(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2006 年2 月23 日 (23.02.2006)

PCT

(10) 国際公開番号
WO 2006/018889 A1

(51) 国際特許分類[7]: H04L 9/32, 9/08, G06F 17/60, 15/00, G06K 17/00

(21) 国際出願番号: PCT/JP2004/011963

(22) 国際出願日: 2004 年8 月20 日 (20.08.2004)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(71) 出願人 (米国を除く全ての指定国について): 三菱電機株式会社 (MITSUBISHI DENKI KABUSHIKI KAISHA) [JP/JP]; 〒1008310 東京都千代田区丸の内二丁目２番３号 Tokyo (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 米田 健 (YONEDA, Takeshi) [JP/JP]; 〒1008310 東京都千代田区丸の内二丁目２番３号 三菱電機株式会社内 Tokyo (JP).

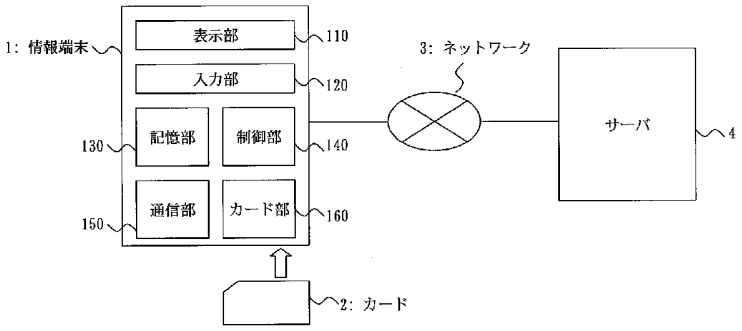
(74) 代理人: 溝井 章司 (MIZOI, Shoji); 〒2470056 神奈川県鎌倉市大船二丁目１７番１０号 ＮＴＡ大船ビル３階 溝井国際特許事務所 Kanagawa (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

[続葉有]

(54) Title: TERMINAL APPARATUS

(54) 発明の名称: 端末装置



1- INFORMATION TERMINAL
110- DISPLAY PART
120- INPUT PART
130- STORAGE PART
140- CONTROL PART
150- COMMUNICATION PART
160- CARD PART
2- CARD
3- NETWORK
4- SERVER

(57) Abstract: When an application uses a user certificate, the number of available certificate candidates is reduced, thereby reducing the user's load of certificate selection. An information terminal (1) communicates with a server (4) via a network (3). The information terminal (1) is so constructed that a card (2) can be removably attached to the information terminal (1). The card (2) holds user certificates and a secret key and has an encrypting function using the secret key. The information terminal (1) includes a display part (110), an input part (120), a storage part (130), a control part (140), a communication part (150) and a card part (160).The control part (140) manages the user certificates and the user certificate utilization conditions acquired from the card (2) via the card part (160), and selects an available user certificate. The selected user certificate is used for an encryption communication between the information terminal (1) and the server (4).

(57) 要約: アプリケーションがユーザ証明書を利用する時に、利用可能な証明書の候補数を減らし、利用者の証明書選択の負荷を軽減する。情報端末１は、ネットワーク３を経由してサーバ４と通信を行う。情報端末１にはカード２を着脱することができる。カード２は、ユーザ証明書や秘密鍵を保持し、秘密鍵による暗号処理機能を有する。情報端末１は、表示部１１０、入力部１２０、記憶部１

[続葉有]

WO 2006/018889 A1

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

３０、制御部１４０、通信部１５０、カード部１６０を備えている。制御部１４０は、カード部１６０を介してカード２から取得したユーザ証明書及びユーザ証明書の利用条件を管理し、利用可能なユーザ証明書を選択する機能を有する。選択されたユーザ証明書は、情報端末１とサーバ４との間の暗号通信に用いられる。

明 細 書

端末装置

技術分野

[0001] 本発明は、端末装置及び認証装置及び暗号通信方法及び証明書提供方法に関するものである。

背景技術

[0002] インターネットを利用したオンラインショッピングが普及してきた。オンラインショッピングでは、商品の購入処理を、ブラウザとサーバがインターネット経由で通信することで実現される。オンラインショッピングにおいて、サーバのなりすましや通信データの盗聴、改ざんの防止は必須の要件である。この要件を満たす技術として、非特許文献1に記載された暗号通信方式SSL(Secure Socket Layer)が広く用いられている。

[0003] SSLを利用したオンラインショッピングにおいて、ユーザ認証は、ユーザ名とパスワードを入力することで実現されることが多い。その場合、成りすましを防止するために、推測されにくいパスワードを選択する必要がある。しかし、多くのユーザは、推測が容易なパスワードを選択してしまう傾向がある。そこで、ユーザ認証にデジタル署名を利用するニーズが高まっている。デジタル署名によるユーザ認証機能はSSLに組み込まれており、デジタル署名は、その生成に用いる秘密鍵さえ盗まれなければ成りすましが困難である。デジタル署名に利用される秘密鍵とデジタル署名を検証する証明書はIC(Integrated Circuit)カードやUSB(Universal Serial Bus)トークンやUIM(User Identity Module)等の秘密鍵の漏洩を防止する仕組みの備わったデバイスに格納される。以降、秘密鍵、秘密鍵に対応する証明書(以降、ユーザ証明書)を保持し、ユーザ認証に用いるデバイスを認証デバイスと呼ぶ。認証デバイスは複数の秘密鍵とユーザ証明書を持つことが今後予想される。なぜなら、異なるサイト毎に利用する秘密鍵・証明書が異なる場合、それぞれが単一の認証デバイスに含まれる方が、別々の認証デバイスに含まれるより利便性が高いからである。

非特許文献1:Alan O. Freier、他2名、"The SSL Protocol Version 3.0

”、[online]、1996年11月18日、Netscape Communications、[2004年8月2日検索]、インターネット<URL:http://wp.netscape.com/eng/ssl3/draft302.txt>

発明の開示

発明が解決しようとする課題

[0004] SSLでは、SSLサーバがSSLクライアントにユーザ証明書の送付要求(Certificate Request)を送る。その際、証明書の送付要求にはユーザ証明書のタイプ(公開アルゴリズム種別等)やユーザ証明書の証明書発行局名の情報を指定できる。SSLクライアントは、複数のユーザ証明書を保持する場合、送付された証明書送付要求の証明書タイプ及び証明書発行局名に合致するユーザ証明書を探す。もし、複数のユーザ証明書が条件に合致した場合、利用者に利用する証明書を選択させる必要がある。また、認証デバイスに格納される秘密鍵・ユーザ証明書の数が増えるにしたがって、利用可能なユーザ証明書の候補数が増える。その結果、候補の中から適切な証明書を選択する利用者の負荷が大きくなる。

[0005] 本発明は、アプリケーションがユーザ証明書を利用する時に、利用可能な証明書の候補数を減らし、利用者の証明書選択の負荷を軽減することを目的とする。

課題を解決するための手段

[0006] 本発明の端末装置は、

1つ以上の電子証明書と当該電子証明書それぞれの利用を制限する利用条件とを記憶する認証装置を接続する認証装置接続部と、

前記認証装置接続部が接続する認証装置から利用条件を受信する利用条件受信部と、

前記利用条件受信部が受信した利用条件を記憶する利用条件格納部と、

前記利用条件格納部に記憶された利用条件を基に電子証明書を選択する証明書選択部と、

前記認証装置接続部が接続する認証装置から前記証明書選択部が選択した電子証明書を受信する証明書受信部と、

前記証明書受信部が受信した電子証明書を利用して暗号通信を行う通信部とを備

えることを特徴とする。

[0007] 前記端末装置は、さらに、

前記証明書選択部が選択した電子証明書を一意的に識別する識別情報を出力する出力部と、

前記出力部が出力した識別情報をユーザに選択させる入力部とを備え、

前記証明書受信部は、

前記認証装置接続部が接続する認証装置から前記入力部がユーザに選択させた識別情報に対応する電子証明書を受信することを特徴とする。

[0008] 前記証明書選択部は、

前記利用条件格納部に記憶された利用条件と前記通信部の暗号通信先に関する情報とを比較し、その結果を基に電子証明書を選択することを特徴とする。

[0009] 前記証明書選択部は、

前記通信部の暗号通信先に関する情報として、少なくとも暗号通信先のホスト名を用いることを特徴とする。

[0010] 前記端末装置は、さらに、

前記通信部が行う暗号通信を利用するプログラムを実行する制御部を備え、

前記証明書選択部は、

前記利用条件格納部に記憶された利用条件と前記制御部が実行するプログラムに関する情報とを比較し、その結果を基に電子証明書を選択することを特徴とする。

[0011] 前記証明書選択部は、

前記制御部が実行するプログラムに関する情報として、少なくともプログラムの名称を用いることを特徴とする。

[0012] 前記認証装置接続部は、

同時に複数の認証装置を接続することを特徴とする。

[0013] 前記認証装置接続部は、

1つ以上の電子証明書と当該電子証明書それぞれの利用を制限する利用条件とを記憶する認証装置と、1つ以上の電子証明書を記憶するが利用条件を記憶しない認証装置とを同時に接続し、

前記利用条件受信部は、

利用条件を記憶しない認証装置からは利用条件を受信せず、

前記利用条件格納部は、

前記利用条件受信部が利用条件を受信しなかった場合、予め定められた利用条件を記憶することを特徴とする。

[0014] 前記端末装置は、さらに、

前記通信部が暗号通信に利用する電子証明書の利用条件を暗号通信先から取得する利用条件取得部を備え、

前記利用条件格納部は、

前記利用条件受信部が受信した利用条件に加えて、前記利用条件取得部が取得した利用条件を記憶することを特徴とする。

[0015] 前記利用条件取得部は、

利用条件として、少なくとも前記通信部が暗号通信に利用する電子証明書を発行した証明書発行局の名称を取得することを特徴とする。

[0016] また、本発明の認証装置は、

電子証明書を利用した暗号通信を行う端末装置を接続する端末装置接続部と、

1つ以上の電子証明書を記憶する証明書記憶部と、

前記証明書記憶部に記憶された電子証明書それぞれの利用を制限する利用条件を記憶する利用条件記憶部と、

前記端末装置接続部が接続する端末装置に前記利用条件記憶部に記憶された利用条件を送信する利用条件送信部と、

前記端末装置接続部が接続する端末装置に前記証明書記憶部に記憶された電子証明書を送信する証明書送信部とを備えることを特徴とする。

[0017] 前記利用条件記憶部は、

前記端末装置接続部が接続する端末装置の暗号通信先に関する情報を用いて前記証明書記憶部に記憶された電子証明書それぞれの利用を制限する利用条件を記憶することを特徴とする。

[0018] 前記利用条件記憶部は、

前記端末装置接続部が接続する端末装置の暗号通信先に関する情報として、少なくとも暗号通信先のホスト名を用いることを特徴とする。

[0019] 前記利用条件記憶部は、

前記端末装置接続部が接続する端末装置が実行するプログラムに関する情報を用いて前記証明書記憶部に記憶された電子証明書それぞれの利用を制限する利用条件を記憶することを特徴とする。

[0020] 前記利用条件記憶部は、

前記端末装置接続部が接続する端末装置が実行するプログラムに関する情報として、少なくともプログラムの名称を用いることを特徴とする。

[0021] また、本発明の暗号通信方法は、

電子証明書を利用した暗号通信を行う端末装置を用い、

前記端末装置が、

1つ以上の電子証明書と当該電子証明書それぞれの利用を制限する利用条件とを記憶する認証装置と接続し、

利用条件を前記認証装置から受信し、

受信した利用条件を記憶し、

記憶された利用条件を基に電子証明書を選択し、

選択した電子証明書を前記認証装置から受信し、

受信した電子証明書を利用して暗号通信を行うことを特徴とする。

[0022] 前記暗号通信方法は、さらに、

前記端末装置が、

選択した電子証明書を一意的に識別する識別情報を出力し、

出力した識別情報をユーザに選択させ、

ユーザに選択させた識別情報に対応する電子証明書を前記認証装置から受信することを特徴とする。

[0023] また、本発明の証明書提供方法は、

電子証明書を記憶する認証装置を用い、

前記認証装置が、

電子証明書を利用した暗号通信を行う端末装置と接続し、

1つ以上の電子証明書を記憶し、

記憶された電子証明書それぞれの利用を制限する利用条件を記憶し、

記憶された利用条件を前記端末装置に送信し、

記憶された電子証明書を前記端末装置に送信することを特徴とする。

発明の効果

[0024] 本発明により、アプリケーションがユーザ証明書を利用する時に、利用可能な証明書の候補数が減り、利用者の証明書選択の負荷を軽減することができる。

発明を実施するための最良の形態

[0025] 以下、本発明の実施の形態を図に基づいて説明する。なお、下記実施の形態1から4では、各実施の形態に係る認証装置(認証デバイス)としてICカード、メモリカード、UIM等のカードを例に説明するが、USBトークン等、他の認証デバイスにも適用可能である。

[0026] また、下記実施の形態1から4では、各実施の形態に係る端末装置として携帯電話等の情報端末を例に説明するが、PDA(Personal Digital Assistant)、パーソナルコンピュータ等、他の情報端末にも適用可能である。

[0027] 実施の形態1.

