

(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
2017年1月26日(26.01.2017)



(10) 国際公開番号
WO 2017/013894 A1

- (51) 国際特許分類:
H04L 12/66 (2006.01) H04L 12/22 (2006.01)
- (21) 国際出願番号: PCT/JP2016/057175
- (22) 国際出願日: 2016年3月8日(08.03.2016)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願 2015-145636 2015年7月23日(23.07.2015) JP
- (71) 出願人: NECプラットフォームズ株式会社
(NEC PLATFORMS, LTD.) [JP/JP]; 〒2138511 神奈川県川崎市高津区北見方2丁目6番1号 Kanagawa (JP).
- (72) 発明者: 鈴木 義明(SUZUKI Yoshiaki); 〒2138511 神奈川県川崎市高津区北見方2丁目6番1号 NECプラットフォームズ株式会社内 Kanagawa (JP).
- (74) 代理人: 永井 道雄(NAGAI Michio); 〒1060041 東京都港区麻布台2丁目4番5号メソニック39 M Tビル LOGOS総合特許商標事務所 Tokyo (JP).

- (81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, KE, KG, KN, KP, KR, 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, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.
- (84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーロパ (AM, AZ, BY, KG, KZ, RU, TJ, TM), ユーロッパ (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).

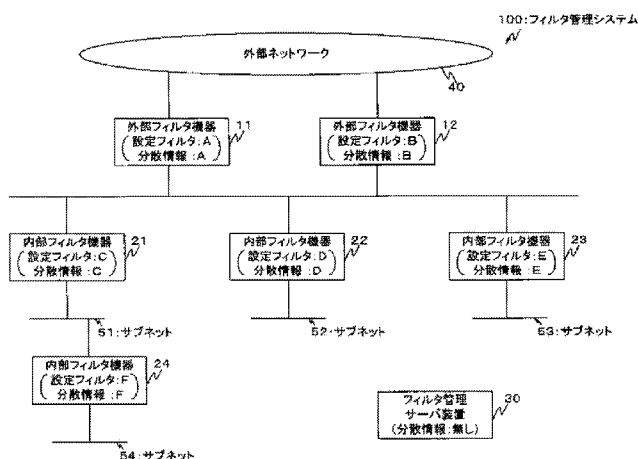
添付公開書類:

— 国際調査報告 (条約第21条(3))

(54) Title: FILTERING SYSTEM, MANAGEMENT DEVICE, FILTERING METHOD, AND MANAGEMENT PROGRAM

(54) 発明の名称: フィルタリングシステム、管理装置、フィルタリング方法及び管理プログラム

[図1]



- 11, 12 External filter apparatus (Set filter: Distribution information:)
21, 22, 23, 24 Internal filter apparatus (Set filter: Distribution information:)
30 Filter management server device (Distribution information: None)
40 External network
51, 52, 53, 54 Subnet
100 Filter management system

(57) Abstract: The present invention prevents all filter rules from leaking out and prevents the filter function of an entire network from stopping even when a problem occurs in a filter apparatus or the like that performs filtering. Provided is a filtering system provided with a plurality of apparatuses for filtering communication data on the basis of filter rules and a management device for managing the filter rules. When a first apparatus connected to an external network without being routed via the other apparatuses enters a prescribed state, distributed filter rules that are set in the first apparatus are restored by the management device on the basis of a plurality of distributed filter rules received from a plurality of second apparatuses connected to the external network via the first apparatus, and the distributed filter rules thus restored are set in the plurality of second apparatuses, the distributed filter rules being distributed such that the filter rules can be restored without using all of the distributed filter rules.

(57) 要約:

[続葉有]

WO 2017/013894 A1



フィルタリングを行なうフィルタ機器等に問題が生じたとしても、フィルタ規則の全てが流出したり、ネットワーク全体のフィルタ機能が停止したりすることを防止する。フィルタ規則に基づいて通信データのフィルタリングを行なう複数の機器と、前記フィルタ規則を管理する管理装置と、を備えるフィルタリングシステムの前記管理装置が、外部ネットワークに他の前記機器を介することなく接続している第1の前記機器が所定の状態になった場合に、前記第1の機器を介して外部ネットワークに接続している複数の第2の前記機器から受信した複数の分散フィルタ規則に基づいて前記第1の機器に設定されている分散フィルタ規則を復元し、該復元した分散フィルタ規則を前記複数の第2の機器に設定し、前記分散フィルタ規則は、全ての分散フィルタ規則を用いることなく前記フィルタ規則を復元可能に分散されている。

明 細 書

発明の名称：

フィルタリングシステム、管理装置、フィルタリング方法及び管理プログラム

技術分野

[0001] 本発明は、通信時に用いるフィルタ規則を管理するための、フィルタリングシステム、管理装置、フィルタリング方法及び管理プログラムに関する。

背景技術

[0002] パケット通信等の通信分野において、所定のフィルタ規則に基づいて、不適切なデータをフィルタリングすることが一般的に行われている。

[0003] 具体的には、通信されるデータをパケット単位で監視する。そして、監視対象のパケットのヘッダ情報に含まれるアドレス、ポート番号及びプロトコルの種別といった所定の項目の内容と、フィルタ規則としてデータベース化されているパケットのアドレス、ポート番号及びプロトコルの種別といった所定の項目のパターンとを比較する。そして、比較した両者の内容が合致するか否かに基づいて、監視対象のパケットを通過させるか否かを決定する。

[0004] このようなフィルタリングを行なう場合に、全てのパケットを正確かつ迅速に判定するためには、設定されたフィルタ規則に基づいてフィルタリングを行なう機器（以下、「フィルタ機器」と呼ぶ。）に十分な処理能力が必要となる。つまり、フィルタ機器の性能とフィルタリングの能力とはトレードオフの関係となる。そして、どのような状況下であっても問題が生じないような、十分な処理能力のフィルタ機器を必ずしも用意できるとは限らない。

[0005] 例えば、現在のルータやファイアウォールの大半には、パケットをフィルタリングする機能が含まれている。つまり、ルータやファイアウォールはフィルタ機器として動作する。しかし、これらルータ等の処理能力には限界がある。そのため、通常使用時には何らの問題も起きないとしても、D o s 攻撃（Denial of Service attack）等の不正な攻撃により大量のパケットを受

信してしまうと、処理を行なうCPU（Central Processing Unit）の負荷が増大してしまい、結果としてフィルタリングの機能自体が停止してしまうことがある。

[0006] このフィルタリング機能の停止のような事態の発生を防止するためには、ルータ等のフィルタ機器にかかる負荷を可能な限り抑えた上で、通信パケットの検査を行う必要がある。

[0007] また、別途の課題として、近年、インターネット等の外部ネットワークのみでなく、LAN（Local Area Network）等の内部ネットワークからの不正アクセス問題も増加しており、内部セキュリティを強化する必要も生じている。

[0008] ここで、フィルタ機器にかかる負荷を軽減すると共に、内部ネットワークでの不正アクセス問題も解消するための一つの方法として、外部及び内部のネットワークに複数のフィルタ機器を設置し、これら複数の機器にフィルタリングの処理を分散させるという手法がある。

[0009] このように、複数のフィルタ機器にフィルタリングの処理を分散させることにより、各フィルタ機器にかかる負荷を軽減すると共に、内部ネットワークでの不正アクセス問題も解消することが可能となる。

[0010] かかる負荷の分散のための技術の一例が、特許文献1に記載されている。特許文献1に記載の技術では、フィルタ規則を、複数のフィルタ機器に分散して設定する。また、特許文献1に記載の技術では、外部ネットワークに設置する機器と、内部ネットワークに設置する機器とで、それぞれ異なる内容のフィルタ規則を設定する。

[0011] 具体的には、通過するトラフィック量が多いことから監視対象とするパケット数が多い外部ネットワークのフィルタ機器には、負荷が軽いフィルタ規則を設定する。例えば、規則の数が比較的少数、且つ更新頻度も低いフィルタ規則を設定する。

[0012] 一方で、通過するトラフィック量が少ないことから監視対象とするパケット数が少ない内部ネットワークの機器には、負荷が重いフィルタ規則を設定

する。例えば、規則数が増加しがちなサブネット毎のフィルタ規則や、更新頻度の大きいフィルタ規則は負荷が重いので、これらのフィルタ規則を内部ネットワークのフィルタ機器に設定する。なお、このようなフィルタ規則の設定に関する情報の管理やフィルタ規則の設定は、専用のフィルタ管理サーバが管理する。

- [0013] 特許文献1に記載の技術では、このように、フィルタ管理サーバが、各フィルタ機器が監視対象とするパケット数を考慮した上でフィルタ規則を分散させることにより、各フィルタ機器にかかる負荷を分散させ、結果として、負荷の増加に対するスケーラビリティを確保する。

先行技術文献

特許文献

- [0014] 特許文献1：特開2003-244247号公報

非特許文献

- [0015] 非特許文献1：土井 洋、“秘密分散法とその応用について”、[online]、平成24年11月、情報セキュリティ総合科学 第4巻、[平成27年6月30日検索]、インターネット<URL：www.iisec.ac.jp/proc/vol0004/doi.pdf>

非特許文献2：岩本 貢、“秘密分散法Secret Sharing Schemes”、[online]、[平成27年6月30日検索]、インターネット<URL：http://ohta-lab.jp/users/mitsugu/research/SSS/main.html>

発明の概要

発明が解決しようとする課題

- [0016] 上述したような、特許文献1等に記載の技術を用いることにより、各フィルタ機器にかかる負荷を分散することができる。
- [0017] しかしながら、負荷分散を行なうことによって各フィルタ機器にかかる負荷を軽減できたとしても、各フィルタ機器が処理できる能力に上限があることには変わりがない。そのため、負荷分散を行ったとしても、各フィルタ機

器が耐えられる以上の負荷をかけるようなD o s 攻撃等があったとしたならば、各フィルタ機器の機能は停止し、各フィルタ機器はそれ以降サービス不能に陥り、通信不可となるという問題が生じる。

[0018] また、特許文献1等に記載の技術では、通信不可となったフィルタ機器に設定されていたフィルタ規則を、他の代替となるフィルタ機器に設定するような仕組みは用意されていない。そのため、以後は、かかるフィルタ規則によりフィルタリングすべきであった攻撃パケットを、ネットワーク内部に通過させてしまう状態になるという問題も生じる。

[0019] 他方で、フィルタ管理サーバに関連する問題も生じる。保守管理において、フィルタ規則を一度設定した後も、フィルタ規則を頻繁に変更するような場合がある。一方で、フィルタをそれほど頻繁に変更しないような場合もある。

[0020] このように、フィルタ規則の管理方法は様々ではあるが、何れの管理方法を用いる場合であっても専用のフィルタ管理サーバを設置し、フィルタ管理サーバにてフィルタ規則を一括で管理する必要がある。

[0021] しかし、この場合にフィルタ管理サーバ自体に直結で不正なアクセスが行われてしまうと、フィルタ管理サーバから全てのフィルタ規則が盗まれたり、フィルタ管理サーバが故障させられたりする。そして、これによりネットワーク全体においてフィルタリング機能がサービス不能となるという問題が生じる。

[0022] そこで本発明は、フィルタリングを行なうフィルタ機器等に問題が生じたとしても、フィルタ規則の全てが流出したり、ネットワーク全体のフィルタ機能が停止したりすることを防止することが可能な、フィルタリングシステム、管理装置、フィルタリング方法及び管理プログラムを提供することを目的とする。

