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

特許第4579597号
(P4579597)

(45)発行日　平成22年11月10日(2010.11.10)　(24)登録日　平成22年9月3日(2010.9.3)

(51)Int.Cl.　　F I
G06F 21/20 (2006.01)　　G06F 15/00 330B
G09C 1/00 (2006.01)　　G09C 1/00 640E

請求項の数 16　(全 18 頁)

(21)出願番号　特願2004-193472(P2004-193472)
(22)出願日　平成16年6月30日(2004.6.30)
(65)公開番号　特開2006-18399(P2006-18399A)
(43)公開日　平成18年1月19日(2006.1.19)
審査請求日　平成18年10月26日(2006.10.26)

(73)特許権者　000001007
キヤノン株式会社
東京都大田区下丸子３丁目３０番２号
(74)代理人　100126240
弁理士　阿部　琢磨
(74)代理人　100124442
弁理士　黒岩　創吾
(72)発明者　内川　慎一
東京都大田区下丸子３丁目３０番２号キヤノン株式会社内

審査官　田中　慎太郎

最終頁に続く

(54)【発明の名称】情報処理装置、情報処理方法およびプログラム

(57)【特許請求の範囲】
【請求項１】
外部装置と通信可能な情報処理装置であって、
ユーザからの指示に従って、外部装置と通信する場合に暗号化通信を使うとの設定または外部装置と通信する場合に暗号化通信を使わないとの設定を行う設定手段と、
暗号化通信を使わないとの設定に基づいて、認証で使われる認証情報を暗号化する第一の認証方法を選択し、暗号化通信を使うとの設定に基づいて、認証で使われる認証情報を暗号化しない第二の認証方法を選択する選択手段とを有することを特徴とする情報処理装置。
【請求項２】
複数のサービスのうちの少なくとも１つと前記選択手段により選択された認証方式とを対応づけて記憶する記憶手段と、
外部装置からのリクエストを受信するリクエスト受信手段と、
前記リクエストが要求するサービスに対応づけられた認証方式に基づく認証処理を実行する認証処理手段とを有することを特徴とする請求項１に記載の情報処理装置。
【請求項３】
前記第一の認証方式はＤｉｇｅｓｔ認証方式であり、前記第二の認証方式はＢａｓｉｃ認証方式であることを特徴とする請求項１または２に記載の情報処理装置。
【請求項４】
ユーザによって入力された、認証で用いられる認証情報を登録する登録手段を有し、

前記登録手段により登録された認証情報は、前記選択手段により選択されたいずれの認証方法においても用いられることを特徴とする請求項１乃至３のいずれか１項に記載の情報処理装置。

【請求項５】

前記暗号化通信とはＳＳＬを用いた通信であることを特徴とする請求項１乃至４のいずれか１項に記載の情報処理装置。

【請求項６】

外部機器と通信可能な情報処理装置であって、

外部機器からのデータを受信する受信手段と、

前記受信手段で受信したデータが暗号化通信によって通信されているかを判断する判断手段と、

前記受信手段で受信したデータが暗号化通信によって通信されていないとの判断に基づいて、認証で使われる認証情報を暗号化する第一の認証方法を選択し、前記受信手段で受信したデータが暗号化通信によって通信されているとの判断に基づいて、認証で使われる認証情報を暗号化しない第二の認証方法を選択する選択手段とを有することを特徴とする情報処理装置。

【請求項７】

前記判断手段は、前記受信手段により受信されたデータが通信されるのに用いられたプロトコルに基づいて、暗号化通信によって通信されているかを判断することを特徴とする請求項６に記載の情報処理装置。

【請求項８】

前記判断手段は、前記受信手段がデータを受信したポート番号に基づいて、暗号化通信によって通信されているかを判断することを特徴とする請求項６に記載の情報処理装置。

【請求項９】

前記第一の認証方式はＤｉｇｅｓｔ認証方式であり、第二の認証方式はＢａｓｉｃ認証方式であることを特徴とする請求項６乃至８のいずれか１項に記載の情報処理装置。

【請求項１０】

ユーザによって入力された、認証で用いられる認証情報を登録する登録手段を有し、

前記登録手段により登録された認証情報は、前記選択手段により選択されたいずれの認証方法においても用いられることを特徴とする請求項６乃至９のいずれか１項に記載の情報処理装置。

【請求項１１】

前記暗号化通信とはＳＳＬを用いた通信であることを特徴とする請求項６乃至１０のいずれか１項に記載の情報処理装置。

【請求項１２】

外部装置と通信可能な情報処理装置であって、

データを暗号化して通信するための所定のプロトコルを使うとの設定または前記所定のプロトコルを使わないとの設定を行う設定手段と、

前記所定のプロトコルを使わないとの設定に基づいて、認証で使われる認証情報を暗号化する第一の認証方法を選択し、前記所定のプロトコルを使うとの設定に基づいて、認証で使われる認証情報を暗号化しない第二の認証方法を選択する選択手段とを有することを特徴とする情報処理装置。

【請求項１３】

外部装置と通信可能な情報処理装置における情報処理方法であって、

ユーザからの指示に従って、外部装置と通信する場合に暗号化通信を使うとの設定または外部装置と通信する場合に暗号化通信を使わないとの設定を行う設定ステップと、

暗号化通信を使わないとの設定に基づいて、認証で使われる認証情報を暗号化する第一の認証方法を選択し、暗号化通信を使うとの設定に基づいて、認証で使われる認証情報を暗号化しない第二の認証方法を選択する選択ステップとを有することを特徴とする情報処理方法。

【請求項１４】
外部機器と通信可能な情報処理装置における情報処理方法であって、
外部機器からのデータを受信する受信ステップと、
前記受信ステップで受信したデータが暗号化通信によって通信されているかを判断する判断ステップと、
前記受信ステップで受信したデータが暗号化通信によって通信されていないとの判断に基づいて、認証で使われる認証情報を暗号化する第一の認証方法を選択し、前記受信ステップで受信したデータが暗号化通信によって通信されているとの判断に基づいて、認証で使われる認証情報を暗号化しない第二の認証方法を選択する選択ステップとを有することを特徴とする情報処理方法。
【請求項１５】
外部装置と通信可能なコンピュータを制御するプログラムであって、
ユーザからの指示に従って、外部装置と通信する場合に暗号化通信を使うとの設定または外部装置と通信する場合に暗号化通信を使わないとの設定を行う設定ステップと、
暗号化通信を使わないとの設定に基づいて、認証で使われる認証情報を暗号化する第一の認証方法を選択し、暗号化通信を使うとの設定に基づいて、認証で使われる認証情報を暗号化しない第二の認証方法を選択する選択ステップとを前記コンピュータに実行させることを特徴とするプログラム。
【請求項１６】
外部機器と通信可能なコンピュータを制御するプログラムであって、
外部機器からのデータを受信する受信ステップと、
前記受信ステップで受信したデータが暗号化通信によって通信されているかを判断する判断ステップと、
前記受信ステップで受信したデータが暗号化通信によって通信されていないとの判断に基づいて、認証で使われる認証情報を暗号化する第一の認証方法を選択し、前記受信ステップで受信したデータが暗号化通信によって通信されているとの判断に基づいて、認証で使われる認証情報を暗号化しない第二の認証方法を選択する選択ステップとを前記コンピュータに実行させることを特徴とするプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
外部機器と通信可能であって認証方式を選択する情報処理装置、及び外部機器と通信可能な情報処理装置において認証方式を選択する方法に関するものである。
【背景技術】
【０００２】
従来、情報処理装置が情報の公開やサービスの提供をする上で、情報処理装置による認証処理が行われていた。認証処理が行われるに当たっては、（１）ユーザ名及びパスワードなどのアカウント情報の設定のほか、認証処理に利用される認証方式の選択が必要である（例えば、特許文献１及び２）。
【０００３】
特許文献１の画像処理装置では、ユーザ自身が、使用する認証方式を設定する。
【特許文献１】特開２００３－０８４９２９号公報
【特許文献２】特開２００３－２９６０８５号公報
【発明の開示】
【発明が解決しようとする課題】
【０００４】
ネットワークを介してサービスなどを提供するサーバがネットワークを介した相手に対して行う認証処理において、選択可能な認証方式が、例えば２つある。
【０００５】
１つは、Ｂａｓｉｃ認証方式である。Ｂａｓｉｃ認証方式は、ＨＴＴＰ（Ｈｙｐｅｒ

