

(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2017-108239

(P2017-108239A)

(43) 公開日 平成29年6月15日(2017.6.15)

(51) Int.Cl.		F I				テーマコード (参考)
H04L	9/32	(2006.01)	H04L	9/00	675B	5J104
G09C	1/00	(2006.01)	G09C	1/00	640E	
G06F	21/33	(2013.01)	H04L	9/00	673A	
G06F	21/31	(2013.01)	G06F	21/33		
			G06F	21/31		

審査請求 未請求 請求項の数 9 O L (全 24 頁)

(21) 出願番号	特願2015-239345 (P2015-239345)	(71) 出願人	000208891
(22) 出願日	平成27年12月8日 (2015.12.8)		KDDI株式会社
			東京都新宿区西新宿二丁目3番2号
		(74) 代理人	100106909
			弁理士 棚井 澄雄
		(74) 代理人	100064908
			弁理士 志賀 正武
		(74) 代理人	100146835
			弁理士 佐伯 義文
		(72) 発明者	竹森 敬祐
			東京都新宿区西新宿二丁目3番2号 KDDI株式会社内
		(72) 発明者	本間 輝彰
			東京都新宿区西新宿二丁目3番2号 KDDI株式会社内

最終頁に続く

(54) 【発明の名称】 通信システム、端末装置、通信装置、通信方法、及びプログラム

(57) 【要約】

【課題】 簡易な構成で端末装置の二要素認証を実現すること。

【解決手段】 通信装置との間で通信を行う端末装置は、クライアント公開鍵証明書と、クライアント公開鍵証明書に登録されている公開鍵とペアをなす秘密鍵とを格納し、通信装置にログインを要求し、ログインの要求に応じて、通信装置によって送信される認証処理の結果に基づいて、通信装置へクライアント公開鍵証明書を送信する制御を行い、通信装置によって送信されるチャレンジを受信し、チャレンジを秘密鍵で暗号化することによってレスポンスを生成し、レスポンスを通信装置へ送信する。

【選択図】 図1

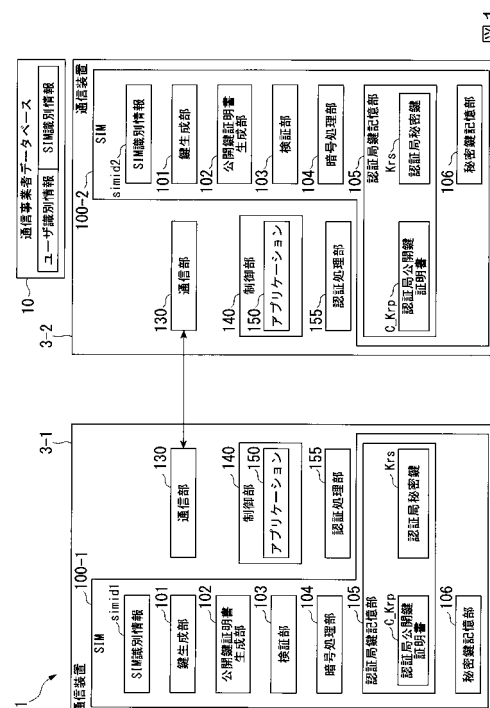


図1

【特許請求の範囲】

【請求項 1】

端末装置と、該端末装置との間で通信を行う通信装置とを有する通信システムであって、

前記端末装置は、

クライアント公開鍵証明書と、該クライアント公開鍵証明書に登録されている公開鍵とペアをなす秘密鍵とを格納する第 1 の記憶部と、

前記通信装置にログインを要求するログイン要求部と、

前記ログインの要求に応じて、前記通信装置によって送信される認証処理の結果に基づいて、前記通信装置へ前記第 1 の記憶部に格納した前記クライアント公開鍵証明書を送信する制御を行う第 1 の通信制御部と、

前記通信装置によって送信されるチャレンジを前記秘密鍵で暗号化することによってレスポンスを生成する暗号化部と

を備え、

前記第 1 の通信制御部は、前記通信装置によって送信されるチャレンジを受信する制御を行い、且つ前記暗号化部によって生成したレスポンスを前記通信装置へ送信する制御を行い、

前記通信装置は、

認証局の公開鍵証明書を格納する第 2 の記憶部と、

前記端末装置によって送信された前記ログインの要求に基づいて、前記端末装置の認証処理を行う第 1 の認証部と、

前記第 1 の認証部によって行われた前記認証処理の結果を前記端末装置に送信する制御を行う第 2 の通信制御部と、

前記端末装置によって送信されたクライアント公開鍵証明書と、前記第 2 の記憶部に格納した前記認証局の公開鍵証明書とに基づいて、該公開鍵証明書に登録されている公開鍵で前記クライアント公開鍵証明書を復号することによって検証する検証部と、

前記検証部によって前記検証が成功した場合にチャレンジを生成し、前記端末装置によって送信されたレスポンスを前記公開鍵で検証する第 2 の認証部と

を備え、

前記第 2 の通信制御部は、前記第 2 の認証部によって生成したチャレンジを前記端末装置へ送信する制御を行い、且つ該端末装置によって送信されたレスポンスを受信する制御を行う、通信システム。

【請求項 2】

前記端末装置は、

前記クライアント公開鍵証明書を発行する認証局

を備える、請求項 1 に記載の通信システム。

【請求項 3】

前記通信装置は、

前記第 1 の認証部は、前記端末装置の認証処理が成功した場合に所定期間の間有効なトークンを発行し、

前記第 2 の認証部は、前記第 1 の認証部によって発行された前記トークンに基づいて、前記端末装置によって送信されたレスポンスを前記公開鍵で検証する、請求項 1 又は 2 に記載の通信システム。

【請求項 4】

前記第 1 の認証部によって行われる前記認証処理が失敗した場合又は前記第 2 の認証部によって行われる検証が失敗した場合に、予め設定された通知先に通知する通知部

を備える、請求項 1 から請求項 3 のいずれか 1 項に記載の通信システム。

【請求項 5】

通信装置との間で通信を行う端末装置であって、

クライアント公開鍵証明書と、該クライアント公開鍵証明書に登録されている公開鍵と

ペアをなす秘密鍵とを格納する記憶部と、

前記通信装置にログインを要求するログイン要求部と、

前記ログインの要求に応じて、前記通信装置によって送信される認証処理の結果に基づいて、前記通信装置へ前記記憶部に格納した前記クライアント公開鍵証明書を送信する制御を行う通信制御部と、

前記通信装置によって送信されるチャレンジを前記秘密鍵で暗号化することによってレスポンスを生成する暗号化部と

を有し、

前記通信制御部は、前記通信装置によって送信されるチャレンジを受信する制御を行い、且つ前記暗号化部によって生成したレスポンスを前記通信装置へ送信する制御を行う、
端末装置。

10

【請求項 6】

端末装置との間で通信を行う通信装置であって、

認証局の公開鍵証明書を格納する記憶部と、

前記端末装置によって送信されたログインの要求に基づいて、前記端末装置の認証処理を行う認証部と、

前記認証部によって行われた前記認証処理の結果を前記端末装置に送信する制御を行う通信制御部と、

前記端末装置によって送信されたクライアント公開鍵証明書と、前記記憶部に格納した前記認証局の公開鍵証明書とに基づいて、該公開鍵証明書に登録されている公開鍵で前記クライアント公開鍵証明書を復号することによって検証する検証部と、

20

前記検証部によって前記検証が成功した場合にチャレンジを生成し、前記端末装置によって送信されたレスポンスを前記公開鍵で検証する認証部と

を備え、

前記通信制御部は、前記認証部によって生成したチャレンジを前記端末装置へ送信する制御を行い、且つ該端末装置によって送信されたレスポンスを受信する制御を行う、通信装置。

【請求項 7】

端末装置と、該端末装置との間で通信を行う通信装置によって実行される通信方法であって、

30

前記端末装置は、クライアント公開鍵証明書と、該クライアント公開鍵証明書に登録されている公開鍵とペアをなす秘密鍵を格納し、

前記通信装置は、認証局の公開鍵証明書を格納し、

前記端末装置は、前記通信装置にログインを要求し、

前記通信装置は、前記端末装置によって送信された前記ログインの要求に基づいて、前記端末装置の認証処理を行い、

前記通信装置は、前記認証処理の結果を前記端末装置に送信し、

前記端末装置は、前記ログインの要求に応じて前記通信装置によって送信される認証処理の結果に基づいて、前記通信装置へ前記クライアント公開鍵証明書を送信し、

前記通信装置は、前記端末装置によって送信されたクライアント公開鍵証明書と、前記認証局の公開鍵証明書とに基づいて、該公開鍵証明書に登録されている公開鍵で前記クライアント公開鍵証明書を復号することによって検証し、

40

前記通信装置は、前記検証が成功した場合にチャレンジを生成し、

前記通信装置は、該チャレンジを前記端末装置へ送信し、

前記端末装置は、前記通信装置によって送信されるチャレンジを受信し、

前記端末装置は、該チャレンジを前記秘密鍵で暗号化し、

前記端末装置は、該暗号化したチャレンジを前記通信装置へ送信し、

前記通信装置は、該端末装置によって送信されたレスポンスを受信し、

前記通信装置は、該端末装置によって送信されたレスポンスを前記公開鍵で検証する、通信方法。

50

【請求項 8】

通信装置との間で通信を行う端末装置に、
クライアント公開鍵証明書と、該クライアント公開鍵証明書に登録されている公開鍵とペアをなす秘密鍵とを格納させ、
前記通信装置にログインを要求させ、
前記ログインの要求に応じて、前記通信装置によって送信される認証処理の結果に基づいて、前記通信装置へ前記クライアント公開鍵証明書を送信する制御を行わせ、
前記通信装置によって送信されるチャレンジを受信させ、
前記チャレンジを前記秘密鍵で暗号化させることによってレスポンスを生成させ、
該レスポンスを前記通信装置へ送信させる、プログラム。

