(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4689942号
(P4689942)
(45)発行日　平成23年6月1日(2011.6.1)　(24)登録日　平成23年2月25日(2011.2.25)

(51)Int.Cl.　　F I
G06F 13/00 (2006.01)　　G06F 13/00 610S
H04L 12/58 (2006.01)　　H04L 12/58 100Z

請求項の数 27　(全 19 頁)

(21)出願番号　特願2002-580190(P2002-580190)
(86)(22)出願日　平成14年4月3日(2002.4.3)
(65)公表番号　特表2004-534294(P2004-534294A)
(43)公表日　平成16年11月11日(2004.11.11)
(86)国際出願番号　PCT/US2002/010643
(87)国際公開番号　WO2002/082293
(87)国際公開日　平成14年10月17日(2002.10.17)
審査請求日　平成15年11月10日(2003.11.10)
審判番号　不服2008-5948(P2008-5948/J1)
審判請求日　平成20年3月10日(2008.3.10)
(31)優先権主張番号　09/825,431
(32)優先日　平成13年4月3日(2001.4.3)
(33)優先権主張国　米国(US)

(73)特許権者　503359854
パーデュー　ファーマ　エルピー
アメリカ合衆国　コネチカット　06901，スタンフォード，ワン　スタンフォード　フォーラム
(74)代理人　100091096
弁理士　平木　祐輔
(74)代理人　100105463
弁理士　関谷　三男
(74)代理人　100102576
弁理士　渡辺　敏章
(74)代理人　100100169
弁理士　大塩　剛

最終頁に続く

(54)【発明の名称】ルーティング制御機構を有する特権通信システム

(57)【特許請求の範囲】
【請求項１】
デジタル通信の機密性を明らかにするためのデジタル通信システムであって、
プロセッサと、
上記プロセッサによって実行可能なプログラムを含むメモリとを備え、
上記プログラムは、
デジタル通信の目的の受信者の特権配信リストを作成するとともにデジタル通信に実行可能モジュールを付加することができ、
上記実行可能モジュールは、
該実行可能モジュールが付加されたデジタル通信へのアクセスを上記目的の受信者に制限し、且つ
該実行可能モジュールが付加されたデジタル通信のルーティングを上記目的の受信者に制限するように構成され、
上記デジタル通信に付加された上記実行可能モジュールは上記特権配信リストに従って上記デジタル通信へのアクセスと上記デジタル通信のルーティングを制限し、上記実行可能モジュールは、上記デジタル通信が転送されると、上記デジタル通信と共に移動することを特徴とする通信システム。
【請求項２】
上記プログラムはさらに、上記デジタル通信へのアクセス権を設定することができ、上記実行可能モジュールは、上記デジタル通信へのアクセスを管理し上記デジタル通信のコ

ンテントの処理を制御することによって上記アクセス権を実施するように実行可能であり、
上記アクセス権は、
上記デジタル通信の転送を許可することと、
上記デジタル通信への応答を許可することと、
事前に選択された受信者へのカーボン・コピーによる上記応答を許可することとを含む、請求項１に記載の通信システム。
【請求項３】
上記デジタル通信はアドレス部およびコンテント部を含み、
上記アクセス権は、
上記デジタル通信のコンテントのコピーを許可することと、上記デジタル通信からの通信のコンテントの切取り、および切り取ったコンテントの、他の位置への貼付けを可能にすることとをさらに含む、請求項２に記載の通信システム。
【請求項４】
上記デジタル通信に実行可能モジュールを付加するプログラムは、自動的に実行され、上記実行可能モジュールを所定の選択基準に従って特定のデジタル通信に付加するように設定される、請求項１に記載の通信システム。
【請求項５】
ユーザに表示され、特権デジタル通信を表示する前にユーザによって肯定応答される機密性通知をさらに備える、請求項１に記載の通信システム。
【請求項６】
上記特権デジタル通信は暗号化される、請求項１に記載の通信システム。
【請求項７】
上記プログラムは、サーバ・オブジェクトおよびクライアント・オブジェクトを備え、
上記クライアント・オブジェクトは、上記実行可能モジュールを付加し、特権デジタル通信を上記サーバ・オブジェクトに送信するように設定され、
上記サーバ・オブジェクトは、上記特権デジタル通信を離れた位置に記憶する、請求項１に記載の通信システム。
【請求項８】
上記クライアント・オブジェクトは既存の通信システムのプラグインである、請求項７に記載の通信システム。
【請求項９】
代理人－依頼人特権デジタル通信を作成する方法であって、
デジタル通信を作成するステップと、
上記デジタル通信に特権属性を付加することによって、特権を有するデジタル通信としてマーク付けするステップと、
上記デジタル通信をデータ記憶装置上の特権デジタル通信のための離れた位置に記憶するステップと、
上記デジタル通信へのアクセス権を設定し少なくとも１人の目的の受信者の特権配信リストを上記デジタル通信に関係付けるステップと、
上記デジタル通信へのアクセスを管理し上記デジタル通信のコンテントの処理を上記特権配信リスト及び上記デジタル通信に付加された特権属性に基づいて制御することによって上記アクセス権を実施するステップとを含み、
上記アクセス権は、
上記デジタル通信の転送と、
上記デジタル通信への応答と、
事前に選択された受信者へのコピーによる上記応答とを含み、
上記デジタル通信はアドレス部およびコンテント部を含み、
上記アクセス権は、
上記デジタル通信のコンテントをコピーすることと、

上記デジタル通信から通信のコンテントを切り取り、切り取ったコンテントを他の位置に貼り付けることとを含む方法。

【請求項１０】

上記デジタル通信に特権属性を付加するステップは、自動的に、特権属性を所定の選択基準に従って特定のデジタル通信に付加することをさらに含む、請求項９に記載の方法。

【請求項１１】

ユーザに機密性通知を表示するステップと、

特権デジタル通信を表示する前にユーザによって機密性通知に肯定応答させるステップとをさらに含む、請求項９に記載の方法。

【請求項１２】

上記デジタル通信に暗号化技術を適用するステップをさらに含む、請求項９に記載の方法。

【請求項１３】

上記デジタル通信のブラインド・カーボン・コピーを作成するステップと、

上記ブラインド・カーボン・コピーを離れたサーバに送信するステップとをさらに含み、上記離れた位置は上記離れたサーバ上に存在する、請求項９に記載の方法。

【請求項１４】

上記デジタル通信の共通の特性によって、上記離れた位置を分類することをさらに含み、上記共通の特性は、

上記デジタル通信の送信者、

上記デジタル通信の受信者、および

企業の部署のうちの１つまたは複数を含む、請求項９に記載の方法。

【請求項１５】

クライアント装置上に第2の離れた位置を作成するステップと、

上記第2の離れた位置上に上記デジタル通信のコピーを記憶するステップとをさらに含む、請求項９に記載の方法。

【請求項１６】

特権によって保護されたデジタル通信を作成する方法であって、

実行可能モジュールを作成するステップであって、少なくとも１人の目的の受信者の特権配信リストに従って該実行可能モジュールが付加されたデジタル通信へのアクセスを制限して特権の適用を維持するようコンピュータに指示するように構成された実行可能モジュールを作成するステップと、

上記実行可能モジュールをデジタル通信に付加し、それによって上記実行可能モジュールは上記特権配信リストに従って上記デジタル通信へのアクセスを制限するようコンピュータに指示するステップと、

を含み、上記実行可能モジュールは、上記デジタル通信が転送されると、上記デジタル通信と共に移動することを特徴とする方法。

【請求項１７】

上記デジタル通信へのアクセス権を設定するステップと、

上記デジタル通信へのアクセスを管理し上記デジタル通信のコンテントの処理を制御することによって上記アクセス権を実施するステップとをさらに含む、請求項１６に記載の方法。

