

WO 2014/185394 A1



NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI 添付公開書類:

(BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, — 国際調査報告 (条約第 21 条(3))
MR, NE, SN, TD, TG).

明 細 書

発明の名称： 中継装置および中継装置の制御方法

技術分野

[0001] この発明は、webアクセスに起因するウィルス感染や詐欺被害を防止する技術に関する。

背景技術

[0002] webサイトを利用した情報収集や商取引の普及に伴い、webアクセスに起因するウィルス感染や詐欺被害などのトラブルが急増している。この種のトラブルの一例としては、会員制webサイトや大企業のwebサイトに成りすましたwebサイト（すなわち、偽のwebサイト）にアクセスした際にウィルスを送り込まれ感染させられることや、クレジットカード番号などの個人情報の入力を促され本物と勘違いして個人情報を入力したところ、その個人情報を不正利用されること（所謂フィッシング詐欺）が挙げられる。そこで、これらトラブルの発生を未然に防ぐための技術が提案されている（例えば、特許文献1に開示の技術等）。

[0003] 特許文献1には、迷惑メールのコンテンツチェックに引っかかった電子メール、或いは送信元IPアドレス毎に集計した流量が所定の閾値を超えていた電子メールを対象としてメール本文にURLを表す文字列を含んでいるかを判定し、含んでいる場合には当該文字列をデータベースに登録し、以降、当該文字列を本文に含む電子メールを破棄する技術が開示されている。一般に、悪意を持ってwebサイトを開設した者は当該webサイトへ被害者を誘い込むために、当該webサイトのURLをメール本文に書き込んだ電子メールを多量に配布するなどの宣伝を行うことが多い。特許文献1に開示の技術はこのような宣伝目的の電子メールの拡散を食い止めることで、ウィルス感染や詐欺被害の発生を食い止めようとするものである。

先行技術文献

特許文献

[0004] 特許文献1：日本国特開2005-208780号公報

特許文献2：日本国特開2010-187340号公報

発明の概要

発明が解決しようとする課題

[0005] しかし、特許文献1に開示の技術では、データベースへのURL登録の契機となった電子メールはその宛先へ配信されてしまう。このため、特許文献1に開示の技術には、当該電子メールに起因してwebアクセスが行われた場合にウィルス感染や詐欺被害を防げないといった問題がある。加えて、特許文献1に開示の技術では、流量が所定の閾値を超えるまでデータベースへのURL登録が行われないため、迅速に対処することができず、データベースへのURL登録が行われた時点では既に被害が拡大している虞がある。

[0006] 本発明は上記課題に鑑みて為されたものであり、悪意を持って開設されたwebサイトへのアクセスを迅速に食い止め、ウィルス感染や詐欺被害の拡大を未然に防ぐことを可能にする技術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

[0007] 上記課題を解決するために本発明の一態様は、ローカルエリアネットワークを広域網に接続する中継装置において、前記ローカルエリアネットワークが前記広域網から受信した電子メールに前記広域網を介して利用可能な資源を一意に示す識別子が含まれているか否かを判定し、含まれている場合に当該識別子をデータベースに登録する識別子チェック手段と、前記広域網を介して利用可能な資源への前記ローカルエリアネットワーク内の端末装置からのアクセスを検知したことを契機として前記データベースに当該資源を示す識別子が登録されているか否かを判定し、登録されていた場合にはアクセスの可否を問い合わせる画面を前記端末装置に表示させ、アクセスを許可する返答が得られた場合に当該アクセスを中継するリダイレクト手段と、を有することを特徴とする中継装置、を提供する。

[0008] 上記広域網の一例としてはインターネットが挙げられ、上記資源の一例としてはインターネットに接続されたwebサーバ装置（webサイトを運営

するためのサーバ装置）やF T Pサーバ装置（F T Pによるデータ配信を行うサーバ装置）、これらサーバ装置に記憶されている各種データ、これらサーバ装置で実行されるプログラムが挙げられる。そして、上記識別子の一例としては、w e bサイトのU R LやU R Iが挙げられる。例えば、上記識別子としてU R Lを用いる場合には上記識別子チェック手段は、受信した電子メールにU R Lが含まれているか否かを判定するU R Lチェック手段となる。この場合、本発明の中継装置によれば、ローカルエリアネットワークが広域網から受信した電子メールであって、本文にU R Lの記載された電子メールの中継を契機として即座に上記データベースへの当該U R Lの登録が行われる。そして、ローカルエリアネットワーク内の端末装置から広域網に接続されるw e bサーバ装置等へのアクセスを検知した場合には、そのw e bアクセス先のU R Lが上記データベースに登録されているか否かを判定し、登録されていた場合には、w e bアクセスの継続の可否を問い合わせる注意喚起画面を端末装置に表示させ、アクセスを許可する旨の返答が得られた場合にw e bアクセスの中継が行われる。このため、本発明の中継装置によれば、メール流量が所定の閾値を超えるまでデータベースへのU R L登録が行われないことに起因する不具合（すなわち、被害の拡大）を回避することができる。なお、本発明の別の態様としてはコンピュータを上記各手段として機能させるプログラムを提供する態様が考えられる。

[0009] 上記中継装置は、前記ローカルエリアネットワークが前記広域網から受信した電子メールをその送信元メールアドレスに基づいてフィルタリングする第1のフィルタリング処理と前記ローカルエリアネットワークから前記広域網へ送信された電子メールをその送信先メールアドレスに基づいてフィルタリングする第2のフィルタリング処理のうち、少なくとも前者を実行するフィルタリング手段と、前記フィルタリング手段によってフィルタリングされた電子メールの送信元メールアドレスまたは送信先メールアドレスとその送信先または送信元の端末装置を示す端末識別子を記憶するメールアドレスデータベースと、を備え、前記リダイレクト手段には、前記広域網を介して利

用可能な資源へのアクセスを行った端末装置を送信先または送信元とする電子メールのうち前記フィルタリング手段によりフィルタリングされたものがあるか否かを前記メールアドレスデータベースの格納内容を参照して判定し、前記第1のフィルタリング処理によりフィルタリングされた電子メールについてはその送信元メールアドレスのフィルタリングの解除の可否を問い合わせる画面を当該端末装置に表示させる一方、前記第2のフィルタリング処理によりフィルタリングされた電子メールについてはその送信先メールアドレスのフィルタリングの解除の可否を問い合わせる画面を当該端末装置に表示させ、各画面に対する操作に応じて前記フィルタリング手段におけるフィルタリング条件を更新する処理を実行させることとしてもよい。

[0010] このような態様によれば、webアクセスの受信を契機として、フィルタリングされた電子メールがあったことをそのwebアクセスの送信元へ通知し、フィルタリング条件の更新を促すことができる。なお、本態様の中継装置におけるフィルタリング処理の実行態様としては、第1のフィルタリング処理のみを実行する態様と第1および第2のフィルタリング処理の両者を実行する態様の2つの態様が考えられる。つまり、本態様の中継装置では第1のフィルタリング処理は必ず実行されるのである。ここで、第1および第2のフィルタリング処理のうち前者を必ず実行するようにしたのは、宣伝目的の電子メールなどが無条件にユーザに送り届けられないようにするためである。

[0011] 上記中継装置は、第1のフィルタリング処理によりフィルタリングされた電子メールを記憶するメール保持手段と、メール保持手段に記憶されている電子メールを当該中継装置を送信元とする電子メールとして送信するメール生成／送信手段と、を備え、リダイレクト手段には、前記第1のフィルタリング処理のフィルタリング条件の更新に応じて、フィルタリング対象から除外された送信元メールアドレスから前記端末装置へ宛てて送信された電子メールを前記メール生成／送信手段に送信させることとしてもよい。このような態様によれば、第1のフィルタリング処理によりフィルタリングした電子

メールを保存しておき、フィルタリング条件の更新の際にフィルタリング対象から除外された送信元メールアドレスから送信された電子メールをその送信先へ再送信することが可能になる。

[0012] 上記中継装置は、フィルタリング手段によりフィルタリングされなかった電子メールが迷惑メールであるか否かをチェックするメールチェック手段を備え、識別子チェック手段は、メールチェック手段によるチェックを通過し電子メールをチェック対象とすることとしてもよい。なお、迷惑メールの具体例としては、コンピュータウイルスの添付された電子メールや所謂スパムメールが挙げられる。このような態様によれば、送信元メールアドレスの偽装等によりフィルタリングされなかった迷惑メールがローカルエリア内の端末装置へ無条件に転送されることを回避することができる。

[0013] 上記中継装置は、ローカルエリアネットワーク内の端末装置のメールアドレス帳データを解析して電子メールアドレスを抽出するアドレス帳解析手段と、アドレス帳解析手段により抽出された電子メールアドレスに基づいてフィルタリング条件を表すメールフィルタデータを生成し、前記フィルタリング手段に与えるメールフィルタデータ生成手段とを有することとしてもよい。このような態様によれば、フィルタリング条件を表すメールフィルタデータをユーザのアドレス帳データから自動生成することができ、メールフィルタデータを人手で作成する場合に比較してその作成に要する手間を省くことができる。

[0014] 本発明の別の態様は、ローカルエリアネットワークを広域網に接続する中継装置の制御方法において、前記ローカルエリアネットワークが前記広域網から受信した電子メールに前記広域網を介して利用可能な資源を一意に示す識別子が含まれているか否かを判定し、含まれている場合に当該識別子をデータベースに登録し、前記広域網を介して利用可能な資源への前記ローカルエリアネットワーク内の端末装置からのアクセスを検知したことを契機として前記データベースに当該資源を示す識別子が登録されているか否かを判定し、登録されていた場合にはアクセスの可否を問い合わせる画面を前記端末

装置に表示させ、アクセスを許可する返答が得られた場合に当該アクセスを中継することを特徴とする制御方法を提供する。

[0015] 特許文献2には、各ユーザの使用している端末のメーラのアドレス帳をサーバに登録し、メールを送信するユーザのアドレス帳とメールを受信するユーザのアドレス帳に他方のメールアドレスが互いに登録されている場合に当該メールの送信を許可することで送信元や宛先が不確かなメールの伝送を防止する技術の開示がある。特許文献2に開示の技術には、相手方のアドレス帳に自分のメールアドレスが登録されていない場合には当該相手方を宛先として電子メールを送信することができないといった制約や、メールを送受信するユーザが同じシステムを使用していなければならないといった制約があり、実状にそぐわないといった問題がある。これに対して上記態様の中継装置では、ローカルエリアネットワーク内の端末装置のメールアドレス帳データのみからメールフィルタデータが生成されるため、上記のような不具合は生じない。つまり、本願発明は特許文献2に開示のものとは異なる技術である。

図面の簡単な説明

[0016] [図1]この発明の一実施形態の中継装置10を含む通信システムの構成例を示す図である。

[図2]同中継装置10の構成例を示すブロック図である。

[図3]同中継装置10に入力されるアドレス帳データの一例を示す図である。

[図4]同中継装置10の制御部110が中継制御プログラム154aにしたがって実現する機能ブロックの一例を示す図である。

[図5]同中継装置10の不揮発性記憶部154に格納されているメールフィルタデータ154b1および154b2の一例を示す図である。

[図6]拠点内LAN20が広域網30側から受信した電子メールの中継制御の流れを示すフローチャートである。

[図7]同中継装置10の不揮発性記憶部154に格納されているメールアドレスデータベース154c1の格納内容の一例を示す図である。

[図8]同中継装置 10 の不揮発性記憶部 154 に格納されている URL データベース 154 d の格納内容の一例を示す図である。

[図9]拠点内 LAN 20 側から広域網 30 側へ送信された電子メールの中継制御の流れを示すフローチャートである。

[図10]拠点内 LAN 20 側から広域網 30 側への web アクセスの中継制御の流れを示すフローチャートである。

[図11]端末装置の表示部に表示されるリダイレクト画面の一例を示す図である。

[図12]端末装置の表示部に表示されるリダイレクト画面の一例を示す図である。

[図13]端末装置の表示部に表示されるリダイレクト画面の一例を示す図である。

発明を実施するための形態

[0017] 以下、本発明の実施形態について説明する。

(A : 構成)

