(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7208707号
(P7208707)

(45)発行日　令和5年1月19日(2023.1.19)

(24)登録日　令和5年1月11日(2023.1.11)

(51)国際特許分類
Ｈ０４Ｌ　9/08 (2006.01)

ＦＩ
Ｈ０４Ｌ　9/08　F

請求項の数　12　（全23頁）

(21)出願番号　特願2017-28424(P2017-28424)
(22)出願日　平成29年2月17日(2017.2.17)
(65)公開番号　特開2018-133785(P2018-133785A)
(43)公開日　平成30年8月23日(2018.8.23)
審査請求日　令和1年12月16日(2019.12.16)
審判番号　不服2022-6255(P2022-6255/J1)
審判請求日　令和4年4月25日(2022.4.25)

(73)特許権者　000001007
キヤノン株式会社
東京都大田区下丸子３丁目３０番２号
(74)代理人　110003281
弁理士法人大塚国際特許事務所
(72)発明者　角谷 直哉
東京都大田区下丸子３丁目３０番２号
キヤノン株式会社内
(72)発明者　山内 久幸
東京都大田区下丸子３丁目３０番２号
キヤノン株式会社内
合議体
審判長　須田 勝巳
審判官　中村 信也
審判官　篠原 功一

最終頁に続く

(54)【発明の名称】　情報処理装置及びその制御方法とプログラム

(57)【特許請求の範囲】
【請求項１】
電子証明書を使用して通信を行う情報処理装置であって、
電子証明書の発行要求を外部装置に送信する送信手段と、
前記発行要求に応答して前記外部装置から電子証明書を受信する受信手段と、
記憶部に記憶された電子証明書を、前記受信した電子証明書で更新する更新手段と、
前記受信手段によって受信した電子証明書の通信プロトコルを設定する設定手段と、
　前記設定手段によって設定された前記通信プロトコルを用いて、前記情報処理装置に接続された装置と暗号化通信を行う手段と、を有し、
前記送信手段と前記受信手段と前記更新手段は、前記記憶部に記憶された電子証明書の有効期限が切れるタイミングとは独立したタイミングで、前記発行要求を前記外部装置に送信して前記電子証明書を受信し、前記受信した電子証明書で前記記憶部に記憶された電子証明書を更新することを特徴とする情報処理装置。
【請求項２】
　前記通信プロトコルは、ＴＬＳ，ＩＰＳＥＣ，ＩＥＥＥ８０２．１Ｘの少なくともいずれかであることを特徴とする請求項１に記載の情報処理装置。
【請求項３】
　前記タイミングは、画面を介して設定される電子証明書を更新する時刻に基づくタイミングであることを特徴とする請求項１又は２に記載の情報処理装置。
【請求項４】

前記受信した電子証明書に含まれる電子署名を検証する検証手段を更に有し、
前記検証手段が前記受信した電子証明書に含まれる前記電子署名が前記外部装置により発行されたことを検証したことにより、前記更新手段は、前記記憶部に記憶された電子証明書を、前記受信した電子証明書で更新することを特徴とする請求項１乃至３のいずれか１項に記載の情報処理装置。
【請求項５】
前記外部装置からＣＡ証明書を取得する取得手段を更に有し、
前記検証手段は、前記取得手段が取得した前記ＣＡ証明書を用いて署名検証を行うことを特徴とする請求項４に記載の情報処理装置。
【請求項６】
前記送信手段は、前記情報処理装置にネットワークを介して接続された装置からの要求に基づいて前記電子証明書の発行要求を送信することを特徴とする請求項１乃至５のいずれか１項に記載の情報処理装置。
【請求項７】
前記外部装置との接続を設定する画面を表示させ、当該画面を介して設定された内容に応じて前記外部装置との接続設定を行う接続設定手段を更に有し、
前記送信手段は、前記接続設定手段により設定された前記外部装置に前記電子証明書の発行要求を送信することを特徴とする請求項１乃至６のいずれか１項に記載の情報処理装置。
【請求項８】
前記電子証明書の発行要求を行う画面を前記ネットワークを介して接続された装置に表示させる表示制御手段を更に有し、
前記送信手段は、前記画面を介して入力される指示に応じて起動されることを特徴とする請求項７に記載の情報処理装置。
【請求項９】
前記電子証明書の設定を前記情報処理装置に反映させる反映手段を、更に有することを特徴とする請求項１乃至８のいずれか１項に記載の情報処理装置。
【請求項１０】
電子証明書を使用して通信を行う情報処理装置を制御する制御方法であって、
前記電子証明書の発行要求を外部装置に送信する送信工程と、
前記発行要求に応答して前記外部装置から電子証明書を受信する受信工程と、
記憶部に記憶された電子証明書を、前記受信した電子証明書で更新する更新工程と、
前記受信工程で受信した電子証明書の通信プロトコルを設定する設定工程と、
前記設定工程で設定された通信プロトコルを用いて、前記情報処理装置に接続された装置と暗号化通信を行う工程と、を有し、
前記送信工程と前記受信工程と前記更新工程は、前記記憶部に記憶された電子証明書の有効期限が切れるタイミングとは独立したタイミングで、前記発行要求を前記外部装置に送信して前記電子証明書を受信し、前記記憶部に記憶された電子証明書を前記受信した電子証明書で更新することを特徴とする制御方法。
【請求項１１】
前記通信プロトコルは、ＴＬＳ，ＩＰＳＥＣ，ＩＥＥＥ８０２．１Ｘの少なくともいずれかであることを特徴とする請求項１０に記載の制御方法。
【請求項１２】
コンピュータを、請求項１乃至９のいずれか１項に記載の情報処理装置の全ての手段として機能させるためのプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、情報処理装置及びその制御方法とプログラムに関するものである。
【背景技術】

【０００２】
オフィス等のネットワークに接続するパーソナルコンピュータ（ＰＣ）や、個人が所持する携帯移動端末は、外部のサーバと通信する際、セキュアな通信と認証を行うために、公開鍵証明書を利用している。
【０００３】
また近年の複合機は、単純に画像の印刷や送信を行うだけではなく、複合機内に画像データを格納し、ＰＣに対してファイルサービスを提供する機能を備えている。そのため複合機も、ネットワーク上に存在するその他のサーバ機器と同様の情報処理装置としての役割を果たすようになってきている。これらの情報処理装置がネットワーク上で利用される中で、安全でかつ安心なオフィス環境を維持するためには、電子証明書を使って認証を行って通信することが求められる。一般的にはこの電子証明書を使った公開鍵基盤（ＰＫＩ：ｐｕｂｌｉｃ　ｋｅｙ　ｉｎｆｒａｓｔｒｕｃｔｕｒｅ）の技術により安全なネットワークの識別と認証が実現されている（非特許文献１参照）。
【０００４】
例えば、情報処理装置がクライアントになる場合、サーバから取得したサーバ公開鍵証明書と、そのサーバ公開鍵証明書を発行した認証局の認証局証明書を取得して、サーバの正当性を検証することができる。他にも、情報処理装置のクライアント公開鍵証明書をサーバに提供することによって、サーバがクライアントの正当性を検証することも可能となる。また情報処理装置がサーバになる場合、接続するクライアントに対して、情報処理装置のサーバ公開鍵証明書を配布することによって、クライアントが情報処理装置の正当性を検証できる。このように電子証明書は、情報処理装置同士がネットワーク通信の認証や識別を行う上で、従来から重要な技術として利用されている。例えば、このような通信で利用される通信プロトコルとして、ＳＳＬやＴＬＳ，ＩＥＥＥ８０２．１Ｘ、ＩＰＳＥＣなどがある。
【０００５】
この電子証明書は、情報処理装置の中に格納・保持しておく必要があるため、従来は、電子証明書は認証局が発行したものを、情報処理装置のユーザが手動で情報処理装置のストレージに格納していた。この格納方法としては、電子証明書を発行する認証局からダウンロードしたり、ＵＳＢメモリなどの外部ストレージからコピーしたり、Ｅ－ｍａｉｌなどで受信した電子証明書を所定のフォルダにコピーするなどの方法で行われている。
【０００６】
この電子証明書は、通信の用途によっては情報処理装置毎に別々の電子証明書を利用する場合がある。例えば、ＩＥＥＥ８０２．１Ｘなどでは、クライアントを認証をするために、情報処理装置毎に個別の電子証明書が格納されるのが一般的である。またこの電子証明書は有効期限があり、有効期限が切れると、その電子証明書を使用した通信が不可能になってしまう。そのため、有効期限が切れた場合や、切れる直前に機器内の電子証明書を更新する必要がある。また更に、電子証明書を利用する際、ＴＬＳやＩＥＥＥ８０２．１Ｘといったどの通信の用途で、どの電子証明書を使うかという設定を情報装置毎に手動で行う必要があった。
【先行技術文献】
【非特許文献】
【０００７】
【文献】ＲＦＣ３６４７：Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
【発明の概要】
【発明が解決しようとする課題】
【０００８】
しかしながら、電子証明書を扱う情報処理装置が大量に存在する場合、それらに対して電子証明書の追加や更新、設定を手動で行うことは、ユーザにとって非常に手間と時間がかかってしまう。

【０００９】
本発明の目的は、上記従来技術の課題を解決することにある。
【００１０】
本発明の目的は、情報処理装置における電子証明書の追加や更新を容易にする技術を提供することにある。
【課題を解決するための手段】
【００１１】
上記目的を達成するために本発明の一態様に係る情報処理装置は以下のような構成を備える。即ち、
電子証明書を使用して通信を行う情報処理装置であって、
電子証明書の発行要求を外部装置に送信する送信手段と、
前記発行要求に応答して前記外部装置から電子証明書を受信する受信手段と、
記憶部に記憶された電子証明書を、前記受信した電子証明書で更新する更新手段と、
前記受信手段によって受信した電子証明書の通信プロトコルを設定する設定手段と、
前記設定手段によって設定された前記通信プロトコルを用いて、前記情報処理装置に接続された装置と暗号化通信を行う手段と、を有し、
前記送信手段と前記受信手段と前記更新手段は、前記記憶部に記憶された電子証明書の有効期限が切れるタイミングとは独立したタイミングで、前記発行要求を前記外部装置に送信して前記電子証明書を受信し、前記受信した電子証明書で前記記憶部に記憶された電子証明書を更新することを特徴とする。
【発明の効果】
【００１２】
本発明によれば、情報処理装置における電子証明書の追加や更新を容易にできるという効果がある。
【図面の簡単な説明】
【００１３】
【図１】本発明の実施形態１に係るネットワーク構成を説明する図。
【図２】実施形態１に係る複合機のハードウェア構成を説明するブロック図。
【図３】実施形態１に係る複合機が有するソフトウェアモジュールを説明するブロック図。
【図４】実施形態１に係るシステムにおける、電子証明書の発行要求に関する初期設定、電子証明書の情報表示、発行要求と受信、再起動と、その電子証明書を反映するまでの全体処理の流れを説明するシーケンス図。
【図５】実施形態１に係る複合機による、図４のＳ４０２の鍵ペア・電子証明書のリストの取得及び表示データの作成処理を説明するフローチャート（Ａ）、実施形態１に係る複合機が、詳細情報を表示する要求をＰＣから受信したときの処理を説明するフローチャート（Ｂ）。
【図６】実施形態１に係る複合機による、図４のＳ４０７の認証局・登録局への接続設定の設定処理を説明するフローチャート。
【図７】実施形態１に係る複合機による、図４のＳ４１２からＳ４１６に示すＣＡ証明書取得・登録処理を説明するフローチャート。
【図８】実施形態１に係る複合機による、図４のＳ４１９からＳ４２４の証明書の発行要求・取得処理を説明するフローチャート。
【図９】実施形態１に係る複合機による、図４のＳ４２４からＳ４２７の複合機１００の再起動に関する処理を説明するフローチャート。
【図１０】実施形態１に係るＰＣで表示されるＲＵＩのＷｅｂページ画面の例を示す図。
【図１１】実施形態１に係るＰＣで表示されるＲＵＩのＷｅｂページ画面の例を示す図。
【図１２】実施形態１に係るＰＣで表示されるＲＵＩのＷｅｂページ画面の例を示す図。
【図１３】実施形態１に係るＰＣで表示されるＲＵＩのＷｅｂページ画面の例を示す図。
【図１４】実施形態１に係るＰＣで表示されるＲＵＩのＷｅｂページ画面の例を示す図。
【図１５】実施形態１に係るＰＣで表示されるＲＵＩのＷｅｂページ画面の例を示す図。

