(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
2023年8月10日(10.08.2023)

WIPO | PCT

(10) 国際公開番号
WO 2023/149124 A1

(51) 国際特許分類:
H04L 9/32 (2006.01) *G06F 21/33* (2013.01)
E05B 49/00 (2006.01) *H04L 9/08* (2006.01)

(21) 国際出願番号： PCT/JP2022/047605

(22) 国際出願日： 2022年12月23日(23.12.2022)

(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 2022-016839 2022年2月7日(07.02.2022) JP

(71) 出願人:パナソニックＩＰマネジメント株式会社(**PANASONIC INTELLECTUAL PROPERTY MANAGEMENT CO., LTD.**) [JP/JP]; 〒5406207 大阪府大阪市中央区城見２丁目１番６１号 Osaka (JP).

(72) 発明者: 藏前 健治 (**KURAMAE, Kenji**). 秋元 正夫(**AKIMOTO, Masao**).

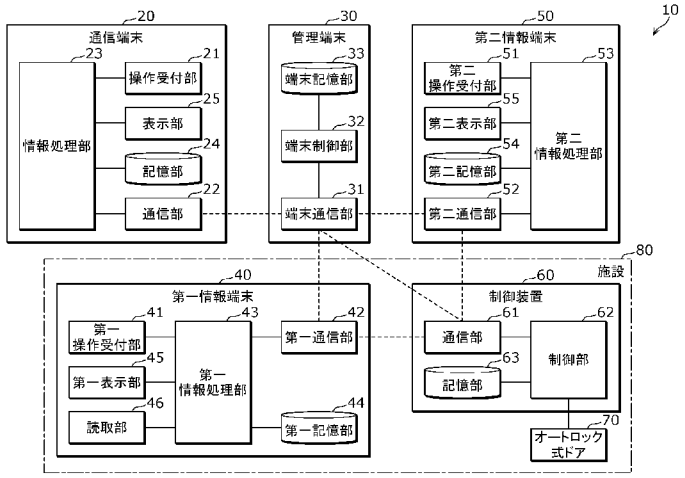
(74) 代理人: 新居 広守, 外 (**NII, Hiromori** et al.); 〒5320011 大阪府大阪市淀川区西中島５丁目３番１０号タナカ・イトーピア新大阪ビル６階新居国際特許事務所内 Osaka (JP).

(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, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP,

(54) **Title:** INFORMATION PROCESSING SYSTEM AND INFORMATION PROCESSING METHOD

(54) 発明の名称： 情報処理システム、及び、情報処理方法

[図2]



20 Communication terminal
21 Operation reception unit
22, 61 Communication unit
23 Information processing unit
24, 63 Storage unit
25 Display unit
30 Management terminal
31 Terminal communication unit
32 Terminal control unit
33 Terminal storage unit
40 First information terminal
41 First operation reception unit
42 First communication unit
43 First information processing unit
44 First storage unit
45 First display unit
46 Reading unit
50 Second information terminal
51 Second operation reception unit
52 Second communication unit
53 Second information processing unit
54 Second storage unit
55 Second display unit
60 Control device
62 Control unit
70 Auto-locking door
80 Facility

(57) **Abstract:** An information processing system (10) comprises a first information terminal (40), a management terminal (30), and a control device (60). The management terminal (30) issues a two-dimensional code that indicates a first server certificate. The first information terminal (40) reads the issued two-dimensional code to acquire the first server certificate and transmits the acquired first server certificate to the control device (60). The control device (60) receives the first server certificate from the first information terminal (40), verifies a first signature included in the acquired first server certificate

WO 2023/149124 A1

[続葉有]

KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, 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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, 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, CV, 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, ME, 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:

一　国際調査報告（条約第21条(3)）

using a second public key included in a root certificate stored at a storage unit, and releases a restriction on an apparatus when the verification has succeeded.

(57) 要約：情報処理システム（１０）は、第一情報端末（４０）、管理端末（３０）、及び、制御装置（６０）を備える。管理端末（３０）は、第一サーバ証明書を示す二次元コードを発行する。第一情報端末（４０）は、発行された二次元コードを読み取ることにより、第一サーバ証明書を取得し、取得された第一サーバ証明書を制御装置（６０）へ送信する。制御装置（６０）は、第一情報端末（４０）から第一サーバ証明書を受信し、受信された第一サーバ証明書に含まれる第一署名を記憶部に記憶されたルート証明書に含まれる第二の公開鍵を用いて検証し、検証に成功した場合に機器の制限を解除する。

