

(19) 日本国特許庁(JP)

(12) 特許公報(B2)

(11) 特許番号

特許第5548256号
(P5548256)

(45) 発行日 平成26年7月16日(2014.7.16)

(24) 登録日 平成26年5月23日(2014.5.23)

(51) Int.Cl.

HO4M 3/42 (2006.01)
HO4M 11/00 (2006.01)

F 1

HO4M 3/42
HO4M 11/00 302

請求項の数 22 (全 16 頁)

(21) 出願番号 特願2012-503366 (P2012-503366)
 (86) (22) 出願日 平成22年2月15日 (2010.2.15)
 (65) 公表番号 特表2012-522458 (P2012-522458A)
 (43) 公表日 平成24年9月20日 (2012.9.20)
 (86) 國際出願番号 PCT/SE2010/050172
 (87) 國際公開番号 WO2010/114459
 (87) 國際公開日 平成22年10月7日 (2010.10.7)
 審査請求日 平成25年1月15日 (2013.1.15)
 (31) 優先権主張番号 12/414,957
 (32) 優先日 平成21年3月31日 (2009.3.31)
 (33) 優先権主張国 米国(US)

(73) 特許権者 598036300
 テレフォンアクチーボラゲット エル エ
 ム エリクソン (パブル)
 スウェーデン国 ストックホルム エスー
 164 83
 (74) 代理人 100079108
 弁理士 稲葉 良幸
 (74) 代理人 100109346
 弁理士 大貫 敏史
 (72) 発明者 シュルツ、ゴラン
 フィンランド国、エスボー エフアイエヌ
 -02320, ヴァグトッペン 7 ビー
 47

最終頁に続く

(54) 【発明の名称】電子メール通信のための方法及び装置

(57) 【特許請求の範囲】

【請求項 1】

eメールの送信者が特定の電話番号に関連付けられた移動通信デバイスを所有する旨を、eメールの受信者に対して証明する方法であつて、

前記送信者側で、インターネットを介してeメール・コンテンツの識別子及び前記電話番号をサーバに送信すること、

前記サーバ側で、前記送信者からの前記識別子及び前記電話番号を受信し、検証コードを生成し、前記インターネットを介して前記検証コードを前記送信者に送信し、前記検証コードを前記識別子及び前記電話番号と共に格納すること、

前記送信者側で、前記サーバから前記検証コードを受信し、前記移動通信デバイスによつて送信されたショート・メッセージ・サービスのメッセージ内で前記検証コードを前記サーバに戻すこと、

前記サーバ側で、前記ショート・メッセージ・サービスのメッセージの発信元である前記受信した検証コード及び前記電話番号が、前記格納された電話番号及び検証コードと一致することを確認した後、前記電話番号及び前記識別子を使用して認証文字列を生成し、前記インターネットを介して前記認証文字列を前記送信者に送信すること、

前記送信者側で、前記サーバから前記認証文字列を受信し、前記認証文字列及び前記電話番号を含む前記eメールを前記インターネットを介して前記受信者に送信すること、

前記受信者側で、前記eメールを受信し、前記認証文字列、前記電話番号、及び前記受信したeメール・コンテンツの前記識別子を、前記サーバ又は他のサーバに転送すること

10

20

、及び、

前記サーバ側で、前記認証文字列、前記電話番号、及び前記識別子を受信し、前記受信した電話番号及び識別子を使用して確認認証文字列を生成し、前記受信した認証文字列が前記確認認証文字列と同じであることを確認し、その確認を前記受信者に送信すること、を含む、方法。

【請求項2】

前記サーバ側で、前記インターネットを介して前記検証コードを前記サーバに送信した時に、タイマを開始すること、前記送信者から前記検証コードを受信した時に、前記タイマが満了したかどうかを判別すること、及び、前記タイマが満了していない場合、前記ショート・メッセージ・サービスのメッセージの発信元である前記受信した検証コード及び前記電話番号が、前記格納された電話番号及び検証コードと一致することを単に確認することを、さらに含む、請求項1に記載の方法。10

【請求項3】

前記送信者側で、前記eメール・コンテンツの前記識別子を、前記受信者に送信される前記eメールに含めることを、さらに含む、請求項1に記載の方法。

【請求項4】

前記eメール・コンテンツの前記識別子が前記eメール・コンテンツのハッシュ値を備え、前記eメール・コンテンツの前記ハッシュ値を生成することをさらに含む、請求項1に記載の方法。

【請求項5】20

インターネットに接続されたユーザ端末上のeメール・クライアントを操作する方法であって、

前記ユーザ端末から受信者へのeメールの送信に先立って、前記eメール・コンテンツの識別子及び前記ユーザ端末のユーザが所有する移動通信デバイスの電話番号をサーバに送信すること、

前記送信に応答して、前記インターネットを介して前記サーバから検証コードを受信すること、

前記移動通信デバイスによって送信されるショート・メッセージ・サービス(SMS)メッセージを介して、前記検証コードを前記サーバに戻すこと、

前記戻すことに続いて、前記インターネットを介して前記サーバから認証文字列を受信すること、30

前記認証文字列及び前記電話番号を前記eメールに埋め込むこと、及び

前記eメールを前記受信者に送信すること、

を含む、方法。

【請求項6】

前記eメール・コンテンツの前記識別子を、前記受信者に送信される前記eメールに含めることをさらに含む、請求項5に記載の方法。

【請求項7】

前記eメール・コンテンツの前記識別子が前記eメール・コンテンツのハッシュ値を備え、前記eメール・コンテンツの前記ハッシュ値を生成することをさらに含む、請求項5に記載の方法。40

【請求項8】

前記ユーザ端末のeメール・クライアントは、前記eメール・コンテンツの前記ハッシュ値を生成するステップと、前記ハッシュ値及び前記電話番号を前記サーバに送信するステップとを、自動的に実行する、請求項7に記載の方法。

【請求項9】

前記認証文字列及び前記電話番号を前記eメールに含めるステップは、前記認証文字列が受信された時に、前記ユーザ端末のeメール・クライアントによって自動的に実行される、請求項5に記載の方法。

