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

特許第5437785号
(P5437785)

(45)発行日　平成26年3月12日(2014.3.12)　(24)登録日　平成25年12月20日(2013.12.20)

(51)Int.Cl.		F I		
G06F 21/31	(2013.01)	G06F	21/20	131A
G06F 21/41	(2013.01)	G06F	21/20	141
G06F 21/45	(2013.01)	G06F	21/20	145

請求項の数 7　(全 45 頁)

(21)出願番号　特願2009-288602 (P2009-288602)
(22)出願日　平成21年12月21日 (2009.12.21)
(65)公開番号　特開2011-129005 (P2011-129005A)
(43)公開日　平成23年6月30日 (2011.6.30)
審査請求日　平成24年9月10日 (2012.9.10)

(73)特許権者　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(74)代理人　100074099
弁理士　大菅　義之
(74)代理人　100133570
弁理士　▲徳▼永　民雄
(74)復代理人　100167483
弁理士　林　裕己
(72)発明者　濱田　圭
福岡県福岡市早良区百道浜２丁目２番１号　富士通九州ネットワークテクノロジーズ株式会社内

最終頁に続く

(54)【発明の名称】認証方法、変換装置、中継装置、及び該プログラム

(57)【特許請求の範囲】

【請求項１】

変換装置は、第１接続先データ及び認証済ユーザの認証情報を含んだ、該認証済ユーザに送付するサービスデータを受信し、

前記変換装置は、前記第１接続先データを特定する第２接続先データを生成し、

前記変換装置は、前記認証済ユーザの認証情報、前記第１接続先データ、および前記第２接続先データを関係付けて中継装置へ送信し、

前記中継装置は、前記認証済ユーザの認証情報、前記第１接続先データ、および前記第２接続先データを関係付けて記憶装置に格納し、

前記変換装置は、前記第１接続先データを前記第２接続先データに置換した前記サービスデータを前記認証済ユーザが操作するクライアント装置へ送信し、

前記クライアント装置は、前記置換されたサービスデータと前記認証済ユーザの操作により選択された前記第２接続先データを前記中継装置に送信し、

前記中継装置は、前記記憶装置から、前記クライアント装置から送信された第２接続先データに対応する、前記変換装置から受信した前記認証情報および前記第１接続先データを抽出し、

前記中継装置は、前記抽出した第１接続先データの示すサーバ装置へ、前記抽出した認証情報を送信し、

前記中継装置は、前記サーバ装置のアドレスを前記クライアント装置へ送信し、

前記クライアント装置は、前記アドレスと前記認証情報を用いて、前記サーバ装置と通

信する
ことを特徴とする認証方法。
【請求項２】
前記中継装置は、前記サーバ装置に対して前記認証情報を送信済である場合は、前記認証情報を送信しない
ことを特徴とする請求項１記載の認証方法。
【請求項３】
前記変換装置および前記中継装置は、前記認証済ユーザの認証情報、該認証情報と関係付けられた前記第１接続先データ、および該認証情報と関係付けられた前記第２接続先データを記憶し、一定時間経過後に消去する
ことを特徴とする請求項１記載の認証方法。
【請求項４】
第１接続先データ及び認証済ユーザの認証情報を含んだ、該認証済ユーザに送付するサービスデータを受信し、
前記第１接続先データを特定する第２接続先データを生成し、
前記認証済ユーザの認証情報、前記第１接続先データ、および前記第２接続先データを関係付けて中継装置へ送信し、
前記第１接続先データを前記第２接続先データに置換した前記サービスデータを前記認証済ユーザが操作するクライアント装置へ送信する
ことを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５】
第１接続先データ及び認証済ユーザの認証情報を含んだ、該認証済ユーザに送付するサービスデータを受信する受信部と、
前記第１接続先データを特定する第２接続先データを生成する生成部と、
前記認証済ユーザの認証情報、前記第１接続先データ、および前記第２接続先データを関係付けて中継装置へ送信し、前記第１接続先データを前記第２接続先データに置換した前記サービスデータを前記認証済ユーザが操作するクライアント装置へ送信する送信部と、
を備えることを特徴とする変換装置。
【請求項６】
認証済ユーザの認証情報、第１接続先データ、および第２接続先データを変換装置から受信し、
前記変換装置から受信した認証済ユーザの認証情報、第１接続先データ、および第２接続先データを関係付けて記憶装置に格納し、
前記認証済ユーザの操作により選択された第２接続先データを該認証済ユーザが操作するクライアント装置から受信し、
前記記憶装置から、前記クライアント装置から受信した第２接続先データに対応する、前記変換装置から受信した前記認証情報および前記第１接続先データを抽出し、
前記抽出した第１接続先データの示すサーバ装置へ、前記抽出した認証情報を送信し、
前記サーバ装置のアドレスを前記クライアント装置へ送信する
ことを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７】
変換装置から、認証済ユーザの認証情報、第１接続先データ、および第２接続先データを受信し、前記認証済ユーザの操作により選択された第２接続先データを該認証済ユーザが操作するクライアント装置から受信する受信部と、
前記変換装置から受信した前記第２接続先データ、前記認証情報および前記第１接続先データを関係付けて記憶する記憶部と、
前記記憶部から、前記クライアント装置から受信した第２接続先データに対応する、前記変換装置から受信した前記認証情報および前記第１接続先データを抽出する抽出部と、
前記抽出した第１接続先データの示すサーバ装置へ前記抽出した認証情報を送信し、前

記サーバ装置のアドレスを前記クライアント装置へ送信する送信部と、
を備えることを特徴とする中継装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本明細書はクライアント－サーバ間のアクセス制御技術に関する。
【背景技術】
【０００２】
近年、ネットワーク技術等の情報技術の発達に伴い、クライアントからサーバへのアクセス制御に関する技術も発達している。アクセス制御に関する技術として、例えば、次のログイン管理方法がある。この方法では、ユーザが認証のための情報を入力してネットワーク上の第１のサイトへログインする。そのログイン後、そのサイトからリンクを辿って第２のサイトへのログインを試みる。このとき、第１のサイトにて前記認証のための情報を第２のサイトへアクセスするためのアドレスに付加して当該アクセスに提供している。
【０００３】
また、アクセス制御に関する技術として、例えば、次のＤＮＳ（Ｄｏｍａｉｎ Ｎａｍｅ Ｓｙｓｔｅｍ）サーバがある。そのＤＮＳサーバは、前記名前解決要求メッセージに含まれる情報に基づいて、名前解決要求メッセージに含まれない送信者であるユーザに関する属性情報を取得し、当該属性情報に基づいて前記名前解決を行なう。
【０００４】
また、アクセス制御に関する技術として、例えば、次の技術がある。ＤＮＳサーバは、ホスト名に対応付けて、複数のＩＰアドレスと、個々のＩＰアドレスへのアクセスを許容するユーザ識別情報を記憶している。アドレス特定部は、その記憶された情報を参照して、ユーザの識別情報、ホスト名から、当該ユーザに対応付けられているＩＰアドレスを特定して、ユーザに回答する。
【先行技術文献】
【特許文献】
【０００５】
【特許文献１】特開２００２－２７８９３１号公報
【特許文献２】特開２００４－２６６５６８号公報
【特許文献３】特開２００３－３２２８１号公報
【発明の概要】
【発明が解決しようとする課題】
【０００６】
本実施形態では、認証情報生成時のサーバ装置への認証情報の設定処理量を削減し、認証情報の設定をサーバ装置数に非依存にする認証方法を提供する。
【課題を解決するための手段】
【０００７】
本実施形態にかかる認証方法では、変換装置は、第１接続先データ及び認証済ユーザの認証情報を含んだ、該認証済ユーザに送付するサービスデータを受信する。前記変換装置は、前記第１接続先データを特定する第２接続先データを生成する。前記変換装置は、前記認証済ユーザの認証情報、前記第１接続先データ、および前記第２接続先データを関係付けて中継装置へ送信する。前記中継装置は、前記認証済ユーザの認証情報、前記第１接続先データ、および前記第２接続先データを関係付けて記憶装置に格納する。前記変換装置は、前記第１接続先データを前記第２接続先データに置換したサービスデータを前記認証済ユーザが操作するクライアント装置へ送信する。前記クライアント装置は、前記変換された前記サービスデータと前記認証済ユーザの操作により選択された前記第２接続先データを前記中継装置に送信する。前記中継装置は、前記記憶装置から、前記クライアント装置から送信された第２接続先データに対応する、前記変換装置から受信した前記認証情報および前記第１接続先データを抽出する。前記中継装置は、前記抽出した第１接続先デ

ータの示すサーバ装置へ、前記抽出した認証情報を送信する。前記中継装置は、前記サーバ装置のアドレスを前記クライアント装置へ送信する。前記クライアント装置は、前記アドレスと前記認証情報を用いて、前記サーバ装置と通信する。

【０００８】

また、本実施形態に係る変換装置は、受信部、生成部、及び送信部を備える。受信部は、第１接続先データ及び認証済ユーザの認証情報を含んだ、該認証済ユーザに送付するサービスデータを受信する。生成部は、前記第１接続先データを特定する第２接続先データを生成する。送信部は、前記認証済ユーザの認証情報、前記第１接続先データ、および前記第２接続先データを関係付けて中継装置へ送信し、前記第１接続先データを前記第２接続先データに置換した前記サービスデータを前記認証済ユーザが操作するクライアント装置へ送信する。

【０００９】

また、本実施形態に係る中継装置は、受信部、記憶部、抽出部、及び送信部を備える。受信部は、変換装置から、認証済ユーザの認証情報、第１接続先データ、および第２接続先データを受信し、前記認証済ユーザの操作により選択された第２接続先データを該ユーザが操作するクライアント装置から受信する。記憶部は、前記変換装置から受信した前記第２接続先データ、前記認証情報および前記第１接続先データを関係付けて記憶する。抽出部は、前記記憶部から、前記クライアント装置から受信した第２接続先データに対応する、前記変換装置から受信した前記認証情報および前記第１接続先データを抽出する。送信部は、前記抽出した第１接続先データの示すサーバ装置へ前記抽出した認証情報を送信し、前記サーバ装置のアドレスを前記クライアント装置へ送信する。

【発明の効果】

【００１０】

本実施形態によれば、認証情報生成時のサーバ装置への認証情報の設定処理量を削減し、認証情報の設定をサーバ装置数に非依存にすることができる。

【図面の簡単な説明】

【００１１】

【図１】１つのサービスプロバイダ１０８のシステム内に閉じたアクセス制御システム１０１の一例を示す。

【図２】サービスプロバイダ１０８ａがＣＤＮサービスを利用する場合のアクセス制御システム１０１ａを示す。

【図３】図２のアクセス制御システム１０１ａの全体シーケンスの一例を示す。

【図４】アクセス制御システム２０の構成例を示す。

【図５】アクセス制御システム２０－１の構成例を示す。

【図６】マッピング機能４０を有するゲートウェイ装置４０－１の構成図である。

【図７】設定先選択機能３０を有するゲートウェイ装置３０－１の構成図である。

【図８】アクセス制御システム２０－１の全体シーケンスの一例を示す。

【図９】コンテンツの一覧などのリソース提供のためのレスポンスメッセージを受信した場合のマッピング機能４０の処理フローを示す。

【図１０】ポータルサーバ７からクライアント２へ送信されるリソース提供のためのレスポンスメッセージ５０の一例を示す。

【図１１】ＩＤ格納箇所定義情報２８の一例を示す。

【図１２】書き換え箇所定義情報２７の一例を示す。

【図１３】ＩＤ－ＦＱＤＮ管理テーブル４４の一例を示す。

【図１４】設定先選択機能アドレスの一例を示す。

【図１５】マッピング機能から設定先選択機能へ送信される通知メッセージの一例を示す。

【図１６】マッピング機能４０からの通知メッセージ６０を受信した場合の設定先選択機能３０の動作（Ｓ７～Ｓ８）の詳細なフローチャートを示す。

【図１７】ＩＤ－ＦＱＤＮテーブル２６の一例を示す。

【図１８】ＦＱＤＮ変換テーブル２５の一例を示す。
【図１９】クライアント２からＤＮＳサーバ１２へのＦＱＤＮについての問い合わせメッセージを受信した場合の設定先選択機能３０の動作（Ｓ１０～Ｓ１５）の詳細なフローチャートを示す。
【図２０】ＩＤ－アドレステーブル３３の一例を示す。
【図２１】設定先選択機能３０からアクセスＧＷ３へ送信される設定メッセージ６１の一例を示す。
【図２２】アクセス制御システム２０－２の構成例を示す。
【図２３】アクセス制御システム２０－２の全体シーケンスの一例を示す。
【図２４】認証サーバ６から認証済みＩＤとその有効期限についての通知メッセージ受信時のマッピング機能４０ａのフローチャートを示す。
【図２５】認証サーバ６からマッピング機能４０ａへ送信される認証済みＩＤの有効期限を通知する通知メッセージ８０の一例を示す。
【図２６】ＩＤ－ＦＱＤＮ管理テーブル４４ａの一例を示す。
【図２７】マッピング機能４０ａから設定先選択機能３０へ送信される通知メッセージ６０ａの一例を示す。
【図２８】ＩＤ－ＦＱＤＮテーブル２６ａの一例を示す。
【図２９】ＦＱＤＮ変換テーブル２５ａの一例を示す。
【図３０】ＩＤ－アドレステーブル３３ａの一例を示す。
【図３１】設定先選択機能３０からアクセスＧＷ３へ送信される設定メッセージ６１ａの一例を示す。
【図３２】マッピング機能４０，４０ａまたは設定先選択機能３０を有するゲートウェイ装置の各部の機能を実現するコンピュータのハードウェア構成の一例を示す。
【発明を実施するための形態】
【００１２】
以下では、クライアントが認証済みか否かに応じて、クライアントからサーバへのリクエストメッセージを中継または遮断するアクセス制御技術について説明する。
図１は、１つのサービスプロバイダ１０８のシステム内に閉じたアクセス制御システム１０１の一例を示す。アクセス制御システム１０１は、アクセスゲートウェイ（以降、「アクセスＧＷ」と称する）１０３と設定機能１０５で構成される。図１では、サービスプロバイダ１０８は、さらに、コンテンツサーバＡ（１０４）、認証サーバ１０６、ポータルサーバ１０７を有する。
【００１３】
アクセスＧＷ１０３はクライアント１０２からサーバへのリクエストを受信する。そして、リクエストメッセージに正当な認証済みＩＤが格納されている場合、アクセスＧＷ１０３はリクエストメッセージをサーバへ中継する。リクエストメッセージに正当な認証済みＩＤが格納されていない場合、アクセスＧＷ１０３はリクエストを遮断する。ここで認証済みＩＤとは、認証サーバ１０６がクライアント１０２の認証処理を完了した際に、クライアント１０２に送信する任意の文字列であり、クライアント１０２の認証が完了していることを一定期間保証するものである。
【００１４】
設定機能１０５はアクセスＧＷ１０３に正当な認証済みＩＤを設定する役割を担い、認証サーバ１０６からの認証済みＩＤの通知を受け付ける。図１に示すような１つのサービスプロバイダ１０８のシステム内に閉じたアクセス制御システム１０１では、設定機能１０５は同一システムのアクセスＧＷ１０３に認証済みＩＤを設定する。
【００１５】
一方、近年、サービスをクライアントに迅速に提供することを目的に、サービスプロバイダがＣＤＮ（Ｃｏｎｔｅｎｔｓ　Ｄｅｌｉｖｅｒｙ　Ｎｅｔｗｏｒｋ）サービスを利用する形態が注目されている。ＣＤＮサービスにより、サービスのコンテンツを提供するサーバ（コンテンツサーバ）及びクライアントからコンテンツサーバまでのネットワーク負

荷を分散することができる。これについて図２を用いて説明する。

【００１６】

図２は、サービスプロバイダ１０８ａがＣＤＮサービスを利用する場合のアクセス制御システム１０１ａを示す。サービスプロバイダ１０８ａがＣＤＮサービスを利用する場合、図２に示すようにコンテンツサーバ１０４はＣＤＮのサービスプロバイダ１１１のシステムに置かれ、地理的に分散配置されることとなる。したがって、アクセス制御システム１０１ａは、地理的に分散配置されたＮ個のサービスプロバイダ１１１のシステムと、１個のサービスプロバイダ１０８ａのシステムから構成される。