課題を解決するための手段

[0023] 本発明の第1の観点によれば、フィルタ規則に基づいて通信データのフィルタリングを行なう複数の機器と、前記フィルタ規則を管理する管理装置と

、を備えるフィルタリングシステムであって、外部ネットワークに他の前記機器を介することなく接続している第1の前記機器が所定の状態になった場合に、前記管理装置が、前記第1の機器を介して外部ネットワークに接続している複数の第2の前記機器から受信した複数の分散フィルタ規則に基づいて前記第1の機器に設定されている分散フィルタ規則を復元し、該復元した分散フィルタ規則を前記複数の第2の機器に設定し、前記分散フィルタ規則は、全ての分散フィルタ規則を用いることなく前記フィルタ規則を復元可能に分散されていることを特徴とするフィルタリングシステムが提供される。

[0024] 本発明の第2の観点によれば、フィルタ規則に基づいて通信データのフィルタリングを行なう複数の機器と通信可能に接続され、前記フィルタ規則を管理する管理装置であって、外部ネットワークに他の前記機器を介することなく接続している第1の前記機器が所定の状態になった場合に、前記第1の機器を介して外部ネットワークに接続している複数の第2の前記機器から受信した複数の分散フィルタ規則に基づいて前記第1の機器に設定されている分散フィルタ規則を復元し、該復元した分散フィルタ規則を前記複数の第2の機器に設定すると共に、前記分散フィルタ規則は、全ての分散フィルタ規則を用いることなく前記フィルタ規則を復元可能に分散されていることを特徴とする管理装置が提供される。

[0025] 本発明の第3の観点によれば、フィルタ規則に基づいて通信データのフィルタリングを行なう複数の機器と、前記フィルタ規則を管理する管理装置と、を備えるシステムが行なうフィルタリング方法であって、外部ネットワークに他の前記機器を介することなく接続している第1の前記機器が所定の状態になった場合に、前記管理装置が、前記第1の機器を介して外部ネットワークに接続している複数の第2の前記機器から受信した複数の分散フィルタ規則に基づいて前記第1の機器に設定されている分散フィルタ規則を復元し、該復元した分散フィルタ規則を前記複数の第2の機器に設定し、前記分散フィルタ規則は、全ての分散フィルタ規則を用いることなく前記フィルタ規則を復元可能に分散されていることを特徴とするフィルタリング方法が提供

される。

[0026] 本発明の第4の観点によれば、フィルタ規則に基づいて通信データのフィルタリングを行なう複数の機器と通信可能に接続され、前記フィルタ規則を管理する管理装置としてコンピュータを機能させるための管理プログラムであって、外部ネットワークに他の前記機器を介することなく接続している第1の前記機器が所定の状態になった場合に、前記第1の機器を介して外部ネットワークに接続している複数の第2の前記機器から受信した複数の分散フィルタ規則に基づいて前記第1の機器に設定されている分散フィルタ規則を復元し、該復元した分散フィルタ規則を前記複数の第2の機器に設定すると共に、前記分散フィルタ規則は、全ての分散フィルタ規則を用いることなく前記フィルタ規則を復元可能に分散されている管理装置として前記コンピュータを機能させることを特徴とする管理プログラムが提供される。

発明の効果

[0027] 本発明によれば、フィルタリングを行なうフィルタ機器等に問題が生じたとしても、フィルタ規則の全てが流出したり、ネットワーク全体のフィルタ機能が停止したりすることを防止することが可能となる。

図面の簡単な説明

[0028] [図1]本発明の実施形態全体の基本的構成を表すブロック図である。

[図2]本発明の実施形態におけるフィルタ管理サーバの基本的構成を表すブロック図である。

[図3]本発明の実施形態全体の基本的動作を表すシーケンス図である。

[図4-1]本発明の実施形態が、外部からの攻撃を受けた際の各機器の状態変化を表すイメージ図（1／2）である。

[図4-2]本発明の実施形態が、外部からの攻撃を受けた際の各機器の状態変化を表すイメージ図（2／2）である。

[図5]本発明の実施形態の第1の変形例の基本的構成を表すブロック図である。

[図6]本発明の実施形態の第2の変形例における、分散情報の組み合わせパタ

ーンについて表すイメージ図である。

[図7]本発明の実施形態の第3の変形例における、フィルタ規則の設定について表すイメージ図である。

発明を実施するための形態

[0029] まず、本発明の実施形態の概略を説明する。本実施形態では、フィルタ規則を分散管理することによってセキュリティの向上を図る。

[0030] そのために、本実施形態では、ネットワーク内の或るフィルタ機器が攻撃を受けた場合に、かかる攻撃対象となっているフィルタ機器がサービス不能となり、通信を遮断する状態が発生する前に、そのフィルタ機器のフィルタ規則の一部もしくは全てを他のフィルタ機器に移譲する。

[0031] 具体的には、システム全体に適用すべきフィルタ規則を、フィルタ管理サーバが「秘密分散法」を用いて分散する。そして、分散後のフィルタ規則を、複数のフィルタ機器のそれぞれに分散して記憶させ、フィルタ管理サーバにはファイル規則を残さないようにする。

[0032] その後、何れかのフィルタ機器が攻撃を受けて、かかるフィルタ機器のフィルタリング機能がダウンするおそれがある場合には、他のフィルタ機器に記憶されているフィルタ規則がフィルタ管理サーバに集められる。そして、フィルタ管理サーバが「秘密分散法」に従い、集められたフィルタ規則から分散前の元々のフィルタ規則を復元する。なお、秘密分散法とは、分散した情報の内の一部の情報に基づいて分散前の全ての情報を復元するための方法である。秘密分散法の具体的な内容については後述する。

[0033] そして、ファイル管理サーバは、他のフィルタ機器に記憶されていたフィルタ規則との差分として、失われたフィルタ規則（攻撃を受けたフィルタ機器が受け持っていたフィルタ規則）を抽出する。

[0034] また、ファイル管理サーバは、抽出された、失われたフィルタ規則を、フィルタリング機能がダウンしてしまったフィルタ機器の内側に位置する、他のフィルタ機器に設定する。これにより、システム全体で、フィルタリング機能を自動的に復旧させる。

- [0035] 以上のようにすることによって、一部のフィルタ機器が攻撃を受けて、フィルタリング機能がダウンしてしまった場合でも、他のフィルタ機器が、失われたフィルタ規則を、代替して実行する体制が自動的に構築される。そのため、より強固なフィルタリングシステムを実現することが可能となる。
- [0036] また、一つのフィルタ機器がサービス不能になるほどに集中していた攻撃の負荷を、複数のフィルタ機器に分散し、ネットワークの深くまで不正なパケットを到達させることを防ぐことができる。
- [0037] 結果として、本実施形態ではフィルタ管理サーバのフィルタ規則の情報を分散管理させることにより、ネットワークのセキュリティを向上させることが可能となる。
- [0038] 以上が本発明の実施形態の概略である。
- [0039] 次に、本発明の実施形態について図面を参照して詳細に説明する。
- [0040] 図1を参照すると、本実施形態であるフィルタ管理システム100は、外部フィルタ機器11、外部フィルタ機器12、内部フィルタ機器21、内部フィルタ機器22、内部フィルタ機器23、内部フィルタ機器24、フィルタ管理サーバ30、外部ネットワーク40、サブネット51、サブネット52、サブネット53及びサブネット54を含む。
- [0041] フィルタ管理サーバ30は、各システム全体に適用すべきフィルタ規則を分散し、分散後のフィルタ規則を各フィルタ機器に記憶させるサーバ装置である。
- [0042] 各フィルタ機器（外部フィルタ機器11、外部フィルタ機器12、内部フィルタ機器21、内部フィルタ機器22、内部フィルタ機器23及び内部フィルタ機器24）は、自フィルタ機器が記憶するフィルタ規則に基づいてフィルタリングを行なう機器である。これら各フィルタ機器は、例えば会社内等に設けられるLANに設置される。
- [0043] また、各フィルタ機器の中で、外部フィルタ機器11及び外部フィルタ機器12は、外部ネットワーク40との接点に位置する。ここで、外部ネットワーク40は、例えばインターネット等のネットワークであるとする。

[0044] 一方で、内部フィルタ機器 2 1 乃至内部フィルタ機器 2 4 は、内部ネットワークである各サブネット（サブネット 5 1 乃至サブネット 5 4）との接点に位置するフィルタ機器である。ここで、各サブネットは、例えば、部署毎に設けられたネットワークであるとする。

[0045] 各サブネットには、パーソナルコンピュータやサーバ装置といった通信端末（図示を省略する）が接続されている。そして、これら通信端末は、自通信端末が接続されたサブネットに接続された他の通信端末や、他のサブネットに接続された通信端末や、外部ネットワーク 4 0 に接続された通信端末と相互にパケット通信を行なう。

[0046] フィルタ管理サーバ 3 0 は、何れかのサブネットや外部ネットワーク 4 0 又は図示を省略した他のネットワークを介して各フィルタ機器と接続される。そして、フィルタ管理サーバ 3 0 は、これらネットワークを介して各フィルタ機器と通信可能な状態にある。フィルタ管理サーバ 3 0 と各フィルタ機器の接続については、図示を省略する。

[0047] 次に、図 2 を参照して、フィルタ管理サーバ 3 0 に含まれる機能ブロックについて説明をする。

[0048] 図 2 を参照すると、フィルタ管理サーバ 3 0 は、フィルタ管理部 3 1 と通信部 3 4 を含む。また、フィルタ管理部 3 1 は、演算部 3 2 と記憶部 3 3 を含む。

[0049] フィルタ管理部 3 1 は、フィルタ管理サーバ 3 0 全体を制御すると共に、フィルタ管理システム 1 0 0 内の各フィルタ機器に設定するフィルタ規則を管理する部分である。ここで、フィルタ管理部 3 1 は、演算部 3 2 及び記憶部 3 3 により実現される。

[0050] 演算部 3 2 は、CPU（Central Processing Unit）等の演算処理装置である。また、記憶部 3 3 は、演算部 3 2 が利用する RAM（Random Access Memory）といった主記憶装置と、HDD（Hard Disk Drive）といった補助記憶装置である。記憶部 3 3 には、本実施形態特有のソフトウェアが格納されている。

- [0051] そして、演算部 32 は、記憶部 33 に格納されているかかるソフトウェアを読み込み、このソフトウェアに基づいて演算処理を行なう。そして、フィルタ管理部 31 は、かかる演算処理の結果に基づいてフィルタ管理サーバ 30 に含まれるハードウェアを制御する。つまり、フィルタ管理サーバ 30 は、ハードウェアとソフトウェアが協働することにより実現できる。
- [0052] 通信部 34 は、フィルタ管理部 31 が各フィルタ機器と通信を行なうための部分である。通信部 34 は、何れかのサブネットや外部ネットワーク 40 等を介して各フィルタ機器と通信を行なう。
- [0053] 次に、フィルタ管理サーバ 30 内のフィルタ管理部 31 が行なう、秘密分散法を用いたフィルタ規則の管理方法について説明する。
- [0054] 本実施形態では、フィルタ管理部 31 が、フィルタ管理システム 100 に適用すべきフィルタ規則を秘密情報として「秘密分散法」を用いて分散することにより、分散後のフィルタ規則を複数生成する。なお、かかる分散後のフィルタ規則は、秘密情報である分散前のフィルタ規則を分散して得られる情報である。そこで、以下の説明においては、かかる分散後のフィルタ規則を、適宜「分散情報」と呼ぶ。
- [0055] また、フィルタ管理サーバ 30 は、生成した分散情報のそれぞれを各フィルタ機器に送信し、送信後にはフィルタ管理サーバ 30 には分散情報を残さないようにする。なお、フィルタ管理サーバ 30 は、何れのフィルタ機器に何れの分散情報を送信したのかを記憶しておく。これにより、フィルタ管理サーバ 30 何れのフィルタ機器が何れの分散情報を記憶しているかを把握しているものとする。
- [0056] そして、各フィルタ機器は、自フィルタ機器が記憶する分散情報に基づいて、自フィルタ機器にフィルタ規則を設定し、設定したフィルタ規則に基づいてフィルタリングを行なう。
- [0057] ここで、本実施形態では、各フィルタ機器に設定されるフィルタ規則は、それぞれ固有のフィルタ規則である。例えば、図 1 に表わされるように、外部フィルタ機器 11 には、フィルタ規則 A が設定される。また、外部フィル

