



(43) 国際公開日
2008 年 10 月 30 日 (30.10.2008)

PCT

(10) 国際公開番号
WO 2008/129641 A1

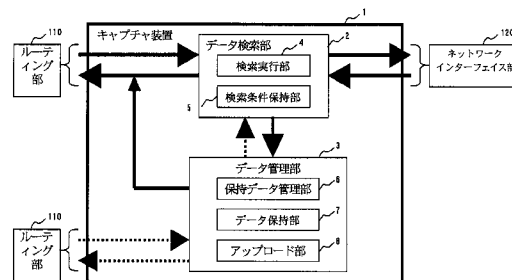
- (51) 国際特許分類:
H04L 12/56 (2006.01) H04L 29/14 (2006.01) 上小田中 4 丁目 1 番 1 号 富士通株式会社内 Kanagawa (JP).
- (21) 国際出願番号: PCT/JP2007/058141 (74) 代理人: 赤澤 日出夫 (AKAZAWA, Hideo); 〒1640001 東京都中野区中野 5-67-3 タガシンビル 6 階 Tokyo (JP).
- (22) 国際出願日: 2007 年 4 月 13 日 (13.04.2007)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (71) 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): 佐藤 雅一 (SATO, Masakazu) [JP/JP]; 〒2118588 神奈川県川崎市中原区
- (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, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

[続葉有]

(54) Title: CAPTURE DEVICE AND CAPTURE METHOD

(54) 発明の名称: キャプチャ装置、キャプチャ方法

[図2]



110 ROUTING PART
1 CAPTURE DEVICE
2 DATA SEARCH PART
4 SEARCH PERFORMING SECTION
5 SEARCH CONDITION HOLDING SECTION
3 DATA MANAGEMENT PART
6 HELD DATA MANAGEMENT SECTION
7 DATA HOLDING SECTION
8 UPLOADING SECTION
120 NETWORK INTERFACE PART

(57) Abstract: A capture device which can be connected with at least one communication path and which captures communication data passing through the communication path and stores it in a storage medium. The capture device is provided with a search condition holding section (5) and a held data management section (6) which hold at least one sets of position information of an area set to the storage medium and the condition of the communication data stored in the area, a search performing section (4) which captures communication data meeting the condition held by the search condition holding section (5) out of the communication data passing through the communication paths as matching data, and a held data management section (6) and a data holding section (7) which capture the position information of the storing area being an area corresponding to the condition suiting the matching data and store the matching data in the storing area.

(57) 要約: 少なくとも1つの通信経路に接続されることができ、該通信経路を通過する通信データを取得して記憶媒体に格納するキャプチャ装置であって、前記記憶媒体に設定された領域の位置情報と該領域に格納する通信データの条件との組を少なくとも1つ保持する検索条件保持部5および保持データ管理部6と、前記通信経路を通過する通信データの

[続葉有]



WO 2008/129641 A1



(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, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK,

TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

明 細 書

キャプチャ装置、キャプチャ方法

技術分野

[0001] 本発明は、パケットキャプチャを行うためのキャプチャ装置、キャプチャ方法に関するものである。

背景技術

[0002] 近年のセキュリティ意識の高まりに伴い、ネットワーク内の異常を検知し、問題解析のためその通信データを保持したいという要望が高まっている。

[0003] このような状況のなかで、更に、ネットワーク中継装置(以下、中継装置)にて特定の通信データを識別し、一時的に保持し、中継装置外の管理装置にて通信データの解析をしたいという要望も高まっている。

[0004] 中継装置を流れる通信データを保持する方法として、中継装置外に、RMON (Remote network MONitoring) プローブ装置や、LANアナライザ装置などの外部キャプチャ装置を取り付ける方法が一般的に知られている。

[0005] 外部キャプチャ装置は、ネットワーク間を相互接続している中継装置の各々のネットワークと中継装置との間に取り付けられることで、ネットワーク間に流れるデータを検索し、保持するものである。また外部キャプチャ装置でキャプチャされたデータは、外部キャプチャ装置自体にて解析されたり、外部キャプチャ装置外にある管理装置と呼ばれる装置にアップロードされた後、閲覧、保存され、解析されたりする。

[0006] 最近では、中継装置内部に外部キャプチャ装置相当の機能を内蔵した中継装置も現れている。このような中継装置は、内部に流れるデータをキャプチャし、キャプチャされたデータをすべて管理装置にアップロードする。この場合のキャプチャされたデータは、外部の管理装置にて本当に必要なデータを再検索された後、解析されることを要する。また、キャプチャデータのうち、本当に必要なデータがキャプチャされず、不必要なキャプチャデータで中継装置内部のキャプチャメモリが一杯となることもあった。

[0007] また中継装置が輻輳状態となった場合、キャプチャメモリがフルになりデータが破

棄された場合、破棄されたという情報が保持されないため、管理装置にてキャプチャデータを解析する際、ユーザはデータがネットワーク内で破棄されたのか、中継装置で破棄されたのかがわからず、キャプチャデータの解析に支障をきたすこともあった。

- [0008] なお、本発明の関連ある従来技術として、特定のアドレス、特定のプロトコルなどの条件によってパケットの取捨選択を行うパケットフィルタにおいて、フィルタ条件を複数に分割して保存しておくメモリと、これらの分割したフィルタ条件を前記メモリから読み出し、それぞれにおいて対応するパケットの一部分と比較判定を行うハードウェアにより構成された比較判定機能部と、これらの判定結果を論理和や論理積によって結合し、この結果によってパケットの取捨を決定するハードウェアにより構成された比較結果結合部とを設けることで、複雑な処理が可能で、且つ回路規模の小さい高速なパケットフィルタ機構を提供するパケットフィルタが公知技術として知られている（例えば、特許文献1参照）。

特許文献1：特開2001－69173号公報

発明の開示

発明が解決しようとする課題

- [0009] しかしながら、特許文献1にて開示されたパケットフィルタは、フィルタ条件によってパケットの取捨選択を行うことができるものの、一旦取得されたパケットのその後の管理は全て同一の扱いとなり、取得する必要があるがさほど重要でないデータでメモリがフルになり、最重要なデータが取得されない可能性がある。
- [0010] また、特許文献1にて開示されたパケットフィルタにおいても、メモリがフルになりデータが破棄された場合、破棄されたという情報が保持されない。よってユーザは、パケットが無くなった原因がメモリのフルによる破棄なのか、またはネットワーク上のトラフィックの影響によるデータ破棄なのかを知ることができない。
- [0011] 本発明は上述した問題点を解決するためになされたものであり、グループ単位でキャプチャデータを保持し、アップロードし、さらに破棄した場合の破棄情報を保持することで、キャプチャデータの解析が容易となるキャプチャ装置およびそのキャプチャ方法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

[0012] 上述した課題を解決するため、本発明は、少なくとも1つの通信経路に接続されることができ、該通信経路を通過する通信データを取得して記憶媒体に格納するキャプチャ装置であって、前記記憶媒体に設定された領域の位置情報と該領域に格納する通信データの条件との組を少なくとも1つ保持する保持部と、前記通信経路を通過する通信データのうち、前記保持部に保持された条件に適合する通信データを適合データとして取得する取得部と、前記適合データに適合する条件に対応する領域である格納領域の位置情報を取得し、該格納領域へ前記適合データを格納する格納部とを備えるものである。

[0013] また上述した課題を解決するため、本発明は、少なくとも1つの通信経路に接続されることができ、該通信経路を通過する通信データを取得して記憶媒体に格納するキャプチャ装置であって、前記通信経路を通過する通信データのうち、設定された条件に適合する通信データを適合データとして取得する取得部と、前記記憶媒体に設定された領域へ前記適合データを格納する格納部と、前記格納部が前記適合データを前記領域へ格納する際、該領域の余地が所定の条件を満たす場合、所定の規則に基づいてデータの破棄を行う破棄部と、前記破棄部により行われた破棄の結果に関する情報を破棄情報として保持する破棄情報保持部とを備えるものである。

[0014] また上述した課題を解決するため、本発明は、通信経路を通過する通信データを取得して記憶媒体に格納するキャプチャ方法であって、前記記憶媒体に設定された領域の位置情報と該領域に格納する通信データの条件との組を取得する組情報取得ステップと、前記通信経路を通過する通信データのうち、前記組情報取得ステップにて取得された条件に適合する通信データを適合データとして取得する適合データ取得ステップと、前記適合データに適合する条件に対応する領域である格納領域の位置情報を取得し、該格納領域へ前記適合データを格納する格納ステップとを実行するものである。

