(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3590936号
(P3590936)
(45)発行日　平成16年11月17日(2004.11.17)　(24)登録日　平成16年9月3日(2004.9.3)

(51)Int.Cl.[7]	F I		
H04L 12/56	H04L	12/56	A
G06F 13/00	G06F	13/00	610Q
H04L 12/58	H04L	12/58	100Z

請求項の数 14　(全 11 頁)

(21)出願番号	特願2002-196075(P2002-196075)
(22)出願日	平成14年7月4日(2002.7.4)
(65)公開番号	特開2003-143182(P2003-143182A)
(43)公開日	平成15年5月16日(2003.5.16)
審査請求日	平成14年7月5日(2002.7.5)
(31)優先権主張番号	2001-61649
(32)優先日	平成13年10月6日(2001.10.6)
(33)優先権主張国	韓国(KR)
(31)優先権主張番号	2002-29828
(32)優先日	平成14年5月29日(2002.5.29)
(33)優先権主張国	韓国(KR)

(73)特許権者　502241969
テラス　テクノロジーズ，インコーポレイテッド
ＴＥＲＲＡＣＥ　ＴＥＣＨＮＯＬＯＧＩＥＳ，ＩＮＣ．
大韓民国ソウル１３３－８２１城東區聖水１街６５６－７６６ゲプンビル４階
(74)代理人　100082418
弁理士　山口　朔生
(74)代理人　100099450
弁理士　河西　祐一
(74)代理人　100114867
弁理士　横山　正治

最終頁に続く

(54)【発明の名称】動的ＩＰフィルタリングモジュールを有する電子メールサービスシステム及び動的ＩＰアドレスフィルタリング方法

(57)【特許請求の範囲】

【請求項１】

動的ＩＰフィルタリングモジュールを有する電子メールサービスシステムにおいて、

遠隔ホストから接続要請を受付ける手段と、

ＩＰブロック単位で前記接続要請したホストの該当ＩＰアドレスを抽出する手段と、

前記該当ＩＰアドレスから所定の管理時間の間の過去に要請した接続要請を累積した値と現在要請を合算した値を、所定の基準値と比較して、接続許容可否を決定する手段とを含み、

前記動的ＩＰフィルタリングモジュールは、接続許容可否を決定する前に、最終接続時間と現在時間との間にある所定の管理時間をスライス数で分割したスライスに該当する接続要請回数を初期化する手段を含むことを特徴とする電子メールサービスシステム。

【請求項２】

前記接続許容可否決定手段で接続が遮断された場合、該当ＩＰアドレスに対して所定の接続不許可時間を設定し、この接続不許可時間中には、該当ＩＰアドレスの接続を遮断することを特徴とする請求項１に記載の電子メールサービスシステム。

【請求項３】

前記ＩＰブロックは、複数のＩＰグループを含み、いずれか１つのＩＰグループに適用される政策は、他のＩＰグループに適用される政策と異なり、前記政策は、前記所定の管理時間、前記所定の基準値、前記所定の接続不許可時間に対する値を含むことを特徴とする請求項２に記載の電子メールサービスシステム。

【請求項４】
前記ＩＰブロックは、複数のＩＰグループを含み、１つのＩＰグループに対して複数の政策が適用され、前記政策は、前記所定の管理時間、前記所定の基準値、前記所定の接続不許可時間に対する値を含むことを特徴とする請求項２に記載の電子メールサービスシステム。
【請求項５】
動的ＩＰフィルタリングモジュールを有する電子メールサービスシステムにおいて、
前記電子メールサービスシステムは、通信網を介して複数の遠隔サーバーに連結されており、前記複数の遠隔サーバーは、固有のメール伝送エージェントを含み、
前記電子メールサービスシステムは、遠隔ホストから前記複数の遠隔サーバーに対する接続要請を受付ける手段と、
ＩＰブロック単位で前記接続要請したホストの該当ＩＰアドレスを抽出する手段と、
前記該当ＩＰアドレスから所定の管理時間の間の過去に要請した接続要請を累積した値と現在要請を合算した値を、所定の基準値と比較して、接続許容可否を決定する手段と、
前記動的ＩＰフィルタリングモジュールが接続許容可否を決定する前に、最終接続時間と現在時間との間にある所定の管理時間をスライス数で分割したスライスに該当する接続要請回数を初期化する手段と、
前記接続許容可否決定手段により接続が許容された要請に対する電子メールを該当遠隔サーバーに伝送する手段とを含むことを特徴とする電子メールサービスシステム。
【請求項６】
前記接続許容可否決定手段で接続が遮断された場合、該当ＩＰアドレスに対して所定の接続不許可時間を設定し、この接続不許可時間中には、該当ＩＰアドレスの接続を遮断することを特徴とする請求項５に記載の電子メールサービスシステム。
【請求項７】
電子メールサービスシステムでＩＰアドレスを動的にフィルタリングする方法において、
遠隔ホストから接続要請を受付ける段階と、
ＩＰブロックを検索して、前記接続要請したホストの該当ＩＰアドレスを抽出する段階と、
該当ＩＰアドレスが所定の管理時間の間の過去に要請した接続要請を累積した値と現在要請を合算した値を、所定の基準値と比較して、接続許容可否を決定する段階と、
前記接続許容可否の決定段階前に、最終接続時間と現在時間との間にある所定の管理時間をスライス数で分割したスライスに該当する接続要請回数を初期化する段階とを含むことを特徴とする動的ＩＰアドレスフィルタリング方法。
【請求項８】
前記接続許容可否の決定段階で接続を許容しないように決定した場合、該当ＩＰアドレスに所定の接続不許可時間を設定し、この接続許容不許可時間中には、該当ＩＰアドレスに対する接続を遮断することを特徴とする請求項７に記載の動的ＩＰアドレスフィルタリング方法。
【請求項９】
前記ＩＰブロックは、１つのＩＰアドレスに対応するレコードで構成され、それぞれのレコードは、所定の管理時間を基準に連続的に管理される複数のスライスで構成され、それぞれのスライスには、該当ＩＰアドレスの接続要請回数が記録されていることを特徴とする請求項７又は８に記載の動的ＩＰアドレスフィルタリング方法。
【請求項１０】
前記接続許容可否の決定段階後には、前記接続要請受付段階に戻ることを特徴とする請求項７又は８に記載の動的ＩＰアドレスフィルタリング方法。
【請求項１１】
前記ＩＰブロックは、複数のＩＰグループを含み、いずれか１つのＩＰグループに適用される政策は、他のＩＰグループに適用される政策と異なり、前記政策は、前記所定の管理時間、前記所定の基準値、前記所定の接続不許可時間に対する値を含むことを特徴とする

