(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4665617号
(P4665617)
(45)発行日　平成23年4月6日(2011.4.6)　(24)登録日　平成23年1月21日(2011.1.21)

(51)Int.Cl.　F I
H04L 9/32 (2006.01)　H04L 9/00 675A
G09C 1/00 (2006.01)　G09C 1/00 640D

請求項の数 19　(全 28 頁)

(21)出願番号　特願2005-171200 (P2005-171200)
(22)出願日　平成17年6月10日 (2005.6.10)
(65)公開番号　特開2006-345408 (P2006-345408A)
(43)公開日　平成18年12月21日 (2006.12.21)
審査請求日　平成19年10月9日 (2007.10.9)

(73)特許権者　000000295
沖電気工業株式会社
東京都港区西新橋三丁目１６番１１号
(74)代理人　100095957
弁理士　亀谷　美明
(74)代理人　100096389
弁理士　金本　哲男
(74)代理人　100101557
弁理士　萩原　康司
(72)発明者　八百　健嗣
東京都港区虎ノ門１丁目７番１２号　沖電気工業株式会社内

審査官　西田　聡子

最終頁に続く

(54)【発明の名称】メッセージ認証システム，メッセージ送信装置，メッセージ受信装置，メッセージ送信方法，メッセージ受信方法およびプログラム

(57)【特許請求の範囲】
【請求項１】
メッセージ送信装置と，複数のメッセージ受信装置とを含んで形成され，前記メッセージ送信装置と各メッセージ受信装置とが途中のメッセージ受信装置を介して通信する無線通信により，前記メッセージ送信装置から各メッセージ受信装置にメッセージを送信し，前記メッセージ受信装置がそのメッセージを認証するメッセージ認証システムであって：
前記メッセージ送信装置は，
メッセージに対する電子署名を，暗号鍵を用いて生成する署名生成部と；
前記メッセージを，前記暗号鍵および電子署名に関連付けて保持するメッセージ保持部と；
前記電子署名をメッセージ受信装置に送信し，かつ，所定の遅延を経て前記メッセージと該メッセージに関連付けられた暗号鍵とを送信するメッセージ送信部と；
を備え，
前記メッセージ受信装置は，
前記メッセージ送信装置から送信された電子署名，および，所定の遅延を経て送信されたメッセージと暗号鍵とを受信するメッセージ受信部と；
前記電子署名を保持する署名保持部と；
前記メッセージに対して前記暗号鍵を用いて生成した電子署名と，前記署名保持部の電子署名とを比較して該メッセージを認証するメッセージ認証部と；
を備えることを特徴とする，メッセージ認証システム。

【請求項２】
複数のメッセージ受信装置に対して無線通信によりメッセージを送信するメッセージ送信装置であって：
メッセージに対する電子署名を，暗号鍵を用いて生成する署名生成部と；
前記メッセージを，前記暗号鍵および電子署名に関連付けて保持するメッセージ保持部と；
前記電子署名をメッセージ受信装置に送信し，かつ，所定の遅延を経て前記メッセージと該メッセージに関連付けられた暗号鍵とを送信するメッセージ送信部と；
を備えることを特徴とする，メッセージ送信装置。
【請求項３】
前記メッセージ受信装置が前記電子署名を正しく受信したことを知らせる受信確認情報を，前記メッセージ受信装置から受信し，前記メッセージに関連付けられた電子署名が前記メッセージ受信装置に到達したかどうかを判断し，到達していれば，前記メッセージと該メッセージに関連付けられた暗号鍵とをメッセージ送信部に送信させる到達確認部をさらに備えることを特徴とする，請求項２のメッセージ送信装置。
【請求項４】
前記署名生成部が生成した電子署名の数に応じて，順次，複数の暗号鍵からなる暗号鍵列から暗号鍵を抽出し，前記署名生成部における暗号鍵を更新する暗号鍵生成部をさらに備えることを特徴とする，請求項３に記載のメッセージ送信装置。
【請求項５】
前記署名生成部は，所定数のメッセージに対する所定数の電子署名を，１つの暗号鍵を用いて生成し，
前記メッセージ送信部は，前記所定数のメッセージと該所定数のメッセージに共通な暗号鍵とを送信することを特徴とする，請求項４に記載のメッセージ送信装置。
【請求項６】
各メッセージ受信装置との時刻同期をとった後，前記電子署名に対するメッセージの送信遅延時間と，暗号鍵の更新時に対する暗号鍵の送信遅延時間とを管理し，該送信遅延時間に応じて，前記メッセージと該メッセージに関連付けられた暗号鍵とをメッセージ送信部に送信させる時刻同期制御部をさらに備えることを特徴とする，請求項２に記載のメッセージ送信装置。
【請求項７】
予め設定された時間に応じて，順次，複数の暗号鍵からなる暗号鍵列から暗号鍵を抽出し，前記署名生成部における暗号鍵を更新する暗号鍵生成部をさらに備えることを特徴とする，請求項６に記載のメッセージ送信装置。
【請求項８】
前記署名生成部は，前記予め設定された時間内のメッセージに対する全ての電子署名を，１つの暗号鍵を用いて生成し，
前記メッセージ送信部は，前記時間内のメッセージと該時間内のメッセージに共通な暗号鍵とを送信することを特徴とする，請求項７に記載のメッセージ送信装置。
【請求項９】
前記暗号鍵列の各暗号鍵は，予め設定された原暗号鍵からの一方向性関数により順次生成されたものであり，
前記暗号鍵生成部は，前記生成順の逆に暗号鍵を抽出することを特徴とする，請求項４または７のいずれかに記載のメッセージ送信装置。
【請求項１０】
署名生成部と，メッセージ保持部と，メッセージ送信部と，を備えるメッセージ送信装置が，複数のメッセージ受信装置に対して無線通信によりメッセージを送信するメッセージ送信方法であって：
前記署名生成部が，メッセージに対する電子署名を，暗号鍵を用いて生成する署名生成ステップと；

前記メッセージ保持部が，前記メッセージを，前記暗号鍵および電子署名に関連付けて保持するメッセージ保持ステップと；
前記メッセージ送信部が，前記電子署名をメッセージ受信装置に送信する署名送信ステップと；
前記メッセージ送信部が，所定の遅延を経て前記メッセージと該メッセージに関連付けられた暗号鍵とを送信するメッセージ送信ステップと；
を含むことを特徴とする，メッセージ送信方法。
【請求項１１】
署名生成部と，メッセージ保持部と，メッセージ送信部と，を備え，複数のメッセージ受信装置に対して無線通信によりメッセージを送信するメッセージ送信装置の機能をコンピュータに実現させるためのプログラムであって：
コンピュータに，
メッセージに対する電子署名を，暗号鍵を用いて生成する署名生成部の機能と；
前記メッセージを，前記暗号鍵および電子署名に関連付けて保持するメッセージ保持部の機能と；
前記電子署名をメッセージ受信装置に送信し，かつ，所定の遅延を経て前記メッセージと該メッセージに関連付けられた暗号鍵とを送信するメッセージ送信部の機能と；
を実現させるためのプログラム。
【請求項１２】
メッセージ送信装置からのメッセージを，無線通信により受信するメッセージ受信装置であって：
前記メッセージ送信装置から送信された電子署名，および，所定の遅延を経て送信されたメッセージと暗号鍵とを受信するメッセージ受信部と；
前記電子署名を保持する署名保持部と；
前記メッセージに対して前記暗号鍵を用いて生成した電子署名と，前記署名保持部の電子署名とを比較して該メッセージを認証するメッセージ認証部と；
を備えることを特徴とする，メッセージ受信装置。
【請求項１３】
前記メッセージ送信装置から電子署名を受信した後，該電子署名を正しく受信したことを知らせる受信確認情報を前記メッセージ送信装置に送信する受信確認送信部をさらに備えることを特徴とする，請求項１２に記載のメッセージ受信装置。
【請求項１４】
前記暗号鍵が，予め設定された，電子署名もしくはメッセージの数毎に更新されていることを検証し，不整合の場合，該暗号鍵をメッセージ送信装置が送信したことを認証しない暗号鍵検証部をさらに備えることを特徴とする，請求項１３に記載のメッセージ受信装置。
【請求項１５】
前記メッセージ送信装置との時刻同期がとられた後，設定された，前記電子署名に対するメッセージの送信遅延時間と，前記暗号鍵の更新時に対する暗号鍵の送信遅延時間に応じて，前記メッセージおよび暗号鍵を受信しているか検証し，受信した時刻が所定範囲を超えて相違する場合，該メッセージを認証しない時刻同期検証部をさらに備えることを特徴とする，請求項１２に記載のメッセージ受信装置。
【請求項１６】
前記暗号鍵が，予め設定された時間毎に更新されていることを検証し，不整合の場合，該暗号鍵をメッセージ送信装置が送信したことを認証しない暗号鍵検証部をさらに備えることを特徴とする，請求項１５に記載のメッセージ受信装置。
【請求項１７】
前記暗号鍵検証部は，さらに，前記暗号鍵を保持し，暗号鍵が更新された場合，更新された暗号鍵から一方向性関数を任意の回数施し，その計算結果と，保持された以前の暗号鍵の値とを比較し，一致しない場合，該暗号鍵をメッセージ送信装置が送信したことを認

証しないことを特徴とする，請求項１４または１６のいずれかに記載のメッセージ受信装置。

【請求項１８】

メッセージ受信部と，署名保持部と，メッセージ認証部と，を備えるメッセージ受信装置が，メッセージ送信装置からのメッセージを，無線通信により受信するメッセージ受信方法であって：

前記メッセージ受信部が，前記メッセージ送信装置から送信された電子署名を受信する署名受信ステップと；

前記署名保持部が，前記電子署名を保持する署名保持ステップと；

前記メッセージ受信部が，前記署名受信ステップから所定の遅延を経てメッセージと暗号鍵とを受信するメッセージ受信ステップと；

前記メッセージ認証部が，前記メッセージに対して前記暗号鍵を用いて生成した電子署名と，前記署名保持部の電子署名とを比較して該メッセージを認証するメッセージ認証ステップと；

を含むことを特徴とする，メッセージ受信方法。

【請求項１９】

メッセージ受信部と，署名保持部と，メッセージ認証部と，を備え，メッセージ送信装置からのメッセージを，無線通信により受信するメッセージ受信装置の機能をコンピュータに実現させるためのプログラムであって：

コンピュータに，

前記メッセージ送信装置から送信された電子署名，および，所定の遅延を経て送信されたメッセージと暗号鍵とを受信するメッセージ受信部の機能と；

前記電子署名を保持する署名保持部の機能と；

前記メッセージに対して前記暗号鍵を用いて生成した電子署名と，前記署名保持部の電子署名とを比較して該メッセージを認証するメッセージ認証部の機能と；

を実現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，メッセージを認証するシステムに関し，特に，システムを管理・制御する例えばサーバといったメッセージ送信装置と，低コストの例えば，センサノードといったメッセージ受信装置とからなるセンサネットワークシステムにおいて，メッセージ送信装置がメッセージ受信装置にメッセージをブロードキャストし，メッセージ受信装置がそのメッセージを認証する，メッセージ認証システム，メッセージ送信装置，メッセージ受信装置，メッセージ送信方法，メッセージ受信方法およびプログラムに関する。

【背景技術】

【０００２】

例えばサーバと，サーバの周囲に配置される複数のノードとが，途中に配置されたノードを介して通信するマルチホップ通信により，サーバが各ノード，例えば計測機能を備えたセンサノードを制御するセンサネットワークシステムが実施されている。

【０００３】

かかるセンサネットワークシステムでは，各ノードに対して低コスト化が要求され，高い処理能力を有するＣＰＵ等を搭載することが難しい状況にある。このような低コスト化の下では，公開鍵暗号を利用した暗号化技術は処理負担の大きさから採用することができず，処理負担の少ない共通鍵暗号が利用される。例えば，サーバと全ノードに対して，全デバイスに共通する共通鍵を保持させ，サーバからのメッセージをその共通鍵によって認証する。

【０００４】

しかし，かかる状況下において，上記ノードが耐タンパの機能を有しているとは限らず，ノードに設けられた共通鍵が上記各ノード以外の他の電子機器に漏洩する可能性がある

。従って，各ノードでメッセージが認証されたとしても，そのメッセージが不正な利用者からの不正メッセージということもあり得る。また，マルチホップ通信におけるノードの中継途中で，不正なルータノードにより改竄されている可能性もないとは言えない。