【請求項１８】

上記アクセス権は、

上記デジタル通信の転送と、

上記デジタル通信への応答と、

事前に選択された受信者へのコピーによる上記応答とを含む、請求項１７に記載の方法。

【請求項１９】

上記デジタル通信はアドレス部およびコンテント部を含み、

上記アクセス権は、

上記デジタル通信のコンテントをコピーすることと、
上記デジタル通信から通信のコンテントを切り取り、切り取ったコンテントを他の位置に貼り付けることとをさらに含む、請求項１７に記載の方法。
【請求項２０】
上記特権配信リストおよび上記アクセス権を含む特権プロファイルを作成するステップをさらに含む、請求項１７に記載の方法。
【請求項２１】
上記実行可能モジュールをデジタル通信に付加するステップは、自動的に、上記実行可能モジュールを所定の選択基準に従って特定のデジタル通信に付加することをさらに含む、請求項１６に記載の方法。
【請求項２２】
ユーザに機密性通知を表示し、特権によって保護されたデジタル通信が表示される前に上記機密性通知がユーザによって肯定応答されることを要求するステップをさらに含む、請求項１６に記載の方法。
【請求項２３】
上記デジタル通信に暗号化技術を適用するステップをさらに含む、請求項１６に記載の方法。
【請求項２４】
特権デジタル通信を作成する方法であって、
実行可能モジュールを作成するステップであって、少なくとも１人の目的の受信者の特権配信リストに従ってデジタル文書へのアクセスを制限し該デジタル文書のコンテントの処理を管理することによって、上記実行可能モジュールが付加された該デジタル文書の通信における機密性を維持するようコンピュータに指示する実行可能モジュールを作成するステップと、
上記実行可能モジュールを上記デジタル文書に付加し、それによって上記実行可能モジュールは上記特権配信リストに従って上記デジタル文書へのアクセスを制限するようコンピュータに指示するステップと、
を含み、上記実行可能モジュールは、上記デジタル文書が転送されると、上記デジタル文書と共に移動することを特徴とする方法。
【請求項２５】
上記デジタル文書が開かれるときに上記実行可能モジュールを実行するステップをさらに含む、請求項２４に記載の方法。
【請求項２６】
上記デジタル文書が暗号化された文書であり、上記実行可能モジュールは、所定の条件が満たされた場合に上記デジタル文書を復号するようコンピュータに指示するように構成される、請求項２４に記載の方法。
【請求項２７】
デジタル通信システムであって、
プロセッサと、上記プロセッサによって実行可能であり、デジタル通信に実行可能モジュールを付加するプログラムを含むメモリとを備え、
上記実行可能モジュールは、
該実行可能モジュールが付加されたデジタル通信へのアクセスを目的の受信者および代理人受信者の事前に登録された被指名人に制限し、
該実行可能モジュールが付加されたデジタル通信のルーティングを目的の受信者および代理人受信者の事前に登録された被指名人に制限し、
該実行可能モジュールは、上記デジタル通信が転送されると、上記デジタル通信と共に移動することを特徴とする通信システム。
【発明の詳細な説明】
【技術分野】
【０００１】

本発明は、電子メール（「eメール」）メッセージ交換を含む、電子的に作成された文書の分野に関し、eメール・ルーティングの分野に関する。

【背景技術】

【０００２】

ユーザ間の電子メールの交換を可能にするeメール・メッセージ送信システムは、世界中の企業および個人によって広く使用されている。eメール・システムは、ローカル・エリア・ネットワーク（LAN）に接続されたユーザにメッセージ交換サービスを提供するように構成することができ、かつインタネットのような外部ネットワークのワイド・エリア・ネットワーク（WAN）を介したLANの外部のユーザへの／からのメッセージの送信／受信を可能にするように構成することができる。eメール・システムはまた、ユーザが、eメール・システム上で受信されたメッセージを保存し、コピーし、転送するのを可能にする。

【０００３】

eメール通信については、代理人－依頼人特権を適用するかどうかが議論の的になっている。eメール通信の特権を確立するための法的要件は、司法管区ごとに異なるが、一般的な規則として、通信を機密にすることを各当事者が意図するときに特権が付加され、この特権によってクライアントの法的代理が推進される。しかし、eメール通信の性質上、eメール通信の機密を維持する意図を確証するものが何であるかが議論の的になっているが、明確に示されてはない。eメールは、その宛先への送信時に、様々な当事者に属する様々なハードウェア上を通る。法的代理関係を有さない当事者への通信では、機密を維持する意図が見つからない場合、通信のコンテントに対する特権が失われる恐れがある。

【発明の開示】

【０００４】

本発明の第1の実施態様によれば、プロセッサ（CPUなど）と、プロセッサによって実行可能であり、デジタル通信に機密属性を付加し、機密デジタル通信へのアクセスを目的の受信者に制限し、この特権デジタル通信を、データ記憶装置上の離れた位置に記憶するプログラムを含むメモリとを含むデジタル通信システムが提供される。この実施態様の他の局面によれば、プロセッサは、特権通信システムへのアクセスを目的の受信者および目的の受信者の事前に登録された被指名人に制限することができる。好ましくは、機密属性は特権属性であり、機密デジタル通信は代理人－依頼人特権通信である。この実施態様の他の局面によれば、プロセッサは、このような特権デジタル通信へのアクセスを目的の受信者および代理人受信者の事前に登録された被指名人に制限することができる。

【０００５】

本発明の第2の実施態様によれば、プロセッサと、CPUによって実行可能であり、デジタル通信に機密（および好ましくは特権）属性を付加し、少なくとも1人の受信者の機密（および好ましくは特権）配信リストを作成し、特権デジタル通信へのアクセスを少なくとも1人の目的の受信者に制限し、特権デジタル通信のルーティングを少なくとも1人の目的の受信者に制限し、この機密（および好ましくは特権）デジタル通信を、データ記憶装置上の離れた位置に記憶するプログラムを含むメモリとを備えた、デジタル通信の機密性を示すデジタル通信システムが提供される。

【０００６】

本発明の第3の実施態様によれば、電子通信を作成するステップと、特権属性を有する通信にマーク付けするステップと、この通信をデータ記憶装置上の離れた位置に記憶するステップと、デジタル通信へのアクセス権を構成するステップと、デジタル通信へのアクセスを管理しデジタル通信のコンテントの処理を制御することによってアクセス権を実施するステップとを含む、代理人－依頼人特権デジタル通信を作成する方法が提供される。この実施態様によれば、アクセス権は、通信の転送と、応答と、事前に選択された受信者へのコピーによる応答とを含む。

【０００７】

本発明の第4の実施態様によれば、プロセッサと、CPUによって実行可能であり、デジタル通信に実行可能モジュールを付加するプログラムを含むメモリとを備え、実行可能モジ

ュールは、デジタル通信の目的の受信者の機密（および好ましくは特権）配信リストを作成し、特権デジタル通信へのアクセスを目的の受信者に制限するように構成される、デジタル通信の機密性を示すデジタル通信システムが提供される。好ましくは、実行可能モジュールは、デジタル通信のルーティングを目的の受信者に制限するようにも構成される。この実施態様のある他の局面によれば、プロセッサは、特権デジタル通信のルーティングおよび／またはアクセスを目的の受信者および目的の受信者の事前に登録された被指名人に制限することができる。好ましくは、機密属性は特権属性であり、機密デジタル通信は代理人－依頼人特権通信である。この実施態様の他の局面によれば、プロセッサは、このような特権デジタル通信へのアクセスおよび／またはルーティングを目的の受信者および代理人受信者の事前に登録された被指名人に制限することができる。