【００１７】

この時、クライアント１０２からコンテンツサーバ１０４へのリクエストをＤＮＳ（Ｄｏｍａｉｎ　Ｎａｍｅ　Ｓｙｓｔｅｍ）サーバ１１２が振り分ける場合、設定機能１０５はクライアント１０２のアクセス先が分からない。具体的には、クライアント１０２がコンテンツサーバ１０４のＦＱＤＮ（Ｆｕｌｌｙ　Ｑｕａｌｉｆｉｅｄ　Ｄｏｍａｉｎ　Ｎａｍｅ）の問い合わせをＤＮＳサーバ１１２へ送信した場合が考えられる。このとき、ＤＮＳサーバ１１２が、クライアント１０２のＩＰアドレスやコンテンツの負荷の状況に応じて、複数存在するコンテンツサーバ１０４のＩＰアドレスの中から適切なものを選択して回答するものとする。このような場合、設定機能５はクライアント１０２のアクセス先が分からない。

【００１８】

図２のアクセス制御システム１０１ａでは、設定機能１０５はクライアント１０２のアクセス先が分からないため、すべてのアクセスＧＷ１０３に認証済みＩＤを通知する必要がある。

【００１９】

図３は、図２のアクセス制御システム１０１ａの全体シーケンスの一例を示す。クライアント１０２は、ポータルサーバ１０７にリソース（コンテンツの一覧など）要求メッセージを送信する（Ｓ１０１）。初めてのリソース要求メッセージには認証済みＩＤが格納されていないため、ポータルサーバ１０７はクライアント１０２にリダイレクトを指示する（認証サーバ１０６にアクセスするよう指示する）レスポンスを送信する（Ｓ１０２）。レスポンスを受信したクライアント１０２は、認証サーバ１０６にリクエストを送信する。

【００２０】

クライアント１０２が認証サーバ１０６にＩＤ・パスワード等を送信するなどして認証処理を行う。認証処理が完了すると、認証サーバ１０６は認証済みＩＤを生成する（Ｓ１０３）。

【００２１】

認証サーバ１０６が生成した認証済みＩＤを設定機能１０５に通知すると、設定機能１０５は認証済みＩＤの設定を行う（Ｓ１０４）。この時点で設定機能１０５は、クライアント１０２がリクエストを送信するアクセスＧＷ１０３を特定できないため、全てのアクセスＧＷ１０３に認証済みＩＤの設定メッセージを送信して設定する。

【００２２】

認証済みＩＤの設定メッセージを受信したアクセスＧＷ１０３は、認証済みＩＤの設定が完了すると、Ａｃｋｎｏｗｌｅｄｇｅｍｅｎｔを設定機能１０５に返信する（Ｓ１０５）。設定機能１０５は、全てのアクセスＧＷ１０３に認証済みＩＤの設定が完了したことを確認して、認証サーバ１０６に設定完了通知を行う。

【００２３】

認証サーバ１０６は、設定が完了した認証済みＩＤをクライアント１０２に通知するとともに、ポータルサーバ１０７へリダイレクトを指示するレスポンスメッセージを送信する（Ｓ１０６）。メッセージを受信したクライアント１０２は、認証済みＩＤを格納したリクエストメッセージをポータルサーバ１０７へ送信する。

【００２４】

認証済みＩＤが格納されたリクエストメッセージを受信した場合、ポータルサーバ１０７は、認証サーバ１０６に対して認証済みＩＤの正当性の確認を行う（Ｓ１０７）。
その認証済みＩＤが正当なものであった場合、ポータルサーバ１０７はクライアント１０２へコンテンツの一覧などのリソースを提供する（Ｓ１０８）。この時提供されるリソースは、ＨＴＭＬ文書等であり、その中には各コンテンツの場所を表すＵＲＬ（Ｕｎｉｆｏｒｍ　Ｒｅｓｏｕｒｃｅ　Ｌｏｃａｔｏｒ）が含まれる。ＵＲＬの中には各コンテンツサーバ１０４のＦＱＤＮが含まれる。

【００２５】
ユーザがコンテンツ一覧の中から閲覧したいコンテンツを選択すると、クライアント１０２は、コンテンツサーバ１０４の名前解決を行うために、ＤＮＳサーバ１２へコンテンツサーバ１０４のＦＱＤＮの問い合わせメッセージを送信する（Ｓ１０９）。

【００２６】
ＤＮＳサーバ１１２は、クライアント１０２の送信元ＩＰアドレスやコンテンツサーバ１０４の負荷状況に基づき適切なコンテンツサーバ１０４を選択し、クライアント１０２に回答するＩＰアドレスを決める。その後、ＤＮＳサーバ１１２は、決定したＩＰアドレスを問い合わせの回答メッセージとして送信する（Ｓ１１０）。

【００２７】
アクセスＧＷ１０３は、コンテンツサーバ１０４へのリクエストを受信する必要があるため、コンテンツサーバ１０４を仮想化する。よって、クライアント１０２が送信するコンテンツサーバ１０４へのリクエストの宛先ＩＰアドレスはアクセスＧＷ１０３のＩＰアドレスである。また、ＤＮＳサーバ１１２が回答するコンテンツサーバ１０４のＩＰアドレスも、各コンテンツサーバ１０４を仮想化するアクセスＧＷ１０３のＩＰアドレスである。

【００２８】
クライアント１０２は、ＤＮＳサーバ１１２から回答として受信したＩＰアドレスを宛先ＩＰアドレスとし、コンテンツのリソース要求メッセージをその宛先アドレスへ送信する（Ｓ１１１）。この時、クライアント１０２は認証済みＩＤをメッセージ内に格納する。

【００２９】
アクセスＧＷ１０３はコンテンツのリソース要求メッセージを受信する。すると、アクセスＧＷ１０３は、要求メッセージ内の認証済みＩＤが既に設定済みの認証済みＩＤの一覧にあるかどうかを調査し、認証済みＩＤの正当性を確認する（Ｓ１１２）。認証済みＩＤが正当なものである場合、アクセスＧＷ１０３は要求メッセージをコンテンツサーバ１０４へ転送する。

【００３０】
コンテンツサーバ１０４はリソース要求メッセージに対するレスポンスメッセージをアクセスＧＷ１０３へ返信する（Ｓ１１３）。
アクセスＧＷ１０３はレスポンスメッセージをクライアント１０２へ転送する（Ｓ１１４）。

【００３１】
上述のシーケンスにおいて、１つの認証済みＩＤが生成された時に要するアクセスＧＷへの認証済みＩＤの設定の処理量がアクセスＧＷ１０３の数（分散配置されるコンテンツサーバ１０４の数）に比例して増大してしまう。すると、システム全体での性能を向上させるためにコンテンツサーバ１０４及びアクセスＧＷ１０３の数を増加させる度に、アクセスＧＷ１０３への認証済みＩＤ設定の処理量が増加することになり、十分なスケーラビリティが得られない。

【００３２】
そこで本実施形態では、１つの認証済みＩＤ生成時のアクセスＧＷへの認証済みＩＤの設定処理量を削減し、認証済みＩＤの設定をアクセスＧＷ数に非依存にすることで、高いスケーラビリティを得ることができる。以下、本実施例のシステムについて説明する。

【００３３】
本実施形態では、サービスの一覧を提供するようなポータルサーバがクライアントに通知するコンテンツサーバのＦＱＤＮを利用する。そして、設定機能が「認証サーバが認証済みＩＤを送信したクライアント」と「ＤＮＳサーバがＩＰアドレスを回答したクライアント」を対応づける。これにより、設定先のアクセスＧＷを１つに減らすことを可能とする。
【００３４】
図４は、本実施形態におけるアクセス制御システム２０の構成例を示す。設定機能２１は、ＦＱＤＮ－アドレス対応付け部２２－１、ＦＱＤＮ変換部２２－２、ＦＱＤＮ生成部２４－１、及び格納部（不図示）を備える。格納部には、ＦＱＤＮ変換テーブル２５、ＩＤ－ＦＱＤＮテーブル２６、書き換え箇所定義情報２７、ＩＤ格納箇所定義情報２８が格納されている。
【００３５】
ＦＱＤＮ生成部２４－１は、ポータルサーバ７がクライアント２に対して送信するメッセージ内のコンテンツサーバのＦＱＤＮを、認証済みＩＤ毎に書き換える。すなわち、ＦＱＤＮ生成部２４－１は、そのメッセージからコンテンツサーバのＦＱＤＮを抽出し、認証済みＩＤ毎に、この抽出したＦＱＤＮを任意のＦＱＤＮへ変換する。そして、ＦＱＤＮ生成部２４－１は、そのメッセージ内のオリジナルのＦＱＤＮ（変換前ＦＱＤＮ）を、その変換したＦＱＤＮ（変換後ＦＱＤＮ）へ書き換える。これにより、ＦＱＤＮ生成部２４－１は、各クライアント２に通知するコンテンツサーバ７のＦＱＤＮをそれぞれ異なる値にすることができる。この時、ＦＱＤＮ生成部２４－１は「変換前ＦＱＤＮ」と「変換後ＦＱＤＮ」とを対応づけた情報をＦＱＤＮ変換テーブル２５に記憶する。また、ＦＱＤＮ生成部２４－１は、「変換後ＦＱＤＮ」と「認証済みＩＤ」とを対応付けた情報をＩＤ－ＦＱＤＮテーブル２６に記憶する。
【００３６】
また、ＦＱＤＮ－アドレス対応付け部２２－１は、各クライアント２がＤＮＳサーバ１２へ問い合わせたＦＱＤＮとＤＮＳサーバ１２が回答したＩＰアドレスとを対応付けて、「変換後ＦＱＤＮ」と「ＩＰアドレス」とを対応付けた情報を作成する。
【００３７】
よって、「変換後ＦＱＤＮ」と「認証済みＩＤ」の対応関係と、「変換後ＦＱＤＮ」と「ＩＰアドレス」の対応関係とが得られる。この２つの対応関係から、「認証サーバ６が認証済みＩＤを送信したクライアント」と「ＤＮＳサーバ１２がＩＰアドレスを回答したクライアント」を対応付けることができる。
【００３８】
ここで、クライアント２がＤＮＳサーバ１２に問い合わせるＦＱＤＮは、変換後のＦＱＤＮである。そのため、その問い合わせ対象のＦＱＤＮは、ＤＮＳサーバ１２には登録されておらず、そのまま問い合わせを行うことはできない。そのためＦＱＤＮ変換部２２－２ではＦＱＤＮ変換テーブル２５を用いて、クライアント２が送信するＤＮＳサーバ１２への問い合わせメッセージ内のＦＱＤＮを、変換後ＦＱＤＮから変換前ＦＱＤＮへと書き換える。
【００３９】
本実施形態によれば、クライアント２から問い合せされたＦＱＤＮが「変換後ＦＱＤＮ」であれば、設定機能２１は、そのクライアントが既に認証されたクライアントであることが分かる。したがって、認証済みＩＤが発行され、認証済みＩＤ毎にＦＱＤＮが書き換えられたメッセージをクライアントが受信した後にセッションが切れても、クライアントは再度認証を受けなくても、ＤＮＳサーバに対して、ＦＱＤＮの問合せ要求を行うことができる。
【００４０】
なお、図４において、矢印に対して「Ｓ」＋「番号」の形式で付した符号は、図８において説明する処理を示す符号に対応するものである。以下では、本実施形態について詳述

する。
【００４１】
＜第１の実施形態＞
本実施形態では、例えば次のネットワーク構成下を例に説明する。すなわち、ポータルサーバ７と認証サーバ６が同一のシステム内に存在する。ＤＮＳサーバ１２は別のシステムである。またコンテンツサーバ４およびコンテンツサーバ４へのアクセスを制御するアクセスＧＷ３が複数のシステムに分散配置されている。
【００４２】
図５は、本実施形態におけるアクセス制御システム２０－１の構成例を示す。図５では、図４における設定機能２１を、ＩＤ－ＦＱＤＮマッピング機能（以下、マッピング機能という）４０と設定先選択機能３０に分けている。そして、それぞれの機能４０，３０をクライアント２－ポータルサーバ７間のメッセージを中継するゲートウェイと、クライアント－ＤＮＳサーバ間のメッセージを中継するゲートウェイに配備する場合について説明する。
【００４３】
クライアント２は、ポータルサーバ７、ＤＮＳサーバ１２、コンテンツサーバ４にリクエストを送信する一般的な情報処理装置である。
コンテンツサーバ４は、アクセスＧＷ３によって仮想化される。そのため、クライアント２が送信するコンテンツサーバ４へのリクエストメッセージのＩＰアドレスは、アクセスＧＷ３となる。
【００４４】
ポータルサーバ７は、クライアント２のアプリケーションプログラムからのリクエストメッセージを受信し、レスポンスメッセージとしてコンテンツの一覧を示すデータ（ここではＨＴＭＬ文書であるとする）を返信する一般的なポータルサーバである。
【００４５】
また、ポータルサーバ７は、認証済みＩＤを確認する機能を有する。すなわち、ポータルサーバ７は、リクエストメッセージに認証済みＩＤが格納されているかどうかを調査する。リクエストメッセージに認証済みＩＤが格納されていた場合、ポータルサーバ７は、認証済みＩＤを認証サーバ６に問い合わせて、認証済みＩＤの正当性を確認する。リクエストメッセージに認証済みＩＤが格納されていない場合、または認証済みＩＤが期限切れ等の理由で正当なものでない場合、ポータルサーバ７は、クライアント２に認証サーバ６へのリダイレクトを指示するレスポンスメッセージを送信する。
【００４６】
認証サーバ６は、クライアント２からの認証要求を受付け、認証処理を行う一般的な認証サーバである。認証処理が正常に完了した場合、認証サーバ６は認証済みＩＤをクライアント２に送信する。
【００４７】
ＤＮＳサーバ１２は、クライアント２からＦＱＤＮについて問い合わせメッセージを受信し、その問い合わせされたＦＱＤＮに対応するＩＰアドレスを返信する。問い合わせ対象のＦＱＤＮがコンテンツサーバ４のＦＱＤＮの場合、ＤＮＳサーバ１２は、問い合わせメッセージの送信元ＩＰアドレスやコンテンツサーバの負荷状況に応じて適切なコンテンツサーバ４を選択する。それから、ＤＮＳサーバ１２は、選択したコンテンツサーバ４を仮想化するアクセスＧＷ３のＩＰアドレスを回答として返信する。
【００４８】
アクセスＧＷ３は、設定先選択機能３０から、認証済みＩＤを設定するための設定メッセージを受付け、正当な認証済みＩＤのリストを保持する。アクセスＧＷ３は、クライアント２からコンテンツサーバ４へのリクエストメッセージを受信し、リクエストメッセージ内の認証済みＩＤを調査する。リクエストメッセージに格納されている認証済みＩＤが正当な認証済みＩＤのリストに存在する場合、アクセスＧＷ３は、リクエストメッセージをコンテンツサーバ４へ転送する。リクエストメッセージに認証済みＩＤが格納されてい

ない場合、または格納されている認証済みＩＤが正当な認証済みＩＤのリストにない場合、アクセスＧＷ３は、リクエストを遮断する。

【００４９】

コンテンツサーバ４は、クライアント２からのリクエストメッセージを受信し、クライアント２にコンテンツを提供する一般的なコンテンツサーバである。

マッピング機能４０は、本実施形態では、ポータルサーバ７のゲートウェイ装置において起動するプログラムである。なお、マッピング機能４０を行うプログラムは、ポータルサーバ７において起動するものであってもよい。マッピング機能４０は、ＦＱＤＮ生成部２４、通知部４１、ＩＤ－ＦＱＤＮ管理部４２、格納部（不図示）を有している。格納部には、書き換え箇所定義情報２７、ＩＤ格納箇所定義情報２８、設定先選択機能アドレス情報４３、ＩＤ－ＦＱＤＮ管理テーブル４４が格納されている。なお、ＦＱＤＮ生成部２４は、図４におけるＦＱＤＮ生成部２４－１に相当する。