図1は本実施の形態に係る暗号通信システムの構成を示すブロック図である。

[0028] 情報端末1は、ネットワーク3を経由してサーバ4と通信を行う。情報端末1にはカード2を着脱することができる。ここで、カード2は認証デバイスの一例である。情報端末1は、表示部110(出力部)、入力部120、記憶部130(利用条件格納部)、制御部140(証明書選択部を含む)、通信部150、カード部160(認証装置接続部、利用条件受信部及び証明書受信部から成る)を備えている。本実施の形態では、情報端末は、図2に示したように、例えば携帯電話とするが、これに限定されるものではない。

[0029] 図3は情報端末1の構成を示すブロック図である。

[0030] 制御部140は、プログラムをロードして情報端末1内の各部の制御を行う。また、ユーザ証明書及びユーザ証明書の利用条件を管理し、利用可能なユーザ証明書を限定する機能を有する。図4のように、記憶部130には、利用者の入力処理を行う入力

サービス131、通信処理を行う通信サービス132、カード2の制御を行うカード制御サービス133、ユーザ証明書を選択するユーザ証明書管理サービス134、カード2から受け取ったユーザ証明書の利用条件を保持するユーザ証明書利用条件234等が記憶されている。各サービスのプログラムは制御部140によって読み出され、実行される。入力部120は、各種指示の入力や、ボタン入力、文字入力等を行う。カード部160は、情報端末1に装着されたICカードやUIM等のカード2の制御を実行する。表示部110は入力情報や出力情報の表示を行う。通信部150は、無線又は有線の通信処理を行う。

[0031] ネットワーク3は、インターネット等のネットワークを示す。サーバ4は、Webサーバ等、ネットワーク3経由で情報端末1からの処理要求に対して、処理を実施し、結果を応答する装置である。

[0032] カード2は、ICカードやUIM等、ユーザ証明書やRSA(Rivest Shamir Adleman)等の公開鍵暗号方式における秘密鍵を保持し、秘密鍵による暗号処理機能を有するカードである。

[0033] 図5のように、カード2は、制御部210、I／O部220(端末装置接続部、利用条件送信部及び証明書送信部から成る)、記憶部230(証明書記憶部及び利用条件記憶部から成る)を備えている。

[0034] カード2において、制御部210は、カード2に送付されるコマンドの解釈、実行を行う。I／O部220は各種接続機器(本実施の形態では、情報端末1)との接続を行う。記憶部230には、図6に示すように、カード2を一意的に識別するカードID231、1つ以上のユーザ証明書から成るユーザ証明書群232、各ユーザ証明書に対応する秘密鍵から成る秘密鍵群233に加えて、ユーザ証明書利用条件234が格納されている。図6では、ユーザ証明書と、それぞれのユーザ証明書に対応する秘密鍵が3つ含まれているが、異なる数でも本実施の形態に適用可能である。

[0035] ユーザ証明書利用条件234の詳細を図7に示す。

[0036] ユーザ証明書利用条件234は、カードに含まれるユーザ証明書を一意的に識別するユーザ証明書ID、ユーザ証明書が利用される時の条件の項目(本実施の形態では、接続先ホスト名と使用アプリケーション名となっているが、これに限らない)、各項

目に対して設定された値(以下、条件値という)からなる。図7の例では、ユーザ証明書利用条件234は以下を示す。

[0037] カード2にはユーザ証明書A、B、Cのユーザ証明書IDをもつ3つのユーザ証明書が存在する。ユーザ証明書Aは、接続先ホスト名が“www. xxx. com”、使用アプリケーション名が“Browser”の場合に利用できる。ユーザ証明書Bは、接続先ホスト名が“www. yyy. co. jp”、使用アプリケーション名が任意の名前の場合に利用できる。ユーザ証明書Cは、接続ホスト名が未指定、利用アプリケーション名が“TheApplication1”である場合に利用できる。アプリケーションにおいて接続ホスト名が未指定となるのは、ユーザ証明書(に対応する秘密鍵)を電子メールの署名に用いる場合のように、接続先ホストが存在しない場合である。ユーザ証明書利用条件234に使用する条件値として、例えば図8のように、ANYは任意を意味する。また、同様に、N／Aは未指定を意味する。

[0038] 次に、上記のように構成された本実施の形態の情報端末1、カード2、ネットワーク3、サーバ4の動作を詳細に説明する。なお、本実施の形態では、SSL(Secure Socket Layer)のクライアント認証におけるユーザ証明書の選択処理を記述しているが、保持する複数のユーザ証明書から利用するユーザ証明書を一つ選択する処理を行うあらゆる暗号処理システムに適用可能である。

[0039] 図9はユーザ証明書の選択処理を含む暗号認証通信の一連動作を示すメッセージシーケンス図である。図10、図11、図12は、順番に、カード2、情報端末1、サーバ4のユーザ証明書の選択処理を含む暗号認証通信の一連動作における処理の流れを示すフロー図である。

[0040] 情報端末1にカード2が装着されると(ステップS1001及びステップS1101)、情報端末1はカード2との通信路を確立し、ユーザ証明書利用条件234の送付をカード2に要求する(ステップS1102)。カード2は、ユーザ証明書利用条件234を情報端末1に送付する(ステップS1002)。情報端末1はユーザ証明書利用条件234を受け取ると、ユーザ証明書利用条件234を記憶部130に保存する(ステップS1103)。

[0041] 情報端末1は、サーバ4と通信路を確立する。するとサーバ4は、情報端末1にサーバ証明書を送付する(ステップS1201)。情報端末1は、受信したサーバ証明書を検

証し(ステップS1104)、検証がOK(サーバ証明書の正当性が確認できた)であれば、セッション鍵を生成する(ステップS1105)。次に、セッション鍵をサーバ証明書に含まれる公開鍵で暗号化し(ステップS1106)、サーバ4のみが復号できる暗号化されたセッション鍵をサーバ4に送付する(ステップS1107)。サーバ4は、暗号化されたセッション鍵を受信するとサーバの秘密鍵で復号する(ステップS1202)。この時点で情報端末1とサーバ4は、セッション鍵を安全に共有したこととなる。

[0042] 次に、サーバ4は、情報端末1の認証を行う。まず、サーバ4は、ユーザ証明書送付要求を情報端末1に送付する(ステップS1203)。ユーザ証明書送付要求を受信した情報端末1は、現在保持する4つのユーザ証明書から送付する1つの証明書を選択するために、これから行おうとする暗号通信において、ユーザ証明書利用条件234の条件項目、“接続先ホスト名”と“利用アプリケーション名”に対応する値(以下、現状値という)を取得する(ステップS1108)。

[0043] 図13は、情報端末1が行うユーザ証明書利用条件234の現状値取得の処理を示すフロー図である。

[0044] 今、ブラウザがURL“https://www.xxx.com/index.htm”にアクセスしようとしているとする。ユーザ証明書利用条件234が図7のような内容であるとすると、ブラウザは、“接続先ホスト名”が“www.xxx.com”であることを特定し(ステップS1301)、次に“利用アプリケーション”が“Browser”であることを特定する(ステップS1302)。

[0045] 次に、情報端末1の制御部140は、記憶部130からユーザ証明書管理サービス134を読み出して、以下に示すユーザ証明書選択処理を実行する(ステップS1109)。

[0046] 図14は、情報端末1が行うユーザ証明書選択の処理を示すフロー図である。

[0047] 制御部140は、ユーザ証明書利用条件234から、“接続先ホスト名”が“www.xxx.com”で、“利用アプリケーション”が“Browser”であるユーザ証明書を特定し、そのユーザ証明書IDを出力する。詳細には、図14に示したように、制御部140は、ユーザ証明書利用条件234に、接続先ホスト名の現状値と一致する証明書があるか検索する(ステップS1401)。もし複数の証明書が一致した場合、各証明書に対して、利用アプリケーション名の現状値が条件とマッチするか判断する(ステップS1402)。

この際もし複数のユーザ証明書がマッチした場合には(ステップS1403)、表示部110が、マッチしたユーザ証明書のサブジェクト名(持ち主名)等を利用者に提示し(ステップS1404)、入力部120より選択させる(ステップS1405)。そしてその結果一つのユーザ証明書が選択される(ステップS1406)。図7の例ではユーザ証明書Aが選択される。

[0048] 次に、情報端末1は、カード2にユーザ証明書Aの送付を要求する(ステップS1110)。カード2は、ユーザ証明書Aを情報端末1に送付する(ステップS1003)。情報端末1は、ユーザ証明書Aを受け取ると、そのユーザ証明書をサーバ4に送付する(ステップS1111)。また、情報端末1は、カード2に署名の送付を要求する(ステップS1112)。カード2は、ユーザ証明書Aに対応する秘密鍵を用いて署名の生成を行い(ステップS1004)、この署名を情報端末1に送付する(ステップS1005)。情報端末1は、カード2から受け取った署名をサーバ4に送付する(ステップS1113)。サーバ4では、送付されたユーザ証明書を検証する(ステップS1204)。検証がOK(ユーザ証明書の正当性が確認できた)であれば、ユーザ証明書に含まれる公開鍵を用いて、送付された署名の検証を行う(ステップS1205)。署名の検証がOK(署名の正当性が確認できた)となれば、サーバ4は通信相手である情報端末1が正しい通信相手であることが認証できたこととなる。その後、情報端末1とサーバ4は、相互に安全に共有したセッション鍵を用いて、盗聴、改ざん、成りすましの防止された暗号認証通信を行う(ステップS1114及びステップS1206)。

[0049] カード2が情報端末1から取り出された場合、情報端末1の記憶部130に保持されているユーザ証明書利用条件234は削除される。図15はカード2が情報端末1から取り出されるイメージ図、図16はカード2が情報端末1から取り出された場合の処理を示すフロー図である。以下図16を用いて情報端末1からカード2が取り出された時の処理の流れを示す。

[0050] カード2が情報端末1から取り出されるとカード部160から制御部140に対してカード2の取り出しが通知される(ステップS1601)。するとユーザ証明書管理サービス134のプログラムが制御部140にロードされ、記憶部130に保持されているユーザ証明書利用条件234を削除する(ステップS1602)。

[0051] 以上のように本実施の形態では、カード2にユーザ証明書とともにユーザ証明書利用条件234が格納され、その情報を情報端末1の記憶部130に保持する。そして、情報端末1でユーザ証明書利用条件234の項目の現状値を取得し、項目の条件値が現状値とマッチするユーザ証明書を選択する手続きにより、複数のユーザ証明書の中から利用可能なユーザ証明書を自動的に選出することができる。その結果利用者が利用可能なユーザ証明書を判断して選出する手間が軽減される。また、カード2を情報端末1から取り出した場合は、情報端末1のユーザ証明書利用条件234が削除されるので、その後ユーザ証明書を利用する要求が発生した場合に、カード部160の処理を必要とせず、記憶部130のユーザ証明書利用条件リスト135を調べるだけで利用できる証明書がないと判断できる。

[0052] 実施の形態2.

本実施の形態では、図17のように、情報端末1に対して2枚のカードを装着する。各カードの構成は実施の形態1の図5、図6に示したものと同一である。情報端末1の構成には、図18、図19に示したように第2カード部161が追加されている。また、実施の形態1におけるカード部160を第2カード部161と区別するため、第1カード部160と呼ぶ。

[0053] 第1カード5、第2カード6を装着した場合、それぞれのカードのユーザ証明書利用条件234を情報端末1に格納する必要がある。そこで、情報端末1は、図20のように、複数のユーザ証明書利用条件234を含むユーザ証明書利用条件リスト135を記憶部130に保持する。

[0054] 図21は、第1カード5、第2カード6を装着したとき、ユーザ証明書利用条件リスト135にユーザ証明書利用条件234が追加される処理の流れを示すフロー図である。

[0055] 情報端末1に第1カード5が装着されると(ステップS2101)、情報端末1は第1カード5との通信路を確立し、ユーザ証明書利用条件234の送付を第1カード5に要求する(ステップS2102)。第1カード5は、ユーザ証明書利用条件234とカードID231を結合して情報端末1に送付する。図22に第1カード5が送付するユーザ証明書利用条件234とカードID231を結合した情報を示す。情報端末1はユーザ証明書利用条件234とカードID231を受け取ると、図23のようにそれらを一つの要素としてユーザ

証明書利用条件リスト135を生成する(ステップS2103)。

[0056] 情報端末1に第2カード6が装着されると(ステップS2104)、情報端末1は第2カード6との通信路を確立し、ユーザ証明書利用条件234の送付を第2カード6に要求する(ステップS2105)。第2カード6は、ユーザ証明書利用条件234とカードID231を結合して情報端末1に送付する。図24に第2カード6が送付するユーザ証明書利用条件234とカードIDを結合した情報を示す。情報端末1はユーザ証明書利用条件234とカードID231を受け取ると、図25のようにそれらを一つの要素としてユーザ証明書利用条件リスト135を更新する(ステップS2106)。

[0057] 図25に示したユーザ証明書利用条件リスト135を情報端末1が保持した状態で、ユーザ証明書の選択が必要となった場合、実施の形態1と同様に、ユーザ証明書利用条件234の項目の現状値を取得して、その現状値に条件値がマッチするユーザ証明書を選択する。現状値に適合するユーザ証明書利用条件234を持つユーザ証明書が存在した場合、そのユーザ証明書のIDを出力する。例えば、ブラウザが“https://www.zzz.org/index.html”にアクセスすることによって、SSLクライアント認証が発生した場合、ユーザ証明書利用条件234の項目“接続先ホスト名”の現状値は“www.zzz.org”となり、“利用アプリケーション名”は“Browser”となる。そして、これらの現状値とマッチする条件値をもつユーザ証明書をユーザ証明書利用条件リスト135から検索すると、“ユーザ証明書D”がマッチして出力される。情報端末1がユーザ証明書Dを取得する場合は、ユーザ証明書管理サービス134が、ユーザ証明書Dを保持するカードのIDが91485であることをユーザ証明書利用条件リスト135から特定し、カードID“91485”のカード、即ち第2カード6と通信路を確立し、証明書IDがユーザ証明書Dの証明書を取得する。そして、それをアプリケーションに返す。

[0058] カードを取り出した際には、実施の形態1と同様に情報端末1は、取り出されたカードのカードID231を取得し、そのカードID231に対応づけられたユーザ証明書利用条件リスト135内のユーザ証明書利用条件234を削除する。

[0059] 以上のように本実施の形態では、2枚のカードを情報端末1に装着した場合でも、情報端末1が、各カードに格納されたユーザ証明書利用条件234を保持できるユーザ証明書利用条件リスト135を有する。そして、情報端末1は、ユーザ証明書利用条

件リスト135から、ユーザ証明書利用条件234の項目の現状値が条件値に適合するユーザ証明書IDを得ることができるので、利用者が利用可能なユーザ証明書を判断して選出する手間が軽減される。

[0060] 本実施の形態では、2枚のカードが同時に装着できる情報端末1の例を記載したが、N枚(Nは2以上の整数とする)のカードを同時に装着できる情報端末1の場合でも、ユーザ証明書利用条件リスト135に含まれるユーザ証明書利用条件234の要素がNになるだけで、ユーザ証明書の選択の手順は同様である。

[0061] 実施の形態3.