【０００８】

本発明の第5の実施態様によれば、特権によって保護されたデジタル通信を作成する方法は、実行可能モジュールが付加された通信へのアクセスを制限して特権の適用を維持するようコンピュータに指示するように構成された実行可能モジュールを作成するステップと、実行可能モジュールを通信に付加するステップとを含む。この実施態様の他の局面によれば、実行可能なモジュールは、通信のコンテントの処理を管理するように構成される。

【０００９】

本発明の第6の実施態様によれば、デジタル通信の機密性を示すデジタル通信システムは、プロセッサと、プロセッサに動作可能に接続されたメモリとを備え、メモリは、仮想コンテナを作成し、特権デジタル通信をこのコンテナに入れるコンテナ・クリエータ・ユーティリティ、および仮想コンテナを開き特権デジタル通信を取り出すコンテナ・オープナ・ユーティリティを含むプログラムを含む。

【００１０】

第6の実施態様によれば、コンテナ・クリエータ・ユーティリティは、コンピュータの電子記憶媒体内の互いに隣接する位置に存在し、ヘッダ部およびデジタル・オブジェクト部を含む仮想コンテナを作成するように動作することができる。なお、コンテナ・クリエータ・ユーティリティは、仮想コンテナに挿入されるデジタル・オブジェクトを選択し、デジタル・オブジェクトに暗号化技術を適用して暗号化デジタル・オブジェクトを作成し、暗号化デジタル・オブジェクトをデジタル・オブジェクト部に書き込み、デジタル・オブジェクト用の特権プロファイルを構成し、特権プロファイルを示す情報を仮想コンテナのヘッダ部に書き込むように動作することもできる。特権プロファイルは好ましくは、目的の受信者および目的の受信者の各々がデジタル・オブジェクトに対して講じる処置のリストを含む。

【００１１】

第6の実施態様の他の局面によれば、コンテナ・オープナ・ユーティリティは、特権プロファイルを示す情報を仮想コンテナのヘッダ部から読み取り、この情報に基づいて、ユーザが、デジタル・オブジェクトのコンテントにアクセスしコンテントを処理する特権を有することが特権プロファイルに定義されているかどうかを判定し、ユーザが特権を有さない場合にオブジェクトへのアクセスを制限し、ユーザは特権を有する場合に、デジタル・オブジェクト部からデジタル・オブジェクトを読み取りデジタル・オブジェクトに復号技術を適用する。

【発明を実施するための最良の形態】

【００１２】

本発明によるeメール・システムは、ユーザが、通信に「特権」属性または「機密」属性を付加し、それによって通信を意図的に特権付きまたは機密として分類することによって、電子形式の通信において機密性を維持する明確な意図を示すのを可能にする。

【００１３】

本発明の特に好ましい実施形態では、属性は「代理人・依頼人特権」属性である。これらの実施形態は、代理人・依頼人通信にeメールが広く利用されていることと、特権を維

持するだけでなく、特権が維持されていたことを（たとえば、裁判や調停で）確証できることの重要性を考慮すると特に有利であると考えられる。

【００１４】

しかし、本発明は、機密性を維持することが重要である他の状況に適用することもできる。たとえば、企業は、その機密情報が、それを受信する業務上の理由を有する従業員にのみ送信されることを望む。たとえば、医師は、患者との通信において医師－患者特権が維持されることを望む。聖職者は、聖職特権を維持することを重視する場合がある。他の用途も本発明によって同様に包含される。したがって、以下では本発明を代理人－依頼人特権に関して説明するが、本発明を他の特権、またはeメール通信の機密性を維持することが重要な任意の状況にも適用できることを理解されたい。

【００１５】

本発明の実施形態によれば、eメール通信が作成されるときにeメール通信に「特権」属性が割り当てられ、それによって、機密性を維持する意図およびeメールにおける法的代理を推進する意図を証明する特権eメールシステムが提供される。eメール・アドレスの特権配信リストがeメール内の最初の受信者のリストから作成される。特権配信リスト内の各ユーザには、対象外の受信者への転送を妨げ、代理人・依頼人特権を有さない人に特権情報が伝搬するのを回避し、それによって特権による保護の喪失を防止するように特権eメールにアクセスしそれを処理する特定の限られた権利が与えられる。本発明によるeメールへの付加は、システムによる制御に従わせることもできる。さらに、特権eメールがアクセスされるたびに機密性通知（および好ましくは特権・機密通知）が表示される。

【００１６】

本発明の他の局面によれば、各特権eメールごとに、活動ログが、eメールに講じられたあらゆる処置を詳細に記述した証跡と共に維持される。

【００１７】

本発明の第1の実施形態によれば、メール・サーバ上のサーバ・ソフトウェア・オブジェクトは、特権eメールを、サーバ上の離れた位置に記憶する。eメールは、特権eメールを、それ特権付きとして識別するフラグと共にサーバ・オブジェクトに送信するクライアント・ソフトウェア・オブジェクトにより、eメールによってイネーブルされるクライアント装置上で作成される。サーバ・オブジェクトは、このフラグを認識し、特権eメールを、他の非特権eメールとは別個に、記憶装置上の離れた位置に記憶する。

【００１８】

特権配布リストは、権利および活動ログと共に、各eメールの特権プロファイルを含んでいる。

【００１９】

コンピュータ・ウィルスは公知である。一般に、コンピュータ・ウィルスは、それ自体をホスト・ファイルに付加する実行可能コードまたはプログラムの一部である。たとえば、「アペンディング・ウィルス」は、それ自体をホスト・プログラムの終了部分に付加し、ホスト・プログラムが実行される前にホスト・プログラムにウィルス・コードを実行させることによって動作する。これに対して、「プリペンディング・ウィルス」は、ホスト・プログラムの開始部分にそれ自体を付加する。他の種類のウィルスはホスト・プログラムの内部に位置する。他の種類のウィルスは「マクロ・ウィルス」として知られている。これらのウィルスは、テキストeメールに埋め込まれ、eメールが開かれるか、作成されるか、または保存されるときに必ず実行されるように環境設定できるマクロである。通常、ホスト・ファイルまたはプログラムと共に残り、他のファイルやプログラムに移らないウィルスを指すのにトロイの木馬という用語が用いられる。

【００２０】

本発明の第2の実施形態によれば、システムは、特権属性が活動化されたときにトロイの木馬の形の実行可能モジュールをeメールおよびあらゆる添付文書に付加する。実行可能モジュールは、実行可能コードまたはプログラムの一部が付加されたeメールが開かれるたびに実行され、eメールのアクセスおよびユーザへの転送を制限する実行可能コード

またはプログラムの一部を含んでいる。実行可能モジュールは、eメールに付加されるので、転送されるときでも、eメールと共に送られる。

【００２１】

本発明の第2の実施形態の他の局面によれば、実行可能モジュールは自動的に、所定の選択基準に従ってすべてのeメールに付加される。

【００２２】

本発明の第1および第2の実施形態の他の局面によれば、eメール、そのコンテント、およびその配信リストは、暗号化技術を用いることによって、特権システムを破壊することを望むユーザから保護することができる。特に、eメール・メッセージは実行可能モジュールまたは他のユーティリティによって暗号化され、実行可能モジュールは、システムが特定のユーザによる復号を可能にする場合にのみeメール・メッセージを復号するように構成されている。このように、ユーザがシステムによる復号なしに特権eメールを開こうとした場合、eメールのコンテントを読み取ることはできない。

