(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2005-208780
(P2005-208780A)
(43)公開日　平成17年8月4日(2005.8.4)

(51)Int.Cl.[7]	F I			テーマコード（参考）
G06F 13/00	G06F	13/00	610Q	5K030
H04L 12/58	H04L	12/58	100F	
H04L 12/66	H04L	12/66	B	

審査請求 未請求　請求項の数 31　ＯＬ　（全 21 頁）

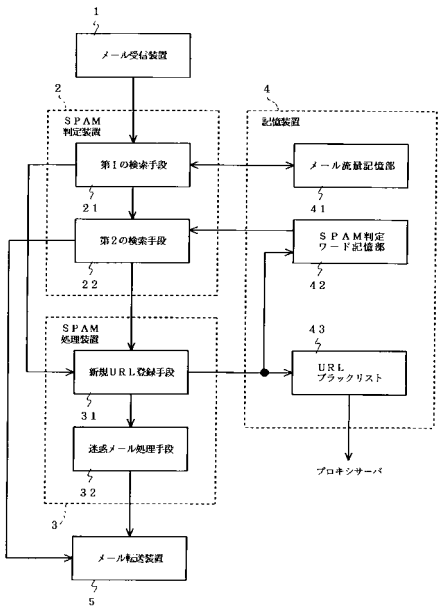
(21)出願番号　特願2004-12542(P2004-12542)
(22)出願日　平成16年1月21日(2004.1.21)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(74)代理人　100088812
弁理士　▲柳▼川　信
(72)発明者　安田　真人
東京都港区芝五丁目７番１号　日本電気株式会社内

Ｆターム(参考)　5K030 GA15 HA08 HC01 HD03 HD06 JA10 KA05 MA13 MB18 MC08

(54)【発明の名称】メールフィルタリングシステム及びそれに用いるＵＲＬブラックリスト動的構築方法

(57)【要約】
【課題】　迷惑メールの検出率を高め、管理負担を軽減可能なメールフィルタリング装置を提供する。
【解決手段】　第１の検索手段２１は電子メールの本文の送信元ＩＰアドレスを基にメール流量記憶部４１のエントリを検索し、対応するエントリが見つかると対応するカウント値を規定値だけ増加させ、対応するエントリが見つからなければ電子メールの送信元ＩＰアドレスとカウンタの初期値とからなるエントリをメール流量記憶部４１に新規に登録する。第２の検索手段２２は電子メールにＳＰＡＭ判定ワード記憶部４２のＳＰＡＭ判定ワードが含まれていないかを検索する。新規ＵＲＬ登録手段３１は電子メールから“ｈｔｔｐ”で始まる文字列を抜き出し、ＳＰＡＭ判定ワード記憶部４２及びＵＲＬブラックリスト４３に記録する。迷惑メール処理手段３２は迷惑メールに予め規定したアクションを実行する。
【選択図】　図１



【特許請求の範囲】
【請求項１】
受信メールが迷惑メールか否かを判定する検索手段と、前記迷惑メールと判定された電子メールの本文に書かれたＵＲＬ（Ｕｎｉｆｏｒｍ　Ｒｅｓｏｕｒｃｅ　Ｌｏｃａｔｏｒ）を前記迷惑メールの判定ワード候補として登録する登録手段とを有し、その登録されたＵＲＬを基に前記検索手段が前記迷惑メールか否かを判定することを特徴とするメールフィルタリングシステム。
【請求項２】
一定時間のメールの流量をチェックするために前記電子メールのソースＩＰ（Ｉｎｔｅｒｎｅｔ　ｐｒｏｔｏｃｏｌ）アドレスとカウンタ値との組み合わせを保持するメール流量記憶手段と、予め設定された判定ワードを記憶する判定ワード記憶手段とを含み、
前記検索手段は、前記受信メールのソースＩＰアドレスに対応する前記メール流量記憶手段のカウント値を規定値だけ増加させかつその値がしきい値を超えた時に前記迷惑メールと判定する第１の検索手段と、前記判定ワード記憶手段に登録された前記判定ワードが前記受信メールの本文中に含まれている時に前記迷惑メールと判定する第２の検索手段とからなることを特徴とする請求項１記載のメールフィルタリングシステム。
【請求項３】
前記迷惑メールと判定された電子メールに対して少なくとも予め設定された廃棄及び遅延を行う迷惑メール処理手段を含むことを特徴とする請求項１または請求項２記載のメールフィルタリングシステム。
【請求項４】
前記迷惑メールと判定された電子メールの本文から前記登録手段で取り出されたＵＲＬを記録するブラックリスト記録手段を含むことを特徴とする請求項１から請求項３のいずれか記載のメールフィルタリングシステム。
【請求項５】
前記登録手段は、前記迷惑メールと判定された電子メールの本文から取り出したＵＲＬが予め設定された所定ＵＲＬの時に当該ＵＲＬの前記ブラックリスト記録手段への記録を抑止することを特徴とする請求項４記載のメールフィルタリングシステム。
【請求項６】
前記ブラックリスト記録手段への記録を抑止するために予め設定された所定ＵＲＬを記録するホワイトリスト記録手段を含むことを特徴とする請求項５記載のメールフィルタリングシステム。
【請求項７】
前記迷惑メールと判定された電子メールの本文から前記登録手段で取り出されたＵＲＬを外部に表示し、その表示内容に基づいた外部からの指示に応じて前記ブラックリスト記録手段への記録を行うことを特徴とする請求項４から請求項６のいずれか記載のメールフィルタリングシステム。
【請求項８】
前記登録手段で取り出されたＵＲＬを一時保持するＵＲＬ候補リスト記録手段を含み、前記ＵＲＬ候補リスト記録手段に保持されたＵＲＬを外部に表示し、その表示内容に基づいた外部からの指示に応じて前記ブラックリスト記録手段への記録を行うことを特徴とする請求項７記載のメールフィルタリングシステム。
【請求項９】
一定時間のメールの流量をチェックするために前記電子メールの本文から取り出されたＵＲＬとカウンタ値との組み合わせを保持するメール流量記憶手段と、予め設定された判定ワードを記憶する判定ワード記憶手段と、前記メール流量記憶手段のカウント値がしきい値を超えたエントリに対応する前記ＵＲＬを取得する取得手段と、前記取得手段が取得したＵＲＬを記録するブラックリスト記録手段とを含み、
前記検索手段は、前記受信メールの本文から取り出されたＵＲＬに対応する前記メール流量記憶手段のカウント値を規定値だけ増加させかつその値がしきい値を超えた時に前記

迷惑メールと判定する第１の検索手段と、前記判定ワード記憶手段に登録された前記判定ワードが前記受信メールの本文中に含まれている時に前記迷惑メールと判定する第２の検索手段とからなることを特徴とする請求項１記載のメールフィルタリングシステム。

【請求項１０】

端末へ送信された電子メールのＩＰ（Ｉｎｔｅｒｎｅｔ　ｐｒｏｔｏｃｏｌ）パケットから前記電子メールの本文を取り出すメール受信装置と、前記電子メールの流量をチェックするとともに迷惑メールと判定される用語が含まれていないかを検索しかつ前記迷惑メールと判定された電子メールの本文からＵＲＬ（Ｕｎｉｆｏｒｍ　Ｒｅｓｏｕｒｃｅ　Ｌｏｃａｔｏｒ）を抽出して少なくとも廃棄及び遅延のうちの一方のアクションを起こすＳＰＡＭ処理装置と、前記ＵＲＬの文字列とカウント値との組み合わせをエントリとして記憶する記憶装置と、前記記憶装置に記憶されたＵＲＬとカウンタ値とからなるエントリの中の前記カウンタ値が予め設定されたしきい値を超えているものを取り出して前記記憶装置内のブラックリストに保存するブラックリスト構築装置と、前記電子メールの本文を前記ＩＰパケットに収容して装置外に転送するメール転送装置とを有することを特徴とするメールフィルタリングシステム。

【請求項１１】

受信メールが迷惑メールか否かを判定する検索手段と、前記迷惑メールと判定された電子メールの本文に書かれたＵＲＬ（Ｕｎｉｆｏｒｍ　Ｒｅｓｏｕｒｃｅ　Ｌｏｃａｔｏｒ）を前記迷惑メールの判定ワード候補として登録する登録手段とを有し、その登録されたＵＲＬを基に前記検索手段が前記迷惑メールか否かを判定することを特徴とするメールフィルタリング装置。

【請求項１２】

一定時間のメールの流量をチェックするために前記電子メールのソースＩＰ（Ｉｎｔｅｒｎｅｔ　ｐｒｏｔｏｃｏｌ）アドレスとカウンタ値との組み合わせを保持するメール流量記憶手段と、予め設定された判定ワードを記憶する判定ワード記憶手段とを含み、

前記検索手段は、前記受信メールのソースＩＰアドレスに対応する前記メール流量記憶手段のカウント値を規定値だけ増加させかつその値がしきい値を超えた時に前記迷惑メールと判定する第一の検索手段と、前記判定ワード記憶手段に登録された前記判定ワードが前記受信メールの本文中に含まれている時に前記迷惑メールと判定する第二の検索手段とからなることを特徴とする請求項１１記載のメールフィルタリング装置。

【請求項１３】

前記迷惑メールと判定された電子メールに対して少なくとも予め設定された廃棄及び遅延を行う迷惑メール処理手段を含むことを特徴とする請求項１１または請求項１２記載のメールフィルタリング装置。