請求項８に記載の動的ＩＰアドレスフィルタリング方法。
【請求項１２】
前記ＩＰブロックは、複数のＩＰグループを含み、１つのＩＰグループに対して複数の政策が適用され、前記政策は、前記所定の管理時間、前記所定の基準値、前記所定の接続不許可時間に対する値を含むことを特徴とする請求項８に記載の動的ＩＰアドレスフィルタリング方法。
【請求項１３】
固有のメール伝送エージェントを有する複数の遠隔サーバーと通信網を介して連結されている電子メールサービスシステムでＩＰアドレスを動的にフィルタリングする方法において、
遠隔ホストから前記複数の遠隔サーバーに対する接続要請を受付ける段階と、ＩＰブロックを検索して、前記接続要請したホストの該当ＩＰアドレスを抽出する段階と、
該当ＩＰアドレスが所定の管理時間の間の過去に要請した接続要請を累積した値と現在要請を合算した値を、所定の基準値と比較して、接続許容可否を決定する段階と、
前記接続許容可否の決定段階前に、最終接続時間と現在時間との間にある所定の管理時間をスライス数で分割したスライスに該当する接続要請回数を初期化する段階と、
前記接続許容可否の決定段階で接続が許容された要請に対する電子メールを該当遠隔サーバーに伝送する段階とを含むことを特徴とする動的ＩＰアドレスフィルタリング方法。
【請求項１４】
前記接続許容可否の決定段階で接続を許容しないように決定した場合、該当ＩＰアドレスに所定の接続不許可時間を設定し、この接続許容不許可時間中には、該当ＩＰアドレスに対する接続を遮断することを特徴とする請求項１３に記載の動的ＩＰアドレスフィルタリング方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、電子メールサービスシステム及び方法に関し、より詳しくは、変動開始時間概念を採択した動的ＩＰフィルタリングモジュール及び方法を用いて、時間間隔の絶え間なく連続的にＩＰフィルタリングをすることができ、ＩＰグループに対して多数のＩＰ遮断政策を具現することができ、１つのＩＰグループに対して時間帯ごとに別のＩＰ遮断政策を実現することができる、電子メールサービスシステム及び方法に関する。
【０００２】
【従来の技術】
インターネットのような分散コンピューターネットワークを介して情報を伝達し流通することが拡大されるにつれて、電子メールシステムによる個人間情報の伝達がだんだん日常化されている。電子メールシステムは、同格サーバーを有する分散クライアント／サーバーシステムを言う。クライアントは、サーバーと通信して、電子メールを送受信し、サーバーは、他のサーバーと通信する、基本的に開放システムを基盤とすることが電子メールシステムである。一方、このような電子メールシステムの開放性は、だんだん増えて行くスパムメール（ｓｐａｍ　ｍａｉｌ）、ジャンクメール（ｊｕｎｋ　ｍａｉｌ）、電子メール爆弾のような「望まない商業的電子メール」（ＵＣＥ；Ｕｎｓｏｌｉｃｉｔｅｄ　Ｃｏｍｍｅｒｃｉａｌ　Ｅｍａｉｌ、以下、スパム電子メールと呼ぶ）による問題点を有している。
【０００３】
スパム電子メールの大部分は、低費用で広告の効果を得るために使われるが、これは、インターネットサービス提供者（ＩＳＰ：Ｉｎｔｅｒｎｅｔ　Ｓｅｒｖｉｃｅ　Ｐｒｏｖｉｄｅｒ））及び実際にこのような電子メールを最終的に受信して処理しなければならない使用者の立場では、共に損失として作用する。例えば、スパム電子メールを処理するために、ＩＳＰが追加的な費用をかけるべき資源には、次のようなものがある。大部分のスパム電子メールは、１０万単位以上の使用者に大規模で伝送され、容量が数ギガ（ｇｉｇ