Ｔｅｘｔ　Ｔｒａｎｓｆｅｒ　Ｐｒｏｔｏｃｏｌ）を用いた通信におけるユーザ認証技術の一つであり、認証情報としてのユーザ名とパスワードとが暗号化されないままネットワーク上を送信される。暗号化をしないため、認証処理における処理負荷は軽減される。

【０００６】

２つ目は、Ｄｉｇｅｓｔ認証方式である。ＨＴＴＰを用いた通信におけるユーザ認証技術の一つであり、ユーザ名とパスワードとが暗号化された上でネットワーク上を送信される。そのため、第三者がネットワークを監視している場合でも、当該第三者によって解読される危険性が軽減される。また、サーバ側の返す返答により、認証だけでなく、メッセージの完全保護、改ざんチェック、サーバ認証を実現可能であるという付加価値がある。ただし、通信のたびに、認証情報や送信するメッセージのＤｉｇｅｓｔ値を算出する必要があるため、認証処理における処理負荷が高くなる。

【０００７】

サーバが上記二種類の認証方式をサポートしていることは有用である一方、背景技術のようにサーバを管理する管理者が認証方式を選択しなければならない場合、いずれの認証方式を用いるべきかを判断するのは難しいことがある。管理者は一般に、誰にアクセスを許可するか、アクセスを許可する場合のユーザ名とパスワードをどうするかを決めることには注意を払うが、それぞれの認証方式がどうなっているかなどの技術的な知識を持ち合わせていない場合があるからである。

【０００８】

特に上記の二種類の認証方式では、暗号化が行われるか否かの違い、処理負荷の大きさの違いがあり、認証処理とは別のところで情報処理装置とその相手との間でネットワークで暗号化通信がなされているか否かによって、選択された認証方式の効果が変わってくる。

【０００９】

図１２は、サーバが行う認証処理のための認証設定画面の一例を示す図である。サーバがディスプレイなどを介してこの認証設定画面１２００を表示し、ユーザは、この設定画面において、サーバの認証機能に関する設定を行う。ここでは例として、サーバがＩＰＰ（Ｉｎｔｅｒｎｅｔ　Ｐｒｉｎｔｉｎｇ　Ｐｒｏｔｏｃｏｌ）サービス（ＩＰＰ機能とも呼ぶ）をクライアントＰＣ（クライアントパーソナルコンピュータ）に対して提供する上で行われる認証処理に関し、その設定画面について説明する。

【００１０】

１２０１は、サーバにおけるＩＰＰ機能を有効とするか（ＯＮ）無効とするか（ＯＦＦ）を選択するための選択スイッチである。無効が選択された場合には、ＩＰＰサービスがサーバにおいて提供されなくなる。

【００１１】

１２０２は、ＩＰＰ機能を提供する上でＨＴＴＰ及びＳＳＬを使って通信をするか（ＯＮ）、ＩＰＰ機能を提供する上でＨＴＴＰだけを使って通信をするか（ＯＦＦ）を選択するための選択スイッチである。ＨＴＴＰだけを使って通信をすると選択された場合には、サーバがＩＰＰ機能をクライアントＰＣに提供するに当たって、サーバとクライアントＰＣとの間ではＳＳＬのよる暗号化通信が行われなくなる。

【００１２】

１２０３は、ユーザがクライアントＰＣからＩＰＰ機能を利用する上で認証が行われるようにするか（ＯＮ）、認証が行われないようにするか（ＯＦＦ）を選択するための選択スイッチである。

【００１３】

１２０４は、認証が行われるように設定された場合に、認証方式としてＢａｓｉｃ認証を用いるかＤｉｇｅｓｔ認証を用いるかを選択するための選択スイッチである。

【００１４】

１２０５及び１２０６は、認証に用いられるユーザ名とパスワードとを設定するための入力ボックスである。ここで入力されたユーザ名とパスワードとが認証で用いられる。こ

こでは、複数のユーザの全てが同一のユーザ名とパスワードとを用いることとしたが、ユーザ名とパスワードとをユーザごとに設定可能にしてもよい。

【００１５】

例えば、ＨＴＴＰ及びＳＳＬを使って通信をするが選択された場合、Ｂａｓｉｃ認証方式とＤｉｇｅｓｔ認証方式とでは機能の違いはあまりなく、Ｄｉｇｅｓｔ認証方式では、認証処理において、ユーザ名、パスワード等の認証情報の盗聴による流出を防ぐために、認証情報のＤｉｇｅｓｔ値を算出し、そのＤｉｇｅｓｔ値を認証に利用する。そのため、認証情報のＤｉｇｅｓｔ値を算出する処理が必要であり、かつ、Ｄｉｇｅｓｔ認証の拡張機能である完全性保護（認証に加え送信/受信メッセージの改竄防止機能を含む方式）を利用する場合、メッセージ全体のＤｉｇｅｓｔ値を算出する必要もあるため、処理負荷が余分に高くなる。よって、処理付加を軽減するために、Ｂａｓｉｃ認証方式が選択される方がよい。しかし、ユーザは認証方式の技術的な内容を知らない場合、Ｄｉｇｅｓｔ認証方式を選択するかもしれない。

【００１６】

一方、ＨＴＴＰだけを使って通信をするが選択された場合、Ｂａｓｉｃ認証方式では、ユーザ名とパスワードとが暗号化されずに送信されることになる。

【００１７】

そこで、本発明では、複数の認証方式において、ユーザによる認証方式の選択がなくても、適切な認証方式を選択できるようにすることを目的とする。

【課題を解決するための手段】

【００１８】

本発明は、上記課題を解決するために、外部装置と通信可能な情報処理装置であって、ユーザからの指示に従って、外部装置と通信する場合に暗号化通信を使うとの設定または外部装置と通信する場合に暗号化通信を使わないとの設定を行う設定手段と、暗号化通信を使わないとの設定に基づいて、認証で使われる認証情報を暗号化する第一の認証方法を選択し、暗号化通信を使うとの設定に基づいて、認証で使われる認証情報を暗号化しない第二の認証方法を選択する選択手段とを有することを特徴とする。