【０００５】

かかる問題に対して，サーバからのブロードキャストメッセージを認証するときに，サーバとノード間で時間軸を合わせ，暗号鍵の送信を所定時間遅延させ，不正な利用者のサーバのなりすましを防止する技術が知られている（例えば，特許文献１）。

【０００６】

しかし，かかる技術では，暗号鍵がノードに到達（公開）するまで，送信された全てのメッセージを保持しておく必要があり，そのメッセージの記憶に費やすコストがノードの低価格化の障害になっている。

【０００７】

【非特許文献１】「ワイヤード／ワイヤレスネットワークにおけるブロードキャスト通信のセキュリティ」Ａｄｒｉａｎ　Ｐｅｒｒｉｇ，Ｊ．Ｄ．　Ｔｙｇｅｒ　著，溝口文雄監訳，共立出版　ｐｐ．１７２－１７７

【発明の開示】

【発明が解決しようとする課題】

【０００８】

本発明は，従来のメッセージ認証システムが有する上記問題点に鑑みてなされたものであり，本発明の目的は，暗号鍵が公開されるまでに上記ノードに対応するメッセージ受信装置にメッセージが保持されず，メッセージのメモリ占有率を最小化することが可能な，新規かつ改良されたメッセージ認証システム，メッセージ送信装置，メッセージ受信装置，メッセージ送信方法，メッセージ受信方法およびプログラムを提供することである。

【課題を解決するための手段】

【０００９】

上記課題を解決するために，本発明のある観点によれば，メッセージ送信装置と，複数のメッセージ受信装置とを含んで形成され，上記メッセージ送信装置と各メッセージ受信装置とが途中のメッセージ受信装置を介して通信する無線通信により，上記メッセージ送信装置から各メッセージ受信装置にメッセージを送信し，上記メッセージ受信装置がそのメッセージを認証するメッセージ認証システムであって：上記メッセージ送信装置は，メッセージに対する電子署名を，暗号鍵を用いて生成する署名生成部と；上記メッセージを，上記暗号鍵および電子署名に関連付けて保持するメッセージ保持部と；上記電子署名をメッセージ受信装置に送信し，かつ，所定の遅延を経て上記メッセージと該メッセージに関連付けられた暗号鍵とを送信するメッセージ送信部と；を備え，上記メッセージ受信装置は，上記メッセージ送信装置から送信された電子署名，および，所定の遅延を経て送信されたメッセージと暗号鍵とを受信するメッセージ受信部と；上記電子署名を保持する署名保持部と；上記メッセージに対して上記暗号鍵を用いて生成した電子署名と，上記署名保持部の電子署名とを比較して該メッセージを認証するメッセージ認証部と；を備えることを特徴とする，メッセージ認証システムが提供される。

【００１０】

上記無線通信は，メッセージ送信装置やメッセージ受信装置等の端末同士が直接通信するシングルホップ通信の場合や，他の端末を経由することでより広い範囲の端末間通信を可能にするマルチホップ通信を含んで構成される。

【００１１】

また，暗号鍵を用いて生成するとは，メッセージに対するＭＡＣ（Ｍｅｓｓａｇｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｃｏｄｅ）を生成することを想定する。ＭＡＣとは，例えば，ＨＭＡＣ（Ｋｅｙｅｄ－Ｈａｓｈｉｎｇ　ｆｏｒ　Ｍｅｓｓａｇｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｃｏｄｅ）のように，暗号鍵とメッセージに規定の処理を施した入力データに対してハッシュ関数を施して生成したビット列や，ＣＢＣ－ＭＡＣ（Ｃｉｐｈｅｒ　Ｂｌｏｃｋ　Ｃｈａｉｎｉｎｇ－Ｍｅｓｓａｇｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｃ

ｏｄｅ）のように，メッセージを複数のブロックに分割して，各ブロックに対して暗号化と重畳を繰り返すことで生成したビット列であり，これらのデータサイズは，メッセージのデータサイズよりも小さくなるのが一般的である。

【００１２】

かかる構成により，暗号鍵が公開されるまでにメッセージ受信装置にメッセージが保持されず，メッセージのメモリ占有率を最小化することが可能となる。このように，メッセージをメッセージ受信装置に送信し，所定の遅延を経て暗号鍵を公開する方法における，複数のメッセージがメッセージ受信装置のメモリを占有してしまい，メッセージを受け付けることができない，もしくは，十分な容量のメモリを確保するためコストが高くなるといった課題を，本発明は解決している。

【００１３】

上記課題を解決するために，本発明の別の観点によれば，複数のメッセージ受信装置に対してマルチホップ通信によりメッセージを送信するメッセージ送信装置であって：メッセージに対する電子署名を，暗号鍵を用いて生成する署名生成部と；上記メッセージを，上記暗号鍵および電子署名に関連付けて保持するメッセージ保持部と；上記電子署名をメッセージ受信装置に送信し，かつ，所定の遅延を経て上記メッセージと該メッセージに関連付けられた暗号鍵とを送信するメッセージ送信部と；を備えることを特徴とする，メッセージ送信装置が提供される。

【００１４】

かかる構成により，メッセージ送信予告として先に電子署名が送信され，所定の遅延を経て，本体であるメッセージ，および，電子署名との確認に利用される暗号鍵が送信される。従って，暗号鍵が公開されるまでにメッセージ受信装置にメッセージが保持されず，メッセージのメモリ占有率を最小化することが可能となる。

【００１５】

かかるメッセージ送信装置は，メッセージ受信装置との関係で不正な利用者によるメッセージ送信装置のなりすましを防止するため，２つの方式がとられる。これは，（１）各メッセージ受信装置の受信状況を確認して，その回数に応じて暗号鍵を送信，更新する回数同期方式と，（２）各メッセージ受信装置と時間軸で同期させ，送受信タイミングでメッセージの有効性を検証する時刻同期方式である。

【００１６】

（１）回数同期方式によるメッセージ送信装置として，上記メッセージ受信装置が上記電子署名を正しく受信したことを知らせる受信確認情報を，上記メッセージ受信装置から受信し，上記メッセージに関連付けられた電子署名が上記メッセージ受信装置に到達したかどうかを判断し，到達していれば，上記メッセージと該メッセージに関連付けられた暗号鍵とをメッセージ送信部に送信させる到達確認部をさらに備えるとしても良い。

【００１７】

かかる構成により，各メッセージ受信装置が，メッセージ送信予告としての電子署名を受け取ったことを確認して，メッセージおよび暗号鍵を送信することができる。この暗号鍵は，電子署名を送信する時点において公開されておらず，メッセージ送信装置になりすまして不正なメッセージを送信したとしても，先に送信されている電子署名との整合がとれない。

【００１８】

上記署名生成部が生成した電子署名の数に応じて，順次，複数の暗号鍵からなる暗号鍵列から暗号鍵を抽出し，上記署名生成部における暗号鍵を更新する暗号鍵生成部をさらに備えるとしても良い。

【００１９】

かかる構成により，メッセージ毎もしくは所定数のメッセージ毎に暗号鍵が更新され，そのうちの１つの鍵が漏洩したとしても連続的な不正を防止できる。また，各メッセージ受信装置と暗号鍵の変更タイミング，例えば，電子署名の数を共通情報とすることで，不正な中継メッセージ受信装置によるメッセージの脱落も検出可能となる。

【００２０】
また，上記暗号鍵列の各暗号鍵は，予め設定された原暗号鍵からの一方向性関数により順次生成されたものであり，上記暗号鍵生成部は，上記生成順の逆に暗号鍵を抽出するとしても良い。
【００２１】
上記暗号鍵列は，一方向には一意に導き出せるが逆方向には導き出せない，例えば，ＭＤ５（Ｍｅｓｓａｇｅ Ｄｉｇｅｓｔ ５）やＳＨＡ－１（Ｓｅｃｕｒｅ Ｈａｓｈ Ａｌｇｏｒｉｔｈｍ １）等のハッシュ関数といった一方向性関数で生成され，かつ，逆方向に並べ換えられて公開されるため，既に公開になっている暗号鍵からは，現在メッセージに利用される未公開の暗号鍵を導き出すことはできず，メッセージ送信装置以外のメッセージ受信装置においてさえメッセージに対する正規の電子署名を生成することはできない。また，メッセージ受信装置におけるメッセージ認証の際にはかかる現在の暗号鍵も公開され，この暗号鍵から一方向性関数により前回の暗号鍵を導き出すことができ，暗号鍵自体の整合性をとることができる。
【００２２】
上記署名生成部は，所定数のメッセージに対する所定数の電子署名を，１つの暗号鍵を用いて生成し，上記メッセージ送信部は，上記所定数のメッセージと該所定数のメッセージに共通な暗号鍵とを送信するとしても良い。
【００２３】
上記暗号鍵の更新を所定数のメッセージ毎に行う場合，その所定数のメッセージに対して暗号鍵は１つであり，送信する暗号鍵は，所定数のメッセージに対して１つあれば足りる。
【００２４】
（２）時刻同期方式によるメッセージ送信装置として，各メッセージ受信装置との時刻同期をとった後，上記電子署名に対するメッセージの送信遅延時間と，暗号鍵の更新時に対する暗号鍵の送信遅延時間とを管理し，該送信遅延時間に応じて，上記メッセージと該メッセージに関連付けられた暗号鍵とをメッセージ送信部に送信させる時刻同期制御部をさらに備えるとしても良い。
【００２５】
かかる構成により，各メッセージ受信装置と時刻同期を行うことができ，メッセージや暗号鍵の送受信時間を合わせることが可能となる。従って，不正なメッセージ受信装置や他の電子機器でメッセージの改竄を行ったとしても上記時刻同期からの時間偏差によってそのメッセージを検出できる。
【００２６】
予め設定された時間に応じて，順次，複数の暗号鍵からなる暗号鍵列から暗号鍵を抽出し，上記署名生成部における暗号鍵を更新する暗号鍵生成部をさらに備えるとしても良い。
【００２７】
かかる構成により，予め設定された時間間隔で暗号鍵が更新され，そのうちの１つの鍵が漏洩したとしても連続的な不正を防止できる。また，各メッセージ受信装置と暗号鍵の変更タイミングが同期されているので，不正な中継メッセージ受信装置によるメッセージの脱落も検出可能となる。
【００２８】
上記暗号鍵列の各暗号鍵は，予め設定された原暗号鍵からの一方向性関数により順次生成されたものであり，上記暗号鍵生成部は，上記生成順の逆に暗号鍵を抽出するとしても良い。
【００２９】
既に公開になっている暗号鍵からは，現在メッセージに利用される未公開の暗号鍵を導き出すことはできず，メッセージ送信装置以外のメッセージ受信装置においてさえメッセージに対する正規の電子署名を生成することはできない。また，メッセージ受信装置にお

けるメッセージ認証の際にはかかる現在の暗号鍵も公開され，この暗号鍵から一方向性関数により前回の暗号鍵を導き出すことができ，暗号鍵自体の整合性をとることができる。

【００３０】

上記署名生成部は，上記予め設定された時間内のメッセージに対する全ての電子署名を，１つの暗号鍵を用いて生成し，上記メッセージ送信部は，上記時間内のメッセージと該時間内のメッセージに共通な暗号鍵とを送信するとしても良い。

【００３１】

上記暗号鍵の更新を所定時間毎に行う場合，その所定時間内のメッセージに対して暗号鍵は１つであり，送信する暗号鍵は，所定時間内のメッセージに対して１つあれば足りる。

【００３２】

また，上記メッセージ送信装置を利用して，複数のメッセージ受信装置に対してマルチホップ通信によりメッセージを送信するメッセージ送信方法も提供され，コンピュータを上記メッセージ送信装置として機能させるプログラムも提供される。

【００３３】

上記課題を解決するために，本発明の別の観点によれば，メッセージ送信装置からのメッセージを，マルチホップ通信により受信するメッセージ受信装置であって：上記メッセージ送信装置から送信された電子署名，および，所定の遅延を経て送信されたメッセージと暗号鍵とを受信するメッセージ受信部と；上記電子署名を保持する署名保持部と；上記メッセージに対して上記暗号鍵を用いて生成した電子署名と，上記署名保持部の電子署名とを比較して該メッセージを認証するメッセージ認証部と；を備えることを特徴とする，メッセージ受信装置が提供される。

