(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5411134号
(P5411134)
(45)発行日　平成26年2月12日(2014.2.12)　(24)登録日　平成25年11月15日(2013.11.15)

(51)Int.Cl.　F I
H04L 12/66 (2006.01)　H04L 12/66 B

請求項の数 28　(全 22 頁)

(21)出願番号	特願2010-514785 (P2010-514785)
(86)(22)出願日	平成20年6月25日 (2008.6.25)
(65)公表番号	特表2010-532633 (P2010-532633A)
(43)公表日	平成22年10月7日 (2010.10.7)
(86)国際出願番号	PCT/US2008/007876
(87)国際公開番号	WO2009/005650
(87)国際公開日	平成21年1月8日 (2009.1.8)
審査請求日	平成23年6月14日 (2011.6.14)
(31)優先権主張番号	11/772,061
(32)優先日	平成19年6月29日 (2007.6.29)
(33)優先権主張国	米国 (US)

(73)特許権者　500090534
イクストリーム・ネットワークス・インコーポレーテッド
アメリカ合衆国・９５０５１・カリフォルニア州・サンタ　クララ・モンロー　ストリート・３５８５
(74)代理人　100064621
弁理士　山川　政樹
(74)代理人　100098394
弁理士　山川　茂樹
(72)発明者　カスラリカー，ラフル・エス
アメリカ合衆国・９５１３５・カリフォルニア州・サンノゼ・フォールズ　クリーク　ディーアール・３２９３

最終頁に続く

(54)【発明の名称】ネットワークスイッチにおけるポートリダイレクトのための方法及びメカニズム

(57)【特許請求の範囲】
【請求項１】
ネットワーク内のスイッチング装置において実行される方法であって、当該方法は、
前記スイッチング装置へ送信された前記ネットワーク内の１又はそれ以上の宛先へ送信すべきデータパケットを受信するステップと、
前記受信したデータパケットが前記スイッチング装置のリダイレクトポートに関連していることを、ネットワーク状態が示しているかどうかを判定するステップであって、前記リダイレクトポートは、リダイレクトされたデータパケットを、該リダイレクトされたデータパケットの分析に基づいて前記スイッチング装置へ戻すように構成されたネットワークサービスに関連する、ステップと、
前記データパケットを前記スイッチング装置からフラッディングすべきかどうかを判定するステップと、
前記受信したデータパケットが前記スイッチング装置からフラッディングすべきと判定された場合、前記リダイレクトポートを、前記受信したデータパケットの前記フラッディングから切り離して、前記受信したデータパケットを前記スイッチング装置からフラッディングするステップと、
前記受信したデータパケットが前記リダイレクトポートに関連していることを前記ネットワーク状態が示していると判定され、かつ前記データパケットを前記スイッチング装置からフラッディングすべきでないと判定された場合、前記受信したデータパケットを前記スイッチング装置のリダイレクトポートへリダイレクトするステップと、

を含むことを特徴とする方法。
【請求項２】
前記ネットワーク状態は、前記受信したデータパケットのトラフィックタイプを含む、
ことを特徴とする請求項１に記載の方法。
【請求項３】
前記データパケットを前記スイッチング装置からフラッディングすべきかどうかを判定するステップは、
前記受信したデータパケットがブロードキャスト媒体アクセス制御（ＭＡＣ）宛先アドレスを含んでいると判定するステップと、
前記受信したデータパケットが、転送用データベースのいずれのエントリにも対応しない媒体アクセス制御（ＭＡＣ）宛先アドレスを含んでいると判定するステップと、
の少なくとも一方を含むことを特徴とする請求項１に記載の方法。
【請求項４】
前記データパケットを前記スイッチング装置からフラッディングすべきかどうかを判定するステップは、前記受信したデータパケットがインターネットプロトコル（ＩＰ）マルチキャスト宛先アドレスを含んでいると判定するステップを含む、
ことを特徴とする請求項１に記載の方法。
【請求項５】
前記受信したデータパケットを前記スイッチング装置からフラッディングするステップは、前記受信したデータパケットを前記スイッチング装置のいずれのリダイレクトポートへも送信せずに実行されることを特徴とする請求項１に記載の方法。
【請求項６】
前記リダイレクトポートは、前記スイッチング装置からのデータパケットのいずれのフラッディングからも切り離されることを特徴とする請求項５に記載の方法。
【請求項７】
前記リダイレクトポートは、仮想ローカルエリアネットワーク（ＶＬＡＮ）をサポートするポートの組から除外されることを特徴とする請求項６に記載の方法。
【請求項８】
前記受信したデータパケットが前記スイッチング装置のリダイレクトポートに関連していることを前記ネットワーク状態が示していると判定され、当該方法は、前記データパケットを前記スイッチング装置のリダイレクトポートへ送信すべき旨の指示を、前記データパケットを前記スイッチング装置の少なくとも１つの他のポートへフラッディングすべき旨の指示に置き換えるステップをさらに含む、
ことを特徴とする請求項５に記載の方法。
【請求項９】
前記データパケットを前記スイッチング装置のリダイレクトポートへ送信すべき旨の指示を、前記データパケットを前記スイッチング装置の少なくとも１つの他のポートへフラッディングすべき旨の指示に置き換えるステップは、シーケンス制御テーブル（ＳＣＴ）に記憶された１又はそれ以上のコマンドを実行して、前記スイッチング装置の少なくとも１つの他のポートの識別子を取り出すステップを含む、
ことを特徴とする請求項８に記載の方法。
【請求項１０】
前記ネットワーク状態が、前記受信したデータパケットが前記スイッチング装置のリダイレクトポートに関連していることを示し、前記受信したデータパケットを前記スイッチング装置からフラッディングするステップは、前記スイッチング装置のリダイレクトポートのアクセス制御リストの規則を実施するステップを含み、該規則は、インターネットプロトコル（ＩＰ）マルチキャスト宛先アドレスを有するあらゆるデータパケットの、スイッチング装置のリダイレクトポートへのリダイレクションを防ぐ、
ことを特徴とする請求項５に記載の方法。
【請求項１１】

命令セットを記憶したマシン可読媒体であって、前記命令セットは、１又はそれ以上のプロセッサにより実行された場合、該１又はそれ以上のプロセッサに、
ネットワーク内のスイッチング装置において、前記ネットワーク内の１又はそれ以上の宛先へ送信すべきデータパケットを受信するステップと、
前記ネットワーク状態が、前記受信したデータパケットが前記スイッチング装置のリダイレクトポートに関連していることを示すかどうかを判定するステップと、
を含み、前記リダイレクトポートは、リダイレクトされたデータパケットを、該リダイレクトされたデータパケットの分析の結果に基づいて前記スイッチング装置へ戻すように構成されたネットワークサービスに関連し、
前記データパケットを前記スイッチング装置からフラッディングすべきかどうかを判定するステップと、
前記受信したデータパケットが前記スイッチング装置からフラッディングすべきと判定された場合、前記リダイレクトポートを、前記受信したデータパケットの前記フラッディングから切り離して、前記受信したデータパケットを前記スイッチング装置からフラッディングするステップと、
前記受信したデータパケットが前記リダイレクトポートに関連していることを前記ネットワーク状態が示していると判定され、かつ前記データパケットを前記スイッチング装置からフラッディングすべきでないと判定された場合、前記受信したデータパケットを前記リダイレクトポートへリダイレクトするステップと、
を含む方法を実行させることを特徴とするマシン可読媒体。
【請求項１２】
前記ネットワーク状態は、前記受信したデータパケットのトラフィックタイプを含む、ことを特徴とする請求項１１に記載のマシン可読媒体。
【請求項１３】
前記データパケットを前記スイッチング装置からフラッディングすべきかどうかを判定するステップは、
前記受信したデータパケットがブロードキャスト媒体アクセス制御（ＭＡＣ）宛先アドレスを含んでいるどうかを判定するステップと、
前記受信したデータパケットが、転送用データベースのいずれのエントリにも対応しない媒体アクセス制御（ＭＡＣ）宛先アドレスを含んでいるかどうかを判定するステップと、
前記受信したデータパケットがインターネットプロトコル（ＩＰ）マルチキャスト宛先アドレスを含んでいるかどうかを判定するステップと、
のうちの少なくとも１つを含むことを特徴とする請求項１１に記載のマシン可読媒体。
【請求項１４】
前記受信したデータパケットを前記スイッチング装置からフラッディングするステップは、前記受信したデータパケットを前記スイッチング装置のいずれのリダイレクトポートへも送信せずに実行されることを特徴とする請求項１１に記載のマシン可読媒体。
【請求項１５】
前記リダイレクトポートは、仮想ローカルエリアネットワーク（ＶＬＡＮ）をサポートするポートの組から切り離されることを特徴とする請求項１４に記載のマシン可読媒体。
【請求項１６】
前記受信したデータパケットが前記スイッチング装置のリダイレクトポートに関連していることを前記ネットワーク状態が示していると判定され、当該方法は、前記データパケットを前記スイッチング装置のリダイレクトポートへ送信すべき旨の指示を、前記データパケットを前記スイッチング装置の少なくとも１つの他のポートへフラッディングすべき旨の指示に置き換えるステップをさらに含む、
ことを特徴とする請求項１４に記載のマシン可読媒体。
【請求項１７】
リダイレクトされたデータパケットを、該リダイレクトされたデータパケットの分析に

