(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2007 年9 月13 日 (13.09.2007)

PCT

(10) 国際公開番号
WO 2007/102422 A1

(51) 国際特許分類:
H04L 9/32 (2006.01) *H04L 9/08* (2006.01)

(21) 国際出願番号: PCT/JP2007/054017

(22) 国際出願日: 2007 年3 月2 日 (02.03.2007)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2006-059493 2006 年3 月6 日 (06.03.2006) JP

(71) 出願人 (米国を除く全ての指定国について): 日本電気株式会社 (NEC CORPORATION) [JP/JP]; 〒1080014 東京都港区芝五丁目７番１号 Tokyo (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 門田 啓 (MONDEN, Akira) [JP/JP]; 〒1080014 東京都港区芝五丁目７番１号 日本電気株式会社内 Tokyo (JP).

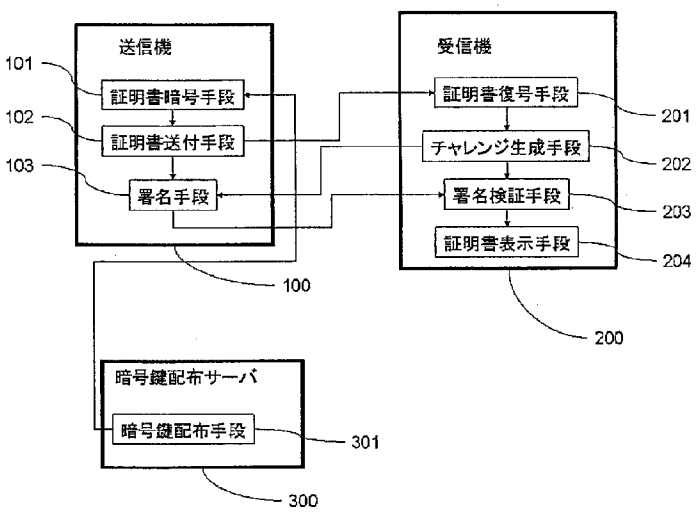
(74) 代理人: 山下 穣平 (YAMASHITA, Johei); 〒1050001 東京都港区虎ノ門五丁目１３番１号虎ノ門４０ＭＴビル 山下国際特許事務所 Tokyo (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL,

[続葉有]

(54) Title: SENDER CONFIRMING SYSTEM, SENDER CONFIRMING METHOD AND SENDER CONFIRMING PROGRAM

(54) 発明の名称: 発信者確認システム、発信者確認方法および発信者確認用プログラム



100 TRANSMITTER
101 CERTIFICATE ENCRYPTING MEANS
102 CERTIFICATE SENDING MEANS
103 SIGNING MEANS
200 RECEIVER
201 CERTIFICATE DECODING MEANS
202 CHALLENGE GENERATING MEANS
203 SIGNATURE VERIFYING MEANS
204 CERTIFICATE DISPLAYING MEANS
300 ENCRYPTION KEY DISTRIBUTION SERVER
301 ENCRYPTION KEY DISTRIBUTION MEANS

(57) **Abstract:** A receiver confirms a sender without using a sender's telephone. A sender confirming system is comprised of a transmitter for an outgoing call, a receiver for receiving the outgoing call, and an encryption key distribution server connected to communicate with the transmitter. The encryption key distribution server has an encryption key distribution means for distributing a public key of the receiver. The transmitter is comprised of a certificate encryption means for encrypting a sender certificate, a certificate sending means for sending the sender certificate, and a signing means for encrypting and signing a challenge. The receiver is provided with a decoding means for decoding the sender certificate, a challenge generating means for generating the challenge, a signature verifying means for verifying a signature, and a certificate display means for displaying the sender certificate. Because of transmitting the sender certificate stored in the transmitter and the signature using the encryption key of the transmitter to the receiver, the sender can be confirmed by the receiver.

(57) 要約: 発信者電話を用いずに受信者が発信者の確認を行う。本発明の発信者確認システムは、発信を行う送信機と、その発信を受ける受信機と、前記送信機に通信可能に接続された暗号鍵配布サーバとを備える。前記暗号鍵配布サーバは、前記受信機の公開鍵を配布する暗号鍵配布手段を有する。前記送信機は、発信者証明書を暗

[続葉有]

WO 2007/102422 A1

SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

号化する証明書暗号手段と、前記発信者証明書を送付する証明書送付手段と、チャレンジに暗号化し署名を行なう署名手段とを有する。前記受信機は、前記発信者証明書を復号化する証明書復号手段と、前記チャレンジを生成するチャレンジ生成手段と、前記署名を検証する署名検証手段と、前記発信者証明書を表示する証明書表示手段とを有する。前記送信機に内蔵された発信者証明書と、前記送信機の暗号鍵を用いた前記署名を前記受信機へ送信することにより、前記受信機で発信者を確認できるようにする。

明 細 書

発信者確認システム、発信者確認方法および発信者確認用プログラム

技術分野

[0001] 本発明は、発信者確認システム、発信者確認方法および発信者確認用プログラムに関し、特に携帯電話の発信者を証明する証明書を用いて、受信者は発信者が誰なのかを確認することができる発信者確認システム、発信者確認方法および発信者確認用プログラムに関する。

背景技術

[0002] 一般に、電話においては、発信者の確認を発信者の電話番号を元に行われる。受信者は、電話に出る前に、電話機のディスプレイ等に表示された電話番号を見て、発信者が誰かを確認することができる。電話機内に電話番号と発信者の名前を関連付けた電話帳を内蔵することで、電話番号を発信者の名前に変換し、発信者の名前を表示することができ、受信者の利便性を高めることもできる。

[0003] この方法において受信者が発信者を確認するためには、かかってくる電話番号が誰のものなのか記憶しておくか、予め電話機内蔵の電話帳へ登録しておく必要がある。つまり、知らない電話番号から着信があった場合には、発信者が誰であるのかがわからないという問題がある。

[0004] 携帯電話の場合なら、発信者が携帯電話機を買い換えた場合や、固定電話の場合なら、発信者が引っ越した場合には、発信者の電話番号が変わってしまうため、この電話番号を元に発信者を特定する方法では、発信者を特定することができないという問題もある。

[0005] また、警察や消防署等の公共機関、宅配便等の訪問サービス業を名乗って電話がかかってきた場合には、それらの電話番号を記憶もしくは記録しておかない限り、本物の公共機関や訪問サービス業の人からの電話なのか、それらになりすましている人からの電話なのかわからないという問題もある。

[0006] これら問題を解決する方法が特許文献1に記載されている。

[0007] 特許文献1記載の個人情報管理システムは、発信者が電話をかける際に、個人情

報管理システムへアクセスするためのパスワードを受信者へ送信する。受信者は発信者の電話番号を元にして個人情報管理システムを検索し、パスワードによって管理された個人情報管理システムから、発信者から送付されたパスワードによって発信者の個人情報を取り出す。

[0008] 特許文献1記載の個人情報管理システムでは、発信者が自分の個人情報を開示してもよいと考える相手に対してだけパスワードを送信することで、発信者の個人情報を開示する範囲を発信者が特定できるようにしている。

特許文献1:特開2005－51475号公報

発明の開示

発明が解決しようとする課題

[0009] 第1の問題点は、発信者の個人情報がパスワードのみで保護されているにすぎないので、発信者が自分の個人情報を開示する範囲を、自分で完全にコントロールはできないことである。

[0010] 発信者の個人情報と、電話番号、パスワードは完全に対応しており、ある発信者のパスワードは、すべての受信者に対して同じとなっている。そのため、受信者のうちの誰かがパスワードを第三者に教えると、発信者の指定した人以外からも発信者の個人情報を参照することが可能となる。

[0011] また、パスワードは各発信者が定めるものであり、パスワードが推測される可能性もある。個人情報サーバへは誰でもアクセスできるため、あてずっぽうでパスワードを当てる可能性もある。

[0012] 第2の問題点は、発信者を詐称される可能性があることである。

[0013] 電話番号は高々数桁の数字であり、電話番号を詐称されるという可能性がある。電話番号の詐称が可能な場合、発信者Aのパスワードを、発信者Aから直接聞く、正規受信者として送付される正規受信者からの漏洩、推測等であてるなどで、発信者A以外が知れば、発信者Aの番号に、電話番号を詐称し、発信者Aのパスワードを送付することにより、発信者A以外の人が発信者Aになりすまして電話をかけることができる。受信者は、発信者Aの電話番号で個人情報管理サーバを検索し、発信者Aのパスワードでアクセスするため、発信者Aの個人情報を閲覧することができる。そのため

、発信者A以外からの電話を発信者を発信者Aだと思い込むことになる。

[0014] 第3の問題点は、個人情報は発信者電話番号で検索するため、電話番号を通知することなく、発信者が誰なのか受信者に伝えることができないことである。

[0015] 発信者は、発信者電話番号を用いて個人情報管理サーバを検索するため、電話番号が非通知では発信者の個人情報を得ることができない。電話番号が非通知の場合、個人情報を得ることもできず、発信者の電話番号もわからないため、受信者は、電話に出る前に、誰からの電話であるのか知るすべがない。

[0016] しかしながら、発信者は、受信者に自分の電話番号を教えたくはないが、自分が誰なのかは通知したい場合もある。この場合には特許文献1の方法では対応できない。

[0017] 本発明は以上の点を考慮してなされたもので、本発明の第1の目的は、発信者が開示したい相手以外には、発信者の個人情報が伝わらない発信者確認システムを提供することにある。

[0018] また本発明の第2の目的は、発信者を詐称されることのない発信者確認システムを提供することにある。

[0019] そして本発明の第3の目的は、発信者の電話番号を受信者に教えることなく、受信者に発信者が誰であるのかを伝えることのできる発信者確認システムを提供することにある。

課題を解決するための手段

[0020] 本発明による発信者確認システムは、発信を行う送信機と、その発信を受ける受信機とを備え、前記送信機は、前記受信機から送付されたチャレンジを、前記送信機の秘密鍵を用いて暗号化することで署名を行い、前記受信機へ前記署名を送付する署名手段を有し、前記受信機は、前記送信機に署名させるための前記チャレンジを生成して、前記送信機に送付するチャレンジ生成手段と、前記送信機から送信された前記署名を、前記送信機の秘密鍵に対応した暗号鍵を用いて復号化し、復号化されたデータが、前記チャレンジ生成手段により生成された前記チャレンジと一致している場合に、前記署名が正しいと判断し、発信者証明書を表示する証明書表示手段と、を備えることを特徴とする。

[0021] 前記発信者証明書を、各通話毎に毎回発信機から受信者へ送付するようにしても

よい。

[0022] また、前記発信者証明書を、予め、発信機から受信機へ送付するようにしてもよい。その場合、通話で利用するネットワークと同一のネットワークを利用して発信者証明書を送付してもよい。また、その場合、通話で利用するネットワークと別のネットワーク(例えば、データ通信用のネットワーク)を利用して発信者証明書を送付してもよい。更に、送信機と受信機との間の近接通信や直接接続を利用することにより、発信者と受信者とが直接会った場合に、発信者証明書を送付するようにしてもよい。

[0023] また、警察などの公共機関を受信機に予め登録しておくようにしておくこともできる。

[0024] 発信者証明書をネットワークを介して送付する場合、受信機のみが発信者情報を読めるように、受信機の秘密鍵に対応する暗号鍵で発信者証明書を暗号化して送付するようにしてもよい。その場合、受信機の秘密鍵に対応する暗号鍵を、予め受信機から送信機に送付しておくようにしてもよい。

[0025] また、本発明の発信者確認システムに、送信機に通信可能に接続された暗号鍵配布サーバを備えさせ、暗号鍵配布サーバが、送信機の送信先となる受信機の秘密鍵に対応する暗号鍵を送信機に送付する暗号鍵配布手段を備えるようにしてもよい。送信機は、暗号鍵配布サーバから取得した暗号鍵を用いて送信機の発信者証明書を暗号化するようにしてもよい。

[0026] 暗号化の方式として、公開鍵暗号方式を用いて、受信機の暗号鍵として、公開鍵暗号方式の秘密鍵を利用し、送信機の暗号鍵として公開鍵暗号方式の公開鍵を利用してもよい。以下では、公開鍵とは、秘密鍵に対応した暗号鍵を意味し、実際に公開されているか否かは問われない。

