

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2013-90089

(P2013-90089A)

(43) 公開日 平成25年5月13日(2013.5.13)

(51) Int.Cl.	F I	テーマコード (参考)
<b>H04L 12/46 (2006.01)</b>	H04L 12/46 E	5K030
<b>H04L 12/66 (2006.01)</b>	H04L 12/66 B	5K033

審査請求 未請求 請求項の数 11 O L (全 16 頁)

(21) 出願番号	特願2011-227926 (P2011-227926)	(71) 出願人	000001007
(22) 出願日	平成23年10月17日 (2011.10.17)		キヤノン株式会社
			東京都大田区下丸子3丁目30番2号
		(74) 代理人	100090273
			弁理士 國分 孝悦
		(72) 発明者	丹治 雅道
			東京都大田区下丸子3丁目30番2号 キ
			ヤノン株式会社内
		Fターム(参考)	5K030 GA15 HA08 HD06 JA11 JT03
			KA05 KX24 LC13
			5K033 CC01 DA01 DB12 EA07 EC03

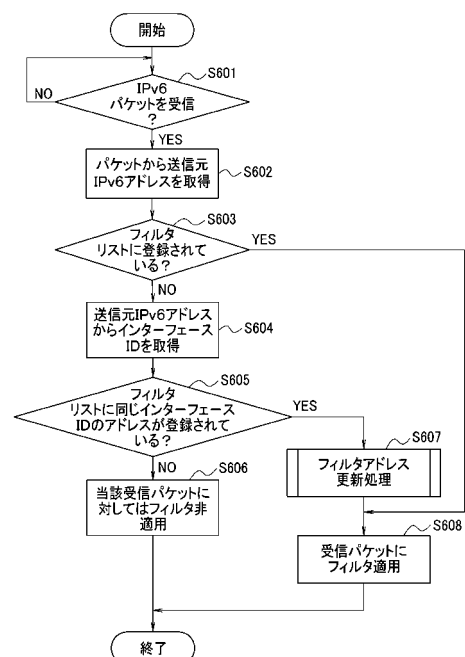
(54) 【発明の名称】 情報処理装置、情報処理方法、及びプログラム

## (57) 【要約】

【課題】外部装置からのパケットをより適切にフィルタリングすることを目的とする。

【解決手段】パケットから外部装置のアドレス情報を取得し、外部装置のアドレス情報がフィルタ情報に登録されているか否かを判断し、登録されていないと判断した場合、外部装置のアドレス情報から外部装置の装置識別情報を取り出し、取り出した装置識別情報と同じ装置識別情報を持つアドレス情報がフィルタ情報に登録されているか否かを判断し、登録されていると判断した場合、フィルタ情報に外部装置のアドレス情報を登録する更新を行うことによって課題を解決する。

【選択図】図6



**【特許請求の範囲】****【請求項 1】**

外部装置と通信可能に接続され、装置を識別可能な装置識別情報を含むアドレス情報が登録されたフィルタ情報に従って前記外部装置から受信したパケットのフィルタリングを行う情報処理装置であって、

前記パケットから前記外部装置のアドレス情報を取得する取得手段と、

前記外部装置のアドレス情報が前記フィルタ情報に登録されているか否かを判断し、登録されていないと判断した場合、前記外部装置のアドレス情報から前記外部装置の装置識別情報を取り出す取出手段と、

前記取出手段で取り出された装置識別情報と同じ装置識別情報を持つアドレス情報が前記フィルタ情報に登録されているか否かを判断し、登録されていると判断した場合、前記フィルタ情報に前記外部装置のアドレス情報を登録する更新を行う更新手段と、を有することを特徴とする情報処理装置。

10

**【請求項 2】**

前記外部装置に設けられているアドレス情報を管理する管理装置と通信可能に接続され、

前記外部装置のアドレス情報をもとに前記管理装置に問合せを行って前記外部装置のアドレス情報とは異なる前記外部装置の他のアドレス情報を取得するアドレス情報取得手段を更に有し、

前記更新手段は、前記装置識別情報を持つアドレス情報が前記フィルタ情報に登録されていると判断し、更に、前記アドレス情報取得手段で前記他のアドレス情報が取得されたと判断した場合、前記フィルタ情報に前記他のアドレス情報を登録する更新を行うことを特徴とする請求項 1 記載の情報処理装置。

20

**【請求項 3】**

前記更新手段は、前記装置識別情報を持つアドレス情報が前記フィルタ情報に登録されていると判断し、更に、前記装置識別情報を持つアドレス情報に対して存在しているかを確認する確認パケットを送付して前記確認パケットに対する応答パケットの受信を一定の時間待ち受け、前記応答パケットを前記一定の時間内に受信しないと判断した場合、前記装置識別情報を持つアドレス情報を前記フィルタ情報から削除する更新を行うことを特徴とする請求項 1 記載の情報処理装置。

30

**【請求項 4】**

アドレス情報には、装置が接続される通信回線を識別可能な通信回線識別情報が更に含まれ、

前記更新手段は、前記装置識別情報を持つアドレス情報が前記フィルタ情報に登録されていると判断し、更に、前記装置識別情報を持つアドレス情報の通信回線識別情報と同じ通信回線識別情報を持つアドレス情報が前記フィルタ情報に登録されているか否かを判断して登録されていると判断した場合、登録されていると判断したアドレス情報の通信回線識別情報を前記外部装置のアドレス情報の通信回線識別情報に変更する更新を行うことを特徴とする請求項 1 又は 2 記載の情報処理装置。

40

**【請求項 5】**

アドレス情報には、装置が接続される通信回線を識別可能な通信回線識別情報が更に含まれ、

前記装置識別情報を持つアドレス情報の通信回線識別情報と同じ通信回線識別情報を持つアドレス情報が前記フィルタ情報に登録されているか否かを判断し、登録されていると判断した場合、登録されていると判断したアドレス情報の通信回線識別情報を前記外部装置のアドレス情報の通信回線識別情報に変更した候補アドレス情報を生成する生成手段を更に有し、

前記更新手段は、前記装置識別情報を持つアドレス情報が前記フィルタ情報に登録されていると判断し、更に、前記候補アドレス情報に対して存在しているかを確認する確認パケットを送付して前記確認パケットに対する応答パケットの受信を一定の時間待ち受け、

50

前記応答パケットを前記一定の時間内に受信したと判断した場合、前記候補アドレス情報を前記フィルタ情報に登録する更新を行うことを特徴とする請求項 1 又は 3 記載の情報処理装置。

【請求項 6】

前記更新手段は、前記生成手段で登録されていると判断されたアドレス情報に対して存在しているかを確認する確認パケットを送付して前記確認パケットに対する応答パケットの受信を一定の時間待ち受け、前記応答パケットを前記一定の時間内に受信しないと判断した場合、前記生成手段で登録されていると判断されたアドレス情報を前記フィルタ情報から削除する更新を行うことを特徴とする請求項 5 記載の情報処理装置。