ａ）以上になるため、ネットワーク資源が損失され、スパム電子メールに対する対策として受信されたスパム電子メールに対して自動に発信者に返送する方法、電子メールアドレス目録から削除すべきことを要請したり、スパム電子メールに対する抗議内容を返送する等の追加的な通信費用と人的資源の浪費及びシステム資源の損失が生ずる。一方、スパム電子メールを受信する個別使用者にとっても、システム資源と共にスパム電子メールを正常的な電子メールと区分して処理する業務資源の損失が発生する。

【０００４】

スパム電子メールの問題を解決するための従来の方法では、受信者接近法及び電子メールサービス提供者接近法がある。サービス提供者接近法は、スパム発送者が匿名の構成要素を使用できないようにし、ＳＭＴＰの中継を防ぐＭＴＡ制御方式と、契約を統制する方式がある。一方、サービス提供者のメールサーバーのトラフィックは、主として発送より受信件数が５～１０倍程度多く、このうちスパム電子メールが６０～８０％を占める。スパム電子メールを防止する最も確実な方法は、電子メールの題目や本文内容を見て、スパム電子メールと正常電子メールとに区別することであるが、この方法は、サービス提供者や使用者の両方とも時間と費用がかかるだけでなく、電子メールを区別する基準が明確でなくて、判断が困難であるという問題がある。

したがって、電子メール共同体またはインターネット共同体のために、スパム電子メールによる損失をより一層効果的に補償できる技術的解決策の用意が要請される。

【０００５】

【発明が解決しようとする課題】

本発明の目的は、スパム電子メールによる電子メールサービス提供者の損失を最小化することにある。

本発明の他の目的は、スパム電子メールから電子メールサービス提供者のトラフィックを効率的に維持し制御することによって、スパム電子メールによる被害を防止することにある。

本発明のさらに他の目的は、接続要請があるＩＰグループ毎に別のスパム遮断政策を適用することができ、同じＩＰグループに対してもいろいろな政策を柔軟に適用できる電子メールサービスシステム及び方法を提供することにある。

【０００６】

【課題を解決するための手段】

前記課題を解決するために、本発明は、電子メールを受信して処理する前に、電子メールを発送しようとする遠隔ホストのＩＰアドレスを基準に接続要請件数または接続要請回数を判断し、この回数が一定の基準値を超過すると、該当ＩＰアドレスのホストで送信した接続要請を拒否することによって、伝送しようとする電子メールの再転送に対する責任を該当ホストに渡し、従って、メールサーバーのトラフィックを効率的に維持管理する。

【０００７】

本発明に係る電子メールサービスシステムは、動的ＩＰアドレスフィルタリングモジュール及びメール伝送エージェント（ＭＴＡ）を含み、遠隔ホストから接続要請を受付ける手段と、ＩＰアドレスを、例えば、ハッシュ関数（ｈａｓｈ　ｆｕｎｃｔｉｏｎ）を用いてＩＰブロックで構成することによって、同時にいろいろな接続要請に対して接続許容可否を決定できるようにするＩＰブロック構成手段と、該当ＩＰアドレスが所定の管理時間のあいだ過去に要請した接続要請を累積した値と現在要請を合算した値を、所定の基準値と比較して、接続許容可否を決定する手段とを含み、前記動的ＩＰフィルタリングモジュールは、接続許容可否を決定する前に、最終接続時間と現在時間との間のスライスに該当する接続回数を初期化する手段を含むことを特徴とする。

【０００８】

本発明に係る電子メールサービスシステムにおける動的ＩＰアドレスフィルタリング方法は、遠隔ホストから接続要請を受付ける段階と、ＩＰブロックを検索して、前記接続要請したホストの該当ＩＰアドレスを抽出する段階と、最終接続時間と現在時間との間のスライスに該当する接続回数を初期化する段階と、該当ＩＰアドレスが所定の管理時間の間の

