(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2005-18421
(P2005-18421A)
(43)公開日　平成17年1月20日(2005.1.20)

(51)Int.Cl.[7]	F I		テーマコード（参考）
G06F 15/00	G06F 15/00	330D	5B085
H04L 9/32	G06F 15/00	330B	5J104
	H04L 9/00	675A	

審査請求 未請求　請求項の数 8　ＯＬ　（全 16 頁）

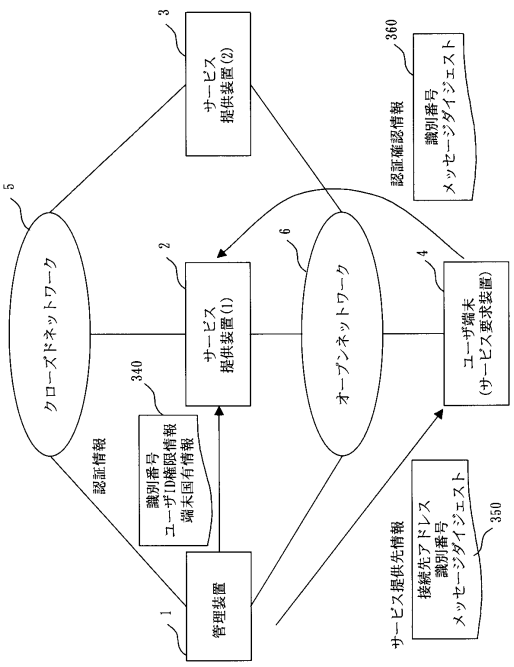
(21)出願番号　特願2003-182522(P2003-182522)
(22)出願日　平成15年6月26日(2003.6.26)

(71)出願人　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目２番３号
(74)代理人　100099461
弁理士　溝井　章司
(74)代理人　100111800
弁理士　竹内　三明
(74)代理人　100114878
弁理士　山地　博人
(72)発明者　石井　洋
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

Ｆターム(参考)　5B085 AE02 AE03 AE23 BA06 BC01 BG02
5J104 LA05 PA07 PA10

(54)【発明の名称】管理装置及びサービス提供装置及び通信システム

(57)【要約】
【課題】改竄や成りすまし等によるサービスの不正利用を防止する。
【解決手段】管理装置１にてユーザ端末４のログオン認証を行った後、ユーザ端末４にサービスを提供させるサービス提供装置を選択サービス提供装置として選択し、識別番号、ユーザＩＤ等を含み、ユーザ端末４を通知する認証情報３４０を選択サービス提供装置にのみ送信し、選択サービス提供装置の接続先アドレス、識別番号、認証情報３４０のメッセージダイジェストを含むサービス提供先情報３５０をユーザ端末４に送信し、ユーザ端末４ではサービス提供先情報３５０の接続先アドレスに基づき、選択サービス提供装置に識別番号とメッセージダイジェストとを含む認証確認情報３６０を送信し、選択サービス提供装置で認証情報３４０と認証確認情報３６０とを用いてユーザ端末４の認証処理を行い、正しく認証できた場合にユーザ端末４に対するサービス提供を開始する。
【選択図】　図１



【特許請求の範囲】
【請求項１】
サービスの提供を要求するサービス要求装置と、
サービスの提供に先立ち所定の認証情報を用いて正当なサービス要求元からのアクセスであるか否かについての認証処理を行ない、認証されたサービス要求元にのみサービスの提供を開始する複数のサービス提供装置とに接続され、
前記サービス要求装置と前記複数のサービス提供装置とを管理する管理装置であって、
前記サービス要求装置に対して所定の認証処理を行う認証処理部と、
前記認証処理部により前記サービス要求装置が認証された場合に、前記サービス要求装置に認められている権限と前記サービス要求装置が要求するサービス内容とに基づき、前記複数のサービス提供装置の中から前記サービス要求装置にサービスを提供させるサービス提供装置を選択サービス提供装置として選択するサービス提供装置選択部と、
前記認証処理部により前記サービス要求装置が認証された場合に、前記サービス要求装置が正当なサービス要求元であることを通知する第１の認証情報と、前記第１の認証情報と照合させた際に前記第１の認証情報との相関が得られることで正当なサービス要求元からのアクセスであることを認証できる第２の認証情報と、前記サービス要求装置に対して前記第２の認証情報を前記選択サービス提供装置に送信するよう指示する送信先指示情報とを生成する認証情報生成部と、
前記第１の認証情報を、前記複数のサービス提供装置のうち前記選択サービス提供装置にのみ送信するサービス提供装置用通信部と、
前記第２の認証情報と前記送信先指示情報とを、前記サービス要求装置に送信するサービス要求装置用通信部とを有することを特徴とする管理装置。
【請求項２】
前記認証情報生成部は、
前記第２の認証情報として、前記第１の認証情報のメッセージダイジェストを生成することを特徴とする請求項１に記載の管理装置。
【請求項３】
前記認証情報生成部は、
前記認証処理部によりサービス要求装置が認証される度に、毎回、異なる識別子を生成するとともに、相互に対応関係にある第１の認証情報及び第２の認証情報に共通の識別子を用いることを特徴とする請求項１に記載の管理装置。
【請求項４】
前記認証情報生成部は、
前記第１の認証情報に先行して前記第２の認証情報と前記送信先指示情報とを生成し、
前記第２の認証情報と前記送信先指示情報とが前記サービス要求装置用通信部から前記サービス要求装置に送信され、前記送信先指示情報により前記第２の認証情報が前記サービス要求装置から前記選択サービス提供装置に送信され、前記選択サービス提供装置が前記第２の認証情報を受信した後、前記選択サービス提供装置からの依頼に基づいて、前記第１の認証情報を生成することを特徴とする請求項１に記載の管理装置。
【請求項５】
所定の管理装置に接続され、
サービス要求元が正当であるか否かについて、前記管理装置から第１の認証情報を受信し、サービス要求元から第２の認証情報を受信し、前記第１の認証情報と前記第２の認証情報とを用いてサービス要求元に対する認証処理を行なうサービス提供装置であって、
前記第１の認証情報を受信した際に、前記第１の認証情報の受信時刻を記憶し、
前記第２の認証情報を受信した際に、前記第１の認証情報の受信時刻と前記第２の認証情報の受信時刻との時刻差を算出し、算出した時刻差が一定以上である場合に、前記第２の認証情報を送信したサービス要求元に対するサービス提供を行なわないことを特徴とするサービス提供装置。
【請求項６】

所定の管理装置に接続され、
サービス要求元が正当であるか否かについて、前記管理装置から第１の認証情報を受信し、サービス要求元から第２の認証情報を受信し、前記第１の認証情報と前記第２の認証情報とを用いてサービス要求元に対する認証処理を行なうサービス提供装置であって、
前記第１の認証情報を受信した際に、サービス要求元に対してサービスが未提供であることを示すサービス提供フラグを設定し、
前記第２の認証情報を受信した際に、前記サービス提供フラグの参照を行なうとともに、前記第１の認証情報と前記第２の認証情報の照合を行い、
前記サービス提供フラグがサービス要求元に対してサービスが未提供であることを示し、
前記第１の認証情報と前記第２の認証情報の照合により前記第１の認証情報と前記第２の認証情報との間に相関が得られた場合に、前記第２の認証情報を送信したサービス要求元に対してサービスの提供を開始するとともに、前記サービス提供フラグをサービス提供済に変更することを特徴とするサービス提供装置。

【請求項７】
前記サービス提供装置は、
前記サービス提供フラグを参照した結果、前記サービス提供フラグがサービス提供済であることを示している場合に、前記第２の認証情報を送信したサービス要求元に対するサービス提供を行なわず、前記第２の認証情報を送信したサービス要求元以外のサービス要求元に対してサービスが提供されている場合に、当該サービス要求元に対するサービスの提供を中止することを特徴とする請求項６に記載のサービス提供装置。