【００２３】

本発明の第3の実施形態によれば、特権eメール・システムは、1つまたは複数のeメールが「入れられる」ウィルス・コンテナを含んでいる。

【００２４】

システムは、コンテナ・クリエータおよびコンテナ・オープナを含んでいる。コンテナ・クリエータおよびコンテナ・オープナは、コンピュータ上で実行される1つまたは複数のソフトウェア・プログラムで実施される。コンテナ内のeメール・メッセージへのすべてのアクセスがコンテナ・オープナを通過する。eメールおよびその付加要素へのアクセスが可能になるのは、アクセスを要求したユーザが特権eメールの特権配信リストに含まれているときだけである。

【００２５】

本発明の第3の実施形態の他の局面によれば、コンテナ内の各eメールは、特権配信リストを有してよい。この特徴によれば、コンテナ内の各eメールは、eメールを受信し転送することができる異なる1組の特権ユーザを有してよい。

【００２６】

この実施形態の他の局面によれば、eメールおよびその特権プロファイルは暗号化される。具体的には、コンテナ・クリエータは、コンテナ内のeメールを暗号化するように構成され、コンテナ・オープナはeメール・メッセージを復号するように構成されている。このように、ユーザがコンテナ・オープナを利用せずにあるeメールを開いた場合、このeメールのコンテントを読み取ることはできない。

【００２７】

本発明の他の実施形態によれば、各々が異なるeメール・システムによって実行できる複数の実行可能モジュールをeメール・メッセージに埋め込むことによって特権eメールが作成される。たとえば、eメールは、第1のシステムによって実行できる第1のモジュールと、第2のシステムによって実行できる第2のモジュールとを含んでよい。eメール自体がいずれかのシステムの影響を受けることができる。この実施形態によれば、eメールに対するアクセス制御はeメールが第1のシステムによって開かれるか、それとも第2のシステムによって開かれるかにかかわらずに実施される。

【００２８】

図1は、本発明を利用できる例示的な従来技術の環境を示している。ローカル・エリア・ネットワーク1（LAN1）は、複数のオフィス・コンピュータ10.1～10.6（以後集合的にコンピュータ10と呼ぶ）およびサーバ20を含んでいる。各コンピュータ10は、それぞれの一次記憶機構12（ハード・ドライブなど）およびそれぞれの二次記憶機構14（フロッピィ・ディスクやCD ROMドライブなど）を含んでいる。サーバ20も同様に、一次ネットワーク記憶機構22（ハード・ドライブなど）および二次ネットワーク記憶機構24（フロッピィ・ディスクやCD ROMドライブなど）を含んでいる。一次および二次ネットワーク記憶機構22、24上のデータは、すべてのコンピュータによってアクセスできるという点で共用される

。これに対して、各コンピュータ10の一次および二次記憶機構12、14は、それぞれのコンピュータ10によってのみアクセスされるという点で専用である。サーバ20は、家庭用コンピュータ40などのネットワーク外コンピュータの、伝送回線50を介したインタネット・アクセスを可能にする。家庭用コンピュータ40は、一次記憶機構42および二次記憶機構44を含んでいる。LAN1は、各コンピュータ10がLAN1内で他のコンピュータ10にメッセージを送信し、かつLAN1の外部で家庭用コンピュータ40などのネットワーク外コンピュータにメッセージを送信するのを可能にする電子メール・メッセージ交換サービスをサポートする。図1に示されている構成は、業務上使用されることが多い典型的なLANを示している。しかし、当業者には、様々なネットワーク構成を用いて本発明を実施できることが理解されよう。さらに、本発明のｅメール・メッセージ交換システムは、たとえば、ｅメール・メッセージがモデムまたは他の接続を介してスタンドアロン・コンピュータによって送受信される非ネットワーク・アプリケーションに適用することもできる。さらに、本発明の特徴は、モデムや外部コンピュータとの他の接続の有無にかかわらず、スタンドアロン・コンピュータ上で実施することができる。

【００２９】

次に、図1の構成を参照して、本発明によって軽減できる問題のいくつかについて説明する。

【００３０】

たとえば、ユーザ-1が、社内弁護士であるユーザ-2宛のｅメールをコンピュータ10.1上で作成すると仮定する。このｅメールは、機密性を維持する意図を示す十分な証拠がある場合に通信に特権を与えることができるように、LAN1を所有する会社の法的代理を推進するためのものである。専用LAN上で通常のｅメールを送信するだけでは不十分な場合がある。ｅメールの作成および送信に関する他の環境ならびにこの問題の決定を下す裁判所に応じて専用LAN上での通常のｅメールの送信以上のことが必要になることがある。

【００３１】

外部の弁護士とのｅメール通信のように、メッセージがインタネット・サーバ30を介してLANの外部のコンピュータ40に転送される場合、ｅメール・メッセージが様々な当事者によって所有される異なるハードウェアに転送されるので機密性を維持する意図を示すことはずっと困難になる。さらに、ｅメール・メッセージが送信されると、作成者、この場合ユーザ-1は、転送中にこのｅメールまたはその添付文書のコンテントにアクセスするかまたはこのコンテントを配信してよい人を管理することはできない。このことは、インタネットがｅメールのパスに含まれているときに特に当てはまる。インタネットは情報を共用する手段として構築されているため、もともとインタネット内にはセキュリティ手段がほとんどない。インタネットを介して情報を送信すると、ある離れたデータ転送点にいる未知の人が情報にアクセスできるため、データが盗まれる可能性が増大する。したがって、ユーザ-1がインタネットの性質を知っており、それにもかかわらずｅメールを使用するときに、必要な意図を示すことは困難である。

【００３２】

標準ｅメール・ソフトウェアを用いてｅメール・メッセージを作成する際、通常、このソフトウェアはｅメールに付加できるいくつかの属性を与える。通常、グラフィカル・ユーザ・インタフェース（GUI）は、ｅメールに付加することのできる特性、機能、および属性を表すいくつかのボタンを備えている。たとえば、ｅメールは、郵便の返信と同様な返信と共に作成することができる。受信者がこのｅメールを開くと、ｅメールが開かれたことを送信者に通知するｅメール通知が送信者に送り返される。さらに、ｅメールを低優先順位または高優先順位で送信することも、メッセージに、追跡ができるようにフラグを付けることも、メッセージを後で供給できるように設定することもできる。特定の属性を選択するときは、マウスを用いてボタンをクリックすることなどにより、入力装置を用いてGUI上で、この属性に対応するボタンが選択される。

【００３３】

ｅメールの受信者を環境設定する場合、ユーザは、「To:」という名称の、GUIにおける

テキスト・ボックスに、目的の受信者のｅメール・アドレスのリストを記入する。コピーの受信者用に「cc:」ボックスも与えられ、ｅメールの主題用の行も与えられる。ユーザは次いで、ｅメールの本文を書き込み、必要に応じてデジタル文書を添付し、eメール向けの任意の属性を選択し、GUIにおける「送信」ボタンをクリックすることによってｅメールを送信する。ｅメールおよびあらゆる添付文書は、目的の受信者にルーティングされる前にメール・サーバに送信される。

【００３４】

本発明によるｅメール・システムでは、新しいｅメールを作成するための「特権」ボックスがGUIに設けられている。「特権」ボックスが選択されると、「To:」ボックス内のユーザは、ｅメール・アドレス指定の特権配信リストを形成する。特権配信リストはたとえば、特定の法律事務所または法律部門の代理人のｅメール・アドレスを含んでよい。ｅメール・アドレスにおける受信者は、唯一の、特権ｅメールの許可された宛先であり、代理人－依頼人特権が適用される当事者のみを含むべきである。実際、特権ｅメールがその目的の受信者を超えず、したがって特権を維持するように、制限された転送が行われる。