本実施の形態では、情報端末1が2枚のカードを装着でき、そのうちの1枚のカード(旧型のカードとする)がユーザ証明書利用条件234を保持しない場合でも、旧型のカードのユーザ証明書が選択候補に含まれる仕組みを記述する。

[0062] 本実施の形態では、図26のように、旧型のカードの例として携帯電話に内蔵されているUIM(内蔵UIM8)を用いる。また、ユーザ証明書利用条件234を保持するカードの例としては、メモリカードインタフェースに装着可能なICカード(外部カード7)を用いる。

[0063] 情報端末1は、外部カード7からユーザ証明書利用条件234を入手後、内蔵UIM8に対してユーザ証明書利用条件234の入手を依頼する。内蔵UIM8は、情報端末1から受け取った証明書利用条件入手要求を解釈できないのでエラーを返す。情報端末1は、内蔵UIM8がユーザ証明書利用条件234を保持しない旧型のカードであると判断して、内蔵UIM8に対してカードID231及び保持するユーザ証明書IDのみの送付を依頼する。すると内蔵UIM8は、カードID“69874”と保持するユーザ証明書ID“ユーザ証明書E”を返す。情報端末1はその情報を基に、図27のように、得ることのできなかった“接続先ホスト名”、“使用アプリケーション名”の条件値を“DEFAULT”とする。“DEFAULT”はN／A以外のあらゆる現状値とマッチするとする。また、現状値“DEFAULT”にマッチするのは“DEFAULT”のみであるとする。

[0064] 以上のように、本実施の形態では、ユーザ証明書利用条件234の項目の条件値に“DEFAULT”を追加することで、ユーザ証明書利用条件234に未対応のカードのユーザ証明書を利用することが事前にわかっているアプリケーションでは、ユーザ証

明書利用条件234の項目の現状値に“DEFAULT”を設定し、ユーザ証明書利用条件234を保持するカードのユーザ証明書を選択対象から除外することができる。また逆に、ユーザ証明書利用条件234を保持するカードが装着されても、ユーザ証明書利用条件234を保持しないカードのユーザ証明書が選択候補から除外されてしまうことを防止することができる。

[0065] 実施の形態4.

本実施の形態では、情報端末1で保持するユーザ証明書利用条件リスト135にサーバ4から送付された条件項目及び条件値を追加可能としている。

[0066] 情報端末1が、図27のようなユーザ証明書利用条件リスト135を保持しているとする。まず、サーバ4は、サーバ4が信用する証明書発行局(CA, Certificate Authority)が発行したCA証明書の持ち主名がAまたはBであることを、情報端末1で動作しているアプリケーションに通知する。すると、図28のように、そのアプリケーションがユーザ証明書利用条件リスト135に項目“サーバ4が信用しているCA証明書の持ち主名”を条件値“A, B”(AまたはB)とともに追加する。

[0067] アプリケーションは、カード2から入手したユーザ証明書利用条件234にマッチするユーザ証明書を特定した後、そのマッチしたユーザ証明書の上位CA証明書が、A又はBであるかを判定し、その判定をパスしたユーザ証明書を、利用するユーザ証明書とする。そして、利用するユーザ証明書の特定後、情報端末1はサーバ4から送付された条件項目及び条件値をユーザ証明書利用条件リスト135から削除する。

[0068] 以上のように、本実施の形態では、カードから入手したユーザ証明書利用条件234にマッチするユーザ証明書の中から、さらに、サーバ4から送付された条件に適合したユーザ証明書を選択するので、他の実施の形態と比較して利用可能なユーザ証明書がさらに限定され、利用者が利用するユーザ証明書を判断する負荷が軽減される。

[0069] 前述した各実施の形態で、情報端末1、サーバ4は、コンピュータで実現できるものである。

図示していないが、情報端末1、サーバ4は、プログラムを実行するCPU(Central Processing Unit)を備えている。

[0070] 例えば、CPUは、バスを介して、ROM(Read Only Memory)、RAM(Random Access Memory)、通信ボード、表示装置、K／B(キーボード)、マウス、FDD(Flexible Disk Drive)、CDD(コンパクトディスクドライブ)、磁気ディスク装置、光ディスク装置、プリンタ装置、スキャナ装置等と接続されている。

RAMは、揮発性メモリの一例である。ROM、FDD、CDD、磁気ディスク装置、光ディスク装置は、不揮発性メモリの一例である。これらは、記憶装置あるいは記憶部の一例である。

前述した各実施の形態の情報端末1、サーバ4が扱うデータや情報は、記憶装置あるいは記憶部に保存され、情報端末1、サーバ4の各部により、記録され読み出されるものである。

[0071] また、通信ボードは、例えば、LAN、インターネット、或いはISDN等のWAN(ワイドエリアネットワーク)に接続されている。

[0072] 磁気ディスク装置には、オペレーティングシステム(OS)、ウィンドウシステム、プログラム群、ファイル群(データベース)が記憶されている。

プログラム群は、CPU、OS、ウィンドウシステムにより実行される。

[0073] 上記情報端末1、サーバ4の各部は、一部或いはすべてコンピュータで動作可能なプログラムにより構成しても構わない。或いは、ROMに記憶されたファームウェアで実現されていても構わない。或いは、ソフトウェア或いは、ハードウェア或いは、ソフトウェアとハードウェアとファームウェアとの組み合わせで実施されても構わない。

[0074] 上記プログラム群には、実施の形態の説明において「ー部」として説明した処理をCPUに実行させるプログラムが記憶される。これらのプログラムは、例えば、C言語やHTMLやSGMLやXMLなどのコンピュータ言語により作成される。

[0075] また、上記プログラムは、磁気ディスク装置、FD(Flexible Disk)、光ディスク、CD(コンパクトディスク)、MD(ミニディスク)、DVD(Digital Versatile Disk)等のその他の記録媒体に記憶され、CPUにより読み出され実行される。

[0076] このように、上記実施の形態1で説明した暗号システムは、

情報端末とその情報端末に装着可能な、ユーザ証明書と秘密鍵と秘密鍵による暗号機能を有するカードとから構成され、カードが、カードに格納されているユーザ証

明書の利用条件を保持し、情報端末が、カードの装着を検出する手段を有し、情報端末がカード装着検出時にそのカードからユーザ証明書利用条件を読み込み情報端末に保存する格納する手段を有し、情報端末がユーザ証明書利用条件の項目の現状値を読み出す手段を有し、読み出した現状値と条件値がマッチすることを判断する手段を有し、マッチしたユーザ証明書のIDを特定する手段を有し、ユーザ証明書利用条件にマッチする複数の証明書のIDを表示する手段を有し、表示されたIDの中から一つのIDを選択する手段を有し、選択されたIDに対応するユーザ証明書をカードから取得する手段を有し、カード抜き時には情報端末に保存されているユーザ証明書利用条件を削除する手段を有することを特徴とする。

[0077] また、前記暗号システムは、カード内に保持されるユーザ証明書利用条件に接続先システムの情報が記載されていることを特徴とする。

[0078] また、前記暗号システムは、カード内に保持されるユーザ証明書利用条件に接続先システムの情報として、ホスト名が記載されていることを特徴とする。

[0079] また、前記暗号システムは、カード内に保持されるユーザ証明書利用条件に利用するアプリケーションの情報が記載されていることを特徴とする。

[0080] また、前記暗号システムは、カード内に保持されるユーザ証明書利用条件に利用するアプリケーションの情報として、アプリケーション名が記載されていることを特徴とする。

[0081] また、上記実施の形態2で説明した暗号システムは、

複数のカードを装着可能な情報端末と、その情報端末に装着可能な、ユーザ証明書と秘密鍵と秘密鍵による暗号機能を有する複数のカードとから構成され、各カードが、カードに格納されているユーザ証明書の利用条件を保持し、情報端末が、カードの装着を検出する手段を有し、情報端末がカード装着検出時に装着されたカードからユーザ証明書利用条件を読み込み情報端末に保存する格納する手段を有し、複数のカードからユーザ証明書利用条件を読み込んだ場合、それら複数のユーザ証明書利用条件をすべて情報端末に保存する格納する手段を有し、情報端末がユーザ証明書利用条件の項目の現状値を読み出す手段を有し、読み出した現状値と条件値がマッチすることを判断する手段を有し、マッチしたユーザ証明書のIDを特定す

る手段を有し、ユーザ証明書利用条件にマッチする複数の証明書のIDを表示する手段を有し、表示されたIDの中から一つのIDを選択する手段を有し、選択されたIDに対応するユーザ証明書をカードから取得する手段を有し、カード抜き時には抜いたカードに対応するユーザ証明書利用条件を情報端末に保存されているユーザ証明書利用条件から削除する手段を有することを特徴とする。

[0082] また、上記実施の形態3及び実施の形態4で説明した暗号システムは、

複数のカードを装着可能な情報端末と、その情報端末に装着可能な、ユーザ証明書と秘密鍵と秘密鍵による暗号機能を有する複数のカードとから構成され、その複数のカードが、カードに格納されているユーザ証明書の利用条件を保持するカードと、保持しないカードとから構成され、情報端末が、カードの装着を検出する手段を有し、情報端末がカード装着検出時に装着されたカードがユーザ証明書利用条件を保持する場合は、その条件を読み込み情報端末に保存する格納する手段を有し、ユーザ証明書利用条件を保持しない場合は、あらゆるユーザ証明書利用条件の現状値にマッチする条件値DEFAULTが設定されたユーザ証明書利用条件を生成し、情報端末に格納する手段を有し、情報端末がユーザ証明書利用条件の項目の現状値を読み出す手段を有し、読み出した現状値と条件値がマッチすることを判断する手段を有し、マッチしたユーザ証明書のIDを特定する手段を有し、ユーザ証明書利用条件にマッチする複数の証明書のIDを表示する手段を有し、表示されたIDの中から一つのIDを選択する手段を有し、選択されたIDに対応するユーザ証明書をカードから取得する手段を有し、カード抜き時には抜いたカードに対応するユーザ証明書利用条件を情報端末に保存されているユーザ証明書利用条件から削除する手段を有することを特徴とする。

[0083] また、前記暗号システムは、

サーバから送付されたユーザ証明書利用条件を、情報端末に保持されたユーザ証明書利用条件に追加する手段を有することを特徴とする。

[0084] また、前記暗号システムは、サーバから送付されるユーザ証明書利用条件に、サーバの信用する証明書発行局の名前が記載されていることを特徴とする。

図面の簡単な説明

[0085] [図1]実施の形態1に係る暗号通信システムの構成を示すブロック図。

[図2]実施の形態1に係る情報端末と情報端末に装着されるカードの例。

[図3]実施の形態1に係る情報端末の構成を示すブロック図。

[図4]実施の形態1に係る情報端末の記憶部の構成を示す概念図。

[図5]実施の形態1に係るカードの構成を示すブロック図。

[図6]実施の形態1に係るカードの記憶部の構成を示す概念図。

[図7]実施の形態1に係るユーザ証明書利用条件の例。

[図8]実施の形態1に係るユーザ証明書利用条件の設定値の例。

[図9]実施の形態1に係るカードと情報端末とサーバが行う処理を示すシーケンス図。

[図10]実施の形態1に係るカードが行う処理を示すフロー図。

[図11]実施の形態1に係る情報端末が行う処理を示すフロー図。

[図12]実施の形態1に係るサーバが行う処理を示すフロー図。

[図13]実施の形態1に係る情報端末が行うユーザ証明書利用条件項目の現状値取得処理を示すフロー図。

[図14]実施の形態1に係る情報端末が行うユーザ証明書選択処理を示すフロー図。

[図15]実施の形態1に係る情報端末と情報端末から取り出されるカードの例。

[図16]実施の形態1に係る情報端末が、カードが取り出される際に行う処理を示すフロー図。

[図17]実施の形態2に係る情報端末と情報端末に装着されるカードの例。

[図18]実施の形態2に係る暗号通信システムの一部の構成を示すブロック図。

[図19]実施の形態2に係る情報端末の構成を示すブロック図。

[図20]実施の形態2に係る情報端末の記憶部の構成を示す概念図。

[図21]実施の形態2に係る情報端末が行う処理を示すフロー図。

[図22]実施の形態2に係る情報端末に第1カードから送付される情報の例。

[図23]実施の形態2に係るユーザ証明書利用条件リストの例(第1カードから情報を取得した直後)。

[図24]実施の形態2に係る情報端末に第2カードから送付される情報の例。

[図25]実施の形態2に係るユーザ証明書利用条件リストの例(第2カードから情報を

取得した直後)。

[図26]実施の形態3に係る情報端末と情報端末に装着されるカードの例。

[図27]実施の形態4に係るユーザ証明書利用条件リストの例(2枚のカードから情報を取得した直後)。

[図28]実施の形態4に係るユーザ証明書利用条件リストの例(サーバから情報を取得した直後)。

符号の説明

[0086] 1 情報端末、2 カード、3 ネットワーク、4 サーバ、5 第1カード、6 第2カード、7 外部カード、8 内蔵UIM、110 表示部、120 入力部、130 記憶部、131 入力サービス、132 通信サービス、133 カード制御サービス、134 ユーザ証明書管理サービス、135 ユーザ証明書利用条件リスト、140 制御部、150 通信部、160 カード部、210 制御部、220 I/O部、230 記憶部、231 カードID、232 ユーザ証明書群、233 秘密鍵群、234 ユーザ証明書利用条件。

