(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
2009 年4 月30 日 (30.04.2009)

PCT

(10) 国際公開番号
WO 2009/054056 A1

(51) 国際特許分類:
G06F 21/20 (2006.01) *G06F 21/24* (2006.01)

(21) 国際出願番号: PCT/JP2007/070796

(22) 国際出願日: 2007 年10 月25 日 (25.10.2007)

(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): 内田 好昭 (UCHIDA, Yoshiaki) [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: 横山 淳一 (YOKOYAMA, Junichi); 〒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).

(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, DO, 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, ME, 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.

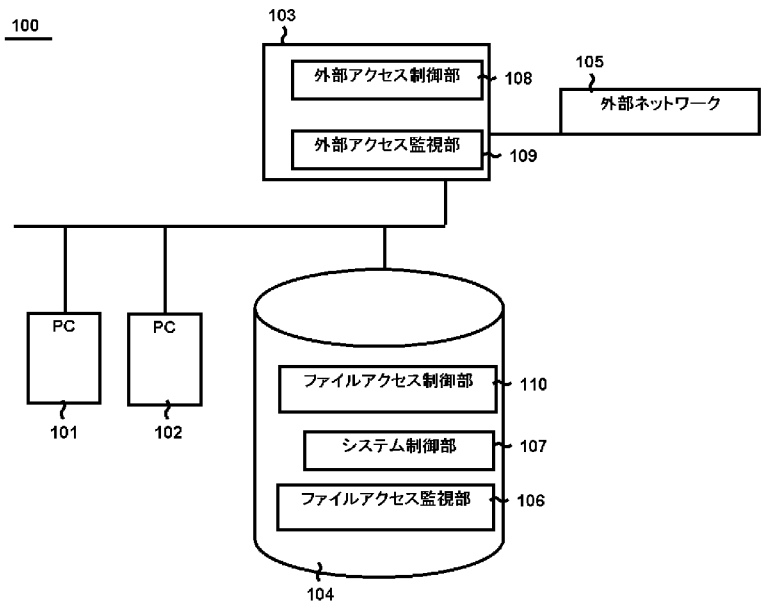
(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG,

[続葉有]

(54) **Title:** INFORMATION PROVIDING METHOD, RELAY METHOD, INFORMATION HOLDING DEVICE AND RELAY DEVICE

(54) 発明の名称: 情報提供方法、中継方法、情報保持装置、中継器

[図1]



108 EXTERNAL ACCESS CONTROL UNIT
109 EXTERNAL ACCESS MONITOR UNIT
105 EXTERNAL NETWORK
110 FILE ACCESS CONTROL UNIT
107 SYSTEM CONTROL UNIT
106 FILE ACCESS MONITOR UNIT

(57) Abstract: [PROBLEMS TO BE SOLVED] It is an object to prevent the leakage of information in a network storage caused by getting a malware mixed in a computer. [MEANS FOR SOLVING THE PROBLEMS] An information providing method, which is executed by an information holding device that stores information and provides the information to an information processing device through a network, is comprised of an access detecting step for detecting that the information processing device has accessed the information in the formation holding device, and a control step for controlling the transfer of information through the network by the information processing device during a period when the information processing device accesses the information in the information holding device. Further, the information holding device is provided with a file access detecting unit for detecting that the information processing device has accessed the information in the information holding device, and a system control unit for controlling the transfer of information through the net work by the information processing device during the access period.

[続葉有]

WO 2009/054056 A1

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

(57) 要約: 【課題】 本発明は、コンピュータ内へのマルウェアの混入に起因するネットワークストレージ内の情報の漏えいを防止することを目的とする。【解決手段】 本発明に係る情報提供方法は、情報を格納し、情報処理装置にネットワークを介して該情報を提供する情報保持装置が実行する情報提供方法において、該情報処理装置が該情報保持装置内の該情報にアクセスしたことを検出するアクセス検出手順と、該情報処理装置が情報保持装置に情報をアクセス中は該情報処理装置のネットワークを介した情報の転送を制御する制御手順とからなることを特徴とする。また上記情報保持装置において、該情報処理装置が該情報保持装置内の該情報にアクセスしたことを検出するファイルアクセス検出部と、該アクセスの中は該情報処理装置の情報の転送を制御するシステム制御部とを備えたことを特徴とする。

明 細 書

情報提供方法、中継方法、情報保持装置、中継器

技術分野

[0001] 本発明は、NAS（Network Attached Storage）などのネットワークストレージに関する。

背景技術

[0002] NASなどのネットワークストレージの利用が増加してきている。コンピュータにおけるインターネットへの常時接続も一般化してきている。このため多くのコンピュータがLANなどの閉じた中で、ユーザがNASへファイルアクセスしている場合でも、インターネットに接続した状態にある。

[0003] これにより悪意のあるソフトウェア（以下、マルウェアと呼ぶ）が、ユーザの意図しない形でNASに格納するデータをインターネット上に公開してしまう問題が発生している。

[0004] また、ユーザがインターネット上の実際には公開される領域を、非公開の作業領域と誤認してそこに重要なデータを置いてしまう場合や、本来公開すべきでないフォルダを公開の状態にしたままネットワークに接続してしまう場合などの不用意・不適切な操作による問題も考えられる。

[0005] 上記問題に対して、単純な解決策は、「直接LANケーブルを抜く」ことがあるが、ルータなどのLANケーブルを抜くことになり煩わしい。

[0006] コンピュータにおける情報漏えいを防止する技術に関して以下の特許文献が存在する。

特許文献1：特開2003－122615号公報

発明の開示

[0007] （発明が解決しようとする課題）

本発明は、コンピュータ内へのマルウェアの混入に起因するネットワークストレージ内の情報の漏えいを防止することを目的とする。

（課題を解決するための手段）

本実施例に係る情報提供方法は、情報を格納し、情報処理装置にネットワークを介して該情報を提供する情報保持装置が実行する情報提供方法において、該情報処理装置が該情報保持装置内の該情報にアクセスしたことを検出するアクセス検出手順と、該情報処理装置が情報保持装置に情報をアクセス中は該情報処理装置の情報の転送を制御する制御手順とからなることを特徴とする。

[0008] また本実施例に係る情報提供方法は、該アクセス検出手順において該情報処理装置から受信する要求パケットを参照して、該情報へのアクセスを検出することを特徴とする。

[0009] また本実施例に係る情報提供方法は、該アクセス検出手順において該情報保持装置が格納する該情報の属性を判別することを特徴とする。

[0010] また本実施例に係る情報提供方法は、該ファイルアクセス検出手順において該情報が保持するフラグに基づいて該情報の属性を判別することを特徴とする。

[0011] また本実施例に係る情報提供方法は、該制御手順において、該アクセス検出手順において判別した該情報の属性に応じて、該情報処理装置の該情報の転送を制御することを特徴とする情報提供方法。

[0012] また本実施例に係る情報提供方法は、該制御手順において該ネットワークの中継を行う中継器に対して該情報の転送を制御することを特徴とする。

[0013] また本実施例に係る中継方法は、情報処理装置と情報保持装置を含むネットワークと外部ネットワークとを接続する中継器が実行する中継方法において、該情報処理装置の該情報保持装置へのアクセス状況を管理するアクセス管理手順と、該アクセス管理手順において管理する該アクセス状況に応じて、該情報処理装置から該外部ネットワークへの該情報の転送を禁止する外部アクセス制御手順とからなることを特徴とする。

[0014] また本実施例に係る中継方法は、該アクセス管理手順において該情報保持装置から該アクセス状況を取得することを特徴とする。

[0015] また本実施例に係る中継方法は、該アクセス管理手順において、該外部アクセス制御手順において該情報処理装置から該外部ネットワークへの該情報の転送を禁止しておく時間を管理することを特徴とする。

[0016] また本実施例に係る中継方法は、さらに該情報処理装置と該外部ネットワークとの接続を検出する外部アクセス検出手順を有することを特徴とする。

（発明の効果）

本発明は、ネットワークストレージへのファイルアクセス中、外部ネットワークへのアクセスを禁止することによって、マルウェアの類が混入することに起因する、ネットワークストレージにおける情報漏えいを防止することを目的とする。

図面の簡単な説明

[0017] [図1]本実施例に係るネットワークストレージシステム100の構成図である。

[図2]本実施例に係るルータ103とNAS104の概略図である。

[図3]本実施例に係るBadPCList203である。

[図4]本実施例に係るネットワークストレージシステム400の構成図である。

[図5]本実施例に係るネットワークストレージシステム500の構成図である。

[図6]本実施例に係るネットワークストレージシステム600の構成図である。

[図7]本実施例に係るネットワークストレージシステム700の構成図である。

[図8]本実施例に係るネットワークストレージシステム800の構成図である。

[図9]本実施例に係るNASのオープン処理に関するフローチャートである。

[図10]本実施例に係るNAS104のクローズ処理に関するフローチャートである。

[図11]本実施例に係るルータ103が行うカウント処理のフローチャートである。

[図12]本実施例に係るルータ103が行うパケット転送処理のフローチャートである

[図13]本実施例に係るNAS104のハードブロック図である。

[図14]本実施例に係るネットワークストレージシステム100の構成図である。

[図15]本実施例に係るネットワークストレージシステム100の構成図である。

符号の説明

[0018] 100…ネットワークストレージシステム

101…パーソナルコンピュータ

102…パーソナルコンピュータ

103…ルータ

104…NAS

105…外部ネットワーク

106…ファイルアクセス監視部

107…システム制御部

108…外部アクセス制御部

201…フォルダ

202…フォルダ

203…BadPCList

(発明を実施するための最良の形態)

本実施例におけるネットワークストレージシステムは、複数のパーソナルコンピュータとNASがLANで接続しており、LAN外部のネットワークとパーソナルコンピュータはルータを介して接続しているシステムである。そしてパーソナルコンピュータがLANを介してファイルアクセスしたり、ルータを介してインターネットアクセスしたりする。本実施例におけるNASは、NASに格納されるデータがユーザの意図に反してインターネット上に流出しないように制御するものである。

[0019] NASに格納されるデータがインターネット上に流出する場合として特に問題なのは、マルウェアに起因するものである。

[0020] マルウェアによって、ユーザの意図に反してインターネット上のデータが流出する経路は、次のような場合が考えられる。

・ マルウェアが秘匿すべきフォルダをファイル共有フォルダの公開フォルダにしてしまう。

・ マルウェアが秘匿すべきファイルを公開フォルダに複写してしまう。

・ マルウェアが秘匿すべきファイルをユーザの意図しないタイミングでメールとして転送してしまう。

[0021] これらの問題に対する従来の対策は、以下のものである。

・ パーソナルコンピュータが、ウィルスソフトウェアにより、「マルウェア」を検出する。

・ パーソナルコンピュータが、ソフトウェアのファイアウォールにより、外部からパーソナルコンピュータへのネットワーク接続を遮断する。

・ パーソナルコンピュータが、物理的なファイアウォールにより、重要データの流失を

監視する。

[0022] しかし、上記1．の対策は、新種のウィルスへの対応が遅れる。「悪意を持ったソフトウェア」が最初、ないし初期に感染したパーソナルコンピュータについては無力である。

[0023] 上記2．の対策は、一旦動作を始めた「悪意を持ったソフトウェア」が、中から外部にアクセスをする場合、これを検出することは難しい。

[0024] 上記3．の対策にはSPAMメールの対策や従業員によるWebアクセスの監視として使われている技術がある。これは外部ネットワークから入ってくる、または外部ネットワークとやりとりするデータに、業務上は考えられないような単語や表現があるとき、送信元や中継地点が不審者と思われるときなどに、これを不正なデータとみなすものである。漏洩を防ぐべき重要データが、固定的なものでパターンが決まっているならば、この技術を流用することが可能と思われる。すなわち、業務上重要と思われる単語や表現が固定的なパターンとして選出できれば、これを含むデータが外部に転送されようとするときにそのデータ送信を禁止するものである。

[0025] しかしながら、ファイアウォールが業務上は考えられないような単語や表現のみによりすべて機械的に異常か正常か見分けることは困難であるように、データ送信を禁止する契機となる単語や表現を用いて検出することも困難である。そのためユーザがファイアウォールのログデータを用いて、後日に対処するしかない。

[0026] 本実施例におけるNASは、ネットワークを介してパーソナルコンピュータと接続している。そして該NASは、該パーソナルコンピュータから該ネットワークストレージへのファイルアクセスを検出するファイルアクセス検出部と、検出したファイルアクセスに応じて、該パーソナルコンピュータと外部ネットワークとの接続の遮断を制御するシステム制御部とから構成される。これにより情報処理装置がNASに対してファイルアクセス中は、情報処理装置と外部ネットワークとを遮断することによって、NASに格納されるデータの外部ネットワークへの流出を防止することができる。

[0027] ［ネットワークストレージシステム100］

以下、図1を用いて、本実施例に係るネットワークストレージシステム100の説明をする。図1は本実施例に係るネットワークストレージシステム100の構成図である。

[0028] ネットワークストレージシステム100は、パーソナルコンピュータ101、102、ルータ103、ネットワークストレージ（以下、NASと呼ぶ。）104から構成されている。ネットワークストレージシステム100はルータ103を介して外部ネットワーク105と接続している。またNAS104は、ファイルアクセス監視部106、システム制御部107、ファイルアクセス制御部110から構成されている。NAS104に搭載するファイルアクセス監視部106、システム制御部107、ファイルアクセス制御部110は新規な機能であり、本実施例のNAS104の特徴である。またルータ103は、外部アクセス制御部108、外部アクセス監視部109を有している。外部アクセス制御部108、外部アクセス監視部109は、ファイルアクセス監視部106、システム制御部107、ファイルアクセス制御部110と連携して機能するものであり、本実施例のルータ103の特徴である。なおファイルアクセス監視部106、システム制御部107、ファイルアクセス制御部110は、NAS104の外部に設けてもよい。

[0029] そして本実施例では、パーソナルコンピュータ101が、NAS104にファイルアクセスする。マルウェアはNAS104のデータ（ファイル、フォルダ等）をインターネット上に公開する場合、NAS104にファイルアクセスするパーソナルコンピュータ101を介して外部ネットワーク105にデータを流出する。

[0030] NAS104は、指定フォルダへのファイルアクセスがあったとき、ルータ103の外部アクセス制御部108を制御する。指定フォルダとは、予めユーザが秘匿すべきフォルダと指定したフォルダである。NAS104に格納されるフォルダは、そのフォルダが秘匿対象か否かを示すフラグを有している。

[0031] 本実施例に係るネットワークストレージシステム100において、パーソナルコンピュータ101が秘匿すべきファイルを編集中、NAS104はパーソナルコンピュータ101の外部ネットワーク105へのアクセスを禁止する。これよりネットワークストレージシステム100は、マルウェアによるNAS104に格納される秘匿ファイルの流出を防ぐことができる。

[0032] なお別のパーソナルコンピュータ102からインターネットを参照することは可能であり、パーソナルコンピュータ101とパーソナルコンピュータ102との間で、LAN内でデータを参照しあうことも可能である。なお外部ネットワーク105とパーソナルコンピュー

タ101、102との接続制御は、ルータ103の制御で実現することに限定されない。

[0033] [NAS104]

本実施例におけるNAS104は、ファイルサーバ機能に加え、ルータ103を制御する機能を有している。そしてルータ103は、外部アクセス制御部108によって、パーソナルコンピュータ101から外部ネットワーク105への通信を制御する。

[0034] NAS104は、フォルダ、ファイルを有している。ファイルはフォルダ内にあってもよいし、フォルダと同じ階層であってもよい。ファイルアクセス監視部106は、パーソナルコンピュータ101、102のファイルアクセスを検出する。本実施例では、ファイルアクセス監視部106は、パーソナルコンピュータ101、102のファイルアクセスに関するapi(Application Program Interface)を検出することによって、パーソナルコンピュータ101、102のファイルアクセスを検出する。apiは、ソフトウェアのプログラム上の手続きを定めた規約の集合である。