【００５０】

ＦＱＤＮ生成部２４は、ポータルサーバ７がクライアント２へ送信するＨＴＭＬ文書内の、コンテンツサーバ４のＦＱＤＮを抽出し、この抽出したＦＱＤＮを認証済みＩＤ毎に任意のＦＱＤＮへ変換する。そして、ＦＱＤＮ生成部２４は、ＨＴＭＬ文書内のオリジナルのＦＱＤＮ（変換前ＦＱＤＮ）をその変換したＦＱＤＮ（変換後ＦＱＤＮ）へ書き換える。このとき、ＦＱＤＮ生成部２４は、ＨＴＭＬ文書内でのコンテンツサーバ７のＦＱＤＮが設定されている箇所を書き換え箇所定義情報２７より取得する。また、ＦＱＤＮ生成部２４は、メッセージ内において認証済みＩＤが設定されている箇所をＩＤ格納箇所定義情報２８より取得する。

【００５１】

ＩＤ－ＦＱＤＮ管理部４２は、ＩＤ－ＦＱＤＮ管理テーブル４４を用いて、認証済みＩＤと変換前ＦＱＤＮおよび変換後ＦＱＤＮの対応関係情報を管理する。

通知部４１は、設定先選択機能アドレス情報４３を用いて、認証済みＩＤ、変換前ＦＱＤＮ、変換後ＦＱＤＮを設定先選択機能３０のアドレスへ通知する。

【００５２】

設定先選択機能３０は、本実施形態では、ＤＮＳサーバ１２のゲートウェイ装置において起動するプログラムである。なお、設定先選択機能３０を行うプログラムは、ＤＮＳサーバ１２において起動するものであってもよい。設定先選択機能３０は、設定部３１、設定制御部３２、変換管理部２２、通信受付部３４、格納部（不図示）を有している。格納部には、ＩＤ－アドレステーブル３３、ＩＤ－ＦＱＤＮテーブル２６、ＦＱＤＮ変換テーブル２５が格納されている。なお、変換管理部２２は、図４におけるＦＱＤＮ書き戻し部２２－２とＦＱＤＮ－アドレス対応付け部２２－１を統合したものに相当する。

【００５３】

通知受付部３４は、マッピング機能４０より通知メッセージを受付ける。通知メッセージには、認証済みＩＤと変換前ＦＱＤＮおよび変換後ＦＱＤＮの組が含まれる。通知受付部３４は、通知メッセージ受信後、ＩＤ－ＦＱＤＮテーブル２６に、認証済みＩＤと変換後ＦＱＤＮの組を記憶する。また、通知受付部３４は、ＦＱＤＮ変換テーブル２５に、変換前ＦＱＤＮと変換後ＦＱＤＮの組を記憶する。

【００５４】

変換管理部２２は、クライアント２とＤＮＳサーバ１２間で受送信されるメッセージ内のＦＱＤＮの書き換えを行う。変換管理部２２は、書き換えるＦＱＤＮをＦＱＤＮ変換テーブル２５から取得する。

【００５５】

変換管理部２２は、クライアント２からＤＮＳサーバ１２へ送信される問い合わせメッセージ内のＦＱＤＮが変換後ＦＱＤＮである場合、そのメッセージ中の変換後ＦＱＤＮを変換前ＦＱＤＮへ書き換える。それから、変換管理部２２は、その書き換え後のメッセージをＤＮＳサーバ１２へ転送する。

【００５６】

変換前ＦＱＤＮへ書き換えた後のメッセージに対してＤＮＳサーバ１２から回答メッセージがあった場合、変換管理部２２は、その回答メッセージ中の変換前ＦＱＤＮを変換後ＦＱＤＮへ書き換える。変換管理部２２は、ＦＱＤＮを変換後ＦＱＤＮへ書き換えたＤＮＳサーバ１２からの回答メッセージをクライアント２へ転送する。

【００５７】

変換管理部２２は、変換後ＦＱＤＮと、そのときの回答メッセージに含まれるＩＰアドレスを対応付けて、設定制御部３２にＦＱＤＮとＩＰアドレスの対応関係情報を通知する。

【００５８】

設定制御部３２は、ＩＤ－ＦＱＤＮテーブル２６の認証済みＩＤと変換後ＦＱＤＮの対応関係と、変換管理部２２より取得する変換後ＦＱＤＮとＩＰアドレスの対応関係とに基づいて、認証済みＩＤとＩＰアドレスを対応付ける。設定制御部３２は、その対応付けた認証済みＩＤとＩＰアドレスを設定部３１へ通知する。

【００５９】

それから、設定制御部３２は、認証済みＩＤとＩＰアドレスの対応関係をＩＤ－アドレステーブル３３に記憶する。クライアント２からの問い合わせに対してＤＮＳサーバ１２から回答メッセージがあった際、得られた認証済みＩＤとＩＰアドレスの組み合わせが既にＩＤ－アドレステーブル３３にあるとする。この場合、設定制御部３２は、その認証済みＩＤとＩＰアドレスの組み合わせについては、設定部３１へは通知しない。

【００６０】

設定部３１は、設定制御部３２からの通知に従い、認証済みＩＤをアクセスＧＷ３に設定するための設定メッセージを、ＩＰアドレスで指定されるアクセスＧＷ３へ送信する。

【００６１】

図６は、本実施形態におけるマッピング機能４０を有するゲートウェイ装置４０－１の構成図である。ゲートウェイ装置４０－１は、例えばクライアント２－ポータルサーバ７間のメッセージを中継するゲートウェイ装置である。ゲートウェイ装置４０－１は、受信部４０－２、生成部４０－３、送信部４０－４を含む。

【００６２】

受信部４０－２は、ポータルサーバ７からクライアント２へのコンテンツの一覧などのリソース提供のためのメッセージを受信する。生成部４０－３は、そのリソース提供のためのメッセージ内におけるコンテンツサーバ７のＦＱＤＮと認証済みＩＤとに基づいて、認証済みＩＤ毎に、そのＦＱＤＮ（変換前ＦＱＤＮ）を特定できるＦＱＤＮ（変換後ＦＱＤＮ）を生成する。生成部４０－３は、そのメッセージ内における変換前ＦＱＤＮを変換後ＦＱＤＮに書き換える。受信部４０－２及び生成部４０－３による処理は、図８のＳ６～Ｓ７の処理に相当する。

【００６３】

送信部４０－４は、認証済みＩＤと、変換前ＦＱＤＮおよび変換後ＦＱＤＮとの対応関係を、設定先選択機能３０を有する、クライアント－ＤＮＳサーバ間のメッセージを中継するゲートウェイ３０－１に通知する。この通知処理は、図８のＳ７の処理に相当する。

【００６４】

また、送信部４０－４は、生成部４０－３にてＦＱＤＮの書き換えを行ったリソース提供のためのメッセージをクライアント２へ転送する。この転送処理は、図８のＳ９の処理に相当する。

【００６５】

図７は、本実施形態における設定先選択機能３０を有するゲートウェイ装置３０－１の構成図である。ゲートウェイ装置３０－１は、例えばクライアント－ＤＮＳサーバ間のメッセージを中継するゲートウェイ装置である。ゲートウェイ装置３０－１は、受信部３０－２、記憶部３０－３、抽出部３０－４、送信部３－５を含む。

【００６６】

受信部３０－２は、マッピング機能４０を有するゲートウェイ３０－１の送信部４０－

４から通知された、認証済みＩＤと、変換前ＦＱＤＮおよび変換後ＦＱＤＮとの対応関係情報を受信する。受信部３０－２は、この受信した認証済みＩＤと、変換前ＦＱＤＮおよび変換後ＦＱＤＮとの対応関係情報を記憶部３０－３に格納する。この受信処理は、図８のＳ７の処理に相当する。

【００６７】

また、受信部３０－２は、次の処理も行う。例えば、リソース提供のためのメッセージを受信したクライアント２において、ユーザがコンテンツ一覧の中から閲覧したいコンテンツを選択する。すると、コンテンツサーバ４の名前解決を行うために、クライアント２はＤＮＳサーバ１２へリソース提供のためのメッセージにおいて設定されていたＦＱＤＮ（変換後ＦＱＤＮ）についての問い合わせメッセージを送信する。受信部３０－２は、クライアント２からその変換後ＦＱＤＮについての問い合わせメッセージを受信する。この受信処理は、図８のＳ１０の処理に相当する。

【００６８】

抽出部３０－４は、記憶部３０－３から、クライアント装置２から受信した問い合わせメッセージ中の変換後ＦＱＤＮに対応する、認証済みＩＤと変換前ＦＱＤＮとを抽出する。

【００６９】

その後、ゲートウェイ３０－１において、クライアント２からの問い合わせメッセージ内のＦＱＤＮが変換後ＦＱＤＮである場合、そのメッセージ内における変換後ＦＱＤＮが変換前ＦＱＤＮへ書き換えられる。

【００７０】

その後、ゲートウェイ３０－１は、ＤＮＳサーバ１２に問い合わせて、その変換前ＦＱＤＮのＩＰアドレスを取得する。なお、ゲートウェイ３０－１がＤＮＳサーバ１２も兼ねていてもよい。ゲートウェイ３０－１は、認証済みＩＤとそのＩＰアドレスを対応付ける。

【００７１】

送信部３０－５は、アクセスＧＷ３に認証済みＩＤを設定するための設定メッセージを、その認証済みＩＤと対応付けたＩＰアドレス（すなわち、アクセスＧＷ３）へ送信する。この送信処理は、図８のＳ１３の処理に相当する。

【００７２】

その問い合わせメッセージに対するＤＮＳサーバ１２からの回答メッセージのＦＱＤＮは、変換前ＦＱＤＮから変換後ＦＱＤＮへ書き換えられる。送信部３０－５は、ＦＱＤＮを変換後ＦＱＤＮへ変換したＤＮＳサーバ１２からの回答メッセージをクライアント２へ転送する。これらの処理は、図８のＳ１１～Ｓ１３，Ｓ１５の処理に相当する。

【００７３】

図５～図７で説明した内容について、図８を用いて詳述する。

図８は、本実施形態におけるアクセス制御システム２０－１の全体シーケンスの一例を示す。クライアント２はポータルサーバ７にリソース（コンテンツの一覧など）要求メッセージを送信する（Ｓ１）。

【００７４】

初めてのリソース要求メッセージには認証済みＩＤが格納されていないため、ポータルサーバ７は、クライアント２にリダイレクトを指示する（認証サーバにアクセスするよう指示する）レスポンスを送信する。そのリダイレクト指示のレスポンスを受信したクライアント２は、認証サーバ６にリクエストを送信する（Ｓ２）。

【００７５】

クライアント２が認証サーバ６にＩＤ・パスワード等を送信するなどして認証処理を行う。認証処理が完了すると、認証サーバ６は認証済みＩＤを生成する（Ｓ３）。

認証サーバ６は、クライアント２に対して、認証済みＩＤを通知するとともに、ポータルサーバ７へリダイレクトを指示するレスポンスメッセージを送信する。そのレスポンスメッセージを受信したクライアント２は、認証済みＩＤを格納したリクエストメッセージ

をポータルサーバ７へ送信する（Ｓ４）。
【００７６】
ポータルサーバ７は、認証済みＩＤが格納されたリクエストメッセージを受信した場合、認証サーバ６に対して認証済みＩＤの正当性の確認を行う（Ｓ５）。
認証済みＩＤが正当なものであった場合、ポータルサーバ７はクライアント２へコンテンツの一覧などのリソースを提供するために、マッピング機能４０にそのリソースを提供する（Ｓ６）。
【００７７】
マッピング機能４０は、ポータルサーバ７からクライアント２へのコンテンツの一覧などのリソース提供のためのメッセージを受信した場合、そのメッセージ内のコンテンツサーバ７のＦＱＤＮの書き換えを行う。すなわち、マッピング機能４０は、そのリソース提供のためのメッセージ内におけるコンテンツサーバ７のＦＱＤＮと認証済みＩＤとに基づいて、認証済みＩＤ毎に、そのＦＱＤＮ（変換前ＦＱＤＮ）を特定できるＦＱＤＮ（変換後ＦＱＤＮ）を生成する。マッピング機能４０は、そのメッセージ内における変換前ＦＱＤＮを変換後ＦＱＤＮに書き換える。以降、変換前のＦＱＤＮを「ｏｒｉｇｉｎａｌ－ｆｑｄｎ」、変換後ＦＱＤＮを「ｐｒｉｖａｔｅ－ｆｑｄｎ」として説明する。
【００７８】
マッピング機能４０は、ｏｒｉｇｉｎａｌ－ｆｑｄｎとｐｒｉｖａｔｅ－ｆｑｄｎおよびメッセージ内の認証済みＩＤの対応関係を設定先選択機能３０に通知する（Ｓ７）。
その後、設定先選択機能３０は、Ａｃｋｎｏｗｌｅｄｇｅｍｅｎｔをマッピング機能４０に返信する（Ｓ８）。
【００７９】
マッピング機能４０は、Ｓ６において変換後ＦＱＤＮ（ｐｒｉｖａｔｅ－ｆｑｄｎ）に書き換えを行ったポータルサーバ７からのリソース提供のためのメッセージをクライアント２へ転送する（Ｓ９）。
【００８０】
そのリソース提供のためのメッセージを受信したクライアント２において、ユーザがコンテンツ一覧の中から閲覧したいコンテンツを選択する。すると、コンテンツサーバ４の名前解決を行うために、クライアント２はＤＮＳサーバ１２へｐｒｉｖａｔｅ－ｆｑｄｎについての問い合わせメッセージを送信する（Ｓ１０）。
【００８１】
設定先選択機能３０は、Ｓ７で通知されたｏｒｉｇｉｎａｌ－ｆｑｄｎとｐｒｉｖａｔｅ－ｆｑｄｎの関係情報に基づいて、クライアント２からのＦＱＤＮについての問い合わせメッセージ内のｐｒｉｖａｔｅ－ｆｑｄｎをｏｒｉｇｉｎａｌ－ｆｑｄｎに書き換える。それから、設定先選択機能３０は、その書き換えた問い合わせメッセージをＤＮＳサーバ１２へ転送する（Ｓ１１）。
【００８２】
ＤＮＳサーバ１２は、クライアント２の送信元ＩＰアドレスやコンテンツサーバ４の負荷状況に基づき適切なコンテンツサーバ４を選択し、クライアント２に回答するＩＰアドレスを決める。ＤＮＳサーバ１２は、決定したＩＰアドレスを、クライアント２からの問い合わせに対する回答メッセージとして送信する（Ｓ１２）。なお、コンテンツサーバ４はアクセスＧＷ３によって仮想化されているため、その決定したＩＰアドレスはアクセスＧＷ３のＩＰアドレスである。
【００８３】
設定先選択機能３０は、ＤＮＳサーバ１２からの回答メッセージ内のｏｒｉｇｉｎａｌ－ｆｑｄｎをｐｒｉｖａｔｅ－ｆｑｄｎに書き換える。また、設定先選択機能３０は、ｐｒｉｖａｔｅ－ｆｑｄｎと回答メッセージ内のＩＰアドレスとを対応づけて、記憶する。設定先選択機能３０は、そのｐｒｉｖａｔｅ－ｆｑｄｎと回答メッセージ内のＩＰアドレスの対応関係と、Ｓ７で通知されたｐｒｉｖａｔｅ－ｆｑｄｎと認証済みＩＤの対応関係とに基づいて、認証済みＩＤとＩＰアドレスを対応付けて記憶する。それから、設定先選

択機能３０は、アクセスＧＷ３に認証済みＩＤを設定するための設定メッセージを、その認証済みＩＤと対応付けたＩＰアドレス（すなわち、アクセスＧＷ３）へ送信する（Ｓ１３）。

【００８４】

上記設定メッセージを受信したアクセスＧＷ３は、認証済みＩＤの設定が完了すると、Ａｃｋｎｏｗｌｅｄｇｅｍｅｎｔを設定先選択機能３０へ返信する（Ｓ１４）。

設定先選択機能３０は、Ｓ１３にてｏｒｉｇｉｎａｌ－ｆｑｄｎからｐｒｉｖａｔｅ－ｆｑｄｎへ書き換えを行った回答メッセージをクライアント２に転送する（Ｓ１５）。

【００８５】

クライアント２はＤＮＳサーバ１２から、ｐｒｉｖａｔｅ－ｆｑｄｎについての問い合わせに対する回答として受信したＩＰアドレスを宛先ＩＰアドレスとして、その宛先ＩＰアドレスにコンテンツのリソース要求メッセージを送信する（Ｓ１６）。この時、認証済みＩＤは、そのリソース要求メッセージ内に格納されている。

