(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5475041号
(P5475041)
(45)発行日　平成26年4月16日(2014.4.16)　(24)登録日　平成26年2月14日(2014.2.14)

(51)Int.Cl.　F I
H04L 12/46 (2006.01)　H04L 12/46　E

請求項の数 22　(全 25 頁)

(21)出願番号　特願2012-60195(P2012-60195)
(22)出願日　平成24年3月16日(2012.3.16)
(65)公開番号　特開2012-195943(P2012-195943A)
(43)公開日　平成24年10月11日(2012.10.11)
審査請求日　平成24年3月16日(2012.3.16)
(31)優先権主張番号　61/453,290
(32)優先日　平成23年3月16日(2011.3.16)
(33)優先権主張国　米国(US)

(73)特許権者　510294195
サムソン　エスディーエス　カンパニー　リミテッド
大韓民国　ソウル　カンナム－ク　ヨクサム－２ドン　７０７－１９　イロック　ビルディング
(74)代理人　100117787
弁理士　勝沼　宏仁
(74)代理人　100107582
弁理士　関根　毅
(74)代理人　100146123
弁理士　木本　大介

最終頁に続く

(54)【発明の名称】システムオンチップ基盤のパケットフィルタリングを提供できるデバイス及びパケットフィルタリング方法

(57)【特許請求の範囲】
【請求項１】
ファイアウォールエンジンを備えたチップと、ドライバと、プロセス別にパケットの送受信を許容又は遮断することを定義したプロセス別ルールデータベース（ＤＢ）を保存する保存部とを有するデバイスであって、
前記ドライバは、送信するパケットに含まれた、任意のパケットに対して当該パケットを外部と送受信するのに使用されるオーナープロセスのオーナープロセスＩＤを獲得し、前記プロセス別ルールＤＢを参照して、前記オーナープロセスＩＤを有したプロセスが外部にパケットを送信することが許容されたものであるかどうかを判断することによって送信するパケットのオーナープロセスを確認し、前記オーナープロセスが外部にパケットを送信することが許容された場合にのみ、前記チップにパケットを送信し、
前記チップは、前記ドライバから受信したパケットに対してパケットフィルタリングのためのルールを適用してフィルタリング動作を行うことを特徴とするデバイス。
【請求項２】
前記ドライバは、また、前記送信するパケットのオーナープロセスが外部にパケットを送信することが許容されない場合には、前記パケットを前記チップに送信しないことを特徴とする請求項１に記載のデバイス。
【請求項３】
前記ドライバは、また、前記送信するパケットのオーナープロセスが外部にパケットを送信することが許容されない場合には、前記オーナープロセスの実行を中断させることを

特徴とする請求項２記載のデバイス。
【請求項４】
前記チップは、ネットワークインタフェースカードをさらに備え、前記ネットワークインタフェースカードを介して受信されたパケットに対して前記ルールを適用して前記パケットを前記ドライバに送信するか、又は送信しないことを特徴とする請求項１に記載のデバイス。
【請求項５】
前記ドライバは、また、前記チップから送信されたパケットのオーナープロセスを確認した後、前記チップから受信したパケットのオーナープロセスが外部からパケットを受信することが許容された場合にのみ、前記パケットを前記オーナープロセスに提供することを特徴とする請求項４に記載のデバイス。
【請求項６】
ＩＰ、プロトコル、及びポートのうち、少なくとも何れか一つの情報をユーザから受け取ることができる領域を含んだルール設定画面を提供するファイアウォールユーザインタフェースをさらに備え、
前記ファイアウォールユーザインタフェースは、前記ルール設定画面を介してユーザから受け取ったルールを前記チップに送信し、前記チップは、前記ファイアウォールユーザインタフェースから送信されたルールを利用してパケットフィルタリング動作を行うことを特徴とする請求項１に記載のデバイス。
【請求項７】
前記ルール設定画面は、コンフィギュレーションヘルパーを備え、
前記コンフィギュレーションヘルパーは、ネットワークアプリケーションに対するリストを提供し、このリストに含まれたネットワークアプリケーションのうち、少なくとも何れか一つのネットワークアプリケーションがユーザにより選択されると、選択されたネットワークアプリケーションが実行するのに必要なＩＰ、プロトコル、及びポートのうち、少なくとも何れか一つを前記領域に自動的に入力することを特徴とする請求項６に記載のデバイス。
【請求項８】
前記ルール設定画面は、
プログラム別にパケットを許容又は遮断することを定義したプロセス別ルールを入力できる領域を備えることを特徴とする請求項６に記載のデバイス。
【請求項９】
システムオンチップが装着され、ネットワークプロセスを備えたデバイスでのパケットフィルタリング方法であって、
前記デバイスは、プロセス別にパケットの送受信を許容又は遮断することを定義したプロセス別ルールＤＢを保存し、
前記デバイスは、前記パケットに含まれた、任意のパケットに対して当該パケットを外部と送受信するのに使用されるオーナープロセスのオーナープロセスＩＤを獲得し、前記プロセス別ルールＤＢを参照して、前記オーナープロセスＩＤを有したプロセスが外部にパケットを送信することが許容されたかどうかを判断することによってオーナープロセスを確認し、送信が許容された場合にのみ前記パケットを前記システムオンチップに送信するステップと、
前記システムオンチップは、前記デバイスから受け取ったパケットに対して、パケットフィルタリングのためのルールを適用してパケットフィルタリング動作を行うステップと
を含むことを特徴とするパケットフィルタリング方法。
【請求項１０】
前記デバイスは、また、前記送信するパケットのオーナープロセスが外部にパケットを送信することが許容されない場合には、前記パケットを前記システムオンチップに送信しないことを特徴とする請求項９に記載のパケットフィルタリング方法。
【請求項１１】

前記デバイスは、また、前記送信するパケットのオーナープロセスが外部にパケットを送信することが許容されない場合には、前記オーナープロセスの実行を中断させることを特徴とする請求項１０に記載のパケットフィルタリング方法。

【請求項１２】

前記システムオンチップは、ネットワークインタフェースカードをさらに備え、前記ネットワークインタフェースカードを介して受信されたパケットに対して前記ルールを適用してパケットフィルタリング動作を行うことを特徴とする請求項９に記載のパケットフィルタリング方法。

【請求項１３】

前記デバイスは、また、前記システムオンチップから受信したパケットのオーナープロセスを確認した後、前記システムオンチップから受信したパケットのオーナープロセスが外部からパケットを受信することが許容された場合にのみ、前記パケットを前記オーナープロセスに提供することを特徴とする請求項１２に記載のパケットフィルタリング方法。

【請求項１４】

前記デバイスは、ＩＰ、プロトコル、及びポートのうち、少なくとも何れか一つの情報をユーザから受け取ることができる領域を含んだルール設定画面を提供するステップと、

前記デバイスは、前記ルール設定画面を介してユーザから受け取ったルールを前記システムオンチップに送信し、前記システムオンチップは、前記デバイスから受信したルールを利用してパケットフィルタリング動作を行うステップと

をさらに含むことを特徴とする請求項９に記載のパケットフィルタリング方法。

【請求項１５】

前記ルール設定画面は、コンフィギュレーションヘルパーを含み、

前記コンフィギュレーションヘルパーは、ネットワークアプリケーションに対するリストを提供し、このリストに含まれたネットワークアプリケーションのうち、少なくとも何れか一つのネットワークアプリケーションがユーザにより選択されると、選択されたネットワークアプリケーションが実行するのに必要なＩＰ、プロトコル、及びポートのうち少なくとも何れか一つを前記領域に自動的に入力することを特徴とする請求項１４に記載のパケットフィルタリング方法。

【請求項１６】

前記ルール設定画面は、

プログラム別にパケットの送信又は受信を許容又は遮断することを定義したプロセス別ルールを入力できる領域を備えることを特徴とする請求項１５に記載のパケットフィルタリング方法。

【請求項１７】

任意のパケットに対して当該パケットを外部と送受信するのに使用されるオーナープロセスを有するパケットから、コンピュータの外部に送信するパケットに対するオーナープロセスＩＤを獲得し、プロセス別ルールＤＢを参照して、前記オーナープロセスＩＤを有したプロセスが外部にパケットを送信することが許容されたかどうかを判断するステップと、

前記送信するパケットの前記オーナープロセスが外部にパケットを送信することが許容された場合にのみ、前記送信するパケットを、パケットフィルタリング機能を有し、前記コンピュータに接続されたチップに送信するステップと

を含む方法を行うプログラムが記録されたコンピュータで読み取り可能な記録媒体。

【請求項１８】

ファイアウォールエンジンを備えたチップと、ドライバを備えたデバイスであって、

前記ドライバは、任意のパケットに対して当該パケットを外部と送受信するのに使用されるオーナープロセスを有するパケットから、外部に送信するパケットに対するオーナープロセスＩＤを獲得し、前記送信するパケットとそのオーナープロセスＩＤとを前記チップに送信し、

前記チップに備えられたファイアウォールエンジンは、プロセス別ルールＤＢを参照し

て、前記オーナープロセスＩＤを有したプロセスが外部にパケットを送信することが許容されたかどうかを判断し、このプロセスが外部にパケットを送信することが許容された場合に前記ファイアウォールエンジンは、パケットフィルタリングのためのルールＤＢを利用して前記送信するパケットに対してフィルタリング動作を行うことを特徴とするデバイス。

【請求項１９】

ネットワークインタフェースカードをさらに備え、

前記ドライバは、また、前記ネットワークインタフェースカードを介して受信したパケットに対してオーナープロセスＩＤを獲得し、このオーナープロセスＩＤと前記受信したパケットとを前記チップに送信することを特徴とする請求項１８に記載のデバイス。

【請求項２０】

前記ルールＤＢは、プロセス別にパケットの送受信を許容又は遮断することを定義したプロセス別ルールを備えることを特徴とする請求項１８に記載のデバイス。

【請求項２１】

任意のパケットに対して当該パケットを外部と送受信するのに使用されるオーナープロセスを有するパケットから、コンピュータの外部に送信するパケットに対するオーナープロセスＩＤを獲得するステップと、

前記外部に送信するパケットとそのオーナープロセスＩＤを、パケットフィルタリング機能を有し、コンピュータに装着されたて前記コンピュータに装着されたチップに送信するステップと