[0027] 本発明の発信者確認システムは、発信を行う送信機と、その発信を受ける受信機と、前記送信機に通信可能に接続された暗号鍵配布サーバとを備え、前記暗号鍵配布サーバは、前記送信機の発信先となる前記受信機の公開鍵を前記送信機に配布する暗号鍵配布手段を有し、前記送信機は、前記暗号鍵配布サーバから取得した前記受信機の公開鍵を用いて前記送信機の公開鍵を含む発信者証明書を暗号化する証明書暗号手段と、暗号化された前記発信者証明書を前記受信機へ送付する証明書送付手段と、前記受信機から送付されたチャレンジを、前記送信機の秘密鍵

を用いて復号化し、復号化された前記チャレンジに対して、前記送信機の秘密鍵を用いて暗号化することで署名を行ない、前記受信機へ前記署名を送付する署名手段とを有し、前記受信機は、暗号化された前記送信機の発信者証明書を、当該受信機の秘密鍵を用いて復号化する証明書復号手段と、前記送信機に前記署名させるための前記チャレンジを生成して、前記発信者証明書から取得した前記送信機の公開鍵を用いて当該チャレンジを暗号化して当該送信機に送付するチャレンジ生成手段と、前記送信機から送付された前記署名を、前記送信機の公開鍵を用いて復号化し、復号化されたデータが前記チャレンジ生成手段により生成された前記チャレンジと一致しているか否かを検証する署名検証手段と、前記復号化されたデータが前記チャレンジと一致している場合に、前記署名が正しいと検証して、前記発信者証明書を表示する証明書表示手段とを有することを特徴とする。

[0028] また、本発明の発信者確認システムは、前記送信機が、前記発信者証明書を前記受信機へ通知するか否かを選択する手段をさらに備えるようにしても良い。

[0029] また、本発明の発信者確認システムは、前記受信機が、前記送信機から前記発信者証明書の通知がない場合に、前記送信機へ前記発信者証明書を通知するように要求する手段をさらに備えるようにしても良い。

[0030] 本発明による発信者確認システムは、発信を行う送信機と、その発信を受ける受信機と、中継器と、を備え、前記送信機は、前記送信機の利用者を示す発信者証明書を前記中継器に送信し、前記中継器は、前記発信機からの通信に応じてチャレンジを前記送信機に送信し、前記送信機は、前記中継器から受信したチャレンジに発信者の秘密鍵で署名を付し、署名されたチャレンジを中継器に送信し、前記中継器は、前記発信者証明書、署名前のチャレンジ及び署名されたチャレンジを前記受信機に送信し、前記受信機は、前記中継器から受信した前記署名を前記発信者証明書に記載された発信者の暗号鍵を用いて確認できた場合に前記発信者証明書に記載された発信者の情報を表示部に表示すること特徴とする。

[0031] 本発明の発信者確認システムは、発信を行う送信機と、その発信を受ける受信機と、前記送信機に通信可能に接続された暗号鍵配布サーバと、前記送信機と前記受信機との間に通信可能に接続された中継器とを備え、前記暗号鍵配布サーバは、前

記送信機が要求する前記受信機の公開鍵を配布する暗号鍵配布手段を有し、前記送信機は、前記暗号鍵配布サーバから取得した前記受信機の公開鍵を用いて前記送信機の公開鍵を含む発信者証明書を暗号化する証明書暗号手段と、暗号化された前記発信者証明書を前記中継器へ送付する証明書送付手段と、前記中継器から送付されたチャレンジを、前記送信機の秘密鍵を用いて復号化し、当該復号化された前記チャレンジに対して、前記送信機の秘密鍵を用いて暗号化することで署名を行ない、前記中継器へ前記署名を送付する署名手段とを有し、前記中継器は、前記送信機に前記署名させるための前記チャレンジを生成して、前記発信者証明書から取得した前記送信機の公開鍵を用いて当該チャレンジを暗号化して当該送信機に送付するチャレンジ生成手段と、前記送信機から取得した前記署名と前記暗号化された前記発信者証明書と前記チャレンジ生成手段で生成された前記チャレンジとを前記受信機へ送付する中継手段とを有し、前記受信機は、前記中継器から送付された前記暗号化された前記送信機の前記発信者証明書を、当該受信機の秘密鍵を用いて復号化する証明書復号手段と、前記中継器から送付された前記署名を、前記送信機の公開鍵を用いて復号化し、復号化されたデータが前記チャレンジ生成手段により生成された前記チャレンジと一致しているか否かを検証する署名検証手段と、前記復号化されたデータが前記チャレンジと一致している場合に、前記署名が正しいと検証して、前記発信者証明書を表示する証明書表示手段と、受信できなかった着信記録を、当該受信機が受信できるようになった後に、前記中継器を介して受信する手段とを有することを特徴とする。

[0032] また、本発明の発信者確認システムは、前記送信機は、生体認証手段と、前記受信機へ前記発信者証明書、又は前記署名を送付する場合に、前記生体認証手段による生体認証結果も通知する手段とをさらに備え、前記受信機は、前記生体認証結果に基づいて前記送信機の持ち主とユーザを確認する手段をさらに備えるようにしても良い。

[0033] また、本発明の発信者確認システムは、前記送信機は、前記生体認証手段に生体情報が入力されることにより前記発信者証明書の通知を行うか否かを選択する手段をさらに備えるようにしても良い。

[0034] また、本発明の発信者確認システムは、前記送信機及び前記受信機が携帯電話によって構成されるようにしても良い。

[0035] 本発明の暗号鍵配布サーバは、受信機の公開鍵をその電話番号に対応付けて保持する手段と、送信機の発信先となる前記受信機の公開鍵をその電話番号に基づいて検索する手段と、検索された前記受信機の公開鍵を前記送信機へ配布する暗号鍵配布手段を備えたことを特徴とする。

[0036] 本発明による送信機は、当該送信機の利用者を示す発信者証明書を受信機に送信する手段と、チャレンジを前記送信機から受信する手段と、前記受信機から受信した前記チャレンジに発信者の秘密鍵で署名を付し、署名されたチャレンジを受信機に送信する手段と、を備えることを特徴とする。

[0037] 本発明の送信機は、暗号鍵配布サーバから取得した受信機の公開鍵を用いて送信機の公開鍵を含む発信者証明書を暗号化する証明書暗号手段と、暗号化された前記発信者証明書を前記受信機へ送付する証明書送付手段と、前記受信機から送付されたチャレンジを、前記送信機の秘密鍵を用いて復号化し、当該復号化された前記チャレンジに対して、前記送信機の秘密鍵を用いて暗号化することで署名を行ない、前記受信機へ前記署名を送付する署名手段とを有し、前記発信者証明書を前記受信機へ通知するか否かを選択する手段をさらに備えたことを特徴とする。

[0038] 本発明による受信機は、送信機から、前記送信機の利用者を示す発信者証明書を受信する手段と、前記発信機からの通信に応じてチャレンジを前記送信機に送信する手段と、前記送信機において発信者の秘密鍵で署名されたチャレンジを受信する手段と、前記送信機から受信した前記署名を前記発信者証明書に記載された発信者の暗号鍵を用いて確認できた場合に前記発信者証明書に記載された発信者の情報を表示部に表示する手段と、を備えること特徴とする。

[0039] 本発明の受信機は、暗号化された送信機の発信者証明書を、受信機の秘密鍵を用いて復号化する証明書復号手段と、前記送信機に署名させるためのチャレンジを生成して、前記発信者証明書から取得した前記送信機の公開鍵を用いて当該チャレンジを暗号化して当該送信機に送付するチャレンジ生成手段と、前記送信機から送付された前記署名を、前記送信機の公開鍵を用いて復号化し、復号化されたデー

タが前記チャレンジ生成手段により生成された前記チャレンジと一致しているか否かを検証する署名検証手段と、前記復号化したデータが前記チャレンジと一致している場合に、前記署名が正しいと検証して、前記発信者証明書を表示する証明書表示手段とを有し、前記送信機から前記発信者証明書の通知がない場合に、前記送信機へ前記発信者証明書を通知するように要求する手段をさらに備えたことを特徴とする。

[0040] 本発明による発信者確認方法は、発信を行う送信機と、その発信を受ける受信機と、を備えるシステムにおける発信者確認方法において、前記送信機は、前記送信機の利用者を示す発信者証明書を前記受信機に送信し、前記受信機は、前記発信機からの通信に応じてチャレンジを前記送信機に送信し、前記送信機は、前記受信機から受信した前記チャレンジに発信者の秘密鍵で署名を付し、署名されたチャレンジを受信機に送信し、前記受信機は、前記送信機から受信した前記署名を前記発信者証明書に記載された発信者の暗号鍵を用いて確認できた場合に前記発信者証明書に記載された発信者の情報を表示部に表示すること特徴とする。

[0041] 本発明の発信者確認方法は、発信を行う送信機と、その発信を受ける受信機と、前記送信機に通信可能に接続された暗号鍵配布サーバとを備える発信者確認システムの発信者確認方法であって、前記暗号鍵配布サーバが、前記送信機の発信先となる前記受信機の公開鍵を前記送信機へ配布し、前記送信機が、前記暗号鍵配布サーバから取得した前記受信機の公開鍵を用いて前記送信機の公開鍵を含む前記発信者証明書を暗号化し、前記送信機が、暗号化された前記発信者証明書を前記受信機へ送付し、前記受信機が、暗号化された前記送信機の発信者証明書を当該受信機の秘密鍵を用いて復号化し、前記受信機が、前記送信機に署名させるためのチャレンジを生成して、前記送信機の公開鍵で暗号化して前記送信機に送付し、前記送信機が、前記受信機から送付された前記チャレンジを、前記送信機の秘密鍵を用いて復号化し、当該復号化された前記チャレンジに対して、前記送信機の秘密鍵を用いて暗号化することで署名し、前記受信機へ前記署名を送付し、前記受信機が、前記送信機から送付された前記署名を、前記送信機の公開鍵を用いて復号化し、復号化されたデータが、生成された前記チャレンジと一致しているか否かを検証し

、前記受信機が、前記復号化されたデータが前記チャレンジと一致している場合に、前記署名が正しいと検証して、前記発信者証明書を表示することを特徴とする。

[0042] 本発明による送信方法は、当該送信機の利用者を示す発信者証明書を受信機に送信し、チャレンジを前記送信機から受信し、前記受信機から受信した前記チャレンジに発信者の秘密鍵で署名を付し、署名されたチャレンジを受信機に送信することを特徴とする。

[0043] 本発明の送信方法は、暗号鍵配布サーバから取得した受信機の公開鍵を用いて送信機の公開鍵を含む前記発信者証明書を暗号化し、前記暗号化された前記発信者証明書を前記受信機へ送付し、前記受信機から送付されたチャレンジを、前記送信機の秘密鍵を用いて復号化し、当該復号化された前記チャレンジに対して、前記送信機の秘密鍵を用いて暗号化することで署名し、前記受信機へ前記署名を送付することを特徴とする。

[0044] 本発明による受信方法は、送信機から、前記送信機の利用者を示す発信者証明書を受信し、前記発信機からの通信に応じてチャレンジを前記送信機に送信し、前記送信機において発信者の秘密鍵で署名されたチャレンジを受信し、前記送信機から受信した前記署名を前記発信者証明書に記載された信者の暗号鍵を用いて確認できた場合に前記発信者証明書に記載された発信者の情報を表示部に表示すること特徴とする。

[0045] 本発明の受信方法は、暗号化された送信機の発信者証明書を受信機の秘密鍵を用いて復号化し、前記送信機に署名させるためのチャレンジを生成して、前記送信機の公開鍵で暗号化して前記送信機に送付し、前記送信機から送付された前記署名を、前記送信機の公開鍵を用いて復号化し、復号化されたデータが、生成された前記チャレンジと一致しているか否かを検証し、前記復号化されたデータが前記チャレンジと一致している場合に、前記署名が正しいと検証し、前記発信者証明書を表示することを特徴とする。

[0046] 本発明の暗号鍵配布方法は、送信機から要求のあった受信機の公開鍵を前記送信機へ配布することを特徴とする。

[0047] 本発明による送信プログラムは、当該送信機の利用者を示す発信者証明書を受信

機に送信する手順と、チャレンジを前記送信機から受信する手順と、前記受信機から受信した前記チャレンジに発信者の秘密鍵で署名を付し、署名されたチャレンジを受信機に送信する手順と、をコンピュータに実行させることを特徴とする。

[0048] 本発明の送信プログラムは、暗号鍵配布サーバから取得した受信機の公開鍵を用いて送信機の公開鍵を含む発信者証明書を暗号化する手順と、前記暗号化された前記発信者証明書を前記受信機へ送付する手順と、前記受信機から送付されたチャレンジを、前記送信機の秘密鍵を用いて復号化し、当該復号化された前記チャレンジに対して、前記送信機の秘密鍵を用いて暗号化することで署名し、前記受信機へ前記署名を送付する手順とをコンピュータに実行させることを特徴とする。