【００１９】

または、外部装置と通信可能な情報処理装置であって、データを暗号化して通信するための所定のプロトコルを使うとの設定または前記所定のプロトコルを使わないとの設定を行う設定手段と、前記所定のプロトコルを使わないとの設定に基づいて、認証で使われる認証情報を暗号化する第一の認証方法を選択し、前記所定のプロトコルを使うとの設定に基づいて、認証で使われる認証情報を暗号化しない第二の認証方法を選択する選択手段とを有することを特徴とする情報処理装置。

【００２０】

または、外部機器と通信可能な情報処理装置であって、外部機器からのデータを受信する受信手段と、前記受信手段で受信したデータが暗号化通信によって通信されているかを判断する判断手段と、前記受信手段で受信したデータが暗号化通信によって通信されていないとの判断に基づいて、認証で使われる認証情報を暗号化する第一の認証方法を選択し、前記受信手段で受信したデータが暗号化通信によって通信されているとの判断に基づいて、認証で使われる認証情報を暗号化しない第二の認証方法を選択する選択手段とを有することを特徴とする。

【００２１】

または、外部装置と通信可能な情報処理装置における情報処理方法であって、ユーザからの指示に従って、外部装置と通信する場合に暗号化通信を使うとの設定または外部装置と通信する場合に暗号化通信を使わないとの設定を行う設定ステップと、暗号化通信を使わないとの設定に基づいて、認証で使われる認証情報を暗号化する第一の認証方法を選択し、暗号化通信を使うとの設定に基づいて、認証で使われる認証情報を暗号化しない第二の認証方法を選択する選択ステップとを有することを特徴とする。

【００２２】

または、外部機器と通信可能な情報処理装置における情報処理方法であって、外部機器からのデータを受信する受信ステップと、前記受信ステップで受信したデータが暗号化通信によって通信されているかを判断する判断ステップと、前記受信ステップで受信したデータが暗号化通信によって通信されていないとの判断に基づいて、認証で使われる認証情報を暗号化する第一の認証方法を選択し、前記受信ステップで受信したデータが暗号化通信によって通信されているとの判断に基づいて、認証で使われる認証情報を暗号化しない第二の認証方法を選択する選択ステップとを有することを特徴とする。

【００２３】

または、外部装置と通信可能なコンピュータを制御するプログラムであって、ユーザからの指示に従って、外部装置と通信する場合に暗号化通信を使うとの設定または外部装置と通信する場合に暗号化通信を使わないとの設定を行う設定ステップと、暗号化通信を使わないとの設定に基づいて、認証で使われる認証情報を暗号化する第一の認証方法を選択し、暗号化通信を使うとの設定に基づいて、認証で使われる認証情報を暗号化しない第二の認証方法を選択する選択ステップとを前記コンピュータに実行させることを特徴とする。

【００２４】

または、外部機器と通信可能なコンピュータを制御するプログラムであって、外部機器からのデータを受信する受信ステップと、前記受信ステップで受信したデータが暗号化通信によって通信されているかを判断する判断ステップと、前記受信ステップで受信したデータが暗号化通信によって通信されていないとの判断に基づいて、認証で使われる認証情報を暗号化する第一の認証方法を選択し、前記受信ステップで受信したデータが暗号化通信によって通信されているとの判断に基づいて、認証で使われる認証情報を暗号化しない第二の認証方法を選択する選択ステップとを前記コンピュータに実行させることを特徴とする。

【発明の効果】

【００２５】

本発明によれば、暗号化通信を行うという設定または暗号化通信を行わないという設定に基づいて認証方式を選択することにより、ユーザによる認証方式の選択作業を不要にすることができる。

【００２６】

または、受信されたデータが暗号化通信によって通信されたという判断または受信されたデータが暗号化通信によって通信されていないという判断に基づいて認証方式を選択することにより、ユーザによる認証方式の選択作業を不要にすることができる。

【００２７】

特に、選択の対象となる複数の認証方式が、認証に用いられる認証情報を暗号化する認証方式と認証に用いられる認証情報を暗号化しない認証方式とを含む場合、通信において暗号化がなされているかどうかに基づいて、適切な認証方式を選択することができる。

【発明を実施するための最良の形態】

【００２８】

以下、本発明の実施の形態を図面に基づいて説明する。

【００２９】

図１は、本発明に係るシステムの構成例を示す図である。１００は、認証設定システム機能を備えたＷＥＢサーバシステム（以下、ＷＥＢサーバと呼ぶ）である。ＷＥＢサーバ１００は、認証を必要とするコンテンツデータの配信や認証を必要とするサービスの提供を行うとともに、その認証も行っている。ＷＥＢサーバ１００は、プリンタ、複合機（ＭＦＰ）などの画像処理装置で実装されていても良い。

【００３０】

２００及び２１０は、ＷＥＢサーバを利用するクライアントＰＣである。ＷＥＢサーバ１００、クライアントＰＣ２００及びクライアントＰＣ２１０はネットワーク３００を介して通信可能に接続されている。なお、ネットワーク３００は、有線に限らず、無線のネ

ットワーク、例えば無線ＬＡＮで構成されていても良い。

【００３１】

図２は、ＷＥＢサーバ１００のハードウェア構成を示す図である。このＷＥＢサーバは一般的なＰＣと同じ構成を有する。すなわち、ＷＥＢサーバ１００は、ＲＯＭ２０２もしくはハードディスク（ＨＤ）２１１に記憶された、あるいはフロッピー（登録商標）ディスクドライブ（ＦＤ）２１２から供給される各種ソフトウェアを実行するＣＰＵ２１０を有しており、ＣＰＵ２０１はシステムバス２０４に接続された各部を総括的に制御する。

【００３２】

２０３はＲＡＭであり、ＣＰＵ２０１の主メモリ、ワークエリア等として機能する。２０５はキーボードコントローラ（ＫＢＣ）であり、キーボード（ＫＢ）２０９やポインティングデバイス（図示せず）等からの指示入力を制御する。２０６はＣＲＴコントローラ（ＣＲＴＣ）であり、ＣＲＴディスプレイ（ＣＲＴ）２１０の表示を制御する。

【００３３】

２０７はディスクコントローラ（ＤＫＣ）であり、ブートプログラム、分散サーバシステムプログラム、種々のアプリケーション、編集ファイル、ユーザファイル等を記憶するハードディスク（ＨＤ）２１１およびフロッピー（登録商標）ディスクドライブ（ＦＤ）２１２へのアクセスを制御する。２０８はネットワークインタフェースカード（ＮＩＣ）であり、ＬＡＮ３００を介してネットワークプリンタ、他のネットワーク機器あるいは他のＰＣと双方向にデータをやりとりする。