【請求項10】50

サーバを操作する方法であって、

eメールの送信者からeメール・コンテンツの識別子及び電話番号を受信すること、検証コードを生成すること、

インターネットを介して前記送信者に前記検証コードを送信すること、

前記識別子及び前記電話番号と共に前記検証コードを格納すること、

ショート・メッセージ・サービスのメッセージ内で前記サーバに戻された前記検証コードを受信すること、及び

前記ショート・メッセージ・サービスのメッセージの発信元である前記受信した検証コード及び前記電話番号が、前記検証コード及び前記電話番号と一致することを判別し、一致する場合は、前記電話番号及び前記識別子を使用して認証文字列を生成し、前記インターネットを介して前記認証文字列を前記送信者に送信すること、

を含む、方法。

【請求項 1 1】

前記インターネットを介して前記送信者に前記検証コードを送信した時に、タイムを開始すること、前記送信者から前記検証コードを受信した時に、前記タイムが満了したかどうかを判別すること、及び、前記タイムが満了していない場合、前記ショート・メッセージ・サービスのメッセージの発信元である前記受信した検証コード及び前記電話番号が、前記格納された電話番号及び検証コードと一致することを単に確認することを、さらに含む、請求項 1 0 に記載の方法。

【請求項 1 2】

サーバを操作する方法であって、

前記サーバが、eメールの受信者から、認証文字列、送信者が所有する移動通信デバイスの電話番号、及びeメール・コンテンツの識別子を受信すること、

前記サーバが、前記受信した電話番号及び識別子を使用して確認認証文字列を生成すること、

前記サーバが、前記受信した認証文字列が前記生成された確認認証文字列と同じであるかどうかを判別すること、及び、

前記受信した認証文字列が前記生成された確認認証文字列と同じであるかどうかの判別に応答して、前記サーバが、前記eメール・コンテンツの前記送信者が前記電話番号に関連付けられた前記移動通信デバイスを所有するか否かを確認するメッセージを前記受信者に送信すること、

を含む、方法。

【請求項 1 3】

インターネットに接続されたユーザ端末上のeメール・クライアントを操作する方法であって、

送信者からeメールを受信することであって、前記eメールは認証文字列及び前記送信者が所有する移動通信デバイスの電話番号を含む、受信すること、

前記認証文字列、前記電話番号、及びeメール・コンテンツの識別子をサーバに送信すること、

前記送信することに応答して、前記eメール・コンテンツの前記送信者が前記電話番号に関連付けられた前記移動通信デバイスを所有するか否かを確認するメッセージを前記サーバから受信すること、及び、

確認の成功時に、前記ユーザ端末上の前記eメール・クライアントによる前記eメール・コンテンツにアクセスすること、

を含む、方法。

【請求項 1 4】

前記eメール・コンテンツの前記識別子が前記eメール・コンテンツのハッシュ値を備え、前記eメール・コンテンツの前記ハッシュ値を生成することをさらに含む、請求項 1 3 に記載の方法。

【請求項 1 5】

10

20

30

40

50

ユーザ端末として動作するように構成された装置であって、

受信者へのeメールを生成するように構成され、及び前記eメールの送信に先立って認証文字列と送信者が所有する移動通信デバイスの電話番号とを前記eメールに埋め込むための、eメール・クライアントと、

eメール・コンテンツの識別子及び前記電話番号をサーバに送信するように構成されたネットワーク送信機と、

前記サーバから検証コードを受信するように、及び、前記eメールに関する前記認証文字列を前記サーバから受信するように構成された、ネットワーク受信機と、
を備え、

さらに前記ネットワーク送信機が、前記認証文字列及び前記電話番号を含む前記eメールを前記受信者に送信するように構成された、
装置。

【請求項16】

前記eメール・クライアントは、ハッシュ関数を前記eメール・コンテンツに適用することによって前記識別子を生成するように配置構成された、請求項15に記載の装置。

【請求項17】

サーバとして動作するように構成された装置であって、

eメールの送信者から、eメール・コンテンツの識別子及び前記送信者が所有する移動通信デバイスの電話番号を受信するように構成された、通信受信機と、

検証コードを生成するように構成されたコード生成ユニットと、

インターネットを介して前記検証コードを前記送信者に送信するように構成された通信送信機と、

前記識別子及び前記電話番号と共に前記検証コードを格納するためのメモリと、

ショート・メッセージ・サービスのメッセージ内で前記サーバに戻された前記検証コードを受信するため通信受信機と、

前記ショート・メッセージ・サービスのメッセージの発信元である前記受信した検証コード及び前記電話番号が、格納された検証コード及び電話番号と一致するかどうかを判別し、一致する場合は、前記電話番号及び前記識別子を使用して認証文字列を生成する、処理ユニットと、

を備え、

さらに前記通信送信機が、前記インターネットを介して前記認証文字列を前記送信者に送信するように構成された、

装置。

【請求項18】

前記検証コードが前記送信者に送信された時に開始されるタイマをさらに備え、前記処理ユニットは、前記送信者から前記検証コードを受信した時に、前記タイマが満了したかどうかを判別し、前記タイマが満了していない場合、前記ショート・メッセージ・サービスのメッセージの発信元である前記受信した検証コード及び前記電話番号が、前記格納された電話番号及び検証コードと一致することを単に確認するように配置構成された、請求項17に記載の装置。

【請求項19】

サーバとして動作するように構成された装置であって、

eメールの受信者から、認証文字列、送信者が所有する移動通信デバイスの電話番号、及びeメール・コンテンツの識別子を受信するように構成された受信機と、

前記受信した電話番号及び識別子を使用して確認認証文字列を生成するように、及び、前記受信した認証文字列と前記生成された確認認証文字列とが同じであるかどうかを判別するように構成された、処理ユニットと、

メッセージを前記受信者に送信するためのネットワーク送信機であって、前記メッセージは、前記eメール・コンテンツの前記送信者が前記電話番号に関連付けられた前記移動通信デバイスを所有するか否かを確認するものである、ネットワーク送信機と、

10

20

30

40

50

を備える、装置。

【請求項 20】

ユーザ端末として動作するように構成された装置であって、

eメールを送信者から受信するように構成されたネットワーク受信機であって、前記eメールは認証文字列及び送信者が所有する移動通信デバイスの電話番号を含む、ネットワーク受信機と、

