(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2010-192947
(P2010-192947A)
(43)公開日　平成22年9月2日(2010.9.2)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 12/56	(2006.01)	H04L	12/56	H	5J104
H04L 9/32	(2006.01)	H04L	9/00	675D	5K030

審査請求 未請求　請求項の数 7　ＯＬ　（全 17 頁）

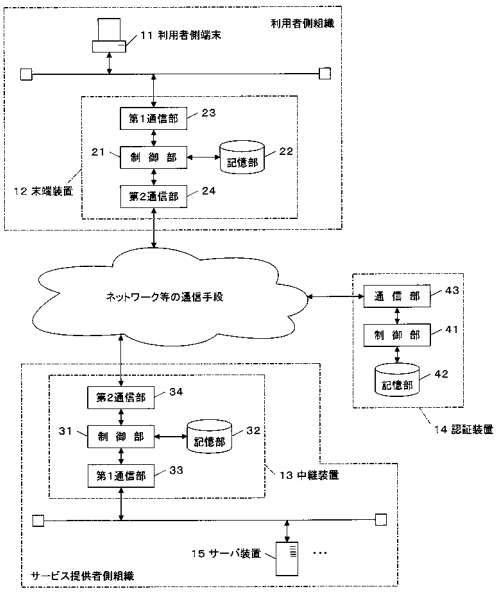
(21)出願番号　特願2009-32037(P2009-32037)
(22)出願日　平成21年2月13日(2009.2.13)

(71)出願人　000005496
富士ゼロックス株式会社
東京都港区赤坂九丁目７番３号
(74)代理人　100122275
弁理士　竹居　信利
(74)代理人　100102716
弁理士　在原　元司
(74)代理人　100115129
弁理士　清水　昇
(72)発明者　吉田　武央
東京都港区赤坂九丁目７番３号　富士ゼロックス株式会社内

Ｆターム(参考)　5J104 AA07 AA16 BA02 EA03 EA04
EA08 EA16 KA02 NA02 NA05
NA36 NA37 NA38 PA07
5K030 GA15 HD03 LD19

(54)【発明の名称】通信システム、中継装置、末端装置、及びプログラム

(57)【要約】
【課題】通信先ごとの通信を制御する。
【解決手段】サーバ装置が要求を受け入れる各通信先ごとに、通信先ごとの認証情報と、通信の条件の情報とを関連づけて記憶し、通信先の認証情報を含む通信認可情報を要求元から受け入れて、当該受け入れた通信認可情報に含まれる認証情報に関連づけられた通信の条件の情報を取得し、要求元が要求する通信が、取得した条件の情報が表す条件に合致するか否かを判断する。要求元が要求する通信が、取得した条件の情報が表す条件に合致すると判断されたときに、予め設定した仮想サービス専用線を介して、要求元からの通信を、要求された通信先へ中継する。
【選択図】図１



【特許請求の範囲】
【請求項１】
末端装置と、中継装置と、認証装置と、サーバ装置とを含み、
前記サーバ装置は、少なくとも一つの通信先への通信を受け入れ、通信先ごとに定められたサービスを提供し、
前記末端装置は、前記サーバ装置の通信先ごとの通信認可情報であって、通信先の認証情報と、中継装置、通信先及び末端装置の鍵情報とを含む通信認可情報を前記認証装置から受け入れて記憶し、いずれかの通信先との通信要求を受け入れて、当該通信要求に係る通信先に対応して定義された通信認可情報を前記中継装置へ送信して、通信を要求し、
前記中継装置は、前記末端装置が提供する通信認可情報に含まれる通信先の認証情報を参照し、当該参照した通信先の認証情報に関連づけて予め規定された通信の条件の情報を取得して、末端装置からの通信が前記取得した条件に合致するか否かを判断し、合致する場合に、末端装置からの要求に応答し、予め設定した仮想サービス専用線を介して、末端装置の要求する通信先と末端装置との間の通信を中継することを特徴とする通信システム。
【請求項２】
サーバ装置が要求を受け入れる各通信先ごとに、通信先ごとの認証情報と、通信の条件の情報とを関連づけて記憶する記憶手段と、
通信先の認証情報を含む通信認可情報を要求元から受け入れて、当該受け入れた通信認可情報に含まれる認証情報に関連づけられた通信の条件の情報を取得する取得手段と、
前記要求元が要求する通信が、前記取得した条件の情報が表す条件に合致するか否かを判断する判断手段と、
前記判断手段により、前記要求元が要求する通信が、前記取得した条件の情報が表す条件に合致すると判断されたときに、予め設定した仮想サービス専用線を介して、前記要求元からの通信を、要求された通信先へ中継する中継手段と、
を含むことを特徴とする中継装置。
【請求項３】
サーバ装置が要求を受け入れる通信先のいずれかに関連して、中継装置が提供する参照情報を指定した、通信の要求を利用者側から受け入れる手段と、
前記サーバ装置の通信先ごとの通信認可情報であって、通信先に関連して中継装置が提供する参照情報と、通信先の認証情報と、中継装置、通信先及び末端装置の鍵情報とを含む通信認可情報を記憶する手段と、
前記受け入れた要求に係る参照情報に対応する前記通信認可情報を検索する手段と、
検索により、前記受け入れた要求に係る参照情報に対応する前記通信認可情報が見出されたときに、当該通信認可情報を中継装置に送信して、予め設定した仮想サービス専用線を介して要求に係る通信先との間の通信を中継するよう要求する手段と、
を含む末端装置。
【請求項４】
末端装置と、中継装置と、認証装置と、サーバ装置とを含み、
前記サーバ装置は、少なくとも一つの通信先への通信を受け入れ、通信先ごとに定められたサービスを提供し、
前記末端装置は、前記サーバ装置の通信先ごとの通信認可情報を記憶する記憶手段と、
いずれかの通信先との通信要求を受け入れて、当該通信要求に係る通信先に対応して定義された通信認可情報を前記認証装置へ送信する送信手段と、
前記認証装置から、中継装置を特定する情報と、認証情報の元となる情報とを受信し、当該認証情報の元となる情報に基づき認証情報を生成して、前記情報で特定される中継装置へ送信する手段と、
を含み、
前記認証装置は、前記末端装置から通信認可情報を受信して、利用可能性を判定し、利用可能と判断したときに、当該通信認可情報に対応する通信先への通信を中継可能な中継

