同。

■對於自我簽章憑證

如果在電腦或網頁瀏覽器中將包含需要附加程序之金鑰的憑證註冊為可信任憑證，請刪除已註冊的憑證。

■對於 CSR/SCEP 憑證

要求核發憑證的憑證授權單位撤銷憑證。請參閱憑證中的 [發佈者] 以瞭解要求的憑證授權單位。

註釋

- 如果在與機器通訊的電腦或網頁瀏覽器中使用 CRL 檢查憑證撤銷，請在撤銷憑證後將更新的 CRL 註冊到電腦或網頁瀏覽器。
- 如果您使用 CRL 以外的方法（例如 OCSP）來檢查憑證撤銷，請執行該方法的程序。

步驟 5：啟用新憑證 (TLS)

啟用機器上新產生的憑證。

■對於自我簽章憑證

在電腦或網頁瀏覽器中將新憑證註冊為可信任憑證。

■對於 CSR/SCEP 憑證

您不需要執行附加程序。

IEEE 802.1X 的程序

步驟 1：檢查認證方法 (IEEE 802.1X)(P. 27)
步驟 2：重新產生金鑰和憑證 (IEEE 802.1X)(P. 29)
步驟 3：重設金鑰和憑證 (IEEE 802.1X)(P. 36)
步驟 4：刪除過去產生的金鑰/憑證 (IEEE 802.1X)(P. 39)
步驟 5：停用憑證 (IEEE 802.1X)(P. 41)
步驟 6：啟用新憑證 (IEEE 802.1X)(P. 42)

步驟 1：檢查認證方法 (IEEE 802.1X)

如果 IEEE 802.1X 認證方法設定為 EAP-TLS，您必須執行後續程序。
遵循以下程序檢查認證方法。
視機器的機型而定，您可能無法從控制面板執行操作。在這種情況下，請從遠端使用者介面執行操作。

使用控制面板(P. 27)
使用遠端使用者介面(P. 27)

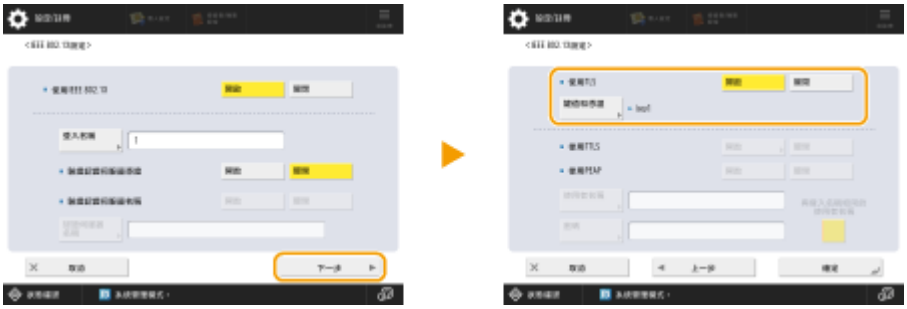
■使用控制面板

1 按下 (設定/註冊)。

2 按 <參數選擇> ▶ <網路> ▶ <IEEE 802.1X 設定>。

3 按 <下一步> ▶ 檢查 <使用 TLS>。

範例畫面：



- 如果 <使用 TLS> 設為 <開啟> 並且 <鍵值和憑證> 顯示金鑰名稱，請執行後續程序。
- 如果 <使用 TLS> 設為 <關閉>，您不需要執行後續程序。

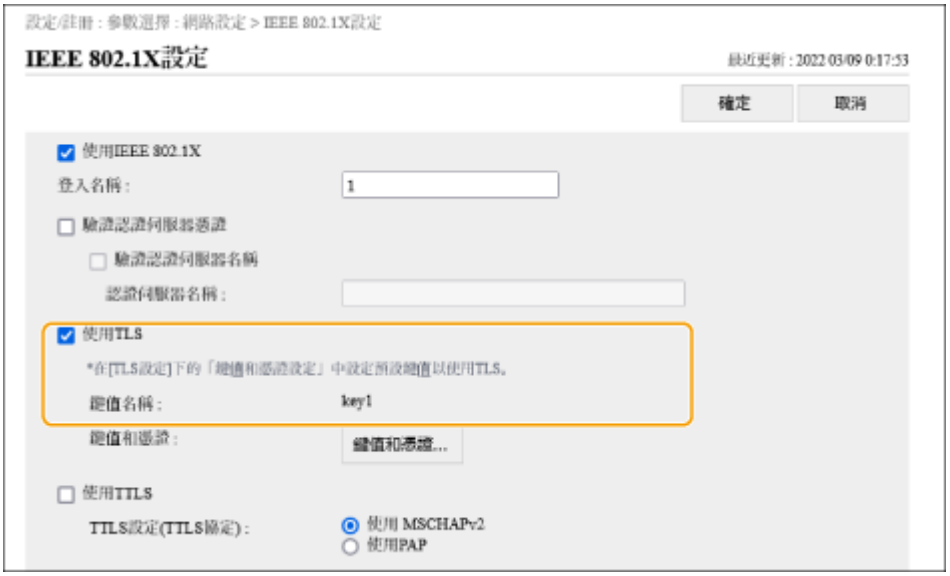
■使用遠端使用者介面

1 啟動遠端使用者介面。

2 按一下入口網站頁面的 [設定/註冊]。

3 按一下 [網路] ▶ [IEEE 802.1X 設定]。

4 檢查 [使用 TLS]。



- 如果選擇了 [使用 TLS] 並且顯示金鑰名稱，請執行後續程序。
- 如果取消選擇 [使用 TLS]，您不需要執行後續程序。

步驟 2：重新產生金鑰和憑證 (IEEE 802.1X)

您可以為本機產生的金鑰產生三種類型的憑證：自我簽章憑證、CSR 憑證和 SCEP 憑證。程序會依憑證類型而有不同。視機器的機型而定，您可能無法從控制面板執行操作。在這種情況下，請從遠端使用者介面執行操作。

對於自我簽章憑證(P. 29)
對於 CSR 憑證(P. 32)
對於 SCEP 憑證(P. 34)

對於自我簽章憑證

使用控制面板(P. 29)
使用遠端使用者介面(P. 30)

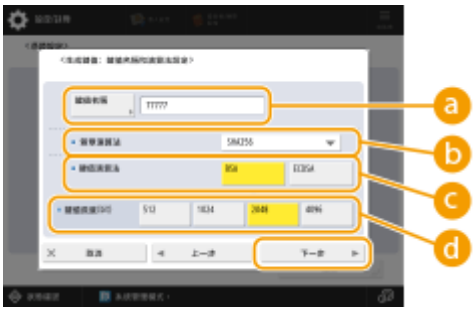
■使用控制面板

1 按下 (設定/註冊)。

2 按 <管理設定> ▶ <裝置管理> ▶ <憑證設定> ▶ <生成鍵值> ▶ <生成網路通訊鍵值>。

3 指定所需的設定，然後前進到下一個畫面。

範例畫面：



a <鍵值名稱>

輸入金鑰的名稱。請輸入可在清單中輕鬆找到的名稱。

b <簽章演算法>

選擇要用於簽章的雜湊演算法。視金鑰長度，可用的雜湊演算法會有不同。長度為 1024 位元或以上的金鑰可支援 SHA384 和 SHA512 雜湊演算法。如果針對 c 選擇了 <RSA>，且針對 d 將 <鍵值長度(bit)> 設定為 <1024> 或更多，可以選擇 SHA384 和 SHA512 雜湊演算法。

c <鍵值演算法>

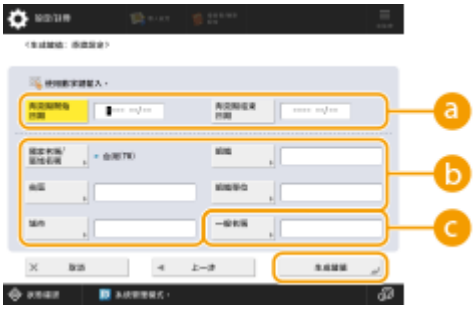
選擇金鑰演算法。如果選擇 <RSA>，<鍵值長度(bit)> 會顯示為 d 的設定項目。如果選擇 <ECDSA>，會改為顯示 <鍵值類型>。

d <鍵值長度(bit)>/<鍵值類型>

無果針對 c 選擇了 <RSA>，請指定金鑰長度，或如果選擇了 <ECDSA>，請指定金鑰類型。在兩種情況中，較高的值提供較好的安全性但會降低通訊處理速度。

4 設定憑證的必要項目 ▶ 按 <生成鍵值>。

範例畫面：



a <有效期開始日期>/<有效期結束日期>

輸入憑證有效期的開始日期和結束日期。

b <國家名稱/區域名稱>/<省區>/<城市>/<組織>/<組織單位>

從清單中選擇國碼，然後輸入地點和組織名稱。

c <一般名稱>

輸入 IP 位址或 FQDN。

- 在 Windows 環境中執行 IPPS 列印時，確認輸入本機的 IP 位址。
- 需要 DNS 伺服器才可輸入本機的 FQDN。若未使用 DNS 伺服器，請輸入本機的 IP 位址。

■使用遠端使用者介面

1 啟動遠端使用者介面。

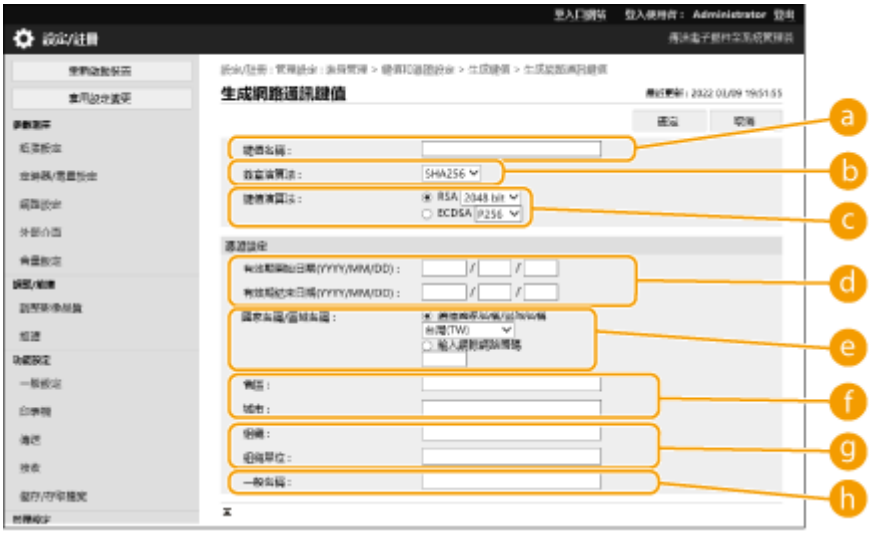
2 按一下入口網站頁面的 [設定/註冊]。

3 按一下 [裝置管理] ▶ [鍵值和憑證設定]。

4 按一下[生成鍵值]。

5 按一下[網路通訊]。

6 指定金鑰和憑證設定。



a [鍵值名稱]

使用英數字元輸入金鑰名稱。請輸入可在清單中輕鬆找到的名稱。

b [簽章演算法]

選擇要用於簽章的雜湊演算法。視金鑰長度，可用的雜湊演算法會有不同。長度為 1024 位元或以上的金鑰可支援 SHA384 和 SHA512 雜湊演算法。

c [鍵值演算法]

選擇 [RSA] 或 [ECDSA] 金鑰產生作為演算法。如果選擇 [RSA]，請指定金鑰長度，或如果選擇 [ECDSA]，請指定金鑰類型。在兩種情況中，較高的值提供較好的安全性但會降低通訊處理速度。

註釋:

- 如果您對 [簽章演算法] 選擇 [SHA384] 或 [SHA512]，則當對 [鍵值演算法] 選擇 [RSA] 時，不能將金鑰長度設定為 [512 bit]。

d [有效期開始日期(YYYY/MM/DD)]/[有效期結束日期(YYYY/MM/DD)]

輸入憑證有效期的開始日期和結束日期。您不能將 [有效期結束日期(YYYY/MM/DD)] 設定為早於 [有效期開始日期(YYYY/MM/DD)] 中的日期。

e [國家名稱/區域名稱]

按一下 [選擇國家名稱/區域名稱]，然後從下拉清單中選擇國家/區域。或者，按一下 [輸入網際網路國碼]，然後輸入國碼，例如「US」代表美國。

f [省區]/[城市]

視需要使用英數字元輸入位置。

g [組織]/[組織單位]

視需要使用英數字元輸入組織名稱。

h [一般名稱]