図面の簡単な説明

[0015] [図1]本実施の形態に係る中継装置の構成の一例を示すブロック図である。

[図2]本実施の形態に係るキャプチャ装置の機能の一例を示すブロック図である。

[図3]本実施の形態に係る検索条件保持部にて保持される検索条件および検索条

件式の一例を示す図である。

[図4]本実施の形態に係るキャプチャグループを管理している管理テーブルを示す図である。

[図5]本実施の形態に係るデータ保持部の区分領域の比率を示す図である。

[図6]本実施の形態に係るリードポインタ、ライトポインタの動きを示す図である。

[図7]本実施の形態に係るネットワークインターフェイス部からルーティング部へ流れる通信データに対するキャプチャ処理を示すフローチャートである。

[図8]本実施の形態に係るルーティング部からネットワークインターフェイス部へ流れる通信データに対するキャプチャ処理を示すフローチャートである。

[図9]本実施の形態に係る外部の管理装置からのアップロード要求をルーティング部が受け付けた場合のアップロード処理を示すフローチャートである。

[図10]本実施の形態に係るアップロード部における内部アップロード処理を示すフローチャートである。

[図11]本実施の形態に係るアップロード部からルーティング部へのアップロード起動要求処理を示すフローチャートである。

[図12]本実施の形態に係る起動要求フラグに基づいたルーティング部側のアップロード処理を示すフローチャートである。

[図13]本実施の形態に係る最古のキャプチャデータから順に破棄していく方式を示す図である。

[図14]本実施の形態に係る最新のキャプチャデータから順に破棄していく方式を示す図である。

発明を実施するための最良の形態

[0016] 以下、本発明の実施の形態について図面を参照しつつ説明する。

[0017] まず、本実施の形態に係る中継装置の構成について図1を参照しつつ説明する。

[0018] 中継装置100は、ルーティング部110、キャプチャ装置1、ネットワークインターフェイス部120から構成されている。ネットワークインターフェイス部120のうち、いずれかのネットワークインターフェイスは、キャプチャされたデータ(適合データ)をユーザが閲覧、解析、保存するための外部の管理装置と接続されている。

- [0019] ルーティング部110は、転送処理を行うものであり、ネットワークインターフェイス部120にて受信された通信データを、最適な経路を選択して別のネットワークに送信する。また、ルーティング部110は中央演算処理装置であるCPU111、記憶装置であるメモリ112にて構成されている。
- [0020] ネットワークインターフェイス部120は、通信データの物理的な入出力を行う。
- [0021] キャプチャ装置1は、ルーティング部110とネットワークインターフェイス部120との間に備えられることで、ルーティング部110とネットワークインターフェイス部120との間を流れる通信データを所定の検索条件および検索条件式に基づきキャプチャする。またキャプチャ装置1は、キャプチャした通信データ(以下、キャプチャデータ)を保持し、外部の管理装置へ保持したキャプチャデータをアップロードする。
- [0022] 尚、本実施の形態に係るキャプチャ装置1は、中継装置内でも、中継装置の外部に備えてもよい。
- [0023] 次に、キャプチャ装置1の機能を図2の機能ブロックを参照しつつ説明する。尚、図2中の実線矢印は通信データ(またはキャプチャデータ)の流れを示し、破線矢印は制御データの流れを示している。
- [0024] キャプチャ装置1は、データ検索部2、データ管理部3を備える。データ検索部2は、データ管理部3、ルーティング部110、ネットワークインターフェイス部120と接続されており、ルーティング部110やネットワークインターフェイス部120からの通信データを検索する。またデータ検索部2は、検索実行部4、検索条件保持部5を備える。
- [0025] 検索条件保持部5は、キャプチャしたい通信データのビット列を1つの検索条件として複数登録される。また検索条件保持部5は、登録された検索条件を組み合わせることで検索条件式としてグループ化することで検索条件を保持する。
- [0026] ここで、検索条件保持部5にて保持される検索条件および検索条件式の一例を図3に示す。検索条件式は検索条件番号として管理される。例えば検索条件番号1は、所定のTCPポート番号を検索条件式としたものであり、検索条件番号2は、相手先IP Address、送信元IP Addressおよび相手先の所定のTCPポート番号の各検索条件をAND条件の検索条件式でグループ化したものである。また検索条件番号3は、ネットワークインターフェイスAを検索条件式とし、ネットワークインターフェイスAに流れる

全ての通信データをキャプチャ対象と定義するものである。尚、検索条件番号1および検索条件番号3は、1つの検索条件のみであるため、検索条件式と検索条件が一致している。

[0027] このように検索条件が複数登録され、さらに検索条件番号2のように検索条件が検索条件式としてグループ化がなされることで、通信データのデータ群ごとの判別が可能となり、更にそれぞれの検索条件を組み合わせた検索が可能となる。上述の検索条件以外にも、ネットワークインターフェイス毎の受信のみ、送信のみを対象とした検索や、実際の通信データの通信内容を識別しての検索が可能である。

[0028] 検索実行部4は、通信データの中身を検索する能力を有しており、検索条件保持部5で保持されている検索条件式と、通信データを比較することにより、キャプチャすべきデータとそうでないデータを判別し、検索条件式に適合したキャプチャデータ(適合データ)を取得する。またキャプチャデータの採取時間、キャプチャデータの PACKET レングス、破棄情報(後述)等の制御情報も同時に取得する。

[0029] 上述のように、データ検索部2の検索実行部4と検索条件保持部5の機能により、通過する通信データを検索し、検索条件式に適合した通信データをキャプチャデータとして判定し、データ管理部3に通知することが可能となる。

[0030] データ管理部3は、ルーティング部110、データ検索部2と接続されており、データ検索部2にてキャプチャされたキャプチャデータを管理する。またデータ管理部3は、保持データ管理部6、データ保持部7、およびアップロード部8を備える。

[0031] 保持データ管理部6は、検索実行部4によってキャプチャされたキャプチャデータを、データ保持部7に内包されるキャプチャメモリに保持する。また保持データ管理部6は、キャプチャメモリの記憶領域を複数に区分し、区分領域(領域)ごとに管理する。

[0032] 保持データ管理部6は、更にキャプチャグループというグループを構成することで、キャプチャデータを管理する。ここで、図4にキャプチャグループを管理している管理テーブル(組)を参照し、キャプチャグループについて説明する。キャプチャグループは、キャプチャデータを識別するための識別番号(キャプチャグループ番号)、キャプチャデータを管理するためのキャプチャメモリ上の開始アドレスおよび終了アドレス(位置情報)、および検索条件保持部6に保持された検索条件番号(複数の検索条件

番号を登録することが可能で、登録された検索条件番号はOR条件で結合) (条件) を主な項目として構成されている。尚、キャプチャメモリ上の開始アドレスおよび終了アドレスの範囲がキャプチャグループの区分領域となる。

- [0033] 保持データ管理部6は、検索条件番号と区分領域を対応付けたキャプチャグループを管理することで、検索実行部4によって検索されたキャプチャデータを、対応する区分領域に保持することができる。すなわち、検索実行部4による検索時に用いられた検索条件式と検索条件番号との対応関係(図3)および検索条件番号と区分領域との対応関係(図4の管理テーブル)から、検索実行部4による検索時に用いられた検索条件式と区分領域との対応が導かれ、この検索条件式にて検索されたキャプチャデータが、対応する区分領域に保持される。
- [0034] 保持データ管理部6は、各キャプチャグループの開始アドレスおよび終了アドレスの項目が変更されることで、図5に示すようにデータ保持部7に対しキャプチャグループごとの区分領域の比率を変更させることができる。保持データ管理部6は、例えば図5のパターン1のように全キャプチャグループの区分領域を同一の比率にさせることができ、またパターン2のようにキャプチャグループ0は、データの重要度が高くまた通信データ量が多量であるため区分領域の比率を多くすることができる。
- [0035] このように保持データ管理部6によって、区分領域の比率を条件ごとに変えることができるため、ユーザは保持対象のデータ属性、予想されるデータ量および緊急度に応じたデータの保持が可能となる。
- [0036] またキャプチャグループは、上述以外に、ルーティング部110が通常の転送処理とキャプチャデータのアップロード処理(送信処理)の方を優先的に実行させるためのフラグ(優先FLG)、キャプチャデータの破棄の方式を決定するフラグ(破棄方式FLG)、キャプチャデータによって区分領域が満たされそうになった場合にアップロード起動要求を発行する場合の閾値(アップロード起動要求閾値)の各項目によって構成されている。これらの項目に関しては後述する。
- [0037] 更に、保持データ管理部6には、制御情報の書き込み機能があり、制御情報をキャプチャデータと1対1で対応させ、書き込む機能を有する。
- [0038] データ保持部7は、実メモリ(キャプチャメモリ)のことであり、保持データ管理部6の