【図１６】実施形態１に係るＰＣで表示される電子証明書の詳細情報の一例を示す図。
【図１７】実施形態１に係る複合機の鍵ペア・証明書管理部が管理している鍵ペア・電子証明書の詳細情報のデータベースを概念図。
【図１８】実施形態２に係る複合機が有する電子証明書の更新予約設定画面の一例を示す図。
【図１９】実施形態２に係る複合機が、電子証明書の更新予約設定を基に電子証明書の自動更新機能を実行するときの処理を説明するフローチャート。
【発明を実施するための形態】
【００１４】
以下、添付図面を参照して本発明の実施形態を詳しく説明する。尚、以下の実施形態は特許請求の範囲に係る本発明を限定するものでなく、また本実施形態で説明されている特徴の組み合わせの全てが本発明の解決手段に必須のものとは限らない。尚、実施形態に係る電子証明書の利用及び管理する情報処理装置として複合機（デジタル複合機／ＭＦＰ／Ｍｕｌｔｉ　Ｆｕｎｃｔｉｏｎ　Ｐｅｒｉｐｈｅｒａｌ）を例に説明する。しかしながら適用範囲は複合機に限定はせず、電子証明書が利用可能な情報処理装置であればよく、適用範囲は複合機に限定はしない。
【００１５】
［実施形態１］
図１は、本発明の実施形態１に係るネットワーク構成を説明する図である。
【００１６】
印刷機能を有する複合機１００は、ネットワーク１１０を介して他の情報処理装置との間で、印刷データ、スキャンした画像データ、デバイスの管理情報等の送受信が可能である。また複合機１００は、ＴＬＳ，ＩＰＳＥＣ，ＩＥＥＥ８０２．１Ｘ等の暗号化通信を行う機能を有し、それらの暗号処理に使用する公開鍵ペアと電子証明書を保持している。ここで複合機１００は画像形成装置の一例であり、画像形成装置としてはこれに限らず、ファクシミリ装置、プリンタ、コピー機の単独の機能、或いはこれらの複合的な機能を併せ持つ装置であってもよい。ネットワーク１００には、複合機１０１も接続されており、この複合機１０１は、複合機１００と同等の機能をもっている。以下、複合機１００を主に説明するが、電子証明書のやりとりについては、複数台の複合機を対象とすることもできるものとする。
【００１７】
認証局・登録局１０２は、電子証明書を発行する認証局ＣＡ（Ｃｅｒｔｉｆｉｃａｔｅ Ａｕｔｈｏｒｉｔｙ）の機能と、電子証明書の発行要求の受付、登録処理を行う登録局ＲＡ（Ｒｅｇｉｓｔｒａｔｉｏｎ Ａｕｔｈｏｒｉｔｙ）の機能を有する。即ち、この認証局・登録局１０２は、ネットワーク１１０を介してＣＡ証明書の配布、電子証明書の発行・登録する機能を有するサーバ装置である。実施形態１では、この際のネットワーク１１０のプロトコルとして、ＳＣＥＰ（Ｓｉｍｐｌｅ Ｃｅｒｔｉｆｉｃａｔｅ Ｅｎｒｏｌｌｍｅｎｔ Ｐｒｏｔｏｃｏｌ）を利用するものとする。複合機１００などの情報処理装置は、このＳＣＥＰを利用し、ネットワーク１１０経由で電子証明書の発行要求、取得のための通信を認証局・登録局１０２に対して行う。実施形態１に係る複合機１００は、Ｗｅｂサーバ機能を有し、電子証明書の発行要求、取得のための処理を実行することが可能なＷｅｂページ型のＲＵＩ（Ｒｅｍｏｔｏ ＵＩ）機能をネットワーク１１０に公開している。
【００１８】
認証局・登録局１０２は、ネットワーク１１０を介して他の情報処理装置から電子証明書の発行要求を受信すると、その発行要求に基づく電子証明書の発行と登録処理を行い、発行した電子証明書を、その発行要求の応答として送信する。尚、実施形態１では、認証局と登録局の機能が同一のサーバ装置で実現されているが、認証局と登録局が別のサーバ装置で実現される構成であってもよく、特に限定はしない。また実施形態１では、電子証明書の発行要求やそれを取得するプロトコルとしてＳＣＥＰを利用しているが、同等の機能を持つプロトコルであればよく、本発明は特に限定はしない。例えば、ＣＭＰ（Ｃｅｒ

ｔｉｆｉｃａｔｅ Ｍａｎａｇｅｍｅｎｔ Ｐｒｏｔｏｃｏｌ）やＥＳＴ（Ｅｎｒｏｌｌｍｅｎｔ ｏｖｅｒ Ｓｅｃｕｒｅ Ｔｒａｎｓｐｏｒｔ）ｐｒｏｔｏｃｏｌ）などでもよい。

【００１９】

ＰＣ１０３はパーソナルコンピュータで、ＰＣ１０３にはＷｅｂブラウザ機能が搭載されており、ネットワーク１１０に接続された情報処理装置が公開しているＨＴＭＬ文書やＷｅｂサイトを閲覧、利用することが可能である。

【００２０】

次に、実施形態１に係る電子証明書の取得・更新の処理概要を説明する。

【００２１】

複合機１００の管理者は、ＰＣ１０３に搭載されているＷｅｂブラウザを利用して、複合機１００が公開している電子証明書の発行要求及びその取得のためにＷｅｂページに接続して、電子証明書の発行要求、取得のための処理の実行のための設定と指示を行う。複合機１００は、管理者が設定及び指示した内容に従って認証局・登録局１０２に対しＳＣＥＰによるＣＡ証明書の取得及び電子証明書の発行要求を行う。また複合機１００は、電子証明書の発行要求の応答に含まれる認証局・登録局１０２が発行した電子証明書を取得し、その取得した電子証明書の複合機１００での利用設定を行う。

【００２２】

次に実施形態１に係る複合機１００のハードウェア構成を説明する。

【００２３】

図２は、実施形態１に係る複合機１００のハードウェア構成を説明するブロック図である。

【００２４】

ＣＰＵ２０１は、複合機１００のソフトウェアプログラムを実行し、装置全体の制御を行う。ＲＯＭ２０２はリードオンリーメモリで、複合機１００のブートプログラムや固定パラメータ等を格納している。ＲＡＭ２０３はランダムアクセスメモリで、ＣＰＵ２０１が複合機１００を制御する際に、プログラムや一時的なデータの格納などに使用される。ＨＤＤ２０４はハードディスクドライブで、システムソフトウェア、アプリケーション、各種データを格納する。ＣＰＵ２０１はＲＯＭ２０２に記憶されているブートプログラムを実行し、ＨＤＤ２０４に格納されているプログラムをＲＡＭ２０３に展開し、その展開したプログラムを実行することにより、この複合機１００の動作を制御する。ネットワークＩ／Ｆ制御部２０５は、ネットワーク１１０とのデータの送受信を制御する。スキャナＩ／Ｆ制御部２０６は、スキャナ２１１による原稿の読み取り制御する。プリンタＩ／Ｆ制御部２０７は、プリンタ２１０による印刷処理などを制御する。パネル制御部２０８は、タッチパネル式の操作パネル２１２を制御し、各種情報の表示、使用者からの指示入力を制御する。バス２０９はＣＰＵ２０１、ＲＯＭ２０２、ＲＡＭ２０３、ＨＤＤ２０４、ネットワークＩ／Ｆ制御部２０５、スキャナＩ／Ｆ制御部２０６、プリンタＩ／Ｆ制御部２０７、パネル制御部２０８を相互に接続している。このバス２０９を介して、ＣＰＵ２０１からの制御信号や各装置間のデータ信号が送受信される。

【００２５】

図３は、実施形態１に係る複合機１００が有するソフトウェアモジュールを説明するブロック図である。尚、この図３に示すソフトウェアモジュールは、ＣＰＵ２０１がＲＡＭ２０３に展開したプログラムを実行することにより実現される。

【００２６】

ネットワークドライバ３０１は、ネットワーク１１０に接続されるネットワークＩ／Ｆ制御装置２０５を制御して、ネットワーク１１０を介して外部とデータの送受信を行なう。ネットワーク制御部３０２は、ＴＣＰ／ＩＰ等のネットワーク通信プロトコルにおけるトランスポート層以下の通信を制御して、データの送受信を行なう。通信制御部３０３は、複合機１００がサポートする複数の通信プロトコルの制御を行うためのモジュールである。実施形態１に係る電子証明書の取得及び更新処理では、通信制御部３０３がＨＴＴＰプロトコル通信のための要求、及び応答データの生成、解析処理とデータ送受信の制御を

行い、認証局・登録局１０２やＰＣ１０３との通信を実行する。また複合機１００がサポートするＴＬＳ，ＩＰＳＥＣ，ＩＥＥＥ８０２．１Ｘの暗号化通信も通信制御部３０３によって実行される。

【００２７】

Ｗｅｂページ制御部３０４は、電子証明書の発行要求とその取得のための処理を実行することが可能なＷｅｂページの表示のためのＨＴＭＬデータの生成及び通信制御を行うモジュールである。Ｗｅｂページ制御部３０４は、ネットワークドライバ３０１から通信制御部３０４を介して送られてきたＷｅｂページの表示要求や、電子証明書の発行要求及び取得の実行指示に対する処理を実行する。Ｗｅｂページ制御部３０４は、ＲＡＭ２０３やＨＤＤ２０４に保存されている既定のＷｅｂページのＨＴＭＬデータ、又は表示要求の内容に応じて生成したＨＴＭＬデータを、Ｗｅｂブラウザからのリクエストへの応答として送信する。

【００２８】

鍵ペア・証明書取得制御部３０５は、Ｗｅｂページ制御部３０４からの指示に基づく電子証明書の取得処理を実行するためのモジュールである。鍵ペア・証明書取得制御部３０５は、ＳＣＥＰによる通信制御、ＰＫＣＳ＃７，ＰＫＣＳ＃１０等のＳＣＥＰによる通信で必要な暗号化データの生成と解析処理及び、取得した電子証明書の保存、用途設定等の処理を行うモジュールである。暗号化処理部３０６は、データの暗号化及び復号処理、電子署名の生成・検証、ハッシュ値生成等の各種暗号処理を実行するためのモジュールである。暗号化処理部３０６は、実施形態１に係る電子証明書の取得及び更新処理で、ＳＣＥＰの要求・応答データの生成、解析処理において必要な各暗号処理を実行する。鍵ペア・証明書管理部３０７は、複合機１００が保持する公開鍵ペア、電子証明書を管理するモジュールである。鍵ペア・証明書管理部３０７は、公開鍵ペア、電子証明書のデータをＲＡＭ２０３やＨＤＤ２０４に各種設定値とともに保存する。また公開鍵ペア、電子証明書の詳細表示、生成、削除等の処理は、実施形態１では図示しないが、操作パネル２１２を介したユーザの指示によって実行することも可能である。操作パネル２１２及びパネル制御部２０８の制御は、ＵＩ制御部３０８によって実行される。尚、通信制御部３０３によって実行されるＴＬＳ，ＩＰＳＥＣ，ＩＥＥＥ８０２．１Ｘ等の暗号化通信処理においても、暗号化処理部３０６で暗号化処理が行われ、鍵ペア・証明書管理部３０７から、使用する公開鍵ペア・電子証明書データを取得する構成となっている。

