(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2014 年 1 月 3 日(03.01.2014)

WIPO | PCT

(10) 国際公開番号
WO 2014/002265 A1

(51) 国際特許分類:
H04L 12/46 (2006.01)

(21) 国際出願番号: PCT/JP2012/066758

(22) 国際出願日: 2012 年 6 月 29 日(29.06.2012)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(71) 出願人 (米国を除く全ての指定国について): 富士通株式会社(FUJITSU LIMITED) [JP/JP]; 〒2118588 神奈川県川崎市中原区上小田中４丁目１番１号 Kanagawa (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 木野 高史(KINO, Takashi) [JP/JP]; 〒1350091 東京都港区台場二丁目３番１号 株式会社富士通ミッションクリティカルシステムズ内 Tokyo (JP). 入江 将勝(IRIE, Masakatsu) [JP/JP]; 〒1350091 東京都港区台場二丁目３番１号 株式会社富士通ミッションクリティカルシステムズ内 Tokyo (JP). 田中 宏行(TANAKA, Hiroyuki) [JP/JP]; 〒2118588 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 Kanagawa (JP). 四ノ宮 大輔(SHINOMIYA, Daisuke) [JP/JP]; 〒2118588 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 Kanagawa (JP). 武仲 正彦(TAKENAKA, Masahiko) [JP/JP]; 〒2118588 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 Kanagawa (JP). 高橋 裕(TAKAHASHI, Yutaka) [JP/JP]; 〒2118588 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 Kanagawa (JP).

(74) 代理人: 服部 毅巖(HATTORI, Kiyoshi); 〒1920082 東京都八王子市東町９番８号 八王子東町センタービル 服部特許事務所 Tokyo (JP).

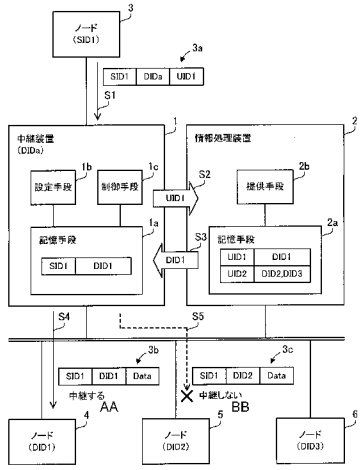
(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS,

[続葉有]

(54) **Title**: RELAY DEVICE, INFORMATION PROCESSING DEVICE, ACCESS CONTROL METHOD, AND PROGRAM

(54) 発明の名称 : 中継装置、情報処理装置、アクセス制御方法およびプログラム

[図1]



1 Relay device (DIDa)
1a Storage means; SID1; DID1
1b Setting means
1c Control means
2 Information processing device
2a Storage means; UID1; DID1; UID2; DID2, DID3
2b Provision means
3 Node (SID1)
3a SID1; DIDa; UID1
3b SID1; DID1; Data
3c SID1; DID2, Data
4 Node (DID1)
5 Node (DID2)
6 Node (DID3)
S2 UID1
S3 DID1
AA Relay
BB Do not relay

(57) **Abstract**: The present invention simplifies access control for each user. Upon receiving first identification information expressing a user and second identification information expressing a transmission-source node (3), a setting means (1b) obtains, from an information processing device (2), third identification information expressing a destination node (4) for which access is allowed, according to the first identification information, and stores, in a storage means (1a), the second identification information and the third identification information as a combination for which the relay of data is allowed. When relaying data (3b) containing the identification information for the transmission-source node (3) and the identification information for the destination node (4), a control means (1c) determines whether or not to relay the data (3b) on the basis of the information stored in the storage means (1a).

(57) 要約: ユーザごとのアクセス制御を容易に行うこと。 設定手段（１ｂ）は、ユーザを示す第１の識別情報および送信元のノード（３）を示す第２の識別情報を受信すると、第１の識別情報に対応してアクセスが許容された宛先のノード（４）を示す第３の識別情報を情報処理装置（２）から取得し、データの中継が許容された組み合わせとして第２の識別情報と第３の識別情報とを記憶手段（１ａ）に設定する。制御手段（１ｃ）は、送信元のノード（３）の識別情報と宛先のノード（４）の識別情報とを含むデータ（３ｂ）の中継を行う際に、記憶手段（１ａ）に設定された情報に基づいて、当該データ（３ｂ）を中継するか否かを判定する。

WO 2014/002265 A1

JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:

— 国際調査報告（条約第 21 条(3)）

明　細　書

発明の名称 ：

中継装置、情報処理装置、アクセス制御方法およびプログラム

技術分野

[0001] 本発明は中継装置、情報処理装置、アクセス制御方法およびプログラムに関する。

背景技術

[0002] コンピュータなどの複数の情報処理装置を、ネットワークを介して接続した情報処理システムが利用されている。例えば、情報処理システムはサービスを提供するサーバ装置と通信データを中継する中継装置とを含む。ユーザはクライアント装置を用いてサーバ装置にアクセスし、サービスを利用し得る。

[0003] しかし、不特定多数のユーザが同じサーバ装置にアクセス可能であると、サーバ装置のセキュリティが問題となる。例えば、当該サーバ装置で扱う機密情報が不正に読み出されたり、サーバ装置を不正に利用されたりするおそれがある。そこで、ネットワーク内のサーバ装置へのアクセスをユーザごとに制限することがある。

[0004] 例えば、ユーザの操作端末からホームネットワーク内の機器を操作する際に、ユーザ名やパスワードを操作端末からホームゲートウェイに送信して認証を行う提案がある。この提案では、ユーザが認証されると、操作端末が当該ユーザの機器単位のアクセス許可情報をもつテーブルをホームゲートウェイから取得する。操作端末が当該テーブルに基づき機器単位のアクセス管理を行う。

[0005] なお、例えばユーザ認証された場合にセッション識別子をユーザに割り当てることで、認証済のユーザを管理し、また、認証済のユーザごとに異なるサーバにアクセスするように受信データの宛先を変換するリバースプロキシ装置の提案がある。更に、例えばユーザがシステムにログインするごとにセ

ッションＩＤ（IDentifier）をユーザ端末に通知し、セッションＩＤを含む情報提供要求をユーザ端末から受信すると、セッションＩＤに基づき情報提供要求の正当性を確認する提案もある。

先行技術文献

特許文献

[0006] 特許文献1：特開２００１－２５１３１２号公報

特許文献2：特開２０１０－５６６６６号公報

特許文献3：特開２００６－１１８３３号公報

発明の概要

発明が解決しようとする課題

[0007] 中継装置を用いてユーザごとのアクセス制御を行うことがある。例えば、論理的に分割された複数の仮想的なネットワーク（ＶＬＡＮ（Virtual Local Area Network）と呼ばれることがある）を中継装置に割り当てることが考えられる。例えば、認証されたユーザに応じたＶＬＡＮにクライアント装置を所属させる。こうして、クライアント装置のアクセス先を同じＶＬＡＮに所属するサーバ装置に制限する。

[0008] しかし、この方法では、ユーザごとのアクセス制御のための情報を中継装置に予め保持させることになる。この場合、当該情報のメンテナンスが容易でないという問題がある。例えば、複数の中継装置を利用するとき、中継装置が増減するたびに個々の中継装置の設定を変更するとなると、設定変更のための作業コストが増大し得る。

[0009] 一側面によれば、本発明は、ユーザごとのアクセス制御を容易に行うことができる中継装置、情報処理装置、アクセス制御方法およびプログラムを提供することを目的とする。

課題を解決するための手段

[0010] 一実施態様によれば、中継装置が提供される。この中継装置は設定手段と制御手段とを有する。設定手段は、ユーザを示す第１の識別情報および送信

元のノードを示す第２の識別情報を受信すると、複数のユーザの識別情報それぞれに対応付けてアクセスが許容された宛先のノードを示す識別情報を記憶する情報処理装置から、第１の識別情報に対応する宛先のノードを示す第３の識別情報を取得し、データの中継が許容された組み合わせとして第２の識別情報と第３の識別情報とを記憶手段に設定する。制御手段は、送信元のノードの識別情報と宛先のノードの識別情報とを含むデータの中継を行う際に、記憶手段に設定された情報に基づいて、当該データを中継するか否かを判定する。

[0011] また、一実施態様によれば、送信元のノードにより送信されたデータを中継する中継装置と通信可能な情報処理装置が提供される。この情報処理装置は記憶手段と提供手段とを有する。記憶手段は、複数のユーザの識別情報それぞれに対応付けてアクセスが許容された宛先のノードを示す識別情報を記憶する。提供手段は、ユーザを示す第１の識別情報および送信元のノードを示す第２の識別情報を中継装置から受信すると、記憶手段を参照して、第１の識別情報に対応する宛先のノードを示す第３の識別情報を検索し、第２の識別情報に対応してデータの中継が許容された宛先のノードの識別情報として第３の識別情報を中継装置に提供する。

[0012] また、一実施態様によれば、送信元のノードにより送信されたデータを中継する中継装置および中継装置と通信可能な情報処理装置を含むシステムで実行されるアクセス制御方法が提供される。このアクセス制御方法では、ユーザを示す第１の識別情報および送信元のノードを示す第２の識別情報を中継装置を用いて受信すると、第１の識別情報および第２の識別情報を情報処理装置に送信する。情報処理装置を用いて、複数のユーザの識別情報それぞれに対応付けてアクセスが許容された宛先のノードの識別情報を記憶する記憶手段を参照して、第１の識別情報に対応する宛先のノードを示す第３の識別情報を検索し、第２の識別情報に対応してデータの中継が許容された宛先のノードの識別情報として第３の識別情報を中継装置に提供する。送信元のノードの識別情報と宛先のノードの識別情報とを含むデータの中継を、中継

装置を用いて行う際に、情報処理装置から提供された情報に基づいて、当該データを中継するか否かを判定する。

[0013] また、一実施態様によれば、送信元のノードにより送信されたデータを中継するためのコンピュータによって実行されるプログラムが提供される。このプログラムは、コンピュータに、ユーザを示す第１の識別情報および送信元のノードを示す第２の識別情報を受信すると、複数のユーザの識別情報それぞれに対応付けてアクセスが許容された宛先のノードを示す識別情報を記憶する情報処理装置から、第１の識別情報に対応する宛先のノードを示す第３の識別情報を取得し、データの中継が許容された組み合わせとして第２の識別情報と第３の識別情報とを記憶手段に設定し、送信元のノードの識別情報と宛先のノードの識別情報とを含むデータの中継を行う際に、記憶手段に設定された情報に基づいて、当該データを中継するか否かを判定する、処理を実行させる。

[0014] また、一実施態様によれば、送信元のノードにより送信されたデータを中継する中継装置と通信可能なコンピュータによって実行されるプログラムが提供される。このプログラムは、コンピュータに、ユーザを示す第１の識別情報および送信元のノードを示す第２の識別情報を中継装置から受信すると、複数のユーザの識別情報それぞれに対応付けてアクセスが許容された宛先のノードを示す識別情報を記憶する記憶手段を参照して、第１の識別情報に対応する宛先のノードを示す第３の識別情報を検索し、第２の識別情報に対応してデータの中継が許容された宛先のノードの識別情報として第３の識別情報を中継装置に提供する、処理を実行させる。

発明の効果

[0015] 一実施態様によれば、ユーザごとのアクセス制御を容易に行うことができる。

本発明の上記および他の目的、特徴および利点は本発明の例として好ましい実施の形態を表す添付の図面と関連した以下の説明により明らかになるであろう。

図面の簡単な説明

[0016] [図1]第１の実施の形態の情報処理システムを示す図である。

[図2]第２の実施の形態の情報処理システムを示す図である。

[図3]第２の実施の形態の中継装置のハードウェア例を示す図である。

[図4]第２の実施の形態の管理サーバのハードウェア例を示す図である。

[図5]第２の実施の形態のソフトウェア例を示す図である。

[図6]第２の実施の形態のユーザ管理テーブルの例を示す図である。

[図7]第２の実施の形態のアクセス管理テーブルの例を示す図である。

[図8]第２の実施の形態の接続管理テーブルの例を示す図である。

[図9]第２の実施の形態のセッション管理テーブルの例を示す図である。

[図10]第２の実施の形態の通信データの例を示す図である。

[図11]第２の実施の形態の認証処理の例を示すフローチャートである。

[図12]第２の実施の形態の中継処理の例を示すフローチャートである。

[図13]第２の実施の形態の認証確認例（その１）を示すフローチャートである。

[図14]第２の実施の形態の通信の具体例（その１）を示す図である。

[図15]第２の実施の形態の通信の具体例（その２）を示す図である。

[図16]第２の実施の形態の通信の具体例（その３）を示す図である。

[図17]第２の実施の形態の通信の具体例（その４）を示す図である。

[図18]第２の実施の形態の認証確認例（その２）を示すフローチャートである。

[図19]第２の実施の形態の通信の具体例（その５）を示す図である。

[図20]第２の実施の形態のログアウト処理の例を示すフローチャートである。

[図21]第２の実施の形態の通信の具体例（その６）を示す図である。

[図22]第２の実施の形態のアクセス可能範囲の例（その１）を示す図である。

[図23]第２の実施の形態のアクセス可能範囲の例（その２）を示す図である

。

[図24]第２の実施の形態の他の例（その１）を示す図である。

[図25]第２の実施の形態の他の例（その２）を示す図である。

[図26]第３の実施の形態のアクセス管理テーブルの例を示す図である。

[図27]第３の実施の形態のセッション管理テーブルの例を示す図である。

[図28]第３の実施の形態のセッション管理の例を示すフローチャートである。

。

[図29]第３の実施の形態のアクセス可能範囲の例（その１）を示す図である。

。

[図30]第３の実施の形態のアクセス可能範囲の例（その２）を示す図である。

。

発明を実施するための形態

[0017] 以下、本実施の形態を図面を参照して説明する。

［第１の実施の形態］

図１は、第１の実施の形態の情報処理システムを示す図である。第１の実施の形態の情報処理システムは、中継装置１、情報処理装置２およびノード３，４，５，６を含む。中継装置１、情報処理装置２およびノード４，５，６は、ネットワークを介して接続されている。ノード３は中継装置１を介してノード４，５，６と通信する。例えば、ノード３はユーザが利用するクライアント装置である。ノード３，４，５，６は、物理的なコンピュータ（物理マシンと呼ぶことがある）でもよいし、物理マシン上で動作する仮想的なコンピュータ（仮想マシンと呼ぶことがある）でもよい。

[0018] 中継装置１は、送信元のノードにより送信されたデータを中継する。中継装置１は、記憶手段１ａ、設定手段１ｂおよび制御手段１ｃを有する。

記憶手段１ａは、制御手段１ｃの処理に用いるデータを記憶する。

[0019] 設定手段１ｂは、ユーザを示す第１の識別情報および送信元のノードを示す第２の識別情報を受信する。第１の識別情報はユーザＩＤでもよい。第２の識別情報はネットワークにおいてデータの転送に用いられるアドレス情報

でもよい。当該アドレス情報として、例えばＯＳＩ（Open Systems Interconnection）参照モデルの第３層の通信制御に用いられるＩＰ（Internet Protocol）アドレスが考えられる。

[0020] 設定手段１ｂは、第１の識別情報に基づいて、第１の識別情報に対応してアクセスが許容された宛先のノードを示す第３の識別情報を情報処理装置２から取得する。第３の識別情報は宛先のノードを示すアドレスでもよい。例えば、第３の識別情報はＩＰアドレスでもよい。例えば、設定手段１ｂは第１の識別情報と第２の識別情報とを情報処理装置２に送信し、その応答として第３の識別情報を情報処理装置２から取得する。設定手段１ｂは、データの中継が許容された組み合わせとして第２の識別情報と第３の識別情報とを記憶手段１ａに設定する。

[0021] 制御手段１ｃは、送信元のノードの識別情報と宛先のノードの識別情報とを含むデータを中継するとき、記憶手段１ａに設定された情報に基づいて、当該データを中継するか否かを判定する。当該データに含まれる各ノードの識別情報の組み合わせが、中継が許容された組み合わせとして記憶手段１ａに設定されている場合、制御手段１ｃは当該データを中継すると判定する。すると、制御手段１ｃは当該データの中継を行う。一方、中継が許容された組み合わせとして記憶手段１ａに設定されていない場合、制御手段１ｃは当該データを中継しないと判定する。すると、制御手段１ｃは当該データを破棄する。

[0022] 情報処理装置２は、記憶手段２ａおよび提供手段２ｂを有する。

記憶手段２ａは、複数のユーザの識別情報それぞれに対応付けてアクセスが許容された宛先のノードを示す識別情報を記憶する。１ユーザの識別情報につきアクセスが許容された複数の宛先のノードを示す識別情報が対応付けられていてもよい。１つの宛先のノードにつき複数の識別情報があってもよい。

[0023] 提供手段２ｂは、第１の識別情報および第２の識別情報を中継装置１から受信すると、記憶手段２ａを参照して、第１の識別情報に対応する宛先のノ

ードを示す第３の識別情報を検索する。提供手段２ｂは、第２の識別情報に対応してデータの中継が許容された宛先のノードの識別情報として第３の識別情報を中継装置１に提供する。

[0024] ここで、ノード３からノード４，５，６にアクセスする場合を考える。中継装置１の識別情報を“ＤＩＤａ”、ノード３の識別情報を“ＳＩＤ１”、ノード４の識別情報を“ＤＩＤ１”、ノード５の識別情報を“ＤＩＤ２”、ノード６の識別情報を“ＤＩＤ３”とする。ノード３を利用するユーザの識別情報を“ＵＩＤ１”とする。また、以下に示すステップＳ１の前には記憶手段１ａに設定されている情報はないものとする。

[0025] まず、中継装置１はデータ３ａをノード３から受信する（ステップＳ１）。データ３ａは送信元“ＳＩＤ１”、宛先“ＤＩＤａ”、ユーザデータ“ＵＩＤ１”を含む。中継装置１はデータ３ａから抽出した“ＵＩＤ１”（および“ＳＩＤ１”）を情報処理装置２に送信する（ステップＳ２）。

[0026] 情報処理装置２は“ＵＩＤ１”をキーに記憶手段２ａを検索し、“ＵＩＤ１”のユーザに対応してアクセスが許容された宛先“ＤＩＤ１”を抽出する。１ユーザにつき複数の宛先へのアクセスを許容してもよい。例えば、記憶手段２ａには“ＵＩＤ２”のユーザにつき宛先“ＤＩＤ２，ＤＩＤ３”へのアクセスを許容することを示すレコードの登録もある。情報処理装置２は、送信元“ＳＩＤ１”に対応してデータの中継が許容された宛先として“ＤＩＤ１”を中継装置１に提供する。中継装置１は“ＳＩＤ１”と“ＤＩＤ１”とをデータの中継が許容された組み合わせとして記憶手段１ａに設定する（ステップＳ３）。

[0027] その後、中継装置１はデータ３ｂをノード３から受信する。データ３ｂは、送信元“ＳＩＤ１”、宛先“ＤＩＤ１”、ユーザデータ“Ｄａｔａ”を含む。この時点で、記憶手段１ａには“ＳＩＤ１”と“ＤＩＤ１”との組み合わせが設定されている。よって、中継装置１はデータ３ｂを中継する（ステップＳ４）。更に、中継装置１はデータ３ｃをノード３から受信する。データ３ｃは、送信元“ＳＩＤ１”、宛先“ＤＩＤ２”、ユーザデータ“Ｄａｔ

ａ”を含む。記憶手段１ａには、“ＳＩＤ１”と“ＤＩＤ２”との組み合わせは設定されていない。よって、中継装置１はデータ３ｃを中継しない（ステップＳ５）。

[0028] このように、中継装置１はユーザごとの各ノードに対するアクセス制御の設定内容を情報処理装置２から取得して保持し、当該設定内容に基づいてデータを中継するか否かを判定する。このため、ユーザごとのアクセス制御の内容を変更したい場合には、記憶手段２ａに記憶された設定内容を変更すればよい。変更内容を中継装置１により取得させ、当該変更内容を反映させることができるからである。したがって、情報処理システムの管理者が中継装置１を個別に設定する手間を省ける。また、中継装置１の他にも複数の中継装置が運用されていることもある。その場合に、設定対象の中継装置１を探し出す手間を省ける。このように、ユーザごとのアクセス制御を容易に行うことができる。また、管理者の作業を省力化でき、アクセス制御の設定を効率的に行うことができる。

[0029] 特に、大規模なネットワークでは、多数の中継装置、ノードが運用され得る。処理能力をスケールアウトにより拡張することもあり、ノードが増大し得る。また、アクセス先ノードに仮想マシンが用いられる場合や、仮想マシンの通信を中継する仮想スイッチが用いられる場合には、仮想マシンと仮想スイッチとの接続関係が頻繁に更新され得る。仮想マシンは稼働状況（ユーザの利用有無や負荷など）に応じて、物理マシン上に追加または削除されたり、他の物理マシンへ移動されたりするからである。このように大規模なネットワークでは、接続変更時の各中継装置（または仮想スイッチ）の設定変更の作業負担が特に大きい。よって、大規模なネットワークに対して中継装置１および情報処理装置２を適用する場合、特に有用である。

[0030] 例えば、アクセス制御したいネットワークの入口に中継装置１を配置すれば、ユーザごとにアクセス可能なノードを容易に制限できる。また、個々の中継装置１が、ユーザごとのアクセス制御の設定内容を情報処理装置２から取得する。よって、アクセス制御したいネットワークごとに中継装置１を複

数設けたとしても個々の中継装置１に対するユーザごとのアクセス制御の設定を容易に行える。

[0031] なお、中継装置１および情報処理装置２は、ＣＰＵ（Central Processing Unit）などのプロセッサとＲＡＭ（Random Access Memory）などのメモリとを備えてもよい。その場合、中継装置１および情報処理装置２の情報処理は、メモリに記憶されたプログラムをプロセッサが実行することで実現できる。

[0032] ［第２の実施の形態］

図２は、第２の実施の形態の情報処理システムを示す図である。第２の実施の形態の情報処理システムは、中継装置１００，１００ａ，１００ｂ、管理サーバ２００、業務サーバ３００，３００ａ，４００，４００ａを含む。中継装置１００は、ファイアウォール１１に接続されている。ファイアウォール１１はネットワーク１０に接続されている。例えば、ネットワーク１０はＬＡＮ（Local Area Network）でもよいし、インターネットやＷＡＮ（Wide Area Network）などの広域ネットワークでもよい。

[0033] ファイアウォール１１は、ネットワーク１０側（外部側）と中継装置１００側（内部側）との間の通信（例えば、ＩＰパケット）を監視し、所定のルールに合致した通信のみを許可し、所定のルールに合致しない通信を拒否する。

[0034] 中継装置１００，１００ａ，１００ｂ、管理サーバ２００および業務サーバ３００，３００ａは、ネットワーク２０に接続されている。中継装置１００ｂおよび業務サーバ４００，４００ａは、ネットワーク３０に接続されている。例えば、ネットワーク２０，３０はＬＡＮである。ネットワーク２０，３０は、同一拠点のネットワークでもよいし、異なる拠点（例えば、本社と支社）のネットワークでもよい。

[0035] 中継装置１００，１００ａ，１００ｂは、通信データを中継するスイッチである。中継装置１００，１００ａ，１００ｂは、異なるネットワークセグメント間のルーティングを行うＬ３（Layer 3）スイッチまたはルータでもよ

い。中継装置１００，１００ａ，１００ｂは、管理サーバ２００と通信して、ユーザごとのアクセス制御の情報を取得し、当該情報に基づいてアクセス制御を行う。中継装置１００，１００ａ，１００ｂは、コンピュータによって実現されてもよい。

[0036] 管理サーバ２００は、ユーザごとのアクセス制御の情報を一元管理するサーバコンピュータである。管理サーバ２００は、中継装置１００，１００ａ，１００ｂにアクセス制御の情報を提供する。なお、管理サーバ２００をネットワーク２０以外のネットワーク（例えば、ネットワーク３０）に接続してもよい。

[0037] 業務サーバ３００，３００ａ，４００，４００ａは、業務アプリケーションを実行するサーバコンピュータである。業務サーバ３００，３００ａ，４００，４００ａは業務アプリケーションによるサービスをクライアント５００，５００ａ，６００，６００ａに提供する。例えば、業務サーバ３００，３００ａ，４００，４００ａはＷｅｂサーバ機能を有する。クライアント５００，５００ａ，６００，６００ａからは、Ｗｅｂブラウザと呼ばれるソフトウェアを用いて、業務サーバ３００，３００ａ，４００，４００ａが提供するサービスを利用できる。

[0038] その場合、ファイアウォール１１では、ＨＴＴＰ（HyperText Transfer Protocol）やＨＴＴＰＳ（HTTP over Secure Socket Layer）などに対応するアプリケーションポートの通信を許可しておく。そうすれば、クライアント５００，５００ａと業務サーバ３００，３００ａ，４００，４００ａの間で、ＨＴＴＰのリクエストやレスポンスを送受信できる。ＦＴＰ（File Transfer Protocol）なども同様である。

[0039] ユーザは、クライアント５００，５００ａ，６００，６００ａを操作して第２の実施の形態の情報処理システムにアクセスできる。クライアント５００，５００ａ，６００，６００ａは、クライアントコンピュータである。クライアント５００，５００ａ，６００，６００ａは、携帯電話機やスマートデバイス（例えば、スマートフォンやタブレット端末）などの電子装置でも

よい。

[0040] クライアント５００，５００ａは、アクセスポイント１２を介してネットワーク１０に接続し、情報処理システムにアクセスする。アクセスポイント１２は無線通信を中継する中継装置である。アクセスポイント１２は移動通信網を介してネットワーク１０に接続する無線基地局でもよい。クライアント６００，６００ａは、中継装置１００ａに接続されている。クライアント６００，６００ａは、他のネットワークを介して中継装置１００ａに接続されてもよい。

[0041] 例えば、クライアント５００からサービスを利用する場合を考える。例えば、ユーザはクライアント５００で動作するＷｅｂブラウザ上で、利用したい業務アプリケーションのＵＲＬ（Uniform Resource Locator）を指定する。クライアント５００はＵＲＬ中のＦＱＤＮ（Fully Qualified Domain Name）を、ネットワーク１０に接続されたＤＮＳ（Domain Name System）サーバに問い合わせることで、ＦＱＤＮに対応するＩＰアドレスを解決する。Ｗｅｂブラウザは、解決したＩＰアドレスを宛先ＩＰアドレスとしたリクエストを送信する。こうして、クライアント５００から業務サーバが提供するサービスを利用できる。例えば、クライアント６００，６００ａからサービスを利用する場合も同様である。ＦＱＤＮでアクセス先を指定する場合、クライアント６００，６００ａからアクセス可能なネットワークセグメントにＤＮＳサーバを設けることが考えられる。

[0042] ここで、一例として、第２の実施の形態の情報処理システムで用いるＩＰアドレスを次の通りとする。ネットワーク２０のネットワークアドレスは“１９２．１６８．１０．０”である。ネットワーク３０のネットワークアドレスは“１９２．１６８．２０．０”である。中継装置１００は“１９２．１６８．１０．１”である。中継装置１００ａは“１９２．１６８．１０．２”である。中継装置１００ｂは“１９２．１６８．２０．１”である。ただし、中継装置１００ｂがネットワーク２０，３０の間のルーティングをする場合にはネットワーク２０側のＩＰアドレスを有してもよい。管理サーバ

２００は“１９２．１６８．１０．１０”である。業務サーバ３００は“１９２．１６８．１０．１０１”である。業務サーバ３００ａは“１９２．１６８．１０．１０２”である。業務サーバ４００は“１９２．１６８．２０．１０１”である。業務サーバ４００ａは“１９２．１６８．２０．１０２”である。

[0043] または、例えばＶＰＮ（Virtual Private Network）の技術を用いて、クライアント５００，５００ａに、所定のＩＰアドレス（例えば、ネットワーク２０のＩＰアドレス）を割り当ててもよい。そして、各業務サーバのＩＰアドレスを宛先に指定したリクエストを発行させてもよい。その場合、例えば、クライアント５００，５００ａにＶＰＮクライアントのソフトウェアを実行させる。例えば、ＶＰＮクライアントと通信してＩＰアドレスを割り当てるＶＰＮサーバをファイアウォール１１と中継装置１００との間などに設ける。ＶＰＮクライアントはリクエストを含むＩＰパケットを、所定のプロトコルを用いてカプセル化してＶＰＮサーバへ送る。ＶＰＮサーバは、カプセル化を解除して得たリクエストを中継装置１００に転送する。ファイアウォール１１に代えて、ＵＴＭ（Unified Threat Management）装置などを用いてＶＰＮを実装してもよい。

[0044] 図３は、第２の実施の形態の中継装置のハードウェア例を示す図である。中継装置１００は、プロセッサ１０１、ＲＡＭ１０２、ＲＯＭ（Read Only Memory）１０３、スイッチ部１０４およびポート部１０５を有する。中継装置１００ａ，１００ｂも中継装置１００と同様のユニットを用いて実現できる。

[0045] プロセッサ１０１は、ファームウェアプログラムを実行する。プロセッサ１０１は、マルチプロセッサであってもよい。プロセッサ１０１は、例えばＣＰＵ、ＭＰＵ（Micro Processing Unit）、ＤＳＰ（Digital Signal Processor）、ＡＳＩＣ（Application Specific Integrated Circuit）、ＦＰＧＡ（Field Programmable Gate Array）またはＰＬＤ（Programmable Logic Device）である。プロセッサ１０１は、ＣＰＵ、ＭＰＵ、ＤＳＰ、ＡＳＩＣ、Ｆ

ＰＧＡ、ＰＬＤのうちの２以上の要素の組み合わせであってもよい。

[0046] ＲＡＭ１０２は、ファームウェアプログラムやデータを一時的に記憶する。

ＲＯＭ１０３は、ファームウェアプログラムやデータを予め記憶している。ＲＯＭ１０３は、フラッシュメモリなど、書き換え可能な不揮発性メモリであってもよい。

[0047] スイッチ部１０４は、ポート部１０５の各ポートで受信されたフレームを取得し、プロセッサ１０１に出力する。スイッチ部１０４は、中継すると判定されたフレームをプロセッサ１０１から取得する。スイッチ部１０４は、当該フレームに含まれる宛先ＭＡＣ（Media Access Control）アドレスに基づき、当該フレームを出力するポートを判定する。スイッチ部１０４は転送先のポートを判定するための転送テーブルを保持してもよい。ネットワーク層でルーティングを行う場合には、フレーム内のＩＰパケットに含まれる宛先ＩＰアドレスから、ＡＲＰ（Address Resolution Protocol）などを用いて、ＭＡＣアドレスおよび転送先ポートを解決してもよい。スイッチ部１０４は当該フレームを判定したポートに対して出力する。

[0048] ポート部１０５は、ファイアウォール１１やネットワーク２０を介して、管理サーバ２００などの他の装置と通信する複数のポートを有する。例えば、ポート部１０５の一部がファイアウォール１１と所定のケーブルにより直接または間接に接続される。また、ポート部１０５の他の一部がネットワーク２０と所定のケーブルにより直接または間接に接続される。

[0049] 図４は、第２の実施の形態の管理サーバのハードウェア例を示す図である。管理サーバ２００は、プロセッサ２０１、ＲＡＭ２０２、ＨＤＤ（Hard Disk Drive）２０３、通信部２０４、画像信号処理部２０５、入力信号処理部２０６、ディスクドライブ２０７および機器接続部２０８を有する。各ユニットが管理サーバ２００のバスに接続されている。業務サーバ３００，３００ａ，４００，４００ａおよびクライアント５００，５００ａ，６００，６００ａも管理サーバ２００と同様のユニットを用いて実現できる。

[0050] プロセッサ２０１は、管理サーバ２００の情報処理を制御する。プロセッサ２０１は、マルチプロセッサであってもよい。プロセッサ２０１は、例えばＣＰＵ、ＭＰＵ、ＤＳＰ、ＡＳＩＣ、ＦＰＧＡまたはＰＬＤである。プロセッサ２０１は、ＣＰＵ、ＭＰＵ、ＤＳＰ、ＡＳＩＣ、ＦＰＧＡ、ＰＬＤのうちの２以上の要素の組み合わせであってもよい。