[0035] ファイルアクセス監視部106が、パーソナルコンピュータ101、102からファイルへのアクセスを検出すると、アクセスの要求元(パーソナルコンピュータ101、102)のMACアドレス、IPアドレスをシステム制御部107へ通知する。

[0036] システム制御部107は、ファイルアクセス監視部106から受信する情報(MACアドレス、IPアドレス)に基づいて、ルータ103が有する外部アクセス制御部108を制御する。

[0037] 外部アクセス制御部108は、システム制御部107からの指示に基づいて、パーソナルコンピュータ101、102の外部ネットワーク105へのアクセスを遮断する。また外部アクセス制御部108は、パーソナルコンピュータ101、102の外部ネットワーク105へのアクセスを遅延する構成でもよい。

[0038] たとえばマルウェアが、本来秘匿されるべきファイル(秘匿を示すフラグが有効になっているファイル)を外部ネットワーク105にメールなどで送信しようとしたとする。本実施例におけるNAS104は、マルウェアが秘匿ファイルを読み出した時点で、秘匿ファイルを読み出したパーソナルコンピュータ(マルウェアが存在するパーソナルコンピュータ)と外部ネットワーク105とのアクセスを禁止する。これによりパーソナルコンピュータによる秘匿ファイルのデータ送信が失敗となり、情報漏えいを防止することができ

る。

[0039] またアクセス制御部105がパーソナルコンピュータと外部ネットワーク105とのアクセスを禁止することにより、アクセス制御部105はパーソナルコンピュータが正規の作業として行っている外部ネットワーク105との通信も一律に禁止する。パーソナルコンピュータのユーザがシステムの動作が不安定であると認識して調査することにより、該ユーザがマルウェアの所在に気づく契機となる。本実施例におけるネットワークストレージシステム100によれば、ユーザはマルウェアの混入を早期に発見することができ、二次的な被害や、被害の拡大を防ぐことができる。

[0040] そのため、パーソナルコンピュータがネットワークストレージにファイルアクセス中に外部ネットワークとファイルアクセスを遮断するように制御することにより、マルウェアによる情報漏えいを防止することができる。

[0041] [ルータ103とNAS104の連携機能]

図2は、本実施例に係るルータ103とNAS104の概略図である。

[0042] 本実施例に係るルータ103とNAS104の連携を詳細に説明する。図2に記載のルータ103とNAS104を図示しており、図1に記載のものと同等のものである。なお図2において、NAS104に搭載されるファイルアクセス制御部106、システム制御部107は図示していないが、図2のNAS104も有する機能である。

[0043] ルータ103は、外部アクセス制御部108に加え、BadPCList203を有している。図3がBadPCList203の具体例である。

[0044] ルータ103は、ソフトウェアによって次の機能を実装している。ルータ103が有する機能の1つは、BadPCList203を管理し、各パーソナルコンピュータ101、102が外部ネットワーク105との通信を許可されているか拒否されるかを判断する機能である。またルータ103が有する機能の1つは、BadPCList203を更新する機能である。さらにルータ103が有する機能の1つは、IPパケットの送信元IPアドレス、MACアドレスがBadPCList203に存在し、IPパケットの送信元(パーソナルコンピュータ)の外部ネットワーク105への通信拒否と判別し、かつIPパケットの宛先が外部ネットワーク105のものと判別した場合は、このパケットを破棄する制御論理機能である。なおルータ103は、パケットのIPアドレス、MACアドレスによって、パケットの送信元と送信先が

内部LANであるか外部ネットワーク105であるかを判別する機能も有する。

[BadPCList203]

図3は本実施例に係るBadPCList203である。

[0045] BadPCList203は、LAN内に存在するパーソナルコンピュータ101、102のIPアドレス301、MACアドレス302、in__use303、BTL304、protectフラグ305、OCN306から構成されている。

[0046] in__use303は、アクセスを拒否させる要因の数を示すカウンタである。

[0047] BTL304は、パーソナルコンピュータ101、102の外部ネットワーク105へのアクセスを許可するまでの時間を示すダウンカウンタである。

[0048] protectフラグ305は、外部ネットワーク105への接続を求める各パーソナルコンピュータ101、102に対応して外部ネットへのアクセス拒否状態を保持するものである。

[0049] OCN306は、パーソナルコンピュータ101、102のNAS104へのアクセスを許可するまでの時間を示すダウンカウンタである。OCN306はパーソナルコンピュータ101、102と外部ネットワーク105との通信が発生するたびに、所定の値(例えば20)セットするカウンタである。

[0050] ルータ103は、パーソナルコンピュータ101、102と外部ネットワーク105とのアクセスを拒否する要因が生じるとin__use303をカウントアップする。具体的にパーソナルコンピュータ101、102と外部ネットワーク105とのアクセスを拒否する要因は、パーソナルコンピュータ101、102がNAS104の指定フォルダにアクセスしたことである。

[0051] ルータ103がパーソナルコンピュータ101、102と外部ネットワーク105とのアクセスを拒否する要因がなくなったと判別すると、ルータ103in__use303をカウントダウンする。なおin__use303の初期値は0である。

[0052] in__use303の値が「0」でないことは、パーソナルコンピュータ101、102と外部ネットワーク105とのアクセスを拒否する要因があることを示すため、ルータ103はprotectフラグ305を「protect＝true」とする。そしてルータ103はBTL304の値を規定値(例えば32)にセットする。

[0053] ルータ103がin__use303を「0」とすると(つまりパーソナルコンピュータ101、102と外部ネットワーク105とのアクセスを拒否すべき要因がなくなる)、ルータ103はBT

L304の値を一定時間間隔（例えば1秒）でカウントダウンする。ルータ103がBTL304をカウントダウンし、BTL304の値を「0」とすると、カウントダウンを停止すると共に、protectフラグ305を「true」から「false」にする。これにより「protect＝false」に対応するパーソナルコンピュータは外部ネットワーク105への通信が可能となる。

[0054] また本実施例では、ルータ103はOCN306もBTL304と同じ時間間隔（例えば1秒）でカウントダウンし、「0」とするとカウントダウンを停止する。もちろんOCN306とBTL304とにおけるカウントダウンの時間間隔は同じであることに限定されない。

[0055] ルータ103がOCN306にセットする値は、パーソナルコンピュータ101、102と外部ネットワーク105との通信プロトコル（ポート番号）によって変える構成でもよい。その場合、ルータ103はOCN306が保持している値より小さい値はOCN306に書き込まないように制御する。

[0056] また本実施例では、BadPCList203はルータ103に搭載するソフトウェアによって管理するテーブルとしているがこれに限定されない。ルータ103がBadPCList203をGate Array等のハードウェアによって実装することも可能である。

[0057] なお以上のことよりBadPCList203は、以下のことを示している。IPアドレスが「192．168．3．32」のパーソナルコンピュータ101は外部ネットへのアクセスは許可されている(protect＝false)がLAN内でのみ通信している（OCN＝0）。一方「192．168．3．33」のパーソナルコンピュータ102は2つの要因により外部ネットワーク105との通信が禁止されている。さらに「192．168．3．34」のパーソナルコンピュータは(20－15＝)5秒前に外部ネットワーク105との間で通信を行ったことを示す。

[0058] ［NAS104の機能］

次に本実施例に係るNAS104の有する機能について詳細に説明する。

[0059] NAS104は、LAN内のパーソナルコンピュータ101、102に対して公開するフォルダごとに、HideフラグとOpenフラグを持つ。

[0060] より具体的には本実施例におけるNAS104はフォルダ201、202を有している。そしてそれぞれのフォルダ201、202はHideフラグとOpenフラグを有している。フォルダ201のHideフラグは「true」であり、Openフラグは「false」である。フォルダ202のHideフラグは「false」であり、Openフラグは「true」である。

[0061] Hideフラグの「true」は、フォルダ201におけるファイルが外部ネットワーク105に対して秘匿すべきファイルであることを示す。Hideフラグの「false」は、フォルダ202におけるファイルが外部ネットワーク105に対して公開可能なファイルであることを示す。つまりHideフラグは、そのHideフラグを有するフォルダにあるファイルが秘匿ファイルか否かを示す情報である。そしてNAS104はフォルダ201、202のHideフラグを参照して、フォルダ201、202内のファイルが秘匿ファイルか否かを判別する。

[0062] Openフラグの「true」は、フォルダ202内のいずれかのファイルが読み出し(読み書き)されていることを示す。Openフラグの「false」は、フォルダ201内のいずれかのファイルも読み出し(読み書き)されていないことを示す。フォルダ201、202はOpenフラグをアクセス元のパーソナルコンピュータごとに有している(図示せず。代表してパーソナルコンピュータ101に対応するOpenフラグのみ記載している)。

[0063] Hideフラグ、Openフラグはファイルシステムが元々持っているフラグを流用することも可能である。たとえばUnix系のファイルシステムであれば「Otherユーザに対して読み出し許可されていないときHide=trueとみなす」、FATファイルシステムであれば「Hidden属性があるときHide＝trueとみなす」等の方法がある。またOpenフラグは、多くのファイルシステムはオープンされた回数を示すカウンタやmountされていることを示すフラグを持つので、この機構と下記b2の機構を組み合わせてアクセス元のパーソナルコンピュータごとに管理するようにすることができる。

[0064] またNAS104は、NAS104にアクセスしたパーソナルコンピュータをIPアドレスまたはMACアドレスによって特定する機能を有する。

[0065] その実装方法の一例として、NAS104への要求がネットワークを介して届くのであるから、その要求パケットから要求元のIPアドレスやMACアドレスを取り出すことができる。これをそのままファイルシステムへの要求ブロックに付加情報として加えておけばよい。なお、ファイルシステムでの処理結果を要求元のパーソナルコンピュータへ送信するところで、送信先のIPアドレス／MACアドレス(アクセス要求元のパーソナルコンピュータのIPアドレス／MACアドレス)を取り出してもよい。

[0066] NAS104が、Hideフラグが「true」のフォルダ201においてOpenフラグのフォルダが「false」から「true」に変化したことを検出すると、アクセス元のパーソナルコンピュ

ータ101、つまり取り出したIPアドレス／MACアドレスに対するBadPCList203について、in__useをカウントアップする。

[0067] NAS104はprotectフラグ305の値を「true」にすると共にBTL304の値を規定値（例えば32）にセットする。NAS104はOpenフラグを「true」から「false」に変えるとき、NAS104は対応するin__useをカウントダウンする。

[0068] 以上により、ルータ103は、パーソナルコンピュータ101が秘匿フォルダへアクセスしている間、およびアクセスが終了してから一定時間（32秒）の間、アクセス元のパーソナルコンピュータ101と外部ネットワーク105へのデータ通信が禁止する。

[0069] アクセス禁止期間（BTL304、OCN306）は、ユーザの通常の作業を妨げるほどではない。たとえばアクセス禁止期間の間、ユーザはメールを読み書きしながら、秘匿すべきフォルダのデータを読み書きすることも可能である。その一方で、マルウェアのようなソフトウェアのネットワークアクセスは禁止され、情報流出の被害を防ぐことができる。さらに通信をブロックしたログやエラーメッセージは、マルウェアが動作していることに警告になる。そのためユーザはマルウェアを早期に発見することができる。

[0070] なお、このルータ103は、NAT機能やDHCP機能を有する必要はない。そのためルータ103は、パケットのあて先、送信元のIP／MACのアドレス検出とスイッチングによって実現できる。したがってルータ103はスイッチングHUBと同程度であり、ハード化することも容易である。

[0071] ［外部アクセス監視部109］

次にルータ103が搭載する新規な機能である外部アクセス監視部109について説明する。

[0072] 外部アクセス監視部109は、パーソナルコンピュータ101、102と外部ネットワーク105との接続状況を検出する機能である。

[0073] パーソナルコンピュータ101、102が外部ネットワーク105にアクセスする場合には、NAS104は外部ネットワーク105にアクセスするパーソナルコンピュータ101、102のファイルアクセスを禁止する。換言すれば、ルータ103がLAN内のパーソナルコンピュータ101、102から外部ネットワーク105へのアクセス要求をうけつけた場合、その後一定時間、NAS104が外部ネットワーク105へのアクセス要求したパーソナルコ

ンピュータ101、102によるNAS104内のフォルダの読み取りをエラーとする。

[0074] これによりパーソナルコンピュータ101、102が、マルウェアの動作に起因して外部ネットワーク105への接続を試みた場合に、NAS104がパーソナルコンピュータ101、102の秘匿ファイル（NAS104内に格納される秘匿ファイル）へのアクセスを禁止することにより、データ流出を防ぐものである。

[0075] 具体的には外部アクセス監視部109は、パーソナルコンピュータ101、102が外部ネットワーク105へアクセスしたことを検出するとBadPCList203のOCN306の値をセットする。

[0076] 外部アクセス監視部109は、OCN306の値をパーソナルコンピュータ101、102の外部ネットワーク105とのやりとりで利用するネットワークプロトコルなどを考慮してセットする。例えばパーソナルコンピュータ101、102がSMTP（Simple Mail Transfer Protocol）を利用して外部ネットワーク105とやりとりする場合、外部アクセス監視部109はOCN306の値を「30」にセットする。パーソナルコンピュータ101、102がHTTP（Hypertext Transfer Protocol）を利用して外部ネットワーク105とやりとりする場合、外部アクセス監視部109はOCN306の値を「10」にセットする。またパーソナルコンピュータ101、102がFTP（File Transfer Protocol）を利用して外部ネットワーク105とやりとりする場合、外部アクセス監視部109はOCN306の値を「40」にセットする。つまりパーソナルコンピュータ101、102がメール送信したりファイル転送する場合は、パーソナルコンピュータ101、102がウェブアクセスする場合よりも、NAS104へのアクセス禁止期間を長くするものである。これはマルウェアによる秘匿ファイルの流出可能性の高い外部ネットワーク105へのアクセスについてアクセス禁止期間を禁止するものである。

[0077] なお外部アクセス監視部109は、ルータ103がファイアウォールと連携してパーソナルコンピュータ101、102と外部ネットワーク105の通信を監視するように実現するものでもよい。

[0078] ［ファイルアクセス制御部110］

またNAS104は、ファイルアクセス制御部110を有している。ファイルアクセス制御部110は、LAN内のパーソナルコンピュータ101、102に公開可能なフォルダへの

アクセスを禁止、または一定時間遅延させる機能である。

[0079] ファイルアクセス制御部110は、ルータ103の外部アクセス監視部109からの情報に基づいて動作する。より具体的にはシステム制御部107がルータ103の外部アクセス監視部109でのアクセス検出を取得する。そしてシステム制御部107が外部アクセス監視部109から取得するアクセス情報に基づいて、ファイルアクセス制御部110に動作指示を与える。ファイルアクセス制御部110は、システム制御部107からの指示に基づいて、パーソナルコンピュータ101、102のNAS104へのアクセスを制御する。

[0080] また上述するように外部アクセス監視部109はOCN306の値をセットする。システム制御部107は、OCN306の値に応じて、ファイルアクセス制御部110に動作指示を与える。ファイルアクセス制御部110は、OCN306の値が「0」のパーソナルコンピュータに対しては、NAS104へのアクセスを許可する。またファイルアクセス制御部110は、OCN306の値が「0」でないパーソナルコンピュータに対しては、NAS104へのアクセスを禁止する。