【請求項 7】

前記外部装置のアドレス情報は、IPv6 ステートレスアドレスであることを特徴とする請求項 1 乃至 6 の何れか 1 項記載の情報処理装置。

【請求項 8】

前記外部装置のアドレス情報の装置識別情報は、インターフェース ID であることを特徴とする請求項 1 乃至 7 の何れか 1 項記載の情報処理装置。

【請求項 9】

前記外部装置のアドレス情報の通信回線識別情報は、プレフィックス番号であることを特徴とする請求項 4 乃至 6 の何れか 1 項記載の情報処理装置。

【請求項 10】

外部装置と通信可能に接続され、装置を識別可能な装置識別情報を含むアドレス情報が登録されたフィルタ情報に従って前記外部装置から受信したパケットのフィルタリングを行う情報処理装置における情報処理方法であって、

前記パケットから前記外部装置のアドレス情報を取得する取得工程と、

前記外部装置のアドレス情報が前記フィルタ情報に登録されているか否かを判断し、登録されていないと判断した場合、前記外部装置のアドレス情報から前記外部装置の装置識別情報を取り出す取出工程と、

前記取出工程で取り出された装置識別情報と同じ装置識別情報を持つアドレス情報が前記フィルタ情報に登録されているか否かを判断し、登録されていると判断した場合、前記フィルタ情報に前記外部装置のアドレス情報を登録する更新を行う更新工程と、を有することを特徴とする情報処理方法。

【請求項 11】

外部装置と通信可能に接続され、装置を識別可能な装置識別情報を含むアドレス情報が登録されたフィルタ情報に従って前記外部装置から受信したパケットのフィルタリングを行うコンピュータを、

前記パケットから前記外部装置のアドレス情報を取得する取得手段と、

前記外部装置のアドレス情報が前記フィルタ情報に登録されているか否かを判断し、登録されていないと判断した場合、前記外部装置のアドレス情報から前記外部装置の装置識別情報を取り出す取出手段と、

前記取出手段で取り出された装置識別情報と同じ装置識別情報を持つアドレス情報が前記フィルタ情報に登録されているか否かを判断し、登録されていると判断した場合、前記フィルタ情報に前記外部装置のアドレス情報を登録する更新を行う更新手段として機能させるプログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、情報処理装置、情報処理方法、及びプログラムに関する。

【背景技術】

【0002】

近年、WWW (world wide web) などインターネットの普及により、不審な外部装置によるリモートアクセス、アタック攻撃、パケット盗聴などのネットワークセキュリティの

10

20

30

40

50

脆弱性が懸念されている。その対応策としてネットワークデバイスでもIPアドレスでフィルタリングする機能（フィルタリング機能）を保持するデバイスが一般的となっている。

フィルタリング機能では、予めユーザが任意のアドレスのアクセスを拒否、或いは任意のアドレスのみのアクセスを許可するように、ネットワークデバイスのフィルタリストに外部装置のアドレスを登録しておく。これにより、ネットワークデバイスは、見知らぬアドレスを持つ外部装置からの接続を切断し、セキュリティを確保している。

【0003】

しかしながら、IPv6では、1つの機器が複数のアドレスを保持することが可能である。そのため、ネットワークデバイスにおいて、フィルタリング機能を用いてIPv6アドレスのフィルタリングを行いたい場合、対象となる外部装置が保有する全てのIPv6アドレスをフィルタリストに登録する必要がある。

複数のIPv6アドレスをユーザが手動でフィルタリストに登録することは作業負荷が高い。また、複数のアドレスを手動で登録することで登録漏れ、登録ミスなどによりフィルタリングの対象から外れてしまい、外部装置からアクセスされてしまうというセキュリティの脆弱性にもつながる問題がある。

【0004】

そこで、ユーザがある1つのアドレスをフィルタリストに登録した際に、ネットワークデバイスがDNSサーバに問い合わせを行い、当該アドレスを持つ外部装置が保持している全てのアドレスを自動的に取得する方法が提案されている（例えば、特許文献1参照）。

ネットワークデバイスが、DNSサーバから取得したアドレスを自動的にフィルタリストに登録することで、ユーザに作業負荷がかかることなく、登録漏れや登録ミスのないフィルタリングを実現している。

【先行技術文献】

【特許文献】

【0005】

【特許文献1】特開2008-154009号公報

【発明の概要】

【発明が解決しようとする課題】

【0006】

ここで、IPv6アドレスの中には、ステートレスアドレスのように、定期的にその値が変更される可能性のあるものが存在する。

ステートレスアドレスは、ルータから定期的に配布されるプレフィックス番号と、機器自身が生成する、ネットワーク上で一意なインターフェースID（通常は機器自身のMACアドレスから所定の計算方法により生成される数値）とから構成されるアドレスである。また、ステートレスアドレスには有効期限が存在し、その期間は、ルータの設定の内容に依存する。そして、有効期限に達した場合には、ルータから新たなプレフィックス番号が配布され、機器では、新たなプレフィックス番号と自身のインターフェースIDとから構成される新たなステートレスアドレスが生成される。

【0007】

しかしながら、ネットワークデバイスのフィルタリストに外部装置が保持する全てのアドレスが適切に登録されても、当該外部装置のからのアクセスをフィルタリングしている環境において、以下のような問題が発生し得る。

即ち、適切なフィルタリングが行われているネットワーク環境において、ある時、フィルタリングの対象の外部装置のステートレスアドレスが変わってしまう場合がある。この場合、外部装置が変更後のステートレスアドレスを用いてアクセスしてきたとき、ネットワークデバイスは、当該アクセスを正しくフィルタリングすることができない。

【0008】

また、外部装置のアドレスの変更に追従してユーザがその都度ネットワークデバイスの

10

20

30

40

50

フィルタリストの内容を更新することは、常にネットワーク上の動向を監視していなければいけなくなることもあり、作業負荷の面から現実的に不可能である。

また、外部装置のアドレスが変更されていないかどうかをネットワークデバイスが定期的にポーリングするのは、処理が冗長で無駄が多く、また、それでもフィルタをすり抜ける時間帯が生じてしまう事態は避けられないため、根本的な解決とはならない。

【 0 0 0 9 】

本発明はこのような問題点に鑑みなされたもので、外部装置からのパケットをより適切にフィルタリングすることを目的とする。

【課題を解決するための手段】

【 0 0 1 0 】

そこで、本発明に係る情報処理装置は、外部装置と通信可能に接続され、装置を識別可能な装置識別情報を含むアドレス情報が登録されたフィルタ情報に従って前記外部装置から受信したパケットのフィルタリングを行う情報処理装置であって、前記パケットから前記外部装置のアドレス情報を取得する取得手段と、前記外部装置のアドレス情報が前記フィルタ情報に登録されているか否かを判断し、登録されていないと判断した場合、前記外部装置のアドレス情報から前記外部装置の装置識別情報を取り出す取出手段と、前記取出手段で取り出された装置識別情報と同じ装置識別情報を持つアドレス情報が前記フィルタ情報に登録されているか否かを判断し、登録されていると判断した場合、前記フィルタ情報に前記外部装置のアドレス情報を登録する更新を行う更新手段と、を有することを特徴とする。

