(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2005-535967
(P2005-535967A)
(43)公表日　平成17年11月24日(2005.11.24)

(51)Int.Cl.[7]	F I	テーマコード（参考）
G06F 13/00	G06F 13/00 610Q	

審査請求 未請求　予備審査請求 未請求　（全 26 頁）

(21)出願番号	特願2004-528000 (P2004-528000)
(86)(22)出願日	平成15年8月11日 (2003.8.11)
(85)翻訳文提出日	平成17年4月8日 (2005.4.8)
(86)国際出願番号	PCT/US2003/025067
(87)国際公開番号	WO2004/015583
(87)国際公開日	平成16年2月19日 (2004.2.19)
(31)優先権主張番号	60/402,574
(32)優先日	平成14年8月9日 (2002.8.9)
(33)優先権主張国	米国 (US)

(71)出願人　505050197
バーリントン　コミュニケーションズ　インコーポレイテッド
アメリカ合衆国　０１８０３　マサチューセッツ、バーリントン、マウンテン　ロード　５６
(74)代理人　100067817
弁理士　倉内　基弘
(74)代理人　100085774
弁理士　風間　弘志
(74)代理人　100126527
弁理士　遠藤　朱砂
(74)代理人　100130465
弁理士　吉田　匠

最終頁に続く

(54)【発明の名称】電子メッセージ受信者へのアクセスを制御するためのシステム及び方法

(57)【要約】
本発明は、電子メールやインスタントメッセージ等の電子通信媒体において、特定のオリジネーターのアイデンティティー（または、オリジネーターの識別）に制御されたアクセスを与えるための手段としてオリジネーターのアイデンティティーに複数のプロキシアイデンティティー（または、代理の識別）を生成するためのシステム及び方法に関する。

【特許請求の範囲】
【請求項１】
電子通信ネットワークに接続されたユーザーへのアクセスを選択的に許可または拒絶するための方法であって、前記ユーザーが関連する受信者の識別子を有し：
Ａ．前記ユーザーに関連した複数のプロキシ識別子を生成することであって、前記プロキシ識別子の各々が少なくとも３つの関連するセキュリティー状態を有し、前記状態の第１の状態が前記ネットワークに接続したパーティーが前記ユーザーにアクセスすることを許可することを示し、前記状態の第２の状態が前記ネットワークに接続したパーティーが前記ユーザーにアクセスすることを拒絶することを示し、さらに、前記状態の第３の状態が、予め決められた基準が満たされた場合に、前記ネットワークに接続したパーティーのうちの少なくとも１つのパーティーであって、全てのパーティーより少ないパーティーが前記ユーザーに条件付でアクセスすることを許可することを示し、基準が満たされていない場合にアクセスを拒絶すること；
Ｂ．インバウンドメッセージの前記送信者に関連付けられた前記送信者の識別子及び受信者の識別子を含む前記ネットワークからの前記インバウンドメッセージへの応答で、前記インバウンドメッセージを前記プロキシ識別子の１つに関連付けられた場所に伝送すること；
Ｃ．前記伝送されたインバウンドメッセージに関連したセキュリティー状態であって、前記送信者の識別子及び前記受信者の識別子に関連付けられているセキュリティー状態を評価するために前記インバウンドメッセージを処理すること；及び、
Ｄ．前記セキュリティー状態が前記１つのプロキシ識別子の前記セキュリティー状態に少なくとも部分的に関連した、１つまたは複数の予め決められた基準を満たすとき、前記伝送されたメッセージの前記ユーザーへのアクセスを許可し、その他の場合に、前記伝送されたメッセージの前記ユーザーへのアクセスを拒絶することを含む方法。
【請求項２】
前記識別子が電子メールアドレスである、請求項１に記載の方法。
【請求項３】
電子通信ネットワークに接続されたユーザーへのアクセスを選択的に許可または拒絶するためのシステムであって、前記ユーザーが関連する受信者の識別子を有し：
Ａ．前記ユーザーに関連した複数のプロキシ識別子を生成する生成器であって、前記プロキシ識別子の各々が少なくとも３つの関連するセキュリティー状態を有し、前記状態の第１の状態が前記ネットワークに接続したパーティーが前記ユーザーにアクセスすることを許可することを示し、前記状態の第２の状態が前記ネットワークに接続したパーティーが前記ユーザーにアクセスすることを拒絶することを示し、さらに、前記状態の第３の状態が、予め決められた基準が満たされた場合に、前記ネットワークに接続したパーティーのうちの少なくとも１つのパーティーであって、全てのパーティーより少ないパーティーが前記ユーザーに条件付でアクセスすることを許可することを示し、基準が満たされていない場合にアクセスを拒絶する生成器；
Ｂ．インバウンドメッセージの前記送信者に関連付けられた前記送信者の識別子及び受信者の識別子を含む前記ネットワークからの前記インバウンドメッセージへの応答で、前記インバウンドメッセージを前記プロキシ識別子の１つに関連付けられた場所に伝送するメッセージ伝送器；
Ｃ．前記送信者の識別子及び前記受信者の識別子に関連付けられている前記セキュリティー状態を評価するためのプロセッサー；及び、
Ｄ．前記セキュリティー状態が前記１つのプロキシ識別子の前記セキュリティー状態に少なくとも部分的に関連した、１つまたは複数の予め決められた基準を満たすとき、前記伝送されたメッセージの前記ユーザーへのアクセスを許可し、その他の場合に、前記伝送されたメッセージの前記ユーザーへのアクセスを拒絶するゲートを備えるシステム。
【請求項４】
前記識別子が電子メールアドレスである、請求項３に記載のシステム。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は概略的にコンピューターネットワークに関し、詳細に述べると、送信者及び受信者の識別子を使用して参加者の間でメッセージが交換される、（「電子メール」、「インスタントメッセージ」等の）電子通信の形式に対するアクセス制御を制御するためのシステム及び方法に関する。
【背景技術】
【０００２】
電子メールの最大の長所は、電子メールメッセージの内容及び伝達を定義する標準的なプロトコルの全世界的な使用である。しかしながら、これらの標準プロトコルは送信者のアイデンティティー（または、身元）を認証しないので、電子メール上のアクセス制御を困難な課題にしている。最近、電子メール上のアクセス制御の不十分さは商業的または他の望まれないメッセージ（スパム（spam）（すなわち、商業上または他の理由により一方的に送られて来る電子メール））の量を劇的に増大させている。
【０００３】
ここ十年間の間に、電子メールの受信箱へのアクセスを制御するためのソフトウェアシステムを作製するための試みが何百となされている。
【０００４】
本願が出願された時点において、既存の対スパム技術は、将来、スパムが媒体を使用不可能にするだろうと予測されてしまう程度に、電子メールのスパム問題を解決することに失敗していると考えられている。
【０００５】
最も一般的な手法は「スパムフィルタリング」と呼ばれている手法である。スパムフィルターはメッセージの内容、送信者のアイデンティティー（または、身元情報）、または他の特徴の評価に基づいて、メッセージが望まれているものかどうかを決定することを試みる。
【０００６】
【特許文献１】米国特許第５９３０４７９号明細書
【特許文献２】米国特許第６５９１２９１号明細書
【発明の開示】
【発明が解決しようとする課題】
【０００７】
これらのフィルター技術は１つまたは複数の共通した欠点を有する。フィルターは度々、スパムメッセージの識別に失敗し、それらの伝達を許可したり、あるいは、正当なメッセージをスパムとして識別（「偽陽性」）したりする。多くのスパムを誤って識別することだけでも重大な問題であるが、正当なメッセージを阻止してしまうことは多くのユーザーにとって、特に、阻止されたメッセージが重要である可能性がある仕事上の使用において許容し難いことである。
【０００８】
フィルターがスパムを識別するために依存している特性（例えば、送信者のアイデンティティー、題目、メッセージの内容）は送信者の制御下に置かれているので、フィルターは容易に迂回されてしまう。
【０００９】
ルールに基づくフィルターはユーザー及び管理者による継続的なルールのメンテナンスを必要とする。フィルターは、全てのメッセージを全てのルールに対して処理することを必要するので計算量的な面から見て不経済であり、メッセージの伝達の待ち時間の増加につながる。
【００１０】
電子通信上のアクセスを制限するための第２の手法は認可された情報源以外の全てのア

クセスを拒絶することであり、「ホワイトリスティング（white listing）」と呼ばれる。これはシステムが招待したメッセージだけが到達することを許可する。

【００１１】

メッセージがホワイトリストで保護されている電子メールアドレスに送信された場合、送信者のアイデンティティーがホワイトリストに掲載されている場合のみメッセージが伝達される。ホワイトリスト上に存在しない送信者からのメッセージは拒絶されるか、疑わしいスパムとして検疫されるか、または、一般的に、挑戦される（または、課題を提示される）。各々の拒絶動作は正当な通信に対して固有の悪化状態及び混乱状態をもたらす。

【００１２】

多くのスパムの送信者は受信メッセージを受信したがらないので、メッセージベースの挑戦（または、課題の提示）は多くの場合、正当なメッセージの送信者のみに到達するので、ホワイトリスティングは上手く作用する。

【００１３】

基礎をなしている電子メールのプロトコルに対する変更は救済とならない。（ＲＦＣ電子メール標準を規定及びサポートする機関である）ＩＥＴＦは１９９９年にＥＳＭＴＰと呼ばれる標準電子メール通信に対する認証用の拡張を規定している。しかしながら、ＥＳＭＴＰが４年以上存在するにもかかわらず、送信者によるＥＳＭＴＰの使用の要求は世界的な非認証標準（ＳＭＴＰ）で送られる大部分のメッセージを拒絶することとなるので、ほとんどの電子メールのホストまたは管理者はＥＳＭＴＰの要求をしていない。すなわち、全ての人がＥＳＭＴＰ標準に移行するまで誰もＥＳＭＴＰに移行しないので、結果的に、ＳＭＴＰの連続的かつ永続的な依存が続いている。

