(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
2020年2月20日(20.02.2020)

WIPO | PCT

(10) 国際公開番号
WO 2020/036070 A1

(51) 国際特許分類:
H04L 9/08 (2006.01) *G09C 1/00* (2006.01)
G06F 21/33 (2013.01) *H04L 9/32* (2006.01)
G06F 21/60 (2013.01)

(21) 国際出願番号： PCT/JP2019/030237

(22) 国際出願日： 2019年8月1日(01.08.2019)

(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 2018-152271 2018年8月13日(13.08.2018) JP

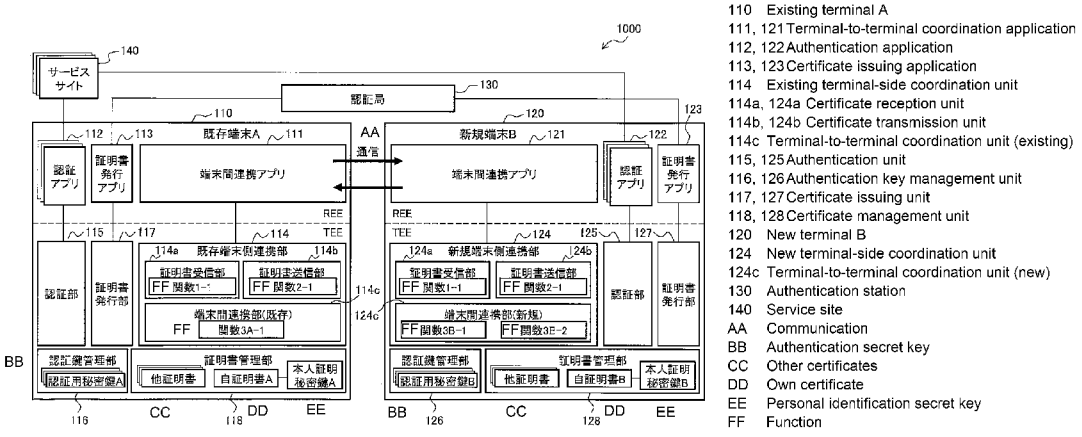
(71) 出願人: 日本電信電話株式会社 (**NIPPON TELEGRAPH AND TELEPHONE CORPORATION**) [JP/JP]; 〒1008116 東京都千代田区大手町一丁目５番１号 Tokyo (JP).

(72) 発明者: 西村 豪生 (**NISHIMURA, Hideo**); 〒1808585 東京都武蔵野市緑町３丁目９－１１ ＮＴＴ 知的財産センタ内 Tokyo (JP). 山下 高生(**YAMASHITA, Takao**); 〒1808585 東京都武蔵野市緑町３丁目９－１１ ＮＴＴ 知的財産センタ内 Tokyo (JP). 吉村 康彦(**YOSHIMURA, Yasuhiko**); 〒1808585 東京都武蔵野市緑町３丁目９－１１ ＮＴＴ 知的財産センタ内 Tokyo (JP).

(74) 代理人: 特許業務法人磯野国際特許商標事務所(**ISONO INTERNATIONAL PATENT OFFICE, P.C.**); 〒1050001 東京都港区虎ノ

(54) **Title:** TERMINAL REGISTRATION SYSTEM AND TERMINAL REGISTRATION METHOD

(54) 発明の名称： 端末登録システムおよび端末登録方法



110 Existing terminal A
111, 121 Terminal-to-terminal coordination application
112, 122 Authentication application
113, 123 Certificate issuing application
114 Existing terminal-side coordination unit
114a, 124a Certificate reception unit
114b, 124b Certificate transmission unit
114c Terminal-to-terminal coordination unit (existing)
115, 125 Authentication unit
116, 126 Authentication key management unit
117, 127 Certificate issuing unit
118, 128 Certificate management unit
120 New terminal B
124 New terminal-side coordination unit
124c Terminal-to-terminal coordination unit (new)
130 Authentication station
140 Service site
AA Communication
BB Authentication secret key
CC Other certificates
DD Own certificate
EE Personal identification secret key
FF Function

(57) **Abstract:** [Problem] To provide a terminal registration system and a terminal registration method with which it is possible to reduce the number of times of communication between terminals. [Solution] A terminal registration system 1000 in which an existing terminal A110 is provided with: a certificate issuing unit 117 which issues, to a secure region including a TEE, an owner certificate indicating an owner of a terminal; an existing terminal-side coordination unit 114 which performs coordination between terminals having the same owner certificates, and which generates an encryption key; and an authenticate key management unit 116 which manages a authentication secret key. The existing terminal A110 is also provided with, in a terminal environment including an REE, a terminal-to-terminal coordination application 111 for performing terminal-to-terminal communication. A new terminal B120 makes a request, from a terminal-to-terminal coordination application 121 of the new terminal B120 side to the existing terminal A110, for starting encrypted communication using the encryption key. The existing terminal-side coordination unit 114 of the existing terminal A110 sends

WO 2020/036070 A1

［続葉有］

門一丁目１番１８号 ヒューリック虎ノ門ビル 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, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, 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, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

添付公開書類：

— 国際調査報告（条約第21条(3)）

coordination data in which the authentication secret key has been encrypted using the encryption key to the new terminal B120 having the same owner certificate.

(57) 要約：【課題】端末間の通信回数を削減することができる端末登録システムおよび端末登録方法を提供する。 【解決手段】端末登録システム１０００は、既存端末Ａ１１０が、ＴＥＥを含むセキュア領域に、端末の所有者を示す所有者証明書を発行する証明書発行部１１７と、同一の所有者証明書を有する端末間で連携をするとともに、暗号鍵を生成する既存端末側連携部１１４と、認証用秘密鍵を管理する認証鍵管理部１１６と、を備え、また、ＲＥＥを含む端末環境に、端末間の通信を行う端末間連携アプリ１１１を備え、新規端末Ｂ１２０は、新規端末Ｂ１２０側の端末間連携アプリ１２１から既存端末Ａ１１０に対して、暗号鍵による暗号化通信の開始要求を行い、既存端末Ａ１１０の既存端末側連携部１１４は、認証用秘密鍵を暗号鍵で暗号化した連携用データを、同一の所有者証明書を有する新規端末Ｂ１２０に送付する。

明　細　書

発明の名称 ： 端末登録システムおよび端末登録方法

技術分野

[0001] 本発明は、端末登録システムおよび端末登録方法に関する。

背景技術

[0002] パスワード認証に替わる利用者認証技術として、パスワードレス認証のデファクト標準技術（ＦＩＤＯ：Fast IDentity Online）という、公開鍵暗号を用いたＷｅｂサービスの利用者認証技術がある（非特許文献１参照）。

ＦＩＤＯでは、サービス毎に異なる公開鍵・秘密鍵ペアを生成し、公開鍵をサービスサイト側に配置して、秘密鍵を端末内に閉じ込める。秘密鍵の利用（チャレンジ・レスポンス認証における署名）は端末上で生体認証を行うことが前提となっており、かつ、秘密鍵の利用はAuthenticator内で行われ、端末外に秘密鍵が出ていくことはないことからセキュリティが高い。

ＦＩＤＯ認証を利用するためには、事前にサービスサイトに対して端末のRegistrationを行い、アカウントにその端末の公開鍵を紐付けておく必要がある。標準技術においてRegistrationは、ＦＩＤＯ以外の認証方法でアカウントにログインした上で実行することが想定されている。

[0003] 図１４は、標準技術（ＦＩＤＯ）の特徴を説明する図であり、図１４（ａ）は端末の認証を示し、図１４（ｂ）は新規端末の登録を示す。

図１４（ａ）に示すように、端末１は、生体認証等でアクセス制御される。端末１と、サービスサイトＡ２１およびサービスサイトＢ２２とは、ＦＩＤＯプロトコルで認証される。利用者は端末１を使ってサービスサイトＡ２１とサービスサイトＢ２２にアクセスしている。

サービスサイトＡ２１およびサービスサイトＢ２２は、端末毎に個別の鍵を登録する。また、端末１は、サイト毎に個別の鍵ペアを生成する。

サービスサイトＡ２１には公開鍵Ａが、サービスサイトＢ２２には公開鍵Ｂが登録済みである。

端末１のセキュア領域（Authenticator）１０には、公開鍵Ａとペアになる秘密鍵Ｂが格納されている。

[0004] 図１４（ｂ）は、標準技術（ＦＩＤＯ）において、新規端末の登録を説明する図である。図１４（ｂ）における端末２は、端末１とは別に新しく追加される端末（以下、新規端末２という）である。新規端末２は、端末の追加、変更（例えば、スマートフォンとタブレット端末の２台持ち、端末の機種変更）によって生じる。新規端末２でＦＩＤＯ認証を利用するためには、事前に全サービスサイトに対して端末のRegistrationを行い、アカウントにその端末の公開鍵を紐付けておく必要がある。

図１４（ｂ）に示すように、新規端末２を利用する場合、新規端末２のAuthenticator１０内には鍵がないことから、サービス毎に再度鍵ペアの生成・登録を行う必要がある。

[0005] 標準技術（ＦＩＤＯ）では、認証用の秘密鍵を端末内に閉じ込めてセキュリティを高める。端末を追加・変更する場合、すべてのサービスサイトに対して新規端末の鍵を再登録する必要があるという利便性上の問題がある。

この問題の解決策として、端末間の連携による手法１と手法２とがある。

[0006] 図１５は、端末間の連携による認証鍵のコピー技術（手法１）を説明する図である。

図１５に示すように、既存端末１と新規端末２間でセキュアな通信路３を確立し、セキュアな通信路３を介して認証鍵を複製する。

両端末の連携（端末間での秘密鍵の複製）によって、複数サイトに対する再登録の利便性を向上させる。

[0007] 図１６は、電子署名の付与による登録認可技術（手法２）を説明する図である。

図１６に示すように、既存端末１と新規端末２間でセキュアな通信路３を確立し、セキュアな通信路３を介して認可情報を付与（電子署名の付与）する。初回アクセス時にサービスサイト２０に電子署名の付与による登録認可を行う。

両端末の連携（電子署名の付与による登録認可）によって、複数サイトに対する再登録の利便性を向上させる。

[0008] 上述した、端末間の連携による手法１および手法２においては、攻撃者がアカウントを乗っ取るために、攻撃者自身の端末（新規端末）とユーザの端末（既存端末）を連携させようとする攻撃が行われることが懸念される。

このような攻撃への対策として、端末のセキュア領域（ＴＥＥ：Trusted Execution Environment等）に、端末の所有者を示す電子証明書（所有者証明書）を発行し、同一の所有者証明書を有する端末間でしか連携をしないようにする手法が提案されている。

[0009] 図１７は、同一の所有者証明書を有する端末間でしか連携をしないようにする手法３を説明する図である。

端末のセキュア領域１０に所有者証明書１１を格納する。所有者証明書１１は、信頼できる第三者が、所有者の本人確認を行った上で発行する電子証明書である。所有者証明書１１は、信頼できる第三者が、対面等の確実性が高い手段でユーザの本人確認を行った上で発行することを想定する。

所有者証明書１１を用いた相互認証により、同一所有者であることが確認できたとき、セキュアな通信路３を確立する。すなわち、両端末の所有者証明書１１を用いた相互認証を行い、所有者の一致が確認できたときのみ、端末間のセキュアな通信路を確立して連携を許容する。

先行技術文献

非特許文献

[0010] 非特許文献1：FIDO Alliance, “SIMPLER, STRONGER AUTHENTICATION”, FIDO is the World’s Largest Ecosystem for Standards-Based, Interoperable Authentication ［online］,［平成３０年８月８日検索］,インターネット〈 https://fidoalliance.org/〉

発明の概要

発明が解決しようとする課題

[0011] ＦＩＤＯの認証鍵は、マルウェア等が手出しできないＴＥＥ等のセキュア領域内で厳密に管理されることが想定されており、そのセキュリティレベルを保つためには、端末間のセキュアな通信路を確立する機能はＴＥＥ内のセキュアアプリケーションとして実装するのが望ましい。また、電子証明書を用いた相互認証に基づき、セキュアな通信路を確立するための汎用的な標準プロトコルとして、ＴＬＳ（Transport Layer Security）が広く用いられている。

[0012] しかし、Android（登録商標）等の通常の端末環境（ＲＥＥ: Rich Execution Environment）と比べて、ＴＥＥには限られた実行環境しか提供されておらず、ＴＬＳプロトコルをフルに実装するセキュアアプリケーションの実装コストは高いことが想定される。特に、汎用的なクライアント・サーバ間の相互認証プロトコルであるＴＬＳをそのまま実装すると、端末間の通信回数が多くなる。通信はＲＥＥで行うことが一般的であり、ＴＥＥとＲＥＥ間のコンテキストスイッチを意識した状態管理が煩雑となることが想定される。なお、ＣＰＵの状態のことをコンテキスト、保存と復帰を行いコンテキストを切り替えることをコンテキストスイッチという。

[0013] このような背景を鑑みて本発明がなされたのであり、本発明は、端末間の通信回数を削減することができる端末登録システムおよび端末登録方法を提供することを課題とする。

課題を解決するための手段

[0014] 前記した課題を解決するため、請求項１に記載の発明は、秘密鍵を用いてＦＩＤＯ認証する複数の端末と、前記端末が利用するサービスサイトとが通信可能に接続され、登録済み端末を用いて、複数の前記サービスサイトに対する新規端末を登録する端末登録システムであって、前記端末は、ＴＥＥを含むセキュア領域に、端末の所有者を示す所有者証明書を発行する証明書発行部と、同一の所有者証明書を有する端末間で連携をする連携部と、暗号鍵を生成する暗号鍵生成部と、認証用秘密鍵を管理する認証鍵管理部と、を備え、ＲＥＥを含む端末環境に、端末間の通信を行う通信部を備え、前記新規

端末は、当該新規端末側の前記通信部から前記登録済み端末に対して、暗号鍵による暗号化通信の開始要求を行い、前記登録済み端末の前記連携部は、前記認証用秘密鍵を前記暗号鍵で暗号化した連携用データを、同一の前記所有者証明書を有する前記新規端末に送付することを特徴とする端末登録システムとした。

[0015] また、請求項７に記載の発明は、秘密鍵を用いてＦＩＤＯ認証する複数の端末と、前記端末が利用するサービスサイトとが通信可能に接続され、登録済み端末を用いて、複数の前記サービスサイトに対する新規端末を登録する端末登録システムの端末登録方法であって、前記端末は、ＴＥＥ（Trusted Execution Environmen）を含むセキュア領域に、端末の所有者を示す所有者証明書を発行する証明書発行部と、同一の所有者証明書を有する端末間で連携をする連携部と、暗号鍵を生成する暗号鍵生成部と、認証用秘密鍵を管理する認証鍵管理部と、を有し、ＲＥＥを含む端末環境に、端末間の通信を行う通信部を有し、前記新規端末は、当該新規端末側の前記通信部から前記登録済み端末に対して、暗号鍵による暗号化通信の開始要求を行うステップを実行し、前記登録済み端末の前記連携部は、前記認証用秘密鍵を前記暗号鍵で暗号化した連携用データを、同一の前記所有者証明書を有する前記新規端末に送付するステップを実行する端末登録方法とした。

[0016] このようにすることで、一つのオペレーション（端末間での証明書の交換処理／端末間の連携処理）において、必須となる通信回数は最大でも端末間で１往復となる。これにより、ＲＥＥへのコンテキストスイッチを意識したＴＥＥ内の状態数が削減される。

[0017] 請求項２に記載の発明は、前記連携部が、所定時間内の通信開始要求回数を判定する閾値を有し、前記登録済み端末の前記連携部は、前記新規端末からの通信開始要求回数が前記閾値を超えた場合、前記連携用データの送付を行わないことを特徴とする請求項１に記載の端末登録システムとした。

[0018] このようにすることで、暗号化データを多数取得することにより暗号鍵の生成方法を推測し、認証鍵を盗難しようとする攻撃を防ぐことができる。

[0019] 請求項３に記載の発明は、前記登録済み端末の前記連携部は、前記新規端末側で前記暗号鍵が利用可能になることを確認することなく、前記連携用データの送付を行うことを特徴とする請求項１に記載の端末登録システムとした。

[0020] このようにすることで、ＴＬＳと比較して端末間の通信回数を削減することができる。

[0021] 請求項４に記載の発明は、前記連携部は、前記新規端末からの通信開始要求回数が前記閾値を超えた場合、ユーザに知らせる提示手段と、ユーザによる可否の判断を受付ける受付手段と、をさらに備えることを特徴とする請求項２に記載の端末登録システムとした。

[0022] このようにすることで、ユーザによる誤操作等の可能性を排除することができる。ＴＥＥの警告画面は、マルウェア等によって改ざんできないため、セキュアにユーザ意志を確認できる。

[0023] 請求項５に記載の発明は、前記連携部は、連携処理時に、連携処理中の前記新規端末をユーザに通知することを特徴とする請求項１に記載の端末登録システムとした。

[0024] このようにすることで、意図しない端末間で連携が行われようとしていることに気づきやすくなる効果がある。

[0025] 請求項６に記載の発明は、前記登録済み端末の前記証明書発行部は、ユーザが命名する前記新規端末の名称を、前記所有者証明書と紐付けて保管することを特徴とする請求項１に記載の端末登録システムとした。

