(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5934808号
(P5934808)
(45)発行日　平成28年6月15日(2016.6.15)　(24)登録日　平成28年5月13日(2016.5.13)

(51)Int.Cl.		F I		
H04L 12/58	(2006.01)	H04L	12/58	100Z
G06F 13/00	(2006.01)	G06F	13/00	610A
H04L 9/32	(2006.01)	H04L	9/00	675B

請求項の数 7　(全 10 頁)

(21)出願番号	特願2014-555270 (P2014-555270)
(86)(22)出願日	平成25年2月19日 (2013.2.19)
(65)公表番号	特表2015-513236 (P2015-513236A)
(43)公表日	平成27年4月30日 (2015.4.30)
(86)国際出願番号	PCT/ES2013/070104
(87)国際公開番号	WO2013/124511
(87)国際公開日	平成25年8月29日 (2013.8.29)
審査請求日	平成26年7月31日 (2014.7.31)
(31)優先権主張番号	12382060.7
(32)優先日	平成24年2月21日 (2012.2.21)
(33)優先権主張国	欧州特許庁 (EP)

(73)特許権者　514167101
レリダネットワークス　セルヴェイス　テレマティクス　エセ．アー．
スペイン，エー－２５００３　レリダ，パルケ　テクノロギコ　アグロアリメンタリオ，エディフィシオ　アチェ１，セグンダ　プランタ
(74)代理人　110000338
特許業務法人HARAKENZO WORLD PATENT & TRADEMARK

最終頁に続く

(54)【発明の名称】電子メール送信の証明方法

(57)【特許請求の範囲】
【請求項１】
送信者であるユーザ（１）から受信者（２）への電子メール送達の証明方法であって、
上記ユーザ（１）および上記受信者（２）の両方によって利用可能である遠距離通信プロバイダである電子メール送達のための証明システムにて実行するステップを含み、
上記ユーザ（１）は電子メール送達のための上記証明システムのクライアントであり、
電子メール送達のための上記証明システムは、相互接続された、
少なくとも到来メールサーバ（１１）として動作するデータの処理ユニット（１１）と、
差出メールサーバ（１４）と、
を少なくとも含み、
上記証明方法は、
（ｉ）第１のメールサーバ（５）および送信先メールサーバ（６）によって第１のルート（３）を介して、上記受信者（２）の少なくとも１つの送信先電子アドレスに上記ユーザからの第１の電子メールを送信するステップと、
（ｉｉ）上記ユーザ（１）から、前のステップにて送信された上記第１の電子メールのコピーを、第２のルート（１０）を介して電子メール送達のための上記証明システムに送信するステップと、
（ｉｉｉ）上記証明システムの上記到来メールサーバ（１１）にて上記第１の電子メールの上記コピーを受信するステップと、

（ｉｖ）上記処理ユニット（１１）によって、上記第１の電子メールの上記コピーに特定の指示を挿入するステップと、
（ｖ）上記特定の指示を含む上記第１の電子メールのコピーに電子署名を適用するステップと、
（ｖｉ）上記特定の指示および上記電子署名を含む上記第１の電子メールの上記コピーから第２の電子メールを生成するステップと、
（ｖｉｉ）上記差出メールサーバ（１４）に上記第２の電子メールを送信するステップと、
（ｖｉｉｉ）上記差出メールサーバ（１４）から上記送信先メールサーバ（６）に上記第２の電子メールを送達するステップと、
（ｉｘ）上記処理ユニット（１１）にて、上記送信先メールサーバ（６）から上記第２の電子メールの受信メッセージを受信するステップと、
（ｘ）上記処理ユニット（１１）にて、上記（ｉ）～上記（ｉｘ）のステップに関するデータを含む証明書を生成するステップと、
（ｘｉ）上記受信者（２）に、
（ａ）上記第１のルート（３）を介した上記第１の電子メールと、
（ｂ）上記第２のルート（１０）を介した上記第１の電子メールの上記コピーと、
を送達するステップと、を含み、
上記第１の電子メールの上記コピーは上記特定の指示を含み、上記特定の指示は証明された指示を含み、
（ｘｉｉ）上記処理ユニット（１１）から上記ユーザ（１）に上記証明書を送達するステップを含むことを特徴とする電子メール送達の証明方法。