【００１４】

電子メールに（ペイパー式の（すなわち、メールの数に依存して料金を払う）電子メール及び保税式の電子メール等の）金銭上の制御システムを与えようとする、または、（メッセージのヘッダーの商標化された財産等の）法的な知的財産から引き出そうとする商業上の画策は多くのユーザーには許容できない程度の煩雑な設定及びサポートを必要とする。

【課題を解決するための手段】

【００１５】

本発明に達するための重要な考え方は、単一の集合として混合されたときに、所望されるメッセージを所望されないメッセージから分離することは、不可能でないにしても非常に困難であるということを認めることである。このような分離を試みる多様な試みは正当なメッセージを阻止せずにスパムに対する完全な保護を与えることができないでいる。

【００１６】

この問題の解決は、同一の集合に所望されるメッセージと所望されないメッセージが混合されることを防止する、ユーザーまたは企業によって一方的に採用することができるシステム及び方法に存在する。

【００１７】

本発明（「本製品」）は、保護された元の識別子（「オリジネーター（originator）」）の代理として作用する複数のプロキシ識別子（「プロキシ」）の確立及び管理を介して、（「電子メール」、「インスタントメッセージ」等の）送信者及び受信者の識別子を使用して参加者の間でメッセージが交換される電子通信の形式のアクセスを制御するためのシステム及び方法であって、前記プロキシの各々がオリジネーターとの通信（「接触」）のために依存しているメッセージの共同体の一部に対応するアクセスの権利を規定する別個のセキュリティー状態を持つシステム及び方法を提供する。

【００１８】

本発明の全ての実施例において、少なくとも３つのセキュリティー状態が存在し、多くの実施例において４つ以上のセキュリティー状態が存在する。セキュリティー状態は、（電子メールアドレス等の）プロキシ識別子がメッセージの伝達中にディスティネーション識別子へのアクセスに制限的であり、生成され、メッセージのソース識別子への参照のた

めに代用される方法を制御する。

【００１９】

本発明の１つの実施例において、システムは集合的に、互いに相互作用し、結果として別個のセキュリティー状態及び対応する挙動のマトリクスの結果となる複数の（すなわち、４つ以上の）セキュリティー設定をサポートする。この実施例におけるセキュリティー状態の多様性は、例えばアクセスが許可か不許可である二者択一的なシステムに比べ、より正確であるシステムの挙動を与える。この実施例及び他の実施例において、ユーザーの特定の共同体は、メッセージが同一のディスティネーション識別子に送信された場合であっても、他のユーザーが許可されないアクセスを許可されることができる。アクセス制御に対して、メッセージは多様な変化とともに拒絶、挑戦、検疫、または容認されることができる。

【００２０】

本発明の１つの実施例において、プロキシ電子メールアドレスはメッセージがシステムを介して処理されるときに本製品によって自動的に生成及び割り当てられる、企業または個人ユーザーによって明確に生成及び割り当てられる、または、ソース電子メールアドレス及び初期のセキュリティー状態を予め決定する名前付け協定（naming convention）に従った暗黙的に生成される等を含む、多様な様式で規定されてもよい。

【００２１】

本発明の１つの実施例において、プロキシ電子メールアドレスへの参照はセキュリティー状態に依存して、対応するソースアドレスに変換されてもよいし、変換されなくてもよい。例えば、本製品によって自動的に生成されたプロキシ識別子への参照はメッセージを通して、ソース識別子によって交換されてもよい。明確に生成された、または名前付け協定を介して規定された（従って、ユーザーに既知である）プロキシアドレスはソース識別子によって交換されなくてもよい。

【発明の効果】

【００２２】

本発明の主要な効果は、所望されないメッセージが本発明のリフレクション（Reflection）システムによって保護されている識別子に伝達されることを優れた正確さで防止できることである。

【００２３】

本発明のリフレクションシステムは電子メールをフィルタリングしないので、リフレクションがインバウンドトラフィック（すなわち、外部の送信者からのトラフィック）のＳＭＴＰ受信中にメッセージを拒絶するときに、物理的なバンド幅（及び、それに関連する費用）が節約される。

【００２４】

また、本発明のリフレクションは「偽陽性」の欠点を有さない。セキュリティーモデルは首尾一貫したもので、常に、ユーザーまたはホストの組織の制御下に置かれる。

【００２５】

本発明のリフレクションはまた、格納するスパムの数が少なくてすむので、電子メールのためにかかる費用を節約することができる。

【００２６】

リフレクションは電子通信で頻繁に起きているが、発見することが難しい問題を除去することができる。例えば、電子メールにおいて、リフレクションはパーティー間の電子メールアドレスの共有を検出し、また、誰かが企業のインフラストラクチャーを介して送信することなく、企業の電子メールアドレスを使用してメールを作成している（それによって、配置されているセキュリティー及び制御を迂回している）ことを検出することができる。

【発明を実施するための最良の形態】

【００２７】

本製品は３つのシステムを備える。

１．リフレクション（Reflection）メールサーバー（ＲＭＳ）
２．管理用ウェブサイト（ＡＷＳ）
３．データベースサーバー
これら３つのシステムは単一のサーバーに存在してもよいし、複数のサーバー上に多様な構成で存在してもよい。

【００２８】

リフレクション（Reflection）メールサーバーについて

本発明は、オリジネーター（originator）からの及びオリジネーターへの全ての外部のメッセージが本製品を通過することを要件とする。オリジネーター（または、保護されている元の識別子）から外部の受信者（「接触者」）へのメッセージは以下の説明において「アウトバウンドメッセージ」と呼ぶ。また、外部の送信者（「接触者」）からオリジネーターへのメッセージを「インバウンドメッセージ」と呼ぶ。

【００２９】

リフレクションメールサーバー（「ＲＭＳ」）は、セキュリティーモジュールが処理するまでインバウンドトラフィックメッセージが存在する１つのキュー（「処理前キュー」）、及び処理されたメッセージ及び戻りメッセージが最終的な伝達まで配置される第２のキュー（「伝達キュー」）の２つの格納キューを利用する。

【００３０】

ＳＭＴＰ伝達のトランスポートエンベロープ（または、伝送用封筒）に明記された送信者及び受信者の電子メールアドレスはセキュリティーモジュールにとって重要部分である。セキュリティーモジュールは後で説明される、相互作用するセキュリティー状態に基づいてメッセージが目的の受信者に伝達されるべきかを決定する。正当な理由がある場合、多様なエラーメッセージ及びウォーニングを送信者に送り返すことができる。

【００３１】

送信されたメッセージは通常、ユーザーの本製品への主要なインターフェースとして作用する多形ブラウザーインターフェース（polymorphic browser interface）である、リフレクションウイザード（Reflection Wizard）へのリンクとともに、ＲＭＳによってメッセージの最下部に取り付けられるフッターを有する。

【００３２】

リフレクションメールサーバーはまた、本発明の中心的なセキュリティー機構であるプロキシ識別子の配列の生成及び使用を管理する。

【００３３】

プロキシアドレス

各接触者には１つまたは複数のプロキシアドレスが割り当てられ、それらの各々はＰＦＣに準拠した電子メールアドレス（すなわち、最も一般的なBST99 1364948-1.065113.0011電子メールプロトコルの名前付け協定に準拠したアドレス（電子メールプロトコルの詳細はhttp://www.ietf.org/rfx.htmlを参照））である。本出願において「プロキシ識別子」は「プロキシアドレス」と同義である。

【００３４】

各接触者にはＲＭＳを通過するメッセージの送信者または受信者として、第１参照にそれ自体のプロキシアドレスが割り当てられる。本製品は各セキュリティーコードにプロパティーとして格納されている、企業及びユーザーの選択、及びデフォルトに基づいてインフラストラクチャーへのアクセスを制御する。

【００３５】

以下はオリジネーターから外部接触者へのメッセージである。
１．アウトバウンドメッセージはホスト組織の既存の電子メールインフラストラクチャーを介して処理され、本発明を実施している本製品に到達する。
２．本製品は接触者による使用のために登録されている、固有のプロキシアドレスを自動的に割り当て、記録する。プロキシアドレスが接触者に予め割り当てられている場合、それが再利用される。

３．アウトバウンドメッセージのヘッダー及び本文内のオリジネーターのアドレスへの全ての参照は対応するプロキシアドレスに変更される。例えば、オリジネーターのアドレスからのメッセージ「From:ssmith@companv.com」が外部の接触者に送信されるとする。メッセージが本製品を通過するとき、オリジネーターのアドレスssmith@company.comへの全ての参照は、この例において「From:ssmith.123@company.com」である、受信者に対応するプロキシアドレスに変更される。メッセージが接触者の受信箱に到達したとき、メッセージはアドレスssmith@company.comではなく、アドレスssmith.123@company.com（「123」に注意）から発信されたような様相を示す。この例において、プロキシアドレスはオリジネーターのアイデンティティーに個人化されたままである。すなわち、ローカルな部分「ssmith」を有し、ドメインは「company.com」のままである。他の実施例においては、プロキシアドレスはオリジネーターアドレスから判読可能な由来を含まなくでもよい。
４．オリジネーターのアドレスの参照がプロキシアドレスに代えられた後、メッセージは他の影響を受けていない電子メールメッセージと同様に伝達される。

