(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
2013 年 8 月 8 日(08.08.2013)

WIPO | PCT

(10) 国際公開番号
WO 2013/114627 A1

(51) 国際特許分類:
H04L 9/08 (2006.01) *H04N 7/167* (2011.01)

(21) 国際出願番号: PCT/JP2012/052560

(22) 国際出願日: 2012 年 2 月 3 日(03.02.2012)

(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): 富士通株式会社(FUJITSU LIMITED) [JP/JP]; 〒2118588 神奈川県川崎市中原区上小田中４丁目１番１号 Kanagawa (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 丸山秀史(MARUYAMA, Hidefumi) [JP/JP]; 〒2118588 神奈川県川崎市中原区上小田中４丁目１番１号 富士通株式会社内 Kanagawa (JP).

(74) 代理人: 大菅義之(OSUGA, Yoshiyuki); 〒1020084 東京都千代田区二番町８番地２０ 二番町ビル３Ｆ 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, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, 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, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, 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, ML, MR, NE, SN, TD, TG).

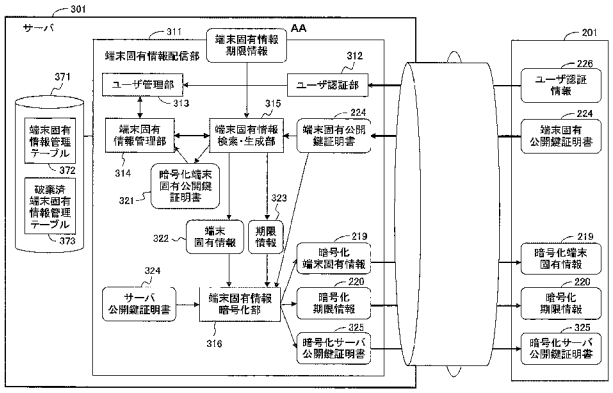
添付公開書類:

— 国際調査報告（条約第 21 条(3)）

(54) **Title**: TRANSMISSION METHOD AND SYSTEM FOR TERMINAL-SPECIFIC INFORMATION

(54) 発明の名称 : 端末固有情報の送信方法およびシステム

[図8]



219 Encrypted terminal-specific information
220 Encrypted time-limit information
224 Terminal-specific public key certificate
226 User authentication information
301 Server
311 Terminal-specific-information distribution unit
312 User authentication unit
313 User management unit
314 Terminal-specific-information management unit
315 Terminal-specific-information retrieval/generation unit
316 Terminal-specific-information encryption unit
321 Encrypted terminal-specific public key certificates
322 Terminal-specific information
323 Time-limit information
324 Server public key certificate
325 Encrypted server public key certificate
372 Terminal-specific-information management table
373 Previously-declined-terminal-specific-information management table
AA Terminal-specific-information time-limit information

(57) **Abstract**: Provided is a transmission method for terminal-specific information used to generate a terminal-specific work key used to encrypt a scramble key used to encrypt data, wherein a server receives from a terminal an acquisition request for terminal-specific information including the terminal-specific public key certificate of the terminal, browses a previously-declined-terminal information table, in which encrypted terminal-specific public key certificates for terminals not permitted to acquire the terminal-specific information are listed, to check whether an encrypted terminal-specific public key certificate of the terminal is listed in the previously-declined-terminal information table, and, in cases when said encrypted terminal-specific public key certificate is not listed, transmits the terminal-specific information to the terminal.

(57) 要約: データの暗号化に用いられるスクランブル鍵の暗号化に用いられる端末固有ワーク鍵の生成に用いられる端末固有情報の送信方法であって、サーバは、端末から、前記端末の端末固有公開鍵証明書を含む端末固有情報取得要求を受信し、前記端末固有情報の取得を許可しない端末の暗号化端末固有公開鍵証明書が記述された破棄済み端末情報テーブルを参照し、前記端末の暗号化端末固有公開鍵証明書が前記破棄済み端末情報テーブルに記述されているか否かチェックし、記述されていない場合、前記端末固有情報を前記端末に送信する。

WO 2013/114627 A1

明　細　書

発明の名称 ： 端末固有情報の送信方法およびシステム

技術分野

[0001] 本発明は、端末固有情報の送信方法およびシステムに関する。

背景技術

[0002] 現在、ダウンロードコンテンツや放送コンテンツを内蔵ハードディスクドライブ（ＨＤＤ）あるいは外部ＨＤＤに蓄積（ダビング）できる機能を持つ端末が利用されている。

それらの蓄積データは、受信した端末でしか再生できないようになっている。そうしないと、ＨＤＤに蓄積されたデータを無制限に複写して利用可能な端末が無制限に増えてしまう可能性があるからである。

[0003] しかしながら、受信した端末でしか再生できない場合、受信した端末が壊れてしまうと、ユーザは蓄積データの再生をあきらめなければならなかった。

その様な問題を解決するため、受信した端末が壊れてしまった場合、蓄積データを再生するために、従来は、サーバで端末毎の蓄積データ復元のための情報を利用者にくくりつけて管理しておき、端末が破損した場合でも、新しい端末でその蓄積データ再生のための情報をセンターから取得することにより蓄積データを再生可能としている。

先行技術文献

特許文献

[0004] 特許文献1：国際公開第２００３／００５２０８号パンフレット

特許文献2：特開２００１－６０９４５号公報

発明の開示

発明が解決しようとする課題

[0005] しかしながら、従来の方式では、端末が破損していなくても別の端末で蓄積データの再生のための情報を取得することにより、蓄積データを再生可能

な端末が不正に増加してしまう問題があった。

[0006] また、新しい端末が蓄積データの再生のための情報を取得中に破損してしまった場合、ユーザは、蓄積データの再生のための情報の取得をあきらめるか、サーバはユーザの不正を覚悟した上で蓄積データの再生のための情報を送信しなければならなかった。

[0007] 1つの側面では、本発明の課題は、蓄積データを利用可能な端末が不正に増加することを抑止することを目的とするである。

課題を解決するための手段

[0008] 実施の形態の方法は、データの暗号化に用いられるスクランブル鍵の暗号化に用いられる端末固有ワーク鍵の生成に用いられる端末固有情報の送信方法である。

サーバは、端末から、前記端末の端末固有公開鍵証明書を含む端末固有情報取得要求を受信し、前記端末の端末固有公開鍵証明書を暗号化して、暗号化端末固有公開鍵証明書を生成する。そして、サーバは、前記端末固有情報の取得を許可しない端末の暗号化端末固有公開鍵証明書が記述された破棄済み端末情報テーブルを参照し、生成された暗号化端末固有公開鍵証明書が前記破棄済み端末情報テーブルに記述されているか否かチェックし、記述されていない場合、前記端末の前記端末固有情報を前記端末に送信する。

発明の効果

[0009] 実施の形態の方法によれば、蓄積データを利用可能な端末が不正に増加することを抑止できる。

図面の簡単な説明

[0010] [図1]実施の形態に係るシステムの構成図である。

[図2]実施の形態に係る端末の詳細な構成図である。

[図3]実施の形態に係るＩＰ放送の受信・再生・蓄積処理のフローチャートである。

[図4]実施の形態に係る端末固有ワーク鍵生成処理のフローチャートである。

[図5]実施の形態に係る端末固有情報取得処理のフローチャートである。

[図6]実施の形態に係る蓄積データ再生処理のフローチャートである。

[図7]実施の形態に係る蓄積ＥＣＭ復号処理のフローチャートである。

[図8]実施の形態に係るサーバの詳細な構成図である。

[図9]端末固有情報管理テーブルの例である。

[図10]端末固有情報管理テーブルの復元先端末証明書リストの例である。

[図11]破棄済端末固有情報管理テーブルの例である。

[図12]実施の形態に係る端末固有情報配信処理のフローチャートである。

[図13]実施の形態に係る端末の詳細な構成図である。

[図14]復元先端末証明書リストの例である。

[図15A]実施の形態に係る端末固有ワーク鍵復元処理のフローチャートである。

[図15B]実施の形態に係る端末固有ワーク鍵復元処理のフローチャートである。

[図15C]実施の形態に係る端末固有ワーク鍵復元処理のフローチャートである。

[図16]更新前と更新後の復元先端末証明書リストの例である。

[図17]実施の形態に係る端末固有情報復元処理（端末側）のフローチャートである。

[図18]実施の形態に係るサーバの詳細な構成図である。

[図19]実施の形態に係る端末固有情報復元要求受信処理のフローチャートである。

[図20]実施の形態に係る端末固有情報復元処理（サーバ側）のフローチャートである。

[図21]情報処理装置（コンピュータ）の構成図である。

発明を実施するための形態

[0011] 以下、図面を参照しながら実施の形態を説明する。

図１は、実施の形態に係るシステムの構成図である。

システム１０１は、端末２０１およびサーバ３０１を備える。

[0012] 端末２０１とサーバ３０１は、有線または無線のネットワークを介して接続されている。

端末２０１は、放送データの受信、蓄積、再生等を行う装置である。端末２０１は、例えば、パーソナルコンピュータ、携帯電話、携帯端末、または映像録画装置などである。

[0013] 端末２０１は、端末固有ワーク鍵生成部２１１、端末固有ワーク鍵復元部２３１、Internet Protocol（ＩＰ）放送処理部２５１、蓄積データ復号部２７１、不揮発記憶域２８１、および記憶部２９１、および再生処理部２９９を備える。

[0014] 端末固有ワーク鍵生成部２１１は、端末固有ワーク鍵を生成する。

端末固有ワーク鍵復元部２３１は、端末固有ワーク鍵を復元する。

ＩＰ放送処理部２５１は、ＩＰ放送（放送データ）を受信し、放送データの復号、放送データの再暗号化や記憶部への格納を行う。

[0015] 蓄積データ復号部２７１は、記憶部２９１に格納された暗号化データを復号する。

不揮発記憶域２８１は、データを格納する不揮発性の記憶装置または記憶媒体である。不揮発記憶域２８１は、例えば、磁気ディスク装置（ハードディスクドライブ）、半導体記憶装置等である。

[0016] 記憶部２９１は、データを格納する記憶装置または記憶媒体である。記憶部２９１は、例えば、磁気ディスク装置（ハードディスクドライブ）、半導体記憶装置、またはメモリカード等である。記憶部２９１は、端末２０１から着脱可能であり、他の端末に接続することが出来る。

[0017] 再生処理部２９９は、復号されたデータを再生処理する。

サーバ３０１は、端末固有情報配信部３１１、端末固有情報復元部３３１、ワーク鍵配信部３５１、放送データ配信部３６１、および記憶部３７１を備える。

[0018] 端末固有情報配信部３１１は、暗号化された端末固有情報を端末に送信する。端末固有情報は、端末ごとに異なる端末固有の情報である。

端末固有情報復元部３３１は、端末固有情報復元要求を受信し、端末２０１が破棄済みであるか否かの判定や暗号化された端末固有情報の送信などを行う。

[0019] ワーク鍵配信部３５１は、ワーク鍵を端末２０１に送信する。

放送データ配信部３６１は、放送データを端末２０１に送信する。放送データは、暗号化ＴＳ／ＴＴＳおよび暗号化ＥＣＭを含む。

記憶部３７１は、データを格納する記憶装置である。記憶部３７１は、例えば、磁気ディスク装置（ハードディスクドライブ）、半導体記憶装置等である。

[0020] 図２は、実施の形態に係る端末の詳細な構成図である。

図２では、放送データの受信、蓄積、および蓄積データの再生に関連する構成要素について記載され、それ以外の構成要素については省略されている。

以下の説明において、図面において同一の符号を付したものは同一の物及び同様の効果を奏するものであるから、説明を省略する場合がある。

[0021] ＩＰ放送処理部２５１は、ワーク鍵取得部２５２、放送データ受信部２５３、ＥＣＭ復号部２５４、ＴＳ／ＴＴＳ復号部２５５、蓄積用ＥＣＭ生成部２５６、ＴＳ／ＴＴＳ再暗号化部２５７、およびＥＣＭ再暗号化部２５８を備える。

[0022] ワーク鍵取得部２５２は、ワーク鍵配信部３５１からワーク鍵２８２を取得し、不揮発記憶域２８１に格納する。

放送データ受信部２５３は、放送データ配信部３６１から放送データを受信する。

[0023] 放送データは、暗号化Transport Stream（ＴＳ）／Timestamped TS（ＴＴＳ）２５９および暗号化Entitlement Control Message（ＥＣＭ）２６０を含む。

暗号化ＴＳ／ＴＴＳ２５９は、ＴＳ形式またはＴＴＳ形式のデータ（ＴＳ／ＴＴＳ）をスクランブル鍵で暗号化したものである。

[0024] 暗号化ＥＣＭ２６０は、ワーク鍵ＩＤと暗号化スクランブル鍵を含む。ワーク鍵ＩＤは、スクランブル鍵の暗号化に用いられたワーク鍵を示す識別子である。暗号化スクランブル鍵は、スクランブル鍵をワーク鍵で暗号化したものである。

[0025] 放送データ受信部２５３は、暗号化ＥＣＭ２６０をＥＣＭ復号部２５４、暗号化ＴＳ／ＴＴＳ２５９をＴＳ／ＴＴＳ復号部２５５にそれぞれに出力する。

ＥＣＭ復号部２５４は、ワーク鍵ＩＤで示されるワーク鍵２８２を用いて暗号化ＥＣＭ２６０を復号（詳細には、暗号化スクランブル鍵を復号）し、ＥＣＭ２６１をＴＳ／ＴＴＳ復号部２５５および蓄積用ＥＣＭ生成部２５６に出力する。ＥＣＭ２６１は、ワーク鍵ＩＤと復号されたスクランブル鍵を含む。

[0026] ＴＳ／ＴＴＳ復号部２５５は、暗号化ＴＳ／ＴＴＳ２５９をＥＣＭ２６１に含まれるスクランブル鍵を用いて復号し、ＴＳ／ＴＴＳ２６２を再生処理部２９９およびＴＳ／ＴＴＳ再暗号化部２５７に出力する。

[0027] 蓄積用ＥＣＭ生成部２５６は、新たに生成したスクランブル鍵（蓄積用スクランブル鍵）と端末固有ワーク鍵２２１を示すワーク鍵ＩＤ（端末固有ワーク鍵ＩＤ）を含むＥＣＭ２６３を生成する。生成されたＥＣＭ２６３は、蓄積用ＥＣＭ２６３と呼ぶ。端末固有ワーク鍵ＩＤは、端末固有ワーク鍵２２１または端末固有ワーク鍵２２１を暗号化した暗号化端末固有ワーク鍵２９３を示す識別子である。

[0028] ＴＳ／ＴＴＳ再暗号化部２５７は、蓄積用スクランブル鍵を用いてＴＳ／ＴＴＳ２６２を暗号化し、暗号化ＴＳ／ＴＴＳ２９５を記憶部２９１に格納する。記憶部２９１に格納された暗号化ＴＳ／ＴＴＳ２９５は、蓄積用ＴＳ／ＴＴＳ２９５とも呼ぶ。

[0029] ＥＣＭ再暗号化部２５８は、蓄積用ＥＣＭ２６３を端末固有ワーク鍵ＩＤが示す端末固有ワーク鍵２２１を用いて暗号化し、暗号化ＥＣＭ２９４を記憶部２９１に格納する。詳細には、ＥＣＭ再暗号化部２５８は、蓄積用ＥＣ

Ｍ２６３に含まれる蓄積用スクランブル鍵を端末固有ワーク鍵２２１を用いて暗号化する。暗号化ＥＣＭ２９４は、端末固有ワーク鍵ＩＤと暗号化スクランブル鍵（暗号化された蓄積用スクランブル鍵）を含む。尚、記憶部２９１に格納された暗号化ＥＣＭ２９４は、蓄積ＥＣＭ２９４と呼称する場合がある。

[0030] 端末固有ワーク鍵生成部２１１は、端末固有情報取得処理部２１２、端末固有ワーク鍵生成処理部２１３、端末証明書暗号化鍵生成部２１４、端末固有ワーク鍵暗号化部２１５、端末証明書暗号化部２１６、および暗号化端末固有ワーク鍵管理部２１７を備える。

[0031] 端末固有情報取得処理部２１２は、サーバ３０１から暗号化端末固有情報２１９および暗号化期限情報２２０を取得する。

端末固有ワーク鍵生成処理部２１３は、端末固有ワーク鍵２２１を生成する。

[0032] 端末証明書暗号化鍵生成部２１４は、端末証明書暗号化鍵２８５を生成する。

端末固有ワーク鍵暗号化部２１５は、端末固有ワーク鍵２２１を暗号化し、暗号化端末固有ワーク鍵２９３を記憶部２９１に格納する。

[0033] 端末証明書暗号化部２１６は、端末固有公開鍵証明書２８４を暗号化し、暗号化端末固有公開鍵証明書２９２を記憶部２９１に格納する。

暗号化端末固有ワーク鍵管理部２１７は、暗号化端末固有ワーク鍵２９３を管理する。

[0034] 不揮発記憶域２８１は、ワーク鍵２８２、端末固有秘密鍵２８３、端末固有公開鍵証明書２８４、および端末証明書暗号化鍵２８５を格納する。端末固有秘密鍵２８３は、端末ごとに異なる端末固有の秘密鍵である。端末固有公開鍵証明書２８４は、端末ごとに異なる端末固有の公開鍵の証明書である。端末固有公開鍵証明書２８４は、端末２０１の公開鍵を含む。

[0035] 記憶部２９１は、暗号化端末固有公開鍵証明書２９２、暗号化端末固有ワーク鍵２９３、暗号化ＥＣＭ２９４、および暗号化ＴＳ／ＴＴＳ２９５を格

納する。

蓄積データ復号部２７１は、蓄積ＥＣＭ復号部２７２およびＴＳ／ＴＴＳ復号部２７３を備える。

[0036] 蓄積ＥＣＭ復号部２７２は、記憶部２９１に格納された暗号化ＥＣＭ２９４を復号し、ＥＣＭ２７４をＴＳ／ＴＴＳ復号部２７３に出力する。

ＴＳ／ＴＴＳ復号部２７３は、記憶部２９１に格納された暗号化ＴＳ／ＴＴＳ２９５をＥＣＭ２７４のスクランブル鍵で復号し、ＴＳ／ＴＴＳ２７５を再生処理部２９９に出力する。

再生処理部２９９は、ＴＳ／ＴＴＳ２６２、２７５のデコードやデジタル／アナログ変換処理などを行い、データを再生する。

[0037] 図３は、実施の形態に係るＩＰ放送の受信・再生・蓄積処理のフローチャートである。

ここで、端末２０１は、サーバ３０１から受信対象チャネルの放送データを受信しているものとする。

[0038] ステップＳ５０１において、ＥＣＭ復号部２５４は、受信対象チャネルのワーク鍵ＩＤを取得する。尚、ワーク鍵ＩＤは、受信された暗号化ＥＣＭ２６０に含まれている。

ステップＳ５０２において、ＥＣＭ復号部２５４は、取得したワーク鍵ＩＤに対応するワーク鍵２８２を不揮発記憶域２８１から検索する。

[0039] ステップＳ５０３において、ワーク鍵２８２が存在する場合、制御はステップＳ５０５に進み、存在しない場合、制御はステップＳ５０４に進む。

ステップＳ５０４において、ワーク鍵取得部２５２は、ワーク鍵配信部３５１からワーク鍵を取得し、不揮発記憶域２８１に格納する。

[0040] ステップＳ５０５において、暗号化端末固有ワーク鍵管理部２１７は、端末固有ワーク鍵ＩＤに対応する暗号化端末固有ワーク鍵２９３が記憶部２９１に存在するか否か検索する。

[0041] ステップＳ５０６において、暗号化端末固有ワーク鍵が存在する場合、制御はステップＳ５１０に進み、暗号化端末固有ワーク鍵が存在しない場合、

制御はステップＳ５０７に進む。

[0042] ステップＳ５０７において、端末固有ワーク鍵生成部２１１は、生成する端末固有ワーク鍵を示すワーク鍵ＩＤを指定して、端末固有ワーク鍵を生成する。端末固有ワーク鍵は、後述の端末固有ワーク鍵生成処理のステップＳ５２５～Ｓ５３２の処理により生成される。

[0043] ステップＳ５０８において、端末固有ワーク鍵の生成が正常に終了した場合、制御はステップＳ５１０に進み、正常に終了しなかった場合、制御はステップＳ５０９に進む。

ステップＳ５０９において、ＩＰ放送処理部２５１は、エラーをユーザに通知し、処理を終了する。

[0044] ステップＳ５１０において、暗号化端末固有ワーク鍵管理部２１７は、暗号化端末固有ワーク鍵２９３を端末証明書暗号化鍵２８５を用いて復号し、端末固有ワーク鍵をＥＣＭ再暗号化部２５８に出力する。

[0045] ステップＳ５１１において、ＩＰ放送処理部２５１は、放送データの復号処理および蓄積処理を行う。詳細には、ＥＣＭ復号部２５４は、受信対象チャネルのワーク鍵ＩＤに対応するワーク鍵２８２を用いて暗号化ＥＣＭ２６０を復号（詳細には、暗号化ＥＣＭ２６０に含まれる暗号化スクランブル鍵を復号）し、ＥＣＭ２６１をＴＳ／ＴＴＳ復号部２５５および蓄積用ＥＣＭ生成部２５６に出力する。