図 1 は、本発明の一実施形態の中継装置 10 を含む通信システムの構成例を示す図である。本実施形態の中継装置 10 は例えばルータである。図 1 に示すように、中継装置 10 は、企業の本社や支社等の各拠点に敷設されたローカルエリアネットワークである拠点内 LAN (Local Area Network) 20 を不特定多数の者に共用される広域網 30 (例えばインターネット) に接続する。図 1 に示すように、拠点内 LAN 20 は、上記拠点にて就労する従業員の使用する端末装置 PC 1 および PC 2 を含んでおり、ネットワーク管理者等によって運用管理されている。

[0018] 端末装置 PC 1 および PC 2 は LAN ケーブルなどの信号線を介して拠点内 LAN 20 に接続されたパーソナルコンピュータである。端末装置 PC 1 や端末装置 PC 2 には、web ブラウザやメールなどの各種アプリケーションソフトウェアが予めインストールされている。なお、図 1 では、拠点内 LAN 20 に 2 台の端末装置が含まれている場合について例示されているが、

3台以上の端末装置が含まれていても良く、また、端末装置が1台だけ含まれていても良い。また、拠点内LAN20に含まれる端末装置は当該拠点内LAN20に有線接続されるものには限定されず、拠点内LAN20に収容される無線端末装置であっても良い。

[0019] 中継装置10は、拠点内LAN20に含まれるコンピュータ装置（本実施形態では端末装置PC1或いは端末装置PC2）と、広域網30を介して利用可能な資源（例えば、広域網30に接続されたwebサーバ装置）との間でHTTPなどの所定の通信プロトコルにしたがって行われるデータ通信を仲介する。本実施形態では、本発明の特徴を顕著に示す中継制御処理を中継装置10に実行させることにより、広域網30を介して利用可能な資源に端末装置PC1やPC2を用いてアクセスする際のウィルス感染や詐欺被害を未然に防ぐことが可能となっている。以下、中継装置10を中心に説明する。

[0020] 図2は、中継装置10の構成例を示す図である。図2に示すように中継装置10は、制御部110、第1通信I/F部120、第2通信I/F部130、外部機器I/F部140、記憶部150、およびこれら構成要素間のデータ授受を仲介するバス160を含んでいる。

[0021] 制御部110はCPU（Central Processing Unit）である。制御部110は記憶部150（より正確には不揮発性記憶部154）に記憶されている中継制御プログラム154aを実行することにより中継装置10の制御中枢として機能する。

[0022] 第1通信I/F部120と第2通信I/F部130は夫々NIC（Network Interface Card）であり、各々異なる通信網に接続されている。より詳細に説明すると第1通信I/F部120は拠点内LAN20に接続されており、第2通信I/F部130は広域網30に接続されている。第1通信I/F部120および第2通信I/F部130の各々は、接続先の通信網から受信したデータを制御部110に引き渡す一方、制御部110から引き渡されたデータを接続先の通信網へと送出する。

[0023] 外部機器 1 / F 部 1 4 0 は、U S B (Universal Serial Bus) インタフェースやシリアルインタフェースなどの集合体である。中継装置 1 0 に接続される外部機器は上記各種インタフェースのうちの好適なものを介して中継装置 1 0 に接続される。例えば、接続対象の外部機器が U S B メモリであれば U S B インタフェースに接続され、接続対象の外部機器がシリアルコンソールである場合にはシリアルインタフェースに接続されるといった具合である。本実施形態では外部機器 1 / F 部 1 4 0 は、拠点内 L A N 2 0 に含まれるコンピュータ装置を使用して電子メールの送受信を行うユーザのアドレス帳データを中継装置 1 0 に入力するための入力手段の役割を果たす。

[0024] アドレス帳データとは、アドレス帳データの所有者の友人や知人、仕事相手など電子メールの送受信先となる相手方の氏名や電子メールにおける表示名、電子メールアドレスなどの各種情報を表すデータの集合体である。このようなアドレス帳データの一例としては、図 3 (a) および図 3 (b) に示すように、上記各種情報を表す文字列をコンマ (,) で区切って配列した C S V 形式のデータが挙げられる。図 3 (a) および図 3 (b) は互いに異なる種類のメーラのアドレス帳データの一例を示す図である。図 3 (a) や図 3 (b) に示すように、アドレス帳データにどのようなデータが含まれているかについてはメーラの種類毎に異なることが一般的であるが、少なくとも相手方の電子メールアドレスを表す文字列が含まれていることに変わりはない。なお、本実施形態では、所定の区切り文字 “@” を途中に含む半角英数字よりなる文字列を電子メールアドレスと見做す。

[0025] 記憶部 1 5 0 は、図 2 に示すように、揮発性記憶部 1 5 2 と不揮発性記憶部 1 5 4 を含んでいる。揮発性記憶部 1 5 2 は例えば R A M (Random Access Memory) である。揮発性記憶部 1 5 2 は中継制御プログラム 1 5 4 a を実行する際のワークエリアとして制御部 1 1 0 によって使用される。不揮発性記憶部 1 5 4 は例えばハードディスクやフラッシュメモリである。不揮発性記憶部 1 5 4 には本実施形態の特徴を顕著に示す中継制御処理を制御部 1 1 0 に実行させるための中継制御プログラム 1 5 4 a と、受信した電子メールが

迷惑メールであるか否かを評価する評価プログラム（ウィルスチェックプログラムなど、図2では図示略）が格納されている。また、不揮発性記憶部154には、中継制御プログラム154aの実行過程で参照および更新される各種データも格納されている。不揮発性記憶部154に格納されているデータの一例としてはメールフィルタデータ154b1および154b2、メールアドレスデータベース154c1および154c2、URLデータベース154dが挙げられる。これら各種データの役割およびデータ構造については重複を避けるため動作例において明らかにする。

[0026] 制御部110は、中継装置10の電源（図2では図示略）投入またはリセットを契機として中継制御プログラム154aを不揮発性記憶部154から揮発性記憶部152に読み出し、その実行を開始する。制御部110は、中継制御プログラム154aを実行することにより、図4に示すアドレス帳解析手段1502、メールフィルタデータ生成手段1504、フィルタリング手段1506aおよび1506b、メールチェック手段1508、URLチェック手段1510、リダイレクト手段1512、およびメール生成／送信手段1514として機能する。また、不揮発性記憶部154はメール保持手段1516としても機能する。これら各手段の役割については重複を避けるため動作例において明らかにする。

以上が中継装置10の構成である。

[0027] (B：動作例)

次いで、中継装置10が実行する動作について説明する。

(B-1：メールフィルタデータ生成動作)

本実施形態では、外部機器I／F部140を介して与えられたアドレス帳データに基づいて、フィルタリング条件を表すメールフィルタデータ154b1および154b2が生成される。フィルタリングとは、拠点内LAN200或いは広域網30から受信した電子メールの転送を見合わせることをいい、フィルタリング条件とは転送を見合わせる電子メールが満たす条件のことをいう。メールフィルタデータ154b1は、拠点内LAN200が広域網3

0から受信した電子メールをその送信元メールアドレスに基づいてフィルタリングする際のフィルタリング条件を表すデータである。一方、メールフィルタデータ154b2は、拠点内LAN20から広域網30へ送信された電子メールをその送信先メールアドレスに基づいてフィルタリングする際のフィルタリング条件を表すデータである。

[0028] 図4のアドレス帳解析手段1502は、外部機器1/F部140を介して入力されたアドレス帳データを解析して電子メールアドレス（前述した所定の区切り文字を途中に含み、かつ半角英数字よりなる文字列）を抽出してメールフィルタデータ生成手段1504に与える。例えば、アドレス帳データとして図3（a）に示すものが外部機器1/F部140を介して入力された場合には、アドレス帳解析手段1502は当該アドレス帳データから電子メールアドレス“1234@example.jp”と“abcd@example.jp”を抽出してメールフィルタデータ生成手段1504に与える。メールフィルタデータ生成手段1504は、メールフィルタデータ154b1および154b2を、アドレス帳解析手段1502から与えられる電子メールアドレスに基づいて生成し、フィルタリング手段1506aおよび1506bの各々に与える。

[0029] 図5（a）は、メールフィルタデータ154b1の一例を示す図であり、図5（b）はメールフィルタデータ154b2の一例を示す図である。図5（a）および図5（b）に示すように、メールフィルタデータ154b1および154b2は、互いに対応付けられた1組の送信先アドレス、送信元アドレスおよびタイプ識別子により形成されるレコードの集合体である。図5（a）および図5（b）におけるタイプ識別子は当該タイプ識別子に対応付けられた送信元アドレスを送信元メールアドレスとし、同送信先アドレスを送信先メールアドレスとする電子メールの転送の可否（passならば転送許可、rejectならば転送拒否）を示す識別子である。また、図5（a）の送信先アドレス、或いは図5（b）の送信元アドレスにおける“*”は電子メールの転送の可否の判定の際に当該アドレスの値を問わないことを意味している。

[0030] メールフィルタデータ生成手段1504は、メールフィルタデータ154b1を、以下の3種類のレコードの集合体として生成する。第1に、送信先アドレスに“*”を、送信元アドレスにアドレス帳解析手段1502から与えられた電子メールアドレスを、タイプ識別子に“pass”を夫々設定したレコードである。第2に、送信先アドレスに“*”を、送信元アドレスに当該中継装置10の電子メールアドレス（本実施形態では、router@example.jp）を、タイプ識別子に“pass”を夫々設定したレコードである。そして、第3に、送信先アドレスに“*”を、送信元アドレスに“それ以外”（すなわち、アドレス帳解析手段1502から与えられた電子メールアドレスではなく、中継装置10の電子メールアドレスでもない電子メールアドレスを示す値）を、タイプ識別子に“reject”をそれぞれ設定したレコードである。なお、メールフィルタデータ154b1が既に生成済である場合には、メールフィルタデータ生成手段1504はアドレス帳解析手段1502から与えられる電子メールアドレスがメールフィルタデータ154b1に登録済であるか否かを電子メールアドレス毎に判定し、未登録の場合に当該電子メールアドレスを追加登録する（メールフィルタデータ154b2についても同様）。

[0031] また、メールフィルタデータ生成手段1504は、メールフィルタデータ154b1においてタイプ識別子に“pass”を設定した送信元アドレスをメールアドレスデータベース154c1に登録する。なお、図4では、図面が煩雑になることを避けるため、メールフィルタデータ生成手段1504によるメールアドレスデータベース154b1へのアクセスを示す矢印の図示を省略した。メールアドレスデータベース154c1は、図7に示すように、送信元アドレス、送信先アドレス、端末識別子、タイプ識別子、結果識別子および判定回数の各データを対応付けて格納するデータベースである。このメールアドレスデータベース154c1には、拠点内LAN20が広域網30から受信した電子メールに関する情報が格納される。例えば、送信元アドレスには上記電子メールの送信元メールアドレスが、送信先アドレスには上記電子メールの送信先メールアドレスが、上記端末識別子には上記電子メー