視需要使用英數字元輸入憑證的一般名稱。「一般名稱」通常縮寫為「CN」。

7 按一下[確定]。

- 金鑰和憑證的產生可能要花一點時間。
- 產生的金鑰和憑證會自動註冊到本機。

對於 CSR 憑證

在本機上產生金鑰和 CSR。使用畫面上顯示的 CSR 資料或輸出為檔案以要求憑證授權單位核發憑證。然後為金鑰註冊核發的憑證。
您只能從遠端使用者介面指定此設定。

■1. 產生金鑰和 CSR

1 **啟動遠端使用者介面。**

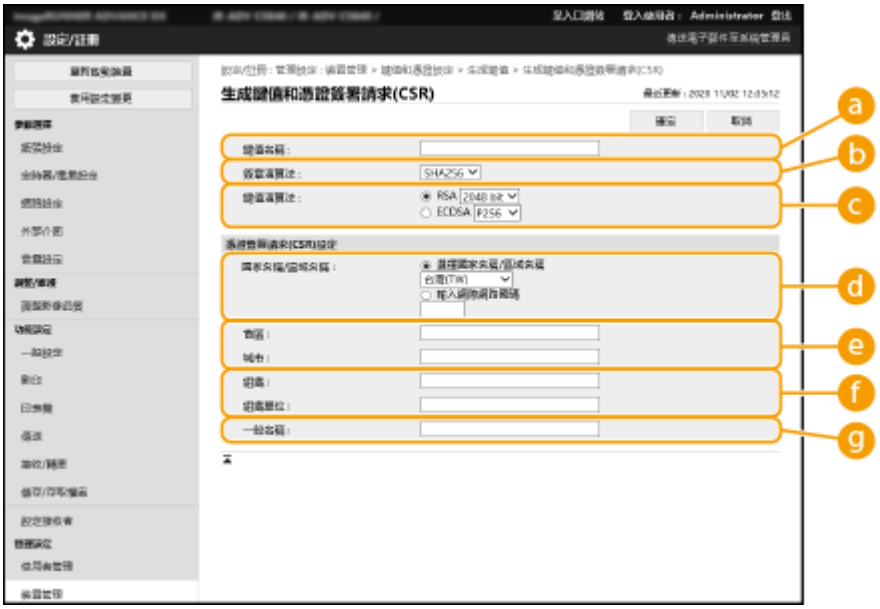
2 **按一下入口網站頁面的 [設定/註冊]。**

3 **按一下 [裝置管理] ▶ [鍵值和憑證設定]。**

4 **按一下[生成鍵值]。**

5 **按一下[鍵值和憑證簽署請求(CSR)]。**

6 **指定金鑰和憑證設定。**



a [鍵值名稱]

輸入金鑰的名稱。請輸入可在清單中輕鬆找到的名稱。

b [簽章演算法]

選擇用於簽章的雜湊演算法。

[鍵值演算法]

選擇金鑰演算法，然後在選擇 [RSA] 時指定金鑰長度，或是在選擇 [ECDSA] 時指定金鑰類型。

[國家名稱/區域名稱]

從清單中選擇國家代碼，或是直接輸入國家代碼。

[省區]/[城市]

輸入位置。

[組織]/[組織單位]

輸入組織名稱。

[一般名稱]

輸入 IP 位址或 FQDN。

- 在 Windows 環境中執行 IPPS 列印時，確認輸入本機的 IP 位址。
- 需要 DNS 伺服器才可輸入本機的 FQDN。若未使用 DNS 伺服器，請輸入本機的 IP 位址。

7 按一下[確定]。

➠ 隨即顯示 CSR 資料。

- 如果您希望將 CSR 資料儲存至檔案，請按一下 [儲存到檔案中] 然後指定儲存位置。

註釋:

- 產生 CSR 的金鑰將會顯示在金鑰與憑證清單畫面上，但是您沒有辦法自行使用。若要使用此金鑰，您需要註冊稍後根據 CSR 核發的憑證。

8 要求憑證授權單位根據 CSR 資料核發憑證。

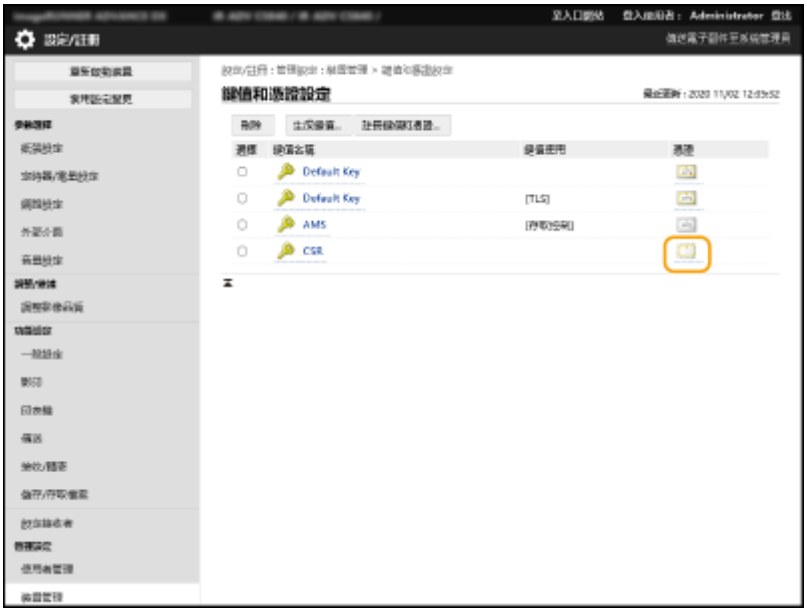
■2. 將核發的憑證註冊到金鑰

1 啟動遠端使用者介面。

2 按一下入口網站頁面的 [設定/註冊]。

3 按一下 [裝置管理] ▶ [鍵值和憑證設定]。

4 在 [憑證] 清單中，為想要註冊的憑證按一下 。



5 **按一下[註冊憑證...]。**

6 **註冊憑證。**

- 按一下 [瀏覽...] ▶ 指定要註冊的檔案 (憑證) ▶ 按一下 [註冊]。

對於 SCEP 憑證

手動要求 SCEP 伺服器核發憑證。
您只能從遠端使用者介面指定此設定。

註釋

- 如果選擇了 [啟用憑證自動發行要求定時器]，則不能傳送核發憑證的手動要求。如果已選擇此選項，請取消選擇。

啟動遠端使用者介面 ▶ 按一下 [設定/註冊] ▶ [裝置管理] ▶ [憑證發行要求的設定(SCEP)] ▶ [憑證自動發行要求設定] ▶ 取消選擇 [啟用憑證自動發行要求定時器] ▶ 按一下 [更新]。

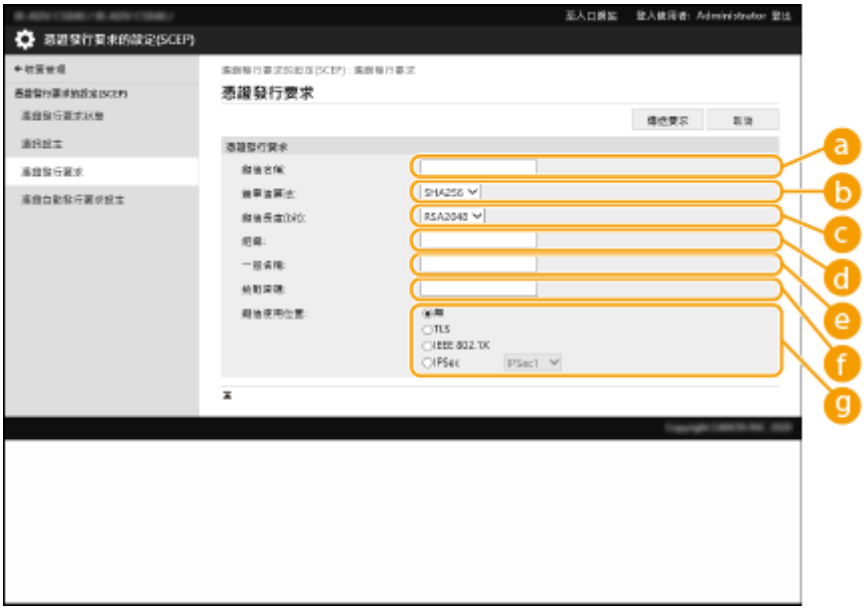
1 **啟動遠端使用者介面。**

2 **按一下入口網站頁面的 [設定/註冊]。**

3 **按一下 [裝置管理] ▶ [憑證發行要求的設定(SCEP)]。**

4 **按一下[憑證發行要求]。**

5 **指定要求憑證所需的設定。**



a [鍵值名稱:]

輸入金鑰的名稱。請輸入可在清單中輕鬆找到的名稱。

b [簽章演算法:]

選擇用於簽章的雜湊演算法。

c [鍵值長度(bit):]

選擇金鑰長度。

d [組織:]

輸入組織名稱。

e [一般名稱:]

輸入 IP 位址或 FQDN。

- 在 Windows 環境中執行 IPPS 列印時，確認輸入本機的 IP 位址。
- 需要 DNS 伺服器才可輸入本機的 FQDN。若未使用 DNS 伺服器，請輸入本機的 IP 位址。

f [挑戰密碼:]

若 SCEP 伺服器端設定密碼，請輸入憑證發行要求資料 (PKCS#9) 中的查問密碼。

g [鍵值使用位置:]

選擇 [IEEE 802.1X] (開啟檔案需要密碼)。

註釋:

- 選擇 [無] 以外的選項時，請事先啟用每個功能。如果在停用每個功能的情況下成功取得憑證，則會將憑證指派給金鑰使用位置，但不會自動啟用每個功能。

6 按一下[傳送要求]。

7 按一下[重新啟動]。

步驟 3：重設金鑰和憑證 (IEEE 802.1X)

視機器的機型而定，您可能無法從控制面板執行操作。在這種情況下，請從遠端使用者介面執行操作。
對於 SCEP 憑證不需要執行此程序。

對於自我簽署憑證/CSR 憑證

使用控制面板(P. 36)
使用遠端使用者介面(P. 37)

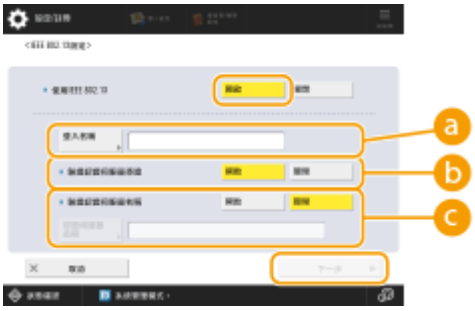
■使用控制面板

1 按下 (設定/註冊)。

2 按 <參數選擇> ▶ <網路> ▶ <IEEE 802.1X 設定>。

3 對於 <使用 IEEE 802.1X> 按 <開啟> ▶ 指定所需的設定 ▶ 按 <下一步>。

範例畫面：



a <登入名稱>

輸入接收 IEEE 802.1X 認證的登入使用者名稱（EAP 身分）。

b <驗證認證伺服器憑證>

驗證從認證伺服器發出的伺服器憑證時，將此設定設為 <開啟>。

c <驗證認證伺服器名稱>

若要確認伺服器憑證中的一般名稱，請選擇 <開啟>。然後輸入在 <認證伺服器名稱> 中註冊登入使用者的認證伺服器名稱。

4 按 <使用 TLS> 的 <開啟> ▶ 按 <鍵值和憑證>。

5 在清單中選擇要使用的金鑰和憑證 ▶ 按 <設定為預設鍵值> ▶ <是>。

6 **按下 <確定>。**

7 **按 (設定/註冊) ▶ (設定/註冊) ▶ <套用設定變更> ▶ <是>。**

➠ 本機重新啟動，然後套用設定。

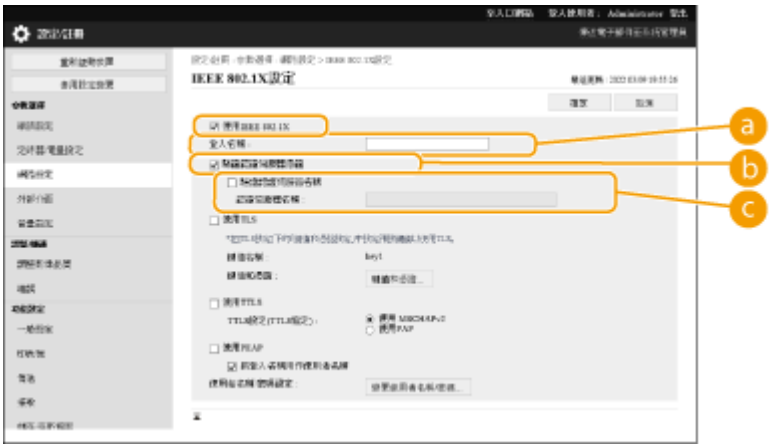
■使用遠端使用者介面

1 **啟動遠端使用者介面。**

2 **按一下入口網站頁面的 [設定/註冊]。**

3 **按一下 [網路設定] ▶ [IEEE 802.1X 設定]。**

4 **選擇 [使用 IEEE 802.1X] ▶ 指定所需的設定。**



a [登入名稱]

輸入接收 IEEE 802.1X 認證的登入使用者名稱（EAP 身分）。

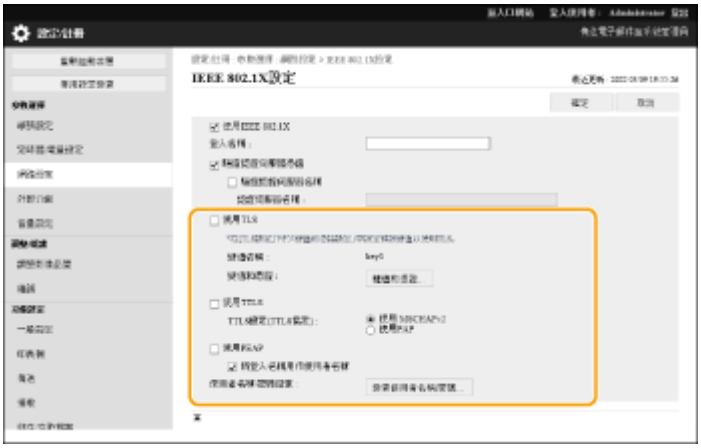
b [驗證認證伺服器憑證]

驗證從認證伺服器發出的伺服器憑證時，勾選此核取方塊。

c [驗證認證伺服器名稱]

若要確認伺服器憑證中的一般名稱，請勾選此核取方塊，然後輸入在 [認證伺服器名稱] 中註冊登入使用者的認證伺服器名稱。

5 **選擇 [使用 TLS] ▶ 按一下 [鍵值和憑證]。**



6 **對清單中要使用的金鑰，按一下 [使用]。**

7 **按一下[確定]。**

8 **按一下 [套用設定變更] 以重新啟動本機。**

➠ 本機重新啟動，然後套用設定。

步驟 4：刪除過去產生的金鑰/憑證 (IEEE 802.1X)