[0049] 本発明による受信プログラムは、送信機から、前記送信機の利用者を示す発信者証明書を受信する手順と、前記発信機からの通信に応じてチャレンジを前記送信機に送信する手順と、前記送信機において発信者の秘密鍵で署名されたチャレンジを受信する手順と、前記送信機から受信した前記署名を前記発信者証明書に記載された信者の暗号鍵を用いて確認できた場合に前記発信者証明書に記載された発信者の情報を表示部に表示する手順と、をコンピュータに実行させること特徴とする。

[0050] 本発明の受信プログラムは、暗号化された送信機の発信者証明書を受信機の秘密鍵を用いて復号化する手順と、前記送信機に署名させるためのチャレンジを生成して、前記送信機の公開鍵で暗号化して前記送信機に送付する手順と、前記送信機から送付された署名を、前記送信機の公開鍵を用いて復号化し、複合化されたデータが、生成された前記チャレンジと一致しているか否かを検証する手順と、前記復号化されたデータが前記チャレンジと一致している場合に、前記署名が正しいと検証して、前記発信者証明書を表示する手順とをコンピュータに実行させることを特徴とする。

[0051] 本発明の暗号鍵配布プログラムは、送信機から要求のあった受信機の公開鍵を前記送信機へ配布することを特徴とする。

[0052] 本発明による中継器は、本発明による中継器は、発信を行う送信機と、その発信を受ける受信機と、中継器と、を備えるシステムにおける中継器において、前記送信機から、前記送信機の利用者を示す発信者証明書を受信する手段と、前記発信機から

の通信に応じてチャレンジを前記送信機に送信する手段と、前記送信機において、当該中継器から受信したチャレンジに発信者の秘密鍵で署名されたチャレンジを、前記送信機から受信する手段と、前記発信者証明書、署名前のチャレンジ及び署名されたチャレンジを前記受信機に送信する手段と、を備えることを特徴とする。

[0053] 本発明の中継器は、送信機に署名させるためのチャレンジを生成して、発信者証明書から取得した前記送信機の公開鍵を用いて当該チャレンジを暗号化して当該送信機に送付するチャレンジ生成手段と、前記送信機から取得した前記署名と暗号化された前記発信者証明書と前記チャレンジ生成手段で生成された前記チャレンジとを前記受信機へ送付する中継手段とを備えたことを特徴とする。

[0054] 本発明による中継方法は、発信を行う送信機と、その発信を受ける受信機と、中継器と、を備えるシステムにおける中継方法において、前記送信機から、前記送信機の利用者を示す発信者証明書を受信し、前記発信機からの通信に応じてチャレンジを前記送信機に送信し、前記送信機において、当該中継器から受信したチャレンジに発信者の秘密鍵で署名されたチャレンジを、前記送信機から受信し、前記発信者証明書、署名前のチャレンジ及び署名されたチャレンジを前記受信機に送信することを特徴とする。

[0055] 本発明の中継方法は、送信機に署名させるためのチャレンジを生成して、発信者証明書から取得した前記送信機の公開鍵を用いて当該チャレンジを暗号化して当該送信機に送付し、前記送信機から取得した前記署名と暗号化された前記発信者証明書と生成された前記チャレンジとを前記受信機へ送付することを特徴とする。

[0056] 本発明による中継プログラムは、発信を行う送信機と、その発信を受ける受信機と、中継器と、を備えるシステムにおける中継方法をコンピュータに行わせるための中継プログラムにおいて、前記送信機から、前記送信機の利用者を示す発信者証明書を受信する手順と、前記発信機からの通信に応じてチャレンジを前記送信機に送信する手順と、前記送信機において、当該中継器から受信したチャレンジに発信者の秘密鍵で署名されたチャレンジを、前記送信機から受信する手順と、前記発信者証明書、署名前のチャレンジ及び署名されたチャレンジを前記受信機に送信する手順と、をコンピュータに行わせることを特徴とする。

[0057] 本発明の中継プログラムは、送信機に署名させるためのチャレンジを生成して、発信者証明書から取得した前記送信機の公開鍵を用いて当該チャレンジを暗号化して当該送信機に送付する手順と、前記送信機から取得した前記署名と暗号化された前記発信者証明書と生成された前記チャレンジとを前記受信機へ送付する手順とをコンピュータに実行させることを特徴とする。

発明の効果

[0058] 本発明による発信者確認システムは、発信を行う送信機と、その発信を受ける受信機とを備え、前記送信機は、前記受信機から送付されたチャレンジを、前記送信機の秘密鍵を用いて暗号化することで署名を行い、前記受信機へ前記署名を送付する署名手段を有し、前記受信機は、前記送信機に署名させるための前記チャレンジを生成して、前記送信機に送付するチャレンジ生成手段と、前記送信機から送信された前記署名を、前記送信機の秘密鍵に対応した暗号鍵を用いて復号化し、復号化されたデータが、前記チャレンジ生成手段により生成された前記チャレンジと一致している場合に、前記署名が正しいと判断し、発信者証明書を表示する証明書表示手段と、を備えることを特徴とするので、、本発明の第1の目的を達成することができる。

[0059] 更に、受信機で発信者の署名を確認しているため、発信者の暗号鍵(秘密鍵)がなければ発信者を詐称することはできず、本発明の第2の目的を達成することができる。

[0060] 更に、本発明では、発信者の電話番号と切り離した、発信者証明書と発信者の署名を用いて発信者を通知しているため、受信者に電話番号を通知することなく、発信者を通知することができる。発信者の通知に発信者の電話番号を必要としないため、本発明の第3の目的を達成することができる。

[0061] 本発明によれば、発信者証明書は、受信者の暗号鍵(公開鍵)で暗号化されており、発信者が受信者の受信機へ発信者証明書を送付するようになっているので、その発信者証明書は、発信者が指定した受信者のみ読むことができる。

[0062] また、本発明によれば、受信機で発信者の署名を確認しており、発信者の署名は、送信機の暗号鍵(秘密鍵)がなければ復号できないので、発信者を詐称することを防ぐことができる。

[0063] 更に、本発明によれば、発信者の電話番号は利用せずに、発信者の発信者証明書と発信者の署名により発信者を通知しているため、発信者の電話番号を通知することなく、受信者に発信者の情報を使えることができる。

図面の簡単な説明

[0064] [図1]本発明の第1の実施の形態を実施するための構成を示すブロック図である。

[図2]本発明の第1の実施の形態を実施するための動作を示すフローチャートである。

[図3]本発明の第2の実施の形態を実施するための構成を示すブロック図である。

[図4]本発明の第2の実施の形態を実施するための動作を示すフローチャートである。

[図5]本発明の第3の実施の形態を実施するための構成を示すブロック図である。

[図6]本発明の第3の実施の形態を実施するための動作を示すフローチャートである。

[図7]本発明の第1の実施例の動作の一例を示す図である。

[図8]本発明の第1の実施例の動作の一例を示す図である。

[図9]本発明の第2の実施例の動作の一例を示す図である。

[図10]本発明の第2の実施例における不在着信時の表示の一例を示す図である。

[図11]本発明の第3の実施例における発信携帯電話の一例を示す図である。

[図12]本発明の第3の実施例における受信携帯電話の一例を示す図である。

符号の説明

[0065] 100, 110 送信機

101 証明書暗号手段

102 証明書送付手段

103 署名手段

111 生体認証手段

112 署名手段

200, 210, 220 受信機

201, 211 証明書復号手段

202, 212 チャレンジ生成手段

203, 221 署名検証手段

204, 222 証明書表示手段

300 暗号鍵配布サーバ

301 暗号鍵配布手段

400 中継器

401 チャレンジ生成手段

402 中継手段

501, 511 発信者

502, 512, 522 発信携帯電話

503, 513 受信者

504, 514, 524 受信携帯電話

505 公開鍵配布サーバ

506 発信者通知ボタン

507 ディスプレイ

508 発信者通知要求ボタン

515 中継器

516 交換機

520 指紋センサ

発明を実施するための最良の形態

[0066] 以下、本発明を実施するための最良の実施の形態について、図面を参照して詳細に説明する。

[0067] (第1の実施の形態)

[0068] 図1を参照すると、本発明の第1の実施の形態では、送信機(発信機)100と、受信機200と、暗号鍵配布サーバ300とを備えている。

[0069] 送信機100は、証明書暗号手段101と、証明書送付手段102と、署名手段103とを備えている。

[0070] 第1の実施の形態では、送信機100は、概略次のように動作する。

[0071] 証明書暗号手段101は、暗号鍵配布サーバ300を用いて、受信機200の暗号鍵(公開鍵)を取得し、取得した受信機200の暗号鍵(公開鍵)を用いて送信機の発信者証明書を暗号化し、証明書送付手段102へ送信する。

[0072] 証明書送付手段102は、暗号化された発信者証明書を受信機200へ送信する。

[0073] 署名手段103は、受信機200より受信した暗号化されたチャレンジを送信機100の暗号鍵(秘密鍵)を用いて復号し、復号したチャレンジに対して送信機100の暗号鍵(秘密鍵)を用いて署名を行い、署名を受信機200へ送付する。

[0074] ここで署名を行うとは、公開鍵暗号方式の秘密鍵を利用したデータの完全性を保証する仕組みのことであり、データの送信者が保有する秘密鍵でデータのハッシュ値を暗号化し、データに付与することをいう。また、ハッシュ値とは、ハッシュ関数の出力値のことであり、また、ハッシュ関数とは、与えられた入力値から固定長の疑似乱数を生成する演算手法であって、ハッシュ値から逆に入力値が求められない仕組みとなっている。

[0075] 第1の実施の形態では、受信機200は、概略次のように動作する。

[0076] 証明書復号手段201は、送信機100から受信した暗号化された送信機の発信者証明書を受信機200の暗号鍵(秘密鍵)を用いて復号し、送信機100の発信者証明書に含まれる送信機100の暗号鍵(公開鍵)を取り出す。チャレンジ生成手段202では、送信機100の署名を受けるためのチャレンジを生成し、そのチャレンジを送信機100の暗号鍵(公開鍵)で暗号化して、送信機100へ送る。

[0077] ここでチャレンジとは、受信機200が予測不能な乱数を生成し、その乱数を元に生成される小さなデータのことをいう。このデータを生成することを、チャレンジを生成するといい、暗号鍵によってこのチャレンジを暗号化するようになっている。このように、チャレンジは乱数を元にして生成されているので、暗号化することにより毎回違った結果が得られるようになっている。

[0078] 署名検証手段203は、送信機100から送られた送信機100の署名を検証し、送信機100の署名が正しいものかどうかを検証する。署名が正しいと認められた場合、証明書表示手段204で、送信機100の発信者証明書を表示し、受信機の使用者に、発信者(送信機の使用者)が誰であるかを通知する。

[0079] 第1の実施の形態では、暗号鍵配布サーバ300は、概略次のように動作する。

[0080] 暗号鍵配布手段301で、送信機100から要求を受け、受信機200の暗号鍵(公開鍵)を送信機100へ配布する。

[0081] 次に、図1及び図2のフローチャートを参照して第1の実施の形態の全体の動作について詳細に説明する。

[0082] 発信機100の証明書暗号手段101は、発信機100の発信者証明書を暗号化するために、暗号鍵配布サーバに受信機200の暗号鍵(公開鍵)を要求する(図2のステップB1)。

[0083] 暗号鍵配布サーバ300の暗号鍵配布手段301は、発信機100から要求された暗号鍵を検索する(図2のステップA1)。暗号鍵配布手段301は、検索された暗号鍵を発信機100へ配布する(図2のステップA2)。

[0084] 発信機100の証明書暗号手段101は、暗号鍵配布サーバ300から配布された受信機200の暗号鍵(公開鍵)を受け取る(図2のステップB2)。発信機100の発信者証明書を暗号化する(図2のステップB3)。発信機100の証明書暗号手段101は、暗号化された発信者証明書を証明書送付手段102へ送付し、その証明書送付手段102は、暗号化された発信者証明書を受信機200へ送信する(図2のステップB4)。

[0085] 受信機200の証明書復号手段201は、発信機100から受け取った発信者証明書を受信機200の暗号鍵(秘密鍵)で復号する(図2のステップC1)。受信機200の証明書復号手段201は、復号した発信機100の発信者証明書から発信機100の暗号鍵(公開鍵)を取り出す(図2のステップC2)。受信機200のチャレンジ生成手段202は、送信機100に署名をさせるチャレンジを生成し(図2のステップC3)、送信機100の暗号鍵(公開鍵)を用いて暗号化(図2のステップC4)すると共に、その暗号化されたチャレンジを送信機100へ送信する(図2のステップC5)。