装置を特定する情報と、認証情報の元となる情報とを前記末端装置に送信するとともに、前記情報で特定される中継装置に、前記末端装置に送信したと同じ認証情報の元となる情報と、前記末端装置を特定する情報とを送信し、
前記中継装置は、前記認証装置から認証情報の元となる情報を受信するまでは、通信の要求に応答しないよう通信手段を制御する制御手段と、
前記認証装置から認証情報の元となる情報と、末端装置を特定する情報とを受信し、前記認証情報の元となる情報に基づき、前記末端装置と同じ方法で認証情報を生成する生成手段と、
前記情報で特定される末端装置から認証情報を受け入れ、前記生成手段によって生成した認証情報と、当該受け入れた認証情報とを比較する比較手段と、
前記比較の結果に基づき、認証が完了したと判断したときに、前記末端装置との間の通信に用いる仮想専用線を設定する設定手段と、
前記設定した仮想専用線を介して、前記末端装置から受信される要求を前記サーバ装置へ中継し、前記サーバ装置からの応答を前記末端装置へ中継する中継手段と、
を有する、
ことを特徴とする通信システム。
【請求項５】
コンピュータを、
サーバ装置が要求を受け入れる通信先ごとに、通信先ごとの認証情報と、通信の条件の情報とを関連づけて記憶する記憶手段と、
通信先の認証情報を含む通信認可情報を要求元から受け入れて、当該受け入れた通信認可情報に含まれる認証情報に関連づけられた通信の条件の情報を取得する取得手段と、
前記要求元が要求する通信が、前記取得した条件の情報が表す条件に合致するか否かを判断する判断手段と、
前記判断手段により、前記要求元が要求する通信が、前記取得した条件の情報が表す条件に合致すると判断されたときに、予め設定した仮想サービス専用線を介して、前記要求元からの通信を、要求された通信先へ中継する中継手段と、
として機能させることを特徴とするプログラム。
【請求項６】
コンピュータを、
サーバ装置が要求を受け入れる通信先のいずれかに関連して、中継装置が提供する参照情報を指定した、通信の要求を利用者側から受け入れる手段と、
前記サーバ装置の通信先ごとの通信認可情報であって、通信先に関連して中継装置が提供する参照情報と、通信先の認証情報と、中継装置、通信先及び末端装置の鍵情報とを含む通信認可情報を記憶する手段と、
前記受け入れた要求に係る参照情報に対応する前記通信認可情報を検索する手段と、
検索により、前記受け入れた要求に係る参照情報に対応する前記通信認可情報が見出されたときに、当該通信認可情報を中継装置に送信して、予め設定した仮想サービス専用線を介して、要求に係る通信先との間の通信を中継するよう要求する手段と、
として機能させることを特徴とするプログラム。
【請求項７】
末端装置と、認証装置と、サーバ装置とに接続され、通信手段を備えたコンピュータを、
前記認証装置から認証情報の元となる情報を受信するまでは、通信の要求に応答しないよう通信手段を制御する制御手段と、
前記認証装置から認証情報の元となる情報と、末端装置を特定する情報とを受信し、前記認証情報の元となる情報に基づき、予め定められた方法で認証情報を生成する生成手段と、
前記情報で特定される末端装置から認証情報を受け入れ、前記生成手段によって生成した認証情報と、当該受け入れた認証情報とを比較する比較手段と、

前記比較の結果に基づき、認証が完了したと判断したときに、前記末端装置との間の通信に用いる仮想専用線を設定する設定手段と、
前記設定した仮想専用線を介して、前記末端装置から受信される要求を前記サーバ装置へ中継し、前記サーバ装置からの応答を前記末端装置へ中継する中継手段と、
として機能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】
本発明は、通信システム、中継装置、末端装置、及びプログラムに関する。
【背景技術】
【０００２】
ＶＰＮ（Virtual Private Network）ルータにＨＤＤ（Hard Disk Drive）を備え、ＣＰＵ（Central Processing Unit）は、ＨＤＤのデータが更新された場合、該当データを暗号・復号モジュール、ＱｏＳ（Quality of Service）モジュールを介してインターネットに送信するという技術が特許文献１に開示されている。
【先行技術文献】
【特許文献】
【０００３】
【特許文献１】特開２００８－２２７８０５号公報
【発明の概要】
【発明が解決しようとする課題】
【０００４】
サーバ装置により提供されるサービスごとに仮想的な専用線を設定できる通信システム、中継装置、末端装置、及びプログラムを提供すること。
【課題を解決するための手段】
【０００５】
請求項１記載の発明は、通信システムであって、末端装置と、中継装置と、認証装置と、サーバ装置とを含み、前記サーバ装置は、少なくとも一つの通信先への通信を受け入れ、通信先ごとに定められたサービスを提供し、前記末端装置は、前記サーバ装置の通信先ごとの通信認可情報であって、通信先の認証情報と、中継装置、通信先及び末端装置の鍵情報とを含む通信認可情報を前記認証装置から受け入れて記憶し、いずれかの通信先との通信要求を受け入れて、当該通信要求に係る通信先に対応して定義された通信認可情報を前記中継装置へ送信して、通信を要求し、前記中継装置は、前記末端装置が提供する通信認可情報に含まれる通信先の認証情報を参照し、当該参照した通信先の認証情報に関連づけて予め規定された通信の条件の情報を取得して、末端装置からの通信が前記取得した条件に合致するか否かを判断し、合致する場合に、末端装置からの要求に応答し、予め設定した仮想サービス専用線を介して、末端装置の要求する通信先と末端装置との間の通信を中継することとしたものである。
【０００６】
請求項２記載の発明は、中継装置であって、サーバ装置が要求を受け入れる各通信先ごとに、通信先ごとの認証情報と、通信の条件の情報とを関連づけて記憶する記憶手段と、通信先の認証情報を含む通信認可情報を要求元から受け入れて、当該受け入れた通信認可情報に含まれる認証情報に関連づけられた通信の条件の情報を取得する取得手段と、前記要求元が要求する通信が、前記取得した条件の情報が表す条件に合致するか否かを判断する判断手段と、前記判断手段により、前記要求元が要求する通信が、前記取得した条件の情報が表す条件に合致すると判断されたときに、予め設定した仮想サービス専用線を介して、前記要求元からの通信を、要求された通信先へ中継する中継手段と、を含むこととしたものである。
【０００７】
請求項３記載の発明は、末端装置であって、サーバ装置が要求を受け入れる通信先のい

ずれかに関連して、中継装置が提供する参照情報を指定した、通信の要求を利用者側から受け入れる手段と、前記サーバ装置の通信先ごとの通信認可情報であって、通信先に関連して中継装置が提供する参照情報と、通信先の認証情報と、中継装置、通信先及び末端装置の鍵情報とを含む通信認可情報を記憶する手段と、前記受け入れた要求に係る参照情報に対応する前記通信認可情報を検索する手段と、検索により、前記受け入れた要求に係る参照情報に対応する前記通信認可情報が見出されたときに、当該通信認可情報を中継装置に送信して、予め設定した仮想サービス専用線を介して要求に係る通信先との間の通信を中継するよう要求する手段と、を含むこととしたものである。

【０００８】

請求項４記載の発明は、通信システムであって、末端装置と、中継装置と、認証装置と、サーバ装置とを含み、前記サーバ装置は、少なくとも一つの通信先への通信を受け入れ、通信先ごとに定められたサービスを提供し、前記末端装置は、前記サーバ装置の通信先ごとの通信認可情報を記憶する記憶手段と、いずれかの通信先との通信要求を受け入れて、当該通信要求に係る通信先に対応して定義された通信認可情報を前記認証装置へ送信する送信手段と、前記認証装置から、中継装置を特定する情報と、認証情報の元となる情報とを受信し、当該認証情報の元となる情報に基づき認証情報を生成して、前記情報で特定される中継装置へ送信する手段と、を含み、前記認証装置は、前記末端装置から通信認可情報を受信して、利用可能性を判定し、利用可能と判断したときに、当該通信認可情報に対応する通信先への通信を中継可能な中継装置を特定する情報と、認証情報の元となる情報とを前記末端装置に送信するとともに、前記情報で特定される中継装置に、前記末端装置に送信したと同じ認証情報の元となる情報と、前記末端装置を特定する情報とを送信し、前記中継装置は、前記認証装置から認証情報の元となる情報を受信するまでは、通信の要求に応答しないよう通信手段を制御する制御手段と、前記認証装置から認証情報の元となる情報と、末端装置を特定する情報とを受信し、前記認証情報の元となる情報に基づき、前記末端装置と同じ方法で認証情報を生成する生成手段と、前記情報で特定される末端装置から認証情報を受け入れ、前記生成手段によって生成した認証情報と、当該受け入れた認証情報とを比較する比較手段と、前記比較の結果に基づき、認証が完了したと判断したときに、前記末端装置との間の通信に用いる仮想専用線を設定する設定手段と、前記設定した仮想専用線を介して、前記末端装置から受信される要求を前記サーバ装置へ中継し、前記サーバ装置からの応答を前記末端装置へ中継する中継手段と、を有する、こととしたものである。