【請求項１４】

前記迷惑メールと判定された電子メールの本文から前記登録手段で取り出されたＵＲＬを記録するブラックリスト記録手段を含むことを特徴とする請求項１１から請求項１３のいずれか記載のメールフィルタリング装置。

【請求項１５】

前記登録手段は、前記迷惑メールと判定された電子メールの本文から取り出したＵＲＬが予め設定された所定ＵＲＬの時に当該ＵＲＬの前記ブラックリスト記録手段への記録を抑止することを特徴とする請求項１４記載のメールフィルタリング装置。

【請求項１６】

前記ブラックリスト記録手段への記録を抑止するために予め設定された所定ＵＲＬを記録するホワイトリスト記録手段を含むことを特徴とする請求項１５記載のメールフィルタリング装置。

【請求項１７】

前記迷惑メールと判定された電子メールの本文から前記登録手段で取り出されたＵＲＬを外部に表示し、その表示内容に基づいた外部からの指示に応じて前記ブラックリスト記録手段への記録を行うことを特徴とする請求項１４から請求項１６のいずれか記載のメー

ルフィルタリング装置。
【請求項１８】
前記登録手段で取り出されたＵＲＬを一時保持するＵＲＬ候補リスト記録手段を含み、前記ＵＲＬ候補リスト記録手段に保持されたＵＲＬを外部に表示し、その表示内容に基づいた外部からの指示に応じて前記ブラックリスト記録手段への記録を行うことを特徴とする請求項１７記載のメールフィルタリング装置。
【請求項１９】
一定時間のメールの流量をチェックするために前記電子メールの本文から取り出されたＵＲＬとカウンタ値との組み合わせを保持するメール流量記憶手段と、予め設定された判定ワードを記憶する判定ワード記憶手段と、前記メール流量記憶手段のカウント値がしきい値を超えたエントリに対応する前記ＵＲＬを取得する取得手段と、前記取得手段が取得したＵＲＬを記録するブラックリスト記録手段とを含み、
前記検索手段は、前記受信メールの本文から取り出されたＵＲＬに対応する前記メール流量記憶手段のカウント値を規定値だけ増加させかつその値がしきい値を超えた時に前記迷惑メールと判定する第一の検索手段と、前記判定ワード記憶手段に登録された前記判定ワードが前記受信メールの本文中に含まれている時に前記迷惑メールと判定する第二の検索手段とからなることを特徴とする請求項１１記載のメールフィルタリング装置。
【請求項２０】
端末へ送信された電子メールのＩＰ（Ｉｎｔｅｒｎｅｔ　ｐｒｏｔｏｃｏｌ）パケットから前記電子メールの本文を取り出すメール受信装置と、前記電子メールの流量をチェックするとともに迷惑メールと判定される用語が含まれていないかを検索しかつ前記迷惑メールと判定された電子メールの本文からＵＲＬ（Ｕｎｉｆｏｒｍ　Ｒｅｓｏｕｒｃｅ　Ｌｏｃａｔｏｒ）を抽出して少なくとも廃棄及び遅延のうちの一方のアクションを起こすＳＰＡＭ処理装置と、前記ＵＲＬの文字列とカウント値との組み合わせをエントリとして記憶する記憶装置と、前記記憶装置に記憶されたＵＲＬとカウンタ値とからなるエントリの中の前記カウンタ値が予め設定されたしきい値を超えているものを取り出して前記記憶装置内のブラックリストに保存するブラックリスト構築装置と、前記電子メールの本文を前記ＩＰパケットに収容して装置外に転送するメール転送装置とを有することを特徴とするメールフィルタリング装置。
【請求項２１】
受信メールのフィルタリング処理を行うメールフィルタリング装置を含むシステムにおいてＵＲＬ（Ｕｎｉｆｏｒｍ　Ｒｅｓｏｕｒｃｅ　Ｌｏｃａｔｏｒ）のブラックリストを構築するＵＲＬブラックリスト動的構築方法であって、
前記メールフィルタリング装置側に、前記受信メールが迷惑メールか否かを判定する第１のステップと、前記迷惑メールと判定された電子メールの本文に書かれたＵＲＬを前記迷惑メールの判定ワード候補として登録する第２のステップとを有し、
前記第１のステップは、その登録されたＵＲＬを基に前記迷惑メールか否かを判定することを特徴とするＵＲＬブラックリスト動的構築方法。
【請求項２２】
前記第１のステップは、一定時間のメールの流量をチェックするために前記電子メールのソースＩＰ（Ｉｎｔｅｒｎｅｔ　ｐｒｏｔｏｃｏｌ）アドレスとカウンタ値との組み合わせを保持するメール流量記憶手段のカウント値を規定値だけ増加させかつその値がしきい値を超えた時に前記迷惑メールと判定する第３のステップと、予め設定された判定ワードを記憶する判定ワード記憶手段に登録された前記判定ワードが前記受信メールの本文中に含まれている時に前記迷惑メールと判定する第４のステップとを含むことを特徴とする請求項２１記載のＵＲＬブラックリスト動的構築方法。
【請求項２３】
前記メールフィルタリング装置側に、前記迷惑メールと判定された電子に対して少なくとも予め設定された廃棄及び遅延を行うステップを含むことを特徴とする請求項２１または請求項２２記載のＵＲＬブラックリスト動的構築方法。

【請求項２４】
前記メールフィルタリング装置側に、前記迷惑メールと判定された電子メールの本文から前記第２のステップで取り出されたＵＲＬをブラックリスト記録手段に記録するステップを含むことを特徴とする請求項２１から請求項２３のいずれか記載のＵＲＬブラックリスト動的構築方法。
【請求項２５】
前記第２のステップは、前記迷惑メールと判定された電子メールの本文から取り出したＵＲＬが予め設定された所定ＵＲＬの時に当該ＵＲＬの前記ブラックリスト記録手段への記録を抑止することを特徴とする請求項２４記載のＵＲＬブラックリスト動的構築方法。
【請求項２６】
前記第２のステップは、前記迷惑メールと判定された電子メールの本文から取り出したＵＲＬが前記ブラックリスト記録手段への記録を抑止するために予め設定された所定ＵＲＬを記録するホワイトリスト記録手段に記録された所定ＵＲＬの時に当該ＵＲＬの前記ブラックリスト記録手段への記録を抑止することを特徴とする請求項２５記載のＵＲＬブラックリスト動的構築方法。
【請求項２７】
前記迷惑メールと判定された電子メールの本文から前記第２のステップで取り出されたＵＲＬを外部に表示し、その表示内容に基づいた外部からの指示に応じて前記ブラックリスト記録手段への記録を行うことを特徴とする請求項２４から請求項２６のいずれか記載のＵＲＬブラックリスト動的構築方法。
【請求項２８】
前記第２のステップで取り出されたＵＲＬをＵＲＬ候補リスト記録手段に一時保持し、前記ＵＲＬ候補リスト記録手段に保持されたＵＲＬを外部に表示し、その表示内容に基づいた外部からの指示に応じて前記ブラックリスト記録手段への記録を行うことを特徴とする請求項２７記載のＵＲＬブラックリスト動的構築方法。
【請求項２９】
前記第１のステップは、一定時間のメールの流量をチェックするために前記電子メールの本文から取り出されたＵＲＬとカウンタ値との組み合わせを保持するメール流量記憶手段のカウント値を規定値だけ増加させかつその値がしきい値を超えた時に前記迷惑メールと判定する第３のステップと、予め設定された判定ワードを記憶する判定ワード記憶手段に登録された前記判定ワードが前記受信メールの本文中に含まれている時に前記迷惑メールと判定する第４のステップとを含み、
前記メールフィルタリング装置側に、前記メール流量記憶手段のカウント値がしきい値を超えたエントリに対応する前記ＵＲＬを取得するステップと、その取得したＵＲＬをブラックリスト記録手段に記録するステップとを含むことを特徴とする請求項２１記載のＵＲＬブラックリスト動的構築方法。
【請求項３０】
端末へ送信された電子メールのＩＰ（Ｉｎｔｅｒｎｅｔ　ｐｒｏｔｏｃｏｌ）パケットから前記電子メールの本文をメール受信装置にて取り出し、前記電子メールの流量をチェックするとともに迷惑メールと判定される用語が含まれていないかを検索しかつ前記迷惑メールと判定された電子メールの本文からＵＲＬ（Ｕｎｉｆｏｒｍ　Ｒｅｓｏｕｒｃｅ　Ｌｏｃａｔｏｒ）を抽出して少なくとも廃棄及び遅延のうちの一方のアクションをＳＰＡＭ処理装置にて実行し、前記ＵＲＬの文字列とカウント値との組み合わせをエントリとして記憶装置に記憶し、前記記憶装置に記憶されたＵＲＬとカウンタ値とからなるエントリの中の前記カウンタ値が予め設定されたしきい値を超えているものをブラックリスト構築装置にて取り出して前記記憶装置内のブラックリストに保存し、メール転送装置にて前記電子メールの本文を前記ＩＰパケットに収容して装置外に転送することを特徴とするＵＲＬブラックリスト動的構築方法。
【請求項３１】
受信メールのフィルタリング処理を行うメールフィルタリング装置を含むシステムにお

いてＵＲＬ（Ｕｎｉｆｏｒｍ　Ｒｅｓｏｕｒｃｅ　Ｌｏｃａｔｏｒ）のブラックリストを構築するＵＲＬブラックリスト動的構築方法のプログラムであって、コンピュータに、前記受信メールが迷惑メールか否かを判定する第１の処理と、前記迷惑メールと判定された電子メールの本文に書かれたＵＲＬを前記迷惑メールの判定ワード候補として登録する第２の処理とを実行させ、前記第１の処理においてその登録されたＵＲＬを基に前記迷惑メールか否かを判定させるためのプログラム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明はメールフィルタリングシステム、メールフィルタリング装置及びそれらに用いるＵＲＬブラックリスト動的構築方法並びにそのプログラムに関し、特に迷惑メール等をフィルタリングするメールフィルタリングシステムに関する。