【００３６】

以下はプロキシアドレスを介して外部の接触者からオリジネーターに送り返されたメッセージである。
１．アウトバウンドメッセージは外部の接触者によってプロキシアドレスに送られ、それは最終的にＲＭＳに到達する。
２．ＲＭＳのセキュリティーモジュールは関連するアドレスのセキュリティー状態に基づいて、（制限ではないが）以下のものを含むメッセージに対する伝達の処置を決定する。
ａ．メッセージ伝達の拒絶、メッセージは送信者に何の依頼もしない。処理の終了。
ｂ．メッセージ伝達の拒絶、メッセージが送信者に新規のプロキシを提供。処理の終了。
ｃ．メッセージ伝達の認可、メッセージは「疑わしい」として示される。３へ進む。
ｄ．メッセージ伝達を何の問題もなく認可。３へ進む。
３．伝達が認可されたメッセージに対して、インバウンドメッセージのヘッダー及び本文のプロキシアドレスへの全ての参照が対応するオリジネーターのアドレスに変更される。例を続けるために、プロキシアドレスへのメッセージは「To:ssmith.123@company.com」であるとする。メッセージが接触者の受信箱に到達したとき、メッセージは外部の接触者からオリジネーターのアドレスssmith@company.comに送信されたような様相を示す。

【００３７】

この様式において、インバウンドメッセージのプロキシアドレスは最終的な伝達で露見しておらず、アクセス制御プロトコルの機構をユーザーに対して透明にする。

【００３８】

ユーザーは他のものに影響を与えずにセキュリティーコードの使用を不能または制限することができる。

【００３９】

セキュリティー設定は電子メールアドレス自体に存在し、それゆえ、送信者が、自分が誰であると名乗るかに関わらず、または、メッセージに何を載せたかに関わらず、アドレス自体は一度不能にされると作用しなくなるので、アクセス制御を回避することは困難である。

【００４０】

管理用ウェブサイトについて

管理用ウェブサイト（「ＡＷＳ」）はプロキシの配列、セキュリティー設定、及びトラフィックの履歴に完全な制御及び完全に露呈しているインターフェースを与える。

【００４１】

ＡＷＳは３層構造で構築されている。
１．Ｊａｖａサーバーページ及びサーブレット（Servlet）
２．データベースサーバー
３．アプリケーションサーバー

【００４２】

サーバーページはアプリケーションインターフェース、更新、及びデータベースサーバーからの要求データを定義し、アプリケーションサーバーによってユーザーのブラウザーで利用される結果のページ及びフォームを構築する。

【００４３】

サーバーページ及びサーブレットによって定義されたインターフェース内には、複数のアプリケーション特定のオブジェクトが存在する。

【００４４】

ユーザー

ＡＷＳ全体へのアクセスはユーザーの資格証明書（credential）の正当な認証を必要とする。好まれる実施例において、ＡＷＳはユーザーＩＤ及び対応するパスワードを使用した、正当なログインを必要とする。

【００４５】

認証及び資格証明書要求はＡＷＳ内の全てのページで施行される。

【００４６】

ＡＷＳでは、各々異なったアクセス権限を有する３つのレベルのユーザーがサポートされる。

１．スーパー管理者－完全なアクセス権を有し、サーバーの初期設定及び制御法にアクセスすることができるユーザーの唯一の種類。全体的なトラフィックの履歴の詳細及び要約へのアクセス。

２．ドメイングループ管理者（ＤＧＡ）－ドメイングループ自体、ドメイングループのユーザー、及びＤＧＡが割り当てられたドメイングループのトラフィックの履歴への完全なアクセス。

３．ユーザー－ユーザー自体のオプション、プロキシアドレス、及び個人的な履歴へのアクセス。

【００４７】

【表１】

プロパティー	記述
	管理用ウェブサイトへのログイン中に使用される名前または電子メールアドレス。
パスワード	管理用ウェブサイトへのログイン中に使用されるパスワード。
モード	リフレクションはユーザーによる異なった全体的なセキュリティーモードを有する。 1．強制－メッセージが伝達できない場合に送信者に拒絶及び挑戦メッセージが送信される。 2．フラグ－全てのメッセージが受信者に伝達されることを保証する。強制モードにて拒絶または挑戦されるメッセージは「目印（フラグ）」が付けられる（すなわち、メッセージが強制モードにおいて伝達されないことを示す可視可能な指標が与えられる）。 3．通過－受信者へのメッセージがセキュリティーモジュールを迂回し、直接伝達される。 4．リバース－製品の除去に対する準備として、表面上、プロキシアドレスへの依存を排除するために使用される。全てのセキュリティーが停止され、プロキシアドレスへの全てのメッセージは、受信者への将来のメッセージが元のアドレスで送信されることを要求する要求メッセージが送信者に送信 される結果となる。メッセージにはメッセージがプロキシアドレスに送信されたことを示す目印が付けられる。
フッター	メッセージが製品を通過するとき、RMSは各メッセージの最下部にフッターを付ける。各ユーザーには3つの有効なフッターが存在する。 1．標準フッター－リフレクションウィザードに接続する単一のリンクを含む。 2．アドバンスドフッター－標準フッターに含まれない、付加的な情報及びリンクを含む。 3．フッター無し－フッターは要求されない。
メッセージ格納	拒絶または挑戦されたメッセージのコピーを保持するためのオプション。
自動的免除	ユーザーが接触からの、目印の付けられたメッセージに返信したときに、接触を自動的に免除するためのオプション。

【００４８】

サーバー

サーバーオブジェクトは本製品の全体の設置に特定のプロパティー及び方法を含む。サーバーオブジェクトは「スーパー管理者」権限を有するユーザーに対してのみ利用可能である。

【００４９】

プロパティーの大部分は本製品の一般的なメールサーバーとしての挙動に関するものである。

【００５０】

これらはキューの寿命、管理ウェブサイトのＩＰアドレス、データベースのバックアップスケジュール等に対する設定を含む。

【００５１】

ドメイングループ

各リフレクションの架設（または、設置）はいかなる数の組織（または、企業）もサポートすることができる。組織は本製品のドメイングループとして管理される。ドメイングループは管理下にいかなる数のドメインを持つことができ、これらのドメインのアドレスを有するいかなる数のユーザーを持つことができ、また、いかなる数のドメイングループ

管理者（ＤＧＡ）がドメイングループを管理してもよい。

【００５２】

接触者

本発明のリフレクションシステムはユーザーからメッセージを受信した、またはユーザーにメッセージを送信した全ての外部の接触者をカタログに載せる。接触者はセキュリティー設定を有するプロキシアドレス及び、それに登録されている接触者のセキュリティープロフィールの両方である。

【００５３】

【表２】

プロパティー	記述
接触名	接触者のプロキシアドレスが登録される接触者の名前。接触名は接触者からのインバウンドメッセージからパーズされる。
本来アドレス	（ユーザーに割当てられたプロキシアドレスと混同しないための）接触者の電子メールアドレス。
プロキシアドレス	リフレクションプロキシアドレスはRMSによって接触者に割当てられる。
セキュリティー状態	各プロキシアドレスは以下のセキュリティー状態の１つを有す 1．パブリック－このプロキシはいかなる人及び伝達されるいかなるメッセージにも使用され、共有されることができる。 2．保護－「適切」な接触だけがこのプロキシアドレスを使用することができ、不適切な接触は挑戦されるか（強制モード）、または目印が付けられる（フラグモード）。 3．非共有－「適切」な接触だけがこのプロキシアドレスを使用することができ、不適切な接触は挑戦されるか（強制モード）、または目印が付けられる（フラグモード）。 4．不能－このプロキシアドレスには（免除された送信者以外の）いかなるメールも伝達されない。
メッセージ格納	拒絶または挑戦されたメッセージのコピーを保持するためのオプション。
自動的免除	ユーザーが接触からの、目印の付けられたメッセージに返信したときに、接触を自動的に免除するためのオプション。
実行中名前付け（NOTF）	イネーブルにされた場合、新規のプロキシアドレスが、「実行中」に（すなわち、製品との相互作用無しに）接触のプロキシアドレスの派生形であるアドレスに定義される。例えば、接触のプロキシアドレスがproxy@company.comであり、NOTFがオンである場合、ユーザーはproxy.new@company.comの形式の新規のプロキシアドレスを作成することができる。ここで「new」はユーザーが任意に決められる。NOTFプロキシはそれを使用した最初の接触に割り当たれられるだろう。
寿命	プロキシアドレスは期限付きの期間だけ割当てられることができる。プロキシの期限が「切れた」場合、セキュリティー状態は不能に設定される。

【００５４】

免除（exemption）

システムは免除（または、例外）をサポートする。

【００５５】

履歴

本製品は組織（または、企業）に送信された、または組織から送信された各メッセージに対する記述的な情報を記録する。個々のメッセージの履歴項目は履歴要約レポートの全体に統合され、設定可能な時間の長さの間オンライン上に残された後、削減される。

【００５６】

図１－好まれる実施例のアーキテクチャー

本発明のリフレクションメールサーバー（「ＲＭＳ」）はセキュリティーモジュールが処理するまでインバウンドトラフィックメッセージが存在する１つのキュー（「処理前キュー」）１０２、及び処理されたメッセージ及び戻りメッセージが最終的な伝達まで配置される第２のキュー（「伝達キュー」）１０６の２つの電子メールキューを利用する。

【００５７】

（組織（または、企業）１００のメールサーバーまたは外部の接触者１１４のメールサーバーからの）インバウンドメッセージはインバウンドキュー１０２で受信され、格納される。外部ソース１１４からのインバウンドメッセージは本製品のセキュリティーを受ける。

【００５８】

セキュリティーの施行はＳＭＴＰプロトコル１１２を使用して、インバウンドメッセージの受信中に行われる。トランスポートエンベロープ（または、伝送用封筒）の送信者及び受信者のアドレスが受信されるとすぐに、ＳＭＴＰプロトコルハンドラーはリフレクションセキュリティーモジュール１１０に、このメッセージ１１６に対するセキュリティー処置を取得するように要求する。入力されるメッセージの残りの部分の引き続きの処理はリフレクションセキュリティーモジュール１０８から戻されるセキュリティー応答１１８に基づいて行われる。

【００５９】

メッセージを伝達できる場合、それは処理前キュー１０２に置かれる。メッセージが伝達できない場合、延期または拒絶１２０が送信サーバー１１４に送り返される。

【００６０】

延期を受けるメッセージは（通常、３０～６０分の）特定の時間だけ延期される。これは送信サーバー１１４が「正しく挙動している」ことのテストである。スパム（すなわち、商業上または他の理由により一方的に送られて来る電子メール）を送信する多くのサーバーは延期されたメッセージを処理しないので、延期されたメッセージはそのようなソース（または、発信源）から再送信されないだろう。