[0081] システム制御部107は、Hideフラグが「true」のフォルダを判別する。ファイルアクセス監視部104がOpenフラグを監視する。ファイルアクセス監視部104が、Openフラグが「false」から「true」に変化したことを検出すると、システム制御部107は変化したOpenフラグに対応するパーソナルコンピュータのOCN306を取得する。そしてシステム制御部107は、取得したOCN306のHideフラグが「true」であると判別する場合には、ファイルアクセス制御部110に対して、OCN306を通知する。

[0082] ファイルアクセス制御部110がOCN306の値が「0」でないと判別する場合、ファイルアクセス制御部100はファイルアクセス要求に対してエラーを返す。つまりファイルアクセス制御部110はOCN306の値が「0」でないパーソナルコンピュータのファイルアクセスを禁止する。

[0083] [ネットワークストレージシステム400]

図4は本実施例に係るネットワークストレージシステム400の構成図である。

[0084] ネットワークストレージシステム400は、パーソナルコンピュータ401、402、ファイアウォール403、NAS404から構成されている。ネットワークストレージシステム400は

ファイアウォール403を介して外部ネットワーク105と接続している。ファイアウォール403はパケット監視部406、特徴パターン辞書409を有している。またNAS404は特徴パターン生成部407、登録機能408を有している。

[0085] NAS404は、ファイルごとに秘匿ファイルか否かを管理可能とする。特徴パターン生成部407は、秘匿ファイルごとに特徴パターンを生成する。そして登録機能408は、特徴パターン生成部407が生成した特徴パターンを特徴パターン辞書409に登録する。特徴パターンは、ファイルが秘匿ファイルか否かを示すものである。特徴パターン生成部407は、例えば秘匿ファイルのファイル名・ファイル内容に基づいて特徴パターンを生成する。

[0086] パケット監視部406は、LAN内のパーソナルコンピュータ401、402から外部ネットワーク405への転送パケットを監視して、該転送パケット内に存在する特徴パターンの有無を判別する。ファイアウォール403が転送パケットを受信した場合、パケット監視部406は特徴パターン辞書409を参照する。パケット監視部406は転送パケット内に特徴パターン辞書409に登録される特徴パターンがあると判別する場合、外部アクセス制御部410は転送パケットを外部ネットワーク105に送信することを禁止する。

[0087] これにより本実施例にかかるネットワークストレージシステム400は、特徴パターンを用いて、秘匿ファイルをファイアウォール403に指定することができ、秘匿ファイルの外部ネットワーク405への流出を防止することができる。また本実施例におけるネットワークストレージシステム400は、マルウェアが秘匿ファイルを公開フォルダに複写してしまった場合であっても防ぐことができる。

[0088] また特徴パターン生成部407が動作するきっかけは、例えば下記a、b、cのいずれか、または組み合わせである。

[0089] a. NAS404のユーザが特徴パターン生成部407に起動指示を行う。

[0090] b. 予め指定した時間に定期的に特徴パターン生成部407を起動する。

[0091] c. ファイルへの書き込み・更新をきっかけにして、パターン生成部407を起動する。

[0092] また特徴パターン生成部407は、NAS404は、変更のあったファイルに存在する特徴パターンを計算する。そのためファイアウォール403は、リアルタイムで転送パケット内の特徴パターン有無を監視することができる。

[0093] なお特徴パターン生成部407の起動トリガーは、NAS404に搭載されるファイルシステム、オペレーションシステムのファイル更新、作成を通知する機能を流用して、実現することができる。

[0094] このように本実施例におけるネットワークストレージ400は、NAS404の特定のフォルダ（protectフラグが「true」）にあるファイル、そのファイルを改変したファイル、またはデータが外部ネットワーク405に流出することを防止できる。protectフラグの話を追記する。

[0095] 本実施例におけるネットワークストレージシステム400は、特徴パターンを有する転送パケットを外部ネットワーク105に送信することを禁止する。そのため本実施例に係るネットワークストレージシステム400は、秘匿ファイルが保護対象でないフォルダに存在する場合であっても、秘匿ファイルの外部ネットワーク405への流出を防ぐことができる。

[ネットワークストレージシステム500]

図5は本実施例に係るネットワークストレージシステム500の構成図である。

[0096] ネットワークストレージシステム500は、パーソナルコンピュータ501、502、ルータ503、NAS504から構成されている。ネットワークストレージシステム500はルータ503を介して外部ネットワーク505と接続している。またルータ503は外部アクセス制御部503を有している。NAS504はファイルアクセス監視部507、システム制御部508、特徴パターン生成部509、特徴パターン辞書510、ファイル検索部511を有している。

[0097] 本実施例におけるネットワークストレージシステム500は、秘匿ファイルにおける特徴パターンを随時検出し、秘匿ファイルへのアクセス有無を随時更新していくシステムである。そして本実施例におけるネットワークストレージシステム500は、秘匿ファイルにファイルアクセスのあったパーソナルコンピュータの外部アクセスネットワーク505へのアクセスを禁止する。これによりネットワークストレージシステム500も、マルウェアによる秘匿ファイルの流出を防止することができる。

[0098] 以下、ネットワークストレージシステム500の動作について説明する。

[0099] パーソナルコンピュータ501、502がNAS504にファイルアクセスを行う。パーソナ

ルコンピュータ501、502が秘匿ファイルを更新すると、特徴パターン生成部509は起動する。特徴パターン生成部509は、更新された秘匿ファイルの特徴パターンを生成する。特徴パターン生成部407は、ファイル名・ファイル内容に基づいて特徴パターンを生成する。そして特徴パターン生成部509は、生成した特徴パターンを特徴パターン辞書510に登録すると共に、ファイル検索部511へ生成した特徴パターンを通知する。ファイル検索部511は、NAS504に存在するすべてのフォルダ内に、通知のあった特徴パターンが存在するか否かを判別する。ファイル検索部511が、生成した特徴パターンを含むフォルダ、ファイルを検出した場合、追加機能512は検出したファイルをファイルアクセス監視部507の新たな監視対象として追加する。ファイルアクセス監視部507は、新たに監視対象となったフォルダ、ファイルおよびすでに監視対象となっているフォルダ、ファイルにおいてもパーソナルコンピュータ501、502からのファイルアクセスを監視する。

[0100] 本実施例におけるネットワークストレージシステム500は、特徴パターンをNAS504内の指定フォルダ（protectフラグが「true」）以外のフォルダや、パーソナルコンピュータ501、502やNAS504の公開フォルダから検索する。

[0101] またはNAS504は、パーソナルコンピュータ上のソフトウェアと連携して特徴パターンをパーソナルコンピュータ上の全フォルダ内で検索する機能を有し、NAS504が次のa、bのいずれかまたは両方の動作を行うものであってもよい。

[0102] a. 特徴パターンを見出したファイルやフォルダの外部ネットワーク505への送信を禁止する。

[0103] b. 特徴パターンを新たに検出したファイルやフォルダについて、パーソナルコンピュータ通知する。

[0104] これにより本実施例にかかるネットワークストレージシステム500は、秘匿ファイルが保護されていないフォルダに複写された場合であっても、秘匿ファイルの外部ネットワーク505への流出を防ぐことができる。

[0105] また本実施例に係るネットワークストレージシステム500は、保護されないフォルダに秘匿ファイルが複写されても監視対象に追加する。そのためユーザの不用意な操作による秘匿ファイルの外部ネットワーク505への流出を減らすことができる。

[0106] また本実施例に係るネットワークストレージシステム500では、ユーザが保護すべきフォルダを指定すれば、そのフォルダに存在するファイルの複写物についても保護対象とすることができる。したがってネットワークストレージシステム500は、ユーザが見落とすNAS504のファイル保護の漏れを防止することができる。

[0107] [ネットワークストレージシステム600]

図6は本実施例に係るネットワークストレージシステム600の構成図である。

[0108] 次に本実施例に係るネットワークストレージシステム600について説明する。

[0109] ネットワークストレージシステム600は、パーソナルコンピュータ601、外部ネットワーク602から構成される。パーソナルコンピュータ601はLANポート603、ネットアクセス制御部604、システム制御部605、ファイルアクセス監視部606、内蔵ディスク607から構成されている。パーソナルコンピュータ601は、パーソナルコンピュータ601上で動作するファイアウォールソフトウェアを有する。

[0110] 内蔵ディスク607には、秘匿フォルダ、秘匿ファイルが格納されている。ファイルアクセス監視部606は、内蔵ディスク607に格納される秘匿フォルダ、秘匿ファイルへのファイルアクセスを検出する。ファイルアクセス監視部606が秘匿フォルダ、秘匿ファイルへのファイルアクセスを検出した場合、ファイルアクセス監視部606はシステム制御部605へファイルアクセスの検出を通知する。

[0111] システム制御部605はファイルアクセス検出の通知を受けると、システム制御部605はファイルアクセス監視部606からのファイルアクセス検出の通知に基づいて、ネットアクセス制御部604に外部ネットワークへ602の遮断を指示する。

[0112] ネットアクセス制御部604は、システム制御部605からの指示に基づいて、パーソナルコンピュータ601の外部ネットワーク602へのアクセスを遮断する。

[0113] [ネットワークストレージシステム700]

図7は本実施例に係るネットワークストレージシステム700の構成図である。

[0114] 本実施例に係るネットワークストレージシステム700について説明する。

[0115] ネットワークストレージシステム700は、パーソナルコンピュータ701、外部ネットワーク702、外部ディスク703から構成されている。ここで外部ディスクはMOディスクやUSBメモリなどである。パーソナルコンピュータ701は、USBインタフェース、SCSIイン

タフェース等を介して、外部ディスク703と接続する。

[0116] パーソナルコンピュータ701は、LANポート704、ネットアクセス制御部705、システム制御部706、保護対象検出部707、ファイルアクセス監視部708、内蔵ディスク709から構成されている。

[0117] パーソナルコンピュータ702が、外部ディスク703に格納されるフォルダ、ファイルにアクセスした場合、保護対象検出部707は外部ディスク703のボリュームラベルやフォルダ名などに基づいて、アクセスしたフォルダ、ファイルが秘匿フォルダ、秘匿ファイルであることを判別する。具体的に保護対象検出部707が行う処理論理は、例えばボリュームラベルが「HIDDENxxx」のフォルダ、ファイルを保護対象と判別する。換言すれば保護対象検出部707は、予め定めた特定のボリュームラベルを有するフォルダ、ファイルを保護対象と判別する。あるいは保護対象検出部707は特定のルートフォルダに存在するフォルダ、ファイルを保護対象と判別する。

[0118] 保護対象検出部707が外部ディスク703に格納されるフォルダ、ファイルが保護対象であると判別すると、保護対象検出部707はシステム制御部706に対して外部ネットワーク702とをパーソナルコンピュータ701とをアクセス禁止することを通知する。

[0119] システム制御部706は保護対象検出部707よりアクセス禁止の通知を受けると、システム制御部706は保護対象検出部707からの通知に基づいて、ネットアクセス制御部705に外部ネットワークへ702の遮断を指示する。

[0120] ネットアクセス制御部705は、システム制御部706からの指示に基づいて、パーソナルコンピュータ701の外部ネットワーク702へのアクセスを遮断する。

[0121] またネットワークストレージシステム700も内蔵ディスク709に格納される秘匿フォルダ、秘匿ファイルにファイルアクセスあったことをファイルアクセス監視部708を用いてファイルへのアクセスを検出する。ファイルアクセス監視部708は内蔵ディスク709に格納される秘匿フォルダ、秘匿ファイルにファイルアクセスがあると判別すると、ファイルアクセス監視部708はシステム制御部706へファイルアクセスの検出を通知する。

[0122] システム制御部706はファイルアクセス監視部708からファイルアクセス検出の通知を受けると、システム制御部706はファイルアクセス監視部708からのファイルアクセス検出の通知に基づいて、ネットアクセス制御部705に外部ネットワーク702への

遮断を指示する。

[0123] ネットアクセス制御部705は、システム制御部706からの指示に基づいて、パーソナルコンピュータ701の外部ネットワーク702へのアクセスを遮断する。

[0124] 本実施例に係るネットワークストレージシステム700は、外部ディスク703の秘匿フォルダ、秘匿ファイルにファイルアクセスした場合に、パーソナルコンピュータ701と外部ネットワーク702とのアクセスを禁止するシステムである。

[0125] これにより本実施例におけるネットワークストレージシステム700は、外部ディスク703に格納した秘匿データを外部ネットワーク702に流出することを防ぐことができる。

[0126] パーソナルコンピュータ701は、外部ディスク703に格納される秘匿フォルダ、秘匿ファイルを外部ディスク703内で更新して管理すれば、マルウェアによる秘匿フォルダ、秘匿ファイルの外部ネットワーク702への流出を防ぐことができる。

[0127] [ネットワークストレージシステム800]

本実施例に係るネットワークストレージシステム800について説明する。

[0128] 図8は本実施例に係るネットワークストレージシステム800の構成図である。

[0129] ネットワークストレージシステム800は、パーソナルコンピュータ801、外部ネットワーク802、外部ディスク803から構成されている。

[0130] パーソナルコンピュータ801は、LANポート804、ネットアクセス制御部805、システム制御部806、アクセス制御部807、ファイルアクセス監視部808、内蔵ディスク809から構成されている。

[0131] ネットワークストレージシステム800においても、ファイルアクセス監視部808が内蔵ディスク809に格納される秘匿フォルダ、秘匿ファイルへのパーソナルコンピュータ801からのファイルアクセスを検出する。

[0132] そしてファイルアクセス監視部808は内蔵ディスク809に格納される秘匿フォルダ、秘匿ファイルにファイルアクセスがあると判別すると、ファイルアクセス監視部808はシステム制御部806へファイルアクセスの検出を通知する。

[0133] システム制御部806はファイルアクセス監視部808からファイルアクセス検出の通知を受けると、システム制御部806はファイルアクセス監視部808からのファイルアクセス検出の通知に基づいて、ネットアクセス制御部805に外部ネットワーク802への

遮断を指示する。

[0134] ネットアクセス制御部805は、システム制御部806からの指示に基づいて、パーソナルコンピュータ801の外部ネットワーク802へのアクセスを遮断する。

[0135] そして外部ディスク803に格納されるデータは暗号されている。外部ディスク803は持ち運び可能な記録媒体である。外部ディスク803内のデータを暗号化しておくことにより、ユーザが不注意で外部ディスク803を落としてしまった場合でもデータの漏えいを防ぐことができる構成となっている。

[0136] パーソナルコンピュータ801はアクセス制御部807を有する。アクセス制御部807は、外部ディスク803に格納された暗号化データを復号化する。具体的にはアクセス制御部807はパスワード認証、指紋認証などを行って、アクセス制御部807は外部ディスク803内に格納される暗号化データを復号化する。アクセス制御部807は外部ディスク803への読み書きが許可されたことを判別すると、アクセス制御部807はシステム制御部806に対して外部ネットワーク802とパーソナルコンピュータ801とをアクセス禁止することを通知する。

[0137] システム制御部806はアクセス制御部807よりアクセス禁止の通知を受けると、システム制御部806はアクセス制御部807からの通知に基づいて、ネットアクセス制御部805に外部ネットワークへ802の遮断を指示する。

[0138] ネットアクセス制御部805は、システム制御部806からの指示に基づいて、パーソナルコンピュータ801の外部ネットワーク802へのアクセスを遮断する。

[0139] またネットアクセス制御部805は、NTP(Network Time Protcol)やping応答などの、秘匿データ(秘匿フォルダ、秘匿ファイル)の外部ネットワーク802への流出の可能性のないネットワークアクセスを許可する構成であってもよい。

[0140] [オープン処理のフローチャート]

図9は本実施例に係るNAS104に格納されるファイル、フォルダへのアクセス処理(オープン処理)に関するフローチャートである。

[0141] パーソナルコンピュータ101、102は、NAS104へアクセスする場合、パーソナルコンピュータ101、102は要求パケットをNAS104に送信する。

