

(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
2024年1月11日(11.01.2024)



(10) 国際公開番号

WO 2024/009441 A1

(51) 国際特許分類:
G06F 21/44 (2013.01)

(21) 国際出願番号: PCT/JP2022/026872

(22) 国際出願日: 2022年7月6日(06.07.2022)

(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: 日本電信電話株式会社 (NIPPON TELEGRAPH AND TELEPHONE CORPORATION) [JP/JP]; 〒1008116 東京都千代田区大手町一丁目5番1号 Tokyo (JP).

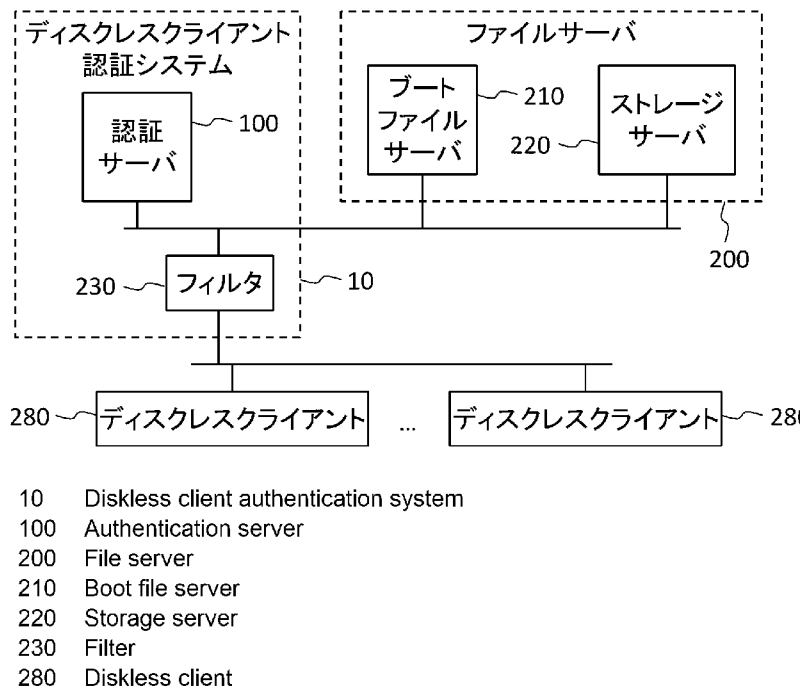
(72) 発明者: 澤崎 文彦 (SAWAZAKI, Fumihiko); 〒1808585 東京都武蔵野市緑町3丁目9-1 NTT 知的財産センタ内 Tokyo (JP).

(74) 代理人: 特許業務法人磯野国際特許商標事務所 (ISONO INTERNATIONAL PATENT OFFICE, P.C.); 〒1050001 東京都港区虎ノ門一丁目1番18号 ヒューリック虎ノ門ビル 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, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG,

(54) Title: DISKLESS CLIENT AUTHENTICATION SYSTEM, AUTHENTICATION SERVER, PROGRAM, AND DISKLESS CLIENT AUTHENTICATION METHOD

(54) 発明の名称: ディスクレスクライアント認証システム、認証サーバ、プログラムおよびディスクレスクライアント認証方法



(57) Abstract: A diskless client authentication system (10) is configured to include an authentication server (100) and a filter (230) that is on a communication path between a diskless client (280) and a file server (200) which stores a startup file. The authentication server (100) comprises: an address allocation unit that allocates a network address to the diskless

KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU,
LY, MA, MD, ME, MG, MK, MN, MW, MX, MY,
MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL,
PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK,
SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA,
UG, US, UZ, VC, VN, WS, 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, SC, SD, SL, ST, 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, KM, ML, MR, NE, SN, TD, TG).

添付公開書類：

一 国際調査報告 (条約第21条(3))

client (280); an authentication unit that authenticates the diskless client (280) to which the network address has been allocated; and a client control unit that, when the diskless client (280) which has been allocated the network address is in an unauthenticated state, instructs the authentication unit to authenticate said diskless client (280), and gives an instruction to permit communication between said diskless client (280) and the file server (200) when authentication is successful.

(57) 要約：ディスクレスクライアント認証システム（１０）は、認証サーバ（１００）、および、ディスクレスクライアント（２８０）と起動用ファイルを格納したファイルサーバ（２００）との通信経路上にあるフィルタ（２３０）を含んで構成される。認証サーバ（１００）は、ディスクレスクライアント（２８０）に対してネットワークアドレスを割り当てるアドレス割当部と、ネットワークアドレスが割り当て済のディスクレスクライアント（２８０）を認証する認証部と、ネットワークアドレス割り当て済のディスクレスクライアント（２８０）が未認証の状態であれば、認証部に指示して当該ディスクレスクライアント（２８０）を認証し、認証に成功すれば当該ディスクレスクライアント（２８０）とファイルサーバ（２００）との通信を許可するように指示するクライアント制御部を備える。

明 細 書

発明の名称：

ディスクレスクライアント認証システム、認証サーバ、プログラムおよび
ディスクレスクライアント認証方法

技術分野

[0001] 本発明は、システム起動前にディスクレスクライアントの認証を行うディスクレスクライアント認証システム、認証サーバ、プログラムおよびディスクレスクライアント認証方法に関する。

背景技術

[0002] ディスクレスクライアントは、OS (Operating System) やアプリケーションプログラム、ユーザデータなどを記憶しておらず、サーバ（ファイルサーバ）に依存しているシステムである。ディスクレスクライアントは、故障が発生しやすいHDD (Hard Disk Drive) を搭載しておらず故障しにくい、同じ構成のシステムを簡単に複製できセットアップが簡単である、リセットすると前回起動時と同じ構成で再起動するため回復性が高いなどのメリットがある。

[0003] ディスクレスクライアントの起動時の大まかな動作は以下の（１）～（３）のとおりである。（１）DHCP (Dynamic Host Configuration Protocol) などを用いてネットワーク設定情報（例えばIPアドレスや、ネットマスク値、ゲートウェイアドレスなど）を取得して、設定する。（２）TFTP (Trivial File Transfer Protocol) サーバからブート用ファイルを取得して、実行する。（３）NFS (Network File System) などを用いてOS (OS ロード他のファイル) を取得して、OSを起動する。

[0004] ディスクレスクライアントは、クライアントやネットワークが信頼できることが前提となっている技術であり、起動時の動作にクライアントやサーバの認証は含まれていない。クライアントの詐称が起こり得る環境でのディスクレスクライアントを利用するときには、クライアントの認証が必要となる

。ディスクレスクライアントにおける端末認証方式として、非特許文献 1 において 3 つの端末認証方式が検討されている。

先行技術文献

非特許文献

- [0005] 非特許文献1：澤崎文彦，中澤奨，”端末サイドの転送系機能のソフトウェア化におけるディスクレスクライアント技術の適用について，” 電子情報通信学会2022年総合大会，通信ソサイエティ B-6-24，2022年3月15日。

発明の概要

発明が解決しようとする課題

- [0006] 非特許文献 1 では、M A C (Media Access Control Address) を利用した認証、公開鍵を用いた認証、回線を利用した認証（例えば N G N (Next Generation Network) 標準）が提案されている。しかしながら、利用可能なシーンが限定的である、デファクトとして利用されているソフトウェアの改変が必要である、ディスクレスクライアントに搭載されるファームウェアの改変が必要であるなどが指摘されている。メーカを問わず一般に市販されているディスクレスクライアント製品に搭載されている普及技術（標準的に搭載されている技術）を利用して認証できることが望ましい。

