

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第4142014号
(P4142014)

(45) 発行日 平成20年8月27日(2008.8.27)

(24) 登録日 平成20年6月20日(2008.6.20)

(51) Int.Cl.

F I

H O 4 L 12/46 (2006.01)

H O 4 L 12/46

A

H O 4 L 12/46

E

請求項の数 16 (全 19 頁)

(21) 出願番号 特願2004-556897 (P2004-556897)
 (86) (22) 出願日 平成15年12月3日(2003.12.3)
 (86) 国際出願番号 PCT/JP2003/015474
 (87) 国際公開番号 W02004/051936
 (87) 国際公開日 平成16年6月17日(2004.6.17)
 審査請求日 平成18年1月13日(2006.1.13)
 (31) 優先権主張番号 PCT/JP02/12795
 (32) 優先日 平成14年12月5日(2002.12.5)
 (33) 優先権主張国 日本国(JP)

(73) 特許権者 396008347
 アライドテレシスホールディングス株式会
 社
 東京都品川区西五反田7-21-11 第
 2 T O C ビル
 (74) 代理人 100104156
 弁理士 龍華 明裕
 (72) 発明者 加藤 秀雄
 東京都品川区西五反田7-22-17 T
 O C ビル アライドテレシス株式会社内

審査官 中木 努

最終頁に続く

(54) 【発明の名称】 ユーザ特定システム、ユーザ特定装置、ユーザ特定方法、アドレス変換装置、及びプログラム

(57) 【特許請求の範囲】

【請求項1】

第1アドレス体系の第1ネットワークに配置され、第2アドレス体系の第2ネットワークにおける通信を行ったユーザ端末のユーザを特定するユーザ特定システムであって、

前記ユーザ端末の端末識別情報と当該端末識別情報に対して割り当てられた前記第1アドレス体系の第1アドレスとを対応づけて格納する第1格納装置と、

第1アドレスと当該第1アドレスに対して割り当てられた前記第2アドレス体系の第2アドレスとを対応づけて格納する第2格納装置と、

前記第1格納装置及び前記第2格納装置が格納する通信情報に基づいて、前記第2ネットワークにおける通信を行った前記ユーザ端末のユーザを特定するユーザ特定装置と
 を備え、

前記ユーザ特定装置は、

前記第1格納装置が格納する前記端末識別情報と前記第1アドレスとが対応づけられた第1通信情報を取得する第1通信情報取得部と、

前記第2格納装置が格納する前記第1アドレスと前記第2アドレスとが対応づけられた第2通信情報を取得する第2通信情報取得部と、

指定された前記第2アドレスに対応づけられた前記第1アドレスを前記第2通信情報に基づいて検出し、当該第1アドレスに対応づけられた前記端末識別情報を前記第1通信情報に基づいて検出するユーザ端末検出部と

を有することを特徴とするユーザ特定システム。

10

20

【請求項 2】

前記第 1 格納装置は、前記端末識別情報である M A C アドレスに対して前記第 1 アドレスであるプライベート I P アドレスを割り当てる D H C P サーバであり、前記 M A C アドレスに対して前記プライベート I P アドレスを割り当てた場合に、前記ユーザ特定装置に対して前記第 1 通信情報を送信することを特徴とする請求項 1 に記載のユーザ特定システム。

【請求項 3】

前記第 1 格納装置は、前記端末識別情報である M A C アドレスと当該 M A C アドレスに対して割り当てられた前記第 1 アドレスであるプライベート I P アドレスとを対応づけて格納する A R P テーブルを有する A R P サーバであり、前記ユーザ端末から A R P リクエストを受信した場合に、前記ユーザ特定装置に対して前記第 1 通信情報を送信することを特徴とする請求項 1 に記載のユーザ特定システム。

10

【請求項 4】

前記第 2 格納装置は、前記第 1 ネットワークと前記第 2 ネットワークとを接続し、前記第 1 アドレスであるプライベート I P アドレスに対して前記第 2 アドレスであるグローバル I P アドレスを割り当てるアドレス変換サーバであり、前記プライベート I P アドレスに対して前記グローバル I P アドレスを割り当てた場合に、前記ユーザ特定装置に対して前記第 2 通信情報を送信することを特徴とする請求項 1 に記載のユーザ特定システム。

【請求項 5】

前記第 1 ネットワークに配置され、複数の前記ユーザ端末がそれぞれ接続された複数の物理ポートを有し、前記物理ポートと当該物理ポートに接続された前記ユーザ端末の端末識別情報とを対応づけて格納する第 3 格納装置をさらに備え、

20

前記ユーザ特定装置は、前記第 3 格納装置が格納する前記物理ポートと前記端末識別情報とが対応づけられた第 3 通信情報を取得する第 3 通信情報取得部をさらに有し、

前記ユーザ端末検出部は、指定された前記第 2 アドレスに対応づけられた前記第 1 アドレスを前記第 2 通信情報に基づいて検出し、当該第 1 アドレスに対応づけられた前記端末識別情報を前記第 1 通信情報に基づいて検出し、当該端末識別情報に対応づけられた前記物理ポートを前記第 3 通信情報に基づいて検出する請求項 1 に記載のユーザ特定システム。

【請求項 6】

30

前記第 3 格納装置は、前記物理ポートと前記端末識別情報である M A C アドレスとを対応づけて格納するフォワーディングデータベースであり、前記フォワーディングデータベースを更新した場合に、前記ユーザ特定装置に対して前記第 3 通信情報を送信することを特徴とする請求項 5 に記載のユーザ特定システム。

【請求項 7】

前記ユーザ端末が接続された中継機器の物理ポートに割り当てられた V L A N を識別する V L A N 識別情報と、当該物理ポートに接続された前記ユーザ端末の端末識別情報とを対応づけて格納する第 3 格納装置をさらに備え、

前記ユーザ特定装置は、前記第 3 格納装置が格納する前記 V L A N 識別情報と前記端末識別情報とが対応づけられた第 3 通信情報を取得する第 3 通信情報取得部をさらに有し、

40

前記ユーザ端末検出部は、指定された前記第 2 アドレスに対応づけられた前記第 1 アドレスを前記第 2 通信情報に基づいて検出し、当該第 1 アドレスに対応づけられた前記端末識別情報を前記第 1 通信情報に基づいて検出し、当該端末識別情報に対応づけられた前記 V L A N 識別情報を前記第 3 通信情報に基づいて検出する請求項 1 に記載のユーザ特定システム。

【請求項 8】

第 1 アドレス体系の第 1 ネットワークに配置され、第 2 アドレス体系の第 2 ネットワークにおける通信を行ったユーザ端末のユーザを特定するユーザ特定システムであって、

前記ユーザ端末の端末識別情報と当該端末識別情報に対して割り当てられた前記第 1 アドレス体系の第 1 アドレスとを対応づけて格納する第 1 通信情報格納部、第 1 アドレスと

50

当該第 1 アドレスに対して割り当てられた前記第 2 アドレス体系の第 2 アドレスとを対応づけて格納する第 2 通信情報格納部、及び前記第 1 通信情報格納部が格納する前記端末識別情報と前記第 1 アドレスとが対応づけられた第 1 通信情報、及び前記第 2 通信情報格納部が格納する前記第 1 アドレスと前記第 2 アドレスとが対応づけられた第 2 通信情報に基づいて、前記端末識別情報と前記第 2 アドレスとが対応づけられたユーザ特定情報を生成するユーザ特定情報生成部を有する中継機器と、

前記第 1 ネットワークに配置され、複数の前記ユーザ端末がそれぞれ接続された複数の物理ポートを有し、前記物理ポートと当該物理ポートに接続された前記ユーザ端末の端末識別情報とを対応づけて格納する第 3 格納装置と、

前記第 3 格納装置が格納する通信情報、及び前記中継機器が生成した前記ユーザ特定情報に基づいて、前記第 2 ネットワークにおける通信を行った前記ユーザ端末のユーザを特定するユーザ特定装置と

を備え、

前記ユーザ特定装置は、

前記第 3 格納装置が格納する前記物理ポートと前記端末識別情報とが対応づけられた第 3 通信情報を取得する第 3 通信情報取得部と、

前記中継機器が格納する前記端末識別情報と前記第 2 アドレスとが対応づけられた前記ユーザ特定情報を取得する第 4 通信情報取得部と、

指定された前記第 2 アドレスに対応づけられた前記端末識別情報を前記ユーザ特定情報に基づいて検出し、当該端末識別情報に対応づけられた前記物理ポートを前記第 3 通信情報に基づいて検出するユーザ端末検出部と

を有することを特徴とするユーザ特定システム。

【請求項 9】

第 1 アドレス体系の第 1 ネットワークに配置されたユーザ端末の端末識別情報と当該端末識別情報に対して割り当てられた前記第 1 アドレス体系の第 1 アドレスとを対応づけて格納する第 1 格納装置と、第 1 アドレスと当該第 1 アドレスに対して割り当てられた第 2 アドレス体系の第 2 アドレスとを対応づけて格納する第 2 格納装置とを備えるユーザ特定システムの、前記第 1 格納装置及び前記第 2 格納装置が格納する通信情報に基づいて、前記第 2 アドレス体系の第 2 ネットワークにおける通信を行った前記ユーザ端末のユーザを特定するユーザ特定装置であって、