【０００９】

また、請求項５記載の発明は、プログラムであって、コンピュータを、サーバ装置が要求を受け入れる通信先ごとに、通信先ごとの認証情報と、通信の条件の情報とを関連づけて記憶する記憶手段と、通信先の認証情報を含む通信認可情報を要求元から受け入れて、当該受け入れた通信認可情報に含まれる認証情報に関連づけられた通信の条件の情報を取得する取得手段と、前記要求元が要求する通信が、前記取得した条件の情報が表す条件に合致するか否かを判断する判断手段と、前記判断手段により、前記要求元が要求する通信が、前記取得した条件の情報が表す条件に合致すると判断されたときに、予め設定した仮想サービス専用線を介して、前記要求元からの通信を、要求された通信先へ中継する中継手段と、として機能させることとしたものである。

【００１０】

請求項６記載の発明は、プログラムであって、コンピュータを、サーバ装置が要求を受け入れる通信先のいずれかに関連して、中継装置が提供する参照情報を指定した、通信の要求を利用者側から受け入れる手段と、前記サーバ装置の通信先ごとの通信認可情報であって、通信先に関連して中継装置が提供する参照情報と、通信先の認証情報と、中継装置、通信先及び末端装置の鍵情報とを含む通信認可情報を記憶する手段と、前記受け入れた要求に係る参照情報に対応する前記通信認可情報を検索する手段と、検索により、前記受け入れた要求に係る参照情報に対応する前記通信認可情報が見出されたときに、当該通信認可情報を中継装置に送信して、予め設定した仮想サービス専用線を介して、要求に係る

通信先との間の通信を中継するよう要求する手段と、として機能させることとしたものである。

【００１１】

請求項７記載の発明は、プログラムであって、末端装置と、認証装置と、サーバ装置とに接続され、通信手段を備えたコンピュータを、前記認証装置から認証情報の元となる情報を受信するまでは、通信の要求に応答しないよう通信手段を制御する制御手段と、前記認証装置から認証情報の元となる情報と、末端装置を特定する情報とを受信し、前記認証情報の元となる情報に基づき、予め定められた方法で認証情報を生成する生成手段と、前記情報で特定される末端装置から認証情報を受け入れ、前記生成手段によって生成した認証情報と、当該受け入れた認証情報とを比較する比較手段と、前記比較の結果に基づき、認証が完了したと判断したときに、前記末端装置との間の通信に用いる仮想専用線を設定する設定手段と、前記設定した仮想専用線を介して、前記末端装置から受信される要求を前記サーバ装置へ中継し、前記サーバ装置からの応答を前記末端装置へ中継する中継手段と、として機能させることとしたものである。

【発明の効果】

【００１２】

請求項１，２，５記載の発明によると、サーバ装置により提供される通信先ごとに仮想的な専用線を設定し、当該専用線を介した通信を行うことができる。

【００１３】

請求項３，６記載の発明によると、サーバ装置により提供される通信先ごとに設定される通信認可情報の有無により、通信先ごとの仮想的な専用線を設定できる。

【００１４】

請求項４，７記載の発明によると、中継装置が基本的に通信を拒否しつつ、例外的な処理を行って、通信先ごとの仮想的な専用線を設定できる。

【図面の簡単な説明】

【００１５】

【図１】本発明の実施の形態に係る通信システムの構成例を表すブロック図である。

【図２】本発明の実施の形態に係る末端装置の例を表す機能ブロック図である。

【図３】本発明の実施の形態に係る通信システムで用いられる通信認可情報としてのチケット情報の例を表す説明図である。

【図４】本発明の実施の形態に係る中継装置の例を表す機能ブロック図である。

【図５】本発明の実施の形態に係る中継装置が保持する通信条件情報の例を表す説明図である。

【図６】本発明の実施の形態に係る認証装置が保持する中継装置のアドレスを特定する情報の例を表す説明図である。

【図７】本発明の実施の形態に係る通信システムでの事前処理の例を表すフローチャート図である。

【図８】本発明の実施の形態に係る通信システムでの通信処理の例を表すフローチャート図である。

【図９】本発明の実施の形態に係る通信システムでの通信処理の続きの例を表すフローチャート図である。

【発明を実施するための形態】

【００１６】

本発明の実施の形態について図面を参照しながら説明する。本発明の実施の形態に係る通信システム１は、図１に例示するように、利用者側端末１１と、末端装置１２と、中継装置１３と、認証装置１４と、アプリケーションサーバ１５とを含んで構成される。ここで末端装置１２と、中継装置１３と、認証装置１４とは、ネットワークなどの通信手段を介して接続されている。また、利用者側端末１１と末端装置１２とは、利用者側の組織に配されてローカルなネットワークなどの通信手段を介して接続されている。さらに、中継装置１３とアプリケーションサーバ１５とは、サービス提供側の組織に配されて、ローカ

ルなネットワークなどの通信手段を介して接続されている。

【００１７】

末端装置１２は、図１に示したように、制御部２１と、記憶部２２と、第１通信部２３と、第２通信部２４とを含んで構成される。中継装置１３は、制御部３１と、記憶部３２と、第１通信部３３と、第２通信部３４とを含んで構成されている。また、認証装置１４は、制御部４１と、記憶部４２と、通信部４３とを含んで構成される。

【００１８】

末端装置１２の制御部２１は、ＣＰＵ（Central Processing Unit）等のプログラム制御デバイスであり、記憶部２２に格納されたプログラムに従って動作している。本実施の形態では、この制御部２１は、プログラムを実行することにより、機能的には図２に例示するように、要求受入部５１と、チケット情報処理部５２と、接続部５３と、ワンタイムパスワード発行部５４と、通信制御部５５とを含んで構成される。

【００１９】

要求受入部５１は、利用者側端末１１から入力されるアプリケーションサーバ１５への通信要求を受け入れる。この通信要求には、アプリケーションサーバ１５が提供するサービス（通信先）を特定する情報の例として、当該サービスの仮想的なＵＲＬ（Uniform Resource Locator）等、利用者側端末１１が利用を希望するサービスに係るアドレスの情報が含まれる。ここでサービスの仮想的なＵＲＬとは、サービスの要求に係る情報を送信する先を表すアドレスに対応して中継装置１３が提供する参照情報であり、ネットワーク上のＤＮＳ（Domain Name Service）によって、アドレスが解決されるものではなく、中継装置１３が専ら、利用者の要求するアプリケーションサーバ１５のサービスを識別するために利用する情報である。従って、この仮想的なＵＲＬは、仮想的なドメイン名や仮想的なホスト名を含んで構成されていてもよい。つまり、この例ではトップレベルドメインですら、仮想的なもの（既存のものと同じであってもよいし、既存のものでなくてもよい）であって構わない。本実施の形態のアプリケーションサーバ１５は、一つのサービスだけでなく、複数のサービスを提供するものであってもよい。この場合は提供するサービスごとに、異なる通信先（利用者側から見れば、通信先ごとに異なる複数の仮想的なＵＲＬ）が予め規定され、どの通信先に対応する参照情報を指定して要求を送信するかによって、提供されるサービスが異なることになる。

