

(19) 世界知的所有権機関
国際事務局



(43) 国際公開日
2009年5月7日 (07.05.2009)

PCT

(10) 国際公開番号
WO 2009/057771 A1

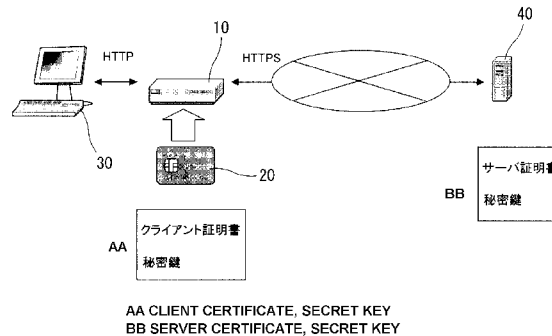
- (51) 国際特許分類:
H04L 9/32 (2006.01) G09C 1/00 (2006.01)
- (21) 国際出願番号: PCT/JP2008/069930
- (22) 国際出願日: 2008年10月31日 (31.10.2008)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願2007-285105 2007年11月1日 (01.11.2007) JP
- (71) 出願人 (米国を除く全ての指定国について): 株式会社明電舎 (MEIDENSHA CORPORATION) [JP/JP];
〒1410032 東京都品川区大崎2丁目1番1号 Tokyo
- (72) 発明者; および
- (75) 発明者/出願人 (米国についてのみ): 稲葉 佳秋 (INABA, Yoshiaki). 飯島 渉 (IIJIMA, Wataru). 松尾 泰一 (MATSUO, Takeichi). 佐藤 昌弘 (SATO, Masahiro). 荒木 義晴 (ARAKI, Yoshiharu). 前田 俊行 (MAEDA, Toshiyuki).
- (74) 代理人: 橋本 剛, 外 (HASHIMOTO, Takeshi et al.);
〒1040044 東京都中央区明石町1番29号 掖済会ビル SHIGA 内外国特許事務所内 Tokyo (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, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH,

[続葉有]

(54) Title: ELECTRONIC AUTHENTICATION DEVICE, ELECTRONIC AUTHENTICATION SYSTEM, ELECTRONIC AUTHENTICATION METHOD AND ITS PROGRAM

(54) 発明の名称: 電子認証装置、電子認証システム、電子認証方法およびこの方法のプログラム

[図1]



(57) Abstract: [PROBLEM TO BE SOLVED] Electronic authentication can be carried out with the enhancement of a security for mutual authentication while its system construction is simplified. [MEANS FOR SOLVING THE PROBLEMS] An IC card (20) stores a secret key and a client certificate. An authentication device (10) receives a request in the form of HTTP from a user terminal device (30), reads in the client certificate from the IC card, and carries out mutual authentication in the form of HTTPS for a server (40) and SSL communication. The client certificate and encrypted authentication data are directly transmitted to a server without a detour through a user terminal device. A secret number is directly input to the authentication device. Any communication except that under a domain name described in a permission list of the authentication device is cut off. The authentication device does not have its own IP address. The justification of a server certificate is made to be automatically confirmable on the authentication device side.

(57) 要約: 【課題】システム構築を簡易にしながら、相互認証のセキュリティ性を高めた電子認証ができる。【解決手段】ICカード20には秘密鍵及びクライアント証明書を記憶する。認証装置10は、ユーザ端末30からHTTP形式のリクエストを受け、ICカードから

[続葉有]



WO 2009/057771 A1



GM, GT, HN, HR, HU, ID, IL, IN, IS, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

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, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

(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,

添付公開書類:
— 国際調査報告書

クライアント証明書を読み込み、サーバ 40 に対して HTTPS 形式による相互認証、SSL 通信を行う。クライアント証明書や暗号化された認証用データはユーザ端末を経由することなく、直接にサーバに送信される。暗証番号は認証装置に直接に入力する。認証装置の許可リストに記述されているドメイン名 (URL) 以外の通信はすべて遮断する。認証装置は自身 IP アドレスを持たない。認証装置側でサーバ証明書の正当性を自動で確認可能とする。

明 細 書

電子認証装置、電子認証システム、電子認証方法およびこの方法のプログラム

技術分野

[0001] 本発明は、ユーザ端末とサーバとの暗号化通信で金融サービス等を受けるための電子認証装置、電子認証システムおよび電子認証方法に関する。

背景技術

[0002] 図13は、金融システムにおける電子認証システムの例を示し、ICカードを利用して、ユーザ端末と金融機関サーバとの暗号化通信でユーザが金融サービスを受ける際に、本人認証処理のためにユーザ端末から金融取引のセキュリティ性を高めて、第三者による不正なアクセスの防止を図る(例えば、特許文献1参照)。

[0003] 図13に示す金融システムは、サーバ1とICカードリーダライタ2を備えたユーザ端末3とICカード4から構成される。ICカード4は、秘密鍵とクライアント証明書を記憶する手段と暗号化手段を有する。ICカードリーダライタ2は、クライアント証明書及び暗号化された認証用データを読み取る手段と、認証用データをICカードに伝送する手段を有する。ユーザ端末3は、クライアント証明書及び暗号化された認証用データをサーバ1に送信する手段を有する。サーバ1は、口座情報が登録されたデータベースと、復号処理手段と、複合化された認証用データと登録されている認証用データを照合する照合手段と、照合手段で一致した場合に、金融取引サービスの処理を行う制御手段を有する。

[0004] ユーザが所有するICカード4は、外部接続用端子からなるデータ入出力手段と、CPUからなる制御手段とメモリからなる記憶手段と暗号化手段を有している。記憶手段には、暗証番号等の認証用データと秘密鍵(公開暗号化システムPKI)、クライアント証明書が記憶されている。クライアント証明書には、ユーザの公開鍵、ユーザ名、有効期間、発行社名、デジタル署名などを含んでいる。

[0005] ICカードリーダライタ2には、データ読み取り手段と、データ書き込み手段とが備えられ、ICカードから記憶されたデータの読み取り／書き込みを行うとともに、ユーザ端

末3とのデータの伝送が行えるように接続されている。

[0006] ユーザ端末3は、ユーザがキーボードから暗証番号(Personal Identified Number)等の認証用データや指示情報の入力を行うことで、本人の認証と、ユーザが希望する所望の金融取引を特定する。これには、ユーザ端末からサーバに対して、本人認証用のデータと、金融取引を特定する情報などを送信し、金融機関のサーバ1から金融サービスに冠するデータを受信する。

[0007] サーバ1は、ユーザ端末と通信を行う通信手段、金融サービス処理手段、記憶手段、復号処理手段、照合手段、制御手段、口座情報データベースなどが備える。このうち、口座データベースには、各ユーザの暗証番号との認証データ、口座番号、預金データ、取引履歴情報などが登録されている。金融サービス処理手段は、ユーザが要求する処理を口座情報データベースのデータに基づいて行う。復号処理手段は、ユーザ端末より受信した暗号化された認証データとクライアント証明書に基づいて、公開鍵で暗号化された認証用データを複合化する。照合手段は、複合化されたデータと口座情報データベースに登録されている認証用データを照合処理することで、本人の認証処理を行う。認証処理が成功した場合に、サーバ1とユーザ端末3による金融取引制御が行われる。

特許文献1:特開2005-38222号公報

発明の開示

[0008] (課題1)

図13において、ユーザ端末3にICカードリーダライタ2を接続して認証を行うには、ユーザ端末3にドライバやPC/SCベースコンポーネント、PKCS #11モジュール、CSPモジュール、さらには、認証用のソフトウェア等のインストールが必要となり、システムへの導入に多くのソフトウェアが必要となる。また、コンピュータの再セットアップの度に、これらのソフトウェアを再インストールしなければならない、ユーザへの負担は大きい。

[0009] (課題2)

クライアント証明書及び暗号化された認証用データは、ユーザ端末3経由でサーバ1に送信されるため、ユーザ端末3がウイルス等に感染していた場合、上記データが

流出してしまう可能性がある。

[0010] (課題3)

ICカード4からクライアント証明書を取り出すときに暗証番号が必要となるが、暗証番号の入力はPC経由となるので、キーロガー等のスパイウェアに感染していた場合、暗証番号の流出の可能性がある。

[0011] (課題4)

ユーザ端末のログは、管理者権限でログインされてしまった場合は、簡単に改ざんが可能である。仮にICカードの不正利用が発覚した場合、ログが重要な証拠となるが、ユーザ端末のログは、改ざんされている可能性もあり、信頼性が低い。

[0012] (課題5)

相互認証時にサーバの証明書やドメイン名(URL)の正当性の確認を行わない利用者が多く、フィッシング等の被害も増加している。

[0013] 本発明の目的は、システム構築を簡易にしながら、相互認証のセキュリティ性を高めた電子認証装置、電子認証システム、電子認証方法およびこの方法のプログラムを提供することにある。

[0014] 本発明は、前記の課題を解決するため、以下の電子認証装置、電子認証システム、電子認証方法およびプログラムを特徴とする。

[0015] (電子認証装置の発明)

(1)ユーザ端末と、ネットワーク接続機能を有するサーバとの間の暗号化通信で電子認証を得る電子認証装置であって、

前記ユーザ端末のネットワークインタフェースと接続されてパケット通信ができ、前記サーバとはネットワークを介して接続されてパケット通信ができる手段を備え、

前記ユーザ端末からのパケットを分析して、接続先情報を取得し、その接続先情報が所望のサービスを提供するサーバへのリクエストであった場合は、秘密鍵及びクライアント証明書を使用して、前記サーバとの間で相互認証と暗号化通信を行う手段を備えたことを特徴とする。

[0016] (2)前記認証装置は、前記サービスを提供するサイトへの暗号化通信を許可する接続先情報をもつ変換許可リストを備え、前記変換許可リストに前記サーバの接続先

情報が存在するときに当該サーバとの相互認証と暗号化通信を行う手段を備えたことを特徴とする。

[0017] (3)前記認証装置は、単にパケットの中継を許可する接続先情報をもつ中継許可リストを備え、前記中継許可リストに前記サーバの接続先情報が存在するときに前記サーバに対しては単にパケットを中継する手段を備えたことを特徴とする。

[0018] (4)前記認証装置は、秘密鍵及びクライアント証明書を自装置内または、外部メディアから読み込む手段を備えたことを特徴とする。

[0019] (5)前記認証装置は、クライアント証明書を読み込むときに、前記クライアント証明書を読み込むための暗証番号を入力する手段を備えたことを特徴とする。

[0020] (6)前記認証装置は、パケット分析により接続元の情報を入手し、その情報を自身の情報として利用する手段を備えたことを特徴とする。

[0021] (7)前記認証装置は、前記許可リスト中の接続先以外のホストとの通信はすべて遮断する手段を備えたことを特徴とする。

[0022] (8)前記認証装置は、自装置内または前記外部メディアに書き込んだサーバ証明書を用いて、相互認証時にサーバの正当性をチェックできた場合のみサーバへの中継を許可する手段を備えたことを特徴とする。

[0023] (9)前記認証装置は、前記認証装置内にブラウザとそのブラウザ中のコンテンツを前記ユーザ端末に表示するブラウザ表示手段を備え、

前記ブラウザ表示手段は、前記所望のサービスを提供するサーバへのリクエストを送信し、その応答を受信し、その応答であるコンテンツをブラウザと共に前記ユーザ端末で表示できる情報として前記ユーザ端末に返す手段を備えたことを特徴とする。