前記第 1 格納装置が格納する前記端末識別情報と前記第 1 アドレスとが対応づけられた第 1 通信情報を取得する第 1 通信情報取得部と、

前記第 2 格納装置が格納する前記第 1 アドレスと前記第 2 アドレスとが対応づけられた第 2 通信情報を取得する第 2 通信情報取得部と、

指定された前記第 2 アドレスに対応づけられた前記第 1 アドレスを前記第 2 通信情報に基づいて検出し、当該第 1 アドレスに対応づけられた前記端末識別情報を前記第 1 通信情報に基づいて検出するユーザ端末検出部と

を備えることを特徴とするユーザ特定装置。

【請求項 10】

前記第 2 通信情報取得部は、前記第 1 アドレス及び前記第 2 アドレスに、当該第 2 アドレスを送信元アドレスとするパケットの宛先アドレスが対応づけられた、前記第 2 格納装置が格納する前記第 2 通信情報を取得し、

前記ユーザ端末検出部は、指定された前記第 2 アドレス及び前記宛先アドレスに基づいて前記第 1 アドレスを検出することを特徴とする請求項 9 に記載のユーザ特定装置。

【請求項 11】

前記第 1 通信情報及び前記第 2 通信情報に対応づけて、前記第 1 通信情報及び前記第 2 通信情報を取得した時刻をそれぞれ格納する通信情報格納部をさらに備え、

前記ユーザ端末検出部は、前記通信情報格納部が格納する前記時刻を参照して、指定された前記第 2 アドレスに対応づけられた前記第 1 アドレスを検出し、当該第 1 アドレスに対応づけられた前記端末識別情報を検出することを特徴とする請求項 9 に記載のユーザ特

10

20

30

40

50

定装置。

【請求項 1 2】

第 1 アドレス体系の第 1 ネットワークに配置されたユーザ端末の端末識別情報と当該端末識別情報に対して割り当てられた前記第 1 アドレス体系の第 1 アドレスとを対応づけて格納する第 1 格納装置と、第 1 アドレスと当該第 1 アドレスに対して割り当てられた第 2 アドレス体系の第 2 アドレスとを対応づけて格納する第 2 格納装置とを備えるユーザ特定システムの、前記第 1 格納装置及び前記第 2 格納装置が格納する通信情報に基づいて、前記第 2 アドレス体系の第 2 ネットワークにおける通信を行った前記ユーザ端末のユーザを特定するユーザ特定方法であって、

前記第 1 格納装置が格納する前記端末識別情報と前記第 1 アドレスとが対応づけられた第 1 通信情報を取得する第 1 通信情報取得段階と、

前記第 2 格納装置が格納する前記第 1 アドレスと前記第 2 アドレスとが対応づけられた第 2 通信情報を取得する第 2 通信情報取得段階と、

指定された前記第 2 アドレスに対応づけられた前記第 1 アドレスを前記第 3 通信情報に基づいて検出し、当該第 1 アドレスに対応づけられた前記端末識別情報を前記第 2 通信情報に基づいて検出するユーザ端末検出段階とを備えることを特徴とするユーザ特定方法。

【請求項 1 3】

第 1 アドレス体系の第 1 ネットワークに配置されたユーザ端末の端末識別情報と当該端末識別情報に対して割り当てられた前記第 1 アドレス体系の第 1 アドレスとを対応づけて格納する第 1 格納装置と、第 1 アドレスと当該第 1 アドレスに対して割り当てられた第 2 アドレス体系の第 2 アドレスとを対応づけて格納する第 2 格納装置とを備えるユーザ特定システムの、前記第 1 格納装置及び前記第 2 格納装置が格納する通信情報に基づいて、前記第 2 アドレス体系の第 2 ネットワークにおける通信を行った前記ユーザ端末のユーザを特定するユーザ特定装置用のプログラムであって、

ユーザ特定装置を、

前記第 1 格納装置が格納する前記端末識別情報と前記第 1 アドレスとが対応づけられた第 1 通信情報を取得する第 1 通信情報取得部、

前記第 2 格納装置が格納する前記第 1 アドレスと前記第 2 アドレスとが対応づけられた第 2 通信情報を取得する第 2 通信情報取得部、

指定された前記第 2 アドレスに対応づけられた前記第 1 アドレスを前記第 3 通信情報に基づいて検出し、当該第 1 アドレスに対応づけられた前記端末識別情報を前記第 2 通信情報に基づいて検出するユーザ端末検出部として機能させることを特徴とするプログラム。

【請求項 1 4】

第 1 アドレス体系の第 1 ネットワークに配置され、第 2 アドレス体系の第 2 ネットワークにおける通信を行ったユーザ端末のユーザを特定するユーザ特定システムであって、

前記第 1 アドレス体系の第 1 アドレスと前記第 2 アドレス体系の第 2 アドレスとを相互に変換して、前記第 1 ネットワークと前記第 2 ネットワークとの間で通信を中継するアドレス変換装置と、

前記アドレス変換装置が生成するユーザ特定情報に基づいて、前記第 2 ネットワークにおける通信を行った前記ユーザ端末のユーザを特定するユーザ特定装置とを備え、

前記アドレス変換装置は、

前記ユーザ端末の端末識別情報と当該端末識別情報に対して割り当てられた前記第 1 アドレス体系の第 1 アドレスとが対応づけられた第 1 通信情報を格納する第 1 通信情報格納部と、

第 1 アドレスと当該第 1 アドレスに対して割り当てられた第 2 アドレス体系の第 2 アドレスとが対応づけられた第 2 通信情報を格納する第 2 通信情報格納部と、

前記第 1 通信情報及び前記第 2 通信情報に基づいて、前記第 2 アドレスと当該第 2 アド

10

20

30

40

50

レスを用いて前記第２ネットワークにおける通信を行った前記ユーザ端末の前記端末識別情報とが対応づけられた前記ユーザ特定情報を生成するユーザ特定情報生成部とを有することを特徴とするユーザ特定システム。

【請求項１５】

前記第１ネットワークに配置され、複数の前記ユーザ端末がそれぞれ接続された複数の物理ポートを有し、前記物理ポートと当該物理ポートに接続された前記ユーザ端末の端末識別情報とを対応づけて格納する第３格納装置をさらに備え、

前記アドレス変換装置は、前記第３格納装置が格納する前記物理ポートと当該物理ポートに接続された前記ユーザ端末の端末識別情報とが対応づけられた第３通信情報を取得する第３通信情報取得部をさらに有し、

10

前記ユーザ特定情報生成部は、前記第１通信情報、前記第２通信情報、及び前記第３通信情報に基づいて、前記第２アドレスと当該第２アドレスを用いて前記第２ネットワークにおける通信を行った前記ユーザ端末が接続された前記物理ポートとが対応づけられた前記ユーザ特定情報を生成することを特徴とする請求項１４に記載のユーザ特定システム。

【請求項１６】

第１アドレス体系の第１アドレスと第２アドレス体系の第２アドレスとを相互に変換して、前記第１アドレス体系の第１ネットワークと前記第２アドレス体系の第２ネットワークとの間で通信を中継するアドレス変換装置であって、

前記第１ネットワークに配置されたユーザ端末の端末識別情報と当該端末識別情報に対して割り当てられた前記第１アドレスとが対応づけられた第１通信情報を格納する第１通信情報格納部と、

20

前記第１アドレスに対して前記第２アドレスを割り当てるアドレス変換部と、

前記第１アドレスと当該第１アドレスに対して割り当てられた第２アドレスとが対応づけられた第２通信情報を格納する第２通信情報格納部と、

前記第１通信情報及び前記第２通信情報に基づいて、前記第２アドレスと当該第２アドレスを用いて前記第２ネットワークにおける通信を行った前記ユーザ端末の前記端末識別情報とが対応づけられたユーザ特定情報を生成するユーザ特定情報生成部とを備えることを特徴とするアドレス変換装置。

【発明の詳細な説明】

【技術分野】

30

本発明は、ユーザ特定システム、ユーザ特定装置、ユーザ特定方法、アドレス変換装置、及びプログラムに関する。特に本発明は、アドレス体系の異なる２つのネットワークを介して通信を行ったユーザ端末のユーザを特定するためのユーザ特定システム、ユーザ特定装置、ユーザ特定方法、アドレス変換装置、及びプログラムに関する。また本出願は、下記の日本特許出願に関連する。文献の参照による組み込みが認められる指定国については、下記の出願に記載された内容を参照により本出願に組み込み、本出願の記載の一部とする。

PCT/JPO2/12795

出願日 2002年12月5日

【背景技術】

近年のインターネットの急速な膨張に伴い、ホームページや電子掲示板における名誉毀損、著作権侵害、プライバシー侵害等の不法行為等の問題が数多く指摘されるようになっている。そのため、近時、「特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律」が施行された。この法律は、特定電気通信による情報の流通によって権利の侵害があった場合について、特定電気通信役務提供者（プロバイダ、サーバの管理者等）の損害賠償責任の制限及び発信者情報の開示を請求する権利について定め、特定電気通信による情報の流通により自己の権利を侵害されたとする者が、関係するプロバイダ等に対し、当該プロバイダ等が保有する発信者の情報の開示を請求できる規定を設けている。そのため、プロバイダは、発信者の情報の開示の請求に対応するため、自己の権利を侵害されたとする者から提供された情報、例えば発信者のＩＰアドレスに基づいて発信者を特定できることが望ましい。