管理に基づきキャプチャデータおよび制御情報が格納される。

- [0039] アップロード部8は、データ保持部7にて保持されている区分領域毎のキャプチャデータと制御情報を、ルーティング部110により外部の管理装置へ転送させる。また、後述するリードポインタ、ライトポインタの制御も行う。
- [0040] ここで、保持データ管理部6による各区分領域へのキャプチャデータの入力、およびアップロード部8による各区分領域からのキャプチャデータの出力に関する、区分領域の管理について図6を参照しつつ説明する。
- [0041] 図6は、1つの区分領域におけるキャプチャメモリの3つの使用状態(キャプチャ開始時、キャプチャ通常動作時、キャプチャバッファフル時)を示しており、#0、#1、・・・、#nは、各キャプチャデータおよび制御情報が格納されるアドレスを示している。アップロード部8は、各区分領域に対し、保持データ管理部6による入力、およびアップロード部8による出力をそれぞれライトポインタ(格納位置情報)、リードポインタ(送信位置情報)で管理する。
- [0042] 中継装置100の電源投入直後は、まだデータがキャプチャメモリに存在しないため、ライトポインタ、リードポインタ共に#0の記憶領域を指している(図6の「キャプチャ開始時」参照)。
- [0043] 保持データ管理部6による書込みが行われる場合、ライトポインタが指し示すアドレスにデータが書き込まれ、ライトポインタは1キャプチャデータおよび1制御情報分次のアドレスへ移動する。またアップロード部8による出力が行われる場合、リードポインタが指し示すアドレスのデータが読み込まれ、リードポインタは1キャプチャデータおよび1制御情報分次のアドレスへ移動する。
- [0044] 図6の「キャプチャ通常動作時」の例では、保持データ管理部6は#18のアドレスにデータを書き込み、アップロード部8は#3のアドレスのデータを読み込む。尚、区分領域はそれぞれリングバッファであるため、終了アドレス(#n)へライトポインタ(またはリードポインタ)が到達した場合、次回は開始アドレス(#0)にライトポインタ(またはリードポインタ)は移動し、キャプチャデータおよび制御情報が書き込まれる。
- [0045] 尚、キャプチャデータによって区分領域の容量がフルになった場合、図6の「キャプチャバッファフル時」に示すように、リードポインタとライトポインタは同じアドレスを示

すことになる。

- [0046] また、保持データ管理部6における書き込み完了後のライトポインタのアドレスの位置は、書き込み後ライトポインタを移動させる場合と、ライトポインタを移動させた後書き込む場合とでは、1データ分ずれが生じることに留意する。アップロード部8における読出し処理も同様である。
- [0047] 次に、本実施の形態の処理をフローチャートを参照しつつ説明する。本実施の形態における処理は、キャプチャ処理およびアップロード処理に分けることができる。
- [0048] まず、キャプチャ処理について説明する。ネットワークインターフェイス部120からルーティング部110へ流れる通信データをキャプチャする処理のフローチャートを図7に示す。
- [0049] ネットワークインターフェイス部120が外部より通信データを受信する(ステップS1)と、検索実行部4は、検索条件式に基づき通信データを検索する(ステップS2)。ここで、通信データが検索条件式のいずれかに適合した場合(ステップS2、検索適合)、検索実行部4は、適合した検索条件式の検索条件番号とキャプチャされた通信データ(キャプチャデータ)を、保持データ管理部6に出力する。
- [0050] また検索実行部4は、現在の時間を取得し、キャプチャデータのレングス計算および破棄情報に値をセット(破棄動作ではないので数値“0”がセットされる)し、これらの情報を制御情報として、キャプチャデータと一緒に保持データ管理部6に出力する。
- [0051] 保持データ管理部6は、検索実行部4より取得した検索条件番号と、管理テーブル(図4参照)から対象キャプチャグループを決定し(ステップS3)、対象キャプチャグループに対応する区分領域内のライトポインタが指し示すアドレスに、キャプチャデータおよび制御情報を書き込む。その後、アップロード部8は、書き込まれた区分領域のライトポインタに1キャプチャデータおよび1制御情報分の値を加算し、ライトポインタが指し示すアドレスを1キャプチャデータおよび制御情報のサイズ分移動させる(ステップS4)。
- [0052] 尚、本実施の形態においては、アップロード部8が区分領域のライトポインタに1キャプチャグループ分の値を加算したが、保持データ管理部6が行ってもよい。また、保持データ管理部6によってキャプチャデータが書き込まれた後に、アップロード部8

はライトポインタを移動させたが、アップロード部8によってライトポインタが移動された後に、保持データ管理部6がキャプチャデータを書き込こんでもよい。

[0053] その後、通信データはルーティング部110に転送され(ステップS5)、従来通りの転送処理がなされる。

[0054] 一方、検索実行部4による検索が適合しなかった場合(ステップS2、検索不適合)、通信データはそのままルーティング部110に転送され(ステップS5)、従来通りの通信データ中継処理がなされる。

[0055] 以上の動作を繰り返すことにより、パケットのキャプチャが可能となる。

[0056] また、ルーティング部110自らがネットワークパケット(通信データ)を生成し、ルーティング部110自らの情報をネットワークインターフェイス部120を介して外部に送信する場合もあり、そのような通信データもキャプチャ対象とする必要がある。次にルーティング部110からネットワークインターフェイス部120へ流れる通信データをキャプチャする処理のフローチャートを図8に示し、処理内容を説明する。

[0057] ルーティング部110は、ネットワークインターフェイス部120に向けた通信データを送信し(ステップS11)、検索実行部4は、検索処理を行う(ステップS12)。検索実行部4による検索が適合した場合(ステップS12、検索適合)、上述の対象キャプチャグループを決定処理、キャプチャデータ書込み処理が行われ(ステップS13、ステップS14)、ネットワークインターフェイス部120に通信データが転送され(ステップS15)、外部に送信される。尚、ステップS12、ステップS13、ステップS14の処理は、それぞれステップS2、ステップS3、ステップS4の処理と同様である。

[0058] 一方、検索実行部4による検索が適合しなかった場合(ステップS12、検索不適合)、通信データはそのままネットワークインターフェイス部120に転送され(ステップS15)、外部に送信される。

[0059] 上述の処理によりキャプチャデータがデータ保持部7の区分領域にストックされてくると、区分領域がキャプチャデータでフルになってしまう。よって、キャプチャデータの読み出し(アップロード)処理を行うことで外部の管理装置にキャプチャデータを転送し、区分領域内のキャプチャデータを削除する必要がある。

[0060] ここで、アップロード処理の種類について説明する。まず、アップロード処理は、ル

ーティング部110における外部の管理装置へのアップロード処理(外部アップロード処理)、アップロード部8におけるルーティング部110へのアップロード処理(内部アップロード処理)がある。またアップロード処理は、外部の管理装置からルーティング部110に対しアップロード要求がなされることで開始される場合と、アップロード部8からルーティング部110に対しアップロード要求がなされることで開始される場合とがある。

- [0061] 図9のフローチャートを参照しつつ、外部の管理装置からのアップロード要求をルーティング部110が受け付けた場合のアップロード処理を説明する。またルーティング部110は、必要に応じてアップロードしたいキャプチャデータ数(もしくは全て)を指定することができるが、本実施の形態では、キャプチャグループnに対応する区分領域から、x個のキャプチャデータがアップロードされる例として説明する。尚、図9にて示した処理は、ステップS24以外はルーティング部110上のソフトウェアにより行われるが、アップロード部8にて行われてもよい。
- [0062] アップロード要求を受け付けたルーティング部110は、データ保持部7のキャプチャグループnに対応する区分領域のライトポイントとリードポイントを確認することで(ステップS21)、アップロード可能なキャプチャデータの有無を判定する(ステップS22)。アップロード可能なキャプチャデータがあった場合(ステップS22、Yes)、ルーティング部110は、xが0かを判定する(ステップS23)。xが0でない場合(ステップS23、No)、アップロード部8に対し内部アップロード処理(後述)を行わせることで、ルーティング部110はキャプチャデータを取得する(ステップS24)。
- [0063] 内部アップロード処理が終了したら、ルーティング部110はxに対し1減算させ(ステップS25)、ステップS23の判定処理に処理を戻す。xが0になるまでステップS24、ステップS25の処理が繰り返される。xが0になった場合(ステップS23、Yes)、ルーティング部110は、ステップS24にて取得されたキャプチャデータおよび制御情報(ともにx個分)をFTPパケット化し(ステップS26)、外部の管理装置に対しFTPプロトコルにてキャプチャデータを送信する(ステップS27、ステップS28)。
- [0064] 外部の管理装置への送信が完了した場合(ステップS28、Yes)、処理は終了する。

- [0065] また、ステップS22にてアップロード可能なキャプチャデータがなかった場合(ステップS22、No)、ルーティング部110は、外部の管理装置に対し転送するキャプチャデータがない旨を通知する(ステップS29)。
- [0066] 次に、アップロード部8における内部アップロード処理について、図10のフローチャートを参照しつつ説明する。尚、内部アップロード処理は図9のステップS24に対応する。
- [0067] アップロード部8は、キャプチャグループnに対応する区分領域に格納されたキャプチャデータおよび制御情報を1データ分読み出す(ステップS31)。尚、アップロード部8は、現在のリードポインタにて指し示したアドレスにあるキャプチャデータおよび制御情報を読み出す。その後、アップロード部8は、読み出したキャプチャデータおよび制御情報をルーティング部110に転送し(ステップS32)、データ保持部7のキャプチャグループnに対応する区分領域のリードポインタを1キャプチャデータ分および1制御情報分加算する(ステップS33)。
- [0068] 尚、アップロード部8はデータを読み出してからリードポインタに加算したが、リードポインタに加算してからデータを読み出してもよい。
- [0069] 通常のアップロード処理は、上述のように外部の管理装置からのアップロード要求をルーティング部110が受け付けた場合に実施される。しかしながら、何らかの理由で外部の管理装置からのアップロード要求がこない状態が続き、アップロード部8が管理しているライトポインタとリードポインタの差分がアップロード閾値(図4に示した管理テーブル上にあるアップロード起動要求閾値)を下回った場合、アップロード部8は、対象キャプチャグループに対応した区分領域がフルになるのを防ぐため、ルーティング部110に対しアップロード起動要求を発行する。
- [0070] このようなアップロード処理は、アップロード部8からのルーティング部110に対するアップロード起動要求処理をトリガとして行われる。ここで、アップロード部8からのルーティング部110へのアップロード起動要求処理を図11に示す。
- [0071] アップロード部8は、所定のキャプチャグループ(ここでは上述同様キャプチャグループnとする)に対応する区分領域のライトポインタとリードポインタとの差分を確認し、管理テーブル(図4参照)のアップロード起動要求閾値(所定の閾値)以下かどうか

