(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2015-225616
(P2015-225616A)
(43)公開日　平成27年12月14日(2015.12.14)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/44	(2013.01)	G06F	21/20	144D	2C061
H04L 9/08	(2006.01)	H04L	9/00	601F	5C062
B41J 29/38	(2006.01)	B41J	29/38	Z	5J104
H04N 1/00	(2006.01)	H04N	1/00	107Z	
G06F 3/12	(2006.01)	G06F	3/12	B	

審査請求 未請求　請求項の数 13　ＯＬ　（全 22 頁）　最終頁に続く

(21)出願番号　特願2014-111795 (P2014-111795)
(22)出願日　平成26年5月29日 (2014.5.29)

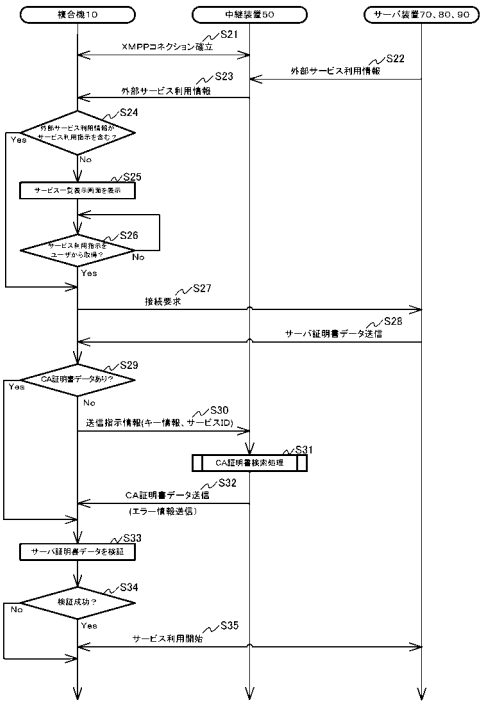
(71)出願人　000005267
ブラザー工業株式会社
愛知県名古屋市瑞穂区苗代町１５番１号
(74)代理人　100117101
弁理士　西木　信夫
(74)代理人　100120318
弁理士　松田　朋浩
(74)代理人　100142561
弁理士　田中　大介
(72)発明者　森　貴章
名古屋市瑞穂区苗代町１５番１号　ブラザー工業株式会社内

Ｆターム(参考)　2C061 AP07　HJ08　HK05　HK11　HN15

最終頁に続く

(54)【発明の名称】クライアント装置、サービス実行システム、及びプログラム

(57)【要約】
【課題】ＣＡ証明書データによって記憶領域が圧迫されることなく、且つ多数のサービスを利用可能なクライアント装置を提供する。
【解決手段】当該装置は、外部サービス利用情報を中継装置から受信する第１受信処理（Ｓ２３）と、外部サーバ証明書データを外部サーバ装置から受信する第２受信処理（Ｓ２８）と、ＣＡ証明書データが記憶されているか否かを判断する判断処理（Ｓ２９）と、ＣＡ証明書データが記憶されていることに応じて（Ｓ２９：Ｙｅｓ）、当該ＣＡ証明書データで外部サーバ証明書データを検証する第１検証処理（Ｓ３３）と、ＣＡ証明書データが記憶されていないことに応じて（Ｓ２９：Ｎｏ）、中継装置５０から受信したＣＡ証明書データで外部サーバ証明書データを検証する第２検証処理（Ｓ３２→Ｓ３３）と、中継装置５０から受信したＣＡ証明書データを記憶部に記憶させる記憶制御処理とを実行する。
【選択図】図５



【特許請求の範囲】
【請求項１】
サービスを提供するサーバ装置及び中継装置と通信する通信部と、
サーバ証明書データを検証するためのＣＡ証明書データを記憶可能な記憶部と、
制御部と、を備えており、
前記制御部は、
外部サービスを利用するための外部サービス利用情報を前記通信部を通じて前記中継装置から受信する第１受信処理と、
前記サービスの提供主体であることを証明するために前記サーバ装置から提供される前記サーバ証明書データであって、前記外部サービス利用情報によって特定される外部サーバ装置の外部サーバ証明書データを、前記通信部を通じて前記外部サーバ装置から受信する第２受信処理と、
前記外部サーバ証明書データを検証するための前記ＣＡ証明書データが前記記憶部に記憶されているか否かを判断する判断処理と、
前記外部サーバ証明書データを検証するための前記ＣＡ証明書データが前記記憶部に記憶されていると前記判断処理で判断したことに応じて、当該ＣＡ証明書データで前記外部サーバ証明書データを検証する第１検証処理と、
前記外部サーバ証明書データを検証するための前記ＣＡ証明書データが前記記憶部に記憶されていないと前記判断処理で判断したことに応じて、当該ＣＡ証明書データを前記通信部を通じて前記中継装置から受信し、且つ前記中継装置から受信した前記ＣＡ証明書データで前記外部サーバ証明書データを検証する第２検証処理と、
前記中継装置から受信した前記ＣＡ証明書データを前記記憶部に記憶させる記憶制御処理と、を実行するクライアント装置。
【請求項２】
前記記憶部は、
予め認められた特定サーバ装置が提供する特定サービスを利用するための特定サービス利用情報を記憶するサービス利用情報記憶領域と、
前記特定サービスの提供主体であることを証明するために前記特定サーバ装置が発行する特定サーバ証明書データを検証するための前記ＣＡ証明書データを記憶する第１記憶領域と、
前記第１検証処理において前記ＣＡ証明書データが読み出され、且つ前記記憶制御処理において前記ＣＡ証明書データが記憶される第２記憶領域と、を含む請求項１に記載のクライアント装置。
【請求項３】
前記制御部は、
前記判断処理において、前記ＣＡ証明書データが前記第２記憶領域に記憶されているか否かを判断し、
前記ＣＡ証明書データが前記第２記憶領域に記憶されていると前記判断処理で判断したことに応じて、前記第１検証処理を実行し、
前記ＣＡ証明書データが前記第２記憶領域に記憶されていないと前記判断処理で判断したことに応じて、前記第２検証処理及び前記記憶制御処理を実行する請求項２に記載のクライアント装置。
【請求項４】
前記第２記憶領域は、前記ＣＡ証明書データと、当該ＣＡ証明書データを前記外部サーバ証明書データの検証に用いた直近の日時を示す日時情報とを対応づけて記憶しており、
前記制御部は、前記第２記憶領域にＮ（Ｎは自然数）個の前記ＣＡ証明書データが記憶された状態で実行される前記記憶制御処理において、前記日時情報が最も古い前記ＣＡ証明書データを、前記中継装置から受信した前記ＣＡ証明書データで上書きする請求項２又は３に記載のクライアント装置。
【請求項５】

前記制御部は、
前記特定サービス利用情報によって特定される前記特定サーバ証明書データを前記通信部を通じて前記特定サーバ装置から受信する第３受信処理と、
前記第１記憶領域に記憶された前記ＣＡ証明書データで前記特定サーバ証明書データを検証する第３検証処理と、を実行する請求項２から４のいずれかに記載のクライアント装置。
【請求項６】
前記第１記憶領域は、不揮発性の記憶領域であり、
前記第２記憶領域は、揮発性の記憶領域である請求項２から５のいずれかに記載のクライアント装置。
【請求項７】
前記制御部は、前記第２検証処理において、
前記ＣＡ証明書データを特定するキー情報を含む送信指示情報を前記通信部を通じて前記中継装置に送信し、
前記キー情報に対応づけて前記中継装置に記憶された前記ＣＡ証明書データを前記通信部を通じて前記中継装置から受信する請求項１から６のいずれかに記載のクライアント装置。
【請求項８】
前記制御部は、
前記第１受信処理において、前記外部サービスを識別するサービス識別子を含む前記外部サービス利用情報を前記通信部を通じて前記中継装置から受信し、
前記第２検証処理において、
前記キー情報及び前記サービス識別子を含む前記送信指示情報を前記通信部を通じて前記中継装置に送信し、
前記キー情報及び前記サービス識別子に対応づけて前記中継装置に記憶された前記ＣＡ証明書データを前記通信部を通じて前記中継装置から受信し、
前記記憶制御処理において、前記中継装置から受信した前記ＣＡ証明書データと前記サービス識別子とを対応づけて前記記憶部に記憶させる請求項７に記載のクライアント装置。
【請求項９】
前記キー情報は、前記外部サーバ証明書データに含まれる情報であって、前記ＣＡ証明書データのコモンネーム或いは組織名を含む請求項７又は８に記載のクライアント装置。
【請求項１０】
前記制御部は、
該クライアント装置と前記中継装置との間でコネクションを確立するコネクション確立処理を前記第１受信処理に先立って実行し、
前記第１受信処理において、前記コネクションを通じて前記外部サービス利用情報を前記中継装置から受信する請求項１から９のいずれかに記載のクライアント装置。
【請求項１１】
サーバ装置及び中継装置と通信する通信部と、
サービスの提供主体であることを証明するために前記サーバ装置から提供されるサーバ証明書データを検証するためのＣＡ証明書データを記憶する記憶部と、
制御部と、を備えており、
前記記憶部は、
予め認められた特定サーバ装置が提供する特定サービスを利用するための特定サービス利用情報を記憶するサービス利用情報記憶領域と、
前記特定サーバ装置から提供される特定サーバ証明書データを検証するための前記ＣＡ証明書データを記憶する第１記憶領域と、
前記特定サービスと異なる外部サービスを提供する外部サーバ装置から提供される外部サーバ証明書データを検証するための前記ＣＡ証明書データを記憶する第２記憶領域と、

