(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5028425号
(P5028425)
(45)発行日　平成24年9月19日(2012.9.19)　(24)登録日　平成24年6月29日(2012.6.29)

(51)Int.Cl.　F I
H04L 12/58 (2006.01)　H04L 12/58　100Z

請求項の数 13　(全 17 頁)

(21)出願番号	特願2008-552876 (P2008-552876)	(73)特許権者	397011166
(86)(22)出願日	平成19年1月30日 (2007.1.30)		トレンドマイクロ株式会社
(65)公表番号	特表2009-525654 (P2009-525654A)		東京都渋谷区代々木２－１－１　新宿マインズタワー
(43)公表日	平成21年7月9日 (2009.7.9)	(74)代理人	100125689
(86)国際出願番号	PCT/GB2007/000300		弁理士　大林　章
(87)国際公開番号	WO2007/088337	(74)代理人	100125335
(87)国際公開日	平成19年8月9日 (2007.8.9)		弁理士　矢代　仁
審査請求日	平成22年1月29日 (2010.1.29)	(72)発明者	ダンサー、アンドリュー
(31)優先権主張番号	0602131.5		イギリス、ビーエス１　６イーエム、ブリストル、テンプル　キー、フライアリー１、アイデンタム・リミテッド内
(32)優先日	平成18年2月2日 (2006.2.2)		
(33)優先権主張国	英国(GB)		

審査官　松崎　孝大

最終頁に続く

(54)【発明の名称】電子データ通信システム

(57)【特許請求の範囲】
【請求項１】
１以上の受信者へ電子メッセージを伝送するためのシステムであって、
通信ネットワークに接続されるネットワーク装置を有する通信ネットワークを有し、
前記ネットワーク装置はメールサーバおよび暗号鍵サーバを有し、
前記メールサーバは複数の前記ネットワーク装置のいずれかを用いた前記１以上の受信者からのアクセスのために電子メッセージを記憶することが可能であり、
少なくとも一つのネットワーク装置が前記１以上の受信者への伝送のために暗号化された電子メッセージを生成することが可能であり、
前記暗号化されたメッセージは、セッション鍵を用いた対称暗号化アルゴリズムにより暗号化された前記１以上の受信者へのメッセージに対応する暗号化されたメッセージデータと、前記受信者に関連する各々の公開鍵を用いた非対称暗号化アルゴリズムによって暗号化された前記セッション鍵に対応する各受信者に対する暗号化されたセッション鍵データとを備え、
前記メールサーバに記憶された暗号化されたメッセージへの１の受信者からのアクセス要求に応答して、前記メールサーバは前記暗号化された当該１の受信者に対応するセッション鍵データを前記暗号鍵サーバに転送するために前記暗号化された電子メッセージから抽出することが可能であり、
前記暗号化されたセッション鍵データの受信に応じて、前記暗号鍵サーバは、前記暗号化されたセッション鍵のデータを前記受信者に関連する秘密鍵を用いて復号化することに

よって、前記暗号鍵サーバから離れたリモートネットワーク装置へ転送するために、セッション鍵を再生することが可能であり、
前記リモートネットワーク装置は、前記暗号鍵サーバにより再生された前記セッション鍵を用いて、前記暗号化されたメッセージデータから前記メッセージを再生することが可能であるシステム。
【請求項２】
前記メールサーバは、前記暗号鍵サーバのネットワークアドレスと前記暗号化されたセッション鍵のデータとリダイレクトネットワークアドレスとを有するリンクデータを生成することが可能であり、
前記暗号鍵サーバは前記再生されたセッション鍵を前記リダイレクトネットワークアドレスへ転送することが可能である、
請求項１に記載のシステム。
【請求項３】
前記リンクデータは、更に前記受信者の識別データを有する、
請求項２に記載のシステム。
【請求項４】
前記リンクデータは、前記暗号化された電子メッセージが送信された期間を特定する時間データを更に有する、
請求項２又は３に記載のシステム。
【請求項５】
前記リンクデータは、統一資源位置指定子を有する、
請求項２～４のいずれかに記載のシステム。
【請求項６】
前記リモートネットワーク装置が前記メールサーバであり、前記再生されたセッション鍵が前記メールサーバに転送され、
前記メールサーバは前記暗号化されたメッセージデータを前記再生されたセッション鍵を用いて復号化することが可能である、
請求項１～５のいずれかに記載のシステム。
【請求項７】
前記受信者に関連する前記公開鍵が前記受信者の識別情報を用いて生成される、
請求項１～６のいずれかに記載のシステム。
【請求項８】
前記識別情報は、前記受信者の電子メールアドレスである、
請求項７に記載のシステム。
【請求項９】
i）セッション鍵を用いた対称暗号化アルゴリズムで暗号化された受信者のメッセージに対応する暗号化されたメッセージデータと、ii）前記受信者に関連する公開鍵を用いた非対称暗号化アルゴリズムで暗号化された前記セッション鍵に対応する暗号化されたセッション鍵データとを有する、暗号化された受信者への電子メッセージを記憶することが可能であるデータ記憶部と、
リモートネットワーク装置とデータを送受信することが可能であるネットワークインタフェースと、
暗号化されたメッセージへのアクセス要求に従い、前記要求された電子メッセージから前記暗号化されたセッション鍵データを抽出し、前記抽出された暗号化されたセッション鍵データをリモートネットワーク装置に転送することが可能であるプロセッサを備え、
前記プロセッサは暗号化されたセッション鍵データと暗号鍵サーバのネットワークアドレスとリダイレクトネットワークアドレスとを有するリンクデータを生成することが可能である、ネットワークサーバ。
【請求項１０】
前記プロセッサは、前記受信者の識別情報を更に有するリンクデータを生成することが