前記認証文字列及び前記電話番号を抽出するように構成されたeメール・クライアントと、

前記認証文字列、前記電話番号、及びeメール・コンテンツの識別子を、サーバに送信するように構成されたネットワーク送信機と、

を備え、

さらに前記ネットワーク受信機が、前記eメール・コンテンツの前記送信者が前記電話番号に関連付けられた前記移動通信デバイスを所有するか否かを示すメッセージを、前記サーバから受信するように構成された、
装置。

【請求項 21】

前記送信者からの前記eメールは前記識別子も含み、前記eメール・クライアントは前記eメールから前記識別子を抽出するように配置構成された、請求項20に記載の装置。

【請求項 22】

前記eメール・クライアントは、ハッシュ関数を前記eメール・コンテンツに適用することによって前記識別子を生成するように配置構成された、請求項20に記載の装置。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、電子メール通信のための方法及び装置に関する。より具体的に言えば、本発明は、送信者が特定の電話番号を所有している旨を、eメールの受信者に対して証明することに関する。

【背景技術】

【0002】

現在、大多数の人々が少なくとも1つのeメール（電子メール）アカウントを有し、個人が様々な方法でeメール・アカウントを取得できる。たとえば、ユーザの雇用主がユーザにeメール・アカウントを与えることができるか、又は、ユーザがインターネット・サービス・プロバイダ（ISP）に加入した場合、通常、ユーザには少なくとも1つのeメール・アカウントが与えられることになる。加えてユーザは、GoogleのGmail（R）、MicrosoftのHotmail（R）などの多くのeメール・サービスのうちの1つを利用して、eメール・アカウントを作成することができる。

【0003】

各eメール・アカウントは、そのアカウントに固有の少なくとも1つのeメール・アドレスに関連付けられるため、このアドレスに送信されたいずれのeメールをも適切に送達することができる。eメール・アドレスは「ローカル部分@ドメイン」の形を取り、ここでドメインは、eメール・アドレスに関連付けられたアカウントをホストする単数又は複数のエンティティを識別し、ローカル部分は、ホストに対して個々のeメール・アカウントを識別する（たとえばIETF RFC 5321を参照のこと）。

【発明の概要】

【発明が解決しようとする課題】

【0004】

eメール・アカウントを作成する場合、しばしばユーザは、自分のeメール・アドレスがホストに対して固有であれば、そのローカル部分をどのようにするかを自由に定義することができる。したがってeメールの受信者は、送信者を正しく識別するための手段として必ずしもeメール・アドレスに依拠することはできない。たとえば、eメール・アドレ

10

20

30

40

50

ス「john.smith@emailservice.com」から送信されたeメールは、実際の名前がJohn Smithである個人からのeメールであるとは限らない。さらに、たとえeメール・アドレスのローカル部分が送信者の実際の名前を何らかの方法で正確に表す場合であっても、eメールの受信者は、そのeメールがどの特定の個人からのものであるかを確認することはできない。これは特に、eメール・アドレスのドメイン部分が、誰でもeメール・アドレスを作成できるようにしているホストを識別するeメール・アドレスのものである場合に当てはまる。

【課題を解決するための手段】

【0005】

本発明は、eメールの送信者が特定の電話番号に関連付けられた移動通信デバイスを所有する旨を、eメールの受信者に対して証明する方法を提供する。この方法は、eメールの送信者がその電話番号にアクセスできる旨をサーバに対して証明するために、送信者からサーバへと送信されたショート・メッセージ・サービスのメッセージを使用すること、及び、eメールを受信した後、受信したeメールの送信者がその電話番号にアクセスできる旨の確認を得るために受信者がサーバとコンタクトを取ることを含む。10

【0006】

本発明の第1の態様によれば、eメールの送信者が特定の電話番号に関連付けられた移動通信デバイスを所有する旨を、eメールの受信者に対して証明する方法が提供される。この方法は、送信者側で、インターネットを介してeメール・コンテンツの識別子及び電話番号をサーバに送信すること、サーバ側で、送信者からの識別子及び電話番号を受信し、検証コードを生成し、インターネットを介して検証コードを送信者に送信し、検証コードを識別子及び電話番号と共に格納すること、送信者側で、サーバから検証コードを受信し、当該移動通信デバイスによって送信されたショート・メッセージ・サービスのメッセージ内で検証コードをサーバに戻すこと、サーバ側で、ショート・メッセージ・サービスのメッセージの発信元である受信した検証コード及び電話番号が、格納された電話番号及び検証コードと一致することを確認した後、認証文字列を生成するために電話番号及び識別子を使用し、インターネットを介して認証文字列を送信者に送信すること、送信者側で、サーバから認証文字列を受信し、当該認証文字列及び当該電話番号を含むeメールをインターネットを介して受信者に送信すること、受信者側で、eメールを受信し、認証文字列、電話番号、及び受信したeメール・コンテンツの識別子を、当該又は他のサーバに転送すること、ならびに、受信サーバ側で、認証文字列、電話番号、及び識別子を受信し、受信した電話番号及び識別子を使用して認証文字列を生成し、受信した認証文字列が生成された認証文字列と同じであることを確認し、その確認を受信者に送信することを、含む。20

【0007】

この方法は、サーバ側で、インターネットを介して検証コードをサーバに送信した時に、タイマを開始すること、送信者から検証コードを受信した時に、タイマが満了したかどうかを判別すること、及び、タイマが満了していない場合、ショート・メッセージ・サービスのメッセージの発信元である受信した検証コード及び電話番号が、格納された電話番号及び検証コードと一致することを単に確認することを、さらに含むことができる。30

【0008】

この方法は、送信者側で、eメール・コンテンツの識別子を受信者に送信されるeメールに含めることを、さらに含むことができる。別 の方法として、eメール・コンテンツの識別子がeメール・コンテンツのハッシュ値を備える場合、この方法は、eメール・コンテンツのハッシュ値を生成することをさらに含むことができる。40

【0009】

本発明の第2の態様によれば、インターネットに接続されたユーザ端末を操作する方法が提供される。この方法は、ユーザ端末から受信者へのeメールの送信に先立って、eメール・コンテンツの識別子及び電話番号をサーバに送信すること、インターネットを介してサーバから検証コードを受信すること、インターネットを介してサーバから認証文字列50

