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

特許第5248057号
(P5248057)

(45)発行日　平成25年7月31日(2013.7.31)　(24)登録日　平成25年4月19日(2013.4.19)

(51)Int.Cl.		F I		
H04L 9/32	(2006.01)	H04L	9/00	675D
G06F 21/71	(2013.01)	G06F	21/02	171B
G06F 21/44	(2013.01)	G06F	21/20	144C

請求項の数 5　(全 14 頁)

(21)出願番号　特願2007-197933(P2007-197933)
(22)出願日　平成19年7月30日(2007.7.30)
(62)分割の表示　特願2000-378061(P2000-378061)の分割
原出願日　平成12年12月12日(2000.12.12)
(65)公開番号　特開2007-325306(P2007-325306A)
(43)公開日　平成19年12月13日(2007.12.13)
審査請求日　平成19年12月10日(2007.12.10)
審判番号　不服2011-14330(P2011-14330/J1)
審判請求日　平成23年7月4日(2011.7.4)

(73)特許権者　392026693
株式会社エヌ・ティ・ティ・ドコモ
東京都千代田区永田町二丁目１１番１号
(74)代理人　100098084
弁理士　川▲崎▼　研二
(72)発明者　平松　孝朗
東京都千代田区永田町二丁目１１番１号
株式会社エヌ・ティ・ティ・ドコモ内
(72)発明者　山本　正明
東京都千代田区永田町二丁目１１番１号
株式会社エヌ・ティ・ティ・ドコモ内
(72)発明者　若林　達明
東京都千代田区永田町二丁目１１番１号
株式会社エヌ・ティ・ティ・ドコモ内

最終頁に続く

(54)【発明の名称】通信方法、サーバ装置および端末装置

(57)【特許請求の範囲】
【請求項１】
第１のノードがサーバ装置に対し、前記第１のノードと第２のノードとの間の通信接続の確立の要求を送信するステップと、
前記サーバ装置が、前記要求に応じて、前記第１のノードと前記第２のノードとの間の通信接続の制御処理を行うステップと、
前記サーバ装置が、前記通信接続の確立を示す通知とともに現在時刻情報を前記第１のノードに対し送信するステップと、
前記第１のノードと前記第２のノードとの間で、前記通信接続を用いて、暗号化通信を開始するステップと、
前記第１のノードが、前記第２のノードを認証するための有効期限のある証明書を受信するステップと、
前記第１のノードが、前記証明書が有効であることを、前記現在時刻情報に基づき検証するステップと、
前記検証において前記証明書が有効であるとの結果が得られなかった場合、前記暗号化通信を終了するステップと
を備える通信方法。
【請求項２】
前記サーバ装置が、前記第１のノードと前記第２のノードとの間で行われる前記暗号化通信をトンネリングするステップ

を備える請求項１に記載の通信方法。
【請求項３】
第１のノードから、前記第１のノードと第２のノードとの間の通信接続の確立の要求を受信する受信手段と、
前記要求に応じて、前記第１のノードと前記第２のノードとの間の通信接続の制御処理を行う制御手段と、
前記通信接続の確立を示す通知とともに現在時刻情報を前記第１のノードに対し送信する送信手段と
を備えるサーバ装置。
【請求項４】
前記第１のノードと前記第２のノードとの間で前記通信接続を用いて行われる暗号化通信をトンネリングにより中継する中継手段
を備える請求項３に記載のサーバ装置。
【請求項５】
サーバ装置に対し、自機とは異なる他のノードとの間の通信接続の確立の要求を送信する送信手段と、
前記サーバ装置から前記通信接続の確立を示す通知とともに現在時刻情報を受信する現在時刻情報受信手段と、
前記他のノードとの間で、前記通信接続を用いて、暗号化通信を行う暗号化通信手段と、
前記他のノードから前記他のノードを認証するための有効期限のある証明書を受信する証明書受信手段と、
前記証明書が有効であることを、前記現在時刻情報受信手段により受信された現在時刻情報に基づき検証する検証手段と
を備え、
前記暗号化通信手段は、前記検証手段による検証において前記証明書が有効であるとの結果が得られなかった場合、前記暗号化通信を終了する
端末装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は通信相手の正当性を判定する認証方法と、この認証方法を実現するための中継装置および通信装置に関する。
【背景技術】
【０００２】
古くから、ネットワークを用いた情報システムにおいて、セキュリティを確保するための認証技術が開発されてきている。近年では、特に、インターネットのような不特定多数のユーザに開放されたオープンネットワークを用いた通信システムに適した認証技術が数多く開発されている。この種の認証技術の一つとして公開鍵暗号方式を利用したディジタル署名方式が広く知られている。ディジタル署名方式では、送信者が、自身のみが知る秘密鍵で平文を暗号化して送信し、この暗号化データを受信した受信者が、送信者の公開鍵を用いて復号化する。この復号化に成功すれば、受信者は、得られた平文は間違いなく送信者によって送信されたものである、と判断できる。
【０００３】
ただし、秘密鍵と公開鍵とが正しく対応して復号化に成功したとしても、十分に高いセキュリティを確保するためには、その公開鍵が真の送信者のものである保証が必要となる。この保証は公正な第３者機関である認証局（ＣＡ）のみが知る秘密鍵で暗号化された公開鍵証明書を用いて実現されている。すなわち、受信者が認証局の公開鍵を保持している状況下で、送信者が上記暗号化データと認証局から取得した自身の公開鍵証明書を送信すると、これらを受信した受信者は、認証局の公開鍵を用いて上述と同様の方法で公開鍵証

明書の正当性を検証し、正当だと判断された公開鍵証明書に含まれている送信者の公開鍵を用いて暗号化データを復号化する。ここで使用される送信者の公開鍵は認証局に保証されたものであることから、上記暗号化データの復号化に成功したということはこの暗号化データの送信者が真の送信者であることを認証局が保証したことに他ならない。

