(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
2006 年2 月23 日 (23.02.2006)

PCT

(10) 国際公開番号
WO 2006/018874 A1

(51) 国際特許分類[7]: G06F 12/14, 15/00, G06K 17/00

(21) 国際出願番号: PCT/JP2004/011883

(22) 国際出願日: 2004 年8 月19 日 (19.08.2004)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(71) 出願人 (米国を除く全ての指定国について): 三菱電機株式会社 (MITSUBISHI DENKI KABUSHIKI KAISHA) [JP/JP]; 〒1008310 東京都千代田区丸の内二丁目２番３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): 馬場 昭宏 (BABA, Akihiro) [JP/JP]; 〒1008310 東京都千代田区丸の内二丁目２番３号 三菱電機株式会社内 Tokyo (JP). 桜井 鐘治 (SAKURAI, Shouji) [JP/JP]; 〒1008310 東京都千代田区丸の内二丁目２番３号 三菱電機株式会社内 Tokyo (JP). 近藤 誠一 (KONDO, Seiichi) [JP/JP]; 〒1008310 東京都千代田区丸の内二丁目２番３号 三菱電機株式会社内 Tokyo (JP). 撫中 達司 (MUNAKA, Tatsuji) [JP/JP]; 〒1008310 東京都千代田区丸の内二丁目２番３号 三菱電機株式会社内 Tokyo (JP). 澤村 真利子 (SAWAMURA, Mariko) [JP/JP]; 〒1008310 東京都千代田区丸の内二丁目２番３号 三菱電機株式会社内 Tokyo (JP).

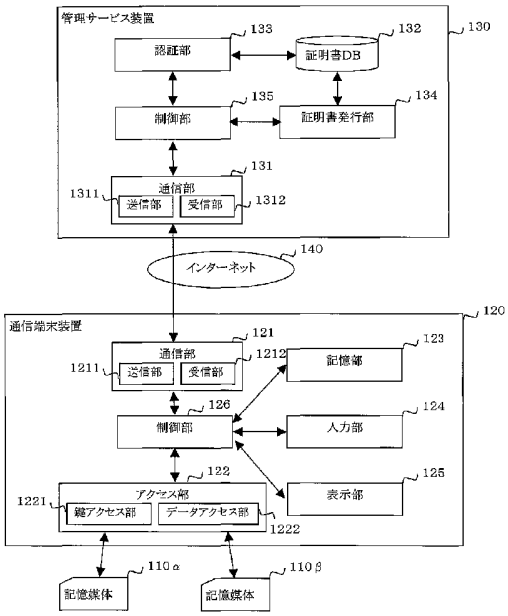
(74) 代理人: 溝井 章司 (MIZOI, Shoji); 〒2470056 神奈川県鎌倉市大船二丁目１７番１０号 ＮＴＡ大船ビル３階 溝井国際特許事務所 Kanagawa (JP).

(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,

[続葉有]

(54) Title: MANAGEMENT SERVICE DEVICE, BACKUP SERVICE DEVICE, COMMUNICATION TERMINAL DEVICE, AND STORAGE MEDIUM

(54) 発明の名称: 管理サービス装置、バックアップサービス装置、通信端末装置及び記憶媒体



130...MANAGEMENT SERVICE DEVICE
133...AUTHENTICATION UNIT
135...CONTROL UNIT
132...CERTIFICATE DB
134...CERTIFICATE ISSUING UNIT
131...COMMUNICATION UNIT
1311...TRANSMISSION UNIT
1312...RECEPTION UNIT
140...INTERNET
120...COMMUNICATION TERMINAL DEVICE
121...COMMUNICATION UNIT
1211...TRANSMISSION UNIT
1212...RECEPTION UNIT
123...STORAGE UNIT
126...CONTROL UNIT
124...INPUT UNIT
122...ACCESS UNIT
1221...KEY ACCESS UNIT
1222...DATA ACCESS UNIT
125...DISPLAY UNIT
110α...STORAGE MEDIUM
110β...STORAGE MEDIUM

(57) Abstract: There are provided a method for invalidating a storage medium and performing new registration, a method for backup of data stored in a storage medium and restoring the backup data into the storage medium, and a method for verifying the encryption and the digital signature of the data to be backed up and decryption and the digital signature of the backup data to be restored. A service device includes: a reception unit for receiving a data processing request concerning the storage medium from a communication terminal device connected to a storage medium; an authentication unit for authenticating the storage medium connected to the communication terminal device; and a database containing the public key of the storage medium. When the reception unit has received a request for invalidating the first storage medium from the communication terminal device and the authentication unit has authenticated that the second storage medium connected to the communication terminal device is an authorized storage medium, the database deletes the public key of the first storage medium.

(57) 要約: 記憶媒体の無効化と新たな登録の方法と、記憶媒体が記憶しているデータのバックアップとバックアップデータの記憶媒体へのリストアの方法と、バックアップするデータの暗号化と電子署名、リストアするバックアップデータの復号と署名の検証の方法を提供することを目的とする。サービス装置は、記憶媒体と接続している通信端末装置から記憶媒体に関するデータ処理の要求を受信する受信部と、通信端末装置と接続している記憶媒体が正当であるか否かの認証を行う認証部と、記憶媒体の公開鍵を記憶しているデータベースを備え、受信部が通信端末装置から第１の記憶媒体の無効化の要求を受信し、認証部が通信端末装置と接続している第２の記憶媒体を正当な記憶媒体であると認証した場合に、データベースは記憶している第１の記憶媒体の公

[続葉有]

WO 2006/018874 A1

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, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, 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, IT, LU, MC, 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。

開鍵を削除することとした。

明 細 書

管理サービス装置、バックアップサービス装置、通信端末装置及び記憶媒体

技術分野

[0001] この発明は、通信ネットワークを介して携帯電話等の通信端末に装着されている既存の記憶媒体による認証の無効化と新たな記憶媒体によって認証可能とするための登録とを実現する技術に関する。また、通信ネットワークを介して通信端末に装着されている記憶媒体が記憶しているデータのバックアップとバックアップしたデータの記憶媒体へのリストアとを実現する技術に関する。また、バックアップするデータの暗号化とその復号、バックアップするデータへの電子署名とその検証を実現する技術に関する。

背景技術

[0002] 利用者の本人認証の手段やサービスのデータを格納するために、クレジットカードやポイントカードなどにICカードが使用されるようになってきている。しかし、ICカードは多量のデータを記憶できることから、それを紛失した際の被害は非常に大きなものとなる。このICカードの紛失に備えて記憶しているデータのバックアップやリカバリ(復旧)を行うための技術が開示されている(例えば、特許文献1)。

[0003] また、ICカードと同様に携帯電話においても、その紛失に備えて電話番号、住所、メモ、写真などの記憶しているデータをバックアップしたいというニーズがある。これを実現するために、携帯電話が記憶しているデータをネットワークを介してサーバにバックアップする技術が開示されている(例えば、特許文献2)。

特許文献1:特開2001−155078号公報

特許文献2:特開2003−319460号公報

発明の開示

発明が解決しようとする課題

[0004] 特許文献1で開示されている方法では、ICカードを再発行する際に、リストア(バックアップしたデータのICカードへの再書き込み)は通信ネットワークを介してオンライ

ンで行う。しかし、ICカード自体の再発行はオフラインで行わなくてはならない。その結果、ICカードの再発行に多くの時間を必要とし、場合によっては対面による本人確認が必要となることから、ICカードの利用者は、ICカード発行者（例えば自治体など）に出向く必要があった。

[0005] また、特許文献2で開示されている方法では、バックアップされる携帯電話のデータは平文であるか、もしくは暗号化された状態でバックアップサーバに保存される。しかし、特許文献2には暗号化の具体的な方式については記載されていない。例えば、バックアップされるデータの暗号化と復号をPC（Personal Computer）で行う方法の場合、暗号化と復号で使用する暗号鍵をPCのメモリに記憶しておくと考えられる。その場合、PCから暗号鍵を読み出すことができないようにするために、PCには暗号鍵を管理するためのソフトウェアやハードウェアが別途必要となる。その結果、データを暗号化してバックアップすることを望む携帯電話の利用者には、余分に費用を負担する必要が生じる。

[0006] この発明はこのような問題点を解決するためになされたものであり、ICカードや携帯電話などの記憶媒体の通信ネットワークを介した認証の無効化と新たな登録と、記憶媒体が記憶しているデータの通信ネットワークを介したサーバへのバックアップとバックアップデータの記憶媒体へのリストアと、バックアップするデータの暗号化と電子署名と、リストアするバックアップデータの復号と署名の検証を実行する装置と方法とを提供することを目的とする。

課題を解決するための手段

[0007] 前記した課題を解決するため管理サービス装置は、以下のような手段を用いることとした。

管理サービス装置は、第2の記憶媒体と接続している通信端末装置からの通信ネットワークを介した第1の記憶媒体に関するデータ処理の要求を受信する受信部と、受信部が通信端末装置から第1の記憶媒体に関するデータ処理の要求を受信した場合に、通信端末装置と接続している第2の記憶媒体が正当であるか否かの認証を行う認証部とを備えることとした。

[0008] 管理サービス装置は、さらに、第1の記憶媒体の公開鍵と第2の記憶媒体の公開鍵

とを記憶するデータベースを備え、受信部が通信端末装置から第1の記憶媒体の無効化の要求を受信し、認証部が通信端末装置と接続している第2の記憶媒体を正当な記憶媒体であると認証した場合に、データベースは記憶している第1の記憶媒体の公開鍵を削除することとした。

[0009] 管理サービス装置は、さらに、第1の記憶媒体の公開鍵と第2の記憶媒体の公開鍵とを記憶するデータベースを備え、受信部が通信端末装置から第1の記憶媒体の無効化の要求を受信し、認証部が通信端末装置と接続している第2の記憶媒体を正当な記憶媒体であると認証した場合に、データベースは記憶している第1の記憶媒体の公開鍵を削除するが、第2の記憶媒体の公開鍵は削除しないこととした。

[0010] 管理サービス装置は、さらに、第2の記憶媒体の公開鍵を記憶するデータベースと、第2の記憶媒体の公開鍵の正当性を証明する証明書を発行する証明書発行部とを備え、受信部が通信端末装置から新たな記憶媒体である第3の記憶媒体の登録の要求と第3の記憶媒体の公開鍵とを受信し、認証部が通信端末装置と接続している第2の記憶媒体を正当な記憶媒体であると認証した場合に、証明書発行部は受信部が受信した第3の記憶媒体の公開鍵の正当性を証明する証明書を発行し、データベースは受信部が受信した第3の記憶媒体の公開鍵と証明書発行部が発行した第3の記憶媒体の公開鍵の正当性を証明する証明書とを記憶することとした。

[0011] 管理サービス装置は、第1の記憶媒体の公開鍵と第1の記憶媒体の公開鍵の正当性を証明する証明書と、第2の記憶媒体の公開鍵と第2の記憶媒体の公開鍵の正当性を証明する証明書とを記憶するデータベースを備え、データベースは第1の記憶媒体の公開鍵と第1の記憶媒体の公開鍵の正当性を証明する証明書と、第2の記憶媒体の公開鍵と第2の記憶媒体の公開鍵の正当性を証明する証明書とを組にして登録することとした。

[0012] 管理サービス装置は、記憶媒体の公開鍵と公開鍵の正当性を証明する証明書とを記憶するデータベースを備え、データベースは複数の記憶媒体の公開鍵と複数の公開鍵の正当性を証明する証明書とをグループにして記憶し、認証部はグループに属する少なくともいずれか1つの公開鍵を用いて記憶媒体が正当であるか否かの認証を行い、記憶媒体を正当な記憶媒体であると認証した場合に、記憶媒体をグループ

に属する記憶媒体であると認証することとした。

[0013] バックアップサービス装置は、第1の記憶媒体と接続する通信端末装置から通信ネットワークを介して第1の記憶媒体が記憶するデータとデータをバックアップデータとして記憶する要求とを受信し、第2の記憶媒体と接続する通信端末装置から通信ネットワークを介してバックアップデータの送信の要求を受信する受信部と、受信部が第1の記憶媒体と接続する通信端末装置から第1の記憶媒体が記憶するデータをバックアップデータとして記憶する要求を受信した場合に、通信端末装置と接続している第1の記憶媒体が正当であるか否かの認証を行い、受信部が第2の記憶媒体と接続する通信端末装置からバックアップデータの送信の要求を受信した場合に、通信端末装置と接続している第2の記憶媒体が正当であるか否かの認証を行う認証部と、認証部が通信端末装置と接続している第1の記憶媒体を正当な記憶媒体であると認証した場合に、受信部が受信した第1の記憶媒体が記憶するデータをバックアップデータとして記憶するバックアップ部と認証部が通信端末装置と接続している第2の記憶媒体を正当な記憶媒体であると認証した場合に、バックアップ部が記憶しているバックアップデータを第2の記憶媒体と接続している通信端末装置へ通信ネットワークを介して送信する送信部とを備えることとした。

[0014] バックアップデータは、第1の記憶媒体と接続する通信端末装置により第2の記憶媒体の公開鍵を用いて暗号化されていることとした。

[0015] バックアップデータは、第1の記憶媒体と接続する通信端末装置により第1の記憶媒体の秘密鍵を用いて電子署名されていることとした。

[0016] 通信端末装置は、第1の公開鍵と第1の公開鍵に対応する第1の秘密鍵とデータとを記憶している第1の記憶媒体と、第2の公開鍵と第2の公開鍵に対応する第2の秘密鍵とデータとを記憶している第2の記憶媒体とのいずれかと接続し、第1の記憶媒体から第1の公開鍵と第1の秘密鍵との読み出しと第1の記憶媒体への第1の公開鍵と第1の秘密鍵との書き込みとを行い、第2の記憶媒体から第2の公開鍵と第2の秘密鍵との読み出しと第2の記憶媒体への第2の公開鍵と第2の秘密鍵との書き込みとを行う鍵アクセス部と、第1の記憶媒体からデータの読み出しと第1の記憶媒体へのデータの書き込みと、第2の記憶媒体からデータの読み出しと第2の記憶媒体へのデ

ータの書き込みとを行うデータアクセス部と、鍵アクセス部が第1の記憶媒体から読み出した第1の公開鍵と第1の秘密鍵と、鍵アクセス部が第2の記憶媒体から読み出した第2の公開鍵と第2の秘密鍵とを記憶する記憶部と、データを送信する送信部と、データを受信する受信部とを備えることとした。

[0017] 通信端末装置は、さらに、第2の公開鍵を用いてデータを暗号化する暗号化部を備え、第1の記憶媒体は第2の記憶媒体の第2の公開鍵を記憶しており、鍵アクセス部は、第1の記憶媒体から第2の公開鍵を読み出して記憶部に記憶し、データアクセス部は、第1の記憶媒体からデータを読み出し、暗号化部は記憶部が記憶している第2の公開鍵を用いてデータアクセス部が第1の記憶媒体から読み出したデータを暗号化し、送信部は暗号化部が暗号化したデータを送信することとした。

[0018] 通信端末装置は、さらに、第2の秘密鍵を用いて暗号化したデータを復号する復号部とを備え、受信部は暗号化されているデータを受信し、鍵アクセス部は第2の記憶媒体から第2の秘密鍵を読み出して記憶部に記憶し、復号部は受信部が受信した暗号化されているデータを記憶部が記憶している第2の秘密鍵を用いて復号し、データアクセス部は復号部が復号したデータを第2の記憶媒体へ書き込むこととした。

[0019] 通信端末装置は、さらに、第1の秘密鍵を用いてデータに電子署名する電子署名部を備え、鍵アクセス部は第1の記憶媒体から第1の秘密鍵を読み出して記憶部に記憶し、データアクセス部は第1の記憶媒体からデータを読み出し、電子署名部は記憶部が記憶している第1の秘密鍵を用いてデータアクセス部が第1の記憶媒体から読み出したデータに電子署名を行い、送信部は電子署名部が電子署名したデータを送信することとした。

[0020] 通信端末装置は、さらに、第1の公開鍵を用いて電子署名したデータを検証する検証部とを備え、第2の記憶媒体は第1の記憶媒体の第1の公開鍵を記憶しており、受信部は電子署名されているデータを受信し、鍵アクセス部は第2の記憶媒体から第1の公開鍵を読み出して記憶部に記憶し、検証部は受信部が受信した電子署名されているデータを記憶部が記憶している第1の公開鍵を用いて検証することとした。

[0021] 記憶媒体は、外部からのデータの入力と外部へのデータの出力とを行う入出力部と、秘密鍵と秘密鍵に対応する公開鍵とを生成する鍵生成部と、公開鍵を用いてデー

タの暗号化を行う暗号化部と、秘密鍵を用いて暗号化したデータの復号を行う復号部と、秘密鍵を用いてデータに電子署名を行う署名部と、公開鍵を用いて電子署名を行ったデータの検証を行う検証部との少なくともいずれか一つである処理部を備えることとした。

[0022] 記憶媒体は、さらに、記憶媒体の利用者が正当であるか否かの認証を行う利用者認証部とを備え、利用者認証部が利用者を正当な利用者であると認証した場合に、記憶媒体が備える処理部の動作を実行することとした。

[0023] 記憶媒体は、外部から秘密鍵を読み出すことができないこととした。

発明の効果

[0024] この発明によれば管理サービス装置は、第1の記憶媒体を紛失した場合、第2の記憶媒体と接続している通信端末装置から通信ネットワークを介して、第1の記憶媒体の無効化の要求を受信し、通信端末装置と接続している第2の記憶媒体の認証を行い、その正当性を確認した場合、第2の記憶媒体の権限にもとづいてデータベースから第1の記憶媒体の公開鍵を削除することにより、第1の記憶媒体を無効化することができる。

発明を実施するための最良の形態

[0025] 実施の形態1.

以下に述べる実施の形態1では、利用者が所持する2つの記憶媒体の一方を紛失した場合に、他方の記憶媒体の権限にもとづいて、インターネットを介して管理サービス装置に記憶媒体の無効化を依頼することにより、紛失した記憶媒体の公開鍵を削除し、紛失した記憶媒体を利用できなくする実施の形態について説明する。また、他方の記憶媒体の権限にもとづいて、インターネットを介して管理サービス装置に新たな記憶媒体の登録を依頼することにより、新たな記憶媒体の公開鍵とその証明書とを登録する実施の形態について説明する。なお、ここでは、証明書には国際電気通信連合(International Telecommunication Union:ITU)が規定した公開鍵証明書の標準仕様であるX.509を使用することを想定しており、このため、公開鍵の正当性を証明する証明書は公開鍵を含むものとする。

[0026] 図1は実施の形態1における鍵管理システムの構成を示す図である。

鍵管理システムは、インターネット140である通信ネットワークを介してサービスの提供を要求する通信端末装置120と、通信端末装置120と接続し、秘密鍵と秘密鍵に対応する公開鍵と公開鍵の正当性を証明する証明書とを記憶する2つの記憶媒体110αと記憶媒体110βと、通信端末装置120がサービスの提供を要求した際に、通信端末装置120と接続する記憶媒体110αと記憶媒体110βとのいずれか一つの認証を行う管理サービス装置130と、管理サービス装置130と通信端末装置120とを接続するインターネット140とから構成される。

[0027] 記憶媒体110αおよび記憶媒体110βは、利用者が使用する不揮発性の記憶媒体であり、例としては不揮発性のメモリ媒体や外付けのハードディスクドライブなどである。通常は記憶媒体110αを通信端末装置120に装着して使用し、記憶媒体110βは予備として持つ。なお、以降は通常使用する記憶媒体110αを正と、予備として持つ記憶媒体110βを副と記載することがある。また、記憶媒体110αと記憶媒体110βとの両者を併せて、単に記憶媒体110と記載することがある。

[0028] 通信端末装置120は、インターネット140を経由して管理サービス装置130との間で通信を行う通信部121と、記憶媒体120αもしくは記憶媒体110βからの読み込みと、記憶媒体120αもしくは記憶媒体110βへの書込みを行うアクセス部122と、アクセス部122で読み込んだデータを一時的に記憶する記憶部123と、利用者からの操作入力を受取る入力部124と、利用者に情報を表示する表示部125と、これらの制御を行う制御部126とから構成され、好適な例は携帯電話端末である。

[0029] 通信部121は、管理サービス装置130へデータを送信する送信部1211と、管理サービス装置130からデータを受信する受信部1212とから構成される。

[0030] アクセス部122は、記憶媒体110への公開鍵と秘密鍵の書き込みと、記憶媒体110からの公開鍵と秘密鍵の読み出しとを行う鍵アクセス部1221と、記憶媒体110へのデータの書き込みと、記憶媒体110からのデータの読み出しとを行うデータアクセス部1222とから構成される。

[0031] 管理サービス装置130は、インターネット140を経由して通信端末装置120との間で通信を行う通信部131と、記憶媒体110に固有の公開鍵と、公開鍵を含む公開鍵の正当性を証明する証明書とを管理する証明書データベース(DB)132と、公開鍵

の証明書を使って公開鍵を記憶している記憶媒体110の認証を行う認証部133と、新たな証明書を発行する証明書発行部134と、これらの制御を行う制御部135とから構成される。

[0032] 通信部131は、通信端末装置120へデータを送信する送信部1311と、通信端末装置120からデータを受信する受信部1312とから構成される。

[0033] 図2に示すように、記憶媒体110αと記憶媒体110βとは、それぞれ通信端末装置と接続し、秘密鍵と秘密鍵に対応する公開鍵と公開鍵の正当性を証明する証明書とを記憶している。図2において、K^{α}_{pub}とK^{β}_{pub}とは、それぞれ記憶媒体αと記憶媒体βとの公開鍵を示しており、K^{α}_{pri}とK^{β}_{pri}とは、それぞれ記憶媒体110αと記憶媒体110βとの秘密鍵を示している。

[0034] 証明書DB132は、記憶媒体110を所有する利用者と、記憶媒体110が記憶している公開鍵の証明書との対応を記載するユーザリストと、失効した公開鍵の証明書を記載する失効リストとを記憶している。

[0035] 管理サービス装置130は、第1の記憶媒体110αの公開鍵と第1の記憶媒体110αの公開鍵の正当性を証明する証明書と、第2の記憶媒体110βの公開鍵と第2の記憶媒体110βの公開鍵の正当性を証明する証明書とを記憶する証明書データベース132を備え、証明書データベース132は、第1の記憶媒体110αの公開鍵と第1の記憶媒体110αの公開鍵の正当性を証明する証明書と、第2の記憶媒体110βの公開鍵と第2の記憶媒体110βの公開鍵の正当性を証明する証明書とを組にして登録する。

[0036] 図3にユーザリストの例を示す。ユーザIDはシステム全体において利用者を一意に識別するためのIDである。証明書(正)は、利用者が所有する正の記憶媒体αが記憶している公開鍵の証明書であり、証明書(副)は、利用者が所有する副の記憶媒体βが記憶している公開鍵の証明書である。公開鍵の証明書はその要素として公開鍵そのものを含んでいる。図3において、例えば、α_Aは利用者Aの正の記憶媒体110αが記憶している公開鍵の証明書、β_Aは利用者Aの副の記憶媒体110βが記憶している公開鍵の証明書をそれぞれ表している。利用者Bと利用者Cについても同様である。

[0037] 次に、利用者が所持する2つの記憶媒体110の一方を紛失した場合に、他方の記憶媒体110の権限にもとづいて、鍵管理システムの通信端末装置120が、インターネット140を介して管理サービス装置130に記憶媒体の無効化を依頼することにより、紛失した記憶媒体の公開鍵を削除し、紛失した記憶媒体を利用できなくする方法を説明する。なお、以下の説明では、認証の対象を記憶媒体としているが、認証の最終的な目的は記憶媒体を所有している利用者の正当性を確認することであり、ここで認証により記憶媒体の正当性を確認することは、それを所有している利用者の正当性を確認することに相当するものとする。