【００６１】

通常のキュースケジュールを使用することにより、各インバウンドメッセージは本製品のメッセージ変換モジュール１０４によって処理され、それは、・メッセージをそのままの状態で、または、・以下に説明されるように、メッセージを何らかのレベルの付加、変更、または他の変換とともに、伝達キュー１０６に置く。

【００６２】

伝達キュー１０６はインバウンドメッセージを組織（または、企業）の内部電子メールインフラストラクチャー１００、または外部のディスティネーション１１４に伝達するだろう。伝達キューは（ドメイン名サービス（ＤＮＳ）等の）伝達場所を決定するための標準的なディスティネーションルックアップ機構（destination lookup mechanism）を使用するか、または、既知の内部ドメインへのメールを内部電子メールインフラストラクチャー１００に送信し、他のメールをインターネット１１４に送信するルーティング表（routing table）を使用することができる。

【００６３】

図２－インバウンドメッセージの準備

本製品がメールを処理するとき、それはデータベースを新規のアドレス、容量統計値（volume statistic）、及び履歴追跡とともに更新する。図２は好まれる実施例における、インバウンドメッセージの受信中になされる、データベースの準備の詳細を示している。

【００６４】

インバウンドメッセージの準備は特定のメッセージにセキュリティー処置（security disposition）が戻される前に実施される。

【００６５】

入力されるメッセージで試験される最初の内容は、受信者のアドレスがリフレクション

（Reflection）によって保護されているドメインに存在するかどうかである２００。
【００６６】
リフレクションに到達したメッセージがリフレクションによって保護されているドメインのアドレスに送信（「インバウンド」）されるか、またはそのようなアドレスから送信（「アウトバウンド」）されなければならないことに注意することは重要である。ローカルメールはローカルに伝達されなければならず、従って、リフレクションは同一のドメインのアドレスからの、または同一のドメインのアドレスへの電子メールを監視しない。
【００６７】
各々のドメインが単一のリフレクションの架設（または、設置）で管理されている１つの組織（または、企業）から他の組織へメールが送信される可能性がある。この場合、メッセージは最初に第１の組織からのアウトバウンドメッセージとして第１の処理がなされ、そして、第２の組織へのインバウンドメッセージとして処理される。
【００６８】
送信者のアドレスがリフレクションのこの設置によって出くわさない場合（または、見つからない場合）２０２、それはデータベースの「本来アドレス（true address）」表に追加される２０４。
【００６９】
次に、本製品は、受信者のアドレスが発行されたプロキシアドレスであるかどうかを調べるためにデータベースを検索する２０６。
【００７０】
エイリアス（または、別名）が存在しない場合、アドレスは「実行中名前付け（Name-on-the-Fly）」（ＮＯＴＦ）として知られている名前付け協定（naming convention）を介して生成された可能性があり２１０、その場合、プロキシアドレスは名前付け協定から引き出される情報に基づいて生成され、保護されたユーザーに対して登録される２１２。ＮＯＴＦが未知のプロキシアドレスに対して許可されていない場合、メッセージは拒絶される２０８。
【００７１】
この時点で、プロキシアドレスはデータベースに存在する。本製品は履歴システムのためにメッセージの結果の追跡を開始する２２０。
【００７２】
プロキシが代用として利用されているユーザーを見つけるために、好まれる実施例において、最初にユーザーの元のアドレス２１８に、そしてそこからユーザー記録２１６に進む必要がある。他の実施例においては、これは多様な他の手法を使用して達成することもできる。しかしながら、進行するためにはユーザーのアイデンティティー（または、身元情報）を手元に保持しておく必要がある。
【００７３】
プロキシアドレスが特定のユーザーに登録されていない場合２１４、それを現在の送信者に対して登録する２２２。この条件は２つの可能な条件によって発生し得る。第１に、プロキシアドレスはＮＯＴＦを使用して作製され、従って、どのユーザーにも所持されていない。第２に、プロキシアドレスは使用される前に明示的に生成され、最初の使用までどのユーザーにも所持されない。この場合、それはＮＯＴＦのプロキシと同様に、最初のユーザーに登録される２２２。
【００７４】
次に、リフレクションセキュリティーモジュール及びアドレス変換モジュールに情報を与えるために送信者の免除状態（exemption）がチェックされる２２４。免除対象（または、例外対象）となっている送信者はアクセス制御を受けず、免除対象となっている接触者から、または免除対象となっている接触者への全てのメールは保護されたユーザーの元の内部アドレスの下で操作される。
【００７５】
図３－強制的セキュリティー

インバウンドメッセージの準備が完了した後、本発明のリフレクションシステムはそのメッセージに対するセキュリティー処置（security disposition）を決定する。

【００７６】

リフレクションのユーザーには強制モードとフラグモードの２つの動的なセキュリティーモードが利用可能である。

【００７７】

図３は強制モードを利用するユーザーに送信されたメッセージに対する、好まれる実施例のセキュリティーモデルに従った論理を詳細に示している。

【００７８】

定義上、受信者のアドレスが元の内部アドレスから区別不可能である場合であっても、本発明のリフレクションによって保護されるドメインへの全てのインバウンドメールはプロキシ識別子である。元の内部アドレスの各々はセキュリティーが元のアドレス自体に置かれるようにするために、同一のアドレスのプロキシアドレスを有する。

【００７９】

受信者のアドレスのセキュリティー状態は最初に尋問される。

【００８０】

パブリックプロキシへのメッセージ

受信者のプロキシアドレスが「パブリック」のセキュリティー状態を有する場合３００、本製品は送信者の例外状態をチェックする３０２。送信者が免除（または、例外）である場合、セキュリティーは迂回され、メッセージは次のメッセージ変換ステージに送られ、伝達される３３８。

【００８１】

送信者に登録されたプロキシアドレスがこのメッセージに対する受信者のアドレスとして使用されているプロキシアドレスと同一でない場合（このケースは図面に明確に示されていないが、可能性がある）、本製品は伝達を許可する前に送信者のプロキシのセキュリティーセットを試験するだろう。

【００８２】

送信者に割り当てられたプロキシがパブリックであるか３１２、または保護されている場合３２０、メッセージはセキュリティーを介して許可される３３８。送信者に登録されたプロキシが保護されている場合、送信者には今後彼ら自身のプロキシアドレスを使用するようにリマインダーメッセージが送信される３２２。

【００８３】

送信者のプロキシが「非共有」である場合３２８、メッセージは伝達することが許可されない。その代わりに、送信者には、（このメッセージの受信者として使用されるプロキシとは対照的に）送信者に登録されたプロキシアドレスを使用してメッセージを再送信する要求が送り返される。

【００８４】

それゆえ、メッセージがパブリックプロキシアドレスに送信された場合であっても、送信者のプロキシアドレスのセキュリティー状態はメッセージの伝達を変更または禁止することができる。

【００８５】

保護されたプロキシへのメッセージ

受信者のプロキシアドレスが「保護される」のセキュリティー状態を有する場合３０４、送信者がこのプロキシアドレスにメールを送信することを許可されているかを調べるためのチェックがなされる。

【００８６】

現在、送信者が保護されたプロキシを使用することができる３つの方法が存在する。第１に、送信者が免除対象である場合３１４、セキュリティーが迂回され、メッセージは次のメッセージ変換ステージに送られ、伝達される３３８。第２に、送信者がプロキシアドレスに登録されているパーティー（または、グループ）である場合３２４、伝達は認証さ

れ、完了する３３８。最後に、送信者がプロキシアドレスに登録されている接触者と同一のドメインの送信者であり、ドメインがＡＯＬ、Ｙａｈｏｏ、Ｈｏｔｍａｉｌ等の大規模なＩＳＰでなく、ドメインレベルの共有を許可するセキュリティーのプロパティーがプロキシに対してイネーブル状態である場合３３２、メッセージは伝達のために認証される３３８。

【００８７】

保護されているプロキシを使用することが認証されていない送信者には、送信者による使用が許可されているプロキシアドレスにメッセージを再送信するように要求が送信される３１６。このメッセージは本質的に、「プロキシアドレスｘは送信者のプロキシアドレスｙに変更されました。あなたのメッセージをｙに再送信して下さい」と記載する。

【００８８】

保護されたアドレスは有効なリターンアドレスを有さないスパムに対する保護を与え、かつ、正当な接触者に対してメッセージの伝達を可能にする再送信機構を与えるために使用される。

【００８９】

非共有プロキシへのメッセージ

受信者のプロキシアドレスが「非共有」のセキュリティー状態を有する場合３０６、送信者がこのプロキシアドレスにメールを送信することを許可されているかを調べるためのチェックがなされる。

【００９０】

現在、送信者が保護されたプロキシを使用することができる３つの方法が存在する。第１に、送信者が免除対象である場合３１４、セキュリティーが迂回され、メッセージは次のメッセージ変換ステージに送られ、伝達される３３８。第２に、送信者がプロキシアドレスに登録されているパーティーである場合３２４、伝達は認証され、完了する３３８。最後に、送信者がプロキシアドレスに登録されている接触者と同一のドメインの送信者であり、ドメインがＡＯＬ、Ｙａｈｏｏ、Ｈｏｔｍａｉｌ等の大規模なＩＳＰでなく、ドメインレベルの共有を許可するセキュリティーのプロパティーがプロキシに対してイネーブル状態である場合３３２、メッセージは伝達のために認証される３３８。

【００９１】

保護されたプロキシを使用することが認証されていない送信者には、メッセージの再送信に対する依頼を与えない、伝達メッセージの拒絶が送信される３１６。保護されたアドレスの認証されていない使用と非共有アドレスの認証されていない使用との間の差は、保護されたプロキシの拒絶が正当なメッセージの再送信のための手段を与えるのに対し、非共有の拒絶がそれを与えないことである。