を判定する(ステップS41)。ここで、差分がアップロード起動要求閾値以下である場合(ステップS41、Yes)、アップロード部8は、ルーティング部110に対し起動要求フラグをONにすることで起動要求を行う(ステップS42)。また、差分がアップロード起動要求閾値より上である場合(ステップS41、No)、アップロード部8は、ルーティング部110へ起動要求フラグをOFFにすることで起動要求を停止する(ステップS43)。尚、起動要求フラグのONまたはOFFは、本実施の形態ではルーティング部110内で保持され、管理されているものとするが、アップロード部8内部にて保持され、管理されていても構わない。

[0072] 上述のアップロード部8のルーティング部110へのアップロード起動要求処理は随時行われる。

[0073] 次に、上述のように起動要求フラグに基づいたルーティング部110のアップロード処理を図12を参照しつつ説明する。ルーティング部110では、ルーティング部110が処理していたタスクをアップロード部8からのアップロード起動要求処理に切り替えることで、アップロード処理が行われる。

[0074] ルーティング部110は、起動要求フラグがONであることを確認する(ステップS51)。ここで、起動要求フラグがONである場合(ステップS51、Yes)、ルーティング部110は、アップロード部8に対対象キャプチャグループ(キャプチャグループn)に対応する区分領域に対する内部アップロード処理の実施を要求する(ステップS52)。内部アップロード処理の実施の要求を受けたアップロード部8は、内部アップロード処理を実施する(ステップS53)。尚、内部アップロード処理は上述した通りであるため、ここでの説明は省略する(図10参照)。

[0075] 内部アップロード処理が終了したら、ルーティング部110は、再度起動要求フラグがONであることを確認する(ステップS51)。このように起動要求フラグがOFFになるまで、ステップS51、ステップS52、ステップS53の処理が繰り返される。

[0076] キャプチャグループnの区分領域のライトポインタとリードポインタとの差分がアップロード起動要求閾値より上となり(図11のステップS41、ステップS43)、起動要求フラグがOFFになった場合(ステップS51、No)、ルーティング部110は、キャプチャ装置(アップロード部8)からのキャプチャデータ(起動要求フラグがONであった最中のス

テップS53処理によってストックされたキャプチャデータ) および制御情報をFTPパケット化し(ステップS54)、外部の管理装置に対しFTPプロトコルにてキャプチャデータを送信する(ステップS55、ステップS56)。

[0077] 外部の管理装置への送信が完了した場合(ステップS56、Yes)、処理は終了する。

[0078] このように、アップロード部8からのルーティング部110に対するアップロード起動要求処理によって、キャプチャデータを区分領域から破棄することなくデータキャプチャが可能となる。

[0079] しかしながら、中継装置100内でキャプチャされるべきアップロード対象のパケットが大量に伝送路上に流れた場合、キャプチャデータの保持のためのメモリライトに対し、アップロードのためのメモリリードが間に合わず、メモリライトがメモリリードに追いついてしまう。よって、対象区分領域がフルになり(所定の条件)、対象キャプチャグループのキャプチャデータの破棄が必要となる。

[0080] ここで、破棄の方式(所定の規則)について説明する。破棄の方式は、各区分領域に保持されているキャプチャデータや制御情報等のデータのうち、最古のデータから順に破棄していく方式、もしくは最新のデータから順に破棄していく方式のいずれかである。また保持データ管理部6は、キャプチャグループごとにこれら2つの破棄方式のうちいずれを採用するかを、管理テーブルの破棄方式FLG(図4参照)を用いてユーザに選択させることができる。

[0081] 最古のデータから順に破棄していく方式を図13を参照しつつ説明する。ここでは、区分領域の容量を仮にキャプチャデータおよび制御情報のデータ16セット分とし、また若い番号が最新のデータであるものとして説明する。

[0082] 図13の「キャプチャデータフル状態」に区分領域がフルになっている状態を示す。この状態で、保持データ管理部6による書込みが発生した場合、保持データ管理部6は最古のデータ(図13の「キャプチャデータフル状態」では「16」のデータ)が格納されたアドレスに、最新のデータを書き込むことで最古のデータを破棄する。そして、アップロード部8は、アップロード部8の内部で管理している破棄カウンタに1加算し、リードポインタを破棄したキャプチャデータおよび制御情報分(すなわち1キャプチャデ

ータおよび1制御情報分)だけ進めておく。

[0083] 上述の処理が保持データ管理部6による書き込みの都度行われる。

[0084] 図13の「キャプチャデータの書き込み1」に「キャプチャデータフル状態」からデータを1つ破棄した状態を示し、「キャプチャデータの書き込み2」に「キャプチャデータフル状態」からデータを2つ破棄した状態を示す。

[0085] そして、中継装置100が輻輳状態を逃れキャプチャデータおよび制御情報のアップロードが開始されると、リードポインタとライトポインタ間に充分余裕ができた状態となる。ここで、保持データ管理部6によるキャプチャデータ等の書き込みが発生した場合は、アップロード部8は、その書き込みが発生したキャプチャデータに対応する制御情報の破棄情報に破棄カウンタで数えた破棄パケット数(本例においては「2」)を書き込み、通常のキャプチャ動作に移行する(図13の「キャプチャデータの書き込み3」参照)。

[0086] 次に、最新のデータから順に破棄していく方式を図14を参照しつつ説明する。図14は、4つの状態(キャプチャデータフル状態、キャプチャデータの書き込み1、キャプチャデータの書き込み2、キャプチャデータの書き込み3)における動作を示す。上述同様、ここでも区分領域の容量を仮にキャプチャデータおよび制御情報16セット分とし、また若い番号が最新のデータであるものとして説明する。

[0087] 図14の「キャプチャデータフル状態」に区分領域がキャプチャデータで満たされている状態を示す。この状態である場合、保持データ管理部6は、最新のキャプチャデータおよび制御情報を書き込まない(よって、最新のデータは破棄される)。そして、データが破棄されている間は、アップロード部8は、内部で管理している破棄カウンタを破棄パケット分だけ増加する。

[0088] 図14の「キャプチャデータの書き込み1」に「キャプチャデータフル状態」からデータを1つ破棄した状態を示し、「キャプチャデータの書き込み2」に「キャプチャデータフル状態」からデータを2つ破棄した状態を示す。

[0089] そして、中継装置100が輻輳状態を逃れキャプチャデータおよび制御情報のアップロードが開始されると、区分領域はリードポインタとライトポインタ間に充分余裕ができた状態となる。ここで、区分領域にキャプチャデータおよび制御情報の書き込みが

発生した場合には、アップロード部8は、書き込みが発生したキャプチャデータの制御情報の破棄情報に破棄カウンタの数を書き込み、通常のキャプチャ動作に移行する(図14の「キャプチャデータの書き込み3」参照)。

[0090] 尚、上述の最古のデータから順に破棄していく方式、最新のデータから順に破棄していく方式の両方式とも、破棄カウンタの管理および破棄情報への書き込みはアップロード部8にて行われるが、保持データ管理部6にて管理および書き込みが行われてもよい。

[0091] また、本実施の形態においては、上述の破棄方式は区分領域に対して適用しているが、有限である記憶領域を有する記憶媒体であつたら如何なるものにも適用することができる。

[0092] 最古のデータから破棄していく方式、および最新のデータを破棄していく方式のいずれかの方式が採用されても、ユーザは外部の管理装置にてパケットの解析をする際、アップロードされたデータの制御情報の破棄情報に記載があるものを発見することにより、その記載があるキャプチャデータの以前において、キャプチャ装置1内で破棄の処理がなされたことを確認することができる。

[0093] また、ユーザはキャプチャグループごとにデータを破棄する方式を選択できるため、キャプチャするデータの特徴に合わせた運用が可能となる。

[0094] 上述の区分領域がフルの状態になる要因として、更に通常ルーティング部110は、キャプチャデータのアップロード処理より、本来の目的である転送処理を優先するため、区分領域にデータがストックされたままとなることが考えられる。次に、ルーティング部110に対し中継データの転送処理よりもキャプチャデータのアップロード処理を優先させることで、輻輳時にキャプチャしたパケットの破棄を防ぐ方法について説明する。

[0095] この方法は、管理テーブルの優先FLG(図4参照)に対し、中継処理よりアップロード処理の優先順位を高く設定するフラグが付与されることで、CPU111は、アップロード処理の要求を受けた場合、中継データの転送処理を中断する方法である。このようにすることで、キャプチャ対象のパケットが大量に伝送路上を流れ、各区分領域へのライト要求が大量に発生した場合であっても、中継装置100はキャプチャデータ