【発明の開示】

【発明が解決しようとする課題】

【０００４】

上記公開鍵証明書は自身の有効期限を内包しており、上記受信者は有効期限を過ぎた公開鍵証明書を正当でない公開鍵証明書と判断する。有効期限を過ぎたか否かの判定は、受信者である受信装置内のリアルタイムクロックに基づいて為される。したがって、認証局はもちろん、受信装置のリアルタイムクロックが正確に現在時刻を計時していないと、正確な判定が行われず、十分に高いセキュリティを確保する上での障害となり得る。このような問題は公開鍵暗号方式に限らず、認証に必要な情報に有効期限が設定されている全ての認証方式に共通して存在しているが、未だ重大な問題として認識されていない。

【０００５】

本発明は上述した事情に鑑みて為されたものであり、十分に高いセキュリティを確実に確保することができる認証方法と、この認証方法を実現するための中継装置および通信装置とを提供することを目的としている。

【課題を解決するための手段】

【０００６】

上述した課題を解決するため、本願発明は、第１のノードがサーバ装置に対し、前記第１のノードと第２のノードとの間の通信接続の確立の要求を送信するステップと、前記サーバ装置が、前記要求に応じて、前記第１のノードと前記第２のノードとの間の通信接続の制御処理を行うステップと、前記サーバ装置が、前記通信接続の確立を示す通知とともに現在時刻情報を前記第１のノードに対し送信するステップと、前記第１のノードと前記第２のノードとの間で、前記通信接続を用いて、暗号化通信を開始するステップと、前記第１のノードが、前記第２のノードを認証するための有効期限のある証明書を受信するステップと、前記第１のノードが、前記証明書が有効であることを、前記現在時刻情報に基づき検証するステップと、前記検証において前記証明書が有効であるとの結果が得られなかった場合、前記暗号化通信を終了するステップとを備える通信方法を提供する（第１の態様）。

【０００７】

第１の態様の通信方法において、前記サーバ装置が、前記第１のノードと前記第２のノードとの間で行われる前記暗号化通信をトンネリングするステップを備えるようにしてもよい（第２の態様）。

【０００８】

また、本願発明は、第１のノードから、前記第１のノードと第２のノードとの間の通信接続の確立の要求を受信する受信手段と、前記要求に応じて、前記第１のノードと前記第２のノードとの間の通信接続の制御処理を行う制御手段と、前記通信接続の確立を示す通知とともに現在時刻情報を前記第１のノードに対し送信する送信手段とを備えるサーバ装置を提供する（第３の態様）。

【０００９】

第３の態様のサーバ装置において、前記第１のノードと前記第２のノードとの間で前記通信接続を用いて行われる暗号化通信をトンネリングにより中継する中継手段を備えるようにしてもよい（第４の態様）。

【００１０】

また、本願発明は、サーバ装置に対し、自機とは異なる他のノードとの間の通信接続の確立の要求を送信する送信手段と、前記サーバ装置から前記通信接続の確立を示す通知とともに現在時刻情報を受信する現在時刻情報受信手段と、前記他のノードとの間で、前記通信接続を用いて、暗号化通信を行う暗号化通信手段と、前記他のノードから前記他のノ

ードを認証するための有効期限のある証明書を受信する証明書受信手段と、前記証明書が有効であることを、前記現在時刻情報受信手段により受信された現在時刻情報に基づき検証する検証手段とを備え、前記暗号化通信手段は、前記検証手段による検証において前記証明書が有効であるとの結果が得られなかった場合、前記暗号化通信を終了する端末装置を提供する（第５の態様）。

【発明の効果】

【００１３】

本発明によれば、現在時刻を用いて通信相手の正当性を判定する通信装置においては、正確な現在時刻を計時している中継装置から送信されてきた時刻情報に基づいた時刻が現在時刻として設定される。すなわち、通信相手の正当性が正確な現在時刻に基づいて判定される。したがって、本発明によれば、十分に高いセキュリティを確実に確保することができる。特に、移動通信網を介して通信するような通信装置については、計時している現在時刻を正確に保つ新しい仕組みを提供することができるという効果もある。

【発明を実施するための最良の形態】

【００１４】

以下、図面を参照して、本発明の実施形態について説明する。

［実施形態］

（１）全体構成

図１は本発明の実施形態に係る認証方法を用いた認証システムの構成を示す図であり、この認証システムはブラウザを搭載した携帯電話機からインターネットを用いてＷＷＷ（World Wide Web）サービスを利用可能な通信システム上に構築されている。このような通信システムは既に実現されており、その仕組みも周知であることから、当該通信システムについては、本発明に直接的に関連する部分についてのみ説明する。

【００１５】

同図において、携帯電話機ＭＳは移動パケット通信網ＭＰＮのパケット通信サービスを受ける携帯電話機であり、移動パケット通信網ＭＰＮ及び図示せぬ移動電話網に収容される。移動電話網は一般的な移動電話の通話サービスを提供する網であり、携帯電話機ＭＳは当該通話サービスを受けることができる。また、携帯電話機ＭＳは、ＳＳＬ（Secure Sockets Layer）をサポートしている。ＳＳＬは２層から構成されており、下位層はデータの配送、圧縮などのための機能を有し、上位層は認証や各種ネゴシエーションのための機能を有する。ＳＳＬ通信では、公開鍵暗号方式により通信相手を認証した後に共通鍵を用いた暗号化通信が行われる。

【００１６】

移動パケット通信網ＭＰＮは、複数の基地局ＢＳ、複数のパケット加入者処理装置ＰＳ、ゲートウェイサーバＧＷＳ、及びこれらを接続する通信回線によって構成されている。基地局ＢＳは、地上を例えば半径５００ｍ等の範囲で分割した所定間隔で配置されており、各々が形成する無線ゾーンに在圏した携帯電話機ＭＳとの間で無線通信を行う。パケット加入者処理装置ＰＳは、複数の基地局ＢＳを収容するパケット加入者交換局に備えられたコンピュータシステムであり、携帯電話機ＭＳからのパケット交換要求を受け付けるとともに、携帯電話機ＭＳとゲートウェイサーバＧＷＳ間でパケットを中継する。