【００８６】

アクセスＧＷ３はクライアント２からコンテンツのリソース要求メッセージを受信すると、要求メッセージ内の認証済みＩＤが既に設定済みの認証済みＩＤの一覧にあるかどうかを調査し、認証済みＩＤの正当性を確認する。認証済みＩＤが正当なものである場合、アクセスＧＷ３は、そのリソース要求メッセージをコンテンツサーバ４へ転送する（Ｓ１７）。

【００８７】

コンテンツサーバ４はそのリソース要求メッセージに対するレスポンスメッセージをアクセスＧＷ３へ返信する（Ｓ１８）。

アクセスＧＷ３は、そのコンテンツサーバ４からのリソース要求メッセージに対するレスポンスメッセージをクライアント２へ転送する（Ｓ１９）。

【００８８】

以上が、本実施形態の全体のシーケンスである。以下では、マッピング機能４０、設定先選択機能３０に着目して説明する。まず、マッピング機能４０の、より詳細な動作について説明する。マッピング機能４０の上記Ｓ６～Ｓ９に対応するフローチャートを図９に示す。

【００８９】

図９は、本実施形態におけるコンテンツの一覧などのリソース提供のためのレスポンスメッセージを受信した場合のマッピング機能４０の処理フローを示す。

ＦＱＤＮ生成部２４は、ポータルサーバ７からクライアント２へのコンテンツの一覧などのリソース提供のためのレスポンスメッセージを受信する（Ｓ２１）。ポータルサーバ７からクライアント２へ送信されるリソース提供のためのレスポンスメッセージ５０の一例を図１０に示す。

【００９０】

図１０において、コンテンツの一覧などのリソース提供のためのレスポンスメッセージ５０は、ＩＰヘッダ５１、ＴＰＣヘッダ５２、レイヤ７プロトコルヘッダ（例えばＨＴＴＰヘッダ）５３、メッセージコンテンツ（例えば、ＨＴＭＬ文書）等を含む。

【００９１】

ＦＱＤＮ生成部２４は、レスポンスメッセージ５０から認証済みＩＤとコンテンツサーバ４のＦＱＤＮを抽出する（Ｓ２２）。ＦＱＤＮ生成部２４は、ＩＤ格納箇所定義情報２８から、レスポンスメッセージ５０中において認証済みＩＤの抽出箇所を特定する属性情報を取得する。また、ＦＱＤＮ生成部２４は、書き換え箇所定義情報２７から、レスポンスメッセージ５０中においてコンテンツサーバ４のＦＱＤＮ抽出箇所を特定する属性情報を取得する。ここで、ＩＤ格納箇所定義情報２８の一例を図１１に示す。

【００９２】

図１１に示すＩＤ格納箇所定義情報２８では、ＨＴＴＰのヘッダフィールド名「Ｓｅｔ－Ｃｏｏｋｉｅ」で指定されるＣｏｏｋｉｅの内、ＮＡＭＥが「Ａｕｔｈｅ」であるもの

が認証済みＩＤであることを定義している。よって、レスポンスメッセージ５０を受信したＦＱＤＮ生成部２４は、ＩＤ格納箇所定義情報２８に基づいて、ＨＴＴＰヘッダ５３の「Ｓｅｔ－Ｃｏｏｋｉｅ：Ａｕｔｈｅ＝１２３４５；」から文字列「１２３４５」を認証済みＩＤとして抽出する。

【００９３】

次に、書き換え箇所定義情報２７の一例を図１２に示す。図１２に示す書き換え箇所定義情報２７では、ＨＴＭＬ文書のＡ要素のＨＲＥＦという属性を書き換え箇所として定義するものである。よって、ＦＱＤＮ生成部２４は、書き換え箇所定義情報２７に基づいて、ＨＴＭＬ文書５４の「＜Ａ　ＨＲＥＦ＝“Ｈｔｔｐ：／／ｓｒｖ１．ｅｘａｍｐｌｅ．ｃｏｍ／ｃｏｎｔｅｎｔ１”＞」から、文字列「ｓｒｖ１．ｅｘａｍｐｌｅ．ｃｏｍ」を抽出する。この文字列「ｓｒｖ１．ｅｘａｍｐｌｅ．ｃｏｍ」は、コンテンツサーバ４のＦＱＤＮとして抽出されたものである。

【００９４】

ＦＱＤＮ生成部２４は、抽出した認証済みＩＤ及びコンテンツサーバのＦＱＤＮをＩＤ－ＦＱＤＮ管理部４２に渡す。

ＩＤ－ＦＱＤＮ管理部４２は、認証済みＩＤと変換前ＦＱＤＮをキーにＩＤ－ＦＱＤＮ管理テーブル４４を検索する（Ｓ２３）。ここで、ＩＤ－ＦＱＤＮ管理テーブル４４の一例を図１３に示す。

【００９５】

図１３において、ＩＤ－ＦＱＤＮ管理テーブル４４は、「認証済みＩＤ」と、その認証済みＩＤに対応する「変換前ＦＱＤＮ」及び「変換後ＦＱＤＮ」の組を１つのエントリとして持つ。

【００９６】

Ｓ２３での検索の結果、該当するエントリが存在しない場合（Ｓ２３で「Ｎｏ」）、ＩＤ－ＦＱＤＮ管理部４２は、認証済みＩＤとコンテンツサーバ４のＦＱＤＮとの組み合わせに対応する任意のＦＱＤＮ（変換後ＦＱＤＮ）を生成する。例えば、ＩＤ－ＦＱＤＮ管理部４２は、認証済みＩＤ「１２３４５」とコンテンツサーバ４のＦＱＤＮ「ｓｒｖ１．ｅｘａｍｐｌｅ．ｃｏｍ」の組み合わせに対応するＦＱＤＮ「ｃｃｃ．ｅｘａｍｐｌｅ．ｃｏｍ」を変換後ＦＱＤＮとして生成する。それから、ＩＤ－ＦＱＤＮ管理部４２は、その生成した変換後ＦＱＤＮを、変換前ＦＱＤＮと認証済みとに対応付けて、ＩＤ－ＦＱＤＮ管理テーブル４４に登録する（Ｓ２４）。

【００９７】

ＩＤ－ＦＱＤＮ管理部４２は、認証済みＩＤ「１２３４５」、コンテンツサーバのＦＱＤＮ「ｓｒｖ１．ｅｘａｍｐｌｅ．ｃｏｍ」、変換後ＦＱＤＮ「ｃｃｃ．ｅｘａｍｐｌｅ．ｃｏｍ」の組を通知部４１へ渡す。

【００９８】

通知部４１は、設定先選択機能アドレス情報４３を参照する。ここで、設定先選択機能アドレスの一例を図１４に示す。図１４において、設定先選択機能アドレス情報４３には、設定先選択機能アドレスとして例えば「１９２．０．２．１１１」が格納されている。

【００９９】

通知部４１は、設定先選択機能アドレス情報４３から得られたＩＰアドレス「１９２．０．２．１１１」を宛先として、認証済みＩＤ、コンテンツサーバ４の変換前ＦＱＤＮ、変換後ＦＱＤＮの組を含む通知メッセージを設定先選択機能３０に送信する（Ｓ２５）。ここで、マッピング機能から設定先選択機能へ送信される通知メッセージの一例を図１５に示す。

【０１００】

図１５において、通知メッセージ６０は、認証済みＩＤ「１２３４５」、コンテンツサーバ４の変換前ＦＱＤＮ「ｓｒｖ１．ｅｘａｍｐｌｅ．ｃｏｍ」、変換後ＦＱＤＮ「ｃｃｃ．ｅｘａｍｐｌｅ．ｃｏｍ」の組を含む。

【０１０１】

通知部４１は、その通知メッセージ６０に対して設定先選択機能３０からＡｃｋｎｏｗｌｅｄｇｅｍｅｎｔを受信すると、Ｓ２５の通知処理が完了する。すると、通知部４１は、ＩＤ－ＦＱＤＮ管理部４２に通知メッセージ６０の送信処理が完了したことを通知する。

【０１０２】

Ｓ２３での検索の結果、該当するエントリが存在する場合（Ｓ２３で「Ｙｅｓ」）、またはＳ２５における通知メッセージ６０の通知処理が完了した場合、ＩＤ－ＦＱＤＮ管理部４２は、次を行う。すなわち、ＩＤ－ＦＱＤＮ管理部４２は、コンテンツサーバ７の変換前ＦＱＤＮ「ｓｒｖ１．ｅｘａｍｐｌｅ．ｃｏｍ」と変換後ＦＱＤＮ「ｃｃｃ．ｅｘａｍｐｌｅ．ｃｏｍ」をＦＱＤＮ生成部２４に渡す。

【０１０３】

ＦＱＤＮ生成部２４は、Ｓ２２にて抽出したＨＴＭＬ文書５４内のコンテンツサーバ４のＦＱＤＮ「ｓｒｖ１．ｅｘａｍｐｌｅ．ｃｏｍ」を、変換後ＦＱＤＮ「ｃｃｃ．ｅｘａｍｐｌｅ．ｃｏｍ」に書き換える（Ｓ２６）。

【０１０４】

ＦＱＤＮ生成部２４は、書き換えたＨＴＭＬ文書５４を含むレスポンスメッセージ５０をクライアント２に送信する（Ｓ２７）。

次に、上述した設定先選択機能３０について、より詳細な動作について説明する。設定先選択機能３０の動作は、マッピング機能４０からの通知メッセージ６０を受信した場合（Ｓ７～Ｓ８）と、クライアント２からＤＮＳサーバ１２への問い合わせメッセージを受信した場合（Ｓ１０～Ｓ１５）とに分かれる。まずは、マッピング機能４０からの通知メッセージ６０を受信した場合の設定先選択機能３０の動作（Ｓ７～Ｓ８）の詳細なフローチャートを図１６に示す。

【０１０５】

通知受付部３４は、マッピング機能４０からの通知メッセージ６０を受信する（Ｓ３１）。図１５に示すように、通知メッセージ６０には認証済みＩＤ、変換前ＦＱＤＮ、及び変換後ＦＱＤＮが含まれる。

【０１０６】

通知受付部３４は、認証済みＩＤと変換後ＦＱＤＮの組をＩＤ－ＦＱＤＮテーブル２６に登録する（Ｓ３２）。また、通知受付部３４は、変換前ＦＱＤＮと変換後ＦＱＤＮの組をＦＱＤＮ変換テーブル２５に登録する。ＩＤ－ＦＱＤＮテーブル２６の一例を図１７に示す。ＦＱＤＮ変換テーブル２５の一例を図１８に示す。

【０１０７】

ＦＱＤＮ変換テーブル２５及びＩＤ－ＦＱＤＮテーブル２６へのエントリの登録が完了すると、通知受付部３４はマッピング機能４０にＡｃｋｎｏｗｌｅｄｇｍｅｎｔを返信する（Ｓ３３）。

【０１０８】

次に、クライアント２からＤＮＳサーバ１２へのＦＱＤＮについての問い合わせメッセージを受信した場合の設定先選択機能３０の動作（Ｓ１０～Ｓ１５）の詳細なフローチャートを図１９に示す。

【０１０９】

まず、変換管理部２２は、クライアント２からＤＮＳサーバ１２への問い合わせメッセージを受信する（Ｓ４１）。図８のＳ１０において説明したように、この問い合わせメッセージにおいて問い合わせ対象のＦＱＤＮは、変換後ＦＱＤＮ（ｐｒｉｖａｔｅ－ｆｑｄｎ）である。

【０１１０】

変換管理部２２は、問い合わせ対象のＦＱＤＮをキーに、ＦＱＤＮ変換テーブル２５の列「変換後ＦＱＤＮ」を検索する（Ｓ４２）。Ｓ４２において、ＦＱＤＮ変換テーブル２５にヒットするエントリが存在しない場合（Ｓ４２で「Ｎｏ」）、この問合せは、変換後ＦＱＤＮを受信したクライアント以外のクライアントからのＤＮＳサーバ１２への問い合

わせである。この場合、変換管理部２２は、ＤＮＳサーバ１２へ問い合わせメッセージを転送し（Ｓ４３）、ＤＮＳサーバ１２から回答メッセージを受信すると、Ｓ５１へ進む。

【０１１１】

Ｓ４２においてＦＱＤＮ変換テーブル２５にヒットするエントリが存在し、変換前ＦＱＤＮが得られた場合について説明する（Ｓ４２で「Ｙｅｓ」）。この場合、変換管理部２２は、この問合せが、変換後ＦＱＤＮを受信したクライアント２からのＤＮＳサーバ１２への問い合わせであることがわかる。

【０１１２】

このとき、変換管理部２２は、問い合わせメッセージのＦＱＤＮ（変更後ＦＱＤＮ）を、Ｓ４２にてＦＱＤＮ変換テーブル２５を検索して得られた変換前ＦＱＤＮに書き換える（Ｓ４４）。例えば、ＦＱＤＮ変換テーブル２５の内容が図１８の通りで、問い合わせ対象のＦＱＤＮが「ｃｃｃ．ｅｘａｍｐｌｅ．ｃｏｍ」であった場合、変換管理部２２は、そのＦＱＤＮを「ｓｒｖ１．ｅｘａｍｐｌｅ．ｃｏｍ」に書き換える。

【０１１３】

変換管理部２２は、問い合わせメッセージをＤＮＳサーバ１２へ送信し、ＤＮＳサーバ１２からの回答メッセージを得る（Ｓ４５）。

変換管理部２２は、回答メッセージ内の変換前ＦＱＤＮを、変換後ＦＱＤＮに書き換える（Ｓ４６）。例えば、変換管理部２２は、回答メッセージ内の「ｓｒｖ１．ｅｘｍａｐｌｅ．ｃｏｍ」を「ｃｃｃ．ｅｘａｍｐｌｅ．ｃｏｍ」に書き換える。

【０１１４】

また、変換管理部２２は、変換後ＦＱＤＮとＤＮＳサーバ１２からの回答メッセージに含まれるＩＰアドレスとを対応づける。それから、変換管理部２２は、その対応付けた変換後ＦＱＤＮとＩＰアドレスの組を設定制御部３２へ渡す。例えば、回答に含まれるＩＰアドレスが「１９２．０．２．２２２」であった場合、変換管理部２２は、「ｃｃｃ．ｅｘａｍｐｌｅ．ｃｏｍ」と「１９２．０．２．２２２」の組を設定制御部３２へ渡す。

【０１１５】

設定制御部３２は、変換後ＦＱＤＮをキーにＩＤ－ＦＱＤＮテーブル２６を検索し、認証済みＩＤを得る（Ｓ４７）。よって、設定制御部３２は、認証済みＩＤとＩＰアドレスを対応づけることが出来る。例えば、ＩＤ－ＦＱＤＮテーブル２６が図１７の場合、設定制御部３２は、変換後ＦＱＤＮ「ｃｃｃ．ｅｘａｍｐｌｅ．ｃｏｍ」をキーに検索を行うと、認証済みＩＤ「１２３４５」が得られる。この時、対応付けられる認証済みＩＤとＩＰアドレスは、「１２３４５」と「１９２．０．２．２２２」である。

【０１１６】

設定制御部３２は、認証済みＩＤとＩＰアドレスの組をキーにＩＤ－アドレステーブル３３を検索する（Ｓ４８）。ここで、ＩＤ－アドレステーブル３３の一例を図２０に示す。図２０では、ＩＤ－アドレステーブル３３は、認証済みＩＤとＩＰアドレスから構成される。

【０１１７】

Ｓ４８における検索の結果、ＩＤ－アドレステーブル３３において、認証済みＩＤとＩＰアドレスの組が既に登録済みである場合（Ｓ４８で「Ｙｅｓ」）、設定制御部３２は変換管理部２２に制御を渡し、Ｓ５１へ進む。Ｓ４８における検索の結果、ＩＤ－アドレステーブル３３において、認証済みＩＤとＩＰアドレスの組が未登録である場合（Ｓ４８で「Ｎｏ」）、Ｓ４９へ進む。例えば、図２０において、認証済みＩＤ「１２３４５」とＩＰアドレス「１９２．０．２．２２２」との組を検索すると、この組はＩＤ－アドレステーブル３３に未登録であるため、Ｓ４９へ進む。