を含み、
前記制御部は、
前記外部サービスを利用するための外部サービス利用情報を前記通信部を通じて前記中継装置から受信する第１受信処理と、
当該サービスを提供する前記サーバ装置から前記サーバ証明書データを前記通信部を通じて受信し、前記記憶部に記憶された前記ＣＡ証明書データで当該サーバ証明書データを検証する検証処理と、を実行可能であり、
前記特定サービスを利用するのに先立って実行される前記検証処理において、前記第１記憶領域に記憶された前記ＣＡ証明書データで前記特定サーバ証明書データを検証し、
前記外部サービスを利用するのに先立って実行される前記検証処理において、前記第２記憶領域に記憶された前記ＣＡ証明書データで前記外部サーバ証明書データを検証するクライアント装置。
【請求項１２】
サービスを提供するサーバ装置及び中継装置と通信する通信部と、サーバ証明書データを検証するためのＣＡ証明書データを記憶可能な記憶部とを備えるコンピュータによって実行可能なプログラムであって、
外部サービスを利用するための外部サービス利用情報を前記通信部を通じて前記中継装置から受信する第１受信処理と、
前記サービスの提供主体であることを証明するために前記サーバ装置から提供される前記サーバ証明書データであって、前記外部サービス利用情報によって特定される外部サーバ装置の外部サーバ証明書データを、前記通信部を通じて前記外部サーバ装置から受信する第２受信処理と、
前記外部サーバ証明書データを検証するための前記ＣＡ証明書データが前記記憶部に記憶されているか否かを判断する判断処理と、
前記外部サーバ証明書データを検証するための前記ＣＡ証明書データが前記記憶部に記憶されていると前記判断処理で判断したことに応じて、当該ＣＡ証明書データで前記外部サーバ証明書データを検証する第１検証処理と、
前記外部サーバ証明書データを検証するための前記ＣＡ証明書データが前記記憶部に記憶されていないと前記判断処理で判断したことに応じて、当該ＣＡ証明書データを前記通信部を通じて前記中継装置から受信し、且つ前記中継装置から受信した前記ＣＡ証明書データで前記外部サーバ証明書データを検証する第２検証処理と、
前記中継装置から受信した前記ＣＡ証明書データを前記記憶部に記憶させる記憶制御処理と、を前記コンピュータに実行させるプログラム。
【請求項１３】
サービスを提供するサーバ装置と、前記サービスを利用するクライアント装置と、中継装置とを備えるサービス実行システムであって、
前記クライアント装置は、
サービスを提供するサーバ装置及び中継装置と通信する通信部と、
サーバ証明書データを検証するためのＣＡ証明書データを記憶可能な記憶部と、
制御部と、を備えており、
前記制御部は、
外部サービスを利用するための外部サービス利用情報を前記通信部を通じて前記中継装置から受信する第１受信処理と、
前記サービスの提供主体であることを証明するために前記サーバ装置から提供される前記サーバ証明書データであって、前記外部サービス利用情報によって特定される外部サーバ装置の外部サーバ証明書データを、前記通信部を通じて前記外部サーバ装置から受信する第２受信処理と、
前記外部サーバ証明書データを検証するための前記ＣＡ証明書データが前記記憶部に記憶されているか否かを判断する判断処理と、
前記外部サーバ証明書データを検証するための前記ＣＡ証明書データが前記記憶部に記

憶されていると前記判断処理で判断したことに応じて、当該ＣＡ証明書データで前記外部サーバ証明書データを検証する第１検証処理と、
前記外部サーバ証明書データを検証するための前記ＣＡ証明書データが前記記憶部に記憶されていないと前記判断処理で判断したことに応じて、当該ＣＡ証明書データを前記通信部を通じて前記中継装置から受信し、且つ前記中継装置から受信した前記ＣＡ証明書データで前記外部サーバ証明書データを検証する第２検証処理と、
前記中継装置から受信した前記ＣＡ証明書データを前記記憶部に記憶させる記憶制御処理と、を実行するサービス実行システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、サーバ装置から取得したサーバ証明書データを検証するクライアント装置に関する。
【背景技術】
【０００２】
従来より、サービスを提供するサーバ装置と当該サービスを利用するクライアント装置との間において、ＳＳＬ（Ｓｅｃｕｒｅ　Ｓｏｃｋｅｔｓ　Ｌａｙｅｒの略）を用いた通信が行われることがある（例えば、特許文献１参照）。ＳＳＬは、サーバ装置になりすました他の機器と通信すること、及びクライアント装置とサーバ装置との間で送受信されるデータの傍受や改ざんを防ぐのに有効である。
【０００３】
具体的には、クライアント装置は、サーバ装置のサービスを利用するに先立って、サーバ装置からサーバ証明書データを取得し、認証局が発行するＣＡ（Ｃｅｒｔｉｆｉｃａｔｉｏｎ　Ａｕｔｈｏｒｉｔｙの略）証明書データで当該サーバ証明書データを検証し、検証されたサーバ証明書データに含まれる公開鍵で暗号化した秘密鍵をサーバ装置へ送信する。そして、クライアント装置とサーバ装置との間で送受信されるデータは、この秘密鍵を用いて暗号化される。
【先行技術文献】
【特許文献】
【０００４】
【特許文献１】特開２００６－２３９９３０号公報
【発明の概要】
【発明が解決しようとする課題】
【０００５】
クライアント装置の記憶部に記憶されるＣＡ証明書データの数は、当該クライアント装置が利用するサービスの増加に伴って増加する。その結果、クライアント装置の記憶領域がＣＡ証明書データで圧迫されるという課題を生じる可能性がある。この課題は、記憶領域のサイズが小さいクライアント装置において特に顕著に現れる。
【０００６】
本発明は、上記の事情に鑑みてなされたものであり、その目的は、ＣＡ証明書データによって記憶領域が圧迫されることなく、且つ多数のサービスを利用可能なクライアント装置を提供することにある。
【課題を解決するための手段】
【０００７】
本明細書の一形態に係るクライアント装置は、サービスを提供するサーバ装置及び中継装置と通信する通信部と、サーバ証明書データを検証するためのＣＡ証明書データを記憶可能な記憶部と、制御部とを備える。前記制御部は、外部サービスを利用するための外部サービス利用情報を前記通信部を通じて前記中継装置から受信する第１受信処理と、前記サービスの提供主体であることを証明するために前記サーバ装置から提供される前記サーバ証明書データであって、前記外部サービス利用情報によって特定される外部サーバ装置

の外部サーバ証明書データを、前記通信部を通じて前記外部サーバ装置から受信する第２受信処理と、前記外部サーバ証明書データを検証するための前記ＣＡ証明書データが前記記憶部に記憶されているか否かを判断する判断処理と、前記外部サーバ証明書データを検証するための前記ＣＡ証明書データが前記記憶部に記憶されていると前記判断処理で判断したことに応じて、当該ＣＡ証明書データで前記外部サーバ証明書データを検証する第１検証処理と、前記外部サーバ証明書データを検証するための前記ＣＡ証明書データが前記記憶部に記憶されていないと前記判断処理で判断したことに応じて、当該ＣＡ証明書データを前記通信部を通じて前記中継装置から受信し、且つ前記中継装置から受信した前記ＣＡ証明書データで前記外部サーバ証明書データを検証する第２検証処理と、前記中継装置から受信した前記ＣＡ証明書データを前記記憶部に記憶させる記憶制御処理とを実行する。

【０００８】

上記構成によれば、必要なＣＡ証明書データが記憶部に記憶されている場合は当該ＣＡ証明書データで第１検証処理を実行し、必要なＣＡ証明書データが記憶部に記憶されていない場合は当該ＣＡ証明書データを中継装置から取得して第２検証処理を実行することができる。その結果、ＣＡ証明書データによって記憶領域が圧迫されることなく、且つ多数のサービスを利用することができる。

【０００９】

本明細書の他の形態に係るクライアント装置は、サーバ装置及び中継装置と通信する通信部と、サービスの提供主体であることを証明するために前記サーバ装置から提供されるサーバ証明書データを検証するためのＣＡ証明書データを記憶する記憶部と、制御部とを備える。前記記憶部は、予め認められた特定サーバ装置が提供する特定サービスを利用するための特定サービス利用情報を記憶するサービス利用情報記憶領域と、前記特定サーバ装置から提供される特定サーバ証明書データを検証するための前記ＣＡ証明書データを記憶する第１記憶領域と、前記特定サービスと異なる外部サービスを提供する外部サーバ装置から提供される外部サーバ証明書データを検証するための前記ＣＡ証明書データを記憶する第２記憶領域とを含む。前記制御部は、前記外部サービスを利用するための外部サービス利用情報を前記通信部を通じて前記中継装置から受信する第１受信処理と、当該サービスを提供する前記サーバ装置から前記サーバ証明書データを前記通信部を通じて受信し、前記記憶部に記憶された前記ＣＡ証明書データで当該サーバ証明書データを検証する検証処理とを実行可能である。そして、前記制御部は、前記特定サービスを利用するのに先立って実行される前記検証処理において、前記第１記憶領域に記憶された前記ＣＡ証明書データで前記特定サーバ証明書データを検証し、前記外部サービスを利用するのに先立って実行される前記検証処理において、前記第２記憶領域に記憶された前記ＣＡ証明書データで前記外部サーバ証明書データを検証する。

【００１０】

本明細書に記載のプログラムは、サービスを提供するサーバ装置及び中継装置と通信する通信部と、サーバ証明書データを検証するためのＣＡ証明書データを記憶可能な記憶部とを備えるコンピュータによって実行可能である。該プログラムは、外部サービスを利用するための外部サービス利用情報を前記通信部を通じて前記中継装置から受信する第１受信処理と、前記サービスの提供主体であることを証明するために前記サーバ装置から提供される前記サーバ証明書データであって、前記外部サービス利用情報によって特定される外部サーバ装置の外部サーバ証明書データを、前記通信部を通じて前記外部サーバ装置から受信する第２受信処理と、前記外部サーバ証明書データを検証するための前記ＣＡ証明書データが前記記憶部に記憶されているか否かを判断する判断処理と、前記外部サーバ証明書データを検証するための前記ＣＡ証明書データが前記記憶部に記憶されていると前記判断処理で判断したことに応じて、当該ＣＡ証明書データで前記外部サーバ証明書データを検証する第１検証処理と、前記外部サーバ証明書データを検証するための前記ＣＡ証明書データが前記記憶部に記憶されていないと前記判断処理で判断したことに応じて、当該ＣＡ証明書データを前記通信部を通じて前記中継装置から受信し、且つ前記中継装置から