を受信すること、認証文字列及び電話番号をeメールに含めること、ならびに、eメールを受信者に送信することを、含む。

【0010】

この方法は、eメール・コンテンツの識別子を受信者に送信されるeメールに含めることを、さらに含むことができる。別の方法として、eメール・コンテンツの識別子がeメール・コンテンツのハッシュ値を備える場合、この方法は、eメール・コンテンツのハッシュ値を生成することをさらに含むことができる。

【0011】

ユーザ端末のeメール・クライアントは、eメール・コンテンツのハッシュ値を生成するステップと、ハッシュ値及び電話番号をサーバに送信するステップとを、自動的に実行することができる。これらのステップは、ユーザ端末のユーザからの入力で自動的に実行することができる。認証文字列及び電話番号をeメールに含めるステップも、認証文字列が受信された時に、ユーザ端末のeメール・クライアントによって自動的に実行することができる。

10

【0012】

本発明の第3の態様によれば、サーバを操作する方法が提供される。この方法は、eメールの送信者からeメール・コンテンツの識別子及び電話番号を受信すること、検証コードを生成すること、インターネットを介して送信者に検証コードを送信すること、識別子及び電話番号と共に検証コードを格納すること、ショート・メッセージ・サービスのメッセージ内でサーバに戻された検証コードを受信すること、ショート・メッセージ・サービスのメッセージの発信元である受信した検証コード及び電話番号が、格納された検証コード及び電話番号と一致することを確認し、一致する場合は、認証文字列を生成するために電話番号及び識別子を使用すること、ならびに、インターネットを介して認証文字列を送信者に送信することを、含む。

20

【0013】

この方法は、インターネットを介して送信者に検証コードを送信した時に、タイマを開始すること、送信者から検証コードを受信した時に、タイマが満了したかどうかを判別すること、及び、タイマが満了していない場合、ショート・メッセージ・サービスのメッセージの発信元である受信した検証コード及び電話番号が、格納された電話番号及び検証コードと一致することを単に確認することを、さらに含むことができる。

30

【0014】

本発明の第4の態様によれば、サーバを操作する方法が提供される。この方法は、eメールの受信者から、文字列、電話番号、及びeメール・コンテンツの識別子を受信すること、受信した電話番号及び識別子を使用して認証文字列を生成すること、受信した文字列が生成された認証文字列と同じであるかどうかを判別すること、ならびに、eメール・コンテンツの送信者が電話番号に関連付けられた移動通信デバイスを所有するか否かを確認するメッセージを受信者に送信することを、含む。

【0015】

本発明の第5の態様によれば、インターネットに接続されたユーザ端末を操作する方法が提供される。この方法は、送信者からeメールを受信することであって、当該eメールは文字列及び電話番号を含む、受信すること、文字列、電話番号、及びeメール・コンテンツの識別子をサーバに送信すること、ならびに、eメール・コンテンツの送信者が電話番号に関連付けられた移動通信デバイスを所有するか否かを確認するメッセージをサーバから受信することを、含む。

40

【0016】

eメール・コンテンツの識別子がeメール・コンテンツのハッシュ値を備える場合、この方法は、eメール・コンテンツのハッシュ値を生成することをさらに含むことができる。

【0017】

文字列、電話番号、及びeメール・コンテンツの識別子をサーバに送信するステップは

50

、文字列及び電話番号を含む e メールが受信された時に、ユーザ端末の e メール・クライアントによって自動的に実行することができる。このステップは、ユーザ端末のユーザからの入力時に自動的に実行することができる。

【 0 0 1 8 】

本発明の第 6 の態様によれば、ユーザ端末として動作するように構成された装置が提供される。この装置は、受信者への e メールを生成するため、及び e メールの送信に先立つて認証文字列と電話番号とを e メールに挿入するための、e メール・クライアントと、e メール・コンテンツの識別子及び電話番号をサーバに送信するための送信機と、サーバから検証コードを受信するため、及び e メールに関する認証文字列をサーバから受信するための、受信機と、認証文字列及び電話番号を含む e メールを受信者に送信するための送信機とを、備える。
10

【 0 0 1 9 】

e メール・クライアントは、ハッシュ関数を e メール・コンテンツに適用することによって識別子を生成するように配置構成することができる。

【 0 0 2 0 】

本発明の第 7 の態様によれば、サーバとして動作するように構成された装置が提供される。この装置は、e メールの送信者から e メール・コンテンツの識別子及び電話番号を受信するための受信機と、検証コードを生成するためのコード生成ユニットと、インターネットを介して検証コードを送信者に送信するための送信機と、識別子及び電話番号と共に検証コードを格納するためのメモリと、ショート・メッセージ・サービスのメッセージ内でサーバに戻された検証コードを受信するための受信機と、ショート・メッセージ・サービスのメッセージの発信元である受信した検証コード及び電話番号が、格納された検証コード及び電話番号と一致するかどうかを判別し、一致する場合は認証文字列を生成するために電話番号及び識別子を使用するための、処理ユニットと、インターネットを介して認証文字列を送信者に送信するための送信機とを、備える。
20

【 0 0 2 1 】

この装置は、検証が送信者に送信された時に開始されるタイマをさらに備えることが可能であり、処理ユニットは、送信者から検証コードを受信した時に、タイマが満了したかどうかを判別し、タイマが満了していない場合、ショート・メッセージ・サービスのメッセージの発信元である受信した検証コード及び電話番号が、格納された電話番号及び検証コードと一致することを単に確認するように配置構成される。
30

【 0 0 2 2 】

本発明の第 8 の態様によれば、サーバとして動作するように構成された装置が提供される。この装置は、文字列、電話番号、及び e メール・コンテンツの識別子を e メールの受信者から受信するための受信機と、受信した電話番号及び識別子を使用して認証文字列を生成するための処理ユニットと、受信した文字列と生成された認証文字列とが同じであるかどうかを判別するための処理ユニットと、メッセージを受信者に送信するための送信機であって、このメッセージは受信した文字列と生成された認証文字列とが同じであるか否かを確認するものである、送信機とを、備える。