【００１７】

ゲートウェイサーバＧＷＳは、移動パケット通信網ＭＰＮとインターネットＩＮＥＴ等の他網とを相互接続するための移動パケット関門中継交換局に備えられたコンピュータシステムであり、移動パケット通信網ＭＰＮの提供事業者によって管理されている。この提供事業者は携帯電話機ＭＳとＩＰサーバＷとのＳＳＬ通信において公正な第３者となっている。ゲートウェイサーバＧＷＳは、いわゆるプロキシサーバの機能を備え、ネットワーク間で異なる通信プロトコルの変換や通信の中継等を行う。ここでいう通信プロトコルの変換とは、具体的には、移動パケット通信網ＭＰＮが従う移動パケット通信網用の伝送プロトコルと、インターネットＩＮＥＴが従う伝送プロトコル（ＴＣＰ／ＩＰ（Transmission Control Protocol / Internet Protocol）やＨＴＴＰ（Hyper Text Transfer Protoco

l）等）との相互変換をいう。また、ゲートウェイサーバＧＷＳは、ＳＳＬ通信等の暗号化通信を通過させる機能（トンネリング機能）を備えている。この通過の際には、ゲートウェイサーバＧＷＳは暗号化通信の内容を把握することはできず、単なるルータとして機能する。

【００１８】

ＩＰサーバWはインターネットＩＮＥＴに接続されたサーバであり、WWWを利用するクライアントに対してWWWサービスを提供する。また、ＩＰサーバWはＳＳＬをサポートしており、クライアントとの間でＳＳＬ通信を行う機能を備えている。すなわち、ＩＰサーバWは、自身の秘密鍵および公開鍵と、認証局Ｃにより発行された公開鍵証明書とを格納しており、インターネットＩＮＥＴ経由でＳＳＬ通信におけるクライアントハロー（ClientHello）メッセージを受信すると、サーバハロー（ServerHello）メッセージと自身の公開鍵証明書を添付したサーバ認証要求（ServerCertificateRequest）メッセージを返信する。

【００１９】

認証局Ｃは公正な第３者機関であり、インターネットＩＮＥＴに接続されたサーバとして実現されている。この認証局Ｃは、公開鍵証明書等の電子証明書を発行・管理するものであり、クライアントからの要求に応じて電子証明書を発行して返信したり、自身の公開鍵を返信したりする。なお、認証局Ｃは、有効期限付きの電子証明書を発行する場合には、公正かつ正確であることが保証されている内部のリアルタイムクロックに基づいて有効期限を決定する。

【００２０】

（２）携帯電話機ＭＳの構成

図２は携帯電話機ＭＳのハードウェア構成を示すブロック図である。

この図に示すように、携帯電話機ＭＳは、基地局ＢＳとの無線通信を行う送受信部（例えばアンテナや無線部、送信機、受信機等を有する）２１、音を入力するための集音部（例えばマイク）２２、発音するための発音部（例えばアンプやスピーカ等を有する）２３、数字入力、文字入力等の入力操作が行われる、キーパッド等を備えた入力部２４、所定サイズの表示領域を有する液晶ディスプレイ２５、現在時刻を計時するリアルタイムクロック２７、及び、これら各部を制御する制御部２６を備えている。

【００２１】

制御部２６は各種制御を行うＣＰＵ（Central Processing Unit）２６１と、ＣＰＵ２６１に実行されるブラウザやＳＳＬ通信処理プログラム等のソフトウェア、及びゲートウェイサーバＧＷＳとの接続に必要な情報等を格納したＲＯＭ２６２と、ＣＰＵ２６１のワークエリアとして使用されるＲＡＭ２６３、認証局Ｃの公開鍵等の各種情報を格納するための不揮発性メモリ２６４とを内蔵しており、図示せぬ電源が投入されると、ＣＰＵ２６１はＲＯＭ２６２に格納されたソフトウェアを読み出して実行し、ＲＯＭ２６２、ＲＡＭ２６３、不揮発性メモリ２６４、および各部２１～２５，２７を制御する。

【００２２】

また、ＣＰＵ２６１は入力部２４から入力されるユーザの指示が所定の指示の場合には、ＲＯＭ２６２に格納されているＳＳＬ通信処理プログラムを実行する。ＳＳＬ通信処理プログラムを実行した状態では、ＣＰＵ２６１は、時刻を表す時刻情報を含んだ特定のメッセージを送受信部２１から受け取ると、当該時刻を現在時刻としてリアルタイムクロック２７に設定する機能を有する。詳しくは後述するが、上記特定のメッセージとは、ＳＳＬ通信の開始をゲートウェイサーバＧＷＳに要求するメッセージに応答してゲートウェイサーバＧＷＳから送信されてきたメッセージである。

【００２３】

また、上記状態のＣＰＵ２６１は、少なくとも一種類の暗号化アルゴリズムおよび圧縮アルゴリズムを使用可能となっており、これらの暗号化アルゴリズムおよび圧縮アルゴリズムを通信相手に通知するクライアントハローメッセージを生成し、これを送信するように送受信部２１を制御する機能と、送受信部２１が受信したサーバハローメッセージに指

定されている暗号化アルゴリズムおよび圧縮アルゴリズムを用いて通信処理を行う機能を有する。さらに、上記状態のＣＰＵ２６１は、送受信部２１が受信したサーバ認証要求メッセージに含まれている公開鍵証明書と認証局Ｃの公開鍵とリアルタイムクロック２７が計時している現在時刻とに基づいて通信相手の正当性を判定し、正当と判定された通信相手とのみＳＳＬ通信を継続する機能を有する。

