(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4892469号
(P4892469)

(45)発行日　平成24年3月7日(2012.3.7)　(24)登録日　平成23年12月22日(2011.12.22)

(51)Int.Cl.		F I		
H04L 12/66	(2006.01)	H04L	12/66	B
B41J 29/38	(2006.01)	B41J	29/38	Z
G06F 3/12	(2006.01)	G06F	3/12	A
		G06F	3/12	K

請求項の数 13　(全 22 頁)

(21)出願番号　特願2007-328728 (P2007-328728)
(22)出願日　平成19年12月20日 (2007.12.20)
(65)公開番号　特開2009-152849 (P2009-152849A)
(43)公開日　平成21年7月9日 (2009.7.9)
審査請求日　平成22年12月14日 (2010.12.14)

(73)特許権者　000001007
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　100126240
弁理士　阿部　琢磨
(74)代理人　100124442
弁理士　黒岩　創吾
(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

審査官　衣鳩　文彦

最終頁に続く

(54)【発明の名称】通信装置及びその制御方法、プログラム

(57)【特許請求の範囲】
【請求項１】
ネットワークに接続するための第１の接続手段と、情報処理装置に接続するための第２の接続手段とを備えた通信装置であって、
前記第１の接続手段を介して前記ネットワークからデータを受信する受信手段と、
前記受信手段が受信したデータを処理する処理手段と、
前記通信装置との通信が拒否されている送信元を示す拒否情報を登録する拒否情報登録手段と、
前記受信手段が受信したデータの送信元を示す情報が前記拒否情報登録手段により登録されていない場合に、前記受信手段が受信したデータの送信元を示す情報を送信元情報として設定した確認データを前記第２の接続手段を介して前記情報処理装置に送信する送信手段と、
前記送信手段による前記確認データの送信が正常に行われた場合は、前記受信手段が受信したデータを前記処理手段により処理させ、前記送信手段による前記確認データの送信が正常に行われなかった場合は、前記受信手段が受信したデータを破棄する制御手段と、
を備えることを特徴とする通信装置。
【請求項２】
前記受信手段が受信したデータの送信元を示す情報が前記拒否情報登録手段により登録されている場合は、前記送信手段による前記確認データの送信を行うことなく、前記制御手段は、前記受信手段が受信したデータを破棄することを特徴とする請求項１に記載の通

信装置。
【請求項３】
前記送信手段による前記確認データの送信が正常に行われなかった場合に、前記拒否情報登録手段は、前記受信手段が受信したデータの送信元を示す情報を新たに登録することを特徴とする請求項１または２に記載の通信装置。
【請求項４】
ネットワークに接続するための第１の接続手段と、情報処理装置に接続するための第２の接続手段とを備えた通信装置であって、
前記第１の接続手段を介して前記ネットワークからデータを受信する受信手段と、
前記受信手段が受信したデータを処理する処理手段と、
前記通信装置との通信が許可されている送信元を示す許可情報を登録する許可情報登録手段と、
前記受信手段が受信したデータの送信元を示す情報が前記許可情報登録手段により登録されていない場合に、前記受信手段が受信したデータの送信元を示す情報を送信元情報として設定した確認データを前記第２の接続手段を介して前記情報処理装置に送信する送信手段と、
前記送信手段による前記確認データの送信が正常に行われた場合は、前記受信手段が受信したデータを前記処理手段により処理させ、前記送信手段による前記確認データの送信が正常に行われなかった場合は、前記受信手段が受信したデータを破棄する制御手段と、
を備えることを特徴とする通信装置。
【請求項５】
前記受信手段が受信したデータの送信元を示す情報が前記許可情報登録手段により登録されている場合は、前記送信手段による前記確認データの送信を行うことなく、前記制御手段は、前記受信手段が受信したデータを前記処理手段により処理させることを特徴とする請求項４に記載の通信装置。
【請求項６】
前記送信手段による前記確認データの送信が正常に行われた場合に、前記許可情報登録手段は、前記受信手段が受信したデータの送信元を示す情報を新たに登録することを特徴とする請求項４または５に記載の通信装置。
【請求項７】
ネットワークに接続するための第１の接続手段と、情報処理装置に接続するための第２の接続手段とを備えた通信装置であって、
前記第１の接続手段を介して前記ネットワークからデータを受信する受信手段と、
前記受信手段が受信したデータを処理する処理手段と、
前記通信装置との通信が拒否されている送信元を示す拒否情報を登録する拒否情報登録手段と、
前記通信装置との通信が許可されている送信元を示す許可情報を登録する許可情報登録手段と、
前記拒否情報登録手段および前記許可情報登録手段のいずれにも前記受信手段が受信したデータの送信元を示す情報が登録されていない場合に、前記受信手段が受信したデータの送信元を示す情報を送信元情報として設定した確認データを前記第２の接続手段を介して前記情報処理装置に送信する送信手段と、
前記送信手段による前記確認データの送信が正常に行われた場合は、前記受信手段が受信したデータを前記処理手段により処理させ、前記送信手段による前記確認データの送信が正常に行われなかった場合は、前記受信手段が受信したデータを破棄する制御手段と、
を備えることを特徴とする通信装置。
【請求項８】
前記送信手段が送信した確認データに対する正常応答が前記情報処理装置から返されてきた場合に、前記送信手段による前記確認データの送信が正常に行われたと判断し、前記確認データに対する正常応答が前記情報処理装置から返されてこなかった場合に、前記送

信手段による前記確認データの送信が正常に行われなかったと判断する判断手段を更に備えることを特徴とする請求項１から７のいずれか１項に記載の通信装置。
【請求項９】
前記受信手段が受信したデータの宛先が前記情報処理装置である場合は、当該受信したデータの送信元に関わらず当該受信したデータを前記情報処理装置に転送する転送手段を更に備えることを特徴とする請求項１から８のいずれか１項に記載の通信装置。
【請求項１０】
ネットワークに接続するための第１の接続手段と、情報処理装置に接続するための第２の接続手段とを備えた通信装置の制御方法であって、
前記第１の接続手段を介して前記ネットワークからデータを受信する受信工程と、
前記受信工程で受信したデータを処理する処理工程と、
前記通信装置との通信が拒否されている送信元を示す拒否情報を登録する拒否情報登録工程と、
前記受信工程で受信したデータの送信元を示す情報が前記拒否情報登録工程において登録されていない場合に、前記受信工程で受信したデータの送信元を示す情報を送信元情報として設定した確認データを前記第２の接続手段を介して前記情報処理装置に送信する送信工程と、
前記送信工程における前記確認データの送信が正常に行われた場合は、前記受信工程で受信したデータを前記処理工程で処理させ、前記送信工程における前記確認データの送信が正常に行われなかった場合は、前記受信工程で受信したデータを破棄する制御工程と、
を備えることを特徴とする通信装置の制御方法。
【請求項１１】
ネットワークに接続するための第１の接続手段と、情報処理装置に接続するための第２の接続手段とを備えた通信装置の制御方法であって、
前記第１の接続手段を介して前記ネットワークからデータを受信する受信工程と、
前記受信工程で受信したデータを処理する処理工程と、
前記通信装置との通信が許可されている送信元を示す許可情報を登録する許可情報登録工程と、
前記受信工程で受信したデータの送信元を示す情報が前記許可情報登録工程において登録されていない場合に、前記受信工程で受信したデータの送信元を示す情報を送信元情報として設定した確認データを前記第２の接続手段を介して前記情報処理装置に送信する送信工程と、
前記送信工程における前記確認データの送信が正常に行われた場合は、前記受信工程で受信したデータを前記処理工程で処理させ、前記送信工程における前記確認データの送信が正常に行われなかった場合は、前記受信工程で受信したデータを破棄する制御工程と、
を備えることを特徴とする通信装置の制御方法。
【請求項１２】
ネットワークに接続するための第１の接続手段と、情報処理装置に接続するための第２の接続手段とを備えた通信装置の制御方法であって、
前記第１の接続手段を介して前記ネットワークからデータを受信する受信工程と、
前記受信工程で受信したデータを処理する処理工程と、
前記通信装置との通信が拒否されている送信元を示す拒否情報を登録する拒否情報登録工程と、
前記通信装置との通信が許可されている送信元を示す許可情報を登録する許可情報登録工程と、
前記拒否情報登録工程および前記許可情報登録工程のいずれにおいても前記受信工程で受信したデータの送信元を示す情報が登録されていない場合に、前記受信工程で受信したデータの送信元を示す情報を送信元情報として設定した確認データを前記第２の接続手段を介して前記情報処理装置に送信する送信工程と、
前記送信工程における前記確認データの送信が正常に行われた場合は、前記受信工程で