ルの送信先の端末装置の端末識別子が夫々セットされる。メールアドレスデータベース154c1への各データの登録は基本的にはフィルタリング手段1506aによって実行されるのであるが、メールフィルタデータ154b1においてタイプ識別子に“pass”を設定した送信元アドレスについてはメールフィルタデータ生成手段1504によって登録される。送信元アドレス、送信先アドレスおよび端末識別子に対応付けてメールアドレスデータベース154c1に登録されるタイプ識別子、結果識別子および判定回数の各データの意味については、フィルタリング手段1506aの説明において明らかにする。メールフィルタデータ154b1においてタイプ識別子に“pass”を設定した送信元アドレスをメールアドレスデータベース154c1に登録する際にメールフィルタデータ生成手段1504は、当該送信元アドレスをメールアドレスデータベース154c1の送信元アドレスにセットし、タイプ識別子および結果識別子に夫々“pass”をセットし、判定回数に0をセットする。なお、メールアドレスデータベース154c1において上記送信元アドレスに対応する送信先アドレスおよび端末識別子については、それらの値を問わないことを示す“*”をセットしても良く、上記アドレス帳データの所有者の電子メールアドレスおよび当該所有者の使用する端末装置の端末識別子を取得してセットしても良い。

- [0032] これに対して、メールフィルタデータ154b2は、以下の2種類のレコードの集合体として生成される。第1に、送信先アドレスにアドレス帳解析手段1502から与えられた電子メールアドレスを、送信元アドレスに“*”を、タイプ識別子に“pass”を設定したレコードである。第2に、送信先アドレスに“それ以外”を、送信元アドレスに“*”を、タイプ識別子に“reject”を設定したレコードである。また、メールフィルタデータ生成手段1504は、メールフィルタデータ154b2においてタイプ識別子に“pass”を設定した送信先アドレスをメールアドレスデータベース154c2に登録する。なお、図4では、図面が煩雑になることを避けるため、メールフィルタデータ生成手段1504によるメールアドレスデータベース154b2

へのアクセスを示す矢印の図示を省略した。メールアドレスデータベース 154c2 は、メールアドレスデータベース 154c1 と同一構造（図 7 参照）のデータベースである。このメールアドレスデータベース 154c2 には、拠点内 LAN20 から広域網 30 へ送信された電子メールに関する情報が格納される。例えば、送信元アドレスには上記電子メールの送信元メールアドレスが、送信先アドレスには上記電子メールの送信先メールアドレスが、上記端末識別子には上記電子メールの送信元の端末装置の端末識別子が夫々セットされる。メールアドレスデータベース 154c2 への各データの登録は基本的にはフィルタリング手段 1506b によって実行されるのであるが、メールフィルタデータ 154b2 においてタイプ識別子に “pass” を設定した送信先アドレスについてはメールフィルタデータ生成手段 1504 によって登録される。メールフィルタデータ 154b2 においてタイプ識別子に “pass” を設定した送信先アドレスをメールアドレスデータベース 154c2 に登録する際にはメールフィルタデータ生成手段 1504 は、当該送信先アドレスをメールアドレスデータベース 154c2 の送信先アドレスにセットし、タイプ識別子および結果識別子に夫々 “pass” をセットし、判定回数に 0 をセットする。なお、メールアドレスデータベース 154c2 において上記送信先アドレスに対応する送信元アドレスおよび端末識別子については、それらの値を問わないことを示す “*” をセットしても良く、上記アドレス帳データの所有者の電子メールアドレスおよび当該所有者の使用する端末装置の端末識別子を取得してセットしても良い。

[0033] 前述したように、メールフィルタデータ 154b1 は、拠点内 LAN20 が広域網 30 から受信した電子メールのフィルタリング条件を規定するデータであり、メールフィルタデータ 154b1 においては送信先アドレスには全て “*” が設定されているのであるから、拠点内 LAN20 が広域網 30 側から受信した電子メールのフィルタリングは当該電子メールの送信元メールアドレスに基づいて行われる。このため、本実施形態では、拠点内 LAN20 が広域網 30 から受信した電子メールのうち、上記ユーザのアドレス帳

に登録されている電子メールアドレスではなく、また、中継装置 10 の電子メールアドレスでもない電子メールアドレスを送信元メールアドレスとするものは中継装置 10 においてフィルタリングされる。これは、上記ユーザが、見知らぬ相手から送信された電子メールを無条件に受信しないようにするためである。同様に、当該ユーザから見知らぬ相手へと送信された電子メールもメールフィルタデータ 154 b 2 にしたがってフィルタリングされる。

[0034] このようなメールフィルタデータ生成動作が実行されるため、拠点内 LAN 20 の運用管理者は、拠点内 LAN 20 の各ユーザのアドレス帳データの記録された記憶装置を中継装置 10 の外部機器 I/F 部 140 に接続するだけで、メールフィルタデータ 154 b 1 および 154 b 2 を制御部 110 に生成させ、記憶させることができる。なお、本実施形態では、アドレス帳データに登録されている電子メールアドレスをメールフィルタデータ 154 b 1 と 154 b 2 の両方に登録する場合について説明したが、何れか一方のみ登録されるように、メールフィルタデータ生成手段 1504 の設定変更を行えるようにしても良い。

[0035] (B-2: 拠点内 LAN 20 が広域網 30 から受信した電子メールの中継動作)

次いで、拠点内 LAN 20 が広域網 30 から受信した電子メールの中継動作について説明する。図 6 は、拠点内 LAN 20 が広域網 30 から受信した電子メールの中継動作の流れを示すフローチャートである。拠点内 LAN 20 が広域網 30 から受信した電子メールは第 2 通信 I/F 部 130 を介して制御部 110 に与えられる。このように、第 2 通信 I/F 部 130 を介して制御部 110 に与えられた電子メールは、まず、フィルタリング手段 1506 a によるフィルタリング評価を受ける (ステップ SA100)。より詳細に説明すると、フィルタリング手段 1506 a は、第 2 通信 I/F 部 130 から受け取った電子メールのヘッダ部に書き込まれている送信元メールアドレスを判定対象アドレスとし、当該判定対象アドレスがメールフィルタデータ 154 b 1 においてタイプ識別子 “pass” を対応付けられている送信元ア

ドレスの何れかと一致するか否かを判定する。

[0036] ステップS A 1 0 0の判定結果が“Y e s”である場合、フィルタリング手段1 5 0 6 aは当該電子メールをメールチェック手段1 5 0 8に与える。これに対して、ステップS A 1 0 0の判定結果が“N o”である場合には、フィルタリング手段1 5 0 6 aは、当該電子メールの送信元メールアドレス、送信先メールアドレスおよび当該電子メールの送信先の端末装置を一意に示す端末識別子（例えば、I Pアドレス）をメールアドレスデータベース1 5 4 c 1に登録（ステップS A 1 5 0）するとともに当該電子メールを不揮発性記憶部1 5 4の所定の記憶領域に書き込んで、当該中継動作を終了する。つまり、この場合は、評価対象の電子メールは中継装置1 0にてフィルタリングされる。なお、本実施形態では上記記憶領域が図4におけるメール保持手段1 5 1 6の役割を果たすのである。

[0037] メールアドレスデータベース1 5 4 c 1には、フィルタリング手段1 5 0 6 aによりフィルタリングされた電子メールの送信元メールアドレス、送信先メールアドレスおよび当該電子メールの送信先の端末装置の端末識別子（以下、送信元メールアドレス等）に対応付けて、タイプ識別子、結果識別子および判定回数の各データが格納される。タイプ識別子は、“pass”、“reject”および“none”の何れかの値を有する識別子であり、当該タイプ識別子に対応付けられた送信元アドレスおよび送信先アドレスにより特定される電子メールを“通過させた”、“通過させなかった”および“通過の可否の判断を見合わせた”、を夫々表す。結果識別子は、通過の可否の判断を見合わせた電子メールについて最終的に受信を許可されたのか、それとも受信を拒否されたのかを示す。フィルタリング手段1 5 0 6 aによるメールアドレスデータベース1 5 4 c 1への送信元メールアドレス等の登録の際には、結果識別子にはタイプ識別子と同じ値（本実施形態では、“none”）がセットされる。そして、値“none”をセットされた結果識別子は、受信の可否についての最終的な判断が下された際に“pass”または“reject”に更新される。

[0038] フィルタリング手段1 5 0 6 aは、フィルタリングした電子メールの送信

元メールアドレス等をメールアドレスデータベース154c1に登録する際には、まず、当該送信元メールアドレス等が登録済であるか否かを判定する。登録済ではない場合には、フィルタリング手段1506aは、登録しようとする送信元メールアドレス等に、タイプ識別子として“none”を、結果識別子として“none”を、判定回数として“0”を対応付けてメールアドレスデータベース154c1に書き込む。これに対して、登録済である場合には、フィルタリング手段1506aは、登録しようとするものと同じ送信元メールアドレス等に対応付けてメールアドレスデータベース154c1に格納されている判定回数の値を1だけカウントアップする。

[0039] ステップSA100の判定結果が“Y e s”である場合に実行されるステップSA110では、メールチェック手段1508は、まず、フィルタリング手段1506aから与えられた電子メールの送信元メールアドレス等を揮発性記憶部152の所定の記憶領域に退避した後に当該電子メールを評価プログラムに与える。ここで、迷惑メールであると判断した場合の評価プログラムの動作はその評価プログラムの仕様や設定により定まり、種々の態様が考えられる。第1に、評価対象の電子メールを破棄する態様である。第2に、評価対象の電子メールを不揮発性記憶部154の所定の記憶領域（評価対象プログラムにて設定された記憶領域）に書き込んで隔離する態様である。これら第1および第2の態様の場合は、評価対象の電子メールが評価プログラムからメールチェック手段1508に返却されることはなく、当該電子メールがその宛先へ転送されることはない。第3の態様は、評価対象の電子メールに迷惑メールであることを示す情報を付与する態様であり、第4の態様は、評価対象の電子メールからコンピュータウイルス等を削除する態様である。これら第3および第4の態様は、迷惑メールであっても受信する旨の設定が評価プログラムに対して為されていた場合等に採用される。評価プログラムにおいて第3或いは第4の態様が採用されていた場合には、評価結果（迷惑メールであったか否か）とともに迷惑メールであることを示す情報の付加等の行われた電子メールがメールチェック手段1508に返却される。

- [0040] 評価プログラムによる評価を通過しなかった場合（評価プログラムによって破棄された場合や隔離された場合：ステップS A 1 1 0：“NG”）には、メールチェック手段1 5 0 8は、評価対象の電子メールの送信元メールアドレス等に対応付けてメールアドレスデータベース1 5 4 c 1に格納されている結果識別子を“pass”から“none”に更新し（ステップS A 1 5 0）、当該中継動作を終了する。これに対して、評価プログラムによる評価を通過した場合（迷惑メールではなかった場合、または迷惑メールではあったものの受信する設定が為されていた場合：ステップS A 1 1 0：“pass”）には、メールチェック手段1 5 0 8は、評価プログラムによる評価結果（迷惑メールであった場合には“NG”、迷惑メールではなかった場合には“OK”）を揮発性記憶部1 5 2の所定の記憶領域に書き込み、当該評価プログラムによる評価を通過した電子メールをURLチェック手段1 5 1 0に与える。
- [0041] URLチェック手段1 5 1 0は、メールチェック手段1 5 0 8から与えられた電子メールを解析してメール本文にURLを含んでいるか否かを判定する（ステップS A 1 2 0）。ここでURLとは、webサイトなど広域網3 0を介して利用可能な資源を一意に示す識別子のことをいう。一般にURLは“HTTP”或いは“HTTPS”で始まる文字列であるため、URLチェック手段1 5 1 0は、メールチェック手段1 5 0 8から与えられた電子メールの表すメール本文に“HTTP”或いは“HTTPS”で始まる文字列が含まれている場合に、当該メール本文にはURLが含まれていると判定する。
- [0042] URLチェック手段1 5 1 0は、メール本文にURLを含んでいると判定した電子メールについては、そのURL等をURLデータベース1 5 4 dに登録（ステップS A 1 3 0）した後に第1通信I/F部1 2 0に与え、その宛先へと転送させる（ステップS A 1 4 0）。これに対して、メール本文にURLを含んでいないと判定した電子メールについては、URLチェック手段1 5 1 0は、URLデータベース1 5 4 dへのURL等の登録を行うことなく第1通信I/F部1 2 0に与え、その宛先へと転送させる。つまり、本実施形態では、メールチェック手段1 5 0 8によるチェックを通過してUR