プロセス別ルールＤＢを参照して、前記オーナープロセスＩＤを有したプロセスが外部にパケットを送信することが許容されたかどうかを判断するステップと、

を含む方法を行うプログラムが記録されたコンピュータで読み取り可能な記録媒体。

【請求項２２】

前記ネットワークインタフェースカードを介して受信したパケットに対してオーナープロセスＩＤを獲得し、このオーナープロセスＩＤと前記受信したパケットを前記チップに送信するステップをさらに含むことを特徴とする請求項２１に記載のプログラムが記録されたコンピュータで読み取り可能な記録媒体。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、システムオンチップ基盤のパケットフィルタリングを提供できるデバイス及びパケットフィルタリング方法に関し、さらに詳細には、ネットワークアプリケーションのプロセス別にファイアウォールの設定を許容又は遮断に設定できるシステムオンチップ基盤のパケットフィルタリングを提供できるデバイス及びパケットフィルタリング方法に関する。

【背景技術】

【０００２】

インターネットが広範囲に使用されるにつれて、ウォームやトロイの木馬、ウイルス、ＤＤｏＳなどのような多様な形態の悪性マルウェアが登場しその被害も大きくなりつつある。そのため、ネットワーク上の情報を保護するためのネットワーク侵害対応方法及びその他の関連装置が必需となった。

【０００３】

特に、モバイル機器の場合は、使用可能なリソースが制限されているため、リソースを最小限使用しながら高速でパケットをフィルタリングできる高速フィルタリング技術が必ず必要であるはずである。

【発明の概要】

【発明が解決しようとする課題】

【０００４】

本発明の一実施形態によれば、ネットワークアプリケーションのプロセス別にファイア

ウォールの設定を許容又は遮断することによって、このプロセスが生成するすべてのパケットに対して許容又は遮断を設定できるデバイス及びパケットフィルタリング方法を提供することを目的とする。

【０００５】

本発明の一実施形態によれば、パケットフィルタリングのためのルール設定時にコンフィギュレーションヘルパーを提供することによって、ユーザの望むサービスに対してファイアウォールの設定作業をより容易に行うことができるデバイス及びパケットフィルタリング方法を提供することを目的とする。

【課題を解決するための手段】

【０００６】

本発明の一実施形態によれば、ファイアウォールエンジンを備えたチップと、ドライバと、プロセス別にパケットの送受信を許容又は遮断することを定義したプロセス別ルールデータベース（ＤＢ）を保存する保存部とを有するデバイスであって、前記ドライバは、送信するパケットに含まれた、任意のパケットに対して当該パケットを外部と送受信するのに使用されるオーナープロセスのオーナープロセスＩＤを獲得し、前記プロセス別ルールＤＢを参照して、前記オーナープロセスＩＤを有したプロセスが外部にパケットを送信することが許容されたものであるかどうかを判断することによって送信するパケットのオーナープロセスを確認し、前記オーナープロセスが外部にパケットを送信することが許容された場合にのみ、前記チップにパケットを送信し、前記チップは、前記ドライバから受信したパケットに対してパケットフィルタリングのためのルールを適用してフィルタリング動作を行うことを特徴とするデバイスが提供される。

【０００７】

本発明の他の一実施形態によれば、システムオンチップが装着され、ネットワークプロセスを備えたデバイスでのパケットフィルタリング方法であって、　前記デバイスは、プロセス別にパケットの送受信を許容又は遮断することを定義したプロセス別ルールＤＢを保存し、　前記デバイスは、前記パケットに含まれた、任意のパケットに対して当該パケットを外部と送受信するのに使用されるオーナープロセスのオーナープロセスＩＤを獲得し、前記プロセス別ルールＤＢを参照して、前記オーナープロセスＩＤを有したプロセスが外部にパケットを送信することが許容されたかどうかを判断することによってオーナープロセスを確認し、送信が許容された場合にのみ前記パケットを前記システムオンチップに送信するステップと、前記システムオンチップは、前記デバイスから受け取ったパケットに対して、パケットフィルタリングのためのルールを適用してパケットフィルタリング動作を行うステップと、を含むことを特徴とするパケットフィルタリング方法が提供される。

【０００８】

本発明のさらに他の一実施形態によれば、任意のパケットに対して当該パケットを外部と送受信するのに使用されるオーナープロセスを有するパケットから、コンピュータの外部に送信するパケットに対するオーナープロセスＩＤを獲得し、プロセス別ルールＤＢを参照して、前記オーナープロセスＩＤを有したプロセスが外部にパケットを送信することが許容されたかどうかを判断するステップと、前記送信するパケットのオーナープロセスが外部にパケットを送信することが許容された場合にのみ、前記送信するパケットを、パケットフィルタリング機能を有し、前記コンピュータに接続されたチップに送信するステップと、を含む方法を行うプログラムが記録されたコンピュータで読み取り可能な記録媒体が提供される。

【０００９】

本発明のさらに他の一実施形態によれば、ファイアウォールエンジンを備えたチップと、ドライバを備えたデバイスであって、前記ドライバは、任意のパケットに対して当該パケットを外部と送受信するのに使用されるオーナープロセスを有するパケットから、外部に送信するパケットに対するオーナープロセスＩＤを獲得し、前記送信するパケットとそのオーナープロセスＩＤとを前記チップに送信し、前記チップに備えられたファイアウォ

ールエンジンは、プロセス別ルールＤＢを参照して、前記オーナープロセスＩＤを有したプロセスが外部にパケットを送信することが許容されたかどうかを判断し、このプロセスが外部にパケットを送信することが許容された場合に前記ファイアウォールエンジンは、パケットフィルタリングのためのルールＤＢを利用して前記送信するパケットに対してフィルタリング動作を行うことを特徴とするデバイスが提供される。

【００１０】

本発明のさらに他の一実施形態によれば、任意のパケットに対して当該パケットを外部と送受信するのに使用されるオーナープロセスを有するパケットから、コンピュータの外部に送信するパケットに対するオーナープロセスＩＤを獲得するステップと、前記外部に送信するパケットとそのオーナープロセスＩＤを、パケットフィルタリング機能を有し、コンピュータに装着されたて前記コンピュータに装着されたチップに送信するステップと、プロセス別ルールＤＢを参照して、前記オーナープロセスＩＤを有したプロセスが外部にパケットを送信することが許容されたかどうかを判断するステップと、を含む方法を行うプログラムが記録されたコンピュータで読み取り可能な記録媒体が提供される。

【発明の効果】

【００１１】

本発明の一つ以上の実施形態によれば、ネットワークアプリケーションのプロセス別にファイアウォールの設定を許容又は遮断することによって、このプロセスが生成するすべてのパケットに対して許容又は遮断を設定できる。

【００１２】

本発明の一つ以上の実施形態によれば、パケットフィルタリングのためのルール設定時にコンフィギュレーションヘルパーを提供することによって、ユーザの望むサービスに対してファイアウォールの設定作業をより容易に行うことができる。

【図面の簡単な説明】

【００１３】

【図１】本発明の例示的な一実施形態に係るシステムオンチップが装着されるデバイスを説明するための図である。

【図２】本発明の例示的な実施形態に係るシステムオンチップが装着されるデバイスを説明するための図である。

【図３Ａ】図２のデバイスにおける本発明の例示的な実施形態に係るパケットフィルタリング方法を説明するためのフローチャートである。

【図３Ｂ】図２のデバイスにおける本発明の例示的な実施形態に係るパケットフィルタリング方法を説明するためのフローチャートである。

【図４】本発明の他の例示的実施形態に係るシステムオンチップが装着されるデバイスを説明するための図である。

【図５】本発明の例示的な実施形態に係るファイアウォールインタフェースが提供するルール設定画面を説明するための図である。

【図６】本発明の例示的な実施形態に係るコンフィギュレーションヘルパーの機能を説明するための図である。

【図７】本発明の例示的な実施形態に係る基本ルールを設定できるルール設定画面を説明するための図である。

【図８】本発明の例示的な実施形態に係るプロセス別ルールを設定できるルール設定画面を説明するための図である。

【図９】本発明の他の例示的実施形態に係るシステムオンチップが装着されるデバイスを説明するための図である。

【図１０】図９のデバイスにおける本発明の例示的な実施形態に係るパケットフィルタリング方法を説明するためのフローチャートである。

【図１１】本発明の他の例示的実施形態に係るシステムオンチップが装着されるデバイスを説明するための図である。

【図１２】図１１のデバイスにおける本発明の例示的な実施形態に係るパケットフィルタ

リング方法を説明するためのフローチャートである。
【図１３】本発明の他の例示的実施形態に係るシステムオンチップが装着されるデバイスを説明するための図である。
【発明を実施するための形態】
【００１４】
以上の本発明の目的、他の目的、特徴及び利点は、添付された図面と関連した以下の好ましい実施形態により容易に理解されるはずである。しかしながら、本発明は、ここで説明される実施形態に限定されず、他の形態で具体化されてもよい。むしろ、ここで紹介される実施形態は、開示された内容が徹底かつ完全になるように、そして当業者に、本発明の思想を十分に理解してもらうために提供されるものである。本明細書において、ある構成要素が他の構成要素上にあると言及される場合には、それは、他の構成要素上に直接形成される場合もあり、それらの間に第３の構成要素が介在される場合もあることを意味する。
【００１５】
また、あるエレメント（または構成要素）が他のエレメント（または構成要素）上で動作または実行されると言及されるとき、そのエレメント（または構成要素）は、他のエレメント（または構成要素）が動作または実行される環境で動作または実行されるか、または他のエレメント（または構成要素）と直接または間接的に相互作用により動作または実行されると理解されなければならない。
【００１６】
あるエレメント、構成要素、装置、またはシステムが、プログラム若しくはソフトウェアからなる構成要素を含むと言及される場合には、明示的な言及がなくても、そのエレメント、構成要素、装置、またはシステムは、そのプログラム若しくはソフトウェアが実行または動作するのに必要なハードウェア（例えば、メモリ、ＣＰＵ（Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）等）や他のプログラムまたはソフトウェア（例えば、オペレーティングシステム（ＯＳ）やハードウェアを駆動するのに必要なドライバ等）を含むと理解されなければならない。
【００１７】
また、あるエレメント（または構成要素）が具現化されるに当たって、特別な言及がない限り、そのエレメント（または構成要素）は、ソフトウェア、ハードウェア、またはソフトウェア及びハードウェアのうち、如何なる形態によっても具現化可能であると理解されなければならない。
【００１８】
本明細書で使用された用語は、実施形態を説明するためのものであって、本発明を限定するものではない。本明細書において、単数形は、特に言及しない限り、複数形も含む。明細書で使用される「含む」と言及された構成要素は、一つ以上の他の構成要素の存在又は追加を排除しない。
【００１９】
以下、図面を参照して本発明を詳細に説明する。以下の特定の実施形態を述べるにおいて、様々に特定された内容は、発明をさらに具体的に説明し、理解を助けるために作成された。しかしながら、本発明を理解することができる程度のこの分野における知識を有した読者は、このような様々に特定された内容がなくても、本発明が実施可能であることを認知できる。ある場合には、周知で発明と大きく関連のない技術的内容は、本発明を説明するにあたって、特別な理由なしでも、読者の混乱を引き起こさないようにあえて述べないこともあることを予め言及しておく。
【００２０】
図１は、本発明の例示的な一実施形態に係るシステムオンチップが装着されるデバイスを説明するための図である。
【００２１】
図１に示すように、本発明の例示的な実施形態に係るデバイス１には、パケットをフィ