視機器的機型而定，您可能無法從控制面板執行操作。在這種情況下，請從遠端使用者介面執行操作。

註釋

- 停用憑證時，您可能需要向憑證授權單位傳達資訊。請參閱 **檢查您是否必須執行附加程序(P. 5)** ，並在刪除金鑰/憑證之前記下所需資訊。

使用控制面板(P. 39)
使用遠端使用者介面(P. 39)

■使用控制面板

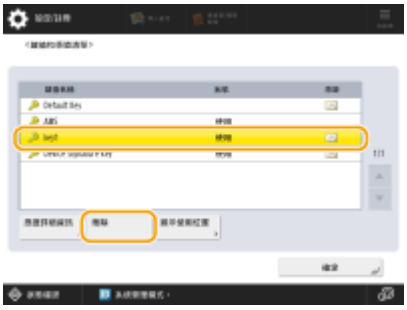
1 **按下 (設定/註冊)。**

2 **按 <管理設定> ▶ <裝置管理> ▶ <憑證設定> ▶ <鍵值和憑證清單> ▶ <本裝置的鍵值和憑證清單>。**

- <本裝置的鍵值和憑證清單> 不會顯示，除非在本機上啟用了使用者簽署功能。在這種情況下，請繼續下一個步驟。

3 **選擇金鑰和憑證 ▶ 按 <刪除> ▶ <是>。**

範例畫面：



註釋:

- 如果顯示 ，表示金鑰損毀或無效。
- 如果未顯示 ，表示金鑰的憑證不存在。
- 如果選擇了金鑰和憑證，並按 <憑證詳細資訊>，則會顯示關於憑證的詳細資訊。您也可以按此畫面上的 <驗證憑證> 以查看憑證是否有效。

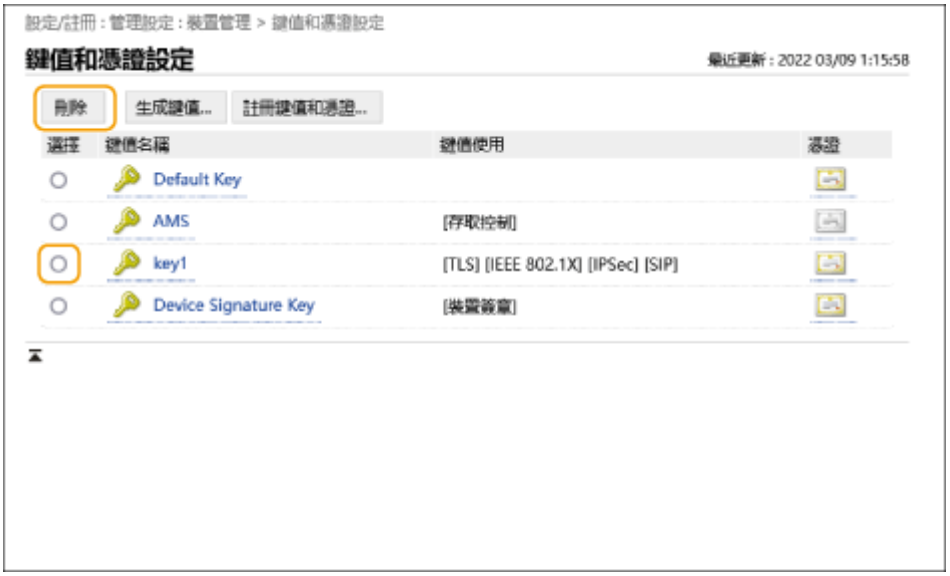
■使用遠端使用者介面

1 **啟動遠端使用者介面。**

2 **按一下入口網站頁面的 [設定/註冊]。**

3 **按一下 [裝置管理] ▶ [鍵值和憑證設定]。**

4 **選擇金鑰和憑證 ▶ 按一下 [刪除] ▶ [確定]。**



註釋

- 如果顯示 ，表示金鑰損毀或無效。
- 如果顯示 ，表示金鑰的憑證不存在。
- 按一下金鑰名稱以顯示有關憑證的詳細資訊。您也可以按一下畫面上的 [確認憑證] 以檢查憑證是否有效。

步驟 5：停用憑證 (IEEE 802.1X)

停用過去產生的憑證。程序會依憑證類型而有不同。

■對於自我簽章憑證

如果在 IEEE 802.1X 認證伺服器中將包含需要附加程序之金鑰的憑證註冊為可信任憑證，請刪除已註冊的憑證。

■對於 CSR/SCEP 憑證

要求核發憑證的憑證授權單位撤銷憑證。請參閱憑證中的 [發佈者] 以瞭解要求的憑證授權單位。

註釋

- 如果在 IEEE 802.1X 認證伺服器中使用 CRL 檢查憑證撤銷，請在撤銷憑證後將更新的 CRL 註冊到電腦或網頁瀏覽器。
- 如果您使用 CRL 以外的方法（例如 OCSP）來檢查憑證撤銷，請執行該方法的程序。

步驟 6：啟用新憑證 (IEEE 802.1X)

啟用憑證。

■對於自我簽章憑證

在 IEEE 802.1X 認證伺服器中將新憑證註冊為可信任憑證。

■對於 CSR/SCEP 憑證

您不需要執行附加程序。

IPSec 的程序

步驟 1：檢查認證方法 (IPSec)(P. 44)
步驟 2：重新產生金鑰和憑證 (IPSec)(P. 46)
步驟 3：重設金鑰和憑證 (IPSec)(P. 53)
步驟 4：刪除過去產生的金鑰/憑證 (IPSec)(P. 55)
步驟 5：停用憑證 (IPSec)(P. 57)
步驟 6：啟用新憑證 (IPSec)(P. 58)

步驟 1：檢查認證方法 (IPSec)

如果 IPSec 中 IKE 設定的認證方法設定為 <數位簽章方法>，您必須執行後續程序。
遵循以下程序檢查認證方法。
視機器的機型而定，您可能無法從控制面板執行操作。在這種情況下，請從遠端使用者介面執行操作。

使用控制面板(P. 44)
使用遠端使用者介面(P. 45)

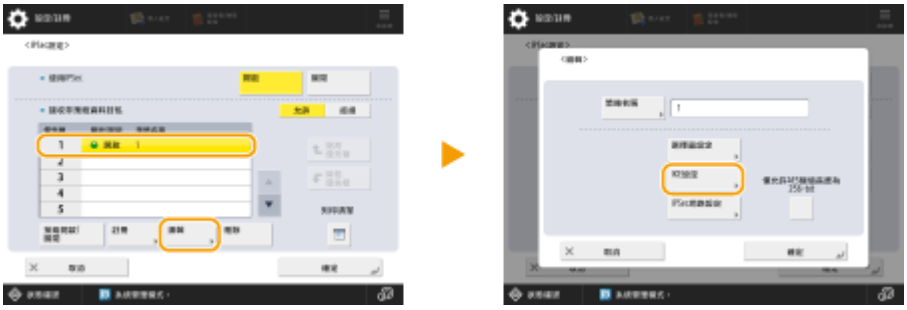
■使用控制面板

1 按下 (設定/註冊)。

2 按 <參數選擇> ▶ <網路> ▶ <TCP/IP 設定> ▶ <IPSec 設定>。

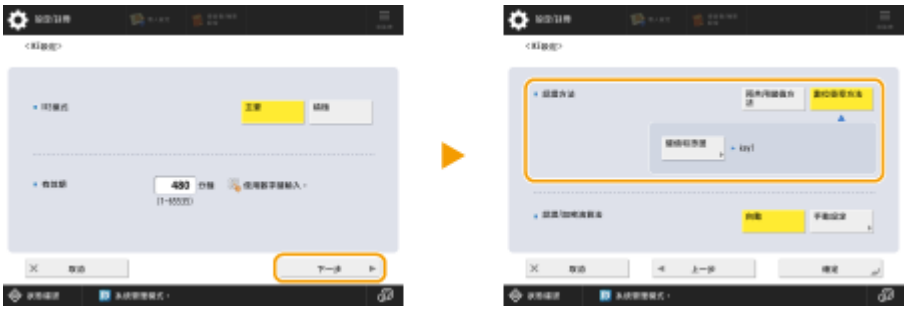
3 選擇已註冊的策略 ▶ 按 <編輯> ▶ <IKE 設定>。

範例畫面：



4 按 <下一步> ▶ 檢查 <認證方法>。

範例畫面：



- 如果 <認證方法> 設為 <數位簽章方法> 並且 <鍵值和憑證> 顯示金鑰名稱，請執行後續程序。
- 如果 <認證方法> 設為 <預共用鍵值方法>，您不需要執行後續程序。

■使用遠端使用者介面

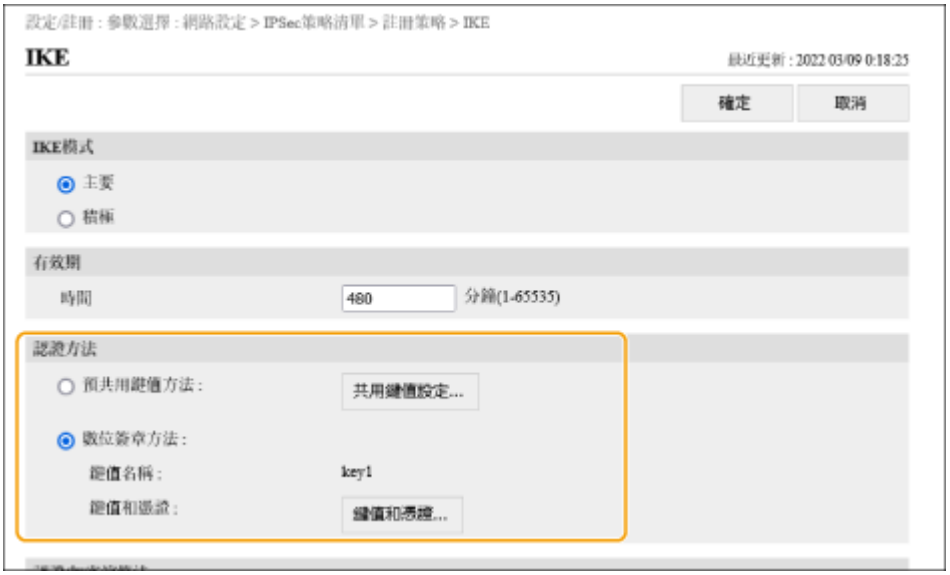
1 **啟動遠端使用者介面。**

2 **按一下入口網站頁面的 [設定/註冊]。**

3 **按一下 [網路設定] ▶ [IPSec 策略清單]。**

4 **按一下清單中的策略 ▶ 按一下 [IKE 設定]。**

5 **檢查 [認證方法]。**



- 如果 [認證方法] 設為 [數位簽章方法] 並顯示金鑰名稱，請執行後續程序。
- 如果 <認證方法> 設為 <預共用鍵值方法>，您不需要執行後續程序。

步驟 2：重新產生金鑰和憑證 (IPSec)

您可以為本機產生的金鑰產生三種類型的憑證：自我簽章憑證、CSR 憑證和 SCEP 憑證。程序會依憑證類型而有不同。視機器的機型而定，您可能無法從控制面板執行操作。在這種情況下，請從遠端使用者介面執行操作。

對於自我簽章憑證(P. 46)
對於 CSR 憑證(P. 49)
對於 SCEP 憑證(P. 51)

對於自我簽章憑證

使用控制面板(P. 46)
使用遠端使用者介面(P. 47)

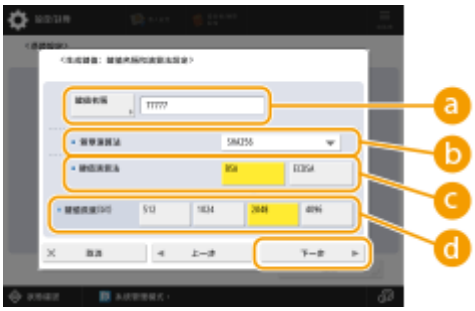
■使用控制面板

1 按下 (設定/註冊)。

2 按 <管理設定> ▶ <裝置管理> ▶ <憑證設定> ▶ <生成鍵值> ▶ <生成網路通訊鍵值>。

3 指定所需的設定，然後前進到下一個畫面。

範例畫面：



a <鍵值名稱>

輸入金鑰的名稱。請輸入可在清單中輕鬆找到的名稱。

b <簽章演算法>

選擇要用於簽章的雜湊演算法。視金鑰長度，可用的雜湊演算法會有不同。長度為 1024 位元或以上的金鑰可支援 SHA384 和 SHA512 雜湊演算法。如果針對 c 選擇了 <RSA>，且針對 d 將 <鍵值長度(bit)> 設定為 <1024> 或更多，可以選擇 SHA384 和 SHA512 雜湊演算法。

c <鍵值演算法>

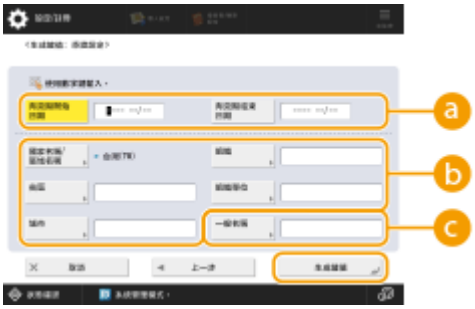
選擇金鑰演算法。如果選擇 <RSA>，<鍵值長度(bit)> 會顯示為 d 的設定項目。如果選擇 <ECDSA>，會改為顯示 <鍵值類型>。

d <鍵值長度(bit)>/<鍵值類型>

無果針對 c 選擇了 <RSA>，請指定金鑰長度，或如果選擇了 <ECDSA>，請指定金鑰類型。在兩種情況中，較高的值提供較好的安全性但會降低通訊處理速度。

4 設定憑證的必要項目 ▶ 按 <生成鍵值>。

範例畫面：



a <有效期開始日期>/<有效期結束日期>

輸入憑證有效期的開始日期和結束日期。

b <國家名稱/區域名稱>/<省區>/<城市>/<組織>/<組織單位>

從清單中選擇國碼，然後輸入地點和組織名稱。

c <一般名稱>

輸入 IP 位址或 FQDN。

- 在 Windows 環境中執行 IPPS 列印時，確認輸入本機的 IP 位址。
- 需要 DNS 伺服器才可輸入本機的 FQDN。若未使用 DNS 伺服器，請輸入本機的 IP 位址。