【 0 0 2 3 】

本発明の第 9 の態様によれば、ユーザ端末として動作するように構成された装置が提供される。この装置は、e メールを送信者から受信するための受信機であって、この e メールは文字列及び電話番号を含む、受信機と、文字列及び電話番号を抽出するための e メール・クライアントと、文字列、電話番号、及び e メール・コンテンツの識別子をサーバに送信するための送信機と、e メール・コンテンツの送信者が電話番号に関連付けられた移動通信デバイスを所有するか否かを示すメッセージをサーバから受信するための受信機とを、備える。
40

【 0 0 2 4 】

送信者からの e メールが識別子も含む場合、e メール・クライアントは e メールから識別子を抽出するように配置構成することができる。別の方針として、e メール・クライア
50

ントは、ハッシュ関数をeメール・コンテンツに適用することによって識別子を生成するように配置構成することができる。

【0025】

本発明の第10の態様によれば、eメール・クライアントを操作する方法が提供される。この方法は、受信者へのeメールの送信に先立ってeメール・コンテンツの識別子を生成すること、識別子及び電話番号をサーバに送信すること、サーバから検証コードを受信すること、検証コードをユーザに表示すること、サーバから認証文字列を受信すること、認証文字列及び電話番号をeメールに含めること、ならびに、eメールを受信者に送信することを、含む。

【0026】

この方法は、eメール・コンテンツの識別子を受信者に送信されるeメールに含めることをさらに含むことができる。別の方法として、ハッシュ関数をeメール・コンテンツに適用することによって生成されたハッシュ値を備える、eメール・コンテンツの識別子を生成することができる。

【0027】

本発明の第11の態様によれば、eメール・クライアントを操作する方法が提供される。この方法は、文字列及び電話番号を含むeメールの受信時に、文字列、電話番号、及びeメール・コンテンツの識別子をサーバに送信すること、ならびに、eメール・コンテンツの送信者が電話番号に関連付けられた移動通信デバイスを所有するか否かを確認するメッセージをサーバから受信することを、含む。

【0028】

eメール・コンテンツの識別子がeメール・コンテンツのハッシュ値を含む場合、この方法は、eメール・コンテンツのハッシュ値を生成することをさらに含むことができる。

【図面の簡単な説明】

【0029】

【図1】eメールの送信者が、受信者に対して、特定の電話番号にアクセスできる旨を証明するために使用可能なプロセスの例を示す概略図である。

【図2】eメールの送信者によって実施されるプロセスを示す流れ図である。

【図3】eメールの送信者と対話する場合に、検証サーバによって実施されるプロセスを示す流れ図である。

【図4】eメールの受信者によって実施されるプロセスを示す流れ図である。

【図5】eメールの受信者と対話する場合に、検証サーバによって実施されるプロセスを示す流れ図である。

【図6】eメールの送信者のユーザ端末の例を示す概略図である。

【図7】検証サーバの例を示す概略図である。

【図8】eメールの受信者のユーザ端末の例を示す概略図である。

【発明を実施するための形態】

【0030】

大多数の個人が移動通信デバイスにアクセスできること、及び、ある個人がコンタクトを取ることが予想されるすべてではないがほとんどの人々が、しばしばその個人に属している電話番号を知り、これを信用することになることが、理解されよう。したがって、次に、受信者に対してeメールの送信者が特定の電話番号を所有する旨を証明する際に使用可能であり、したがって送信者の識別を確認するための方法を受信者に提供する方法について説明する。この方法は、送信者が特定の電話番号にアクセスできる旨をサーバに対して証明するために、eメールの送信者からサーバに送信されたショート・メッセージ・サービス(SMS)のメッセージを使用することを含む。その後サーバは、eメールの受信者に対してこれを確認することができる。

【0031】

図1は、eメールを送信者の電話番号に関連付け、受信者に対してこれを証明するプロセスの例を、概略的に示す。実行されるステップは以下の通りである。

10

20

30

40

50

A 1 . 送信者 1 は、送信を希望する e メールのコンテンツを生成する。次に、送信者 1 側の e メール・クライアントは、e メール・コンテンツに関する識別子を生成する。たとえば送信者 1 は、ハッシュ値を生成するためのこのコンテンツにハッシュ関数を適用することができる。次にこのハッシュ値は、送信者の電話番号と共にインターネットを介して検証サーバ 2 へと送信される。

A 2 . サーバ 2 は、送信者 1 からハッシュ値及び電話番号を受信し、短検証コード (short verification code) 又は PIN を生成し、ハッシュ値及び電話番号と共に PIN を格納し、インターネットを介してこの PIN を送信者 1 に戻す。同時にサーバ 2 は、事前に定義された時間だけ実行されるタイマを開始する。送信者 1 に送信された PIN は、このタイマの持続時間についてのみ有効である。

A 3 . 送信者 1 はサーバ 2 から PIN を受信すると、電話番号に関連付けられた移動通信デバイスを使用して、SMS のメッセージ内で PIN をサーバ 2 に戻す。別の方法として、送信者 1 は、その移動通信デバイスを使用して、サーバ 2 に関連付けられた番号を呼び出し、接続されると、PIN をタイピング又はダイヤル・インすることができる。

A 4 . サーバ 2 は PIN を受信すると、タイマが満了したか否かを判別する。タイマがまだ満了していない場合、サーバ 2 は、SMS の発信元である受信した PIN 及び電話番号が、サーバのメモリに格納された PIN 及び電話番号と一致することを検証する。一致する場合、サーバ 2 は、認証文字列を生成する何らかのプロセス又は関数への入力として電話番号及びハッシュ値を使用する。認証文字列は、ハッシュ値及び電話番号の組み合わせに対して固有であるものとする。たとえば認証文字列は、e メール・コンテンツのハッシュ値及び電話番号の連結にハッシュ関数を適用することによって、生成可能である。サーバ 2 は、インターネットを介してこの認証文字列を送信者 1 に戻す。

A 5 . 送信者 1 は、認証文字列を受信した場合、この認証文字列、e メール・コンテンツのハッシュ値、及びそれらの電話番号を e メールに含めることができる。次に e メールは受信者 3 に送信される。e メールは、認証文字列、ハッシュ値、及び電話番号の間の関連付けを検証するために受信者 3 がコンタクトを取るべき、サービス・プロバイダの識別も含むものとする。