Ｌチェック手段１５１０に与えられた電子メールはその本文にＵＲＬを含んでいるか否かを問わずにその宛先へと転送される。

[0043] 図８は、ＵＲＬデータベース１５４ｄの格納内容の一例を示す図である。図８に示すようにＵＲＬデータベース１５４ｄには、メール本文にＵＲＬを含んでいた電子メールの送信元メールアドレス、送信先メールアドレスおよび当該電子メールの送信先の端末識別子に対応付けて当該ＵＲＬ、結果識別子、迷惑メール識別子および受信回数が格納される。結果識別子は、当該結果識別子に対応付けられたＵＲＬへのアクセスがユーザによって承認されたのか（pass）、承認されなかったのか(reject)、それとも承認の可否の問い合わせの前であるのか（none）を表す。迷惑メール識別子は当該ＵＲＬをメール本文に含む電子メールについて迷惑メールではないと評価されたのか（OK）、それとも迷惑メールと評価されたのか（NG）を表す。この迷惑メール識別子には評価プログラムから返却された評価結果（メールチェック手段１５０８によって揮発性記憶部１５２の所定の記憶領域に格納された値）が設定される。

[0044] ＵＲＬチェック手段１５１０は、ＵＲＬデータベース１５４ｄにＵＲＬ等を登録する際には、まず、当該ＵＲＬ、当該ＵＲＬをメール本文に含む電子メールの送信元メールアドレス、送信先メールアドレスおよび送信先の端末識別子の組が既登録であるか否かを判定する。既登録ではない場合には、ＵＲＬチェック手段１５１０は、上記ＵＲＬ、送信元メールアドレス、送信先メールアドレスおよび送信先の端末識別子の組に、結果識別子として“none”を、迷惑メール識別子として評価プログラムによる評価結果に応じた値を、受信回数として“０”を各々対応付けてＵＲＬデータベース１５４ｄに書き込む。これに対して、既登録である場合には、上記ＵＲＬ、送信元メールアドレス、送信先メールアドレスおよび送信先の端末識別子の組に対応付けてＵＲＬデータベース１５４ｄに格納されている受信回数を１だけカウントアップする。

[0045] 上記動作が実行されるため、拠点内ＬＡＮ２０の端末装置のユーザが広域

網30側から受信する電子メールのうち、見知らぬ相手から受信した電子メールはフィルタリング手段1506aによってフィルタリングされメール保持手段1516に蓄積される。また、送信元メールアドレスを詐称するなどして上記フィルタリングを潜り抜けた電子メールがあったとしても、評価プログラムによる評価を通過しなかった電子メールはその宛先への転送は見合わされる。フィルタリングを通過し、かつ評価プログラムによる評価を通過した電子メールはその宛先へと転送されるのであるが、その電子メールのメール本文にURLが含まれている場合にはそのURLはURLデータベース154dに登録され、拠点内LAN20から広域網30へのwebアクセスの中継制御の際に利用される。

以上が、拠点内LAN20が広域網30側から受信した電子メールの中継動作である。

[0046] (B-3: 拠点内LAN20から広域網30へ送信された電子メールの中継動作)

図9は、拠点内LAN20から広域網30へ送信された電子メールの中継動作の流れを示す図である。図9のステップSA200は図6のステップSA100に、図9のステップSA250は図6のステップSA150に夫々対応している。図9と図6とを対比すれば明らかなように、拠点内LAN20から広域網30へ送信された電子メールの中継動作は、ステップSA100に代えてステップSA200を実行する点、ステップSA120およびステップSA130を省略した点、およびステップSA150に代えてステップSA250を実行する点が、拠点内LAN20が広域網30側から受信した電子メールの中継動作と異なる。以下、拠点内LAN20が広域網30側から受信した電子メールの中継動作との相違点であるステップSA200およびステップSA250を中心に説明する。

[0047] 図9のステップSA200は、第1通信I/F部120を介して拠点内LAN20から電子メールを受信したことを契機としてフィルタリング手段1506bによって実行される処理である。このステップSA200では、

フィルタリング手段1506bは、受信した電子メールの送信先メールアドレスに基づくフィルタリングをメールフィルタデータ154b2を参照して実行する。より詳細に説明すると、フィルタリング手段1506bは受信した電子メールの送信先メールアドレスに対応付けてメールフィルタデータ154b2に格納されているタイプ識別子が“pass”である場合には当該電子メールはフィルタリング対象ではないと判定する（ステップSA200：Yes）。

[0048] 図9のステップSA250は、ステップSA200にてフィルタリング対象と判定された電子メールの送信先メールアドレス等をメールアドレスデータベース154c2に登録する処理である。メールアドレスデータベース154c2のテーブルフォーマットはメールアドレスデータベース154c1のテーブルフォーマットと同一である。ただし、メールアドレスデータベース154c2には、送信先の端末識別子ではなく、フィルタリング対象と判定された電子メールの送信元の端末装置の端末識別子が格納される。また、このステップSA250では、メールアドレスデータベース154c2への送信先メールアドレス等の登録のみが行われ、メール保持手段1516への当該電子メールの書き込みは行われない点が前述したステップSA150の処理と異なる。

以上が、拠点内LAN20から広域網30へ送信された電子メールの中継動作である。

[0049] （B-4：拠点内LAN20から広域網30へのwebアクセスの中継動作）

次いで、拠点内LAN20から広域網30のwebサーバ装置へのwebアクセスの中継動作について説明する。図10は、当該中継動作の流れを示すフローチャートである。上記webアクセスにおけるアクセス先のURLは、第1通信I/F部120を介してリダイレクト手段1512に与えられる。リダイレクト手段1512は、まず、第1通信I/F部120から受け取ったwebアクセス先のURLおよび当該webアクセスの送信元の端末

識別子が、“none” または “reject” の結果識別子と対応付けてURLデータベース154dに格納されているURLおよび端末識別子の組の何れかに一致するか否かを判定する（ステップSA300）。

[0050] webアクセス先のURLおよびそのwebアクセスの送信元の端末識別子の組に対応付けてURLデータベース154dに格納されているタイプ識別子の値が“reject”であった場合には、リダイレクト手段1512は、アクセスを拒絶する旨のメッセージを記載した画面のHTMLデータを当該webアクセスの送信元へ返信する（ステップSA340）。このHTMLデータを受信した端末装置では当該HTMLデータにしたがって上記画面が表示される。

[0051] webアクセス先のURLおよびそのwebアクセスの送信元の端末識別子の組に対応付けてURLデータベース154dに格納されているタイプ識別子の値が“none”であった場合には、リダイレクト手段1512は、アクセスの継続の可否を問い合わせるメッセージを記載した画面のHTMLデータを当該webアクセスの送信元へ返信する（ステップSA330）。webアクセスを指示したユーザから見れば、自らのwebアクセスがリダイレクト手段1512の働きによって他の画面へのアクセスにリダイレクトされたかのように見える。以下、リダイレクト手段1512の働きによってwebアクセスの送信元の端末装置に表示される画面（すなわち、webアクセスによる当初のアクセス先とは異なる画面）のことを「リダイレクト画面」と呼ぶ。

[0052] 図11（a）および図11（b）は、上記リダイレクト画面の一例を示す図である。より詳細に説明すると、図11（a）は、URL、端末識別子および値が“none”の結果識別子に対応付けてURLデータベース154dに格納されている迷惑メール識別子が“OK”である場合に、webアクセスの送信元の端末装置に表示させるリダイレクト画面を示す図である。これに対して、図11（b）は、URL、端末識別子および値が“none”の結果識別子に対応付けてURLデータベース154dに格納されている迷惑メール識

別子が“NG”である場合に、webアクセスの送信元の端末装置に表示させるリダイレクト画面を示す図である。リダイレクト手段1512は、上記URL、端末識別子および値が“none”の結果識別子に対応付けてURLデータベース154dに格納されている迷惑メール識別子が“OK”である場合には、図11(a)に示すリダイレクト画面のHTMLデータを返信し、逆に、上記URL、端末識別子および値が“none”の結果識別子に対応付けてURLデータベース154dに格納されている迷惑メール識別子が“NG”である場合には、図11(b)に示すリダイレクト画面のHTMLデータを返信する。一般に、迷惑メールを送信してくるような相手方の信頼性には疑問が残る。本実施形態では、メールチェック手段1508のチェック結果を反映してリダイレクト画面の表示内容を異ならせることで、webアクセスを継続することの危険の度合いをユーザに把握させるのである。

[0053] 上記HTMLデータを受信した端末装置では当該HTMLデータにしたがって上記リダイレクト画面が表示される。当該リダイレクト画面を視認したユーザは、図11(a)或いは図11(b)のリダイレクト画面における[許可する]ボタンをマウスクリック等することでwebアクセスの継続を許可することや、同[拒否する]ボタンをマウスクリック等することでwebアクセスの継続を拒否することを指示することができる。図11(a)或いは図11(b)のリダイレクト画面に対する操作によってwebアクセスの継続の可否が指示されると、上記端末装置はユーザの指示内容を反映した応答を中継装置10へ返信する。拒否する旨の応答を受信した場合には、リダイレクト手段1512は上記URLおよび端末識別子に対応付けてURLデータベース154dに格納されている結果識別子を“none”から“reject”に更新し、webアクセス中継処理を終了する。以後、上記webアクセスの送信元が当該URLをアクセス先とするwebアクセスを行ったとしても、当該送信元の端末識別子および当該URLに対応付けてURLデータベース154dに格納されている結果識別子は“reject”であるため、前述したステップSA340の処理が実行される。つまり、アクセスを継続しない旨の応答

が行われた以降は図 1 1 (b) のリダイレクト画面による問い合わせが再度行われることはない。

[0054] 逆に、許可する旨の応答を受信した場合には、リダイレクト手段 1 5 1 2 は上記 URL および端末識別子に対応付けて URL データベース 1 5 4 d に格納されている結果識別子を “none” から “pass” に更新し、さらに上記 web アクセスメッセージを第 2 通信 I / F 部 1 3 0 に引き渡して web アクセス中継処理を終了する。以降、上記 web アクセスは広域網 3 0 内の中継装置によって適宜ルーティングされてその宛先の web サーバ装置へ到達し、当該 web サーバ装置から上記 web アクセス先の URL に対応する HTML データが返信されてくる。この HTML データは広域網 3 0、中継装置 1 0 および拠点内 LAN 2 0 を介して上記 web アクセスの送信元の端末装置へ伝送され、当該端末装置では当該 HTML データにしたがって画面表示が行われる。以後、上記 web アクセスの送信元が当該 URL をアクセス先とする web アクセスを行った場合には、当該送信元の端末識別子および当該 URL に対応付けて URL データベース 1 5 4 d に格納されている結果識別子は “pass” であるため、ステップ SA 3 1 0 以降の処理が実行される。したがって、アクセスを継続する旨の応答があった以降は図 1 1 (a) のリダイレクト画面による問い合わせが再度行われることはない。