のアップロード処理を優先して処理し、ライトポインタがリードポインタを追い越すことがなくなる。

[0096] これにより、一旦キャプチャしたキャプチャデータを破棄することなく、また中継したデータとキャプチャデータが同一となることを保証する。また、重要なキャプチャグループのアップロード処理を優先して行うことができる。

[0097] 以上説明したように、本実施の形態における中継装置は、一般的なキャプチャ中継装置と異なり、検索条件を検索条件式としてグループ化でき、そのグループ単位で区分領域への保持およびアップロードが可能のため、外部の管理装置にてキャプチャデータの解析がなされる場合、ユーザは対象のキャプチャデータ群のみを解析することができる。

[0098] なお、保持部は、実施の形態における検索条件保持部5、保持データ管理部6に対応し、取得部は、実施の形態における検索実行部4に対応する。さらに格納部は、実施の形態における保持データ管理部6、データ保持部7に対応する。また送信部は、実施の形態におけるアップロード部8に対応する。また破棄部は、実施の形態における保持データ管理部6に対応し、破棄情報保持部は、実施の形態におけるアップロード部8もしくは保持データ管理部6に対応する。

産業上の利用可能性

[0099] 以上のように、本発明によれば、ユーザはキャプチャデータの解析を容易に行うことができる。

請求の範囲

- [1] 少なくとも1つの通信経路に接続されることができ、該通信経路を通過する通信データを取得して記憶媒体に格納するキャプチャ装置であって、
- 前記記憶媒体に設定された領域の位置情報と該領域に格納する通信データの条件との組を少なくとも1つ保持する保持部と、
- 前記通信経路を通過する通信データのうち、前記保持部に保持された条件に適合する通信データを適合データとして取得する取得部と、
- 前記適合データに適合する条件に対応する領域である格納領域の位置情報を取得し、該格納領域へ前記適合データを格納する格納部と、
- を備えるキャプチャ装置。
- [2] 請求項1に記載のキャプチャ装置において、
- 前記領域に格納されているデータを外部へ送信する送信処理を行う送信部を備えることを特徴とするキャプチャ装置。
- [3] 請求項2に記載のキャプチャ装置において、
- 前記送信部は、領域毎に、前記適合データを格納する位置である格納位置を設定し、前記格納部は該格納位置に適合データを書き込むとともに前記送信部は前記格納部によって書き込まれたサイズ分格納位置を移動させ、さらに前記送信部は、前記適合データを送信する位置である送信位置を設定し、該送信位置に格納されたデータを送信するとともに前記送信位置を送信したサイズ分移動させることを特徴とするキャプチャ装置。
- [4] 請求項3に記載のキャプチャ装置において、
- 前記領域は、リングバッファであり、前記格納位置および前記送信位置は前記リングバッファ上を移動することを特徴とするキャプチャ装置。
- [5] 請求項4に記載のキャプチャ装置において、
- 前記格納位置と前記送信位置との差が所定の閾値以下となった場合、前記送信部は前記適合データを外部へ送信することを特徴とするキャプチャ装置。
- [6] 請求項1に記載のキャプチャ装置において、
- 前記格納部は、前記適合データを前記格納領域へ格納する際、該格納領域の余

地が所定の条件を満たす場合、所定の規則に基づいてデータの破棄を行うことを特徴とするキャプチャ装置。

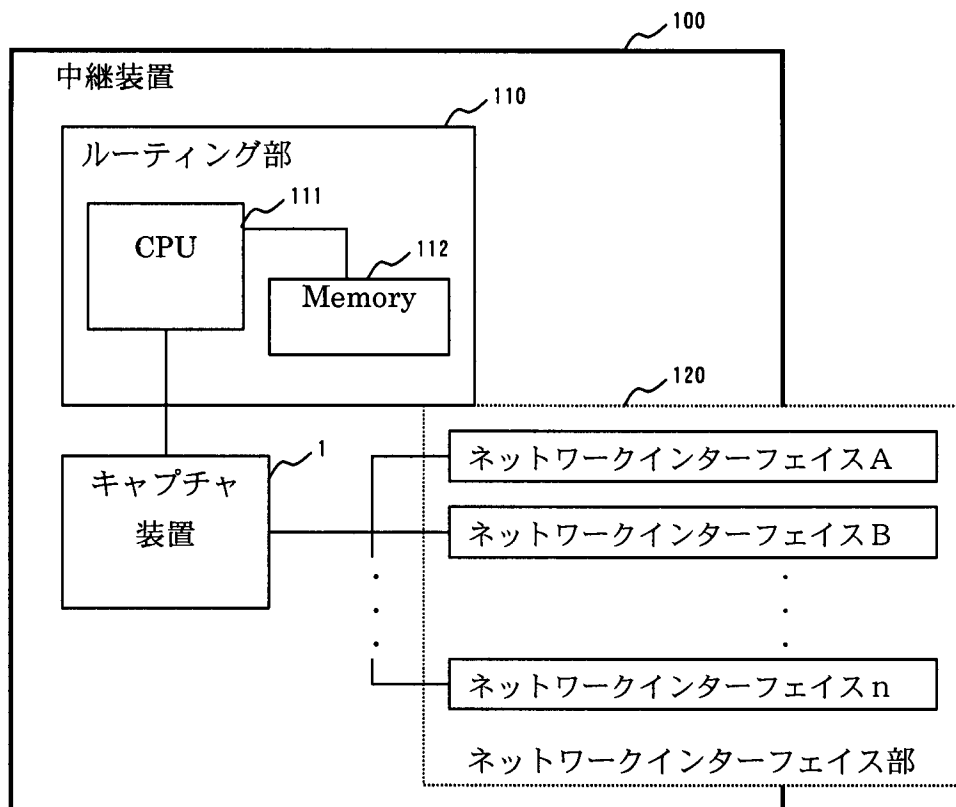
- [7] 請求項6に記載のキャプチャ装置において、
前記格納部は、更に前記破棄の結果に関する情報を破棄情報として格納すること
を特徴とするキャプチャ装置。
- [8] 請求項6に記載のキャプチャ装置において、
前記所定の規則は、前記適合データを格納する際、該適合データを破棄する規則
であることを特徴とするキャプチャ装置。
- [9] 請求項6に記載のキャプチャ装置において、
前記所定の規則は、前記適合データを格納する際、該適合データを格納する領域
に格納されているデータのうち、最古のデータを破棄する規則であることを特徴とす
るキャプチャ装置。
- [10] 請求項6に記載のキャプチャ装置において、
前記保持部は、前記領域毎に前記所定の規則を保持し、
前記格納部は、前記保持部から前記格納領域に対応する前記規則を取得し、該
規則に基づいて前記破棄を行うことを特徴とするキャプチャ装置。
- [11] 請求項2に記載のキャプチャ装置において、
前記送信部は、前記通信経路における中継処理を行い、
前記保持部は、前記領域毎に前記中継処理に対する前記送信処理の優先度を保
持し、
前記送信部は、前記優先度に基づいて前記中継処理及び前記送信処理を行うこ
とを特徴とするキャプチャ装置。
- [12] 少なくとも1つの通信経路に接続されることができ、該通信経路を通過する通信デ
ータを取得して記憶媒体に格納するキャプチャ装置であって、
前記通信経路を通過する通信データのうち、設定された条件に適合する通信デー
タを適合データとして取得する取得部と、
前記記憶媒体に設定された領域へ前記適合データを格納する格納部と、
前記格納部が前記適合データを前記領域へ格納する際、該領域の余地が所定の

条件を満たす場合、所定の規則に基づいてデータの破棄を行う破棄部と、
前記破棄部により行われた破棄の結果に関する情報を破棄情報として保持する破棄情報保持部と、
を備えるキャプチャ装置。

