(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6909233号
(P6909233)
(45)発行日　令和3年7月28日(2021.7.28)　(24)登録日　令和3年7月6日(2021.7.6)

(51)Int.Cl.		F I		
G06F 13/00	(2006.01)	G06F	13/00	610S
H04L 9/32	(2006.01)	H04L	9/00	675B
G09C 1/00	(2006.01)	G09C	1/00	640D
H04L 12/58	(2006.01)	H04L	12/58	100Z

請求項の数 5　(全 10 頁)

(21)出願番号　特願2018-552128(P2018-552128)
(86)(22)出願日　平成28年12月22日(2016.12.22)
(65)公表番号　特表2019-503550(P2019-503550A)
(43)公表日　平成31年2月7日(2019.2.7)
(86)国際出願番号　PCT/EP2016/082298
(87)国際公開番号　WO2017/114731
(87)国際公開日　平成29年7月6日(2017.7.6)
審査請求日　令和1年12月2日(2019.12.2)
(31)優先権主張番号　15382665.6
(32)優先日　平成27年12月28日(2015.12.28)
(33)優先権主張国・地域又は機関
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】認定された電子署名を含む電子メールを電気通信事業者の側で認証する方法

(57)【特許請求の範囲】
【請求項１】
デジタル署名された電子メールを、電気通信事業者によって認証する方法であって、
前記方法は、
ｉ．前記電気通信事業者のユーザである送信者（１、２、３）が少なくとも１つの電子メールを生成するステップと、
ｉｉ．前記電子メールを、前記電気通信事業者のクライアントメールサーバ（４、１５）に到着させるステップと、
ｉｉｉ．前記電子メールを、インターネット（５）を介してメール送信先サーバ（７、２４）に送って当該電子メールを認証済みメール送信先（８、２５）に到着させ、かつ、前記電子メールを前記事業者の受信メールサーバ（９）に送信するステップと、
ｉｖ．前記電子メールを認証（１７）するステップであって、当該認証は、前記電子メールのコピー（１８）を生成することと、前記電子メールを各部分へ分解することと、を順に含み、前記各部分は、前記メールの送信の詳細、受信の詳細、およびコンテンツを含む、ステップと、を含み、
前記デジタル署名された電子メールを認証する方法は、
ｖ．前記電子メールの前記コピー（１８）が分解されたら、前記コピー（１８）およびその各部分を第１データベース（１９、３２、４３）にダンプするステップと、
ｖｉ．前記電子メールの前記コピー（１８）をコンテナにカプセル化（２０）するステップと、