【０１１８】

設定制御部３２は認証済みＩＤとＩＰアドレスの組をＩＤ－アドレステーブル３３に登録し（Ｓ４９）、認証済みＩＤとＩＰアドレスの組を設定部３１に渡す。

設定部３１は、設定制御部３２から渡された認証済みＩＤの設定メッセージを、設定制御部３２から渡されたＩＰアドレス宛てに送信する（Ｓ５０）。そのＩＰアドレスは、分

散配置されたアクセスＧＷ３の内の１つのＩＰアドレスである。設定先選択機能３０からアクセスＧＷ３へ送信される設定メッセージ６１の一例を図２１に示す。図２１において、設定メッセージ６１には認証済みＩＤ「１２３４５」が設定されている。

【０１１９】

アクセスＧＷ３は、その設定メッセージ６１を受信すると、認証済みＩＤを設定する。アクセスＧＷ３は、認証済みＩＤの設定が完了すると、設定先選択機能３０にＡｃｋｎｏｗｌｅｄｇｅｍｅｎｔを返信する。

【０１２０】

設定部３１は、設定先選択機能３０からのＡｃｋｎｏｗｌｅｄｇｅｍｅｎｔを受信すると、設定制御部３２に認証済みＩＤの設定の完了を通知する。すると、設定制御部３２は変換管理部２２に制御を渡す。

【０１２１】

変換管理部２２は、ＤＮＳサーバ１２からの回答メッセージをクライアント２へ転送する（Ｓ５１）。

本実施形態によれば、クライアントと認証サーバ間、クライアントとＤＮＳサーバ間にＨＴＴＰプロキシサーバやＤＮＳキャッシュサーバが存在する場合でも、次のことができる。すなわち、「認証サーバが認証済みＩＤを送信したクライアント」と「ＤＮＳサーバがＩＰアドレスを回答したクライアント」を対応づけることができる。そのため、認証済みＩＤの設定先を常にそれぞれのクライアントがアクセスするアクセスＧＷのみにすることが可能である。よって認証済みＩＤの設定処理量はアクセスＧＷ数に非依存となり、分散配置されるコンテンツサーバ及びアクセスＧＷ数に応じてシステム全体の性能向上が見込める。

【０１２２】

また、クライアント２から問い合せされたＦＱＤＮが「変換後ＦＱＤＮ」であれば、設定先選択機能２１は、そのクライアントが既に認証されたクライアントであることが分かる。したがって、認証済みＩＤが発行され、ポータルサーバ７から認証済みＩＤ毎にＦＱＤＮが書き換えられたメッセージをクライアントが受信した後にセッションが切れたとする。この場合、クライアントは再度認証を受けなくても、ＤＮＳサーバに対して、ＦＱＤＮの問合せ要求を行うことができる。すなわち、図８のＳ９とＳ１０との間でセッションが切れた後、Ｓ１０からシーケンスを開始しても、クライアントから問い合せされたＦＱＤＮが「変換後ＦＱＤＮ」であれば、既に認証されたクライアントであることを確認することができる。

【０１２３】

＜第２の実施形態＞

本実施形態では、認証済みＩＤの有効期限に従って、マッピング機能が持つＩＤ－ＦＱＤＮ管理テーブル及び、設定先選択機能が持つＩＤ－ＦＱＤＮテーブル、ＦＱＤＮ変換テーブル、ＩＤ－アドレステーブルの各エントリに有効期限を設定する例を示す。なお、本実施形態において、第１の実施形態と同一の構成要素については同一の符号を付し、その説明を省略する。

【０１２４】

図２２は、本実施形態におけるアクセス制御システム２０－２の構成例を示す。アクセス制御システム２０－２において、マッピング機能４０ａは、図５のマッピング機能４０に通知受付部４５、有効期限管理部４６を追加したものである。また、設定先選択機能３０ａは、図５の設定先選択機能３０に有効期限管理部４７を追加したものである。

【０１２５】

図２３は、本実施形態におけるアクセス制御システム２０－２の全体シーケンスの一例を示す。Ｓ１～Ｓ３については、図８と同様である。

Ｓ３において認証サーバ６は認証済みＩＤを生成すると、その生成した認証済みＩＤの有効期限を設定する。それから、認証サーバ６は、認証済みＩＤとその有効期限をマッピング機能４０ａに通知する（Ｓ３－１）。

【０１２６】
マッピング機能４０ａは、認証サーバ６からの通知を受信すると、ＩＤ－ＦＱＤＮ管理テーブル４４ａに認証済みＩＤと有効期限を格納する。その後、マッピング機能４０ａは、認証サーバ６にＡｃｋｎｏｗｌｅｄｇｅｍｅｎｔを送信する（Ｓ３－２）。
【０１２７】
Ｓ４～Ｓ６については、図８と同様である。
それから、マッピング機能４０ａは、ポータルサーバ７からクライアント２へのコンテンツの一覧などのリソース提供のためのメッセージを受信する。すると、マッピング機能４０ａは、図８のＳ７で説明したのと同様に、そのメッセージ内のコンテンツサーバ７のＦＱＤＮの書き換えを行う。それから、マッピング機能４０は、ｏｒｉｇｉｎａｌ－ｆｑｄｎと、ｐｒｉｖａｔｅ－ｆｑｄｎと、メッセージ内の認証済みＩＤとの対応関係情報、及び認証済みＩＤの有効期限を設定先選択機能３０ａに通知する（Ｓ７－１）。
【０１２８】
Ｓ８～Ｓ１２については、図８と同様である。
それから、設定先選択機能３０ａは、ＤＮＳサーバ１２から、クライアント２からの問い合わせに対する回答メッセージを受信する。すると、設定先選択機能３０ａは、図８のＳ１３で説明したのと同様に、その回答メッセージ内のｏｒｉｇｉｎａｌ－ｆｑｄｎをｐｒｉｖａｔｅ－ｆｑｄｎに書き換える。それから、設定先選択機能３０ａは、ｐｒｉｖａｔｅ－ｆｑｄｎと回答メッセージ内のＩＰアドレスを対応づける。設定先選択機能３０ａは、ｐｒｉｖａｔｅ－ｆｑｄｎと回答メッセージ内のＩＰアドレスとの対応関係と、Ｓ７－１で通知されたｐｒｉｖａｔｅ－ｆｑｄｎと認証済みＩＤとの対応関係に基づいて、認証済みＩＤとＩＰアドレスを対応付ける。それから、設定先選択機能３０ａは、有効期限を含む認証済みＩＤを設定するための設定メッセージを、その認証済みＩＤと対応付けたＩＰアドレス（すなわち、アクセスＧＷ３）へ送信する（Ｓ１３－１）。
【０１２９】
Ｓ１４～Ｓ１９については、図８と同様である。
有効期限管理部４６，４７はそれぞれ、認証済みＩＤの有効期限を管理する。認証済みＩＤはその有効期限が過ぎると、有効期限管理部４６は、ＩＤ－ＦＱＤＮ管理テーブル４４ａからその有効期限が過ぎた認証済みＩＤに関係するエントリを削除する。また、認証済みＩＤはその有効期限が過ぎると、有効期限管理部４７は、ＩＤ－ＦＱＤＮテーブル２６ａ、ＦＱＤＮ変換テーブル２５ａ、ＩＤ－アドレステーブル３３ａからその有効期限が過ぎた認証済みＩＤに関係するエントリを削除する。
【０１３０】
図２４は、本実施形態における、認証サーバ６から認証済みＩＤとその有効期限についての通知メッセージ受信時のマッピング機能４０ａのフローチャートを示す。図２４のフローチャートは、図２３のＳ３－１～Ｓ３－２の詳細を示す。
【０１３１】
まず、通知受付部４５は、認証サーバ６からの通知メッセージ８０を受信する（Ｓ５１）。認証サーバ６からマッピング機能４０ａへ送信される認証済みＩＤの有効期限を通知する通知メッセージ８０の一例を図２５に示す。図２５に示すように、通知メッセージ８０は、認証済みＩＤと、認証済みＩＤの有効期限を有している。
【０１３２】
通知受付部４５は、通知メッセージ８０から得られる認証済みＩＤとその有効期限をＩＤ－ＦＱＤＮ管理テーブル４４ａに登録する（Ｓ５２）。ここで、ＩＤ－ＦＱＤＮ管理テーブル４４ａの一例を図２６に示す。ＩＤ－ＦＱＤＮ管理テーブル４４ａは、図１３のＩＤ－ＦＱＤＮ管理テーブル４４に、データ項目「有効期限」が追加されたものである。
【０１３３】
認証済みＩＤとその有効期限の登録後、通知受付部４５は認証サーバ６にＡｃｋｎｏｗｌｅｄｇｅｍｅｎｔを送信する（Ｓ５３）。
なお、マッピング機能４０ａの、ポータルサーバ７からのコンテンツの一覧などのリソ

ース提供のためのレスポンスメッセージ受信時の動作（Ｓ６～Ｓ９）は、図９のフローと同様である。

【０１３４】

次に、設定先選択機能３０ａの動作について説明する。設定先選択機能３０ａの動作は、基本的には図１６と同様である。ただし、マッピング機能４０ａから設定先選択機能３０ａへ送信される通知メッセージ６０ａ（図２７）には、認証済みＩＤの「有効期限」が設定される。また、ＩＤ－ＦＱＤＮテーブル２６ａ（図２８）、ＦＱＤＮ変換テーブル２５ａ（図２９）、ＩＤ－アドレステーブル３３ａ（図３０）にも、認証済みＩＤの「有効期限」が設定される。また、設定先選択機能３からアクセスＧＷ３へ送信される設定メッセージ６１ａ（図３１）にも、認証済みＩＤの「有効期限」が設定される。

【０１３５】

認証済みＩＤの「有効期限」が過ぎれば、有効期限管理部４６は、ＩＤ－ＦＱＤＮ管理テーブル４４ａから、その「有効期限」を含むエントリを削除する。同様に、認証済みＩＤの「有効期限」が過ぎれば、有効期限管理部４７は、ＩＤ－ＦＱＤＮテーブル２６ａ（図２８）、ＦＱＤＮ変換テーブル２５ａ（図２９）、ＩＤ－アドレステーブル３３ａ（図３０）から、その「有効期限」を含むエントリを削除する。

【０１３６】

図１９において、例えば、有効期限が過ぎた認証済みＩＤに対応する変換後ＦＱＤＮについての問い合わせがクライアント２からあったとする（Ｓ４１）。しかしながら、ＦＱＤＮ変換テーブル２５ａには、問い合わせ対象のＦＱＤＮを含むエントリが存在しない（Ｓ４２で「Ｎｏ」）。この場合、換え管理部２２は、ＤＮＳサーバ１２へ問い合わせメッセージを転送し（Ｓ４３）、ＤＮＳサーバ１２から回答メッセージを受信すると、その回答メッセージをクライアント２へ転送する（Ｓ５１）。なお、ここでのＤＮＳサーバ１２からの回答メッセージは、そのＦＱＤＮに対応するＩＰアドレスがない旨のエラーメッセージである。

【０１３７】

本実施形態によれば、第１の実施形態の効果に加えて、さらに、認証済みＩＤの「有効期限」を設けることにより、その有効期限が過ぎた場合、その「有効期限」を含むエントリが全てのテーブルから削除される。これにより、使用されなくなった認証済みＩＤが登録されたままになるのを防止することができる。したがって、認証済みＩＤの信頼性を高めることができる。また、記憶領域の容量を必要以上に圧迫することがなく、メモリ資源を節約することができる。

【０１３８】

次に図３２について説明する。図３２は、第１または第２の実施形態におけるマッピング機能４０，４０ａまたは設定先選択機能３０，３０ａを有するゲートウェイ装置の各部の機能を実現するコンピュータのハードウェア構成の一例を示す。

【０１３９】

図３２において、コンピュータ９０は、ＣＰＵ９１、ＲＯＭ９２、ＲＡＭ９３、ハードディスク装置（ＨＤＤ）９４、インタフェース装置（Ｉ／Ｆ）９５、入力装置９６、出力装置９７を備えている。これらの要素はいずれもバス９８に接続されており、ＣＰＵ９１の管理の下で各種のデータを相互に授受することができる。

【０１４０】

ＣＰＵ９１は、マッピング機能４０，４０ａを有するゲートウェイ装置または設定先選択機能３０，３０ａを有するゲートウェイ装置全体の動作を制御する中央演算処理装置である。ＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）９２は、各種の制御動作を行うための制御プログラムを格納する。ＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）９３は、ＣＰＵ９１が制御プログラムを実行する際に必要に応じて使用する作業用の一時記憶領域を提供する。ＲＯＭ９２には、ＣＰＵ９１が実行する基本制御プログラムが予め格納されている。ＲＯＭ９２に格納されている基本制御プログラムをＣＰＵ９１が読み出してその実行を開始すると、コンピュータ９０の各部の制御が可能となる。

【０１４１】
ＨＤＤ９４は、ＣＰＵ９１によって実行される各種の制御プログラム、本実施形態に係るプログラムやデータ、テーブル等を記憶しておく記憶装置である。例えば、コンピュータ９０が第１の実施形態のマッピング機能４０を有するゲートウェイ装置の場合、ＨＤＤ９４には、書き換え箇所定義情報２７、ＩＤ格納箇所定義情報２８、設定先選択機能アドレス情報４３、ＩＤ－ＦＱＤＮ管理テーブル４４が格納されている。また、例えば、コンピュータ９０が第１の実施形態の設定先選択機能３０を有するゲートウェイ装置の場合、ＨＤＤ９４には、ＩＤ－アドレステーブル３３、ＩＤ－ＦＱＤＮテーブル２６、ＦＱＤＮ変換テーブル２５が格納されている。例えば、コンピュータ９０が第２の実施形態のマッピング機能４０ａを有するゲートウェイ装置の場合、ＨＤＤ９４には、書き換え箇所定義情報２７、ＩＤ格納箇所定義情報２８、設定先選択機能アドレス情報４３、ＩＤ－ＦＱＤＮ管理テーブル４４ａが格納されている。また、例えば、コンピュータ９０が第２の実施形態の設定先選択機能３０ａを有するゲートウェイ装置の場合、ＨＤＤ９４には、ＩＤ－アドレステーブル３３ａ、ＩＤ－ＦＱＤＮテーブル２６ａ、ＦＱＤＮ変換テーブル２５ａが格納されている。
【０１４２】
ＣＰＵ９１はハードディスク装置９４に記憶されている上述した実施形態に係るマッピング機能４０，４０ａ又は設定先選択機能３０，３０ａを実現する処理プログラム（例えば、図９、図１６、図１９、図２４等）を読み出して実行する。
【０１４３】
Ｉ／Ｆ装置９５は、外部コンピュータ等とコンピュータ９０との間の各種データの送受信の管理を行う。入力装置９６は、例えばキーボード装置やマウス装置である。出力装置９７は、例えばディスプレイ、プリンタ等の出力装置である。
【０１４４】
上記の実施形態によれば、認証方法は以下のようになる。変換装置（例えば、マッピング機能４０，４０ａ）は、第１接続先データ（例えば、変換前ＦＱＤＮ）及び認証済ユーザの認証情報を含んだ、該認証済ユーザに送付するサービスデータを受信する（Ｓ６，Ｓ２１）。
【０１４５】
前記変換装置は、前記第１接続先データを特定する第２接続先データ（例えば、変換後ＦＱＤＮ）を生成する（Ｓ２４）。前記変換装置は、前記認証済ユーザの認証情報、前記第１接続先データ、および前記第２接続先データを中継装置（例えば、設定先選択機能３０，３０ａ）へ送信する（Ｓ７，Ｓ２５）。すると、前記中継装置は、前記認証済ユーザの認証情報、前記第１接続先データ、および前記第２接続先データを関係付けて記憶装置に格納する（Ｓ３２）。それから、前記変換装置は、前記第１接続先データを前記第２接続先データに置換したサービスデータを前記認証済ユーザが操作するクライアント装置（例えば、クライアント２）へ送信する（Ｓ９，Ｓ２６，Ｓ２７）。すると、前記クライアント装置は、前記置換されたサービスデータと前記ユーザの操作により選択された前記第２接続先データを前記中継装置に送信する（Ｓ１０，Ｓ４１）。前記中継装置は、前記記憶部から、前記クライアント装置から送信された第２接続先データに対応する、前記変換装置から受信した前記認証情報および前記第１接続先データを抽出する（Ｓ４２）。前記中継装置は、前記抽出した第１接続先データの示すサーバ装置（例えば、アクセスＧＷ３）へ、前記抽出した認証情報を送信する（Ｓ１３，Ｓ５０）。前記中継装置は、前記サーバ装置のアドレスを前記クライアント装置へ送信する（Ｓ１５，Ｓ５１）。前記クライアント装置は、前記アドレスと前記認証情報を用いて、前記サーバ装置と通信する（Ｓ１６）。
【０１４６】
このように構成することにより、１つの認証済みＩＤ生成時のアクセスＧＷへの認証済みＩＤの設定量をアクセスＧＷ数に非依存にすることができる。また、認証済みＩＤが発行され、認証済みＩＤ毎にＦＱＤＮが書き換えられたメッセージをクライアントが受信し