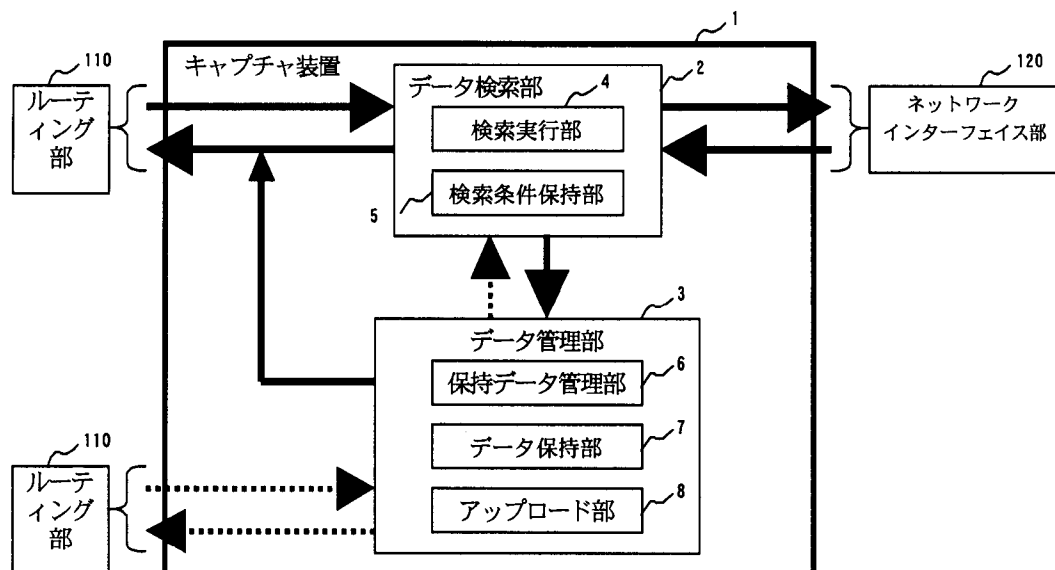
- [13] 請求項12に記載のキャプチャ装置において、
前記所定の規則は、前記格納部が前記適合データを格納する際、該適合データを破棄する規則であることを特徴とするキャプチャ装置。
- [14] 請求項12に記載のキャプチャ装置において、
前記所定の規則は、前記格納部が前記適合データを格納する際、該適合データを格納する領域に格納されているデータのうち、最古のデータを破棄する規則であることを特徴とするキャプチャ装置。
- [15] 請求項12に記載のキャプチャ装置において、
前記所定の規則を保持する保持部を備え、
前記格納部は、前記保持部から前記規則を取得し、該規則に基づいて前記破棄を行うことを特徴とするキャプチャ装置。
- [16] 請求項12に記載のキャプチャ装置において、
前記破棄情報保持部は、前記破棄部にて破棄されたデータの数を破棄情報として保持することを特徴とするキャプチャ装置。
- [17] 通信経路を通過する通信データを取得して記憶媒体に格納するキャプチャ方法であって、
前記記憶媒体に設定された領域の位置情報と該領域に格納する通信データの条件との組を取得する組情報取得ステップと、
前記通信経路を通過する通信データのうち、前記組情報取得ステップにて取得された条件に適合する通信データを適合データとして取得する適合データ取得ステップと、
前記適合データに適合する条件に対応する領域である格納領域の位置情報を取得し、該格納領域へ前記適合データを格納する格納ステップと、
を実行するキャプチャ方法。

- [18] 請求項17に記載のキャプチャ方法において、
前記領域に格納されているデータを外部へ送信する送信処理を行う送信ステップを備えることを特徴とするキャプチャ方法。
- [19] 請求項18に記載のキャプチャ方法において、
前記送信ステップは、領域毎に、前記適合データを格納する位置である格納位置を設定し、前記格納ステップは該格納位置に適合データを書き込むとともに前記送信部は前記格納ステップによって書き込まれたサイズ分格納位置を移動させ、さらに前記送信ステップは、前記適合データを送信する位置である送信位置を設定し、該送信位置に格納されたデータを送信するとともに前記送信位置を送信したサイズ分移動させることを特徴とするキャプチャ方法。
- [20] 請求項17に記載のキャプチャ方法において、
前記格納ステップは、前記適合データを前記格納領域へ格納する際、該格納領域の余地が所定の条件を満たす場合、所定の規則に基づいてデータの破棄を行うことを特徴とするキャプチャ方法。

[図1]



[図2]



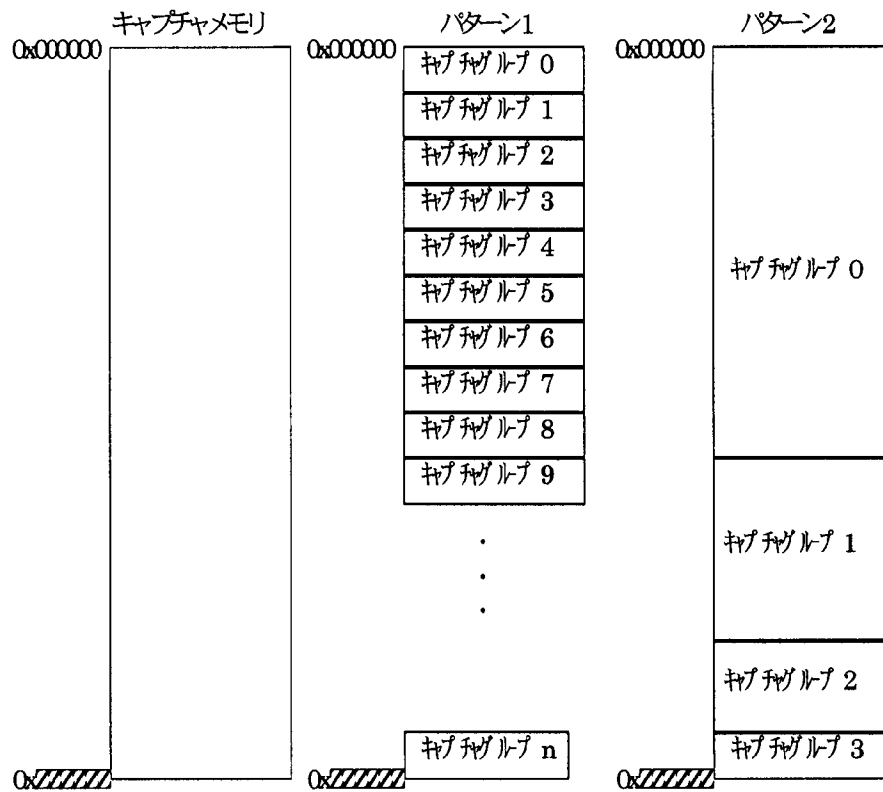
[図3]

検索条件番号	検索対象 (AND 条件)	キャプチャ内容
1	TCP PORT 番号 ZZZZ	TCP PORT 番号 ZZZZ を使った通信すべてをキャプチャ
2	相手先 IP Address AA:AA:AA:AA 送信元 IP Address BB:BB:BB:BB 相手先 TCP PORT 番号 XXXX	ステーション BB:BB:BB:BB からステーション AA:AA:AA:A 間の TCP PORT 番号 XXXX の通信をキャプチャ
3	ネットワークインターフェイス A	ネットワークインターフェイス A を流れるデータすべてをキャプチャ
・ ・ ・		

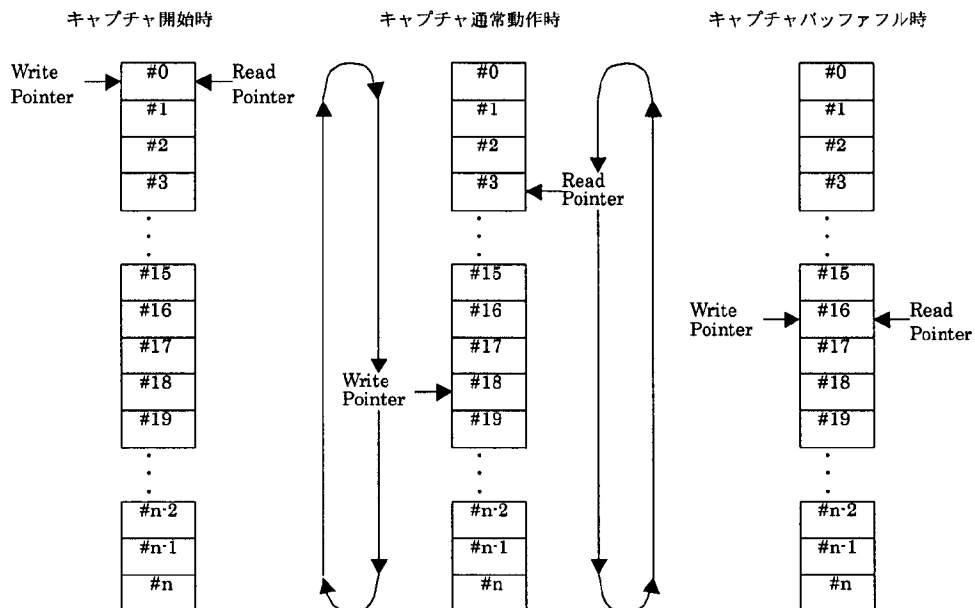
[図4]

キャプチャ グループ番号	開始アドレス	終了アドレス	優先 FLG	検索条件 番号	破棄方式 FLG	アップロード起 動要求閾値
1						
2						
・ ・ ・						