【背景技術】

【０００２】

メールフィルタリングシステムは、広告業者が大量のメールアドレスに対して送信した迷惑メールをユーザに届く前に遮断したり、遅延させることによって、ユーザのＳＰＡＭメールによる被害及びネットワーク内に掛かる負荷を低減させるために用いられている。

【０００３】

従来、メールフィルタリング装置の一例としては、ＳＰＡＭ判定ワードが電子メールの本文中に含まれていた場合、その電子メールを拒否する装置がある。このメールフィルタリング装置は、主にネットワークインタフェース部（ＩＦ部）と、メール記憶部と、不要メール情報管理部と、メール受信制御部と、ＷＥＢメール装置とから構成されている（例えば、特許文献１参照）。

【０００４】

ネットワークインタフェース部は、ネットワークとの情報・データの授受を制御し、送信者端末からの電子メールを受信する。メール記憶部はインタフェース部で受信する電子メールを保管する。不要メール情報管理部はメール送信元の識別情報等、不要メールや迷惑メールに関する各種情報を記憶する。

【０００５】

ＷＥＢメール装置は受信者端末当てに送られてきた電子メールの各種情報が表示されるＷＥＢ上の所定領域である。メール受信制御部はネットワークインタフェース部とメール記憶部と不要メール情報管理部とＷＥＢメール装置とを制御し、不要メールや迷惑メールのフィルタリング設定等を行う。

【０００６】

上記のメールフィルタリング装置では、受信した電子メールをメール記憶部に記憶し、その電子メールを不要メール情報管理部の記憶内容と比較し、一致した場合に迷惑メールとみなし、その電子メールの受信を拒否している。

【０００７】

【特許文献１】特開２００３－１７３３１４号公報

【発明の開示】

【発明が解決しようとする課題】

【０００８】

しかしながら、上述した従来のメールフィルタリング装置では、不要メール情報管理部にＳＰＡＭ判定ワードのリストのみが記入されており、一定時間のメールの流量をチェックしていないので、不要メール情報管理部に記憶したＳＰＡＭ判定ワードがメール本文中に記載されていない限り、ネットワークの負荷が増大してしまうような迷惑メールも全て通過してしまうという問題がある。

【０００９】

また、従来のメールフィルタリング装置では、迷惑メールを検知した時に、迷惑メールを拒否するだけで、当該迷惑メールの内容を不要メール情報管理部のデータベースにフィ

ードバックしていないので、ＳＰＡＭ判定ワードを手作業で登録しなければならないという問題がある。

【００１０】

さらに、従来のメールフィルタリング装置では、迷惑メールを検知した時に、迷惑メールを拒否するだけで、当該迷惑メールの内容を不要メール情報管理部のデータベースにフィードバックしていないので、迷惑メールを見つけた場合、迷惑メールを拒否するだけなので、同一広告業者が電子メールの本文の内容を変えて迷惑メールを送信すると、それに対処することができないという問題がある。

【００１１】

そこで、本発明の目的は上記の問題点を解消し、迷惑メールの検出率を高めることができ、管理負担を軽減することができるメールフィルタリングシステム、メールフィルタリング装置及びそれらに用いるＵＲＬブラックリスト動的構築方法並びにそのプログラムを提供することにある。

【課題を解決するための手段】

【００１２】

本発明によるメールフィルタリングシステムは、受信メールが迷惑メールか否かを判定する検索手段と、前記迷惑メールと判定された電子メールの本文に書かれたＵＲＬ（Ｕｎｉｆｏｒｍ　Ｒｅｓｏｕｒｃｅ　Ｌｏｃａｔｏｒ）を前記迷惑メールの判定ワード候補として登録する登録手段とを備え、その登録されたＵＲＬを基に前記検索手段が前記迷惑メールか否かを判定している。

【００１３】

本発明によるメールフィルタリング装置は、受信メールが迷惑メールか否かを判定する検索手段と、前記迷惑メールと判定された電子メールの本文に書かれたＵＲＬ（Ｕｎｉｆｏｒｍ　Ｒｅｓｏｕｒｃｅ　Ｌｏｃａｔｏｒ）を前記迷惑メールの判定ワード候補として登録する登録手段とを備え、その登録されたＵＲＬを基に前記検索手段が前記迷惑メールか否かを判定している。

【００１４】

本発明によるＵＲＬブラックリスト動的構築方法は、受信メールのフィルタリング処理を行うメールフィルタリング装置を含むシステムにおいてＵＲＬ（Ｕｎｉｆｏｒｍ　Ｒｅｓｏｕｒｃｅ　Ｌｏｃａｔｏｒ）のブラックリストを構築するＵＲＬブラックリスト動的構築方法であって、

前記メールフィルタリング装置側に、前記受信メールが迷惑メールか否かを判定する第１のステップと、前記迷惑メールと判定された電子メールの本文に書かれたＵＲＬを前記迷惑メールの判定ワード候補として登録する第２のステップとを備え、

前記第１のステップは、その登録されたＵＲＬを基に前記迷惑メールか否かを判定している。

【００１５】

本発明によるＵＲＬブラックリスト動的構築方法のプログラムは、受信メールのフィルタリング処理を行うメールフィルタリング装置を含むシステムにおいてＵＲＬ（Ｕｎｉｆｏｒｍ　Ｒｅｓｏｕｒｃｅ　Ｌｏｃａｔｏｒ）のブラックリストを構築するＵＲＬブラックリスト動的構築方法のプログラムであって、コンピュータに、前記受信メールが迷惑メールか否かを判定する第１の処理と、前記迷惑メールと判定された電子メールの本文に書かれたＵＲＬを前記迷惑メールの判定ワード候補として登録する第２の処理とを実行させ、前記第１の処理においてその登録されたＵＲＬを基に前記迷惑メールか否かを判定させている。

【００１６】

すなわち、本発明のメールフィルタリングシステムは、迷惑メール（ＳＰＡＭメール）の本文に書かれたＵＲＬ（Ｕｎｉｆｏｒｍ　Ｒｅｓｏｕｒｃｅ　Ｌｏｃａｔｏｒ）をＳＰＡＭ判定ワードの候補として登録し、同じ広告業者から来たメールをフィルタリング可能にすることを特徴としている。

【００１７】
また、本発明のメールフィルタリングシステムは、迷惑メールと判定した後、迷惑メールの本文に書かれたＵＲＬを新規にデータベースに登録し、広告業者のＵＲＬブラックリストの候補を自動生成することを特徴としている。
【００１８】
より具体的に説明すると、本発明のメールフィルタリングシステムでは、ＳＰＡＭ判定装置がメール受信装置から電子メールのパケット情報を受け取り、第一の検索手段及び第二の検索手段の２カ所で迷惑メールかどうかの判定を行っている。
【００１９】
第一の検索手段ではメール流量記憶部内の受信メールのソースＩＰ（Ｉｎｔｅｒｎｅｔ Ｐｒｏｔｏｃｏｌ）アドレスに対応するエントリのカウント値を規定値だけ増加させ、その値がしきい値を超えた場合、迷惑メールと判定する。
【００２０】
第二の検索手段ではＳＰＡＭ判定ワード記憶部に記憶されたＳＰＡＭ判定ワードが電子メールの本文中に含まれていないかを検索し、ＳＰＡＭ判定ワードが含まれていた場合に迷惑メールと判定する。
【００２１】
ＳＰＡＭ判定ワード記憶部には、予め設定したＳＰＡＭ判定ワードリストが記録されている。ＳＰＡＭ判定ワードとは、電子メールの本文中に含まれていたら迷惑メールと判定される“出会い系”、“アダルト”等の言葉である。
【００２２】
迷惑メールとみなされたメールは、新規ＵＲＬ登録手段によって、電子メール本文から“ｈｔｔｐ（ｈｙｐｅｒ ｔｅｘｔ ｔｒａｎｓｆｅｒ ｐｒｏｔｏｃｏｌ）”から始まる文字列がＵＲＬとして取り出され、取り出したＵＲＬがＳＰＡＭ判定ワード記憶部とＵＲＬブラックリストとに登録されていない場合、新規にＳＰＡＭ判定ワード記憶部とＵＲＬブラックリストとに登録する。
【００２３】
ＵＲＬ登録後、迷惑メール処理手段は、電子メールに対してユーザが設定したアクション（電子メールの廃棄や電子メールの遅延等）が行われる。装置外に電子メールが転送されるアクションの場合には、メール送信装置によって電子メールの本文が送られる。
【００２４】
これによって、本発明のメールフィルタリングシステムでは、迷惑メールを発送した広告業者のＵＲＬブラックリストを動的に構築することが可能となる。つまり、本発明のメールフィルタリングシステムでは、携帯電話機等に送られるＳＰＡＭメールの文字数が少ない代わりに、広告サイトのＵＲＬリンクがメール本文中にほぼ必ず貼られるという点に着目し、ＳＰＡＭメール内にあったＵＲＬリンクをＳＰＡＭ判定ワードとして登録することによって、ＳＰＡＭメールの検出率を高めることが可能となる。
【００２５】
また、本発明のメールフィルタリングシステムでは、迷惑メールからＵＲＬを取得して自動的にＵＲＬブラックリストを生成しているので、迷惑メールに記載されたＵＲＬへのアクセスを禁止するために、管理者がブラックリストのＵＲＬを自ら収集して手作業で登録する必要がなくなり、管理負担を軽減することが可能となる。
【００２６】
迷惑メールからＵＲＬを抽出する理由は、迷惑メールの多くが広告用サイトの宣伝に用いられ、電子メールの本文の中にほぼ必ず広告用サイトのＵＲＬリンクが貼られているので、その抽出したＵＲＬから迷惑メールを特定することが可能となるからである。
【００２７】
しかしながら、実用の際には、取得したＵＲＬを、ブラックリストに登録しても良いかどうかをチェックする必要がある。その際、取得したＵＲＬをＳＰＡＭ判定ワード記憶部及びＵＲＬブラックリストに登録する前に、一旦、別に用意したＵＲＬ候補リストに保存