受信したデータを前記処理工程で処理させ、前記送信工程における前記確認データの送信が正常に行われなかった場合は、前記受信工程で受信したデータを破棄する制御工程と、
を備えることを特徴とする通信装置の制御方法。
【請求項１３】
請求項１０から１２のいずれか１項に記載の通信装置の制御方法をコンピュータに実行させるためのプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ネットワーク及び情報処理装置に接続される通信装置及びその制御方法、プログラムに関するものである。
【背景技術】
【０００２】
ネットワーク環境においては、しばしば、異なる機能や能力を有する、種々のタイプの多数の印刷装置が存在していることがある。この場合、例えば、ネットワーク環境におけるいくつかのより新しい印刷装置はセキュア・プリンティング機能をサポートしているのに、より古い印刷装置はサポートしていないという状態が生じ得る。
【０００３】
この問題に対する解決方法として、インターフェイスを介して既存の印刷装置と接続可能な、既存の印刷装置のための所望の機能を追加可能なネットワークカードデバイスを用いることが考えられている。
【０００４】
例えば、特許文献１には、ＣＰＵを持ったインテリジェントなネットワークカードデバイスを印刷装置本体に接続して使用することが記載されている。また、通常、ネットワークカードデバイスは、ネットワーク経由での各種プリントサービスの統括制御を行うプリントサーバ機能を備えている。そして、印刷装置とネットワークカードデバイスはインターフェイスを介して通信し、所望のサービスを提供している。
【０００５】
ここで、上記のネットワークカードデバイスは、上記の印刷装置と同じネットワークアドレス（例えばＩＰアドレス）を使用することがある。この場合、上記のネットワークカードデバイスは、ネットワーク上から見た場合、印刷装置のフロントエンドに位置している。そして、ネットワーク上に存在する他の通信端末から見た場合、印刷装置とネットワークカードデバイスとがネットワーク上に存在するただ１つの通信端末として認識される。
【０００６】
これにより、ネットワークカードデバイス側に備えられたプリントサーバ機能などのサービスが、あたかも印刷装置本体に追加拡張されたサービスであるかのように振る舞うことを可能としている。更には、ネットワークカードデバイスが提供していない、元から印刷装置側に備えられた既存のサービスに関しては、ネットワークカードデバイスの存在に影響されること無く従来通りに機能することも可能としている。
【０００７】
また、これを実現するため、ネットワークカードデバイスには、ネットワーク上に存在する他の通信端末から通信パケットを受け取った際に、当該パケットが自身に備わるサービスに対するものであるかを判定する機能が備えられている。
【０００８】
ネットワークカードデバイスは、受信したパケットが自身に備わるサービスに対するものである場合には、当該パケットを自身で処理し、当該パケットに応じたサービスを実行する。一方、自身に備わるサービスに対するものでない場合は、インターフェイスを介して当該パケットを印刷装置に転送する。印刷装置は転送されたパケットに応じたサービスを実行するようにしている。

【０００９】
ところで、近年では印刷装置において通信のフィルタリング機能を備えたものが知られている。フィルタリング機能とは、予めネットワーク管理者等のユーザが印刷装置にフィルタリング情報を登録することにより、当該フィルタリング情報に合致する通信相手からの通信パケットを受信した際に、当該パケットを破棄する機能である。あるいは逆に、登録されたフィルタリング情報に合致する通信相手からの通信パケットのみを受け入れ、その他の相手からの通信パケットを破棄する機能である。なお、上記フィルタリング情報の設定は、印刷装置が備える操作パネルなどから行うことが可能である。
【００１０】
また、上記のフィルタリング情報としては、物理アドレスおよびネットワークアドレスのいずれかもしくは両方が使用されることが一般的である。より具体的には、ＴＣＰ／ＩＰプロトコルにおいては、物理アドレスとしてはＭＡＣ（Ｍｅｄｉａ　Ａｃｃｅｓｓ　Ｃｏｎｔｒｏｌ）アドレスが、ネットワークアドレスとしてはＩＰアドレスが、それぞれ用いられる。
【特許文献１】特開２００５－０３８０１１号公報
【特許文献２】特開２００５－３５４４１０号公報
【発明の開示】
【発明が解決しようとする課題】
【００１１】
ネットワーク上に存在する所定の通信端末に対して、上記フィルタリング機能を用いて、自身が備えるサービスへのアクセスを拒否している印刷装置に、上述したネットワークカードデバイスを装着したとする。その場合、ネットワークカードデバイスは上述の通り印刷装置よりもフロントエンドに位置しているため、ネットワークカードデバイス自身が備えるサービスに関しては、上記フィルタリング機能を適用することが出来ない。
【００１２】
従って、印刷装置が備えるサービスへのアクセスを拒否されている通信端末からであっても、ネットワークカードデバイスが備えるサービスに対してはアクセス出来てしまうという問題がある。
【００１３】
この問題への解決方法としては、まず第１に、ネットワークカードデバイス側にも印刷装置と同様なフィルタリング機能を持たせるという方法が考えられる。しかしながらこの場合、ユーザは印刷装置に対して行ったのと同様なフィルタリング情報の設定をネットワークカードデバイスに対して再度行わなければならなくなる。
【００１４】
そのため、ユーザは予め印刷装置側のフィルタリング情報を把握しておくか、印刷装置側のフィルタリング情報を参照しながらネットワークカードデバイス側にも同じ内容のフィルタリング情報を設定する必要がある。このような設定作業はユーザにとって煩雑であり、設定ミスも生じやすい。更には、ネットワークカードデバイス側にも印刷装置と同様に、操作パネルなどのフィルタリング情報を設定するための手段を設ける必要がある。
【００１５】
また、第２に、特許文献２に記載された方法も考え出されている。即ち、特許文献２によれば、バックエンドに位置するホストとフロントエンドに位置するルータとの間で予め定めた所定のマルチキャストアドレスを用いた通信を実施する。その通信の中で、ホストに設定されたフィルタリング情報をルータに通知し、ルータは当該フィルタリング情報を自身に設定する。
【００１６】
しかしながら、上記の方法を実現するためには、所定のマルチキャストアドレスを用いて自身のフィルタリング情報をルータに通知するという機能をホスト側が備えておく必要がある。そのため、当該機能を備えていないホストにルータを組み合わせて使用する場合は、やはり上記第１に述べた方法を用いて個別に設定を行わなくてはならない。

【００１７】
本発明は、上記の問題点に鑑みなされたものであり、ネットワークを介してデータを受信した場合に、情報処理装置に対して確認データを送信し、この確認データの送信の結果に応じて受信したデータを処理する通信装置及びその制御方法、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】
【００１８】
上記の目的を達成するために本願発明の通信装置は、ネットワークに接続するための第１の接続手段と、情報処理装置に接続するための第２の接続手段とを備えた通信装置であって、前記第１の接続手段を介して前記ネットワークからデータを受信する受信手段と、前記受信手段が受信したデータを処理する処理手段と、前記通信装置との通信が拒否されている送信元を示す拒否情報を登録する拒否情報登録手段と、前記受信手段が受信したデータの送信元を示す情報が前記拒否情報登録手段により登録されていない場合に、前記受信手段が受信したデータの送信元を示す情報を送信元情報として設定した確認データを前記第２の接続手段を介して前記情報処理装置に送信する送信手段と、前記送信手段による前記確認データの送信が正常に行われた場合は、前記受信手段が受信したデータを前記処理手段により処理させ、前記送信手段による前記確認データの送信が正常に行われなかった場合は、前記受信手段が受信したデータを破棄する制御手段とを備えることを特徴とする。
【００１９】
また、本願発明の通信装置は、ネットワークに接続するための第１の接続手段と、情報処理装置に接続するための第２の接続手段とを備えた通信装置であって、前記第１の接続手段を介して前記ネットワークからデータを受信する受信手段と、前記受信手段が受信したデータを処理する処理手段と、前記通信装置との通信が許可されている送信元を示す許可情報を登録する許可情報登録手段と、前記受信手段が受信したデータの送信元を示す情報が前記許可情報登録手段により登録されていない場合に、前記受信手段が受信したデータの送信元を示す情報を送信元情報として設定した確認データを前記第２の接続手段を介して前記情報処理装置に送信する送信手段と、前記送信手段による前記確認データの送信が正常に行われた場合は、前記受信手段が受信したデータを前記処理手段により処理させ、前記送信手段による前記確認データの送信が正常に行われなかった場合は、前記受信手段が受信したデータを破棄する制御手段とを備えることを特徴とする。
【００２０】
また、本願発明の通信装置は、ネットワークに接続するための第１の接続手段と、情報処理装置に接続するための第２の接続手段とを備えた通信装置であって、前記第１の接続手段を介して前記ネットワークからデータを受信する受信手段と、前記受信手段が受信したデータを処理する処理手段と、前記通信装置との通信が拒否されている送信元を示す拒否情報を登録する拒否情報登録手段と、前記通信装置との通信が許可されている送信元を示す許可情報を登録する許可情報登録手段と、前記拒否情報登録手段および前記許可情報登録手段のいずれにも前記受信手段が受信したデータの送信元を示す情報が登録されていない場合に、前記受信手段が受信したデータの送信元を示す情報を送信元情報として設定した確認データを前記第２の接続手段を介して前記情報処理装置に送信する送信手段と、前記送信手段による前記確認データの送信が正常に行われた場合は、前記受信手段が受信したデータを前記処理手段により処理させ、前記送信手段による前記確認データの送信が正常に行われなかった場合は、前記受信手段が受信したデータを破棄する制御手段とを備えることを特徴とする。
【発明の効果】
【００２１】
通信装置がネットワークを介してデータを受信した場合に、情報処理装置に対して確認データを送信し、この確認データの送信の結果に応じて受信したデータを処理することにより、通信装置においても容易にフィルタリング処理を行うことが可能となる。