過去に要請した接続要請を累積した値と現在要請を合算した値を、所定の基準値と比較して、接続許容可否を決定する段階とを含むことを特徴とする。
本発明の他の局面によれば、異なるＩＰグループに対して互いに異なるＩＰ遮断政策（管理単位時間、基準値、接続不許可時間）を適用したり、同じＩＰグループに対して時間によって互いに異なるＩＰ遮断政策を適用する等の多数ＩＰ遮断政策を適用して、メールサービスシステムのトラフィックをより一層効率的に管理し、動的ＩＰフィルタリング技術をより一層柔軟で且つ多様に適用することが可能である。
【０００９】
【発明の実施の形態】
以下、図面を参照して本発明の実施形態を説明する。
図１は、本発明に係る電子メールネットワークの全体的な構成を示すブロック図である。本発明に係る電子メールネットワークは、電子メールを作成し、アクセスし、送受信する分散コンピュータシステムであって、ＩＭＡＰ（Ｉｎｔｅｒｎｅｔ Ｍｅｓｓａｇｉｎｇ Ａｃｃｅｓｓ Ｐｒｏｔｏｃｏｌ）、ＰＯＰ（Ｐｏｓｔ Ｏｆｆｉｃｅ Ｐｒｏｔｏｃｏｌ）またはＳＭＴＰ（Ｓｉｍｐｌｅ Ｍａｉｌ Ｔｒａｎｓｆｅｒ Ｐｒｏｔｏｃｏｌ）のようなプロトコルを基盤に成立する。
遠隔ホスト（１０）は、インターネットのような公衆ネットワークまたは近距離通信網（ＬＡＮ：Ｌｏｃａｌ Ａｒｅａ Ｎｅｔｗｏｒｋ）のようなネットワークで電子メールサービスシステム（１００）と連結されている。遠隔ホスト（１０）は、個人使用者クライアントシステムであるか、電子メールサービスシステム（１００）と同格のサーバーシステムを含む。ネットワークは、数多くの接続ノードを有し、インターネットプロトコル（ＩＰ）を用いて通信が行われる。ＩＰは、データを通信する標準方式として広く知られている。ＨＴＴＰとＦＴＰのような高レベルプロトコルは、アプリケーション階層の通信を担当し、ＴＣＰ／ＩＰのような低レベルプロトコルは、トランスポート階層とネットワーク階層の通信を担当する。メールメッセージは、ＳＭＴＰプロトコルを介して、例えば、＜ｒｅｃｅｉｖｅｒ@ｔｅｒｒａｃｅｔｅｃｈ．ｃｏｍ＞のアドレスに伝送される。
【００１０】
電子メールサービスシステム（１００）は、１つ以上のサーバーコンピュータを含み、公衆網と連結した私設ネットワーク（イントラネット）の一部分を構成することができる。保安のために、インターネットとイントラネット構成要素間の通信は、ファイヤーウォール（ｆｉｒｅｗａｌｌ）を用いてフィルタリングし制御することが可能である。ファイヤーウォールは、イントラネットの特定資源に対する外部アクセスを制限する。電子メールサービスシステム（１００）に含まれたサーバーコンピュータは、クライアントのためにサーバープログラムを実行する。サーバーコンピュータは、使用者アカウントを維持し、電子メールメッセージを受信し、フィルタリングして、メッセージ情報のエンコードに関係なく電子メールメッセージを捜し出し、復元することができるようにする。サーバーコンピュータは、例えば、ウェブサーバー、ＣＧＩプログラム部、アカウント管理者、ＳＭＴＰメールサーバーを含むことができる。
【００１１】
電子メールサービスシステム（１００）は、動的ＩＰアドレスフィルタリングモジュール（２０）と、Ｓｅｎｄｍａｉｌ（登録商標）、Ｑｍａｉｌ（登録商標）のようなメール伝送エージェント（５０、ＭＴＡ：Ｍａｉｌ Ｔｒａｎｓｆｅｒ Ａｇｅｎｔ）とを含む。ＭＴＡ（５０）は、伝達ＭＴＡと受信ＭＴＡ及びゲートウェイＭＴＡを含む。フィルタリングモジュール（２０）は、接続処理部（３０）及びＩＰブロック（４０）を含む。サービスシステム（１００）は、遠隔ホスト（１０）から例えばＰＯＰ－３プロトコルを用いて新しい電子メールメッセージを受信し、例えば、ＳＭＴＰ（Ｓｉｍｐｌｅ Ｍａｉｌ Ｔｒａｎｓｆｅｒ Ｐｒｏｔｏｃｏｌ）またはＥＳＭＴＰ（Ｅｘｔｅｎｄｅｄ ＳＭＴＰ）プロトコルを介して電子メールメッセージを伝送する。
【００１２】
遠隔ホスト（１０）は、サービスシステム（１００）に接続要請（ｃｏｎｎｅｃｔｉｏｎ

ｒｅｑｕｅｓｔ）信号を送り、電子メールメッセージの伝送に必要なデータ、例えば、ＭＡＩＬ Ｆｒｏｍ＜ｓｐａｍ@ｈｏｓｔ．ｄｏｍａｉｎ＞、ＲＣＰＴ Ｔｏ＜ｒｅｃｅｉｖｅｒ@ｈｏｓｔ．ｄｏｍａｉｎ＞とメッセージ、添付ファイルデータなどを送る。動的ＩＰアドレスフィルタリングモジュール（２０）の接続処理部（３０）は、遠隔ホスト（１０）の接続要請に対してＩＰブロック（４０）を参照して接続許容可否を判断する。接続が許容されると、遠隔ホスト（１０）から伝送されたデータとメッセージなどは、ＭＴＡ（５０）に伝達され、電子メール受信者または他の遠隔ホストに伝送される。遠隔ホスト（１０）の接続許容可否の判断は、遠隔ホストのＩＰアドレスを基準に接続要請件数または接続要請回数を判断し、この回数が一定の基準値を超過するか否かによって決定されるが、これについての詳細は後述する。