タ機器 1 1 は、フィルタ規則 A を分散情報 A として記憶する。

[0058] 一方で、外部フィルタ機器 1 2 には、フィルタ規則 B が設定される。また、フィルタ規則 B を分散情報 B として記憶する。

[0059] 次に、「秘密分散法」について説明する。上述したように、本実施形態では、フィルタ規則を秘密分散法で管理することでフィルタの効率的な負荷分散とセキュリティの向上を図る。

[0060] 秘密分散法では、秘密にしたいデータ情報を幾つか（N 個とする。）の分散情報に分けて管理する。そして、その内、幾つか必要最低の個数（K 個とする。ここで、本実施形態では、 $K < N$ の関係を満たすものとする。）の分散情報を集めると元の秘密データが復元でき、K 個未満の個数の分散情報を集めたとしても元の秘密データは復元できないというものである。かかる秘密分散法は、Shamir の（K，N）閾値法として知られている方法である。Shamir の（K，N）閾値法の詳細については、例えば、非特許文献 1 や非特許文献 2 に記載されている。

[0061] そして、本実施形態では、この Shamir の（K，N）閾値法を利用し、フィルタ規則を秘密データとして扱い、かかるフィルタ規則を分散することで得られる分散後の複数のフィルタ規則の各々を分散情報として分散管理する。また、負荷が増大しているフィルタ機器に適用されているフィルタ規則を、残りの機器が記憶している分散情報で復元する。そして、復元した分散情報を利用して、残りの機器が、負荷が増大しているフィルタ機器の代わりを請け負うことで、ネットワーク内のセキュリティの著しい低下を防ぐ。

[0062] また、このようにすれば、フィルタ規則を移譲して、フィルタ機能を停止したフィルタ機器が不正アクセスによって占拠されたとしても、その機器から得られるのは、そのフィルタ機器が記憶している一つの分散情報のみとなる。よって、他の機器が持つフィルタ規則が漏洩することを防止できる。同様の理由で、フィルタ規則はフィルタ管理サーバ 3 0 が一括で記憶するのではなく、各フィルタ機器で分散して記憶されているため、仮にフィルタ管理サーバ 3 0 に直接アクセスされてしまったとしても、全てのフィルタ規則の

情報が漏洩することを防止することができる。

[0063] 次に、図3のシーケンス図と、図4-1及び図4-2の情報の送受信を表す図を参照して、本実施形態の動作について説明する。なお、以下の説明では、一例として外部フィルタ機器11がD o s 攻撃等の攻撃対象となる場合を想定する。

[0064] まず、D o s 攻撃等に起因して外部ネットワーク40を介して外部フィルタ機器11に対して大量のパケットが送信される。これにより、外部フィルタ機器11の負荷が増大する（図4-1の「(1) 負荷」）。

[0065] ここで、本実施形態における各フィルタ機器は、自身にかかる負荷を常に監視している。そして、外部フィルタ機器11は、外部フィルタ機器11に対する攻撃に伴って外部フィルタ機器11自身にかかる負荷が一定以上になったことを検知すると（図3のステップS101）、その旨を他のフィルタ機器全て、若しくは一部に通知する（図3のステップS103、図4-1の「(2-1) 通知、(2-2) 通知及び(2-3) 通知」）。

[0066] なお、一部のフィルタ機器に通知をすれば良いのであるが、少なくとも秘密分散法として（K，N）閾値法におけるK個のフィルタ機器に対して通知する必要がある。本説明では、秘密分散法として（3，6）閾値法を用いるものとする。これは、6つ（N個）ある分散情報のうち、少なくとも3つ（K個）があれば元の情報が復元できるというものである。つまり、本説明では、K=3であるので、外部フィルタ機器11は、少なくとも3台のフィルタ機器に対して通知を行なう必要がある。本例では、外部フィルタ機器11よりもサブネット側に近い位置に位置する内部フィルタ機器21、内部フィルタ機器22及び内部フィルタ機器23の3台のフィルタ機器に対して通知を行なう。

[0067] 外部フィルタ機器11からの負荷増大の通知を受け付けた、内部フィルタ機器21、内部フィルタ機器22及び内部フィルタ機器23の3台のフィルタ機器は、自身が保有している分散情報を、フィルタ管理サーバ30に送信する（図3のステップS105、図4-1の「(3-1) 分散情報C、(3-

2) 分散情報D及び(3-3)分散情報E)。

[0068] 各フィルタ機器それぞれから、合計K個以上の分散情報を受信したフィルタ管理サーバ30は、秘密分散法を用いて、受信したK個の分散情報から秘密情報であるフィルタ規則の復元をする(図3のステップS107、図4-1の(4)フィルタ規則復元)。本説明では、分散情報C、分散情報D及び分散情報Eの3個の分散情報から、秘密情報であるフィルタ規則の復元処理をする。かかる復元処理により、フィルタ規則Aを含んだ全てのフィルタ規則は復元される。

[0069] ここで、フィルタ管理サーバ30は、ステップS103にて外部フィルタ機器11の負荷が増大している旨を外部フィルタ機器11から受信しているか、もしくは、ステップS105にて負荷が増大しているフィルタ機器が外部フィルタ機器11である旨を内部フィルタ機器21、内部フィルタ機器22及び内部フィルタ機器23から受信しているものとする。そして、これにより、フィルタ管理サーバ30は、攻撃対象となっているフィルタ機器が、外部フィルタ機器11であることを把握しているものとする。

[0070] そこで、フィルタ管理サーバ30は、外部フィルタ機器11に対応するフィルタ規則であるフィルタ規則Aを、分散情報の提供を行った内部フィルタ機器21、内部フィルタ機器22及び内部フィルタ機器23の3台のフィルタ機器に対して送信する(図3のステップS109、図4-2の(51)フィルタ規則A、(52)フィルタ規則A及び(53)フィルタ規則A)。

[0071] ここで、フィルタ管理サーバ30が復元したフィルタ規則を保持していると、その後フィルタ管理サーバ30が不正アクセスされたような場合に、フィルタ規則が漏洩してしまうおそれがある。そこで、フィルタ管理サーバ30は、ステップS109における送信を実行すると、フィルタ管理サーバ30自身が復元したフィルタ規則をフィルタ管理サーバ30から削除する。

[0072] これにより、フィルタ管理サーバ30からフィルタ規則が漏洩することを防止することができる。なお、かかる状態を表すため、図4-2ではフィルタ管理サーバ30が記憶する分散情報は「無し」と表記している。

- [0073] フィルタ規則Aを受信した、内部フィルタ機器21、内部フィルタ機器22及び内部フィルタ機器23の3台のフィルタ機器は現在自身に設定されているフィルタ規則に加えて、受信したフィルタ規則Aを新たに自身に設定する（図3のステップS111）。
- [0074] また、内部フィルタ機器21、内部フィルタ機器22及び内部フィルタ機器23の3台のフィルタ機器は受信したフィルタ規則Aを自身が記憶する分散情報に追加する。
- [0075] これにより、図4-2に表わされるように内部フィルタ機器21には、フィルタ規則C及びフィルタ規則Aが設定されると共に、フィルタ規則C及びフィルタ規則Aが分散情報として記憶される。また、同様に、内部フィルタ機器22には、フィルタ規則D及びフィルタ規則Aが設定されると共に、フィルタ規則D及びフィルタ規則Aが分散情報として記憶される。更に、同様に、内部フィルタ機器23には、フィルタ規則E及びフィルタ規則Aが設定されると共に、フィルタ規則E及びフィルタ規則Aが分散情報として記憶される。
- [0076] そして、内部フィルタ機器21、内部フィルタ機器22及び内部フィルタ機器23は、自フィルタ機器に設定したフィルタ規則に基づいたフィルタリングを継続する。
- [0077] また、内部フィルタ機器21、内部フィルタ機器22及び内部フィルタ機器23の3台のフィルタ機器は、自身にフィルタ規則Aを新たに追加すると、自身にフィルタ規則Aを新たに追加した旨を外部フィルタ機器11に対して通知する（図3のステップS113、図4-2の（6-1）通知、（6-2）通知及び（6-3）通知）。
- [0078] ステップS103において通知を行った全てのフィルタ機器から、ステップS113の通知を受け取った外部フィルタ機器11は、自身のフィルタリング機能が無効にする（図3のステップS115、図4-2（7）フィルタ無効）。
- [0079] なお、外部フィルタ機器11は、フィルタ規則Aを分散情報として記憶し

ていても良いが、攻撃元により外部フィルタ機器 11 に対する不正なアクセスがなされて、攻撃元に分散情報が取得されてしまうおそれがある。そこで、ステップ S 115 において外部フィルタ機器 11 が、自身が記憶する分散情報を削除するようにしても良い。なお、かかる状態を表すため、図 4-2 では外部フィルタ機器 11 が記憶する分散情報及び外部フィルタ機器 11 に設定されるフィルタ規則は「無し」と表記している。

[0080] これ以降は、外部フィルタ機器 11 でフィルタリングされることなく通過してきたパケットを、内部フィルタ機器 21、内部フィルタ機器 22 及び内部フィルタ機器 23 の 3 台のフィルタ機器にてフィルタリングすることが可能となる。

[0081] 以上説明した本発明の実施形態は、以下に示すような多くの効果を奏する。

[0082] 第 1 の効果は、通信の遮断によるサービス不能状態を回避できることである。

[0083] その理由は、フィルタリング処理の処理量の増加がフィルタ機器の負荷増大の主な要因の場合に、そのフィルタリングの機能を他のフィルタ機器に分散することができるからである。

[0084] 第 2 の効果は、内部ネットワークのセキュリティが著しく低下することがないことである。

[0085] その理由は、フィルタ機能を無効にした機器はセキュリティが低下するが、その機器の持つフィルタ規則は残りの機器に引き継がれているからである。

[0086] 第 3 の効果は、攻撃を受けたフィルタ機器から分散情報を取得されたとしても、ネットワーク全体のフィルタ規則は漏洩しないことである。

[0087] その理由は、秘密分散法として (K, N) 閾値法を用いており、仮に一部のフィルタ規則が漏洩したとしても、K 個の分散情報が取得されない限りは、ネットワーク全体のフィルタ規則を復元することはできないからである。