A 6 . 受信者 3 は e メールを受信すると、認証文字列、ハッシュ値、及び電話番号を、サーバ 2 に転送することができる。受信者 3 は、e メールと共に送信されたサービス・プロバイダの識別を使用して、コンタクトを取る適切なサーバ 2 を決定することができる。

A 7 . 次にサーバ 2 は、受信者 3 から受信した電話番号及びハッシュ値を、文字列を生成するためにステップ A 4 で使用されたものと同じプロセス又は関数への入力として使用する。次にサーバ 2 は、この生成された文字列が、受信者 3 から受信された文字列と同じであるかどうかを判別する。同じである場合、サーバ 2 は、e メール・コンテンツの送信者 1 がその電話番号に関連付けられた移動通信デバイスを所有する旨を、受信者に対して確認することができる。

【 0 0 3 2 】

加えて、受信した e メールのコンテンツに同じハッシュ関数を適用することにより、受信者 3 は、これと受信したハッシュ値とを比較し、e メール・コンテンツがサーバによって最初に検証されたものと同じであることを確認することができる。別の方法として、送信者からの e メールがハッシュ値を含まなかった場合、受信者は、ハッシュ値を生成するために、送信者によって使用されたものと同じハッシュ関数を使用することができる。このハッシュ値は、電話番号及び認証文字列と共にサーバに送信されることになる。このケースでは、受信した e メールのコンテンツが、送信者によってサーバに送信されたハッシュ値を作成するために使用されたものと同じである場合のみ、生成される文字列が e メールと共に送信された文字列と一致することになる。

【 0 0 3 3 】

図 2 は、特定の電話番号にアクセスできることを検証するために、e メールの送信者によって実施されるプロセスを示す流れ図である。実行されるステップは以下の通りである

10

20

30

40

50

。

B 1 . 送信者 1 は、送信されることになる e メールのコンテンツを生成する。

B 2 . 次に、送信者 1 の e メール・クライアント又は何らかの他のアプリケーションは、ハッシュ値を生成するためにこのコンテンツにハッシュ関数を適用することができる。

B 3 . 次に送信者は、インターネットを介して、送信者の電話番号と共にこのハッシュ値をサーバ 2 に送信する。

B 4 . 次に送信者 1 は、サーバ 2 から検証コード又は PIN を受信する。

B 5 . 次に送信者 1 は、送信者の電話番号に関連付けられた移動通信デバイスから、ショート・メッセージ・サービスのメッセージ内で PIN をサーバ 2 へ戻す。別の方 10 として、送信者 1 は、その移動通信デバイスを使用してサーバ 2 に関連付けられた番号を呼び出し、接続されると、PIN をタイピング又はダイヤル・インすることができる。

B 6 . 次に送信者 1 は、送信者の電話番号が正常に検証された旨の確認をサーバ 2 から受信し、この確認は認証文字列を含む。

B 7 . 次に送信者 1 側の e メール・クライアントは、この認証、識別子、及び送信者の電話番号を e メールに自動的に含め、この e メールを受信者に送信する。

【 0 0 3 4 】

図 3 は、e メールの送信者が特定の電話番号を所有する旨を検証するために、検証サーバによって実施されるプロセスを示す流れ図である。実行されるステップは以下の通りである。

20

C 1 . サーバ 2 は、送信者 1 からハッシュ値及び電話番号を受信する。

C 2 . サーバ 2 は、短検証コード又は PIN を生成し、インターネットを介してこの PIN を送信者 1 に送信し、ハッシュ値及び電話番号と共に PIN を格納し、タイマを開始する。

C 3 . サーバ 2 は、SMS メッセージ内で送信された PIN を受信する。

C 4 . 次にサーバ 2 は、タイマが満了したかどうかを判別する。

C 5 . タイマが満了した場合、サーバ 2 は検証が失敗した旨を送信者に通知し、ハッシュ値、電話番号、及び PIN の記録をそのメモリから消去する。

C 6 . タイマが満了していない場合、サーバ 2 は、SMS の発信元である受信した PIN 及び電話番号が、そのメモリ内に格納された PIN 及び電話番号と一致するかどうかを判別する。

30

C 7 . SMS の発信元である受信した PIN 及び電話番号が、メモリ内に格納された PIN 及び電話番号と一致しないものと判別された場合、サーバ 2 は、電話番号の検証が失敗した旨を送信者 1 に通知する。

C 8 . SMS の発信元である受信した PIN 及び電話番号が、メモリ内に格納された PIN 及び電話番号と一致するものと判別された場合、サーバ 2 は、認証文字列を生成するために何らかのプロセス又は関数への入力として電話番号及びハッシュ値を使用する。たとえば認証文字列は、e メール・コンテンツのハッシュ値及び電話番号の連結にハッシュ関数を適用することによって生成可能である。次に、サーバ 2 は、インターネットを介して認証文字列を送信者 1 に送信する。

40

【 0 0 3 5 】

e メールの送信者の電話番号がサーバに対して検証され、認証文字列が受信されると、送信者は受信者に e メールを送信することができる。少なくとも送信者は、検証された電話番号及び認証文字列を e メールに含めなければならない。図 4 は、e メールに含められた電話番号に関連付けられた移動通信デバイスを所有する旨を検証するために、e メールの受信によって実施されるプロセスを示す流れ図である。実行されるステップは以下の通りである。

D 1 . 受信者 3 は送信者から e メールを受信する。e メールは、電話番号、ハッシュ値、文字列、及びサービス・プロバイダの識別を含む。

D 2 . 受信者 3 は、サービス・プロバイダの識別を使用して、コンタクトを取るサー

50

バ2を識別する。次に受信者3は、識別されたサーバ2に対して、文字列、ハッシュ値、及び電話番号を送信する。これは、受信者のeメール・クライアントによって自動的に実行可能である。

D 3 . 受信者3は、eメールの送信者が電話番号に関連付けられた移動通信デバイスを所有するか否かを確認する応答を、サーバ2から受信する。

【0036】

図5は、eメールの送信者が特定の電話番号を所有する旨をeメールの受信者に対して確認するために、検証サーバによって実施されるプロセスを示す流れ図である。実行されるステップは以下の通りである。