【００３４】

ＷＥＢサーバがプリンタ及び複合機などの画像処理装置である場合には、ＣＲＴ２１０の代わりに操作パネル、ＫＢ２０９の代わりに操作キーが設けられることなる。

【００３５】

図３は、ＷＥＢサーバ１００のソフトウェアモジュール構成を示す図である。３０１は、ＷＥＢサーバ１００が提供するコンテンツデータを格納するためのファイルシステムである。３０２は、ＷＥＢサーバ１００が情報またはサービスを提供するのに必要な設定情報、ＷＥＢサーバ１００が認証処理を行うのに必要な認証アカウント情報などを格納するアクセス設定情報データベースである。

【００３６】

３０３は、ＴＣＰ／ＩＰ通信を行うためのＴＣＰ／ＩＰモジュールである。ＴＣＰ／ＩＰモジュール３０３は、ＩＰパケットの解析又は生成、ＴＣＰパケットの解析又は生成を行い、上位のモジュールからのデータに対してＴＣＰヘッダやＩＰヘッダを付け、ネットワークからのデータからＴＣＰヘッダやＩＰヘッダを外して、その後のデータを上位のモジュールに渡す。

【００３７】

３０４は、暗号化通信を行うためのＳＳＬ（Ｓｅｃｕｒｅ　Ｓｏｃｋｅｔ　Ｌａｙｅｒ）モジュールである。ＳＳＬは、インターネット上で情報を暗号化して送受信するプロトコルであり、公開鍵暗号や秘密鍵暗号、デジタル証明書、ハッシュ関数などのセキュリティ技術を組み合わせ、データの盗聴や改ざん、なりすましを防ぐことができる。ＳＳＬモジュールは、ＴＣＰ／ＩＰモジュールの上位のモジュールである。

【００３８】

３０５は、ＨＴＴＰ（Ｈｙｐｅｒ　Ｔｅｘｔ　Ｔｒａｎｓｆｅｒ　Ｐｒｏｔｏｃｏｌ）を使って情報の公開又はサービスの提供を行うためのＨＴＴＰサーバモジュールである。３０６、３０７及び３０８は、所定のデータ処理を行ってクライアントＰＣに対してサービスを提供するＣＧＩ（Ｃｏｍｍｏｎ　Ｇａｔｅｗａｙ　Ｉｎｔｅｒｆａｃｅ）モジュールである。ＣＧＩモジュール３０６、３０７及び３０８は、ＨＴＴＰサーバモジュール３０５上で動作し、あるいはＨＴＴＰサーバモジュール３０５から起動されて動作する。

【００３９】

ＷＥＢサーバ１００は、情報に対するリクエスト（要求）またはサービスへのリクエストをクライアントＰＣから受信すると、そのリクエストは、ＴＣＰ／ＩＰモジュール３０

３またはＳＳＬモジュール３０４を介してＨＴＴＰサーバモジュール３０５に渡る。ＨＴＴＰサーバモジュール３０５は、そのリクエストを解析して、設定情報を参照してリクエストに対応した処理を実行する。ＷＥＢサーバ１００における認証処理は、ＨＴＴＰサーバモジュール３０５によって行われる場合と、ＣＧＩモジュール３０６によって行われる場合とがある。

【００４０】

図４は、ＷＥＢサーバ１００が行う認証処理のための認証設定画面の一例を示す図である。ＷＥＢサーバ１００がディスプレイなどを介してこの認証設定画面４００を表示し、ユーザは、この設定画面において、ＷＥＢサーバ１００の認証機能に関する設定を行う。ここでは例として、ＷＥＢサーバ１００がＩＰＰ（Ｉｎｔｅｒｎｅｔ　Ｐｒｉｎｔｉｎｇ　Ｐｒｏｔｏｃｏｌ）サービス（ＩＰＰ機能とも呼ぶ）をクライアントＰＣに対して提供する上で行われる認証処理に関し、その設定画面について説明する。なお、ＩＰＰ機能はＣＧＩモジュールによって提供される。

【００４１】

４０１は、ＷＥＢサーバ１００におけるＩＰＰ機能を有効とするか（ＯＮ）無効とするか（ＯＦＦ）を選択するための選択スイッチである。無効が選択された場合には、ＩＰＰサービスがＷＥＢサーバ１００において提供されなくなる。

【００４２】

４０２は、ＩＰＰ機能を提供する上でＨＴＴＰ及びＳＳＬを使って通信をするか（ＯＮ）、ＩＰＰ機能を提供する上でＨＴＴＰだけを使って通信をするか（ＯＦＦ）を選択するための選択スイッチである。ＨＴＴＰだけを使って通信をすると選択された場合には、ＷＥＢサーバ１００がＩＰＰ機能をクライアントＰＣに提供するに当たって、ＷＥＢサーバ１００とクライアントＰＣとの間ではＳＳＬのよる暗号化通信が行われなくなる。

【００４３】

４０３は、ユーザがクライアントＰＣからＩＰＰ機能を利用する上で認証が行われるようにするか（ＯＮ）、認証が行われないようにするか（ＯＦＦ）を選択するための選択スイッチである。

【００４４】

４０４及び４０５は、認証に用いられるユーザ名とパスワードとを設定するための入力ボックスである。ここで入力されたユーザ名とパスワードとが認証で用いられる。ここでは、複数のユーザの全てが同一のユーザ名とパスワードとを用いることとしたが、ユーザ名とパスワードとをユーザごとに設定可能にしてもよい。

【００４５】

図１２との相違点は、認証方式を選択するための選択スイッチがないことである。ＷＥＢサーバ１００では、ユーザが認証方式を選択することなく、設定画面の内容に応じた認証方式をＷＥＢサーバ１００が決定するからである。

【００４６】

＜第１の認証方式自動決定処理＞

図５は、ＷＥＢサーバ１００が認証設定画面の設定内容に従って認証方式を決定する認証方式自動決定処理を示すフローチャートである。この認証方式自動決定処理は、ＷＥＢサーバ１００のＣＰＵ２０１が、図５のフローチャートに基づくプログラムを実行することにより行われる。

【００４７】

ユーザが図４の設定画面のＯＫボタンを押すと、ＷＥＢサーバ１００はＳＳＬを使用するがＯＮになっているかＯＦＦになっているかを判断する（ステップＳ５０１）。

【００４８】

ＯＮになっている場合には、認証方式としてＢａｓｉｃ認証方式を選択して、ＩＰＰサービスの認証方式としてＢａｓｉｃ認証方式をアクセス設定情報データベース３０２に登録する（ステップＳ５０２）。ＯＦＦになっている場合には、認証方式としてＤｉｇｅｓｔ認証方式を選択して、ＩＰＰサービスの認証方式としてＤｉｇｅｓｔ認証方式をアクセ

ス設定情報データベース３０２に登録する。

【００４９】

図６は、ＷＥＢサーバ１００が保持するアクセス設定情報データベース３０２を示す図である。列６００には、リクエストで要求可能なサービスに対応するＵＲＩパス（Ｕｎｉｆｏｒｍ　Ｒｅｓｏｕｒｃｅ　Ｉｄｅｎｔｉｆｉｅｒ　Ｐａｔｈ）情報が格納されている。この列６００には存在しないパス情報を指定したリクエストは受け付けることができない。例えば、「／ｉｐｐ」はＩＰＰサービスに対応するパス情報である。図４の設定画面において、ＩＰＰ機能を有効とすると選択された場合に、「／ｉｐｐ」がデータベースに登録される。