ｖｉｉ．前記電子メールの前記カプセル化されたコピー（１８）を含む、認証済みメール（２１）を生成し、当該認証済みメール（２１）を事業者の送信メールサーバ（２３、２６）に到着させるステップと、
ｖｉｉｉ．前記認証済みメール（２１）を、前記事業者の送信メールサーバ（２３、２６、３８、５０）から、前記メール送信先サーバ（７、２４）に到着させるステップと、
ｉｘ．前記認証済みメール（２１）を、前記メール送信先サーバ（７、２４）から、
ａ．前記認証済みメール送信先（８、２５）、および
ｂ．前記事業者の送信メールサーバ（２３、２６、３８、５０）
に到着させるステップと、
ｘ．前記事業者の送信メールサーバ（２３、２６、３８、５０）に到着するように設定された要素を含む第２データベース（２２、３３、４６）に、前記認証済みメール（２１）をダンプするステップと、
ｘｉ．前記認証済みメール（２１）が前記認証済みメール送信先（８、２５）に送達されたかどうかの送達チェック（２７）を実行するステップと、
ｘｉｉ．前記電気通信事業者の認証サーバ（３０、４１）によって認証証明書（３７、４９）を生成するステップであって、当該認証証明書（３７、４９）は、
ａ．前記メールの送信の詳細、受信の詳細、およびコンテンツを含む第１部分（３１、４２）と、
ｂ．前記認証証明書（２１）が前記事業者の送信メールサーバ（２３、２６）に到着した詳細を含む第２部分（３４、４５）と、
ｃ．前記電気通信事業者のデジタル署名とタイムスタンプ（３５、４８）と、を含む、ステップと、
ｘｉｉｉ．前記認証証明書（３７、４９）を前記送信者（１、２、３）に到着させるステップと、を含むことを特徴とする、方法。
【請求項２】
ユーザ／権限リストとの比較によって、前記送信者（１、２、３）が認証権限を有することをチェックする（１０）ステップをさらに含み、
当該チェックは、前記電子メールを認証データ処理サーバに送信することによって実行されることを特徴とする、請求項１に記載の方法。
【請求項３】
ステップｘｉの前記送達チェック（２７）の結果として、前記認証済みメール（２１）が前記認証済みメール送信先（８、２５）に不送達であることが示され、
送達を試みた時刻および送達アドレスを含む、前記不送達の詳細を前記認証証明書（３７、４９）に追加するステップをさらに含むことを特徴とする、請求項１または２に記載の方法。
【請求項４】
ステップｘｉの前記送達チェック（２７）の結果として、前記認証済みメール（２１）が前記認証済みメール送信先（８、２５）に送達されたことが示され、
ステップｘｉｉ．ａにおいて、前記第１部分（３１、４２）を生成した後、前記認証済みメール送信先サーバ（８、２５）が返送／ブラックリストサーバのリストにあるかをチェックすることを含む検証（４４）をさらに含み、
前記返送／ブラックリストサーバは、デフォルトで、すべてのメッセージを受け入れるが、前記対応する認証済みメール受信者（８、２５）が存在しない場合、前記受け入れたメッセージをあとで拒否することを特徴とする、請求項１から３のいずれか一項に記載の方法。
【請求項５】
前記検証（４４）の結果として、前記認証済みメール送信先サーバ（８、２５）が前記返送／ブラックリストサーバのリストにあり、
前記認証済みメール送信先サーバ（８、２５）に前記受信者が不存在である詳細を前記認証証明書（３７、４９）に追加するステップをさらに含むことを特徴とする、請求項４

に記載の方法。
【発明の詳細な説明】
【発明の詳細な説明】
【０００１】
〔発明の目的〕
本発明は、電気通信事業者が、当該事業者のクライアントである任意の送信ユーザの認定された電子署名で署名された電子メールを、当該事業者のクライアントでない１つまたは複数の受信者へ、非侵入的に受信、転送、送達および認証し、オリジナルのメールの電子署名を損なうことなく管理の連鎖を壊さずに、元の署名が変わらない状態で、ＤＭＡＲＣ規格に適合するようにメールを再送信し、すべての操作トランザクションの証拠を生成し、最終的に、電気通信事業者としてメールにデジタル署名し、送信者の詳細、送信日、送信された全文、ユーザによって電子署名され、オリジナルの署名を損なわないオリジナルのメールを含む（クライアントでない受信者への不送達または送達遅延の場合には、送達の日時や最後の状況も含む）認証証明書を、信頼された第三者として送信ユーザクライアントに送達することができる方法である。
【０００２】
〔発明の背景〕
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すべての種類の活動について使用されている。
【０００３】
電気通信事業者は、このトラフィックの大部分を管理し、方向付け、保存する基盤を提供する。これらの電気通信事業者は、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】
電気通信事業者は、特に、請求のために、当該請求に請求書参照先として関連付けられた番号を登録するために、また、ユーザへの請求に使用された他の処理の詳細を記録するために、ユーザの行った処理をさらに登録する。これらの登録は、ユーザの側で後日、請求を確認するために、および／または、ユーザのトラフィックを監視するために、保存される。
【０００５】
時には、司法当局が、電気通信事業者に、行われた電子トランザクションの登録の詳細を提供するよう要求することがある。司法当局は、電気通信事業者を、これらの詳細や、対象の行為を実行した私人または法人を特定するのに役立つ任意の他の詳細を提供するための信頼された第三者だと見なしているからである。
【０００６】
司法当局の要求した詳細が一度特定されたら、事業者は、関連司法当局の要求した処理の詳細、頻度、宛先、および任意の他の情報を明示的に宣言する認証証明書を発行する。
【０００７】
このやり方は、関係者によって電気通信事業者に対して要求され、証拠として提示された場合、最近、証拠として我が国の最高裁判所（ＡＴＳ２５０１／２０１３、スペイン最高裁判所民事部）でも認められた。
【０００８】
最新技術は、認証済み電子メールを送信する多様な方法およびシステムに詳しい。こうした技術の中には、信頼された第三者が管理し、認証済みのコンテンツがダウンロードされるウェブ環境へのリンクを、クライアントの側で送ることに基づくものもあるが、そうした技術は、認証証明書を生成するために、通知された関係者が上述のコンテンツをダウンロードする意思を有することが必要であるという基本的な欠点がある。他の技術としては、コンテンツに電子的な検証が追加され、当該検証が送信者を真似て、コンテンツを宛先に再送信するものもある。この最後の技術は３つの深刻な欠点がある。