【 0 0 1 1 】

また、本発明は、システム、記憶媒体等としてもよい。

【発明の効果】

【 0 0 1 2 】

本発明によれば、外部装置からのパケットをより適切にフィルタリングすることができる。

【図面の簡単な説明】

【 0 0 1 3 】

【図 1】デジタル複合機のハードウェアの構成の一例を示す図である。

【図 2】デジタル複合機の処理部の構成の一例を示す図である。

【図 3】システムの構成の一例を示す図である。

【図 4】フィルタアドレスの一例を示す図である。

【図 5】IPアドレスとホスト名とを対応付けた情報の一例を示す図である。

【図 6】フィルタアドレス自動更新処理に係るフローチャートの一例を示す図である。

【図 7】フィルタアドレス更新処理に係るフローチャートの一例を示す図である。

【図 8】フィルタアドレス更新処理に係るフローチャートの一例を示す図である。

【図 9】フィルタアドレス更新処理に係るフローチャートの一例を示す図である。

【図 10】フィルタアドレス更新処理に係るフローチャートの一例を示す図である。

【発明を実施するための形態】

【 0 0 1 4 】

以下、本発明の実施形態について図面に基づいて説明する。なお、実施形態は、本発明を限定するものではなく、また、実施形態で説明されている全ての構成が本発明の課題を解決するための手段に必須であるとは限らない。

【 0 0 1 5 】

図 1 は、本実施形態に係るデジタル複合機のハードウェアの構成の一例を示す図である。プリンタコントローラ 100 は、情報処理装置（コンピュータ）の一例であり、プリンタ 120 を制御する。

プリンタコントローラ 100 内部で、CPU 101 は、デジタル複合機のソフトウェアプログラムを実行し、デジタル複合機全体の制御を行う。即ち、CPU 101 が、ROM 102、HDD 108 等に格納されたプログラムの手順に従って処理を行うことによって

10

20

30

40

50

、デジタル複合機における機能及び後述するフローチャートに係る処理が実現される。なお、デジタル複合機における機能、後述するフローチャートに係る処理の一部、又は全部を専用のハードウェアを用いて構成してもよい。

#### 【0016】

ROM 102は、リードオンリーメモリであり、デジタル複合機のブートプログラム、固定パラメータ等を記憶する。RAM 103は、ランダムアクセスメモリであり、CPU 101がデジタル複合機を制御する際に用いる一時的なデータなどを記憶する。HDD 108は、ハードディスクドライブであり、印刷データなど、様々なデータを記憶する。

タイマ 109は、タイマ処理における経過時刻の管理を行う。プリンタ I/F 制御部 104は、プリンタ 120とのデータの送受信（データ通信）などを制御する。NVRAM 105は、不揮発性のメモリであり、デジタル複合機の各種の設定値を記憶する。

#### 【0017】

パネル制御部 106は、オペレーションパネル 111を制御し、各種の情報の表示、使用者からの指示の入力を行う。ネットワーク I/F 制御部 107は、LAN 112等のネットワークを介して接続された外部装置とのデータの送受信を制御する。

バス 110には、CPU 101、ROM 102、RAM 103、HDD 108、タイマ 109、プリンタ I/F 制御部 104、NVRAM 105、パネル制御部 106、及びネットワーク I/F 制御部 107が通信可能に接続される。なお、バス 110は、CPU 101からの制御信号や各装置間のデータ信号が送受信されるシステムバスである。

#### 【0018】

図2は、デジタル複合機の処理部（モジュール）の構成の一例を示す図である。ユーザインターフェース部 201は、ユーザがフィルタリングを行うアドレス（アドレス情報）を登録する操作を受け付ける。ユーザインターフェース部 201より入力されたアドレスは、フィルタアドレス登録部 202により、フィルタアドレス記憶部 204に記憶（登録）される。なお、フィルタアドレス記憶部 204に記憶されているアドレスをフィルタアドレス（フィルタ情報の一例）と適宜称する。ここで、フィルタアドレス記憶部 204は、ROM 102、HDD 108、或いはNVRAM 105上に存在する。

また、フィルタアドレス登録部 202は、アドレスを登録した場合、登録したアドレスを保持する外部装置が他のアドレスも保持しているかを判別するために、登録したアドレスをアドレス拡張制御部 203に渡す。アドレス拡張制御部 203は、フィルタアドレス登録部 202からアドレスを受け取ると、ネットワークパケット送受信部 206を利用し、受け取ったアドレスを保持する外部装置の他のアドレスを、外部装置を管理する管理装置等から取得する。また、ネットワークパケット送受信部 206は、外部装置とのデータ通信のやり取りの制御を行う。

#### 【0019】

ここで、フィルタアドレス記憶部 204にアドレスが登録されている場合、ネットワークパケット送受信部 206は、外部装置からパケット（ネットワークパケット）を受信するたびに、ネットワークフィルタ制御部 205に当該外部装置のアドレスを渡す。

ネットワークフィルタ制御部 205は、アドレスを受け取った場合、フィルタアドレス記憶部 204を参照し、受け取ったアドレスに該当するフィルタアドレスが存在するかどうかを確認する。ネットワークフィルタ制御部 205は、該当するフィルタアドレスを発見した場合、予め設定されている処理を、接続要求を送信してきた外部装置に対して行う。

#### 【0020】

図3は、本実施形態に係るシステムの構成の一例を示す図である。本システムは、ネットワークデバイス 300、外部装置 301、外部装置 302、DNSサーバ 303、ルータ 304等を含んで構成される。

ネットワークデバイス 300は、プリンタコントローラ 100、オペレーションパネル 111、及びプリンタ 120を有するデジタル複合機の一例である。また、ネットワークデバイス 300は、フィルタリング機能を実装し、外部装置（301、302）に対する

フィルタリングの設定を行うことが可能に構成されている。

【 0 0 2 1 】

外部装置 3 0 1 及び外部装置 3 0 2 は、ルータ 3 0 4 によって、異なるサブネットからネットワークデバイス 3 0 0 と通信を行う。本実施形態では、外部装置 3 0 1 には、I P v 6 アドレス ( I P v 6 ステートレスアドレス ) として「fee0:1::203:3ff:fe30:1」及び「fee0:2::203:3ff:fe30:1」という 2 つのアドレスが保持されているものとする。また、外部装置 3 0 2 には I P v 6 アドレスとして「fee0:1::204:4ff:fe40:2」及び「fee0:2::204:4ff:fe40:2」という 2 つのアドレスが保持されているものとする。

なお、外部装置 3 0 1 及び外部装置 3 0 2 は、I P v 6 アドレスとして更に少なくともリンクローカルアドレスを保持している。しかしながら、リンクローカルアドレスは、ルータ 3 0 4 等の中継装置を超える通信には使用されないもので、ここでは表示を省略している。

【 0 0 2 2 】

D N S サーバ 3 0 3 は、ネットワーク内のデバイスの I P アドレスとホスト名とを解決する。

なお、本実施形態では、外部装置 3 0 1、外部装置 3 0 2、及び D N S サーバ 3 0 3 がネットワークデバイス 3 0 0 とは異なるサブネット上に存在するケースを例としているが、このネットワークの構成に限定されるものではない。例えば、外部装置 3 0 1、外部装置 3 0 2、及び D N S サーバ 3 0 3 は、それぞれ、ネットワークデバイス 3 0 0 と同じサブネット上に存在していてもよいし、異なるサブネット上に存在していてもよい。