【００２４】

（３）ゲートウェイサーバＧＷＳの構成

図３はゲートウェイサーバＧＷＳのハードウェア構成を示すブロック図である。

この図に示すように、ゲートウェイサーバＧＷＳは、基地局ＢＳ及びパケット加入者処理装置ＰＳを介して携帯電話機ＭＳとの間で無線通信を行うための無線系通信装置３１、インターネットＩＮＥＴを介してＩＰサーバW等との間で通信を行うためのインターネット接続インタフェース３２、基本プログラム等のソフトウェアや各種データを書き換え可能に記憶した記憶装置（例えば、半導体ディスクやハードディスク等）３３、現在時刻を計時するリアルタイムクロック３５、上記各部を制御する制御部３４を備えている。

【００２５】

制御部３４は各種制御を行うＣＰＵ３４１と、ＣＰＵ３４１に実行される制御プログラム等を格納したＲＯＭ３４２と、ＣＰＵ３４１のワークエリアとして使用されるＲＡＭ３４３とを内蔵しており、ＣＰＵ３４１は、ＲＯＭ３４２に格納された制御プログラムを読み出して実行することで、ＲＯＭ３４２、ＲＡＭ３４３及び各部３１～３３，３５を制御し、さらに記憶装置３３に記憶された基本プログラムを読み出して実行することで前述の機能を実現している。

【００２６】

基本プログラムを実行した状態では、ＣＰＵ３４１は、正確であることが保証されている内部のリアルタイムクロック３５に基づいて有効期限を設定する。リアルタイムクロック３５の時刻を正確に保つ手法としては広く普及しているＮＴＰ（Network Time Protocol）を用いる方法も考えられるが、本実施形態では、ＣＰＵ３４１が正確であることが保証されているリアルタイムクロック（例えば認証局Ｃのリアルタイムクロック）から図示せぬ専用線を介して時刻情報を取得し、これを用いてリアルタイムクロック３５の時刻を正確に保っている。

【００２７】

また、上記状態のＣＰＵ３４１は、上記状態のＣＰＵ３４１は、移動パケット通信網ＭＰＮの伝搬遅延時間を計測し、ＲＡＭ３４３に記憶させる機能を有する。さらに、上記状態のＣＰＵ３４１は、無線系通信装置３１を介して通信希望先とのＳＳＬ通信の開始を要求するメッセージを受け取ると、このメッセージの送信元の携帯電話機と通信希望先のＩＰサーバとの間にＴＣＰコネクションを設定するとともに、リアルタイムクロック３５の現在時刻に移動パケット通信網ＭＰＮの伝搬遅延時間を加算して得られる時刻を表す時刻情報を含んだメッセージを生成し、このメッセージをＳＳＬ通信の開始を要求するメッセージへの応答として返信するように無線系通信装置３１を制御する機能を有する。

【００２８】

（４）ＩＰサーバWの構成

図４はＩＰサーバWのハードウェア構成を示すブロック図である。

この図に示すように、ＩＰサーバWは、インターネットＩＮＥＴを介してゲートウェイサーバＧＷＳとの間で通信を行うためのインターネット接続インタフェース４１、各種コンテンツやＩＰサーバWの秘密鍵および公開鍵、ＳＳＬ通信処理プログラム等を書き換え可能に記憶した記憶装置（例えば、半導体ディスクやハードディスク等）４２、現在時刻を計時するリアルタイムクロック４４、及びこれらを制御する制御部４３を備えている。

【００２９】

制御部４３は各種制御を行うＣＰＵ４３１と、ＣＰＵ４３１に実行される制御プログラム等を格納したＲＯＭ４３２と、ＣＰＵ４３１のワークエリアとして使用されるＲＡＭ４３３とを内蔵しており、ＣＰＵ４３１は、ＲＯＭ４３２に格納された制御プログラムを読

み出して実行することで、ＲＯＭ４３２、ＲＡＭ４３３、及び各部４１～４２，４４を制御する。

【００３０】

制御プログラムを実行した状態のＣＰＵ４３１は、インターネット接続インタフェース４１を介してクライアントハローメッセージを受け取ると、ＳＳＬ通信処理プログラムを用いて当該メッセージの送信元に対応したＳＳＬ通信プロセスを生成する。このＳＳＬ通信プロセスにおいて、ＣＰＵ４３１は、ＩＰサーバＷで使用可能な複数の暗号化および圧縮アルゴリズムから、上記クライアントハローメッセージに含まれている暗号化および圧縮アルゴリズムを抽出し、最終的にいずれか一つの暗号化および圧縮アルゴリズムを選択し、選択した暗号化および圧縮アルゴリズムを通知するサーバハローメッセージを上記送信元へ返信するとともに、記憶装置４２に記憶されたＩＰサーバＷの公開鍵証明書を内包したサーバ認証要求メッセージを上記送信元へ送信する機能を有する。

【００３１】

（５）動作

携帯電話機ＭＳが認証されたＩＰサーバＷとＳＳＬ通信を開始するまでの動作について主に図５～図８を参照して説明する。図５はＳＳＬ通信開始時に携帯電話機ＭＳにおいて行われる処理の流れを示すフローチャート、図６はＳＳＬ通信開始時にゲートウェイサーバＧＷＳにおいて行われる処理の流れを示すフローチャート、図７はＳＳＬ通信開始時にＩＰサーバＷにおいて行われる処理の流れを示すフローチャート、図８は携帯電話機ＭＳがＩＰサーバＷとのＳＳＬ通信を開始するまでのメッセージの流れを示すシーケンス図である。