[0051] ＲＡＭ２０２は、管理サーバ２００の主記憶装置である。ＲＡＭ２０２は、プロセッサ２０１に実行させるＯＳ（Operating System）のプログラムやアプリケーションプログラムの少なくとも一部を一時的に記憶する。また、ＲＡＭ２０２は、プロセッサ２０１による処理に用いる各種データを記憶する。

[0052] ＨＤＤ２０３は、管理サーバ２００の補助記憶装置である。ＨＤＤ２０３は、内蔵した磁気ディスクに対して、磁気的にデータの書き込みおよび読み出しを行う。ＨＤＤ２０３には、ＯＳのプログラム、アプリケーションプログラム、および各種データが格納される。管理サーバ２００は、フラッシュメモリやＳＳＤ（Solid State Drive）などの他の種類の補助記憶装置を備えてもよく、複数の補助記憶装置を備えてもよい。

[0053] 通信部２０４は、ネットワーク２０を介して他のコンピュータや中継装置１００，１００ａ，１００ｂなどと通信を行えるインタフェースである。通信部２０４は、有線インタフェースでもよいし、無線インタフェースでもよい。

[0054] 画像信号処理部２０５は、プロセッサ２０１からの命令に従って、管理サーバ２００に接続されたディスプレイ２１に画像を出力する。ディスプレイ２１としては、ＣＲＴ（Cathode Ray Tube）ディスプレイや液晶ディスプレイなどを用いることができる。

[0055] 入力信号処理部２０６は、管理サーバ２００に接続された入力デバイス２２から入力信号を取得し、プロセッサ２０１に出力する。入力デバイス２２としては、例えば、マウスやタッチパネルなどのポインティングデバイス、キーボードなどを用いることができる。

[0056] ディスクドライブ２０７は、レーザ光などを利用して、光ディスク２３に記録されたプログラムやデータを読み取る駆動装置である。光ディスク２３として、例えば、ＤＶＤ（Digital Versatile Disc）、ＤＶＤ－ＲＡＭ、ＣＤ－ＲＯＭ（Compact Disc Read Only Memory）、ＣＤ－Ｒ（Recordable）／ＲＷ（ReWritable）などを使用できる。ディスクドライブ２０７は、例えば、プロセッサ２０１からの命令に従って、光ディスク２３から読み取ったプログラムやデータをＲＡＭ２０２またはＨＤＤ２０３に格納する。

[0057] 機器接続部２０８は、管理サーバ２００に周辺機器を接続するための通信インタフェースである。例えば、機器接続部２０８にはメモリ装置２４やリーダライタ装置２５を接続することができる。メモリ装置２４は、機器接続部２０８との通信機能を搭載した記録媒体である。リーダライタ装置２５は、メモリカード２６へのデータの書き込み、またはメモリカード２６からのデータの読み出しを行う装置である。メモリカード２６は、カード型の記録媒体である。機器接続部２０８は、例えば、プロセッサ２０１からの命令に従って、メモリ装置２４またはメモリカード２６から読み取ったプログラムやデータをＲＡＭ２０２またはＨＤＤ２０３に格納する。

[0058] 図５は、第２の実施の形態のソフトウェア例を示す図である。図５に示す各ユニットの一部または全部は、中継装置１００，１００ａ，１００ｂおよび管理サーバ２００のプロセッサが実行するプログラムのモジュールであってもよい。また、図５に示す各ユニットの一部または全部は、中継装置１００，１００ａ，１００ｂおよび管理サーバ２００が備えるＡＳＩＣやＦＰＧＡなどの電子回路であってもよい。なお、図５ではファイアウォール１１やアクセスポイント１２の図示を省略している。

[0059] 中継装置１００は、記憶部１１０およびアクセス制御部１２０を有する。

記憶部１１０は、アクセス制御部１２０の処理に用いられる情報を記憶する。当該情報には、セッション管理テーブルが含まれる。セッション管理テーブルは、中継することが許容されたＩＰアドレスの組み合わせを登録したアクセス制御のための情報である。以下では、当該組み合わせを示す情報を

セッション情報と呼ぶことがある。例えば、記憶部１１０はＲＡＭ１２０を用いて実装できる。

[0060] アクセス制御部１２０は、クライアント５００，５００ａからログイン認証用の情報を受信する。以下の説明では、当該ログイン認証をネットワークログイン認証ということがある。ネットワークログイン認証とは、ネットワーク２０，３０に接続するためのログイン認証である。ここで、業務サーバそれぞれが提供するサービスに対して個々にログイン認証が発生することもある。ただし、以下の説明では単にログイン認証という場合、ネットワークログイン認証を指すものとする。アクセス制御部１２０は、クライアント５００，５００ａからログイン認証用の情報を受信する。アクセス制御部１２０は、当該ログイン認証用の情報を管理サーバ２００に送信して認証を依頼する。ログイン認証用の情報は、ユーザＩＤおよびパスワードを含む。また、ログイン認証用の情報は、クライアントのアドレス情報（ＩＰアドレスやＭＡＣアドレス）などを含み得る。

[0061] アクセス制御部１２０は、ログイン認証用の情報を入力するためのＧＵＩ（Graphical User Interface）をクライアント５００，５００ａに提供してもよい。例えば、中継装置１００がＷｅｂサーバ機能を備えれば、当該ＧＵＩをＷｅｂページ（ログインページ）としてクライアント５００，５００ａに提供できる。あるいは、ログインページを提供するＷｅｂサーバを別個に設けてもよい。そして、クライアント５００，５００ａからログイン認証前に業務サーバを宛先に指定したアクセスを受け付けた場合に、ログインページのＵＲＬへアクセス先をリダイレクトさせてもよい。更に、アクセス制御部１２０は当該ログインページで入力されたユーザＩＤやパスワードを受信してもよい。

[0062] アクセス制御部１２０は、認証結果に応じたセッション情報を管理サーバ２００から受信し、記憶部１１０に記憶されたセッション管理テーブルに登録する。そして、アクセス制御部１２０は、ログイン認証後、業務サーバ３００，３００ａ，４００，４００ａ宛のリクエストを中継するとき、記憶部

１１０に記憶されたセッション管理テーブルに基づいて、当該リクエストを中継するか否かを判定する。当該リクエストを中継する場合、アクセス制御部１２０は、スイッチ部１０４に当該リクエストを出力する。スイッチ部１０４は、当該リクエストの宛先を参照し、所定のポートから当該リクエストを送出する。当該リクエストを中継しない場合、アクセス制御部１２０は当該リクエストを破棄する。

[0063] なお、記憶部１１０は第１の実施の形態の記憶手段１ａの一例である。アクセス制御部１２０は第１の実施の形態の設定手段１ｂおよび制御手段１ｃの一例である。

中継装置１００ａは、記憶部１１０ａおよびアクセス制御部１２０ａを有する。中継装置１００ｂは、記憶部１１０ｂおよびアクセス制御部１２０ｂを有する。ここで、記憶部１１０ａ，１１０ｂは記憶部１１０と同様に、セッション管理テーブルを記憶する。また、アクセス制御部１２０ａはアクセス制御部１２０と同様に、記憶部１１０ａに記憶されたセッション管理テーブルに基づいて業務サーバ３００，３００ａ，４００，４００ａに対するアクセス制御を行う。また、アクセス制御部１２０ｂはアクセス制御部１２０と同様に、記憶部１１０ｂに記憶されたセッション管理テーブルに基づいて業務サーバ３００，３００ａ，４００，４００ａに対するアクセス制御を行う。

[0064] 管理サーバ２００は、記憶部２１０および管理部２２０を有する。

記憶部２１０は、管理部２２０の処理に用いられる情報を記憶する。当該情報には、ユーザ管理テーブル、アクセス管理テーブルおよび接続管理テーブルが含まれる。ユーザ管理テーブルは、ユーザの基本情報を登録した情報である。ユーザの基本情報は、例えば、ユーザＩＤ、パスワードおよび複数クライアントを用いた同時接続（以下では多重接続ということがある）の可否などを示す情報を含む。アクセス管理テーブルは、ユーザごとにアクセスを許容する業務サーバのＩＰアドレスを登録した情報である。接続管理テーブルは、中継装置１００，１００ａ，１００ｂにおける現在の接続状態を管

理するための情報である。例えば、記憶部２１０はＲＡＭ２０２やＨＤＤ２０３を用いて実装できる。

[0065] 管理部２２０は、中継装置１００，１００ａ，１００ｂから認証依頼を受信すると、記憶部２１０に記憶された情報に基づいて、認証処理を実行する。管理部２２０は、認証結果に応じて、セッション情報を生成し、依頼元の中継装置に提供する。

[0066] なお、記憶部２１０は第１の実施の形態の記憶手段２ａの一例である。管理部２２０は第１の実施の形態の提供手段２ｂの一例である。

図６は、第２の実施の形態のユーザ管理テーブルの例を示す図である。ユーザ管理テーブル２１１は記憶部２１０に格納される。ユーザ管理テーブル２１１は、ユーザＩＤ、パスワードおよび多重接続設定の項目を含む。

[0067] ユーザＩＤの項目には、ユーザＩＤが登録される。パスワードの項目には、パスワードが登録される。多重接続設定の項目には、多重接続を許容するか否かを示す許可情報が登録される。例えば、多重接続が許容される場合には“可”という情報が、多重接続が許容されていない場合には“不可”という情報が、多重接続設定の項目に登録される。

[0068] 例えば、ユーザ管理テーブル２１１には、ユーザＩＤが“ＵＩＤ０００１”、パスワードが“ｐａｓｓ１”、多重接続設定が“可”という情報が登録されている。これは、ユーザＩＤ“ＵＩＤ０００１”に対してログイン用のパスワードとして“ｐａｓｓ１”が設定されていること、当該ユーザについて多重接続が許容されていることを示す。

[0069] ここで、以下ではユーザＩＤ“ＵＩＤ０００１”のユーザをユーザＡと呼ぶ。ユーザＩＤ“ＵＩＤ０００２”のユーザをユーザＢと呼ぶ。ユーザＩＤ“ＵＩＤ０００３”のユーザをユーザＣと呼ぶ。

[0070] ユーザ管理テーブル２１１の設定内容は、ユーザごとの多重接続の許可情報を変更したい場合などに、例えば情報処理システムの管理者により、適宜変更可能である。

図７は、第２の実施の形態のアクセス管理テーブルの例を示す図である。

アクセス管理テーブル２１２は記憶部２１０に格納される。アクセス管理テーブル２１２は、ＲＯＬＥ、ユーザＩＤ、端末ＩＰアドレス、端末ＭＡＣアドレスおよびＡＣＬ（Access Control List）の項目を含む。

[0071] ＲＯＬＥの項目には、レコード（１行分のデータ単位）を識別するためのＲＯＬＥ番号が登録される。例えば、“ＲＯＬＥ１”という場合、アクセス管理テーブル２１２のＲＯＬＥの項目にＲＯＬＥ番号“１”が設定されたレコードを示す。ＲＯＬＥという用語をアクセス管理テーブル２１２のある１つのレコードを指す用語として用いることがある。

[0072] ユーザＩＤの項目には、ユーザＩＤが登録される。端末ＩＰアドレスの項目には、クライアントのＩＰアドレスが登録される。端末ＭＡＣアドレスの項目には、クライアントのＭＡＣアドレスが登録される。ＡＣＬの項目には、アクセスが許容された業務サーバのＩＰアドレスのリストが登録される。ＡＣＬの項目には、１つのＲＯＬＥにつき複数のＩＰアドレスを登録できる。ＡＣＬの項目を細分化した“１”、“２”、“３”、“４”の番号は便宜的に付したものである。更に多数のアクセス先サーバが存在する場合には、５個以上のＩＰアドレスが登録されてもよい。

[0073] アクセス管理テーブル２１２には、各レコードにおいて情報が登録されていない項目もある。その場合にはハイフン記号“－”を表記している。端末ＩＰアドレスの項目で“－”が登録されている場合は、任意の端末ＩＰアドレスを示す。端末ＭＡＣアドレスの項目で“－”が登録されている場合は、任意のＭＡＣアドレスを示す。

[0074] 例えば、アクセス管理テーブル２１２には、ＲＯＬＥが“１”、ユーザＩＤが“ＵＩＤ０００１”、端末ＩＰアドレスが“１９２．１６８．１０．１１”、端末ＭＡＣアドレスが“０８－ｂ４－２５－９ｅ－０ｃ－４６”、ＡＣＬが“１９２．１６８．１０．１０１”、“１９２．１６８．１０．１０２”、“１９２．１６８．２０．１０１”、“１９２．１６８．２０．１０２”という情報が登録されている。

[0075] これは、ユーザＩＤ“０００１”のユーザＡが、ＩＰアドレス“１９２．

１６８．１０．１１”、ＭＡＣアドレス“０８－ｂ４－２５－９ｅ－０ｃ－４６”であるクライアントからアクセスする場合、当該ＡＣＬのＩＰアドレスへのアクセスが許容されることを示す。この場合、業務サーバ３００，３００ａ，４００，４００ａへのアクセスが許容されていることになる。

[0076] これに対し、“ＲＯＬＥ２”では、同一のユーザＩＤ“ＵＩＤ０００１”およびＩＰアドレス“１９２．１６８．１０．１１”に対して、ＡＣＬが“１９２．１６８．１０．１０１”、“１９２．１６８．２０．１０１”である。

[0077] これは、ユーザＩＤ“０００１”のユーザＡが、ＩＰアドレス“１９２．１６８．１０．１１”であるクライアントからアクセスする場合、当該ＡＣＬのＩＰアドレスへのアクセスが許容されることを示す。“ＲＯＬＥ２”では、“ＲＯＬＥ１”に比べて、ＭＡＣアドレスの一致は課していない。この場合、業務サーバ３００，４００へのアクセスが許容されていることなる。なお、ＩＰアドレス“１９２．１６８．１０．１１”およびＭＡＣアドレス“０８－ｂ４－２５－９ｅ－０ｃ－４６”の両方が認証用の情報から検出される場合は、“ＲＯＬＥ２”よりも“ＲＯＬＥ１”が優先して適用される。

[0078] また、“ＲＯＬＥ３”では、同一のユーザＩＤ“ＵＩＤ０００１”に対して、ＡＣＬが“１９２．１６８．１０．１０１”という情報が登録されている。“ＲＯＬＥ３”では、“ＲＯＬＥ１”や“ＲＯＬＥ２”に比べて、ＩＰアドレスおよびＭＡＣアドレスの一致は課していない。この場合、業務サーバ３００へのアクセスが許容されていることになる。ＩＰアドレス“１９２．１６８．１０．１１”およびＭＡＣアドレス“０８－ｂ４－２５－９ｅ－０ｃ－４６”の両方が認証用の情報から検出される場合は、“ＲＯＬＥ３”よりも“ＲＯＬＥ１”が優先して適用される。ＩＰアドレス“１９２．１６８．１０．１１”のみが認証用の情報から検出される場合は、“ＲＯＬＥ３”よりも“ＲＯＬＥ２”が優先して適用される。それ以外の場合に“ＲＯＬＥ３”が適用される。

[0079] このように、アクセス管理テーブル２１２にはユーザごとのＲＯＬＥが登

録される。１ユーザに対して複数のＲＯＬＥを登録してもよい。また、ＡＣＬにはネットワークアドレスなどを用いてアクセスを許容するＩＰアドレスの範囲を登録してもよい。

[0080] １つの業務サーバで（例えば、提供するサービスごとに）複数のＩＰアドレスを利用することもある。その場合には、当該１つの業務サーバの複数のＩＰアドレスのうち、アクセスを許容したいＩＰアドレスのみをＡＣＬに登録すればよい。

[0081] アクセス管理テーブル２１２の設定内容は、ユーザの追加／削除、業務サーバの追加／削除、業務サーバのネットワーク接続変更などが発生した際に、設定変更が可能である。例えば、情報処理システムの管理者は、これらの変更が発生した際に、アクセス管理テーブル２１２の設定内容を変更することができる。

[0082] 図８は、第２の実施の形態の接続管理テーブルの例を示す図である。接続管理テーブル２１３は、記憶部２１０に格納される。接続管理テーブル２１３は、管理部２２０により更新される。接続管理テーブル２１３は、ユーザＩＤ、端末ＩＰアドレス、中継装置ＩＰアドレスおよび適用ＲＯＬＥの項目を含む。

[0083] ユーザＩＤの項目には、ユーザＩＤが登録される。端末ＩＰアドレスの項目には、クライアントのＩＰアドレスが登録される。中継装置ＩＰアドレスの項目には、認証依頼を行った中継装置のＩＰアドレスが登録される。適用ＲＯＬＥの項目には、認証された結果、適用されるＲＯＬＥを示す情報が登録される。ここで、適用されるＲＯＬＥとは、管理サーバ２００により当該中継装置に提供されるＲＯＬＥである。ＲＯＬＥの提供を受けた後、当該中継装置は、当該ＲＯＬＥに基づくアクセス制御を行えるようになる。接続管理テーブル２１３は、中継装置に提供されたＲＯＬＥの履歴ということもできる。

[0084] 例えば、接続管理テーブル２１３には、ユーザＩＤが“ＵＩＤ０００１”、端末ＩＰアドレスが“５０．２２３．３．４”、中継装置ＩＰアドレスが

“１９２．１６８．１０．１”、適用ＲＯＬＥが“ＲＯＬＥ３”という情報が登録されている。

[0085] これは、ユーザＩＤ“ＵＩＤ０００１”のユーザＡがＩＰアドレス“５０．２２３．３．４”のクライアントを用いて、中継装置１００（ＩＰアドレス“１９２．１６８．１０．１”）を介した業務サーバへのアクセスが可能であることを示す。また、アクセス制御のために適用されるＲＯＬＥが“ＲＯＬＥ３”であることを示す。ここで、ＩＰアドレス“５０．２２３．３．４”は、例えばクライアント５００のＩＰアドレスである。

[0086] また、例えば接続管理テーブル２１３には、ユーザＩＤが“ＵＩＤ０００１”、端末ＩＰアドレスが“１９２．１６８．１０．１１”、中継装置ＩＰアドレスが“１９２．１６８．１０．２”、適用ＲＯＬＥが“ＲＯＬＥ１”という情報が登録されている。

[0087] これは、ユーザＩＤ“ＵＩＤ０００１”のユーザＡが、ＩＰアドレス“１９２．１６８．１０．１１”のクライアントを用いて、中継装置１００ａ（ＩＰアドレス“１９２．１６８．１０．２”）を介した業務サーバへのアクセスが可能であることを示す。また、アクセス制御のために適用されるＲＯＬＥが“ＲＯＬＥ１”であることを示す。ここで、ＩＰアドレス“１９２．１６８．１０．１１”は、例えばクライアント６００のＩＰアドレスである。

[0088] 例えば、接続管理テーブル２１３には、ユーザＩＤ“ＵＩＤ０００２”のユーザＢおよびユーザＩＤ“ＵＩＤ０００３”のユーザＣに対しても同様のレコードが登録されている。レコードに登録された各情報の意味は上述した通りである。ここで、ユーザＢはクライアント５００ａを利用しているとする。接続管理テーブル２１３において、ＩＰアドレス“５０．２２３．５．５”はクライアント５００ａのＩＰアドレスである。また、ユーザＣはクライアント６００ａを利用しているとする。接続管理テーブル２１３において、ＩＰアドレス“１９２．１６８．１０．１２”はクライアント６００ａのＩＰアドレスである。

[0089] １つのクライアントに対して、２つのレコードが接続管理テーブル２１３に登録されることもある。例えば、クライアント６００，６００ａについて２つ目のレコードが次のように登録されている。

[0090] 例えば、接続管理テーブル２１３には、ユーザＩＤが“ＵＩＤ０００１”、端末ＩＰアドレスが“１９２．１６８．１０．１１”、中継装置ＩＰアドレスが“１９２．１６８．２０．１”、適用ＲＯＬＥが“ＲＯＬＥ１”という情報が登録されている。

[0091] これは、ユーザＩＤ“ＵＩＤ０００１”のユーザＡが、クライアント６００（ＩＰアドレス“１９２．１６８．１０．１１”）を用いて、中継装置１００ｂ（ＩＰアドレス“１９２．１６８．２０．１”）を介した業務サーバへのアクセスが可能であることを示す。また、アクセス制御のために適用されるＲＯＬＥが“ＲＯＬＥ１”であることを示す。

[0092] また、例えば接続管理テーブル２１３には、ユーザＩＤが“ＵＩＤ０００３”、端末ＩＰアドレスが“１９２．１６８．１０．１２”、中継装置ＩＰアドレスが“１９２．１６８．２０．１”、適用ＲＯＬＥが“ＲＯＬＥ６”という情報が登録されている。

[0093] これは、ユーザＩＤ“ＵＩＤ０００３”のユーザＣが、クライアント６００ａ（ＩＰアドレス“１９２．１６８．１０．１２”）を用いて、中継装置１００ｂ（ＩＰアドレス“１９２．１６８．２０．１”）を介した業務サーバへのアクセスが可能であることを示す。またアクセス制御のために適用されるＲＯＬＥが“ＲＯＬＥ６”であることを示す。

[0094] なお、接続管理テーブル２１３では、中継装置ＩＰアドレス以外を用いて、中継装置を登録してもよい。例えば、中継装置１００，１００ａ，１００ｂそれぞれに所定の識別名称を予め付与しておく。そして、接続管理テーブル２１３には、中継装置ＩＰアドレスの項目に代えて、当該識別名称を設定する項目を設けてもよい。

[0095] 図９は、第２の実施の形態のセッション管理テーブルの例を示す図である。図９（Ａ）はセッション管理テーブル１１１を例示している。セッション

管理テーブル１１１は、記憶部１１０に格納される。セッション管理テーブル１１１は、アクセス制御部１２０により更新される。セッション管理テーブル１１１は、ＲＯＬＥ、端末ＩＰアドレスおよびＡＣＬの項目を含む。

[0096] ＲＯＬＥの項目には、セッション情報の元となったＲＯＬＥのＲＯＬＥ番号が登録される。端末ＩＰアドレスの項目には、クライアントのＩＰアドレスが登録される。ＡＣＬの項目には、中継を許容する業務サーバのＩＰアドレスが登録される。ＡＣＬの項目を細分化した“１”、“２”、“３”、“４”の番号は、アクセス管理テーブル２１２と同様に、便宜的に付したものである。セッション管理テーブル１１１には、各レコードにおいて情報が登録されていない箇所もある。その箇所にはハイフン記号“－”を表記している。

[0097] 例えば、セッション管理テーブル１１１には、ＲＯＬＥが“３”、端末ＩＰアドレスが“５０．２２３．３．４”、ＡＣＬが“１９２．１６８．１０．１０１”という情報が登録されている。これは、送信元／宛先ＩＰアドレスの組が“５０．２２３．３．４”、“１９２．１６８．１０．１０１”である通信データの中継を許容することを示す。すなわち、送信元ＩＰアドレス“５０．２２３．３．４”、宛先ＩＰアドレス“１９２．１６８．１０．１０１”の場合（上り）も、送信元ＩＰアドレス“１９２．１６８．１０．１０１”、宛先ＩＰアドレス“５０．２２３．３．４”の場合（下り）も中継を許容する。

[0098] また、例えばセッション管理テーブル１１１には、ＲＯＬＥが“５”、端末ＩＰアドレスが“５０．２２３．５．５”、ＡＣＬが“１９２．１６８．１０．１０１”、“１９２．１６８．１０．１０２”という情報が登録されている。これは、送信元／宛先ＩＰアドレスの組が“５０．２２３．５．５”、“１９２．１６８．１０．１０１”である通信データの中継を許容することを示す。また、送信元／宛先ＩＰアドレスの組が“５０．２２３．５．５”、“１９２．１６８．１０．１０２”である通信データの中継を許容することを示す。

[0099] 図９（Ｂ）はセッション管理テーブル１１１ａを例示している。セッション管理テーブル１１１ａは、記憶部１１０ａに格納される。セッション管理テーブル１１１ａは、アクセス制御部１２０ａにより更新される。セッション管理テーブル１１１ａに含まれる項目の設定内容はセッション管理テーブル１１１と同様であるため、説明を省略する。

[0100] 図９（Ｃ）はセッション管理テーブル１１１ｂを例示している。セッション管理テーブル１１１ｂは、記憶部１１０ｂに格納される。セッション管理テーブル１１１ｂは、アクセス制御部１２０ｂにより更新される。セッション管理テーブル１１１ｂに含まれる項目の設定内容はセッション管理テーブル１１１と同様であるため、説明を省略する。

[0101] ここで、セッション管理テーブル１１１，１１１ａ，１１１ｂは、接続管理テーブル２１３で示される接続状態である場合の、中継装置１００，１００ａ，１００ｂが保持するセッション情報群に相当する。１レコードが１つのセッション情報である。

[0102] なお、セッション管理テーブル１１１，１１１ａ，１１１ｂはユーザＩＤやパスワードの項目を含んでもよい。管理サーバ２００はユーザＩＤやパスワードを含むセッション情報を中継装置１００，１００ａ，１００ｂに提供してもよい。このようにすれば、例えば、中継装置１００はセッション管理テーブル１１１に登録された端末ＩＰアドレスからアクセスを受け付けたとき、当該端末ＩＰアドレスに対するユーザＩＤをアクセスログに記録できる。

[0103] また、セッション管理テーブル１１１，１１１ａ，１１１ｂは、ＭＡＣアドレスの項目を含んでもよい。管理サーバ２００は端末ＭＡＣアドレスを含むセッション情報を中継装置１００，１００ａ，１００ｂに提供してもよい。例えば、中継装置１００におけるクライアント５００などの識別にＭＡＣアドレスを用いたい場合も考えられるからである。

[0104] 図１０は、第２の実施の形態の通信データの例を示す図である。図１０では、第２の実施の形態の情報処理システムで送受信される通信データを例示

している。フレーム４０は、イーサネットフレーム（イーサネットおよびＥｔｈｅｒｎｅｔは登録商標）の例である。フレーム４０は、プリアンブル、宛先ＭＡＣアドレス、送信元ＭＡＣアドレス、タイプ、ペイロード、ＦＣＳ（Frame Check Sequence）のフィールドを含む。

[0105] プリアンブルは同期用の信号を含むフィールドである。宛先ＭＡＣアドレスはＯＳＩ参照モデルの第２層（データリンク層）の経路選択に用いられる宛先のＭＡＣアドレスを設定するフィールドである。送信元ＭＡＣアドレスは送信元のＭＡＣアドレスを設定するフィールドである。タイプは上位層プロトコル（例えば、ＩＰ）を示す情報を設定するフィールドである。ペイロードは上位層プロトコルで扱うデータの本体を設定するフィールドである。ＦＣＳはフレームエラーを検出するための情報を設定するフィールドである。

[0106] ＩＰパケット５０はフレーム４０のペイロードに含まれる。ＩＰパケット５０はデータグラムと呼ばれることもある。ＩＰパケット５０は送信元ＩＰアドレス、宛先ＩＰアドレスおよびデータのフィールドを含む。

[0107] 送信元ＩＰアドレスは、ＯＳＩ参照モデルの第３層（ネットワーク層）の経路選択に用いられる送信元のＩＰアドレスを設定するフィールドである。宛先ＩＰアドレスは送信元のＩＰアドレスを設定するフィールドである。データは、通信データ本体を設定するフィールドである。

[0108] データ６０は、ＩＰパケット５０のデータのフィールドに含まれる。例えば、何れかのクライアントが何れかの中継装置に対してログイン認証用の情報を送信する場合、データ６０にはユーザＩＤおよびパスワードが含まれ得る。また、何れかの中継装置が管理サーバ２００に認証依頼などを行う場合、データ６０にはクライアントのＩＰアドレスやＭＡＣアドレスなどが含まれ得る。データ６０に含まれるユーザＩＤ、パスワードおよびアドレス情報などは、ＯＳＩ参照モデルの第７層（アプリケーション層）の情報でもよい。

[0109] 次に、第２の実施の形態における各処理の手順を説明する。以下では、ク

ライアント５００が中継装置１００などを介して業務サーバにアクセスする場合を主に例示するが、他のクライアントおよび他の中継装置を用いる場合も同様の手順である。まず、ネットワークログイン認証の手順を説明する。

[0110] 図１１は、第２の実施の形態の認証処理の例を示すフローチャートである。以下、図１１に示す処理をステップ番号に沿って説明する。

（ステップＳ１１）アクセス制御部１２０は、クライアント５００からログイン認証用の情報を受信する。例えば、ユーザＡは、クライアント５００上のＷｅｂブラウザを用いてユーザＩＤやパスワードを入力するためのＷｅｂページ（ログインページ）へアクセスする。例えば、ユーザＡは自身のユーザＩＤ“ＵＩＤ０００１”およびパスワード“ｐａｓｓ１”を当該ログインページに入力する。クライアント５００は、入力された情報（ログイン認証用の情報）を含むフレームを中継装置１００へ宛てて送信する。アクセス制御部１２０は当該フレームを受信する。フレーム内のＩＰパケットには、送信元ＩＰアドレスおよび送信元ＭＡＣアドレスが含まれる。この場合、送信元ＩＰアドレスは“５０．２２３．３．４”である。送信元ＭＡＣアドレスは所定のＭＡＣアドレスである。アクセス制御部１２０は、これらのアドレス情報も抽出して、ログイン認証用の情報に加える。

[0111] （ステップＳ１２）アクセス制御部１２０は、ログイン認証用の情報を含む認証依頼を管理サーバ２００に送信する。ログイン認証用の情報は、ＩＰパケットのデータ部分に格納されて管理サーバ２００に送信される。管理部２２０は中継装置１００から認証依頼を受信する。

[0112] （ステップＳ１３）管理部２２０は、記憶部２１０に記憶されたユーザ管理テーブル２１１を参照して、ユーザＩＤとパスワードとを照合する。照合成功である場合、処理をステップＳ１４に進める。照合成功でない（照合失敗）の場合、処理をステップＳ１９に進める。具体的には、認証依頼に含まれるユーザＩＤとパスワードとの組がユーザ管理テーブル２１１に登録されていれば照合成功である。認証依頼に含まれるユーザＩＤとパスワードとの組がユーザ管理テーブル２１１に登録されていなければ照合失敗である。

[0113] （ステップＳ１４）管理部２２０は、記憶部２１０に記憶されたアクセス管理テーブル２１２を参照して、ＡＣＬを検索する。検索のキーは、認証依頼に含まれるユーザＩＤ、送信元ＩＰアドレスおよび送信元ＭＡＣアドレスである。管理部２２０は、少なくともユーザＩＤが一致するレコードがあれば、該当のレコードを検索結果として抽出する。検索結果が複数件になる場合もある。その場合は、一致するキーが最大のものを１件抽出して検索結果とする。本例の場合は、ユーザＩＤ“ＵＩＤ０００１”、クライアント５００のＩＰアドレス“５０．２２３．３．４”（および送信元ＭＡＣアドレス）を取得している。この場合、“ＲＯＬＥ３”のレコードが検索結果として得られることになる。

[0114] （ステップＳ１５）管理部２２０は、ステップＳ１４においてＡＣＬを検索できたか否かを判定する。検索できた場合、処理をステップＳ１６に進める。検索できなかった場合、処理をステップＳ１９に進める。

[0115] （ステップＳ１６）管理部２２０は、処理中のユーザにつき多重接続の制約があるか否かを判定する。多重接続の制約がある場合、処理をステップＳ１９に進める。多重接続の制約がない場合、処理をステップＳ１７に進める。多重接続の制約があるとは次の場合である。すなわち、（１）処理中のユーザにつきユーザ管理テーブル２１１の多重接続設定が“不可”であり、かつ、（２）当該ユーザにつき認証依頼で受け付けた送信元ＩＰアドレスとは別の端末ＩＰアドレスのレコードが接続管理テーブル２１３に登録済の場合である。（１）、（２）の何れか一方が満たされていない場合は、多重接続の制約はないと判定する。

[0116] （ステップＳ１７）管理部２２０は、接続管理テーブル２１３を更新する。具体的には、管理部２２０は認証依頼で受け付けたユーザＩＤ、送信元ＩＰアドレス（端末ＩＰアドレス）およびステップＳ１４で検索したレコードのＲＯＬＥ番号（適用ＲＯＬＥ）を接続管理テーブル２１３に登録する。また、認証依頼（のフレームに含まれるＩＰパケット）には、送信元ＩＰアドレスとして中継装置１００のＩＰアドレスが設定されている。よって、当該