基づいてスイッチング装置へ戻すように構成されたネットワークサービスに関連するリダイレクトポートと、
データパケットを前記スイッチング装置からフラッディングすべきかどうかを判定するためのフローハンドラと、
前記データパケットが前記リダイレクトポートに関連していることを、ネットワーク状態が示すかどうかを判定するためのトラフィックセレクタと、
前記トラフィックセレクタと前記フローハンドラに連結されたスイッチングメカニズムと、
を備え、
前記データパケットが前記リダイレクトポートに関連していることを前記ネットワーク状態が示していると判定され、かつ前記データパケットを前記スイッチング装置からフラッディングすべきでないと判定された場合、前記スイッチングメカニズムは、前記データパケットを前記リダイレクトポートへ送信し、
前記受信したデータパケットが前記スイッチング装置からフラッディングすべきと判定された場合、前記スイッチングメカニズムは、前記受信したデータパケットを前記スイッチング装置からフラッディングし、前記スイッチングメカニズムは、前記リダイレクトポートを前記受信したデータパケットの前記フラッディングから切り離すことを特徴とするスイッチング装置。
【請求項１８】
前記ネットワーク状態は、前記データパケットのトラフィックタイプを含む、
ことを特徴とする請求項１７に記載のスイッチング装置。
【請求項１９】
前記フローハンドラが前記データパケットを前記スイッチング装置からフラッディングすべきかどうかを判定することは、
前記受信したデータパケットがブロードキャスト媒体アクセス制御（ＭＡＣ）宛先アドレスを含んでいるどうかを前記フローハンドラが判定すること、
前記受信したデータパケットが、転送用データベースのいずれのエントリにも対応しない媒体アクセス制御（ＭＡＣ）宛先アドレスを含んでいるかどうかを前記フローハンドラが判定すること、
前記受信したデータパケットがインターネットプロトコル（ＩＰ）マルチキャスト宛先アドレスを含んでいるかどうかを前記フローハンドラが判定すること、
のうちの少なくとも１つを含むことを特徴とする請求項１７に記載のスイッチング装置。
【請求項２０】
前記スイッチングメカニズムは、前記リダイレクトポートを仮想ローカルエリアネットワーク（ＶＬＡＮ）をサポートするポートの組から除外することを特徴とする請求項１９に記載のスイッチング装置。
【請求項２１】
前記受信したデータパケットが前記リダイレクトポートに関連していることを前記ネットワーク状態が示していることを判断し、前記スイッチングメカニズムは、前記データパケットを前記スイッチング装置のリダイレクトポートへ送信すべき旨の指示を、前記データパケットを前記スイッチング装置の少なくとも１つの他のポートへフラッディングすべき旨の指示に置き換えることを特徴とする請求項１９に記載のスイッチング装置。
【請求項２２】
スイッチング装置を備えたシステムであって、当該スイッチング装置は、
複数のポートと、
リダイレクトポートと、
前記複数のポートと、前記リダイレクトポートに連結されたスイッチングメカニズムと、
前記リダイレクトされたデータパケットを前記スイッチング装置のリダイレクトポートから受信し、さらに、前記リダイレクトされたデータパケットの分析に基づいて前記リダ

イレクトされたデータパケットを前記スイッチング装置へ戻すためのネットワークサービスと、
前記スイッチング装置を前記ネットワークサービスに結合するためのシリアルバスと、
を備え、
前記データパケットが前記リダイレクトポートに関連していることをネットワーク状態が示していると判定され、かつ前記データパケットを前記スイッチング装置からフラッディングすべきでないと判定された場合、前記スイッチングメカニズムは、前記データパケットを前記リダイレクトポートへリダイレクトし、
前記受信したデータパケットが前記スイッチング装置からフラッディングすべきと判定された場合、前記スイッチングメカニズムは、前記受信したデータパケットを前記スイッチング装置からフラッディングし、前記スイッチングメカニズムは、前記リダイレクトポートを、前記受信したデータパケットの前記フラッディングから切り離し、
前記受信したデータパケットがブロードキャスト宛先アドレスを含んでいると判定され、または、前記受信したデータパケットが、転送用データベースのいずれのエントリにも対応しないブロードキャスト宛先アドレスを含んでいると判定された場合、前記データパケットは前記スイッチング装置の前記複数のポートからフラッディングされる、
ことを特徴とするシステム。
【請求項２３】
前記ネットワーク状態が、前記データパケットのトラフィックタイプを含む、
ことを特徴とする請求項２２に記載のシステム。
【請求項２４】
前記データパケットが、ブロードキャスト媒体アクセス制御（ＭＡＣ）宛先アドレスを含まないか、
前記データパケットが、前記スイッチング装置の転送先データベースのいずれのエントリにも対応しない媒体アクセス制御（ＭＡＣ）宛先アドレスを含まないか、
前記データパケットが、インターネットプロトコル（ＩＰ）マルチキャスト宛先アドレスを含まない場合、
前記データパケットを前記スイッチング装置からフラッディングすべきでない、
ことを特徴とする請求項２２に記載のシステム。
【請求項２５】
前記リダイレクトポートは、仮想ローカルエリアネットワーク（ＶＬＡＮ）をサポートするポートの組から除外されることを特徴とする請求項２２に記載のシステム。
【請求項２６】
前記受信したデータパケットが前記リダイレクトポートに関連していることを前記ネットワーク状態が示していると判定され、前記スイッチングメカニズムは、前記データパケットを前記スイッチング装置のリダイレクトポートへ送信すべき旨の指示を、前記データパケットを前記スイッチング装置の少なくとも１つの他のポートへフラッディングすべき旨の指示に置き換えることを特徴とする請求項２２に記載のシステム。
【請求項２７】
前記スイッチングメカニズムが、前記データパケットを前記スイッチング装置のリダイレクトポートへ送信すべき旨の前記指示を、前記データパケットを前記スイッチング装置の少なくとも１つの他のポートへフラッディングすべき旨の前記指示に置き換えることは、前記スイッチングメカニズムが、シーケンス制御テーブル（ＳＣＴ）に記憶された１又はそれ以上のコマンドを実行して、前記スイッチング装置の少なくとも１つの他のポートの識別子を取り出すことを含む、
ことを特徴とする請求項２６に記載のシステム。
【請求項２８】
前記受信したデータパケットが前記リダイレクトポートに関連していることを前記ネットワークの状態が示していると判定され、
前記スイッチングメカニズムは、前記スイッチング装置のリダイレクトポートのアクセ

ス制御リストの規則を実施し、該規則は、インターネットプロトコル（ＩＰ）マルチキャスト宛先アドレスを有するあらゆるデータパケットの、スイッチング装置のリダイレクトポートへのリダイレクションを防ぐ、
ことを特徴とする請求項２２に記載のシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、一般にスイッチドネットワークにおけるデータパケットのポートリダイレクションに関する。より具体的には、本発明の実施形態は、ネットワークサービスに関連するスイッチング装置のリダイレクトポートへデータパケットを選択的にリダイレクトする。
【背景技術】
【０００２】
マルウェアの量及び多様性は、スイッチドネットワーキングシステムをかつて無いほどの脅威にさらしている。スイッチドネットワーキングシステムの保護は、スイッチング行為を修正するために、到来するネットワークトラフィック上のデータを収集し評価できるインテリジェントネットワークスイッチにより高められる。ネットワークトラフィックフローに物理的に従わずに、ネットワークスイッチにセキュリティ及び／又はその他のサービスを提供する侵入防止システム（「ＩＰＳ」）などの外部ネットワークサービスを活用することにより、インテリジェントスイッチングの利点はさらにまた高められる。ネットワーキング技術では、「ＩＰＳ」とは、アクセス制御を行って装置をセキュリティ脅威から保護することができるメカニズムのことを意味すると理解される。
【０００３】
ネットワークスイッチ及び／又はその他のネットワークスイッチング装置は、１又はそれ以上のネットワーク状態に基づいてネットワークトラフィックを様々にフィルタリングし、リダイレクトし、ブロックし、及び／又は転送することができる。例えば、特定のデータパケットを検査のためにＩＰＳなどの外部ネットワークサービスへリダイレクトするようにスイッチを構成することができ、このリダイレクトは、（データパケットのメールメッセージサービスなどの）データパケットのトラフィックタイプに基づく。十分な検査後、この外部サービスは、リダイレクトされたデータパケットをスイッチへ戻して、この検査済みのデータパケットの元々の宛先への送信を続行することができる。
【０００４】
データパケットを「ｂｕｍｐ－ｉｎ－ｔｈｅ－ｗｉｒｅ」ネットワークサービスへリダイレトすることは複雑な場合があり、この場合、１又はそれ以上のデータパケットがスイッチング装置から「フラッディング」されることになる。本明細書で使用する場合、データパケットをスイッチからフラッディングするということは、一般に特定の１又はそれ以上のネットワーク経路でデータパケットを送信すべき旨の指示が無い場合に、代わりに多くのネットワーク経路でデータパケットを送信することを意味する。データリンク層における媒体アクセス制御（ＭＡＣ）ブロードキャスティング及びネットワーク層におけるインターネットプロトコル（ＩＰ）マルチキャスティングは、スイッチング装置からネットワークトラフィックをどのようにフラッディングできるかを示すほんの２つの例である。
【先行技術文献】
【非特許文献】
【０００５】
【非特許文献１】２００１年８月出版、Ａｌｂａｎｎａ，Ｚ．，Ａｌｍｅｒｏｔｈ，Ｋ．，Ｍｅｙｅｒ，Ｄ．，及びＭ．ＳｃｈｉｐｐｅｒによるＩｎｔｅｒｎｅｔ Ａｓｓｉｇｎｅｄ Ｎｕｍｂｅｒｓ Ａｕｔｈｏｒｉｔｙ（ＩＡＮＡ）の「ＩＰｖ４マルチキャストアドレス割り当てのためのＩＡＮＡガイドライン」、Ｂｅｓｔ Ｃｕｒｒｅｎｔ Ｐｒａｃｔｉｃｅ（ＢＣＰ）５１、Ｒｅｑｕｅｓｔ ｆｏｒ Ｃｏｍｍｅｎｔｓ（ＲＦＣ）３１７１