■使用遠端使用者介面

1 啟動遠端使用者介面。

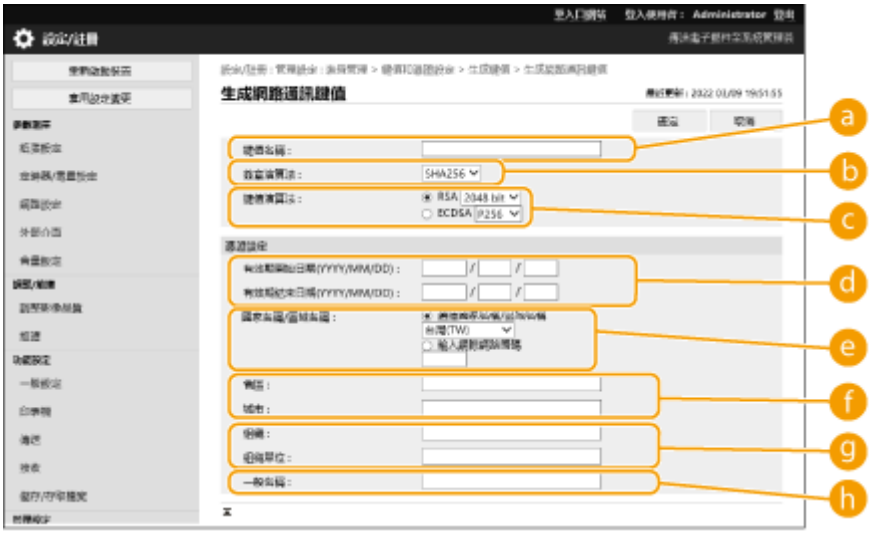
2 按一下入口網站頁面的 [設定/註冊]。

3 按一下 [裝置管理] ▶ [鍵值和憑證設定]。

4 按一下[生成鍵值]。

5 按一下[網路通訊]。

6 指定金鑰和憑證設定。



a [鍵值名稱]

使用英數字元輸入金鑰名稱。請輸入可在清單中輕鬆找到的名稱。

b [簽章演算法]

選擇要用於簽章的雜湊演算法。視金鑰長度，可用的雜湊演算法會有不同。長度為 1024 位元或以上的金鑰可支援 SHA384 和 SHA512 雜湊演算法。

c [鍵值演算法]

選擇 [RSA] 或 [ECDSA] 金鑰產生作為演算法。如果選擇 [RSA]，請指定金鑰長度，或如果選擇 [ECDSA]，請指定金鑰類型。在兩種情況中，較高的值提供較好的安全性但會降低通訊處理速度。

註釋:

- 如果您對 [簽章演算法] 選擇 [SHA384] 或 [SHA512]，則當對 [鍵值演算法] 選擇 [RSA] 時，不能將金鑰長度設定為 [512 bit]。

d [有效期開始日期(YYYY/MM/DD)]/[有效期結束日期(YYYY/MM/DD)]

輸入憑證有效期的開始日期和結束日期。您不能將 [有效期結束日期(YYYY/MM/DD)] 設定為早於 [有效期開始日期(YYYY/MM/DD)] 中的日期。

e [國家名稱/區域名稱]

按一下 [選擇國家名稱/區域名稱]，然後從下拉清單中選擇國家/區域。或者，按一下 [輸入網際網路國碼]，然後輸入國碼，例如「US」代表美國。

f [省區]/[城市]

視需要使用英數字元輸入位置。

g [組織]/[組織單位]

視需要使用英數字元輸入組織名稱。

h [一般名稱]

視需要使用英數字元輸入憑證的一般名稱。「一般名稱」通常縮寫為「CN」。

7 按一下[確定]。

- 金鑰和憑證的產生可能要花一點時間。
- 產生的金鑰和憑證會自動註冊到本機。

對於 CSR 憑證

在本機上產生金鑰和 CSR。使用畫面上顯示的 CSR 資料或輸出為檔案以要求憑證授權單位核發憑證。然後為金鑰註冊核發的憑證。
您只能從遠端使用者介面指定此設定。

■1. 產生金鑰和 CSR

1 **啟動遠端使用者介面。**

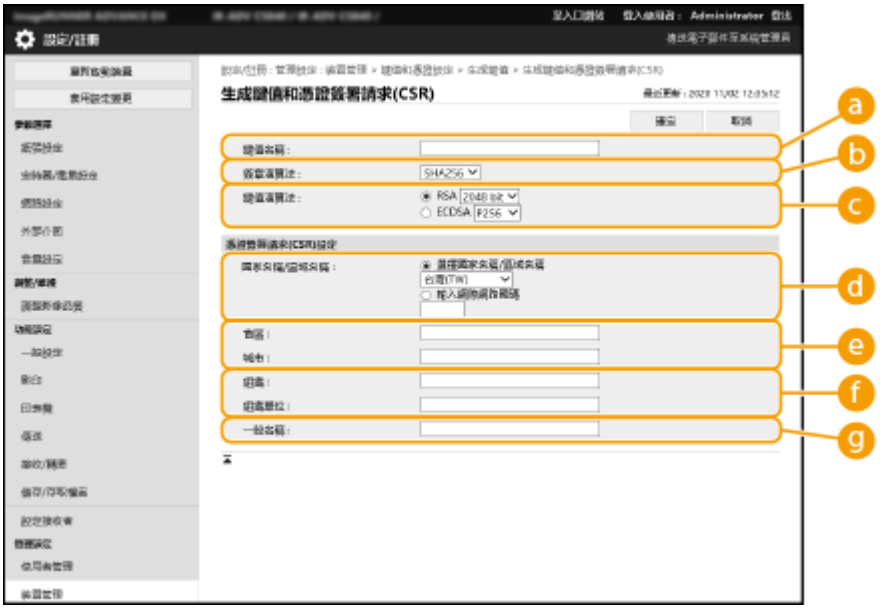
2 **按一下入口網站頁面的 [設定/註冊]。**

3 **按一下 [裝置管理] ▶ [鍵值和憑證設定]。**

4 **按一下[生成鍵值]。**

5 **按一下[鍵值和憑證簽署請求(CSR)]。**

6 **指定金鑰和憑證設定。**



a [鍵值名稱]

輸入金鑰的名稱。請輸入可在清單中輕鬆找到的名稱。

b [簽章演算法]

選擇用於簽章的雜湊演算法。

[鍵值演算法]

選擇金鑰演算法，然後在選擇 [RSA] 時指定金鑰長度，或是在選擇 [ECDSA] 時指定金鑰類型。

[國家名稱/區域名稱]

從清單中選擇國家代碼，或是直接輸入國家代碼。

[省區]/[城市]

輸入位置。

[組織]/[組織單位]

輸入組織名稱。

[一般名稱]

輸入 IP 位址或 FQDN。

- 在 Windows 環境中執行 IPPS 列印時，確認輸入本機的 IP 位址。
- 需要 DNS 伺服器才可輸入本機的 FQDN。若未使用 DNS 伺服器，請輸入本機的 IP 位址。

7 按一下[確定]。

➠ 隨即顯示 CSR 資料。

- 如果您希望將 CSR 資料儲存至檔案，請按一下 [儲存到檔案中] 然後指定儲存位置。

註釋:

- 產生 CSR 的金鑰將會顯示在金鑰與憑證清單畫面上，但是您沒有辦法自行使用。若要使用此金鑰，您需要註冊稍後根據 CSR 核發的憑證。

8 要求憑證授權單位根據 CSR 資料核發憑證。

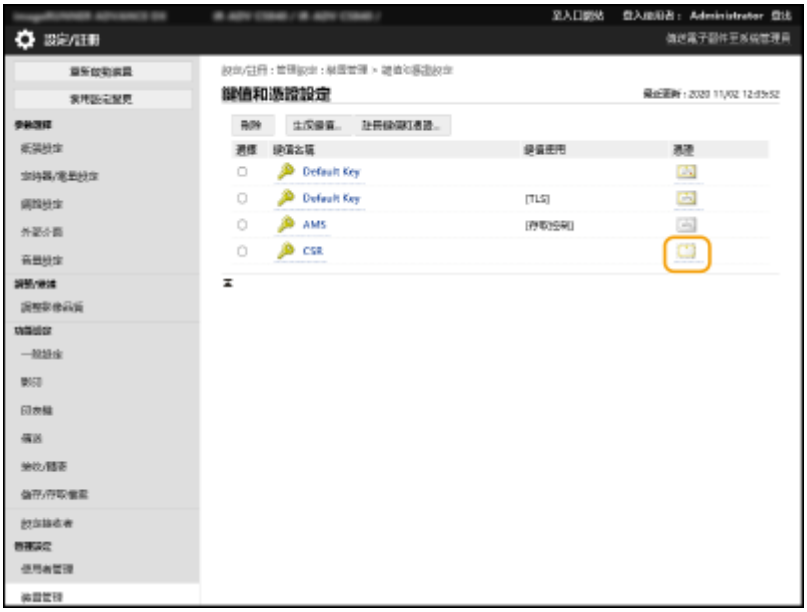
■2. 將核發的憑證註冊到金鑰

1 啟動遠端使用者介面。

2 按一下入口網站頁面的 [設定/註冊]。

3 按一下 [裝置管理] ▶ [鍵值和憑證設定]。

4 在 [憑證] 清單中，為想要註冊的憑證按一下 。



5 **按一下[註冊憑證...]。**

6 **註冊憑證。**

- 按一下 [瀏覽...] ▶ 指定要註冊的檔案 (憑證) ▶ 按一下 [註冊]。

對於 SCEP 憑證

手動要求 SCEP 伺服器核發憑證。
您只能從遠端使用者介面指定此設定。

註釋

- 如果選擇了 [啟用憑證自動發行要求定時器]，則不能傳送核發憑證的手動要求。如果已選擇此選項，請取消選擇。

啟動遠端使用者介面 ▶ 按一下 [設定/註冊] ▶ [裝置管理] ▶ [憑證發行要求的設定(SCEP)] ▶ [憑證自動發行要求設定] ▶ 取消選擇 [啟用憑證自動發行要求定時器] ▶ 按一下 [更新]。

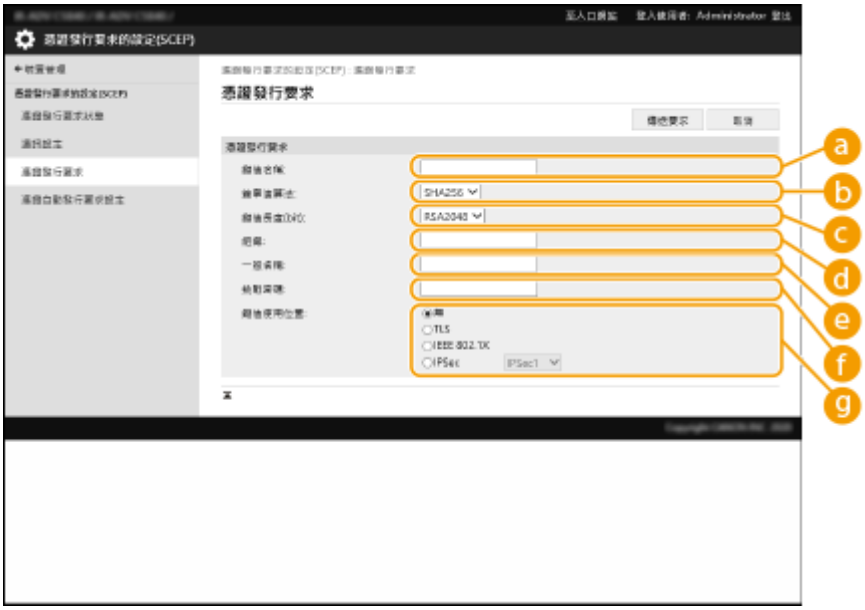
1 **啟動遠端使用者介面。**

2 **按一下入口網站頁面的 [設定/註冊]。**

3 **按一下 [裝置管理] ▶ [憑證發行要求的設定(SCEP)]。**

4 **按一下[憑證發行要求]。**

5 **指定要求憑證所需的設定。**



a [鍵值名稱:]

輸入金鑰的名稱。請輸入可在清單中輕鬆找到的名稱。

b [簽章演算法:]

選擇用於簽章的雜湊演算法。

c [鍵值長度(bit):]

選擇金鑰長度。

d [組織:]

輸入組織名稱。

e [一般名稱:]

輸入 IP 位址或 FQDN。

- 在 Windows 環境中執行 IPPS 列印時，確認輸入本機的 IP 位址。
- 需要 DNS 伺服器才可輸入本機的 FQDN。若未使用 DNS 伺服器，請輸入本機的 IP 位址。

f [挑戰密碼:]

若 SCEP 伺服器端設定密碼，請輸入憑證發行要求資料 (PKCS#9) 中的查問密碼。

g [鍵值使用位置:]

選擇 [IPSec] (開啟檔案需要密碼)。

註釋:

- 選擇 [無] 以外的選項時，請事先啟用每個功能。如果在停用每個功能的情況下成功取得憑證，則會將憑證指派給金鑰使用位置，但不會自動啟用每個功能。

6 按一下[傳送要求]。

7 按一下[重新啟動]。

步驟 3：重設金鑰和憑證 (IPSec)