【０００９】
ａ）ユーザのために再送信する途中、送信元の状況がまったく変わったため、認定された電子署名が破壊され、管理の連鎖が破壊され、不信感が生じる。
【００１０】
ｂ）電子メールの認証をその後、チェックするために、内部に検証を追加することによって、さらに、オリジナルの認定された電子署名および管理の連鎖が新たに破壊される。
【００１１】
ｃ）ユーザの代わりにユーザであるかのように再送信する際、認証済み電子メールは世界的規格としてのＤＭＡＲＣ規格と一致せず、認証済み電子メールの有効な送達が妨げられる。
【００１２】
本出願の目的である本発明は、上記デメリットの解決策を提供する。当該解決策は、認証対象であるコンテンツを後でダウンロードする必要がなく、管理の連鎖を維持するためのユーザのオリジナルの認定された電子署名、および、ＤＭＡＲＣ規格下のサービスのすべての機能性を損なうことなく、結果として、オリジナルの認定された署名を破壊せずに、電気通信事業者によって認証証明書が発行される。当該認証証明書は、特定の日時に事業者によってその電子メールコンテンツが宛先に送信されたこと、当該電子メールコンテンツがその公式電子代表者に最終的に送達されたことまたは送達されなかったことを認定し、さらに、送信の詳細、送信された詳細、添付物、単一登録番号および使用された処理の詳細を含む。
【００１３】
〔発明の概要〕
上記によれば、本発明の目的は、電気通信事業者の認証対象である、認定された電子署名を有する電子メールを送信して、送信先が二つのコピー（クライアントからのオリジナルのメールと、オリジナルのクライアントだと装わない電気通信事業者からのメール）を受信し、上記認定された電子署名および管理の連鎖を損なわないようにする、方法である。事業者のクライアントまたは送信者は、オリジナルの電子メールを誰が送信したかに応じて認証証明書を受信し、当該認証証明書は、オリジナルのメール、閲覧可能なコンテンツ、その日付、時刻およびトレーサビリティ、単一処理番号、さらに、可能なら、最後に送達の日付や時刻や状況を含む。
【００１４】
本発明の目的は、電気通信事業者によって認証された電子メールを作成する方法であって、当該方法は、以下の各ステップを含むとともに、事業者のクライアントの少なくとも１つの外部のメールサーバと、認証済みメールの送信先サーバと、事業者の受信メールサーバと、コピーおよび断片化された要素のデータベースサーバと、事業者の送信メールサーバと、ＴＳＡタイムスタンプサーバと、送信された要素のデータベースサーバと、認証サーバとしてのデータ処理ユニットと、を含み、それらすべてが互いに連結されている。上記各ステップは、電気通信事業者のクライアントによって、電子メールを、特定の送信先に、インターネットプロバイダーを介して任意のプラットホームを用いて、当該電気通信事業者のサーバのメールアドレス、たとえば、correo@certificado.lleida.netをコピーして、送信するステップと、送信先において、権限のあるデジタル代表者が、標準的な電子メールを受信するステップと、事業者の受信メールサーバにおいて、電気通信事業者のユーザクライアントによって送信されたメッセージのコピーを受信するステップと、ユーザが権限を有しており、メールを認証する信用があることをチェックし、続いて、データベースに、受信したテキストおよび各部分を挿入し登録するステップと、電気通信事業者のデータ処理ユニットにおいて電子メールを生成するステップであって、当該電子メールは、電気通信事業者のサーバのアドレスnoreply@mailcert.lleida.netから送信されるものであり、事業者のクライアントによって送信されたコンテンツをカプセル化して、認定されたオリジナルのデジタル署名を損なわないようにし、当該コンテンツを特に「認証済み電子メール」のような電子メールの件名の中に挿入するステップと、送信電子メール