受信した前記ＣＡ証明書データで前記外部サーバ証明書データを検証する第２検証処理と、前記中継装置から受信した前記ＣＡ証明書データを前記記憶部に記憶させる記憶制御処理とを前記コンピュータに実行させる。

【００１１】

本明細書に記載のサービス実行システムは、サービスを提供するサーバ装置と、前記サービスを利用するクライアント装置と、中継装置とを備える。前記クライアント装置は、サービスを提供するサーバ装置及び中継装置と通信する通信部と、サーバ証明書データを検証するためのＣＡ証明書データを記憶可能な記憶部と、制御部とを備える。前記制御部は、外部サービスを利用するための外部サービス利用情報を前記通信部を通じて前記中継装置から受信する第１受信処理と、前記サービスの提供主体であることを証明するために前記サーバ装置から提供される前記サーバ証明書データであって、前記外部サービス利用情報によって特定される外部サーバ装置の外部サーバ証明書データを、前記通信部を通じて前記外部サーバ装置から受信する第２受信処理と、前記外部サーバ証明書データを検証するための前記ＣＡ証明書データが前記記憶部に記憶されているか否かを判断する判断処理と、前記外部サーバ証明書データを検証するための前記ＣＡ証明書データが前記記憶部に記憶されていると前記判断処理で判断したことに応じて、当該ＣＡ証明書データで前記外部サーバ証明書データを検証する第１検証処理と、前記外部サーバ証明書データを検証するための前記ＣＡ証明書データが前記記憶部に記憶されていないと前記判断処理で判断したことに応じて、当該ＣＡ証明書データを前記通信部を通じて前記中継装置から受信し、且つ前記中継装置から受信した前記ＣＡ証明書データで前記外部サーバ証明書データを検証する第２検証処理と、前記中継装置から受信した前記ＣＡ証明書データを前記記憶部に記憶させる記憶制御処理とを実行する。

【発明の効果】

【００１２】

本明細書に記載のクライアント装置によれば、必要なＣＡ証明書データが記憶部に記憶されている場合は当該ＣＡ証明書データで第１検証処理を実行し、必要なＣＡ証明書データが記憶部に記憶されていない場合は当該ＣＡ証明書データを中継装置から取得して第２検証処理を実行することができる。その結果、ＣＡ証明書データによって記憶領域が圧迫されることなく、且つ多数のサービスを利用することができる。

【図面の簡単な説明】

【００１３】

【図１】図１は、実施形態に係るサービス実行システム１００のブロック図である。

【図２】図２は、複合機１０のデータ記憶領域３２Ｂのデータ構造の一例であって、（Ａ）はサービス利用情報記憶領域３６を、（Ｂ）は第１記憶領域３７を、（Ｃ）は第２記憶領域３８を示す。

【図３】図３は、中継装置５０のデータ記憶領域６２Ｂのデータ構造の一例であって、（Ａ）は第１記憶領域６６を、（Ｂ）は第２記憶領域６７を示す。

【図４】図４は、ＣＡ証明書登録処理のフローチャートである。

【図５】図５は、サービス実行システム１００の動作を示すフローチャートである。

【図６】図６は、検証処理のフローチャートである。

【図７】図７は、ＣＡ証明書検索処理のフローチャートである。

【図８】図８は、サービス一覧表示画面の一例である。

【発明を実施するための形態】

【００１４】

以下、適宜図面を参照して本発明の実施形態について説明する。なお、以下に説明される実施形態は本発明の一例にすぎず、本発明の要旨を変更しない範囲で、本発明の実施形態を適宜変更できることは言うまでもない。

【００１５】

図１は、本実施形態に係るサービス実行システム１００の概略図である。図１に示されるサービス実行システム１００は、複合機１０と、中継装置５０と、サーバ装置７０、８

０、９０とで構成されている。複合機１０、中継装置５０、及びサーバ装置７０～９０は、通信ネットワーク１０２を介して相互に通信可能とされている。通信ネットワーク１０２の具体例は特に限定されないが、例えば、インターネット、移動体通信網、有線ＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋの略）、無線ＬＡＮ、或いはこれらの組み合わせであってもよい。本実施形態では、複合機１０はＬＡＮに接続されており、中継装置５０及びサーバ装置７０～９０はインターネットに接続されている。

【００１６】

また、複合機１０が接続されたＬＡＮは、不図示のルータを通じてインターネットに接続されている。このルータは、ファイアウォールとして機能する。すなわち、当該ルータは、複合機１０から中継装置５０或いはサーバ装置７０～９０へ送信されるリクエスト、及び中継装置５０或いはサーバ装置７０～９０から複合機１０へ送信されるレスポンスを通過させる。一方、当該ルータは、中継装置５０或いはサーバ装置７０～９０から複合機１０へ送信されるリクエストを遮断する。

【００１７】

そこで、複合機１０と中継装置５０との間でＸＭＰＰ　ｏｖｅｒ　ＢＯＳＨ（Ｅｘｔｅｎｓｉｂｌｅ　Ｍｅｓｓａｇｉｎｇ　ａｎｄ　Ｐｒｅｓｅｎｃｅ　Ｐｒｏｔｏｃｏｌ　Ｏｖｅｒ　Ｂｉｄｉｒｅｃｔｉｏｎａｌ－Ｓｔｒｅａｍｓ　Ｏｖｅｒ　Ｓｙｎｃｈｒｏｎｏｕｓ　ＨＴＴＰの略）によるコネクションを確立させることによって、中継装置５０からのリクエストをルータを経由して複合機１０に受信させることができる。

【００１８】

ＸＭＰＰ　ｏｖｅｒ　ＢＯＳＨは、コネクションを確立した状態をほぼ常時維持するプロトコルである。但し、複合機１０と中継装置５０との間でコネクションを確立させるプロトコルは、ＸＭＰＰ　ｏｖｅｒ　ＢＯＳＨに限定されず、例えば、接続確立型のプロトコル、常時接続型のプロトコル、或いは接続維持型のプロトコルと呼ばれるプロトコルであればよい。

【００１９】

［複合機１０］

複合機１０は、図１に示されるように、プリンタ部１１と、スキャナ部１２と、表示部２３と、操作部２４と、通信部２５と、ＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔの略）３１と、記憶部３２と、通信バス３３とを主に備える。複合機１０を構成する各構成要素は、通信バス３３を介して相互に接続されている。複合機１０は、サーバ装置７０～９０が提供するサービスを利用するクライアント装置或いは画像記録装置の一例である。但し、クライアント装置の具体例は複合機１０に限定されず、例えば、プリンタ、ラベルプリンタ、スキャナ、ＦＡＸ装置、ミシン、工作機械等の専用機、スマートフォン、携帯電話、タブレット端末等の携帯端末、ＰＣ（Ｐｅｒｓｏｎａｌ　Ｃｏｍｐｕｔｅｒの略）等であってもよい。

【００２０】

［プリンタ部１１、スキャナ部１２］

プリンタ部１１は、画像データで示される画像を記録用紙に記録する記録処理を実行する。プリンタ部１１の記録方式は特に限定されないが、例えば、インクジェット方式や電子写真方式などの公知の方式を採用することができる。スキャナ部１２は、記録用紙に記録されている画像を読み取って画像データを生成するスキャン処理を実行する。複合機１０は、ＦＡＸの送受信を行うＦＡＸ機能、記録用紙に記録された画像を読み取って他の記録用紙に記録するコピー機能等をさらに有してもよい。

【００２１】

［表示部２３］

表示部２３は、各種情報を表示する表示画面を備える。表示部２３の具体的な構成は特に限定されないが、例えば、液晶ディスプレイ（Ｌｉｑｕｉｄ　Ｃｒｙｓｔａｌ　Ｄｉｓｐｌａｙの略）、有機ＥＬディスプレイ（Ｏｒｇａｎｉｃ　Ｅｌｅｃｔｒｏ－Ｌｕｍｉｎｅｓｃｅｎｃｅ　Ｄｉｓｐｌａｙの略）等を採用することができる。

【００２２】
［操作部２４］
操作部２４は、表示部２３の表示画面に表示されたオブジェクトを選択するユーザの操作を受け付ける。具体的には、操作部２４は、例えば押ボタンを有しており、押下された押ボタンに対応づけられた各種の操作信号をＣＰＵ３１へ出力する。さらに、操作部２４は、表示部２３の表示画面に重畳された膜状のタッチセンサを有していてもよい。すなわち、表示部２３がタッチパネルディスプレイとして構成されてもよい。タッチセンサには、静電容量方式、抵抗膜方式等の周知の方式を採用することができる。
【００２３】
なお、「オブジェクト」とは、ユーザが操作部２４を操作することによって選択可能な画像を指す。一例として、オブジェクトは表示部２３に表示された文字列であって、操作部２４の方向キーを押下することによってオブジェクトの１つがハイライト表示され、操作部２４の決定ボタンを押下することによってハイライト表示されたオブジェクトが選択されてもよい。他の例として、操作部２４がタッチパネルである場合のオブジェクトは表示部２３に表示されたアイコン、ボタン、リンク等であって、タッチ位置に表示されたオブジェクトが選択されてもよい。
【００２４】
［通信部２５］
通信部２５は、通信ネットワーク１０２を通じて外部装置と通信を行うためのインタフェースである。すなわち、複合機１０は、通信部２５を通じて中継装置５０或いはサーバ装置７０～９０に各種情報を出力し、通信部２５を通じて中継装置５０或いはサーバ装置７０～９０から各種データ又は各種情報を受信する。
【００２５】
［ＣＰＵ３１］
ＣＰＵ３１は、複合機１０の全体動作を制御するものである。ＣＰＵ３１は、操作部２４から出力される各種情報、及び通信部２５を通じて外部装置から取得した各種情報等に基づいて、後述する各種プログラムを記憶部３２から取得して実行する。すなわち、ＣＰＵ３１及び記憶部３２は、制御部の一例を構成する。
【００２６】
［記憶部３２］
記憶部３２は、プログラム記憶領域３２Ａと、データ記憶領域３２Ｂとを有する。プログラム記憶領域３２Ａには、ＯＳ（Ｏｐｅｒａｔｉｎｇ　Ｓｙｓｔｅｍの略）３４と、制御プログラム３５とが格納される。なお、制御プログラム３５は、単一のプログラムであってもよいし、複数のプログラムの集合体であってもよい。データ記憶領域３２Ｂには、制御プログラム３５の実行に必要なデータ或いは情報が記憶される。
【００２７】
なお、本明細書中の「データ」と「情報」とは、コンピュータによって取り扱い可能なビット或いはビット列である点において共通する。「データ」とは、各ビットが示す意味内容をコンピュータが考慮することなく取り扱えるものを指す。これに対して、「情報」とは、各ビットが示す意味内容によってコンピュータの動作が分岐するものを指す。さらに、「指示」は、送信先の装置に対して次の動作を促すための制御信号であって、情報を含んでいることもあるし、それ自体が情報としての性質を有していることもある。
【００２８】
また、「データ」及び「情報」は、形式（例えば、テキスト形式、バイナリ形式、フラグ形式等）がコンピュータ毎に変更されたとしても、同一の意味内容と認識される限り、同一のデータ及び情報として取り扱われる。例えば、「２つ」であることを示す情報が、あるコンピュータではＡＳＣＩＩコードで”０ｘ３２”というテキスト形式の情報として保持され、別のコンピュータでは二進数表記で”１０”というバイナリ形式の情報として保持されてもよい。
【００２９】