【発明の概要】
【０００６】
以前にリダイレクトされたデータパケットをフラッディングすることにより、誤ってデータパケットのコピーが送信される可能性がある。例えば、リダイレクトされたデータパケットがＩＰＳからスイッチへ戻された後にスイッチからフラッディングされた場合、戻されたデータパケットが、スイッチング装置が最初にデータパケットを受信したネットワーク経路に沿って誤って返送される可能性がある。これとは別に、或いはこれに加えて、戻されたデータパケットが、このデータパケットを戻した同じネットワークサービスへ誤って返送される可能性があり、これによりネットワークにおけるデータパケットループが生じる。ネットワークループ及びその他の誤ったデータパケットの送信により、結果として送信時間が遅くなるとともにネットワークパフォーマンスが低下する。これまで、フラッディングされるトラフィックの問題が、スイッチング装置が受信したデータパケットを分析するネットワークサービスに関連するスイッチング装置のポートへの、データパケットのデータリンク層におけるリダイレクトの実施を阻んできた。
【０００７】
本発明の様々な実施形態を添付図面の図に限定的な意味ではなく一例として示す。
【図面の簡単な説明】
【０００８】
【図１】本発明の１つの実施形態による、スイッチング装置がデータパケットのポートリダイレクトを実行できるシステムを示すブロック図である。
【図２】本発明の１つの実施形態による、データパケットのポートリダイレクトを実行できるスイッチのメカニズムを示すブロック図である。
【図３】本発明の１つの実施形態による、リダイレクトできるデータパケットのコンテンツを示すパケット図である。
【図４Ａ】本発明の１つの実施形態によるポートリダイレクションの方法を示すフロー図である。
【図４Ｂ】本発明の別の実施形態によるポートリダイレクションの方法を示すフロー図である。
【発明を実施するための形態】
【０００９】
図１は、本発明の１つの実施形態による、スイッチング装置１１０がデータパケットを選択的にリダイレクトできるシステム１００を示す図である。システム１００は、様々な「ｂｕｍｐ－ｉｎ－ｔｈｅ－ｗｉｒｅ」構成のいずれかを表すことができ、受信したネットワークトラフィックから得られるデータパケットを、外部ネットワークサービス１２０に関連するスイッチング装置１１０のポートへ少なくとも一時的に選択的にリダイレクトすることができる。ネットワーク１３０及び１４０はそれぞれ、スイッチング装置１１０がデータパケットを受信する先のソースネットワーク、及びスイッチング装置１１０が受信したデータパケットを選択的に送信する先の宛先ネットワークを表す。本発明の１つの実施形態による、スイッチング装置１１０が受信したデータパケットをいかにしてリダイレクトできるかの実証に役立つように、ネットワーク１３０及び１４０を異なるネットワークとして示している。当業者であれば、スイッチング装置１１０は、ネットワークトラフィックをネットワーク１４０からネットワーク１３０へ送信及び／又は選択的にリダイレクトすることもできると理解するであろう。ネットワーキング技術における当業者であれば、ネットワーク１３０及び１４０は、単一のより大きなネットワーク（図示せず）の任意の部分を表すものであってもよく、これにスイッチング装置１１０も属するということも理解するであろう。例えば、ネットワーク１３０、１４０を、１又はそれ以上のその他のネットワーク経路（図示せず）を介して追加の装置、ネットワークに、及び／又は互いにさらに接続することができる。
【００１０】
ネットワークスイッチ１１０は、ネットワークスイッチング機能を有するあらゆるネッ

トワーク装置を表す。例えば、スイッチング装置１１０は、開放型システム間相互接続（ＯＳＩ）レイヤ２（Ｌ２）に代表されるようなデータリンク層においてデータパケットをスイッチするためのメカニズムを含むことができる。いくつかの実施形態では、スイッチング装置１１０が、ネットワークの状態に少なくとも部分的に基づいてデータパケットをスイッチするためのインテリジェントスイッチングメカニズムを含むことができる。スイッチング装置１１０は、単純なＬ２ネットワークスイッチ、或いは追加のルーティング機能又はその他のネットワーキング機能を含むことができる様々なその他の装置のいずれであってもよい。例えば、スイッチング装置１１０は、マルチレイヤスイッチ（ＭＬＳ）、ハイブリッドＯＳＩ　Ｌ２／Ｌ３スイッチルータ、又はスイッチング機能を有するその他のネットワーク装置であってもよい。説明を簡潔にするために、本明細書では本発明の実施形態を「スイッチ」に関して説明する。当業者であれば、本発明の実施形態に関するスイッチの意味を広げて、より一般的に、上述した種類のスイッチング装置に適用できることを理解するであろう。

【００１１】

スイッチング装置１１０は、ネットワークサービス１２０にさらに接続される。ネットワークサービス１２０は、スイッチング装置１１０が受信した１又はそれ以上のデータパケットの分析に少なくとも部分的に基づく様々なセキュリティ又はその他のサービスのいずれであってもよい。ネットワークサービス１２０は、スイッチング装置１１０が受信した１又はそれ以上のデータパケットを分析するためのハードウェア、ソフトウェア、仮想機械（バーチャル・マシン）、及び／又はその他の手段のあらゆる組合せを含むことができる。１又はそれ以上のデータパケットの分析は、例えば、個々のデータパケットのコンテンツの分析及び／又はリダイレクトされたネットワークトラフィックの時間に伴う統計分析を含むことができる。１つの実施形態では、ネットワークサービス１２０が侵入防止サービス（ＩＰＳ）を提供して、スイッチング装置１１０のネットワークトラフィックにおいて発見されるセキュリティ脅威を検出することができる。例えば、ネットワークトラフィックのためのサービス品質（ＱｏＳ）を実現する際に、ネットワークサービス１２０が行う分析を参照することができる。例えば、ネットワークサービス１２０を使用して、スイッチ１１０におけるメカニズムにより実現されるサービス品質をサポートすることができる。説明を簡潔にするために、本明細書では本発明の実施形態を「ＩＰＳ」に関して説明する。当業者であれば、本発明の実施形態に関するＩＰＳの意味を広げて、より一般的に、上述した種類のネットワークサービスに適用できることを理解するであろう。

【００１２】

スイッチング装置１１０及びネットワークサービス１２０が、システム１００における多くの「ｂｕｍｐ－ｉｎ－ｔｈｅ－ｗｉｒｅ」構成のうちの１つのみを表すことができる点に留意されたい。例えば、ネットワークサービス１２０の構成に類似した構成でスイッチング装置１１０に接続された１又はそれ以上のその他のネットワークサービス（図示せず）により、スイッチング装置１１０をサポートすることができる。さらに、ネットワークサービス１２０を、他のネットワーク装置で運ばれたネットワークトラフィックのための「ｂｕｍｐ－ｉｎ－ｔｈｅ－ｗｉｒｅ」として構成することもできる。説明を簡潔にするために、本明細書における本発明についての説明は、図１に示す例示的なシステム１００の変形例に限定するが、これらの説明を広げて、あるスイッチング装置が受信したデータパケットを分析するあらゆる「ｂｕｍｐ－ｉｎ－ｔｈｅ－ｗｉｒｅ」ネットワークサービスに一般的に適用することができる。

【００１３】

本発明の実施形態は、ＩＰＳに関連するポートへの、データパケットのデータリンク層におけるリダイレクトを選択的に実行する。説明を明確にするために、本明細書では「データパケットをリダイレクトすること」とは、データパケットを送信するはずだった１又はそれ以上の宛先経路のいずれかでデータパケットを送信するのではなく、少なくとも一時的に異なるネットワーク経路で別様にデータパケットを送信することを意味する。換言すれば、データパケットは、非宛先経路で「リダイレクト」されない場合、異なる宛先経

路へ「送信」されると言える。スイッチング装置１１０が、データパケットを別の経路へリダイレクトすることを最終的に決定できるとしても、このデータパケットは、代わりに宛先経路へ「送信すべき」データパケットであると説明することができる。同様に、例えばスイッチング装置１１０が、データパケットを宛先経路へ送信することを最終的に決定できるとしても、このデータパケットは、代わりにリダイレクトポートへ「リダイレクトすべき」データパケットであると説明することができる。

【００１４】

スイッチング装置１１０がデータパケットをスイッチング装置１１０の特定のポートへ選択的にリダイレクトする限りにおいて、データリンク層におけるリダイレクトを、本明細書では代わりに「ポートリダイレクト」と呼ぶことができる。１０５において、スイッチ１１０が、ネットワーク１４０における１又はそれ以上の宛先へ送信すべきデータパケットをネットワーク１３０から受信する。スイッチング装置１１０から、データパケットをネットワーク１４０へ送信することができ、この場合、スイッチング装置１１０は、最初にデータパケットをネットワークサービスへリダイレクトせずに、ネットワーク１４０における１又はそれ以上のデータパケットの宛先に関連するスイッチング装置１１０のポートに直接データパケットを切り替える。

【００１５】

或いは、スイッチング装置１１０から、データパケットを１１５においてネットワークサービス１２０へリダイレクトすることができ、この場合、スイッチング装置１１０のスイッチングメカニズムは、データパケットをネットワーク１４０へ送信するのではなく、ネットワークサービス１２０に関連するスイッチング装置１１０のリダイレクトポートにデータパケットを切り替える。本明細書で説明するように、このデータパケットのリダイレクティング１１５は、ネットワーク状態に少なくとも部分的に基づくことができる。データパケットが、スイッチング装置１１０からネットワークサービス１２０に関連するリダイレクトポートへリダイレクトされた場合、ネットワークサービス１２０が、リダイレクトされたデータパケットの分析を行うことができる。行われた分析の結果に少なくとも部分的に基づいて、リダイレクトされたデータパケットを１２５においてネットワークサービス１２０からスイッチング装置１１０へ戻すことができる。本発明の１つの実施形態では、いずれの戻されたデータパケットも、スイッチング装置１１０からネットワーク１４０における１又はそれ以上の宛先の少なくとも１つへ送信することができる。図１では、通信１３５は、一般にネットワーク１４０へのデータパケットの転送を表す。例えば、通信１３５は、（１）受信したデータパケットのスイッチング装置１１０からネットワーク１４０への送信、或いは（２）戻されたデータパケットのスイッチング装置１１０からネットワーク１４０への送信を表すことができる。