ルタリングするファイアウォール機能付きシステムオンチップ（Ｓｙｓｔｅｍ　Ｏｎ　Ｃｈｉｐ）３が装着されうる。

【００２２】

デバイス１は、ネットワークを介して送受信するパケットを利用する一つ以上のネットワークアプリケーションを含むことができ、各々のアプリケーションは、一つ以上のプロセスを含むことができる。本発明の目的のために、任意のパケットに対して、このパケットを外部に送信したり又は外部から受信して使用するプロセスをそのパケットの「オーナープロセス（ｏｗｎｅｒ　ｐｒｏｃｅｓｓ）」と呼ぶことにする。一実施形態においてプロセスには、各々ＩＤが付与されているから互いに識別可能であり、各パケットには、該当パケットを使用するオーナープロセスのプロセスＩＤが含まれている。したがって、各パケットを使用するオーナープロセスは、各々のパケットに含まれたプロセスＩＤによって識別されうる。

【００２３】

一実施形態でシステムオンチップ３がネットワークインタフェースカード（ＮＩＣ）を備えることができ、これによりデバイス１は、システムオンチップ３を介してパケットを外部に送信し、システムオンチップ３を介してパケットを外部から受信することができる。

【００２４】

システムオンチップ３は、パケットの遮断又は許容の基準になるルール（ｒｕｌｅ）を保存する保存部、及び前記ルールを適用してパケットの送受信を遮断又は許容するファイアウォールエンジンを備えることができる。この構成において、システムオンチップ３がデバイス１からパケットを受信すると、システムオンチップ３に保存されたルールデータベース（ＤＢ）を適用して、パケットを外部に送信又は遮断する。また、システムオンチップ３は、外部からパケットを受信すると、前記ルールＤＢを適用してパケットをデバイス１に送信又は遮断できる。

【００２５】

一方、デバイス１が外部にパケットを送信する際には、例えば以下のように動作できる。

【００２６】

システムオンチップ３がネットワークインタフェースカード（ＮＩＣ）を備え、デバイス１が外部とパケットを送受信する際に前記ＮＩＣを介して通信すると仮定する場合、デバイス１は、送信するパケットのオーナープロセスを確認し、送信するパケットのオーナープロセスが外部にパケットを送信することが許容された場合のみに該当パケットをシステムオンチップ３に送信する。

【００２７】

システムオンチップ３は、予め定義されたルールをルールＤＢに保存し、前記ルールを適用して外部にパケットを送信することを許容又は遮断する。システムオンチップ３は、このためにハードウェア的及び／又はソフトウェア的に構成されたファイアウォールエンジンを備えることができる。

【００２８】

デバイス１は、プロセス別にパケットの送受信を許容又は遮断することを定義したプロセス別ルールＤＢを備えることができる。また、デバイス１は、外部に送信されるパケットに含まれたオーナープロセスのプロセスＩＤを獲得し、プロセス別ルールＤＢを参照して、オーナープロセスが外部にパケットを送信することが許容されたかどうかをを判断し、許容された場合にのみ該当パケットをシステムオンチップ３に送信する。

【００２９】

また、デバイス１は、外部に送信するパケットに対してプロセス別ルールを適用した結果、送信するパケットのオーナープロセスが外部にパケットを送信することが許容されない場合には、該当パケットをシステムオンチップ３に送信しない。

【００３０】

追加的機能として、デバイス１は、外部に送信するパケットのオーナープロセスが外部にパケットを送信することが許容されない場合には、該当パケットのオーナープロセスの実行を中断させることができる。

【００３１】

デバイス１が外部からパケットを受信するときには、例えば次の通りに動作できる。

【００３２】

システムオンチップ３がＮＩＣを備えており、外部からパケットが前記ＮＩＣを介して受信される場合、システムオンチップ３は、外部から受信したパケットに対してシステムオンチップ３内のルールＤＢを適用してパケットを通過させるか又は遮断するかを決定する。

【００３３】

システムオンチップ３は、ルールを適用した結果、前記パケットを通過させることと決定した場合にのみ、該当パケットをデバイス１に送信する。

【００３４】

一実施形態においてデバイス１は、プロセス別にパケットの送受信を許容又は遮断することを定義したプロセス別ルールＤＢを備えている。これにより、デバイス１がシステムオンチップ３から受信したパケットをオーナープロセスに送信する前に、受信したパケットに対してプロセス別ルールを適用できる。

【００３５】

プロセス別ルールを適用した結果、システムオンチップ３から受信したパケットのオーナープロセスが受信の禁止されたプロセスに該当する場合、該当パケットをオーナープロセスに提供せずに捨てる（ｄｉｓｃａｒｄ）。一実施形態において、デバイス１は、捨てたパケットに対するオーナープロセスの動作を中断させうる。

【００３６】

一方、デバイス１は、ユーザからルールを設定されうるルール設定画面を提供できる。ここで、ルール設定画面は、ＩＰ、プロトコル、及びポートのうち、少なくとも何れか一つの情報をユーザから受け取ることができる領域を含むことができる。ルール設定画面については後述する。

【００３７】

デバイス１は、ルール設定画面を介してユーザから受け取ったルールをシステムオンチップ３に送信し、システムオンチップ３は、デバイス１から送信されたルールを自身３の保存部に保存されたルールＤＢに反映できる。

【００３８】

デバイス１は、ユーザから入力されたルールのうち、プロセス別ルールは、システムオンチップ３に送信せずに、デバイス１自身が保存部（図示せず）に保存させうる。以後、デバイス１は、デバイス１自身の保存部（図示せず）に保存されたプロセス別ルールを使用して、プロセス別にパケットを遮断又は許容することができる。

【００３９】

図１には示していないが、システムオンチップ３は、中央処理装置（ＣＰＵ）、メモリ、メモリコントローラ、及びルールＤＢ保存部を有したハードウェア及び／ソフトウェアリソースを備えることができる。本発明の説明において、プログラムが駆動されるために必要なリソース（例えば、中央処理装置、メモリ、メモリコントローラ、ルールＤＢ保存部）に対して明示的に言及されなくても、プログラムが駆動されるために必要なハードウェア及びソフトウェア資源及びその動作は、内在されると理解しなければならない。例えば、システムオンチップ３に備えられたファイアウォールエンジンは、ルールＤＢとパケットとを互いにマッチングさせるマッチャー（ｍａｔｃｈｅｒ）と、このマッチャーを動作させるファームウェアを備えるように構成されうるが、このような場合、明示的言及がなくてもそういうファームウェアを保存する保存部、及びファームウェアをメモリにロードさせる中央処理装置は、システムオンチップ３に内蔵されると理解しなければならない。

【００４０】
このような類似の方式で本願明細書において、デバイス１があるアプリケーションやドライバを備えるように構成されると述べられた場合には、そういうアプリケーションとドライバとを動作させるためのハードウェア及び／又はソフトウェアリソースを当然に備えると理解しなければならない。
【００４１】
デバイス１は、スマートフォンやＰＤＡのようなモバイル機器でありうるが、これは、例示に過ぎず、デスクトップパソコンのように固定型デバイスであっても良い。
【００４２】
図２は、本発明の例示的な実施形態に係るシステムオンチップが装着されるデバイスを説明するための図である。図２の実施形態は、ファイアウォールシステムオンチップ（ＳｏＣ）の基盤により具現化されて、デバイス２００に装着された例である。
【００４３】
図２に示すように、デバイス２００は、機能的にアプリケーション層、カーネル層、ＳｏＣ層、及びＮＩＣ層に区分されうる。実施形態によって前記機能層の一部が省略されえ、他の機能層が追加されえ、また各機能層の細部構成要素も変更されうることはもちろんである。したがって、図２の構成は、一実施形態に過ぎないので、本発明的概念を図２に限定してはならず、以下では、図２の実施形態に基づいて本発明的概念を例示する。
【００４４】
図２に示すように、アプリケーション層は、アプリケーション２０３を備えることができる。アプリケーション層は、デバイス２００の最上位機能層に該当し、パケットフィルタリングの対象になるパケットデータを使用するアプリケーション２０３を備える。例えば、アプリケーション２０３は、ウェブブラウザ２０３－１、テレネット２０３－２、ＦＴＰサーバ２０３－３のうち、少なくとも一つになりえ、その他にも所定のパケットデータを使用する任意のアプリケーションのうちの何れか一つでありうる。
【００４５】
図示の一実施形態でデバイス２００のカーネル層は、デバイス２００が外部から受信したパケットデータ内の情報をアプリケーション層に伝達したりアプリケーション層の要請によってパケットデータを生成して外部に送信する役割をすることができる。
【００４６】
図示の一実施形態のように、データの送信のためにＴＣＰ／ＩＰプロトコルを使用してパケットデータを送受信する場合、デバイス２００は、ＴＣＰ／ＩＰプロトコルドライバ２１５を備える。また、デバイス２００がオペレーティングシステム（ＯＳ）としてウィンドウ（ＷＩＮＤＯＷＳ）を使用する場合にＷｉｎＳｏｃｋ２１３を備える。ＴＣＰ／ＩＰプロトコルドライバ２１５とＷｉｎＳｏｃｋ２１３の動作は、従来より周知のものであるから、これらの動作については説明しない。
【００４７】
デバイス２００がＴＣＰ／ＩＰプロトコルでない他のプロトコルを利用する場合であると、その他のプロトコルの使用のためのドライバを備えることができ、またデバイス２００がウィンドウズオペレーティングシステムでない他のオペレーティングシステムを使用する場合には、ＷｉｎＳｏｃｋ２１３でない他の構成要素を備えうることはもちろんである。
【００４８】
図示の実施形態におけるカーネル層は、ネットワークドライバインタフェース仕様（Ｎｅｔｗｏｒｋ Ｄｒｉｖｅｒ Ｉｎｔｅｒｆａｃｅ Ｓｐｅｃｉｆｉｃａｔｉｏｎ：ＮＤＩＳ）２１８をさらに備え、ＮＤＩＳ２１８には、アンチマルウェアＳｏＣミニポートドライバ２１７（以下、ミニポートドライバとする）を備えることができる。
【００４９】
ミニポートドライバ２１７は、アプリケーション２０３からパケットデータを受信してＡＰドライバ２２１に送信するか、ＡＰドライバ２２１からパケットデータを受信して上