本発明は、このような背景に鑑みてなされたものであり、普及技術を用いたディスクレスクライアントの認証を可能にすることを課題とする。

課題を解決するための手段

- [0007] 前記した課題を解決するため、本発明に係るディスクレスクライアント認証システムは、ディスクレスクライアントの認証サーバ、および、前記ディスクレスクライアントと当該ディスクレスクライアントの起動用ファイルを格納したファイルサーバとの通信経路上にあるフィルタを含んで構成されるディスクレスクライアント認証システムであって、前記フィルタは、前記認証サーバの指示により、前記ディスクレスクライアントと前記ファイルサーバとの通信を許可または禁止し、前記認証サーバは、前記ディスクレスクラ

クライアントの識別情報と認証状態とを関連付けて記憶するクライアント管理データベースを備える記憶部と、前記ディスクレスクライアントに対してネットワークアドレスを割り当てる処理を実行するアドレス割当部と、ネットワークアドレスが割り当て済の前記ディスクレスクライアントを認証する処理を実行する認証部と、前記フィルタに、前記ディスクレスクライアントと前記ファイルサーバとの通信を許可または禁止を指示するフィルタ制御部と、ネットワークアドレス割り当て済のディスクレスクライアントが前記クライアント管理データベースを参照して未認証の状態であれば、前記認証部に指示して当該ディスクレスクライアントを認証する処理を実行し、前記認証する処理が成功すれば、前記フィルタ制御部に当該ディスクレスクライアントと前記ファイルサーバとの通信を許可するように指示するクライアント制御部と、を備える。

発明の効果

[0008] 本発明によれば、普及技術を用いたディスクレスクライアントの認証を可能にすることができる。

図面の簡単な説明

[0009] [図1]本実施形態に係るディスクレスクライアント認証システムの全体構成を説明するための図である。

[図2]本実施形態に係る認証サーバの機能ブロック図である。

[図3]本実施形態に係るクライアント管理データベースのデータ構成図である。

[図4]本実施形態に係る認証処理のシーケンス図である。

[図5]本実施形態に係る終了処理のシーケンス図である。

[図6]本実施形態に係る認証サーバの機能を実現するコンピュータの一例を示すハードウェア構成図である。

発明を実施するための形態

[0010] 《ディスクレスクライアント認証システムの概要》

以下に本発明を実施するための形態（実施形態）におけるディスクレスク

クライアント認証システムについて説明する。ディスクレスクライアント認証システムは、認証サーバとフィルタとを含んで構成される。フィルタは、ディスクレスクライアントと、ブート用ファイルやOSのファイルを格納するファイルサーバ（ストレージ）との間にあり、通信データをフィルタリングする。フィルタは、例えばルータ（エッジルータ）であって、MACアドレスやネットワークアドレス、プロトコルを基にIPデータグラムフィルタリングを行う。フィルタは、ディスクレスクライアントとファイルサーバ間の通信を原則として禁止する。しかし、認証サーバからの許可の指示があればフィルタは、禁止の指示があるまでディスクレスクライアントとファイルサーバ間の通信を許可する。

[0011] 認証サーバは、DHCPを用いてディスクレスクライアントにIPアドレスを割り当てた後に、標準的なハードウェアベースマネージメントの認証機能を用いてディスクレスクライアントを認証する。認証に成功すると認証サーバは、フィルタにディスクレスクライアントとファイルサーバ間の通信を許可するように指示して、ディスクレスクライアントに再起動を指示する。再起動したディスクレスクライアントは、ファイルサーバとの通信が可能であり、通常の手順に従ってOSを起動する。認証が失敗ならば、ディスクレスクライアントとファイルサーバとの通信は禁止のままであり、ディスクレスクライアントはOSを起動できない。

[0012] このようなディスクレスクライアント認証システムによれば、普及技術を搭載したディスクレスクライアントや既存のファイルサーバを用いて、認証済みのディスクレスクライアントだけが（OSを）起動できるようになる。ディスクレスクライアントやファイルサーバの改変が不要になり、ディスクレスクライアントシステムが容易に導入できるようになる。

[0013] 《ディスクレスクライアント認証システムの全体構成》

図1は、本実施形態に係るディスクレスクライアント認証システム10の全体構成を説明するための図である。ディスクレスクライアント認証システム10は、認証サーバ100とフィルタ230とを含んで構成される。ディ

スクレスクライアント認証システム１０は、さらにブートファイルサーバ２１０およびストレージサーバ２２０を含んでもよい。

[0014] ブートファイルサーバ２１０は、例えばＴＦＴＰのサーバであり、ディスクレスクライアント２８０からの要求に応じてブート用ファイル（例えばＰＸＥ（Preboot eXecution Environment）のブートイメージ）を送信する。ストレージサーバ２２０は、例えばＮＦＳサーバであり、ディスクレスクライアント２８０からの要求に応じてＯＳやアプリケーションプログラム、ユーザデータをやり取りする。以下では、ブートファイルサーバ２１０およびストレージサーバ２２０を総称して、ファイルサーバ２００と記す。

[0015] フィルタ２３０は、ディスクレスクライアント２８０が接続されるネットワークと、ファイルサーバ２００が接続されるネットワークとの間に設置され、通信データのフィルタリングを行う。フィルタ２３０は、例えば物理アドレスやネットワークアドレス（ＩＰアドレス）、プロトコル（例えばポート番号）を基にフィルタリングを行う。

[0016] フィルタ２３０は、ディスクレスクライアント２８０と認証サーバ１００とでやり取りされるネットワークアドレスを含むネットワーク情報設定用の通信や認証用の通信を許可する。しかし、フィルタ２３０は、ディスクレスクライアント２８０と、ファイルサーバ２００との間の通信を原則として禁止（フィルタリング）する。認証サーバ１００からの許可の指示があるとフィルタ２３０は、指示されたディスクレスクライアント２８０と、ファイルサーバ２００との間の通信を許可する。他のディスクレスクライアント２８０と、ファイルサーバ２００との間の通信は禁止されたままである。認証サーバ１００からの禁止の指示があるとフィルタ２３０は、指示されたディスクレスクライアント２８０と、ファイルサーバ２００との間の通信を禁止する。

[0017] ≪認証サーバの構成≫

図２は、本実施形態に係る認証サーバ１００の機能ブロック図である。認証サーバ１００はコンピュータであり、制御部１１０、記憶部１２０、およ

び入出力部 180 を備える。入出力部 180 には、ディスプレイやキーボード、マウスなどのユーザインターフェイス機器が接続される。入出力部 180 が通信デバイスを備え、フィルタ 230 やディスクレスクライアント 280 とのデータ送受信が可能である。また入出力部 180 にメディアドライブが接続され、記録媒体を用いたデータのやり取りが可能であってもよい。

[0018] ‹記憶部›

記憶部 120 は、ROM (Read Only Memory) や RAM (Random Access Memory)、SSD (Solid State Drive) などの記憶機器を含んで構成される。記憶部 120 には、クライアント管理データベース 130、アドレス管理データベース 140、およびプログラム 128 が記憶される。プログラム 128 には、後記する認証処理（後記する図 4 参照）における認証サーバ 100 の処理手順の記述が含まれる。

[0019] 図 3 は、本実施形態に係るクライアント管理データベース 130 のデータ構成図である。クライアント管理データベース 130 は、例えば表形式のデータであって、行（レコード）はディスクレスクライアント 280 の状態を示す。レコードは、物理アドレス、ネットワークアドレス、認証状態、認証日時、および認証情報の列（属性）を含む。