【００３４】

上述したように当該メッセージ受信装置は，メッセージ受信装置との関係で不正な利用者によるメッセージ送信装置のなりすましを防止するため，（１）回数同期方式と，（２）時刻同期方式の方式を有する。

【００３５】

（１）回数同期方式によるメッセージ受信装置として，上記メッセージ送信装置から電子署名を受信した後，該電子署名を正しく受信したことを知らせる受信確認情報を上記メッセージ送信装置に送信する受信確認送信部をさらに備えるとしても良い。

【００３６】

かかる構成により，メッセージ送信予告としての電子署名を受け取ったことをメッセージ送信装置に返信することができ，その受信確認情報をもってして暗号鍵を受信することができる。この暗号鍵は，電子署名を送信する時点において公開されておらず，メッセージ送信装置になりすまして不正なメッセージが送信されたとしても，先に送信されている電子署名との整合がとれないこととなる。

【００３７】

上記暗号鍵が，予め設定された，電子署名もしくはメッセージの数毎に更新されていることを検証し，不整合の場合，該暗号鍵をメッセージ送信装置が送信したことを認証しない暗号鍵検証部をさらに備えるとしても良い。また，上記暗号鍵検証部は，さらに，上記暗号鍵を保持し，暗号鍵が更新された場合，更新された暗号鍵から一方向性関数を任意の回数施し，その計算結果と，保持された以前の暗号鍵の値とを比較し，一致しない場合，該暗号鍵をメッセージ送信装置が送信したことを認証しないとしても良い。

【００３８】

（２）時刻同期方式によるメッセージ受信装置として，上記メッセージ送信装置との時刻同期がとられた後，設定された，上記電子署名に対するメッセージの送信遅延時間と，上記暗号鍵の更新時に対する暗号鍵の送信遅延時間に応じて，上記メッセージおよび暗号鍵を受信しているか検証し，受信した時刻が所定範囲を超えて相違する場合，該メッセージを認証しない時刻同期検証部をさらに備えるとしても良い。

【００３９】

かかる構成により，メッセージ送信装置と時刻同期を行うことができ，メッセージや暗号鍵の送受信時間を合わせることが可能となる。従って，不正なメッセージ受信装置や他の電子機器でメッセージの改竄を行ったとしても上記時刻同期からの時間偏差によってそのメッセージを検出できる。

【００４０】

上記暗号鍵が，予め設定された時間毎に更新されていることを検証し，不整合の場合，該暗号鍵をメッセージ送信装置が送信したことを認証しない暗号鍵検証部をさらに備えるとしても良い。また，上記暗号鍵検証部は，さらに，上記暗号鍵を保持し，暗号鍵が更新された場合，更新された暗号鍵から一方向性関数を任意の回数施し，その計算結果と，保持された以前の暗号鍵の値とを比較し，一致しない場合，該暗号鍵をメッセージ送信装置が送信したことを認証しないとしても良い。

【００４１】

また，上記メッセージ受信装置を利用して，メッセージ送信装置からのメッセージを，マルチホップ通信により受信するメッセージ受信方法も提供され，コンピュータを上記メッセージ受信装置として機能させるプログラムも提供される。

【００４２】

上述したメッセージ認証システムにおいてメッセージと暗号鍵は同時に送信されるとしても良く，さらに，次のメッセージの電子署名と同時に送信されるとしても良い。

【００４３】

また，上記メッセージ送信装置は，例えば，サーバとして機能し，メッセージ受信装置に対して，最低限メッセージを無線で配信することができるとしても良い。また，メッセージ受信部は，例えば，無線のよるメッセージを受信可能なノードとして構成可能であり，計測機能を備えたセンサノードとしても構築できる。従って，上記メッセージ受信装置は，安価なＣＰＵを備えるとしても良い。また，メッセージ送信装置やメッセージ受信装置は，パーソナルコンピュータ，ＰＤＡ（Ｐｅｒｓｏｎａｌ　Ｄｉｇｉｔａｌ　Ａｓｓｉｓｔａｎｔ），携帯電話，携帯型音声プレーヤ，家庭ゲーム機，情報家電等により実現することも可能である。

【００４４】

上記メッセージ認証システムは，複数の装置の集合体で表されるが，各構成要素，機能モジュールがどの装置に属するかを限定しないとしても良く，また，それ自体が単体で存在するとしても良い。また，かかるメッセージ送信装置とメッセージ受信装置は，１つの装置で構成することもできる。

【発明の効果】

【００４５】

以上説明したように本発明によれば，暗号鍵が公開されるまでメッセージ受信装置にメッセージが保持されないので，メッセージのメモリ占有率を最小化することが可能となる。また，中継メッセージ受信装置や他の電子機器による，メッセージの改竄，メッセージの中断，またはメッセージ送信装置のなりすましも防止される。

【発明を実施するための最良の形態】

【００４６】

以下に添付図面を参照しながら，本発明の好適な実施の形態について詳細に説明する。なお，本明細書及び図面において，実質的に同一の機能構成を有する構成要素については，同一の符号を付することにより重複説明を省略する。

【００４７】

図１は，本実施形態で利用できるマルチホップ通信を説明するための概略図である。かかるマルチホップ通信は，メッセージ送信装置１００と，メッセージ送信装置１００の周囲１１０に配置される複数のメッセージ受信装置１２０とによって形成される。マルチホップ通信では，メッセージ送信装置１００からメッセージがブロードキャストされた場合，途中に配置されたメッセージ受信装置１２０を介してさらに遠くのメッセージ受信装置１２０にもメッセージが伝達される。

【００４８】
また，各メッセージ受信装置１２０は，例えば，計測機能を備えた低コストのセンサノードで構成することができる。このようなセンサノードは，通常，複数設置され，更新作業の度に回収するのは困難である。従って，メッセージ送信装置１００が送信したデータをメッセージ受信装置１２０が自動的に更新する環境を作る必要がある。しかし，かかる更新データは，当該メッセージ認証システムにおいて非常に重要な情報なので，安全対策にも気を使わなければならない。本実施形態のメッセージ受信装置１２０は，低コストでありながら，メッセージ送信装置１００からのメッセージを確実に認証し，また，他の電子機器のメッセージ送信装置なりすまし等を回避することができる。
【００４９】
また，メッセージ送信装置１００やメッセージ受信装置１２０は，パーソナルコンピュータ，ＰＤＡ（Ｐｅｒｓｏｎａｌ　Ｄｉｇｉｔａｌ　Ａｓｓｉｓｔａｎｔ），携帯電話，携帯型音声プレーヤ，家庭ゲーム機，情報家電を含んで構成するとしても良く，両者の機能を一体形成することも可能である。従って，一体形成されたメッセージ送信装置１００およびメッセージ受信装置１２０は，他のメッセージ送信装置１００から送信されたメッセージをメッセージ受信装置１２０として受信し，かつ，メッセージ送信装置１００として他のメッセージ受信装置１２０に送信する，即ち，メッセージを中継することもできる。
【００５０】
本実施形態によると，メッセージ受信装置との関係で不正な利用者によるメッセージ送信装置のなりすましを防止するため，２つの方式がとられる。これは，（１）各メッセージ受信装置の受信状況を確認して，その回数に応じて暗号鍵を送信，更新する回数同期方式と，（２）各メッセージ受信装置と時間軸で同期させ，送受信タイミングでメッセージの有効性を検証する時刻同期方式である。以下では，かかる方式を実施形態に分けて説明する。
【００５１】
（第１の実施形態：回数同期方式によるメッセージ認証システム）
図２は，回数同期方式によるメッセージ認証システムを説明するためのフローチャートである。ここでは，メッセージ送信装置１００から２つのメッセージ受信装置１２０ａ，１２０ｂを介して末端のメッセージ受信装置１２０ｃにメッセージを伝達する流れを説明している。
【００５２】
メッセージ送信装置１００において，送信すべきメッセージに対する電子署名を暗号鍵を用いて生成した後，そのメッセージと電子署名とをブロードキャストする。かかるメッセージと電子署名は，メッセージ受信装置１２０ａ，１２０ｂを経由して（Ｓ１５０，Ｓ１５２），メッセージ受信装置１２０ｃに到達する（Ｓ１５４）。メッセージ受信装置１２０ｃは，受信したメッセージと電子署名とを保存し，メッセージが到達したことを証明する受信確認情報をメッセージ送信装置１００に返信する（Ｓ１６０，Ｓ１６２，Ｓ１６４）。
【００５３】
メッセージ送信装置１００は，受信確認情報によりメッセージ受信装置１２０ｃにメッセージが到達したことを確認し，送信完了のメッセージとしてカウントする（Ｓ１６６）。続いて，メッセージ送信装置１００は，他のメッセージと電子署名とを送信し（Ｓ１７０，Ｓ１７２，Ｓ１７４），メッセージ受信装置１２０ｃは，上述したのと同様の返信を行う（Ｓ１７６，Ｓ１８０，Ｓ１８２，Ｓ１８４）。
【００５４】
次に，メッセージ送信装置１００は，送信したメッセージおよびカウントした受信確認情報が所定数（ここでは２つ）になったことを受けて（Ｓ１８６），送信完了したメッセージの電子署名を生成するときに利用した暗号鍵をメッセージ受信装置１２０ｃに送信する（Ｓ１９０，Ｓ１９２，Ｓ１９４）。メッセージ受信装置１２０ｃは，かかる暗号鍵を

利用して，既に受信完了し保存しているメッセージを暗号化し，その結果と既に受信している電子署名とを比較することによってメッセージを認証する。

【００５５】

ここでは，理解を容易にするため，メッセージ送信装置１００からメッセージ受信装置１２０ｃへのメッセージ送信のみを説明したが，勿論かかる場合に限られず，例えば，メッセージ送信装置１００とメッセージ受信装置１２０ａ間や，メッセージ送信装置１００とメッセージ受信装置１２０ｂ間においても同様の処理が行われる。このような処理の詳細は，本件出願人による特願２００４－３２４０９４号を参照することで理解される。

【００５６】

上記のようデータの流れにより，メッセージ送信装置１００は，各メッセージ受信装置１２０がメッセージと電子署名を受け取ったことを確認して暗号鍵を送信することができる。この暗号鍵は，メッセージおよび電子署名を送信する時点において公開されておらず，不正な利用者が，メッセージ送信装置になりすまして不正なメッセージを送信したとしても，先に送信されている電子署名との整合がとれないので安全にメッセージが送信される。

【００５７】

しかし，かかるメッセージ認証システムでは，暗号鍵がメッセージ受信装置に到達（公開）するまで，メッセージ送信装置から送信された全てのメッセージをメッセージ受信装置が保持しておく必要があり，そのメッセージの記憶に費やすコストがメッセージ受信装置の低価格化の障害になっている。

【００５８】

本実施形態においては，かかるメッセージの送信を暗号鍵の送信タイミングに合わせることにより，暗号鍵が公開されるまでにメッセージ受信装置にメッセージが保持されず，メッセージのメモリ占有率を最小化することが可能となる。

【００５９】

（メッセージ送信装置１００）

図３は，第１の実施形態におけるメッセージ送信装置１００の概略的な構成を示したブロック図である。かかるメッセージ送信装置１００は，メッセージ生成部２００と，暗号鍵生成部２０２と，署名生成部２０４と，メッセージ保持部２０６と，メッセージ送信部２０８と，到達確認部２１０とを含んで構成される。上記メッセージ送信装置１００は，メッセージ送信予告として先に電子署名を送信し，所定の遅延を経て，ここでは，上記送信予告としての電子署名がメッセージ受信装置に受信されたことを確認して，本体であるメッセージ，および，電子署名との確認に利用される暗号鍵を送信する。

【００６０】

上記メッセージ生成部２００は，メッセージ送信装置１００から各メッセージ受信装置１２０にブロードキャストすべきメッセージを生成する。上記メッセージは，ユーザインターフェースからの入力により生成されても良いし，既存の文書をそのまま利用して生成されるとしても良い。また，メッセージ自体を暗号化するとしても良い。メッセージ生成部２００は，生成されたメッセージを署名生成部２０４に転送する。