40

50

しかしながら、複数のユーザが同一のＩＰアドレスを用いてインターネット上で通信を行う、インターネットマンション等のサービスを提供するプロバイダでは、発信者のＩＰアドレスに基づいてユーザを特定することが困難であり、発信者の情報の開示の請求に迅速に対応することができないという問題がある。

そこで本発明は、上記の課題を解決することのできるユーザ特定システム、ユーザ特定装置、ユーザ特定方法、アドレス変換装置、及びプログラムを提供することを目的とする。この目的は請求の範囲における独立項に記載の特徴の組み合わせにより達成される。また従属項は本発明の更なる有利な具体例を規定する。

【発明の開示】

このような目的を達成するために、本発明の第１の形態によれば、第１アドレス体系の第１ネットワークに配置され、第２アドレス体系の第２ネットワークにおける通信を行ったユーザ端末のユーザを特定するユーザ特定システムであって、ユーザ端末の端末識別情報と当該端末識別情報に対して割り当てられた第１アドレス体系の第１アドレスとを対応づけて格納する第１格納装置と、第１アドレスと当該第１アドレスに対して割り当てられた第２アドレス体系の第２アドレスとを対応づけて格納する第２格納装置と、第１格納装置及び第２格納装置が格納する通信情報に基づいて、第２ネットワークにおける通信を行ったユーザ端末のユーザを特定するユーザ特定装置とを備える。

ユーザ特定装置は、第１格納装置が格納する端末識別情報と第１アドレスとが対応づけられた第１通信情報を取得する第１通信情報取得部と、第２格納装置が格納する第１アドレスと第２アドレスとが対応づけられた第２通信情報を取得する第２通信情報取得部と、指定された第２アドレスに対応づけられた第１アドレスを第２通信情報に基づいて検出し、当該第１アドレスに対応づけられた端末識別情報を第１通信情報に基づいて検出するユーザ端末検出部とを有する。

第１格納装置は、端末識別情報であるＭＡＣアドレスに対して第１アドレスであるプライベートＩＰアドレスを割り当てるＤＨＣＰサーバであり、ＭＡＣアドレスに対してプライベートＩＰアドレスを割り当てた場合に、ユーザ特定装置に対して第１通信情報を送信してもよい。

第１格納装置は、端末識別情報であるＭＡＣアドレスと当該ＭＡＣアドレスに対して割り当てられた第１アドレスであるプライベートＩＰアドレスとを対応づけて格納するＡＲＰテーブルを有するＡＲＰサーバであり、ユーザ端末からＡＲＰリクエストを受信した場合に、ユーザ特定装置に対して第１通信情報を送信してもよい。

第２格納装置は、第１ネットワークと第２ネットワークとを接続し、第１アドレスであるプライベートＩＰアドレスに対して第２アドレスであるグローバルＩＰアドレスを割り当てるアドレス変換サーバであり、プライベートＩＰアドレスに対してグローバルＩＰアドレスを割り当てた場合に、ユーザ特定装置に対して第２通信情報を送信してもよい。

第１ネットワークに配置され、複数のユーザ端末がそれぞれ接続された複数の物理ポートを有し、物理ポートと当該物理ポートに接続されたユーザ端末の端末識別情報とを対応づけて格納する第３格納装置をさらに備え、ユーザ特定装置は、第３格納装置が格納する物理ポートと端末識別情報とが対応づけられた第３通信情報を取得する第３通信情報取得部をさらに有し、ユーザ端末検出部は、指定された第２アドレスに対応づけられた第１アドレスを第２通信情報に基づいて検出し、当該第１アドレスに対応づけられた端末識別情報を第１通信情報に基づいて検出し、当該端末識別情報に対応づけられた物理ポートを第３通信情報に基づいて検出してもよい。

第３格納装置は、物理ポートと端末識別情報であるＭＡＣアドレスとを対応づけて格納するフォワーディングデータベースであり、フォワーディングデータベースを更新した場合に、ユーザ特定装置に対して第３通信情報を送信してもよい。

ユーザ端末が接続された中継機器の物理ポートに割り当てられたＶＬＡＮを識別するＶＬＡＮ識別情報と、当該物理ポートに接続されたユーザ端末の端末識別情報とを対応づけて格納する第３格納装置をさらに備え、ユーザ特定装置は、第３格納装置が格納するＶＬＡＮ識別情報と端末識別情報とが対応づけられた第３通信情報を取得する第３通信情報取

得部をさらに有し、ユーザ端末検出部は、指定された第2アドレスに対応づけられた第1アドレスを第2通信情報に基づいて検出し、当該第1アドレスに対応づけられた端末識別情報を第1通信情報に基づいて検出し、当該端末識別情報に対応づけられたVLAN識別情報を第3通信情報に基づいて検出してもよい。

また、本発明の第2の形態によれば、第1アドレス体系の第1ネットワークに配置され、第2アドレス体系の第2ネットワークにおける通信を行ったユーザ端末のユーザを特定するユーザ特定システムであって、ユーザ端末の端末識別情報と当該端末識別情報に対して割り当てられた第1アドレス体系の第1アドレスとを対応づけて格納する第1通信情報格納部、第1アドレスと当該第1アドレスに対して割り当てられた第2アドレス体系の第2アドレスとを対応づけて格納する第2通信情報格納部、及び第1通信情報格納部が格納する端末識別情報と第1アドレスとが対応づけられた第1通信情報、及び第2通信情報格納部が格納する第1アドレスと第2アドレスとが対応づけられた第2通信情報に基づいて、端末識別情報と第2アドレスとが対応づけられたユーザ特定情報を生成するユーザ特定情報生成部を有する中継機器と、第1ネットワークに配置され、複数のユーザ端末がそれぞれ接続された複数の物理ポートを有し、物理ポートと当該物理ポートに接続されたユーザ端末の端末識別情報とを対応づけて格納する第3格納装置と、第3格納装置が格納する通信情報、及び中継機器が生成したユーザ特定情報に基づいて、第2ネットワークにおける通信を行ったユーザ端末のユーザを特定するユーザ特定装置とを備える。

ユーザ特定装置は、第3格納装置が格納する物理ポートと端末識別情報とが対応づけられた第3通信情報を取得する第3通信情報取得部と、中継機器が格納する端末識別情報と第2アドレスとが対応づけられたユーザ特定情報を取得する第4通信情報取得部と、指定された第2アドレスに対応づけられた端末識別情報をユーザ特定情報に基づいて検出し、当該端末識別情報に対応づけられた物理ポートを第3通信情報に基づいて検出するユーザ端末検出部とを有する。

また、本発明の第3の形態によれば、第1アドレス体系の第1ネットワークに配置されたユーザ端末の端末識別情報と当該端末識別情報に対して割り当てられた第1アドレス体系の第1アドレスとを対応づけて格納する第1格納装置と、第1アドレスと当該第1アドレスに対して割り当てられた第2アドレス体系の第2アドレスとを対応づけて格納する第2格納装置とを備えるユーザ特定システムの、第1格納装置及び第2格納装置が格納する通信情報に基づいて、第2アドレス体系の第2ネットワークにおける通信を行ったユーザ端末のユーザを特定するユーザ特定装置であって、第1格納装置が格納する端末識別情報と第1アドレスとが対応づけられた第1通信情報を取得する第1通信情報取得部と、第2格納装置が格納する第1アドレスと第2アドレスとが対応づけられた第2通信情報を取得する第2通信情報取得部と、指定された第2アドレスに対応づけられた第1アドレスを第2通信情報に基づいて検出し、当該第1アドレスに対応づけられた端末識別情報を第1通信情報に基づいて検出するユーザ端末検出部とを備える。

第2通信情報取得部は、第1アドレス及び第2アドレスに、当該第2アドレスを送信元アドレスとするパケットの宛先アドレスが対応づけられた、第2格納装置が格納する第2通信情報を取得し、ユーザ端末検出部は、指定された第2アドレス及び宛先アドレスに基づいて第1アドレスを検出してもよい。

第1通信情報及び第2通信情報に対応づけて、第1通信情報及び第2通信情報を取得した時刻をそれぞれ格納する通信情報格納部をさらに備え、ユーザ端末検出部は、通信情報格納部が格納する時刻を参照して、指定された第2アドレスに対応づけられた第1アドレスを検出し、当該第1アドレスに対応づけられた端末識別情報を検出してもよい。

また、本発明の第4の形態によれば、第1アドレス体系の第1ネットワークに配置されたユーザ端末の端末識別情報と当該端末識別情報に対して割り当てられた第1アドレス体系の第1アドレスとを対応づけて格納する第1格納装置と、第1アドレスと当該第1アドレスに対して割り当てられた第2アドレス体系の第2アドレスとを対応づけて格納する第2格納装置とを備えるユーザ特定システムの、第1格納装置及び第2格納装置が格納する通信情報に基づいて、第2アドレス体系の第2ネットワークにおける通信を行ったユーザ

端末のユーザを特定するユーザ特定方法であって、第1格納装置が格納する端末識別情報と第1アドレスとが対応づけられた第1通信情報を取得する第1通信情報取得段階と、第2格納装置が格納する第1アドレスと第2アドレスとが対応づけられた第2通信情報を取得する第2通信情報取得段階と、指定された第2アドレスに対応づけられた第1アドレスを第3通信情報に基づいて検出し、当該第1アドレスに対応づけられた端末識別情報を第2通信情報に基づいて検出するユーザ端末検出段階とを備える。