し、オペレータがその候補リストの中から登録しても良いものを選び出すことによって登録されるようにするとよい。

【００２８】

さらに、本発明のメールフィルタリングシステムでは、迷惑メールから抽出したＵＲＬをＳＰＡＭ判定ワード記憶部に登録することによって、一度、迷惑メールを配布した広告主と同じ広告主から送信元を変えてその迷惑メールが配布される場合でも、同じ広告主からの電子メールを全て迷惑メールとして処理することが可能となる。

【００２９】

ＳＰＡＭ判定ワード記憶部に登録して迷惑メールのチェックをする理由として、時間Ｔ０から迷惑メールが大量に送信されたとすると、時間Ｔ０から時間Ｔ１にかけてメール流量記憶部で流量がカウントされ、時間Ｔ１で閾値を超えるとすると、時間Ｔ１以降の迷惑メールが迷惑メールとして認識される。逆に言えば、時間Ｔ０から時間Ｔ１にかけての電子メールは迷惑メールとして処理されない。

【００３０】

続いて、時間Ｔ２から充分に時間が経過した時間Ｔ３に、同じ広告業者の迷惑メールが大量に流れてきたとすると、時間Ｔ３から時間Ｔ４にかけての電子メールは、もし迷惑メールから抽出したＵＲＬをＳＰＡＭ判定ワード記憶部に記憶していなければ、メール流量記憶部のカウント値がリセットされる程、充分に時間が経過しているために、カウントが閾値を超えるまでは迷惑メールが通過してしまうが、迷惑メールから抽出したＵＲＬをＳＰＡＭ判定ワード記憶部に記憶していれば、第一の検索手段で迷惑メールとして検出されなかった迷惑メールも、第二の検索手段で迷惑メールとして認識されるので、一度、迷惑メールとして認識した電子メールを再び通過させてしまうことがなくなる。

【００３１】

さらにまた、本発明のメールフィルタリングシステムでは、迷惑メールからＵＲＬを抽出して直接ブラックリストを生成しているので、局所的にしか出回らない広告メールのＵＲＬもブラックリストに登録することが可能となる。

【００３２】

本発明のメールフィルタリングシステムでは、電子メールの本文の内容が変わっても、同一広告業者のサイトとして同じＵＲＬが迷惑メールの本文中に含まれていることを利用し、ＵＲＬを不要メール情報管理部のデータベースにフィードバックしているので、同一広告業者が電子メールの本文の内容を変えて迷惑メールを送信しても、あるいは送信元を変えて迷惑メールを送信しても、それらに対処することが可能となる。

【発明の効果】

【００３３】

本発明は、以下に述べるような構成及び動作とすることで、迷惑メールの検出率を高めることができ、管理者の管理負担を軽減することができるという効果が得られる。

【発明を実施するための最良の形態】

【００３４】

次に、本発明の実施例について図面を参照して説明する。図１は本発明の一実施例によるメールフィルタリング装置（システム）の構成を示すブロック図である。図１において、本発明の一実施例によるメールフィルタリング装置は、携帯電話やメール端末等へ送信された電子メールのＩＰ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）パケットから電子メールの本文を取り出すメール受信装置１と、電子メールの流量をチェックするとともに迷惑（ＳＰＡＭ）メールと判定される用語が含まれていないかを検索するＳＰＡＭ判定装置２と、迷惑メールと判定された電子メールの本文からＵＲＬ（Ｕｎｉｆｏｒｍ　Ｒｅｓｏｕｒｃｅ　Ｌｏｃａｔｏｒ）を抽出して廃棄・遅延等のアクションを起こすＳＰＡＭ処理装置３と、情報を記憶する記憶装置４と、電子メールの本文をＩＰパケットに収容して装置外に転送するメール転送装置５とから構成されている。

【００３５】

これらメール受信装置１、ＳＰＡＭ判定装置２、ＳＰＡＭ処理装置３、記憶装置４、メ

ール転送装置５は、それぞれプログラム制御によって動作する。ここで言うプログラムは、ＦＰＧＡ（Ｆｉｅｌｄ　Ｐｒｏｇｒａｍｍａｂｌｅ　Ｇａｔｅ　Ａｒｒａｙ）等の論理回路を含む。

【００３６】

メール受信装置１はパケットから電子メールの送信元ＩＰアドレス情報と電子メールの本文とを文字列として取り出し、その文字列をＳＰＡＭ判定装置２に出力する。

【００３７】

ＳＰＡＭ判定装置２は第１の検索手段２１と、第２の検索手段２２とを備えている。第１の検索手段２１はメール受信装置１から与えられた電子メールの本文の送信元ＩＰアドレスをキーとしてメール流量記憶部４１に記憶されたエントリを検索する。

【００３８】

第１の検索手段２１は対応するエントリが見つかった場合、対応するカウント値を規定値だけ増加させる。また、第１の検索手段２１は対応するエントリが存在しない場合、メールの送信元ＩＰアドレスとカウンタの初期値とからなるエントリをメール流量記憶部４１に新規に登録する。

【００３９】

第２の検索手段２２はＳＰＡＭ判定ワード記憶部４２からＳＰＡＭ判定ワードのリストを取得し、電子メールの本文中にＳＰＡＭ判定ワードが含まれていないかを検索する。

【００４０】

ＳＰＡＭメール処理装置３は新規ＵＲＬ登録手段３１と、迷惑メール処理手段３２とを備えている。新規ＵＲＬ登録手段３１は電子メールの本文中から“ｈｔｔｐ（ｈｙｐｅｒ　ｔｅｘｔ　ｔｒａｎｓｆｅｒ　ｐｒｏｔｏｃｏｌ）”で始まる文字列を抜き出し、ＳＰＡＭ判定ワード記憶部４２及びＵＲＬブラックリスト４３に記録する。

【００４１】

迷惑メール処理手段３２は予め規定したアクションを受信した迷惑メールに対して実行する。例えば、迷惑メール処理手段３２は規定されたアクションが廃棄であれば、メール転送装置５に受信メールを渡さずに、電子メールの情報を解放する。また、迷惑メール処理手段３２は規定されたアクションが遅延であれば、メール転送装置５に受信メールを渡す時間を遅らせる。

【００４２】

記憶装置４はメール流量記憶部４１と、ＳＰＡＭ判定ワード記憶部４２と、ＵＲＬブラックリスト４３とを備えている。メール流量記憶部４１は一定時間のメールの流量をチェックするために検索テーブル形式をとり、検索キーとしてソースＩＰアドレス、対応データとしてカウンタ値をとる。このカウンタ値は一定時間毎に値が減算され、カウンタ値が「０」になると、対応するエントリが削除される。

【００４３】

ＳＰＡＭ判定ワード記憶部４２はＳＰＡＭメールの判定基準となる言葉がリスト形式で記録されている。このリストはオペレータによって予め登録された項目と、新規ＵＲＬ登録手段３１から登録された項目とからなる。ＵＲＬブラックリスト４３は新規ＵＲＬ登録手段３１によって取り出されたＵＲＬを記録しており、その記憶内容は図示せぬプロキシサーバ等から読み出し可能となっている。

【００４４】

プロキシサーバでは、上記のＵＲＬブラックリスト４３から読み出した記憶内容を基に、迷惑メールと判定された電子メールから取り出したＵＲＬへのアクセスを禁止する制御を行う。したがって、本実施例では、プロキシサーバの代わりに、上記のＵＲＬへのアクセスを禁止する手段であれば、インタネットへのアクセス制御手段を配置することも可能である。

【００４５】

メール転送装置５は上記の第２の検索手段２２または迷惑メール処理手段３２から渡された電子メールの本文を、ＩＰパケットとして送信先に転送する。このメール転送装置５

としてはメールサーバ等が考えられ、その転送先としては電子メールの送受信を行う端末等が考えられる。

【００４６】

尚、この端末としては携帯電話端末も考えられる。その場合、携帯電話端末にはＳＰＡＭ判定装置２とＳＰＡＭ処理装置３と記憶装置４とが搭載され、ＵＲＬブラックリスト４３の記憶内容がアクセス制御手段に渡されることで、迷惑メールに記載されたＵＲＬへのアクセスをアクセス制御手段によって制限することが可能となる。

【００４７】

図２及び図３は本発明の一実施例によるメールフィルタリング装置の動作を示すフローチャートである。これら図１～図３を参照して本発明の一実施例によるメールフィルタリング装置の動作について説明する。

【００４８】

メール受信装置１は電子メールの入ったＩＰパケットを受信すると、その電子メールのＩＰパケットから送信元のＩＰアドレスを含むパケット情報と電子メールの本文とを含むメール情報を取得し、第１の検索手段２１に供給する（図２ステップＳ１）。