【００１６】

ネットワークトラフィックをネットワークサービス１２０へリダイレクトするために、スイッチング装置１１０は、本明細書ではリダイレクトポートと呼ぶ、ネットワークサービス１２０に関連する少なくとも１つのポートを含むことができる。それぞれネットワークサービス１２０に関連するスイッチング装置の単一のリダイレクトポート、或いは別個の出口及び入口リダイレクトポートのいずれかにおいて通信１１５及び１２５を行うことができる。本発明の１つの実施形態では、スイッチング装置１１０が受信したデータパケットをリダイレクトポートへリダイレクトするか否かは、ネットワーク状態に少なくとも部分的に基づく。換言すれば、ネットワーク状態の存在により、受信したデータパケットがスイッチング装置１１０のリダイレクトポートに関連しており、このポートがさらにネットワークサービス１２０に関連していることをスイッチング装置１１０に示すことができる。

【００１７】

１つの実施形態では、ネットワーク状態はデータパケット自体の状態であってもよい。例えば、ネットワーク状態は、データパケットが表すトラフィックの種類であってもよい。データパケット自体に含まれる情報により、このデータパケットのトラフィックタイプ

を示すことができる。例えば、データパケットのトラフィックタイプは、以下に限定されるわけではないが、データパケットのネットワークソース識別子、データパケットのネットワーク宛先識別子、データパケットのプロトコルタイプ、データパケットのサービスタイプ、及び／又はデータパケットに関連するアプリケーションを含む情報に基づくことができる。データリンク層情報、ネットワーク層情報及び／又はデータパケット内のその他のＯＳＩレイヤ情報により、トラフィックタイプを示すことができる。これとは別に、或いはこれに加えて、データパケットのトラフィックタイプは、ネットワークにおけるデータパケットの通信に関する情報を含むことができる。例えば、データパケットのトラフィックタイプは、以下に限定されるわけではないが、データパケットを受信したポート、データパケットを受信した時間、及び／又はデータパケットの受信が結果として何らかのしきい値を超えたという指標を含む情報に様々に基づくことができる。例示を目的とするために、本明細書における本発明についての説明は、データパケット自体のトラフィックタイプであるデータパケットのリダイレクションに関するネットワーク状態の典型的な例で行う。これらの説明を広げて、他の種類のネットワーク状態について言及できることを理解されたい。

【００１８】

ネットワーク状態により、データパケットがネットワークサービス１２０へリダイレクト１１５される場合、ネットワークサービス１２０が提供するサービスの一部としてデータパケットの分析を行うことができる。分析の結果に少なくとも部分的に基づいて、リダイレクトされたデータパケットをネットワークサービス１２０により遮断する（図示せず）ことができる。或いは、１２５において、分析の結果に少なくとも部分的に基づいてデータパケットをスイッチング装置１１０へ戻すことができる。データパケットが戻される場合、スイッチング装置１１０は、戻されたデータパケットにいずれかの追加の分析又は他の操作を行うことができる。その後、スイッチング装置１１０は、戻されたデータパケットを遮断する（図示せず）か、或いは１３５においてネットワーク１４０における１又はそれ以上の宛先へ転送するかのいずれかを行うことができる。

【００１９】

図２は、本発明の１つの実施形態を実施するための構成２００を示す図である。例示を目的として、構成２００は、図１の特徴を上回る追加の特徴を示している。本発明の他の実施形態は、図２に示す構成に代わる構成、或いはこれに追加を加えた構成を含むことができる点に留意されたい。１又はそれ以上のセキュリティサービスによる検査のためにネットワークトラフィックを選択的にリダイレクトできるスイッチング装置によって本発明の１つの実施形態を実施することができ、この場合、リダイレクトは何らかのネットワーク特性識別子のリストに基づく。１つの実施形態では、ネットワーク識別子のリストは、１又はそれ以上のポリシの組による修正を受けることができる。図１のシステム１００のスイッチング装置１１０のように、構成２００におけるスイッチ２０１は、データパケットを、受信したネットワークトラフィックからＩＰＳ２１１に関連するポートへ選択的にリダイレクトすることができる。本発明の１つの実施形態では、スイッチ２０１は、データパケットの選択的ポートリダイレクションのための論理の少なくとも一部を実行するためのプロセッサ２３０を含むことができる。例えば、プロセッサ２３０は、プロセッサ２３０により実行された場合にＩＰＳ２１１に関連するスイッチ２０１上のポートへのデータパケットの選択的ポートリダイレクションの少なくとも一部をプロセッサ２３０に実行させる１又はそれ以上の命令を記憶できたマシン可読メモリ２３１を含むことができる。これとは別に、或いはこれに加えて、スイッチ２０１は、ハードウェアを使用してデータパケットの選択的ポートリダイレクションの少なくとも一部を実行することができる。

【００２０】

構成２００によれば、スイッチ２０１は、ＩＰＳ２１１が以前にネットワークにとって安全であると分析及び判定したことのあるフローを識別するフローハンドラ２０２において（例えば、ポート、バス接続又はその他のインターフェイスを介して）トラフィック２２０を受信することができる。フローハンドラ２０２は、例えば、データパケットをスイ

ッチ２０１からフラッディングすべきかどうかを判定するためのメカニズムをさらに含むことができる。或いは、フローハンドラ２０２とは別のスイッチ２０１の専用コンポーネント（図示せず）がこの判定を行ってもよい。このようなフローから得られるデータパケットは、さらなる中断を伴わずにスイッチ２０１を介して直接転送される。そうでなければ、他のあらゆるデータパケット２２２をトラフィックセレクタ２０８へ送信してもよい。トラフィックセレクタ２０８は、ネットワーク状態が、受信したデータパケットがスイッチング装置のリダイレクトポートに（トラフィックを運ぶなど）関連していることを示すかどうかを判定することができる。本発明の特定の実施形態に応じて、トラフィックセレクタ２０８は、データパケットがスイッチング装置からフラッディングすべきデータパケットであるかどうかをさらに判定することができる。１つの実施形態では、トラフィックセレクタ２０８は、ＩＰＳ２１１に関連するスイッチ２０１上のポートへリダイレクトするために、データパケット２２２のトラフィックタイプを識別することができる。１つの例では、フロー毎、又は（電子メール、ウェブ、ＳＱＬ、ＦＴＰなどの）サービス毎にリダイレクトすべきトラフィックタイプの識別を行うことができる。

【００２１】

データパケット２２２が、ＩＰＳ２１１に関連するポートと関連性があると示されたトラフィックタイプであることに少なくとも部分的に基づいて、このデータパケットを前記「リダイレクトポート」へリダイレクトすることができる。トラフィックセレクタ２０８は、スイッチ２０１においてデータパケットをリダイレクト２２３する形で示している。或いは、トラフィックセレクタ２０８におけるメカニズムとは別のスイッチ２０１の専用スイッチングメカニズム（図示せず）がこのリダイレクティング２２３を行って、受信したデータパケットがリダイレクトポートに関連することをネットワーク状態が示すかどうかを判定することができる。

【００２２】

ＩＰＳは、例えば、同軸ケーブル、ツイストペアケーブル、パラレルバス、シリアルバスなどのいずれかを介して、リダイレクトされたデータ２２３を受信することができる。トラフィックセレクタ２０８は、さらにパケット検査を行うためにフラグを立てられたフロー及び／又はサービスを識別するエントリを有するテーブル２０９を含むことができる。この場合、テーブル２０９内のエントリに適合するサービスに関連するデータパケットを、ＩＰＳ２１１に関連するスイッチ２０１のポートへリダイレクトすることができる。テーブル２０９は、キャッシュ又はメモリ内に実装することができる。１つの実施形態では、テーブル２０９が連想メモリ（ＣＡＭ）内に実装される。別の実施形態では、ターナリＣＡＭ、すなわちＴＣＡＭを使用してテーブルを実装する。

【００２３】

ＩＰＳ２１１は、リダイレクトされたトラフィック２２３を分析して、特定のフローが（安全な、脅威ではないものなどの）良いものであるか、或いは（ウィルス、ワーム、サービス妨害（ＤｏＳ）攻撃などの）悪いものであるかを判定することができる。例えば、ＩＰＳ装置が、（フローＡなどの）特定のフローが良いフローであると判定することがある。良いフロー２２４から得られるデータパケットをパケットフォワーダ２３２へ戻し、戻されたデータパケットに対してここでさらなる分析及び／又はその他の操作を実行することができる。何らかの追加の分析又はその他の操作の後、パケットフォワーダ２３２は、戻されたデータパケットを遮断するか、或いはスイッチ２０１のアウトバウンドネットワークトラフィック２２５として送信するかのいずれかを行うことができる。ＩＰＳ２１１は、フローＡを良いフローと見なす通知をフローハンドラ２０２へ送信することができる。スイッチ２０１は、フローＡのフロー識別子をメモリ２３１に記憶することができる。従って、フローＡのフロー識別子がメモリに記憶されると、フローＡに関連するその後受信されるいずれのパケットも、フローハンドラ２０２においてメモリ２３１内のフローＡ識別子との適合を生じることができ、これによりスイッチ２０１が、フローＡパケットをトラフィックセレクタ２０８を通過させることなく、或いはフローＡパケットをＩＰＳ２１１へリダイレクトすることなく、２２１においてフローＡパケットを転送し、２２５