[0055] 図 1 0 のステップ SA 3 0 0 に戻って、web アクセス先の URL およびその web アクセスの送信元の端末識別子の組に対応付けて URL データベース 1 5 4 d に格納されているタイプ識別子の値が “pass” であった場合、または web アクセス先の URL およびその web アクセスの送信元の端末識別子の組が URL データベース 1 5 4 d に登録されていない場合には、リダイレクト手段 1 5 1 2 は、当該 web アクセスの送信元の端末装置が広域網 3 0 から受信する電子メールであって中継装置 1 0 にて転送を見合わせたもの、または当該 web アクセスの送信元の端末装置から広域網 3 0 へ送信された電子メールであって中継装置 1 0 にて転送を見合わせたものが有ったか否かをメールアドレスデータベース 1 5 4 c 1 および 1 5 4 c 2 の格納内

容を参照して判定する（ステップS A 3 1 0）。具体的には、リダイレクト手段1 5 1 2は、w e bアクセスの送信元の端末識別子を含むレコードであって、結果識別子の値が” none” のレコードがメールアドレスデータベース1 5 4 c 1に登録されている場合には、前者の電子メールがあったと判定し、同端末識別子を含むレコードであって、結果識別子の値が” none” のレコードがメールアドレスデータベース1 5 4 c 2に登録されている場合には、後者での電子メールがあったと判定する。中継装置1 0にて転送を見合わせたものがなかった場合には、リダイレクト手段1 5 1 2はw e bアクセスメッセージを第1通信1 / F部1 2 0に引き渡して（ステップS A 3 2 0）、w e bアクセス中継処理を終了する。

- [0056] これに対して転送を見合わせた電子メールがあった場合には、リダイレクト手段1 5 1 2は、転送の可否を問い合わせるメッセージを記載したリダイレクト画面のHTMLデータを上記w e bアクセスの送信元へ返信する（ステップS A 3 3 0）。図1 2（a）および図1 2（b）は、上記リダイレクト画面の一例を示す図である。図1 2（a）はw e bアクセスの送信元の端末装置が広域網3 0から受信する電子メールであって中継装置1 0にて転送を見合わせたものがあつた場合のリダイレクト画面の一例を示す図である。一方、図1 2（b）はw e bアクセスの送信元の端末装置から広域網3 0へ送信されたものの、中継装置1 0にて転送を見合わせた電子メールがあつた場合のリダイレクト画面の一例を示す図である。図1 2（a）に示すリダイレクト画面を視認したユーザは、転送を所望する（或いは拒否する）送信元メールアドレスに対応するチェックボックスにチェックを入れ、[許可する]（或いは[拒否する]）を選択することで送信元毎に転送の可否を指示し、その指示内容を反映した応答を端末装置に返信させることができる。同様に図1 2（b）に示すリダイレクト画面を視認したユーザは、転送を所望する（或いは拒否する）送信先メールアドレスに対応するチェックボックスにチェックを入れ、[許可する]（或いは[拒否する]）を選択することで送信先毎に転送の可否を指示し、その指示内容を反映した応答を端末装置に返信させる

ことができる。

- [0057] 一方、リダイレクト手段 1512 は、上記応答を受信すると、上記応答によって転送を許可する旨を指示された送信元から送信された電子メール（或いは転送を許可する旨を指示された送信先宛ての電子メール）について、以後、転送の見合わせが行われないように、その送信元メールアドレス（或いは送信先メールアドレス）をタイプ識別子 “pass” と対応付けてメールフィルタデータ 154b1（或いはメールフィルタデータ 154b2）に登録し、当該メールアドレスおよび上記応答の送信元の端末識別子に対応付けてメールアドレスデータベース 154c1（或いはメールアドレスデータベース 154c2）に登録されている結果識別子を “pass” に更新する。
- [0058] また、図 12（a）に示すリダイレクト画面に対する応答によって、web アクセスの送信元の端末装置が広域網 30 から受信する電子メールの転送が許可された場合には、リダイレクト手段 1512 は、該当する電子メールをメール保持手段 1516 から読み出してメール生成／送信手段 1514 に与える。ここで、該当する電子メールとは、メール保持手段 1516 に格納されている電子メールのうち、上記応答の送信元の端末識別子および値が “pass” のタイプ識別子に対応付けてメールアドレスデータベース 154c1 に格納されている送信元アドレスおよび送信先アドレスを、送信元メールアドレスおよび送信先メールアドレスとする電子メールのことをいう。メール生成／送信手段 1514 は、当該電子メールのヘッダ部の送信元メールアドレスを当該中継装置 10 を示すメールアドレスに書き換えて広域網 30 のメールサーバへ送信する。以降、当該電子メールは広域網 30 内のメールサーバによって受信され、上記端末装置からの要求等に応じて当該端末装置へ転送されるのであるが、その送信元メールアドレスである中継装置 10 の電子メールアドレスはタイプ識別子 “pass” を対応付けてメールフィルタデータ 154b1 に登録されているため、フィルタリング手段 1506a によってフィルタリングされることはなく、当該端末装置へ転送される。
- [0059] これに対して、上記応答によって転送を拒否する旨を指定された送信元か

ら送信された電子メール（或いは転送を拒否する旨を指定された送信先宛ての電子メール）については、その送信元メールアドレス（或いは送信先メールアドレス）および上記応答の送信元の端末識別子に対応づけてメールアドレスデータベース154c1（或いはメールアドレスデータベース154c2）に登録されている結果識別子を“reject”に更新する。このように、メールアドレスデータベース154c1（或いはメールアドレスデータベース154c2）に登録されている結果識別子が“reject”に更新されたメールアドレスを送信元メールアドレス（或いは送信先メールアドレス）とする電子メールについては、以降、ステップSA310において転送を見合わせた電子メールと判定されることはない。

[0060] 本実施形態によれば、拠点内LAN20が広域網30から受信した電子メールであって、本文にURLの記載された電子メールの中継を契機として即座にURLデータベース154dへの当該URLへの登録が行われる。そして、拠点内LAN20の端末装置から広域網30のwebサーバ装置へのwebアクセスを検知した場合には、中継装置10は当該webアクセス先のURLがURLデータベース154dに登録されているか否かを判定し、アクセスを拒絶する旨のタイプ識別子を対応付けて登録されている場合に当該webアクセスは拒絶される。

[0061] 一方、上記URLについてアクセスの可否についての判断が未だなされていない場合には、中継装置10はwebアクセスの継続の可否を問い合わせるリダイレクト画面を端末装置に表示させ、アクセスする旨の返答が得られた場合にwebアクセスを中継する。このため、本実施形態によれば、メール流量が所定の閾値を超えるまでURLデータベース154dへのURLの登録が行われないことに起因する不具合（迅速に登録が行われないためにウィルス感染や詐欺被害の拡大すること）が発生することはない。また、本実施形態では、既にアクセス許可が為されたwebサイトやURLデータベース154dに登録されていないURLへのwebアクセスの際に、転送を見合わせた電子メールがある場合には、そのアクセス元へ通知して転送の可否

の判断を行わせ、その判断結果に即してメールフィルタを迅速に更新し、以降の電子メールの送受信に支障が生じないようにすることもできる。なお、転送を見合わせた電子メールの保存および当該電子メールの転送は必須ではなく、これらを省略する場合にはメール生成／送信手段 1514 およびメール保持手段 1516 を省略しても勿論良い。

[0062] 上記実施形態では、web アクセスの継続の可否と転送を見合わせた電子メールの転送の可否を各々別個のリダイレクト画面により問い合わせたが、図 13 に示すように、1 つのリダイレクト画面で問い合わせるようにしても良い。具体的には、図 10 のステップ SA300 において URL データベース 154d の検索とメールアドレスデータベース 154c1 および 154c2 の検索を行い、その検索結果に応じて異なるリダイレクト画面を表示させるようにすれば良い。例えば、web アクセス先の URL および当該 web アクセスの送信元の端末識別子の組に対応付けて URL データベース 154d に格納されている結果識別子の値が “none” であり、かつ、転送を見合わせた電子メールがない場合には、迷惑メールチェックの結果に応じて図 11 (a) 或いは図 11 (b) に示すリダイレクト画面を表示させ、転送を見合わせた電子メールがあった場合には、図 13 に示すリダイレクト画面を表示させるのである。なお、図 13 に示すリダイレクト画面を表示させた場合、当該画面に対する操作に応じて URL データベース 154d、メールアドレスデータベース 154c1 (或いは 154c2)、およびメールフィルタデータ 154b1 (或いは 154b2) の更新を行わせても良いことは勿論である。

[0063] 上記実施形態では、拠点内 LAN20 が広域網 30 から受信する電子メールのうち中継装置 10 にて転送を見合わせたもの (すなわち、フィルタリング手段 1506a によってフィルタリングされた電子メール) をメール保持手段 1516 に保持し、メール生成／送信手段 1514 によるメール送信処理の対象とした。しかし、拠点内 LAN20 から広域網 30 へ送信された電子メールのうち中継装置 10 にて転送を見合わせたもの (すなわち、フィル

タリング手段 1506b によってフィルタリングされた電子メール)もメール保持手段 1516 に保持し、メール生成/送信手段 1514 によるメール送信処理の対象としても良い。ただし、この場合は、メール生成/送信手段 1514 による送信元メールアドレスの書き換えを行う必要はなく、メール保持手段 1516 に保持されていた電子メールをそのまま広域網 30 へ送出すれば良い。

[0064] 上記実施形態では、フィルタリング手段 1506b によるフィルタリングが行われた場合には、リダイレクト画面により転送の見合わせを通知するのではなく、転送を見合わせた旨を通知する電子メールであって、図 12 (b) に示すリダイレクト画面へのリンク情報が記載された電子メールの送信指示をフィルタリング手段 1506b からメール生成/送信手段 1514 に与え、当該電子メールを送信する処理をメール生成/送信手段 1514 に実行させるようにしても良い。この場合、当該電子メールが URL チェック手段 1510 によるチェックにひっかからないようにするために、中継装置 10 の電子メールアドレスを送信元メールアドレスとする電子メールを URL チェック手段 1510 によるチェック対象から除外しておいても良い。また、中継装置 10 の電子メールアドレスの他にも URL チェック手段 1510 によるチェック対象から除外する送信元メールアドレスを定めておいても良い。

[0065] (C : 変形)

以上本発明の実施形態について説明したが、この実施形態に以下の変形を加えても勿論良い。

(1) 上記実施形態では、拠点内 LAN 20 が広域網 30 から受信した電子メールと拠点内 LAN 20 から広域網 30 へ送信された電子メールの両方をメールフィルタチェックの対象としたが前者のみをメールフィルタチェックの対象としても良い。拠点内 LAN 20 が広域網 30 から受信した電子メールについてのみメールフィルタチェックを行う場合にはフィルタリング手段 1506b を省略すれば良い。また、迷惑メールであるか否かのチェックに