請求の範囲

[1] 電子証明書を利用した暗号通信を行う端末装置において、

1つ以上の電子証明書と当該電子証明書それぞれの利用を制限する利用条件とを記憶する認証装置を接続する認証装置接続部と、

前記認証装置接続部が接続する認証装置から利用条件を受信する利用条件受信部と、

前記利用条件受信部が受信した利用条件を記憶する利用条件格納部と、

前記利用条件格納部に記憶された利用条件を基に電子証明書を選択する証明書選択部と、

前記認証装置接続部が接続する認証装置から前記証明書選択部が選択した電子証明書を受信する証明書受信部と、

前記証明書受信部が受信した電子証明書を利用して暗号通信を行う通信部とを備えることを特徴とする端末装置。

[2] 前記端末装置は、さらに、

前記証明書選択部が選択した電子証明書を一意的に識別する識別情報を出力する出力部と、

前記出力部が出力した識別情報をユーザに選択させる入力部とを備え、

前記証明書受信部は、

前記認証装置接続部が接続する認証装置から前記入力部がユーザに選択させた識別情報に対応する電子証明書を受信することを特徴とする請求項1に記載の端末装置。

[3] 前記証明書選択部は、

前記利用条件格納部に記憶された利用条件と前記通信部の暗号通信先に関する情報とを比較し、その結果を基に電子証明書を選択することを特徴とする請求項2に記載の端末装置。

[4] 前記証明書選択部は、

前記通信部の暗号通信先に関する情報として、少なくとも暗号通信先のホスト名を用いることを特徴とする請求項3に記載の端末装置。

[5] 前記端末装置は、さらに、

前記通信部が行う暗号通信を利用するプログラムを実行する制御部を備え、

前記証明書選択部は、

前記利用条件格納部に記憶された利用条件と前記制御部が実行するプログラムに関する情報とを比較し、その結果を基に電子証明書を選択することを特徴とする請求項3に記載の端末装置。

[6] 前記証明書選択部は、

前記制御部が実行するプログラムに関する情報として、少なくともプログラムの名称を用いることを特徴とする請求項5に記載の端末装置。

[7] 前記認証装置接続部は、

同時に複数の認証装置を接続することを特徴とする請求項2に記載の端末装置。

[8] 前記認証装置接続部は、

1つ以上の電子証明書と当該電子証明書それぞれの利用を制限する利用条件とを記憶する認証装置と、1つ以上の電子証明書を記憶するが利用条件を記憶しない認証装置とを同時に接続し、

前記利用条件受信部は、

利用条件を記憶しない認証装置からは利用条件を受信せず、

前記利用条件格納部は、

前記利用条件受信部が利用条件を受信しなかった場合、予め定められた利用条件を記憶することを特徴とする請求項7に記載の端末装置。

[9] 前記端末装置は、さらに、

前記通信部が暗号通信に利用する電子証明書の利用条件を暗号通信先から取得する利用条件取得部を備え、

前記利用条件格納部は、

前記利用条件受信部が受信した利用条件に加えて、前記利用条件取得部が取得した利用条件を記憶することを特徴とする請求項2に記載の端末装置。

[10] 前記利用条件取得部は、

利用条件として、少なくとも前記通信部が暗号通信に利用する電子証明書を発行

した証明書発行局の名称を取得することを特徴とする請求項9に記載の端末装置。

[11] 電子証明書を記憶する認証装置において、

電子証明書を利用した暗号通信を行う端末装置を接続する端末装置接続部と、

1つ以上の電子証明書を記憶する証明書記憶部と、

前記証明書記憶部に記憶された電子証明書それぞれの利用を制限する利用条件を記憶する利用条件記憶部と、

前記端末装置接続部が接続する端末装置に前記利用条件記憶部に記憶された利用条件を送信する利用条件送信部と、

前記端末装置接続部が接続する端末装置に前記証明書記憶部に記憶された電子証明書を送信する証明書送信部とを備えることを特徴とする認証装置。

[12] 前記利用条件記憶部は、

前記端末装置接続部が接続する端末装置の暗号通信先に関する情報を用いて前記証明書記憶部に記憶された電子証明書それぞれの利用を制限する利用条件を記憶することを特徴とする請求項11に記載の認証装置。

[13] 前記利用条件記憶部は、

前記端末装置接続部が接続する端末装置の暗号通信先に関する情報として、少なくとも暗号通信先のホスト名を用いることを特徴とする請求項12に記載の認証装置。

[14] 前記利用条件記憶部は、

前記端末装置接続部が接続する端末装置が実行するプログラムに関する情報を用いて前記証明書記憶部に記憶された電子証明書それぞれの利用を制限する利用条件を記憶することを特徴とする請求項12に記載の認証装置。

[15] 前記利用条件記憶部は、

前記端末装置接続部が接続する端末装置が実行するプログラムに関する情報として、少なくともプログラムの名称を用いることを特徴とする請求項14に記載の認証装置。

[16] 電子証明書を利用した暗号通信を行う端末装置を用いた暗号通信方法において、

前記端末装置が、

1つ以上の電子証明書と当該電子証明書それぞれの利用を制限する利用条件とを記憶する認証装置と接続し、

利用条件を前記認証装置から受信し、

受信した利用条件を記憶し、

記憶された利用条件を基に電子証明書を選択し、

選択した電子証明書を前記認証装置から受信し、

受信した電子証明書を利用して暗号通信を行うことを特徴とする暗号通信方法。

[17] 前記暗号通信方法は、さらに、

前記端末装置が、

選択した電子証明書を一意的に識別する識別情報を出力し、

出力した識別情報をユーザに選択させ、

ユーザに選択させた識別情報に対応する電子証明書を前記認証装置から受信することを特徴とする請求項16に記載の暗号通信方法。

[18] 電子証明書を記憶する認証装置を用いた証明書提供方法において、

前記認証装置が、

電子証明書を利用した暗号通信を行う端末装置と接続し、

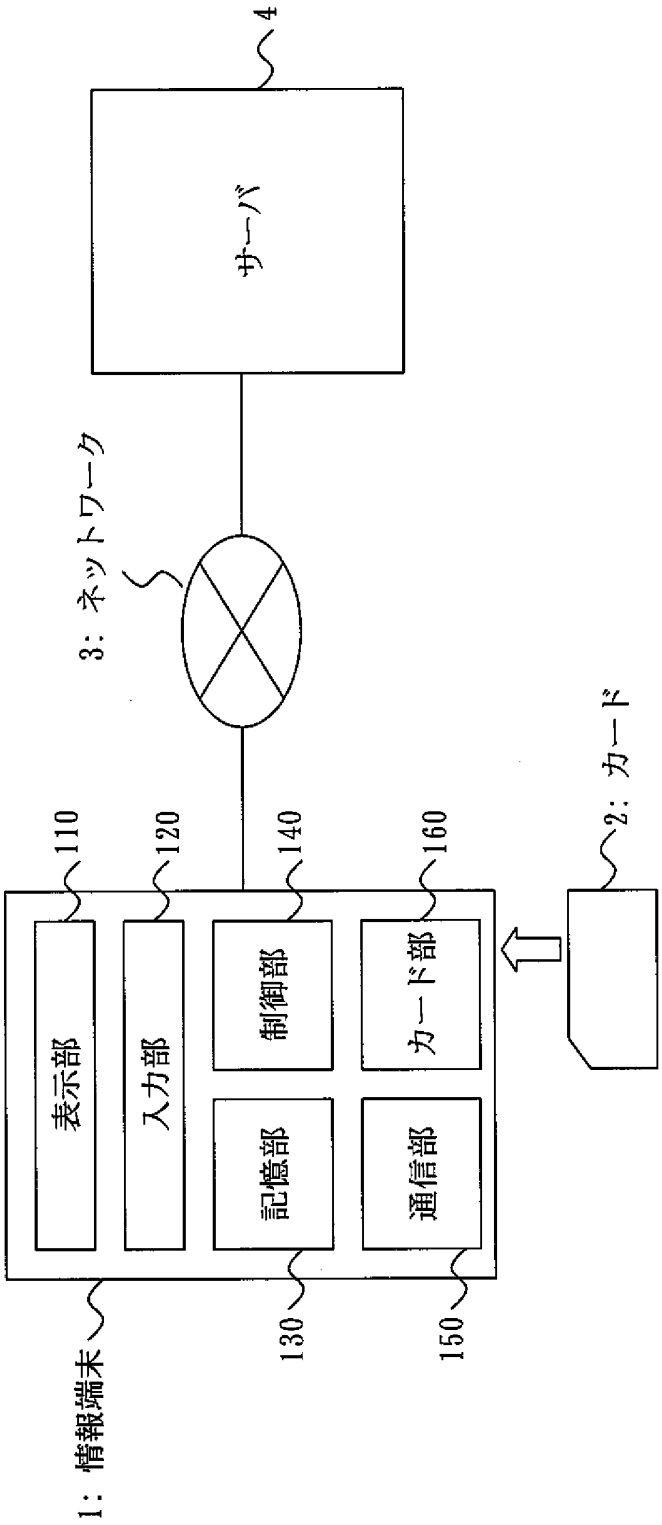
1つ以上の電子証明書を記憶し、

記憶された電子証明書それぞれの利用を制限する利用条件を記憶し、

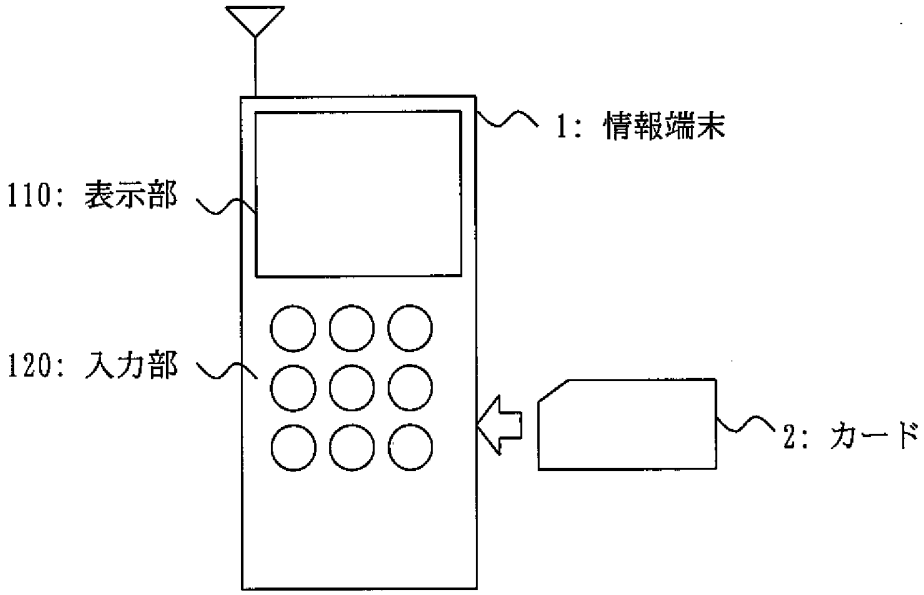
記憶された利用条件を前記端末装置に送信し、

記憶された電子証明書を前記端末装置に送信することを特徴とする証明書提供方法。

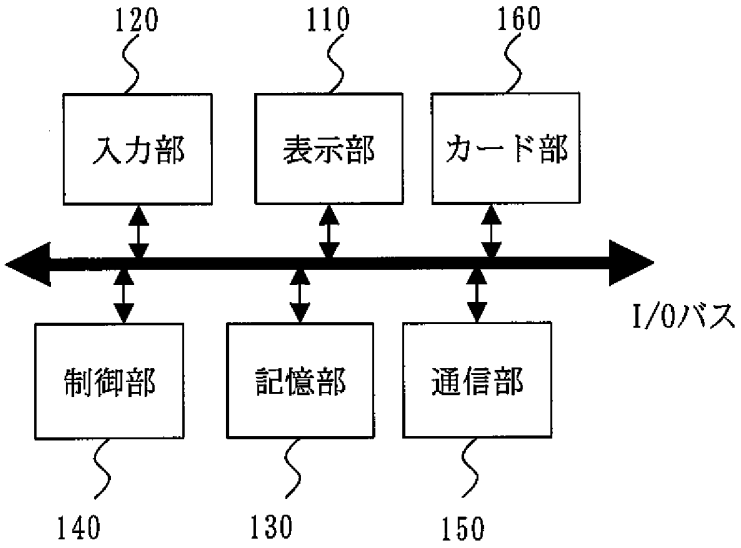
[図1]


