

(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2018-139078
(P2018-139078A)

(43) 公開日 平成30年9月6日(2018.9.6)

(51) Int.Cl.			F I			テーマコード (参考)
G06F	21/64	(2013.01)	G06F	21/64		5B084
G06Q	10/10	(2012.01)	G06Q	10/10	330	5J104
G06F	12/00	(2006.01)	G06F	12/00	537H	5L049
G06F	13/00	(2006.01)	G06F	13/00	520C	
H04L	9/32	(2006.01)	H04L	9/00	675B	

審査請求 未請求 請求項の数 12 O L (全 27 頁) 最終頁に続く

(21) 出願番号 特願2017-33956 (P2017-33956)
(22) 出願日 平成29年2月24日 (2017.2.24)

(71) 出願人 313006647
セイコーソリューションズ株式会社
千葉県千葉市美浜区中瀬1丁目8番地
(74) 代理人 100096655
弁理士 川井 隆
(74) 代理人 100091225
弁理士 仲野 均
(72) 発明者 中嶋 勝治
千葉県千葉市美浜区中瀬1丁目8番地 セイコーソリューションズ株式会社内
Fターム(参考) 5B084 AA01 AA29 AA30 AB01 AB36
BA01 BB16 CB04 CB23 DB08
DC02 DC03 DC06
5J104 AA09 LA03 NA38
5L049 AA11

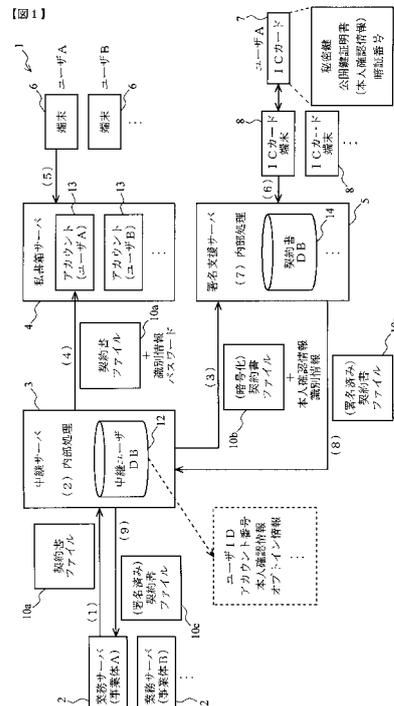
(54) 【発明の名称】 署名支援サーバ、中継サーバ、署名支援プログラム、及び中継プログラム

(57) 【要約】

【課題】電子私書箱に宛てて送信されたファイルに対してユーザが電子的に署名を行えるようにする。

【解決手段】中継サーバ3は、業務サーバ2から契約書ファイル10aを受信すると、これを複製して契約書ファイル10bを作成すると共に、契約書ファイル10bを識別する識別情報を生成する。中継サーバ3は、契約書ファイル10aと識別情報を私書箱サーバ4に送信し、契約書ファイル10bと識別情報を署名支援サーバ5に送信する。ユーザは、アカウント13で契約書ファイル10aを閲覧した後、識別情報を控える。ユーザは、ICカード端末8にICカード7をセットし、識別情報を入力して署名支援サーバ5に送信する。署名支援サーバ5は、当該識別情報によって契約書ファイル10bを特定してハッシュ値を計算し、当該ハッシュ値と暗証番号をICカード7に送信して電子署名の実行を指令する。

【選択図】 図1



【特許請求の範囲】**【請求項 1】**

秘密鍵を記憶し、当該秘密鍵を用いて電子署名する携帯型半導体装置との接続インターフェースを備えた端末と接続する接続手段と、

電子私書箱によって、署名内容を規定する原本ファイルと共に通知した識別情報の入力を、前記端末を介して受け付ける識別情報受付手段と、

前記受け付けた識別情報を用いて署名対象ファイルを特定する署名対象ファイル特定手段と、

前記特定した署名対象ファイルの署名対象値を取得する署名対象値取得手段と、

前記取得した署名対象値を前記接続インターフェースを介して前記携帯型半導体装置に送信する署名対象値送信手段と、

前記携帯型半導体装置が前記送信した署名対象値を用いて生成した電子署名を前記接続インターフェースを介して受信する電子署名受信手段と、

を具備したことを特徴とする署名支援サーバ。

10

【請求項 2】

前記署名対象値取得手段は、前記特定した署名対象ファイルから署名対象値を計算して取得することを特徴とする請求項 1 に記載の署名支援サーバ。

【請求項 3】

前記受信した電子署名を前記特定した署名対象ファイルに付随させる付随手段と、

前記電子署名を付随させた署名対象ファイルを出力する署名対象ファイル出力手段と、

を具備したことを特徴とする請求項 2 に記載の署名支援サーバ。

20

【請求項 4】

前記特定した署名対象ファイルは所定のパスワードで復号化可能に暗号化されており、

前記接続した端末から、前記電子私書箱で前記識別情報と共に通知したパスワードを取得するパスワード取得手段と、

前記取得したパスワードを用いて前記署名対象ファイルを復号化する復号化手段と、

を具備し、

前記署名対象値取得手段は、前記復号化した署名対象ファイルから署名対象値を取得することを特徴とする請求項 1、請求項 2、又は請求項 3 に記載の署名支援サーバ。

【請求項 5】

前記特定した署名対象ファイルを所定期間後に消去する消去手段を具備したことを特徴とする請求項 1 から請求項 4 までのうちの何れか 1 の請求項に記載の署名支援サーバ。

30

【請求項 6】

署名内容を規定し、所定の電子私書箱アカウントに対応づけられた原本ファイルを所定の事業体の業務サーバから取得する原本ファイル取得手段と、

前記取得した原本ファイルに対応し、電子署名の対象となる署名対象ファイルを作成する署名対象ファイル作成手段と、

前記作成した署名対象ファイルを識別する識別情報を生成する識別情報生成手段と、

前記取得した原本ファイルと前記生成した識別情報に対応させて前記所定の電子私書箱アカウントに送信する原本ファイル送信手段と、

40

前記作成した署名対象ファイルと前記生成した識別情報に対応させて所定の署名支援サーバに送信する署名対象ファイル送信手段と、

前記署名支援サーバから、前記送信した署名対象ファイルに対して生成された電子署名を受信する署名受信手段と、

前記受信した電子署名を前記業務サーバに送信する署名送信手段と、

を具備したことを特徴とする中継サーバ。

【請求項 7】

前記署名対象ファイル作成手段は、所定のパスワードで復号化可能に暗号化して前記署名対象ファイルを作成し、

前記原本ファイル送信手段は、前記パスワードを前記原本ファイルと対応させて送信す

50

ることを特徴とする請求項 6 に記載の中継サーバ。

【請求項 8】

前記署名対象ファイル作成手段は、前記署名対象ファイルとして、前記原本ファイルの複製を作成することを特徴とする請求項 6、又は請求項 7 に記載の中継サーバ。

【請求項 9】

前記署名対象ファイル作成手段は、前記原本ファイルに対応する複数の署名対象ファイルを作成し、

前記識別情報生成手段は、前記作成した複数の署名対象ファイルのそれぞれに対応させて識別情報を生成し、

前記署名対象ファイル送信手段は、前記作成した複数の署名対象ファイルを前記生成した識別情報と対応させて前記署名支援サーバに送信することを特徴とする請求項 6、請求項 7、又は請求項 8 に記載の中継サーバ。

10

【請求項 10】

前記取得した原本ファイルには、複数の電子私書箱アカウントが対応づけられており、当該複数の電子私書箱アカウントのリストを取得するリスト取得手段を具備し、

前記原本ファイル送信手段は、前記取得した原本ファイルと前記生成した識別情報を対応させて、前記取得したリストに含まれる複数の電子私書箱アカウントに送信することを特徴とする請求項 9 に記載の中継サーバ。

【請求項 11】

秘密鍵を記憶し、当該秘密鍵を用いて電子署名する携帯型半導体装置との接続インターフェースを備えた端末と接続する接続機能と、

電子私書箱によって、署名内容を規定する原本ファイルと共に通知した識別情報の入力を、前記端末を介して受け付ける識別情報受付機能と、

前記受け付けた識別情報を用いて署名対象ファイルを特定する署名対象ファイル特定機能と、

前記特定した署名対象ファイルの署名対象値を取得する署名対象値取得機能と、

前記取得した署名対象値を前記接続インターフェースを介して前記携帯型半導体装置に送信する署名対象値送信機能と、

前記携帯型半導体装置が前記送信した署名対象値を用いて生成した電子署名を前記接続インターフェースを介して受信する電子署名受信機能と、

30

をコンピュータで実現する署名支援プログラム。

【請求項 12】

署名内容を規定し、所定の電子私書箱アカウントに対応づけられた原本ファイルを所定の事業体の業務サーバから取得する原本ファイル取得機能と、

前記取得した原本ファイルに対応し、電子署名の対象となる署名対象ファイルを作成する署名対象ファイル作成機能と、

前記作成した署名対象ファイルを識別する識別情報を生成する識別情報生成機能と、

前記取得した原本ファイルと前記生成した識別情報を対応させて前記所定の電子私書箱アカウントに送信する原本ファイル送信機能と、

前記作成した署名対象ファイルと前記生成した識別情報を対応させて所定の署名支援サーバに送信する署名対象ファイル送信機能と、

40

前記署名支援サーバから、前記送信した署名対象ファイルに対して生成された電子署名を受信する署名受信機能と、

前記受信した電子署名を前記業務サーバに送信する署名送信機能と、

をコンピュータで実現する中継プログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、署名支援サーバ、中継サーバ、署名支援プログラム、及び中継プログラムに関し、例えば、電子私書箱システムを支援するものに関する。

50

【背景技術】

【0002】

電子メールが広く利用されている。電子メールは、個人間の通信に利用されるだけでなく、事業者と顧客との通信手段としても利用されている。

しかし、電子メールは、例えば、アドレスが無効となっていたり、メールアドレスの所有者（ユーザ）が放置していたりなど信頼性が乏しいという問題があった。

【0003】

そこで、本人確認の下でユーザに電子的な郵便ポストを設け、従来の郵便サービスを通信ネットワーク上に拡充する電子私書箱が利用されるようになってきた。

電子私書箱は、物理的な郵便ポストと同様に信頼性が高いため、例えば、事業者が電子的な文書ファイルで契約書を作成し、これを電子郵便物として送達することができる。

【0004】

このような電子私書箱を用いた技術に特許文献1の「サービス提供システム、改ざんチェック方法および改ざんチェックプログラム」がある。

この技術は、ユーザが何らかのサーバにアクセスして当該サーバからサービスを受ける際に、電子私書箱を介在させ、ユーザのアクセス履歴を電子私書箱に記録するものである。

サーバに残っている履歴と、電子私書箱のアクセス履歴を照合することにより、第三者による不正アクセス（なりすまし、改ざんなど）を検出することができる。

【0005】

以上のように電子私書箱は、従来の紙媒体による書面の郵送と同様に電子郵便物を文書ファイルにてユーザに送達できるため、事業者は、契約書などの従来では紙媒体でしか送付できなかった取引書類を電子データによって電子私書箱に送信することができる。