【発明を実施するための最良の形態】
【００２２】
以下、図面を参照して本発明の実施の形態を詳しく説明する。尚、以下の実施の形態は特許請求の範囲に係る発明を限定するものでなく、また実施の形態で説明されている特徴の組み合わせの全てが発明の解決手段に必須のものとは限らない。
【００２３】
（第１の実施形態）
まず、本発明に係る第１の実施形態について説明する。
【００２４】
図１は、第１の実施形態に係る印刷装置（プリンタ）１００の構成を説明するブロック図である。プリンタ１００は、大きく分けて、ネットワークカードデバイス１５０とプリンタコントローラ１６０といった制御系を司る機器により構成されている。
【００２５】
ネットワークカードデバイス１５０はインテリジェント型ネットワークカードモジュールにより実現された、プリンタ１００に対して着脱可能なネットワーク装置である。プリンタコントローラ１６０は、プリンタ１００全体を制御する。
【００２６】
また、プリンタ１００は、プリンタコントローラ１６０に接続されたハードディスク等で構成される外部メモリ１０と、印刷を行うプリントエンジン１６と、操作パネル１８（操作部）とを備える。
【００２７】
ネットワークカードデバイス１５０は、ネットワークカードデバイス用のＣＰＵ１と、ＲＡＭ２と、書き換え可能なＲＯＭであるＦｌａｓｈＲＯＭ３とを備える。さらに、ネットワークカードデバイス１５０は、ネットワークコントローラ（ＬＡＮＣ）５と、ＬＥＤ６と、拡張インターフェイスコントローラ（ＥＸＰＣ）７と、これらを互いに接続するシステムバス４とを備える。
【００２８】
ＣＰＵ１は、ＦｌａｓｈＲＯＭ３に記憶された制御プログラムを読み出して各種制御処理を実行する。例えば、システムバス４に接続されるＬＡＮＣ５を介してローカルエリアネットワーク（ＬＡＮ）１８０に接続されたホストコンピュータ等の外部装置（不図示）と所定のネットワーク通信プロトコルを用いて通信する。これにより、外部装置から送られる印刷データやプリンタ制御命令等の各種データの送受信を統括的に制御し、ＥＸＰＣ７を介して接続されるプリンタコントローラ１６０に対して適切なデータ転送制御を行う。
【００２９】
ＲＡＭ２は、ＣＰＵ１の主メモリ、ワークエリア等の一時記憶領域として用いられる。ＬＥＤ６は、ネットワークカードデバイス１５０の動作状態を示す表示部として用いられている。ＬＥＤ６は、例えば、ＬＡＮＣ５とＬＡＮ１８０との電気的な接続状態（ＬＩＮＫ）やネットワーク通信モード（１０Ｂａｓｅや１００Ｂａｓｅ、全二重、半二重）等の各種動作状態をＬＥＤの色や点滅パターンで示すこと可能となっている。
【００３０】
ＥＸＰＣ７は、ネットワークカードデバイス１５０とプリンタコントローラ１６０を接続するためのインターフェイスであり、不図示のコネクタを含んで構成されている。ネットワークカードデバイス１５０は、このコネクタによってプリンタ１００（プリンタコントローラ１６０）との着脱が可能となっており、同じ構成を有する他のプリンタに当該ネットワークカードデバイス１５０を装着することが可能である。
【００３１】
一方、プリンタコントロータ１６０は、プリンタコントローラ用のＣＰＵ８と、ＲＯＭ９と、ラスタコントローラ１２とを備える。さらに、プリンタコントローラ１６０は、拡張インターフェイスコントローラ（ＥＸＰＣ）１３と、ＲＡＭ１４と、ディスクコントロ

ーラ（ＤＫＣ）１５と、これらを互いに接続するシステムバス１１とを備える。
【００３２】
ＣＰＵ８は、ＲＯＭ９に記憶された制御プログラム等或いはＤＫＣ１５を介して接続された外部メモリ１０に記憶された制御プログラムやリソースデータ（資源情報）等に基づいて、システムバス１１に接続される各種デバイスとのアクセスを統括的に制御する。
【００３３】
また、ＣＰＵ８は、ＥＸＰＣ１３を介してネットワークカードデバイス１５０から受信する印刷データを基にラスタコントローラ１２によって出力画像情報を生成し、プリントエンジン１６に対して画像信号を出力する。
【００３４】
ＲＡＭ１４は、ＣＰＵ８の主メモリ、ワークエリア等として機能する。また、ＲＡＭ１４は、図示しない増設ポートに接続されるオプションＲＡＭによりメモリ容量を拡張することができるように構成されている。
【００３５】
操作パネル１８には、プリンタ１００の動作モード等の設定や印刷データの取り消し等の操作を行うためのボタンと、プリンタ１００の動作状態を示す液晶パネルやＬＥＤ等の表示部とが配されている。
【００３６】
プリントエンジン１６は、既知の印刷技術を利用した画像形成処理部であり、例えば電子写真方式（レーザービーム方式）やインクジェット方式、昇華方（熱転写）方式等を採用可能である。
【００３７】
図２は、図１のネットワークカードデバイス１５０及びプリンタコントローラ１６０の制御プログラムのソフトウェア構成を示すブロック図である。図２に示す制御プログラムは、ネットワークカードデバイス１５０及びプリンタコントローラ１６０の各記憶部（例えば、ＦｌａｓｈＲＯＭ３やＲＯＭ９）に記憶され、上述したＣＰＵ１，８によってそれぞれ実行される。
【００３８】
ネットワークカードデバイス１５０側において、オペレーティングシステム（ＯＳ）２０１は、ネットワークカードデバイス１５０の基本的なデータの入出力制御を統括する。ＯＳ２０１は、拡張インターフェイスドライバ２０５と、ネットワークインターフェイスドライバ２０６と、パケット振り分け判定部２０７と、フィルタリング制御部２０８を内包している。
【００３９】
拡張インターフェイスドライバ２０５は、プリンタコントローラ１６０と拡張インターフェイス１７を介して通信制御を行う。ネットワークインターフェイスドライバ２０６はＬＡＮ１８０を介してホストコンピュータ等の外部装置（不図示）と通信を行う。
【００４０】
パケット振り分け判定部２０７は、ネットワークインターフェイスドライバ２０６がＬＡＮ１８０上から受け取った受信パケットが、自身の備えるアプリケーションプログラム２０２に対するものであるかを判定する。
【００４１】
具体的には、当該受信パケットのヘッダ情報を解析して、送信先ネットワークアドレスや送信先ポート番号などの送信先ネットワーク情報を取得する。次に、アプリケーションプログラム２０２が使用している通信ソケットのソケット情報を取得し、前記送信先ネットワーク情報と一致するソケットが存在するかどうか検索する。
【００４２】
存在した場合は、当該受信データはアプリケーションプログラム２０２宛てであると判断して、当該受信パケットをアプリケーションプログラム２０２に渡す。一方、一致するソケットが存在しない場合は、拡張インターフェイスドライバ２０５によって拡張インタ