[0038] 管理サービス装置130では、受信部1312が、第2の記憶媒体110βと接続している通信端末装置120から、インターネット140である通信ネットワークを介した第1の記憶媒体100αに関するデータ処理の要求を受信する。受信部1312が、通信端末装置120から、第1の記憶媒体110αに関するデータ処理の要求を受信した場合に、認証部133が、通信端末装置120と接続している第2の記憶媒体110βが正当であるか否かの認証を行う。

[0039] 管理サービス装置130では、証明書データベース132が、第1の記憶媒体110αの公開鍵と第2の記憶媒体110βの公開鍵とを記憶している。受信部1312が、通信端末装置120から、第1の記憶媒体110αの無効化の要求を受信し、認証部133が、通信端末装置120と接続している第2の記憶媒体110βを正当な記憶媒体であると認証した場合に、証明書データベース132は、記憶している第1の記憶媒体110αの公開鍵を削除する。

[0040] 利用者が記憶媒体110αもしくは記憶媒体110βを紛失した際などに、記憶媒体を無効化する具体的な方法を図4に示すフローチャートを用いて説明する。なお、ここで記憶媒体の無効化は、管理サービス装置130の証明書DB132に記憶されている公開鍵を削除することにより、管理サービス装置130に認証を要求した際、認証できないようにすることにより実現する。

[0041] 利用者は通信端末装置120の入力部124から記憶媒体110の無効化を要求する（ステップS501）。通信端末装置120は、管理サービス装置130に対して記憶媒体の無効化の要求を送信し、管理サービス装置130は、通信端末装置120が接続して

いる記憶媒体110の認証を行い(認証の方法は後述する)、認証が成功したか否かを判断する(ステップS502)。成功したと判断しなかった場合(ステップS502のNoの場合)、無効化を継続することはできず、処理を終了する。成功したと判断した場合(ステップS502のyesの場合)、管理サービス装置130は、ステップS502で認証した記憶媒体110が、正の記憶媒体110αであるか否かを判断する(ステップS503)。正の記憶媒体110αであった場合(ステップS503のyesの場合)、すなわち紛失したのが副の記憶媒体110βであった場合、管理サービス装置130は、証明書DB132のユーザリストに記載されている正の記憶媒体110αを所有する利用者の証明書(副)を失効リストに追加し(ステップS504)、証明書(副)に含まれる副の記憶媒体βの公開鍵を削除する(ステップS505)。ステップS502において認証した記憶媒体が正の記憶媒体110αでなかった場合(ステップS503のNoの場合)、すなわち紛失したのが正の記憶媒体110αであった場合、管理サービス装置130は、証明書DB132のユーザリストに記載されている副の記憶媒体110βを所持する利用者の証明書(正)を失効リストに追加し(ステップS506)、証明書(正)に含まれる公開鍵を削除した上で、証明書(副)に含まれる公開鍵を証明書(正)が含む公開鍵として記載する(ステップS507)。その後、証明書(副)が含む公開鍵を削除する(ステップS505)。

[0042] 前記した無効化の具体的な方法のステップS502で行った認証の具体的な方法を、図5に示すフローチャートを用いて説明する。

利用者が通信端末装置120からインターネット140を介して管理サービス装置130に対してサービスを要求した場合、管理サービス装置130によって通信端末装置120に接続している記憶媒体の認証が行われ、記憶媒体を認証することにより、それを所持する利用者が正当であることを確認した後、サービスが提供される。

[0043] 管理サービス装置130は、記憶媒体110が記憶している公開鍵と秘密鍵を用いたPKI(Public Key Infrastructure)の仕組みを利用して、通信端末装置120に接続している記憶媒体110の認証を行う(ステップS401)。管理サービス装置130は、認証が成功したか否かを判断する(ステップS402)。成功したと判断しなかった場合(ステップS402のNoの場合)、管理サービス装置130は、通信端末装置120を介して記憶媒体110の正当性が確認されなかったことにより認証に失敗したことを利用者

に通知し(ステップS403)、処理を終了する。成功したと判断した場合(ステップS402のyesの場合)、管理サービス装置130は、証明書DB132の失効リストを参照して、この記憶媒体110が記憶している公開鍵の証明書の失効状況を取得し(ステップS404)、公開鍵の証明書が失効しているか否かを判断する(ステップS405)。失効していた場合(ステップS405のyesの場合)、管理サービス装置130は、通信端末装置120を介して公開鍵の証明書が失効していることにより認証に失敗したことを利用者に通知し(ステップS403)、処理を終了する。失効していなかった場合(ステップS405のNoの場合)、管理サービス装置130は、証明書DB132のユーザリストを参照し、失効していなかった公開鍵の証明書に対応する利用者のユーザIDを取得する(ステップS406)。その後、管理サービス装置130は、通信端末装置120を介して利用者に対して、認証により、記憶媒体を所持する利用者の正当性が確認されたことを通知する(ステップS407)。

[0044] ここで、ステップS506において証明書DB132のユーザリストからユーザIDを取得しているが、X. 509が規定する証明書が持っている発行先(Subject)の情報をユーザIDとして利用してもよい。

[0045] 前記したPKIの仕組みを利用した認証の具体的な方法を、図6に示すフローチャートを用いて説明する。

通信端末装置120は、管理サービス装置130に対して、接続している記憶媒体110が記憶している公開鍵の証明書(証明書は公開鍵を含む)を送信する(ステップS2101)。管理サービス装置130は、通信端末装置120から受信した公開鍵の証明書の正当性を検証する(ステップS2102)。正当性の検証は、公開鍵の証明書に管理サービス装置の電子署名がなされているか否かにより判断する。正当であると判断されなかった場合(ステップS2102のNoの場合)、不正な証明書であると判断され、処理を終了する。正当であると判断された場合(ステップS2102のyesの場合)、管理サービス装置130は乱数を生成して(ステップS2103)、証明書から取り出した公開鍵を用いて、この乱数を暗号化する(ステップS2104)。管理サービス装置130は、暗号化した乱数を通信端末装置120に送信する(ステップS2105)。管理サービス装置130から暗号化した乱数を受信した通信端末装置120は、接続している記憶媒体

110が記憶している秘密鍵を用いて、暗号化された乱数を復号し、管理サービス装置130に送信する(ステップS2106)。通信端末装置120から復号された乱数を受信した管理サービス装置130は、先に生成した乱数と、受信した復号された乱数を比較し、これらが一致するか否かを判断する(ステップS2107)。一致した場合、正当な記憶媒体110であり、認証は成功する(ステップS2108)。一致しない場合、不正な記憶媒体110と判断されて認証は失敗し、処理を終了する。

[0046] 次に、利用者が所持する正の記憶媒体110αを紛失した場合に、副の記憶媒体110βの権限にもとづいて、鍵管理システムの通信端末装置120が、インターネット140を介して管理サービス装置130に正の記憶媒体110αの無効化を依頼することにより、紛失した正の記憶媒体110αの公開鍵を削除し、紛失した正の記憶媒体110αを利用できなくすることはできるが、正の記憶媒体110αの権限にもとづいて、副の記憶媒体110βを無効化することはできない方法を説明する。

[0047] 管理サービス装置130では、受信部1312が、第2の記憶媒体110βと接続している通信端末装置120から、インターネット140である通信ネットワークを介した第1の記憶媒体110αに関するデータ処理の要求を受信する。受信部1312が、通信端末装置120から、第1の記憶媒体110αに関するデータ処理の要求を受信した場合に、認証部133が、通信端末装置120と接続している第2の記憶媒体110βが正当であるか否かの認証を行う。

[0048] 管理サービス装置130では、証明書データベース132が、第1の記憶媒体110αの公開鍵と第2の記憶媒体110βの公開鍵とを記憶している。受信部1312が、通信端末装置120から、第1の記憶媒体110αの無効化の要求を受信し、認証部133が、通信端末装置120と接続している第2の記憶媒体110βを正当な記憶媒体であると認証した場合に、証明書データベース132は、記憶している第1の記憶媒体110αの公開鍵を削除するが、第2の記憶媒体110βの公開鍵は削除しない。

[0049] 利用者が、通常利用している正の記憶媒体110αを紛失し、それを悪意を持つ第三者が拾得した場合、悪意を持つ第三者は、拾得した正の記憶媒体110αを用いて、不正に副の記憶媒体110βを無効化したり、または、新たな記憶媒体を登録したりすることも考えられる(新たな記憶媒体を登録方法は後述する)。そこで、利用者が

正の記憶媒体110αを紛失した場合に、副の記憶媒体110βは正の記憶媒体110αを無効化することはできるが、正の記憶媒体110αは副の記憶媒体110βを無効化することはできない具体的な方法を図7に示すフローチャートを用いて説明する。

[0050] 利用者または悪意を持つ第三者が、通信端末装置120の入力部124から記憶媒体の無効化を要求する(ステップS701)。通信端末装置120は、管理サービス装置130に対して記憶媒体の無効化の要求を送信し、管理サービス装置130は、図5に示した方法を用いて、通信端末装置120が接続している記憶媒体110の認証を行い、記憶媒体110が正当であるか否かを判断する(ステップS702)。正当でないと判断した場合(ステップS702のNoの場合)、無効化を継続することはできず、処理を終了する。正当であると判断した場合(ステップS702のyesの場合)、管理サービス装置130は、ステップS702で認証した記憶媒体が正の記憶媒体110αであるか否かを判断する(ステップS703)。ステップS702で認証した記憶媒体が正の記憶媒体110αであった場合(ステップS703のyesの場合)、正の記憶媒体110αは副の記憶媒体110βの無効化を継続することはできず、処理を終了する。ステップS702において認証に使用した記憶媒体が正の記憶媒体110αでなかった場合(ステップS703のNoの場合)、管理サービス装置130は、証明書DB132のユーザリストに記載されている副の記憶媒体110βを所持する利用者の証明書(正)を失効リストに追加し(ステップS704)、証明書(正)が含む公開鍵を削除した上で、証明書(副)が含む公開鍵を証明書(正)が含む公開鍵として記載し(ステップS705)、その後、証明書(副)が含む公開鍵を削除する(ステップS706)。

[0051] 次に、記憶媒体を新たに登録する方法について説明する。

管理サービス装置130では、受信部1312が、第2の記憶媒体110βと接続している通信端末装置120から、インターネット140である通信ネットワークを介した第1の記憶媒体110αに関するデータ処理の要求を受信する。受信部1312が、通信端末装置120から、第1の記憶媒体110αに関するデータ処理の要求を受信した場合に、認証部133が、通信端末装置120と接続している第2の記憶媒体110βが正当であるか否かの認証を行う。

[0052] 管理サービス装置130では、証明書データベース132が、第2の記憶媒体110β

の公開鍵を記憶している。受信部1312が、通信端末装置120から、新たな記憶媒体である第3の記憶媒体の登録の要求と、第3の記憶媒体の公開鍵とを受信し、認証部133が通信端末装置120と接続している第2の記憶媒体110βを正当な記憶媒体であると認証した場合に、証明書発行部134は、受信部1312が受信した第3の記憶媒体の公開鍵の正当性を証明する証明書を発行し、証明書データベース132は、受信部1312が受信した第3の記憶媒体の公開鍵と、証明書発行部134が発行した第3の記憶媒体の公開鍵の正当性を証明する証明書とを記憶する。

[0053] 利用者が記憶媒体110αもしくは記憶媒体110βを紛失した際に、新たに購入した記憶媒体を、紛失した記憶媒体110αもしくは記憶媒体110βに替わって使用できるように管理サービス装置に登録する具体的な方法を、図8に示すフローチャートを用いて説明する。なお、以下の説明では、正の記憶媒体110αを紛失したものとし、新たに購入した記憶媒体を記憶媒体110γとして登録する。

[0054] 利用者は記憶媒体110γに生成した公開鍵と秘密鍵を記憶する(ステップS601)。公開鍵と秘密鍵の生成は、例えば、利用者のPC等を利用して行うことができる。利用者は通信端末装置120の入力部124から記憶媒体110γの新規登録の要求を入力し(ステップS602)、記憶媒体110γを通信端末装置120に装着する(ステップS603)。通信端末装置120は、記憶媒体110γが記憶している公開鍵を記憶部123に読み込む(ステップS604)。利用者は記憶媒体110γを通信端末装置120から取り外し、記憶媒体110βを通信端末装置120に装着する(ステップS605)。管理サービス装置130は、図5に示した方法を用いて認証を行い、認証が成功したか否かを判断する(ステップS606)。成功したと判断しなかった場合(ステップS606のNoの場合)、記憶媒体110γの登録を継続することはできず、処理を終了する。成功したと判断した場合(ステップS606yesの場合)、通信端末装置120は、記憶部123に記憶してある記憶媒体110γの公開鍵を管理サービス装置130に送信する(ステップS607)。管理サービス装置130の証明書発行部134は、記憶媒体110γの公開鍵の証明書を作成する(ステップS608)。管理サービス装置130は、証明書発行部134が作成した記憶媒体110γの公開鍵の証明書を、証明書DB132のユーザリストに、証明書(副)として記憶する(ステップS609)。管理サービス装置130は、証明書

発行部134が作成した記憶媒体110γの公開鍵の証明書を、通信端末装置120に送信する(ステップS610)。通信端末装置120は、管理サービス装置130から受信した証明書を記憶部123に記憶する(ステップS611)。利用者は、記憶媒体110βを通信端末装置120から取り外し、記憶媒体110γを通信端末装置120に装着する(ステップS612)。通信端末装置120は、記憶部123に記憶してある証明書を、鍵アクセス部1221を介して記憶媒体110γに書き込む(ステップS613)。

[0055] なお、正の記憶媒体110αではなく、副の記憶媒体110βを紛失した場合も同様である。また、前記した説明においては、記憶媒体の無効化と新たな記憶媒体の登録とを別々に行っていたが、この2つを同時に行ってもよい。また、記憶媒体の無効化と新たな記憶媒体の登録との実行の順序は、どちらを先に行ってもよい。

[0056] この実施の形態によれば、管理サービス装置130は、第1の記憶媒体110αを紛失した場合、第2の記憶媒体110βと接続している通信端末装置120からインターネット140である通信ネットワークを介して、第1の記憶媒体110αの無効化の要求を受信し、通信端末装置120と接続している第2の記憶媒体110βの認証を行い、その正当性を確認した場合、第2の記憶媒体110βの権限にもとづいて証明書データベース132から第1の記憶媒体110αの公開鍵を削除することにより、第1の記憶媒体110αを無効化することができる。これにより、紛失した記憶媒体の無効化をインターネット140である通信ネットワークを介して行うことができる。

[0057] この実施の形態によれば、管理サービス装置130は、第1の記憶媒体110αを紛失した場合、第2の記憶媒体110βと接続している通信端末装置120からインターネット140である通信ネットワークを介して、第1の記憶媒体110αの無効化の要求を受信し、通信端末装置120と接続している第2の記憶媒体110βの認証を行い、その正当性を確認した場合、第2の記憶媒体110βの権限にもとづいて証明書データベース132から第1の記憶媒体110αの公開鍵を削除することにより、第1の記憶媒体110αを無効化することができるが、第1の記憶媒体110αの権限にもとづいて、第2の記憶媒体110βを無効化することはできないようにすることができる。これにより、紛失した第1の記憶媒体110αを拾得した悪意を持つ第三者による、不正な第2の記憶媒体110βの無効化や新たな記憶媒体の登録を防止することができる。

[0058] この実施の形態によれば、管理サービス装置130は、第2の記憶媒体110βと接続している通信端末装置120からインターネット140である通信ネットワークを介して第3の記憶媒体γの登録の要求と第3の記憶媒体γの公開鍵とを受信し、通信端末装置120と接続している第2の記憶媒体110βの認証を行い、第2の記憶媒体110βを正当な記憶媒体であると確認した場合、その権限にもとづいて第3の記憶媒体γの公開鍵の正当性を証明する証明書を発行し、第3の記憶媒体γの公開鍵と証明書発行部が発行した第3の記憶媒体γの公開鍵の正当性を証明する証明書とを記憶することができる。これにより、第3の記憶媒体γの新たな登録をインターネット140である通信ネットワークを介して行うことができる。

[0059] この実施の形態によれば、管理サービス装置130は、第1の記憶媒体110αの公開鍵と第1の記憶媒体110αの公開鍵の正当性を証明する証明書と、第2の記憶媒体110βの公開鍵と第2の記憶媒体110βの公開鍵の正当性を証明する証明書とを記憶する証明書データベース132に、第1の記憶媒体110αの公開鍵と第1の記憶媒体110αの公開鍵の正当性を証明する証明書と、第2の記憶媒体110βの公開鍵と第2の記憶媒体110βの公開鍵の正当性を証明する証明書とを組にして登録することができる。これにより、1人の利用者が所有する2つの記憶媒体を一括して管理することができる。

[0060] この実施の形態によれば、利用者が2枚の記憶媒体を持ち、これら2つのうちいずれかの記憶媒体の公開鍵・秘密鍵によって利用者の認証を行うことにより、記憶媒体を紛失した際や盗難に遭った際の記憶媒体の再発行処理をオンラインで行うことができる。また、紛失もしくは盗難に遭った記憶媒体の無効化を行うことにより、第三者が当該紛失記憶媒体を不正に使用してサービスを利用するのを防止することができる。副の記憶媒体を使用して正の記憶媒体の無効化および新規記憶媒体の登録を行えるようにして、逆に正の記憶媒体を使用して副の記憶媒体の無効化および新規記憶媒体の登録を行えないようにする場合には、正の記憶媒体を不正に取得した第三者によって副の記憶媒体の無効化および新規記憶媒体の登録を行われるのを防ぐことができる。

[0061] 実施の形態2.

以下に述べる実施の形態2では、記憶媒体が記憶しているデータをインターネットを介して受信し、バックアップサービス装置に記憶させてバックアップデータとし、記憶媒体を紛失した場合、他の記憶媒体にバックアップデータを送信してリストアする実施の形態について説明する。

[0062] 図9は実施の形態2における鍵管理システムの構成を示す図である。

実施の形態2における鍵管理システムの構成は、実施の形態1における鍵管理システムの構成に加えて、記憶媒体110が記憶しているデータをインターネット140を介して受信し、バックアップデータとして記憶するバックアップサービス装置710を備えている。

[0063] バックアップサービス装置710は、インターネット140を経由して通信を行う通信部711と、通信端末装置120から送信された記憶媒体110が記憶しているデータを記憶するバックアップ部712と、これらの制御を行う制御部713と、公開鍵の証明書を使って公開鍵を記憶している記憶媒体110の認証を行う認証部714とから構成される。

[0064] 通信部711は、通信端末装置120または管理サービス装置130へデータを送信する送信部7111と、通信端末装置120または管理サービス装置130からデータを受信する受信部7112とから構成される。

[0065] 通信端末装置120は、実施の形態1での構成要素に加えて、指定された時間に指定されたプログラムを起動するタイマー部127を備えている。

また、図示されないバックアッププログラムを備える。バックアッププログラムは、記憶媒体内のデータをバックアップサービス装置710に送信する機能を持つ。バックアッププログラムは、当初より通信端末装置120に内蔵されていてもよいし、記憶媒体110αに記憶されていてもよい。

[0066] 次に、記憶媒体110が記憶しているデータをインターネット140を介してバックアップサービス装置710にバックアップする方法と、バックアップサービス装置710が記憶しているバックアップデータを、インターネット140を介して通信端末装置120に接続している記憶媒体110にリストアする方法を説明する。

[0067] バックアップサービス装置710では、受信部7112が、第1の記憶媒体110αと接

続する通信端末装置120から、インターネット140である通信ネットワークを介して、第1の記憶媒体110αが記憶するデータと、データをバックアップデータとして記憶する要求とを受信する。また、受信部7112が、第2の記憶媒体110βと接続する通信端末装置120から、インターネット140である通信ネットワークを介して、バックアップデータの送信の要求を受信する。受信部7112が、第1の記憶媒体110αと接続する通信端末装置120から、第1の記憶媒体110αが記憶するデータをバックアップデータとして記憶する要求を受信した場合に、認証部714が、通信端末装置120と接続している第1の記憶媒体110αが正当であるか否かの認証を行う。受信部7112が、第2の記憶媒体110βと接続する通信端末装置120から、バックアップデータの送信の要求を受信した場合に、認証部714が、通信端末装置120と接続している第2の記憶媒体110βが正当であるか否かの認証を行う。認証部714が、通信端末装置120と接続している第1の記憶媒体110αを、正当な記憶媒体であると認証した場合に、バックアップ部712は、受信部7112が受信した第1の記憶媒体110αが記憶するデータをバックアップデータとして記憶する。認証部714が、通信端末装置120と接続している第2の記憶媒体110βを正当な記憶媒体であると認証した場合に、送信部7111は、バックアップ部712が記憶しているバックアップデータを、第2の記憶媒体110βと接続している通信端末装置120へインターネット140である通信ネットワークを介して送信する。

[0068] 記憶媒体110α中のデータのバックアップを行う具体的な方法を、図10に示すフローチャートを用いて説明する。

通信端末装置120のタイマー部127が、バックアッププログラムを起動する(ステップS801)。タイマー部127から起動されたバックアッププログラムは、記憶媒体110αからバックアップの対象となるデータを読み出す(ステップS802)。バックアップの対象となるデータは、例えば、前回のバックアップからの差分のみであってもよいし、全体であってもよい。タイマー部127から起動されたバックアッププログラムは、バックアップサービス装置710にバックアップの要求を送信する(ステップS803)。バックアップの要求を受信したバックアップサービス装置710は、通信端末装置120を介して記憶媒体110αの認証を行い(認証の方法は後述する)、認証が成功したか否かを

判断する(ステップS804)。成功したと判断しなかった場合(ステップS804のNoの場合)、バックアップを継続することはできす、処理を終了する。成功したと判断した場合(ステップS804のyesの場合)、タイマー部127から起動されたバックアッププログラムがバックアップの対象となるデータを、バックアップサービス装置710に送信する(ステップS805)。

[0069] 次に、前記したバックアップサービス装置710が行う認証の具体的な方法を、図11に示すフローチャートを用いて説明する。

バックアップサービス装置710は、記憶媒体110が記憶している公開鍵と秘密鍵を用いて、PKI(Public Key Infrastructure)の仕組みを利用して通信端末装置120に接続されている記憶媒体110の認証を行い(ステップS901)、認証が成功したか否かを判断する(ステップS902)。成功したと判断しなかった場合(ステップS902のNoの場合)、認証に失敗したことを利用者に通知し、処理を終了する(ステップS903)。成功したと判断した場合(ステップS902のyesの場合)、バックアップサービス装置710は、管理サービス装置130に記憶媒体110が記憶している公開鍵の証明書の失効状況の調査と、ユーザID取得とを依頼する(ステップS904)。管理サービス装置130は、証明書DB132の失効リストを参照して、証明書の失効状況を取得し(ステップS905)、証明書が失効しているか否かを判断する(ステップS906)。失効していた場合、その旨利用者に通知し、処理を終了する(ステップS903)。失効していなかった場合、管理サービス装置130は、証明書DB132のユーザリストを参照して、証明書に対応する利用者にユーザIDを取得する(ステップS907)。管理サービス装置130は、バックアップサービス装置710にユーザIDを送信する(ステップS908)。バックアップサービス装置710は、利用者に認証成功を通知する(ステップS909)。

[0070] なお、図11に示したバックアップサービス装置710が行う認証の具体的な方法の中で行っているPKIに仕組みを利用して記憶媒体を認証する方法は、図6で示した方法と同じである。

[0071] 記憶媒体110αを紛失して使用できなくなり、バックアップサービス装置710にバックアップしておいたデータを記憶媒体110βにリストアする具体的な方法について、図12に示すフローチャートを用いて説明する。

[0072] 利用者が通信端末装置120の入力部124から、バックアップサービス装置710に対してバックアップデータのリストアを要求する(ステップS1001)。バックアップサービス装置710は、図11に示す方法を用いて通信端末装置120に接続する記憶媒体110βの認証行い、認証が成功したか否かを判断する(ステップS1002)。成功したと判断しなかった場合(ステップS1002のNoの場合)、その旨利用者に通知し、処理を終了する。成功したと判断した場合(ステップS1002のyesの場合)、バックアップサービス装置710はバックアップデータを通信端末装置120に送信する(ステップS1003)。通信端末装置120は記憶媒体110βにデータを書き込む(ステップS1004)。

[0073] この実施の形態によれば、バックアップサービス装置710は、第1の記憶媒体110αと接続している通信端末装置120からのインターネット140である通信ネットワークを介した第1の記憶媒体110αが記憶しているデータのバックアップの要求を受信し、通信端末装置120と接続している第1の記憶媒体110αの認証を行い、第1の記憶媒体110αを正当な記憶媒体であると確認した場合、通信端末装置120から受信した第1の記憶媒体110αが記憶しているデータを記憶することができる。これにより、記憶媒体110αが記憶しているデータをバックアップサービス装置710にバックアップすることができる。

[0074] この実施の形態によれば、バックアップサービス装置710は、第2の記憶媒体110βと接続している通信端末装置120からのインターネット140である通信ネットワークを介したバックアップデータの送信の要求を受信し、通信端末装置120からバックアップデータの送信の要求を受信した場合、通信端末装置120と接続している第2の記憶媒体110βの認証を行い、第2の記憶媒体110βを正当な記憶媒体であると確認した場合、バックアップサービス装置710が記憶しているバックアップデータを通信端末装置120へ送信することができる。これにより、バックアップサービス装置710のバックアップデータを記憶媒体110βにリストアすることができる。

[0075] この実施の形態によれば、バックアップサービス装置710にデータをバックアップすることで第1の記憶媒体110αを紛失した場合、第2の記憶媒体110βにデータをリストアすることができる。リストア時には第2の記憶媒体110βの公開鍵と秘密鍵を使用して、管理サービス装置130との間でPKIの仕組みを用いた認証を行うため、パス

ワードによる認証を行う場合と比較して認証の強度を高くすることができる。

[0076] 実施の形態3.