[0026] このようにすることで、他証明書を取得する際に、その端末を識別可能なわかりやすい名称を、ユーザがセキュアに命名できる。

発明の効果

[0027] 本発明によれば、端末間の通信回数を削減することができる端末登録システムおよび端末登録方法を提供することができる。

図面の簡単な説明

[0028] [図1]本発明の実施形態に係る端末登録システムを示す構成図である。

[図2]本実施形態に係る端末登録システムの端末間の相互認証を実装する場合のシーケンス図である。

[図3]比較例のＴＬＳ標準を実装した場合のＴＥＥの必要状態を示す状態遷移図である。

[図4]本実施形態に係る端末登録システムのＴＥＥの必要状態を示す状態遷移図であり、（ａ）は端末間での証明書の交換処理を示し、（ｂ）は端末間の連携処理を示す。

[図5]本実施形態に係る端末登録システムの所有者証明書の発行シーケンスを示す図である。

[図6]本実施形態に係る端末登録システムのサービスサイトへの鍵登録を示すシーケンス図である。

[図7]本実施形態に係る端末登録システムのサービスサイトへの認証を示すシーケンス図である。

[図8]本実施形態に係る端末登録システムの証明書の交換シーケンスを示す図である。

[図9]本実施形態に係る端末登録システムの端末間の連携のシーケンスを示す図である。

[図10]図９に続くシーケンス図である。

[図11]本実施形態に係る端末登録システムの閾値超過時の処理を適用した端末間の連携のシーケンスを示す図である。

[図12]本実施形態に係る端末登録システムの名称命名機能を適用した証明書の交換のシーケンスを示す図である。

[図13]本実施形態に係る端末登録システムの意図しない端末の確認処理を適用した端末間の連携のシーケンスを示す図である。

[図14]標準技術（ＦＩＤＯ）の特徴を説明する図であり、（ａ）は端末の認証を示し、（ｂ）は新規端末の登録を示す。

[図15]端末間の連携による認証鍵のコピー技術（手法１）を説明する図である。

[図16]電子署名の付与による登録認可技術（手法２）を説明する図である。

[図17]同一の所有者証明書を有する端末間でしか連携をしないようにする手法３を説明する図である。

[図18]標準的なＴＬＳに基づいて端末間の相互認証を実装する場合のシーケンス図である。

発明を実施するための形態

[0029] 以下、図面を参照して本発明を実施するための形態（以下、「本実施形態」という）における端末登録システム等について説明する。

まず、本発明と既存技術との関係性について説明する。

図１８は、標準的なＴＬＳに基づいて端末間の相互認証を実装する場合のシーケンス図である。

図１８おいて、端末１は既存端末Ａ（以下、既存端末Ａ１）であり、端末２は新規端末Ｂ（以下、新規端末Ｂ２）であるとする。

新規端末Ｂ２は、例えば追加や変更（例えば、スマートフォンとタブレット端末の２台持ち、端末の機種変更）である。この場合、ＦＩＤＯ標準では、新規端末Ｂ２で新たに鍵ペアの生成・各Ｗｅｂサービスへの紐づけ（Registration）が必要となる。しかし、煩雑となる。そこで、秘密鍵を既存端末Ａ１から複製してくることにより、新規端末Ｂ２でのRegistration実行を回避する。

[0030] シーケンスは、ＴＬＳにおけるクライアントとなった側、ここでは既存端末Ａ１から通信を開始する。既存端末Ａ１は、新規端末Ｂ２に通信開始要求を送信する（ステップＳ１１）。

新規端末Ｂ２は、リプレイ攻撃を防ぐために、乱数を生成して通信要求（乱数Ｂ＋所有者証明書Ｂ）を送付する（ステップＳ１２）。

[0031] 既存端末Ａ１は、新規端末Ｂ２から送付された証明書を検証・比較する（ステップＳ１３）。証明書の検証がＯＫであれば、新規端末Ｂ２に所有者証明書Ａを送信する（ステップＳ１４）。

新規端末Ｂ２は、既存端末Ａ１から送付された証明書を検証・比較する（

ステップＳ１５）。

[0032] 既存端末Ａ１は、所有者証明書Ａの送信後、連携用データを送付する側である既存端末Ａで暗号鍵Ａを生成する（ステップＳ１６）。

既存端末Ａ１は、受信した所有者証明書Ｂに紐づく公開鍵で暗号鍵Ａ Wrapする（ステップＳ１７）。

新規端末Ｂ２は、所有者証明書Ｂのユーザが通信していることの証明のため、所有者証明書Ｂに紐づく秘密鍵で暗号鍵Ａ Unwrapする（ステップＳ１８）。

[0033] 既存端末Ａ１は、所有者証明書Ａのユーザが通信していることの証明のため、これまでの通信内容に所有者証明書Ａに紐づく秘密鍵で署名する（ステップＳ１９）。

新規端末Ｂ２は、所有者証明書Ａのユーザが通信相手であることの確認のため、公開鍵Ａで署名検証する（ステップＳ２０）。

[0034] 既存端末Ａ１は、新規端末Ｂ２に暗号化通信の開始通知を行う（ステップＳ２１）。

新規端末Ｂ２は、既存端末Ａ１からの開始通知を受けて、既存端末Ａ１にUnwrapした暗号鍵Ａを利用して暗号化通信の開始通知を行う（ステップＳ２２）。

既存端末Ａ１は、新規端末Ｂ２からの開始通知により、所有者証明書Ｂのユーザが通信相手であることの確認ができる。

[0035] 既存端末Ａ１は、実際のデータ通信を開始し、暗号鍵Ａで暗号化して連携用データを送信する（ステップＳ２３）。

以上、標準的なＴＬＳに基づいて端末間の相互認証を実装する場合のシーケンスについて説明した。

[0036] 標準的なＴＬＳは、汎用的なクライアント・サーバ間の相互認証プロトコルであるＴＬＳをそのまま実装する。図１８に示すように、ＴＬＳをそのまま実装しているので、端末間の通信回数が多くなる。また、通信は、ＲＥＥで行うことが一般的であり、ＴＥＥとＲＥＥ間のコンテキストスイッチを意

識した状態管理が煩雑となることが想定される。

ここで、想定するＴＥＥアプリ開発における一般的な制限について述べる。

（１）ＴＥＥアプリ実装時に利用可能な標準ライブラリ群は限定されている。

（２）ＴＥＥアプリはＣ言語による実装が前提である。このため、より生産性の高い先端的な開発言語（Java, Python等）は利用できない。

（３）ＲＥＥアプリとは別の個別の配信サーバを用意することが前提である。このため、ＴＥＥアプリのアップデートは高コストとなる。

[0037]（実施形態）

図１は、本発明の実施形態に係る端末登録システムを示す構成図である。

［端末登録システムの全体構成］

図１に示すように、本実施形態に係る端末登録システム１０００は、既存端末Ａ１１０（登録済み端末）、新規端末Ｂ１２０に加え、ネットワーク上に、他の当事者に公開鍵証明書を発行する認証局１３０と、サービスサイト１４０と、を含んで構成される。

端末登録システム１０００は、秘密鍵を用いてＦＩＤＯ認証する複数の端末と、端末が利用するサービスサイト１４０とが通信可能に接続され、既存端末Ａ１１０を用いて、サービスサイト１４０に対する新規端末Ｂ１２０を登録する。

なお、既存端末Ａ１１０と、新規端末Ｂ１２０と、認証局１３０と、サービスサイト１４０とは、通信ネットワーク（図示省略）で接続されており、相互に通信可能である。

[0038]〈サービスサイト１４０〉

サービスサイト１４０は、Ｗｅｂアプリケーションサーバ（Web application server）と、ＦＩＤＯサーバと、を備える。Ｗｅｂアプリケーションサーバは、ソフトウェアの実行環境や連携機能などを持つＷｅｂサーバである。Ｗｅｂアプリケーションサーバは、ＦＩＤＯサーバと接続・連携して複雑な

処理を行う機能を持つ。Ｗｅｂアプリケーションサーバは、例えばＥＣ（Electronic Commerce）サイトを運営するサービス事業者が運用するＷｅｂサーバであり、サービスを利用するユーザの登録と認証とを行う。

[0039] 〈既存端末Ａ１１０，新規端末Ｂ１２０の構成〉

既存端末Ａ１１０，新規端末Ｂ１２０は、認証用端末であり、例えばスマートフォン，携帯電話，タブレット等の携帯端末、ノート型／デスクトップ型ＰＣ、各種電子機器である。本実施形態では、スマートフォンを例に採る。

既存端末Ａ１１０，新規端末Ｂ１２０は、通常のアプリケーション（以下、アプリという）等が動作する領域である通常の端末環境（ＲＥＥ）と、マルウェア等が混入しないように管理されたセキュア領域（ＴＥＥ）とを論理的に備える。ＲＥＥは、一般のアプリケーションプログラムが実行される環境である。また、ＴＥＥは、セキュア領域であり、生体情報（指紋情報など）が保管される。ＴＥＥは、ＣＰＵ（Central Processing Unit）やＯＳ（Operating System）の特権モードで実行され、特定のプログラムや特定の手順によってのみ、ＴＥＥのプログラムの呼び出しやデータへのアクセスが可能となる。

[0040] まず、既存端末Ａ１１０の構成について説明する。

既存端末Ａ１１０のＲＥＥには、端末間連携アプリ１１１（通信部）と、認証アプリ１１２と、証明書発行アプリ１１３とが備わる。

図１の矢印に示すように、既存端末Ａ１１０の端末間連携アプリ１１１は、新規端末Ｂ１２０の端末間連携アプリ１２１との間でＲＥＥによる通信を行う。

[0041] 既存端末Ａ１１０のＴＥＥには、同一の所有者証明書を有する端末間で連携をする既存端末側連携部１１４と、認証アプリ１１２に接続される認証部１１５と、認証用秘密鍵を管理する認証鍵管理部１１６と、証明書発行アプリ１１３に接続され、端末の所有者を示す所有者証明書を発行する証明書発行部１１７と、証明書管理部１１８とが備わる。

[0042] 既存端末側連携部１１４は、既存端末側連携機能群として、関数１－１（後記）に従って証明書を受信する証明書受信部１１４ａと、関数２－１（後記）に従って証明書を送信する証明書送信部１１４ｂと、関数３Ａ－１（後記）に従って端末間連携を行う端末間連携部１１４ｃと、を有する。上記関数は、制御シーケンスのなかで、各部が特定の操作または処理を実行する機能を便宜的にいうものである。

また、既存端末側連携部１１４は、暗号鍵を生成する暗号鍵生成部としての機能を有する。

[0043] 既存端末側連携部１１４は、所定時間内の通信開始要求回数を判定する閾値を有し、新規端末Ｂ１２０からの通信開始要求回数が閾値を超えた場合、連携用データの送付を行わない。

既存端末側連携部１１４は、新規端末Ｂ１２０側で暗号鍵が利用可能になることを確認することなく、連携用データの送付を行う。

既存端末側連携部１１４は、端末間の所有者証明書の交換、検証および比較を、端末間の連携に先立って行う。

既存端末側連携部１１４は、新規端末Ｂ１２０からの通信開始要求回数が閾値を超えた場合、ユーザに知らせる提示手段と、ユーザによる可否の判断を受付ける受付手段と、をさらに備える。

既存端末側連携部１１４は、連携処理時に、連携処理中の新規端末をユーザに通知する。

[0044] 認証鍵管理部１１６は、サービスサイト１４０ごとの鍵（例えばＲＳＡ等の非対称鍵）である認証用秘密鍵Ａを有する。

[0045] 証明書発行部１１７は、端末の所有者を示す所有者証明書を発行する。証明書発行部１１７は、ユーザが命名する新規端末の名称を、所有者証明書と紐付けて保管する。

[0046] 証明書管理部１１８は、本人証明秘密鍵Ａと、自証明書Ａと、他証明書とを管理する。

上記自証明書Ａは、自端末の公開鍵証明書（例えばX.509形式）であり、ま

た本人証明秘密鍵Ａは、この公開鍵証明書に紐づく秘密鍵である。上記他証明書は、保存した他端末の公開鍵証明書（例えばX.509形式）である。

[0047] 次に、新規端末Ｂ１２０の構成について説明する。新規端末Ｂ１２０は、既存端末Ａ１１０と同様の構成を採る。

新規端末Ｂ１２０のＲＥＥには、端末間連携アプリ１２１（通信部）と、認証アプリ１２２と、証明書発行アプリ１２３とが備わる。

図１の矢印に示すように、新規端末Ｂ１２０の端末間連携アプリ１２１は、既存端末Ａ１１０の端末間連携アプリ１１１との間でＲＥＥによる通信を行う。

[0048] 新規端末Ｂ１２０のＴＥＥには、同一の所有者証明書を有する端末間で連携をする新規端末側連携部１２４と、認証アプリ１２２に接続される認証部１２５と、認証用秘密鍵を管理する認証鍵管理部１２６と、証明書発行アプリ１２３に接続され、端末の所有者を示す所有者証明書を発行する証明書発行部１２７と、証明書管理部１２８とが備わる。

[0049] 新規端末側連携部１２４は、新規端末側連携機能群として、関数１－１（後記）に従って証明書を受信する証明書受信部１２４ａと、関数２－１（後記）に従って証明書を送信する証明書送信部１２４ｂと、関数３Ａ－１（後記）に従って端末間連携を行う端末間連携部１２４ｃと、を有する。

認証鍵管理部１２６は、サービスサイト１４０ごとの鍵（例えばＲＳＡ等の非対称鍵）である認証用秘密鍵Ａを有する。

証明書管理部１２８は、本人証明秘密鍵Ｂと、自証明書Ｂと、他証明書とを管理する。

上記自証明書Ａは、自端末の公開鍵証明書（例えばX.509形式）であり、また本人証明秘密鍵Ｂは、この公開鍵証明書に紐づく秘密鍵である。上記他証明書は、保存した他端末の公開鍵証明書（例えばX.509形式）である。

[0050] 以下、上述のように構成された端末登録システムの端末登録方法について説明する。

［動作概要］

まず、本実施形態に係る端末登録システムの端末登録方法の動作概要について述べる。

本実施形態に係る端末登録システムは、新規端末をセットアップするための端末間の相互認証というユースケースに絞ることで、ＴＬＳのシーケンス図（図１８参照）と比較して端末間の通信回数を削減することを特徴とする。

[0051] 想定するユースケースとシンプル化ポイントは、下記の通りである。

（１）端末間の関係性は、同等であるとする。すなわち、どちらの端末がクライアント、サーバというわけではなく、同等である。これにより、クライアントから通信の開始要求を行うプロセスを省略する。

（２）端末間連携の頻度は、それほど多くないものとする。端末間連携の頻度は、新規端末を利用開始する場合、あるいはいずれかの端末で新規サイトの登録を行い、端末間の鍵の同期が必要となった場合に限定する。

（３）一定時間内の通信要求回数に制限をつけた上で、相手側で暗号鍵が利用可能になったかを確認せずに連携用データの送付を行う。

（４）特定の端末間でのみ連携を行う（すなわち、サーバが不特定多数のクライアントから通信を受け付けるモデルではない）。このため、端末間での所有者証明書の交換・検証・比較は、連携時ではなく事前に行っておくことにする。

[0052] なお、同一人物が、既存端末Ａと新規端末Ｂとを両方持っており、既存端末Ａから新規端末Ｂに、乗り換えて鍵を登録する場合は問題ない。また、既存端末Ａから通信の開始要求を始める場合は、新規端末Ｂが悪意の人であるとしても攻撃されるおそれはない。しかし、本実施形態の構成を採り、しかも新規端末Ｂが悪意の人だった場合、端末間の関係性が同等であるとすると、新規端末Ｂによる擾乱のリスクが増えるおそれがある。

そこで、本実施形態に係る端末登録システムでは、悪意の第三者にデータを集めさせないために、一定時間内の通信要求回数に制限することで、擾乱のリスク回避を図る。

[0053] 図２は、本実施形態に係る端末登録システムの端末間の相互認証を実装する場合のシーケンス図である。

図２では、前記図１８に示すシーケンス図と同一処理を行うシーケンスには同一ステップ番号を付している。

図２において、図１８と対比して削減された処理ブロックおよび通信手順については破線で示している。すなわち、図２の破線に示す処理ブロックおよび通信手順は、削減されており存在しないが、説明の便宜上、表記したものである。

[0054] ＴＬＳ標準では暗号鍵を生成するクライアントから通信を開始するが、本実施形態に係る端末登録システムの端末間連携のユースケースでは、サーバ側（暗号鍵を受け取る側）、ここでは新規端末Ｂ２から通信を開始する。新規端末Ｂ２は、リプレイ攻撃を防ぐために、乱数を生成して通信要求（乱数Ｂ＋所有者証明書Ｂ）を送付する（ステップＳ１２）。すなわち、図２の破線に示す既存端末Ａ１からの通信開始要求（前記図１８のステップＳ１１）は存在しない。

上記（１）の「端末間の関係性が同等であること」を適用したものである。

[0055] 次に、上記（４）の「特定の端末間でのみ連携を行うこと」を適用することで、前記図１８のステップＳ１３、ステップＳ１４、ステップＳ１５を省く。連携の可能性がある端末間で事前に所有者証明書の交換・検証が済んでいることを前提とする。

[0056] 既存端末Ａ１は、ＴＬＳ標準のシーケンスのように新規端末Ｂ２に所有者証明書Ａを送信することなく、直ちに暗号鍵Ａを生成する（ステップＳ１６）。

既存端末Ａ１は、受信した所有者証明書Ｂに紐づく公開鍵で暗号鍵Ａ Wrapする（ステップＳ１７）。

新規端末Ｂ２は、所有者証明書Ｂのユーザが通信していることの証明のため、所有者証明書Ｂに紐づく秘密鍵で暗号鍵Ａ Unwrapする（ステップＳ１８

）。

[0057] 既存端末Ａ１は、所有者証明書Ａのユーザが通信していることの証明のため、これまでの通信内容に所有者証明書Ａに紐づく秘密鍵で署名する（ステップＳ１９）。

新規端末Ｂ２は、所有者証明書Ａのユーザが通信相手であることの確認のため、公開鍵Ａで署名検証する（ステップＳ２０）。

[0058] ＴＬＳ標準では暗号鍵を生成するクライアントから暗号化通信の開始通知を行い、クライアントはサーバからの開始通知を受け取るが、本実施形態に係る端末登録システムの端末間連携のシーケンスでは、これらクライアント・サーバ間の暗号化通信の開始通知を省略する（前記図１８のステップＳ２１、ステップＳ２２を省略する）。すなわち、上記ステップＳ２０までで、たがいに暗号鍵でやり取りができている。第三者は鍵をもっておらず、Unwrapできないので、鍵を送るのと同時に先行してデータを送っても、第三者は復号化できないであろうという考え方である。

[0059] ただし、暗号学的にはセキュリティレベルを少し下げていることになる。本実施形態に係る端末登録システムでは、鍵の再登録の頻度は低く攻撃を受ける可能性が小さいことと、悪意の第三者にデータを集めさせないために、一定時間内の通信要求回数に制限することで、リスク回避を行っている。