中継装置１００のＩＰアドレス（中継装置ＩＰアドレス）も接続管理テーブル２１３に登録する。

[0117] （ステップＳ１８）管理部２２０は、アクセス管理テーブル２１２に基づいて、セッション情報を生成する。具体的には、ステップＳ１４で検索したＲＯＬＥのＲＯＬＥ番号、端末ＩＰアドレスおよびＡＣＬの組み合わせをセッション情報とする。ステップＳ１４で“ＲＯＬＥ３”を取得している場合、当該レコードには端末ＩＰアドレスが未設定である。この場合、管理部２２０は認証依頼で受け付けた送信元ＩＰアドレスを端末ＩＰアドレスに設定してセッション情報とする。ユーザＩＤも提供する場合、管理部２２０はセッション情報にユーザＩＤを含めて提供してもよい（以下、同様）。管理部２２０は、当該セッション情報と認証成功とを中継装置１００に応答する。そして、処理をステップＳ２０に進める。

[0118] （ステップＳ１９）管理部２２０は、認証失敗を中継装置１００に応答する。

（ステップＳ２０）アクセス制御部１２０は、認証依頼に対する応答を管理サーバ２００から受信し、当該応答に基づいて認証成功であるか否かを判定する。認証成功である場合、処理をステップＳ２１に進める。認証失敗である場合、処理をステップＳ２３に進める。

[0119] （ステップＳ２１）アクセス制御部１２０は、認証成功とともに受信したセッション情報を記憶部１１０に記憶されたセッション管理テーブル１１１に登録する。上記の例では、セッション管理テーブル１１１に“ＲＯＬＥ３”のレコードが登録されることになる。

[0120] （ステップＳ２２）アクセス制御部１２０は、クライアント５００に認証成功を応答する。そして、処理を終了する。

（ステップＳ２３）アクセス制御部１２０は、クライアント５００に認証失敗を応答する。そして、処理を終了する。

[0121] このようにして、中継装置１００および管理サーバ２００は、ネットワークログイン認証を行う。ステップＳ１８では、受け付けた送信元ＩＰアドレ

スと一致する端末ＩＰアドレスのレコードが存在しない場合でも、対応するユーザにつき所定のＲＯＬＥ（端末ＩＰアドレスが設定されていないＲＯＬＥ）を抽出してセッション情報を生成する。このため、例えば、クライアント５００のＩＰアドレスが動的に割り当てられている場合にも当該所定のＲＯＬＥを適用することができる。具体的には、クライアント５００が移動通信網を介して通信する場合やクライアント６００に固定のＩＰアドレスを割り当てない場合など、ＤＨＣＰ（Dynamic Host Configuration Protocol）を用いてクライアントに動的にＩＰアドレスが割り当てられることもある。すなわち、クライアントに静的ＩＰアドレスが割り当てられている場合に限らず、動的ＩＰアドレスが割り当てられている場合にもクライアントからのアクセス制御が可能である。

[0122] なお、ステップＳ１８では、アクセス管理テーブル２１２のＲＯＬＥにおいて、端末ＩＰアドレスが未設定のものを用いてセッション情報を生成する際に、中継装置１００から取得したクライアント６００のＩＰアドレスを管理部２２０が設定するものとした。一方、アクセス制御部１２０が当該設定の処理を行ってもよい。具体的には、管理部２２０は、“ＲＯＬＥ３”について端末ＩＰアドレスを未設定の状態でセッション情報を生成し、中継装置１００に送る。そして、ステップＳ２１において、アクセス制御部１２０の責任によりステップＳ１１で抽出した送信元ＩＰアドレスを当該セッション情報に設定して、セッション管理テーブル１１１に登録する。

[0123] また、ユーザ管理テーブル２１１でパスワードを管理するものとしたが、アクセス管理テーブル２１２でパスワードを管理してもよい。そうすれば、同一ユーザであってもＲＯＬＥごとに異なるパスワードを認証用に利用できる。すなわち、管理部２２０は、ステップＳ１４においてＡＣＬを検索する際にパスワードもキーに用いる。この場合、ステップＳ１３をスキップしてもよい。

[0124] 次に、中継装置１００による通信データの中継処理の手順を説明する。

図１２は、第２の実施の形態の中継処理の例を示すフローチャートである

。以下、図１２に示す処理をステップ番号に沿って説明する。

[0125] （ステップＳ３１）アクセス制御部１２０は、中継対象の通信データを受信する。例えば、この通信データはクライアント５００が業務サーバ３００へ宛てて送信したリクエストである。その場合、当該リクエストの宛先ＩＰアドレスは“１９２．１６８．１０．１０１”である。また、当該リクエストの送信元ＩＰアドレスは“５０．２２３．３．４”である。アクセス制御部１２０は、通信データのＩＰパケットから送信元ＩＰアドレスを抽出する。

[0126] （ステップＳ３２）アクセス制御部１２０は、記憶部１１０に記憶されたセッション管理テーブル１１１を参照して、当該送信元ＩＰアドレスに対応するセッション情報があるか否かを判定する。送信元ＩＰアドレスに対応するセッション情報がある場合、処理をステップＳ３８に進める。送信元ＩＰアドレスに対応するセッション情報がない場合、処理をステップＳ３３に進める。

[0127] （ステップＳ３３）アクセス制御部１２０は、当該送信元ＩＰアドレスが接続管理テーブル２１３に登録済であるか否かを問い合わせるための確認要求を管理サーバ２００に送信する。この確認要求を認証の確認要求と呼ぶことがある。このように呼ぶ理由は次の通りである。図１１で説明した認証処理に成功していれば（認証済であれば）、管理サーバ２００は接続管理テーブル２１３に当該送信元ＩＰアドレスを登録しているはずである。このため、当該送信元ＩＰアドレスが接続管理テーブル２１３に登録済であるか否かの確認は、結果的に認証処理の成否（認証済か否か）を確認することになるからである。当該確認要求に対する管理サーバ２００の処理手順は後述する。

[0128] （ステップＳ３４）アクセス制御部１２０は、認証の確認要求に対する応答を管理サーバ２００から受信する。当該応答には、認証済であるか否かの確認結果が含まれる。また、確認結果が認証済である場合、適用ＲＯＬＥに対応するセッション情報が当該応答に含まれる。セッション情報はステップ

Ｓ３１で抽出された送信元ＩＰアドレスとＡＣＬとの組み合わせを含む。

[0129] （ステップＳ３５）アクセス制御部１２０は、当該応答に基づいて認証済であるか否かを判定する。認証済である場合、処理をステップＳ３６に進める。認証済でない場合、処理をステップＳ３７に進める。

[0130] （ステップＳ３６）アクセス制御部１２０は、受信したセッション情報をセッション管理テーブル１１１に登録する。そして、処理をステップＳ３８に進める。

（ステップＳ３７）アクセス制御部１２０は、ログインページにリダイレクトさせる。例えば、クライアント５００から受信したＨＴＴＰのリクエスト（ステップＳ３１のリクエスト）を、ログインページのＵＲＬを指定したリクエストに置き換えて転送する。ログインページの提供は中継装置１００が行ってもよいし、他のＷｅｂサーバが行ってもよい。すると、クライアント５００のＷｅｂブラウザにはログインページが表示され、ユーザＩＤやパスワード（認証用の情報）の入力がユーザに促される。そして、処理を終了する。ユーザＩＤおよびパスワードを受け付けた後の手順は図１１の認証処理の手順となる。この場合、ステップＳ３１で受信した通信データの中継は行われないことになる。例えば、当該通信データをＲＡＭなどに格納して中継を保留しておき、認証に成功した後に、中継を行うかを再度判断するようにしてもよい。

[0131] （ステップＳ３８）アクセス制御部１２０は、セッション管理テーブル１１１を参照して、ステップＳ３１で抽出された送信元／宛先ＩＰアドレス間の中継が許容されているか否かを判定する。中継が許容されている場合、処理をステップＳ３９に進める。中継が許容されていない場合、処理をステップＳ４０に進める。

[0132] （ステップＳ３９）アクセス制御部１２０は、ステップＳ３１で受信した通信データをスイッチ部１０４に出力する。スイッチ部１０４は宛先ＩＰアドレスに対して通信データを転送する（通信データが中継される）。そして、処理を終了する。

[0133] （ステップＳ４０）アクセス制御部１２０は、ステップＳ３１で受信した通信データを破棄する。すなわち、当該通信データを中継しない。そして、処理を終了する。

このようにして、中継装置１００は通信データの中継を行う。中継装置１００は、通信データに含まれる送信元ＩＰアドレスおよび宛先ＩＰアドレスの組み合わせと、セッション管理テーブル１１１とを照合して、通信データを中継するか否かを判定する。通信データを中継しない場合には、当該宛先ＩＰアドレスへのアクセスが許可されていない旨をクライアント５００に通知してもよい。

[0134] また、ステップＳ３３，Ｓ３４のように管理サーバ２００に認証の確認要求を行う理由は、１つのクライアントが複数の中継装置を介して異なる業務サーバにアクセスする可能性があるからである。例えば、クライアント６００，６００ａは中継装置１００ａ，１００ｂの両方を経由して業務サーバ４００，４００ａにアクセスする可能性がある。認証の確認要求を行うことで、ユーザに対して中継装置１００ａで認証操作を行った後、中継装置１００ｂで再度の認証操作を課さずに済む。よって、再度の認証操作を課す場合よりもユーザの手間を省ける。

[0135] 次に、ステップＳ３３，Ｓ３４の間で実行される管理サーバ２００の処理手順を説明する。

図１３は、第２の実施の形態の認証確認例（その１）を示すフローチャートである。以下、図１３に示す処理をステップ番号に沿って説明する。

[0136] （ステップＳ４１）管理部２２０は、ステップＳ３３の確認要求を中継装置１００から受信する。確認要求には確認対象のクライアントのＩＰアドレスが含まれる。

（ステップＳ４２）管理部２２０は、記憶部２１０に記憶された接続管理テーブル２１３を参照して、当該ＩＰアドレスが登録済であるか否かを判定する。登録済である場合、処理をステップＳ４３に進める。登録済でない場合、処理をステップＳ４５に進める。接続管理テーブル２１３の端末ＩＰア

ドレスの項目に、当該ＩＰアドレスが設定されたレコードが存在する場合、登録済である。一方、接続管理テーブル２１３の端末ＩＰアドレスの項目に当該ＩＰアドレスが設定されたレコードが存在しない場合、登録済でない。

[0137] （ステップＳ４３）管理部２２０は、接続管理テーブル２１３を更新する。具体的には、管理部２２０は確認要求で受け付けたクライアントのＩＰアドレス（端末ＩＰアドレス）を含むレコードを接続管理テーブル２１３に追加する。追加されるレコードは、ステップＳ４２で登録済と判断した根拠となるレコードのユーザＩＤおよび適用ＲＯＬＥの設定値を含む。また、追加されるレコードは、確認要求の送信元ＩＰアドレスである中継装置１００のＩＰアドレス（中継装置ＩＰアドレス）を含む。具体的には、確認要求（のフレームに含まれるＩＰパケット）は送信元ＩＰアドレスとして中継装置１００のＩＰアドレスを含む。このＩＰアドレスを当該レコードの中継装置ＩＰアドレスの項目に設定する。

[0138] （ステップＳ４４）管理部２２０は、アクセス管理テーブル２１２に基づいて、セッション情報を生成する。具体的には、ステップＳ４３で新たなレコードに設定した適用ＲＯＬＥのＲＯＬＥ番号、端末ＩＰアドレスおよび当該ＲＯＬＥ番号に対応するＡＣＬの組み合わせをセッション情報とする。そして、管理部２２０は、確認要求に対して、認証済である旨を中継装置１００に応答する。当該応答には、生成したセッション情報が含まれる。そして、処理を終了する。

[0139] （ステップＳ４５）管理部２２０は、確認要求に対して未認証である旨を中継装置１００に応答する。そして、処理を終了する。

このようにして、管理サーバ２００は中継装置１００からの確認要求に対して認証確認の処理を実行する。次に、図１１～１３の手順を実行する中継装置１００，１００ａ，１００ｂおよび管理サーバ２００の通信の具体例を説明する。

[0140] 図１４は、第２の実施の形態の通信の具体例（その１）を示す図である。以下、図１４に示す処理をステップ番号に沿って説明する。ステップＳＴ１

０１の直前では、セッション管理テーブル１１１および接続管理テーブル２１３のエントリ（登録されたレコード）はないものとする。

[0141] （ステップＳＴ１０１）クライアント５００は、ログインページでユーザＡにより入力されたログイン認証用の情報を中継装置１００に送信する。当該認証用の情報には、ユーザＩＤ“ＵＩＤ０００１”およびパスワード“ｐａｓｓ１”が含まれる。中継装置１００は認証用の情報を受信する。認証用の情報は、図１０で説明したフレームを用いて中継装置１００に送られる。

[0142] （ステップＳＴ１０２）中継装置１００は、当該フレームから送信元ＩＰアドレス“５０．２２３．３．４”および送信元ＭＡＣアドレスを抽出する。中継装置１００は送信元ＩＰアドレスおよび送信元ＭＡＣアドレスを、ステップＳＴ１０１で受信した認証用の情報に加える。すなわち、抽出した送信元ＩＰアドレスおよび送信元ＭＡＣアドレスをＩＰパケットのデータ部分に設定した新たなフレームを生成する。中継装置１００は、当該フレームを管理サーバ２００に送信する。このフレームは認証依頼に相当する。認証依頼は、ユーザＩＤ、パスワード、ステップＳＴ１０１で受信したフレームの送信元ＩＰアドレスおよび送信元ＭＡＣアドレスを認証用の情報として含む。管理サーバ２００は認証依頼を受信する。

[0143] （ステップＳＴ１０３）管理サーバ２００は、認証依頼に含まれるユーザＩＤおよびパスワードを、ユーザ管理テーブル２１１の登録内容と照合する。ユーザ管理テーブル２１１には、ユーザＩＤ“ＵＩＤ０００１”とパスワード“ｐａｓｓ１”との組が登録されている。このため本照合は成功する。また、ユーザＩＤ“ＵＩＤ０００１”、送信元ＩＰアドレス“５０．２２３．３．４”に対して、アクセス管理テーブル２１２にはユーザＩＤ“ＵＩＤ０００１”、端末ＩＰアドレス“－”、ＭＡＣアドレス“－”の“ＲＯＬＥ３”が存在する。管理サーバ２００は適用ＲＯＬＥとして“ＲＯＬＥ３”を特定する。また、ユーザ管理テーブル２１１によれば、ユーザＡには多重接続の制約はない（多重接続設定が“可”であるため）。よって、管理サーバ２００は“ＲＯＬＥ３”を用いて送信元ＩＰアドレス“５０．２２３．３．

４”を含むセッション情報を生成し、認証成功の通知とともに、中継装置１００に送信する。中継装置１００はセッション情報と認証成功の通知とを受信する。また、管理サーバ２００は接続管理テーブル２１３の更新も行う。具体的には、ユーザＩＤ“ＵＩＤ０００１”、端末ＩＰアドレス“５０．２２３．３．４”、中継装置ＩＰアドレス“１９２．１６８．１０．１”、適用ＲＯＬＥ“ＲＯＬＥ３”のレコードを接続管理テーブル２１３に追加する。

[0144] （ステップＳＴ１０４）中継装置１００は、受信したセッション情報をセッション管理テーブル１１１に登録する。この場合、ＲＯＬＥ“３”、端末ＩＰアドレス“５０．２２３．３．４”、ＡＣＬ“１９２．１６８．１０．１０１”のレコードがセッション管理テーブル１１１に登録されることになる。中継装置１００は、認証成功の通知をクライアント５００に送信する。クライアント５００は認証成功の通知を受信する。

[0145] （ステップＳＴ１０５）クライアント５００は、業務サーバ３００へ宛てたリクエストを送信する。例えば、リクエストの宛先ＩＰアドレスは “１９２．１６８．１０．１０１”である。また、送信元ＩＰアドレスは“５０．２２３．３．４”である。中継装置１００は当該リクエストを受信する。

[0146] （ステップＳＴ１０６）中継装置１００は、受信したリクエストのＩＰパケットに含まれる送信元／宛先ＩＰアドレスの組を、セッション管理テーブル１１１の登録内容と照合する。セッション管理テーブル１１１には、ステップＳＴ１０４で登録された“ＲＯＬＥ３”のレコードが存在する。すなわち、当該リクエストの中継は許容されている。よって、中継装置１００は業務サーバ３００に対して当該リクエストを転送する。業務サーバ３００は当該リクエストを受信する。

[0147] （ステップＳＴ１０７）業務サーバ３００は、受信したリクエストに応じた処理を実行する。業務サーバ３００は、処理結果に応じたレスポンスをクライアント５００に送信する。当該レスポンスは、中継装置１００を介してクライアント５００に送信される。前述のように中継装置１００は、業務サ

ーバ３００からクライアント５００への通信についても、セッション管理テーブル１１１に基づいて中継が許容されていると判断する。よって、中継装置１００は当該レスポンスを中継する。クライアント５００は当該レスポンスを受信する。

[0148] （ステップＳＴ１０８）クライアント５００は、業務サーバ３００ａへ宛てたリクエストを送信する。当該リクエストはファイアウォール１１を介して中継装置１００へ転送される。当該リクエストのＩＰパケットに含まれる宛先ＩＰアドレスは“１９２．１６８．１０．１０２”である。送信元ＩＰアドレスは“５０．２２３．３．４”である。中継装置１００は当該リクエストを受信する。

[0149] （ステップＳＴ１０９）中継装置１００は、受信したリクエストのＩＰパケットに含まれる送信元／宛先ＩＰアドレスの組を、セッション管理テーブル１１１の登録内容と照合する。この時点でセッション管理テーブル１１１には、送信元ＩＰアドレス“５０．２２３．３．４”を含むレコードは存在する。しかし、対応するＡＣＬには宛先ＩＰアドレス“１９２．１６８．１０．１０２”は含まれていない。すなわち、当該リクエストの中継は許容されていない。よって、中継装置１００は当該リクエストの中継を行わずに、当該リクエストを破棄する。

[0150] このように、クライアント５００はネットワークログイン認証を経て、“ＲＯＬＥ３”のＡＣＬに登録された業務サーバ３００にアクセス可能となる。一方、“ＲＯＬＥ３”のＡＣＬで他の業務サーバについてはアクセスが許されていない。このため、中継装置１００により他の業務サーバに対するアクセスは制限される。

[0151] 次に、ネットワークログイン認証を経ずに、クライアント５００から業務サーバ３００へのアクセスを受け付けた場合の通信を例示する。

図１５は、第２の実施の形態の通信の具体例（その２）を示す図である。以下、図１５に示す処理をステップ番号に沿って説明する。ステップＳＴ１１１の直前では、セッション管理テーブル１１１および接続管理テーブル２

１３のエントリはないものとする。

[0152] （ステップＳＴ１１１）クライアント５００は、業務サーバ３００へ宛てたリクエストを送信する。当該リクエストはファイアウォール１１を介して中継装置１００へ転送される。中継装置１００はリクエストを受信する。中継装置１００により受信されるリクエストのＩＰパケットに含まれる宛先ＩＰアドレスは“１９２．１６８．１０．１０１”である。送信元ＩＰアドレスは“５０．２２３．３．４”である。

[0153] （ステップＳＴ１１２）中継装置１００は、受信したリクエストのＩＰパケットに含まれる送信元／宛先ＩＰアドレスの組を、セッション管理テーブル１１１の登録内容と照合する。セッション管理テーブル１１１には、この時点でエントリはない。すなわち、送信元ＩＰアドレス“５０．２２３．３．４”を含むレコードは存在しない。よって、中継装置１００は、認証の確認要求を管理サーバ２００に送信する。当該確認要求（ＩＰパケットのデータ部分）には送信元ＩＰアドレス“５０．２２３．３．４”が含まれる。管理サーバ２００は確認要求を受信する。

[0154] （ステップＳＴ１１３）管理サーバ２００は、確認要求に含まれる送信元ＩＰアドレスを、接続管理テーブル２１３の登録内容と照合する。接続管理テーブル２１３には、この時点でエントリはない。すなわち、送信元ＩＰアドレス“５０．２２３．３．４”を含むレコードは存在しない。よって、管理サーバ２００は、未認証である旨を中継装置１００に応答する。中継装置１００は当該応答を受信する。

[0155] （ステップＳＴ１１４）中継装置１００は、受信したリクエストをログインページへリダイレクトさせる。中継装置１００がログインページを提供可能な場合には、例えば、当該ログインページのデータをクライアント５００に提供する。クライアント５００はログインページのデータを受信する。他のＷｅｂサーバが提供するログインページにリダイレクトさせてもよい。すると、クライアント５００のＷｅｂブラウザはログインページをユーザＡに提示する。

[0156] （ステップＳＴ１１５）クライアント５００は、ログインページでユーザＡにより入力されたログイン認証用の情報を中継装置１００に送信する。当該認証用の情報には、ユーザＩＤ“ＵＩＤ０００１”およびパスワード“ｐａｓｓ１”が含まれる。中継装置１００は認証用の情報（フレーム）を受信する。

[0157] （ステップＳＴ１１６）中継装置１００は、受信したフレームから送信元ＩＰアドレス“５０．２２３．３．４”および送信元ＭＡＣアドレスを抽出する。中継装置１００は、抽出した送信元ＩＰアドレスおよび送信元ＭＡＣアドレスをＩＰパケットのデータ部分に設定した新たなフレーム（認証依頼）を生成し、管理サーバ２００に送信する。管理サーバ２００は認証依頼を受信する。認証依頼にはユーザＩＤおよびパスワードも含まれる。

[0158] （ステップＳＴ１１７）管理サーバ２００は、図１４のステップＳＴ１０３と同様にして、セッション情報を生成する。また、接続管理テーブル２１３に新たなレコードを追加する。管理サーバ２００は、生成したセッション情報と認証成功の通知とを中継装置１００に送信する。中継装置１００はセッション情報と認証成功の通知とを受信する。

[0159] （ステップＳＴ１１８）中継装置１００は、図１４のステップＳＴ１０４と同様に、管理サーバ２００から受信したセッション情報をセッション管理テーブル１１１に登録する。中継装置１００は、認証成功の通知をクライアント５００に送信する。クライアント５００は認証成功の通知を受信する。

[0160] 以後、図１４のステップＳＴ１０５以降と同様の手順により、クライアント５００から業務サーバ３００へのアクセスが可能となる。次に、ユーザＡがクライアント５００，６００の両方を用いてネットワークログイン認証を行う場合を例示する。

[0161] 図１６は、第２の実施の形態の通信の具体例（その３）を示す図である。以下、図１６に示す処理をステップ番号に沿って説明する。ステップＳＴ１２１の直前では、セッション管理テーブル１１１，１１１ａおよび接続管理テーブル２１３のエントリはないものとする。

[0162] （ステップＳＴ１２１）クライアント５００は、ログインページでユーザＡにより入力されたログイン認証用の情報を中継装置１００に送信する。当該認証用の情報には、ユーザＩＤ“ＵＩＤ０００１”およびパスワード“ｐａｓｓ１”が含まれる。中継装置１００は認証用の情報（フレーム）を受信する。

[0163] （ステップＳＴ１２２）中継装置１００は、受信したフレームから送信元ＩＰアドレス“５０．２２３．３．４”および送信元ＭＡＣアドレスを抽出する。中継装置１００は、抽出した送信元ＩＰアドレスおよび送信元ＭＡＣアドレスをＩＰパケットのデータ部分に設定した新たなフレーム（認証依頼）を生成し、管理サーバ２００に送信する。管理サーバ２００は認証依頼を受信する。認証依頼にはユーザＩＤおよびパスワードも含まれる。

[0164] （ステップＳＴ１２３）管理サーバ２００は、図１４のステップＳＴ１０３と同様にして、セッション情報を生成する。また、接続管理テーブル２１３にレコードを追加する。具体的には、ユーザＩＤ“ＵＩＤ０００１”、端末ＩＰアドレス“５０．２２３．３．４”、中継装置ＩＰアドレス“１９２．１６８．１０．１”、適用ＲＯＬＥ“ＲＯＬＥ３”のレコードである。管理サーバ２００は、生成したセッション情報と認証成功の通知とを中継装置１００に送信する。中継装置１００はセッション情報と認証成功の通知とを受信する。

[0165] （ステップＳＴ１２４）中継装置１００は、図１４のステップＳＴ１０４と同様に、管理サーバ２００から受信したセッション情報（“ＲＯＬＥ３”のレコード）をセッション管理テーブル１１１に登録する。中継装置１００は、認証成功の通知をクライアント５００に送信する。クライアント５００は認証成功の通知を受信する。

[0166] （ステップＳＴ１２５）クライアント６００は、ログインページでユーザＡにより入力されたログイン認証用の情報を中継装置１００ａに送信する。当該認証用の情報には、ユーザＩＤ“ＵＩＤ０００１”およびパスワード“ｐａｓｓ１”が含まれる。中継装置１００ａは認証用の情報（フレーム）を

受信する。

[0167] （ステップＳＴ１２６）中継装置１００ａは、受信したフレームから送信元ＩＰアドレス“１９２．１６８．１０．１１”および送信元ＭＡＣアドレス“０８－ｂ４－２５－９ｅ－０ｃ－４６”を抽出する。中継装置１００ａは、抽出した送信元ＩＰアドレスおよび送信元ＭＡＣアドレスをＩＰパケットのデータ部分に設定した新たなフレーム（認証依頼）を生成し、管理サーバ２００に送信する。管理サーバ２００は認証依頼を受信する。認証依頼にはユーザＩＤおよびパスワードも含まれる。

[0168] （ステップＳＴ１２７）管理サーバ２００は、認証依頼に含まれるユーザＩＤおよびパスワードを、ユーザ管理テーブル２１１の登録内容と照合する。ユーザ管理テーブル２１１には、ユーザＩＤ“ＵＩＤ０００１”とパスワード“ｐａｓｓ１”との組が登録されている。このため、本照合は成功する。また、ユーザＩＤ“ＵＩＤ０００１”、送信元ＩＰアドレス“１９２．１６８．１０．１１”、送信元ＭＡＣアドレス“０８－ｂ４－２５－９ｅ－０ｃ－４６”を含むレコードとして、アクセス管理テーブル２１２には“ＲＯＬＥ１”が存在する。管理サーバ２００は適用ＲＯＬＥとして“ＲＯＬＥ１”を特定する。更に、接続管理テーブル２１３にはステップＳＴ１２３で“ＲＯＬＥ３”のレコードが既に追加されている。これに対し、ユーザ管理テーブル２１１によればユーザＩＤ“ＵＩＤ０００１”は多重接続設定が“可”である。よって、管理サーバ２００は“ＲＯＬＥ１”での新たな接続が許容されている（すなわち、多重接続の制約がない）と判断する。

[0169] （ステップＳＴ１２８）管理サーバ２００は、アクセス管理テーブル２１２の“ＲＯＬＥ１”を用いてセッション情報を生成し、認証成功の通知とともに、中継装置１００ａに送信する。中継装置１００ａはセッション情報と認証成功の通知とを受信する。管理サーバ２００は接続管理テーブル２１３の更新も行う。具体的には、ユーザＩＤ“ＵＩＤ０００１”、端末ＩＰアドレス“１９２．１６８．１０．１１”、中継装置ＩＰアドレス“１９２．１６８．１０．２”、適用ＲＯＬＥ“ＲＯＬＥ１”のレコードを接続管理テー

ブル２１３に追加する。

[0170] （ステップＳＴ１２９）中継装置１００ａは、管理サーバ２００から受信したセッション情報をセッション管理テーブル１１１ａに登録する（“ＲＯＬＥ１”のレコード）。中継装置１００ａは、認証成功の通知をクライアント６００に送信する。クライアント６００は認証成功の通知を受信する。

[0171] このようにして、ユーザ管理テーブル２１１の設定により、多重接続を許容するか否かを制御できる。ユーザ管理テーブル２１１において、ユーザＡ（“ＵＩＤ０００１”）は多重接続設定が“可”である。このため、ユーザＡはクラアント５００，６００の両方を用いて業務サーバにアクセス可能となる。これに対し、ユーザＢ（“ＵＩＤ０００２”）は多重接続設定が“不可”である。このため、ユーザＢに対しては複数のクライアントを用いたアクセスは許容されていないことになる。

[0172] また、このように多重接続した場合にも、クライアント５００，６００からアクセス可能な業務サーバの範囲は、クライアント５００，６００の通信を中継する中継装置１００，１００ａそれぞれにより制限されることになる。アクセス可能な業務サーバの範囲は、クライアント５００，６００で相違し得る。このように、１ユーザが複数のクライアントを利用する場合にもクライアント単位のアクセス制御を行える。

[0173] 次に、クライアント６００から中継装置１００ａ，１００ｂを介したアクセスを行う場合を例示する。

図１７は、第２の実施の形態の通信の具体例（その４）を示す図である。以下、図１７に示す処理をステップ番号に沿って説明する。ステップＳＴ１３１の直前では、セッション管理テーブル１１１ａ，１１１ｂおよび接続管理テーブル２１３のエントリはないものとする。

[0174] （ステップＳＴ１３１）クライアント６００は、ログインページでユーザＡにより入力されたログイン認証用の情報を中継装置１００ａに送信する。当該認証用の情報には、ユーザＩＤ“ＵＩＤ０００１”およびパスワード“ｐａｓｓ１”が含まれる。中継装置１００ａは認証用の情報（フレーム）を

受信する。

[0175] （ステップＳＴ１３２）中継装置１００ａは、受信したフレームから送信元ＩＰアドレス“１９２．１６８．１０．１１”および送信元ＭＡＣアドレス“０８－ｂ４－２５－９ｅ－０ｃ－４６”を抽出する。中継装置１００ａは、抽出した送信元ＩＰアドレスおよび送信元ＭＡＣアドレスをＩＰパケットのデータ部分に設定した新たなフレーム（認証依頼）を生成し、管理サーバ２００に送信する。管理サーバ２００は認証依頼を受信する。認証依頼にはユーザＩＤおよびパスワードも含まれる。

[0176] （ステップＳＴ１３３）管理サーバ２００は、ユーザＩＤとパスワードの照合などを行い、また、アクセス管理テーブル２１２を参照して“ＲＯＬＥ１”のセッション情報を生成する。“ＲＯＬＥ１”が選択される理由は、ユーザＩＤ“ＵＩＤ０００１”、端末ＩＰアドレス“１９２．１６８．１０．１１”および送信元ＭＡＣアドレス“０８－ｂ４－２５－９ｅ－０ｃ－４６”を含み、これらが認証依頼に含まれる情報に一致するからである。また、接続管理テーブル２１３にレコードを追加する。具体的には、“ＵＩＤ０００１”、端末ＩＰアドレス“１９２．１６８．１０．１１”、中継装置ＩＰアドレス“１９２．１６８．１０．２”、適用ＲＯＬＥ“ＲＯＬＥ１”のレコードである。管理サーバ２００は、生成したセッション情報と認証成功の通知とを中継装置１００ａに送信する。中継装置１００ａはセッション情報と認証成功の通知とを受信する。

[0177] （ステップＳＴ１３４）中継装置１００ａは、管理サーバ２００から受信したセッション情報をセッション管理テーブル１１１ａに登録する（“ＲＯＬＥ１”のレコード）。中継装置１００ａは、認証成功の通知をクライアント６００に送信する。クライアント６００は認証成功の通知を受信する。

[0178] （ステップＳＴ１３５）クライアント６００は、業務サーバ４００へ宛てたリクエストを送信する。当該リクエストは中継装置１００ａへ転送される。当該リクエストのＩＰパケットに含まれる宛先ＩＰアドレスは“１９２．１６８．２０．１０１”である。送信元ＩＰアドレスは“１９２．１６８．

１０．１１”である。中継装置１００ａは当該リクエストを受信する。

[0179] （ステップＳＴ１３６）中継装置１００ａは、受信したリクエストのＩＰパケットに含まれる送信元／宛先ＩＰアドレスの組を、セッション管理テーブル１１１ａの登録内容と照合する。セッション管理テーブル１１１ａには、ステップＳＴ１３４で登録された“ＲＯＬＥ１”のレコードが存在する。“ＲＯＬＥ１”では、端末ＩＰアドレス“１９２．１６８．１０．１１”に対し、ＡＣＬに“１９２．１６８．２０．１０１”がある。すなわち、当該リクエストの中継は許容されている。よって、中継装置１００ａは業務サーバ４００に対して当該リクエストを転送する。業務サーバ４００への通信経路には、中継装置１００ｂが存在している。中継装置１００ｂは当該リクエストを受信する。