前記した実施の形態2では、PKIの仕組みを利用して記憶媒体の認証を行う際に、記憶媒体が記憶している公開鍵とその証明書とを、バックアップサービス装置に送信していた。これに対して以下に述べる実施の形態3では、バックアップサービス装置が、当初より公開鍵を記憶しており、その結果、公開鍵の証明書の正当性の検証が不要となる実施の形態について説明する。

[0077] 図13は実施の形態3における鍵管理システムの構成を示す図である。

実施の形態3における鍵管理システムの構成は、実施の形態2における鍵管理システムの構成と同じである。管理サービス装置130も実際には存在するが、ここでは図示しない。

[0078] 実施の形態3におけるバックアップサービス装置710の構成は、実施の形態2のバックアップサービス装置710の構成に加え、さらに、記憶媒体110が記憶している公開鍵を記憶する公開鍵DB715と、公開鍵を使って記憶媒体110の認証を行う認証部716を備えている。

[0079] 記憶媒体110αと記憶媒体110βとは、図14に示すようにそれぞれに固有の秘密鍵のみを記憶している。

[0080] 公開鍵DB715は、ユーザIDと公開鍵との対応を記載したユーザリストを記憶している。図15は公開鍵DB715のユーザリストの例を示す。ユーザIDはシステム全体において利用者を一意に識別するためのIDである。公開鍵(正)は利用者が所有する正の記憶媒体110αの公開鍵であり、公開鍵(副)は利用者が所有する副の記憶媒体110βの公開鍵である。図15において、$K^{\alpha A}_{pub}$は利用者Aの正の記憶媒体の公開鍵を、$K^{\beta A}_{pub}$は利用者Aの副の記憶媒体の公開鍵をそれぞれ表している。利用者Bと利用者Cについても同様である。

[0081] 次に、本実施の形態におけるバックアップとリストアの方法について説明する。

記憶媒体110が記憶しているデータのバックアップおよびバックアップデータの記憶媒体110へのリストアの方法は、その中で実行する認証を除き、実施の形態2と同様である。

[0082] 本実施の形態における認証の方法を図16に示すフローチャートを用いて説明する。

通信端末装置120が、記憶媒体110を所有する利用者のユーザIDをバックアップサービス装置710に送信する(ステップS1401)。バックアップサービス装置710は、通信端末装置120から受信したユーザIDが公開鍵DB715のユーザリストに存在するか否かを確認する(ステップS1402)。存在しない場合(ステップS1402のNoの場合)、バックアップサービス装置710は、利用者に認証が失敗したことを通知し、処理を終了する(ステップS1403)。存在する場合(ステップS1402のyesの場合)、バックアップサービス装置710は、乱数を生成して、それを通信端末装置120に送信する(ステップS1404)。通信端末装置120は、記憶媒体110が記憶している秘密鍵を用いて、バックアップサービス装置710から受信した乱数を暗号化し、それをバックアップサービス装置710に送信する(ステップS1405)。バックアップサービス装置710は、公開鍵DB715からステップS1402で受信したユーザIDに対応する公開鍵(正)と公開鍵(副)とを取得する(ステップS1406)。バックアップサービス装置710は、取得した公開鍵(正)と公開鍵(副)とを使用して、通信端末装置120から受信した暗号化された乱数をそれぞれ復号する(ステップS1407)。バックアップサービス装置は、ステップS1404で生成した乱数と、復号した2つの乱数のそれぞれとを比較し(ステップS1408)、生成した乱数と復号した2つの乱数のそれぞれとが一致したか否かを判断する(ステップS1409)。生成した乱数と復号した2つの乱数のそれぞれとが一致しなかった場合(ステップS1409でNoの場合)、バックアップサービス装置は利用者に認証が失敗したことを通知し、処理を終了する(ステップS1403)。生成した乱数と復号した2つの乱数のいずれかとが一致した場合(ステップS1409でyesの場合)、バックアップサービス装置710は利用者に認証が成功したことを通知する(ステップS1410)。

[0083] この実施の形態によれば、バックアップサービス装置710が、利用者が所有する記憶媒体110の公開鍵を記憶することにより、記憶媒体110を認証する際に、管理サービス装置130による公開鍵の証明書の検証が不要となる。

[0084] 実施の形態4.

前記した実施の形態2と実施の形態3では、記憶媒体が記憶しているデータを平文の状態でバックアップサービス装置にバックアップした。以下に述べる実施の形態4では、図17に示すように、副の記憶媒体βが記憶している公開鍵を正の記憶媒体αに書き込み、それを用いて記憶媒体に格納されているデータを暗号化してネットワークを介してバックアップサービス装置にバックアップし、その後、バックアップデータを復号して、他の記憶媒体にリストアする実施の形態について説明する。

[0085] 実施の形態4における鍵管理システムの構成は、実施の形態2または実施の形態3における鍵管理システムの構成と同じである。

[0086] 通信端末装置120は、図18に示すように、実施の形態2における構成に加えて、第1の記憶媒体が記憶している第2の記憶媒体の公開鍵を用いてバックアップの対象となるデータを暗号化する暗号化部1281と、第2の記憶媒体が記憶している秘密鍵を用いてバックアップデータを復号する復号部1282とを備える。

[0087] 次に、本実施の形態における記憶媒体が記憶しているデータを暗号化してバックアップする方法について説明する。

[0088] 通信端末装置120では、鍵アクセス部1221が、第1の公開鍵と第1の公開鍵に対応する第1の秘密鍵とデータとを記憶している第1の記憶媒体110αと、第2の公開鍵と第2の公開鍵に対応する第2の秘密鍵とデータとを記憶している第2の記憶媒体110βとのいずれかと接続し、第1の記憶媒体110αから第1の公開鍵と第1の秘密鍵との読み出しと第1の記憶媒体110αへの第1の公開鍵と第1の秘密鍵との書き込みとを行い、第2の記憶媒体110βから第2の公開鍵と第2の秘密鍵との読み出しと第2の記憶媒体110βへの第2の公開鍵と第2の秘密鍵との書き込みとを行う。データアクセス部1222が、第1の記憶媒体110αからデータの読み出しと第1の記憶媒体110αへのデータの書き込みと、第2の記憶媒体110βからデータの読み出しと第2の記憶媒体110βへのデータの書き込みとを行う。送信部1211がデータを送信し、受信部1212がデータを受信する。

[0089] 通信端末装置120は、さらに、第2の公開鍵を用いてデータを暗号化する暗号化部1281を備えている。第1の記憶媒体110αは第2の記憶媒体110βの第2の公開鍵を記憶し、鍵アクセス部1221は第1の記憶媒体110αから第2の公開鍵を読み出

し、データアクセス部1222は第1の記憶媒体110αからデータを読み出し、暗号化部1281は第2の公開鍵を用いてデータアクセス部1222が第1の記憶媒体110αから読み出したデータを暗号化し、送信部1211は暗号化部1281が暗号化したデータを送信する。

[0090] 通信端末装置120は、さらに、第2の秘密鍵を用いて暗号化したデータを復号する復号部1282を備えている。受信部1212は暗号化されているデータを受信し、鍵アクセス部1221は第2の記憶媒体110βから第2の秘密鍵を読み出し、復号部1282は受信部1212が受信した暗号化されているデータを第2の秘密鍵を用いて復号し、データアクセス部1222は復号部1282が復号したデータを第2の記憶媒体110βへ書き込む。

[0091] バックアップサービス装置710では、受信部7112が、第1の記憶媒体110αと接続する通信端末装置120から、インターネット140である通信ネットワークを介して、第1の記憶媒体110αが記憶するデータと、データをバックアップデータとして記憶する要求とを受信する。受信部7112が、第1の記憶媒体110αと接続する通信端末装置120から、第1の記憶媒体110αが記憶するデータをバックアップデータとして記憶する要求を受信した場合に、認証部714が、通信端末装置120と接続している第1の記憶媒体110αが正当であるか否かの認証を行う。認証部714が、通信端末装置120と接続している第1の記憶媒体110αを、正当な記憶媒体であると認証した場合に、バックアップ部712は、受信部7112が受信した第1の記憶媒体110αが記憶するデータをバックアップデータとして記憶する。

[0092] その際、バックアップデータは、第1の記憶媒体110αと接続する通信端末装置120により第2の記憶媒体110βの公開鍵を用いて暗号化されている。

[0093] バックアップサービス装置710では、受信部7112が、第2の記憶媒体110βと接続する通信端末装置120から、インターネット140である通信ネットワークを介して、バックアップデータの送信の要求を受信する。受信部7112が、第2の記憶媒体110βと接続する通信端末装置120から、バックアップデータの送信の要求を受信した場合に、認証部714が、通信端末装置120と接続している第2の記憶媒体110βが正当であるか否かの認証を行う。認証部714が、通信端末装置120と接続している

第2の記憶媒体110βを正当な記憶媒体であると認証した場合に、送信部7111は、バックアップ部712が記憶しているバックアップデータを、第2の記憶媒体110βと接続している通信端末装置120へインターネット140である通信ネットワークを介して送信する。

[0094] 通信端末装置120は、バックアップサービス装置710から受信したバックアップデータが第2の記憶媒体110βの公開鍵を用いて暗号化されている場合、第2の記憶媒体110βの秘密鍵を用いて復号する。

[0095] 記憶媒体110が記憶しているデータを暗号化してバックアップサービス装置710にバックアップする具体的な方法を図19に示すフローチャートを用いて説明する。

通信端末装置120のタイマー部127がバックアッププログラムを起動する(ステップS1601)。バックアッププログラムが、記憶媒体110α中のバックアップの対象となるデータを読み出す(ステップS1602)。バックアッププログラムが、記憶媒体110αが記憶している記憶媒体110βの公開鍵を使用してバックアップの対象となるデータを暗号化する(ステップS1603)。バックアッププログラムが、バックアップサービス装置710に対してバックアップの要求をインターネット140を介して送信する(ステップS1604)。通信端末装置120からバックアップの要求を受信したバックアップサービス装置710は、図11または図16に示す方法を用いて通信端末装置に接続している記憶媒体110αの認証を行い、認証が成功したか否かを判断する(ステップS1605)。成功したと判断しなかった場合(ステップS1605のNoの場合)、バックアップを継続することはできず、処理を終了する。成功したと判断した場合(ステップS1605のyesの場合)、バックアッププログラムが、暗号化されたバックアップデータをインターネット140を介してバックアップサービス装置710に送信する(ステップS1606)。

[0096] 次に、バックアップデータを復号して記憶媒体へリストアする方法について説明する。

記憶媒体110αを紛失などして使用できなくなり、バックアップサービス装置710の暗号化したバックアップデータを復号して記憶媒体110βにリストアする具体的な方法を図20に示すフローチャートを用いて説明する。

利用者が通信端末装置120の入力部124からバックアップデータをリストアする要

求を入力する(ステップS1701)。バックアップサービス装置710が、図11または図16に示す方法を用いて、通信端末装置120と接続している記憶媒体110βの認証を行い、認証が成功したか否かを判断する(ステップS1702)。成功したと判断しなかった場合(ステップS1702のNoの場合)、リストアを継続することはできず、処理を終了する。成功したと判断した場合(ステップS1702のyesの場合)、バックアップサービス装置710は、バックアップデータをインターネット140を介して通信端末装置120に送信する(ステップS1703)。バックアップサービス装置710からバックアップデータを受信した通信端末装置120は、記憶媒体110βの秘密鍵を使用してバックアップデータを復号する(ステップS1704)。通信端末装置120は、記憶媒体110βに復号したデータをリストアする(ステップS1705)。

[0097] 実施の形態4では、バックアップする際にデータを記憶媒体110βの公開鍵を用いて暗号化した。しかし、公開鍵を用いて暗号化するかわりに、バックアップに固有の一時的な共通鍵を生成し、それを用いてバックアップするデータを暗号化し、さらに、この共通鍵を記憶媒体110βの公開鍵で暗号化する方法を用いてもよい。この場合、バックアップデータをリストアする際には、記憶媒体110βの秘密鍵を用いて一時的な共通鍵を復号し、復号した共通鍵を用いてバックアップデータを復号して、記憶媒体110βに書き込むこととなる。

[0098] この実施の形態によれば、通信端末装置120は、第1の公開鍵と第1の公開鍵に対応する第1の秘密鍵とデータとを記憶している第1の記憶媒体110αと、第2の公開鍵と第2の公開鍵に対応する第2の秘密鍵とデータとを記憶している第2の記憶媒体110βとのいずれかと接続しており、鍵アクセス部1221が第1の記憶媒体110αから第1の公開鍵と第1の秘密鍵との読み出しと第1の記憶媒体110αへの第1の公開鍵と第1の秘密鍵との書き込みとを行い、第2の記憶媒体110βから第2の公開鍵と第2の秘密鍵との読み出しと第2の記憶媒体110βへの第2の公開鍵と第2の秘密鍵との書き込みとを行い、データアクセス部1222が第1の記憶媒体110αからデータの読み出しと第1の記憶媒体110αへのデータの書き込みと、第2の記憶媒体110βからデータの読み出しと第2の記憶媒体110βへのデータの書き込みとを行い、送信部1211がデータを送信し、受信部がデータを受信することができる。

[0099] この実施の形態によれば、通信端末装置120は、さらに、第2の公開鍵を用いてデータを暗号化する暗号化部1281を備え、第1の記憶媒体110αは第2の記憶媒体110βの第2の公開鍵を記憶していることにより、鍵アクセス部1221は、第1の記憶媒体110αから第2の公開鍵を読み出し、データアクセス部1222は、第1の記憶媒体110αからデータを読み出し、暗号化部1281は第2の公開鍵を用いてデータアクセス部1222が第1の記憶媒体110αから読み出したデータを暗号化し、送信部1211は暗号化部1281が暗号化したデータを送信することができる。

[0100] この実施の形態によれば、通信端末装置120は、さらに、第2の秘密鍵を用いて暗号化したデータを復号する復号部1282とを備えることにより、受信部1212は暗号化されているデータを受信し、鍵アクセス部1221は第2の記憶媒体110βから第2の秘密鍵を読み出し、復号部1282は受信部1212が受信した暗号化されているデータを第2の秘密鍵を用いて復号し、データアクセス部1222は復号部1282が復号したデータを第2の記憶媒体110βへ書き込むことができる。

[0101] この実施の形態によれば、通信端末装置120は、接続している第1の記憶媒体110αから第2の公開鍵の読み出し、接続している第1の記憶媒体110αからのデータの読み出し、読み出した第2の公開鍵を用いて第1の記憶媒体110αから読み出したデータを暗号化し、暗号化したデータを、バックアップデータを記憶するバックアップサービス装置へ送信することができる。これにより、バックアップデータを不正に見られることを防止することができ、さらに、バックアップデータを第2の記憶媒体110βにリストアする際には、第2の記憶媒体110βが記憶している第2の秘密鍵を用いて容易に復号することができる。

[0102] この実施の形態によれば、通信端末装置120は、バックアップデータを記憶しているバックアップサービス装置710から第2の記憶媒体110βが記憶している第2の公開鍵を用いて暗号化した第1の記憶媒体110αのバックアップデータを受信し、接続している第2の記憶媒体110βから第2の秘密鍵を読み出し、受信したバックアップデータを読み出した第2の記憶媒体110β第2の秘密鍵を用いて復号し、復号した第1の記憶媒体110αのバックアップデータを、接続している第2の記憶媒体110βに記憶することができる。これにより、第1の記憶媒体110αを紛失した場合、バック

アップサービス装置710が記憶している暗号化したバックアップデータを復号して、第2の記憶媒体110βに記憶することにより、紛失したデータを容易に復旧することができる。

[0103] この実施の形態によれば、データを記憶媒体110βの公開鍵で暗号化してバックアップサービス装置710にバックアップすることにより、バックアップしたデータは、記憶媒体110βの秘密鍵を記憶している記憶媒体β以外は復号することができず、インターネット140やバックアップサービス装置710等でデータを不正に見られることを防止することができる。

[0104] 実施の形態5.

前記した実施の形態4では、記憶媒体が記憶しているデータを暗号化してバックアップを行った。以下に述べる実施の形態5では、図21に示すように、副の記憶媒体が記憶している公開鍵を正の記憶媒体に書き込み、正の記憶媒体が記憶している公開鍵を副の記憶媒体に書き込んだ後、記憶媒体に格納されているデータに対して、暗号化と共に電子署名を行い、ネットワークを介してバックアップサービス装置にバックアップし、その後、バックアップデータの署名を検証し復号した後、他の記憶媒体にリストアする実施の形態について説明する。

[0105] 実施の形態5における鍵管理システムの構成は、実施の形態2または実施の形態3における鍵管理システムの構成と同じである。

[0106] 通信端末装置120は、図22に示すように、実施の形態2における構成に加えて、第1の記憶媒体110αが記憶している秘密鍵を用いてバックアップの対象となるデータに電子署名を行う電子署名部1291と、記憶部123が記憶している公開鍵を用いてバックアップデータの電子署名を検証する検証部1292とを備える。

[0107] 通信端末装置120では、鍵アクセス部1221が、第1の公開鍵と第1の公開鍵に対応する第1の秘密鍵とデータとを記憶している第1の記憶媒体110αと、第2の公開鍵と第2の公開鍵に対応する第2の秘密鍵とデータとを記憶している第2の記憶媒体110βとのいずれかと接続し、第1の記憶媒体110αから第1の公開鍵と第1の秘密鍵との読み出しと第1の記憶媒体110αへの第1の公開鍵と第1の秘密鍵との書き込みとを行い、第2の記憶媒体110βから第2の公開鍵と第2の秘密鍵との読み出しと

第2の記憶媒体110βへの第2の公開鍵と第2の秘密鍵との書き込みとを行う。データアクセス部1222が、第1の記憶媒体110αからデータの読み出しと第1の記憶媒体110αへのデータの書き込みと、第2の記憶媒体110βからデータの読み出しと第2の記憶媒体110βへのデータの書き込みとを行う。送信部1211がデータを送信し、受信部1212がデータを受信する。

[0108] 通信端末装置120は、さらに、第1の秘密鍵を用いてデータに電子署名する電子署名部1291を備えており、鍵アクセス部1221は第1の記憶媒体110αから第1の秘密鍵を読み出し、データアクセス部1222は第1の記憶媒体110αからデータを読み出し、電子署名部1291は第1の秘密鍵を用いてデータアクセス部1222が第1の記憶媒体110αから読み出したデータに電子署名を行い、送信部1211は電子署名部1291が電子署名したデータを送信する。

[0109] 通信端末装置120は、さらに、第1の公開鍵を用いて電子署名したデータを検証する検証部1292とを備えており、第2の記憶媒体110βは第1の記憶媒体110αの第1の公開鍵を記憶しており、受信部1212は電子署名されているデータを受信し、鍵アクセス部1221は第2の記憶媒体110βから第1の公開鍵を読み出し、検証部1292は受信部1212が受信した電子署名されているデータを第1の公開鍵を用いて検証する。

[0110] 次に、本実施の形態における記憶媒体110が記憶しているデータに電子署名を行い、バックアップする方法について説明する。

バックアップサービス装置710では、受信部7112が、第1の記憶媒体110αと接続する通信端末装置120から、インターネット140である通信ネットワークを介して、第1の記憶媒体110αが記憶するデータと、データをバックアップデータとして記憶する要求とを受信する。受信部7112が、第1の記憶媒体110αと接続する通信端末装置120から、第1の記憶媒体110αが記憶するデータをバックアップデータとして記憶する要求を受信した場合に、認証部714が、通信端末装置120と接続している第1の記憶媒体110αが正当であるか否かの認証を行う。認証部714が、通信端末装置120と接続している第1の記憶媒体110αを、正当な記憶媒体であると認証した場合に、バックアップ部712は、受信部7112が受信した第1の記憶媒体110αが記

憶するデータをバックアップデータとして記憶する。

[0111] その際、バックアップデータは、第1の記憶媒体110αと接続する通信端末装置120により第1の記憶媒体110αの秘密鍵を用いて電子署名されている。

[0112] バックアップサービス装置710では、受信部7112が、第2の記憶媒体110βと接続する通信端末装置120から、インターネット140である通信ネットワークを介して、バックアップデータの送信の要求を受信する。受信部7112が、第2の記憶媒体と接続する通信端末装置120から、バックアップデータの送信の要求を受信した場合に、認証部714が、通信端末装置120と接続している第2の記憶媒体110βが正当であるか否かの認証を行う。認証部714が、通信端末装置120と接続している第2の記憶媒体110βを正当な記憶媒体であると認証した場合に、送信部7111は、バックアップ部712が記憶しているバックアップデータを、第2の記憶媒体110βと接続している通信端末装置120へインターネット140である通信ネットワークを介して送信する。

[0113] 通信端末装置120は、バックアップサービス装置710から受信したバックアップデータが第1の記憶媒体110αの秘密鍵を用いて電子署名されている場合、第1の記憶媒体110αの公開鍵を用いて検証する。

[0114] 記憶媒体110が記憶しているデータに電子署名と暗号化を行い、バックアップサービス装置710にバックアップする具体的な方法を図23に示すフローチャートを用いて説明する。

通信端末装置120のタイマー部127が、バックアッププログラムを起動する(ステップS1901)。バックアッププログラムが、記憶媒体110αからバックアップの対象となるデータを読み出す(ステップS1902)。バックアッププログラムが、記憶媒体110αが記憶している記憶媒体110βの公開鍵を使用してバックアップの対象となるデータを暗号化する(ステップS1903)。バックアッププログラムが、記憶媒体110αが記憶している記憶媒体110αの秘密鍵を使用してバックアップ対象に電子署名を行う(ステップS1904)。バックアッププログラムが、バックアップサービス装置710に対してバックアップの要求をインターネット140を介して送信する(ステップS1905)。バックアップサービス装置710は、図11または図16の方法を用いて通信端末装置120と接続する記憶媒体110αの認証を行い、認証が成功したか否かを判断する(ステップS

1906)。成功したと判断しなかった場合(ステップS1906のNoの場合)、バックアップを継続することはできず、処理を終了する。成功したと判断した場合(ステップS1906のyesの場合)、バックアッププログラムは、暗号化と電子署名を行ったバックアップの対象となるデータをバックアップサービス装置710にインターネット140を介して送信する(ステップS1907)。