[0086] 送信機100の署名手段103は、受信機200から暗号化されたチャレンジを受け取り(図2のステップB5)、受け取った暗号化されたチャレンジを、送信機100の暗号鍵(秘密鍵)を用いて復号する(図2のステップB6)。送信機100の署名手段103は、復号したチャレンジに対し送信機100の暗号鍵(秘密鍵)を用いて署名し(図2のステップB7)、送信機200へ署名を送付する(図2のステップB8)。

[0087] 受信機200の署名検証手段203は、送信機100から送られた署名を検証し、送信機100が発信者証明書に記載されたものであることを確認する(図2のステップC6)。受信機200の証明書表示手段204は、送信機100が正当なものであることが署名検証手段203で確認されれば、発信者証明書の内容を表示する(図2のステップC7)。

[0088] 次に、第1の実施の形態の効果について説明する。

[0089] 本実施の形態では、発信機100から送付される発信者証明書は、受信機200の暗号鍵(公開鍵)で暗号化されており、かつ発信者が指定する受信機200にのみ送付されるようになされているため、発信者が指定した受信機200の利用者しか、発信者証明書を読むことができない。

[0090] また、本実施の形態では、送信機100の署名を用いて送信者を確認するようになされているため、送信機の暗号鍵(秘密鍵)がないかぎり署名を偽造することはできず、発信者を詐称することができない。

[0091] さらに、本実施の形態では、発信者証明書と発信者の署名を用いて、発信者(送信機100)を確認するようになされているため、受信者(受信機200の利用者)に発信者の電話番号を通知することなく、発信者が誰であるか通知することができる。

[0092] (第2の実施の形態)

[0093] 次に、本発明の第2の実施の形態について図3を参照して詳細に説明する。なお、第1の実施の形態と同一の構成、同一の信号には同一の符号を付すものとする。

[0094] 図3に示す第2の実施の形態では、受信機210が、受信機200のチャレンジ生成手段202にかえてチャレンジ検証手段212を備えることと、証明書復号手段211の動作が、受信機200の証明書復号手段201の動作と異なることと、送信機100、受信機210、暗号鍵配布サーバ300に加えて、中継器400が備えられ、送信機100の送信先が受信機200ではなく、中継器400であることが異なっており、このことを特徴とする。

[0095] 中継器400は、チャレンジ生成手段401と中継手段402を備える。チャレンジ生成手段401は、送信機100が署名するチャレンジを生成し、そのチャレンジを暗号化して送信機100の署名手段へ送付する。中継手段402は、送信機100から送付された受信機200の暗号鍵(公開鍵)で暗号化された発信者証明書と、送信機100の署名

と、チャレンジ生成手段401で生成したチャレンジとを受信機210へ送付する。

[0096] 受信機210は、証明書復号手段211で中継器402から送られ、暗号化された発信者証明書を復号し、チャレンジ検証手段212で中継器402の生成したチャレンジであることを確認し、署名検証手段203で、送信機100の署名を確認して、送信機100が正当なものと認められれば、証明書表示手段204で、発信者証明書を表示する。

[0097] 次に、図3及び図4のフローチャートを参照して第2の実施の形態の全体の動作について詳細に説明する。

[0098] 送信機100の動作は、送信先が受信機200ではなく、中継器400であることを除けば、第1の実施の形態の送信機100の動作と同じである。

[0099] 暗号鍵配布サーバ300の動作は、第1の実施の形態の暗号鍵配布サーバ300の動作と同じである。

[0100] 中継器400は、中継手段402で送信機100から暗号化された発信者証明書を受信する(図4のステップD1)。中継器400は、チャレンジを生成し(図4のステップD2)、そのチャレンジを送信機100の暗号鍵(公開鍵)で暗号化する(図4のステップD3)。また中継器400は、暗号化されたチャレンジを送信機100へ送付する(図4のステップD4)。

[0101] 送信機100から見ると、中継器400によって行われる図4のステップD1からステップD4の動作は、第1の実施の形態における受信機200の図2のステップC1からステップC5の動作に相当する。

[0102] 送信機100は、第1の実施の形態における送信機100の図2のステップB5からステップB8の動作を行い、中継器400へ署名を送付する(図4のステップB5からステップB8)。

[0103] 中継器400は、中継手段402で発信機100の送付した署名を受信する(図4のステップD5)。中継手段402は、送信機100から受け取った暗号化された発信者証明書と、送信機100の署名と、チャレンジ生成手段401で生成したチャレンジとを受信機210へ送付する。

[0104] 受信機210は、証明書復号手段211で、受信機210の暗号鍵(秘密鍵)を用いて暗号化された発信者証明書を復号する(図4のステップE1)。また受信機210は、チ

ャレンジ検証手段212で、中継器400から送付されたチャレンジを検証し(図4のステップE2)、署名検証手段203及び証明書表示手段204は、第1の実施の形態の動作と同じ動作を行う。

[0105] 次に、第2の実施の形態の効果について説明する。

[0106] 本実施の形態では、受信機210は、受信動作のみであり、能動的に発信することはないようにされているため、受信機210が受信できない状態であった場合、受信できる状態になった後に、受信できない状態であった間の着信履歴を表示することができる。

[0107] 第1の実施の形態では、受信機200がチャレンジを生成し、送信機100へ送付するため、送信機100と受信機200とが相互に通信できる状態に限り、送信者を特定することができた。

[0108] 従って、第1の実施の形態では、送信機100と受信機200とが相互に通信できない場合は通信できないが、第2の実施の形態では、受信機200が受信できない状態であっても、送信機100は中継器400へ送信を行うことができるので、通信が再開されてから、中継器400が受信機200に着信履歴を通知することができる。

[0109] (第3の実施の形態)

[0110] 次に、本発明の第3の実施の形態について、図5を参照して詳細に説明する。なお、第1の実施の形態、及び第2の実施の形態と同一の構成、同一の信号には同一の符号を付すものとする。

[0111] 図5を参照すると、第3の実施の形態では、送信機110が、第1の実施の形態の送信機100の各手段に加えて、生体認証手段111を備えていることと、送信機110の署名手段112、受信機220の署名検証手段221、証明書表示手段222の動作が異なることを特徴とする。

[0112] 送信機110は、生体認証手段111で生体認証を行い、署名手段112で生体認証結果を含めて署名を行う。

[0113] 受信機220は、署名検証手段221では署名の検証と生体認証結果の検証を行い、証明書表示手段222で、送信機110を示す発信者証明書と、送信機110の利用者が発信者証明書の持ち主か否かを表示する。

[0114] 次に、図5及び図6のフローチャートを参照して本実施の形態の全体の動作について詳細に説明する。

[0115] 送信機110でチャレンジを復号する図6のステップB6までの暗号鍵配布サーバ300と、送信機110と、受信機220の動作は、第1の実施の形態における図2のステップB6までの動作と同じである。

[0116] 次に、送信機110は、生体認証手段111で生体認証を行い、送信機110の利用者が、送信機110の持ち主(発信者証明書のユーザ)か否かを判定する(図6のステップF1)。署名手段112で、生体認証結果を含めて、チャレンジに署名を行い(図6のステップF2)、受信機220へ署名を送付する(図6のステップB8)。

[0117] 受信機220は、署名検証手段221で、生体認証結果から送信機110の利用者が発信者証明書記載の人物か否かを確認し(図6のステップG1)、図2のステップ6同様に署名を検証する(図6のステップ6)。証明書表示手段222で、発信者証明書と、送信機の利用者が発信者証明書記載の人物か否かを表示する(図6のステップG2)。

[0118] 次に、第3の実施の形態の効果について説明する。

[0119] 本実施の形態では、生体認証により、送信機110の利用者を確認するよう構成されているため、発信者証明書に記載の人物が送信機110を利用しているか否かを受信者513が確認できる。

[0120] 発信者証明書だけでは、受信者513が確認できるのが、どの送信機110から発信されたかのみであり、送信機110の貸し借り、紛失、盗難等により、送信機110の持ち主以外の人物が送信機110を利用している可能性がある。本実施の形態によれば、発信者501が送信機110の持ち主である場合に、受信者503が発信者501を確認することができる。

[0121] 第3の実施の形態は、第1の実施の形態に生体認証を追加する形で記載したが、第2の実施の形態にも、同様に追加することができる。

実施例 1

[0122] 次に、第1の実施例について、図7を用いて具体的な動作を説明する。

[0123] 図7では、送信機100及び受信機200として携帯電話(図7の送信携帯電話502、

受信携帯電話504)を用いることとする。送信機100及び受信機200は、携帯電話以外に固定電話やトランシバーなどの通話装置を用いることができ、ハンドセットマイク等の通話装置を付けたパーソナルコンピュータなどを用いることもできる。また、本実施の形態では、送信機、受信機間の通信は音声通信であり、音声通信開始前の発信者確認を行うこととするが、通信は、音声通信以外に電子メール等の通信を行う場合にも適用可能である。

[0124] 暗号鍵配布サーバ300として、公開鍵配布サーバ505があり、この公開鍵配布サーバ505は、電話番号を鍵として検索することができ、電話番号に対応した受信携帯電話の暗号鍵(公開鍵)を配布する。また、この公開鍵配布サーバ505は、送信携帯電話502からアクセスすることができる。ここでは、公開鍵配布サーバ505は、電話番号で検索することとしたが、受信携帯電話IDなど、受信携帯電話504を特定できるので、発信者501(発信携帯電話502)が利用できるものであれば利用できる。音声通信でなく電子メールに応用する場合は、電子メールアドレスを用いて検索することができる。

[0125] まず、発信者501は、送信携帯電話502を用いて受信者503の持つ受信携帯電話504へ電話をかける。

[0126] 発信者501は、誰に電話をかける場合でも、相手に自分が発信者であることを伝えたいわけではない。このため、送信携帯電話502には、発信者証明書を通知するかどうかを発信者501が選択できる手段を備えるようにしても良い。

[0127] 第1の実施例では、送信携帯電話502は発信者通知ボタン506を備えており、発信者501は、相手に発信者証明書を通知したい場合には、発信者通知ボタン506を押すこととする。

[0128] 発信者501は、発信者通知ボタン506を押した後、受信携帯電話504の電話番号を入力して電話をかける。発信者通知ボタン506が押されているので、発信携帯電話502は、公開鍵配布サーバ505にアクセスし、受信携帯電話504を用いて検索し、受信携帯電話504の暗号鍵(公開鍵)を取得する。

[0129] 発信携帯電話502は、受信携帯電話504の暗号鍵(公開鍵)で、発信携帯電話502の発信者証明書を暗号化し、その暗号化された発信者証明書を受信携帯電話50

4へ送付する。発信者証明書には、発信携帯電話502の所有者情報(名前等)と、発信携帯電話502の暗号鍵(公開鍵)が記載されており、信頼できる認証局から認証を受け、認証局の署名を受けている。

[0130] 受信携帯電話504は、受信携帯電話504の暗号鍵(公開鍵)で暗号化された発信者証明書を受け取ると、受信携帯電話504の暗号鍵(秘密鍵)で復号する。受信携帯電話504の暗号鍵(公開鍵)で暗号化された発信者証明書は、受信携帯電話504の暗号鍵(秘密鍵)でのみ復号できるので、受信携帯電話504でしか復号できない。発信者証明書を、発信者の指定した人以外受け取れないようにしておくためには、復号された発信者証明書は、受信携帯電話504の外へは出ない構造にしておくことが必要である。そのため、発信者証明書が外部に出ない構造にしても良い。

[0131] 受信携帯電話504は、復号した発信者証明書が正当なものであるかを認証局の署名を用いて確認する。ここでは、認証局の暗号鍵(公開鍵)は、受信携帯電話504に販売時からあらかじめ保存されており、差し替えはできないため、認証局の暗号鍵(公開鍵)を詐称することはできないとする。復号した発信者証明書から、発信携帯電話502の暗号鍵(公開鍵)を取り出す。

[0132] また受信携帯電話504は、乱数を用いてチャレンジを生成し、発信携帯電話502の暗号鍵(公開鍵)を用いて暗号化する。そして受信携帯電話504は、暗号化されたチャレンジを、発信携帯電話502へ送付する。