[0180] （ステップＳＴ１３７）中継装置１００ｂは、受信したリクエストのＩＰパケットに含まれる送信元／宛先ＩＰアドレスの組を、セッション管理テーブル１１１ｂの登録内容と照合する。セッション管理テーブル１１１ｂには、この時点でエントリはない。すなわち、送信元ＩＰアドレス“１９２．１６８．１０．１１”を含むレコードは存在しない。よって、中継装置１００ｂは、認証の確認要求を管理サーバ２００に送信する。当該確認要求（ＩＰパケットのデータ部分）にはクライアント６００のＩＰアドレス“１９２．１６８．１０．１１”が含まれる。管理サーバ２００は確認要求を受信する。なお、中継装置１００ｂは、ステップＳＴ１３６で受信したリクエストを保留する（例えば、ＲＡＭに格納する）。

[0181] （ステップＳＴ１３８）管理サーバ２００は、確認要求に含まれる送信元ＩＰアドレスを、接続管理テーブル２１３の登録内容と照合する。接続管理テーブル２１３には、ステップＳＴ１３３で登録されたレコードが存在する。このレコードの端末ＩＰアドレスは“１９２．１６８．１０．１１”である。これは確認対象のクライアント６００のＩＰアドレスと一致するので、管理サーバ２００は認証済であると判断する。管理サーバ２００は、当該レコードから適用ＲＯＬＥ“ＲＯＬＥ１”を特定する。管理サーバ２００は、

アクセス管理テーブル２１２の“ＲＯＬＥ１”を参照して、セッション情報を生成する。管理サーバ２００は、生成したセッション情報と認証済の通知とを中継装置１００ｂに送信する。中継装置１００ｂはセッション情報と認証済の通知とを受信する。管理サーバ２００は、接続管理テーブル２１３にレコードを追加する。具体的には、ユーザＩＤ“ＵＩＤ０００１”、端末ＩＰアドレス“１９２．１６８．１０．１１”、中継装置ＩＰアドレス“１９２．１６８．２０．１”、適用ＲＯＬＥ“ＲＯＬＥ１”のレコードである。

[0182] （ステップＳＴ１３９）中継装置１００ｂは、管理サーバ２００から受信したセッション情報をセッション管理テーブル１１１ｂに登録する（“ＲＯＬＥ１”のレコード）。中継装置１００ｂは、ステップＳＴ１３７で中継を保留したリクエストのＩＰパケットに含まれる送信元／宛先ＩＰアドレスの組を、セッション管理テーブル１１１ｂの登録内容と照合する。この時点でセッション管理テーブル１１１ｂには“ＲＯＬＥ１”のレコードが存在する。“ＲＯＬＥ１”では、端末ＩＰアドレス“１９２．１６８．１０．１１”に対し、ＡＣＬに“１９２．１６８．２０．１０１”が含まれる。すなわち、当該リクエストの中継は許容されている。よって、中継装置１００ｂは業務サーバ４００に対して当該リクエストを転送する。業務サーバ４００は当該リクエストを受信する。

[0183] （ステップＳＴ１４０）業務サーバ４００は、受信したリクエストに応じた処理を実行する。業務サーバ４００は、処理結果に応じたレスポンスをクライアント６００に送信する。当該レスポンスは中継装置１００ｂ，１００ａの順に経由してクライアント６００に転送される。クライアント６００は当該レスポンスを受信する。

[0184] このようにして、クライアント６００は、中継装置１００ａ，１００ｂを介して業務サーバ４００にアクセスできる。すなわち、１つのクライアントから複数の中継装置を介して業務サーバにアクセスする場合にも、最初の中継装置に適用されたＲＯＬＥを用いて、適正にアクセス制御を行える。このとき、中継装置１００ｂはユーザＡに対してログイン認証用の情報を再度入

力させずに済むので、ユーザＡによる重複した情報を入力する手間を省ける。また、認証処理を重複して行わずに済む。

[0185] これまでの説明では、中継装置１００，１００ａ，１００ｂと管理サーバ２００との間の認証の流れを例示した。これに対し、管理サーバ２００は、業務サーバ３００，３００ａ，４００，４００ａに認証結果を提供してもよい。例えば、業務サーバ３００，３００ａ，４００，４００ａで動作する業務アプリケーションが個別にユーザ認証を行うことがある。この場合に、管理サーバ２００の認証結果を流用することが考えられる。そうすれば、各業務アプリケーションに対する一括認証が可能である。このような一括認証はシングルサインオンと呼ばれることがある。

[0186] 以下では、そのための管理サーバ２００の処理手順を説明する。なお、管理サーバ２００と業務サーバ３００との間の処理を説明するが、業務サーバ３００ａ，４００，４００ａについても同様の処理手順である。

[0187] 図１８は、第２の実施の形態の認証確認例（その２）を示すフローチャートである。以下、図１８に示す処理をステップ番号に沿って説明する。

（ステップＳ５１）管理部２２０は、業務サーバ３００から認証の確認要求を受信する。確認要求には確認対象のＩＰアドレスが含まれる。ここで、確認対象のＩＰアドレスとは、業務サーバ３００へアクセスしてきたクライアントのＩＰアドレスである。例えば、クライアント５００であれば、当該ＩＰアドレスは“５０．２２３．３．４”である。例えば、業務サーバ３００では認証確認用のエージェントが実行される。例えば、当該エージェントは、クライアントからのリクエストを受信すると、管理サーバ２００に認証の確認要求を送信する。

[0188] （ステップＳ５２）管理部２２０は、記憶部２１０に記憶された接続管理テーブル２１３を参照して、クライアントのＩＰアドレスが登録済であるか否かを判定する。登録済である場合、処理をステップＳ５３に進める。登録済でない場合、処理をステップＳ５４に進める。例えば、接続管理テーブル２１３の端末ＩＰアドレスの項目に当該ＩＰアドレスが設定されたレコード

が存在する場合、当該ＩＰアドレスは登録済である。一方、接続管理テーブル２１３の端末ＩＰアドレスの項目に当該ＩＰアドレスが設定されたレコードが存在しない場合、当該ＩＰアドレスは登録済でない。

[0189] （ステップＳ５３）管理部２２０は、接続管理テーブル２１３から該当レコードに含まれるユーザＩＤを抽出する。管理部２２０は、確認要求に対して、認証済である旨を業務サーバ３００に応答する。当該応答には、抽出したユーザＩＤが含まれる。そして、処理を終了する。

[0190] （ステップＳ５４）管理部２２０は、確認要求に対して未認証である旨を業務サーバ３００に応答する。そして、処理を終了する。

このように、認証済の場合、業務サーバ３００は管理サーバ２００からユーザＩＤの提供を受ける。そして、業務サーバ３００はクライアントへのサービス提供を開始する。管理サーバ２００が業務サーバ３００にユーザＩＤを提供する理由は、業務サーバが提供するサービスがユーザごとに管理されている場合があり得るからである。例えば、ユーザごとにカスタマイズされたＧＵＩを提供する、業務サーバ単位でユーザごとに利用可能な機能を制限する、などが考えられる。次に、このようなシングルサインオンの通信の具体例を説明する。

[0191] 図１９は、第２の実施の形態の通信の具体例（その５）を示す図である。以下、図１９に示す処理をステップ番号に沿って説明する。ステップＳＴ１４１の直前では、セッション管理テーブル１１１ａには“ＲＯＬＥ１”のレコードが存在するものとする。接続管理テーブル２１３にはユーザＩＤ“ＵＩＤ０００１”、端末ＩＰアドレス“１９２．１６８．１０．１１”、中継装置ＩＰアドレス“１９２．１６８．１０．２”、適用ＲＯＬＥ“ＲＯＬＥ１”のレコードが存在するものとする。

[0192] （ステップＳＴ１４１）クライアント６００は、業務サーバ３００へ宛てたリクエストを送信する。当該リクエストは中継装置１００ａへ転送される。当該リクエストのＩＰパケットに含まれる宛先ＩＰアドレスは“１９２．１６８．１０．１０１”である。送信元ＩＰアドレスは“１９２．１６８．

１０．１１”である。中継装置１００ａは当該リクエストを受信する。

[0193] （ステップＳＴ１４２）中継装置１００ａは、受信したリクエストのＩＰパケットに含まれる送信元／宛先ＩＰアドレスの組をセッション管理テーブル１１１ａの登録内容と照合する。セッション管理テーブル１１１ａには“ＲＯＬＥ１”のレコードが存在する。すなわち、当該リクエストの中継は許容されている。よって、中継装置１００ａは業務サーバ３００に対して当該リクエストを転送する。業務サーバ３００は当該リクエストを受信する。例えば、このリクエストは業務サーバ３００がクライアント６００からアクセスの初回に受け付けるリクエストであるものとする。

[0194] （ステップＳＴ１４３）業務サーバ３００は、当該リクエストのＩＰパケットに含まれる送信元ＩＰアドレスを抽出する。送信元ＩＰアドレスは“１９２．１６８．１０．１１”である。業務サーバ３００は、認証の確認要求を管理サーバ２００に送信する。当該確認要求のＩＰパケットのデータ部分には、抽出された送信元ＩＰアドレス（クライアント６００のＩＰアドレス）が含まれる。管理サーバ２００は当該確認要求を受信する。

[0195] （ステップＳＴ１４４）管理サーバ２００は、確認要求に含まれるクライアント６００のＩＰアドレスを、接続管理テーブル２１３の登録内容と照合する。接続管理テーブル２１３には、端末ＩＰアドレスが“１９２．１６８．１０．１１”を含むレコードが存在する。よって、管理サーバ２００は認証済であると判断し、当該レコードに登録されたユーザＩＤ“ＵＩＤ０００１”を取得する。管理サーバ２００はユーザＩＤとともに認証済である旨を業務サーバ３００に応答する。業務サーバ３００は当該応答を受信する。

[0196] （ステップＳＴ１４５）業務サーバ３００は、当該応答により認証済であることを確認する。すると、業務サーバ３００は、ステップＳＴ１４２で受信したリクエストに応じた処理を実行する。その際、管理サーバ２００から提供されたユーザＩＤを用いる。例えば、ユーザごとに異なる業務メニューページを提供する。これにより、ユーザごとにカスタマイズされたサービスを提供できる。業務サーバ３００は、処理結果に応じたレスポンスをクライ

アント６００に送信する。当該レスポンスは中継装置１００ａを経由してクライアント６００に転送される。クライアント６００は当該レスポンスを受信する。

[0197] （ステップＳＴ１４６）クライアント６００は、業務サーバ３００ａへ宛てたリクエストを送信する。当該リクエストは中継装置１００ａへ転送される。当該リクエストのＩＰパケットに含まれる宛先ＩＰアドレスは“１９２．１６８．１０．１０２”である。送信元ＩＰアドレスは“１９２．１６８．１０．１１”である。中継装置１００ａは当該リクエストを受信する。

[0198] （ステップＳＴ１４７）中継装置１００ａは、受信したリクエストのＩＰパケットに含まれる送信元／宛先ＩＰアドレスの組をセッション管理テーブル１１１ａの登録内容と照合する。セッション管理テーブル１１１ａには“ＲＯＬＥ１”のレコードが存在する。すなわち、当該リクエストの中継は許容されている。よって、中継装置１００ａは業務サーバ３００ａに対して当該リクエストを転送する。業務サーバ３００ａは当該リクエストを受信する。例えば、このリクエストは業務サーバ３００ａがクライアント６００からアクセスの初回に受け付けたリクエストであるものとする。

[0199] （ステップＳＴ１４８）業務サーバ３００ａは、当該リクエストのＩＰパケットに含まれる送信元ＩＰアドレスを抽出する。送信元ＩＰアドレスは“１９２．１６８．１０．１１”である。業務サーバ３００ａは、認証の確認要求を管理サーバ２００に送信する。当該確認要求のＩＰパケットのデータ部分には、抽出された送信元ＩＰアドレスが含まれる。管理サーバ２００は当該確認要求を受信する。

[0200] （ステップＳＴ１４９）管理サーバ２００は、確認要求に含まれる送信元ＩＰアドレスを、接続管理テーブル２１３の登録内容と照合する。接続管理テーブル２１３には、端末ＩＰアドレスが“１９２．１６８．１０．１１”を含むレコードが存在する。よって、管理サーバ２００は認証済であると判断し、当該レコードに登録されたユーザＩＤ“ＵＩＤ０００１”を取得する。管理サーバ２００はユーザＩＤとともに認証済である旨を業務サーバ３０

０ａに応答する。業務サーバ３００ａは当該応答を受信する。

[0201] （ステップＳＴ１５０）業務サーバ３００ａは、当該応答により認証済であることを確認する。すると、業務サーバ３００ａは、ステップＳＴ１４７で受信したリクエストに応じた処理を実行する。その際、ステップＳＴ１４５と同様に、管理サーバ２００から提供されたユーザＩＤを用いる。業務サーバ３００ａは、処理結果に応じたレスポンスをクライアント６００に送信する。当該レスポンスは中継装置１００ａを経由してクライアント６００に転送される。クライアント６００は当該レスポンスを受信する。

[0202] このようにして、業務サーバ３００，３００ａに対するシングルサインオンを実行する。業務サーバ４００，４００ａについても同様である。管理サーバ２００が各業務サーバへユーザＩＤを提供すれば、各業務サーバは、サービス提供にあたり、クライアントに個別にユーザＩＤの提供を求めなくてもよい。ステップＳＴ１４４，ＳＴ１４９で認証済が確認された後は、業務サーバ３００，３００ａは管理サーバ２００に対する認証の確認を行わずにサービスの提供を継続することになる。

[0203] このようにして、シングルサインオンを実現すれば、ネットワークログイン認証により、各業務アプリケーションに対する認証も一括して行える。シングルサインオンを実現すれば、ユーザによる認証情報の重複入力の手間を省けるので、ユーザの利便性を一層向上し得る。

[0204] 次に、ネットワークログインに対するログアウトの手順を説明する。

図２０は、第２の実施の形態のログアウト処理の例を示すフローチャートである。以下、図２０に示す処理をステップ番号に沿って説明する。

[0205] （ステップＳ６１）アクセス制御部１２０は、クライアント５００からログアウト要求を受信する。

（ステップＳ６２）アクセス制御部１２０は、ログアウト要求のＩＰパケットに含まれる送信元ＩＰアドレスを抽出する。ここでは、抽出される送信元ＩＰアドレスは“５０．２２３．３．４”である。アクセス制御部１２０は、抽出したクライアント５００のＩＰアドレスをＩＰパケットのデータ部

分に含めたログアウト要求を生成し、管理サーバ２００に送信する。

[0206] （ステップＳ６３）管理部２２０は、中継装置１００が送信したログアウト要求を受信する。

（ステップＳ６４）管理部２２０は、記憶部２１０に記憶された接続管理テーブル２１３を参照し、ログアウト要求（ＩＰパケットのデータ部分）に含まれるクライアント５００のＩＰアドレスが、端末ＩＰアドレスの項目に設定されたレコードを検索する。管理サーバ２００は、検索されたレコードに含まれる中継装置ＩＰアドレスおよび適用ＲＯＬＥの設定を取得する。管理サーバ２００は、取得された中継装置ＩＰアドレスを宛先として、当該適用ＲＯＬＥに対応するセッション情報を削除するように指示する。例えば、クライアント５００からのログアウト要求では、“ＲＯＬＥ３”のレコードを削除するように中継装置１００に指示する。当該削除の指示は、複数の中継装置に対して行われることもある。また、管理サーバ２００は、接続管理テーブル２１３上から検索されたレコードを削除する。例えば、クライアント５００からのログアウト要求では端末ＩＰアドレス“５０．２２３．３．４”の全レコードが接続管理テーブル２１３から削除されることになる。

[0207] （ステップＳ６５）アクセス制御部１２０は、管理サーバ２００からの指示に基づいて、記憶部１１０に記憶されたセッション管理テーブル１１１のレコード（セッション情報）を削除する。例えば、アクセス制御部１２０は“ＲＯＬＥ３”のレコードをセッション管理テーブル１１１から削除する。

[0208] （ステップＳ６６）アクセス制御部１２０は、セッション情報の削除が完了した旨を管理サーバ２００に応答する。

（ステップＳ６７）管理部２２０は、ステップＳ６４で削除の指示を行った中継装置から削除完了の応答を受信する。複数の中継装置に対して削除の指示を行った場合には、管理部２２０は複数の中継装置から削除完了の応答を受信する。

[0209] （ステップＳ６８）管理部２２０は、指示を行った全ての中継装置から削除完了の応答を受信するとログアウト完了を中継装置１００に応答する。

（ステップＳ６９）アクセス制御部１２０は、管理サーバ２００から当該応答を受信すると、ログアウト完了をクライアントに応答する。

[0210] このようにして、中継装置１００および管理サーバ２００はログアウト処理を実行する。管理サーバ２００は、１つの中継装置からあるクライアントのログアウト要求を受信すると、当該クライアントに係るセッション情報を保持する全ての中継装置に対してセッション情報の削除を指示する。このため、各中継装置に余計なセッション情報が残留することを防げる。次にログアウト処理における通信の具体例を説明する。

[0211] 図２１は、第２の実施の形態の通信の具体例（その６）を示す図である。以下、図２１に示す処理をステップ番号に沿って説明する。ステップＳＴ１５１の直前では、セッション管理テーブル１１１ａ，１１１ｂには“ＲＯＬＥ１”のレコードが存在するものとする。接続管理テーブル２１３には、ユーザＩＤ“ＵＩＤ０００１”、端末ＩＰアドレス“１９２．１６８．１０．１１”、中継装置ＩＰアドレス“１９２．１６８．１０．２”、適用ＲＯＬＥ“ＲＯＬＥ１”のレコードが存在するものとする。また、接続管理テーブル２１３には、ユーザＩＤ“ＵＩＤ０００１”、端末ＩＰアドレス“１９２．１６８．１０．１１”、中継装置ＩＰアドレス“１９２．１６８．２０．１”、適用ＲＯＬＥ“ＲＯＬＥ１”のレコードが存在するものとする。

[0212] （ステップＳＴ１５１）クライアント６００は、中継装置１００ａ宛てにログアウト要求を送信する。中継装置１００ａはログアウト要求を受信する。中継装置１００ａが受信するログアウト要求には、ＩＰパケットの送信元ＩＰアドレスとしてクライアント６００のＩＰアドレス“１９２．１６８．１０．１１”が含まれる。

[0213] （ステップＳＴ１５２）中継装置１００ａは、当該送信元ＩＰアドレスを抽出する。中継装置１００ａは、抽出されたクライアント６００のＩＰアドレスをＩＰパケットのデータ部分に含めたログアウト要求を生成して管理サーバ２００に送信する。管理サーバ２００は当該ログアウト要求を受信する。

[0214] （ステップＳＴ１５３）管理サーバ２００は、接続管理テーブル２１３を参照して、当該ＩＰアドレスが端末ＩＰアドレスの項目に設定されたレコードを検索する。ここでは、端末ＩＰアドレスの項目の設定値が“１９２．１６８．１０．１１”である上記の２つのレコードが存在している。管理サーバ２００は、これらのレコードから２つの中継装置ＩＰアドレス“１９２．１６８．１０．２”、“１９２．１６８．２０．１”を取得する。また、当該２つのレコードによれば、これら２つの中継装置１００ａ，１００ｂに適用されたＲＯＬＥは“ＲＯＬＥ１”である。よって、管理サーバ２００は、中継装置１００ａに“ＲＯＬＥ１”のセッション情報の削除を指示する。

[0215] （ステップＳＴ１５４）管理サーバ２００は、中継装置１００ｂにも“ＲＯＬＥ１”のセッション情報の削除を指示する。ただし、ステップＳＴ１５４の指示はステップＳＴ１５３と同時に行われてもよい。

[0216] （ステップＳＴ１５５）管理サーバ２００は、ステップＳＴ１５３で検索された２つのレコードを接続管理テーブル２１３から削除する。

（ステップＳＴ１５６）中継装置１００ａは、管理サーバ２００からの削除指示に基づいて、セッション管理テーブル１１１ａから“ＲＯＬＥ１”のレコードを削除する。そして、中継装置１００ａは削除完了を管理サーバ２００に応答する。管理サーバ２００は当該応答を受信する。

[0217] （ステップＳＴ１５７）中継装置１００ｂは、管理サーバ２００からの削除指示に基づいて、セッション管理テーブル１１１ｂから“ＲＯＬＥ１”のレコードを削除する。そして、中継装置１００ｂは削除完了を管理サーバ２００に応答する。管理サーバ２００は当該応答を受信する。

[0218] （ステップＳＴ１５８）管理サーバ２００は、ステップＳＴ１５２のログアウト要求に対してログアウト完了を中継装置１００ａに応答する。中継装置１００ａは当該応答を受信する。

[0219] （ステップＳＴ１５９）中継装置１００ａは、ステップＳＴ１５１のログアウト要求に対してログアウト完了をクライアント６００に応答する。クライアント６００は当該応答を受信する。

[0220] このようにして、中継装置１００ａ，１００ｂおよび管理サーバ２００はログアウト処理を実行する。例えば、図１７で説明したように、クライアント６００から中継装置１００ａ，１００ｂの両方を経由した業務サーバへのアクセスも可能である。このような場合にも、クライアント６００からの１回のログアウト要求で、中継装置１００ａ，１００ｂの両方が保持するセッション情報を適正に消去できる。これによって、クライアント６００からの接続を閉塞させることができる。

[0221] なお、中継装置１００，１００ａ，１００ｂからセッション情報が削除されるタイミングは、クライアント５００などからログアウト要求を受信したタイミング以外のタイミングも考え得る。例えば、中継装置１００，１００ａ，１００ｂは、セッション情報についてタイムアウトを検出し、タイムアウトを検出した場合に、当該セッション情報を削除してもよい。具体的には、中継装置１００，１００ａ，１００ｂは、セッション情報ごとに前回クライアントからの接続を受け付けてからの時間を監視する。そして、現在までの未接続の時間が閾値以上となった場合に、当該セッション情報を削除する。

[0222] 中継装置１００，１００ａ，１００ｂは、タイムアウトでセッション情報を削除した場合にも、管理サーバ２００に削除した旨（削除したセッション情報のＲＯＬＥ番号を含む）を通知する。すると、管理サーバ２００は、接続管理テーブル２１３から、当該通知の送信元の中継装置のＩＰアドレスおよびＲＯＬＥ番号を含むレコードを削除する。このように、タイムアウトによりクライアントからの接続を閉塞させることも可能である。

[0223] 図２２は、第２の実施の形態のアクセス可能範囲の例（その１）を示す図である。図２２では、ユーザＡ，Ｂ，Ｃそれぞれがクライアント５００，５００ａ，６００ａを用いてアクセスできる業務サーバを例示している。図７～９で例示した各テーブル内容が中継装置１００，１００ａ，１００ｂおよび管理サーバ２００に保持されている場合である。

[0224] この場合、ユーザＡはクライアント５００を用いて業務サーバ３００にア

クセス可能である。クライアント５００のリクエストを中継する中継装置１００が“ＲＯＬＥ３”のセッション情報を保持するからである。

[0225] また、ユーザＢはクライアント５００ａを用いて業務サーバ３００，３００ａにアクセス可能である。クライアント５００ａのリクエストを中継する中継装置１００が“ＲＯＬＥ５”のセッション情報を保持するからである。

[0226] 更に、ユーザＣはクライアント６００ａを用いて業務サーバ４００，４００ａにアクセス可能である。クライアント６００ａのリクエストを中継する中継装置１００ａ，１００ｂが“ＲＯＬＥ６”のセッション情報を保持するからである。

[0227] 図２３は、第２の実施の形態のアクセス可能範囲の例（その２）を示す図である。図２２では、ユーザＡがクライアント５００，６００を用いてアクセスできる業務サーバを例示している。図７～９で例示した各テーブル内容が中継装置１００，１００ａ，１００ｂおよび管理サーバ２００に保持されている場合である。

[0228] この場合、ユーザＡはクライアント５００を用いて業務サーバ３００にアクセス可能である。クライアント５００のリクエストを中継する中継装置１００が“ＲＯＬＥ３”のセッション情報を保持するからである。

[0229] また、ユーザＡはクライアント６００を用いて業務サーバ３００，３００ａ，４００，４００ａにアクセス可能である。クライアント６００のリクエストを中継する中継装置１００ａ，１００ｂが“ＲＯＬＥ１”のセッション情報を保持するからである。

[0230] このようにして、中継装置１００，１００ａ，１００ｂおよび管理サーバ２００は、ユーザごとおよび、ユーザが利用するクライアントごとにアクセス可能な業務サーバの範囲を制限することができる。

[0231] ところで、業務サーバは仮想サーバを用いて実装されてもよい。

図２４は、第２の実施の形態の他の例（その１）を示す図である。例えば、ネットワーク２０に実行サーバ７００，７００ａを設ける。実行サーバ７００，７００ａは仮想マシンおよび仮想スイッチが動作可能なサーバコンピ

ュータである。実行サーバ７００，７００ａは、管理サーバ２００と同様のハードウェアを用いて実現できる。例えば、実行サーバ７００はハイパーバイザと呼ばれるソフトウェアを実行する。

[0232] ハイパーバイザは、実行サーバ７００上で仮想スイッチ７１０および仮想マシン７２０，７３０を動作させる。ハイパーバイザは、仮想スイッチ７１０および仮想マシン７２０，７３０に、実行サーバ７００が備えるＣＰＵなどの演算のリソースやＲＡＭなどの記憶領域のリソースの一部を割り当てる。実行サーバ７００ａも実行サーバ７００と同様に仮想スイッチおよび仮想マシンを動作させる。

[0233] 仮想スイッチ７１０は、仮想マシン７２０，７３０とネットワーク２０との間の通信を中継する。仮想マシン７２０，７３０は、業務サーバとして用いられる。ここで、仮想スイッチ７１０は、中継装置１００，１００ａ，１００ｂ（中継装置１００ｂは図２４では図示を省略）と同様に、セッション情報を記憶する記憶部やアクセス制御部を有してもよい。そして、仮想スイッチ７１０を用いて仮想マシン７２０，７３０に関するアクセス制御を行ってもよい。その場合、実行サーバ７００を中継装置と呼ぶこともできる。

[0234] 図２５は、第２の実施の形態の他の例（その２）を示す図である。図２で例示した第２の実施の形態の情報処理システムでは、中継装置１００，１００ａ，１００ｂを含む多数のネットワーク機器、および、物理マシンや仮想マシンが含まれ得る。そして、ユーザごとのアクセス制御の設定を変更する場合、例えば、情報処理システムの管理者が対象となる中継装置を探し出して、個別にＶＬＡＮなどを設定することも考えられる。しかし、多数のネットワーク機器の中から、対象の中継装置を探し出すことは容易でない。また、中継装置に対して個々に設定変更を行うための作業コストも問題となる。

[0235] 特に、大規模なネットワークでは、物理マシン、仮想マシンおよび中継装置の数も多い。また、物理マシンや仮想マシンの追加や物理マシン、仮想マシン、中継装置および仮想スイッチの接続変更も頻繁に起こり得る。このような場合、中継装置を管理者が個別に設定変更するための作業負担は特に大

きくなり得る。

[0236] これに対し、第２の実施の形態では、ユーザのアクセス制御の設定内容を管理サーバ２００により一元管理する。そして、各中継装置は、クライアントからのアクセスが発生した際に、当該ユーザに対するアクセス制御の設定内容を管理サーバ２００から取得する。各業務サーバのアクセス制御の設定変更を行いたい場合には、管理サーバ２００が保持するユーザ管理テーブル２１１やアクセス管理テーブル２１２を変更すればよい。

[0237] このため、管理者が設定対象の中継装置を探し出す手間を省け、また、中継装置に対して個々に設定変更を行うための作業コストも削減できる。このようにして、中継装置に対するユーザごとのアクセス制御の設定を容易に行うことができる。また、管理者の作業を省力化でき、アクセス制御の設定を効率的に行うことができる。また、新たにネットワークセグメントを設けたい場合にも、第２の実施の形態の中継装置を当該セグメントの入口に設ければ、当該セグメントに対するアクセス制御を容易に導入することができる。

[0238] また、アクセス制御の設定にＩＰアドレスを用いることで、例えばＶＬＡＮのように多数のスイッチに対してデータリンク層レベルでの細かな設定を行わずに済む。アクセスを許容したい両末端のノードをＩＰアドレスにより指定すればよいため、データリンク層レベルでの設定に比べて設定内容も平易である。このため、メンテナンスを行い易く、運用管理の効率化にも寄与し得る。

[0239] なお、管理サーバ２００はその負荷に応じて複数設けてもよい。例えば、ネットワーク２０，３０の両方に設けてもよい。その場合、各管理サーバでユーザ管理テーブル２１１、アクセス管理テーブル２１２および接続管理テーブル２１３の内容を同期してもよい。

[0240] また、上述したように中継装置１００，１００ａ，１００ｂはＬ３スイッチやルータでもよい。更に、中継装置１００，１００ａ，１００ｂは、業務サーバ３００，３００ａ，４００，４００ａに対するアクセス負荷を分散する負荷分散装置でもよい。あるいは、中継装置１００にファイアウォール１

１の機能を集約してもよい。その場合、中継装置１００をファイアウォールと呼ぶことができる。中継装置１００は、ファイアウォールやＶＰＮサーバの機能を組み込んだＵＴＭ装置などのアプライアンス装置でもよい。中継装置１００，１００ａ，１００ｂを管理サーバ２００と同様の構成を有するコンピュータによって実現することもできる。

[0241] 更に、図２の説明において、ＶＰＮサーバを設けてもよいことを説明した。中継装置１００がＶＰＮサーバ機能を備え、ユーザ認証の処理をＶＰＮにおける認証と連携してもよい。そうすれば、例えばユーザＡがＶＰＮへの認証に成功した時点で、ユーザＡが利用するクライアント５００に対するアクセス制御の設定を中継装置１００に行えることになる。よって、ユーザに対して重複した認証情報の入力を課さずに済み、アクセスの利便性を一層向上し得る。

[0242] ［第３の実施の形態］

以下、第３の実施の形態を説明する。前述の第２の実施の形態との相違点を主に説明し、共通の事項の説明を省略する。

[0243] 第２の実施の形態では、ユーザごと、またはユーザが利用するクライアント装置ごとのアクセス制御を行うことを例示した。これに加え、ユーザごとのアクセス制御を更に詳細に行うことも可能である。第３の実施の形態では、そのための方法を例示する。

[0244] ここで、第３の実施の形態の情報処理システムおよび各装置のハードウェア例／ソフトウェア例は、図２～５で説明した第２の実施の形態の情報処理システムおよび各装置のハードウェア例／ソフトウェア例と同様であるため説明を省略する。また、第３の実施の形態の各装置についても第２の実施の形態と同一の名称・符号を用いる。

[0245] 第３の実施の形態では、管理サーバ２００が保持するアクセス管理テーブルの内容が第２の実施の形態と異なる。また、中継装置１００，１００ａ，１００ｂそれぞれが保持するセッション管理テーブルの内容が第２の実施の形態と異なる。

[0246] 図２６は、第３の実施の形態のアクセス管理テーブルの例を示す図である。アクセス管理テーブル２１２ａは、記憶部２１０に格納される。アクセス管理テーブル２１２ａはＲＯＬＥ、ユーザＩＤ、端末ＩＰアドレス、端末ＭＡＣアドレス、接続許可時間帯、接続許可中継装置およびＡＣＬの項目を含む。ここで、ＲＯＬＥ、ユーザＩＤ、端末ＩＰアドレス、端末ＭＡＣアドレスおよびＡＣＬの項目に登録される情報は、アクセス管理テーブル２１２と同様であるため説明を省略する。

[0247] 接続許可時間帯の項目には、ＡＣＬへのアクセスを許容する時間帯が登録される。接続許可中継装置の項目には、アクセス元として許容される中継装置のＩＰアドレスが登録される。

[0248] 例えば、アクセス管理テーブル２１２ａには、ＲＯＬＥが“１１”、ユーザＩＤが“ＵＩＤ０００１”、端末ＩＰアドレスが“１９２．１６８．１０．１１”、端末ＭＡＣアドレスが“０８－ｂ４－２５－９ｅ－０ｃ－４６”、接続許可時間帯が“９：００－１７：００”、接続許可中継装置が“１９２．１６８．１０．２”、ＡＣＬが“１９２．１６８．１０．１０１，・・・”という情報が登録されている。