E 1 . 次にサーバ2は、ハッシュ値、文字列、及び電話番号を受信者3から受信する 10
。

E 2 . 次にサーバ2は、受信者3から受信した電話番号及びハッシュ値を、文字列を生成するために上記ステップC 8で使用されたものと同じプロセス又は関数への入力として使用する。

E 3 . 次にサーバ2は、この生成された文字列が受信者3から受信した文字列と同じであるかどうかを判別する。

E 4 . 生成された文字列が受信した文字列と同じでない場合、サーバ2は電話番号の検証が失敗した旨を受信者3に通知する。

E 5 . 生成された文字列が受信した文字列と同じである場合、サーバは、eメール・コンテンツの送信者1が電話番号に関連付けられた移動通信デバイスを所有する旨の確認を、受信者3に送信する。 20

【0037】

前述のように、受信したeメールのコンテンツに同じハッシュ関数を適用することによって、受信者3は、eメール・コンテンツがサーバによって最初に検証されたものと同じであることを確認するために、受信したハッシュ値とこれを比較することができる。別 の方法として、送信者からのeメールがハッシュ値を含まなかった場合、受信者は、ハッシュ値を生成するために送信者によって使用されたものと同じハッシュ関数を使用することができる。次にこのハッシュ値は、電話番号及び認証文字列と共にサーバに送信されることになる。このケースでは、受信したeメールのコンテンツが、送信者によってサーバに送信されたハッシュ値を作成するために使用されたものと同じである場合のみ、生成された文字列はeメールと共に送信された文字列と一致することになる。 30

【0038】

前述の方法により、eメールの送信者は、送信者が特定の電話番号に関連付けられた移動通信デバイスを所有する旨を検証することによって、送信者の識別を確認するための手段を受信者に提供することができる。この検証を提供するために使用されるサーバは、通常、送信者及び受信者の双方から信頼されているサービス・プロバイダに属することになる。検証コード又はPINがSMSメッセージ内で、又は通信デバイスを使用した電話呼び出しによって、サーバに戻されることを条件として、この方法は、送信者が電話番号を所有する旨をサーバが検証できることを提供する。さらに、送信者の通信デバイスからサーバにPINが送信されなければならないことを条件として、サービス・プロバイダは、検証サービスに関して送信者に課金するための手段を有する。 40

【0039】

eメール・コンテンツのハッシュ値及び送信者の電話番号を使用した認証文字列の生成により、サーバはこの文字列を格納する必要がなくなり、それによってサーバのメモリにかかる負荷が削減される。したがって、サーバが受信者に対して確認を提供する必要がある場合、受信者から受信したハッシュ値及び電話番号のみを使用して、認証文字列を再作成することができる。ハッシュ値及び電話番号が、受信した文字列を作成するために使用されたものと同じである場合のみ、生成された文字列が受信した文字列と一致することになる。したがって認証文字列を作成するために使用される関数又はプロセスは、文字列がeメール・コンテンツ及び電話番号の特定の組み合わせに対して固有であることを保証す 50

るものとし、さらに、容易に反転(invert)できないものとする。たとえば認証文字列は、サーバのみに知られているハッシュ関数をeメール・コンテンツのハッシュ値及び電話番号の連結に適用することによって、生成可能である。

【 0 0 4 0 】

図6は、eメールの送信に使用される予定であり、前述の方法を実施するために好適な、ユーザ端末4の例を概略的に示す。ユーザ端末4は、コンピュータのハードウェア及びソフトウェアの組み合わせとして実装可能である。ユーザ端末4は、eメール・クライアント5、送信機6、及び受信機7を備える。eメール・クライアント5は、ユーザから受信者へのeメールを生成するため、及び、ハッシュ値を生成するためにeメール・コンテンツにハッシュ関数を適用するために、好適である。送信機6は、eメール・コンテンツのハッシュ値及び電話番号をサーバに送信するため、及び、固有文字列及び電話番号と共にeメールを受信者に送信するために、好適である。送信機6は、eメール・コンテンツのハッシュ値をeメールと共に受信者に送信するためにも好適な可能性がある。受信機7は、サーバからPINを受信するため、及びサーバからeメールに関する固有文字列を受信するために、好適である。10

【 0 0 4 1 】

図7は、前述の方法を実施するために好適な検証サーバ2の例を概略的に示す。サーバ2は、コンピュータのハードウェア及びソフトウェアの組み合わせとして実装可能である。サーバ2は、受信機8、コード生成ユニット9、送信機10、メモリ11、SMSクライアント12、及び処理ユニット13を備える。受信機8は、eメールの送信者からeメール・コンテンツのハッシュ値及び電話番号を受信するために好適である。PIN生成ユニット9は、PINを生成するために好適である。送信機10は、PINを送信するため、及びインターネットを介して固有文字列を送信者に送信するために、好適である。メモリ11は、ハッシュ値及び電話番号と共にPINを格納するために好適である。SMSクライアント12は、PINを含むショート・メッセージ・サービスのメッセージを受信するために好適である。処理ユニット13は、受信したPINが格納されたPINと一致するかどうかについて電話番号を検証するために好適であり、一致する場合は、電話番号及びハッシュ値を使用してeメールに関する固有文字列を生成するために好適である。サーバ2は、PINが送信者に送信された時に開始されるタイマ14も備えることができる。次に処理ユニット13は、PINを含むショート・メッセージ・サービスのメッセージがタイマ14の満了に先立って受信されたかどうかについてのみ、電話番号を検証することになる。20

【 0 0 4 2 】

加えて、受信機8は、eメールの受信者から、文字列、電話番号、及びeメール・コンテンツのハッシュ値を受信するためにも好適である。処理ユニット13は、受信した文字列が、受信した電話番号及びハッシュ値を使用して生成された固有文字列と同じであるかどうかを判別するためにも好適であり、同じである場合、eメール・コンテンツの送信者が電話番号にアクセスできることを検証するために好適であり、送信機10は、検証が成功したか否かを示すメッセージを受信者に送信するためにも好適である。30