サーバの側で、カプセル化されたメールを送信するステップと、クライアントでない送信先の、権限のあるデジタル代表者によって、カプセル化された電子メールを受け入れるまたは受け入れないステップと、電気通信事業者の認証証明書を最終的に生成するステップであって、当該認証証明書は、認定されたデジタル署名を損なうことのないオリジナルのメール、送信された詳細、受信された詳細、送信の日付および時刻、受信の日付および時刻、認定されたデジタル署名の適用、電気通信事業者のタイムスタンプを含む、ステップと、認証証明書を、メールサーバを介して、送信ユーザに送信するステップである。

【００１５】

上記によれば、本発明の目的である本方法は、オリジナルのメールをいじらずに、管理の連鎖を維持し、ユーザによって認定されたデジタルフォームを使用することができる利点、メールのカプセル化されたコピーが、ユーザの名前ではなく電気通信事業者の名前で再送信されるため、ＤＭＡＲＣ規格に適合する利点、をさらに提供する。最終的に、電気通信事業者の側で、コンテンツの送信、受信、受け入れの証拠が生成される。

【００１６】

説明を補完し、本発明のよりよい理解に寄与するため、本発明の実施形態の好ましい例に従って、上述の説明の必須の部分として、一組の図面を添付する。当該図面は例示的なものであり、限定的なものではなく、以下のことが示されている。

【００１７】

〔図面の説明〕

〔図１〕本発明の目的である方法の実施形態の実施例において、認証済み電子メールの生成の開始、および、カプセル化されたコピーの送達または不送達を示すフローチャートである。

〔図２〕本発明の目的である方法の実施形態の実施例において、カプセル化された電子メールの送達または不送達の場合の最終的な認証証明書の構成および送信を示すフローチャートである。

【００１８】

〔発明の好ましい形態〕

図１および２では、本発明の目的である方法に関する一連のダイアグラムが示される。当該方法は、電気通信事業者の側で、認定された電子署名を含む電子メールを認証する方法である。当該方法は、送信者（１、２、３）（電気通信事業者のユーザ）から電子メールを送信することと、送信が有効であり、電子メールが送達されたことを、コンテンツおよび送信の詳細を用いて確認する認証証明書を受信することを含む。上記すべては、事業者の認定された電子署名および第三者のタイムスタンプによって署名されている。

【００１９】

電気通信事業者の送信ユーザクライアントが認証済み電子メールを送信したい場合、電気通信事業者の受信メールサーバのメールアドレス、たとえばcorreo@certificado.lleida.netをコピーし、任意のプラットホーム、ＰＣ、タブレットまたは携帯電話を通して、当該メールを送信する。これをするために、電気通信事業者のユーザである送信者（１、２、３）が、少なくとも１つの電子メールを生成し、当該電子メールを電気通信事業者のクライアントメールサーバ（４、１５）に到着させる。たとえば、当該電子メールがLleida.netのクライアントメールサーバに送信される。電気通信事業者のクライアントメールサーバ（４、１５）は、任意のインターネットプロバイダーに属する。電子メールが、法的目的で権限のある電子代表者である送信先サーバに送達される。言い換えれば、電子メールは、メッセージを特定の送信先に送達できるインターネットレベルにあるから、電子メールをインターネット（５）を経由してメール送信先サーバ（７、２４）に到着させ、あるメール送信先（８、２５）に到達させることができる。また、このメッセージのコピーを事業者の受信メールサーバ（９）（この例ではLleida.netの受信メールサーバ）に送達する。

【００２０】

事業者の受信メールサーバ（９）は電子メールを認証データ処理サーバ（Mailcert）に

送信する。認証データ処理サーバは、電気通信事業者の一部を構成し、ユーザがホワイトリストにあるかどうか、言い換えれば、ユーザが認証済み電子メールを送信できるシステムとともに登録されているかどうかをチェックする。登録されていない場合、当該メールは無視されるが、登録されている場合、信用のあるユーザであるかどうかの確認に進む。これは、ユーザ／権限リストとの比較によって、ユーザ（１、２、３）が認証権限を有することをチェックする（１０）ことを意味する。当該チェックは、電子メールを認証データ処理サーバに送信することによって実行される。