[0020] 物理アドレスは、ディスクレスクライアント 280 の物理アドレスを示し、例えば Ethernet アドレスである。物理アドレスは、ディスクレスクライアント 280 の識別情報として参照される。ネットワークアドレスは、ディスクレスクライアント 280 に割り当てられたネットワークアドレスを示し、例えば割り当てられた IP アドレスである。

認証状態は、ディスクレスクライアント 280 が認証に成功済か否か（認証済／未認証（認証前、認証失敗を含む））を示す。認証日時は、ディスクレスクライアント 280 が最後に認証された日時（図 3 では時刻のみを記載）を示す。

[0021] 認証情報は、ディスクレスクライアント 280 を認証するときに参照される情報を示し、例えば公開鍵や、ディスクレスクライアント 280 と共有す

る秘密情報（パスワード）である。認証情報は、物理アドレスとともに、予め設定されている（登録されている）。

クライアント管理データベース１３０は、他の情報（属性）を含んでもよい。例えば認証に成功した日時や、ネットワークアドレスが割り当てられた日時などを含んでもよい。

[0022] 図１に戻って記憶部１２０の説明を続ける。アドレス管理データベース１４０は、ディスクレスクライアント２８０に割り当てられるネットワークアドレスが格納されている。各ネットワークアドレスは、割り当て済か否か、割り当ての期限、割り当てられたディスクレスクライアント２８０の物理アドレス、最後に割り当てられたディスクレスクライアント２８０の物理アドレスなどに関連付けられている。

[0023] ≪制御部≫

制御部１１０は、ＣＰＵ（Central Processing Unit）を含んで構成され、アドレス割当部１１１、認証部１１２、クライアント制御部１１３、およびフィルタ制御部１１４が備わる。

[0024] アドレス割当部１１１は、ディスクレスクライアント２８０にネットワークアドレスを割り当てる。またアドレス割当部１１１は、各種ネットワークの設定情報（例えばデフォルトゲートウェイやブートファイルサーバ２１０のネットワークアドレス）をディスクレスクライアント２８０に通知する。アドレス割当部１１１は、例えばＤＨＣＰを用いて割り当てや通知を行う。

[0025] 認証部１１２は、ディスクレスクライアント２８０を認証する。認証開始時点のディスクレスクライアント２８０は、ネットワークアドレスは割り当て済であるが、ＯＳ起動前の状態である。認証部１１２は、ディスクレスクライアント２８０のハードウェアベースマネージメントの認証機能を用いて認証する。ハードウェアベースマネージメントの例として、Intel AMT（Active Management Technology）やAMD PROなどがある。認証部１１２は、ディスクレスクライアント２８０のハードウェアに標準搭載されている認証機能を利用して、ディスクレスクライアント２８０を認証する。

クライアント制御部 113 は、ディスクレスクライアント 280 に対して認証処理や再起動などを指示して制御する。

[0026] フィルタ制御部 114 は、フィルタ 230 にディスクレスクライアント 280 とファイルサーバ 200 間の通信のフィルタリングを指示する。例えばフィルタ制御部 114 は、フィルタにディスクレスクライアント 280 の物理アドレスとネットワークアドレスとを通知して、当該ディスクレスクライアント 280 とファイルサーバ 200 との通信を許可するように指示する。指示を受けるとフィルタ 230 は、物理アドレスやネットワークアドレス、ポート番号（プロトコル識別情報）などを参照して、当該ディスクレスクライアント 280 とファイルサーバ 200 とでやり取りされる通信データの通過を許可する。

[0027] ≪認証処理≫

図 4 は、本実施形態に係る認証処理のシーケンス図である。図 4 を参照しながら、ディスクレスクライアント 280 が起動（電源投入）以降の、OS を起動するまでの処理を説明する。なお図 4 では、ディスクレスクライアント 280 を「クライアント」、クライアント制御部 113 を「C 制御部」と記載している。

[0028] ステップ S 11 においてディスクレスクライアント 280 とアドレス割当部 111 とは、例えば DHCP を用いてネットワークアドレス割り当て処理を実行する。ネットワークアドレス割り当ての他に、デフォルトゲートウェイやブートファイルサーバ 210 のアドレスが通知される。

[0029] なおクライアント管理データベース 130（図 3 参照）において、物理アドレスで特定されるディスクレスクライアント 280 のレコードの認証状態が「認証済」であるならば、アドレス割当部 111 は当該レコードのネットワークアドレスにあるネットワークアドレスを割り当てる。

[0030] クライアント管理データベース 130 にディスクレスクライアント 280 のレコードがない場合（未登録の場合）にアドレス割当部 111 は、ディスクレスクライアント 280 にエラーを通知してアドレスを割り当てない。レ

コードの認証状態が「未認証」である場合にアドレス割当部 111 は、アドレス管理データベース 140 を参照して未割り当てのネットワークアドレスを割り当てる。このように処理する理由は、後記する。

[0031] ステップ S 12 においてアドレス割当部 111 は、クライアント管理データベース 130 を更新する。詳しく説明すると、ステップ S 11 において未割り当てのネットワークアドレスを割り当てた場合にアドレス割当部 111 は、物理アドレスで特定されるディスクレスクライアント 280 のレコードのネットワークアドレスを、ステップ S 11 において割り当てたネットワークアドレスに更新する。なお当該レコードの認証状態は「未認証」である。

[0032] クライアント管理データベース 130 の認証状態が「認証済」でネットワークアドレスにあるネットワークアドレスを割り当てた場合にアドレス割当部 111 は、クライアント管理データベース 130 を更新しない。

ステップ S 13 においてアドレス割当部 111 は、アドレスを割り当てたディスクレスクライアント 280 の物理アドレスをクライアント制御部 113 に通知する。

[0033] ステップ S 14 においてクライアント制御部 113 は、クライアント管理データベース 130 を参照して、ステップ S 13 で通知されたディスクレスクライアント 280 が認証状態を取得する。クライアント制御部 113 は、認証済みならば（ステップ S 14 → YES）認証処理を終了し、未認証ならば（ステップ S 14 → NO）ステップ S 15 に進む。認証サーバ 100 の認証処理が終了した後のディスクレスクライアント 280 の動作については、後記する。

[0034] ステップ S 15 においてクライアント制御部 113 は、ディスクレスクライアント 280 の認証処理を実行するように、認証部 112 に指示する。

ステップ S 16 においてディスクレスクライアント 280 と認証部 112 とは、認証処理を実行する。

ステップ S 17 において認証部 112 は、クライアント管理データベース 130 を更新する。詳しく説明すると認証部 112 は、認証の成功または失

敗に応じて、認証状態を「認証済」または「未認証」に更新する。

[0035] ステップS 1 8において認証部 1 1 2は、認証処理（ステップS 1 6参照）の結果をクライアント制御部 1 1 3に通知する。

ステップS 1 9においてクライアント制御部 1 1 3は、認証が成功ならば（ステップS 1 9→Y E S）ステップS 2 0に進み、失敗ならば（ステップS 1 9→N O）認証処理を終了する。

[0036] ステップS 2 0においてクライアント制御部 1 1 3は、ディスクレスクライアント 2 8 0の物理アドレスとネットワークアドレスとを通知して、当該ディスクレスクライアント 2 8 0とファイルサーバ 2 0 0との通信を許可するようにフィルタ制御部 1 1 4に指示する。