[0024] (10)前記認証装置は、前記ユーザ端末からのリクエストを受けて、前記サーバと相互認証と暗号化通信を開始する手段を備え、

前記サーバは、前記相互認証後にワンタイムパスワードを前記認証装置を介して前記ユーザ端末に送信する手段を備え、

前記ユーザ端末は、前記ワンタイムパスワードを前記サーバに送信する手段を備え、

前記サーバは、前記認証装置を介して送られてきたユーザ端末からのワンタイムパ

スワードを使って前記ユーザ端末とサーバ間で暗号化通信を行う手段を備えたことを特徴とする。

[0025] (電子認証システムの発明)

(11)ユーザ端末と、ネットワーク接続機能を有するサーバとの間の暗号化通信で電子認証を得る電子認証システムであって、

前記ユーザ端末のネットワークインタフェースと接続されてパケット通信ができ、前記サーバとはネットワークを介して接続されてパケット通信ができる認証装置を備え、前記認証装置は、前記ユーザ端末からのパケットを分析して、接続先情報を取得し、その接続先情報が所望のサービスを提供するサーバへのリクエストであった場合は、秘密鍵及びクライアント証明書を使用して、前記サーバとの間で相互認証と暗号化通信を行う手段を備えたことを特徴とする。

[0026] (12)前記認証装置は、前記サービスを提供するサイトへの暗号化通信を許可する接続先情報をもつ変換許可リストを備え、前記変換許可リストに前記サーバの接続先情報が存在するときに当該サーバとの相互認証と暗号化通信を行う手段を備えたことを特徴とする。

[0027] (13)前記認証装置は、単にパケットの中継を許可する接続先情報をもつ中継許可リストを備え、前記中継許可リストに前記サーバの接続先情報が存在するときに前記サーバに対しては単にパケットを中継する手段を備えたことを特徴とする。

[0028] (14)前記認証装置は、秘密鍵及びクライアント証明書を自装置内または、外部メディアから読み込む手段を備えたことを特徴とする。

[0029] (15)前記認証装置は、クライアント証明書を読み込むときに、前記クライアント証明書を読み込むための暗証番号を入力する手段を備えたことを特徴とする。

[0030] (16)前記認証装置は、パケット分析により接続元の情報を入手し、その情報を自身の情報として利用する手段を備えたことを特徴とする。

[0031] (17)前記認証装置は、前記許可リスト中の接続先以外のホストとの通信はすべて遮断する手段を備えたことを特徴とする。

[0032] (18)前記認証装置は、自装置内または前記外部メディアに書き込んだサーバ証明書を用いて、相互認証時にサーバの正当性をチェックできた場合のみサーバへの

中継を許可する手段を備えたことを特徴とする。

[0033] (19)前記認証装置は、前記認証装置内にブラウザとそのブラウザ中のコンテンツを前記ユーザ端末に表示するブラウザ表示手段を備え、

前記ブラウザ表示手段は、前記所望のサービスを提供するサーバへのリクエストを送信し、その応答を受信し、その応答であるコンテンツをブラウザと共に前記ユーザ端末で表示できる情報として前記ユーザ端末に返す手段を備えたことを特徴とする。

[0034] (20)前記認証装置は、前記ユーザ端末からのリクエストを受けて、前記サーバと相互認証と暗号化通信を開始する手段を備え、

前記サーバは、前記相互認証後にワンタイムパスワードを前記認証装置を介して前記ユーザ端末に送信する手段を備え、

前記ユーザ端末は、前記ワンタイムパスワードを前記サーバに送信する手段を備え、

前記サーバは、前記認証装置を介して送られてきたユーザ端末からのワンタイムパスワードを使って前記ユーザ端末とサーバ間で暗号化通信を行う手段を備えたことを特徴とする。

[0035] (電子認証方法の発明)

(21)ユーザ端末と、ネットワーク接続機能を有するサーバとの間の暗号化通信で電子認証を得る電子認証方法であって、

前記ユーザ端末のネットワークインタフェースと接続されてパケット通信ができ、前記サーバとはネットワークを介して接続されてパケット通信ができる認証装置を備え、

前記認証装置は、前記ユーザ端末からのパケットを分析して、接続先情報を取得し、その接続先情報が所望のサービスを提供するサーバへのリクエストであった場合は、秘密鍵及びクライアント証明書を使用して、前記サーバとの間で相互認証と暗号化通信を行う手順を有することを特徴とする。

[0036] (22)前記認証装置は、前記サービスを提供するサイトへの暗号化通信を許可する接続先情報をもつ変換許可リストを備え、前記変換許可リストに前記サーバの接続先情報が存在するときに当該サーバとの相互認証と暗号化通信を行う手順を有することを特徴とする。

- [0037] (23)前記認証装置は、単にパケットの中継を許可する接続先情報をもつ中継許可リストを備え、前記中継許可リストに前記サーバの接続先情報が存在するときに前記サーバに対しては単にパケットを中継する手順を有することを特徴とする。
- [0038] (24)前記認証装置は、秘密鍵及びクライアント証明書を自装置内または、外部メディアから読み込む手順を有することを特徴とする。
- [0039] (25)前記認証装置は、クライアント証明書を読み込むときに、前記クライアント証明書を読み込むための暗証番号を入力する手順を有することを特徴とする。
- [0040] (26)前記認証装置は、パケット分析により接続元の情報を入手し、その情報を自身の情報として利用する手順を有することを特徴とする。
- [0041] (27)前記認証装置は、前記許可リスト中の接続先以外のホストとの通信はすべて遮断する手順を有することを特徴とする。
- [0042] (28)前記認証装置は、自装置内または前記外部メディアに書き込んだサーバ証明書を用いて、相互認証時にサーバの正当性をチェックできた場合のみサーバへの中継を許可する手順を有することを特徴とする。
- [0043] (29)前記認証装置は、前記認証装置内にブラウザとそのブラウザ中のコンテンツを前記ユーザ端末に表示するブラウザ表示手順を有し、
前記ブラウザ表示手順は、前記所望のサービスを提供するサーバへのリクエストを送信し、その応答を受信し、その応答であるコンテンツをブラウザと共に前記ユーザ端末で表示できる情報として前記ユーザ端末に返す手順を有することを特徴とする。
- [0044] (30)前記認証装置は、前記ユーザ端末からのリクエストを受けて、前記サーバと相互認証と暗号化通信を開始する手順を有し、
前記サーバは、前記相互認証後にワンタイムパスワードを前記認証装置を介して前記ユーザ端末に送信する手順を有し、
前記ユーザ端末は、前記ワンタイムパスワードを前記サーバに送信する手順を有し、
前記サーバは、前記認証装置を介して送られてきたユーザ端末からのワンタイムパスワードを使って前記ユーザ端末とサーバ間で暗号化通信を行う手順を有することを特徴とする。

[0045] (プログラムの発明)

(31) 上記(21)～(30)のいずれか1項に記載の電子認証方法における処理手順をコンピュータで実行可能にしたことを特徴とする。

図面の簡単な説明

[0046] [図1]本発明の実施形態1を示す電子認証システムの構成図。

[0047] [図2]ユーザ端末の構成図。

[0048] [図3]クライアント証明書の例。

[0049] [図4]認証装置の構成図。

[0050] [図5]許可リストの例。

[0051] [図6]イーサネットのパケットの構成図。

[0052] [図7]認証装置とサーバとの相互認証手順図。

[0053] [図8]相互認証とSSL通信の処理フロー。

[0054] [図9]本発明の実施形態2を示す電子認証システムの構成図。

[0055] [図10]相互認証とSSL通信の処理フロー。

[0056] [図11]本発明の実施形態3を示す電子認証システムの構成図。

[0057] [図12]相互認証とSSL通信の処理フロー。

[0058] [図13]電子認証システムの例。

発明を実施するための最良の形態

[0059] (実施形態1)

図1は、本発明の実施形態を示す電子認証システムの構成図であり、ユーザが端末(PC)を用いてWWWサーバと相互認証、暗号化通信を行う状況において、ユーザ端末のネットワークインターフェース(以降NICと称す)とインターネット網の間に介挿されて、自身を経由する通信内容(パケット)の解析機能をもつコンピュータ構成の認証装置10を介挿する。

[0060] このシステム構成により、ユーザ端末にICカードリーダ用のドライバや専用ソフトを導入することなく、単にPCのNICとLANケーブルの間に接続するだけで、簡単にICカードを利用した相互認証(クライアント認証)を実現できるようにする。

[0061] 認証装置10は、ICカードリーダ機能を有し、ICカード20が挿入されている場合、ユ

ユーザ端末30からのHTTP形式のリクエストを受けて、ICカードからクライアント証明書を読み込み、WWWサーバ40に対して、HTTPS形式による相互認証、SSL通信を行う。さらに、認証装置10は、ユーザ端末30に対しては、サーバ40からの応答をHTTP形式に変換してリクエストに対する応答を返す。その後は、HTTP形式とHTTPS形式の変換を行い、通信を中継する。

[0062] なお、認証装置10は、自身のIPアドレスを持たず、パケット分析の結果、取得したIPアドレスを利用する。これにより、ユーザにとって複雑な設定や操作をすることなく、簡単に相互認証、SSL通信を実現する。さらに、クライアント証明書は、ユーザ端末を経由しないで、認証装置10からサーバに直接に送信されるため、従来のセキュリティ上の問題も解決する。

[0063] 以下、各部の構成、処理機能を詳細に説明する。

[0064] (1) ユーザ端末

ユーザ端末30は、図2に示すとおり、PCにおけるディスプレイ装置としての表示部31、キーボードやマウスとしての入力部32、CPUとしての制御部33、ブラウザ機能を含むROMやRAM構成のメモリ34、HTTP形式によるパケット通信処理機能をもつ通信処理部35などを有している。

[0065] ユーザ端末30の基本的な動作としては、メモリ34のブラウザからWWWサーバ40にHTTP接続のリクエストを出すと、サーバよりユーザ端末に対してクライアント認証が要求される(サーバ側で要求画面を用意)。この要求に応じて、ユーザが認証装置10にICカード20を挿入して、付属のキー経由で暗証番号を入力することで、ICカードからクライアント証明書を読み出し、認証装置10とサーバ間で相互認証を行い、暗号化(SSL)通信を行う。このとき、認証装置10によりSSL通信(HTTPS)から平文通信(HTTP)に変換されて、中継されてきたサーバからの応答をユーザ端末30に送信する。

[0066] (2) ICカード

ICカード20は、記憶するクライアント証明書にサーバのドメイン名(URL)を登録する。一例として証明書のExtensionsに登録した例を示す(図3参照)。

[0067] (3) 認証装置

図4は、認証装置10の構成を示し、ICカード制御部11、暗証番号の入力部12、通信処理部13、14、制御部15、メモリ部16から構成される。

[0068] 通信処理部13は、ユーザ端末30に接続され、ユーザ端末からのHTTP形式でリクエストを受信及び、ユーザ端末にHTTP形式で応答を送信するパケット通信機能を担う。通信処理部14は、サーバ40に接続され、HTTP形式またはHTTPS形式でのパケット通信機能を担う。ICカード制御部11は、ICカード20に対してデータの読み取り／書き込みを担う。制御部15は、通信処理部13、14から得るパケットの分析、HTTP⇔HTTPSプロトコル変換を担う。入力部12は、ユーザが暗証番号を入力する際に使用するキーをもつ。