ーフェイス１７を介して当受信該パケットをプリンタコントローラ１６０に転送する。
【００４３】
フィルタリング制御部２０８は、フィルタリング情報記憶部２０９の入出力制御を行い、外部装置からのアプリケーションプログラム２０２へのアクセスを制御する。
【００４４】
アプリケーションプログラム２０２は、ネットワークカードデバイス１５０内で動作するユーザアプリケーション２０３や登録アプリケーション２０４より構成される。ユーザアプリケーション２０３は例えばＪａｖａ（登録商標）言語によって記述され、ユーザが自由にインストール可能な、追加拡張性を備えたアプリケーションである。管理アプリケーション２０４はユーザアプリケーション２０３のインストール・アンインストールなどを行う役割を担うアプリケーションである。
【００４５】
プリンタコントローラ１６０側において、オペレーティングシステム（ＯＳ）２１１は、プリンタコントローラ１６０の各種処理制御を統括する。ＯＳ２１１は、拡張インターフェイスドライバ２１３と、プリントエンジン制御部２１４と、フィルタリング制御部２１５を内包している。
【００４６】
拡張インターフェイスドライバ２１３は、ネットワークカードデバイス１５０と拡張インターフェイス１７を介して通信制御を行う。プリントエンジン制御部２１４はプリントエンジン１６との通信制御を行う。フィルタリング制御部２１５は、フィルタリング情報記憶部２１６との入出力制御を行い、外部装置からのアプリケーションプログラム２１２へのアクセスを制御する。フィルタリング情報記憶部２１６へのフィルタリング情報の登録は、操作パネル１８から行うことが可能である。
【００４７】
アプリケーションプログラム２１２は、プリンタコントローラ１６０が備える印刷処理などの各種機能を実現するアプリケーションである。また、プリンタコントローラ１６０のネットワーク設定・フィルタリング設定などの各種機能設定を行う登録機能も内包している。
【００４８】
図３にネットワークカードデバイス１５０のフィルタリング情報記憶部２０９に記憶される許可リスト３００を示す。許可リスト３００は、ＩＰアドレス設定部３０１とＭＡＣアドレス設定部３０２とから構成されている。ＩＰアドレス設定部３０１及びＭＡＣアドレス設定部３０２には、アプリケーションプログラム２０２へのアクセスを許可する外部装置のＩＰアドレス及びＭＡＣアドレスが格納される。
【００４９】
図４にネットワークカードデバイス１５０のフィルタリング情報記憶部２０９に記憶される拒否リスト４００を示す。拒否リスト４００は、ＩＰアドレス設定部４０１とＭＡＣアドレス設定部４０２とから構成されている。ＩＰアドレス設定部４０１及びＭＡＣアドレス設定部４０２には、アプリケーションプログラム２０２へのアクセスを拒否する外部装置のＩＰアドレス及びＭＡＣアドレスが格納される。
【００５０】
次に、図５は本実施形態におけるネットワークシステム全体の構成を示す図である。ネットワークシステムは、プリンタ１００やパーソナル・コンピュータ（以下、ＰＣ）５００、５０１といった通信端末を有し、プリンタ１００、ＰＣ５００、ＰＣ５０１等がＬＡＮ１８０を介して互いに通信可能に接続されている。プリンタ１００にはネットワークカードデバイス１５０がすでに装着されており、ネットワークカードデバイス１５０とプリンタコントローラ１６０とから構成されている。
【００５１】
図５に示すネットワークシステムにおいては、説明を簡単にするために、ＬＡＮ１８０に接続された各通信端末（プリンタ１００、ＰＣ５００、５０１）は、ＴＣＰ／ＩＰプロ

トコルを用いて互いに通信を行うものとする。

【００５２】

また、本実施形態においては、図５に示すように、プリンタ１００にはＩＰアドレス：１９２．１６８．０．１００、ＭＡＣアドレス：ｆ０：１０：ｅ０：２０：ｄ０：３０が割り振られているものとする。同様に、ＰＣ５００にはＩＰアドレス：１９２．１６８．０．１０、ＭＡＣアドレス：００：０ａ：０ｂ：０ｃ：０ｄ：０ｅが割り振られているものとする。また、ＰＣ５０１にはＩＰアドレス：１９２．１６８．０．５０、ＭＡＣアドレス：００：０１：０２：０３：０４：０５が割り振られているものとする。

【００５３】

なお、プリンタ１００、ＰＣ５００、５０１等を接続するネットワークは、ＬＡＮ１８０に限定されるものではなく、任意の通信ネットワークを適用することが可能である。

【００５４】

更に、プリンタ１００に内包されたプリンタコントローラ１６０のフィルタリング情報記憶部２１６には、ネットワーク管理者などのユーザが操作パネル１８を介してフィルタリング情報を既に設定済みであるものとする。

【００５５】

ここでは、ＰＣ５００からプリンタ１００へのデータの送信は許可するが、ＰＣ５０１からプリンタ１００へのデータの送信は拒否することを示す情報がすでにフィルタリング情報記憶部２１６に記憶されているものとする。

【００５６】

図６は、図５に示したネットワークシステムにおいて、ネットワークカードデバイス１５０におけるフィルタリング処理にかかる一連の動作を示すフローチャートである。Ｓ６０１～Ｓ６０９は各処理ステップを示し、ネットワークカードデバイス１５０におけるフィルタリング処理の流れに対応する。なお、各ステップの制御手順に対応するプログラムはネットワークカードデバイス１５０のＦｌａｓｈＲＯＭ３に記憶されており、ＣＰＵ１がこれらを読み出して実行する。

【００５７】

ネットワークカードデバイス１５０は電源投入直後の起動処理で、許可リスト３００および拒否リスト４００の内容をクリアする（Ｓ５０１）。これにより、ネットワークカードデバイス１５０のフィルタリング情報記憶部２０９にはフィルタリング情報が何も登録されていない状態となる。

【００５８】

次に、ネットワークカードデバイス１５０はＳ６０２で、ネットワークインターフェイスドライバ２０６がＬＡＮ１８０上の任意の端末から通信パケットを受信するのを待ち受ける。

【００５９】

パケットを受信するとＳ６０３に進み、パケット振り分け判定部２０７において、当該受信パケットがアプリケーションプログラム２０２宛てであるかどうかを判定する。判定の結果、アプリケーションプログラム２０２宛てで無い場合は、Ｓ６０４において、拡張インターフェイス１７を介して当該受信パケットをプリンタコントローラ１６０に転送する。転送処理が終了すると、Ｓ６０２に戻り、再びＬＡＮ１８０上の任意の端末から通信パケットを受信するのを待ち受ける。

【００６０】

この後、プリンタコントローラ１６０はフィルタリング制御部２１５において、フィルタリング情報記憶部２１６を参照して、転送された受信パケットの処理方法を決定する。例えば、当該受信パケットの送信元がＰＣ５００であった場合は、当該受信パケットをアプリケーションプログラム２１２に渡す。あるいは、当該受信パケットの送信元がＰＣ５０１であった場合は、当該受信パケットをアプリケーションプログラム２１２に渡すことなく、直ちに破棄する。

【００６１】

一方、Ｓ６０３において、アプリケーションプログラム２０２宛てである場合はＳ６０５に進む。Ｓ６０５では、当該受信パケットの送信元が拒否リスト４００に登録されているかどうかを判定する。より詳細には、受信パケットのヘッダ情報を読み出して、送信元ＩＰアドレス及び送信元ＭＡＣアドレスを抽出する。次に、拒否リスト４００のＩＰアドレス設定部４０１およびＭＡＣアドレス設定部４０２を検索して、前記抽出した送信元ＩＰアドレス及び送信元ＭＡＣアドレスに合致する情報が登録されているかを判定する。

【００６２】

合致する情報が登録されている場合は、Ｓ６０６で当該受信パケットを破棄した後、Ｓ６０２に戻り、再びＬＡＮ１８０上の任意の端末から通信パケットを受信するのを待ち受ける。

【００６３】

合致する情報が登録されていない場合は、Ｓ６０７に進み、当該受信パケットの送信元が許可リスト３００に登録されているかどうかを判定する。より詳細には、許可リスト３００のＩＰアドレス設定部３０１およびＭＡＣアドレス設定部３０２を検索して、前記抽出した送信元ＩＰアドレス及び送信元ＭＡＣアドレスに合致する情報が登録されているかを判定する。

【００６４】

合致する情報が登録されている場合は、Ｓ６０８で当該受信パケットをアプリケーションプログラム２０２に渡した後、Ｓ６０２に戻り、再びＬＡＮ１８０上の任意の端末から通信パケットを受信するのを待ち受ける。合致しない場合は、Ｓ６０９に進み、フィルタリング新規判定処理を実施する。

