(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2010-45617
(P2010-45617A)
(43)公開日　平成22年2月25日(2010.2.25)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 12/66	(2006.01)	H04L	12/66	B	5B285
G06F 9/50	(2006.01)	G06F	9/46	465C	5K030
G06F 21/20	(2006.01)	G06F	15/00	330A	

審査請求 未請求　請求項の数 5　ＯＬ　（全 7 頁）

(21)出願番号　特願2008-208436 (P2008-208436)
(22)出願日　平成20年8月13日 (2008.8.13)

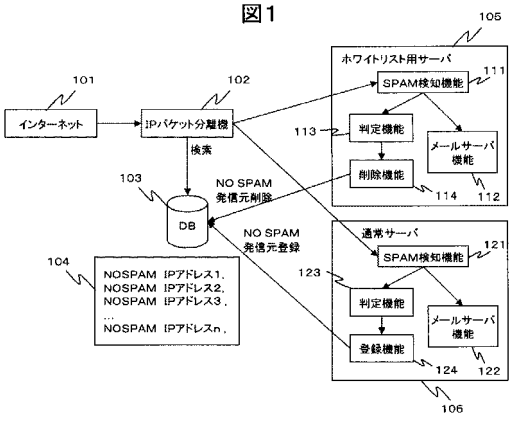
(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(74)代理人　100083552
弁理士　秋田　収喜
(74)代理人　100103746
弁理士　近野　恵一
(74)代理人　100119703
弁理士　井上　雅夫
(72)発明者　西田　晴彦
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　藤浦　豊徳
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

最終頁に続く

(54)【発明の名称】ホワイトリストを利用したサーバ割り当てシステムおよびその方法

(57)【要約】
【課題】信頼できる送信元からのパケットの処理を、それ以外の送信元からのパケットの増加による処理速度の低下から守る技術を提供する。
【解決手段】インターネット１０１からのＩＰパケットは、ＩＰパケット分離機１０２に入る。ＩＰパケット分離機１０２は、ＩＰアドレスが格納されているＤＢ１０３内のホワイトリスト１０４を検索し、そのＩＰアドレスが登録されているか検索する。登録されていればホワイトリスト用サーバ１０５に転送する。登録されていないときは通常サーバ１０６へ転送する。ホワイトリスト用サーバ１０５は判定機能１１３が信頼できない送信元として判定した場合にそのＩＰアドレスをホワイトリスト１０４から削除する削除機能１１４を持つ。通常サーバ１０６は判定機能１２３が信頼できる送信元として判定した場合にそのＩＰアドレスをホワイトリスト１０４に登録する登録機能１２４を持つ。
【選択図】図１

図1



【特許請求の範囲】
【請求項１】
ホワイトリストを利用したサーバ割り当てシステムであって、
信頼できる送信元のアドレスが登録されるホワイトリストと、
通信網からパケットを受信するパケット受信手段と、受信したパケットのアドレスが前記ホワイトリストに登録されているかどうかを検索する検索手段と、受信したパケットのアドレスが前記ホワイトリストに登録されている場合は当該パケットをホワイトリスト用サーバに転送し、登録されていない場合は当該パケットを通常のサーバに転送する転送手段と、を備えるパケット分離機と、
を有することを特徴とするサーバ割り当てシステム。
【請求項２】
請求項１に記載のサーバ割り当てシステムであって、
前記パケット分離機から受信したパケットの送信元アドレスが信頼できるかどうかを判定する判定手段と、信頼できない送信元アドレスと判定した場合に当該送信元アドレスを前記ホワイトリストから削除する削除手段と、を備えるホワイトリスト用サーバを有することを特徴とするサーバ割り当てシステム。
【請求項３】
請求項１または２に記載のサーバ割り当てシステムであって、
前記パケット分離機から受信したパケットの送信元アドレスが信頼できるかどうかを判定する判定手段と、信頼できる送信元アドレスと判定した場合に当該送信元アドレスを前記ホワイトリストに登録する登録手段と、を備える通常のサーバを有することを特徴とするサーバ割り当てシステム。
【請求項４】
請求項１ないし３のうちいずれか１項に記載のサーバ割り当てシステムであって、
前記ホワイトリスト用サーバおよび前記通常のサーバは、メールサーバ機能とＳＰＡＭ検知機能を備えることを特徴とするサーバ割り当てシステム。
【請求項５】
ホワイトリストを利用したサーバ割り当てシステムにおけるサーバ割り当て方法であって、
前記サーバ割り当てシステムは、信頼できる送信元のアドレスが登録されるホワイトリストと、パケット分離機と、を備え、
前記パケット分離機は、通信網からパケットを受信するパケット受信し、受信したパケットのアドレスが前記ホワイトリストに登録されているかどうかを検索し、受信したパケットのアドレスが前記ホワイトリストに登録されている場合は当該パケットをホワイトリスト用サーバに転送し、登録されていない場合は当該パケットを通常のサーバに転送することを特徴とするサーバ割り当て方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明はサーバ割り当て技術に関し、特にホワイトリストを利用したサーバ割り当て技術に関する。
【背景技術】
【０００２】
送信元からのＩＰパケットを複数のサーバに振り分ける装置として、ロードバランサがある。ロードバランサには単純にランダム、あるいは順送りにサーバを選択するものや、パケットをサーバへの既接続数や、サーバのＣＰＵ負荷などをもとに、もっとも適切なサーバに割り振る機能を有するものがある（特許文献１参照）。ロードバランサはメール受信用サーバを複数用意して大量の受信要求を処理する際にも使用されている。
【０００３】
一般に知られているメールのＳＰＡＭ送信元対策としてはもっぱらＳＰＡＭを送信して