ステップS 2 1においてフィルタ制御部 1 1 4は、ディスクレスクライアント 2 8 0の物理アドレスとネットワークアドレスとを通知して、当該ディスクレスクライアント 2 8 0とファイルサーバ 2 0 0との通信を許可するようにフィルタ 2 3 0に指示する。

[0037] ステップS 2 2においてクライアント制御部 1 1 3は、ディスクレスクライアント 2 8 0に再起動を指示する。再起動の指示を受けたディスクレスクライアント 2 8 0は、再起動してステップS 1 1に戻ることになる。この時点でディスクレスクライアント 2 8 0とファイルサーバ 2 0 0とは通信可能になっているため、通常の起動処理ができる。即ち再起動したディスクレスクライアント 2 8 0は、ネットワークアドレス他のネットワーク情報を取得し（ステップS 1 1参照）、ブートファイルサーバ 2 1 0からブート用ファイルを取得して実行して、ストレージサーバ 2 2 0からOSローダ他のファイルを取得して実行することでOSを起動する。割り当てられるネットワークアドレスは、認証済みの状態であるために前回（未認証の状態を取得したネットワークアドレス、ステップS 1 1参照）と同じである。

[0038] 《終了処理》

図 5 は、本実施形態に係る終了処理のシーケンス図である。図 5 を参照して、ディスクレスクライアント 2 8 0からのアドレス解放通知を受信した場

合や、ネットワークアドレスの割り当て期限が過ぎた場合、管理者からディスクレスクライアント280の切断指示を受けた場合などの処理を説明する。

[0039] ステップS31においてアドレス割当部111は、クライアント管理データベース130（図3参照）を更新する。詳しく説明するとアドレス割当部111は、ディスクレスクライアント280に対応するネットワークアドレスを「N/A」とし、認証状態を「未認証」とし、認証日時を「N/A」とする。なお「N/A」は、該当なし、不適用、無効などを意味するNot Applicableの略号である。またアドレス割当部111は、アドレス管理データベース140にあるディスクレスクライアント280に割り当てられていたネットワークアドレスを未割り当ての状態に更新する。

[0040] ステップS32においてアドレス割当部111は、ディスクレスクライアント280の物理アドレスをクライアント制御部113に通知する。

ステップS33においてクライアント制御部113は、ディスクレスクライアント280の物理アドレスを通知して、当該ディスクレスクライアント280とファイルサーバ200との通信を禁止するようにフィルタ制御部114に指示する。

ステップS34においてフィルタ制御部114は、ディスクレスクライアント280の物理アドレスを通知して、当該ディスクレスクライアント280とファイルサーバ200との通信を禁止（フィルタリング）するようにフィルタ230に指示する。

[0041] 《ディスクレスクライアント認証システムの特徴》

認証サーバ100は、ディスクレスクライアント280がネットワークに接続または起動すると、ネットワークアドレスを割り当て（ステップS11参照）、認証を行って（ステップS16参照）成功すれば（ステップS19→YES参照）ファイルサーバ200との通信を許可する（ステップS21参照）。クライアント管理データベース130に未登録など認証に成功しない場合には、ディスクレスクライアント280はファイルサーバ200と通

信ができず、OSを起動できない。認証処理は、普及技術であるハードウェアベースマネージメントの機能により実行されており、市場に流通する多くのディスクレスクライアントで利用可能である。またディスクレスクライアント280の利用者の介在不要であり、従来の使い勝手と変わらない。

[0042] 《変形例：再起動の指示》

上記した実施形態の認証サーバ100は、認証処理（ステップS16参照）に成功した後にディスクレスクライアント280に再起動を指示している（ステップS22参照）。認証処理を行っている間中、ディスクレスクライアント280がブートファイルサーバ210へのアクセスを試行しているならば、再起動の指示をなくしてもよい。

[0043] 例えばTFTPのパケットタイムアウト時間とパケット再伝送回数との積の時間の間に認証処理が終了するのであれば、再起動の指示をなくしてもよい。通信が許可された時点から（ステップS21参照）ディスクレスクライアント280はブートファイルサーバ210にアクセスが可能となり、ネットワークアドレス取得（ステップS11参照）を含めた通常の起動処理が継続できる。

[0044] 《変形例》

以上、本発明のいくつかの実施形態について説明したが、これらの実施形態は、例示に過ぎず、本発明の技術的範囲を限定するものではない。例えば認証サーバ100は、アドレス割当部111を備え、ディスクレスクライアント280にネットワークアドレスを割り当てているが、ネットワークアドレス割り当てサーバ（DHCPサーバ）として分離してもよい。但し認証済みのディスクレスクライアント280に対しては、割り当て済のネットワークアドレスを割り当てる。

[0045] 上記した実施形態では、アドレス割当部111が、クライアント管理データベース130（図3参照）におけるディスクレスクライアント280の認証状態を「未認証」に更新している（図5記載のステップS31参照）。代わりにクライアント制御部113が、通知を受けた後に（ステップS32参

照) 更新してもよい。

[0046] 本発明はその他の様々な実施形態を取ることが可能であり、さらに、本発明の要旨を逸脱しない範囲で、省略や置換等種々の変更を行うことができる。これら実施形態やその変形は、本明細書等に記載された発明の範囲や要旨に含まれるとともに、特許請求の範囲に記載された発明とその均等の範囲に含まれる。

[0047] ≪ハードウェア構成≫

上記した実施形態に係る認証サーバ100は、例えば図6に示すような構成のコンピュータ900によって実現される。図6は、本実施形態に係る認証サーバ100の機能を実現するコンピュータ900の一例を示すハードウェア構成図である。コンピュータ900は、CPU901、ROM902、RAM903、SSD904、入出力インターフェイス905（図6では入出力I/F（Interface）と記載）、通信インターフェイス906（図6では通信I/Fと記載）、およびメディアインターフェイス907（図6ではメディアI/Fと記載）を備える。コンピュータ900は、SSD904に替わりにHDD（Hard Disc Drive）を備えてもよいし、SSD904に加えて、さらにHDDを備えてもよい。

[0048] CPU901は、ROM902またはSSD904に記憶されたプログラムに基づいて作動し、図2の制御部110による制御を行う。ROM902は、コンピュータ900の起動時にCPU901により実行されるブートプログラムや、コンピュータ900のハードウェアに係るプログラムなどを記憶する。

CPU901は、入出力インターフェイス905を介して、マウスやキーボードなどの入力装置910、およびディスプレイやプリンタなどの出力装置911を制御する。CPU901は、入出力インターフェイス905を介して、入力装置910からデータを取得するとともに、生成したデータを出力装置911へ出力する。

[0049] SSD904は、CPU901により実行されるプログラムおよび当該プ

プログラムによって使用されるデータなどを記憶する。通信インターフェイス 906 は、通信網を介して不図示の他の装置（例えば、フィルタ 230 やディスクレスクライアント 280）からデータを受信して CPU 901 へ出力し、また、CPU 901 が生成したデータを、通信網を介して他の装置へ送信する。

メディアインターフェイス 907 は、記録媒体 912 に格納されたプログラムまたはデータを読み取り、RAM 903 を介して CPU 901 へ出力する。CPU 901 は、プログラムを、メディアインターフェイス 907 を介して記録媒体 912 から RAM 903 上にロードし、ロードしたプログラムを実行する。記録媒体 912 は、DVD (Digital Versatile Disk) などの光学記録媒体、MO (Magneto Optical disk) などの光磁気記録媒体、磁気記録媒体、導体メモリーテープ媒体または半導体メモリなどである。