[0069] メモリ部16は、コンピュータ処理とネットワーク通信処理のためのソフトウェアの他に許可リストをデータとして格納している。この許可リストは、中継を許可するドメイン名のリストで、リスト中のドメイン以外の通信はすべて遮断する。許可リストには、プロトコル変換(HTTP⇔HTTPS)してパケット中継を許可するドメイン名のリストである変換許可リスト、プロトコル変換を行わずパケット中継を許可するドメイン名のリストである中継許可リストの2種類を定義しておく(図5参照)。

[0070] 認証装置10の基本的な動作は、ユーザ端末30とサーバ40間で送受信されるパケットの分析を行い、相互認証、SSL(暗号化)通信、プロトコル変換(HTTP⇔HTTPS)を行い、パケットを中継する。

[0071] (4) 認証装置の暗号化通信処理機能の詳細

＜パケット分析＞

図6は、イーサネット(登録商標)のパケット構成を示す。認証装置10は、サーバおよびユーザ端末との通信経路を確立するため、自身を通過するパケットの分析を行い、IPアドレス、ドメイン名等の情報を取得する。

[0072] ・イーサネットヘッダ部からSourceのMACアドレス、Destination(デフォルトゲートウェイ)のMACアドレスを取得する。

[0073] ・IPヘッダ部よりSource(ユーザ端末)のIPアドレス、Destination(WWWサーバ)のIPアドレスを取得する。

[0074] ・TCPヘッダ部よりDestination Port(接続先のポート番号)を取得する。

[0075] ・HTTPコマンドよりRequest Method、アクセスするロケーション、リクエストバージョン、ホスト名を取得する。

[0076] <許可リスト及びプロキシ機能>

認証装置は、変換許可リストと中継許可リストの2種類を有する。変換許可リスト中のドメイン(URL)に対しては、HTTP(ユーザ端末ー認証装置間)⇔HTTPS(認証装置ーサーバ間)のプロトコル変換を行い、通信を中継する。このとき、ユーザ端末から見ると認証装置は、目的のWWWサーバのIPアドレスを有するHTTPサーバに見える。逆に、WWWサーバから認証装置は、SourceのIPアドレスをもつクライアントに見える。

[0077] 一方、中継許可リスト中のドメイン名(URL)に対しては、プロトコル変換は行わず、そのまま通信を中継する。ICカードが挿入されているときは、許可リスト以外のドメインへの通信は全て遮断する。なお、HTTPSの通信では、暗号化されているためパケット分析からホスト名の取得ができないため、中継許可リストに登録されているIPアドレスに対してのみ中継が許可される。

[0078] 許可リストには、図5のようにIPアドレス及びドメイン名での入力を可能とする。

[0079] <相互認証とSSL通信>

図7は、認証装置とサーバとの相互認証手順を示す。認証装置10は、ユーザ端末30からのHTTPリクエストを受けて、サーバとの間でハンドシェイク・プロトコルによるセッション確立を行う。認証装置10は、上記のパケット分析から得た情報及び、ICカードから読み込んだ情報を元に、IPヘッダ部から取得したSourceのIPアドレス(接続元情報)を自身のアドレスとして、WWWサーバ40に対して相互認証後、SSL通信を行う。

[0080] 認証装置10は、TCPヘッダ部のDestination Portが80(Webサーバのポート番号)であること、変換許可リスト中のドメイン名と、HTTPコマンド中から取得したホスト名が一致した場合のみ、ICカードから読み込んだクライアント証明書を利用して、相互認証、SSL通信を行う。さらにSSL通信でサーバから受信した応答をHTTPに変換して、WWWサーバからの応答として(WWWサーバのIPアドレスを使用して)ユーザ端末に送信する。

- [0081] 図8は相互認証とSSL通信の処理フローを示す。認証装置10は、ユーザ端末30からHTTP通信のリクエストを受信したとき(S1)、ICカードが挿入されているか否かをチェックし(S2)、ICカードが挿入されていない場合は通常のブリッジとして動作し、サーバ側へのすべての通信を中継する(S3)。
- [0082] ICカードが挿入されている場合は、リクエストをパケット分析し、ICカードからクライアント証明書を読み込むと共に、変換許可リストを取得する(S4)。この変換許可リスト中に接続先ホストが存在するか否かをチェックし(S5)、接続先ホストが存在するときは、HTTPS通信のリクエストをサーバに送信する(S6)。
- [0083] 変換許可リスト中に接続先ホストが存在しないときは、中継許可リストに接続先ホストが存在するか否かをチェックし(S7)、存在する場合は接続先ホストとのパケットの中継処理を行う(S8)。中継許可リストに接続先ホストが存在しない場合、エラーページをユーザ端末に送信する(S9)。
- [0084] サーバ40は、上記のHTTPS通信(S6)、または通常のパケットの中継(S3、S8)のリクエストに対する応答を返し(S10)、この応答を認証装置10が受信し(S11)、これをユーザ端末(クライアント)に中継する(S12)。
- [0085] ユーザ端末30は、サーバ40へのリクエストに対する応答を認証装置経由(S9、12)で受信する(S13)。
- [0086] なお、認証装置10は、ICカードが抜かれたとき変換許可リストの接続先ホストのセッションを切る。また、ICカードが抜かれた時点で変換／中継許可リストをクリアする。
- [0087] < 認証装置の追加機能 >
- ・認証装置10には、サーバ証明書の正当性をチェックする機能を追加可能とする。正しいサーバ証明書をあらかじめ認証装置に組み込んでおき、もしくは、正しいサーバ証明書をあらかじめICカードに書き込んでおき、相互認証時に証明書の正当性をチェック(証明書を比較)して、一致していた場合のみサーバへの中継を許可する。
- [0088] ・認証装置10の変換許可リストには、ICカード中の証明書に記載されているドメイン名を登録する。一方、変換許可リスト中のドメイン名のサーバからHTTPSで中継可能なドメインのリストをダウンロード(特定のURLにある)して、そこに登録してあるドメイン名を、認証装置の中継許可リストに追加することを可能とする。中継許可リスト

に書かれているドメインに対しては、通信の中継を許可する。変換許可リストと中継許可リスト中のドメイン以外の通信は全て遮断する。

[0089] ・認証装置10は、ドメイン名が変換許可リスト及び中継許可リストにない場合は、クライアントに対して、その旨を通達するエラーページを自動生成し、送信できる機能を追加可能とする。

[0090] (5) WWWサーバの処理機能の詳細

HTTPサーバの機能として、認証装置にICカードを入れて、暗証番号入力を促すメッセージを表示する。すなわち、サーバ40は、HTTPでリクエストがあった場合、認証装置10にICカード挿入後、暗証番号入力を促すメッセージを、クライアントに対して送信する。

[0091] サーバ40は、HTTPS通信により金融サービスを提供する。さらに、HTTPS通信にはクライアント認証を要求する。すなわち、サーバ40は、HTTPSのリクエストに対しては、クライアントの証明書を要求、相互認証後にSSL通信で金融サービスを提供する。

[0092] <サーバの追加機能>

認証装置は、中継可能なドメイン名のリストをサーバ上の特定の場所(URL)からダウンロード可能としてもよい。

[0093] (実施形態2)

前記までの実施形態1は、既存のサーバの構成をほとんど変更することなくシステムを構築することが可能であるが、ユーザ端末と認証装置間はHTTP通信であり、認証装置とサーバ間はHTTPSの通信であるため、ユーザが正しいサーバに接続していることを直接確認できない。

[0094] 本実施形態では、この問題点を解決する方式を提案する。図9はシステム構成図を示し、認証装置10、ICカード20、ユーザ端末30、サーバ40で構成される。同図において、ユーザ端末30からのHTTPリクエストを受けて、認証装置10がサーバ40と相互認証後、SSL通信を開始するまでは実施形態1と同じ手順になる。

[0095] ここで、サーバ40は、SSL通信でパケットを受信したときに、URLとワンタイムパスワードを埋め込んだページを認証装置10に送信する。認証装置10は、該ページを

HTTPに変換してユーザ端末に送信し、このページ受信でユーザ端末30側は表示されたURLに移動する。この後、サーバ40では、ユーザからのリクエストと共に送られてきたワンタイムパスワードが一致すれば、サーバ認証後に、SSL通信で金融サービスを提供する。この金融サービスは、ユーザ端末とサーバ間のSSL通信となり、認証装置10はその通信を中継する。先の相互認証によりユーザ端末の認証が成功したが、ワンタイムパスワードの受け渡し比較を行うことで、ユーザ端末—サーバ間のサーバ認証を相互認証と紐付けることができ、相互認証と同等のセキュリティを実現できる。

- [0096] 図10は相互認証とSSL通信の処理フローを示し、図8と同等の処理は同じ符号で示す。認証装置10はユーザ端末からのHTTP通信のリクエストに対し、変換許可リスト中に接続先ホストが存在し、接続先ホストのポートが「80」のときに(S5A)、HTTP S通信のリクエストをサーバに送信する(S6)。このリクエストに対し、相互認証後に、サーバ40はURLとランダムに生成する4桁の英数字(ワンタイムパスワード)を埋め込んだページを認証装置10に送信する(S21)。
- [0097] 認証装置10は、それがハンドシェイク・プロトコル終了直後であるとき(S22)、中継許可リストにサーバ40のIPアドレスを登録し(S23)、ユーザ端末への応答としてワンタイムパスワードをもつページをHTTPに変換して中継する(S24)。
- [0098] ユーザ端末30は、URL及びワンタイムパスワードが埋め込まれたページが表示されるため、表示されたURL(HTTPSのポート番号「443」)に移動する。この際、受信したワンタイムパスワードは、POSTやGET METHODを利用することにより、自動的に認証装置10を介してサーバに送られる。
- [0099] 認証装置10は、変換許可リストに存在する中継許可リストにIPアドレスが存在するため(S7)、サーバ認証のリクエストをサーバに中継する(S8)。
- [0100] サーバ40は、サーバ認証後にワンタイムパスワードをもつリクエストを受信したとき、それが、先にワンタイムパスワードを埋め込んだページを受信した直後であるとき(S25)、送信したワンタイムパスワードと受信したワンタイムパスワードが一致するか否かをチェックし(S26)、一致するときは金融サービスの提供を開始し(S27)、一致しないときはエラーページを送信する(S28)。これら応答は認証装置10を介してユーザ

端末30に送信される。

[0101] (実施形態3)

前記の実施形態2では、ユーザ端末と認証装置間がHTTP通信のためユーザが正しいサーバに接続していることを直接確認できないという問題を解決できる。しかし、ユーザは、一度の操作で目的のサービスを受けることができない、サーバ側の構成が複雑になるといった問題が発生する。

[0102] 本実施形態では、この問題点を解決する方式を提案する。図11はシステム構成図を示し、認証装置10、ICカード20、ユーザ端末30、サーバ40で構成される。構成は同じであるが、本実施形態では、認証装置10は、従来のWEBクライアント機能(ブラウザ)に追加してWEBサーバの機能を搭載する。WEBサーバ機能は、認証装置上のブラウザをユーザ端末30に表示する機能を有するものとする。