[0142] NAS104に搭載されるファイルアクセス監視部106は、NAS104にファイルアクセ

スした要求元のIPアドレス／MACアドレスを要求パケットから取り出す（ステップS901）。

[0143] ファイルアクセス監視部106は、BadPCList203を参照して、アクセス要求元に対応するOCN306の値は0より大きいか否かを判別する（ステップS902）。ファイルアクセス監視部106は、アクセス要求元に対応するOCN306の値が「0」より大きいと判別する場合（ステップS902 YES）、ファイルアクセス監視部106は要求元のファイルアクセスを禁止し（ステップS905）、アクセス処理を終了する（ステップS906）。

[0144] またファイルアクセス監視部106は、アクセス要求元に対応するOCN306の値が0よりも大きくない（具体的にはOCN306の値が0。）場合（ステップS902 NO）、システム制御部107はファイルアクセスを許可してオープン処理を実行する（ステップS903）。オープン処理は、システム制御部107がアクセス要求のあったファイルを開く処理である。

[0145] そしてシステム制御部107はオープン処理を失敗したか否かを判別する（ステップS904）。システム制御部107がオープン処理を失敗したと判別する場合（ステップS904 YES）、ファイルアクセス監視部106は要求元のファイルアクセスを禁止し（ステップS905）、アクセス処理を終了する（ステップS906）。システム制御部107がオープン処理に成功したと判別する場合（ステップS904 NO）、システム制御部107はオープン処理するファイルが保護対象のファイルであるか否かを判別する（ステップS907）。

[0146] システム制御部107が、オープン処理するファイルは保護対象であると判別する場合（ステップS908 YES）、システム制御部107はアクセス要求元に対応するin_use303をカウントアップして1増やし、protectフラグ305を「true」とし、BTLを「32」に設定する（ステップS908）。システム制御部107が、オープン処理するファイルは保護対象でないと判別する場合（ステップS909）、システム制御部107はオープン処理を終了する（ステップS909）。

[0147] ［クローズ処理のフローチャート］

図10は本実施例に係るNAS104に格納されるファイル、フォルダへのアクセス処理（クローズ処理）に関するフローチャートである。

[0148] パーソナルコンピュータ101、102は、NAS104へアクセスする場合、パーソナルコンピュータ101、102は要求パケットをNAS104に送信する。

[0149] NAS104に搭載されるファイルアクセス監視部106は、NAS104にファイルアクセスした要求元のIPアドレス／MACアドレスを要求パケットから取り出す（ステップS1001）。

[0150] ファイルアクセス監視部106は、要求元のIPアドレス／MACアドレスをシステム制御部107に通知し、システム制御部107はクローズ処理を行う（ステップS1002）。

[0151] そしてシステム制御部107はクローズ処理するファイルが保護対象のファイルであるか否かを判別する（ステップS1003）。システム制御部107が、クローズ処理するファイルは保護対象でないと判別する場合（ステップS1003 NO）、システム制御部107はクローズ処理を終了する（ステップS1006）。システム制御部107が、クローズ処理するファイルが保護対象であると判別する場合（ステップS1003 YES）、システム制御部107はその保護対象ファイルが属するフォルダ内のすべてのファイルがクローズであるか否かを判別する（ステップS1004）。

[0152] システム制御部107が、フォルダ内のすべてのファイルがクローズであると判別する場合（ステップS1004 YES）、システム制御部107はアクセス要求元に対応するin__use303をカウントダウンして1減らし（ステップS1005）、クローズ処理を終了する（ステップS1006）。またシステム制御部107が、フォルダ内のすべてのファイルはクローズでなわけではないと判別する場合（ステップS1004 NO）、システム制御部107はクローズ処理を終了する（ステップS1006）。

[0153] ［カウント処理のフローチャート］

図11は本実施例に係るルータ103が行うカウント処理のフローチャートである。図11に示すフローチャートを実行するルータ103の機能は、先述したBadPCList203を管理し、各パーソナルコンピュータ101、102が外部ネットワーク105との通信を許可されているか拒否されるかを判断する機能である。なおカウント処理は、パーソナルコンピュータ101、102と外部ネットワーク105との接続を遮断する時間を計る処理である。

[0154] ルータ103は内部タイマー（図示せず）を有している。ルータ103は、内部タイマー

によって1秒ごとに起動する。ルータ103はBadPCList203を参照する(ステップS1101)。ルータ103は、BadPCList203に登録される全てのパーソナルコンピュータ(パーソナルコンピュータ101、102)に対応するBTL304が「0」よりも大きいか否かを判別する(ステップS1102)。ルータ103が、BTL304が「0」よりも大きいと判別した場合(ステップS1103 YES)、ルータ103は「0」より大きいと判別したBTL304の値をカウントダウンして1減らす(ステップS1103)。

[0155] そしてルータ103は、カウントダウンして1減らした結果、BTL304が「0」になったか否かを判別する(ステップS1104)。ルータ103が、BTL304が「0」になったと判別した場合(ステップS1104 YES)、ルータ103は、BTL304が「0」になったと判別したprotectフラグ305を「true」から「false」にする(ステップS1105)。ルータ103が、BTL304が「0」でないと判別した場合(ステップS1104 NO)、ルータ103は全てのパーソナルコンピュータ(パーソナルコンピュータ101、102)に対応するOCN306が「0」よりも大きいか否かを判別する(ステップS1106)。またステップS1102において、BadPCList203に登録される全てのパーソナルコンピュータ(パーソナルコンピュータ101、102)に対応するBTL304が「0」よりも大きくないと判別する場合(ステップS1102 NO)、ルータ103は全てのパーソナルコンピュータ(パーソナルコンピュータ101、102)に対応するOCN306が「0」よりも大きいか否かを判別する(ステップS1106)。

[0156] ルータ103が、OCN306は「0」よりも大きいと判別した場合(ステップS1106 YES)、ルータ103はOCN306の値をカウントダウンして1減らす(ステップS1107)。ルータが全てのパーソナルコンピュータ(パーソナルコンピュータ101、102)に対応するOCN306が「0」よりも大きくないと判別する場合(ステップS1106 NO)、ルータ103はBadPCList203に登録される全てのエントリのBTL304、OCN306についてカウント処理を実行したか否かを判別する(ステップS1108)。

[0157] ルータ103がBadPCList203に登録される全エントリのBTL304、OCN306についてカウント処理を実行したと判別する場合(ステップS1108 YES)、ルータ103は処理を終了する(ステップS1109)。またルータ103がBadPCList203に登録される全エントリのBTL304、OCN306についてカウント処理を実行していないと判別する

場合（ステップS1108　NO）、ルータ103は再びBTL304の値が「0」よりも大きいか否かを判別する（ステップS1102）。

[0158] ［パケット転送処理のフローチャート］

図12は本実施例に係るルータ103が行うパケット転送処理のフローチャートである

ルータ103はパーソナルコンピュータ101、102からパケットを受信するとパケット転送処理を開始する（ステップS1201）。

[0159] ルータ103は受信したパケットのあて先が外部ネットワーク105、かつ受信したパケットの送信元がLAN内部のパーソナルコンピュータ101、102であるか否かを判別する（ステップS1202）。ルータ103が、パケットのあて先が外部ネットワーク105ではなく、又は受信したパケットの送信元がLAN内部のパーソナルコンピュータ101、102でないと判別する場合（換言すれば、少なくともパケットのあて先は外部ネットワーク105でなく、パケットの送信元はパーソナルコンピュータ101、102でない場合）（ステップS1202　NO）、ルータ103は、受信したパケットを所定のあて先へ転送して（ステップS1203）、パケット転送処理を終了する（ステップS1204）。

[0160] ルータ103が、パケットのあて先が外部ネットワーク105であり、かつ受信したパケットの送信元がLAN内部のパーソナルコンピュータ101、102であると判別する場合（ステップS1202　YES）、ルータ103は、パケット送信先のパーソナルコンピュータに対応するprotectフラグ305が「true」であるか否か判別する（ステップS1205）。

[0161] ルータ103がパケット送信先のパーソナルコンピュータに対応するprotectフラグ305が「true」でない（protectフラグ305が「false」）と判別する場合（ステップS1205　NO）、ルータ103は通信に使用するプロトコルに応じて、遅延値（X）を決定する（ステップS1208）。

[0162] そしてルータ103は、OCN306の値が遅延値（X）よりも小さいか否かを判別する（ステップS1209）。ルータ103が、OCN306の値は遅延値（X）よりも小さいと判別する場合（ステップS1209　YES）、ルータ103はOCNの値を遅延値（X）に設定する（ステップS1210）。

[0163] そしてルータ103が、OCN306の値は遅延値（X）よりも小さくないと判別する場合（ステップS1209　NO）、ルータ103はパケットの転送処理を行い（ステップS1211）、

パケット転送処理を終了する(ステップS1212)。

[0164] 図13は本実施例に係るNAS104のハードブロック図である。

[0165] NAS104におけるハード構成について説明する。NAS104はCPU(Central Processing Unit)1301、記憶部1302、メモリ1303、LANポート1304、1305から構成されている。

[0166] NAS104はLANポート1304を介してパーソナルコンピュータ101、102と接続している。またNAS104はLANポート1305を介してルータ103と接続している。

[0167] NAS104が有するファイルアクセス監視部106、システム制御部107、ファイルアクセス制御部110はそれぞれ、ソフトウェアとしてCPU1301が実行する機能である。そのためファイルアクセス監視部106、システム制御部107、ファイルアクセス制御部110はソフトウェアとして記憶部1302に格納されている。そしてCPU1301はファイルアクセス監視部106、システム制御部107、ファイルアクセス制御部110を実行する場合、CPU1301はファイルアクセス監視部106、システム制御部107、ファイルアクセス制御部110をメモリ1303に展開して実行する。

[0168] また図14は本実施例に係るNAS104の機能を記したネットワークストレージシステム100の構成図である。NAS104は、ファイルアクセス監視部106、システム制御部107、ファイルアクセス制御部110の機能を有している。ファイルアクセス監視部106、システム制御部107、ファイルアクセス制御部110はネットワークストレージシステム100を制御する機能である。マルウェアに感染したパーソナルコンピュータがNAS104にファイルアクセスした場合であっても、NAS104は、NAS104が格納するファイル、フォルダを外部ネットワーク105に流出することを防ぐことができる。

[0169] また図15は本実施例に係るルータ103の機能を記したネットワークストレージシステム100の構成図である。ルータ103は外部アクセス制御部108、外部アクセス監視部109の機能を有している。外部アクセス制御部108、外部アクセス監視部109は、ネットワークストレージシステム100を制御する機能である。外部アクセス制御部108は、パーソナルコンピュータ101、102から受信したパケットを外部ネットワーク105へ転送するか否かを制御する機能である。また外部アクセス監視部109は、外部ネットワーク105とパーソナルコンピュータ101、102との接続状況を監視する機能である。

ルータ103は、ソフトウェアとして外部アクセス制御部108、外部アクセス監視部109を実行して制御する。したがってルータ103も外部アクセス制御部108、外部アクセス監視部109を実行するためにCPU、記憶部、メモリ、またはこれらに順ずるハードウェアを有している。外部アクセス制御部108、外部アクセス監視部109はハード構成で物理的に存在するものであってもよい。

[0170] 外部アクセス制御部108、外部アクセス監視部109は、マルウェアに感染したパーソナルコンピュータがNAS104にファイルアクセスした場合であっても、NAS104が格納するファイル、フォルダを外部ネットワーク105に流出することを防ぐことができる。

産業上の利用可能性

[0171] 本実施例に係るネットワークストレージシステムは、ネットワークを介して接続するストレージ内のデータ保護に関する。

[0172] 本実施例におけるネットワークストレージシステムによれば、マルウェアや不用意・不適切なネットアクセスによるデータの外部ネットワークへの流出を有効に防ぐことができる。

請求の範囲

[1] 情報を格納し、情報処理装置にネットワークを介して該情報を提供する情報保持装置が実行する情報提供方法において、

該情報処理装置が該情報保持装置内の該情報にアクセスしたことを検出するアクセス検出手順と、

該情報処理装置が情報保持装置に情報をアクセス中は該情報処理装置の情報の転送を制御する制御手順と、

からなることを特徴とする情報提供方法。

[2] 請求項1に記載の情報提供方法において、

該アクセス検出手順は、該情報処理装置から受信する要求パケットを参照して、該情報へのアクセスを検出することを特徴とする情報提供方法。

[3] 請求項1に記載の情報提供方法において、

該アクセス検出手順は、該情報保持装置が格納する該情報の属性を判別することを特徴とする情報提供方法。

[4] 請求項3に記載の情報提供方法において、

該ファイルアクセス検出手順は、該情報が保持するフラグに基づいて該情報の属性を判別することを特徴とする情報提供方法。

[5] 請求項4に記載の情報提供方法において、

該制御手順は、該アクセス検出手順において判別した該情報の属性に応じて、該情報処理装置の該情報の転送を制御することを特徴とする情報提供方法。

[6] 請求項5に記載の情報提供方法において、

該制御手順は、該ネットワークの中継を行う中継器に対して該情報の転送を制御することを特徴とする情報提供方法。

[7] 情報処理装置と情報保持装置を含むネットワークと外部ネットワークとを接続する中継器が実行する中継方法において、

該情報処理装置の該情報保持装置へのアクセス状況を管理するアクセス管理手順と、

該アクセス管理手順において管理する該アクセス状況に応じて、該情報処理装置

から該外部ネットワークへの該情報の転送を禁止する外部アクセス制御手順と、

からなることを特徴とする中継方法。

[8] 請求項7に記載の中継方法において、

該アクセス管理手順は、該情報保持装置から該アクセス状況を取得することを特徴とする中継方法。

[9] 請求項8に記載の中継方法において、

該アクセス管理手順は、該外部アクセス制御手順において該情報処理装置から該外部ネットワークへの該情報の転送を禁止しておく時間を管理することを特徴とする中継方法。

[10] 請求項9に記載の中継方法において、

さらに該情報処理装置と該外部ネットワークとの接続を検出する外部アクセス検出手順を有することを特徴とする中継方法。

[11] 請求項10に記載の中継器において、

該アクセス管理手順は、該情報処理装置と該外部ネットワークとの接続状況を管理することを特徴とする中継方法。

[12] 請求項11に記載の中継方法において、

該アクセス管理手順は、該情報処理装置と該外部ネットワークとの接続状況に応じて、該情報処理装置から該情報保持装置へのアクセスを禁止する時間を管理することを特徴とする中継方法。

[13] 情報処理装置とネットワークを介して接続される情報保持装置が実行する情報提供方法において、

該情報保持装置が保持するファイルに対応する特徴パターンを生成する特徴パターン生成手順と

該特徴パターンを格納する格納手順と、

からなることを特徴とする情報提供方法。

[14] 請求項13に記載の情報提供方法は、

さらに該特徴パターンに対応するファイルを検索するファイル検索手順を有することを特徴とする情報提供方法。

[15] 請求項14に記載の情報提供方法は、

さらに該情報処理装置から該情報保持装置へのファイルアクセスを検出するファイルアクセス検出手順を有することを特徴とする情報提供方法。

[16] 請求項15に記載の情報提供方法は、

さらに該ファイル検索手順において該特徴パターンに対応するファイルを新たに検出した場合、検出したファイルをファイルアクセス検出手順における監視対象として追加する追加手順を有することを特徴とする情報提供方法。