についても必ずしも必須ではなくメールチェック手段1508を省略しても良い。また、メールフィルタデータ154b1および154b2を外部機器I/F部140を介して中継装置10に与えるようにしても良く、この場合はアドレス帳解析手段1502およびメールフィルタデータ生成手段1504を省略することができる。また、上記実施形態では、広域網30を介して利用可能な資源の一例としてwebサーバ装置を挙げたが、FTPサーバ装置などの他のサーバ装置であっても良く、これらサーバ装置に記憶されている各種データ、これらサーバ装置で実行されるプログラムであっても良い。また、当該資源を示す識別子として上記実施形態ではURLを用いたがURI (Uniform Resource Identifier) を用いても勿論良い。要は、広域網を介して利用可能な資源を一意に示す識別子であれば良い。

[0066] (2) 上記実施形態では、webサイトへのアクセスの制御を端末装置毎（すなわち、端末識別子毎）に行ったが、拠点内LAN20に属する全ての端末装置に対して一括して行うようにしても良い。具体的には、URLチェック手段1510にはURLデータベース154dにURLの登録を行う際には当該URLをメール本文に含む電子メールの送信先の端末識別子を対応付けずにその登録を行わせ、リダイレクト手段1512にはwebアクセス先のURLがURLデータベース154dに登録されているか否か、そして登録されている場合には当該URLに対応付けられているタイプ識別子が”none”、“pass”および”reject”の何れであるかに応じてアクセス中継制御を行わせるようにすれば良い。

[0067] (3) 上記実施形態では、URLデータベース154dが中継装置10の不揮発性記憶部154に記憶されていた。しかし、拠点内LAN20や広域網30などの通信網に接続された記憶装置（ネットワーク対応のハードディスク装置等）であって、中継装置10の制御部110が当該通信網経由でアクセス可能な記憶装置にURLデータベース154dを記憶させておいても良い。そして、この場合、複数の中継装置に1つのURLデータベースを共有させるようにしても良い。

[0068] (4) 上記実施形態では、拠点内LAN20を広域網30に接続する中継装置10に、不用意なwebアクセスに起因する詐欺被害等を防止する機能と、受信者にとって見知らぬ送信元から送信された電子メールや迷惑メールをフィルタリングする機能と、を担わせたが何れか一方の機能のみを担わせても良い。前者の機能のみを有する中継装置の構成例としては、ローカルエリアネットワークを広域網に接続する中継装置に、ローカルエリアネットワークが広域網から受信した電子メールにURLが含まれているか否かを判定し、含まれている場合に当該URLをURLデータベースに登録するURLチェック手段と、ローカルエリアネットワーク内の端末装置から広域網に接続されるwebサーバ装置へのアクセスの検知を契機として、当該webサーバ装置に対応するURLがURLデータベースに登録されているか否かを判定し、URLデータベースに登録されたURLである場合に、webアクセスの可否を問い合わせるリダイレクト画面を当該端末装置に表示させ、アクセスを許可する返答が得られた場合にwebアクセスを中継するリダイレクト手段とを設ける構成が考えられる。このような中継装置であっても、不用意なwebアクセスに起因する詐欺被害等を防止することができるからである。

[0069] また、後者の機能（受信者にとって見知らぬ送信元から送信された電子メールやウィルスを含んだ電子メールなどの迷惑メールをフィルタリングする機能）のみを有する中継装置の構成例としては、ローカルエリアネットワークを広域網に接続する中継装置に、ローカルエリアネットワーク内の端末装置が広域網から受信する電子メールをその送信元メールアドレスに基づいてフィルタリングする第1のフィルタリング処理と、当該端末装置から広域網へ送信された電子メールをその送信先メールアドレスに基づいてフィルタリングする第2のフィルタリング処理のうち少なくとも前者を実行するフィルタリング手段と、フィルタリング手段によりフィルタリングされなかった電子メールについて迷惑メールであるか否かをチェックし、迷惑メールではないと判定した場合にその宛先へ転送するメールチェック手段と、ローカルエ

リアネットワーク内の端末装置のメールアドレス帳データを解析して電子メールアドレスを抽出するアドレス帳解析手段と、アドレス帳解析手段により抽出された電子メールアドレスに基づいてフィルタリング手段におけるフィルタリング条件を表すメールフィルタデータを生成し、フィルタリング手段に与えるメールフィルタデータ生成手段とを設ける構成が考えられる。

[0070] メールアドレス帳データに基づくフィルタリング制御に関する先行技術の一例としては特許文献2に開示の技術が挙げられるが、前述したように、この技術には相手方のアドレス帳に自分のメールアドレスが登録されていない場合には当該相手方を宛先として電子メールを送信することができないといった制約や、メールを送受信するユーザが同じシステムを使用していなければならないといった制約があり、実状にそぐわないといった問題があった。これに対して、上記フィルタリング手段、メールチェック手段、アドレス帳解析手段およびメールフィルタデータ生成手段を組み合わせた構成の中継装置であれば特段の制約を課されることなく、受信者にとって見知らぬ送信元から送信された電子メールや迷惑メールをフィルタリングすることが可能になる。

[0071] (5) 上記実施形態では本発明の特徴を顕著に示す各手段をソフトウェアモジュールにより実現したが上記各手段を電子回路により実現し、それら電子回路を組み合わせることで本発明の中継装置を実現しても勿論良い。

[0072] (6) 上記実施形態では本実施形態の特徴を顕著に示すプログラム（中継制御プログラム154a）が中継装置10の不揮発性記憶部154に予め記憶されていた。しかし、CD-ROM（Compact Disc-Read Only Memory）などのコンピュータ読み取り可能な記録媒体に上記プログラムを書き込んで配布しても勿論良く、インターネットなどの電気通信回線経由のダウンロードにより上記プログラムを配布しても良い。このようにして配布されるプログラムにしたがって一般的なコンピュータを作動させることで当該コンピュータを本発明の中継装置として機能させることが可能になるからである。

[0073] (7) 上記実施形態では、端末装置PC1や端末装置PC2にインストール

されたメーラを用いて電子メールの送受信を行う例を説明した。しかしながら、本発明の電子メールはいわゆるWebメールをも含む。すなわち、端末装置にインストールされたWebブラウザを通じてアクセスするWebアプリケーションの電子メールクライアントを用いて端末装置が電子メールを送受信し、中継装置が該電子メールに対して処理を行う構成としてもよい。

[0074] (8) 中継装置10と拠点内LAN20との接続(通信経路)は、有線でも無線でも構わない。無線を使用する場合、中継装置は無線LANルータや無線アクセスポイントなどの無線中継装置として機能する。

[0075] 本出願は、2013年5月16日に出願された日本特許出願(特願2013-103857)に基づくものであり、その内容はここに参照として取り込まれる。

符号の説明

[0076] 10…中継装置、20…拠点内LAN、30…広域網、110…制御部、120…第1通信I/F部、130…第2通信I/F部、140…外部機器I/F部、150…記憶部、152…揮発性記憶部、154…不揮発性記憶部、154a…中継制御プログラム、154b1, 154b2…メールフィルタデータ、154c1, 154c2…メールアドレスデータベース、154d…URLデータベース、160…バス。

請求の範囲

- [請求項1] ローカルエリアネットワークを広域網に接続する中継装置において、
- 、
- 前記ローカルエリアネットワークが前記広域網から受信した電子メールに前記広域網を介して利用可能な資源を一意に示す識別子が含まれているか否かを判定し、含まれている場合に当該識別子をデータベースに登録する識別子チェック手段と、
- 前記広域網を介して利用可能な資源への前記ローカルエリアネットワーク内の端末装置からのアクセスを検知したことを契機として前記データベースに当該資源を示す識別子が登録されているか否かを判定し、登録されていた場合にはアクセスの可否を問い合わせる画面を前記端末装置に表示させ、アクセスを許可する返答が得られた場合に当該アクセスを中継するリダイレクト手段と、
- を有することを特徴とする中継装置。
- [請求項2] 前記ローカルエリアネットワークが前記広域網から受信した電子メールをその送信元メールアドレスに基づいてフィルタリングする第1のフィルタリング処理と前記ローカルエリアネットワークから前記広域網へ送信された電子メールをその送信先メールアドレスに基づいてフィルタリングする第2のフィルタリング処理のうち、少なくとも前者を実行するフィルタリング手段と、
- 前記フィルタリング手段によってフィルタリングされた電子メールの送信元メールアドレスまたは送信先メールアドレスとその送信先または送信元の端末装置を示す端末識別子を記憶するメールアドレスデータベースと、を備え、
- 前記リダイレクト手段は、前記広域網を介して利用可能な資源へのアクセスを行った端末装置を送信先または送信元とする電子メールのうち前記フィルタリング手段によりフィルタリングされたものがあるか否かを前記メールアドレスデータベースの格納内容を参照して判定

し、前記第1のフィルタリング処理によりフィルタリングされた電子メールについてはその送信元メールアドレスのフィルタリングの解除の可否を問い合わせる画面を当該端末装置に表示させる一方、前記第2のフィルタリング処理によりフィルタリングされた電子メールについてはその送信先メールアドレスのフィルタリングの解除の可否を問い合わせる画面を当該端末装置に表示させ、各画面に対する操作に応じて前記フィルタリング手段におけるフィルタリング条件を更新することを特徴とする請求項1に記載の中継装置。

[請求項3] 前記第1のフィルタリング処理によりフィルタリングされた電子メールを記憶するメール保持手段と、

前記メール保持手段に記憶されている電子メールを、当該中継装置を送信元とする電子メールとして送信するメール生成／送信手段と、を備え、

前記リダイレクト手段は、前記第1のフィルタリング処理のフィルタリング条件の更新に応じて、フィルタリング対象から除外された送信元メールアドレスから前記端末装置へ宛てて送信された電子メールを前記メール生成／送信手段に送信させる

ことを特徴とする請求項2に記載の中継装置。

[請求項4] 前記フィルタリング手段によりフィルタリングされなかった電子メールが迷惑メールであるか否かをチェックするメールチェック手段を備え、

前記識別子チェック手段は、前記メールチェック手段によるチェックを通過した電子メールをチェック対象とする

ことを特徴とする請求項2または3に記載の中継装置。

[請求項5] 前記ローカルエリアネットワーク内の端末装置のメールアドレス帳データを解析して電子メールアドレスを抽出するアドレス帳解析手段と、

前記アドレス帳解析手段により抽出された電子メールアドレスに基

づいて前記フィルタリング手段におけるフィルタリング条件を表すメールフィルタデータを生成し、前記フィルタリング手段に与えるメールフィルタデータ生成手段と、

を有することを特徴とする請求項2から4の何れか1の請求項に記載の中継装置。

[請求項6]

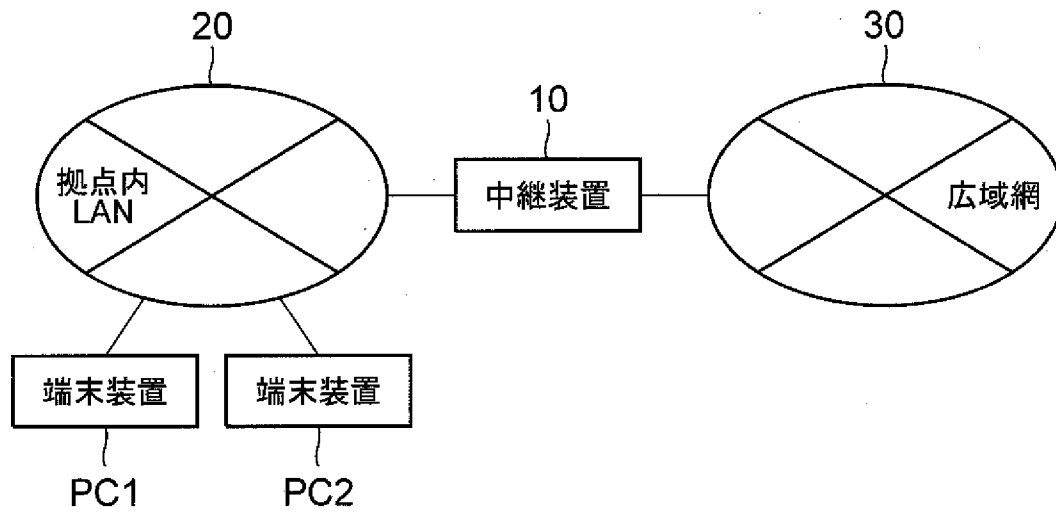
ローカルエリアネットワークを広域網に接続する中継装置の制御方法において、

前記ローカルエリアネットワークが前記広域網から受信した電子メールに前記広域網を介して利用可能な資源を一意に示す識別子が含まれているか否かを判定し、含まれている場合に当該識別子をデータベースに登録し、