【００２１】

該当のユーザが信用のないユーザの場合、信用がないことを示す電子メールを生成し、事業者の送信メールサーバ（２３、２６、３８、５０）に送信し、当該送信メールサーバ（２３、２６、３８、５０）が、最終的に、当該電子メールを、通信事業者のユーザクライアントであるユーザ（１、２、３）に送達する。

【００２２】

信用のあるユーザの場合、電子メールの認証（１７）に進む。上述の認証は、順に、電子メールのコピー（１８）を生成することと、電子メールを各部分（当該メールの送信の詳細、受信の詳細、およびコンテンツを、その処理のために含む）に分解することとを含み、当該詳細は、好ましくは、コピー（１８）とともに、第１データベース（１９、３２、４３）に保存される。

【００２３】

その後、電子メールのコピー（１８）を、コンテナにカプセル化（２０）し、認証済みメール（２１）を生成する。電子メールのカプセル化されたコピー（１８）を含む当該認証済みメール（２１）は、それから、事業者の送信メールサーバ（２３、２６）に到着し、事業者の送信メールサーバ（２３、２６、３８、５０）からメール送信先サーバ（７、２４）に到着し、メール送信先サーバ（７、２４）から、認証済みメール送信先（８、２５）および事業者の送信メールサーバ（２３、２６、３８、５０）に到着する。

【００２４】

電気通信事業者の一部を構成する認証データ処理サーバを起点とする電子メールアドレス、たとえば、service@correo electronicocert.lleida.netから、認証済みメール（２１）を生成する。当該認証済みメール（２１）のメッセージの件名は「認証済み電子メール」であり、オリジナルの件名のテキスト、および、必要と思われるだけの数のコントロールテキストを追加する。認証サーバservice@correo electronicocert.lleida.netとして電気通信事業者から送信されること、および、クライアントのオリジナルの電子メールアドレスを起点としないことによって、当該サービスをＤＭＡＲＣ対応のサービスにすることができる。クライアントのために電子メールを送達する権限を与えられるが、クライアントに取って代わるものではないからである。

【００２５】

認証済みメール（２１）のテキストの中に、当該メールが認証済みメッセージであることを示すバナーが含まれ、最終的に当該メールはカプセル化（２０）される。言い換えれば、内部操作によってオリジナルの認定された電子署名が破壊されメッセージの真実性についての不信感が生じるのを避けるために当該認定された署名を損なわない目的で、オリジナルのメッセージ全体が含まれる。電子メールのカプセル化されたコピー（１８）は、第２データベース（２２、３３、４６）に保存され、送信のために、事業者の送信メールサーバ（２３、２６、３８、５０）に到着する。

【００２６】

事業者の送信メールサーバ（２３、２６、３８、５０）は、電子メールのカプセル化されたコピー（１８）を送達するが、送達のために、それから１０分～１時間、その後に生じる拒否応答を待つ。言い換えれば、最初に、送信先の電子メールサーバは、まず、すべてを受け入れるが、その後、拒否する。これは、システムが自動的に自己調節をする行為である。

【００２７】

認証済み電子メールを最終的に送達できた場合、当該方法は図２の「ＹＥＳ」プロセスに進む。認証済み電子メールを送達できなかった場合、当該方法は図２の「ＮＯ」プロセスに進む。

【００２８】

事業者の送信メールサーバ（２３、２６、３８、５０）は、カプセル化された電子メールをその権限のあるデジタル代表者に送達する。送達のために、それから１０分～１時間、その後に生じる拒否応答を待つ。言い換えれば、最初に、メール送信先サーバ（７、２４）は、まず、すべてを受け入れるが、その後、拒否する。これは、ここに記載の方法が自動的に自己調節をする行為である。

【００２９】

認証済みメール（２１）が認証済みメール送信先（８、２５）に送達されたかどうかの送達チェック（２７）がある。認証済みメール（２１）を最終的に送達できた場合、当該方法は図２の「ＹＥＳ」プロセスに進む。認証済み電子メールを送達できなかった場合、当該方法は図２に示す「ＮＯ」プロセスに進む。