【００１３】

図２は、本発明に係る電子メールサービスシステムにおいてＩＰブロック、レコードの構成を示す概念図である。電子メールサービスシステム（１００）のＩＰブロックは、予め格納されているデータで、遠隔ホスト（１０）から接続要請があれば、このホストに該当する該当ＩＰアドレスが登録される。ＩＰブロック（４０）は、ＩＰアドレスを一定の基準に配列したグループ単位（４０ａ、４０ｂ、…、４０ｋ）で構成されている。遠隔ホスト（１０）から接続要請を受付ければ、接続処理部（３０）は、遠隔ホストに対応するＩＰアドレスをＩＰブロックから検索して抽出する。ＩＰアドレスは、例えば、ハッシュ関数を用いてＩＰブロックで構成することによって、同時にいろいろな接続要請に対する接続許容可否を決定できるようにすることが好ましい。１つのＩＰブロックグループ（４０ａ）は、複数のレコード（＃０～＃ｍ－１）で構成されるが、１つのＩＰアドレスに対して１つのレコードが形成される。それぞれのレコードは、複数のスライス（ｓｌｉｃｅ）、例えば、「スライス０」から「スライスｎ－１」までのｎ個のスライスで構成される。スライスは、レコードを時間基準に区分した単位を言う。それぞれのスライスには、遠隔ホストから受付けた接続要請回数または接続要請件数が記録されている。

【００１４】

図３は、本発明に係る電子メールサービスシステムにおいて動的ＩＰアドレスフィルタリング方法の全体過程を示す流れ図である。

遠隔ホストから接続要請を受付ければ（段階１１０）、ＩＰブロックを検索し（段階１１５）、接続を要請した遠隔ホストの該当ＩＰアドレスを抽出する（段階１２０）。該当ＩＰアドレスの累積接続要請回数に基づいて遠隔ホストの接続許容可否を決定する（段階１３０）。接続許容可否の決定は、接続要請された現在時間に最も近い過去接続要請時間（すなわち、最終接続時間）から所定の管理期間だけ遡及された時間に該当するスライスに記録されている接続回数を累積した値と現在接続要請を合算した結果値が、所定の基準値を超過するか判断することによって、一次的に行われる（段階１３５）。例えば、１つのレコードに１０個のスライスがあり、この１０個のスライスが１０分単位で管理されるとしたら、１２時１３分に現在接続要請があり、最終接続要請が１２時１１分にあったと仮定する。接続回数の累積値は、全体スライス０－９のうちスライス３－９（すなわち、１２時０３分～１２時１０分までの時間に該当するスライス）に記録されている接続回数と、スライス０（すなわち、１２時１０分～１２時１１分までの時間に該当するスライス）に記録されている接続回数及び現在接続要請回数を加算した値となり、段階１３５では、この累積値を基準値と比較する。基準値は、電子メールサービス提供者のシステム資源、使用者の規模、トラフィックなどを総合的に考慮して決定されるが、時間当り回数単位で表現される。累積接続回数が基準値を超過した場合には、該当ＩＰアドレスに対応する遠隔ホストに対する接続を遮断し（段階１４５）、累積接続回数が基準値を超過しない場合、さらに接続不許可時間が経過したか判断する（段階１４０）。接続不許可時間がまだ経過しない場合には、該当ＩＰアドレスに対応する遠隔ホストに対する接続を遮断し、接続不許可時間が経過したり、接続を許可しない事例がない場合には、遠隔ホストに対する接続を許容し（段階１５０）、電子メールメッセージとデータをＭＴＡに伝達して、正常的な電子メール伝送処理を行う。

