(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第6882080号
(P6882080)

(45)発行日　令和3年6月2日(2021.6.2)　(24)登録日　令和3年5月10日(2021.5.10)

(51)Int.Cl.		F I		
G06F 21/32	(2013.01)	G06F	21/32	
G06F 21/44	(2013.01)	G06F	21/44	
G06F 21/60	(2013.01)	G06F	21/60	380
G06F 3/12	(2006.01)	G06F	3/12	322
G09C 1/00	(2006.01)	G06F	3/12	338

請求項の数 13　(全 22 頁)　最終頁に続く

(21)出願番号　特願2017-108255 (P2017-108255)
(22)出願日　平成29年5月31日 (2017.5.31)
(65)公開番号　特開2018-205906 (P2018-205906A)
(43)公開日　平成30年12月27日 (2018.12.27)
審査請求日　令和2年5月28日 (2020.5.28)

(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　100126240
弁理士　阿部　琢磨
(74)代理人　100124442
弁理士　黒岩　創吾
(72)発明者　太田　峻輔
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

審査官　桜井　茂行

最終頁に続く

(54)【発明の名称】画像処理装置、方法、プログラム及びシステム

(57)【特許請求の範囲】
【請求項１】
生体認証のための認証モジュールと、該認証モジュールにより認証処理を行う際に必要なユーザーの生体情報および秘密鍵を関連付けて格納する耐タンパー性を備える記憶手段と、を有する携帯端末と通信できる通信機能を備える画像処理装置であって、
サービス提供システムで発行された検証用データを受信した場合に、前記携帯端末に対して、該検証用データを送信する第１送信手段と、
前記携帯端末の有する前記認証モジュールによる前記ユーザーの認証処理の成功に応じて、前記記憶手段に格納された前記秘密鍵と前記検証用データとを用いて生成される署名データを、前記携帯端末から受信する第１受信手段と、
前記サービス提供システムと連携する機器認証システムに対して、機器認証のための要求を送信する第２送信手段と、
前記機器認証システムで発行された認証トークンを受信する第２受信手段と、
前記署名データと前記認証トークンとを、前記サービス提供システムに対して送信する第３送信手段と、
を有し、
前記サービス提供システムにおいて、前記サービス提供システムに登録されている前記秘密鍵に対応する公開鍵による前記署名データの検証、および、前記機器認証システムと連携した前記認証トークンの検証に従って、前記サービス提供システムにより前記画像処理装置に対してサービスが提供されることを特徴とする画像処理装置。

【請求項２】
前記サービス提供システムでは、サービスの提供先として、ユーザー識別情報とデバイス識別情報が管理されており、
前記サービス提供システムに登録されている前記秘密鍵に対応する公開鍵により前記署名データが検証され、かつ、前記機器認証システムに対して前記認証トークンの検証を要求して前記画像処理装置の識別情報が得られた場合に、前記携帯端末で生体認証されたユーザーに対応するユーザー識別情報および、前記機器認証システムから得られた前記画像処理装置の識別情報に紐付けて管理されるサービスが前記サービス提供システムにより前記画像処理装置に対して提供されることを特徴とする請求項１に記載の画像処理装置。
【請求項３】
前記第３送信手段は、前記署名データをアサーション情報として前記サービス提供システムに対して送信し、
さらに、前記認証トークンは、前記アサーション情報の拡張領域に設定されることを特徴とする請求項１または２に記載の画像処理装置。
【請求項４】
前記第２送信手段は、前記サービス提供システムからの機器認証の指示に応じて、前記機器認証システムに対して機器認証のための要求を送信することを特徴とする請求項１乃至３のいずれか１項に記載の画像処理装置。
【請求項５】
前記携帯端末では、前記認証モジュールに対する前記ユーザーの生体情報の登録に際して、前記秘密鍵と前記公開鍵が作成され、
前記サービス提供システムで前記ユーザーのユーザー識別情報に対応づけて登録されるよう前記携帯端末から前記公開鍵が前記サービス提供システムに対して送信されることを特徴とする請求項１乃至４のいずれか１項に記載の画像処理装置。
【請求項６】
前記第１送信手段は、前記画像処理装置での前記ユーザーの操作に従い、携帯端末で認証処理を行うことが指定された場合に、前記携帯端末に対して、検証用データ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項に記載の画像処理装置。
【請求項７】
前記サービス提供システムは、前記サービスとして、前記ユーザーが前記サービス提供システムに登録したデータを前記画像処理装置に対して提供し、前記画像処理装置が該提供されたデータを用いたプリント処理を実行することを特徴とする請求項１乃至６のいずれか１項に記載の画像処理装置。
【請求項８】
前記サービス提供システムは、前記サービスとして、前記ユーザーが前記サービス提供システムに登録したデータを前記画像処理装置に対して提供し、前記画像処理装置が該提供されたデータを用いた３次元造形物の造形処理を実行することを特徴とする請求項１乃至６のいずれか１項に記載の画像処理装置。
【請求項９】
前記生体情報は、前記ユーザーの指紋、静脈、虹彩、声紋、及び顔画像の少なくともいずれかに係る情報であることを特徴とする請求項１乃至８のいずれか１項に記載の画像処理装置。
【請求項１０】
生体認証のための認証モジュールと、該認証モジュールにより認証処理を行う際に必要なユーザーの生体情報および秘密鍵を関連付けて格納する耐タンパー性を備える記憶手段と、を有する携帯端末と通信できる通信機能を備える画像処理装置における方法であって、
サービス提供システムで発行された検証用データを受信した場合に、前記携帯端末に対して、該検証用データを送信する第１送信ステップと、
前記携帯端末の有する前記認証モジュールによる前記ユーザーの認証処理の成功に応じ

て、前記記憶手段に格納された前記秘密鍵と前記検証用データとを用いて生成される署名データを、前記携帯端末から受信する第１受信ステップと、
前記サービス提供システムと連携する機器認証システムに対して、機器認証のための要求を送信する第２送信ステップと、
前記機器認証システムで発行された認証トークンを受信する第２受信ステップと、
前記署名データと前記認証トークンとを、前記サービス提供システムに対して送信する第３送信ステップと、
を有し、
前記サービス提供システムにおいて、前記サービス提供システムに登録されている前記秘密鍵に対応する公開鍵による前記署名データの検証、および、前記機器認証システムと連携した前記認証トークンの検証に従って、前記サービス提供システムにより前記画像処理装置に対してサービスが提供されることを特徴とする方法。
【請求項１１】
請求項１乃至９のいずれか１項に記載の各手段としてコンピューターを機能させるためのプログラム。
【請求項１２】
生体認証のための認証モジュールと、該認証モジュールにより認証処理を行う際に必要なユーザーの生体情報および秘密鍵を関連付けて格納する耐タンパー性を備える記憶手段と、を有する携帯端末と、
前記携帯端末と通信できる通信機能を備える画像処理装置と、
前記秘密鍵に対応する公開鍵が登録されたサービス提供システムと、
画像処理装置の認証のための認証トークンを発行する機器認証システムと、を含むシステムであって、
前記画像処理装置における、前記サービス提供システムで発行された検証用データを受信した場合に、前記携帯端末に対して、該検証用データを送信する第１送信手段と、
前記携帯端末における、前記ユーザーの前記認証モジュールによる認証処理の成功に応じて、前記記憶手段に格納された前記秘密鍵と前記検証用データとを用いて署名データを生成する生成手段と、
前記画像処理装置における、前記携帯端末から、前記生成される署名データを受信する第１受信手段と、
前記画像処理装置における、前記機器認証システムに対して、機器認証のための要求を送信する第２送信手段と、
前記機器認証システムにおける、前記画像処理装置のために、認証トークンを発行する発行手段と、
前記画像処理装置における、前記機器認証システムから、前記発行された認証トークンを受信する第２受信手段と、
前記画像処理装置における、前記署名データと前記認証トークンとを、前記サービス提供システムに対して送信する第３送信手段と、
前記サービス提供システムにおける、前記サービス提供システムに登録されている前記秘密鍵に対応する公開鍵による前記署名データの検証、および、前記機器認証システムと連携した前記認証トークンの検証に従って、前記画像処理装置に対してサービスを提供する提供手段と、
を有することを特徴とするシステム。
【請求項１３】
生体認証のための認証モジュールと、該認証モジュールにより認証処理を行う際に必要なユーザーの生体情報および秘密鍵を関連付けて格納する耐タンパー性を備える記憶手段と、を有する携帯端末と、
前記携帯端末と通信できる通信機能を備える画像処理装置と、
前記秘密鍵に対応する公開鍵が登録されたサービス提供システムと、
画像処理装置の認証のための認証トークンを発行する機器認証システムと、を含むシス