においてスイッチ２０１を通り抜けさせることができるようになる。

【００２４】

フローハンドラ２０２からトラフィックセレクタ２０８へ渡されるデータに関しては、テーブル２０９を使用してサービス及び／又はデータのフローを識別し、脆弱性検査を行うためのフラグを立てられたサービス及び／又はフローとこれらを比較する。現在の全体的なスイッチトラフィック状態に基づいて、テーブル２０９内のエントリを動的／自動的に更新することができる。センサ２１０により、全体的なスイッチトラフィック状態を検出することができる。１つの実施形態では、スイッチ２０１が、フローハンドラ２０２からトラフィックセレクタ２０８に渡されたトラフィックをモニタするための第１のセンサ２１０と、トラフィックセレクタ２０８とＩＰＳ２１１との間のトラフィックをモニタするための第２のセンサ２１０とを含むことができる。他の実施形態では、スイッチ２０１が、トラフィックをモニタし状態を検出するために、スイッチ２０１内の様々なロケーションにおける１又はそれ以上のセンサのあらゆる組み合わせを含むことができる。

【００２５】

センサ２１０は、１又はそれ以上のフローに関する累積パケットカウント、ある時間間隔にわたるパケットカウントの変化又は差分、２つの累積パケットカウントの比率、及び／又はある時間間隔に渡る２つの異なるパケットカウントの変化又は差分の比率などの様々なパケット統計値を収集することができる。通常、（電子メール、ＳＱＬ、ＦＴＰなどの）サービスが標準ポート番号を使用して通信を行うことを考えれば、センサは、サービスタイプに基づいて、パケットカウント、変化したトラフィックレート、及び比率を追跡することもできる。センサ２１０はまた、フローに関連するリバース／アウトバウンドトラフィックに関する統計値を収集することもできる。例えば、１つの実施形態では、センサが、特定のフローに関して受信される到来する送信制御プロトコル（ＴＣＰ）同期（ＳＹＮ）パケットの数を追跡する。この一方で、センサはまた、フローに関連するアウトバウンドＴＣＰ　ＳＹＮ－確認応答（ＳＹＮ－ＡＣＫ）パケットの数を追跡することもできる。

【００２６】

センサ２１０は、検出した状態を選択マネージャ２０６に報告することができる。選択マネージャ２０６は１又はそれ以上のポリシの組２０７を含む。このポリシの組２０７をポリシデータベースとして実装することができる。ポリシの組２０７の規則及び／又はしきい値を使用して、（トラフィックにおけるスパイク、トラフィック輻輳などの）検出した状態を分析し、検出した状態に関連するサービス又はフローがＩＰＳ２１１によるさらなる検査を必要とするかどうかを決定する。１つの実施形態では、センサ２１０が、スイッチ２０１に入る電子メールトラフィックの異常な増加を検出することができる。この異常が、規則を呼び起こすか、或いはポリシの組２０７の１つのしきい値を超えた場合、選択マネージャ２０６は、電子メールトラフィックを含むようにテーブル２０９を自動的に更新することができる。従って、トラフィックセレクタ２０８が受信するその後のあらゆる電子メールトラフィックを、脆弱性検出を行うためにＩＰＳ２１１へリダイレクトできるようになる。別の実施形態では、センサ２１０が、リダイレクトされたトラフィック２２３におけるＩＰＳ２１１の限られた帯域幅に起因する輻輳を検出することができる。この場合、選択マネージャ２０６が、ＩＰＳ２１１へ流れるリダイレクトされたトラフィック２２３を低減させる必要に応じて、１又はそれ以上のサービスを取り除くことによりテーブル２０９を自動的に修正することができる。

【００２７】

スイッチ２０１の動作をマニュアル設定したり、及び／又は中断したりする必要なくトラフィック選択ポリシ２０７を動的に更新できるようにするために、本発明の実施形態は、スイッチ２０１が使用する異常検出情報を受信し処理するための異常受信器２０５を含むことができる。本明細書で使用する「異常検出」とは、ネットワークに対するセキュリティリスクの可能性を判定するために行われる、ネットワーキング技術で周知の様々な分析方法のいずれかを意味するものと理解される。単一のデータパケットのコンテンツの分

析から、及び／又は数多くのデータパケット、フロー、サービスなどにわたる時間に伴うパターンの分析などから異常検出情報を生成することができる。例えば、異常受信器２０５において受信される種類の異常検出情報として、以下に限定されるわけではないが、マルウェア記述、署名ベースの侵入検出データ、プロファイルベースの侵入検出データ、トラフィックパターン照合データ、ステートフルトラフィックパターン照合データ、プロトコルデコードベースの分析データ、ヒューリスティックベースの分析データなどを挙げることができる。

【００２８】

異常受信器２０５で受信されるような異常検出情報を様々な実施形態において使用して、トラフィックセレクタ２０８、セキュリティ規則エンジン２０３及び／又はＩＰＳ２１１などの、ネットワークトラフィックにおけるデータを処理するメカニズムへ伝達される行為を生み出すことができる。図２の例では、選択マネージャ２０６が、受信した異常検出情報に基づいて、いかなる様々なこのような行為及び／又は前記行為を行うことができる様々な対応する状態をも生み出すことができる。データ処理行為を行うことができるかどうか、及び／又はどのように行うことができるかを判定するために使用できる状態の１つの例に、ある警戒レベルの状態がある。例えば、トラフィックセレクタ２０８などの、スイッチ２０１におけるメカニズムの１つが、構成２００の少なくとも一部に対する存在するセキュリティ脅威を示す警戒レベル（図示せず）へのアクセス権を記憶し、或いは別様に有することができる。受信したトラフィック２２２の処理において取る行為を決定する際に、トラフィックセレクタ２０８は、この警戒レベルを、選択マネージャ２０６が提供する状態と比較することができる。例えば接続２３１及び／又は接続２３０を介して、ネットワークトラフィックにおけるデータを処理するメカニズムへこのような行為及び／又は状態を選択的に伝達することができる。接続２３１は、例えば、同軸ケーブル、ツイストペアケーブル、パラレルバス、シリアルバスなどのいずれであってもよい。

【００２９】

異常受信器２０５において受信される異常検出情報は、様々なソースのいずれからも生じる可能性があり、これらの選択を例示として図２に示す。まず、図２は、ＩＰＳ２１１が、異常受信器２０５に異常検出情報を、この場合は選択マネージャ２０６への接続２３１を介して提供することを示している。次に、異常受信器２０５に異常検出情報を提供できるフローハンドラ２０２に、この場合は選択マネージャ２０５への接続２３０を介して接続されたセキュリティ規則エンジン２０３を含むようにスイッチ２０１を示している。セキュリティ規則エンジン２０３は、例えば、トラフィック２２０を分析し、該トラフィック分析に基づいてセキュリティ規則の組２０４を引き出し、及び／又は実行することにより、フローハンドラ２０２における１次脅威検出及び軽減を行うためのモジュールであってもよい。このようなセキュリティ規則エンジン２０３の例に、ネットワークトラフィック分析及び規則２０４などのセキュリティ規則に基づいて、サービス及び／又はフローをフィルタリング、リダイレクト、遮断、及び／又は転送するかどうかを決定することができるＥｘｔｒｅｍｅ　Ｎｅｔｗｏｒｋｓ（商標）ＣＬＥＡＲ－Ｆｌｏｗセキュリティ規則エンジンがある。さらに、ＣＬＥＡＲ－Ｆｌｏｗセキュリティ規則エンジンなどのセキュリティ規則エンジン２０３はまた、このネットワークトラフィック分析がもたらすあらゆる異常検出情報を異常受信器２０５へリレーすることもできる。３番目に、異常受信器２０５が、スイッチ２０１内部の様々なセンサ２１０が提供する情報を受信することができる。図２には示していないが、さらに他の異常検出情報のソースとして、スイッチ２０１外部のネットワークトラフィックに作用するセキュリティ検出及び／又は軽減エージェントを挙げることができる。

【００３０】

異常検出情報のソースは、以下に限定されるわけではないが、異常受信器２０５によるポーリング、異常検出情報のソースによる認められている中断の送信、及び／又は同意済みのデータ通信プロトコルを含む様々な手段により、異常受信器２０５と通信することができる。異常受信器２０５が受信を行うと、異常検出情報を処理し、ポリシ２０７及び／

又はテーブル２０９の更新に使用する選択マネージャ２０６へ伝送することができる。本発明の１つの実施形態では、スイッチ２０１におけるデータ処理システムのある部分を再起動する必要なく、ポリシ２０７を動的に更新することができる。例えば、選択マネージャ２０６の機能の少なくともいくつかをモジュラーオペレーティングシステムの１又はそれ以上の独立コンポーネントとして実装することによりこれを行うことができる。モジュラーオペレーティングシステム又は同様の技術を使用して、構成２００のあるコンポーネントのランタイム動作を切り離すことにより、スイッチ２０１による受信したネットワークトラフィック２２０の処理を中断することなく、これらのコンポーネントをリアルタイムで更新することができる。このようなモジュラー方法の１つの例として、選択マネージャの少なくとも一部をＥｘｔｒｅｍｅ　Ｎｅｔｗｏｒｋｓ（登録商標）ＥｘｔｒｅｍｅＸＯＳ（商標）モジュラーオペレーティングシステムのモジュールとして実装する方法がある。

【００３１】

構成２００における特徴の全てが本発明のいくつかの実施形態の実現に必要なわけではないが、上述の特徴は、スイッチ２０１によるデータパケットのポートリダイレクションの決定において使用できる様々なネットワーク状態を示すものである。例えば、ＯＳＩレイヤ２においてポートリダイレクトが実行されている間に、リダイレクトされたデータパケットに含まれるいずれのＯＳＩレイヤ２データにも関係しないネットワーク情報により、ポートリダイレクトの基礎を成すネットワーク状態を示すことができる。