【００２９】

印刷／読取処理部３０９は、プリンタ２１０による印刷や、スキャナ２１１による原稿の読み取り等の機能を実行するためのモジュールである。デバイス制御部３１０は、複合機１００の制御コマンドや制御データを生成して、複合機１００を統括的に制御するためのモジュールである。尚、実施形態１に係るデバイス制御部３０６は、複合機１００の電源の制御を行い、Ｗｅｂページ制御部３０４からの指示によって複合機１００の再起動処理を実行する。

【００３０】

図４は、実施形態１に係るシステムにおける、電子証明書の発行要求に関する初期設定、電子証明書の情報表示、発行要求と受信、再起動と、その電子証明書を反映するまでの全体処理の流れを説明するシーケンス図である。

【００３１】

このシーケンスは、鍵ペア及び選書証明書リストの表示指示がユーザにより入力されたことに応答して開始される。実施形態１では、一つの複合機１００に対する処理の例で説明するが、一回の開始指示に応じて、複数の複合機１００，１０１に対して実行させてもよい。例えば、ＰＣ１０３から、複合機１００及び１０１に対してリクエストを出し、それぞれの複合機で、後述する図５乃至図９のフローチャートで示す処理を実行させてもよい。この際、複合機１００，１０１から証明書を取得して表示して確認させる工程をスキップしてもよい。そして、有効期限が切れた証明書を自動的に複合機で検出し、その書誌情報（証明書ＩＤや有効期限）をＰＣ１０３に送信し、ＰＣ１０３では有効期限が切れそ

う、或いは切れた証明書の更新を、複数の複合機に自動的に実行させてもよい。これは、所謂、サイレントインストールと呼ばれるものである。

【００３２】

まずＳ４０１で複合機１００は、ＰＣ１０３からの接続を受け付けると、ＰＣ１０３から送信される複合機１００が保持している鍵ペア・電子証明書のリスト表示要求を受信する。実施形態１では、複合機１００の管理者は、ＰＣ１０３に搭載されているＷｅｂブラウザを利用して、複合機１００が公開している電子証明書の発行要求・取得のためのＷｅｂページ形式のＲＵＩ形式に接続し、指示などの操作を行うものとする。このＲＵＩはリモートユーザインタフェースの略であり、ＰＣ１０３のウェブブラウザを使用して、遠隔で複合機１００や１０１の操作画面データを要求してＰＣ１０３で表示できる技術である。このとき画面は、ＨＴＭＬやサーブレット等で実装できる。

【００３３】

次にＳ４０２で複合機１００は、複合機１００が保持している鍵ペア・電子証明書のリスト表示のためのデータの取得、及びそれを表示するためのＷｅｂページ画面の生成処理を実行する。

【００３４】

図５（Ａ）は、図４のＳ４０２の鍵ペア・電子証明書のリストの取得及び表示データの作成処理を説明するフローチャートである。尚、この処理は、ＣＰＵ２０１がＲＡＭ２０３に展開したプログラムを実行することにより達成される。

【００３５】

また図１７は、鍵ペア・証明書管理部３０７が管理している鍵ペア・電子証明書の詳細情報のデータベースを概念図であり、このデータベースは、複合機１００のＨＤＤ２０４に保存されている。

【００３６】

図５（Ａ）のフローチャートを説明する。この処理は、鍵ペア・電子証明書リストの取得要求を受信することにより開始される。まずＳ５０１でＣＰＵ２０１は、鍵ペア・電子証明書リストの取得要求を受信する。次にＳ５０２に進みＣＰＵ２０１は、鍵ペア・証明書管理部３０７が管理している、例えば図１７（Ａ）に示す鍵ペア・電子証明書の詳細情報を取得する。次にＳ５０３に進みＣＰＵ２０１は、Ｓ５０２で取得した鍵ペア・電子証明書の詳細情報を使用して、ＲＵＩとして提供するＷｅｂページ画面のＨＴＭＬデータを生成する。

【００３７】

図１０～図１５は、実施形態１に係るＰＣ１０３で表示されるＲＵＩのＷｅｂページ画面の例を示す図である。実施形態１に係る図５のＳ５０３では、図１０（Ａ）に示すＷｅｂページ画面のＨＴＭＬデータが生成されるものとし、これはＰＣ１０３のＷｅｂブラウザによって表示される。これにより、ＰＣ１０３で複合機１００が保持している鍵ペア・電子証明書リストが確認可能となる。

【００３８】

図１０（Ａ）のリストに表示される電子証明書の情報は、証明書の名前１０１１、用途１０１２、発行者１０１３、有効期限終了日１０１４、証明書の詳細１０１５を含んでいる。名前１０１１は、鍵ペア・電子証明書の発行の際に、複合機１００の管理者等の操作者が任意に付与した文字列である。用途１０１２は、その鍵ペア・電子証明書がＴＬＳ，ＩＰＳＥＣ，ＩＥＥＥ８０２．１Ｘの何れかの用途で使用される事を示す設定値である。発行者１０１３は、電子証明書を発行した認証局の識別名（ＤＮ：Ｄｉｓｔｉｎｇｕｉｓｈｅｄ　Ｎａｍｅ）である。有効期限終了日１０１４は、その電子証明書の有効期限が終了する日の情報である。詳細１０１５は、電子証明書の詳細情報を表示させるためのアイコンである。そしてＳ５０４に進みＣＰＵ２０１は、Ｓ５０３で生成したＨＴＭＬデータをＳ５０１への応答としてＰＣ１０３へ送信して、この処理を終了する。こうして図４のＳ４０３が実行される。

【００３９】

尚、図４のシーケンス図には図示しないが、複合機１００の管理者が、ＰＣ１０３に表示された図１０（Ａ）の詳細１０１５のアイコンをクリックすると、該当の電子証明書の詳細情報の表示要求がＰＣ１０３から複合機１００へ送信される。その表示要求を受信した複合機１００は、その電子証明書の詳細情報を取得し、その取得した情報に基づく証明書の詳細情報のＨＴＭＬデータを生成し、生成したデータを、応答としてＰＣ１０３へ送信する。

【００４０】

これにより例えば図１６に示すような、電子証明書の詳細情報がＰＣ１０３のＷｅｂブラウザにより表示される。図１６は、ＰＣ１０３で表示される電子証明書の詳細情報の一例を示す図である。

【００４１】

図５（Ｂ）は、実施形態１に係る複合機１００が、この詳細情報を表示する要求をＰＣ１０３から受信したときの処理を説明するフローチャートである。尚、この処理は、ＣＰＵ２０１がＲＡＭ２０３に展開したプログラムを実行することにより達成される。

【００４２】

まずＳ５１１でＣＰＵ２０１は、ＰＣ１０３から電子証明書の詳細情報の取得要求を受信する。次にＳ５１２に進みＣＰＵ２０１は、鍵ペア・証明書管理部３０７が管理している図１７（Ａ）に示す鍵ペア・電子証明書の詳細情報を取得する。次にＳ５１３に進みＣＰＵ２０１は、Ｓ５１２で取得した鍵ペア・電子証明書の詳細情報を使用してＷｅｂページ画面のＨＴＭＬデータを生成し、Ｓ５１４でそれをＰＣ１０３に送信する。

【００４３】

図１６は、実施形態１に係る電子証明書の詳細情報の表示画面の一例を示す図で、この画面はＰＣ１０３でＲＵＩとしてＷｅｂページ形式で表示される。

【００４４】

再び図４の説明に戻り、Ｓ４０３で複合機１００は、Ｓ４０２で生成した図１０（Ａ）で示すＷｅｂページ画面のＨＴＭＬデータを、応答としてＰＣ１０３へ送信する。

【００４５】

尚、上述の図４のＳ４０１～Ｓ４０３及び、図５のＳ５０１～Ｓ５０４、Ｓ５１１～Ｓ５１４で示す処理は、鍵ペア・電子証明書リストの表示要求を受信した複合機１００における電子証明書情報の表示処理に関する制御処理を示している。

【００４６】

そしてＳ４０４で複合機１００は、ＰＣ１０３から、ＳＣＥＰサーバの接続設定画面の表示要求を受信する。実施形態１では、複合機１００の管理者は認証局・登録局１０２との接続設定を行うために、図１０（Ａ）の接続設定１００２をクリックすることで、接続設定画面の表示要求を複合機１００に対して送信するものとする。

【００４７】

次にＳ４０５で複合機１００は、Ｓ４０４の応答として、図１０（Ｂ）に示す既定のＳＣＥＰサーバの接続設定画面のＨＴＭＬデータを応答としてＰＣ１０３に送信する。

【００４８】

図１０（Ｂ）に示す接続設定画面は、ＳＣＥＰサーバのホスト名及び接続先ポート番号を入力するサーバ名１０１６、ポート番号１０１７の入力フィールドと、入力した設定値の設定を指示する設定ボタン１０１８を含んでいる。

【００４９】

次にＳ４０６で複合機１００は、ＰＣ１０３から接続設定の設定指示要求を受信する。実施形態１における複合機１００の管理者は、ＰＣ１０３から図１０（Ｂ）のサーバ名１０１６、ポート番号１０１７へ入力を行い、設定ボタン１０１８をクリックすることで複合機１００に対して、この設定指示要求を送信するものとする。

【００５０】

次にＳ４０７で複合機１００は、接続設定の設定処理と設定結果を示すＷｅｂページ画面の生成処理を実行し、Ｓ４０８で、Ｓ４０７で生成した図１１（Ａ）に示すＷｅｂペー

ジ画面のＨＴＭＬデータを、応答としてＰＣ１０３へ送信する。
【００５１】
図６は、実施形態１に係る複合機１００による、図４のＳ４０７の認証局・登録局１０２への接続設定の設定処理を説明するフローチャートである。尚、この処理は、ＣＰＵ２０１がＲＡＭ２０３に展開したプログラムを実行することにより達成される。
【００５２】
まずＳ６０１でＣＰＵ２０１は、ＰＣ１０３から接続設定の設定要求を受信する。次にＳ６０２に進みＣＰＵ２０１は、その接続設定の設定要求に含まれるホスト名と、ポート番号の設定値を取得し、その取得した設定値をＲＡＭ２０３或いはＨＤＤ２０４に保存する。次にＳ６０３に進みＣＰＵ２０１は、例えば図１１（Ａ）のＷｅｂページ画面のＨＴＭＬデータを生成する。そしてＳ６０４に進みＣＰＵ２０１は、Ｓ６０３で生成したＨＴＭＬデータをＳ６０１の応答として送信して、この処理を終了する。こうしてＳ４０８に移行する。
【００５３】
これによりＰＣ１０３では、図１１（Ａ）に示すように、設定が反映されたことを示す文字列１１０１が表示される。
【００５４】
上述のＳ４０６～Ｓ４０８及びＳ６００～６０４で示す処理が、複合機１００における接続設定の処理に関する制御である。
【００５５】
次に図４のＳ４０９で複合機１００は、ＰＣ１０３のブラウザから送信されるＣＡ証明書の取得画面の表示要求を受信する。実施形態１では、複合機１００の管理者が、認証局・登録局１０２が発行したＣＡ証明書の取得を行うため、図１０（Ａ）のＣＡ証明書取得１００３をクリックすることでＣＡ証明書の取得画面の表示要求を複合機１００に送信するものとする。
【００５６】
これによりＳ４１０で複合機１００は、Ｓ４０９の応答として、図１１（Ｂ）に示す既定のＣＡ証明書の取得画面のＨＴＭＬデータを応答として送信する。
【００５７】
図１１（Ｂ）の接続設定画面は、ＣＡ証明書の取得を指示する実行ボタン１１０２を含んでいる。
【００５８】
次にＳ４１１で複合機１００は、図１１（Ｂ）の実行ボタン１１０２がクリックされてＰＣ１０３のブラウザから送信されるＣＡ証明書の取得要求を受信する。実施形態１では、複合機１００の管理者が図１１（Ｂ）の実行ボタン１１０２をクリックすることで、ＣＡ証明書の取得要求を複合機１００に送信するものとする。
【００５９】
次にＳ４１２で複合機１００は、ＣＡ証明書の取得要求データの生成処理を実行する。そしてＳ４１３に進み複合機１００は、Ｓ４１２で生成したＣＡ証明書の取得要求データを、Ｓ４０７で設定した情報に基づいて、ＳＣＥＰサーバである認証局・登録局１０２に対して送信する。そしてＳ４１４に進み複合機１００は、認証局・登録局１０２から送信されるＣＡ証明書の取得要求に対する応答を受信する。これによりＳ４１５に進み複合機１００は、受信したＣＡ証明書の取得応答を解析し、その応答に含まれるＣＡ証明書を取得し、その取得したＣＡ証明書を複合機１００が信頼するＣＡ証明書として登録する処理を行う。そしてＳ４１６に進み複合機１００は、Ｓ４１５で生成した図１２（Ａ）又は図１２（Ｂ）に示すＷｅｂページ画面のＨＴＭＬデータをＰＣ１０３へ送信する。図１２（Ａ）は、ＣＡ証明書の取得に成功して、ＣＡ証明書として登録したときに表示される画面例を示す。一方、図１２（Ｂ）は、ＣＡ証明書の取得に失敗したときに表示される画面例を示す。
【００６０】