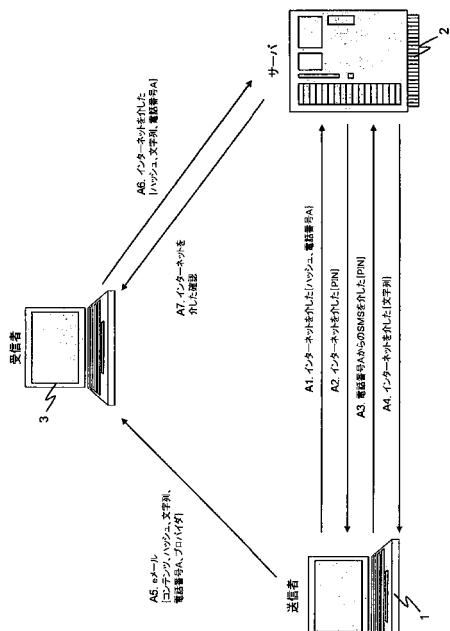
【 0 0 4 3 】

図8は、eメールを受信するために使用され、前述の方法を実施するために好適な、ユーザ端末15の例を概略的に示す。ユーザ端末15は、コンピュータのハードウェア及びソフトウェアの組み合わせとして実装可能である。ユーザ端末15は、受信機16、送信機17、及びeメール・クライアント18を備える。受信機16は、送信者から文字列及び電話番号と共にeメールを受信するため、及び、eメール・コンテンツの送信者が電話番号にアクセスできる旨の検証をサーバから受信するために、好適である。送信機17は、文字列、電話番号、及びeメール・コンテンツのハッシュ値をサーバに送信するために好適である。eメール・クライアント18は、ハッシュ値を生成するためにeメール・コンテンツにハッシュ関数を適用するため、及びeメールから文字列及び電話番号を自動的に抽出するために好適である。4050

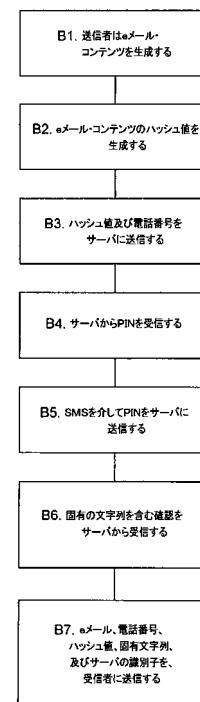
【 0 0 4 4 】

当業者であれば、本発明の範囲を逸脱することなく、前述の諸実施形態に対して様々な修正が実行可能であることを理解されよう。

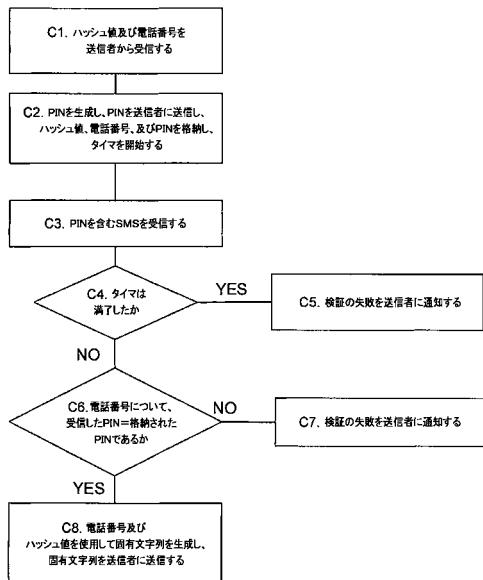
【 図 1 】



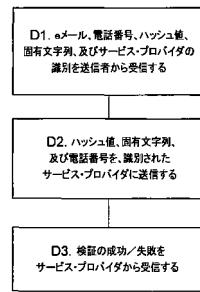
【 図 2 】



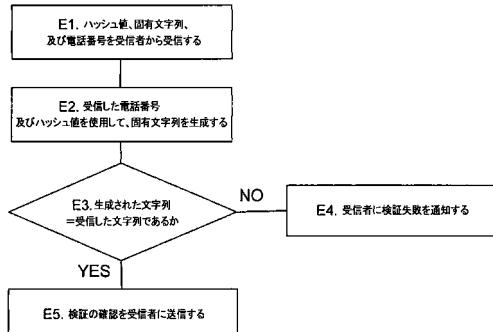
【図3】



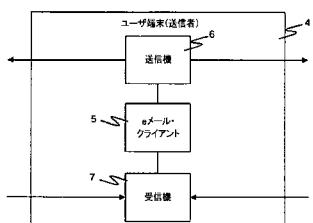
【図4】



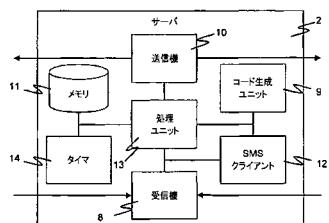
【図5】



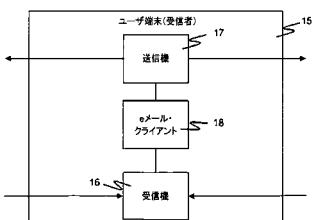
【図6】



【図7】



【図8】



フロントページの続き

(72)発明者 サルメラ , パトリック

フィンランド国 , カークコナミ エフアイエヌ - 0 2 4 0 0 , クーニンカンティエ 5 - 7 ピー
2 0

(72)発明者 アミン , パース イレシュクマー

インド , アフマダーバード 3 8 0 0 1 3 , ナランプラ , プラティマ パーク 2 ピー

(72)発明者 スシタイヴァル , リーツカ

フィンランド国 , ヘルシンキ エフアイエヌ - 0 0 2 5 0 , マンネルヘイミンティエ 8 2 エー
1 3

(72)発明者 ウェイジャー , ステファン

フィンランド国 , エスポー エフアイ - エフユーエヌ - 0 2 3 6 0 , ガルトスグランデン 8 エ
イチ

審査官 松元 伸次

(56)参考文献 特開2004-159164(JP,A)

特開2005-051475(JP,A)

(58)調査した分野(Int.Cl. , DB名)

H 0 4 M 3 / 0 0

3 / 1 6 - 3 / 2 0

3 / 3 8 - 3 / 5 8

7 / 0 0 - 7 / 1 6

1 1 / 0 0 - 1 1 / 1 0