【００３５】

本発明の他の局面では、ｅメールの作成者は、ｅメールの受信者に特定のアクセス権を与える。各特権ｅメールのアクセス権を環境設定するための「アクセス権」ウィンドウまたはツール・メニューが設けられている。このウィンドウでは、目的の受信者の特権配信リストが、検討および修正できるようにユーザに示される。修正が不要である場合、ユーザは配信リストを検証し、ｅメールの作成者の決定に応じてｅメールを特定の方法で処理するアクセス権を各受信者に与える。

【００３６】

たとえば、アクセス権は、転送、コピー、切取り、および貼付けを含んでよい。応答および応答に対するコピーは常に通常許可されるが、制限された転送を維持するために、応答の受信者はプルダウン・メニューを介して配信リストから選択される。転送権によって、ユーザは、ｅメールの作成者によって決定される特定のユーザにｅメールを転送することができる。受信者が特権ｅメールを転送する際、システムは、転送受信者を選択できるように特権配信リストを与える。たとえば、ｅメールを上級管理者に送信する代理人は、この管理者に、その従業員への転送権を与え、したがって、管理者は、その部内での転送を制限するために代理人によって最初に課された制約に従ってｅメールを誰に転送すべきかを決定することができる。管理者がｅメールを転送する際、システムは、管理者がｅメール・アドレスを入力することを許容しない。その代わり、ｅメール・アドレスは特権配信リストから選択される。

【００３７】

この実施形態の他の局面によれば、ユーザは「自動」転送受信者を指定することができる。たとえば、代理人はその助手が、代理人が受信する各ｅメールのコピーを自動的に受信することを望むことがある。これを行うには、この助手を代理人の自動転送受信者としてｅメール・システムに事前に登録することができる。ある実施形態では、この事前登録および自動転送をｅメールの送信者に対して完全に透過的に行うことができる。代理人－依頼人特権通信の場合、システムは、自動転送機能を、システム上に代理人として登録されているユーザに制限することができる。

【００３８】

本発明の代理人－依頼人特権実施形態の他の態様によれば、システムは、代理人ユーザが「From」フィールドまたは「To」フィールドに存在しないかぎり特権属性を有するｅメール・メッセージの送信を拒否することができる。

【００３９】

コピー権によって、ユーザはディスクまたは他の記憶装置に対してｅメールのコピーを作成することができる。切取り・貼付け権によって、ユーザはｅメール・コンテントを切り取り、他の文書に貼り付けることができる。切取り・貼付け権は、それによって特権材料をシステムの影響を受けないようにすることができるので、選択的に許可すべきであり

、好ましくは、代理人、上級管理者、および送信者が信用している受信者にのみ許可される。特権ｅメールの添付文書も、システム・アクセス権による制御を受ける。

【００４０】

アクセス権が環境設定された後、特権配信リスト、リスト内の各受信者用のアクセス権、ならびに配信リストおよびアクセス権を修正するためのパスワードのような、ｅメールに固有の他の情報を含む対応する特権プロファイルが作成される。このプロファイルをｅメールと共にパッケージングしても、ｅメールとは別に作成し中央サーバ上に記憶してもよい。ユーザが「送信」をクリックすると、ｅメールがメール・サーバに送信される。

【００４１】

たとえば、ユーザ-1が、「To:」テキスト・ボックスにユーザ-2およびユーザ-3を含む配信リストを含むｅメールを作成すると仮定する。ユーザ-1は、特権配信リスト内のすべてのアドレスに対する転送権をユーザ-2に許可し、ユーザ-3にはどの権利も許可しない。ｅメールを転送する権利を持つユーザ-2、および常に通常許可されるｅメールを見る権利以外の権利を持たないユーザ-3を含む特権配信リストがシステムによって作成される。この場合、ユーザ-2は、ユーザ-1に応答することができ、かつユーザ-3が特権リストに含まれており、したがって応答を受信する特権を持っているのでユーザ-3にコピーを送信することができる。しかし、ユーザ-2は、eメールや、応答のような、eメールに関係するものをユーザ-4に転送することはできない。というのは、ユーザ-4がこの特定のeメールに対する権利を有さないからである。ユーザ-3は、ユーザ-1に応答することができるが、eメールやその応答をどのユーザにも転送することができない。なぜならユーザ-3はどの権利も有さないからである。

【００４２】

あるいは、特権配信リストおよびアクセス権は、管理エンティティによって設定されたある所定の基準に従ってシステムによって自動的に作成し構成することができる。たとえば、大企業の社内弁護士は、法律部門からのすべての着信eメールおよび発信eメールにこのシステムの下である権利を許可することなど、ある文書に代理人－依頼人特権を確実に適用する機密性方針を作成することができる。権利は、さらに、各個人に許可することも、社内の地位または部署に応じて許可することもできる。会社の社長にすべての権利を許可し、副社長に転送権およびコピー権を許可し、責任者に転送権を許可し、従業員には権利を一切許可しない（読取りおよび応答）ようにすることができる。eメールのルーティングをグループ、部署、または企業に制限することができる。

【００４３】

eメールが作成された後、特権プロファイルを修正することが望ましい場合がある。このために、各特権eメールごとに固有のパスワードを作成することができる。パスワードは、eメールの特権プロファイルを作成するあらゆる人に発行される。システムがeメール特権プロファイルを構成すると、管理エンティティは、システムの下で作成されたすべてのeメールを修正できるマスタ・パスワードにアクセスすることができる。あるいは、マスタ・パスワードは、システムによって維持されているパスワード・データベースへのアクセスを許可することができる。システムによってeメールが作成されるたびに、その固有のパスワードがデータベースに記録され、eメールIDと関連付けされる。特定のeメールの特権プロファイルを修正する場合、システムの管理者はマスタ・パスワードおよびeメールのIDを用いてデータベースにアクセスし、特定のeメールに割り当てられた固有のパスワードを検索して特権プロファイルを修正する。

【００４４】

さらに、システムは自動的に、各eメールと共に機密性通知を含む。この通知は、通信が機密扱いされており、eメールを読み取ることができるのが目的の受信者だけであることを、eメールを見ているユーザに知らせるために、eメールが開かれるたびに表示される。好ましくは、eメールのコンテントは、ユーザが機密性通知に合意するボックスにクリックするまで表示されない。したがって、eメールを見ているユーザが目的の受信者の1人でない場合に、特権関係を持たない人が特権情報にアクセスできることをeメールの作成

者が意図したと推論することはできないため、機密性を維持する意図はさらに確証される。例示的な通知を以下に示す。
「この通信は特権付きで機密扱いです。
このeメールおよびそのあらゆる添付文書は、そこに指定されているアドレスによってのみ使用されるものです。このeメールの目的の受信者ではない場合、このeメールおよびそのあらゆる添付文書の読取り、伝搬、配信、コピーが堅く禁じられていることをこの通知によってお知らせします。誤ってこのeメールを受信した場合は、直ちに送信者に知らせ、あらゆるeメールのオリジナルおよびあらゆるコピーならびにそのプリントアウトを永久的に削除してください。」

【００４５】

さらに、eメールに対して講じられたすべての処置を追跡する証跡ファイルが各特権eメールごとに作成される。この証跡ファイルは、eメールがアクセスされるたびに更新される。このファイルは、開くこと、転送、コピー、応答、カーボン・コピー応答、切取りおよび貼付けのようなeメールに対して講じられたあらゆる処置の記録を維持する。

【００４６】

アクセス権を含む特権配信リストは、特権eメールの特権プロファイルを含んでいる。このプロファイルは、特権eメールの特権条件に関するすべての情報、すなわち、特権配信リストや各ユーザに許可されている権利を含んでいる。このプロファイルは、eメールとは別に作成し維持しても、eメールと共にパッケージングしてもよい。