【 0 0 2 3 】

図 4 は、ネットワークデバイス 3 0 0 のフィルタアドレス記憶部 2 0 4 に登録されているフィルタアドレスの一例 ( フィルタアドレス情報 4 0 1 ) を示す図である。

フィルタアドレス情報 4 0 1 には、外部装置 3 0 1 が保持する「fee0:1::203:3ff:fe30:1」及び「fee0:2::203:3ff:fe30:1」が登録されているものとする。更に、フィルタアドレス情報 4 0 1 には、外部装置 3 0 2 が保持する「fee0:1::204:4ff:fe40:2」及び「fee0:2::204:4ff:fe40:2」が登録されているものとする。

なお、この登録は、ユーザが全て手動で行ったものであっても、特許文献 1 に記載の手段などにより自動的に登録されたものであってもよい。何れの場合であっても、外部装置 3 0 1 及び外部装置 3 0 2 が保持するアドレスが全て適切に登録されているので、ネットワークデバイス 3 0 0 は、これらの外部装置からのアクセスを適切に制御できる状態である。

【 0 0 2 4 】

例えば、外部装置 3 0 1 からネットワークデバイス 3 0 0 に対してアクセスが試みられた場合、まず、ネットワークパケット送受信部 2 0 6 は、当該アクセスのパケット ( アクセスパケット ) を受信し、そのアクセスパケット中から送信元のアドレスを取得する。本例では、送信元のアドレスとして「fee0:1::203:3ff:fe30:1」が取得できたものとする。そして、ネットワークパケット送受信部 2 0 6 は、送信元のアドレスをネットワークフィルタ制御部 2 0 5 に渡す。

ネットワークフィルタ制御部 2 0 5 は、フィルタアドレス記憶部 2 0 4 を参照し、受け取った送信元のアドレスに該当するフィルタアドレスが存在するかどうかを参照する。本例では、図 4 に示すとおり、フィルタアドレスとして「fee0:1::203:3ff:fe30:1」が登録されているので、ネットワークフィルタ制御部 2 0 5 は、予め設定されている処理を当該アクセスパケットに対して行う。

【 0 0 2 5 】

図 5 は、D N S サーバ 3 0 3 が管理する、ネットワークデバイス 3 0 0、外部装置 3 0 1、外部装置 3 0 2 等の I P アドレスとホスト名とを対応付けた情報の一例 ( 設定ファイル情報 5 0 1 ) を示す図である。

D N S サーバ 3 0 3 は、ネットワークデバイス 3 0 0 等のクライアントからクエリ ( D N S 要求 ) されるたびに、設定ファイル情報 5 0 1 を参照し、名前解決等を行ってレスポ

10

20

30

40

50

ンスする。また、設定ファイル情報 5 0 1 は、各デバイスのアドレスが更新されたタイミングなど、各デバイスの動的更新（DDNS：Dynamic DNS）機能等によって適時更新される。

#### 【 0 0 2 6 】

ここで、図 3 に示すシステムの構成下において、ある時、外部装置 3 0 1 の I P v 6 アドレスが変更されたものとする。即ち、従来の「fee0:1::203:3ff:fe30:1」及び「fee0:2::203:3ff:fe30:1」から「1234:1::203:3ff:fe30:1」及び「1234:2::203:3ff:fe30:1」に変更されたものとする。

これは、ルータ 3 0 4 において、管理するプレフィックス番号（「fee0:1」及び「fee0:2」）が有効期限に達したことによるものである。これにより、ルータ 3 0 4 は、新たなプレフィックス番号（「1234:1」及び「1234:2」）を外部装置 3 0 1 が存在するネットワーク上に送出した。なお、プレフィックス番号は、装置（外部装置 3 0 1 等）が接続される通信回線（ネットワーク等）を識別可能な通信回線識別情報の一例である。

#### 【 0 0 2 7 】

図 6 は、フィルタリングの対象であった外部装置（以下では、外部装置 3 0 1 を例に挙げて適宜説明する。）のアドレスが変更された際の、ネットワークデバイス 3 0 0 におけるフィルタアドレス自動更新処理に係るフローチャートの一例を示す図である。ここで、本フローチャートに係るプログラム、及びプログラムの実行に必要なデータは、ROM 1 0 2、HDD 1 0 8 等に記憶されており、CPU 1 0 1 によって RAM 1 0 3 に読み出されて実行される。

まず、ネットワークパケット送受信部 2 0 6 は、外部装置からパケットを受信したか否かを判断する（S 6 0 1）。このとき、ネットワークパケット送受信部 2 0 6 は、受信したと判断した場合、S 6 0 2 に処理を移し、他方、受信していないと判断した場合、S 6 0 1 に処理を移す。換言するならば、ネットワークデバイス 3 0 0 は、ネットワークパケット送受信部 2 0 6 において外部装置からネットワークパケットを受信するのを待ち受ける。本例では、ネットワークデバイス 3 0 0 が、アドレスの変更後の外部装置 3 0 1 から新たな I P v 6 アドレスの「1234:1::203:3ff:fe30:1」を送信元とするパケットを受信したものとする。

#### 【 0 0 2 8 】

S 6 0 2 では、ネットワークパケット送受信部 2 0 6 は、受信したパケットから送信元のアドレスを取得する（S 6 0 2）。本例では、「1234:1::203:3ff:fe30:1」が取得されることとなる。そして、ネットワークパケット送受信部 2 0 6 は、送信元のアドレスをネットワークフィルタ制御部 2 0 5 に渡す。

続いて、ネットワークフィルタ制御部 2 0 5 は、フィルタアドレス記憶部 2 0 4（フィルタリスト）を参照し、受け取った送信元のアドレスに該当するフィルタアドレスが存在するかを判定する（S 6 0 3）。このとき、ネットワークフィルタ制御部 2 0 5 は、存在すると判断した場合、S 6 0 8 に処理を移し、他方、存在しないと判断した場合、S 6 0 4 に処理を移す。

#### 【 0 0 2 9 】

S 6 0 4 では、ネットワークフィルタ制御部 2 0 5 は、送信元のアドレスのインターフェース ID を取得する（送信元のアドレスからインターフェース ID を取出す）。なお、インターフェース ID は、装置（外部装置 3 0 1 等）を識別可能な装置識別情報の一例であり、例えば送信元のアドレスの規定の下位ビット部分である。

続いて、ネットワークフィルタ制御部 2 0 5 は、取得したインターフェース ID を持つフィルタアドレスがフィルタアドレス記憶部 2 0 4 に存在するかを判定する（S 6 0 5）。このとき、ネットワークフィルタ制御部 2 0 5 は、存在すると判断した場合、S 6 0 7 に処理を移し、存在しないと判断した場合、S 6 0 6 に処理を移す。

S 6 0 6 では、ネットワークフィルタ制御部 2 0 5 は、外部装置 3 0 1 からのパケット（アクセスパケット）に対して予め設定されている処理を実施せずに（フィルタ非適用）、本フローチャートの処理を終了する。