【００１５】
一方、接続許容可否の決定段階（１３０）以前には、接続件数を初期化する処理（段階１２５）が行われる。接続件数初期化段階（１２５）は、最終接続時間と現在時間との間のスライスに該当する接続件数を「０」に初期化させる。上述した例の場合、最終接続時間である１２時１１分と現在時間１２時１３分との間のスライスには、実際に１２時０２分に対応するスライスが存在する。なぜならば、最終接続時間と現在時間との間には、接続件数が発生しなかったことを意味し、従って、この時間中には、スライス管理時間（この例では１０分）前の過去時間に対応するスライスに記録された接続件数データが存在する。従って、このスライスに該当する接続件数を「０」に初期化することによって、管理時間を連続的な時間値に維持することが可能である。
接続許容可否を決定した後、さらに新しい接続要請を受付ける段階１１０に戻る。接続許容可否を決定したＩＰアドレスを格納することで、同じＩＰアドレスに対するＩＰブロックを再び検索しないことも考慮することができるが、ＩＰアドレスデータを接続許容可否と関連させて格納するのに必要なシステム資源を勘案する時、新たにＩＰブロックを検索し、該当ＩＰアドレスを抽出することがより好ましい。
このような本発明の動的ＩＰアドレスフィルタリング技術によれば、１つのデータ構造に多数の時間政策を適用することが可能である。
【００１６】
図４は、いろいろなＩＰグループ各々に対して別の政策を適用した多数時間政策技術を示すブロック図である。ＩＰグループＡ（４０ａ）に対して適用される政策Ａ（２００ａ）は、管理単位時間、基準値及び接続不許可時間が他のＩＰグループＢ、Ｃ（２００ｂ、２００ｃ）に適用される政策Ｂ（２００ｂ）、政策Ｃ（２００ｃ）と異なる。ここで、「管理単位時間」とは、図３の判断段階（１３５）で要請された接続回数を合算するのに用いられる管理期間を言い、「基準値」とは、管理単位時間中に累積した接続回数と現在接続要請を合算した値を比較する基準値を言う。多数時間政策技術は、例えば、ＩＰアドレスが２１０．２２０．１０．０－２１０．２２０．２５０．２５５であるＩＰグループＡ（４０ａ）に対して管理単位時間ａ１を１時間とし、基準値ａ２を１０回とし、接続不許可時間ａ３を２時間とするのに対して、ＩＰアドレスが２１０．０．１０．０－２１０．２２０．０．０であるＩＰグループＢ（４０ｂ）に対して管理単位時間ｂ１＝１０分、基準値ｂ２＝１０回、接続不許可時間ｂ３＝３０分である政策Ｂ（２００ｂ）を適用して説明することができる。多数の時間政策を適用する場合、特別な政策が適用されないＩＰグループに対してデフォルト政策（ｄｅｆａｕｌｔ　ｐｏｌｉｃｙ）を適用することが好ましい。特定ＩＰに対してＩＰ遮断可否を確認しようとする時には、多数の政策の中で該当ＩＰが属するＩＰグループに対する政策に関連した値を取る。取られた政策値（例えば、管理単位時間、基準値、接続不許可時間）をＩＰ遮断アルゴリズムに適用して計算する。
【００１７】
本発明によれば、図５に示されたように、１つのＩＰグループ（４０ｎ）に対して時間帯ごとに互いに異なる政策を適用することが可能である。こうして、スパムメール発送要請が多い時間帯に対して特別に強化された政策を動的に適用することによって、メールサーバーのトラフィックを一層効率的に管理することができる。
【００１８】
図６は、本発明に係る電子郵便サービスシステムをＡＳＰモデルで具現したブロック構成図である。電子メールサービスシステム（２１０）は、遠隔ホスト（１０）の接続要請信号、電子メールメッセージ伝送に必要な信号、メッセージ、添付ファイルデータを受付け、動的ＩＰフィルタリングモジュール（２２０）は、遠隔ホスト（１０）の接続要請に対して接続許容可否を判断する。接続が許容されると、本発明に係る電子メールサービスシステム（２１０）は、通信網（４００）、例えば、インターネットを介して連結されている複数の遠隔サーバー（３００ａ、３００ｂ、３００ｃ）のうち電子メール宛先サーバーに電子メールメッセージなどを伝送する。動的ＩＰフィルタリングモジュール（２２０）は、図１の電子メールシステム（１００）の動的ＩＰフィルタリングモジュール（２０）

と同様に、接続処理部（２３０）及びＩＰブロック（２４０）を含む。遠隔サーバー（３００ａ、３００ｂ、３００ｃ）は、それぞれのＭＴＡ（２５０ａ、２５０ｂ、２５０ｃ）を含み、このＭＴＡは、伝達ＭＴＡ、受信ＭＴＡ及びゲートウェイＭＴＡを含むことができる。

【００１９】

このようにＡＳＰ（Ａｐｐｌｉｃａｔｉｏｎ　Ｓｅｒｖｉｃｅ　Ｐｒｏｖｉｄｅｒ）モデルで電子メールサービスシステムを具現する場合、それぞれの遠隔サーバー（３００ａ、３００ｂ、３００ｃ）は、外部資源によるＩＰフィルタリングモジュールを利用することができるので、それ自体の資源を節約することができる。

本発明は、本発明の技術的思想から逸脱することなく、他の種々の形態で実施することができる。前述の実施例は、あくまでも、本発明の技術内容を明らかにするものであって、そのような具体例のみに限定して狭義に解釈されるべきものではなく、本発明の精神と特許請求の範囲内で、いろいろと変更して実施することができるものである。

【００２０】

【発明の効果】

以上説明したように、本発明によれば、時間間隔の絶え間なく連続的にＩＰフィルタリングが可能なので、スパム電子メールから電子メールサービス提供者のトラフィックを効率的に維持し制御することが可能である。また、本発明のシステム及び方法によれば、スパム電子メールによる電子メールサービス提供者の資源損失を最小化することができる。