また、本発明の第5の形態によれば、第1アドレス体系の第1ネットワークに配置されたユーザ端末の端末識別情報と当該端末識別情報に対して割り当てられた第1アドレス体系の第1アドレスとを対応づけて格納する第1格納装置と、第1アドレスと当該第1アドレスに対して割り当てられた第2アドレス体系の第2アドレスとを対応づけて格納する第2格納装置とを備えるユーザ特定システムの、第1格納装置及び第2格納装置が格納する通信情報に基づいて、第2アドレス体系の第2ネットワークにおける通信を行ったユーザ端末のユーザを特定するユーザ特定装置用のプログラムであって、ユーザ特定装置を、第1格納装置が格納する端末識別情報と第1アドレスとが対応づけられた第1通信情報を取得する第1通信情報取得部、第2格納装置が格納する第1アドレスと第2アドレスとが対応づけられた第2通信情報を取得する第2通信情報取得部、指定された第2アドレスに対応づけられた第1アドレスを第3通信情報に基づいて検出し、当該第1アドレスに対応づけられた端末識別情報を第2通信情報に基づいて検出するユーザ端末検出部として機能させる。

また、本発明の第5の形態によれば、第1アドレス体系の第1ネットワークに配置され、第2アドレス体系の第2ネットワークにおける通信を行ったユーザ端末のユーザを特定するユーザ特定システムであって、第1アドレス体系の第1アドレスと第2アドレス体系の第2アドレスとを相互に変換して、第1ネットワークと第2ネットワークとの間で通信を中継するアドレス変換装置と、アドレス変換装置が生成するユーザ特定情報に基づいて、第2ネットワークにおける通信を行ったユーザ端末のユーザを特定するユーザ特定装置とを備える。

アドレス変換装置は、ユーザ端末の端末識別情報と当該端末識別情報に対して割り当てられた第1アドレス体系の第1アドレスとが対応づけられた第1通信情報を格納する第1通信情報格納部と、第1アドレスと当該第1アドレスに対して割り当てられた第2アドレス体系の第2アドレスとが対応づけられた第2通信情報を格納する第2通信情報格納部と、第1通信情報及び第2通信情報に基づいて、第2アドレスと当該第2アドレスを用いて第2ネットワークにおける通信を行ったユーザ端末の端末識別情報とが対応づけられたユーザ特定情報を生成するユーザ特定情報生成部とを有する。

第1ネットワークに配置され、複数のユーザ端末がそれぞれ接続された複数の物理ポートを有し、物理ポートと当該物理ポートに接続されたユーザ端末の端末識別情報とを対応づけて格納する第3格納装置をさらに備え、アドレス変換装置は、第3格納装置が格納する物理ポートと当該物理ポートに接続されたユーザ端末の端末識別情報とが対応づけられた第3通信情報を取得する第3通信情報取得部をさらに有し、ユーザ特定情報生成部は、第1通信情報、第2通信情報、及び第3通信情報に基づいて、第2アドレスと当該第2アドレスを用いて第2ネットワークにおける通信を行ったユーザ端末が接続された物理ポートとが対応づけられたユーザ特定情報を生成してもよい。

また、本発明の第6の形態によれば、第1アドレス体系の第1アドレスと第2アドレス体系の第2アドレスとを相互に変換して、第1アドレス体系の第1ネットワークと第2アドレス体系の第2ネットワークとの間で通信を中継するアドレス変換装置であって、第1ネットワークに配置されたユーザ端末の端末識別情報と当該端末識別情報に対して割り当てられた第1アドレスとが対応づけられた第1通信情報を格納する第1通信情報格納部と、第1アドレスに対して第2アドレスを割り当てるアドレス変換部と、第1アドレスと当該第1アドレスに対して割り当てられた第2アドレスとが対応づけられた第2通信情報を格納する第2通信情報格納部と、第1通信情報及び第2通信情報に基づいて、第2アドレスと当該第2アドレスを用いて第2ネットワークにおける通信を行ったユーザ端末の端

末識別情報とが対応づけられたユーザ特定情報を生成するユーザ特定情報生成部とを備える。

なお上記の発明の概要は、本発明の必要な特徴の全てを列挙したものではなく、これらの特徴群のサブコンビネーションも又発明となりうる。

【図面の簡単な説明】

図 1 は、第 1 実施形態に係るユーザ特定システム 10 のシステム構成の一例を示す。

図 2 は、第 1 実施形態に係るユーザ特定装置 22 のブロック構成の一例を示す。

図 3 は、第 1 実施形態に係る通信情報格納部 108 のデータ構成の一例を示す。

図 4 は、第 1 実施形態に係るユーザ特定システム 10 のユーザ特定方法の一例を示す

。

図 5 は、第 1 実施形態に係るユーザ特定装置 22 のハードウェア構成の一例を示す。

図 6 は、第 2 実施形態に係るユーザ特定システム 30 の構成の一例を示す。

図 7 は、第 2 実施形態に係るルータ 32a のブロック構成の一例を示す。

図 8 は、第 2 実施形態に係るユーザ特定装置 34 のブロック構成の一例を示す。

【発明を実施するための最良の形態】

以下、発明の実施の形態を通じて本発明を説明するが、以下の実施形態は請求の範囲に係る発明を限定するものではなく、又実施形態の中で説明されている特徴の組み合わせの全てが発明の解決手段に必須であるとは限らない。

(第 1 実施形態)

図 1 は、本発明の第 1 実施形態に係るユーザ特定システム 10 のシステム構成の一例を示す。ユーザ特定システム 10 は、LAN (Local Area Network) 12a 又は 12b に配置され、複数のユーザ端末 14a ~ 14l がそれぞれ接続されたインテリジェントハブ 16a ~ 16d と、LAN 12a 及び 12b とインターネット 18 とを接続するルータ 20a 及び 20b と、インターネット 18 における通信を行ったユーザ端末のユーザ特定するユーザ特定装置 22 とを備える。なお、LAN 12a 及び 12b は、本発明の第 1 アドレス体系の第 1 ネットワークの一例であり、インターネット 18 は、本発明の第 2 アドレス体系の第 2 ネットワークの一例である。また、LAN 12a 及び 12b は、例えばインターネットマンション等の集合建築物内に構築され、インテリジェントハブ 16a ~ 16d の VLAN (Virtual LAN) 機能により、ユーザ端末間の通信が制限されている。なお、プライベート IP アドレスは、本発明の第 1 アドレス体系の第 1 アドレスの一例であり、グローバル IP アドレスは、本発明の第 2 アドレス体系の第 2 アドレスの一例である。また、本発明の第 2 アドレス体系の第 2 アドレスは、グローバル IP アドレス及びポート番号を含んでもよい。

ルータ 20a 及び 20b は、本発明の第 1 格納装置の一例であり、複数のユーザ端末の端末識別情報である MAC アドレスと、当該 MAC アドレスに対して割り当てられたプライベート IP アドレスとを対応づけて格納する。ルータ 20a 及び 20b は、DHCP サーバを有し、ユーザ端末の MAC アドレスに対して、プライベート IP アドレスの割り当て及び解放を行う。そして、ルータ 20a 及び 20b は、MAC アドレスとプライベート IP アドレスとを対応づけて、第 1 通信情報としてユーザ特定装置 22 に送信する。ルータ 20a 及び 20b は、例えば MAC アドレスに対してプライベート IP アドレスを割り当てた場合に第 1 通信情報をユーザ特定装置 22 に送信する。また、ルータ 20a 及び 20b は、例えばプライベート IP アドレスを解放した場合に第 1 通信情報をユーザ特定装置 22 に送信してもよい。

また、ルータ 20a 及び 20b は、ユーザ端末の MAC アドレスと、当該 MAC アドレスに対して割り当てられたプライベート IP アドレスとを対応づけて格納する ARP テーブルを含む ARP サーバを有する。そして、ルータ 20a 及び 20b は、MAC アドレスとプライベート IP アドレスとを対応づけて、第 1 通信情報としてユーザ特定装置 22 に送信する。ルータ 20a 及び 20b は、例えばユーザ端末から ARP リクエストを受信した場合に第 1 通信情報をユーザ特定装置 22 に送信する。また、ルータ 20a 及び 20b は、例えばユーザ端末に ARP リプライを返信した場合に第 1 通信情報をユーザ特定装置

10

20

30

40

50

22に送信してもよい。また、ルータ20a及び20bは、例えばSyslog Messageを用いて第1通信情報を送信してもよいし、SNMPのTrapを用いて第1通信情報を送信してもよい。

また、ルータ20a及び20bは、本発明の第2格納装置の一例であり、ユーザ端末に割り当てられたプライベートIPアドレスと、当該プライベートIPアドレスに割り当てられたグローバルIPアドレスを格納する。ルータ20a及び20bは、プライベートIPアドレスに対してグローバルIPアドレスを割り当てるアドレス変換装置を有し、受信したパケットのプライベートIPアドレスとグローバルIPアドレスとを相互に変換して、LAN12a又は12bとインターネット18との間で通信を中継する。そして、ルータ20a及び20bは、格納するプライベートIPアドレスとグローバルIPアドレスとを対応づけて、第2通信情報としてユーザ特定装置22に送信する。ルータ20a及び20bは、例えばプライベートIPアドレスに対してグローバルIPアドレスを割り当てた場合に第2通信情報をユーザ特定装置22に送信する。また、ルータ20a及び20bは、例えばSyslog Messageを用いて第2通信情報を送信してもよいし、SNMPのTrapを用いて第2通信情報を送信してもよい。