位階層に送信する。

【００５０】

本発明の一実施形態に係るミニポートドライバ２１７は、また、パケットデータをＡＰドライバ２２１に送信する前に、プロセス別にフィルタリングする動作を行うことができる。ユーザの設定したルールのうち、プロセス別に設定されたルールがある場合に、その該当ルールは、カーネルが管理する領域に保存される。図示の実施形態において前記プロセス別ルールは、ルールＤＢ２１９に保存されうる。ここで、ルールＤＢ２１９は、前記プロセス別ルールＤＢのみを保存することもでき、パケットをフィルタリングする際に用いられるルールをさらに備えうる。ミニポートドライバ２１７は、アプリケーション２０３からパケットデータを受信すると、オーナープロセスを把握した後にプロセス別ルールと比較してパケットを通過させるかどうかを判断する。前記動作については、図３を参照して後述する。

【００５１】

図２の実施形態において、デバイス２００に装着されるシステムオンチップ（ＳｏＣ）は、ＡＰドライバ２２１、ファイアウォールエンジン２２９、ＮＩＣドライバ２２８、及びＮＩＣ２３１を備える。

【００５２】

ＡＰドライバ２２１は、ミニポートドライバ２１７からデータを受信してファイアウォールエンジン２２９に送信する。ファイアウォールエンジン２２９は、パケット検証（Ｖｅｒｉｆｉｃａｔｉｏｎ）過程を経てパケットフィルタリング動作を行うことができる。ここで、パケット検証過程は、例えばＳｙｎ　Ｆｌｏｏｄｉｎｇのような攻撃を防止するためである。

【００５３】

ファイアウォールエンジン２２９は、パケットデータに対してフィルタリングルールを適用してパケットデータの通過又は遮断如何を判断し、判断結果に従ってパケットデータを通過又は遮断するフィルタリング動作を行うことができる。システムオンチップ（ＳｏＣ）は、ルールＤＢ２２４を備えており、ファイアウォールエンジン２２９は、ルールＤＢ２２４に保存されたルールを利用してパケットフィルタリング動作を行うことができる。

【００５４】

デバイス２００の外部にパケットを送信する場合、ファイアウォールエンジン２２９は、パケットフィルタリングの結果、「通過」と判断されたパケットのみをＮＩＣドライバ２２８に送信する。ＮＩＣドライバ２２８は、ファイアウォールエンジン２２９から受信したパケットをＮＩＣ２３１に送信する。以後、ＮＩＣ２３１は、外部ネットワークにパケットを送信する。

【００５５】

デバイス２００が外部からパケットを受信する場合、ファイアウォールエンジン２２９は、パケットフィルタリングの結果、「通過」と判断されたパケットのみをＡＰドライバ２２１に送信し、ＡＰドライバ２２１は、パケットをミニポートドライバ２１７に送信する。

【００５６】

ＮＩＣ２３１は、パケットデータ網にパケットデータを送信するか、又はそれから受信するためのものであって、システムオンチップ（ＳｏＣ）の一部として装着されうる。ＮＩＣ２３１は、例えば有線又は無線ラン網を介してパケットデータを受信することができる。

【００５７】

このような構成において本発明の一実施形態に係るパケットフィルタリング動作を図３を参照して説明する。

【００５８】

図３は、本発明の例示的な実施形態に係るパケットフィルタリング方法を説明するため

のフローチャートであって、図３Ａは、デバイス２００からパケットを外部に送信する時のパケットフィルタリングのフローチャートであり、図３Ｂは、デバイス２００が外部からパケットを受信する時のフローチャートである。

【００５９】

図３Ａに示すように、ステップＳ１０１にて、任意のアプリケーション２０３によりパケットが生成されてデバイス２００の外部に送信される前に、ミニポートドライバ２１７は前記送信されるパケットを受信する。

【００６０】

ステップＳ１０３にてミニポートドライバ２１７は、このパケットのオーナープロセスを確認する。一実施形態において、オーナープロセスは、前記パケットに含まれたプロセスＩＤから確認されうる。

【００６１】

その後、ステップＳ１０５にて、前記確認されたオーナープロセスが前記パケットを外部に送信することが許容されるかどうかを判断する。このとき、この判断過程にプロセス別ルールＤＢが利用されうる。すなわち、デバイス２００がプロセス別にパケットの送受信を許容又は遮断することを定義したルールＤＢ２１９を備えることができ、このルールＤＢ２１９に保存されたプロセス別ルールに応じて、前記オーナープロセスがパケットを送信することが許容されるかどうかを判断する。

【００６２】

前記ステップＳ１０５にて判断した結果、前記オーナープロセスがパケットを送信することが許容される場合、ステップＳ１０７に進んでミニポートドライブ２１７は、前記パケットをシステムオンチップ（ＳｏＣ）に送信する。

【００６３】

システムオンチップ（ＳｏＣ）は、前記デバイスからパケットを受け取ると、ステップＳ１０９にてパケットフィルタリングを行う。例えば、ファイアウォールエンジン２２９でパケットフィルタリングを行うことができ、その結果に応じて、パケットの送信を許容又は遮断する。このとき、ファイアウォールエンジン２２９は、ルールＤＢ２２４に保存された既定義されたルールを適用してフィルタリングを行うことができる。

【００６４】

一方、ステップＳ１０５にて、前記オーナープロセスがパケットを送信することが許容されない場合、ステップＳ１１１に進んで、ミニポートドライバ２１７は、前記パケットをシステムオンチップ（ＳｏＣ）に送信しない。すなわち、一実施形態においてミニポートドライバ２１７が前記パケットを廃棄できる。そして、追加的なステップとして、ステップＳ１１３にてオーナープロセスの実行までも中断させうる。

【００６５】

一方、デバイス２００が外部からパケットを受信する時は、図３Ｂの流れによってパケットフィルタリングが行われることができる。

【００６６】

図３Ｂに示すように、ステップＳ２０１にて、外部から送信されたパケットがデバイス２００のミニポートドライバ２１７に受信される。図２の実施形態の場合、パケットがまずシステムオンチップ（ＳｏＣ）を経てミニポートドライバ２１７に送信されるが、実施形態によってシステムオンチップ（ＳｏＣ）を経なくても良い。また、システムオンチップ（ＳｏＣ）を経る場合、システムオンチップ内のファイアウォールエンジン２２９がパケットフィルタリングを行い、このパケットフィルタリングを通過したパケットがミニポートドライバ２１７に送信されるが、実施形態によって、ファイアウォールエンジンによるパケットフィルタリングを経ずにミニポートドライバ２１７に送信されうる。

【００６７】

ステップＳ２０３にてミニポートドライバ２１７は、このパケットのオーナープロセスを確認する。一実施形態において、オーナープロセスは、前記パケットに含まれたプロセスＩＤ（ＩＤ）から確認されうる。

【００６８】
その後、ステップＳ２０５にて、前記確認されたオーナープロセスが前記パケットを受信することが許容されるかどうかを判断する。このとき、この判断過程にプロセス別ルールＤＢが利用されうる。すなわち、デバイス２００がルールＤＢ２１９を備える場合、このルールＤＢ２１９に保存されたプロセス別ルールに従って、前記オーナープロセスがパケットを受信することが許容されるかどうかを判断する。
【００６９】
前記ステップＳ２０５での判断結果、前記オーナープロセスがパケットを受信することが許容される場合、ステップＳ２０７に進んで、ミニポートドライブ２１７は、前記パケットをオーナープロセスに伝達する。
【００７０】
しかしながら、ステップＳ２０５にて前記オーナープロセスがパケットを受信することが許容されない場合、ステップＳ２０９に進んで、ミニポートドライバ２１７は、前記パケットをオーナープロセスに送信しない。一実施形態において、ミニポートドライバ２１７は、前記パケットを廃棄できる。そして、追加的なステップとしてステップＳ２１１にてオーナープロセスの実行を中断させうる。
【００７１】
図４は、本発明の他の例示的実施形態に係るシステムオンチップが装着されるデバイスを説明するための図である。
【００７２】
図２に比べて図４の実施形態に係るデバイス２００は、ファイアウォールユーザインタフェース（ＵＩ）アプリケーション２０１及びアンチマルウェア（ＡＭ）ＳｏＣストリームインタフェースドライバ２１１をさらに備え、システムオンチップ（ＳｏＣ）は、ファイアウォールマネジャー２２７をさらに備える。その他の残りの構成要素の構成と機能は、図２と同一又は類似している。
【００７３】
ファイアウォールＵＩアプリケーション２０１は、ファイアウォール動作と関わったユーザインタフェースを提供する。例えば、ファイアウォールＵＩアプリケーション２０１は、ファイアウォール動作作業、ファイアウォール停止作業、ルール追加作業、ルール変更作業、特定ルール除去作業、全体ルール除去作業、ルール状態表示作業、各ルールに適用されたパケットログ出力作業、及び基本ルール設定変更作業などを提供できる。
【００７４】
ファイアウォールＵＩアプリケーション２０１は、ユーザからパケットデータフィルタリングに対するルールを受け取ることができ、ファイアウォールエンジン２２９によったパケットデータフィルタリング結果をユーザに表示できる。ファイアウォールＵＩアプリケーション２０１は、ルールＤＢ２２４に対するアップデート動作を行うことができる。
【００７５】
また、本発明の一実施形態によって、ファイアウォールＵＩアプリケーション２０１は、ミニポートドライバ２１７によるプロセス別パケットフィルタリングの結果をユーザに表示でき、ユーザからプロセス別ルールを受け取ってルールＤＢ２１９のアップデート動作を行うことができる。
【００７６】
アンチマルウェアＳｏＣストリームインタフェースドライバ２１１（以下、ストリームインタフェースドライバとする）は、ファイアウォールＵＩアプリケーション２０１からデータを受信してシステムオンチップ（ＳｏＣ）のＡＰドライバ２２１に送信でき、ＡＰドライバ２２１からデータを受信してファイアウォールＵＩアプリケーション２０１に送信できる。
【００７７】
ファイアウォールマネジャー２２７は、ファイアウォールＵＩアプリケーション２０１を介して受け取ったユーザ命令を処理する機能を行う。例えば、ユーザ命令に応じてルー