【００３２】

ただし、前提として、携帯電話機ＭＳのＣＰＵ２６１は既にブラウザを実行しており、ゲートウェイサーバＧＷＳのＣＰＵ３４１は既に基本プログラムを実行しており、ＩＰサーバＷのＣＰＵ４３１は既に制御プログラムを実行しているものとする。また、ＩＰサーバＷの記憶装置４２にはＩＰサーバＷの秘密鍵と、この秘密鍵に対応した公開鍵に対して認証局Ｃにより発行された公開鍵証明書が記憶されているものとする。また、携帯電話機ＭＳの不揮発性メモリ２６４には認証局Ｃの公開鍵が記憶されているものとする。

【００３３】

携帯電話機ＭＳのユーザがＩＰサーバＷとの通信を行う旨の指示を入力部２４から入力すると、携帯電話機ＭＳのＣＰＵ２６１はＲＯＭ２６２に格納されたＳＳＬ通信プログラムを実行し、図５に示す処理を行う。すなわち、ＣＰＵ２６１は、まず、ＩＰユーザにより指定されたＩＰサーバＷとのＳＳＬ通信を要求するメッセージ（例えば“Connect https:// ...”）を生成し、これをゲートウェイサーバＧＷＳへ送信するように送受信部２１を制御する（ステップＳＡ１）。この結果、図８に示すように、携帯電話機ＭＳからゲートウェイサーバＧＷＳへメッセージｍ１が送信される。

【００３４】

ゲートウェイサーバＧＷＳでは、ＣＰＵ３４１が、無線系通信装置３１を介してメッセージｍ１を受け取ると、図６のステップＳＢ１に示すように、まず、携帯電話機ＭＳとＩＰサーバＷとの間にＴＣＰコネクションを確立する（図８のメッセージｍ２）。次に、ＣＰＵ３４１は、リアルタイムクロック３５から現在時刻を表す時刻情報を取得し（ステップＳＢ２）、現在時刻から伝搬遅延時間経過後の時刻を表す時刻情報を生成する（ステップＳＢ３）。さらにＣＰＵ３４１は、こうして生成された時刻情報を含むメッセージｍ３を生成し、これを携帯電話機ＭＳへ送信するように無線系通信装置３１を制御する（ステップＳＢ４）。この結果、図８に示すように、ゲートウェイサーバＧＷＳから携帯電話機ＭＳへ、ＴＣＰコネクションが確立されたことを示すメッセージｍ３がメッセージｍ１への応答メッセージとして送信される。以後、ゲートウェイサーバＧＷＳは当該ＴＣＰコネクションの通信に関してトンネリング処理を行う。

【００３５】

携帯電話機ＭＳでは、ＣＰＵ２６１が、送受信部２１を介してメッセージｍ３を受け取

ると（図５のステップＳＡ２）、このメッセージｍ３に含まれている時刻情報で表される時刻を現在時刻としてリアルタイムクロック２７に設定する。この結果、リアルタイムクロック２７が計時する現在時刻はゲートウェイサーバＧＷＳのリアルタイムクロック３５が計時している現在時刻と略一致する。

【００３６】

次に、ＣＰＵ２６１は、ＳＳＬ通信で用いる暗号化および圧縮アルゴリズムを決定する（ステップＳＡ４）。具体的には、ＣＰＵ２６１は、まず、携帯電話機ＭＳにおいて使用可能な暗号化および圧縮アルゴリズムをＩＰサーバＷへ知らせるクライアントハローメッセージｍ４を生成し、これをＩＰサーバＷへ送信するように送受信部２１を制御する。この結果、図８に示すように、携帯電話機ＭＳから上記ＴＣＰコネクションを介してＩＰサーバＷへクライアントハローメッセージｍ４が送信される。

【００３７】

ＩＰサーバＷでは、ＣＰＵ４３１が、上記ＴＣＰコネクションおよびインターネット接続インタフェース４１を介してメッセージｍ４を受け取ると、図７のステップＳＣ１に示すように、まず、メッセージｍ４の内容とＩＰサーバＷで使用可能な暗号化アルゴリズムおよび圧縮アルゴリズムとに基づいて、当該ＴＣＰコネクションでのＳＳＬ通信において使用する暗号化および圧縮アルゴリズムを選択する。次にＣＰＵ４３１は、選択した暗号化および圧縮アルゴリズムを携帯電話機ＭＳへ通知するメッセージｍ５を生成し、これを携帯電話機ＭＳへ送信するようにインターネット接続インタフェース４１を制御する（ステップＳＣ２）。この結果、図８に示すように、ＩＰサーバＷから上記ＴＣＰコネクションを介して携帯電話機ＭＳへメッセージｍ５が返信される。

【００３８】

携帯電話機ＭＳでは、ＣＰＵ２６１が、送受信部２１を介してメッセージｍ５を受け取ると、このメッセージｍ５が示す暗号化および圧縮アルゴリズムを、上記ＴＣＰコネクションを用いた通信において使用することを決定する。

【００３９】

一方、ＩＰサーバＷでは、メッセージｍ５が携帯電話機ＭＳへ送信された後に、ＣＰＵ４３１が、記憶装置４２からＩＰサーバＷの公開鍵証明書を読み出し、この公開鍵証明書を含むメッセージｍ６を生成し、これを携帯電話機ＭＳへ送信するようにインターネット接続インタフェース４１を制御する（ステップＳＣ３）。この結果、図８に示すように、ＩＰサーバＷから上記ＴＣＰコネクションを介して携帯電話機ＭＳへメッセージｍ６が送信される。