くる送信元をサーバ内でブラックリストとして登録しておき、そこからの接続を拒否する方式、またこのブラックリストを外部に持ち、接続要求を受け取った際にブラックリストを参照して接続を拒否する方式がある。また、信頼できる送信元をホワイトリストとしてサーバ内に持つことで受け取ったメールがＳＰＡＭであるかどうかの判定を簡略化する、あるいはホストの信頼性について検査をしないことにより受信側の負荷を下げる方式が知られている。このホワイトリストの作成方法として、サーバが、接続してきた送信元がＳＰＡＭ送信元ではないときに、その送信元のＩＰアドレスをサーバ内のホワイトリストにファイルとして登録する方式が提案されている（非特許文献１参照）。

【０００４】

【特許文献１】特許第３９６４８９６号

【非特許文献１】“Rgrey - S25R + greylisting”、[online]、［平成２０年７月１５日検索］、インターネット＜http://k2net.hakuba.jp/rgrey/＞

【発明の開示】

【発明が解決しようとする課題】

【０００５】

近年、インターネットにおいて、悪意のあるサーバへのアクセスが増えている。これらの中にはサーバの負荷を高くし、サービス停止させることを目的とするものがある。

【０００６】

従来のロードバランサは、サーバへの既接続数やＣＰＵ負荷など、サーバの状況によりサーバを割り振り、送信元の性質は考慮しない。このため、悪意のある送信元からのアクセスも均等に割り振られ、全てのサーバの負荷が高くなってしまう。そのため、悪意のあるアクセスにより、サービスが停止してしまうという課題がある。特にメールの受信に着目した場合、この問題は一部の大量ＳＰＡＭ送信者からのものを含めたメールの総量が増えていくとすべての受信用サーバの負荷が平均的に上がっていき、メール全体の到達遅延を起こすという課題に相当する。

【０００７】

従来技術で挙げた接続してきた送信元がＳＰＡＭ送信者かどうかをサーバが判別し、ＳＰＡＭ送信者でなければ、その送信元のＩＰアドレスをホワイトリストに登録し、以降、判別処理をしない方式はこの判別処理によるサーバの負荷を低減するが、メール総量の増加によるメール全体の遅延を根本的には解決しない。またサーバ本体にホワイトリストを持つ方式はサーバ間でホワイトリストが共有されないため、ある信頼できる送信元からのメールの処理の負荷低減がすべてのサーバで実現されるまでに時間がかかるという課題がある。

【０００８】

本発明の目的は、信頼できる送信元からのパケットの処理を、それ以外の送信元からのパケットの増加による処理速度の低下から守る技術を提供することにある。

【課題を解決するための手段】

【０００９】

本明細書において開示される発明のうち、代表的なものの概要を簡単に説明すれば、以下のとおりである。

【００１０】

第１の発明は、ホワイトリストを利用したサーバ割り当てシステムであって、信頼できる送信元のアドレスが登録されるホワイトリストと、通信網からパケットを受信するパケット受信手段と、受信したパケットのアドレスが前記ホワイトリストに登録されているかどうかを検索する検索手段と、受信したパケットのアドレスが前記ホワイトリストに登録されている場合は当該パケットをホワイトリスト用サーバに転送し、登録されていない場合は当該パケットを通常のサーバに転送する転送手段と、を備えるパケット分離機と、を有するサーバ割り当てシステムである。

【００１１】

第２の発明は、第１の発明のサーバ割り当てシステムであって、前記パケット分離機か

ら受信したパケットの送信元アドレスが信頼できるかどうかを判定する判定手段と、信頼できない送信元アドレスと判定した場合に当該送信元アドレスを前記ホワイトリストから削除する削除手段と、を備えるホワイトリスト用サーバを有するサーバ割り当てシステムである。