【００２０】

チケット情報処理部５２は、通信先ごと（提供されるサービスごと）に定義される通信認可情報としてのチケット情報を管理する。このチケット情報は、具体的には図３に例示するように、ログイン情報Ｌと、中継装置１３により発行された鍵情報Ｘと、認証装置１４を特定する情報ＡＡＡ（複数あってもよい）とを含む。ここに鍵情報Ｘは中継装置１３において固有な情報であり、中継装置１３のＩＰアドレスなど、中継装置１３を特定する情報を含むものとすればよい。さらに、チケット情報には、このチケット情報を利用する末端装置１２を特定する情報Ａ（例えば末端装置１２のＩＰアドレスなど）を含んでもよい。ここでログイン情報Ｌは、通信先となるサービスを特定する情報（プレフィックスＰＦ）と、当該サービスを提供するアプリケーションサーバ１５へのログインに必要となる情報（ユーザー名、パスワードなど、サフィックス：ＳＦ）とを含むサービス名ＳＮである。またはログイン情報Ｌは、このサービス名ＳＮを予め定めた方法でハッシュ値としたものであってもよい。また認証装置１４を特定する情報は、認証装置１４との通信時に用いる情報で、例えば認証装置１４のドメイン名アドレスや（ＩＰ（Internet Protocol）アドレスなど）でよい。

【００２１】

このチケット情報処理部５２は、認証装置１４にて発行されたチケット情報を、それぞれ対応する通信先に関連して中継装置１３が提供する参照情報に関連づけて記憶部２２に格納して保持する。またこのチケット情報処理部５２は、通信制御部５５から入力される指示に従って、通信制御部５５が情報の送信先として指定する参照情報に対応するチケット情報を記憶部２２から読み出し、通信制御部５５に出力する。

【００２２】
接続部５３は、中継装置１３との間に、仮想的な専用線（仮想専用線）を設定する。この仮想専用線の一例は、通信内容を暗号化してカプセル化し、トンネリングした通信経路を形成したものである。このような通信経路としてはＶＰＮ（Virtual Private Network）と呼ばれるものがある。尤も本実施の形態の仮想専用線は、ＶＰＮに限らず、種々の方法で内容を秘匿した通信が可能なものであればよい。この接続部５３は、末端装置１２の電源が投入されたときや、接続が遮断されたときなどに、仮想専用線を設定する。
【００２３】
具体的に、この末端装置１２の接続部５３は認証装置１４に対して中継装置１３への仮想専用線の設定と、ログインとを要求する。すなわち、まず末端装置１２の接続部５３は認証装置１４に対して問い合わせを送信する。この問い合わせの際にはチケット情報、またはチケット情報のハッシュを送信する。このチケット情報には、中継装置１３が発行した鍵情報Ｘとサービス名とが含まれる。認証装置１４は末端装置１２からの認証に基づいて最適な中継装置の接続情報を末端装置１２に通知し、中継装置１３には、チケット情報もしくはそのハッシュと末端装置１２のＩＰアドレスを通知する。また末端装置１２と中継装置１３には認証情報の元となる同一の情報として、同一のハッシュシード情報ＨＳが配布される。
【００２４】
接続部５３は、ワンタイムパスワード発行部５４に対して認証装置１４から受信したハッシュシード情報ＨＳを出力し、当該ハッシュシード情報ＨＳに基づいてワンタイムＩＤパスワード（以下、ワンタイムＩＤＰと呼ぶ）を生成させる。そして、このワンタイムＩＤＰは、末端装置１２を介して中継装置１３へ仮想専用線の接続認証のための情報として利用される。このワンタイムＩＤＰが通信先にて認証されることで、中継装置１３が予め設定した仮想専用線を介して、通信先と末端装置１２との間の通信の中継を開始する。この中継装置１３の動作については後に述べる。
【００２５】
ワンタイムパスワード発行部５４は、接続部５３から入力される指示に従って、予め定められたアルゴリズムで、接続部５３から入力された情報を変換し、変換後の情報を、ワンタイムＩＤＰとして出力する。
【００２６】
通信制御部５５は、要求受入部５１にて受け入れた参照情報等で特定される通信先に対する通信を中継するよう、設定されている仮想専用線を介して中継装置１３に対して要求する。中継装置１３が中継を開始すると、仮想専用線を介して中継装置１３が中継する通信先からの応答を受信して、要求受入部５１に対する要求元である利用者側端末１１に対して、当該受信した応答を出力する。本実施の形態では、仮想専用線が参照情報等で識別されるサービスごとに設定され、いわば、サービスごとの仮想専用線が設定されているのと同じ状態となるので、以下、中継装置１３を介して行われるこの通信の経路を仮想サービス専用線と称する。この通信制御部５５の具体的動作を含め、制御部２１の詳しい動作については、後に述べる。
【００２７】
記憶部２２は、メモリデバイスや、ディスクなどのストレージデバイスなどであり、制御部２１によって実行されるプログラムを記憶している。このプログラムは、ＤＶＤ－ＲＯＭ（Digital Versatile Disc - Read Only Memory）等のコンピュータ可読な記憶媒体に格納された状態で提供され、この記憶部２２に複写されたものであってもよい。また、この記憶部２２は、制御部２１のワークメモリとしても動作する。
【００２８】
第１通信部２３は、ネットワークインタフェース等であり、ローカルなネットワークなどの通信手段に接続され、利用者側端末１１との間で情報を送受する。第２通信部２４も、またネットワークインタフェース等であるが、この第２通信部２４は、中継装置１３や、認証装置１４との間で情報を送受可能に接続されている。

【００２９】
中継装置１３の制御部３１は、ＣＰＵ（Central Processing Unit）等のプログラム制御デバイスであり、記憶部３２に格納されたプログラムに従って動作している。本実施の形態では、この制御部３１は、プログラムを実行することにより、機能的には図４に例示するように、鍵情報発行部６１と、通信条件管理部６２と、中継接続部６３と、中継処理部６４とを含んで構成される。
【００３０】
ここに鍵情報発行部６１は、サービス名、要求元である末端装置１２を特定する情報、及び、認証装置１４を特定する情報とともに、鍵情報の要求の入力を外部から受けて鍵情報Ｘを発行する。そしてこの鍵情報発行部６１は、サービス名と、要求元である末端装置１２を特定する情報Ａと、認証装置１４を特定する情報ＡＡＡと、発行した鍵情報Ｘとを含む情報（これらを、予め定めた順序で連接した情報等とすればよい）を、予め定めた方法でハッシュし、ハッシュ値を得る。そして鍵情報発行部６１は、このハッシュ値を鍵情報Ｘの要求元へ出力する。
【００３１】
通信条件管理部６２は、図５に例示するように、サービス名と、当該サービス名によって特定するサービスに対する通信の条件とを関連づけた通信条件情報を記憶部３２に保持する。ここで通信の条件は、中継装置１３から通信先へアクセスするために必要となる通信先のアドレスの情報（以下、末端装置１２から指定される仮想的なＵＲＬ等の参照情報と区別するために、実ＵＲＬと呼ぶ）そのものであってもよいし、また通信の要求があったときに実行するべき処理を規定したものであってもよい。この処理としては例えば、アプリケーションサーバ１５の負荷の情報を取得し、当該取得した情報に応じて通信先として指定可能な実ＵＲＬである場合に限り、通信を行うという処理も行い得る。この場合、取得した情報により表されるアプリケーションサーバ１５の負荷が予め定めたしきい値より大きい場合に、一部の実ＵＲＬで特定される通信先へのアクセスを制限するようにしてもよい。
【００３２】
また、この通信の条件により指定される処理としては、中継装置１３自体の処理に関わるものであってもよい。例えば、中継装置１３は、一般に複数の中継の処理を並行して、時分割的に実行している。具体的には、実行の要求があった順に待ち行列に記録し、要求があった順に処理を実行するが、通信の条件によっては、受け入れた要求を、待ち行列の先頭（次に処理するべき要求を表す）に割り込ませてもよい。
【００３３】
中継装置１３の中継接続部６３は、第２通信部３４に到来する情報を原則として破棄する動作を行っている。つまり本実施の形態では、第２通信部３４は、原則として通信に応答することがなく、不正な攻撃にも応答しないので、一般的には存在しないかのような状態になっている。ただし、この中継接続部６３は、例外的に、認証装置１４からチケット情報のうち、少なくともプレフィックスＰＦと、サフィックスＳＦとを特定する情報（それら自体であっても、それらのハッシュ結果であってもよい）が到来すると、当該情報を受信し、仮想専用線の設定動作を開始する。
【００３４】
そして中継接続部６３は、認証装置１４からさらにハッシュシード情報ＨＳと、仮想専用線の相手先となる末端装置１２を特定する情報（例えば末端装置１２のＩＰアドレスなど）とを受信する。このハッシュシード情報は、例えばランダムな値でよい。
【００３５】
中継接続部６３は、ここで通知された情報で特定される末端装置１２からの通信内容については、これも例外的に破棄せず、ログインを待機する。また、中継接続部６３は、末端装置１２のワンタイムパスワード発行部５４が利用するものと同じアルゴリズムで、認証装置１４から受信したハッシュシードＨＳを変換し、変換後の情報を比較用ワンタイムＩＤＰとして保持する。