【００４０】

携帯電話機ＭＳでは、ＣＰＵ２６１が、送受信部２１を介してメッセージｍ６を受け取ると（ステップＳＡ５）、メッセージｍ６に含まれている公開鍵証明書を不揮発性メモリ２６４に記憶された公開鍵（認証局Ｃの公開鍵）で復号化する（ステップＳＡ６）。この復号化に成功すると（ステップＳＡ７）、ＣＰＵ２６１は、リアルタイムクロック２７から現在時刻を取得し（ステップＳＡ８）、現在時刻が有効期限以前の時刻であるか否かを判定する（ステップＳＡ９）。現在時刻が有効期限以前の時刻である場合には、当該証明書は認証局Ｃに保証された有効期限内の公開鍵証明書（すなわち正当な公開鍵証明書）であることから、ＣＰＵ２６１は暗号化通信を継続する処理を行う（ステップＳＡ１０）。したがって、以後、携帯電話機ＭＳとＩＰサーバＷとの間で暗号化通信が継続して行われる。

【００４１】

逆に、ステップＳＡ６における復号化に成功しなかった場合や、復号化に成功しても有効期限を過ぎている場合には、ＩＰサーバＷを認証することはできないため、ＣＰＵ２６１は上記ＴＣＰコネクションを切断するよう送受信部２１を制御し、ＩＰサーバＷの認証に成功しなかった旨をユーザに通知するよう液晶ディスプレイ２５および発音部２３を制御する（ステップＳＡ１１）。これにより、携帯電話機ＭＳとＩＰサーバＷとの間のＴＣＰコネクションが切断され、ＩＰサーバＷの認証に成功しなかった旨がユーザに通知され

る。
【００４２】
上述したように、本実施形態によればＩＰサーバＷの認証処理の直前に、携帯電話機ＭＳのリアルタイムクロック２７が計時している時刻がゲートウェイサーバＧＷＳのリアルタイムクロック３５（極めて正確な時刻を計時している）が計時している時刻と略一致するため、携帯電話機ＭＳにおいてＩＰサーバＷの公開鍵証明書の有効期限のチェックを正確に行うことができる。したがって、ＩＰサーバＷの認証をより正確に行うことができる。また、当然の結果として、携帯電話機ＭＳのリアルタイムクロック２７を正確に保つことができるという利点もある。
【００４３】
［変形例］
なお、上述した実施形態では、ＳＳＬ通信のクライアントとして携帯電話機ＭＳを例示したが、無線通信機能を備えたＰＤＡ（Personal Digital(Data) Assistants）等の携帯通信端末をクライアントとしてもよいし、ＰＨＳ（Personal Handyphone System）端末や携帯電話機とＰＤＡや携帯型コンピュータ等を組み合わせた端末システムをクライアントとしてもよいし、無線通信端末や有線通信端末と据え置き型のコンピュータを組み合わせた端末システムをクライアントとしてもよい。もちろん、有線通信を行う場合には有線通信区間とインターネットとがゲートウェイサーバで接続されることになる。
【００４４】
さらに、上述した実施形態ではＩＰサーバＷの公開鍵証明書の有効期限のチェックをより正確に行うために携帯電話機ＭＳのリアルタイムクロック２７による現在時刻をゲートウェイサーバＧＷＳのリアルタイムクロック３５による現在時刻に略一致させたが、両者を一致させる目的は公開鍵証明書の有効期限のチェックのみに限らない。例えば、電子鍵やパスワード等に有効期限が設定されている認証システムにおいては電子鍵やＩＤ、パスワード等の有効期限をチェックする目的であってもよい。また、サーバではなく、クライアントの公開鍵証明書や電子鍵、ＩＤ、パスワード等の有効期限をチェックする目的でサーバのリアルタイムクロックをゲートウェイサーバのリアルタイムクロックに追従させるようにしてもよい。
【００４５】
また、上述した実施形態においては、クライアントのリアルタイムクロックをゲートウェイサーバのリアルタイムクロックに追従させる例を挙げたが、サーバにおいて通信相手の認証を行う場合にはサーバのリアルタイムクロックをゲートウェイサーバのリアルタイムクロックに追従させるようにしてもよいし、サーバおよびクライアントにおいて相互に通信相手の認証を行う場合には両者のリアルタイムクロックをゲートウェイサーバのリアルタイムクロックに追従させるようにしてもよい。
【００４６】
また、クライアント（あるいはサーバ）に伝搬遅延時間を測定する機能を設け、ゲートウェイサーバにおける現在時刻をそのままクライアント（あるいはサーバ）へ通知し、クライアント（あるいはサーバ）において、通知された現在時刻から伝搬遅延時間だけ経過した時刻を現在時刻として設定するようにしてもよい。この方法は、インターネットや衛星を介したネットワーク等の伝搬遅延時間が通信路に応じて大幅に異なり得るネットワークを介した通信を行う際に特に有効である。
【００４７】
さらに、上述した実施形態では、接続元（クライアント）からの接続を要求するメッセージに対する応答メッセージが時刻情報を内包する例を示したが、時刻情報の送信方法はこの例に限定されるものではない。例えば、接続元（クライアントまたはサーバ）からの接続を要求するメッセージの受信を契機として接続先（サーバまたはクライアント）へ時刻情報を送信するようにしてもよい。
【００４８】
また、上述した実施形態では、クライアントが自機のリアルタイムクロックから現在時

刻を取得して有効期限のチェックに使用する例を挙げたが、これに限定されるものではない。例えば、ゲートウェイサーバから供給された現在時刻を有効期限のチェックにそのまま使用するようにしてもよい。この場合、リアルタイムクロックを持たないクライアント（あるいはサーバ）であっても有効期限のチェックを行うことができる。

【００４９】

さらに、上述したように、本実施形態では、クライアントからゲートウェイサーバへのメッセージに対する応答メッセージに時刻情報が含まれている場合に、クライアントにおいて新しい現在時刻が設定される。このため、新しい現在時刻の設定はゲートウェイサーバから送信された時刻情報のみに基づいて行われることになり、より高いセキュリティが確保されている。しかし、より高いセキュリティを確保するためには本実施形態に例示された仕組みを必ず採用しなければならないという訳ではない。すなわち、時刻情報の送信元がゲートウェイサーバであるか否かをクライアントにおいて判断できればよく、例えば、クライアントにおいてパケットの送信元アドレスを調べることで時刻情報の送信元がゲートウェイサーバであるか否かを判定するようにしてもよい。