[0103] 図11において、ユーザ端末30からHTTPリクエストを受けて、ICカードが挿入されていて、変換許可リストのホスト名と一致する場合に、WEBサーバ10Aは受信したパケットから、URLの情報およびHTTPリクエストをクライアント(ブラウザ)10Bに渡す。ブラウザ10Bは、該当URLを有するサーバに対して相互認証を行い、サーバからの応答を表示する。ブラウザ10Bは、WEBサーバ上のコンテンツとして動いているため、ユーザ端末30からは、ブラウザの中に、認証装置のブラウザが表示される。このとき、認証装置10のブラウザから(認証装置－サーバ間は、HTTPS通信であるため)、サーバの証明書を確認し、正しいサーバに接続していることを直接確認することも可能となる。

[0104] 図12は、相互認証とSSL通信の処理フローを示し、図10と同等の処理は同じ符号で示す。認証装置10は、ユーザ端末からのHTTP通信のリクエストに対し、WEBサーバが受信する。WEBサーバは、変換許可リスト中に接続先ホストが存在し、接続先のポートが「80」のときに、ホストとリクエストをWEBブラウザに渡す。WEBブラウザは、接続先ホストに対して、HTTPS通信のリクエストを送信する(S30)。この後、相互認証が確立された後、WWWサーバからの応答をWEBブラウザは、認証装置のWEBサーバ経由でユーザ端末に送信する(S31, S32)。

[0105] 実施形態1では、パケットをそのままユーザ端末に返していたが、本実施形態では

、受信したパケットをコンテンツとしてWEBサーバ上で表示すること(S32)が大きな特徴となる。

[0106] なお、上記説明は、認証装置10内のWEBクライアント機能とWEBサーバの機能が独立しているが、WEBクライアント機能は、WEBサーバ上で実現してもよい。

[0107] (変形例)

以上までの実施形態では、ユーザ端末30としてPCによる認証システムを例として取り上げているが、インターネット機能及びブラウザを持つクライアントであれば、PCに限定されるものではない。

[0108] また、認証装置は、PLC、ルータなどの中継装置に搭載し、この中継装置が認証機能を持つ電子認証システム、電子認証方法とすることができる。

[0109] また、HTTP及びHTTPSを用いた通信を例としてあげているが、通信のプロトコルはこれに限定されず、TCP/IPの範疇でなくてもよい。

[0110] また、金融システムへの適用例を挙げているが、相互認証、暗号化通信を行うものであれば、これに限定されるものではない。

[0111] また、ICカードは、カードタイプのものを例として取り上げているが、ICチップを利用するものであれば、カードタイプに限定されるものではない。また、ICカードに代えたUSBカードなど、クライアント証明書と秘密鍵を記録した外部メディアでもよい。

[0112] なお、本発明は、図7や図8、図10、図12に示した一部又は全部の電子認証処理機能をプログラムで記載してコンピュータで実行可能にすることができる。

[0113] (発明の効果)

以上のとおり、本発明によれば、システム構築を簡易にしながら、相互認証のセキュリティ性を高めた電子認証ができる。

[0114] 具体的には、

(1)ユーザ端末にカードリーダーを備える方式に比べて、ドライバや専用ソフトの導入が一切不要で、特別な設定(IPアドレス設定など)を行わずに、従来では設定が難しかった相互認証、暗号化通信が容易に実現可能であり、導入時や再セットアップ時には効果が高い。

[0115] (2)クライアント証明書や暗号化された認証用データは、ユーザ端末を経由するこ

となく、直接にサーバに送信されるため、データの流出を防止できる。

- [0116] (3)暗証番号は、ユーザ端末経由ではなく認証装置に直接に入力するため、ユーザ端末などにキーロガーのようなスパイウェアが入っていても、暗証番号の流出はないため、従来のシステムよりセキュリティ強度が高い。
- [0117] (4)ICカードなどの外部メディアが不正利用された場合、ログイン情報や通信記録等のユーザ端末上のログは、管理者権限で、簡単に改ざんされてしまうが、本システムの認証装置は、組込機器という製品の位置づけであるため、ユーザインターフェースがなく、ログの改ざんは不可能である。
- [0118] (5)認証装置の許可リストに記述されているドメイン名(URL)以外の通信はすべて遮断するため、なりすましやフィッシングに対して有効である。
- [0119] (6)認証装置は、パケット分析により接続元の情報(IPアドレス)を入手し、その情報を自身の情報として利用するため、自身IPアドレスを持たず、ネットワーク上では隠れた存在となり、不正攻撃の対象や、ネットワーク経由のウイルス感染の対象にはならない。
- [0120] (7)従来は、正しいサイトに接続されていることを保証するため、ユーザがブラウザから手動でサーバ証明書の正当性を確認する必要があったが、認証装置側でサーバ証明書の正当性を自動で確認可能となり、よりセキュリティの高い通信を提供することが可能となる。

符号の説明

- [0121] 10 認証装置
20 ICカード
30 ユーザ端末
40 サーバ

請求の範囲

- [1] ユーザ端末と、ネットワーク接続機能を有するサーバとの間の暗号化通信で電子認証を得る電子認証装置であって、
- 前記ユーザ端末のネットワークインタフェースと接続されてパケット通信ができ、前記サーバとはネットワークを介して接続されてパケット通信ができる手段を備え、
- 前記ユーザ端末からのパケットを分析して、接続先情報を取得し、その接続先情報が所望のサービスを提供するサーバへのリクエストであった場合は、秘密鍵及びクライアント証明書を使用して、前記サーバとの間で相互認証と暗号化通信を行う手段を備えたことを特徴とする電子認証装置。
- [2] 前記認証装置は、前記サービスを提供するサイトへの暗号化通信を許可する接続先情報をもつ変換許可リストを備え、前記変換許可リストに前記サーバの接続先情報が存在するときに当該サーバとの相互認証と暗号化通信を行う手段を備えたことを特徴とする請求項1に記載の電子認証装置。
- [3] 前記認証装置は、単にパケットの中継を許可する接続先情報をもつ中継許可リストを備え、前記中継許可リストに前記サーバの接続先情報が存在するときに前記サーバに対しては単にパケットの中継する手段を備えたことを特徴とする請求項1又は2に記載の電子認証装置。
- [4] 前記認証装置は、秘密鍵及びクライアント証明書を自装置内または、外部メディアから読み込む手段を備えたことを特徴とする請求項1乃至3のいずれか1つに記載の電子認証装置。
- [5] 前記認証装置は、クライアント証明書を読み込むときに、前記クライアント証明書を読み込むための暗証番号を入力する手段を備えたことを特徴とする請求項1乃至4のいずれか1つに記載の電子認証装置。
- [6] 前記認証装置は、パケット分析により接続元の情報を入手し、その情報を自身の情報として利用する手段を備えたことを特徴とする請求項1乃至5のいずれか1つに記載の電子認証装置。
- [7] 前記認証装置は、前記許可リスト中の接続先以外のホストとの通信はすべて遮断する手段を備えたことを特徴とする請求項1乃至6のいずれか1つに記載の電子認証

装置。

- [8] 前記認証装置は、自装置内または前記外部メディアに書き込んだサーバ証明書を
用いて、相互認証時にサーバの正当性をチェックできた場合のみサーバへの中継を
許可する手段を備えたことを特徴とする請求項1乃至7のいずれか1つに記載の電子
認証装置。
- [9] 前記認証装置は、前記認証装置内にブラウザとそのブラウザ中のコンテンツを前記
ユーザ端末に表示するブラウザ表示手段を備え、
前記ブラウザ表示手段は、前記所望のサービスを提供するサーバへのリクエストを
送信し、その応答を受信し、その応答であるコンテンツをブラウザと共に前記ユーザ
端末で表示できる情報として前記ユーザ端末に返す手段を備えたことを特徴とする
請求項1乃至8のいずれか1つに記載の電子認証装置。
- [10] 前記認証装置は、前記ユーザ端末からのリクエストを受けて、前記サーバと相互認
証と暗号化通信を開始する手段を備え、
前記サーバは、前記相互認証後にワンタイムパスワードを前記認証装置を介して
前記ユーザ端末に送信する手段を備え、
前記ユーザ端末は、前記ワンタイムパスワードを前記サーバに送信する手段を備え
、
前記サーバは、前記認証装置を介して送られてきたユーザ端末からのワンタイムパ
スワードを使って前記ユーザ端末とサーバ間で暗号化通信を行う手段を備えたことを
特徴とする請求項1乃至8のいずれか1つに記載の電子認証装置。
- [11] ユーザ端末と、ネットワーク接続機能を有するサーバとの間の暗号化通信で電子認
証を得る電子認証システムであって、
前記ユーザ端末のネットワークインタフェースと接続されてパケット通信ができ、前
記サーバとはネットワークを介して接続されてパケット通信ができる認証装置を備え、
前記認証装置は、前記ユーザ端末からのパケットを分析して、接続先情報を取得し
、その接続先情報が所望のサービスを提供するサーバへのリクエストであった場合は
、秘密鍵及びクライアント証明書を使用して、前記サーバとの間で相互認証と暗号化
通信を行う手段を備えたことを特徴とする電子認証システム。

- [12] 前記認証装置は、前記サービスを提供するサイトへの暗号化通信を許可する接続先情報をもつ変換許可リストを備え、前記変換許可リストに前記サーバの接続先情報が存在するときに当該サーバとの相互認証と暗号化通信を行う手段を備えたことを特徴とする請求項11に記載の電子認証システム。
- [13] 前記認証装置は、単にパケットの中継を許可する接続先情報をもつ中継許可リストを備え、前記中継許可リストに前記サーバの接続先情報が存在するときに前記サーバに対しては単にパケットの中継する手段を備えたことを特徴とする請求項11又は12に記載の電子認証システム。
- [14] 前記認証装置は、秘密鍵及びクライアント証明書を自装置内または、外部メディアから読み込む手段を備えたことを特徴とする請求項11乃至13のいずれか1つに記載の電子認証システム。
- [15] 前記認証装置は、クライアント証明書を読み込むときに、前記クライアント証明書を読み込むための暗証番号を入力する手段を備えたことを特徴とする請求項11乃至14のいずれか1つに記載の電子認証システム。
- [16] 前記認証装置は、パケット分析により接続元の情報を入手し、その情報を自身の情報として利用する手段を備えたことを特徴とする請求項11乃至15のいずれか1つに記載の電子認証システム。
- [17] 前記認証装置は、前記許可リスト中の接続先以外のホストとの通信はすべて遮断する手段を備えたことを特徴とする請求項11乃至16のいずれか1つに記載の電子認証システム。
- [18] 前記認証装置は、自装置内または前記外部メディアに書き込んだサーバ証明書を用いて、相互認証時にサーバの正当性をチェックできた場合のみサーバへの中継を許可する手段を備えたことを特徴とする請求項11乃至17のいずれか1つに記載の電子認証システム。
- [19] 前記認証装置は、前記認証装置内にブラウザとそのブラウザ中のコンテンツを前記ユーザ端末に表示するブラウザ表示手段を備え、
前記ブラウザ表示手段は、前記所望のサービスを提供するサーバへのリクエストを送信し、その応答を受信し、その応答であるコンテンツをブラウザと共に前記ユーザ

端末で表示できる情報として前記ユーザ端末に返す手段を備えたことを特徴とする請求項11乃至18のいずれか1つに記載の電子認証システム。

- [20] 前記認証装置は、前記ユーザ端末からのリクエストを受けて、前記サーバと相互認証と暗号化通信を開始する手段を備え、

前記サーバは、前記相互認証後にワンタイムパスワードを前記認証装置を介して前記ユーザ端末に送信する手段を備え、

前記ユーザ端末は、前記ワンタイムパスワードを前記サーバに送信する手段を備え、

前記サーバは、前記認証装置を介して送られてきたユーザ端末からのワンタイムパスワードを使って前記ユーザ端末とサーバ間で暗号化通信を行う手段を備えたことを特徴とする請求項11乃至18のいずれか1つに記載の電子認証システム。