[0060] 上記（３）の「一定時間内の通信要求回数に制限」（後記）するため、既存端末Ａ１は、一定時間内の送信回数を確認する（ステップＳ３１）。

既存端末Ａ１は、実際のデータ通信を開始し、暗号鍵Ａで暗号化して連携用データを送信する（ステップＳ２３）。

[0061] 上記一定時間内の通信要求回数に制限（ステップＳ３１）について説明する。

・通信回数の削減アプローチ

本実施形態に係る端末登録システムの端末間連携のシーケンスでは、暗号化通信の開始通知（新規端末Ｂ２で暗号鍵ＡのUnwrapができたかどうかの確認）を行うことなく、暗号鍵Ａによる暗号通信を開始する。暗号化通信の開

始通知を行うことなく、暗号鍵Ａによる暗号通信を開始できる理由は、相手が秘密鍵Ｂを持たない攻撃者の端末でも、暗号鍵ＡのUnwrapができないと連携用データを復号できない、からである。ただし、下記リスクが残存する。

[0062] ・残存するリスク

新規端末Ｂ２が悪意の端末であるとする。攻撃者である新規端末Ｂ２が何度も通信要求を行い、多数の暗号化された連携用データを取得する。これにより、新規端末Ｂ２は、暗号鍵Ａの生成ルールの推測を試みることができる。

・上記リスクの対策

本実施形態では、一定時間内に、既存端末Ａが通信要求に対応する回数の閾値を設けておき、その回数を超過した場合、要求を拒否する（ステップＳ３１）。

以上、本実施形態に係る端末登録システムの端末間連携のシーケンスについて説明した。

[0063] ［作用効果］

次に、本実施形態に係る端末登録システムの作用効果について説明する。

〈比較例〉

図３は、比較例のＴＬＳ標準を実装した場合のＴＥＥの必要状態を示す状態遷移図である。図３中、左側が既存端末Ａ側の状態、右側が新規端末Ｂ側の状態である。

ＴＬＳ標準を実装した場合のＴＥＥでは、既存端末Ａ側と新規端末Ｂ側とは、端末間の連携処理を行う。換言すれば、既存端末Ａ側と新規端末Ｂ側とは、端末間の連携処理を行うことが前提である。

既存端末Ａ側の状態Ａ－１では、新規端末Ｂ側に通信開始要求を発行する（図３の符号ａ参照）。また、通信によるコンテキストスイッチを行って、状態Ａ－２に遷移する（図３の符号ｂ参照）。

[0064] 新規端末Ｂ側では、既存端末Ａ側からの通信開始要求をトリガとして状態Ｂ－１が発生する。新規端末Ｂ側の状態Ｂ－１では、乱数Ｂの生成および証

明書Ｂを取得して、既存端末Ａ側に乱数Ｂおよび証明書Ｂを送付するとともに（図３の符号ｃ参照）、状態Ｂ－２に遷移する（図３の符号ｄ参照）。

[0065] 既存端末Ａ側の状態Ａ－２では、新規端末Ｂ側からの応答待ち、証明書Ｂ検証／（「／」は、「および／または」、を表記する。以下同様。）比較、証明書Ａ取得、暗号鍵生成／Wrap、および通信内容署名を行って、新規端末Ｂ側にこれら証明書Ａ、Wrap暗号鍵、署名付情報、および暗号通信開始通知を送付するとともに（図３の符号ｅ参照）、状態Ａ－３に遷移する（図３の符号ｆ参照）。

[0066] 新規端末Ｂ側の状態Ｂ－２では、既存端末Ａ側からの証明書Ａ、Wrap暗号鍵、署名付情報、暗号通信開始通知を受信する。状態Ｂ－２では、既存端末Ａ側からの応答待ち、証明書Ａ検証／比較、暗号鍵Unwrap、および署名検証を行って、既存端末Ａ側に暗号通信開始通知を送付するとともに（図３の符号ｇ参照）、状態Ｂ－３に遷移する（図３の符号ｈ参照）。

[0067] 既存端末Ａ側の状態Ａ－３では、新規端末Ｂ側からの応答待ち、データ暗号化を行って、新規端末Ｂ側に連携用データを送付する（図３の符号ｉ参照）。

新規端末Ｂ側の状態Ｂ－３では、既存端末Ａ側からの応答待ち、受信した連携用データをデータ保管する。

なお、既存端末Ａ側の状態Ａ－３と新規端末Ｂ側の状態Ｂ－３で状態遷移は終了となる。

[0068] 〈実施形態〉

図４は、本実施形態に係る端末登録システムのＴＥＥの必要状態を示す状態遷移図であり、図４（ａ）は端末間での証明書の交換処理を示し、図４（ｂ）は端末間の連携処理を示す。図４（ａ）（ｂ）中、左側が既存端末Ａ側の状態、右側が新規端末Ｂ側の状態である。

本実施形態に係る端末登録システムは、端末間での証明書の交換処理と、端末間の連携処理とに分けられる。

図４（ａ）に示す端末間での証明書の交換処理は、端末ペアごとに一度だ

け実行される。なお、図４（ａ）の状態ｘは、既存端末Ａ側または新規端末Ｂ側で同じ処理であることを示している。

[0069] 図４（ａ）に示すように、一方の端末側の状態ｘ－１では、証明書ｘを取得し、他方の端末側の状態ｙ－１にこの証明書ｘを送付する。

他方の端末側の状態ｙ－１では、証明書ｘを検証／比較し、証明書ｘ保管する。

例えば、一方の端末側が既存端末Ａ側である場合、既存端末Ａ側の状態ｘ－１では、証明書ｘを取得し、新規端末Ｂ側の状態ｙ－１にこの証明書ｘを送付する（図４（ａ）の符号ｊ参照）。新規端末Ｂ側の状態ｙ－１では、証明書ｘを検証／比較し、証明書ｘ保管する。このような証明書の交換処理は、端末ペア毎に一度だけ実行される。

[0070] 図４（ｂ）に示すように、端末間の連携処理は、新規端末Ｂ側の状態Ｂ－１が開始となる。新規端末Ｂ側の状態Ｂ－１が開始となる理由については、前記図２の暗号鍵を受け取る側の新規端末Ｂ２から通信を開始するシーケンスで説明した。

[0071] 新規端末Ｂ側の状態Ｂ－１では、乱数Ｂを生成し、既存端末Ａ側に生成した乱数Ｂを送付するとともに（図４（ｂ）の符号ｋ参照）、通信によるコンテキストスイッチを行って、状態Ｂ－３に遷移する（図４（ｂ）の符号ｌ参照）。

[0072] 既存端末Ａ側の状態Ａ－１では、受信した乱数Ｂをもとに、暗号鍵生成／Wrap、通信内容署名、通信回数確認、およびデータ暗号化を行って、新規端末Ｂ側にこれらWrap暗号鍵、署名付情報、および連携用データを送付する（図４（ｂ）の符号ｍ参照）。

[0073] 新規端末Ｂ側の状態Ｂ－３では、既存端末Ａ側からの応答待ち、暗号鍵Unwrap、署名検証、およびデータ保管する。

なお、既存端末Ａ側の状態Ａ－１と新規端末Ｂ側の状態Ｂ－３で状態遷移は終了となる。

[0074] 図３に示す比較例と、図４に示す本実施形態とを比較して分かるように、

本実施形態では、一つのオペレーション（端末間での証明書の交換処理／端末間の連携処理）において、必須となる通信回数は最大でも端末間で１往復となる。これにより、ＲＥＥへのコンテキストスイッチを意識したＴＥＥ内の状態数が削減される。

[0075] ［実施例］

以下、本実施形態の実施例について説明する。

所有者証明書の発行シーケンス（図５参照）、サービスサイトへの鍵登録（図６参照）、およびサービスサイトへの認証シーケンス（図７参照）は、既存技術にそのまま適用したものである。この既存技術については、既存端末Ａ１１０と新規端末Ｂ１２０とは、同一処理を行う。このため、既存端末Ａ１１０の処理を代表して説明する。

[0076] 〈所有者証明書の発行シーケンス〉

所有者証明書の発行シーケンスは、一般的な電子証明書の発行手順に従い、端末に所有者証明書（自証明書）を発行する。

図５は、所有者証明書の発行シーケンスを示す図である。

ユーザは、申請情報入力を含む証明書発行の操作を行う（ステップＳ１０１）。ユーザによる証明書発行の操作は、証明書発行アプリ１１３が受付ける。

証明書発行アプリ１１３は、証明書発行部１１７に本人証明鍵の生成要求を送付する（ステップＳ１０２）。

証明書発行部１１７は、非対称鍵ペアの生成を行う（ステップＳ１０３）。

証明書発行部１１７は、証明書管理部１１８に本人証明用秘密鍵を送付する（ステップＳ１０４）。

証明書管理部１１８は、証明書管理部１１８から送付された本人証明用秘密鍵を保管する（ステップＳ１０５）。

[0077] 証明書発行部１１７は、証明書発行アプリ１１３に本人証明用公開鍵を送付する（ステップＳ１０６）。

証明書発行アプリ１１３は、証明書発行要求（ＣＳＲ）の生成を行う（ステップＳ１０７）。

証明書発行アプリ１１３は、証明書発行部１１７を経由して証明書管理部１１８にＣＳＲへの署名要求を送付する（ステップＳ１０８）。

証明書管理部１１８は、秘密鍵での署名を行う（ステップＳ１０９）。

証明書管理部１１８は、証明書発行部１１７を経由して証明書発行アプリ１１３に署名付きＣＳＲを送付する（ステップＳ１１０）。

証明書発行アプリ１１３は、認証局１３０に署名付きＣＳＲを送付する（ステップＳ１１１）。

[0078] 認証局１３０は、署名検証を行う（ステップＳ１１２）。

認証局１３０は、ユーザに対面での身分証確認等により申請情報の正当性を確認する（ステップＳ１１３）。

認証局１３０は、申請情報の正当性確認した場合、証明書発行アプリ１１３に所有者証明書を発行する（ステップＳ１１４）。

証明書発行アプリ１１３は、証明書発行部１１７を経由して証明書管理部１１８に所有者証明書を送付する（ステップＳ１１５）。

証明書管理部１１８は、秘密鍵と紐付けて自証明書として保管する（ステップＳ１１６）。

証明書管理部１１８は、証明書発行部１１７を経由して証明書発行アプリ１１３に完了通知を送付する（ステップＳ１１７）。

証明書発行アプリ１１３は、ユーザに完了通知を送付する（ステップＳ１１８）。

[0079] 〈サービスサイトへの鍵登録〉

ＦＩＤＯ ＵＡＦが規定する認証方式に基づき、端末の公開鍵をサービスサイト１４０に登録する。

本登録処理は、ユーザが所有する端末のいずれか１台（ここでは既存端末Ａ１１０とする）でのみ行えばよい。それ以外の端末（ここでは新規端末Ｂ１２０）は、後述の端末間連携処理を行うことにより、既存端末Ａ１１０が

生成した秘密鍵を利用可能となるため、新たに新規端末Ｂ１２０で生成した公開鍵を登録する処理は不要となる。

[0080] 図６は、サービスサイトへの鍵登録を示すシーケンス図である。

ユーザは、認証アプリ１１２にサービスサイト１４０への登録操作を行う（ステップＳ２０１）。

認証アプリ１１２は、サービスサイト１４０の登録サイトへアクセスする（ステップＳ２０２）。

サービスサイト１４０は、認証アプリ１１２に登録要求を送付する（ステップＳ２０３）。

認証アプリ１１２は、認証部１１５に認証鍵の生成要求を送付する（ステップＳ２０４）。

認証部１１５は、ユーザに同意確認する（ステップＳ２０５）。

認証部１１５は、非対称鍵ペアの生成を行う（ステップＳ２０６）。

認証部１１５は、認証鍵管理部１１６に認証用秘密鍵を送付する（ステップＳ２０７）。

[0081] 認証鍵管理部１１６は、認証用秘密鍵を保管する（ステップＳ２０８）。

認証部１１５は、登録応答の生成を行う（ステップＳ２０９）。

認証部１１５は、登録応答への署名要求を送付する（ステップＳ２１０）。

認証鍵管理部１１６は、秘密鍵で署名生成する（ステップＳ２１１）。

認証鍵管理部１１６は、認証部１１５を経由して認証アプリ１１２に署名付き登録応答を送付する（ステップＳ２１２）。

認証アプリ１１２は、サービスサイト１４０に署名付き登録応答する（ステップＳ２１３）。

サービスサイト１４０は、署名検証する（ステップＳ２１４）。

サービスサイト１４０は、認証アプリ１１２に登録完了通知を送付する（ステップＳ２１５）。

認証アプリ１１２は、ユーザに完了通知を送付する（ステップＳ２１６）

。

[0082] 〈サービスサイトへの認証〉

ＦＩＤＯ ＵＡＦが規定する認証方式（チャレンジ・レスポンス認証）に基づき、サービスサイトへの認証を行う。

図７は、サービスサイトへの認証を示すシーケンス図である。

ユーザは、認証アプリ１１２にサービスサイトへの認証操作を行う（ステップＳ３０１）。

認証アプリ１１２は、サービスサイト１４０の認証サイトへアクセスする（ステップＳ３０２）。

サービスサイト１４０は、認証アプリ１１２にチャレンジ文字列等による認証要求を送付する（ステップＳ３０３）。

認証アプリ１１２は、認証部１１５に署名要求を送付する（ステップＳ３０４）。

[0083] 認証部１１５は、ユーザに同意確認する（ステップＳ３０５）。

認証部１１５は、認証鍵管理部１１６にチャレンジ文字列への署名要求を送付する（ステップＳ３０６）。

認証鍵管理部１１６は、サイトに対応する認証用秘密鍵での署名を行う（ステップＳ３０７）。

認証鍵管理部１１６は、認証部１１５を経由して認証アプリ１１２に署名付きチャレンジによる認証応答を行う（ステップＳ３０８）。

認証アプリ１１２は、サービスサイト１４０に署名付き認証応答を送付する（ステップＳ３０９）。

サービスサイト１４０は、署名検証を行う（ステップＳ３１０）。

サービスサイト１４０は、認証アプリ１１２に認証完了通知する（ステップＳ３１１）。

認証アプリ１１２は、ユーザに完了通知を送付する（ステップＳ３１２）。

[0084] 〈証明書の交換〉

証明書の交換シーケンスは、連携を行う端末間で所有者証明書を交換し、保管する。

証明書の交換シーケンスは、動作概要で述べた前記（４）の特定の端末間でのみ連携を行う動作の具体例である。サーバが不特定多数のクライアントから通信を受け付けるモデルではないため、端末間での所有者証明書の交換・検証・比較は、連携時ではなく事前に行っておく。この操作は、連携を行う端末ペア（既存端末Ａ１１０と新規端末Ｂ１２０）について、双方向に行っておく必要がある。

[0085] 図８は、証明書の交換シーケンスを示す図である。

送信側端末は、既存端末Ａまたは新規端末Ｂのいずれであってもよく、受信側端末は、既存端末Ａまたは新規端末Ｂのいずれであってもよい（ただし、送信側端末で選んだ端末の他方側）。図８では、送信側端末に図１の既存端末Ａ１１０を用い、受信側端末に図１の新規端末Ｂ１２０を用いた例である。

ユーザは、既存端末Ａ１１０の端末間連携アプリ１１１に対し証明書の送信操作を行うとともに（ステップＳ４０１）、新規端末Ｂ１２０の端末間連携アプリ１２１に対し証明書の受信操作を行う（ステップＳ４０２）。

新規端末Ｂ１２０の端末間連携アプリ１２１は、既存端末Ａ１１０の端末間連携アプリ１１１との間でＮＦＣ，Bluetooth等による通信路を確立する（ステップＳ４０３）。

[0086] 既存端末Ａ１１０の端末間連携アプリ１１１は、証明書送信部１１４ｂを経由して証明書管理部１１８に証明書取得要求を送信する（ステップＳ４０４）。

既存端末Ａ１１０の証明書管理部１１８は、証明書送信部１１４ｂを経由して端末間連携アプリ１１１に自証明書を発行する（ステップＳ４０５）。

上記、証明書送信部１１４ｂが証明書管理部１１８に証明書取得要求を送信し、証明書管理部１１８が証明書送信部１１４ｂに自証明書を発行する操作（図８の関数２－１破線囲み参照）が前記図１の証明書送信部１１４ｂの

「関数２－１」操作に該当する。

[0087] 既存端末Ａ１１０の端末間連携アプリ１１１は、証明書管理部１１８が発行した自証明書をもとに、新規端末Ｂ１２０の端末間連携アプリ１２１に所有者証明書（送信側証明書）を送付する（ステップＳ４０６）。

[0088] 新規端末Ｂ１２０の端末間連携アプリ１２１は、新規端末側連携部１２４の証明書受信部１２４ａに、新規端末Ｂ１２０の端末間連携アプリ１２１から送信された送信側証明書を送付する（ステップＳ４０７）。

証明書受信部１２４ａは、送信側証明書の検証を行う（ステップＳ４０８）。

証明書受信部１２４ａは、証明書管理部１２８に自証明書の要求を送付する（ステップＳ４０９）。

証明書管理部１２８は、証明書受信部１２４ａに受信側証明書を送付する（ステップＳ４１０）。

証明書受信部１２４ａは、送信側証明書と受信側証明書とを比較する（ステップＳ４１１）。送信側証明書と受信側証明書との比較は、ＣＮ（Common name）値が一致する等、予め定められた所有者一致条件を満たすか否かを確認する。

[0089] 証明書受信部１２４ａは、証明書管理部１２８に送信側証明書の保管要求を送付する（ステップＳ４１２）。

証明書管理部１２８は、送信側証明書を他証明書として保管する（ステップＳ４１３）。

証明書管理部１２８は、証明書受信部１２４ａに完了通知を送付する（ステップＳ４１４）。

上記図８の関数１－１破線囲み操作が前記図１の新規端末Ｂ１２０の証明書受信部１２４ａの「関数１－１」操作に該当する。

[0090] 証明書受信部１２４ａは、端末間連携アプリ１２１に完了通知を送付する（ステップＳ４１５）。

端末間連携アプリ１２１は、既存端末Ａ１１０の端末間連携アプリ１１１

に完了通知を送信する（ステップＳ４１６）。

既存端末Ａ１１０の端末間連携アプリ１１１は、ユーザに完了通知を送信する（ステップＳ４１７）。

新規端末Ｂ１２０の端末間連携アプリ１２１は、ユーザに完了通知を送信する（ステップＳ４１８）。

[0091] 〈端末間の連携〉

端末間の連携は、端末間を連携させて、認証用秘密鍵のセキュアな端末間複製を実現する。

[0092] 図９および図１０は、端末間の連携のシーケンスを示す図である。図１０は、図９に続くシーケンス図である。

送信側端末は、既存端末Ａであり、受信側端末は、新規端末Ｂである。

図９に示すように、ユーザは、既存端末Ａ１１０の端末間連携アプリ１１１に対し連携操作（例えば、端末間連携アプリの起動操作）を行うとともに（ステップＳ５０１）、新規端末Ｂ１２０の端末間連携アプリ１２１に対し連携操作を行う（ステップＳ５０２）。