10

【請求項 9】

端末装置との間で通信を行う通信装置に、
認証局の公開鍵証明書を格納させ、
前記端末装置によって送信されたログインの要求に基づいて、前記端末装置の認証処理を行わせ、
前記認証処理の結果を前記端末装置に送信する制御を行わせ、
前記端末装置によって送信されたクライアント公開鍵証明書と、認証局の公開鍵証明書とに基づいて、該公開鍵証明書に登録されている公開鍵で前記クライアント公開鍵証明書を復号することによって検証させ、
該検証が成功した場合にチャレンジを生成させ、
該生成したチャレンジを前記端末装置へ送信させ、
該端末装置によって送信されたレスポンスを受信させ、
該端末装置によって送信されたレスポンスを前記公開鍵で検証させる、プログラム。

20

【発明の詳細な説明】

【技術分野】

【0001】

本発明の実施形態は、通信システム、端末装置、通信装置、通信方法、及びプログラムに関する。

【背景技術】

【0002】

ネット銀行（Direct bank）やネットショップ（EC（electronic commerce））サイトでのログインや決済などの重要な処理において、IDとパスワードとを使用した認証に加えて、乱数表やハードウェアトークンの文字列を回答させて、二要素認証を行う技術が知られている（例えば、非特許文献 1、2 参照）。

30

【先行技術文献】

【非特許文献】

【0003】

【非特許文献 1】“eセキュリティカード（乱数表カード）”、[online]、株式会社東京スター銀行、[平成 27 年 12 月 1 日検索]、インターネット<URL: http://www.tokyostarbank.co.jp/service/tokyostardirect/e_security/>

40

【非特許文献 2】“HARDEARE TOKENS”、[online]、EMC ジャパン株式会社、[平成 27 年 12 月 1 日検索]、インターネット<URL: <http://japan.emc.com/security/rsa-securid/rsa-securid-hardware-tokens.htm>>

【発明の概要】

【発明が解決しようとする課題】

【0004】

乱数表の文字列を入力させることによって認証を行う場合、ユーザに偽の Web サイトへアクセスさせ、該 Web サイトで乱数表の文字列を入力させるなどして、該乱数表の内

50

容を盗み出す攻撃が問題となっている。

また、ハードウェアトークンの文字列を入力させる場合、安全性は高いもののハードウェアトークンの調達や、配布にコストを要する問題がある。

【0005】

本発明は、このような事情を考慮してなされたものであり、簡易な構成で端末装置の二要素認証を実現する通信システム、端末装置、通信装置、通信方法、及びプログラムを提供することを目的とする。

【課題を解決するための手段】

【0006】

(1) 本発明の一態様は、端末装置と、該端末装置との間で通信を行う通信装置とを有する通信システムであって、前記端末装置は、クライアント公開鍵証明書と、該クライアント公開鍵証明書に登録されている公開鍵とペアをなす秘密鍵とを格納する第1の記憶部と、前記通信装置にログインを要求するログイン要求部と、前記ログインの要求に応じて、前記通信装置によって送信される認証処理の結果に基づいて、前記通信装置へ前記第1の記憶部に格納した前記クライアント公開鍵証明書を送信する制御を行う第1の通信制御部と、前記通信装置によって送信されるチャレンジを前記秘密鍵で暗号化することによってレスポンスを生成する暗号化部とを備え、前記第1の通信制御部は、前記通信装置によって送信されるチャレンジを受信する制御を行い、且つ前記暗号化部によって生成したレスポンスを前記通信装置へ送信する制御を行い、前記通信装置は、認証局の公開鍵証明書を格納する第2の記憶部と、前記端末装置によって送信された前記ログインの要求に基づいて、前記端末装置の認証処理を行う第1の認証部と、前記第1の認証部によって行われた前記認証処理の結果を前記端末装置に送信する制御を行う第2の通信制御部と、前記端末装置によって送信されたクライアント公開鍵証明書と、前記第2の記憶部に格納した前記認証局の公開鍵証明書とに基づいて、該公開鍵証明書に登録されている公開鍵で前記クライアント公開鍵証明書を復号することによって検証する検証部と、前記検証部によって前記検証が成功した場合にチャレンジを生成し、前記端末装置によって送信されたレスポンスを前記公開鍵で検証する第2の認証部とを備え、前記第2の通信制御部は、前記第2の認証部によって生成したチャレンジを前記端末装置へ送信する制御を行い、且つ該端末装置によって送信されたレスポンスを受信する制御を行う、通信システムである。

【0007】

(2) 本発明の一態様は、上記(1)に記載の通信システムにおいて、前記端末装置は、前記クライアント公開鍵証明書を発行する認証局を備える通信システムである。

【0008】

(3) 本発明の一態様は、上記(1)または(2)に記載の通信システムにおいて、前記通信装置は、前記第1の認証部は、前記端末装置の認証処理が成功した場合に所定期間の間有効なトークンを発行し、前記第2の認証部は、前記第1の認証部によって発行された前記トークンに基づいて、前記端末装置によって送信されたレスポンスを前記公開鍵で検証する、通信システムである。

【0009】

(4) 本発明の一態様は、上記(1)から(3)のいずれか1項に記載の通信システムにおいて、前記第1の認証部によって行われる前記認証処理が失敗した場合又は前記第2の認証部によって行われる検証が失敗した場合に、予め設定された通知先に通知する通知部を備える、通信システムである。

【0010】

(5) 本発明の一態様は、通信装置との間で通信を行う端末装置であって、クライアント公開鍵証明書と、該クライアント公開鍵証明書に登録されている公開鍵とペアをなす秘密鍵とを格納する記憶部と、前記通信装置にログインを要求するログイン要求部と、前記ログインの要求に応じて、前記通信装置によって送信される認証処理の結果に基づいて、前記通信装置へ前記記憶部に格納した前記クライアント公開鍵証明書を送信する制御を行う通信制御部と、前記通信装置によって送信されるチャレンジを前記秘密鍵で暗号化するこ

とによってレスポンスを生成する暗号化部とを有し、前記通信制御部は、前記通信装置によって送信されるチャレンジを受信する制御を行い、且つ前記暗号化部によって生成したレスポンスを前記通信装置へ送信する制御を行う、端末装置である。

【0011】

(6) 本発明の一態様は、端末装置との間で通信を行う通信装置であって、認証局の公開鍵証明書を格納する記憶部と、前記端末装置によって送信されたログインの要求に基づいて、前記端末装置の認証処理を行う認証部と、前記認証部によって行われた前記認証処理の結果を前記端末装置に送信する制御を行う通信制御部と、前記端末装置によって送信されたクライアント公開鍵証明書と、前記記憶部に格納した前記認証局の公開鍵証明書とに基づいて、該公開鍵証明書に登録されている公開鍵で前記クライアント公開鍵証明書を復号することによって検証する検証部と、前記検証部によって前記検証が成功した場合にチャレンジを生成し、前記端末装置によって送信されたレスポンスを前記公開鍵で検証する認証部とを備え、前記通信制御部は、前記認証部によって生成したチャレンジを前記端末装置へ送信する制御を行い、且つ該端末装置によって送信されたレスポンスを受信する制御を行う、通信装置である。

10

【0012】

(7) 本発明の一態様は、端末装置と、該端末装置との間で通信を行う通信装置によって実行される通信方法であって、前記端末装置は、クライアント公開鍵証明書と、該クライアント公開鍵証明書に登録されている公開鍵とペアをなす秘密鍵を格納し、前記通信装置は、認証局の公開鍵証明書を格納し、前記端末装置は、前記通信装置にログインを要求し、前記通信装置は、前記端末装置によって送信された前記ログインの要求に基づいて、前記端末装置の認証処理を行い、前記通信装置は、前記認証処理の結果を前記端末装置に送信し、前記端末装置は、前記ログインの要求に応じて前記通信装置によって送信される認証処理の結果に基づいて、前記通信装置へ前記クライアント公開鍵証明書を送信し、前記通信装置は、前記端末装置によって送信されたクライアント公開鍵証明書と、前記認証局の公開鍵証明書とに基づいて、該公開鍵証明書に登録されている公開鍵で前記クライアント公開鍵証明書を復号することによって検証し、前記通信装置は、前記検証が成功した場合にチャレンジを生成し、前記通信装置は、該チャレンジを前記端末装置へ送信し、前記端末装置は、前記通信装置によって送信されるチャレンジを受信し、前記端末装置は、該チャレンジを前記秘密鍵で暗号化し、前記端末装置は、該暗号化したチャレンジを前記通信装置へ送信し、前記通信装置は、該端末装置によって送信されたレスポンスを受信し、前記通信装置は、該端末装置によって送信されたレスポンスを前記公開鍵で検証する、通信方法である。

20

30

【0013】

(8) 本発明の一態様は、通信装置との間で通信を行う端末装置に、クライアント公開鍵証明書と、該クライアント公開鍵証明書に登録されている公開鍵とペアをなす秘密鍵とを格納させ、前記通信装置にログインを要求させ、前記ログインの要求に応じて、前記通信装置によって送信される認証処理の結果に基づいて、前記通信装置へ前記クライアント公開鍵証明書を送信する制御を行わせ、前記通信装置によって送信されるチャレンジを受信させ、前記チャレンジを前記秘密鍵で暗号化させることによってレスポンスを生成させ、該レスポンスを前記通信装置へ送信させる、プログラムである。

40

【0014】

(9) 本発明の一態様は、端末装置との間で通信を行う通信装置に、認証局の公開鍵証明書を格納させ、前記端末装置によって送信されたログインの要求に基づいて、前記端末装置の認証処理を行わせ、前記認証処理の結果を前記端末装置に送信する制御を行わせ、前記端末装置によって送信されたクライアント公開鍵証明書と、認証局の公開鍵証明書とに基づいて、該公開鍵証明書に登録されている公開鍵で前記クライアント公開鍵証明書を復号することによって検証させ、該検証が成功した場合にチャレンジを生成させ、該生成したチャレンジを前記端末装置へ送信させ、該端末装置によって送信されたレスポンスを受信させ、該端末装置によって送信されたレスポンスを前記公開鍵で検証させる、プログラ