[0115] 次に、本実施の形態におけるバックアップデータの電子署名を検証して記憶媒体110へリストアする方法について説明する。

記憶媒体110αを紛失などして使用できなくなり、バックアップサービス装置710の暗号化と電子署名を行ったバックアップデータを電子署名を検証して復号し記憶媒体110βにリストアする具体的な方法を図24に示すフローチャートを用いて説明する。

利用者が通信端末装置120の入力部124からリストアの要求を入力する(ステップS2001)。通信端末装置120は、バックアップサービス装置710に対してインターネット140を介してリストアの要求を送信し、バックアップサービス装置710が、図11または図16の方法を用いて通信端末装置120と接続する記憶媒体110βの認証を行い、認証が成功したか否かを判断する(ステップS2002)。成功したと判断しなかった場合(ステップS2002のNoの場合)、リストアを継続することはできず、処理を終了する。成功したと判断した場合(ステップS2002のyesの場合)、バックアップサービス装置710は、バックアップデータを通信端末装置120に送信する(ステップS2003)。バックアップサービス装置710からバックアップデータを受信した通信端末装置120は、記憶媒体110αの公開鍵を使用して電子署名を検証し(ステップS2004)、署名が正当になされたものであるか否かを判断する(ステップS2005)。検証の結果、正当になされたものであると判断されなかった場合(ステップS2005でNoの場合)、バックアップデータが改竄されている、もしくは不正に生成されたデータであるため、リストアせず、処理を終了する。正当になされたものであると判断された場合(ステップS2005でyesの場合)、通信端末装置120は、記憶媒体110βの秘密鍵を使用してバックアップデータを復号する(ステップS2006)。通信端末装置120は、復号したバックアップデータを記憶媒体110βに書き込む(ステップS2007)。

[0116] この実施の形態によれば、通信端末装置120は、第1の公開鍵と第1の公開鍵に対応する第1の秘密鍵とデータとを記憶している第1の記憶媒体110αと、第2の公開鍵と第2の公開鍵に対応する第2の秘密鍵とデータとを記憶している第2の記憶媒体110βとのいずれかと接続しており、鍵アクセス部1221が第1の記憶媒体110αから第1の公開鍵と第1の秘密鍵との読み出しと第1の記憶媒体110αへの第1の公開鍵と第1の秘密鍵との書き込みとを行い、第2の記憶媒体110βから第2の公開鍵と第2の秘密鍵との読み出しと第2の記憶媒体110βへの第2の公開鍵と第2の秘密鍵との書き込みとを行い、データアクセス部1222が第1の記憶媒体110αからデータの読み出しと第1の記憶媒体110αへのデータの書き込みと、第2の記憶媒体110βからデータの読み出しと第2の記憶媒体110βへのデータの書き込みとを行い、送信部1211がデータを送信し、受信部1212がデータを受信することができる。

[0117] この実施の形態によれば、通信端末装置120は、さらに、第1の秘密鍵を用いてデータに電子署名する電子署名部1291を備えることにより、鍵アクセス部1221は第1の記憶媒体110αから第1の秘密鍵を読み出し、データアクセス部1222は第1の記憶媒体110αからデータを読み出し、電子署名部1291は第1の秘密鍵を用いてデータアクセス部1222が第1の記憶媒体110αから読み出したデータに電子署名を行い、送信部1211は電子署名部1291が電子署名したデータを送信することができる。

[0118] この実施の形態によれば、通信端末装置120は、さらに、第1の公開鍵を用いて電子署名したデータを検証する検証部1292とを備えることにより、第2の記憶媒体110βは第1の記憶媒体110αの第1の公開鍵を記憶しており、受信部1212は電子署名されているデータを受信し、鍵アクセス部1221は第2の記憶媒体110βから第1の公開鍵を読み出し、検証部1292は受信部1212が受信した電子署名されているデータを第1の公開鍵を用いて検証することができる。

[0119] この実施の形態によれば、通信端末装置120は、接続している第1の記憶媒体110αから第1の秘密鍵を読み出し、接続している第1の記憶媒体110αからデータを読み出し、読み出した第1の秘密鍵を用いて第1の記憶媒体110αから読み出したデータに電子署名し、電子署名したデータを、バックアップデータを記憶するバック

アップサービス装置710へ送信することができる。

[0120] この実施の形態によれば、通信端末装置120は、バックアップデータを記憶するバックアップサービス装置710から、第1の記憶媒体110αが記憶している第1の秘密鍵を用いて電子署名したバックアップデータを受信し、接続している第1の記憶媒体110αからの第1の公開鍵を読み出し、読み出した第1の公開鍵を用いて電子署名した第1の記憶媒体110αのバックアップデータの署名を検証し、検証した第1の記憶媒体110αのバックアップデータを、接続している第2の記憶媒体110βに記憶することができる。

[0121] この実施の形態によれば、バックアップサービス装置710にデータを記憶媒体110αの秘密鍵を用いて署名してバックアップすることで、データの生成元は記憶媒体110αの秘密鍵を所持している人ということになり、インターネット140である通信ネットワーク上やバックアップサービス装置710等によるデータの改竄を防ぐことができる。

[0122] 実施の形態6.

前記した実施の形態1から実施の形態5では、事前に外部で生成された公開鍵と秘密鍵を記憶媒体が記憶しており、通信端末装置が記憶媒体から公開鍵と秘密鍵とを読み出して利用していた。以下に述べる実施の形態6では、記憶媒体が公開鍵と秘密鍵を生成する機能と、暗号化と復号を行う機能と、電子署名と検証を行う機能とを有して、外部から秘密鍵を読み出す必要をなくした場合の実施の形態について説明する。

[0123] 図25は実施の形態6における記憶媒体110の構成を示す図である。

記憶媒体110は、外部からのデータの入力と外部へのデータの出力とを行う入出力部111と、秘密鍵と秘密鍵に対応する公開鍵とを生成する鍵生成部112と、公開鍵を用いてデータの暗号化を行う暗号化部113と、秘密鍵を用いて暗号化したデータの復号を行う復号部114と、秘密鍵を用いてデータに電子署名を行う署名部115と、公開鍵を用いて電子署名を行ったデータの検証を行う検証部116との少なくともいずれか一つである処理部を備える。

[0124] 記憶媒体110は、外部から読み出すことができない領域を持ち、ここに秘密鍵を格納する。つまり、外部の機器等は、記憶媒体110から秘密鍵を読み出すことができな

い。

[0125] 前記した実施の形態1から実施の形態5では、秘密鍵を使用して復号や電子署名を行う際には、通信端末装置120が記憶媒体110から秘密鍵を読み出して、秘密鍵を使用した復号と電子署名を行っていた。

[0126] 本実施の形態では、記憶媒体110の鍵生成部112が、秘密鍵と公開鍵とを生成する。記憶媒体110がデータを暗号化する際には、暗号化部113が、公開鍵を用いてデータの暗号化を行い、暗号化したデータを復号する際には、記憶媒体110の復号部114が、秘密鍵を用いて暗号化したデータの復号を行う。また、記憶媒体110がデータの電子署名する際には、署名部115が、秘密鍵を用いてデータに電子署名を行い、記憶媒体110がデータの電子署名を検証する際には、検証部116が、公開鍵を用いて電子署名を行ったデータの検証を行う。なお、秘密鍵は、外部から読み出すことができない領域に、公開鍵は、外部から読み出すことができる領域に記憶する。

[0127] その結果、記憶媒体110で生成された秘密鍵は記憶媒体110から取り出すことなく、秘密鍵を用いた演算が必要な際には、通信端末装置120がデータを記憶媒体110に書き込んで、記憶媒体110の内部で暗号化や復号化等を行い、その結果を通信端末装置120が読み出す。

[0128] 例えば、図23のステップS1904では、バックアッププログラムが記憶媒体110αが記憶している秘密鍵を使用してバックアップの対象となるデータに署名しているが、本実施の形態では、この処理は図26に示すフローチャートのようになる。

[0129] 通信端末装置120内のタイマー部127から起動されたバックアッププログラムが、バックアップの対象となるデータのハッシュ値を作成する(ステップS2401)。バックアッププログラムは、作成したハッシュ値を引数として、記憶媒体110αに署名を依頼する(ステップS2402)。記憶媒体110αは、記憶している秘密鍵を使用して電子署名を行い、その結果をバックアッププログラムが読み出す(ステップS2403)。この処理過程においては、秘密鍵は記憶媒体110の内部から一切外部に出ていない。

[0130] この実施の形態によれば、記憶媒体110は、入出力部111による外部からのデータの入力と外部へのデータの出力と、鍵生成部112による秘密鍵と秘密鍵に対応する公開鍵との生成と、暗号化部113による公開鍵を用いたデータの暗号化と、復号

部114による秘密鍵を用いた暗号化したデータの復号と、署名部115による秘密鍵を用いたデータへの電子署名と、検証部116による公開鍵を用いた電子署名を行ったデータの検証を行うとの少なくともいずれか一つを実行することができる。

[0131] 記憶媒体110は、外部から秘密鍵を読み出すことができないようにすることにより、秘密鍵の漏洩を防止することができる。

[0132] この実施の形態によれば、記憶媒体110が公開鍵と秘密鍵を生成する機能と、暗号化と復号を行う機能と、電子署名と検証を行う機能とを有して、外部から秘密鍵を読み出す必要をなくすことにより、秘密鍵は常にその記憶媒体から外部に出ることがなくなり、データの完全性、秘匿性を高めることができる。また、利用者は、鍵生成とその管理のためにPC等の機器を保持する必要がなくなる。

[0133] 実施の形態7.

前記した実施の形態6は、記憶媒体が公開鍵と秘密鍵を生成する機能と、暗号化と復号を行う機能と、電子署名と検証を行う機能とを有して、外部から秘密鍵を読み出す必要をなくした場合の実施の形態であったが、実施の形態7では、前記した実施の形態6に加えて、記憶媒体110が、データの書き込みと読み出しと、公開鍵と秘密鍵の生成と、暗号化と復号と、電子署名と検証との要求に対して、それらを要求した利用者の認証を行い、利用者が正当であると確認された場合のみ、これらを実行する実施の形態について説明する。

[0134] 図27は実施の形態7における記憶媒体110の構成を示す図である。

実施の形態7における記憶媒体は、実施の形態6の構成に加えて、さらに、記憶媒体の利用者が正当であるか否かの認証を行う利用者認証部117とを備えており、利用者認証部117が利用者を正当な利用者であると認証した場合に、記憶媒体110が備える処理部の動作を実行する。

[0135] この実施の形態では、データの書き込みと読み出しと、公開鍵と秘密鍵の生成と、暗号化と復号と、電子署名と検証とを実行する前に、記憶媒体110が、これらの実行を要求した利用者に認証情報の入力を要求する。

[0136] 認証情報としては、例えば、PIN(Personal Identification Number)や指紋の特徴量などが考えられるが、ここでは特に限定しない。記憶媒体110が記憶している

認証情報と、利用者が通信端末装置120の入力部124から入力した認証情報とが一致した場合にのみ、記憶媒体110は前記した機能を実行する。

[0137] 認証情報は、記憶媒体110の機能を利用する際に、毎回利用者が明示的に入力してもよいし、また、一定時間や一定回数などの条件に応じて、通信端末装置120の記憶部123に保存し、一度利用者が入力したら通信端末装置120が自動的に記憶媒体110に渡すようにしてもよい。

[0138] この実施の形態によれば、記憶媒体110は、さらに、記憶媒体110の利用者が正当であるか否かの認証を行う利用者認証部117とを備えることにより、利用者認証部117が利用者を正当な利用者であると認証した場合に、記憶媒体110が備える処理部の動作を実行することができる。

[0139] 以上のように、認証情報を知らない、もしくは持っていない第三者は、記憶媒体110を利用できないため、よりセキュリティを高めることができる。例えば、通常使用していない副の記憶媒体110βが盗難に遭った場合でも、第三者はこれを使用できないため、副の記憶媒体110βを使用して正の記憶媒体110αを無効化するといった不正利用を防止することができる。

[0140] 実施の形態8.

前記した実施の形態1から実施の形態7では、1人の利用者が2枚の記憶媒体110を持つことで紛失に備えていた。以下に述べる実施の形態8では、証明書DB132において1人の利用者が保有する記憶媒体の数を2枚以上のM枚とし、M枚をM以下のN人で所持することで、匿名でサービスを利用する実施の形態について説明する。

[0141] 管理サービス装置130は、記憶媒体110の公開鍵と公開鍵の正当性を証明する証明書とを記憶する証明書データベース132を備え、証明書データベース132は複数の記憶媒体110の公開鍵と複数の公開鍵の正当性を証明する証明書とをグループにして記憶し、認証部133はグループに属する少なくともいずれか1つの公開鍵を用いて記憶媒体110が正当であるか否かの認証を行い、記憶媒体110を正当な記憶媒体であると認証した場合に、記憶媒体110をグループに属する記憶媒体であると認証する。

[0142] この実施の形態では、管理サービス装置130の証明書DB132は、図28に示すように、1つのユーザIDに対して2つ以上の複数の証明書を保持している。これらの証明書に対応する記憶媒体110を、図29に示すように複数の利用者が所持すると仮定すると、「ユーザID」が表す「利用者」は仮想的な利用者であり、実際には同じユーザIDを共有するグループであると考えられる。

[0143] この実施の形態における利用者の認証の動作は図11と同様である。図28では3人の利用者が、それぞれ証明書α_A、β_A、γ_Aに対応する記憶媒体110を使用してバックアップサービス装置にアクセスしている(ステップS1101からステップS1103)。バックアップサービス装置710から管理サービス装置130に対して失効状況調査とユーザID取得を依頼する(ステップS1104)。このとき利用者によって証明書α_A、β_A、γ_Aのいずれかがバックアップサービス装置710から管理サービス装置130に送信される。管理サービス装置130は認証の結果としては認証失敗、またはユーザIDを返す(ステップS1105からステップS1108)。このとき、どの利用者についてもユーザID「A」がバックアップサービス装置に返却される。証明書の中に個人を特定する情報が含まれていなければ、バックアップサービス装置から見ると、その証明書を持っている人物であるということ以外は特定できず、PKIの仕組みを使用した認証を行いながら匿名性を確保することができる。

[0144] なお、本実施の形態においては実施の形態4のように公開鍵を用いて暗号化しても対応する秘密鍵を共有できないためにバックアップサービス装置にバックアップする際に公開鍵を用いて暗号化する方法は使用できない。しかし、認証に使用する公開鍵と秘密鍵とは別に、グループで共有する、暗号化のために公開鍵と秘密鍵を持つことによって、同様のことを実現できる。実施の形態5における署名も同様である。

[0145] この実施の形態によれば、管理サービス装置130は、記憶媒体110の公開鍵と公開鍵の正当性を証明する証明書とを記憶する証明書データベース132を備え、証明書データベース132は複数の記憶媒体110の公開鍵と複数の公開鍵の正当性を証明する証明書とをグループにして記憶し、認証部133はグループに属する少なくともいずれか1つの公開鍵を用いて記憶媒体110が正当であるか否かの認証を行い、記憶媒体110を正当な記憶媒体であると認証した場合に、記憶媒体110をグループに

属する記憶媒体であると認証することができる。

[0146] この実施の形態によれば、複数の利用者が同一のユーザIDに対応した記憶媒体110を所持することで、特定のグループに所属した利用者にのみ、その利用者が誰であるかを特定することなく情報を開示するようなサービスを提供することが可能となる。

[0147] 以上、鍵管理システムでの通信端末装置と管理サービス装置とバックアップサービス装置の実施の形態について述べた。

鍵管理システムは、第1の秘密鍵および第1の秘密鍵に対応する第1の公開鍵の証明書を格納した第1の記憶媒体と、第2の秘密鍵および第2の秘密鍵に対応する第2の公開鍵に関する証明書を格納した第2の記憶媒体と、第1の公開鍵の証明書および第2の公開鍵の証明書を生成する機能と、証明書の正当性を検証する機能と、第1の公開鍵の証明書および第2の公開鍵の証明書を対で記憶し、第1の公開鍵または第2の公開鍵を用いて、対応する秘密鍵を用いて生成された電子署名の正当性を調べることで第1および第2の記憶媒体の所有者であるところの利用者の認証を行う機能を持つ管理サービス装置と、第1の記憶媒体または第2の記憶媒体を装着し、記憶媒体の所有者であるところの利用者の認証を行う機能と管理サービス装置と通信手段を介して通信を行う機能を持つ端末装置とを備えてもよい。

[0148] 管理サービス装置は、第2の公開鍵を用いて利用者の認証を行った後に、利用者からの第1の記憶媒体の無効化要求を受信した際には、第1の公開鍵を無効化し、以後に第1の記憶媒体についての認証要求を受信すると認証に失敗する、もしくは、第1の公開鍵を用いて利用者の認証を行った後に、利用者からの第2の記憶媒体の無効化要求を受信し、第2の公開鍵を無効化し、以後に第2の記憶媒体についての認証要求を受信すると認証に失敗することとしてもよい。

[0149] 管理サービスは、第1の公開鍵を正の公開鍵とし第2の公開鍵を副の公開鍵としてこれらの公開鍵を対で記憶し、第2の記憶媒体を用いて利用者の認証を行った後にのみ利用者からの第1の記憶媒体の無効化要求を受付け、第1の記憶媒体を用いてユーザ認証を行った後の利用者からの第2の記憶媒体の無効化要求はこれを受付けないこととしてもよい。

[0150] 管理サービス装置は、第2の記憶媒体を用いて利用者の認証を行い、利用者から

第3の公開鍵および第3の公開鍵に対応する第3の秘密鍵を格納した第3の記憶媒体の登録要求を受信し、利用者から第3の秘密鍵に対応する公開鍵を受信し、第3の公開鍵の証明書を生成し、受信した第3の公開鍵のを第2の公開鍵の証明書と第3の公開鍵の証明書とを対で記憶し、第3の公開鍵の証明書を利用者に送信し、以降は第3の公開鍵を用いた認証の要求を受信すると認証に成功することとしてもよい。

[0151] 管理サービス装置により認証された利用者からのデータを受信して保存し、後に利用者から要求があった際にデータを利用者に送信するバックアップサービス装置を備えることとしてもよい。

[0152] 第1の記憶媒体は第2の公開鍵を格納し、第1の記憶媒体に格納された第2の公開鍵を用いて第1の記憶媒体に格納されたデータを暗号化した上でバックアップサービス装置に送信し、バックアップサービス装置は暗号化されたデータを保存し、後に第2の記憶媒体にリストアした暗号化されたデータは第2の秘密鍵を使って復号化することとしてもよい。

[0153] 第2の記憶媒体は、第1の公開鍵を格納し、第1の記憶媒体に格納された第1の秘密鍵を用いて、第1の記憶媒体に格納されたデータに署名を行った上で、バックアップサービス装置に送信して保存し、後に第2の記憶媒体にリストアした署名されたデータは、第1の公開鍵を使って検証することとしてもよい。

[0154] 第1の記憶媒体および第2の記憶媒体は公開鍵と秘密鍵のペアを生成する機能と、秘密鍵を用いて暗号化・復号化する機能と、秘密鍵を外部から取り出すことができないようにする機能と、を持つこととしてもよい。

[0155] 第1の記憶媒体および第2の記憶媒体は、データの格納または取り出しまたは公開鍵と秘密鍵のペアの生成または秘密鍵を用いた暗号化・復号化の要求があった際には利用者の認証を行い、認証に成功したときのみデータの格納または取り出しまたは公開鍵と秘密鍵のペアの生成または秘密鍵を用いた暗号化・復号化を行う機能を持つこととしてもよい。

[0156] 管理サービス装置が管理する1人の利用者に対応する記憶媒体の公開鍵の証明書は2つ以上の任意個数であり、これら複数の記憶媒体を記憶媒体の個数以下であ

る任意人数の利用者が各自1枚以上所有することによって、任意人数の利用者を管理サービス装置は1人の利用者とみなし、利用者が匿名でサービスを利用できることとしてもよい。

[0157] 以上、実施の形態1から実施の形態8までにおいて述べた鍵管理システムの通信端末装置と管理サービス装置とバックアップサービス装置とは、コンピュータにより実現することができる。図30は、実施の形態1から実施の形態8までにおいて述べた鍵管理システムの通信端末装置と管理サービス装置とバックアップサービス装置とを、コンピュータを用いて実現した場合のハードウェア構成を示す図である。

[0158] 通信端末装置120と管理サービス装置130と、バックアップサービス装置とは、プログラムを実行するCPU(Central Processing Unit)911を備えている。CPU911は、バス912を介してROM913、RAM914、通信ボード915、表示装置901、キーボード(K/B)902、マウス903、FDD(Flexible Disk Drive)904、磁気ディスク装置920、CDD(Compact Disk Drive)905、プリンタ装置906、スキャナ装置907と接続されている。

[0159] RAM914は、揮発性メモリの一例である。ROM913、FDD904、CDD905、磁気ディスク装置920は、不揮発性メモリの一例である。これらは、記憶部の一例である。

[0160] 通信ボード915は、FAX機、電話器、LAN等に接続されている。例えば、通信ボード915、K/B902、FDD904、スキャナ装置907などは、入力部の一例である。また、例えば、表示装置901などは表示部の一例である。

[0161] 磁気ディスク装置920には、オペレーティングシステム(OS)921、ウィンドウシステム922、プログラム群923、ファイル群924が記憶されている。プログラム群923は、CPU911、OS921、ウィンドウシステム922により実行される。

[0162] 上記プログラム群923には、各機能を実行するプログラムが記憶されている。プログラムは、CPU911により読み出され実行される。ファイル群924には、各ファイルが記憶されている。また、前記した実施の形態で説明したフローチャートの矢印の部分は主としてデータの入出力を示し、そのデータの入出力のためにデータは、磁気ディスク装置920、FD(Flexible Disk)、光ディスク、CD(Compact Disk)、MD(Mini

Disk)、DVD(Digital Versatile Disk)等のその他の記憶媒体に記録される。あるいは、信号線やその他の伝送媒体により伝送される。

[0163] また、通信端末装置120と管理サービス装置130と、バックアップサービス装置とは、ROM913に記憶されたファームウェアで実現されていても構わない。或いは、ソフトウェアのみ、或いは、ハードウェアのみ、或いは、ソフトウェアとハードウェアとの組み合わせ、さらには、ファームウェアとの組み合わせで実施されても構わない。

[0164] また、プログラムは、また、磁気ディスク装置920、FD(Flexible Disk)、光ディスク、CD(Compact Disk)、MD(Mini Disk)、DVD(Digital Versatile Disk)等のその他の記憶媒体による記録装置を用いて記憶されても構わない。

図面の簡単な説明

[0165] [図1]実施の形態1における鍵管理システムの構成を示す図である。

[図2]正の記憶媒体と副の記憶媒体とが記憶する秘密鍵と秘密鍵に対応する公開鍵とを示す図である。

[図3]実施の形態1における証明書DBが記憶しているユーザリストの例を示す図である。

[図4]実施の形態1における記憶媒体を無効化する具体的な方法を示すフローチャートである。

[図5]実施の形態1における認証の具体的な方法を示すフローチャートである。

[図6]実施の形態1におけるPKIの仕組みを利用した認証の具体的な方法を示すフローチャートである。

[図7]実施の形態1における正の記憶媒体を紛失した場合に副の記憶媒体は正の記憶媒体を無効化することはできるが、正の記憶媒体は副の記憶媒体を無効化することはできない具体的な方法を示すフローチャートである。