これにより、事業者側はコストを大きく削減できるほか、ユーザ側も書類の本人受け取りや保管などの手間を省くことができ、また、書類の紛失も防止することができる。更に、電子政府推進の方向性とも合致する。

また、このような電子私書箱が推進されている一方で、マイナンバー制度が開始され、個々の国民が固有のマイナンバーカード（ICカード）を保有する方向で行政が活動している。

マイナンバーカードは、電子署名用の秘密鍵を記憶しており、これを用いてマイナンバーカード内で電子署名する機能を有している。

【0006】

ところで、取引書類には、署名や捺印が求められる場合が多いが、電子私書箱に宛てた文書ファイルに対しては、署名や捺印を行って配信者に返送する手段がないという問題があった。

そのため、ユーザは、文書ファイルを紙媒体にプリントアウトして署名・捺印を行い、配信者に通常の郵便で郵送しなければならなかった。

【先行技術文献】

【特許文献】

【0007】

【特許文献1】特開2011-22825号公報

【発明の概要】

【発明が解決しようとする課題】

【0008】

本発明は、電子私書箱に宛てて送信された電子郵便物のファイルに対してユーザが電子的に署名を行えるようにすることを目的とする。

【課題を解決するための手段】

【0009】

(1) 請求項1に記載の発明では、秘密鍵を記憶し、当該秘密鍵を用いて電子署名する携帯型半導体装置との接続インターフェースを備えた端末と接続する接続手段と、電子私書

10

20

30

40

50

箱によって、署名内容を規定する原本ファイルと共に通知した識別情報の入力を、前記端末を介して受け付ける識別情報受付手段と、前記受け付けた識別情報を用いて署名対象ファイル特定する署名対象ファイル特定手段と、前記特定した署名対象ファイルの署名対象値を取得する署名対象値取得手段と、前記取得した署名対象値を前記接続インターフェースを介して前記携帯型半導体装置に送信する署名対象値送信手段と、前記携帯型半導体装置が前記送信した署名対象値を用いて生成した電子署名を前記接続インターフェースを介して受信する電子署名受信手段と、を具備したことを特徴とする署名支援サーバを提供する。

(2) 請求項2に記載の発明では、前記署名対象値取得手段が、前記特定した署名対象ファイルから署名対象値を計算して取得することを特徴とする請求項1に記載の署名支援サーバを提供する。

10

(3) 請求項3に記載の発明では、前記受信した電子署名を前記特定した署名対象ファイルに付随させる付随手段と、前記電子署名を付随させた署名対象ファイルを出力する署名対象ファイル出力手段と、を具備したことを特徴とする請求項2に記載の署名支援サーバを提供する。

(4) 請求項4に記載の発明では、前記特定した署名対象ファイルは所定のパスワードで復号化可能に暗号化されており、前記接続した端末から、前記電子私書箱で前記識別情報と共に通知したパスワードを取得するパスワード取得手段と、前記取得したパスワードを用いて前記署名対象ファイルを復号化する復号化手段と、を具備し、前記署名対象値取得手段は、前記復号化した署名対象ファイルから署名対象値を取得することを特徴とする請求項1、請求項2、又は請求項3に記載の署名支援サーバを提供する。

20

(5) 請求項5に記載の発明では、前記特定した署名対象ファイルを所定期間後に消去する消去手段を具備したことを特徴とする請求項1から請求項4までのうちの何れか1の請求項に記載の署名支援サーバを提供する。

(6) 請求項6に記載の発明では、署名内容を規定し、所定の電子私書箱アカウントに対応づけられた原本ファイルを所定の事業体の業務サーバから取得する原本ファイル取得手段と、前記取得した原本ファイルに対応し、電子署名の対象となる署名対象ファイルを作成する署名対象ファイル作成手段と、前記作成した署名対象ファイルを識別する識別情報を生成する識別情報生成手段と、前記取得した原本ファイルと前記生成した識別情報に対応させて前記所定の電子私書箱アカウントに送信する原本ファイル送信手段と、前記作成した署名対象ファイルと前記生成した識別情報に対応させて所定の署名支援サーバに送信する署名対象ファイル送信手段と、前記署名支援サーバから、前記送信した署名対象ファイルに対して生成された電子署名を受信する署名受信手段と、前記受信した電子署名を前記業務サーバに送信する署名送信手段と、を具備したことを特徴とする中継サーバを提供する。

30

(7) 請求項7に記載の発明では、前記署名対象ファイル作成手段が、所定のパスワードで復号化可能に暗号化して前記署名対象ファイルを作成し、前記原本ファイル送信手段は、前記パスワードを前記原本ファイルと対応させて送信することを特徴とする請求項6に記載の中継サーバを提供する。

(8) 請求項8に記載の発明では、前記署名対象ファイル作成手段が、前記署名対象ファイルとして、前記原本ファイルの複製を作成することを特徴とする請求項6、又は請求項7に記載の中継サーバを提供する。

40

(9) 請求項9に記載の発明では、前記署名対象ファイル作成手段が、前記原本ファイルに対応する複数の署名対象ファイルを作成し、前記識別情報生成手段は、前記作成した複数の署名対象ファイルのそれぞれに対応させて識別情報を生成し、前記署名対象ファイル送信手段は、前記作成した複数の署名対象ファイルを前記生成した識別情報と対応させて前記署名支援サーバに送信することを特徴とする請求項6、請求項7、又は請求項8に記載の中継サーバを提供する。

(10) 請求項10に記載の発明では、前記取得した原本ファイルには、複数の電子私書箱アカウントが対応づけられており、当該複数の電子私書箱アカウントのリストを取得す

50

るリスト取得手段を具備し、前記原本ファイル送信手段は、前記取得した原本ファイルと前記生成した識別情報に対応させて、前記取得したリストに含まれる複数の電子私書箱アカウントに送信することを特徴とする請求項 9 に記載の中継サーバを提供する。

(11) 請求項 11 に記載の発明では、秘密鍵を記憶し、当該秘密鍵を用いて電子署名する携帯型半導体装置との接続インターフェースを備えた端末と接続する接続機能と、電子私書箱によって、署名内容を規定する原本ファイルと共に通知した識別情報の入力を、前記端末を介して受け付ける識別情報受付機能と、前記受け付けた識別情報を用いて署名対象ファイル特定する署名対象ファイル特定機能と、前記特定した署名対象ファイルの署名対象値を取得する署名対象値取得機能と、前記取得した署名対象値を前記接続インターフェースを介して前記携帯型半導体装置に送信する署名対象値送信機能と、前記携帯型半導体装置が前記送信した署名対象値を用いて生成した電子署名を前記接続インターフェースを介して受信する電子署名受信機能と、をコンピュータで実現する署名支援プログラムを提供する。

10

(12) 請求項 12 に記載の発明では、署名内容を規定し、所定の電子私書箱アカウントに対応づけられた原本ファイルを所定の事業体の業務サーバから取得する原本ファイル取得機能と、前記取得した原本ファイルに対応し、電子署名の対象となる署名対象ファイルを作成する署名対象ファイル作成機能と、前記作成した署名対象ファイルを識別する識別情報を生成する識別情報生成機能と、前記取得した原本ファイルと前記生成した識別情報に対応させて前記所定の電子私書箱アカウントに送信する原本ファイル送信機能と、前記作成した署名対象ファイルと前記生成した識別情報に対応させて所定の署名支援サーバに送信する署名対象ファイル送信機能と、前記署名支援サーバから、前記送信した署名対象ファイルに対して生成された電子署名を受信する署名受信機能と、前記受信した電子署名を前記業務サーバに送信する署名送信機能と、をコンピュータで実現する中継プログラムを提供する。

20

【発明の効果】

【0010】

本発明によれば、ユーザは、電子私書箱に送信された電子郵便物のファイルに対して電子署名を付与することができる。

【図面の簡単な説明】

【0011】

30

【図 1】電子郵便システムの構成を示した図である。

【図 2】中継サーバなどのハードウェア的な構成を示した図である。

【図 3】各 DB の論理的な構成を説明するための図である。

【図 4】各画面を説明するための図である。

【図 5】電子郵便システムへの登録手順を説明するためのフローチャートである。

【図 6】電子署名する準備を行う手順を説明するためのフローチャートである。

【図 7】電子署名を行う手順を説明するためのフローチャートである。

【図 8】変形例 1 を説明するための図である。

【図 9】変形例 2 を説明するための図である。

40

【発明を実施するための形態】

【0012】

(1) 実施形態の概要

中継サーバ 3 (図 1) は、業務サーバ 2 からアカウント 13 に宛てた契約書ファイル 10 a を受信すると、これを複製した契約書ファイル 10 b を作成すると共に、契約書ファイル 10 b を識別する識別情報を生成する。

これにより、契約書の内容を規定した原本ファイルである契約書ファイル 10 a と、これに代わって電子署名を受ける契約書ファイル 10 b が識別情報により対応づけられる。

そして、中継サーバ 3 は、契約書ファイル 10 a と識別情報を私書箱サーバ 4 に送信し、契約書ファイル 10 b と識別情報を署名支援サーバ 5 に送信する。

【0013】

50

ユーザは、端末 6 から自己のアカウント 1 3 にアクセスし、契約書ファイル 1 0 a を閲覧した後、識別情報をメモするなどして控える。

そして、ユーザは、自己の IC カード 7 (例えば、マイナンバーカード) と控えた識別情報を持参して公共の施設 (例えば、コンビニエンスストアや役所) などに設置された IC カード端末 8 を訪れる。

【0014】

ユーザが IC カード端末 8 に IC カード 7 をセットすると、署名支援サーバ 5 と IC カード 7 は、IC カード端末 8 を介して通信可能な状態となる。

署名支援サーバ 5 は、IC カード端末 8 のディスプレイを用いてユーザに識別情報の入力を促し、ユーザは、これに応じて控えておいた識別情報を IC カード端末 8 から入力する。IC カード端末 8 は、このようにして入力された識別情報を署名支援サーバ 5 に送信する。

【0015】

署名支援サーバ 5 は、当該識別情報によって契約書ファイル 1 0 b を特定する。

更に、署名支援サーバ 5 は、IC カード端末 8 によってユーザに IC カード 7 で電子署名するための暗証番号の入力を要求する。

署名支援サーバ 5 は、暗証番号を受信すると、契約書ファイル 1 0 b のハッシュ値を計算し、当該ハッシュ値と暗証番号を IC カード 7 に送信して電子署名の実行を指令する。

【0016】

これに対して IC カード 7 は、暗証番号が適正であることを確認した後、ハッシュ値を IC カード 7 に記憶してある秘密鍵で暗号化することにより電子署名を生成して署名支援サーバ 5 に送信する。