明　細　書

発明の名称 ： 情報処理システム、及び、情報処理方法

技術分野

[0001]　本発明は、情報処理システム、及び、情報処理方法に関する。

背景技術

[0002]　従来、ドアなどを施錠または解錠するための技術が知られている。特許文献１には、ユーザが所持する携帯端末と、制御対象物（特定のゲート、ゲートに具備される錠前、エレベータなど）と接続するリーダーとの間で制御対象物の制御に必要な鍵データを通信する鍵データ通信システムが開示されている。

先行技術文献

特許文献

[0003] 特許文献1：特開２０１６－１８４８７５号公報

発明の概要

発明が解決しようとする課題

[0004]　本発明は、二次元コードを用いて比較的安全に物品または人の出入りの制限を解除することができる情報処理システム等を提供する。

課題を解決するための手段

[0005]　本発明の一態様に係る情報処理システムは、空間に対する物品または人の出入りを制限する機器の前記制限を解除するために用いられる情報処理システムであって、第一情報端末、管理端末、及び、制御装置を備え、前記第一情報端末は、第一の秘密鍵及び第一の公開鍵が記憶された第一記憶部と、前記第一の公開鍵を前記管理端末へ送信する第一通信部とを有し、前記管理端末は、第二の秘密鍵及び第二の公開鍵が記憶された端末記憶部と、前記第一情報端末から前記第一の公開鍵を受信する端末通信部と、受信された前記第一の公開鍵に対する第一署名を前記第二の秘密鍵を用いて生成し、前記第一の公開鍵、及び、前記第一署名を含む第一サーバ証明書を示す二次元コード

を発行する端末制御部とを有し、前記第一情報端末は、前記管理端末によって発行された前記二次元コードを読み取る読取部と、前記読取部が読み取った前記二次元コードにより、前記第一サーバ証明書を取得する第一情報処理部を有し、前記第一通信部は、取得された前記第一サーバ証明書を前記制御装置へ送信し、前記制御装置は、前記第二の公開鍵を含むルート証明書が記憶された記憶部と、前記第一情報端末から前記第一サーバ証明書を受信する通信部と、受信された前記第一サーバ証明書に含まれる前記第一署名を前記記憶部に記憶された前記ルート証明書に含まれる前記第二の公開鍵を用いて検証し、検証に成功した場合に前記機器の前記制限を解除する制御部とを有する。

[0006] 本発明の一態様に係る情報処理方法は、空間に対する物品または人の出入りを制限する機器の前記制限を解除するために用いられる情報処理システムが実行する情報処理方法であって、第一の秘密鍵及び第一の公開鍵が記憶された第一記憶部を有する第一情報端末と、第二の秘密鍵及び第二の公開鍵が記憶された端末記憶部を有する管理端末と、前記第二の公開鍵を含むルート証明書が記憶された記憶部を有する制御装置とを備え、前記情報処理方法は、前記第一情報端末が前記第一の公開鍵を前記管理端末へ送信し、前記管理端末が前記第一情報端末から前記第一の公開鍵を受信する第一通信ステップと、前記管理端末が、受信された前記第一の公開鍵に対する第一署名を前記第二の秘密鍵を用いて生成し、前記第一の公開鍵、及び、前記第一署名を含む第一サーバ証明書を示す二次元コードを発行する発行ステップと、前記第一情報端末が、発行された前記二次元コードを読み取ることにより、前記第一サーバ証明書を取得する取得ステップと、前記第一情報端末が取得された前記第一サーバ証明書を前記制御装置へ送信し、前記制御装置が前記第一情報端末から前記第一サーバ証明書を受信する第二通信ステップと、前記制御装置が、受信された前記第一サーバ証明書に含まれる前記第一署名を前記記憶部に記憶された前記ルート証明書に含まれる前記第二の公開鍵を用いて検証し、検証に成功した場合に前記機器の前記制限を解除する制御ステップと

を含む。

[0007] 本発明の一態様に係るプログラムは、前記情報処理方法をコンピュータに実行させるためのプログラムである。

発明の効果

[0008] 本発明の一態様に係る情報処理システム等は、二次元コードを用いて比較的安全に物品または人の出入りの制限を解除することができる。

図面の簡単な説明

[0009] [図1]図１は、実施の形態に係る情報処理システムの外観図である。

[図2]図２は、実施の形態に係る情報処理システムの機能構成を示すブロック図である。

[図3]図３は、実施の形態に係る情報処理システムの動作例１の前半のシーケンス図である。

[図4]図４は、実施の形態に係る情報処理システムの動作例１の後半のシーケンス図である。

[図5]図５は、サーバ証明書のフォーマットの一例を示す図である。

[図6]図６は、実施の形態に係る情報処理システムの動作例２の前半のシーケンス図である。

[図7]図７は、実施の形態に係る情報処理システムの動作例２の後半のシーケンス図である。

発明を実施するための形態

[0010] 以下、実施の形態について、図面を参照しながら具体的に説明する。なお、以下で説明する実施の形態は、いずれも包括的または具体的な例を示すものである。以下の実施の形態で示される数値、形状、材料、構成要素、構成要素の配置位置及び接続形態、ステップ、ステップの順序などは、一例であり、本発明を限定する主旨ではない。また、以下の実施の形態における構成要素のうち、独立請求項に記載されていない構成要素については、任意の構成要素として説明される。