【００６１】

上記暗号鍵生成部２０２は，署名生成部２０４が生成した電子署名の数（所定数）に応じて，順次，複数の暗号鍵からなる暗号鍵列から暗号鍵を抽出し，署名生成部２０４における暗号鍵を更新する。また，暗号鍵生成部２０２は，暗号鍵列および暗号鍵を管理し，暗号鍵列の中で，ネットワークに未公開である暗号鍵と既に公開されており暗号鍵を把握している。従って，所定数のメッセージ毎に暗号鍵を更新する場合，その履歴を到達確認部２１０に伝送することもできる。この暗号鍵は，数字や記号によって表されるとしても良く，暗号鍵自体をさらに暗号化して利用するとしても良い。

【００６２】

かかる構成により，メッセージ毎もしくは所定数のメッセージ毎に暗号鍵が更新され，そのうちの１つの鍵が漏洩したとしても連続的な不正を防止できる。また，各メッセージ

受信装置と暗号鍵の変更タイミング，例えば，電子署名の数を共通情報とすることで，不正な中継メッセージ受信装置によるメッセージの脱落も検出可能となる。

【００６３】

また，上記暗号鍵列の各暗号鍵は，予め設定された原暗号鍵からの一方向性関数により順次生成されたものであり，上記暗号鍵生成部は，上記生成順の逆に暗号鍵を抽出するとしても良い。

【００６４】

図４は，上述した一方向性関数ｆによる暗号鍵列を説明するための説明図である。メッセージ送信装置１００は，所定の原暗号鍵K_nを有しており，その原暗号鍵K_nから，一方向には一意に導き出せるが逆方向には導き出せない，例えば，ＭＤ５（Ｍｅｓｓａｇｅ Ｄｉｇｅｓｔ ５）やＳＨＡ－１（Ｓｅｃｕｒｅ Ｈａｓｈ Ａｌｇｏｒｉｔｈｍ １）等のハッシュ関数といった一方向性関数ｆにより順次暗号鍵を生成する。従って，図４に示すように，K_n，K_{n-1}，…，K_2，K_1，K_0といった具合にｎ＋１個の暗号鍵列が生成される。ここで，例えば，K_nからK_{n-1}への計算は，一方向性関数ｆ一回に限られず，任意の回数施されるとしても良い。そして，暗号鍵生成部２０２は，かかる生成順K_n，K_{n-1}，…，K_2，K_1，K_0の逆に暗号鍵を抽出する。従って，暗号鍵として利用される順番は，K_0，K_1，K_2，…，K_{n-1}，K_nとなる。

【００６５】

このように生成された暗号鍵列は，既に公開になっている暗号鍵，例えば，K_0からは，現在メッセージに利用される未公開の暗号鍵K_1を導き出すことはできず，メッセージ送信装置以外のメッセージ受信装置においてさえメッセージに対する正規の電子署名を生成することはできない。また，メッセージ受信装置１２０におけるメッセージ認証の際にはかかる現在の暗号鍵K_1も公開され，この暗号鍵K_1から，一方向性関数ｆ（メッセージ送信装置，メッセージ受信装置共有）により前回の暗号鍵K_0を導き出すことができ，暗号鍵自体の整合性をとることが可能となる。詳細は後述する。

【００６６】

上記署名生成部２０４は，メッセージ生成部２００から与えられたメッセージを証明するための電子署名を，暗号鍵生成部２０２から与えられた暗号鍵を用いて生成する。この暗号化は，ＭＡＣ（Ｍｅｓｓａｇｅ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｃｏｄｅ）生成アルゴリズム，例えば，ＡＥＳ暗号等のブロック暗号を用いたＣＢＣ－ＭＡＣ（Ｃｉｐｈｅｒ Ｂｌｏｃｋ Ｃｈａｉｎｉｎｇ－Ｍｅｓｓａｇｅ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｃｏｄｅ）によって実行されても良い。そして，上記暗号鍵および電子署名に関連付けてメッセージをメッセージ保持部２０６に送信し，また，電子署名のみをメッセージ送信部２０８に送信する。ここで生成される電子署名は，メッセージの認証子として利用され，数字や記号によって表される。

【００６７】

ここで，署名生成部２０４は，メッセージだけでなく，電子署名を生成するための暗号鍵もメッセージ保存部２０６に送信することができる。上記暗号鍵は，後述するメッセージ保持部２０６によって管理されるとしても良く，メッセージ送信装置１００自体や暗号鍵生成部２０２によって管理されるとしても良い。いずれにしても，メッセージ送信部２０８から暗号鍵を送信するタイミングで暗号鍵が参照されれば良い。

【００６８】

上記メッセージ保持部２０６は，上記メッセージを，上記暗号鍵および電子署名に関連付けて保持する。また，上述したように，メッセージと共にそのメッセージの暗号化に利用された暗号鍵も保持できる。また，メッセージ保持部２０６は，後述する到達確認部２１０からの指令に応じて，かかるメッセージおよび／または暗号鍵をメッセージ送信部２０８に送信する。

【００６９】

上記メッセージ送信部２０８は，署名生成部２０４から与えられた電子署名をメッセージ受信装置に送信し，かつ，メッセージ保持部２０６から与えられたメッセージおよび暗

号鍵もメッセージ受信装置に送信する。かかるメッセージは，電子署名に対して所定の遅延を伴って送信され，ここでは，メッセージ受信装置が送信予告としての電子署名を受信したことを確認するという処理を経て送信されている。

【００７０】

また，メッセージ送信部２０８は，メッセージと暗号鍵を同時に送信するとしても良く，さらに，次のメッセージの電子署名，即ち，更新された暗号鍵によって暗号化された電子署名と同時に送信することもできる。

【００７１】

また，メッセージ送信部２０８は，署名生成部２０４が所定数のメッセージに対する所定数の電子署名を，１つの暗号鍵を用いて生成している場合，所定数のメッセージと該所定数のメッセージに共通な暗号鍵とを送信するとしても良い。即ち，電子署名を生成するのに利用される暗号鍵が等しい所定数のメッセージの送信に対して，上記暗号鍵を１回のみ送信する。上記暗号鍵の更新を所定数のメッセージ毎に行う場合，その所定数のメッセージに対して暗号鍵は１つであり，送信する暗号鍵は，所定数のメッセージに対して１つあれば足りる。

【００７２】

上記到達確認部２１０は，上記メッセージ受信装置１２０が電子署名を正しく受信したことを知らせる受信確認情報を，上記メッセージ受信装置から受信し，上記メッセージに関連付けられた電子署名が上記メッセージ受信装置に到達したかどうかを判断し，到達していれば，メッセージと該メッセージに関連付けられた暗号鍵とをメッセージ送信部２０８に送信させる。

【００７３】

かかる到達判断は，例えば，メッセージ受信装置が受信確認情報中に電子署名をそのまま含めて返信し，メッセージ送信装置において，受け取った電子署名と，メッセージ送信装置が有する電子署名とを比較したり，または，メッセージ送信装置において電子署名にインデックスを付し，受信確認情報中に当該インデックスのみが返信され，このインデックスと，メッセージ送信装置が有するインデックスとを比較したりする等，様々な方法が考えられる。

【００７４】

また，これら受信確認情報自体の正当性に疑問が生じる場合（受信確認情報を偽造される脅威が存在する場合）には，メッセージ送信装置とメッセージ受信装置が新たに１対１の秘密鍵を共有し，受信確認情報を暗号化したり，受信確認情報に対する電子署名を生成・付加したりすることで，メッセージ送信装置が受け取った受信確認情報を認証することも考えられる。

【００７５】

到達確認部２１０は，電子署名の到達を確認した際に，単に受信確認情報中の電子署名に関する情報をメッセージ保持部２０６に送信するとしても良く，その場合，メッセージ保持部２０６は，与えられた電子署名に関する情報に対応したメッセージおよび暗号鍵をメッセージ送信部２０８に送信することとなる。

【００７６】

また，到達確認部２１０は，上記暗号鍵生成部２０２において署名生成部２０４が生成した電子署名の数（所定数）に応じて暗号鍵を更新する構成がとられる場合，かかる数と等しい数の受信確認情報を得た時点で，はじめて，メッセージ保持部２０６において電子署名に関連づけられた上記数分のメッセージと，そのメッセージ共通の暗号鍵とをメッセージ送信部２０８に送信させるとしても良い。

【００７７】

さらには，上記の数分の受信確認情報を得た時点で，到達確認部２１０が暗号鍵生成部２０２にその旨を伝達し，暗号鍵生成部２０２は，その時点で暗号鍵を更新するとしても良い。この場合，更新前の暗号鍵の各メッセージ受信装置への公開と，更新後の暗号鍵の署名生成部２０４への送信が同時に行われることとなり，メッセージ送信装置１００内の

暗号鍵同期が図られる。

【００７８】

かかる受信確認情報により，メッセージ送信装置１００が送信した電子署名等の情報が各メッセージ受信装置に偽りなく届いたかどうかを検証することができる。この検証をパスした場合，メッセージおよび暗号鍵を送信することができる。この暗号鍵は，電子署名を送信する時点において公開されておらず，不正な利用者がメッセージ送信装置になりすまして不正なメッセージを送信したとしても，先に送信されている電子署名との整合がとれないこととなる。

【００７９】

また，コンピュータを上記メッセージ送信装置１００として機能させるプログラムおよびその記憶媒体も提供される。

【００８０】

（メッセージ受信装置１２０）

図５は，第１の実施形態におけるメッセージ受信装置１２０の概略的な構成を示したブロック図である。かかるメッセージ受信装置１２０は，メッセージ受信部２５０と，受信確認送信部２５２と，署名保持部２５４と，暗号鍵検証部２５６と，メッセージ認証部２５８とを含んで構成される。上記メッセージ受信装置１２０は，メッセージ送信予告としての電子署名を受信し，受信したことを証明する受信確認情報を返信することにより，メッセージと暗号鍵をさらに受信することが可能となる。また，受信したメッセージは，暗号鍵と電子署名によって認証される。

【００８１】

上記メッセージ受信部２５０は，メッセージ送信装置１００から送信された電子署名，および，所定の遅延を経て送信されたメッセージと暗号鍵とを受信する。受信された電子署名は受信確認送信部２５２および署名保持部２５４に，メッセージはメッセージ認証部２５８に，暗号鍵は暗号鍵検証部２５６にそれぞれ送信される。

【００８２】

上記受信確認送信部２５２は，メッセージ受信部２５０から電子署名を受信し，該電子署名を正しく受信したことを知らせる受信確認情報を生成する。そして生成された受信確認情報をメッセージ送信装置１００に送信する。

【００８３】

かかる構成により，メッセージ送信予告としての電子署名を受け取ったことをメッセージ送信装置に返信することができ，その受信確認情報をもってしてメッセージおよび暗号鍵を受信することができる。この暗号鍵は，電子署名を送信する時点において公開されておらず，不正なメッセージの受信を検出することが可能となる。

【００８４】

上記署名保持部２５４は，メッセージ受信部２５０から与えられた電子署名を保持する。このとき，署名保持部２５４は，メッセージ受信部２５０が受信した，即ち，メッセージ送信装置１００が電子署名を送信した順番も把握する。また，署名保持部２５４は，所定の時間経過後，メッセージを認証するタイミングで，保持している電子署名を受信順にメッセージ認証部２５８に送信する。

【００８５】

上記暗号鍵検証部２５６は，メッセージ受信部２５０より与えられた暗号鍵が，正規のメッセージ送信装置１００の管理する暗号鍵列の鍵であることを検証する。詳細には，上記暗号鍵が，予め設定された，電子署名もしくはメッセージの数毎に更新されていることを検証し，不整合の場合，該暗号鍵をメッセージ送信装置１００が送信したことを認証しない。

【００８６】

また，暗号鍵検証部２５６は，さらに，暗号鍵を保持し，暗号鍵が更新された場合，更新された暗号鍵から一方向性関数ｆを任意の回数施し，その計算結果と，保持された以前の暗号鍵の値とを比較し，一致しない場合，該暗号鍵をメッセージ送信装置１００が送信

したことを認証しないとすることができる。このようにして更新された暗号鍵が正規の暗号鍵であるかどうかを検証することができる。

【００８７】

上述したようにメッセージ送信装置１００は，暗号鍵K_0，K_1，K_2，…，K_{n-1}，K_nの暗号鍵列を有しており，例えば，暗号鍵K_1で暗号化した電子署名を一通り送信した後，暗号鍵K_2への更新タイミングで，かかる暗号鍵K_1を公開する。