【請求項２】
上記第１の電子メールの上記コピーをデータベース（１２）に記憶するステップをさらに含むことを特徴とする請求項１に記載の電子メール送達の証明方法。

【請求項３】
上記第１の電子メールの上記コピーをデータベース（１２）に記憶するステップの前に、上記処理ユニット（１１）は、少なくとも、出所、送信先、および添付データについて、上記第１の電子メールの上記コピーの分解を行うことを特徴とする請求項２に記載の電子メール送達の証明方法。

【請求項４】
上記処理ユニット（１１）はさらに、上記第１の電子メールの上記コピーが分解された要素のすべてに番号を付し、上記ユーザ（１）に上記番号を割り当てることを特徴とする請求項３に記載の電子メール送達の証明方法。

【請求項５】
上記特定の指示は、上記証明を示すテキストを含む証明書（４）であって、
上記ユーザ（１）に上記証明書（４）を送達する前に、上記差出メールサーバ（１４）は、第２の電子署名を実行するために第三者に電子文書を送信することを特徴とする請求項１から４のいずれか１項に記載の電子メール送達の証明方法。

【請求項６】
上記処理ユニット（１１）は、上記ユーザ（１）の口座から費用を回収することを特徴とする請求項１から５のいずれか１項に記載の電子メール送達の証明方法。

【請求項７】
上記証明システムにおいて、上記ユーザ（１）を認証するステップをさらに含むことを特徴とする請求項１から６のいずれか１項に記載の電子メール送達の証明方法。

【発明の詳細な説明】
【発明の詳細な説明】

【０００１】
本発明は、遠距離通信のオペレータが、送信ユーザから１以上の受信者に電子メールを受信、転送、送信し、全ての処理データの証明を生成し、最後に、電子的にメールにサイ

ンし、上記オペレータおよび信頼された第三者として、送信ユーザに証明書を提示する方法である。

【０００２】

〔背景技術〕

現在、電子通信は、合法および非合法のあらゆる操作に関して、重要かつ欠くことのできない手段になっていることが知られている。通信は、電話やメッセージの発生等、発信元から発信先への全ての種類の処理について使用されている。

【０００３】

遠距離通信オペレータは、このトラフィックの大部分を管理、指揮および蓄積する通信施設を提供する。これらの遠距離通信オペレータは、特に、限りのある無線スペクトルの使用に関して、または、限りのある電話番号リソースの使用に関して、規則に従う。

【０００４】

遠距離通信オペレータは、さらに、ユーザによって実行された処理の記録を、特に目的物の評価、ユーザに関する登録番号、請求書送付証明書、および、ユーザへの請求書送付に使用された任意の処理データの記録と共に保存する。これらの記録は、さらなる確認の評価のために、および／または、一部のユーザに関するトラフィックの追跡のために保護される。

【０００５】

時折、司法当局は、遠距離通信オペレータが実行した、記録された電子処理データの提供の目的に関して、遠距離通信オペレータを信頼された第三者であるとみなして、上記電子処理データに加えて、質問について応答した物理的または法上の人を特定するために役立つ任意のデータを遠距離通信オペレータに要求する。

【０００６】

しかしながら、遠距離通信オペレータに対して要求したデータの調査は、通常、大量の行動記録上で実行されるという事情により面倒であり、通常、データの痕跡の追跡よりも請求書の送付に向けて設計されている。それゆえ、上述の要求したデータの調査は、遠距離通信オペレータに関するリソースを大量に消費することになる。

【０００７】

司法当局によって要求されたデータが探し当てられると、オペレータは、要求された処理データ、回数、送信先および適切な司法当局によって要求された任意の情報が明示的に示されている証明書を発行する。

【０００８】

また、例えば、送信されたデータ、日付、受信データまたは任意の他のユーザにとって有用な情報などの処理データをユーザ自身が認識し、確認するために、ユーザの間でも、遠距離通信オペレータに対して情報を要求する能力を持つ必要性が上記と同様にある。この必要性は、第三者からユーザへの前述した処理データの要求によって誘導され得る。

【０００９】

従来、種々の方法およびシステムが、電子メールに含まれるデータのインテグリティだけでなく、送信の証明のための技術として知られている。これらの方法は一般的に、送信の証明を可能とする技術的な解決手段に基づく電子メールの送達および受信の証明、並びに、送信コンテンツおよび受信コンテンツを提供する。