[0249] これは、ユーザＩＤ“０００１”のユーザＡが、ＩＰアドレス“１９２．１６８．１０．１１”、ＭＡＣアドレス“０８－ｂ４－２５－９ｅ－０ｃ－４６”であるクライアントから９時から１７時の間に、中継装置１００ａを介してアクセスする場合に、当該ＡＣＬのＩＰアドレスへのアクセスが許容されることを示す。

[0250] 一方、アクセス管理テーブル２１２ａには、“ＲＯＬＥ１２”のレコードが登録されている。“ＲＯＬＥ１２”は、“ＲＯＬＥ１１”と同じアドレス情報をもつクライアントが、１７時から９時の間にアクセスを行う場合のＲＯＬＥである。例えば、“ＲＯＬＥ１１”とは異なるＡＣＬを登録することで、時間帯によってアクセスを許容する業務サーバの範囲を変えることができる。

[0251] また、アクセス管理テーブル２１２ａの“ＲＯＬＥ１３”および“ＲＯＬ

Ｅ１４”も同様である。ただし、“ＲＯＬＥ１４”では、接続許可中継装置の設定も異なっている。具体的には“ＲＯＬＥ１３”では接続許可中継装置の項目の設定が中継装置１００ａ（ＩＰアドレス“１９２．１６８．１０．２”）であるのに対し、“ＲＯＬＥ１４”では同項目の設定が中継装置１００ｂ（ＩＰアドレス“１９２．１６８．２０．１”）である。すなわち、“ＲＯＬＥ１３”によれば、ユーザＩＤ“ＵＩＤ０００２”のユーザＢは、８時から１９時の間は中継装置１００ａを介したアクセスのみが許容されている。一方、“ＲＯＬＥ１４”によれば、ユーザＢは、１９時から０時の間は中継装置１００ｂを介したアクセスのみが許容されている。それ以外の時間帯では、ユーザＢによるアクセスは許容されていない。

[0252] なお、アクセス管理テーブル２１２ａでは、中継装置のＩＰアドレス以外を用いて、接続許可中継装置を登録してもよい。例えば、中継装置１００，１００ａ，１００ｂそれぞれに所定の識別名称を予め付与しておく。そして、接続許可中継装置の項目には、中継装置のＩＰアドレスに代えて、当該識別名称を設定してもよい。

[0253] 管理部２２０は、アクセス管理テーブル２１２ａに基づいてセッション情報を生成し、中継装置１００，１００ａ，１００ｂに提供する。次に、中継装置１００が保持するセッション管理テーブルの例を説明する。中継装置１００ａ，１００ｂが保持するセッション管理テーブルも同様のデータ構造である。

[0254] 図２７は、第３の実施の形態のセッション管理テーブルの例を示す図である。セッション管理テーブル１１１ｃは、記憶部１１０に格納される。セッション管理テーブル１１１ｃは、アクセス制御部１２０により更新される。セッション管理テーブル１１１ｃは、ＲＯＬＥ、端末ＩＰアドレス、接続許可時間帯およびＡＣＬの項目を含む。ここで、ＲＯＬＥ、端末ＩＰアドレスおよびＡＣＬの項目に登録される情報は、セッション管理テーブル１１１と同様であるため説明を省略する。接続許可時間帯の項目には、ＡＣＬへのアクセスを許容する時間帯が登録される。

[0255] 例えば、セッション管理テーブル１１１ｃには、ＲＯＬＥが“１１”、端末ＩＰアドレスが“１９２．１６８．１０．１１”、接続許可時間帯が“９：００－１７：００”、ＡＣＬが“１９２．１６８．１０．１０１，・・・”という情報が登録されている。これは、送信元／宛先ＩＰアドレスの組が“１９２．１６８．１０．１１”およびＡＣＬに含まれる何れかのＩＰアドレスである通信データの中継が、９時から１７時の間において許容されていることを示す。

[0256] 次に、第３の実施の形態の処理手順を説明する。ここで、第３の実施の形態の中継装置１００，１００ａ，１００ｂは、図１１～１３、図１８および図２０で説明した各手順を実行する。これらの各手順については説明を省略する。

[0257] ただし、管理部２２０は、図１１のステップＳ１４においてＡＣＬを検索する際に、現在の時刻および認証依頼の送信元の中継装置のＩＰアドレスをも考慮する。すなわち、ユーザＩＤ、端末ＩＰアドレス、端末ＭＡＣアドレス、接続許可時間帯および接続許可中継装置の条件が一致するＡＣＬをアクセス管理テーブル２１２ａから抽出することになる。条件に一致するＡＣＬが存在しない場合はステップＳ１５において認証失敗と判定する。

[0258] 第３の実施の形態では、第２の実施の形態の処理手順に加えて、中継装置１００，１００ａ，１００ｂは時間帯に応じたセッション管理テーブルの更新も行う。次に、当該セッション管理の処理手順を例示する。以下では、アクセス制御部１２０について説明するが、アクセス制御部１２０ａ，１２０ｂの処理も同様の手順である。

[0259] 図２８は、第３の実施の形態のセッション管理の例を示すフローチャートである。以下、図２８に示す処理をステップ番号に沿って説明する。

（ステップＳ７１）アクセス制御部１２０は、記憶部１１０に記憶されたセッション管理テーブル１１１ｃを監視する。

[0260] （ステップＳ７２）アクセス制御部１２０は、セッション管理テーブル１１１ｃに登録されたセッション情報のうち、接続許可時間帯を超過したセッ

ション情報があるか否かを判定する。接続許可時間帯を超過したセッション情報がある場合、処理をステップＳ７３に進める。接続許可時間帯を超過したセッション情報がない場合、処理をステップＳ７１に進める。例えば、アクセス制御部１２０は、中継装置１００が備えるＲＴＣ（Real Time Clock）の時刻と、セッション管理テーブル１１１ｃの各レコード（セッション情報）の接続許可時間帯とを対比することで、当該判定を行える。例えば、セッション管理テーブル１１１ｃの“ＲＯＬＥ１１”のセッション情報は接続許可時間帯が９時から１７時である。よって、アクセス制御部１２０は１７時を超えると、“ＲＯＬＥ１１”のセッション情報を削除する。

[0261] （ステップＳ７３）アクセス制御部１２０は、ステップＳ７２で接続許可時間帯を超過したと判断されたセッション情報をセッション管理テーブル１１１ｃから削除する。

（ステップＳ７４）アクセス制御部１２０は、セッション情報を削除した旨を管理サーバ２００に通知する。当該通知には、削除したセッション情報に含まれる端末ＩＰアドレスの情報が含まれる。

[0262] （ステップＳ７５）アクセス制御部１２０は、ステップＳ７４の通知に対して、削除したセッション情報と同一の端末ＩＰアドレスを含む次の時間帯のセッション情報を管理サーバ２００から受信したか否かを判定する。受信した場合、処理をステップＳ７６に進める。受信していない場合、処理をステップＳ７１に進める。例えば、セッション管理テーブル１１１ｃから“ＲＯＬＥ１１”のレコードを削除した場合、アクセス制御部１２０は、次の時間帯のセッション情報として“ＲＯＬＥ１２”に対応するセッション情報を管理サーバ２００から受信し得る。

[0263] （ステップＳ７６）アクセス制御部１２０は、受信した次の時間帯のセッション情報をセッション管理テーブル１１１ｃに登録する。そして、処理をステップＳ７１に進める。

このようにして、中継装置１００は、接続許可時間帯を超過したセッション情報を削除する。すると、ユーザが次に中継装置１００を介したアクセス

を試みるとき、当該ユーザに対して再度の認証が課されることになる。これにより、接続許可時間帯を超過したアクセスを制限することができる。

[0264] 更に、管理サーバ２００の管理部２２０は、削除の通知があったセッション情報と同一の端末ＩＰアドレス（任意の送信元ＩＰアドレスによってセッション情報が提供されていた場合は、任意のＩＰアドレス）を含む次の時間帯のレコードをアクセス管理テーブル２１２から検索する。次の時間帯のレコードとは削除の通知があったセッション情報に含まれる時間帯の次の時間帯を接続許可時間帯に含むレコードである。

[0265] 管理部２２０は、何れかのレコードが検索された場合は、当該レコードに基づいてセッション情報を生成し、中継装置１００に提供する。何れのレコードも検索されない場合は、管理部２２０は次の時間帯のセッション情報の送信を行わない。管理部２２０は、新たなセッション情報を中継装置１００に提供した場合、当該セッション情報の提供状況を接続管理テーブル２１３に登録する。

[0266] このようにして、中継装置１００のセッション情報が更新されれば、ＡＣＬも別時間帯のものに更新されることになり、アクセス可能な業務サーバの範囲が変更されることになる。また、次の時間帯のＡＣＬを適用する場合に、ユーザに対して再度の認証操作を課さずに済む。

[0267] なお、ステップＳ７４の通知を受けた管理サーバ２００は、接続管理テーブル２１３から該当の端末ＩＰアドレスを含むレコードを抽出する。管理サーバ２００は、当該端末ＩＰアドレスに対応する全ての中継装置ＩＰアドレスを取得する。そして、管理サーバ２００は、取得した中継装置ＩＰアドレスに対応する全ての中継装置に対して当該端末ＩＰアドレスを含むセッション情報の削除を指示する。これにより、ログアウトする場合と同様に、各中継装置に余計なセッション情報が残留することの防止を図れる。

[0268] 図２９は、第３の実施の形態のアクセス可能範囲の例（その１）を示す図である。図２９では、ユーザＡがクライアント６００を用いてアクセスできる業務サーバを例示している。図２６で示したアクセス管理テーブル２１２

ａの設定内容に基づくアクセス制御の例である。

[0269] この場合、ユーザＡは９時から１７時の間は業務サーバ３００，３００ａ，４００，４００ａにアクセス可能である。クライアント６００のリクエストを中継する中継装置１００ａ，１００ｂが“ＲＯＬＥ１１”のセッション情報を用いて中継の可否を判断するからである。

[0270] 一方、ユーザＡは１７時から９時の間は業務サーバ４００，４００ａにアクセス可能である。中継装置１００ａ，１００ｂが“ＲＯＬＥ１２”のセッション情報を用いて中継の可否を判断するからである。

[0271] このようにして、中継装置１００，１００ａ，１００ｂおよび管理サーバ２００は、ユーザごと、かつ、時間帯ごとに、アクセス可能な業務サーバの範囲を制限することができる。

[0272] 図３０は、第３の実施の形態のアクセス可能範囲の例（その２）を示す図である。図３０では、ユーザＢがクライアント６００ａを用いてアクセスできる業務サーバを例示している。図２６で示したアクセス管理テーブル２１２ａの設定内容に基づくアクセス制御の例である。

[0273] この場合、ユーザＢは８時から１９時の間は、中継装置１００ａを介して、業務サーバ３００，３００ａ，４００，４００ａにアクセス可能である。中継装置１００ａ，１００ｂが“ＲＯＬＥ１３”のセッション情報を用いて中継の可否を判断するからである。

[0274] 一方、ユーザＢは１９時から０時の間は、中継装置１００ｂを介して、業務サーバ４００，４００ａにアクセス可能である。中継装置１００ｂが“ＲＯＬＥ１４”のセッション情報を用いて中継の可否を判断するからである。

[0275] このように、ユーザごとに時間帯に応じたアクセス制御を行える。更に、クライアントごとに接続する中継装置を制限することができる。接続する中継装置の制限を時間帯に応じて変更することも可能である。これらのアクセス制御の内容は、管理サーバ２００により一元管理される。例えば、情報処理システムの管理者は、アクセス管理テーブル２１２ａの設定を変更すれば、当該変更内容を各中継装置に反映させたアクセス制御を行うことが可能で

ある。これにより、中継装置ごとのアクセス制御の設定を容易に行うことができる。

[0276] なお、前述のように、第１の実施の形態の情報処理は、中継装置１および情報処理装置２にプログラムを実行させることで実現できる。また、第２の実施の形態の情報処理は、中継装置１００，１００ａ，１００ｂおよび管理サーバ２００にプログラムを実行させることで実現できる。プログラムは、コンピュータ読み取り可能な記録媒体（例えば、光ディスク２３、メモリ装置２４およびメモリカード２６など）に記録できる。

[0277] プログラムを流通させる場合、例えば、当該プログラムを記録した可搬記録媒体が提供される。また、プログラムを他のコンピュータの記憶装置に格納しておき、ネットワーク経由でプログラムを配布することもできる。コンピュータは、例えば、可搬記録媒体に記録されたプログラムまたは他のコンピュータから受信したプログラムを、記憶装置に格納し、当該記憶装置からプログラムを読み込んで実行する。ただし、可搬記録媒体から読み込んだプログラムを直接実行してもよく、他のコンピュータからネットワークを介して受信したプログラムを直接実行してもよい。

[0278] また、上記の情報処理の少なくとも一部を、ＤＳＰ、ＡＳＩＣ、ＰＬＤなどの電子回路で実現することもできる。

更に、上記の説明ではＩＰｖ４（Internet Protocol version 4）を例示して説明したが、ＩＰｖ６（Internet Protocol version 6）を通信プロトコルとして用いた場合も同様である。具体的には、ＩＰｖ４を用いて例示したＩＰアドレスに代えて、ＩＰｖ６に対応したＩＰｖ６アドレスを用いることができる。

[0279] 上記については単に本発明の原理を示すものである。更に、多数の変形や変更が当業者にとって可能であり、本発明は上記に示し、説明した正確な構成および応用例に限定されるものではなく、対応する全ての変形例および均等物は、添付の請求項およびその均等物による本発明の範囲とみなされる。

符号の説明

[0280] １　中継装置

１ａ，２ａ　記憶手段

１ｂ　設定手段

１ｃ　制御手段

２　情報処理装置

２ｂ　提供手段

３，４，５，６　ノード

３ａ，３ｂ，３ｃ　データ

請求の範囲

[請求項1] ユーザを示す第１の識別情報および送信元のノードを示す第２の識別情報を受信すると、複数のユーザの識別情報それぞれに対応付けてアクセスが許容された宛先のノードを示す識別情報を記憶する情報処理装置から、前記第１の識別情報に対応する宛先のノードを示す第３の識別情報を取得し、データの中継が許容された組み合わせとして前記第２の識別情報と前記第３の識別情報とを記憶手段に設定する設定手段と、

送信元のノードの識別情報と宛先のノードの識別情報とを含むデータの中継を行う際に、前記記憶手段に設定された情報に基づいて、当該データを中継するか否かを判定する制御手段と、を有する中継装置。

[請求項2] 前記情報処理装置は、ユーザの識別情報および送信元のノードの識別情報に対応付けてアクセスが許容された宛先のノードを示す識別情報を記憶しており、

前記設定手段は、前記第１の識別情報および前記第２の識別情報に対応する宛先のノードを示す前記第３の識別情報を取得する、請求の範囲第１項記載の中継装置。

[請求項3] 前記情報処理装置は、ユーザの識別情報に対応付けて送信元のノードの識別情報によらずにアクセスが許容された宛先のノードを示す識別情報を記憶しており、

前記設定手段は、前記第１の識別情報および前記第２の識別情報に対応する宛先のノードを示す識別情報が前記情報処理装置に記憶されていない場合には、前記第１の識別情報に対して送信元のノードの識別情報によらずにアクセスが許容された宛先のノードを示す識別情報を前記第３の識別情報として取得する、請求の範囲第２項記載の中継装置。

[請求項4] 前記制御手段は、データの中継を行う際に、送信元および宛先のノ

ードの識別情報の組み合わせが前記記憶手段に設定された組み合わせに一致する場合にはデータを中継すると判定して当該データを宛先のノードに対して転送し、また、送信元および宛先のノードの識別情報の組み合わせが前記記憶手段に設定されていない場合には当該データを中継しないと判定して当該データを破棄する、請求の範囲第１項乃至第３項の何れか１項に記載の中継装置。

［請求項5］ 前記情報処理装置は、他の中継装置に設定されている送信元および宛先のノードの識別情報の組み合わせを記憶しており、

前記制御手段は、データの中継を行う際に、送信元のノードの識別情報を含む組み合わせが前記記憶手段に設定されていない場合、当該送信元のノードの識別情報を含む組み合わせが他の中継装置に設定されているか否かを前記情報処理装置に問い合わせ、当該組み合わせが他の中継装置に設定されている場合には前記情報処理装置から当該組み合わせを取得し、取得された当該組み合わせに基づいて当該データを中継するか否かを判定し、また、当該組み合わせが他の中継装置に設定されていない場合には当該データを中継しない、請求の範囲第１項乃至第４項の何れか１項に記載の中継装置。

［請求項6］ 前記設定手段は、前記第３の識別情報とともにアクセスが許容される時間帯を示す情報を前記情報処理装置から取得し、前記第２の識別情報および前記第３の識別情報に対応付けて前記記憶手段に設定し、

前記制御手段は、現時刻が前記時間帯を過ぎると、前記時間帯を示す情報に対応する前記第２の識別情報および前記第３の識別情報の組み合わせを前記記憶手段から削除する、請求の範囲第１項乃至第５項の何れか１項に記載の中継装置。

［請求項7］ 送信元および宛先のノードの識別情報はデータの転送に用いられるアドレス情報である、請求の範囲第１項乃至第６項の何れか１項に記載の中継装置。

［請求項8］ 送信元のノードにより送信されたデータを中継する中継装置と通信

可能な情報処理装置であって、

複数のユーザの識別情報それぞれに対応付けてアクセスが許容された宛先のノードを示す識別情報を記憶する記憶手段と、

ユーザを示す第１の識別情報および送信元のノードを示す第２の識別情報を中継装置から受信すると、前記記憶手段を参照して、前記第１の識別情報に対応する宛先のノードを示す第３の識別情報を検索し、前記第２の識別情報に対応してデータの中継が許容された宛先のノードの識別情報として前記第３の識別情報を当該中継装置に提供する提供手段と、を有する情報処理装置。

[請求項9] 前記記憶手段は、ユーザの識別情報に対応付けて複数の送信元のノードを用いた多重のアクセスを許容するか否かを示す許可情報を記憶しており、

前記提供手段は、前記第３の識別情報を中継装置に提供した後に、前記第１の識別情報および送信元のノードを示しており前記第２の識別情報とは異なる識別情報を中継装置から受信すると、前記許可情報に基づいて、前記第３の識別情報を当該中継装置に提供するか否かを判定する、請求の範囲第８項記載の情報処理装置。

[請求項10] 前記記憶手段は、ユーザの識別情報および送信元のノードの識別情報に対応付けてアクセスが許容された宛先のノードを示す識別情報を記憶しており、

前記提供手段は、前記第１の識別情報および前記第２の識別情報に対応する宛先のノードを示す前記第３の識別情報を検索する、請求の範囲第８項または第９項記載の情報処理装置。

[請求項11] 前記記憶手段は、ユーザの識別情報に対応付けて送信元のノードの識別情報によらずにアクセスが許容された宛先のノードを示す識別情報を記憶しており、

前記提供手段は、前記第１の識別情報および前記第２の識別情報に対応する宛先のノードを示す識別情報が前記記憶手段に記憶されてい

ない場合には、前記第１の識別情報に対して送信元のノードの識別情報によらずにアクセスが許容された宛先のノードを示す識別情報を検索し、前記第３の識別情報として中継装置に提供する、請求の範囲第１０項記載の情報処理装置。

［請求項12］ 前記提供手段は、送信元のノードの識別情報に対応付けて宛先のノードの識別情報を中継装置に提供したことの履歴を前記記憶手段に登録し、前記第２の識別情報が前記履歴に登録済か否かの問い合わせを他の中継装置から受信すると、前記履歴を参照して、前記第２の識別情報が登録済であれば前記第３の識別情報を当該他の中継装置に提供し、また、前記第２の識別情報が登録済でなければ未登録である旨を当該他の中継装置に応答する、請求の範囲第８項乃至第１１項の何れか１項に記載の情報処理装置。

［請求項13］ 前記提供手段は、宛先のノードの識別情報を提供した中継装置の識別情報も送信元のノードの識別情報に対応付けて前記履歴に登録し、前記第２の識別情報を含むログアウト要求を受信すると、前記履歴を参照して、前記第２の識別情報に対して前記第３の識別情報を提供した全ての中継装置に前記第２の識別情報と前記第３の識別情報との組み合わせについて中継を許容する旨の設定を削除させ、前記履歴の前記第２の識別情報の記録を削除する、請求の範囲第１２項記載の情報処理装置。

［請求項14］ 前記記憶手段は、ユーザの識別情報および時間帯を示す情報に対応付けてアクセスが許容される宛先のノードの識別情報を記憶しており、

前記提供手段は、前記記憶手段を参照して、前記第１の識別情報および現時刻の時間帯を示す情報に対応する宛先のノードを示す前記第３の識別情報を検索する、請求の範囲第８項乃至第１３項の何れか１項に記載の情報処理装置。

［請求項15］ 前記記憶手段は、ユーザの識別情報および中継装置の識別情報に対

応付けてアクセスが許容される宛先のノードの識別情報を記憶しており、

前記提供手段は、前記記憶手段を参照して、前記第１の識別情報および前記第２の識別情報を送信した中継装置の識別情報に対応する宛先のノードを示す前記第３の識別情報を検索する、請求の範囲第８項乃至第１４項の何れか１項に記載の情報処理装置。

［請求項16］ 前記提供手段は、ユーザの識別情報および送信元のノードの識別情報に対応付けて中継装置に情報を提供したことの履歴を前記記憶手段に登録し、宛先のノードに対して転送されたデータに含まれる送信元のノードの識別情報が前記履歴に登録済か否かの問い合わせを当該宛先のノードから受信すると、前記履歴を参照して、当該送信元のノードの識別情報が登録済であれば当該送信元のノードの識別情報に対応するユーザの識別情報を前記履歴から取得して当該宛先のノードに提供し、また、当該送信元のノードの識別情報が前記履歴に登録済でなければ未登録である旨を当該宛先のノードに応答する、請求の範囲第８項乃至第１５項の何れか１項に記載の情報処理装置。

［請求項17］ 送信元および宛先のノードの識別情報はデータの転送に用いられるアドレス情報である、請求の範囲第８項乃至第１６項の何れか１項に記載の情報処理装置。

［請求項18］ 送信元のノードにより送信されたデータを中継する中継装置および前記中継装置と通信可能な情報処理装置を含むシステムで実行されるアクセス制御方法であって、

ユーザを示す第１の識別情報および送信元のノードを示す第２の識別情報を前記中継装置を用いて受信すると、前記第１の識別情報および前記第２の識別情報を前記情報処理装置に送信し、

前記情報処理装置を用いて、複数のユーザの識別情報それぞれに対応付けてアクセスが許容された宛先のノードの識別情報を記憶する記憶手段を参照して、前記第１の識別情報に対応する宛先のノードを示

す第３の識別情報を検索し、前記第２の識別情報に対応してデータの中継が許容された宛先のノードの識別情報として前記第３の識別情報を前記中継装置に提供し、

送信元のノードの識別情報と宛先のノードの識別情報とを含むデータの中継を、前記中継装置を用いて行う際に、前記情報処理装置から提供された情報に基づいて、当該データを中継するか否かを判定する、アクセス制御方法。

[請求項19] 送信元のノードにより送信されたデータを中継するためのコンピュータに、

ユーザを示す第１の識別情報および送信元のノードを示す第２の識別情報を受信すると、複数のユーザの識別情報それぞれに対応付けてアクセスが許容された宛先のノードを示す識別情報を記憶する情報処理装置から、前記第１の識別情報に対応する宛先のノードを示す第３の識別情報を取得し、データの中継が許容された組み合わせとして前記第２の識別情報と前記第３の識別情報とを記憶手段に設定し、

送信元のノードの識別情報と宛先のノードの識別情報とを含むデータの中継を行う際に、前記記憶手段に設定された情報に基づいて、当該データを中継するか否かを判定する、処理を実行させるプログラム。

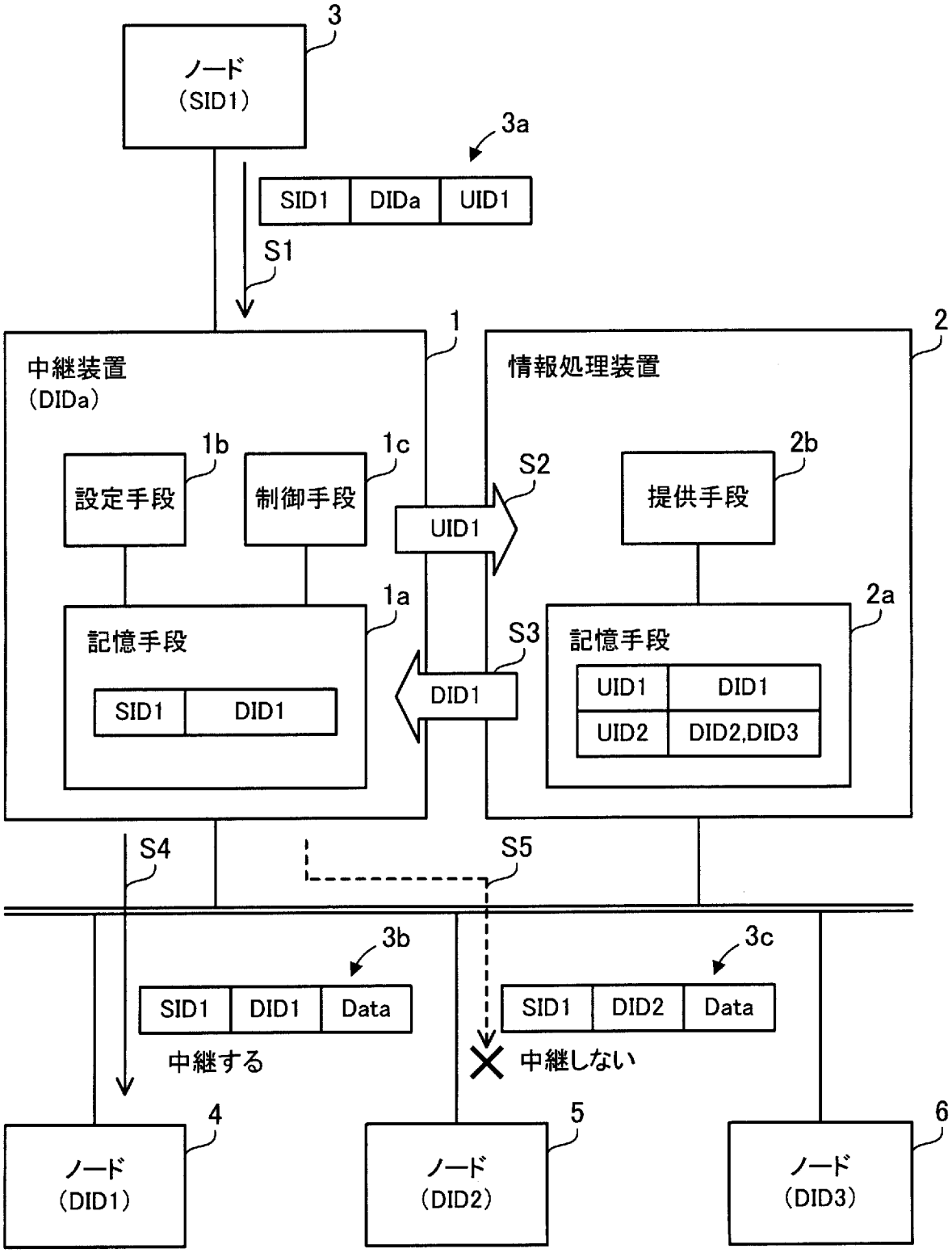
[請求項20] 送信元のノードにより送信されたデータを中継する中継装置と通信可能なコンピュータに、

ユーザを示す第１の識別情報および送信元のノードを示す第２の識別情報を前記中継装置から受信すると、複数のユーザの識別情報それぞれに対応付けてアクセスが許容された宛先のノードを示す識別情報を記憶する記憶手段を参照して、前記第１の識別情報に対応する宛先のノードを示す第３の識別情報を検索し、

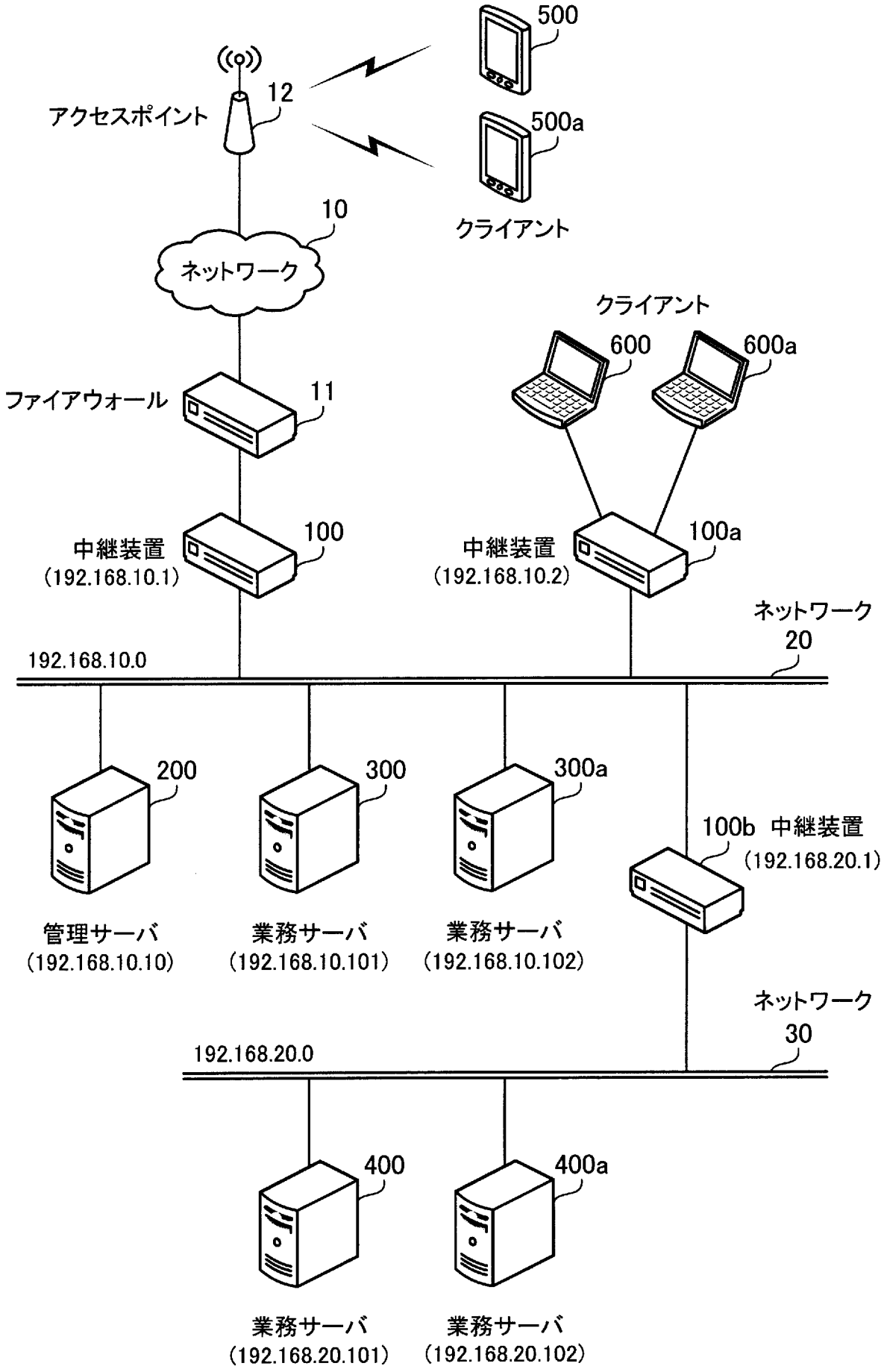
前記第２の識別情報に対応してデータの中継が許容された宛先のノードの識別情報として前記第３の識別情報を前記中継装置に提供する