【００８８】

図６は，上述した一方向性関数ｆによる暗号鍵の検証を説明するための説明図である。かかる図６を参照して説明すると，メッセージ受信装置１２０は，暗号鍵K_0を保持し，その後，暗号鍵K_1で暗号化された電子署名を受信する。そして，一通り（所定数）電子署名を受信した後で，暗号鍵K_1が公開される。この暗号鍵K_1をメッセージ送信装置１００と同じ一方向性関数ｆを任意の回数用いて計算すると暗号鍵K_0が導出されるはずである。従って，$f(K_1)=K_0$となった場合，暗号鍵K_1は正しい暗号鍵であると判断され，後の処理に暗号鍵K_1が利用される。また，暗号鍵K_1は，次の暗号鍵K_2の認証のために保持される。

【００８９】

既に公開になっている暗号鍵，例えば，K_0からは，現在メッセージに利用される未公開の暗号鍵K_1を導き出すことはできないので，メッセージ送信装置以外のメッセージ受信装置においてさえメッセージに対する正規の電子署名を生成することはできない。

【００９０】

上記メッセージ認証部２５８は，メッセージ受信部２５０より与えられたメッセージが，メッセージ送信装置１００が生成した正しいメッセージであることを認証する。従って，メッセージ認証部２５８は，メッセージ受信部２５０で受信されたメッセージに対して，同時に受信した暗号鍵を用いて新たな電子署名を生成し，それと上記署名保持部２５４で保持された電子署名とを比較し該メッセージを認証する。また，かかる暗号鍵が所定数のメッセージに共通に付与されている場合，メッセージ認証部２５８は，対応する数分だけ共通の鍵を利用し，メッセージを認証する。この所定数は，メッセージ送信装置１００との間で規定されている。

【００９１】

また，コンピュータを上記メッセージ受信装置１２０として機能させるプログラムおよびその記憶媒体も提供される。

【００９２】

（メッセージ送信方法，メッセージ受信方法）

続いて，第１の実施形態におけるマルチホップ通信によりメッセージ送信装置から複数のメッセージ受信装置にメッセージを送信するメッセージ送信方法および，そのメッセージを受信するメッセージ受信方法を説明する。

【００９３】

図７は，メッセージ送信方法およびメッセージ受信方法の処理の流れを示したフローチャートである。先ず，メッセージ送信装置１００は，メッセージM_iを生成し（Ｓ３００），かかるメッセージM_iに対する電子署名$MAC_{K_i}(M_i)$を，各メッセージ受信装置１２０（ネットワーク）に未公開の暗号鍵K_iを用いて（暗号化して）生成する（Ｓ３０２）。ここでｉは整数である。そして，生成された電子署名$MAC_{K_i}(M_i)$をメッセージ受信装置１２０ｃに送信し（Ｓ３０４），メッセージM_iを電子署名$MAC_{K_i}(M_i)$に関連づけてメッセージ送信装置１００内に保持する（Ｓ３０６）。かかる暗号鍵K_iは，上述した一方向関数を利用して生成された暗号鍵列から順次抽出された暗号鍵である。従って，K_{i+1}からK_iは生成できるが，K_iからK_{i+1}は導くことができない。

【００９４】

続いて，メッセージ受信装置１２０ｃは，電子署名$MAC_{K_i}(M_i)$を受信し，その電子署名$MAC_{K_i}(M_i)$を暗号鍵K_iが送信されるまで保持し（Ｓ３１０），電子署

名$MAC_{K_i}(M_i)$を正しく受信したことを知らせる受信確認情報をメッセージ送信装置１００に返信する（Ｓ３１２）。ここで，メッセージ受信装置１２０ｃは，受信した電子署名$MAC_{K_i}(M_i)$の順番を把握している。

【００９５】

メッセージ送信装置１００は，かかる受信確認情報を検証することによって，電子署名$MAC_{K_i}(M_i)$がメッセージ受信装置１２０ｃに到達したかどうかを判断し（Ｓ３２０），到達していれば，暗号鍵K_iを各メッセージ受信装置（ネットワーク）に公開することを決定し，メッセージ受信装置１２０ｃに対して暗号鍵K_iを送信する（Ｓ３２２）。このとき，次のメッセージM_{i+1}を暗号化する暗号鍵をK_{i+1}に更新し，その暗号鍵K_{i+1}を署名生成部に与える。また，暗号鍵K_iの送信タイミングと同時，もしくはその前後にメッセージM_iも送信する（Ｓ３２４）。送信完了後，次のメッセージM_{i+1}送信の準備を行う（Ｓ３２６）。

【００９６】

メッセージ受信装置１２０ｃでは，受信した暗号鍵K_iの検証を行う（Ｓ３３０）。この暗号鍵K_iの検証は，一方向性関数ｆによって暗号鍵K_iを計算した結果と，メッセージ受信装置１２０ｃで保持してある前回の暗号鍵K_{i-1}とを比較することによって実行される。両値が一致した場合，暗号鍵K_iが次のメッセージM_{i+1}に関する暗号鍵K_{i+1}のために保持され，後段のステップに移行する。不一致の場合，認証エラーとなって，エラー処理が行われる。

【００９７】

上記受信した暗号鍵K_iが正しいと判断された場合，メッセージ送信装置１００から署名受信・保持ステップ（Ｓ３１０）で受信した電子署名$MAC_{K_i}(M_i)$の検証が行われる（Ｓ３３２）。この電子署名$MAC_{K_i}(M_i)$の検証の計算は，メッセージ送信装置１００で電子署名を生成したのと同じ手順により電子署名を生成し，メッセージ受信装置１２０ｃで保持された電子署名$MAC_{K_i}(M_i)$と一致するかどうかを判断することによって行われる。

【００９８】

これによってメッセージ送信装置１００から送信されたメッセージM_iもしくは電子署名$MAC_{K_i}(M_i)$のいずれかが変更されていることを抽出することが可能となる。このような検証（Ｓ３３２）を通過すると，メッセージM_iが認証され（Ｓ３３４），メッセージ受信装置１２０ｃは，かかるメッセージM_iの処理と次のメッセージM_{i+1}受信の準備を行う（Ｓ３３６）。

【００９９】

ここでは，理解を容易にするため，図２同様，メッセージ送信装置１００からメッセージ受信装置１２０ｃへのメッセージ送信のみを説明したが，勿論かかる場合に限られず，例えば，メッセージ送信装置１００とメッセージ受信装置１２０ａ間や，メッセージ送信装置１００とメッセージ受信装置１２０ｂ間においても同様の処理が行われている。また，図７においては，メッセージ送信装置１００からメッセージ受信装置１２０ｃへのデータ転送を直線で示しているが，メッセージ受信装置１２０ａ，１２０ｂをルータメッセージ受信装置として経由する場合も含んでいる。

【０１００】

また，上記ではメッセージ１個に対して暗号鍵を１つ更新する場合を記載しているが，所定数のメッセージに対して暗号鍵を１つ利用するといった構成をとることもできる。その場合，先ず，メッセージ送信装置１００とメッセージ受信装置１２０との間で，電子署名と受信確認情報とのやりとりが１０回行われ，その後，１０のメッセージと１つの暗号鍵とを送信することになる。

【０１０１】

図８は，上記に示したメッセージ送信装置１００とメッセージ受信装置１２０との通信を簡単に示したフローチャートである。図８によると，メッセージ送信装置１００は，メッセージ受信装置１２０に対してメッセージの数分の電子署名のみを送信しているので，

メッセージ受信装置１２０にはメッセージが保持されず，メッセージを認証する時点ａではじめてメッセージを受信する。従って，メッセージ受信装置１２０におけるメッセージのメモリ占有率を最小化することが可能となる。

【０１０２】

これは，メッセージのデータサイズが，送信予告としての電子署名のデータサイズよりも大きい場合に特に効果がある。

【０１０３】

また，上記の構成により，他のメッセージ受信装置である中継メッセージ受信装置による，メッセージの改竄，メッセージの中断，またはメッセージ送信装置のなりすましも防止される。

【０１０４】

図９は，中継メッセージ受信装置の不正回避を説明するためのフローチャートである。例えば，メッセージ送信装置１００からメッセージM_{0-0}の電子署名MAC_{K0}（M_{0-0}）が送信され，中継メッセージ受信装置３５０を介してメッセージ受信装置１２０に到達した場合，メッセージ受信装置１２０は，中継メッセージ受信装置３５０を介してメッセージ送信装置に受信確認情報$_0$を送信する。引き続きメッセージ送信装置１００は，メッセージM_{0-1}の電子署名MAC_{K0}（M_{0-1}）を送信したが，中継メッセージ受信装置３５０が不正にその電子署名MAC_{K0}（M_{0-1}）のメッセージ受信装置１２０への送信を中断したとする。このとき，メッセージ受信装置１２０からは，受信確認情報$_0$が送信されないので，メッセージ送信装置１００は，メッセージM_{0-0}，M_{0-1}を送信することはない。

【０１０５】

また，上記不正な中継メッセージ受信装置３５０がメッセージ送信装置１００になりすまして，一旦，メッセージ受信装置１２０への電子署名MAC_{K0}（M_{0-1}）の送信を中断し，後にメッセージ受信装置１２０から送信される暗号鍵K_0を利用して，メッセージ受信装置１２０に不正なメッセージを送ろうとしても，そもそもメッセージ送信装置１００で受信確認情報の検証が行われるので，暗号鍵K_0は公開されることがなく，このような中継メッセージ受信装置３５０がメッセージ送信装置１００のなりすましを実行できない。

【０１０６】

（第２の実施形態：時刻同期方式によるメッセージ認証システム）

次に（２）時刻同期式のメッセージ認証システムを説明する。

【０１０７】

図１０は，時刻同期方式によるメッセージ認証システムを説明するためのタイミングチャートである。ここでは，メッセージ送信装置４００から直接または１以上の中継メッセージ受信装置を介して，メッセージ受信装置４２０にメッセージが伝送される。このとき，メッセージ送信装置４００，中継メッセージ受信装置，メッセージ受信装置４２０は同一の時間軸で同期して動作する。

【０１０８】

メッセージ送信装置４００内の，例えば暗号鍵K_1が有効な期間４０２において，送信すべきメッセージM_{1-0}，M_{1-1}は暗号鍵K_1で暗号化される。そしてメッセージ送信装置４００は，かかるメッセージM_{1-0}，M_{1-1}の電子署名MAC_{K1}（M_{1-0}），MAC_{K1}（M_{1-1}）を生成した後，その電子署名MAC_{K1}（M_{1-0}），MAC_{K1}（M_{1-1}）をメッセージ受信装置４２０に対してブロードキャストする。そして，メッセージ送信装置４００は，暗号鍵が更新された時刻から所定の時間４０４経過後に暗号鍵K_1を，その電子署名MAC_{K1}（M_{1-0}），MAC_{K1}（M_{1-1}）の送信から所定の時間４０６経過後にメッセージM_{1-0}，M_{1-1}をメッセージ受信装置４２０に送信する。

【０１０９】

メッセージ送信装置４００から電子署名MAC_{K1}（M_{1-0}），MAC_{K1}（M_{1-

$_1$）を受信したメッセージ受信装置４２０は，かかる電子署名の受信からメッセージM_{1-0}，M_{1-1}の受信までの時間をカウントし，また，K_1の有効期間が切り換わってから，かかる未公開のK_1が公開されるまでの時間もカウントする。そして，かかるカウント値，即ち，送信遅延時間４１０，４１２がメッセージ送信装置４００と共有している所定の時間４０４や４０６と等しいか検証する。

【０１１０】

ここで，メッセージや暗号鍵を所定時間遅延させて送信するのは，一番離れたメッセージ受信装置にも送信データが確実に届いてから暗号鍵を公開し，他のメッセージ受信装置や電子機器のメッセージ送信装置なりすましを回避するためである。従って，上記送信遅延時間は，メッセージ受信装置との通信時間を考慮して，通信が完了する十分に長い時間が採用され，メッセージ送信装置４００およびメッセージ受信装置４２０間で共有される。

【０１１１】

このように時刻同期がとられたメッセージ認証システムでは，中継メッセージ受信装置や他の電子機器が不正を行おうとすると，必ずタイミングのずれが生じ，かかるタイミングのずれを検出することでメッセージの認証が成立する。