【００６５】

なお、図６に示す例では、Ｓ６０５において受信パケットの送信元が拒否リスト４００に登録されているかどうかを判定した後で、Ｓ６０７において受信パケットの送信元が許可リスト３００に登録されているかどうかを判定しているが、以下の態様であってもよい。

【００６６】

即ち、Ｓ６０３において、受信パケットがアプリケーションプログラム２０２宛てであると判定された場合に、Ｓ６０５よりも先にＳ６０７に進み、当該受信パケットの送信元が許可リスト３００に登録されているかどうかを判定する。そして、この判定において、受信パケットの送信元が許可リスト３００に登録されている場合は、Ｓ６０８に進む。

【００６７】

一方、受信パケットの送信元が許可リスト３００に登録されていない場合は、Ｓ６０５に進み、受信パケットの送信元が拒否リスト４００に登録されているかどうかを判定する。そして、受信パケットの送信元が拒否リスト４００に登録されている場合は、Ｓ６０６に進み、登録されていない場合は、Ｓ６０９に進むようにしても構わない。

【００６８】

次に、図７は、ネットワークカードデバイス１５０におけるフィルタリング新規判定処理にかかる一連の動作を示すフローチャートである。Ｓ７０１～Ｓ７０７は各処理ステップを示し、ネットワークカードデバイス１５０におけるフィルタリング新規判定処理の流れに対応する。なお、各ステップに対応する制御手順に対応するプログラムはネットワークカードデバイス１５０のＦｌａｓｈＲＯＭ３に記憶されており、ＣＰＵ１がこれらを読み出して実行する。

【００６９】

まず始めに、ネットワークカードデバイス１５０は、フィルタリング確認パケットを生成する（Ｓ７０１）。このフィルタリング確認パケットは、プリンタコントローラ１６０が備える通信プロトコルのパケットであれば何でも良い。本実施形態では、フィルタリング確認パケットとして、ＩＣＭＰ（Ｉｎｔｅｒｎｅｔ Ｃｏｎｔｒｏｌ Ｍｅｓｓａｇｅ Ｐｒｏｔｏｃｏｌ）のＥＣＨＯパケットを用いることとする。

【００７０】

ＩＣＭＰのＥＣＨＯパケットを生成する際に、送信先ＩＰアドレスにはプリンタ１００のＩＰアドレス：１９２．１６８．０．１００が設定される。また、送信先ＭＡＣアドレスにはプリンタ１００のＭＡＣアドレス：ｆ０：１０：ｅ０：２０：ｄ０：３０が設定される。

【００７１】

更に、送信元ＩＰアドレス及び送信元ＭＡＣアドレスには、図６に示すフローチャートの中で抽出した受信パケットの送信元ＩＰアドレス及び送信元ＭＡＣアドレスが設定される。例えば、当該受信パケットがＰＣ５００から送信されたパケットである場合、前記フィルタリング確認パケットであるＩＣＭＰのＥＣＨＯパケットのヘッダ情報には、送信元情報として以下が格納される。送信元ＩＰアドレス：１９２．１６８．０．１０、送信元ＭＡＣアドレス：００：０ａ：０ｂ：０ｃ：０ｄ：０ｅ。あるいは、当該受信パケットがＰＣ５０１から送信されたパケットである場合、送信元ＩＰアドレス：１９２．１６８．０．５０、送信元ＭＡＣアドレス：００：０１：０２：０３：０４：０５が格納される。

【００７２】

次に、Ｓ７０２において、拡張インターフェイス１７を介して前記ＩＣＭＰのＥＣＨＯパケットをプリンタコントローラ１６０に転送する。

【００７３】

その後、プリンタコントローラ１６０に対して前記フィルタリング確認パケットが正常に送信できたかどうかを判定する（Ｓ７０３）。より詳細には、本実施形態においては、所定の期間内に前記ＩＣＭＰのＥＣＨＯパケットに対するＲＥＰＬＹパケットがプリンタコントローラ１６０から拡張インターフェイス１７を介して返信されるかどうかを判定する。

【００７４】

所定の期間内に前記ＩＣＭＰのＥＣＨＯパケットに対するＲＥＰＬＹパケットが返信されない場合は、Ｓ７０４に進み、当該受信パケットの送信元情報を拒否リスト４００に登録する。より詳細には、当該受信パケットの送信元ＩＰアドレスを拒否リスト４００のＩＰアドレス設定部４０１に、送信元ＭＡＣアドレスをＭＡＣアドレス設定部４０２にそれぞれ登録する。

【００７５】

次に、当該受信パケットを破棄した後（Ｓ７０５）、本フローチャートを終了する。

【００７６】

一方、Ｓ７０３において、所定の期間内にＲＥＰＬＹパケットが返信された場合は、Ｓ７０６に進み、当該受信パケットの送信元情報を許可リスト３００に登録する。より詳細には、当該受信パケットの送信元ＩＰアドレスを許可リスト３００のＩＰアドレス設定部３０１に、送信元ＭＡＣアドレスをＭＡＣアドレス設定部３０２にそれぞれ登録する。

【００７７】

次に、Ｓ７０７で、当該受信パケットをアプリケーションプログラム２０２に渡した後、本フローチャートを終了する。

【００７８】

以上が、図６のＳ６０９に示すフィルタリング新規判定処理の説明である。図６に示すフローチャートでは、Ｓ６０９において上記フィルタリング新規判定処理を行うと、次にＳ６０２に戻り、再びＬＡＮ１８０上の任意の端末から通信パケットを受信するのを待ち受ける。

【００７９】

以上、第１の実施形態によれば、ネットワークカードデバイス１５０は、受信したパケットが、自身が備えるアプリケーション宛てで無い場合は、当該パケットをプリンタコントローラ１６０に転送する。プリンタコントローラ１６０は当該受信パケットを、プリンタコントローラ１６０が備えるフィルタリング制御処理に基づいてフィルタリングする。

【００８０】

一方、ネットワークカードデバイス１５０は、自身が備えるアプリケーション宛てのパ

ケットを受信した場合に、当該パケットの送信元情報を格納した確認パケットを生成する。そして、当該確認パケットを用いてプリンタコントローラ１６０と通信可能であるかどうかを確かめることで、当該受信パケットを自身で処理して良いか、あるいは破棄すべきであるかを判定する。

【００８１】

これにより、ネットワークカードデバイス１５０においても、プリンタコントローラ１６０に設定されたフィルタリング情報と同様のフィルタリング処理を実行することが可能となる。更に、前記確認パケットはプリンタコントローラ１６０が標準で備えているＩＣＭＰプロトコルを用いているため、プリンタコントローラ１６０側では本実施形態のために何ら特別な対応は不要である。

【００８２】

（第２の実施形態）

次に、本発明に係る第２の実施形態について説明する。

【００８３】

第２の実施形態におけるハードウェア構成およびソフトウェア構成は、上述した第１の実施形態と相違は無いため、説明は省略する。また、第２の実施形態におけるネットワークシステムの構成についても、上述した第１の実施形態と相違は無いものとする。

【００８４】

図８は、第２の実施形態における、ネットワークカードデバイス１５０のフィルタリング処理にかかる一連の動作を示すフローチャートである。Ｓ８０１～Ｓ８０９は各処理ステップを示し、ネットワークカードデバイス１５０におけるフィルタリング処理の流れに対応する。なお、各ステップの制御手順に対応するプログラムはネットワークカードデバイス１５０のＦｌａｓｈＲＯＭ３に記憶されており、ＣＰＵ１がこれらを読み出して実行する。

【００８５】

ネットワークカードデバイス１５０は電源投入直後の起動処理で、許可リスト３００および拒否リスト４００の内容をクリアする（Ｓ８０１）。これにより、ネットワークカードデバイス１５０のフィルタリング情報記憶部２０９にはフィルタリング情報が何も登録されていない状態となる。

【００８６】

次に、ネットワークカードデバイス１５０はＳ８０２で、ネットワークインターフェイスドライバ２０６がＬＡＮ１８０上の任意の端末から通信パケットを受信するのを待ち受ける。

【００８７】

パケットを受信するとＳ８０３に進み、当該受信パケットの送信元が拒否リスト４００に登録されているかどうかを判定する。より詳細には、受信パケットのヘッダ情報を読み出して、送信元ＩＰアドレス及び送信元ＭＡＣアドレスを抽出する。次に、拒否リスト４００のＩＰアドレス設定部４０１およびＭＡＣアドレス設定部４０２を検索して、前記抽出した送信元ＩＰアドレス及び送信元ＭＡＣアドレスに合致する情報が登録されているかを判定する。