ルＤＢ２２４にルールを追加又は変更でき、現在ルールＤＢ２２４の状態を読み込んでファイアウォールＵＩアプリケーション２０１に送信することによって、ユーザに現在状態を見せることもできる。

【００７８】

前記説明したファイアウォールＵＩアプリケーション２０１、ストリームインタフェースドライバ２１１、及びファイアウォールマネジャー２２７以外の残りの構成要素は、構成や機能が図２に示したものと同一又は類似しているので、その説明を省略する。

【００７９】

このような図４の構成において、ユーザがファイアウォールＵＩアプリケーション２０１を介してルールＤＢ２１９及び／又はルールＤＢ２２４のルール設定を変更でき、以下、図５ないし図８を参照して後述する。

【００８０】

図５は、本発明の例示的な実施形態に係るファイアウォールインタフェースが提供するルール設定画面を説明するための図である。

【００８１】

本発明の例示的な実施形態によって、デバイス２００のファイアウォールＵＩアプリケーション２０１は、ユーザによるルールＤＢ２１９及び／又はルールＤＢ２２４の設定のためのルール設定画面５００をユーザに提供できる。

【００８２】

デバイス２００は、ルール設定画面５００を介してユーザから受け取ったルールをシステムオンチップ（ＳｏＣ）に送信し、前記システムオンチップは、デバイスから送信されたルールを自身の保存部に保存されたルールＤＢに反映できる。

【００８３】

図５に示すように、ルール設定画面５００は、三個のサブウィンドウ、すなわち基本設定ウィンドウ５１０、基本ルール設定ウィンドウ５２０、及びプロセス別設定ウィンドウ５３０を備える。ユーザは、ルール設定画面５００から前記３個のサブウィンドウのうち、任意のサブウィンドウを選択してルール設定を行うことができ、図５は、基本設定ウィンドウ５１０が選択された状態を示す。

【００８４】

図５に示す基本設定ウィンドウ５１０は、例えばユーザがある特定ＩＰアドレス又は特定ネットワーク帯域のＩＰアドレスに該当するサイトを許容（ａｌｌｏｗ）又は遮断（ｂｌｏｃｋ）しようとするときにこれを設定する画面である。

【００８５】

図示の一実施形態において基本設定ウィンドウ５１０は、コンフィギュレーションヘルパー（ｃｏｎｆｉｇｕｒａｔｉｏｎ　ｈｅｌｐｅｒ）５１１機能のための入力ウィンドウ５１２を備え、その下にルールネーム、ＩＰ、プロトコル、ポートなどの各種フィールドを満たすための入力ウィンドウを備えることができる。

【００８６】

コンフィギュレーションヘルパー５１１は、ネットワークを全く知らないユーザを助ける機能を果たす。本発明の一実施形態においてコンフィギュレーションヘルパー５１１は、ネットワークアプリケーションに対するリストを提供し、このリストに含まれたネットワークアプリケーションのうち、少なくとも何れか一つのネットワークアプリケーションがユーザにより選択されると、該選択されたネットワークアプリケーションを実行するのに必要なＩＰ、プロトコル、及びポートのうち、少なくとも何れか一つを該当フィールドの入力ウィンドウに自動的に表示できる。

【００８７】

例えば、ユーザがコンフィギュレーションヘルパー５１１の入力ウィンドウ５１２のボタンを選択すると、図６に示したようなメニューが広まる。広まったネットワークアプリケーションのうち、ユーザが何れか一つを選択すると、図５においてコンフィギュレーションヘルパー５１１の下にあるルールネーム、ＩＰ、プロトコル、ポートなどのフィール

ドに該当する値が自動的に入力されるようになる。

【００８８】

図６のリストには、メッセンジャー、Ｐ２Ｐ、ゲームなどのみを例示しましたが、実施形態によってｆｔｐ、ｈｔｔｐ、テレネット、ｓｓｈ、ｐｒｉｎｔｅｒなどのプロトコルも選択できるように前記リストに含まれうる。

【００８９】

前記実施形態のように、コンフィギュレーションヘルパー５１１を備えるのは、一般的なユーザは、特定プロトコルあるいは特定サービスのポートを全く知らない場合が多く、またネットワークをよく知っているユーザであっても、例えばＭＳＮメッセンジャーでファイルをやり取りするために６８９１～６９００番ポートと４１８００～４１８９９番ポートとを許容しなければならないという事実を、関連文書を探す前には分かり難いためである。したがって、前記実施形態のように、通常のユーザのためのコンフィギュレーションヘルパー５１１を提供することによって、ユーザ自身の望むサービスに対してファイアウォールの設定作業をより容易に行うことができる。

【００９０】

図５を再度参照して、コンフィギュレーションヘルパー５１１の下部の各種フィールドについて説明する。

【００９１】

－ルールネーム（Ｒｕｌｅ　Ｎａｍｅ）：ルールの名称を入力するフィールドである。

【００９２】

－インターネットプロトコル（ＩＰ）：ルールを適用するＩＰを設定するフィールドである。一実施形態においてＩＰフィールドには、下記の表１に例示したタイプの設定が可能である。

【００９３】

【表１】

ＩＰフィールド表記	意味
192.168.0.1	特定ネットワーク帯域を指定
192.168.0.*	特定ネットワーク帯域を指定
192.168.*.*	特定ネットワーク帯域を指定
192.***.*	特定ネットワーク帯域を指定
..*.*	すべてのＩＰを意味
*	すべてのＩＰを意味
空欄にしたとき	すべてのＩＰを意味
192.168.0.0/255.255.255.0	特定ネットワーク帯域を指定
192.168.0.10/255.255.255.224	特定ネットワーク帯域を指定（サブネットを使用）
192.168.0.20/24	特定ネットワーク帯域を指定
192.168.0.30/27	特定ネットワーク帯域を指定（サブネットを使用）
FDEC:BA98:0074:3210:000F:BBFF:0000:2345	IPv6 IPを意味
FDEC:BA98:74:3210:F:BBFF:0:2345	IPv6 IPを意味
FDEC:BA98:74:3210:F:BBFF:0:FFFF/26	IPv6 IP特定ネットワーク帯域を意味

【００９４】

前記表１の入力例では、「１９２．１６８．＊．＊」の表記のように「＊」表記法を使用できるようにした。「１９２．１６８．＊．＊」の表記は、特定ネットワーク帯域を意味するという点で「１９２．１６８．０．０／２５５．２５５．０．０」の表記又は「１９２．１６８．０．０／１６」の表記と同一である。しかしながら、一般ユーザには、「１９２．１６８．０．０／２５５．２５５．０．０」の表記や「１９２．１６８．０．０／１６」の表記よりは、「１９２．１６８．＊．＊」のような表記がより理解しやすいために、前記実施形態は、「１９２．１６８．＊．＊」のような表記も許容する。

【００９５】
ただし「１９２．１６８．＊．＊」のような表記でネットワーク帯域を指定する場合、サブネットマスクを指定できないために、「１９２．１６８．０．０／２５５．２５５．０．０」又は「１９２．１６８．０．０／１６」のような表記方法も共に使用できるようにする。
【００９６】
また、前記表１の入力例は、ネットマスク（ｎｅｔｍａｓｋ）フィールドがなく、その代わりにＩＰフィールドに統合された。ネットワークを全く知らないユーザであってもＩＰとポート程度は分かるが、ネットマスクの意味や使用法は、分からない可能性が大きいためである。
【００９７】
－プロトコル（Ｐｒｏｔｏｃｏｌ）：ルールを適用するプロトコルを設定する部分である。一実施形態においてプロトコルに該当するボタンを押すと、「ＡＬＬ」、「ＴＣＰ」、「ＵＤＰ」、「ＩＣＭＰ」などのメニューリストが出ることができる。その他にも前記基本的なプロトコルだけでなく、他の多様なプロトコルも支援できる。
－ポート（Ｐｏｒｔ）：ルールを適用するポートを設定する部分である。ユーザが直接入力することもでき、メニューボタンを押して選択することもできる。メニューボタンを押すと、ｆｔｐ、ｈｔｔｐ、テレネット、ｓｓｈなどのようなプロトコル文字列が出、この中で一つを選択すると、最小ポート番号（ｍｉｎ　ｐｏｒｔ）と最大ポート番号（ｍａｘ　ｐｏｒｔ）が自動的に入力されるようにすることができ、ユーザが直接入力することもできる。
－パケット方向（Ｄｉｒｅｃｔｉｏｎ）：ルールを適用するパケットの方向を指定する部分である。一実施形態において、ボタンを押すと「ＡＬＬ」、「内部→外部」、「外部→内部」のようなメニューリストが出ることができる。「内部→外部」は、デバイス２００の外部に送信されるパケットにのみルールが適用されることを意味し、「外部→内部」は、デバイス２００が受信するパケットにのみルールが適用されることで、「ＡＬＬ」は、送信及び受信されるパケットのすべてにルールが適用されることを意味する。
－ローカルデバイス（Ｌｏｃａｌ　Ｄｅｖｉｃｅ）：ルールを適用するネットワークインタフェースＩＰを設定する部分である。例えば、デバイス２００に二つのＮＩＣが存在する場合、特定ＮＩＣに入るパケットに対してルールを適用しようとすると、このフィールドで該当ＮＩＣのＩＰを入力すればよい。一実施形態においてこのフィールドのボタンを押すと、「ＡＬＬ」又はローカルデバイスのＩＰリストが列挙されて選択可能である。
－ＭＡＣアドレス（ＭＡＣ　Ａｄｄｒｅｓｓ）：ルールを適用するＭＡＣアドレスを設定する部分である。
－アクション（Ａｃｔｉｏｎ）：該当ルールと一致するパケットが入ったときに行う動作を設定する部分である。「Ｎｏｔｈｉｎｇ」、「Ａｌｌｏｗ」、「Ｂｌｏｃｋ」、「Ｌｏｇｇｉｎｇ」などがありうる。「Ｌｏｇｇｉｎｇ」は、ルールに適用されるパケットに対してログを残す機能である。
【００９８】
以下、図７を参照して基本ルール設定のための実施形態を説明する。図７は、本発明の例示的な実施形態に係る基本ルールを設定できるルール設定画面５００を説明するための図であって、基本ルール設定ウィンドウ５２０が選択された状態を示す。
【００９９】
図７の基本ルール設定は、図５の入力例によって設定されたルールと一致しないパケットが入った時の適用するルールのことを意味する。図７に示すように、基本ルール設定ウィンドウ５２０は、基本ルール説明５２１及び現在基本ルール状態５２２をそれぞれ表すウィンドウを備え、またすべて遮断ボタン５２３及びすべて許容ボタン５２４を備えることができる。
【０１００】
基本ルール説明５２１は、基本ルール設定の意味をユーザに説明する説明ウィンドウで