署名支援サーバ 5 は、この電子署名を契約書ファイル 1 0 b に添付して契約書ファイル 1 0 c を生成し、これを中継サーバ 3 に送信する。中継サーバ 3 は、これを業務サーバ 2 に送信する。

【0017】

以上のようにして、業務サーバ 2 は、契約書ファイル 1 0 a に対してユーザの電子署名が成された契約書ファイル 1 0 c を得ることができる。

以上の処理は、ユーザが端末 6 から IC カード 7 にアクセスできる環境があれば、例えば、自宅などで行うこともできるが、例え、そのような環境を個人的に有しない場合でも、公共の IC カード端末 8 を用いて電子署名することができる。

【0018】

(2) 実施形態の詳細

図 1 は、本発明の第 1 実施形態に係る電子郵便システム 1 の構成を示した図である。

電子郵便システム 1 は、事業体 A、B、・・・が運営する業務サーバ 2、2、・・・、中継サーバ 3、私書箱サーバ 4、署名支援サーバ 5、ユーザの端末 6、6、・・・、IC カード端末 8、8、・・・、IC カード 7、7、・・・などがインターネットなどの通信ネットワークを介して接続可能に配設されて構成されている。

【0019】

これらが行う通信は、例えば、SSL (Secure Sockets Layer) などを用いて暗号化されており、外部から内容が秘匿された状態で行われる。

以下では、図の括弧で示した番号に対応させて説明する。

【0020】

業務サーバ 2 は、例えば、金融機関、保険会社、自動車販売店、不動産事業者、コンテンツ販売会社などの企業や、会計事務所、政府・自治体の機関など、各種の事業体や個人が運営するサーバであり、ユーザ (例えば、ユーザ A) に宛てた契約書ファイル 1 0 a を中継サーバ 3 に対して送信する (1)。

【0021】

契約書ファイル 1 0 a は、郵便物の住所・宛名に対応するアカウント番号や契約書の文書データなどを含む電子郵便物であって、以下の処理で署名内容を規定する原本となる原

10

20

30

40

50

本ファイルに相当する。

なお、本実施の形態では、処理対象の電子郵便物を契約書ファイル10aとするが、これに限定するものではなく、その他の文書ファイル（例えば、請求書）やコンテンツなど、電子署名の対象となる電子情報を広く用いることができる。

【0022】

中継サーバ3は、中継サーバ運営事業者が運営するサーバであって、業務サーバ2、私書箱サーバ4、及び署名支援サーバ5の間に介在し、これらと連携してユーザが契約書ファイル10aに対して電子署名を行う操作を支援する。

中継サーバ3は、電子署名支援サービスに申し込んだユーザのユーザ情報を記憶した中継ユーザDB12を備えている。

【0023】

中継ユーザDB12のユーザ情報は、後述するように、ユーザID、当該ユーザの私書箱サーバ4でのアカウント番号、本人確認情報、オプトイン情報、その他の情報から構成されている。

本人確認情報は、基本4情報（ユーザの氏名、生年月日、性別、住所）などから構成されている。

【0024】

オプトイン情報は、契約書ファイル10aを送信する事業者のうち、ユーザが受け取りを指定したものを特定する情報である。オプトイン情報で指定されていない事業者から当該ユーザに送信された契約書ファイル10aは、中継サーバ3によってブロックされる。

なお、オプトイン情報は、ユーザが私書箱サーバ4に対して提示し登録したものであり、これを中継サーバ3が引き継いで私書箱サーバ4に代理してブロック処理を行うものである。

【0025】

なお、これは一例であって、一般的には、私書箱サーバ4がオプトイン情報を用いてブロック処理を行う。

このように、中継サーバ3は、私書箱サーバ4に代わって、ブロック処理を行うことにより、私書箱サーバ4の負荷の低減を図っており、私書箱サーバ4の業務処理を一部肩代わりすることができる。

【0026】

中継サーバ3は、業務サーバ2が私書箱サーバ4に宛てて送信した契約書ファイル10aを私書箱サーバ4に届く前に受信する。

このように、中継サーバ3は、署名内容を規定し、所定の電子私書箱アカウント（アカウント13）に対応づけられた原本ファイル（契約書ファイル10a）を所定の事業者の業務サーバから取得する原本ファイル取得手段を備えている。

中継サーバ3が業務サーバ2から契約書ファイル10aを取得する方式は、プル型とプッシュ型のどちらでもよい。

【0027】

中継サーバ3は、業務サーバ2から受信した契約書ファイル10aに対して次のような内部処理を行う（2）。

まず中継サーバ3は、図示しないタイムスタンプサーバと通信し、契約書ファイル10aにタイムスタンプを付与する。これにより契約書ファイル10aの改ざんを防止する。

【0028】

次に、中継サーバ3は、署名支援サーバ5に対する内部処理として、契約書ファイル10aを複製し、これを所定のパスワードで復号化可能に暗号化することで契約書ファイル10bを生成する。

【0029】

契約書ファイル10bは、原本ファイル（契約書ファイル10a）に対応し、電子署名の対象となる署名対象ファイルとして機能し、中継サーバ3は、署名対象ファイルを作成する署名対象ファイル作成手段を備えている。

10

20

30

40

50

そして、署名対象ファイル作成手段は、所定のパスワードで復号化可能に暗号化して署名対象ファイルを作成し、署名対象ファイルとして、原本ファイルの複製を作成している。

【0030】

更に、中継サーバ3は、契約書ファイル10aと契約書ファイル10bに対応づけた固有の識別情報を生成する。これにより、識別情報を用いて契約書ファイル10aや契約書ファイル10bを特定することが可能となる。

このように、中継サーバ3は、署名対象ファイルを識別する識別情報を生成する識別情報生成手段を備えている。

【0031】

そして、中継サーバ3は、暗号化した契約書ファイル10bに、中継ユーザDB12が記憶する当該ユーザの本人確認情報と識別情報を対応づけて（付随させて）署名支援サーバ5に送信する（3）。

このように、中継サーバ3は、署名対象ファイルに識別情報を対応させて所定の署名支援サーバ5に送信する署名対象ファイル送信手段を備えている。

なお、契約書ファイルを暗号化して契約書ファイル10bとするのは、署名支援サーバ5の事業者に対して内容を秘匿し、セキュリティを高めるためである。

【0032】

中継サーバ3は、私書箱サーバ4に対する内部処理として、契約書ファイル10aに識別情報と復号化用のパスワードを付随させて（対応させて）私書箱サーバ4の当該ユーザのアカウント13に宛てて送信する（4）。

中継サーバ3は、この付随を、ユーザがアカウント13にアクセスして契約書ファイル10aを閲覧する際に識別情報とパスワードも表示されるような形態で行う。

【0033】

これによりユーザは、契約書ファイル10aの閲覧の際に、識別情報とパスワードを紙媒体にメモするなどして控えることができる。

このように、中継サーバ3は、原本ファイルと識別情報とパスワードを対応させて所定の電子私書箱アカウントに送信する原本ファイル送信手段を備えている。

【0034】

なお、本実施の形態では、複製元のファイルである契約書ファイル10aを原本とし、これから複製したものを暗号化して契約書ファイル10bとしているが、複製では同一のものが作成されるため、複製されたファイルを原本として私書箱サーバ4に送信し、複製元のファイルを暗号化して署名支援サーバ5に送信してもよい。これにより、複製ではなく、業務サーバ2から送信された原本の契約書ファイルに署名することができる。

【0035】

私書箱サーバ4は、例えば、郵便事業者などの公的な機関、あるいは、同程度の信頼性が担保されている団体が運営するサーバであって、本人確認を経て登録したユーザに対して電子私書箱サービスを提供する。

【0036】

私書箱サーバ4には、ユーザA、B、・・・ごとのアカウント13、13、・・・が設けられており、これらアカウント13は、アカウント番号により一意に管理されている。

私書箱サーバ4は、端末6からアカウント13へのログインを各ユーザに対して発行したアカウント13用のパスワードによって認証している。

【0037】

なお、私書箱サーバ4は、公共性が高いため、アカウント13に送達された電子郵便物の転送や外部からの参照などは許可していない。

このため、電子郵便システム1では、中継サーバ3、私書箱サーバ4、署名支援サーバ5、ICカード端末8を連携させることにより、アカウント13内の契約書ファイル10aの転送や参照を回避しつつ、アカウント13に対する電子署名を可能としたものである。

。

10

20

30

40

50

【 0 0 3 8 】

端末 6 は、無線や有線によって通信ネットワークに接続するコンピュータであって、例えば、パーソナルコンピュータ、スマートフォン、携帯電話、ゲーム機器などで構成されている。

端末 6 は、私書箱サーバ 4 の電子郵便サイトが提供する画面を表示するディスプレイなどの出力機器や、これに対してユーザが操作を行うキーボードやタッチパネルなどの入力機器を備えている。

【 0 0 3 9 】

端末 6 は、ユーザが使用する汎用の端末装置であるが、電子郵便システム 1 においては、次のように使用される。

端末 6 は、ユーザの操作により、私書箱サーバ 4 のログイン画面にアクセスし、これに対してユーザが入力したアカウント番号とアカウント 1 3 用のパスワードを私書箱サーバ 4 に送信することにより当該ユーザのアカウント 1 3 にログインする (5) 。

【 0 0 4 0 】

アカウント 1 3 には、当該ユーザ宛の電子郵便物が記憶されているが、端末 6 は、ユーザ操作により、これらを一覧表示し、その中から所望の電子郵便物を選択してその内容を表示する。

ユーザが契約書ファイル 1 0 a の表示を選択すると、端末 6 は、私書箱サーバ 4 が提供する電子郵便閲覧画面にて、契約書ファイル 1 0 a の内容、及びこれに付随する識別情報と、暗号化された契約書ファイル 1 0 b の復号化用のパスワードを表示する。

ユーザは、後ほど電子署名を行うために識別情報とパスワードを控える。

【 0 0 4 1 】

IC カード 7 は、IC チップ (半導体装置) を内蔵した IC カードであり、マイナンバカードがその典型である。

また、IC チップを内蔵した電子マネーカードや社員証カードなどのカード媒体のほか、IC チップを内蔵したスマートフォン、携帯電話、携帯ゲーム機などがある。更に、IC チップと同等の機能をスマートホンの CPU など代替してもよい。

【 0 0 4 2 】

IC カード 7 は、IC チップとこれを IC カード端末 8 に接続するインターフェースを備えている。

インターフェースには、接触式と非接触式がある。接触式の場合には、IC カード 7 に接続用の電極が設けられており、当該電極の接触を介して電力の供給と信号の送受信が行われる。