テムにおける方法であって、
前記画像処理装置における、前記サービス提供システムで発行された検証用データを受信した場合に、前記携帯端末に対して、該検証用データを送信する第１送信ステップと、
前記携帯端末における、前記ユーザーの前記認証モジュールによる認証処理の成功に応じて、前記記憶手段に格納された前記秘密鍵と前記検証用データとを用いて署名データを生成する生成ステップと、
前記画像処理装置における、前記携帯端末から、前記生成される署名データを受信する第１受信ステップと、
前記画像処理装置における、前記機器認証システムに対して、機器認証のための要求を送信する第２送信ステップと、
前記機器認証システムにおける、前記画像処理装置のために、認証トークンを発行する発行ステップと、
前記画像処理装置における、前記機器認証システムから、前記発行された認証トークンを受信する第２受信手ステップと、
前記画像処理装置における、前記署名データと前記認証トークンとを、前記サービス提供システムに対して送信する第３送信ステップと、
前記サービス提供システムにおける、前記サービス提供システムに登録されている前記秘密鍵に対応する公開鍵による前記署名データの検証、および、前記機器認証システムと連携した前記認証トークンの検証に従って、前記画像処理装置に対してサービスを提供する提供ステップと、
を有することを特徴とする方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、画像処理装置の利用時において、生体認証されたユーザーが利用可能な機器を制御する手法に関する。
【背景技術】
【０００２】
近年、生体認証を含む新たな認証システムとして、ＦＩＤＯ（Ｆａｓｔ　ＩｄｅｎｔｉｔｙＯｎｌｉｎｅの略）が注目されている。
【０００３】
生体認証で用いられる指紋や静脈といった生体情報は、外部に情報が流出してしまった場合に、ＩＤ／パスワード認証におけるパスワードと異なり情報を書き換えることができないため、情報漏洩が致命的になる。これに対して、ＦＩＤＯでは認証作業を、インターネットを経由してサーバー上で行うのではなく、ユーザーの手元にある端末上で行うため、生体情報がネットワーク上に流れることがなく、情報漏洩のリスクが少ないと言える。このような、生体情報がネットワーク上に流出する懸念が低い、特殊な認証な仕組みにおいては、生体情報は認証を行う端末内のセキュアな領域で厳密に管理される。
【０００４】
従来から、オフィスや公共の場で、セキュリティを担保するために、認証を行った上でネットワークサービスを利用できる機器上で、ユーザーに対してサービスを提供するシステムが存在する。例えば、特許文献１には、ユーザーが画像処理装置を操作する際に、ＩＣカードから読み取った情報を用いて認証サーバーで認証させ、認証が成功したユーザーＩＤに対応する印刷ジョブをプリントサーバーからその画像処理装置にダウンロードするシステムがある。さらに、特許文献１では、ＩＣカード認証の代わり、指紋、指静脈など生体情報を用いて認証サーバーで認証させる点も開示している。
【０００５】
このようなシステムには、前述のＦＩＤＯのような、よりセキュアな生体認証を含む特殊な仕組みを採用することが望まれる。
【先行技術文献】

【特許文献】
【０００６】
【特許文献１】特開２０１３－１９１２３６号公報
【発明の概要】
【発明が解決しようとする課題】
【０００７】
ここで、ネットワークサービスをユーザーに提供するために設置された画像処理装置を含むシステムでの認証に、前述のＦＩＤＯのような特殊な認証の仕組みを適用した場合を想定する。このような仕組みでは、仕様上、ユーザーは認証が成功した場合であればどこに設置された画像処理装置でもサービス提供を受けられることになる。例えば、提供サービスによって出力されるデータが機密などである場合には、提供する画像処理装置を、設置場所や機器性能などの条件に応じて制限したい場合がある。
【０００８】
そこで、本発明は、前述のＦＩＤＯの仕組みを含む生体認証を用いたシステムにおいて、サービス提供する画像処理装置を制御し得る手法を提供する。
【課題を解決するための手段】
【０００９】
本発明における画像処理装置は、生体認証のための認証モジュールと、該認証モジュールにより認証処理を行う際に必要なユーザーの生体情報および秘密鍵を関連付けて格納する耐タンパー性を備える記憶手段と、を有する携帯端末と通信できる通信機能を備える画像処理装置であって、サービス提供システムで発行された検証用データを受信した場合に、前記携帯端末に対して、該検証用データを送信する第１送信手段と、前記携帯端末の有する前記認証モジュールによる前記ユーザーの認証処理の成功に応じて、前記記憶手段に格納された前記秘密鍵と前記検証用データとを用いて生成される署名データを、前記携帯端末から受信する第１受信手段と、前記サービス提供システムと連携する機器認証システムに対して、機器認証のための要求を送信する第２送信手段と、前記機器認証システムで発行された認証トークンを受信する第２受信手段と、前記署名データと前記認証トークンとを、前記サービス提供システムに対して送信する第３送信手段と、を有し、前記サービス提供システムにおいて、前記サービス提供システムに登録されている前記秘密鍵に対応する公開鍵による前記署名データの検証、および、前記機器認証システムと連携した前記認証トークンの検証に従って、前記サービス提供システムにより前記画像処理装置に対してサービスが提供されることを特徴とする。
【発明の効果】
【００１０】
本発明によれば、前述の生体認証を用いたシステムを拡張し、サービス提供する画像処理装置を制御することができる。
【図面の簡単な説明】
【００１１】
【図１】本発明におけるシステム構成の例を示す図
【図２】本発明における各装置のハードウェア構成の例を示す図
【図３】本発明におけるソフトウェアによる機能ブロックの例を示す図
【図４】実施例１における全体シーケンス図
【図５】実施例１における認証機能を呼び出す際のパラメータ
【図６】実施例１における携帯端末での生体認証処理に関するフローチャート
【図７】実施例１における画像処理装置で表示される画面の例
【図８】応用例１おける交換タイミングの予測処理に関するフローチャート
【図９】携帯端末上に表示される生体認証の要求画面
【発明を実施するための形態】
【００１２】
以下、本発明を実施するための最良の形態について図面を用いて説明する。

【００１３】
（実施例１）
図１は、本発明におけるシステム構成の例を示す図である。
【００１４】
本システムは、画像処理装置１０１と、印刷サービスサーバー１０３、機器認証サービスサーバー１０４、テナント管理サービスサーバー１０５、および機器管理サービスサーバー１０６から構成されている。また、画像処理装置１０１は、携帯端末１０２ともネットワーク１１２を介して接続される。ネットワーク１１１は、例えば、インターネット等のＬＡＮ、ＷＡＮ、電話回線、専用デジタル回線、ＡＴＭやフレームリレー回線、ケーブルテレビ回線、データ放送用無線回線等のいずれであり。または、これらの組み合わせにより実現される、いわゆる通信ネットワークである。ネットワーク１１２は、ＬＡＮなどの上述のネットワーク回線に加え、例えばＢｌｕｅＴｏｏｔｈ（登録商標）等の近距離通信なども含む。
【００１５】
なお、画像処理装置１０１としては、プリンターや、複写機、デジタル健康機器（血圧測定器やルームランナーなど）、ＡＴＭ、（３次元造形物をプリント（造形処理）する）３Ｄプリンターといった、ネットワークからデータを取得して画像データや物理媒体として出力処理する機器であれば、本発明が適用可能である。従って、印刷サービスサーバー１０３についても、出力対象となるデータを画像処理装置に供給できるサービスを提供するような様々なサービス提供システムに代替され、本発明に適用することが可能である。また、印刷サービスサーバー１０３は、マルチユーザーのドキュメントデータを蓄積して他の装置からの要求に応じて提供できる画像処理装置により構築することも可能である。
【００１６】
本発明では、以下、プリントデータを画像処理装置に提供し、画像処理装置で印刷出力するシステムの例について詳しく説明する。
【００１７】
なお、携帯端末１０２は、ノート型のＰＣや携帯端末（スマートフォンやタブレット）、スマートウォッチやスマートグラスなどのウェアラブル端末などのことである。
【００１８】
機器認証サービスサーバー１０４は、機器認証システムを構築するサーバーであって、機器管理サービスサーバー１０６に登録されている画像処理装置などを一意に特定するために、認証トークンを用いた機器認証を行うために用意されたサーバーである。機器認証サービスサーバー１０４は、印刷サービスサーバー１０３に対して適切な画像処理装置を保証するために、印刷サービスサーバー１０３と連携している。
【００１９】
なお、テナント管理サービスサーバー１０５は実施例２で利用されるサーバーであり、その詳細については後述する。
【００２０】
図２は、本発明を構成する各装置のハードウェアの構成例を示す図である。
【００２１】
図２（ａ）は、印刷サービスサーバー１０３、機器認証サービスサーバー１０４、テナント管理サービスサーバー１０５、および機器管理サービスサーバー１０６を構築する情報処理装置のハードウェア構成図である。これらは、一般的なパーソナルコンピューター（ＰＣ）と同様なハードウェアで構成することもできる。
【００２２】
ＣＰＵ２０１は、ＲＯＭ２０３内に記憶されたプログラムや、ハードディスク２１０からＲＡＭ２０２にロードされたＯＳ（オペレーションシステム）やアプリケーション等のプログラムを実行する。すなわち、ＣＰＵ２０１が、読み取り可能な記憶媒体に格納された該プログラムを実行することにより、後述する各フローチャートの処理を実行する各処理部として機能する。ＲＡＭ２０２は、ＣＰＵ２０１のメインメモリであり、ワークエリ

ア等として機能する。キーボードコントローラ２０４は、キーボード２０８や図示しないポインティングデバイス（マウス、タッチパッド、タッチパネル、トラックボールなど）からの操作入力を制御する。ディスプレイコントローラ２０５は、ディスプレイ２０９の表示を制御する。ディスクコントローラ２０６は、各種データを記憶するハードディスク（ＨＤ）やフレキシブルディスク（ＦＤ）等の外部メモリ２１０へのデータアクセスを制御する。ネットワークＩ／Ｆ２０７はネットワークに接続されて、ネットワークに接続された他の機器との通信制御処理を実行する。

【００２３】

印刷サービスサーバー１０３、機器認証サービスサーバー１０４、テナント管理サービスサーバー１０５、および機器管理サービスサーバー１０６は、後述する各サーバーが管理すべき情報を自装置が備える外部メモリ２１０や、ネットワーク上のストレージといった記憶装置に格納する。