【００１２】

第３の発明は、第１または第２の発明のサーバ割り当てシステムであって、前記パケット分離機から受信したパケットの送信元アドレスが信頼できるかどうかを判定する判定手段と、信頼できる送信元アドレスと判定した場合に当該送信元アドレスを前記ホワイトリストに登録する登録手段と、を備える通常のサーバを有するサーバ割り当てシステムである。

【００１３】

第４の発明は、第１～３の発明のサーバ割り当てシステムであって、前記ホワイトリスト用サーバおよび前記通常のサーバは、メールサーバ機能とＳＰＡＭ検知機能を備えるサーバ割り当てシステムである。

【００１４】

第５の発明は、ホワイトリストを利用したサーバ割り当てシステムにおけるサーバ割り当て方法であって、前記サーバ割り当てシステムは、信頼できる送信元のアドレスが登録されるホワイトリストと、パケット分離機と、を備え、前記パケット分離機は、通信網からパケットを受信するパケット受信し、受信したパケットのアドレスが前記ホワイトリストに登録されているかどうかを検索し、受信したパケットのアドレスが前記ホワイトリストに登録されている場合は当該パケットをホワイトリスト用サーバに転送し、登録されていない場合は当該パケットを通常のサーバに転送するサーバ割り当て方法である。

【発明の効果】

【００１５】

本発明により、信頼できる送信元からのパケットの処理を、それ以外の送信元からのパケットの増加による処理速度の低下から守ることができる。

【発明を実施するための最良の形態】

【００１６】

以下、本発明の実施例を図を用いて詳細に説明する。

【００１７】

図１は、本発明の実施例のホワイトリストを利用したサーバ割り当てシステムを説明するための図である。

【００１８】

１０１はインターネット、１０２はＩＰパケット分離機、１０３はＤＢ、１０４はＤＢ１０３内に格納されたホワイトリスト、１０５はホワイトリスト用サーバ、１０６は通常サーバである。１０１はインターネット以外の通信網であってもよい。

【００１９】

ホワイトリスト用サーバ１０５は、ＳＰＡＭ検知機能１１１とメールサーバ機能１１２と判定機能１１３と削除機能１１４とを備える。通常サーバ１０６はＳＰＡＭ検知機能１２１とメールサーバ機能１２２と判定機能１２３と登録機能１２４を備える。

【００２０】

図２に、本実施例のＩＰパケット分離機１０２の内部の構成図を示す。２０１はインターネット１０１からＩＰパケットを受信する受信手段、２０２は受信したＩＰパケットのＩＰアドレスがホワイトリスト１０４に登録されているかどうかを検索する検索手段、２０３は受信したＩＰパケットのＩＰアドレスがホワイトリスト１０４に登録されている場合は当該ＩＰパケットをホワイトリスト用サーバ１０５に転送し、登録されていない場合は当該ＩＰパケットを通常サーバ１０６に転送する転送手段である。ＩＰパケット分離機１０２はハードウェアで構成する方が処理速度の点で有利であり望ましいが、その一部または全部をコンピュータとプログラムで構成してもよい。

【００２１】

次に本実施例のサーバ割り当てシステムの動作について説明する。

【００２２】

インターネット１０１からのＩＰパケットは、ＩＰパケット分離機１０２の受信手段２０１に入る。ＩＰパケット分離機１０２の検索手段２０２は、ＩＰアドレスが格納されているＤＢ１０３内のホワイトリスト１０４を検索し、そのＩＰアドレスが登録されているか検索する。そのＩＰアドレスがホワイトリスト１０４に登録されていれば、ＩＰパケット分離機１０２の転送手段２０３は、ホワイトリスト用サーバ１０５にそのＩＰパケットを転送する。一方、そのＩＰアドレスがホワイトリスト１０４に登録されていないときは、ＩＰパケット分離機１０２の転送手段２０３は通常サーバ１０６へそのＩＰパケットを転送する。

【００２３】

ホワイトリスト用サーバ１０５は、通常のメールサーバの機能１１２に加えて、ＳＰＡＭ検知機能１１１と、送信元をＳＰＡＭを送信してきたかどうか等の情報から信頼できる送信元であるかどうかを判定する判定機能１１３と、信頼できない送信元として判定した場合にそのＩＰアドレスをＤＢ１０３のホワイトリスト１０４から削除する削除機能１１４を持つ。

【００２４】

通常サーバ１０６は、通常のメールサーバの機能１２２に加えて、ＳＰＡＭ検知機能１２１と、送信元をＳＰＡＭを送信してきたかどうか等の情報から信頼できる送信元であるかどうかを判定する判定機能１２３と、信頼できる送信元として判定した場合にそのＩＰアドレスをＤＢ１０３のホワイトリスト１０４に登録する登録機能１２４を持つ。