10

20

30

40

50



## 【 0 0 3 0 】

S 6 0 7では、後述するフィルタアドレス更新処理（サブルーチン）が実行される。なお、フィルタアドレス更新処理では、例えば、送信元のアドレスが登録される。

ここで、本例では、フィルタアドレス記憶部 2 0 4 には、送信元のアドレス「1234:1::203:3ff:fe30:1」と同じフィルタアドレスは存在しない。しかしながら、フィルタアドレス記憶部 2 0 4 には、「1234:1::203:3ff:fe30:1」と同じインターフェース I D の「fee0:1::203:3ff:fe30:1」及び「fee0:2::203:3ff:fe30:1」が登録されている。故に、フィルタアドレス更新処理が実行されることとなる。

S 6 0 8では、ネットワークフィルタ制御部 2 0 5 は、予め設定されている処理をアクセスパケットに対して行い（フィルタ適用）、本フローチャートの処理を終了する。

10

## 【 0 0 3 1 】

図 7 は、フィルタアドレス更新処理に係るフローチャートの一例を示す図である。ここで、本フローチャートに係るプログラム、及びプログラムの実行に必要なデータは、R O M 1 0 2、H D D 1 0 8 等に記憶されており、C P U 1 0 1 によって R A M 1 0 3 に読み出されて実行される。

まず、アドレス拡張制御部 2 0 3 は、ネットワークパケット送受信部 2 0 6 を利用して、D N S サーバ 3 0 3 に問い合わせを行う。この問合せにより、送信元のアドレスを保持する外部装置のホスト名を取得する（S 7 0 1）。本例では、アドレス拡張制御部 2 0 3 は、「1234:1::203:3ff:fe30:1」のホスト名を D N S サーバ 3 0 3 に問い合わせることになる。D N S サーバ 3 0 3 は、設定ファイル情報 5 0 1 の内容を参照して、対応するホスト名である「dev1」をネットワークデバイス 3 0 0 に返す。なお、設定ファイル情報 5 0 1 については、上述したように外部装置 3 0 1 のアドレスが変更された際に更新されている。

20

## 【 0 0 3 2 】

続いて、アドレス拡張制御部 2 0 3 は、ホスト名「dev1」の I P v 6 アドレスを D N S サーバ 3 0 3 にクエリし、「dev1」の全ての I P v 6 アドレスを取得する（S 7 0 2）。なお、S 7 0 1 及び S 7 0 2 の処理は、外部装置（外部装置 3 0 1 等）のアドレス情報をもとに管理装置（D N S サーバ 3 0 3 等）に問合せを行って外部装置のアドレス情報とは異なる外部装置の他のアドレス情報を取得するアドレス情報取得処理の一例である。

本例では、「dev1」に対応する I P v 6 アドレスとして「1234:1::203:3ff:fe30:1」及び「1234:2::203:3ff:fe30:1」が取得される。そして、アドレス拡張制御部 2 0 3 は、「dev1」の全ての I P v 6 アドレスをフィルタアドレス登録部 2 0 2 に渡す。

30

続いて、フィルタアドレス登録部 2 0 2 は、フィルタアドレス記憶部 2 0 4 の内容を更新する（S 7 0 3）。即ち、フィルタアドレス記憶部 2 0 4 に「1234:1::203:3ff:fe30:1」及び「1234:1::203:3ff:fe30:1」が登録される。なお、既に登録されているフィルタアドレスのうち、「fee0:1::203:3ff:fe30:1」及び「fee0:2::203:3ff:fe30:1」が削除される。そして、フィルタアドレス登録部 2 0 2 は、本フローチャートの処理を終了する。

## 【 0 0 3 3 】

以上、本実施形態によれば、フィルタリングの対象の外部装置のステートレスアドレスが変更された場合にも、ネットワークデバイスでその変更を検知し、フィルタリストを最新のアドレスに更新することが可能となる。

40

この構成によれば、ネットワークデバイスでは、フィルタをすり抜ける時間帯を生じさせることなく、適切なフィルタリングを実施し続けることが可能となる。更に、この際、ユーザが手動で設定の内容を変更する必要がないので、ユーザの作業負荷も大幅に軽減できる。

## 【 0 0 3 4 】

## &lt; 第 2 の実施形態 &gt;

本実施形態では、第 1 の実施形態のフィルタアドレス更新処理において、D N S サーバ 3 0 3 を用いない構成について説明する。なお、本実施形態では、第 1 の実施形態の構成と同一の構成については同一の符号を用いて、その説明を適宜省略する。

50

図 8 は、本実施形態に係るフィルタアドレス更新処理に係るフローチャートの一例を示す図である。ここで、本フローチャートに係るプログラム、及びプログラムの実行に必要なデータは、ROM 102、HDD 108 等に記憶されており、CPU 101 によって RAM 103 に読み出されて実行される。

なお、フィルタアドレス更新処理は、第 1 の実施形態と同様に、図 6 の S 607 において呼び出される。

#### 【0035】

まず、ネットワークフィルタ制御部 205 は、フィルタアドレス登録部 202 を介して、送信元のアドレスをフィルタアドレス記憶部 204 に登録する (S 801)。本例においては、「1234:1::203:3ff:fe30:1」が新たにフィルタアドレス記憶部 204 に登録されることとなる。そして、「1234:1::203:3ff:fe30:1」と同じインターフェース ID の「fee0:1::203:3ff:fe30:1」及び「fee0:2::203:3ff:fe30:1」がアドレス拡張制御部 203 に渡される。

10

続いて、アドレス拡張制御部 203 は、ネットワークパケット送受信部 206 を利用して、「fee0:1::203:3ff:fe30:1」及び「fee0:2::203:3ff:fe30:1」に対して存在確認パケットを送信 (送付) する (S 802)。存在確認パケットは、当該アドレスの外部装置で未だ使用されているか否か、即ち当該アドレスが存在しているか否かを外部装置に確認するためのパケットである。例えば、存在確認パケットは、当該アドレスに対する ICMPv6 (Internet Control Message Protocol for IPv6) の近隣要請 (Neighbor Solicitation) パケットである。

20

#### 【0036】

そして、アドレス拡張制御部 203 は、存在確認パケットに対する存在応答パケットを受信するのを所定の期間待ち受ける (一定の時間待ち受ける)。続いて、アドレス拡張制御部 203 は、存在応答パケットを受信したか否かを判断する (S 803)。

このとき、アドレス拡張制御部 203 は、所定の期間内 (一定の時間内) に受信したと判断した場合、フィルタアドレス記憶部 204 の更新に係る処理は行わず、本フローチャートの処理を終了する。この場合、例えば、「1234:1::203:3ff:fe30:1」というアドレスは、外部装置 301 に新たに追加された IPv6 アドレスであることになる。

他方、アドレス拡張制御部 203 は、所定の期間内 (一定の時間内) に受信していないと判断した場合、当該アドレスが既に使用されていないものと判断し、S 804 に処理を移す。なお、存在応答パケットは、存在確認パケットに対するパケットであり、例えば、ICMPv6 の近隣広告 (Neighbor Advertisement) パケットである。

30

S 804 では、アドレス拡張制御部 203 は、フィルタアドレス登録部 202 を介して、フィルタアドレス記憶部 204 から存在していないと判断したアドレスを削除し、本フローチャートの処理を終了する。

#### 【0037】

以上、本実施形態によれば、ネットワークデバイスは、DNS サーバが存在しないネットワーク環境下においても、フィルタリングの対象の外部装置のステータスアドレスが変更されたことを自動で検知することができる。故に、フィルタリストを最新のアドレスに更新することが可能となる。