図７は、実施形態１に係る複合機１００による、図４のＳ４１２からＳ４１６に示すＣＡ証明書取得・登録処理を説明するフローチャートである。尚、この処理は、ＣＰＵ２０１がＲＡＭ２０３に展開したプログラムを実行することにより達成される。

【００６１】

先ずＳ７０１でＣＰＵ２０１は、ＰＣ１０３からＣＡ証明書の取得要求を受信する。次にＳ７０２に進みＣＰＵ２０１は、Ｓ４０７で取得した認証局・登録局１０２への接続設定の情報を基にＣＡ証明書の取得要求のメッセージを生成する。以下は、実施形態１において生成される取得要求のメッセージの例である。実施形態１では、通信プロトコルとしてＳＣＥＰを利用しており、このプロトコルを利用するためのリクエストメッセージとなる。

【００６２】

xxxxxxx/yyyyy?operation=GetCAXyz&message=CAIdentifier

次にＳ７０３に進みＣＰＵ２０１は、図４のＳ４０７で取得した認証局・登録局１０２への接続設定に基づき、ＳＣＥＰサーバである認証局・登録局１０２に対してＴＣＰ／ＩＰプロトコルでの接続を行う。次にＳ７０４に進みＣＰＵ２０１は、Ｓ７０３における接続が成功したかを判断し、成功した場合はＳ７０５へ進み、失敗した場合はＳ７１４へ進む。

【００６３】

Ｓ７０５でＣＰＵ２０１は、Ｓ７０２で生成したＣＡ証明書の取得メッセージをＨＴＴＰプロトコルのＧＥＴまたはＰＯＳＴメソッドで認証局・登録局１０２に送信する。次にＳ７０６に進みＣＰＵ２０１は、Ｓ７０５における送信が成功したかを判断し、成功した場合はＳ７０７へ進み、失敗した場合はＳ７１４へ進む。Ｓ７０７でＣＰＵ２０１は、ＣＡ証明書の取得要求に対する、認証局・登録局１０２からの応答データを受信する。そしてＳ７０８に進みＣＰＵ２０１は、Ｓ７０７における応答データの受信が成功したかを判定し、成功した場合はＳ７０９へ進み、失敗した場合はＳ７１４へ進む。Ｓ７０９でＣＰＵ２０１は、Ｓ７０８で受信した応答データを解析し、その応答データに含まれるＣＡ証明書のデータを取得する。この応答データの解析処理とＣＡ証明書の取得処理は、暗号処理部３０６によって行われる。

【００６４】

尚、実施形態１における応答データは、X.509(RFC5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile)形式のバイナリデータとする。但し、例えばPKCS＃7(RFC5652: Cryptographic Message Syntax）形式のデータが応答として送信されてもよく、データ形式については限定しない。

【００６５】

次にＳ７１０に進みＣＰＵ２０１は、Ｓ７０９におけるＣＡ証明書の取得に成功したかを判定し、成功した場合はＳ７１１へ進み、失敗した場合はＳ７１４へ進む。Ｓ７１１でＣＰＵ２０１は、Ｓ７０９で取得したＣＡ証明書を、複合機１００が信頼するＣＡ証明書として登録する。このときＣＰＵ２０１は、取得したＣＡ証明書をＲＡＭ２０３に保持するとともに、鍵ペア・証明書管理部３０７によってＨＤＤ２０４の複合機１００が信頼するＣＡ証明書を格納する所定のディレクトリに保存する。そしてＳ７１２に進みＣＰＵ２０１は、Ｓ７１１におけるＣＡ証明書の登録処理が成功したか否かを判定し、成功したと判定した場合はＳ７１３へ進み、失敗した場合はＳ７１４へ進む。Ｓ７１３でＣＰＵ２０１は、ＣＡ証明書の取得成功の際に図１２（Ａ）の１２０１に表示するＣＡ証明書の拇印（ＳＨＡ１アルゴリズムによるハッシュ値）を生成する。この拇印の生成は、暗号処理部３０６によって実行される。そしてＳ７１５に進みＣＰＵ２０１は、Ｓ７０３からＳ７１４までの処理結果から図１２（Ａ）、図１２（Ａ）のＣＡ証明書の取得結果の表示データのＨＴＭＬデータを生成する。そしてＳ７１６に進みＣＰＵ２０１は、Ｓ７１５で生成したＨＴＭＬデータをＳ７０１の応答としてＰＣ１０３に送信して、この処理を終了する。そして図４のＳ４１７に移行する。実施形態１では、ＣＡ証明書の取得結果に応じて図１

２（Ａ）の文字列１２０１を表示する。また或いはＳ７１４でエラー処理を実行した場合は、図１２（Ｂ）の文字列１２０２を表示する。つぎに図４の説明に戻る。

【００６６】

Ｓ４１７で複合機１００は、ＰＣ１０３のブラウザから送信される証明書の発行要求画面の表示要求を受信する。実施形態１では、複合機１００の管理者が、図１０（Ａ）の証明書発行要求１００４をクリックすることで、認証局・登録局１０２に対する証明書の発行要求・取得を行うものとする。

【００６７】

次にＳ４１８で複合機１００は、Ｓ４１７の応答として、図１３（Ａ）に示す既定の証明書の発行要求画面のＨＴＭＬデータを応答としてＰＣ１０３に送信する。これによりＰＣ１０３は、図１３（Ａ）に示す画面を表示する表示制御を行う。

【００６８】

図１３（Ａ）の証明書の発行要求画面は、証明書の名前１３０１、生成する鍵ペアの鍵長を設定する鍵の長さ１３０２、発行先情報の入力フィールド１３０３、認証局・登録局１０２から送信される証明書の発行要求の応答に付与される署名を検証するか否かの設定署名検証１３０４、発行された証明書の用途設定を行うための鍵の用途１３０５、証明書発行要求に含めるパスワード１３０６、証明書の発行要求を実行する実行ボタン１３０７を含んでいる。用途１３０５はチェックボックスになっており、一つの証明書に対して複数の用途を設定できることを示している。

【００６９】

次にＳ４１９で複合機１００は、図１３（Ａ）の画面の実行ボタン１３０７がクリックされてＰＣ１０３のブラウザから送信される１３０１～１３０６までの各入力・設定情報を含む証明書の発行要求を受信する。実施形態１では、複合機１００の管理者が図１３（Ａ）の１３０１～１３０６までの各入力・設定を行い、実行ボタン１３０７をクリックすることで、ＰＣ１０３から証明書の発行要求を送信する。

【００７０】

次にＳ４２０で複合機１００は、証明書の発行要求データの生成処理を実行する。そしてＳ４２１で複合機１００は、Ｓ４２０で生成した証明書の発行要求データを、Ｓ４０７で設定した情報に基づきＳＣＥＰサーバである認証局・登録局１０２に対して送信する。そしてＳ４２２で複合機１００は、認証局・登録局１０２から送信される証明書の発行要求に対する応答を受信する。次にＳ４２３で複合機１００は、Ｓ４２２で受信した証明書の発行要求に対する応答の解析（設定に応じた署名検証の実行、応答に含まれる証明書の取得、取得した証明書を指定された用途に設定）処理を行う。そして、証明書の発行要求の結果を示すＷｅｂページ画面の生成処理を実行する。

【００７１】

ここで証明書の発行・取得が成功した場合は、Ｓ４２３の処理によって、電子証明書データの保存、用途設定が行われる。ここで用途設定とは、電子証明書を使う通信機能のことであり、実施形態１では、ＴＬＳ，ＩＰＳＥＣ，ＩＥＥＥ８０２．１Ｘといった暗号化通信が設定可能となる。また実施形態１に係る複合機１００は、複数の電子証明書を持つことが可能であり、且つその電子証明書毎に用途設定を行うものとする。例えば複合機１００がＷｅｂサーバとしてＴＬＳ通信を行うサーバサービスを提供する際に使う電子証明書と、複合機１００がＩＥＥＥ８０２．１Ｘを使ったクライアント通信を行うための電子証明書が異なる場合にそれぞれが設定可能となる。但し、１つの電子証明書を全ての通信の用途に自動的に適用してもよい。

【００７２】

そしてＳ４２４で複合機１００は、Ｓ４２３で生成した図１３（Ｂ）又は図１４（Ａ）に示すＷｅｂページ画面のＨＴＭＬデータをＰＣ１０３へ送信する。なお、証明書の発行要求の結果に応じて図１３（Ｂ）の１３０８、図１４（Ａ）の１４０１に示すように設定結果の文字列が表示される。図１３（Ｂ）は、証明書の発行及び取得に成功した場合の画面例を示し、図１４（Ａ）は、証明書の発行及び取得に失敗した場合の画面例を示す。