あり、現在基本ルール状態５２２は、現在設定されている基本ルールの状態を示すウィンドウである。

【０１０１】

一実施形態において基本的なデフォルト値として基本ルールは、外部に送信されるパケット（アウトゴウイングパケット）に対しては、許容（ａｌｌｏｗ）に、デバイスの内部に受信されるパケット（インカミングパケット）に対しては、遮断（ｂｌｏｃｋ）に設定されていることができる。すべて遮断ボタン５２３及びすべて許容ボタン５２４は、このような基本ルールの設定をアウトゴウイングパケットとインカミングパケットの両方に対して「遮断」又は「許容」に設定する機能のことを意味する。

【０１０２】

一方、一実施形態において、設定画面５００の基本設定ウィンドウ５１０や基本ルール設定ウィンドウ５２０においてユーザが入力したルール設定情報は、ストリームインタフェースドライバ２１１を経てシステムオンチップ（ＳｏＣ）のファイアウォールマネジャー２２７に送信され、ファイアウォールマネジャー２２７により前記ルール設定情報がルールＤＢ２２４に反映されることによって、ルールＤＢがアップデートされる。

【０１０３】

図８は、本発明の例示的な実施形態に係るプロセス別ルールを設定できるルール設定画面を説明するための図であって、プロセス別設定ウィンドウ５３０が選択された状態を示す。

【０１０４】

プロセス別設定ウィンドウ５３０は、アプリケーションのプロセス別にパケットを許容又は遮断することを定義したプロセス別ルールを入力できる領域であって、図示の実施形態においてプロセス別設定ウィンドウ５３０は、プロセスリスト５３１、選択ウィンドウ５３２、遮断ボタン５３３、及び許容ボタン５３４などを備えることができる。

【０１０５】

ユーザは、このようなプロセス別設定ウィンドウ５３０を介して例えばある特定アプリケーションのプロセスに対するファイアウォールの設定を許容（ａｌｌｏｗ）することで、このプロセスが生成するすべてのソケットのパケットの通過を許容（ａｌｌｏｗ）でき、反対に、ある特定アプリケーションのプロセスに対するファイアウォールの設定を遮断（ｂｌｏｃｋ）することで、該当プロセスが生成するすべてのソケットのパケットの通過を遮断できる。

【０１０６】

一実施形態において、設定画面５００のプロセス別設定ウィンドウ５３０でユーザが入力したルール設定情報は、ストリームインタフェースドライバ２１１により前記ルール設定情報がルールＤＢ２１９に反映されることによって、プロセス別ルールＤＢがアップデートされうる。しかしながら、代案的な実施形態によってファイアウォールＵＩアプリケーション２０１又は他の構成要素によりルールＤＢ２１９がアップデートされうる。

【０１０７】

図９は、本発明の他の例示的実施形態に係るシステムオンチップが装着されるデバイスを説明するための図である。

【０１０８】

図４に比べて図９の実施形態では、カーネル層のルールＤＢ（図４の２１９）が選択的である。したがって、図９では、前記ルールＤＢ２１９が存在しないと仮定した。その他の残りの構成要素の機能や役割は、図４とすべて同一又は似ているので説明は省略する。

【０１０９】

図９の実施形態においてミニポートドライバ２１７は、ルールＤＢからプロセス別ルールＤＢを受けてパケットと直接比較する動作を行わない。その代りに、例えば、デバイス２００がパケットを外部に送信する場合、ミニポートドライバ２１７は、所定パケットを受信すると、該当パケットのオーナープロセスのＩＤを確認した後、このプロセスＩＤを該当パケットと共にシステムオンチップ（ＳｏＣ）に送信し、システムオンチップ（Ｓｏ

Ｃ）上でプロセス別ルールＤＢをパケットに適用する。

【０１１０】

すなわち、図示の一実施形態においてルールＤＢ２２４がプロセス別ルールＤＢをさらに含み、このとき、プロセス別ルールＤＢは、プロセス別にパケットの送受信を許容又は遮断することを定義したルールＤＢを含んでいる。これにより、例えばファイアウォールエンジン２２９に任意のパケットが送信されてくるとき、ファイアウォールエンジン２２９は、ルールＤＢ２２４に保存されたプロセス別ルールに従って、前記パケットのオーナープロセスがパケットを送受信することが許容されるかどうかを判断し、判断結果に応じて前記パケットの通過を許容又は遮断し、なお前記オーナープロセス自体の実行中断を要請できる。

【０１１１】

このようなパケットフィルタリングの動作を図１０を参照して説明する。

【０１１２】

図１０は、図９のデバイスにおける本発明の例示的な実施形態に係るパケットフィルタリング方法を説明するためのフローチャートであって、デバイス２００からパケットを外部に送信する時のパケットフィルタリング過程を示す。

【０１１３】

図１０に示すように、ステップＳ１００１にて任意のアプリケーション２０３によりパケットが生成されてデバイス２００の外部に送信される前に、ミニポートドライバ２１７が前記送信されるパケットを受信する。

【０１１４】

ステップＳ１００３にてミニポートドライバ２１７は、このパケットのオーナープロセスを確認する。一実施形態において、オーナープロセスは、前記パケットに含まれたプロセスＩＤ（ＩＤ）から確認されうる。

【０１１５】

その後、ステップＳ１００５にて、前記パケットを使用するオーナープロセスを識別する情報を生成して、前記パケットと共にシステムオンチップ（ＳｏＣ）に送信する。このとき、前記識別情報は、例えばプロセスＩＤになりうる。

【０１１６】

前記パケット及び識別情報（例えば、プロセスＩＤ）は、システムオンチップ（ＳｏＣ）のファイアウォールエンジン２２９に送信され、ステップＳ１００７にてファイアウォールエンジン２２９が前記オーナープロセスが前記パケットを外部に送信することが許容されるかどうかを判断する。このとき、この判断過程にプロセス別ルールＤＢが利用されうる。すなわちデバイス２００がプロセス別にパケットの送受信を許容又は遮断することを定義したルールをルールＤＢ２２４が備えることができ、前記プロセス別ルールに従って、前記オーナープロセスがパケットを送信することが許容されるかどうかを判断する。

【０１１７】

前記ステップＳ１００７にて判断した結果、前記オーナープロセスがパケットを送信することが許容される場合、ステップＳ１００９に進んで、ファイアウォールエンジン２２９がステップＳ１００９にてパケットフィルタリングを行う。すなわち、ルールＤＢ２２４に保存されたパケットフィルタリングルールに従ってパケット送信の許容又は遮断を判断するフィルタリング作業を行うことができ、その結果に応じてパケットの送信を許容又は遮断する。

【０１１８】

代案的な実施形態において、前記パケットフィルタリングステップＳ１００９は、前記判断するステップＳ１００７の前に行われうる。すなわち、パケットフィルタリングを経て通過されたパケットに対してのみ前記判断ステップＳ１００７を行うこともできる。

【０１１９】

一方、ステップＳ１００７にて、前記オーナープロセスがパケットを送信することが許容されない場合、ステップＳ１０１１に進んで、ファイアウォールエンジン２２９は、前

記パケットをＮＩＣドライバ２２８側に送信しない。一実施形態においてファイアウォールエンジン２２９は、前記パケットを廃棄できる。そして、追加的なステップとして、ステップＳ１０１３にてファイアウォールエンジン２２９は、オーナープロセスの実行の中断を要請する信号をカーネル側に送信できる。

【０１２０】

図１１は、本発明の他の例示的実施形態に係るシステムオンチップが装着されるデバイスを説明するための図である。

【０１２１】

図９に比べて図１１の実施形態は、デバイス２００が外部と通信するための構成要素であるＮＩＣドライバ２２８及びＮＩＣ２３１の位置が図９の実施形態と異なる。図１１に示すように、ＮＩＣ２３１がシステムオンチップ（ＳｏＣ）でないデバイス２００の本体側に位置しており、ＮＩＣドライバ２２８もカーネル層のＮＤＩＳ２１８に位置する。その他の残りの構成要素の機能や役割は、図９と同一又は似ているので、説明を省略する。

【０１２２】

前記構成によれば、デバイス２００の内部から外部に送信されるパケット又は外部からデバイス２００に受信されるパケットがミニポートドライバ２１７に送信されうる。したがって、ミニポータードライバ２１７は、送信又は受信されるすべてのパケットに対して該当パケットのオーナープロセスのＩＤを確認した後、このプロセスＩＤを該当パケットと共にシステムオンチップ（ＳｏＣ）に伝達し、システムオンチップ（ＳｏＣ）上でプロセス別ルールＤＢを前記パケットに適用できる。

【０１２３】

このようなパケットフィルタリングの動作を図１２を参照して説明する。図１２は、図１１のデバイスにおける本発明の例示的な実施形態に係るパケットフィルタリング方法を説明するためのフローチャートである。

【０１２４】

図１２に示すように、ステップＳ１２０１にて、送信又は受信されるパケットがミニポートドライバ２１７に送信され、ステップＳ１２０３にてミニポートドライバ２１７は、このパケットのオーナープロセスを確認する。一実施形態において、オーナープロセスは、前記パケットに含まれたプロセスＩＤ（ＩＤ）から確認されうる。

【０１２５】

その後、ステップＳ１２０５にて、前記パケットを使用するオーナープロセスを識別する情報を生成して、前記パケットと共にシステムオンチップ（ＳｏＣ）に送信する。このとき、前記識別情報は、例えばプロセスＩＤになりうる。

【０１２６】

前記パケット及び識別情報（例えばプロセスＩＤ）は、システムオンチップ（ＳｏＣ）のファイアウォールエンジン２２９に送信され、ステップＳ１２０７にて、ファイアウォールエンジン２２９は、プロセス別ルールＤＢを利用して、前記オーナープロセスが前記パケットを外部に送信又は受信することが許容されるかどうかを判断する。すなわち、外部に送信されるパケットに対しては、該当パケットのオーナープロセスがこのパケットを送信することが許容されるかどうかを判断し、外部から受信するパケットに対しては、該当パケットのオーナープロセスがこのパケットを受信することが許容されるかどうかを判断できる。