[0050] 例えば、コンピュータ 900 が上記した実施形態に係る認証サーバ 100 として機能する場合、コンピュータ 900 の CPU 901 は、RAM 903 上にロードされたプログラム 128（図 2 参照）を実行することにより、認証サーバ 100 の機能を実現する。CPU 901 は、プログラムを記録媒体 912 から読み取って実行する。この他、CPU 901 は、他の装置から通信網を介してプログラムを読み込んでもよいし、記録媒体 912 から SSD 904 にプログラム 128 をインストールして実行してもよい。

[0051] ≪効果≫

以下に、ディスクレスクライアント認証システム 10 の効果を説明する。

[0052] 上記した実施形態に係るディスクレスクライアント認証システム 10 は、ディスクレスクライアント 280 の認証サーバ 100、および、ディスクレスクライアント 280 と当該ディスクレスクライアント 280 の起動用ファイル（ブート用のファイルや OS のファイル）を格納したファイルサーバ 200 との通信経路上にあるフィルタ 230 を含んで構成される。

フィルタ 230 は、認証サーバ 100 の指示により、ディスクレスクライアント 280 とファイルサーバ 200 との通信を許可または禁止する。

認証サーバ１００は、ディスククライアント２８０の識別情報（物理アドレス）と認証状態とを関連付けて記憶するクライアント管理データベース１３０を備える記憶部１２０を備える。

認証サーバ１００は、ディスククライアント２８０に対してネットワークアドレスを割り当てる処理を実行するアドレス割当部１１１を備える。

認証サーバ１００は、ネットワークアドレスが割り当て済のディスククライアント２８０を認証する処理を実行する認証部１１２を備える。

認証サーバ１００は、フィルタ２３０に、ディスククライアント２８０とファイルサーバ２００との通信を許可または禁止を指示するフィルタ制御部１１４を備える。

認証サーバ１００は、ネットワークアドレス割り当て済のディスククライアント２８０がクライアント管理データベース１３０を参照して未認証の状態であれば、前記認証部に指示して当該ディスククライアントを認証する処理を実行し、認証する処理が成功すれば、フィルタ制御部１１４に当該ディスククライアント２８０とファイルサーバ２００との通信を許可するように指示するクライアント制御部１１３を備える。

[0053] このようなディスククライアント認証システム１０によれば、認証に成功したディスククライアント２８０は、ファイルサーバ２００にアクセス可能となって（ＯＳ／システムの）起動に成功する。認証に失敗したディスククライアント２８０は、ファイルサーバ２００にアクセスできず起動できない。認証は、普及技術であるハードウェアベースマネジメントの機能により実行可能であり、市場に流通する多くのディスククライアントで利用可能である。

[0054] 上記した実施形態に係るクライアント制御部１１３は、フィルタ制御部１１４にディスククライアント２８０とファイルサーバ２００との通信を許可するように指示する際に、当該ディスククライアント２８０に再起動を指示する。

[0055] このようなディスククライアント認証システム１０によれば、ディス

クレスクライアント 280 における認証処理の後の起動処理が中断した場合であっても、再起動することによって、再度ネットワークアドレスを取得した後にファイルサーバ 200 にアクセスして、起動することができるようになる。

[0056] 上記した実施形態に係るクライアント制御部 113 は、ディスクレスクライアント 280 から、割り当てたネットワークアドレスの解放通知を受け取った場合、ネットワークアドレスの割り当て期限に達した場合、および、（例えば管理者から）ディスクレスクライアント 280 の切断指示を受けた場合の何れかの場合に、フィルタ制御部 114 に当該ディスクレスクライアント 280 とファイルサーバ 200 との通信を禁止するように指示するとともに、当該ディスクレスクライアント 280 の認証状態を未認証にする。

[0057] このようなディスクレスクライアント認証システム 10 によれば、ネットワークアドレスを解放したり、ネットワークアドレスの期限が過ぎたり、管理者から指定されたりしたディスクレスクライアント 280 は、ファイルサーバ 200 にアクセスできない。延いては、認証なしに再起動できない。

[0058] フィルタ 230 は、ディスクレスクライアント 280、および、ファイルサーバ 200 の、物理アドレス、ネットワークアドレス、およびプロトコル識別情報（例えばポート番号）の少なくとも 1 つを基に、ディスクレスクライアント 280 とファイルサーバ 200 との間でやり取りされる通信データの通過を許可または禁止する。

[0059] このようなディスクレスクライアント認証システム 10 によれば、標準的なルータやスイッチをフィルタ 230 として利用することができるようになる。

符号の説明

- [0060] 10 ディスクレスクライアント認証システム
100 認証サーバ
111 アドレス割当部
112 認証部

- 1 1 3 クライアント制御部
- 1 1 4 フィルタ制御部
- 1 3 0 クライアント管理データベース
- 2 0 0 ファイルサーバ
- 2 3 0 フィルタ
- 2 8 0 ディスクレスクライアント

請求の範囲

[請求項1]

ディスクレスクライアントの認証サーバ、および、前記ディスクレスクライアントと当該ディスクレスクライアントの起動用ファイルを格納したファイルサーバとの通信経路上にあるフィルタを含んで構成されるディスクレスクライアント認証システムであって、

前記フィルタは、

前記認証サーバの指示により、前記ディスクレスクライアントと前記ファイルサーバとの通信を許可または禁止し、

前記認証サーバは、

前記ディスクレスクライアントの識別情報と認証状態とを関連付けて記憶するクライアント管理データベースを備える記憶部と、

前記ディスクレスクライアントに対してネットワークアドレスを割り当てる処理を実行するアドレス割当部と、

ネットワークアドレスが割り当て済の前記ディスクレスクライアントを認証する処理を実行する認証部と、

前記フィルタに、前記ディスクレスクライアントと前記ファイルサーバとの通信を許可または禁止を指示するフィルタ制御部と、

ネットワークアドレス割り当て済のディスクレスクライアントが前記クライアント管理データベースを参照して未認証の状態であれば、前記認証部に指示して当該ディスクレスクライアントを認証する処理を実行し、

前記認証する処理が成功すれば、前記フィルタ制御部に当該ディスクレスクライアントと前記ファイルサーバとの通信を許可するように指示するクライアント制御部と、を備える

ディスクレスクライアント認証システム。

[請求項2]

前記クライアント制御部は、

前記フィルタ制御部に前記ディスクレスクライアントと前記ファイルサーバとの通信を許可するように指示する際に、当該ディスクレス

クライアントに再起動を指示する

請求項1に記載のディスクレスクライアント認証システム。

[請求項3]

前記クライアント制御部は、

前記ディスクレスクライアントから、割り当てたネットワークアドレスの解放通知を受け取った場合、

前記ネットワークアドレスの割り当て期限に達した場合、および、

前記ディスクレスクライアントの切断指示を受けた場合の何れかの場合に、

前記フィルタ制御部に当該ディスクレスクライアントと前記ファイルサーバとの通信を禁止するように指示するとともに、当該ディスクレスクライアントの認証状態を未認証にする

請求項1に記載のディスクレスクライアント認証システム。

[請求項4]

前記フィルタは、

前記ディスクレスクライアント、および、前記ファイルサーバの、物理アドレス、ネットワークアドレス、およびプロトコル識別情報の少なくとも1つを基に、前記ディスクレスクライアントと前記ファイルサーバとの間でやり取りされる通信データの通過を許可または禁止する