可能である、
請求項９に記載のネットワークサーバ。
【請求項１１】
前記プロセッサは、前記暗号化された電子メッセージが送信された期間を特定する時間データを更に有するリンクデータを生成することが可能である、
請求項９に記載のネットワークサーバ。
【請求項１２】
前記リンクデータは、統一資源位置指定子を有する、
請求項９に記載のネットワークサーバ。
【請求項１３】
コンピュータを請求項９～１２のいずれかに記載のネットワークサーバとして動作させるためのプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、電子メールメッセージングシステム、特に、人に対して電子的にメッセージを送ったり、人からメッセージを電子的に受信したりするシステムに関わる。
【背景技術】
【０００２】
電子メールメッセージングは広く利用されている。また、非対称暗号化アルゴリズムを用いた公開鍵暗号方式によって電子メールメッセージを暗号化することもよく知られている。特に、電子メール受信者の公開鍵は、送信者がメッセージを暗号化するのに使用されている。得られた暗号化メッセージは、公開鍵と異なった、メッセージ受信者によりアクセスが管理されている秘密鍵によってのみ復号化されうる。
【０００３】
公開鍵暗号方式に用いられる非対称暗号化アルゴリズムにおける問題点は、同一の暗号鍵を暗号化にも復号化にも使用する対称暗号化アルゴリズムと比較して、動作が遅いことである。以前より、この問題点はいわゆるＫＥＭ－ＤＥＭアプローチを用いた電子メールメッセージングによって対処されてきている。ＫＥＭ－ＤＥＭアプローチとは、受信者の公開鍵を用いて暗号化された（メッセージに対し固有な）セッション鍵を記憶する鍵カプセル化メカニズム（Key Encapsulation Mechanism，ＫＥＭ）部分と、ＫＥＭ部分に暗号鍵として記憶されたセッション鍵を用いた対称暗号化アルゴリズムによって暗号化された電子メールメッセージを記憶するデータカプセル化部分（Data Encapsulation Mechanism，ＤＥＭ）とから成る暗号化電子メールメッセージを作成する方法である。この方法で、非対称暗号化アルゴリズムによって復号化されるデータ量を削減している。
【０００４】
公開鍵暗号方式は、受信者が電子メールメッセージを見るときに、常に私有のコンピュータ、すなわち受信者の管理下にあって他人は自由にアクセスできないコンピュータを使うときには有効である。
【０００５】
今日では、インターネットに接続しているどんなコンピュータからでも、リモートネットワーク機器上のメールボックス内に記憶された電子メールメッセージにアクセスできる”ウェブメール”サービスが利用可能である。このようなウェブメールサービスは、ユーザのメールボックスを電子メールメッセージングサービス提供者（例えばホットメール（商標）およびヤフー（登録商標））のサーバ上に恒久的に記憶するというサービス、および受信者が関連するコンピュータにダウンロードされるまで電子メールメッセージングサービス提供者に一時的に格納されたメッセージへのアクセスを可能にするサービスも提供している。ユーザはこれらのウェブメールサービスを利用することで、誰でも使用できるコンピュータ、例えばインターネットカフェにあるコンピュータから電子メールメッセージにアクセスできる。

【発明の開示】
【発明が解決しようとする課題】
【０００６】
誰でも使用できるコンピュータを用いて電子メールメッセージにアクセスすることの問題点は、自由に使えるコンピュータ上で秘密鍵を用いることによりその秘密鍵の情報が漏洩する危険性があるため、従来の公開鍵暗号方式の使用が安全とは言えないことである。
【課題を解決するための手段】
【０００７】
本発明は、上記のＫＥＭ－ＤＥＭアプローチを用いて暗号化された電子メールメッセージを受信者に送信する電子データ通信システムを提供するものである。第１のネットワーク装置を操作する受信者がウェブメールサービスを使用して第２のネットワーク装置に記憶された暗号化電子メールメッセージにアクセスするときに、そのメッセージの中にある暗号化されたセッション鍵を記憶している部分が、信頼できる第三者機関が運用する第３のネットワーク装置に送信される。第３のネットワーク装置はユーザの秘密鍵にアクセスする。第３のネットワーク装置が暗号化されたセッション鍵をユーザの秘密鍵を用いて復号化した後、復号化されたセッション鍵をリモートネットワーク装置（例えば第１または第２のネットワーク装置）に対して第三者機関が送信し、セッション鍵によってＤＥＭ部分がそのリモートネットワーク装置で復号化されることでユーザはメッセージを読めるようになる。このようにして、信頼できる第三者機関はユーザの秘密鍵にはアクセスするが、暗号化されたメッセージには全くアクセスしないようになっている。
【０００８】
１つの実施形態では、信頼できる第三者機関がユーザへの秘密鍵の提供者である。この方法では、他のいかなる者にも秘密鍵を明らかにする必要はない。
【０００９】
好ましい実施形態では、電子メールメッセージの受信者のための非対称暗号化アルゴリズムの公開鍵を、受信者識別情報を含む公的に利用可能な情報を用いて生成する。この方法によれば、たとえ電子メールメッセージの送信時に受信者が秘密鍵を持っていなくても、送信者は受信者のための公開鍵を生成できる。このような非対称暗号化アルゴリズムは１９８４年にShamirによって初めて提唱され、２０００年にSakaiとKasaharaによって初めて生成され、以来多くの研究グループによって更なる開発が進められている。
【発明を実施するための最良の形態】
【００１０】
図１に示されるように、電子メールメッセージングシステムは、メールメッセージの送信者に関連する送信コンピュータ１と、受信者に関連する受信コンピュータ３を有しており、これらはインターネット５によって相互に接続されている。当然のことながら、インターネットに接続されている他の多数のコンピュータが存在し、それらのコンピュータのいずれもが送信コンピュータおよび／または受信コンピュータと成り得る。
【００１１】
この実施形態において、電子メールメッセージの受信者は、ウェブメールサービスを提供する電子メールメッセージングサービス提供者のクライアントである。具体的には、電子メールメッセージングサービス提供者は、インターネットに接続され受信者向けの電子メールメッセージを記憶するサーバ７を有する。説明のために、この実施形態においては電子メールメッセージングサービス提供者のサーバ７（以後ＥＭＳＰサーバと呼ぶ）に、架空の統一資源位置指定子（Uniform Resource Locator，ＵＲＬ）としてwww.privatewebmail.comを割り当て、受信者には電子メールアドレスbob@privatewebmail.comを割り当てる。
【００１２】
更に、この実施形態においては、受信者はインターネットに接続されたサーバ９を運用する暗号鍵機関のクライアントでもある。以後、サーバ９を信頼できる第三者機関サーバと呼ぶ。説明のために、信頼できる第三者機関サーバ９に架空のＵＲＬとしてwww.myencr

yption.comを割り当てる。

【００１３】

この実施形態において、暗号鍵機関は、WO03/017559号公報に記載された暗号化アルゴリズムによるルート公開鍵K^{G}_{pub}を有する公開鍵証明書を発行する。ここにWO03/017559号公報を参照することによりその全内容は本明細書の一部とする。この暗号化アルゴリズムにより、"client_ID"という電子メールアドレスを有するクライアントの公開鍵K^{C}_{pub}が以下の式で与えられる。

【数１】

$$K^{c}_{pub} = F(client\_ID, K^{G}_{pub})$$

【００１４】

ここで、Ｆは公に利用可能な関数である。この方法においては、電子メールアドレスＩＤに関連する公開鍵は誰にでも算出し得る。しかし、この電子メールアドレスと関連する秘密鍵は、暗号鍵機関によって秘密に保たれているルート秘密鍵K^{G}_{pri}を知っている場合にのみ算出し得る。具体的には、電子メールアドレス"client_ID"を有するクライアントの秘密鍵K^{C}_{pri}は信頼できる第三者機関サーバ９により、以下の方程式に従って算出される。