【０１１２】

ここでは，理解を容易にするため，メッセージ送信装置４００からメッセージ受信装置４２０へのメッセージ送信のみを説明したが，勿論かかる場合に限られず，例えば，メッセージ送信装置４００と中継メッセージ受信装置間においても同様の処理が行われている。

【０１１３】

また，上記のメッセージ認証システムでは，かかるメッセージの送信を暗号鍵の送信タイミングに合わせることにより，暗号鍵が公開されるまでにメッセージ受信装置にメッセージが保持されず，メッセージのメモリ占有率を最小化することが可能となる。

【０１１４】

（メッセージ送信装置４００）

図１１は，第２の実施形態におけるメッセージ送信装置４００の概略的な構成を示したブロック図である。かかるメッセージ送信装置４００は，メッセージ生成部２００と，暗号鍵生成部２０２と，署名生成部２０４と，メッセージ保持部２０６と，メッセージ送信部２０８と，時刻同期制御部４１６とを含んで構成される。上記メッセージ送信装置４００は，メッセージ送信予告として先に電子署名を送信し，所定の遅延を経て，ここでは，上記電子署名に対するメッセージの送信遅延時間と，暗号鍵の更新に対する暗号鍵の送信遅延時間経過後に，本体であるメッセージ，および，電子署名との確認に利用される暗号鍵を送信する。

【０１１５】

第１の実施形態における構成要素として既に述べたメッセージ生成部２００と，暗号鍵生成部２０２と，署名生成部２０４と，メッセージ保持部２０６と，メッセージ送信部２０８とは，実質的に機能が同一なので重複説明を省略し，ここでは，新たな機能を有す時刻同期制御部４１６を主に説明する。

【０１１６】

上記時刻同期制御部４１６は，各メッセージ受信装置との時刻同期をとった後，暗号鍵生成部２０２における暗号鍵の有効時間（利用時間）と，上記電子署名に対するメッセージの送信遅延時間と，暗号鍵の更新時に対する暗号鍵の送信遅延時間とを管理し，該送信遅延時間に応じて，上記メッセージと該メッセージに関連付けられた暗号鍵とをメッセージ送信部に送信させる。

【０１１７】

具体的に，時刻同期制御部４１６は，暗号鍵生成部２０２に対して暗号鍵の更新タイミングを指示し，暗号鍵生成部２０２は，そのタイミングで新たな暗号鍵を暗号鍵列から抽出する。また，時刻同期制御部４１６は，メッセージ保持部２０６に，その更新タイミン

グから所定の送信遅延時間を経て暗号鍵を送信させること，および，電子署名の送信から所定の送信遅延時間を経てメッセージを送信させることを指示する。

【０１１８】

かかる構成により，各メッセージ受信装置と時刻同期を行うことができ，メッセージや暗号鍵の送受信時間を合わせることが可能となる。従って，不正なメッセージ受信装置や他の電子機器でメッセージの改竄を行ったとしても時刻同期からの時間偏差によってそのメッセージを検出できる。

【０１１９】

このとき，第１の実施形態で述べたように，暗号鍵がメッセージに関連付けられてメッセージ保持部２０６に保持されても良いし，メッセージ送信装置１００自体や暗号鍵生成部２０２によって管理されるとしても良い。いずれにしても，メッセージ送信部２０８から暗号鍵を送信すべきタイミングで暗号鍵が参照されれば良い。

【０１２０】

また，コンピュータを上記メッセージ送信装置４００として機能させるプログラムおよびその記憶媒体も提供される。

【０１２１】

（メッセージ受信装置４２０）

図１２は，第２の実施形態におけるメッセージ受信装置４２０の概略的な構成を示したブロック図である。かかるメッセージ受信装置４２０は，メッセージ受信部２５０と，署名保持部２５４と，暗号鍵検証部２５６と，メッセージ認証部２５８と，時刻同期検証部４５２とを含んで構成される。上記メッセージ受信装置４２０は，メッセージ送信予告としての電子署名を受信し，その後のメッセージおよび暗号鍵の受信タイミングによってメッセージの認証が行われる。

【０１２２】

第１の実施形態における構成要素として既に述べたメッセージ受信部２５０と，署名保持部２５４と，暗号鍵検証部２５６と，メッセージ認証部２５８とは，実質的に機能が同一なので重複説明を省略し，ここでは，新たな機能を有す時刻同期検証部４５２を主に説明する。

【０１２３】

上記時刻同期検証部４５２は，先ず，メッセージ送信装置４００から送信された時刻同期情報と時刻制御情報をメッセージ受信部２５０から得て，メッセージ送信装置４００との時刻同期をとる。また，上記時刻制御情報によって，メッセージ送信装置４００の暗号鍵の有効時間（利用時間）と，電子署名に対するメッセージの送信遅延時間と，暗号鍵の更新時に対する暗号鍵の送信遅延時間とを共通の情報として保持する。

【０１２４】

時刻同期検証部４５２は，メッセージ送信装置４００との時刻同期がとられた後，メッセージ送信装置４００との間で設定され，共通の情報として保持する，電子署名に対するメッセージの送信遅延時間と，上記暗号鍵の更新時に対する暗号鍵の送信遅延時間に応じて，上記メッセージおよび暗号鍵を受信しているか検証し，受信した時刻が所定範囲を超えて相違する場合，該メッセージを認証しない。

【０１２５】

これは，図１０を用いて説明したように，時刻同期検証部４５２において時刻同期がとられ，メッセージ受信部２５０に到達したメッセージや暗号鍵が所定の送信遅延時間が守られて受信されているかを検証する。上記メッセージの検証では，時刻同期検証部４５２が電子署名を受信してカウントを開始し，メッセージを受信した時にその送信遅延時間を設定された時間と比較する。上記暗号鍵の検証では，メッセージ送信装置４００と同期された暗号鍵の更新タイミングから暗号鍵の受信までをカウントし，その送信遅延時間を設定された時間と比較している。

【０１２６】

上記では，暗号鍵を，更新時からの時間で検証しているがかかる場合に限られず，電子

署名からの送信遅延時間によって検証されるとしても良い。また，上記では，時刻同期検証部４５２によって，メッセージおよび暗号鍵の送信遅延時間を検証しているが，各検証をメッセージ認証部２５８や暗号鍵検証部２５６で行うとしても良い。このとき，署名保持部２５４は，メッセージ受信部２５０が電子署名を受信した時刻もメッセージに関連付けて保持することができる。

【０１２７】

かかる構成により，メッセージ送信装置４００と時刻同期を行うことができ，メッセージや暗号鍵の送受信時間を合わせることが可能となる。従って，不正なメッセージ受信装置や他の電子機器でメッセージの改竄を行ったとしても上記時刻同期からの時間偏差によってそのメッセージを検出できる。

【０１２８】

また，コンピュータを上記メッセージ受信装置４２０として機能させるプログラムおよびその記憶媒体も提供される。

【０１２９】

（メッセージ送信方法，メッセージ受信方法）

続いて，第２の実施形態におけるマルチホップ通信によりメッセージ送信装置から複数のメッセージ受信装置にメッセージを送信するメッセージ送信方法および，そのメッセージを受信するメッセージ受信方法を説明する。

【０１３０】

図１３は，メッセージ送信方法およびメッセージ受信方法の処理の流れを示したフローチャートである。先ず，メッセージ送信装置４００は，メッセージM_iを生成し（Ｓ５００），各メッセージ受信装置４２０（ネットワーク）に未公開の暗号鍵K_iが有効な期間において，かかるメッセージM_iに対する電子署名$MAC_{K_i}(M_i)$を，暗号鍵K_iを用いて生成する（Ｓ５０２）。ここでｉは整数である。

【０１３１】

そして，メッセージ送信装置４００は，生成された電子署名$MAC_{K_i}(M_i)$をメッセージ受信装置４２０ｃに送信し（Ｓ５０４），メッセージM_iを電子署名$MAC_{K_i}(M_i)$に関連づけてメッセージ送信装置４００内に保持する（Ｓ５０６）。かかる暗号鍵K_iは，上述した一方向関数を利用して生成された暗号鍵列から順次抽出された暗号鍵である。従って，K_{i+1}からK_iは生成できるが，K_iからK_{i+1}は導くことができない。

【０１３２】

続いて，メッセージ受信装置４２０ｃは，電子署名$MAC_{K_i}(M_i)$を受信し，その電子署名$MAC_{K_i}(M_i)$を暗号鍵K_iが送信されるまで保持する（Ｓ５１０）。このとき，メッセージ受信装置４２０ｃでは，電子署名$MAC_{K_i}(M_i)$が受信された時刻も確認され，かかる電子署名$MAC_{K_i}(M_i)$の受信時からメッセージの送信遅延時間を判断するためのカウントが開始される（Ｓ５１２）。ここで，メッセージ受信装置１２０ｃは，メッセージの認証のため，受信した電子署名$MAC_{K_i}(M_i)$の順番も把握している。

【０１３３】

メッセージ送信装置４００は，管理している時刻同期に基づいて，次のメッセージM_{i+1}を暗号化する暗号鍵をK_{i+1}暗号鍵列から抽出して更新し，その暗号鍵K_{i+1}を署名生成部に与える。即ち，その時点で暗号鍵K_iの有効時間は終了し，新たに暗号鍵K_{i+1}が有効になる。そして，このような暗号鍵の更新時点から設定された暗号鍵K_iの送信遅延時間をカウントし（Ｓ５２０），その送信遅延時間に到達すると，暗号鍵K_iを各メッセージ受信装置（ネットワーク）に公開することを決定し，メッセージ受信装置４２０ｃに対して暗号鍵K_iを送信する（Ｓ５２２）。

【０１３４】

また，メッセージ送信装置４００では，暗号鍵同様，電子署名$MAC_{K_i}(M_i)$の送信時からメッセージM_iの送信遅延時間をカウントし（Ｓ５２４），その送信遅延時間に

到達すると，メッセージM_iを，メッセージ受信装置４２０ｃを含む各メッセージ受信装置に送信する（Ｓ５２６）。このメッセージM_iの送信タイミングは，暗号鍵K_iの送信タイミングと前後しても良い。送信完了後，次のメッセージM_{i+1}送信の準備を行う（Ｓ５２８）。

【０１３５】

メッセージ受信装置４２０ｃでは，受信した暗号鍵K_iの検証を行う（Ｓ５３０）。この暗号鍵K_iの検証は，第１に，暗号鍵K_iから暗号鍵K_{i+1}の更新タイミングから設定された送信遅延時間に暗号鍵が公開されているかどうかにより実行される。第２に，一方向性関数ｆによって暗号鍵K_iを計算した結果と，メッセージ受信装置４２０ｃで保持してある前回の暗号鍵K_{i-1}とを比較することによって実行される。両値が一致した場合，暗号鍵K_iが次のメッセージM_{i+1}に関する暗号鍵K_{i+1}のために保持され，後段のステップに移行する。不一致の場合，認証エラーとなって，エラー処理が行われる。

【０１３６】

上記受信した暗号鍵K_iが正しいと判断された場合，上記同様，メッセージ送信装置４００から署名受信・保持ステップ（Ｓ５１０）で受信した電子署名$MAC_{Ki}(M_i)$からメッセージM_i到達までの送信遅延時間が検証される（Ｓ５３２）。そして，引き続き，電子署名$MAC_{Ki}(M_i)$の検証が行われる（Ｓ５３４）。この電子署名$MAC_{Ki}(M_i)$の検証の計算は，メッセージ送信装置４００で電子署名を生成したのと同じ手順により電子署名を生成し，メッセージ受信装置４２０ｃで保持された電子署名$MAC_{Ki}(M_i)$と一致するかどうかを判断することによって行われる。

【０１３７】

これによってメッセージ送信装置４００から送信されたメッセージM_iもしくは電子署名$MAC_{Ki}(M_i)$のいずれかが変更されていることを抽出することが可能となる。このような検証（Ｓ５３２，Ｓ５３４）を通過すると，メッセージM_iが認証され（Ｓ５３６），メッセージ受信装置４２０ｃは，かかるメッセージM_iの処理と次のメッセージM_{i+1}受信の準備を行う（Ｓ５３８）。