[0088] 第 4 の効果は、フィルタ管理サーバ自体に障害が発生してもネットワーク

全体のフィルタ規則は漏洩しないことである。

[0089] その理由は、フィルタ管理サーバ自体にはフィルタ規則の情報は常時保持されておらず、攻撃などにより何れかのフィルタ機器が負荷増大を検知したときのみ各フィルタ機器からフィルタ管理サーバに対して分散情報が送られてフィルタ規則の復元を行うからである。

[0090] 第5の効果は、攻撃対象となったフィルタ機器が動作不能な状態となってしまうことを防止することができることである。

[0091] その理由は、ステップS 1 1 5において攻撃対象のフィルタ機器のフィルタリング機能を停止するからである。これにより、攻撃対象のフィルタ機器はフィルタリングに伴う処理を行なう必要がなくなることから、攻撃対象のフィルタ機器に対する負荷が軽減する。そのため、攻撃対象のフィルタ機器が動作不能な状態となってしまうことを防止することができる。また、これにより攻撃対象のフィルタ機器のCPU等はフィルタリングに伴う処理以外の処理を継続して行なうことが可能となる。例えば、攻撃対象のフィルタ機器がルータなのであれば、フィルタリングに伴う処理を行わないかわりに、ルーティングに関する処理を継続して行なうことが可能となる。

[0092] また、上述した実施形態は、本発明の好適な実施形態ではあるが、上記実施形態のみに本発明の範囲を限定するものではなく、本発明の要旨を逸脱しない範囲において種々の変更を施した形態での実施が可能である。

[0093] その一例として、以下に秘密分散法の特性を活かした三つの変形例を表す。なお、以下の各変形例は、基本的な構成及び動作において、上述した実施形態と同じである。そこで、説明の重複を防ぐため、以下では、各変形例特有の構成及び動作について説明し、上述の実施形態と共通する部分については説明を省略する。

[0094] <第1の変形例>

まず、図5を参照して、第1の変形例について説明する。図5に表すように、本変形例では、フィルタ管理サーバ30にも分散情報を記憶させることとする。

- [0095] ここで、上述した実施形態では、ステップS 109において、フィルタ管理サーバ30から各フィルタ機器に対して、分散情報を送信した後に、フィルタ管理サーバ30からは復元したフィルタ規則を全て削除していた。つまり、フィルタ管理サーバ30にはフィルタ規則を記憶させないようにしていた。これに対して、本変形例においても、フィルタ管理サーバ30に全てのフィルタ規則は記憶させないが、各フィルタ機器と同様に分散情報は記憶させるようにする。
- [0096] 具体的には、本変形例では、フィルタ管理サーバ30が、フィルタ管理システム100に適用すべきフィルタ規則を秘密情報として「秘密分散法」を用いて分散することにより、分散情報A乃至Gを生成する。
- [0097] そして、フィルタ管理サーバ30は、各フィルタ機器に分散情報A乃至Fをそれぞれ記憶させる。また、フィルタ管理サーバ30自身は、分散情報Gを記憶する。
- [0098] これにより、フィルタ管理サーバ30も分散情報の配布対象とでき、分散情報の配布の組み合わせに幅をもたせることが可能となる。
- [0099] この点について具体例を用いて説明する。秘密分散法として（3，7）閾値法を用いた場合に、外部フィルタ機器11に加えて、内部フィルタ機器23に対して攻撃があった場合を想定する。この場合に、本実施例では、内部フィルタ機器23から分散情報を取得できないが、内部フィルタ機器21、内部フィルタ機器22及びフィルタ管理サーバ30が記憶する分散情報に基づいてフィルタ規則を復元するようなことが可能となる。
- [0100] なお、本変形例のようにする代わりに、秘密分散法として（2，6）閾値法を用いることにしても、外部フィルタ機器11に加えて、内部フィルタ機器23に対して攻撃があった場合でも、内部フィルタ機器21及び内部フィルタ機器22が記憶する分散情報に基づいてフィルタ規則を復元するようなことができる。しかしながら、このように秘密分散法として（2，6）閾値法を用いることとすると、攻撃者に外部フィルタ機器11及び内部フィルタ機器21から分散情報を取得されてしまった場合には、攻撃者側においても

、フィルタ規則を復元することが可能となってしまうので問題となる。しかし、本変形のようにすれば、このような問題が発生することを防止することが可能となる。

[0101] <第2の変形例>

次に、第2の変形例について説明する。上述の実施形態では、各分散情報に重み付けをするようなことはせず、常に均等配分でフィルタ規則を分散することにより分散情報を生成した。これに対し、本実施例では、それぞれの分散情報に重みを付けてフィルタ規則を分散する。

[0102] 上述の実施形態の説明では、各分散情報の末尾に識別子としてアルファベットを付すことにより、各分散情報を識別して説明した。これに対して、本変形例では、各分散情報を「分散情報XY」として説明する。ここで、Xはアルファベット、Yは数字である。例えば、各分散情報を「分散情報A1」や、「分散情報C2」のように表記して説明する。

[0103] ここで、アルファベットXは上述の実施形態同様に各分散情報を識別するための識別子である。また、数字Yは分散情報の重みを表す。

[0104] ここで言う重みとはC2、D2、E2及びG2は、A1の二倍の情報量を持ち、F3はA1の三倍の情報量を持つ、というように数字の分、情報量が多いことを表す。

[0105] このとき、フィルタ管理サーバ30がフィルタ規則を復元するのに必要な分散情報の数量は、復元に用いる分散情報の重みにより決定される。例えば復元秘密分散法として(5, 7)閾値法を用いるのであれば、重みが1である分散情報、つまり分散情報X1であれば5個分($1 \times 5 \geq 5$)の分散情報がフィルタ規則の復元のために必要となる。また、重みが2である分散情報、つまり分散情報X2であれば3個分($2 \times 3 \geq 5$)の分散情報が必要となる。更に、重みが3である分散情報、つまり分散情報X3であれば2個分($3 \times 2 \geq 5$)の分散情報が必要となる。また、異なる重みの分散情報を利用してフィルタ規則を復元することもできる。

[0106] このように、分散情報の持つ情報量によって、秘密復元に最低限必要な集

めるべき情報の個数が異なってくる。

[0107] この点について図6を参照して説明する。なお、図6の例では、フィルタ管理サーバ30にも分散情報を記憶させている。つまり、図6の例は第1の変形例と第2の変形例を組み合わせた場合の例である。なお、第2の変形例を、必ずしも第1の変形例と組み合わせる必要はない。

[0108] 図6のように、各フィルタ機器及びフィルタ管理サーバ30に分散情報を記憶させるとする。その上で、秘密分散法として(5, 7)閾値法を用いるとする。

[0109] すると、例えば外部フィルタ機器11又は外部フィルタ機器12が外部からの攻撃を受けた場合に、フィルタ規則を復元するために必要となる分散情報の組み合わせは、例えば2つが考えられる。

[0110] 具体的には、例えば、分散情報C2、分散情報D2及び分散情報G2の三つを合わせた重み6つ分の情報量で復元することが第1のパターンとして考えられる(図6、(8-1)分散情報C2及び(8-2)分散情報D2)。

[0111] また、他にも第2のパターンとして、分散情報F3と分散情報G2の二つを合わせた重み5つ分の情報量で復元することが第2のパターンとして考えられる(図6、(8-3)分散情報F3)。

[0112] 本変形例のようにすることにより、フィルタ規則の配置の自由度を高めることができる。例えば、フィルタ管理サーバ30や内部フィルタ機器が、外部フィルタ機器よりも攻撃を受ける可能性が低いのであれば、これらフィルタ管理サーバ30や内部フィルタ機器が、情報量が多い分散情報を記憶するようにすると良い。

[0113] このようにすれば、これらフィルタ管理サーバ30や内部フィルタ機器が、少数でも通常に動作していれば分散情報を復元できるからである。また、外部フィルタ機器が攻撃されて分散情報の一部が漏洩してしまったとしても、かかる漏洩する分散情報の情報量は少ないため、フィルタ規則に関する情報の漏洩する量を少なくおさえることができるからである。

[0114] <第3の変形例>

次に、第3の変形例について説明する。本実施例では、或るフィルタ機器が攻撃を受けた場合に、かかる或るフィルタ機器に設定されていたフィルタ規則を複数のフィルタ規則に分ける。そして、分けた複数のフィルタ規則をそれぞれ異なるフィルタ機器に追加で設定する。

[0115] この点について、図7を参照して説明する。なお、図7の例では、外部フィルタ機器11が攻撃を受けていると想定する。また、図7の例では、フィルタ管理サーバ30にも分散情報を記憶させている。また、各分散情報に重み付けを行っている。つまり、図7の例は第1の変形例と第2の変形例を第3の変形例と組み合わせた場合の例である。なお、第3の変形例を、必ずしも第1の変形例や第2の変形例と組み合わせる必要はない。

[0116] 上述の実施形態の説明において述べたように、外部フィルタ機器11が攻撃を受けると、内部フィルタ機器21、内部フィルタ機器22及び内部フィルタ機器23等は自フィルタ機器が記憶している分散情報をフィルタ管理サーバ30に対して送信する。

[0117] そして、フィルタ管理サーバ30はこれら分散情報に基づいてフィルタ規則を復元する。そして、復元したフィルタ規則から、外部フィルタ機器11に対応するフィルタ規則であるフィルタ規則Aを抽出する。

[0118] そして、抽出したフィルタ規則Aを内部フィルタ機器22や内部フィルタ機器23に対して送信する（図7、（10-1）フィルタ規則A及び（10-2）フィルタ規則A）。内部フィルタ機器22や内部フィルタ機器23はかかるフィルタ規則Aを自フィルタ機器に設定する。ここまでは、上述の実施形態と同様の動作である。

[0119] 一方で、本変形例では、フィルタ規則Aを、フィルタ規則Aaと、フィルタ規則Abに分け、内部フィルタ機器21と、かかる内部フィルタ機器21の内側に位置する内部フィルタ機器24にこれらを送信する。

[0120] 具体的には、フィルタ規則Aaを内部フィルタ機器21に送信する（図7、フィルタ規則Aa）。また、フィルタ規則Abを内部フィルタ機器24に送信する（図7、フィルタ規則Ab）。

- [0121] 内部フィルタ機器 2 1 及び内部フィルタ機器 2 4 は、受信したフィルタ規則を自フィルタ機器に追加で設定する。また、内部フィルタ機器 2 1 及び内部フィルタ機器 2 4 は、受信したフィルタ規則を分散情報として追加で記憶する。ここで、図中に表わされるように、本例では分散情報 A の情報量は 1 である。そして、分散情報 A を分けたものが、分散情報 A a と、分散情報 A b に相当するので、これらの情報量は 0.5 となる。そのため、図中では、分散情報 A 1、分散情報 A a 0.5 及び分散情報 A b 0.5 と表記する。
- [0122] 以上説明した、本実施例では、攻撃を受けたフィルタ機器のフィルタ規則を、一つのフィルタ機器に丸ごと追加する必要はなく、同じネットワーク内にフィルタ機器があれば、分散して処理分けの配置を行うことができる。
- [0123] そのため、例えば、特許文献 1 に記載の技術のように、任意のフィルタ機器に情報量の多いフィルタ規則を適用させ、他のフィルタ機器には情報量の少ないフィルタ規則を適用させたいような要望がある場合に本実施例は好適となる。その理由は、本実施例であれば情報量の多いフィルタ規則が適用されているフィルタ機器が攻撃を受けた場合に、かかる情報量が多いフィルタ規則を分けることにより、情報量の少ないフィルタ規則とし、かかる情報量の少ないフィルタ規則を、他のフィルタ機器に適用することができるからである。
- [0124] なお、上述の各実施形態及び変形例では、分散情報の数と、フィルタ機器の数は 1 対 1 の関係であった。これを変形して、1 対多の関係としても良い。例えば、フィルタ規則を 5 つの分散情報に分散する。そして、外部フィルタ機器 1 1 と外部フィルタ機器 1 2 に同じ分散情報を送信する。これにより、外部フィルタ機器 1 1 と外部フィルタ機器 1 2 には同様のフィルタ規則が適用される。そして、残り 4 つの分散情報を、内部フィルタ機器 2 1 乃至内部フィルタ機器 2 4 に送信する。このようにすることにより、仮に外部フィルタ機器 1 1 及び外部フィルタ機器 1 2 の双方が攻撃を受けて、双方から分散情報が漏洩したとしても、漏洩する分散情報の数を 1 つに抑えることが可能となる。