また、本発明によれば、異なるＩＰグループに対して互いに異なるＩＰ遮断政策を適用して、管理単位時間、基準値、接続不許可時間を変動的に適用することができ、１つのＩＰグループに対して時間によって異なるＩＰ遮断政策を適用する等の多数ＩＰ遮断政策を適用することによって、メールサービスシステムのトラフィックをより効率的に管理し、動的ＩＰフィルタリング技術を一層柔軟で且つ多様に適用することが可能である。

また、本発明によれば、動的ＩＰフィルタリングモジュールをＡＳＰモデルで具現することによって、遠隔サーバーの自体資源を節約すると同時に、スパム電子メールによる遠隔サーバーの損失を最小化し、効率的なトラフィック維持が可能である。

【図面の簡単な説明】

【図１】本発明に係る電子メールネットワークの全体構成を示すブロック図である。

【図２】本発明に係る電子メールサービスシステムにおいてＩＰブロック、レコードの構成を示す概念図である。

【図３】本発明に係る電子メールサービスシステムにおいて動的ＩＰアドレスフィルタリング方法の全体過程を示す流れ図である。

【図４】本発明によって、異なるＩＰグループに対して相異なるＩＰ遮断政策を適用する多数時間政策適用技術を示すブロック図である。

【図５】本発明によって、１つのＩＰグループに対して時間帯毎に異なるＩＰ遮断政策を適用する技術を説明するブロック図である。

【図６】本発明に係る電子郵便サービスシステムをＡＳＰ（Ａｐｐｌｉｃａｔｉｏｎ　Ｓｅｒｖｉｃｅ　Ｐｒｏｖｉｄｅｒ）モデルで具現したブロック構成図である。

【符号の説明】

１０　遠隔ホスト

２０、２２０　動的ＩＰアドレスフィルタリングモジュール

３０、２３０　接続処理部

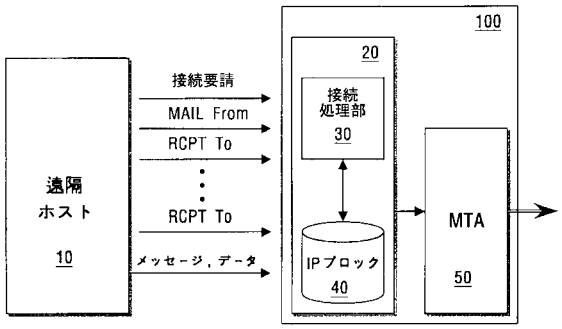
４０、２４０　ＩＰブロック

５０　ＭＴＡ（Ｍａｉｌ　Ｔｒａｎｓｆｅｒ　Ａｇｅｎｔ）

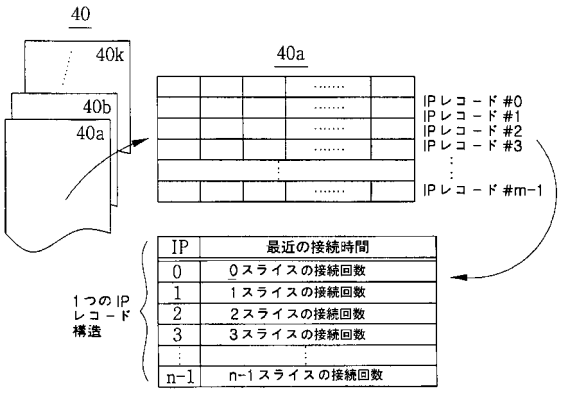
１００、２１０　電子メールサービスシステム

２００　ＩＰ遮断政策

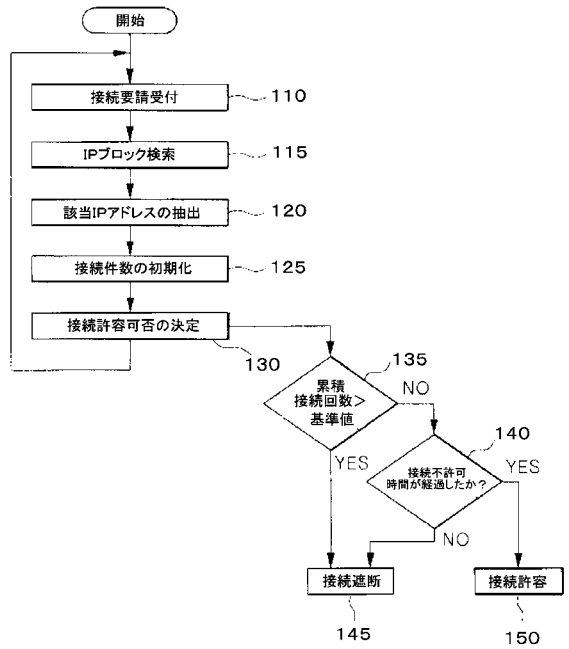
【図１】


100
20
接続
処理部
30
IPブロック
40
MTA
50
遠隔
ホスト
10
接続要請
MAIL From
RCPT To
RCPT To
メッセージ，データ