10

また、ルータ20a及び20bは、例えばグローバルIPアドレスを解放した場合に第2通信情報をユーザ特定装置22に送信してもよい。また、ルータ20a及び20bは、IPマスカレード機能を有する場合、ユーザ端末に割り当てられたプライベートIPアドレスと、当該プライベートIPアドレスに割り当てられたグローバルIPアドレス及びポート番号を格納し、プライベートIPアドレスとグローバルIPアドレス及びポート番号と対応づけて、第2通信情報としてユーザ特定装置22に送信してもよい。

20

また、ルータ20a及び20bは、プライベートIPアドレス及びグローバルIPアドレスに、当該グローバルIPアドレスを送信元アドレスとするパケットの宛先アドレスをさらに対応づけて、第2通信情報としてユーザ特定装置22に送信してもよい。ルータ20a及び20bは、例えばユーザ端末とインターネット18との通信を中継する場合に第2通信情報をユーザ特定装置22に送信してもよい。

インテリジェントハブ16a～16dは、本発明の第3格納装置及び中継器の一例であり、複数のユーザ端末14a～14lがそれぞれ接続された複数の物理ポートを有する。また、インテリジェントハブ16a及び16dは、物理ポートと、当該物理ポートに接続されたユーザ端末のMACアドレスとを対応づけて格納するフォワーディングデータベースを有する。そして、インテリジェントハブ16a～16dは、フォワーディングデータベースが格納する物理ポートとMACアドレスとを対応づけて、第3通信情報としてユーザ特定装置22に送信する。さらに、インテリジェントハブ16a～16dは、物理ポート及びMACアドレスに、当該インテリジェントハブの機器識別情報をさらに対応づけて、第3通信情報としてユーザ特定装置22に送信してもよい。

30

インテリジェントハブ16a～16dは、例えばフォワーディングデータベースを更新した場合に第3通信情報をユーザ特定装置22に送信する。また、インテリジェントハブ16a～16dは、例えばフォワーディングデータベースからMACアドレスを消去した場合に第3通信情報をユーザ特定装置22に送信してもよい。また、インテリジェントハブ16a～16dは、例えばSyslog Messageを用いて第3通信情報を送信してもよいし、SNMP(Simple Network Management Protocol)のTrapを用いて第3通信情報を送信してもよい。

40

また、インテリジェントハブ16a～16dの複数の物理ポートに対して複数のVLANがそれぞれ割り当てられている場合には、インテリジェントハブ16a～16dは、物理ポートに割り当てられたVLANを識別するVLAN識別情報と、当該物理ポートに接続されたユーザ端末のMACアドレスとを対応づけて格納しており、VLAN識別情報とMACアドレスとを対応づけて、第3通信情報としてユーザ特定装置22に送信してもよい。また、他の例においては、LAN12a若しくは12b又はインターネット18に設けられた、本発明の第3格納装置の一例であるRADIUSサーバ等の管理装置が、インテリジェントハブ16a～16dの複数の物理ポートに割り当てられたVLANを識別す

50

るVLAN識別情報と、当該物理ポートに接続されたユーザ端末のMACアドレスとを対応づけて格納しており、VLAN識別情報とMACアドレスとを対応づけて、第3通信情報としてユーザ特定装置22に送信してもよい。

ユーザ特定装置22は、ルータ20a及び20bが格納する第1通信情報及び第2通信情報に基づいて、インターネット18における通信を行ったユーザ端末のMACアドレスを検出し、当該MACアドレスに基づいてユーザ端末のユーザを特定する。また、ユーザ特定装置22は、ルータ20a及び20bが格納する第1通信情報及び第2通信情報、並びにインテリジェントハブ16a~16dが格納する第3通信情報に基づいて、インターネット18における通信を行ったユーザ端末が接続されるインテリジェントハブ16a~16dの物理ポート又はVLAN識別情報を検出し、当該物理ポート又は当該VLAN識別情報に基づいてユーザ端末のユーザを特定してもよい。なお、ユーザ特定装置22は、図1に示すようにインターネット18上に配置されてもよいし、またLAN12a又は12b内に配置されてもよい。

10

ルータ20a及び20bは、ユーザ端末14a~14lから受信したパケットの送信元IPアドレスを、ユーザ端末14a~14lに割り当てられたプライベートIPアドレスから、ルータ20a又は20bに割り当てられたグローバルIPアドレスに変換してインターネット18に送信する。そのため、ルータ20a又はルータ20bからインターネット18に送信されたパケットの送信元IPアドレスから、ユーザ端末14a~14lを特定することができない。しかしながら、このような場合において、ユーザ特定システム10は、インターネット18における通信を行ったユーザ端末のユーザを特定することを可能にする。

20

図2は、第1実施形態に係るユーザ特定装置22のブロック構成の一例を示す。ユーザ特定装置22は、インターネット18に対してデータの送受信を行う送受信部100と、ルータ20a及び20bが格納するMACアドレスとプライベートIPアドレスとが対応づけられた第1通信情報を送受信部100を介して取得する第1通信情報取得部102と、ルータ20a及び20bが格納するプライベートIPアドレスとグローバルIPアドレスとが対応づけられた第2通信情報を送受信部100を介して取得する第2通信情報取得部104と、インテリジェントハブ16a~16dが格納する物理ポート又はVLAN識別情報とMACアドレスと機器識別情報とが対応づけられた第3通信情報を送受信部100を介して取得する第3通信情報取得部106と、第1通信情報、第2通信情報、及び第3通信情報を格納する通信情報格納部108と、管理者によって指定されたグローバルIPアドレスを用いてインターネット18における通信を行ったユーザ端末のMACアドレス、又は当該ユーザ端末が接続された物理ポートを検出するユーザ端末検出部110とを備える。

30

なお、第1通信情報取得部102、第2通信情報取得部104、及び第3通信情報取得部106のそれぞれは、ルータ20a若しくは及び20b又はインテリジェントハブ16a~16dが送信する第1通信情報、第2通信情報、及び第3通信情報のそれぞれを受動的に取得してもよいし、送信要求パケットを送ることによって能動的にルータ20a若しくは及び20b又はインテリジェントハブ16a~16dから第1通信情報、第2通信情報、及び第3通信情報のそれぞれを取得してもよい。

40

ユーザ端末検出部110は、通信情報格納部108が格納する通信情報を参照して、管理者によって指定されたグローバルIPアドレスに対応づけられたプライベートIPアドレスを第2通信情報に基づいて検出し、当該プライベートIPアドレスに対応づけられたMACアドレスを第1通信情報に基づいて検出する。また、ユーザ端末検出部110は、管理者によって指定されたグローバルIPアドレスに対応づけられたプライベートIPアドレスを第2通信情報に基づいて検出し、当該プライベートIPアドレスに対応づけられたMACアドレスを第1通信情報に基づいて検出し、当該MACアドレスに対応づけられた機器識別情報、及び物理ポート又はVLAN識別情報を第3通信情報に基づいて検出してもよい。そして、ユーザ特定装置22は、ユーザ端末検出部110によって検出されたMACアドレスを有するユーザ端末、ユーザ端末検出部110によって検出された物理ポ

50

ートを介して通信を行うユーザ端末、又はユーザ端末検出部110によって検出されたVLAN識別情報で識別されるVLANに属するユーザ端末のユーザを特定する。

図3は、第1実施形態に係る通信情報格納部108のデータ構成の一例を示す。通信情報格納部108は、第1通信情報、第2通信情報、及び第3通信情報に対応づけて、第1通信情報、第2通信情報、及び第3通信情報をインテリジェントハブ16a~16d又はルータ20a若しくは20bから取得した時刻を格納する。

第1行(L1)は、第3通信情報取得部106がインテリジェントハブのフォワーディングデータベース(FDB)から取得した第3通信情報である。通信情報格納部108は、時刻「2003 Sep 1 23:50:23」と、ルータのグローバルIPアドレス「218.47.62.aaa」と、インテリジェントハブの機器識別情報「System Name」と、物理ポート「Port1」と、VLAN識別情報「V200」と、ユーザ端末のMACアドレス「00-90-99-48-85-**」とが対応づけられた第3通信情報を格納する。

10

第2行(L2)及び第3行(L3)は、第1通信情報取得部102がルータが有するDHCPサーバから取得した第1通信情報である。通信情報格納部108は、第2行(L2)に示すように、時刻「2003 Sep 1 23:50:34」と、ルータのグローバルIPアドレス「218.47.62.aaa」と、プライベートIPアドレス「192.168.1.100」と、MACアドレス「00-90-99-48-85-**」とが対応づけられた第1通信情報を格納する。当該第1通信情報は、時刻「2003 Sep 1 23:50:34」にMACアドレス「00-90-99-48-85-**」に割り当てられていたプライベートIPアドレス「192.168.1.100」が解放されたことを示す。また、通信情報格納部108は、第3行(L3)に示すように、時刻「2003 Sep 1 23:50:38」と、ルータのグローバルIPアドレス「218.47.62.aaa」と、プライベートIPアドレス「192.168.1.100」と、MACアドレス「00-90-99-48-85-**」とが対応づけられた第1通信情報を格納する。当該第1通信情報は、時刻「2003 Sep 1 23:50:34」にMACアドレス「00-90-99-48-85-**」に対してプライベートIPアドレス「192.168.1.100」を割り当てたことを示す。