【数２】

$$K^{c}_{pri} = G(client\_ID, K^{G}_{pri})$$

【００１５】

ここで、ＧはＦと対になった関数である。

【００１６】

暗号化電子メールメッセージを受信者に送信するために、送信コンピュータ１は受信者の電子メールアドレスと、暗号機関（暗号鍵機関）により提供され受信者の公開鍵を算出するためのルート公開鍵を使用する。それから送信コンピュータ１は、WO2005/050908号公報に開示された過程に従い受信者に対して算出された公開鍵を用いて、暗号化電子メールメッセージを生成する。ここに、WO2005/050908号公報を参照することによりその内容を本明細書の一部とする。

【００１７】

要約すれば、図２に示すように、ユーザの指示に応答して電子メールメッセージの暗号化が開始（Ｓ１）した後、送信コンピュータが電子署名を生成し、その電子署名をメッセージに添付して署名済みのメッセージを作成する（Ｓ３）。具体的には、送信コンピュータ１は、メッセージを一方向性の暗号化アルゴリズム（ハッシング関数とも呼ばれる）を用いて処理し、そのメッセージを表すハッシュ値を生成した後、送信コンピュータ１のユーザに関連する秘密鍵を用いてハッシュ値を暗号化する。

【００１８】

それから、送信コンピュータ１は乱数発生器を用いてセッション鍵K_sを生成する（Ｓ５

）。その後、送信コンピュータ１はセッション鍵K_sを対称暗号化アルゴリズムの暗号鍵として用いて署名済みのメッセージを暗号化して、暗号化電子メールメッセージのＤＥＭ部分を生成する（Ｓ７）。具体的には、この実施形態において使用される対称暗号化アルゴリズムは高度暗号化標準（Advanced Encryption Standard，ＡＥＳ）アルゴリズムである。

【００１９】

送信コンピュータ１は電子メールメッセージの各受信者に対し、受信者の公開鍵K^C_{pub}を用いてセッション鍵K_sを暗号化し、得られた複数の暗号化セッション鍵を結合して暗号化電子メールメッセージのＫＥＭ部分を生成する（Ｓ９）。言い換えれば、電子メールメッセージが３人の受信者に送信されるとすると、ＫＥＭ部分はそれぞれ異なった受信者の公開鍵を用いて暗号化された３バージョンのセッション鍵K_sを含むことになる。

【００２０】

その後、送信コンピュータ１はＫＥＭ部分とＤＥＭ部分を結合し暗号化電子メールメッセージを作成する（Ｓ１１）。最後に、送信コンピュータ１は暗号化電子メールメッセージを複数の受信者に送信する（Ｓ１３）。

【００２１】

上記のように、受信コンピュータ３に関連する受信者はＥＭＳＰサーバ７に関連する電子メールメッセージングサービス提供者で有効なアカウントを有する。従って、暗号化電子メールメッセージは任意のコンピュータからアクセスしうるＥＭＳＰサーバ７に向けて送信される。

【００２２】

図３はＥＭＳＰサーバ７の主要な構成要素を概略的に示している。図示のように、ＥＭＳＰサーバ７は、バスシステム２９によって相互に接続された、プロセッサ２１、メモリ２３、操作者インタフェース２５およびネットワークインタフェース２７を有する。

【００２３】

この実施形態においては、操作者インタフェース２５は操作者がＥＭＳＰサーバ７にデータを入力するためのキーボードと、ＥＭＳＰサーバ７で生成されたデータを読むためのディスプレイを有する。この操作者インタフェース２５は、ＣＤ－ＲＯＭ３１に記憶されたデータをＥＭＳＰサーバに入力したり、記録可能なＣＤ－ＲＯＭ３１にデータを書き込んだりするＣＤ－ＲＯＭ読み書き装置も有する。

【００２４】

ネットワークインタフェース２７は、リモート装置とデータの送受信をネットワーク信号３３の形式にて行う。

【００２５】

プロセッサ２１はメモリ２３に記憶されたプログラムルーチンに従い演算処理を行う。これらのプログラムルーチンは製造工程中に記憶されてもよいし、操作者インタフェース２５またはネットワークインタフェース２７を経由してＥＭＳＰサーバ７に入力されてもよい。これらのプログラムルーチンはメモリ２３に記憶されたデータおよび操作者インタフェース２５またはネットワークインタフェース２７で受信されたデータを処理する。

【００２６】

当業者には理解できるように、従来と同様に、メモリ２３はデータの読み出しにあたってそれぞれが異なるアクセス時間を持つ様々な形態のメモリによって構成される。例えば、アクセス時間の比較的遅いハードディスクドライブ領域と、比較的早いランダムアクセスメモリ（ＲＡＭ）領域をメモリ２３は有する。必要になりそうなデータを前もってＲＡＭにキャッシュしておくことによって処理速度を改善するために従来の処理技術が用いられる。

【００２７】

メモリ２３は、ＥＭＳＰサーバ７が使用するプログラムルーチンを記憶する領域３５、データ記憶領域３７および作業メモリとなる領域３９を含む。

【００２８】

具体的には、領域３５に記憶されるプログラムは以下のものである。
・ソフトウェアルーチンとサーバ７のハードウェア構成要素とを結び付けるオペレーティングシステム（Operating_System）４１。
・ウェブサーバ機能を提供するウェブサーバ（Web_Server）４３。
・主制御ルーチン（Master_Control routine）４５。
・メッセージ表示サブルーチン（Display_Message sub-routine）４７。
・暗号化アルゴリズムルーチン（Encryption_algorithm routine）４９（この実施形態においてはＡＥＳ暗号化アルゴリズム）。

【００２９】
データ記憶メモリ領域３７は以下を記憶する。
・各クライアントのユーザ名、電子メールアドレスおよびログオン情報（例えばパスワード）を記憶するクライアントデータベース５１。
・送信者および受信者の電子メールアドレスを含むメッセージを記憶するメッセージデータベース５３。
・ブラウザプログラムへ送信されるウェブページを生成する際にウェブサーバ４３に使用されるウェブページのテンプレート。
・以下に記述するセッション鍵を待つ間、暗号化されたメッセージのＤＥＭ部分を記憶するメッセージキャッシュ５７。

【００３０】
受信コンピュータ３のクライアントがＥＭＳＰサーバ７に記憶された電子メールメッセージにアクセスしようとする際、クライアントは従来のブラウザプログラム（例えばマイクロソフト（登録商標）インターネットエクスプローラー（商標））の受信コンピュータ上で使用し、ＥＭＳＰサーバ７のＵＲＬ（すなわちこの実施例ではwww.privatewebmail.com）を入力することによってアクセス要求をＥＭＳＰサーバ７に送信する。