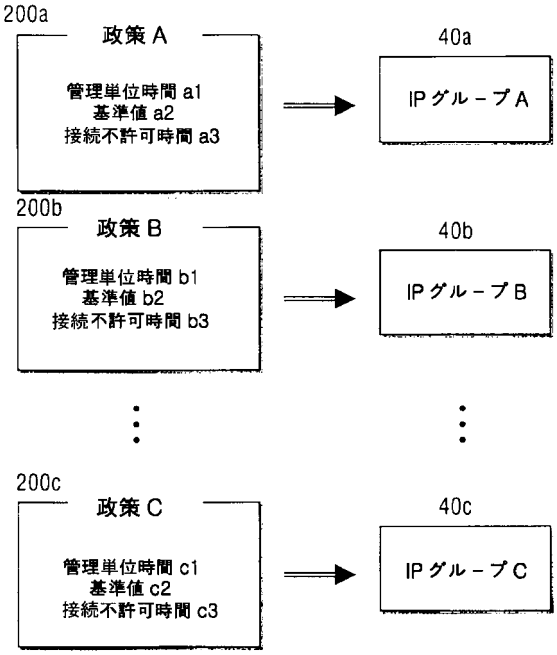
【図２】


40
40k
40b
40a
40a
IPレコード#0
IPレコード#1
IPレコード#2
IPレコード#3
IPレコード#m-1
IP
最近の接続時間
0
0スライスの接続回数
1
1スライスの接続回数
2
2スライスの接続回数
3
3スライスの接続回数
n-1
n-1スライスの接続回数
1つのIPレコード構造

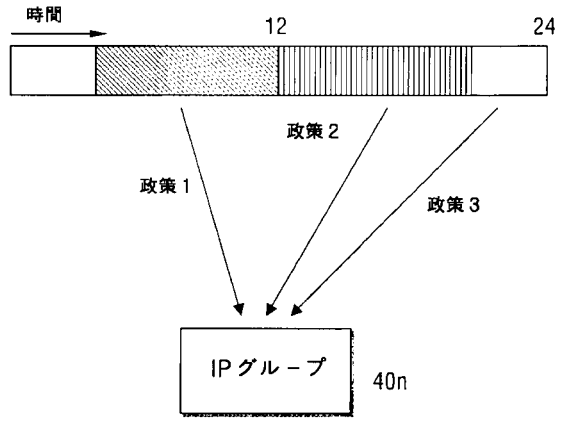
【図３】


開始
接続要請受付
110
IPブロック検索
115
該当IPアドレスの抽出
120
接続件数の初期化
125
接続許容可否の決定
130
累積
接続回数>
基準値
135
NO
YES
接続不許可
時間が経過したか？
140
YES
NO
接続遮断
145
接続許容
150

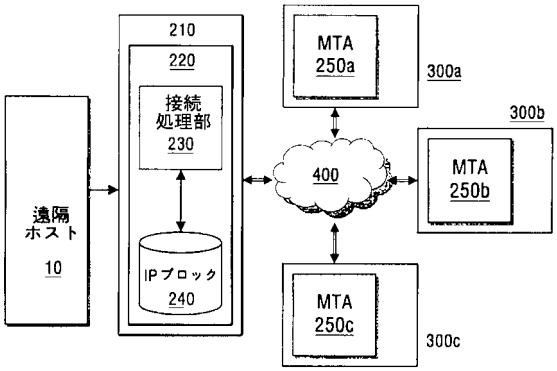
【図４】


200a
政策A
管理単位時間 a1
基準値 a2
接続不許可時間 a3
40a
IPグループA
200b
政策B
管理単位時間 b1
基準値 b2
接続不許可時間 b3
40b
IPグループB
200c
政策C
管理単位時間 c1
基準値 c2
接続不許可時間 c3
40c
IPグループC

【図５】


時間
12
24
政策１
政策２
政策３
IPグループ
40n

【図６】


遠隔
ホスト
10
210
220
接続
処理部
230
IPブロック
240
400
MTA
250a
300a
MTA
250b
300b
MTA
250c
300c

フロントページの続き

(72)発明者 林星▲華▼
大韓民国ソウル１３１－１２０中浪區中和洞ハンシンアパート１０３棟８０６號
(72)発明者 李▲祐▼周
大韓民国ソウル１４３－２２２廣津區中谷２洞１１８－３１番地

審査官 石井 研一

(56)参考文献 特開２０００－１６３３４１（ＪＰ，Ａ）
米国特許第０６１８９０３５（ＵＳ，Ｂ１）
T. Bass et al., E-Mail Bombs and Countermeasures: Cyber Attacks on Availability and Br and Integrity, IEEE Network March/April 1998, １９９８年 3月, Vol.12, No.2, pp.10-17

(58)調査した分野(Int.Cl.[7], ＤＢ名)
H04L 12/56
G06F 13/00 610
H04L 12/58 100