但し、上記の「データ」及び「情報」の区別は厳密なものではなく、例外的な取り扱いも許容される。例えば、データが一時的に情報として扱われてもよいし、情報が一時的にデータとして扱われてもよい。また、ある装置ではデータとして扱われるものが、他の装置では情報として扱われてもよい。さらには、データの中から情報が取り出されてもよいし、情報の中からデータが取り出されてもよい。

【００３０】

記憶部３２は、例えば、ＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙの略）、ＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙの略）、ＥＥＰＲＯＭ（Ｅｌｅｃｔｒｉｃａｌｌｙ　Ｅｒａｓａｂｌｅ　Ｐｒｏｇｒａｍｍａｂｌｅ　Ｒｅａｄ－Ｏｎｌｙ　Ｍｅｍｏｒｙの略）、ＨＤＤ（Ｈａｒｄ　Ｄｉｓｋ　Ｄｒｉｖｅの略）、ＣＰＵ３１が備えるバッファ等、或いはそれらの組み合わせによって構成される。

【００３１】

なお、記憶部３２は、コンピュータが読み取り可能なストレージ媒体であってもよい。コンピュータが読み取り可能なストレージ媒体とは、ｎｏｎ－ｔｒａｎｓｉｔｏｒｙな媒体である。ｎｏｎ－ｔｒａｎｓｉｔｏｒｙな媒体には、上記の例の他に、ＣＤ－ＲＯＭ、ＤＶＤ－ＲＯＭ等の記録媒体も含まれる。また、ｎｏｎ－ｔｒａｎｓｉｔｏｒｙな媒体は、ｔａｎｇｉｂｌｅな媒体でもある。一方、インターネット上のサーバなどからダウンロードされるプログラムを搬送する電気信号は、コンピュータが読み取り可能な媒体の一種であるコンピュータが読み取り可能な信号媒体であるが、ｎｏｎ－ｔｒａｎｓｉｔｏｒｙなコンピュータが読み取り可能なストレージ媒体には含まれない。

【００３２】

プログラム記憶領域３２Ａに記憶されているプログラムは、ＣＰＵ３１によって実行される。しかしながら、本明細書では、ＣＰＵ３１を省略して各プログラムの動作を説明することがある。すなわち、以下の説明において、「プログラムＡが処理Ａを実行する」という趣旨の記述は、「ＣＰＵ３１がプログラムＡに記述された処理Ａを実行する」ことを指してもよい。後述する中継装置５０についても同様である。

【００３３】

ＯＳ３４は、複合機１０を構成するハードウェアであるプリンタ部１１、スキャナ部１２、表示部２３、操作部２４、及び通信部２５等を制御するためのＡＰＩ（Ａｐｐｌｉｃａｔｉｏｎ　Ｐｒｏｇｒａｍｍｉｎｇ　Ｉｎｔｅｒｆａｃｅの略）を提供する基本プログラムである。すなわち、上記の各プログラムは、ＯＳ３４が提供するＡＰＩを呼び出すことによって、各ハードウェアを制御する。しかしながら、本明細書では、ＯＳ３４を省略して各プログラムの動作を説明する。すなわち、以下の説明において、「プログラムＢがハードウェアＣを制御する」という趣旨の記述は、「プログラムＢがＯＳ３４のＡＰＩを通じてハードウェアＣを制御する」ことを指してもよい。後述する中継装置５０についても同様である。

【００３４】

データ記憶領域３２Ｂは、図２に示されるように、図２（Ａ）に示されるサービス利用情報記憶領域３６と、図２（Ｂ）に示される第１記憶領域３７と、図２（Ｃ）に示される第２記憶領域３８とを含む。サービス利用情報記憶領域３６及び第１記憶領域３７は、例えば、不揮発性のＲＯＭによって構成されている。一方、第２記憶領域３８は、例えば、揮発性のＲＡＭによって構成されている。但し、各記憶領域３６～３８の具体的な構成は、これらに限定されない。また、各記憶領域３６～３８に記憶されるデータ及び情報の詳細は、後述する。

【００３５】

［中継装置５０］

中継装置５０は、図１に示されるように、表示部５３と、操作部５４と、通信部５５と、ＣＰＵ６１と、記憶部６２と、通信バス６３とを主に備える。中継装置５０に含まれる表示部５３、操作部５４、通信部５５、ＣＰＵ６１、記憶部６２、及び通信バス６３は、複合機１０に含まれる表示部２３、操作部２４、通信部２５、ＣＰＵ３１、記憶部３２、

及び通信バス３３と共通するので、再度の説明は省略する。ＣＰＵ６１及び記憶部６２は制御部の一例を構成する。記憶部６２のプログラム記憶領域６２Ａには、ＯＳ６４と、制御プログラム６５とが格納されている。記憶部６２のデータ記憶領域６２Ｂは、図３（Ａ）に示される第１記憶領域６６と、図３（Ｂ）に示される第２記憶領域６７とを含む。各記憶領域６６、６７に記憶されるデータ及び情報の詳細は、後述する。

【００３６】

［サーバ装置７０、８０、９０］

サーバ装置７０、８０、９０は、複合機１０に利用させるサービスを提供する装置である。サーバ装置７０、８０は、中継装置５０の管理者に予め認められた特定サーバ装置の一例である。以下、サーバ装置７０、８０が提供するサービスを特定サービスと表記する。サーバ装置７０、８０の具体例は特に限定されないが、例えば、「Ｄｒｏｐｂｏｘ（登録商標）」、「Ｇｏｏｇｌｅ　Ｄｏｃｓ（登録商標）」、「Ｅｖｅｒｎｏｔｅ（登録商標）」等のサービスを提供する装置である。一方、サーバ装置９０は、特定サーバ装置と異なる外部サーバ装置の一例である。以下、サーバ装置９０が提供するサービスを外部サービスと表記する。

【００３７】

サーバ装置７０～９０が提供するサービスの具体例は特に限定されないが、例えば、クラウドプリント処理、スキャンＴｏクラウド処理、デバイス情報収集処理等が挙げられる。クラウドプリント処理は、サーバ装置７０～９０に記憶された画像データを複合機１０に受信させ、当該画像データに対する記録処理をプリンタ部１１に実行させる処理である。スキャンＴｏクラウド処理は、スキャナ部１２にスキャン処理を実行させ、当該スキャン処理で生成された画像データをサーバ装置７０～９０に送信させる処理である。デバイス情報収集処理は、複合機１０のデバイス情報をサーバ装置７０～９０に送信させる処理である。デバイス情報は、例えば、プリンタ部１１によって画像が記録された記録用紙の枚数、プリンタ部１１に装着されたインクカートリッジ内のインク残量等を含む。

【００３８】

また、サーバ装置７０～９０が提供するサービスによって送受信されるデータ或いは情報は、ＳＳＬによって暗号化される。サーバ装置７０～９０は、例えばクラウドプリント処理において、暗号化した画像データを複合機１０へ送信する。また、複合機１０は、例えばスキャンＴｏクラウド処理において、暗号化した画像データをサーバ装置７０～９０へ送信する。さらに、複合機１０は、例えばデバイス情報収集処理において、暗号化したデバイス情報をサーバ装置７０～９０へ送信する。

【００３９】

図２（Ａ）に示されるサービス利用情報記憶領域３６には、サーバ装置７０、８０が提供する特定サービスを利用するための特定サービス利用情報が記憶されている。サービスＩＤ”００１”で識別されるサービス利用情報は、例えば、サーバ装置７０が提供するサービスを利用するための情報である。サービスＩＤ”００２”で識別されるサービス利用情報は、例えば、サーバ装置８０が提供するサービスを利用するための情報である。特定サービス利用情報は、特定サービスを識別するサービスＩＤと、インタフェース定義ファイルと、アクセスＵＲＬ（Ｕｎｉｆｏｒｍ　Ｒｅｓｏｕｒｃｅ　Ｌｏｃａｔｏｒの略）とを含む。後述する外部サービス利用情報についても同様である。特定サービス利用情報及び外部サービス利用情報は、サービス利用情報の一例である。

【００４０】

サービスＩＤは、サービスを一意に識別するための識別子である。サービスＩＤは、例えば、中継装置５０の管理者によって各サービスに割り当てられる。サービスＩＤは、サービス識別子の一例である。インタフェース定義ファイルは、サービスの利用を開始するサービス利用指示を複合機１０のユーザから受け付けるために、サービス一覧表示画面に含めるサービスアイコンを定義するファイルである。インタフェース定義ファイルは、例えば、ＨＴＭＬ（ＨｙｐｅｒＴｅｘｔ　Ｍａｒｋｕｐ　Ｌａｎｇｕａｇｅの略）或いはＸＭＬ（Ｅｘｔｅｎｓｉｂｌｅ　Ｍａｒｋｕｐ　Ｌａｎｇｕａｇｅの略）で記述される。ア