50

ムである。

【発明の効果】

【0015】

本発明の実施形態によれば、簡易な構成で端末装置の二要素認証を実現することができる。

【図面の簡単な説明】

【0016】

【図1】第1実施形態に係る通信システム1を示す構成図である。

【図2】第1実施形態に係る通信方法の説明図である。

【図3】第2実施形態に係る通信システム1を示す構成図である。

【図4】第3実施形態に係る通信システム1を示す構成図である。

【図5】第3実施形態の実施例1に係る通信システム1を示す説明図である。

【図6】第3実施形態の実施例2に係る通信システム1を示す説明図である。

【図7】変形例に係る通信装置、通信端末を示す説明図である。

【発明を実施するための形態】

【0017】

次に、本発明を実施するための形態を、図面を参照しつつ説明する。以下で説明する実施形態は一例に過ぎず、本発明が適用される実施形態は、以下の実施形態に限られない。

なお、実施形態を説明するための全図において、同一の機能を有するものは同一符号を用い、繰り返しの説明は省略する。

【0018】

〔第1実施形態〕

図1は、第1実施形態に係る通信システム1を示す構成図である。図1において、通信システム1は、通信装置3-1と通信装置3-2を備える。通信装置3-1は、SIM (Subscriber Identity Module) 100-1と、通信部130と、制御部140とを備える。SIM 100-1はSIM識別情報simid1を格納する。SIM識別情報simid1は、SIM 100-1に固有の識別情報である。SIM 100-1は、鍵生成部101と、公開鍵証明書生成部102と、検証部103と、暗号処理部104と、認証局鍵記憶部105と、秘密鍵記憶部106と、ログイン処理部107とを備える。

【0019】

通信装置3-2は通信装置3-1と同様の構成である。図1に示す通信装置3-2において、通信装置3-1の各部に対応する部分には同一の符号を付している。以下の説明において、通信装置3-1と通信装置3-2とを特に区別しないときは「通信装置3」と称する。なお、1つの通信装置3が複数のSIMを備えてもよい。例えば、通信装置3は、複数のSIMスロットを具備し、各SIMスロットに挿入されたSIMに対応する通信ネットワークの中から任意の通信ネットワークに接続先を切り替えることができる通信装置であってもよい。

【0020】

通信装置3-2は、SIM 100-2を備える。SIM 100-2はSIM識別情報simid2を格納する。SIM識別情報simid2は、SIM 100-2に固有の識別情報である。

【0021】

SIM 100-1は、通信事業者が認証したユーザに対して発行されたSIMである。SIM 100-1のSIM識別情報simid1は、通信事業者が認証したユーザのユーザ識別情報に関連付けて通信事業者データベース10に格納されている。SIM 100-2も、SIM 100-1と同様に、通信事業者が認証したユーザに対して発行されたSIMである。SIM 100-2のSIM識別情報simid2は、通信事業者が認証したユーザのユーザ識別情報に関連付けて通信事業者データベース10に格納されている。以下の説明において、SIM 100-1とSIM 100-2とを特に区別しないときは「S I

10

20

30

40

50

M100」と称する。なお、SIM100は、仮想通信事業者（Virtual Network Operator）が認証したユーザに対して発行されたSIMであってもよい。

【0022】

SIM識別情報として、例えば、IMSI（International Mobile Subscriber Identity）又はICCID（Integrated Circuit Card ID）を使用してもよい。また、SIM100に関連付けられた電話番号を該SIM100のSIM識別情報に使用してもよい。

【0023】

通信装置3-1の通信部130と、通信装置3-2の通信部130とは、通信を行う。通信装置3-1の通信部130と通信装置3-2の通信部130間の通信は、無線通信であってもよく、又は、有線通信であってもよい。例えば、通信装置3-1の通信部130と、通信装置3-2の通信部130とは、無線LANや携帯電話ネットワーク等の無線通信ネットワークを介して通信を行ってもよい。又は、通信装置3-1の通信部130と、通信装置3-2の通信部130とは、近距離無線通信技術により直接に信号を送受して通信を行ってもよい。又は、通信装置3-1の通信部130と、通信装置3-2の通信部130とは、インターネットや固定電話ネットワーク、有線LAN等の通信ネットワークを介して通信を行ってもよい。又は、通信装置3-1の通信部130と、通信装置3-2の通信部130とは、通信ケーブルにより接続されて通信を行ってもよい。

【0024】

通信装置3において、制御部140は、CPU（Central Processing Unit）及びメモリを備えており、通信装置3が備える各部を制御する。制御部140は、その機能部として、アプリケーション150を備える。

【0025】

SIM100は、コンピュータの一種であり、コンピュータプログラムによって所望の機能を実現する。SIM100において、認証局鍵記憶部105は、認証局公開鍵証明書C_Krpと認証局秘密鍵Krsのペアを記憶する。認証局公開鍵証明書C_Krpは、認証局秘密鍵Krsのペアの認証局公開鍵の公開鍵証明書である。認証局公開鍵証明書C_Krpと認証局秘密鍵Krsとは、例えばSIM100の製造時などに、安全にSIM100に格納される。通信装置3-1のSIM100-1に格納される認証局公開鍵証明書C_Krp及び認証局秘密鍵Krsと、通信装置3-2のSIM100-2に格納される認証局公開鍵証明書C_Krp及び認証局秘密鍵Krsとは、同じである。

【0026】

認証局鍵記憶部105は、SIM100内の記憶領域のうち、SIM100の外部からアクセスできない不揮発性記憶領域に設けられる。よって、認証局鍵記憶部105に格納された認証局公開鍵証明書C_Krp及び認証局秘密鍵Krsは、SIM100の外部からはアクセスされない。また、SIM100は、耐タンパー性を有する。よって、認証局鍵記憶部105に格納された認証局公開鍵証明書C_Krp及び認証局秘密鍵Krsは、SIM100に対する攻撃から保護される。

【0027】

鍵生成部101は、公開鍵と秘密鍵のペアを生成する。公開鍵証明書生成部102は、認証局鍵記憶部105に記憶されている認証局公開鍵証明書C_Krpと認証局秘密鍵Krsのペアを使用して、公開鍵証明書を生成する。秘密鍵記憶部106は、公開鍵証明書生成部102が生成した公開鍵証明書とペアの秘密鍵を記憶する。秘密鍵記憶部106は、認証局鍵記憶部105と同様に、SIM100内の記憶領域のうち、SIM100の外部からアクセスできない不揮発性記憶領域に設けられる。よって、秘密鍵記憶部106に格納された秘密鍵は、SIM100の外部からはアクセスされない。また、SIM100が耐タンパー性を有するので、秘密鍵記憶部106に格納された秘密鍵は、SIM100に対する攻撃から保護される。

【0028】

検証部 103 は、通信部 130 が他の通信装置 3 から受信した公開鍵証明書を、認証局鍵記憶部 105 に記憶されている認証局公開鍵証明書 C__K r p を使用して検証する。暗号処理部 104 は、秘密鍵記憶部 106 に記憶されている秘密鍵を使用して、公開鍵暗号方式の暗号処理を実行する。

【0029】

次に図 2 を参照して、図 1 に示す通信システム 1 の動作を説明する。図 2 は、本実施形態に係る通信方法の説明図である。図 2 には、通信装置 3-1 から通信装置 3-2 へ情報を送信する場合が示される。ここでは、通信装置 3-1 から通信装置 3-2 へ情報を送信する場合を例に挙げて説明するが、逆に通信装置 3-2 から通信装置 3-1 へ情報を送信する場合も同様である。なお、通信装置 3-1 から、通信装置 3-2 以外の、別の通信装置との間で情報を送受信する場合も同様である。つまり、3 つ以上の、複数の通信装置間で情報を送受信する場合も同様である。

10

【0030】

通信装置 3-1 の S I M 100-1 と通信装置 3-2 の S I M 100-2 とは、各認証局鍵記憶部 105 に、同じ認証局公開鍵証明書 C__K r p 及び認証局秘密鍵 K r s を格納している。図 2 では、認証局公開鍵証明書 C__K r p と認証局秘密鍵 K r s とは、S I M 100 内のセキュア R O M (S e c u r e R O M) に格納されている。S I M 100 内のセキュア R O M は、S I M 100 の外部からアクセスできない不揮発性記憶領域である。

【0031】

通信装置 3-1 の制御部 140 は、アプリケーション 150 として、ログイン処理アプリケーションと、公開鍵／秘密鍵発行アプリケーションと、署名生成アプリケーションとを備える。これらアプリケーションの処理は、通信装置 3-1 の制御部 140 内のフラッシュメモリ (F l a s h メモリ) において行われる。通信装置 3-2 の制御部 140 は、アプリケーション 150 として、認証処理アプリケーションと、公開鍵証明書管理アプリケーションと、署名検証アプリケーションとを備える。これらアプリケーションの処理は、通信装置 3-2 の制御部 140 内のフラッシュメモリにおいて行われる。

20

【0032】

[認証処理手順]

認証処理手順のステップ S 1 から S 4 までを説明する。

30

(ステップ S 1) 通信装置 3-1 において、ログイン処理アプリケーションは、制御部 140 を認証処理部 155 として機能させることによって通信装置 3-1 のユーザに対して、ユーザ I D とパスワードとの入力を指示する。通信装置 3-1 において、認証処理部 155 は、ユーザによって入力されたユーザ I D とパスワードを取得し、該ユーザ I D とパスワードを暗号化して通信部 130 へ入力する。

【0033】

(ステップ S 2) 通信装置 3-1 において、通信部 130 は、ユーザによって入力された暗号化されたユーザ I D とパスワードとを通信装置 3-2 へ送信する。

【0034】

(ステップ S 3) 通信装置 3-2 において、認証処理アプリケーションは、制御部 140 を認証処理部 155 として機能させることによって、通信装置 3-1 によって送信された暗号化されたユーザ I D とパスワードを復号し、該復号したユーザ I D とパスワードに基づいて、ユーザを認証する。通信装置 3-2 において、認証処理部 155 は、ユーザを認証した結果を、通信部 130 へ入力する。

40

【0035】

(ステップ S 4) 通信装置 3-2 において、通信部 130 は、ユーザを認証した結果を通信装置 3-1 へ送信する。

以下、通信装置 3-2 において認証が成功した場合について説明を続ける。認証が失敗した場合には、認証処理アプリケーションは、制御部 140 を認証処理部 155 として機能させることによって、認証処理が失敗したことをユーザに通知する。

50

【0036】

[公開鍵証明書の送付手順]