視機器的機型而定，您可能無法從控制面板執行操作。在這種情況下，請從遠端使用者介面執行操作。
對於 SCEP 憑證不需要執行此程序。

對於自我簽署憑證/CSR 憑證

使用控制面板(P. 53)
使用遠端使用者介面(P. 54)

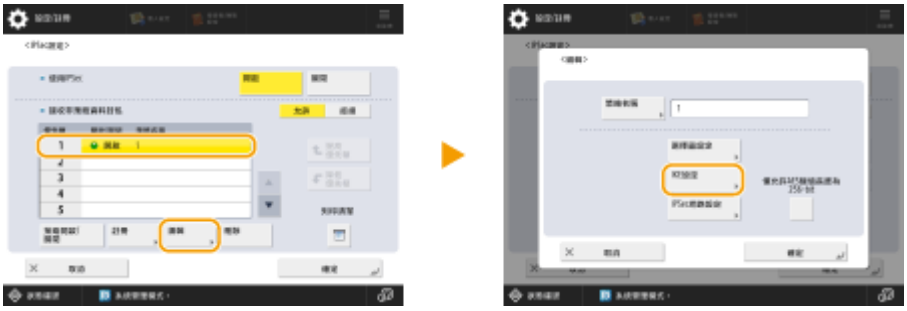
■使用控制面板

1 **按下 (設定/註冊)。**

2 **按 <參數選擇> ▶ <網路> ▶ <TCP/IP 設定> ▶ <IPSec 設定>。**

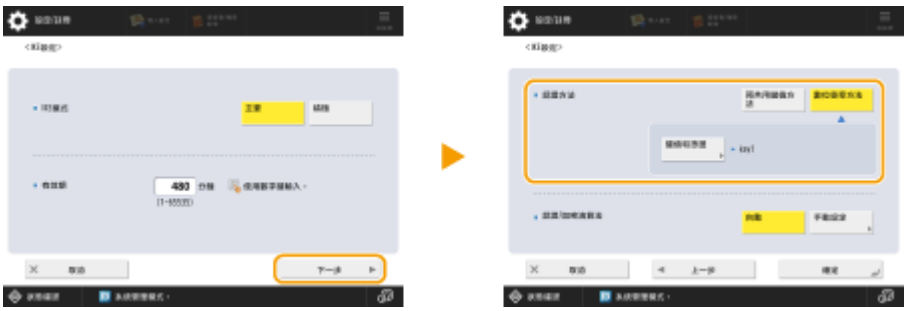
3 **選擇重設金鑰和憑證的策略 ▶ 按 <編輯> ▶ <IKE 設定>。**

範例畫面：



4 **按 <下一步> ▶ 在 <認證方法> 中選擇 <數位簽章方法> ▶ 按 <鍵值和憑證>。**

範例畫面：



5 **在清單中選擇要使用的金鑰和憑證 ▶ 按 <設定為預設鍵值> ▶ <是>。**

6 **按下 <確定>。**

7 **按 (設定/註冊) ▶ (設定/註冊) ▶ <套用設定變更> ▶ <是>。**

➠ 本機重新啟動，然後套用設定。

■使用遠端使用者介面

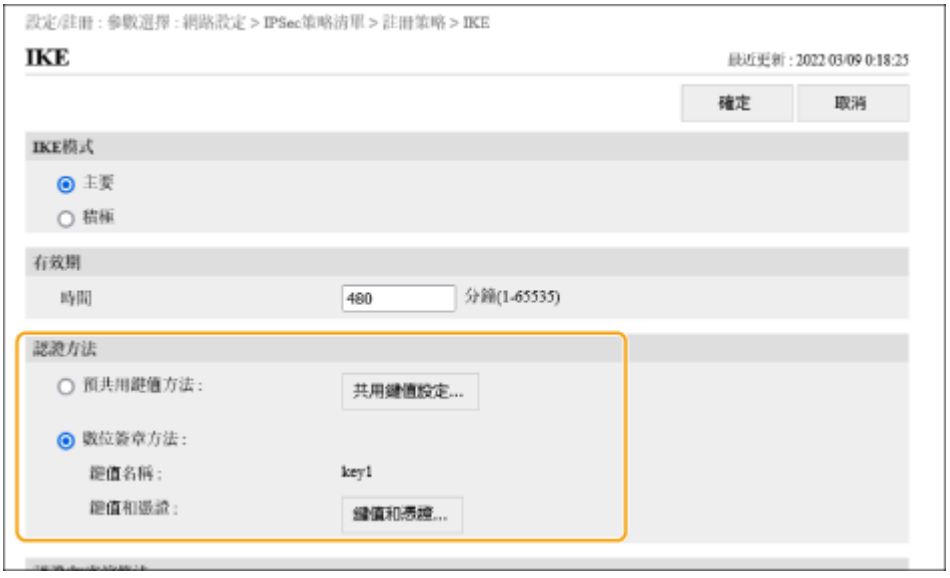
1 **啟動遠端使用者介面。**

2 **按一下入口網站頁面的 [設定/註冊]。**

3 **按一下 [網路設定] ▶ [IPSec 策略清單]。**

4 **在清單中按一下重設金鑰和憑證的策略 ▶ 按一下 [IKE 設定]。**

5 **選擇 [認證方法] 中的 [數位簽章方法] ▶ 按一下 [鍵值和憑證]。**



6 **對清單中要使用的金鑰，按一下 [使用]。**

7 **按一下[確定]。**

8 **按一下 [套用設定變更] 以重新啟動本機。**

➠ 本機重新啟動，然後套用設定。

步驟 4：刪除過去產生的金鑰/憑證 (IPSec)

視機器的機型而定，您可能無法從控制面板執行操作。在這種情況下，請從遠端使用者介面執行操作。

註釋

- 停用憑證時，您可能需要向憑證授權單位傳達資訊。請參閱 **檢查您是否必須執行附加程序(P. 5)** ，並在刪除金鑰/憑證之前記下所需資訊。

使用控制面板(P. 55)
使用遠端使用者介面(P. 55)

■使用控制面板

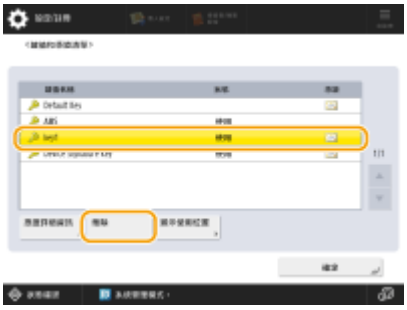
1 **按下 (設定/註冊)。**

2 **按 <管理設定> ▶ <裝置管理> ▶ <憑證設定> ▶ <鍵值和憑證清單> ▶ <本裝置的鍵值和憑證清單>。**

- <本裝置的鍵值和憑證清單> 不會顯示，除非在本機上啟用了使用者簽署功能。在這種情況下，請繼續下一個步驟。

3 **選擇金鑰和憑證 ▶ 按 <刪除> ▶ <是>。**

範例畫面：



註釋:

- 如果顯示 ，表示金鑰損毀或無效。
- 如果未顯示 ，表示金鑰的憑證不存在。
- 如果選擇了金鑰和憑證，並按 <憑證詳細資訊>，則會顯示關於憑證的詳細資訊。您也可以按此畫面上的 <驗證憑證> 以查看憑證是否有效。

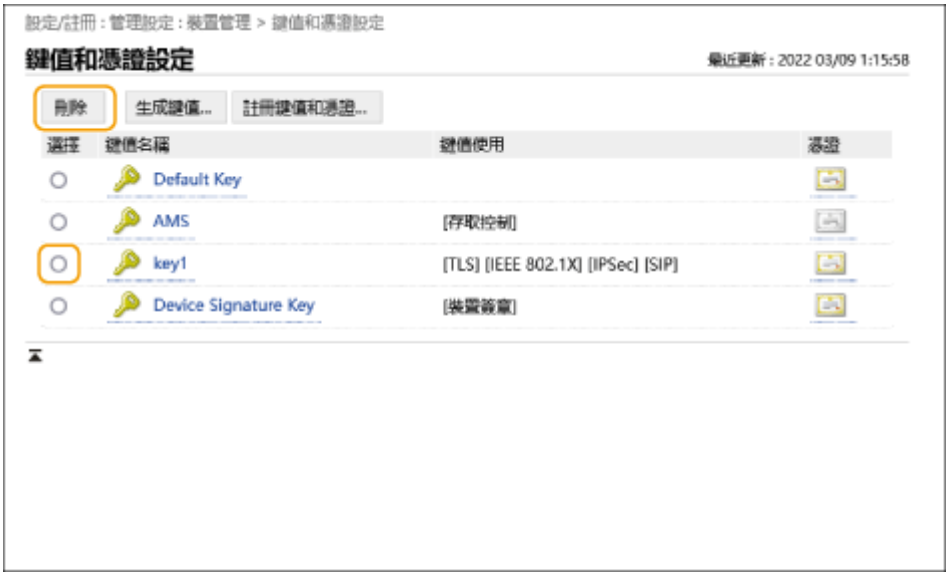
■使用遠端使用者介面

1 **啟動遠端使用者介面。**

2 **按一下入口網站頁面的 [設定/註冊]。**

3 **按一下 [裝置管理] ▶ [鍵值和憑證設定]。**

4 **選擇金鑰和憑證 ▶ 按一下 [刪除] ▶ [確定]。**



註釋

- 如果顯示 ，表示金鑰損毀或無效。
- 如果顯示 ，表示金鑰的憑證不存在。
- 按一下金鑰名稱以顯示有關憑證的詳細資訊。您也可以按一下畫面上的 [確認憑證] 以檢查憑證是否有效。

步驟 5：停用憑證 (IPSec)

停用過去產生的憑證。程序會依憑證類型而有不同。

■對於自我簽章憑證

如果在透過 IPSec 通訊的裝置中將包含需要附加程序之金鑰的憑證註冊為可信任憑證，請刪除已註冊的憑證。刪除已註冊的憑證後，請註冊重新產生之金鑰的憑證。

■對於 CSR/SCEP 憑證

要求核發憑證的憑證授權單位撤銷憑證。請參閱憑證中的 [發佈者] 以瞭解要求的憑證授權單位。

註釋

- 如果在透過 IPSec 通訊的裝置中使用 CRL 檢查憑證撤銷，請在撤銷憑證後將更新的 CRL 註冊到電腦或網頁瀏覽器。
- 如果您使用 CRL 以外的方法（例如 OCSP）來檢查憑證撤銷，請執行該方法的程序。

步驟 6：啟用新憑證 (IPSec)

啟用憑證。

■對於自我簽章憑證

在透過 IPSec 通訊的裝置中將新憑證註冊為可信任憑證。

■對於 CSR/SCEP 憑證

您不需要執行附加程序。

SIP 的程序

步驟 1：檢查設定 (SIP)(P. 60)
步驟 2：重新產生金鑰和憑證 (SIP)(P. 63)
步驟 3：重設金鑰和憑證 (SIP)(P. 69)
步驟 4：刪除過去產生的金鑰/憑證 (SIP)(P. 72)
步驟 5：停用憑證 (SIP)(P. 74)
步驟 6：啟用新憑證 (SIP)(P. 75)

步驟 1：檢查設定 (SIP)

滿足以下兩個條件時，必須執行附加程序：

- 在 <SIP 設定> 的 <內部網路設定> 中啟用了 <使用 TLS>
- 在 <SIP 設定> 的 <TLS 設定> 中 <鍵值和憑證> 顯示金鑰名稱

遵循以下程序檢查設定。

使用控制面板(P. 60)
使用遠端使用者介面(P. 61)

使用控制面板

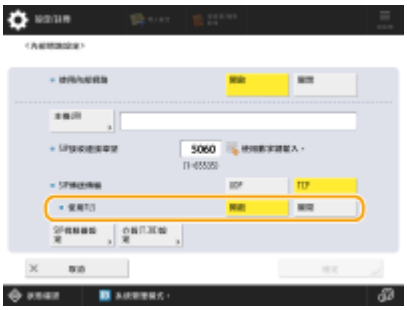
■檢查 <使用 TLS>

1 按下 (設定/註冊)。

2 按 <參數選擇> ▶ <網路> ▶ <TCP/IP 設定> ▶ <SIP 設定> ▶ <內部網路設定>。

3 檢查 <使用 TLS>。

範例畫面：



- 如果 <使用 TLS> 設為 <開啟>，請繼續檢查 <鍵值和憑證>。
- 如果 <使用 TLS> 設為 <關閉>，您不需要執行後續程序。

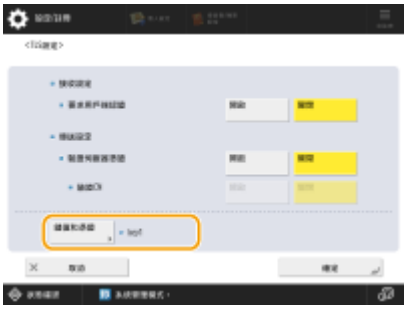
■檢查 <鍵值和憑證>

1 按下 (設定/註冊)。

2 按 <參數選擇> ▶ <網路> ▶ <TCP/IP 設定> ▶ <SIP 設定> ▶ <TLS 設定>。

3 **檢查 <鍵值和憑證> 是否顯示金鑰名稱。**

範例畫面：



- 如果 <鍵值和憑證> 顯示金鑰名稱，請執行後續程序。
- 如果 <鍵值和憑證> 沒有顯示金鑰名稱，則不需要執行後續程序。

使用遠端使用者介面

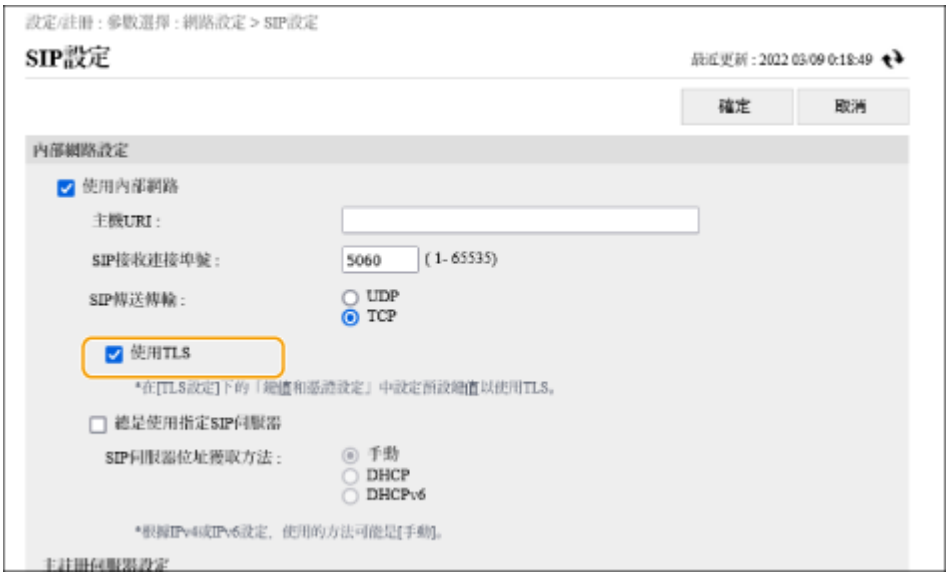
■檢查 [使用 TLS] 和 [鍵值和憑證]