[0011] なお、各図は模式図であり、必ずしも厳密に図示されたものではない。ま

た、各図において、実質的に同一の構成に対しては同一の符号を付し、重複する説明は省略または簡略化される場合がある。

[0012] （実施の形態）

［構成］

まず、実施の形態に係る情報処理システムの構成について説明する。図１は、実施の形態に係る情報処理システムの外観図である。図２は、実施の形態に係る情報処理システムの機能構成を示すブロック図である。

[0013] 図１に示されるように、実施の形態に係る情報処理システム１０は、施設８０を訪れる訪問者に、施設８０の共同玄関に設けられたオートロック式ドア７０の一時的な解錠権限を付与するためのシステムである。施設８０は、例えば、集合住宅であるが、オフィスビルなどの住宅以外の施設であってもよい。訪問者は、例えば、家事代行サービスの提供事業者から派遣される者、または、荷物の配達員などである。

[0014] 情報処理システム１０は、上記一時的な解錠権限を付与するために、ＱＲコード（登録商標）などの二次元コードを使用する。二次元コードは、二次元バーコードなどと呼ばれる場合もある。二次元コードは、従来のバーコード（一次元コード）に比べて情報量が多く、キャッシュレス決済の手段、飛行機の搭乗チケット、または、ロッカーの解錠キーといった用途に利用されている。

[0015] 二次元コードをオートロック式ドア７０の解錠許可証として利用する場合、二次元コードが施設８０の管理者から発行された正規の許可証であることをオートロック式ドア７０の制御装置６０が検証する必要がある。このような検証を実現するために、一般的には、制御装置６０に新たな解錠許可証が発行されたことを事前登録する必要がある。

[0016] これに対し、情報処理システム１０においては、サーバ証明書を二次元コードに変換し、当該二次元コードを認証に用いることで、制御装置６０への事前登録の省略を図っている。

[0017] 以下、情報処理システム１０の具体的な構成について説明する。情報処理

システム１０は、通信端末２０と、管理端末３０と、第一情報端末４０と、第二情報端末５０と、制御装置６０と、オートロック式ドア７０とを備える。

[0018] 通信端末２０は、施設８０への訪問者が所持する端末である。通信端末２０は、訪問者がオートロック式ドア７０の解錠を図るときに、二次元コードを表示部２５に表示する。通信端末２０は、例えば、スマートフォンまたはタブレット端末などの携帯型の端末である。通信端末２０は、操作受付部２１と、通信部２２と、情報処理部２３と、記憶部２４と、表示部２５とを備える。

[0019] 操作受付部２１は、訪問者の操作を受け付ける。操作受付部２１は、例えば、タッチパネルによって実現されるが、ハードウェアキーなどによって実現されてもよい。

[0020] 通信部２２は、通信端末２０が管理端末３０と通信を行うための通信回路である。通信部２２は、例えば、管理端末３０と、インターネットなどの広域通信ネットワークを通じた無線通信を行う。

[0021] 情報処理部２３は、二次元コードの表示処理などを行う。情報処理部２３は、例えば、マイクロコンピュータによって実現されるが、プロセッサによって実現されてもよい。情報処理部２３の機能は、例えば、情報処理部２３を構成するマイクロコンピュータまたはプロセッサ等（ハードウェア）が記憶部２４に記憶されたコンピュータプログラム（ソフトウェア）を実行することによって実現される。

[0022] 記憶部２４は、上記表示処理に必要な情報、及び、上記コンピュータプログラムなどが記憶される記憶装置である。記憶部２４は、例えば、半導体メモリによって実現される。

[0023] 表示部２５は、上記表示処理によって二次元コードが表示されるディスプレイである。表示部２５は、例えば、液晶パネルまたは有機ＥＬ（Ｅｌｅｃｔｒｏ－Ｌｕｍｉｎｅｓｃｅｎｃｅ）パネルなどの表示パネルによって実現される。

[0024] 管理端末３０は、施設８０の管理者等が使用する端末である。管理者等とは、施設８０のオーナーまたは施設８０の管理事業者の従業員などである。管理端末３０は、訪問者の求めに応じて管理者が二次元コードを発行するために使用される。管理端末３０は、例えば、スマートフォンまたはタブレット端末などの携帯型の端末であるが、パーソナルコンピュータまたはサーバ装置などの据え置き型の端末であってもよい。管理端末３０は、端末通信部３１と、端末制御部３２と、端末記憶部３３とを備える。