【００２４】

図２（ｂ）は、画像処理装置１０１のハードウェア構成図である。ここでは、画像処理装置１０１として、プリンターの構成を例示している。

【００２５】

ＣＰＵ２２１はＲＯＭ２２３に格納されているプログラム（後述する各処理を実現するプログラムも含む）を備え、内部バス２３１を介して各デバイスを総括的に制御する。ＲＡＭ２２２は、ＣＰＵ２２１のメモリやワークエリアとして機能する。ネットワークＩ／Ｆ２２５は、外部のネットワーク機器と片方向または双方向にデータをやり取りする。近接通信Ｉ／Ｆ２２６はＢｌｕｅＴｏｏｔｈなどの近接通信用のネットワークＩ／Ｆであり、携帯端末１０２等と通信し、データのやり取りを行うための通信機能となる構成である。デバイス制御２２７は印刷部２２８を制御する。ＣＰＵ２２１は、ＲＡＭ２２２やＲＯＭ２２３と共にプログラムの実行処理をおこなうとともに、記憶装置２２４等の記録媒体に画像データを記録する処理を行う。記憶装置２２４は外部記憶装置として機能する。入出力装置２３０は画像処理装置１０１における入出力を担う複数の構成を示す。具体的には、ユーザーからの入力（ボタン入力など）を受け付け、該入力に対応する信号を入出力Ｉ／Ｆ２２９によって前述した各処理部へ伝える。ほかにも、ユーザーに対して必要な情報を提供したり、ユーザー操作を受付けたりするための表示装置（タッチパネルなど）も入出力装置２３０に含まれる。入出力装置２３０は、ネットワーク上からサービス提供装置から提供されたデータを表示出力（通知）することができる。

【００２６】

さらに、原稿を読み取り、入力として電子データを受付けるためのスキャン装置も入出力装置２３０に含まれてよい。３Ｄプリンターなどでは、印刷部２２８として、３次元造形物を造形するためのステージやヘッドなどが実装されることになる。

【００２７】

図２（ｃ）は、携帯端末１０２のハードウェア構成図である。

【００２８】

ＣＰＵ２４２は、ＲＯＭ２４４に格納されているプログラム（後述する各処理を実現するプログラムも含む）を備え、内部バス２４１を介して各デバイスを総括的に制御する。ＲＡＭ２４３は、ＣＰＵ２４２のメモリやワークエリアとして機能する。ネットワークＩ／Ｆ２４７は、ＷｉＦｉなどを用いた、外部のネットワーク機器と片方向または双方向にデータをやり取りする。ＣＰＵ２４２は、ＲＡＭ２４３やＲＯＭ２４４と共にプログラムの実行処理をおこなうとともに、記憶装置２４５等の記録媒体にデータを記録する処理を行う。記憶装置２２４は、外部記憶装置として機能し、ＳＤカードなどで構成される。

【００２９】

Ｔｒｕｓｔｅｄ Ｐｌａｔｆｏｒｍ Ｍｏｄｕｌｅ（ＴＰＭ）２４６は、機密情報を処理したり格納したりする目的で、格納したデータを外部から読み取られることを防ぐ耐タンパー性を備えた記憶手段である。耐タンパー性を備えた記憶手段の具体例としては、業界標準であるＴＰＭ２．０（もしくはそれ以上のバージョン）の仕様に準拠したものを想

定している。本発明では、生体認証に用いる生体情報自体、またはその生体情報の特徴量や、その生体情報に対応する秘密鍵などがＴＰＭ２４６に格納される。なお、後述では、センサーで取得できた生体情報を示す信号の特徴量についても生体情報と呼ぶ場合がある。生体情報センサー２４８は、ユーザーの生体情報を読取るセンサーであり、例えばユーザーの指紋、虹彩、静脈、声紋、顔画像の情報を読み取り信号に変換する。専用の読み取り機や、カメラ、マイクなどを用いて実現される。

【００３０】

タッチパネル２４９は、表示と入力の２つの機能を備えており、アプリケーションの画面やキーボードなどを表示したりするとともに、ユーザーが画面に手や専用のペンで圧力を加えることにより、触れられた画面位置情報を外部へ情報信号として出力する。出力された信号情報をアプリケーションが利用することで、ユーザーはタッチパネル２０６を通じてアプリケーションを操作することができる。生体情報センサー２４８とタッチパネル２４９とは、重ねて実装することが可能で、タッチパネル２４９への操作により利用者の指紋情報を読み取るといった構成も可能である。

【００３１】

近接通信Ｉ／Ｆ２５０は、ＭＦＰ１０１のそれと同様に、ＮＦＣやＢｌｕｅＴｏｏｔｈなどの近接通信用の通信方式に対応したＩ／Ｆであり、本実施例においては、ＭＦＰ１０１とこのＩ／Ｆを介して通信を行う。

【００３２】

図３は、本発明の各装置が有するソフトウェアによって実現される機能モジュールの構成を示している。これらの構成は、大きく分けて、「印刷サービスサーバー１０３によるクライアントＰＣ１０７からの印刷指示受付」、「印刷サービスサーバー１０３に対する携帯端末１０２からの認証情報の登録処理」、および「印刷サービスサーバー１０３に対する画像処理装置からの印刷要求」の３つの処理を実現する。以下では、図３の各構成の説明も含めて、これら３つの処理について説明する。

【００３３】

なお、図３で示す印刷サービスサーバー１０３、機器認証サービスサーバー１０４、テナント管理サービスサーバー１０５の各部は、ＲＯＭ２０３にプログラムとして格納され、ＲＡＭ２０２上でＣＰＵ２０１によって実行される。また、画像処理装置１０１の各部は、ＲＯＭ２２３にプログラムとして格納され、ＲＡＭ２２３上でＣＰＵ２２１によって実行される。同様に、携帯端末１０２の各部は、ＲＯＭ２４４にプログラムとして格納され、ＲＡＭ２４３上でＣＰＵ２４２によって実行される。

【００３４】

≪印刷サービスサーバー１０３に対するクライアントＰＣ１０７からの印刷指示受付≫

まず、ユーザーはクライアントＰＣ１０６などを用いて、印刷サービスサーバー１０３の印刷サービスにログインして、印刷サービスサーバー１０３に対する印刷指示として、印刷対象のドキュメントを選択する。この時、クライアントＰＣ１０７のユーザーは、後述する機器管理サービスサーバー１０６が保持するデバイスデータの中から、選択したドキュメントの印刷を可能とする画像処理装置を選択指定することもできる。選択指定がされない場合は、いずれの画像処理装置でも印刷可能と判断しても良い。

【００３５】

印刷サービスサーバー１０３の印刷指示受付部３１１は、印刷対象のドキュメントのデータと、印刷を可能とする画像処理装置を示すデバイス情報とを含む印刷指示を受け付ける。印刷データ管理部３１８は、印刷指示に含まれるそれらデータを記憶装置に、以下の表Ａに示す形式で格納する。ドキュメントのデータとしては、ドキュメント名などの属性情報と、データファイル、ファイル保存場所を示す情報などが含まれる。

【００３６】

表Ａにおいて、ドキュメント名は、ユーザーが印刷指示として選択したドキュメントの名称を表し、後述する印刷フローにおいて、画像処理装置１０１上に表示される名称となる。ドキュメントデータは、印刷するドキュメントのバイナリデータとなる。ユーザー識

別情報（ＩＤ）は、印刷を指示したユーザーを一意に表すＩＤとなる。このユーザーＩＤは、印刷サービスにログインした後に、印刷指示が行われるため、特定できる情報である。印刷可能デバイスＩＤは、ユーザーが印刷を指示した際に、指定したデバイスを識別するデバイス識別情報となる。印刷時にデバイスを指定しなかった場合には、いずれのデバイスでも印刷可能であることを示す情報として、例えば「＊」などの特別なフラグを設定する。表Ａにより、印刷サービスサーバー１０３は、サービスの提供先として、印刷可能ユーザー並びに印刷可能機器を管理することができる。

【００３７】

【表１】

表Ａ

ドキュメント名	ドキュメントデータ	ユーザーＩＤ	印刷可能デバイスＩＤ
ａａａ．ｄｏｃ	０１０１００１０１０１０１０１０…	ｕｓｅｒ００１	ｄｅｖ００１
ｂｂｂ．ｐｐｔ	００１０１００１０１０１００１１１…	ｕｓｅｒ００３	ｄｅｖ００２，ｄｅｖ００３
ｃｃｃ．ｔｘｔ	０１１１１１０１０１１０１１１０１１１…	ｕｓｅｒ００４	＊
：	：	：	

【００３８】

なお、クライアントＰＣ１０７を利用するユーザーは、事前に印刷サービスサーバー１０３に対して、ＩＤ／Ｐａｓｓｗｏｒｄのように、一般的な方法で、印刷サービスを利用するためのユーザーを作成している。また、印刷指示時にも、該ユーザーで印刷サービスにログインした上で、印刷指示を行う。なお、本実施例においては、事前に作成されたＩＤ／Ｐａｓｓｗｏｒｄの組をレガシークレデンシャルと表記する。レガシークレデンシャルはユーザー管理部３１２が記憶装置に格納し、管理する。

【００３９】

機器管理サービスサーバー１０６のデバイス登録要求受信部３９１は、画像処理装置１０１のデバイス登録要求部３５５からデバイス登録要求を受信する。該登録要求に含まれるデバイス情報はデバイス情報管理部３９２によって記憶装置上で管理される。管理される情報としては、デバイスＩＤやその製品名称、設置場所等、ユーザーが印刷指示をする際に印刷可能としたい装置の判別が可能な情報である。

【００４０】

印刷サービスサーバー１０３が、後に印刷されるドキュメントデータがクライアントＰＣ１０７から登録される際には、クライアントＰＣ１０７のユーザーに、印刷を行う画像処理装置を指定させてもよい。そのために、印刷サービスサーバー１０３は、クライアントＰＣ１０７に対して、デバイスリストを表示させる。そのために、印刷サービスサーバー１０３は、機器管理サービスサーバー１０６のデバイス情報管理部３９２にデバイス情報を要求する。印刷サービスサーバー１０３は、デバイス情報に基づくデバイスリストをクライアントＰＣに提供することになる。