非接触式の場合には、IC カード 7 に通信、及び電力供給用のアンテナが埋め込んであり、無線にて電力の供給と信号の送受信が行われる。

【 0 0 4 3 】

IC チップは、CPU や記憶装置などを備えたコンピュータとして機能する携帯可能な半導体装置であって、記憶装置は、CPU に電子署名を行わせるためのプログラム、電子署名を行うための秘密鍵、当該秘密鍵と鍵ペアを成す公開鍵の公開鍵証明書、電子署名を行う際にユーザが入力する暗証番号などを記憶している。また、公開鍵証明書には、ユーザを特定する本人確認情報 (基本 4 情報) が記録されている。

IC チップ (IC カード 7) は、秘密鍵を記憶し、当該秘密鍵を用いて電子署名する携帯型半導体装置として機能する。

【 0 0 4 4 】

IC チップは、電子署名対象の文書ファイルのハッシュ値が入力されると、これを CPU にて秘密鍵で暗号化し、これに公開鍵証明書を添付するなどして電子署名を行う。

電子署名が行われる仕組みは、以下の通りである。

ハッシュ値は、文書ファイルから計算される署名対象値 (数値) であり、文書の内容が僅かでも異なるとハッシュ値は大きく変化する。また、ハッシュ値から文書ファイルを復元することはできない。そのため、文書ファイルとハッシュ値は、一対一に対応している

10

20

30

40

50

。

【0045】

このハッシュ値をICチップの記憶する秘密鍵で暗号化すると、当該秘密鍵に対応する公開鍵でのみ復号化することができる。

そのため、電子署名値（ハッシュ値）を秘密鍵に対応する公開鍵で復号化し、これを非改竄性の検証対象となる文書ファイルのハッシュ値と比較したところ、両者が一致するのであれば、当該ユーザが当該文書ファイルに対して署名したと確認することができる。

【0046】

ICカード端末8は、例えば、コンビニエンスストアに設置された端末（複合コピー機や券売機など）であって、通信ネットワークに接続する機能とICカード7に接続するリーダライタを備えている。

ICカード端末8は、秘密鍵を記憶し、当該秘密鍵を用いて電子署名する携帯型半導体装置との接続インターフェース（リーダライタなど）を備えた端末として機能している。

ICカード7がリーダライタに設置されると、ICカード端末8は、署名支援サーバ5とICカード7の通信を仲介し、署名支援サーバ5とICカード7の通信を可能とする。

【0047】

また、ICカード端末8は、メッセージを表示する画面などの出力機器や、情報を入力するキーボードなどの入力機器も備えている。

これによって、ICカード端末8は、ユーザに識別情報を入力させる指示を与えたり、ユーザからの識別情報の入力を受け付けることができる。

【0048】

なお、端末6にリーダライタを接続して、端末6にICカード端末8と同様の機能を発揮させることもできる。

そのため、例えば、自宅の端末6にICカード7用のリーダライタを設置してあるユーザは、ICカード端末8まで行かなくても自宅で電子署名することができる。

このように、電子郵便システム1は、自宅にリーダライタがあるユーザに関しては、自宅で電子署名することができるが、そのような環境にないユーザについてもICカード端末8で電子署名することができる。

【0049】

このように構成されたICカード端末8を介して署名支援サーバ5とICカード7は、次のようにして電子署名を行う（6）。

まず、ユーザがICカード7をICカード端末8のリーダライタに設置することにより、ICカード端末8を介してICカード7と署名支援サーバ5が接続する。

次に、ICカード端末8は、ユーザから識別情報と復号化用のパスワードの入力を受け付け、これを署名支援サーバ5に送信する。

【0050】

署名支援サーバ5は、識別情報によって契約書ファイル10bを特定すると、これをパスワードによって復号化し、復号化した契約書ファイル10bのハッシュ値を計算してICカード7に送信する。

ICカード7は、当該ハッシュ値を秘密鍵で暗号化することにより電子署名を作成して署名支援サーバ5に送信する。

電子署名処理の骨子は、以上の通りであるが、後述するように、更に電子署名用の暗証番号の入力、本人確認などを行ってセキュリティを高めることができる。

【0051】

署名支援サーバ5は、中継サーバ3から契約書ファイル10bを受信して契約書DB14に記憶しておき、ICカード端末8を介してユーザから要求があった場合にICカード7に電子署名を行わせて、当該作成された電子署名を中継サーバ3に送信するサーバである（7）。

【0052】

より詳細には、まず、署名支援サーバ5は、中継サーバ3から暗号化された契約書ファ

10

20

30

40

50

イル10bと、これに付随する本人確認情報と識別情報を受信し、それぞれ対応付けて契約書DB14に記憶する。

そして、署名支援サーバ5は、ICカード端末8を介してユーザから電子署名の要求があるまで待機する。

【0053】

ユーザがICカード7をICカード端末8にセットして所定の操作を行うと、署名支援サーバ5は、ICカード端末8を介してICカード7との通信を開始する。

このように、署名支援サーバ5は、秘密鍵を記憶し、当該秘密鍵を用いて電子署名する携帯型半導体装置との接続インターフェースを備えた端末(ICカード端末8)と接続する接続手段を備えている。

10

【0054】

そして、署名支援サーバ5は、ICカード端末8を介して識別情報と復号化用のパスワードの入力をユーザに要求し、ユーザが入力したこれらの情報をICカード端末8から受信する。

次いで、署名支援サーバ5は、識別情報を検索キーとして契約書DB14を検索することにより、電子署名の対象となっている契約書ファイル10bを特定し、パスワードでこれを復号化する。

【0055】

このように、署名支援サーバ5は、電子私書箱によって署名内容を規定する原本ファイルと共に通知した識別情報の入力を、端末(ICカード端末8)を介して受け付ける識別情報受付手段と、当該受け付けた識別情報を用いて署名対象ファイル(契約書ファイル10b)を特定する署名対象ファイル特定手段を備えている。

20

更に、署名対象ファイルは所定のパスワードで復号化可能に暗号化されており、署名支援サーバ5は、端末(ICカード端末8)から、電子私書箱で識別情報と共に通知したパスワードを取得するパスワード取得手段と、当該取得したパスワードを用いて署名対象ファイルを復号化する復号化手段を備えている。

【0056】

そして、署名支援サーバ5は、ICカード端末8からICカード7に設定されている電子署名用の暗証番号の入力をユーザに要求する。

署名支援サーバ5は、これによってICカード端末8から入力された暗証番号をICカード7に送信し、ICカード7によって暗証番号が承認されると、ICカード7に公開鍵証明書の送信を要求する。

30

なお、暗証番号は、署名支援サーバ5を経由せずにICカード端末8からICカード7に直接送信して、ICカード端末8が暗証番号の認証結果を署名支援サーバ5に送信するようにしてもよい。

【0057】

そして、署名支援サーバ5は、公開鍵証明書に含まれる本人確認情報と中継サーバ3から送信されてきた本人確認情報によってユーザの本人確認を行い、本人確認が成功すると、復号化した契約書ファイル10bからハッシュ値を計算によって生成し、これを取得する。

40

このように、署名支援サーバ5は、署名対象ファイルの署名対象値(ハッシュ値)を復号化した署名対象ファイルから計算して取得する署名対象値取得手段を備えている。

【0058】

そして、署名支援サーバ5は、生成した当該ハッシュ値と暗証番号をICカード7に送信してICカード7に当該ハッシュ値を用いた電子署名の作成を命令する。

このように、署名支援サーバ5は、署名対象値をICカード端末8の接続インターフェースを介して携帯型半導体装置(ICカード7のICチップ)に送信する署名対象値送信手段を備えている。

【0059】

署名支援サーバ5は、ICカード7が作成して送信した契約書ファイル10bに対する

50

電子署名を受信し、これを契約書ファイル 10b に付随させて署名済みの契約書ファイル 10c を作成して、中継サーバ 3 に送信する (8)。

このように、署名支援サーバ 5 は、携帯型半導体装置が署名対象値を用いて生成した電子署名を接続インターフェースを介して受信する電子署名受信手段と、ICカード 7 から受信した電子署名を署名対象ファイルに付随させる付随手段と、電子署名を付随させた署名対象ファイルを出力する署名対象ファイル出力手段を備えている。

【0060】

なお、署名支援サーバ 5 は、暗号化された契約書ファイル 10b、及び復号化した契約書ファイル 10b を所定タイミングで契約書 DB 14 から消去することで、セキュリティを高めている。

ここで、所定タイミングとしては、例えば、契約書ファイル 10b に対する電子署名が行われた場合には、署名済みの契約書ファイル 10c の中継サーバ 3 への送信が完了した後に直ちに、又は完了後所定時間経過後に消去する。

一方、契約書ファイル 10b の電子署名がなされなかった場合には、暗号化された契約書ファイル 10b を中継サーバ 3 から受信後、電子署名のために許容された期間が経過した後に消去される。

【0061】

電子署名のために許容された期間としては、例えば、一律に 1 週間が規定されるようにしてもよく、契約書ファイル毎に各事業体が指定した期間 (指定が無い場合にはデフォルトの期間、例えば、1 週間) としてもよい。

事業体が期間を指定する場合には、契約書ファイル 10a とともに指定された期間が業務サーバ 2 から中継サーバ 3 に送信され、中継サーバ 3 は暗号化した契約書ファイル 10b、本人確認情報と共に指定された期間を署名支援サーバ 5 に送信する。

このように署名支援サーバ 5 は、署名対象ファイル (契約書ファイル 10b) を所定期間後に消去する消去手段を備えている。

【0062】

中継サーバ 3 は、署名支援サーバ 5 から契約書ファイル 10b に電子署名して作成した契約書ファイル 10c を受信すると、受信した電子署名済みの契約書ファイル 10c を、契約書ファイル 10a の送信元である業務サーバ 2 に送信する (9)。

このように、中継サーバ 3 は、署名対象ファイルに対して生成された電子署名を受信する署名受信手段と、当該受信した電子署名を業務サーバ 2 に送信する署名送信手段を備えている。

【0063】

以上に電子郵便システム 1 の構成の一例を説明したが、各種の変形例が可能である。

例えば、電子郵便システム 1 では、署名支援サーバ 5 が契約書ファイル 10b を記憶し、内部処理を行ったが、この内部処理を中継サーバ 3 で行い、署名支援サーバ 5 は、中継サーバ 3 と ICカード端末 8 の通信を単に仲介するサーバとしてもよい。

【0064】

この場合、中継サーバ 3 は、契約書ファイル 10b を記憶しておき、署名支援サーバ 5 を介して ICカード端末 8 から識別情報を受信する。

そして、中継サーバ 3 は、契約書ファイル 10b からハッシュ値を計算して、ICカード 7 に電子署名を行わせる。

この例では、電子署名に関する処理は、全て中継サーバ 3 が行い、中継サーバ 3 が署名支援サーバ 5 の機能も兼ね備えている。

【0065】

先に説明した実施の形態は、例えば、中継サーバ 3 と署名支援サーバ 5 を同じ事業体が運営する場合に適した形態であり、当該変形例は、例えば、署名支援サーバ 5 として ICカード端末 8 を設置したコンビニエンスストアのサーバシステムを援用する場合などに適した形態である。