【００９２】

非共有プロキシの場合、正当に電子メールを送信するための要件は、単に受信者のアドレスを知ることではなく、受信者及び、プロキシに登録されている対応する送信者のアドレスを知ることである。非共有のプロキシはセキュリティーを重視している組織（または、企業）に、「ディレクトリーハーベスト攻撃（directory harvest attack）」として知られる攻撃に対して非常に有効でかつ軽快な保護を与える。ディレクトリーハーベスト攻撃は目的とするドメインに膨大な数の異なったアドレスにメッセージを送信することによって有効な電子メールアドレスを収集するために使用される技術である。この攻撃において、「該当するユーザー無し」という結果にならないアドレスは有効であると仮定される。

【００９３】

非共有プロキシにより、ディレクトリーハーベスト攻撃は、送信者が各試みにて送信者の正確なアドレスをかつぐ（または、だましとる）方法を知らない限り、失敗に終わるだろう。

【００９４】

無効化されたプロキシへのメッセージ

受信者のプロキシアドレスが「無効」のセキュリティー状態を有する場合３０８、送信者が免除対象であるかを調べるためのチェックがなされる。すなわち、ユーザーが強制セキュリティーモードを利用している場合、免除対象となっていることが無効化されたプロキシへメッセージが伝達されるための唯一の方法である。

【００９５】

図４－フラグセキュリティー

図４はフラグモード（Flag Mode）を利用するユーザーに送信されたメッセージに対する、好まれる実施例のセキュリティーモデルに従った論理を詳細に示している。

【００９６】

フラグモードは、全てのインバウンドメッセージがユーザーの受信箱に伝達されることを保証する。

【００９７】

図４の論理は図３とともに記述されたものとほとんど同一であり、唯一の本質的な差異は、フラグモードにおいては、送信者が受信者のプロキシにメッセージを送信することが認証されていないと決定されたときに、強制モードのように拒絶または再送信のためのメッセージを送信するのではなく、送信者がこのメッセージを選択されたプロキシアドレスに送信することを認証されていないことを示すためのプレフィックス（または、接頭語）で題目行（または、件名の行）に目印（または、フラグ）を付けることである４２２／４２６。

【００９８】

題目へのマーク付けがホストの組織内のみで可視可能であり、目印を付けられたメッセージの組織外への返信において、リフレクションシステムが目印を除去することに注意することは重要である。

【００９９】

フラグモードは以下の３つの重要な本製品の要求のために作用する。

１．新規のユーザーに本発明のリフレクションシステムの使用に対してスムーズな移行のための動作モードを与え、外部の接触者がリフレクションシステムによって悪化しないことを保証する（「移行」）。既存のスパム問題は新規のユーザーの移行期間中に解決される。

２．正当であるが予期できないメッセージの阻止を許容できないユーザーに対し、全てのメールがユーザーの受信箱に伝達されることを保証する。フラグモードは、大量な名刺が交換され、予期されないメッセージの価値及び頻度が高い、販売、マーケット開発、または重役等の人員に対して理想的である。

３．電子メールの挙動を変更しない、またはできないユーザーは本製品を永続的にフラグモードで動作させるだろう。これらのユーザー（または、管理者）はプロキシアドレスの使用を一切禁止することができ、スパムに対する軽減を受けながら、ユーザーが通常どおりに、彼らの唯一のアドレスを使用し続けることを可能にする。

【０１００】

既に存在するスパム問題をどのように止めるか

既に存在するスパム問題を抱えている、本製品を使用し始めた新規のユーザーは以下の方法により、既存のアドレスにスパムが送信されることを止めることができる。

１．セキュリティーの施行の全体をフラグモードに初期設定する。

２．免除方法の多様な実施例のどれかを使用して全ての既知の接触者を免除対象にする。接触者の免除は元の内部アドレスに既に依存している正当な接触者が影響を受けずにそれの使用を続けることを可能にする。

３．元の内部アドレスと同じアドレスを有するプロキシ上のセキュリティーを増強する。これは、接触者が免除リストに存在しない限り、そのプロキシに送信されたメールに目印（または、フラグ）を付けることを生じさせる。これは、スパムの阻止に対して非常に効果的であるが、特に仕事上等の、広範囲の適用に対して制限があるという欠点を有する一般的な技術である「ホワイトリスティング（white listing）」の非攻撃的な形式である

。
【０１０１】
本発明のリフレクションはこのホワイトリストを既に存在するスパム問題に対してのみ利用する。新規のユーザーがスパム問題を抱えていない場合、ホワイトリストは必要でない。
【０１０２】
図５－アドレス変換
インバウンドメッセージが伝達に対して正確に通過した後、プロキシアドレスへの大部分の参照は対応する元の内部アドレスに変換される。好まれる実施例において、プロキシアドレス、特に実行中名前付け（Name-on-the-Fly）プロキシアドレスの変換を禁止するいくつかのセキュリティー状態が存在する。
【０１０３】
ＮＯＴＦプロキシ（実行中名前付け（Name-on-the-Fly）プロキシ）はユーザーによって定義され、ユーザーの名前空間（name space）に存在する。しばしば、ＮＯＴＦプロキシアドレスはログインシーケンスまたはＮＯＴＦプロキシアドレスによって調節される他の処理で使用される。（既存の電子メールインフラストラクチャー内のメッセージの伝達を確実にするために変換されなければならない、メッセージのヘッダーとは対照的に）電子メールメッセージの本文内のＮＯＴＦの変換を禁止することによって、ＮＯＴＦプロキシの使用を明記する確認メッセージが正確になるだろう。（すなわち、変換は情報を不正確にする。）
【０１０４】
アドレス変換を考慮するとき、個々のリフレクションシステムの架設（または、設置）によって保護されるドメインのプロキシアドレスだけが変換の候補であることを理解しなければならない。保護されてないドメインのアドレスは変換されない。
【０１０５】
リフレクションはデータベース内に「本来の」アドレスのカタログを保持する。保護されているドメインの外部アドレス及び元の内部アドレスは両方とも、本来アドレスカタログに格納される５００。プロキシアドレスはプロキシアドレス自体（例えば、proxy.123@company.com）をキーとして検索することによって、または、元の内部アドレスの代用の使用に対する外部の接触者に割り当てられたプロキシを検索することによって見つけ出される５０２。
【０１０６】
送信者及び受信者の本来のアドレスを考えると、対応するプロキシはアウトバウンドメッセージから検索されることができ、元の内部アドレスへの全ての参照に対してメッセージ内で代用される。プロキシアドレスを考えると、対応する元の内部アドレスはインバウンドメッセージから検索されることができ、プロキシアドレスへの全ての参照に対してメッセージ内で代用される。
【０１０７】
本製品がインバウンド及びアウトバウンドの両方のメッセージに対して、（存在するかどうかわからないが、必要に応じて生成される）同僚のプロキシアドレスも変換する場合、アドレス変換はより複雑になる。
【０１０８】
免除接触者へのまたは免除接触者からの電子メールは禁止されたアドレス変換の結果となるので、免除状態は付加的なレベルの複雑さを招く。
【０１０９】
付加的に、いくつかの外部接触者はサードパーティープロキシに依存し、それゆえ、これらの接触者へのメッセージは予期されるプロキシの使用の連続性を維持すべきである（すなわち、ユーザーからその接触者への全てのメッセージにおいて同一の接触者には同一のプロキシが与えられる）。
【０１１０】

図５を理解するために、文法に対する理解を深めることは非常に重要である。

【０１１１】

５０４は「何らかのアドレス「ａ」を受け取り、それに対する正確な変換を戻す変換方法」として読まれる。

【０１１２】

５０６は「外部の接触者が見ることを予期するプロキシアドレス（それは必ずしも接触者に割り当てられたプロキシアドレスと同一ではない）を戻す方法」として読まれる。

【図面の簡単な説明】

【０１１３】

【図１】本発明の好まれる実施例のアーキテクチャーの高レベルのブロック図である。

【図２】好まれる実施例において、セキュリティーモジュールの実施の前に、データベースが電子メールのトラフィックによってどのように利用されるか、及び、他の事前のステップを図示するフローチャートである。

【図３】本製品が強制モードで動作したときの、好まれる実施例のセキュリティーモジュールの論理及び挙動を図示するフローチャートである。

【図４】本製品がフラグモードで動作したときの、好まれる実施例のセキュリティーモジュールの論理及び挙動を図示するフローチャートである。

【図５】メッセージの内容（すなわち、だれが、どのプロキシを使用して、だれにメッセージを送信したか）、及び多様なセキュリティー設定に依存した、多様なアドレス変換を記述する公式の表である。