【００４１】

なお、クライアントＰＣ１０７から印刷サービスサーバー１０３に対する画像処理装置の処理対象に成り得るデータの登録や画像処理装置の選択は、クライアントＰＣ１０７のウェブブラウザを用いて行われる。従って、画像処理装置の処理対象に成り得るデータの登録や画像処理装置の選択は携帯端末１０２から行われてもよい。

【００４２】

≪印刷サービスサーバー１０３に対する携帯端末１０２からの認証情報の登録処理≫

携帯端末１０２の認証情報登録要求部３３１は、印刷サービスにアクセスし、認証情報の登録処理を開始する。ここで、認証情報とは、携帯端末１０２内で行われる生体認証の成功に応じて、携帯端末１０２の認証されたユーザーを、印刷サービスサーバー１０３においても認証するために必要となる情報である。詳しくは後述するが、認証情報には、公開鍵や認証情報ＩＤなどが含まれる。一方で、この認証情報はネットワーク上を流れるため、生体認証に用いるようなユーザー固有の生体情報やそれに対応して生成される秘密鍵は含まれない。認証情報登録要求部３３１は、印刷サービスがウェブブラウザなどによってアクセスされるアプリケーションであった場合は、ｊａｖａ　ｓｃｒｉｐｔによって実現されても良いし、印刷サービス用のアプリケーションがある場合にはその中で実現されても良い。

【００４３】

携帯端末１０２のユーザーの指示に応じて本登録処理が開始されると、印刷サービスサーバー１０３の印刷サービスは、携帯端末１０２にレガシークレデンシャルの入力を要求する。ユーザーは、携帯端末のウェブブラウザやアプリを介して、印刷サービスにログインするためのレガシークレデンシャルを入力する。レガシークレデンシャルが正しく入力され、その認証が成功した場合、そのユーザーについて、印刷サービスサーバー１０３における、レガシークレデンシャルとは異なる認証情報の登録処理が可能となる。

【００４４】

携帯端末１０２の生体情報入力部３３２は、生体情報センサー２４８を介して、ユーザーから指紋情報などの生体情報の入力を受付ける。生体情報管理部３３３は、入力された生体情報と、該生体情報を識別するための生体情報ＩＤを紐付けて、ＴＰＭ２４６に格納する。ここで、本発明では、生体情報センサー２４８やＴＰＭ２４６といったハードウェアを用いて、携帯端末１０２内の生体認証を制御するための認証モジュールとして、生体情報管理部３３３、認証要求受信部３３４、生体認証部３３５が実装される。この認証モジュールは、オーセンティケータ（Ａｕｔｈｅｎｔｉｃａｔｏｒ）とも呼ばれる。認証情報登録要求部３３１など、その他のモジュールも認証モジュールの一部として実現することも可能である。

【００４５】

生体認証部３３５は、生体情報が入力された後、当該生体情報に対応する公開鍵、秘密鍵のペアを作成する。生体情報管理部３３３は、作成された秘密鍵と、それに対応する生体情報を識別するための生体情報ＩＤと、レガシークレデンシャルと、印刷サービスサーバー１０３を示すようなＩＤなど、を紐付けてＴＰＭ２４６に格納して管理する。ここで格納される情報の例を、表Ｂで説明する。

【００４６】

【表２】

表Ｂ

認証情報ＩＤ	サービスＩＤ	秘密鍵	生体情報ＩＤ
４０７ｃ－８８４１－７９ｄ	ｐｒｉｎｔ．ｃｏｍ	１ｆａｅａ２ｄａ－ａ２６９－４ｆａ７－８１２ａ－５０９４７０ｄ９ａ０ｃｂ	ｄ４９３ａ７４４
：	：	：	

【００４７】

表Ｂの認証情報ＩＤ列は、各登録情報に対して生体情報管理部３３３で一意に割り当てられる識別情報（ＩＤ）である。サービスＩＤ列は、ユーザーが連携するシステム（本実施例においては、印刷サービスサーバー１０６）を示すＩＤで、該システムのトップレベルドメイン、セカンドレベルドメインの情報を格納する。秘密鍵列は、秘密鍵を格納する。生体情報ＩＤ列にはユーザーから入力された指紋などの情報に１対１に対応する特徴量情報（生体情報）に対応するＩＤを格納する。

【００４８】

前述した公開鍵は、認証情報登録要求部３３１によって、認証情報として、表Ｂで対応づけて管理される認証情報ＩＤとともに、印刷サービスサーバー１０３に送信される。印刷サービスサーバー１０３の認証情報登録部３１４は、受信した認証情報を、記憶装置にレガシークレデンシャルに紐付けて保存する。ここで保存される情報例を表Ｃに示す。

【００４９】

【表３】

表Ｃ

認証情報ＩＤ	公開鍵	ユーザーＩＤ
４０７ｃ－８８４１－７９ｄ	ＡＣ４３Ｃ５ＦＢ－ＢＦＡ２－４８Ｄ１－Ａ７１Ｂ－ＦＢ０４ＡＣＤＡ３４７Ａ	ｕｓｅｒ００１
４ｃ０４－４２８ｂ－ａ７ａ２	８１４３ＣＡ９Ｆ－３５Ｃ９－４３３３－９４８Ｆ－ＢＦＣＥ６６Ａ７４３１０	ｕｓｅｒ００２
：	：	

【００５０】

認証情報ＩＤ列は、表Ｂにおける認証情報ＩＤ列の値が格納される。公開鍵列は表Ｂにおける秘密鍵とペアになる公開鍵を格納する。即ち、表Ｂで認証情報ＩＤが同一の秘密鍵と公開鍵について、表Ｂの秘密鍵で暗号化したものは表Ｃの公開鍵で復号化できるということである。ここでは、レガシークレデンシャルとの紐付けのために、ユーザーＩＤを利用して管理している。

【００５１】

≪画像処理装置での、印刷サービスサーバー１０３に対する要求処理及び出力処理≫

クライアントＰＣ１０７から印刷サービスサーバー１０３に対して予め印刷指示されたドキュメントを、ユーザーが任意の画像処理装置１０１を操作することで、画像処理装置１０１で印刷サービスサーバー１０３から取得して、出力する処理について説明する。この処理については、図３に加え、図４のシーケンス図を用いて説明を行う。

【００５２】

Ｓ４０１では、ユーザーの操作に応じて、画像処理装置１０１は印刷サービスサーバー１０３の印刷サービスのＵＲＬに対してアクセスする。この際に、画像処理装置１０１のドキュメント要求部３５１は、印刷サービスサーバー１０３のドキュメント要求受信部３１５に対して、ドキュメント要求を発行してもよい。このタイミングでは、まだ画像処理装置１０１を操作するユーザーの印刷サービスサーバー１０３の印刷サービスに対する認証は行われていない。

【００５３】

Ｓ４０２では、ユーザー検証部３１６は、印刷サービスへのアクセス、またはドキュメント要求の受信に応じて、図５（ａ）で示す認証用パラメータ５０１を作成する。Ｓ４０３では、ドキュメント要求受信部３１５は、Ｓ４０１のレスポンスとして、Ｓ４０２で作成した認証用パラメータ５０１を返却する。

【００５４】

ここで、認証用パラメータ５０１は、アサーションチャレンジ５０２とアサーション拡張領域５０３から構成される。アサーションチャレンジ５０２はチャレンジレスポンス認証をするために利用する検証用データである。アサーション拡張領域５０３は、印刷サービスサーバー１０３が携帯端末１０２での生体認証に関する処理を制御するため拡張パラメータが格納される。

【００５５】

Ｓ４０４では、画像処理装置１０１の認証要求部３５３は、Ｓ４０３で返却された認証用パラメータと共に、ＮＦＣやＢｌｕｅＴｏｏｔｈなどを用いて構築されるネットワーク１１２を介して接続された携帯端末１０２の認証要求受信部３３４に対して生体認証要求

を行う。ユーザーは、画像処理装置１０１の表示装置を操作して、印刷サービスサーバー１０３に携帯端末１０２で生体認証を行うことを指定することができる。この場合には、画像処理装置１０１は認証用パラメータを携帯端末１０２に転送する。

【００５６】

Ｓ４０５では、生体認証部３３５は、生体認証要求の受信に応じて、生体認証処理の制御を行う。生体認証処理の詳細について、図６を用いて、説明する。図６で示すフローチャートは、携帯端末１０２のＣＰＵ２４２がプログラムを実行することで実現される処理を説明するためのものである。

【００５７】

Ｓ６１１では、生体認証部３３５は、図９に示すような生体認証のための生体情報の入力をユーザーに促すための要求画面を表示する。本実施例においては生体情報として指紋情報を扱っているが、虹彩や顔など別の情報を用いても良い。Ｓ６１２では、生体情報入力部３３２は、生体情報センサー２４８を介して、ユーザーからの指紋情報の入力を受け付け、指紋情報の特徴量を取得する。この特徴量は、指紋のパターン・虹彩の模様・静脈の形など個人に対してユニークであるものを、ユニーク性を損なわないような値に変換したものである。Ｓ６１３では、生体認証部３３５は、生体情報センサー２４８で受け付けた生体情報による認証処理の結果を確認する。ユーザーから入力された生体情報が登録済みであり、認証処理に成功した場合には、Ｓ６１４に進む。

【００５８】

Ｓ６１４では、生体認証部３３５は、Ｓ６１３の認証処理に成功した生体情報に対応する秘密鍵を、表Ｂを参照することで取得し、その秘密鍵を用いた暗号化処理を実行することで、アサーションチャレンジ５０２から署名データを作成する。さらに、生体認証部３３５は、図５（ｂ）に示すアサーション（Ａｓｓｅｒｔｉｏｎ）情報５２１を生成する。