[図8]実施の形態1における新たな記憶媒体を管理サービス装置に登録する具体的な方法を示すフローチャートである。

[図9]実施の形態2における鍵管理システムの構成を示す図である。

[図10]実施の形態2における記憶媒体のデータのバックアップを行う具体的な方法を示すフローチャートである。

[図11]実施の形態2におけるバックアップサービス装置が行う認証の具体的な方法を示すフローチャートである。

[図12]実施の形態2におけるバックアップサービス装置にバックアップしておいたデータを記憶媒体にリストアする具体的な方法示すフローチャートである。

[図13]実施の形態3における鍵管理システムの構成を示す図である。

[図14]実施の形態3における正に記憶媒体と副の記憶媒体とが記憶している固有の秘密鍵を示す図である。

[図15]実施の形態3における公開鍵DBが記憶しているユーザリストの例を示す図である。

[図16]実施の形態3における認証の方法を示すフローチャートである。

[図17]実施の形態4における副の記憶媒体が記憶している公開鍵を正の記憶媒体に書き込む図である。

[図18]実施の形態4における鍵管理システムの構成を示す図である。

[図19]実施の形態4における記憶媒体が記憶しているデータを暗号化してバックアップサービス装置にバックアップする具体的な方法を示すフローチャートである。

[図20]バックアップサービス装置の暗号化したバックアップデータを復号して記憶媒体にリストアする具体的な方法を示すフローチャートである。

[図21]実施の形態5における副の記憶媒体が記憶している公開鍵を正の記憶媒体に書き込み、正の記憶媒体が記憶している公開鍵を副の記憶媒体に書き込む図である。

[図22]実施の形態5における鍵管理システムの構成を示す図である。

[図23]実施の形態5における記憶媒体が記憶しているデータに電子署名と暗号化を行い、バックアップサービス装置にバックアップする具体的な方法を示すフローチャートである。

[図24]実施の形態5におけるバックアップサービス装置の暗号化と電子署名を行ったバックアップデータを電子署名を検証して復号し記憶媒体にリストアする具体的な方法を示すフローチャートである。

[図25]実施の形態6における記憶媒体の構成を示す図である。

[図26]実施の形態6におけるバックアップの対象となるデータへの署名を示すフローチャートである。

[図27]実施の形態7における記憶媒体の構成を示す図である。

[図28]実施の形態8における証明書DBが記憶しているユーザリストの例を示す図である。

[図29]実施の形態8における記憶媒体を複数の利用者が所持する場合の利用形態を示す図である。

[図30]各実施の形態における通信端末装置と管理サービス装置とバックアップサービス装置とをコンピュータを用いて実現した場合のハードウェア構成を示す図である。

符号の説明

[0166] 110, 110α, 110β, 110γ 記憶媒体、111 入出力部、112 鍵生成部、113 暗号化部、114 復号部、115 署名部、116 検証部、117 利用者認証部、120 通信端末装置、121 通信部、1211 送信部、1212 受信部、122 アクセス部、1221 鍵アクセス部、1222 データアクセス部、123 記憶部、124 入力部、125 表示部、126 制御部、127 タイマー部、1281 暗号化部、1282 復号部、1291 電子署名部、1292 検証部、130 管理サービス装置、131 通信部、1311 送信部、1312 受信部、132 証明書データベース(DB)、133 認証部、134 証明書発行部、135 制御部、140 インターネット、710 バックアップサービス装置、711 通信部、7111 送信部、7112 受信部、712 バックアップ部、713 制御部、714 認証部、715 公開鍵データベース(DB)、901 表示装置、902 キーボード(K/B)、903 マウス、904 FDD、905 CDD、906 プリンタ装置、907 スキャナ装置、911 CPU、912 バス、913 ROM、914 RAM、915 通信ボード、920 磁気ディスク装置、921 OS、922 ウィンドウシステム、923 プログラム群、924 ファイル群。

請求の範囲

[1] 第2の記憶媒体と接続している通信端末装置から通信ネットワークを介した第1の記憶媒体に関するデータ処理の要求を受信する受信部と、

前記受信部が前記通信端末装置から第1の記憶媒体に関するデータ処理の要求を受信した場合に、前記通信端末装置と接続している第2の記憶媒体が正当であるか否かの認証を行う認証部と

を備えることを特徴とする管理サービス装置。

[2] 前記管理サービス装置は、さらに

前記第1の記憶媒体の公開鍵と前記第2の記憶媒体の公開鍵とを記憶するデータベースを備え、

前記受信部が前記通信端末装置から第1の記憶媒体の無効化の要求を受信し、前記認証部が前記通信端末装置と接続している第2の記憶媒体を正当な記憶媒体であると認証した場合に、

前記データベースは記憶している第1の記憶媒体の公開鍵を削除する

ことを特徴とする請求項1に記載の管理サービス装置。

[3] 前記管理サービス装置は、さらに

前記第1の記憶媒体の公開鍵と前記第2の記憶媒体の公開鍵とを記憶するデータベースを備え、

前記受信部が前記通信端末装置から第1の記憶媒体の無効化の要求を受信し、前記認証部が前記通信端末装置と接続している第2の記憶媒体を正当な記憶媒体であると認証した場合に、

前記データベースは記憶している第1の記憶媒体の公開鍵を削除するが、第2の記憶媒体の公開鍵は削除しない

ことを特徴とする請求項1に記載の管理サービス装置

[4] 前記管理サービス装置は、さらに

前記第2の記憶媒体の公開鍵を記憶するデータベースと、

前記第2の記憶媒体の公開鍵の正当性を証明する証明書を発行する証明書発行部とを備え、

前記受信部が前記通信端末装置から新たな記憶媒体である第3の記憶媒体の登録の要求と第3の記憶媒体の公開鍵とを受信し、前記認証部が前記通信端末装置と接続している第2の記憶媒体を正当な記憶媒体であると認証した場合に、

前記証明書発行部は前記受信部が受信した第3の記憶媒体の公開鍵の正当性を証明する証明書を発行し、

前記データベースは前記受信部が受信した第3の記憶媒体の公開鍵と前記証明書発行部が発行した第3の記憶媒体の公開鍵の正当性を証明する証明書とを記憶する

ことを特徴とする請求項1に記載の管理サービス装置。

[5] 前記管理サービス装置は、

前記第1の記憶媒体の公開鍵と第1の記憶媒体の公開鍵の正当性を証明する証明書と、前記第2の記憶媒体の公開鍵と第2の記憶媒体の公開鍵の正当性を証明する証明書とを記憶するデータベースを備え、

前記データベースは前記第1の記憶媒体の公開鍵と第1の記憶媒体の公開鍵の正当性を証明する証明書と、前記第2の記憶媒体の公開鍵と第2の記憶媒体の公開鍵の正当性を証明する証明書とを組にして登録すること

を特徴とする請求項1に記載の管理サービス装置。

[6] 前記管理サービス装置は、

前記記憶媒体の公開鍵と公開鍵の正当性を証明する証明書とを記憶するデータベースを備え、

前記データベースは複数の記憶媒体の公開鍵と複数の公開鍵の正当性を証明する証明書とをグループにして記憶し、

前記認証部は前記グループに属する少なくともいずれか1つの公開鍵を用いて記憶媒体が正当であるか否かの認証を行い、記憶媒体を正当な記憶媒体であると認証した場合に、

前記記憶媒体を前記グループに属する記憶媒体であると認証すること

を特徴とする請求項1に記載の管理サービス装置。

[7] 第1の記憶媒体と接続する通信端末装置から通信ネットワークを介して第1の記憶

媒体が記憶するデータと前記データをバックアップデータとして記憶する要求とを受信し、

第2の記憶媒体と接続する通信端末装置から通信ネットワークを介してバックアップデータの送信の要求を受信する受信部と、

前記受信部が第1の記憶媒体と接続する通信端末装置から第1の記憶媒体が記憶するデータをバックアップデータとして記憶する要求を受信した場合に、前記通信端末装置と接続している第1の記憶媒体が正当であるか否かの認証を行い、

前記受信部が第2の記憶媒体と接続する通信端末装置からバックアップデータの送信の要求を受信した場合に、前記通信端末装置と接続している第2の記憶媒体が正当であるか否かの認証を行う認証部と、

前記認証部が前記通信端末装置と接続している第1の記憶媒体を正当な記憶媒体であると認証した場合に、前記受信部が受信した第1の記憶媒体が記憶するデータをバックアップデータとして記憶するバックアップ部と

前記認証部が前記通信端末装置と接続している第2の記憶媒体を正当な記憶媒体であると認証した場合に、前記バックアップ部が記憶しているバックアップデータを第2の記憶媒体と接続している通信端末装置へ通信ネットワークを介して送信する送信部と

を備えることを特徴とするバックアップサービス装置。

[8] 前記バックアップデータは、

前記第1の記憶媒体と接続する通信端末装置により第2の記憶媒体の公開鍵を用いて暗号化されていること

を特徴とする請求項7に記載のバックアップサービス装置。

[9] 前記バックアップデータは、

前記第1の記憶媒体と接続する通信端末装置により第1の記憶媒体の秘密鍵を用いて電子署名されていること

を特徴とする請求項7に記載のバックアップサービス装置。

[10] 第1の公開鍵と第1の公開鍵に対応する第1の秘密鍵とデータとを記憶している第1の記憶媒体と、第2の公開鍵と第2の公開鍵に対応する第2の秘密鍵とデータとを記

憶している第2の記憶媒体とのいずれかと接続し、

前記第1の記憶媒体から第1の公開鍵と第1の秘密鍵との読み出しと前記第1の記憶媒体への第1の公開鍵と第1の秘密鍵との書き込みとを行い、前記第2の記憶媒体から第2の公開鍵と第2の秘密鍵との読み出しと前記第2の記憶媒体への第2の公開鍵と第2の秘密鍵との書き込みとを行う鍵アクセス部と、

前記第1の記憶媒体からデータの読み出しと前記第1の記憶媒体へのデータの書き込みと、前記第2の記憶媒体からデータの読み出しと前記第2の記憶媒体へのデータの書き込みとを行うデータアクセス部と、

前記鍵アクセス部が前記第1の記憶媒体から読み出した第1の公開鍵と第1の秘密鍵と、前記鍵アクセス部が前記第2の記憶媒体から読み出した第2の公開鍵と第2の秘密鍵とを記憶する記憶部と、

データを送信する送信部と、

データを受信する受信部と

を備えることを特徴とする通信端末装置。

[11] 前記通信端末装置は、さらに

前記第2の公開鍵を用いてデータを暗号化する暗号化部を備え、

前記第1の記憶媒体は前記第2の記憶媒体の第2の公開鍵を記憶しており、

前記鍵アクセス部は、前記第1の記憶媒体から第2の公開鍵を読み出して前記記憶部に記憶し、

前記データアクセス部は、前記第1の記憶媒体からデータを読み出し、

前記暗号化部は前記記憶部が記憶している第2の公開鍵を用いて前記データアクセス部が前記第1の記憶媒体から読み出したデータを暗号化し、

前記送信部は前記暗号化部が暗号化したデータを送信する

ことを特徴とする請求項10に記載の通信端末装置。

[12] 前記通信端末装置は、さらに

前記第2の秘密鍵を用いて暗号化したデータを復号する復号部とを備え、

前記受信部は暗号化されているデータを受信し、

前記鍵アクセス部は前記第2の記憶媒体から第2の秘密鍵を読み出して前記記憶

部に記憶し、

前記復号部は前記受信部が受信した暗号化されているデータを前記記憶部が記憶している第2の秘密鍵を用いて復号し、

前記データアクセス部は前記復号部が復号したデータを第2の記憶媒体へ書き込む

ことを特徴とする請求項10に記載の通信端末装置。

[13] 前記通信端末装置は、さらに

前記第1の秘密鍵を用いてデータに電子署名する電子署名部を備え、

前記鍵アクセス部は前記第1の記憶媒体から第1の秘密鍵を読み出して前記記憶部に記憶し、

前記データアクセス部は前記第1の記憶媒体からデータを読み出し、

前記電子署名部は前記記憶部が記憶している第1の秘密鍵を用いて前記データアクセス部が前記第1の記憶媒体から読み出したデータに電子署名を行い、

前記送信部は前記電子署名部が電子署名したデータを送信する

ことを特徴とする請求項10に記載の通信端末装置。

[14] 前記通信端末装置は、さらに

前記第1の公開鍵を用いて電子署名したデータを検証する検証部とを備え、

前記第2の記憶媒体は前記第1の記憶媒体の第1の公開鍵を記憶しており、

前記受信部は電子署名されているデータを受信し、

前記鍵アクセス部は前記第2の記憶媒体から第1の公開鍵を読み出して前記記憶部に記憶し、

前記検証部は前記受信部が受信した電子署名されているデータを前記記憶部が記憶している第1の公開鍵を用いて検証する

ことを特徴とする請求項10に記載の通信端末装置。

[15] 外部からのデータの入力と外部へのデータの出力とを行う入出力部と、

秘密鍵と秘密鍵に対応する公開鍵とを生成する鍵生成部と、

公開鍵を用いてデータの暗号化を行う暗号化部と、

秘密鍵を用いて暗号化したデータの復号を行う復号部と、

秘密鍵を用いてデータに電子署名を行う署名部と、

公開鍵を用いて電子署名を行ったデータの検証を行う検証部と

の少なくともいずれか一つである処理部を備えることを特徴とする記憶媒体。

[16] 前記記憶媒体は、さらに

前記記憶媒体の利用者が正当であるか否かの認証を行う利用者認証部とを備え、

前記利用者認証部が前記利用者を正当な利用者であると認証した場合に、

前記記憶媒体が備える処理部の動作を実行すること

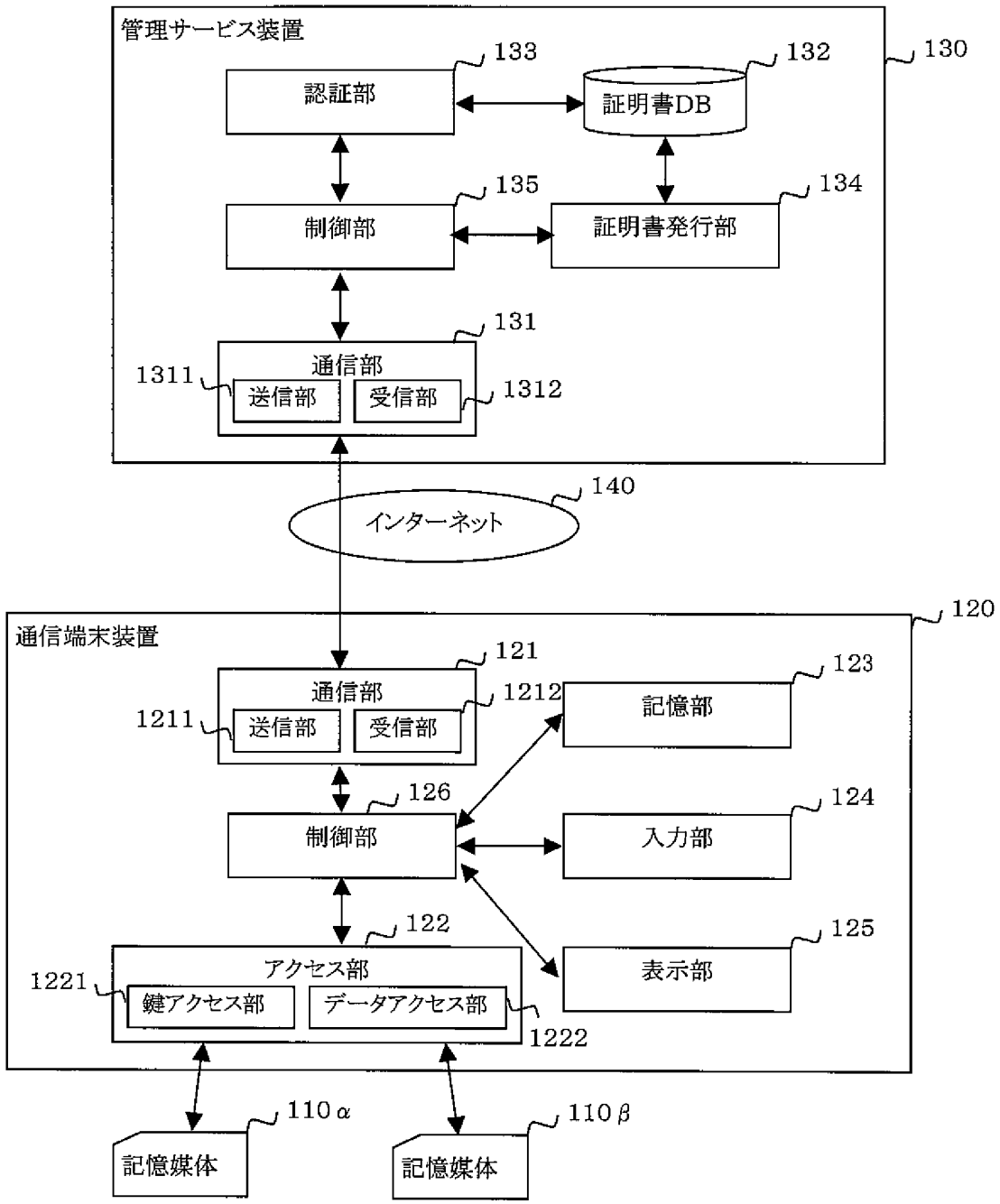
を特徴とする請求項15に記載の記憶媒体。

[17] 前記記憶媒体は、

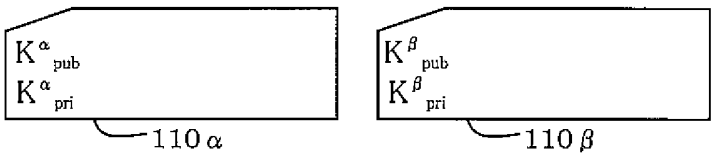
外部から秘密鍵を読み出すことができないこと

を特徴とする請求項15に記載の記憶媒体。

[図1]



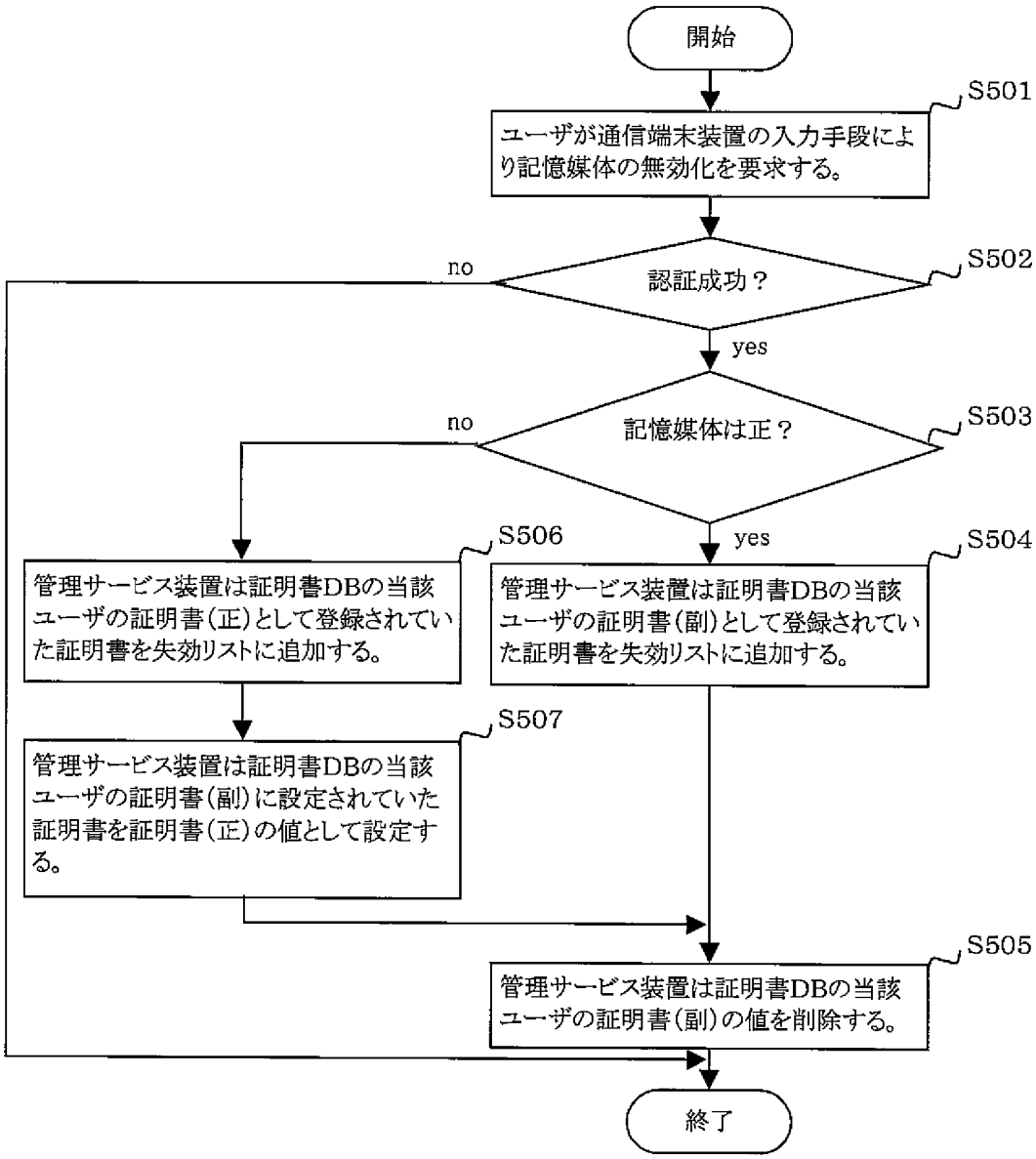
[図2]



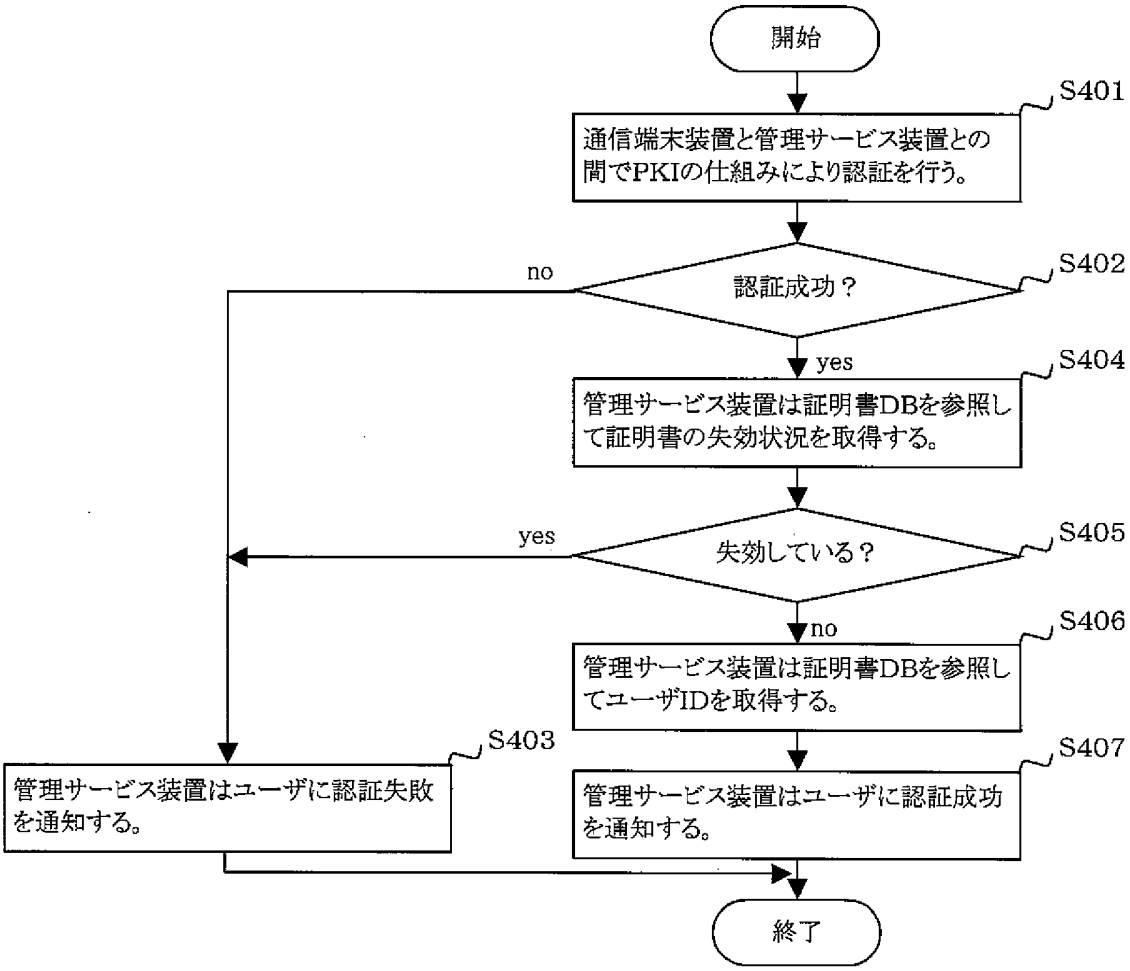
[図3]