、処理を実行させるプログラム。

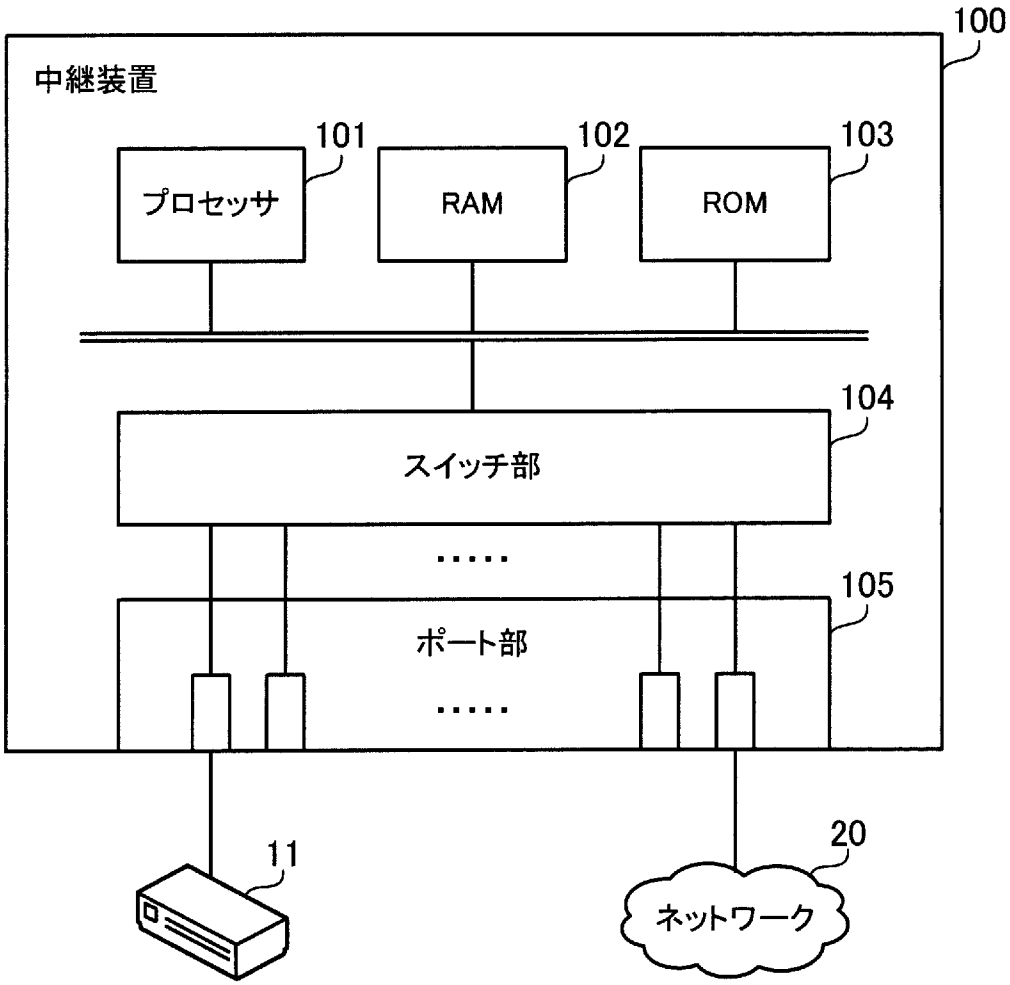
[図1]


3
ノード
(SID1)
3a
SID1
DIDa
UID1
S1
1
中継装置
(DIDa)
2
情報処理装置
1b
設定手段
1c
制御手段
S2
UID1
2b
提供手段
1a
記憶手段
SID1
DID1
S3
DID1
2a
記憶手段
UID1
DID1
UID2
DID2,DID3
S4
S5
3b
SID1
DID1
Data
中継する
3c
SID1
DID2
Data
中継しない
4
ノード
(DID1)
5
ノード
(DID2)
6
ノード
(DID3)

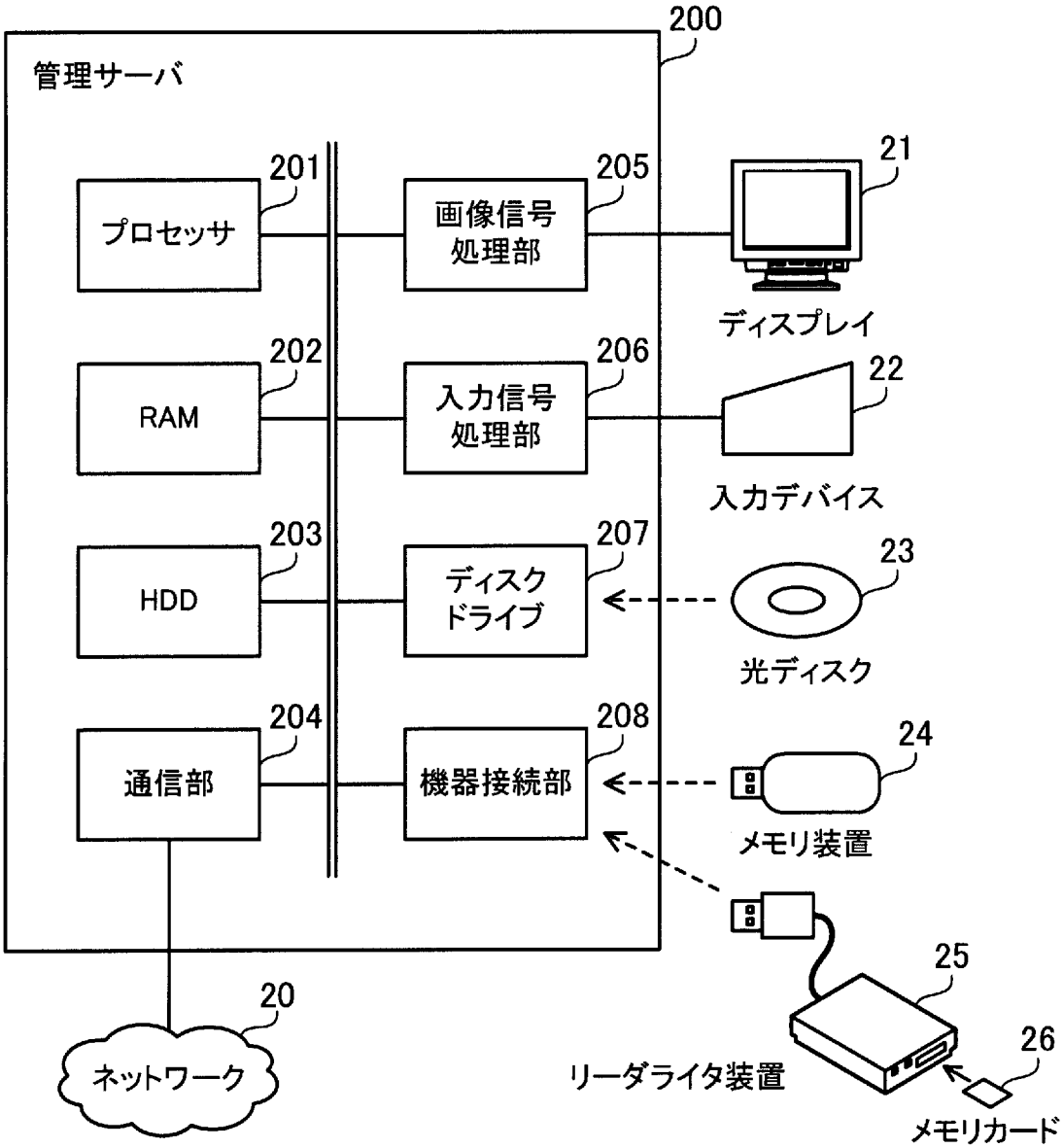
[図2]


500
アクセスポイント
12
500a
クライアント
10
ネットワーク
クライアント
600
600a
ファイアウォール
11
中継装置
(192.168.10.1)
100
中継装置
(192.168.10.2)
100a
ネットワーク
20
192.168.10.0
200
300
300a
100b 中継装置
(192.168.20.1)
管理サーバ
(192.168.10.10)
業務サーバ
(192.168.10.101)
業務サーバ
(192.168.10.102)
ネットワーク
30
192.168.20.0
400
400a
業務サーバ
(192.168.20.101)
業務サーバ
(192.168.20.102)

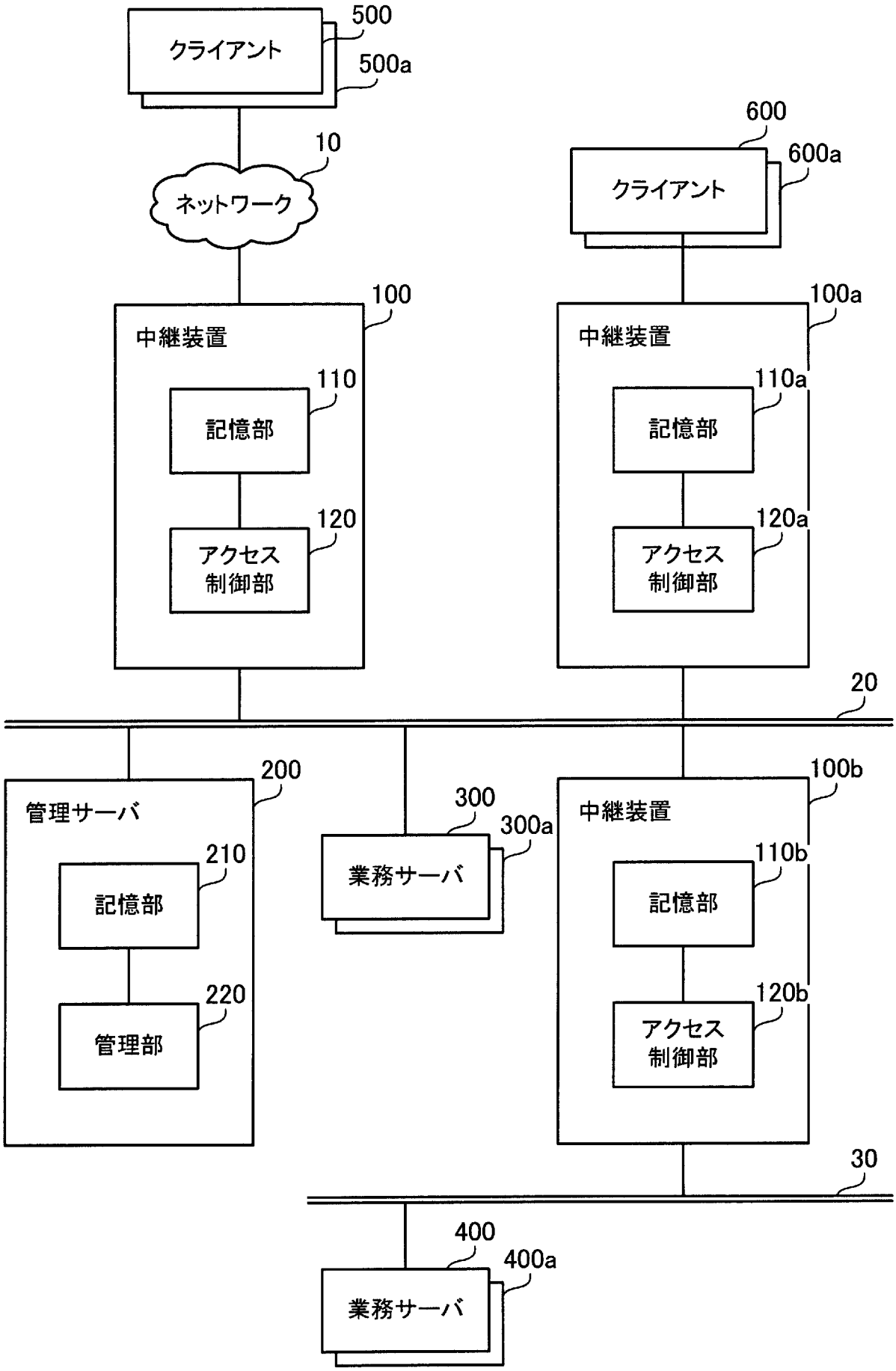
[図3]


100
中継装置
101
プロセッサ
102
RAM
103
ROM
104
スイッチ部
105
ポート部
11
20
ネットワーク

[図4]


200
管理サーバ
201
プロセッサ
202
RAM
203
HDD
204
通信部
205
画像信号処理部
206
入力信号処理部
207
ディスクドライブ
208
機器接続部
21
ディスプレイ
22
入力デバイス
23
光ディスク
24
メモリ装置
25
リーダライタ装置
26
メモリカード
20
ネットワーク

[図5]

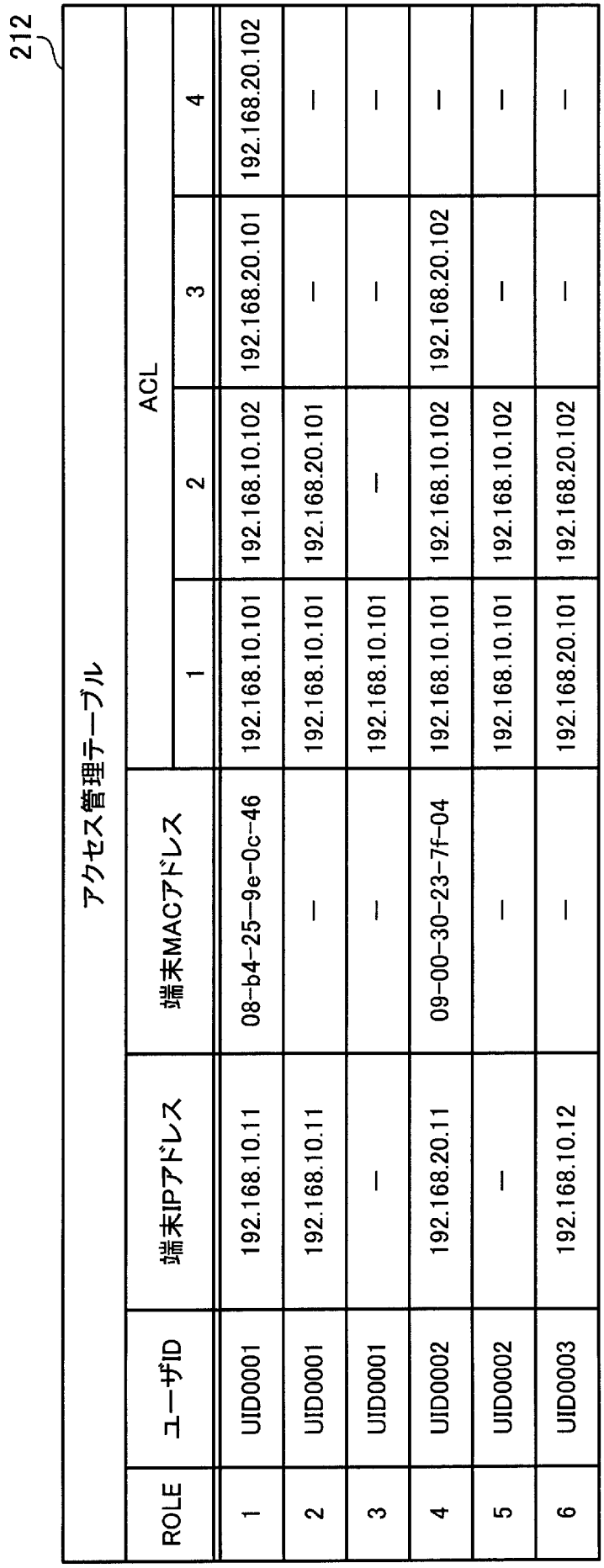

クライアント
500
500a
10
ネットワーク
600
600a
クライアント
100
中継装置
110
記憶部
120
アクセス
制御部
100a
中継装置
110a
記憶部
120a
アクセス
制御部
20
200
管理サーバ
210
記憶部
220
管理部
300
300a
業務サーバ
100b
中継装置
110b
記憶部
120b
アクセス
制御部
30
400
400a
業務サーバ

[図6]

211

ユーザ管理テーブル		
ユーザID	パスワード	多重接続設定
UID0001	pass1	可
UID0002	pass2	不可
UID0003	pass3	不可
・・・	・・・	・・・

[図7]


212
アクセス管理テーブル
ROLE
ユーザID
端末IPアドレス
端末MACアドレス
ACL
1
2
3
4
1 UID0001 192.168.10.11 08-b4-25-9e-0c-46 192.168.10.101 192.168.10.102 192.168.20.101 192.168.20.102
2 UID0001 192.168.10.11 — 192.168.10.101 192.168.20.101 — —
3 UID0001 — — 192.168.10.101 — — —
4 UID0002 192.168.20.11 09-00-30-23-7f-04 192.168.10.101 192.168.10.102 192.168.20.102 —
5 UID0002 — — 192.168.10.101 192.168.10.102 — —
6 UID0003 192.168.10.12 — 192.168.20.101 192.168.20.102 — —

[図8]

213

接続管理テーブル			
ユーザID	端末IPアドレス	中継装置 IPアドレス	適用ROLE
UID0001	50.223.3.4	192.168.10.1	ROLE3
UID0001	192.168.10.11	192.168.10.2	ROLE1
UID0002	50.223.5.5	192.168.10.1	ROLE5
UID0003	192.168.10.12	192.168.10.2	ROLE6
UID0001	192.168.10.11	192.168.20.1	ROLE1
UID0003	192.168.10.12	192.168.20.1	ROLE6

[図9]

(A)

111

セッション管理テーブル					
ROLE	端末IPアドレス	ACL			
		1	2	3	4
3	50.223.3.4	192.168.10.101	—	—	—
5	50.223.5.5	192.168.10.101	192.168.10.102	—	—

(B)

111a

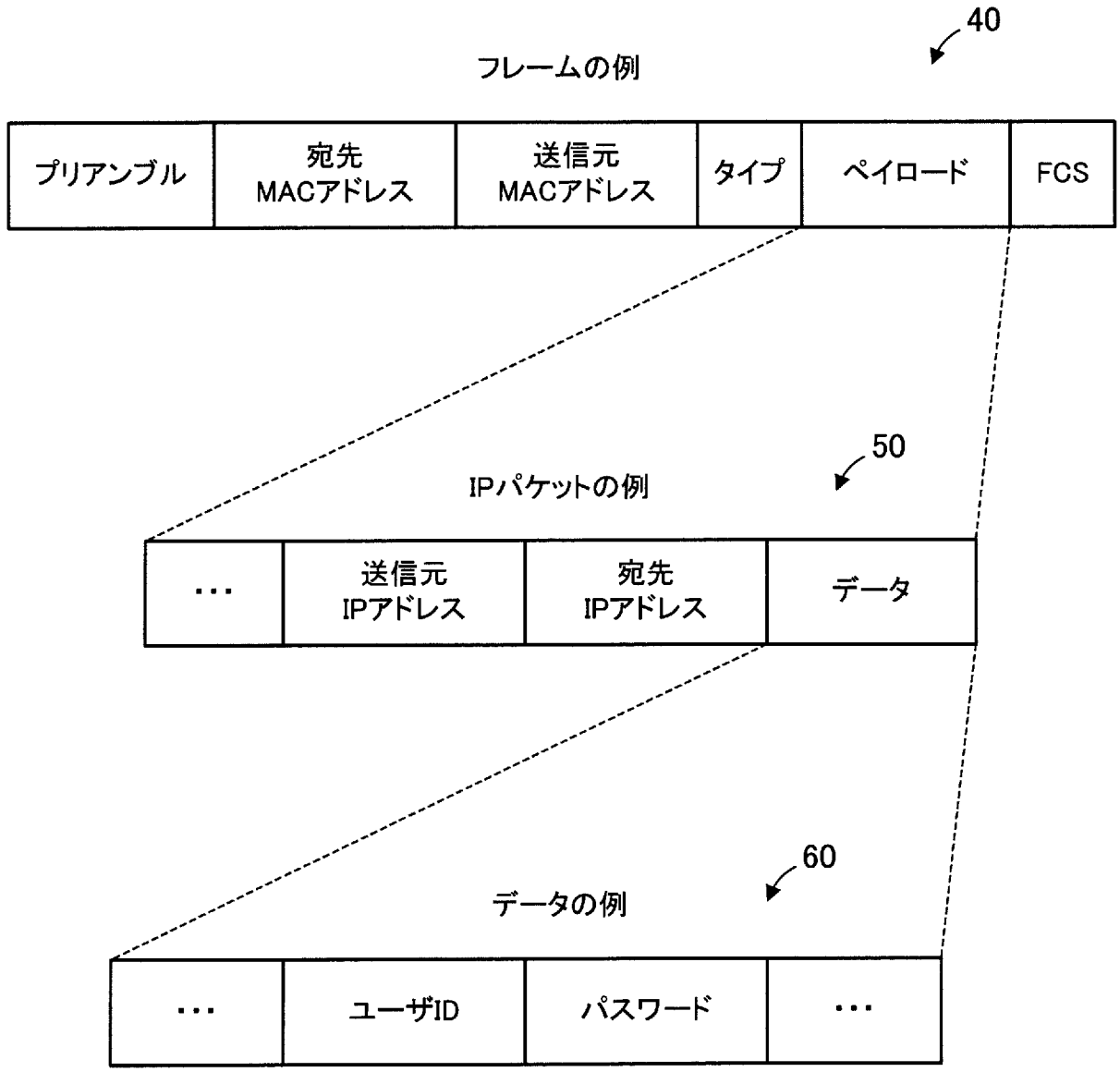
セッション管理テーブル					
ROLE	端末IPアドレス	ACL			
		1	2	3	4
1	192.168.10.11	192.168.10.101	192.168.10.102	192.168.20.101	192.168.20.102
6	192.168.10.12	192.168.20.101	192.168.20.102	—	—

(C)

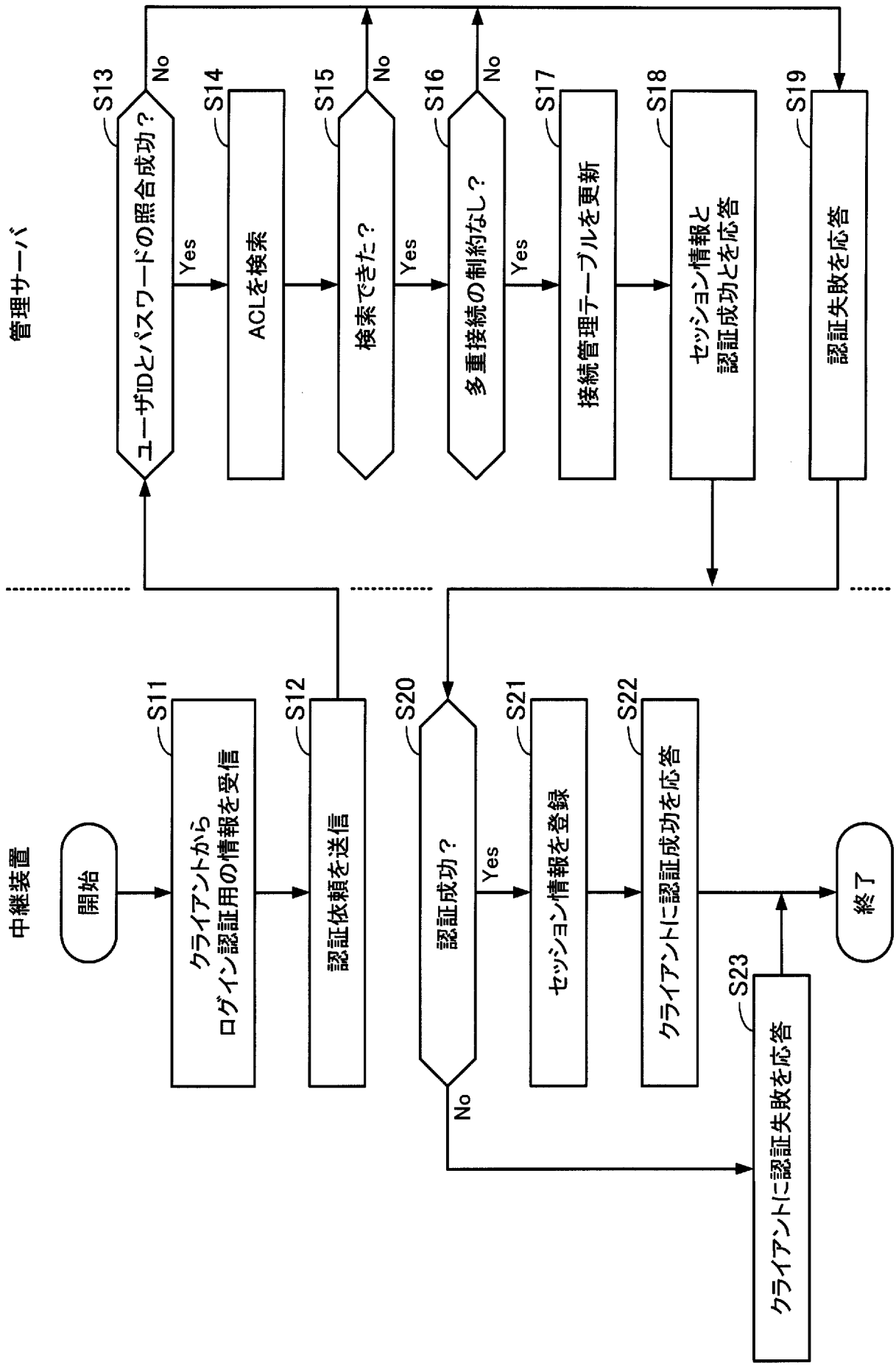
111b

セッション管理テーブル					
ROLE	端末IPアドレス	ACL			
		1	2	3	4
1	192.168.10.11	192.168.10.101	192.168.10.102	192.168.20.101	192.168.20.102
6	192.168.10.12	192.168.20.101	192.168.20.102	—	—

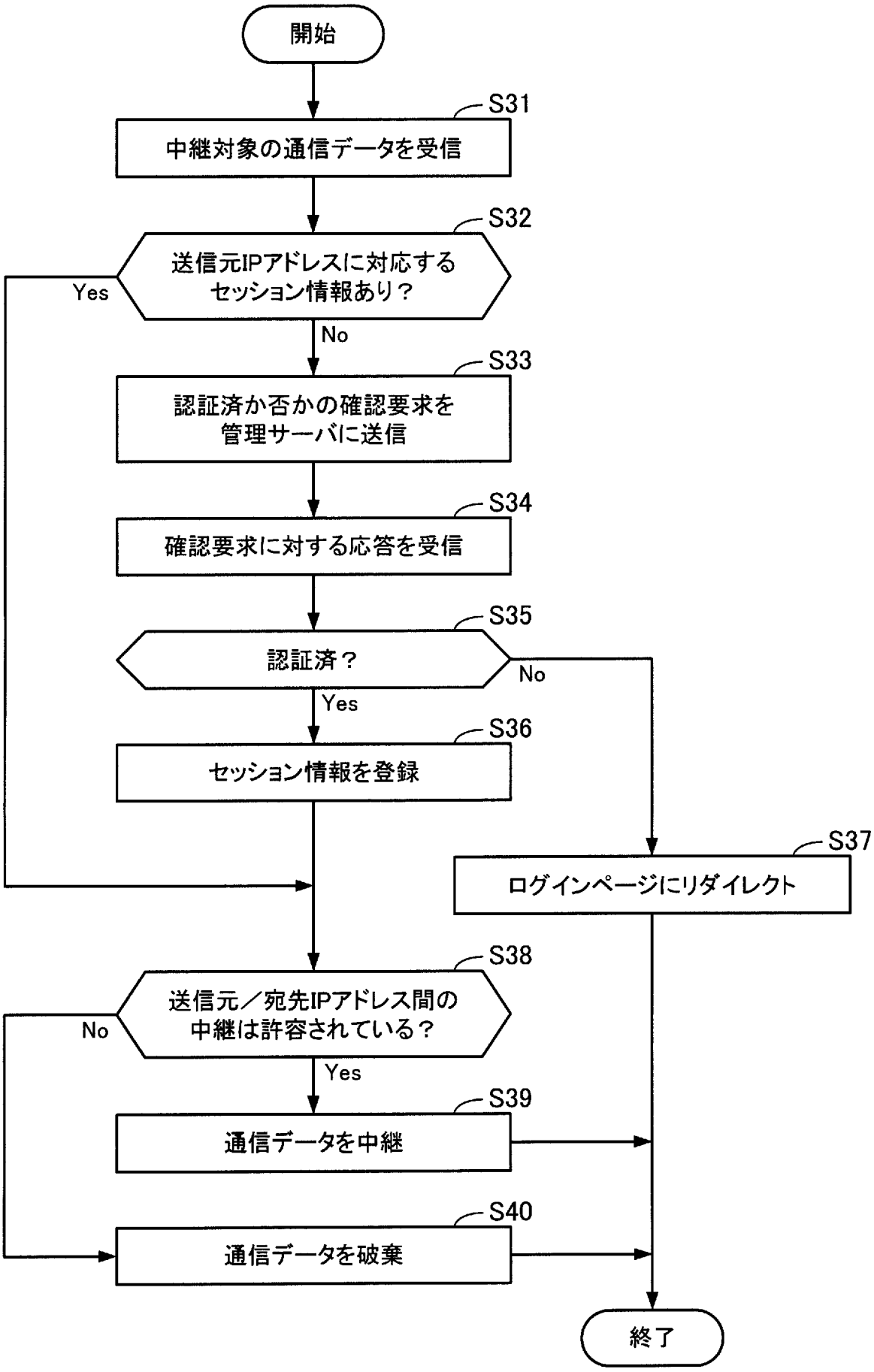
[図10]


40
フレームの例
プリアンブル
宛先
MACアドレス
送信元
MACアドレス
タイプ
ペイロード
FCS
50
IPパケットの例
・・・
送信元
IPアドレス
宛先
IPアドレス
データ
60
データの例
・・・
ユーザID
パスワード
・・・

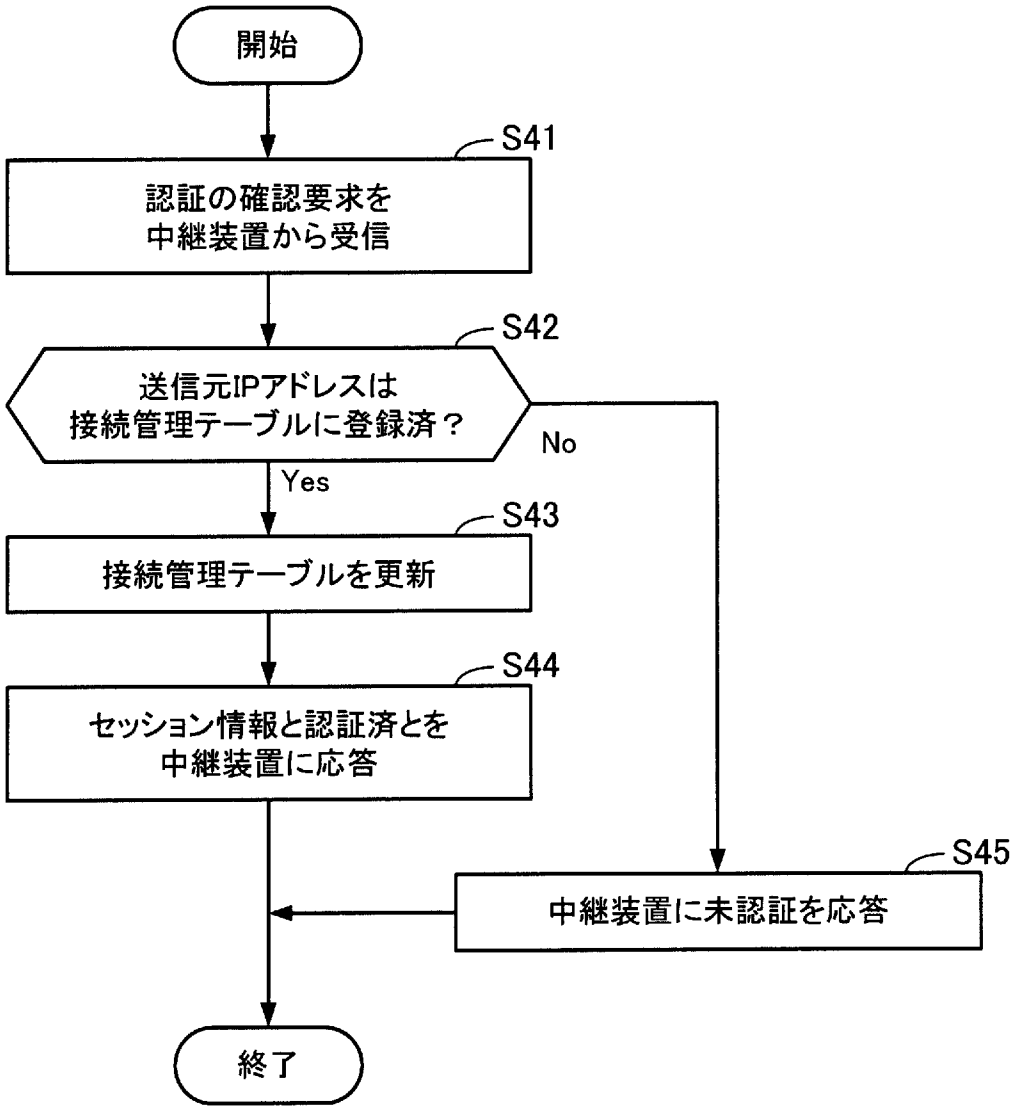
[図11]