[17] 情報処理装置と情報保持装置を含むネットワークと外部ネットワークとを接続する中継方法において、

該情報処理装置から受信するパケット内に、該情報保持装置が保持するファイルに対応する特徴パターンが有るか否かを判別するパケット監視手順と、

該特徴パターンを有するパケットを破棄する外部アクセス制御手順と、

からなることを特徴とする情報提供方法。

[18] 情報を格納し、情報処理装置にネットワークを介して該情報を提供する情報保持装置において、

該情報処理装置が該情報保持装置内の該情報にアクセスしたことを検出するファイルアクセス検出部と、

該情報処理装置が情報保持装置に情報をアクセス中は該情報処理装置の情報の転送を制御するシステム制御部と、

を備えたことを特徴とする情報保持装置。

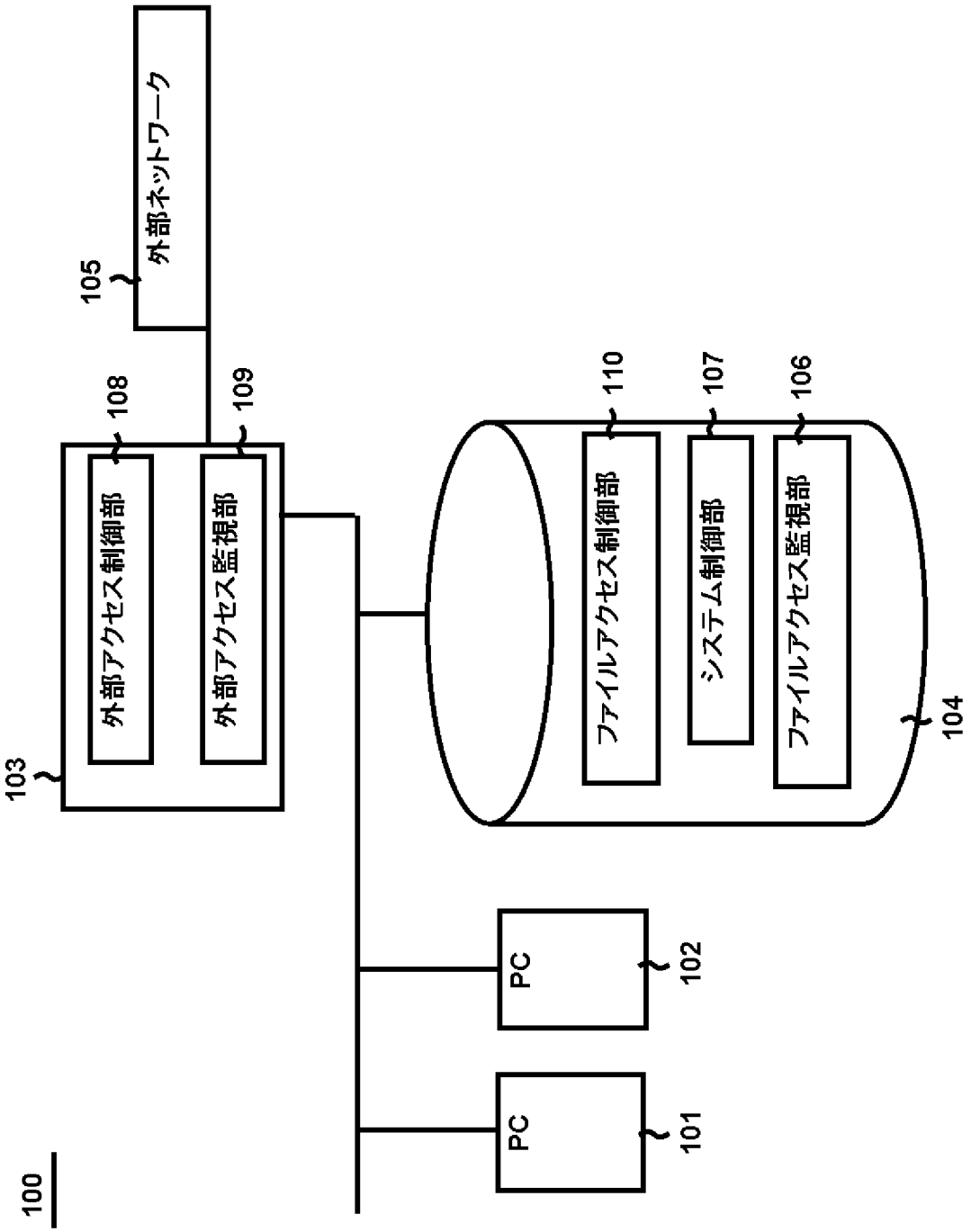
[19] 情報処理装置と情報保持装置を含むネットワークと外部ネットワークとを接続する中継器において、

該情報処理装置の該情報保持装置へのアクセス状況を管理するアクセス管理部と、

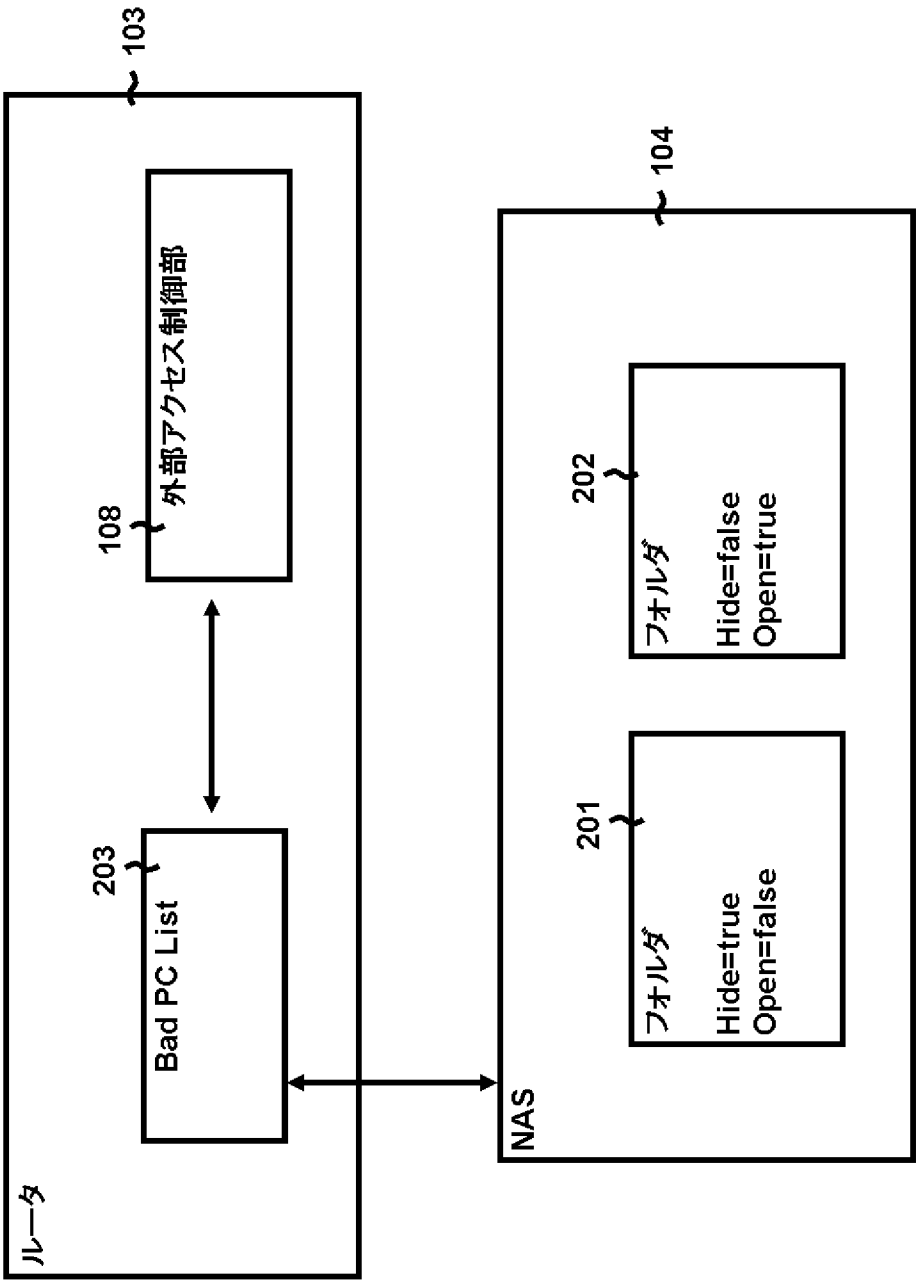
該アクセス管理部が管理する該アクセス状況に応じて、該情報処理装置から該外部ネットワークへの該情報の転送を禁止する外部アクセス制御部と、

からなることを特徴とする中継器。

[図1]


外部ネットワーク
105
外部アクセス制御部
108
外部アクセス監視部
109
103
ファイルアクセス制御部
110
システム制御部
107
ファイルアクセス監視部
106
104
PC
102
PC
101
100

[図2]

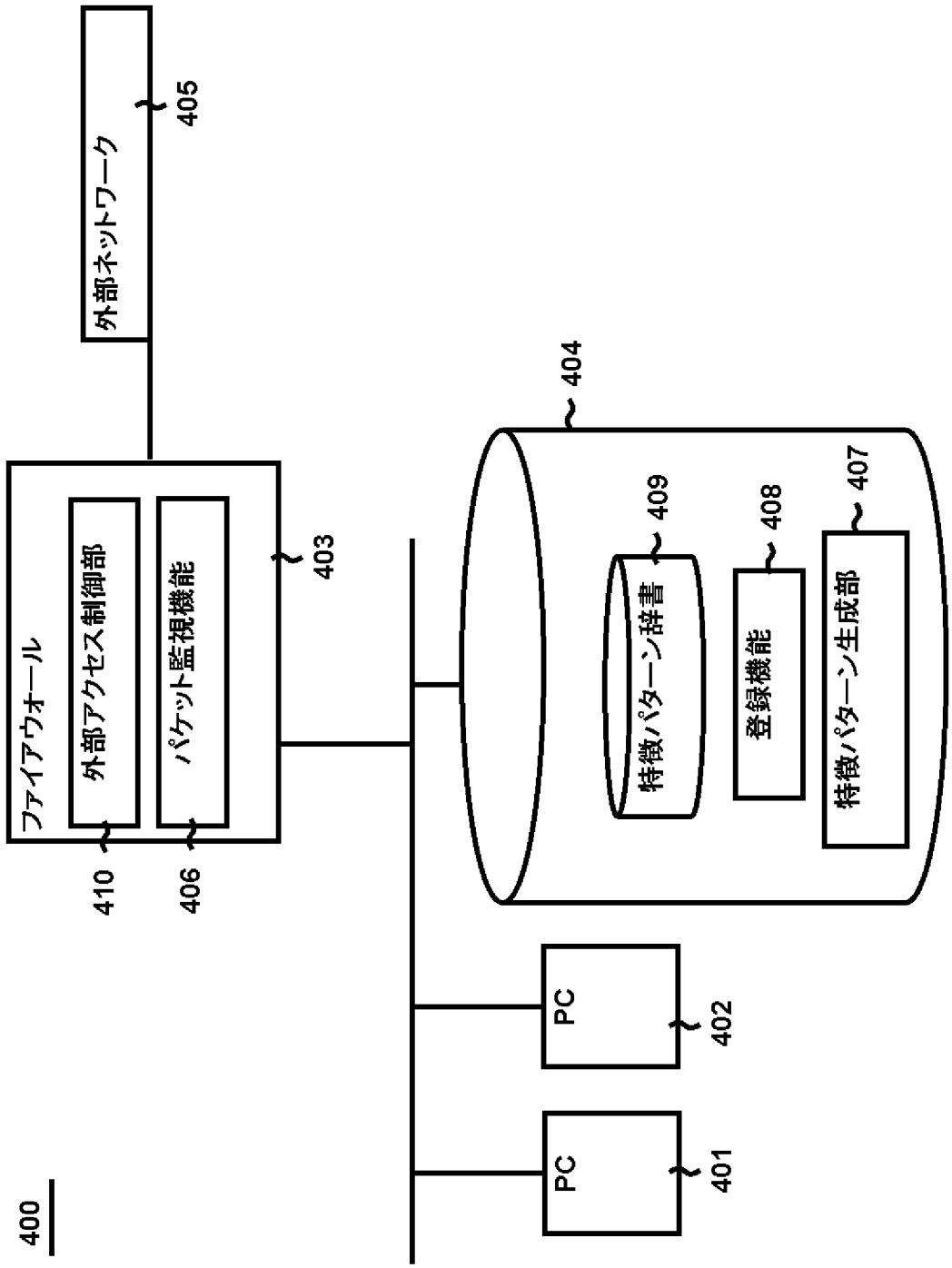

103
ルータ
外部アクセス制御部
108
Bad PC List
203
104
NAS
202
フォルダ
Hide=false
Open=true
201
フォルダ
Hide=true
Open=false

[図3]

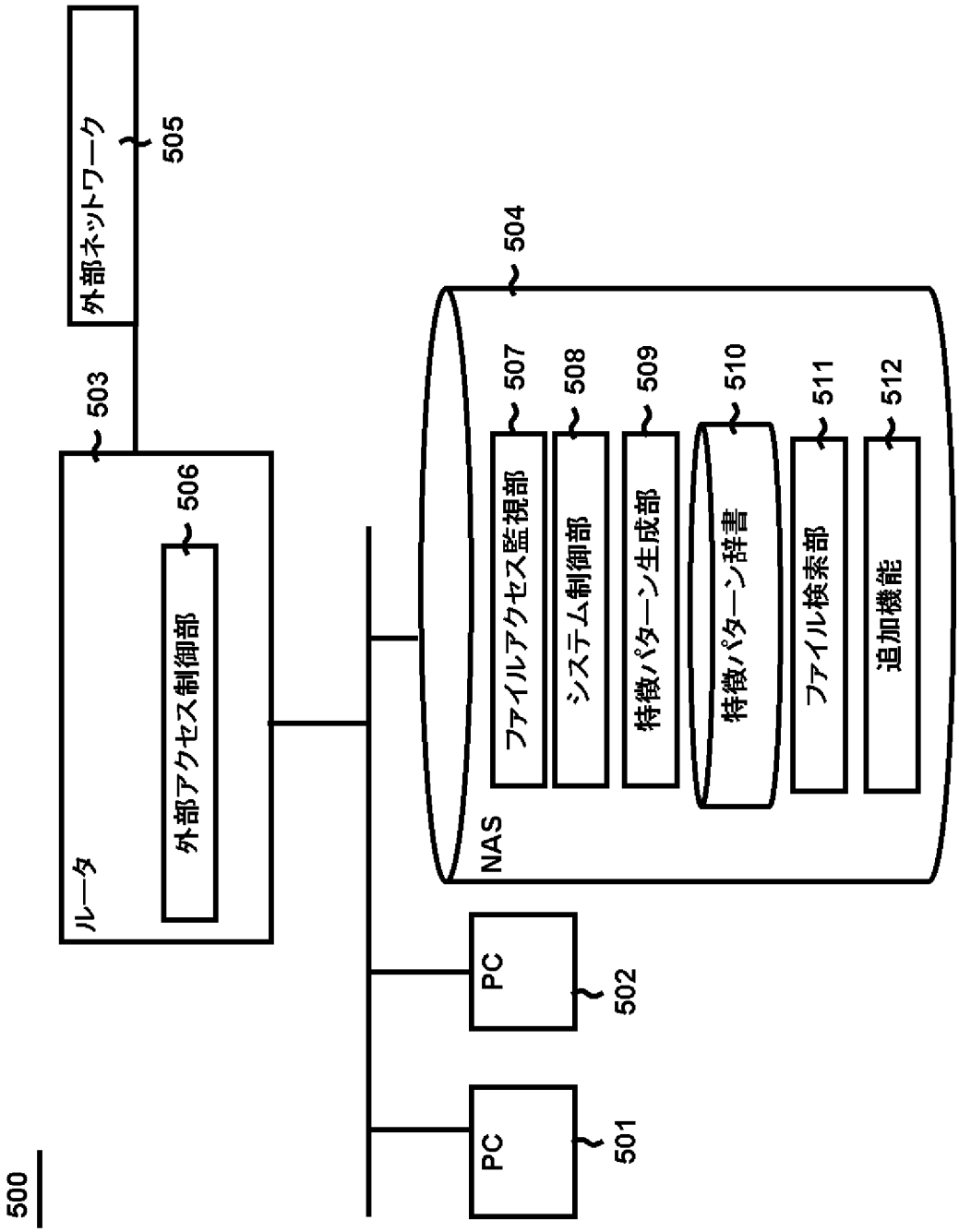
203

301 IPアドレス	302 MACアドレス	303 in_use	304 BTL	305 protect	306 OCN
192.168.3.32	10:20:30:40:50:01	0	0	false	0
192.168.3.33	10:20:30:40:50:02	2	32	true	0
192.168.3.34	10:20:30:40:50:03	0	0	false	15