新規端末Ｂ１２０の端末間連携アプリ１２１は、既存端末Ａ１１０の端末間連携アプリ１１１との間でＮＦＣ，Bluetooth等による通信路の確立を行う（ステップＳ５０３）。

[0093] 新規端末Ｂ１２０の端末間連携アプリ１２１は、新規端末側連携部１２４の端末間連携部１２４ｃに受信側開始処理を要求する（ステップＳ５０４）。

端末間連携部１２４ｃは、乱数Ｂを生成／保持する（ステップＳ５０５）。

端末間連携部１２４ｃは、証明書管理部１２８に自証明書のＩＤ参照を要求する（ステップＳ５０６）。

証明書管理部１２８は、端末間連携部１２４ｃに自証明書のＩＤ参照結果を送付する（ステップＳ５０７）。

上記、端末間連携部１２４ｃが乱数Ｂを生成／保持するとともに、証明書

管理部１２８に自証明書のＩＤ参照を要求し、証明書管理部１２８が端末間連携部１２４ｃに自証明書のＩＤ参照結果を送付する、操作（図９の関数３Ｂ－１破線囲み参照）が前記図１の端末間連携部１２４ｃの「関数３Ｂ－１」操作に該当する。

[0094] 端末間連携部１２４ｃは、端末間連携アプリ１２１に、乱数Ｂおよび自証明書ＩＤについて処理引き渡しを行う（ステップＳ５０８）。

新規端末Ｂ１２０の端末間連携アプリ１２１は、既存端末Ａ１１０の端末間連携アプリ１１１に、乱数Ｂおよび受信側証明書ＩＤについて複製要求通信を行う（ステップＳ５０９）。

既存端末Ａ１１０の端末間連携アプリ１１１は、既存端末側連携部１１４の端末間連携部１１４ｃに対し複製要求処理（複製要求通信）を行う（ステップＳ５１０）。

[0095] 以下、端末間連携部１１４ｃは、図９の破線囲みに示す関数３Ａ－１操作を実行する。この関数３Ａ－１操作は、図１の端末間連携部１１４ｃの「関数３Ａ－１」操作に該当する。すなわち、端末間連携部１１４ｃは、一定時間内の要求回数確認・更新を行う（ステップＳ５１１）。なお、要求回数が閾値を超過した場合の準正常処理は図１１で後述する。

端末間連携部１１４ｃは、暗号鍵Ａ生成を行う（ステップＳ５１２）。

端末間連携部１１４ｃは、証明書管理部１１８に他証明書（受信側証明書ＩＤ）を要求する（ステップＳ５１３）。

証明書管理部１１８は、端末間連携部１１４ｃに他証明書（受信側）を送付する（ステップＳ５１４）。

[0096] 端末間連携部１１４ｃは、他証明書の公開鍵で暗号鍵ＡをWrapする（ステップＳ５１５）。

端末間連携部１１４ｃは、証明書管理部１１８に複製要求通信への署名要求を送付（ステップＳ５１６）。

証明書管理部１１８は、自証明書に紐づく秘密鍵で署名する（ステップＳ５１７）。

証明書管理部１１８は、端末間連携部１１４ｃに対し署名付き複製要求通信を行う（ステップＳ５１８）。

[0097] 端末間連携部１１４ｃは、ユーザとの間でユーザの同意確認を行う（ステップＳ５１９）。

端末間連携部１１４ｃは、認証鍵管理部１１６に認証用秘密鍵取得の要求を送付する（ステップＳ５２０）。

認証鍵管理部１１６は、取得要求された認証用秘密鍵を端末間連携部１１４ｃに送付する（ステップＳ５２１）。

端末間連携部１１４ｃは、秘密鍵を暗号鍵Ａで暗号化する（ステップＳ５２２）。

端末間連携部１１４ｃは、証明書管理部１１８に自証明書のＩＤ参照を要求する（ステップＳ５２３）。

証明書管理部１１８は、端末間連携部１１４ｃに自証明書を送付する（ステップＳ５２４）。

上記、端末間連携部１１４ｃが一定時間内の要求回数確認・更新（ステップＳ５１１）～端末間連携部１１４ｃが証明書管理部１１８から自証明書を受け取る（ステップＳ５２４）までの操作（図９の関数３Ａ－１破線囲み参照）が前記図１の端末間連携部１１４ｃの「関数３Ａ－１」操作に該当する。

[0098] 端末間連携部１１４ｃは、端末間連携アプリ１１１を経由して新規端末Ｂ１２０の端末間連携アプリ１２１に、Wrapされた暗号鍵Ａ、署名付き複製要求通信、暗号化された認証鍵、送信側証明書ＩＤを送付する複製応答通信を行う（ステップＳ５２５）。

[0099] 図１０に示すように、新規端末Ｂ１２０の端末間連携アプリ１２１は、端末間連携部１２４ｃに複製応答通信のために処理戻しを行う（ステップＳ５２６）。

以下、端末間連携部１２４ｃは、図１０の破線囲みに示す関数３Ｂ－２操作を実行する。この関数３Ｂ－２操作は、図１の端末間連携部１２４ｃの「

関数３Ｂ－２」操作に該当する。すなわち、端末間連携部１２４ｃは、証明書管理部１２８に他証明書（送信側証明書ＩＤ）を要求する（ステップＳ５２７）。

証明書管理部１２８は、端末間連携部１２４ｃに他証明書（送信側）を送付する（ステップＳ５２８）。

[0100] 端末間連携部１２４ｃは、他証明書の公開鍵で署名検証する（ステップＳ５２９）。

端末間連携部１２４ｃは、証明書管理部１２８に暗号鍵AのUnwrap要求を送付（ステップＳ５３０）。

証明書管理部１２８は、自証明書に紐づく秘密鍵でUnwrapする（ステップＳ５３１）。

証明書管理部１２８は、暗号鍵Ａで認証用秘密鍵を復号化する（ステップＳ５３２）。

証明書管理部１２８は、認証用秘密鍵を保管する（ステップＳ５３３）。

上記、端末間連携部１２４ｃが他証明書（送信側証明書ＩＤ）要求（ステップＳ５２７）～端末間連携部１２４ｃが認証用秘密鍵を保管（ステップＳ５３３）までの操作（図９の関数３Ｂ－２破線囲み参照）が前記図１の端末間連携部１２４ｃの「関数３Ｂ－２」操作に該当する。

[0101] 端末間連携部１２４ｃは、端末間連携アプリ１２１に処理完了通知を送付する（ステップＳ５３３）。

端末間連携アプリ１２１は、既存端末Ａ１１０の端末間連携アプリ１１１に完了通知を送信する（ステップＳ５３４）。

既存端末Ａ１１０の端末間連携アプリ１１１は、ユーザに完了通知を送信する（ステップＳ５３５）。

新規端末Ｂ１２０の端末間連携アプリ１２１は、ユーザに完了通知を送信する（ステップＳ５３６）。

以上、「証明書の交換」（図８参照）と「端末間の連携」（図９および図１０参照）について説明した。

[0102] 〈閾値超過時の処理方法〉

次に、閾値超過時の処理方法について説明する。

暗号化データを多数取得することで、暗号鍵の生成方法を推測し、認証鍵を盗難しようとする攻撃が考えられる。

本実施形態では、認証鍵の複製要求の回数が、事前に定められた閾値（例えば１時間に３回まで等）を超過した場合、その要求を拒否する。

一方で、ユーザによる誤操作等の可能性もあるため、その時点でユーザに警告画面を表示し、操作に進むかどうかを選択させる機能をＴＥＥ内に配備する。ＴＥＥの警告画面は、マルウェア等によって改ざんできないため、セキュアにユーザ意志を確認できる。その際に、事前に登録されたユーザしか持ちえないクレデンシャル（ＰＩＮ入力や生体情報の提示等）の入力をセキュアに受付、検証する機能をＴＥＥに配備することで、より確実性を高めることが好ましい。

[0103] 図１１は、閾値超過時の処理を適用した端末間の連携のシーケンスを示す図である。図９と同一処理を行うステップには同一符号を付している。閾値超過時の処理は、送信側端末で行う処理であるので、図１１は、図９のうち送信側端末（既存端末Ａ）のシーケンスを抜粋して示している。

図１１に示すように、既存端末Ａ１１０の端末間連携アプリ１１１は、既存端末側連携部１１４の端末間連携部１１４ｃに対し複製要求処理（複製要求通信）を行う（ステップＳ５１０）。

端末間連携部１１４ｃは、図１１の破線囲みに示す関数３Ａ－１操作を実行する。この関数３Ａ－１操作は、図１の端末間連携部１１４ｃの「関数３Ａ－１」操作に該当する。すなわち、端末間連携部１１４ｃは、一定時間内の要求回数確認・更新を行う（ステップＳ５１１）。

端末間連携部１１４ｃは、ユーザに対し一定時間内の要求回数が多いことの警告画面を表示する（ステップＳ６０１）。

端末間連携部１１４ｃは、ユーザによる承諾・拒否の判断（ＰＩＮ等クレデンシャルの提示）を受け取る（ステップＳ６０２）。

端末間連携部１１４ｃは、ユーザ意志およびクレデンシャルを確認する（ステップＳ６０３）。

以下、図９の端末間連携部１１４ｃの「関数３Ａ－１」操作と同様の処理を行う。

[0104] 〈名称命名機能〉

次に、名称命名機能について説明する。

他証明書を取得する際に、その端末を識別可能なわかりやすい名称を、ユーザがセキュアに命名できる機能をＴＥＥに設置する。

図１２は、名称命名機能を適用した証明書の交換のシーケンスを示す図である。図８と同一処理を行うステップには同一符号を付している。名称命名機能の処理は、受信側端末で行う処理であるので、図１２は、図８のうち受信側端末（新規端末Ｂ１２０）のシーケンスを抜粋して示している。

図１２に示す関数１－１破線囲み操作が前記図１の新規端末Ｂ１２０の証明書受信部１２４ａの「関数１－１」操作に該当する。

証明書受信部１２４ａは、予め定められた所有者一致条件を満たすかを確認（ＣＮ値が一致する等）して、送信側証明書と受信側証明書の比較を行う（ステップＳ４１１）。

[0105] 証明書受信部１２４ａは、ユーザに送信側端末の命名要求を送付する（ステップＳ７０１）。

証明書受信部１２４ａは、ユーザから、わかりやすい名称の入力を受け取る（ステップＳ７０２）。

証明書受信部１２４ａは、証明書管理部１２８に、わかりやすい名称が付加された送信側証明書の保管要求を送付する（ステップＳ７０３）。

証明書管理部１２８は、送信側証明書を他証明書として名称と紐づけて保管する（ステップＳ７０４）。

証明書管理部１２８は、証明書受信部１２４ａに完了通知を送付する（ステップＳ７０５）。

[0106] 〈意図しない端末の確認〉

連携処理時に、相手の端末をセキュアにユーザに通知する機能をＴＥＥに設置することで、意図しない端末間で連携が行われようとしていることに気づきやすくなる。

[0107] 図１３は、意図しない端末の確認処理を適用した端末間の連携のシーケンスを示す図である。図９と同一処理を行うステップには同一符号を付している。意図しない端末の確認処理は、送信側端末で行う処理であるので、図１３は、図９のうち送信側端末（既存端末Ａ）のシーケンスを抜粋して示している。

図１１に示す関数３Ａ－１操作が図１の端末間連携部１１４ｃの「関数３Ａ－１」操作に該当する。すなわち、端末間連携部１１４ｃは、証明書管理部１１８に他証明書要求（受信側証明書ＩＤ）を送付する（ステップＳ８０１）。

証明書管理部１１８は、端末間連携部１１４ｃに他証明書、名称（受信側）を送付する（ステップＳ８０２）。

端末間連携部１１４ｃは、ユーザに対し、端末の名称を表示する（ステップＳ８０３）。

端末間連携部１１４ｃは、ユーザから、意図している端末であることを確認する（ステップＳ８０４）。

[0108] 以上説明したように、本実施形態に係る端末登録システム１０００は、既存端末Ａ１１０が、ＴＥＥを含むセキュア領域に、端末の所有者を示す所有者証明書を発行する証明書発行部１１７と、同一の所有者証明書を有する端末間で連携をするとともに、暗号鍵を生成する既存端末側連携部１１４と、認証用秘密鍵を管理する認証鍵管理部１１６と、を備え、また、ＲＥＥを含む端末環境に、端末間の通信を行う端末間連携アプリ１１１を備え、新規端末Ｂ１２０は、新規端末Ｂ１２０側の端末間連携アプリ１２１から既存端末Ａ１１０に対して、暗号鍵による暗号化通信の開始要求を行い、既存端末Ａ１１０の既存端末側連携部１１４は、認証用秘密鍵を暗号鍵で暗号化した連携用データを、同一の所有者証明書を有する新規端末Ｂ１２０に送付する。

[0109] この構成により、ＴＬＳと比較して端末間の通信回数を削減することができる。例えば、一つのオペレーション（端末間での証明書の交換処理／端末間の連携処理）において、必須となる通信回数は最大でも端末間で１往復となる。これにより、ＲＥＥへのコンテキストスイッチを意識したＴＥＥ内の状態数が削減される。

[0110] なお、上記実施形態において説明した各処理のうち、自動的に行われるものとして説明した処理の全部又は一部を手動的に行うこともでき、あるいは、手動的に行われるものとして説明した処理の全部又は一部を公知の方法で自動的に行うこともできる。この他、明細書中や図面中に示した処理手順、制御手順、具体的名称、各種のデータやパラメータを含む情報については、特記する場合を除いて任意に変更することができる。

また、図示した各装置の各構成要素は機能概念的なものであり、必ずしも物理的に図示の如く構成されていることを要しない。すなわち、各装置の分散・統合の具体的形態は図示のものに限られず、その全部又は一部を、各種の負荷や使用状況などに応じて、任意の単位で機能的又は物理的に分散・統合して構成することができる。

[0111] また、上記の各構成、機能、処理部、処理手段等は、それらの一部又は全部を、例えば集積回路で設計する等によりハードウェアで実現してもよい。また、上記の各構成、機能等は、プロセッサがそれぞれの機能を実現するプログラムを解釈し、実行するためのソフトウェアで実現してもよい。各機能を実現するプログラム、テーブル、ファイル等の情報は、メモリや、ハードディスク、ＳＳＤ（Solid State Drive）等の記録装置、又は、ＩＣ（Integrated Circuit）カード、ＳＤ（Secure Digital）カード、光ディスク等の記録媒体に保持することができる。

符号の説明

[0112] １１０　既存端末Ａ（登録済み端末）

１１１，１２１　端末間連携アプリ（通信部）

１１２　認証アプリ

１１３　証明書発行アプリ

１１４　既存端末側連携部

１１４ａ　証明書受信部

１１４ｂ　証明書送信部

１１４ｃ　端末間連携部

１１５，１２５　認証部

１１６，１２６　認証鍵管理部

１１７，１２７　証明書発行部

１１８，１２８　証明書管理部

１２０　新規端末Ｂ

１２４　新規端末側連携部

１３０　認証局

１４０　サービスサイト

１０００　端末登録システム

請求の範囲

[請求項1] 秘密鍵を用いてＦＩＤＯ（Fast IDentity Online）認証する複数の端末と、前記端末が利用するサービスサイトとが通信可能に接続され、

登録済み端末を用いて、複数の前記サービスサイトに対する新規端末を登録する端末登録システムであって、

前記端末は、ＴＥＥ（Trusted Execution Environmen）を含むセキュア領域に、端末の所有者を示す所有者証明書を発行する証明書発行部と、同一の所有者証明書を有する端末間で連携をする連携部と、暗号鍵を生成する暗号鍵生成部と、認証用秘密鍵を管理する認証鍵管理部と、を備え、

ＲＥＥ（Rich Execution Environment）を含む端末環境に、端末間の通信を行う通信部を備え、

前記新規端末は、当該新規端末側の前記通信部から前記登録済み端末に対して、暗号鍵による暗号化通信の開始要求を行い、

前記登録済み端末の前記連携部は、前記認証用秘密鍵を前記暗号鍵で暗号化した連携用データを、同一の前記所有者証明書を有する前記新規端末に送付する

ことを特徴とする端末登録システム。

[請求項2] 前記連携部は、所定時間内の通信開始要求回数を判定する閾値を有し、

前記登録済み端末の前記連携部は、前記新規端末からの通信開始要求回数が前記閾値を超えた場合、前記連携用データの送付を行わない

ことを特徴とする請求項１に記載の端末登録システム。

[請求項3] 前記登録済み端末の前記連携部は、前記新規端末側で前記暗号鍵が利用可能になることを確認することなく、前記連携用データの送付を行う

ことを特徴とする請求項１に記載の端末登録システム。

[請求項4] 前記連携部は、前記新規端末からの通信開始要求回数が前記閾値を超えた場合、ユーザに知らせる提示手段と、

ユーザによる可否の判断を受付ける受付手段と、をさらに備える

ことを特徴とする請求項２に記載の端末登録システム。

[請求項5] 前記連携部は、連携処理時に、連携処理中の前記新規端末をユーザに通知する

ことを特徴とする請求項１に記載の端末登録システム。

[請求項6] 前記登録済み端末の前記証明書発行部は、ユーザが命名する前記新規端末の名称を、前記所有者証明書と紐付けて保管する

ことを特徴とする請求項１に記載の端末登録システム。

[請求項7] 秘密鍵を用いてＦＩＤＯ（Fast IDentity Online）認証する複数の端末と、前記端末が利用するサービスサイトとが通信可能に接続され、

登録済み端末を用いて、複数の前記サービスサイトに対する新規端末を登録する端末登録システムの端末登録方法であって、

前記端末は、ＴＥＥ（Trusted Execution Environmen）を含むセキュア領域に、端末の所有者を示す所有者証明書を発行する証明書発行部と、同一の所有者証明書を有する端末間で連携をする連携部と、暗号鍵を生成する暗号鍵生成部と、認証用秘密鍵を管理する認証鍵管理部と、を有し、