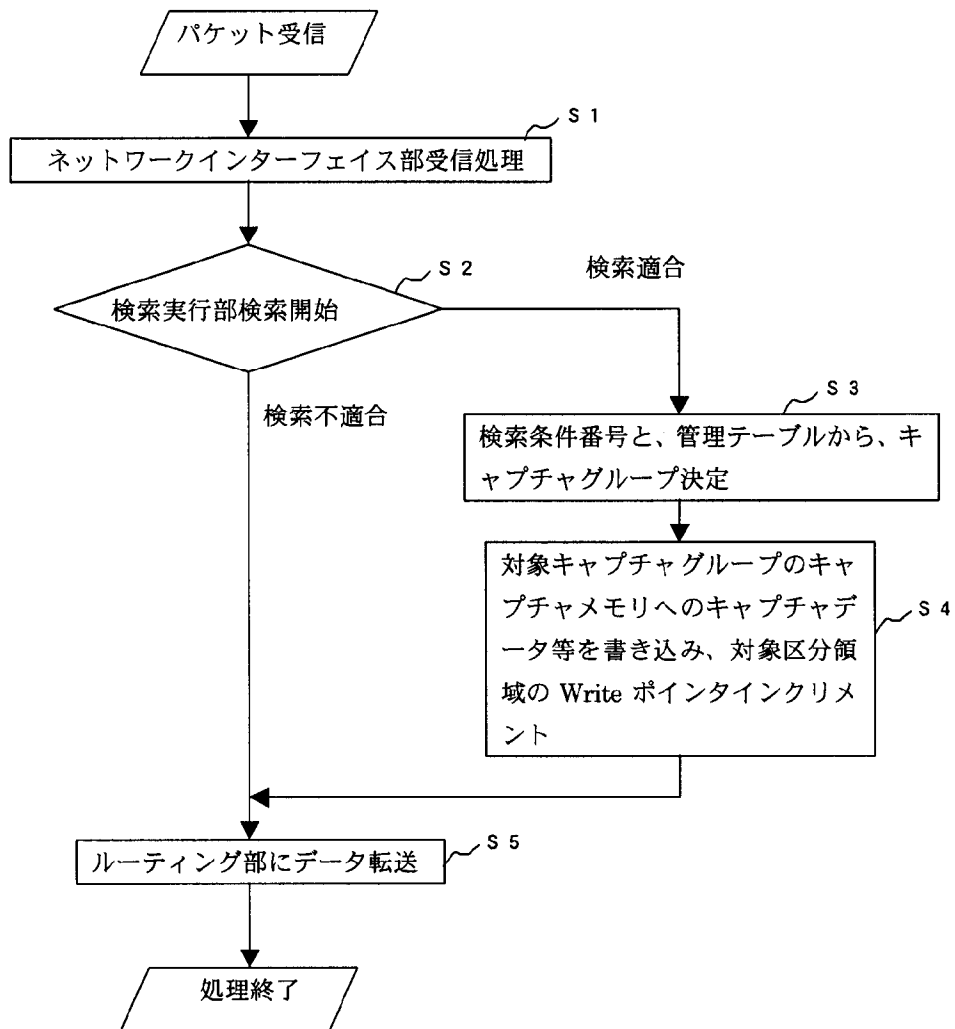
[図5]



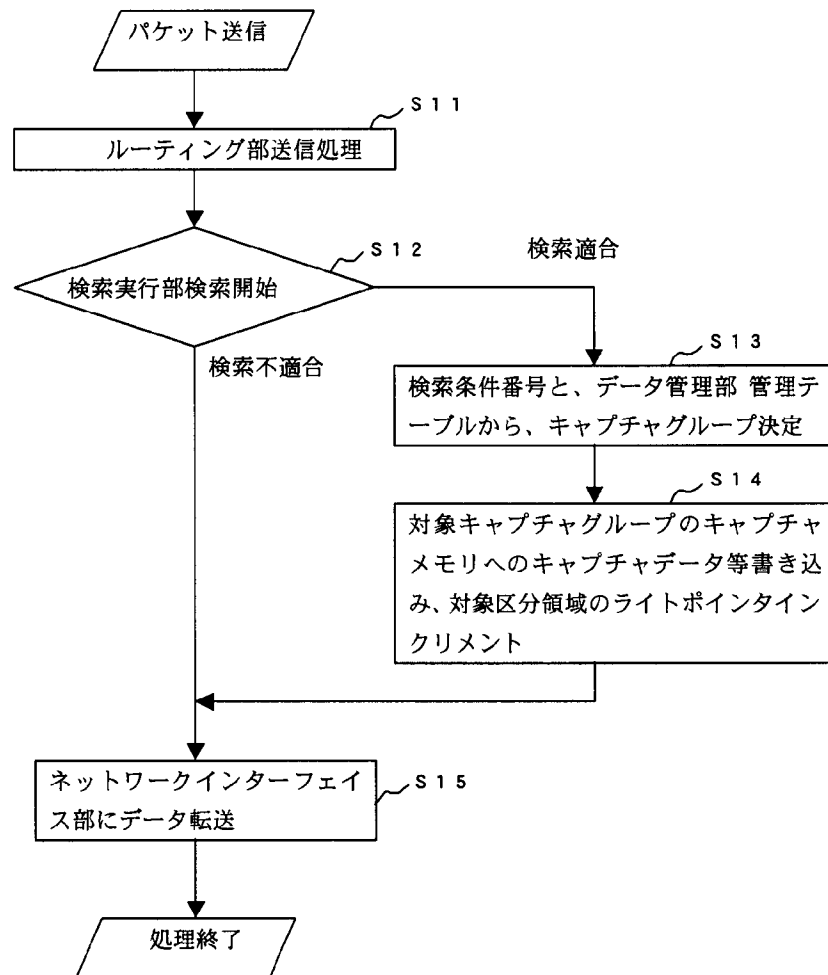
[図6]



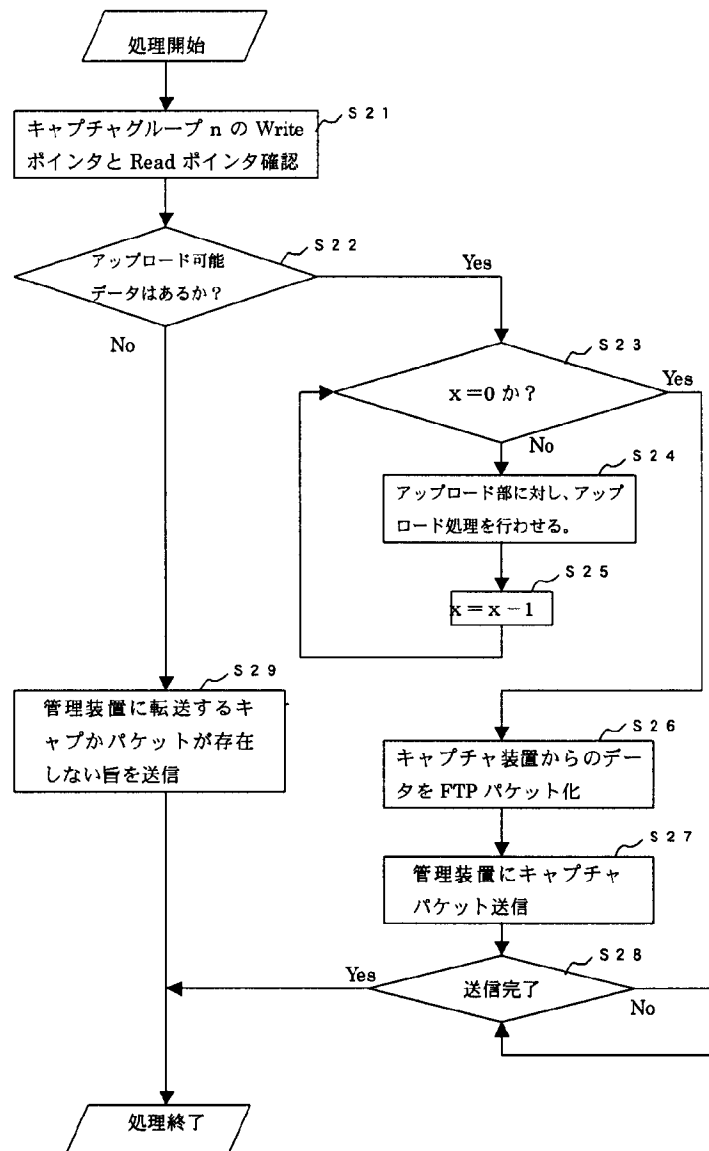
[図7]



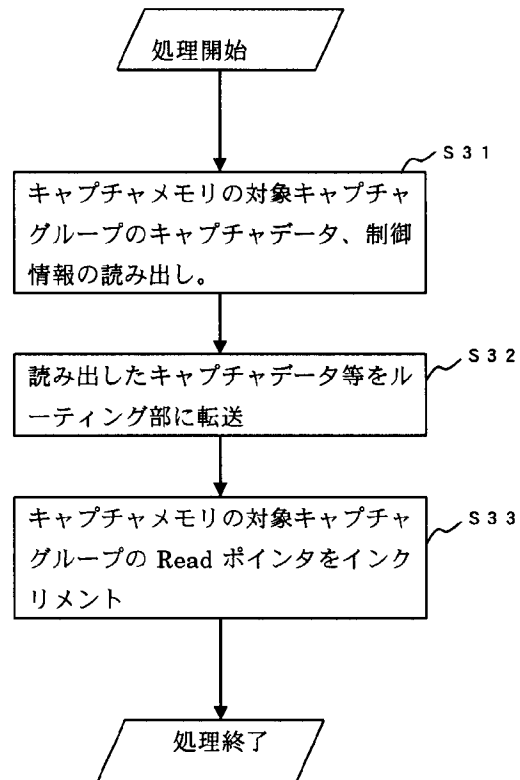
[図8]