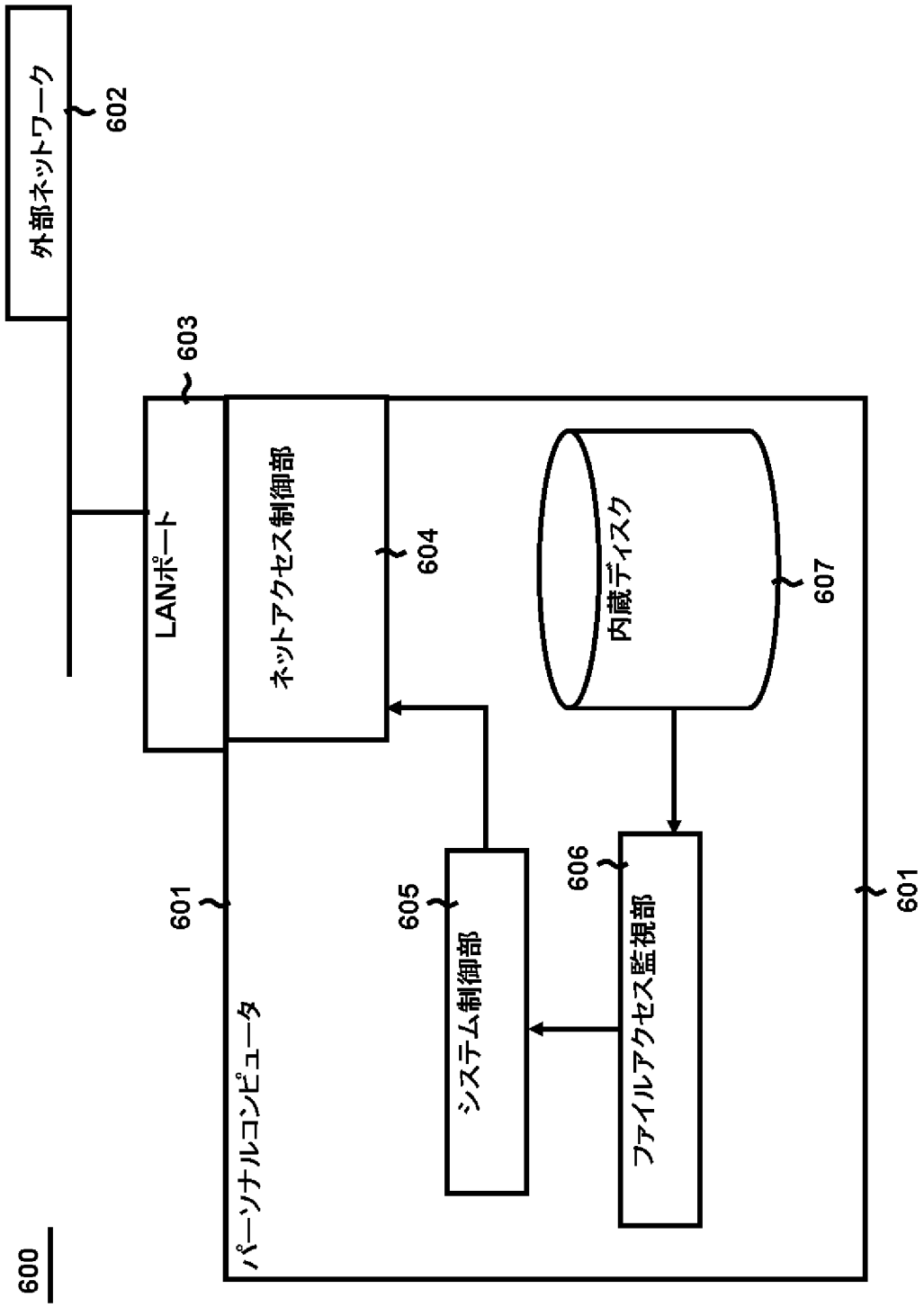
[図4]


400
PC
401
PC
402
ファイアウォール
外部アクセス制御部
パケット監視機能
403
410
406
外部ネットワーク
405
404
特徴パターン辞書
409
登録機能
408
特徴パターン生成部
407

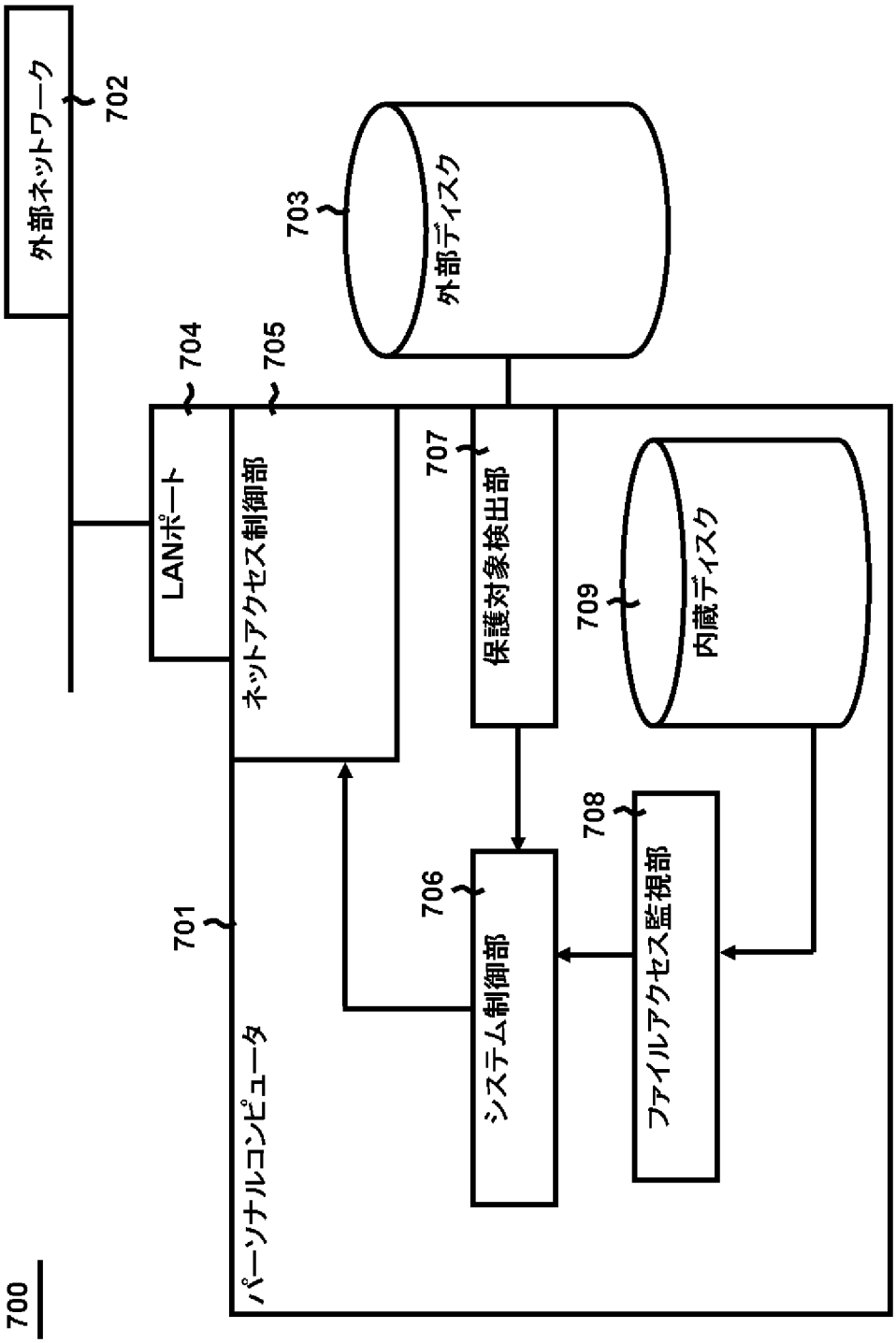
[図5]


500
PC
501
PC
502
ルータ
503
外部アクセス制御部
506
外部ネットワーク
505
NAS
504
ファイルアクセス監視部
507
システム制御部
508
特徴パターン生成部
509
特徴パターン辞書
510
ファイル検索部
511
追加機能
512

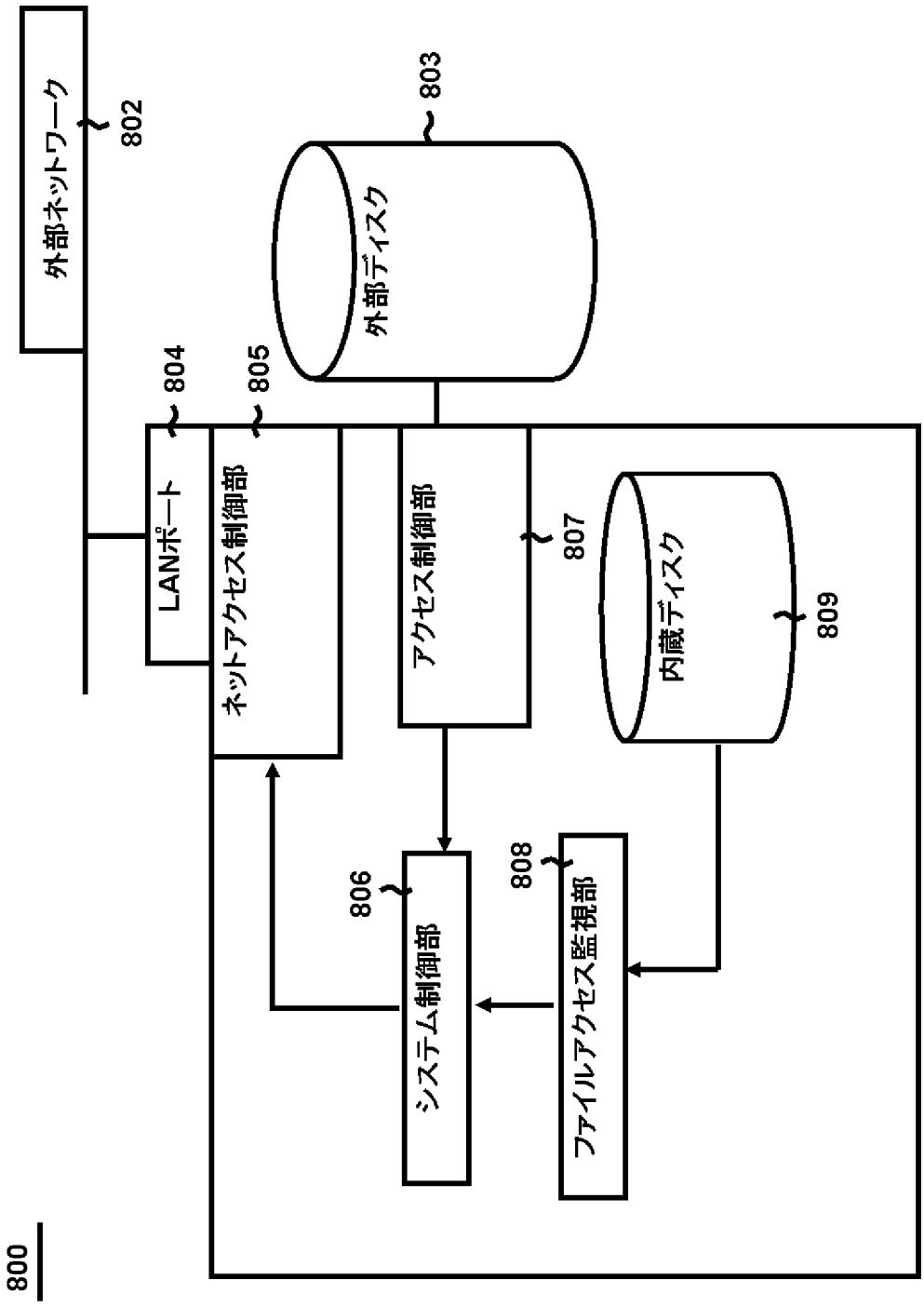
[図6]


外部ネットワーク
602
603
LANポート
ネットアクセス制御部
604
内蔵ディスク
607
601
605
システム制御部
606
ファイルアクセス監視部
601
パーソナルコンピュータ
600

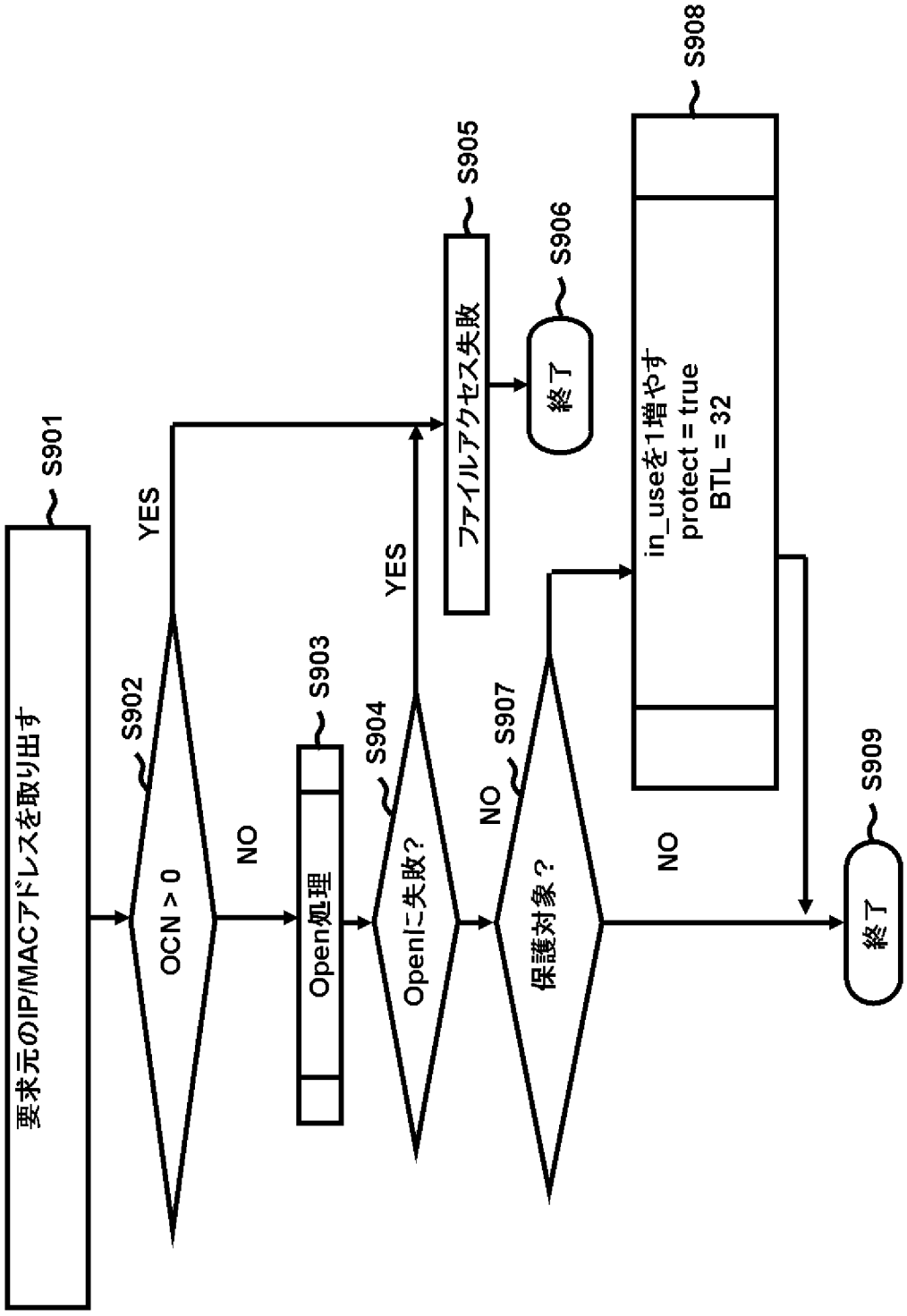
[図7]