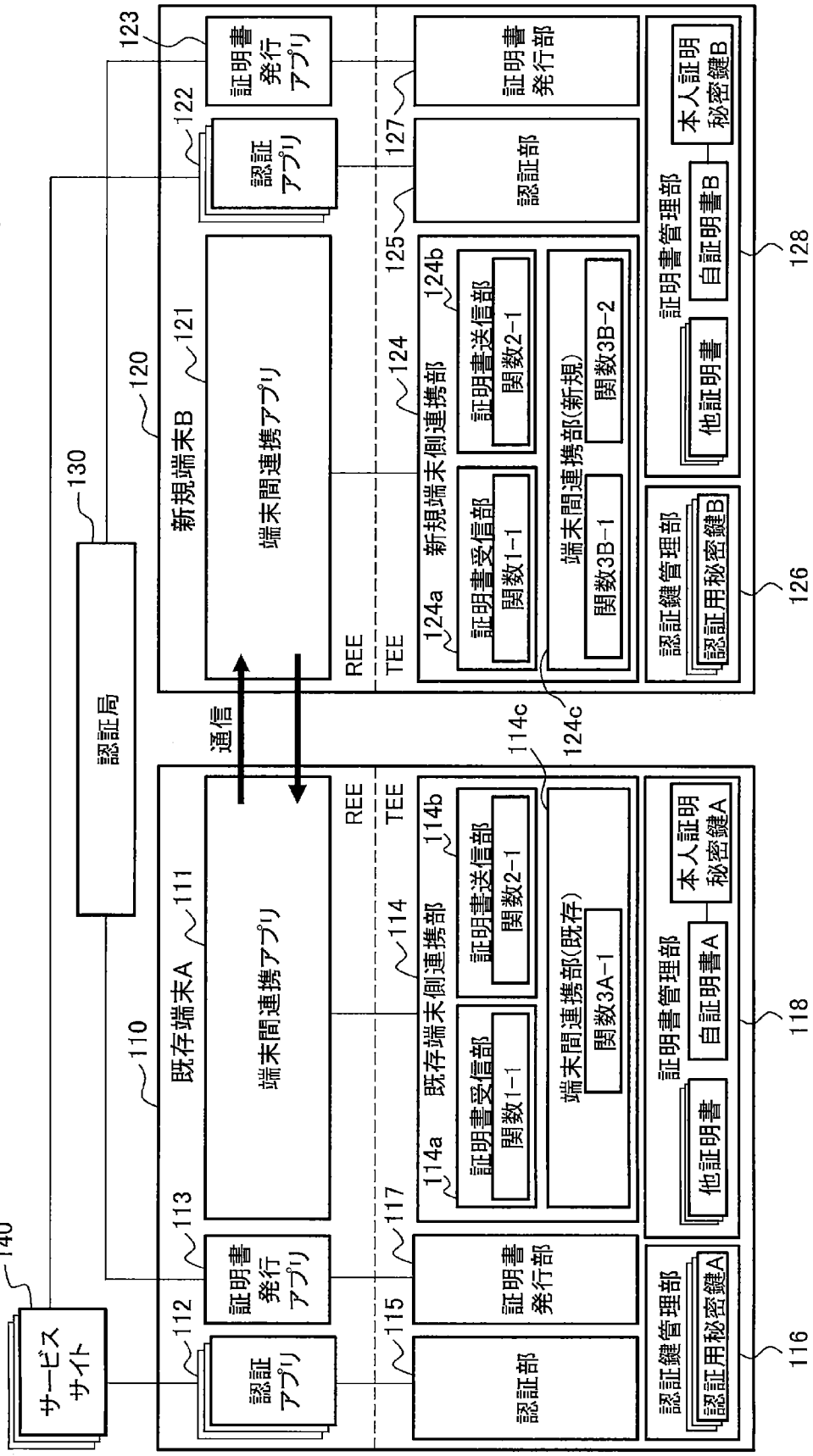
ＲＥＥを含む端末環境に、端末間の通信を行う通信部を有し、

前記新規端末は、当該新規端末側の前記通信部から前記登録済み端末に対して、暗号鍵による暗号化通信の開始要求を行うステップを実行し、

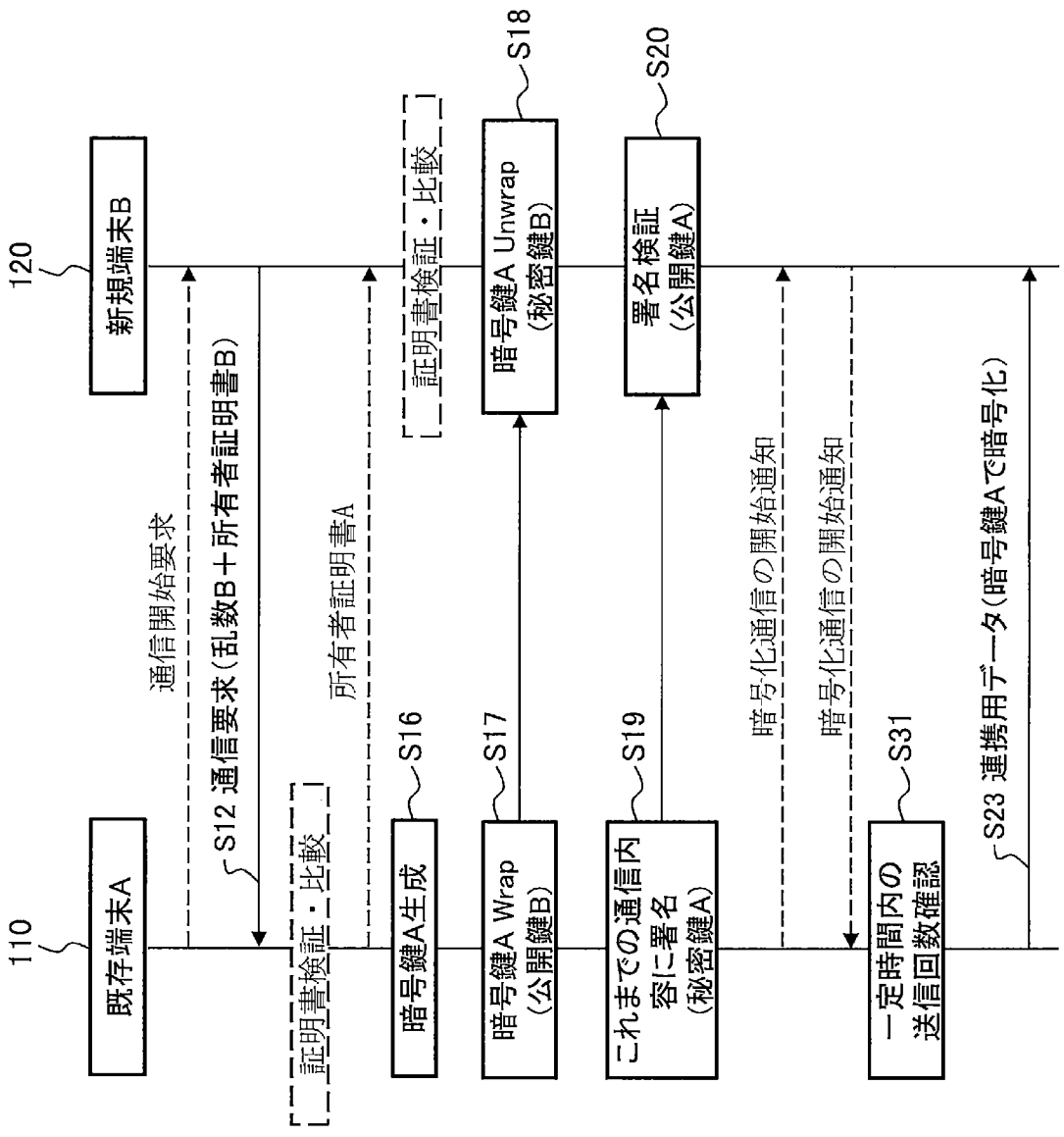
前記登録済み端末の前記連携部は、前記認証用秘密鍵を前記暗号鍵で暗号化した連携用データを、同一の前記所有者証明書を有する前記新規端末に送付するステップを実行する

端末登録方法。

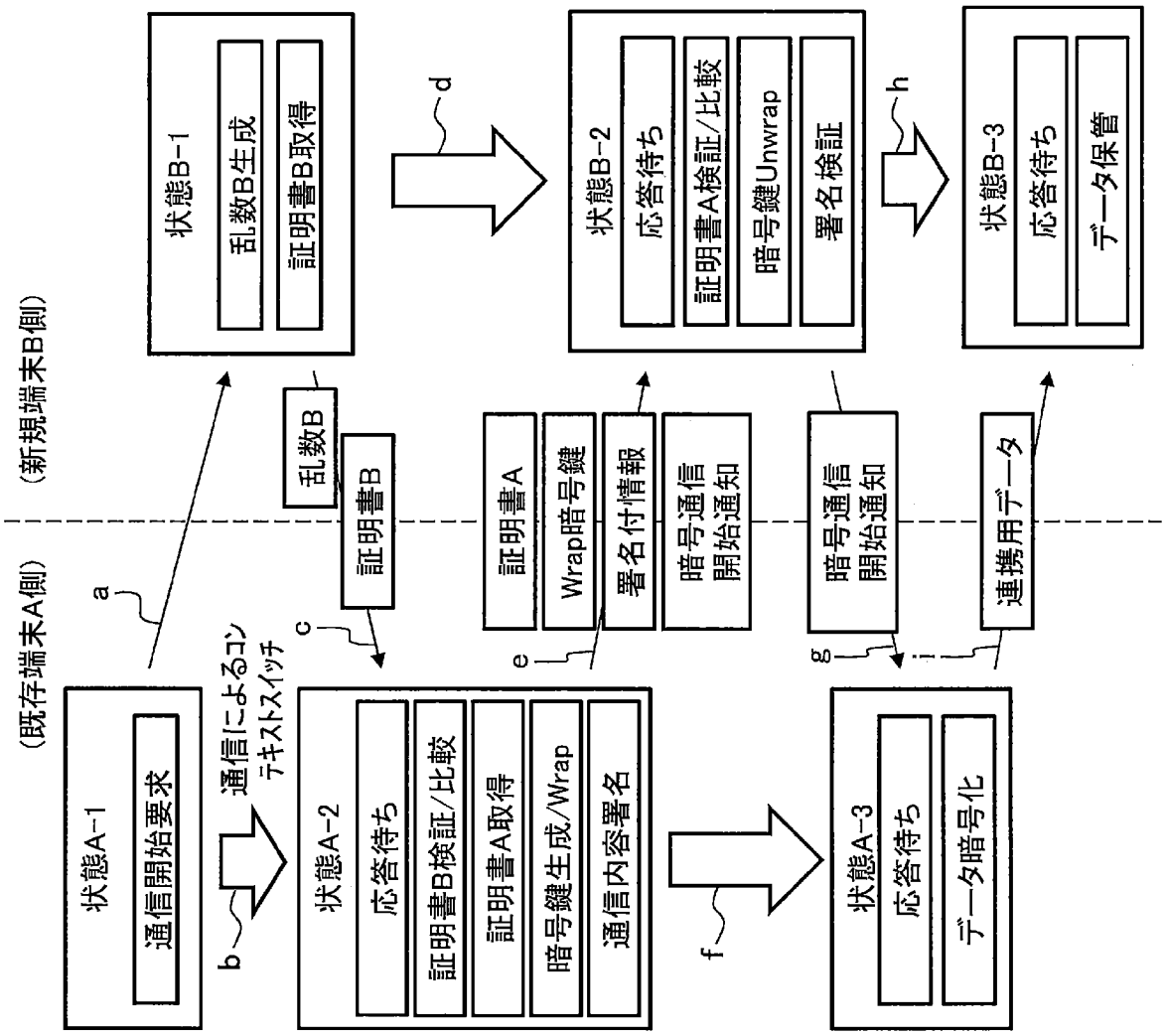
[図1]


1000
サービスサイト
140
認証局
130
110
既存端末A
111
端末間連携アプリ
112
認証アプリ
113
証明書発行アプリ
115
認証部
117
証明書発行部
114
既存端末側連携部
114a
証明書受信部
関数1-1
114b
証明書送信部
関数2-1
端末間連携部(既存)
関数3A-1
114c
認証鍵管理部
認証用秘密鍵A
116
証明書管理部
他証明書
自証明書A
本人証明秘密鍵A
118
通信
120
新規端末B
121
端末間連携アプリ
122
認証アプリ
123
証明書発行アプリ
125
127
認証部
証明書発行部
124
新規端末側連携部
124a
証明書受信部
関数1-1
124b
証明書送信部
関数2-1
端末間連携部(新規)
関数3B-1
関数3B-2
124c
認証鍵管理部
認証用秘密鍵B
126
証明書管理部
他証明書
自証明書B
本人証明秘密鍵B
128
REE
TEE

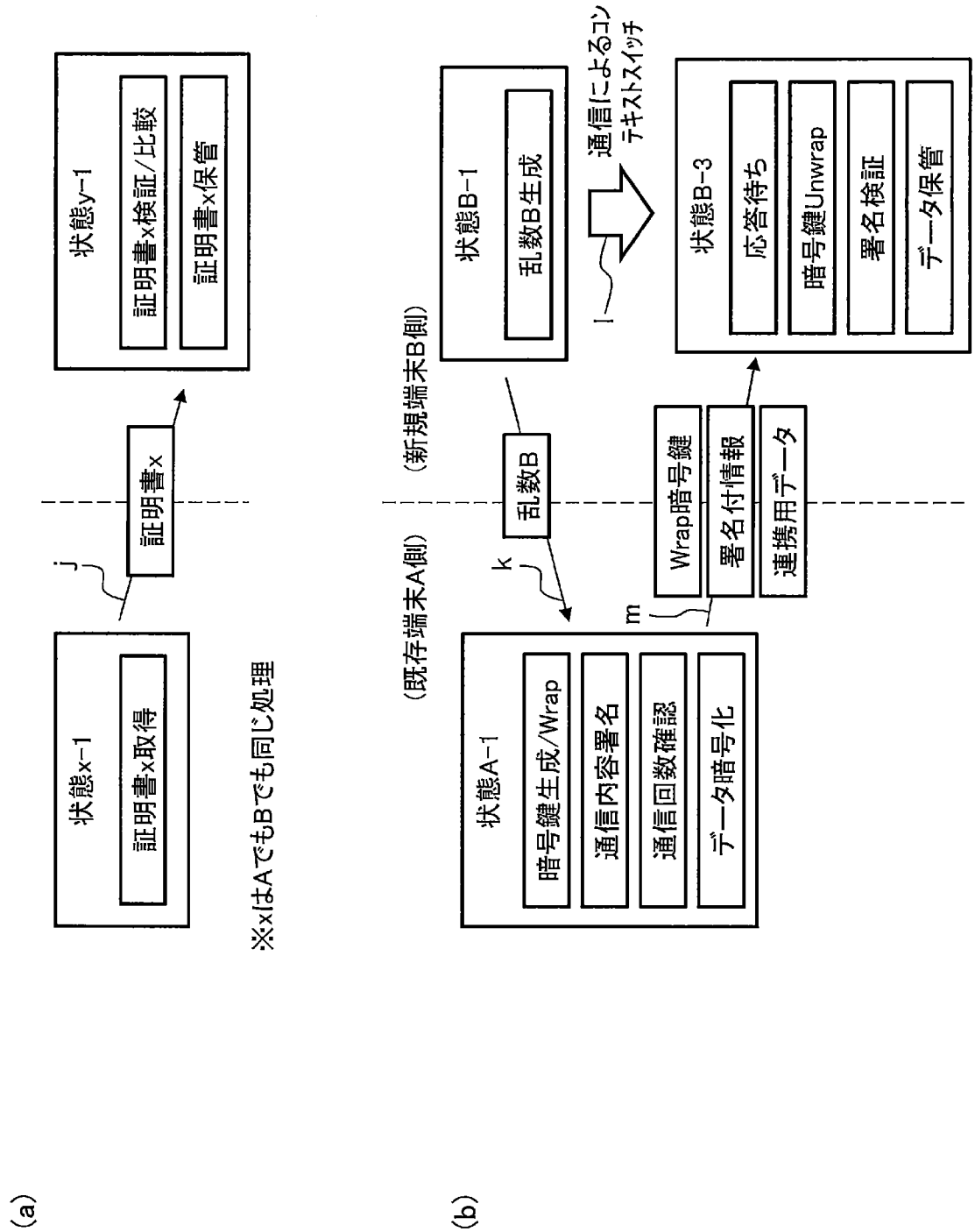
[図2]


110
既存端末A
120
新規端末B
通信開始要求
S12 通信要求(乱数B＋所有者証明書B)
証明書検証・比較
所有者証明書A
証明書検証・比較
S16
暗号鍵A生成
S17
暗号鍵A Wrap
(公開鍵B)
S18
暗号鍵A Unwrap
(秘密鍵B)
S19
これまでの通信内
容に署名
(秘密鍵A)
S20
署名検証
(公開鍵A)
暗号化通信の開始通知
暗号化通信の開始通知
S31
一定時間内の
送信回数確認
S23 連携用データ(暗号鍵Aで暗号化)