【００４９】

第１の検索手段２１はメール受信装置１から受け取ったパケット情報のソースＩＰアドレスと同じソースＩＰアドレスがメール流量記憶部４１に記載されているかどうかを調べる（図２ステップＳ２）。

【００５０】

第１の検索手段２１はメール流量記憶部４１に同じソースＩＰアドレスが記憶されていた場合（図２ステップＳ３）、対応するカウンタ値を読み出し、そのカウンタ値を規定値だけ増加させる（図２ステップＳ４）。その結果、カウンタ値が予め設定したしきい値を超えた場合（図２ステップＳ５）、第１の検索手段２１はそのＩＰアドレスに対応したメールを迷惑メールとみなし、電子メールの本文をＳＰＡＭメール処理装置３に送る。超えなかった場合（図２ステップＳ５）、第１の検索手段２１はその電子メールの本文を第２の検索手段２２に送る。

【００５１】

第１の検索手段２１は同じソースＩＰアドレスがメール流量記憶部４１に記憶されていなかった場合（図２ステップＳ３）、ソースＩＰアドレスとカウンタの初期値とからなるエントリをメール流量記憶部４１に記録する（図２ステップＳ６）。

【００５２】

メール流量記憶部４１ではソースＩＰアドレスとカウンタ値との組み合わせからなるエントリが登録されており、一定時間が経過する毎に全エントリのカウンタ値が規定値だけ減少し、カウンタ値が「０」以下になると、そのエントリが削除される。

【００５３】

第２の検索手段２２は第１の検索手段２１から受け取った電子メールの本文にＳＰＡＭ判定ワードが含まれていないかどうかを検索する（図２ステップＳ７）。第２の検索手段２２は検索するＳＰＡＭ判定ワードをＳＰＡＭ判定ワード記憶部４１から取得する。

【００５４】

電子メールの本文にＳＰＡＭ判定ワードが含まれていない場合（図２ステップＳ８）、第２の検索手段２２はメール情報をメール転送装置５に送る。ＳＰＡＭ判定ワードが含まれていた場合（図２ステップＳ８）、第２の検索手段２２はメール情報をＳＰＡＭメール処理装置３に送る。

【００５５】

ＳＰＡＭメール処理装置３に送られたメール情報は、最初に新規ＵＲＬ登録手段３１で処理される。新規ＵＲＬ登録手段３１は電子メールの本文中から“ｈｔｔｐ”で始まるＵＲＬを文字列として取り出す（図３ステップＳ９）。

【００５６】

ＵＲＬの取得に成功した場合（図３ステップＳ１０）、新規ＵＲＬ登録手段３１は取得

したＵＲＬをＳＰＡＭ判定ワード記憶部４２及びＵＲＬブラックリスト４３に記憶し、迷惑メール処理手段３２に処理を移す（図３ステップＳ１１，Ｓ１２）。

【００５７】

ＵＲＬの取得に失敗した場合（図３ステップＳ１０）、新規ＵＲＬ登録手段３１はＵＲＬの登録処理なしとし、処理を迷惑メール処理手段３２に移す。迷惑メール処理手段３２は新規ＵＲＬ登録手段３１から受け取った電子メールに対して予め規定したアクションを実行する（図３ステップＳ１３）。

【００５８】

規定したアクションの例としては、通過や廃棄、そして遅延がある。通過の場合には、メール情報をそのままメール転送装置５に転送する。廃棄の場合には、メール情報を迷惑メール処理手段３２で止め、全て解放する。遅延の場合には、迷惑メール処理手段３２で遅延されてメール転送装置５に送られる。

【００５９】

メール転送装置５は迷惑メール処理手段３２もしくは第２の検索手段２２から送られてきたメール情報をＩＰパケットの形式に変換し、電子メールの送信先へと転送する（図３ステップＳ１４）。

【００６０】

このように、本実施例では、携帯電話機等に送られる迷惑メールが、文字数が少ない代わりに、広告サイトのＵＲＬリンクが電子メールの本文中にほぼ必ず貼られるという点に着目し、迷惑メール内にあったＵＲＬリンクをＳＰＡＭ判定ワードとして登録することによって、ＳＰＡＭメールの検出率を高めることができる。

【００６１】

また、本実施例では、迷惑メールからＵＲＬを取得して自動的にＵＲＬブラックリストを生成しているので、管理者がブラックリストのＵＲＬを自ら収集して手作業で登録する必要がなくなり、管理負担を軽減することができる。迷惑メールからＵＲＬを抽出する理由としては、迷惑メールの多くが広告用サイトの宣伝に用いられ、電子メールの本文中にほぼ必ず広告用サイトのＵＲＬリンクが貼られているので、そのＵＲＬから迷惑メールを特定することができるためである。

【００６２】

しかしながら、実用の際には、取得したＵＲＬにブラックリストに登録されても良いかどうかをチェックする必要がある。その際、後述するように、取得したＵＲＬをＳＰＡＭ判定ワード記憶部４２及びＵＲＬブラックリスト４３に登録する前に、一旦、別に用意したＵＲＬ候補リストに保存し、オペレータがその候補リストの中から登録しても良いものを選び出すことによって登録されるようにするとよい。

【００６３】

さらに、本実施例では、迷惑メールから抽出したＵＲＬをＳＰＡＭ判定ワード記憶部４２に登録することによって、一度、迷惑メールを配布した広告主と同じ広告主からのメールを全て迷惑メールとして処理することができる。

【００６４】

図４を参照してＳＰＡＭ判定ワード記憶部４２にＵＲＬを登録して迷惑メールのチェックを行う理由について説明する。図４に示すように、時間Ｔ０から迷惑メールが大量に送信されたとすると、時間Ｔ０から時間Ｔ１にかけての時間帯Ａ１に、メール流量記憶部４１で流量がカウントされ、時間Ｔ１で閾値を超えるとすると、時間Ｔ１以降の時間帯Ａ２の迷惑メールが迷惑メールとして認識される。逆に言えば、時間Ｔ０から時間Ｔ１にかけて時間帯Ａ１の電子メールは、迷惑メールとして処理されない。

【００６５】

続いて、時間Ｔ２から充分に時間が経過した時間Ｔ３に、同じ広告業者の迷惑メールが大量に流れてきたとすると、時間Ｔ３から時間Ｔ４にかけての時間帯Ａ３の電子メールは、もし迷惑メールから抽出したＵＲＬをＳＰＡＭ判定ワード記憶部４２に記憶させていなければ、メール流量記憶部４１のカウント値がリセットされる程、充分に時間が経過して

いるために、カウントが閾値を超えるまでは迷惑メールが通過してしまう。但し、時間Ｔ４で閾値を超えると、時間Ｔ４以降の時間帯Ａ４の迷惑メールが迷惑メールとして認識される。

【００６６】

しかしながら、迷惑メールから抽出したＵＲＬをＳＰＡＭ判定ワード記憶部４２に記憶していれば、第１の検索手段２１で迷惑メールとして検出されなかった迷惑メールも、第２の検索手段２２で迷惑メールとして認識されるので、一度、時間帯Ａ２で迷惑メールとして認識した電子メールを、時間帯Ａ３において再び通過させてしまうことがなくなる。

【００６７】

さらにまた、本実施例では、迷惑メールからＵＲＬを抽出して直接ブラックリストを生成しているので、局所的にしか出回らない広告メールのＵＲＬもブラックリストに登録することができる。

【００６８】

図５は本発明の他の実施例によるメールフィルタリング装置の構成を示すブロック図である。図５において、本発明の他の実施例によるメールフィルタリング装置は記憶装置６にＵＲＬホワイトリスト６１を追加した以外は図１に示す本発明の一実施例と同様の構成となっており、同一構成要素には同一符号を付してある。本実施例において、ＵＲＬホワイトリスト６１にはＵＲＬブラックリスト４３に登録させたくないＵＲＬが予め登録されている。

【００６９】

例えば、短時間に大量に送信されるメールとしては、必ずしも迷惑メールだけではなく、メールマガジン等がある。このメールマガジン等では同一ＩＰアドレスから大量にメールが送信されるので、メール流量のしきい値を超えて迷惑メールとみなされることがある。

【００７０】

このメールマガジン等のＵＲＬはＵＲＬホワイトリスト６１にＵＲＬブラックリスト４３に登録させたくないＵＲＬとして登録しておくことで、上記の不具合を解消することができる。

【００７１】

図６及び図７は本発明の他の実施例によるメールフィルタリング装置の動作を示すフローチャートである。これら図５～図７を参照して本発明の他の実施例によるメールフィルタリング装置の動作について説明する。図６のステップＳ２１～Ｓ２８及び図７のステップＳ２９，Ｓ３２～Ｓ３５は図２のステップＳ１～Ｓ８及び図３のステップＳ９，Ｓ１１～Ｓ１４と同様の動作であるので、その動作についての説明は省略する。

【００７２】

メールコンテンツからＵＲＬを抽出した後（図７ステップＳ２９）、新規ＵＲＬ登録手段３１は抽出したＵＲＬをキーとしてＵＲＬホワイトリスト６１を検索する（図７ステップＳ３０）。新規ＵＲＬ登録手段３１は検索に成功すれば（図７ステップＳ３１）、迷惑メール処理を行わず、メール転送装置５に渡してその電子メールを転送する（図７ステップＳ３５）。