認証処理が成功した場合、公開鍵証明書の送付手順が実行される。公開鍵証明書の送付手順のステップS5からS10までを説明する。

【0037】

(ステップS5) 通信装置3-1において、公開鍵／秘密鍵発行アプリケーションは、SIM100-1に対して、公開鍵と秘密鍵のペアの生成を指示する。SIM100-1の鍵生成部101は、該指示に応じて、公開鍵K1pと秘密鍵K1sを生成する。この公開鍵K1pと秘密鍵K1sの生成は、SIM100-1内のセキュアRAM (Secure RAM) において行われる。SIM100-1内のセキュアRAMは、SIM100-1の外部からアクセスできない揮発性記憶領域である。よって、SIM100-1内のセキュアRAMにおいて行われる処理は、SIM100-1の外部から秘匿される。

10

【0038】

(ステップS6) SIM100-1において、秘密鍵記憶部106は、鍵生成部101が生成した秘密鍵K1sを格納する。図2では、秘密鍵K1sは、SIM100-1内のセキュアROMに格納される。

【0039】

(ステップS7) SIM100-1において、公開鍵証明書生成部102は、鍵生成部101が生成した公開鍵K1pの公開鍵証明書C_K1pを生成する。この公開鍵証明書C_K1pの生成は、SIM100-1内のセキュアRAMにおいて行われる。公開鍵証明書C_K1pは、公開鍵K1pと、SIM識別情報simidlと、公開鍵K1pの電子署名とを含む。公開鍵K1pの電子署名は、公開鍵K1pとSIM識別情報simidlとを含むデータのダイジェストを認証局秘密鍵Krsで暗号化した結果の暗号化データである。ここでは、ダイジェストの例としてハッシュ(hash)値を使用する。また、公開鍵証明書フォーマットの例として、ITU-T (International Telecommunication Union-Telecommunication) 等で規定されている「X.509」規格の公開鍵証明書フォーマットを使用する。「X.509」規格の公開鍵証明書フォーマット中の所定位置に公開鍵K1pを格納する。また、「X.509」規格の公開鍵証明書フォーマット中の「サブジェクトパラメータ：主体者の名前」の位置にSIM識別情報simidlを格納する。

20

30

【0040】

SIM100-1における公開鍵証明書C_K1pの生成方法を具体的に説明する。SIM100-1において、公開鍵証明書生成部102は、公開鍵K1pとSIM識別情報simidlとを格納した「X.509」規格の公開鍵証明書フォーマットのデータのハッシュ値hash(K1p, simidl)を算出する。次いで、公開鍵証明書生成部102は、ハッシュ値hash(K1p, simidl)を、SIM100-1の認証局鍵記憶部105に記憶されている認証局秘密鍵Krsで暗号化する。この暗号化データKrs(hash(K1p, simidl))は、公開鍵K1pの電子署名である。次いで、公開鍵証明書生成部102は、公開鍵K1pと、SIM識別情報simidlと、公開鍵K1pの電子署名Krs(hash(K1p, simidl))とを含む「X.509」規格の公開鍵証明書フォーマットの公開鍵証明書C_K1p「K1p, simidl, Krs(hash(K1p, simidl))」を構成する。

40

【0041】

SIM100-1は、公開鍵証明書生成部102が生成した公開鍵証明書C_K1p「K1p, simidl, Krs(hash(K1p, simidl))」を、公開鍵／秘密鍵発行アプリケーションへ渡す。

【0042】

(ステップS8) 通信装置3-1において、公開鍵／秘密鍵発行アプリケーションは、SIM100-1から受け取った公開鍵証明書C_K1p「K1p, simidl, Krs(hash(K1p, simidl))」を通信部130へ出力する。通信部130は、

50

該公開鍵証明書C_K1p「K1p, simid1, Krs(hash(K1p, simid1))」を通信装置3-2へ送信する。

【0043】

通信装置3-2において、通信部130は、通信装置3-1から公開鍵証明書C_K1p「K1p, simid1, Krs(hash(K1p, simid1))」を受信する。通信部130は、該公開鍵証明書C_K1p「K1p, simid1, Krs(hash(K1p, simid1))」を公開鍵証明書管理アプリケーションへ渡す。

【0044】

(ステップS9) 通信装置3-2において、公開鍵証明書管理アプリケーションは、通信装置3-1から受信した公開鍵証明書C_K1p「K1p, simid1, Krs(hash(K1p, simid1))」をSIM100-2に渡し、該公開鍵証明書C_K1pの検証を指示する。SIM100-2において、検証部103は、SIM100-2の認証局鍵記憶部105に記憶されている認証局公開鍵証明書C_Krpを使用して、公開鍵証明書C_K1p「K1p, simid1, Krs(hash(K1p, simid1))」の正当性を検証する。この公開鍵証明書C_K1pの検証は、SIM100-2内のセキュアRAMにおいて行われる。SIM100-2内のセキュアRAMは、SIM100-2の外部からアクセスできない揮発性記憶領域である。よって、SIM100-2内のセキュアRAMにおいて行われる処理は、SIM100-2の外部から秘匿される。

【0045】

SIM100-2における公開鍵証明書C_K1pの検証方法を具体的に説明する。SIM100-2において、検証部103は、公開鍵証明書C_K1p「K1p, simid1, Krs(hash(K1p, simid1))」から公開鍵K1pとSIM識別情報simid1とを取得し、取得した公開鍵K1pとSIM識別情報simid1とを「X.509」規格の公開鍵証明書フォーマットに格納した検証データを生成する。該検証データにおいて、公開鍵K1pは、「X.509」規格の公開鍵証明書フォーマット中の所定位置に格納される。該検証データにおいて、SIM識別情報simid1は、「X.509」規格の公開鍵証明書フォーマット中の「サブジェクトパラメータ：主体者の名前」の位置に格納される。次いで、検証部103は、該検証データのハッシュ値である検証ハッシュ値hash'(K1p, simid1)を算出する。次いで、検証部103は、公開鍵証明書C_K1p「K1p, simid1, Krs(hash(K1p, simid1))」から電子署名Krs(hash(K1p, simid1))を取得し、取得した電子署名Krs(hash(K1p, simid1))を、SIM100-2の認証局鍵記憶部105に記憶されている認証局公開鍵証明書C_Krpの認証局公開鍵Krpで復号する。この復号により、復号データ「Krp・Krs(hash(K1p, simid1))」が得られる。次いで、検証部103は、検証ハッシュ値hash'(K1p, simid1)と復号データ「Krp・Krs(hash(K1p, simid1))」とが一致するかを判定する。この判定の結果、一致する場合には公開鍵証明書C_K1p「K1p, simid1, Krs(hash(K1p, simid1))」の検証が合格であり、一致しない場合には公開鍵証明書C_K1p「K1p, simid1, Krs(hash(K1p, simid1))」の検証が不合格である。

【0046】

通信装置3-2において、SIM100-2は、公開鍵証明書C_K1p「K1p, simid1, Krs(hash(K1p, simid1))」の検証の結果を公開鍵証明書管理アプリケーションへ通知する。

【0047】

(ステップS10) 通信装置3-2において、公開鍵証明書管理アプリケーションは、SIM100-2から通知された公開鍵証明書C_K1p「K1p, simid1, Krs(hash(K1p, simid1))」の検証の結果が合格である場合には、公開鍵証明書C_K1p「K1p, simid1, Krs(hash(K1p, simid1))」を保管する。この公開鍵証明書C_K1pの保管では、公開鍵証明書C_K1p「K1

p, simid1, Krs(hash(K1p, simid1))」の「サブジェクトパラメータ：主体者の名前」の位置に格納されているSIM識別情報simid1を取得し、取得したSIM識別情報simid1に関連付けて該公開鍵証明書C_K1p「K1p, simid1, Krs(hash(K1p, simid1))」を、通信装置3-2の制御部140内のフラッシュメモリに格納する。

【0048】

一方、公開鍵証明書管理アプリケーションは、SIM100-2から通知された公開鍵証明書C_K1p「K1p, simid1, Krs(hash(K1p, simid1))」の検証の結果が不合格である場合には、公開鍵証明書C_K1p「K1p, simid1, Krs(hash(K1p, simid1))」を破棄する。また、所定のエラー処理を実行してもよい。

10

【0049】

[情報の送付手順]

次に情報の送付手順のステップS11からS16までを説明する。

【0050】

(ステップS11) 通信装置3-1において、署名生成アプリケーションは、通信装置3-2へ送信する情報のダイジェストを算出する。ここでは、ダイジェストの例としてハッシュ(hash)値を使用する。署名生成アプリケーションは、算出したハッシュ値hash(情報)をSIM100-1へ渡し、署名の生成を指示する。

【0051】

20

(ステップS12) SIM100-1の暗号処理部104は、署名生成アプリケーションから受け取ったハッシュ値hash(情報)と、SIM識別情報simid1とを含むデータのハッシュ値hash(hash(情報), simid1)を算出する。さらに、暗号処理部104は、算出したハッシュ値hash(hash(情報), simid1)を、SIM100-1の秘密鍵記憶部106に記憶されている秘密鍵K1sで暗号化する。この暗号化データK1s(hash(hash(情報), simid1))は、通信装置3-2へ送信する情報の電子署名である。この電子署名K1s(hash(hash(情報), simid1))の生成は、SIM100-1内のセキュアRAMにおいて行われる。

【0052】

30

(ステップS13) SIM100-1は、暗号処理部104が生成した電子署名K1s(hash(hash(情報), simid1))を、署名生成アプリケーションへ渡す。

【0053】

(ステップS14) 通信装置3-1において、署名生成アプリケーションは、SIM100-1から受け取った電子署名K1s(hash(hash(情報), simid1))を通信部130へ出力する。通信部130は、該電子署名K1s(hash(hash(情報), simid1))と、通信装置3-2へ送信する情報と、SIM識別情報simid1とを通信装置3-2へ送信する。

【0054】

40

通信装置3-2において、通信部130は、通信装置3-1から、電子署名K1s(hash(hash(情報), simid1))と、情報と、SIM識別情報simid1とを受信する。通信部130は、該受信した電子署名K1s(hash(hash(情報), simid1))、情報及びSIM識別情報simid1を、署名検証アプリケーションへ渡す。

【0055】

(ステップS15) 通信装置3-2において、署名検証アプリケーションは、通信装置3-1から受信した情報のハッシュ値である検証ハッシュ値hash'(情報)を算出する。さらに、署名検証アプリケーションは、該検証ハッシュ値hash'(情報)と、通信装置3-1から受信したSIM識別情報simid1とを含むデータのハッシュ値である検証ハッシュ値hash'(hash'(情報), simid1)を算出する。