40

#### 【0038】

##### < 第 3 の実施形態 >

本実施形態では、第 1 の実施形態のフィルタアドレス更新処理において、フィルタアドレス記憶部 204 の中に他にもアドレスが変更されている可能性のあるフィルタアドレスが存在するかが更に判断される。そして、存在していた場合、そのフィルタアドレスも更新される。なお、本実施形態では、第 1 の実施形態の構成と同一の構成については同一の符号を用いて、その説明を適宜省略する。

図 9 は、本実施形態に係るフィルタアドレス更新処理に係るフローチャートの一例を示す図である。ここで、本フローチャートに係るプログラム、及びプログラムの実行に必要なデータは、ROM 102、HDD 108 等に記憶されており、CPU 101 によって R

50

A M 1 0 3 に読み出されて実行される。

なお、フィルタアドレス更新処理は、第 1 の実施形態と同様に、図 6 の S 6 0 7 において呼び出される。

#### 【 0 0 3 9 】

まず、アドレス拡張制御部 2 0 3 は、ネットワークパケット送受信部 2 0 6 を利用して、D N S サーバ 3 0 3 に問い合わせを行う。この問合せにより、送信元のアドレスを保持する外部装置のホスト名を取得する ( S 9 0 1 )。本例では「1234:1::203:3ff:fe30:1」のホスト名を D N S サーバ 3 0 3 に問い合わせることになる。D N S サーバ 3 0 3 は、設定ファイル情報 5 0 1 の内容を参照して、対応するホスト名である「dev1」をネットワークデバイス 3 0 0 に返す。

10

続いて、アドレス拡張制御部 2 0 3 は、ネットワークパケット送受信部 2 0 6 を利用して、ホスト名「dev1」の I P v 6 アドレスを D N S サーバ 3 0 3 にクエリし、「dev1」の全ての I P v 6 アドレスを取得する ( S 9 0 2 )。本例では、「dev1」に対応する I P v 6 アドレスとして「1234:1::203:3ff:fe30:1」及び「1234:2::203:3ff:fe30:1」が取得される。そして、アドレス拡張制御部 2 0 3 は、「dev1」の全ての I P v 6 アドレスをフィルタアドレス登録部 2 0 2 に渡す。

#### 【 0 0 4 0 】

続いて、フィルタアドレス登録部 2 0 2 は、フィルタアドレス記憶部 2 0 4 の内容を更新する ( S 9 0 3 )。即ち、フィルタアドレス登録部 2 0 2 は、フィルタアドレス記憶部 2 0 4 に登録されているフィルタアドレスのうち、「fee0:1::203:3ff:fe30:1」を「1234:1::203:3ff:fe30:1」に書き換える。また、フィルタアドレス登録部 2 0 2 は、「fee0:2::203:3ff:fe30:1」を「1234:2::203:3ff:fe30:1」に書き換える。

20

続いて、フィルタアドレス登録部 2 0 2 は、書き換えたフィルタアドレス (書き換え前のフィルタアドレス) と同じプレフィックス番号を持つフィルタアドレスがフィルタアドレス記憶部 2 0 4 に存在するか否かを判断する ( S 9 0 4 )。このとき、存在すると判断した場合、S 9 0 5 に処理を移し、他方、存在しないと判断した場合、本フローチャートの処理を終了する。

#### 【 0 0 4 1 】

本例では、「fee0:1::203:3ff:fe30:1」のプレフィックス番号である「fee0:1」と同じプレフィックス番号を持つ「fee0:1::204:4ff:fe40:2」というフィルタアドレスが存在している。また、「fee0:2::203:3ff:fe30:1」のプレフィックス番号である「fee0:2」と同じプレフィックス番号を持つ「fee0:2::204:4ff:fe40:2」というフィルタアドレスが存在している。

30

ここで、同じプレフィックス番号を持つ外部装置に関しては、同様にアドレスが変更されていると判断することができる。

したがって、S 9 0 5 では、フィルタアドレス登録部 2 0 2 は、同じプレフィックス番号を持つフィルタアドレスが存在していると判断した場合、そのフィルタアドレスを、S 9 0 3 で更新したフィルタアドレスと同じプレフィックス番号で更新する。即ち、フィルタアドレス登録部 2 0 2 は、「fee0:1::204:4ff:fe40:2」を「1234:1::204:4ff:fe40:2」に書き換える。また、フィルタアドレス登録部 2 0 2 は、「fee0:2::204:4ff:fe40:2」を「1234:2::204:4ff:fe40:2」に書き換える。そして、フィルタアドレス登録部 2 0 2 は、本フローチャートの処理を終了する。

40

#### 【 0 0 4 2 】

以上、本実施形態では、アクセスパケットの送信元のアドレスを更新するタイミングで、その他にもアドレスが変更されている可能性のあるフィルタアドレスを探し、その情報も更新する。

この構成によれば、以降に当該アドレスを備えた外部装置からアクセスパケットを受信した際に、迅速に予め設定されているフィルタリング処理を行うことが可能となる。

#### 【 0 0 4 3 】

< 第 4 の実施形態 >

50

本実施形態では、第 2 の実施形態のフィルタアドレス更新処理において、フィルタアドレス記憶部 204 の中に他にもアドレスが変更されている可能性のあるフィルタアドレスが存在するかを更に判断する。そして、存在していた場合、そのフィルタアドレスも更新する。なお、本実施形態では、第 1 の実施形態及び第 2 の実施形態の構成と同一の構成については同一の符号を用いて、その説明を適宜省略する。

図 10 は、本実施形態に係るフィルタアドレス更新処理に係るフローチャートの一例を示す図である。ここで、本フローチャートに係るプログラム、及びプログラムの実行に必要なデータは、ROM 102、HDD 108 等に記憶されており、CPU 101 によって RAM 103 に読み出されて実行される。

なお、フィルタアドレス更新処理は、第 1 の実施形態と同様に、図 6 の S 607 において呼び出される。

#### 【0044】

まず、ネットワークフィルタ制御部 205 は、フィルタアドレス登録部 202 を利用して、送信元のアドレスをフィルタアドレス記憶部 204 に登録する (S 1001)。本例においては、「1234:1::203:3ff:fe30:1」が新たにフィルタアドレス記憶部 204 に登録されることとなる。そして、「1234:1::203:3ff:fe30:1」と同じインターフェース ID の「fe0:1::203:3ff:fe30:1」及び「fe0:2::203:3ff:fe30:1」がアドレス拡張制御部 203 に渡される。

続いて、アドレス拡張制御部 203 は、ネットワークパケット送受信部 206 を利用して、「fe0:1::203:3ff:fe30:1」及び「fe0:2::203:3ff:fe30:1」に対して存在確認パケットを送信する (S 1002)。存在確認パケットは、例えば、当該アドレスに対する ICMPv6 の近隣要請パケットである。そして、アドレス拡張制御部 203 は、存在確認パケットに対する存在応答パケットを受信するのを所定の期間待ち受ける。

#### 【0045】

続いて、アドレス拡張制御部 203 は、存在応答パケットを受信したか否かを判断する (S 1003)。存在応答パケットは、例えば、ICMPv6 の近隣広告パケットである。