【００８８】

合致する情報が登録されている場合は、Ｓ８０４で当該受信パケットを破棄した後、Ｓ８０２に戻り、再びＬＡＮ１８０上の任意の端末から通信パケットを受信するのを待ち受ける。

【００８９】

合致する情報が登録されていない場合は、Ｓ８０５に進み、当該受信パケットの送信元が許可リスト３００に登録されているかどうかを判定する。より詳細には、許可リスト３００のＩＰアドレス設定部３０１およびＭＡＣアドレス設定部３０２を検索して、前記抽出した送信元ＩＰアドレス及び送信元ＭＡＣアドレスに合致する情報が登録されているかを判定する。

【００９０】
合致する情報が登録されている場合は、Ｓ８０６に進み、パケット振り分け判定部２０７において、当該受信パケットがアプリケーションプログラム２０２宛てであるかどうかを判定する。
【００９１】
判定の結果、アプリケーションプログラム２０２宛てである場合は、Ｓ８０７に進み、当該受信パケットをアプリケーションプログラム２０２に渡す。その後、Ｓ８０２に戻り、再びＬＡＮ１８０上の任意の端末から通信パケットを受信するのを待ち受ける。
【００９２】
Ｓ８０６において、アプリケーションプログラム２０２宛てで無い場合は、Ｓ８０８において拡張インターフェイス１７を介して当該受信パケットをプリンタコントローラ１６０に転送する。転送処理が終了すると、Ｓ６０２に戻り、再びＬＡＮ１８０上の任意の端末から通信パケットを受信するのを待ち受ける。
【００９３】
一方、Ｓ８０５の判定において、当該受信パケットの送信元が許可リスト３００に登録されていない場合は、Ｓ８０９に進み、フィルタリング新規判定処理を実施する。
【００９４】
なお、図８に示す例では、Ｓ８０３において受信パケットの送信元が拒否リスト４００に登録されているかどうかを判定した後で、Ｓ８０５において受信パケットの送信元が許可リスト３００に登録されているかどうかを判定しているが、以下の態様であってもよい。
【００９５】
即ち、Ｓ８０２において、パケットを受信した場合に、Ｓ８０３よりも先にＳ８０５に進み、当該受信パケットの送信元が許可リスト３００に登録されているかどうかを判定する。そして、この判定において、受信パケットの送信元が許可リスト３００に登録されている場合は、Ｓ８０６に進む。
【００９６】
一方、受信パケットの送信元が許可リスト３００に登録されていない場合は、Ｓ８０３に進み、受信パケットの送信元が拒否リスト４００に登録されているかどうかを判定する。そして、受信パケットの送信元が拒否リスト４００に登録されている場合は、Ｓ８０４に進み、登録されていない場合は、Ｓ８０９に進むようにしても構わない。
【００９７】
図９は、第２の実施形態におけるネットワークカードデバイス１５０におけるフィルタリング新規判定処理にかかる一連の動作を示すフローチャートである。Ｓ９０１～Ｓ９０９は各処理ステップを示し、ネットワークカードデバイス１５０におけるフィルタリング新規判定処理の流れに対応する。なお、各ステップに対応する制御手順に対応するプログラムはネットワークカードデバイス１５０のＦｌａｓｈＲＯＭ３に記憶されており、ＣＰＵ１がこれらを読み出して実行する。
【００９８】
まず始めに、ネットワークカードデバイス１５０は、フィルタリング確認パケットを生成する（Ｓ９０１）。このフィルタリング確認パケットは、プリンタコントローラ１６０が備える通信プロトコルのパケットであれば何でも良い。第２の実施形態においても、フィルタリング確認パケットとして、ＩＣＭＰのＥＣＨＯパケットを用いることとする。
【００９９】
第１の実施形態と同様に、ＩＣＭＰのＥＣＨＯパケットの送信先ＩＰアドレス及び送信先ＭＡＣアドレスにはプリンタ１００の情報が設定される。更に、送信元ＩＰアドレス及び送信元ＭＡＣアドレスには、図８に示すフローチャートの中で抽出した当該受信パケットの送信元ＩＰアドレス及び送信元ＭＡＣアドレスが設定される。
【０１００】
次に、Ｓ９０２において、拡張インターフェイス１７を介して前記ＩＣＭＰのＥＣＨＯ

パケットをプリンタコントローラ１６０に転送する。

【０１０１】

その後、プリンタコントローラ１６０に対して前記フィルタリング確認パケットが正常に送信できたかどうかを判定する（Ｓ９０３）。より詳細には、第２の実施形態においても、所定の期間内に前記ＩＣＭＰのＥＣＨＯパケットに対するＲＥＰＬＹパケットがプリンタコントローラ１６０から拡張インターフェイス１７を介して返信されるかどうかを判定する。

【０１０２】

所定の期間内に前記ＩＣＭＰのＥＣＨＯパケットに対するＲＥＰＬＹパケットが返信されない場合は、Ｓ９０４に進み、当該受信パケットの送信元情報を拒否リスト４００に登録する。より詳細には、当該受信パケットの送信元ＩＰアドレスを拒否リスト４００のＩＰアドレス設定部４０１に、送信元ＭＡＣアドレスをＭＡＣアドレス設定部４０２にそれぞれ登録する。

【０１０３】

次に、当該受信パケットを破棄した後（Ｓ９０５）、本フローチャートを終了する。

【０１０４】

一方、Ｓ９０３において、所定の期間内にＲＥＰＬＹパケットが返信された場合は、Ｓ９０６に進み、当該受信パケットの送信元情報を許可リスト３００に登録する。より詳細には、当該受信パケットの送信元ＩＰアドレスを許可リスト３００のＩＰアドレス設定部３０１に、送信元ＭＡＣアドレスをＭＡＣアドレス設定部３０２にそれぞれ登録する。

【０１０５】

次に、Ｓ９０７に進み、パケット振り分け判定部２０７において、当該受信パケットがアプリケーションプログラム２０２宛てであるかどうかを判定する。

【０１０６】

アプリケーションプログラム２０２宛てである場合は、Ｓ９０８に進み、当該受信パケットをアプリケーションプログラム２０２に渡した後、本フローチャートを終了する。

【０１０７】

一方、アプリケーションプログラム２０２宛てでない場合は、Ｓ９０９に進み、拡張インターフェイス１７を介して当該受信パケットをプリンタコントローラ１６０に転送した後、本フローチャートを終了する。

【０１０８】

以上が、図８のＳ８０９に示すフィルタリング新規判定処理の説明である。図８に示すフローチャートでは、Ｓ８０９において上記フィルタリング新規判定処理を行うと、次にＳ８０２に戻り、再びＬＡＮ１８０上の任意の端末から通信パケットを受信するのを待ち受ける。

【０１０９】

以上、第２の実施形態によれば、第１の実施形態の効果に加えて、以下に述べる効果も得ることが出来る。すなわち、第２の実施形態によれば、プリンタコントローラ１６０宛ての受信パケットに関しても、ネットワークカードデバイス１５０側でフィルタリングを行う。従って、プリンタコントローラ１６０に、通信拒否の設定を行っている端末からの通信パケットが転送されることが減少する。そのため、プリンタコントローラ１６０側では、不要な通信パケットによって処理負荷がかかってしまう事態を避けることが可能となる。

【０１１０】

（第３の実施形態）

次に、本発明に係る第３の実施形態について説明する。

【０１１１】

前述の第１の実施形態または第２の実施形態において使用される上記フィルタリング確認パケットは、ＩＣＭＰのＥＣＨＯパケットでなくても良い。プリンタコントローラ１６０が標準で備えている各種プロトコルを用いることが可能である。