【請求項８】
サービスの提供に先立ち所定の認証情報を用いて正当なサービス要求元からのアクセスであるか否かについての認証処理を行ない、認証されたサービス要求元にのみサービスの提供を開始する複数のサービス提供装置と、
サービスの提供を要求するサービス要求装置と前記複数のサービス提供装置とに接続され、前記サービス要求装置と前記複数のサービス提供装置とを管理する管理装置と、
を有する通信システムであって、
前記管理装置は、
前記サービス要求装置に対して所定の認証処理を行い、
前記認証処理により前記サービス要求装置が認証された場合に、前記サービス要求装置に認められている権限と前記サービス要求装置が要求するサービス内容とに基づき、前記複数のサービス提供装置の中から前記サービス要求装置にサービスを提供させるサービス提供装置を選択サービス提供装置として選択し、
前記認証処理により前記サービス要求装置が認証された場合に、前記サービス要求装置が正当なサービス要求元であることを通知する第１の認証情報と、前記第１の認証情報と照合させた際に前記第１の認証情報との相関が得られることで正当なサービス要求元からのアクセスであることを認証できる第２の認証情報と、前記サービス要求装置に対して前記第２の認証情報を前記選択サービス提供装置に送信するよう指示する送信先指示情報とを生成し、
前記第１の認証情報を、前記複数のサービス提供装置のうち前記選択サービス提供装置にのみ送信し、
前記第２の認証情報と前記送信先指示情報とを前記サービス要求装置に送信し、前記送信先指示情報により前記第２の認証情報を前記サービス要求装置から前記選択サービス提供装置に送信させ、
前記複数のサービス提供装置のそれぞれは、
前記管理装置により前記選択サービス提供装置として選択されている場合に、
前記第１の認証情報と前記第２の認証情報とを受信し、
前記第２の認証情報の送信元が前記第１の認証情報により通知された前記サービス要求装置と一致するか否かを判断するとともに、前記第１の認証情報と前記第２の認証情報の照合を行い、

前記第２の認証情報の送信元が前記サービス要求装置と一致し、前記第１の認証情報と前記第２の認証情報との間に相関が得られた場合に、前記第２の認証情報の送信元である前記サービス要求装置を正当なサービス要求元と認証し、前記サービス要求装置に対してサービスの提供を開始することを特徴とする通信システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、改竄や成りすまし等による情報サービスの不正利用を防止するための認証技術に関する。

【０００２】

【従来の技術】

従来の技術として、例えば、特開平１１－１２０１４１では、ユーザ端末についての認証情報を認証システムからユーザ端末を経由してサービス提供システムに送信し、その認証情報の正当性のみが評価され正しければサービスが提供される。

このような、認証情報をユーザ端末経由で送信する手段を用いた方法だと、認証情報は暗号化されていたとしても盗用によって不正利用される可能性がある。また、暗号は充分な時間を用いれば解読される可能性があり、改竄によっても不正利用の可能性がある。

【０００３】

更に、特開２００１－３３１４４９では、ユーザ端末についての認証情報が認証システムから全てのサービス提供システムに送信され、更に認証システムからはサービス提供システムにおける突き合わせのための認証情報がユーザ端末に送信され、この突き合わせのための認証情報がユーザ端末からユーザ端末がサービスの利用を希望する特定のサービス提供システムに送信され、当該特定のサービス提供システムにおいてこれらの認証情報を突き合わせることによって正しければサービスが提供される。

このような方法だと、成りすましによる不正利用に対して、該当ユーザ端末がシステムを利用しているときに限り不正利用される可能性がある。つまり、全てのサービス提供システムに認証情報が送信されるため、正当なユーザに成りすまして不正利用を図ろうとする第三者は、全てのサービス提供システムに対して突合せのための認証情報を送信すれば、全てのサービス提供システムにおいて不正利用を行うことが可能である。

【０００４】

【特許文献１】

特開平１１－１２０１４１号公報

【特許文献２】

特開２００１－３３１４４９号公報

【０００５】

【発明が解決しようとする課題】

本発明は、このような問題点を解決することを目的の一つとしており、改竄や成りすまし等によるサービスの不正利用を防止することを目的の一つとする。

【０００６】

【課題を解決するための手段】

本発明に係る管理装置は、

サービスの提供を要求するサービス要求装置と、

サービスの提供に先立ち所定の認証情報を用いて正当なサービス要求元からのアクセスであるか否かについての認証処理を行ない、認証されたサービス要求元にのみサービスの提供を開始する複数のサービス提供装置とに接続され、

前記サービス要求装置と前記複数のサービス提供装置とを管理する管理装置であって、

前記サービス要求装置に対して所定の認証処理を行う認証処理部と、

前記認証処理部により前記サービス要求装置が認証された場合に、前記サービス要求装置に認められている権限と前記サービス要求装置が要求するサービス内容とに基づき、前記複数のサービス提供装置の中から前記サービス要求装置にサービスを提供させるサービス

提供装置を選択サービス提供装置として選択するサービス提供装置選択部と、
前記認証処理部により前記サービス要求装置が認証された場合に、前記サービス要求装置が正当なサービス要求元であることを通知する第１の認証情報と、前記第１の認証情報と照合させた際に前記第１の認証情報との相関が得られることで正当なサービス要求元からのアクセスであることを認証できる第２の認証情報と、前記サービス要求装置に対して前記第２の認証情報を前記選択サービス提供装置に送信するよう指示する送信先指示情報とを生成する認証情報生成部と、
前記第１の認証情報を、前記複数のサービス提供装置のうち前記選択サービス提供装置にのみ送信するサービス提供装置用通信部と、
前記第２の認証情報と前記送信先指示情報とを、前記サービス要求装置に送信するサービス要求装置用通信部とを有することを特徴とする。

【０００７】

【発明の実施の形態】

実施の形態１.

図１は、本実施の形態に係る通信システムの全体構成例を示す図である。

管理装置１は、クローズドネットワーク（例えば、プライベートＬＡＮ、専用線ネットワーク、ＤＭＺ（ＤｅＭｉｌｉｔａｒｉｚｅｄ　Ｚｏｎｅ）など）５を介してサービス提供装置（１）２、サービス提供装置（２）３と接続され、オープンネットワーク（例えば、オープンＬＡＮ、企業内ＬＡＮ、インターネットなど）６を介してユーザ端末４と接続されている。

サービス提供装置（１）２及びサービス提供装置（２）３は、例えば電子決済等の所定の情報サービスを提供するサーバである。サービス提供装置（１）２及びサービス提供装置（２）３は、サービスの提供に先立ち所定の認証情報を用いて正当なサービス要求元からのアクセスであるか否かについての認証処理を行ない、認証されたサービス要求元にのみサービスの提供を開始する。

なお、図１では、説明の便宜のため２台のサービス提供装置を示しているが、２台以上のサービス提供装置が配置されていてもよい。

ユーザ端末４は、サービス提供装置（１）２又はサービス提供装置（２）３によるサービスの提供を要求する装置であり、サービス要求装置の例に相当する。

【０００８】

次に、図１を参照して、本実施の形態に係る通信システムの動作を概説する。

本実施の形態に係る通信システムでは、ユーザ端末４は、サービス提供装置（１）２又はサービス提供装置（２）３からのサービスを受ける場合は、まず、管理装置１にアクセスしなければならず、直接サービス提供装置（１）２又はサービス提供装置（２）３にアクセスすることはできない。