【００７３】
こうして証明書の発行・取得が成功した場合には、Ｓ４２３の処理によって、電子証明書データの保存、用途設定が行われる。実施形態１に係る通信制御部３０３は、ＴＬＳ，ＩＰＳＥＣ，ＩＥＥＥ８０２．１Ｘの暗号化通信が使用する電子証明書のデータを複合機１００の起動時に取得するため、用途変更された場合は、複合機１００の再起動が必要になる。
【００７４】
図８は、実施形態１に係る複合機１００による、図４のＳ４１９からＳ４２４の証明書の発行要求・取得処理を説明するフローチャートである。尚、この処理は、ＣＰＵ２０１がＲＡＭ２０３に展開したプログラムを実行することにより達成される。
【００７５】
まずＳ８０１でＣＰＵ２０１は、ＰＣ１０３から証明書の発行要求を受信する。次にＳ８０２に進みＣＰＵ２０１は、Ｓ８０１で受信した証明書の発行要求に含まれる証明書の名前１３０１、鍵の長さ１３０２、発行先情報の入力１３０３、署名検証１３０４、鍵の用途１３０５の情報を取得する。次にＳ８０３に進みＣＰＵ２０１は、図４のＳ４１２からＳ４１５で取得したＣＡ証明書を取得する。そしてＳ８０４に進みＣＰＵ２０１は、Ｓ８０２で取得した名前１３０１、鍵の長さ１３０２の情報に基づく鍵ペアの生成処理と、発行先情報の入力１３０３、パスワード１３０６の情報に基づくPKSC＃10（RFC2986: PKCS ＃10: Certification Request Syntax Specification）形式の証明書署名要求（CSR:Certificate Signing Request）データを暗号処理部３０６によって生成する。次にＳ８０５に進みＣＰＵ２０１は、Ｓ８０４における鍵ペア・証明書の署名要求の生成が成功したかを判定し、成功したと判定した場合はＳ８０６へ進み、失敗した場合はＳ８２３へ進む。Ｓ８０６でＣＰＵ２０１は、証明書の発行要求データを生成する。このＳ８０６で生成される取得要求データは、図４のＳ４０７で取得した認証局・登録局１０２への接続設定に基づき、ＳＣＥＰで定義されているＰＫＣＳ＃７形式のデータとなる。
【００７６】
次にＳ８０８に進みＣＰＵ２０１は、図４のＳ４０７で取得した認証局・登録局１０２への接続設定に基づきＳＣＥＰサーバである認証局・登録局１０２にＴＣＰ／ＩＰプロトコルでの接続を行う。次にＳ８０９に進みＣＰＵ２０１は、Ｓ８０８における接続が成功したかを判定し、成功した場合はＳ８１０へ進み、失敗した場合はＳ８２３へ進む。Ｓ８１０でＣＰＵ２０１は、Ｓ８０６で生成した証明書の発行要求データをＨＴＴＰプロトコルのＧＥＴ又はＰＯＳＴメソッドで送信する。そしてＳ８１１でＣＰＵ２０１は、Ｓ８１０における送信が成功したかを判定し、成功した場合はＳ８１２へ進み、失敗した場合はＳ８２３へ進む。Ｓ８１２でＣＰＵ２０１は、認証局・登録局１０２から、証明書の発行要求に対する応答データを受信する。ＳＣＥＰで定義されている応答データは、ＰＫＣＳ＃７形式のデータが応答として送信される。
【００７７】
次にＳ８１３に進みＣＰＵ２０１は、Ｓ８１２における応答データの受信に成功したかを判定し、成功した場合はＳ８１４へ進み、失敗した場合はＳ８２３へ進む。Ｓ８１４でＣＰＵ２０１は、Ｓ８０２で取得した署名検証１３０４の設定に基づき、署名検証する設定かどうか判定し、そうであればＳ８１５へ進み、署名検証しない設定の場合はＳ８１７へ進む。Ｓ８１５でＣＰＵ２０１は、Ｓ８１２で受信したデータに付与されている署名データを、Ｓ８０３において取得したＣＡ証明書に含まれる公開鍵を用いて検証する。そしてＳ８１６に進みＣＰＵ２０１は、Ｓ８１５での署名検証の結果が成功したかどうか判定し、成功した場合はＳ８１７へ進み、失敗した場合はＳ８２３へ進む。
【００７８】
Ｓ８１７でＣＰＵ２０１は、Ｓ８１２で受信したデータを解析し、その応答データに含まれる証明書のデータを取得する。このとき暗号処理部３０６によって応答データの解析と証明書の取得処理を行う。次にＳ８１８に進みＣＰＵ２０１は、Ｓ８１７における証明書の取得に成功したかを判定し、成功した場合はＳ８１９へ進み、失敗した場合はＳ８２

３へ進む。Ｓ８１９でＣＰＵ２０１は、Ｓ８１８で取得した証明書を、Ｓ８０４で生成した鍵ペアに対応する電子証明書として登録する。このときＣＰＵ２０１は、Ｓ８０４で生成した公開鍵ペア、及び取得した電子証明書を、鍵ペア・証明書管理部３０７によってＨＤＤ２０４の鍵ペア・電子証明書を格納する所定のディレクトリに保存する。このとき鍵ペア・証明書管理部３０７は、図１７（Ｂ）に示すように鍵ペア・証明書の詳細情報のリストにＳ８０４で生成した公開鍵ペア及び取得した電子証明書の情報を追加する。図１７（Ｂ）では、新たに鍵ペア・証明書Ｘｙｚ４が追加されている。

【００７９】

次にＳ８２０に進みＣＰＵ２０１は、Ｓ８１９におけるＣＡ証明書の登録処理が成功したかを判定し、成功した場合はＳ８２１へ進み、失敗した場合はＳ８２３へ進む。Ｓ８２１でＣＰＵ２０１は、Ｓ８０２で取得した鍵の用途１３０５の情報に基づき、証明書の用途設定を行う。このとき鍵ペア・証明書管理部３０７は、例えば図１７（Ｃ）に示したように鍵ペア・証明書の詳細情報のリストにある、用途の情報を更新する。図１７（Ｃ）では、ＴＬＳで使用する鍵ペア・証明書が、Ｘｙｚ１からＸｙｚ４に変更されている。

【００８０】

次にＳ８２４に進みＣＰＵ２０１は、Ｓ８０１からＳ８２３までの処理結果に応じた図１３（Ｂ）に示した証明書の発行要求結果のＨＴＭＬデータを生成し、Ｓ８２５においてＳ８２４で生成したＨＴＭＬデータをＳ８０１の証明書の発行要求に対する応答としてＰＣ１０３に送信して、この処理を終了する。そして図４のＳ４２５に移行する。

【００８１】

上述のＳ４１９～Ｓ４２４及びＳ８０１～Ｓ８２５の処理が、複合機１００における電子証明書の発行要求と受信処理、通信用途の設定に関する制御となる。この実施形態１では、これらの発行要求と受信処理、通信用途の設定までの処理を総称して「電子証明書の自動更新機能」と称する。

【００８２】

この電子証明書の自動更新機能によって、複合機１００はネットワークを介して電子証明書の発行要求や受信処理を自動で行い、更に、受信した電子証明書の用途設定も行うことができ、ユーザの作業の手間を削減することが可能となる。図４の説明に戻る。

【００８３】

Ｓ４２５で複合機１００は、複合機１００の再起動のリクエストを受信する。実施形態１では、複合機１００の管理者が、複合機１００の再起動を行うため、図１３（Ｂ）の再起動ボタン１３０９をクリックするものとする。

【００８４】

次にＳ４２６に進み複合機１００は、Ｓ４２５の応答として、図１４（Ｂ）に示す既定の再起動実行画面のＨＴＭＬデータを応答として送信する。次にＳ４２７に進み複合機１００は、複合機１００の再起動処理を実行する。

【００８５】

実施形態１に係る複合機１００は、受信した電子証明書に対してＩＥＥＥ８０２．１Ｘなどの通信の用途を設定した際、再起動を行わなければ反映できないことを想定している。これは例えばＩＥＥＥ８０２．１Ｘなどの電子証明書は、複合機１００の起動時にＲＡＭ２０３に展開されて使用され続けるため、ＨＤＤ２０４に保存される受信した電子証明書に置き換わらない場合があるためである。但し、もしも複合機１００が再起動を必要せずに通信の用途で使われる電子証明書を切り替えることが可能であれば、再起動は不要でもよい。例えば、ＴＬＳの用途に設定した場合は、再起動を不要にすることとしてもよい。例えば、予め、複数の用途に対してそれぞれ再起動の要否を設定しておき、複合機１００は、その再起動要否情報に応じて再起動の有無を自動的に決定してもよい。

【００８６】

図９は、実施形態１に係る複合機１００による、図４のＳ４２４からＳ４２７の複合機１００の再起動に関する処理を説明するフローチャートである。尚、この処理は、ＣＰＵ２０１がＲＡＭ２０３に展開したプログラムを実行することにより達成される。

【００８７】
まずＳ９０１でＣＰＵ２０１は、ＰＣ１０３から複合機１００の再起動要求を受信する。次にＳ９０２に進みＣＰＵ２０１は、図１４（Ｂ）に示した既定の複合機１００の再起動要求のＨＴＭＬデータを、Ｓ５０１への応答としてＰＣ１０３に送信する。次にＳ９０３に進みＣＰＵ２０１は、デバイス制御部３１０へ再起動処理の開始を指示して、この処理を終了する。
【００８８】
以上の一連の動作によって、再起動した後の複合機１００は、認証局・登録局１０２から取得した電子証明書が利用される。
【００８９】
図１５は、証明書の発行・取得が成功した場合に、再びＳ４０１の処理によって鍵ペア・電子証明書リストの表示を行った場合の画面例を示す図で、認証局・登録局１０２が発行した証明書（Ｘｙｚ４）の情報１５０１が追加されている。
【００９０】
以上が実施形態１に係る電子証明書の発行要求に関する初期設定、電子証明書の情報表示、発行要求と受信、再起動と電子証明書の反映までの全体処理の流れである。
【００９１】
尚、図４に示す処理の流れとしては、接続設定から電子証明書の要求や反映まで一連の動作としていたが、接続設定などの初期設定に関する処理は、複合機１００に対して１度だけ行う場合でもよい。例えば、Ｓ４０１～Ｓ４０３の電子証明書情報の表示処理、Ｓ４０６～Ｓ４０８の接続設定の処理、Ｓ４０９～Ｓ４１８のＣＡ証明書の取得処理に関しては、初回のみ設定を行う。そして２回目以降の電子証明書の発行要求時は、その設定をそのまま引き継いで利用する運用でもよい。言い換えると、２回目以降の電子証明書の更新時は、Ｓ４１９～Ｓ４２４の電子証明書の発行要求と受信処理、通信用途の設定に関する処理と、Ｓ４２５～Ｓ４２７の再起動と反映に関する処理のみが実行される運用でもよい。
【００９２】
また実施形態１では、複合機１００は自身が持つＷｅｂページ型のＲＵＩを介してＰＣ１０３からそれぞれの処理の指示を受け付け、その指示によって制御を行っていた。Ｗｅｂページ型のＲＵＩではなく、複合機１００が持つオペレーションパネル２１０を利用したＬＵＩ（ローカルＵＩ）からでもよく、特に管理者から複合機１００に対して指示を受け付けるインターフェイスを限定はしない。
【００９３】
またＷｅｂページ型のＲＵＩに対して、管理者が直接手動で操作するのではなく、予めＷｅｂページの入力領域や操作指示をテンプレート化、ルール化し、ＰＣ又は別の管理サーバから自動で入力して指示することで、複合機１００に対して要求を出してもよい。この場合、例えばウェブスクレイピング（ＷｅｂＳｃｒａｐｉｎｇ）技術などを利用してもよい。
【００９４】
また実施形態１では、ＣＡ証明書の取得・登録を行うための操作を複合機１００の管理者が行う構成としているが、ＣＡ証明書の取得は、証明書の発行要求の際に自動で取得する構成としても良い。
【００９５】
また実施形態１では、認証局・登録局１０２からの証明書の発行要求の応答に含まれる署名検証の実行を選択する設定を設けているが、その設定を設けずに、必ず署名検証する、又は署名検証は行わないというようにしても良い。
【００９６】
また実施形態１では、証明書の発行要求のデータにパスワードを入力し、証明書の署名要求にパスワードを含める構成としているが、パスワードを必要としない構成としてもよい。
【００９７】

以上説明したように実施形態１によれば、ＲＵＩからの指示をもとに証明書の自動更新プロトコルを使用して認証局・登録局である外部装置に対して証明書の追加・更新要求を発行できる。そして、その要求に対応する応答により、証明書を受信して複合機に登録するとともに、その証明書の用途設定を行うことができる。

【００９８】

［実施形態２］

次に、本発明の実施形態２について説明する。前述の実施形態１では、複合機１００の持つＷｅｂサーバ機能を使ってＷｅｂページ型のＲＵＩを複合機１００の利用者に提供していた。そして利用者は、そのＲＵＩを介して複合機１００に指示をすることによって電子証明書の追加や更新、用途の設定を行っていた。この電子証明書は有効期限があるため、有効期限が過ぎた電子証明書は無効となり、無効となった電子証明書では正しい通信の認証が行われないため、ネットワーク通信に支障を及ぼすことになる。そのため、機器が持つ電子証明書の有効期限が近づいたり、切れていたりする場合、電子証明書を更新する必要がある。しかしながら、電子証明書を利用する機器が複数台ある場合、機器の管理者がそれぞれの電子証明書の有効期限を把握した上で電子証明書を更新するのは困難である。

【００９９】

そこで実施形態２では、実施形態１のような電子証明書の自動更新機能を有する情報処理装置において、利用者からの指示ではなく、所定の日時になると電子証明書の更新機能を自動的に起動する制御について説明する。尚、本実施形態２において、ネットワーク構成、情報処理装置である複合機１００のハードウェア構成、ソフトウェア構成、鍵ペア・電子証明書のリスト表示処理、接続設定の設定処理などは、前述の実施形態１と同じであるため、その説明を省略する。