50

【0056】

(ステップS16) 通信装置3-2において、署名検証アプリケーションは、通信装置3-1から受信したSIM識別情報simid1を公開鍵証明書管理アプリケーションへ通知して公開鍵証明書を要求する。公開鍵証明書管理アプリケーションは、署名検証アプリケーションから通知されたSIM識別情報simid1に関連づけて保管されている公開鍵証明書C_K1p「K1p, simid1, Krs(hash(K1p, simid1))」を署名検証アプリケーションへ渡す。署名検証アプリケーションは、公開鍵証明書管理アプリケーションから受け取った公開鍵証明書C_K1p「K1p, simid1, Krs(hash(K1p, simid1))」から公開鍵K1pを取得する。署名検証アプリケーションは、該取得した公開鍵K1pで、通信装置3-1から受信した電子署名K1s(hash(hash(情報), simid1))を復号する。この復号により、復号データ「K1p・K1s(hash(hash(情報), simid1))」が得られる。署名検証アプリケーションは、検証ハッシュ値hash'(hash'(情報), simid1)と復号データ「K1p・K1s(hash(hash(情報), simid1))」とが一致するかを判定する。この判定の結果、一致する場合には、通信装置3-1から受信した情報についての正当性の検証が合格である。一方、一致しない場合には、通信装置3-1から受信した情報についての正当性の検証が不合格である。不合格である場合には、通信装置3-1から受信した情報を破棄する。また、所定のエラー処理を実行してもよい。例えば、通信装置3-1から受信した情報が改ざんされている旨を報知したり、又は、情報の送信側が偽者(なりすまし等)である旨を報知したりしてもよい。

10

20

【0057】

本実施形態によれば、通信装置3が、認証局(CA)として機能し、公開鍵証明書を生成する。よって、公開鍵(公開鍵証明書)の供給側は、第三者機関の認証局へ公開鍵を送って公開鍵証明書を発行してもらう手間がかからない。これにより、公開鍵(公開鍵証明書)のやり取りの手間を軽減できるという効果が得られる。また、従来のPKIを利用する場合に比して、コストや申請手続き等の負担を軽減することができる。

【0058】

本実施形態において、通信装置3が備えるSIM100は、通信事業者によりユーザ認証済みのSIMである。このことは通信装置3が認証局としての信頼の基盤となり得る。

【0059】

本実施形態において、SIM100の暗号処理部104は、第1の暗号処理部の例である。通信装置3の制御部140のアプリケーション150の一つである署名検証アプリケーションは、第2の暗号処理部の例である。通信装置3の制御部140のアプリケーション150の一つである公開鍵証明書管理アプリケーションは、公開鍵証明書管理部の例である。SIM100は加入者識別部の例である。

30

【0060】

なお、通信装置3を操作している人物と該通信装置3とをバインド(関連付け)させるようにしてもよい。例えば、認証したい操作や情報に対して、所定のパスワードを入力させる記憶認証を付加する。具体的には、例えば、通信装置3が公開鍵や公開鍵証明書を生成する際に、該通信装置3を操作している人物に所定のパスワードを入力させるようにしてもよい。また、通信装置3のSIM100内の秘密鍵で電子署名を付す際に、該通信装置3を操作している人物に所定のパスワードを入力させるようにしてもよい。

40

【0061】

また、通信装置3の所有者の承諾を経ることを条件にして、通信装置3の操作履歴(操作時の位置の情報、アプリケーションの実行履歴など)を公開鍵証明書又は公開鍵証明書に関連付けられた属性証明書のフォームに記載して電子署名を施してもよい。

【0062】

また、通信装置3の所有者の承諾を経ることを条件にして、通信事業者が有する該所有者の情報を公開鍵証明書又は公開鍵証明書に関連付けられた属性証明書のフォームに記載して電子署名を施してもよい。

50

【0063】

また、SIMは、ユーザ識別情報に関連付けられた固有識別情報を格納する通信モジュールの総称であり、特定の通信システム方式で用いられる通信モジュールに限定されない。例えば、UIM (User Identity Module)、USIM (Universal Subscriber Identity Module)、eSIM (Embedded Subscriber Identity Module) などを使用してもよい。

【0064】

また、上述した実施形態では、通信装置3-1のユーザによって入力されたユーザIDとパスワードに基づいて、通信装置3-2の認証処理部155が通信装置3-1のユーザを認証する場合について説明したが、この例に限られない。例えば、ワンタイムパスワードが適用されてもよい。具体的には、タイムスタンプ方式が適用される場合、通信装置3-1側にトークンと呼ばれるパスワード生成器を予め設けておく。トークンには、ICカードのようなもの、USBキーのようなもの、キーホルダーのような形をしているもの、インストールして使用するソフトウェアタイプなどさまざまな形態があるがいずれも適用できる。トークンには例えば数字列が表示され、この数字列が時刻の経過に伴って別の数字に切り替わる。該数字列がパスワードとして使用される。

【0065】

通信装置3-1のユーザは、認証を受けるときにユーザIDなどの識別情報とともに、トークンに表示された数字列をパスワードとして入力し、通信装置3-2へ送信する。

通信装置3-2では、トークンを使用しているユーザと、各トークンがどの時刻にはどんな数値を表示するかを把握しており、通信装置3-2は、通信装置3-1がアクセスしてきた時刻と送られてきたパスワード、および識別番号を検証することにより、アクセス元が正規ユーザかどうかを認証する。

【0066】

ワンタイムパスワードが適用される場合、通信装置3-2の認証処理部155は、ユーザIDとパスワードによる認証が成功した場合に、所定期間の間有効なトークンを発行し、通信部130から通信装置3-1へ送信するようにしてもよい。そして、該トークンを受信した通信装置3-1は、所定期間の間は、ログイン処理アプリケーションを実行せずに、公開鍵／秘密鍵発行アプリケーションと、署名生成アプリケーションとを実行するようにしてもよい。

【0067】

また、通信装置3-2の認証処理部155は、ユーザIDとパスワードによる認証が失敗した場合には、通信装置3-1に認証が失敗したことを通知することによって、通信装置3-1のユーザに認証が失敗したことを通知するようにしてもよい。また、通信装置3-2の検証部103は、ユーザの検証に失敗した場合には、サービス事業者や、管理者に通知するようにしてもよい。

【0068】

なお、公開鍵証明書の送信側の通信装置3は、公開鍵証明書の検証機能および公開鍵証明書の保管機能を備えなくてもよい。具体的には、公開鍵証明書の送信側の通信装置3は、検証部103と公開鍵証明書管理アプリケーションとを備えなくてもよい。

【0069】

また、公開鍵証明書の受信側の通信装置3は、公開鍵証明書の生成機能を備えなくてもよい。具体的には、公開鍵証明書の受信側の通信装置3は、公開鍵証明書生成部102と秘密鍵記憶部106とを備えなくてもよい。

【0070】

また、SIM100は、予め、公開鍵と秘密鍵のペアを格納していてもよい。例えば、SIM100の製造時に、公開鍵と秘密鍵のペアを該SIM100に格納してもよい。SIM100が、予め、公開鍵と秘密鍵のペアを格納している場合には、該SIM100は鍵生成部101を備えなくてもよい。

また、SIM100にて、生成または保管される公開鍵（公開鍵証明書）と秘密鍵のペアは、複数であってもよい。この場合、例えば、通信装置3は、通信相手先に応じて公開鍵（公開鍵証明書）と秘密鍵のペアを使い分けてもよい。また、通信装置3は、ある公開鍵（公開鍵証明書）と秘密鍵のペアが漏洩した場合に、別のペアに切り替えてもよい。

【0071】

なお、SIM識別情報に関連付けられたユーザ識別情報を公開鍵証明書に含めるようにしてもよい。ユーザ識別情報を公開鍵証明書に含める場合には、該公開鍵証明書に該SIM識別情報を含めなくてもよい。また、ユーザ識別情報を公開鍵証明書に含める場合には、公開鍵証明書管理部は該公開鍵証明書を該ユーザ識別情報に関連付けて格納するようにしてもよい。

10

【0072】

また、SIM識別情報に関連付けられたユーザ識別情報を、送信する情報の電子署名に含めるようにしてもよい。この場合、該情報を送信する際に、該ユーザ識別情報と該電子署名とを一緒に送信する。

【0073】

[第2実施形態]

第2実施形態は、上述した第1実施形態の変形例である。図3は、第2実施形態に係る通信システム1を示す構成図である。図3において図1の各部に対応する部分には同一の符号を付け、その説明を省略する。図3に示す第2実施形態に係る通信装置3は、上述した図1に示す第1実施形態の通信装置3に対してさらに無線通信部160と認証局鍵更新部170とを備える。以下、上述した第1実施形態との差分を主に説明する。

20

【0074】

通信装置3において、無線通信部160は、SIM100を使用して接続する無線通信ネットワーク40を介して通信を行う。SIM100は、無線通信ネットワーク40を利用するための情報を格納する。無線通信部160は、SIM100を使用することにより無線通信ネットワーク40を利用できる。無線通信部160は、SIM100を使用して確立される無線通信回線により無線通信ネットワーク40に接続する。

【0075】

認証局鍵更新部170は、他の通信装置3のSIM100と共有する新しい認証局公開鍵証明書と認証局秘密鍵のペアを、無線通信ネットワーク40を介して管理サーバ装置30から受信する。管理サーバ装置30は、認証局公開鍵証明書と認証局秘密鍵のペアを管理する。管理サーバ装置30は、複数の通信装置3のSIM100で共有させる新しい認証局公開鍵証明書と認証局秘密鍵のペアを、無線通信ネットワーク40を介して、該複数の通信装置3へ送信する。認証局鍵更新部170は、無線通信ネットワーク40を介して管理サーバ装置30から受信した認証局公開鍵証明書と認証局秘密鍵のペアをSIM100へ渡して、認証局公開鍵証明書と認証局秘密鍵のペアの更新を指示する。SIM100は、認証局鍵更新部170から受け取った認証局公開鍵証明書と認証局秘密鍵のペアを最新の認証局公開鍵証明書と認証局秘密鍵のペアとして認証局鍵記憶部105に格納する。これにより、複数の通信装置3のSIM100において共有される認証局公開鍵証明書と認証局秘密鍵のペアが新しい認証局公開鍵証明書と認証局秘密鍵のペアに更新される。