【００５０】

また、上述した実施形態では通信相手の認証に必要な情報（公開鍵証明書）を用いる通信としてＳＳＬ通信を例示したが、本発明は提案されている各種の公開鍵暗号方式の通信に適用可能である。さらに言えば、認証に必要な情報がＩＤやパスワードのように暗号化通信を前提としていない場合には、本発明を暗号化されていない通信に適用することもできる。

【００５１】

また、時刻情報の送信元が中継装置の場合にのみ現在時刻を設定するように通信装置を構成すれば、中継装置を除いた他の装置が通信装置における現在時刻を変更することはできない。したがって、より高いセキュリティを確保することができる。この効果は、時刻情報を応答メッセージに含めて中継装置から通信装置へ渡すようにすることでも得られる。後者の場合には、通信装置と中継装置との間でやり取りされるメッセージの数を減らすこともできる。

【００５２】

また、通信装置において通信相手を正当と判定した後に初めて暗号化通信を行うようにすれば、暗号化通信のセキュリティを十分に高くすることができる。

また、中継装置における現在時刻よりも進んだ時刻を表す時刻情報を通信装置へ送信するようにすれば、伝搬遅延時間による誤差を排除することができる。

【図面の簡単な説明】

【００５３】

【図１】本発明の実施形態に係る認証方法を用いた認証システムの構成を示す図である。

【図２】同認証システムを構成する携帯電話機ＭＳのハードウェア構成を示すブロック図である。

【図３】同認証システムを構成するゲートウェイサーバＧＷＳのハードウェア構成を示すブロック図である。

【図４】同認証システムを構成するＩＰサーバWのハードウェア構成を示すブロック図である。

【図５】ＳＳＬ通信開始時に同携帯電話機ＭＳにおいて行われる処理の流れを示すフローチャートである。

【図６】ＳＳＬ通信開始時に同ゲートウェイサーバＧＷＳにおいて行われる処理の流れを示すフローチャートである。

【図７】ＳＳＬ通信開始時に同ＩＰサーバWにおいて行われる処理の流れを示すフローチャートである。

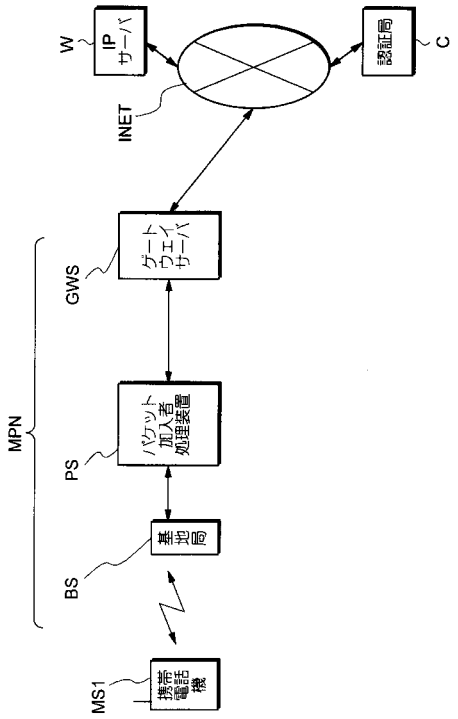
【図８】携帯電話機ＭＳがＩＰサーバWとのＳＳＬ通信を開始するまでのメッセージの流れを示すシーケンス図である。

【符号の説明】

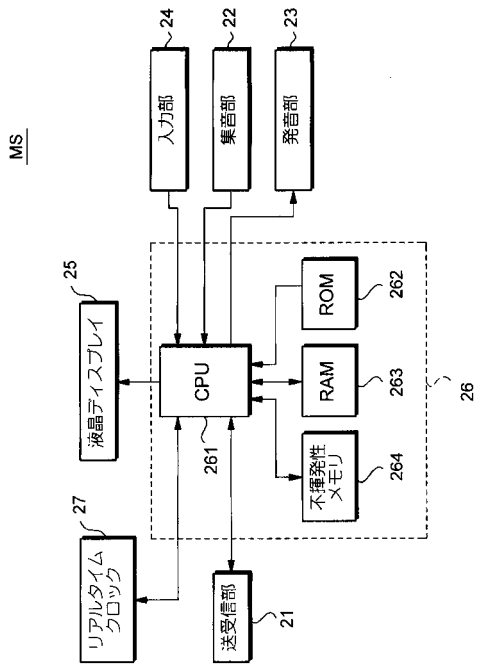
【００５４】

ＢＳ…基地局、ＧＷＳ…ゲートウェイサーバ、ＩＮＥＴ…インターネット、ＭＰＮ…移動パケット通信網、ＭＳ…携帯電話機、ＰＳ…パケット加入者処理装置、Ｗ…ＩＰサーバ、２１…送受信部、２２…集音部、２３…発音部、２４…入力部、２５…液晶ディスプレイ、２６，３４，４３…制御部、２７、３５、４４…リアルタイムクロック、３１…無線系通信装置、３２，４１…インターネット接続インタフェース、３３，４２…記憶装置、２６１，３４１，４３１…ＣＰＵ、２６２，３４２，４３２…ＲＯＭ、２６３，３４３，４３３…ＲＡＭ、２６４…不揮発性メモリ。