[0046] 蓄積用ＥＣＭ生成部２５６は、新たに生成したスクランブル鍵（蓄積用スクランブル鍵）と端末固有ワーク鍵２２１を示す端末固有ワーク鍵ＩＤを含む蓄積用ＥＣＭ２６３を生成する。

[0047] ＥＣＭ再暗号化部２５８は、蓄積用ＥＣＭ２６３を端末固有ワーク鍵２２１を用いて暗号化（詳細には、蓄積用ＥＣＭ２６３に含まれる蓄積用スクランブル鍵を暗号化）し、暗号化ＥＣＭ２９４を記憶部２９１に格納する。

[0048] ＴＳ／ＴＴＳ復号部２５５は、暗号化ＴＳ／ＴＴＳ２５９をＥＣＭ２６１に含まれるスクランブル鍵を用いて復号し、ＴＳ／ＴＴＳ２６２を再生処理部２９９およびＴＳ／ＴＴＳ再暗号化部２５７に出力する。

[0049] 再生処理部２９９は、ＴＳ／ＴＴＳ２６２のデコードやデジタル／アナログ変換処理などを行い、データを再生する。

ＴＳ／ＴＴＳ再暗号化部２５７は、蓄積用ＥＣＭ２６３に含まれる蓄積用スクランブル鍵を用いてＴＳ／ＴＴＳ２６２を暗号化し、暗号化ＴＳ／ＴＴＳ２９５を記憶部２９１に格納する。

[0050] 図４は、実施の形態に係る端末固有ワーク鍵生成処理のフローチャートである。

ステップＳ５２１において、端末固有ワーク鍵生成部２１１は、不揮発記憶域２８１から端末証明書暗号化鍵２８５を読み出す。

[0051] ステップＳ５２２において、端末固有ワーク鍵生成部２１１は、指定されたワーク鍵ＩＤに対応する暗号化端末固有ワーク鍵２９３を端末証明書暗号化鍵２８５を用いて復号する。

[0052] ステップＳ５２３において、端末固有ワーク鍵生成部２１１は、端末固有ワーク鍵２２１の期限情報を参照し、端末固有ワーク鍵２２１の期限情報と端末時刻と比較し、端末固有ワーク鍵２２１が期限切れであるか否か判定する。端末時刻は、端末２０１に設定されている時刻であり、現在の時刻である。期限情報には、端末固有ワーク鍵２２１の有効期限を示す終了時刻が含まれており、終了時刻が端末時刻を過ぎているか否かで、端末固有ワーク鍵２２１が期限切れであるか否か判定される。

[0053] ステップＳ５２４において、端末固有ワーク鍵２２１が期限切れの場合、処理は終了し、期限切れで無い場合、制御はステップＳ５２５に進む。

ステップＳ５２５において、端末固有情報取得処理部２１２は、端末固有公開鍵証明書２８４を指定して、端末固有情報取得処理を実行する。尚、端末固有情報取得処理の詳細は後述する。

[0054] ステップＳ５２６において、端末固有情報取得処理でエラーが応答された場合、制御はステップＳ５２７に進み、エラーが応答されなかった場合、制御はステップＳ５２８に進む。

[0055] ステップＳ５２７において、端末固有ワーク鍵生成部２１１は、エラーを

応答する。

ステップＳ５２８において、端末固有ワーク鍵生成処理部２１３は、端末固有情報取得処理によりサーバ３０１から受信した暗号化端末固有情報２１９と暗号化期限情報２２０を端末固有秘密鍵２８３を用いて復号する。

[0056] ステップＳ５２９において、端末固有ワーク鍵生成処理部２１３は、端末固有情報、期限情報、および指定されたワーク鍵ＩＤから端末固有ワーク鍵２２１を生成する。詳細には、端末固有ワーク鍵生成処理部２１３は、端末固有情報および指定されたワーク鍵ＩＤを用いて鍵情報を生成する。鍵情報は、端末固有情報および指定されたワーク鍵ＩＤから生成される一意な値である。鍵情報は、例えば、端末固有情報および指定されたワーク鍵ＩＤを暗号化したデータである。そして、端末固有ワーク鍵生成処理部２１３は、鍵情報に期限情報を付加し、期限情報が付加された鍵情報を端末固有ワーク鍵２２１とする。

[0057] ステップＳ５３０において、端末証明書暗号化鍵生成部２１４は、サーバ３０１から受信したサーバ公開鍵証明書内の公開鍵と端末固有秘密鍵２８３からDiffie-Hellman(DH)方式により、共用鍵を生成する。そして、端末証明書暗号化鍵生成部２１４は、共用鍵を端末証明書暗号化鍵２８５として不揮発記憶域２８１に格納する。

[0058] ステップＳ５３１において、端末固有ワーク鍵暗号化部２１５は、端末固有ワーク鍵２２１を端末証明書暗号化鍵２８５を用いて暗号化し、暗号化端末固有ワーク鍵２９３を記憶部２９１に格納する。

[0059] ステップＳ５３２において、端末証明書暗号化部２１６は、端末固有公開鍵証明書２８４を端末証明書暗号化鍵２８５を用いて暗号化し、暗号化端末固有公開鍵証明書２９２を記憶部２９１に格納する。

[0060] 図５は、実施の形態に係る端末固有情報取得処理の詳細なフローチャートである。

図５のフローチャートは、図４のステップＳ５２５に対応する。

ステップＳ５４１において、端末固有情報取得処理部２１２は、不揮発記

憶域２８１から端末固有公開鍵証明書２８４を読み出す。

[0061] ステップＳ５４２において、端末固有情報取得処理部２１２は、端末固有公開鍵証明書２８４を指定してサーバ３０１にサーバ公開鍵証明書取得要求を送信する。

ステップＳ５４３において、サーバ３０１からエラー応答を受信した場合、制御はステップＳ５４４に進み、エラー応答を受信しない場合、制御はステップＳ５４５に進む。

[0062] ステップＳ５４４において、端末固有情報取得処理部２１２は、エラーを応答する。

ステップＳ５４５において、端末固有情報取得処理部２１２は、サーバ３０１から受信した暗号化サーバ公開鍵証明書を端末固有秘密鍵２８３を用いて復号し、サーバ公開鍵証明書を不揮発記憶域２８１に格納する。サーバ公開鍵証明書は、サーバの公開鍵の証明書であり、サーバの公開鍵（サーバ公開鍵）を含む。

[0063] ステップＳ５４６において、端末固有情報取得処理部２１２は、ユーザ認証情報２２６をサーバ公開鍵証明書の公開鍵を用いて暗号化し、ワンタイムパスワード取得要求を作成する。ワンタイムパスワード取得要求には、暗号化されたユーザ認証情報が含まれる。尚、使用されるユーザ認証情報２２６は、処理開始時に入力パラメータとして指定される。

[0064] ステップＳ５４７において、端末固有情報取得処理部２１２は、サーバ３０１にワンタイムパスワード取得要求を送信する。

ステップＳ５４８において、端末固有情報取得処理部２１２は、サーバ３０１からエラー応答を受信した場合、制御はステップＳ５４９に進み、エラー応答を受信しない場合、制御はステップＳ５５０に進む。

[0065] ステップＳ５４９において、端末固有情報取得処理部２１２は、エラーを応答する。

ステップＳ５５０において、端末固有情報取得処理部２１２は、サーバ３０１から暗号化ワンタイムパスワードを受信する。

[0066] ステップＳ５５１において、端末固有情報取得処理部２１２は、暗号化ワンタイムパスワードを端末固有秘密鍵２８３を用いて復号する。

ステップＳ５５２において、端末固有情報取得処理部２１２は、ワンタイムパスワードと端末固有公開鍵証明書２８４をサーバ公開鍵証明書の公開鍵を用いて暗号化し、端末固有情報取得要求を作成する。すなわち、端末固有情報取得要求には、暗号化されたワンタイムパスワード（暗号化ワンタイムパスワード）と暗号化された端末固有公開鍵証明書（暗号化端末固有公開鍵証明書）が含まれる。

[0067] ステップＳ５５３において、端末固有情報取得処理部２１２は、端末固有情報取得要求をサーバ３０１に送信する。

ステップＳ５５４において、端末固有情報取得処理部２１２は、サーバ３０１からエラー応答を受信した場合、制御はステップＳ５５５に進み、エラー応答を受信しない場合、制御はステップＳ５５６に進む。

[0068] ステップＳ５５５において、端末固有情報取得処理部２１２は、エラーを応答する。

ステップＳ５５６において、端末固有情報取得処理部２１２は、サーバ３０１から暗号化端末固有情報２１９および暗号化期限情報２２０を受信する。

[0069] 次に、記憶部２９１に格納された暗号化ＴＳ／ＴＴＳ（蓄積データ）２９５の再生処理について説明する。

図６は、実施の形態に係る蓄積データ再生処理のフローチャートである。

[0070] ステップＳ５６１において、蓄積ＥＣＭ復号部２７２は、再生対象の暗号化ＴＳ／ＴＴＳ２９５に対応する暗号化ＥＣＭ２９４を特定する。すなわち、蓄積ＥＣＭ復号部２７２は、暗号化ＴＳ／ＴＴＳ２９５の暗号化に用いられたスクランブル鍵を含む暗号化ＥＣＭ２９４を特定する。

[0071] ステップＳ５６２において、蓄積ＥＣＭ復号部２７２は、特定された暗号化ＥＣＭ２９４を指定して蓄積ＥＣＭ復号処理を行い、復号されたＥＣＭ２７４をＴＳ／ＴＴＳ復号部２７３に出力する。尚、蓄積ＥＣＭ復号処理の詳

細については後述する。

[0072] ステップＳ５６３において、ＴＳ／ＴＴＳ復号部２７３は、暗号化ＴＳ／ＴＴＳ２９５をＥＣＭ２７４のスクランブル鍵で復号し、ＴＳ／ＴＴＳ２７５を再生処理部に２９９に出力する。

ステップＳ５６４において、再生処理部２９９は、ＴＳ／ＴＴＳ２７５のデコードやデジタル／アナログ変換処理などを行い、データを再生する。

[0073] 図７は、実施の形態に係る蓄積ＥＣＭ復号処理のフローチャートである。

図７のフローチャートは、図６のステップＳ５６２に対応する。

ステップＳ５７１において、蓄積ＥＣＭ復号部２７２は、指定された暗号化ＥＣＭ２９４に含まれるワーク鍵ＩＤを取得する。

[0074] ステップＳ５７２において、蓄積ＥＣＭ復号部２７２は、取得したワーク鍵ＩＤに対応する暗号化端末固有ワーク鍵２９３が記憶部２９１に存在するか否か検索する。

ステップＳ５７３において、蓄積ＥＣＭ復号部２７２は、暗号化端末固有ワーク鍵２９３が存在する場合、制御はステップＳ５７５に進み、存在しない場合、制御はステップＳ５７４に進む。

[0075] ステップＳ５７４において、蓄積ＥＣＭ復号部２７２は、エラーを応答する。

ステップＳ５７５において、蓄積ＥＣＭ復号部２７２は、取得したワーク鍵ＩＤを指定して端末固有ワーク鍵生成処理を実行し、端末証明書暗号化鍵２８５を取得する。端末固有ワーク鍵生成処理は、図４で説明した通りである。

[0076] ステップＳ５７６において、端末固有ワーク鍵生成処理において、正常終了した（エラーが応答されなかった）場合、制御はステップＳ５７８に進み、正常終了しなかった（エラーが応答された）場合、制御はステップＳ５７７に進む。

[0077] ステップＳ５７７において、蓄積ＥＣＭ復号部２７２は、エラーを応答する。

ステップＳ５７８において、蓄積ＥＣＭ復号部２７２は、暗号化端末固有ワーク鍵２９３を端末証明書暗号化鍵２８５を用いて復号し、端末固有ワーク鍵２１１を取得する。

[0078] ステップＳ５７９において、蓄積ＥＣＭ復号部２７２は、指定された暗号化ＥＣＭ２９４を端末固有ワーク鍵２２１を用いて復号する。詳細には、蓄積ＥＣＭ復号部２７２は、指定された暗号化ＥＣＭ２９４に含まれる暗号化スクランブル鍵を端末固有ワーク鍵２２１の鍵情報を用いて復号する。蓄積ＥＣＭ復号部２７２は、復号されたスクランブル鍵を含むＥＣＭ２７４をＴＳ／ＴＴＳ復号部２７３に出力する。

[0079] 次に、端末固有情報取得処理時のサーバ側の処理（端末固有情報配信処理）について説明する。

図８は、実施の形態に係るサーバの詳細な構成図である。

[0080] 図８では、端末固有情報の配信に関連する構成要素について記載され、それ以外の構成要素については省略されている。

端末固有情報配信部３１１は、ユーザ認証部３１２、ユーザ管理部３１３、端末固有情報管理部３１４、端末固有情報検索・生成部３１５、および端末固有情報暗号化部３１６を備える。

[0081] ユーザ認証部３１２は、暗号化ユーザ認証情報を復号する。

ユーザ管理部３１３は、ユーザ認証を行う。

端末固有情報管理部３１４は、端末固有情報管理テーブル３７２および破棄済端末固有情報管理テーブル３７３へのデータの書き込み、削除等を行う。

[0082] 端末固有情報検索・生成部３１５は、端末固有情報管理テーブル３７２の検索やレコードの生成等を行う。

端末固有情報暗号化部３１６は、端末固有情報３２２、期限情報３２３、およびサーバ公開鍵証明書３２４を暗号化し、暗号化端末固有情報２１９、暗号化期限情報２２０、および暗号化サーバ公開鍵証明書３２５を生成する。

[0083] 記憶部３７１は、端末固有情報管理テーブル３７２および破棄済端末固有情報管理テーブル３７３を有する。

図９は、端末固有情報管理テーブルの例である。

[0084] 端末固有情報管理テーブル３７２には、暗号化端末固有公開鍵証明書、復元先端末証明書リスト、端末固有情報、期限情報が対応付けられて記述されている。

暗号化端末固有公開鍵証明書は、暗号化された端末固有の公開鍵の証明書である。

[0085] 復元先端末証明書リストは、過去に端末固有ワーク鍵復元処理を行った端末を示す情報である。尚、復元先端末証明書リストの詳細については後述する。

端末固有情報は、端末固有公開鍵証明書から生成される端末固有の情報である。

[0086] 期限情報は、端末固有ワーク鍵の有効期限の開始時刻と終了時刻を示す。

図１０は、端末固有情報管理テーブルの復元先端末証明書リストの例である。

復元先端末証明書リストは、過去に端末固有ワーク鍵復元処理を行った端末の端末固有公開鍵証明書と電子署名を含む。

[0087] 過去に端末固有ワーク鍵復元処理を行った端末の端末固有公開鍵証明書は、端末固有ワーク鍵復元処理を行った順に先頭から配置される。

復元先端末証明書リストの最後尾には、電子署名として、最後の端末固有公開鍵証明書の端末の秘密鍵で過去に端末固有ワーク鍵復元処理を行った端末の端末固有公開鍵証明書を署名した値が記述されている。

[0088] 図１０の復元先端末証明書リストは、端末Ａおよび端末Ｂの端末固有公開鍵証明書と端末Ｂの端末固有秘密鍵で端末ＡおよびＢの端末固有公開鍵証明書を署名した電子署名で構成されている。

[0089] 図１１は、破棄済端末固有情報管理テーブルの例である。

破棄済端末固有情報管理テーブル３７３には、破棄済みとなった端末に対

応する暗号化端末固有公開鍵証明書が記述されている。すなわち、破棄済端末固有情報管理テーブル３７３には、端末固有情報の取得を許可しない端末に対応する暗号化端末固有公開鍵証明書が記述されている。

[0090] 図１２は、実施の形態に係る端末固有情報配信処理のフローチャートである。

ステップＳ６０１において、端末固有情報配信部３１１は、端末２０１から要求を受信する。

[0091] ステップＳ６０２において、端末固有情報配信部３１１は、要求がサーバ公開鍵証明書取得要求であるか否か判定する。要求がサーバ公開鍵証明書取得要求である場合、制御はステップＳ６０３に進み、サーバ公開鍵証明書取得要求でない場合、制御はステップＳ６０５に進む。

[0092] ステップＳ６０３において、端末固有情報暗号化部３１６は、サーバ公開鍵証明書３２４をサーバ公開鍵証明書取得要求で指定された端末固有公開鍵証明書の公開鍵で暗号化し、暗号化サーバ公開鍵証明書３２５を作成する。

[0093] ステップＳ６０４において、端末固有情報暗号化部３１６は、暗号化サーバ公開鍵証明書を端末２０１に送信する。

ステップＳ６０５において、端末固有情報配信部３１１は、要求がワンタイムパスワード取得要求であるか否か判定する。要求がワンタイムパスワード取得要求である場合、制御はステップＳ６０６に進み、ワンタイムパスワード取得要求でない場合、制御はステップＳ６１１に進む。なお、要求がワンタイムパスワード取得要求でない場合、端末から受信した要求は、端末固有情報取得要求である。

[0094] ステップＳ６０６において、ユーザ認証部３１２は、ワンタイムパスワード要求に含まれる暗号化ユーザ認証情報をサーバ秘密鍵を用いて復号し、ユーザ認証情報２２６を取得する。

[0095] ステップＳ６０７において、ユーザ管理部３１３は、ユーザ認証情報をチェックし、ユーザ認証を行う。ユーザ認証がエラーの場合、制御はステップＳ６０８に進み、ユーザ認証がエラーでない場合、制御はステップＳ６０９

に進む。

[0096] ステップＳ６０８において、端末固有情報配信部３１１は、エラー応答を端末２０１に送信する。

ステップＳ６０９において、端末固有情報配信部３１１は、ワンタイムパスワードを生成し、端末固有公開鍵証明書の公開鍵で暗号化し、暗号化ワンタイムパスワードを作成する。

[0097] ステップＳ６１０において、端末固有情報配信部３１１は、暗号化ワンタイムパスワードを端末２０１に送信する。

ステップＳ６１１において、ユーザ認証部３１２は、端末固有情報取得要求をサーバ秘密鍵を用いて復号し、ワンタイムパスワードおよび端末固有公開鍵証明書２８４を取得する。そして、ユーザ認証部３１２は、ワンタイムパスワードが期限切れであるかチェックする。

[0098] ステップＳ６１２において、ワンタイムパスワードが期限切れである場合、制御はステップＳ６１３に進み、期限切れでない場合、制御はステップＳ６１４に進む。

ステップＳ６１３において、端末固有情報配信部３１１は、エラー応答を端末２０１に送信する。

[0099] ステップＳ６１４において、端末固有情報検索・生成部３１５は、暗号化端末固有公開鍵証明書３２１を生成する。詳細には、端末固有情報検索・生成部３１５は、端末固有公開鍵証明書２８４の公開鍵とサーバ秘密鍵からDiffie-Hellman(DH)方式により、共用鍵を生成する。端末固有情報検索・生成部３１５は、生成した共用鍵を端末証明書暗号化鍵とする。そして、端末固有情報検索・生成部３１５は、端末固有公開鍵証明書２８４を端末証明書暗号化鍵を用いて暗号化し、暗号化端末固有公開鍵証明書３２１を生成する。

[0100] ステップＳ６１５において、端末固有情報検索・生成部３１５は、破棄済端末固有情報管理テーブル３７３を参照し、暗号化端末固有公開鍵証明書３２１が破棄済み端末のものであるか、すなわち、破棄済端末固有情報管理テーブル３７３に暗号化端末固有公開鍵証明書３２１が記述されているかチェ

ックする。破棄済端末固有情報管理テーブル３７３に暗号化端末固有公開鍵証明書３２１が記述されている場合、制御はステップＳ６１６に進み、記述されていない場合、制御はステップＳ６１７に進む。

[0101] ステップＳ６１６において、端末固有情報配信部３１１は、エラー応答を端末２０１に送信する。

ステップＳ６１７において、端末固有情報検索・生成部３１５は、端末固有情報管理テーブル３７２から、生成された暗号化端末固有公開鍵証明書３２１が出現するレコードを検出する。

[0102] ステップＳ６１８において、端末固有情報検索・生成部３１５は、検出されたレコードに端末固有情報が登録（記述）されているか否か判定する。検出されたレコードに端末固有情報が登録されている場合、制御はステップＳ６２０に進み、登録されていない場合、制御はステップＳ６１９に進む。また、検出されたレコードに端末固有情報が登録されている場合、端末固有情報検索・生成部３１５は、検出されたレコードの端末固有情報と期限情報を端末固有情報暗号化部３１６に出力する。

[0103] ステップＳ６１９において、端末固有情報検索・生成部３１５は、端末固有公開鍵証明書と乱数から端末固有情報を作成し、期限情報を設定し、端末固有情報および期限情報を端末固有情報管理部３１４および端末固有情報暗号化部３１６に出力する。端末固有情報管理部３１４は、端末固有情報および期限情報を端末固有情報管理テーブル３７２に書き込む。尚、端末固有情報は、端末固有公開鍵証明書と乱数から生成される一意な値である。

[0104] ステップＳ６２０において、端末固有情報暗号化部３１６は、端末固有情報と期限情報を端末固有公開鍵証明書の公開鍵を用いて暗号化し、暗号化端末固有情報および暗号化期限情報を作成する。