[0133] 発信携帯電話502は、発信携帯電話502の暗号鍵(公開鍵)を用いて暗号化されたチャレンジを受け取り、発信携帯電話502の暗号鍵(秘密鍵)を用いて復号する。また発信携帯電話502は、復号したチャレンジを発信携帯電話502の暗号鍵(秘密鍵)で暗号化して署名する。発信携帯電話502は、署名を受信携帯電話504へ送付する。受信携帯電話504の暗号鍵(公開鍵)で暗号化して送ることもでき、この場合、受信携帯電話504以外は、署名を取り出すことができない。

[0134] 受信携帯電話504は、署名を受け取ると、発信者証明書に記載された発信携帯電話502の暗号鍵(公開鍵)を用いて、署名を確認する。受信携帯電話504は、署名を発信携帯電話502の暗号鍵(公開鍵)で復号し、元のチャレンジと一致していれば、その発信携帯電話502は、発信携帯電話502の暗号鍵(秘密鍵)を保持していること

がわかり、署名は正当なものであると確認できる。

[0135] 署名が正当なものであると確認できると受信携帯電話504は、発信携帯電話502の持ち主が、発信者証明書に記載された人物であることが確認でき、受信携帯電話504のディスプレイ507に、誰の携帯電話からの発信であるかを表示する。

[0136] 受信者503は、着信時に受信携帯電話504のディスプレイ507に表示された発信者の表示を見て、電話を取る前に誰からの着信か知ることができる。

[0137] この発信携帯電話502は、発信者通知ボタン506を備えており、発信者501が発信者通知ボタン506を押さなかった場合、受信者503には発信者証明書は送付されず、ディスプレイ507には、発信者不明と表示される。発信者通知ボタン506が電話の発信ボタンを兼ねるようにしておくと、電話をかける際に押すボタンの数を減らすことができ、発信者の利便性を高めることができる。また、受信者503が、発信者不明の電話は受けない場合、着信拒否とすることもできるが、図8のように、受信携帯電話504に発信者証明書要求ボタン508を備え、発信者501へ受信者503が発信者証明書を要求できるようにすることもできる。発信者証明書要求を受けた場合、発信携帯電話502のディスプレイ508に、発信者証明書が要求されている旨表示し、発信者501に発信者証明書を通知するかどうかを選択させるようにすることもできる。

[0138] また、警察等が受信し、発信者証明書が通知されていない場合で犯罪捜査等で必要な場合は、特殊な証明書要求を発行し、発信者の選択に関わらず発信者証明書を通知したり、発信者に選択の余地を与えず発信者証明書を通知したりすることもできる。

[0139] ここでは、発信者通知ボタン506により、発信者501が発信者証明書を通知するか否かを選択するようにしたが、例えば、警察署や消防署、病院等の公的機関やそれに類するものは必ず通知するようにし、個人の電話だけ選択できるようにすることもできる。このようにすれば、非通知として公的機関を名乗る詐欺等はできなくなるという利点がある。

[0140] この第1の実施例では、発信者の確認に電話番号を利用していないため、電話番号で発信者を確認する場合と異なり、携帯電話を買い換えたりして電話番号が変わってしまった場合にも、発信者を確認することができる。

[0141] また、電話番号を詐称して警察等になりすます詐欺があるが、第1の実施例では、発信携帯電話502の暗号鍵(秘密鍵)がなければ、なりすますことはできないため、電話番号で相手を確認する場合に比べて、安全性が高い。

[0142] 更に、電話番号で確認する場合は、予めどの電話番号が誰の電話番号であるのか覚えておくか、電話帳等に記録しておく必要がある。しかし、例えば、宅配便のドライバーから荷物配達時の在宅確認の電話を受けた場合など、発信者の電話番号と発信者の対応付けは必ずしもできているわけではなく、本当に荷物を配達する宅配便のドライバーなのか、宅配便のドライバーを名乗った強盗なのかはわからない。

[0143] この第1の実施例では、発信者証明書を通知することによって発信者を確認するため、予め受信者が準備していなくても、発信者を確認することができ、発信者が身分を偽る詐欺に会う危険を減らすことができる。

実施例 2

[0144] 次に、第2の実施例について、図9を用いて具体的な動作を説明する。

[0145] 図9に示す第2の実施例は第1の実施の形態と異なり、中継機515が発信携帯電話512との送受信を行い、受信携帯電話514は、中継器515から一方的に受信だけを行う。中継器515は、図9に示すように通信キャリア内にある通信を制御する交換機516に内蔵されているとする。ここでは、中継器515は、交換機516に内蔵されているとしたが、通信を中継する場所であれば、どこにあってもよい。

[0146] 中継器515は、チャレンジの生成を行い、その生成されたチャレンジを、発信携帯電話512へ送付する。発信携帯電話512は、受信携帯電話514の暗号鍵(公開鍵)で暗号化した発信者証明書と、チャレンジに対して行った署名を中継器515へ送付する。中継器515は、受信携帯電話514の暗号鍵(公開鍵)で暗号化した発信者証明書と、発信携帯電話512がチャレンジに対して行った署名と、そのチャレンジを受信携帯電話514へ送付する。受信携帯電話514は、受信携帯電話514の暗号鍵(公開鍵)で暗号化した発信者証明書を復号し、発信携帯電話512がチャレンジに対して行った署名と、チャレンジとから、発信携帯電話512が発信者証明書に記載されているものであることを確認する。

[0147] 第1の実施例では、発信携帯電話512と受信携帯電話514とが、相互に通信する

必要があるため、例えば、受信携帯電話514が電波の圏外にいたり、電源が切れていると相互通信できないため、その間の着信履歴を残すことができない。しかし、本実施例では、発信携帯電話512との相互通信は中継器515が行い、受信携帯電話514は受信のみを行うため、受信携帯電話514が通信できない間にあった着信について、受信携帯電話514が通信できる状態になった後に、中継器515から着信情報を通知されることで、誰から着信があったのかを確認することができる。その場合の具体例を図10に示す。

[0148] 図10では、受信携帯電話514のディスプレイ507に、受信携帯電話514が通信することができなかった時間と発信者証明書が記載されている。

[0149] これにより、受信者513は、何時及び誰から着信があったのか確認することができる。

実施例 3

[0150] 次に、第3の実施の形態について、図11を用いて具体的な動作を説明する。本実施例は、第1及び第2の実施例に加えて、発信携帯電話522に生体認証手段(指紋センサ520)を持つことを特徴とする。その発信携帯電話522を図11に示す。

[0151] 図11には、発信携帯電話502の所定の位置に指紋センサ520を備えている。そして発信者501は、発信者証明書を送付する時に指紋センサ520へ指を置き、指紋認証を行う。受信者は、受信携帯電話524のディスプレイ507に、発信者証明書と、指紋認証の結果が表示されることで、発信されたのが誰の携帯電話で、その携帯電話を携帯電話の持ち主が使用しているかどうかを確認することができる。その場合の受信携帯電話524を図12に示す。

[0152] 図12には、受信携帯電話524のディスプレイ507に、発信者証明書と、指紋認証の結果とが表示されている。

[0153] このように、受信者は、発信者を容易に確認することができるようになっている。

[0154] ところで、携帯電話を貸し借りして、他人の携帯電話を使用することや、盗難等によって携帯電話の持ち主以外が携帯電話を利用している可能性がある。第1の実施例や第2の実施例のように、誰の携帯電話なのかを特定するだけでは、例えば警察官の携帯電話を盗んで警察官になりすますようなことも可能であるが、第3の実施例に

よると、携帯電話の実際の利用者も特定することができる。

[0155] また、複数人の共有の携帯電話であるような場合、電話機を特定するだけでは誰からの発信か確認することはできないが、共有している人全員の指紋を登録しておき、指紋認証を用いて誰の指が押されたかを調べれば、共有している人のうち誰が発信したのかを調べることができ、受信者503へ通知することができる。

[0156] 発信者証明書を送付するか否かを選択できる発信携帯電話502の場合、指紋センサ520へ指を押し当てることで、発信者証明書を通知することを選択することにすれば、ボタンの押捺回数を減らすことができ、発信者の利便性を高めることができる。

[0157] 上述した実施の形態においては、携帯電話を構成する図示しないCPU, ROM, RAM, RFモジュール等によって実施されるようになっていたが、本発明はこれに限らず、その他種々の回路構成でなる携帯電話を構成しても良い。

[0158] また、上述した実施の形態においては、送信機100の証明書送付手段、受信機200のチャレンジ生成手段、暗号鍵配布サーバ300の暗号鍵配布手段は、無線による送信や受信を司るRFモジュール(図示せず)から構成されるようになされていたが、本発明はこれに限らず、他の装置と通信が行なえるものであれば良く、有線でも無線でも良い。

[0159] さらに、上述した実施の形態においては、送信機100、受信機200、暗号鍵配布サーバ300のそれぞれがCPU(図示せず)を備え、証明書暗号化手段、署名手段、証明書復号手段、チャレンジ生成手段、署名検証手段は、各CPU(図示せず)によって制御されるようになされていたが、本発明はこれに限らず、予めコンピュータに実行させるプログラムをROM(図示せず)に格納するようにしても良く、また交換可能な記憶媒体を介してプログラムを取得するようにしても良い。

[0160] また、上述した第1の実施例においては、証明書送付手段として発信者通知ボタン506、証明書復号手段として発信者証明書要求ボタン508を備えるようにしたが、本発明はこれに限らず、標準設定や初期設定として設けるようにしても良い。

産業上の利用可能性

[0161] 本発明によれば、携帯電話等で通信をする場合に、受信者が発信者を確認する用途に適用することができる。

請求の範囲

[1] 発信を行う送信機と、その発信を受ける受信機と、を備え、

前記送信機は、前記送信機の利用者を示す発信者証明書を前記受信機に送信し、

前記受信機は、前記発信機からの通信に応じてチャレンジを前記送信機に送信し、

前記送信機は、前記受信機から受信した前記チャレンジに発信者の秘密鍵で署名を付し、署名されたチャレンジを受信機に送信し、

前記受信機は、前記送信機から受信した前記署名を前記発信者証明書に記載された発信者の暗号鍵を用いて確認できた場合に前記発信者証明書に記載された発信者の情報を表示部に表示すること特徴とする発信者確認システム。

[2] 発信を行う送信機と、その発信を受ける受信機と、前記送信機に通信可能に接続された暗号鍵配布サーバとを備え、

前記暗号鍵配布サーバは、

前記送信機の発信先となる前記受信機の公開鍵を前記送信機に配布する暗号鍵配布手段

を有し、

前記送信機は、

前記暗号鍵配布サーバから取得した前記受信機の公開鍵を用いて前記送信機の公開鍵を含む発信者証明書を暗号化する証明書暗号手段と、

暗号化された前記発信者証明書を前記受信機へ送付する証明書送付手段と、

前記受信機から送付されたチャレンジを、前記送信機の秘密鍵を用いて復号化し、復号化された前記チャレンジに対して、前記送信機の秘密鍵を用いて暗号化することで署名を行ない、前記受信機へ前記署名を送付する署名手段と

を有し、

前記受信機は、

暗号化された前記送信機の発信者証明書を、当該受信機の秘密鍵を用いて復号化する証明書復号手段と、

前記送信機に前記署名させるための前記チャレンジを生成して、前記発信者証明書から取得した前記送信機の公開鍵を用いて当該チャレンジを暗号化して当該送信機に送付するチャレンジ生成手段と、

前記送信機から送付された前記署名を、前記送信機の公開鍵を用いて復号化し、復号化されたデータが前記チャレンジ生成手段により生成された前記チャレンジと一致しているか否かを検証する署名検証手段と、

前記復号化されたデータが前記チャレンジと一致している場合に、前記署名が正しいと検証して、前記発信者証明書を表示する証明書表示手段と

を有することを特徴とする請求項1に記載の発信者確認システム。

[3] 前記送信機は、前記発信者証明書を前記受信機へ通知するか否かを選択する手段をさらに備えたことを特徴とする請求項2記載の発信者確認システム。

[4] 前記受信機は、前記送信機から前記発信者証明書の通知がない場合に、前記送信機へ前記発信者証明書を通知するように要求する手段をさらに備えたことを特徴とする請求項2又は3のいずれか1項に記載の発信者確認システム。