このとき、アドレス拡張制御部 203 は、存在すると判断した場合、S 1005 に処理を移す。この場合、例えば、「1234:1::203:3ff:fe30:1」というアドレスは、外部装置に新たに追加された IPv6 アドレスであることになる。他方、アドレス拡張制御部 203 は、存在しないと判断した場合、即ち当該アドレスは既に使用されていないものと判断した場合、S 1004 に処理を移す。

S 1004 では、アドレス拡張制御部 203 は、フィルタアドレス登録部 202 を利用して、フィルタアドレス記憶部 204 から存在していないと判断したアドレスを削除する。

#### 【0046】

続いて、フィルタアドレス登録部 202 は、書き換えたフィルタアドレスと同じプレフィックス番号を持つフィルタアドレスがフィルタアドレス記憶部 204 に存在するか否かを判断する (S 1005)。このとき、フィルタアドレス登録部 202 は、存在すると判断した場合、S 1006 に処理を移し、他方、存在しないと判断した場合、本フローチャートの処理を終了する。

本例では、「fe0:1::203:3ff:fe30:1」のプレフィックス番号である「fe0:1」と同じプレフィックス番号を持つ「fe0:1::204:4ff:fe40:2」というフィルタアドレスが存在している。また、「fe0:2::203:3ff:fe30:1」のプレフィックス番号である「fe0:2」と同じプレフィックス番号を持つ「fe0:2::204:4ff:fe40:2」というフィルタアドレスが存在している。

#### 【0047】

ここで、同じプレフィックス番号を持つ外部装置に関しては、同様にアドレスが変更されている可能性があるとは判断することができる。

したがって、アドレス拡張制御部 203 は、同じプレフィックス番号を持つフィルタア

10

20

30

40

50

ドレスが存在した場合、それらに対しても存在確認を実行する。

続いて、アドレス拡張制御部 203 は、「fee0:1::204:4ff:fe40:2」及び「fee0:2::204:4ff:fe40:2」の変更後の候補アドレスと考えられるアドレスを生成する（S1006）。候補アドレス（候補アドレス情報の一例）は、これらアドレスのプレフィックス番号を、S1001で登録した送信元のアドレスのプレフィックス番号に置き換えることで生成される。即ち、本例においては、「1234:1::204:4ff:fe40:2」及び「1234:2::204:4ff:fe40:2」が候補アドレスとなる。

#### 【0048】

続いて、アドレス拡張制御部 203 は、ネットワークパケット送受信部 206 を利用して、上記候補アドレスに対して存在確認パケットを送信する（S1007）。そして、アドレス拡張制御部 203 は、存在確認パケットに対する存在応答パケットを受信するのを所定の期間待ち受ける。続いて、アドレス拡張制御部 203 は、存在応答パケットを受信したか否かを判断する（S1008）。このとき、アドレス拡張制御部 203 は、受信したと判断した場合、S1009に処理を移し、他方、受信していないと判断した場合、本フローチャートの処理を終了する。

S1009では、ネットワークフィルタ制御部 205 は、フィルタアドレス登録部 202 を利用して、上記候補アドレスをフィルタアドレス記憶部 204 に登録する。そして、フィルタアドレス登録部 202 は、フィルタアドレス記憶部 204 に登録されている既存のアドレスをアドレス拡張制御部 203 に渡す。本例では「fee0:1::204:4ff:fe40:2」及び「fee0:2::204:4ff:fe40:2」が渡ることとなる。

#### 【0049】

続いて、アドレス拡張制御部 203 は、ネットワークパケット送受信部 206 を利用して、上記既存のアドレスに対して存在確認パケットを送信する（S1010）。そして、アドレス拡張制御部 203 は、存在確認パケットに対する存在応答パケットを受信するのを所定の期間待ち受ける。

続いて、アドレス拡張制御部 203 は、存在応答パケットを受信したか否かを判断する（S1011）。このとき、アドレス拡張制御部 203 は、受信したと判断した場合、フィルタアドレス記憶部 204 の更新に係る処理は行わず、上記既存のアドレスは登録したままにし、本フローチャートの処理を終了する。他方、アドレス拡張制御部 203 は、受信しなかったと判断した場合、即ち、当該アドレスは既に使用されていないものと判断した場合、S1012に処理を移す。

S1012では、アドレス拡張制御部 203 は、フィルタアドレス登録部 202 を利用して、フィルタアドレス記憶部 204 から上記既存のアドレスを削除する。

#### 【0050】

以上、本実施形態によれば、DNSサーバが存在しないネットワーク環境下においても、アクセスパケットの送信元のアドレスを更新するタイミングで、その他にもアドレスが変更している可能性のあるフィルタアドレスを検出する。そして、疎なアドレスに対しても存在確認を行う。

この構成によれば、以降に当該アドレスを備えた外部装置からアクセスパケットを受信した際に、迅速に予め設定されているフィルタリング処理を行うことが可能となる。

#### 【0051】

<その他の実施形態>

図6において、S601で受信したアクセスパケットに予め設定されている処理を実施するタイミングは、フィルタアドレス更新処理を実施するタイミングよりも前であってもよい。この場合、フィルタアドレス更新処理に時間がかかり、アクセスパケットの送信元が長い時間応答を待たされる事態を回避することが可能となる。

また、本発明は、以下の処理を実行することによっても実現される。即ち、上述した実施形態の機能を実現するソフトウェア（プログラム）を、ネットワーク又は各種記憶媒体を介してシステム或いは装置に供給し、そのシステム或いは装置のコンピュータ（又はCPUやMPU等）がプログラムを読み出して実行する処理である。

## 【 0 0 5 2 】

上述した実施形態の構成によれば、外部装置からのパケットをより適切にフィルタリングすることができる。

## 【 0 0 5 3 】

以上、本発明の好ましい実施形態について詳述したが、本発明は係る特定の実施形態に限定されるものではなく、特許請求の範囲に記載された本発明の要旨の範囲内において、種々の変形・変更が可能である。