- [0125] また、上述の各実施形態及び変形例では、分散情報の提供を行ったフィルタ機器に対して、攻撃を受けているフィルタ機器に対応するフィルタ規則を送信していた。しかし、攻撃を受けているフィルタ機器よりも内側に、分散情報の提供を行ったフィルタ機器以外のフィルタ機器が存在する場合には、かかるフィルタ機器にも攻撃を受けているフィルタ機器に対応するフィルタ規則を送信するようにすると良い。そして、かかるフィルタ機器に送信したフィルタ規則を設定させるようにすると良い。
- [0126] なお、上記のフィルタ管理システムに含まれるフィルタ管理サーバ及びフィルタ機器のそれぞれは、それぞれが、ハードウェア、ソフトウェア又はこれらの組み合わせにより実現することができる。また、上記のフィルタ管理システムに含まれるフィルタ管理サーバ及びフィルタ機器により行なわれるフィルタ管理方法も、ハードウェア、ソフトウェア又はこれらの組み合わせにより実現することができる。ここで、ソフトウェアによって実現されるとは、コンピュータがプログラムを読み込んで実行することにより実現されることを意味する。
- [0127] プログラムは、様々なタイプの非一時的なコンピュータ可読媒体(non-transitory computer readable medium)を用いて格納され、コンピュータに供給することができる。非一時的なコンピュータ可読媒体は、様々なタイプの実体のある記録媒体(tangible storage medium)を含む。非一時的なコンピュータ可読媒体の例は、磁気記録媒体（例えば、フレキシブルディスク、磁気テープ、ハードディスクドライブ）、光磁気記録媒体（例えば、光磁気ディスク）、CD-ROM(Read Only Memory)、CD-R、CD-R/W、半導体メモリ（例えば、マスクROM、PROM(Programmable ROM)、EPROM(Erasable PROM)、フラッシュROM、RAM(random access memory)）を含む。
- [0128] 上記の実施形態の一部又は全部は、以下の付記のようにも記載されうるが、以下には限られない。
- [0129] （付記１） フィルタ規則に基づいて通信データのフィルタリングを行な

う複数の機器と、前記フィルタ規則を管理する管理装置と、を備えるフィルタリングシステムであって、

外部ネットワークに他の前記機器を介することなく接続している第１の前記機器が所定の状態になった場合に、前記管理装置が、前記第１の機器を介して外部ネットワークに接続している複数の第２の前記機器から受信した複数の分散フィルタ規則に基づいて前記第１の機器に設定されている分散フィルタ規則を復元し、該復元した分散フィルタ規則を前記複数の第２の機器に設定し、

前記分散フィルタ規則は、全ての分散フィルタ規則を用いることなく前記フィルタ規則を復元可能に分散されていることを特徴とするフィルタリングシステム。

[0130] (付記２) 前記第１の機器は、自機器が前記所定の状態になった場合に複数の前記第２の機器に対して通知を行い、

前記通知を受けた複数の第２の機器のそれぞれが、前記分散フィルタ規則を前記管理装置に送信し、

前記管理装置は、前記複数の第２の機器のそれぞれから受信した分散フィルタ規則に基づいて前記復元を行なうことを特徴とする付記１に記載のフィルタリングシステム。

[0131] (付記３) 前記第１の機器は、前記通信データのフィルタリングの実行に起因して、自機器が所定の状態となった場合に前記通知を行なうことを特徴とする付記２に記載のフィルタリングシステム。

[0132] (付記４) 前記第１の機器は、前記自機器が前記所定の状態になった場合に前記フィルタリングの実行を中止するが、前記外部ネットワークと前記第２の機器間での通信データの送受信の中継は継続することを特徴とする付記１乃至３の何れか１に記載のフィルタリングシステム。

[0133] (付記５) 前記管理装置は、前記分散フィルタ規則を各機器に設定したならば、分散前のフィルタ規則及び分散フィルタ規則を自管理装置から削除することを特徴とする付記１乃至４の何れか１に記載のフィルタリングシス

テム。

[0134] (付記 6) 前記管理装置は、前記第 1 の機器に設定する分散フィルタ規則と、前記第 2 の機器に設定する分散フィルタ規則とを異ならせることを特徴とする付記 1 乃至 5 の何れか 1 に記載のフィルタリングシステム。

[0135] (付記 7) 前記第 2 の機器は、前記第 1 の機器に対応する分散フィルタ規則を設定された場合には、自機器に設定されていた自機器に対応する分散フィルタ規則と、前記第 1 の機器に対応する分散フィルタ規則との双方のフィルタ規則に基づいて前記フィルタリングを実行することを特徴とする付記 1 乃至 6 の何れか 1 に記載のフィルタリングシステム。

[0136] (付記 8) 前記管理装置は、前記複数の第 2 の機器のそれぞれから受信した分散フィルタ規則に基づいて分散前のフィルタ規則を復元し、復元後のフィルタ規則を再度分散することにより前記第 1 の機器に対応する分散フィルタ規則を復元することを特徴とする付記 1 乃至 7 の何れか 1 に記載のフィルタリングシステム。

[0137] (付記 9) フィルタ規則に基づいて通信データのフィルタリングを行なう複数の機器と通信可能に接続され、前記フィルタ規則を管理する管理装置であって、

外部ネットワークに他の前記機器を介することなく接続している第 1 の前記機器が所定の状態になった場合に、前記第 1 の機器を介して外部ネットワークに接続している複数の第 2 の前記機器から受信した複数の分散フィルタ規則に基づいて前記第 1 の機器に設定されている分散フィルタ規則を復元し、該復元した分散フィルタ規則を前記複数の第 2 の機器に設定すると共に、

前記分散フィルタ規則は、全ての分散フィルタ規則を用いることなく前記フィルタ規則を復元可能に分散されていることを特徴とする管理装置。

[0138] (付記 10) フィルタ規則に基づいて通信データのフィルタリングを行なう複数の機器と、前記フィルタ規則を管理する管理装置と、を備えるシステムが行なうフィルタリング方法であって、

外部ネットワークに他の前記機器を介することなく接続している第 1 の前

記機器が所定の状態になった場合に、前記管理装置が、前記第 1 の機器を介して外部ネットワークに接続している複数の第 2 の前記機器から受信した複数の分散フィルタ規則に基づいて前記第 1 の機器に設定されている分散フィルタ規則を復元し、該復元した分散フィルタ規則を前記複数の第 2 の機器に設定し、

前記分散フィルタ規則は、全ての分散フィルタ規則を用いることなく前記フィルタ規則を復元可能に分散されていることを特徴とするフィルタリング方法。

[0139] (付記 1 1) フィルタ規則に基づいて通信データのフィルタリングを行なう複数の機器と通信可能に接続され、前記フィルタ規則を管理する管理装置としてコンピュータを機能させるための管理プログラムであって、

外部ネットワークに他の前記機器を介することなく接続している第 1 の前記機器が所定の状態になった場合に、前記第 1 の機器を介して外部ネットワークに接続している複数の第 2 の前記機器から受信した複数の分散フィルタ規則に基づいて前記第 1 の機器に設定されている分散フィルタ規則を復元し、該復元した分散フィルタ規則を前記複数の第 2 の機器に設定すると共に、

前記分散フィルタ規則は、全ての分散フィルタ規則を用いることなく前記フィルタ規則を復元可能に分散されている管理装置として前記コンピュータを機能させることを特徴とする管理プログラム。

[0140] (付記 1 2) 通信データのフィルタリングをするために用いるフィルタ規則を分散することにより、複数の分散後フィルタ規則を生成するフィルタ管理手段と、

前記複数の分散後フィルタ規則を、前記フィルタリングを実行する複数の機器に対して送信する送信手段と、を備え、

前記フィルタ管理手段は、前記分散後のフィルタ規則を所定個数以上用いれば前記分散前のフィルタ規則を復元できるように前記分散を行なうことを特徴とするフィルタ管理装置。

[0141] (付記 1 3) 前記複数の機器に対して以前送信した前記分散後のフィル

タ規則を、前記複数の機器から前記所定個数以上受信し、該受信した所定個数のフィルタ規則を用いて前記分散前のフィルタ規則を復元することを特徴とする付記 1 2 に記載のフィルタ管理装置。

[0142] (付記 1 4) 前記分散前のフィルタ規則を再度分散することにより、前記機器の内の第 1 の機器に以前送信した分散後のフィルタ規則と同一のフィルタ規則を生成し、該生成したフィルタ規則を前記機器の内の第 2 の機器に送信することを特徴とする付記 1 2 又は 1 3 に記載のフィルタ管理装置。

[0143] (付記 1 5) 前記第 1 の機器は、自機器に所定の重さ以上の負荷がかかっている機器であることを特徴とする付記 1 4 に記載のフィルタ管理装置。

[0144] (付記 1 6) 前記第 1 の機器は、外部ネットワークに他の機器を介することなく接続している機器であり、前記第 2 の機器は、前記第 1 の機器を介して前記外部ネットワークに接続されている機器であることを特徴とする付記 1 4 に記載のフィルタ管理装置。

[0145] (付記 1 7) 前記送信手段が前記分散後の前記フィルタ規則を送信したならば、前記分散前のフィルタ規則及び前記分散後のフィルタ規則を自フィルタ管理装置から削除することを特徴とする付記 1 2 乃至 1 6 の何れか 1 に記載のフィルタ管理装置。

[0146] (付記 1 8) 付記 1 2 乃至 1 7 の何れか 1 に記載のフィルタ管理装置と、前記機器とを含んだフィルタ管理システムであって、

前記機器は、前記フィルタ管理装置から前記分散後のフィルタ規則を受信すると、該受信したフィルタ規則に基づいて前記フィルタリングを実行することを特徴とするフィルタ管理システム。

[0147] (付記 1 9) 前記機器は、自機器に所定の重さ以上の負荷がかかっていることを検出すると、他の機器に対して通知を行い、

前記通知を受けた他の機器は、自機器が記憶している前記分散後のフィルタ規則を前記フィルタ管理装置に送信し、

前記フィルタ管理装置は、前記他の機器から前記分散後のフィルタ規則を前記所定個数以上受信し、該受信した所定個数のフィルタ規則を用いて前記

分散前のフィルタ規則を復元することを特徴とする付記 18 に記載のフィルタ管理システム。

[0148] この出願は、2015 年 7 月 23 日に提出された日本出願特願 2015-145636 を基礎とする優先権を主張し、その開示の全てをここに取り込む。