[5] 発信を行う送信機と、その発信を受ける受信機と、中継器と、を備え、

前記送信機は、前記送信機の利用者を示す発信者証明書を前記中継器に送信し、

前記中継器は、前記発信機からの通信に応じてチャレンジを前記送信機に送信し、

前記送信機は、前記中継器から受信したチャレンジに発信者の秘密鍵で署名を付し、署名されたチャレンジを中継器に送信し、

前記中継器は、前記発信者証明書、署名前のチャレンジ及び署名されたチャレンジを前記受信機に送信し、

前記受信機は、前記中継器から受信した前記署名を前記発信者証明書に記載された発信者の暗号鍵を用いて確認できた場合に前記発信者証明書に記載された発信者の情報を表示部に表示すること特徴とする発信者確認システム。

[6] 発信を行う送信機と、その発信を受ける受信機と、前記送信機に通信可能に接続された暗号鍵配布サーバと、前記送信機と前記受信機との間に通信可能に接続され

た中継器とを備え、

前記暗号鍵配布サーバは、

前記送信機が要求する前記受信機の公開鍵を配布する暗号鍵配布手段

を有し、

前記送信機は、

前記暗号鍵配布サーバから取得した前記受信機の公開鍵を用いて前記送信機の公開鍵を含む発信者証明書を暗号化する証明書暗号手段と、

暗号化された前記発信者証明書を前記中継器へ送付する証明書送付手段と、

前記中継器から送付されたチャレンジを、前記送信機の秘密鍵を用いて復号化し、当該復号化された前記チャレンジに対して、前記送信機の秘密鍵を用いて暗号化することで署名を行ない、前記中継器へ前記署名を送付する署名手段と

を有し、

前記中継器は、

前記送信機に前記署名させるための前記チャレンジを生成して、前記発信者証明書から取得した前記送信機の公開鍵を用いて当該チャレンジを暗号化して当該送信機に送付するチャレンジ生成手段と、

前記送信機から取得した前記署名と前記暗号化された前記発信者証明書と前記チャレンジ生成手段で生成された前記チャレンジとを前記受信機へ送付する中継手段と

を有し、

前記受信機は、

前記中継器から送付された前記暗号化された前記送信機の前記発信者証明書を、当該受信機の秘密鍵を用いて復号化する証明書復号手段と、

前記中継器から送付された前記署名を、前記送信機の公開鍵を用いて復号化し、復号化されたデータが前記チャレンジ生成手段により生成された前記チャレンジと一致しているか否かを検証する署名検証手段と、

前記復号化されたデータが前記チャレンジと一致している場合に、前記署名が正しいと検証して、前記発信者証明書を表示する証明書表示手段と、

受信できなかった着信記録を、当該受信機が受信できるようになった後に、前記中継器を介して受信する手段とを有することを特徴とする請求項5に記載の発信者確認システム。

[7] 前記送信機は、生体認証手段と、前記受信機へ前記発信者証明書、又は前記署名を送付する場合に、前記生体認証手段による生体認証結果も通知する手段とをさらに備え、

前記受信機は、前記生体認証結果に基づいて前記送信機の持ち主とユーザを確認する手段をさらに備えたことを特徴とする請求項1乃至6のいずれか1項に記載の発信者確認システム。

[8] 前記送信機は、前記生体認証手段に生体情報が入力されることにより前記発信者証明書の通知を行うか否かを選択する手段をさらに備えたことを特徴とする請求項7記載の発信者確認システム。

[9] 前記送信機及び前記受信機が携帯電話によって構成されることを特徴とする請求項1乃至8のいずれか1項記載の発信者確認システム。

[10] 受信機の公開鍵をその電話番号に対応付けて保持する手段と、送信機の発信先となる前記受信機の公開鍵をその電話番号に基づいて検索する手段と、検索された前記受信機の公開鍵を前記送信機へ配布する暗号鍵配布手段を備えたことを特徴とする暗号鍵配布サーバ。

[11] 当該送信機の利用者を示す発信者証明書を受信機に送信する手段と、

チャレンジを前記送信機から受信する手段と、

前記受信機から受信した前記チャレンジに発信者の秘密鍵で署名を付し、署名されたチャレンジを受信機に送信する手段と、

を備えることを特徴とする送信機。

[12] 暗号鍵配布サーバから取得した受信機の公開鍵を用いて送信機の公開鍵を含む発信者証明書を暗号化する証明書暗号手段と、

暗号化された前記発信者証明書を前記受信機へ送付する証明書送付手段と、

前記受信機から送付されたチャレンジを、前記送信機の秘密鍵を用いて復号化し、当該復号化された前記チャレンジに対して、前記送信機の秘密鍵を用いて暗号化

することで署名を行ない、前記受信機へ前記署名を送付する署名手段と

を有し、

前記発信者証明書を前記受信機へ通知するか否かを選択する手段をさらに備えたことを特徴とする請求項11に記載の送信機。

[13] 送信機から、前記送信機の利用者を示す発信者証明書を受信する手段と、

前記発信機からの通信に応じてチャレンジを前記送信機に送信する手段と、

前記送信機において発信者の秘密鍵で署名されたチャレンジを受信する手段と、

前記送信機から受信した前記署名を前記発信者証明書に記載された発信者の暗号鍵を用いて確認できた場合に前記発信者証明書に記載された発信者の情報を表示部に表示する手段と、

を備えること特徴とする受信機。

[14] 暗号化された送信機の発信者証明書を、受信機の秘密鍵を用いて復号化する証明書復号手段と、

前記送信機に署名させるためのチャレンジを生成して、前記発信者証明書から取得した前記送信機の公開鍵を用いて当該チャレンジを暗号化して当該送信機に送付するチャレンジ生成手段と、

前記送信機から送付された前記署名を、前記送信機の公開鍵を用いて復号化し、復号化されたデータが前記チャレンジ生成手段により生成された前記チャレンジと一致しているか否かを検証する署名検証手段と、

前記復号化したデータが前記チャレンジと一致している場合に、前記署名が正しいと検証して、前記発信者証明書を表示する証明書表示手段と

を有し、

前記送信機から前記発信者証明書の通知がない場合に、前記送信機へ前記発信者証明書を通知するように要求する手段をさらに備えたことを特徴とする受信機。

[15] 発信を行う送信機と、その発信を受ける受信機と、を備えるシステムにおける発信者確認方法において、

前記送信機は、前記送信機の利用者を示す発信者証明書を前記受信機に送信し、

前記受信機は、前記発信機からの通信に応じてチャレンジを前記送信機に送信し、

前記送信機は、前記受信機から受信した前記チャレンジに発信者の秘密鍵で署名を付し、署名されたチャレンジを受信機に送信し、

前記受信機は、前記送信機から受信した前記署名を前記発信者証明書に記載された発信者の暗号鍵を用いて確認できた場合に前記発信者証明書に記載された発信者の情報を表示部に表示すること特徴とする発信者確認方法。

[16] 発信を行う送信機と、その発信を受ける受信機と、前記送信機に通信可能に接続された暗号鍵配布サーバとを備える発信者確認システムの発信者確認方法であって、

前記暗号鍵配布サーバが、前記送信機の発信先となる前記受信機の公開鍵を前記送信機へ配布し、

前記送信機が、前記暗号鍵配布サーバから取得した前記受信機の公開鍵を用いて前記送信機の公開鍵を含む前記発信者証明書を暗号化し、

前記送信機が、暗号化された前記発信者証明書を前記受信機へ送付し、

前記受信機が、暗号化された前記送信機の発信者証明書を当該受信機の秘密鍵を用いて復号化し、

前記受信機が、前記送信機に署名させるためのチャレンジを生成して、前記送信機の公開鍵で暗号化して前記送信機に送付し、

前記送信機が、前記受信機から送付された前記チャレンジを、前記送信機の秘密鍵を用いて復号化し、当該復号化された前記チャレンジに対して、前記送信機の秘密鍵を用いて暗号化することで署名し、前記受信機へ前記署名を送付し、前記受信機が、前記送信機から送付された前記署名を、前記送信機の公開鍵を用いて復号化し、復号化されたデータが、生成された前記チャレンジと一致しているか否かを検証し、

前記受信機が、前記復号化されたデータが前記チャレンジと一致している場合に、前記署名が正しいと検証して、前記発信者証明書を表示することを特徴とする請求項15に記載の発信者確認方法。

[17] 当該送信機の利用者を示す発信者証明書を受信機に送信し、

チャレンジを前記送信機から受信し、

前記受信機から受信した前記チャレンジに発信者の秘密鍵で署名を付し、署名されたチャレンジを受信機に送信することを特徴とする送信方法。

[18] 暗号鍵配布サーバから取得した受信機の公開鍵を用いて送信機の公開鍵を含む前記発信者証明書を暗号化し、

前記暗号化された前記発信者証明書を前記受信機へ送付し、

前記受信機から送付されたチャレンジを、前記送信機の秘密鍵を用いて復号化し、当該復号化された前記チャレンジに対して、前記送信機の秘密鍵を用いて暗号化することで署名し、前記受信機へ前記署名を送付することを特徴とする請求項17に記載の送信方法。

[19] 送信機から、前記送信機の利用者を示す発信者証明書を受信し、

前記発信機からの通信に応じてチャレンジを前記送信機に送信し、

前記送信機において発信者の秘密鍵で署名されたチャレンジを受信し、

前記送信機から受信した前記署名を前記発信者証明書に記載された信者の暗号鍵を用いて確認できた場合に前記発信者証明書に記載された発信者の情報を表示部に表示すること特徴とする受信方法。

[20] 暗号化された送信機の発信者証明書を受信機の秘密鍵を用いて復号化し、

前記送信機に署名させるためのチャレンジを生成して、前記送信機の公開鍵で暗号化して前記送信機に送付し、

前記送信機から送付された前記署名を、前記送信機の公開鍵を用いて復号化し、復号化されたデータが、生成された前記チャレンジと一致しているか否かを検証し、

前記復号化されたデータが前記チャレンジと一致している場合に、前記署名が正しいと検証し、前記発信者証明書を表示することを特徴とする受信方法。

[21] 送信機から求のあった受信機の公開鍵を前記送信機へ配布することを特徴とする暗号鍵配布方法。

[22] 当該送信機の利用者を示す発信者証明書を受信機に送信する手順と、

チャレンジを前記送信機から受信する手順と、

前記受信機から受信した前記チャレンジに発信者の秘密鍵で署名を付し、署名さ

れたチャレンジを受信機に送信する手順と、をコンピュータに実行させることを特徴とする送信プログラム。

[23] 暗号鍵配布サーバから取得した受信機の公開鍵を用いて送信機の公開鍵を含む発信者証明書を暗号化する手順と、

前記暗号化された前記発信者証明書を前記受信機へ送付する手順と、

前記受信機から送付されたチャレンジを、前記送信機の秘密鍵を用いて復号化し、当該復号化された前記チャレンジに対して、前記送信機の秘密鍵を用いて暗号化することで署名し、前記受信機へ前記署名を送付する手順と

をコンピュータに実行させることを特徴とする請求項22に記載の送信プログラム。

[24] 送信機から、前記送信機の利用者を示す発信者証明書を受信する手順と、

前記発信機からの通信に応じてチャレンジを前記送信機に送信する手順と、

前記送信機において発信者の秘密鍵で署名されたチャレンジを受信する手順と、

前記送信機から受信した前記署名を前記発信者証明書に記載された信者の暗号鍵を用いて確認できた場合に前記発信者証明書に記載された発信者の情報を表示部に表示する手順と、

をコンピュータに実行させること特徴とする受信プログラム。

[25] 暗号化された送信機の発信者証明書を受信機の秘密鍵を用いて復号化する手順と、

前記送信機に署名させるためのチャレンジを生成して、前記送信機の公開鍵で暗号化して前記送信機に送付する手順と、

前記送信機から送付された署名を、前記送信機の公開鍵を用いて復号化し、複合化されたデータが、生成された前記チャレンジと一致しているか否かを検証する手順と、

前記復号化されたデータが前記チャレンジと一致している場合に、前記署名が正しいと検証して、前記発信者証明書を表示する手順と

をコンピュータに実行させることを特徴とする請求項24に記載の受信プログラム。

[26] 送信機から要求のあった受信機の公開鍵を前記送信機へ配布することを特徴とする暗号鍵配布プログラム。

[27] 発信を行う送信機と、その発信を受ける受信機と、中継器と、を備えるシステムにおける中継器において、

前記送信機から、前記送信機の利用者を示す発信者証明書を受信する手段と、

前記発信機からの通信に応じてチャレンジを前記送信機に送信する手段と、

前記送信機において、当該中継器から受信したチャレンジに発信者の秘密鍵で署名されたチャレンジを、前記送信機から受信する手段と、

前記発信者証明書、署名前のチャレンジ及び署名されたチャレンジを前記受信機に送信する手段と、

を備えることを特徴とする中継器。

[28] 送信機に署名させるためのチャレンジを生成して、発信者証明書から取得した前記送信機の公開鍵を用いて当該チャレンジを暗号化して当該送信機に送付するチャレンジ生成手段と、