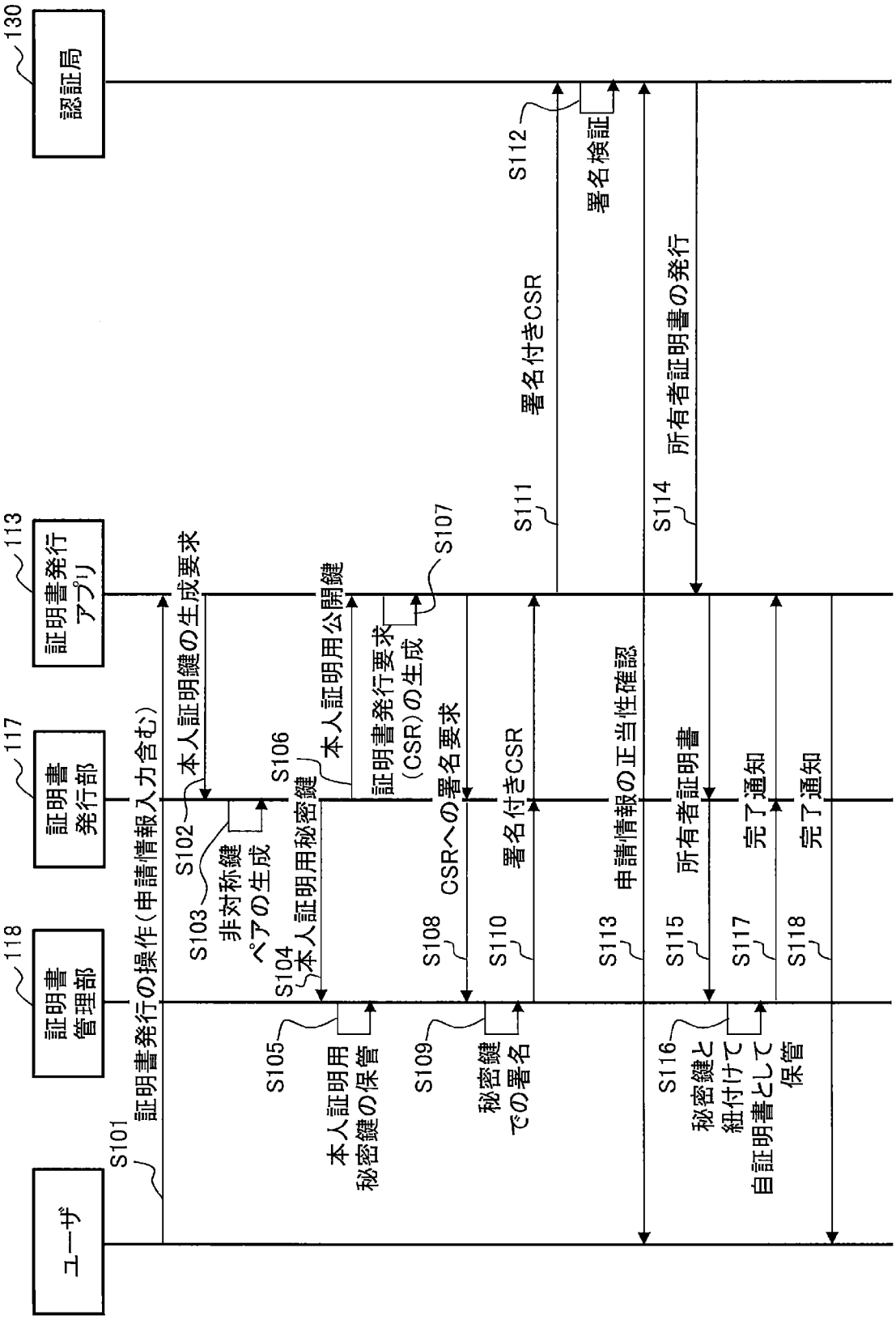
[図3]


(既存端末A側)
(新規端末B側)
状態A-1
通信開始要求
a
通信によるコンテキストスイッチ
b
状態A-2
応答待ち
証明書B検証/比較
証明書A取得
暗号鍵生成/Wrap
通信内容署名
c
乱数B
証明書B
状態B-1
乱数B生成
証明書B取得
d
証明書A
Wrap暗号鍵
署名付情報
暗号通信開始通知
e
状態B-2
応答待ち
証明書A検証/比較
暗号鍵Unwrap
署名検証
f
暗号通信開始通知
g
状態A-3
応答待ち
データ暗号化
連携用データ
i
h
状態B-3
応答待ち
データ保管

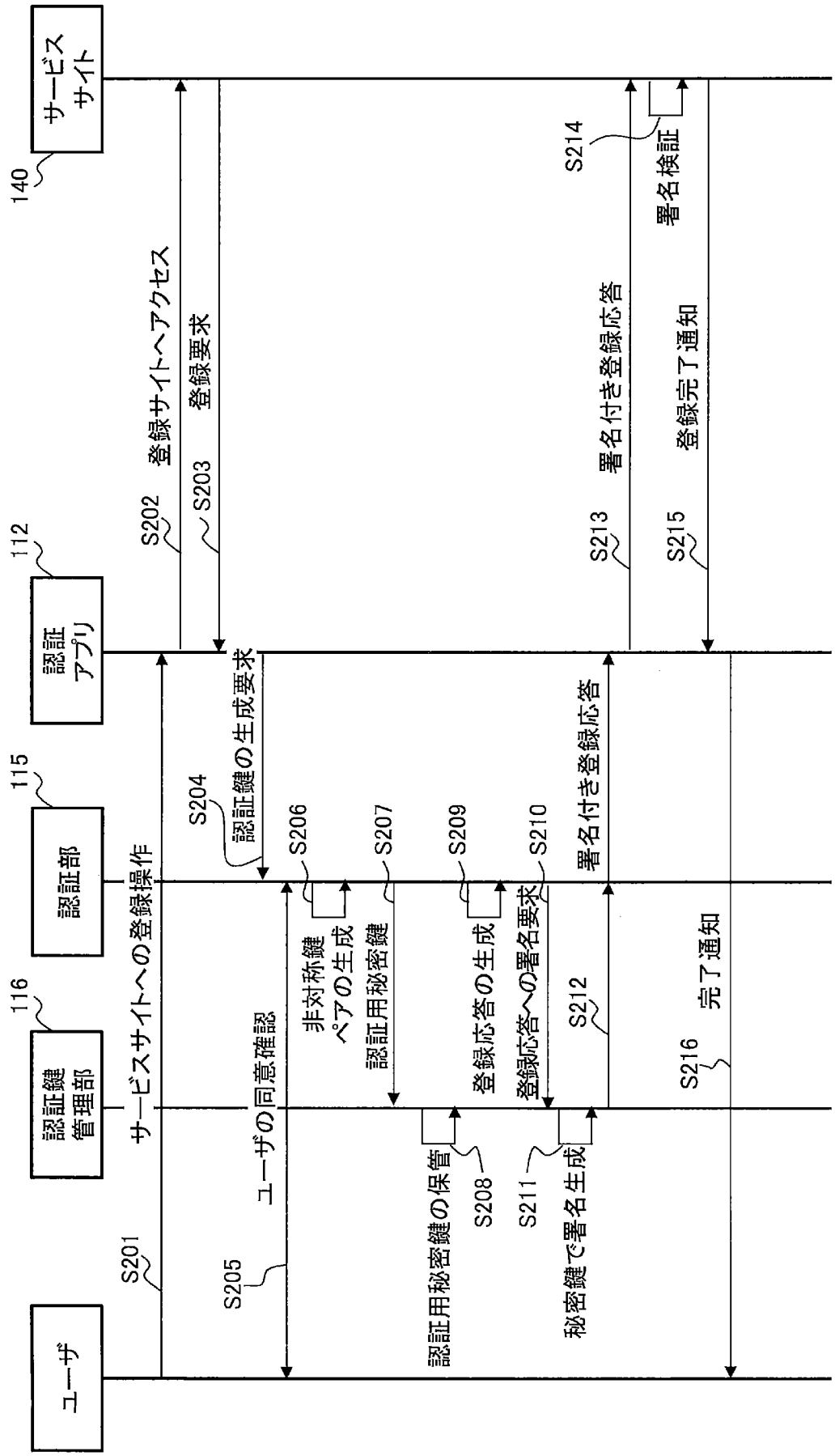
[図4]


(a)
状態x-1
証明書x取得
j
証明書x
状態y-1
証明書x検証/比較
証明書x保管
※xはAでもBでも同じ処理
(b)
(既存端末A側)
(新規端末B側)
状態A-1
暗号鍵生成/Wrap
通信内容署名
通信回数確認
データ暗号化
k
乱数B
状態B-1
乱数B生成
l
通信によるコンテキストスイッチ
m
Wrap暗号鍵
署名付情報
連携用データ
状態B-3
応答待ち
暗号鍵Unwrap
署名検証
データ保管

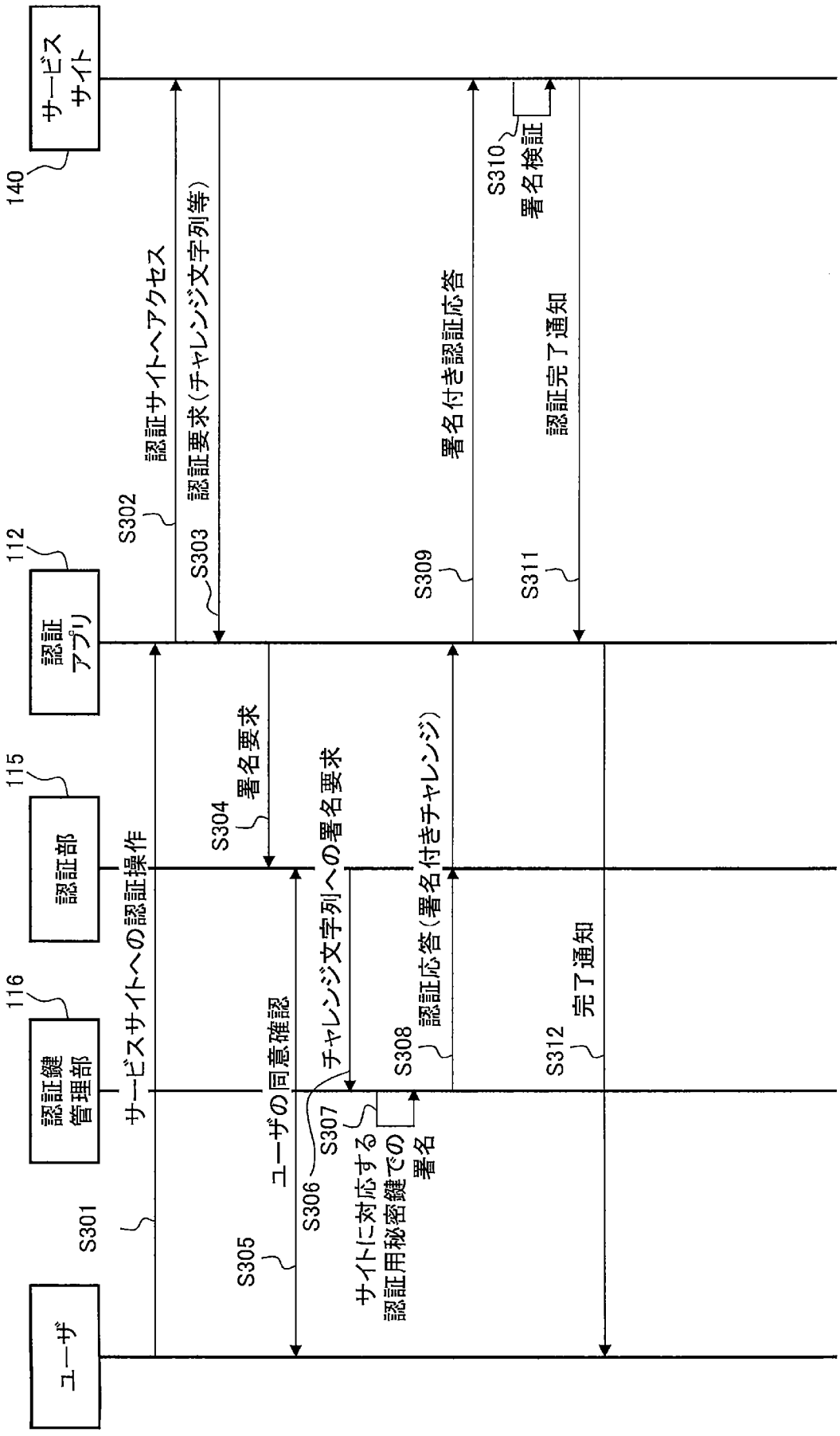
[図5]


ユーザ
証明書管理部
118
証明書発行部
117
証明書発行アプリ
113
認証局
130
S101
証明書発行の操作(申請情報入力含む)
S102
本人証明鍵の生成要求
S103
非対称鍵ペアの生成
S104
本人証明用秘密鍵
S105
本人証明用秘密鍵の保管
S106
本人証明用公開鍵
S107
証明書発行要求(CSR)の生成
S108
CSRへの署名要求
S109
秘密鍵での署名
S110
署名付きCSR
S111
署名付きCSR
S112
署名検証
S113
申請情報の正当性確認
S114
所有者証明書の発行
S115
所有者証明書
S116
秘密鍵と紐付けて自証明書として保管
S117
完了通知
S118
完了通知

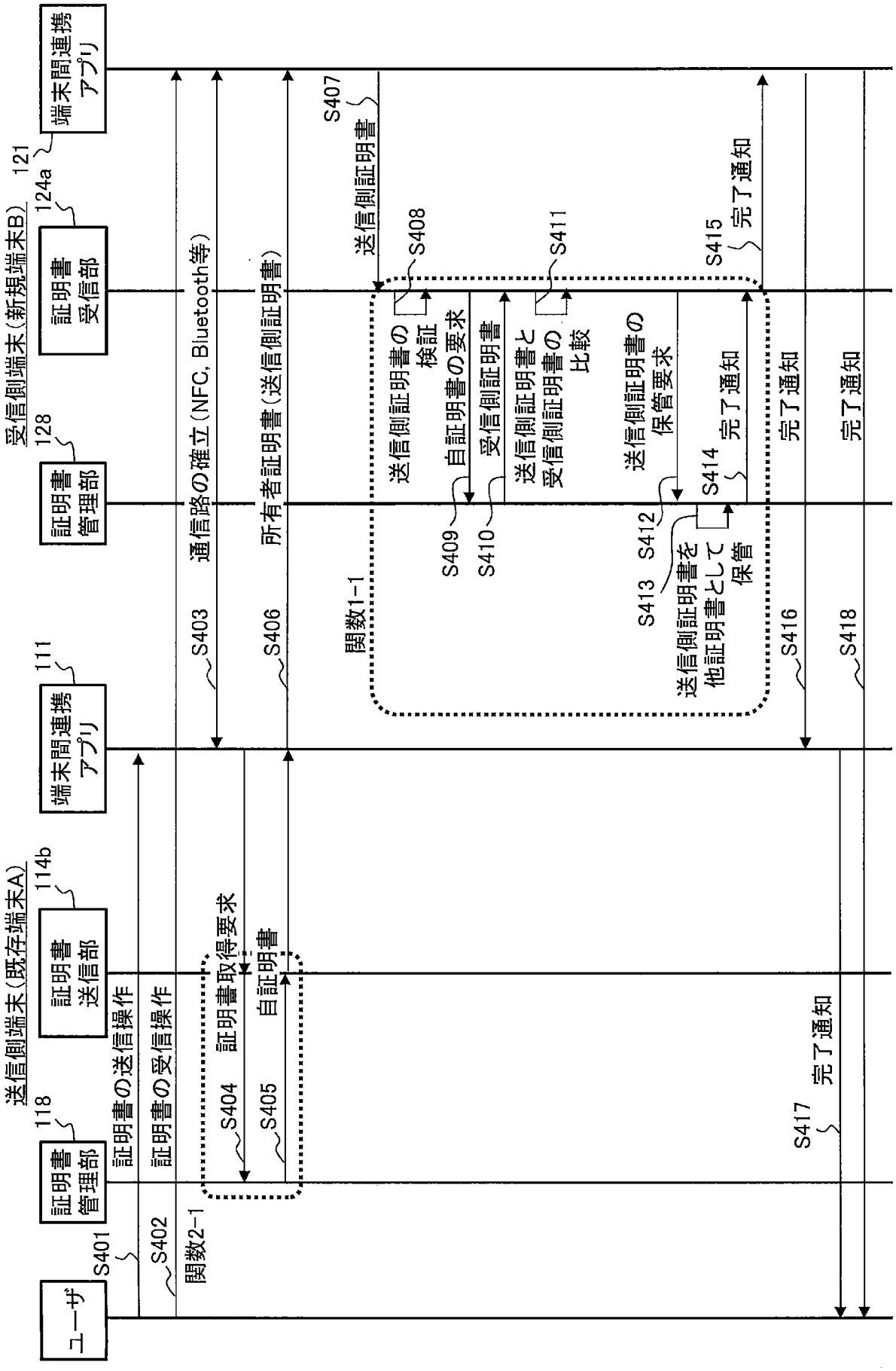
[図6]


ユーザ
認証鍵管理部
116
認証部
115
認証アプリ
112
サービスサイト
140
S201
サービスサイトへの登録操作
S202
登録サイトへアクセス
S203
登録要求
S204
認証鍵の生成要求
S205
ユーザの同意確認
S206
非対称鍵ペアの生成
S207
認証用秘密鍵
S208
認証用秘密鍵の保管
S209
登録応答の生成
S210
登録応答への署名要求
S211
秘密鍵で署名生成
S212
署名付き登録応答
S213
署名付き登録応答
S214
署名検証
S215
登録完了通知
S216
完了通知