クセスＵＲＬは、サービスの利用を開始する際に複合機１０にアクセスさせるサーバ装置７０～９０の所在を示す所在情報の一例である。なお、サービス利用情報記憶領域３６には、インタフェース定義ファイルに代えて、当該サービスを表す文字列が記憶されてもよい。この場合、サービス一覧表示画面には、サービスアイコンに代えて当該文字列が含まれてもよい。

【００４１】

図２（Ｂ）に示される複合機１０の第１記憶領域３７には、ＣＡ証明書データと、当該ＣＡ証明書データを特定するキー情報とが互いに対応づけられて記憶されている。ＣＡ証明書データは、サーバ装置７０～９０から提供されるサーバ証明書データを検証するために、認証局（「Ｃｅｒｔｉｆｉｃａｔｉｏｎ　Ａｕｔｈｏｒｉｔｙ」を指す。）によって発行されたものである。第１記憶領域３７に記憶されるＣＡ証明書データは、例えば、複合機１０の製造時にプリインストールされたものである。

【００４２】

ＣＡ証明書データは、例えば、当該証明書の発行者（ＩＴＵ－Ｔ　Ｘ．５０９で規定される「Ｉｓｓｕｅｒ」を指す。）、コモンネーム（ＩＴＵ－Ｔ　Ｘ．５０９で規定される「Ｃｏｍｍｏｎ　Ｎａｍｅ」を指す。）、組織名（ＩＴＵ－Ｔ　Ｘ．５０９で規定される「Ｏｒｇａｎｉｚａｔｉｏｎａｌ　Ｕｎｉｔ」を指す。）、当該証明書の有効期限（ＩＴＵ－Ｔ　Ｘ．５０９で規定される「Ｖａｌｉｄｉｔｙ」を指す。）、及びＣＡ公開鍵データ等を含む。キー情報は、ＣＡ証明書データに含まれる情報によって構成される。キー情報は、例えば、コモンネーム或いは組織名を含む。ＣＡ証明書データ及びサーバ証明書データは、例えば、ＩＴＵ－Ｔ　Ｘ．５０９で規定されたデジタル証明書のフォーマットに対応する。

【００４３】

図２（Ｃ）に示される複合機１０の第２記憶領域３８には、ＣＡ証明書データと、キー情報と、サービスＩＤと、最終アクセス日時とが互いに対応づけられて記憶可能となっている。最終アクセス日時は、対応するＣＡ証明書データをサーバ証明書データの検証に用いた直近の日時を示す日時情報の一例である。第２記憶領域３８には、Ｎ（Ｎは自然数）個のＣＡ証明書データ、より詳細には図２（Ｃ）に示されるＮ行のレコードを記憶可能なメモリサイズが割り当てられている。そして、第２記憶領域３８には、中継装置５０から受信したＣＡ証明書データ及びサービスＩＤと、当該ＣＡ証明書データから抽出されたキー情報とが記憶可能である。但し、ＲＡＭによって構成された第２記憶領域３８には、複合機１０の電源をＯＮした時点において、何も記憶されていない。

【００４４】

図３（Ａ）に示される中継装置５０の第１記憶領域６６には、ＣＡ証明書データと、キー情報とが互いに対応づけられて記憶される。図３（Ｂ）に示される中継装置５０の第２記憶領域６７には、ＣＡ証明書データと、キー情報と、サービスＩＤとが互いに対応づけられて記憶されている。データ記憶領域６２Ｂに記憶されるＣＡ証明書データは、例えば、図４に示されるＣＡ証明書登録処理によって登録される。図４に示されるＣＡ証明書登録処理は、例えば、中継装置５０の制御プログラム６５によって実現される。ＣＡ証明書登録処理は、登録処理の一例である。

【００４５】

［ＣＡ証明書登録処理］

まず、制御プログラム６５は、中継装置５０の管理者から管理者Ｉ／Ｆを通じてＣＡ証明書データを取得したことに応じて（Ｓ１１：管理者Ｉ／Ｆ）、取得したＣＡ証明書データと、当該ＣＡ証明書データから抽出したキー情報とを対応づけて第１記憶領域６６に記憶させる（Ｓ１２）。管理者Ｉ／Ｆは、例えば、中継装置５０の表示部５３及び操作部５４の組み合わせによって実現される。なお、本明細書中の「に応じて」は、当該文字列の前に記載された条件が満たされた場合に、当該文字列の後に記載された処理が実行されることを示す。なお、処理が実行されるタイミングは、条件が満たされた後であればよく、当該条件が満たされた直後である必要は必ずしもない。

【００４６】
一方、制御プログラム６５は、ＣＡ証明書データ及びサービスＩＤを通信部５５を通じてサーバ装置９０から受信したことに応じて（Ｓ１１：サーバ装置）、受信したＣＡ証明書データ及びサービスＩＤと、当該ＣＡ証明書データから抽出したキー情報とを対応づけて第２記憶領域６７に記憶させる（Ｓ１３）。なお、第２記憶領域６４に記憶されるＣＡ証明書データの取得方法は、上記の例に限定されない。例えば、サーバ装置９０の管理者は、中継装置５０にＣＡ証明書データをアップロードするための受付画面をサーバ装置９０と異なる端末に表示させ、当該受付画面を通じてＣＡ証明書データを中継装置５０にアップロードしてもよい。そして、制御プログラム６５は、受付画面を通じて受信したＣＡ証明書データを第２記憶領域６４に記憶させてもよい。

【００４７】
なお、複合機１０の第１記憶領域３７及び中継装置５０の第１記憶領域６６には、例えば、パブリック認証局によって発行されたＣＡ証明書データのみが記憶される。また、中継装置５０の第２記憶領域６７には、例えば、プライベート認証局によって発行されたＣＡ証明書データのみが記憶されてもよいし、パブリック認証局によって発行されたＣＡ証明書データがさらに記憶されてもよい。さらに、複合機１０の第２記憶領域３８には、中継装置５０の第１記憶領域６６或いは第２記憶領域６７に記憶されたＣＡ証明書データが記憶され得る。なお、各記憶領域３７、３８、６６、６７に記憶されるＣＡ証明書データの種類は、上記の例に限定されない。例えば、プライベート認証局によって発行されたＣＡ証明書データが第１記憶領域３７、６６にさらに記憶されてもよい。また、第１記憶領域３７、６６と第２記憶領域３８、６７とが区別されていなくてもよい。

【００４８】
パブリック認証局とは、認証業務運用規程を公開する等によって世間一般に高い信頼性が認められている認証局であって、例えば、ＧＭＯグローバルサイン株式会社や日本ベリサイン株式会社等によって設立されたものである。一方、プライベート認証局とは、例えば、サーバ装置９０の管理者等が独自の運用基準を設けて設立したものである。但し、パブリック認証局とプライベート認証局との区別は一義的なものではなく、複合機１０の製造者或いは中継装置５０の管理者によって適宜判断されてもよい。

【００４９】
［サービス実行システム１００の動作］
図５～図８を参照して、サービス実行システム１００の動作を説明する。本実施形態に係るサービス実行システム１００において、サーバ装置７０～９０が提供するサービスを利用しようとする複合機１０は、当該サーバ装置７０～９０から受信したサーバ証明書データを、データ記憶領域３２Ｂに記憶されたＣＡ証明書データ或いは中継装置５０から受信したＣＡ証明書データを用いて検証（ＳＳＬにおける「ｖａｌｉｄａｔｅ」を指す。）する。

【００５０】
まず、複合機１０の制御プログラム３５は、ＸＭＰＰ　ｏｖｅｒ　ＢＯＳＨに準拠した手順で中継装置５０との間にコネクション（以下、「ＸＭＰＰコネクション」と表記する。）を確立する（Ｓ２１）。ＸＭＰＰコネクションは、中継装置５０から複合機１０へリクエストを送信する（所謂、「サーバプッシュ」を指す。）ためのコネクションである。なお、ＸＭＰＰコネクションは、予め定められた接続維持期間が経過したことによって切断される。そこで、制御プログラム３５は、接続維持期間より短い再接続期間が経過したことに応じて、中継装置５０との間にＸＭＰＰコネクションを確立する。ＸＭＰＰコネクションは、例えば図５～図７の処理が実行されている間、複合機１０によって維持される。

【００５１】
次に、中継装置５０の制御プログラム６５は、通信部５５を通じてサーバ装置９０から外部サービス利用情報を受信したことに応じて（Ｓ２２）、当該外部サービス利用情報を通信部５５を通じて複合機１０に送信する（Ｓ２３）。中継装置５０と複合機１０とは、

ステップＳ２３において、ＸＭＰＰコネクションを通じて外部サービス利用情報を送受信する。ステップＳ２２、Ｓ２３の処理は、中継処理の一例である。

【００５２】

外部サービス利用情報は、複数のアクセスＵＲＬと、各アクセスＵＲＬに対応する複数のサービスＩＤとを含んでいてもよい。また、外部サービス利用情報は、インタフェース定義ファイルに代えて、サービス利用指示を含んでもよい。サービス利用指示は、当該外部サービス利用情報によって利用可能な外部サービスの利用を複合機１０に開始させるための指示である。そして、この場合の外部サービス利用情報は、サービス利用指示によって利用されるサービスに対応するアクセスＵＲＬ及びサービスＩＤを１つずつ含んでいればよい。

【００５３】

次に、複合機１０の制御プログラム３５は、通信部２５を通じて中継装置５０から外部サービス利用情報を受信する（Ｓ２３）。ステップＳ２３において外部サービス利用情報を受信する処理は、第１受信処理の一例である。制御プログラム３５は、通信部２５を通じて中継装置５０から受信した外部サービス利用情報にインタフェース定義ファイルが含まれている、換言すれば、当該外部サービス利用情報にサービス利用指示が含まれていないことに応じて（Ｓ２４：Ｎｏ）、サービス一覧表示画面を表示部２３に表示させる（Ｓ２５）。図８は、サービス一覧表示画面の一例である。図８に示されるサービス一覧表示画面は、サービス利用情報記憶領域３６に記憶されたインタフェース定義ファイル、及び外部サービス利用情報に含まれるインタフェース定義ファイルそれぞれで定義されるサービスアイコンを含む。また、各サービスアイコンには、対応するサービスを特定する情報の一例であるサービスの名称が記述されている。