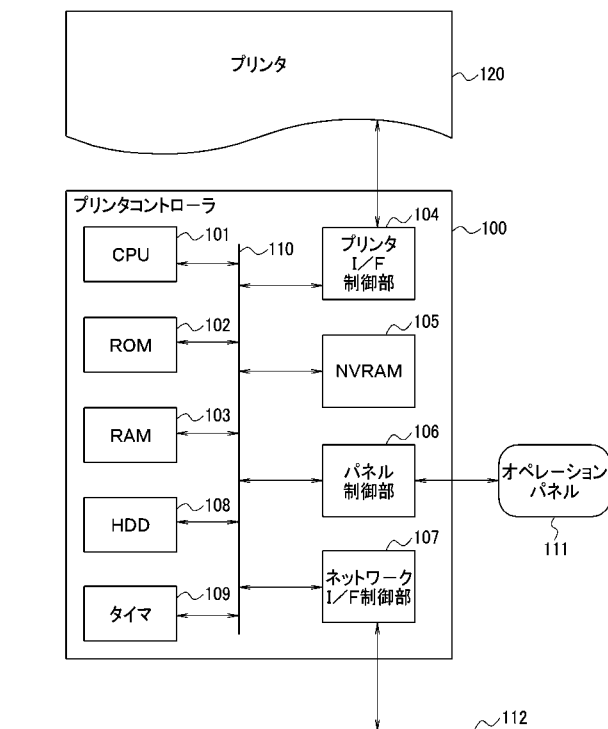
## 【 符号の説明 】

## 【 0 0 5 4 】

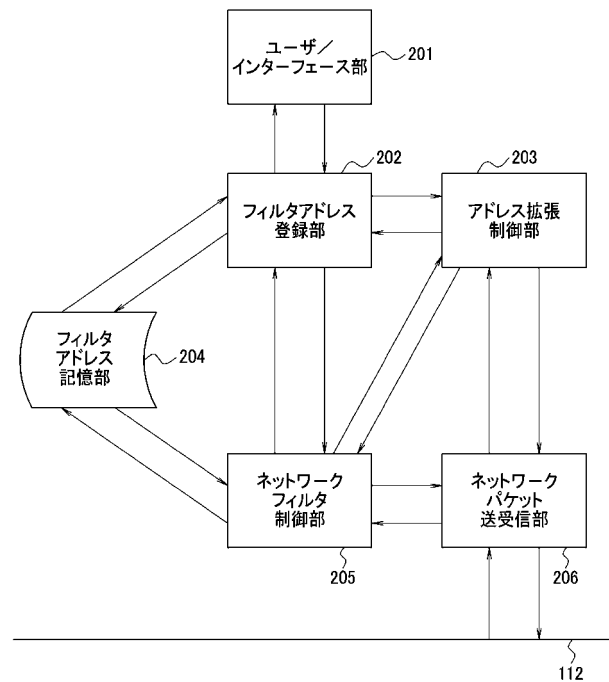
1 0 0 プリンタコントローラ、 1 2 0 プリンタ

10

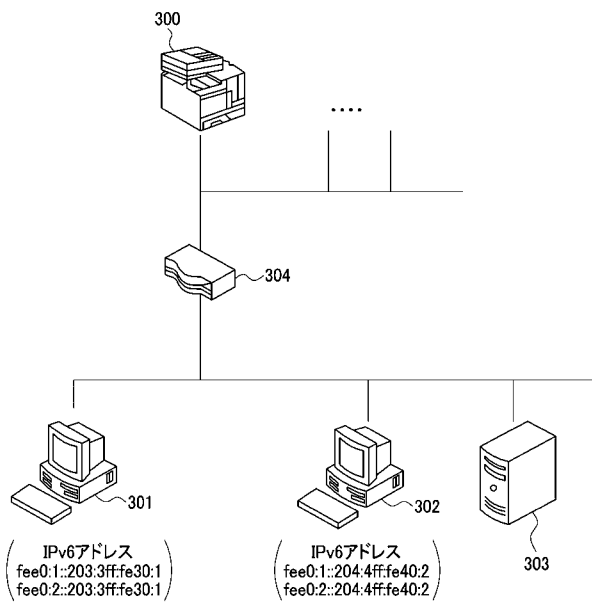
【 図 1 】



【 図 2 】



【図 3】



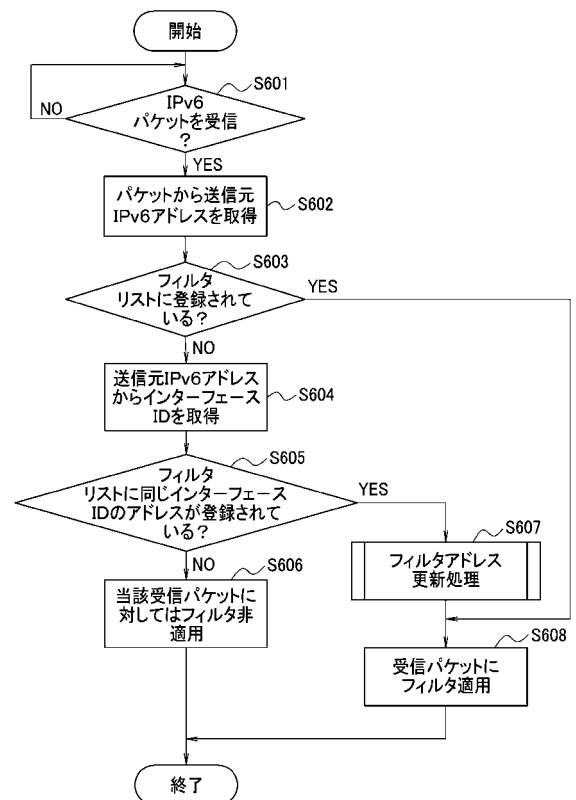
【図 4】



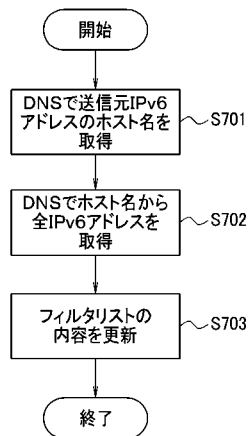
【図 5】

501				
net	IN	A	192.168.0.120	
net	IN	AAAA	ffe:2::201:1ff:fe10:1	
net	IN	AAAA	ffe:2::201:1ff:fe10:1	
dev1	IN	A	192.168.100.80	
dev1	IN	AAAA	fee0:1::203:3ff:fe30:1	
dev1	IN	AAAA	fee0:2::203:3ff:fe30:1	
dev2	IN	A	192.168.100.90	
dev2	IN	AAAA	fee0:1::204:4ff:fe40:2	
dev2	IN	AAAA	fee0:2::204:4ff:fe40:2	
dev3	IN	A	192.168.0.70	
dev3	IN	AAAA	ffe:2::201:1ff:fe10:5	
dev3	IN	AAAA	ffe:2::201:1ff:fe10:5	

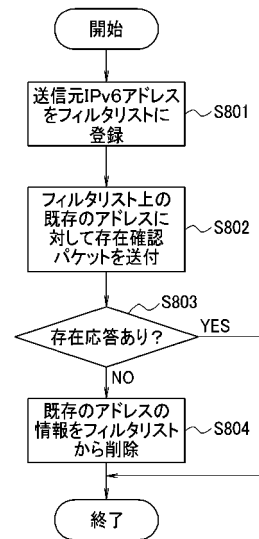
【図 6】



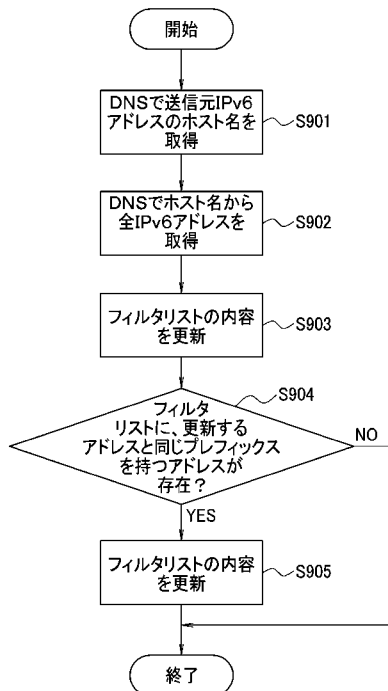
【 図 7 】



【 図 8 】



【 図 9 】



【 図 10 】