【００７３】

新規ＵＲＬ登録手段３１は検索に失敗した場合（図７ステップＳ３１）、ＳＰＡＭ判定ワード記憶部４２とＵＲＬブラックリスト４３とにそれぞれエントリを追加し（図７ステップＳ３２，Ｓ３３）、迷惑メール処理手段３２にて迷惑メール処理を行う（図７ステップＳ３４）。

【００７４】

尚、ＵＲＬホワイトリスト６１ではホワイトリストのエントリをＵＲＬとしているが、ホワイトリストのエントリをＵＲＬではなく、送信元メールアドレスとして登録してもよい。この場合、メールマガジンの本文にＵＲＬが含まれていなくても迷惑メールとしてフィルタリングされることはない。

【００７５】
図８は本発明の別の実施例によるメールフィルタリング装置の構成を示すブロック図である。図８において、本発明の別の実施例によるメールフィルタリング装置は記憶装置７に登録候補リスト７１を追加し、登録候補リスト７１に登録許可を指示するオペレータ制御部８を設けた以外は図１に示す本発明の一実施例と同様の構成となっており、同一構成要素には同一符号を付してある。
【００７６】
迷惑メールの本文から取得したＵＲＬは、必ずしも広告業者のＵＲＬのみが含まれているとは限らない。そのため、取得したＵＲＬをＵＲＬブラックリスト４３に登録すべきか否かの判断をする必要がある。
【００７７】
そこで、本実施例では記憶装置７内に新たに登録候補リスト７１を設置し、新規ＵＲＬ登録手段３１によって取得したＵＲＬを一時的に登録候補リスト７１に記憶する。
【００７８】
オペレータはオペレータ制御部８から登録候補リスト７１に記憶されているＵＲＬのリストを参照し、登録の許可・不許可を決定し、登録を許可されたＵＲＬのみＳＰＡＭ判定ワード記憶部４２及びＵＲＬブラックリスト４３に記憶させるようにする。これによって、本実施例では、本来、ＵＲＬブラックリスト４３に載せるべきではないＵＲＬを事前に排除することができる。
【００７９】
図９は本発明の別の実施例によるメールフィルタリング装置の動作を示すフローチャートであり、図１０は本発明の別の実施例によるオペレータ制御部８における登録候補リスト選択処理を示すフローチャートである。これら図８～図１０を参照して本発明の別の実施例によるメールフィルタリング装置の動作について説明する。
【００８０】
メール受信装置１は電子メールの入ったＩＰパケットを受信すると、その電子メールのＩＰパケットから送信元のＩＰアドレスを含むパケット情報と電子メールの本文とを含むメール情報を取得し、第１の検索手段２１に供給する（図９ステップＳ６１）。
【００８１】
第１の検索手段２１はメール受信装置１から受け取ったパケット情報のソースＩＰアドレスと同じソースＩＰアドレスがメール流量記憶部４１に記載されているかどうかを調べる（図９ステップＳ６２）。
【００８２】
第１の検索手段２１はメール流量記憶部４１に同じソースＩＰアドレスが記憶されていた場合（図９ステップＳ６３）、対応するカウンタ値を読み出し、そのカウンタ値を規定値だけ増加させる（図９ステップＳ６４）。その結果、カウンタ値が予め設定したしきい値を超えた場合（図９ステップＳ６５）、第１の検索手段２１はそのＩＰアドレスに対応したメールを迷惑メールとみなし、電子メールの本文をＳＰＡＭメール処理装置３に送る。超えなかった場合（図９ステップＳ６５）、第１の検索手段２１はその電子メールの本文を第２の検索手段２２に送る。
【００８３】
第１の検索手段２１は同じソースＩＰアドレスがメール流量記憶部４１に記憶されていなかった場合（図９ステップＳ６３）、ソースＩＰアドレスとカウンタの初期値とからなるエントリをメール流量記憶部４１に記録する（図９ステップＳ６６）。
【００８４】
メール流量記憶部４１ではソースＩＰアドレスとカウンタ値との組み合わせからなるエントリが登録されており、一定時間が経過する毎に全エントリのカウンタ値が規定値だけ減少し、カウンタ値が「０」以下になると、そのエントリが削除される。
【００８５】
第２の検索手段２２は第１の検索手段２１から受け取った電子メールの本文にＳＰＡＭ

判定ワードが含まれていないかどうかを検索する（図９ステップＳ６７）。第２の検索手段２２は検索するＳＰＡＭ判定ワードをＳＰＡＭ判定ワード記憶部４１から取得する。

【００８６】

電子メールの本文にＳＰＡＭ判定ワードが含まれていない場合（図９ステップＳ６８）、第２の検索手段２２はメール情報をメール転送装置５に送る。ＳＰＡＭ判定ワードが含まれていた場合（図９ステップＳ６８）、第２の検索手段２２はメール情報をＳＰＡＭメール処理装置３に送る。

【００８７】

ＳＰＡＭメール処理装置３に送られたメール情報は、最初に新規ＵＲＬ登録手段３１で処理される。新規ＵＲＬ登録手段３１は電子メールの本文中から“ｈｔｔｐ”で始まるＵＲＬを文字列として取り出す（図９ステップＳ６９）。

【００８８】

ＵＲＬの取得に成功した場合（図９ステップＳ７０）、新規ＵＲＬ登録手段３１は取得したＵＲＬを登録候補リスト７１に記憶し、迷惑メール処理手段３２に処理を移す（図９ステップＳ７１，Ｓ７２）。

【００８９】

ＵＲＬの取得に失敗した場合（図９ステップＳ７０）、新規ＵＲＬ登録手段３１はＵＲＬの登録処理なしとし、処理を迷惑メール処理手段３２に移す。迷惑メール処理手段３２は新規ＵＲＬ登録手段３１から受け取った電子メールに対して予め規定したアクションを実行する（図９ステップＳ７３）。

【００９０】

規定したアクションの例としては、通過や廃棄、そして遅延がある。通過の場合には、メール情報をそのままメール転送装置５に転送する。廃棄の場合には、メール情報を迷惑メール処理手段３２で止め、全て解放する。遅延の場合には、迷惑メール処理手段３２で遅延されてメール転送装置５に送られる。

【００９１】

メール転送装置５は迷惑メール処理手段３２もしくは第２の検索手段２２から送られてきたメール情報をＩＰパケットの形式に変換し、電子メールの送信先へと転送する（図９ステップＳ７４）。

【００９２】

次に、オペレータが登録候補リスト７１に登録されたＵＲＬの中からＵＲＬを選択してＳＰＡＭ判定ワード記憶部４２やＵＲＬブラックリスト４３に登録する処理について説明する。

【００９３】

この場合、オペレータ制御部８はオペレータから指示があると、メールフィルタリング装置にログインし（図１０ステップＳ８１）、登録候補リスト７１に登録されたＵＲＬをダウンロードして表示する（図１０ステップＳ８２）。

【００９４】

オペレータ制御部８はオペレータが表示されたＵＲＬの中から登録ＵＲＬを選択すると（図１０ステップＳ８３）、その登録ＵＲＬをＳＰＡＭ判定ワード記憶部４２及びＵＲＬブラックリスト４３に追加登録し（図１０ステップＳ８４）、メールフィルタリング装置からログアウトする（図１０ステップＳ８５）。

【００９５】

このように、本実施例では、オペレータがオペレータ制御部８から登録候補リスト７１に記憶されているＵＲＬのリストを参照し、登録の許可・不許可を決定し、登録を許可されたＵＲＬのみＳＰＡＭ判定ワード記憶部４２及びＵＲＬブラックリスト４３に記憶させることで、本来、ＵＲＬブラックリスト４３に載せるべきではないＵＲＬを事前に排除することができる。

【００９６】

図１１は本発明のさらに別の実施例によるメールフィルタリング装置の構成を示すブロ

ック図である。図１１において、本発明のさらに別の実施例によるメールフィルタリング装置は携帯電話やメール端末等へ送信された電子メールのＩＰパケットから電子メールの本文を取り出すメール受信装置１と、電子メールの流量をチェックするとともに迷惑（ＳＰＡＭ）メールと判定される用語が含まれていないかを検索し、迷惑メールと判定された電子メールの本文からＵＲＬを抽出して廃棄・遅延等のアクションを起こすＳＰＡＭ処理装置９と、情報を記憶する記憶装置１０と、ブラックリスト構築装置１１と、電子メールの本文をＩＰパケットに収容して装置外に転送するメール転送装置５とから構成されている。

【００９７】

本実施例は、迷惑メールの判定後に行っていた電子メールの本文からのＵＲＬ取得をメール受信の次に行わせることにした点で、上述した本発明の一実施例によるメールフィルタリング装置と異なっている。

【００９８】

また、本実施例では、装置構成を、図１に示すＳＰＡＭ判定装置２及びＳＰＡＭ処理装置３をＳＰＡＭ処理装置９に統合し、図１の記憶装置４のＵＲＬブラックリスト４３をブラックリスト構築装置１１のＵＲＬブラックリスト記憶部１１２に分割させた点で、上述した本発明の一実施例によるメールフィルタリング装置と異なっている。

【００９９】

ＳＰＡＭ処理装置９はＵＲＬ取得手段９１と、第１の検索手段９２と、第２の検索手段９３と、迷惑メール処理手段９４とを備えている。ＵＲＬ取得手段９１はメール受信装置１から受け取った電子メールの本文の文面から“ｈｔｔｐ”で始まる文字列をＵＲＬとして取得する。第１の検索手段２２は取得されたＵＲＬをキーとして、メール流量記憶部１０１に記憶されたＵＲＬを検索する。