外部ネットワーク
702
703
外部ディスク
704
705
LANポート
ネットアクセス制御部
707
保護対象検出部
709
内蔵ディスク
708
706
システム制御部
ファイルアクセス監視部
701
パーソナルコンピュータ
700

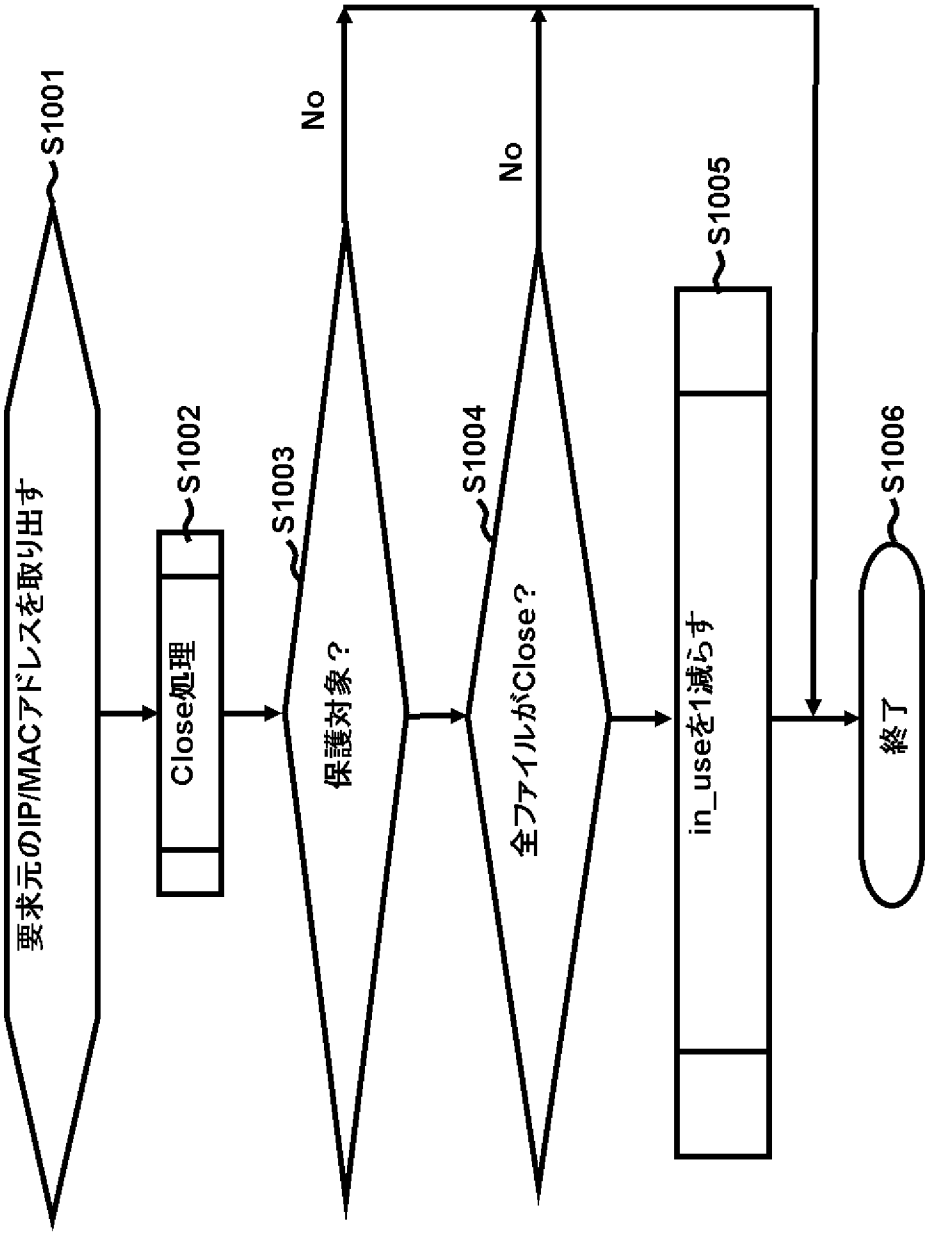
[図8]


外部ネットワーク
802
803
外部ディスク
804
805
LANポート
ネットアクセス制御部
アクセス制御部
807
内蔵ディスク
809
806
システム制御部
808
ファイルアクセス監視部
800

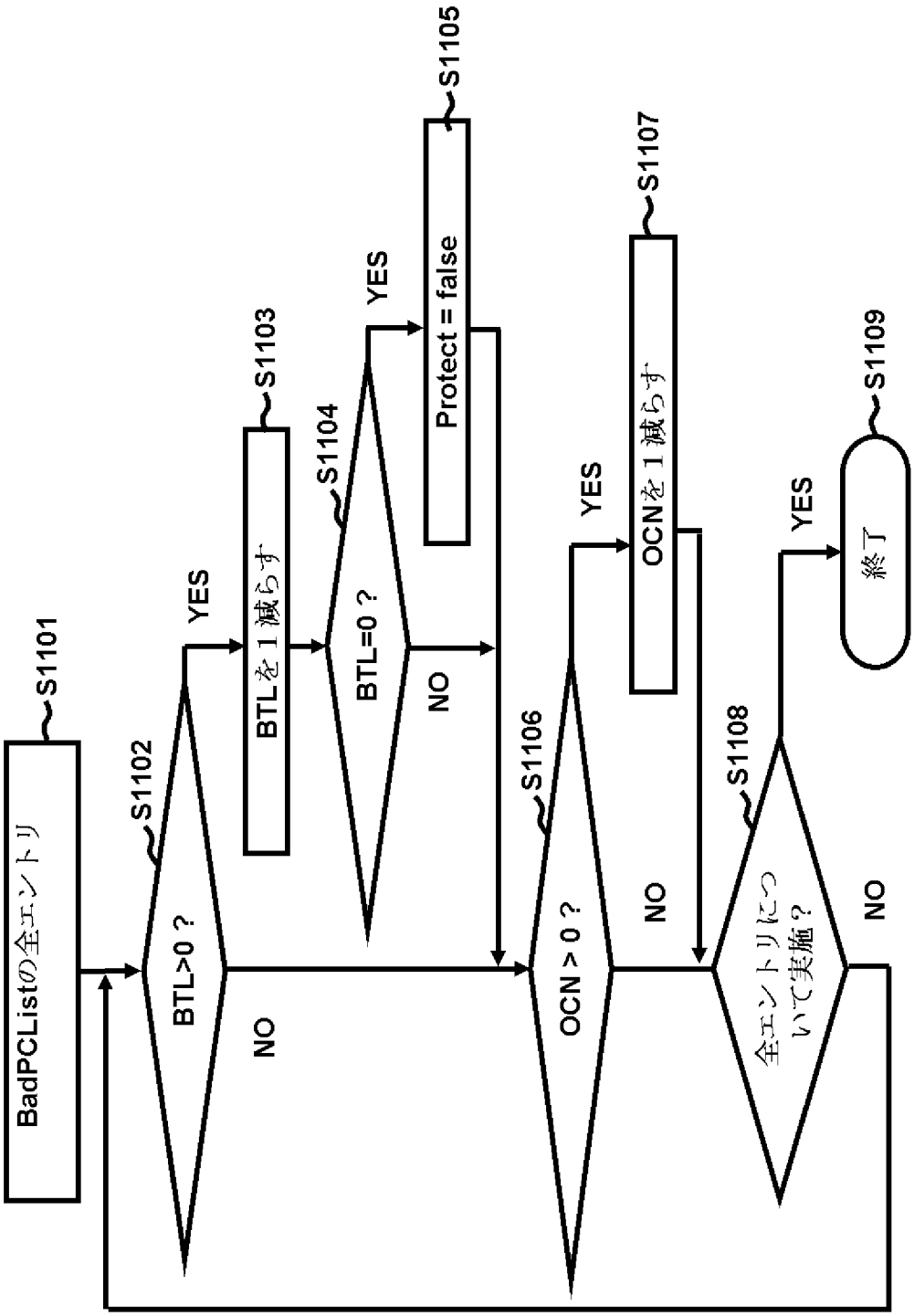
[図9]


S901
要求元のIP/MACアドレスを取り出す
S902
OCN > 0
YES
NO
S903
Open処理
S904
Openに失敗?
YES
S905
ファイルアクセス失敗
S906
終了
NO
S907
保護対象?
S908
in_useを1増やす
protect = true
BTL = 32
NO
S909
終了

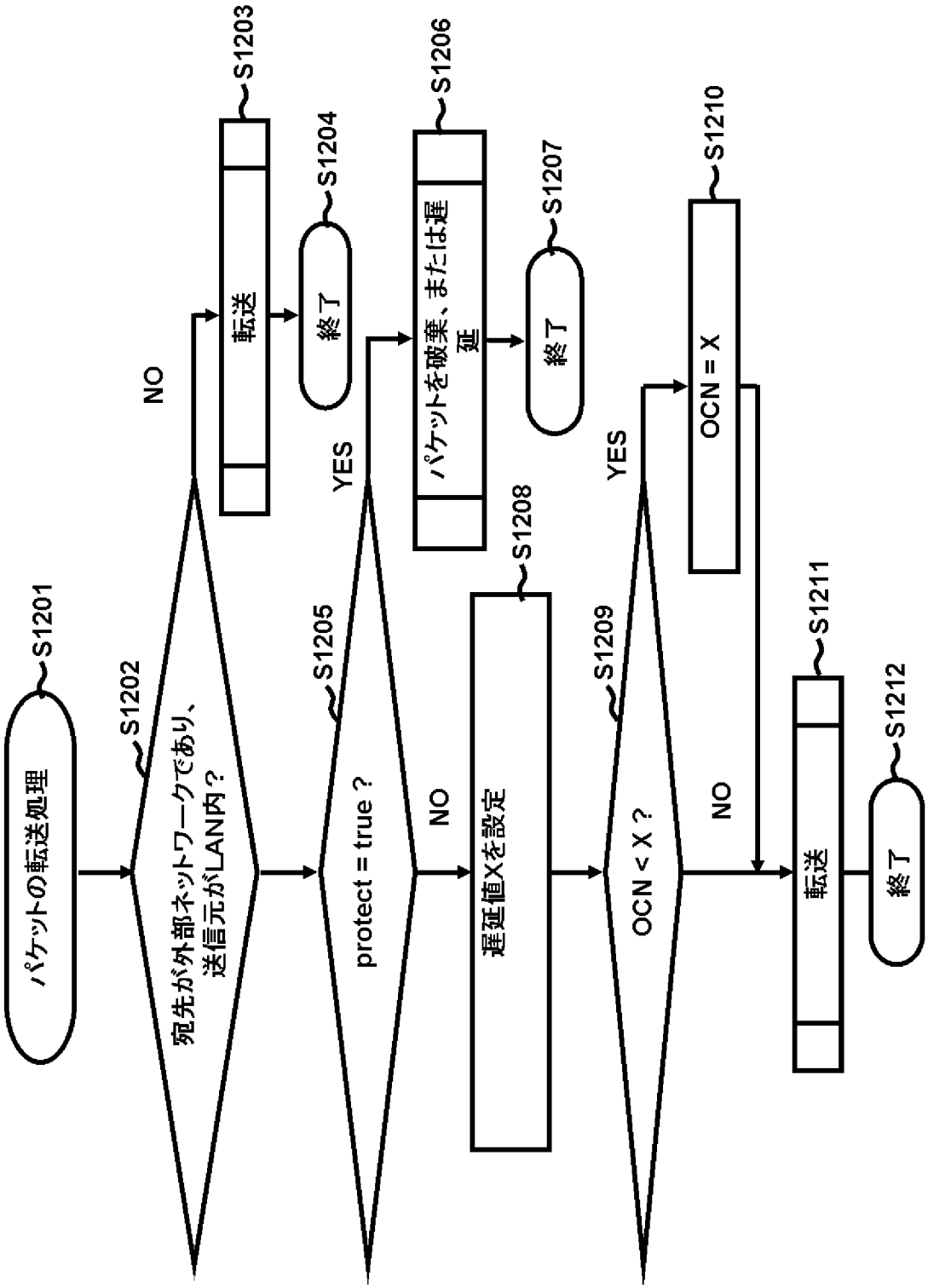
[図10]


S1001
要求元のIP/MACアドレスを取り出す
S1002
Close処理
S1003
保護対象？
No
S1004
全ファイルがClose？
No
S1005
in_useを1減らす
S1006
終了

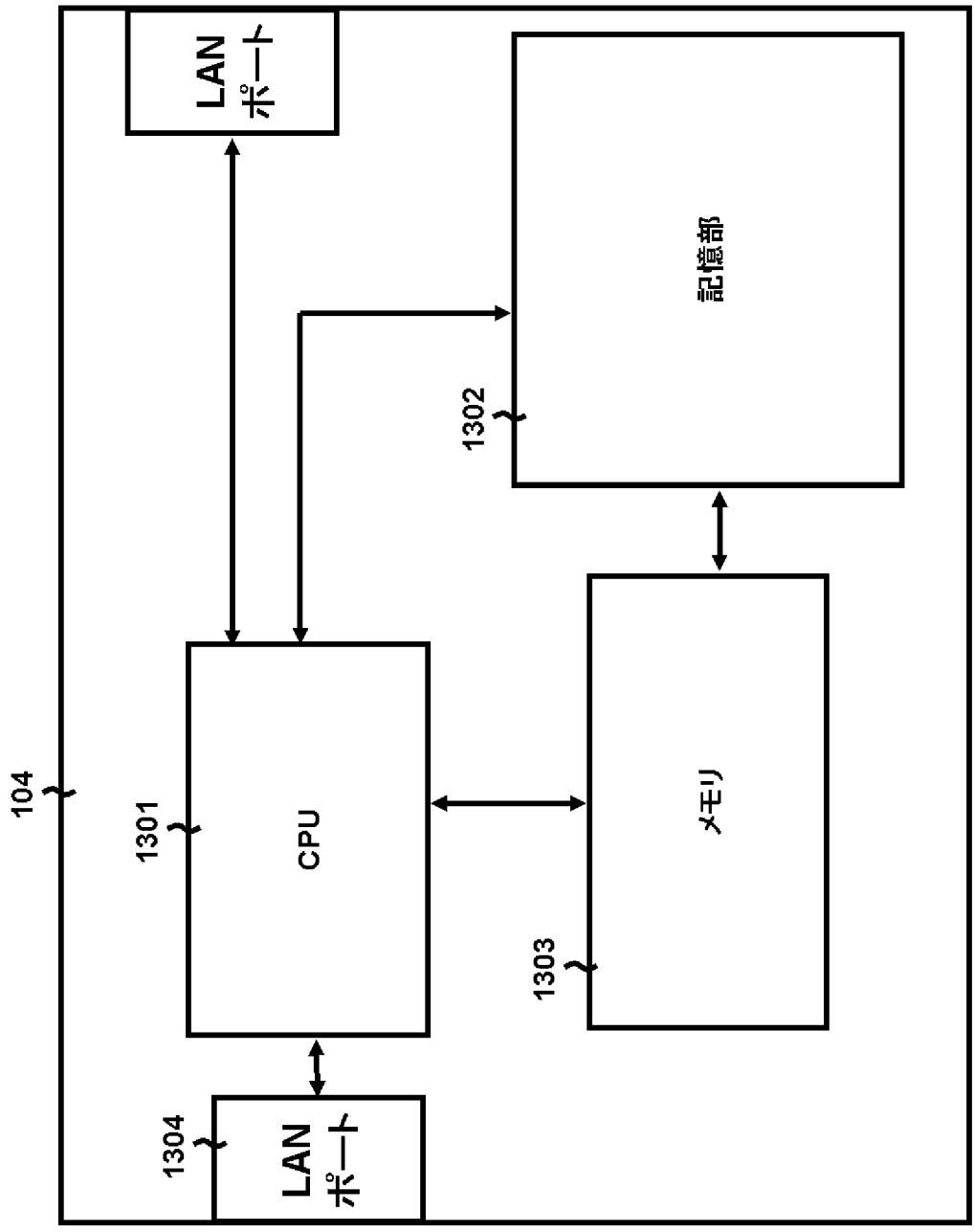
[図11]