【０１１２】
例えば、上記フィルタリング検査パケットはＨＴＴＰ（Ｈｙｐｅｒｔｅｘｔ Ｔｒａｎｓｆｅｒ Ｐｒｏｔｏｃｏｌ）やＦＴＰ（Ｆｉｌｅ Ｔｒａｎｓｆｅｒ Ｐｒｏｔｏｃｏｌ）のパケットであっても良い。
【０１１３】
例えば、ＨＴＴＰであれば、ネットワークカードデバイス１５０は、プリンタ１００を送信先、前記受信パケットの送信元を送信元として、プリンタコントローラ１６０のＨＴＴＰサーバとのセッション確立を試みる。
【０１１４】
セッションが確立されると、次に、ネットワークカードデバイス１５０は、ＨＴＴＰのＧｅｔメソッドをプリンタコントローラ１６０に送信する。
【０１１５】
上記Ｇｅｔメソッドに対するレスポンスをプリンタコントローラ１６０より受け取った場合には、上記受信パケットの送信元とは通信が許可されているものと判断する。
【０１１６】
一方、プリンタコントローラ１６０のＨＴＴＰサーバとのセッションが確立できない場合には、上記受信パケットの送信元は通信が拒否されているものと判断する。あるいは、セッションは確立できたがＧｅｔメソッドに対するレスポンスが来ない場合にも、上記受信パケットの送信元は通信が拒否されているものと判断する。
【０１１７】
同様に、ＦＴＰであれば、ネットワークカードデバイス１５０は、プリンタ１００を送信先、前記受信パケットの送信元を送信元として、プリンタコントローラ１６０のＦＴＰサーバとのセッション確立を試みる。
【０１１８】
プリンタコントローラ１６０よりセッション確立ＯＫ（ｃｏｎｎｅｃｔｉｏｎ ｅｓｔａｂｌｉｓｈｅｄ）のレスポンスが返された場合には、上記受信パケットの送信元とは通信が許可されているものと判断する。
【０１１９】
一方、プリンタコントローラ１６０よりセッション確立ＮＧ（ｃｏｎｎｅｃｔｉｏｎ ｒｅｑｕｅｓｔ ｒｅｊｅｃｔｅｄ）のレスポンスが返された場合には、上記受信パケットの送信元は通信が拒否されているものと判断する。
【０１２０】
なお、上述した第１乃至第３の実施形態において、ネットワークカードデバイス１５０は、プリンタ１００から物理的に切り離されて存在する別個の機器であっても良い。この場合、プリンタ１００は、内部にプリンタコントローラ１６０からなる制御系を司る制御部を備えている。
【０１２１】
ネットワークカードデバイス１５０において、図１に示すＥＸＰＣ７はシステムバス４に接続される第２のネットワークコントローラであっても良い。また、プリンタコントローラ１６０において、図１に示すＥＸＰＣ１３は、システムバス１１に接続される第２のネットワークコントローラであっても良い。この場合、拡張インターフェイス１７は、第２のローカルエリアネットワークである。更に、ネットワークカードデバイス１５０とプリンタコントローラ１６０とは、この第２のローカルエリアネットワークに共に接続されている。
【０１２２】
また、上述した第１乃至第３の実施形態におけるフィルタリング処理では、ＩＰアドレスとＭＡＣアドレスの両方を用いる例について説明したが、これらのうちいずれか一方のみを用いるようにしても構わない。また、各端末を識別することができる情報であれば、ＩＰアドレスやＭＡＣアドレス以外の情報であっても構わない。
【０１２３】

（その他の実施形態）

以上、実施形態例を詳述したが、本発明は、例えば、システム、装置、方法、プログラム若しくは記憶媒体（記録媒体）等としての実施態様をとることが可能である。具体的には、複数の機器から構成されるシステムに適用しても良いし、また、一つの機器からなる装置に適用しても良い。

【０１２４】

尚、本発明は、前述した実施形態の機能を実現するソフトウェアのプログラム（実施形態では図に示すフローチャートに対応したプログラム）を、システムあるいは装置に直接あるいは遠隔から供給する。そして、そのシステムあるいは装置のコンピュータが該供給されたプログラムコードを読み出して実行することによっても達成される場合を含む。

【０１２５】

従って、本発明の機能処理をコンピュータで実現するために、該コンピュータにインストールされるプログラムコード自体も本発明を実現するものである。つまり、本発明は、本発明の機能処理を実現するためのコンピュータプログラム自体も含まれる。

【０１２６】

その場合、プログラムの機能を有していれば、オブジェクトコード、インタプリタにより実行されるプログラム、ＯＳに供給するスクリプトデータ等の形態であっても良い。

【０１２７】

プログラムを供給するための記録媒体としては、例えば、以下のようなものがある。フロッピー（登録商標）ディスク、ハードディスク、光ディスク、光磁気ディスク、ＭＯ、ＣＤ－ＲＯＭ、ＣＤ－Ｒ、ＣＤ－ＲＷ、磁気テープ、不揮発性のメモリカード、ＲＯＭ、ＤＶＤ（ＤＶＤ－ＲＯＭ，ＤＶＤ－Ｒ）。

【０１２８】

その他、プログラムの供給方法としては、クライアントコンピュータのブラウザを用いてインターネットのホームページからハードディスク等の記録媒体にダウンロードすることによっても供給できる。すなわち、ホームページに接続し、該ホームページから本発明のコンピュータプログラムそのもの、もしくは圧縮され自動インストール機能を含むファイルをダウンロードする。また、本発明のプログラムを構成するプログラムコードを複数のファイルに分割し、それぞれのファイルを異なるホームページからダウンロードすることによっても実現可能である。つまり、本発明の機能処理をコンピュータで実現するためのプログラムファイルを複数のユーザに対してダウンロードさせるＷＷＷサーバも、本発明に含まれるものである。

【０１２９】

また、本発明のプログラムを暗号化してＣＤ－ＲＯＭ等のコンピュータ読み取り可能な記憶媒体に格納してユーザに配布する。そして、所定の条件をクリアしたユーザに対し、インターネットを介してホームページから暗号化を解く鍵情報をダウンロードさせる。そして、その鍵情報を使用することにより暗号化されたプログラムを実行してコンピュータにインストールさせて実現することも可能である。

【０１３０】

また、コンピュータが、読み出したプログラムを実行することによって、前述した実施形態の機能が実現される。その他にも、そのプログラムの指示に基づき、コンピュータ上で稼動しているＯＳなどが、実際の処理の一部または全部を行い、その処理によっても前述した実施形態の機能が実現され得る。

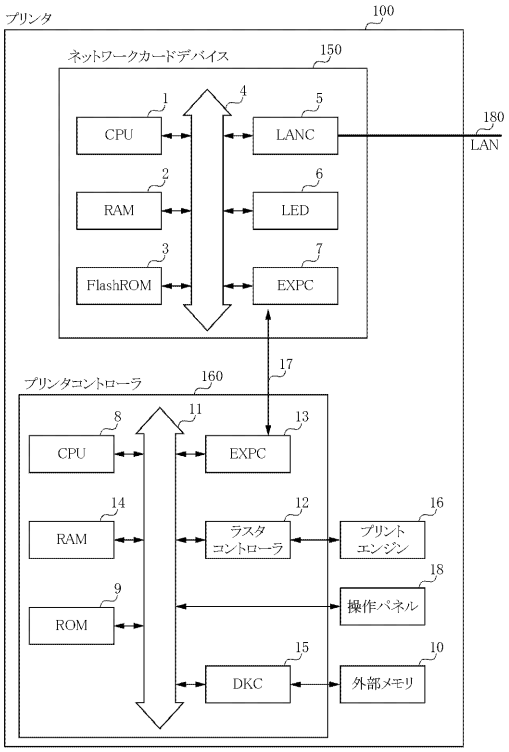
【０１３１】

さらに、記録媒体から読み出されたプログラムが、コンピュータに挿入された機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに書き込まれた後にも前述した実施形態の機能が実現される。すなわち、そのプログラムの指示に基づき、その機能拡張ボードや機能拡張ユニットに備わるＣＰＵなどが実際の処理の一部または全部を行うことによっても前述した実施形態の機能が実現される。

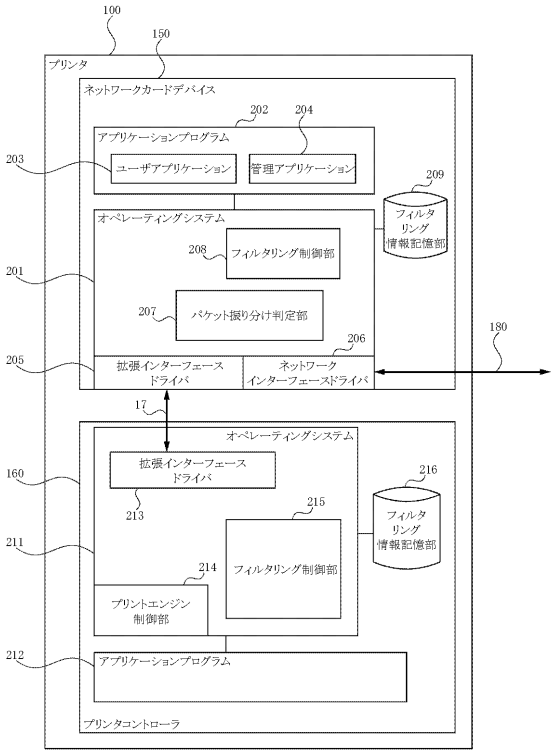
【図面の簡単な説明】

【０１３２】
【図１】本発明の実施形態におけるプリンタ１００及びネットワークカードデバイス１５０の構成を示すブロック図である。
【図２】本発明の実施形態におけるプリンタ１００及びネットワークカードデバイス１５０のソフトウェア構成図である。
【図３】本発明の実施形態における許可リスト３００を示す図である。
【図４】本発明の実施形態における拒否リスト４００を示す図である。
【図５】本発明の実施形態におけるシステム全体図である。
【図６】本発明の実施形態におけるフィルタリング処理の手順を示すフローチャートである。
【図７】本発明の実施形態におけるフィルタリング処理の手順を示すフローチャートである。
【図８】本発明の実施形態におけるフィルタリング処理の手順を示すフローチャートである。
【図９】本発明の実施形態におけるフィルタリング処理の手順を示すフローチャートである。
【符号の説明】
【０１３３】
１００　プリンタ
１５０　ネットワークカードデバイス
１６０　プリンタコントローラ
１８０　ＬＡＮ
１　ＣＰＵ
２　ＲＡＭ
３　Ｆｌａｓｈ　ＲＯＭ
４　システムバス
５　ＬＡＮＣ
６　ＬＥＤ
７　ＥＸＰＣ