【００５９】

ここで、アサーション情報５２１は、認証情報５２２と署名５２３とクライアントデータ５２４から構成される。認証情報５２２には、Ｓ６１４で用いた秘密鍵に紐付けて表Ｂで管理される認証情報ＩＤが設定される。署名５２３には、Ｓ６１４で作成された署名が設定される。クライアントデータ５２４は、図５（ｃ）に示すような構成をとる。

【００６０】

さらに、クライアントデータ５２４の構成例を説明する。クライアントデータ５２４は、アサーションチャレンジ５３１、拡張領域５３２、およびハッシュアルゴリズム５３３から構成される。アサーションチャレンジ５３１は、Ｓ４０２にて印刷サービスサーバー１０３より送られたアサーションチャレンジ５０２と同じものである。拡張領域５３２には、任意の情報が設定される。ハッシュアルゴリズム５３３は、署名５２３を作成したときのハッシュ化アルゴリズムを示す情報であり、例えばＳ２５６（＝ＳＨＡ－２５６）、Ｓ３８４（＝ＳＨＡ－３８４）などの文字列が設定される。

【００６１】

図４のシーケンスの説明に戻る。

【００６２】

Ｓ４０６で、認証要求受信部３３４は、図６で示す処理により作成されたアサーション情報５２１を、Ｓ４０４の応答として、画像処理装置１０１に返却する。

【００６３】

Ｓ４０７では、画像処理装置１０１の機器認証要求部３５２は、機器認証サービスサーバー１０４の機器認証要求受信部３７１に対して、機器認証要求を送信する。この時、画像処理装置１０１は、画像処理装置内のセキュアな領域に保存された、画像処理装置の識別情報であるデバイスＩＤとＰａｓｓｗｏｒｄを併せて送信する。

【００６４】

Ｓ４０８では、機器認証部３７３は、機器認証要求の受信に応じて、Ｓ４０７で送信されたデバイスＩＤ／Ｐａｓｓｗｏｒｄの組合せが登録済みの組合せと一致するか否かを検証し、登録済みであった場合には、認証トークンを発行する。発行された認証トークンは

、機器認証情報管理部３７５が、デバイスＩＤと紐付けて、記憶装置に保存する。Ｓ４０９では、機器認証要求受信部３７１は、Ｓ４０７のレスポンスとして発行された認証トークンを返却する。

【００６５】

Ｓ４１０では、画像処理装置１０１のドキュメント要求部３５１は、印刷サービスサーバー１０３のドキュメント要求受信部３１５に対して、アサーション情報５２１と認証トークンとを送信する。この際に、本実施例においては、認証トークンの印刷サービスサーバー１０３に対する送信方法の一例として、ドキュメント要求部３５１がアサーション情報５２１に含まれるクライアントデータ５２４内の拡張領域５３２に対して認証トークンを設定している。拡張領域５３２には下記のようなＪｓｏｎ等のスキーマに従って情報が設定される。

｛‘ｄｅｖｉｃｅｔｏｋｅｎ’：‘００ｆｄｅ７ｅｄ－０６ｂｃ－４ｄ０ｆ－８７７３－ｃｂ３９９ｅ７３ｅｂ６ｃ’｝

【００６６】

Ｓ４１１では、印刷サービスサーバー１０３のユーザー検証部３１６は、受信したアサーション情報５２１に含まれる認証情報ＩＤを元に、表Ｃより公開鍵情報を取得し、公開鍵をもちいてアサーション情報に含まれる署名５２３を検証する。署名５２３を取得した公開鍵で復号して得られたデータと、Ｓ４０３で認証用パラメータ内に設定したアサーションチャレンジ５０２とを照合（一致判定）することで、検証を行う。ここで正しく検証できた場合には、携帯端末１０２で生体認証に成功したユーザーが、印刷サービスサーバー１０３においても登録済みユーザーとして認証に成功したとみなし、Ｓ４１２に進む。ユーザー検証部３１６でのアサーション情報の検証に失敗した場合には、ドキュメント要求受信部３１５は認証失敗を画像処理装置１０１に応答する（不図示）。

【００６７】

Ｓ４１２では、機器検証要求部３１７は、画像処理装置１０１から受信した認証トークンを含む、認証トークンの検証要求を機器認証サービスサーバー１０４の機器検証要求受信部３７２に送信する。

【００６８】

Ｓ４１３では、機器検証部３７４が、機器認証情報管理部３７２により管理された発行済みの認証トークンのうち、機器検証要求受信部３７２を介して受信した認証トークンと一致するものがあるか否かを判断する。判断の結果、一致する認証トークンが存在する場合には正しく検証できたものとして、Ｓ４１４にて、機器検証要求受信部３７２は、機器認証情報管理部３７２がその認証トークンと紐付けて管理していたデバイスＩＤを、検証の成功とともに印刷サービスサーバー１０３に対して返却する。一方で、機器検証要求受信部３７２は、判断の結果、一致する認証トークンが存在しない場合には、機器の検証に失敗した旨の通知を印刷サービスサーバー１０３に対して返却する（不図示）。印刷サービスサーバー１０３は、機器の検証に失敗した場合には、Ｓ４１０の応答として、画像処理装置１０１に対して印刷できるドキュメントがない旨の通知を返却してもよい。

【００６９】

Ｓ４１５では、ドキュメント要求受信部３１５は、検証に成功したアサーション情報５２１に含まれる認証情報ＩＤを元に表ＣよりユーザーＩＤを特定する。さらに、印刷データ管理部３１８は、表Ａを参照し、特定されたユーザーＩＤのドキュメントであり、かつ、Ｓ４１４で返却されたデバイスＩＤでの印刷が可能なドキュメントのデータを抽出する。抽出されたデータに基づき、印刷データ管理部３１８は、印刷可能なドキュメントの識別情報（ドキュメントＩＤ）を含むドキュメントリストを作成する。印刷データ管理部３１８は、表Ａで、ユーザーＩＤ、およびデバイスＩＤに一致するレコードが存在しないときは、空のドキュメントリストを作成する。

【００７０】

Ｓ４１６では、ドキュメント要求受信部３１５は、Ｓ４１５にて作成したドキュメントリストを、画像処理装置１０１のドキュメント要求部３５１に返却する。なお、Ｓ４１５

で、表ＡにユーザーＩＤに紐づくドキュメントは存在するが、Ｓ４１３で取得されたデバイスＩＤで印刷可能なドキュメントがない場合には、そのことを示す情報を返却されるレスポンスに加えても良い。

【００７１】

Ｓ４１７では、リスト表示部３５４は、Ｓ４１６にて返却されたドキュメントリストを、画像処理装置１０１の表示装置に表示する。ドキュメント選択部３５５は、表示されたリストを介した、ユーザーの選択を受け付ける。図７を用いて、表示の例を説明する。

【００７２】

図７（ａ）では、画像処理装置１０１の表示装置上に返却されたドキュメントリスト（ドキュメント７０１、７０２、７０３を含む）が表示される。携帯端末１０２で生体認証されたユーザーは、これら一覧の中から、印刷したいドキュメントを選択し、印刷ボタン（７０４）を押下する。

【００７３】

図７（ｂ）は、Ｓ４１６にて返却されたレスポンスに、携帯端末１０２で生体認証されたユーザーに紐づくドキュメントがない場合に表示される画面の例を示す。一方で、図７（ｃ）は、携帯端末１０２で生体認証されたユーザーが操作している画像処理装置１０１を用いて印刷可能なドキュメントがない場合に表示される画面の例を示す。

【００７４】

Ｓ４１８では、ドキュメント要求部３５１は、ドキュメント選択部３５５を介して受け付けたユーザーの選択に対応するドキュメントＩＤを含めた取得要求を印刷サービスサーバー１０３に対して送信する。Ｓ４１９では、ドキュメント要求受信部３１５は、Ｓ４１８で指定されたドキュメントＩＤに基づき、ドキュメントのデータを表Ａから取得し、画像処理装置１０１に返却する。Ｓ４２０では、画像処理装置１０１では、Ｓ４１９で受信したデータの印刷処理を実行する。

【００７５】

なお、画像処理装置１０１に生体認証センサー、ＴＰＭが含まれており、予め、表Ｂ、Ｃで示すような情報の登録が画像処理装置１０１と印刷サービスサーバー１０３との間で行われていたとする。その場合には、携帯端末１０２を利用することなく、生体認証処理を画像処理装置１０１で実行してもよい。この場合には、Ｓ４０４～Ｓ４０６の処理が省略され、その代わりに、画像処理装置１０１で、図６で示す処理が実行された上で、アサーション情報が作成されることになる。

【００７６】

以上、実施例１に記載の機器制御システムを実現することで、生体認証と機器認証を組み合わせた機器制御システムの実現が可能となる。

【００７７】

（実施例２）

本発明に係る第２の実施形態について説明する。以下、実施例１と異なる点について、とくに詳細に説明する。

【００７８】

実施例１においては、クライアントＰＣ１０７からの印刷指示の際に、印刷可能なデバイスを指示していた。しかしながら、例えば会社内の機密ドキュメントを印刷する際には、多くの場合において、情報漏えい防止の観点から、社内の指定画像処理装置でのみ印刷可能とするケースが多いと考える。そういった場合でも、毎回印刷をするたびに、画像処理装置を指定することはユーザービリティの観点から、非常に非効率であるといえる。そこで、本実施例においては、画像処理装置、およびユーザーのテナント管理機能を追加し、印刷指示を行うユーザーと同じテナントに所属する画像処理装置であれば、印刷可能とするようにする。