[0025] 端末通信部３１は、管理端末３０が、通信端末２０、第一情報端末４０、第二情報端末５０、及び、制御装置６０のそれぞれと通信を行うための通信回路である。端末通信部３１は、例えば、通信端末２０、第一情報端末４０、第二情報端末５０、及び、制御装置６０のそれぞれと広域通信ネットワークを通じた通信を行う。端末通信部３１は、有線通信を行ってもよいし、無線通信を行ってもよい。

[0026] 端末制御部３２は、二次元コードを発行するための情報処理を行う。端末制御部３２は、例えば、マイクロコンピュータによって実現されるが、プロセッサによって実現されてもよい。端末制御部３２の機能は、例えば、端末制御部３２を構成するマイクロコンピュータまたはプロセッサ等（ハードウェア）が端末記憶部３３に記憶されたコンピュータプログラム（ソフトウェア）を実行することによって実現される。

[0027] 端末記憶部３３は、上記情報処理に必要な情報、及び、上記コンピュータプログラムなどが記憶される記憶装置である。端末記憶部３３は、例えば、半導体メモリによって実現されるが、ＨＤＤ（Ｈａｒｄ　Ｄｉｓｋ　Ｄｒｉｖｅ）によって実現されてもよい。

[0028] 第一情報端末４０は、施設８０への訪問者がオートロック式ドア７０を解錠するために操作する端末である。第一情報端末４０は、施設８０の共用部８１であってオートロック式ドア７０の外側（屋外側）に固定設置される。第一情報端末４０は、言い換えれば、受付端末であり、二次元コードの読み取りを行う。第一情報端末４０は、例えば、タブレット端末などの携帯型の

端末であるが、ロビーインターホンなどの専用端末であってもよい。第一情報端末４０は、第一操作受付部４１と、第一通信部４２と、第一情報処理部４３と、第一記憶部４４と、第一表示部４５と、読取部４６を備える。

[0029] 第一操作受付部４１は、訪問者の操作を受け付ける。第一操作受付部４１は、例えば、タッチパネルによって実現されるが、ハードウェアキーなどによって実現されてもよい。なお、第一操作受付部４１は、第一情報端末４０に外付けされるキーボードなどの入力装置によって実現されてもよい。

[0030] 第一通信部４２は、第一情報端末４０が管理端末３０及び制御装置６０と通信を行うための通信回路である。第一通信部４２は、例えば、管理端末３０とインターネットなどの広域通信ネットワークを通じた無線通信を行い、制御装置６０と局所通信ネットワークを通じた無線通信を行う。

[0031] 第一情報処理部４３は、通信端末２０の表示部２５に表示される二次元コードの読取処理などを行う。第一情報処理部４３は、例えば、マイクロコンピュータによって実現されるが、プロセッサによって実現されてもよい。第一情報処理部４３の機能は、例えば、第一情報処理部４３を構成するマイクロコンピュータまたはプロセッサ等（ハードウェア）が第一記憶部４４に記憶されたコンピュータプログラム（ソフトウェア）を実行することによって実現される。

[0032] 第一記憶部４４は、上記読取処理に必要な情報、及び、上記コンピュータプログラムなどが記憶される記憶装置である。第一記憶部４４は、例えば、半導体メモリによって実現される。

[0033] 第一表示部４５は、訪問者へ読取部４６付近に二次元コードを提示することを促す情報などが表示されるディスプレイである。第一表示部４５は、例えば、液晶パネルまたは有機ＥＬパネルなどの表示パネルによって実現される。

[0034] 読取部４６は、通信端末２０の表示部２５に表示される二次元コードを読み取る。読取部４６は、カメラによって実現される。なお、読取部４６は、第一情報端末４０に外付けされるカメラ、または、第一情報端末４０に外付

けされる二次元コードリーダ（二次元コードの読み取りに特化したカメラ）によって実現されてもよい。

[0035] 第二情報端末５０は、施設８０の専有部８２に居住する居住者が所持する端末である。第二情報端末５０は、居住者がオートロック式ドア７０を解錠するために操作する端末である。第二情報端末５０は、例えば、スマートフォンまたはタブレット端末などの携帯型の端末である。第二情報端末５０は、第二操作受付部５１と、第二通信部５２と、第二情報処理部５３と、第二記憶部５４と、第二表示部５５とを備える。

[0036] 第二操作受付部５１は、居住者の操作を受け付ける。第二操作受付部５１は、例えば、タッチパネルによって実現されるが、ハードウェアキーなどによって実現されてもよい。