20

第4行(L4)は、第1通信情報取得部102がルータが有するARPテーブルから取得した第1通信情報である。通信情報格納部108は、時刻「2003 Sep 1 23:50:55」と、ルータのグローバルIPアドレス「218.47.62.aaa」と、MACアドレス「00-90-99-48-85-**」と、プライベートIPアドレス「192.168.1.100」とが対応づけられた第1通信情報を格納する。当該第1通信情報は、時刻「2003 Sep 1 23:50:55」にMACアドレス「00-90-99-48-85-**」とプライベートIPアドレス「192.168.1.100」との組み合わせがARPテーブルに追加されたことを示す。

30

第5行(L5)は、第2通信情報取得部104がルータが有するアドレス変換装置の一例であるFirewallサーバから取得した第2通信情報である。通信情報格納部108は、時刻「2003 Sep 1 23:51:12」と、ルータのグローバルIPアドレス「218.47.62.aaa」と、プライベートIPアドレス及びポート番号「192.168.1.100:1031」と、パケットの宛先アドレスであるグローバルIPアドレス及びポート番号「210.153.1.bbb:53」とが対応づけられた第2通信情報を格納する。当該第2通信情報は、時刻「2003 Sep 1 23:51:12」に、プライベートIPアドレス「192.168.1.100」が割り当てられたユーザ端末がグローバルIPアドレス「210.153.1.bbb」の通信機器に対してUDPによりパケットを送信したことを示す。第6行(L6)~第11行(L11)は、第5行(L5)と同様の第2通信情報である。

40

例えば、管理者によってグローバルIPアドレス「218.47.62.aaa」、宛先アドレス「210.153.1.bbb」、及び時刻が指定された場合、ユーザ端末検出部110は、通信情報格納部108が格納する時刻を参照して、グローバルIPアドレ

50

ス「218.47.62.aaa」及び宛先アドレス「210.153.1.bbb」に対応づけられたプライベートIPアドレス「192.168.1.100」を第7行(L7)の第2通信情報に基づいて検出する。そして、ユーザ端末検出部110は、プライベートIPアドレス「192.168.1.100」に対応づけられたMACアドレス「00-90-99-48-85-**」を第4行(L4)の第1通信情報に基づいて検出する。さらに、ユーザ端末検出部110は、MACアドレス「00-90-99-48-85-**」に対応づけられた機器識別情報「System Name」、及び物理ポート「Port1」又はVLAN識別情報「V200」を第1行(L1)の第3通信情報に基づいて検出してもよい。

以上のように、通信情報格納部108が第1通信情報及び第2通信情報を時刻に対応づけて格納し、ユーザ端末検出部110が時刻を参照してユーザ端末のMACアドレスの検出を行うことにより、ユーザ端末のMACアドレスを正確に検出することができ、ユーザを正確に特定することができる。また、通信情報格納部108がさらに第3通信情報を時刻に対応づけて格納し、ユーザ端末検出部110が時刻を参照して物理ポート又はVLAN識別情報の検出を行うことにより、ユーザ端末が接続された物理ポートを正確に検出することができ、ユーザを正確に特定することができる。

図4は、第1実施形態に係るユーザ特定システム10のユーザ特定方法の一例を示す。ユーザ端末14aは、電源が投入されて起動すると、DHCP Requestをルータ20aのDHCPサーバに送信する(S100)。インテリジェントハブ16aは、ユーザ端末14aとルータ20aとの間でDHCP Requestを中継する場合に、フォワーディングデータベースを更新し、ユーザ端末14aが接続された物理ポートとユーザ端末14aのMACアドレスとが対応づけられた第3通信情報を含むSyslog Message #1をユーザ特定装置22に送信する(S102)。これにより、ユーザ特定装置22の第3通信情報取得部106は、第3通信情報をインテリジェントハブ16aから取得する。

次に、ルータ20aのDHCPサーバは、ユーザ端末14aのMACアドレスに対してプライベートIPアドレスを割り当て、DHCP Ackをユーザ端末14aに送信する(S104)。そして、ルータ20aは、ユーザ端末14aのMACアドレスと、当該MACアドレスに割り当てられたプライベートIPアドレスとが対応づけられた第1通信情報を含むSyslog Message #2をユーザ特定装置22に送信する(S106)。これにより、ユーザ特定装置22の第1通信情報取得部102は、第1通信情報をルータ20aから取得する。

次に、ユーザ端末14aは、ARP Requestをルータ20aのARPサーバに送信する(S108)。そして、ルータ20aのARPサーバは、ARPテーブルを参照して、ARP Replyをユーザ端末14aに送信する(S110)。そして、ルータ20aは、ARPテーブルに格納されたユーザ端末14aのMACアドレスとプライベートIPアドレスとが対応づけられた第1通信情報を含むSyslog Message #3をユーザ特定装置22に送信する(S112)。これにより、ユーザ特定装置22の第1通信情報取得部102は、第1通信情報をルータ20aから取得する。

次に、ユーザ端末14aは、TCP/IP通信によりインターネット18で通信を行う(S114)。ルータ20aのFirewallサーバは、ユーザ端末14aとインターネット18との間の通信を中継する場合、ユーザ端末14aのプライベートIPアドレスに対してグローバルIPアドレスを割り当てる。そして、ルータ20aは、ユーザ端末14aのプライベートIPアドレスと、当該プライベートIPアドレスに割り当てられたグローバルIPアドレスとが対応づけられた第2通信情報を含むSyslog Message #4をユーザ特定装置22に送信する(S116)。

そして、ユーザ特定装置22のユーザ端末検出部110は、ルータ20aから取得した第1通信情報及び第2通信情報に基づいて、インターネット18における通信を行ったユーザ端末14aのMACアドレスを検出し、MACアドレスに基づいてユーザ端末14aのユーザを特定する。また、ユーザ特定装置22のユーザ端末検出部110は、インテリ

10

20

30

40

50

ジェントハブ 16 a から取得した第 3 通信情報、並びにルータ 20 a から取得した第 1 通信情報及び第 2 通信情報に基づいて、インターネット 18 における通信を行ったユーザ端末 14 a が接続されるインテリジェントハブ 16 a の物理ポートを検出し、物理ポートに基づいてユーザ端末 14 a のユーザを特定してもよい。

図 5 は、第 1 実施形態に係るユーザ特定装置 22 のハードウェア構成の一例を示す。ユーザ特定装置 22 は、CPU 700、ROM 702、RAM 704、通信インタフェース 706、ハードディスクドライブ 708、データベースインタフェース 710、フレキシブルディスクドライブ 712、及び CD-ROM ドライブ 714 を備える。CPU 700 は、ROM 702 及び RAM 704 に格納されたプログラムに基づいて動作し、各部の制御を行う。通信インタフェース 706 は、インターネット 18 に対して通信を行う。データベースインタフェース 710 は、データベースへのデータの書込、及びデータベースの内容の更新を行う。

10

フレキシブルディスクドライブ 712 は、フレキシブルディスク 720 からデータ又はプログラムを読み取り CPU 700 に提供する。CD-ROM ドライブ 714 は、CD-ROM 722 からデータ又はプログラムを読み取り CPU 700 に提供する。データベースインタフェース 710 は、各種データベース 724 と接続してデータを送受信する。

ユーザ特定装置 22 に提供されるプログラムは、フレキシブルディスク 720 又は CD-ROM 722 等の記録媒体に格納されて利用者によって提供される。記録媒体に格納されたプログラムは圧縮されていても非圧縮であってもよい。プログラムは記録媒体から読み出され、CPU 700 により実行される。

20

記録媒体に格納されて提供されるプログラム、即ちユーザ特定装置 22 にインストールされるプログラムは、機能構成として、送受信モジュール、第 1 通信情報取得モジュール、第 2 通信情報取得モジュール、第 3 通信情報取得モジュール、通信情報格納モジュール、及びユーザ端末検出モジュールを有する。各モジュールがユーザ特定装置 22 に働きかけて行わせる動作は、図 1 から図 4 において説明したユーザ特定装置 22 における、対応する部材の動作と同一であるから、説明を省略する。

記録媒体の一例としてのフレキシブルディスク 720 又は CD-ROM 722 には、本出願で説明する全ての実施形態におけるユーザ特定装置 22 の動作の一部又は全ての機能を格納することができる。

これらのプログラムは記録媒体から直接 RAM 704 に読み出されて実行されても、一旦ハードディスクにインストールされた後に RAM に読み出されて実行されてもよい。更に、上記プログラムは単一の記録媒体に格納されても複数の記録媒体に格納されてもよい。また、暗号化、圧縮等により符号化された形態で格納されていてもよい。