【００４７】

セキュリティを高めるために、特権eメールおよびそのプロファイルを、公衆通信回線上で送信される前にシステムによって符号化することができる。

【００４８】

本発明の上記の機能は、不慮の開示を防止し、機密性を維持して代理人－依頼人特権の通信への適用を維持するための予防策が取られたことの証拠となるものである。

【００４９】

特権eメールを作成するプロセスが図2に示されている。ユーザが「特権」条件を選択する（ステップ50）と、システムは「To:」テキスト・ボックス内の受信者eメール・アドレスから特権配信リストを作成する（ステップ52）。アクセス権が構成され（ステップ54）、次いで検証できるようにユーザに示される（ステップ56）。配信リストまたはアクセス権を訂正する必要がある場合、ユーザはアクセス権の構成（ステップ54）に戻される。配信リストおよびアクセス権が正しい場合、システムはこのeメール用の特権プロファイルを作成する（ステップ58）。固有のパスワードが生成され、ある中央データ記憶装置上に記憶される（ステップ60）。eメールはパッケージングされ送信される（ステップ62）。

【００５０】

あるいは、最初に特権eメールとして作成されなかったeメールを受信者によってそのようなステータスに一致させることができる。法人弁護士などの受信者は、作成時に特権条件を与えられなかったeメールを受信したが、そのeメールに特権を与えるべきであると判定した場合、そのeメールをさらに伝搬する前にそのeメールに特権を与えることができる。さらに、システムは、このeメールの発信者とその最初の受信者に新しい特権条件を知らせるように環境設定することができる。さらに、最初のeメールがサーバから取り出され、メモリ内の最初の記憶場所から削除され、特権eメール用の離れた記憶位置に再配置される。

【００５１】

サーバ・ベースの特権eメール・システム

本発明の第1の実施形態は、クライアント装置上に存在するクライアント・ソフトウェア・オブジェクトと、メール・サーバ上に存在するサーバ・ソフトウェア・オブジェクトとを含んでいる。この2つのオブジェクトは、一般に知られているようにネットワーク接続を介して通信する。クライアント・オブジェクトは、ユーザと対話して特権eメールおよびそれに対応するプロファイルを作成するGUIを実現する。クライアント・オブジェク

トはまた、eメールを対応する特権プロファイルと一緒にメール・サーバに送信し、必要に応じて暗号化および復号を行う。サーバ・オブジェクトは、特権eメールをサーバのデータ記憶装置上の離れた位置に維持し、特権eメールへのアクセスを制御し、暗号化が使用されるときに暗号化を管理する。

【００５２】

オブジェクトは、どんな種類のソフトウェア・アーキテクチャの下でも構成することができ、「オブジェクト」という語の使用は、システムをオブジェクト指向プログラミング言語の下での実施に制限することを意味するものではない。

【００５３】

クライアント・オブジェクトは、既存のeメール・プラットフォーム用のプラグインであっても、本発明によるeメール・ソフトウェア・パッケージのクライアント・バージョンであってもよい。プラグインは、Microsoft OutlookやLotus Notesのような既存のeメール・システム上にインストールされ追加される。プラグインは、インストールされると、既存のGUI上に「特権」ボタンを付加し、したがって、このボタンがクリックされると、システムはユーザと対話してeメールおよび特権プロファイルを作成し、eメールをプロファイルおよびあらゆる添付文書と共にシステム・サーバに送信する。

【００５４】

特権eメールの受信者も、サーバと通信し特権eメールをダウンロードするためにプラグインを有する必要がある。受信者のクライアント・オブジェクトは、eメールを必要な機密通知と共に表示し、復号を実行する。クライアント・オブジェクトは、受信側で特権プロファイルを実施することもできる。

【００５５】

ユーザが特権属性を選択し、特権eメールを作成すると、クライアント・オブジェクトによってeメールにフラグが付けられ、eメールはサーバに送信され、したがって、サーバ・オブジェクトは、eメールを受信者に送信する前に、特権条件を検出し、特権eメールを、サーバ・オブジェクトの記憶装置上の「特権」フォルダのような離れた位置に記憶する。好ましくは、すべてのコピー、および添付文書のような特権eメールの関連文書が同じ位置に記憶される。

【００５６】

他の実施形態では、離れた位置は、eメールのルーティングに用いられるメール・サーバ以外のサーバ上に存在する。この実施形態では、各eメールのコピーは、離れたサーバ、すなわち、離れた位置を有するサーバに送信される。これはたとえば、特権eメールが送信されるとき必ず離れたサーバにブラインド・カーボン・コピー（bcc）を送信することによって、実施することができる。この実施形態は、特権通信の発信者が、専用eメール・サーバを用いずに直接インタネット上でeメールを送信するスタンドアロン・クライアント・コンピュータを使用しているとき特に有用である。

【００５７】

他の実施形態によれば、離れた位置は、コンピュータによって送信されたすべての特権eメールのコピーを記憶するために、eメールを送信するコンピュータ上に存在する。これは、上述の分離サーバ実施形態とは別に行っても、この分離サーバ実施形態と組み合わせて行ってもよい。

【００５８】

離れた位置は、いくつかの方法で構成することができる。eメールは、特権eメールが有する可能性のある共通の特性に基づいて、送信者、受信者、企業の部署、法律の分野、または任意の他の分類に基づいてグループ分けすることができる。

【００５９】

ある管理エンティティには、離れた位置全体へのアクセスを可能にすることができる。アクセスは、マスタ・パスワードによって制御することができ、また、ネットワーク・ステータスによって許可することも、すなわち、管理者のみに許可することもできる。

【００６０】

サーバ・オブジェクトは、各特権eメールの受信時にこの特権eメール用の監査ファイルを作成する。サーバは、あらゆるアクセス要求およびeメールに対して講じられたあらゆる処置のログを各eメールの対応する監査ファイル内に維持する。許可されたクライアント・オブジェクトに特権eメールが送信される際、クライアント・オブジェクトによってeメールに対して講じられたすべての処置による更新のために証跡ファイルのコピーがeメールと共に送信される。

【００６１】

暗号化が用いられる場合、暗号化は、eメールが転送時に暗号化されるように好ましくはクライアント・オブジェクトによって行われる。各eメールのキーは、各eメールの対応する特権プロファイルに記憶するか、またはサーバに記憶することができる。サーバ上に維持される場合は、キー自体を、それに対応するeメールと共に送信される前に暗号化することができる。

【００６２】

eメールは、作成されサーバに送信された後、受信者によって取り出されるサーバのデータ記憶装置上に存在する。

【００６３】

eメールがサーバ・オブジェクトに送信されると、サーバは、このeメールの対応する特権プロファイルにアクセスしてeメールの受信者を判定し、受信者のeメール装置上の対応するクライアント・オブジェクトに通知を送信する。この通知は、クライアント・オブジェクトによってeメール・システム用のGUIを通じてユーザに与えられる。ユーザが、新しいメールを見るためのアイコンを選択すると、ユーザのアカウント内のeメールの概要が、特権条件を表す何らかのグラフィカル・マーキングと共に示される。ユーザは、eメールを見たい場合、それに対応するグラフィカル表現アイコンをクリックする。クライアント・オブジェクトは、特権eメールへのアクセスを求める要求をサーバ・オブジェクトに送信する。サーバは、この要求を受信すると、その送信元を調べ、特定のeメールにアクセスし、特権プロファイルを調べ、アクセスを許可すべきかどうかを判定する。アクセスを許可すべきでない場合、ユーザがそのeメールに対する権利を有していないことがユーザに通知される。ユーザが配信リスト内の特権ユーザの1人である場合、eメールは特権ファイルおよび証跡と共にクライアント・オブジェクトに送信される。