【００５４】

次に、制御プログラム３５は、サービス一覧表示画面に含まれる複数のサービスアイコンの１つをタップするユーザ操作を操作部２４が受け付けたことに応じて（Ｓ２６：Ｙｅｓ）、対応するサーバ装置７０～９０に通信部２５を通じて接続要求する（Ｓ２７）。具体的には、制御プログラム３５は、ステップＳ２６においてタップされたサービスアイコンに対応するアクセスＵＲＬに、ＨＴＴＰＳ（Ｈｙｐｅｒｔｅｘｔ　Ｔｒａｎｓｆｅｒ　Ｐｒｏｔｏｃｏｌ　Ｓｅｃｕｒｅの略）接続要求する。本実施形態において、サービスＡはサーバ装置７０が提供するサービスの名称であり、サービスＢはサーバ装置８０が提供するサービスの名称であり、サービスＣ及びサービスＤはサーバ装置９０が提供するサービスの名称である。ステップＳ２６においてサービスアイコンをタップする操作は、対応するサービスの利用を開始するサービス利用指示の入力の一例である。

【００５５】

一方、制御プログラム３５は、通信部２５を通じて中継装置５０から受信した外部サービス利用情報にサービス利用指示が含まれている、換言すれば、当該外部サービス利用情報にインタフェース定義ファイルが含まれていないことに応じて（Ｓ２４：Ｙｅｓ）、ステップＳ２５、Ｓ２６の処理をスキップする。そして、制御プログラム３５は、通信部２５を通じてサーバ装置９０にＨＴＴＰＳ接続要求する（Ｓ２７）。

【００５６】

次に、サーバ装置７０、８０は、複合機１０からの接続要求に応じて（Ｓ２７）、ＨＴＴＰＳ通信におけるＳＳＬネゴシエーション処理の一環として、サーバ装置７０、８０のサーバ証明書データ（以下、「特定サーバ証明書データ」と表記する。）を複合機１０に送信する（Ｓ２８）。同様に、サーバ装置９０は、複合機１０からの接続要求に応じて（Ｓ２７）、ＨＴＴＰＳ通信におけるＳＳＬネゴシエーション処理の一環として、サーバ装置９０のサーバ証明書データ（以下、「外部サーバ証明書データ」と表記する。）を複合機１０に送信する（Ｓ２８）。

【００５７】

サーバ証明書データは、サーバ装置７０～９０が信頼できることを証明するために、認証局によって発行され、サーバ装置７０～９０に設定されるものである。本実施形態にお

いて、特定サーバ証明書データは、パブリック認証局によって発行される。一方、外部サーバ証明書データは、パブリック認証局によって発行されてもよいし、プライベート認証局によって発行されてもよい。

【００５８】

サーバ証明書データは、例えば、サーバ公開鍵データ、当該サーバ証明書データを検証するＣＡ証明書データを特定するキー情報、及び署名データを含む。署名データは、例えば、キー情報で特定されるＣＡ証明書データに含まれるＣＡ公開鍵データに対応するＣＡ秘密鍵データでサーバ公開鍵データを暗号化したものである。なお、サーバ証明書データに含まれるキー情報は、第１記憶領域３７、６６及び第２記憶領域３８、６７に記憶されたＣＡ証明書データを一意に特定することができればよく、第１記憶領域３７、６６及び第２記憶領域３８、６７に記憶されたキー情報と厳密に一致していなくてもよい。

【００５９】

次に、複合機１０の制御プログラム３５は、通信部２５を通じてサーバ装置７０～９０からサーバ証明書データを受信したことに応じて（Ｓ２８）、当該サーバ証明証データを検証するための一連の処理（以下、「検証処理」と表記する。）を実行する（Ｓ２９～Ｓ３３）。ステップＳ２８において外部サーバ証明書データを受信する処理は、第２受信処理の一例である。また、ステップＳ２８において特定サーバ証明書データを受信する処理は、第３受信処理の一例である。

【００６０】

制御プログラム３５は、ステップＳ２８において特定サーバ証明書データを受信したことに応じて（Ｓ４１：Ｙｅｓ）、第１記憶領域３７に記憶されたＣＡ証明書データを用いて、当該特定サーバ証明書データを検証（Ｓ４２）し、検証処理を終了する。ステップＳ４２における制御プログラム３５は、特定サーバ証明書データに含まれるキー情報に対応づけられたＣＡ証明書データを第１記憶領域３７から取得する。次に、制御プログラム３５は、取得したＣＡ証明書データに含まれるＣＡ公開鍵データを用いて、特定サーバ証明書データに含まれる署名データを復号する。そして、制御プログラム３５は、特定サーバ証明書データに含まれるサーバ公開鍵データと、署名データを復号して得られる復号公開鍵データとを比較する。ステップＳ４２の処理は、第３検証処理の一例である。

【００６１】

また、制御プログラム３５は、ステップＳ２８において外部サーバ証明書データを受信したことに応じて（Ｓ４１：Ｎｏ）、当該外部サーバ証明書データを検証するためのＣＡ証明書データが第２記憶領域３８に記憶されているか否かを判断する（Ｓ４３）。具体的には、ステップＳ４３における制御プログラム３５は、当該外部サーバ証明書データに含まれるキー情報及び外部サービス利用情報に含まれるサービスＩＤに対応づけられたＣＡ証明書データが第２記憶領域３８に記憶されているか否かを判断する。ステップＳ４３の処理は、判断処理の一例である。

【００６２】

そして、制御プログラム３５は、外部サーバ証明書データを検証するためのＣＡ証明書データが第２記憶領域３８に記憶されていることに応じて（Ｓ４３：Ｙｅｓ）、当該ＣＡ証明書データを用いて外部サーバ証明書データを検証する（Ｓ４４）。外部サーバ証明書データの具体的な検証方法はステップＳ４２と共通であってもよい。ステップＳ４４の処理は、第１検証処理の一例である。また、制御プログラム３５は、ステップＳ４４において検証に用いたＣＡ証明書データに対応づけて第２記憶領域３８に記憶された最終アクセス日時を現在日時に更新して検証処理を終了する（Ｓ４５）。

【００６３】

また、制御プログラム３５は、外部サーバ証明書データを検証するためのＣＡ証明書データが第２記憶領域３８に記憶されていないことに応じて（Ｓ４３：Ｎｏ）、通信部２５を通じて中継装置５０に送信指示情報を送信する（Ｓ４６）。送信指示情報は、外部サーバ証明書データを検証するためのＣＡ証明書データを中継装置５０に送信させるための情報である。送信指示情報は、例えば、外部サーバ証明書データに含まれるキー情報と、外

部サービス利用情報に含まれるサービスＩＤとを含む。

【００６４】

中継装置５０の制御プログラム６５は、通信部５５を通じて複合機１０から送信指示情報を受信したことに応じて（Ｓ３０）、ＣＡ証明書検索処理を実行する（Ｓ３１）。ＣＡ証明書検索処理は、第１記憶領域６６及び第２記憶領域６７に記憶されたＣＡ証明書データのうちから、送信指示情報で特定されるＣＡ証明書データを検索する処理である。図７を参照して、ＣＡ証明書検索処理を詳細に説明する。

【００６５】

まず、制御プログラム６５は、送信指示情報に含まれるキー情報に対応づけられたＣＡ証明書データが第１記憶領域６６に記憶されているか否かを判断する（Ｓ６１）。また、制御プログラム６５は、当該ＣＡ証明書データが第１記憶領域６６に記憶されていないことに応じて（Ｓ６１：Ｎｏ）、送信指示情報に含まれるキー情報及びサービスＩＤに対応づけられたＣＡ証明書データが第２記憶領域６７に記憶されているか否かを判断する（Ｓ６３）。

【００６６】

そして、制御プログラム６５は、当該ＣＡ証明書データが第１記憶領域６６に記憶されていることに応じて（Ｓ６１：Ｙｅｓ）、当該ＣＡ証明書データを第１記憶領域６６から取得する（Ｓ６２）。また、制御プログラム６５は、当該ＣＡ証明書データが第１記憶領域６６に記憶されておらず且つ当該ＣＡ証明書データが第２記憶領域６７に記憶されていることに応じて（Ｓ６３：Ｙｅｓ）、当該ＣＡ証明書データを第２記憶領域６７から取得する（Ｓ６４）。さらに、制御プログラム６５は、当該ＣＡ証明書データが第１記憶領域６６に記憶されておらず且つ当該ＣＡ証明書データが第２記憶領域６７に記憶されていないことに応じて（Ｓ６３：Ｎｏ）、エラー情報を生成する（Ｓ６５）。エラー情報は、送信指示情報で特定されるＣＡ証明書データが中継装置５０に登録されていないことを示す情報である。

【００６７】

そして、制御プログラム６５は、ステップＳ６２において第１記憶領域６６から取得したＣＡ証明書データ、ステップＳ６４において第２記憶領域６７から取得したＣＡ証明書データ、或いはステップＳ６５において生成したエラー情報を、通信部５５を通じて複合機１０に送信する（Ｓ３２）。ステップＳ２２の処理は、送信処理の一例である。

【００６８】

図６に戻って、複合機１０の制御プログラム３５は、通信部２５を通じて中継装置からＣＡ証明書データを受信したことに応じて（Ｓ４７：Ｙｅｓ）、当該ＣＡ証明書データで外部サーバ証明書データを検証する（Ｓ４８）。外部サーバ証明書データの具体的な検証方法はステップＳ４２、Ｓ４４と共通であってもよい。ステップＳ４６～Ｓ４８の処理は、第２検証処理の一例である。