【００１０】

しかしながら、従来技術における方法において、メッセージのコンテンツが変更され、サーバに記憶された電子署名と、生成された文書ファイルの電子署名とを比較する必要があるアルゴリズムおよび証明を実行するためには問題がある。このサービスを要求するいくつかの第三者にとって問題があるこれらの証明は、電子的にオンラインで行われる。

【００１１】

上記の目的のために、送信ユーザが電子メールメッセージの証明を望む場合、上記メッセージは、受信者への送達のための従来のルートに代えて、証明者のサーバを介して受信者にメッセージを送達するルートである第２のルートを通る。しかしながら、この方法は

、最終的にメッセージを受信した受信者が、送信者によって送信されたオリジナルのメッセージでなく、証明者によって変容させられたメッセージを受信するため、メッセージが証明者のサーバを介しての送達中に改竄されるという問題がある。

【００１２】

さらに、従来技術における方法は、各メッセージに適合する唯一の暗号アルゴリズム、すなわち電子署名を有している。その後、メッセージが証明される必要がある場合、生成された文書ファイルの電子署名は、証明者のサーバに記憶されている電子署名と比較され、比較アルゴリズムが、従来技術におけるシステムによって生成され記憶されるデータである暗号アルゴリズムの実行と、比較アルゴリズムを用いて実行される上記比較との間に生成される。

【００１３】

受信者への送達証明が必要とされる特別の場合のように、生成ユーザによって発行された請求書が送達されて、受信者へサービスまたは商品を供給した後に、受信ユーザがそれらのサービスについての請求書を受け取ることを見せることができる。それゆえ、商品またはサービスを受け取った受信ユーザがそれらの支払いを避けるまたは遅らせるために、対応する請求書を受け取っていないことを主張することを防ぐことができる。

【００１４】

電報、事務所ファックスまたは書留のような、公的な通知のための従来技術における方法は、工程の非機械化、その結果として消費時間の増大および高コストのようないくつかの問題がある。例えば、ＵＳ２００７１７４４０２は、サーバが送信先アドレスに送信者からのメッセージを送信する、電子メールの送達およびインテグリティを証明するシステムおよび方法について開示している。送信中に、サーバおよび送信先アドレスは、メッセージ、サーバ、および送信先アドレスに関し、ＳＭＴＰプロコトルおよびＥＳＭＴＰプロコトルのうちの特定の１つを介し、添付物を構成するダイアログを有する。メッセージは、サーバおよび送信先アドレスの間にあるサーバ群を通る。この経路は添付物に含まれている。メッセージおよび添付ファイルに対して認証機が提供される。認証機は、メッセージおよび添付物の暗号化されたハッシュを構成してもよい。送信者は、認証の前にサーバからメッセージ、添付物、および証明書を受信し、サーバからの認証を得るために、メッセージ、添付書、および証明書をサーバに送信する。サーバは、メッセージおよびメッセージの証明書を操作することによってメッセージを認証し、添付物および添付物の証明書を操作することによって添付物を認証する。ＵＳ２００８２７８７４０には、複数の送達メディアを介して、受信者に対して情報を大量に通信するための方法、システム、およびコンピュータプログラムが開示されている。メディアは、ファクシミリ、電子メール、郵便、ＳＭＳメッセージ、およびアーカイブを含む（さらに、メディアは将来の新しいメディアにも適合する）。単一のインターフェースは、１以上のテンプレート文書および各受信者に固有のデータを含む配布物のための情報を受信するために使用される。少なくとも、受信した情報に基づく文書が、受信者の送達の優先度に基づく各受信者のための特定の送達を通じて、送信される。文書の送信の拡大が、特定の送達メディアによる送信を失敗した受信者による異なる送達メディアの使用を引き起こしてもよい。拡大ステップは、各受信者への文書の送達に関するキャリアからのステータス情報に依存してもよい。ＵＳ５８１５５５５には、電話ネットワークを介した、送信された電子メールの送達証明方法が開示されている。上記方法は、電話ネットワークのコントローラによる、送信元のコンピュータから送信先のコンピュータへの電子メールの証明要求を検出するステップと、コントローラに送信された電子メールのコピーを記憶するステップとを含む。上記方法はさらに、記憶されたコピーと、送信先のコンピュータによって受信された、送信された電子メールのコピーとが一致するかによって、送信された電子メールの送達証明を行うステップを含む。最後に、ＵＳ２００４１７７０４８は、通信のソーティング、優先順位付け、特定、管理、およびその他には制御（これらをまとめて、通信の「制御」と呼ぶ）のための方法および装置を開示する。フランク（Ｆｒａｎｋ、署名）が、通信と価値および等級とを関連付けるために使用されてもよい。通信は、複数のフランクタイプの中から価値と関