【０１００】

図１８は、実施形態２に係る複合機１００が有する電子証明書の更新予約設定画面の一例を示す図であり、他の画面と同様にＷｅｂページ型のＲＵＩによって表示される。この電子証明書の更新予約の設定画面を介して電子証明書の更新日を設定できる。実施形態２では、更新日や更新間隔の指定として、更新日１８０１、有効期限１８０２、周期１８０３の３つの設定を可能とする。更新日１８０１は、更新する年月日時刻を指定可能であり、複合機１００に保持されている現在日時が、この更新日１８０１の日時となったときに、電子証明書の自動更新機能を実行する。有効期限１８０２は、利用している電子証明書の有効期限に到達するまでの日数を指定する。複合機１００に保持されている現在日時が、有効期限から指定された日数よりも短くなった場合に電子証明書の自動更新機能を実行する。周期１８０３は、この周期で電子証明書の自動更新機能を実行する。実施形態２では、この周期は、日数、毎月所定の日付、毎年所定の月日で設定できる。また実施形態２では、これらの電子証明書の更新日や更新周期の設定を「電子証明書の更新予約設定」と称する。これらの電子証明書の更新予約設定が更新されると、ＣＰＵ２０１が、それをＨＤＤ２０４に保存する。

【０１０１】

図１８は、有効期限１８０２で、有効期限より１４日前になると電子証明書の自動更新機能を実行することを設定した画面の例を示す。実施形態２では、上述の電子証明書の更新予約設定の種別で電子証明書の自動更新機能の予約を行っているが、別の日時やタイミングの指定方法でもよく、特に限定はしない。

【０１０２】

図１９は、実施形態２に係る複合機１００が、電子証明書の更新予約設定を基に電子証明書の自動更新機能を実行するときの処理を説明するフローチャートである。図１９は、複合機１００に対して設定している。最初に複数の複合機を指定（複合機ごとに異なる時間設定も可）することで、複数の複合機に対して図１９で入力できる指示を実行することもできる。その場合、図１９の処理は、複数の複合機において並列で実行される。尚、この処理は、ＣＰＵ２０１がＲＡＭ２０３に展開したプログラムを実行することにより達成される。

【０１０３】
先ずＳ１９０１でＣＰＵ２０１は、ＨＤＤ２０４から電子証明書の更新予約設定を取得する。次にＳ１９０２に進みＣＰＵ２０１は、現在利用されている電子証明書の情報を取得する。この情報は図１７で保持している情報などである。次にＳ１９０３に進みＣＰＵ２０１は、複合機１００が管理している現在の日時を取得する。そしてＳ１９０４に進みＣＰＵ２０１は、電子証明書の更新予約設定と電子証明書の情報とを比較し、現在利用している電子証明書の更新が必要かどうか判定する。ここで電子証明書の更新が必要ではないと判定した場合はＳ１９０１に戻る。一方、電子証明書の更新が必要であると判定した場合はＳ１９０５に進み、図８の「証明書発行要求処理」の制御に移行する。そして図８の処理が完了するとＳ１９０６に移行する。

【０１０４】
上述の処理によって、ユーザからの手動の指示を行わなくとも、指定した更新日や更新周期によって、自動的に電子証明書の更新が可能となる。これによって機器の管理者がそれぞれの電子証明書の有効期限を把握しなくても、所望なタイミングで、且つユーザの手間を削減しながら電子証明書を更新できる。

【０１０５】
次にＳ１９０６でＣＰＵ２０１は、電子証明書を更新した際、複合機１００の再起動が必要か否かを判断する。ここでＣＰＵ２０１が、再起動が必要と判定した場合はＳ１９０７に進み、図９に示す「再起動・設定反映処理」を実行する。一方ＣＰＵ２０１が、再起動は不要と判断した場合は、この処理を終了する。これは例えば複合機１００が利用する電子証明書を切り替えた際、ＴＬＳでは再起動が不要であるが、ＩＥＥＥ８０２．１Ｘでは再起動が必須となるネットワーク構成などの場合において、必要な場合のみ再起動を行うための制御である。

【０１０６】
以上説明したように実施形態２によれば、電子証明書の更新のタイミングを予約しておくことにより、ユーザが指示しなくても、複合機が自動的に電子証明書の発行要求を送信して電子証明書の更新及び登録を行うことができる。これにより、ユーザが電子証明書の有効期限を把握しない場合でも、電子証明書の有効期限が過ぎてしまうことにより、電子証明書が無効となって、ネットワーク通信に支障をきたすという事態の発生を防止できる。

【０１０７】
（その他の実施形態）
本発明は、上述の実施形態の１以上の機能を実現するプログラムを、ネットワーク又は記憶媒体を介してシステム又は装置に供給し、そのシステム又は装置のコンピュータにおける１つ以上のプロセッサーがプログラムを読出し実行する処理でも実現可能である。また、１以上の機能を実現する回路（例えば、ＡＳＩＣ）によっても実現可能である。

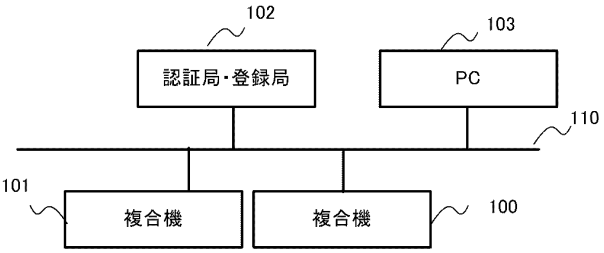
【０１０８】
本発明は上記実施形態に制限されるものではなく、本発明の精神及び範囲から離脱することなく、様々な変更及び変形が可能である。従って、本発明の範囲を公にするために、以下の請求項を添付する。

【符号の説明】

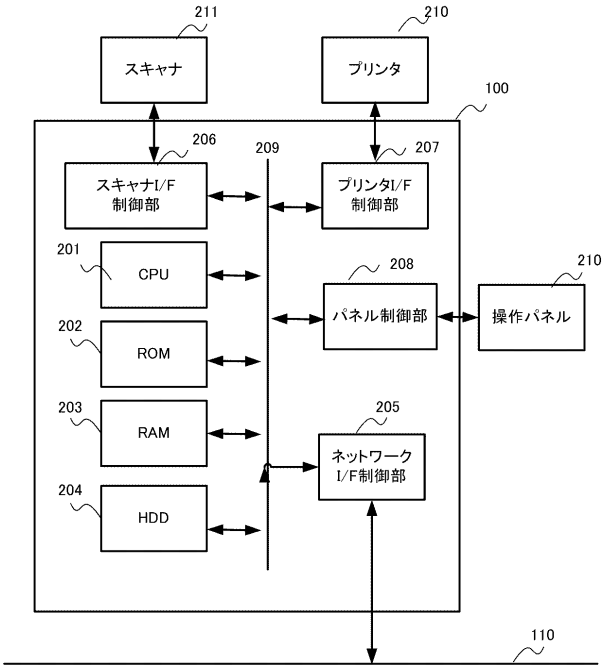
【０１０９】
１００，１０１…複合機、１０２…認証局・登録局、１０３…ＰＣ，３０４…Ｗｅｂページ制御部、３０５…鍵ペア・証明書取得制御部、３０６…暗号化処理部

【図面】

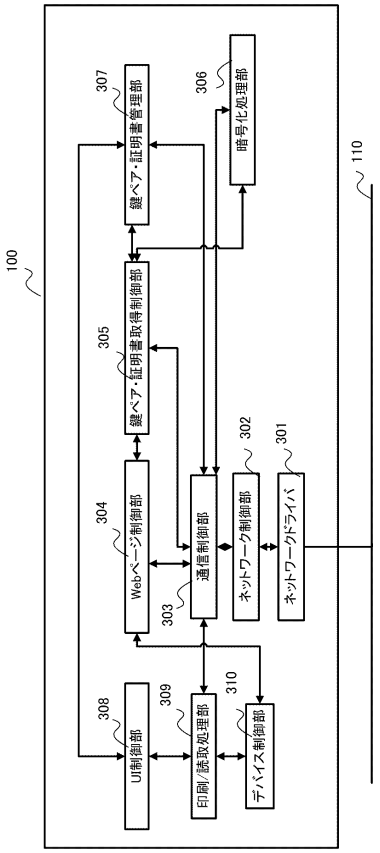
【図１】


102
103
認証局・登録局
PC
110
101
複合機
複合機
100

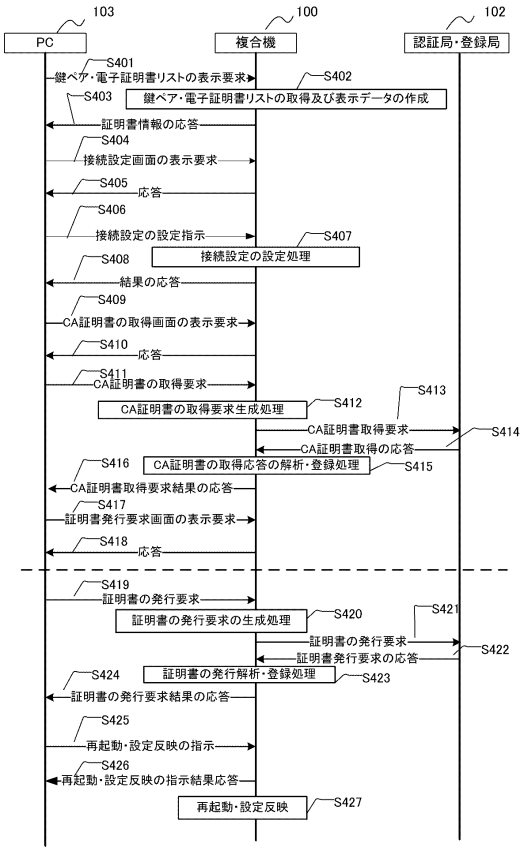
【図２】


211
210
スキャナ
プリンタ
100
206
209
207
スキャナI/F
制御部
プリンタI/F
制御部
201
CPU
208
210
パネル制御部
操作パネル
202
ROM
203
RAM
205
ネットワーク
I/F制御部
204
HDD
110

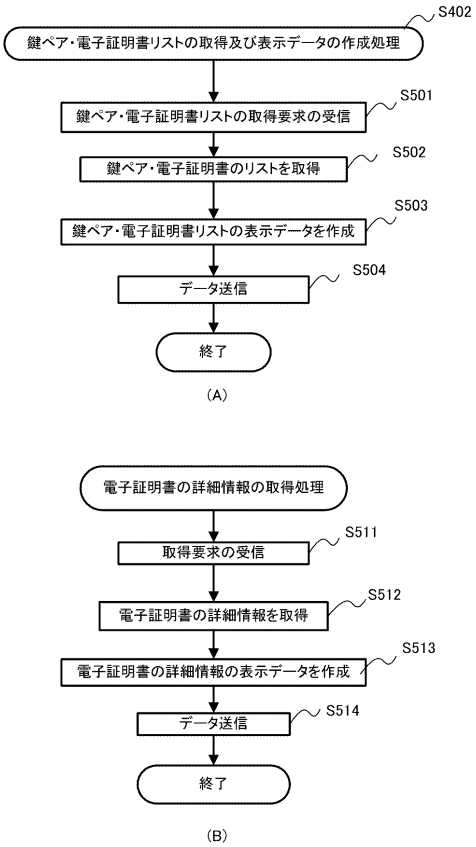
【図３】


100
307
鍵ペア・証明書管理部
306
暗号化処理部
110
305
鍵ペア・証明書取得制御部
304
Webページ制御部
302
301
通信制御部
ネットワーク制御部
ネットワークドライバ
303
308
309
310
UI制御部
印刷/読取処理部
デバイス制御部