【００３０】

認証済みメール（２１）の送達とともに、当該方法は、事業者自体の認証証明書（３７、４９）を生成するプロセスに進む。言い換えれば、認証済みメール（２１）が認証済みメール送信先（８、２５）に送達されたかどうかの送達チェック（２７）を行う際にＹＥＳが得られたならば、認証済みメール（２１）は、メール送信先サーバ（７、２４）から、認証済みメール送信先（８、２５）および事業者の送信メールサーバ（２３、２６、３８、５０）に到着したことになる。次に、電気通信事業者の認証サーバ（３０、４１）によって、認証証明書（３７、４９）が生成される。上述の認証証明書（３７、４９）は、メールの送信の詳細、受信の詳細、およびコンテンツを含む第１部分（３１、４２）と、認証証明書（２１）が事業者の送信メールサーバ（２３、２６）に到着する詳細を含む第２部分（３４、４５）と、電気通信事業者のデジタル署名とタイムスタンプ（３５、４８）と、を含む。

【００３１】

そのため、コンテンツおよびオリジナルの電子メールを、最初のコピーの第１データベース（１９、３２、４３）から回収し、認証証明書（３７、４９）の第１部分を構成する。これが終わったら、第１部分（３１、４２）の生成後、検証（４４）によって、メール送信先サーバ（７、２４）が返送／ブラックリストにあるか確かめる。上述の検証（４４）は、認証済み電子メールの送信先サーバ（８、２５）が返送／ブラックリストサーバのリストにあるかチェックすることを含み、当該返送／ブラックリストサーバは、デフォルトですべてのメッセージを受け入れ、その後、対応する認証済みメールの受信者（８、２５）が存在しない場合に、当該メッセージを拒否するものである。言い換えれば、検証（４４）は、デフォルトですべてのメッセージを受け入れ、その後、ユーザが存在しない場合に、当該メッセージを拒否するサーバのリストに、送信先サーバがあるか検証するものであり、その後に生じる拒否メッセージが、メール送信先サーバ（７、２４）から到着したかをチェックする。その後に生じる拒否のメッセージが到着した場合、当該方法は「ＮＯ」プロセスに進む。

【００３２】

検証（４４）の結果として、認証済みメール送信先サーバ（８、２５）が返送／ブラックリストサーバのリストにある場合、認証済みメール送信先サーバ（８、２５）に受信者が不存在である詳細を、認証証明書（３７、４９）に追加することに進む。検証（４４）の結果として、メール送信先サーバ（７、２４）がブラックリストまたは返送リストにない場合、認証証明書の第２部分がすべての処理の詳細を含み、第三者のタイムスタンプ（３５、４８）を追加し、認証証明書（３７、４９）の第２部分（３４、４５）のコンテンツを説明する際に上記した、電気通信事業者の認定された電子署名で認証証明書（３７、４９）に署名する。

【００３３】

認証証明書（３７、４９）が完成した後、この生成された認証証明書（３７、４９）が添付された電子メールを生成し、当該電子メールを電気通信事業者の送信メールサーバ（２３、２６）に送信し、当該送信メールサーバ（２３、２６）が、当該電子メールを、最終的に権限のある電子代表者に送達し、それをクライアントに送達する。

【００３４】

「ＮＯ」プロセスは、認証済みメール（２１）を認証済みメール送信先（８、２５）に送達することができなかった場合に利用されるプロセスである。当該プロセスが重点を置いているのは、たとえ妨げる状況があったとしてもコンテンツを送るという公的に明白で明瞭な意思を示すことが目的であるならば、信頼できる通知を送信するプロセスにおいて、送達と不送達の両方が重要であることであり、信頼できる通知を克明な通知、すなわち、送達を有効にするために技術的に可能なことがすべて行われたという通知にする。

【００３５】

認証済みメール（２１）が「ＮＯ」プロセスに進むことが決定されたら、認定証明書（３７、４９）を再構成して、当該認定証明書（３７、４９）は、受信者を特定し、メッセージを権限のある電子代表者に有効に送達することを妨げたすべての変化とともに、当該受信者の詳細を含む。たとえば、認定証明書（３７、４９）に、送達を試みた時刻、送達アドレス、受信者の身元など、不送達についての詳細を追加することができる。認定証明書（３７、４９）が完成したら、当該認定証明書（３７、４９）は電気通信事業者の認定されたデジタル署名で電子的に署名され、第三者のタイムスタンプが追加される。