連付けられたフランクを選択する方法を通じてフランクと関連付けられてもよい。上記フランクタイプの各々は、予め割り当てられた価値を有し、通信とフランクとを関連付け、ネットワークを介してフランクを付された通信の送信を開始する。価値は、例えば、お金、借款（または支払約束）、しばしば使用する飛行機のマイル、およびその他を含む、当事者たちにとって意味を持つ重要なものであってもよい。「フランクを付した」通信は、一般的に、通信に価値および／またはサービスの等級を示すいくつかの印を関連付けている。

【００１５】

〔本発明の説明〕

本発明の目的は、データ送信、送信されたデータ、送信オペレータ、受信オペレータ、および送信の最終ステータスのデータを含む証明の簡単な方法によって、上述の問題の解決手段を提供することである。ユーザがシステムのクライアントである。上記システムが自動的に上記証明方法を実行する間に、従来のルートを使用する典型的な方法にてユーザが電子メールを送信する。上記システムは、送信ユーザの情報ファイルが、管理能力と同様に、証明能力および利用可能な証明の数とともに格納されているデータベースにアクセスする。そして、上記証明システムは、電子メールの証明プロセスを開始する。ユーザが利用できる証明を有するクライアントであると判断されると、上記システムは上記証明方法を実行する。ユーザは、パソコン、タブレット端末、スマートフォン、インターネットを通じたナビゲーションが可能な装置を用いてもよい。上述のように、本発明は、遠距離通信オペレータが、送信証明および電子メールに含まれるデータに基づいて、電子メールの送達を証明するための方法である。

【００１６】

本発明の、送信ユーザから受信者への電子メールの送達証明方法は、相互接続された少なくとも１つのメールサーバおよびデータ処理ユニットを含む電子メール送達証明システムにおいて実行される以下のステップを含むことを特徴としている。

・送信ユーザから受信者に送信される第１の電子メールのコピーをメールサーバにて受信する。すなわち、オリジナルの電子メールが送信ユーザから受信者に従来のルートを介して送信されると同時に、証明システムは送信ユーザによって送信されたオリジナルの電子メールを受信せず、電子メールのコピーを受信する。

・特定の指示とともに受信者に第１の電子メールのコピーを送達する。このため、受信者は、メールサーバから上記特定の指示を含む第１の電子メールのコピーである第２の電子メールを受信する。よって、受信者は２つの電子メールを受信する。

・メールサーバにおいて、送達された電子メールのコピーを受信者に送達することに関する通知データを受信する。

・データ処理ユニットにおいて、少なくとも送信ユーザのデータ、発行日、添付データのコンテンツ、および送信された電子メールのコピーの送達に関する通知データを含む電子文書を生成する。

・データ処理ユニットにおいて、証明書の生成のための電子文書に電子署名アルゴリズムを適用する。

・メールサーバを介して送信ユーザに証明書を送達する。

【００１７】

上述したように、本発明の方法は、受信者によって受信された電子メールのコンテンツを変更しないという効果を奏する。また、本発明の方法は、電子署名の比較のためのアルゴリズムを生成しない。そのため、第１に、本発明の方法は、従来技術として知られた方法よりシンプルである。さらに、本発明の方法は、受信者によって受信された電子メールを変更せず、受信者は、証明者のルート、すなわち証明システムのルートを通る第２のメッセージを受信する。