産業上の利用可能性

[0149] 本発明は、通信機器の種別やネットワークの種別を問うことなく、ネットワークにおけるフィルタリングの用途に広く好適である。

符号の説明

[0150] 11、12 外部フィルタ機器
21、22、23、24 内部フィルタ機器
30 フィルタ管理サーバ
31 フィルタ管理部
32 演算部
33 記憶部
34 通信部
40 外部ネットワーク
51、52、53、54 サブネット
100 フィルタ管理システム

請求の範囲

- [請求項1] フィルタ規則に基づいて通信データのフィルタリングを行なう複数の機器と、前記フィルタ規則を管理する管理装置と、を備えるフィルタリングシステムであって、
- 外部ネットワークに他の前記機器を介することなく接続している第1の前記機器が所定の状態になった場合に、前記管理装置が、前記第1の機器を介して外部ネットワークに接続している複数の第2の前記機器から受信した複数の分散フィルタ規則に基づいて前記第1の機器に設定されている分散フィルタ規則を復元し、該復元した分散フィルタ規則を前記複数の第2の機器に設定し、
- 前記分散フィルタ規則は、全ての分散フィルタ規則を用いることなく前記フィルタ規則を復元可能に分散されていることを特徴とするフィルタリングシステム。
- [請求項2] 前記第1の機器は、自機器が前記所定の状態になった場合に複数の前記第2の機器に対して通知を行い、
- 前記通知を受けた複数の第2の機器のそれぞれが、前記分散フィルタ規則を前記管理装置に送信し、
- 前記管理装置は、前記複数の第2の機器のそれぞれから受信した分散フィルタ規則に基づいて前記復元を行なうことを特徴とする請求項1に記載のフィルタリングシステム。
- [請求項3] 前記第1の機器は、前記通信データのフィルタリングの実行に起因して、自機器が所定の状態となった場合に前記通知を行なうことを特徴とする請求項2に記載のフィルタリングシステム。
- [請求項4] 前記第1の機器は、前記自機器が前記所定の状態になった場合に前記フィルタリングの実行を中止するが、前記外部ネットワークと前記第2の機器間での通信データの送受信の中継は継続することを特徴とする請求項1乃至3の何れか1項に記載のフィルタリングシステム。
- [請求項5] 前記管理装置は、前記分散フィルタ規則を各機器に設定したならば

、分散前のフィルタ規則及び分散フィルタ規則を自我管理装置から削除することを特徴とする請求項1乃至4の何れか1項に記載のフィルタリングシステム。

[請求項6] 前記管理装置は、前記第1の機器に設定する分散フィルタ規則と、前記第2の機器に設定する分散フィルタ規則とを異ならせることを特徴とする請求項1乃至5の何れか1項に記載のフィルタリングシステム。

[請求項7] 前記第2の機器は、前記第1の機器に対応する分散フィルタ規則を設定された場合には、自機器に設定されていた自機器に対応する分散フィルタ規則と、前記第1の機器に対応する分散フィルタ規則との双方のフィルタ規則に基づいて前記フィルタリングを実行することを特徴とする請求項1乃至6の何れか1項に記載のフィルタリングシステム。

[請求項8] フィルタ規則に基づいて通信データのフィルタリングを行なう複数の機器と通信可能に接続され、前記フィルタ規則を管理する管理装置であって、

外部ネットワークに他の前記機器を介することなく接続している第1の前記機器が所定の状態になった場合に、前記第1の機器を介して外部ネットワークに接続している複数の第2の前記機器から受信した複数の分散フィルタ規則に基づいて前記第1の機器に設定されている分散フィルタ規則を復元し、該復元した分散フィルタ規則を前記複数の第2の機器に設定すると共に、

前記分散フィルタ規則は、全ての分散フィルタ規則を用いることなく前記フィルタ規則を復元可能に分散されていることを特徴とする管理装置。

[請求項9] フィルタ規則に基づいて通信データのフィルタリングを行なう複数の機器と、前記フィルタ規則を管理する管理装置と、を備えるシステムが行なうフィルタリング方法であって、

外部ネットワークに他の前記機器を介することなく接続している第1の前記機器が所定の状態になった場合に、前記管理装置が、前記第1の機器を介して外部ネットワークに接続している複数の第2の前記機器から受信した複数の分散フィルタ規則に基づいて前記第1の機器に設定されている分散フィルタ規則を復元し、該復元した分散フィルタ規則を前記複数の第2の機器に設定し、

前記分散フィルタ規則は、全ての分散フィルタ規則を用いることなく前記フィルタ規則を復元可能に分散されていることを特徴とするフィルタリング方法。

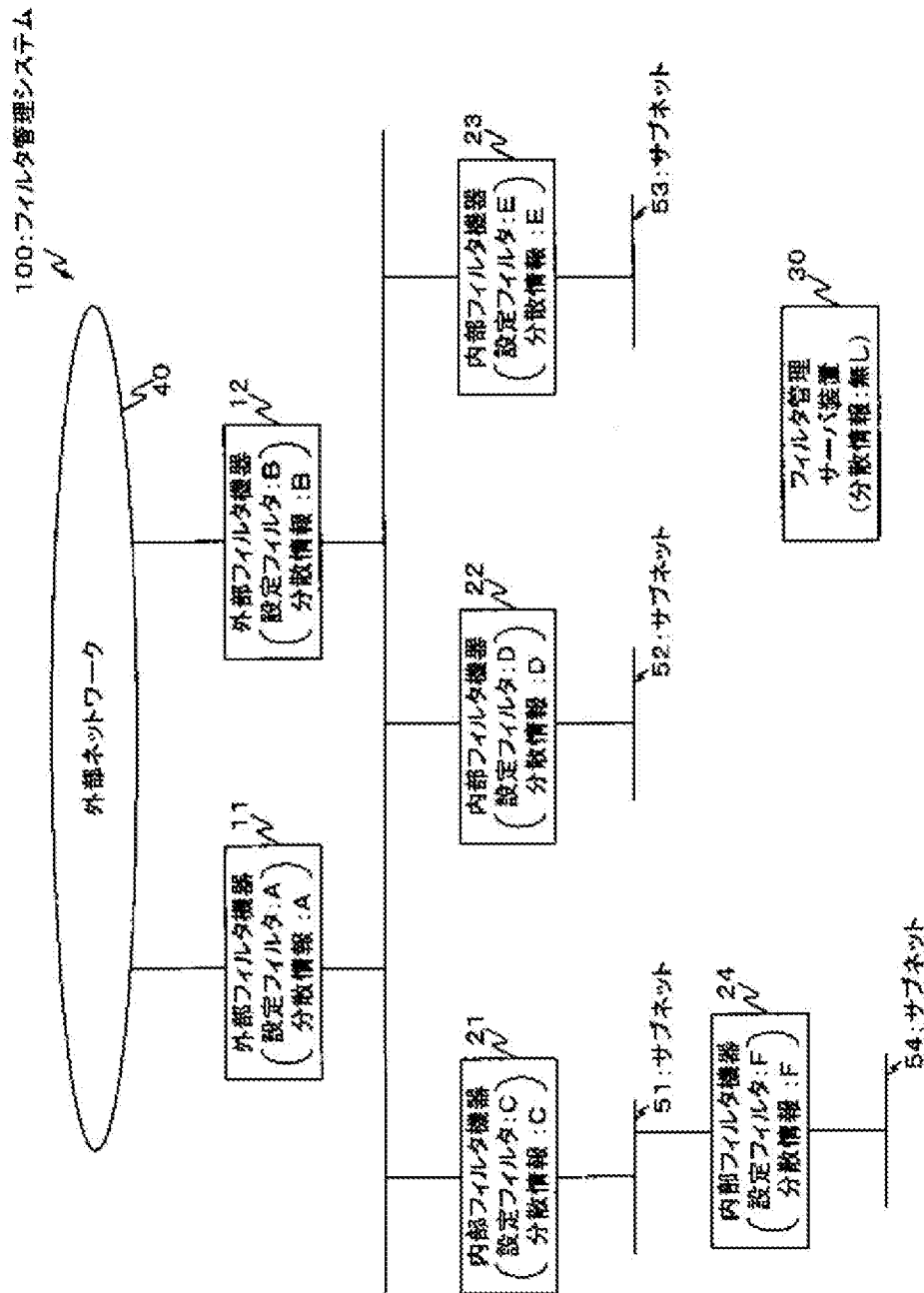
[請求項10]

フィルタ規則に基づいて通信データのフィルタリングを行なう複数の機器と通信可能に接続され、前記フィルタ規則を管理する管理装置としてコンピュータを機能させるための管理プログラムであって、

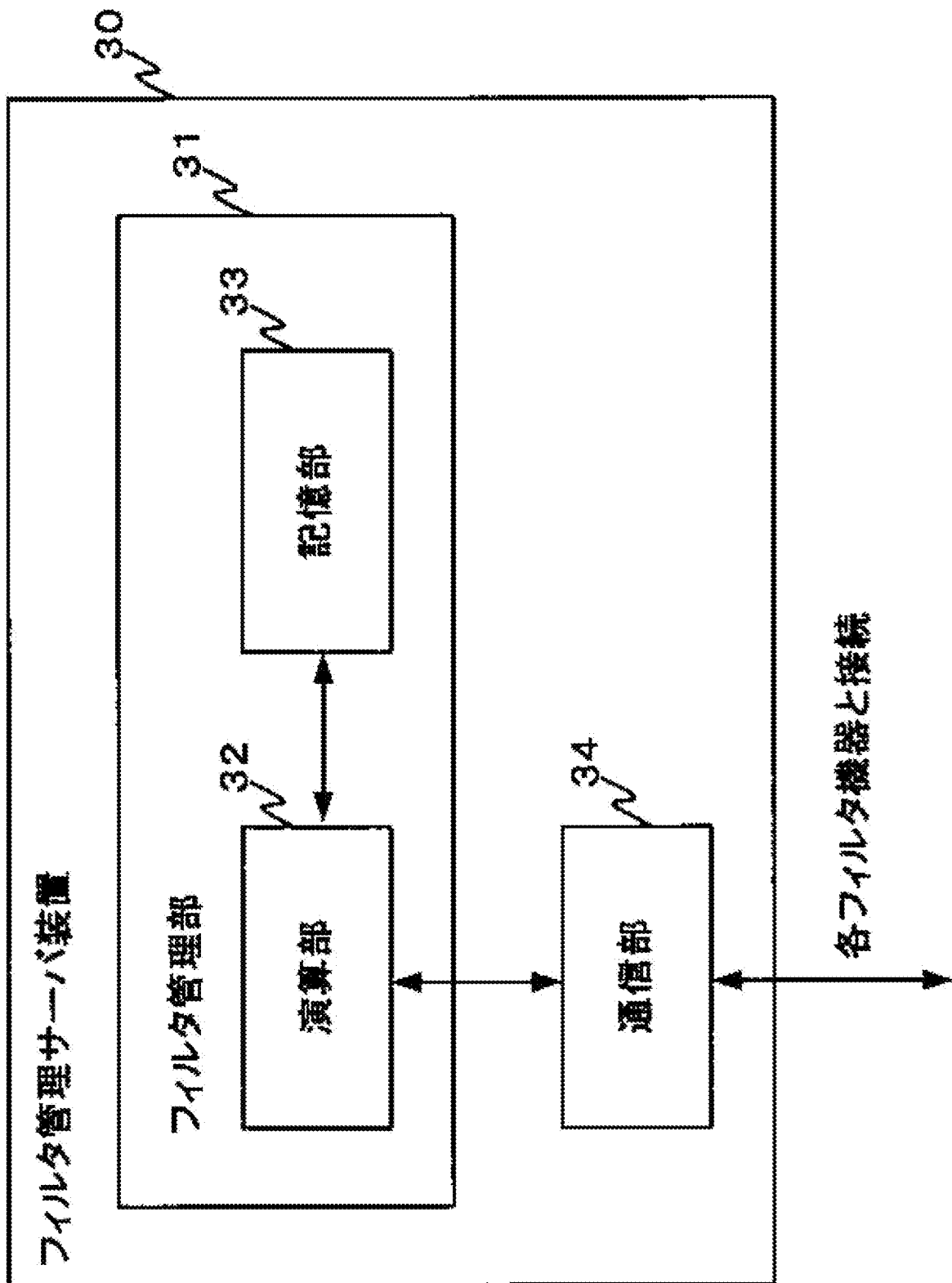
外部ネットワークに他の前記機器を介することなく接続している第1の前記機器が所定の状態になった場合に、前記第1の機器を介して外部ネットワークに接続している複数の第2の前記機器から受信した複数の分散フィルタ規則に基づいて前記第1の機器に設定されている分散フィルタ規則を復元し、該復元した分散フィルタ規則を前記複数の第2の機器に設定すると共に、