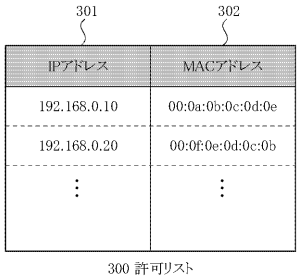
【図１】



【図２】



【図３】

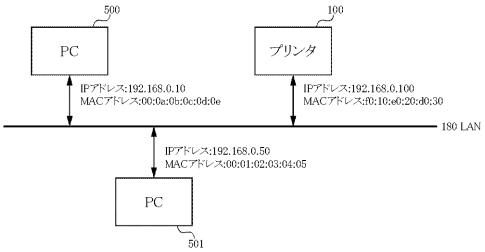


300 許可リスト

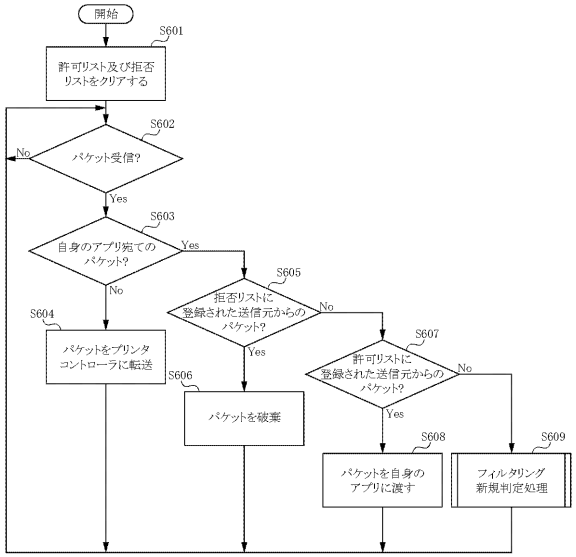
【図４】

400 拒否リスト

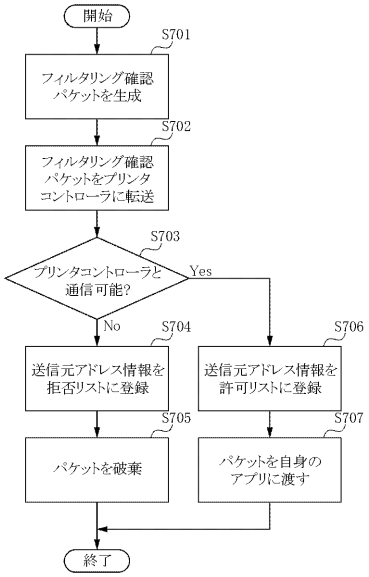
【図５】


500
PC
IPアドレス:192.168.0.10
MACアドレス:00:0a:0b:0c:0d:0e
100
プリンタ
IPアドレス:192.168.0.100
MACアドレス:f0:10:e0:20:d0:30
180 LAN
IPアドレス:192.168.0.50
MACアドレス:00:01:02:03:04:05
PC
501

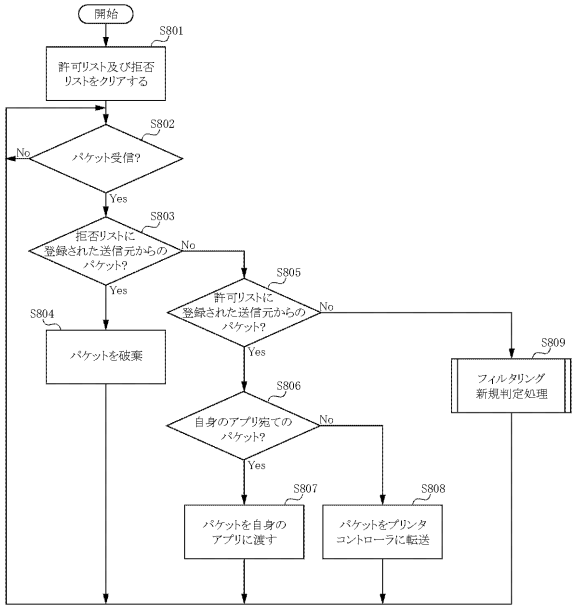
【図６】


開始
S601
許可リスト及び拒否リストをクリアする
S602
パケット受信?
No
Yes
S603
自身のアプリ宛てのパケット?
Yes
No
S605
拒否リストに登録された送信元からのパケット?
No
Yes
S604
パケットをプリンタコントローラに転送
S606
パケットを破棄
S607
許可リストに登録された送信元からのパケット?
No
Yes
S608
パケットを自身のアプリに渡す
S609
フィルタリング新規判定処理

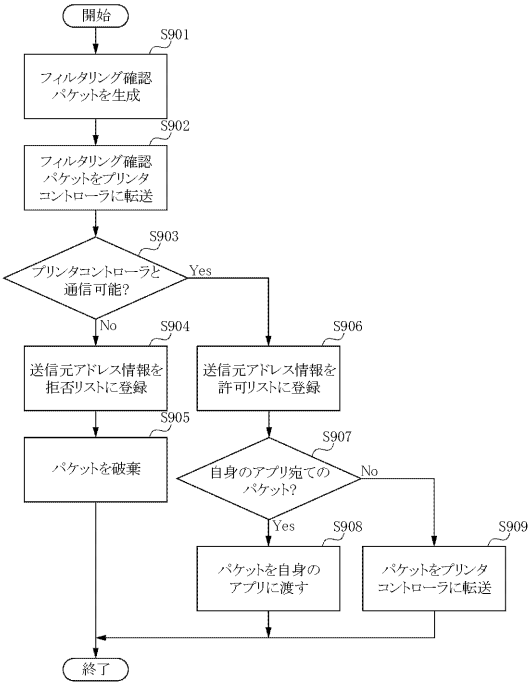
【図７】


開始
S701
フィルタリング確認パケットを生成
S702
フィルタリング確認パケットをプリンタコントローラに転送
S703
プリンタコントローラと通信可能?
Yes
No
S704
送信元アドレス情報を拒否リストに登録
S705
パケットを破棄
S706
送信元アドレス情報を許可リストに登録
S707
パケットを自身のアプリに渡す
終了

【図８】


開始
S801
許可リスト及び拒否リストをクリアする
S802
パケット受信?
No
Yes
S803
拒否リストに登録された送信元からのパケット?
No
Yes
S804
パケットを破棄
S805
許可リストに登録された送信元からのパケット?
No
Yes
S806
自身のアプリ宛てのパケット?
No
Yes
S807
パケットを自身のアプリに渡す
S808
パケットをプリンタコントローラに転送
S809
フィルタリング新規判定処理

【図９】


開始
S901
フィルタリング確認パケットを生成
S902
フィルタリング確認パケットをプリンタコントローラに転送
S903
プリンタコントローラと通信可能?
Yes
No
S904
送信元アドレス情報を拒否リストに登録
S905
パケットを破棄
S906
送信元アドレス情報を許可リストに登録
S907
自身のアプリ宛てのパケット?
No
Yes
S908
パケットを自身のアプリに渡す
S909
パケットをプリンタコントローラに転送
終了

フロントページの続き

(56)参考文献 特開２０００－２４２４５５（ＪＰ，Ａ）
特開２００５－１４９０８６（ＪＰ，Ａ）
特開２００３－２２９９１３（ＪＰ，Ａ）
特開２００３－３３３０６３（ＪＰ，Ａ）
特開２００８－１５４００９（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　１２／６６
Ｂ４１Ｊ　２９／３８
Ｇ０６Ｆ　３／１２