4
サーバ
3: ネットワーク
2: カード
110
120
140
160
表示部
入力部
制御部
カード部
記憶部
通信部
130
150
1: 情報端末

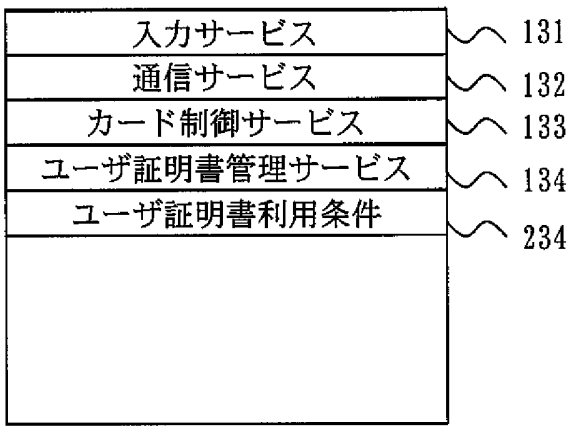
[図2]


1: 情報端末
110: 表示部
120: 入力部
2: カード

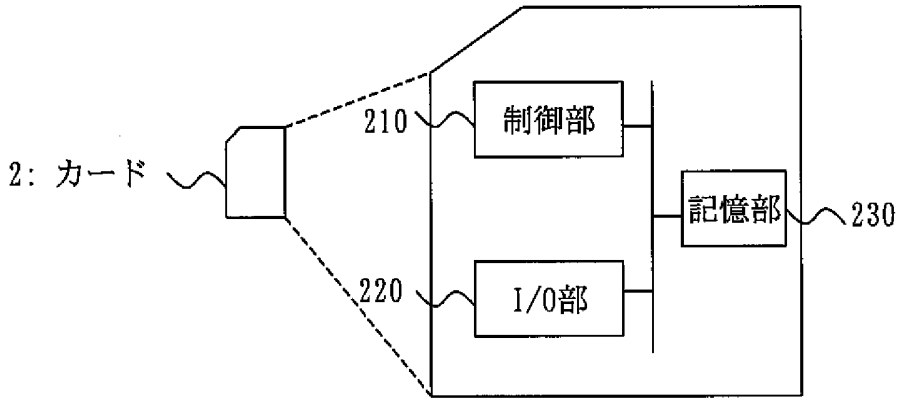
[図3]


120
110
160
入力部
表示部
カード部
I/Oバス
制御部
記憶部
通信部
140
130
150

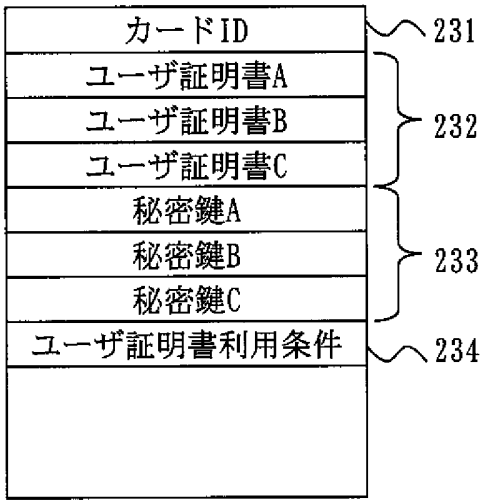
[図4]


入力サービス
131
通信サービス
132
カード制御サービス
133
ユーザ証明書管理サービス
134
ユーザ証明書利用条件
234

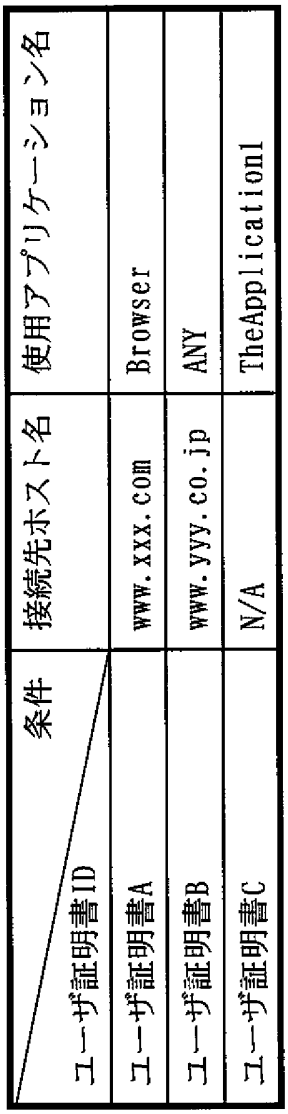
[図5]


2: カード
210
制御部
記憶部
230
220
I/O部

[図6]


カードID
231
ユーザ証明書A
ユーザ証明書B
ユーザ証明書C
232
秘密鍵A
秘密鍵B
秘密鍵C
233
ユーザ証明書利用条件
234

[図7]

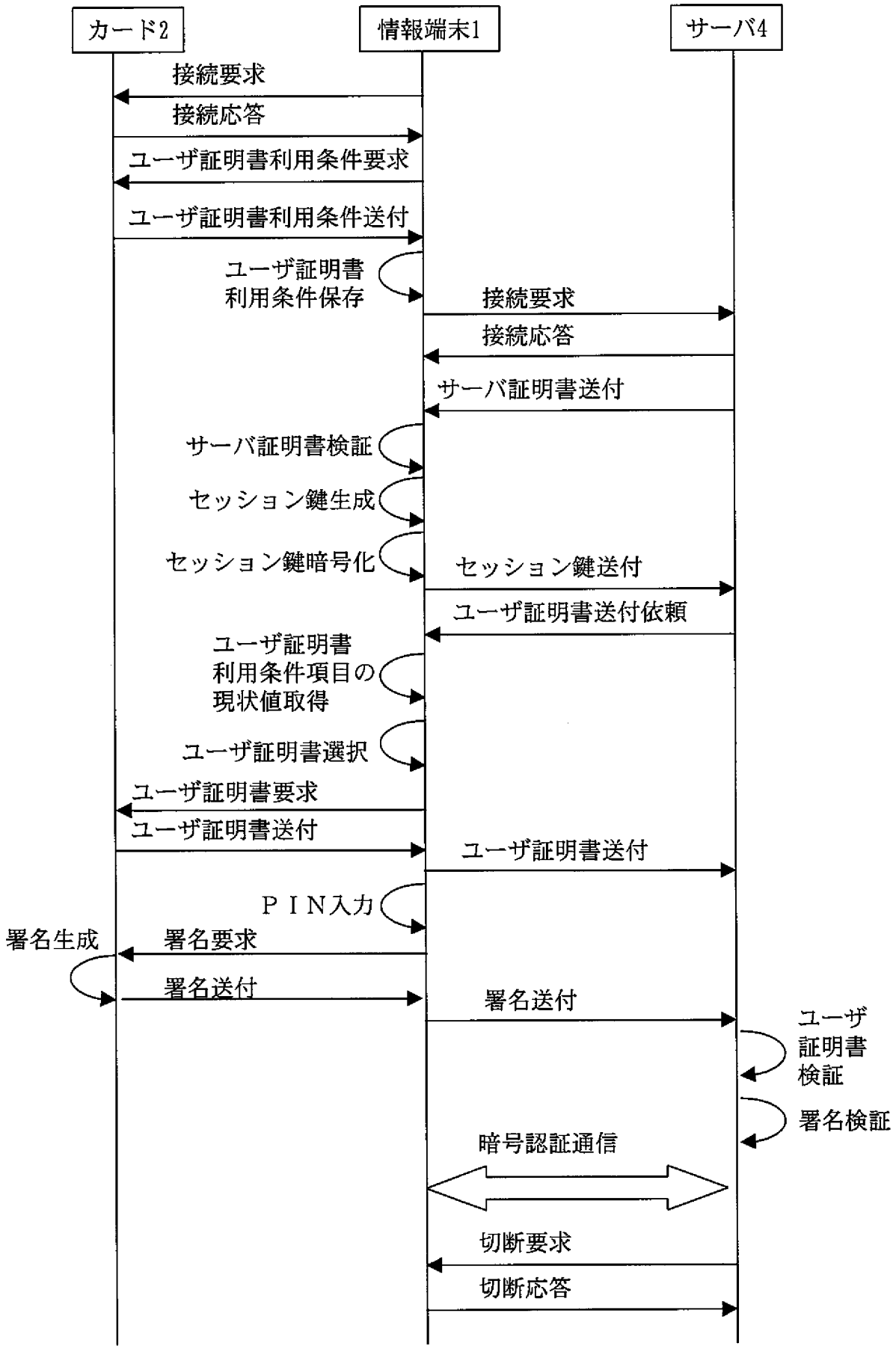


条件 / ユーザ証明書ID	接続先ホスト名	使用アプリケーション名
ユーザ証明書A	www.xxx.com	Browser
ユーザ証明書B	www.yyy.co.jp	ANY
ユーザ証明書C	N/A	TheApplication1

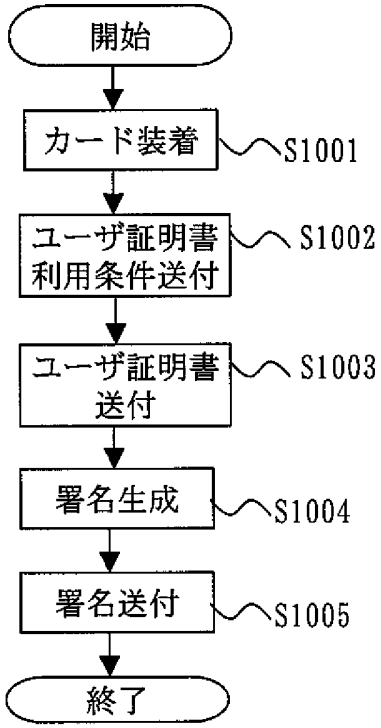
[図8]

値	意味
ANY	任意の値と一致する
N/A	項目の値がない

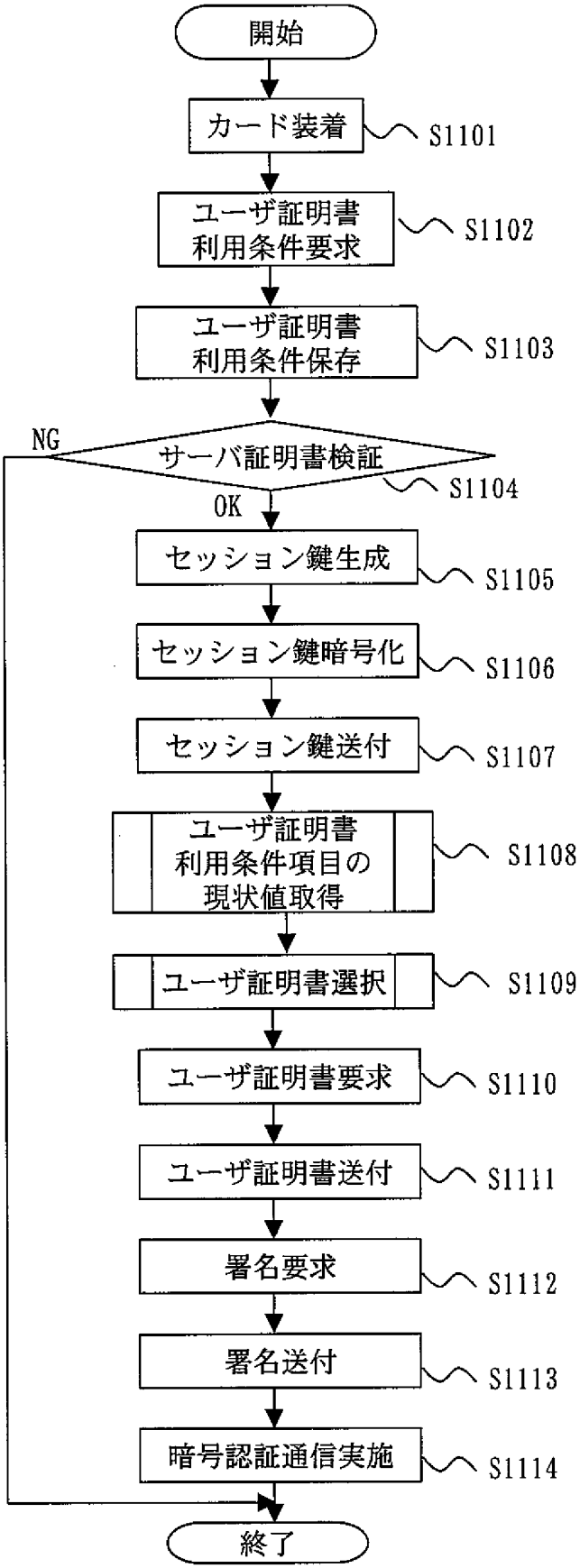
[図9]


カード2
情報端末1
サーバ4
接続要求
接続応答
ユーザ証明書利用条件要求
ユーザ証明書利用条件送付
ユーザ証明書
利用条件保存
接続要求
接続応答
サーバ証明書送付
サーバ証明書検証
セッション鍵生成
セッション鍵暗号化
セッション鍵送付
ユーザ証明書送付依頼
ユーザ証明書
利用条件項目の
現状値取得
ユーザ証明書選択
ユーザ証明書要求
ユーザ証明書送付
ユーザ証明書送付
ＰＩＮ入力
署名生成
署名要求
署名送付
署名送付
ユーザ
証明書
検証
署名検証
暗号認証通信
切断要求
切断応答