た後にセッションが切れても、クライアントは再度認証を受けなくても、ＤＮＳサーバに対して、ＦＱＤＮの問合せ要求を行うことができる。

【０１４７】

前記中継装置は、前記サーバ装置に対して前記認証情報を送信済である場合は、前記認証情報を送信しない。

このように構成することにより、既にアクセスＧＷに認証済みＩＤが設定されている場合には、アクセスＧＷに対して再度認証済みＩＤの設定を行う必要がないので、アクセスＧＷへの認証済みＩＤの設定処理量を削減できる。

【０１４８】

前記変換装置および前記中継装置は、前記認証済ユーザの認証情報、該認証情報と関係付けられた前記第１接続先データ、および該認証情報と関係付けられた前記第２接続先データを記憶し、一定時間経過後に消去する。当該消去は、例えば、本実施形態で言えば、有効期限管理部４６，４７により行われる。

【０１４９】

このように構成することにより、認証済みＩＤの「有効期限」を設けることにより、その有効期限が過ぎた場合、その「有効期限」を含むエントリを全てのテーブルから削除することができる。

【０１５０】

変換装置（例えば、ゲートウェイ４０－１）は、受信部（例えば、受信部４０－２）、生成部（例えば、生成部４０－３）、送信部（例えば、送信部４０－４）を含む。受信部は、第１接続先データ及び認証済ユーザの認証情報を含んだ、該認証済ユーザに送付するサービスデータを受信する。生成部は、前記第１接続先データを特定する第２接続先データを生成する。送信部は、前記認証済ユーザの認証情報、前記第１接続先データ、および前記第２接続先データを関係付けて中継装置（例えば、ゲートウェイ３０－１）へ送信し、前記第１接続先データを前記第２接続先データに置換した前記サービスデータを前記認証済ユーザが操作するクライアント装置（例えば、クライアント２）へ送信する。

【０１５１】

このように構成することにより、変換装置は、クライアントと設定先選択機能に、認証済みＩＤ毎に生成された変換後ＦＱＤＮを通知することにより、クライアントと設定先選択機能間では、変換後ＦＱＤＮを用いて、通信することができる。

【０１５２】

中継装置（例えば、ゲートウェイ３０－１）は、受信部（例えば、受信部３０－２）、記憶部（例えば、記憶部３０－３）、抽出部（例えば、抽出部３０－４）、送信部（例えば、送信部３０－５）を含む。受信部は、変換装置（例えば、ゲートウェイ４０－１）から、認証済ユーザの認証情報、第１接続先データ、および第２接続先データを受信する。また、受信部は、ユーザの操作により選択された第２接続先データを該ユーザが操作するクライアント装置から受信する。記憶部は、前記変換装置から受信した前記第２接続先データ、前記認証情報および前記第１接続先データを関係付けて記憶する。抽出部は、前記記憶部から、前記クライアント装置から受信した第２接続先データに対応する、前記変換装置から受信した前記認証情報および前記第１接続先データを抽出する。送信部は、前記抽出した第１接続先データの示すサーバ装置へ前記抽出した認証情報を送信し、前記サーバ装置のアドレスを前記クライアント装置へ送信する。

【０１５３】

このように構成することにより、中継装置は、クライアントとの間では、変換後ＦＱＤＮを用いて通信をし、アクセスＧＷとの間では、変換前ＦＱＤＮを用いて通信をすることができる。

【０１５４】

なお、本実施形態は、以上に述べた実施の形態に限定されるものではなく、本実施形態の要旨を逸脱しない範囲内で種々の構成または実施形態を取ることができる。

【０１５５】

上記実施形態に関し、更に以下の付記を開示する。

（付記1）

変換装置は、第１接続先データ及び認証済ユーザの認証情報を含んだ、該認証済ユーザに送付するサービスデータを受信し、

前記変換装置は、前記第１接続先データを特定する第２接続先データを生成し、

前記変換装置は、前記認証済ユーザの認証情報、前記第１接続先データ、および前記第２接続先データを関係付けて中継装置へ送信し、

前記中継装置は、前記認証済ユーザの認証情報、前記第１接続先データ、および前記第２接続先データを関係付けて記憶装置に格納し、

前記変換装置は、前記第１接続先データを前記第２接続先データに置換した前記サービスデータを前記認証済ユーザが操作するクライアント装置へ送信し、

前記クライアント装置は、前記置換されたサービスデータと前記ユーザの操作により選択された前記第２接続先データを前記中継装置に送信し、

前記中継装置は、前記記憶部から、前記クライアント装置から送信された第２接続先データに対応する、前記変換装置から受信した前記認証情報および前記第１接続先データを抽出し、

前記中継装置は、前記抽出した第１接続先データの示すサーバ装置へ、前記抽出した認証情報を送信し、

前記中継装置は、前記サーバ装置のアドレスを前記クライアント装置へ送信し、

前記クライアント装置は、前記アドレスと前記認証情報を用いて、前記サーバ装置と通信する

ことを特徴とする認証方法。

（付記２）

前記中継装置は、前記サーバ装置に対して前記認証情報を送信済である場合は、前記認証情報を送信しない

ことを特徴とする付記１記載の認証方法。

（付記３）

前記変換装置および前記中継装置は、前記認証済ユーザの認証情報、該認証情報と関係付けられた前記第１接続先データ、および該認証情報と関係付けられた前記第２接続先データを記憶し、一定時間経過後に消去する

ことを特徴とする付記１記載の認証方法。

（付記４）

第１接続先データ及び認証済ユーザの認証情報を含んだ、該認証済ユーザに送付するサービスデータを受信し、

前記第１接続先データを特定する第２接続先データを生成し、

前記認証済ユーザの認証情報、前記第１接続先データ、および前記第２接続先データを関係付けて中継装置へ送信し、

前記第１接続先データを前記第２接続先データに置換した前記サービスデータを前記認証済ユーザが操作するクライアント装置へ送信する

ことを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。

（付記５）

第１接続先データ及び認証済ユーザの認証情報を含んだ、該認証済ユーザに送付するサービスデータを受信する受信部と、

前記第１接続先データを特定する第２接続先データを生成する生成部と、

前記認証済ユーザの認証情報、前記第１接続先データ、および前記第２接続先データを関係付けて中継装置へ送信し、前記第１接続先データを前記第２接続先データに置換した前記サービスデータを前記認証済ユーザが操作するクライアント装置へ送信する送信部と、

を備えることを特徴とする変換装置。

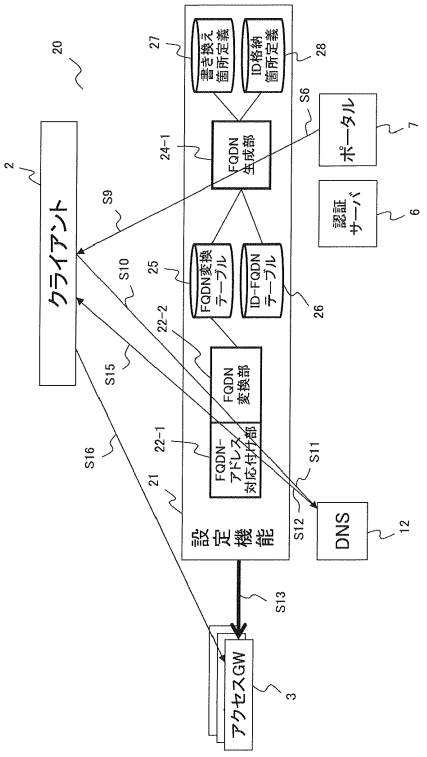
（付記６）

認証済ユーザの認証情報、第１接続先データ、および第２接続先データを変換装置から受信し、
前記変換装置から受信した認証済ユーザの認証情報、第１接続先データ、および第２接続先データを関係付けて記憶装置に格納し、
ユーザの操作により選択された第２接続先データを該ユーザが操作するクライアント装置から受信し、
前記記憶装置から、前記クライアント装置から受信した第２接続先データに対応する、前記変換装置から受信した前記認証情報および前記第１接続先データを抽出し、
前記抽出した第１接続先データの示すサーバ装置へ、前記抽出した認証情報を送信し、
前記サーバ装置のアドレスを前記クライアント装置へ送信する
ことを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。
（付記７）
変換装置から、認証済ユーザの認証情報、第１接続先データ、および第２接続先データを受信し、ユーザの操作により選択された第２接続先データを該ユーザが操作するクライアント装置から受信する受信部と、
前記変換装置から受信した前記第２接続先データ、前記認証情報および前記第１接続先データを関係付けて記憶する記憶部と、
前記記憶部から、前記クライアント装置から受信した第２接続先データに対応する、前記変換装置から受信した前記認証情報および前記第１接続先データを抽出する抽出部と、
前記抽出した第１接続先データの示すサーバ装置へ前記抽出した認証情報を送信し、前記サーバ装置のアドレスを前記クライアント装置へ送信する送信部と、
を備えることを特徴とする中継装置。
（付記８）
変換装置と中継装置を含む認証システムであって、
前記変換装置は、
第１接続先データ及び認証済ユーザの認証情報を含んだ、該認証済ユーザに送付するサービスデータを受信する受信部と、
前記第１接続先データを特定する第２接続先データを生成する生成部と、
前記認証済ユーザの認証情報、前記第１接続先データ、および前記第２接続先データを関係付けて中継装置へ送信し、前記第１接続先データを前記第２接続先データに置換した前記サービスデータを前記認証済ユーザが操作するクライアント装置へ送信する送信部と、
を備え、
前記中継装置は、
前記変換装置から、前記認証済ユーザの認証情報、前記第１接続先データ、および前記第２接続先データを受信し、前記ユーザの操作により選択された第２接続先データを前記クライアント装置から受信する受信部と、
前記変換装置から受信した前記第２接続先データ、前記認証情報および前記第１接続先データを関係付けて記憶する記憶部と、
前記記憶部から、前記クライアント装置から受信した第２接続先データに対応する、前記変換装置から受信した前記認証情報および前記第１接続先データを抽出する抽出部と、
前記抽出した第１接続先データの示すサーバ装置へ前記抽出した認証情報を送信し、前記サーバ装置のアドレスを前記クライアント装置へ送信する送信部と、
を備えることを特徴とする認証システム。
【符号の説明】
【０１５６】
２　　クライアント
３　　アクセスＧＷ
４　　コンテンツサーバ
６　　認証サーバ

７　　ポータルサーバ
１２　　ＤＮＳサーバ
２０，２０－１，２０－２　　アクセス制御システム
２１　　設定機能
２２－１　　ＦＱＤＮ－アドレス対応付け部
２２－２　　ＦＱＤＮ変換部
２２　　変換管理部
２４，２４－１　　ＦＱＤＮ生成部
２５　　ＦＱＤＮ変換テーブル
２６　　ＩＤ－ＦＱＤＮテーブル
２７　　書き換え箇所定義情報
２８　　ＩＤ格納箇所定義情報
３０，３０ａ　　設定先選択機能
３０－１　　ゲートウェイ装置
３０－２　　受信部
３０－３　　記憶部
３０－４　　抽出部
３０－５　　送信部
３１　　設定部
３２　　設定制御部
３４　　通信受付部
４０，４０ａ　　マッピング機能
４０－１　　ゲートウェイ装置
４０－２　　受信部
４０－３　　生成部
４０－４　　送信部
４１　　通知部
４２　　ＩＤ－ＦＱＤＮ管理部
４３　　設定先選択機能アドレス情報
４４　　ＩＤ－ＦＱＤＮ管理テーブル
４５　　通知受付部
４６，４７　　有効期限管理部