ユーザ端末４からのアクセスがあった場合は、管理装置１はユーザ端末４に対するログオン認証を行なった後、ユーザ端末４に認められた権限及びユーザ端末４の要求するサービス内容に基づき、ユーザ端末４にサービスを提供させるサービス提供装置を選択する。ここでは、サービス提供装置（１）２を選択したとする。

次に、管理装置１は、サービス提供装置（１）２にユーザ端末４を通知するための認証情報３４０を生成する。この認証情報は、例えば、識別番号、ユーザＩＤ、権限情報、端末固有情報（例えば、ユーザ端末４のＩＰアドレス）からなる。そして、生成した認証情報３４０をクローズドネットワーク５を介してサービス提供装置（１）２にのみを送信する。

また、ユーザ端末４に対してサービス提供先情報３５０を送信する。このサービス提供先情報３５０は、接続先アドレス（サービス提供装置（１）２のアドレス）、認証情報３４０に含ませたものと同じ識別番号、認証情報３４０のメッセージダイジェスト（認証情報３４０を一方向関数によりデータ変換した情報）により構成される。

【０００９】

次に、ユーザ端末４では、サービス提供先情報３５０に含まれた識別番号とメッセージダ

イジェストとからなる認証確認情報３６０を、サービス提供先情報３５０に含まれた接続先アドレスにより、サービス提供装置（１）２に送信する。

【００１０】

次に、サービス提供装置（１）２では、識別番号をキーにして、相互に対応関係にある認証情報３４０と認証確認情報３６０を特定し、認証情報３４０に含まれた端末固有情報（ユーザ端末４のＩＰアドレス）と認証確認情報３６０の送信の際に認証確認情報３６０に付加された端末固有情報（ユーザ端末４のＩＰアドレス）が一致するかを判断する。両者が一致する場合は、認証情報３４０と認証確認情報３６０に含まれたメッセージダイジェストとの間に相関があるかどうかの照合を行なう。具体的には、認証情報３４０のメッセージダイジェストを生成し、生成したメッセージダイジェストと認証確認情報３６０に含まれたメッセージダイジェストとが一致するかの検証を行なう。両者が一致している場合には、情報認証情報３４０と認証確認情報３６０に含まれたメッセージダイジェストとの間に相関があり、これにより、サービス提供装置（１）２は、認証確認情報３６０の送信元であるユーザ端末４を正当なサービス要求元と認証し、ユーザ端末４に対するサービスの提供を開始する。

【００１１】

なお、管理装置１からサービス提供装置（１）２に送信される認証情報３４０は、ユーザ端末４が正当なサービス要求元であることを通知する情報であり、第１の認証情報の例に相当する。

また、管理装置１からユーザ端末４に送信され、ユーザ端末４からサービス提供装置（１）２に送信されるメッセージダイジェストは、認証情報（第１の認証情報）と照合させた際に認証情報（第１の認証情報）との相関が得られ、これにより正当なサービス要求元からのアクセスであることを認証できる情報であり、第２の認証情報の例に相当する。

また、管理装置１からユーザ端末４に送信される接続先アドレスは、ユーザ端末４に対してメッセージダイジェスト（第２の認証情報）の送信先を指示する情報であり、送信先指示情報の例に相当する。

【００１２】

次に、図２を参照して、本実施の形態に係る管理装置１の構成例について説明する。

クローズドネットワーク用通信部１０１は、クローズドネットワーク５を介してサービス提供装置（１）２又はサービス提供装置（２）３との間でデータを送受信する。クローズドネットワーク用通信部１０１は、サービス提供装置用通信部の例に相当する。

オープンネットワーク用通信部１０２は、オープンネットワーク６を介してユーザ端末４との間でデータを送受信する。オープンネットワーク用通信部１０２はサービス要求装置用通信部の例に相当する。

認証処理部１０３は、ユーザ端末４からのアクセスがあった場合にユーザ端末４に対するログオン認証を行なう。

ユーザ管理情報記憶部１０４は、ユーザ端末４に関する情報を記憶しており、例えば、ユーザＩＤ、パスワード、権限情報を記憶している。

サービス管理情報記憶部１０５は、サービス提供装置に関する情報を記憶しており、例えば、サービス名称、サービス提供アドレス、権限情報を記憶している。

サービス提供装置選択部１０６は、ユーザ管理情報記憶部１０４及びサービス管理情報記憶部１０５の情報を参照しながら、ユーザ端末４に認められた権限及びユーザ端末４の要求するサービス内容に基づき、ユーザ端末４にサービスを提供させるサービス提供装置を選択する。

認証情報生成部１０７は、ユーザ管理情報記憶部１０４及びサービス管理情報記憶部１０５の情報等を参照しながら、認証情報３４０及びサービス提供先情報３５０を生成する。

【００１３】

なお、管理装置１は、図示していないが、例えばマイクロプロセッサ等のＣＰＵ、半導体メモリ等や磁気ディスク等の記録手段、及び通信手段を有する計算機により実現することができる。記録手段には、管理装置１に含まれる各構成要素の機能を実現するプログラム

が記録されており、ＣＰＵがこれらのプログラムを読み込むことにより管理装置１の動作を制御し、各構成要素の機能を実現することができる。

【００１４】

次に、図３を参照して、本実施の形態に係るサービス提供装置の構成例について説明する。

クローズドネットワーク用通信部２０１は、クローズドネットワーク５を介して管理装置１との間でデータを送受信する。

オープンネットワーク用通信部２０２は、オープンネットワーク６を介してユーザ端末４との間でデータを送受信する。

認証処理部２０３は、ユーザ端末４に対する認証処理を行なう。具体的には、前述したように、認証情報３４０の端末固有情報と認証確認情報３６０の端末固有情報が一致するか否かの判断や、情報認証情報３４０のメッセージダイジェストと認証確認情報３６０に含まれたメッセージダイジェストとが一致するか否かの判断を行なう。

認証管理情報記憶部２０４は、管理装置１から認証情報３４０を受信した後、ユーザ端末４から認証確認情報３６０を受信するまでの間、管理装置１からの認証情報３４０の内容を記憶しておく。

サービス提供部２０５は、認証処理部２０３により認証されたサービス要求元に対して所定の情報サービスの提供を行う。

【００１５】

なお、サービス提供装置は、図示していないが、例えばマイクロプロセッサ等のＣＰＵ、半導体メモリ等や磁気ディスク等の記録手段、及び通信手段を有する計算機により実現することができる。記録手段には、サービス提供装置に含まれる各構成要素の機能を実現するプログラムが記録されており、ＣＰＵがこれらのプログラムを読み込むことにより管理装置１の動作を制御し、各構成要素の機能を実現することができる。

【００１６】

次に、図４を参照しながら本実施の形態に係る通信システムの動作を説明する。

まず、ステップＳ１０１において、ユーザ端末４はサービス利用の前段階として管理装置１に接続を行う。

次に、ステップＳ１０２において、管理装置１では、ユーザ端末４の接続に対して、認証処理部１０３がオープンネットワーク用通信部１０２より認証画面を送信する。

次に、ステップＳ１０３において、ユーザ端末４は管理装置１にログオン情報３１０（ユーザＩＤ、パスワード）を送信する。

【００１７】

次に、ステップＳ１０４において、管理装置１では、認証処理部１０３がユーザ端末４から受信したログオン情報３１０と、ユーザ管理情報記憶部１０４に記憶されているユーザ端末４のユーザ管理情報とを照合してユーザ端末４に対するログオン認証を行う。認証が正しければ、認証処理部１０３はユーザ端末４のユーザ管理情報より権限情報を抽出し、抽出した権限情報をサービス提供装置選択部１０６に渡す。サービス提供装置選択部１０６では、この権限情報を用いてサービス管理情報記憶部１０５に記憶されているサービス管理情報よりユーザ端末４が利用可能なサービス名称を抽出しメニュー情報３２０を生成し、オープンネットワーク用通信部１０２から送信する。認証処理部１０３によるログオン認証が正しくなければ、認証処理部１０３は、再度、認証画面を送信する。正しいログオン情報３１０が送信されるまではサービス提供は行われない。