【００３６】
中継接続部６３は、末端装置１２からハッシュシード情報ＨＳに基づいて生成されたワンタイムＩＤＰをログインの要求として受信する。そしてこのログインの要求を受けて、先に生成した比較用ワンタイムＩＤＰと、受信したワンタイムＩＤＰとを比較する。そして中継接続部６３は、これら比較用ワンタイムＩＤＰと、受信したワンタイムＩＤＰとが一致すると、ログインがされたものとして、要求元である末端装置１２との間に、仮想専用線を設定する。
【００３７】
さらに、この中継接続部６３は、仮想専用線を設定した後、チケット情報によるプレフィックスとサフィックス情報をキーとして、通信条件管理部６２が保持する通信条件情報を参照し、実行する処理を決定する。既に述べたように、この処理としては、例えばサービスのうち、特定の処理要求の許否判定や、仮想的なＵＲＬから実ＵＲＬ（実際に通信のためにアプリケーションサーバ１５へ送信するＵＲＬ）への変換の処理などがある。
【００３８】
中継処理部６４は、仮想専用線を介して末端装置１２から、チケット情報を含む要求の情報を受信すると、当該要求の情報に含まれるチケット情報を参照し、対応するサービス名を見いだす。ここではチケット情報に含まれるサービス名（プレフィックス）はハッシュされているものとしているので、中継処理部６４は、チケット情報に含まれるサービス名（プレフィックス）のハッシュ結果と、通信条件管理部６２が保持する通信条件情報に保持されているサービス名（プレフィックス）のハッシュ結果とを比較し、ハッシュ結果が一致するサービス名を見出す。中継処理部６４は、当該見出したサービス名に関連づけられている通信の条件の情報を参照し、見いだしたサービス名に対応して、実行するべきとして決定された処理を実行する。
【００３９】
この処理の例は、例えば要求されたサービス名から通信先となるサービス（例えばサービスの実ＵＲＬ）を特定して、当該実ＵＲＬに対応するアプリケーションサーバ１５に対し、末端装置１２から受信した要求を送信するものである。
【００４０】
また、この中継処理部６４は、処理の別の例として通信先となるサービス（例えばサービスの実ＵＲＬ）を特定した後、次のような処理を行ってもよい。すなわち既に述べたように、当該特定した実ＵＲＬに対応するアプリケーションサーバ１５の負荷の情報を取得し、当該取得した負荷の情報に応じて指定可能な実ＵＲＬ情報として予め設定された情報を参照する。そして、取得した負荷の情報に応じて、特定した実ＵＲＬが指定可能であると設定されている場合は、当該実ＵＲＬに対応するアプリケーションサーバ１５に対し、末端装置１２から受信した要求を送信する。また、取得した負荷の情報に応じて、特定した実ＵＲＬが指定可能であると設定されていなければ、末端装置１２にエラーを報知する。これにより、取得した情報により表されるアプリケーションサーバ１５の負荷が予め定めたしきい値より大きい場合に、一部の実ＵＲＬで特定される通信先へのアクセスを制限するなどの処理が実装される。
【００４１】
このようにして中継処理部６４は、チケット情報に基づいて末端装置１２に許可された通信のみを対応するアプリケーションサーバ１５へ中継するよう制御する。
【００４２】
中継処理部６４は、仮想専用線を介して末端装置１２から受信した要求の情報を、中継装置の制御部３１へ中継する。また、この中継処理部６４は、末端装置１２がチケット情報に基づいてアプリケーションサーバ１５に許可された通信のみを制御する。
【００４３】
記憶部３２は、メモリデバイスや、ディスクなどのストレージデバイスなどであり、制御部３１によって実行されるプログラムを記憶している。このプログラムは、ＤＶＤ－ＲＯＭ（Digital Versatile Disc - Read Only Memory）等のコンピュータ可読な記憶媒体

に格納された状態で提供され、この記憶部３２に複写されたものであってもよい。また、この記憶部３２は、制御部３１のワークメモリとしても動作する。さらに本実施の形態では、この記憶部３２は、図５に例示した通信条件情報を保持している。

【００４４】

第１通信部３３は、ネットワークインタフェース等であり、ネットワークインタフェース等であり、ローカルなネットワークなどの通信手段を介して、アプリケーションサーバ１５との間で情報の送受ができるように接続されている。また、第２通信部３４も、末端装置１２や、認証装置１４との間で情報を送受可能に接続されている。

【００４５】

認証装置１４の制御部４１は、ＣＰＵ（Central Processing Unit）等のプログラム制御デバイスであり、記憶部４２に格納されたプログラムに従って動作している。本実施の形態では、この認証装置１４の制御部４１は、末端装置１２からチケット情報の発行要求を受けて、チケット情報の発行処理を実行する。また、この制御部４１は、末端装置１２と中継装置１３との間で仮想専用線を設定させる処理を実行する。これらの処理の詳しい内容については、後に述べる。

【００４６】

記憶部４２は、メモリデバイスや、ディスクデバイスなどであり、制御部４１によって実行されるプログラムを保持している。このプログラムは、ＤＶＤ－ＲＯＭ（Digital Versatile Disc - Read Only Memory）等のコンピュータ可読な記憶媒体に格納された状態で提供され、この記憶部４２に複写されたものであってもよい。また、この記憶部４２は、サービスごとに予め定められているサービス名の情報と、各サービスの提供を受けるための通信先への通信を仲介する中継装置１３のアドレス（ＩＰアドレスなど）とを関連づけたテーブルを保持している（図６）。さらに記憶部４２は、制御部４１のワークメモリとしても動作する。通信部４３は、ネットワークインタフェース等であり、末端装置１２や、中継装置１３との間で情報を送受可能に接続されている。