- [21] ユーザ端末と、ネットワーク接続機能を有するサーバとの間の暗号化通信で電子認証を得る電子認証方法であって、

前記ユーザ端末のネットワークインタフェースと接続されてパケット通信ができ、前記サーバとはネットワークを介して接続されてパケット通信ができる認証装置を備え、

前記認証装置は、前記ユーザ端末からのパケットを分析して、接続先情報を取得し、その接続先情報が所望のサービスを提供するサーバへのリクエストであった場合は、秘密鍵及びクライアント証明書を使用して、前記サーバとの間で相互認証と暗号化通信を行う手順を有することを特徴とする電子認証方法。

- [22] 前記認証装置は、前記サービスを提供するサイトへの暗号化通信を許可する接続先情報をもつ変換許可リストを備え、前記変換許可リストに前記サーバの接続先情報が存在するときに当該サーバとの相互認証と暗号化通信を行う手順を有することを特徴とする請求項21に記載の電子認証方法。

- [23] 前記認証装置は、単にパケットの中継を許可する接続先情報をもつ中継許可リストを備え、前記中継許可リストに前記サーバの接続先情報が存在するときに前記サーバに対しては単にパケットの中継する手順を有することを特徴とする請求項21又は22に記載の電子認証方法。

- [24] 前記認証装置は、秘密鍵及びクライアント証明書を自装置内または、外部メディア

から読み込む手順を有することを特徴とする請求項21乃至23のいずれか1つに記載の電子認証方法。

[25] 前記認証装置は、クライアント証明書を読み込むときに、前記クライアント証明書を読み込むための暗証番号を入力する手順を有することを特徴とする請求項21乃至24のいずれか1つに記載の電子認証方法。

[26] 前記認証装置は、パケット分析により接続元の情報を入手し、その情報を自身の情報として利用する手順を有することを特徴とする請求項21乃至25のいずれか1つに記載の電子認証方法。

[27] 前記認証装置は、前記許可リスト中の接続先以外のホストとの通信はすべて遮断する手順を有することを特徴とする請求項21乃至26のいずれか1つに記載の電子認証方法。

[28] 前記認証装置は、自装置内または前記外部メディアに書き込んだサーバ証明書を用いて、相互認証時にサーバの正当性をチェックできた場合のみサーバへの中継を許可する手順を有することを特徴とする請求項21乃至27のいずれか1つに記載の電子認証方法。

[29] 前記認証装置は、前記認証装置内にブラウザとそのブラウザ中のコンテンツを前記ユーザ端末に表示するブラウザ表示手順を有し、

前記ブラウザ表示手順は、前記所望のサービスを提供するサーバへのリクエストを送信し、その応答を受信し、その応答であるコンテンツをブラウザと共に前記ユーザ端末で表示できる情報として前記ユーザ端末に返す手順を有することを特徴とする請求項21乃至28のいずれか1つに記載の電子認証方法。

[30] 前記認証装置は、前記ユーザ端末からのリクエストを受けて、前記サーバと相互認証と暗号化通信を開始する手順を有し、

前記サーバは、前記相互認証後にワンタイムパスワードを前記認証装置を介して前記ユーザ端末に送信する手順を有し、

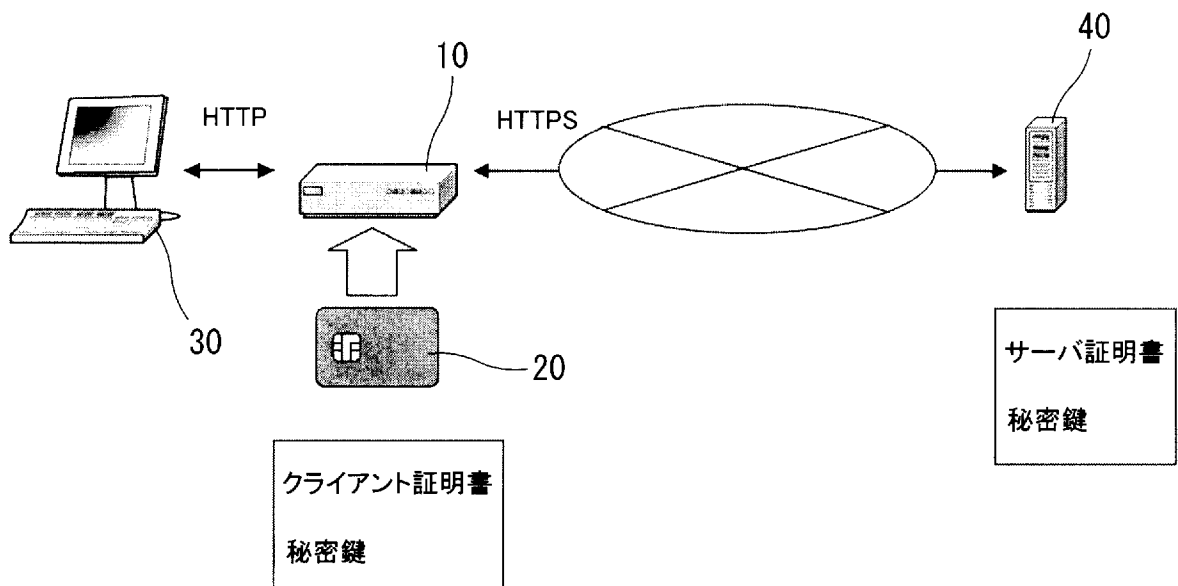
前記ユーザ端末は、前記ワンタイムパスワードを前記サーバに送信する手順を有し、

前記サーバは、前記認証装置を介して送られてきたユーザ端末からのワンタイムパ

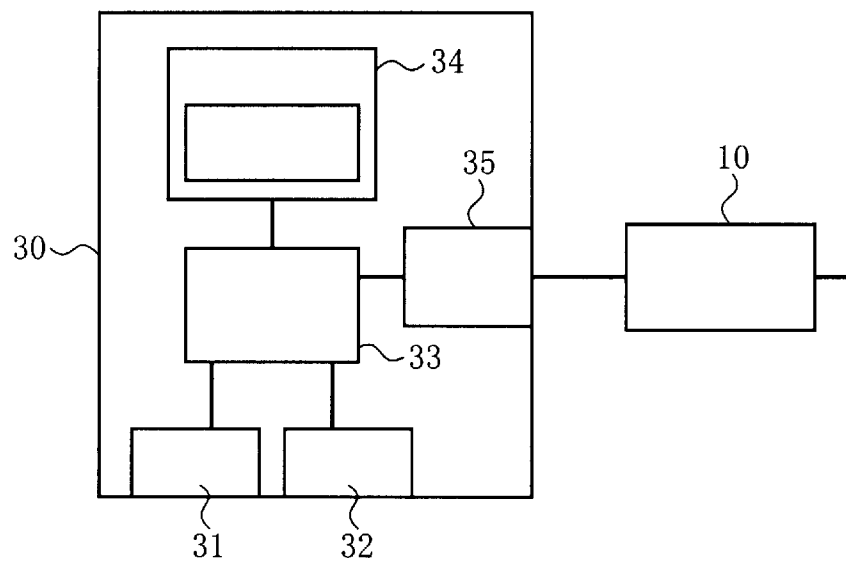
スワードを使って前記ユーザ端末とサーバ間で暗号化通信を行う手順を有することを特徴とする請求項21乃至28のいずれか1つに記載の電子認証方法。

- [31] 前記請求項21～30のいずれか1項に記載の電子認証方法における処理手順をコンピュータで実行可能にしたことを特徴とするプログラム。

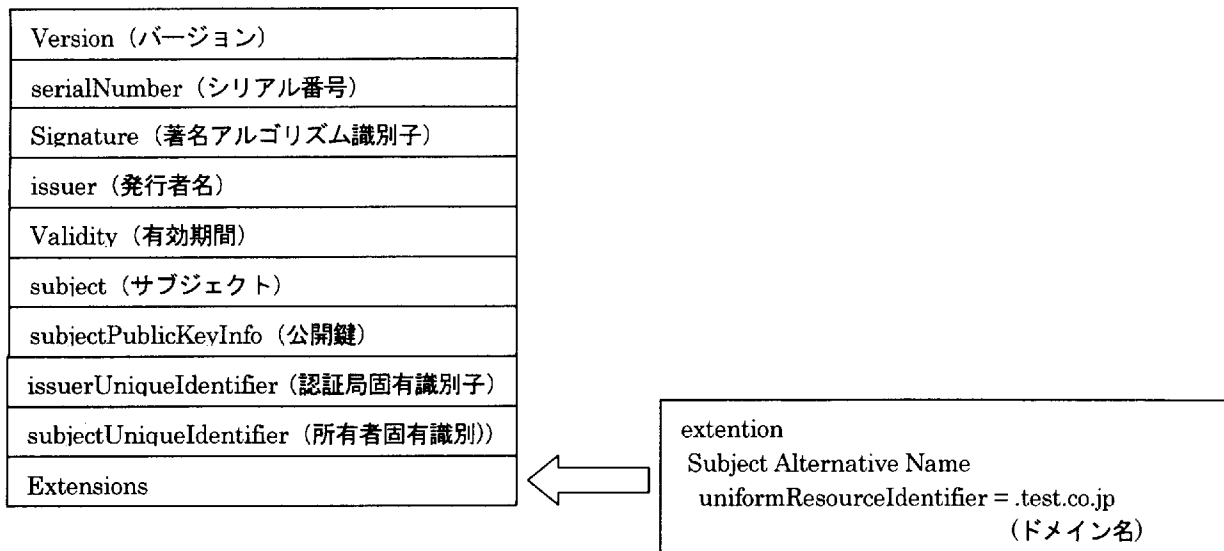
[図1]



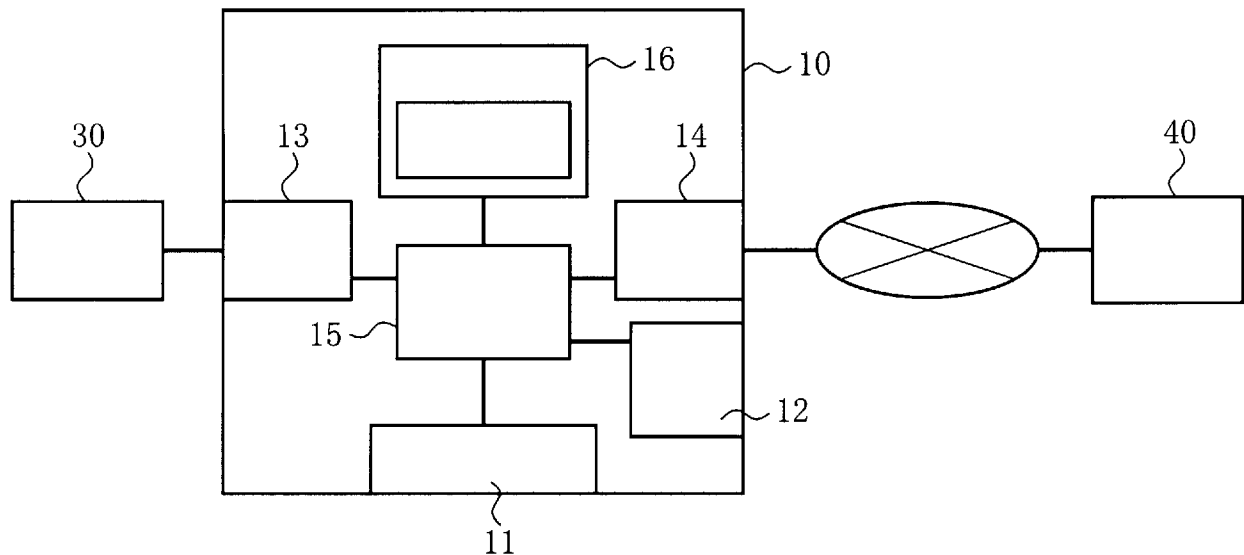
[図2]