[0037] 第二通信部５２は、第二情報端末５０が管理端末３０、及び、制御装置６０と通信を行うための通信回路である。第二通信部５２は、例えば、管理端末３０とインターネットなどの広域通信ネットワークを通じた無線通信を行い、制御装置６０と局所通信ネットワークを通じた無線通信を行う。

[0038] 第二情報処理部５３は、管理端末３０へ第二サーバ証明書の発行を要求するための情報処理、及び、第二サーバ証明書を制御装置６０へ送信する処理などを行う。第二情報処理部５３は、例えば、マイクロコンピュータによって実現されるが、プロセッサによって実現されてもよい。第二情報処理部５３の機能は、例えば、第二情報処理部５３を構成するマイクロコンピュータまたはプロセッサ等（ハードウェア）が第二記憶部５４に記憶されたコンピュータプログラム（ソフトウェア）を実行することによって実現される。

[0039] 第二記憶部５４は、上記情報処理に必要な情報、及び、上記コンピュータプログラムなどが記憶される記憶装置である。第二記憶部５４は、例えば、半導体メモリによって実現される。

[0040] 第二表示部５５は、第二操作受付部５１が操作を受け付けるときの表示画面などが表示されるディスプレイである。第二表示部５５は、例えば、液晶パネルまたは有機ＥＬパネルなどの表示パネルによって実現される。

[0041] 制御装置６０は、オートロック式ドア７０の解錠及び施錠を制御する制御装置である。制御装置６０は、例えば、施設８０の共用部８１であってオートロック式ドア７０に近傍に設置される。制御装置６０は、第一情報端末４０と一体的な装置であってもよいが、情報処理システム１０においては、第一情報端末４０とは別体の装置であり、第一情報端末４０と近距離無線通信を行う。このため、制御装置６０の設置場所と離れた場所に、受付端末である第一情報端末４０を設置することも可能である。制御装置６０は、通信部６１と、制御部６２と、記憶部６３とを備える。

[0042] 通信部６１は、制御装置６０が、管理端末３０、第一情報端末４０、及び、第二情報端末５０のそれぞれと通信を行うための通信回路である。通信部６１は、例えば、第一情報端末４０及び第二情報端末５０とは局所通信ネットワークを通じた無線通信を行い、管理端末３０とは広域通信ネットワークを通じた無線通信を行う。

[0043] 制御部６２は、オートロック式ドア７０を施錠または解錠するための情報処理を行う。制御部６２は、具体的には、オートロック式ドア７０に制御信号を出力することにより、オートロック式ドア７０を施錠または解錠する。制御部６２は、例えば、マイクロコンピュータによって実現されるが、プロセッサによって実現されてもよい。制御部６２の機能は、例えば、制御部６２を構成するマイクロコンピュータまたはプロセッサ等（ハードウェア）が記憶部６３に記憶されたコンピュータプログラム（ソフトウェア）を実行することによって実現される。

[0044] 記憶部６３は、上記情報処理に必要な情報、及び、上記コンピュータプログラムなどが記憶される記憶装置である。記憶部６３は、例えば、半導体メモリによって実現される。

[0045] オートロック式ドア７０は、施設８０の共同玄関（エントランス）に設けられたドア装置である。オートロック式ドア７０は、制御装置６０により、解錠（または開放）されてから一定時間の経過後に自動的に施錠（または閉鎖）される。オートロック式ドア７０が有するドアは、引き戸であってもよ

いし、開き戸であってもよい。なお、ここでの解錠は、例えば、オートロック式ドア７０のロック機構（電気錠など）のロックを解除（解錠）することを意味する。開放は、例えば、オートロック式ドア７０が解錠された後にオートロック式ドア７０を開放することを意味する。以下の実施の形態における「オートロック式ドア７０の解錠」は、オートロック式ドア７０が少なくとも解錠されることを意味し、解錠された後に開放されてもよいことを意味している。

[0046] ［動作例１］

次に、情報処理システム１０の動作例１について説明する。図３及び図４は、情報処理システム１０の動作例１のシーケンス図である。以下の動作例１においては、通信端末２０は、施設８０への訪問者によって使用され、管理端末３０は、施設８０の管理者等によって使用されるものとして説明が行われる。

[0047] まず、図３を参照しながら、通信端末２０の記憶部２４にサーバ証明書を示す二次元コードの二次元コード情報が記憶されるまでの動作について説明する。サーバ証明書は、オートロック式ドア７０の解錠許可証の役割を果たすものである。図３に示されるように、第一情報端末４０の第一記憶部４４には、第一の公開鍵及び第一の秘密鍵が記憶される。第一の公開鍵及び第一の秘密鍵は、例えば、第一情報端末４０に情報処理システム１０用のアプリケーションプログラム（以下、単にアプリとも記載される）をインストールしたときに生成され、第一記憶部４４に記憶される。