前記送信機から取得した前記署名と暗号化された前記発信者証明書と前記チャレンジ生成手段で生成された前記チャレンジとを前記受信機へ送付する中継手段と

を備えたことを特徴とする請求項27に記載の中継器。

[29] 発信を行う送信機と、その発信を受ける受信機と、中継器と、を備えるシステムにおける中継方法において、

前記送信機から、前記送信機の利用者を示す発信者証明書を受信し、

前記発信機からの通信に応じてチャレンジを前記送信機に送信し、

前記送信機において、当該中継器から受信したチャレンジに発信者の秘密鍵で署名されたチャレンジを、前記送信機から受信し、

前記発信者証明書、署名前のチャレンジ及び署名されたチャレンジを前記受信機に送信することを特徴とする中継方法。

[30] 送信機に署名させるためのチャレンジを生成して、発信者証明書から取得した前記送信機の公開鍵を用いて当該チャレンジを暗号化して当該送信機に送付し、

前記送信機から取得した前記署名と暗号化された前記発信者証明書と生成された前記チャレンジとを前記受信機へ送付することを特徴とする請求項29に記載の中継方法。

[31] 発信を行う送信機と、その発信を受ける受信機と、中継器と、を備えるシステムにおける中継方法をコンピュータに行わせるための中継プログラムにおいて、

前記送信機から、前記送信機の利用者を示す発信者証明書を受信する手順と、

前記発信機からの通信に応じてチャレンジを前記送信機に送信する手順と、

前記送信機において、当該中継器から受信したチャレンジに発信者の秘密鍵で署名されたチャレンジを、前記送信機から受信する手順と、

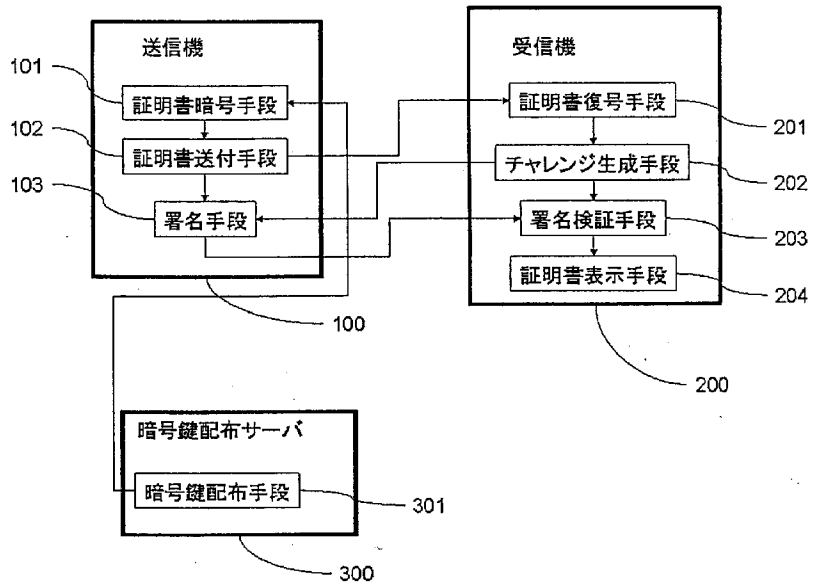
前記発信者証明書、署名前のチャレンジ及び署名されたチャレンジを前記受信機に送信する手順と、

をコンピュータに行わせるための中継プログラム。

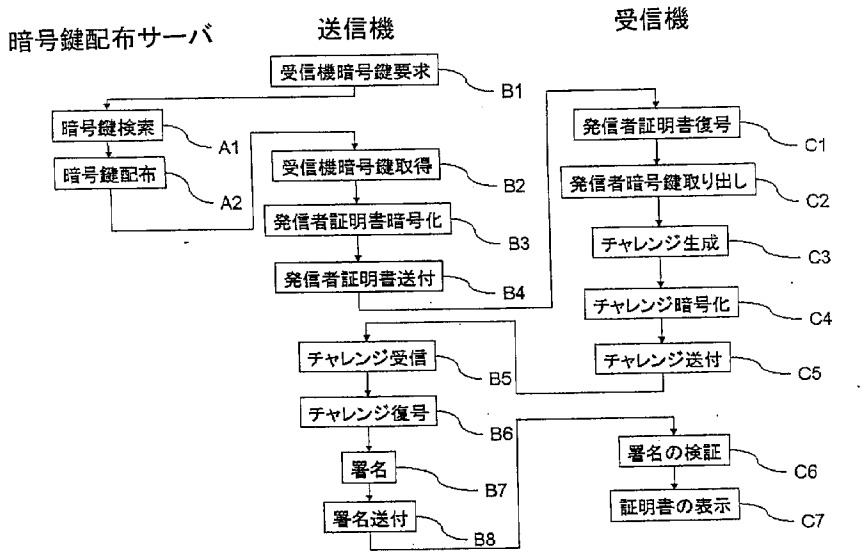
[32] 送信機に署名させるためのチャレンジを生成して、発信者証明書から取得した前記送信機の公開鍵を用いて当該チャレンジを暗号化して当該送信機に送付する手順と、

前記送信機から取得した前記署名と暗号化された前記発信者証明書と生成された前記チャレンジとを前記受信機へ送付する手順とをコンピュータに実行させることを特徴とする請求項31に記載の中継プログラム。

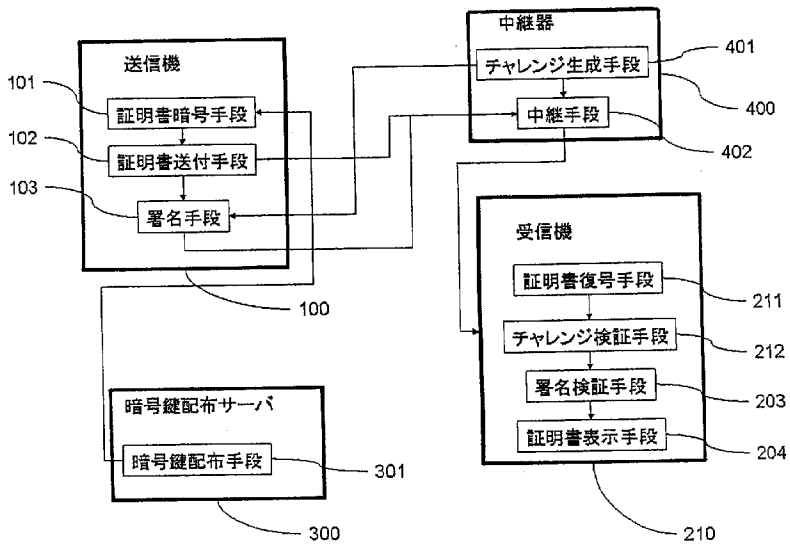
[図1]


送信機
101
証明書暗号手段
102
証明書送付手段
103
署名手段
100
受信機
証明書復号手段
201
チャレンジ生成手段
202
署名検証手段
203
証明書表示手段
204
200
暗号鍵配布サーバ
暗号鍵配布手段
301
300

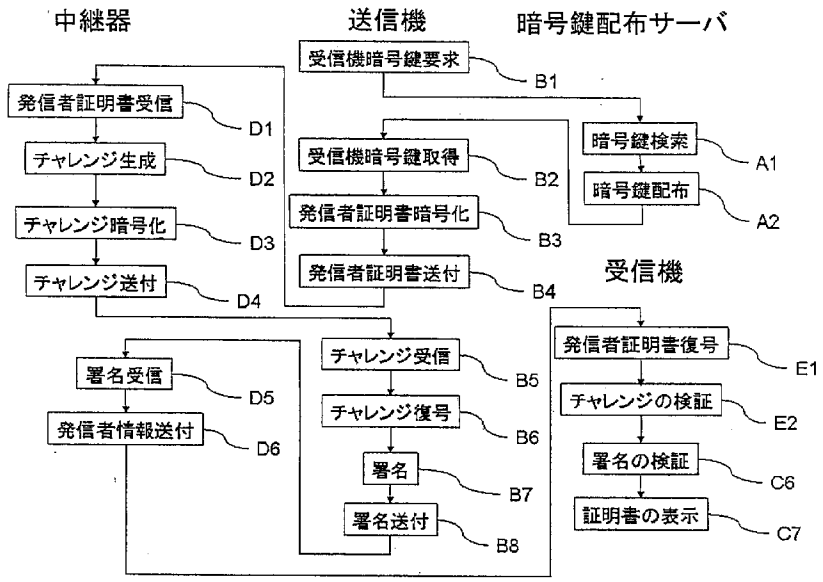
[図2]


暗号鍵配布サーバ
送信機
受信機
受信機暗号鍵要求
B1
暗号鍵検索
A1
暗号鍵配布
A2
受信機暗号鍵取得
B2
発信者証明書暗号化
B3
発信者証明書送付
B4
チャレンジ受信
B5
チャレンジ復号
B6
署名
B7
署名送付
B8
発信者証明書復号
C1
発信者暗号鍵取り出し
C2
チャレンジ生成
C3
チャレンジ暗号化
C4
チャレンジ送付
C5
署名の検証
C6
証明書の表示
C7

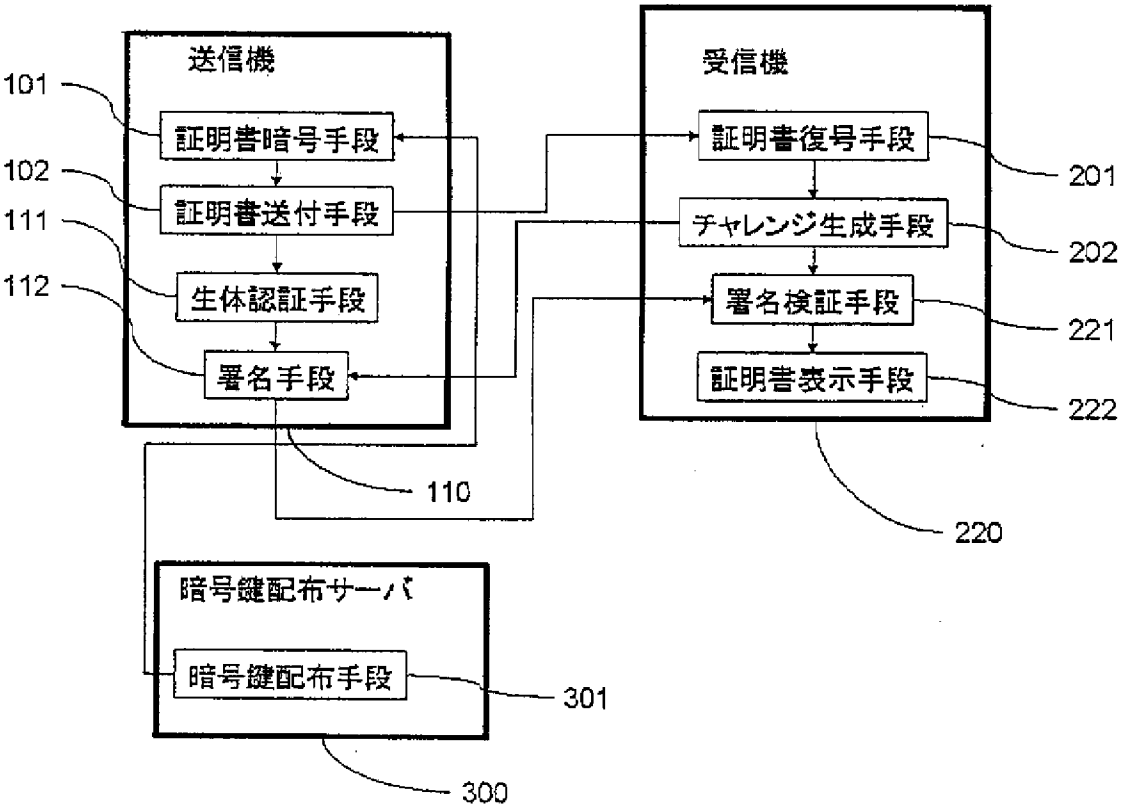
[図3]


送信機
101
証明書暗号手段
102
証明書送付手段
103
署名手段
100
中継器
チャレンジ生成手段
401
400
中継手段
402
受信機
証明書復号手段
211
チャレンジ検証手段
212
署名検証手段
203
証明書表示手段
204
210
暗号鍵配布サーバ
暗号鍵配布手段
301
300