30

40

【0076】

本実施形態によれば、何らかの理由により、SIM100が保持する認証局公開鍵証明書と認証局秘密鍵のペアを新しいものに更新する場合に、新しい認証局公開鍵証明書と認証局秘密鍵のペアを無線通信により各SIM100へ供給することができる。よって、認証局公開鍵証明書と認証局秘密鍵のペアを新しいものに更新するためにSIM100を交換する等の手間がかからない。これにより、認証局公開鍵証明書と認証局秘密鍵のペアを新しいものに更新する際の負担を軽減できるという効果が得られる。

【0077】

[第3実施形態]

第3実施形態は、上述した第1実施形態又は第2実施形態の適用例である。図4は、第

50

3実施形態に係る通信システム1を示す構成図である。図4に示す通信システム1は、通信端末3-3と通信端末3-4を備える。通信端末3-3及び通信端末3-4は、上述した第1実施形態又は第2実施形態の通信装置3と同様の構成を備える。通信端末3-3及び通信端末3-4は、例えば、スマートフォンやタブレット型のコンピュータ（タブレットPC）等の携帯通信端末装置であってもよく、又は、据置き型の通信端末装置（例えば、据置き型のパーソナルコンピュータやサーバコンピュータ、ホームゲートウェイ等）であってもよい。

【0078】

通信端末3-3はSIM100-3を備える。通信端末3-4はSIM100-4を備える。SIM100-3及びSIM100-4は、上述した第1実施形態又は第2実施形態のSIM100と同様の構成を備える。これにより、SIM100-3及びSIM100-4は、その機能部として、認証局（CA）210を備える。よって、通信端末3-3及び通信端末3-4は、認証局（CA）として機能する。SIM100-3の認証局210とSIM100-4の認証局210とは、同じ認証局公開鍵証明書と認証局秘密鍵のペアを有する。

【0079】

SIM100-3及びSIM100-4は、その機能部として、クライアント220を備える。SIM100-3において、クライアント220は、自己の公開鍵を認証局210に渡して該公開鍵の公開鍵証明書（クライアント公開鍵証明書）を生成してもらう。同様に、SIM100-4において、クライアント220は、自己の公開鍵を認証局210に渡して該公開鍵の公開鍵証明書（クライアント公開鍵証明書）を生成してもらう。

【0080】

通信端末3-3及び通信端末3-4は、アプリケーション240を備える。アプリケーション240の処理は、自通信端末内のメモリ230において行われる。アプリケーション240は、認証処理と署名処理とを行う。

【0081】

図4に示すように、第3実施形態に係る通信システム1では、通信端末3-3と通信端末3-4とは、自己のクライアント公開鍵証明書を通信相手に送信する。通信端末3-3と通信端末3-4とは、各々、受信したクライアント公開鍵証明書の正当性を自己の認証局210により検証する。通信端末3-3と通信端末3-4とは、通信相手のクライアント公開鍵証明書を、自己の認証局210により正当性を確認した上で使用する。クライアント公開鍵証明書は、通信端末間の相互認証や、通信端末間で交換される情報の電子署名などに使用される。相互認証方法として、例えばチャレンジ・レスポンス認証方法が挙げられる。

【0082】

次に第3実施形態に係る実施例を説明する。

【0083】

（実施例1）

図5を参照して第3実施形態に係る実施例1を説明する。図5は、第3実施形態の実施例1に係る通信システム1を示す説明図である。図5に示す通信システム1は、オンラインバンキングサービスシステムに適用されている。図5において、通信端末3-3は、オンラインバンキングサービスシステムのアプリケーション310を備える。通信端末3-4は、オンラインバンキングサービスシステムのサービスサイト320を備える。以下、図5に示す通信システム1に係る通信方法を説明する。

【0084】

（ステップS101）通信端末3-3において、アプリケーション310は、サービスサイト320へのログイン処理として、ユーザのID（識別情報）とパスワード（Password）の入力処理を行う。アプリケーション310は、ユーザから入力されたIDとパスワードを通信端末3-4のサービスサイト320へ送信する。通信端末3-4において、サービスサイト320は、ログイン処理として、通信端末3-3のアプリケーション

310から受信したIDとパスワードの正当性を検証する。この検証の結果が合格である場合には以降の処理へ進む。一方、IDとパスワードの検証が不合格である場合には処理を終了する。IDとパスワードの検証が不合格である場合には所定のエラー処理を実行してもよい。

【0085】

(ステップS102) 通信端末3-3において、アプリケーション310は、自通信端末のクライアント公開鍵証明書を通信用端末3-4のサービスサイト320へ送信する。

【0086】

(ステップS103) 通信端末3-4において、サービスサイト320は、通信端末3-3のアプリケーション310から受信したクライアント公開鍵証明書の正当性を、自通信端末の認証局210により検証する。この検証の結果が合格である場合には以降の処理へ進む。一方、クライアント公開鍵証明書の検証が不合格である場合には処理を終了する。クライアント公開鍵証明書の検証が不合格である場合には所定のエラー処理を実行してもよい。

【0087】

(ステップS104) 通信端末3-4において、サービスサイト320は、乱数を生成し、生成した乱数をチャレンジ値とする。サービスサイト320は、チャレンジ値(乱数)を通信用端末3-3のアプリケーション310へ送信する。

【0088】

(ステップS105) 通信端末3-3において、アプリケーション310は、通信端末3-4のサービスサイト320から受信したチャレンジ値(乱数)を、自通信端末のクライアント公開鍵証明書の公開鍵とペアの秘密鍵Ksで暗号化する。このチャレンジ値(乱数)の暗号化は、通信端末3-3のSIM100-3内のセキュアRAMにおいて行われる。アプリケーション310は、チャレンジ値(乱数)の暗号化の結果である暗号化データKs(乱数)をレスポンス値として、通信端末3-4のサービスサイト320へ送信する。

【0089】

(ステップS106) 通信端末3-4において、サービスサイト320は、通信端末3-3のアプリケーション310から受信したレスポンス値Ks(乱数)の正当性を、通信端末3-3のクライアント公開鍵証明書の公開鍵を使用して検証する。例えば、レスポンス値Ks(乱数)を公開鍵で復号した結果がチャレンジ値(乱数)と一致する場合には検証を合格とし、一方、チャレンジ値(乱数)と一致しない場合には検証を不合格とする。レスポンス値Ks(乱数)の検証の結果が合格である場合にはサービスサイト320へのログインを成功とする。一方、レスポンス値Ks(乱数)の検証が不合格である場合にはサービスサイト320へのログインを失敗とする。レスポンス値Ks(乱数)の検証が不合格である場合には所定のエラー処理を実行してもよい。

【0090】

本実施例1によれば、ユーザ認証において、ID・パスワード認証に加えて、さらにチャレンジ・レスポンス認証も実施することができる。これにより、ID・パスワード認証とチャレンジ・レスポンス認証との二つの認証要素によってユーザ認証を実施することができるので、ユーザ認証の信頼性が向上する。このことから、従来、ID・パスワード認証の信頼性を高めるために、パスワード更新用の乱数表や、時刻同期型のワンタイムパスワード生成アプリケーションなどのツールが利用されていたが、本実施例1によれば、それらツールを使用せずに済ますことが可能になる。

【0091】

また、サービスサイト320が通信端末3-3のクライアント公開鍵証明書を保管することにより、もし通信端末3-3の紛失によってユーザが通信端末3-3のクライアント公開鍵証明書を使用できなくなった場合には、当該ユーザのユーザ認証がチャレンジ・レスポンス認証で失敗する。これは、通信端末3-3の紛失時において当該ユーザのIDによるサービスサイト320へのログインに対するリモートロックとして機能する。

【0092】

(実施例2)

図6を参照して第3実施形態に係る実施例2を説明する。図6は、第3実施形態の実施例2に係る通信システム1を示す説明図である。図6に示す通信システム1は、オンラインショッピングサービスシステムに適用されている。図6において、通信端末3-3は、オンラインショッピングサービスシステムのアプリケーション410を備える。通信端末3-4は、オンラインショッピングサービスシステムのサービスサイト420を備える。以下、図6に示す通信システム1に係る通信方法を説明する。図6において図5の各ステップに対応する部分には同一の符号を付け、その説明を省略する。

【0093】

図6において、ステップS101からS106までの処理が実行された結果、ユーザ認証が合格し、当該ユーザのIDでのサービスサイト420へのログインが成功した。以降、当該ユーザは、サービスサイト420において当該IDでのオンラインショッピングの購買操作を実行する。

【0094】

(ステップS201) 通信端末3-3において、アプリケーション410は、ユーザが行った購買操作を示す購買操作情報の電子署名を、自通信端末のクライアント公開鍵証明書の公開鍵とペアの秘密鍵Ksにより生成する。この電子署名の生成は、通信端末3-3のSIM100-3内のセキュアRAMにおいて行われる。アプリケーション410は、購買操作情報と該購買操作情報の電子署名を通信端末3-4のサービスサイト320へ送信する。

【0095】

(ステップS202) 通信端末3-4において、サービスサイト420は、通信端末3-3のアプリケーション410から受信した購買操作情報の電子署名の正当性を、通信端末3-3のクライアント公開鍵証明書の公開鍵を使用して検証する。購買操作情報の電子署名の検証の結果が合格である場合には、サービスサイト420は、通信端末3-3のアプリケーション410から受信した購買操作情報で示される購買操作を受け付ける。これにより、ユーザが行った購買操作はサービスサイト420で実行される。一方、購買操作情報の電子署名の検証が不合格である場合には、サービスサイト420は、通信端末3-3のアプリケーション410から受信した購買操作情報で示される購買操作を受け付けない。これにより、ユーザが行った購買操作はサービスサイト420で実行されない。購買操作情報の電子署名の検証が不合格である場合には所定のエラー処理を実行してもよい。

【0096】

本実施例2によれば、上述の実施例1と同様に、ID・パスワード認証とチャレンジ・レスポンス認証との二つの認証要素によってユーザ認証を実施することができるので、ユーザ認証の信頼性が向上する。