【００１８】

次に、ステップＳ１０５において、ユーザ端末４は、メニュー情報３２０からサービスを選択し、管理装置１に対してサービス要求３３０を送信する。

管理装置１では、ユーザ端末４からのサービス要求３３０を受信すると、サービス提供装置選択部１０６がサービス要求３３０に示されたサービス名称に基づきサービス管理情報記憶部１０５に記憶されているサービス管理情報からサービス提供先アドレスを指定し、ユーザ端末４にサービスを提供させるサービス提供装置を選択する。この選択されたサー

ビス提供装置を選択サービス提供装置という。

【００１９】

サービス提供装置選択部１０６により選択サービス提供装置が選択された後、認証情報生成部１０７が識別番号（識別子）を生成するとともに、ユーザ管理情報記憶部１０４に記憶されているユーザＩＤ、権限情報を抽出し、また、ステップＳ１０５のサービス要求３３０のパケットからユーザ端末４を特定する端末固有情報（例えばユーザ端末４のＩＰアドレス）を抽出し、これら識別番号、ユーザＩＤ、権限情報、端末固有情報を含む認証情報３４０を生成し、クローズドネットワーク用通信部１０１から選択サービス提供装置に送信する（Ｓ１０６）。なお、認証情報生成部１０７では、認証処理部１０３によりユーザ端末が認証される度に、毎回、異なる値の識別番号をランダムに生成する。

一方、選択サービス提供装置では、クローズドネットワーク用通信部２０１が認証情報３４０を受信し、認証処理部２０３が認証情報３４０に含まれた識別番号をキーにユーザＩＤと、権限情報と、端末固有情報とを認証管理情報として認証管理情報記憶部２０４に格納し、この時点で初めて当該ユーザ端末に対するサービス提供準備が整う。

【００２０】

更に、管理装置１では、認証情報生成部１０７が、サービス提供装置選択部１０６の指定に従ってサービス管理情報記憶部１０５に記憶されているサービス管理情報から選択サービス提供装置の接続先アドレス（サービス提供アドレス）を抽出するとともに、ステップＳ１０６で選択サービス提供装置に送信した認証情報３４０のメッセージダイジェストを生成し、接続先アドレスと、ステップＳ１０６で選択サービス提供装置に送信した認証情報３４０と同一の識別番号と、メッセージダイジェストとを含むサービス提供先情報３５０を生成し、オープンネットワーク用通信部２０２からユーザ端末４に送信する（Ｓ１０７）。

【００２１】

次に、ステップＳ１０８において、ユーザ端末４は管理装置１から受信したサービス提供先情報３５０によって、サービス提供装置の接続先アドレスに自動的に接続を行い、サービス提供先情報３５０に含まれていた識別番号とメッセージダイジェストとを認証確認情報３６０として送信する。

【００２２】

選択サービス提供装置ではユーザ端末４から受信した認証確認情報３６０の識別番号を元に、認証処理部２０３が、認証管理情報記憶部２０４から当該認証確認情報３６０と対応関係にある認証情報３４０を検索し、検索した認証情報３４０から端末固有情報を抽出し、認証確認情報３６０のパケットに含まれている端末固有情報と抽出した端末固有情報とが一致するか否かの検証を行なう。

更に、認証処理部２０３は、認証管理情報記憶部２０４から、当該認証確認情報３６０と対応関係にある認証情報３４０のユーザＩＤと権限情報とを抽出し、識別番号、ユーザＩＤ、権限情報、端末固有情報のメッセージダイジェスト、すなわち、認証情報３４０のメッセージダイジェストを生成する。その後、認証処理部２０３は、ユーザ端末４から受信した認証確認情報３６０のメッセージダイジェストと、生成した認証情報３４０のメッセージダイジェストとが一致するか否かの検証を行う。

【００２３】

以上の検証が全て正しければ、認証処理部２０３は認証管理情報より当該ユーザ端末４についてのレコード（認証情報３４０）を削除し、サービス提供部２０５がユーザ端末４に対して権限情報に従ってサービスを提供する（Ｓ１０９）。

一方、以上の検証においていずれか一つでも条件に合致しない場合は、ユーザ端末４に対するサービスの提供を行わない。

【００２４】

このように、本実施の形態に係る通信システムでは、ステップＳ１０５でユーザ端末４からサービス要求３３０があってはじめてステップＳ１０６で選択サービス提供装置に対して認証情報３４０を送信し、これにより選択サービス提供装置においてユーザ端末４との

接続準備が整い、ステップＳ１０７で管理装置１がユーザ端末４にサービス提供先情報３５０を送信し、ステップＳ１０８でユーザ端末４が選択サービス提供装置に認証確認情報３６０を送信することで、選択サービス提供装置でメッセージダイジェストの検証が行われ正しければサービスが提供される。
つまり、ユーザ端末４からサービス要求３３０が送信された直後に、選択サービス提供装置に認証情報３４０が送信され、同時にユーザ端末４に選択サービス提供装置の接続先アドレスなどが送信され自動的に接続先アドレスに接続されるので、選択サービス提供装置は受信した認証情報に示されたユーザ端末が接続してくるわずかな時間だけ認証の口を開けて待てばよく（逆にいうと、不正利用のチャンスはこのわずかな時間しかない上、正しい認証確認情報を送信する必要がある）、不正アクセスされる可能性を極めて少なくする効果がある。換言すると、選択サービス提供装置は認証情報を受信してから以降十数秒以内に該当ユーザ端末からの接続がくることを前提に接続を待機し、接続がなければ該当の認証情報を無効とすることで成りすましによる不正利用を防止することができる。
【００２５】
また、本実施の形態に係る管理装置は、複数のサービス提供装置のうち選択サービス提供装置にのみ認証情報を送信し、また、ユーザ端末に対して認証確認情報を選択サービス提供装置に送信するよう指示するため、他のサービス提供装置において認証情報と認証確認情報の突き合わせが行われるという事態が発生せず、このため、成りすまし等による不正利用を有効に防止することができる。
【００２６】
また、本実施の形態に係る管理装置は、ユーザ端末が認証される度に、毎回、異なる値の識別番号（識別子）をランダムに生成し、この識別番号を付加して認証情報及びサービス提供先情報を生成するため、すべての認証情報及びサービス提供先情報（認証確認情報）の識別番号が異なり、成りすまし等に対する有効な対策となり、成りすまし等による不正利用を有効に防止することができる。
【００２７】
実施の形態２．
以上の実施の形態１では、選択サービス提供装置は、管理装置から認証情報を受信した後に、ユーザ端末から認証確認情報を受信することとなっていったが、本実施の形態では、選択サービス提供装置がユーザ端末からの認証確認情報を管理装置からの認証情報よりも先に受信する場合について説明する。
【００２８】
図５は、本実施の形態に係る管理装置１の構成例を示す図である。
図５において、１０１～１０７は図２に示したものと同様であるため、説明を省略する。
認証管理情報記憶部１０８は、ユーザ端末へのサービス提供先情報を生成した後、選択サービス提供装置への認証情報を生成するまでの間、サービス提供先情報の生成に用いた識別番号、ユーザＩＤ、権限情報、端末固有情報（ユーザ端末のＩＰアドレス等）を認証管理情報として記憶する。
また、本実施の形態においても、サービス提供装置の構成は図３と同様である。但し、実施の形態１では、認証管理情報記憶部２０４は管理装置からの認証情報の内容を記憶していたが、本実施の形態では認証確認情報の内容及び認証確認情報のパケットに含まれている端末固有情報を記憶する。
【００２９】
次に、図６を参照しながら本実施の形態に係る通信システムの動作を説明する。
ステップＳ２０１～Ｓ２０５は、実施の形態１のステップＳ１０１～Ｓ１０５と同様である。
つまり、ユーザ端末４からの接続（Ｓ２０１）に対して管理装置１の認証処理部１０３が認証画面を送信し（Ｓ２０２）、応答としてユーザ端末４がログオン情報３１０を送信し（Ｓ２０３）、認証処理部１０３がユーザ端末４に対するログオン認証を行なう。そして、ユーザ端末４が認証された場合には、サービス提供装置選択部１０６がメニュー情報を