【００６９】

次に、制御プログラム３５は、第２記憶領域３８に記憶されているＣＡ証明書データの数を確認する（Ｓ４９）。そして、制御プログラム３５は、第２記憶領域３８に記憶されているＣＡ証明書データがＮ個であることに応じて（Ｓ４９：Ｙｅｓ）、最も古い最終アクセス日時に対応づけられて第２記憶領域３８に記憶されたキー情報、サービスＩＤ、及びＣＡ証明書データを、送信指示情報に含めたキー情報及びサービスＩＤと、ステップＳ４７において受信したＣＡ証明書データとで上書きし、さらに最終アクセス日時を現在日時に更新して検証処理を終了する（Ｓ５０）。

【００７０】

なお、ステップＳ５０における「上書き」とは、最も古いＣＡ証明書データが記憶されていた第２記憶領域３８のメモリ領域そのものに、新たに受信したＣＡ証明書データを書き込むことに限定されない。例えば、第２記憶領域３８は、ステップＳ４３において検索の対象となるか否かを示すフラグを、各ＣＡ証明書データに対応づけて記憶していてもよい。本実施形態では、検索対象となるＣＡ証明書データに対応づけられたフラグには”Ｏ

Ｎ”が設定され、検索対象から外れるＣＡ証明書データに対応づけられたフラグには”ＯＦＦ”が設定される。そして、制御プログラム３５は、ステップＳ５０において、最も古いＣＡ証明書データに対応するフラグに”ＯＦＦ”を設定し、第２記憶領域３８に新たに記憶させるＣＡ証明書データに対応するフラグに”ＯＦＦ”を設定してもよい。

【００７１】

一方、制御プログラム３５は、第２記憶領域３８に記憶されているＣＡ証明書データがＮ個未満であることに応じて（Ｓ４９：Ｎｏ）、送信指示情報に含めたキー情報及びサービスＩＤと、ステップＳ４７において受信したＣＡ証明書データと、現在日時とを対応づけて第２記憶領域３８に追加して検証処理を終了する（Ｓ５１）。ステップＳ５１における「追加」とは、第２記憶領域３８に既に記憶されているＣＡ証明書データと異なるメモリ領域に、新たに受信したＣＡ証明書データを記憶させることを指す。ステップＳ４９～Ｓ５１の処理は、記憶制御処理の一例である。

【００７２】

一方、制御プログラム３５は、通信部２５を通じて中継装置からエラー情報を受信したことに応じて（Ｓ４７：Ｎｏ）、検索処理を終了する。なお、ステップＳ４６における送信指示情報の送信、ステップＳ４７におけるＣＡ証明書データ或いはエラー情報の受信は、ＸＭＰＰコネクションを通じて行ってもよいし、中継装置５０との間に新たに確立されたＸＭＰＰコネクションとは異なるコネクションを通じて行ってもよい。

【００７３】

制御プログラム３５は、ステップＳ３３において、サーバ証明書データに含まれるサーバ公開鍵データと、署名データを復号して得られる復号公開鍵データとが一致したことに応じて、検証が成功したと判断する。一方、制御プログラム３５は、ステップＳ３３において、サーバ証明書データに含まれるサーバ公開鍵データと、署名データを復号して得られる復号公開鍵データとが一致しないことに応じて、検証が失敗したと判断する。そして、制御プログラム３５は、サーバ証明書データの検証が成功したことに応じて（Ｓ３４：Ｙｅｓ）、ステップＳ２４、Ｓ２６で取得したサービス利用指示で示されるサービスの利用を開始する（Ｓ３５）。一方、制御プログラム３５は、サーバ証明書データの検証が失敗したことに応じて（Ｓ３４：Ｎｏ）、ステップＳ３５をスキップする。

【００７４】

ステップＳ３５における制御プログラム３５は、例えば、利用するサービスに用いる秘密鍵データをサーバ公開鍵データで暗号化し、暗号化した秘密鍵データを通信部２５を通じて当該サービスを提供するサーバ装置７０～９０に送信する。暗号化された秘密鍵データを複合機１０から受信したサーバ装置７０～９０は、当該暗号化された秘密鍵データを、サーバ公開鍵データに対応するサーバ秘密鍵データで復号する。そして、複合機１０及びサーバ装置７０～９０は、送信するデータ或いは情報を秘密鍵データで暗号化し、受信したデータ或いは情報を秘密鍵データで復号する。

【００７５】

［本実施形態の作用効果］

上記の実施形態によれば、必要なＣＡ証明書データがデータ記憶領域３２Ｂに記憶されている場合は当該ＣＡ証明書データで第１検証処理（Ｓ４３：Ｙｅｓ→Ｓ４４）を実行し、必要なＣＡ証明書データがデータ記憶領域３２Ｂに記憶されていない場合は当該ＣＡ証明書データを中継装置５０から取得して第２検証処理（Ｓ４４：Ｎｏ→Ｓ４６～Ｓ４８）を実行することができる。その結果、ＣＡ証明書データによってデータ記憶領域３２Ｂのメモリ領域が圧迫されることなく、且つ多数のサービスを利用することができる。

【００７６】

また、上記の実施形態によれば、データ記憶領域３２Ｂを第１記憶領域３７及び第２記憶領域３８に分割することによって、特定サーバ証明書データを検証するためのＣＡ証明書データと、外部サーバ証明書データを検証するためのＣＡ証明書データとを区別して記憶することができる。その結果、通信部２５を通じて中継装置５０から受信したＣＡ証明書データで、プリインストールされたＣＡ証明書データが上書きされることを防止できる

。また、中継装置５０から取得したＣＡ証明書データで特定サーバ証明書データが検証されることを防止できる。

【００７７】

また、上記の実施形態によれば、Ｎ個のＣＡ証明書データを記憶するメモリ領域を第２記憶領域３８として確保すればよい。その結果、ＣＡ証明書データを記憶させるために記憶部３２の記憶容量を大きくする必要がない。また、第１記憶領域３７をＲＯＭで構成することにより、特定サーバ証明書データを検証するためのＣＡ証明書データを常に保持することができる。一方、第２記憶領域３８をＲＡＭで構成することにより、中継装置５０から取得したＣＡ証明書データの記憶領域を安価に確保することができる。さらに、ステップＳ５０において、最も古い最終アクセス日時に対応づけられたＣＡ証明書データから順に上書きされるので、ＣＡ証明書データを中継装置５０から取得する頻度を低下させることができる。

【００７８】

また、上記の実施形態によれば、ステップＳ４６においてサービスＩＤを含めた送信指示情報を中継装置５０に送信することにより、外部サービス利用情報に含まれるサービスＩＤに対応づけられたＣＡ証明書データを中継装置５０から取得するので、サーバ装置９０になりすました他の機器と複合機１０とが通信することを抑制できる。

【００７９】

なお、第１記憶領域３７、６６及び第２記憶領域３８、６７のデータ構造は、図２及び図３の例に限定されず、例えばキー情報が省略されていてもよい。そして、制御プログラム３５、６５は、ステップＳ４２、Ｓ４３、Ｓ６１、Ｓ６３において、各記憶領域３７、３８、６６、６７に記憶されたＣＡ証明書データを解析することによって、キー情報に対応するＣＡ証明書データを特定してもよい。また、制御プログラム３５は、ステップＳ４３において、キー情報に対応するＣＡ証明書データが第１記憶領域３７に記憶されているか否かをさらに判断してもよい。

【００８０】

また、各実施形態の複合機１０及び中継装置５０において、記憶部３２、６２のプログラム記憶領域３２Ａ、６２Ａに記憶された各種プログラムがＣＰＵ３１、６１によって実行されることによって、本発明の制御部が実行する各処理が実現される例を説明した。しかしながら、制御部の構成はこれに限定されず、その一部又は全部を集積回路（ＩＣ（Ｉｎｔｅｇｒａｔｅｄ　Ｃｉｒｃｕｉｔの略）とも言う。）等のハードウェアで実現してもよい。

【００８１】

さらに、本発明は、複合機１０或いは中継装置５０として実現できるだけでなく、複合機１０或いは中継装置５０に処理を実行させるプログラムとして実現してもよい。そして、当該プログラムは、ｎｏｎ－ｔｒａｎｓｉｔｏｒｙな記録媒体に記録されて提供されてもよい。ｎｏｎ－ｔｒａｎｓｉｔｏｒｙな記録媒体は、ＣＤ－ＲＯＭ、ＤＶＤ－ＲＯＭ等の他、通信ネットワーク１０２を介して複合機１０或いは中継装置５０に接続可能なサーバ装置に搭載された記憶部を含んでもよい。そして、サーバ装置の記憶部に記憶されたプログラムは、当該プログラムを示す情報或いは信号として、インターネット等の通信ネットワーク１０２を介して配信されてもよい。

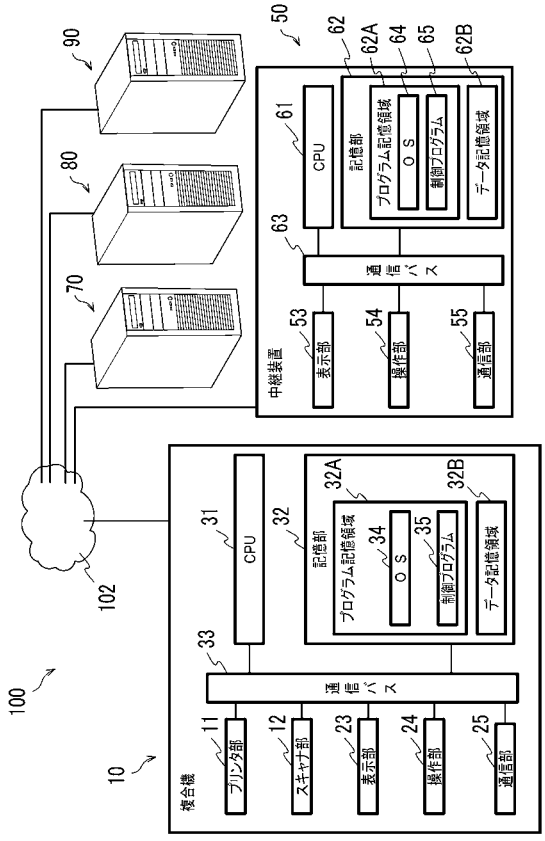
【符号の説明】

【００８２】

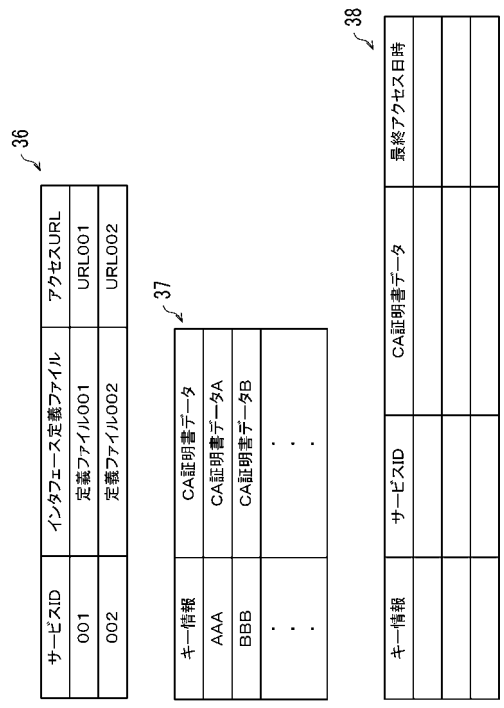
１０・・・複合機
２５，５５・・・通信部
３１，６１・・・ＣＰＵ
３２，６２・・・記憶部
３５，６５・・・制御プログラム
５０・・・中継装置
７０，８０，９０・・・サーバ装置