【００１８】

〔図面の説明〕

本発明の好ましい実施形態による説明を補完するため、および本発明の特徴をより理解

するために、図面を上記説明の一体部分として添付している。なお、本発明は以下に示す図面に記載された方法に限定されるものではない。

【００１９】

図１は、本発明に係る方法の好ましい実施形態を示すフロー図である。

【００２０】

図２は、電子証明書の生成における好ましい実施形態を示すフロー図である。

【００２１】

図３は、電子メールのコピーが受信者に送達されない場合における、本発明に係る方法の好ましい実施携帯を示すフロー図である。

【００２２】

図４は、送信ユーザの証明方法における好ましい実施形態を示すフロー図である。

【００２３】

〔本発明に係る好ましい実施形態〕

図１は、送信ユーザ（１）から受信者（２）への電子メールの送達を含む、本発明に係る電子メール証明方法の好ましい実施形態を示す図である。

【００２４】

証明エンティティのクライアントである送信ユーザ（１）は、彼または彼女が証明を希望する電子メールを、送信先の電子アドレス、すなわち、電子メールの送達のための一般的なルートである第１の（initial）ルート（３）を通じて受信者（２）に対して送信する。また、送信ユーザ（１）は、到来メールサーバ（１１）が前述したコピーを受信する、第１のルート（３）とは異なる第２のルートを通じて、証明エンティティにコピーを送信する。ここに示す好ましい実施形態では、証明プロセスを管理するデータ処理ユニット（１１）は、到来メールサーバ（１１）と同じものである。

【００２５】

このため、送信ユーザ（１）は、受信者（２）に対して電子メールを送達する、これらの通常の電子メールプロバイダを使用する。この目的のために、第１の（initial）メールサーバ（５）は、送信ユーザ（１）によって指定された各送信先アドレスに電子メールのコピーを送信する。そして、受信者（２）が最終的に電子メールを読むことができるように、送信先メールサーバ（６）は、証明エンティティまたは証明システムによるいくつかの操作を許容しない電子メールを含む電子メールを収集する。

【００２６】

加えて、上記方法は、データベース（１２）中に電子メールのコピーを記憶するステップを含んでもよい。または、処理ユニット（１１）は、電子メールのコピーを、出所、１または複数の送信先、添付ファイル、添付ファイルの分類、および、送信ユーザ（１）に割り当てられたすべてのオブジェクトの番号といった、異なるオブジェクトに予め分解（decompose）してもよい。

【００２７】

添付ファイルのより好ましい実施形態として、添付ファイルに請求書が含まれていてもよく、この場合、請求書が受信者（２）に送達されたことを証明することが望ましい。

【００２８】

すべてのオブジェクトについて分解、索引付け、分類が行われると、電子メールのコピーは、「証明済電子メール」、または、より具体的な「証明済請求書」というテキストを含み得る特定の表示が、添付データに含まれる請求書のコンテンツとして好ましい場合、当該表示を挿入されて送信される。その後、新たなコピーが第２のデータベース（１３）にて生成され、証明システムの差出メールサーバ（１４）に送達される。差出メールサーバ（１４）は、受信者（２）が利用可能な送付先サーバ（６）にこのコピーを送信する。

【００２９】

これにより、受信者（２）は２つの電子メールを受信する。一方は、自身のサーバ（５、６）を使用する送信ユーザ（１）から、第１のルート（３）を介して送信されたオリジナルの電子メールである。他方は、例えば「証明済み電子メール」または「証明済請求書

」といった特定の証明表示を含み、証明者の証明システムを中継して第２のルート（１０）を介して送信された電子メールである。

【００３０】

電子メールのコピーが正しい電子メールアドレスを有し、サーバ（６）に送達された場合、好ましい実施形態が図２に示される証明プロセスが継続される。送達不可能、または上記アドレスが存在しない場合、証明プロセスは図３に含まれる好ましい実施形態に従って継続される。

【００３１】

電子メールのコピーがサーバ（６）に送達されると、差出メールサーバ（１４）は電子メールのコピーの送達に関する通知データを受信し、証明プロセスを管理する処理ユニット（１１）に通知データを送信する。

【００３２】

送達指示、ステップ、インシデント、または証明プロセスに有用な各種情報を受信すると、図２に示す好ましい実施形態において、処理ユニット（１１）は、例えば、送信ユーザ（１）のデータ、発行日、コンテンツ、添付ファイル（添付ファイルがある場合）、電子メールのコピーの送達日時を含むＰＤＦフォーマットである電子文書を生成する。

【００３３】

電子文書が生成されると、電子文書は、証明書（４）の生成のためのデジタル署名アルゴリズムによって電子的にサインされる。

【００３４】

加えて、上述したコンテンツのすべて、すなわち、電子文書およびデジタル署名は電子的にまとめられ、より法的に強化された証明書（４）を提供するために、２つの会社からの２つのデジタル署名を有する電子文書を取得して、信頼されたタイムスタンプ（２０）に送信される。