ユーザ端末４に送信し（Ｓ２０４）、応答としてユーザ端末４サービス要求３３０を送信し（Ｓ２０５）、サービス提供装置選択部１０６が選択サービス提供装置を選択する。

【００３０】

サービス提供装置選択部１０６により選択サービス提供装置が選択されると、管理装置１では、認証情報生成部１０７がサービス提供先情報３５０を生成する。具体的には、認証情報生成部１０７が識別番号（識別子）を生成するとともに、サービス提供装置選択部１０６の指定に従ってサービス管理情報記憶部１０５に記憶されているサービス管理情報から選択サービス提供装置の接続先アドレス（サービス提供アドレス）を抽出し、更に、ユーザ管理情報記憶部１０４に記憶されているユーザＩＤ、権限情報を抽出し、また、ステップＳ２０５のサービス要求のパケットからユーザ端末４を特定する端末固有情報（例えばユーザ端末４のＩＰアドレス）を抽出し、これら識別番号、ユーザＩＤ、権限情報、端末固有情報のメッセージダイジェストを生成し、接続先アドレスと、識別番号と、メッセージダイジェストとを含むサービス提供先情報３５０を生成する。このとき、認証情報生成部１０７は、並行して、サービス提供先情報３５０の生成に用いた識別番号、ユーザＩＤ、権限情報、端末固有情報を認証管理情報として認証管理情報記憶部１０８に格納する。

【００３１】

このようにして認証情報生成部１０７によりサービス提供先情報３５０が生成されると、オープンネットワーク用通信部１０２からユーザ端末４に送信される（Ｓ２０６）。

【００３２】

次に、ステップＳ２０７において、ユーザ端末４は管理装置１から受信したサービス提供先情報３５０によって、選択サービス提供装置の接続先アドレスに自動的に接続を行い、サービス提供先情報３５０に含まれていた識別番号とメッセージダイジェストとを認証確認情報３６０として送信する。

【００３３】

選択サービス提供装置では、オープンネットワーク用通信部２０２がユーザ端末から送信された認証確認情報を受信する。

そして、認証処理部２０３が認証確認情報に含まれているメッセージダイジェスト及び認証確認情報のパケットに含まれていた端末固有情報（ユーザ端末のＩＰアドレス等）を識別番号をキーにして認証管理情報記憶部２０４に格納し、更に、認証確認情報から識別番号を抽出し、当該識別番号を含み管理装置１に対して認証情報の送信を依頼する認証情報要求３７０を生成し、クローズドネットワーク用通信部２０１から管理装置１に送信する（Ｓ２０８）。

【００３４】

管理装置１では、クローズドネットワーク用通信部１０１が選択サービス提供装置からの認証情報要求３７０を受信する。

そして、認証情報生成部１０７が認証情報要求３７０から識別番号を抽出し、当該識別番号に基づき認証管理情報からユーザＩＤ、権限情報、端末固有情報を抽出し、識別番号、ユーザＩＤ、権限情報、端末固有情報を含む認証情報３４０を生成し、クローズドネットワーク用通信部２０１から選択サービス提供装置に送信する（Ｓ２０９）。

また、認証情報生成部１０７は、認証情報３４０の送信後、認証管理情報から当該ユーザ端末についてのレコード（識別番号、ユーザＩＤ、権限情報、端末固有情報）を削除する。

【００３５】

選択サービス提供装置では、クローズドネットワーク用通信部２０１が管理装置１からの認証情報を受信し、認証処理部２０３が、認証管理情報として記憶されている認証確認情報の識別番号を元に、認証確認情報のパケットに含まれていた端末固有番号を認証管理情報から抽出し、また、管理装置１から受信した認証情報から端末固有情報を抽出し、これら２つの端末固有情報が、一致するか否かを検証する。

更に、認証処理部２０３は、認証情報３４０より識別番号と、ユーザＩＤと、権限情報と

、端末固有情報とを抽出し、識別番号、ユーザＩＤ、権限情報、端末固有情報のメッセージダイジェスト、すなわち、認証情報３４０のメッセージダイジェストを生成する。その後、認証処理部２０３は、認証管理情報として記憶されている認証確認情報３６０のメッセージダイジェストと、生成した認証情報３４０のメッセージダイジェストとが一致するか否かの検証を行う。

【００３６】

以上の検証が全て正しければ、認証処理部２０３は認証管理情報より当該ユーザ端末４についてのレコード（認証確認情報３６０）を削除し、サービス提供部２０５がユーザ端末４に対して権限情報に従ってサービスを提供する（Ｓ２０９）。

一方、以上の検証においていずれか一つでも条件に合致しない場合は、ユーザ端末４に対するサービスの提供を行わない。

【００３７】

このように、本実施の形態に係る通信システムでは、ユーザ端末４からサービス要求３３０が送信された際に管理装置１からユーザ端末４に対してサービス提供先情報３５０を送信し、ユーザ端末４が選択サービス提供装置に対して認証確認情報３６０を送信し、これにより、選択サービス提供装置は管理装置１に対して認証情報要求３７０を送信し、この結果、管理装置１から選択サービス提供装置に認証情報が送信される。

つまり、管理装置がユーザ端末へのサービス提供先情報を生成してから選択サービス提供装置が認証情報を受信するまでのわずかな時間しか不正利用のチャンスはなく、また、正しい認証確認情報を送信する必要があるため、不正アクセスされる可能性を極めて少なくすることが可能となる。

【００３８】

実施の形態３．

本実施の形態では、実施の形態１で示した手法を用いた場合に、選択サービス提供装置において認証情報の受信時刻と認証確認情報の受信時刻とを管理する場合について説明する。

【００３９】

本実施の形態に係る管理装置１の構成例は図２に示すものと同様である。

また、サービス提供装置の構成例も図３に示すものと同様であるが、本実施の形態では、認証処理部２０３は管理装置１からの認証情報３４０の受信の際に認証情報３４０の受信時刻を認証管理情報記憶部２０４に記憶させ、また、ユーザ端末４からの認証確認情報３６０の受信の際に認証情報３４０の受信時刻を参照してユーザ端末４に対する認証処理を行う。

【００４０】

次に、図７を参照して本実施の形態に係る通信システムの動作を説明する。

ステップＳ３０１～Ｓ３０６は、図１のステップＳ１０１～Ｓ１０６と場合と同様である。このため、ステップＳ３０６以降の動作を説明する。

選択サービス提供装置では、クローズドネットワーク用通信部２０１が管理装置１からの認証情報３４０を受信し、認証処理部２０３が、認証情報３４０の受信の際の時刻を取得して受信時刻とし、認証情報３４０に含まれた識別番号をキーにユーザＩＤと、権限情報と、端末固有情報と、更に、認証情報３４０の受信時刻とを認証管理情報として認証管理情報記憶部２０４に格納する。この時点で初めて当該ユーザ端末に対するサービス提供準備が整う。

【００４１】

また、管理装置１では、実施の形態１と同様に、サービス提供先情報３５０を生成し、オープンネットワーク用通信部２０２からユーザ端末４に送信し（Ｓ３０７）、ユーザ端末４では、実施の形態１と同様に、認証確認情報３６０を選択サービス提供装置に送信する（Ｓ３０８）。