【００３２】

データパケットの処理中、スイッチ２０１は、データパケットを送信すべき場所についての現在の指示、スイッチ２０１がこれまで行ってきたデータパケットの処理に少なくとも部分的に基づく指示を記憶及び／又は更新することができる。最も簡単なケースでは、メモリ２３１が、データパケットがスイッチ２０１に届いた際のデータパケットに関連するデータのブロックを含む。データパケットを送信すべき場所についての最初の指示が、例えば、フローハンドラ２０２によるデータパケットの処理後にメモリ２３１に書き込まれる。このメモリ２３１内の現在の指示は、例えば単一のポート識別子、或いはビットマップなどのポートタグインデックス（ＰＴＩ）を含むことができ、この場合、個々の組「ビット」が、データパケットを送信すべきポートであると現在考えられているスイッチ２０１上のポートを指示する。１つの実施形態では、データパケットを送信すべき場所についての記憶された指示は、例えば、データパケットのＭＡＣ　ＤＡ或いはＩＰ　ＤＡに基づくものであってもよい。

【００３３】

データパケットが、トラフィックセレクタ２０８へ、ＩＰＳ２１１へ、及び／又はパケットフォワーダ２３２へと様々に送信される場合、例えば、メモリ２３１内のデータ上にデータパケットを送信すべき場所についてのより新しい「現在」の指示が書き込まれるか、或いは追加されたときに、データパケットを送信すべき場所についての「現在」の指示は「以前」の指示となる。１つの実施形態では、スイッチ２０１が、データパケットを送信すべき場所についての新しい現在の指示、及び１又はそれ以上の古い指示の両方を記憶することができる。最終的には、データパケットをスイッチ２０１から送信する前に、データパケットを送信すべき場所についての現在の指示をメモリ２３１から読み出して、データパケットの最終的な１又はそれ以上の宛先ポートを決定することができる。

【００３４】

本発明の様々な他の実施形態では、スイッチ２０１における個々のコンポーネントが、データパケットを送信すべき場所についての１又はそれ以上の指示の記憶を様々にサポートすることができる。例えば、フローハンドラ２０２、トラフィックセレクタ２０８、及び／又はパケットフォワーダ２３２の１又はそれ以上が、これらの固有のデータ構造を各々保持して、データパケットを送信すべき（又は送信すべきだった）場所についての１又はそれ以上の指示を様々に記憶、追跡及び又は提供することができる。本発明の１つの実施形態を実施するために、データパケットを送信すべき場所についての記憶された指示を

容易に取り出せることにより、スイッチ２０１が、本明細書で説明するようなポートリダイレクション方法をさらに迅速に実行できるようになる。

【００３５】

図３は、本発明の１つの実施形態による、ネットワークサービスに関連するポートへリダイレクトできるデータパケット３００の例示的な構造を示す図である。データパケット３００の正確なコンテンツ及び／又は構造は、データの送信及び／又はデータのカプセル化に使用する特定のプロトコルに基づいて変化することができる。データパケットは、ネットワークソースから１又はそれ以上のネットワーク宛先へ通信すべきデータのペイロード３４０を含むことができる。ネットワークを介して送信する間に、ペイロード３４０を１又はそれ以上のヘッダによりカプセル化することができる。例えば、データパケット３００は、電気電子技術者協会（ＩＥＥＥ）８０２．３に準拠するような媒体アクセス制御（ＭＡＣ）ヘッダ３１０を含むことができ、このＭＡＣヘッダ３１０は、データパケットの到来元であるソースのＭＡＣアドレスを示すＭＡＣソースアドレス３１１と、データパケットの少なくとも１つの送信する宛先を示すＭＡＣ宛先アドレス３１２と、データパケットが属する仮想ローカルエリアネットワーク（ＶＬＡＮ）を示すＶＬＡＮタグ３１３と、ペイロード３４０の長さ又はプロトコルタイプの少なくとも一方を示す長さ／タイプフィールド３１４とを含むことができる。データパケット３００はまた、インターネットプロトコル（ＩＰ）ヘッダを含むこともでき、このインターネットプロトコル（ＩＰ）ヘッダは、データパケットの到来元であるソースのＩＰアドレスを示すＩＰソースアドレス３１１と、データパケットの少なくとも１つの送信する宛先を示すＩＰ宛先アドレス３１２と、特定のデータグラムのフラグメントとしてデータパケットを示す識別フィールド３２３と、データパケットの処理に必要なパラメータを示すｔｙｐｅ ｏｆ ｓｅｒｖｉｃｅ（ＴＯＳ）フィールドと、データグラムの寿命を示すｔｉｍｅ ｔｏ ｌｉｖｅ（ＴＴＬ）フィールドと、ＩＰパケットヘッダ３２０の特定のフォーマットを示すバージョンフィールド３２６とを含むことができる。

【００３６】

ＭＡＣヘッダ３１０及びＩＰヘッダ３２０における様々なフィールドは、各々が、ネットワークサービスに関連するスイッチのリダイレクトポートへデータパケット３００をリダイレクトすべきかどうかを決定することができるデータパケット３００のトラフィックタイプの例である。これとは別に、或いはこれに加えて、本発明の様々な実施形態では、データパケット３００のその他のヘッダ３３０における１又はそれ以上のフィールド、ペイロード３４０内の情報及び／又はセンサ２１０が検出した状態などの全体的なスイッチトラフィックの状態に少なくとも部分的に基づいて、データパケット３００をリダイレクトポートへリダイレクトすることができる。

【００３７】

例示を目的として、本明細書では構成２００を参照しながらデータパケット３００のリダイレクティングについて説明する。しかしながら、本発明の様々な実施形態では、構成２００が他の種類のデータパケットをリダイレクトすることができ、或いは構成２００以外の構成によって実現される本発明の様々な実施形態により、データパケット３００をリダイレクトできることを理解されたい。この例示的なケースでは、スイッチ２０１においてデータパケット３００を受信し、これをトラフィックセレクタ２０８へ送信して、ネットワーク状態が、ＩＰＳ２１１に関連するスイッチ２０１のリダイレクトポートにデータパケット３００が関連していることを示すかどうかを判定する。本発明の１つの実施形態によれば、スイッチ２０１からＩＰＳ２１１に関連するポートへのデータパケット３００のリダイレクトはさらに、このデータパケットがスイッチ２０１からフラッディングすべきデータパケットであるかどうかに少なくとも部分的に基づく。

【００３８】

本明細書で使用する場合、データパケットをスイッチからフラッディングするということは、一般に特定の１又はそれ以上のネットワーク経路へデータパケットを送信すべき旨の指示が無い場合に、代わりに多くのネットワーク経路へデータパケットを送信すること

を意味する。データリンク層におけるスイッチングでは、データパケットをスイッチング装置からフラッディングするということは、より具体的には、スイッチング装置の特定のポート又は複数のポートへデータパケットを送信すべき旨の指示が無い場合に、代わりにスイッチング装置のいくつかの使用できるポートへデータパケットを送信することを意味する。説明を簡潔かつ明確にするために、データリンク層におけるフラッディングに関連してデータパケットのフラッディングについて説明する。ネットワーキング技術における当業者であれば、本明細書では、本発明の実施形態の説明におけるフラッディングの意味を広げて、ネットワーク層におけるＩＰマルチキャスティングなどの他の種類のデータフラッディングを含めることができることを理解するであろう。

【００３９】

ＭＡＣ宛先アドレス（ＤＡ）３１２が、一般にスイッチ２０１の全てのポートからデータパケットをブロードキャストすべき旨を示すブロードキャストＭＡＣ　ＤＡである場合、データパケット３００をスイッチ２０１からフラッディングすることができる。或いは、ＭＡＣ　ＤＡ３１２がスイッチ２０１にとって未知のＭＡＣアドレスである場合、データパケット３００をスイッチ２０１からフラッディングすることができる。例えば、スイッチ２０１が、転送用データベース（ＦＤＢ）内でＭＡＣ　ＤＡ３１２の検索を行って、ＭＡＣ　ＤＡ３１２に関連するポートを判定しようと試みる場合にこのケースが生じることがある。ＦＤＢ検索がうまくいかなかった場合、データパケット３００を特定のポートへ送信すべき旨の指示が無ければ、スイッチ２０１は、いくつかの状況においてデータパケット３００を代わりにスイッチ２０１の１又はそれ以上のポートへフラッディングすることができる。

【００４０】

ＩＰＳ２１１が、リダイレクトされたデータパケットをスイッチ２０１へ戻す可能性があると、データパケットが誤ったポートで送信されたり、及び／又はデータパケットループなどの問題が生じる可能性がある。スイッチ２０１からフラッディングすべきデータパケットの場合、特にそう言える。従って、本発明の実施形態は、データパケット３００の選択的リダイレクティングに、データパケット３００が、スイッチ２０１からフラッディングされるこれらの潜在的に問題のあるデータパケットの１つであるかどうかについての評価を含める。この評価をポートリダイレクトの一部としてどのように含めることができるかの例について以下で説明する。

【００４１】

本発明の様々な実施形態では、ネットワークにおいてデータパケットをスイッチ２０１を介して確実に送信するようにするために追加の手段が講じられる。例えば、ＩＰＳ２１１にトラフィックを運ぶリダイレクトポートを、スイッチング装置２０１からのいずれのデータパケットのフラッディングからも切り離すことができる。これにより、データパケット３００がスイッチ２０１のリダイレクトポートに関連していないと判定されたものの、これにも関らずデータパケット３００がスイッチ２０１からフラッディングすべきデータパケットであるというような場合、あらゆる不注意によるデータパケット３００のＩＰＳ２１１へのリダイレクトが阻止される。リダイレクトポートが、フラッディングされたトラフィックを運ぶことができる場合、ＩＰＳ２１１には、分析が必要であるとされていないトラフィック、又は分析が必要ないとされているトラフィックのいずれかが不必要に送信される。リダイレクトポートの切り離しは、例えば、特定の仮想ローカルエリアネットワーク（ＶＬＡＮ）のトラフィックを運ぶ（又は別様にサポートする）ポートの組からリダイレクトポートを除外するステップを含むことができる。