【００７９】

本実施例のために、図３で示すテナント管理サービスサーバー１０５を追加する。これは、ユーザー、および画像処理装置がどのテナントに所属するかといった情報を管理する

。
【００８０】
テナント管理サービスサーバー１０５のテナント情報管理部３８２が保持するデータ例を、表を用いて説明する。
【００８１】
表Ｄは、テナントとユーザー間の関係を管理するためのユーザー管理テーブルの一例である。テナントＩＤ列は組織を一意に表すためのＩＤである。また、ユーザーＩＤ列は、前述したレガシークレデンシャルのユーザーＩＤに対応する情報である。下表の場合、ｕｓｅｒ００１，およびｕｓｅｒ００２は、テナントＡに所属し、ｕｓｅｒ００３は、テナントＢに所属するということを表す。
【００８２】
【表４】

表Ｄ：ユーザー管理テーブル

テナントＩＤ	ユーザーＩＤ
テナントＡ	ｕｓｅｒ００１
テナントＡ	ｕｓｅｒ００２
テナントＢ	ｕｓｅｒ００３
・・・	・・・

【００８３】
表Ｅは、テナントと画像処理装置との間の関係を管理するためのデバイス管理テーブルの一例である。下表の場合、デバイスＩＤが“ｄｅｖ００１”の画像処理装置はテナントＡに所属し、デバイスＩＤが“ｄｅｖ００２”、および“ｄｅｖ００３”の画像処理装置は、テナントＢに所属するということを表す。
【００８４】
【表５】

表Ｅ：デバイス管理テーブル

テナントＩＤ	デバイスＩＤ
テナントＡ	ｄｅｖ００１
テナントＢ	ｄｅｖ００２
テナントＢ	ｄｅｖ００３
・・・	・・・

【００８５】
クライアントＰＣ１０７を用いてユーザーが印刷指示を発行した場合、実施例１で説明したとおり、印刷指示受付部３１１がその指示を受信する。その後、印刷指示をしたユーザーが所属するテナント情報、および同テナントに所属する画像処理装置の情報を、テナント情報要求部３１９を介して、テナント情報要求受信部３８１に要求する。テナント情報要求受信部３８１が受信した要求は、テナント情報処理部３８３を介して、デバイス管理テーブルより指示ユーザーが所属するテナントＩＤが求める。
【００８６】
ついで、そのテナントＩＤに所属するデバイスＩＤをデバイス管理テーブルより取得し、これらの情報がテナント情報要求部３１９に返却される。これらの情報は、実施例１と同様に印刷データ管理部３１８が記憶装置に保存する。
【００８７】
本実施例では、前述の図４のＳ４１５で、ドキュメント要求受信部３１５は、検証に成

功したアサーション情報５２１に含まれる認証情報ＩＤを元に表Ｃよりユーザーの特定する。また、Ｓ４１４で返却されたデバイスＩＤが特定されたユーザーＩＤが所属するテナントＩＤで示すテナントに属するものかをチェックする。そのテナントに属するものであることが核にされた場合には、表Ａを参照し、特定されたユーザーＩＤに対応するドキュメントのデータを抽出する。印刷データ管理部３１８は、抽出されたデータに基づき、印刷可能なドキュメントの識別情報（ドキュメントＩＤ）を含むドキュメントリストを作成する。

【００８８】

（応用例１）

実施例１、および２では、画像処理装置について機器認証が必要であった。しかしながら、利用ユーザーによっては、印刷可能な機器を指定しない場合も数多く存在すると考えられる。このような場合、毎回、機器認証サービスサーバー１０４への認証要求を行っていては、画像処理装置１０１の処理負荷が高まるという課題が存在する。

【００８９】

そこで、本実施例では、印刷指示をしたユーザーに紐づくドキュメントのうち、印刷デバイスが指定されているドキュメントが存在する場合にのみ、画像処理装置１０１が機器認証サービスサーバー１０４への機器認証の要求を行うようにする。

【００９０】

図８は、本応用例におけるシーケンスを示す。なお図４で示した処理と同様の処理については説明を割愛する。

【００９１】

Ｓ８０１では、画像処理装置１０１のドキュメント要求部３５１は、Ｓ４０６の結果得られたアサーション情報を、印刷サービスサーバー１０３に送信する。実施例１では、機器認証サービスサーバー１０４から得た認証トークンを、図５（ｃ）に示した拡張領域５３２に設定したが、本応用例では、図５（ｄ）に示すように拡張領域にデータが設定されていないクライアントデータ５２４を含むアサーション情報が、印刷サービスサーバー１０３に対して送信される。

【００９２】

印刷サービスサーバー１０３にでは、図４のＳ４１１の処理の後に、Ｓ８０２で、ドキュメント要求受信部３１５は、表Ａを参照し、Ｓ４１１での検証の結果特定されたユーザーＩＤに紐づくドキュメントのデータを検索する。表Ａで、検索されたデータの中で、印刷可能なデバイスが指定されているドキュメントのデータが存在した場合にはＳ８０３～Ｓ８１２の処理が実行され、存在しなかった場合にはＳ８１３の処理が実行される。

【００９３】

Ｓ８０３では、印刷サービスサーバー１０３のドキュメント要求受信部３１５が、画像処理装置１０１に対して、Ｓ８０１のレスポンスとして、機器認証を指示する。

【００９４】

Ｓ８０４では、機器認証の指示に応答して、画像処理装置１０１が機器認証サービスサーバー１０４に対して機器認証の要求を行う。Ｓ８０４乃至Ｓ８０６は、図４で述べたＳ４０７乃至Ｓ４０９と同じであるため、説明を割愛する。

【００９５】

Ｓ８０７では、Ｓ４０６にて返却されたアサーション情報データにＳ８０６で返却された認証トークンを追加し、印刷サービスサーバー１０３に送信する。この際の送信されるアサーション情報データに含まれるクライアントデータは、図５（ｃ）で述べた拡張領域に認証トークンが設定されたものとなる。

【００９６】

Ｓ８０８乃至Ｓ８１２は、図４で述べたＳ４１１乃至Ｓ４１５と同じであるため、説明を割愛する。

【００９７】

Ｓ８１３では、ドキュメント要求受信部３１５は、表Ａの中からＳ４１１での検証の結

果特定されたユーザーＩＤに紐づくドキュメントのデータを用いたドキュメントリストを作成する。

【００９８】

Ｓ４１６以降の処理は、図４で前述した通りであるため、ここでは説明を割愛する。

【００９９】

以上、応用例１によれば、生体認証されたユーザーの印刷対象のドキュメントが機器認証を必要とする場合にのみ、画像処理装置１０１が機器認証サービスサーバー１０４に対して機器認証の要求を行うことになる。従って、本システムに対する負荷を軽減する事が可能となる。

【０１００】

（応用例２）

ここまで説明してきた各実施例では、画像処理装置のデバイスＩＤ／Ｐａｓｓｏｗｒｄによるデバイス登録を前提に厳密な機器認証を行っていた。本応用例では、画像処理装置の位置情報によって、出力に利用できる機器の制限を行う例について説明する。

【０１０１】

本応用例では、画像処理装置１０１の設置場所を示す位置情報、または画像処理装置１０１と生体認証のために接続された携帯端末１０２で取得した位置情報をアサーション情報に含めて、画像処理装置１０１から印刷サービスサーバー１０３に送信する。印刷サービスサーバー１０３は、位置情報に基づき、携帯端末１０２で生体認証されたユーザーが、該画像処理装置１０１で印刷可能であるドキュメントのデータを特定する。

【０１０２】

具体的には、アサーション情報を送信する際に、図５（ｃ）で説明したクライアントデータ５２４内の拡張領域５３２に、上述した認証トークに代えて、下記に示すような位置情報などの情報を設定する。たとえは、下記例では、ｇｅｏｉｎｆｏキー内に、緯度（Ｌａｔｉｔｕｄｅ）情報と、経度（Ｌｏｎｇｉｔｕｄｅ）情報を設定している。

｛‘ｇｅｏｉｎｆｏ’：｛‘Ｌａｔｉｔｕｄｅ’：５７．６４９１１，‘Ｌｏｎｇｉｔｕｄｅ’：１０．４０７４４｝｝

【０１０３】

印刷サービスサーバー１０４は、Ｓ４１６で、位置情報でおおよそ特定される画像処理装置で印刷可能なドキュメントのドキュメントＩＤのみドキュメントリストに含めるようにする。

【０１０４】

（応用例３）

実施例１、２，応用例１，２では、印刷サービスを例として挙げた。本発明によれば、前述の印刷処理に代えて、ネットワーク上のサービス提供装置から取得されたリストから選択したデータをＳ４１９で取得して、画像処理装置が、画面出力や３次元造形物の印刷出力などを行うシステムも同様に実現できる。

【０１０５】

また、本発明によれば、ネットワーク上のサービス提供装置から取得されたストレージサービス（ＵＲＬやフォルダなど）のリストの中からユーザーの選択に従い、画像処理装置に入力されたデータ（スキャンデータ、撮影画像など）を選択された先に出力してもよい。

【０１０６】

例えば、画像処理装置１０１は、Ｓ４１７のタイミングで、スキャンされたデータをいずれのストレージサービスに保存するかを画像処理装置１０１の表示装置上の表示から選択する。この場合、印刷サービスサーバー１０３の代わりに、サービス提供装置として、スキャンサービスサーバー（不図示）を配置する。このストレージサービスの選択において利用されるユーザーが利用可能なサービスを含むリストは、ストレージサービスから画像処理装置１０１に対して提供される。ストレージサービスは、上述の実施例と同様に、アサーション情報の署名を検証することで、ユーザーＩＤを特定する。なお、ストレージ