1 **啟動遠端使用者介面。**

2 **按一下入口網站頁面的 [設定/註冊]。**

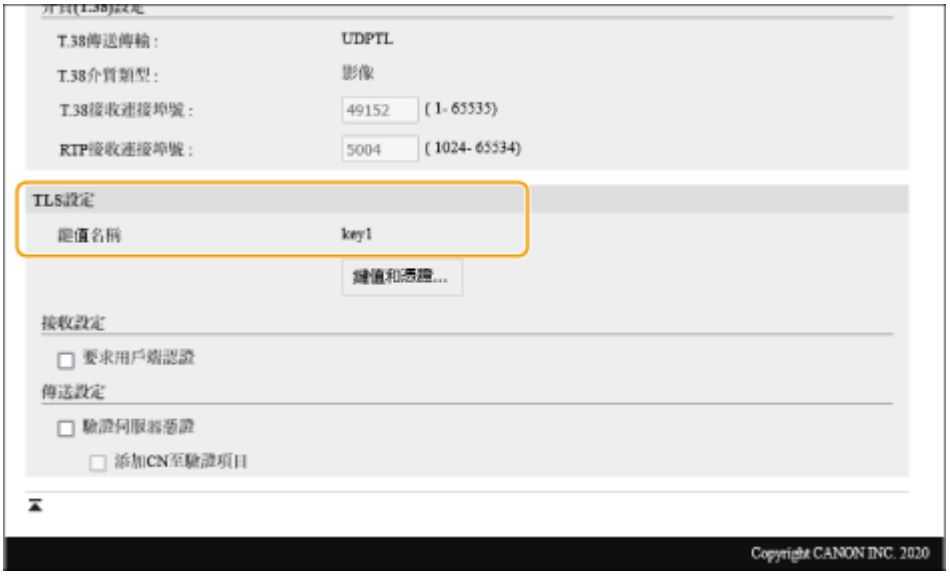
3 **按一下 [網路設定] ▶ [SIP 設定]。**

4 **檢查 [內部網路設定] 中的 [使用 TLS]。**



- 如果選擇了 [使用 TLS]，請繼續檢查 [鍵值和憑證]。
- 如果取消選擇 [使用 TLS]，您不需要執行後續程序。

5 檢查 [TLS 設定] 中的 [鍵值名稱]。



- 如果顯示金鑰名稱，請執行後續程序。
- 如果沒有顯示金鑰名稱，則不需要執行後續程序。

步驟 2：重新產生金鑰和憑證 (SIP)

您可以為本機產生的金鑰產生兩種類型的憑證：自我簽章憑證和 CSR 憑證。程序會依憑證類型而有不同。
視機器的機型而定，您可能無法從控制面板執行操作。在這種情況下，請從遠端使用者介面執行操作。

對於自我簽章憑證(P. 63)
對於 CSR 憑證(P. 66)

對於自我簽章憑證

使用控制面板(P. 63)
使用遠端使用者介面(P. 64)

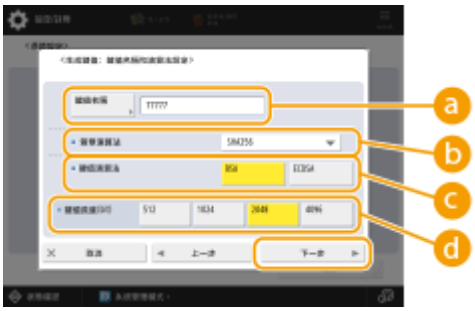
■使用控制面板

1 按下 (設定/註冊)。

2 按 <管理設定> ▶ <裝置管理> ▶ <憑證設定> ▶ <生成鍵值> ▶ <生成網路通訊鍵值>。

3 指定所需的設定，然後前進到下一個畫面。

範例畫面：



a <鍵值名稱>

輸入金鑰的名稱。請輸入可在清單中輕鬆找到的名稱。

b <簽章演算法>

選擇要用於簽章的雜湊演算法。視金鑰長度，可用的雜湊演算法會有不同。長度為 1024 位元或以上的金鑰可支援 SHA384 和 SHA512 雜湊演算法。如果針對 c 選擇了 <RSA>，且針對 d 將 <鍵值長度(bit)> 設定為 <1024> 或更多，可以選擇 SHA384 和 SHA512 雜湊演算法。

c <鍵值演算法>

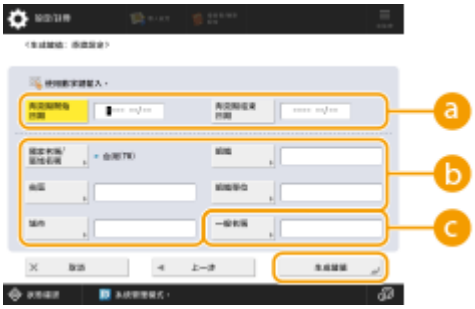
選擇金鑰演算法。如果選擇 <RSA>，<鍵值長度(bit)> 會顯示為 d 的設定項目。如果選擇 <ECDSA>，會改為顯示 <鍵值類型>。

d <鍵值長度(bit)>/<鍵值類型>

無果針對 c 選擇了 <RSA>，請指定金鑰長度，或如果選擇了 <ECDSA>，請指定金鑰類型。在兩種情況中，較高的值提供較好的安全性但會降低通訊處理速度。

4 設定憑證的必要項目 ▶ 按 <生成鍵值>。

範例畫面：



a <有效期開始日期>/<有效期結束日期>

輸入憑證有效期的開始日期和結束日期。

b <國家名稱/區域名稱>/<省區>/<城市>/<組織>/<組織單位>

從清單中選擇國碼，然後輸入地點和組織名稱。

c <一般名稱>

輸入 IP 位址或 FQDN。

- 在 Windows 環境中執行 IPPS 列印時，確認輸入本機的 IP 位址。
- 需要 DNS 伺服器才可輸入本機的 FQDN。若未使用 DNS 伺服器，請輸入本機的 IP 位址。

■使用遠端使用者介面

1 啟動遠端使用者介面。

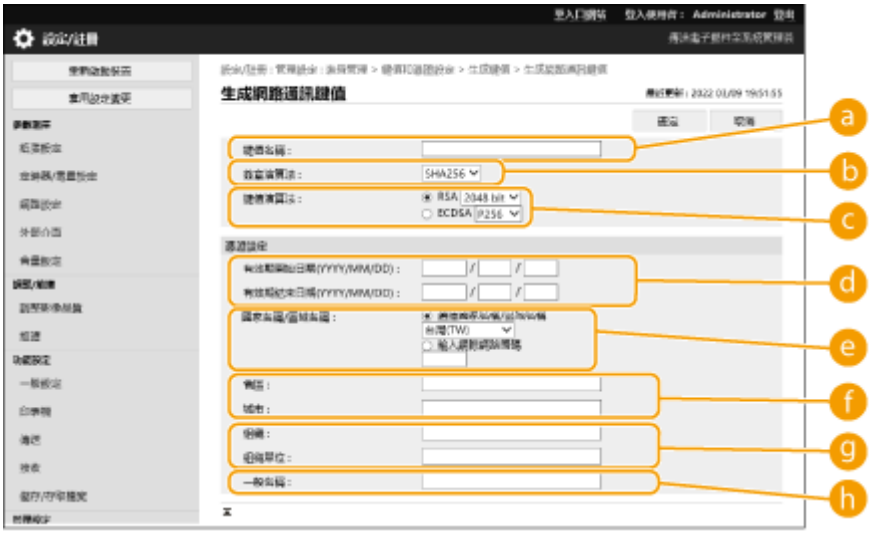
2 按一下入口網站頁面的 [設定/註冊]。

3 按一下 [裝置管理] ▶ [鍵值和憑證設定]。

4 按一下[生成鍵值]。

5 按一下[網路通訊]。

6 指定金鑰和憑證設定。



a [鍵值名稱]

使用英數字元輸入金鑰名稱。請輸入可在清單中輕鬆找到的名稱。

b [簽章演算法]

選擇要用於簽章的雜湊演算法。視金鑰長度，可用的雜湊演算法會有不同。長度為 1024 位元或以上的金鑰可支援 SHA384 和 SHA512 雜湊演算法。

c [鍵值演算法]

選擇 [RSA] 或 [ECDSA] 金鑰產生作為演算法。如果選擇 [RSA]，請指定金鑰長度，或如果選擇 [ECDSA]，請指定金鑰類型。在兩種情況中，較高的值提供較好的安全性但會降低通訊處理速度。

註釋:

- 如果您對 [簽章演算法] 選擇 [SHA384] 或 [SHA512]，則當對 [鍵值演算法] 選擇 [RSA] 時，不能將金鑰長度設定為 [512 bit]。

d [有效期開始日期(YYYY/MM/DD)]/[有效期結束日期(YYYY/MM/DD)]

輸入憑證有效期的開始日期和結束日期。您不能將 [有效期結束日期(YYYY/MM/DD)] 設定為早於 [有效期開始日期(YYYY/MM/DD)] 中的日期。

e [國家名稱/區域名稱]

按一下 [選擇國家名稱/區域名稱]，然後從下拉清單中選擇國家/區域。或者，按一下 [輸入網際網路國碼]，然後輸入國碼，例如「US」代表美國。

f [省區]/[城市]

視需要使用英數字元輸入位置。

g [組織]/[組織單位]

視需要使用英數字元輸入組織名稱。

h [一般名稱]

視需要使用英數字元輸入憑證的一般名稱。「一般名稱」通常縮寫為「CN」。

7 按一下[確定]。

- 金鑰和憑證的產生可能要花一點時間。
- 產生的金鑰和憑證會自動註冊到本機。

對於 CSR 憑證

在本機上產生金鑰和 CSR。使用畫面上顯示的 CSR 資料或輸出為檔案以要求憑證授權單位核發憑證。然後為金鑰註冊核發的憑證。
您只能從遠端使用者介面指定此設定。

■1. 產生金鑰和 CSR

1 **啟動遠端使用者介面。**

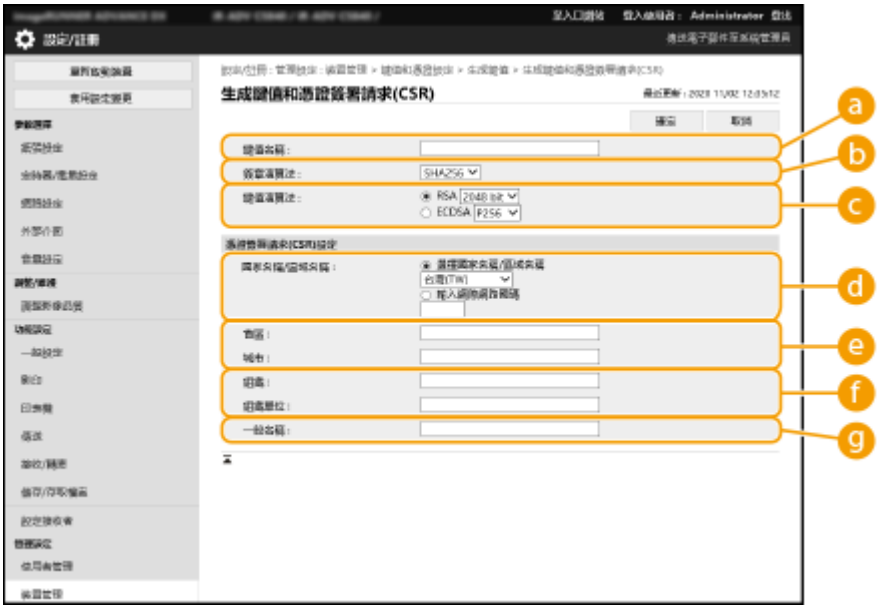
2 **按一下入口網站頁面的 [設定/註冊]。**

3 **按一下 [裝置管理] ▶ [鍵值和憑證設定]。**

4 **按一下[生成鍵值]。**

5 **按一下[鍵值和憑證簽署請求(CSR)]。**

6 **指定金鑰和憑證設定。**



a [鍵值名稱]

輸入金鑰的名稱。請輸入可在清單中輕鬆找到的名稱。

b [簽章演算法]

選擇用於簽章的雜湊演算法。

[鍵值演算法]

選擇金鑰演算法，然後在選擇 [RSA] 時指定金鑰長度，或是在選擇 [ECDSA] 時指定金鑰類型。

[國家名稱/區域名稱]