S1101
BadPCListの全エントリ
S1102
BTL>0 ?
YES
NO
S1103
BTLを1減らす
S1104
BTL=0 ?
YES
NO
S1105
Protect = false
S1106
OCN > 0 ?
YES
NO
S1107
OCNを1減らす
S1108
全エントリについて実施？
YES
NO
S1109
終了

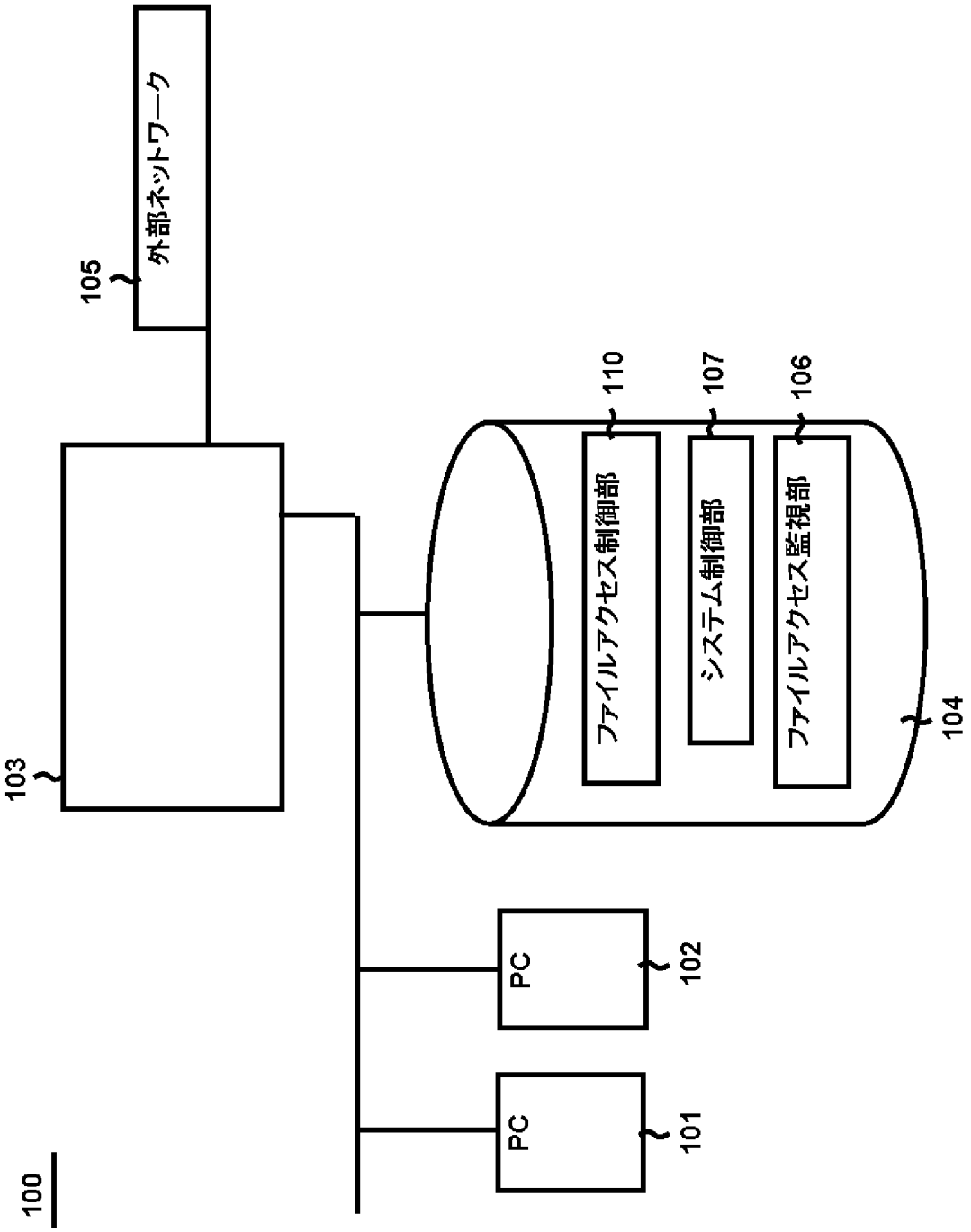
[図12]


S1201
パケットの転送処理
S1202
宛先が外部ネットワークであり、送信元がLAN内？
NO
S1203
転送
S1204
終了
YES
S1205
protect = true ？
NO
S1206
パケットを破棄、または遅延
S1207
終了
S1208
遅延値Xを設定
S1209
OCN < X ？
YES
S1210
OCN = X
NO
S1211
転送
S1212
終了

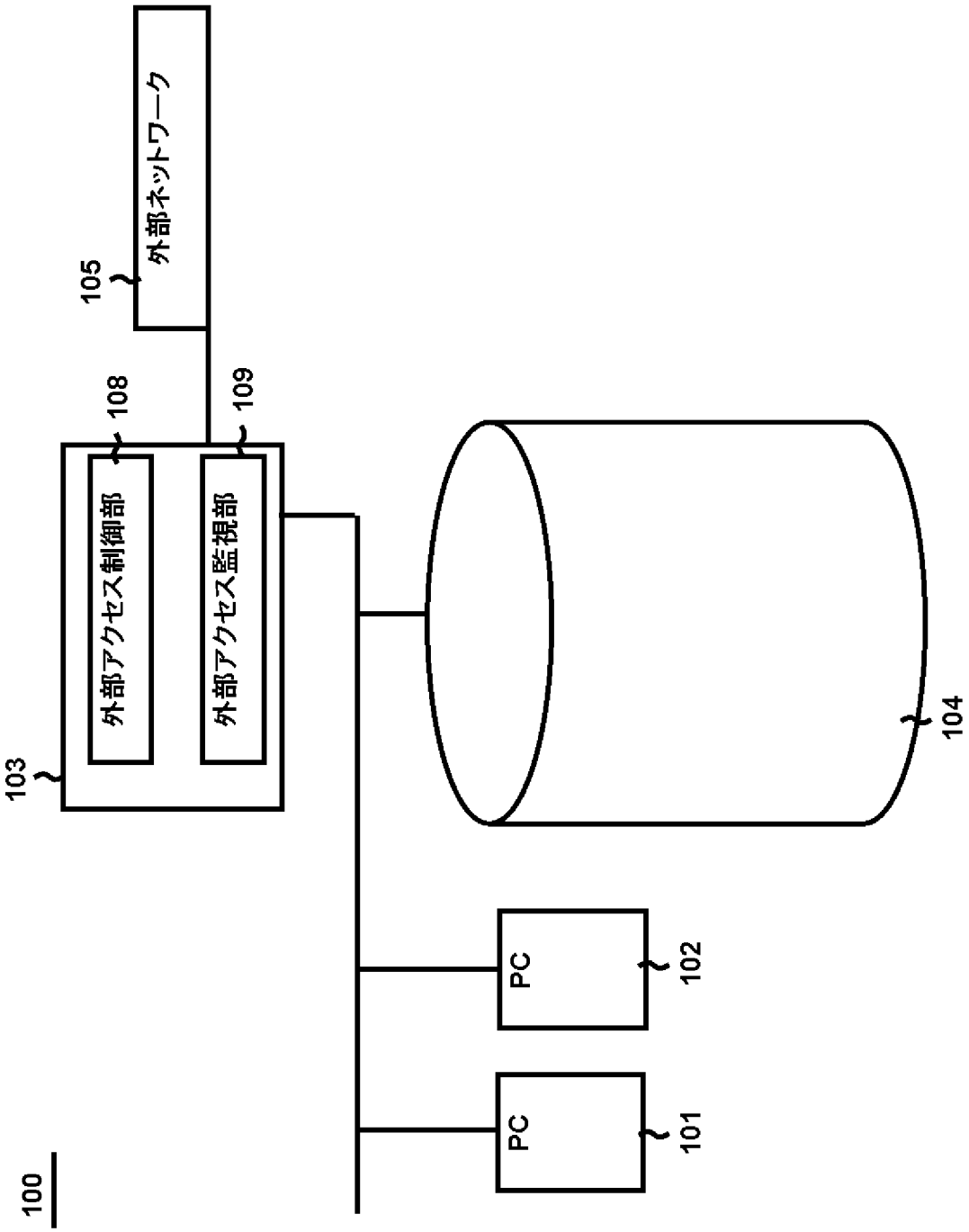
[図13]



[図14]


外部ネットワーク
105
110
107
106
ファイルアクセス制御部
システム制御部
ファイルアクセス監視部
104
103
PC
102
PC
101
100

[図15]


外部ネットワーク
105
108
109
外部アクセス制御部
外部アクセス監視部
103
104
PC
102
PC
101
100

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2007/070796

A. CLASSIFICATION OF SUBJECT MATTER
G06F21/20(2006.01)i, *G06F21/24*(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)
G06F21/20, G06F21/24

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 1996-2008
Kokai Jitsuyo Shinan Koho 1971-2008 Toroku Jitsuyo Shinan Koho 1994-2008

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	JP 2006-085401 A (Hitachi, Ltd.), 30 March, 2006 (30.03.06), Par. Nos. [0021] to [0024] & US 2006/0059279 A1	1-6,18
X Y	JP 2005-130214 A (Shimane University), 19 May, 2005 (19.05.05), Par. Nos. [0016], [0017]; Figs. 1, 2 (Family: none)	17 13-16
Y	WO 2004/100456 A1 (Sony Corp.), 18 November, 2004 (18.11.04), Pages 10, 15, 16; Figs. 1, 7, 8 & US 2005/0229245 A1 & EP 1624622 A1 & JP 2004-336619 A	7-12,19

☒ 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
11 March, 2008 (11.03.08)	18 March, 2008 (18.03.08)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2007/070796

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2002-312316 A (Sumisho Computer Systems Corp.), 25 October, 2002 (25.10.02), Par. Nos. [0038], [0061], [0063]; Fig. 6 (Family: none)	7-12,19
Y	JP 2004-185312 A (Canon Inc.), 02 July, 2004 (02.07.04), Par. No. [0029] & US 2004/0111603 A1	13-16
Y	JP 3994126 B1 (Quality Corp.), 17 October, 2007 (17.10.07), Par. No. [0125] (Family: none)	16

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2007/070796

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

Prior art publication: JP 2006-085401 A (Hitachi, Ltd.), 30 March, 2006 (30.03.06), paragraphs [0021]-[0024] & US 2006/0059279 A1.
The inventions in claims 1 and 2 have been publicly known by the publication, and the inventions in the claims of this application are categorized into the following five groups:
(continued to extra sheet)

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☒ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

the

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☐ No protest accompanied the payment of additional search fees.

Continuation of Box No.III of continuation of first sheet(2)

Invention group A: Claims 1, 2 and 18
Invention group B: Claims 3-6
Invention group C: Claims 7-12 and 19
Invention group D: Claims 13-16
Invention group E: Claim 17

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００７／０７０７９６

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　G06F21/20(2006.01)i, G06F21/24(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.　G06F21/20, G06F21/24

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	１９７１－２００８年
日本国実用新案登録公報	１９９６－２００８年
日本国登録実用新案公報	１９９４－２００８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	JP 2006-085401 A (株式会社日立製作所) 2006.03.30, par.nos.[0021]-[0024] & US 2006/0059279 A1	1-6, 18
X	JP 2005-130214 A (国立大学法人島根大学) 2005.05.19,	17
Y	par.nos.[0016], [0017]; Figs. 1, 2 (ファミリーなし)	13-16
Y	WO 2004/100456 A1 (ソニー株式会社) 2004.11.18, p.10, 15, 16; Fig.1, 7, 8 & US 2005/0229245 A1 & EP 1624622 A1 & JP 2004-336619 A	7-12, 19

☑　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 １１．０３．２００８	国際調査報告の発送日 １８．０３．２００８
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）　５Ｓ　３４４９ 石川　正二 電話番号　０３－３５８１－１１０１　内線　３５４６

C（続き）．　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
Y	JP 2002-312316 A (住商情報システム株式会社) 2002.10.25, par.nos.[0038], [0061], [0063]; Fig.6 (ファミリーなし)	7-12, 19
Y	JP 2004-185312 A (キヤノン株式会社) 2004.07.02, par.no.[0029] & US 2004/0111603 A1	13-16
Y	JP 3994126 B1 (クオリティ株式会社) 2007.10.17, par.no.[0125] (ファミリーなし)	16

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００７／０７０７９６

第Ⅱ欄　請求の範囲の一部の調査ができないときの意見（第１ページの２の続き）

法第8条第3項（ＰＣＴ17条(2)(a)）の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

１．☐ 請求の範囲＿＿＿＿＿＿＿＿は、この国際調査機関が調査をすることを要しない対象に係るものである。
つまり、

２．☐ 請求の範囲＿＿＿＿＿＿＿＿は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、

３．☐ 請求の範囲＿＿＿＿＿＿＿＿は、従属請求の範囲であってＰＣＴ規則6.4(a)の第２文及び第3文の規定に従って記載されていない。

第Ⅲ欄　発明の単一性が欠如しているときの意見（第１ページの３の続き）

次に述べるようにこの国際出願に二以上の発明があるとこの国際調査機関は認めた。

公知文献：JP 2006-085401 A（株式会社日立製作所）2006.03.30,
par.nos.[0021]-[0024] & US 2006/0059279 A1

請求の範囲１及び２に係る発明は、上記の先行技術によって公知のものであり、本願の各請求の範囲に係る発明は、上記の先行技術との対比によって、以下の５群に区分される。

発明群Ａ：請求の範囲１、２、１８
発明群Ｂ：請求の範囲３－６
発明群Ｃ：請求の範囲７－１２、１９
発明群Ｄ：請求の範囲１３－１６
発明群Ｅ：請求の範囲１７

１．☐ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。

２．☑ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。

３．☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったので、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。

４．☐ 出願人が必要な追加調査手数料を期間内に納付しなかったので、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

追加調査手数料の異議の申立てに関する注意

☐ 追加調査手数料及び、該当する場合には、異議申立手数料の納付と共に、出願人から異議申立てがあった。
☐ 追加調査手数料の納付と共に出願人から異議申立てがあったが、異議申立手数料が納付命令書に示した期間内に支払われなかった。
☐ 追加調査手数料の納付はあったが、異議申立てはなかった。