【００５０】

列６０１には、それぞれのサービスで使用されるプロトコルを示すプロトコル情報が格納されている。ＨＴＴＰが指定されている場合には、ＨＴＴＰによるアクセスが可能となり、ＨＴＴＰＳが指定されている場合には、ＨＴＴＰ及びＳＳＬによるアクセスのみが可能となる。図６では、ＩＰＰサービスでは「ＨＴＴＰＳ」が指定されている。図４の設定画面において、ＳＳＬを用いると選択された場合に、「ＨＴＴＰＳ」が登録される。

【００５１】

列６０２には、ＵＲＩパスに対応するポート番号が格納されている。ＵＲＩパスで指定されたシステム資源への接続を許可するポート番号が記載されている。ＩＰＰサービスのポート番号は４４３であるので、ＩＰＰサービスに対するリクエストはポート番号「４４３」宛てに送信されなければならない。

【００５２】

列６０３には、ＵＲＩパスに対応したシステム資源の所在を示す情報が格納される。システム資源とは、ＷＥＢサーバ１００が保有するファイルであったり、ＷＥＢサーバ１００のＨＴＴＰサーバモジュール上で動作するＣＧＩモジュールであったりする。ＩＰＰサービスが要求された場合には、「ＩｐｐＳｅｒｖｉｃｅ」と言う名前のＣＧＩモジュールが起動される。

【００５３】

列６０４には、サービスを要求したりまたはシステム資源にアクセスしたりする場合に、認証が必要であるか否かを示す情報が格納されている。ＯＮは認証要を意味し、ＯＦＦは認証不要を意味する。ＩＰＰサービスでは「ＯＮ」が格納されている。図４の設定画面において、認証が行われるようにすると選択された場合、「ＯＮ」が登録される。

【００５４】

列６０５には、認証が行われる場合の認証方式を示す情報が格納されている。ここには、図５のステップＳ５０２またはＳ５０３で選択された認証方式が登録される。「Ｂａｓｉｃ」はＢａｓｉｃ認証方式を意味し、「Ｄｉｇｅｓｔ」はＤｉｇｅｓｔ認証方式を意味する。「Ｎｏｎｅ」は認証が行われない場合には格納される。

【００５５】

列６０６には、認証で用いられるユーザ名とパスワードとが格納される。これらのユーザ名とパスワードとが認証処理において指定された場合に限り、サービスへのアクセスが許可される。図４の設定画面において入力されたユーザ名とパスワードとがここに格納される。

【００５６】

図６の例では、ＷＥＢサーバ１００が、８０番ポートへのリクエストであって「／ｔｅｓｔ．ｔｘｔ」というパスを指定したリクエストをＨＴＴＰプロトコルを用いて受信した場合、ＷＥＢサーバ１００は、ＢＡＳＩＣ認証による認証をクライアントＰＣに要求する。その後、ＷＥＢサーバ１００が、ユーザ名及びパスワードとして「ｔｅｓｔ」及び「ｈｉｍｉｔｕ」をクライアントＰＣから受信した場合、ＷＥＢサーバ１００は、「／ＦＩＬＥ／ｔｅｓｔ．ｔｘｔ」へのアクセスをクライアントＰＣに許可する。

【００５７】

図７は、ＷＥＢサーバ１００がリクエストを受信した際に実行する処理を示すフローチ

ャートである。この処理は、ＷＥＢサーバ１００のＣＰＵ２０１が、図７のフローチャートに基づくプログラムを実行することにより行われる。

【００５８】

ＨＴＴＰサーバモジュール３０５は、クライアントＰＣからのリクエストデータを受信すると、そのリクエストデータのヘッダ情報を解析し、リクエストが指定するＵＲＩパス情報を取得する（ステップＳ７０１）。

【００５９】

取得したＵＲＩパス情報がアクセス設定情報データベース３０２に存在するか否かを確認し、リクエスト先として正しいか否かを判定する（ステップＳ７０２）。正しい場合には、ステップＳ７０３に進み、正しくない場合には、ステップＳ７０９に進む。

【００６０】

ステップＳ７０３では、アクセス設定情報データベース３０２の列６０４を確認して、指定されたＵＲＩパス情報において、認証要（ＯＮ）が登録されているか否かを判定する（ステップＳ７０３）。認証不要（ＯＦＦ）が登録されている場合には、認証処理が必要ないので、リクエストに応じた処理を実行する（ステップＳ７０８）。認証要（ＯＮ）が登録されている場合には、ステップＳ７０４に進む。

【００６１】

ステップＳ７０４では、アクセス設定情報データベース３０２の列６０５を確認して、指定されたＵＲＩパス情報に対応する認証方式がＢａｓｉｃ認証方式であるかＤｉｇｅｓｔ認証方式であるかを判断する（ステップＳ７０４）。

【００６２】

ステップＳ７０４において、Ｂａｓｉｃ認証方式であると判断した場合には、Ｂａｓｉｃ認証方式に基づく認証処理を行い（ステップＳ７０６）、Ｄｉｇｅｓｔ認証方式であると判断した場合には、Ｄｉｇｅｓｔ認証方式に基づく認証処理を行う（ステップＳ７０５）。

【００６３】

その後、認証処理が成功したかどうかを判断する（ステップＳ７０７）。成功した場合には、ステップＳ７０７に進み、失敗した場合には、ステップＳ７０９に進む。

【００６４】

ステップＳ７０７では、クライアントＰＣからのリクエストに基づく処理を行う。一方、ステップＳ７０９では、発生したエラーに応じたエラーレスポンスデータを作成する。ステップＳ７１０では、ステップＳ７０７で行われた処理の結果をレスポンスとして送信する。あるいは、ステップＳ７０９で作成されたエラーレスポンスデータをレスポンスとして送信する。

【００６５】

＜第２の認証方式自動決定処理＞

第１の認証方式自動決定処理では、認証設定画面において設定が行われたときに認証方式を決定したが、第２の認証方式自動決定処理では、クライアントＰＣからのリクエストを受信したときに認証方式を決定する。

【００６６】

図８は、第２の認証方式自動決定処理で用いられるアクセス設定情報データベース３０２を示す図である。図６のアクセス設定情報データベースとの相違点は、列６０５が存在しないことである。第２の認証方式自動決定処理では、ＷＥＢサーバがリクエストを受信した際に自動的に認証方式を決定するからである。それ以外の項目に関しては、図６と図８とでは同じ意味合いを持つので、ここでは説明を省略する。

【００６７】

図９は、ＷＥＢサーバ１００がリクエストを受信した際に認証方式を決定する認証方式自動決定処理を示すフローチャートである。この認証方式自動決定処理は、ＷＥＢサーバ１００のＣＰＵ２０１が、図９のフローチャートに基づくプログラムを実行することにより行われる。