前記分散フィルタ規則は、全ての分散フィルタ規則を用いることなく前記フィルタ規則を復元可能に分散されている管理装置として前記コンピュータを機能させることを特徴とする管理プログラム。

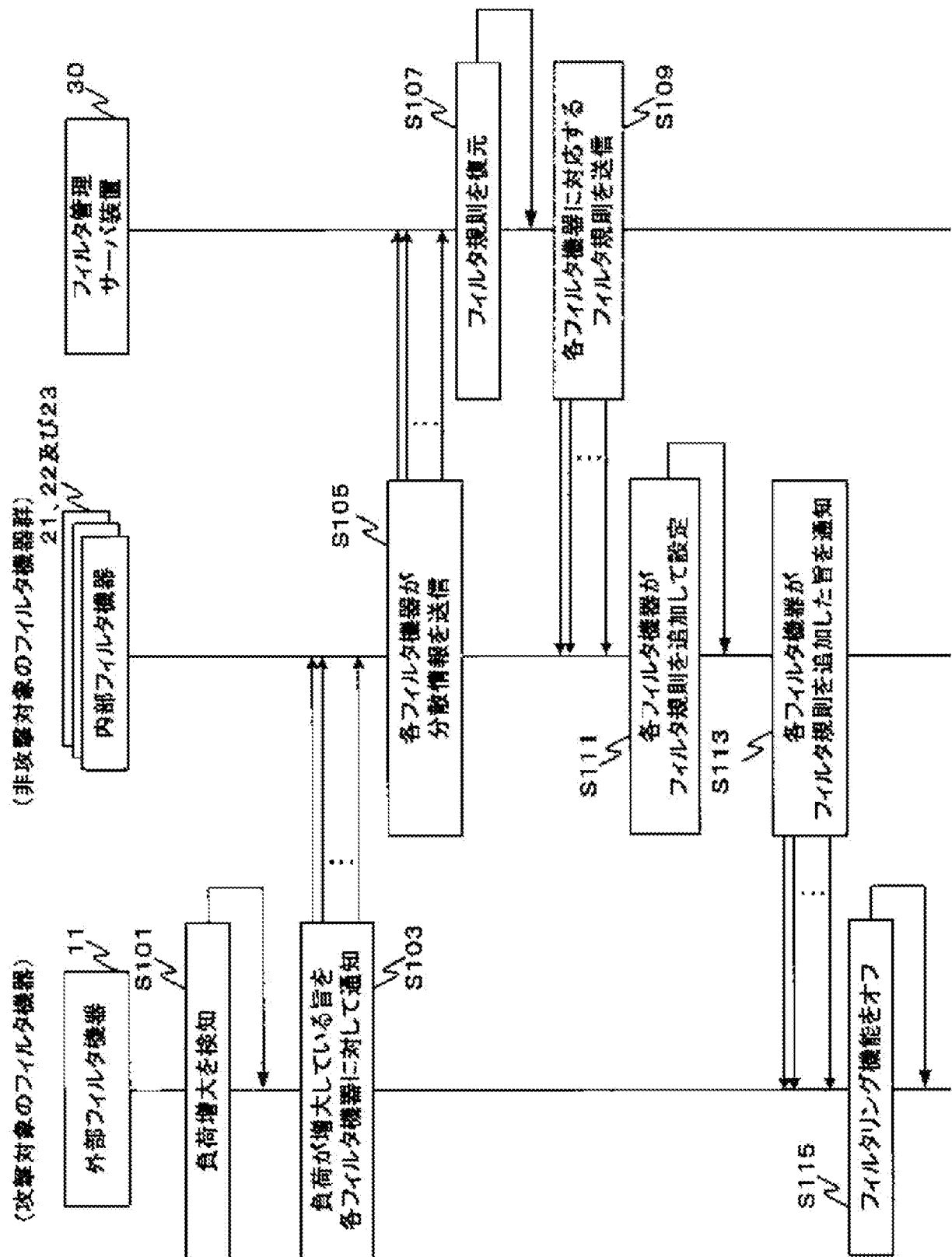
[図1]



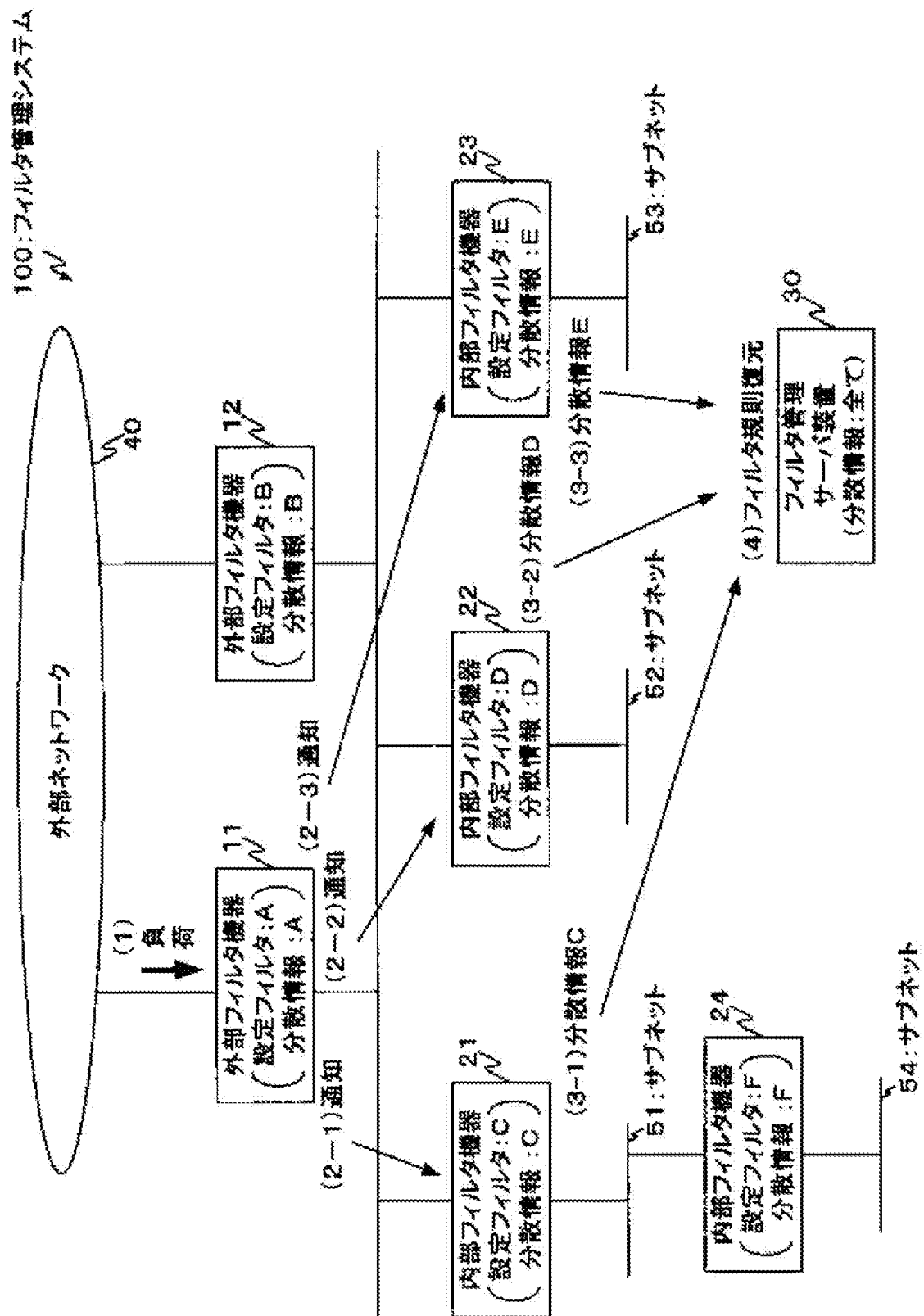
[図2]



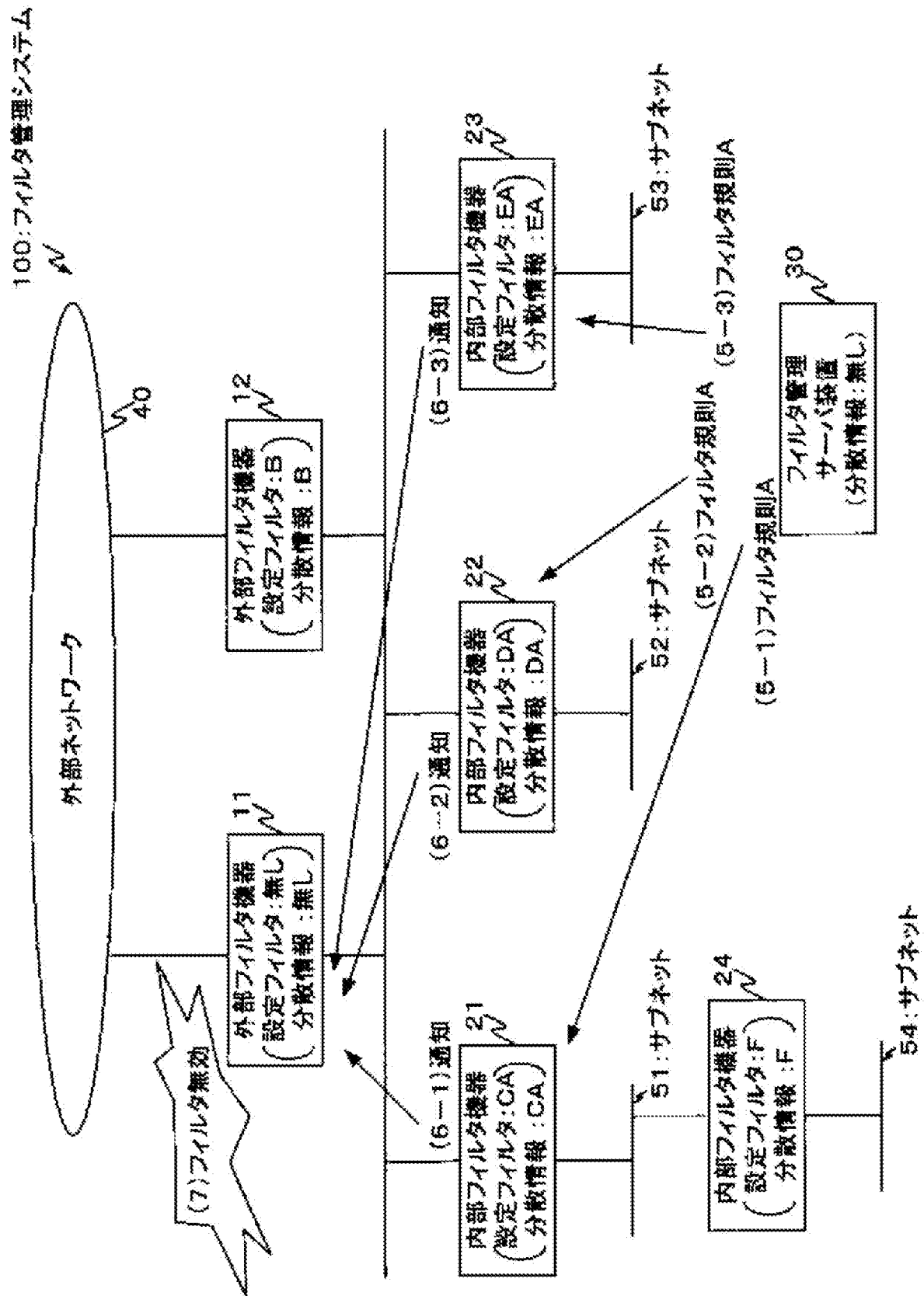
[図3]