30

記録媒体としては、フレキシブルディスク、CD-ROM の他にも、DVD、PD 等の光学記録媒体、MD 等の光磁気記録媒体、テープ媒体、磁気記録媒体、IC カードやミニチュアカードなどの半導体メモリ等を用いることができる。また、専用通信ネットワークやインターネットに接続されたサーバシステムに設けたハードディスク又は RAM 等の格納装置を記録媒体として使用し、通信網を介してプログラムをユーザ特定装置 22 に提供してもよい。

なお、第 1 実施形態においては、ルータ 20 a とインテリジェントハブ 16 a 及び 16 b とが別個に設けられ、ルータ 20 b とインテリジェントハブ 16 c 及び 16 d とが別個に設けられているが、ルータ 20 a とインテリジェントハブ 16 a 及び 16 b とが一体となって、ルータ 20 a がインテリジェントハブ 16 a 及び 16 b の機能を有し、ルータ 20 b とインテリジェントハブ 16 c 及び 16 d とが一体となって、ルータ 20 b がインテリジェントハブ 16 c 及び 16 d の機能を有してもよい。即ち、本発明に係る第 1 格納装置、第 2 格納装置、及び第 3 格納装置は、同一筐体内に設けられた 1 個の機器であってもよい。

40

また、第 1 実施形態において、ユーザ特定システム 10 は、インテリジェントハブ 16 a ~ 16 d を備えるが、インテリジェントハブ 16 a ~ 16 d に換えて、フォワーディングデータベースを有しないリピータハブを備えてもよい。この場合、ユーザ特定装置 22

50

は、物理ポートとMACアドレスとが対応づけられた第3通信情報を取得することができないので、ユーザ端末14aが接続される物理ポートを検出することができないが、ルータ20aから取得した第1通信情報及び第2通信情報に基づいて、ユーザ端末14aのMACアドレスを検出し、ユーザ端末14aのユーザを特定することができる。

(第2実施形態)

図6は、本発明の第2実施形態に係るユーザ特定システム30の構成の一例を示す。第2実施形態において、以下に説明する部分を除き、第1実施形態と同一であってよい。

ユーザ特定システム30は、LAN12a又は12bに配置され、複数のユーザ端末14a~14lがそれぞれ接続されたインテリジェントハブ16a~16dと、LAN12a及び12bとインターネット18とを接続するルータ32a及び32bと、インターネット18における通信を行ったユーザ端末のユーザ特定するユーザ特定装置34とを備える。

ルータ32a及び32bは、本発明のアドレス変換装置及び中継機器の一例であり、プライベートIPアドレスとグローバルIPアドレスとを相互に変換して、LAN12a及び12bとインターネット18との間で通信を中継する。ルータ32a及び32bは、第1通信情報及び第2通信情報に基づいて、グローバルIPアドレスと、当該グローバルIPアドレスを用いてインターネット18における通信を行ったユーザ端末のMACアドレスとが対応づけられたユーザ特定情報を生成して、ユーザ特定装置34に供給する。また、ルータ32a及び32bは、第1通信情報、第2通信情報、及び第3通信情報に基づいて、グローバルIPアドレスと、当該グローバルIPアドレスを用いてインターネット18における通信を行ったユーザ端末が接続されたインテリジェントハブの物理ポートとが対応づけられたユーザ特定情報を生成して、ユーザ特定装置34に供給してもよい。ユーザ特定装置34は、ルータ32a又は32bからユーザ特定情報を取得し、ユーザ特定情報に基づいて、管理者によって指定されたグローバルIPアドレスに対応づけられたユーザ端末のMACアドレスを検出し、第3通信情報に基づいて、当該MACアドレスを有するユーザ端末のユーザを特定する。また、ユーザ特定装置34は、ルータ32a又は32bからユーザ特定情報を取得し、ユーザ特定情報に基づいて、管理者によって指定されたグローバルIPアドレスに対応づけられたインテリジェントハブの物理ポートを検出し、当該物理ポートに接続されたユーザ端末のユーザを特定してもよい。

図7は、第2実施形態に係るルータ32aのブロック構成の一例を示す。ルータ32aは、インターネット18に対してデータの送受信を行う外部送受信部200と、LAN12aに対してデータの送受信を行う内部送受信部202と、ユーザ端末のプライベートIPアドレスに対してグローバルIPアドレスを割り当て、外部送受信部200と内部送受信部202との間で、受信したパケットのプライベートIPアドレスとグローバルIPアドレスとを相互に変換するアドレス変換部204と、第1通信情報を格納する第1通信情報格納部208と、第2通信情報を格納する第2通信情報格納部210と、インテリジェントハブ16a及び16bから第3通信情報を取得する第3通信情報取得部206と、少なくとも第1通信情報及び第2通信情報に基づいて、ユーザ特定情報を生成するユーザ特定情報生成部212とを備える。

第3通信情報取得部206は、物理ポートとMACアドレスと機器識別情報とが対応づけられた第3通信情報を内部送受信部202を介してインテリジェントハブ16a及び16bから取得する。

第1通信情報格納部208は、例えばDHCPサーバであり、ユーザ端末のMACアドレスに対して、プライベートIPアドレスの割り当て及び解放を行う。そして、第1通信情報格納部208は、ユーザ端末のMACアドレスと、当該MACアドレスに対して割り当てられたプライベートIPアドレスとを対応づけて格納する。また、第1通信情報格納部208は、ユーザ端末のMACアドレスと、当該MACアドレスに対して割り当てられたプライベートIPアドレスとを対応づけて格納するARPテーブルを含むARPサーバであってもよい。

第2通信情報格納部210は、アドレス変換部204のアドレス変換テーブルであり、

ユーザ端末に割り当てられたプライベートIPアドレスと、当該プライベートIPアドレスに割り当てられたグローバルIPアドレスを格納する。

ユーザ特定情報生成部212は、第1通信情報及び第2通信情報に基づいて、グローバルIPアドレスと、当該グローバルIPアドレスを用いてインターネット18における通信を行ったユーザ端末のMACアドレスとが対応づけられたユーザ特定情報を生成する。また、ユーザ特定情報生成部212は、第1通信情報、第2通信情報、及び第3通信情報に基づいて、グローバルIPアドレスと、当該グローバルIPアドレスを用いてインターネット18における通信を行ったユーザ端末が接続されたインテリジェントハブの物理ポートとが対応づけられたユーザ特定情報を生成してもよい。そして、ユーザ特定情報生成部212は、生成したユーザ特定情報を外部送受信部200を介してユーザ特定装置34

10

図8は、第2実施形態に係るユーザ特定装置34のブロック構成の一例を示す。ユーザ特定装置34は、インターネット18に対してデータの送受信を行う送受信部300と、ルータ32a又は32bが生成したユーザ特定情報を送受信部300を介して取得する第4通信情報取得部302と、インテリジェントハブ16a～16dが格納する物理ポートとMACアドレスと機器識別情報とが対応づけられた第3通信情報を送受信部100を介して取得する第3通信情報取得部306と、ユーザ特定情報及び第3通信情報を格納する通信情報格納部308と、管理者によって指定されたグローバルIPアドレスを用いてインターネット18における通信を行ったユーザ端末のMACアドレス、又は当該ユーザ端末が接続された物理ポートを検出するユーザ端末検出部310とを備える。

20

ユーザ端末検出部310は、通信情報格納部308を参照して、管理者によって指定されたグローバルIPアドレスに対応づけられたMACアドレスをユーザ特定情報に基づいて検出し、当該MACアドレスに対応づけられた機器識別情報及び物理ポートを第3通信情報に基づいて検出する。また、ユーザ端末検出部310は、通信情報格納部308を参照して、管理者によって指定されたグローバルIPアドレスに対応づけられた機器識別情報及び物理ポートをユーザ特定情報に基づいて検出してもよい。そして、ユーザ特定装置34は、ユーザ端末検出部310によって検出されたMACアドレスを有するユーザ端末、又はユーザ端末検出部110によって検出された物理ポートを介して通信を行うユーザ端末のユーザを特定する。

第2実施形態のユーザ特定システム30によれば、ルータ32a及び32bが第1通信情報及び第2通信情報、又は第1通信情報、第2通信情報、及び第3通信情報からユーザ特定情報を生成してユーザ特定装置34に送信するので、ルータ32a及び32bからユーザ特定装置34へ送信されるデータの量を低減させることができる。また、ユーザ特定装置34が多数のLANを管理する場合に、管理するデータの量を低減させることができ、ユーザ特定装置34の記録資源を効率的に利用することができる。

30

以上発明の実施の形態を説明したが、本出願に係る発明の技術的範囲は上記の実施の形態に限定されるものではない。上記実施の形態に種々の変更を加えて、請求の範囲に記載の発明を実施することができる。そのような発明が本出願に係る発明の技術的範囲に属することもまた請求の範囲の記載から明らかである。