【００２５】

これにより、信頼できる送信元と判定された送信元からのパケットはそれ以降、ＩＰパケット分離機１０２により、ホワイトリスト用サーバ１０５に届けられる。

【００２６】

ここではホワイトリスト用サーバ１０５、通常サーバ１０６をそれぞれ１台ずつ記載しているが、ＩＰパケット分離機１０２と各サーバの間にロードバランサを置くことでサーバを複数置いて負荷分散をはかることもできる。また、ＩＰパケット分離機１０２の機能をロードバランサに実装する形態も可能である。

【００２７】

本実施例により、ＩＰパケット分離機１０２は、ホワイトリストを利用して、ＳＰＡＭ以外のメールを発信する信頼できる送信元のみにホワイトリスト用サーバ１０５を利用させることができる。

【００２８】

このため、信頼できる送信元からのメールの処理を、それ以外の送信元からのメールの増加による処理速度の低下から守ることが出来る。

【００２９】

また、サーバがＳＰＡＭ送信元かどうか判定し、ＳＰＡＭ送信元ではないことを確認した場合、それをＩＰパケット分離機のホワイトリストに登録する機能により、ホワイトリストは複数のサーバ間で共有されるため、従来のホワイトリストをサーバ本体に持つ方式に比べて登録の効果が現れるのが速い。

【００３０】

本技術はメール受信要求のうち、大手ＩＳＰや頻繁に業務上のメールのやりとりがある送信元等ＳＰＡＭを送信してくる可能性が少ない、あるいは送られてきたとしても送信元として拒否する可能性の無い送信元と、それ以外の送信元の間に優先順位をつけることで、メール受信者にとってより重要なメールの遅延を防ぐ特徴を持つ。また、信頼していない送信元からのメールをチェックし、信頼できると判定した場合には信頼できる送信元リストに加えることでホワイトリストの維持管理のコストを低減するとともにホワイトリストを複数サーバ間で共有できるという特徴を持つ。

【００３１】

以上の実施例においてはメールサーバの例について説明したが、ホワイトリスト用サーバおよび通常サーバはメールサーバ以外のサーバであってもよく、その場合は、メールサーバ機能１１２、１２２はそのサーバの機能となり、ＳＰＡＭ検知機能１１１、１２１はそのサーバにおける有害なものを検知する機能となる。

【００３２】

本実施例のホワイトリストを利用したサーバ割り当てシステムの実装はハードウェアでもソフトウェアでも実現できる。

【００３３】

以上、本発明者によってなされた発明を、前記実施例に基づき具体的に説明したが、本発明は、前記実施例に限定されるものではなく、その要旨を逸脱しない範囲において種々変更可能であることは勿論である。

【図面の簡単な説明】

【００３４】

【図１】本発明の実施例のホワイトリストを利用したサーバ割り当てシステムを説明するための図である。

【図２】本発明の実施例のＩＰパケット分離機１０２の内部の構成図を示す。

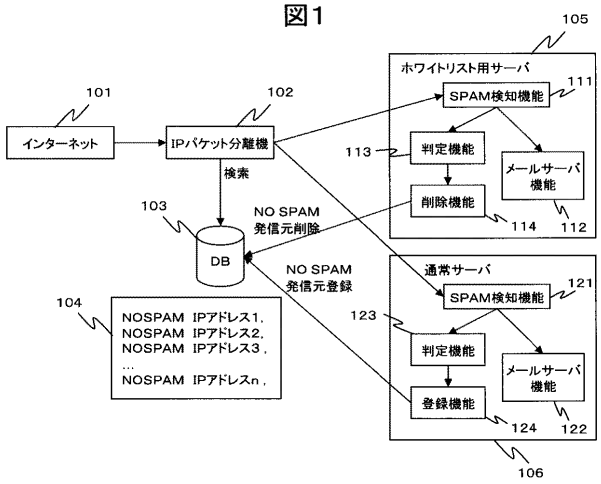
【符号の説明】

【００３５】

１０１…インターネット、１０２…ＩＰパケット分離機、１０３…ＤＢ、１０４…ホワイトリスト、１０５…ホワイトリスト用サーバ、１０６…通常サーバ、１１１、１２１…ＳＰＡＭ検知機能、１１２、１２２…メールサーバ機能、１１３、１２３…判定機能、１１４…削除機能、１２４…登録機能、２０１…受信手段、２０２…検索手段、２０３…転送手段

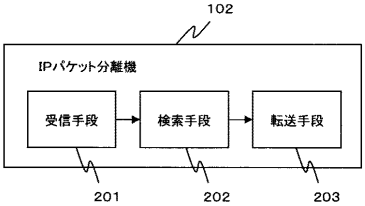
【図１】

図1



【図２】

図2



フロントページの続き

Ｆターム(参考) 5B285 AA05 AA06 AA07 BA01 CA04 CA32 DA05
5K030 GA03 HA08 HD03 LB05 LC11 LC13