【００３６】

文書が署名されたら、このＰＤＦ書類が添付された電子メールを生成し、当該ＰＤＦ書類は電子メールによって電気通信事業者のユーザである送信者（１、２、３）に送信される。

【００３７】

最終的に生成された認定証明書（３７、４９）により、電気通信事業者のユーザである送信者（１、２、３）は、認証済みメール（２１）を特定の認証済みメール送信先（８、２５）に送信したことを、それ独自の認定された電子署名を用いて、電子メールをそのトランザクションの点で変更せずに、またはインターネットで実行される新たな規格により電子メールの送達が妨げられることなしに、信頼性をもって証明することができる。

【図面の簡単な説明】

【００３８】

【図１】本発明の目的である方法の実施形態の実施例において、認証済み電子メールの生成の開始、および、カプセル化されたコピーの送達または不送達を示すフローチャートである。

【図２】本発明の目的である方法の実施形態の実施例において、カプセル化された電子メールの送達または不送達の場合の最終的な認証証明書の構成および送信を示すフローチャートである。

【図１】

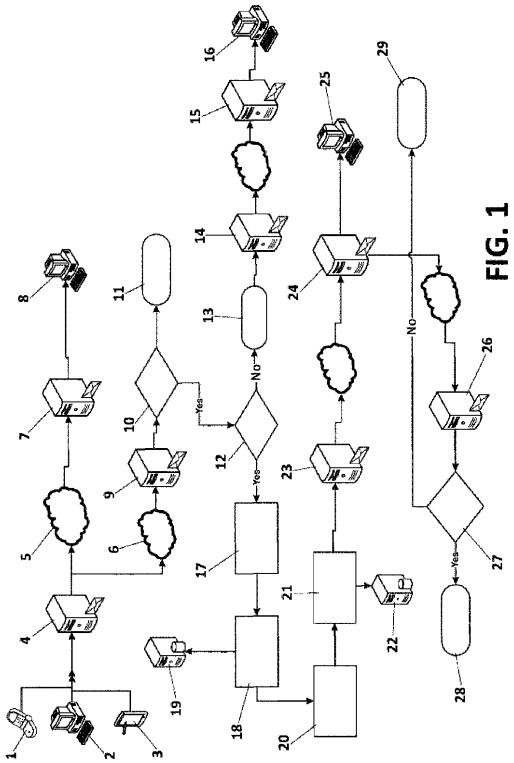

FIG. 1

【図２】

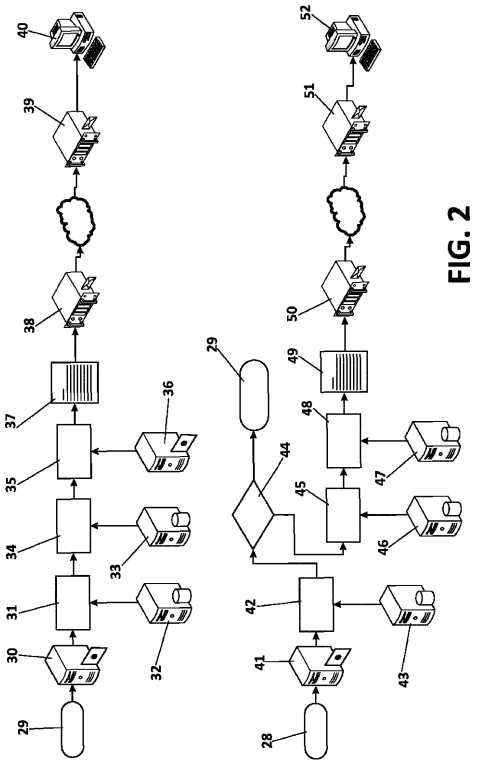

FIG. 2

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，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　今川　悟

(56)参考文献　特表２０１６－５００９６１（ＪＰ，Ａ）
特開２００７－２４３８１５（ＪＰ，Ａ）
米国特許出願公開第２０１５／００７４００６（ＵＳ，Ａ１）
中国特許出願公開第１０２４９７３６７（ＣＮ，Ａ）
特表２０１５－５１３２３６（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　１３／００
Ｇ０９Ｃ　１／００
Ｈ０４Ｌ　９／３２
Ｈ０４Ｌ　１２／５８