１００・・・サービス実行システム

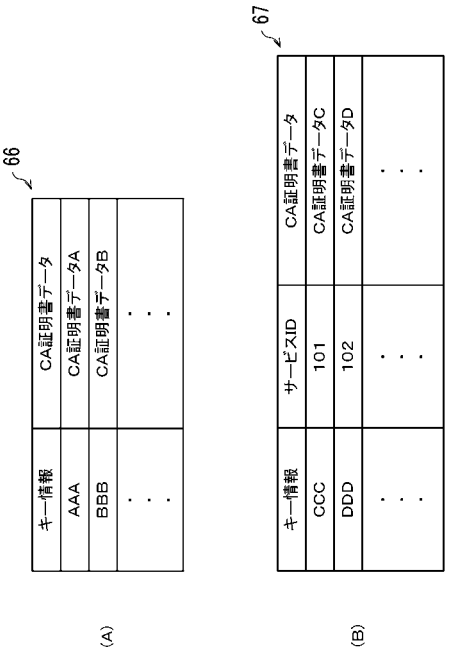
【図１】



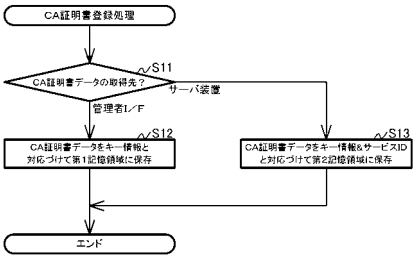
【図２】



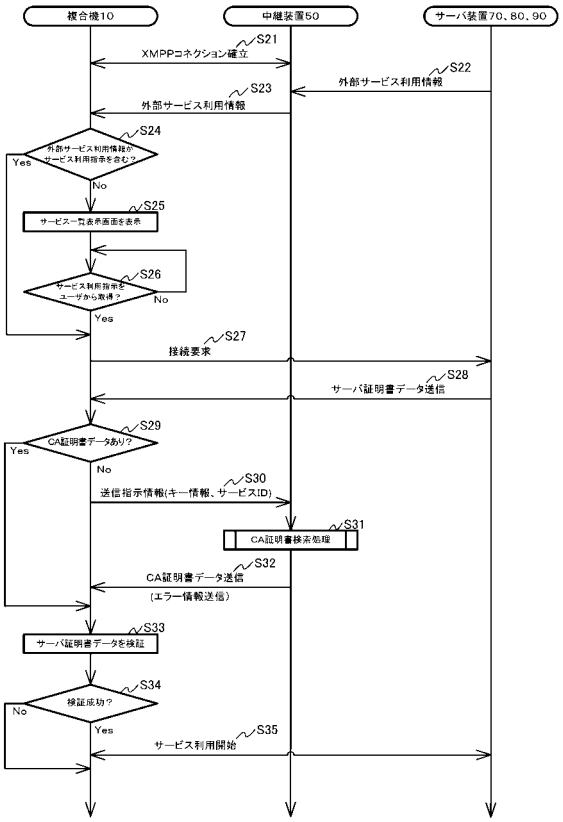
【図３】


66
CA証明書データ
キー情報
AAA
CA証明書データA
BBB
CA証明書データB
(A)
67
CA証明書データ
サービスID
101
CA証明書データC
102
CA証明書データD
キー情報
CCC
DDD
(B)

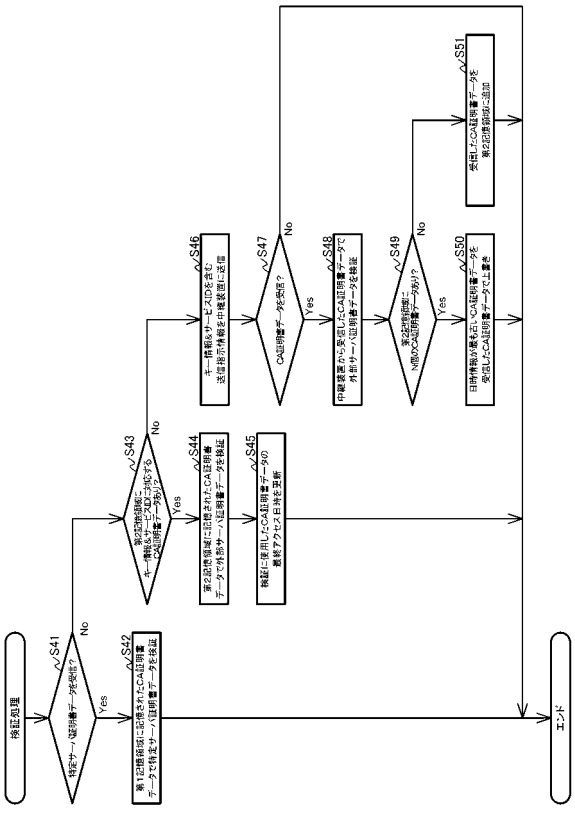
【図４】


CA証明書登録処理
S11
CA証明書データの取得先？
サーバ装置
管理者I／F
S12
CA証明書データをキー情報と対応づけて第1記憶領域に保存
S13
CA証明書データをキー情報&サービスIDと対応づけて第2記憶領域に保存
エンド

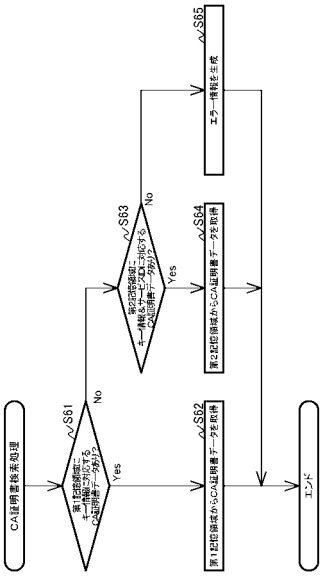
【図５】


複合機10
中継装置50
サーバ装置70、80、90
S21
XMPPコネクション確立
S22
外部サービス利用情報
S23
外部サービス利用情報
S24
外部サービス利用情報がサービス利用指示を含む？
Yes
No
S25
サービス一覧表示画面を表示
S26
サービス利用指示をユーザから取得？
No
Yes
S27
接続要求
S28
サーバ証明書データ送信
S29
CA証明書データあり？
Yes
No
S30
送信指示情報(キー情報、サービスID)
S31
CA証明書検索処理
S32
CA証明書データ送信
(エラー情報送信)
S33
サーバ証明書データを検証
S34
検証成功？
No
Yes
S35
サービス利用開始

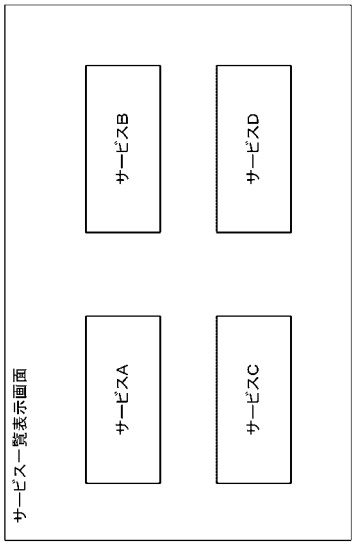
【図６】


検証処理
S41
検証サーバ証明書データを保持？
No
Yes
S42
第1記憶領域に記憶されたCA証明書データで検証
S43
受信証明書にキー情報&サービスIDに対応するCA証明書データあり？
No
Yes
S44
第2記憶領域に記憶されたCA証明書データで外部サーバ証明書データを検証
S45
検証に使用したCA証明書データの最終アクセス日時を更新
S46
キー情報とサービスIDを含む送信指示情報を中継装置に送信
S47
CA証明書データを保持？
No
Yes
S48
中継装置から受信したCA証明書データで外部サーバ証明書データを検証
S49
第2記憶領域にNEWのCA証明書データあり？
No
Yes
S50
当該情報処理装置において受信したCA証明書データで上書き
S51
受信したCA証明書データを第2記憶領域に追加
エンド

【図７】


CA証明書検索処理
S61
第1記憶領域に
十分な証明書データがある
CA証明書データがない
No
Yes
S62
第1記憶領域からCA証明書データを取得
S63
第2記憶領域に
十分な証明書データがある
CA証明書データがない
No
Yes
S64
第2記憶領域からCA証明書データを取得
S65
エラー情報を生成
エンド

【図８】


サービス一覧表示画面
サービスA
サービスB
サービスC
サービスD

フロントページの続き

(51)Int.Cl.	FI	テーマコード（参考）
	Ｇ０６Ｆ 3/12 Ｋ	

Ｆターム(参考) 5C062 AA02 AA05 AA13 AA29 AA35 AB02 AB17 AB22 AB38 AB42
AC22 AC35 AC43 AE07 AE14 AF01 AF02 AF12 AF14 BC03
5J104 EA05 NA37 PA07