サービス例としては、ｅｖｅｒｎｏｔｅや、ｄｒｏｐｂｏｘなどが挙げられる。

【０１０７】

このスキャンサービスサーバーは、図４のＳ４１１にてアサーション情報検証をし、ユーザーを特定した際に、該ユーザーが事前に連携設定をしていた、ストレージサービス一覧を作成する。ここで作成されたストレージサービス一覧は、それらのログイン画面へのＵＲＬなどを含み、下記に示すような構成となる。

｛‘ｓｔｏｒａｇｅｌｉｓｔ’：｛‘ｅｖｅｒｎｏｔｅ’：‘ｈｔｔｐ：／／ｅｖｅｒｎｏｔｅ．ｃｏｍ／ｌｏｇｉｎ’｝，｛‘ｄｒｏｐｂｏｘ’：‘ｈｔｔｐ：／／ｄｒｏｐｂｏｘ．ｃｏｍ／ｌｏｇｉｎ’｝｝

【０１０８】

このストレージサービス一覧を、印刷可能ドキュメントリストの代わりにＳ４１６にて返却し、Ｓ４１７にてストレージサービスに表示する。ユーザーは、表示されたストレージサービス一覧の中から、スキャンデータを格納したいサービスを選択し、ログイン作業を実施することで、スキャンサービスサーバーによる選択されたストレージサービスへのスキャンデータの保存が実行される。

【０１０９】

（他の実施例）

本発明は、上述した実施形態（実施例１、２、応用例１，２，３）を適宜組み合わせることにより構成された装置あるいはシステムやその方法も含まれるものとする。

【０１１０】

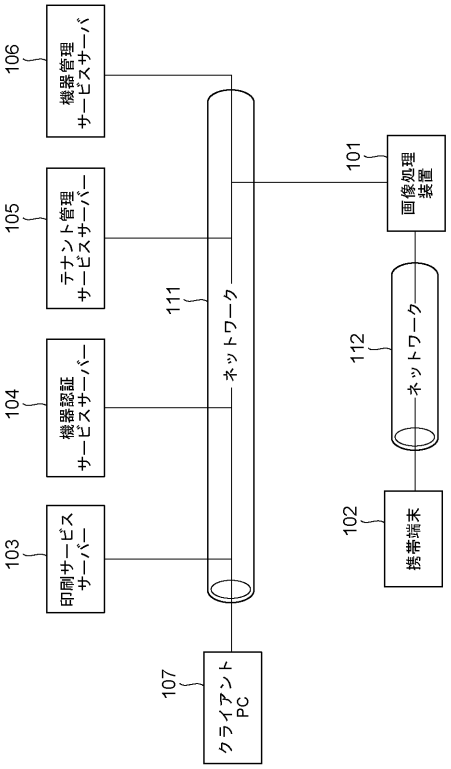
ここで、本発明は、上述した実施形態の機能を実現する１以上のソフトウェア（プログラム）を実行する主体となる装置あるいはシステムである。また、その装置あるいはシステムで実行される上述した実施形態を実現するための方法も本発明の一つである。また、そのプログラムは、ネットワーク又は各種記憶媒体を介してシステム或いは装置に供給され、そのシステム或いは装置の１以上のコンピューター（ＣＰＵやＭＰＵ等）によりそのプログラムが読み出され、実行される。つまり、本発明の一つとして、さらにそのプログラム自体、あるいは該プログラムを格納したコンピューターにより読み取り可能な各種記憶媒体も含むものとする。また、上述した実施形態の機能を実現する回路（例えば、ＡＳＩＣ）によっても、本発明は実現可能である。

【符号の説明】

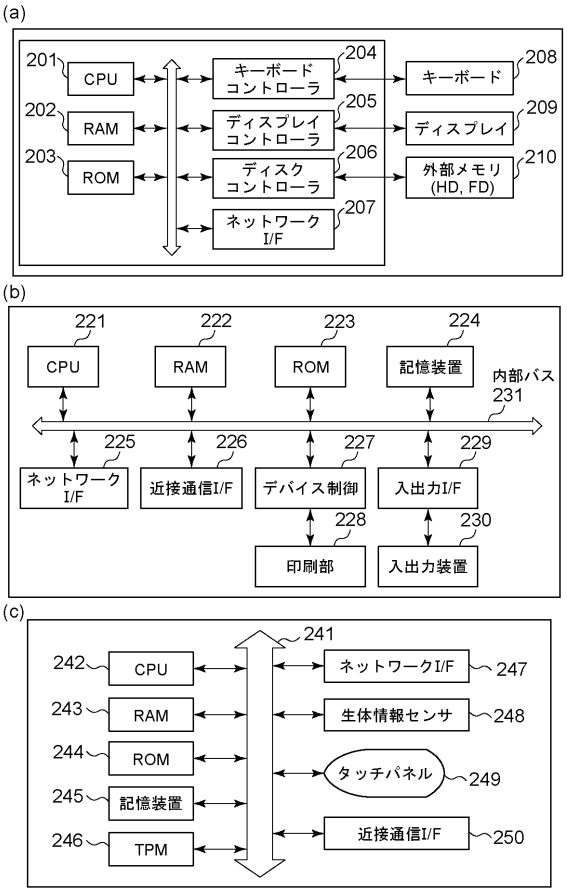
【０１１１】

１０１　画像処理装置
１０２　携帯端末
１０３　印刷サービスサーバー
１０４　機器認証サービスサーバー

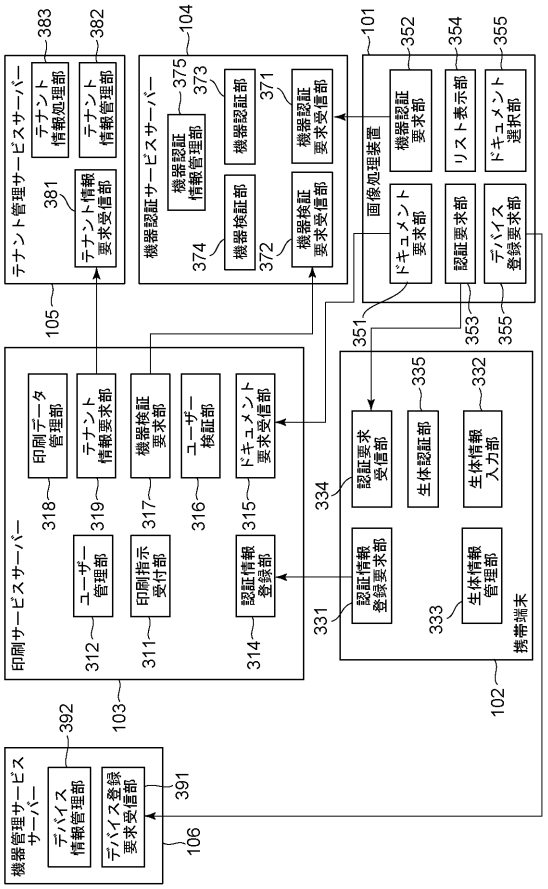
【図１】


106
機器管理サービスサーバ
105
テナント管理サービスサーバー
104
機器認証サービスサーバー
103
印刷サービスサーバー
111
ネットワーク
101
画像処理装置
112
ネットワーク
102
携帯端末
107
クライアントPC

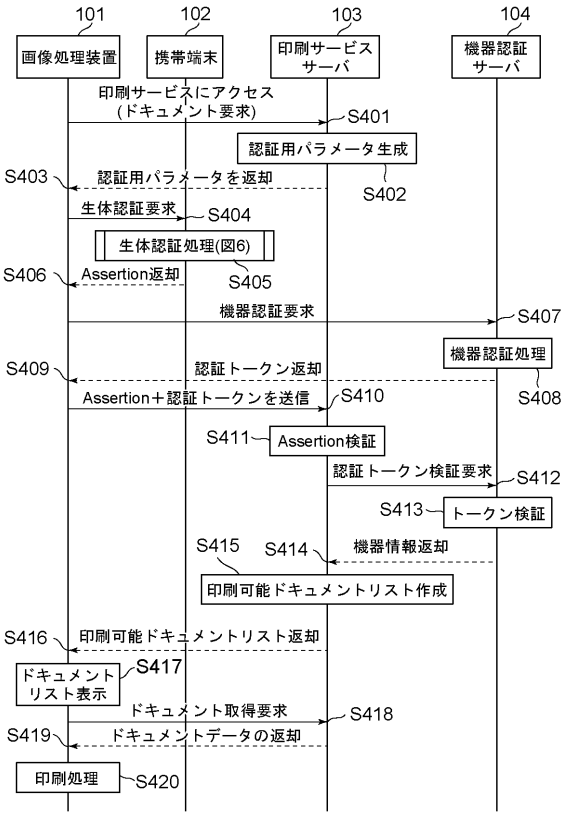
【図２】


(a)
201 CPU
202 RAM
203 ROM
キーボードコントローラ 204
ディスプレイコントローラ 205
ディスクコントローラ 206
ネットワークI/F 207
キーボード 208
ディスプレイ 209
外部メモリ(HD, FD) 210
(b)
221 CPU
222 RAM
223 ROM
224 記憶装置
内部バス 231
225 ネットワークI/F
226 近接通信I/F
227 デバイス制御
229 入出力I/F
228 印刷部
230 入出力装置
(c)
241
242 CPU
243 RAM
244 ROM
245 記憶装置
246 TPM
ネットワークI/F 247
生体情報センサ 248
タッチパネル 249
近接通信I/F 250