請求項1に記載のディスクレスクライアント認証システム。

[請求項5]

ディスクレスクライアントと当該ディスクレスクライアントの起動用ファイルを格納したファイルサーバとの通信経路上にあって、前記ディスクレスクライアントと前記ファイルサーバとの通信を許可または禁止するフィルタに通信接続され、前記ディスクレスクライアントを認証する認証サーバであって、

前記ディスクレスクライアントの識別情報と認証状態とを関連付けて記憶するクライアント管理データベースを備える記憶部と、

前記ディスクレスクライアントに対してネットワークアドレスを割り当てる処理を実行するアドレス割当部と、

ネットワークアドレスが割り当て済の前記ディスクレスクライアントを認証する処理を実行する認証部と、

前記フィルタに、前記ディスクレスクライアントと前記ファイルサーバとの通信を許可または禁止を指示するフィルタ制御部と、

ネットワークアドレス割り当て済のディスクレスクライアントが前記クライアント管理データベースを参照して未認証の状態であれば、前記認証部に指示して当該ディスクレスクライアントを認証する処理を実行し、

前記認証する処理が成功すれば、前記フィルタ制御部に当該ディスクレスクライアントと前記ファイルサーバとの通信を許可するように指示するクライアント制御部と、を備える

認証サーバ。

[請求項6] コンピュータを請求項5の認証サーバとして機能させるためのプログラム。

[請求項7] ディスクレスクライアントと当該ディスクレスクライアントの起動用ファイルを格納したファイルサーバとの通信経路上にあって、前記ディスクレスクライアントと前記ファイルサーバとの通信を許可または禁止するフィルタに通信接続され、前記ディスクレスクライアントを認証する認証サーバのディスクレスクライアント認証方法であって、

前記認証サーバは、

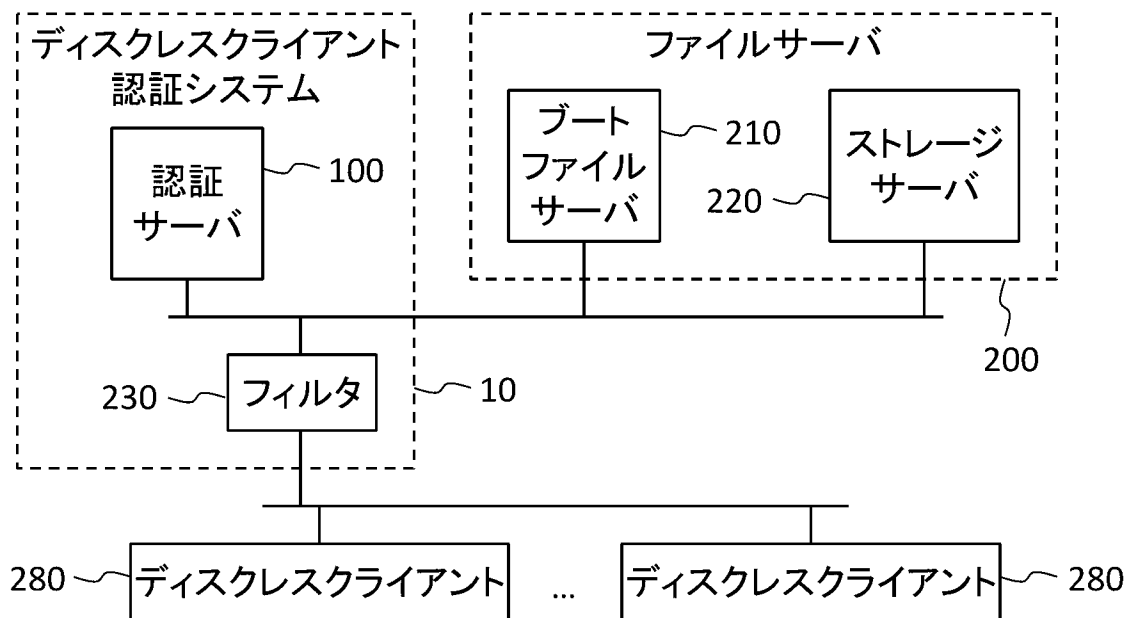
前記ディスクレスクライアントの識別情報と認証状態とを関連付けて記憶するクライアント管理データベースを備える記憶部を備え、

前記ディスクレスクライアントに対してネットワークアドレスを割り当てる処理を実行するステップと、

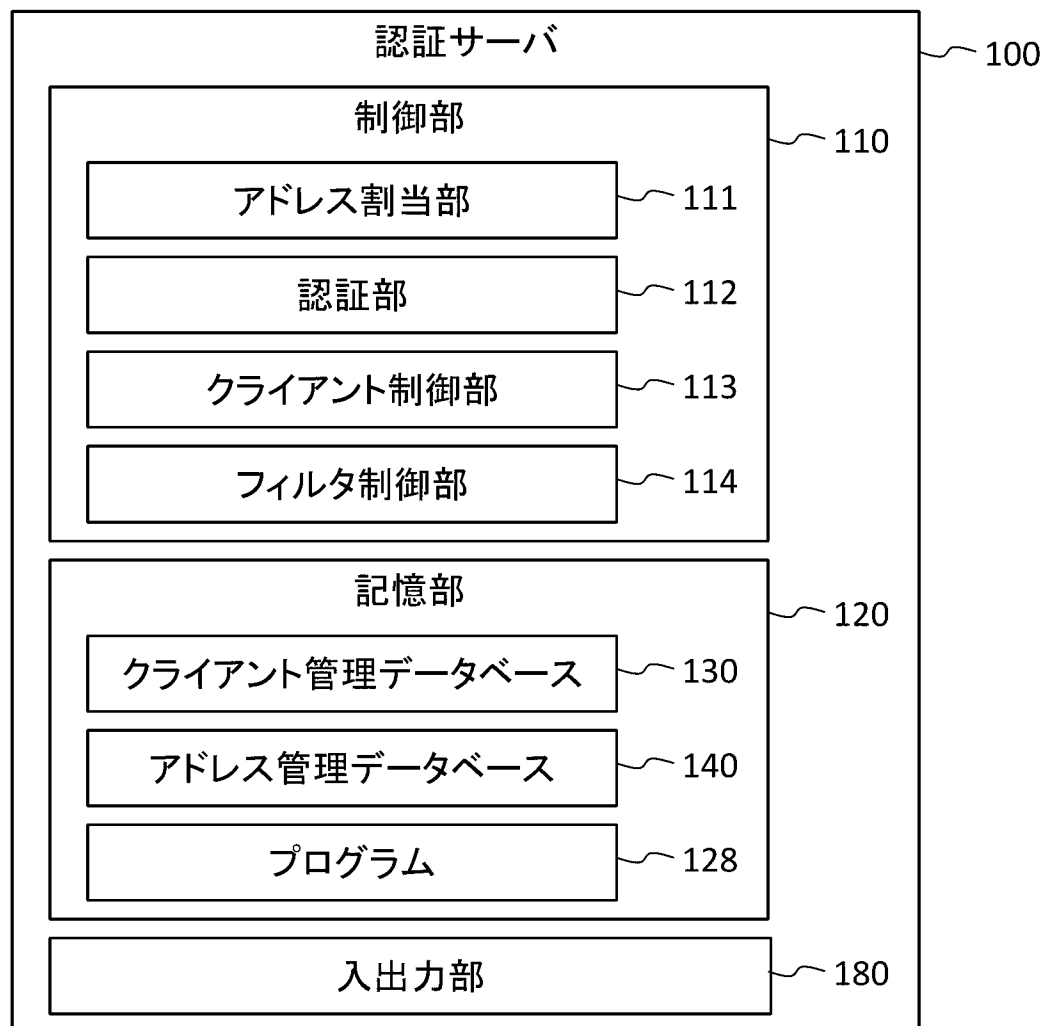
ネットワークアドレス割り当て済のディスクレスクライアントが前記クライアント管理データベースを参照して未認証の状態であれば、当該ディスクレスクライアントを認証するステップと、