【０１３８】

ここでは，理解を容易にするため，図２同様，メッセージ送信装置４００からメッセージ受信装置４２０ｃへのメッセージ送信のみを説明したが，勿論かかる場合に限られず，例えば，メッセージ送信装置４００とメッセージ受信装置４２０ａ間や，メッセージ送信装置４００とメッセージ受信装置４２０ｂ間においても同様の処理が行われている。また，図１３においては，メッセージ送信装置４００からメッセージ受信装置４２０ｃへのデータ転送を直線で示しているが，メッセージ受信装置４２０ａ，４２０ｂを，ルータ機能を有する中継メッセージ受信装置として経由する場合も含んでいる。

【０１３９】

また，上記ではメッセージ１個に対して暗号鍵を１つ更新する場合を記載しているが，暗号鍵K_iの有効時間内に電子署名を生成された全てのメッセージに対して暗号鍵が１つ送信されることになる。

【０１４０】

（第３の実施形態：メッセージ送信装置およびメッセージ受信装置）

図１４は，上述した第１および第２の実施形態で利用することが可能なメッセージ送信装置１００（，４００）の具体的な構成を示したブロック図である。上記メッセージ送信装置１００は，ＣＰＵ６００と，ＲＯＭ６０２と，ＲＡＭ６０４と，キーボード６０６と，マウス６０８と，送信ドライバ６２０と，受信ドライバ６２２と，アンテナ６２４と，表示部６３０とを含んで構成される。

【０１４１】

上記ＣＰＵ６００は，メッセージ受信装置１００全体を制御すると共に，上述した実施形態におけるメッセージ送信方法を遂行する。

【０１４２】

上記ＲＯＭ６０２は，上述したメッセージ受信装置１００として機能させるプログラム

を格納するとしても良い。また，上記ＲＡＭ６０４は，上記プログラムを遂行する上での補助的な役目を担い，ハードディスクドライブと共に，メッセージ保持部としても利用できる。

【０１４３】

上記キーボード６０６やマウス６０８は，ユーザインターフェースであり，本実施形態においては，主として，メッセージ受信装置１２０に送信されるメッセージの作成を補助する。また，かかるユーザインターフェースを利用して，例えば，インターネット等の通信網から既存のメッセージをダウンロードし，メッセージとしてメッセージ受信装置１２０に送信するとしても良い。

【０１４４】

上記送信ドライバ６２０は，ＣＰＵ６００により送信される電子署名，メッセージ，および，暗号鍵等の電子データをシリアル送信可能なフォーマットに変更してアンテナ６２４に送信する。

【０１４５】

上記受信ドライバ６２２はアンテナ６２４で受信したメッセージ受信装置１２０からのデータをＣＰＵ６００が処理できるフォーマットに変換し，ＣＰＵ６００に転送する。

【０１４６】

上記表示部６３０は，メッセージの生成や，プログラムのメンテナンス等において，その内容を確認するために利用され得る。

【０１４７】

図１５は，上述した第１および第２の実施形態で利用することが可能なメッセージ受信装置１２０（，４２０）の具体的な構成を示したブロック図である。上記メッセージ受信装置１２０は，ＣＰＵ７００と，ＲＯＭ７０２と，ＲＡＭ７０４と，センサ７０６と，送信ドライバ７２０と，受信ドライバ７２２と，アンテナ７２４とを含んで構成される。

【０１４８】

上記ＣＰＵ７００と，ＲＯＭ７０２と，ＲＡＭ７０４と，送信ドライバ７２０と，受信ドライバ７２２と，アンテナ７２４とは，上述したメッセージ送信装置１００におけるＲＯＭ６０２と，ＲＡＭ６０４と，送信ドライバ６２０と，受信ドライバ６２２と，アンテナ６２４と実質的に機能が同一なので重複説明を省略する。

【０１４９】

上記センサ７０６は，輝度等の光量，音量，温度，気圧，湿度といった様々な計測装置で構成される。従って，本実施形態のメッセージ受信装置１２０は，センサ機能を有するメッセージ受信装置，例えばセンサノードとして利用でき，メッセージ送信装置１台に対して，複数のセンサノードが準備され，各センサノードが配置された場所の様々な情報を収集することができる。

【０１５０】

以上，添付図面を参照しながら本発明の好適な実施形態について説明したが，本発明は係る例に限定されないことは言うまでもない。当業者であれば，特許請求の範囲に記載された範疇内において，各種の変更例または修正例に想到し得ることは明らかであり，それらについても当然に本発明の技術的範囲に属するものと了解される。

【０１５１】

上記各実施形態においては，暗号鍵を暗号鍵列から抽出して利用しているがかかる場合に限られず，例えば，署名生成部で利用される暗号鍵として暗号鍵列の各暗号鍵から派生した情報を用いても良い。この場合，メッセージ送信装置とメッセージ受信装置間でかかる情報を共有する。

【０１５２】

また，上記各実施形態では，マルチホップ通信においてメッセージ送信装置と他のメッセージ受信装置間を中継する中継メッセージ受信装置（ルータメッセージ受信装置）に関して詳述していないが，上記メッセージ受信装置は，他のメッセージ受信装置への中継器を有するとしても良く，その場合，各メッセージ受信装置からメッセージ送信装置に送ら

れるデータも中継することができる。

【０１５３】

また，本実施形態は，図１に示したようなマルチホップツリー構造を用いて説明しているが，かかる構造に限定されるものではなく，例えば，本件出願人による特願２００４－３２４０９４号に示されるようなワンホップのスター型のネットワーク構造にも適用することが可能である。

【０１５４】

なお，本明細書のメッセージ送信方法やメッセージ受信方法における各工程は，必ずしもフローチャートとして記載された順序に沿って時系列に処理する必要はなく，並列的あるいは個別に実行される処理（例えば，並列処理あるいはオブジェクトによる処理）も含むとしても良い。

【図面の簡単な説明】

【０１５５】

【図１】マルチホップ通信を説明するための概略図である。

【図２】回数同期方式によるメッセージ認証システムを説明するためのフローチャートである。

【図３】第１の実施形態におけるメッセージ送信装置の概略的な構成を示したブロック図である。

【図４】一方向性関数による暗号鍵列を説明するための説明図である。

【図５】第１の実施形態におけるメッセージ受信装置の概略的な構成を示したブロック図である。

【図６】一方向性関数による暗号鍵の検証を説明するための説明図である。

【図７】メッセージ送信方法およびメッセージ受信方法の処理の流れを示したフローチャートである。

【図８】メッセージ送信装置とメッセージ受信装置との通信を簡単に示したフローチャートである。

【図９】中継メッセージ受信装置の不正回避を説明するためのフローチャートである。

【図１０】時刻同期方式によるメッセージ認証システムを説明するためのタイミングチャートである。

【図１１】第２の実施形態におけるメッセージ送信装置の概略的な構成を示したブロック図である。

【図１２】第２の実施形態におけるメッセージ受信装置の概略的な構成を示したブロック図である。

【図１３】メッセージ送信方法およびメッセージ受信方法の処理の流れを示したフローチャートである。

【図１４】メッセージ送信装置の具体的な構成を示したブロック図である。

【図１５】メッセージ受信装置の具体的な構成を示したブロック図である。

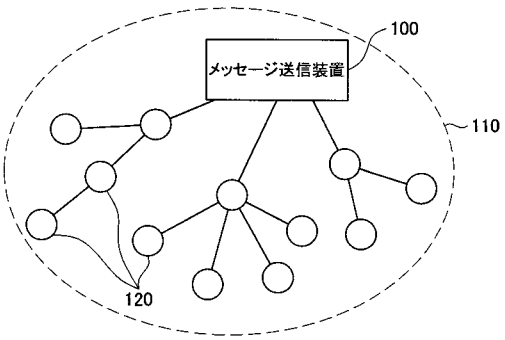
【符号の説明】

【０１５６】

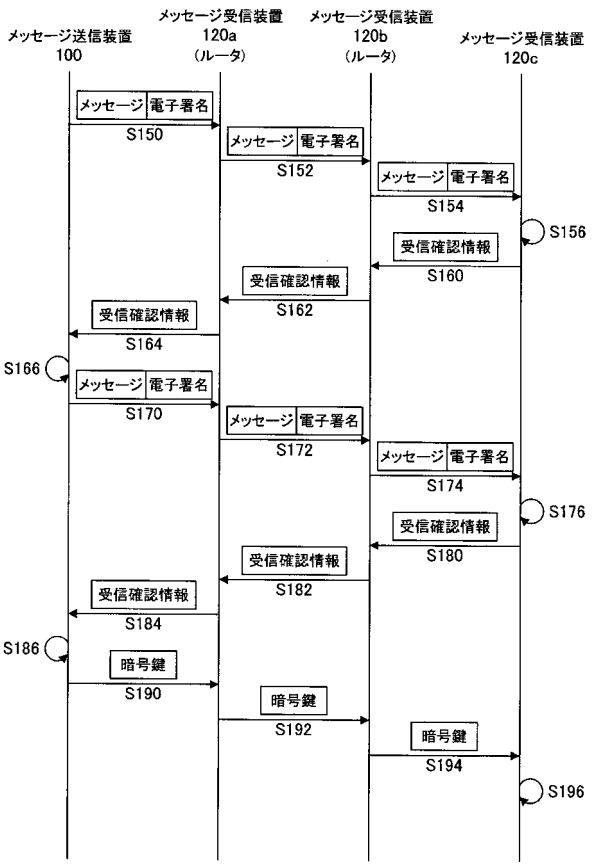
１００，４００　メッセージ送信装置
１２０，４２０　メッセージ受信装置
２０２　暗号鍵生成部
２０４　署名生成部
２０６　メッセージ保持部
２０８　メッセージ送信部
２１０　到達確認部
２５０　メッセージ受信部
２５２　受信確認送信部
２５４　署名保持部
２５６　暗号鍵検証部

２５８　メッセージ認証部
４１６　時刻同期制御部
４５２　時刻同期検証部

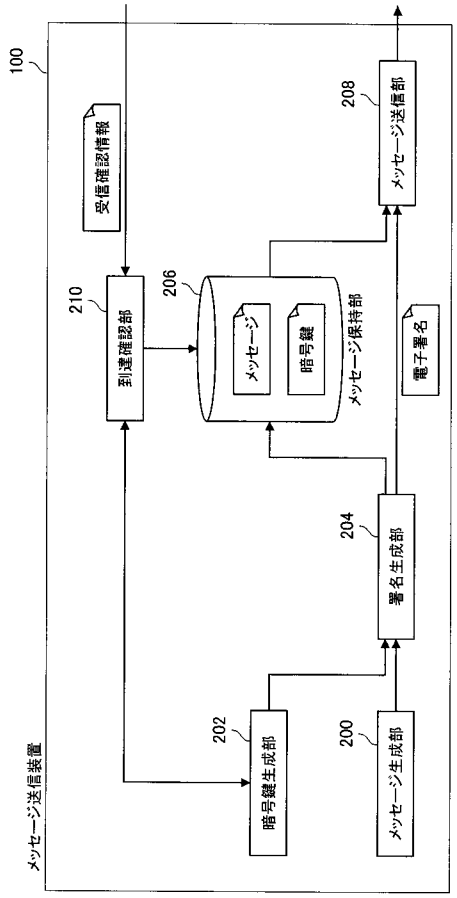
【図１】



【図２】



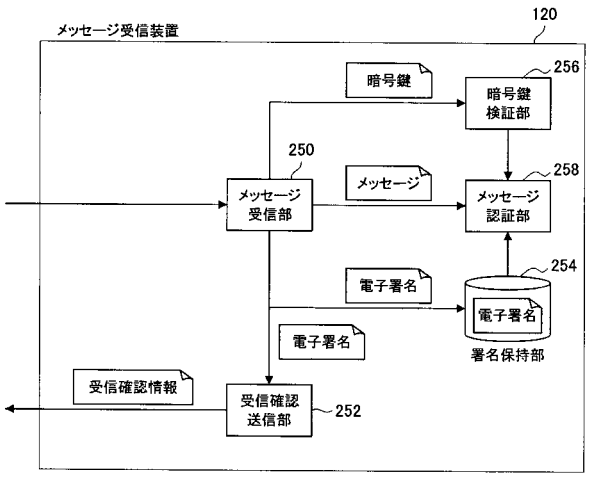
【図３】


100
メッセージ送信装置
受信確認情報
208
メッセージ送信部
210
到達確認部
206
メッセージ
暗号鍵
メッセージ保持部
電子署名
204
署名生成部
202
暗号鍵生成部
200
メッセージ生成部