【００４７】

［事前処理］

本実施の形態に係る通信システムは、以上のような構成を備え、次のように動作する。まず、事前に実行される処理について説明する。事前の処理は、図７に例示するように、末端装置１２と、中継装置１３と、認証装置１４との間で行われる。まず末端装置１２が、当該末端装置１２を特定する情報Ａと、接続を希望する接続先を特定する情報Ｂとを含むチケット情報の申請を認証装置１４に送信する（Ｓ１）。

【００４８】

このチケット情報の申請に含まれる、接続先を特定する情報は、サービス名ＳＮのプレフィックスＰＦ部分を含む。認証装置１４は、当該チケット情報の申請に含まれる情報からサービス名ＳＮの少なくともプレフィックスＰＦ部分を参照し、当該プレフィックスＰＦ部分で特定されるサービスとの通信を中継可能な中継装置１３を特定する（Ｓ２）。具体的に認証装置１４は、図６に例示したように、サービス名ＳＮのうちプレフィックスＰＦ部分と、当該サービスを中継可能な中継装置１３を特定する情報（中継装置１３のＩＰアドレスなど）とを関連づけたテーブルを記憶しておく。そして認証装置１４は、このテーブルを参照して、要求されたチケット情報に係るサービスとの通信を中継可能な中継装置１３を特定する。中継装置１３は、可用性向上などの目的で複数設置されていてもよい。また中継装置１３そのものに接続するためのＩＰアドレスも複数あってもよい。

【００４９】

認証装置１４は、処理Ｓ２にて特定した中継装置１３に対して、チケット情報の要求元である末端装置１２を特定する情報Ａとともに、チケット情報の申請を送信する（Ｓ３）。中継装置１３では、認証装置１４からチケット情報の申請を受け付けると、鍵情報Ｘと、申請元である認証装置１４を特定する情報ＡＡＡと、末端装置１２を特定する情報Ａと、プレフィックスＰＦ及び、当該サービスを提供するアプリケーションサーバ１５へログインする際に必要な情報であるサフィックスＳＦを含むログイン情報Ｌとを含んだチケッ

ト情報を生成する（Ｓ４）。そして中継装置１３は、このチケット情報を末端装置１２へ送信する（Ｓ５）。また、中継装置１３は、このとき、末端装置１２と中継装置１３との間の接続方法を規定する情報（中継装置１３のアドレス情報や、通信プロトコルなどに関連する情報）、並びに、予め中継装置１３から通知されている、当該サービスに係る仮想的なＵＲＬをチケット情報とともに、末端装置１２に対して送信する。末端装置１２では、このチケット情報と接続方法を規定する情報とを、対応する通信先（サービス）を特定する情報（仮想的なＵＲＬ）に関連づけて保持しておく。

【００５０】

なお、認証装置１４に対する接続のために、末端装置１２は、予め認証装置１４から認証装置１４への接続のためのチケット情報を受信して記憶しておいてもよい。

【００５１】

［通信処理］

次に、本実施の形態に係る通信システムによる、利用者側端末１１とサービスを提供するアプリケーションサーバ１５との間の通信について図８と図９とを参照しつつ説明する。

【００５２】

本実施の形態では、利用者側端末１１からの要求が行われる前に、末端装置１２と中継装置１３との間で、仮想専用線を設定しておく。すなわち末端装置１２は、電源の投入時や通信が切断された後などにおいて、図８に例示する処理を開始し、認証装置１４に対して、通信を予定しているサービスに関わるチケット情報を送信する（Ｓ１１）。

【００５３】

認証装置１４は、受信したチケット情報を参照し、利用可能なチケット情報であるか否かを調べる（Ｓ１２）。具体的には、チケット情報に自己自身を特定する情報ＡＡＡが含まれているか否かを調べるなどすればよい。認証装置１４は、利用可能なチケット情報でなければ、要求を無視する。一方、利用可能なチケット情報であると判断すると、認証装置１４は、末端装置１２と中継装置１３との間で仮想専用線を設定させる処理を開始し、認証情報の元となる情報としてハッシュシード情報ＨＳを生成して、受信したチケット情報に係るサービスを中継可能な中継装置１３のＩＰアドレスを選択する。この選択は、例えばチケット情報に係るサービスを中継可能な中継装置１３のＩＰアドレスが複数あれば、それぞれに対して要求を送信し、最も早く応答したＩＰアドレスとするなど、各ＩＰアドレスで特定される中継装置１３の処理の負荷に応じ、最も処理負荷の軽いＩＰアドレスを選択するなどとすればよい。

【００５４】

認証装置１４は、選択した中継装置１３のＩＰアドレスと、発行したハッシュシード情報ＨＳとを末端装置１２に通知し（Ｓ１３）、また、選択した中継装置１３のＩＰアドレスに対して、要求元の末端装置１２のＩＰアドレスと、発行したハッシュシード情報ＨＳとを含む、接続の予告情報を送信する（Ｓ１４）。

【００５５】

この接続の予告情報の送信は、いわゆるポート・ノッキング（port knocking）に相当する。このポート・ノッキングを受けるために、中継装置１３は予め、認証装置１４との間で仮想専用線（ＶＰＮ等）を構築しておくこととしてもよい。

【００５６】

そして末端装置１２と、中継装置１３とはそれぞれ受信したハッシュシード情報ＨＳを利用する共通の処理で、ワンタイムＩＤＰを生成する（Ｓ１５，Ｓ１６）。

【００５７】

末端装置１２は、認証装置１４から通知されたＩＰアドレスをチケット情報に関連づけて記憶しておく。また末端装置１２は、生成したワンタイムＩＤＰを、認証装置１４から通知されたＩＰアドレス宛（つまり中継装置１３宛）に送信し（Ｓ１７）、中継装置１３では、末端装置１２から送信されたワンタイムＩＤＰと、処理Ｓ１６にて自ら生成したワンタイムＩＤＰとを比較して、これらが一致するか否かにより末端装置１２のログイン処

理を行う（Ｓ１８）。ここでは各ワンタイムＩＤＰが一致した場合に認証がされたものとして、中継装置１３が、末端装置１２との間に仮想専用線（後に述べる通りサービスごとの仮想専用線なので、仮想サービス専用線と言える）を設定する（Ｓ１９）。

【００５８】

こうして以降は、利用者側端末１１の利用者が仮想的なＵＲＬを指定してサービスの要求を行うと、末端装置１２は、当該仮想的なＵＲＬに関連づけられたチケット情報と、接続方法とを参照し、当該接続方法によって、事前に（チケット情報に関連づけられたＩＰアドレスで特定される）中継装置１３との間に設定された仮想専用線を介して、サービスの要求を中継するよう、中継装置１３に要求することになる。

【００５９】

次に、この実際に利用者側端末１１の利用者がサービスを受ける手順について、図９を参照しながら説明する。

【００６０】

利用者側端末１１の利用者が、受けたいサービスに対応する仮想的なＵＲＬを指定すると、利用者側端末１１が当該指定された仮想的なＵＲＬへのアクセス要求を末端装置１２に送信する（Ｓ２１）。ここで仮想的なＵＲＬは、実際に存在し得ないＵＲＬで構わない。具体的に、この仮想的なＵＲＬは、http://myapplicationfolder/groupwareのように、ＤＮＳ（Domain Name Service）によって解決されない名称であってもよい。

【００６１】

このような仮想的なＵＲＬは、サービスに関連して、事前に利用者側に通知される。この仮想的なＵＲＬを用いると、利用者側端末１１の通信が傍受されても、傍受者は、実際の通信先であるアプリケーションサーバ１５を特定できない。