【００３１】
主制御ルーチン４５は、アクセス要求の受信に応答しウェブセッションを起動する。図４はウェブセッションにおいて実行される主ステップを示したフローチャートである。

【００３２】
ウェブセッションの起動（Ｓ２１）後、ＥＭＳＰサーバ７がログオンプロシージャを実行する（Ｓ２３）。具体的には、ＥＭＳＰサーバ７は、クライアントが自分の電子メールメッセージアドレスとログオン情報を記入するデータ入力ボックスを持つログオンページを受信コンピュータ３に表示させるよう、ログオンウェブページのデータをウェブページテンプレート５５から受信コンピュータ３に送信する。それから、入力された電子メールメッセージアドレスとログオン情報は受信コンピュータ３によってＥＭＳＰサーバ７に送信され、ＥＭＳＰサーバ７は、受信されたデータと、クライアントデータベース５１上に記憶された対応するデータを比較して、クライアントの本人確認をする。

【００３３】
クライアントの本人確認の後、ＥＭＳＰサーバ７はメッセージデータベース５３に記憶されたそのクライアントのためのメッセージのリストを表示するウェブページのデータを送信する（Ｓ２５）。具体的には、ＥＭＳＰサーバ７がメッセージデータベース５３に「このクライアントが指定された受信者であるメッセージ」というクエリーを行い、これにより特定されたメッセージの送信者欄、タイトル欄、送信時欄およびメッセージサイズ欄を含むデータを、メモリ領域５５に記憶されたウェブページテンプレートへ入れる。この実施形態においては、従来のＨＴＭＬプログラミング技術を用いて各メッセージのタイトルがハイパーリンク化され、メッセージデータベース５３内の対応したメッセージにアクセスできるようになっている。メッセージのリストに加え、このウェブページはウェブセッションを終了するためのログアウトボタンも表示する。

【００３４】
ＥＭＳＰは受信コンピュータ３に対しメッセージのリストを表示するウェブページのデータを送信した後、受信コンピュータ３からの次のコマンドを待つ（Ｓ２９）。クライア

ントは、ウェブページ上のメッセージのリストとログアウトボタンを見ながら、見たいメッセージのタイトルをクリックして選択するか、ログアウトボタンを押してセッションを終了するかを選ぶ。

【００３５】

ＥＭＳＰサーバ７は、受信コンピュータ３からのコマンドを受信すると、このコマンドがメッセージを表示するための選択なのかどうか確認する（Ｓ２９）。もしこのコマンドがメッセージを表示するための選択でなければ（言い換えると、クライアントがログアウトボタンを押したら）、ＥＭＳＰサーバ７はクライアントをログアウトさせ（Ｓ３７）、ウェブセッションを終了する（Ｓ３９）。

【００３６】

このコマンドがメッセージを表示するための選択であれば、主制御ルーチン４５が後に詳述されるメッセージ表示サブルーチンを起動する（Ｓ３１）。このメッセージ表示サブルーチンによって、メッセージを表示するためのウェブページデータが、メッセージのリストへ戻るボタンおよびログアウトボタンを表示するためのデータと共に受信コンピュータ３に送信される。それから、ＥＭＳＰサーバ７は受信コンピュータ３からのコマンドを待つ（Ｓ３３）。

【００３７】

次のコマンドを受信すると、クライアントが受信コンピュータ３でボタンを押して送信したコマンドはメッセージリスト再表示を要求するのか、それともログアウトを要求するのかをＥＭＳＰサーバ７が確認する（Ｓ３５）。そのコマンドがメッセージリスト再表示の要求であれば、ＥＭＳＰサーバ７はメッセージリストのウェブページデータを再送信する（Ｓ２５）。そのコマンドがログアウト要求であれば、ＥＭＳＰサーバ７はこのクライアントをログアウトさせ（Ｓ３７）、ウェブセッションを終了する（Ｓ３９）。

【００３８】

メッセージ表示サブルーチン４７について詳細を説明する。図５に示されるように、表示すべきメッセージが選択されたのに応答してメッセージ表示サブルーチン４７が起動する（Ｓ５１）と、選択されたイメージが暗号化されているかどうかをＥＭＳＰサーバ７が解析する（Ｓ５３）。具体的には、選択されたメッセージ内に、それが暗号化されたメッセージであることを示すバイト列があるかどうかＥＭＳＰサーバ７が探索する。

【００３９】

選択されたメッセージが暗号化されていないとＥＭＳＰサーバ７が判断すると（Ｓ５５）、そのメッセージを表示するためのウェブページのデータを、「受信ボックスに戻る」ボタンとログアウトボタンのデータと共に、ＥＭＳＰサーバ７が受信コンピュータ３に送信する（Ｓ５７）。その後、メッセージ表示サブルーチン４７が終了する（Ｓ７１）。

【００４０】

選択されたメッセージが暗号化されているとＥＭＳＰサーバ７が判断すると（Ｓ５５）、そのメッセージのＫＥＭ部分から、受信コンピュータ３で既にクライアントの公開鍵で暗号化されたバージョンのセッション鍵をＥＭＳＰサーバ７が抽出する（Ｓ５９）。それから、ＥＭＳＰサーバ７は、メッセージキャッシュ５７にＤＥＭ部分を記憶しＵＲＬリンクを算出する（Ｓ６１）。このＵＲＬリンクは、受信コンピュータ３のブラウザプログラムを信頼できる第三者機関サーバ９へ導くため、かつ、第三者機関サーバ９がセッション鍵を再生したりＥＭＳＰサーバ７にこのセッション鍵を送信したりするのに必要な情報を伝えるためのものである。このＵＲＬの例を以下に示す。

https://www.myencryption.com/webmail/?user=bob@privatewebmail.com&key=fnf94338b3b8b43fb93n43n&date=20051229110300&returnurl=www.privatewebmail.com/ViewPPMessage?MessageID=12345

【００４１】

このＵＲＬのフォーマットをこれから説明する。

https://www.myencryption.com/webmail/　－　信頼できる第三者機関サーバと暗号化されたウェブセッションを確立し、セッション鍵の復号化が必要であることを示す。

user=bob@privatewebmail.com　－　信頼できる第三者機関サーバ９へ容易にログオンできるよう受信コンピュータ３を使うクライアントの識別情報を示す。
key=fnf94338b3b8b43fb93n43n　－　暗号化されたセッション鍵を提供する。
date=20051229110300　－　正しいルート秘密鍵を選択できるように、選択されたメッセージが送信された日時を提供する。
returnurl=www.privatewebmail.com/ViewPPMessage　－　復号化されたセッション鍵が転送されるべきウェブアドレスを与える。
MessageID=12345　－　セッション鍵を用いて復号化されるべきメッセージキャッシュ５７の中にあるメッセージを示す。