【００４２】

選択サービス提供装置ではユーザ端末４から受信した認証確認情報３６０の識別番号を元

に、認証処理部２０３が、認証管理情報記憶部２０４に格納されている認証管理情報より端末固有情報を抽出し、認証確認情報３６０のパケットに含まれている端末固有情報と抽出した端末固有情報とが一致するか否かの検証を行なう。
更に、選択サービス提供装置では、認証処理部２０３が、ユーザ端末４から受信した認証確認情報３６０の識別番号を元に、認証管理情報より認証情報３４０の受信時刻を抽出し、抽出した認証情報３４０の受信時刻と現在の時刻（認証確認情報３６０の受信時刻）との時刻差を算出し、算出した時刻差が正常な範囲内であることの検証を行う。ここで、正常な範囲内とは、例えば、１分以内程度をいう。
更に、認証処理部２０３は、識別番号をキーに、認証管理情報よりユーザＩＤと権限情報とを抽出し、識別番号、ユーザＩＤ、権限情報、端末固有情報のメッセージダイジェスト、すなわち、認証情報３４０のメッセージダイジェストを生成する。その後、認証処理部２０３は、ユーザ端末４から受信した認証確認情報３６０のメッセージダイジェストと、生成した認証情報３４０のメッセージダイジェストとが一致するか否かの検証を行う。
【００４３】
以上の検証が全て正しければ、認証処理部２０３は認証管理情報より当該ユーザ端末４についてのレコード（認証情報３４０及び受信時刻）を削除し、サービス提供部２０５がユーザ端末４に対して権限情報に従ってサービスを提供する（Ｓ３０９）。
一方、以上の検証においていずれか一つでも条件に合致しない場合は、ユーザ端末４に対するサービスの提供を行わない。
【００４４】
本実施の形態に係るサービス提供装置は、認証情報の受信時刻と認証確認情報の受信時刻の時刻差が一定以上である場合はユーザ端末に対するサービス提供を行わないこととしているので、管理装置に対してサービス要求を行ったユーザ端末が何らかのトラブルのために選択サービス提供装置に接続できなかった場合に、選択サービス提供装置が保有している認証情報が不正利用されるのを防ぐ効果がある。
【００４５】
なお、以上の説明では、受信時刻の時刻差についての検証とメッセージダイジェストについての検証の双方を行うこととしているが、受信時刻の時刻差についての検証を行った結果、受信時刻の時刻差が正常な範囲内になかった場合には、メッセージダイジェストについての検証を行わずにユーザ端末に対するサービス提供を行わないことを決定してもよい。
【００４６】
実施の形態４.
本実施の形態では、実施の形態１で示した手法を用いた場合に、選択サービス提供装置においてユーザ端末へのサービス提供状況を管理する場合について説明する。
【００４７】
本実施の形態に係る管理装置１の構成例は図２に示すものと同様である。
また、サービス提供装置の構成例も図３に示すものと同様であるが、本実施の形態では、実施の形態３と同様に、認証処理部２０３は、管理装置１からの認証情報３４０の受信の際に認証情報３４０の受信時刻を認証管理情報記憶部２０４に記憶させ、また、ユーザ端末４からの認証確認情報３６０の受信の際に認証情報３４０の受信時刻を参照してユーザ端末４に対する認証処理を行う。また、認証処理部２０３はユーザ端末４に対するサービス提供状況を示すサービス提供フラグを設定可能であり、管理装置１からの認証情報３４０の受信の際にユーザ端末４に対するサービスが未提供であることを示すサービス提供フラグを設定し、また、ユーザ端末４からの認証確認情報３６０の受信の際にサービス提供フラグを参照して、ユーザ端末４に対する認証処理を行う。
【００４８】
次に、図８を参照して本実施の形態に係る通信システムの動作を説明する。
ステップＳ４０１～Ｓ４０６は、図１のステップＳ１０１～Ｓ１０６と場合と同様である。このため、ステップＳ４０６以降の動作を説明する。

選択サービス提供装置では、クローズドネットワーク用通信部２０１が管理装置１からの認証情報３４０を受信し、認証処理部２０３が、認証情報３４０の受信の際の時刻を取得して受信時刻とし、認証情報３４０に含まれた識別番号をキーにユーザＩＤと、権限情報と、端末固有情報と、更に、認証情報３４０の受信時刻とを認証管理情報として認証管理情報記憶部２０４に格納する。また、サービス提供フラグ（ステータス：サービス未提供）を設定する。この時点で初めて当該ユーザ端末に対するサービス提供準備が整う。

【００４９】

また、管理装置１では、実施の形態１と同様に、サービス提供先情報３５０を生成し、オープンネットワーク用通信部２０２からユーザ端末４に送信し（Ｓ４０７）、ユーザ端末４では、実施の形態１と同様に、認証確認情報を選択サービス提供装置に送信する（Ｓ４０８）。

【００５０】

選択サービス提供装置ではユーザ端末４から受信した認証確認情報３６０の識別番号を元に、認証処理部２０３が、認証管理情報記憶部２０４に格納されている認証管理情報より端末固有情報を抽出し、認証確認情報３６０のパケットに含まれている端末固有情報と抽出した端末固有情報とが一致するか否かの検証を行なう。

更に、選択サービス提供装置では、認証処理部２０３が、ユーザ端末４から受信した認証確認情報３６０の識別番号を元に、認証管理情報より認証情報３４０の受信時刻を抽出し、抽出した認証情報３４０の受信時刻と現在の時刻（認証確認情報３６０の受信時刻）との時刻差を算出し、算出した時刻差が正常な範囲内であることを検証を行う。ここで、正常な範囲内とは、例えば、１分以内程度をいう。

また、認証処理部２０３は、サービス提供フラグを参照し、サービス提供フラグのステータスがサービス未提供であることの検証を行う。

更に、認証処理部２０３は、識別番号をキーに、認証管理情報よりユーザＩＤと権限情報とを抽出し、識別番号、ユーザＩＤ、権限情報、端末固有情報のメッセージダイジェスト、すなわち、認証情報３４０のメッセージダイジェストを生成する。その後、認証処理部２０３は、ユーザ端末４から受信した認証確認情報３６０のメッセージダイジェストと、生成した認証情報３４０のメッセージダイジェストとが一致するか否かの検証を行う。

【００５１】

以上の検証が全て正しければ、認証処理部２０３は当該ユーザ端末４のサービス提供フラグのステータスをサービス提供済に変更し、サービス提供部２０５がユーザ端末４に対して権限情報に従ってサービスを提供する（Ｓ４０９）。

一方、以上の検証においていずれか一つでも条件に合致しない場合は、ユーザ端末４に対するサービスの提供を行わない。

また、サービス提供フラグのみの検証が誤り（サービス提供フラグを参照した際にサービス提供フラグのステータスがサービス提供済となっていた場合）でそれ以外の検証が全て正しい場合は、１つの正しい認証確認情報３６０を複数回行使しようとしたことになり、盗用の可能性があるため、当該認証確認情報３６０を送信したユーザ端末以外に既にサービスを利用している他のユーザ端末が存在している場合は、認証確認情報を送信してきたユーザ端末に対するサービス提供を行わないだけでなく、既にサービスを利用している他のユーザ端末に対するサービスの提供を直ちに中止する。

【００５２】

本実施の形態に係るサービス提供装置は、サービス提供フラグを用いてユーザ端末に対するサービス提供状況を管理しているため、認証確認情報を盗用して行う不正利用があっても、当該不正利用を即座に検出することができる効果がある。