[0105] ステップＳ６２１において、端末固有情報暗号化部３１６は、暗号化端末固有情報および暗号化期限情報を端末２０１に送信する。

次に端末固有ワーク鍵の復元について説明する。

[0106] 端末が故障した場合、ユーザは、記憶部を故障した端末から取り外し、他

の端末に接続する。若しくは、ユーザは、故障した端末の記憶部のデータを他の端末の記憶部にコピーする。

[0107] 上述の蓄積データ再生処理で説明したように、蓄積データの再生には、端末固有ワーク鍵が必要となる。端末固有ワーク鍵を得るためには、暗号化端末固有ワーク鍵を端末証明書暗号化鍵を用いて復号する必要がある。

[0108] 故障した端末から新たな端末に記憶部を移動させた場合、端末証明書暗号化鍵は、端末ごとに異なるため、記憶部に格納された暗号化端末固有ワーク鍵は、新たな端末で復号できない。

[0109] したがって、故障した端末から新たな端末に記憶部を移動させただけでは、記憶部に格納された蓄積データを再生することは出来ない。

新たな端末で、破損した端末で格納した蓄積データを再生するためには、新たな端末に対応した端末固有ワーク鍵が必要となる。

[0110] したがって、ユーザは、記憶部を新たな端末に接続したときは、以下に説明するような端末固有ワーク鍵復元処理を新たな端末に実行させる。

それにより、記憶部に格納された暗号化端末固有ワーク鍵は、新たな端末で復号可能な暗号化端末固有ワーク鍵に更新される。

[0111] 図１３は、実施の形態に係る端末の詳細な構成図である。

図１３では、端末固有ワーク鍵の復元に関連する構成要素について記載され、それ以外の構成要素または説明済みの構成要素については省略されている。

[0112] 端末固有ワーク鍵復元部２３１は、端末固有情報復元処理部２３２、端末固有ワーク鍵生成処理部２３３、端末証明書暗号鍵生成部２３４、端末固有ワーク鍵暗号化部２３５、端末証明書暗号化部２３６、および復元要求生成部２３７を備える。

[0113] 端末固有情報復元処理部２３２は、端末固有情報復元処理（端末側）を実行する。

端末固有ワーク鍵生成処理部２３３は、端末固有ワーク鍵２４２を生成する。

端末証明書暗号鍵生成部２３４は、端末証明書暗号化鍵２８５を生成する。

[0114] 端末固有ワーク鍵暗号化部２３５は、端末固有ワーク鍵２４２を端末証明書暗号化鍵２８５を用いて暗号化し、暗号化端末固有ワーク鍵２９３を記憶部２９１に格納する。

端末証明書暗号化部２３６は、端末固有公開鍵証明書２８４を端末証明書暗号化鍵２８５を用いて暗号化し、暗号化端末固有公開鍵証明書２９２を記憶部２９１に格納する。

[0115] 復元要求生成部２３７は、端末固有情報復元要求２４３を生成する。

不揮発記憶域２８１は、端末固有秘密鍵２８３、端末固有公開鍵証明書２８４、端末証明書暗号化鍵２８５を格納する。

[0116] 記憶部２９１は、暗号化端末固有公開鍵証明書２９２、暗号化端末固有ワーク鍵２９３、暗号化ＥＣＭ２９４、暗号化ＴＳ／ＴＴＳ２９５、および復元先端末証明書リスト２９６を格納する。

[0117] 図１４は、復元先端末証明書リストの例である。

復元先端末証明書リスト２９６は、過去に端末固有ワーク鍵復元処理を行った端末の端末固有公開鍵証明書と電子署名を含む。

[0118] 過去に端末固有ワーク鍵復元処理を行った端末の端末固有公開鍵証明書は、端末固有ワーク鍵復元処理を行った順に先頭から配置される。

復元先端末証明書リストの最後尾には、電子署名として、最後の端末固有公開鍵証明書の端末の秘密鍵（端末固有秘密鍵）で過去に端末固有ワーク鍵復元処理を行った端末の端末固有鍵証明書を署名した値が記述されている。

[0119] 図１４の復元先端末証明書リストは、端末Ａおよび端末Ｂの端末固有公開鍵証明書と端末Ｂの端末固有秘密鍵で端末ＡおよびＢの端末固有公開鍵証明書を署名した電子署名で構成されている。

[0120] 図１５Ａ、１５Ｂ、および１５Ｃは、実施の形態に係る端末固有ワーク鍵復元処理のフローチャートである。

ステップＳ７０１において、端末固有ワーク鍵復元部２３１は、不揮発記

憶域２８１に端末証明書暗号化鍵２８５が存在するかチェックする。端末証明書暗号化鍵２８５が存在する場合、聖書はステップＳ７０２に進み、端末証明書暗号化鍵２８５が存在しない場合、制御はステップＳ７１２に進む。

[0121] ステップＳ７０２において、端末証明書暗号化部２３６は、端末固有公開鍵証明書２８４を端末証明書暗号化鍵２８５を用いて暗号化し、暗号化端末固有公開鍵証明書を生成する。

[0122] ステップＳ７０３において、端末固有ワーク鍵復元部２３１は、記憶部２９１に格納されている暗号化端末固有公開鍵証明書２９２とステップＳ７０２で生成された暗号化端末固有公開鍵証明書とが等しいか否か判定する。暗号化端末固有公開鍵証明書２９２とステップＳ７０２で生成された暗号化端末固有公開鍵証明書とが等しい場合、制御はステップＳ７０４に進み、等しくない場合、制御はステップＳ７１２に進む。

[0123] ステップＳ７０４において、端末固有ワーク鍵復元部２３１は、記憶部２９１に復元先端末証明書リスト２９６があるかチェックする。端末固有ワーク鍵復元部２３１は、記憶部２９１に復元先端末証明書リスト２９６がある場合、復元先端末証明書リスト２９６を削除する。

[0124] ステップＳ７０５において、端末固有情報取得処理部２１２は、端末固有公開鍵証明書を指定して、端末固有情報取得処理を実行する。

ステップＳ７０６において、端末固有情報取得処理でエラーが応答された場合、制御はステップＳ７０７に進み、エラーが応答されなかった場合、制御はステップＳ７０８に進む。

[0125] ステップＳ７０７において、端末固有ワーク鍵生成部２１１は、エラーを応答する。

ステップＳ７０８において、端末固有ワーク鍵生成処理部２３３は、端末固有情報取得処理によりサーバ３０１から受信した暗号化端末固有情報２４０と暗号化期限情報２４１を端末固有秘密鍵２８３を用いて復号する。

[0126] ステップＳ７０９において、端末証明書暗号化鍵生成部２３４は、サーバ３０１から受信したサーバ公開鍵証明書内の公開鍵と端末固有秘密鍵２８３

からDiffie-Hellman(DH)方式により、共用鍵を生成する。そして、端末証明書暗号化鍵生成部２３４は、共用鍵を端末証明書暗号化鍵２８５として不揮発記憶域２８１に格納する。

[0127] ステップＳ７１０において、端末証明書暗号化部２３６は、端末固有公開鍵証明書２８４を端末証明書暗号化鍵２８５を用いて暗号化し、暗号化端末固有公開鍵証明書２９２を記憶部２９１に格納する。

[0128] ステップＳ７１２において、端末固有ワーク鍵復元部２３１は、記憶部２９１に格納された暗号化端末固有公開鍵証明書２９２と復元先端末証明書リスト２９６、および不揮発記憶域２８１に格納された端末固有公開鍵証明書２８４を参照する。

[0129] ステップＳ７１３において、端末固有ワーク鍵復元部２３１は、復元先端末証明書リスト２９６の最新エレメントを比較対象に設定する。復元先端末証明書リスト２９６の最新エレメントは、復元先端末証明書リスト２９６に含まれる端末固有公開鍵証明書の内、最後（最後尾）に記述された端末固有公開鍵証明書である。比較対象に設定されたエレメント（端末固有公開鍵証明書）は、比較対象エレメントと呼ぶ。

[0130] ステップＳ７１４において、比較対象として設定されるエレメントが無い場合、制御はステップＳ７１５に進み、比較対象として設定されるエレメントがある場合、制御はステップＳ７１８に進む。

[0131] ステップＳ７１５において、端末固有ワーク鍵復元部２３１は、復元先端末証明書リスト２９６の端末固有公開鍵証明書の最後尾に端末固有公開鍵証明書２８４を追加（記述）する。新たに記述された端末固有公開鍵証明書２８４は最新エレメントとなる。

[0132] ステップＳ７１６において、端末固有ワーク鍵復元部２３１は、端末固有秘密鍵２８３を用いて作成した電子署名を作成し、電子署名を復元先端末証明書リスト２９６に付加する。尚、古い電子署名は新たな電子署名に上書きされる。

[0133] ステップＳ７１７において、端末固有ワーク鍵復元部２３１は、新たに生

成された復元先端末証明書リスト２９６を記憶部２９１に書き込む。

ここで、ステップＳ７１５～Ｓ７１７の実行前（更新前）と実行後（更新後）の復元先端末証明書リストについて示す。

[0134] 図１６は、更新前と更新後の復元先端末証明書リストの例である。

ここで、端末固有ワーク鍵復元処理は、端末Ｃで実行されているとする。

更新前の復元先端末証明書リスト２９６－１は、図１４で説明した復元先端末証明書リスト２９６と同様である。

[0135] 新たに生成された（更新後の）復元先端末証明書リスト２９６－２は、端末Ａ、Ｂ、およびＣの端末固有公開鍵証明書と端末Ｃの端末固有秘密鍵で端末Ａ、Ｂ、およびＣの端末固有鍵証明書を署名した電子署名で構成されている。

[0136] すなわち、更新後の復元先端末証明書リスト２９６－２は、更新前の復元先端末証明書リスト２９６－１の端末Ｂの端末固有公開鍵証明書の後に端末Ｃの端末固有公開鍵証明書が記述され、端末Ｃの端末固有公開鍵証明書の後に端末Ｃの端末固有秘密鍵で端末Ａ、Ｂ、およびＣの端末固有鍵証明書を署名した電子署名が記述されたものである。

[0137] ステップＳ７１８において、端末固有ワーク鍵復元部２３１は、不揮発記憶域２８１の端末固有公開鍵証明書２８４と比較対象に設定された端末固有公開鍵証明書とが等しいか判定する。端末固有公開鍵証明書２８４と比較対象に設定された端末固有公開鍵証明書とが等しい場合、制御はステップＳ７２０に進み、等しくない場合、制御はステップＳ７１９に進む。

[0138] ステップＳ７１９において、端末固有ワーク鍵復元部２３１は、比較対象エレメントの１つ前のエレメントを新たな比較対象として設定する。

ステップＳ７２０において、端末固有ワーク鍵復元部２３１は、端末固有公開鍵証明書２８４と等しい復元先端末証明リスト２９６内の端末固有公開鍵証明書は、最新エレメントであるか否か判定する。端末固有公開鍵証明書２８４と等しい復元先端末証明リスト２９６内の端末固有公開鍵証明書が最新エレメントである場合、制御はステップＳ７２２に進み、最新エレメント

で無い場合、制御はステップＳ７２１に進む。

[0139] ステップＳ７２１において、端末固有ワーク鍵復元部２３１は、エラーを応答する。このように、以前に端末固有ワーク鍵復元処理を行い、他の端末に端末固有ワーク鍵を復元済みの端末である場合は、エラーとなる。

[0140] ステップＳ７２２において、端末固有情報復元処理部２３２は、暗号化端末固有公開鍵証明書２９２と復元先端末証明書リスト２９６を指定して、端末固有情報復元処理を実行する。端末固有情報復元処理（端末側）の詳細については、後述する。

[0141] ステップＳ７２３において、端末固有情報復元処理（端末側）でエラーが応答された場合、制御はステップＳ７２４進み、エラーが応答されなかった場合、制御はステップＳ７２５に進む。

[0142] ステップＳ７２４において、端末固有情報復元処理部２３２は、エラーを応答する。

ステップＳ７２５において、端末固有ワーク鍵復元部２３１は、サーバ３０１から受信した暗号化端末固有情報２４０および暗号化期限情報２４１を端末固有秘密鍵２８３を用いて復号する。

[0143] ステップＳ７２６において、端末証明書暗号化鍵生成部２３４は、サーバ３０１から受信したサーバ公開鍵証明書２３９内の公開鍵と端末固有秘密鍵２８３からDiffie-Hellman(DH)方式により、共用鍵を生成する。そして、端末証明書暗号化鍵生成部２３４は、共用鍵を端末証明書暗号化鍵２８５として不揮発記憶域２８１に格納する。

[0144] ステップＳ７２７において、端末証明書暗号化部２３６は、端末固有公開鍵証明書２８４を端末証明書暗号化鍵２８５を用いて暗号化し、暗号化端末固有公開鍵証明書２９２を記憶部２９１に格納する。

[0145] ステップＳ７２８において、端末固有ワーク鍵復元部２３１は、記憶部２９１に格納された復元先端末証明書リスト２９６を削除する。

ステップＳ７２９において、端末固有ワーク鍵復元部２３１は、記憶部２９１に格納された暗号化端末固有ワーク鍵２９３の内、未処理の（すなわち

、ステップＳ７３２の上書きをされていない）暗号化端末固有ワーク鍵２９３を一つ読み込む。

[0146] ステップＳ７３０において、読み込みエラーの場合（すなわち、未処理の暗号化端末固有ワーク鍵２９３が無かった場合）、処理を終了し、読み込みエラーで無い場合、ステップＳ７３１に進む。

[0147] ステップＳ７３１において、端末固有ワーク鍵生成処理部２３３は、サーバ３０１から受信した端末固有公報、期限情報、および記憶部２９１から読み出した暗号化端末固有ワーク鍵２９３のワーク鍵ＩＤを用いて、端末固有ワーク鍵２４２を作成する。

[0148] ステップＳ７３２において、端末固有ワーク鍵暗号化部２３５は、作成した端末固有ワーク鍵２４２を端末証明書暗号化鍵２８５を用いて暗号化し、暗号化端末固有ワーク鍵を作成する。そして、端末固有ワーク鍵暗号化部２３５は、作成した暗号化端末固有ワーク鍵を記憶部２９１から読み出した暗号化端末固有ワーク鍵２９３のワーク鍵ＩＤが示す記憶部２９１に格納された暗号化端末ワーク鍵２９３に上書きする。

[0149] 図１７は、実施の形態に係る端末固有情報復元処理（端末側）のフローチャートである。

図１７のフローチャートは、図１５Ｃのステップ７２２に対応する。

[0150] ステップＳ７４１において、端末固有情報復元処理部２３２は、不揮発記憶域２８１から端末固有公開鍵証明書２８４を読み出す。

ステップＳ７４２において、端末固有情報復元処理部２３２は、端末固有公開鍵証明書２８４を指定してサーバ３０１にサーバ公開鍵証明書取得要求を送信する。

[0151] ステップＳ７４３において、サーバ３０１からエラー応答を受信した場合、制御はステップＳ７４４に進み、エラー応答を受信しない場合、制御はステップＳ７４５に進む。

ステップＳ７４４において、端末固有情報復元処理部２３２は、エラーを応答する。

[0152] ステップＳ７４５において、端末固有情報復元処理部２３２は、サーバ３０１から受信した暗号化サーバ公開鍵証明書を端末固有秘密鍵２８３を用いて復号し、サーバ公開鍵証明書２３９を取得する。

[0153] ステップＳ７４６において、端末固有情報復元処理部２３２は、ユーザ認証情報２４７をサーバ公開鍵証明書２３９の公開鍵を用いて暗号化し、ワンタイムパスワード取得要求を作成する。ワンタイムパスワード取得要求には、暗号化されたユーザ認証情報２４７が含まれる。尚、使用されるユーザ認証情報２４７は、処理開始時に入力パラメータとして指定される。

[0154] ステップＳ７４７において、端末固有情報復元処理部２３２は、サーバ３０１にワンタイムパスワード取得要求を送信する。

ステップＳ７４８において、端末固有情報復元処理部２３２は、サーバ３０１からエラー応答を受信した場合、制御はステップＳ７４９に進み、エラー応答を受信しない場合、制御はステップＳ７５０に進む。

[0155] ステップＳ７４９において、端末固有情報復元処理部２３２は、エラーを応答する。

ステップＳ７５０において、端末固有情報復元処理部２３２は、サーバ３０１から暗号化ワンタイムパスワードを受信する。

[0156] ステップＳ７５１において、端末固有情報復元処理部２３２は、暗号化ワンタイムパスワードを端末固有秘密鍵２８３を用いて復号し、ワンタイムパスワードを取得する。

ステップＳ７５２において、復元要求生成部２３７は、ワンタイムパスワードと暗号化端末固有公開鍵証明書２９２と復元先端末証明書リスト２９６をサーバ公開鍵証明書２３９の公開鍵を用いて暗号化し、端末固有情報復元要求２４３を作成する。

[0157] ステップＳ７５３において、端末固有情報復元処理部２３２は、端末固有情報復元要求２４３をサーバ３０１に送信する。

ステップＳ７５４において、端末固有情報復元処理部２３２は、サーバ３０１からエラー応答を受信した場合、制御はステップＳ７５５に進み、エラ

一応答を受信しない場合、制御はステップＳ７５６に進む。

[0158] ステップＳ７５５において、端末固有情報復元処理部２３２は、エラーを応答する。

ステップＳ７５６において、端末固有情報復元処理部２３２は、サーバ３０１から暗号化端末固有情報２４０および暗号化期限情報２４１を受信する。

[0159] 次に、端末固有情報復元処理（端末側）時のサーバ側の処理（端末固有情報復元要求受信処理）について説明する。

図１８は、実施の形態に係るサーバの詳細な構成図である。

[0160] 図１８では、端末固有情報復元要求受信処理に関連する構成要素について記載され、それ以外の構成要素または説明済みの構成要素については省略されている。

端末固有情報復元部３３１は、ユーザ認証部３３２、ユーザ管理部３３３、端末固有情報管理部３３４、復元先端末証明書リスト処理部３３５、端末固有情報暗号化部３３６、および端末固有情報復元処理部３３７を備える。

[0161] ユーザ認証部３３２は、暗号化されたユーザ認証情報２４７や端末固有情報復元要求２４３等を復号する。

ユーザ管理部３３３は、ユーザ認証を行う。

[0162] 端末固有情報管理部３３４は、端末固有情報管理テーブル３７２および破棄済端末固有情報管理テーブル３７３へのデータの書き込み、削除等を行う。

復元先端末証明書リスト処理部３３５は、復元先端末証明書リスト内の端末固有公開鍵証明書３４１を抽出し、出力する。また復元先端末証明書リスト処理部３３５は、暗号された端末固有公開鍵証明書を復号し、端末固有公開鍵証明書３４２を出力する。

[0163] 端末固有情報暗号化部３３６は、端末固有情報３４４、期限情報３４５、サーバ公開鍵証明書３４６を暗号化し、暗号化端末固有情報２４０、暗号化期限情報２４１、暗号化サーバ公開鍵証明書３４７を出力する。

[0164] 端末固有情報復元処理部３３７は、端末固有情報復元処理（サーバ側）を行う。

図１９は、実施の形態に係る端末固有情報復元要求受信処理のフローチャートである。

ステップＳ８０１において、端末固有情報復元部３３１は、端末２０１から要求を受信する。

[0165] ステップＳ８０２において、端末固有情報復元部３３１は、要求がサーバ公開鍵証明書取得要求であるか否か判定する。要求がサーバ公開鍵証明書取得要求である場合、制御はステップＳ８０３に進み、サーバ公開鍵証明書取得要求でない場合、制御はステップＳ８０５に進む。

[0166] ステップＳ８０３において、端末固有情報暗号化部３３６は、サーバ公開鍵証明書３４６をサーバ公開鍵証明書取得要求で指定された端末固有公開鍵証明書の公開鍵で暗号化し、暗号化サーバ公開鍵証明書３４７を作成する。

[0167] ステップＳ８０４において、端末固有情報暗号化部３３６は、暗号化サーバ公開鍵証明書３４７を端末２０１に送信する。

ステップＳ８０５において、端末固有情報復元部３３１は、要求がワンタイムパスワード取得要求であるか否か判定する。要求がワンタイムパスワード取得要求である場合、制御はステップＳ８０６に進み、ワンタイムパスワード取得要求でない場合、制御はステップＳ８１１に進む。なお、要求がワンタイムパスワード取得要求でない場合、端末から受信した要求は、端末固有情報復元要求である。

[0168] ステップＳ８０６において、ユーザ認証部３３２は、ワンタイムパスワード要求に含まれる暗号化ユーザ認証情報をサーバ秘密鍵を用いて復号する。

ステップＳ８０７において、ユーザ管理部３３３は、ユーザ認証情報をチェックし、ユーザ認証を行う。ユーザ認証がエラーの場合、制御はステップＳ８０８に進み、ユーザ認証がエラーでない場合、制御はステップＳ８０９に進む。

[0169] ステップＳ８０８において、端末固有情報復元部３３１は、エラー応答を

端末２０１に送信する。

ステップＳ８０９において、端末固有情報復元部３３１は、ワンタイムパスワードを生成し、端末固有公開鍵証明書の公開鍵で暗号化し、暗号化ワンタイムパスワードを作成する。