【００６４】

あるいは、クライアント・オブジェクトはサーバ・オブジェクトと対話し、eメールのコンテントをクライアント装置にダウンロードせずにeメールを表示することができる。公知のように、クライアント・オブジェクトを用いてネットワーク接続を介してサーバ・オブジェクト上でeメールを見ることができる。サーバ・オブジェクトは、クライアント・オブジェクトからの要求を受け入れ、表示、転送、コピー、eメールに対して講じることのできる任意の他の処置などの処置をeメールに対して講じる。

【００６５】

eメールに対して講じられた処置はシステム・オブジェクトを通過し、したがって、添付文書を含むeメールのコンテントの処理を管理することによって、あらゆる許可されない処置を防止することができる。eメールにアクセスするかまたはeメールに対して処置を講じるために、システム・オブジェクト（システムの環境設定に応じて、たとえばクライアント・オブジェクトやサーバ・オブジェクト）に要求が発行される。システム・オブジェクトは、特定の要求されたeメールにアクセスし、その対応する特権プロファイルを読み取り、アクセスを要求しているユーザが特権を持っているかどうかを検証する。要求側のユーザが特権を有する場合、転送やコピーのような要求された処置が許可される。

【００６６】

機密性通知を表示すると共に、eメールのコンテントを表示する前に「OK」ボタンをクリックすることのような何らかのユーザ処置による通知の肯定応答を必ず行わせることが望ましい。ユーザが機密性通知に対して肯定応答しなかった場合、アクセスは拒否され、ユーザは通知を受け、クライアント・オブジェクトはeメールを閉じる。クライアント・

オブジェクトはさらに、受信者がeメールの機密性に対して肯定応答するのを拒否した旨の通知をサーバに送信することができる。サーバ・オブジェクトはeメールの作成者に対して通知を行う。

【００６７】

受信者が機密性通知に合意した場合、クライアント・オブジェクトは、eメールの特権プロファイルを読み取り、eメールをシステムGUIを介してユーザに表示する。eメールに対して講じられるすべての処置はクライアント・オブジェクトを通じて行われる。たとえば、ユーザがeメールに対してカーボン・コピーで応答する場合、コピーの受信者は、特権関係を有さない受信者にeメールが送信されるのを妨げるように特権配信リストから選択される。eメールの転送も同様に行われ、受信者は、「To:」ボックスに受信者を入力するのではなく特権受信者のメニューから選択される。

【００６８】

サーバ・ベースのシステムの他の実施形態によれば、中央サーバは、各種のeメール・プラットフォーム、すなわち、Lotus Notes、Microsoft Outlook用のインタフェースを有するシステムの下ですべてのeメールを記憶することができる。

【００６９】

eメール・メッセージに埋め込まれた実行可能モジュール

本発明の第2の実施形態によれば、引用によってその全体が本明細書に組み込まれる「自己破壊文書およびeメール・メッセージ交換システム（Self-Destructing Document and E-mail Messaging System）」国際公開公報第98/58321号で開示された実行可能モジュールをeメールに付加する特権eメール・システムが提供される。

【００７０】

第2の実施形態は、好ましくはeメール・システムのクライアント装置上に存在するプラグインであるソフトウェア・オブジェクトによって、既存のeメール・システム上で実施することができる。このオブジェクトは、独立して働き、サーバ・バージョンと共に働くことはない。また、この実施形態では本発明の各オブジェクト間の通信は必要とされない。さらに、付加される実行可能モジュールは、ユーザの、eメールによってイネーブルされる装置上のオペレーティング・システムとは無関係に実行できるようにプラットフォームから独立すべきであるため、受信者がシステム・プラグインを有する必要はない。

【００７１】

プラグイン・オブジェクトは、既存のeメール・パッケージにインストールされ追加されると、既存のeメール・ソフトウェア・インタフェース上にシステム用のGUIを追加する。新しいeメールを作成するための「特権」ボックスが既存のウィンドウに挿入される。ユーザが、前述のように新しいeメールを作成し特権属性を選択すると、プラグインが後を引き継ぎ、eメールの特権プロファイルを環境設定するためのシステムGUIを表示する。

【００７２】

ユーザがeメールを送信する際、プラグインは、プロファイル内のアクセス権および配信を実施し、すなわち、プロファイル内に指定された人にのみアクセスおよび権利を許可するようにプログラムされた実行可能モジュールを作成する。証跡ファイルにも、実行可能モジュールと、対応するパスワードを含む修正機能とが含められる。eメールは、既存のシステムによって通常どおりに送信され、受信者によって取り出されるまでシステムのサーバ上に存在する。

【００７３】

受信者がeメールを開くと、モジュールが実行され、ユーザがeメールを読み取れるようにするインタフェースを与える。eメールにアクセスするか、または他の処置を講じることを求める要求は、実行可能モジュールを通過する。この処置が特権プロファイルによって許可されていることを検証するために、あらゆる要求に対して特権プロファイルがアクセスされる。制限されている処置が試みられた場合、ユーザにこの制限が通知され、実行可能モジュールはeメールを閉じる。許可されている処置が要求された場合、機密性通知が表示され、肯定応答された後、モジュールは、要求された処置、たとえば、eメールの

表示、転送、コピーや、プロファイルによって許可されている任意の他の処置を実行する。

【００７４】

特権eメールを、付加された実行可能モジュールと共に、システム・プラグインを持たないクライアント装置から複数の受信者に転送する際、モジュール自体が、転送される各eメールに付加される他の実行可能モジュールを作成する。

【００７５】

付加された実行可能モジュールは、eメールへのアクセスおよびeメールの転送を制限する。さらに、上述の特権eメールによる実行可能モジュールは、ユーザが、たとえば、アクセスおよび転送を制限する実行可能モジュールを実行できないアプリケーションを用いて特権eメールを開くことによって、アクセス制御機構を破るのを、暗号化技術を用いて防止することもできる。このような実施形態によれば、eメールがまず保存されるかまたは閉じられるときに、実行可能モジュールはeメールを暗号化する。次いで、eメールがその後開かれるとき、実行可能モジュールは、ユーザがアクセス制御機構の下でアクセス権を有する場合にのみeメールを復号する。さらに、実行可能モジュールを実行できないアプリケーションを用いてeメールが開かれた場合、eメールは暗号化されたままであり、ユーザはeメールを見ることができない。適切な暗号化技術をどのように選択するかは、所望のセキュリティの程度、およびそれを実施するのに用いられるマクロまたはスクリプトの能力に依存する。

【００７６】

機能を様々なプラットフォームに対応できるようにするために、複数の実行可能モジュールをeメールに付加することができ、その場合、各モジュールを異なるeメール・システムによって実行することができる。たとえば、eメールは、第1のシステムによって実行できる第1のモジュールと、第2のシステムによって実行できる第2のモジュールとを含んでよい。eメール自体がいずれかのシステムの影響を受けることができる。この実施形態によれば、eメールに対する特権プロファイルはeメールが第1のシステムによって開かれるか、それとも第2のシステムによって開かれるかにかかわらずに実施される。

【００７７】

仮想コンテナ

本発明の第3の実施形態によれば、eメールは、引用によってその全体が本明細書に組み込まれる「自己破壊文書およびeメール・メッセージ交換システム（Self-Destructing Document and E-mail Messaging System）」国際公開公報第98/58321号で開示された仮想コンテナに入れられる。

【００７８】

この実施形態も好ましくは、既存のeメール・システム用のプラグインによいって実施される。プラグインは、コンテナ・クリエータ・ユーティリティおよびコンテナ・オープナ・ユーティリティと、ユーザと対話するシステムGUIとを備えている。