【０１００】

記憶装置１０のメール流量記憶部１０１は、図１のメール流量記憶部４１がソースＩＰアドレスとカウント値との組み合わせがエントリとして記憶しているのに対し、ＵＲＬの文字列とカウント値との組み合わせをエントリとして記憶している点で、上述した本発明の一実施例によるメールフィルタリング装置と異なっている。カウント値は一定時間経過すると規定値だけ減少し、カウント値が「０」以下になると対応したエントリが削除される。

【０１０１】

ブラックリスト構築装置１１はブラックリスト抽出手段１１１と、ＵＲＬブラックリスト記憶部１１２とを備えている。ブラックリスト抽出手段１１１はメール流量記憶部１０１に記憶されたＵＲＬとカウンタ値とからなるエントリから、カウンタ値がしきい値を超えているものを取り出し、ＵＲＬブラックリスト記憶部１１２に保存する。

【０１０２】

図１２は本発明のさらに別の実施例によるメールフィルタリング装置の動作を示すフローチャートである。これら図１１及び図１２を参照して本発明のさらに別の実施例によるメールフィルタリング装置の動作について説明する。

【０１０３】

メール受信装置１はパケット情報及び電子メールの本文を取り出し、ＳＰＡＭ処理装置９に転送する（図１２ステップＳ４１）。ＳＰＡＭ処理装置９は、まず最初にＵＲＬ取得手段９１によって電子メールの本文に含まれる“ｈｔｔｐ”から始まる文字列をＵＲＬとして取得する（図１２ステップＳ４２）。

【０１０４】

ＵＲＬ取得手段９１は電子メールの本文中にＵＲＬが含まれていなかった場合（図１２ステップＳ４３）、その電子メールを第２の検索手段９３に渡し、第２の検索手段９３の処理を行う（図１２ステップＳ４９）。

【０１０５】

また、ＵＲＬ取得手段９１はメール本文中にＵＲＬに含まれていた場合（図１２ステッ

プＳ４３）、その電子メールを第１の検索手段９２に渡す。第１の検索手段９２は取得ＵＲＬをキーとしたエントリがメール流量記憶部１０１に含まれていないかどうかの検索を行う（図１２ステップＳ４４）。

【０１０６】

第１の検索手段９２はメール流量記憶部１０１に抽出したＵＲＬをキーとするエントリが記憶されていた場合（図１２ステップＳ４５）、それに対応するカウンタ値を取り出して規定値だけ増加させる（図１２ステップＳ４６）。

【０１０７】

第１の検索手段９２はメール流量記憶部１０１に抽出したＵＲＬをキーとするエントリが記憶されていなかった場合（図１２ステップＳ４５）、取得したＵＲＬとカウンタの初期値とからなるエントリをメール流量記憶部１０１に新規エントリとして保存する（図１２ステップＳ４８）。

【０１０８】

第１の検索手段９２は規定値だけ増加させたカウンタ値がしきい値を超えていた場合（図１０ステップＳ４７）、その電子メールを迷惑メールとみなして迷惑メール処理手段９４に渡すので、迷惑メール処理手段９４はＳＰＡＭ判定ワード記憶部１０２のエントリ追加処理を行う（図１２ステップＳ５１）。

【０１０９】

第１の検索手段９２は規定値だけ増加させたカウンタ値がしきい値を超えていなければ、その電子メールを第２の検索手段９３に渡す。第２の検索手段９３はコンテンツのチェックを行い（図１２ステップＳ４９）、ＳＰＡＭ判定ワードが見つかれば（図１２ステップＳ５０）、その電子メールを迷惑メールとみなして迷惑メール処理手段９４に渡すので、迷惑メール処理手段９４はＳＰＡＭ判定ワード記憶部１０２のエントリ追加処理を行う（図１２ステップＳ５１）。

【０１１０】

この後、迷惑メール処理手段９４はＳＰＡＭ判定ワード記憶部１０２のエントリ追加処理を行った電子メールに対して迷惑メール処理を行い（図１２ステップＳ５２）、その電子メールをメール転送装置５に渡す。メール転送装置５は迷惑メール処理手段９４もしくは第２の検索手段９３から送られてきたメール情報をＩＰパケットの形式に変換し、電子メールの送信先へと転送する（図１２ステップＳ５３）。

【０１１１】

ブラックリスト抽出手段１１１はメール流量記憶部１０１に保存されているＵＲＬリストからカウンタ値が閾値を超えているもののみを取り出し、ＵＲＬブラックリスト記憶部１１２に保存する。

【０１１２】

本発明の一実施例では、電子メールの本文に含まれたＵＲＬを抽出してしきい値をとるので、同一サイトから大量に送られた迷惑メールを検出することができるが、複数のサイトから同一業者の広告メールが同時に送られた場合で、かつ各サイトから送られるメールの流量が閾値を下回る場合には迷惑メールとして検出されない。本実施例を用いると、それらのメールも迷惑メールとして検出することができるという新たな効果を奏する。

【図面の簡単な説明】

【０１１３】

【図１】本発明の一実施例によるメールフィルタリング装置の構成を示すブロック図である。

【図２】本発明の一実施例によるメールフィルタリング装置の動作を示すフローチャートである。

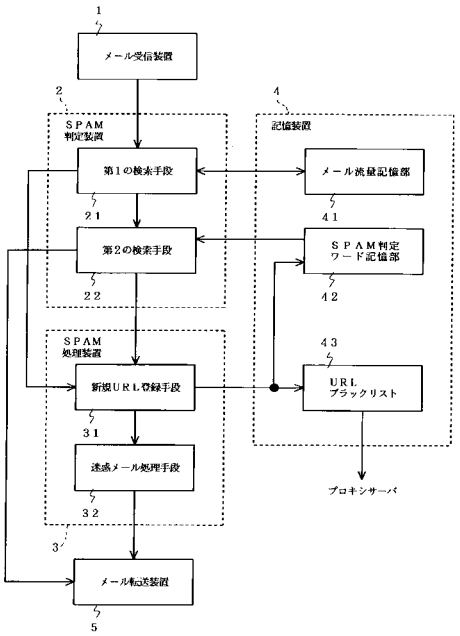
【図３】本発明の一実施例によるメールフィルタリング装置の動作を示すフローチャートである。

【図４】本発明の一実施例においてＳＰＡＭ判定ワード記憶部に登録して迷惑メールのチェックを行う理由を示す図である。

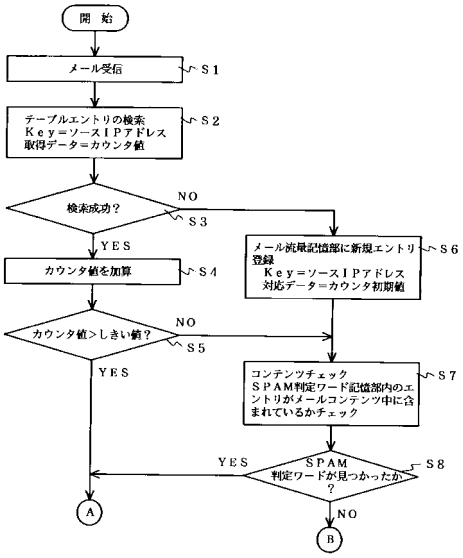
【図５】本発明の他の実施例によるメールフィルタリング装置の構成を示すブロック図である。
【図６】本発明の他の実施例によるメールフィルタリング装置の動作を示すフローチャートである。
【図７】本発明の他の実施例によるメールフィルタリング装置の動作を示すフローチャートである。
【図８】本発明の別の実施例によるメールフィルタリング装置の構成を示すブロック図である。
【図９】本発明の別の実施例によるメールフィルタリング装置の動作を示すフローチャートである。
【図１０】本発明の別の実施例によるオペレータ制御部における登録候補リスト選択処理を示すフローチャートである。
【図１１】本発明のさらに別の実施例によるメールフィルタリング装置の構成を示すブロック図である。
【図１２】本発明のさらに別の実施例によるメールフィルタリング装置の動作を示すフローチャートである。
【符号の説明】
【０１１４】

１	メール受信装置
２	ＳＰＡＭ判定装置
３，９	ＳＰＡＭ処理装置
４，６，７，１０	記憶装置
５	メール転送装置
８	オペレータ制御部
１１	ブラックリスト構築装置
２１，９２	第１の検索手段
２２，９３	第２の検索手段
３１	新規ＵＲＬ登録手段
３２，９４	迷惑メール処理手段
４１，１０１	メール流量記憶部
４２，１０２	ＳＰＡＭ判定ワード記憶部
４３	ＵＲＬブラックリスト
６１	ＵＲＬホワイトリスト
７１	登録候補リスト
９１	ＵＲＬ取得手段
１１１	ブラックリスト抽出手段
１１２	ＵＲＬブラックリスト記憶部

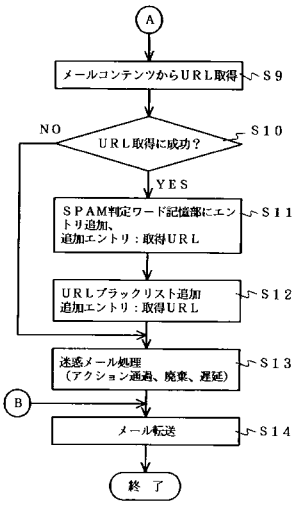
【図１】


1
メール受信装置
2
SPAM
判定装置
第１の検索手段
21
第２の検索手段
22
SPAM
処理装置
新規ＵＲＬ登録手段
31
迷惑メール処理手段
32
3
メール転送装置
5
4
記憶装置
メール流量記憶部
41
ＳＰＡＭ判定
ワード記憶部
42
43
ＵＲＬ
ブラックリスト
プロキシサーバ