【0066】

10

20

30

40

50

図 2 (a) は、中継サーバ 3 のハードウェア的な構成を模式的に示した図である。

中継サーバ 3 は、CPU 3 1、ROM 3 2、RAM 3 3、通信制御部 3 4、及び記憶装置 3 5 などがバスラインで接続されて構成されている。

CPU 3 1 は、中央処理装置であって、記憶装置 3 5 が記憶する図示しない中継プログラムに従って動作し、業務サーバ 2、私書箱サーバ 4、及び署名支援サーバ 5 の間で上述した中継処理を行う。

【 0 0 6 7 】

ROM 3 2 は、読み出し専用のメモリであって、CPU 3 1 を動作させるための基本的なプログラムやパラメータを記憶している。

RAM 3 3 は、読み書きが可能なメモリであって、CPU 3 1 が契約書ファイル 1 0 b の複製や暗号化、URL の生成など中継処理を行う際のワーキングメモリを提供する。

【 0 0 6 8 】

通信制御部 3 4 は、中継サーバ 3 と通信ネットワークを接続するインターフェースである。中継サーバ 3 は、通信制御部 3 4 で接続された通信ネットワークを介して、各業務サーバ 2、私書箱サーバ 4、署名支援サーバ 5 等と接続される。

記憶装置 3 5 は、例えば、ハードディスクなどの記憶媒体を用いて構成されており、CPU 3 1 に中継処理機能を発揮させるための中継プログラムや中継ユーザ DB 1 2 などを記憶している。

【 0 0 6 9 】

図 2 (b) は、署名支援サーバ 5 のハードウェア的な構成を模式的に示した図である。

署名支援サーバ 5 は、CPU 5 1、ROM 5 2、RAM 5 3、通信制御部 5 4、及び記憶装置 5 5 などがバスラインで接続されて構成されている。

CPU 5 1 ~ RAM 5 3 の機能は、CPU 3 1 ~ RAM 3 3 と同様である。

【 0 0 7 0 】

通信制御部 5 4 は、署名支援サーバ 5 と通信ネットワークとを接続するインターフェースである。署名支援サーバ 5 は、通信制御部 5 4 で接続された通信ネットワークを介して、中継サーバ 3、IC カード端末 8、IC カード 7 等と接続される。

記憶装置 5 5 は、例えば、ハードディスクなどの記憶媒体を用いて構成されており、CPU 5 1 に IC カード 7 と協働して電子署名するためのプログラム、契約書 DB 1 4 などを記憶している。

【 0 0 7 1 】

図 2 (c) は、IC カード 7 のハードウェア的な構成を模式的に示した図である。

IC カード 7 は、CPU 7 1、ROM 7 2、RAM 7 3、通信制御部 7 4、及び記憶装置 7 5 などがバスラインで接続されて構成されており、これらは、IC チップ上に形成されている。

CPU 7 1 ~ RAM 7 3 の機能は、CPU 3 1 ~ RAM 3 3 と同様である。

【 0 0 7 2 】

通信制御部 7 4 は、IC カード端末 8 に接続するための電極（接触式の場合）やアンテナ（非接触式の場合）を備えており、IC カード端末 8 側のインターフェースと接続して、通信を行う。

記憶装置 7 5 は、CPU 7 1 に通信を行わせたり、電子署名処理を行わせるためのプログラムや、電子署名に用いる秘密鍵や公開鍵証明書、及び、電子署名処理を行わせるための暗証番号などを記憶している。

【 0 0 7 3 】

図 3 (a) は、中継ユーザ DB 1 2 の論理的な構成を示した図である。

中継ユーザ DB 1 2 は、ユーザごとの「ユーザ ID」、「アカウント番号」、「本人確認情報」、「オプトイン情報」、その他の項目から構成されている。

「ユーザ ID」は、中継サーバ 3 がユーザを識別するための ID 情報である。

【 0 0 7 4 】

「アカウント番号」は、ユーザの私書箱サーバ 4 におけるアカウント 1 3 のアカウント

10

20

30

40

50

番号である。

中継サーバ3は、業務サーバ2が送信した契約書ファイル10aの宛先のアカウント番号を当該「アカウント番号」と照合することによりユーザを特定し、当該ユーザの本人確認情報やオプトイン情報などを特定する。

「本人確認情報」は、ユーザの基本4情報であり、「オプトイン情報」は、ユーザが設定したオプトイン情報である。

なお、オプトイン情報に基づく電子郵便物のブロックを私書箱サーバ4で行う場合は、この項目は不要である。

【0075】

図3(b)は、契約書DB14の論理的な構成を示した図である。

契約書DB14は、中継サーバ3から送信されてくる識別情報、契約書ファイル、本人確認情報の組を電子署名のために蓄積しておくデータベースであり、「識別情報」、「契約書ファイル」、「本人確認情報」、その他の項目から構成されている。

【0076】

「識別情報」は、契約書ファイル10bを特定する検索キーとなる情報であり、上に説明した識別情報である。

「契約書ファイル」は、暗号化された契約書ファイル10bである。

「本人確認情報」は、本人確認のための基本4情報であり、中継ユーザDB12の「本人確認情報」と同じ内容のものである。

【0077】

図示しないが、ICカード端末8のハードウェア的な構成は、署名支援サーバ5などと同様であり、CPU、ROM、RAM、記憶装置、通信制御部、ICカード7と接続するインターフェースなどがバスラインで接続されて構成されている。

【0078】

図4の各図は、ユーザが操作を行う画面を説明するための図である。

図4(a)は、端末6に表示される電子郵便閲覧画面21の一例を示した図である。

端末6からアカウント13にログインするとアカウント13に送達されている電子郵便物がディスプレイに一覧表示される。ユーザがこれらの中から所望の電子郵便物に対して選択操作するとその内容が電子郵便閲覧画面21に表示される。

【0079】

図の例では、契約書ファイル10aの内容が表示されている。

電子郵便閲覧画面21の下方には、契約書ファイル10aに付随している識別情報22が「通知番号」として表示され、復号化用のパスワード23もこれと共に表示されている。

ユーザは、識別情報22とパスワード23をメモするなどして控えて、ICカード端末8が設置された店舗に持参する。

【0080】

図4(b)は、ICカード端末8のディスプレイに表示された識別情報入力画面24の一例を示した図である。

ユーザがICカード端末8のリーダライタにICカード7を設置すると共に、ICカード端末8のディスプレイに表示されたメニュー画面から適当な項目を選択すると、識別情報入力画面24が表示される。

識別情報入力画面24は、通知番号入力欄とパスワード入力欄を備えており、ユーザは、メモしてきた識別情報とパスワードを、それぞれ、通知番号入力欄とパスワード入力欄に入力し、図示しない送信ボタンを選択する。

これにより、ICカード端末8は、識別番号とパスワードを署名支援サーバ5に送信する。

【0081】

図4(c)は、ICカード端末8のディスプレイに表示された暗証番号入力画面26の一例を示した図である。

10

20

30

40

50

暗証番号入力画面 26 は、暗証番号入力欄を備えており、電子署名を行う直前に表示される。

ユーザは、ICカード 7 に電子署名を実行させるために暗証番号を暗証番号入力欄に入力して図示しない送信ボタンを選択する。

これにより、署名支援サーバ 5 と IC カード 7 が通信して電子署名が行われる。

【0082】

図 5 は、ユーザが電子郵便システム 1 に登録する手順を説明するためのフローチャートである。

以下の処理は、端末 6 や各サーバの CPU が所定のプログラムに従って行うものである。

まず、端末 6 は、ユーザの操作により私書箱サーバ 4 の登録画面にアクセスする（ステップ 5）。

【0083】

私書箱サーバ 4 は、これに応じて端末 6 に登録画面データを送信する（ステップ 10）。

端末 6 は、私書箱サーバ 4 から登録画面データを受信し、登録画面をディスプレイに表示する。登録画面には、本人確認情報（基本 4 情報）やオプトイン情報を入力する欄が設けられている。

ユーザがこれらを入力し、送信操作を行うと、端末 6 は、これらの登録情報を私書箱サーバ 4 に送信する（ステップ 15）。

【0084】

私書箱サーバ 4 は、端末 6 から登録情報を受信すると、当該ユーザのアカウント 13 を作成し、当該アカウント 13 のアカウント番号と、これにログインするためのパスワードを端末 6 に送信する（ステップ 20）。

次いで、私書箱サーバ 4 は、作成したアカウント 13 のアカウント番号、本人確認情報、オプトイン情報などを中継サーバ 3 に送信する（ステップ 25）。

【0085】

なお、本実施形態による、署名支援サーバ 5 の署名を希望せず、企業サーバからの電子郵便の受領だけを希望するユーザは、私書箱サーバ 4 に対し、アカウント 13 を作成する際にその旨を通知することも可能である。この場合、私書箱サーバ 4 は、ステップ 25 以降の処理を行わずに登録処理を終了する。

【0086】

中継サーバ 3 は、これらの情報を私書箱サーバ 4 から受信するとユーザ ID を発行し、私書箱サーバ 4 から受信したこれらの情報を中継ユーザ DB 12 に記憶してユーザを登録する（ステップ 30）。

【0087】

図 6 は、電子郵便システム 1 が電子署名する準備を行う手順を説明するためのフローチャートである。

まず、業務サーバ 2 がある特定のユーザのアカウント 13 に宛てた契約書ファイル 10 a を中継サーバ 3 に送信する（ステップ 100）。

【0088】

中継サーバ 3 は、契約書ファイル 10 a を受信すると、改ざん防止のため、図示しないタイムスタンプサーバと通信して契約書ファイル 10 a のタイムスタンプを取得する（ステップ 105）。

次に、中継サーバ 3 は、契約書ファイル 10 a のコピーを作成してこれを暗号化することにより契約書ファイル 10 b を生成し、更に、これを復号化するパスワードを生成する（ステップ 110）。

【0089】

次に、中継サーバ 3 は、契約書ファイル 10 b を識別するための識別情報を生成する（ステップ 115）。

10

20

30

40

50

そして、中継サーバ3は、契約書ファイル10aに識別情報と契約書ファイル10bを復号化するパスワードを対応させて（付随させて）、私書箱サーバ4に送信する（ステップ120）。

私書箱サーバ4は、契約書ファイル10aと識別情報、及びパスワードを受信し、契約書ファイル10aの宛先で指定されているアカウント13に記憶して格納する（ステップ125）。

【0090】

更に、中継サーバ3は、本人確認情報を中継ユーザDB12で検索し、暗号化した契約書ファイル10bに、識別情報、及び本人確認情報を対応づけて署名支援サーバ5に送信する（ステップ130）。

署名支援サーバ5は、中継サーバ3から契約書ファイル10b、識別情報、及び本人確認情報を受信して、これらに対応づけて契約書DB14に記憶する（ステップ135）。

【0091】

このようにして、私書箱サーバ4と署名支援サーバ5は、それぞれ、端末6とICカード端末8からのアクセスを受ける準備が整い、ユーザからこれらを用いてアクセスがあるまで待機する。