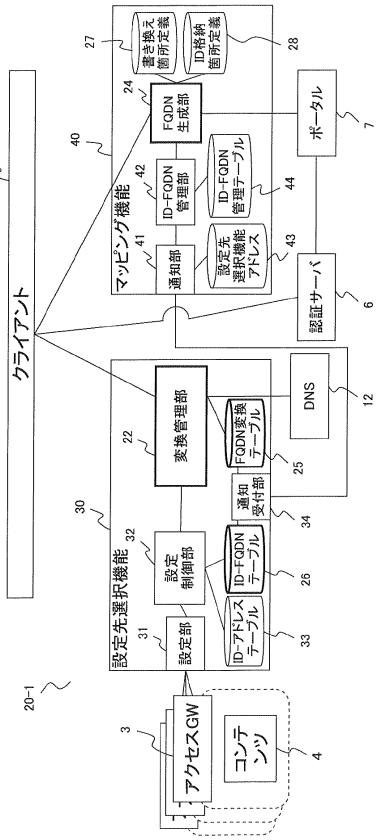
【図４】

アクセス制御システム20の構成例



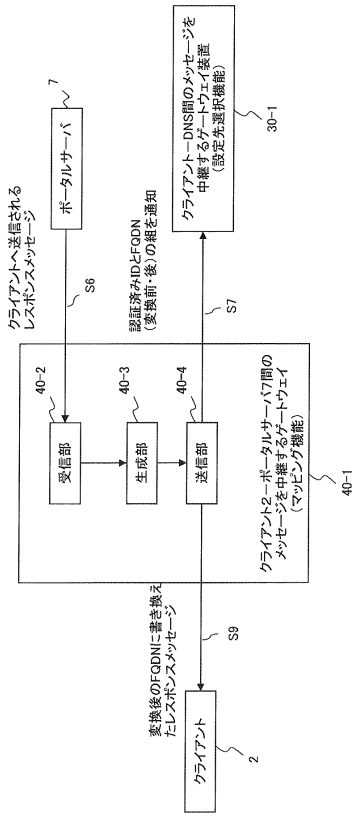
【図５】

アクセス制御システム20－1の構成例



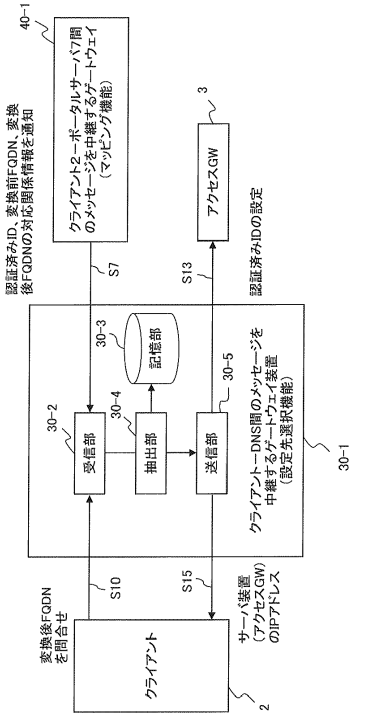
【図６】

マッピング機能40を有するゲートウェイ装置40－1の構成図



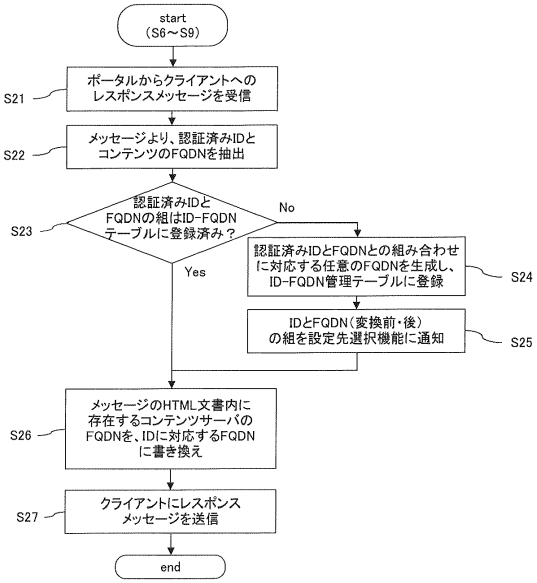
【図７】

設定先選択機能30を有するゲートウェイ装置30－1の構成図



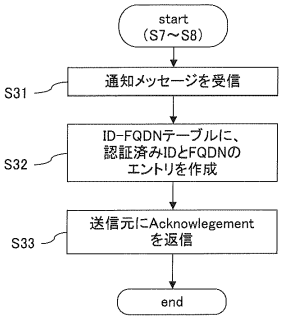
【図９】

コンテンツの一覧などのリソース提供のための
レスポンスメッセージを受信した場合の
マッピング機能40の処理フロー



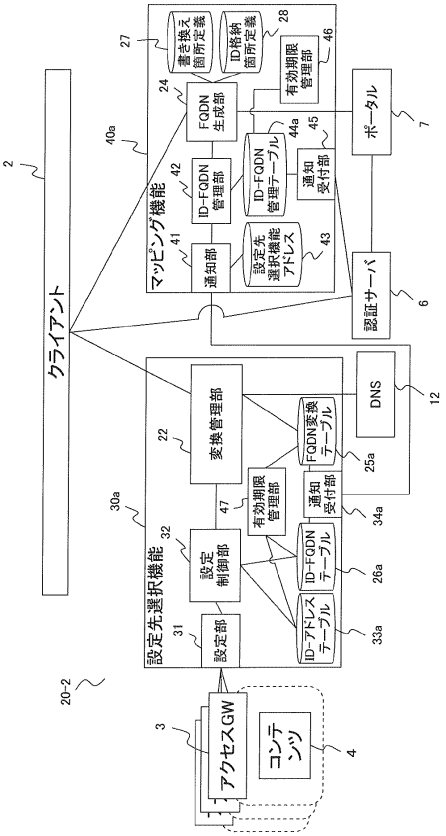
【図１６】

マッピング機能40からの通知メッセージ60を受信した場合の
設定先選択機能30の動作（S7～S8）の詳細なフローチャート



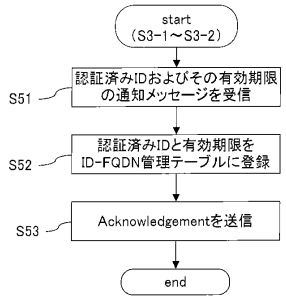
【図２２】

アクセス制御システム20－2の構成例



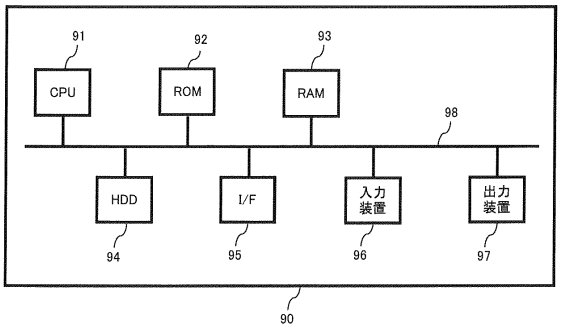
【図２４】

認証サーバ6から認証済みIDとその有効期限についての
通知メッセージ受信時のマッピング機能40aのフローチャート

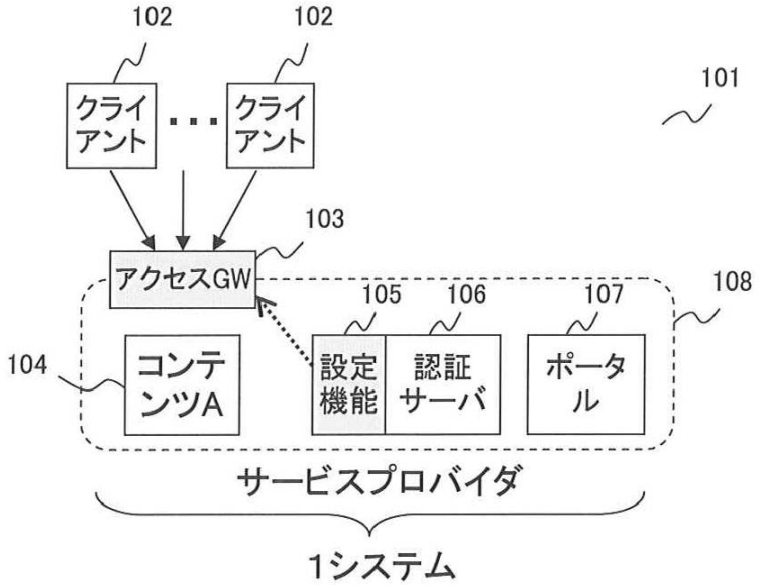


【図３２】

マッピング機能40，40aまたは設定先選択機能30を
有するゲートウェイ装置の各部の機能を実現するコンピュータの
ハードウェア構成の一例

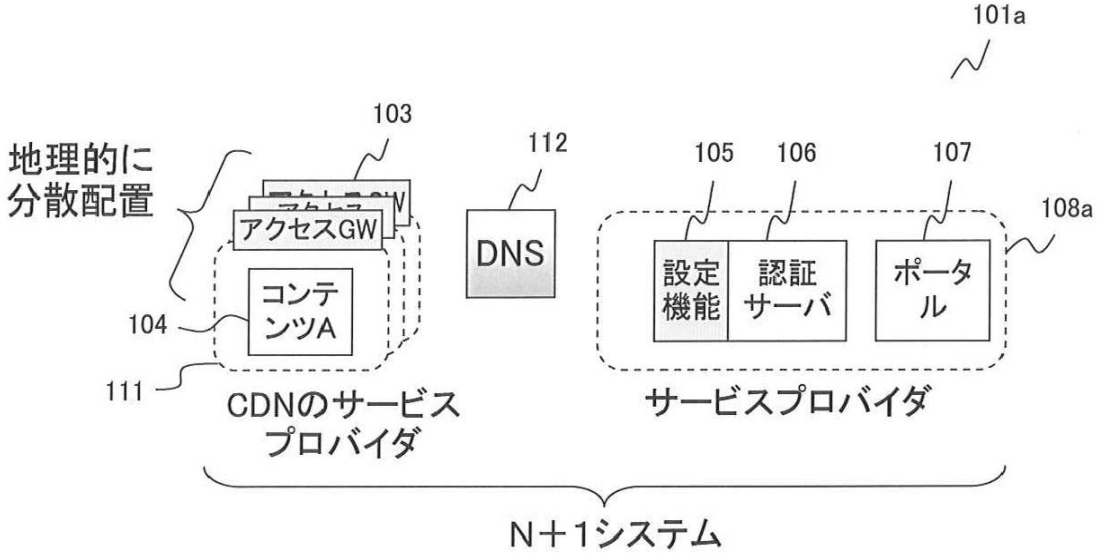


【図１】


1つのサービスプロバイダ108のシステム内に
閉じたアクセス制御システム101の一例
102
102
101
クライアント
クライアント
103
アクセスGW
105
106
107
108
104
コンテンツA
設定機能
認証サーバ
ポータル
サービスプロバイダ
1システム