【００３５】

最終ファイル、すなわち証明書（４）が得られると、証明書（４）が送信ユーザ（１）に送信される。具体的には、まず送信ユーザ（１）の口座から費用が回収され、次に、証明書（４）が差出メールサーバ（１４）に送達される。このサーバ（１４）は、送信ユーザ（１）に、証明書（４）を含む電子メールを送信する。

【００３６】

図３は、電子メールのコピーが受信者（２）に送達されない場合のフローチャートの好ましい実施形態を示す図である。受信者（２）が存在しない、またはドメインが無効であるために、電子メールが送達されない場合、電子メールは、例えば２４時間という期間の間に、再送信を試みられる。

【００３７】

最終的に送達された場合、上述した処理が継続されるが、送達されなかった場合、証明者の証明システムにおける差出メールサーバ（１４）は、生成されたトランザクションから、処理ユニット（１１）に送信されるデータを受信する。

【００３８】

送達指示、ステップ、インシデント、および証明プロセスに有用な各種情報を受信すると、図３に示す好ましい実施形態において、処理ユニット（１１）は、例えば、送信ユーザ（１）のデータ、送信日、コンテンツ、添付ファイル（添付ファイルがある場合）、電子メールのコピーの送達を試みた日時を含むＰＤＦフォーマットである電子文書を生成する。

【００３９】

この電子文書が生成されると、電子文書は、証明書（４）の生成のためのデジタル署名アルゴリズムによって電子的にサインされる。

【００４０】

加えて、上述したコンテンツのすべて、すなわち、電子文書およびデジタル署名は電子的にまとめられ、より法的に強化された証明書（４）を提供するために、２つの企業から

の２つのデジタル署名を有する電子文書を取得して、信頼されたタイムスタンプ（２０）に送信される。

【００４１】

最終ファイル、すなわち証明書（４）が得られると、証明書（４）が送信ユーザ（１）に送信される。具体的には、まず送信ユーザ（１）の口座から費用が回収され、次に、証明書（４）が差出メールサーバ（１４）に送達される。このサーバ（１４）は、送信ユーザ（１）に、証明書（４）を含む電子メールを送信する。

【００４２】

図４は、送信ユーザ（１）が、証明者の処理ユニット（１１）との接続を開始する上記のステップの好ましい実施形態を示す図である。

【００４３】

送信ユーザ（１）は、例えば、パソコン、タブレット、スマートフォン、またはインターネットを通じたナビゲーションが可能な装置などの異なるアクセスシステムによって参加してもよい。

【００４４】

好ましい実施形態において、送信ユーザ（１）は、ウェブコントロールアクセスシステムにアクセスする。このシステムは、管理能力と同様に、送信ユーザ（１）の情報ファイルが、証明能力および利用可能な証明の数とともに格納されているデータベースにアクセスする。

【００４５】

送信ユーザ（１）は、彼または彼女のユーザネームおよびパスワードを入力する。これらが正しくない場合、サインアップする方法の説明を有するヘルプシステムへリダイレクトされ、彼または彼女は認証システムへ再入力することとなる。

【００４６】

ユーザが正しく認証された場合、彼または彼女は、発行される証明書がどのように生成されるか、および、電子メールの証明が許可されるアドレスに関する特徴が明記され得るメニューにアクセスしてもよい。これらのパラメータが定義されると、送信ユーザ（１）は証明処理の時間枠を要求し、そのスケジュールを調整してもよい。換言すれば、特定の瞬間から証明システムは電子メールを承認し、証明プロセスを開始する。

【００４７】

最後に、上記プロセスが開始されるときに、送信ユーザ（１）が証明されたメールのための送達時間枠にある場合、プロセスは開始される。そうでない場合、メールは、時間枠外である、または送信ユーザ（１）が不明であるという通知を返される。