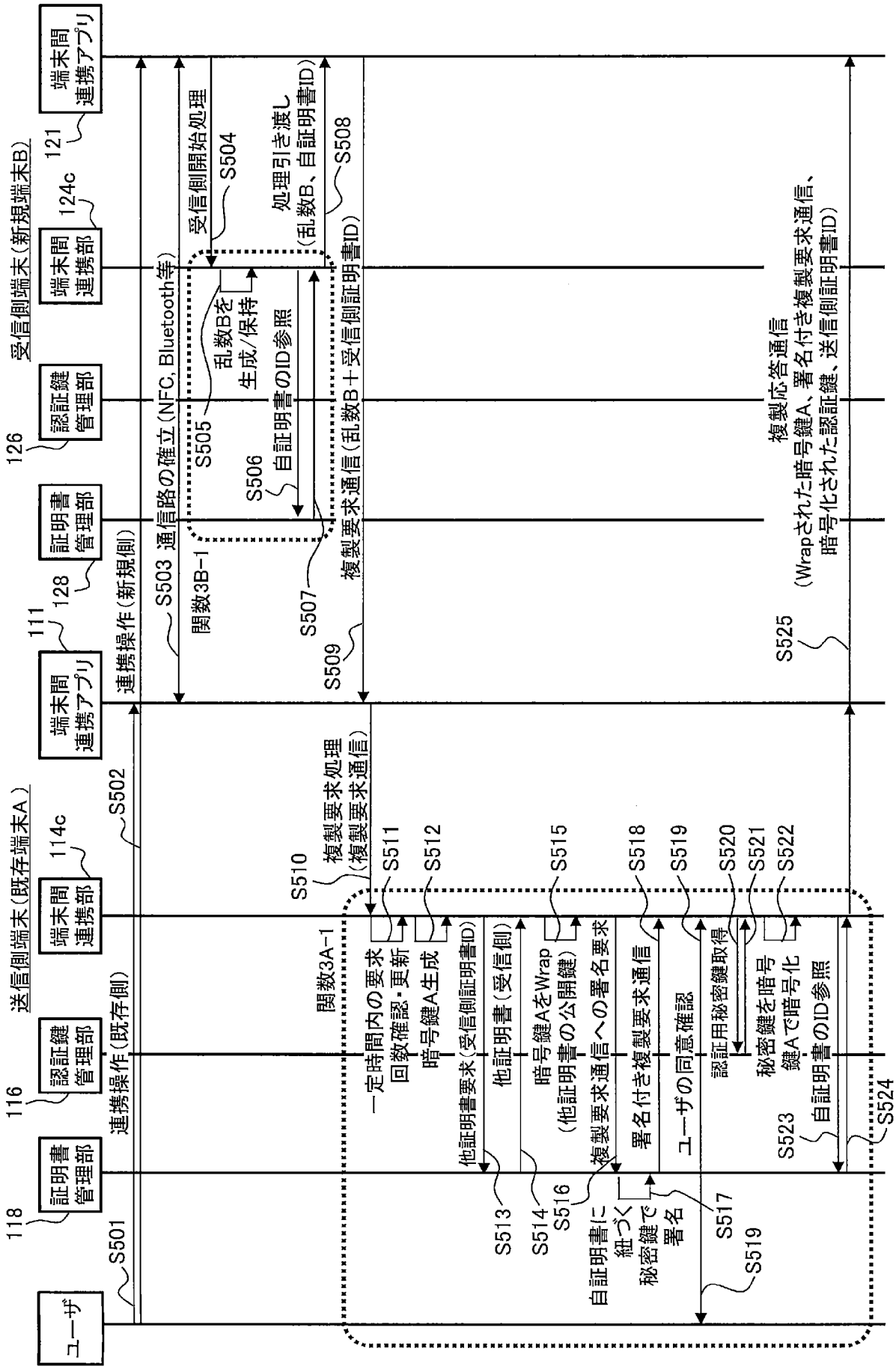
[図7]


ユーザ
認証鍵管理部
116
認証部
115
認証アプリ
112
サービスサイト
140
S301
サービスサイトへの認証操作
S302
認証サイトへアクセス
S303
認証要求（チャレンジ文字列等）
S304
署名要求
S305
ユーザの同意確認
S306
チャレンジ文字列への署名要求
S307
サイトに対応する認証用秘密鍵での署名
S308
認証応答（署名付きチャレンジ）
S309
署名付き認証応答
S310
署名検証
S311
認証完了通知
S312
完了通知

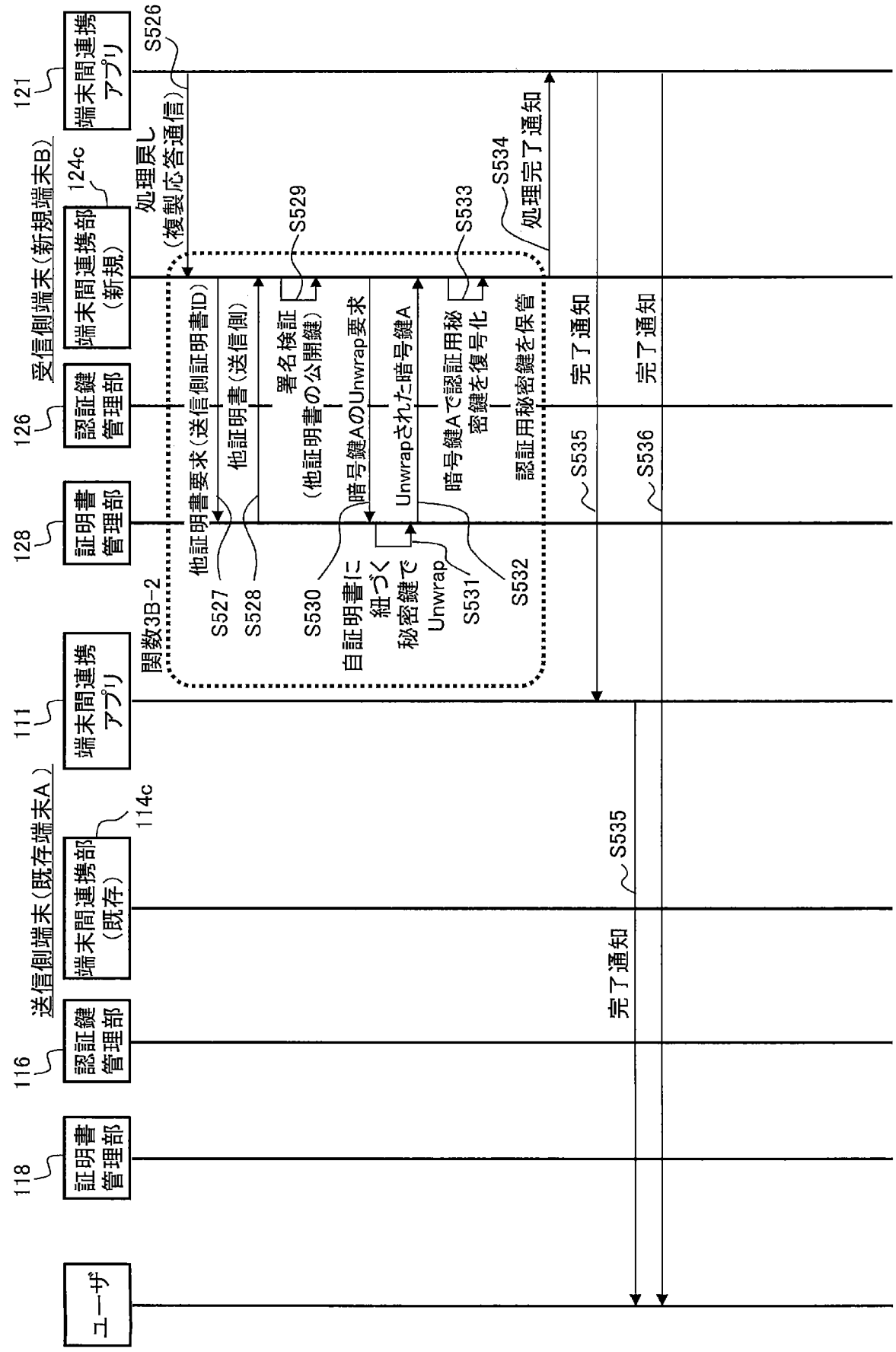
[図8]


送信側端末(既存端末A)
受信側端末(新規端末B)
ユーザ
証明書管理部
118
証明書送信部
114b
端末間連携アプリ
111
証明書管理部
128
証明書受信部
124a
端末間連携アプリ
121
S401
S402
証明書の送信操作
証明書の受信操作
関数2-1
S403
通信路の確立(NFC, Bluetooth等)
S404
証明書取得要求
S405
自証明書
S406
所有者証明書(送信側証明書)
S407
送信側証明書
関数1-1
S408
送信側証明書の検証
S409
自証明書の要求
S410
受信側証明書
S411
送信側証明書と受信側証明書の比較
S412
送信側証明書の保管要求
S413
送信側証明書を他証明書として保管
S414
完了通知
S415
完了通知
S416
完了通知
S417
完了通知
S418
完了通知

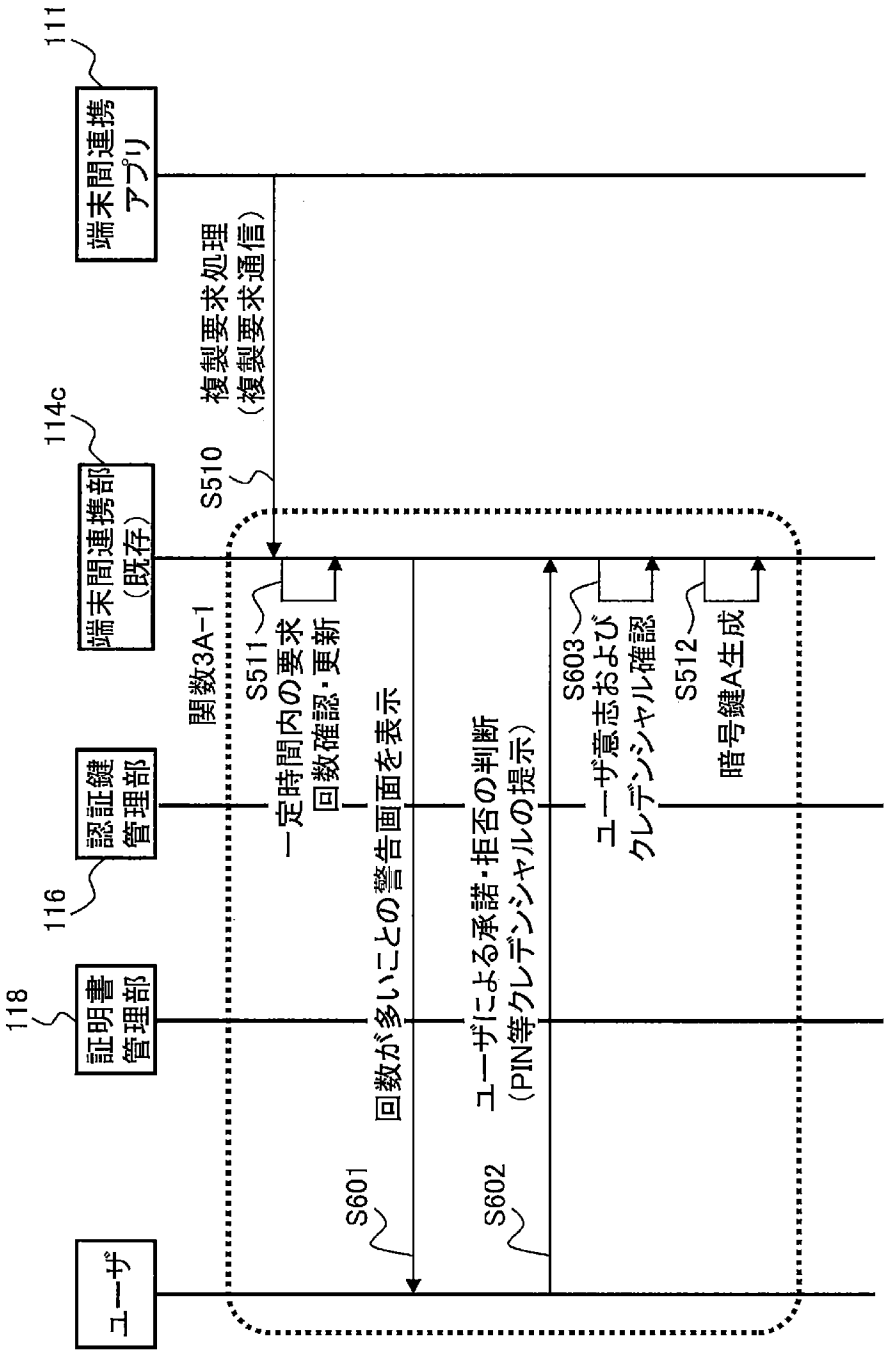
[図9]


ユーザ
118
送信側端末(既存端末A)
証明書管理部
116
認証鍵管理部
端末間連携部
114c
端末間連携アプリ
111
連携操作(既存側)
連携操作(新規側)
S501
S502
S503 通信路の確立(NFC, Bluetooth等)
関数3A-1
関数3B-1
S504 受信側開始処理
S505 乱数Bを生成/保持
S506 自証明書のID参照
S507 処理引き渡し(乱数B、自証明書ID)
S508 複製要求通信(乱数B+受信側証明書ID)
S509
S510 複製要求処理(複製要求通信)
S511 一定時間内の要求回数確認・更新
S512 暗号鍵A生成
S513 他証明書要求(受信側証明書ID)
S514 他証明書(受信側)
S515 暗号鍵AをWrap(他証明書の公開鍵)
S516 複製要求通信への署名要求
S517 自証明書に紐づく秘密鍵で署名
S518 署名付き複製要求通信
S519 ユーザの同意確認
S519
S520 認証用秘密鍵取得
S521 秘密鍵を暗号鍵Aで暗号化
S522
S523 自証明書のID参照
S524
S525 複製応答通信(Wrapされた暗号鍵A、署名付き複製要求通信、暗号化された認証鍵、送信側証明書ID)
受信側端末(新規端末B)
121
端末間連携アプリ
124c
端末間連携部
126
認証鍵管理部
128
証明書管理部

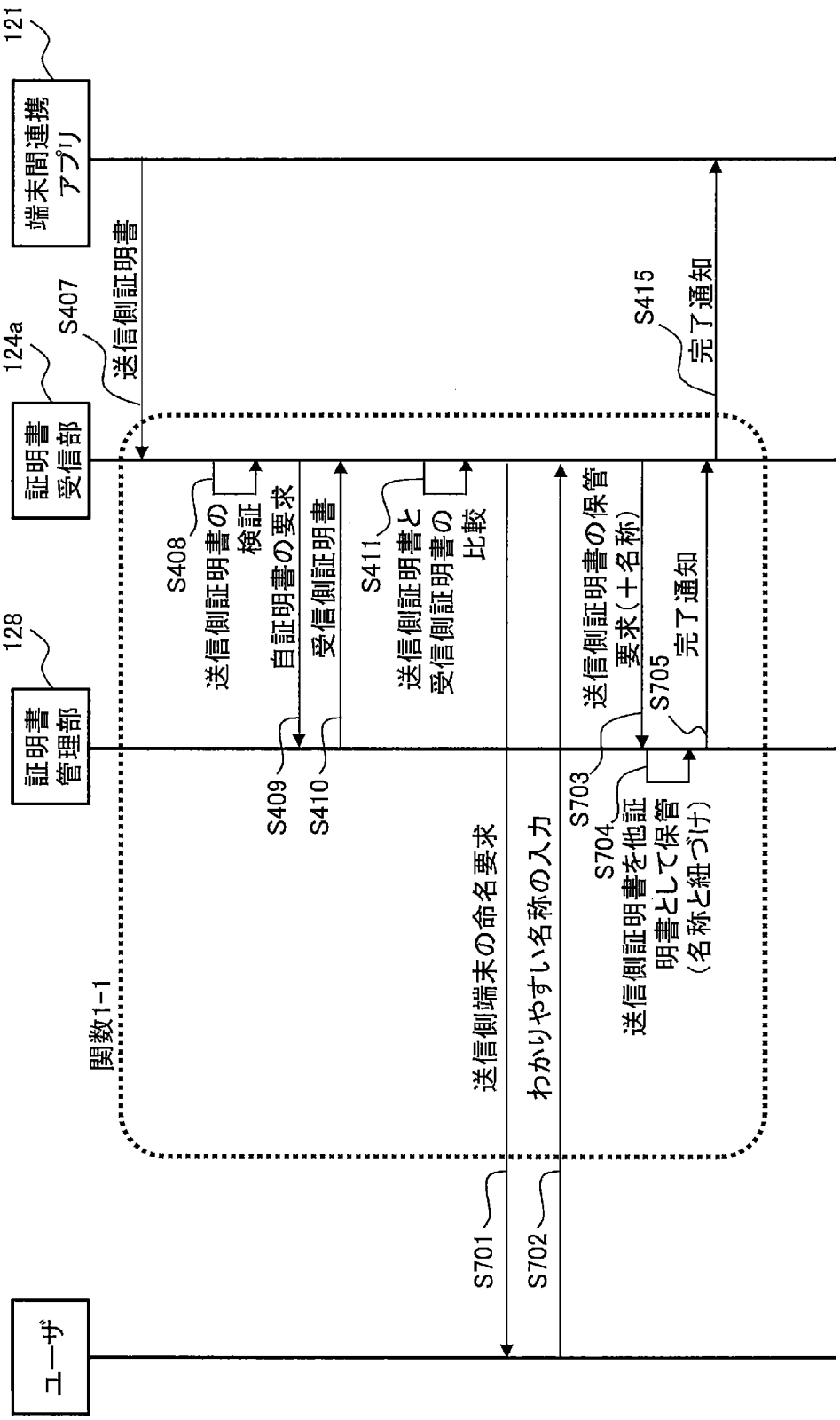
[図10]


ユーザ
証明書管理部
118
認証鍵管理部
116
送信側端末(既存端末A)
端末間連携部(既存)
114c
端末間連携アプリ
111
証明書管理部
128
認証鍵管理部
126
受信側端末(新規端末B)
端末間連携部(新規)
124c
端末間連携アプリ
121
関数3B-2
他証明書要求(送信側証明書ID)
S527
他証明書(送信側)
S528
署名検証(他証明書の公開鍵)
S529
S530
自証明書に紐づく秘密鍵でUnwrap
暗号鍵AのUnwrap要求
Unwrapされた暗号鍵A
S531
暗号鍵Aで認証用秘密鍵を復号化
S532
認証用秘密鍵を保管
S533
処理完了通知
S534
処理戻し(複製応答通信)
S526
完了通知
S535
完了通知
S536
完了通知
S535