【００４２】

それから、ＥＭＳＰサーバ７はウェブページを表示するためのデータを受信コンピュータ３に送信する（Ｓ６３）。このウェブページは、そのメッセージが暗号化されていることを示すとともに、受信コンピュータ３のクライアントが算出されたＵＲＬリンクをクリックするよう要求するものである。その後、ＥＭＳＰサーバ７は復号化されたセッション鍵を待つ（Ｓ６５）。

【００４３】

信頼できる第三者機関サーバ９がセッション鍵を復号化する方法を、図６と図７を参照して説明する。

【００４４】

図６に示すように、信頼できる第三者機関サーバ９は、バスシステム７９によって相互に接続されたプロセッサ７１、メモリ７３、操作者インタフェース７５およびネットワークインタフェース７７を有する。プロセッサ７１、操作者インタフェース７５およびネットワークインタフェースの機能はＥＭＳＰサーバ７の対応する構成要素と同じであるため、再び詳述しない。ただし、作業者インタフェースによってＣＤ－ＲＯＭ８１とデータ転送ができ、ネットワークインタフェース７７によってリモートネットワークに対してネットワーク信号８３の形式でデータ転送ができる。

【００４５】

メモリ７３は、信頼できる第三者機関サーバ９の使うプログラムルーチンを記憶する領域８５、データを記憶する領域８７および作業メモリとなる領域８９を含む。

【００４６】

具体的には、プログラムルーチン記憶領域８５に記憶されるプログラムは以下のものである。

・ソフトウェアルーチンとサーバ９のハードウェア構成要素とを結び付けるオペレーティングシステム（Operating_System）９１。
・ウェブサーバ機能を提供するウェブサーバ（Web_Server）９３。
・主制御ルーチン（Master_Control routine）９５。
・秘密鍵算出サブルーチン（Calculate_Private_Key sub-routine）９７。
・セッション鍵復号化サブルーチン（Decrypt_Session_Key sub-routine）９９。

【００４７】

この実施形態においては、秘密鍵算出サブルーチン９７とセッション鍵復号化サブルーチンは、WO03/017559号公報に述べられた暗号化アルゴリズムを利用しているため、ここでは詳述しない。

【００４８】

データ記憶メモリ領域８７は以下を記憶する：

・各クライアントのユーザ名、電子メールアドレスおよびログオン情報を記憶するクライアントデータベース１０１。
・各期間のルート秘密鍵を示すテーブルを記憶する鍵データベース。
・ブラウザプログラムへ送信されるウェブページを生成する際にウェブサーバ９３に使用されるウェブページのテンプレート。

【００４９】

クライアントが受信コンピュータ３でＥＭＳＰサーバ７が提供したＵＲＬリンクをクリックした際の送信シグナルに応答して、信頼できる第三者機関サーバ９はウェブセッションを開始する（Ｓ８１）。はじめに、信頼できる第三者機関サーバ９はそのＵＲＬに付加された情報を記憶し（Ｓ８３）、このクライアントの本人認証をする（Ｓ８５）。この実施形態においては、多くのオンラインバンキングウェブサイトで採用されている方法である、そのクライアントのログオン情報のうちランダムに選択された要素を要求するウェブページを送信することで認証を実行する。この方法では、受信コンピュータ３を肩越しに覗かれたり、受信コンピュータ３と信頼できる第三者機関サーバ９の間のネットワーク信号を傍受されたりして、入力された情報がコピーされてそのクライアントになりすますために使われないように、要求されるログオン情報はログオンごとに変化する。

【００５０】

ユーザの認証後、信頼できる第三者機関サーバ９は、秘密鍵算出サブルーチン９７を起動する（Ｓ８７）。秘密鍵算出サブルーチン９７は、暗号化されたセッション鍵を復号化するためのクライアントの秘密鍵を算出する。このため、秘密鍵算出サブルーチン９７は、メッセージが送信された時の期間に、鍵データベース１０３に記憶されているルート秘密鍵と、クライアントの識別情報を使う。それから、算出されたクライアントの秘密鍵を使ってセッション鍵を復号化するセッション鍵復号化サブルーチン９９を信頼できる第三者機関サーバ９が起動する（Ｓ８９）。

【００５１】

その後、信頼できる第三者機関サーバ９が受信コンピュータ３に送るリダイレクトＵＲＬを算出する（Ｓ９１）。以下にリダイレクトＵＲＬの例を示す。

https://www.privatewebmail.com/ViewPPMessage?MessageID=12345&Key=4n9gn9gn94n9ghjy

【００５２】

このＵＲＬのフォーマットを以下に説明する。

www.privatewebmail.com/ViewPPMessage?MessageID=12345　－　ＥＭＳＰサーバ７が提供する、セッション鍵を用いて復号化されるべきＥＭＳＰサーバ７のメッセージキャッシュ５７内のメッセージを特定する返信用ＵＲＬ。

Key=4n9gn9gn94n9ghjy　－　復号化されたセッション鍵。

【００５３】

その後、信頼できる第三者機関サーバ９がリダイレクトＵＲＬを受信コンピュータ３のブラウザに送信し（Ｓ９３）、それからウェブセッションを終了する（Ｓ９５）。

【００５４】

リダイレクトＵＲＬを受信すると、受信コンピュータ３のブラウザは自動的にそのＵＲＬに対する要求をＥＭＳＰサーバ７へ送信する。この要求は復号化されたセッション鍵を含む。

【００５５】

図５に戻って、復号化されたセッション鍵を受信すると、ＥＭＳＰサーバ７はこのセッション鍵を用いてメッセージキャッシュ５７内に記憶されているメッセージ（これは前記ＵＲＬにて特定される）のＤＥＭ部分を復号化する（Ｓ６７）。それから、復号化されたメッセージを受信コンピュータ３に表示するためのウェブページデータをＥＭＳＰサーバ７が送信して（Ｓ６９）、メッセージ表示サブルーチン４７が終了する（Ｓ７１）。

【００５６】

前述の通り、暗号化されたメッセージのＤＥＭ部分は元のメッセージとデジタル署名を記憶している。この実施形態においては、元のメッセージとデジタル署名がＥＭＳＰサーバ７から受信コンピュータ３へ伝達される。元のメッセージの完全性（すなわち、改竄されているかどうか）は、受信コンピュータ３がデジタル署名を用いて従来の方法で確認する。具体的には、送信コンピュータ１がデジタル署名を生成する際に使用したのと同じハッシュ関数を用いて受信コンピュータ３がテストハッシュ値を作り、送信者の公開鍵で受信コンピュータ３がデジタル署名を復号化し参照ハッシュ値を生成する。もしテストハッ