【0097】

また、本実施例2によれば、購買操作の受け付けにおいて、当該購買操作の正当性を購買操作情報の電子署名の正当性の検証によって確認することができる。このことから、従来、購買操作の正当性の確認のために電話による本人確認を行っていたが、本実施例2によれば、その電話による本人確認を実施せずに済ますことが可能になる。

【0098】

<変形例>

図7は、上述した実施形態に係る通信装置3-1、通信装置3-2や、通信端末3-3、通信端末3-4に搭載される機能の一例を示す。

具体的には、通信装置3-1、通信装置3-2や、通信端末3-3、通信端末3-4が盗難された場合や、紛失した場合に、SIM100による公開鍵証明書を付与する動作を停止させるのが好ましい。また、通信装置3-1、通信装置3-2や、通信端末3-3、通信端末3-4が盗難された場合や、紛失した場合に、そのことをユーザや、サービス業者に通知できるようにするのが好ましい。

10

20

30

40

50

【0099】

SIM100には、管理アプリ502と、アプリケーションインタフェース504と、1又は複数のアプリ（アプリA506、アプリB、アプリX）とが記憶されている。管理アプリ502は、アプリケーションインタフェース504と、各サービス事業者の使用するアプリ領域とを制御する。ここで、管理アプリ502は、通信装置3-1、通信装置3-2や、通信端末3-3、通信端末3-4へインストールされているアプリの一覧と、その状態を管理するテーブルを保持する。

【0100】

アプリケーションインタフェース504は、各事業者のサービスがSIM内に格納されたアプリを利用するために端末装置からアクセスを行うためのものである。1又は複数のアプリは、各サービス事業者が使用するアプリである。

10

【0101】

端末装置に搭載されたSIMを制御するには、ネットワークを介して接続された事業者が有するDM（Device Management）サーバから通信装置などの移動機のオペレーティングシステム（Operating System：OS）等に予め搭載されているDMクライアント（DM Client）512等のアプリ（以下、「移動機のアプリ」という）を通じて、SIM内の管理アプリ502を動作させる。しかし、移動機のアプリとSIM内の管理アプリ502を連携させるには、端末毎にOS等を含めた改修が必要となり、汎用的なアプリのように簡易に設定変更ができない。

20

【0102】

一方、通信事業者が有するSIM内の所定の領域を制御可能なSIM情報管理サーバ（Mobile Network Operator - Trusted Service Manager：MNO-TSM）（以下、「MNO-TSM」という）からは、移動機のアプリを経由することなく、直接SIM内の所定の領域に対してSIM内のアプリを制御するためのコマンドを投入できる。

【0103】

管理アプリ502へコマンドが投入されることによって、アプリ全体または個別の状態を管理することができる。管理アプリ502へのコマンドの投入は、DMクライアント512を経由して行われてもよいし、設定アプリ514を経由して行われてもよいし、TSM Proxy 516を経由して行われてもよい。また、管理アプリ502へのコマンドの投入は、MNO-TSM 700からリモートコマンドを投入することによって行われてもよい。このようにできるのは、コマンドの投入元が通信事業者であるためであり、直接SIM内の所定の領域に対してSIM内のアプリを制御するためのコマンドを投入できるためである。この方法では、管理アプリ502に対して直接コマンドを投入することができる。

30

【0104】

通信装置のSIMは、該SIMを利用して動作するアプリを管理する管理アプリ502を有しており、管理アプリ502はアプリケーション毎の動作状態を管理する。例えば、SIM内に記憶された各サービスに関するアプリケーションの状態を全部又は一部の動作をロック又はアンロックとすることができる。動作状態の変更は、例えば、MNO-TSMなどのSIM情報管理サーバからSIM内の管理アプリ502に対して、SIM内のアプリケーションを制御するリモートコマンドを投入することにより実行する。

40

【0105】

<ログ管理の案件>

購入等の所定の手続きに関する暗号化された情報を受信したサーバによって、認証の結果不一致であると判定された場合、サービス事業者は、不適切な端末装置（通信装置）又はユーザからの手続きがあったと判断する。例えば、ユーザIDとパスワードが漏洩し、不正の端末装置によって購入手続きが行われた場合や、サービス事業者によって認められていないことによって本人の認証がされていないSIMを備えた端末装置によって購入手続きが行われた場合にサービス事業者は、不適切な端末装置（通信装置）又はユーザから

50

の手続きがあったと判断する。

【0106】

この判断結果に基づいて、サービス事業者は、通信事業者に対してユーザの署名を無効化する手続きの依頼を送信する。通信事業者は、署名を無効化する手続きの依頼に応じて、該ユーザの署名機能を無効にする。通信事業者は、該ユーザの署名機能を無効にして以降、該無効を端末装置への所定の操作や、適切な依頼元からの所定の解除依頼により端末装置に対して解除処理を行うまで、該ユーザの端末装置での購入等の手続きができない様にロックする。このように構成することによって、該不適切な端末装置又はユーザからの手続きによる、該ユーザの署名機能を無効にして以降の不正利用を継続して行うことは不可能となる。

10

【0107】

具体的には、サービス事業者の管理サーバは、通信事業者が有するMNO-TSMに対して所定の制御信号を送信し、MNO-TSMはネットワーク又はユーザ端末を介して管理アプリ502へサービス事業者の提供するアプリの使用するSIM内のアプリをロックするコマンドを送信する。

【0108】

なお、サービス事業者は、管理アプリ502を介して各アプリ領域をロックさせてもよいし、アプリケーションインタフェース504を無効にしてもよい。このように構成することによって、認証に必要とされる暗号化処理、複合化処理ができなくなるため1つのサービスの不正利用に基づいて、他のアプリの不正利用も防ぐことができる。

20

また、サービス事業者は、通信事業者にSIM内のアプリのロックを依頼する際に、ユーザに対しても不正利用のおそれに関する通知を行うようにしてもよい。

【0109】

以上、本発明の実施形態、及び変形例について図面を参照して詳述してきたが、具体的な構成はこの実施形態に限られるものではなく、本発明の要旨を逸脱しない範囲の設計変更等も含まれる。

【0110】

なお、上述した実施形態に係る通信装置又は通信端末の機能を実現するためのコンピュータプログラムをコンピュータ読み取り可能な記録媒体に記録して、この記録媒体に記録されたプログラムをコンピュータシステムに読み込ませ、実行するようにしてもよい。なお、ここでいう「コンピュータシステム」とは、OSや周辺機器等のハードウェアを含むものであってもよい。

30

また、「コンピュータ読み取り可能な記録媒体」とは、フレキシブルディスク、光磁気ディスク、ROM、フラッシュメモリ等の書き込み可能な不揮発性メモリ、DVD(Digital Versatile Disc)等の可搬媒体、コンピュータシステムに内蔵されるハードディスク等の記憶装置のことをいう。

【0111】

さらに「コンピュータ読み取り可能な記録媒体」とは、インターネット等のネットワークや電話回線等の通信回線を介してプログラムが送信された場合のサーバやクライアントとなるコンピュータシステム内部の揮発性メモリ(例えばDRAM(Dynamic Random Access Memory))のように、一定時間プログラムを保持しているものも含むものとする。

40

【0112】

また、上記プログラムは、このプログラムを記憶装置等に格納したコンピュータシステムから、伝送媒体を介して、あるいは、伝送媒体中の伝送波により他のコンピュータシステムに伝送されてもよい。ここで、プログラムを伝送する「伝送媒体」は、インターネット等のネットワーク(通信網)や電話回線等の通信回線(通信線)のように情報を伝送する機能を有する媒体のことをいう。

また、上記プログラムは、前述した機能の一部を実現するためのものであっても良い。さらに、前述した機能をコンピュータシステムにすでに記録されているプログラムとの組

50

み合わせで実現できるもの、いわゆる差分ファイル（差分プログラム）であっても良い。

【0113】

本発明は特定の実施例、変形例を参照しながら説明されてきたが、各実施例、変形例は単なる例示に過ぎず、当業者は様々な変形例、修正例、代替例、置換例などを理解するであろう。説明の便宜上、本発明の実施例に従った装置は機能的なブロック図を用いて説明されたが、そのような装置はハードウェアで、ソフトウェアでまたはそれらの組み合わせで実現されてもよい。本発明は上記実施例に限定されず、本発明の精神から逸脱することなく、様々な変形例、修正例、代替例、置換例等が包含される。