【0092】

私書箱サーバ4と署名支援サーバ5が待機している間に、ユーザの操作により端末6は、私書箱サーバ4にアクセスし、アカウント番号、パスワードを送信してアカウント13にログインする（ステップ140）。

私書箱サーバ4は、端末6がアカウント13にログインすると、アカウント13に送達されている電子郵便物を一覧する画面データを端末6に送信する。

【0093】

ユーザが端末6を操作して当該一覧から契約書ファイル10aを選択すると、私書箱サーバ4は、電子郵便閲覧画面21（図4（a））を表示する画面データを端末6に送信することにより、契約書ファイル10aの内容、これに付随する識別情報22、及びパスワード23を端末6に送信する（ステップ145）。

【0094】

端末6は、当該画面データを受信すると、ディスプレイに電子郵便閲覧画面21を表示することにより契約書ファイル10aの文面、識別情報とパスワードを表示する（ステップ150）。これを参照し、ユーザは、識別情報とパスワードを控える。

【0095】

図7は、電子郵便システム1が電子署名を行う手順を説明するためのフローチャートである。

ユーザは、控えた識別情報とパスワードを携えてICカード端末8が設置された店舗などに赴く。

ユーザは、持参したICカード7をICカード端末8に設置し、ICカード端末8のメニュー画面から電子郵便システム1による電子署名サービスを選択する。

すると、ICカード端末8は、署名支援サーバ5に接続し、署名支援サーバ5とICカード7の通信が開始される（ステップ205）。

【0096】

通信を開始すると、署名支援サーバ5は、識別情報入力画面24の画面データを生成してICカード端末8に送信する（ステップ210）。

これに対し、ICカード端末8は、画面データを受信してディスプレイに識別情報入力画面24を表示する（ステップ215）。

【0097】

ユーザは、識別情報入力画面24から識別情報と復号化用のパスワードを入力し、送信ボタンを選択する。

これにより、ICカード端末8は、識別情報とパスワードを署名支援サーバ5に送信する（ステップ220）。

10

20

30

40

50

【 0 0 9 8 】

署名支援サーバ5は、ICカード端末8から識別情報とパスワードを受信し、識別情報に対応づけられた契約書ファイル10bを検索して、これをパスワードで復号化する。そして、復号化した契約書ファイル10bからハッシュ値を計算する(ステップ225)。

次に、署名支援サーバ5は、暗証番号入力画面データを作成してICカード端末8に送信する(ステップ230)。

【 0 0 9 9 】

ICカード端末8は、暗証番号入力画面データを受信して暗証番号入力画面26をディスプレイに表示する。

ユーザは、暗証番号入力画面26から電子署名用の暗証番号を入力し、送信ボタンを選択する。 10

これにより、ICカード端末8は、暗証番号を署名支援サーバ5に送信する(ステップ235)。

【 0 1 0 0 】

署名支援サーバ5は、暗証番号を受信すると、これをICカード7に送信し、公開鍵証明書(本人確認情報)の送信を要求する(ステップ240)。

ICカード端末8は、当該要求をICカード7に中継し(ステップ245)、ICカード7は、当該要求を受信する。

ICカード7は、受信した暗証番号を認証し、公開鍵証明書(本人確認情報)を署名支援サーバ5に送信する(ステップ250)。 20

ICカード端末8は、公開鍵証明書の送信を中継する(ステップ255)。

【 0 1 0 1 】

署名支援サーバ5は、ICカード7から公開鍵証明書を受信すると、公開鍵証明書に含まれている本人確認情報と、契約書DB14で当該識別情報と対応づけられている本人確認情報とを照合する(ステップ260)。

本人確認情報が照合できない場合、署名支援サーバ5は、エラーメッセージをICカード端末8に送信して処理を終了する。

本人確認情報が照合できた場合、署名支援サーバ5は、暗証番号及びハッシュ値をパラメータとする電子署名指令をICカード7に送信する(ステップ265)。

ICカード端末8は、当該指令をICカード7に中継する(ステップ270)。 30

【 0 1 0 2 】

ICカード7は、署名支援サーバ5から電子署名指令を受けると、暗証番号の確認をした後、ハッシュ値を秘密鍵で暗号化して電子署名を作成し、これを署名支援サーバ5に送信する(ステップ275)。

ICカード端末8は、この送信を中継する(ステップ280)。

【 0 1 0 3 】

署名支援サーバ5は、ICカード7から電子署名を受信すると、これを復号化後の契約書ファイル10bに添付して契約書ファイル10cを生成し、中継サーバ3に送信する(ステップ285)。

中継サーバ3は、署名支援サーバ5から電子署名済みの契約書ファイル10cを受信すると、これを契約書ファイル10aの送信元の業務サーバ2に送信する(ステップ290)。 40

業務サーバ2は、電子署名済みの契約書ファイル10cを受信して記憶する(ステップ295)。

【 0 1 0 4 】

以上のようにして、電子郵便システム1は、業務サーバ2が私書箱サーバ4に宛てて送信した電子郵便物に対応して電子署名を付与することができる。

また、業務サーバ2は、契約書等に対するユーザの合意意志が反映された書類である、署名付きの電子郵便物を受領することで、当該電子郵便物に対するユーザの意思を得ることができる。 50

【 0 1 0 5 】

更に、ユーザがリーダライタを介してICカード7を通信ネットワークに接続する設備を有しない場合でも、市中に存在する公共のICカード端末8を用いて電子署名することができる。

【 0 1 0 6 】

(変形例1)

例えば、金融機関の連帯保証契約や賃貸契約など、一つの契約書に複数人の同意が必要な契約が広く行われている。

本変形例は、このように複数人による契約を電子郵便システム1で行う。電子郵便システム1の構成は、実施の形態と同様である。

10

【 0 1 0 7 】

図8は、複数人による契約書ファイルへの電子署名を行う手順を説明するための図である。

この例では、ユーザAが主契約者、ユーザB、Cが連帯契約者とする。図示しないが、ユーザA、B、Cのアカウント13をアカウント13A、13B、13Cとし、ユーザA、B、Cが使用するICカード端末8をICカード端末8A、8B、8Cとする。ICカード端末8A、8B、8Cは、同じICカード端末8であっても異なるICカード端末8であってもよい。

【 0 1 0 8 】

また、契約書ファイルの暗号化や本人確認手法は、実施の形態と同様であり、以下では、煩雑化をさけるため、これらの処理を省略し、複数人が契約書ファイルに電子署名する手順の骨子を図中の括弧で示した番号に従って説明する。

20

【 0 1 0 9 】

まず、業務サーバ2は、契約書ファイル10aと、これに電子署名するユーザのアカウント13A、13B、13Cを規定した署名者リスト300を中継サーバ3に送信する(1)。

電子郵便システム1は、署名者リスト300に登録されたユーザA、B、Cの順で電子署名を行い、主契約者であるユーザAが最初の電子署名を行うようになっている。

このように、原本ファイル(契約書ファイル10a)には、複数の電子私書箱アカウントが対応づけられており、中継サーバ3は、当該複数の電子私書箱アカウントのリスト(署名者リスト300)を取得するリスト取得手段を備えている。

30

【 0 1 1 0 】

中継サーバ3は、契約書ファイル10aを複製して契約書ファイル10dを生成すると共に、これらに対応する識別情報Aを生成する。

そして、中継サーバ3は、署名者リスト300を参照して、契約書ファイル10aと識別情報Aを対応づけて私書箱サーバ4のアカウント13Aに送信し(2)、契約書ファイル10dと識別情報Aを対応づけて署名支援サーバ5に送信する(3)。

【 0 1 1 1 】

ユーザAは、アカウント13Aで契約書ファイル10aを閲覧し、識別情報Aを控える。そして、ユーザAは、ICカード端末8Aを設置した店舗に赴き、ICカード端末8Aに自己のICカード7Aを接続して、控えた識別情報Aを入力する。

40

署名支援サーバ5は、ユーザAがICカード端末8Aから入力した識別情報Aによって契約書ファイル10dを特定し、これのハッシュ値をICカード7Aに送信して電子署名させて、ICカード端末8Aから当該電子署名を受信する。

そして、署名支援サーバ5は、当該電子署名を契約書ファイル10dに付与してユーザAの電子署名が付与された契約書ファイル10eを生成し、これを中継サーバ3に送信する(4)。

【 0 1 1 2 】

中継サーバ3は、署名支援サーバ5から契約書ファイル10eを受信すると、これを署名者リスト300でユーザAの次に指定されたユーザBに対する原本ファイルとし、契約

50

書ファイル 10 e を複製して契約書ファイル 10 f を生成すると共に、これらに対応する識別情報 B を生成する。

そして、中継サーバ 3 は、署名者リスト 300 を参照して、契約書ファイル 10 e と識別情報 B を私書箱サーバ 4 のアカウント 13 B に送信し (5)、契約書ファイル 10 f と識別情報 B を署名支援サーバ 5 に送信する (6)。

なお、本変形例では、ユーザ A、B、C 用に、それぞれ異なる識別情報 A、B、C を生成するが、同じものでもよい。

【0113】

ユーザ B は、アカウント 13 B で契約書ファイル 10 e を閲覧し、識別情報 B を控える。そして、ユーザ B は、IC カード端末 8 B を設置した店舗に赴き、IC カード端末 8 B に自己の IC カード 7 B を接続して、控えた識別情報 B を入力する。

署名支援サーバ 5 は、ユーザ B が IC カード端末 8 B から入力した識別情報 B によって契約書ファイル 10 f を特定し、これのハッシュ値を IC カード 7 B に送信して電子署名させて、IC カード端末 8 B から当該電子署名を受信する。

そして、署名支援サーバ 5 は、当該電子署名を契約書ファイル 10 f に付与してユーザ A、B の電子署名が付与された契約書ファイル 10 g を生成し、これを中継サーバ 3 に送信する (7)。

【0114】

中継サーバ 3 は、署名支援サーバ 5 から契約書ファイル 10 g を受信すると、これを署名者リスト 300 でユーザ B の次に指定されたユーザ C に対する原本ファイルとし、契約書ファイル 10 g を複製して契約書ファイル 10 h を生成すると共に、これらに対応する識別情報 C を生成する。

そして、中継サーバ 3 は、署名者リスト 300 を参照して、契約書ファイル 10 g と識別情報 C を私書箱サーバ 4 のアカウント 13 C に送信し (8)、契約書ファイル 10 h と識別情報 C を署名支援サーバ 5 に送信する (9)。

【0115】

ユーザ C は、アカウント 13 C で契約書ファイル 10 g を閲覧し、識別情報 C を控える。そして、ユーザ C は、IC カード端末 8 C を設置した店舗に赴き、IC カード端末 8 C に自己の IC カード 7 C を接続して、控えた識別情報 C を入力する。