[0048] また、管理端末３０の端末記憶部３３には、第二の公開鍵及び第二の秘密鍵が記憶される。第二の公開鍵及び第二の秘密鍵は、例えば、管理端末３０に情報処理システム１０用のアプリをインストールしたときに端末記憶部３３に記憶される。

[0049] まず、第一情報端末４０は、第一記憶部４４に記憶された第一の公開鍵を管理端末３０へ送信する（Ｓ１１）。第一の公開鍵は、例えば、第一情報端末４０の施設（共同玄関）への設置時に行われる初期設定作業の際に、設置

者が第一操作受付部４１に対して所定の操作を行うことで管理端末３０へ送信される。第一の公開鍵の管理端末３０への送信方法、及び、第一の公開鍵の送信タイミングは特に限定されない。

[0050] 管理端末３０の端末通信部３１は、第一の公開鍵を受信する。端末制御部３２は、受信した第一の公開鍵を端末記憶部３３に記憶する（Ｓ１２）。

[0051] その後、訪問者は、施設８０を実際に訪問する前などに、通信端末２０の操作受付部２１へ所定の操作を行う。所定の操作には、パスワードを設定するための設定操作が含まれる。操作受付部２１によって所定の操作が受け付けられると（Ｓ１３）、情報処理部２３は、二次元コードの発行要求を生成し、生成した発行要求を通信部２２に管理端末３０へ送信させる。つまり、通信部２２は、二次元コードの発行要求を管理端末３０へ送信する（Ｓ１４）。なお、通信部２２は、広域通信ネットワークを通じた無線通信により発行要求を管理端末３０へ送信する。発行要求には、訪問者によって設定されたパスワードが含まれる。

[0052] 管理端末３０の端末通信部３１は、発行要求を受信する。管理者が訪問者の発行要求を確認し、訪問者によるオートロック式ドア７０の解錠を許可する場合、端末制御部３２は、第一サーバ証明書を発行する（Ｓ１５）。端末制御部３２は、具体的には、ステップＳ１１において受信した（ステップＳ１２において端末記憶部３３に記憶された）第一の公開鍵及び利用条件に対する第一署名を第二の秘密鍵を用いて生成し、第一の公開鍵、利用条件、及び、第一署名を含む第一サーバ証明書を発行する。利用条件は、例えば、時期的な条件（言い換えれば、有効期限）を示す情報であり、例えば、管理端末３０を使用する管理者などによってあらかじめ定められる。なお、利用条件は、有効回数に関する条件であってもよい。ここでの有効回数とは、第一サーバ証明書によってオートロック式ドア７０を解錠することができる上限回数を意味する。

[0053] なお、第一サーバ証明書のフォーマットとしては、例えば、Ｘ．５０９証明書が用いられる。図５は、第一サーバ証明書のフォーマットの一例を示す

図である。図５における証明書の有効期間は、上記利用条件（有効期限）に相当し、主体者公開鍵情報は、第一の公開鍵に相当し、ｓｉｇｎａｔｕｒｅＶａｌｕｅは、第一署名に相当する。なお、図５のフォーマットの拡張領域に、有効期限以外の利用条件（有効回数など）が格納されてもよい。

[0054] 次に、端末制御部３２は、ステップＳ１５において発行した第一サーバ証明書を、ステップＳ１４において受信した発行要求に含まれるパスワードによって暗号化する（Ｓ１６）。第一サーバ証明書をパスワードによって暗号化する方法については既存のどのようなアルゴリズムが用いられてもよく、特に限定されない。

[0055] 次に、端末制御部３２は、暗号化された第一サーバ証明書を二次元コード化する（Ｓ１７）。つまり、端末制御部３２は、第一の公開鍵、及び、第一署名を含む第一サーバ証明書であって、パスワードによって暗号化された第一サーバ証明書を示す二次元コードを発行する。また、端末制御部３２は、二次元コードを表示するための二次元コード情報を、端末通信部３１に通信端末２０へ送信させる（Ｓ１８）。二次元コード情報は、例えば、電子メールなどによって管理端末３０から通信端末２０へ送信される。

[0056] 通信端末２０の通信部２２は、二次元コード情報を受信する。情報処理部２３は、受信された二次元コード情報を記憶部２４に記憶する（Ｓ１９）。

[0057] 次に、図４を参照しながら、二次元コード（第一サーバ証明書）を用いてオートロック式ドア７０が解錠されるまでの動作について説明する。図４に示されるように、制御装置６０の記憶部６３には、ルート証明書が記憶される。ルート証明書には第二の公開鍵が含まれる。ルート証明書は、例えば、管理端末３０の端末制御部３２によって生成され、端末通信部３１によって制御装置６０に送信されることで記憶部６３に記憶される。ルート証明書は、制御装置６０の製造時に製造設備により記憶部６３に記憶されてもよい。