【００７９】

プラグインは、上述のように既存のGUIを通じてユーザと対話し、特権eメールを作成する。アクセス権は、前述のように特権プロファイルとして構成され、特権eメールと共に仮想コンテナに「入れられる」。コンテナ・クリエータ・ユーティリティは、コンテナを作成し、eメールおよびその特権プロファイルを、修正パスワードのような任意の他の関連情報と共にコンテナに入れる。eメールは次いで、既存のシステムによって通常どおりに特権受信者に送信される。

【００８０】

受信者が特権eメールを開くと、コンテナ・オープナは、受信者の権限を検証して特権eメールにアクセスする。eメールへのアクセスを求める要求が、特権配信リスト内にeメール・アドレスを有するユーザからの要求である場合、コンテナ・オープナは、eメールを抽出し、システムGUIを通じて機密性通知と共に表示する。しかし、ユーザがeメールにアクセスする特権を有していない場合、コンテナ・オープナは、eメール・アプリケーショ

ンへのアクセスを拒否する。このようにして、コンテナ・オープナ・ユーティリティは、特権プロファイルを実施し、すべてのアクセス要求に対処するか、または対応するコンテン内のeメールに対して他の処置を講じる。コンテナ・オープナは、前述の実施形態による実行可能モジュールとしてコンテナに付加しても、eメール・ソフトウェアのプラグインとしてクライアント装置上にインストールしてもよい。

【００８１】

eメールへのアクセスを試みているユーザが特権配信リストに含まれている場合、システムは、ユーザはeメールにアクセスするのを許可する前に、ユーザに許可されている権利をプロファイルから読み取る。ユーザが特権リストに含まれていない場合、アクセスは拒否され、ユーザがeメールにアクセスできないことがユーザに通知される。

【００８２】

上述の実施形態のうちのどれでも、システムは、ユーザが、eメールの特権プロファイル内のユーザに許可されている権利に従ってeメールに作用し、それによってeメールのコンテントのあらゆる処理を制御するのを可能にするに過ぎない。ユーザがeメールを転送する権利を有する場合、転送が許可され、システムによって特権アドレスのみに対して実行される。eメールに対して処置を講じることができるのは、ユーザが権利を有するときだけである。ユーザが特権を有さないeメールに対して処置を講じようとすると、制限を受け、ユーザに通知が与えられる。好ましくは、特権eメールを転送する際、ユーザは宛先eメール・アドレスを入力しない。配信リストを含むメニューから選択が行われる。

【００８３】

本発明のそれぞれの異なる実施形態を組み合わせることができる。サーバ・ベースの実施形態では、ディスクにコピーされたeメールや、特権eメールから切り取られ貼り付けられたマテリアルのような、システムから取り出された任意のコンテントに実行可能モジュールを付加することができる。あるいは、システムから取り出されたコンテントを本発明による仮想コンテナに入れることができる。

【００８４】

本発明の他の実施形態によれば、本発明の様々な実施形態に関して上記で説明したコンピュータで実行可能なプロセス・ステップが記憶されたコンピュータ可読媒体が提供される。

【００８５】

前述の明細書では、本発明をその具体的で例示的な実施形態を参照して説明した。しかし、特許請求の範囲に記載された本発明のより広義の趣旨および範囲から逸脱せずに、これらの実施形態に様々な修正および変更を加えられることが明白であろう。したがって、明細書および図面は、制限的なものではなく例示的なものとみなすべきである。

【図面の簡単な説明】

【００８６】

【図１】本発明を実施できる例示的な従来技術の環境を示す図である。

【図２】本発明による特権eメールを作成する際に実行されるステップの流れ図である。

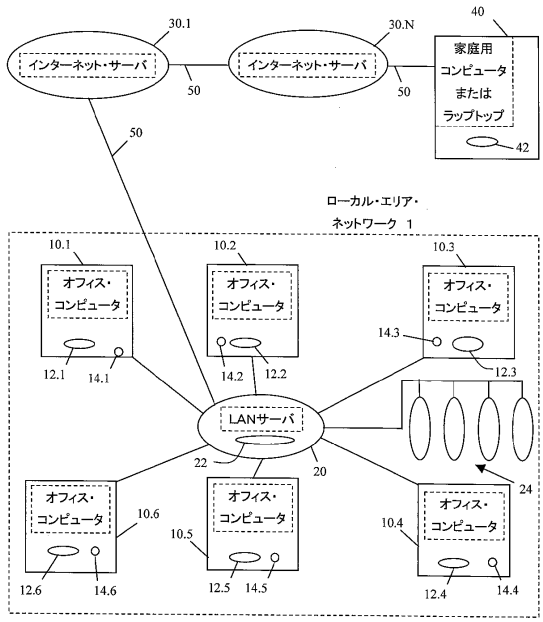
【符号の説明】

【００８７】

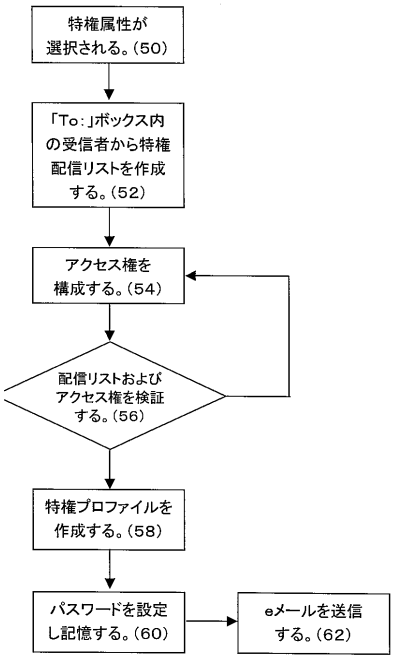
1　ローカル・エリア・ネットワーク
10.1～10.6　オフィス・コンピュータ
12.1～12.6　一次記憶機構
14.1～14.6　二次記憶機構
20　サーバ
22　一次ネットワーク記憶機構
24　二次ネットワーク記憶気候
30.1～30.N　インタネット・サーバ
40　家庭用コンピュータまたはラップトップ
42　一次記憶機構

44　二次記憶機構
50　伝送回線

【図１】



【図２】



フロントページの続き

(72)発明者　ストラスバーガー，フィリップ，シー.
アメリカ合衆国　０６９０５　コネチカット州，スタンフォード，イースト　レーン　１２３
(72)発明者　ベイカー，スチュアート，ディー.
アメリカ合衆国　１００２２　ニューヨーク州，ニューヨーク，サットン　プレース　１６，アパートメント　ナンバー１２シー

合議体
審判長　和田　志郎
審判官　清水　稔
審判官　中野　裕二

(56)参考文献　特開２０００－２３１５２３（ＪＰ，Ａ）
特開２００１－５６７９７（ＪＰ，Ａ）
特開２０００－２８６８８４（ＪＰ，Ａ）
特開平９－２５２３１８（ＪＰ，Ａ）
特開２０００－１１３０６６（ＪＰ，Ａ）
特開平１０－１３３９７２（ＪＰ，Ａ）
特表２０００－５０１５４０（ＪＰ，Ａ）
特開平１１－１７５３４２（ＪＰ，Ａ）
特開平４－１０４５４１（ＪＰ，Ａ）
特開昭６０－８５６４７（ＪＰ，Ａ）
特開平９－２５２３１８（ＪＰ，Ａ）
西村裕、「盗み見、のぞき見からプライバシーを守る　誰でも使える暗号化メール」、日経パソコン、第３４４号、日経ＢＰ社、１９９６年9月6日発行、ｐ．１５０－１５９

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F 13/00, H04L 12/58