【図６】

【図７】ログインページ。

【図８】接触者リスト。

【図９】接触者の詳細のページ

【図１０】リフレクションユーザーオプションページ。

【図１１】管理者がグローバルな免除を追加するページ。

【図１２】管理者が新規ユーザーを作成するページ。

【符号の説明】

【０１１４】

１００　組織の内部電子メールインフラストラクチャー

１０２　処理前キュー

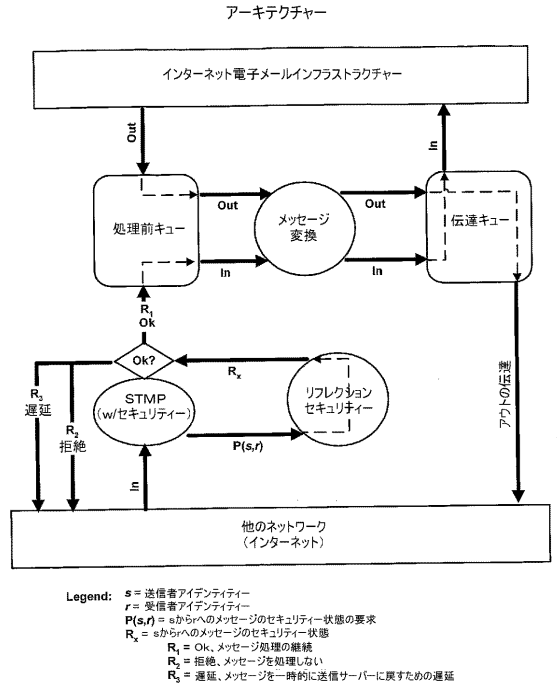
１０４　メッセージ変換モジュール

１０６　伝達キュー

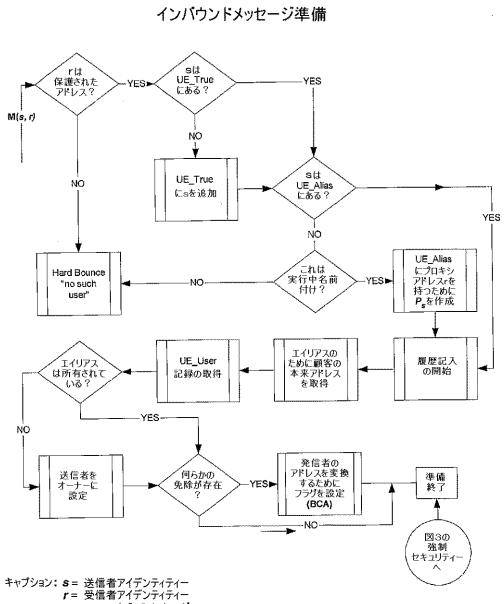
１０８　リフレクションセキュリティーモジュール

１１４　送信サーバー

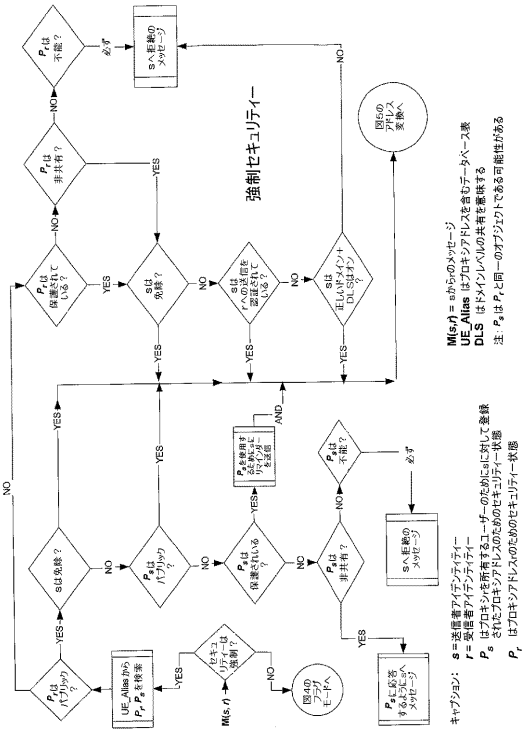
【図１】


アーキテクチャー
インターネット電子メールインフラストラクチャー
Out
In
処理前キュー
メッセージ変換
伝達キュー
Ok?
STMP (w/セキュリティー)
リフレクションセキュリティー
アウトの伝達
他のネットワーク（インターネット）
Legend:
s = 送信者アイデンティティー
r = 受信者アイデンティティー
P(s,r) = sからrへのメッセージのセキュリティー状態の要求
Rx = sからrへのメッセージのセキュリティー状態
R1 = Ok、メッセージ処理の継続
R2 = 拒絶、メッセージを処理しない
R3 = 遅延、メッセージを一時的に送信サーバーに戻すための遅延

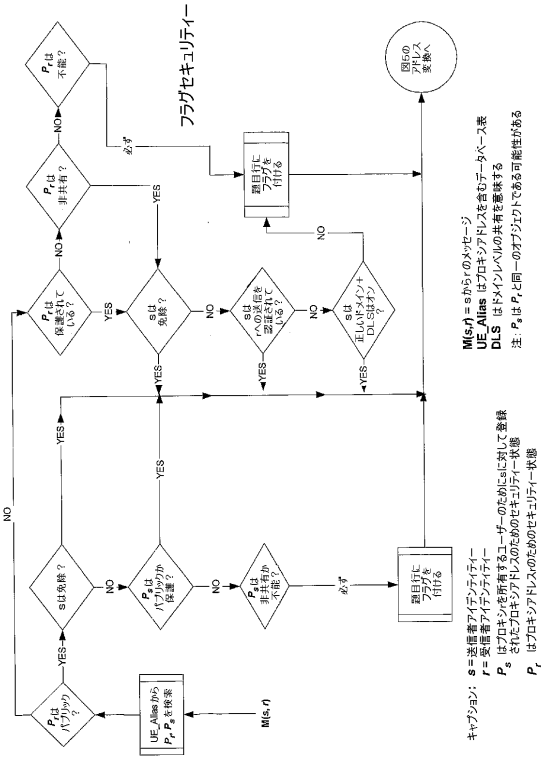
【図２】


インバウンドメッセージ準備
M(s, r)
UE_True にsを追加
UE_Alias にプロキシアドレスrを持つために Psを作成
Hard Bounce "no such user"
履歴記入の開始
エイリアスのために顧客の本来アドレスを取得
UE_User 記録の取得
送信者をオーナーに設定
発信者のアドレスを変換するために フラグを設定 (BCA)
準備終了
図3の強制セキュリティーへ
キャプション：
s = 送信者アイデンティティー
r = 受信者アイデンティティー
M(s,r) = sからrのメッセージ
UE_TRUE は「本当」の（すなわち、非プロキシのアドレスを含むデータベース表
UE_ALIAS はプロキシアドレスを含むデータベース表
UE_User はユーザー情報を含むデータベース表
BCA =「名刺アドレス」、内部メール移送エージェント（すなわち、メールサーバー）によって管理される発信者のアドレス
Ps はプロキシが代用である発信者アドレスを所有するユーザーに登録されているプロキシアドレスに対するセキュリティー状態

【図３】


強制セキュリティー
M(s,r) = sからrのメッセージ
UE_Alias はプロキシアドレスを含むデータベース表
DLS はドメインレベルの共有を意味する
注 Ps は Pr と同一のオブジェクトである可能性がある
キャプション：
s = 送信者アイデンティティー
r = 受信者アイデンティティー
Ps はプロキシを所有するユーザーのために sに対して登録されたプロキシアドレスのためのセキュリティー状態
Pr はプロキシアドレスのためのセキュリティー状態

【図４】


フラグセキュリティー
M(s,r) = sからrのメッセージ
UE_Alias はプロキシアドレスを含むデータベース表
DLS はドメインレベルの共有を意味する
注 Ps は Pr と同一のオブジェクトである可能性がある
キャプション：
s = 送信者アイデンティティー
r = 受信者アイデンティティー
Ps はセッションを所有するユーザーのために sに対して登録されたプロキシアドレスのためのセキュリティー状態
Pr はプロキシアドレスのためのセキュリティー状態

【図５】

アドレス変換

「本来」識別子（UE_True表）
T1 = 内部識別子 1
T2 = 外部識別子 1
T3 = 外部識別子 2
T4 = 内部識別子 1
Tn = 外部識別子 n

プロキシ識別子（UE_Alias表）
$P_{(T2,T1)}$ = T2に登録された、T1に対する代理識別子
$P_{(T3,T1)}$ = T3に登録された、T1に対する代理識別子
$P_{(Tn,T1)}$ = Tnに登録された、T1に対する代理識別子

$P_{(Tx,Tx)}$ = Txに登録された、Tx

s = 送信者アイデンティティー
r = 受信者アイデンティティー
a = 変換するためのアドレス参照
M(*s*,*r*) = sからrへのメッセージ

T(*a*) = sからrへのメッセージに対するアドレス a の変換を戻す方法

$D_{(Tx,T1)}$ = TxがT1に電子メールを送信するために使用するプロキシPを戻す方法
場合によっては$D_{(Tx,T1)} <> P_{(Tx,T1)}$

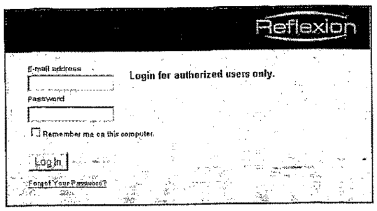
インバウンド、通過に成功したセキュリティー、ここで：

1. ***a*** = ***r***, ***s*** = **T2**, ***r*** = $P_{(T2,T1)}$, then **T(*a*)** = **T1**
2. ***a*** = ***r***, ***s*** = **T2**, ***r*** = $P_{(T3,T1)}$, then **T(*a*)** = **T1**
3. ***a*** = $P_{(T4,T4)}$, ***s*** = **T2**, ***r*** = $P_{(T2,T1)}$, then **T(*a*)** = **T4**
4. ***a*** = $P_{(T4,T4)}$, ***s*** = **T2**, ***r*** = $P_{(T3,T1)}$, then **T(*a*)** = **T4**
5. ***a*** = **T3**, ***s*** = **T2**, ***r*** = $P_{(Tx,T1)}$, then **T(*a*)** = **T3**
6. ***a*** = $P_{(Tx,Ty)}$, ***s*** = **T2**, **T2** is exempt, ***r*** = any P, then **T(*a*)** = **Ty**