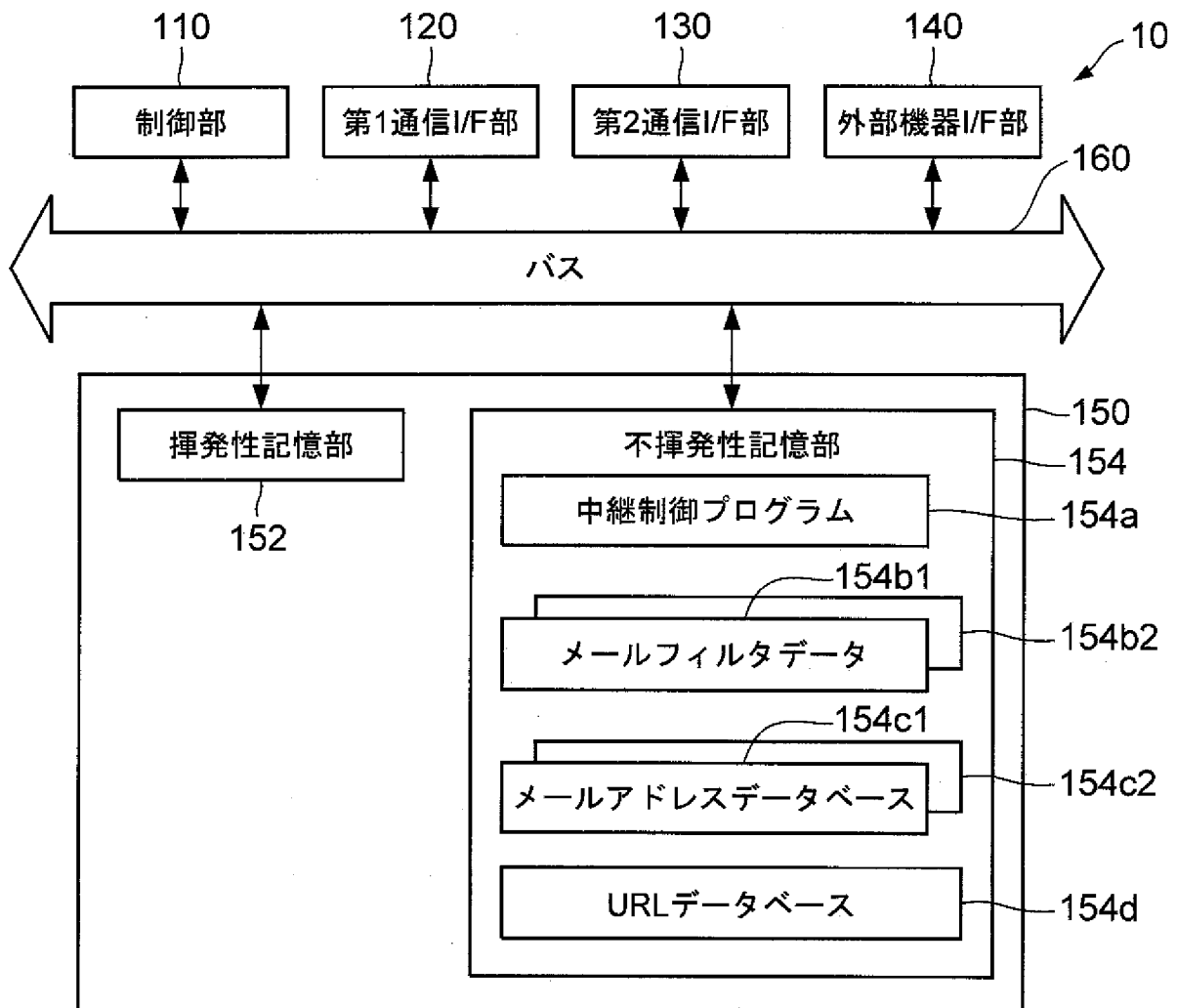
前記広域網を介して利用可能な資源への前記ローカルエリアネットワーク内の端末装置からのアクセスを検知したことを契機として前記データベースに当該資源を示す識別子が登録されているか否かを判定し、登録されていた場合にはアクセスの可否を問い合わせる画面を前記端末装置に表示させ、アクセスを許可する返答が得られた場合に当該アクセスを中継する、

ことを特徴とする制御方法。

[図1]



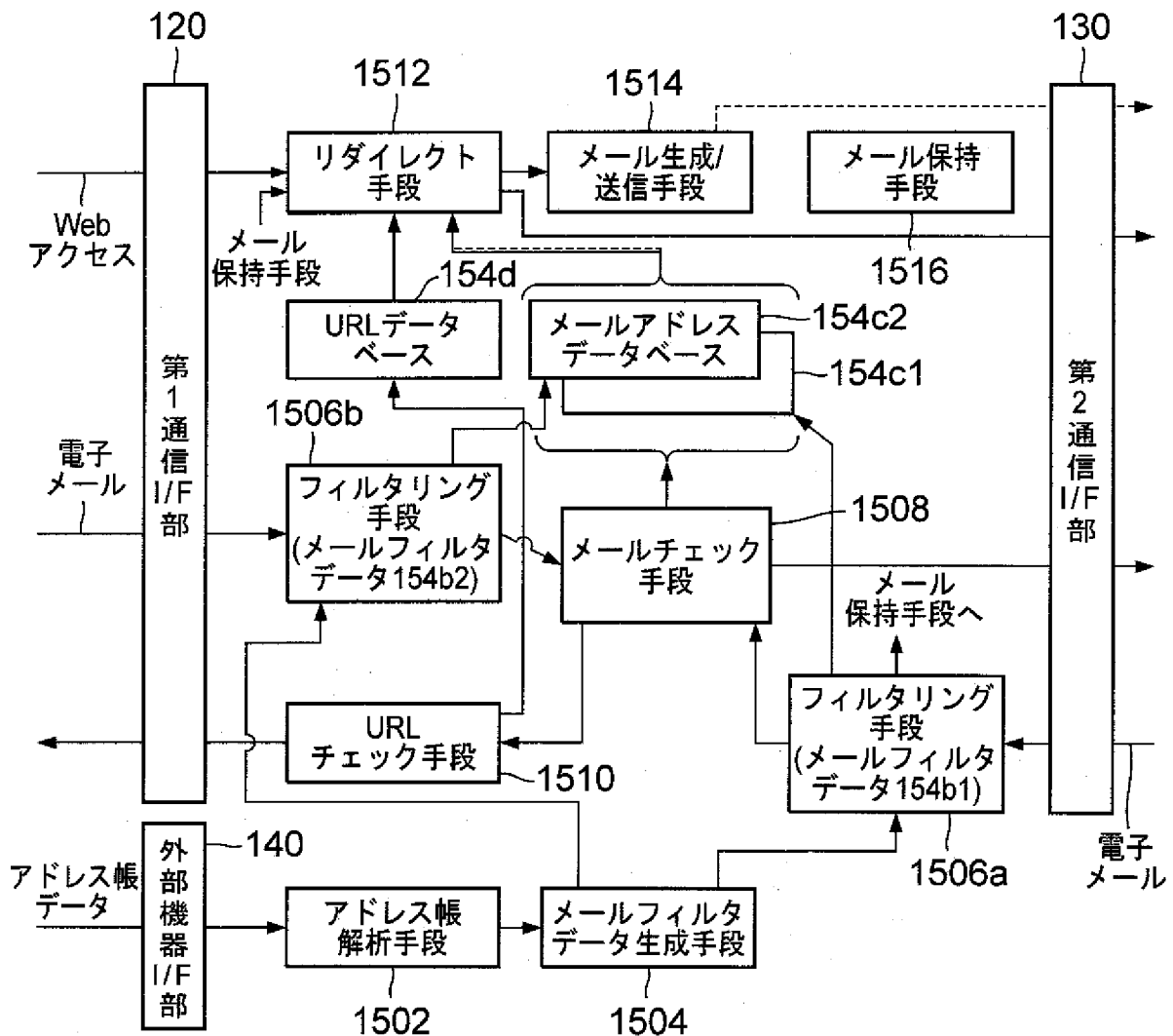
[図2]



[図3]

- (a) 名,姓,表示名,ニックネーム,メールアドレス,別のメールアドレス,...,メモ,
,,1234,,1234@example.jp,,...,,
,,abcd,,abcd@example.jp,,...,,
- (b) 表示名,電子メールアドレス,自宅の番地,...,役職
1234, 1234@example.jp,,...,,

[図4]

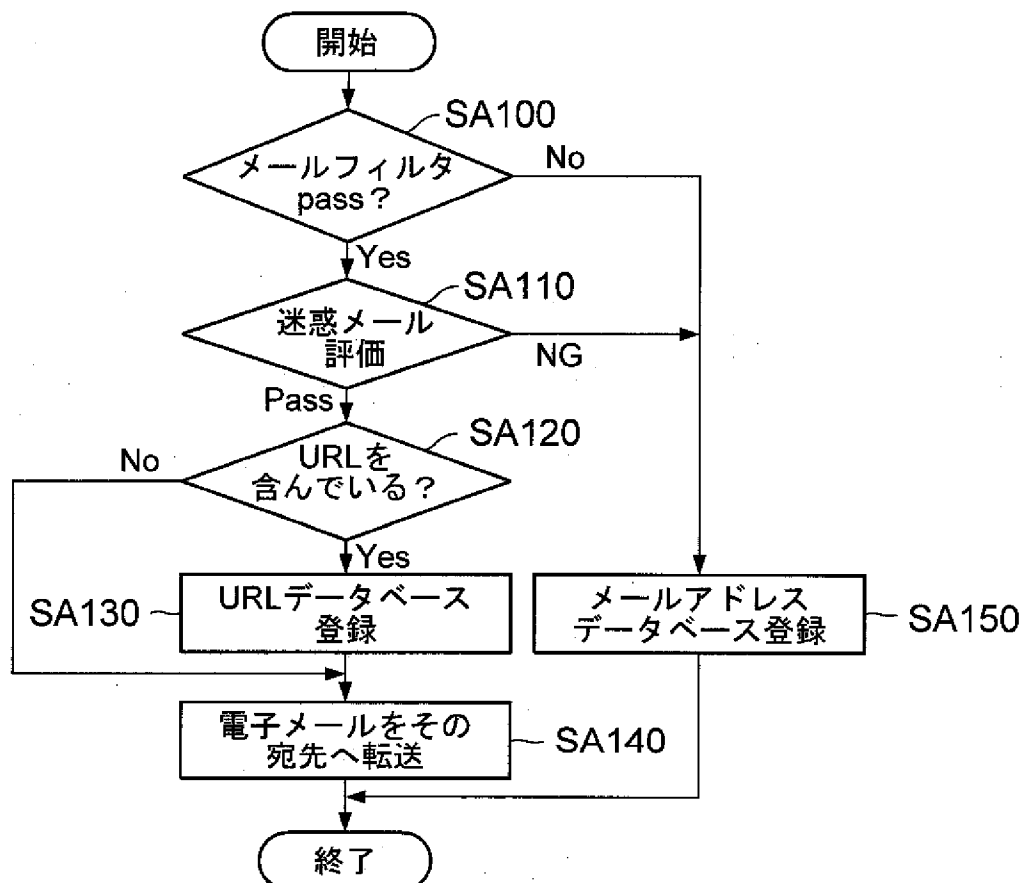


[図5]