[0170] ステップＳ８１０において、端末固有情報復元部３３１は、暗号化ワンタイムパスワードを端末２０１に送信する。

ステップＳ８１１において、ユーザ認証部３３２は、端末固有情報復元要求に含まれる暗号化ワンタイムパスワードをサーバ秘密鍵を用いて復号し、ワンタイムパスワードが期限切れであるかチェックする。また、ユーザ認証部３３２は、端末固有情報復元要求に含まれる暗号化された暗号化端末固有公開鍵証明書２９２および暗号化された暗号化復元先端末証明書リスト２９６をサーバ秘密鍵を用いて復号し、暗号化端末固有公開鍵証明書２９２および復元先端末証明書リスト２９６を取得する。尚、暗号化端末固有公開鍵証明書２９２および復元先端末証明書リスト２９６は、後述の端末固有情報復元処理（サーバ側）（ステップＳ８１４）で使用される。

[0171] ステップＳ８１２において、ワンタイムパスワードが期限切れである場合、制御はステップＳ８１３に進み、期限切れでない場合、制御はステップＳ８１４に進む。

ステップＳ８１３において、端末固有情報復元部３３１は、エラー応答を端末２０１に送信する。

[0172] ステップＳ８１４において、端末固有情報復元処理部３３７は、端末固有情報復元処理（サーバ側）を実行する。端末固有情報復元処理（サーバ側）の詳細については、後述する。

[0173] ステップＳ８１５において、端末固有情報復元処理においてエラーが応答された場合、制御はステップＳ８１３に進み、エラーが応答されなかった場合、制御はステップＳ８１６に進む。

[0174] ステップＳ８１６において、端末固有情報暗号化部３３６は、暗号化サーバ公開鍵証明書、暗号化端末固有情報、および暗号化期限情報を端末２０１

に送信する。

図２０は、実施の形態に係る端末固有情報復元処理（サーバ側）のフローチャートである。

[0175] 図２０のフローチャートは、図１９のステップＳ８１４に対応する。

ステップＳ８２１において、端末固有情報復元処理部３３７は、端末２０１から受信した暗号化端末固有公開鍵証明書を検索キーとして、端末固有情報管理テーブル３７２を検索する。

[0176] ステップＳ８２２において、検索キーに一致するレコードが端末固有情報管理テーブル３７２に存在する場合、制御はステップＳ８２３に進み、存在しない場合、制御はステップＳ８３０に進む。尚、検索により検出された検索キーに一致するレコードは、検出レコードと呼ぶ。

[0177] ステップＳ８２３において、端末固有情報復元処理部３３７は、端末２０１から受信した復元先端末証明書リスト２９６に含まれる端末固有公開鍵証明書のうち、最新エレメントである端末固有公開鍵証明書の公開鍵とサーバ秘密鍵からDiffie-Hellman(DH)方式により、共用鍵を生成する。そして、端末固有情報復元処理部３３７は、生成した共用鍵を端末証明書暗号化鍵とする。

[0178] ステップＳ８２４において、端末固有情報復元処理部３３７は、端末２０１から受信した復元先端末証明書リスト２９６に含まれる端末固有公開鍵証明書のうち、最新エレメントである端末固有公開鍵証明書をステップＳ８２３で生成した端末証明書暗号化鍵を用いて暗号化し、新しい暗号化端末固有公開鍵証明書を生成する。

[0179] ステップＳ８２５において、端末固有情報復元処理部３３７は、ステップＳ８２４で生成した新しい暗号化端末固有公開鍵証明書が破棄済端末固有情報管理テーブル３７３に登録されているかチェックする。

[0180] ステップＳ８２６において、新しい暗号化端末固有公開鍵証明書が破棄済端末固有情報管理テーブルに登録されている場合、制御はステップＳ８３７に進み、登録されていない場合、制御はステップＳ８２７に進む。

[0181] ステップＳ８２７において、端末固有情報復元処理部３３７は、検出レコードの暗号化端末固有公開鍵証明書を破棄済端末固有情報管理テーブル３７３に登録する。

ステップＳ８２８において、端末固有情報復元処理部３３７は、検出レコードの暗号化端末固有公開鍵証明書をステップＳ８２４で生成した新しい暗号化端末固有公開鍵証明書に更新する。さらに、端末固有情報復元処理部３３７は、検出したレコードの復元先端末証明書リストを端末２０１から受信した復元先端末証明書リスト２９６に更新する。

[0182] ステップＳ８２９において、端末固有情報暗号化部３３６は、サーバ公開鍵証明書３４６、ステップＳ８２８で更新したレコードの端末固有情報と期限情報を端末固有公開鍵証明書３４２の公開鍵を用いて暗号化し、暗号化サーバ公開鍵証明書３４７、暗号化端末固有情報２４０、および暗号化期限情報２４１を生成する。

[0183] ステップＳ８３０において、端末固有情報復元処理部３３７は、端末２０１から受信した復元先端末証明書リスト２９６に含まれる電子署名を復元先端末証明書リスト２９６の最新エレメントである端末固有公開鍵証明書により検証する。

[0184] ステップＳ８３１において、検証エラーの場合、制御はステップＳ８３７に進み、検証エラーで無い場合、制御はステップＳ８３２に進む。

ステップＳ８３２において、端末固有情報復元処理部３３７は、端末２０１から受信した復元先端末証明書リスト２９６の端末固有公開鍵証明書の最新エレメントを比較対象最終エレメントに設定する。復元先端末証明書リスト２９６の最新エレメントは、復元先端末証明書リスト２９６に含まれる端末固有公開鍵証明書の内、最後（最後尾）に記述された端末固有公開鍵証明書である。

[0185] ステップＳ８３３において、端末固有情報復元処理部３３７は、端末２０１から受信した復元先端末証明書リスト２９６の１番古い（先頭の）エレメントから比較対象最終エレメントまでの端末固有公開鍵証明書を検索キーと

して、端末固有情報管理テーブル３７２を検索する。そして、端末固有情報復元処理部３３７は、検索キーと一致する復元先端末証明書リストが記述されたレコードを検出する。

[0186] ステップＳ８３４において、検索キーに一致するレコードが端末固有情報管理テーブル３７２に存在する場合、制御はステップＳ８２３に進み、存在しない場合、制御はステップＳ８３５に進む。尚、検索により検出された検索キーに一致するレコードは、検出レコードと呼ぶ。

[0187] ステップＳ８３５において、端末固有情報復元処理部３３７は、現在の比較対象最終エレメントの一つ前の（古い）エレメントを新たな比較対象最終エレメントとして設定する。

[0188] ステップＳ８３６において、新たな比較対象最終エレメントが設定された場合、制御はステップＳ８３３に戻り、新たな比較対象最終エレメントが設定できなかった場合（すなわち、現在の比較対象最終エレメントが先頭のエレメントであった場合）、制御はステップＳ８３７に進む。

[0189] ステップＳ８３７において、端末固有情報復元処理部３３７は、エラーを応答する。

実施の形態のシステムによれば、蓄積データを利用可能な端末が不正に増加することを抑止できる。

[0190] 実施の形態のシステムによれば、端末固有ワーク鍵復元処理時に、端末固有ワーク鍵の復元中に端末が破損した場合でも、復元先端末証明書リストをチェックすることにより、更新元のデータと更新先の端末の組み合わせで、再度復元処理を行って良いか判断出来、不当に復元の権利が無くなるのを抑止できる。

[0191] 図２１は、情報処理装置（コンピュータ）の構成図である。

実施の形態の端末２０１およびサーバ３０１は、例えば、図２１に示すような情報処理装置１によって実現される。

[0192] 情報処理装置１は、CPU２、メモリ３、入力部４、出力部５、記憶部６、記録媒体駆動部７、およびネットワーク接続部８を備え、それらはバス９によ

り互いに接続されている。

[0193] CPU２は、情報処理装置１全体を制御する中央処理装置である。CPU２は、端末固有ワーク鍵生成部２１１、端末固有ワーク鍵復元部２３１、ＩＰ放送処理部２５１、蓄積データ復号部２７１、再生処理部２９９、端末固有情報配信部３１１、端末固有情報復元部３３１、ワーク鍵配信部３５１、および放送データ配信部３６１に対応する。

[0194] メモリ３は、プログラム実行の際に、記憶部６（あるいは可搬記録媒体１０）に記憶されているプログラムあるいはデータを一時的に格納するRead Only Memory(ROM)やRandom Access Memory(RAM)等のメモリである。CPU２は、メモリ３を利用してプログラムを実行することにより、上述した各種処理を実行する。

[0195] この場合、可搬記録媒体１０等から読み出されたプログラムコード自体が実施の形態の機能を実現する。

入力部４は、例えば、キーボード、マウス、タッチパネル等である。

[0196] 出力部５は、例えば、ディスプレイ、プリンタ等である。

記憶部６は、例えば、磁気ディスク装置、光ディスク装置、テープ装置等である。情報処理装置１は、記憶部６に、上述のプログラムとデータを保存しておき、必要に応じて、それらをメモリ３に読み出して使用する。

[0197] メモリ３または記憶部６は、不揮発記憶域２８１、記憶部２９１、３７１に対応する。

記録媒体駆動部７は、可搬記録媒体１０を駆動し、その記録内容にアクセスする。可搬記録媒体としては、メモリカード、フレキシブルディスク、Compact Disk Read Only Memory(CD-ROM)、光ディスク、光磁気ディスク等、任意のコンピュータ読み取り可能な記録媒体が用いられる。ユーザは、この可搬記録媒体１０に上述のプログラムとデータを格納しておき、必要に応じて、それらをメモリ３に読み出して使用する。

[0198] ネットワーク接続部８は、LAN等の任意の通信ネットワークに接続され、通信に伴うデータ変換を行う。

請求の範囲

[請求項1] データの暗号化および復号に用いられるスクランブル鍵の暗号化および復号に用いられる端末固有ワーク鍵の生成に用いられる端末固有情報の送信方法であって、

サーバは、

端末から、前記端末の端末固有公開鍵証明書を含む端末固有情報取得要求を受信し、

前記端末の端末固有公開鍵証明書を暗号化して、暗号化端末固有公開鍵証明書を生成し、

前記端末固有情報の取得を許可しない端末の暗号化端末固有公開鍵証明書が記述された破棄済み端末情報テーブルを参照し、

生成された暗号化端末固有公開鍵証明書が前記破棄済み端末情報テーブルに記述されているか否かチェックし、

記述されていない場合、前記端末の前記端末固有情報を前記端末に送信する、

ことを特徴とする送信方法。

[請求項2] 前記端末固有情報の送信処理において、

暗号化端末固有公開鍵証明書と端末固有情報が対応付けられて記述された端末固有情報テーブルを参照し、

前記端末固有情報テーブルに前記生成された暗号化端末固有公開鍵証明書に対応付けられた前記端末固有情報が記述されているか否かチェックし、

記述されている場合、前記生成された暗号化端末固有公開鍵証明書に対応付けられた前記端末固有情報を送信し、

記述されていない場合、前記端末の端末固有公開鍵証明書を用いて、前記端末固有情報を生成し、前記端末固有情報を送信することを特徴とする請求項１記載の送信方法。

[請求項3] 前記サーバは、さらに

前記端末から、他の端末の端末固有公開鍵証明書を暗号化した他の暗号化端末固有公開鍵証明書、および最新エレメントとして少なくとも前記端末の端末固有公開鍵証明書が記述された復元先端末証明書リストを含む端末固有情報更新要求を受信し、

前記端末固有情報テーブルに前記他の暗号化端末固有公開鍵証明書が記述されているか否かチェックし、

記述されている場合、前記他の暗号化端末固有公開鍵証明書に対応付けられた前記端末固有情報を前記端末に送信し、前記他の暗号化端末固有公開鍵証明書を前記破棄済み端末情報テーブルに記述する、

ことを特徴とする請求項１または２記載の送信方法。

［請求項4］ 前記端末固有情報テーブルには、端末固有公開鍵証明書が記述された他の復元先端末証明書リストが暗号化端末固有公開鍵証明書および端末固有情報と対応付けられてさらに記述され、

前記端末固有情報テーブルに前記他の暗号化端末固有公開鍵証明書が記述されていない場合、

前記端末固有情報更新要求に含まれる復元先端末証明書リストの先頭エレメントからいずれかのエレメントまでを検索キーとして、前記端末固有情報テーブルを検索し、

前記検索キーと一致する前記他の復元先端末証明書リストを有するレコードを検出した場合、検出したレコードの端末固有情報を前記端末に送信し、

前記検出したレコードの暗号化端末固有公開鍵証明書を前記破棄済み端末情報テーブルに記述する、

ことを特徴とする請求項３記載の送信方法。

［請求項5］ データの暗号化に用いられるスクランブル鍵の暗号化に用いられる端末固有ワーク鍵の生成に用いられる端末固有情報の送受信を行うシステムであって、

前記システムは、端末とサーバを備え、

前記端末は、

前記データを暗号化するデータ処理部と、

暗号化された前記データを格納する第１の記憶部と、

前記データの暗号化時に、前記サーバに前記端末の端末固有公開鍵証明書を含む端末固有情報取得要求を送信し、前記サーバから受信した端末固有情報を用いて、前記端末固有ワーク鍵を生成する端末固有ワーク鍵生成部と、

を備え、

前記サーバは、

前記端末固有情報の取得を許可しない端末の暗号化端末固有公開鍵証明書が記述された破棄済み端末情報テーブルを格納する第２の記憶部と、

前記端末固有情報取得要求を受信し、前記端末の端末固有公開鍵証明書を暗号化して、暗号化端末固有公開鍵証明書を生成し、生成された暗号化端末固有公開鍵証明書が前記破棄済み端末情報テーブルに記述されているか否かチェックし、記述されていない場合、前記端末の前記端末固有情報を前記端末に送信する端末固有情報送信部と、

を備えることを特徴とするシステム。

［請求項6］ 前記端末固有ワーク鍵生成部は、暗号化された前記データの復号時に、前記端末固有ワーク鍵の期限をチェックし、期限切れの場合、前記端末固有情報取得要求を送信することを特徴とする請求項５記載のシステム。

［請求項7］ 前記第２の記憶部は、暗号化端末固有公開鍵証明書と端末固有情報が対応付けられて記述された端末固有情報テーブルを格納し、

端末固有情報送信部は、

前記端末固有情報テーブルを参照し、

前記端末固有情報テーブルに前記端末固有情報取得要求の前記暗号化端末固有公開鍵証明書に対応付けられた前記端末固有情報が記述

されているか否かチェックし、

記述されている場合、前記生成された暗号化端末固有公開鍵証明書に対応付けられた前記端末固有情報を送信し、

記述されていない場合、前記端末の端末固有公開鍵証明書を用いて、前記端末固有情報を生成し、前記端末固有情報を送信することを特徴とする請求項５または６記載システム。

［請求項8］ 第１の記憶部は、他の端末の端末固有公開鍵証明書を暗号化した他の暗号化端末固有公開鍵証明書および端末固有公開鍵証明書が記述された復元先端末証明書リストを格納し、

前記端末は、

前記他の暗号化端末固有公開鍵証明書および最新エレメントとして前記端末の端末固有公開鍵証明書が記述された復元先端末証明書リストを含む端末固有情報更新要求を送信し、前記サーバから受信した端末固有情報を用いて新たな端末固有ワーク鍵を生成し、前記新たな端末固有ワーク鍵を暗号化し、前記第１の記憶部に格納されている暗号化された前記端末固有ワーク鍵を暗号化された前記新たな端末固有ワーク鍵で更新する端末固有ワーク鍵更新部、

をさらに備え、

前記サーバは、

前記端末固有情報更新要求を受信し、前記端末固有情報テーブルに前記他の暗号化端末固有公開鍵証明書が記述されているか否かチェックし、記述されている場合、前記他の暗号化端末固有公開鍵証明書に対応付けられた前記端末固有情報を前記端末に送信する端末固有情報更新部、

をさらに備えることを特徴とする請求項５乃至７のいずれか１項に記載のシステム。

［請求項9］ 前記端末固有ワーク鍵更新部は、

前記第１の記憶部に格納された前記復元先端末証明書リストに前記

端末の端末固有公開鍵証明書が記述されているかチェックし、

記述されていない場合、前記端末の端末固有公開鍵証明書を最新エレメントとして前記復元先端末証明書リストに付加し、前記他の暗号化端末固有公開鍵証明書および最新エレメントとして前記端末の端末固有公開鍵証明書が付加された復元先端末証明書リストを含む前記端末固有情報更新要求を送信し、

記述されている場合、前記復元先端末証明書リストの最新エレメントが前記端末の端末固有公開鍵証明書と一致するかチェックし、一致する場合、前記他の暗号化端末固有公開鍵証明書および前記復元先端末証明書リストを含む前記端末固有情報更新要求を送信する、

ことを特徴とする請求項８記載のシステム。

［請求項10］ 前記端末固有情報テーブルには、端末固有公開鍵証明書が記述された他の復元先端末証明書リストが暗号化端末固有公開鍵証明書および端末固有情報と対応付けられてさらに記述され、

前記端末固有情報更新部は、

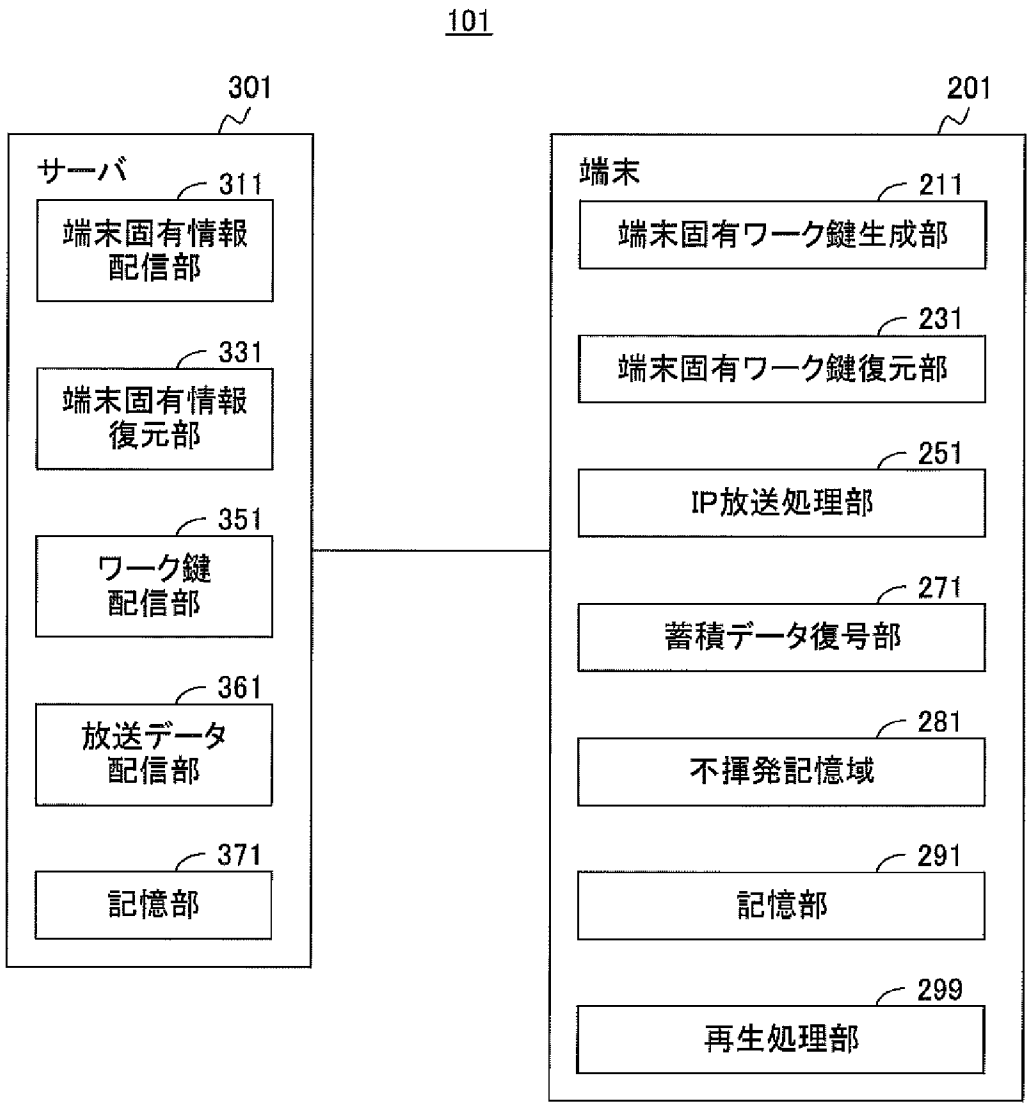
前記端末固有情報テーブルに前記他の暗号化端末固有公開鍵証明書が記述されていない場合、