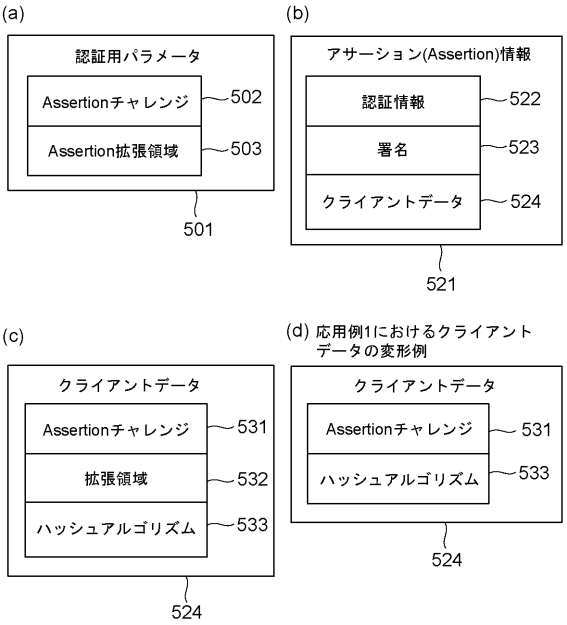
【図３】


テナント管理サービスサーバー 105
テナント情報管理部 383
テナント情報管理部 382
テナント情報要求受信部 381
機器認証サービスサーバー 104
機器認証情報管理部 375
機器認証部 373
機器検証部 374
機器検証要求受信部 372
機器認証要求受信部 371
画像処理装置 101
機器認証要求部 352
リスト表示部 354
ドキュメント選択部 355
ドキュメント要求部 351
認証要求部 353
デバイス登録要求部 355
印刷サービスサーバー 103
印刷データ管理部 318
テナント情報要求部 319
機器検証要求部 317
ユーザー検証部 316
ドキュメント要求受信部 315
ユーザー管理部 312
印刷指示受付部 311
認証情報登録部 314
認証要求受信部 334
生体認証部 335
生体情報入力部 332
認証情報登録要求部 331
生体情報管理部 333
携帯端末 102
機器管理サーバー 106
デバイス情報管理部 392
デバイス登録要求受信部 391

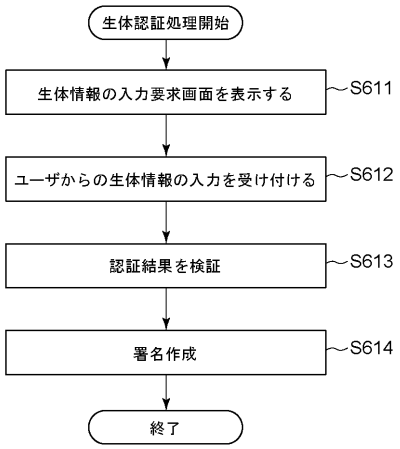
【図４】


101 画像処理装置
102 携帯端末
103 印刷サービスサーバ
104 機器認証サーバ
印刷サービスにアクセス（ドキュメント要求）
S401
認証用パラメータ生成
S402
S403 認証用パラメータを返却
生体認証要求
S404
生体認証処理(図6)
S405
S406 Assertion返却
機器認証要求
S407
機器認証処理
S408
S409 認証トークン返却
Assertion＋認証トークンを送信
S410
S411 Assertion検証
認証トークン検証要求
S412
S413 トークン検証
S414 機器情報返却
S415 印刷可能ドキュメントリスト作成
S416 印刷可能ドキュメントリスト返却
S417 ドキュメントリスト表示
ドキュメント取得要求
S418
S419 ドキュメントデータの返却
印刷処理
S420

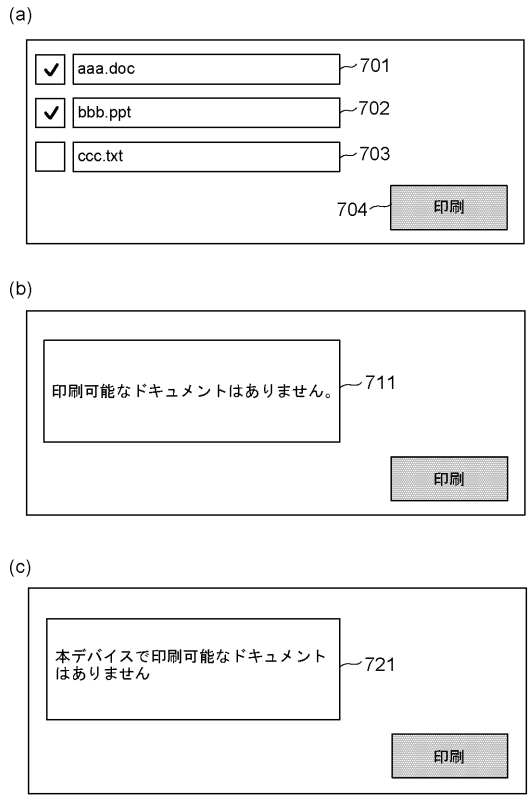
【図５】


(a)
認証用パラメータ
Assertionチャレンジ
502
Assertion拡張領域
503
501
(b)
アサーション(Assertion)情報
認証情報
522
署名
523
クライアントデータ
524
521
(c)
クライアントデータ
Assertionチャレンジ
531
拡張領域
532
ハッシュアルゴリズム
533
524
(d) 応用例1におけるクライアントデータの変形例
クライアントデータ
Assertionチャレンジ
531
ハッシュアルゴリズム
533
524

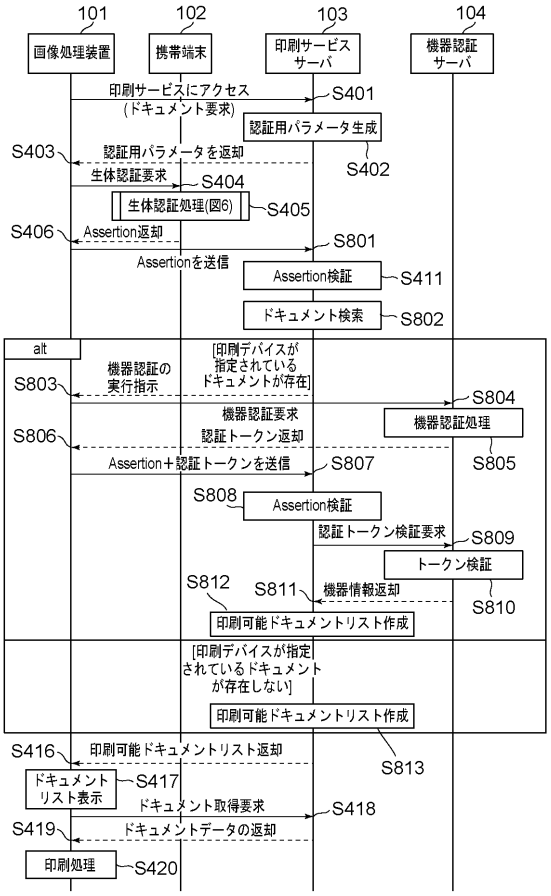
【図６】


生体認証処理開始
生体情報の入力要求画面を表示する
S611
ユーザからの生体情報の入力を受け付ける
S612
認証結果を検証
S613
署名作成
S614
終了

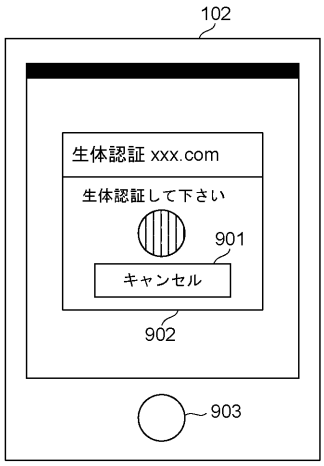
【図７】


(a)
aaa.doc
701
bbb.ppt
702
ccc.txt
703
704
印刷
(b)
印刷可能なドキュメントはありません。
711
印刷
(c)
本デバイスで印刷可能なドキュメントはありません
721
印刷

【図８】


101
102
103
104
画像処理装置
携帯端末
印刷サービスサーバ
機器認証サーバ
印刷サービスにアクセス
(ドキュメント要求)
S401
認証用パラメータ生成
S402
S403
認証用パラメータを返却
生体認証要求
S404
生体認証処理(図6)
S405
S406
Assertion返却
S801
Assertionを送信
Assertion検証
S411
ドキュメント検索
S802
alt
機器認証の実行指示
[印刷デバイスが指定されているドキュメントが存在]
S803
S804
機器認証要求
機器認証処理
S806
認証トークン返却
S805
Assertion＋認証トークンを送信
S807
S808
Assertion検証
認証トークン検証要求
S809
トークン検証
S812
S811
機器情報返却
S810
印刷可能ドキュメントリスト作成
[印刷デバイスが指定されているドキュメントが存在しない]
印刷可能ドキュメントリスト作成
S813
S416
印刷可能ドキュメントリスト返却
ドキュメントリスト表示
S417
ドキュメント取得要求
S418
S419
ドキュメントデータの返却
印刷処理
S420

【図９】



フロントページの続き

(51)Int.Cl.　　FI
　　G09C　1/00　　640E

(56)参考文献　特開２０１６－０９１２１０（ＪＰ，Ａ）
特開２０１１－２３８０８３（ＪＰ，Ａ）
特表２０１６－５１１８４９（ＪＰ，Ａ）
特開２０１５－１０３０１７（ＪＰ，Ａ）
緒方祐介　ほか，公開鍵秘密鍵を用いた認証方式に関するセキュリティ、利便性、運用性における一考察，電子情報通信学会技術研究報告，日本，一般社団法人　電子情報通信学会，２０１５年１０月　８日，Vol.115，No.252，pp.13-18（IN2015-55），ISSN 0913-5685

(58)調査した分野(Int.Cl.，ＤＢ名)
　　Ｇ０６Ｆ　２１／００－２１／１０
　　Ｇ０６Ｆ　２１／３０－２１／４６
　　Ｇ０６Ｆ　２１／６０－２１／８８
　　Ｇ０６Ｆ　３／１２
　　Ｇ０９Ｃ　１／００