アウトバウンド、アウトバウンドにセキュリティー無し、ここで：

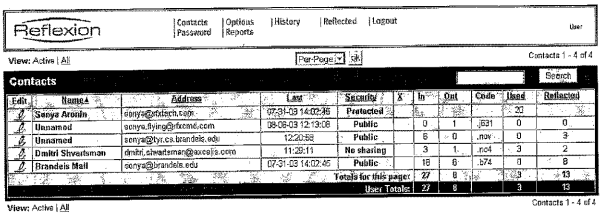
7. ***a*** = ***r***, ***s*** = **T1**, ***r*** = **T2**, then **T(*a*)** = $P_{(T2,T1)}$
8. ***a*** = ***r***, ***s*** = **T1**, ***r*** = **T2**, $D_{(T2,T1)} <> P_{(T2,T1)}$, then **T(*a*)** = $D_{(T2,T1)}$
9. ***a*** = ***r***, ***s*** = **T1**, ***r*** = **T2**, $D_{(T2,T1)} = P_{(T2,T1)}$, then **T(*a*)** = $P_{(T2,T1)}$
10. ***a*** = ***r***, ***s*** = **T1**, ***r*** = **T2**, r is exempt, then **T(*a*)** = $P_{(T1,T1)}$ **[*s*]**
11. ***a*** = **T3**, ***s*** = **T1**, ***r*** = **T2**, then **T(*a*)** = $P_{(T3,T1)}$
12. ***a*** = **T3**, ***s*** = **T1**, ***r*** = **T2**, $D_{(T3,T1)} <> P_{(T3,T1)}$, then **T(*a*)** = $D_{(T3,T1)}$
13. ***a*** = **T3**, ***s*** = **T1**, ***r*** = **T2**, $D_{(T1,T2)} = P_{(T2,T1)}$, then **T(*a*)** = $P_{(T3,T1)}$
14. ***a*** = **T3**, ***s*** = **T1**, ***r*** = **T2**, **T3** is exempt, then **T(*a*)** = $P_{(T1,T1)}$ **[*s*]**

【図７】



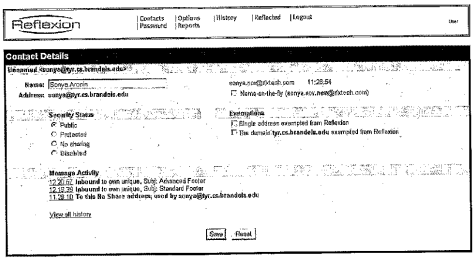
ログインページ

【図８】



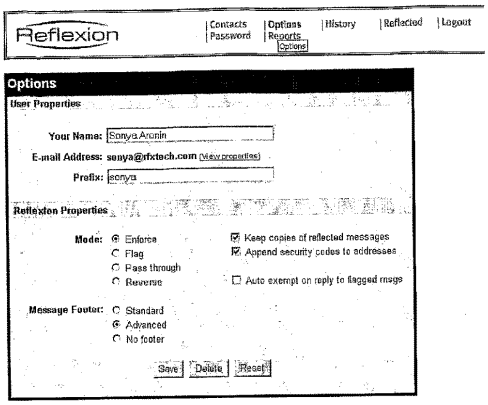
接触リスト

【図９】



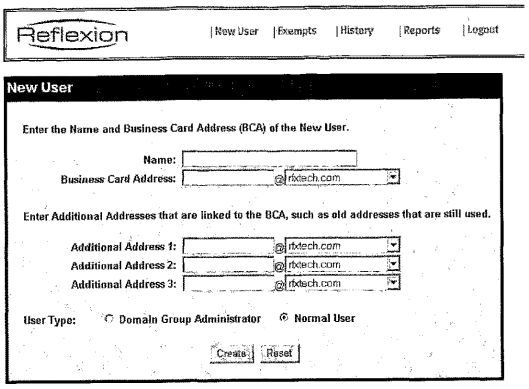
接触の詳細のページ

【図１０】



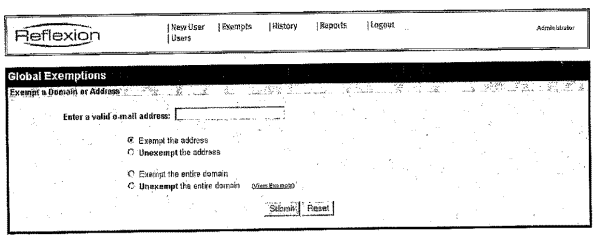
リフレクションユーザーオプションページ

【図１２】



管理者作成新規ユーザーページ

【図１１】



管理者追加グローバル免除ページ

【手続補正書】
【提出日】平成17年4月12日(2005.4.12)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
電子通信ネットワークに接続されたユーザーへのアクセスを選択的に許可または拒絶するための方法であって、前記ユーザーが関連する受信者の識別子を有し：
Ａ．前記ユーザーに関連した複数のプロキシ識別子を生成することであって、前記プロキシ識別子の各々が少なくとも３つの関連するセキュリティー状態を有し、前記状態の第１の状態が前記ネットワークに接続したパーティーが前記ユーザーにアクセスすることを許可することを示し、前記状態の第２の状態が前記ネットワークに接続したパーティーが前記ユーザーにアクセスすることを拒絶することを示し、さらに、前記状態の第３の状態が、予め決められた基準が満たされた場合に、前記ネットワークに接続したパーティーのうちの少なくとも１つのパーティーであって、全てのパーティーより少ないパーティーが前記ユーザーに条件付でアクセスすることを許可することを示し、基準が満たされていない場合にアクセスを拒絶すること；
Ｂ．インバウンドメッセージの送信者に関連付けられた送信者の識別子及び前記受信者の識別子を含む前記ネットワークからの前記インバウンドメッセージへの応答で、前記インバウンドメッセージを前記プロキシ識別子の１つに関連付けられた場所に伝送すること；
Ｃ．前記伝送されたインバウンドメッセージに関連したセキュリティー状態であって、前記送信者の識別子及び前記受信者の識別子に関連付けられているセキュリティー状態を評価するために前記インバウンドメッセージを処理すること；及び、
Ｄ．前記セキュリティー状態が前記１つのプロキシ識別子の前記セキュリティー状態に少なくとも部分的に関連した、１つまたは複数の予め決められた基準を満たすとき、前記伝送されたメッセージの前記ユーザーへのアクセスを許可し、その他の場合に、前記伝送されたメッセージの前記ユーザーへのアクセスを拒絶することを含む方法。
【請求項２】
前記識別子が電子メールアドレスである、請求項１に記載の方法。
【請求項３】
電子通信ネットワークに接続されたユーザーへのアクセスを選択的に許可または拒絶するためのシステムであって、前記ユーザーが関連する受信者の識別子を有し：
Ａ．前記ユーザーに関連した複数のプロキシ識別子を生成する生成器であって、前記プロキシ識別子の各々が少なくとも３つの関連するセキュリティー状態を有し、前記状態の第１の状態が前記ネットワークに接続したパーティーが前記ユーザーにアクセスすることを許可することを示し、前記状態の第２の状態が前記ネットワークに接続したパーティーが前記ユーザーにアクセスすることを拒絶することを示し、さらに、前記状態の第３の状態が、予め決められた基準が満たされた場合に、前記ネットワークに接続したパーティーのうちの少なくとも１つのパーティーであって、全てのパーティーより少ないパーティーが前記ユーザーに条件付でアクセスすることを許可することを示し、基準が満たされていない場合にアクセスを拒絶する生成器；
Ｂ．インバウンドメッセージの送信者に関連付けられた送信者の識別子及び前記受信者の識別子を含む前記ネットワークからの前記インバウンドメッセージへの応答で、前記インバウンドメッセージを前記プロキシ識別子の１つに関連付けられた場所に伝送するメッセージ伝送器；
Ｃ．前記伝送されたインバウンドメッセージに関連したセキュリティー状態であって、前記送信者の識別子及び前記受信者の識別子に関連付けられている前記セキュリティー状態

を評価するためのプロセッサー；及び、
Ｄ．前記セキュリティー状態が前記１つのプロキシ識別子の前記セキュリティー状態に少なくとも部分的に関連した、１つまたは複数の予め決められた基準を満たすとき、前記伝送されたメッセージの前記ユーザーへのアクセスを許可し、その他の場合に、前記伝送されたメッセージの前記ユーザーへのアクセスを拒絶するゲートを備えるシステム。
【請求項４】
前記識別子が電子メールアドレスである、請求項３に記載のシステム。
【請求項５】
前記ユーザーに関連付けられている生成されたプロキシ識別子の少なくとも１つが実質的に前記ユーザーを識別するための内容を含まない、請求項１に記載の方法。
【請求項６】
前記ユーザーに関連付けられている生成されたプロキシ識別子の少なくとも１つが予め定義された時間間隔だけ有効である、請求項１に記載の方法。
【請求項７】
前記複数のプロキシ識別子がデータベースに格納されている、請求項１に記載の方法。
【請求項８】
前記データベースへのエントリーが前記ユーザーに関連する接触者の名前を表すデータ、前記ユーザーに割り当てられたプロキシアドレス、及び前記プロキシアドレスに割り当てられたセキュリティー状態を含む、請求項７に記載の方法。
【請求項９】
前記伝送されたインバウンドメッセージの処理が前記受信者の識別子を前記ユーザーに関連付けられた複数のプロキシ識別子の少なくとも１つに一致するために試みることを含む、請求項１に記載の方法。
【請求項１０】
前記伝送されたインバウンドメッセージの処理が前記受信者の識別子を前記ユーザーの接触者に関連付けられた複数のプロキシ識別子の少なくとも１つに一致するために試みることを含む、請求項１に記載の方法。
【請求項１１】
前記伝送されたインバウンドメッセージを処理することが前記ユーザーに関連付けられたセキュリティー状態を決定することを含む、請求項１に記載の方法。
【請求項１２】
前記メッセージの前記ユーザーへの伝送を拒絶することが前記送信者に返信メッセージを送信することを含む、請求項１に記載の方法。
【請求項１３】
前記メッセージの前記ユーザーへの伝送を拒絶することが前記送信者に返信メッセージを送信することを含み、前記返信メッセージが前記ユーザーに関連付けられた前記複数のプロキシ識別子の１つを含む、請求項１に記載の方法。
【請求項１４】
前記メッセージの前記ユーザーへの伝送を拒絶することが前記ユーザーに関連付けられたプロキシ識別子を生成すること、及び前記送信者に返信メッセージを送信することを含み、前記返信メッセージが前記ユーザーに関連付けられた前記複数のプロキシ識別子の１つを含む、請求項１に記載の方法。
【請求項１５】
前記メッセージの前記ユーザーへの伝送を拒絶することが前記送信者の識別子をデータベースに入力することを含む、請求項１に記載の方法。
【請求項１６】
前記メッセージの前記ユーザーへの伝送を許可することが、前記ユーザーが前記送信者から事前に送信されたメッセージへ返信しているかどうかを決定することを含む、請求項１に記載の方法。
【請求項１７】