【００６８】
ＨＴＴＰサーバモジュール３０５は、クライアントＰＣからのリクエストデータを受信すると、そのリクエストデータのヘッダ情報を解析し、リクエストが指定するＵＲＩパス情報を取得する（ステップＳ９０１）。
【００６９】
取得したＵＲＩパス情報がアクセス設定情報データベース３０２に存在するか否かを確認し、リクエスト先として正しいか否かを判定する（ステップＳ９０２）。正しい場合には、ステップＳ９０３に進み、正しくない場合には、ステップＳ９０９に進む。
【００７０】
ステップＳ９０３では、アクセス設定情報データベース３０２の列６０４を確認して、指定されたＵＲＩパス情報において、認証要（ＯＮ）が登録されているか否かを判定する（ステップＳ９０３）。認証不要（ＯＦＦ）が登録されている場合には、認証処理が必要ないので、リクエストに応じた処理を実行する（ステップＳ９０８）。認証要（ＯＮ）が登録されている場合には、ステップＳ９０４に進む。
【００７１】
ステップＳ９０４では、リクエストが暗号化通信によって通信されてきたかを判断する。暗号化通信が行われているか否かの判断は、以下の３つの方法のうちの少なくとも１つで行われる。
【００７２】
第１の判断方法は、アクセス設定情報データベース３０２の列６０１を確認して、指定されたＵＲＩパス情報に対応するプロトコルとして、ＨＴＴＰＳが登録されている場合には暗号化通信が行われていると判断し、ＨＴＴＰが登録されている場合には暗号化通信が行われていないと判断する。
【００７３】
第２の判断方法は、ＨＴＴＰサーバモジュール３０５がリクエストデータを受け取ったときに、ＳＳＬモジュール３０４から受け取った場合には暗号化通信が行われていると判断し、ＴＣＰ／ＩＰモジュール３０３から受け取った場合には暗号化通信が行われていないと判断する。
【００７４】
第３の判断方法は、リクエストを受信したポート番号が、暗号化通信が行うことになっているポート番号である場合には暗号化通信が行われていると判断し、暗号化通信が行われることになっていないポート番号である場合には暗号化通信が行われていないと判断する。
【００７５】
ステップＳ９０４において、暗号化通信が行われていると判断した場合には、Ｂａｓｉｃ認証方式に基づく認証処理を行い（ステップＳ９０６）、暗号化通信が行われていないと判断した場合には、Ｄｉｇｅｓｔ認証方式に基づく認証処理を行う（ステップＳ９０５）。
【００７６】
その後、認証処理が成功したかどうかを判断する（ステップＳ９０７）。成功した場合には、ステップＳ９０７に進み、失敗した場合には、ステップＳ９０９に進む。
【００７７】
ステップＳ９０７では、クライアントＰＣからのリクエストに基づく処理を行う。一方、ステップＳ９０９では、発生したエラーに応じたエラーレスポンスデータを作成する。ステップＳ９１０では、ステップＳ９０７で行われた処理の結果をレスポンスとして送信する。あるいは、ステップＳ９０９で作成されたエラーレスポンスデータをレスポンスとして送信する。
【００７８】
＜Ｂａｓｉｃ認証方式に基づく認証処理＞
図１０は、Ｂａｓｉｃ認証方式に基づく認証処理を示すフローチャートである。認証処

理は、図７のステップＳ７０６または図９のステップＳ９０６で実行されるものであり、ＷＥＢサーバ１００のＣＰＵ２０１が、図１０のフローチャートに基づくプログラムを実行することにより行われる。

【００７９】

クライアントＰＣからのリクエストデータには認証情報が設定されていないため、ＷＥＢサーバ１００は、Ｂａｓｉｃ認証を要求するレスポンスメッセージをクライアントＰＣに送信する（ステップＳ１００１）。

【００８０】

クライアントＰＣは、Ｂａｓｉｃ認証を要求するレスポンスメッセージを受信すると、ユーザ名とパスワードを入力するための入力画面を表示し、入力されたユーザ名とパスワードとから構成される認証情報が付加されたリクエストをＷＥＢサーバ２００に送信する。認証情報は、ユーザ名とパスワードとを「：」で接続したデータをＢａｓｅ６４コードで変換したものである。

【００８１】

ＷＥＢサーバはクライアントＰＣから再びリクエストを受信すると、当該リクエストに認証情報が付加されているかを判断する（ステップＳ１００２）。認証情報が無い場合には、認証失敗と判断する（ステップＳ１００６）。

【００８２】

認証情報がある場合には、認証情報をデコードして（ステップＳ１００３）、認証情報に含まれているユーザ名及びパスワードと、アクセス設定情報データベースに登録されているユーザ名及びパスワードと比較する。

【００８３】

比較の結果、一致していれば、認証成功と判断し（ステップＳ１００５）、一致していなければ、認証失敗と判断する（Ｓ１００６）。

【００８４】

＜Ｄｉｇｅｓｔ認証方式に基づく認証処理＞

図１１は、Ｄｉｇｅｓｔ認証方式に基づく認証処理を示すフローチャートである。認証処理は、図７のステップＳ７０５または図９のステップＳ９０５で実行されるものであり、ＷＥＢサーバ１００のＣＰＵ２０１が、図１１のフローチャートに基づくプログラムを実行することにより行われる。

【００８５】

クライアントＰＣからのリクエストデータには認証情報が設定されていないため、ＷＥＢサーバ１００は、Ｄｉｇｅｓｔ認証を要求するレスポンスメッセージをクライアントＰＣに送信する（ステップＳ１１０１）。

【００８６】

クライアントＰＣは、Ｄｉｇｅｓｔ認証を要求するレスポンスメッセージを受信すると、ユーザ名とパスワードを入力するための入力画面を表示し、入力されたユーザ名とパスワードとから構成される認証情報、ＷＥＢサーバ１００から受信したｎｏｎｃｅ値及びリクエストＵＲＩからＤｉｇｅｓｔ値を算出し、その値を含むＨＴＴＰヘッダが付加されたリクエストをＷＥＢサーバ１００に送信する。

【００８７】

ＷＥＢサーバはクライアントＰＣから再びリクエストを受信すると、当該リクエストにＤｉｇｅｓｔ値が付加されているかを判断する（ステップＳ１００２）。Ｄｉｇｅｓｔ値が無い場合には、認証失敗と判断する（ステップＳ１００６）。

【００８８】

Ｄｉｇｅｓｔ値がある場合には、その他の認証パラメータが正しいかどうかを判断し（ステップＳ１１０３）、正しくない場合には、ステップＳ１１０８に進み、正しい場合には、ステップＳ１１０４に進む。

【００８９】

ステップＳ１１０４では、アクセス設定情報データベースを確認して、ユーザ名及びパ

スワードが存在してるかを判断し、これらが存在しない場合には、ステップＳ１１０８に進み、存在する場合にはステップＳ１１０６に進む。

【００９０】

ステップＳ１１０６では、アクセス設定情報データベースに登録されているユーザ名及びパスワード、上記ｎｏｎｃｅ値、リクエストＵＲＩからＤｉｇｅｓｔ値を算出する。そして、クライアントＰＣから受信したＤｉｇｅｓｔ値とステップＳ１１０６で算出したＤｉｇｅｓｔ値とを比較し（ステップＳ１１０６）、一致していれば、認証成功と判断し（ステップＳ１１０７）、一致していなければ、認証失敗と判断する（ステップＳ１１０８）。