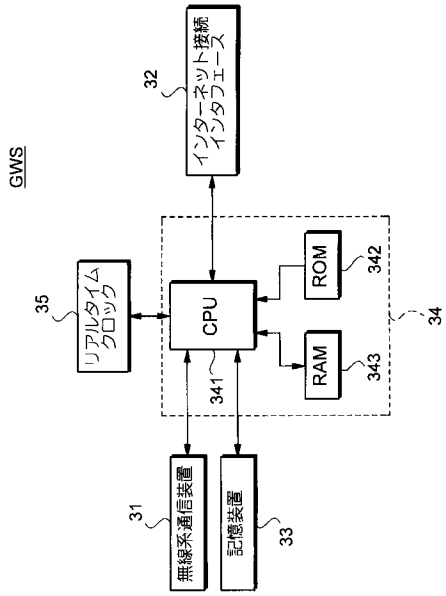
【図１】



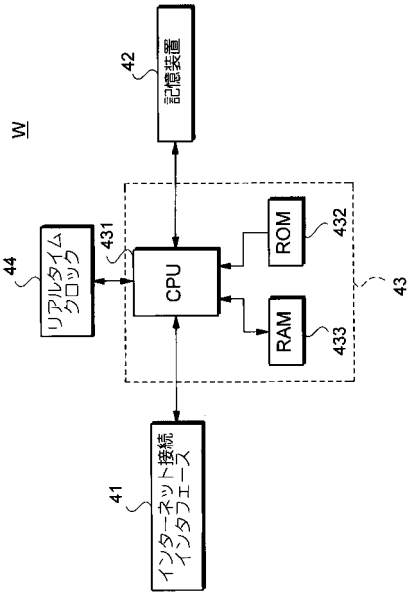
【図２】



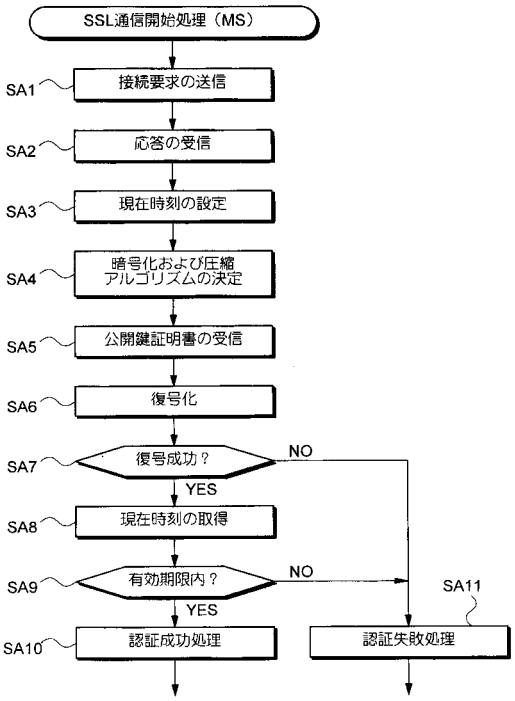
【図３】


GWS
32
インターネット接続インタフェース
35
リアルタイムクロック
CPU
ROM
342
RAM
343
341
34
31
無線系通信装置
記憶装置
33

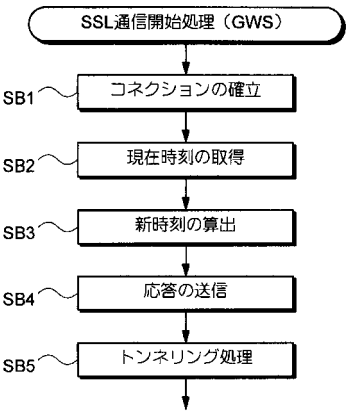
【図４】


W
42
記憶装置
44
リアルタイムクロック
431
CPU
ROM
432
RAM
433
43
41
インターネット接続インタフェース

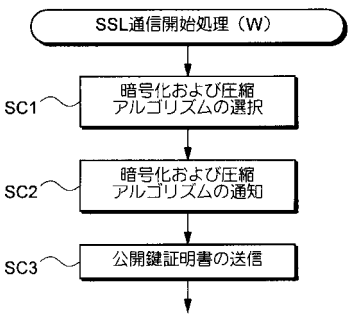
【図５】


SSL通信開始処理（MS）
SA1
接続要求の送信
SA2
応答の受信
SA3
現在時刻の設定
SA4
暗号化および圧縮アルゴリズムの決定
SA5
公開鍵証明書の受信
SA6
復号化
SA7
復号成功？
NO
YES
SA8
現在時刻の取得
SA9
有効期限内？
NO
YES
SA10
認証成功処理
SA11
認証失敗処理

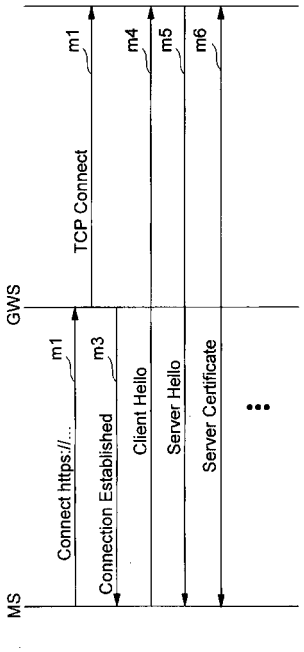
【図６】


SSL通信開始処理（GWS）
SB1
コネクションの確立
SB2
現在時刻の取得
SB3
新時刻の算出
SB4
応答の送信
SB5
トンネリング処理

【図７】


SSL通信開始処理（W）
SC1
暗号化および圧縮アルゴリズムの選択
SC2
暗号化および圧縮アルゴリズムの通知
SC3
公開鍵証明書の送信

【図８】


GWS
MS
m1
TCP Connect
m4
m5
m6
m1
Connect https://...
m3
Connection Established
Client Hello
Server Hello
Server Certificate
...

フロントページの続き

(72)発明者　高木　一裕
東京都千代田区永田町二丁目１１番１号　株式会社エヌ・ティ・ティ・ドコモ内

合議体
審判長　仲間　晃
審判官　石井　茂和
審判官　原　秀人

(56)参考文献　特開平１１－０１７６７４（ＪＰ，Ａ）
特開平０９－０１８９５９（ＪＰ，Ａ）
特開昭６３－０４２５３８（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F21/02