【００４８】

他の実施形態として、ユーザは、ウェブを介してウィンドウを開くことなく、証明要求を実行するための証拠または暗号化されたトークンを別の方法で要求してもよい。

【図面の簡単な説明】

【００４９】

【図１】本発明に係る方法の好ましい実施形態を示すフロー図である。

【図２】電子証明書の生成における好ましい実施形態を示すフロー図である。

【図３】電子メールのコピーが受信者に送達されない場合における、本発明に係る方法の好ましい実施携帯を示すフロー図である。

【図４】送信ユーザの証明方法における好ましい実施形態を示すフロー図である。

【図１】

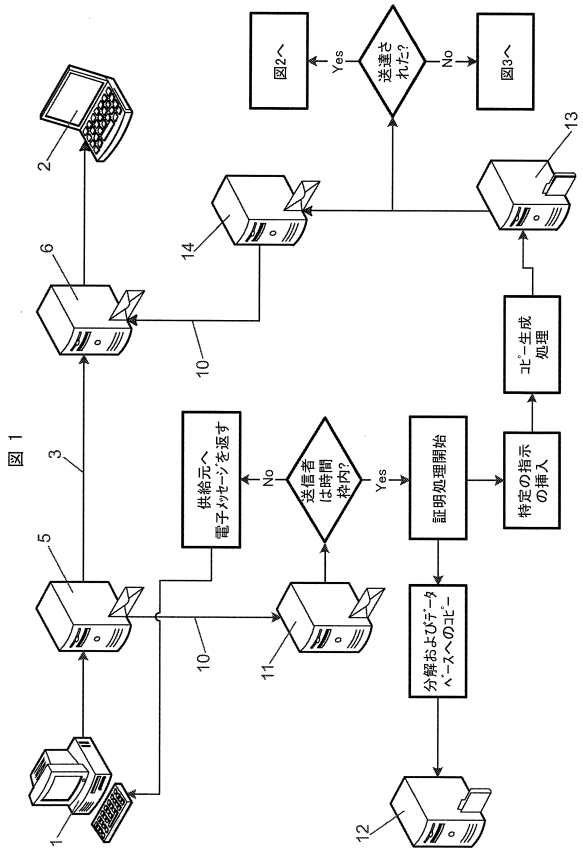
図１
図2へ
Yes
送達された?
No
図3へ
コピー生成処理
特定の指示の挿入
証明処理開始
送信者は時間枠内?
No
Yes
供給元へ電子メッセージを返す
分解およびデータベースへのコピー

【図２】

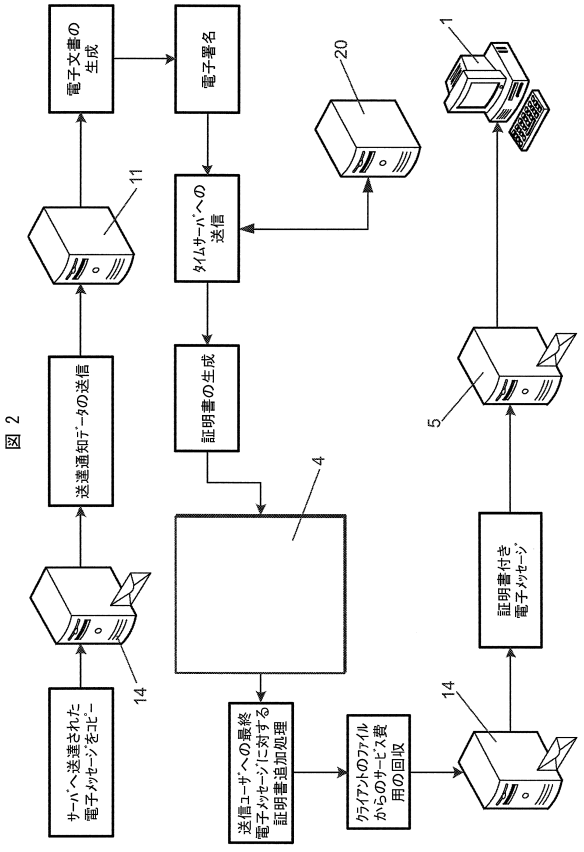
図２
電子文書の生成
電子署名
タイムサーバへの送信
送達通知データの送信
証明書の生成
サーバへ送達された電子メッセージをコピー
送信ユーザへの最終電子メッセージに対する証明書追加処理
クライアントのファイルからのサービス資用の回収
証明書付き電子メッセージ