[0058] まず、訪問者は、施設８０の周辺に到着すると、第一情報端末４０の近くへ移動し、通信端末２０の操作受付部２１へ所定の操作を行う。情報処理部２３は、受け付けられた所定の操作を契機に、ステップＳ１９において記憶

部２４に記憶された二次元コード情報に基づいて二次元コードを表示部２５に表示する（Ｓ２０）。訪問者は、通信端末２０を読取部４６にかざすことにより、表示部２５に表示された二次元コードを第一情報端末４０の読取部４６に提示する。読取部４６は、二次元コードを読み取る（Ｓ２１）。

[0059] また、訪問者は、第一情報端末４０の第一操作受付部４１へパスワードの入力操作を行う。第一操作受付部４１は、パスワードの入力操作を受け付ける（Ｓ２２）。ステップＳ２２において入力されるパスワードは、ステップＳ１３において訪問者自身が設定したパスワードである。

[0060] 第一操作受付部４１によってパスワードの入力操作が受け付けられると、第一情報処理部４３は、ステップＳ２１において読取部４６を通じて読み取った二次元コード、及び、ステップＳ２２において入力されたパスワードに基づいて、第一サーバ証明書を取得する（Ｓ２３）。第一情報処理部４３は、具体的には、二次元コードを暗号化された第一サーバ証明書に変換し、暗号化された第一サーバ証明書をパスワードによって復号することで第一サーバ証明書を取得する。つまり、第一情報処理部４３は、発行された二次元コードを読み取り、かつ、入力されたパスワードを用いた復号処理を行うことにより、第一サーバ証明書を取得する。

[0061] 次に、第一情報処理部４３は、取得した第一サーバ証明書を第一通信部４２に制御装置６０へ送信させる。つまり、第一通信部４２は、サーバ証明書を制御装置６０へ送信する（Ｓ２４）。なお、通信部２２は、局所通信ネットワークを通じた無線通信により、サーバ証明書を制御装置６０へ送信する。この無線通信は、例えば、Ｂｌｕｅｔｏｏｔｈ（登録商標）などの通信規格に基づく近距離無線通信である。

[0062] 制御装置６０の通信部６１は、第一サーバ証明書を受信する。制御部６２は、受信された第一サーバ証明書に含まれる第一署名を、記憶部６３に記憶されたルート証明書に含まれる第二の公開鍵を用いて検証する（Ｓ２５）。制御部６２は、第一署名の検証に成功した場合に、第一サーバ証明書に含まれている利用条件の判定を行う（Ｓ２６）。上述のように、利用条件は、例

えば、時期的な条件であり、制御部６２は、時期的な条件が満たされるか否かを判定する。制御部６２は、時期的な要件が満たされると判定した場合に、第一サーバ証明書に含まれる第一の公開鍵を用いてセッション鍵を生成する（Ｓ２７）。制御部６２は、生成したセッション鍵を第一の公開鍵で暗号化し、暗号化されたセッション鍵を通信部６１に第一情報端末４０へ送信させる（Ｓ２８）。

[0063] 第一情報端末４０の第一通信部４２は、暗号化されたセッション鍵を受信する。第一情報処理部４３は、第一の秘密鍵を用いてセッション鍵を復号し、セッション鍵を用いた暗号化通信により、解錠指令を第一通信部４２に制御装置６０へ送信させる（Ｓ２９）。

[0064] 制御装置６０の通信部６１は、解錠指令を受信する。制御部６２は、受信された解錠指令に基づいてオートロック式ドア７０を解錠する（Ｓ３０）。制御部６２は、具体的には、オートロック式ドア７０に制御信号を送信することによりオートロック式ドア７０を解錠する。

[0065] このように、情報処理システム１０においては、管理端末３０は、第一サーバ証明書及びルート証明書を用いて、安全に通信端末２０にオートロック式ドア７０の解錠権限を付与することができる。動作例１のような解錠方法は、訪問者に関する情報をあらかじめ第一情報端末４０または制御装置６０に登録しなくても、訪問者に解錠権限を付与することができる。また、動作例１のような解錠方法によれば、訪問者は通信端末２０にアプリ（公開鍵及び秘密鍵）をインストールする必要がないことから、訪問者への負担が少ない利点がある。

[0066] また、第一情報端末４０及び制御装置６０は、セッション鍵を用いた暗号化通信（無線通信）を行うことから、第一情報端末４０及び制御装置６０を分離して配置したとしても、盗聴などにより第一情報端末４０になりすました他の情報端末が不正にオートロック式ドア７０を解錠することが抑制される。