ユーザID	証明書(正)	証明書(副)
A	α_A	β_A
B	α_B	β_B
C	α_C	β_C
…	…	…

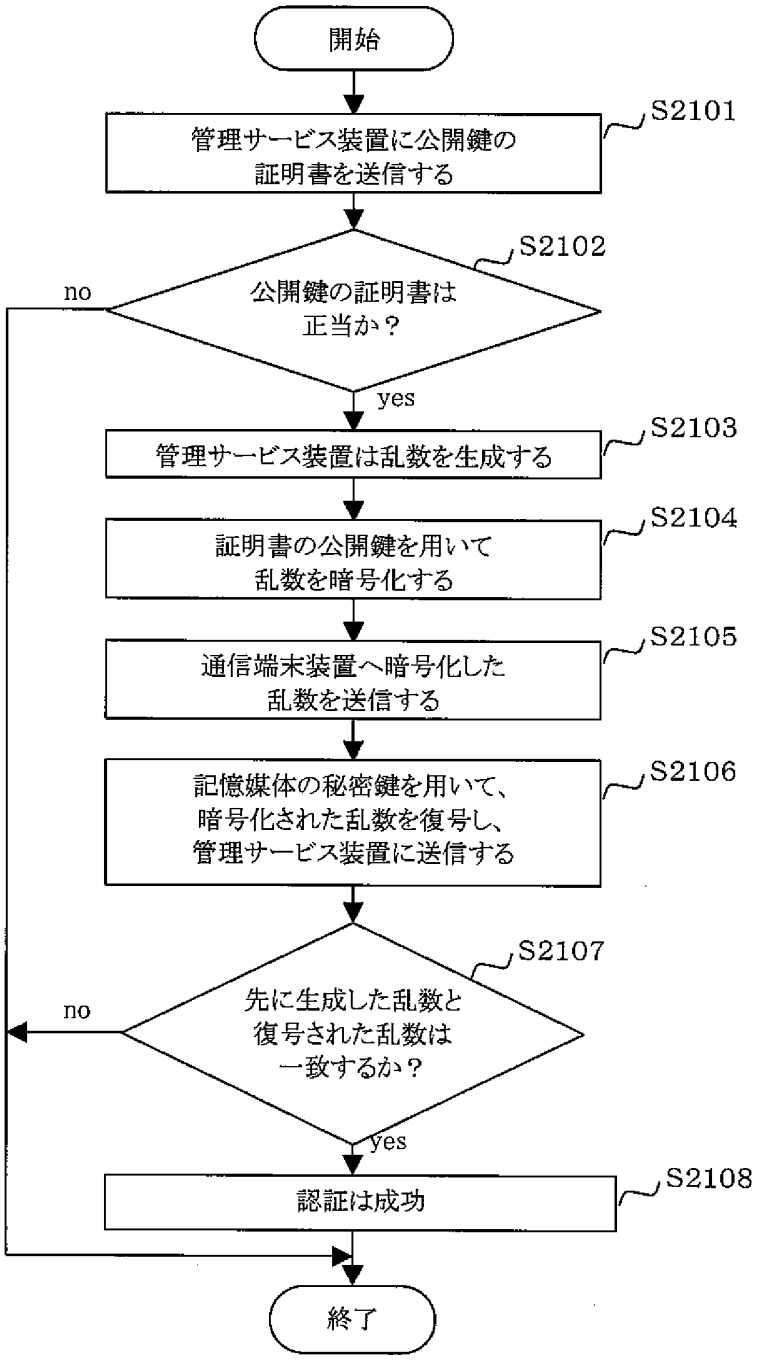
[図4]


開始
S501
ユーザが通信端末装置の入力手段により記憶媒体の無効化を要求する。
S502
認証成功？
no
yes
S503
記憶媒体は正？
no
yes
S504
管理サービス装置は証明書DBの当該ユーザの証明書(副)として登録されていた証明書を失効リストに追加する。
S506
管理サービス装置は証明書DBの当該ユーザの証明書(正)として登録されていた証明書を失効リストに追加する。
S507
管理サービス装置は証明書DBの当該ユーザの証明書(副)に設定されていた証明書を証明書(正)の値として設定する。
S505
管理サービス装置は証明書DBの当該ユーザの証明書(副)の値を削除する。
終了

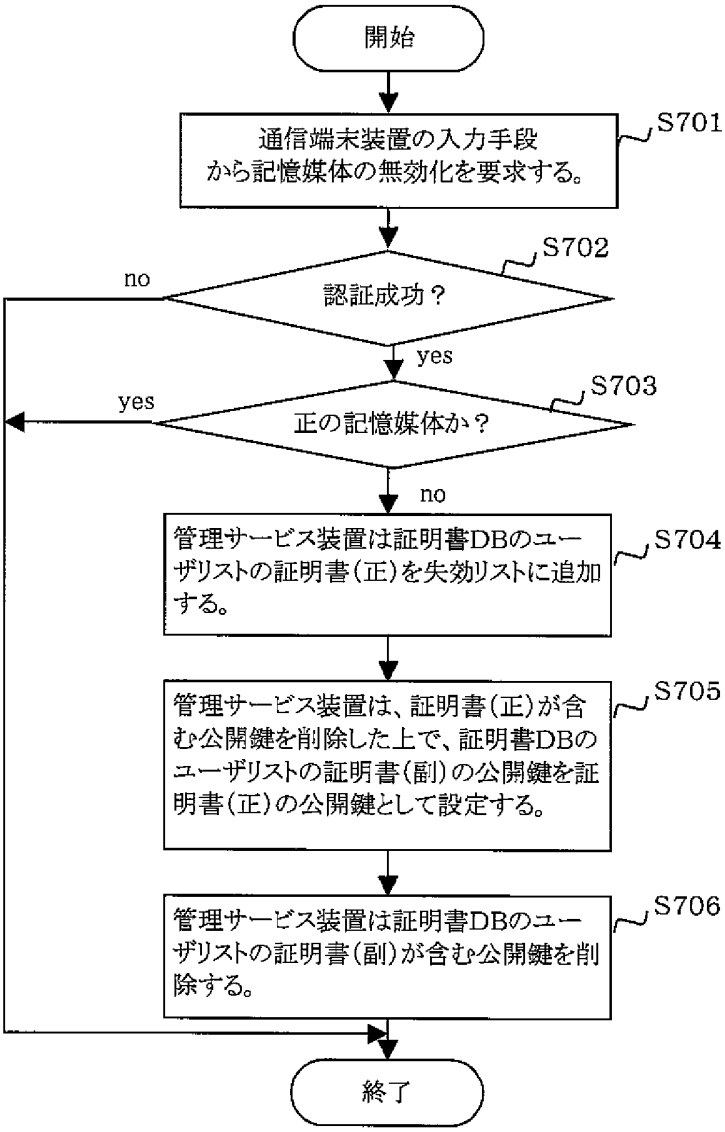
[図5]


開始
S401
通信端末装置と管理サービス装置との間でPKIの仕組みにより認証を行う。
S402
認証成功？
no
yes
S404
管理サービス装置は証明書DBを参照して証明書の失効状況を取得する。
S405
失効している？
yes
no
S406
管理サービス装置は証明書DBを参照してユーザIDを取得する。
S407
管理サービス装置はユーザに認証成功を通知する。
S403
管理サービス装置はユーザに認証失敗を通知する。
終了

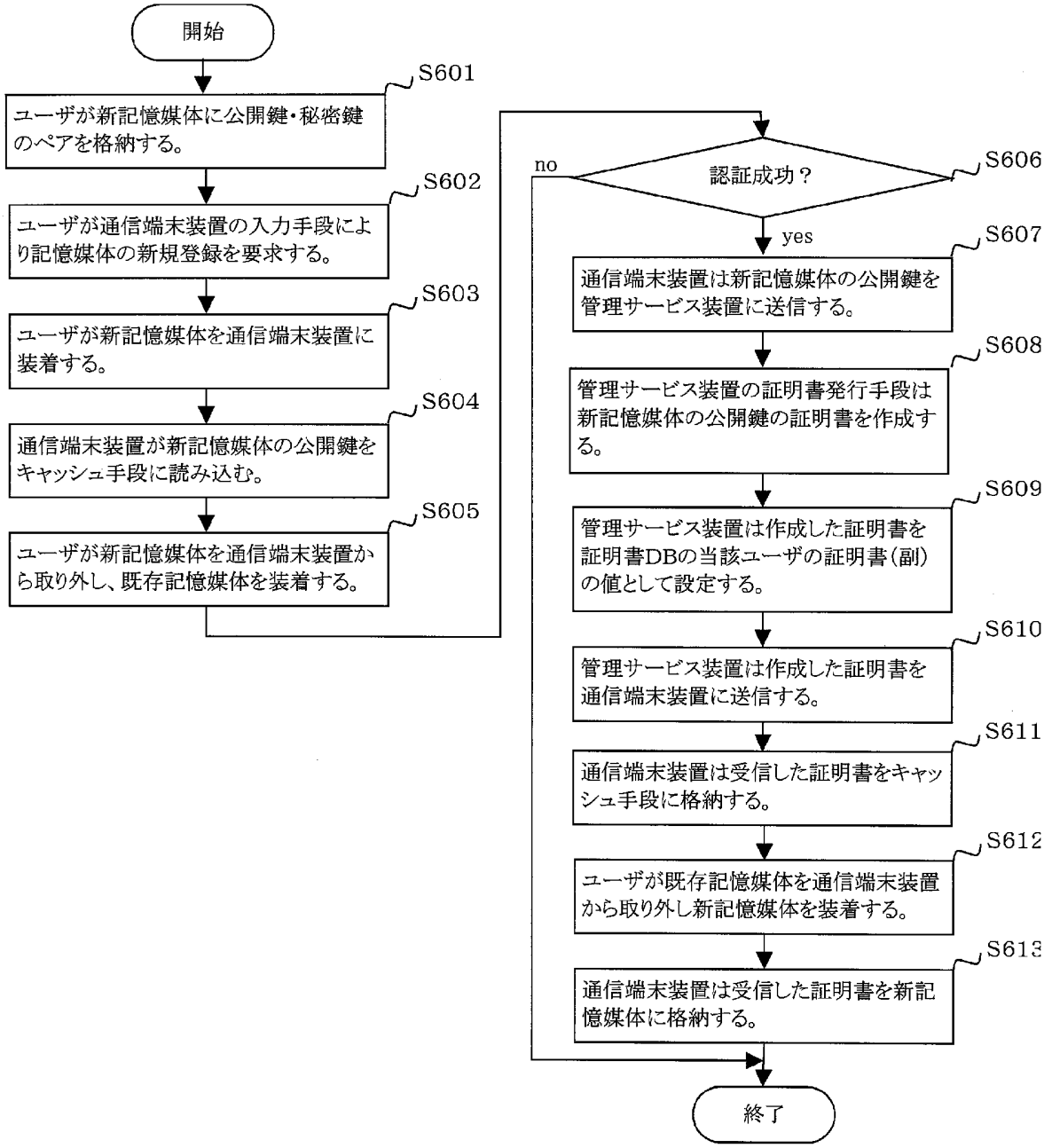
[図6]


開始
管理サービス装置に公開鍵の証明書を送信する
S2101
公開鍵の証明書は正当か？
S2102
no
yes
管理サービス装置は乱数を生成する
S2103
証明書の公開鍵を用いて乱数を暗号化する
S2104
通信端末装置へ暗号化した乱数を送信する
S2105
記憶媒体の秘密鍵を用いて、暗号化された乱数を復号し、管理サービス装置に送信する
S2106
先に生成した乱数と復号された乱数は一致するか？
S2107
no
yes
認証は成功
S2108
終了

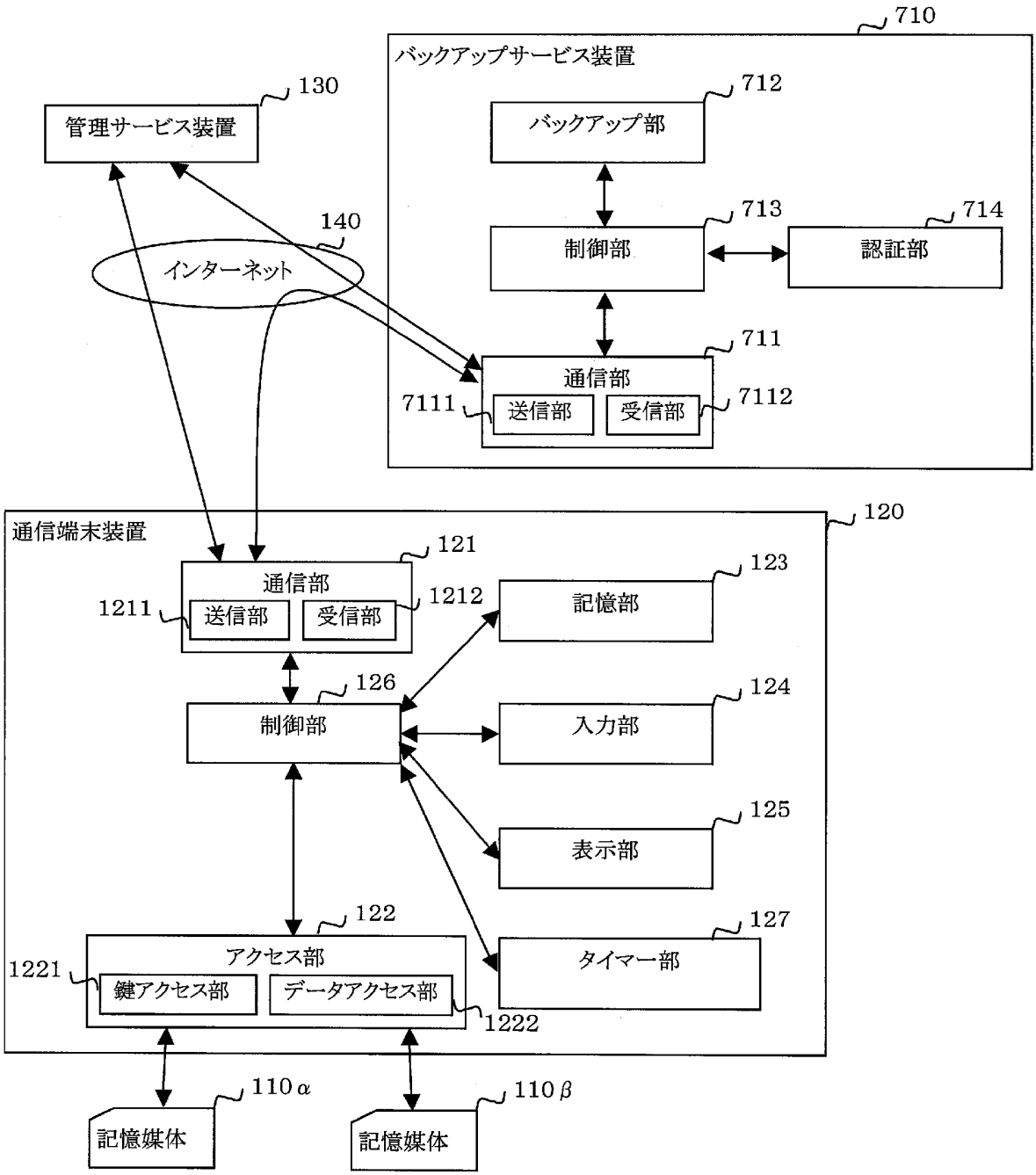
[図7]


開始
通信端末装置の入力手段から記憶媒体の無効化を要求する。
S701
S702
認証成功？
no
yes
S703
正の記憶媒体か？
yes
no
管理サービス装置は証明書DBのユーザリストの証明書(正)を失効リストに追加する。
S704
管理サービス装置は、証明書(正)が含む公開鍵を削除した上で、証明書DBのユーザリストの証明書(副)の公開鍵を証明書(正)の公開鍵として設定する。
S705
管理サービス装置は証明書DBのユーザリストの証明書(副)が含む公開鍵を削除する。
S706
終了

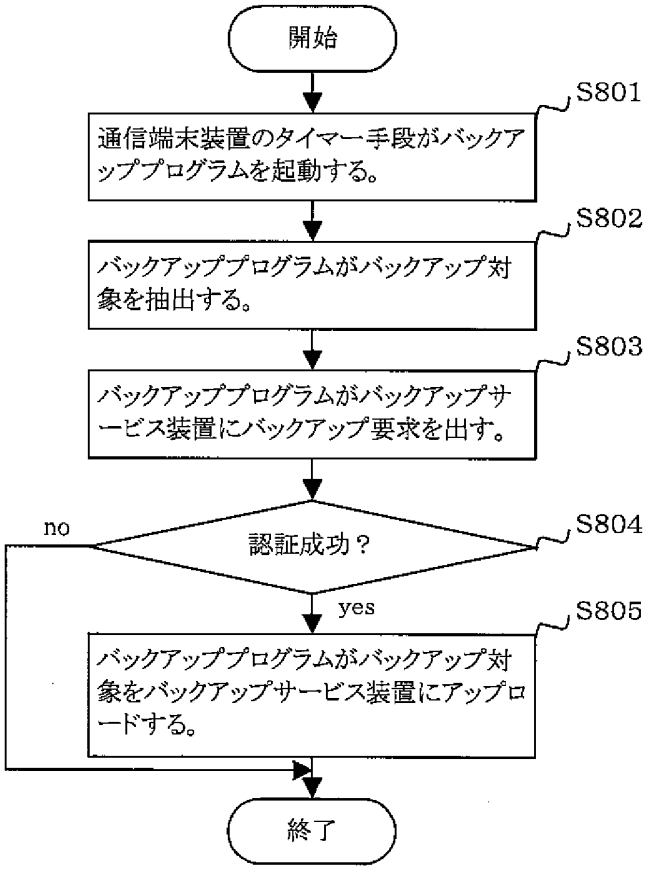
[図8]


開始
S601
ユーザが新記憶媒体に公開鍵・秘密鍵のペアを格納する。
S602
ユーザが通信端末装置の入力手段により記憶媒体の新規登録を要求する。
S603
ユーザが新記憶媒体を通信端末装置に装着する。
S604
通信端末装置が新記憶媒体の公開鍵をキャッシュ手段に読み込む。
S605
ユーザが新記憶媒体を通信端末装置から取り外し、既存記憶媒体を装着する。
S606
認証成功？
no
yes
S607
通信端末装置は新記憶媒体の公開鍵を管理サービス装置に送信する。
S608
管理サービス装置の証明書発行手段は新記憶媒体の公開鍵の証明書を作成する。
S609
管理サービス装置は作成した証明書を証明書DBの当該ユーザの証明書(副)の値として設定する。
S610
管理サービス装置は作成した証明書を通信端末装置に送信する。
S611
通信端末装置は受信した証明書をキャッシュ手段に格納する。
S612
ユーザが既存記憶媒体を通信端末装置から取り外し新記憶媒体を装着する。
S613
通信端末装置は受信した証明書を新記憶媒体に格納する。
終了

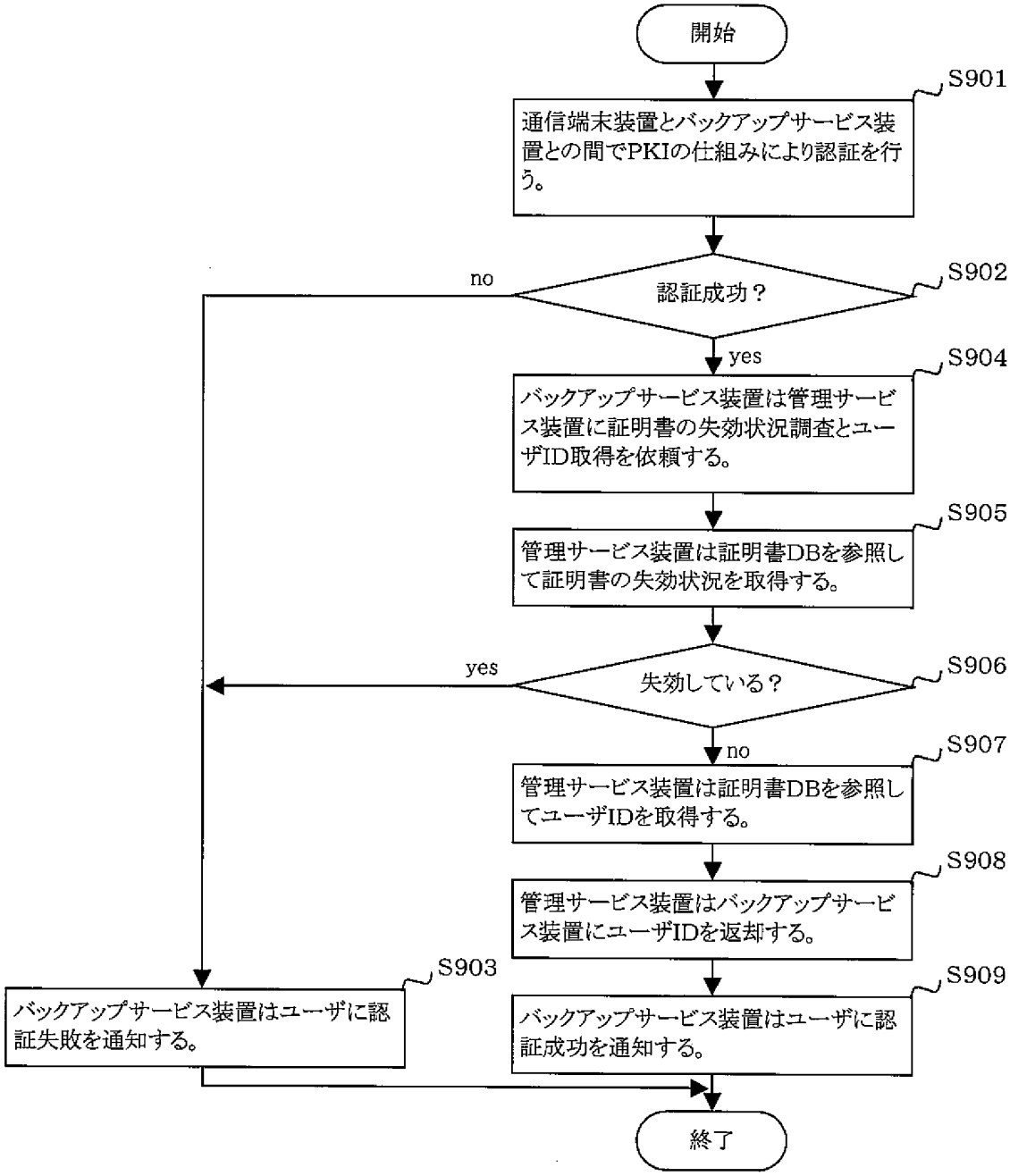
[図9]


710
バックアップサービス装置
712
バックアップ部
713
制御部
714
認証部
711
通信部
7111
送信部
受信部
7112
130
管理サービス装置
140
インターネット
120
通信端末装置
121
通信部
1211
送信部
受信部
1212
123
記憶部
126
制御部
124
入力部
125
表示部
122
アクセス部
1221
鍵アクセス部
データアクセス部
1222
127
タイマー部
110α
記憶媒体
110β
記憶媒体