前記端末固有情報更新要求に含まれる復元先端末証明書リストの先頭エレメントからいずれかのエレメントまでを検索キーとして、前記端末固有情報テーブルを検索し、

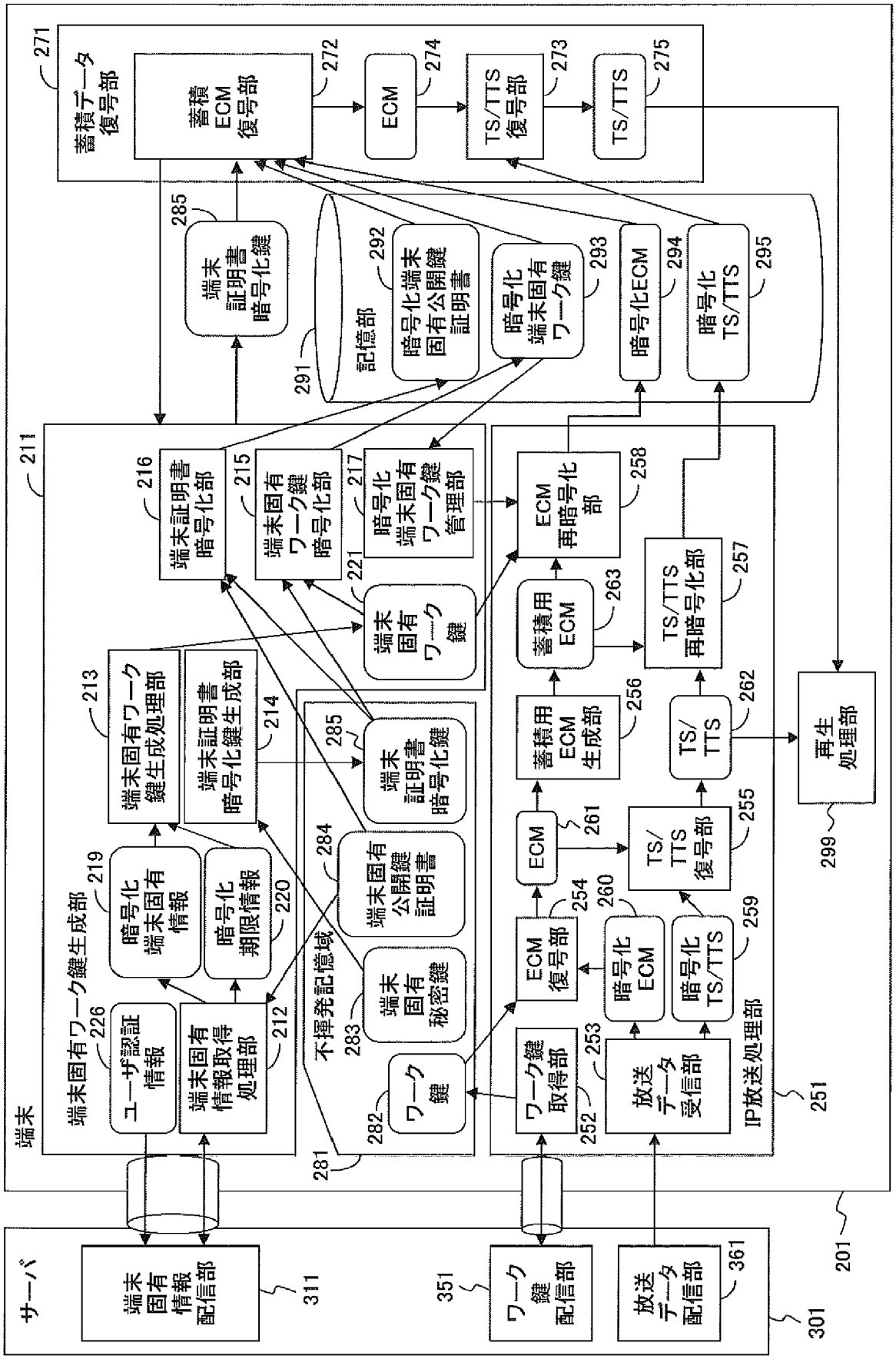
前記検索キーと一致する前記他の復元先端末証明書リストを有するレコードを検出した場合、検出したレコードの端末固有情報を前記端末に送信する、

ことを特徴とする請求項８または９記載のシステム。

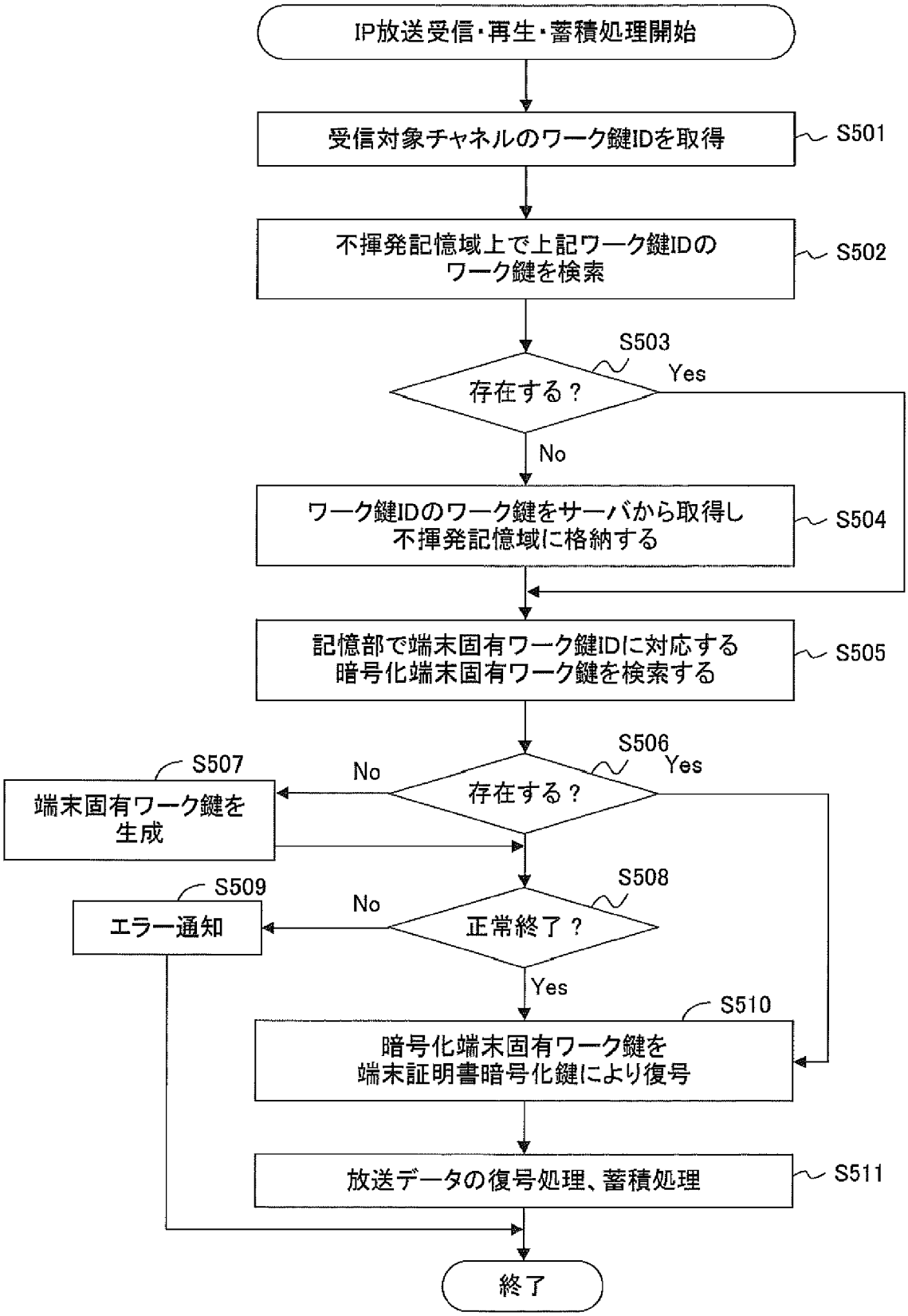
[図1]


101
301
サーバ
311
端末固有情報
配信部
331
端末固有情報
復元部
351
ワーク鍵
配信部
361
放送データ
配信部
371
記憶部
201
端末
211
端末固有ワーク鍵生成部
231
端末固有ワーク鍵復元部
251
IP放送処理部
271
蓄積データ復号部
281
不揮発記憶域
291
記憶部
299
再生処理部

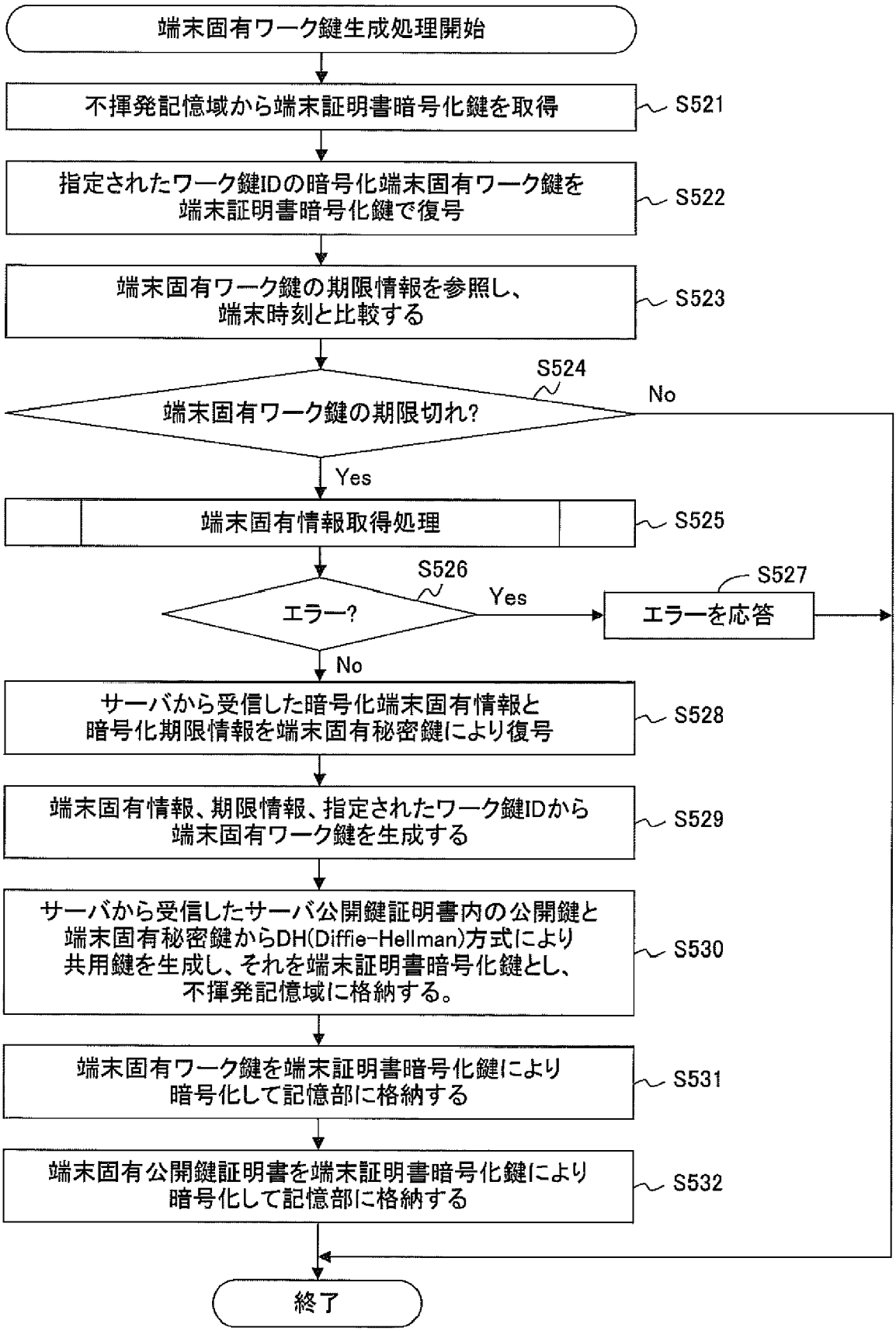
[図2]


サーバ
端末固有情報配信部
311
ワーク鍵配信部
351
放送データ配信部
361
301
201
端末
端末固有ワーク鍵生成部
ユーザ認証情報
226
端末固有情報取得処理部
212
暗号化端末固有情報
219
暗号化期限情報
220
端末固有ワーク鍵生成処理部
213
端末証明書暗号化鍵生成部
214
端末証明書暗号化部
216
端末固有ワーク鍵暗号化部
215
暗号化端末固有ワーク鍵管理部
217
端末固有ワーク鍵
221
端末証明書暗号化鍵
285
端末固有秘密鍵
283
端末固有公開鍵証明書
284
ワーク鍵
282
不揮発記憶領域
281
ワーク鍵取得部
252
253
ECM復号部
254
暗号化ECM
260
暗号化TS/TTS
259
放送データ受信部
IP放送処理部
251
ECM
261
TS/TTS復号部
255
蓄積用ECM生成部
256
蓄積用ECM
263
ECM再暗号化部
258
TS/TTS再暗号化部
257
TS/TTS
262
再生処理部
299
蓄積データ復号部
271
蓄積ECM復号部
272
ECM
274
TS/TTS復号部
273
TS/TTS
275
端末証明書暗号化鍵
285
記憶部
291
暗号化端末固有公開鍵証明書
292
暗号化端末固有ワーク鍵
293
暗号化ECM
294
暗号化TS/TTS
295

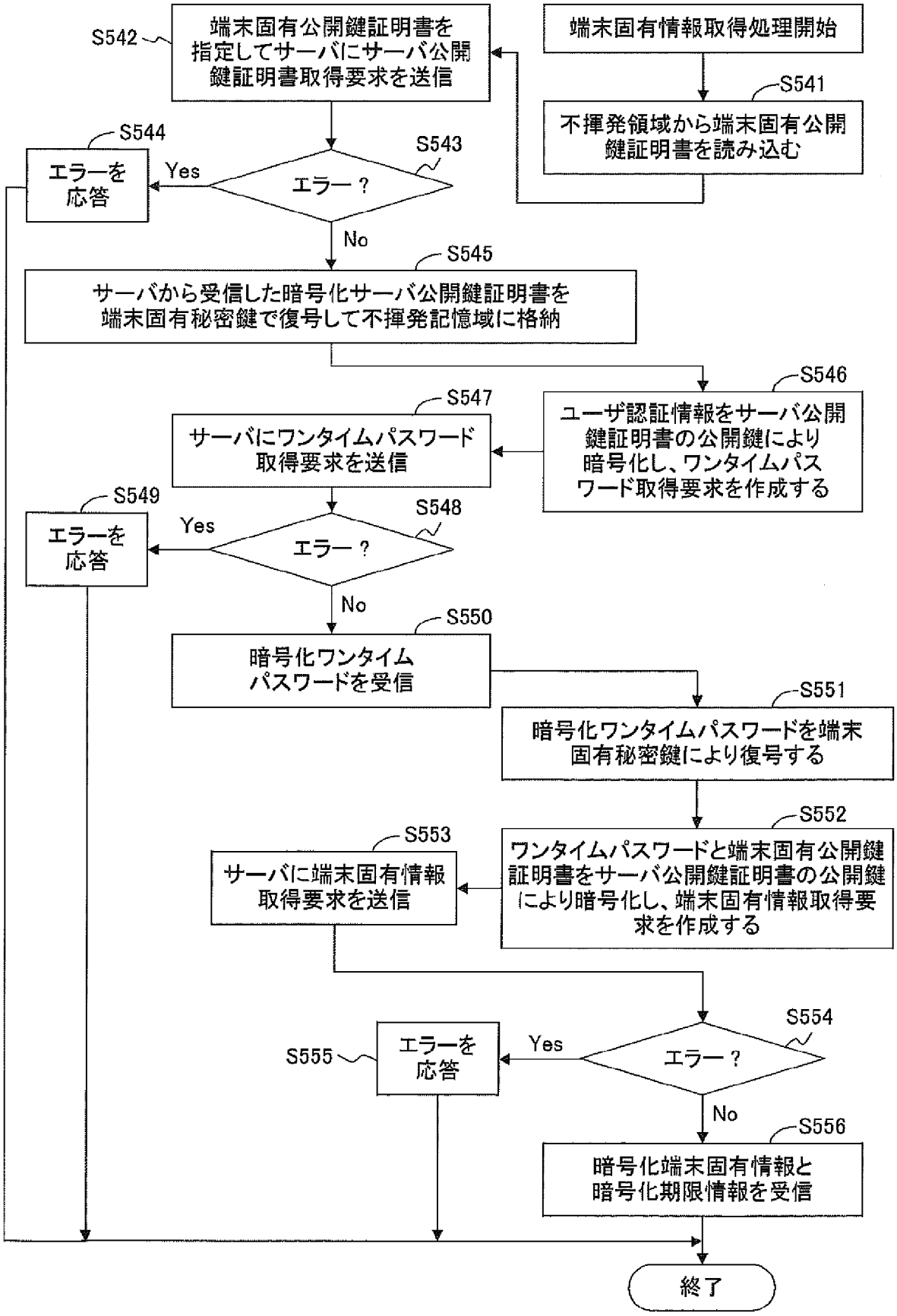
[図3]


IP放送受信・再生・蓄積処理開始
受信対象チャネルのワーク鍵IDを取得
S501
不揮発記憶域上で上記ワーク鍵IDの
ワーク鍵を検索
S502
S503
存在する？
Yes
No
ワーク鍵IDのワーク鍵をサーバから取得し
不揮発記憶域に格納する
S504
記憶部で端末固有ワーク鍵IDに対応する
暗号化端末固有ワーク鍵を検索する
S505
S506
存在する？
Yes
No
S507
端末固有ワーク鍵を
生成
S508
正常終了？
No
S509
エラー通知
Yes
S510
暗号化端末固有ワーク鍵を
端末証明書暗号化鍵により復号
放送データの復号処理、蓄積処理
S511
終了

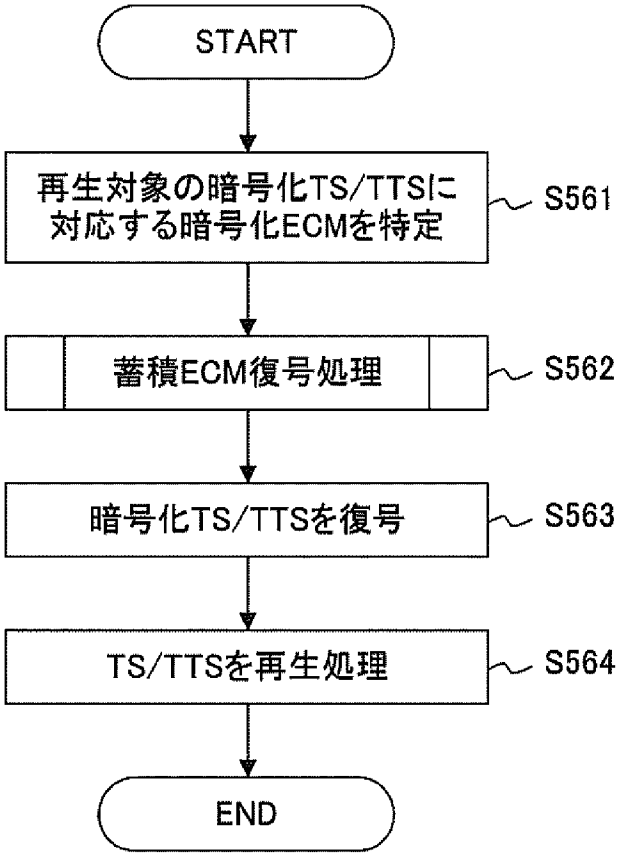
[図4]


端末固有ワーク鍵生成処理開始
不揮発記憶域から端末証明書暗号化鍵を取得
S521
指定されたワーク鍵IDの暗号化端末固有ワーク鍵を
端末証明書暗号化鍵で復号
S522
端末固有ワーク鍵の期限情報を参照し、
端末時刻と比較する
S523
S524
端末固有ワーク鍵の期限切れ?
No
Yes
端末固有情報取得処理
S525
S526
エラー?
Yes
S527
エラーを応答
No
サーバから受信した暗号化端末固有情報と
暗号化期限情報を端末固有秘密鍵により復号
S528
端末固有情報、期限情報、指定されたワーク鍵IDから
端末固有ワーク鍵を生成する
S529
サーバから受信したサーバ公開鍵証明書内の公開鍵と
端末固有秘密鍵からDH(Diffie-Hellman)方式により
共用鍵を生成し、それを端末証明書暗号化鍵とし、
不揮発記憶域に格納する。
S530
端末固有ワーク鍵を端末証明書暗号化鍵により
暗号化して記憶部に格納する
S531
端末固有公開鍵証明書を端末証明書暗号化鍵により
暗号化して記憶部に格納する
S532
終了