シュ値が参照ハッシュ値と同一ならば、メッセージの完全性は立証される。

【００５７】

上記の通り、ＥＭＳＰサーバ７も受信コンピュータ３もクライアントの秘密鍵にはアクセスしない。従って、たとえ選択されたメッセージのセッション鍵の安全性が危険に曝されたとしても、他の全てのメッセージはクライアントの秘密鍵を知らないと再生できない異なるセッション鍵を使用するから、ＥＭＳＰサーバ７に記憶されたクライアントの他のメッセージは安全である。この方式では、もし受信コンピュータ３がインターネットカフェなどにあっても、電子メールメッセージングサービス提供者のクライアントは暗号化されたメッセージを安全に見ることができる。というのも、その暗号化されたメッセージの情報が漏洩する可能性は、誰でも使用できるコンピュータを用いてそのメッセージが見られてしまうかも知れないといういずれにせよ避けられない危険によるものだけだと知っているからである。

【００５８】

更に、信頼できる第三者機関サーバ９は暗号化されたメッセージのＤＥＭ部分にアクセスしない。従って、信頼できる第三者はクライアントの電子メールメッセージの中身を盗み見ることはできない。

【００５９】

上記の実施形態の利点は、受信コンピュータには従来のブラウザプログラムしか必要でないことである。従って、インターネットカフェなどのコンピュータを何ら改良する必要なしに用いることができる。

【００６０】

上記の実施形態では、送信コンピュータ１はデジタル署名を送信者の秘密鍵を用いて生成する。しかし、送信コンピュータ１が誰でも使用可能であれば（例えばインターネットカフェ内にあるなど）、送信者の秘密鍵情報が漏洩するおそれがある。代わりの実施の形態では、送信コンピュータ１はデジタル署名を生成するために、ハッシュ値を生成するが、そのハッシュ値は送信者の秘密鍵で暗号化するために信頼できる第三者機関サーバへ送信される。１つの実施の形態では、このことは、ある要求を信頼できる第三者機関サーバへ送付することにより行われる。この要求は、ハッシュ値を有するＵＲＬと、この要求に付加された返信用ＵＲＬからなる。ＵＲＬとそこに付加されたハッシュ値を受信した信頼できる第三者機関サーバが実行する処理を、図８を参照して以下に説明する。

【００６１】

ＵＲＬを受信すると、信頼できる第三者機関サーバがウェブセッションを開始し（Ｓ１０１）、受信したＵＲＬ情報を記憶する（Ｓ１０３）。それから、信頼できる第三者機関サーバは、図７を参照して説明した方法と同じ方法でユーザを認証する（Ｓ１０５）。ユーザ認証後、ユーザ識別情報と鍵データベースに記憶されたルート秘密鍵を用いてユーザに関連する秘密鍵を算出する秘密鍵算出サブルーチンを、信頼できる第三者機関サーバが起動する（Ｓ１０７）。その後、信頼できる第三者機関サーバは、算出された秘密鍵を用いて、受信したハッシュ値を暗号化してデジタル署名を生成する（Ｓ１０９）。それから、信頼できる第三者機関サーバは、デジタル署名を返信用ＵＲＬに送信し（Ｓ１１１）、ウェブセッションを終了する（Ｓ１１３）。

【００６２】

上記の実施形態では、元のメッセージは署名されてから暗号化されるが、暗号化してからそのメッセージを署名する実施形態とすることも考えられる。

【００６３】

上記の実施形態では、信頼できる第三者機関サーバは、復号化されたセッション鍵を受信コンピュータ３に送信し、受信コンピュータ３は、メッセージを復号化するＥＭＳＰサーバ７に自動的にそのセッション鍵をリダイレクトする。代わりの実施の形態では、暗号化されたメッセージのＤＥＭ部分がＥＭＳＰサーバ７によって受信コンピュータ３へ転送され、復号化されたセッション鍵で受信コンピュータ３によって復号化される。これはＥＭＳＰサーバ７が復号化されたメッセージにアクセスしないという利点がある。しかし、

受信コンピュータ３が復号化を実行するための追加機能を必要とする不利な点もある。

【００６４】

さらに他の実施の形態では、復号化されたセッション鍵と暗号化されたメッセージのＤＥＭ部分がＥＭＳＰサーバ７または信頼できる第三者機関サーバ９以外のリモートコンピュータに転送されて復号化された後、その復号化されたメッセージが受信コンピュータ３に送信される。

【００６５】

上記の実施形態では、ＥＭＳＰサーバ７が暗号化されたメッセージを検出すると、クライアントに通知され、クライアントがクリックすると復号化が始まるＵＲＬリンクが与えられる。これは、受信コンピュータが復号化されたメッセージを受信するのに十分安全かどうかをクライアントが判断できるという点で有利である。他の実施の形態では、暗号化されたメッセージが検出されたら直ちにクライアントを信頼できる第三者機関サーバ９にリダイレクトするという設定オプションの提供が考えられる。これはクリック数を減らすという点では有利だが、クライアントへの分かりやすさは低下する（is less transparent to the client）。

【００６６】

上記の実施形態では、暗号化されたメッセージを検出すると、暗号化されたメッセージのＫＥＭ部分から、クライアントの秘密鍵で暗号化されたバージョンのセッション鍵だけをＥＭＳＰサーバ７が抽出する。他の実施の形態では、ＥＭＳＰサーバがＫＥＭ部分の全体を受信コンピュータ３に送信し、受信コンピュータ３が信頼できる第三者機関サーバ９へこれを転送する。しかし、もし暗号化されたメッセージが多数の受信者を有するならば、この方法はネットワークトラフィックの著しい増加をもたらす。

【００６７】

上記の実施形態では、信頼できる第三者機関サーバ９はルート公開鍵を記憶しており、クライアント識別情報とルート公開鍵とを用いてクライアントの秘密鍵を算出する。しかし、必要なのは、信頼できる第三者機関サーバ９がクライアントの秘密鍵にアクセスすることだけである。従って、他の実施の形態では、信頼できる第三者機関サーバ９が各クライアントの秘密鍵そのものを記憶してもよいし、別の装置から必要なクライアントの秘密鍵にアクセスしてもよい。