当該ディスクリスクライアントの認証に成功すれば、前記フィルタ
に対して当該ディスクリスクライアントと前記ファイルサーバとの通
信を許可するように指示するステップと、を実行する
ディスクリスクライアント認証方法。

[図1]



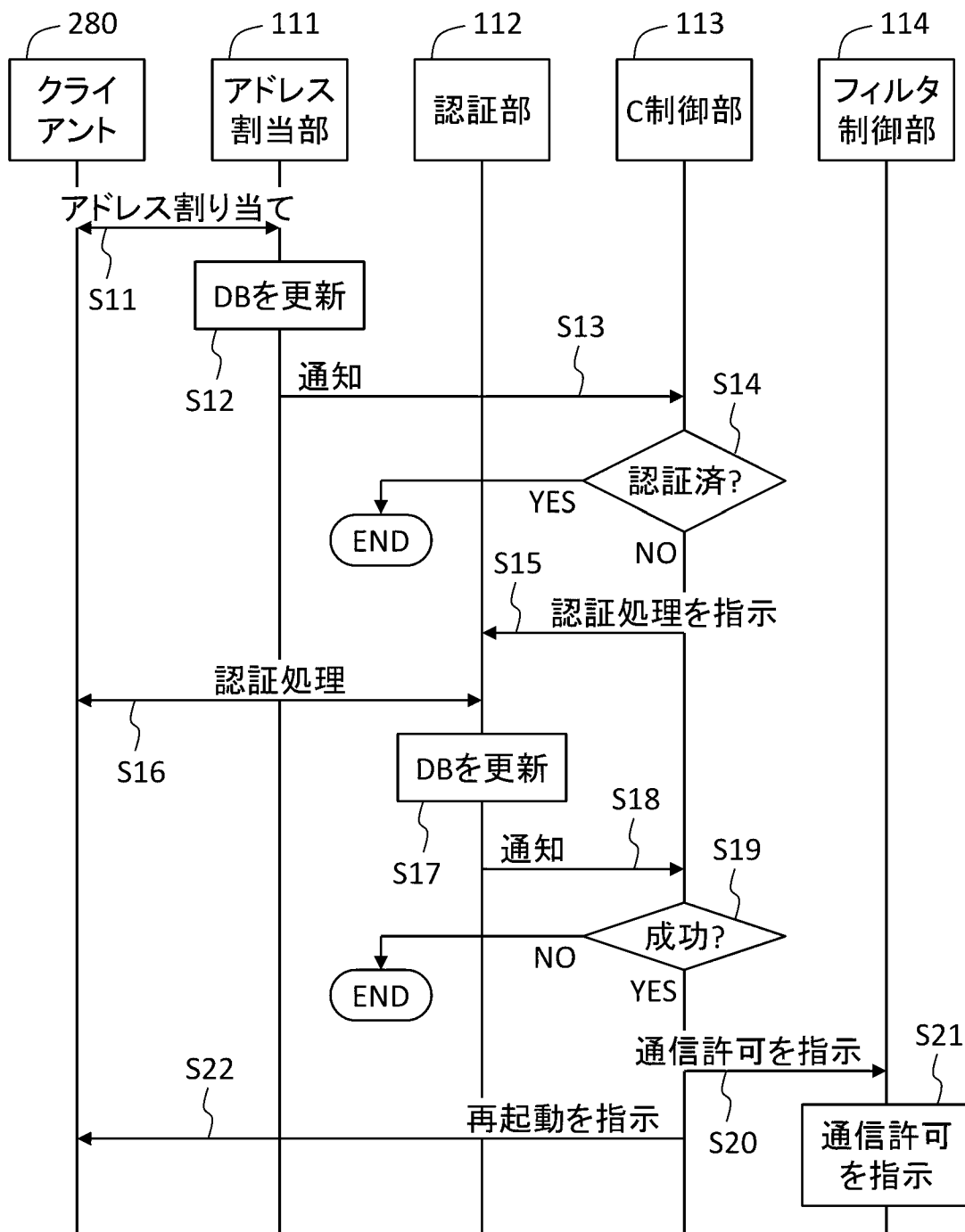
[図2]



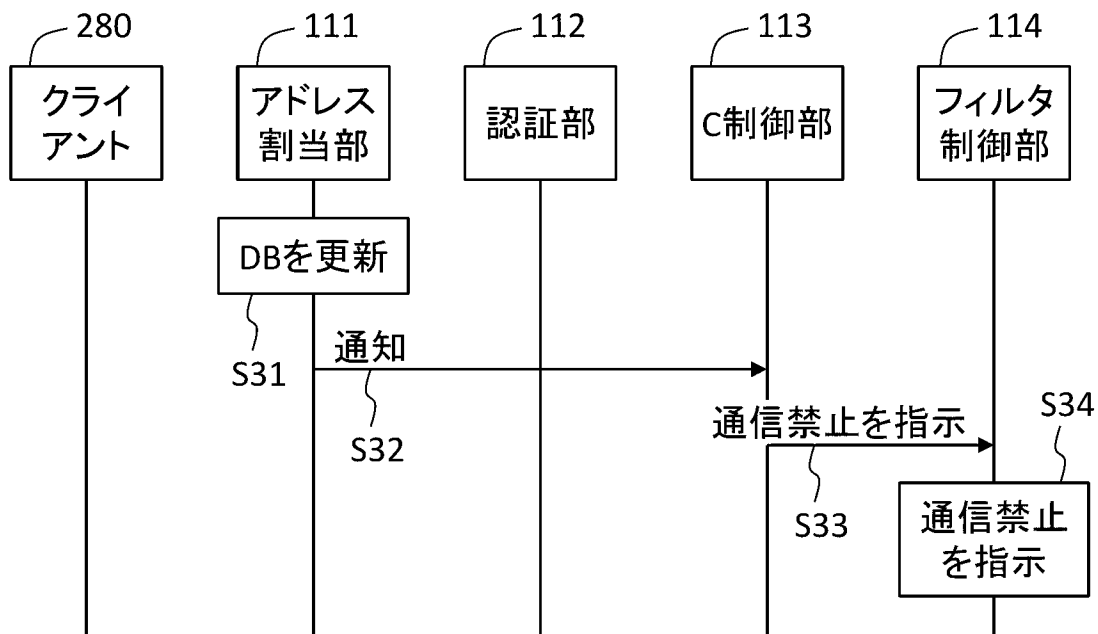
[図3]

物理アドレス	ネットワーク アドレス	認証 状態	認証 日時	認証 情報	← 130
abcd: ... :3434	192.4.3.194	未認証	N/A	#####	
abcd: ... :34b4	192.4.3.184	認証済	14:34:34	#####	
...	...	...	...	...	