【０１２７】

前記ステップＳ１２０７にて判断した結果、前記オーナープロセスがパケット送信（又は受信）が許容されるプロセスに属する場合、ステップＳ１２０９に進んで、ファイアウォールエンジン２２９がステップＳ１２０９にてパケットフィルタリングを行う。すなわち、ルールＤＢ２２４に保存されたパケットフィルタリングルールに従ってパケットフィルタリング作業を行うことができ、その結果に応じてパケットの送信を許容又は遮断する。代案的な実施形態において、前記パケットフィルタリングステップＳ１２０９は、前記判断するステップＳ１２０７の前に行われうる。

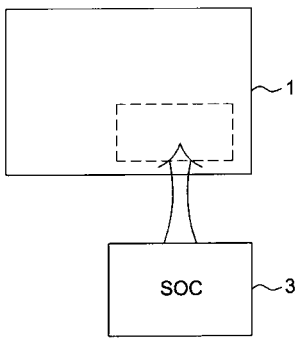
【０１２８】
一方、ステップＳ１２０７にて、外部に送信されるパケットの場合、前記オーナープロセスがパケットを送信することが許容されない場合、ステップＳ１２１１に進んで、ファイアウォールエンジン２２９は、前記パケットをＮＩＣドライバ２２８側に送信しない。一実施形態においてファイアウォールエンジン２２９は、前記パケットを廃棄できる。そして、追加的なステップとして、ステップＳ１２１３にてファイアウォールエンジン２２９は、オーナープロセスの実行の中断を要請する信号をカーネル側に送信できる。
【０１２９】
万一、ステップＳ１２０７にて、デバイス外部から受信するパケットの場合、前記オーナープロセスがパケットを受信することが許容されないと、ステップＳ１２１１に進んで、ファイアウォールエンジン２２９は、前記パケットをアプリケーション２０３側に送信しない。一実施形態においてファイアウォールエンジン２２９は、前記パケットを廃棄できる。そして、追加的なステップとして、ステップＳ１２１３にてファイアウォールエンジン２２９は、オーナープロセスの実行の中断を要請する信号をカーネル側に送信できる。
【０１３０】
図１３は、本発明の他の例示的実施形態に係るシステムオンチップが装着されるデバイスを説明するための図である。
【０１３１】
図１１に比べて図１３の実施形態は、システムオンチップ（ＳｏＣ）がハードウェア的構成要素のみを備えているという点で図１１と異なる。すなわち、図示の実施形態においてシステムオンチップ（ＳｏＣ）は、デバイス２００のカーネル層と通信するためのＡＰドライバ２２１及びファイアウォールエンジン２２９を備える。一実施形態においてファイアウォールエンジン２２９は、メモリ２４１及びマッチャー（ｍａｔｃｈｅｒ）２４２を備えることができる。
【０１３２】
メモリ２４１は、デバイス２００の任意の保存装置に保存されているルールＤＢをロードして一時的に保存するためのメモリであって、揮発性保存装置でありうる。マッチャー２４２は、パケットをルールＤＢのパケットフィルタリングルール及び／又はプロセス別ルールと比較してパケットの遮断又は許容を判断できる。その他の残り構成要素の機能や役割は、図１１と同一又は似ているので説明を省略する。
【０１３３】
前記実施形態に係るパケットフィルタリング動作は、基本的に図１２と同一又は似ている。ただし、ファイアウォールエンジン２２９によるパケットフィルタリングを行う前にデバイス２００の保存装置に保存されているルールＤＢ２１９がシステムオンチップ（ＳｏＣ）のメモリ２４１にロードされる。その後、ミニポータードライバ２１７は、送信又は受信されるすべてのパケットに対して該当パケットのオーナープロセスのＩＤを確認した後、このプロセスＩＤを該当パケットと共にシステムオンチップ（ＳｏＣ）に伝達し、システムオンチップ（ＳｏＣ）のファイアウォールエンジン２２９は、プロセス別ルールを含んだパケットフィルタリングルールを適用する。
【０１３４】
一方、以上で説明した実施形態では、アプリケーション（プログラム）の「プロセス」単位でパケットの許容又は遮断を設定するか、又はプロセス自体の実行を中断すると説明したが、実施形態によって、プロセスでないプログラム単位で前記動作を行うこともできる。例えば、遮断された所定パケットに対してこのパケットのオーナープログラムを確認してこのオーナープログラムの実行を中断できる。すなわち、前記図面を参照して説明した実施形態において「プロセス」を「プログラム」に置き換えても本発明的概念に含まれうる。
【０１３５】
以上説明した本発明に係る実施形態は、またコンピュータ読み取り可能な記録媒体にコ

ンピュータが読み取ることのできるコードとして具現化することが可能である。コンピュータ読み取り可能な記録媒体は、コンピュータシステムによって読まれることができるデータが保存されるすべての種類の記録装置を含む。コンピュータ読み取り可能な記録媒体の例には、ＲＯＭ、ＲＡＭ、ＣＤ－ＲＯＭ、磁気テープ、フロッピーディスク、光データ保存装置などがあり、またキャリアウェーブ（例えば、インターネットを介した送信）の形態で具現化されることも含む。また、コンピュータ読み取り可能な記録媒体は、ネットワークで接続されたコンピュータシステムに分散されて、分散方式でコンピュータが読み出すことができるコードが保存され実行されうる。

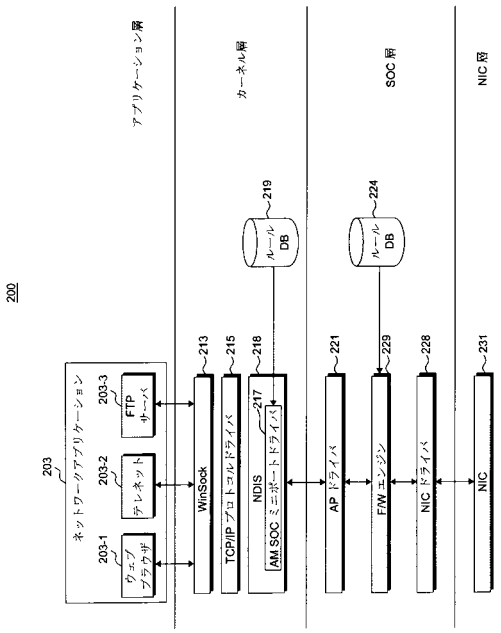
【０１３６】

以上、本発明は、限定された実施形態と図面により説明されたが、本発明は、上記の実施形態に限定されるものではなく、本発明が属する分野における通常の知識を有した者であればこのような記載から多様な修正及び変形が可能である。したがって、本発明の範囲は、説明された実施形態に限定されてはならず、後述する特許請求の範囲だけでなく、この特許請求の範囲と均等なものによって定められねばならない。

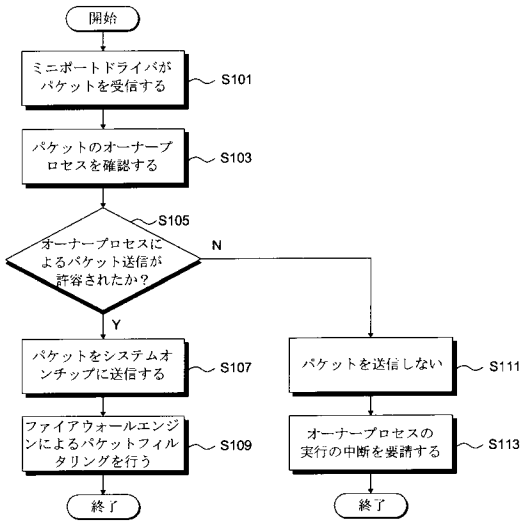
【図１】



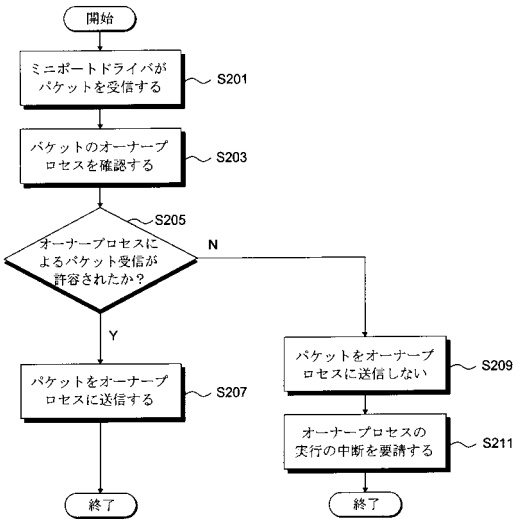
【図２】



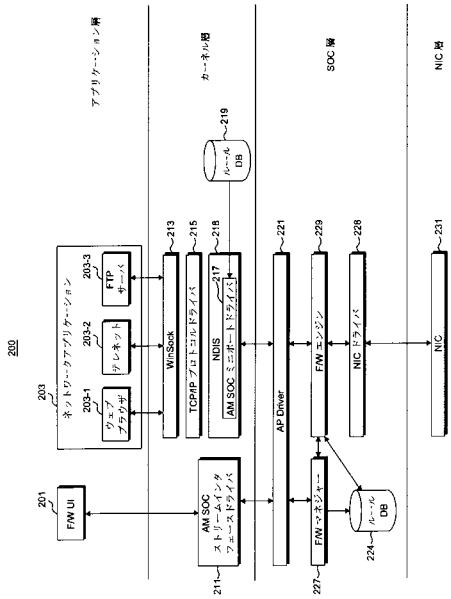
【図３Ａ】


開始
ミニポートドライバがパケットを受信する
S101
パケットのオーナープロセスを確認する
S103
S105
オーナープロセスによるパケット送信が許容されたか？
N
Y
パケットをシステムオンチップに送信する
S107
ファイアウォールエンジンによるパケットフィルタリングを行う
S109
終了
パケットを送信しない
S111
オーナープロセスの実行の中断を要請する
S113
終了