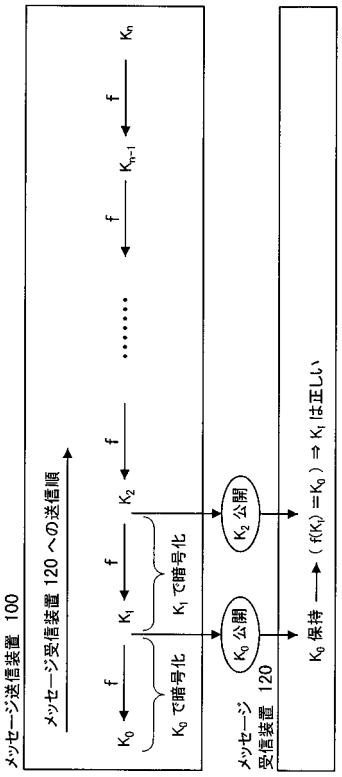
【図４】


K0
f
K1
K2
Kn-1
Kn

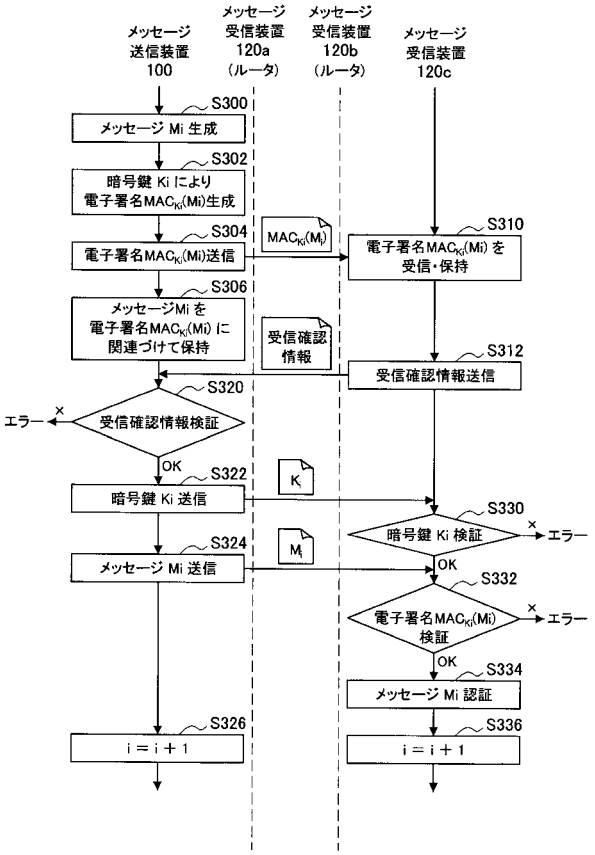
【図５】


メッセージ受信装置
120
暗号鍵
256
暗号鍵
検証部
250
メッセージ
受信部
メッセージ
258
メッセージ
認証部
電子署名
254
電子署名
電子署名
署名保持部
受信確認情報
受信確認
送信部
252

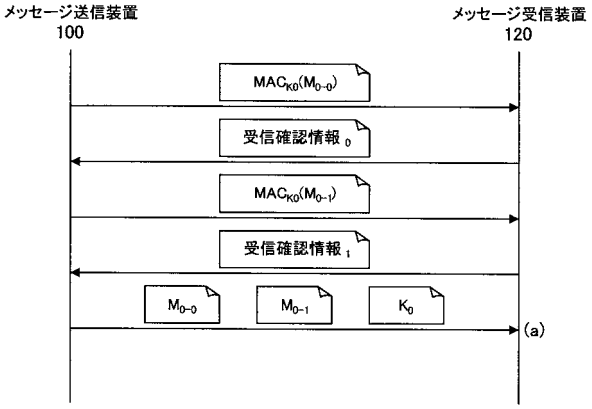
【図６】


メッセージ送信装置 100
メッセージ受信装置 120への送信順
K0
K1
K2
Kn-1
Kn
f
K0で暗号化
K1で暗号化
K0 公開
K2 公開
メッセージ
受信装置 120
K0 保持 ⟶ (f(K0)=K0) ⇒ K1 は正しい

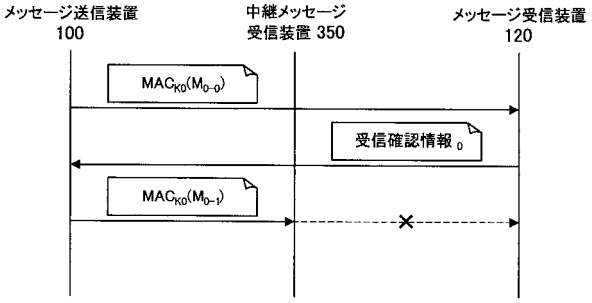
【図７】



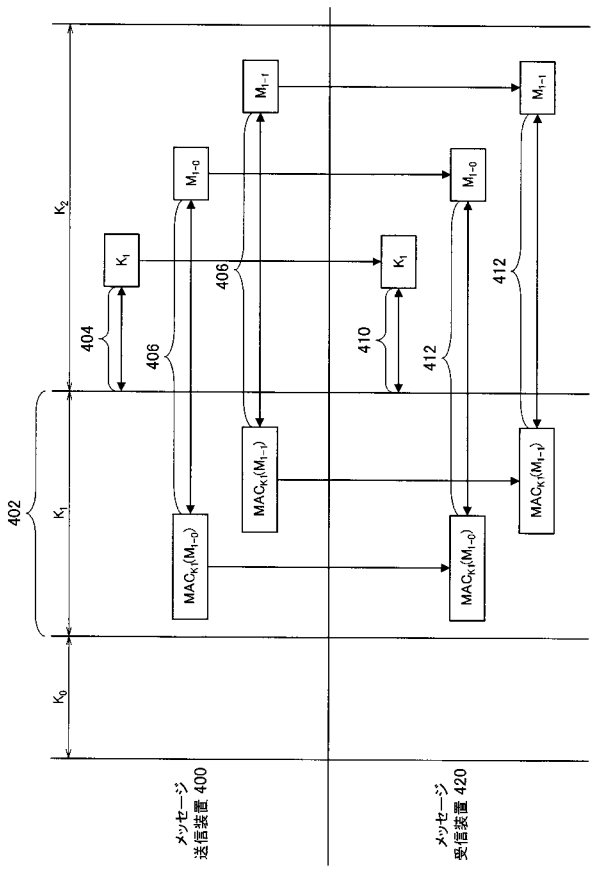
【図８】



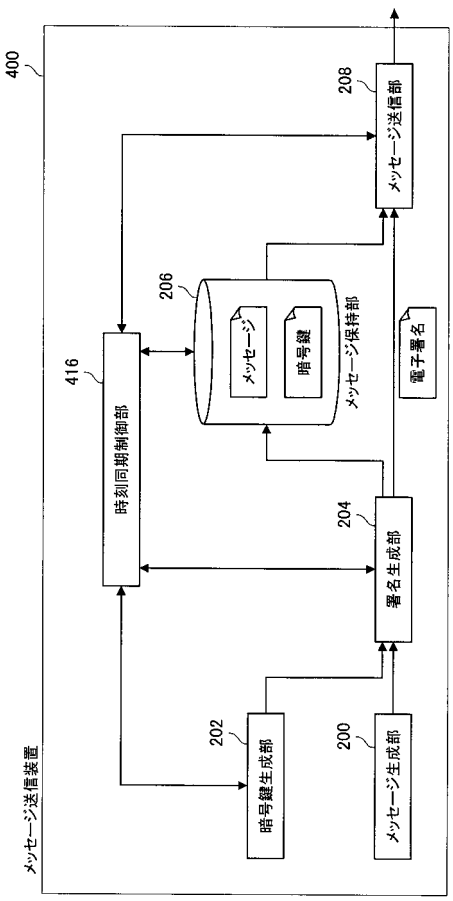
【図９】



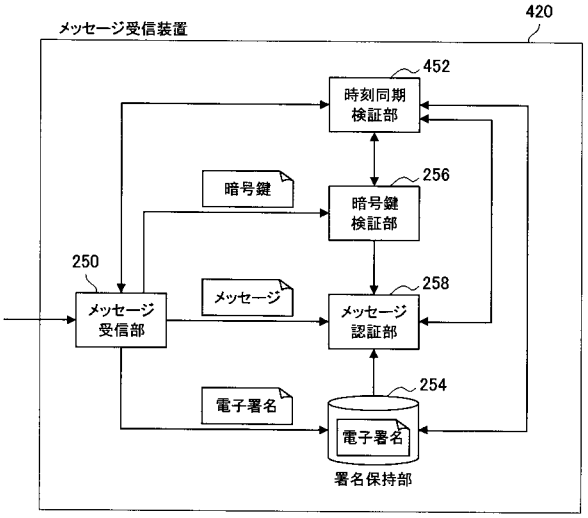
【図１０】



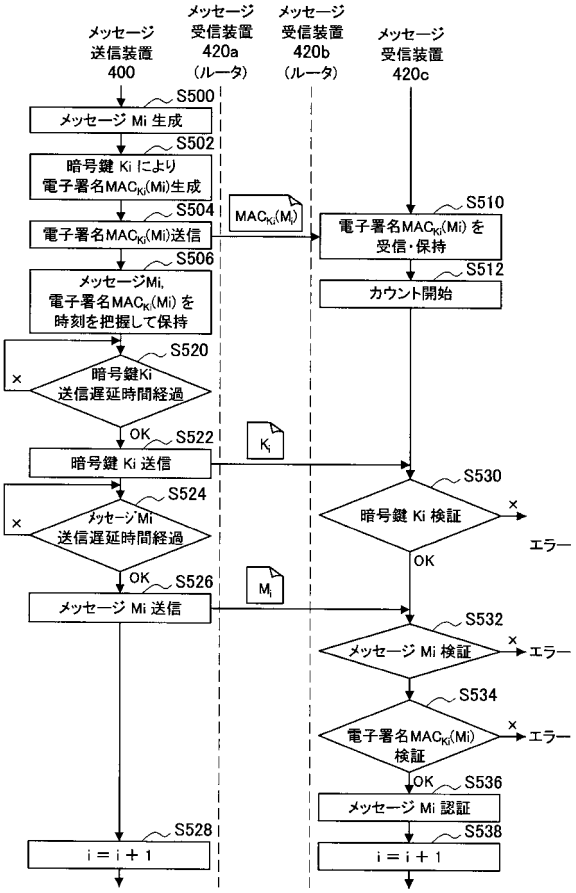
【図１１】



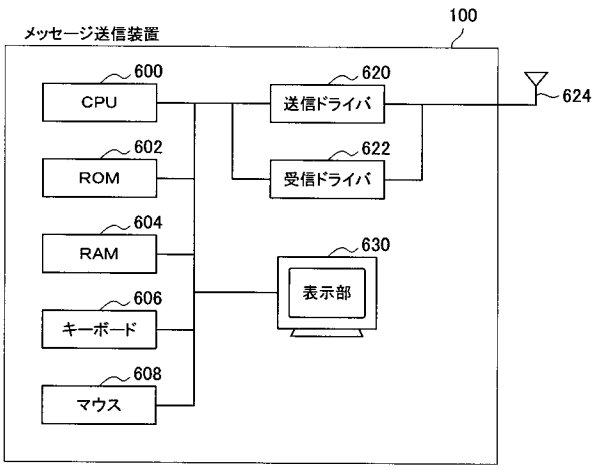
【図１２】



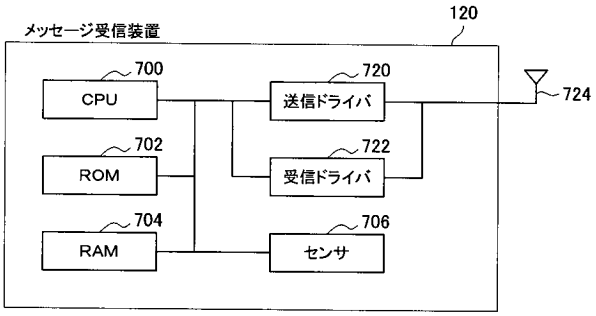
【図１３】



【図１４】



【図１５】



フロントページの続き

(56)参考文献 特開平１０－０６９２２２（ＪＰ，Ａ）
特開２００３－２２４５６０（ＪＰ，Ａ）
特開２００４－２４８２７０（ＪＰ，Ａ）

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