中継装置
管理サーバ
開始
S11
クライアントから
ログイン認証用の情報を受信
S12
認証依頼を送信
S13
ユーザIDとパスワードの照合成功？
Yes
No
S14
ACLを検索
S15
検索できた？
Yes
No
S16
多重接続の制約なし？
Yes
No
S17
接続管理テーブルを更新
S18
セッション情報と
認証成功とを応答
S19
認証失敗を応答
S20
認証成功？
Yes
No
S21
セッション情報を登録
S22
クライアントに認証成功を応答
S23
クライアントに認証失敗を応答
終了

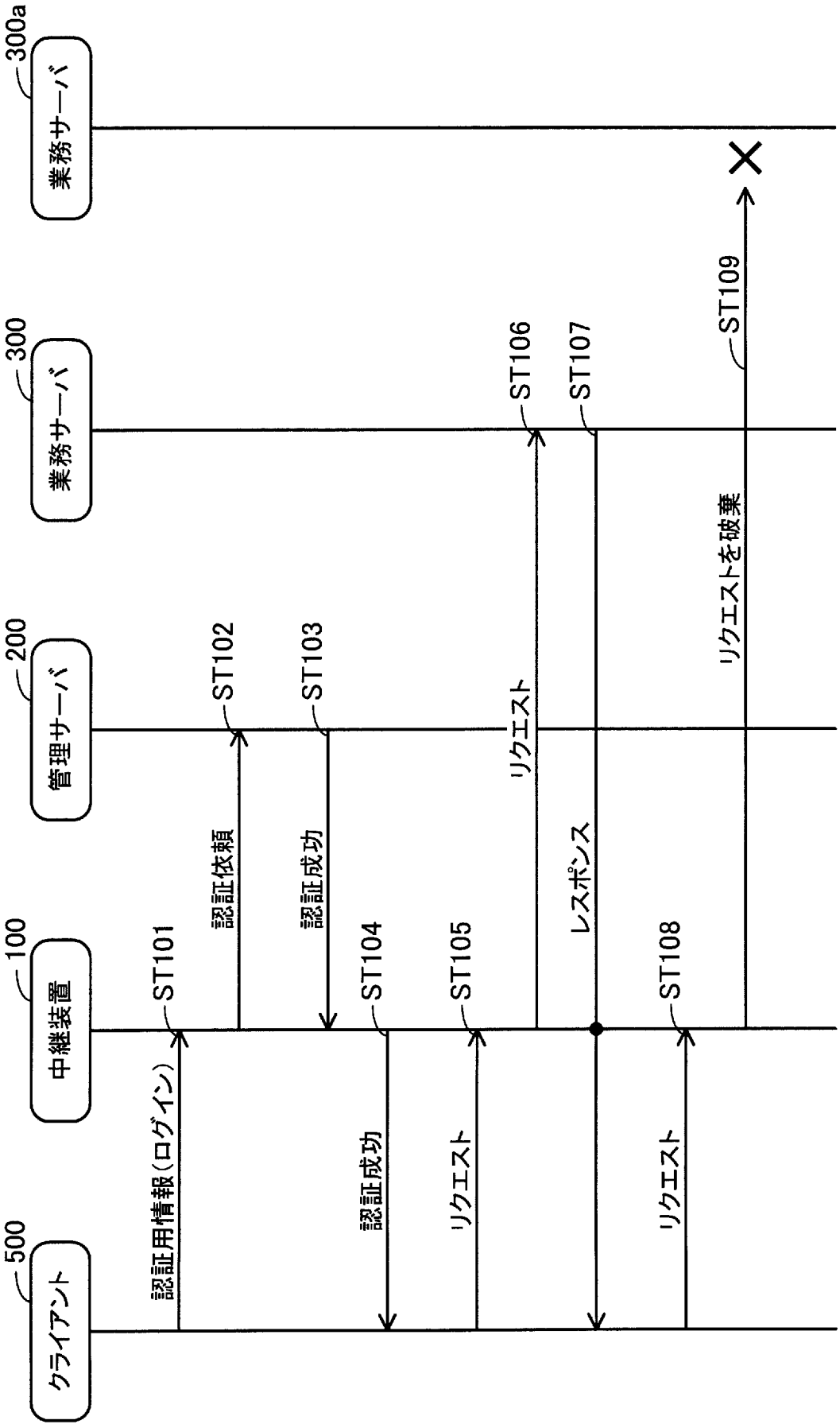
[図12]


開始
S31
中継対象の通信データを受信
S32
送信元IPアドレスに対応する
セッション情報あり？
Yes
No
S33
認証済か否かの確認要求を
管理サーバに送信
S34
確認要求に対する応答を受信
S35
認証済？
No
Yes
S36
セッション情報を登録
S37
ログインページにリダイレクト
S38
送信元／宛先IPアドレス間の
中継は許容されている？
No
Yes
S39
通信データを中継
S40
通信データを破棄
終了

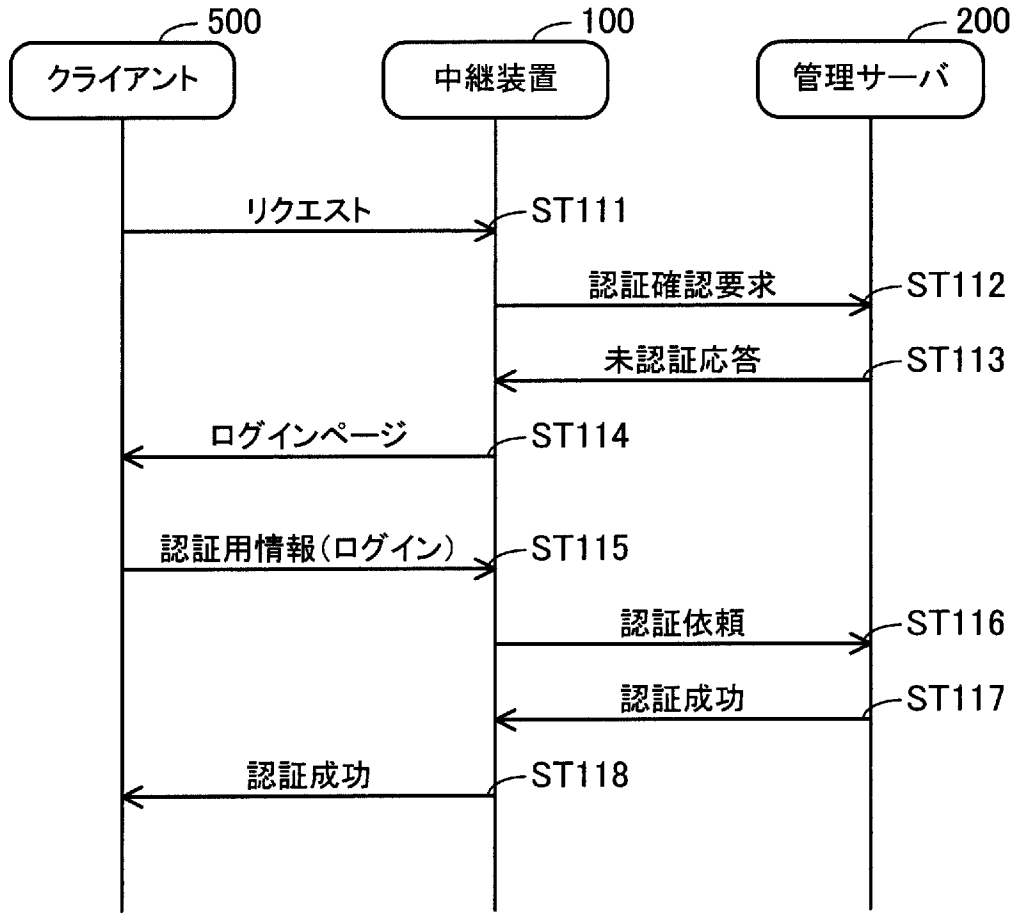
[図13]


開始
S41
認証の確認要求を
中継装置から受信
S42
送信元IPアドレスは
接続管理テーブルに登録済？
No
Yes
S43
接続管理テーブルを更新
S44
セッション情報と認証済とを
中継装置に応答
S45
中継装置に未認証を応答
終了

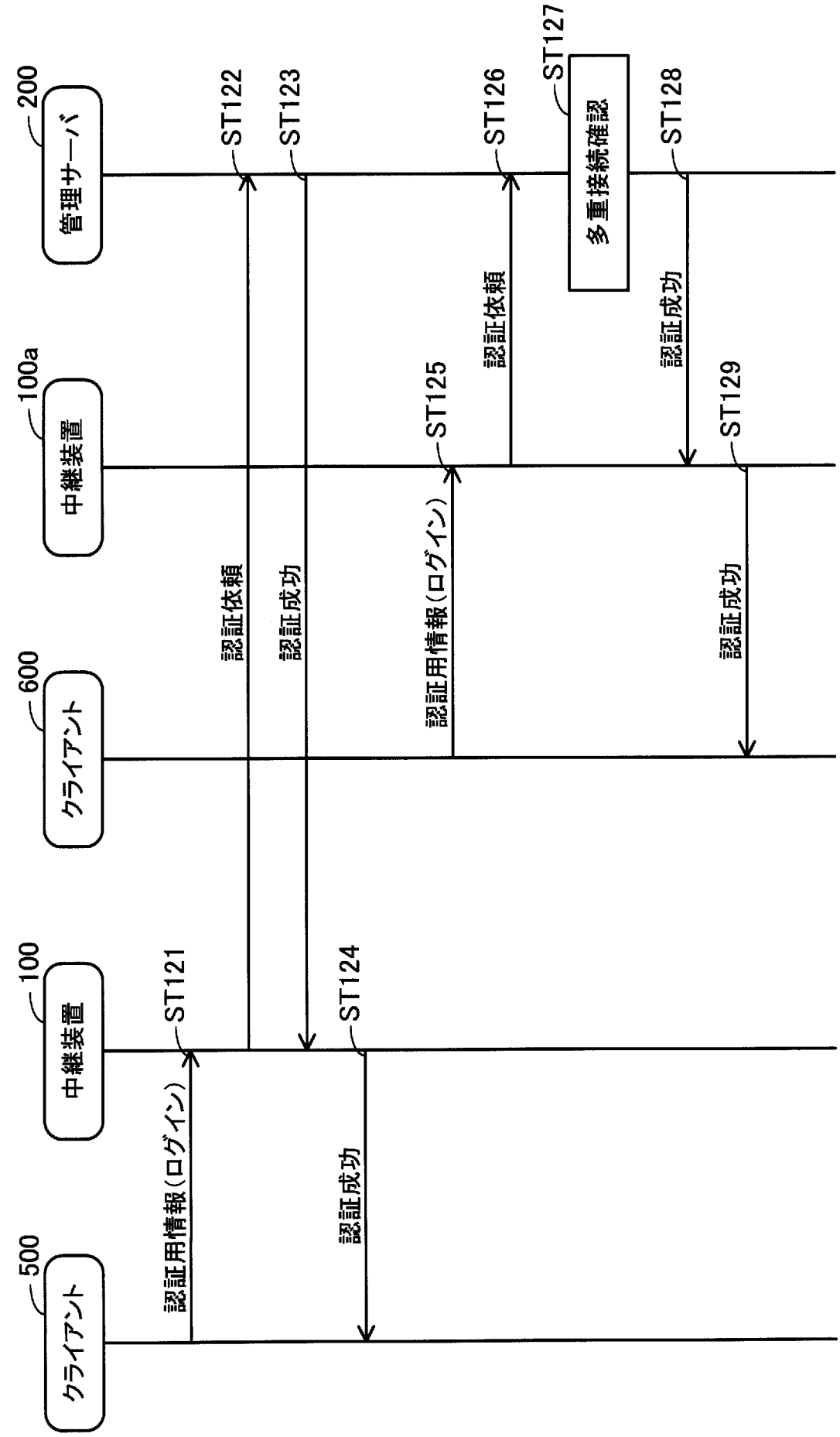
[図14]


300a
業務サーバ
300
業務サーバ
200
管理サーバ
100
中継装置
500
クライアント
ST101
ST102
ST103
ST104
ST105
ST106
ST107
ST108
ST109
認証用情報(ログイン)
認証依頼
認証成功
認証成功
リクエスト
リクエスト
レスポンス
リクエスト
リクエストを破棄

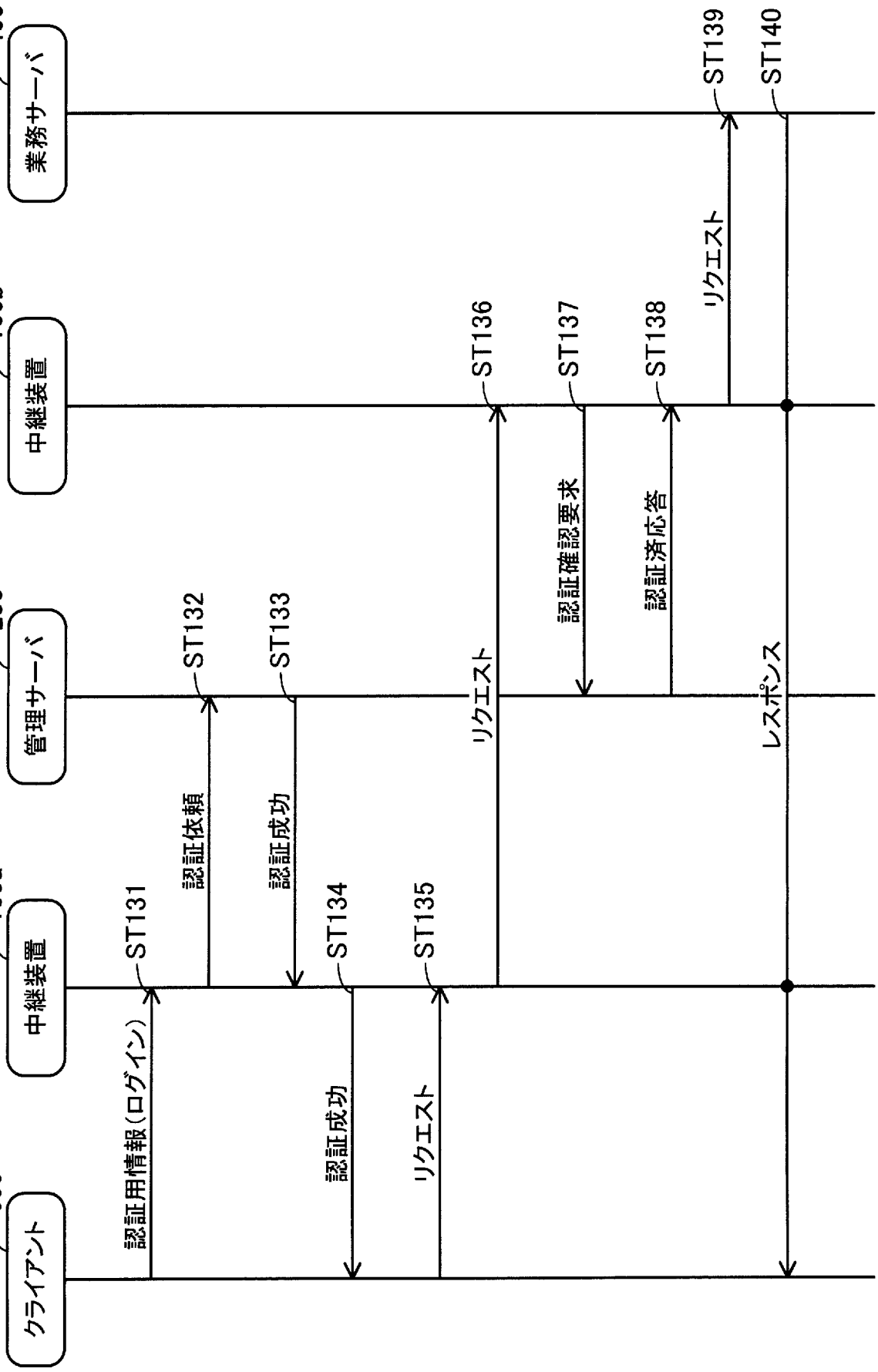
[図15]


500
クライアント
100
中継装置
200
管理サーバ
リクエスト
ST111
認証確認要求
ST112
未認証応答
ST113
ログインページ
ST114
認証用情報(ログイン)
ST115
認証依頼
ST116
認証成功
ST117
認証成功
ST118

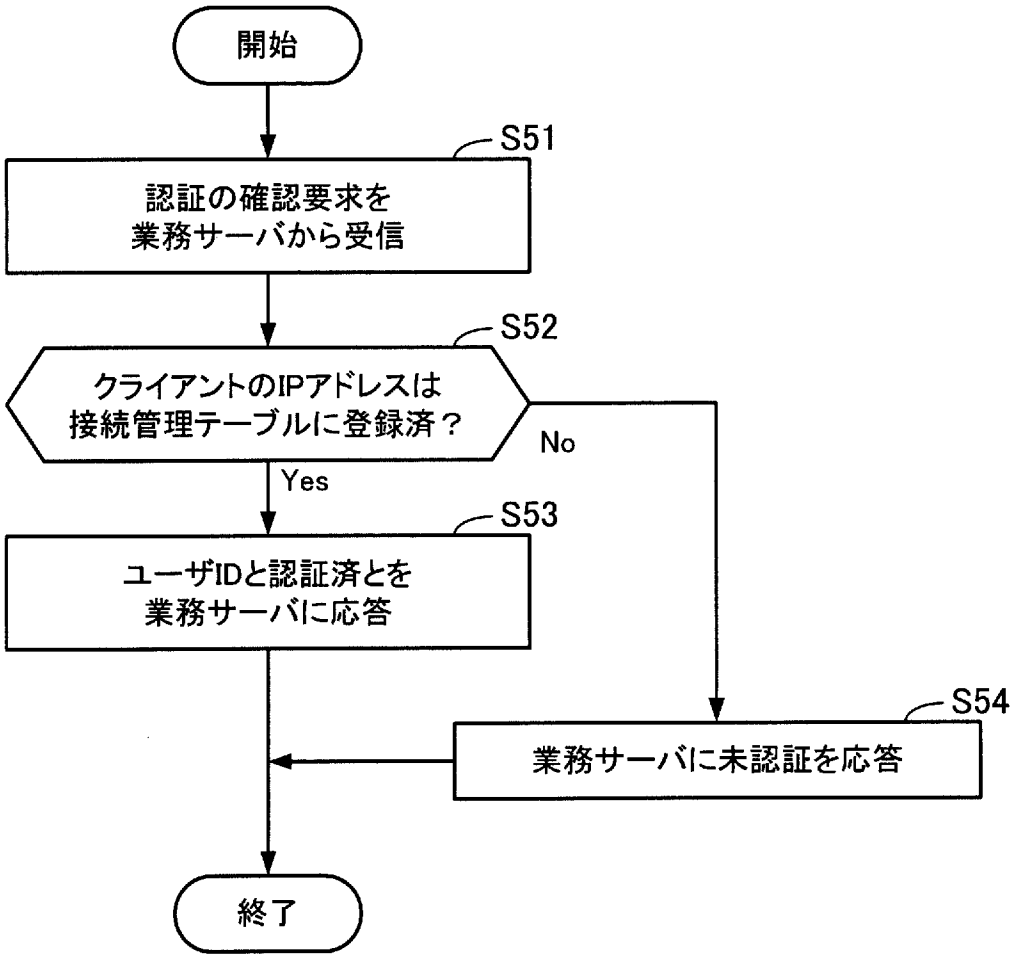
[図16]


500
クライアント
100
中継装置
600
クライアント
100a
中継装置
200
管理サーバ
ST121
認証用情報(ログイン)
ST122
認証依頼
ST123
認証成功
ST124
認証成功
ST125
認証用情報(ログイン)
ST126
認証依頼
ST127
多重接続確認
ST128
認証成功
ST129
認証成功

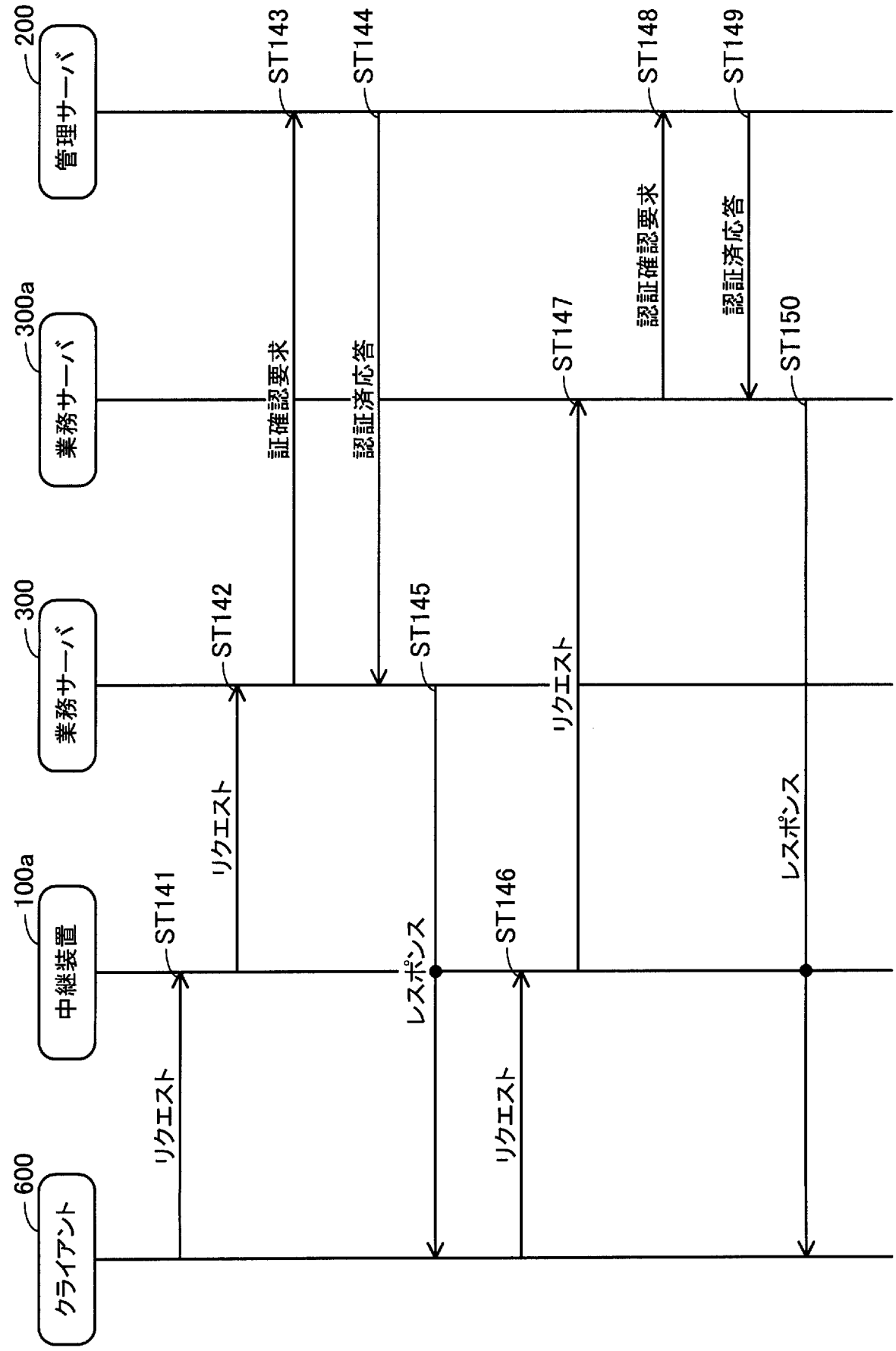
[図17]


600
クライアント
100a
中継装置
200
管理サーバ
100b
中継装置
400
業務サーバ
認証用情報（ログイン）
ST131
認証依頼
ST132
認証成功
ST133
ST134
認証成功
ST135
リクエスト
ST136
認証確認要求
ST137
認証済応答
ST138
リクエスト
ST139
レスポンス
ST140

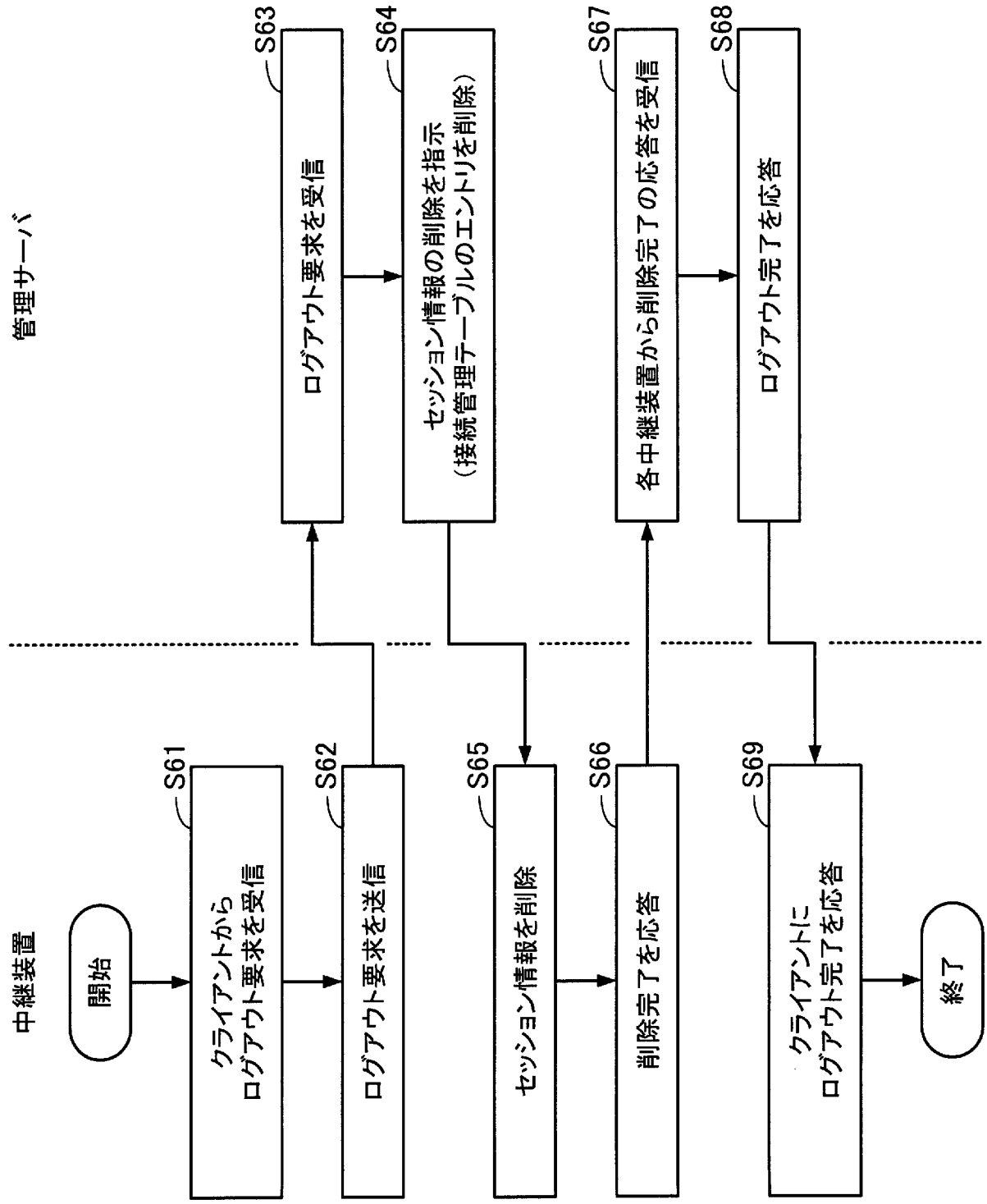
[図18]


開始
S51
認証の確認要求を
業務サーバから受信
S52
クライアントのIPアドレスは
接続管理テーブルに登録済？
No
Yes
S53
ユーザIDと認証済とを
業務サーバに応答
S54
業務サーバに未認証を応答
終了

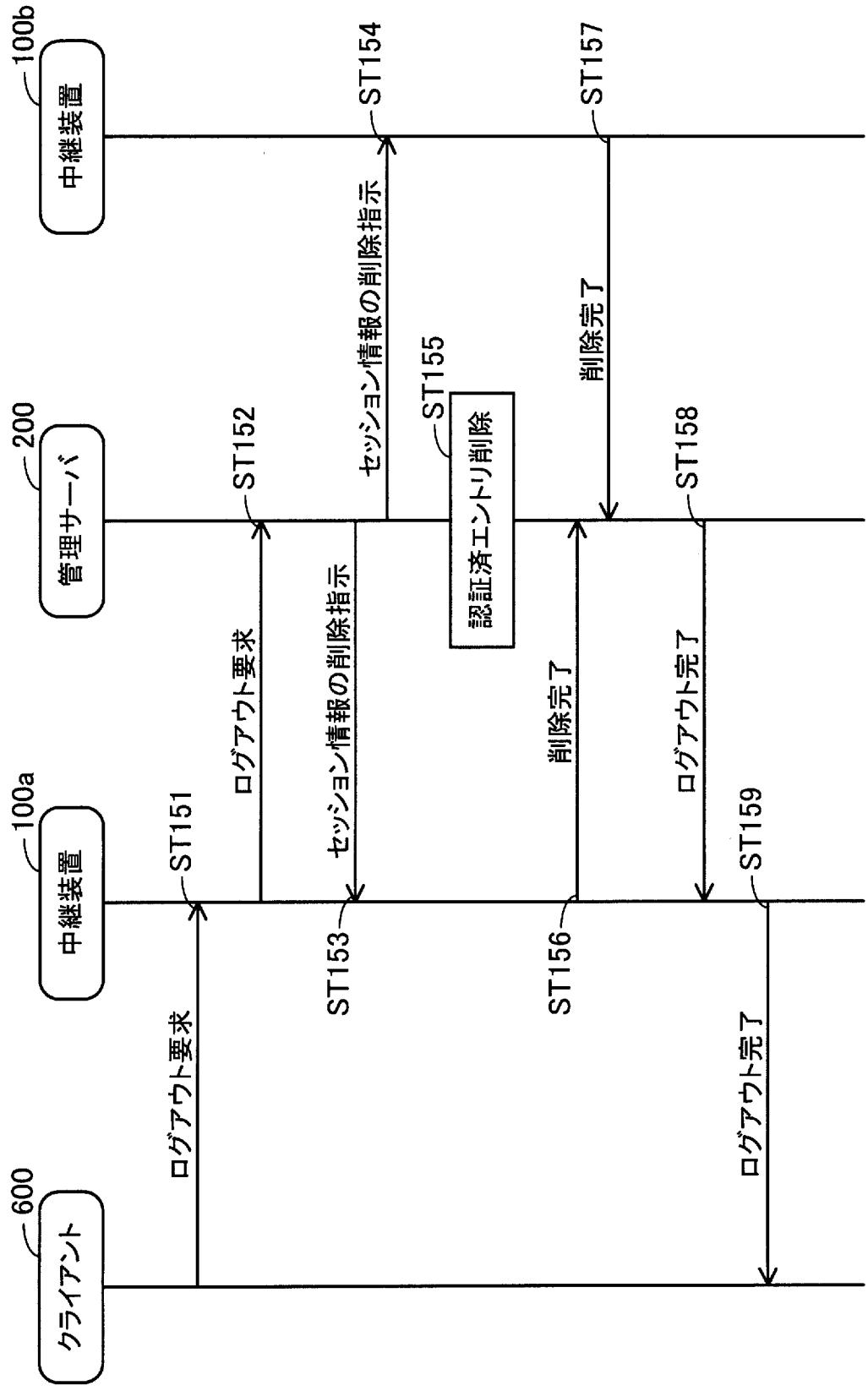
[図19]