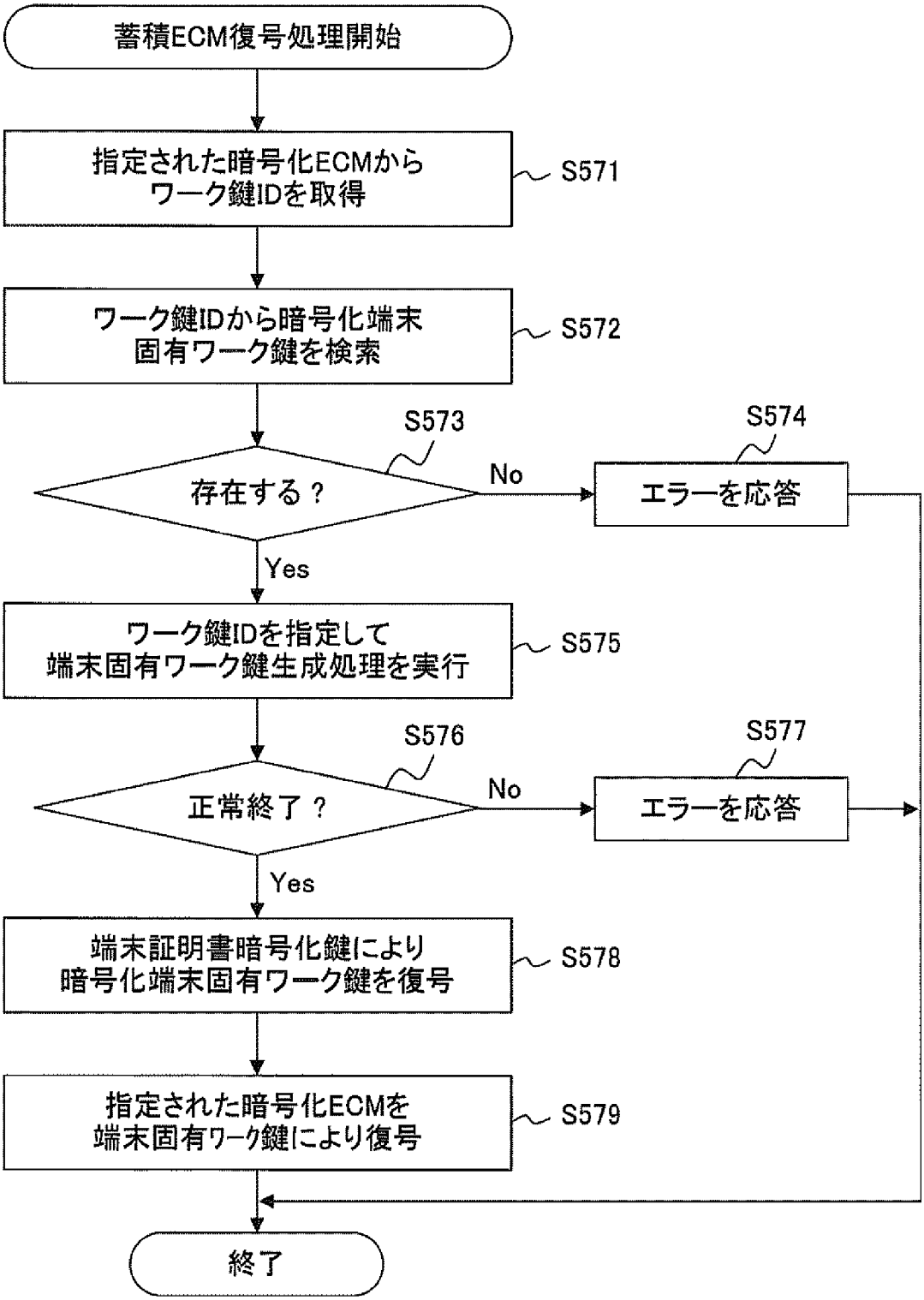
[図5]


端末固有情報取得処理開始
S541
不揮発領域から端末固有公開鍵証明書を読み込む
S542
端末固有公開鍵証明書を指定してサーバにサーバ公開鍵証明書取得要求を送信
S543
エラー？
Yes
S544
エラーを応答
No
S545
サーバから受信した暗号化サーバ公開鍵証明書を端末固有秘密鍵で復号して不揮発記憶域に格納
S546
ユーザ認証情報をサーバ公開鍵証明書の公開鍵により暗号化し、ワンタイムパスワード取得要求を作成する
S547
サーバにワンタイムパスワード取得要求を送信
S548
エラー？
Yes
S549
エラーを応答
No
S550
暗号化ワンタイムパスワードを受信
S551
暗号化ワンタイムパスワードを端末固有秘密鍵により復号する
S552
ワンタイムパスワードと端末固有公開鍵証明書をサーバ公開鍵証明書の公開鍵により暗号化し、端末固有情報取得要求を作成する
S553
サーバに端末固有情報取得要求を送信
S554
エラー？
Yes
S555
エラーを応答
No
S556
暗号化端末固有情報と暗号化期限情報を受信
終了

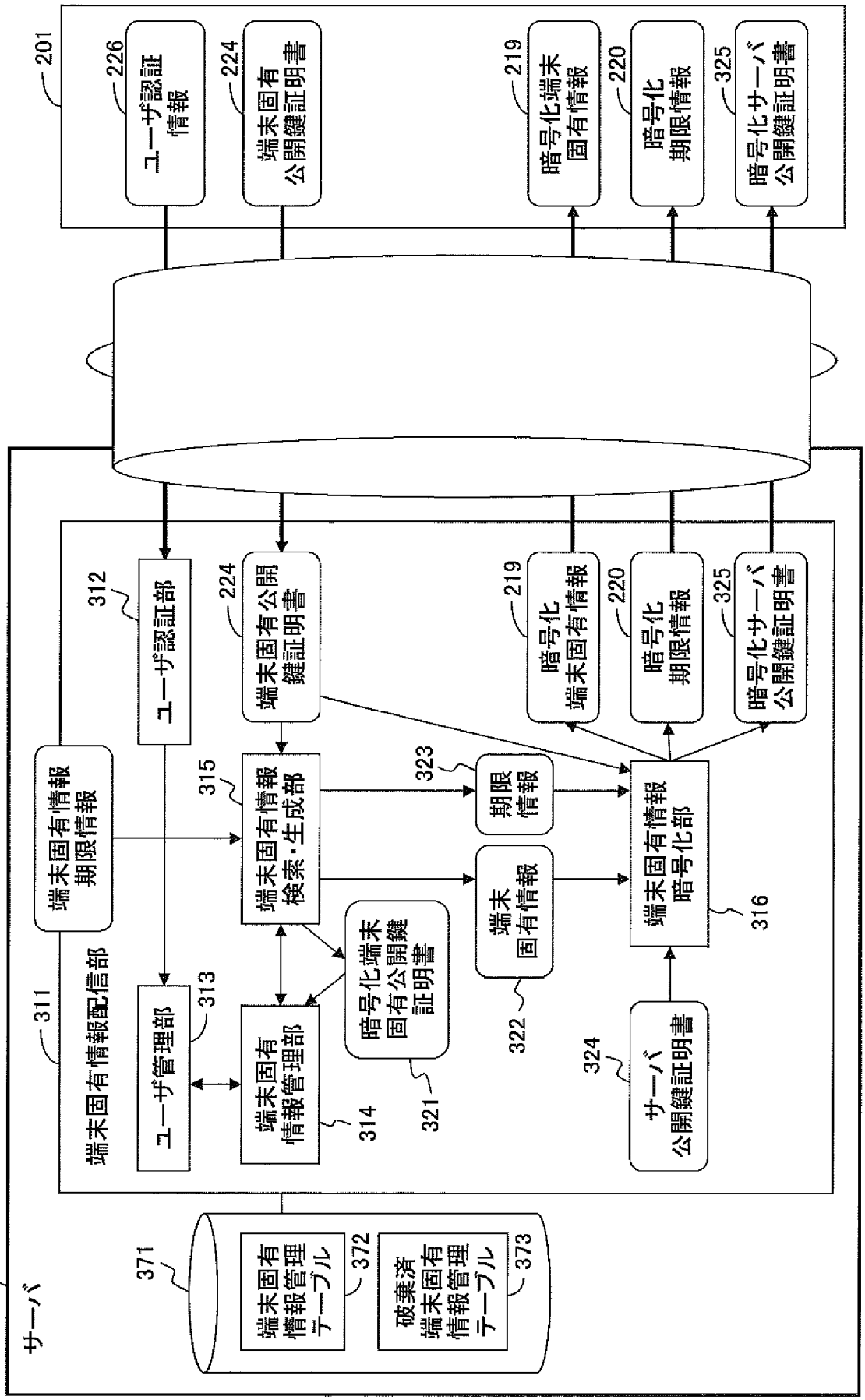
[図6]


START
再生対象の暗号化TS/TTSに対応する暗号化ECMを特定
S561
蓄積ECM復号処理
S562
暗号化TS/TTSを復号
S563
TS/TTSを再生処理
S564
END

[図7]


蓄積ECM復号処理開始
指定された暗号化ECMから
ワーク鍵IDを取得
S571
ワーク鍵IDから暗号化端末
固有ワーク鍵を検索
S572
S573
存在する？
No
S574
エラーを応答
Yes
ワーク鍵IDを指定して
端末固有ワーク鍵生成処理を実行
S575
S576
正常終了？
No
S577
エラーを応答
Yes
端末証明書暗号化鍵により
暗号化端末固有ワーク鍵を復号
S578
指定された暗号化ECMを
端末固有ワーク鍵により復号
S579
終了

[図8]


201
226
ユーザ認証情報
224
端末固有公開鍵証明書
219
暗号化端末固有情報
220
暗号化期限情報
325
暗号化サーバ公開鍵証明書
301
サーバ
311
端末固有情報配信部
312
ユーザ認証部
313
ユーザ管理部
314
端末固有情報管理部
315
端末固有情報検索・生成部
316
端末固有情報暗号化部
321
暗号化端末固有公開鍵証明書
322
端末固有情報
323
期限情報
324
サーバ公開鍵証明書
371
372
端末固有情報管理テーブル
373
破棄済端末固有情報管理テーブル
端末固有情報期限情報

[図9]

372

暗号化端末固有公開鍵証明書	復元先端末証明書リスト	端末固有情報	期限情報	
			開始時刻	終了時刻
xxxxxxxxxxxxxxxxxxx	xxxxxxxxxxxxxxxxxx	xxxxxxxxxxxxxxxxxx	YYYYMMDD:hhmmss	YYYYMMDD:hhmmss

[図10]

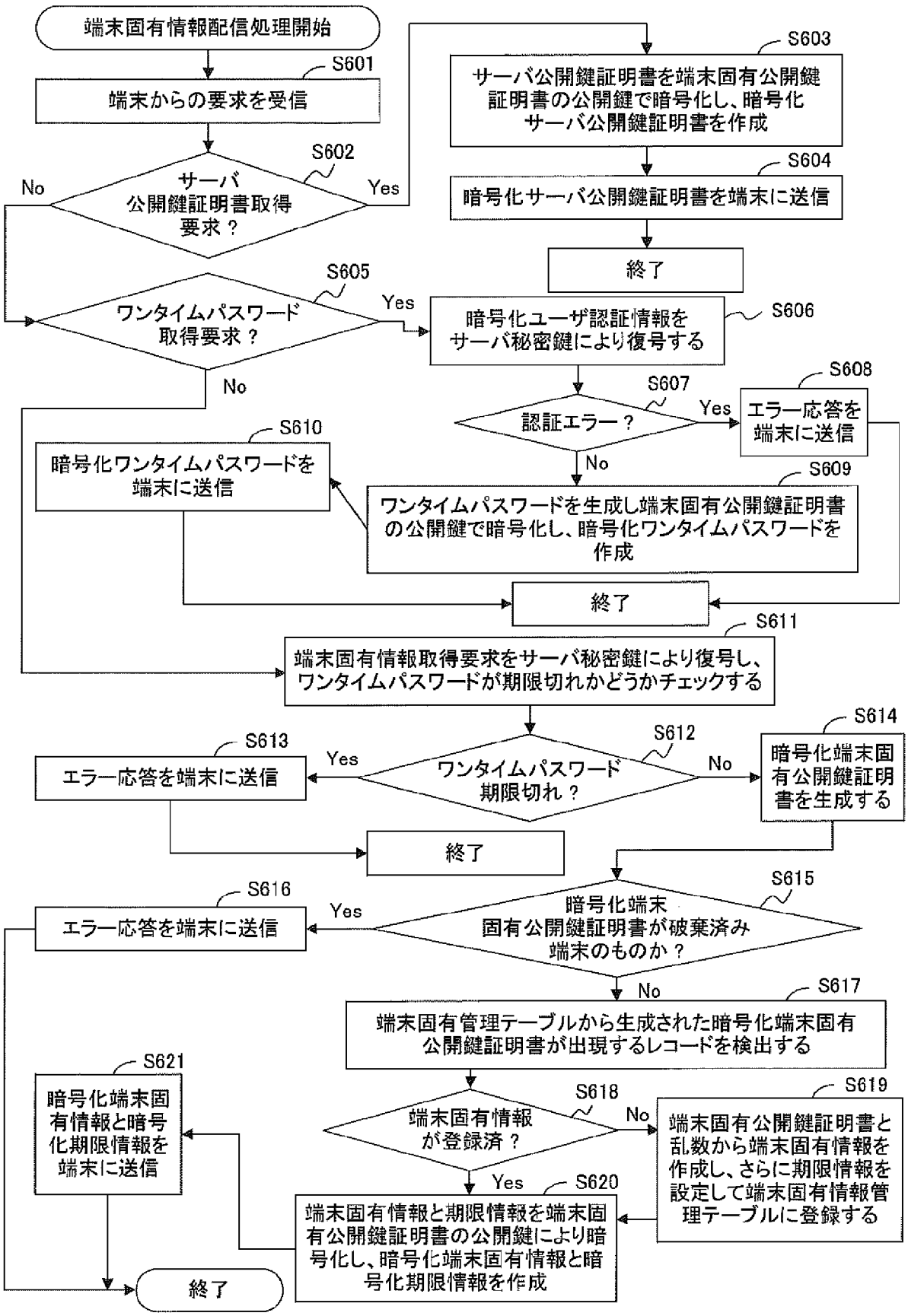
端末Aの端末固有公開鍵証明書	端末Bの端末固有公開鍵証明書	電子署名（端末Bの端末固有秘密鍵で署名）

[図11]

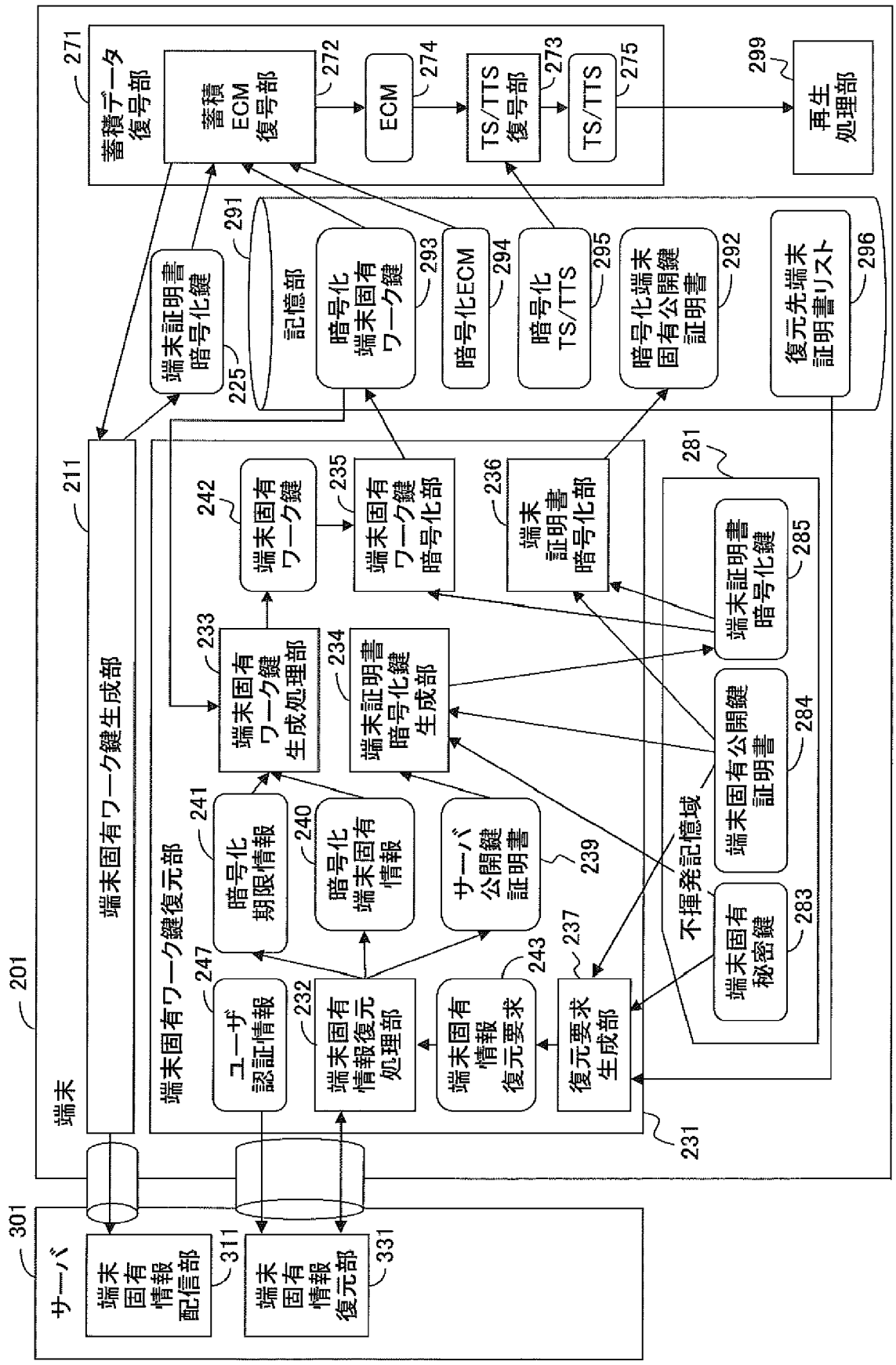
373

暗号化端末固有公開鍵証明書
xxxxxxxxxxxxxxxxxx

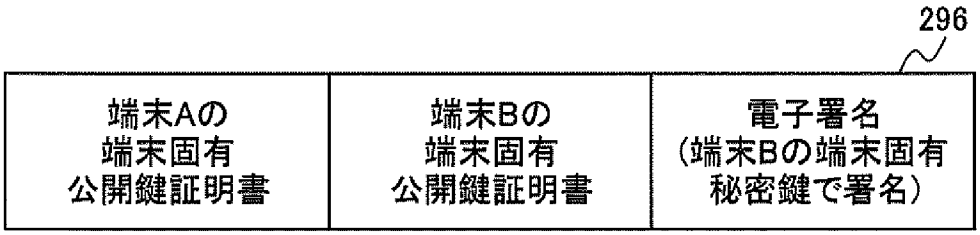
[図12]


端末固有情報配信処理開始
S601
端末からの要求を受信
S602
サーバ公開鍵証明書取得要求？
No
Yes
S603
サーバ公開鍵証明書を端末固有公開鍵証明書の公開鍵で暗号化し、暗号化サーバ公開鍵証明書を作成
S604
暗号化サーバ公開鍵証明書を端末に送信
終了
S605
ワンタイムパスワード取得要求？
Yes
No
S606
暗号化ユーザ認証情報をサーバ秘密鍵により復号する
S607
認証エラー？
Yes
No
S608
エラー応答を端末に送信
S609
ワンタイムパスワードを生成し端末固有公開鍵証明書の公開鍵で暗号化し、暗号化ワンタイムパスワードを作成
S610
暗号化ワンタイムパスワードを端末に送信
終了
S611
端末固有情報取得要求をサーバ秘密鍵により復号し、ワンタイムパスワードが期限切れかどうかチェックする
S612
ワンタイムパスワード期限切れ？
Yes
No
S613
エラー応答を端末に送信
終了
S614
暗号化端末固有公開鍵証明書を生成する
S615
暗号化端末固有公開鍵証明書が破棄済み端末のものか？
Yes
No
S616
エラー応答を端末に送信
S617
端末固有管理テーブルから生成された暗号化端末固有公開鍵証明書が出現するレコードを検出する
S618
端末固有情報が登録済？
No
Yes
S619
端末固有公開鍵証明書と乱数から端末固有情報を作成し、さらに期限情報を設定して端末固有情報管理テーブルに登録する
S620
端末固有情報と期限情報を端末固有公開鍵証明書の公開鍵により暗号化し、暗号化端末固有情報と暗号化期限情報を作成
S621
暗号化端末固有情報と暗号化期限情報を端末に送信
終了