【００６２】

末端装置１２は、アクセス要求が行われた仮想的なＵＲＬに対応するチケット情報と、接続方法を規定する情報と、当該仮想的なＵＲＬへの通信を中継する中継装置１３のＩＰアドレスとを検索する（Ｓ２２）。一例としてチケット情報が、鍵情報Ｘと、認証装置１４を特定する情報ＡＡＡと、末端装置１２を特定する情報Ａと、ログイン情報Ｌとを含む場合、末端装置１２は、指定された通信先に対応し、自己を特定する情報Ａを含むチケット情報を検索する。ここで利用が許可されていないサービスのＵＲＬが指定されたとしても、末端装置１２は対応するチケット情報や接続方法を規定する情報を見いだすことができないので、以下の通信は行われず、利用者は指定したサービスを受けることはない。

【００６３】

一方、末端装置１２が、指定された仮想的なＵＲＬに対応するチケット情報と接続方法を規定する情報とを見い出した場合、末端装置１２は、当該見い出した情報で規定される接続方法で、事前に設定された仮想専用線を介して、検索により見いだされたＩＰアドレスで特定される中継装置１３との通信を開始し、当該チケット情報と、利用者により指定された仮想的なＵＲＬとを含む中継の要求を中継装置１３に送信する（Ｓ２３）。

【００６４】

中継装置１３では、当該中継の要求に含まれるチケット情報を参照し、チケット情報に含まれるサービス名（ハッシュされていてもよい）と、予め通信条件情報に保持されているサービス名（ハッシュされていてもよい）とを比較し、これらが一致するサービス名を見出す。中継装置１３は、当該見出したサービス名に関連づけられている通信の条件の情報を参照し（Ｓ２４）、要求に含まれる仮想的なＵＲＬを、通信先となるサービス（例えばサービスの実ＵＲＬ）に変換する（Ｓ２５）。ここで変換の結果として得られる実ＵＲＬには、使用するポート（ＴＣＰ（Transfer Control Protocol）のポート番号）や、ログイン情報（末端装置１２から受信したチケット情報に含まれるログイン情報Ｌの少なくとも一部など）などを含んでもよい。また、アプリケーションサーバ１５のＩＰアドレスを具体的に含むものであってもよい。またＩＰｖ６のアドレスからＩＰｖ４のアドレスへの変換も、ここで行ってもよい。すなわち、仮想的なＵＲＬとして指定されるＩＰｖ６アドレスに対応して実ＵＲＬをＩＰｖ４のアドレスで記述しておけばよい。

【００６５】
なお、この処理Ｓ２４で参照した通信条件により、通信先となるサービスへのアクセスができないこととなった場合（末端装置１２からの通信が、処理Ｓ２４で参照した通信条件を満足しない場合）は、アクセスができないことを表す情報が、末端装置１２に対して送信される。
【００６６】
また中継装置１３は、通信の条件の情報として指定された個別に実行するべきルールがある場合、当該ルールに基づいて、アプリケーションサーバ１５へのアクセスルールを決定し、また負荷分散の処理などを行ってもよい。中継装置１３は、末端装置１２から中継を要求された情報（指定された仮想的なＵＲＬ）を、サービスの実ＵＲＬ宛に（つまりアプリケーションサーバ１５へ）伝達し、また、当該実ＵＲＬで特定されるアプリケーションサーバ１５から受信した情報を末端装置１２へ送信する（通信の中継：Ｓ２６）。
【００６７】
つまり、末端装置１２は利用者向け（利用者側端末１１）のプロキシサーバであるかのように動作しており、また中継装置１３はアプリケーションサーバ１５向けのアクセス制御プロキシとして動作していることとなる。これらの動作により、末端装置１２から、アプリケーションサーバ１５が提供するサービスごとの仮想専用線が設定されることになる。既に述べたように、この仮想専用線は、いわゆるＶＰＮとは異なり、アプリケーションサーバ１５が提供するサービスごとに設定されているのである。より詳しく述べれば、互いに異なるＵＲＬごとに仮想専用線を設定してもよいし、一群のＵＲＬセットに対応して一つの仮想専用線を設定して、その内部でアクセス制御（負荷分散制御など）をすることとしても構わない。ここでは、このような仮想専用線を、ＶＰＮと区別する意味で、仮想サービス専用線と呼んでいるが、この処理Ｓ２６における通信の中継の処理が、仮想サービス専用線を通じた通信の処理に相当している。
【００６８】
また、既に述べたように、利用者が仮想的なＵＲＬの入力時に、通信プロトコルとしてＨＴＴＰ（Hyper Text Transfer Protocol）を指定したとしても、末端装置１２と中継装置１３の間は別のプロトコル（通信方法として別途定められる）を利用してもよい。
【００６９】
［接続先変更処理］
本実施の形態では、末端装置１２は中継装置１３との間に設定された仮想専用線を介して、中継装置１３に対してアプリケーションサーバ１５が提供するサービスへの通信内容を送信し、また、中継装置１３からサービスに係る情報を受信する。従って、例えばアプリケーションサーバ１５のＩＰアドレス等が変更となったとしても、末端装置１２が当該変更の内容を知る必要はなく、チケットの再発行は不要である。
【００７０】
すなわち、アプリケーションサーバ１５のＩＰアドレスが変更になった場合は、アプリケーションサーバ１５の管理者などが、中継装置１３に対して、当該変更を通知すればよい。中継装置１３は、当該通知を行ったアプリケーションサーバ１５が提供する各サービスの実ＵＲＬに対して、通知された変更後のＩＰアドレスを関連づけて保持する。この情報は、図９に示した通信処理における処理Ｓ２５にて参照される情報となる。
【００７１】
［パケットモニタ］
また本実施の形態では、中継装置１３は、一般的なネットワークプロトコルにより情報をパケット化して送受している。そこで中継装置１３は、末端装置１２から受信する情報や、アプリケーションサーバ１５から受信するパケットのうちに、予め定めたパケット破棄条件を満足する情報が含まれる場合に、当該パケットを破棄することとしてもよい。
【００７２】
ここでのパケット破棄条件には、例えばＳＱＬ（データベースへのアクセスのための言語）インジェクションを利用した情報（シングル・クオテーションを含むＳＱＬ文など）

や、予め定めたデータパターンを含むウィルス・コードなどに一致する情報であることを表す条件などがある。

【００７３】

［通信条件情報］

ここまでの説明において、中継装置１３が用いる通信条件情報は、例えばアプリケーションサーバ１５のＵＲＬを指定する情報であったり、またはアプリケーションサーバ１５の負荷に応じて指定可能なＵＲＬを選択する情報であったりするものとしたが、本実施の形態はこれに限られない。