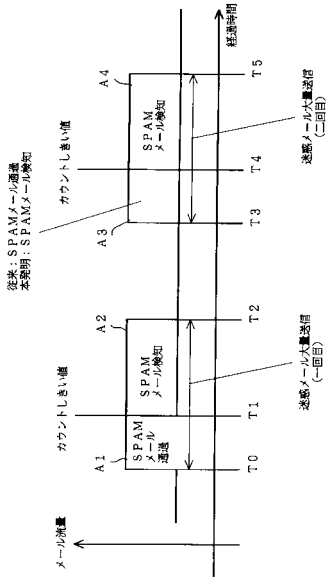
【図２】


開 始
メール受信
S1
テーブルエントリの検索
Ｋｅｙ＝ソースＩＰアドレス
取得データ＝カウンタ値
S2
検索成功？
NO
S3
YES
カウンタ値を加算
S4
メール流量記憶部に新規エントリ登録
Ｋｅｙ＝ソースＩＰアドレス
対応データ＝カウンタ初期値
S6
カウンタ値＞しきい値？
NO
S5
YES
コンテンツチェック
ＳＰＡＭ判定ワード記憶部内のエントリがメールコンテンツ中に含まれているかチェック
S7
YES
SPAM
判定ワードが見つかったか？
S8
NO
A
B

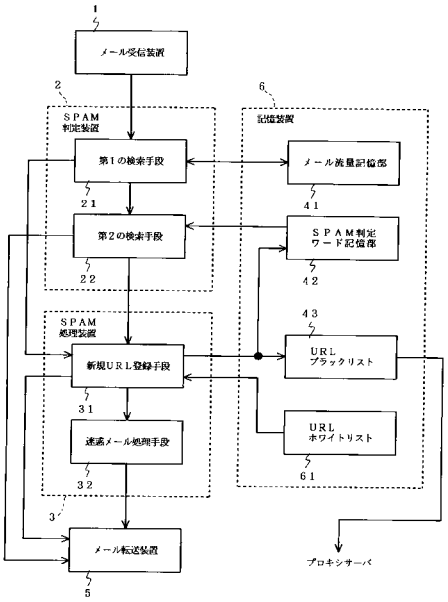
【図３】


A
メールコンテンツからＵＲＬ取得
S9
NO
ＵＲＬ取得に成功？
S10
YES
ＳＰＡＭ判定ワード記憶部にエントリ追加、
追加エントリ：取得ＵＲＬ
S11
ＵＲＬブラックリスト追加
追加エントリ：取得ＵＲＬ
S12
迷惑メール処理
（アクション通過、廃棄、遅延）
S13
B
メール転送
S14
終 了

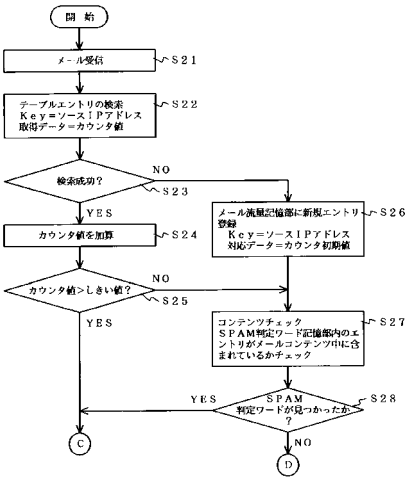
【図４】


経過時間
T5
T4
T3
T2
T1
T0
A4
A3
A2
A1
SPAM
メール検知
SPAM
メール
通過
カウントしきい値
従来：SPAMメール通過
本発明：SPAMメール検知
迷惑メール大量送信
（二回目）
迷惑メール大量送信
（一回目）
メール流量

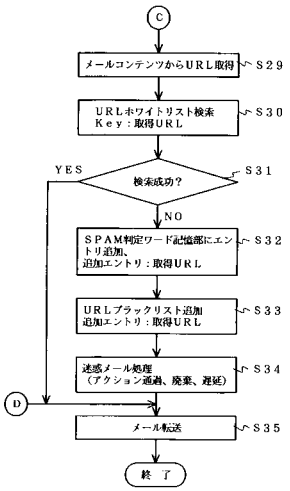
【図５】


1
メール受信装置
2
SPAM
判定装置
第１の検索手段
21
第２の検索手段
22
SPAM
処理装置
新規URL登録手段
31
迷惑メール処理手段
32
3
メール転送装置
5
6
記憶装置
メール流量記憶部
41
SPAM判定
ワード記憶部
42
43
URL
ブラックリスト
URL
ホワイトリスト
61
プロキシサーバ

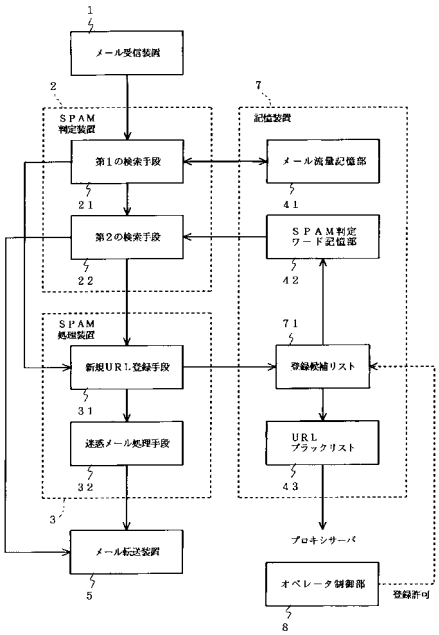
【図６】


開 始
メール受信
S21
テーブルエントリの検索
Ｋｅｙ＝ソースＩＰアドレス
取得データ＝カウンタ値
S22
検索成功？
NO
S23
YES
カウンタ値を加算
S24
メール流量記憶部に新規エントリ登録
Ｋｅｙ＝ソースＩＰアドレス
対応データ＝カウンタ初期値
S26
カウンタ値>しきい値？
NO
S25
YES
コンテンツチェック
ＳＰＡＭ判定ワード記憶部内のエントリがメールコンテンツ中に含まれているかチェック
S27
YES
SPAM
判定ワードが見つかったか？
S28
NO
C
D

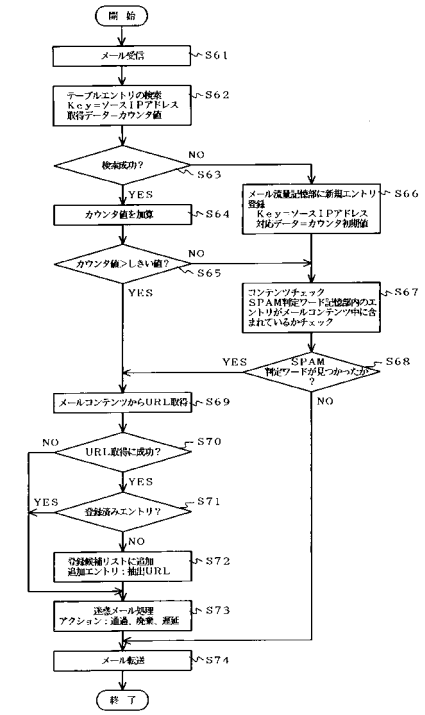
【図７】


C
メールコンテンツからURL取得
S29
URLホワイトリスト検索
Ｋｅｙ：取得URL
S30
YES
検索成功？
S31
NO
ＳＰＡＭ判定ワード記憶部にエントリ追加、
追加エントリ：取得URL
S32
URLブラックリスト追加
追加エントリ：取得URL
S33
迷惑メール処理
（アクション通過、廃棄、遅延）
S34
D
メール転送
S35
終 了

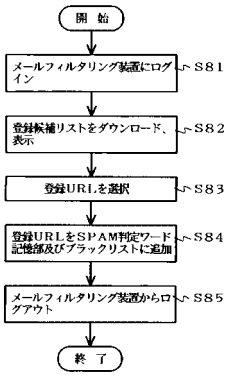
【図８】


1
メール受信装置
2
SPAM
判定装置
第１の検索手段
21
第２の検索手段
22
SPAM
処理装置
新規URL登録手段
31
迷惑メール処理手段
32
3
メール転送装置
5
7
記憶装置
メール流量記憶部
41
ＳＰＡＭ判定
ワード記憶部
42
71
登録候補リスト
URL
ブラックリスト
43
プロキシサーバ
オペレータ制御部
8
登録許可

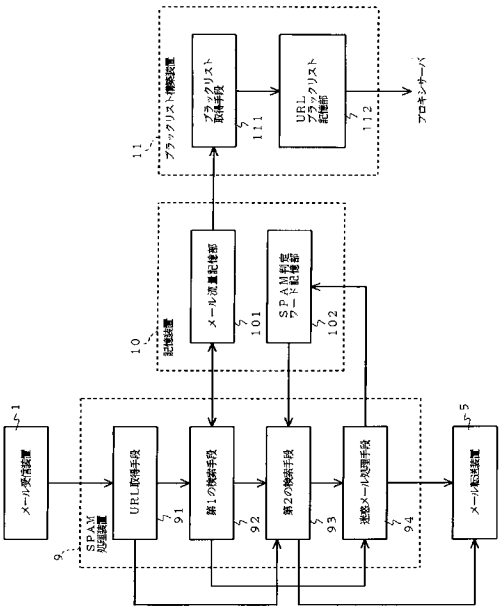
【図９】



【図１０】



【図１１】



【図１２】