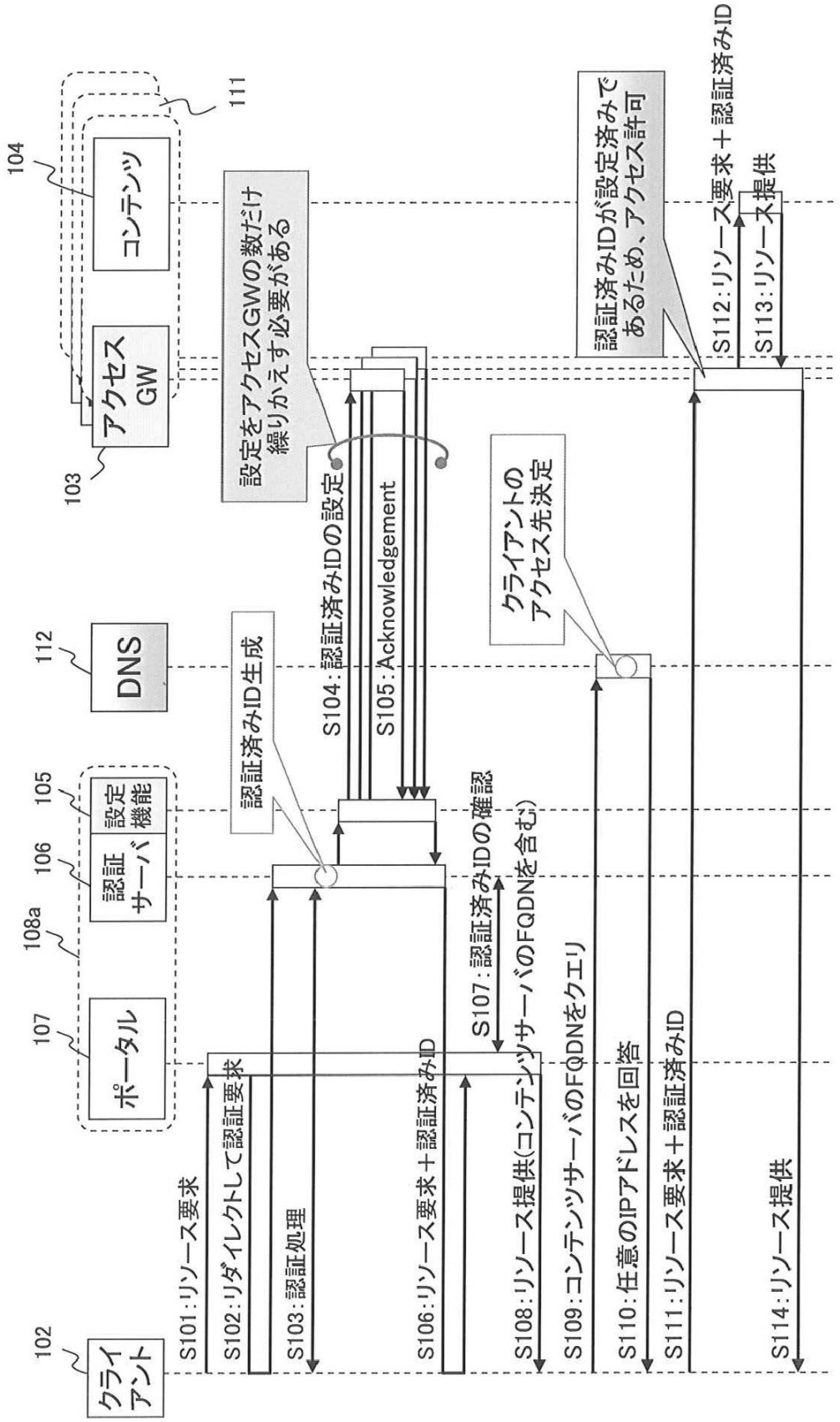
【図２】

サービスプロバイダ108aがCDNサービスを
利用する場合のアクセス制御システム101aを示す。



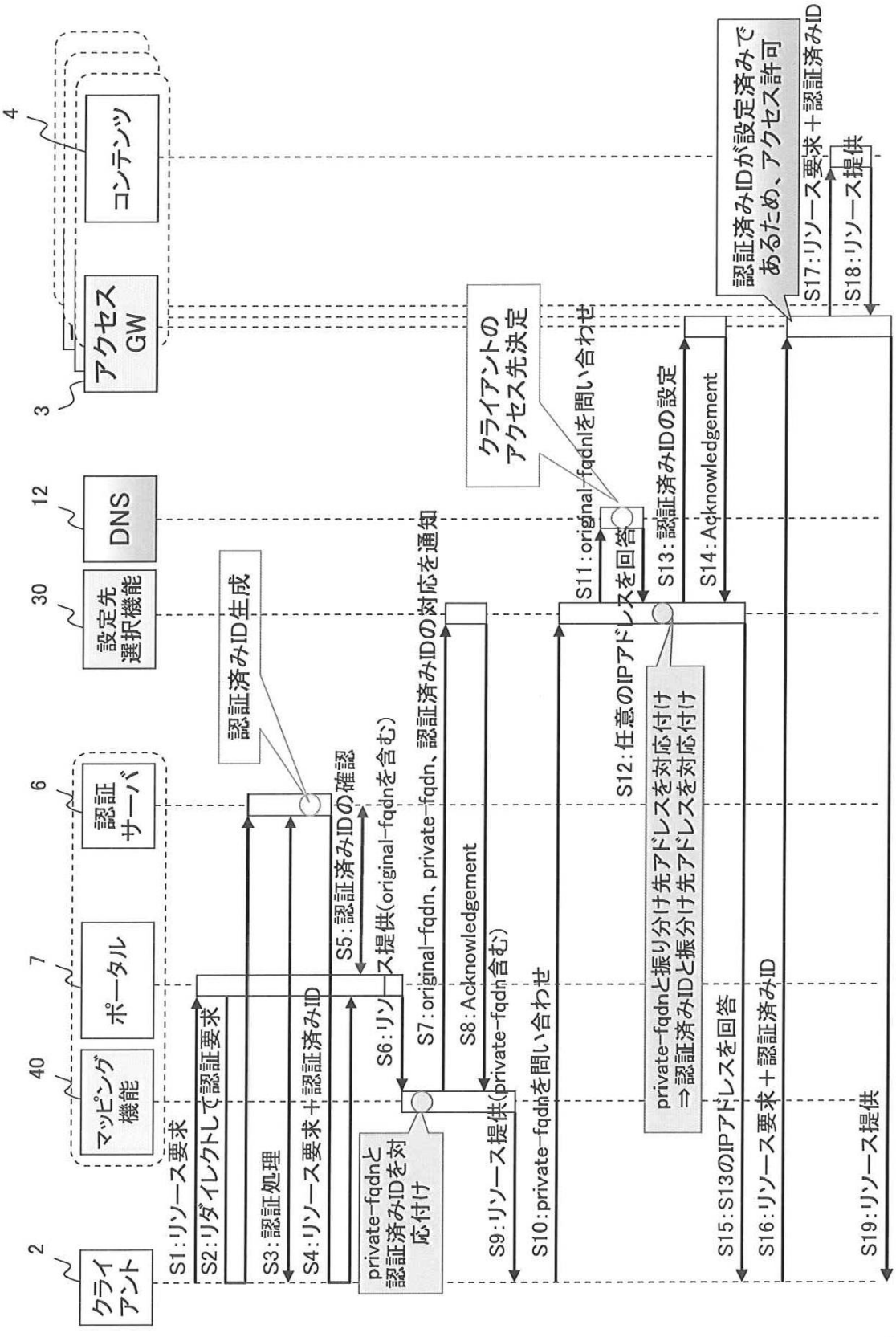
【図３】

図2のアクセス制御システム101aの全体シーケンスの一例

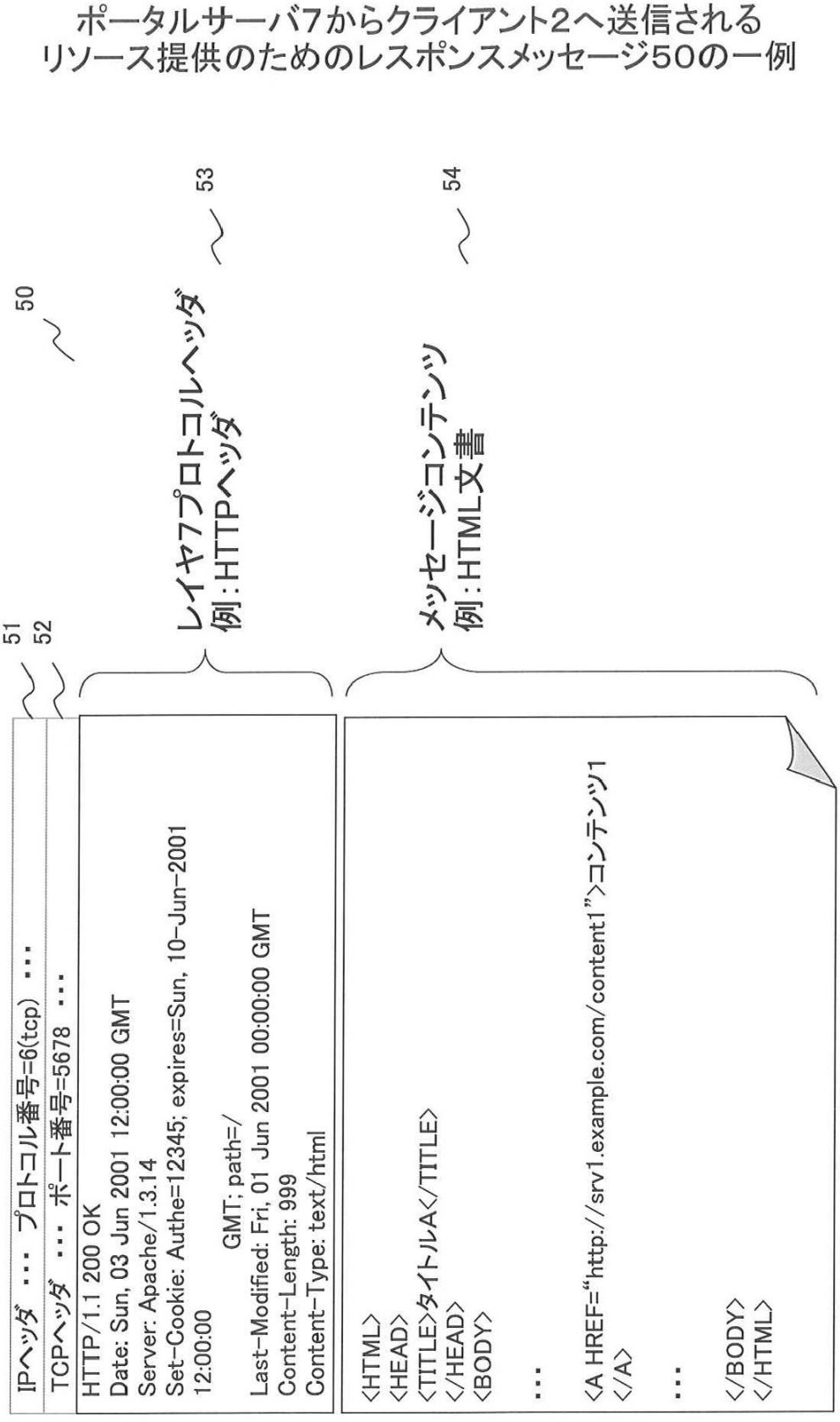


【図８】

アクセス制御システム20－1の全体シーケンスの一例



【図１０】


ポータルサーバ7からクライアント2へ送信される
リソース提供のためのレスポンスメッセージ50の一例
50
51
52
53
54
レイヤ7プロトコルヘッダ
例：HTTPヘッダ
メッセージコンテンツ
例：HTML文書
IPヘッダ ・・・ プロトコル番号=6(tcp) ・・・
TCPヘッダ ・・・ ポート番号=5678 ・・・
HTTP/1.1 200 OK
Date: Sun, 03 Jun 2001 12:00:00 GMT
Server: Apache/1.3.14
Set-Cookie: Authe=12345; expires=Sun, 10-Jun-2001
12:00:00
GMT; path=/
Last-Modified: Fri, 01 Jun 2001 00:00:00 GMT
Content-Length: 999
Content-Type: text/html
<HTML>
<HEAD>
<TITLE>タイトルA</TITLE>
</HEAD>
<BODY>
・・・
<A HREF="http://srv1.example.com/content1">コンテンツ1
</A>
・・・
</BODY>
</HTML>

【図１１】

ID格納箇所定義情報28の一例

HTTPヘッダフィールド名	オプション
Set-Cookie	NAME==Authe

28

【図１２】

書き換え箇所定義情報27の一例

HTML文書書き換え箇所
//a/@href

27

【図１３】

ID－FQDN管理テーブル44の一例

認証済みID	変換前FQDN	変換後FQDN
abc123	srv1.example.com	aaa.example.com
98765432	srv2.example.com	bbb.example.com

44

【図１４】

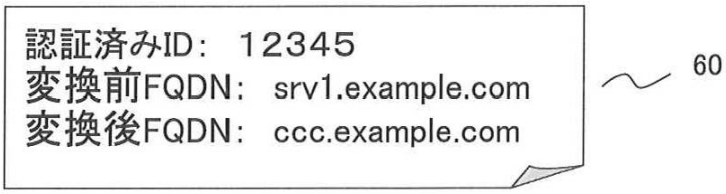
設定先選択機能アドレスの一例

設定先選択機能アドレス
192.0.2.111

43

【図１５】

マッピング機能から設定先選択機能へ
送信される通知メッセージの一例



【図１７】

ID－FQDNテーブル26の一例

認証済みID	変換後FQDN
abc123	aaa.example.com
98765432	bbb.example.com
12345	ccc.example.com

26

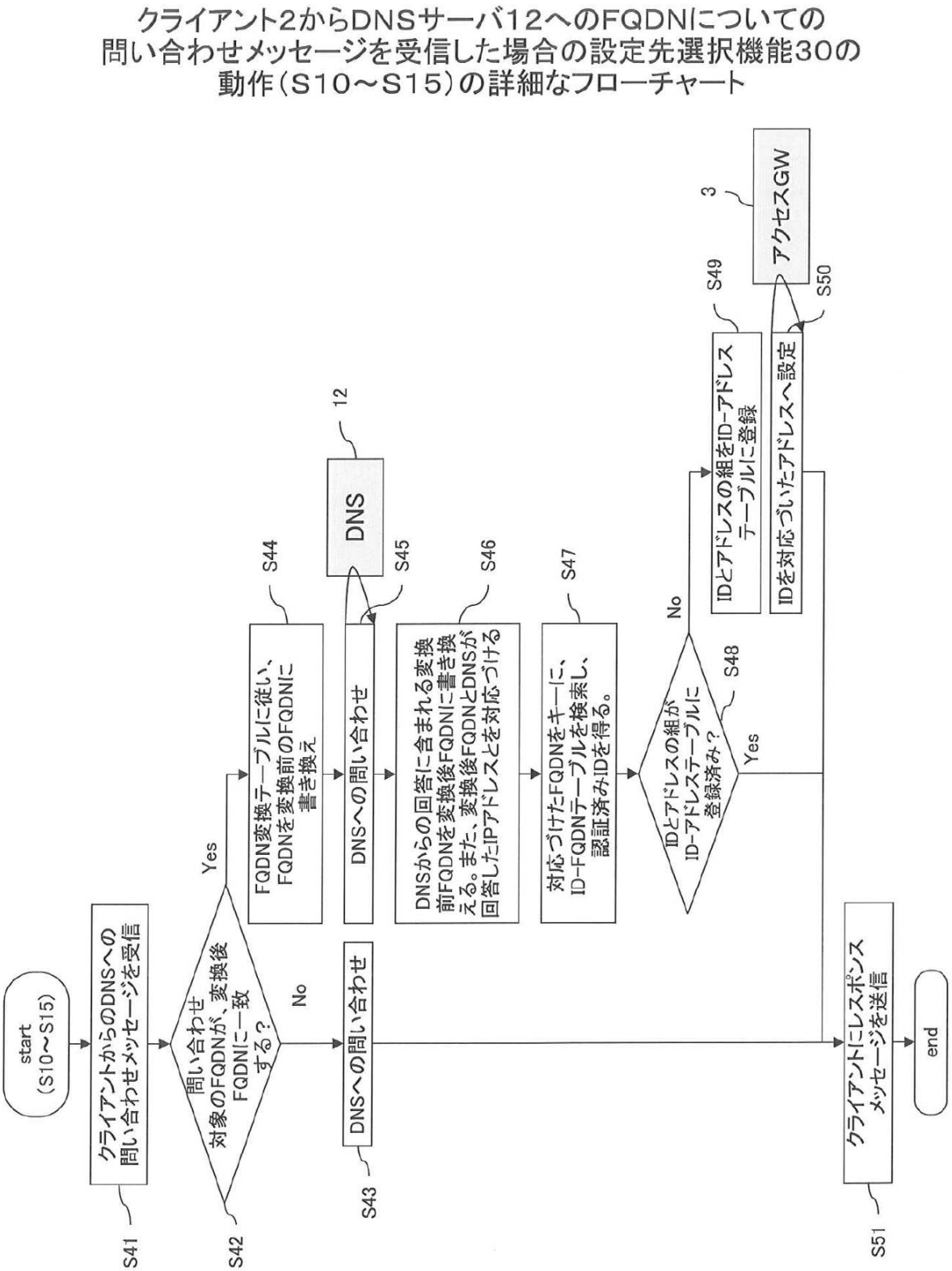
【図１８】

FQDN変換テーブル25の一例

変換後FQDN	変換前FQDN
aaa.example.com	srv1.example.com
bbb.example.com	srv2.example.com
ccc.example.com	srv1.example.com

25

【図１９】


クライアント2からDNSサーバ12へのFQDNについての
問い合わせメッセージを受信した場合の設定先選択機能30の
動作（S10～S15）の詳細なフローチャート
start
（S10～S15）
クライアントからのDNSへの
問い合わせメッセージを受信
S41
問い合わせ
対象のFQDNが、変換後
FQDNに一致
する？
S42
Yes
No
FQDN変換テーブルに従い、
FQDNを変換前のFQDNに
書き換え
S44
DNSへの問い合わせ
S45
DNS
12
DNSからの回答に含まれる変換
前FQDNを変換後FQDNに書き換
える。また、変換後FQDNとDNSが
回答したIPアドレスとを対応づける
S46
DNSへの問い合わせ
S43
対応づけたFQDNをキーに、
ID-FQDNテーブルを検索し、
認証済みIDを得る。
S47
IDとアドレスの組が
ID-アドレステーブルに
登録済み？
S48
Yes
No
IDとアドレスの組をID-アドレス
テーブルに登録
S49
IDを対応づいたアドレスへ設定
S50
アクセスGW
3
クライアントにレスポンス
メッセージを送信
S51
end

【図２０】

ID－アドレステーブル33の一例

認証済みID	IPアドレス
abc123	10.10.10.10
98765432	192.168.0.254

33

【図２１】

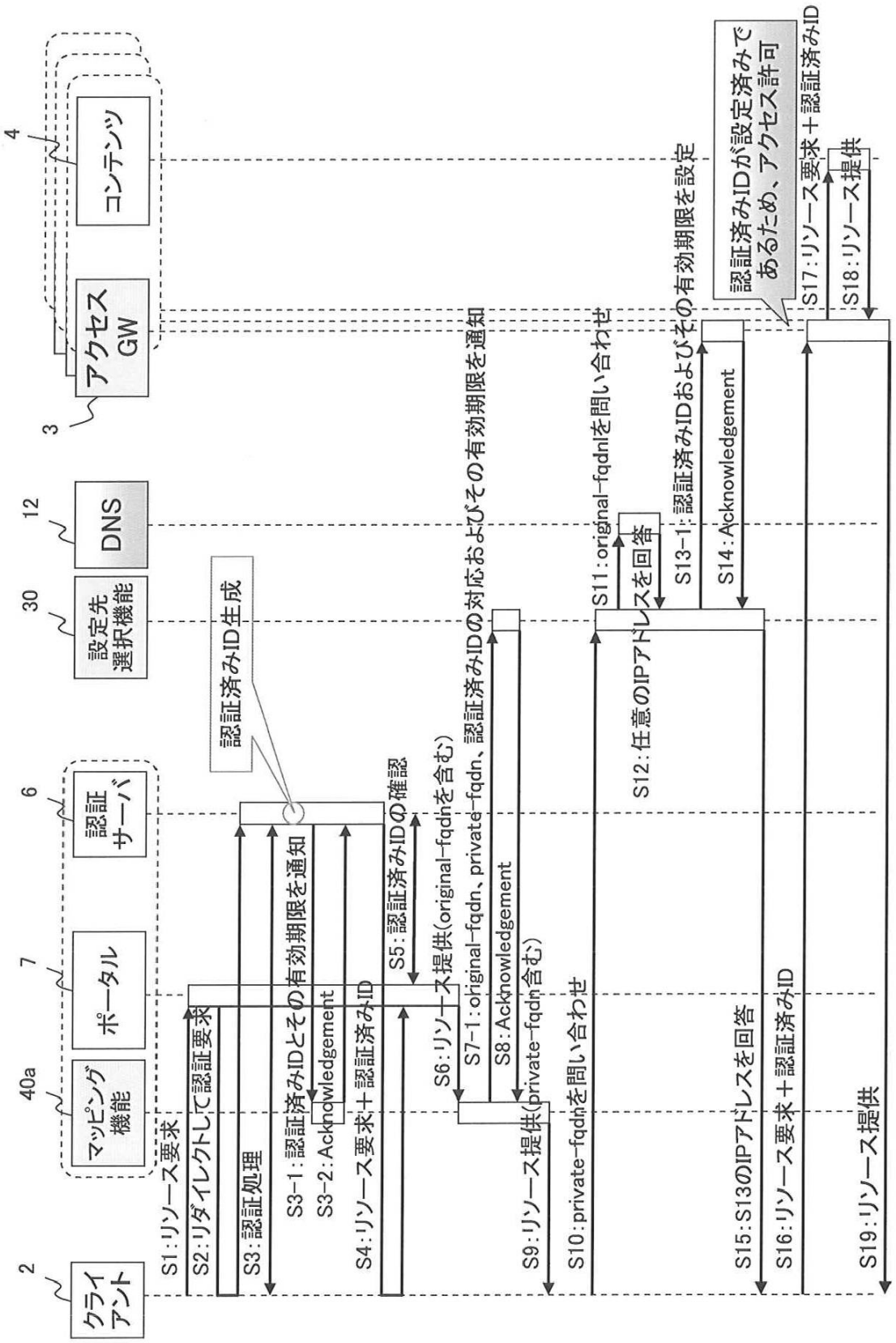
設定先選択機能30からアクセスGW3へ
送信される設定メッセージ61の一例

認証済みID： 12345

61

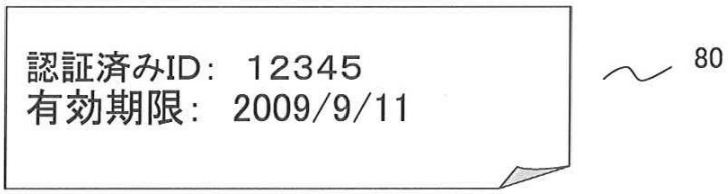
【図２３】

アクセス制御システム20－2の全体シーケンスの一例



【図２５】

認証サーバ6からマッピング機能40aへ送信される
認証済みIDの有効期限を通知する通知メッセージ80の一例



【図２６】

ID－FQDN管理テーブル44aの一例

認証済みID	変換前FQDN	変換後FQDN	有効期限
abc123	srv1.example.com	aaa.example.com	2009/9/11
98765432	srv2.example.com	bbb.example.com	2009/10/10
12345	未登録	未登録	2009/9/11

44a

【図２７】

マッピング機能40aから設定先選択機能30へ
送信される通知メッセージ60aの一例

【図２８】

ID－FQDNテーブル26aの一例

認証済みID	変換後FQDN	有効期限
abc123	aaa.example.com	2009/9/11
98765432	bbb.example.com	2009/10/10
12345	ccc.example.com	2009/9/11

26a

【図２９】

FQDN変換テーブル25aの一例

変換後FQDN	変換前FQDN	有効期限
aaa.example.com	srv1.example.com	2009/9/11
bbb.example.com	srv2.example.com	2009/10/10
ccc.example.com	srv1.example.com	2009/9/11

25a

【図３０】

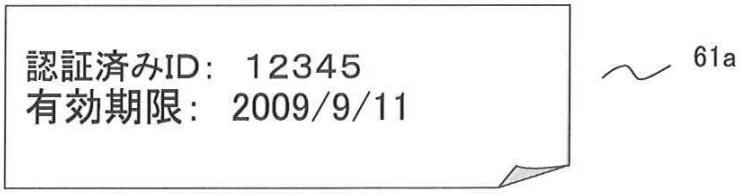
ID－アドレステーブル33aの一例

認証済みID	IPアドレス	有効期限
abc123	10.10.10.10	2009/9/11
98765432	192.168.0.254	2009/10/10

33a

【図３１】

設定先選択機能30からアクセスGW3へ
送信される設定メッセージ61aの一例



フロントページの続き

(72)発明者　小倉　孝夫
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　上野　仁
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

審査官　金木　陽一

(56)参考文献　特開２０００－００３３３４（ＪＰ，Ａ）
特開２００３－０４４５０８（ＪＰ，Ａ）
特開２００６－０３１５２２（ＪＰ，Ａ）
特開２００７－０４１６５１（ＪＰ，Ａ）
特開２００８－１５２３６８（ＪＰ，Ａ）
榎堀 優ほか，サービスアクセスに連動したトンネルネットワークの自動構築，マルチメディア，分散，協調とモバイル（DICOMO2008）シンポジウム論文集 [CD-ROM]，Vol．2008，No．1，pp．177-184，情報処理学会シンポジウムシリーズ

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／３１
Ｇ０６Ｆ　２１／４１
Ｇ０６Ｆ　２１／４５