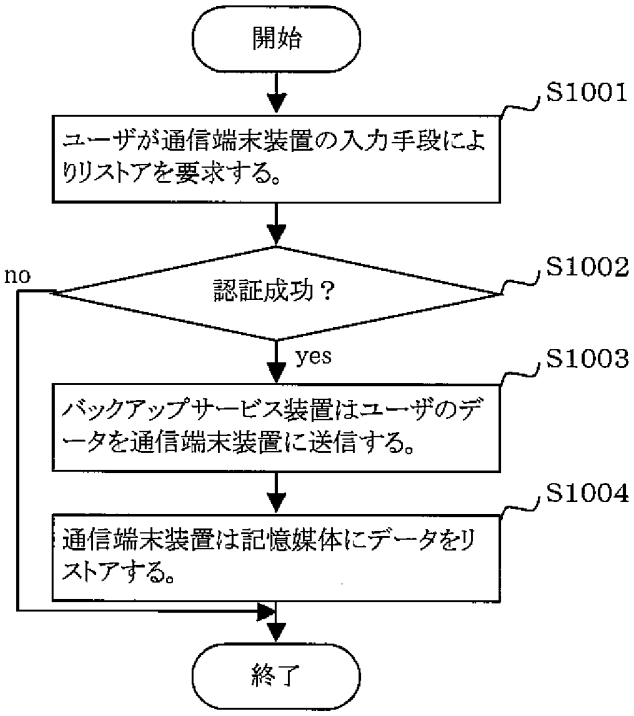
[図10]


開始
S801
通信端末装置のタイマー手段がバックアッププログラムを起動する。
S802
バックアッププログラムがバックアップ対象を抽出する。
S803
バックアッププログラムがバックアップサービス装置にバックアップ要求を出す。
S804
認証成功？
no
yes
S805
バックアッププログラムがバックアップ対象をバックアップサービス装置にアップロードする。
終了

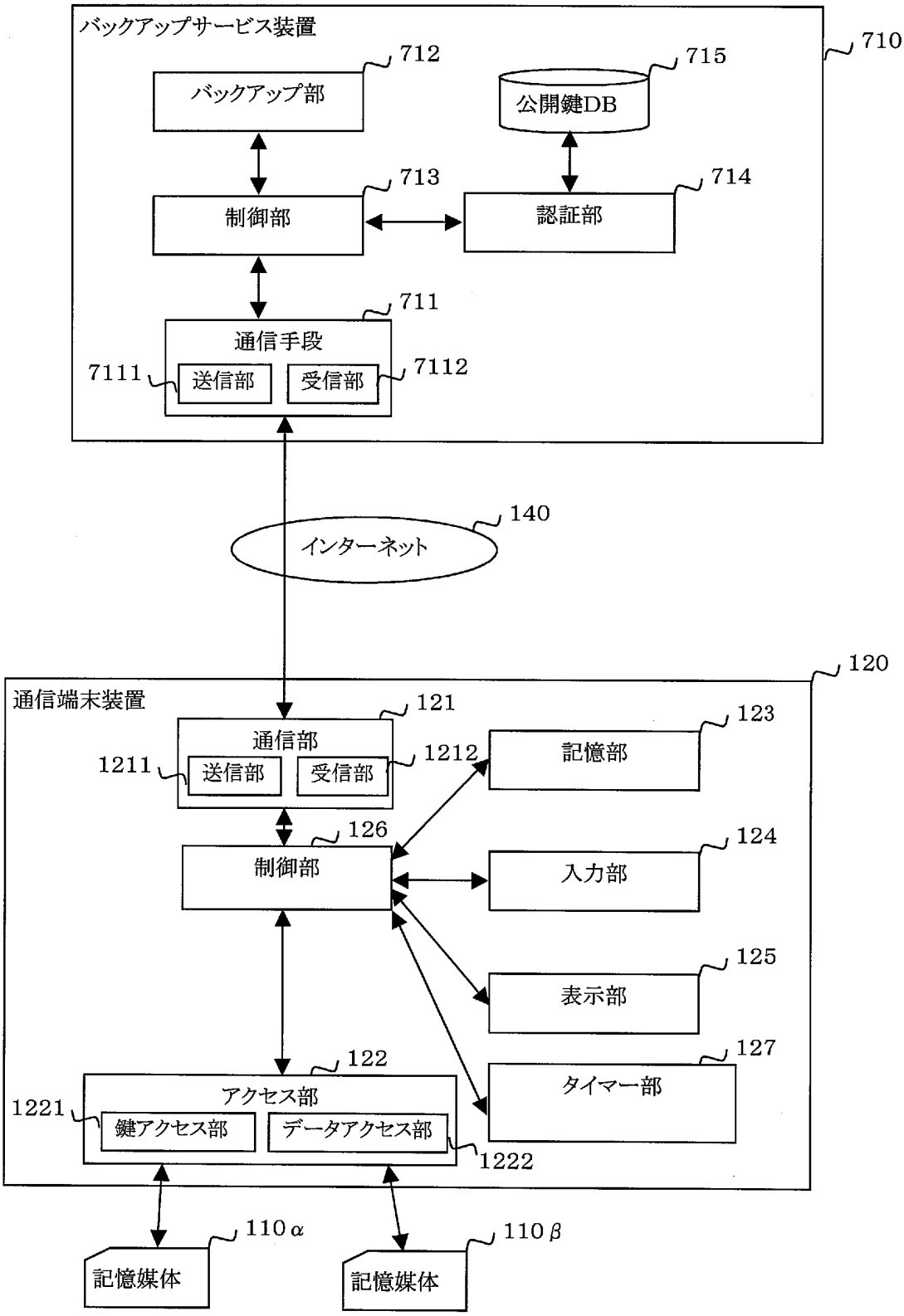
[図11]


開始
S901
通信端末装置とバックアップサービス装置との間でPKIの仕組みにより認証を行う。
S902
認証成功？
no
yes
S904
バックアップサービス装置は管理サービス装置に証明書の失効状況調査とユーザID取得を依頼する。
S905
管理サービス装置は証明書DBを参照して証明書の失効状況を取得する。
S906
失効している？
yes
no
S907
管理サービス装置は証明書DBを参照してユーザIDを取得する。
S908
管理サービス装置はバックアップサービス装置にユーザIDを返却する。
S909
バックアップサービス装置はユーザに認証成功を通知する。
S903
バックアップサービス装置はユーザに認証失敗を通知する。
終了

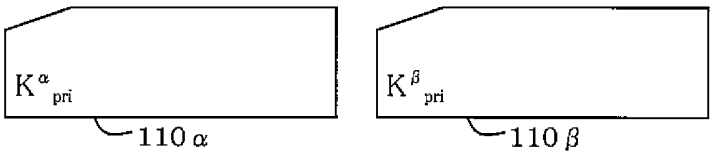
[図12]


開始
S1001
ユーザが通信端末装置の入力手段によりリストアを要求する。
S1002
認証成功？
no
yes
S1003
バックアップサービス装置はユーザのデータを通信端末装置に送信する。
S1004
通信端末装置は記憶媒体にデータをリストアする。
終了

[図13]


バックアップサービス装置
710
712
バックアップ部
715
公開鍵DB
713
制御部
714
認証部
711
通信手段
7111
送信部
受信部
7112
140
インターネット
120
通信端末装置
121
通信部
1211
送信部
受信部
1212
123
記憶部
126
制御部
124
入力部
125
表示部
127
タイマー部
122
アクセス部
1221
鍵アクセス部
データアクセス部
1222
110α
記憶媒体
110β
記憶媒体

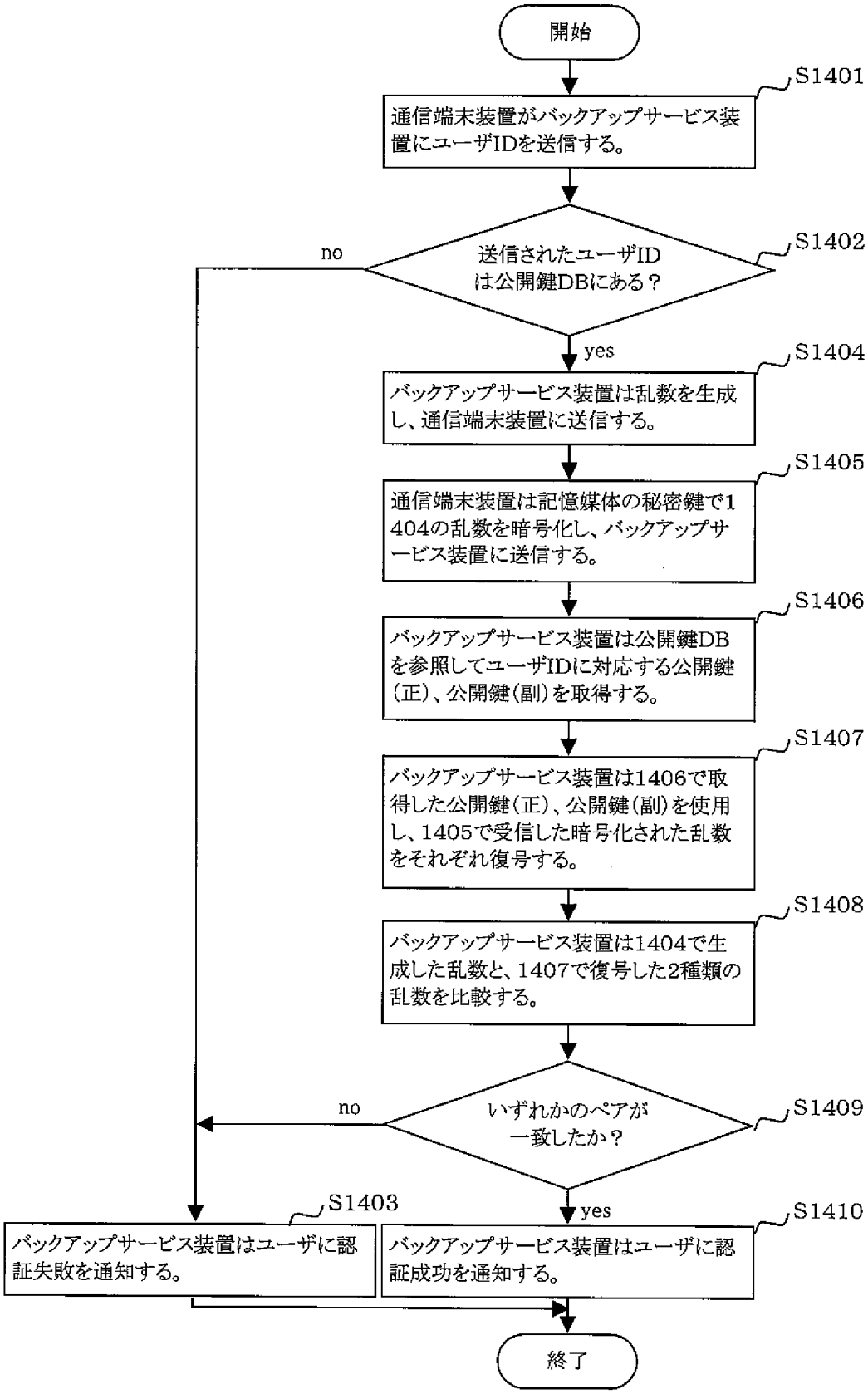
[図14]


K^{α}_{pri}
110α
K^{β}_{pri}
110β

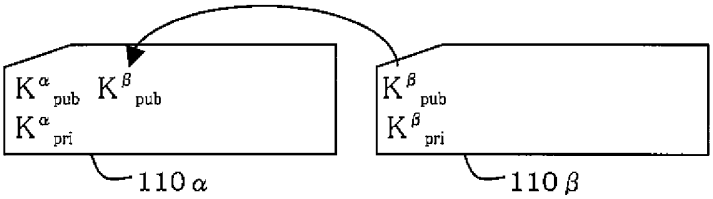
[図15]

ユーザID	公開鍵(正)	公開鍵(副)
A	$K^{\alpha A}_{pub}$	$K^{\beta A}_{pub}$
B	$K^{\alpha B}_{pub}$	$K^{\beta B}_{pub}$
C	$K^{\alpha C}_{pub}$	$K^{\beta C}_{pub}$
…	…	…

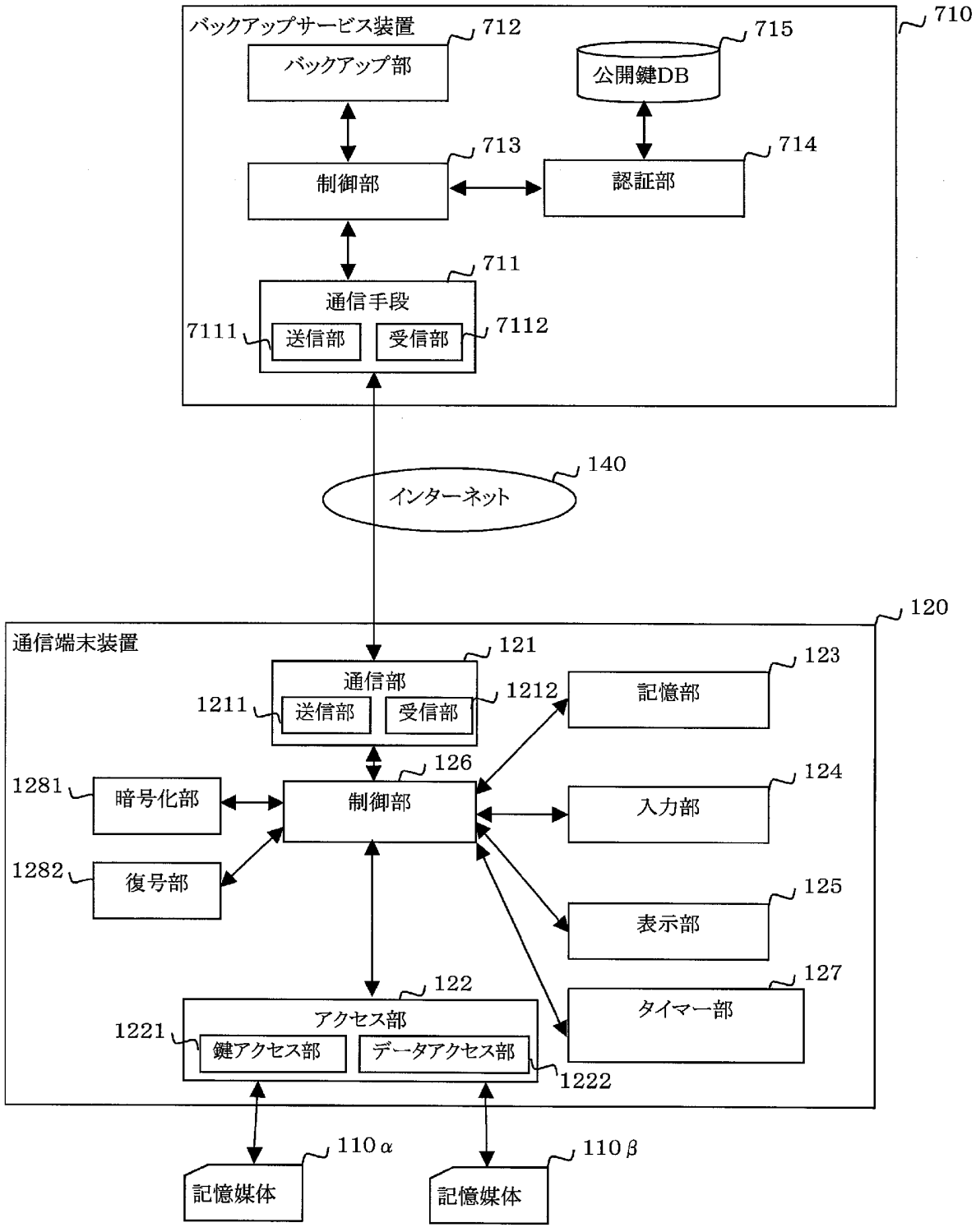
[図16]


開始
S1401
通信端末装置がバックアップサービス装置にユーザIDを送信する。
S1402
送信されたユーザID は公開鍵DBにある？
no
yes
S1404
バックアップサービス装置は乱数を生成し、通信端末装置に送信する。
S1405
通信端末装置は記憶媒体の秘密鍵で1404の乱数を暗号化し、バックアップサービス装置に送信する。
S1406
バックアップサービス装置は公開鍵DBを参照してユーザIDに対応する公開鍵(正)、公開鍵(副)を取得する。
S1407
バックアップサービス装置は1406で取得した公開鍵(正)、公開鍵(副)を使用し、1405で受信した暗号化された乱数をそれぞれ復号する。
S1408
バックアップサービス装置は1404で生成した乱数と、1407で復号した2種類の乱数を比較する。
S1409
いずれかのペアが一致したか？
no
yes
S1403
バックアップサービス装置はユーザに認証失敗を通知する。
S1410
バックアップサービス装置はユーザに認証成功を通知する。
終了

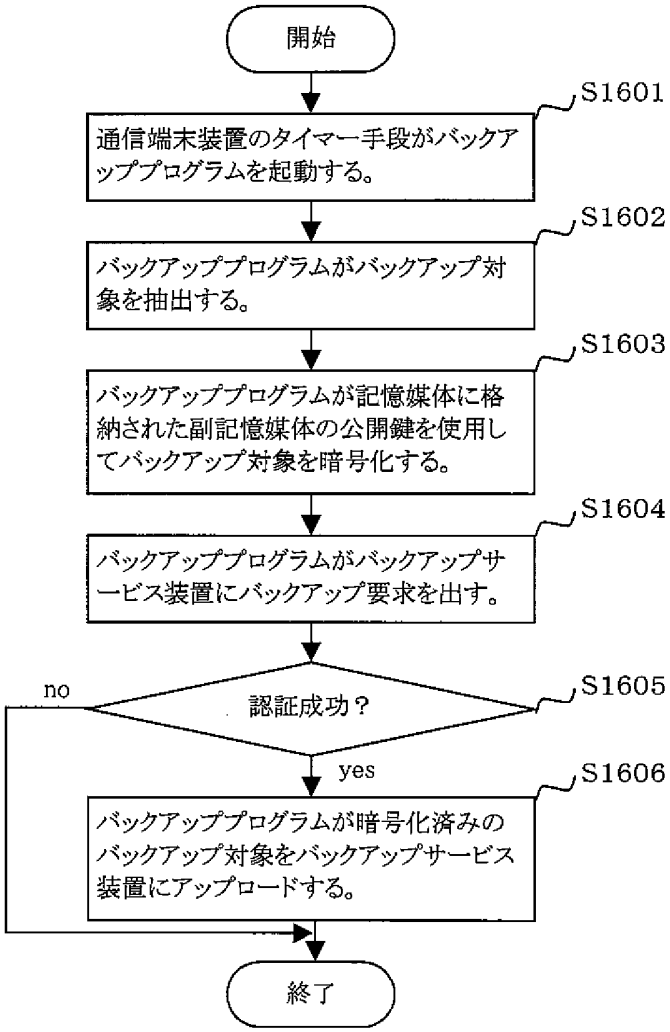
[図17]


K^{α}_{pub} K^{β}_{pub}
K^{α}_{pri}
K^{β}_{pub}
K^{β}_{pri}
110α
110β

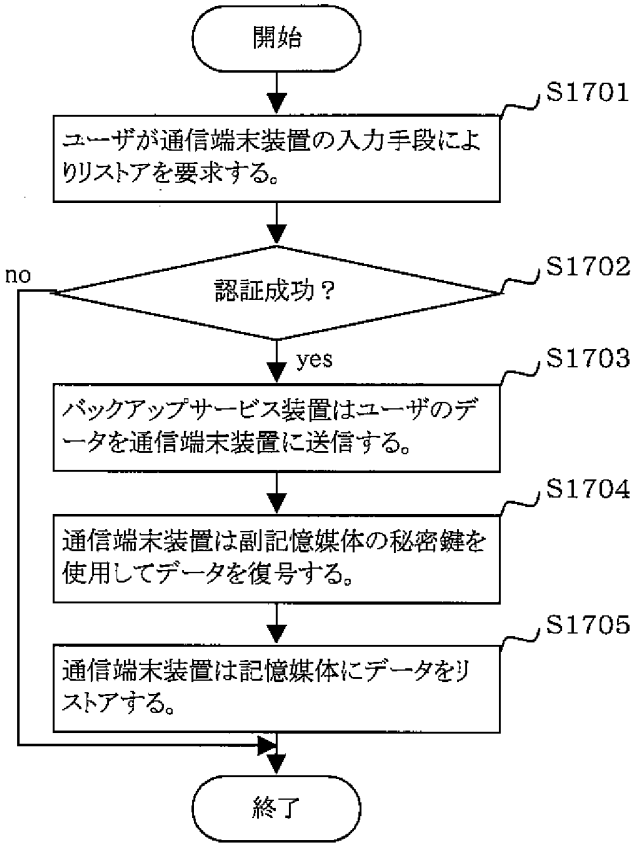
[図18]


バックアップサービス装置
712
バックアップ部
715
公開鍵DB
713
制御部
714
認証部
711
通信手段
7111
送信部
受信部
7112
710
140
インターネット
120
通信端末装置
121
通信部
1211
送信部
受信部
1212
123
記憶部
126
1281
暗号化部
制御部
124
入力部
1282
復号部
125
表示部
127
タイマー部
122
アクセス部
1221
鍵アクセス部
データアクセス部
1222
110α
記憶媒体
110β
記憶媒体

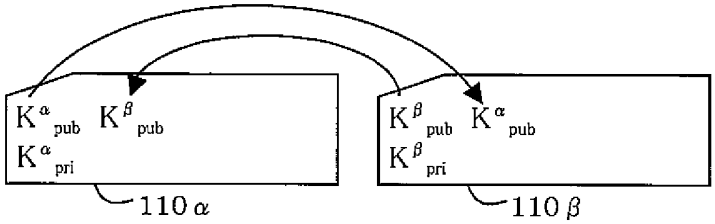
[図19]


開始
S1601
通信端末装置のタイマー手段がバックアッププログラムを起動する。
S1602
バックアッププログラムがバックアップ対象を抽出する。
S1603
バックアッププログラムが記憶媒体に格納された副記憶媒体の公開鍵を使用してバックアップ対象を暗号化する。
S1604
バックアッププログラムがバックアップサービス装置にバックアップ要求を出す。
S1605
認証成功？
no
yes
S1606
バックアッププログラムが暗号化済みのバックアップ対象をバックアップサービス装置にアップロードする。
終了

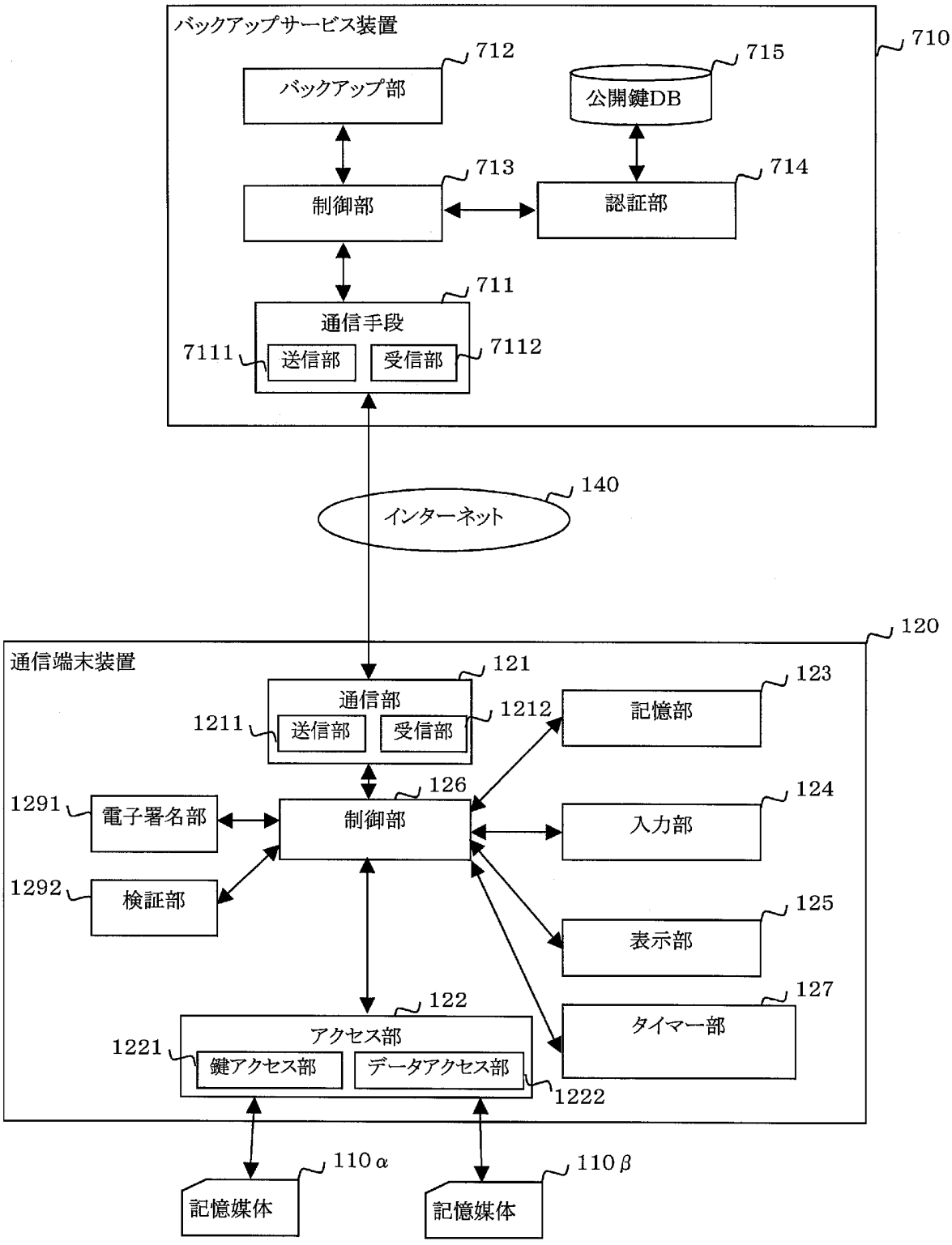
[図20]