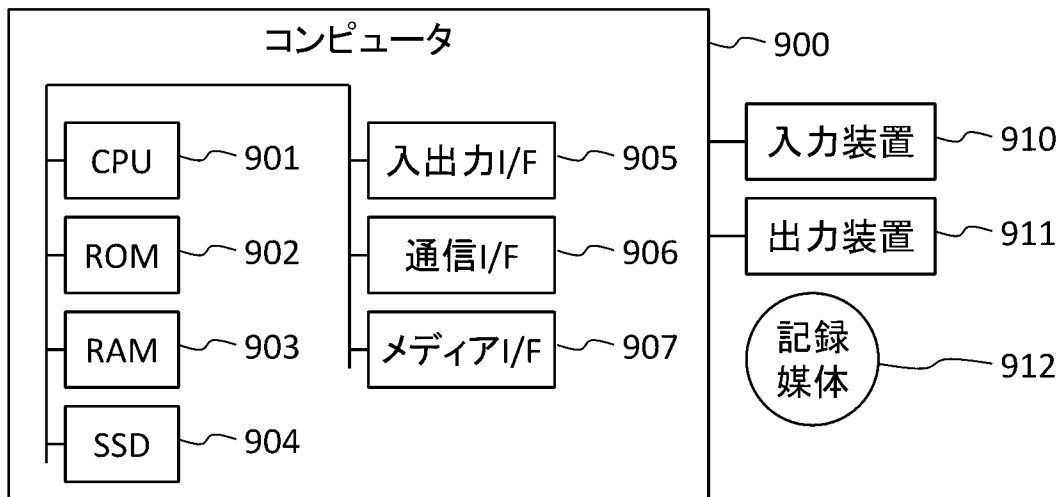
[図4]



[図5]



[図6]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2022/026872

A. CLASSIFICATION OF SUBJECT MATTER G06F 21/44 (2013.01)i FI: G06F21/44 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) G06F21/44 Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched Published examined utility model applications of Japan 1922-1996 Published unexamined utility model applications of Japan 1971-2022 Registered utility model specifications of Japan 1996-2022 Published registered utility model applications of Japan 1994-2022 Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)														
C. DOCUMENTS CONSIDERED TO BE RELEVANT <table border="1"> <thead> <tr> <th>Category*</th> <th>Citation of document, with indication, where appropriate, of the relevant passages</th> <th>Relevant to claim No.</th> </tr> </thead> <tbody> <tr> <td>Y</td> <td>JP 2008-015786 A (HITACHI, LTD.) 24 January 2008 (2008-01-24) paragraphs [0026]-[0069], [0097], [0098], fig. 1, 5, 16</td> <td>1-7</td> </tr> <tr> <td>Y</td> <td>JP 2004-341578 A (NIPPON TELEGR. & TELEPH. CORP.) 02 December 2004 (2004-12-02) paragraphs [0005], [0064]-[0071], fig. 1, 2</td> <td>1-7</td> </tr> <tr> <td>Y</td> <td>JP 2003-218873 A (FUJITSU LTD.) 31 July 2003 (2003-07-31) paragraphs [0017]-[0021], fig. 7-9</td> <td>1-7</td> </tr> </tbody> </table>			Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.	Y	JP 2008-015786 A (HITACHI, LTD.) 24 January 2008 (2008-01-24) paragraphs [0026]-[0069], [0097], [0098], fig. 1, 5, 16	1-7	Y	JP 2004-341578 A (NIPPON TELEGR. & TELEPH. CORP.) 02 December 2004 (2004-12-02) paragraphs [0005], [0064]-[0071], fig. 1, 2	1-7	Y	JP 2003-218873 A (FUJITSU LTD.) 31 July 2003 (2003-07-31) paragraphs [0017]-[0021], fig. 7-9	1-7
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.												
Y	JP 2008-015786 A (HITACHI, LTD.) 24 January 2008 (2008-01-24) paragraphs [0026]-[0069], [0097], [0098], fig. 1, 5, 16	1-7												
Y	JP 2004-341578 A (NIPPON TELEGR. & TELEPH. CORP.) 02 December 2004 (2004-12-02) paragraphs [0005], [0064]-[0071], fig. 1, 2	1-7												
Y	JP 2003-218873 A (FUJITSU LTD.) 31 July 2003 (2003-07-31) paragraphs [0017]-[0021], fig. 7-9	1-7												
☐ 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 10 August 2022		Date of mailing of the international search report 23 August 2022												
Name and mailing address of the ISA/JP Japan Patent Office (ISA/JP) 3-4-3 Kasumigaseki, Chiyoda-ku, Tokyo 100-8915 Japan		Authorized officer Telephone No.												

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/JP2022/026872

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
JP	2008-015786	A	24 January 2008	US 2008/0034092 A1 paragraphs [0049]-[0090], [0118], [0119], fig. 1, 5, 16 CN 101102247 A	
JP	2004-341578	A	02 December 2004	(Family: none)	
JP	2003-218873	A	31 July 2003	US 2003/0167411 A1 paragraphs [0034]-[0037], fig. 7-9	

A. 発明の属する分野の分類（国際特許分類（IPC）） G06F 21/44(2013.01)i FI: G06F21/44										
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）） G06F21/44										
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 <table border="0"> <tr> <td>日本国実用新案公報</td> <td>1922 - 1996年</td> </tr> <tr> <td>日本国公開実用新案公報</td> <td>1971 - 2022年</td> </tr> <tr> <td>日本国実用新案登録公報</td> <td>1996 - 2022年</td> </tr> <tr> <td>日本国登録実用新案公報</td> <td>1994 - 2022年</td> </tr> </table>			日本国実用新案公報	1922 - 1996年	日本国公開実用新案公報	1971 - 2022年	日本国実用新案登録公報	1996 - 2022年	日本国登録実用新案公報	1994 - 2022年
日本国実用新案公報	1922 - 1996年									
日本国公開実用新案公報	1971 - 2022年									
日本国実用新案登録公報	1996 - 2022年									
日本国登録実用新案公報	1994 - 2022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								
Y	JP 2008-015786 A（株式会社日立製作所）24.01.2008（2008 - 01 - 24） 段落[0026]-[0069], [0097]-[0098], 図1, 5, 16	1-7								
Y	JP 2004-341578 A（日本電信電話株式会社）02.12.2004（2004 - 12 - 02） 段落[0005], [0064]-[0071], 図1-2	1-7								
Y	JP 2003-218873 A（富士通株式会社）31.07.2003（2003 - 07 - 31） 段落[0017]-[0021], 図7-9	1-7								
☐ 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。										
<table border="0"> <tr> <td style="vertical-align: top;"> * 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 </td> <td style="vertical-align: top;"> “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抵触するものではなく、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 </td> </tr> </table>			* 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抵触するものではなく、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						
* 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抵触するものではなく、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 10.08.2022	国際調査報告の発送日 23.08.2022									
名称及びあて先 日本国特許庁(ISA/JP) 〒100-8915 日本国 東京都千代田区霞が関三丁目4番3号	権限のある職員（特許庁審査官） 上島 拓也 5S 6293 電話番号 03-3581-1101 内線 3546									

国際調査報告
 パテントファミリーに関する情報

国際出願番号

PCT/JP2022/026872

引用文献			公表日	パテントファミリー文献	公表日
JP	2008-015786	A	24.01.2008	US 2008/0034092 A1 段落[0049]-[0090], [0118]- [0119], 図1, 5, 16 CN 101102247 A	
JP	2004-341578	A	02.12.2004	(ファミリーなし)	
JP	2003-218873	A	31.07.2003	US 2003/0167411 A1 段落[0034]-[0037], 図7-9	