前記メッセージの前記ユーザーへの伝送を許可することが、前記ユーザーがメッセージに含まれているプロキシ識別子の生成に着手しているかどうかを決定することを含む、請求項１に記載の方法。

【請求項１８】

前記ユーザーによって生成されたプロキシ識別子が前記複数のプロキシ識別子に存在しない、請求項１７に記載の方法。

【請求項１９】

前記ユーザーによって生成されたプロキシ識別子が前記複数のプロキシ識別子に存在しない場合に、前記ユーザーによって生成されたプロキシ識別子を前記複数のプロキシ識別子に加えることをさらに含む、請求項１８に記載の方法。

【請求項２０】

前記メッセージの前記ユーザーへの伝送を許可することが前記メッセージ内の前記ユーザーによって生成されたプロキシ識別子への参照を除去することを含む、請求項１７に記載の方法。

【請求項２１】

前記メッセージの前記ユーザーへの伝送を許可することが、前記メッセージ内の前記ユーザーによって生成されたプロキシ識別子への参照を除去し、前記メッセージに前記ユーザーに関連付けられた電子メールアドレスを付加することを含む、請求項１７に記載の方法。

【請求項２２】

前記伝送されたインバウンドメッセージを処理することが前記メッセージ内の前記受信者識別子への参照を除去することを含む、請求項１に記載の方法。

【請求項２３】

前記ネットワークに接続したパーティーが前記ユーザーにアクセスすることを許可することを示す前記第１の状態が前記ユーザーの前記パーティーからのメッセージの伝送を許可することを含む、請求項１に記載の方法。

【請求項２４】

前記ネットワークに接続したパーティーが前記ユーザーにアクセスすることを拒絶することを示す前記第２の状態が前記ユーザーのパーティーからのメッセージの伝送を阻止することを含む、請求項１に記載の方法。

【請求項２５】

前記予め決められた基準が、ユーザーが送信者によって事前に送信されたメッセージに対して事前に応答していることを含む、請求項１に記載の方法。

【請求項２６】

前記事前に送信されたメッセージが前記送信者の識別子を含む、請求項２５に記載の方法。

【請求項２７】

前記予め決められた基準の１つが、送信者の識別子が前記複数の識別子の１つに一致していることを含む、請求項１に記載の方法。

【請求項２８】

前記予め決められた基準の１つが、受信者の識別子が前記複数の識別子の１つに一致していることを含む、請求項１に記載の方法。

【請求項２９】

前記予め決められた基準の１つが、受信者の識別子及び送信者の識別子の両方が同一のネットワークドメインに関連付けられていることを含む、請求項１に記載の方法。

【請求項３０】

前記ユーザーに関連付けられた生成されたプロキシ識別子の少なくとも１つが実質的に前記ユーザーを識別するための内容を含まない、請求項３に記載のシステム。

【請求項３１】

前記ユーザーに関連付けられている生成されたプロキシ識別子の少なくとも１つが予め

定義された時間間隔だけ有効である、請求項３に記載のシステム。
【請求項３２】
前記複数のプロキシ識別子を格納するために設定されているデータベースをさらに含む、請求項３に記載のシステム。
【請求項３３】
前記データベースが前記ユーザーに関連する接触者の名前を表すデータ、前記ユーザーに割り当てられたプロキシ識別子、及び前記プロキシアドレスに割り当てられたセキュリティー状態を格納するエントリーを含む、請求項３２に記載のシステム。
【請求項３４】
前記プロセッサーが前記送信者の識別子を前記ユーザーに関連付けられた複数の識別子の少なくとも１つに一致させることを試みる、請求項３に記載のシステム。
【請求項３５】
前記プロセッサーが前記ユーザーに関連付けられたセキュリティー状態を決定し、前記メッセージに関連付けられたセキュリティー状態を上書きする、請求項３に記載のシステム。
【請求項３６】
前記プロセッサーが、前記受信者の識別子が前記ユーザーに関連付けられた前記複数のプロキシ識別子の１つに一致しているかを決定する、請求項３に記載のシステム。
【請求項３７】
前記ゲートが前記メッセージの伝送の拒絶を報告するために前記送信者に返信メッセージを送信することを着手する、請求項３に記載のシステム。
【請求項３８】
前記ゲートが前記メッセージの伝送の拒絶を報告するために前記送信者に返信メッセージを送信することを着手し、前記返信メッセージが前記ユーザーに関連付けられた前記複数のプロキシ識別子の１つを含む、請求項３に記載のシステム。
【請求項３９】
前記プロセッサーが、前記メッセージの伝送によるユーザーへのアクセスが拒絶されたときに、前記送信者の識別子のデータベースへの入力を着手する、請求項３に記載のシステム。
【請求項４０】
前記プロセッサーが前記メッセージを前記ユーザーに伝送するかを決定するために、前記ユーザーが前記送信者から事前に送信されたメッセージに返信しているかを決定する、請求項３に記載のシステム。
【請求項４１】
前記プロセッサーが前記メッセージを前記ユーザーに伝送するかを決定するために、前記ユーザーが前記受信者の識別子の生成に着手しているかを決定する、請求項３に記載のシステム。
【請求項４２】
前記ユーザーによって生成された受信者の識別子が前記複数のプロキシ識別子に存在しない、請求項４１に記載のシステム。
【請求項４３】
前記プロセッサーが前記ユーザーによって生成された受信者の識別子が存在しないと決定した場合、前記プロセッサーが前記ユーザーによって生成された受信者の識別子を前記複数のプロセッサー識別子に追加する、請求項４２に記載のシステム。
【請求項４４】
前記メッセージが前記ユーザーに伝送される場合、前記プロセッサーが前記メッセージ内の前記受信者の識別子への全ての参照を除去することを着手する、請求項３に記載のシステム。
【請求項４５】
前記メッセージが前記ユーザーに伝送される場合、前記プロセッサーが前記メッセージ

の受信者に関連付けられた識別子への参照を付加することを着手する、請求項３に記載のシステム。

【請求項４６】

前記第１のセキュリティー状態が検出された場合、前記ゲートが前記ユーザーへの前記インバウンドメッセージの伝送を許可する、請求項３に記載のシステム。

【請求項４７】

前記第２セキュリティー状態が検出された場合、前記ゲートが前記ユーザーへの前記インバウンドメッセージの伝送を阻止する、請求項３に記載のシステム。

【請求項４８】

前記予め決められた基準が、ユーザーが前記送信者から事前に送信されたメッセージに応答していることを含む、請求項３に記載のシステム。

【請求項４９】

前記事前に送信されたメッセージが送信者の識別子を含む、請求項４８に記載のシステム。

【請求項５０】

前記予め決められた基準が、前記プロセッサーが送信者の識別子を前記複数の識別子の１つに一致させたことを含む、請求項３に記載のシステム。

【請求項５１】

前記予め決められた基準が、前記プロセッサーが受信者の識別子を前記複数の識別子の１つに一致させたことを含む、請求項３に記載のシステム。

【請求項５２】

前記予め決められた基準が、前記プロセッサーが受信者の識別子及び送信者の識別子を同一のネットワークドメインに関連付けられていることを決定することを含む、請求項３に記載のシステム。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US03/25067

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) : G06F 13/38, 17/00; H04M 11/00
US CL : 713/200, 201; 709/200.68, 206
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)
U.S. : 713/200, 201; 709/200.68, 206, 200.36, 200.7, 207, 219, 245, 249, 238, 219

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

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EAST: access control, e-mail address, control list, security

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6,192,114 B1 (COUNCIL.) 20 February 2001 (20.01.2001), Abstract, col. 4, lines 8-23.	1-4

☐ 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 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
20 November 2003 (20.11.2003)

Date of mailing of the international search report
09 DEC 2003

Name and mailing address of the ISA/US
Mail Stop PCT, Attn: ISA/US
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
Facsimile No. (703) 305-3230

Authorized officer
Ly V. Hua Peggy Harrod
Telephone No. (703) 305-9600

Form PCT/ISA/210 (second sheet) (July 1998)

フロントページの続き

(81)指定国 AP(GH,GM,KE,LS,MW,MZ,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HU,IE,IT,LU,MC,NL,PT,RO,SE,SI,SK,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AT,AU,AZ,BA,BB,BG,BR,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DZ,EC,EE,ES,FI,GB,GD,GE,GH,GM,HR,HU,ID,IL,IN,IS,JP,KE,KG,KP,KR,KZ,LC,LK,LR,LS,LT,LU,LV,MA,MD,MG,MK,MN,MW,MX,MZ,NO,NZ,OM,PH,PL,PT,RO,RU,SD,SE,SG,SK,SL,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VN,YU,ZA,ZM,ZW

（特許庁注：以下のものは登録商標）
ＪＡＶＡ

(74)代理人 100129333
弁理士 中島 拓
(72)発明者 ジョーゼフ イー．マキザック
アメリカ合衆国 ０１８０３ マサチューセッツ、バーリントン、マウンテン ロード ５６
(72)発明者 マークス ダーロフ
ノルウェー国 エヌ０２５０ オスロ、ベディンゲン ２６
(72)発明者 エル．ブルース タタースキ
アメリカ合衆国 ０３０６２ ニューハンプシャー、ナシュア、ピール ストリート ４９
(72)発明者 リチャード ケイ．バレット
アメリカ合衆国 ０１８８７ マサチューセッツ、ウィルミントン、パーカー ストリート ７