開始
S1701
ユーザが通信端末装置の入力手段によりリストアを要求する。
S1702
認証成功？
no
yes
S1703
バックアップサービス装置はユーザのデータを通信端末装置に送信する。
S1704
通信端末装置は副記憶媒体の秘密鍵を使用してデータを復号する。
S1705
通信端末装置は記憶媒体にデータをリストアする。
終了

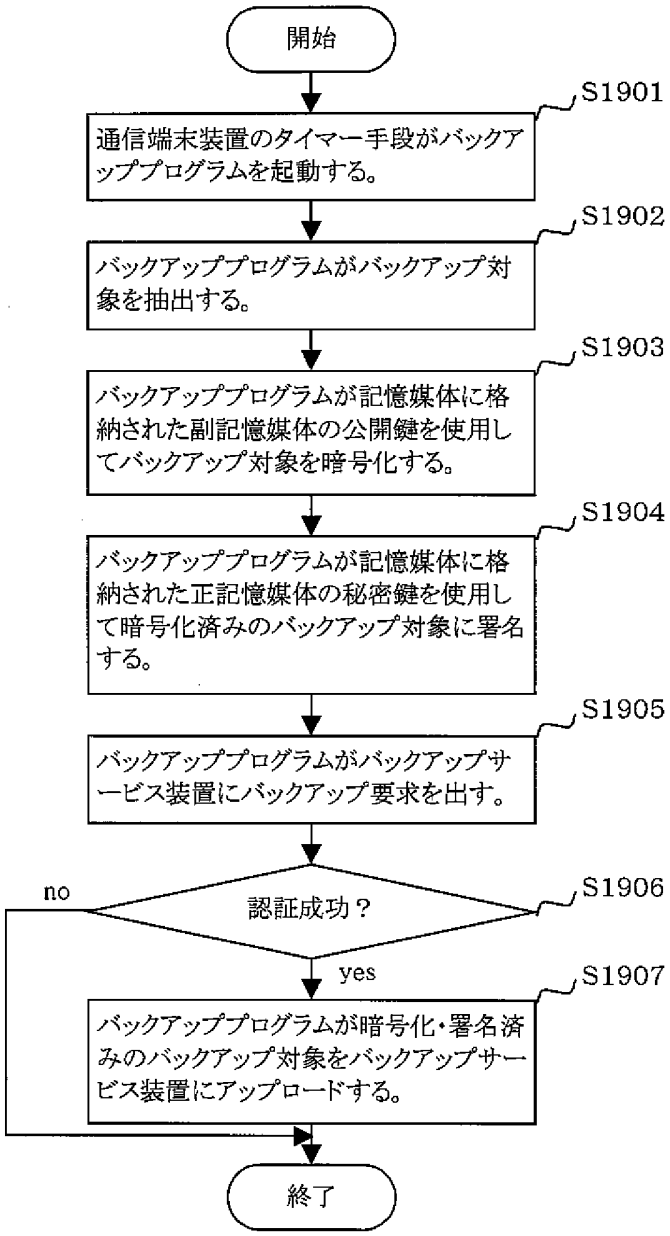
[図21]


K^{α}_{pub} K^{β}_{pub}
K^{α}_{pri}
110α
K^{β}_{pub} K^{α}_{pub}
K^{β}_{pri}
110β

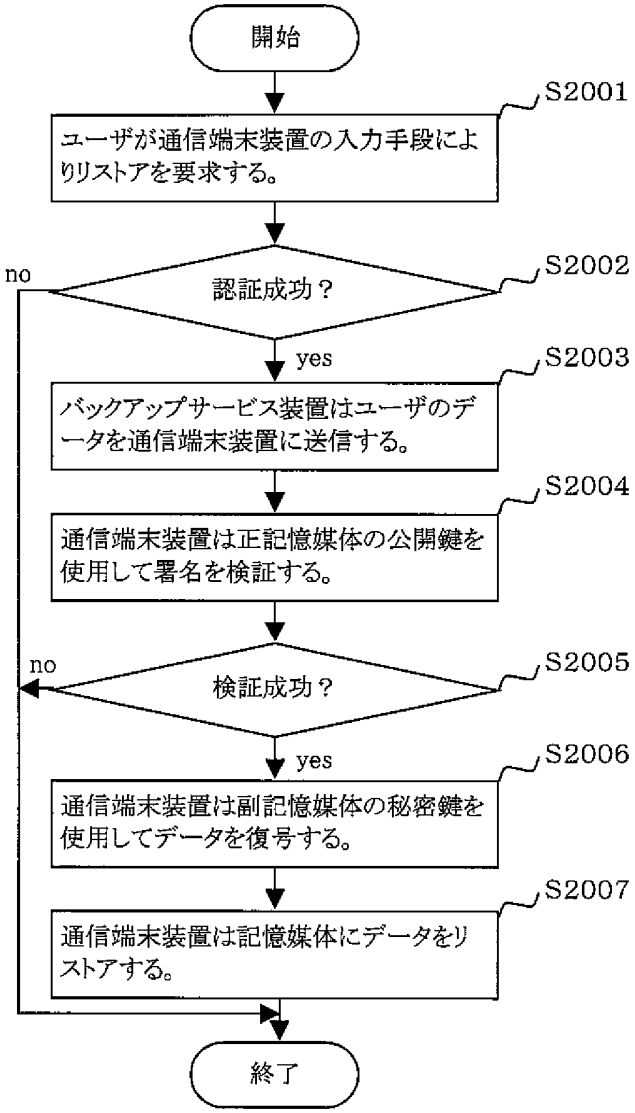
[図22]


バックアップサービス装置
710
712
バックアップ部
715
公開鍵DB
713
制御部
714
認証部
711
通信手段
7111
送信部
受信部
7112
140
インターネット
120
通信端末装置
121
通信部
1211
送信部
受信部
1212
123
記憶部
126
1291
電子署名部
制御部
124
入力部
1292
検証部
125
表示部
127
タイマー部
122
アクセス部
1221
鍵アクセス部
データアクセス部
1222
110α
記憶媒体
110β
記憶媒体

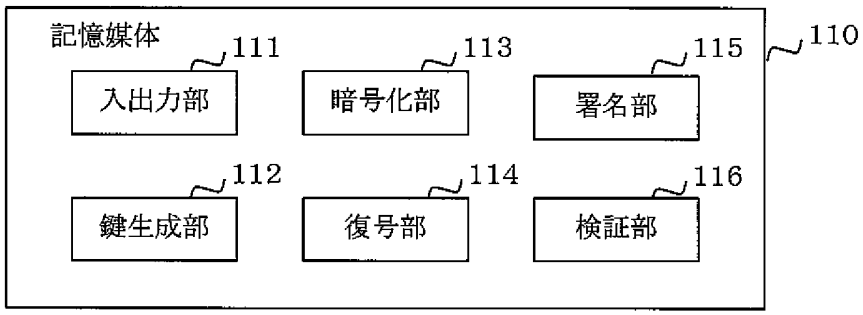
[図23]


開始
S1901
通信端末装置のタイマー手段がバックアッププログラムを起動する。
S1902
バックアッププログラムがバックアップ対象を抽出する。
S1903
バックアッププログラムが記憶媒体に格納された副記憶媒体の公開鍵を使用してバックアップ対象を暗号化する。
S1904
バックアッププログラムが記憶媒体に格納された正記憶媒体の秘密鍵を使用して暗号化済みのバックアップ対象に署名する。
S1905
バックアッププログラムがバックアップサービス装置にバックアップ要求を出す。
S1906
認証成功？
no
yes
S1907
バックアッププログラムが暗号化・署名済みのバックアップ対象をバックアップサービス装置にアップロードする。
終了

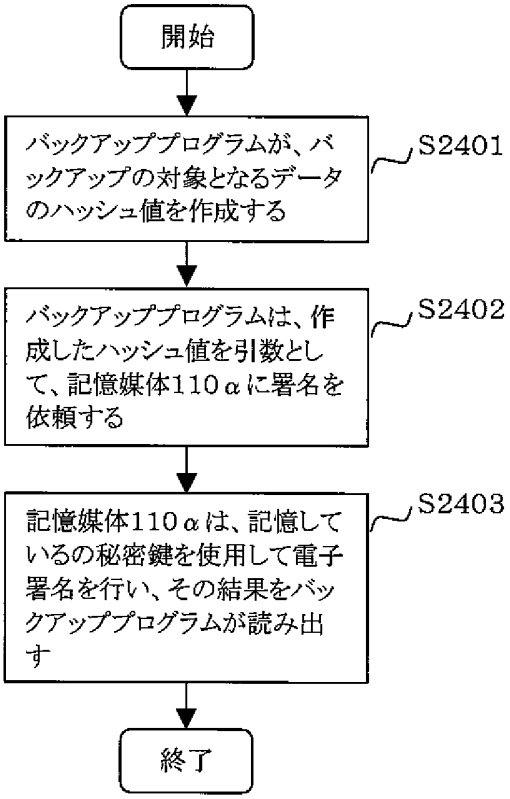
[図24]


開始
S2001
ユーザが通信端末装置の入力手段によりリストアを要求する。
S2002
認証成功？
no
yes
S2003
バックアップサービス装置はユーザのデータを通信端末装置に送信する。
S2004
通信端末装置は正記憶媒体の公開鍵を使用して署名を検証する。
S2005
検証成功？
no
yes
S2006
通信端末装置は副記憶媒体の秘密鍵を使用してデータを復号する。
S2007
通信端末装置は記憶媒体にデータをリストアする。
終了

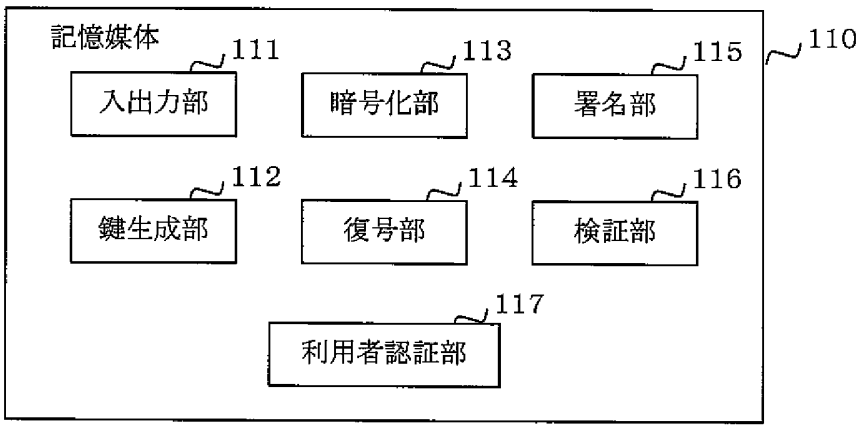
[図25]


記憶媒体
110
111
入出力部
113
暗号化部
115
署名部
112
鍵生成部
114
復号部
116
検証部

[図26]



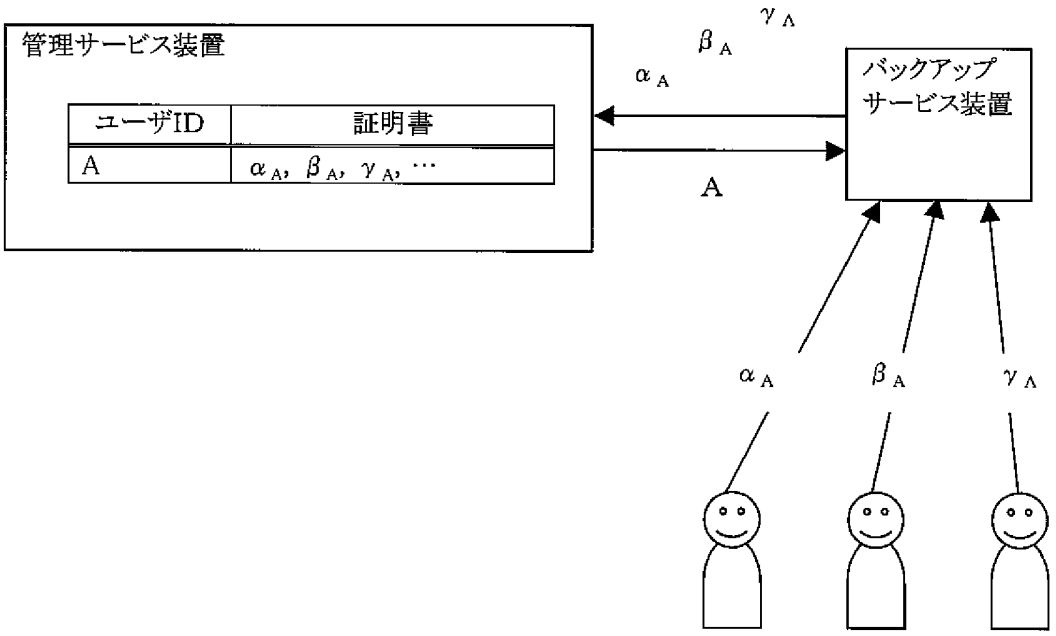
[図27]



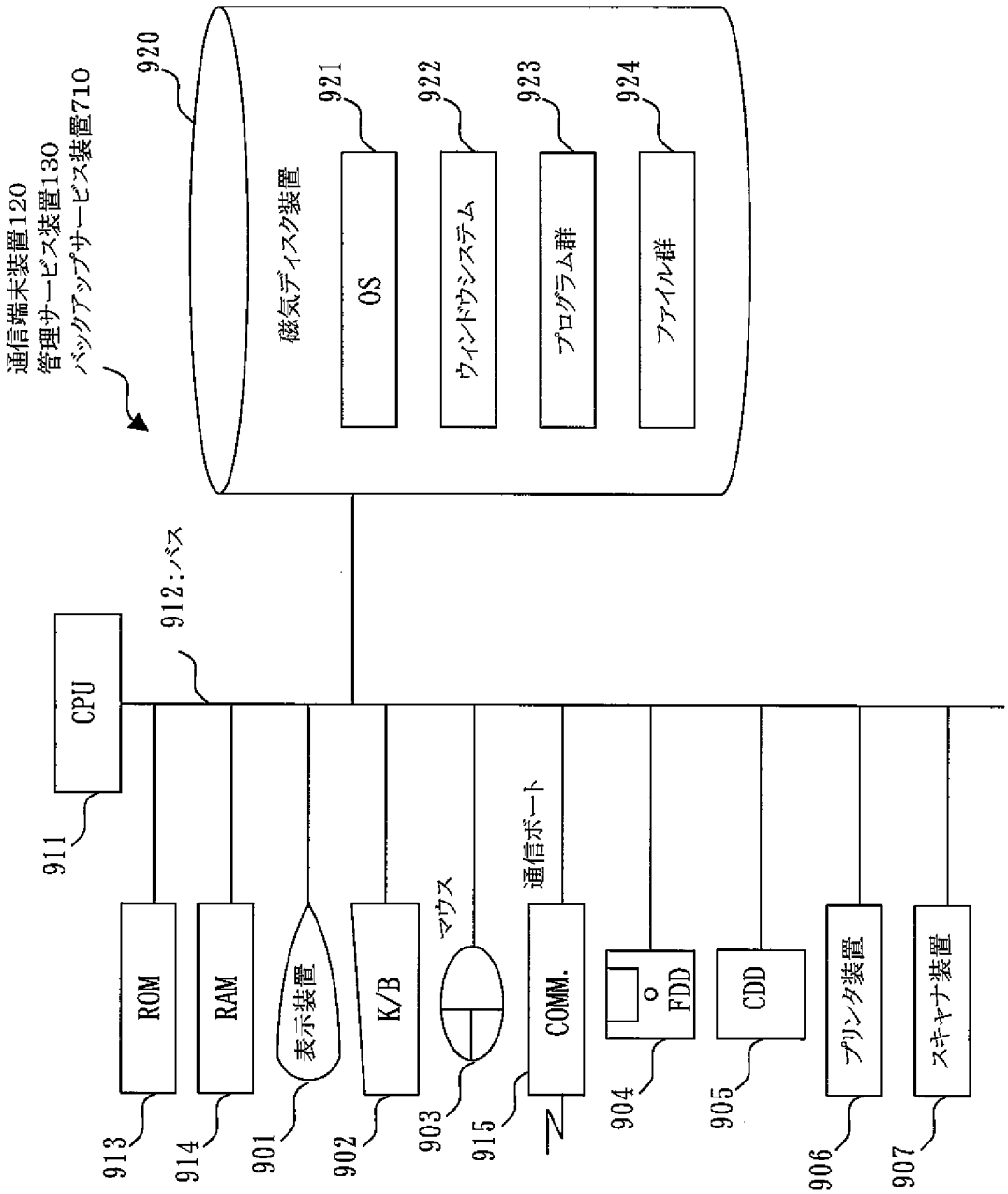
[図28]

ユーザID	証明書
A	α_A, β_A, γ_A, …
B	α_B, β_B, …
C	α_C, β_C, γ_C, …
…	…

[図29]


管理サービス装置
ユーザID
証明書
A
α_A, β_A, γ_A, …
γ_A
β_A
α_A
バックアップ
サービス装置
A
α_A
β_A
γ_A

[図30]


通信端末装置120
管理サービス装置130
バックアップサービス装置710
920
磁気ディスク装置
921
OS
922
ウィンドウシステム
923
プログラム群
924
ファイル群
912:バス
CPU
911
ROM
913
RAM
914
表示装置
901
K/B
902
マウス
903
通信ポート
915
COMM.
FDD
904
CDD
905
プリンタ装置
906
スキャナ装置
907

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/011883

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G06F12/14, G06F15/00, G06K17/00

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)
Int.Cl[7] G06F12/14, G06F12/00, G06F15/00, G06K17/00, H04L9/32, G09C1/00

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 1996-2005
Kokai Jitsuyo Shinan Koho 1971-2005 Toroku Jitsuyo Shinan Koho 1994-2005

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.
Y	JP 2003-233775 A (Hitachi, Ltd.), 22 August, 2003 (22.08.03), Full text; all drawings (Family: none)	1-17
Y	JP 2002-245427 A (Toshiba Corp.), 30 August, 2002 (30.08.02), Full text; all drawings & US 2002/0114468 A1 & EP 1233381 A2	1-17
Y	JP 2000-268137 A (Hitachi, Ltd.), 29 September, 2000 (29.09.00), Full text; all drawings (Family: none)	1-17

☒ 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
18 March, 2005 (18.03.05)	05 April, 2005 (05.04.05)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/011883

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	Takao NAKAYAMA, "UNIX no Dogubako 21 SSH, UNIX MAGAZINE, Vol.18, No.7, 01 July, 2003 (01.07.03), pages 87 to 101	1-17
Y	JP 2004-220175 A (Seiko Epson Corp.), 05 August, 2004 (05.08.04), Par. Nos. [0002] to [0003] (Family: none)	16

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/011883

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

Between the inventions of claims 1-9, the inventions of claims 10-14, and the inventions of claims 15-17, there is no common or corresponding composing elements. Accordingly, there is no technical relationship among those inventions involving one or more of the same or corresponding special technical feature within the meaning of PCT Rule. 13.2, second sentence.

Consequently, no technical relationship within the meaning of PCT Rule 13 between the inventions of claims 1-9, the inventions of claims 10-14, and the inventions of claims 15-17 can be seen.

(Continued to extra sheet)

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☒ No protest accompanied the payment of additional search fees.

Continuation of Box No.III of continuation of first sheet(2)

Therefore, the inventions of claims 1-9, the inventions of claims 10-14, and the inventions of claims 15-17 do not satisfy the requirement of unity of invention.

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００４／０１１８８３

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））
Int. Cl[7] G06F12/14, G06F15/00, G06K17/00

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[7] G06F12/14, G06F12/00, G06F15/00, G06K17/00, H04L9/32, G09C1/00

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　１９７１－２００５年
日本国実用新案登録公報　１９９６－２００５年
日本国登録実用新案公報　１９９４－２００５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
Y	JP 2003-233775 A(株式会社日立製作所) 2003.08.22, 全文, 全図 (ファミリーなし)	1 - 17
Y	JP 2002-245427 A(株式会社東芝) 2002.08.30, 全文, 全図 & US 2002/0114468 A1 & EP 1233381 A2	1 - 17
Y	JP 2000-268137 A(株式会社日立製作所) 2000.09.29, 全文, 全図 (ファミリーなし)	1 - 17

☒ 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
18.03.2005	05.4.2005

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）	
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	原　秀人 電話番号　０３－３５８１－１１０１　内線　３５８５	５Ｎ　９６４４

Ｃ（続き）．　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
Y	中山貴夫, UNIXの道具箱 21　SSH, UNIX MAGAZINE, 第18巻, 第7号, 2003.07.01, p. 87—101	1 - 17
Y	JP 2004-220175 A(セイコーエプソン株式会社) 2004.08.05, 段落【０００２】－【０００３】（ファミリーなし）	16

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００４／０１１８８３

第Ⅱ欄　請求の範囲の一部の調査ができないときの意見（第１ページの２の続き）

法第８条第３項（ＰＣＴ１７条(2)(a)）の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1．☐ 請求の範囲 _____ は、この国際調査機関が調査をすることを要しない対象に係るものである。
つまり、

2．☐ 請求の範囲 _____ は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、

3．☐ 請求の範囲 _____ は、従属請求の範囲であってＰＣＴ規則6.4(a)の第２文及び第３文の規定に従って記載されていない。

第Ⅲ欄　発明の単一性が欠如しているときの意見（第１ページの３の続き）

次に述べるようにこの国際出願に二以上の発明があるとこの国際調査機関は認めた。

請求の範囲１－９、請求の範囲１０－１４及び請求の範囲１５－１７の間には、共通又は対応する構成要素が存在しない。したがって、上記請求の範囲には、ＰＣＴ規則１３．２の第２文の意味における、同一の又は対応する特別な技術的特徴はない。

それ故、請求の範囲１－９、請求の範囲１０－１４及び請求の範囲１５－１７の間にＰＣＴ規則１３の意味における技術的関連を見いだすことはできない。

よって、請求の範囲１－９、請求の範囲１０－１４及び請求の範囲１５－１７に係る発明は発明の単一性を満たしていない。

1．☒ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。

2．☐ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。

3．☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったので、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。

4．☐ 出願人が必要な追加調査手数料を期間内に納付しなかったので、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

追加調査手数料の異議の申立てに関する注意

☐ 追加調査手数料の納付と共に出願人から異議申立てがあった。

☒ 追加調査手数料の納付と共に出願人から異議申立てがなかった。