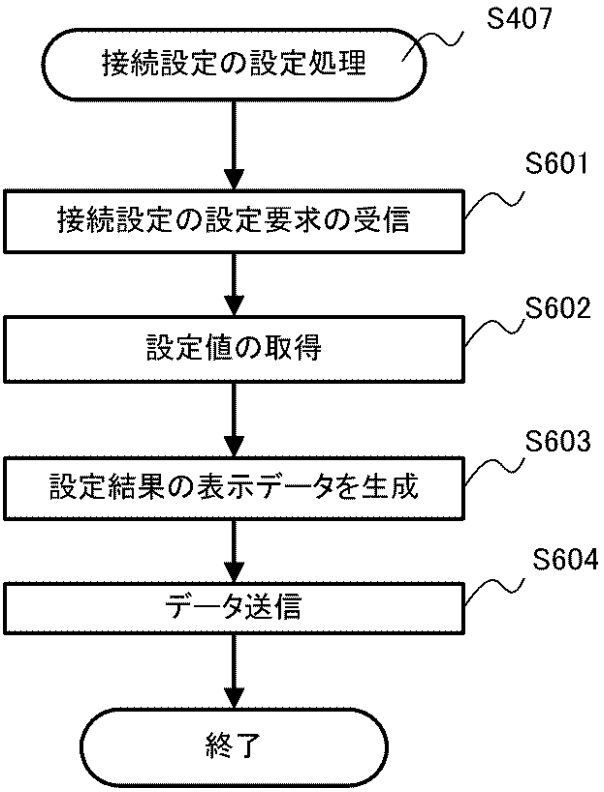
【図４】


103
100
102
PC
複合機
認証局・登録局
S401
鍵ペア・電子証明書リストの表示要求
S402
S403
鍵ペア・電子証明書リストの取得及び表示データの作成
証明書情報の応答
S404
接続設定画面の表示要求
S405
応答
S406
接続設定の設定指示
S407
S408
接続設定の設定処理
結果の応答
S409
CA証明書の取得画面の表示要求
S410
応答
S411
CA証明書の取得要求
S412
S413
CA証明書の取得要求生成処理
CA証明書取得要求
S414
CA証明書取得の応答
S416
CA証明書の取得応答の解析・登録処理
S415
CA証明書取得要求結果の応答
S417
証明書発行要求画面の表示要求
S418
応答
S419
証明書の発行要求
S420
S421
証明書の発行要求の生成処理
証明書の発行要求
S422
証明書発行要求の応答
S424
証明書の発行解析・登録処理
S423
証明書の発行要求結果の応答
S425
再起動・設定反映の指示
S426
再起動・設定反映の指示結果応答
再起動・設定反映
S427

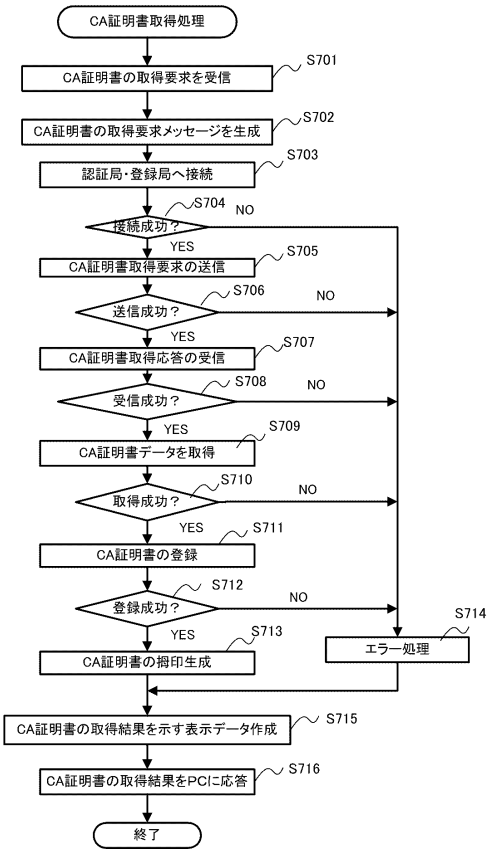
【図５】


S402
鍵ペア・電子証明書リストの取得及び表示データの作成処理
S501
鍵ペア・電子証明書リストの取得要求の受信
S502
鍵ペア・電子証明書のリストを取得
S503
鍵ペア・電子証明書リストの表示データを作成
S504
データ送信
終了
(A)
電子証明書の詳細情報の取得処理
S511
取得要求の受信
S512
電子証明書の詳細情報を取得
S513
電子証明書の詳細情報の表示データを作成
S514
データ送信
終了
(B)

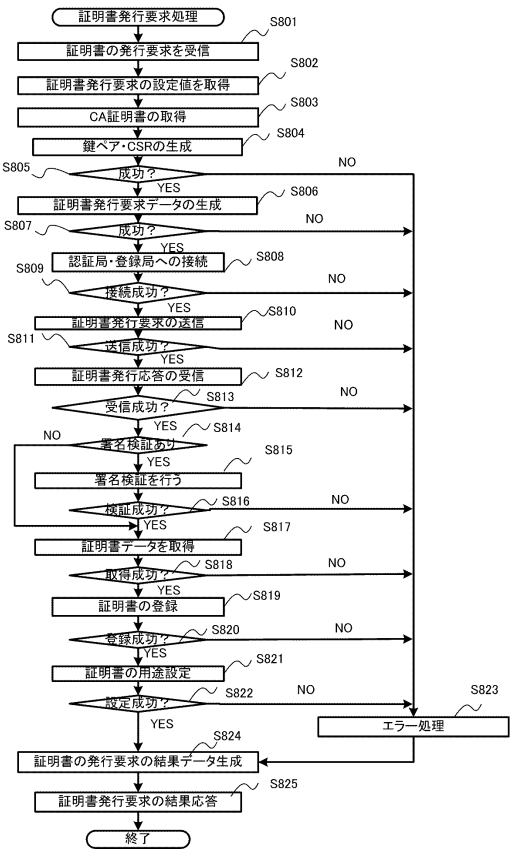
【図６】


S407
接続設定の設定処理
S601
接続設定の設定要求の受信
S602
設定値の取得
S603
設定結果の表示データを生成
S604
データ送信
終了

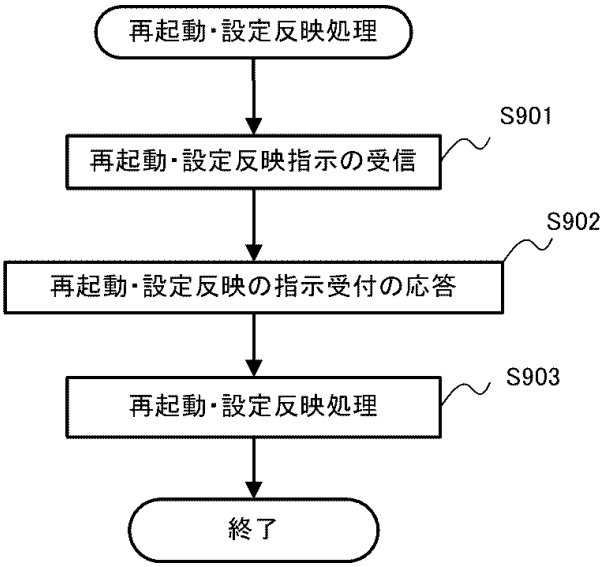
【図７】


CA証明書取得処理
S701
CA証明書の取得要求を受信
S702
CA証明書の取得要求メッセージを生成
S703
認証局・登録局へ接続
S704
接続成功？
NO
YES
S705
CA証明書取得要求の送信
S706
送信成功？
NO
YES
S707
CA証明書取得応答の受信
S708
受信成功？
NO
YES
S709
CA証明書データを取得
S710
取得成功？
NO
YES
S711
CA証明書の登録
S712
登録成功？
NO
YES
S713
CA証明書の捺印生成
S714
エラー処理
S715
CA証明書の取得結果を示す表示データ作成
S716
CA証明書の取得結果をPCに応答
終了

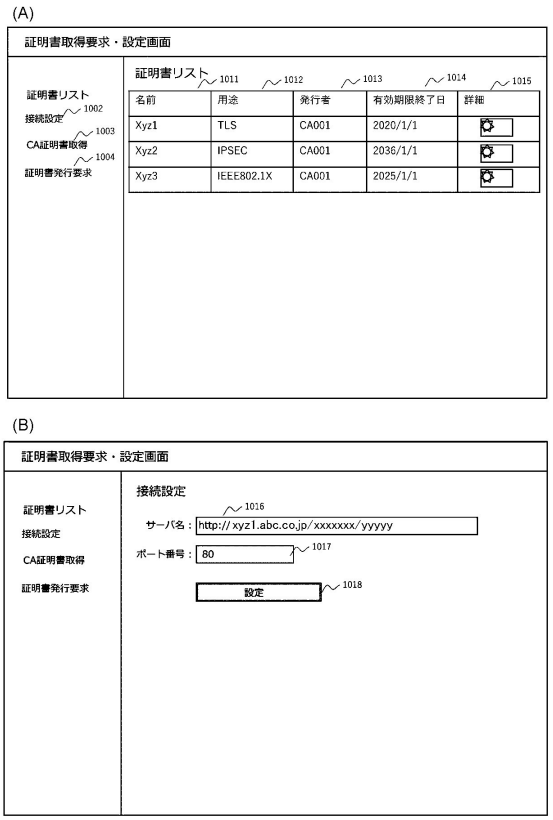
【図８】


証明書発行要求処理
S801
証明書の発行要求を受信
S802
証明書発行要求の設定値を取得
S803
CA証明書の取得
S804
鍵ペア・CSRの生成
S805
成功？
NO
YES
S806
証明書発行要求データの生成
S807
成功？
NO
YES
S808
認証局・登録局への接続
S809
接続成功？
NO
YES
S810
証明書発行要求の送信
S811
送信成功？
NO
YES
S812
証明書発行応答の受信
S813
受信成功？
NO
YES
S814
署名検証あり
NO
YES
S815
署名検証を行う
S816
検証成功？
NO
YES
S817
証明書データを取得
S818
取得成功？
NO
YES
S819
証明書の登録
S820
登録成功？
NO
YES
S821
証明書の用途設定
S822
設定成功？
NO
YES
S823
エラー処理
S824
証明書の発行要求の結果データ生成
S825
証明書発行要求の結果応答
終了