【００４２】

これに加えて、或いはこれとは別に、スイッチ２０１を、ＩＰＳ２１１から戻されたトラフィックをスイッチ２０１へ運ぶリダイレクトポートでＭＡＣラーニングが行われないように構成することができる。ＭＡＣラーニングは、スイッチ２０１に、データパケットの特定のソースＭＡＣアドレスを、データパケットを受信したスイッチのポートに関連付けさせる。ＭＡＣソースアドレス３１１をデータパケット３００が最初に到来した元の場

所（すなわちトラフィック２２０を運ぶポートであり、ＩＰＳ２１１からデータパケットを戻すリダイレクトポートではない）に関連付けるべきである場合、ＭＡＣの動き、すなわちあるＭＡＣソースアドレスに関連するポートの望ましくない再学習を防ぐために、リターンリダイレクトポートに対してＭＡＣラーニングを停止すべきである。ネットワークポートにおいてＭＡＣラーニングを停止させるための様々な周知のスイッチ構成方法は商業的にサポートされており、本発明の実施形態の動作の説明に必要な場合を除き、本明細書では詳述しない。

【００４３】

図４Ａは、本発明の１つの実施形態による、データパケットのネットワークサービスへのポートリダイレクトを選択的に行う方法４００を示す図である。例えば、図２に示すスイッチ２０１のトラフィックセレクタ２０８により、この方法を行うことができる。方法４００は、ネットワークサービスに関連するポートへのデータパケットのリダイレクトを行う準備のできたスイッチング装置により４０５から開始する。４１０において、スイッチング装置がデータパケットを受信し、このデータパケットがネットワーク内の１又はそれ以上の宛先へ送信される。データパケットの受信時に、４１５において、受信したデータパケットをスイッチング装置からフラッディングすべきかどうかに関する判定が行われる。前述したように、例えば、データパケットのブロードキャストＭＡＣ　ＤＡにより、或いはデータパケットのＭＡＣ　ＤＡのＦＤＢ検索がうまくいかなかったことにより、このフラッディングを指示することができる。

【００４４】

ＩＰマルチキャストデータパケットの場合、データパケットが、２００１年８月出版、Ａｌｂａｎｎａ，Ｚ．，Ａｌｍｅｒｏｔｈ，Ｋ．，Ｍｅｙｅｒ，Ｄ．，及びＭ．ＳｃｈｉｐｐｅｒによるＩｎｔｅｒｎｅｔ　Ａｓｓｉｇｎｅｄ　Ｎｕｍｂｅｒｓ　Ａｕｔｈｏｒｉｔｙ（ＩＡＮＡ）の「ＩＰｖ４マルチキャストアドレス割り当てのためのＩＡＮＡガイドライン」、Ｂｅｓｔ　Ｃｕｒｒｅｎｔ　Ｐｒａｃｔｉｃｅ（ＢＣＰ）５１、Ｒｅｑｕｅｓｔ　ｆｏｒ　Ｃｏｍｍｅｎｔｓ（ＲＦＣ）３１７１に記載されるようなマルチキャストＩＰ　ＤＡを含むと判定することにより、データパケットをスイッチング装置からフラッディングすべきであるという判定を示すことができる。例えば、トラフィックセレクタＡＣＬの形のエントリを加えて、リダイレクトポートにおけるあらゆるマルチキャストトラフィックを捕らえることにより、これを行うことができる。例えば、ＡＣＬエントリを、ＩＰマルチキャストトラフィックを捕らえるために、ＩＰ　ＤＡ２２４．０．０．０でトラフィックに応答するように設定することができる。

【００４５】

データパケットをフラッディングすべき場合、データパケットは、ネットワークサービスに関連するリダイレクトポートへ前もってリダイレクトされることなく、４２０においてスイッチング装置からフラッディングされる。１つの実施形態では、４２０におけるスイッチング装置からのデータパケットのフラッディングは、リダイレクトポートでのデータパケットの送信を除外する。データパケットをスイッチング装置からフラッディングすべきでない場合、４２５において、データパケットのトラフィックタイプ（又は同様のネットワーク状態）が、データパケットの、スイッチング装置のリダイレクトポートとの関連性を示すかどうかのような、トラフィックセレクタの一致が生じたかどうかに関して判定が行われる。トラフィックセレクタの一致が存在する場合、４３５において、データパケットが、ネットワークサービスに関連するリダイレクトポートへリダイレクトされる。トラフィックセレクタの一致が存在しない場合、４３０において、データパケットが転送され、この場合、さらなる分析を行うためにデータパケットが最初にネットワークサービスへリダイレクトされることなく、スイッチング装置からデータパケットの１又はそれ以上の宛先へ送信される。トラフィックセレクタ２０８は、例えば方法４００を全て実行するための論理を含むことができるが、代替の実施形態では、データパケットをスイッチング装置からフラッディングすべきかどうかを判定するためのメカニズムを、トラフィックセレクタの一致が存在するかどうかを判定するためのメカニズムとは別個に実装すること

ができる。

【００４６】

図４Ｂは、本発明の別の実施形態による、ネットワークサービスへのデータパケットのポートリダイレクトを選択的に行う方法４５０を示す図である。例えば、図２に示す構成２００におけるスイッチ２０１により、この方法を実行することができる。方法４５０は、ネットワークサービスに関連するポートへのデータパケットのリダイレクトを行う準備のできたスイッチング装置により４５５から開始する。４６０において、スイッチング装置がデータパケットを受信し、このデータパケットがネットワーク内の１又はそれ以上の宛先へ送信される。データパケットの受信時に、４６５において、データパケットのトラフィックタイプ（又は同様のネットワーク状態）が、データパケットの、スイッチング装置のリダイレクトポートとの関連性を示すかどうかのような、トラフィックセレクタの一致が生じたかどうかに関して判定が行われる。トラフィックセレクタの一致が存在しない場合、４７０において、さらなる分析を行うためにデータパケットが最初にネットワークサービスへリダイレクトされることなく、データパケットがスイッチング装置からデータパケットの１又はそれ以上の宛先へ送信される。

【００４７】

トラフィックセレクタの一致が存在する場合、受信したデータパケットをスイッチング装置からフラッディングすべきかどうかに関する判定が４７５において行われる。前述したように、例えば、データパケットのブロードキャストＭＡＣ　ＤＡにより、或いはデータパケットのＭＡＣ　ＤＡのＦＤＢ検索がうまくいかなかったことにより、このフラッディングを指示することができる。データパケットをフラッディングすべき場合、データパケットは、ネットワークサービスに関連するリダイレクトポートへ前もってリダイレクトされることなく、４８５においてスイッチング装置からフラッディングされる。１つの実施形態では、４２０におけるスイッチング装置からのデータパケットのフラッディングは、リダイレクトポートでのデータパケットの送信を除外する。データパケットをフラッディングすべきでない場合、４８０において、さらなる分析を行うためにデータパケットがネットワークサービスへリダイレクトされる。方法４００と同様に、データパケットをスイッチング装置からフラッディングすべきかどうかを判定するためのメカニズムを、トラフィックセレクタの一致が存在するかどうかを判定するためのメカニズムと共に実装してもよいし、或いは別個に実装してもよい。

【００４８】

本発明の実施形態の特定の実施構成、及び特定のデータパケットが選択的にリダイレクトされることにもよるが、本発明の特定の実施形態は、スイッチング装置がデータパケットを処理する際に、データパケットを送信すべき場所についてのあらゆる数の異なる指示を記憶することができる。例えば、４６０においてデータパケットを受信した後に、データパケットを、データパケットのＭＡＣ　ＤＡに関連する１又はそれ以上のポートへ送信すべき旨を指示するＰＴＩを記憶することができる。しかしながら、トラフィックセレクタの一致が存在するという４６５における判定の後に、データパケットをリダイレクトポートへ送信すべき旨を指示する別のＰＴＩを記憶することもできる。最終的に、データパケットをスイッチング装置からフラッディングすべきであるという４７５における判定の結果、今回はデータパケットをスイッチング装置からフラッディングすべき旨を指示するＰＴＩを再び記憶する必要が生じることがある。

【００４９】

最も簡単なケースでは、本発明の実施形態は、再度データパケットのＭＡＣ　ＤＡを単純に見ることができる。しかしながら、これにより、データパケットの無駄なリダイレクティング、及び、例えば反復的かつリソースを消費するＦＤＢ検索が行われる可能性がある。本発明の別の実施形態では、データパケットの１又はそれ以上の宛先ポートの正しい指示を、以前に記憶した指示の１つから取り出すことができる。

【００５０】

例えば、データパケットをスイッチング装置からフラッディングすべきであるという４

７５における判定の結果、シーケンス制御テーブル（ＳＣＴ）に記憶された特別な命令を引き起こすことができる。プロセッサ２３０による実行のために、これらのＳＣＴ命令を、例えばメモリ２３１に記憶することができる。本発明の１つの実施形態では、ＳＣＴ命令が、データパケットをフラッディングすべきスイッチング装置のポートについてのいくつかの以前に記憶した指示を取り出す。１つの実施形態では、ＳＣＴ命令を実行した結果、データパケットのＭＡＣ　ＤＡ又はＩＰ　ＤＡのいずれかに基づく、データパケットを送信すべき場所についての指示が取り出される。次にこの取り出された指示が、データパケットを送信すべき場所についての現在の指示に取って代わり、データパケットをスイッチング装置から実際に送信すると決定することができる。

【００５１】

本明細書では、スイッチング装置においてデータパケットをリダイレクトするための技術及びアーキテクチャについて説明している。説明では、本発明を完全に理解するために、数多くの特定の詳細を説明目的で示している。しかしながら、当業者には、これらの特定の詳細を伴わずに本発明を実施できることが明らかであろう。他の例では、説明を曖昧にしないために、構造及び装置をブロック図の形式で示している。