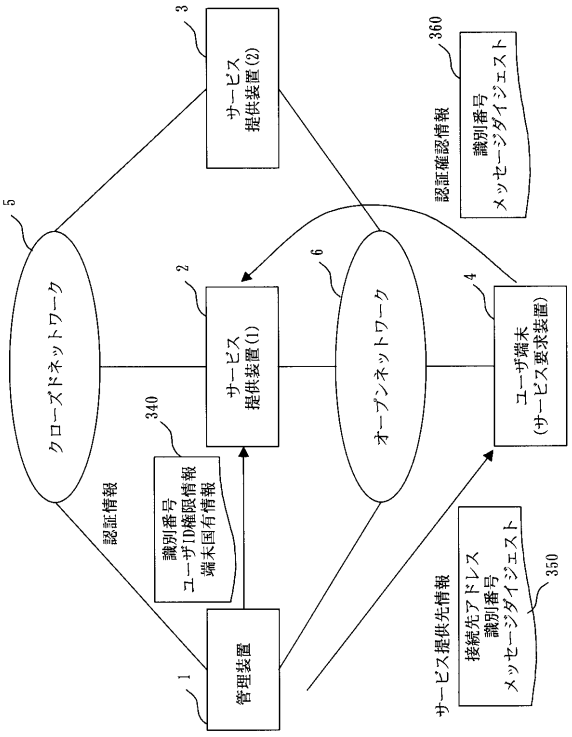
【００５３】

なお、以上の説明では、受信時刻の時刻差についての検証とサービス提供フラグについての検証の双方を行うこととしたが、受信時刻の時刻差についての検証を行わずにサービス提供フラグについての検証のみを行うようにしてもよい。

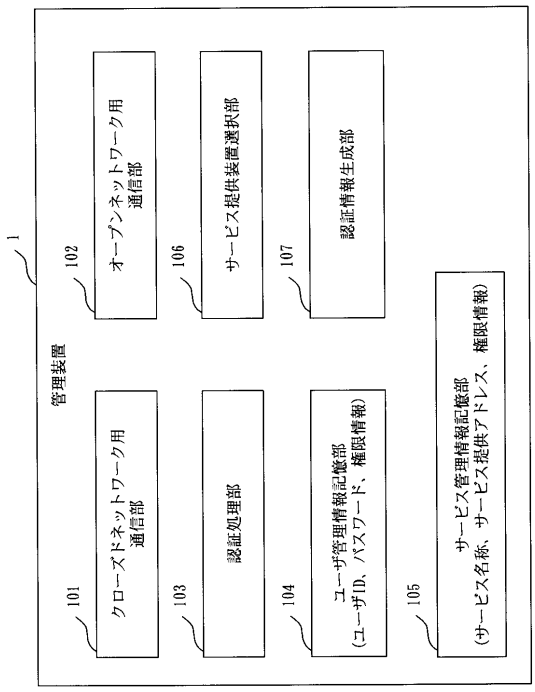
【００５４】

【発明の効果】
このように本発明によれば、複数のサービス提供装置のうち選択サービス提供装置にのみ第１の認証情報を送信し、また、サービス要求装置に対して第２の認証情報を選択サービス提供装置に送信するよう指示して第２の認証情報を送信するため、成りすまし等による不正利用を有効に防止することができる。
【図面の簡単な説明】
【図１】実施の形態１～４に係る通信システムの全体構成例を示す図。
【図２】実施の形態１に係る管理装置の構成例を示す図。
【図３】実施の形態１に係るサービス提供装置の構成例を示す図。
【図４】実施の形態１に係る通信システムの動作例を示す図。
【図５】実施の形態２に係る管理装置の構成例を示す図。
【図６】実施の形態２に係る通信システムの動作例を示す図。
【図７】実施の形態３に係る通信システムの動作例を示す図。
【図８】実施の形態４に係る通信システムの動作例を示す図。
【符号の説明】
１　管理装置、２　サービス提供装置（１）、３　サービス提供装置（２）、４　ユーザ端末、５　クローズドネットワーク、６　オープンネットワーク、１０１　クローズドネットワーク用通信部、１０２　オープンネットワーク用通信部、１０３　認証処理部、１０４　ユーザ管理情報記憶部、１０５　サービス管理情報記憶部、１０６　サービス提供装置選択部、１０７　認証情報生成部、１０８　認証管理情報記憶部、２０１　クローズドネットワーク用通信部、２０２オープンネットワーク用通信部、２０３　認証処理部、２０４　認証管理情報記憶部、２０５　サービス提供部。

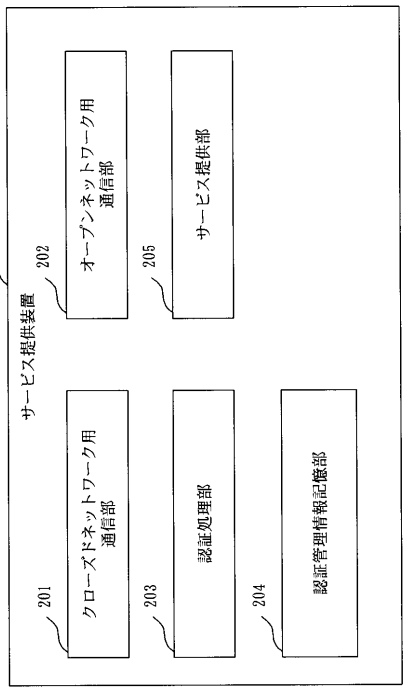
【図１】



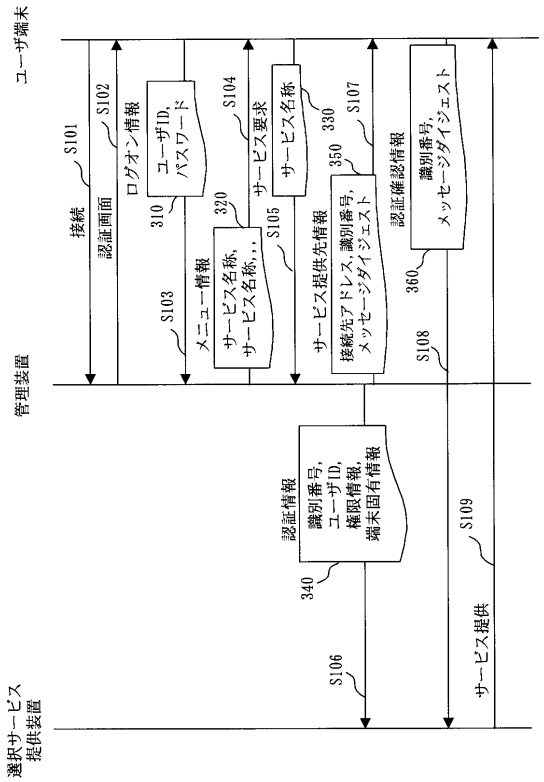
【図２】



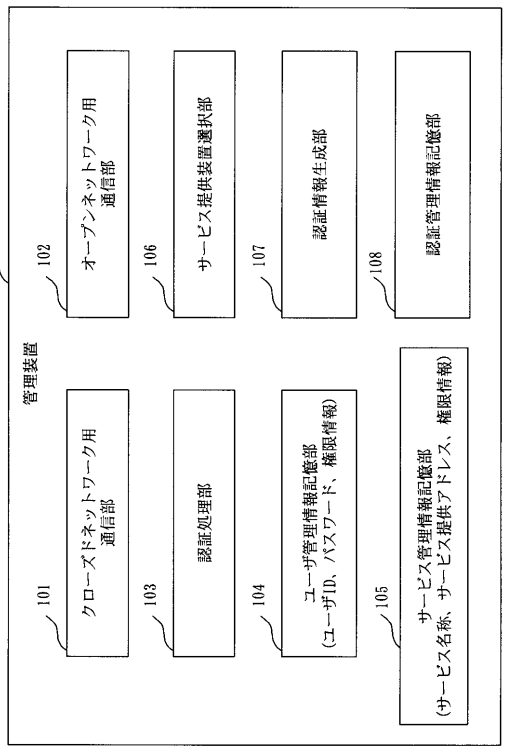
【図３】


2,3
サービス提供装置
201
クローズドネットワーク用
通信部
202
オープンネットワーク用
通信部
203
認証処理部
204
認証管理情報記憶部
205
サービス提供部