[図3]



[図4]



[図5]

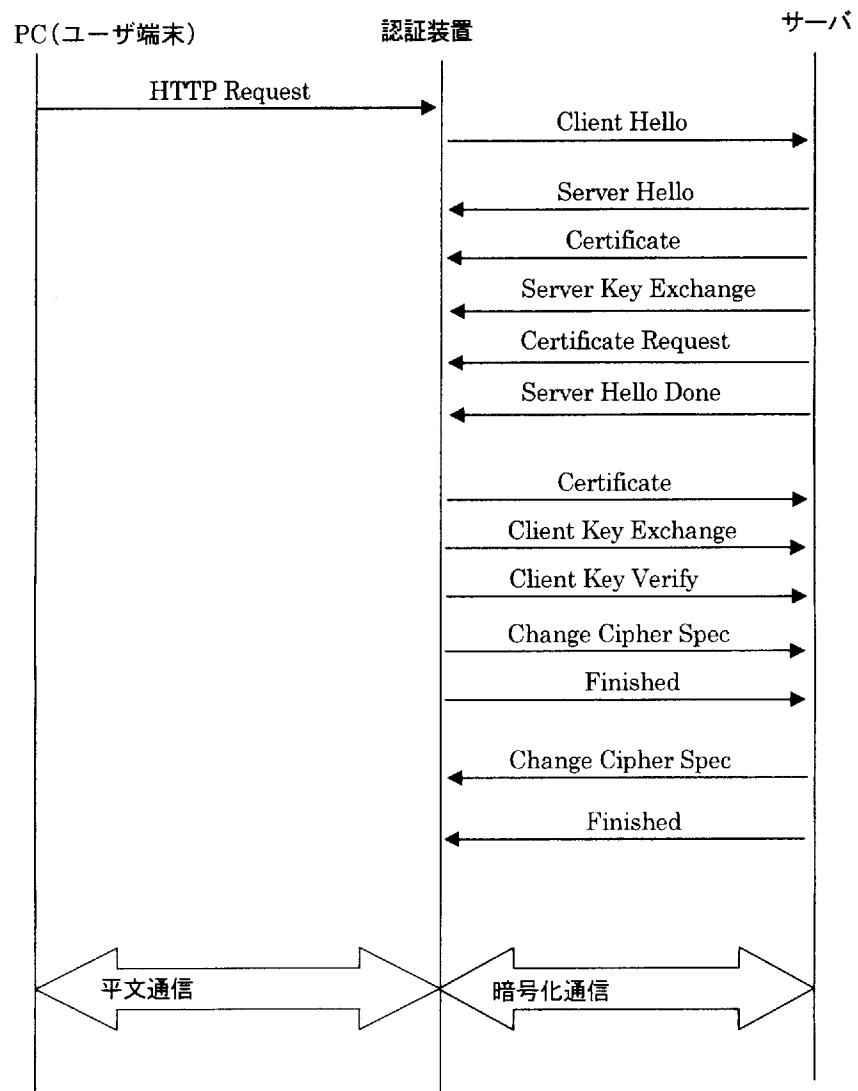
変換許可リスト	中継許可リスト
www.test.com www.abc.com	www.efg.com www.hij.com 192.168.1.1

ドメイン名およびIPアドレス

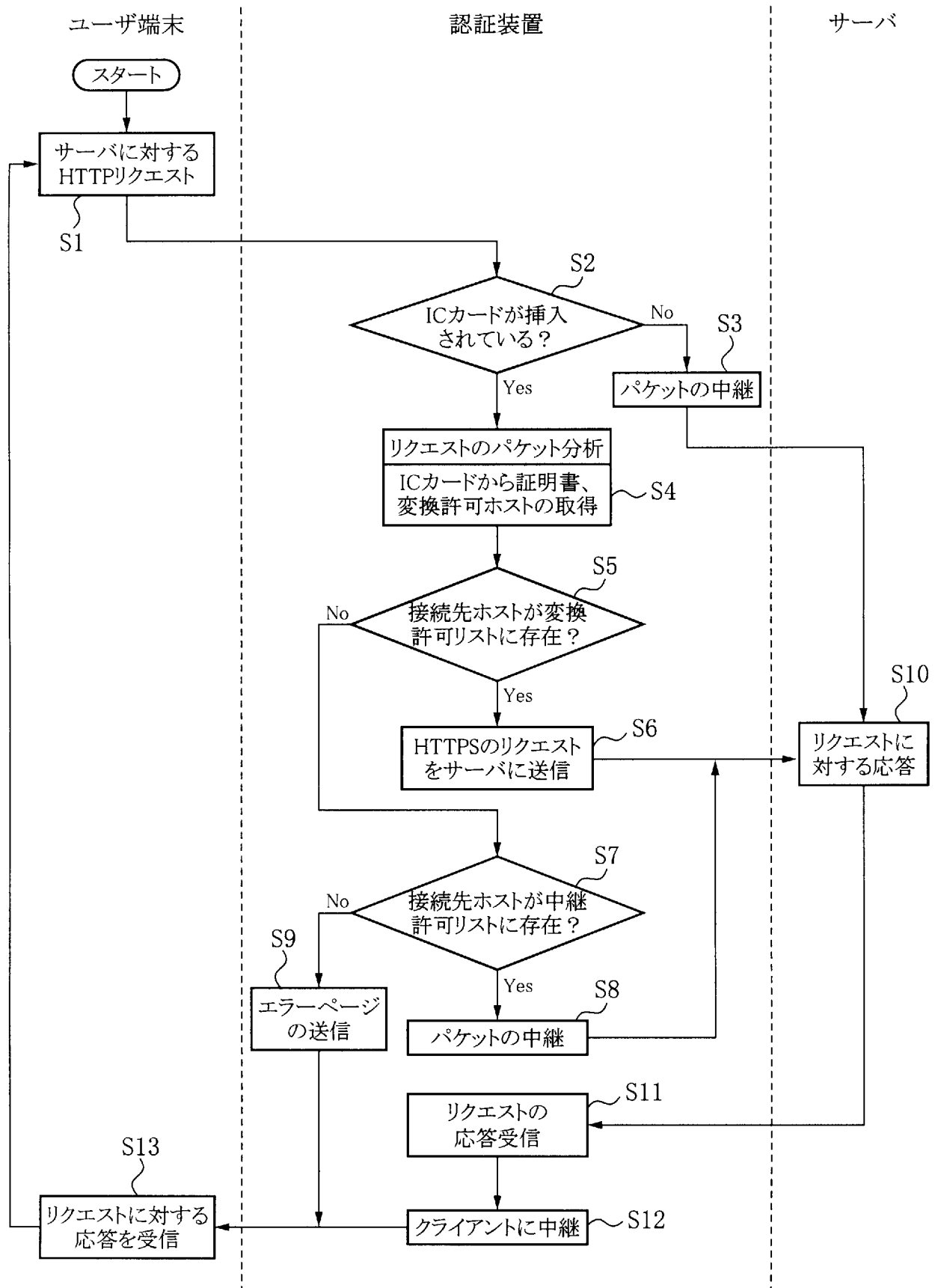
[図6]

イーサーヘッダ	IP ヘッダ	TCP ヘッダ	HTTP コマンド
---------	--------	---------	-----------

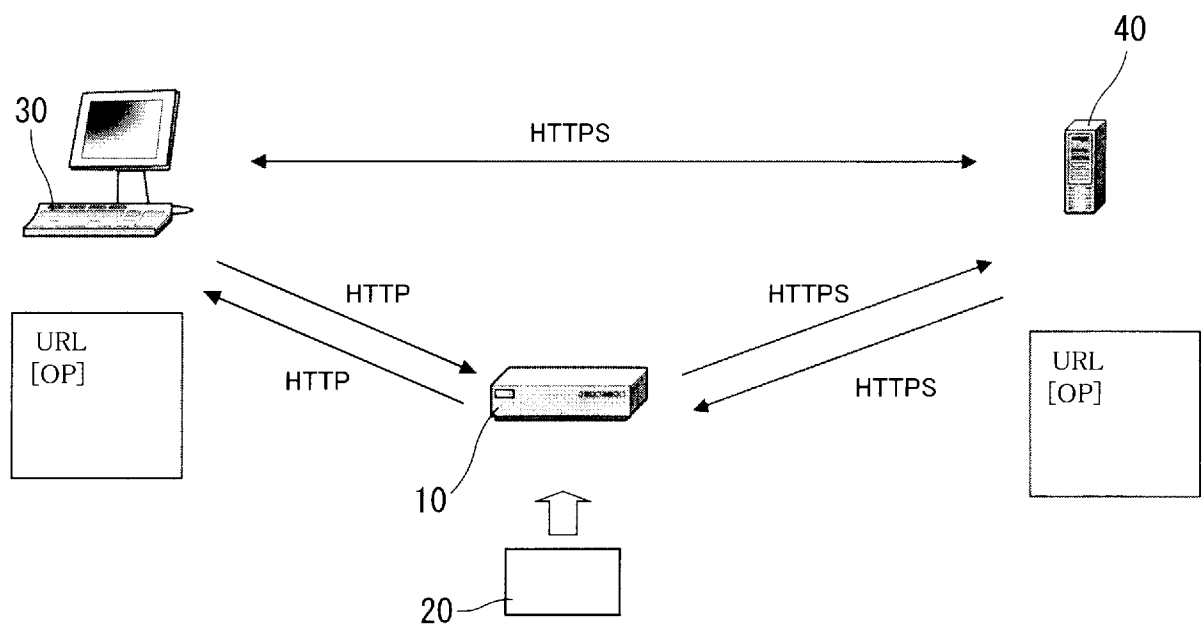
[図7]