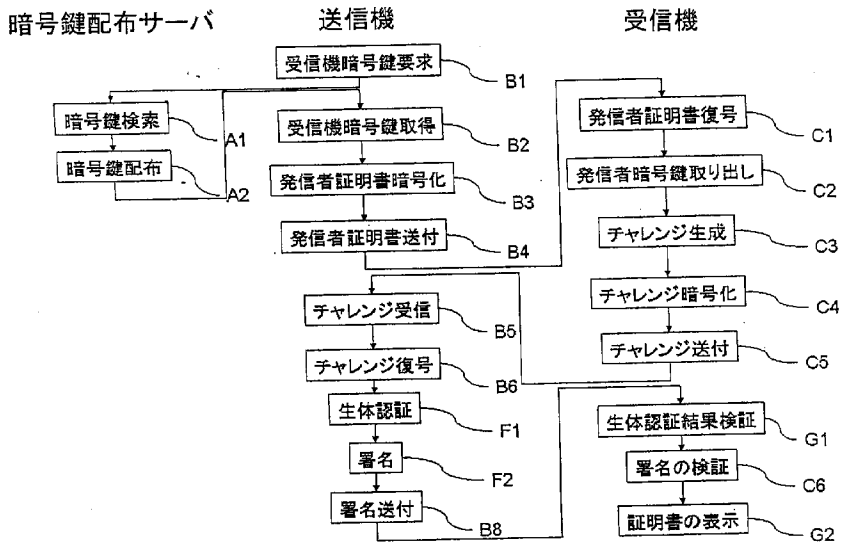
[図4]


中継器
送信機
暗号鍵配布サーバ
受信機暗号鍵要求
B1
発信者証明書受信
D1
暗号鍵検索
A1
受信機暗号鍵取得
B2
チャレンジ生成
D2
暗号鍵配布
A2
発信者証明書暗号化
B3
チャレンジ暗号化
D3
発信者証明書送付
B4
受信機
チャレンジ送付
D4
発信者証明書復号
E1
チャレンジ受信
B5
署名受信
D5
チャレンジの検証
E2
チャレンジ復号
B6
発信者情報送付
D6
署名の検証
C6
署名
B7
証明書の表示
C7
署名送付
B8

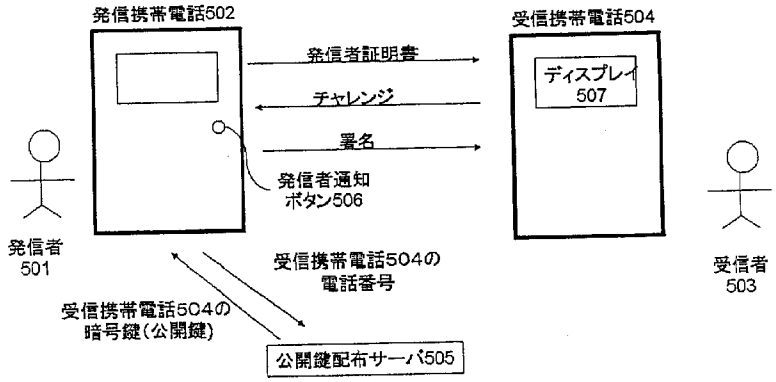
[図5]


送信機
101
証明書暗号手段
102
証明書送付手段
111
生体認証手段
112
署名手段
110
受信機
証明書復号手段
201
チャレンジ生成手段
202
署名検証手段
221
証明書表示手段
222
220
暗号鍵配布サーバ
暗号鍵配布手段
301
300

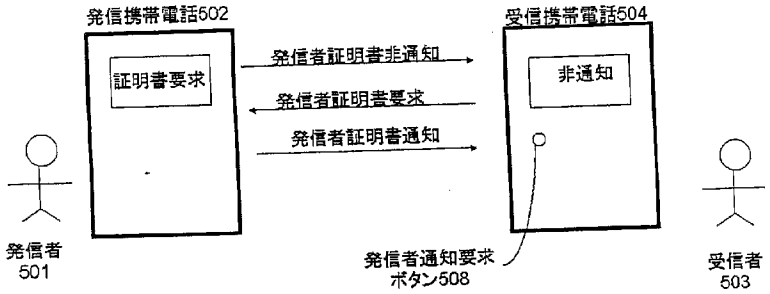
[図6]


暗号鍵配布サーバ
送信機
受信機
受信機暗号鍵要求
B1
暗号鍵検索
A1
受信機暗号鍵取得
B2
暗号鍵配布
A2
発信者証明書暗号化
B3
発信者証明書送付
B4
チャレンジ受信
B5
チャレンジ復号
B6
生体認証
F1
署名
F2
署名送付
B8
発信者証明書復号
C1
発信者暗号鍵取り出し
C2
チャレンジ生成
C3
チャレンジ暗号化
C4
チャレンジ送付
C5
生体認証結果検証
G1
署名の検証
C6
証明書の表示
G2

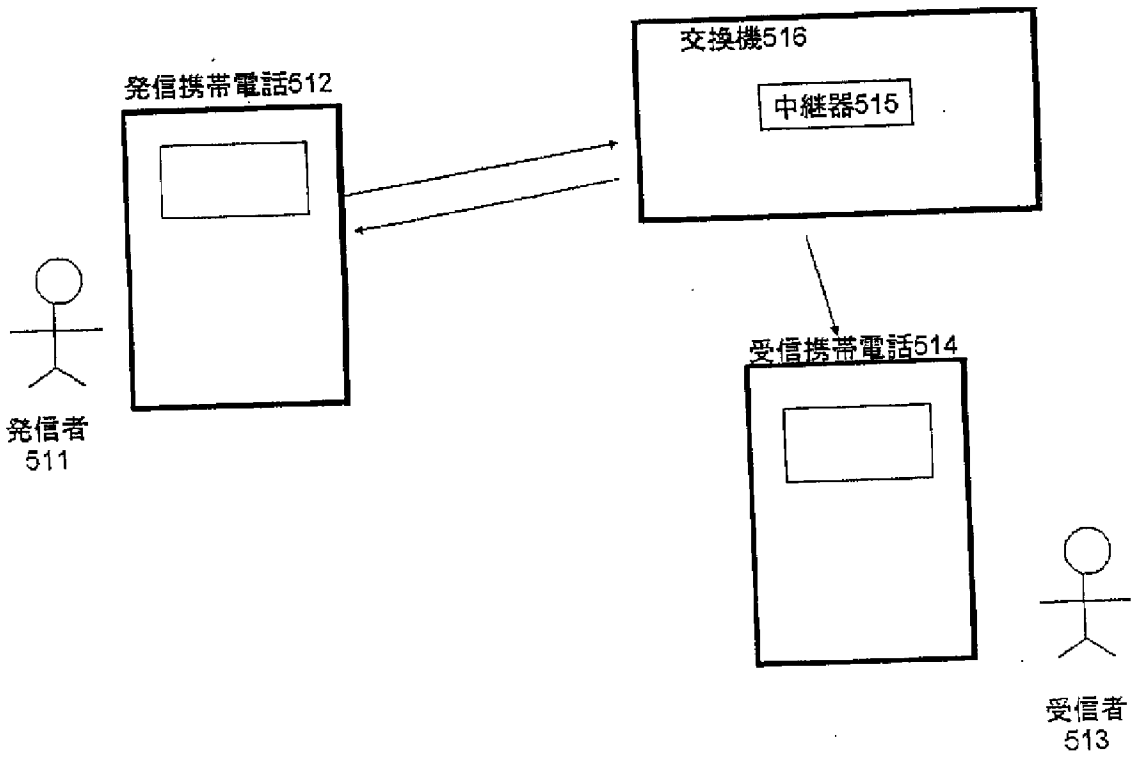
[図7]


発信携帯電話502
受信携帯電話504
発信者証明書
チャレンジ
署名
ディスプレイ
507
発信者通知
ボタン506
発信者
501
受信者
503
受信携帯電話504の
電話番号
受信携帯電話504の
暗号鍵(公開鍵)
公開鍵配布サーバ505

[図8]


発信携帯電話502
受信携帯電話504
証明書要求
発信者証明書非通知
発信者証明書要求
発信者証明書通知
非通知
発信者
501
受信者
503
発信者通知要求
ボタン508

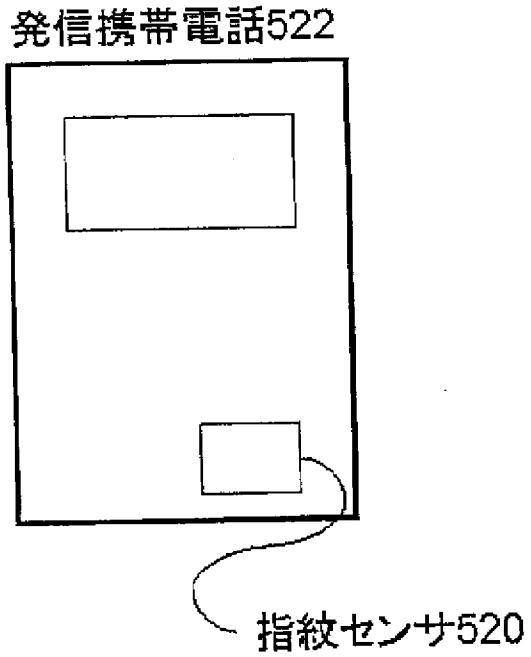
[図9]



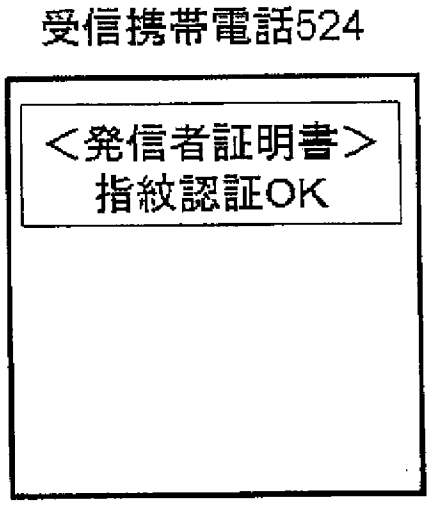
[図10]

10:02 不在着信
<発信者証明書1>
13:48 不在着信
<発信者証明書2>
・・・

[図11]



[図12]



INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2007/054017

A. CLASSIFICATION OF SUBJECT MATTER
H04L9/32(2006.01)i, *H04L9/08*(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L9/32, H04L9/08

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2007
Kokai Jitsuyo Shinan Koho 1971-2007 Toroku Jitsuyo Shinan Koho 1994-2007

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP 2003-500921 A (Silverbrook Research Pty Ltd.), 07 January, 2003 (07.01.03), Full text; all drawings & US 6290349 B1 & EP 1224614 A1 & WO 2000/072503 A1 & AU 4728200 A1	1-32
A	JP 2005-252347 A (Nippon Telegraph And Telephone Corp.), 15 September, 2005 (15.09.05), Full text; all drawings (Family: none)	1-32

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
20 March, 2007 (20.03.07)	27 March, 2007 (27.03.07)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2007/054017

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2001-265731 A (Nippon Telegraph And Telephone Corp.), 28 September, 2001 (28.09.01), Full text; all drawings (Family: none)	1-32

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００７／０５４０１７

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　H04L9/32(2006.01)i, H04L9/08(2006.01)i

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.　H04L9/32, H04L9/08

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２００７年
日本国実用新案登録公報	１９９６－２００７年
日本国登録実用新案公報	１９９４－２００７年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X	JP 2003-500921 A（シルバーブルック　リサーチ　ピーティーワイ　リミテッド）2003.01.07, 全文, 全図 & US 6290349 B1 & EP 1224614 A1 & WO 2000/072503 A1 & AU 4728200 A1	1-32
A	JP 2005-252347 A（日本電信電話株式会社）2005.09.15, 全文, 全図（ファミリーなし）	1-32
A	JP 2001-265731 A（日本電信電話株式会社）2001.09.28, 全文, 全図（ファミリーなし）	1-32

☐　Ｃ欄の続きにも文献が列挙されている。

☐　パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー

「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの

「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）

「Ｏ」口頭による開示、使用、展示等に言及する文献

「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献

「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「＆」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
２０．０３．２００７	２７．０３．２００７

国際調査機関の名称及びあて先
日本国特許庁（ＩＳＡ／ＪＰ）
郵便番号１００－８９１５
東京都千代田区霞が関三丁目４番３号

特許庁審査官（権限のある職員）　５Ｓ　３５７４
金丸　昌司
電話番号　０３－３５８１－１１０１　内線　３５４６