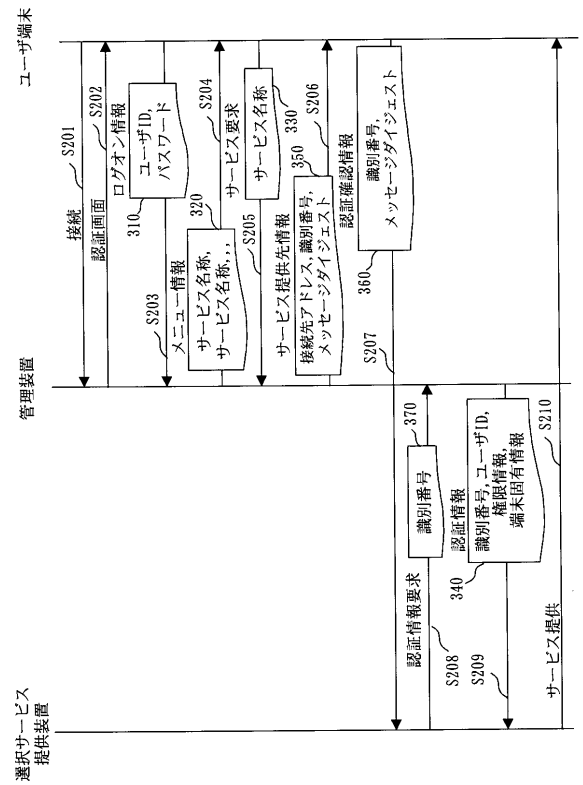
【図４】


ユーザ端末
管理装置
選択サービス
提供装置
接続
S101
認証画面
S102
ログオン情報
ユーザID,
パスワード
310
メニュー情報
S103
サービス名称,
サービス名称,,,
320
S104
サービス要求
S105
サービス名称
330
サービス提供先情報
接続先アドレス,識別番号,
メッセージダイジェスト
350
認証確認情報
識別番号,
メッセージダイジェスト
360
S107
S108
認証情報
識別番号,
ユーザID,
権限情報,
端末固有情報
340
S106
サービス提供
S109

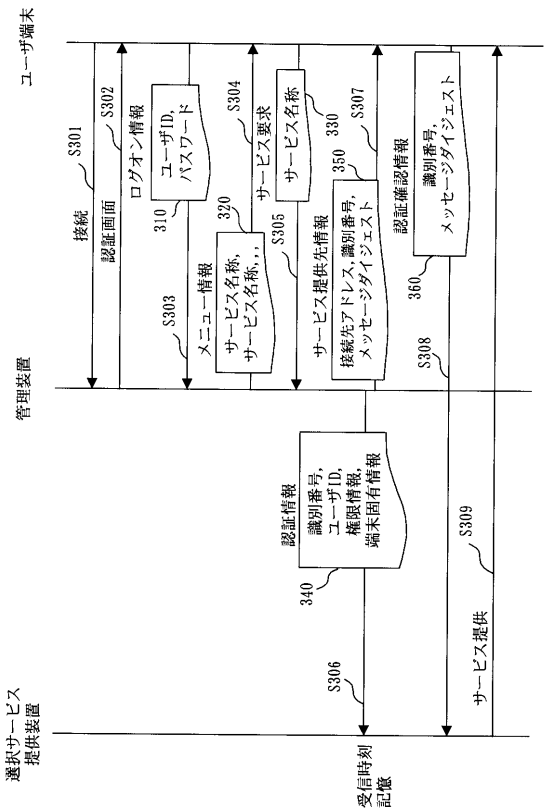
【図５】


1
管理装置
101
クローズドネットワーク用
通信部
102
オープンネットワーク用
通信部
103
認証処理部
104
ユーザ管理情報記憶部
(ユーザID、パスワード、権限情報)
105
サービス管理情報記憶部
(サービス名称、サービス提供アドレス、権限情報)
106
サービス提供装置選択部
107
認証情報生成部
108
認証管理情報記憶部

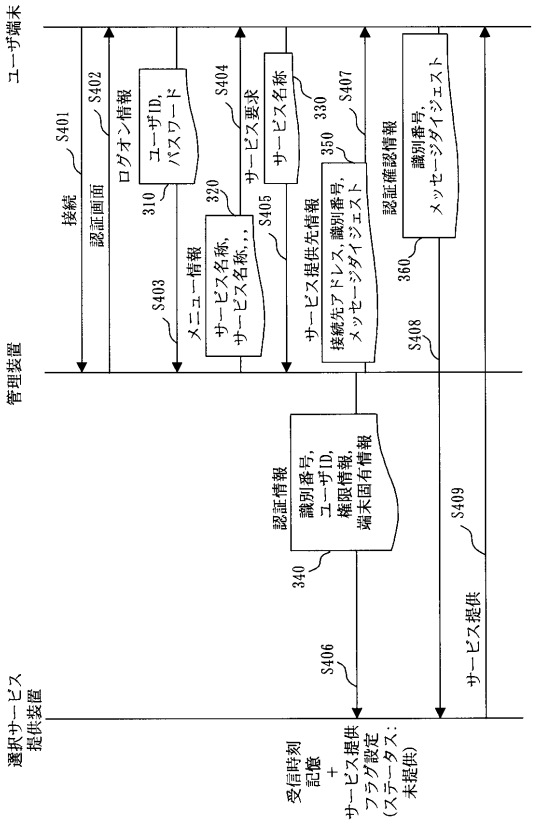
【図６】


ユーザ端末
管理装置
選択サービス
提供装置
接続
S201
認証画面
S202
ログオン情報
ユーザID,
パスワード
310
メニュー情報
S203
サービス名称,
サービス名称,,,
320
S204
サービス要求
S205
サービス名称
330
サービス提供先情報
接続先アドレス,識別番号,
メッセージダイジェスト
350
S206
認証確認情報
識別番号,
メッセージダイジェスト
360
S207
認証情報要求
S208
識別番号
370
認証情報
識別番号,ユーザID,
権限情報,
端末固有情報
340
S209
S210
サービス提供

【図７】


ユーザ端末
管理装置
選択サービス提供装置
接続
S301
認証画面
S302
ログオン情報
ユーザID,
パスワード
310
S303
メニュー情報
サービス名称,
サービス名称,,,
320
S304
サービス要求
S305
サービス名称
330
サービス提供先情報
接続先アドレス,識別番号,
メッセージダイジェスト
350
S307
認証確認情報
識別番号,
メッセージダイジェスト
360
S308
認証情報
識別番号,
ユーザID,
権限情報,
端末固有情報
340
S306
S309
サービス提供
受信時刻
記憶

【図８】


ユーザ端末
管理装置
選択サービス提供装置
接続
S401
認証画面
S402
ログオン情報
ユーザID,
パスワード
310
S403
メニュー情報
サービス名称,
サービス名称,,,
320
S404
サービス要求
S405
サービス名称
330
サービス提供先情報
接続先アドレス,識別番号,
メッセージダイジェスト
350
S407
認証確認情報
識別番号,
メッセージダイジェスト
360
S408
認証情報
識別番号,
ユーザID,
権限情報,
端末固有情報
340
S406
S409
サービス提供
受信時刻
記憶
+
サービス提供
フラグ設定
(ステータス:
未提供)