【００７４】

例えば、この通信条件情報は、通信時に実行するべき処理を規定する情報であってもよい。また、サービスに対して要求可能な情報の一部を制限するものであってもよい。具体的には、あるサービスのＵＲＬが、

http://aaaa.bbbb.cccc/cgi-bin/service

であるとし、このサービスのＵＲＬに対してパラメータとして、「?schedule」を送信するとスケジュール情報が提供され、また別のパラメータとして「?address」と送信するとアドレス情報が提供される場合、つまり、

http://aaaa.bbbb.cccc/cgi-bin/service?schedule

としたときにスケジュール情報が提供され、

http://aaaa.bbbb.cccc/cgi-bin/service?address

としたときにアドレス情報が提供される場合、上記の通信条件情報は、このパラメータの内容によって、通信を許可したり、拒否したりする条件を表す情報であってもよい。

【００７５】

すなわち、中継装置１３は、通信条件情報として、パラメータ部分（ＣＧＩ（Common Gateway Interface）コマンドであれば、「?」より後の部分）が、「schedule」であれば通信を中継し、「address」であれば通信を拒否する情報を保持し、

http://aaaa.bbbb.cccc/cgi-bin/service?schedule

なるＵＲＬへの通信の中継が要求されたときに、当該通信を中継し、

http://aaaa.bbbb.cccc/cgi-bin/service?address

なるＵＲＬへの通信の中継が要求されたときに、当該通信を拒否する。

【００７６】

［鍵情報により接続方法を異ならせる例］

さらに、ここまでの説明において、末端装置１２と中継装置１３との間の通信は必ず仮想専用線であるものとしてきたが、これに限られない。例えば末端装置１２と中継装置１３との通信は、通常のルーティングにより行われてもよい。この場合、内部の通信は暗号化されてもよい。このように通信の態様を異ならせる場合、中継装置１３は発行する鍵情報Ｘにより、どちらの通信態様を採用するかを末端装置１２に対して通知してもよい。

【００７７】

例えば鍵情報Ｘとして、中継装置１３のＩＰアドレスと、仮想専用線を設定する場合の暗号鍵を生成するための情報（ＤＨ（Diffie-Hellman）鍵交換法を用いる場合に送信するべき情報）とを含む場合は、仮想専用線を設定するものとし、鍵情報Ｘとして、中継装置１３のＩＰアドレスと、公開鍵とを含む場合には通常のルーティングにより通信を行うものとしてもよい。

【００７８】

末端装置１２では、利用者から指定された仮想的なＵＲＬに対応するチケット情報に含まれる鍵情報Ｘを参照し、上記のいずれであるかにより、通信の態様を異ならせる。

【００７９】

なお、ここまでの説明においては、利用者からは仮想的なＵＲＬが指定され、末端装置１２において、当該仮想的なＵＲＬに対応するサービスが特定され、特定されたサービスを中継する中継装置１３との間に事前に設定された仮想専用線を介して当該指定された仮想的なＵＲＬを送信し、中継装置１３が、当該仮想的なＵＲＬを実ＵＲＬに変換して、ア

プリケーションサーバ１５へ送信することとしているが、セキュリティのレベルによっては、利用者が実ＵＲＬを指定し、中継装置１３が変換を行わずに、そのままアプリケーションサーバ１５に当該利用者が指定した実ＵＲＬを送信することとしてもよい。

【００８０】

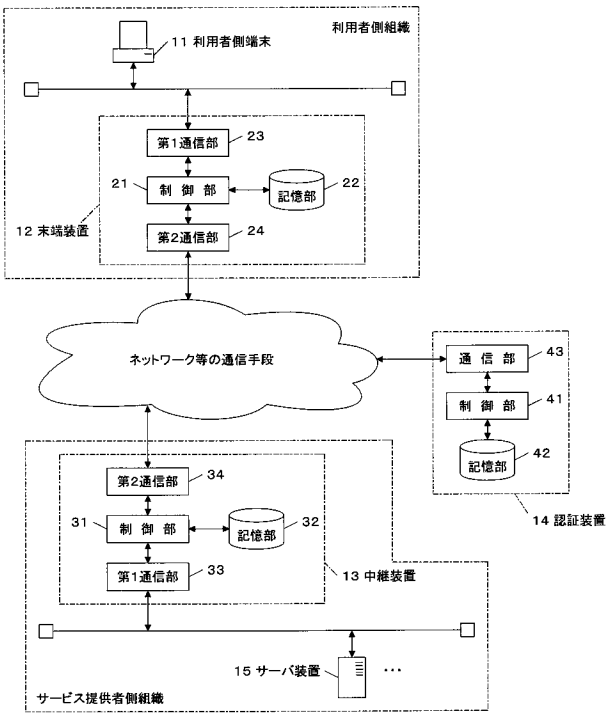
さらに、本実施の形態の末端装置１２は、認証装置１４に対して繰り返し問い合わせを行って、サービスの仮想ＵＲＬの更新を行ってもよい。

【符号の説明】

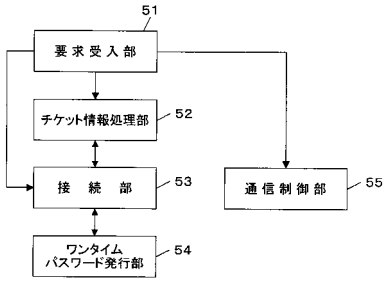
【００８１】

１　通信システム、１１　利用者側端末、１２　末端装置、１３　中継装置、１４　認証装置、１５　アプリケーションサーバ、２１，３１，４１　制御部、２２，３２，４２　記憶部、２３，２４，３３，３４，４３　通信部、５１　要求受入部、５２　チケット情報処理部、５３　接続部、５４　ワンタイムパスワード発行部、５５　通信制御部、６１　鍵情報発行部、６２　通信条件管理部、６３　中継接続部、６４　中継処理部。

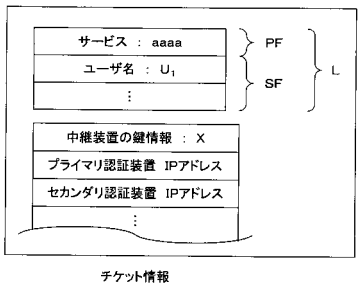
【図１】



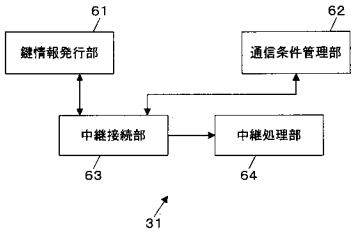
【図２】



【図３】



【図４】



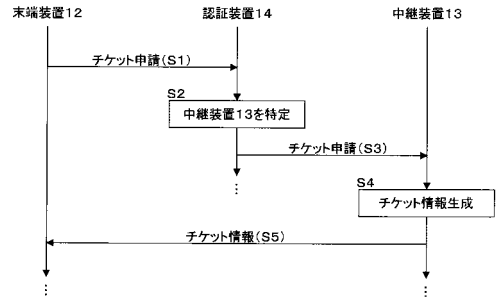
【図５】

サービス名		通　信　条　件
プレフィクス	サフィクス	
aaaa	u_1	(1)仮想的URLのxxxxをyyyyに変換 (2)yyyy/?cgi? …にのみアクセス可
aaaa	u_2	(1)仮想的URLのxxxxをzzzzに変換 (2)負荷がしきい値Th以下ならばzzz …にアクセス可
⋮	⋮	⋮

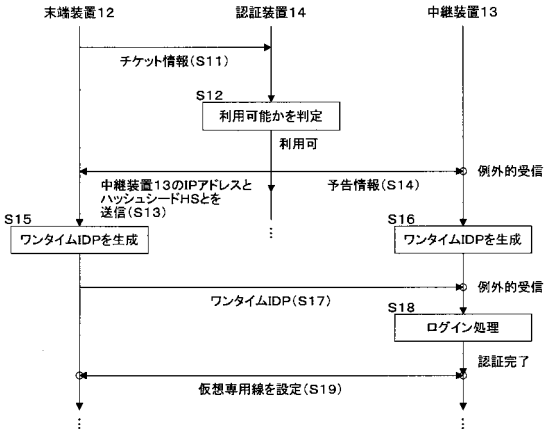
【図６】

サービス名プレフィクス	中継装置のアドレス
aaaa	192. ……
bbbb	192. ……
⋮	⋮

【図７】



【図８】



【図９】