從清單中選擇國家代碼，或是直接輸入國家代碼。

[省區]/[城市]

輸入位置。

[組織]/[組織單位]

輸入組織名稱。

[一般名稱]

輸入 IP 位址或 FQDN。

- 在 Windows 環境中執行 IPPS 列印時，確認輸入本機的 IP 位址。
- 需要 DNS 伺服器才可輸入本機的 FQDN。若未使用 DNS 伺服器，請輸入本機的 IP 位址。

7 按一下[確定]。

➠ 隨即顯示 CSR 資料。

- 如果您希望將 CSR 資料儲存至檔案，請按一下 [儲存到檔案中] 然後指定儲存位置。

註釋:

- 產生 CSR 的金鑰將會顯示在金鑰與憑證清單畫面上，但是您沒有辦法自行使用。若要使用此金鑰，您需要註冊稍後根據 CSR 核發的憑證。

8 要求憑證授權單位根據 CSR 資料核發憑證。

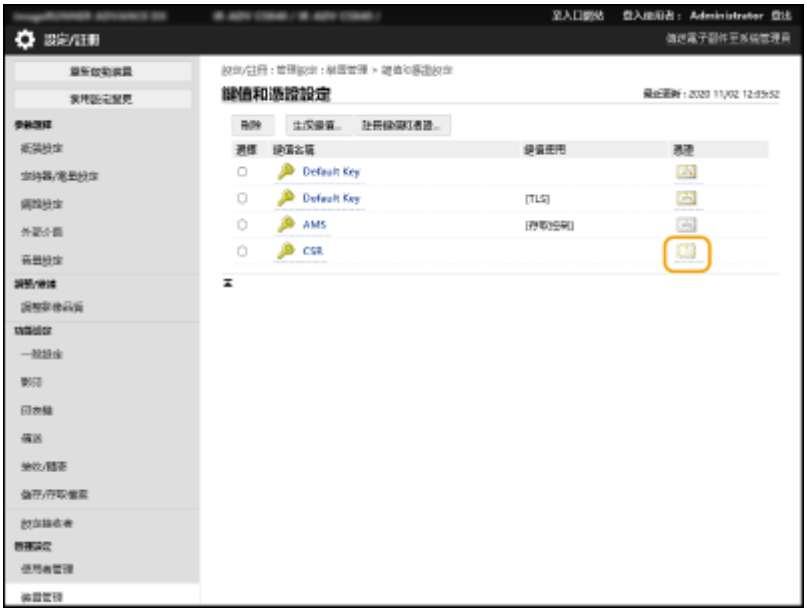
■2. 將核發的憑證註冊到金鑰

1 啟動遠端使用者介面。

2 按一下入口網站頁面的 [設定/註冊]。

3 按一下 [裝置管理] ▶ [鍵值和憑證設定]。

4 在 [憑證] 清單中，為想要註冊的憑證按一下 。



5 按一下[註冊憑證...]。

6 註冊憑證。

- 按一下 [瀏覽...] ▶ 指定要註冊的檔案 (憑證) ▶ 按一下 [註冊]。

步驟 3：重設金鑰和憑證 (SIP)

將產生的金鑰和憑證設定為用於 SIP 之 TLS 加密通訊的金鑰和憑證。

使用控制面板(P. 69)
使用遠端使用者介面(P. 70)

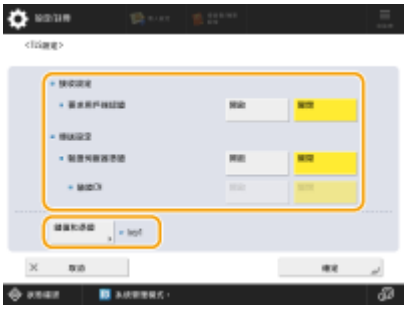
■使用控制面板

1 按下 (設定/註冊)。

2 按 <參數選擇> ▶ <網路> ▶ <TCP/IP 設定> ▶ <SIP 設定> ▶ <TLS 設定>。

3 在 <接收設定> 和 <傳送設定> 中指定各種設定 ▶ 按 <鍵值和憑證>。

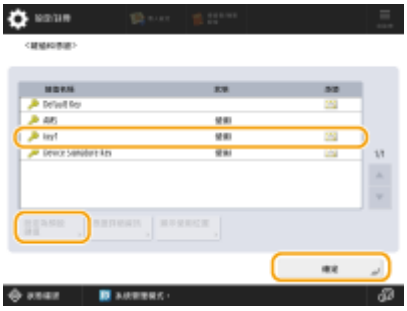
範例畫面：



<接收設定>	
<要求用戶端認證>	選擇 <開啟> 或 <關閉>。 如果您選擇 <開啟>，當本機接收 IP 傳真時會要求客戶端認證。
<傳送設定>	
<驗證伺服器憑證>	選擇 <開啟> 或 <關閉>。 如果您選擇 <開啟>，當本機接收 IP 傳真時會檢查 TLS 伺服器憑證是否有效。
<驗證 CN>	選擇 <開啟> 或 <關閉>。 如果您選擇 <開啟>，當本機接收 IP 傳真時會檢查 CN（一般名稱）。

4 選擇 SIP 的 TLS 加密通訊要使用的金鑰和憑證 ▶ 按 <設定為預設鍵值> ▶ <確定>。

範例畫面：



註釋

- 如果金鑰和憑證的狀態是「使用」，則不能選擇該金鑰和憑證。
- 您可以按 <憑證詳細資訊> 以檢查關於憑證的詳細資訊。
- 您可以按 <顯示使用位置> 以檢查金鑰/憑證用途。

5 **按下 <確定>。**

6 **按 (設定/註冊) ▶ (設定/註冊) ▶ <套用設定變更> ▶ <是>。**

➠ 本機重新啟動，然後套用設定。

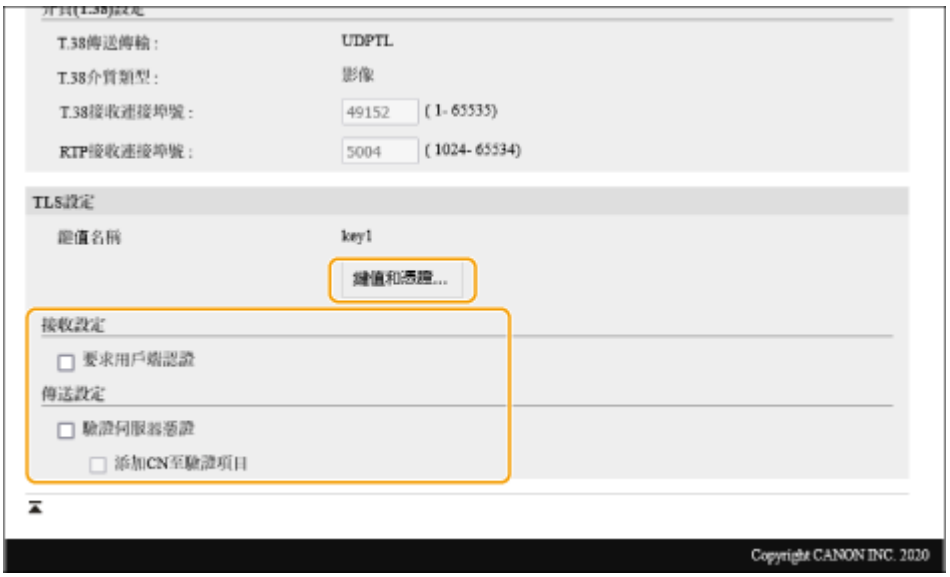
■使用遠端使用者介面

1 **啟動遠端使用者介面。**

2 **按一下入口網站頁面的 [設定/註冊]。**

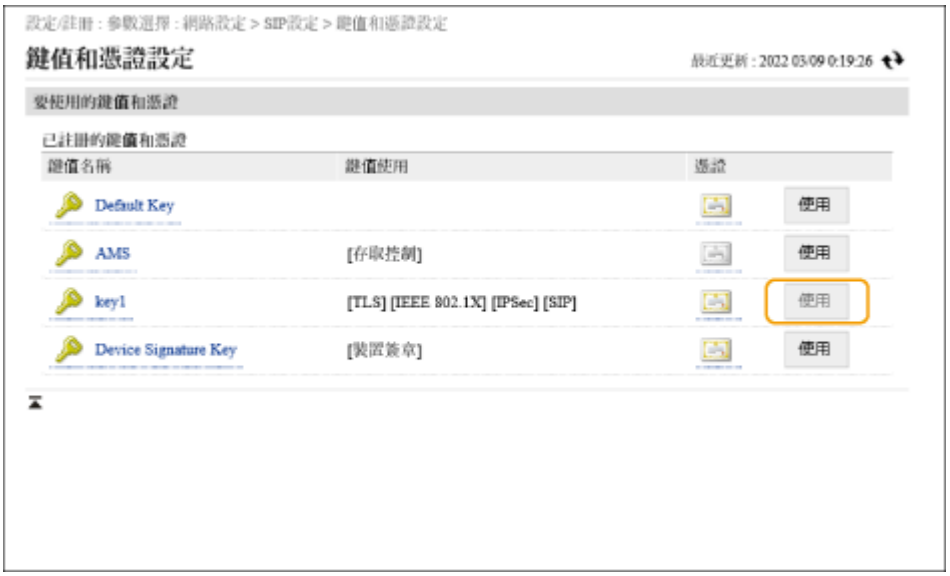
3 **按一下 [網路設定] ▶ [SIP 設定]。**

4 **在 [TLS 設定] 中指定各種設定 ▶ 按一下 [鍵值和憑證]。**



[接收設定]	
[要求用戶端認證]	如果您勾選此核取方塊，當本機接收 IP 傳真時會要求用戶端認證。
[傳送設定]	
[驗證伺服器憑證]	如果勾選此核取方塊，當本機接收 IP 傳真時會檢查 TLS 伺服器憑證是否有效。
[添加 CN 至驗證項目]	選擇 [開啟] 或 [關閉]。 如果您勾選此核取方塊，當本機接收 IP 傳真時會檢查 CN（一般名稱）。

5 對清單中要使用的金鑰，按一下 [使用]。



6 按一下[確定]。

7 按一下 [套用設定變更] 以重新啟動本機。

➠ 本機重新啟動，然後套用設定。

步驟 4：刪除過去產生的金鑰/憑證 (SIP)

視機器的機型而定，您可能無法從控制面板執行操作。在這種情況下，請從遠端使用者介面執行操作。

註釋

- 停用憑證時，您可能需要向憑證授權單位傳達資訊。請參閱 **檢查您是否必須執行附加程序(P. 5)** ，並在刪除金鑰/憑證之前記下所需資訊。

使用控制面板(P. 72)
使用遠端使用者介面(P. 72)

■使用控制面板

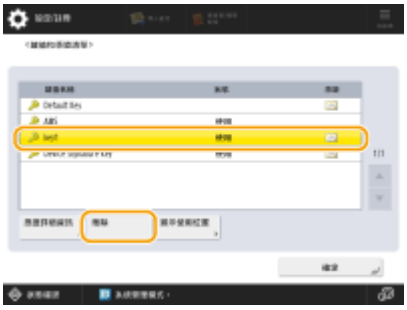
1 **按下 (設定/註冊)。**

2 **按 <管理設定> ▶ <裝置管理> ▶ <憑證設定> ▶ <鍵值和憑證清單> ▶ <本裝置的鍵值和憑證清單>。**

- <本裝置的鍵值和憑證清單> 不會顯示，除非在本機上啟用了使用者簽署功能。在這種情況下，請繼續下一個步驟。

3 **選擇金鑰和憑證 ▶ 按 <刪除> ▶ <是>。**

範例畫面：



註釋:

- 如果顯示 ，表示金鑰損毀或無效。
- 如果未顯示 ，表示金鑰的憑證不存在。
- 如果選擇了金鑰和憑證，並按 <憑證詳細資訊>，則會顯示關於憑證的詳細資訊。您也可以按此畫面上的 <驗證憑證> 以查看憑證是否有效。

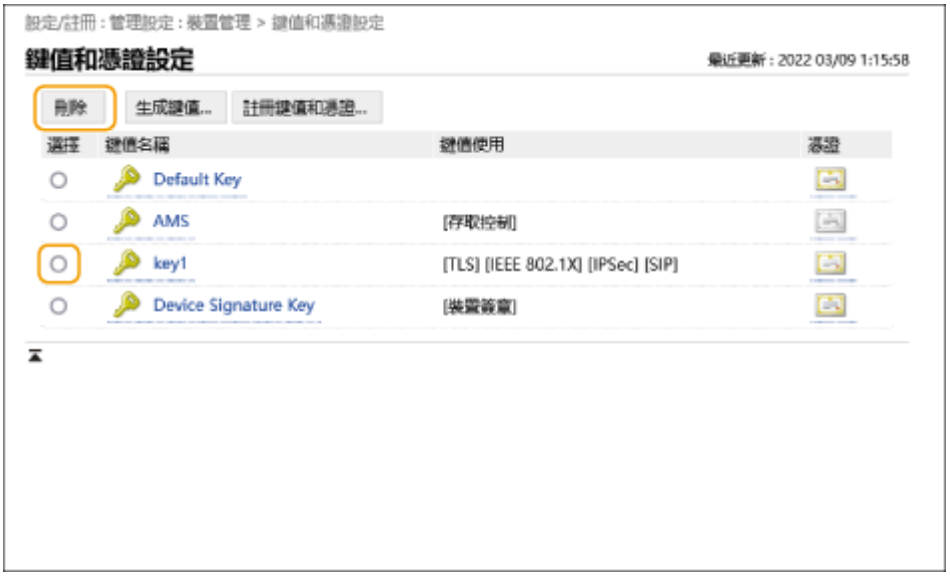
■使用遠端使用者介面

1 **啟動遠端使用者介面。**

2 **按一下入口網站頁面的 [設定/註冊]。**

3 **按一下 [裝置管理] ▶ [鍵值和憑證設定]。**

4 **選擇金鑰和憑證 ▶ 按一下 [刪除] ▶ [確定]。**



註釋

- 如果顯示 ，表示金鑰損毀或無效。
- 如果顯示 ，表示金鑰的憑證不存在。
- 按一下金鑰名稱以顯示有關憑證的詳細資訊。您也可以按一下畫面上的 [確認憑證] 以檢查憑證是否有效。