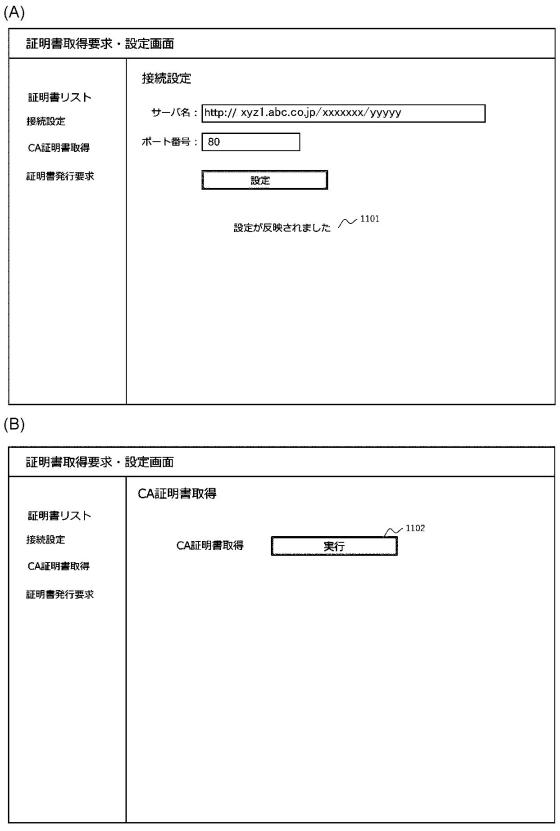
【図９】



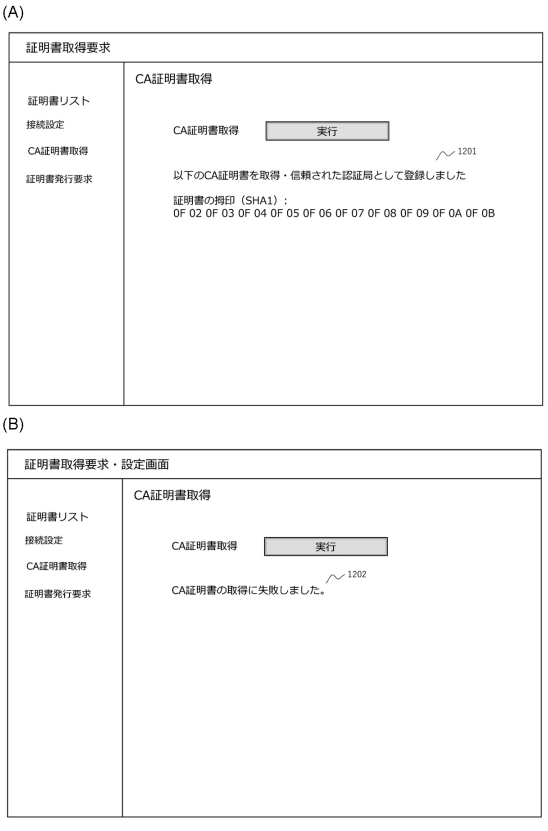
【図１０】



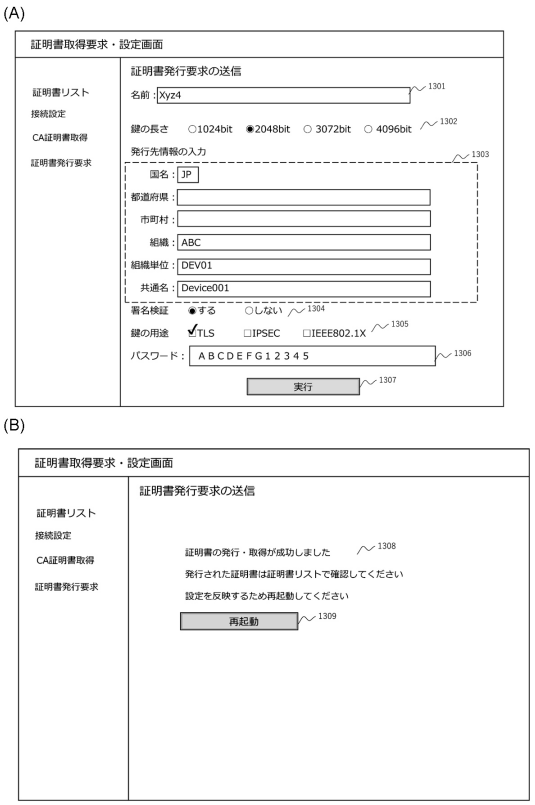
【図１１】



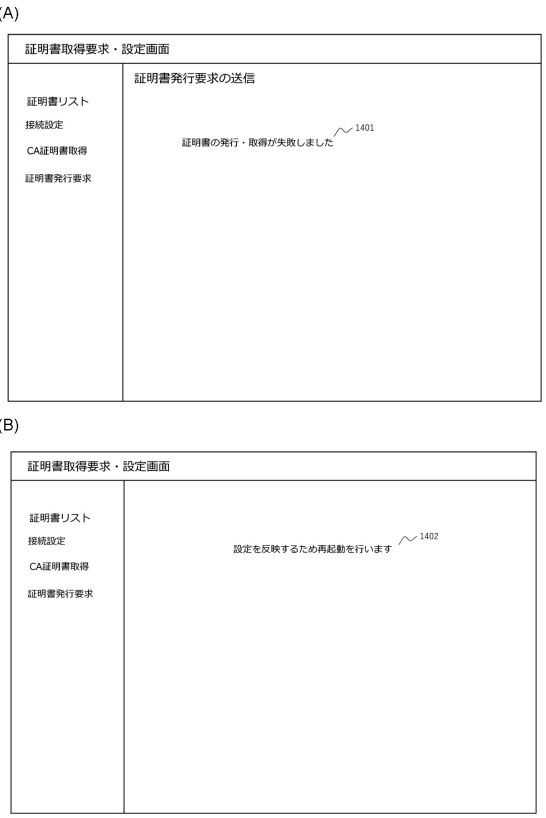
【図１２】



【図１３】

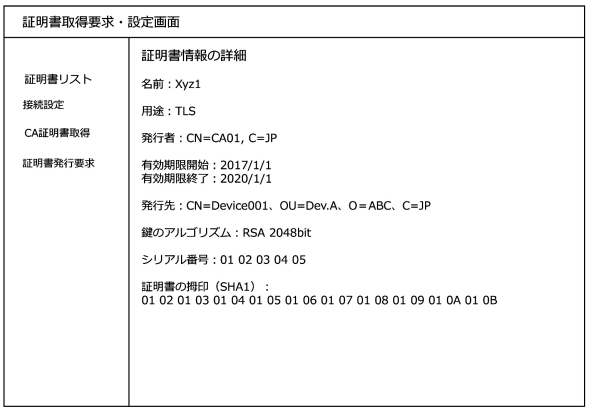


【図１４】



【図１５】

【図１６】



【図１７】

(A)

名前	用途	発行者	有効期間開始日	有効期間終了日	発行先	アルゴリズム	鍵長	シリアル番号	拇印
Xyz1	TLS	CN=CA01, C=JP	2019/1/1	2020/1/1	CN=Device001, OU=Dev.A, O=ABC, C=JP	RSA	1024	01 02 03 04 05	81 82 83 01 81 84 01 85 01 86 01 87 01 88 81 89 01 8A 01 8B
Xyz2	IPSEC	CN=CA01, C=JP	2015/1/1	2016/1/1	CN=Device001, OU=Dev.A, O=ABC, C=JP	RSA	2048	01 02 03 04 06	82 82 82 03 82 84 82 85 82 86 82 87 02 88 82 89 02 8A 02 8B
Xyz3	IEEE802.1X	CN=CA01, C=JP	2020/1/1	2025/1/1	CN=Device003, OU=Dev.A, O=ABC, C=JP	RSA	2048	01 02 03 04 07	83 82 83 03 83 84 83 85 83 86 83 87 03 88 83 89 03 8A 03 8B

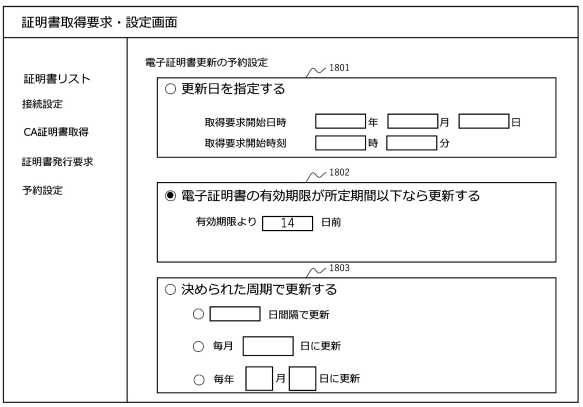
(B)

名前	用途	発行者	有効期間開始日	有効期間終了日	発行先	アルゴリズム	鍵長	シリアル番号	拇印
Xyz1	TLS	CN=CA01, C=JP	2019/1/1	2020/1/1	CN=Device001, OU=Dev.A, O=ABC, C=JP	RSA	1024	01 02 03 04 05	81 82 83 01 81 84 01 85 01 86 01 87 01 88 81 89 01 8A 01 8B
Xyz2	IPSEC	CN=CA01, C=JP	2015/1/1	2016/1/1	CN=Device001, OU=Dev.A, O=ABC, C=JP	RSA	2048	01 02 03 04 06	82 82 82 03 82 84 82 85 82 86 82 87 02 88 82 89 02 8A 02 8B
Xyz3	IEEE802.1X	CN=CA01, C=JP	2020/1/1	2025/1/1	CN=Device001, OU=Dev.A, O=ABC, C=JP	RSA	2048	01 02 03 04 07	83 82 83 03 83 84 83 85 83 86 83 87 03 88 83 89 03 8A 03 8B
XYz4	なし	CN=CA02, C=JP	2020/1/1	2025/1/1	CN=Device001, OU=Dev.A, O=ABC, C=JP	RSA	2048	01 02 03 04 08	84 82 84 03 84 84 84 85 84 86 84 87 04 88 84 89 04 8A 04 8B

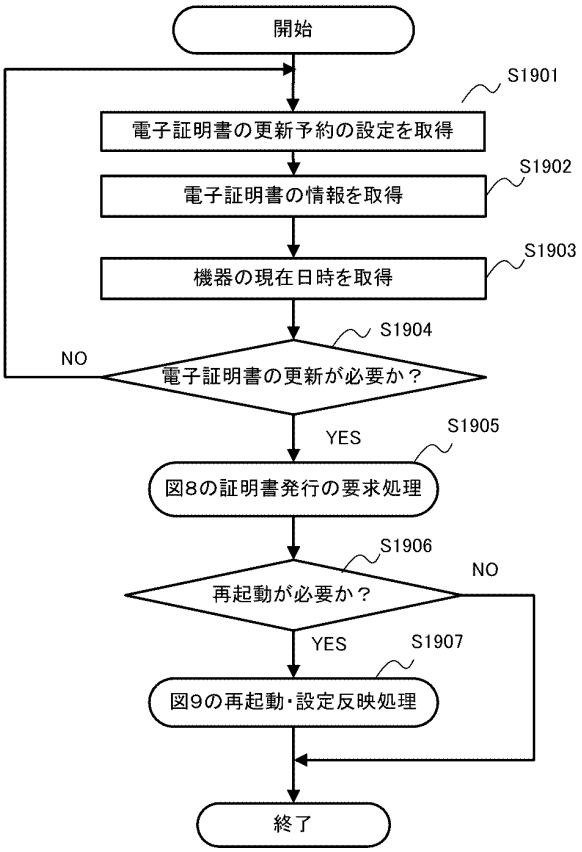
(C)

名前	用途	発行者	有効期間開始日	有効期間終了日	発行先	アルゴリズム	鍵長	シリアル番号	拇印
Xyz1	なし	CN=CA01, C=JP	2019/1/1	2020/1/1	CN=Device001, OU=Dev.A, O=ABC, C=JP	RSA	1024	01 02 03 04 05	81 82 83 01 81 84 01 85 01 86 01 87 01 88 81 89 01 8A 01 8B
Xyz2	IPSEC	CN=CA01, C=JP	2015/1/1	2016/1/1	CN=Device001, OU=Dev.A, O=ABC, C=JP	RSA	2048	01 02 03 04 06	82 82 82 03 82 84 82 85 82 86 82 87 02 88 82 89 02 8A 02 8B
Xyz3	IEEE802.1X	CN=CA01, C=JP	2020/1/1	2025/1/1	CN=Device003, OU=Dev.A, O=ABC, C=JP	RSA	2048	01 02 03 04 07	83 82 83 03 83 84 83 85 83 86 83 87 03 88 83 89 03 8A 03 8B
Xyz4	TLS	CN=CA01, C=JP	2020/1/1	2025/1/1	CN=Device005, OU=Dev.A, O=ABC, C=JP	RSA	2048	01 02 03 04 08	84 82 84 03 84 84 84 85 84 86 84 87 04 88 84 89 04 8A 04 8B

【図１８】



【図１９】



フロントページの続き

(56)参考文献 特開２０１４－１７４５６０（ＪＰ，Ａ）
特開２０１４－０１７７０７（ＪＰ，Ａ）
特開２０１６－１７８４５８（ＪＰ，Ａ）
特開平１１－２３１７７６（ＪＰ，Ａ）
特開平１１－００８６１９（ＪＰ，Ａ）
特開２０１０－１７７７４４（ＪＰ，Ａ）
特開平０６－１６２０５９（ＪＰ，Ａ）

(58)調査した分野 (Int.Cl.，ＤＢ名)
H04L9/08