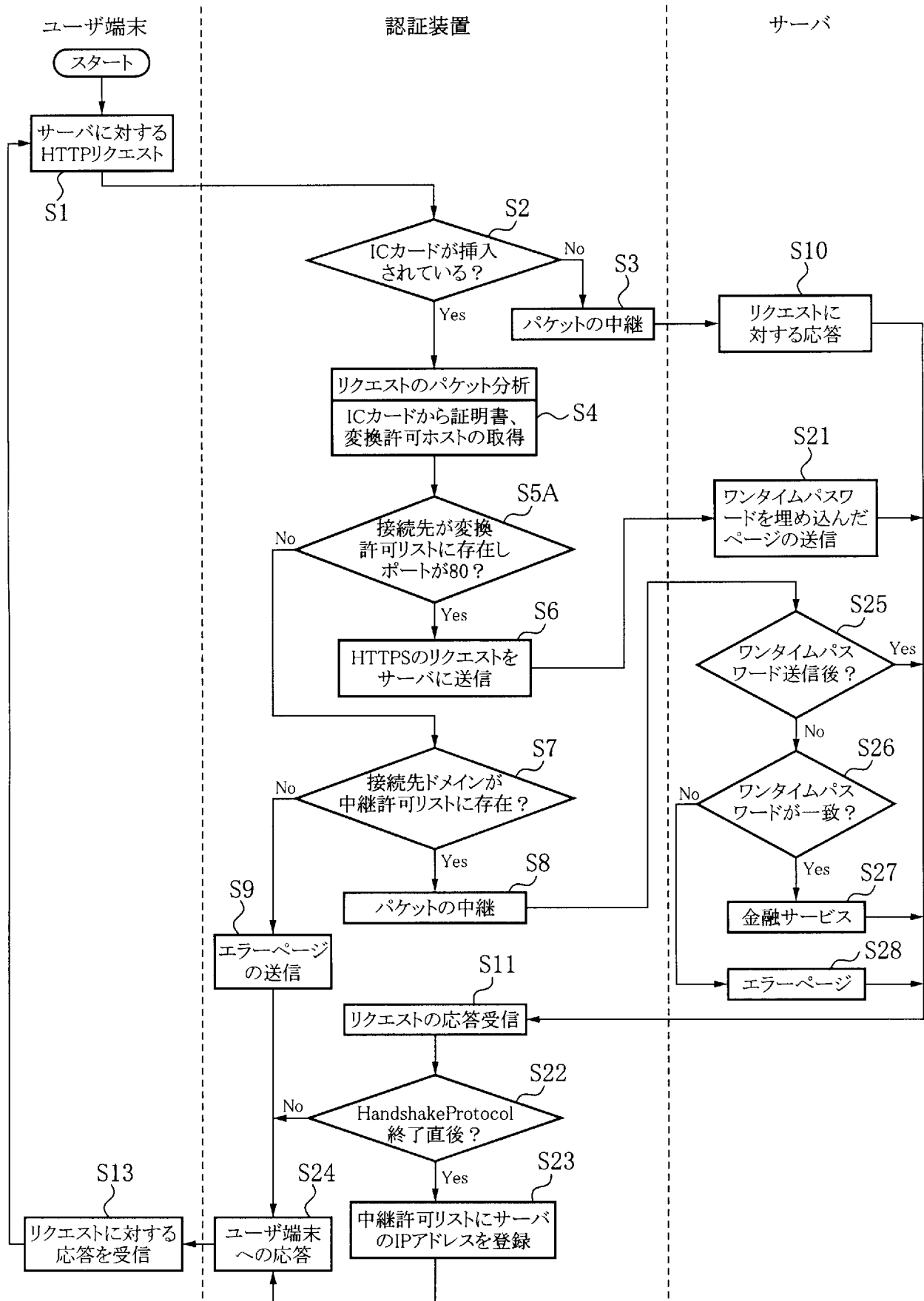
[図8]



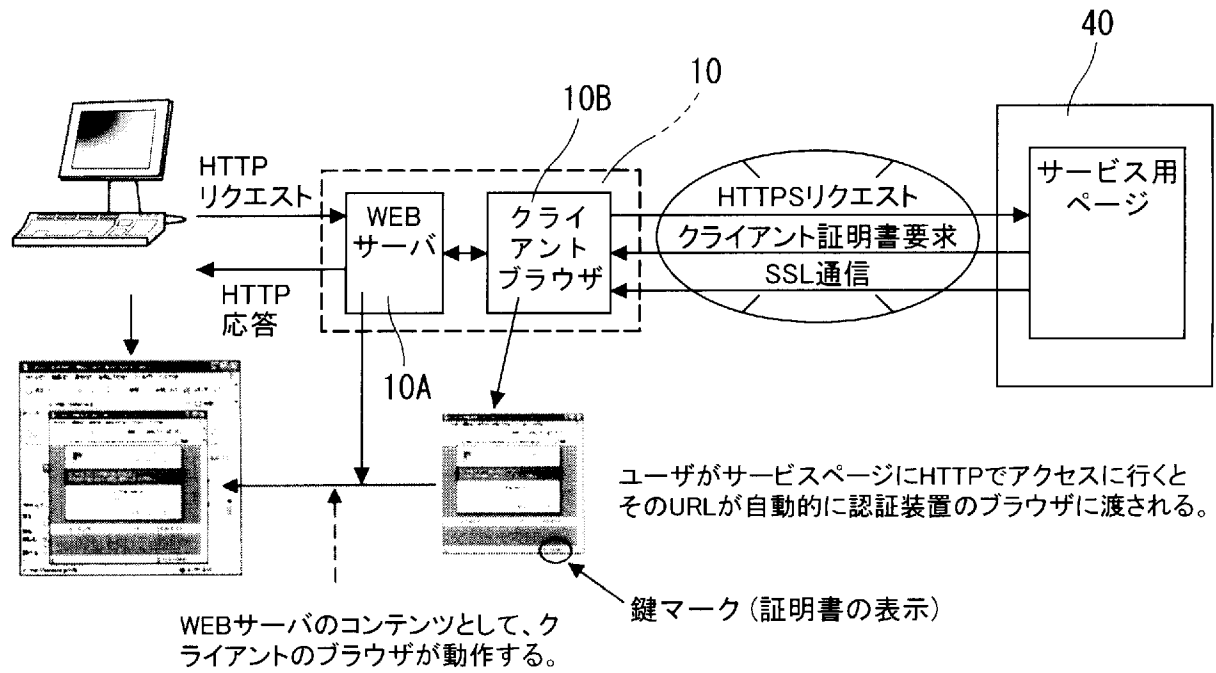
[図9]



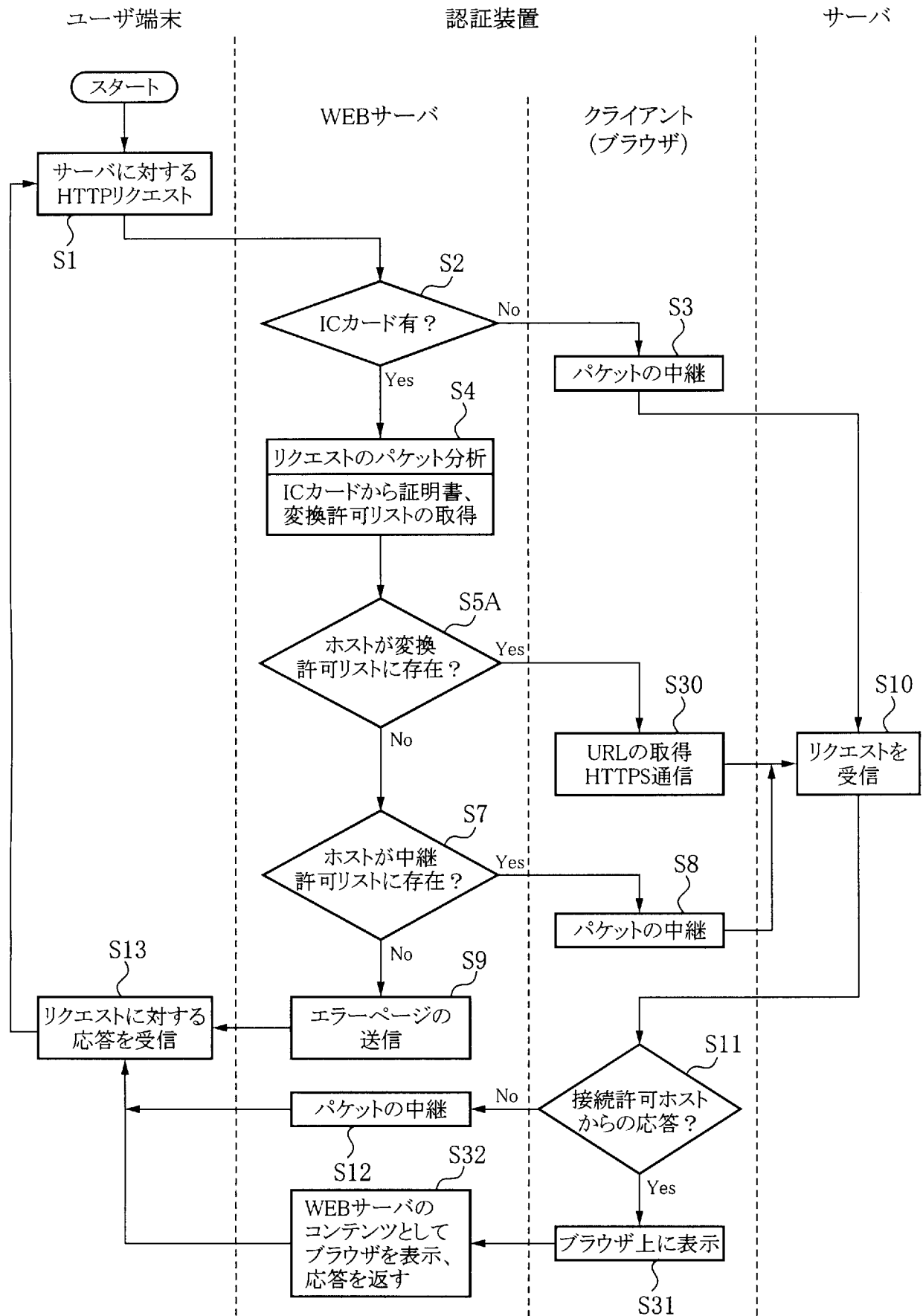
[図10]



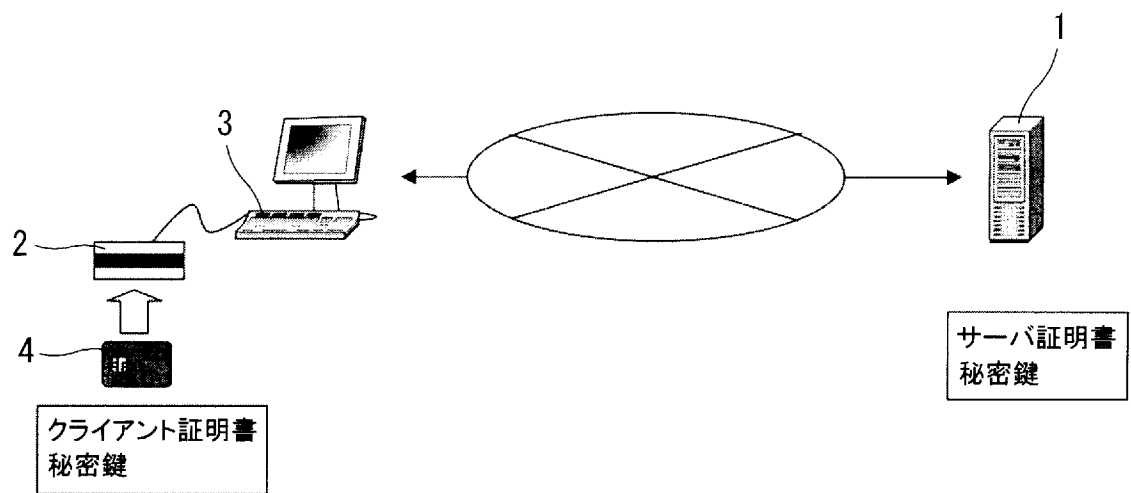
[図11]



[図12]