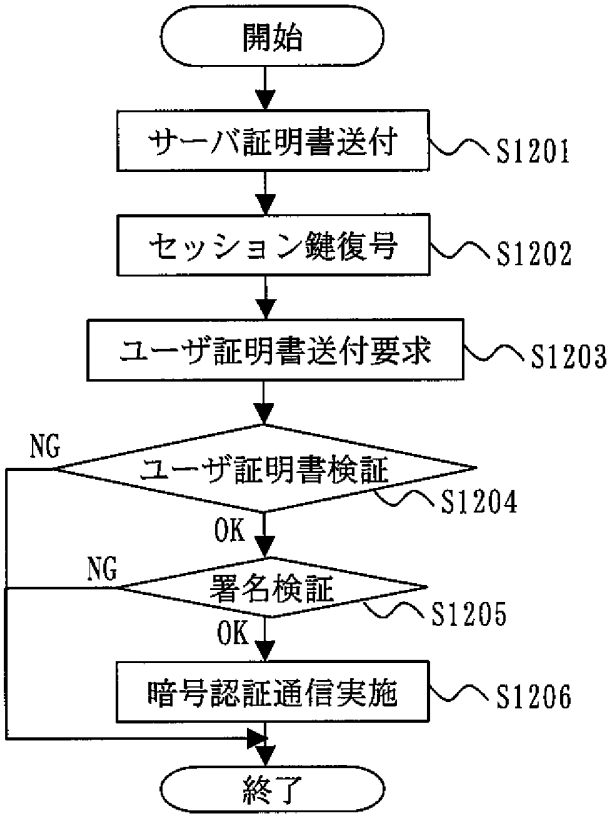
[図10]


開始
カード装着
S1001
ユーザ証明書
利用条件送付
S1002
ユーザ証明書
送付
S1003
署名生成
S1004
署名送付
S1005
終了

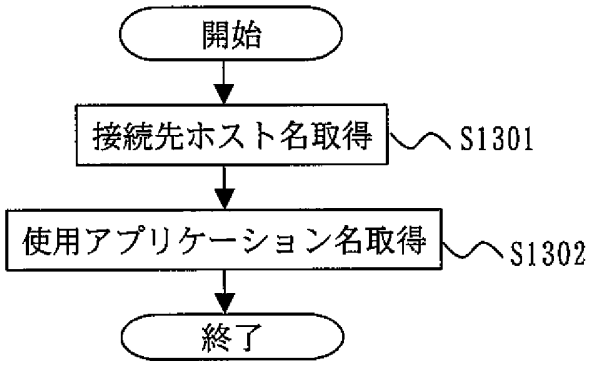
[図11]


開始
カード装着
S1101
ユーザ証明書
利用条件要求
S1102
ユーザ証明書
利用条件保存
S1103
NG
サーバ証明書検証
S1104
OK
セッション鍵生成
S1105
セッション鍵暗号化
S1106
セッション鍵送付
S1107
ユーザ証明書
利用条件項目の
現状値取得
S1108
ユーザ証明書選択
S1109
ユーザ証明書要求
S1110
ユーザ証明書送付
S1111
署名要求
S1112
署名送付
S1113
暗号認証通信実施
S1114
終了

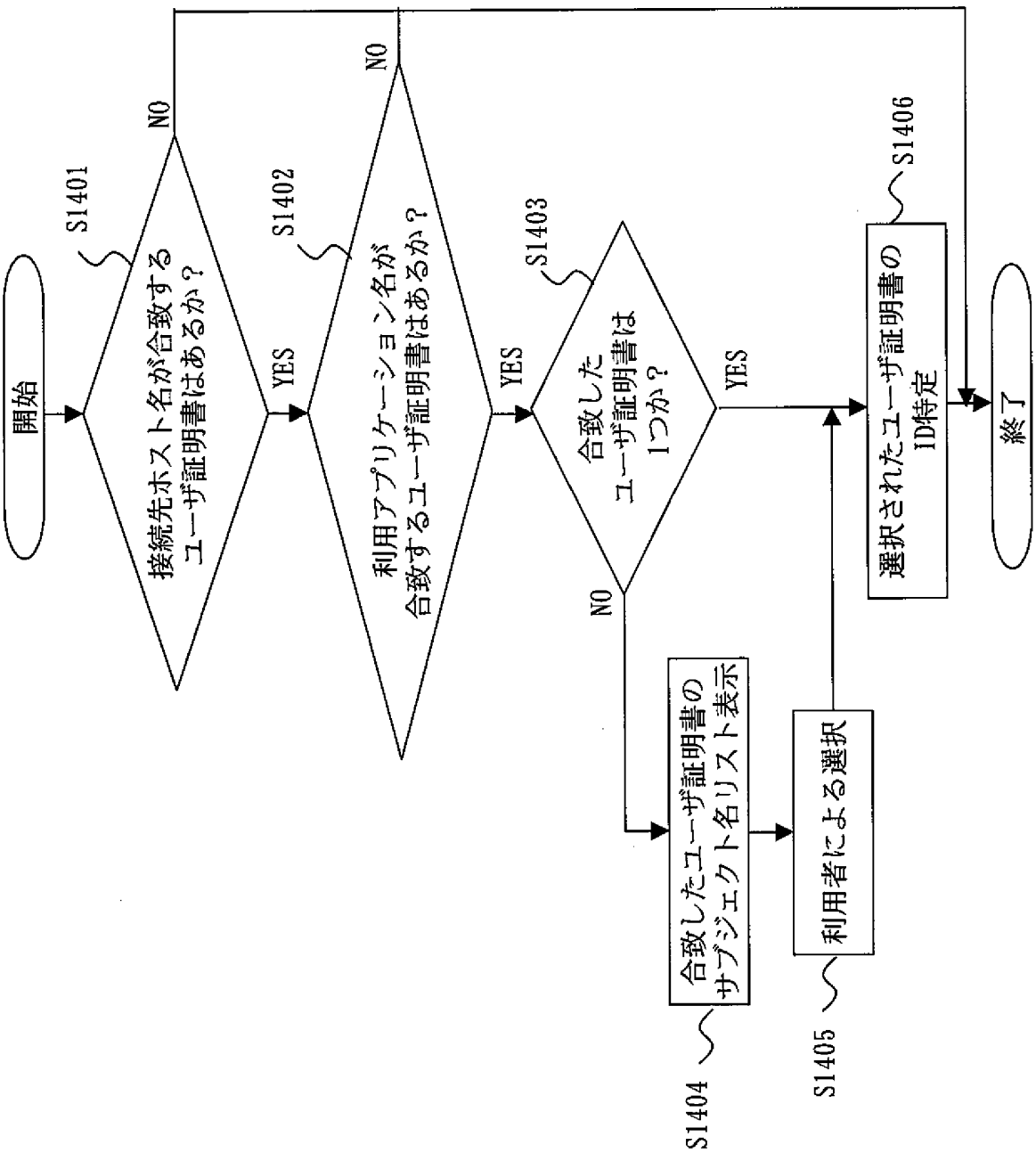
[図12]


開始
サーバ証明書送付
S1201
セッション鍵復号
S1202
ユーザ証明書送付要求
S1203
NG
ユーザ証明書検証
S1204
OK
NG
署名検証
S1205
OK
暗号認証通信実施
S1206
終了

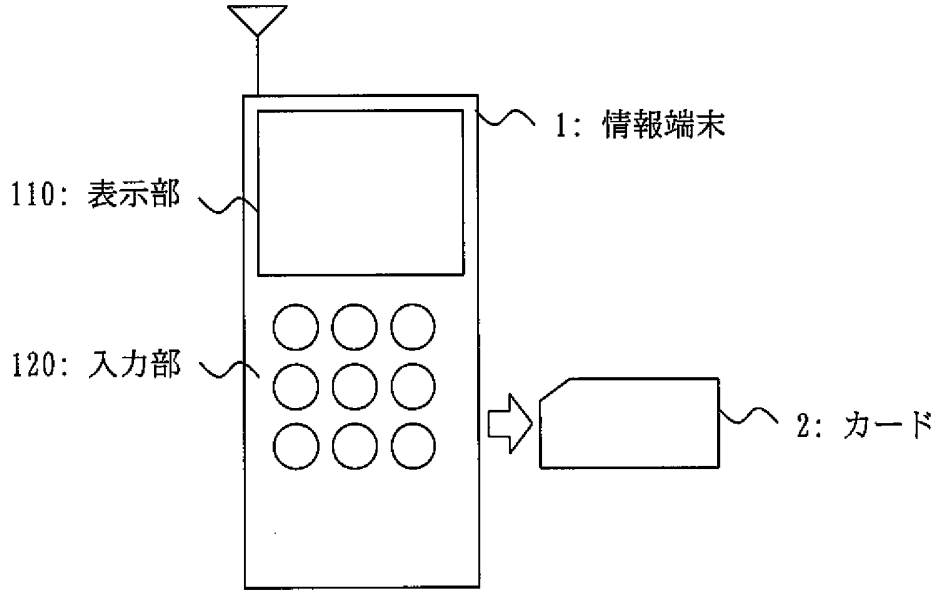
[図13]


開始
接続先ホスト名取得
S1301
使用アプリケーション名取得
S1302
終了

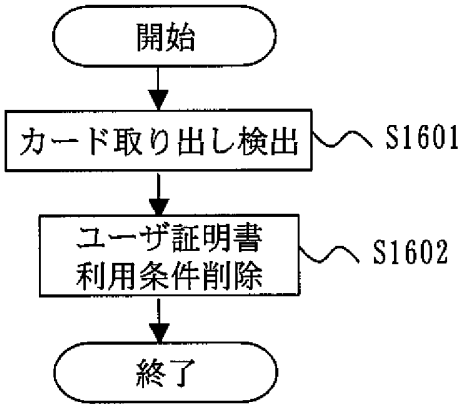
[図14]


開始
S1401
接続先ホスト名が合致する
ユーザ証明書はあるか？
NO
YES
S1402
利用アプリケーション名が
合致するユーザ証明書はあるか？
NO
YES
S1403
合致した
ユーザ証明書は
1つか？
NO
YES
S1404
合致したユーザ証明書の
サブジェクト名リスト表示
S1405
利用者による選択
S1406
選択されたユーザ証明書の
ID特定
終了

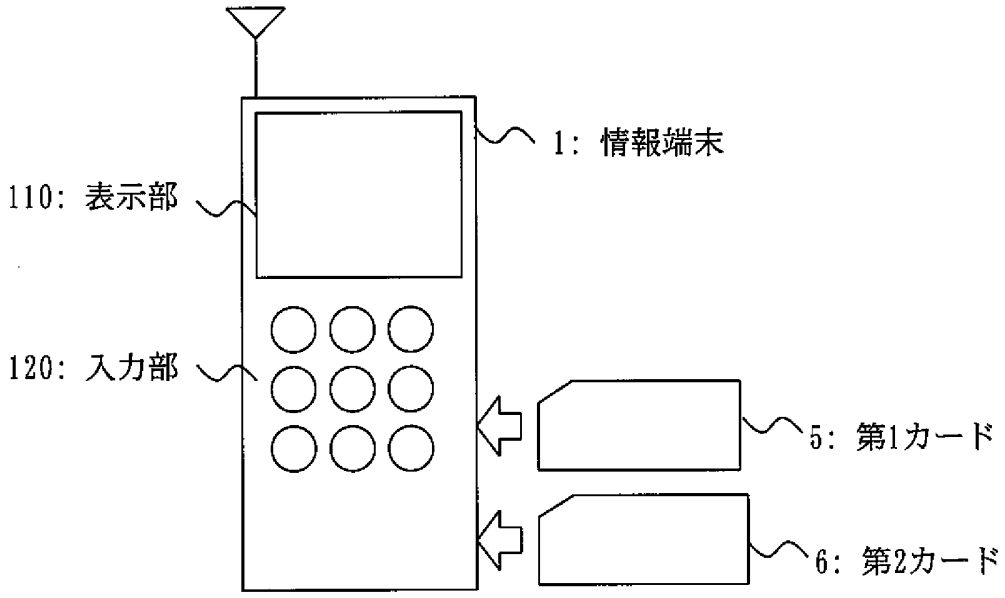
[図15]


1: 情報端末
110: 表示部
120: 入力部
2: カード

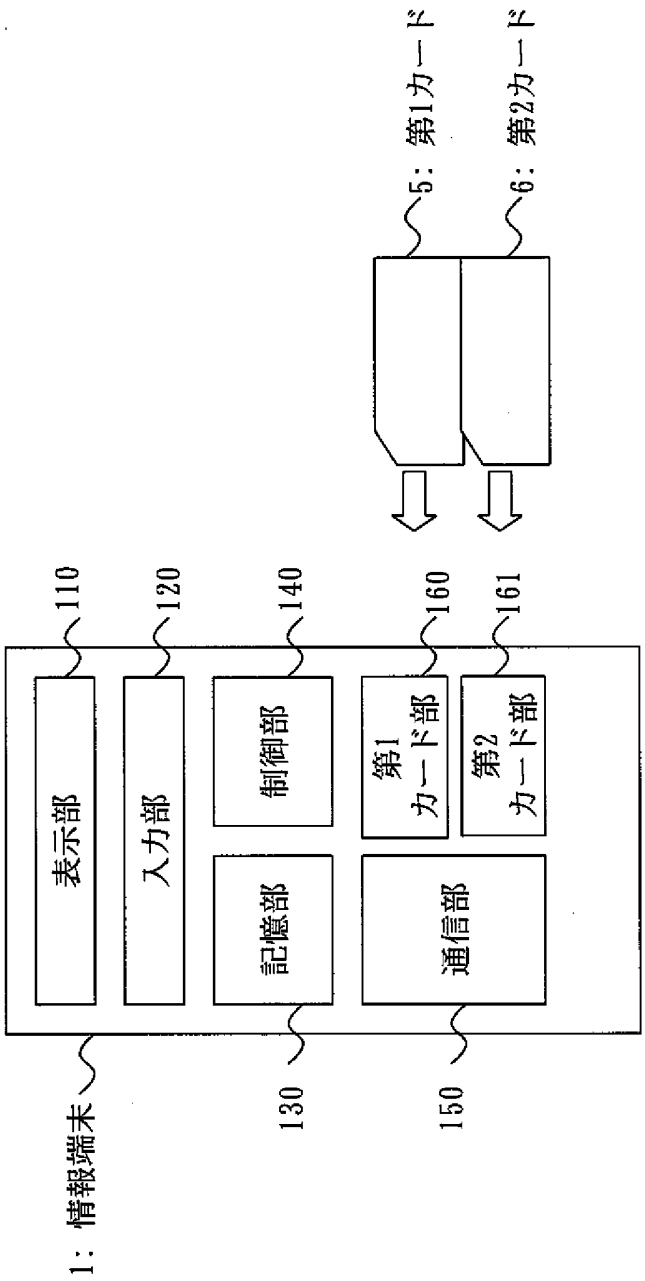
[図16]