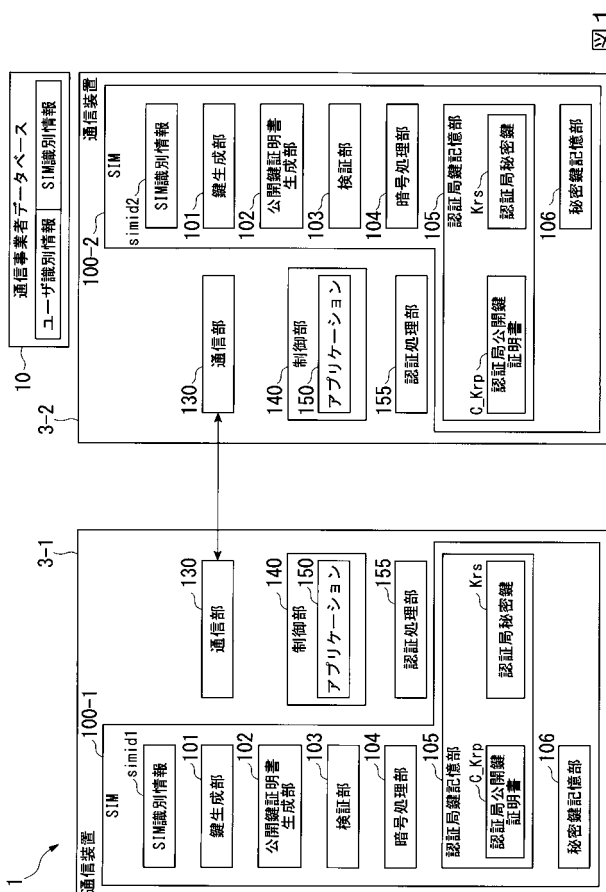
【符号の説明】

【0114】

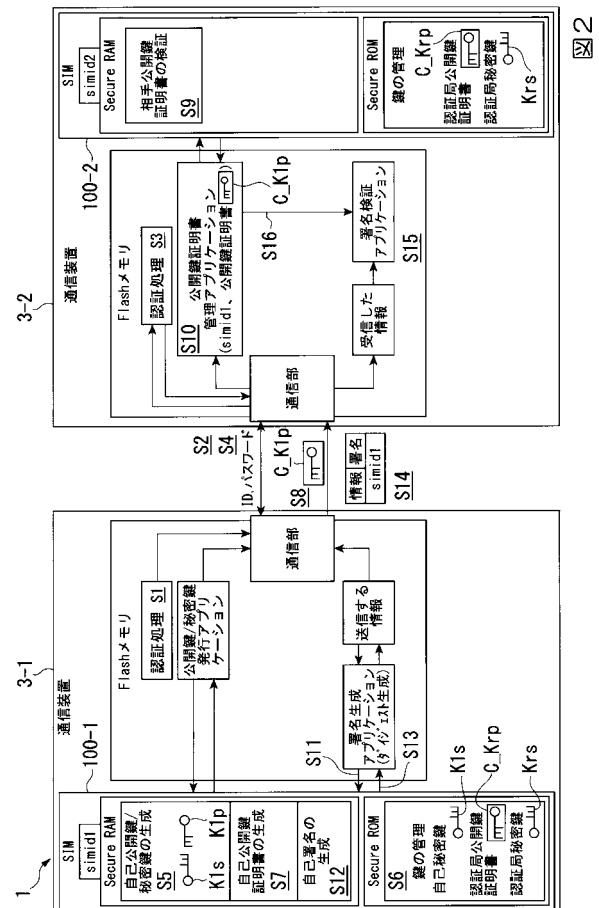
1…通信システム、3-1, 3-2…通信装置、3-3, 3-4…通信端末、10…通信事業者データベース、30…管理サーバ装置、40…無線通信ネットワーク、100-1~4…SIM、101…鍵生成部、102…公開鍵証明書生成部、103…検証部、104…暗号処理部、105…認証局鍵記憶部、106…秘密鍵記憶部、130…通信部、140…制御部、155…認証処理部、160…無線通信部、170…認証局鍵更新部、210…認証局

10

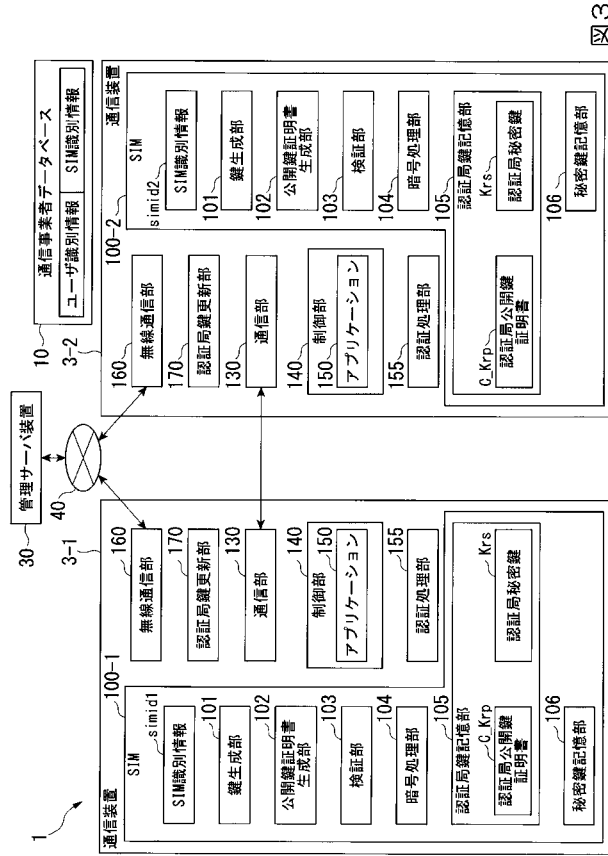
【図1】



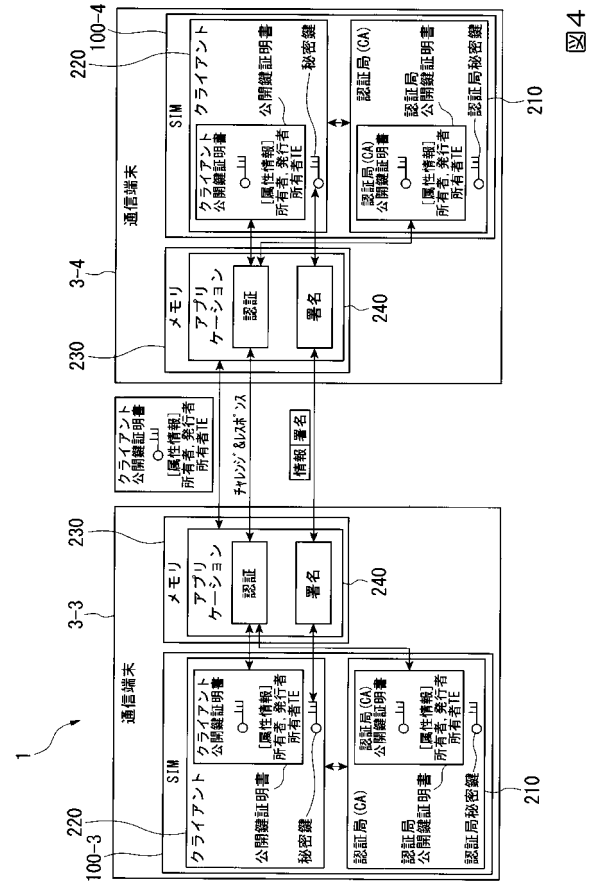
【図2】



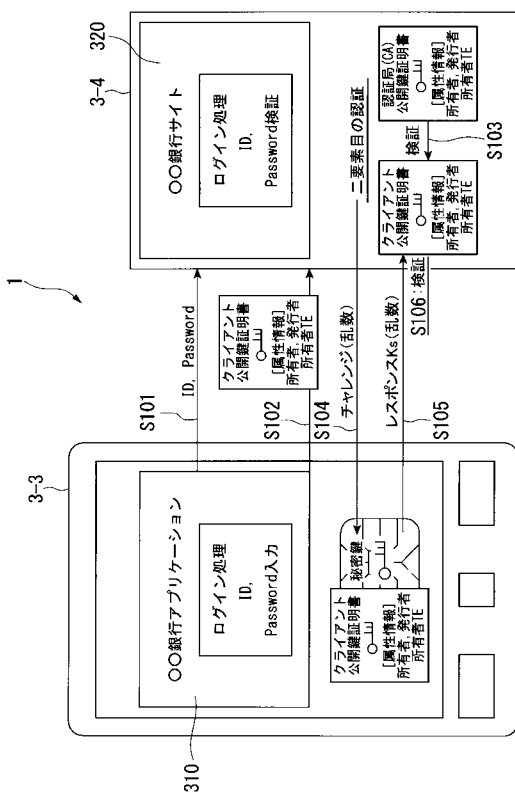
【 図 3 】



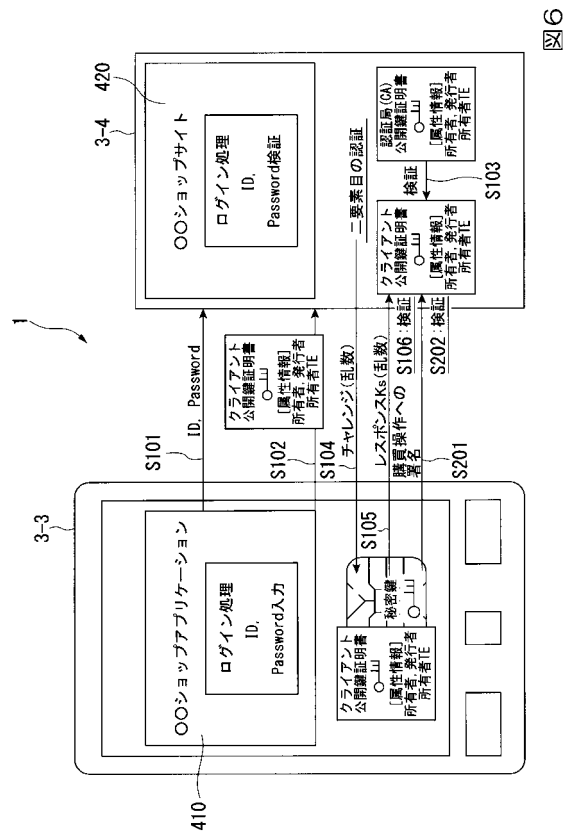
【図 4】



【 図 5 】



【図 6】



【図 7】

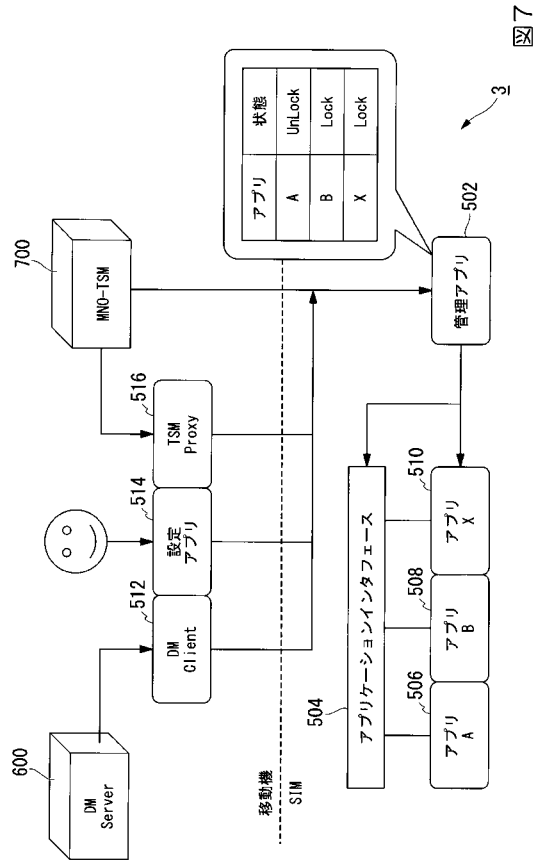


図 7

フロントページの続き

(72)発明者 磯原 隆将

東京都新宿区西新宿二丁目3番2号 KDDI株式会社内

Fターム(参考) 5J104 AA07 AA09 KA01 KA05 LA01 LA06 NA12 NA38 PA07