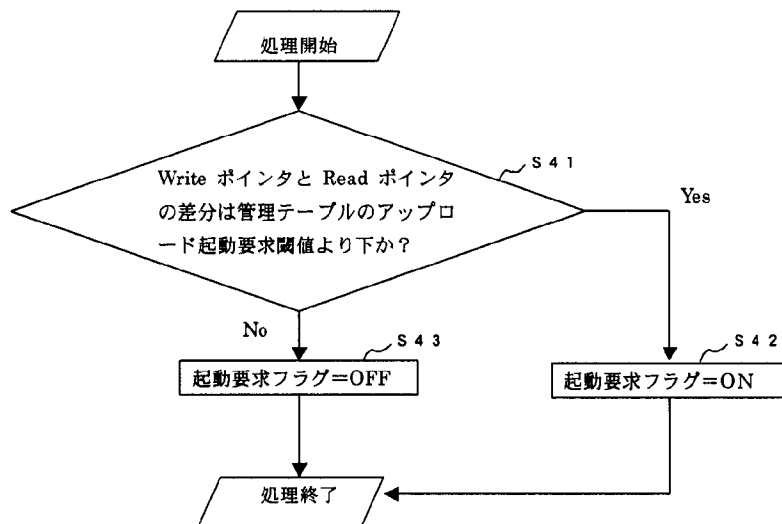
[図9]



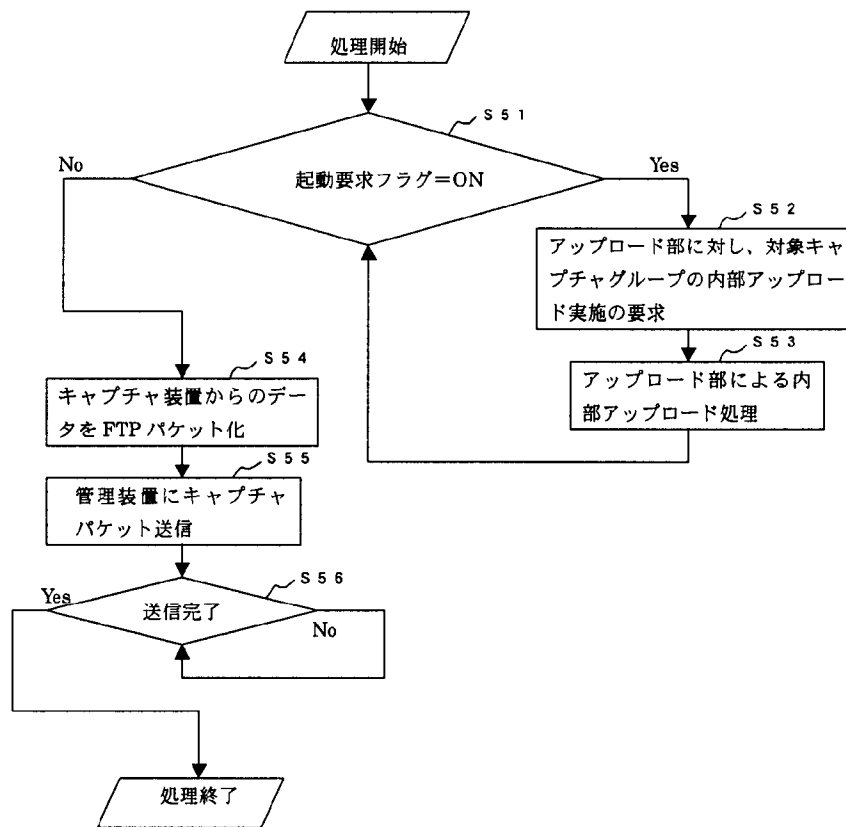
[図10]



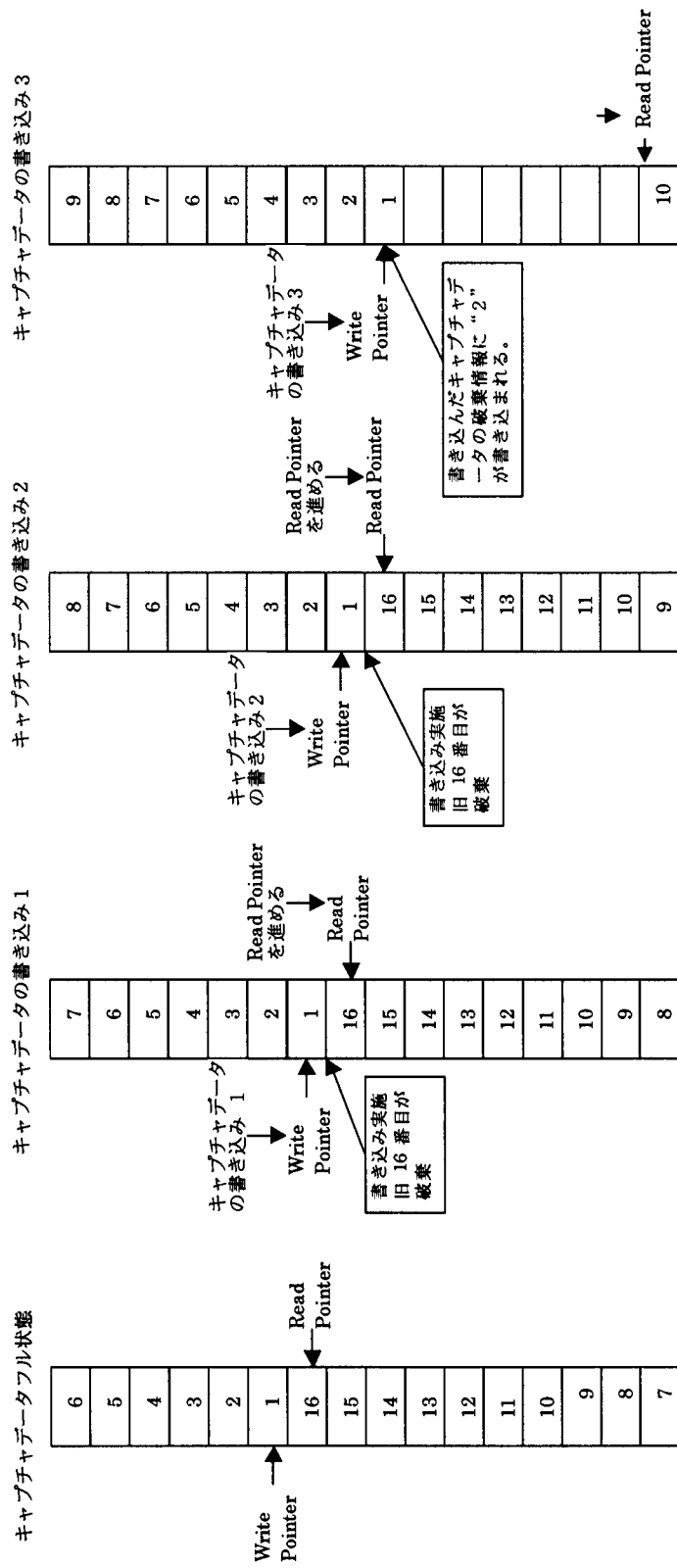
[図11]



[図12]



[図13]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2007/058141

A. CLASSIFICATION OF SUBJECT MATTER

H04L12/56(2006.01) i, H04L29/14(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)

H04L12/56, H04L29/14

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	1996-2007
Kokai Jitsuyo Shinan Koho	1971-2007	Toroku Jitsuyo Shinan Koho	1994-2007

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 A	US 2005/0132046 A1 (Erik de la Iglesia et al.), 16 June, 2005 (16.06.05), Par. No. [0033]; Fig. 5 (Family: none)	1, 17 2-11, 18-20
A	JP 2001-147834 A (Hitachi, Ltd.), 29 May, 2001 (29.05.01), Par. Nos. [0055] to [0059]; Fig. 4 & US 6732307 B1	12-16

☐ 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
07 May, 2007 (07.05.07)

Date of mailing of the international search report
15 May, 2007 (15.05.07)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

A. 発明の属する分野の分類 (国際特許分類 (I P C))

Int.Cl. H04L12/56(2006.01)i, H04L29/14(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 (I P C))

Int.Cl. H04L12/56, H04L29/14

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	1 9 2 2 - 1 9 9 6 年
日本国公開実用新案公報	1 9 7 1 - 2 0 0 7 年
日本国実用新案登録公報	1 9 9 6 - 2 0 0 7 年
日本国登録実用新案公報	1 9 9 4 - 2 0 0 7 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 請求の範囲の番号
X A	US 2005/0132046 A1 (Erik de la Iglesia et al.) 2005.06.16, 第 [0033]段落, Figure 5 (ファミリーなし)	1, 17 2-11, 18-20
A	JP 2001-147834 A (株式会社日立製作所) 2001.05.29, 第 0 0 5 5 - 第 0 0 5 9 段落, 図 4 & US 6732307 B1	12-16

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

0 7 . 0 5 . 2 0 0 7

国際調査報告の発送日

1 5 . 0 5 . 2 0 0 7

国際調査機関の名称及びあて先

日本国特許庁 (I S A / J P)

郵便番号 1 0 0 - 8 9 1 5

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)

清水 稔

電話番号 0 3 - 3 5 8 1 - 1 1 0 1 内線 3 5 9 6

5 X

8 5 2 5