[図4-1]

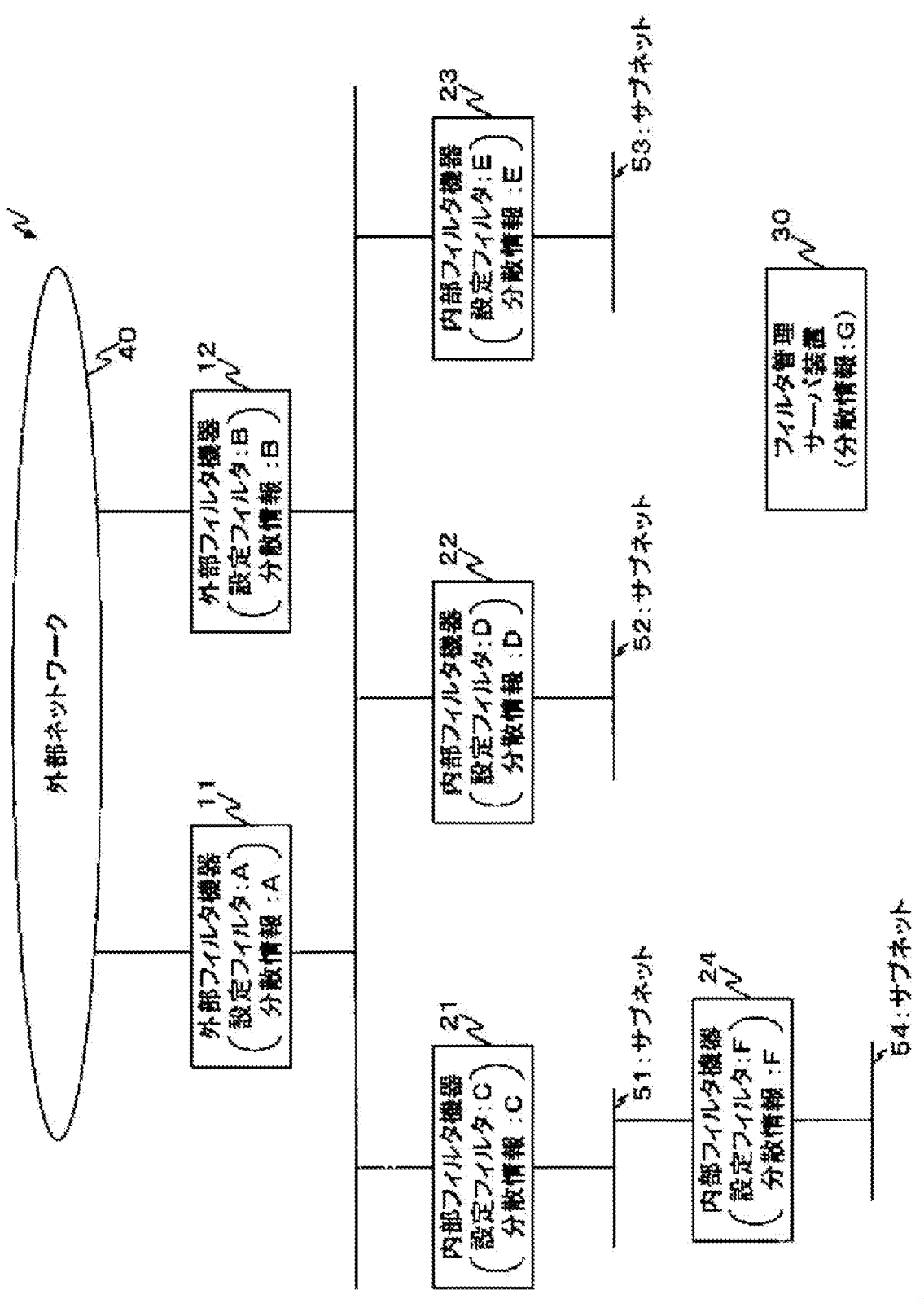


[図4-2]



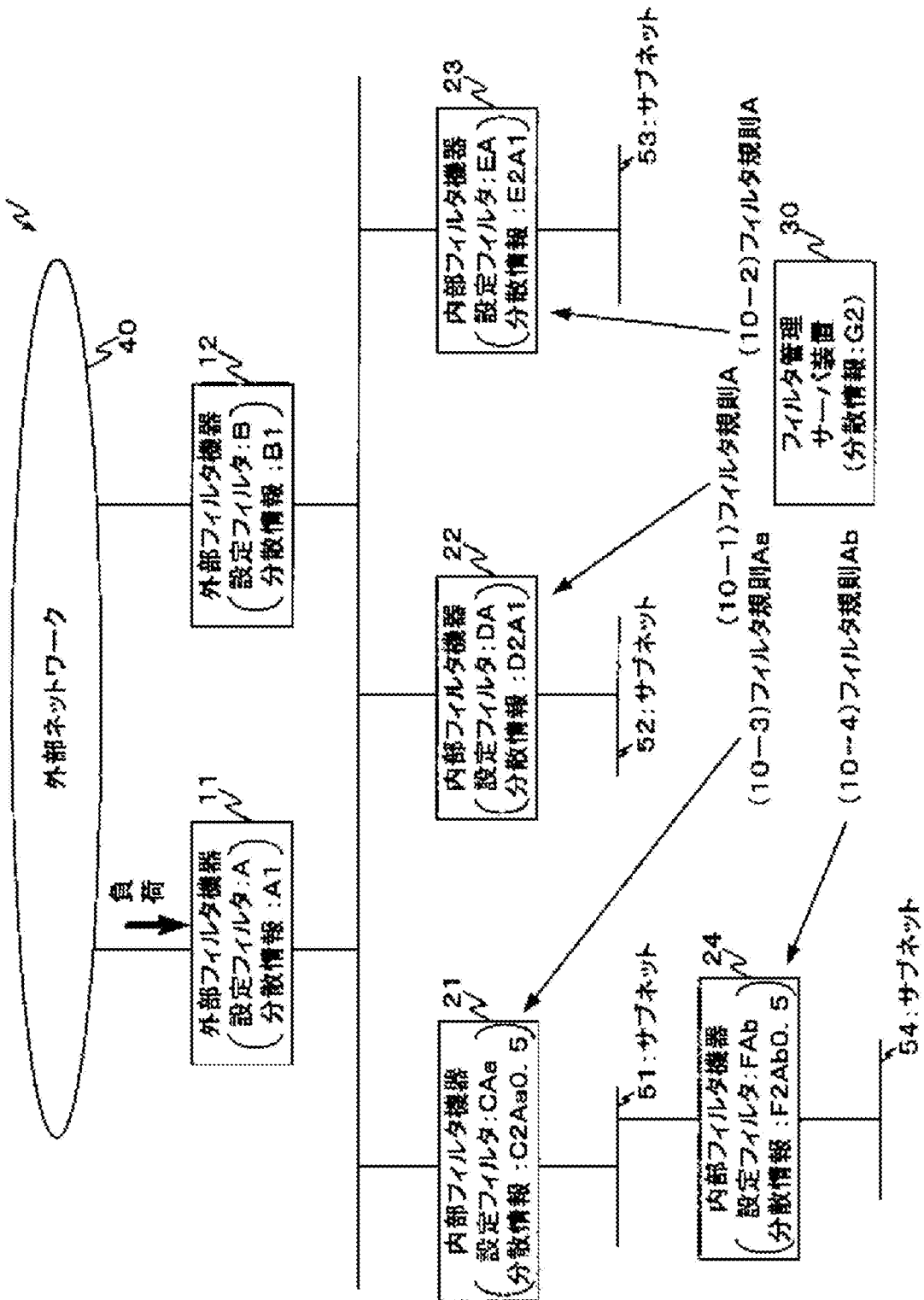
[図5]

100:フィルタ管理システム



[図7]

100:フィルタ管理システム



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2016/057175

A. CLASSIFICATION OF SUBJECT MATTER

H04L12/66(2006.01)i, H04L12/22(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)

G06F21/00, G06F21/12-21/57, H04L12/00-12/28, H04L12/44-12/955

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	1996-2016
Kokai Jitsuyo Shinan Koho	1971-2016	Toroku Jitsuyo Shinan Koho	1994-2016

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.
A	JP 2003-244247 A (Nippon Telegraph and Telephone Corp.), 29 August 2003 (29.08.2003), entire text; all drawings (Family: none)	1-10
A	JP 2011-172126 A (Mitsubishi Electric Corp.), 01 September 2011 (01.09.2011), entire text; all drawings (Family: none)	1-10
A	JP 2001-249866 A (Fujitsu Ltd.), 14 September 2001 (14.09.2001), entire text; all drawings (Family: none)	1-10

☐ 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
12 May 2016 (12.05.16)

Date of mailing of the international search report
24 May 2016 (24.05.16)

Name and mailing address of the ISA/
Japan Patent Office
3-4-3, Kasumigaseki, Chiyoda-ku,
Tokyo 100-8915, Japan

Authorized officer

Telephone No.

A. 発明の属する分野の分類（国際特許分類（IPC））

Int.Cl. H04L12/66(2006.01)i, H04L12/22(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. G06F21/00, G06F21/12-21/57, H04L12/00-12/28, H04L12/44-12/955

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	1971-2016年
日本国実用新案登録公報	1996-2016年
日本国登録実用新案公報	1994-2016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
A	JP 2003-244247 A（日本電信電話株式会社）2003.08.29, 全文, 全図（ファミリーなし）	1-10
A	JP 2011-172126 A（三菱電機株式会社）2011.09.01, 全文, 全図（ファミリーなし）	1-10
A	JP 2001-249866 A（富士通株式会社）2001.09.14, 全文, 全図（ファミリーなし）	1-10

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

12.05.2016

国際調査報告の発送日

24.05.2016

国際調査機関の名称及びあて先

日本国特許庁（ISA/J P）

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）

浦口 幸宏

5X

3358

電話番号 03-3581-1101 内線 3596