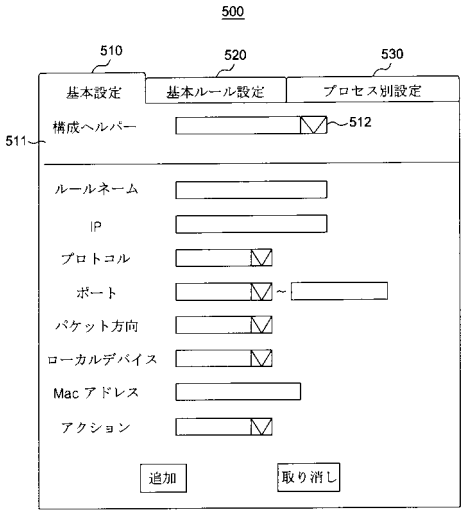
【図３Ｂ】


開始
ミニポートドライバがパケットを受信する
S201
パケットのオーナープロセスを確認する
S203
S205
オーナープロセスによるパケット受信が許容されたか？
N
Y
パケットをオーナープロセスに送信する
S207
終了
パケットをオーナープロセスに送信しない
S209
オーナープロセスの実行の中断を要請する
S211
終了

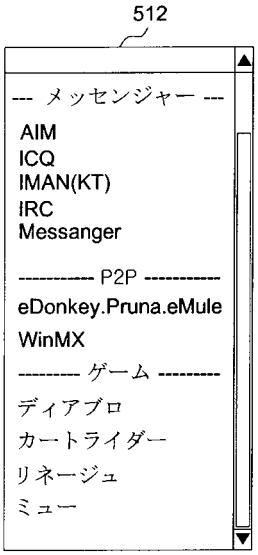
【図４】


アプリケーション層
カーネル層
SOC 層
NIC 層
200
203
ネットワークアプリケーション
203-1
ウェブブラウザ
203-2
テレネット
203-3
FTP
201
F/W UI
211
AM SOC ストリームインタフェースドライバ
213
WinSock
215
TCP/IP プロトコルドライバ
217
AM SOC ミニポートドライバ
218
NDIS
219
ルール DB
221
AP Driver
224
ルール DB
227
F/W マネジャー
229
F/W エンジン
228
NIC ドライバ
231
NIC

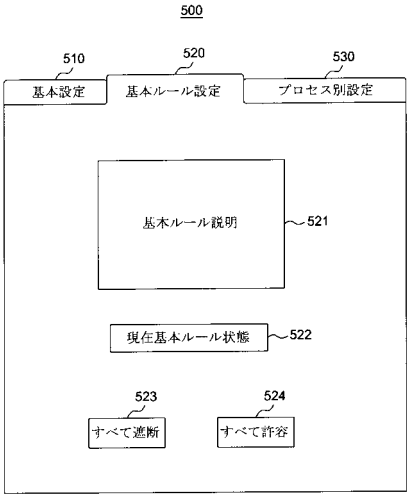
【図５】


500
510
520
530
基本設定
基本ルール設定
プロセス別設定
構成ヘルパー
512
511
ルールネーム
IP
プロトコル
ポート
パケット方向
ローカルデバイス
Mac アドレス
アクション
追加
取り消し

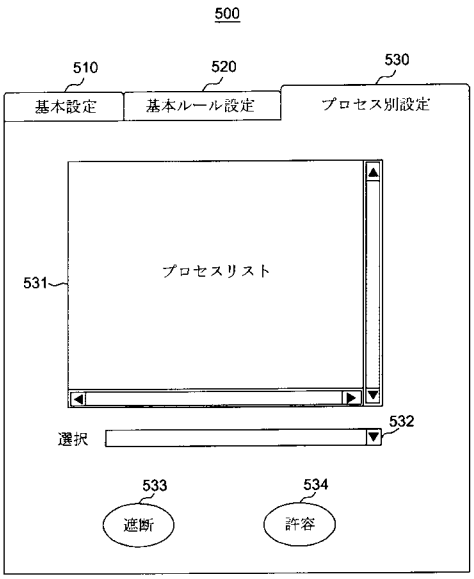
【図６】


512
--- メッセンジャー ---
AIM
ICQ
IMAN(KT)
IRC
Messanger
---------- P2P ----------
eDonkey.Pruna.eMule
WinMX
--------- ゲーム ---------
ディアブロ
カートライダー
リネージュ
ミュー

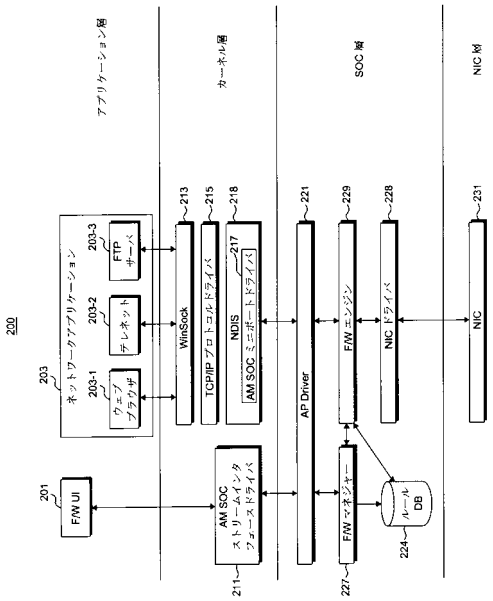
【図７】


500
510
基本設定
520
基本ルール設定
530
プロセス別設定
基本ルール説明
521
現在基本ルール状態
522
523
すべて遮断
524
すべて許容

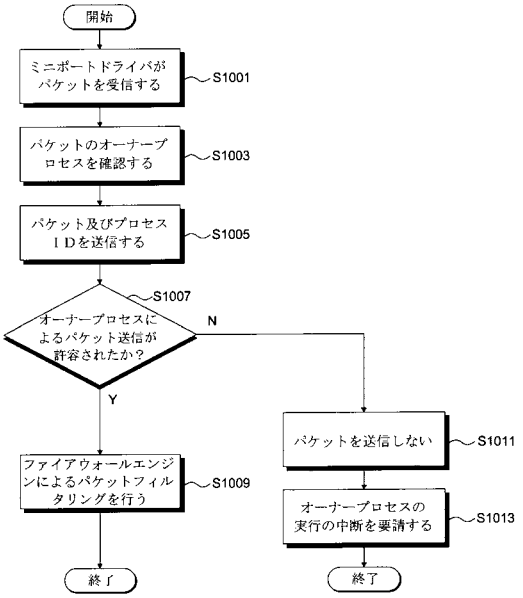
【図８】


500
510
基本設定
520
基本ルール設定
530
プロセス別設定
プロセスリスト
531
選択
532
533
遮断
534
許容

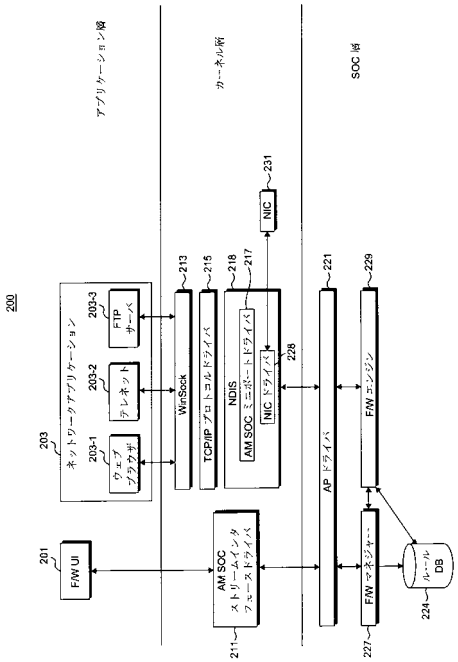
【図９】


200
アプリケーション層
カーネル層
SOC 層
NIC 層
ネットワークアプリケーション
203
203-1
ウェブブラウザ
203-2
テレネット
203-3
FTP サーバ
WinSock
213
TCP/IP プロトコルドライバ
215
NDIS
217
AM SOC ミニポートドライバ
218
AP Driver
221
F/W エンジン
229
NIC ドライバ
228
NIC
231
F/W UI
201
AM SOC ストリームインタフェースドライバ
211
F/W マネジャー
227
ルール DB
224

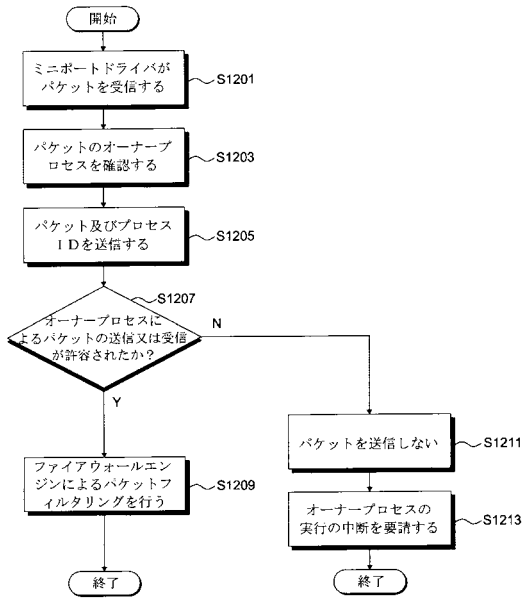
【図１０】



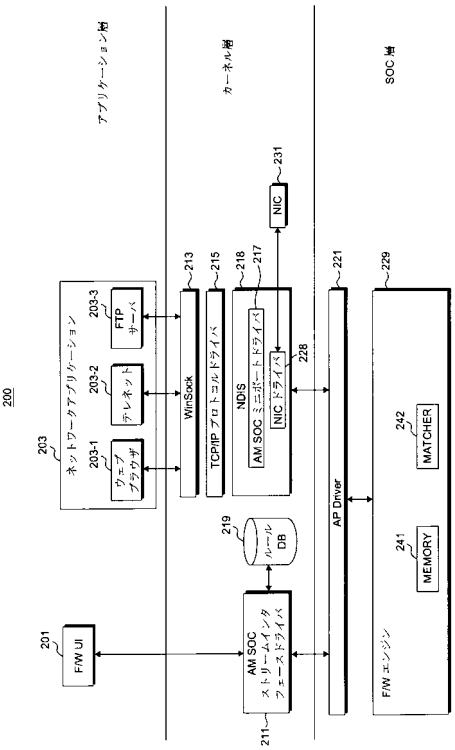
【図１１】



【図１２】



【図１３】



フロントページの続き

(72)発明者　ユ、インソン
大韓民国キョンキド、オサンシ、ガルゴッドン、オサン、ケイシーシー、スイチェンアパート、１０１－１４０４

審査官　玉木　宏治

(56)参考文献　特開２００６－３３１４２２（ＪＰ，Ａ）
特開２００６－１５７３１３（ＪＰ，Ａ）
Kristen Accardi et al., Network processor acceleration for a Linux netfilter firewall, Symposium on Architecture for networking and communications systems, 2005. ANCS 2005., ２００５年１０月

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　１２／００－９５５