【００９１】

本発明は、上述した実施形態の装置に限定されず、複数の機器から構成されるシステムに適用しても、１つの機器から成る装置に適用してもよい。前述した実施形態の機能を実現するソフトウェアのプログラムコードを記憶した記憶媒体をシステムあるいは装置に供給し、そのシステムあるいは装置のコンピュータ（またはＣＰＵやＭＰＵ）が記憶媒体に格納されたプログラムコードを読み出し実行することによっても、完成されることは言うまでもない。

【００９２】

この場合、記憶媒体から読み出されたプログラムコード自体が前述した実施形態の機能を実現することになり、そのプログラムコードを記憶した記憶媒体は本発明を構成することになる。プログラムコードを供給するための記憶媒体としては、例えば、フロッピー（登録商標）ディスク、ハードディスク、光ディスク、光磁気ディスク、ＣＤ－ＲＯＭ、ＣＤ－Ｒ、磁気テープ、不揮発性のメモリカード、ＲＯＭを用いることができる。また、コンピュータが読み出したプログラムコードを実行することにより、前述した実施形態の機能が実現されるだけではなく、そのプログラムコードの指示に基づき、コンピュータ上で稼動しているＯＳなどが実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

【００９３】

さらに、記憶媒体から読み出されたプログラムコードが、コンピュータに挿入された機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに書き込まれた後、次のプログラムコードの指示に基づき、その拡張機能を拡張ボードや拡張ユニットに備わるＣＰＵなどが処理を行って実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

【図面の簡単な説明】

【００９４】

【図１】本発明に係るシステムの構成例を示す図である。

【図２】ＷＥＢサーバ１００のハードウェア構成を示す図である。

【図３】ＷＥＢサーバ１００のソフトウェアモジュール構成を示す図である。

【図４】ＷＥＢサーバ１００が行う認証処理のための認証設定画面の一例を示す図である。

【図５】ＷＥＢサーバ１００が認証設定画面の設定内容に従って認証方式を決定する認証方式自動決定処理を示すフローチャートである。

【図６】ＷＥＢサーバ１００が保持するアクセス設定情報データベース３０２を示す図である。

【図７】ＷＥＢサーバ１００がリクエストを受信した際に実行する処理を示すフローチャートである。

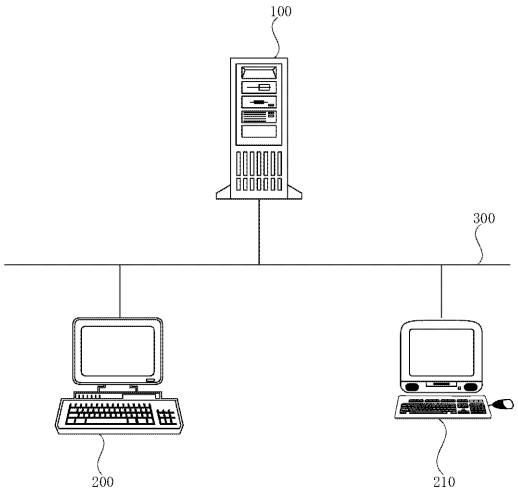
【図８】第２の認証方式自動決定処理で用いられるアクセス設定情報データベース３０２を示す図である。

【図９】ＷＥＢサーバ１００がリクエストを受信した際に認証方式を決定する認証方式自動決定処理を示すフローチャートである。

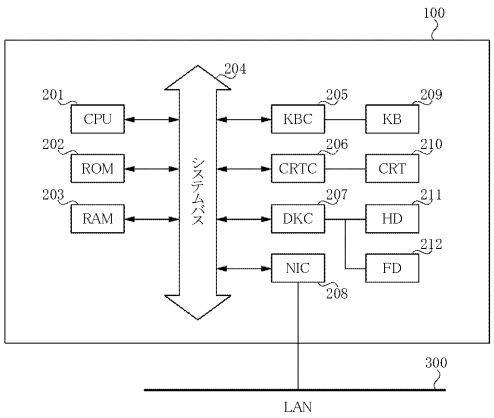
【図１０】Ｂａｓｉｃ認証方式に基づく認証処理を示すフローチャートである。

【図１１】Ｄｉｇｅｓｔ認証方式に基づく認証処理を示すフローチャートである。
【図１２】サーバが行う認証処理のための認証設定画面の一例を示す図である。
【符号の説明】
【００９５】
１００　ＷＥＢサーバ
２００　クライアントＰＣ
２１０　クライアントＰＣ
３００　ＬＡＮ
３０１　ファイルシステム
３０２　アクセス設定情報データベース
３０３　ＴＣＰ／ＩＰモジュール
３０４　ＳＳＬモジュール
３０５　ＨＴＴＰサーバモジュール
３０６　ＣＧＩモジュール
３０７　ＣＧＩモジュール
３０８　ＣＧＩモジュール