(a)	送信元アドレス	送信先アドレス	タイプ識別子
	1234@example.jp	*	pass
	abcd@example.jp	*	pass
	router@example.jp	*	pass
	それ以外	*	reject

(b)	送信元アドレス	送信先アドレス	タイプ識別子
	*	1234@example.jp	pass
	*	abcd@example.jp	pass
	*	それ以外	reject

[図6]



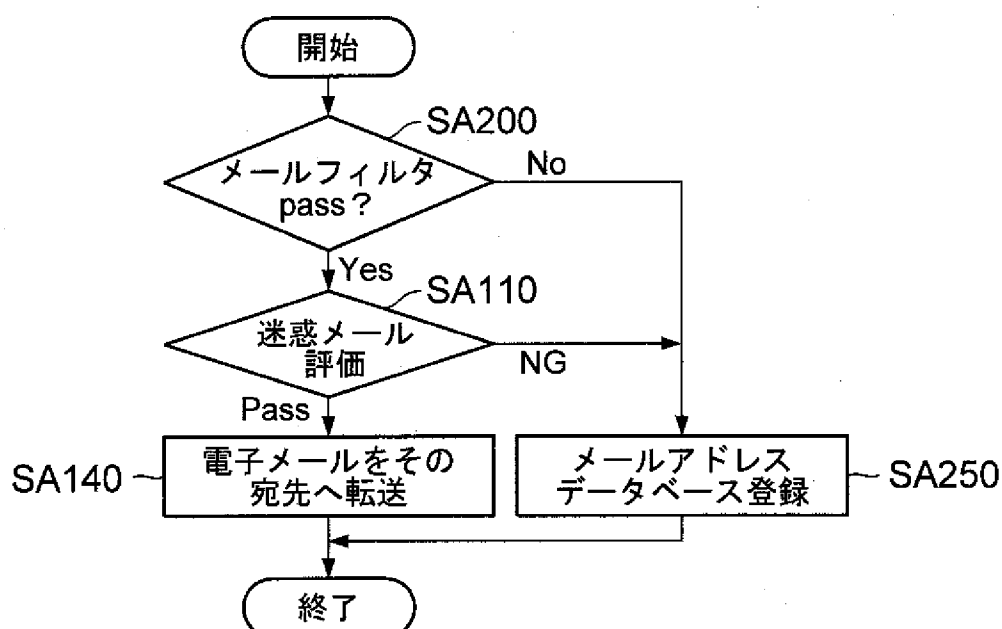
[図7]

送信元 アドレス	送信先 アドレス	端末 識別子	タイプ 識別子	結果 識別子	判定 回数
user0@example.jp	a@example.jp	IP-0	none	none	cnt0
user1@example.jp	b@example.jp	IP-1	pass	pass	cnt1
⋮	⋮	⋮	⋮	⋮	⋮
userN@example.jp	N@example.jp	IP-N	reject	reject	cntN

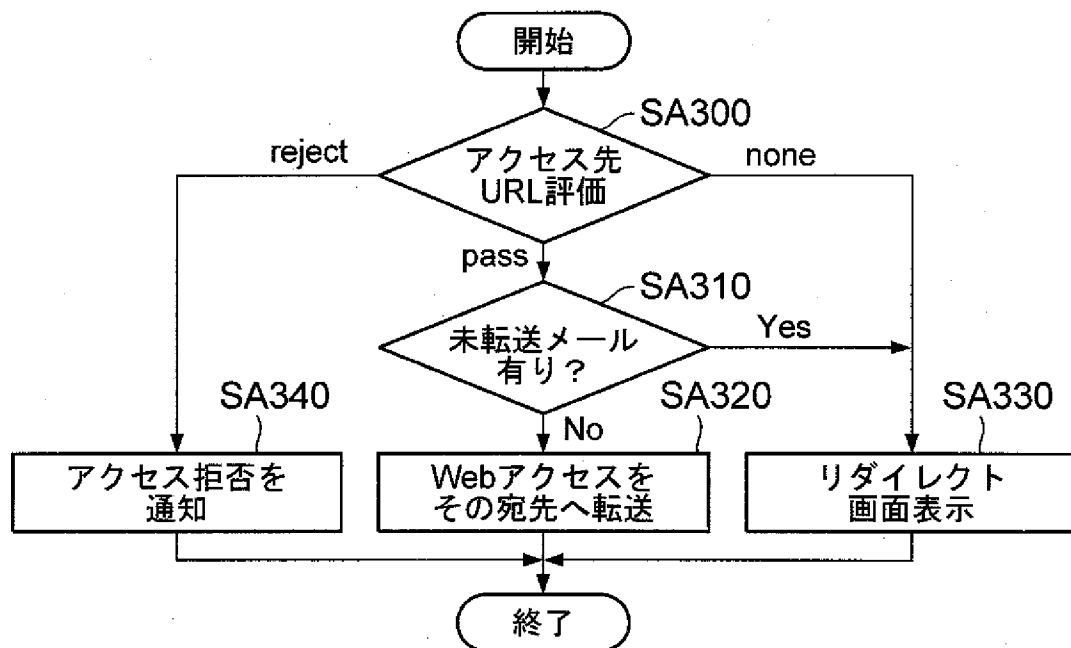
[図8]

URL	送信元 アドレス	送信先 アドレス	端末 識別子	結果 識別子	迷惑メール 識別子	受信 回数
URL2	user2@example.jp	a@example.jp	IP-2	pass	OK	cnt2
URL3	user3@example.jp	b@example.jp	IP-3	none	NG	cnt3
⋮	⋮	⋮	⋮	⋮	⋮	⋮
URLX	userX@example.jp	X@example.jp	IP-X	none	OK	cntX

[図9]



[図10]



[図11]

- (a) 以下のURLにアクセスしようとしています。
このURLは「local1@example.jp」が受信したメールに記載されていたURLで、危険性のあるサイトの可能性があります。
<http://www.abcdefghijklmn.com>
このままこのサイトにアクセスする場合は[許可する]ボタンを押してください。
許可リストに登録され、次回以降、この画面は表示されなくなります。
拒否すると、拒否リストに追加されます。
[許可する] [拒否する]
- (b) 以下のURLにアクセスしようとしています。
このURLは「local1@example.jp」が受信したウィルス感染したメール、またはスパムメールに記載されていたURLで、[ウィルス感染やクリック詐欺]の危険性があります。
<http://www.abcdefghijklmn.com>
このままこのサイトにアクセスする場合は[許可する]ボタンを押してください。
許可リストに登録され、次回以降、この画面は表示されなくなります。
拒否すると、拒否リストに追加されます。
[許可する] [拒否する]

[図12]

- (a) 以下のメールを受信しようとしています。
- ☐user100@example.jp
☐user200@example.jp
⇒ local1@exsample.jp
- 送信元アドレスはアドレス帳に登録されていないため、受信できていません。
受信を許可する場合は[許可する]ボタンを押してください。
許可したメールアドレスは宛先許可リストに追加され、次回以降、この画面は表示されなくなります。
拒否すると宛先拒否リストに追加されます。
- [許可する] [拒否する]
- (b) 以下のメールを送信しようとしています。
- local1@example.jp⇒
☐user100@example.jp
☐user200@example.jp
- 宛先アドレスはアドレス帳に登録されていないため、送信されていません。
送信を許可する場合は許可するメールアドレスのチェックボックスをチェックして
[許可する]ボタンを押してください。
許可したメールアドレスは宛先許可リストに追加され、次回以降、この画面は表示
されなくなります。
拒否すると宛先拒否リストに追加されます。
- [許可する] [拒否する]

[図13]

以下のURLにアクセスしようとしています。

このURLは「local1@example.jp」が受信したウィルス感染したメール、またはスパム
メールに記載されていたURLで、【ウィルス感染やクリック詐欺】の危険性があります。

<http://www.abcdefghijklmn.com>

また、以下のメールも受信しようとしています。

☐user100@example.jp
☐user200@example.jp
...
⇒ local1@example.jp

送信元アドレスはアドレス帳に登録されていないため、受信できていません。
受信を許可する場合は[許可する]ボタンを押してください。
許可したメールアドレスは宛先許可リストに追加され、次回以降、この画面は
表示されなくなります。
拒否すると宛先拒否リストに追加されます。

[許可する] [拒否する]

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2014/062672

A. CLASSIFICATION OF SUBJECT MATTER

G06F13/00(2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F13/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2014
Kokai Jitsuyo Shinan Koho	1971-2014	Toroku Jitsuyo Shinan Koho	1994-2014

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	JP 2008-276760 A (Canon Electronics Inc.), 13 November 2008 (13.11.2008), paragraphs [0100] to [0127]; fig. 24 & US 2008/0244070 A1	1, 6 2-5
Y A	JP 2007-226608 A (KDDI Corp.), 06 September 2007 (06.09.2007), paragraphs [0019] to [0038] (Family: none)	1, 6 2-5
A	JP 2009-124194 A (Kabushiki Kaisha Interlink), 04 June 2009 (04.06.2009), paragraphs [0033] to [0040], [0048] to [0050] (Family: none)	2-5

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
29 July, 2014 (29.07.14)

Date of mailing of the international search report
05 August, 2014 (05.08.14)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

A. 発明の属する分野の分類（国際特許分類（I P C））

Int.Cl. G06F13/00(2006.01)i

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（I P C））

Int.Cl. G06F13/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1 9 2 2 - 1 9 9 6 年
日本国公開実用新案公報	1 9 7 1 - 2 0 1 4 年
日本国実用新案登録公報	1 9 9 6 - 2 0 1 4 年
日本国登録実用新案公報	1 9 9 4 - 2 0 1 4 年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
Y A	JP 2008-276760 A (キヤノン電子株式会社) 2008. 11. 13, 段落【0100】 - 【0127】, 【図 24】 & US 2008/0244070 A1	1, 6 2-5
Y A	JP 2007-226608 A (K D D I 株式会社) 2007. 09. 06, 段落【0019】 - 【0038】 (ファミリーなし)	1, 6 2-5
A	JP 2009-124194 A (株式会社インターリンク) 2009. 06. 04, 段落 【0033】 - 【0040】, 【0048】 - 【0050】 (ファミリーなし)	2-5

☐ C 欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の 1 以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日

2 9 . 0 7 . 2 0 1 4

国際調査報告の発送日

0 5 . 0 8 . 2 0 1 4

国際調査機関の名称及びあて先

日本国特許庁（I S A / J P）
郵便番号 1 0 0 - 8 9 1 5
東京都千代田区霞が関三丁目 4 番 3 号

特許庁審査官（権限のある職員）

小林 義晴

5 T

9 5 7 2

電話番号 0 3 - 3 5 8 1 - 1 1 0 1 内線 3 5 6 8