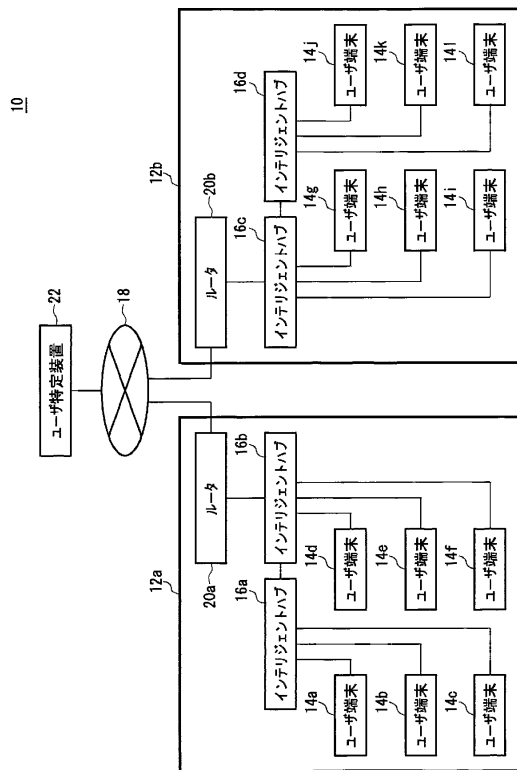
【産業上の利用可能性】

40

以上の説明から明らかなように、本発明によれば、プライベートIPアドレスとグローバルIPアドレスとを相互に変換するルータを介してインターネットにおける通信を行ったユーザ端末のユーザを特定することができる。

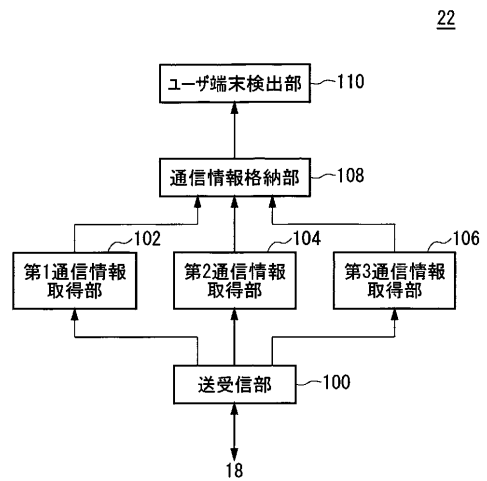
【図 1】

図 1



【図 2】

図 2



22

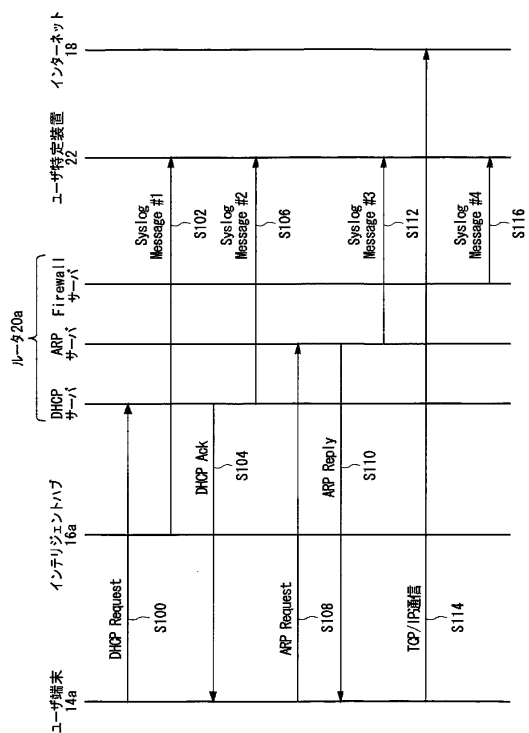
【図 3】

図 3

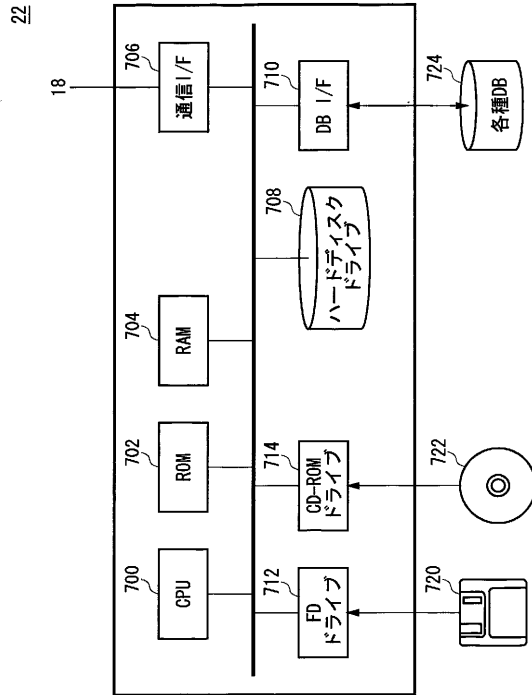
L1	2003 Sep 1 23:50:23 218.47.62.aaa FDB: New Address - System Name Port1 V200 00-90-99-48-85-**-
L2	2003 Sep 1 23:50:34 218.47.62.aaa DHCP:00027/00002, IP address 192.168.1.100 Freed by 00-90-99-48-85-**-
L3	2003 Sep 1 23:50:38 218.47.62.aaa DHCP:00027/00001, IP address 192.168.1.100 bound to 00-90-99-48-85-**-
L4	2003 Sep 1 23:50:55 218.47.62.aaa ARP: New Table - eth0 add 00-90-99-48-85-90(192.168.1.100)
L5	2003 Sep 1 23:51:12 218.47.62.aaa FIREWALL:FIRE/OUTAUDP, UDP 192.168.1.100:1031 210.153.1.bbb:53
L6	2003 Sep 1 23:51:12 218.47.62.aaa FIREWALL:FIRE/OUTAUDP, UDP 192.168.1.100:1031 210.153.1.ccc:53
L7	2003 Sep 1 23:51:12 218.47.62.aaa FIREWALL:FIRE/OUTATOP, TCP 192.168.1.100:1032 202.247.127.ddd:80
L8	2003 Sep 1 23:51:12 218.47.62.aaa FIREWALL:FIRE/OUTATOP, TCP 192.168.1.100:1033 202.247.127.ddd:80
L9	2003 Sep 1 23:51:50 218.47.62.aaa FIREWALL:FIRE/OUTAUDP, TCP 192.168.1.100:1034 210.153.1.bbb:53
L10	2003 Sep 1 23:51:50 218.47.62.aaa FIREWALL:FIRE/OUTAUDP, TCP 192.168.1.100:1034 210.153.1.ccc:53
L11	2003 Sep 1 23:51:50 218.47.62.aaa FIREWALL:FIRE/OUTATOP, TCP 192.168.1.100:1035 216.239.33.eee:80
	⋮

【図 4】

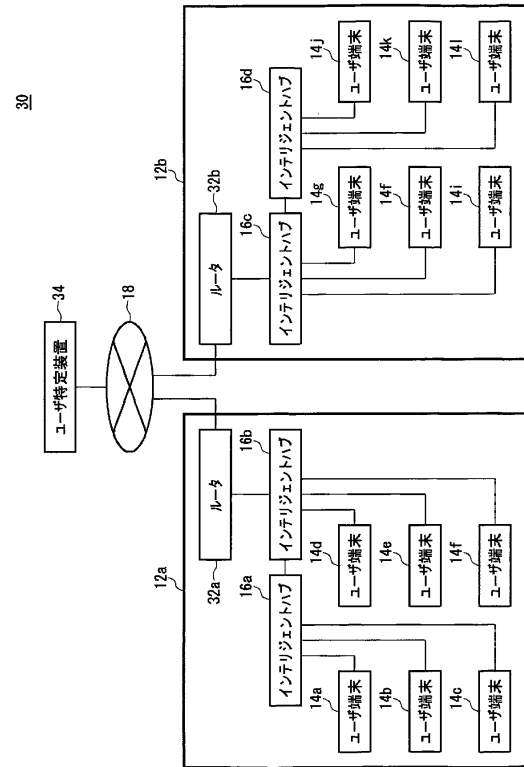
図 4



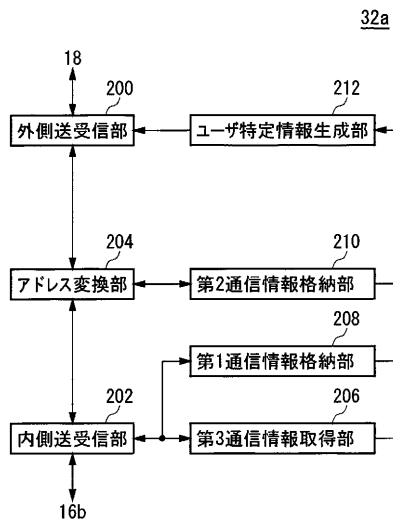
【図 5】
図 5



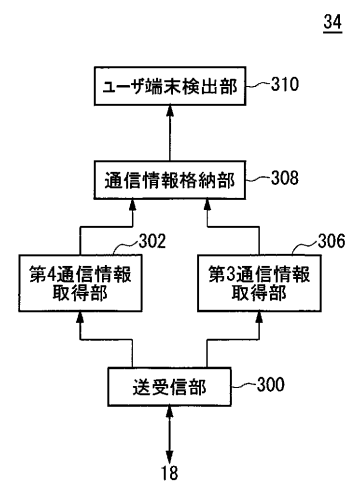
【図 6】
図 6



【図 7】
図 7



【図 8】
図 8



フロントページの続き

(56)参考文献 特開 2 0 0 1 - 1 2 7 7 7 0 (J P , A)
特開平 1 1 - 1 4 6 0 0 3 (J P , A)
特開平 1 1 - 2 6 1 5 8 3 (J P , A)

(58)調査した分野(Int.Cl. , D B 名)
H04L 12/28-46