[図13]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2008/069930

A. CLASSIFICATION OF SUBJECT MATTER

H04L9/32(2006.01) i, G09C1/00(2006.01) i

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)

H04L9/32, G09C1/00

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

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2009
Kokai Jitsuyo Shinan Koho	1971-2009	Toroku Jitsuyo Shinan Koho	1994-2009

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 2002-158650 A (Fujitsu Ltd.), 31 May, 2002 (31.05.02), Par. Nos. [0034] to [0048], [0063] to [0066]; Figs. 1 to 2, 11 & US 2002/0062440 A1 & EP 1209874 A2	1, 4-5, 8, 10-11, 14-15, 18, 20-21, 24-25, 28, 30-31
A	JP 2005-141333 A (Matsushita Electric Industrial Co., Ltd.), 02 June, 2005 (02.06.05), Par. Nos. [0045] to [0058], [0112] to [0136], [0178]; Figs. 8 to 9, 31 to 35 (Family: none)	1, 4-5, 8, 10-11, 14-15, 18, 20-21, 24-25, 28, 30-31

☐ 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
16 January, 2009 (16.01.09)

Date of mailing of the international search report
27 January, 2009 (27.01.09)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2008/069930

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

Document 1: JP 2002-158650 A (Fujitsu Ltd.), 31 May, 2002 (31.05.02), paragraphs [0034] - [0048] and [0063] - [0066], Figs. 1-2 and 11

The document 1 describes an invention of a home server (1-1), wherein the home server (1-1) (corresponding to the "electronic authentication device" of this application. See the document 1, paragraphs [0034] - [0040] and Figs. 1 and 11), which carries out authentication and encryption processing with a user terminal device (1-3) (corresponding to the "user terminal device" of the application) and an electronic market server (1-5) (corresponding to the "server" of the application), (to be continued on the extra sheet)

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.: 1, 4-5, 8, 10-11, 14-15, 18, 20-21, 24-25, 28 and 30-31.

Remark on Protest
the

- ☐ The additional search fees were accompanied by the applicant's protest and, where applicable, payment of a protest fee.
- ☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.
- ☐ No protest accompanied the payment of additional search fees.

Continuation of Box No.III of continuation of first sheet(2)

is characterized in comprising a means (corresponding to the "... means that can carry out packet communication" of this application. See the document 1, paragraphs [0035] and [0039]-[0040]) that can carry out data communication with the user terminal device (1-3) and data communication with the electronic market server (1-5) through the internet, and a means (corresponding to the "... means that carries out mutual authentication and encryption communication" of this application. See paragraphs [0045] and [0064]-[0066]) that receives an access request from the user terminal device (1-3), sets up a communication channel with the electronic market server (1-5), and carries out server authentication, client (user) authentication, and encrypted data communication by means of a secret key and a user certificate.

It is clear that, after receiving the access request from the user terminal device (1-3), the home server acquires connection destination information of the access request, and judges that the access request is a request directed to the electronic market server (1-5), thereby setting up the communication channel with the electronic market server (1-5).

Thus, since the inventions in claims 1, 11, 21 and 31 of the present application are described in the document 1, they are lack of the novelty and the inventive step.

By comparison of the inventions in claims 1-31 with the description of the document 1, the inventions in claims 1-31 are categorized into the following groups (1)-(4) in the light of the special technical features:

(1) Claims 1, 4-5, 8, 10-11, 14-15, 18, 20-21, 24-25, 28 and 30-31

A) The invention are described in the document 1, and no special technical features can be found:

- Claims 1, 11, 21 and 31

The reason is the same as set forth just above.

- Claims 4, 14 and 24

The document 1 describes that the home server (1-1) reads out the secret key and the user certificate from a home card (1-2). See the document 1, paragraph [0064].

B) No inventive step can be found in view of the description of the document 1 and the well known matter of a person skilled in the art.

- Claims 5, 15 and 25

It is well known to input a secret number when data are read in.

- Claims 8, 18 and 28

It is well known to make the relay to the server possible only when server authentication is confirmed.

- Claims 10, 20 and 30

The document 1 also describes that the electronic market server (1-5) and the user terminal (1-3) exchange a common key (X) through the home server (1-1) to carry out encryption communication (see the document 1, paragraph [0047], Fig. 2). The use of a one-time password is well known.

(To be continued on the next page)

(2) Claims 2-3, 7, 12-13, 17, 22-23 and 27

The subject matter is directed to the home server provided with a permission list.

(3) Claims 6, 16 and 26

The home server utilizes information of a connecting origin as its own information based on a packet analysis.

(4) Claims 9, 19 and 29

A browser display means is provided in the authentication device.

Further, since there are no other common features among the above-mentioned groups in the meaning of PCT Rule 13.2, second sentence, no technical relationship in the meaning of PCT Rule 13 can be found among them.

Therefore, it is clear that claims 1-31 do not comply with the requirement of unity of invention.

A. 発明の属する分野の分類 (国際特許分類 (I P C))

Int.Cl. H04L9/32(2006.01)i, G09C1/00(2006.01)i

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 (I P C))

Int.Cl. H04L9/32, G09C1/00

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	1 9 2 2 - 1 9 9 6 年
日本国公開実用新案公報	1 9 7 1 - 2 0 0 9 年
日本国実用新案登録公報	1 9 9 6 - 2 0 0 9 年
日本国登録実用新案公報	1 9 9 4 - 2 0 0 9 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 2002-158650 A (富士通株式会社) 2002.05.31, 段落 0034-0048, 0063-0066, 図 1-2, 11 & US 2002/0062440 A1 & EP 1209874 A2	1, 4-5, 8, 10-11, 14-15, 18, 20-21, 24-25, 28, 30-31

☒ 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

1 6 . 0 1 . 2 0 0 9

国際調査報告の発送日

2 7 . 0 1 . 2 0 0 9

国際調査機関の名称及びあて先

日本国特許庁 (I S A / J P)

郵便番号 1 0 0 - 8 9 1 5

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)

高橋 克

5 S

4 5 3 8

電話番号 0 3 - 3 5 8 1 - 1 1 0 1 内線 3 5 4 6

C (続き) . 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
A	JP 2005-141333 A (松下電器産業株式会社) 2005. 06. 02, 段落 0045-0058, 0112-0136, 0178, 図 8-9, 31-35 (ファミリーなし)	1, 4-5, 8, 10-11, 14-15, 18, 20-21, 24-25, 28, 30-31

第Ⅱ欄 請求の範囲の一部の調査ができないときの意見（第1ページの2の続き）

法第8条第3項（PCT17条(2)(a)）の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1. ☐ 請求の範囲 _____ は、この国際調査機関が調査をすることを要しない対象に係るものである。つまり、
2. ☐ 請求の範囲 _____ は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、
3. ☐ 請求の範囲 _____ は、従属請求の範囲であってPCT規則6.4(a)の第2文及び第3文の規定に従って記載されていない。

第Ⅲ欄 発明の単一性が欠如しているときの意見（第1ページの3の続き）

次に述べるようにこの国際出願に二以上の発明があるところの国際調査機関は認めた。

文献1：JP 2002-158650 A（富士通株式会社）2002.05.31，
段落0034-0048, 0063-0066，図1-2, 11

文献1には、
ユーザ端末機器1-3（本願の「ユーザ端末」に相当）と、電子マーケットサーバ1-5（本願の「サーバ」に相当）との間で、認証・暗号化処理を行うホームサーバ1-1（本願の「電子認証装置」に相当。同文献の段落0034-0040、図1, 11参照。）であって、前記ユーザ端末機器1-3とデータ通信ができ、前記電子マーケットサーバ1-5とインターネットを介してデータ通信ができる手段（本願の「・・・パケット通信ができる手段」に相当。同文献の段落0035，（特別ページに続く）

1. ☐ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。
2. ☐ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。
3. ☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったため、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。
4. ☒ 出願人が必要な追加調査手数料を期間内に納付しなかったため、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

請求の範囲1, 4-5, 8, 10-11, 14-15, 18, 20-21, 24-25, 28, 30-31

追加調査手数料の異議の申立てに関する注意

- ☐ 追加調査手数料及び、該当する場合には、異議申立手数料の納付と共に、出願人から異議申立てがあった。
- ☐ 追加調査手数料の納付と共に出願人から異議申立てがあったが、異議申立手数料が納付命令書に示した期間内に支払われなかった。
- ☐ 追加調査手数料の納付はあったが、異議申立てはなかった。

(第Ⅲ欄のつづき)

0039-0040 参照)を備え、前記ユーザ端末 1-3 からアクセス要求を受信し、電子マーケットサーバ 1-5 との通信路を確立し、秘密鍵とユーザの証明書を用いて、サーバ認証及びクライアント(ユーザ)認証並びに暗号化されたデータ通信を行う手段(本願の「・・・相互認証と暗号化通信を行う手段」に相当。同文献の段落 0045, 0064-0066 参照)を備えたことを特徴とするホームサーバ 1-1 の発明が記載されている。

なお、ユーザ端末 1-3 からアクセス要求を受信した後、当該アクセス要求の接続先情報を取得し、当該アクセス要求が電子マーケットサーバ 1-5 へのリクエストであることを判断してから、前記電子マーケットサーバ 1-5 との通信路を確立することは明らかである。

したがって、本願の請求の範囲 1, 11, 21, 31 に係る発明は、文献 1 に記載されているから、新規性及び進歩性を有しない。

請求の範囲 1-31 に係る発明と、文献 1 の記載とを対比すると、請求の範囲 1-31 に係る発明は、その特別な技術的特徴により以下の群(1)-(4)に区分される。

(1) 請求の範囲 1, 4-5, 8, 10-11, 14-15, 18, 20-21, 24-25, 28, 30-31

(ア) 文献 1 に記載されており、特別な技術的特徴を見出せないもの。

- ・ 請求の範囲 1, 11, 21, 31
上述のとおりである。

- ・ 請求の範囲 4, 14, 24

文献 1 には、ホームサーバ 1-1 が、ホームカード 1-2 から秘密鍵及びユーザの証明書を読み出すことも記載されている。同文献の段落 0064 参照。

(イ) 文献 1 の記載及び当業者の周知事項から、進歩性を見出せないもの。

- ・ 請求の範囲 5, 15, 25

データを読み込む際に、暗証番号を入力することは、周知の事項である。

- ・ 請求の範囲 8, 18, 28

サーバ認証ができた場合に限り、サーバへの中継を可能とすることは、周知の事項である。

- ・ 請求の範囲 10, 20, 30

文献 1 には、電子マーケットサーバ 1-5 とユーザ端末 1-3 とが、ホームサーバ 1-1 を介して、共通鍵 X を交換し、暗号化通信を行う(同文献の段落 0047、図 2 参照。)ことも記載されている。ワンタイムパスワードを用いることは周知の事項である。

(2) 請求の範囲 2-3, 7, 12-13, 17, 22-23, 27

許可リストを備えるもの。

(3) 請求の範囲 6, 16, 26

パケット分析により接続元の情報を自身の情報として利用するもの。

(4) 請求の範囲 9, 19, 29

認証装置内にブラウザ表示手段を備えるもの。

そして、上記各群の間には、PCT 規則 13.2 の第 2 文の意味において特別な技術的特徴と考えられる他の共通の事項は存在しないので、上記各群の間に PCT 規則 13 の意味における技術的な関連を見出すことはできない。

よって、請求の範囲 1-31 は発明の単一性の要件を満たしていないことが明らかである。