開始
カード取り出し検出
S1601
ユーザ証明書
利用条件削除
S1602
終了

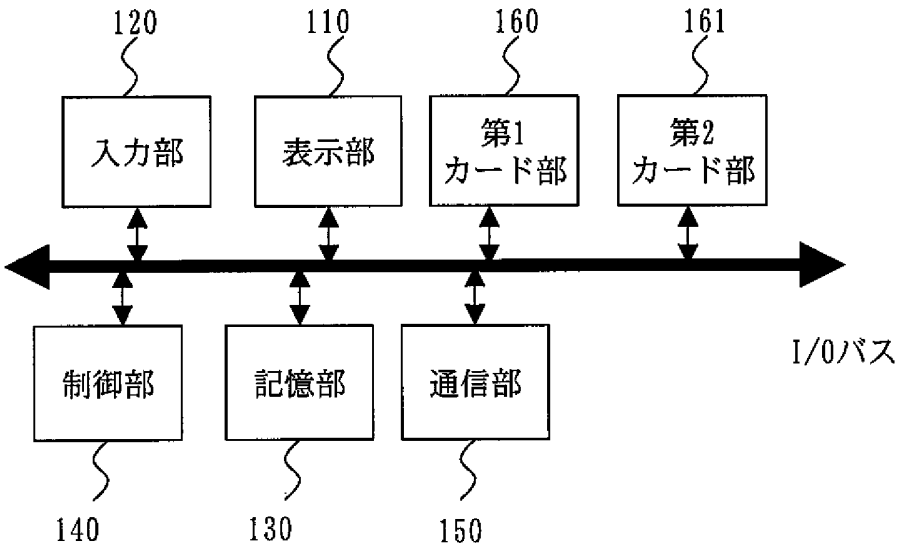
[図17]


1: 情報端末
110: 表示部
120: 入力部
5: 第1カード
6: 第2カード

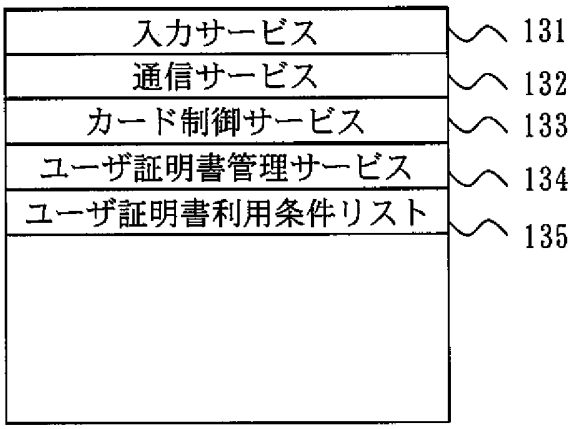
[図18]


1：情報端末
110
表示部
120
入力部
130
記憶部
140
制御部
150
通信部
160
第1
カード部
161
第2
カード部
5：第1カード
6：第2カード

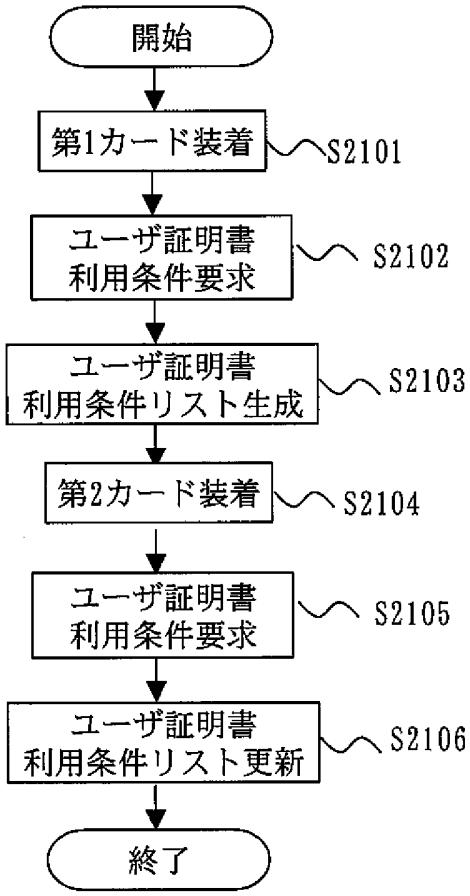
[図19]


120
110
160
161
入力部
表示部
第1
カード部
第2
カード部
制御部
記憶部
通信部
I/Oバス
140
130
150

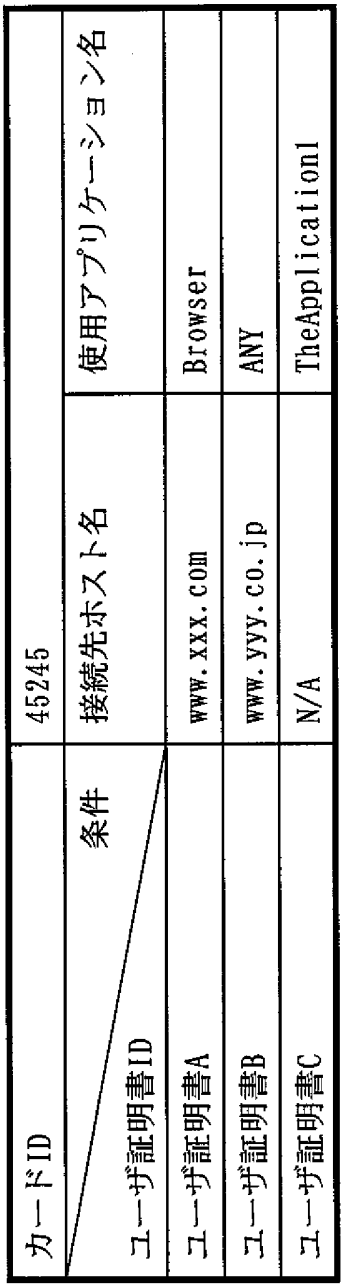
[図20]


入力サービス
131
通信サービス
132
カード制御サービス
133
ユーザ証明書管理サービス
134
ユーザ証明書利用条件リスト
135

[図21]

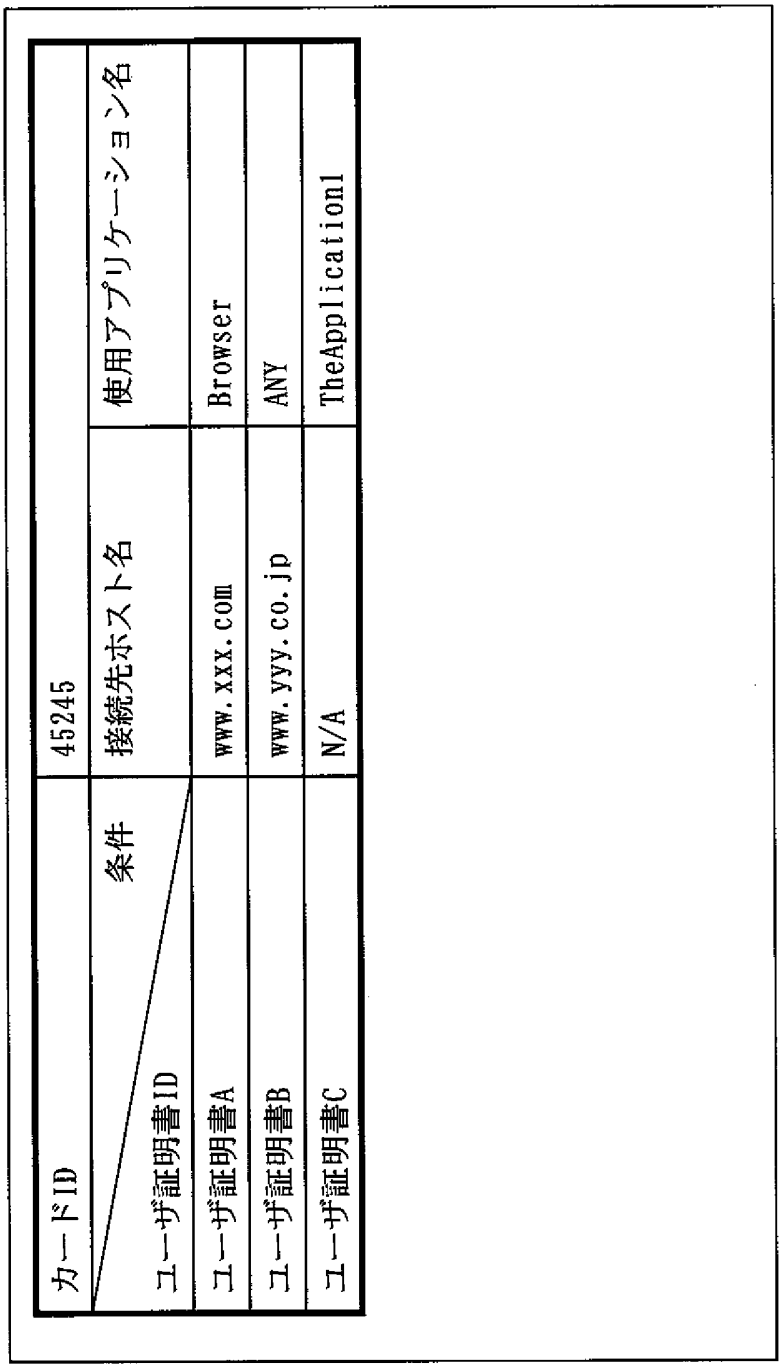

開始
第1カード装着
S2101
ユーザ証明書
利用条件要求
S2102
ユーザ証明書
利用条件リスト生成
S2103
第2カード装着
S2104
ユーザ証明書
利用条件要求
S2105
ユーザ証明書
利用条件リスト更新
S2106
終了

[図22]



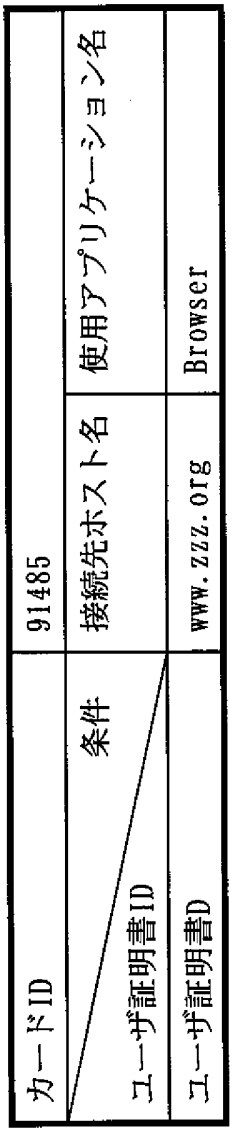
カードID	45245	
条件 / ユーザ証明書ID	接続先ホスト名	使用アプリケーション名
ユーザ証明書A	www.xxx.com	Browser
ユーザ証明書B	www.yyy.co.jp	ANY
ユーザ証明書C	N/A	TheApplication1

[図23]



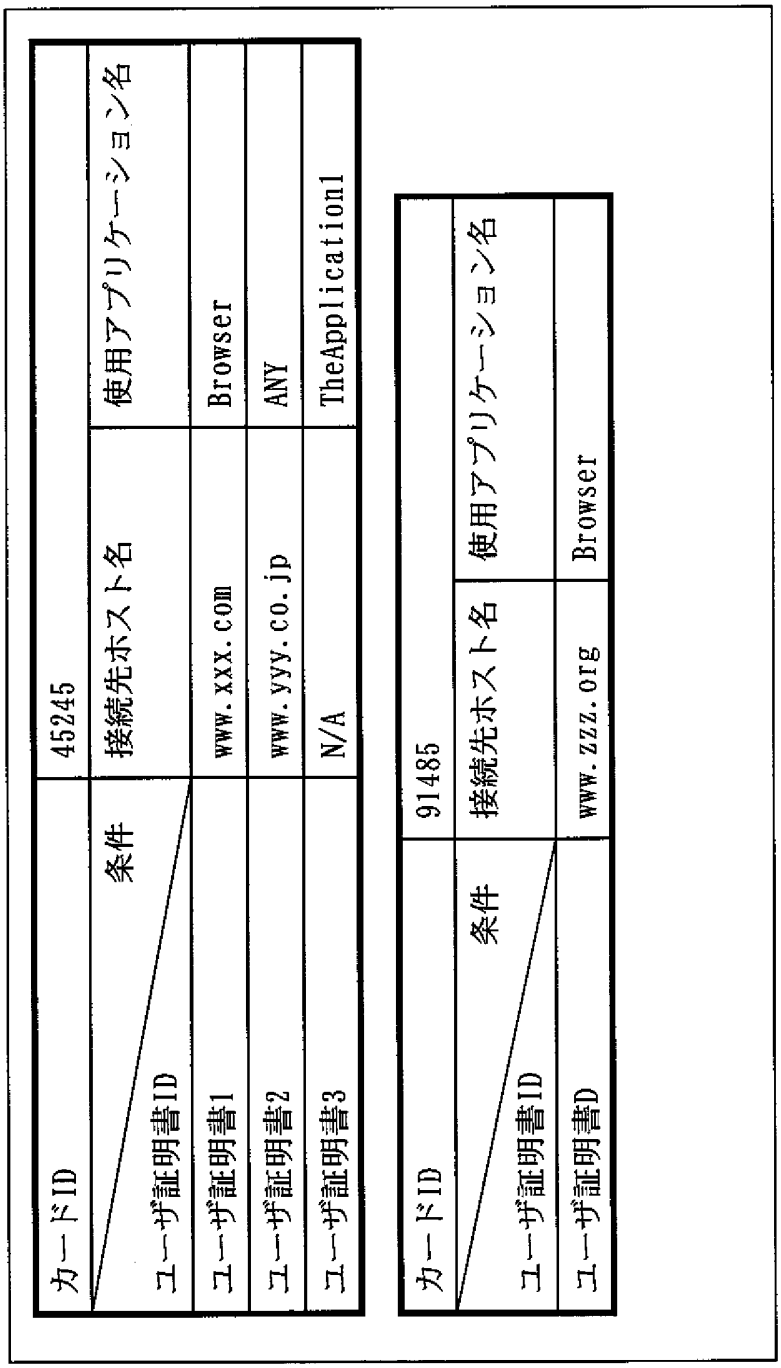
カードID	45245	
条件 / ユーザ証明書ID	接続先ホスト名	使用アプリケーション名
ユーザ証明書A	www.xxx.com	Browser
ユーザ証明書B	www.yyy.co.jp	ANY
ユーザ証明書C	N/A	TheApplication1