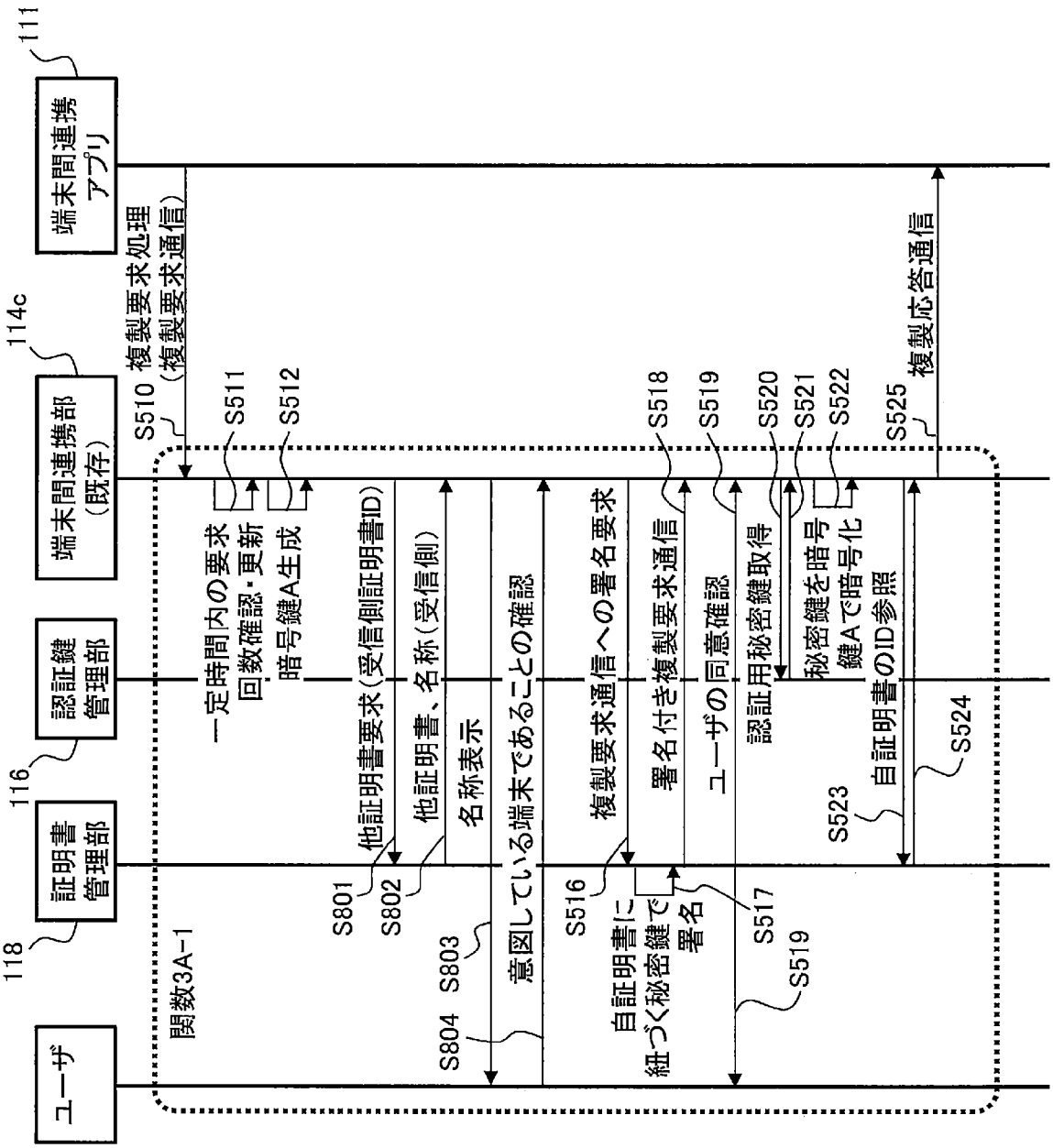
[図11]


111
端末間連携アプリ
114c
端末間連携部（既存）
116
認証鍵管理部
118
証明書管理部
ユーザ
S510
複製要求処理（複製要求通信）
関数3A-1
S511
一定時間内の要求回数確認・更新
回数が多いことの警告画面を表示
S601
ユーザによる承諾・拒否の判断（PIN等クレデンシャルの提示）
S602
S603
ユーザ意志およびクレデンシャル確認
S512
暗号鍵A生成

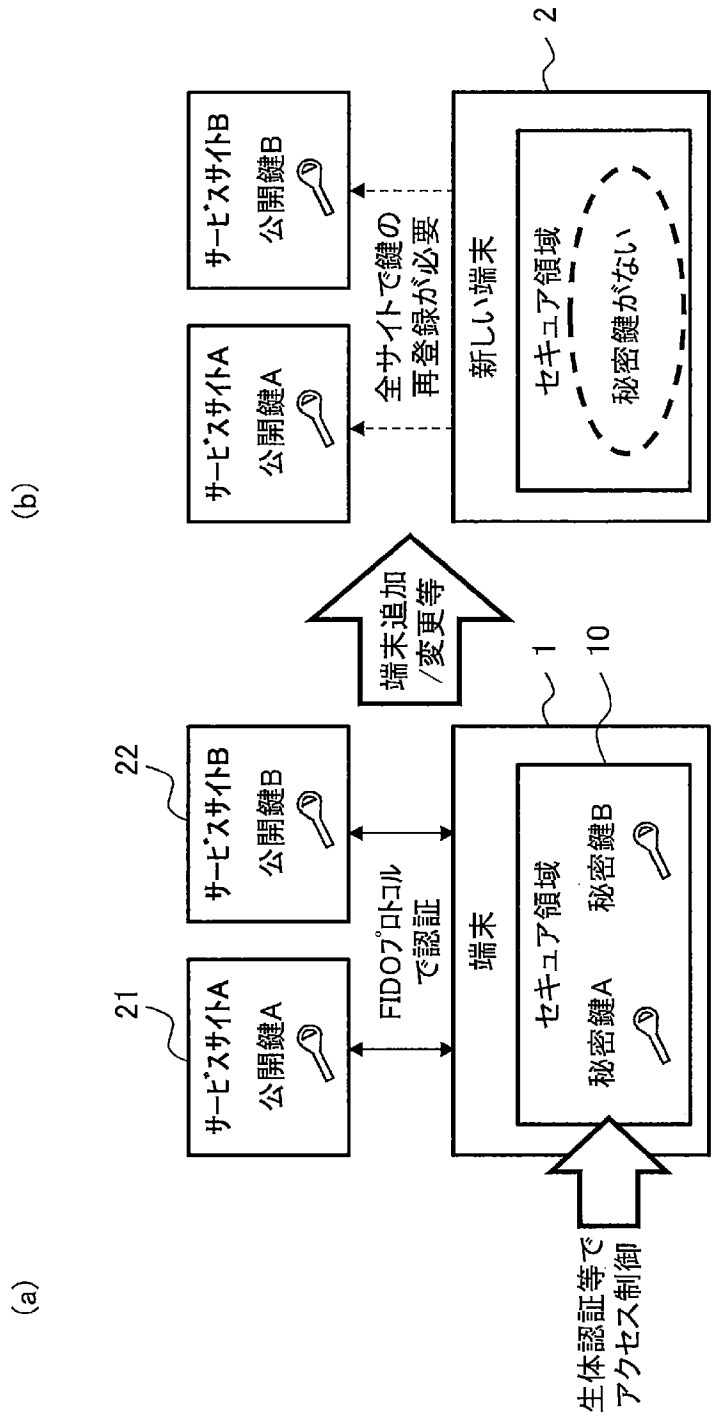
[図12]


ユーザ
証明書管理部
128
証明書受信部
124a
端末間連携アプリ
121
関数1-1
送信側端末の命名要求
S701
わかりやすい名称の入力
S702
送信側証明書の保管要求（＋名称）
S703
送信側証明書を他証明書として保管（名称と紐づけ）
S704
完了通知
S705
送信側証明書と受信側証明書の比較
S411
受信側証明書
S410
自証明書の要求
S409
送信側証明書の検証
S408
送信側証明書
S407
完了通知
S415

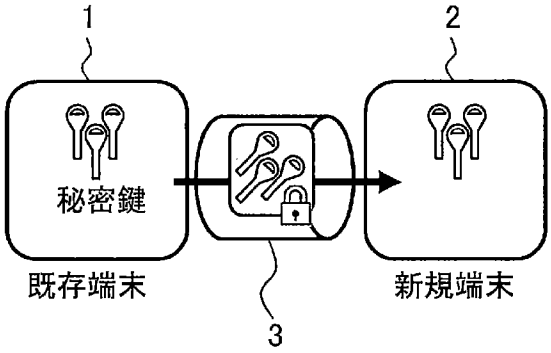
[図13]


ユーザ
118
証明書管理部
116
認証鍵管理部
端末間連携部（既存）
114c
端末間連携アプリ
111
関数3A-1
S510 複製要求処理（複製要求通信）
S511 一定時間内の要求回数確認・更新
S512 暗号鍵A生成
S801 他証明書要求（受信側証明書ID）
S802 他証明書、名称（受信側）
S803 名称表示
S804 意図している端末であることの確認
S516 複製要求通信への署名要求
自証明書に紐づく秘密鍵で署名
S517 署名付き複製要求通信
S518
S519 ユーザの同意確認
S519
S520 認証用秘密鍵取得
S521 秘密鍵を暗号鍵Aで暗号化
S522
S523 自証明書のID参照
S524
S525 複製応答通信

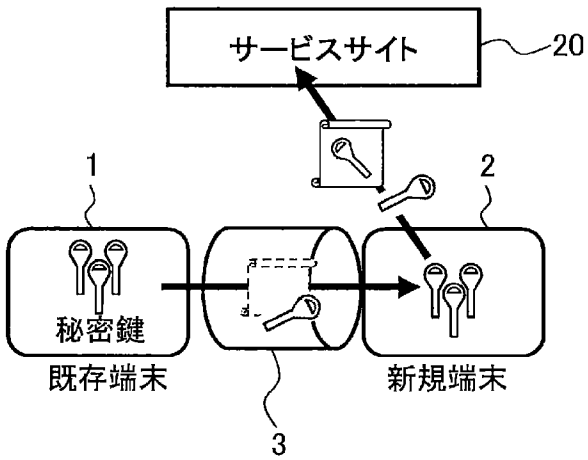
[図14]


(a)
生体認証等で
アクセス制御
端末
セキュア領域
秘密鍵A
秘密鍵B
10
1
FIDOプロトコル
で認証
サービスサイトA
公開鍵A
21
サービスサイトB
公開鍵B
22
端末追加
/変更等
(b)
新しい端末
セキュア領域
秘密鍵がない
2
全サイトで鍵の
再登録が必要
サービスサイトA
公開鍵A
サービスサイトB
公開鍵B

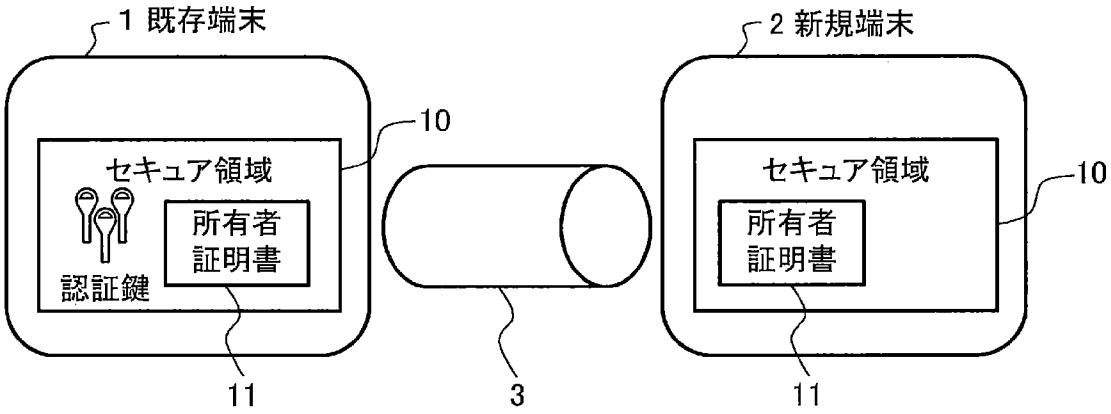
[図15]



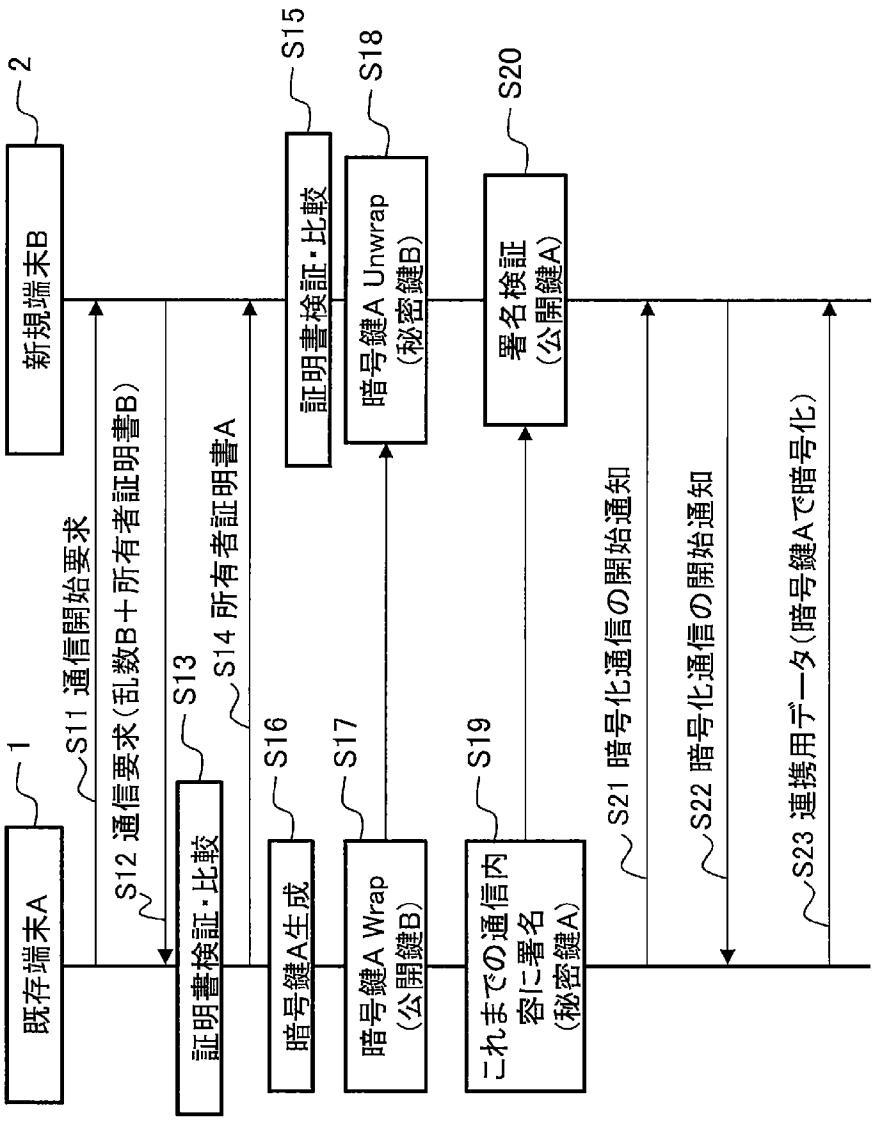
[図16]



[図17]



[図18]


1
既存端末A
2
新規端末B
S11 通信開始要求
S12 通信要求(乱数B＋所有者証明書B)
S13
証明書検証・比較
S14 所有者証明書A
S15
証明書検証・比較
S16
暗号鍵A生成
S17
暗号鍵A Wrap
(公開鍵B)
S18
暗号鍵A Unwrap
(秘密鍵B)
S19
これまでの通信内
容に署名
(秘密鍵A)
S20
署名検証
(公開鍵A)
S21 暗号化通信の開始通知
S22 暗号化通信の開始通知
S23 連携用データ(暗号鍵Aで暗号化)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2019/030237

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl. H04L9/08(2006.01)i, G06F21/33(2013.01)i, G06F21/60(2013.01)i, G09C1/00(2006.01)i, H04L9/32(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)
Int.Cl. H04L9/08, G06F21/33, G06F21/60, G09C1/00, H04L9/32

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Published examined utility model applications of Japan	1922-1996
Published unexamined utility model applications of Japan	1971-2019
Registered utility model specifications of Japan	1996-2019
Published registered utility model applications of Japan	1994-2019

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	西村豪生，ほか3名，同一所有者に属する端末間のユーザ認証用秘密鍵のセキュアな共有に関する一検討，電子情報通信学会技術研究報告，23 February 2017, vol. 116, no. 485, pp. 449-454, ISSN 0913-5685, in particular, p. 450, right column, line 30 to p. 452, left column, line 32, fig. 4, (NISHIMURA, Hideo et al., "A Study on the Secure Sharing of User Authentication Private Keys among Devices Belonging to the Same Owner", IEICE technical report)	1-7

☒ 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 03 October 2019 (03.10.2019)	Date of mailing of the international search report 15 October 2019 (15.10.2019)
Name and mailing address of the ISA/ Japan Patent Office 3-4-3, Kasumigaseki, Chiyoda-ku, Tokyo 100-8915, Japan	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2019/030237

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	飯田正樹，ほか４名， IoTのためのPKIによるシステム構築方法の提案，CSS2016コンピュータセキュリティシンポジウム2016論文集，04 October 2016, vol. 2016, no. 2, pp. 602-608, p. 604, right column, line 11 to p. 605, right column, line 25, (IIDA, Masaki et al., "The Proposal of a PKI-based System Design for IoT", CSS2016, Proceedings of Computer Security Symposium 2016)	1-7
A	JP 2018-516026 A (RIVETZ CORP.) 14 June 2018 & US 2016/0275461 A1 & CA 2980002 A1 & CN 107533501 A & KR 10-2017-0129866 A	1-7
A	WO 2017/157859 A1 (DP SECURITY CONSULTING SAS) 21 September 2017 & FR 3049083 A	1-7

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１９／０３０２３７

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　H04L9/08(2006.01)i, G06F21/33(2013.01)i, G06F21/60(2013.01)i, G09C1/00(2006.01)i, H04L9/32(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.　H04L9/08, G06F21/33, G06F21/60, G09C1/00, H04L9/32

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	１９７１－２０１９年
日本国実用新案登録公報	１９９６－２０１９年
日本国登録実用新案公報	１９９４－２０１９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	関連する請求項の番号
Y	西村 豪生，ほか3名，同一所有者に属する端末間のユーザ認証用秘密鍵のセキュアな共有に関する一検討，電子情報通信学会技術研究報告，2017.02.23，Vol.116，No.485，p.449-454，ISSN 0913-5685，特にp.450 右欄第30行-p.452 左欄第32行，図4	1-7
Y	飯田 正樹，ほか4名，ＩｏＴのためのＰＫＩによるシステム構築方法の提案，CSS2016コンピュータセキュリティシンポジウム2016論文集，2016.10.04，Vol.2016，No.2，p.602-608，p.604 右欄第11行-p.605右欄第25行	1-7

☑　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
０３．１０．２０１９	１５．１０．２０１９

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　１２０６
吉田　歩
電話番号　０３－３５８１－１１０１　内線　３５４６

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	関連する請求項の番号
A	JP 2018-516026 A (リヴェッツ・コーポレーション) 2018.06.14, & US 2016/0275461 A1 & CA 2980002 A1 & CN 107533501 A & KR 10-2017-0129866 A	1-7
A	WO 2017/157859 A1 (DP SECURITY CONSULTING SAS) 2017.09.21, & FR 3049083 A	1-7