署名支援サーバ 5 は、ユーザ C が IC カード端末 8 C から入力した識別情報 C によって契約書ファイル 10 h を特定し、これのハッシュ値を IC カード 7 C に送信して電子署名させて、IC カード端末 8 C から当該電子署名を受信する。

そして、署名支援サーバ 5 は、当該電子署名を契約書ファイル 10 h に付与してユーザ A、B、C の電子署名が付与された契約書ファイル 10 i を生成し、これを中継サーバ 3 に送信する (10)。

【0116】

中継サーバ 3 は、署名者リスト 300 に登録されている全員 (ユーザ A、B、C) が電子署名した契約書ファイル 10 i を受信すると、これを業務サーバ 2 に送信する (11)。

このようにして、業務サーバ 2 は、署名者リスト 300 に登録されているユーザ A、B、C が登録順に電子署名した契約書ファイル 10 i を得ることができる。

【0117】

このように中継サーバ 3 が備える署名対象ファイル作成手段は、原本ファイル (契約書ファイル 10 a、10 e、10 g) に対応する複数の署名対象ファイル (契約書ファイル 10 d、10 f、10 h) を作成し、識別情報生成手段は、当該作成した複数の署名対象ファイルのそれぞれに対応させて識別情報 (識別情報 A、B、C) を生成し、署名対象ファイル送信手段は、当該作成した複数の署名対象ファイルを当該生成した識別情報と対応させて署名支援サーバ 5 に送信している。

【0118】

更に、中継サーバ 3 の原本ファイル送信手段は、取得した原本ファイル (契約書ファイ

10

20

30

40

50

ル 10 a とこれから生成した契約書ファイル 10 e、10 g) と生成した識別情報 (識別情報 A、B、C) を対応させて、取得した署名者リスト 300 に含まれる複数の電子私書箱アカウント (アカウント 13 A、13 B、13 C) に送信している。

【 0 1 1 9 】

変形例 1 では、ユーザ B は、ユーザ A が電子署名した契約書ファイル 10 e に電子署名し、ユーザ C は、ユーザ A、B が電子署名した契約書ファイル 10 g に電子署名するため、例えば、ユーザ A が電子署名したことを条件としてユーザ B が電子署名するといったように、電子署名の順序が契約の効力発生要件となっている場合に有効である。

【 0 1 2 0 】

また、変形例 1 では、ユーザ A、B、C が私書箱サーバ 4 にアカウント 13 を持っていることが前提となっているが、アカウント 13 を持っていないユーザがいる場合でも実施することができる。

例えば、ユーザ A がアカウント 13 を持っており、ユーザ B、C がアカウント 13 を持っていない場合は、ユーザ A のアカウントにユーザ B、C 用の識別情報 B、C を通知し、ユーザ A が識別情報 B、C をユーザ B、C に個別に伝えるなどする。

【 0 1 2 1 】

このように、アカウント 13 を持っていないユーザであっても IC カード 7 さえ保有していれば、別途識別情報を得ることにより電子署名することができる。

更に、電子署名は、通信ネットワークを介して行われるため、複数のユーザは、互いに顔を合わさずに一つの契約書ファイル 10 に電子署名することができる。

【 0 1 2 2 】

(変形例 2)

変形例 1 では、ユーザ A ユーザ B ユーザ C の順に電子署名を重ねていったが、本変形例では、複数のユーザ A、B、C に平行して契約書ファイル 10 を送信して電子署名させる。

図 9 は、複数人が平行して契約書ファイル 10 に電子署名を行う手順を説明するための図である。

まず、業務サーバ 2 は、契約書ファイル 10 a と、これに電子署名するユーザのアカウント 13 A、13 B、13 C の署名者リスト 300 を中継サーバ 3 に送信する (1) 。

電子郵便システム 1 は、署名者リスト 300 に登録されたユーザ A、B、C に対して同時に平行して電子署名を行わせる。

【 0 1 2 3 】

中継サーバ 3 は、契約書ファイル 10 a をアカウント 13 用に複製して電子署名するユーザの人数分だけ用意し、それぞれのユーザ用に識別情報 A、B、C を生成する。なお、識別情報は、ユーザごとに異なる値とする。

更に、中継サーバ 3 は、電子署名用に契約書ファイル 10 a をユーザの人数分だけ複製して契約書ファイル 10 j を生成する。

以下では、3つの契約書ファイル 10 a と契約書ファイル 10 j を契約書ファイル 10 a 1、契約書ファイル 10 a 2、契約書ファイル 10 a 3、及び、契約書ファイル 10 j 1、契約書ファイル 10 j 2、契約書ファイル 10 j 3 とする。

【 0 1 2 4 】

そして、中継サーバ 3 は、署名者リスト 300 を参照して、契約書ファイル 10 a 1 と識別情報 A を対応させて私書箱サーバ 4 のアカウント 13 A に送信し、契約書ファイル 10 a 2 と識別情報 B を対応させて私書箱サーバ 4 のアカウント 13 B に送信し、契約書ファイル 10 a 3 と識別情報 C を対応させて私書箱サーバ 4 のアカウント 13 C に送信する (2) 。

更に、中継サーバ 3 は、契約書ファイル 10 j 1 と識別情報 A を対応させ、契約書ファイル 10 j 2 と識別情報 B を対応させ、及び契約書ファイル 10 j 3 と識別情報 C を対応させて署名支援サーバ 5 に送信する (3) 。

【 0 1 2 5 】

10

20

30

40

50

ユーザ A は、アカウント 13 A で契約書ファイル 10 a 1 を閲覧し、識別情報 A を控える。そして、ユーザ A は、IC カード端末 8 A を設置した店舗に赴き、IC カード端末 8 A に自己の IC カード 7 A を接続して、控えた識別情報 A を入力する。

署名支援サーバ 5 は、ユーザが IC カード端末 8 A から入力した識別情報 A によってこれと対応する契約書ファイル 10 j 1 を特定し、これのハッシュ値を IC カード 7 A に送信して電子署名させることにより、ユーザ A の電子署名が付与された契約書ファイル 10 k を生成して中継サーバ 3 に送信する (4)。

【0126】

ユーザ B は、アカウント 13 B で契約書ファイル 10 a 2 を閲覧し、識別情報 B を控える。そして、ユーザ B は、IC カード端末 8 B を設置した店舗に赴き、IC カード端末 8 B に自己の IC カード 7 B を接続して、控えた識別情報 B を入力する。

署名支援サーバ 5 は、ユーザ B が IC カード端末 8 B から入力した識別情報 B によってこれと組を成す契約書ファイル 10 j 2 を特定し、これのハッシュ値を IC カード 7 B に送信して電子署名させることにより、ユーザ B の電子署名が付与された契約書ファイル 10 l を生成して中継サーバ 3 に送信する (5)。

【0127】

ユーザ C は、アカウント 13 C で契約書ファイル 10 a 3 を閲覧し、識別情報 C を控える。そして、ユーザ C は、IC カード端末 8 C を設置した店舗に赴き、IC カード端末 8 C に自己の IC カード 7 C を接続して、控えた識別情報 C を入力する。

署名支援サーバ 5 は、ユーザ C が IC カード端末 8 C から入力した識別情報 C によってこれと組を成す契約書ファイル 10 j 3 を特定し、これのハッシュ値を IC カード 7 C に送信して電子署名させることにより、ユーザ C の電子署名が付与された契約書ファイル 10 m を生成して中継サーバ 3 に送信する (6)。

【0128】

中継サーバ 3 は、署名支援サーバ 5 から契約書ファイル 10 k、10 l、10 m を受信すると、これらを結合して契約書ファイル 10 n を生成し (7)、業務サーバ 2 に送信する (8)。

以上のようにして、本変形例では、署名者リスト 300 の記載順序に関係なく、複数のユーザが個別に電子署名するため、迅速に契約書ファイル 10 n を得ることができる。

【0129】

ところで、例えば、契約者 A がローンの借手で契約者 B、C が連帯保証人であるといったように、複数の契約者の間で主従関係がある場合は、変形例 1 と変形例 2 を組み合わせればよい。

この場合、電子郵便システム 1 は、まず、契約書ファイル 10 に対して主契約者の電子署名を取得する。

【0130】

そして、契約書ファイル 10 a に主契約者の電子署名を付与して契約書ファイル 10 o を生成し、契約書ファイル 10 o を複数の従契約者に対して平行に送信してこれらの電子署名を取得する。

そして、従契約者の電子署名を付与した契約書ファイル 10 p、10 q、・・・を生成して、これらを一つに結合する。

【0131】

以上の実施の形態、及び変形例によれば、電子私書箱サービスでの閲覧書類に対する署名サービスを提供することができる。

(1) 重要情報の漏洩や改ざんを防止するために、電子データをシステムへ連携する前に、あらかじめ電子署名、タイムスタンプを付与するとともに、ユーザが検索キーとなる識別情報を入力しない限り電子データを特定しないので、電子データを暗号化した状態のままとすることができる。