【００６８】

上記の実施形態では、WO03/017559号公報に記載された非対称暗号化アルゴリズムが使用される。このアルゴリズムでは、クライアントの秘密鍵がクライアントの識別情報とルート公開鍵とを用いて算出される。当然の事だが、全体として同じ機能性を有する他のアルゴリズムも使用されうる。例えば"ID based cryptosystems with pairing on elliptic curve" by R. Sakai and M. Kasahara, Cryptology ePrint archive, Report 2003/054に述べられたアルゴリズムおよび"An Efficient ID-KEM Based On the Sakai-Kasahara Key Construction" by Chen et al, Cryptology ePrint archive, Report 2005/224に述べられたアルゴリズムも使用され得る（ここに両刊行物を参照することによりその内容を本明細書の一部とする）。

【００６９】

更に、この非対称暗号化アルゴリズムはクライアント識別情報を用いてクライアントの秘密鍵を算出する必要はなく、任意の非対称暗号化アルゴリズム（例えばＲＳＡアルゴリズム）を用いうる。同様に、前述の実施形態ではＡＥＳ暗号化アルゴリズムをＤＥＭ部分の暗号化に用いていたが、他の対称暗号化アルゴリズム（例えばＤＥＳアルゴリズム）を用いうる。

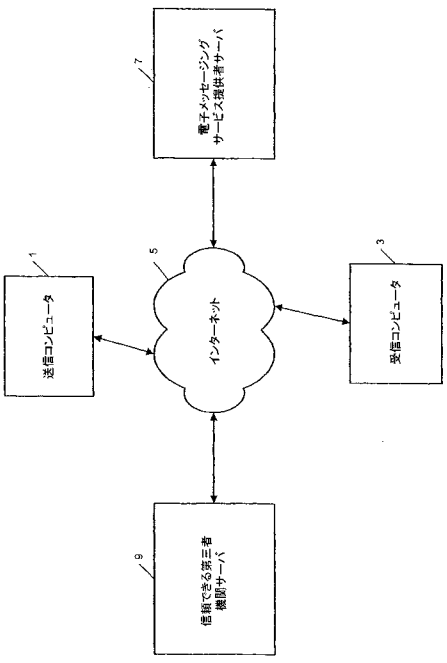
【００７０】

前述の実施形態では、本発明のインターネットを用いた実施を記載しているが、当然の事ながら、インターネットに接続していないコンピュータネットワークにも本発明は使用され得る。例えば、ある組織は本発明を実施した内部ネットワークを有してもよいし、この場合、本発明を使用する者は任意のコンピュータから電子メールメッセージにアクセス

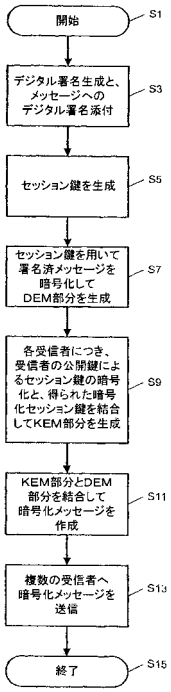
し得る。
【００７１】
上記の実施形態では、ＥＭＳＰサーバ７の各クライアントはユーザ名を有する。クライアントの電子メールアドレスをユーザ名として使用してもよいと理解される。
【００７２】
上記の実施形態では、受信コンピュータ３は標準的なパーソナルコンピュータである。他の種類のコンピュータ、例えばシンクライアントまたは携帯情報端末（ＰＤＡ）を受信コンピュータ３として用いてもよいと理解される。
【００７３】
上記の本発明の実施形態はコンピュータ装置とコンピュータ装置によって実行される処理を有するが、本発明の範囲は、発明を実現するために適合させられたコンピュータプログラム、具体的には搬送体上のもしくは搬送体内のコンピュータプログラムにまで及ぶ。このプログラムは、ソースコード、オブジェクトコード、部分的にコンパイルされた形態のようなソースコードとオブジェクトコードの中間的なコード、または本発明の処理を実施するのに適した他のあらゆる形態であり得る。
【００７４】
この搬送体はプログラムを搬送し得るいかなる実在物（entity）または装置であってもよい。例えばこの搬送体は、ＲＯＭ（例えばＣＤ－ＲＯＭまたは半導体ＲＯＭ）のような記憶媒体、または磁気記録媒体（例えばフロッピー（登録商標）ディスクまたはハードディスク）であってもよい。更にこの担体は、電気的光学的信号を、電気的もしくは光学的なケーブル又は無線もしくはその他の手段によって搬送し得る伝送性の搬送体であってもよい。
【００７５】
このプログラムがケーブル、その他の装置、またはその他の手段によって直接的に搬送され得る信号で具体化されるなら、その搬送体は当該ケーブルまたはその他の装置もしくは手段によって構成されてもよい。また、その搬送体はこのプログラムが組み込まれた集積回路でもよく、この集積回路は関連する処理の実行のために、または関連する処理での使用のために適合化される。
【００７６】
前記の実施形態の全てにおいて本発明はソフトウェアを用いて実現されているが、代わりに本発明をハードウェア装置またはハードウェア装置とソフトウェアの組合せを用いて実現されるとも理解される。
【図面の簡単な説明】
【００７７】
【図１】本発明に係る電子メールメッセージングシステムの主な構成要素を概略的に示している。
【図２】図１に示された電子メールメッセージングシステムの一部を構成する、暗号化メールメッセージを送信する電子メールメッセージ送信機側コンピュータの動作を図式的に示したフローチャートである。
【図３】図１に示された電子メールメッセージングシステムの一部を構成する、電子メールメッセージングサービス提供者のサーバの主な構成要素を概略的に示している。
【図４】図３に示された電子メールメッセージングサービス提供者のサーバの動作を概略的に示したフローチャートである。
【図５】図３に示された電子メールメッセージングサービス提供者のサーバが選択されたメッセージをユーザへ表示する、より詳細な動作を概略的に示したフローチャートである。
【図６】図１に示された電子メールメッセージングシステムの一部を構成する信頼できる第三者機関のサーバの主な構成要素を概略的に示している。
【図７】図６に示された第三者機関のサーバの動作を概略的に示したフローチャートである。