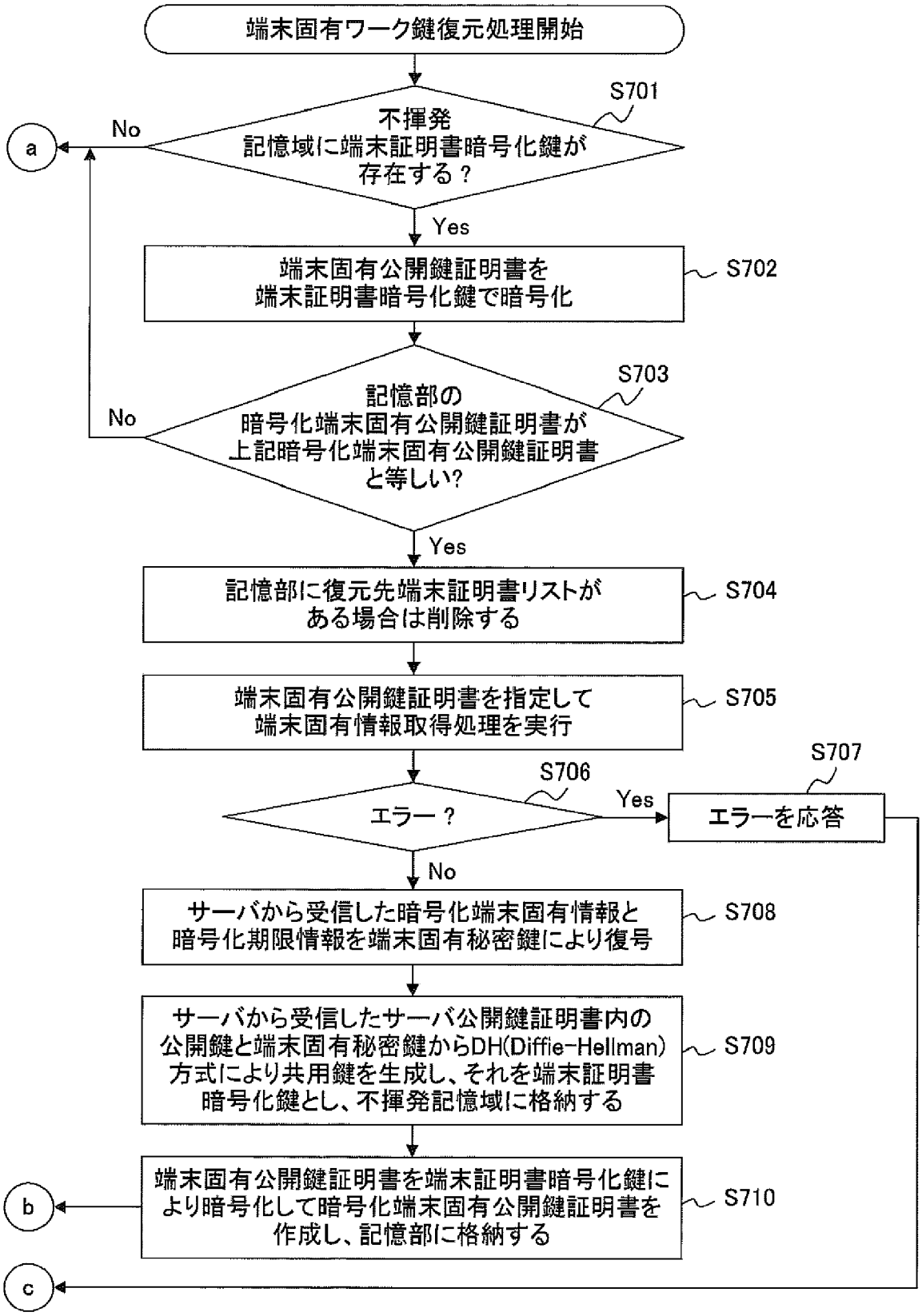
[図13]


201
端末
211
端末固有ワーク鍵生成部
271
蓄積データ復号部
272
蓄積ECM復号部
274
ECM
273
TS/TTS復号部
275
TS/TTS
299
再生処理部
291
記憶部
225
端末証明書暗号化鍵
293
暗号化端末固有ワーク鍵
294
暗号化ECM
295
暗号化TS/TTS
292
暗号化端末固有公開鍵証明書
296
復元先端末証明書リスト
端末固有ワーク鍵復元部
242
端末固有ワーク鍵
235
端末固有ワーク鍵暗号化部
236
端末証明書暗号化部
233
端末固有ワーク鍵生成処理部
234
端末証明書暗号化鍵生成部
241
暗号化期限情報
240
暗号化端末固有情報
239
サーバ公開鍵証明書
247
ユーザ認証情報
232
端末固有情報復元処理部
243
端末固有情報復元要求
237
復元要求生成部
231
281
不揮発記憶域
285
端末証明書暗号化鍵
284
端末固有公開鍵証明書
283
端末固有秘密鍵
301
サーバ
311
端末固有情報配信部
331
端末固有情報復元部

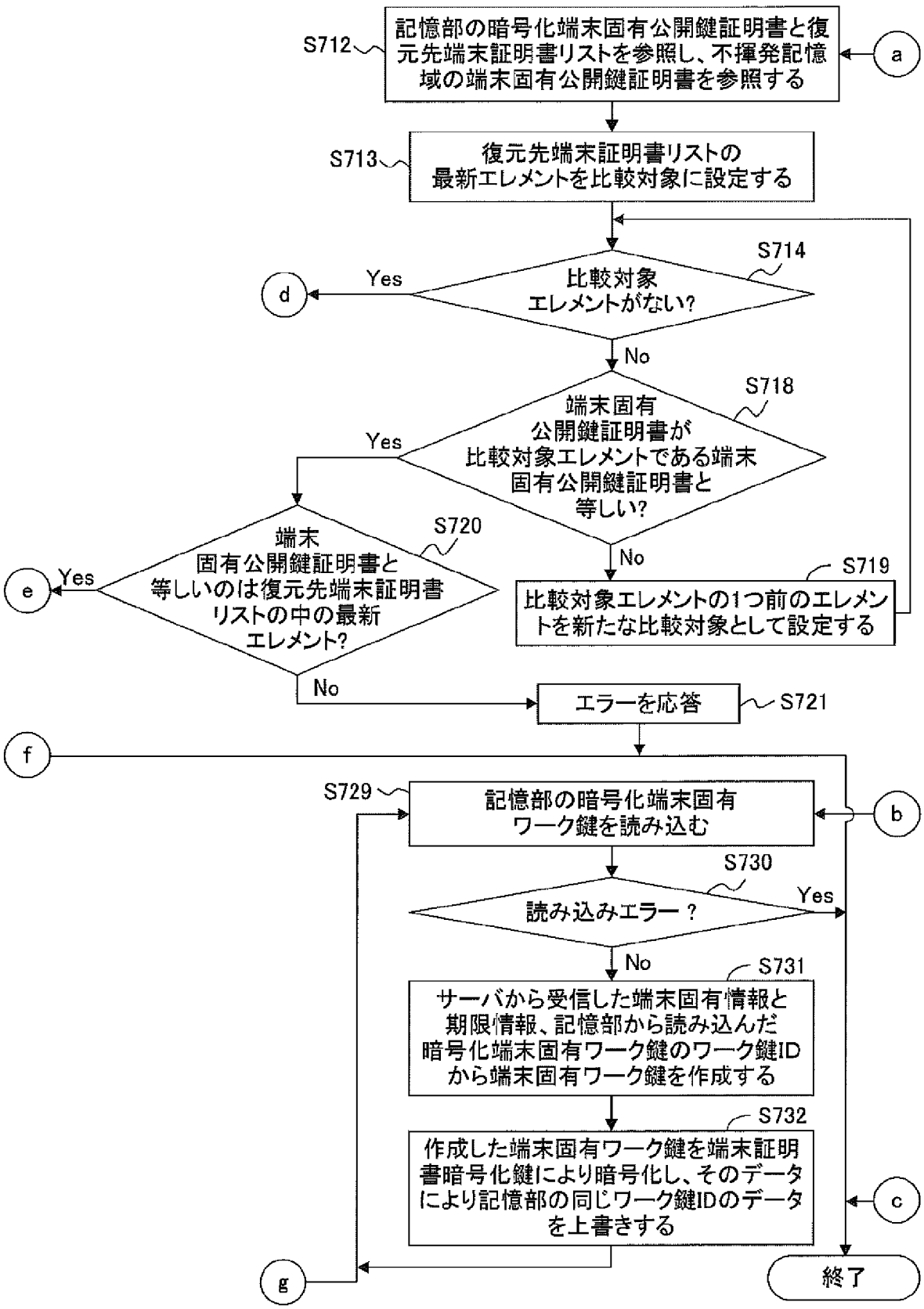
[図14]



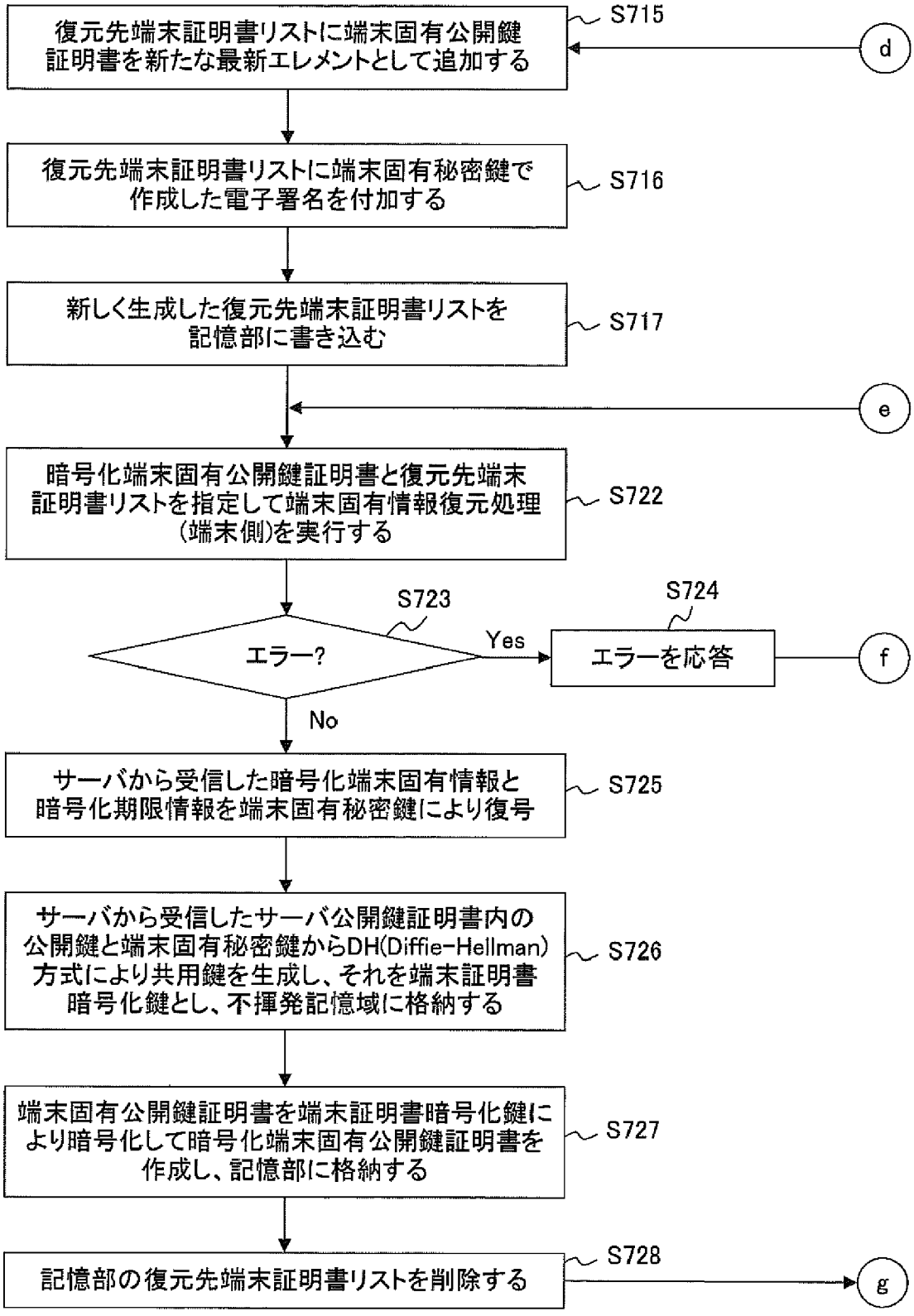
[図15A]


端末固有ワーク鍵復元処理開始
S701
不揮発
記憶域に端末証明書暗号化鍵が
存在する？
No
a
Yes
端末固有公開鍵証明書を
端末証明書暗号化鍵で暗号化
S702
S703
記憶部の
暗号化端末固有公開鍵証明書が
上記暗号化端末固有公開鍵証明書
と等しい?
No
Yes
記憶部に復元先端末証明書リストが
ある場合は削除する
S704
端末固有公開鍵証明書を指定して
端末固有情報取得処理を実行
S705
S706
エラー？
Yes
S707
エラーを応答
No
サーバから受信した暗号化端末固有情報と
暗号化期限情報を端末固有秘密鍵により復号
S708
サーバから受信したサーバ公開鍵証明書内の
公開鍵と端末固有秘密鍵からDH(Diffie-Hellman)
方式により共用鍵を生成し、それを端末証明書
暗号化鍵とし、不揮発記憶域に格納する
S709
端末固有公開鍵証明書を端末証明書暗号化鍵に
より暗号化して暗号化端末固有公開鍵証明書を
作成し、記憶部に格納する
S710
b
c

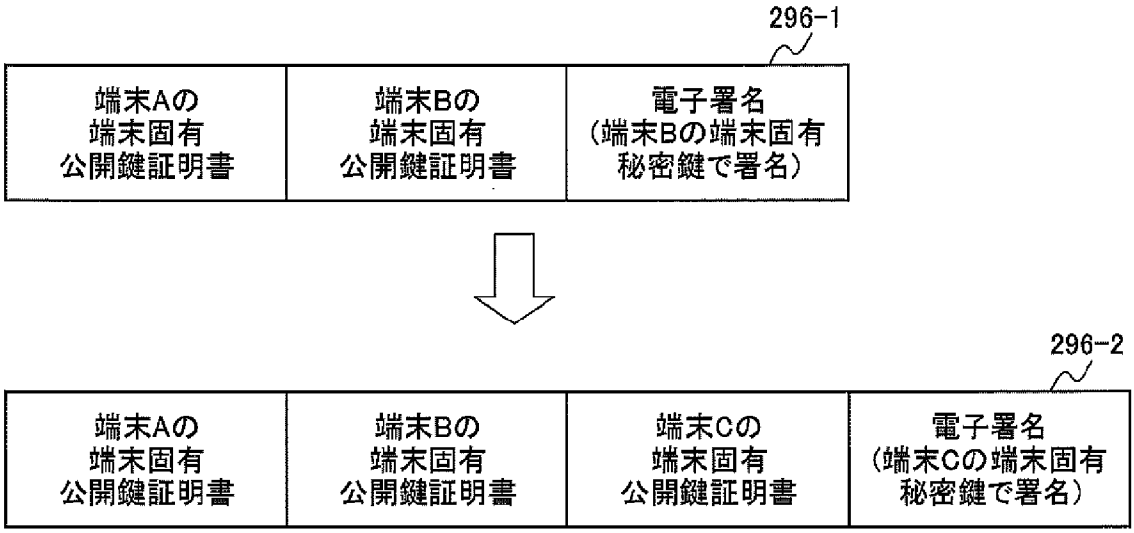
[図15B]


S712
記憶部の暗号化端末固有公開鍵証明書と復元先端末証明書リストを参照し、不揮発記憶域の端末固有公開鍵証明書を参照する
a
S713
復元先端末証明書リストの最新エレメントを比較対象に設定する
S714
比較対象エレメントがない?
Yes
d
No
S718
端末固有公開鍵証明書が比較対象エレメントである端末固有公開鍵証明書と等しい?
Yes
No
S720
端末固有公開鍵証明書と等しいのは復元先端末証明書リストの中の最新エレメント?
Yes
e
No
S719
比較対象エレメントの1つ前のエレメントを新たな比較対象として設定する
エラーを応答
S721
f
S729
記憶部の暗号化端末固有ワーク鍵を読み込む
b
S730
読み込みエラー ?
Yes
No
S731
サーバから受信した端末固有情報と期限情報、記憶部から読み込んだ暗号化端末固有ワーク鍵のワーク鍵IDから端末固有ワーク鍵を作成する
S732
作成した端末固有ワーク鍵を端末証明書暗号化鍵により暗号化し、そのデータにより記憶部の同じワーク鍵IDのデータを上書きする
c
g
終了

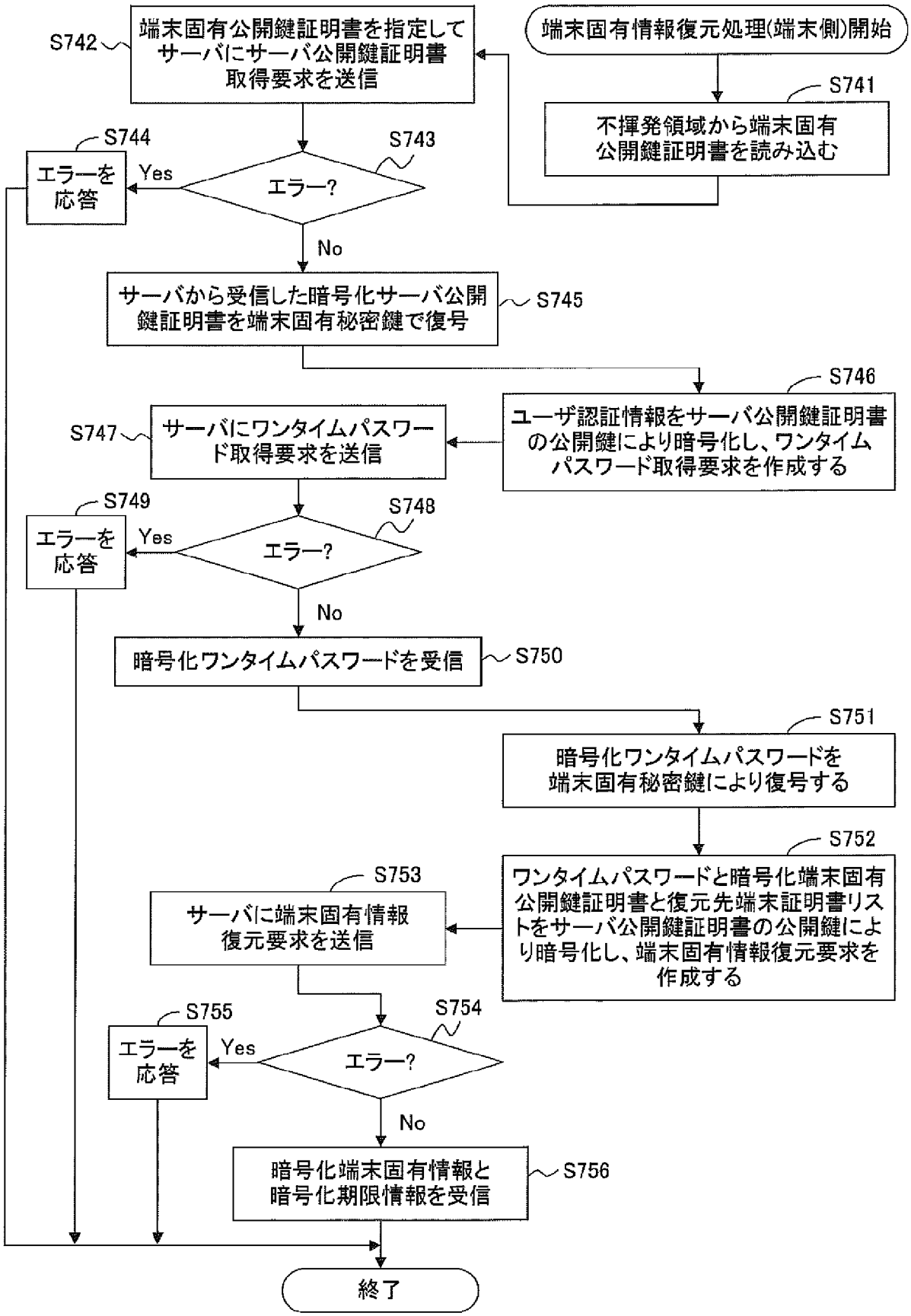
[図15C]


復元先端末証明書リストに端末固有公開鍵証明書を新たな最新エレメントとして追加する
S715
d
復元先端末証明書リストに端末固有秘密鍵で作成した電子署名を付加する
S716
新しく生成した復元先端末証明書リストを記憶部に書き込む
S717
e
暗号化端末固有公開鍵証明書と復元先端末証明書リストを指定して端末固有情報復元処理(端末側)を実行する
S722
S723
エラー?
Yes
S724
エラーを応答
f
No
サーバから受信した暗号化端末固有情報と暗号化期限情報を端末固有秘密鍵により復号
S725
サーバから受信したサーバ公開鍵証明書内の公開鍵と端末固有秘密鍵からDH(Diffie-Hellman)方式により共用鍵を生成し、それを端末証明書暗号化鍵とし、不揮発記憶域に格納する
S726
端末固有公開鍵証明書を端末証明書暗号化鍵により暗号化して暗号化端末固有公開鍵証明書を作成し、記憶部に格納する
S727
記憶部の復元先端末証明書リストを削除する
S728
g