【図３】

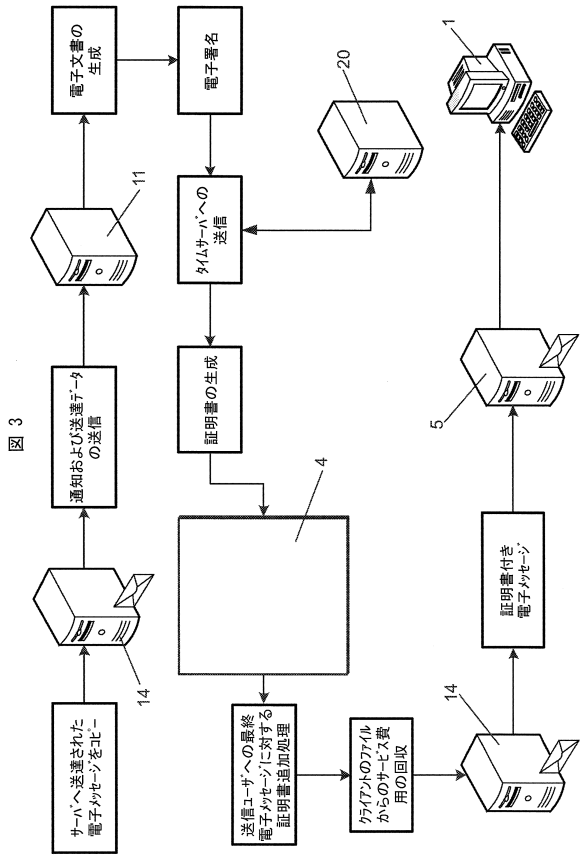
図３
電子文書の生成
電子署名
タイムサーバへの送信
通知および送達データの送信
証明書の生成
サーバへ送達された電子メッセージをコピー
送信ユーザへの最終電子メッセージに対する証明書追加処理
クライアントのファイルからのサービス資用の回収
証明書付き電子メッセージ

【図４】

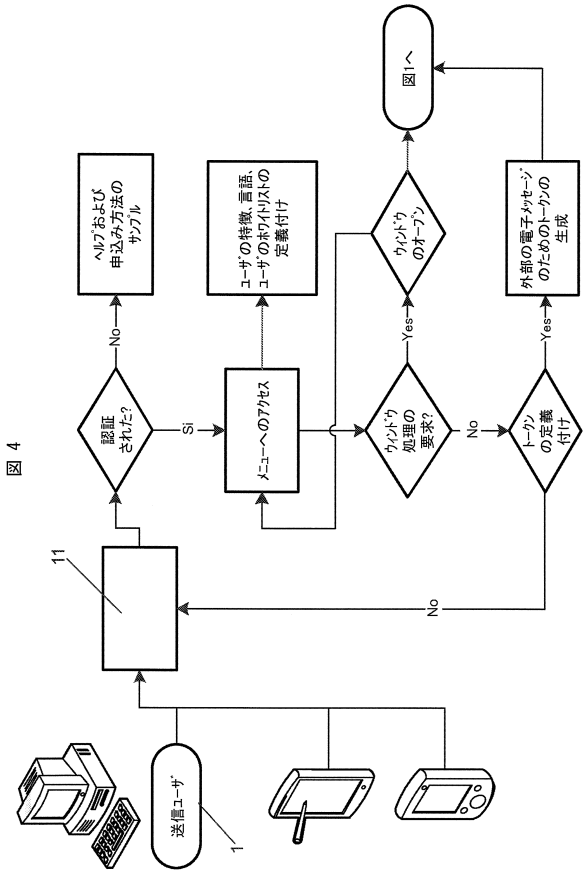
図４
図1へ
ヘルプおよび申込み方法のサンプル
ユーザの特徴、言語、ユーザのホワイトリストの定義付け
認証されたか?
No
Si
メニューへのアクセス
ウィンドウのオープン
ウィンドウ処理の要求?
Yes
No
外部の電子メッセージのためのトークンの生成
トークンの定義付け
Yes
No
送信ユーザ

フロントページの続き

(72)発明者　サペーナ　ソレル，フランシスコ
スペイン，エー－２５００３　レリダ，パルケ　テクノロギコ　アグロアリメンタリオ，エディフィシオ　アチェ１，セグンダ　プランタ，レリダネットワークス　セルヴェイス　テレマティクス　エセ．アー．

審査官　安藤　一道

(56)参考文献　特表２００４－５２１４０４（ＪＰ，Ａ）
特開２００２－３４４５２５（ＪＰ，Ａ）
特開平１１－２３４３３０（ＪＰ，Ａ）
特開２００２－０６４５３５（ＪＰ，Ａ）
米国特許出願公開第２００１／００２７５２３（ＵＳ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　１２／５８
Ｇ０６Ｆ　１３／００
Ｈ０４Ｌ　９／３２