步驟 5：停用憑證 (SIP)

停用過去產生的憑證。程序會依憑證類型而有不同。

■對於自我簽章憑證

如果在其他 IP 傳真機器中將包含需要附加程序之金鑰的憑證註冊為可信任憑證，請刪除已註冊的憑證。刪除已註冊的憑證後，請註冊重新產生之金鑰的憑證。

■對於 CSR 憑證

要求核發憑證的憑證授權單位撤銷憑證。請參閱憑證中的 [發佈者] 以瞭解要求的憑證授權單位。

註釋

- 如果使用其他 IP 傳真機器檢查憑證撤銷，請在撤銷憑證後將更新的 CRL 註冊到電腦或網頁瀏覽器。
- 如果您使用 CRL 以外的方法（例如 OCSP）來檢查憑證撤銷，請執行該方法的程序。

步驟 6：啟用新憑證 (SIP)

啟用憑證。

■對於自我簽章憑證

在其他 IP 傳真機器中將新憑證註冊為可信任憑證。

■對於 CSR 憑證

您不需要執行附加程序。

裝置簽章的程序

步驟 1：檢查 S/MIME 設定 (裝置簽章)(P. 77)
步驟 2：重新產生金鑰和憑證 (裝置簽章)(P. 79)
步驟 3：停用憑證 (裝置簽章)(P. 80)
步驟 4：啟用新憑證 (裝置簽章)(P. 81)

步驟 1：檢查 S/MIME 設定 (裝置簽章)

檢查您是否需要執行 S/MIME 和裝置簽章的附加程序。

遵循以下程序檢查 S/MIME 設定。

使用控制面板(P. 77)
使用遠端使用者介面(P. 77)

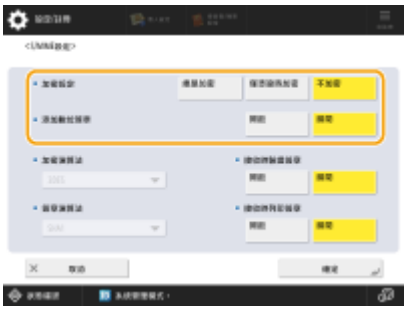
■使用控制面板

1 按下 (設定/註冊)。

2 按 <功能設定> ▶ <傳送> ▶ <電子郵件/網際網路傳真設定> ▶ <S/MIME 設定>。

3 檢查 <加密設定> 和 <添加數位簽章>。

範例畫面：



- 如果 <加密設定> 設定為 <不加密>，且 <添加數位簽章> 設定為 <關閉>，請僅執行裝置簽章的後續程序。
- 如果指定了其他設定，請執行 S/MIME 和裝置簽章的後續程序。

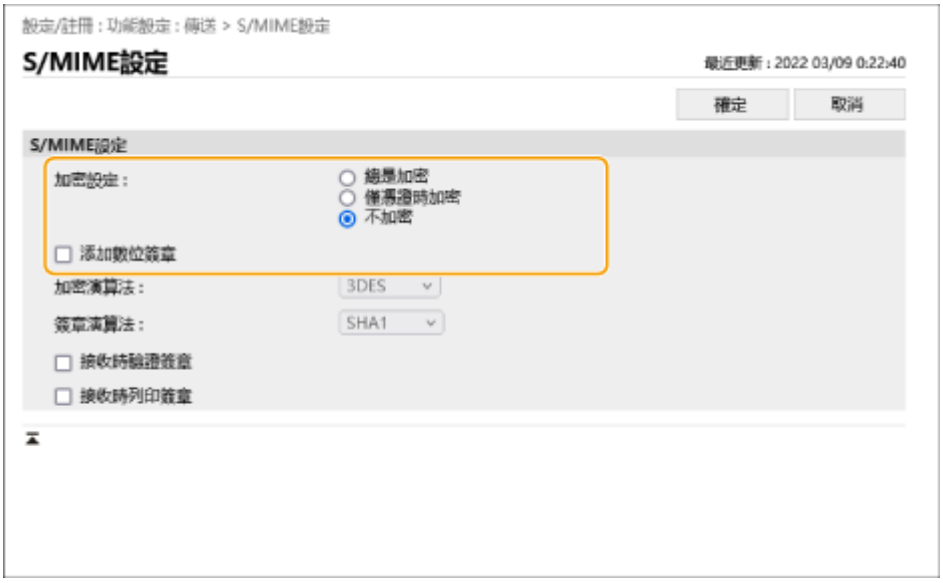
■使用遠端使用者介面

1 啟動遠端使用者介面。

2 按一下入口網站頁面的 [設定/註冊]。

3 按一下 [傳送] ▶ [S/MIME 設定]。

4 檢查 [加密設定] 和 [添加數位簽章]。



- 如果對 [加密設定] 選擇 [不加密]，且取消選擇了 [添加數位簽章]，請僅執行裝置簽章的後續程序。
- 如果指定了其他設定，請執行 S/MIME 和裝置簽章的後續程序。

步驟 2：重新產生金鑰和憑證 (裝置簽章)

使用控制面板(P. 79)
使用遠端使用者介面(P. 79)

■使用控制面板

1 按下 (設定/註冊)。

2 按 <管理設定> ▶ <裝置管理> ▶ <憑證設定> ▶ <生成鍵值>。

3 按 <生成/更新裝置簽章鍵值> ▶ <是> ▶ <確定>。

■使用遠端使用者介面

1 啟動遠端使用者介面。

2 按一下入口網站頁面的 [設定/註冊]。

3 按一下 [裝置管理] ▶ [鍵值和憑證設定]。

4 按一下 [生成鍵值] ▶ [裝置簽章]。

5 按一下 [生成/更新] ▶ [確定]。

步驟 3：停用憑證 (裝置簽章)

停用過去產生憑證。

■如果裝置簽章的憑證已註冊到 Acrobat

如果已在 Acrobat 中註冊裝置簽章的憑證，請刪除已註冊的憑證。

■如果從本機匯出的 S/MIME 憑證已匯入其他機器

如果您本機匯出用於透過 S/MIME 加密電子郵件/I-fax 的公開金鑰憑證（S/MIME 憑證），且將此憑證匯入其他機器，請遵循下列程序從匯入憑證的機器處刪除憑證。

1. **啟動遠端使用者介面。**
2. **按一下入口網站頁面的 [設定/註冊]。**
3. **按一下 [裝置管理] ▶ [S/MIME 憑證設定]。**
4. **選擇對應的憑證 ▶ 按一下 [刪除] ▶ [確定]。**

步驟 4：啟用新憑證 (裝置簽章)

啟用憑證。

■如果裝置簽章的憑證已註冊到 Acrobat

如果已在 Acrobat 中註冊裝置簽章的憑證，請匯出重新產生的裝置簽章憑證，並將新憑證註冊到 Acrobat。

從本機匯出憑證(P. 81)

■如果從本機匯出的 S/MIME 憑證已匯入其他機器

如果您本機匯出用於透過 S/MIME 加密電子郵件/I-fax 的公開金鑰憑證（S/MIME 憑證），且將此憑證匯入其他機器，請匯出重新產生的憑證並將其註冊到其他機器。

從本機匯出憑證(P. 81)
將憑證註冊到其他機器(P. 81)

■從本機匯出憑證

執行下列程序以匯出憑證。

1. **啟動遠端使用者介面。**
2. **按一下入口網站頁面的 [設定/註冊]。**
3. **按一下 [裝置管理] ▶ [匯出裝置簽章]。**
4. **按一下 [開始匯出] ▶ 將檔案儲存到您選擇的位置。**

■將憑證註冊到其他機器

執行下列程序以將憑證註冊到其他機器。

1. **啟動遠端使用者介面。**
2. **按一下入口網站頁面的 [設定/註冊]。**
3. **按一下 [裝置管理] ▶ [S/MIME 憑證設定]。**

4 按一下[註冊 S/MIME 憑證]。

5 註冊 S/MIME 憑證。

- 按一下 [瀏覽...] ▶ 指定要註冊的檔案 (S/MIME 憑證) ▶ 按一下 [註冊]。

藍芽設定的附加程序

藍芽設定的附加程序 84
藍芽的程序 85
步驟 1：刪除在 Canon PRINT Business 中註冊的裝置 (藍芽) 86
步驟 2：將裝置重新註冊到 Canon PRINT Business (藍芽) 87

藍芽設定的附加程序

藍芽的金鑰會在機器更新韌體後自動更新。如果您在行動裝置上使用 Canon PRINT Business 應用程式，您必須重新註冊裝置。

藍芽的程序(P. 85)

藍芽的程序

步驟 1：刪除在 Canon PRINT Business 中註冊的裝置 (藍芽)(P. 86)
步驟 2：將裝置重新註冊到 Canon PRINT Business (藍芽)(P. 87)

步驟 1：刪除在 Canon PRINT Business 中註冊的裝置 (藍芽)

如果藍芽設定為 <開啟>，請遵循以下程序。

iOS 的操作(P. 86)
Android 的操作(P. 86)

■iOS 的操作

1 **輕按 Canon PRINT Business 首頁畫面左上方的 [ ]。**

[選取印表機] 畫面出現。

2 **輕按 [ ] ▶ [刪除]，從清單中刪除裝置。**

■Android 的操作

1 **輕按 Canon PRINT Business 首頁畫面左上方的 [ ]。**

[選取印表機] 畫面出現。

2 **按住裝置名稱 ▶ 在顯示的對話方塊中輕按 [刪除]。**

步驟 2：將裝置重新註冊到 Canon PRINT Business (藍芽)

如果藍芽設定為 <開啟>，請遵循以下程序。

iOS 的操作(P. 87)
Android 的操作(P. 87)

■iOS 的操作

1 輕按 Canon PRINT Business 首頁畫面左上方的 []。

[選取印表機] 畫面出現。

2 輕按 [附近的印表機]。

即會顯示偵測到的裝置。

■如果沒有偵測到裝置

更靠近本機，然後輕按 [搜尋]。藍芽可以偵測裝置的距離最遠為 2 公尺或 80 英吋。

3 選擇裝置 ▶ 輕按 [加入]。

■Android 的操作

1 輕按 Canon PRINT Business 首頁畫面左上方的 []。

[選取印表機] 畫面出現。

2 輕按 [附近的印表機]。

即會顯示偵測到的裝置。

■如果沒有偵測到裝置

更靠近本機，然後輕按 [搜尋]。藍芽可以偵測裝置的距離最遠為 2 公尺或 80 英吋。

3 選擇裝置。

4 在顯示的對話方塊中檢查裝置資訊 ▶ 輕按 [新增]。

如果顯示 Wi-Fi 網路設定畫面，請按照畫面上的指示操作。

Access Management System 設定的附加程序

Access Management System 設定的附加程序 89
Access Management System 設定的程序 90

Access Management System 設定的附加程序

更新機器韌體後，Access Management System 的金鑰會自動更新。

金鑰自動更新約 30 分鐘後，會再次自動擷取限制資訊。之後可以使用 Access Management System 功能正常執行列印。

如果想在韌體更新後立即使用列印驅動程式的 Access Management System 功能進行列印，則需重新手動擷取 Access Management System 的限制資訊。

Access Management System 設定的程序(P. 90)

如果不重新擷取限制資訊就嘗試列印，則會發生錯誤。

Access Management System 設定的程序

如果想在韌體更新後立即使用列印驅動程式的 Access Management System 功能進行列印，您必須手動擷取 Access Management System 的限制資訊。

遵照下面的程序進行操作。

韌體更新後約 30 分鐘後不需要執行以下程序，因為屆時已自動擷取限制資訊。

1 登入到電腦。

2 顯示要搭配啟用 Access Management System 功能之印表機驅動程式使用的印表機內容。

■Windows Vista

- 按一下 [開始] ▶ [控制台] ▶ [硬體和音效] ▶ 選擇 [印表機]。
- 在印表機圖示上按一下滑鼠右鍵 ▶ 選擇 [內容]。

■Windows Server 2008

- 按一下 [開始] ▶ [控制台] ▶ [硬體和音效] ▶ 選擇 [印表機]。
- 在印表機圖示上按一下滑鼠右鍵 ▶ 選擇 [內容]。

■Windows Server 2008 R2

- 按一下 [開始] ▶ [控制台] ▶ [硬體] ▶ 選擇 [裝置和印表機]。
- 在印表機圖示上按一下滑鼠右鍵 ▶ 選擇 [印表機內容]。

■Windows 7

- 按一下 [開始] ▶ [控制台] ▶ [硬體和音效] ▶ 選擇 [裝置和印表機]。
- 在印表機圖示上按一下滑鼠右鍵 ▶ 選擇 [印表機內容]。

■Windows 8.1/Windows Server 2012

- 移至桌面，然後在畫面右側顯示快速鍵。
- 按一下 [設定] ▶ [控制台] ▶ 選擇 [檢視裝置和印表機]。
- 在印表機圖示上按一下滑鼠右鍵 ▶ 選擇 [印表機內容]。

■Windows 10/Windows Server 2016

- 以滑鼠右鍵按一下 [開始] ▶ 選擇 [控制台] ▶ [檢視裝置和印表機]。
- 在印表機圖示上按一下滑鼠右鍵 ▶ 選擇 [印表機內容]。

3 按一下 [AMS] 標籤。

4 按一下[獲取限制資訊]。

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.