(2) システム連携時には暗号化されたままの状態データ連携を行い、実際にユーザが、合意の電子署名を行う際に、ユーザが識別情報を入力することで、ユーザのみがデータ

10

20

30

40

50

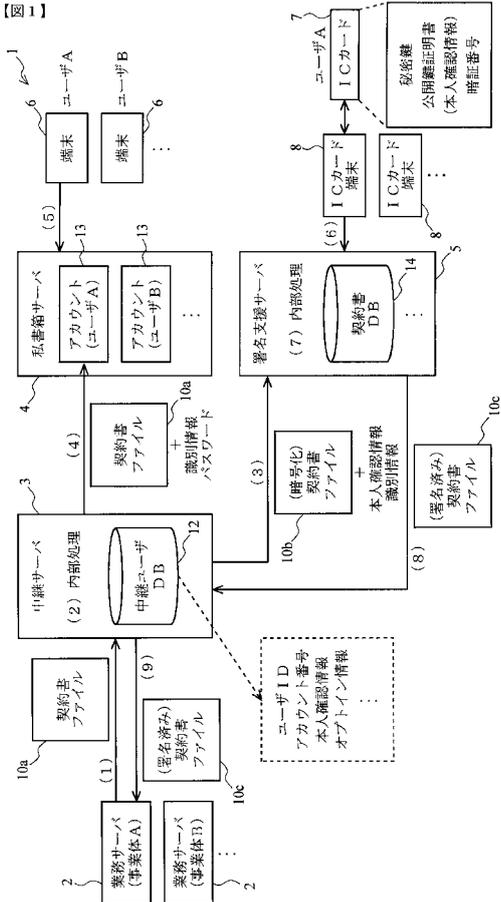
を連携システムでデータを閲覧できる状態として署名処理を実行することができる。

【符号の説明】

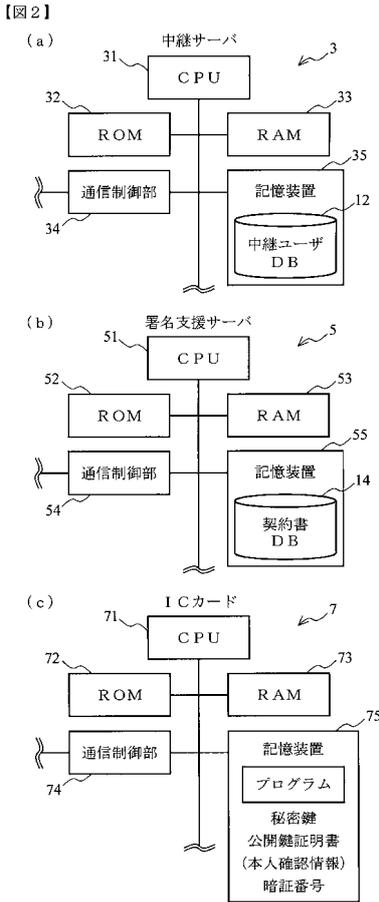
【0132】

1	電子郵便システム	
2	業務サーバ	
3	中継サーバ	
4	私書箱サーバ	
5	署名支援サーバ	
6	端末	
7	ICカード	10
8	ICカード端末	
10、10a~q	契約書ファイル	
12	中継ユーザDB	
13	アカウント	
14	契約書DB	
21	電子郵便閲覧画面	
22	識別情報	
23	パスワード	
24	識別情報入力画面	
26	暗証番号入力画面	20
31	CPU	
32	ROM	
33	RAM	
34	通信制御部	
35	記憶装置	
51	CPU	
52	ROM	
53	RAM	
54	通信制御部	
55	記憶装置	30
71	CPU	
72	ROM	
73	RAM	
74	通信制御部	
75	記憶装置	
300	署名者リスト	

【図1】



【図2】



【図3】

【図3】

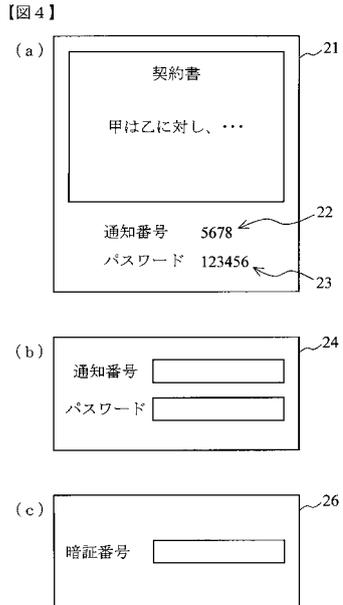
(a) 中継ユーザDB

ユーザID	アカウント番号	本人確認情報	オプトイン情報	...
12345	ACS67	基本4情報
⋮	⋮	⋮	⋮	⋮

(b) 契約書DB

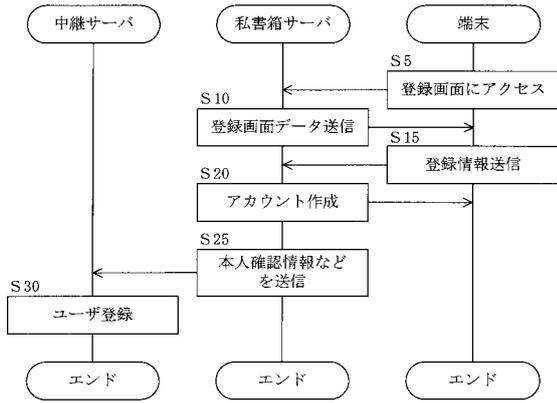
識別情報	契約書ファイル	本人確認情報	...
5678	...	基本4情報	...
⋮	⋮	⋮	⋮

【図4】



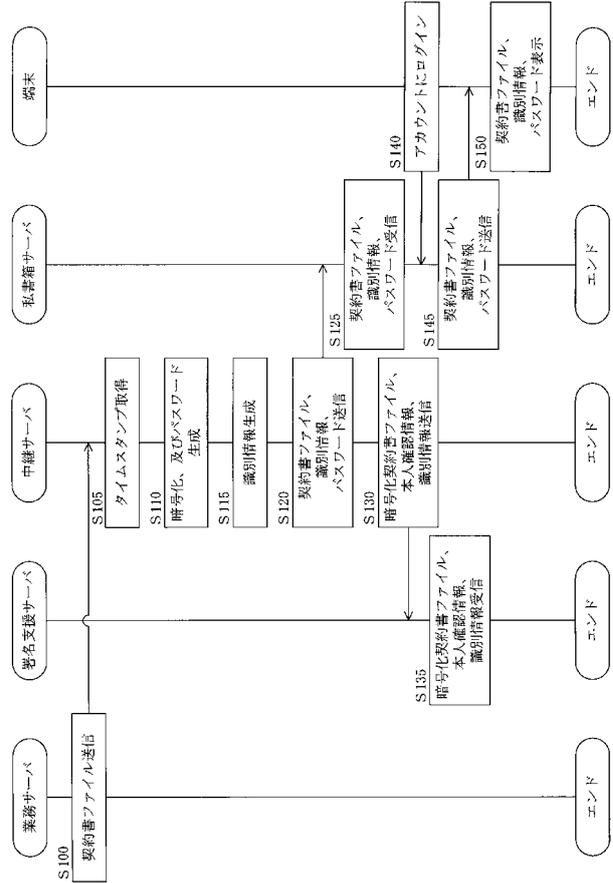
【図5】

【図5】



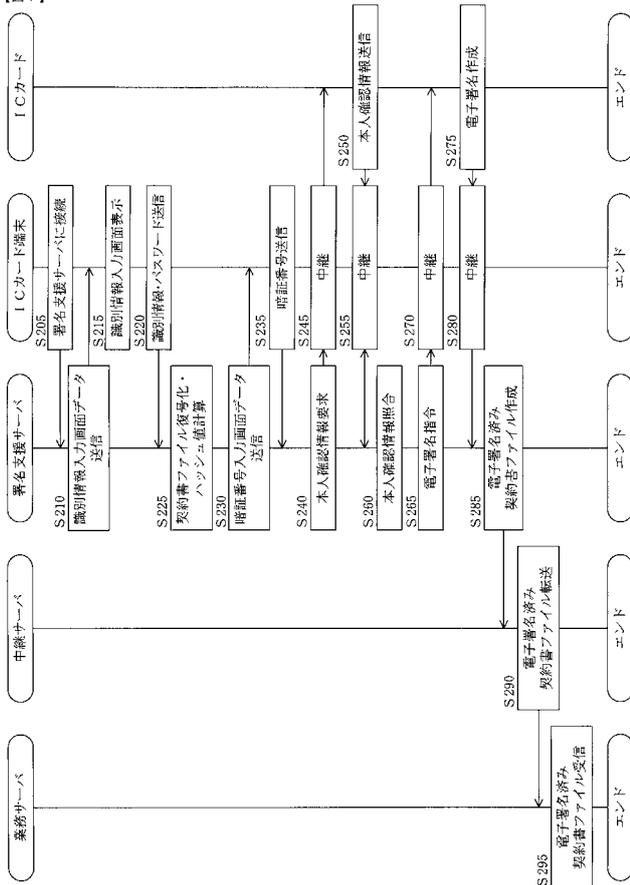
【図6】

【図6】



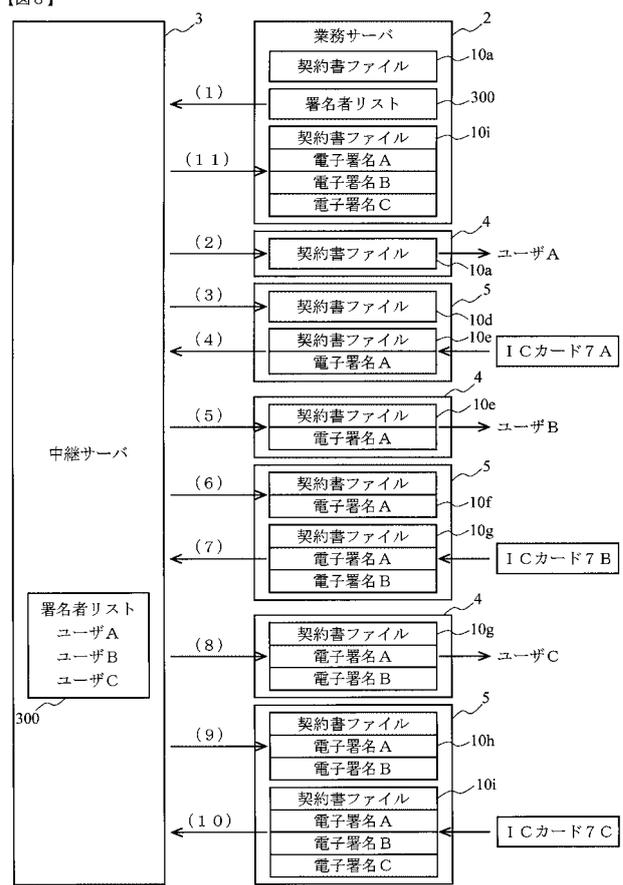
【図7】

【図7】



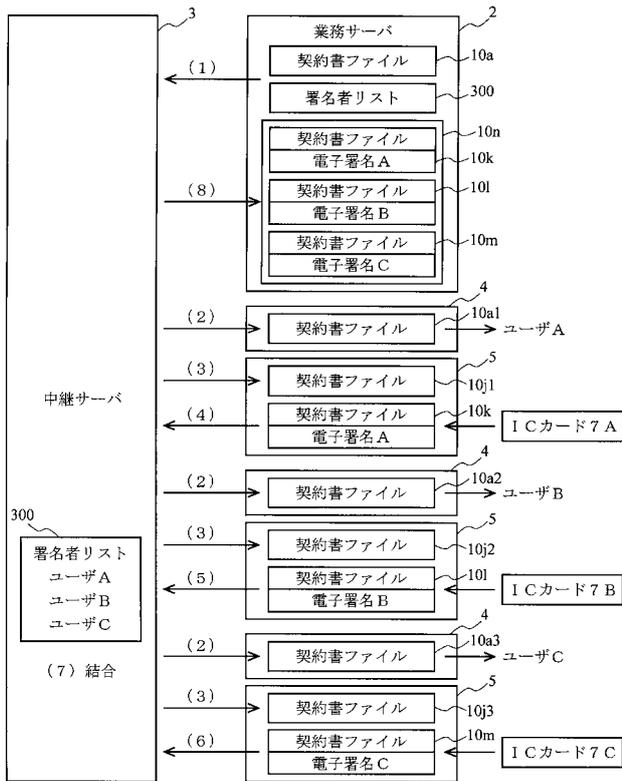
【図8】

【図8】



【図 9】

【図 9】



フロントページの続き

(51) Int.Cl.			F I			テーマコード(参考)
G 0 9 C	1/00	(2006.01)	G 0 9 C	1/00	6 4 0 D	