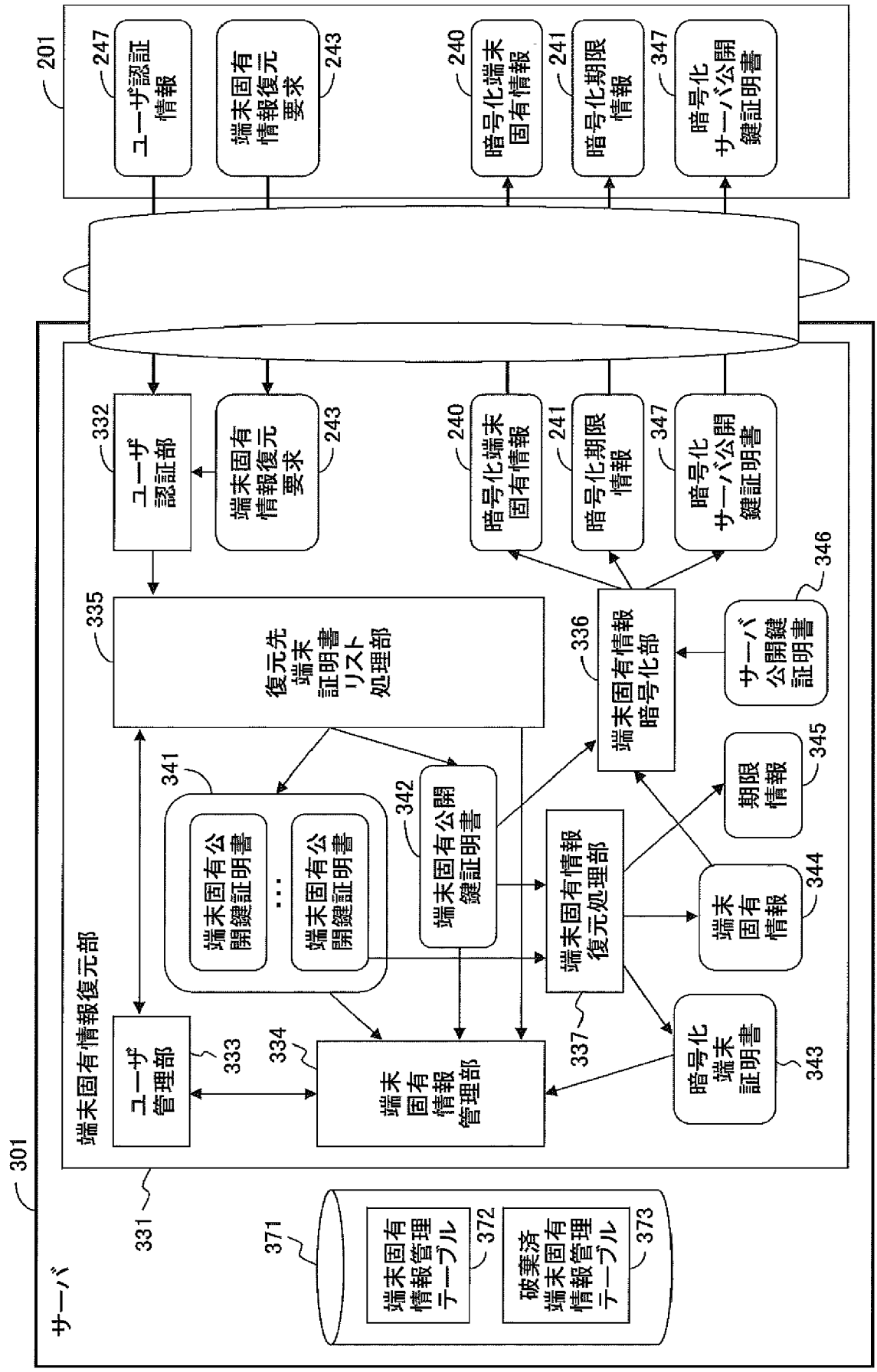
[図16]


296-1
端末Aの
端末固有
公開鍵証明書
端末Bの
端末固有
公開鍵証明書
電子署名
(端末Bの端末固有
秘密鍵で署名)
296-2
端末Aの
端末固有
公開鍵証明書
端末Bの
端末固有
公開鍵証明書
端末Cの
端末固有
公開鍵証明書
電子署名
(端末Cの端末固有
秘密鍵で署名)

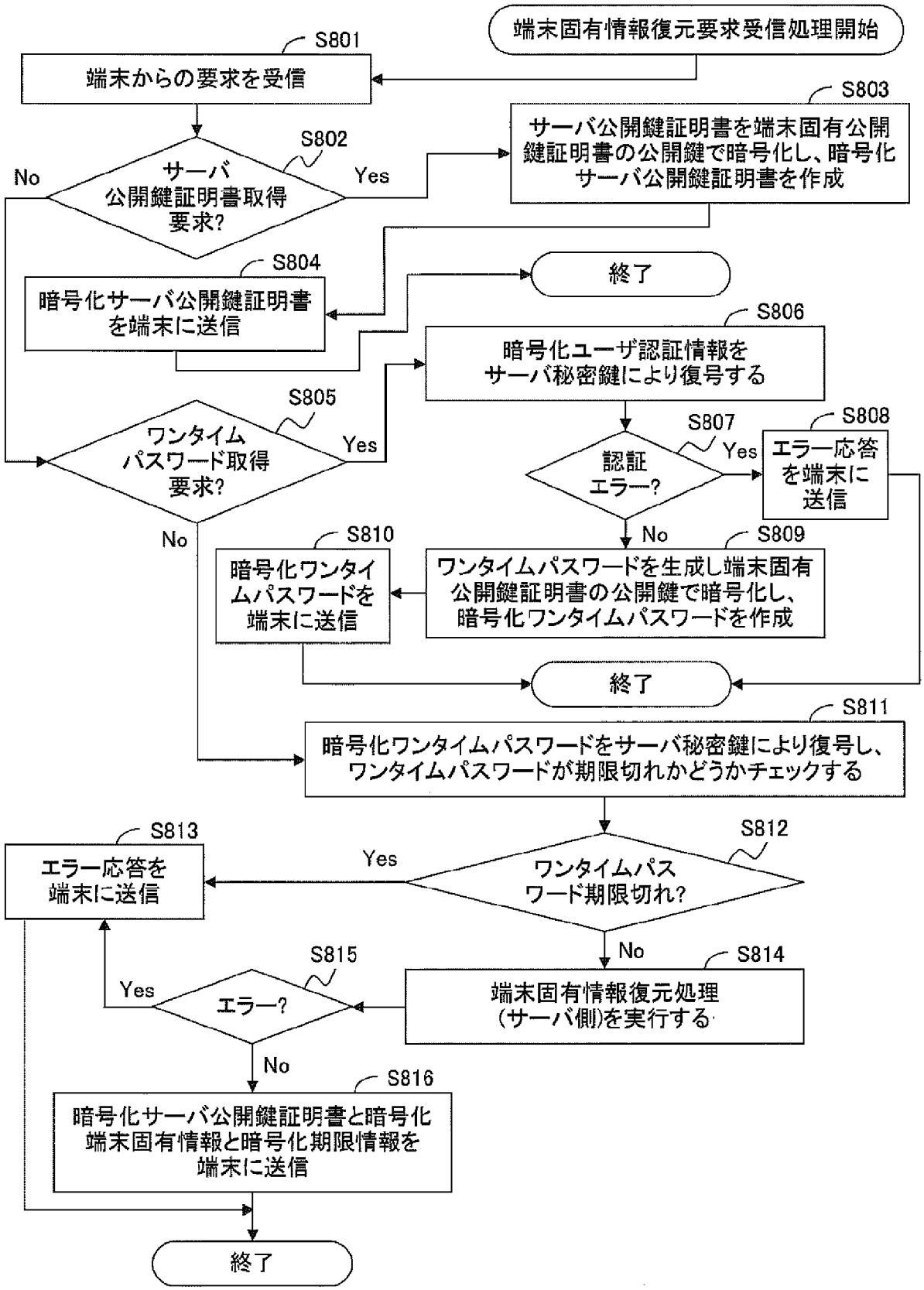
[図17]


端末固有情報復元処理(端末側)開始
S741
不揮発領域から端末固有公開鍵証明書を読み込む
S742
端末固有公開鍵証明書を指定してサーバにサーバ公開鍵証明書取得要求を送信
S743
エラー?
Yes
S744
エラーを応答
No
S745
サーバから受信した暗号化サーバ公開鍵証明書を端末固有秘密鍵で復号
S746
ユーザ認証情報をサーバ公開鍵証明書の公開鍵により暗号化し、ワンタイムパスワード取得要求を作成する
S747
サーバにワンタイムパスワード取得要求を送信
S748
エラー?
Yes
S749
エラーを応答
No
S750
暗号化ワンタイムパスワードを受信
S751
暗号化ワンタイムパスワードを端末固有秘密鍵により復号する
S752
ワンタイムパスワードと暗号化端末固有公開鍵証明書と復元先端末証明書リストをサーバ公開鍵証明書の公開鍵により暗号化し、端末固有情報復元要求を作成する
S753
サーバに端末固有情報復元要求を送信
S754
エラー?
Yes
S755
エラーを応答
No
S756
暗号化端末固有情報と暗号化期限情報を受信
終了

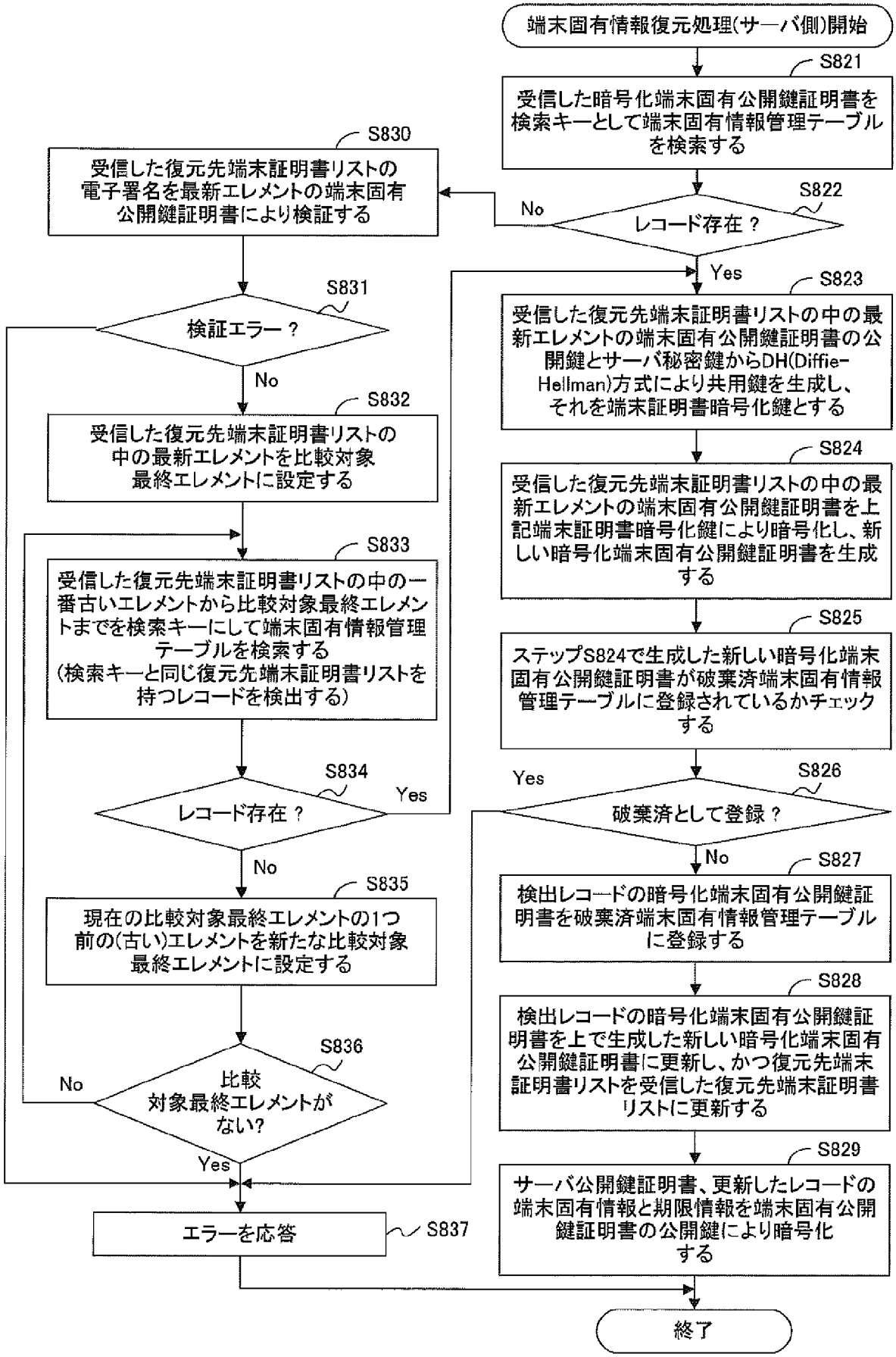
[図18]


201
247
ユーザ認証情報
243
端末固有情報復元要求
240
暗号化端末固有情報
241
暗号化期限情報
347
暗号化サーバ公開鍵証明書
301
サーバ
331
端末固有情報復元部
332
ユーザ認証部
335
復元先端末証明書リスト処理部
341
端末固有公開鍵証明書
端末固有公開鍵証明書
342
端末固有公開鍵証明書
333
ユーザ管理部
334
端末固有情報管理部
336
端末固有情報暗号化部
346
サーバ公開鍵証明書
345
期限情報
344
端末固有情報
337
端末固有情報復元処理部
343
暗号化端末証明書
371
372
端末固有情報管理テーブル
373
破棄済端末固有情報管理テーブル

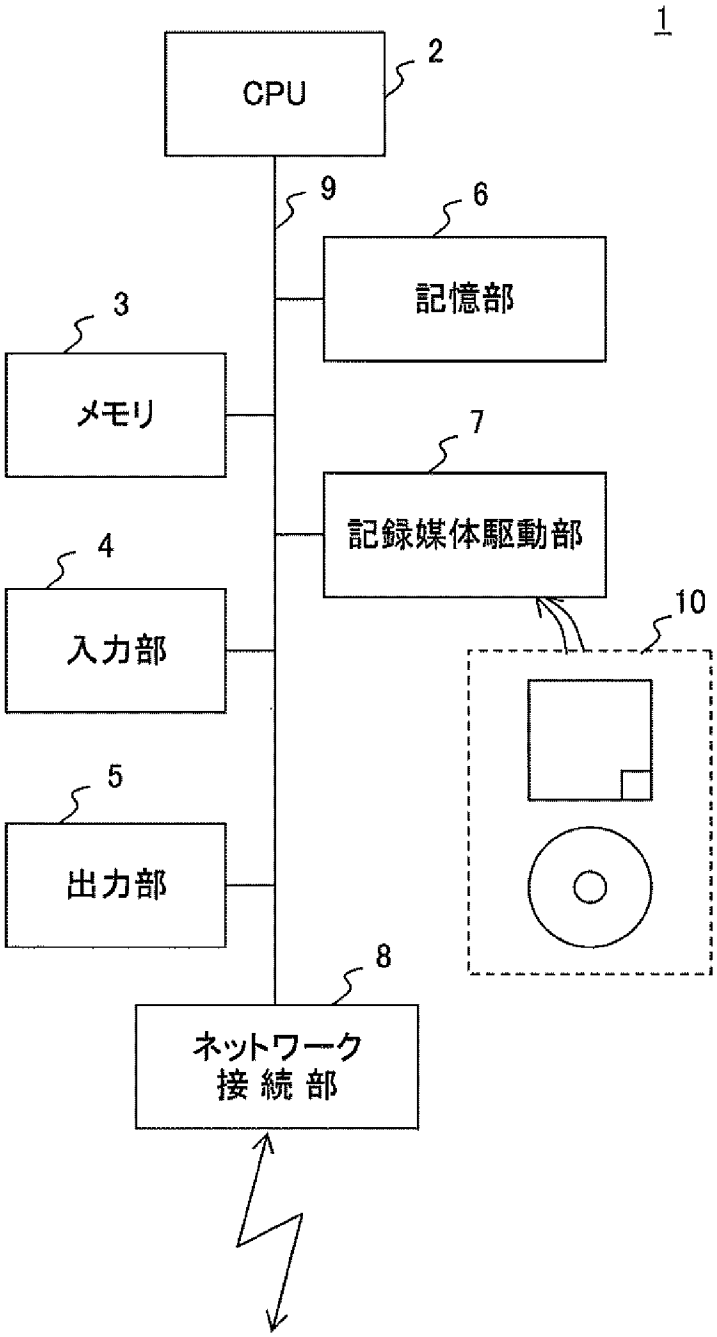
[図19]


端末固有情報復元要求受信処理開始
S801
端末からの要求を受信
S802
サーバ公開鍵証明書取得要求?
No
Yes
S803
サーバ公開鍵証明書を端末固有公開鍵証明書の公開鍵で暗号化し、暗号化サーバ公開鍵証明書を作成
S804
暗号化サーバ公開鍵証明書を端末に送信
終了
S806
暗号化ユーザ認証情報をサーバ秘密鍵により復号する
S805
ワンタイムパスワード取得要求?
Yes
No
S807
認証エラー?
Yes
No
S808
エラー応答を端末に送信
S810
暗号化ワンタイムパスワードを端末に送信
S809
ワンタイムパスワードを生成し端末固有公開鍵証明書の公開鍵で暗号化し、暗号化ワンタイムパスワードを作成
終了
S811
暗号化ワンタイムパスワードをサーバ秘密鍵により復号し、ワンタイムパスワードが期限切れかどうかチェックする
S813
エラー応答を端末に送信
Yes
S812
ワンタイムパスワード期限切れ?
No
S815
Yes
エラー?
No
S814
端末固有情報復元処理(サーバ側)を実行する
S816
暗号化サーバ公開鍵証明書と暗号化端末固有情報と暗号化期限情報を端末に送信
終了

[図20]


端末固有情報復元処理(サーバ側)開始
S821
受信した暗号化端末固有公開鍵証明書を検索キーとして端末固有情報管理テーブルを検索する
S822
レコード存在？
No
Yes
S830
受信した復元先端末証明書リストの電子署名を最新エレメントの端末固有公開鍵証明書により検証する
S831
検証エラー？
No
S832
受信した復元先端末証明書リストの中の最新エレメントを比較対象最終エレメントに設定する
S833
受信した復元先端末証明書リストの中の一番古いエレメントから比較対象最終エレメントまでを検索キーにして端末固有情報管理テーブルを検索する
(検索キーと同じ復元先端末証明書リストを持つレコードを検出する)
S834
レコード存在？
Yes
No
S835
現在の比較対象最終エレメントの1つ前の(古い)エレメントを新たな比較対象最終エレメントに設定する
S836
比較対象最終エレメントがない?
No
Yes
エラーを応答
S837
S823
受信した復元先端末証明書リストの中の最新エレメントの端末固有公開鍵証明書の公開鍵とサーバ秘密鍵からDH(Diffie-Hellman)方式により共用鍵を生成し、それを端末証明書暗号化鍵とする
S824
受信した復元先端末証明書リストの中の最新エレメントの端末固有公開鍵証明書を上記端末証明書暗号化鍵により暗号化し、新しい暗号化端末固有公開鍵証明書を生成する
S825
ステップS824で生成した新しい暗号化端末固有公開鍵証明書が破棄済端末固有情報管理テーブルに登録されているかチェックする
S826
破棄済として登録？
Yes
No
S827
検出レコードの暗号化端末固有公開鍵証明書を破棄済端末固有情報管理テーブルに登録する
S828
検出レコードの暗号化端末固有公開鍵証明書を上で生成した新しい暗号化端末固有公開鍵証明書に更新し、かつ復元先端末証明書リストを受信した復元先端末証明書リストに更新する
S829
サーバ公開鍵証明書、更新したレコードの端末固有情報と期限情報を端末固有公開鍵証明書の公開鍵により暗号化する
終了

[図21]



INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2012/052560

A. CLASSIFICATION OF SUBJECT MATTER
H04L9/08(2006.01)i, *H04N7/167*(2011.01)i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L9/08, H04N7/167

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	1996-2012
Kokai Jitsuyo Shinan Koho	1971-2012	Toroku Jitsuyo Shinan Koho	1994-2012

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.
A	JP 2002-374240 A (Matsushita Electric Industrial Co., Ltd.), 26 December 2002 (26.12.2002), paragraphs [0018] to [0054]	1-10
A	WO 2005/088896 A1 (KONINKLIJKE PHILIPS ELECTRONICS N.V.), 22 September 2005 (22.09.2005), page 12, line 23 to page 16, line 33	1-10
A	JP 2010-220093 A (Canon Inc.), 30 September 2010 (30.09.2010), paragraphs [0018] to [0031]	1-10

☐ 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
22 March, 2012 (22.03.12)	03 April, 2012 (03.04.12)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/JP2012/052560

JP 2002-374240 A	2002.12.26	US 2002/0164035 A1 EP 1249964 A2
WO 2005/088896 A1	2005.09.22	JP 2007-528658 A US 2007/0180497 A1 EP 1728350 A1 CN 1930818 A KR 2007022019 A
JP 2010-220093 A	2010.09.30	(Family: none)

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１２／０５２５６０

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, H04N7/167(2011.01)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, H04N7/167

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	１９７１－２０１２年
日本国実用新案登録公報	１９９６－２０１２年
日本国登録実用新案公報	１９９４－２０１２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
A	JP 2002-374240 A（松下電器産業株式会社）2002.12.26, 18-54段落	1-10
A	WO 2005/088896 A1（KONINKLIJKE PHILIPS ELECTRONICS N.V.）2005.09.22, 12頁23行-16頁33行	1-10
A	JP 2010-220093 A（キヤノン株式会社）2010.09.30, 18-31段落	1-10

☐　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
２２．０３．２０１２	０３．０４．２０１２

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　９３６４
中里　裕正
電話番号　０３－３５８１－１１０１　内線　３５４６

JP 2002-374240 A	2002.12.26	US 2002/0164035 A1 EP 1249964 A2
WO 2005/088896 A1	2005.09.22	JP 2007-528658 A US 2007/0180497 A1 EP 1728350 A1 CN 1930818 A KR 2007022019 A
JP 2010-220093 A	2010.09.30	ファミリーなし