200
管理サーバ
300a
業務サーバ
300
業務サーバ
100a
中継装置
600
クライアント
ST141
ST142
ST143
ST144
ST145
ST146
ST147
ST148
ST149
ST150
リクエスト
証確認要求
認証済応答
リクエスト
レスポンス
リクエスト
認証確認要求
認証済応答
リクエスト
レスポンス

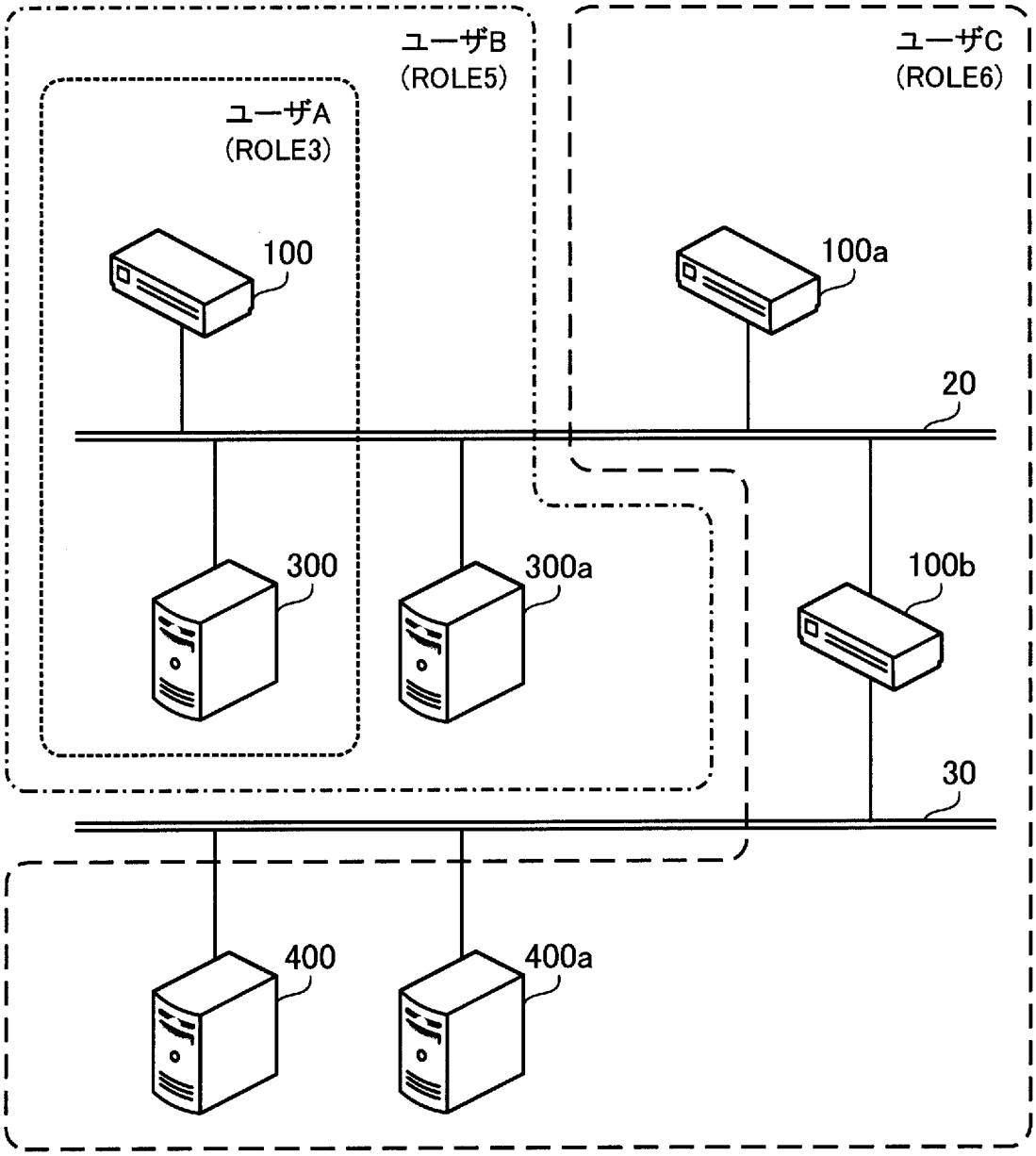
[図20]


中継装置
管理サーバ
開始
S61
クライアントから
ログアウト要求を受信
S62
ログアウト要求を送信
S63
ログアウト要求を受信
S64
セッション情報の削除を指示
(接続管理テーブルのエントリを削除)
S65
セッション情報を削除
S66
削除完了を応答
S67
各中継装置から削除完了の応答を受信
S68
ログアウト完了を応答
S69
クライアントに
ログアウト完了を応答
終了

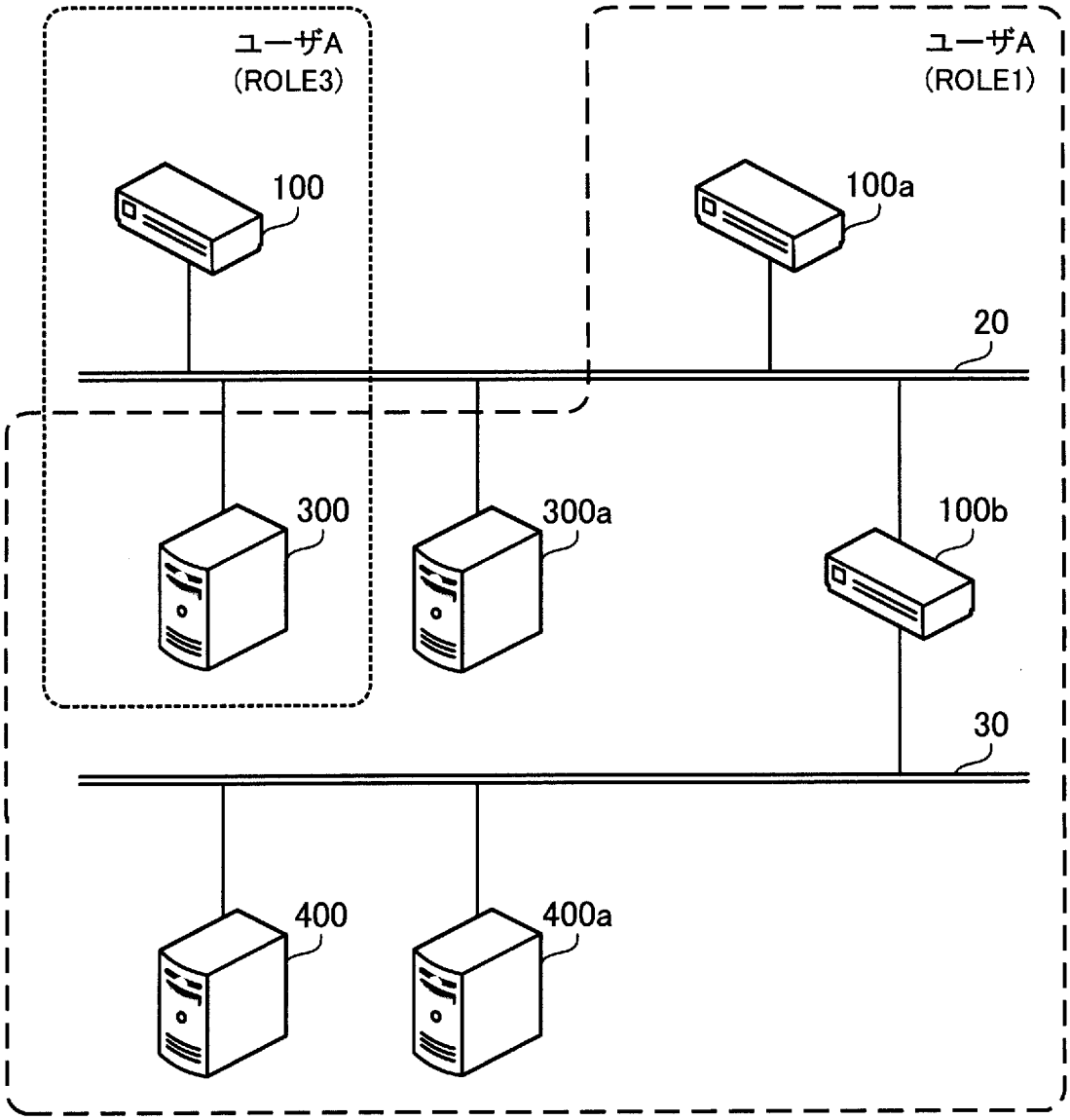
[図21]


100b
中継装置
200
管理サーバ
100a
中継装置
600
クライアント
ST151
ST152
ST153
ST154
ST155
ST156
ST157
ST158
ST159
ログアウト要求
ログアウト要求
セッション情報の削除指示
セッション情報の削除指示
認証済エントリ削除
削除完了
削除完了
ログアウト完了
ログアウト完了

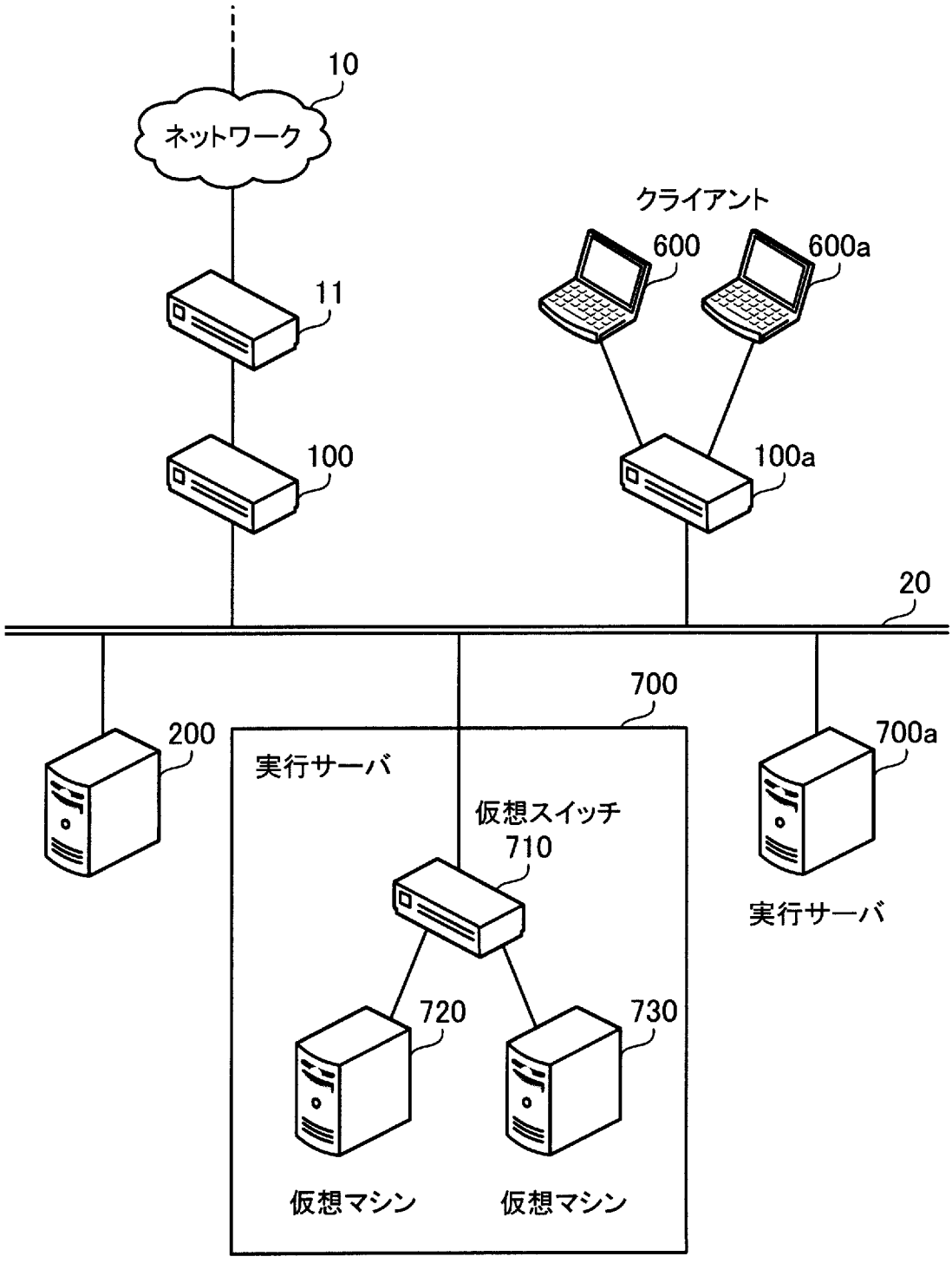
[図22]


ユーザB
(ROLE5)
ユーザC
(ROLE6)
ユーザA
(ROLE3)
100
100a
20
300
300a
100b
30
400
400a

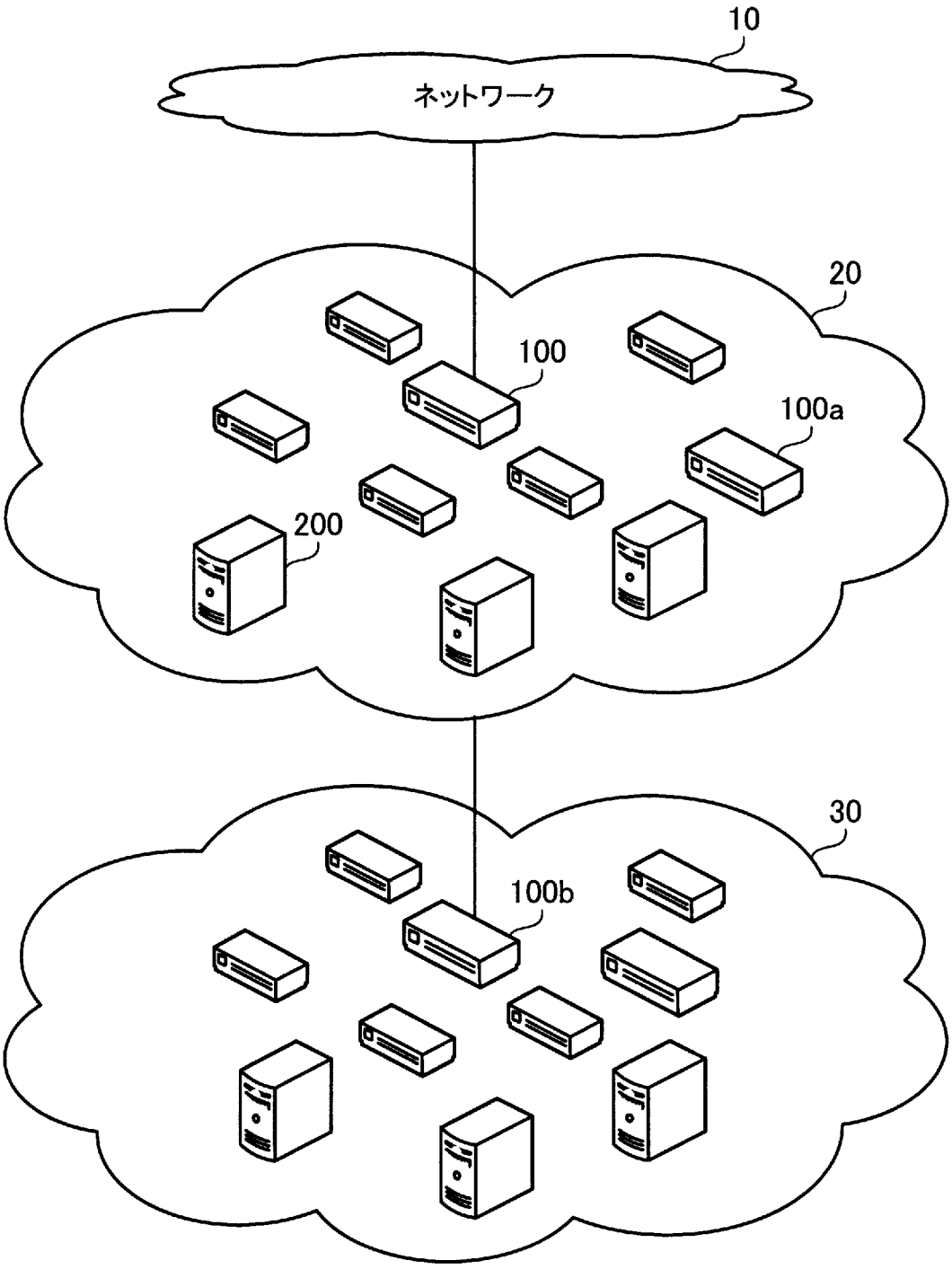
[図23]



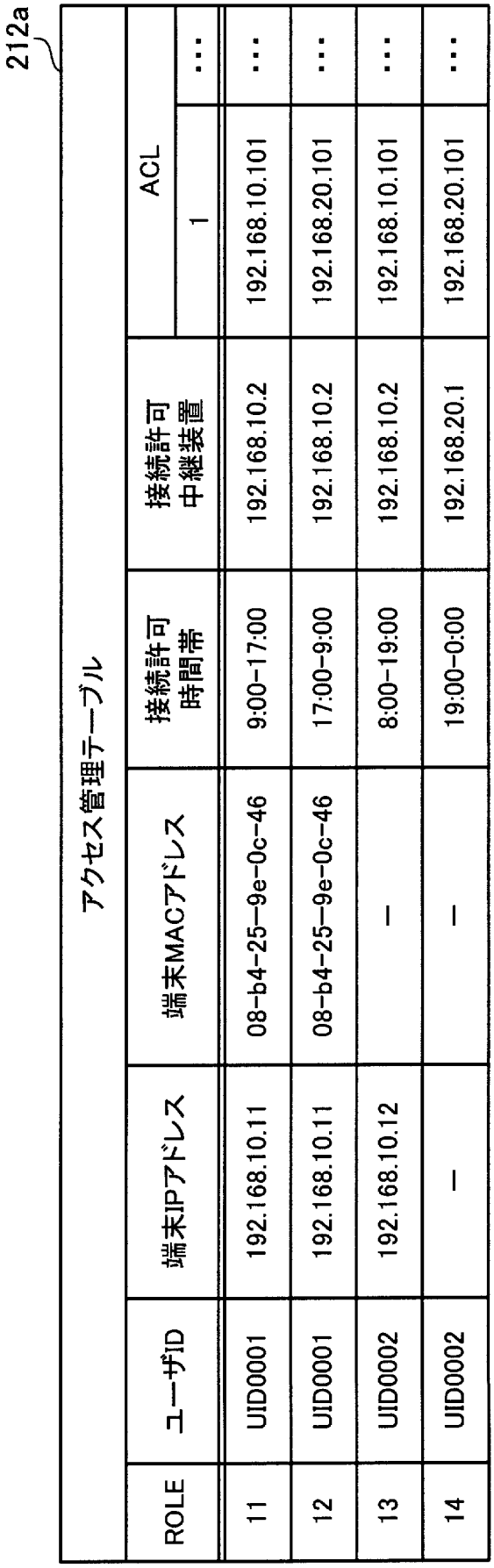
[図24]


10
ネットワーク
クライアント
600
600a
11
100
100a
20
700
200
実行サーバ
700a
仮想スイッチ
710
実行サーバ
720
730
仮想マシン
仮想マシン

[図25]



[図26]



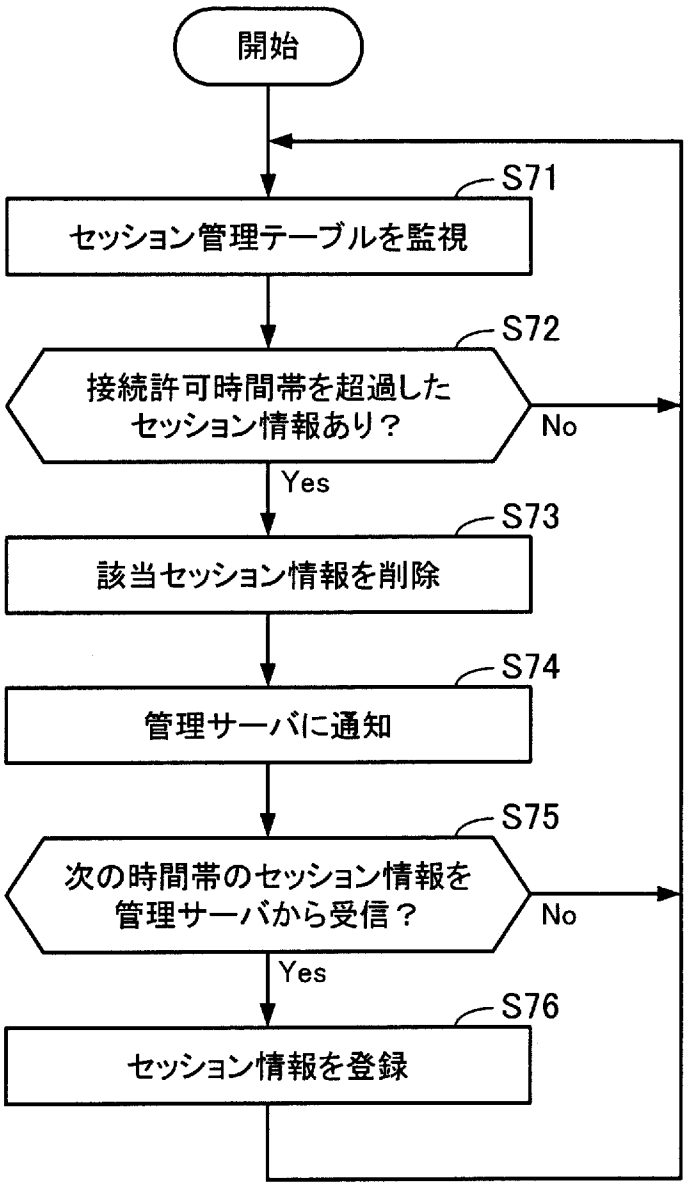
ROLE	ユーザID	端末IPアドレス	端末MACアドレス	接続許可時間帯	接続許可中継装置	ACL	
						1	・・・
11	UID0001	192.168.10.11	08-b4-25-9e-0c-46	9:00-17:00	192.168.10.2	192.168.10.101	・・・
12	UID0001	192.168.10.11	08-b4-25-9e-0c-46	17:00-9:00	192.168.10.2	192.168.20.101	・・・
13	UID0002	192.168.10.12	—	8:00-19:00	192.168.10.2	192.168.10.101	・・・
14	UID0002	—	—	19:00-0:00	192.168.20.1	192.168.20.101	・・・

[図27]

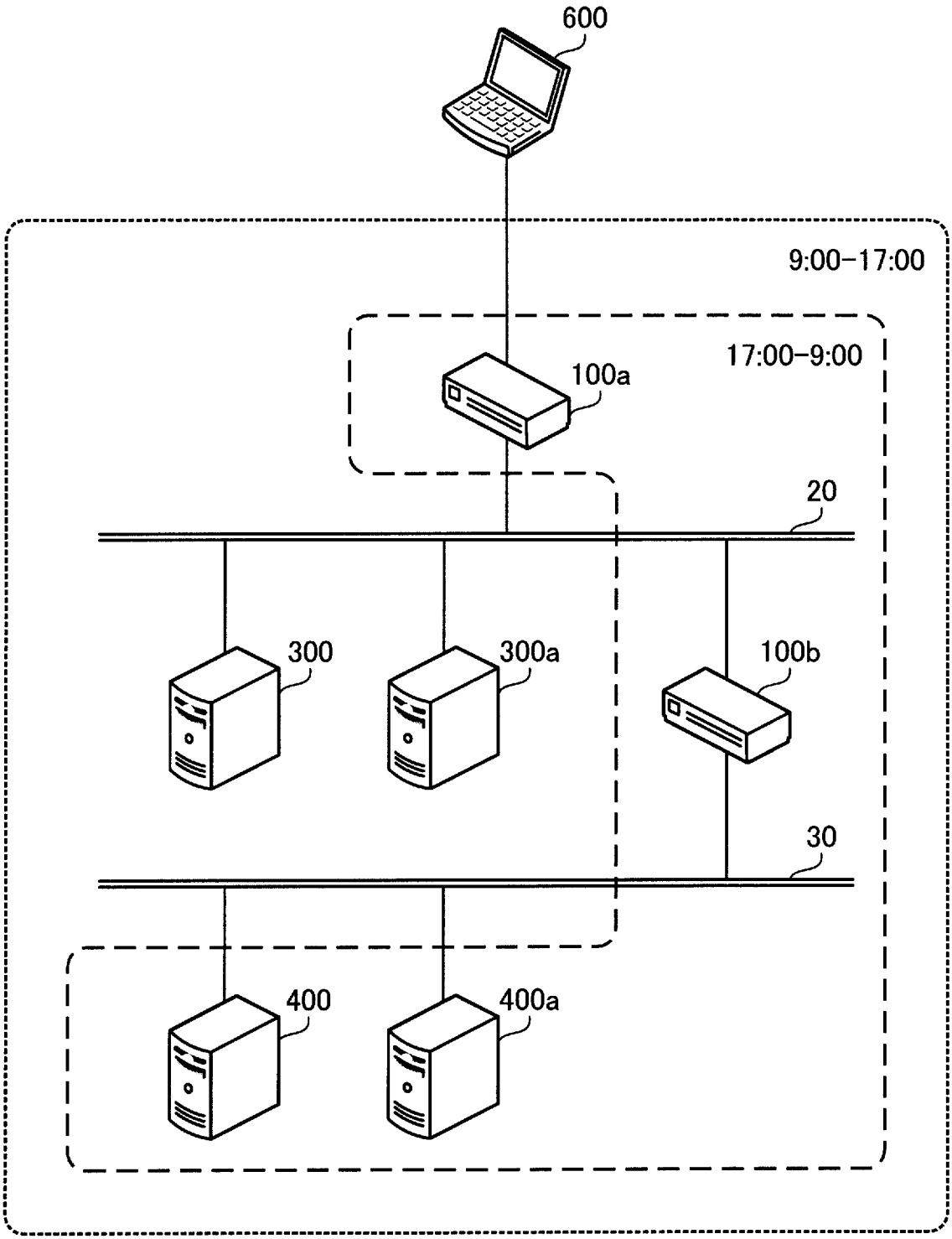
111c

セッション管理テーブル				
ROLE	端末 IPアドレス	接続許可 時間帯	ACL	
			1	・・・
11	192.168.10.11	9:00-17:00	192.168.10.101	・・・
13	192.168.10.12	8:00-19:00	192.168.10.101	・・・

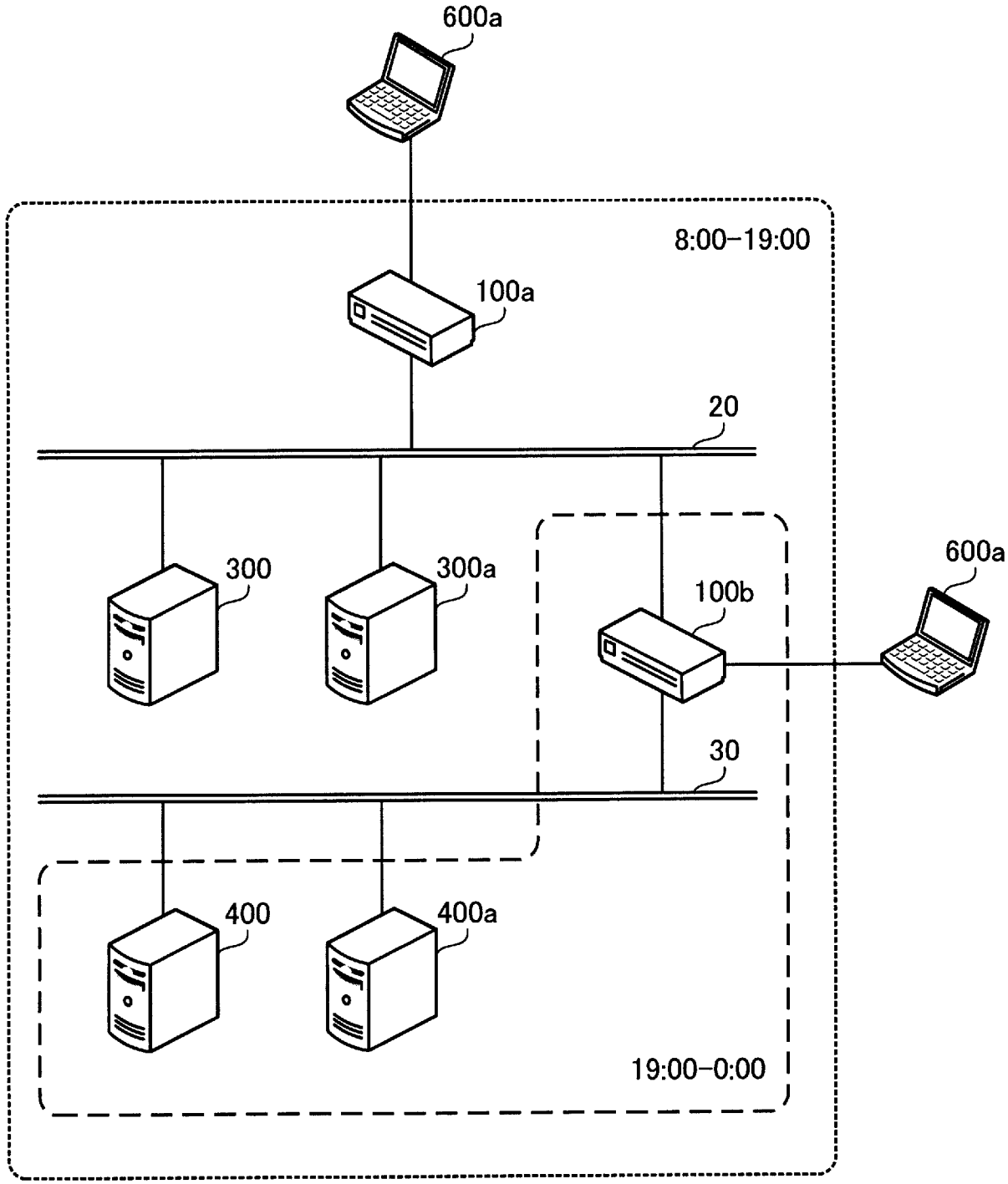
[図28]



[図29]



[図30]



INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2012/066758

A. CLASSIFICATION OF SUBJECT MATTER
H04L12/46(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L12/46

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2012
Kokai Jitsuyo Shinan Koho	1971-2012	Toroku Jitsuyo Shinan Koho	1994-2012

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	JP 2005-159683 A (Nippon Telegraph and Telephone Corp.), 16 June 2005 (16.06.2005), paragraphs [0031], [0032], [0058], [0059] (Family: none)	1-5,7-13, 15-20 6,14
Y	JP 2002-223228 A (Alcatel Internetworking Inc.), 09 August 2002 (09.08.2002), paragraph [0021] & EP 1244265 A2 & CN 1359212 A	6,14

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
12 July, 2012 (12.07.12)	31 July, 2012 (31.07.12)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１２／０６６７５８

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　H04L12/46(2006.01)i

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.　H04L12/46

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２０１２年
日本国実用新案登録公報	１９９６－２０１２年
日本国登録実用新案公報	１９９４－２０１２年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
X	JP 2005-159683 A（日本電信電話株式会社）2005.06.16, 【００３１】【００３２】【００５８】【００５９】（ファミリーなし）	1-5,7-13,15-20
Y		6,14
Y	JP 2002-223228 A（アルカテル・インターネットワーキング・インコーポレイテッド）2002.08.09, 【００２１】 & EP 1244265 A2 & CN 1359212 A	6,14

☐　Ｃ欄の続きにも文献が列挙されている。

☐　パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
１２．０７．２０１２	３１．０７．２０１２

国際調査機関の名称及びあて先
日本国特許庁（ＩＳＡ／ＪＰ）
郵便番号１００－８９１５
東京都千代田区霞が関三丁目４番３号

特許庁審査官（権限のある職員）　５Ｘ　３３６１
岩田　玲彦
電話番号　０３－３５８１－１１０１　内線　３５９６