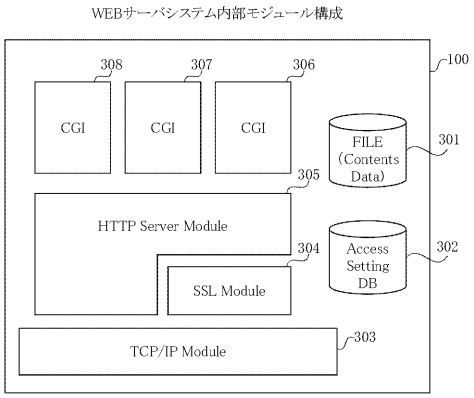
【図１】



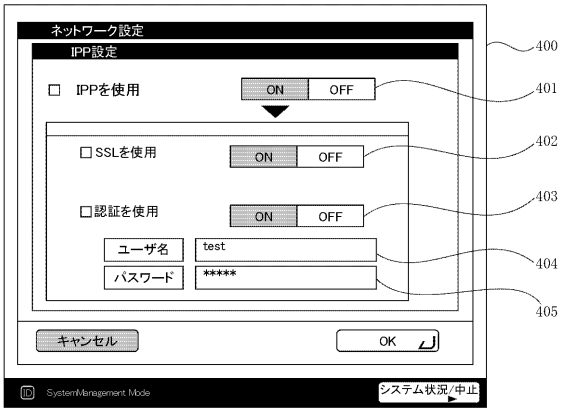
【図２】



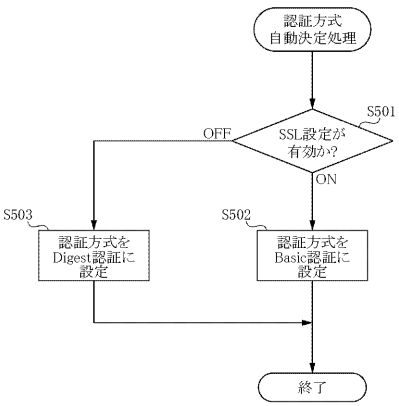
【図３】



【図４】



【図５】

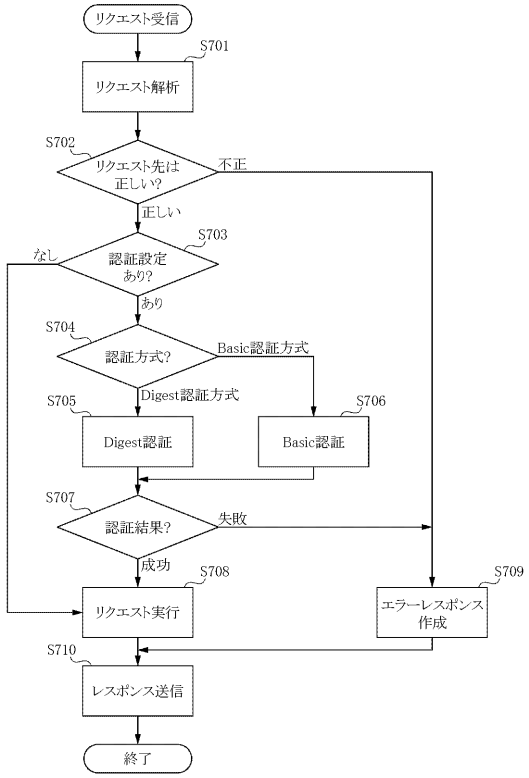


【図６】

600 601 602 603 604 605 606

URI Path	Protocol	Port	File/Service	Auth	Auth Mode	Authentication (user,pass)
/test.txt	HTTP	80	/FILE/test.txt	ON	Basic	test,himitu
/image.gif	HTTP	80	/FILE/Pic/image.gif	OFF	None	
/ipp	HTTPS	443	IppService()	ON	Digest	uchikawa,kimitu
/bmlinks	HTTP	443	BmlinksService()	ON	Digest	Kigyou,himitu
:	:	:	:	:	:	:

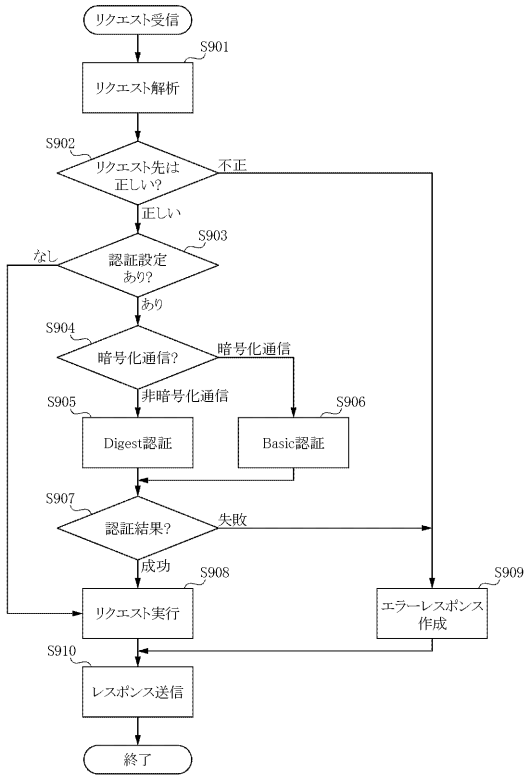
【図７】



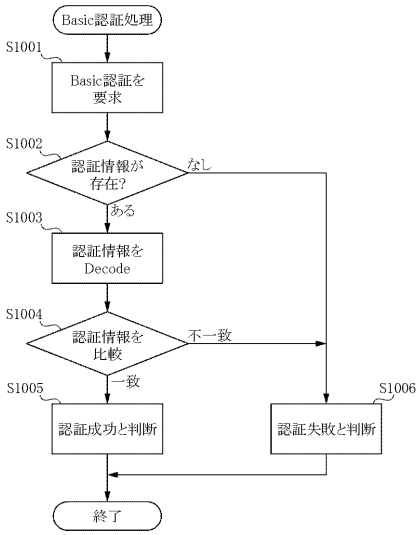
【図８】

600	601	602	603	604	606
IRL Path	Protocol	Port	File/Service	Auth	Authentication (user,pass)
/test.txt	HTTP	80	/FILE/test.txt	ON	test,himitu
/image.gif	HTTP	80	/FILE/Pic/image.gif	OFF	
/ipp	HTTPS	443	IppService()	ON	uchikawa,kimitu
/bmlinks	HTTP	443	BmlinksService()	ON	Kigyou,himitu
:	:	:	:	:	:

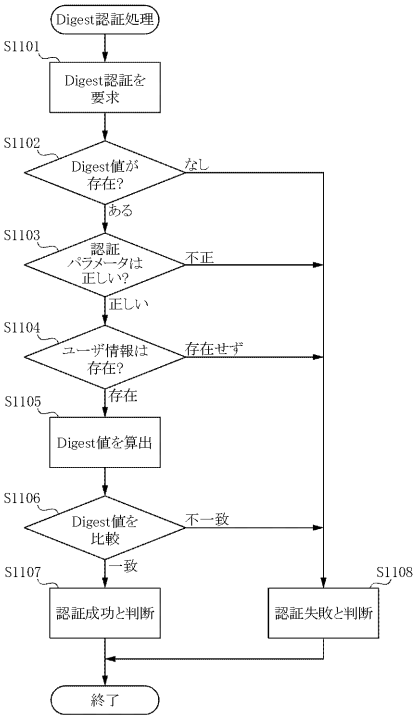
【図９】



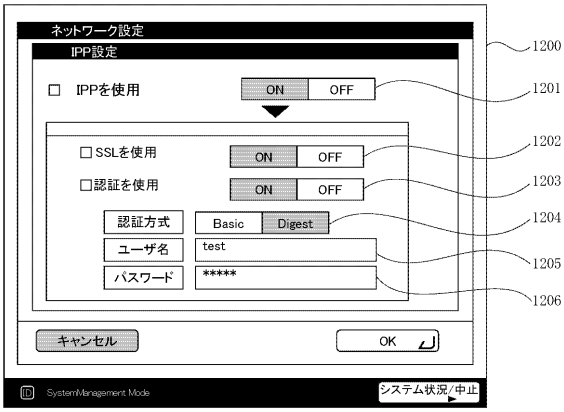
【図１０】



【図１１】


Digest認証処理
S1101
Digest認証を要求
S1102
Digest値が存在?
なし
ある
S1103
認証パラメータは正しい?
不正
正しい
S1104
ユーザ情報は存在?
存在せず
存在
S1105
Digest値を算出
S1106
Digest値を比較
不一致
一致
S1107
認証成功と判断
S1108
認証失敗と判断
終了

【図１２】


ネットワーク設定
IPP設定
1200
IPPを使用
ON
OFF
1201
SSLを使用
ON
OFF
1202
認証を使用
ON
OFF
1203
認証方式
Basic
Digest
1204
ユーザ名
test
1205
パスワード
*****
1206
キャンセル
OK
SystemManagement Mode
システム状況/中止

フロントページの続き

(56)参考文献 特開２００４－１２０４６２（ＪＰ，Ａ）
特開２００３－１５７２３４（ＪＰ，Ａ）
池田圭一，ネットワークまるわかり読本，ＡＳＣＩＩ 第２８巻 第１号，日本，株式会社アスキー，２００４年 １月 １日，第２８巻 第１号，p.56-59