【図８】デジタル署名を生成する、信頼できる第三者機関の他のサーバの動作を概略的に示したフローチャートである。

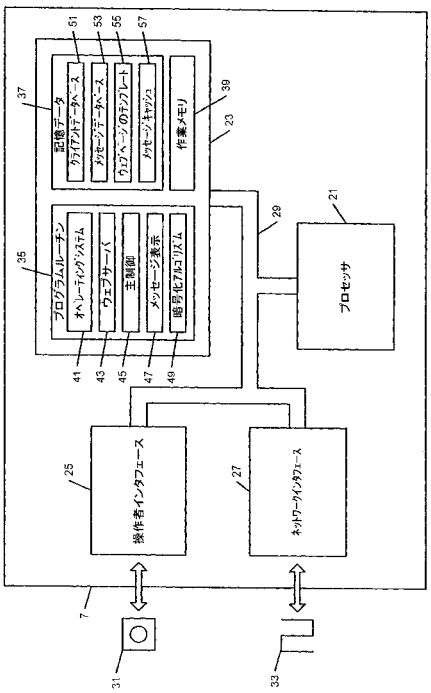
【図１】



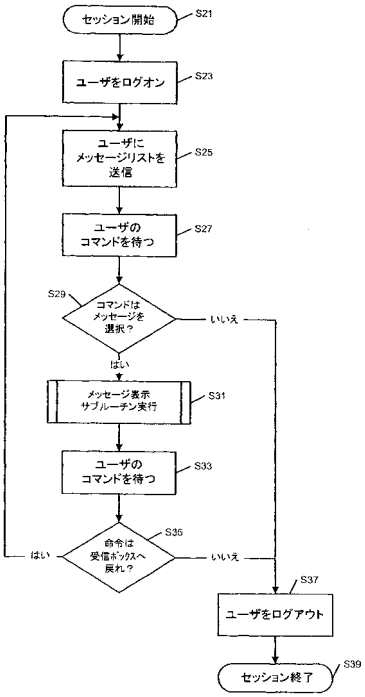
【図２】



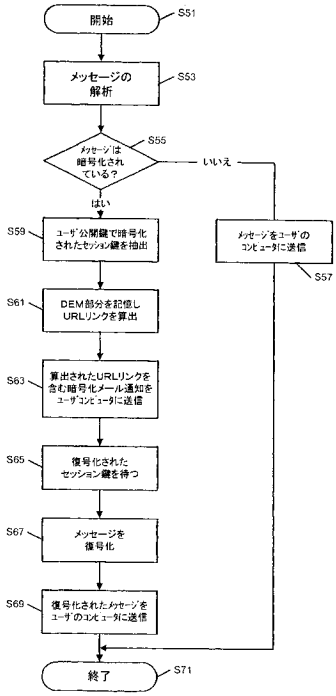
【図３】


記憶データ
クライアントデータベース
メッセージデータベース
ウェブページのテンプレート
メッセージキャッシュ
作業メモリ
プログラムルーチン
オペレーティングシステム
ウェブサーバ
主制御
メッセージ表示
暗号化アルゴリズム
プロセッサ
操作者インタフェース
ネットワークインタフェース

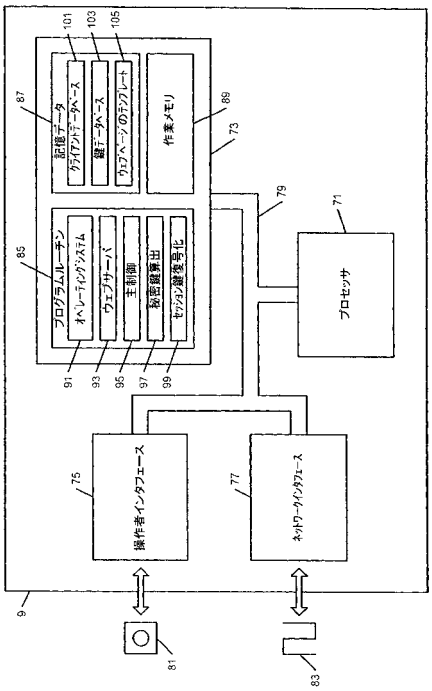
【図４】


セッション開始
ユーザをログオン
ユーザにメッセージリストを送信
ユーザのコマンドを待つ
コマンドはメッセージを選択？
いいえ
はい
メッセージ表示サブルーチン実行
ユーザのコマンドを待つ
命令は受信ボックスへ戻れ？
はい
いいえ
ユーザをログアウト
セッション終了

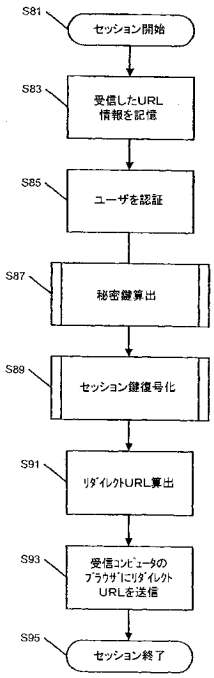
【図５】


開始
メッセージの解析
メッセージは暗号化されている？
いいえ
はい
ユーザ公開鍵で暗号化されたセッション鍵を抽出
DEM部分を記憶しURLリンクを算出
算出されたURLリンクを含む暗号化メール通知をユーザコンピュータに送信
復号化されたセッション鍵を待つ
メッセージを復号化
復号化されたメッセージをユーザのコンピュータに送信
メッセージをユーザのコンピュータに送信
終了

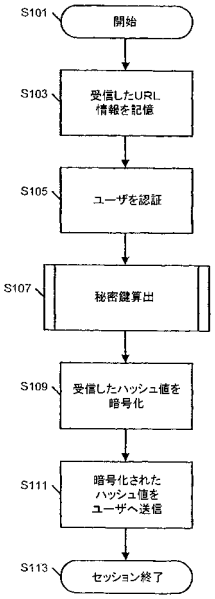
【図６】


記憶データ
クライアントデータベース
鍵データベース
ウェブページのテンプレート
作業メモリ
プログラムルーチン
オペレーティングシステム
ウェブサーバ
主制御
秘密鍵算出
セッション鍵復号化
プロセッサ
操作者インタフェース
ネットワークインタフェース

【図７】


S81
セッション開始
S83
受信したURL情報を記憶
S85
ユーザを認証
S87
秘密鍵算出
S89
セッション鍵復号化
S91
ﾘﾀﾞｲﾚｸﾄURL算出
S93
受信ｺﾝﾋﾟｭｰﾀのﾌﾞﾗｳｻﾞにﾘﾀﾞｲﾚｸﾄURLを送信
S95
セッション終了

【図８】


S101
開始
S103
受信したURL情報を記憶
S105
ユーザを認証
S107
秘密鍵算出
S109
受信したハッシュ値を暗号化
S111
暗号化されたハッシュ値をユーザへ送信
S113
セッション終了

フロントページの続き

(56)参考文献 特開平１１－３０８２１３（ＪＰ，Ａ）
特開２００２－１６３２１２（ＪＰ，Ａ）
特表２００５－５１７３４８（ＪＰ，Ａ）
特表２００５－５３４０４９（ＪＰ，Ａ）
北川 正，ノーツ／ドミノ ６ 徹底解剖，Ｎｏｔｅｓ／Ｄｏｍｉｎｏ Ｍａｇａｚｉｎｅ Ｎｏ．６６，ソフトバンクパブリッシング株式会社，２００２年 4月 1日，ｐ.４０－４１

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L 12/58