[図24]



カードID	91485	
条件 / ユーザ証明書ID	接続先ホスト名	使用アプリケーション名
ユーザ証明書D	www.zzz.org	Browser

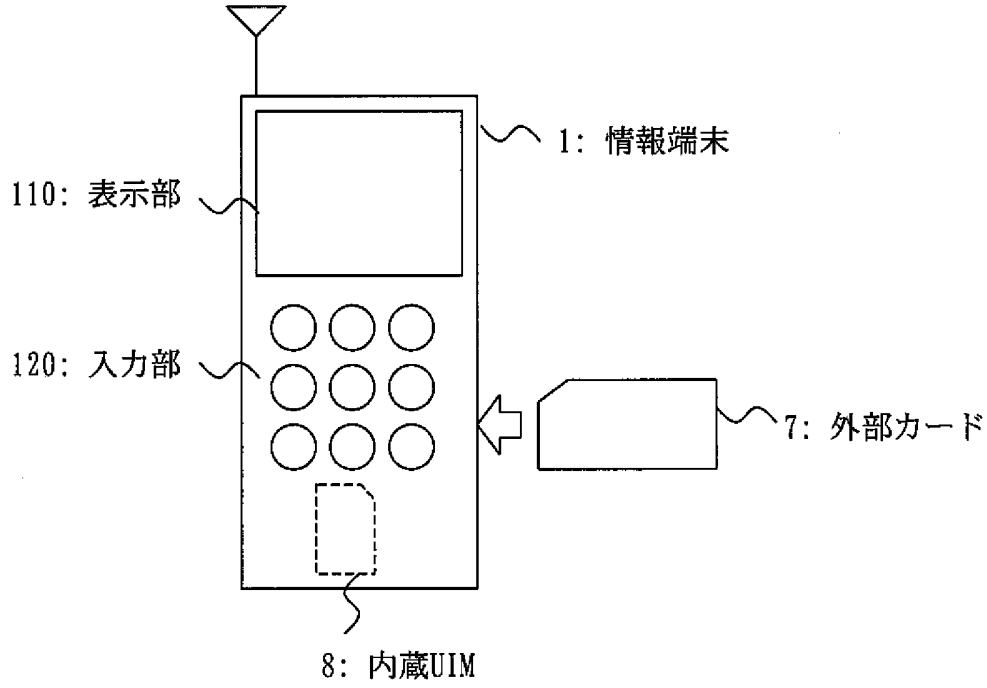
[図25]



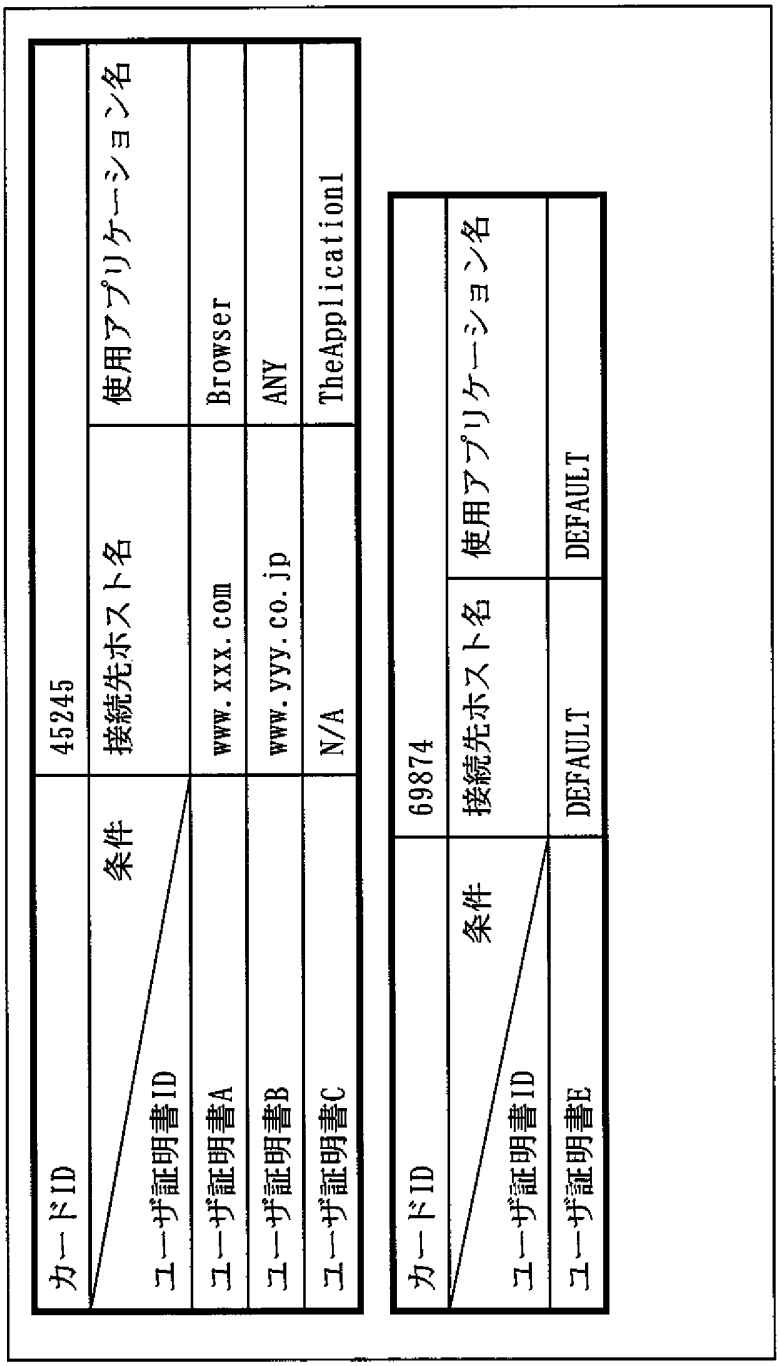
カードID	45245	
条件 / ユーザ証明書ID	接続先ホスト名	使用アプリケーション名
ユーザ証明書1	www.xxx.com	Browser
ユーザ証明書2	www.yyy.co.jp	ANY
ユーザ証明書3	N/A	TheApplication1

カードID	91485	
条件 / ユーザ証明書ID	接続先ホスト名	使用アプリケーション名
ユーザ証明書D	www.zzz.org	Browser

[図26]



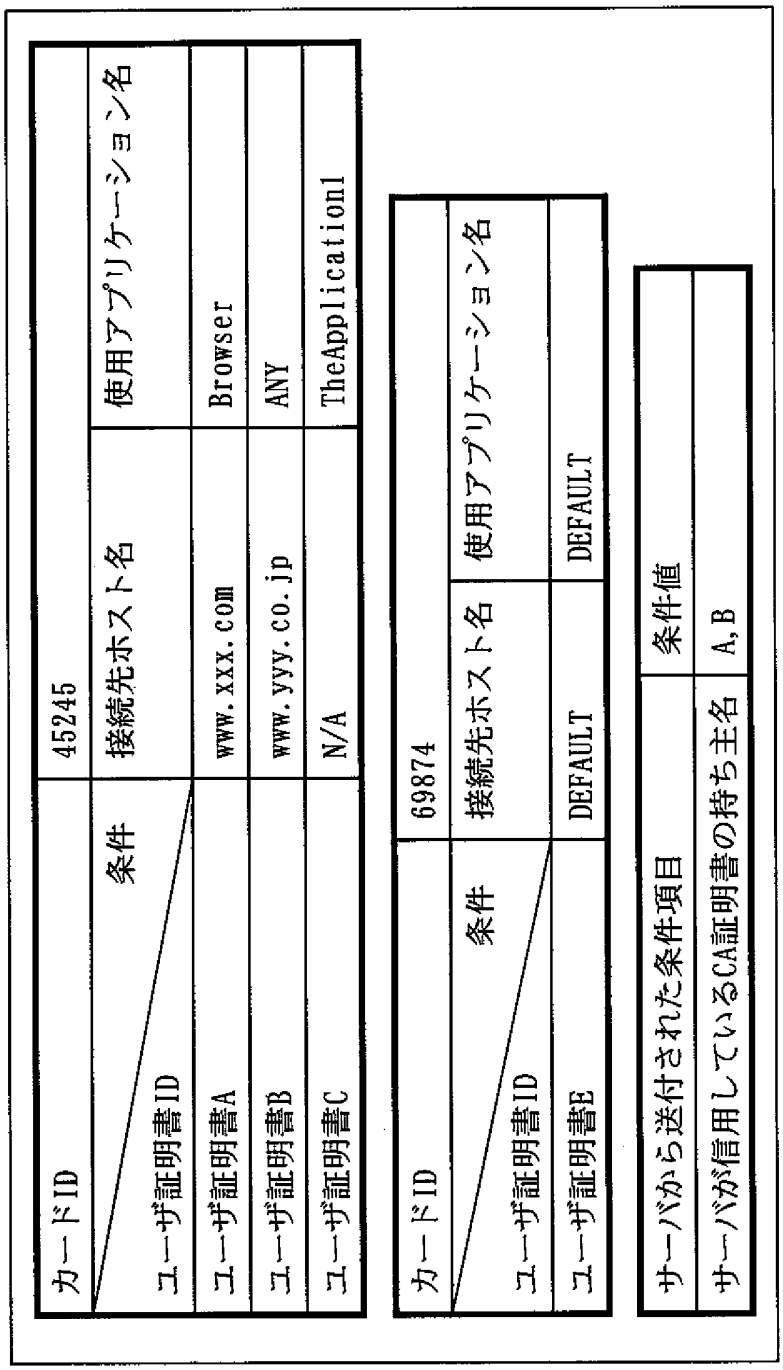
[図27]



カードID	45245	
ユーザ証明書ID ＼ 条件	接続先ホスト名	使用アプリケーション名
ユーザ証明書A	www.xxx.com	Browser
ユーザ証明書B	www.yyy.co.jp	ANY
ユーザ証明書C	N/A	TheApplication1

カードID	69874	
ユーザ証明書ID ＼ 条件	接続先ホスト名	使用アプリケーション名
ユーザ証明書E	DEFAULT	DEFAULT

[図28]


カードID
45245
条件
ユーザ証明書ID
接続先ホスト名
使用アプリケーション名
ユーザ証明書A
www.xxx.com
Browser
ユーザ証明書B
www.yyy.co.jp
ANY
ユーザ証明書C
N/A
TheApplication1
カードID
69874
条件
ユーザ証明書ID
接続先ホスト名
使用アプリケーション名
ユーザ証明書E
DEFAULT
DEFAULT
サーバから送付された条件項目
条件値
サーバが信用しているCA証明書の持ち主名
A, B

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/011963

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] H04L9/32, H04L9/08, G06F17/60, G06F15/00, G06K17/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] H04L9/32, H04L9/08, G06F17/60, G06F15/00, G06K17/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2004
Kokai Jitsuyo Shinan Koho	1971-2004	Jitsuyo Shinan Toroku Koho	1996-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP 2001-211169 A (Akinobu HATADA), 03 August, 2001 (03.08.01), Par. Nos. [0039] to [0049]; Figs. 2, 5, 6, 8 (Family: none)	1-18

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
16 November, 2004 (16.11.04)	14 December, 2004 (14.12.04)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

国際調査報告

国際出願番号　PCT／JP2004／011963

A.　発明の属する分野の分類（国際特許分類（IPC））

Int. Cl⁷　H04L9／32, H04L9／08, G06F17／60, G06F15／00, G06K17／00

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int. Cl⁷　H04L9／32, H04L9／08, G06F17／60, G06F15／00, G06K17／00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922－1996年
日本国公開実用新案公報	1971－2004年
日本国登録実用新案公報	1994－2004年
日本国実用新案登録公報	1996－2004年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X	JP　2001－211169　A（畑田　秋信） 2001．08．03 第【0039】－【0049】段落，図2，5，6，8 （ファミリーなし）	1－18

☐ C欄の続きにも文献が列挙されている。

☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの

「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）

「O」口頭による開示、使用、展示等に言及する文献

「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」同一パテントファミリー文献

国際調査を完了した日 16．11．2004	国際調査報告の発送日　14.12.2004
国際調査機関の名称及びあて先 日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官（権限のある職員）　5M　4229 青木　重徳 電話番号　03－3581－1101　内線　3597