【００５２】

本明細書における「１つの実施形態」又は「ある実施形態」への言及は、本発明の少なくとも１つの実施形態に、実施形態に関連して説明する特定の特徴、構造、又は特性が含まれることを意味する。本明細書において至るところに出現する「１つの実施形態では」という表現は、必ずしも全てが同じ実施形態について言及するものではない。

【００５３】

コンピュータメモリ内のデータビット上のアルゴリズム及び記号による動作表現の観点から以下の詳細な説明のいくつかの部分を提示している。これらのアルゴリズム記述及び表現は、ネットワーキング技術における当業者が自らの研究内容を他の当業者に最も効果的に伝えるために使用する手段である。本明細書において及び一般的に、アルゴリズムとは、望ましい結果をもたらす首尾一貫した一連のステップであると考えられる。これらのステップは、物理量の物理的操作を必要とするものである。必ずしもそうではないが、通常これらの量は、記憶、転送、合成、比較、及び別様に操作できる電気又は磁気信号の形をとる。主に共通使用という理由で、時にはこれらの信号をビット、値、要素、記号、文字、用語、番号などと呼ぶことが便利であることが分かっている。

【００５４】

しかしながら、これらの及び同様の用語の全ては、適当な物理量に関連付けられるべきものであり、またこれらの量に与えられた便利な表記に過ぎないことに留意されたい。以下の説明から明らかなように、別途特別に述べない限り、本発明全体を通じて「ｐｒｏｃｅｓｓｉｎｇ（処理する）」又は「ｃｏｍｐｕｔｉｎｇ（計算する）」又は「ｃａｌｃｕｌａｔｉｎｇ（計算する）」又は「ｄｅｔｅｒｍｉｎｉｎｇ（決定する）」又は「ｄｉｓｐｌａｙｉｎｇ（表示する）」などの用語を利用した説明は、コンピュータシステムのレジスタ及びメモリ内の物理（電子）量として表されるデータを操作し、コンピュータシステムのメモリ、レジスタ、又はその他のこのような情報記憶装置、送信又は表示装置内の物理量として同様に表される他のデータに変換するコンピュータシステム又は同様の電子コンピュータ装置の動作及び処理を意味するものである。

【００５５】

本発明の実施形態はまた、本明細書における動作を行うための装置にも関する。この装置は、必要な目的のために特別に構成したり、或いはコンピュータに記憶されたコンピュータプログラムにより選択的に作動又は再構成された汎用コンピュータを含むことができる。このようなコンピュータプログラムを、以下に限定されるわけではないが、フロッピー（登録商標）ディスク、光ディスク、ＣＤ－ＲＯＭ、及び磁気光ディスクを含むあらゆる種類のディスク、読出し専用メモリ（ＲＯＭ）、ランダムアクセスメモリ（ＲＡＭ）、ＥＰＲＯＭ、ＥＥＰＲＯＭ、磁気又は光カード、或いは電子命令の記憶に適したあらゆる種類の媒体などのコンピュータ可読記憶媒体に記憶することができ、これらの各々をコン

ピュータシステムバスに結合することができる。

【００５６】

本明細書で示すアルゴリズム及び表示は、本質的にいずれかの特定のコンピュータ又はその他の装置に関連するものではない。様々な汎用システムを、本明細書の教示に従うプログラムと共に使用し、或いは必要な方法ステップを実行するために、より特殊化した装置を構成することが便利であると証明することができる。以下の説明から様々なこれらのシステムに必要な構造が明らかとなるであろう。また、本発明は、いずれかの特定のプログラミング言語に関連して説明するものではない。様々なプログラミング言語を使用して、本明細書で説明するような本発明の教示を実現できることが理解できよう。

【符号の説明】

【００５７】

１００　システム
１０５　受信
１１０　スイッチング装置
１１５　通信（リダイレクト）
１２０　ネットワークサービス
１２５　通信（戻す）
１３０　ネットワーク
１３５　通信
１４０　ネットワーク

【図１】

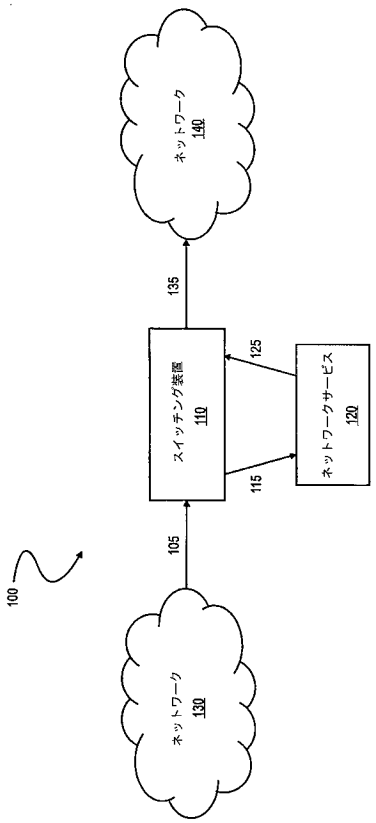

FIG. 1

【図２】

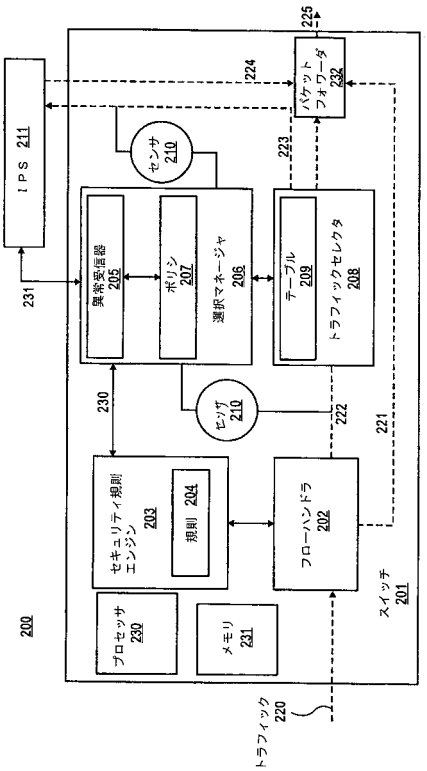

FIG. 2

【図３】

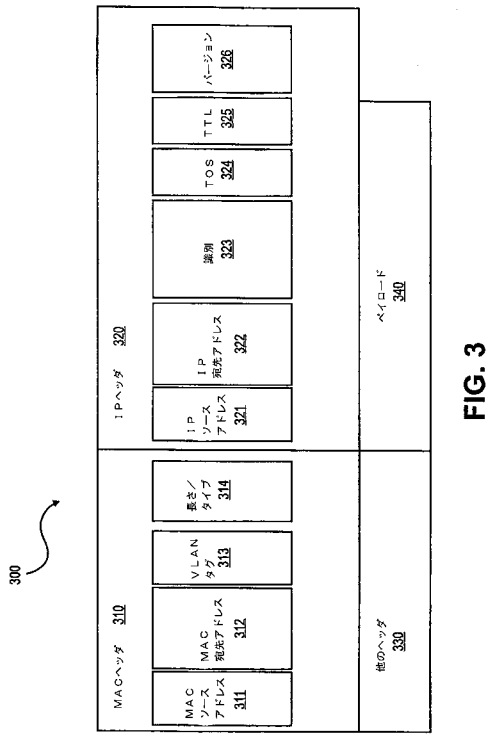

FIG. 3

【図４Ａ】

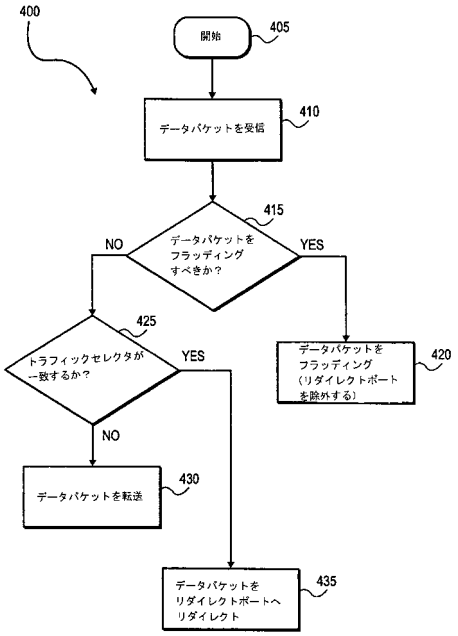

FIG. 4A

【図４Ｂ】

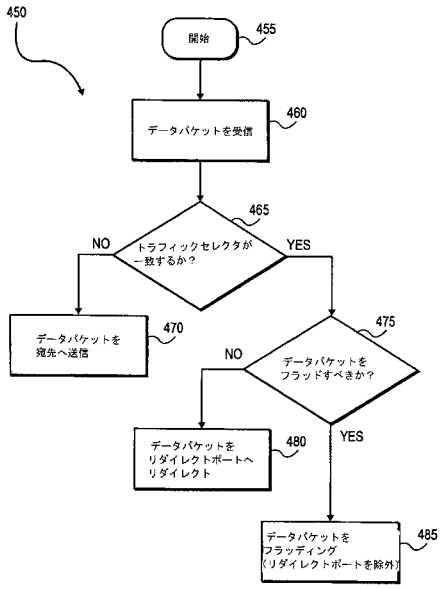

FIG. 4B

フロントページの続き

(72)発明者　クリシュナン, ラム
アメリカ合衆国・９４０８６・カリフォルニア州・サニイベイル・ウェスト　ワシントン　アベニュ・９１９

審査官　衣鳩　文彦

(56)参考文献　米国特許出願公開第２００５／０２６５２４８（ＵＳ, Ａ1）
特開２００２－２１５４７８（ＪＰ, Ａ）
特表２００８－５４１５５８（ＪＰ, Ａ）

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