[0067] また、第一情報端末４０及び制御装置６０を分離して配置できることによ

れば、後述の動作例２（居住者によるオートロック式ドア７０の解錠）を実行することができる既存のシステムに、第一情報端末４０を新規に導入することで動作例１（訪問者によるオートロック式ドア７０の解錠）を容易に実現することができる。後述の動作例２で説明されるように、訪問者が通信端末２０を使用してオートロック式ドア７０を解錠する場合、及び、居住者が第二情報端末５０を使用してオートロック式ドア７０を解錠する場合も制御装置６０が行う処理は共通化されている。この点からも、情報処理システム１０は、既存のシステムに第一情報端末４０を新規に導入することで動作例１を容易に実現することができる。

[0068] なお、動作例１では、二次元コードは通信端末２０の表示部２５に表示されたが、訪問者は、二次元コードを印刷した紙を施設８０に持参し、これを読取部４６に提示することによっても、オートロック式ドア７０を解錠することができる。

[0069] また、動作例１においてパスワードを使用することは必須ではないが、パスワードが使用されることで訪問者以外の第三者が二次元コードを使用してオートロック式ドア７０を解錠することを抑制することができる。動作例１では、パスワードは訪問者によって設定されたが、管理者によって設定されて訪問者に通知されてもよい。

[0070] ［動作例２］

次に、情報処理システム１０の動作例２について説明する。図６及び図７は、情報処理システム１０の動作例２のシーケンス図である。以下の動作例２においては、第二情報端末５０は、施設８０の専有部８２の居住者によって使用され、管理端末３０は、施設８０の管理者等によって使用されるものとして説明が行われる。

[0071] まず、図６を参照しながら、第二情報端末５０の第二記憶部５４に第二サーバ証明書が記憶されるまでの動作について説明する。第二サーバ証明書は、オートロック式ドア７０の解錠許可証の役割を果たすものである。図６に示されるように、第二情報端末５０の第二記憶部５４には、第三の公開鍵及

び第三の秘密鍵が記憶される。第三の公開鍵及び第三の秘密鍵は、例えば、第二情報端末５０に情報処理システム１０用のアプリをインストールしたときに生成され、第二記憶部５４に記憶される。また、動作例１と同様に、管理端末３０の端末記憶部３３には、第二の公開鍵及び第二の秘密鍵が記憶される。

[0072] まず、居住者は、上記アプリを実行中の第二情報端末５０の第二操作受付部５１へ所定の操作を行う。所定の操作は、第二サーバ証明書をインストールするための操作である。第二操作受付部５１は、所定の操作を受け付ける（Ｓ３１）。

[0073] 第二操作受付部５１によって所定の操作が受け付けられると、第二情報処理部５３は、第二サーバ証明書の発行要求を生成し、生成した発行要求を第二通信部５２に管理端末３０へ送信させる。発行要求には、第三の公開鍵が含まれる。つまり、第二通信部５２は、第三の公開鍵を管理端末３０へ送信する（Ｓ３２）。なお、第二通信部５２は、広域通信ネットワークを通じた無線通信により第三の公開鍵を管理端末３０へ送信する。

[0074] 管理端末３０の端末通信部３１は、第三の公開鍵を含む発行要求を受信する。管理者が居住者の発行要求を確認し、居住者によるオートロック式ドア７０の解錠を許可する場合、端末制御部３２は、受信した第三の公開鍵及び利用条件に対する第二署名を第二の秘密鍵を用いて生成する（Ｓ３３）。また、端末制御部３２は、第三の公開鍵、利用条件、及び、第二署名を含む第二サーバ証明書を、端末通信部３１に第二情報端末５０へ送信させる（Ｓ３４）。利用条件は、例えば、時期的な条件（言い換えれば、有効期限）を示す情報であり、例えば、管理端末３０を使用する管理者などによってあらかじめ定められる。なお、利用条件は、有効回数に関する条件であってもよい。ここでの有効回数とは、第二サーバ証明書によってオートロック式ドア７０を解錠することができる上限回数を意味する。

[0075] なお、第二サーバ証明書のフォーマットとしては、例えば、Ｘ．５０９証明書（図５）が用いられる。図５における証明書の有効期間は、上記利用条

件に相当し、主体者公開鍵情報は、第三の公開鍵に相当し、ｓｉｇｎａｔｕｒｅＶａｌｕｅは、第二署名に相当する。なお、図５のフォーマットの拡張領域に、有効期限以外の利用条件（有効回数など）が格納されてもよい。

[0076] 第二情報端末５０の第二通信部５２は、第二サーバ証明書を受信する。第二情報処理部５３は、受信された第二サーバ証明書を第二記憶部５４に記憶する（Ｓ３５）。

[0077] 次に、図７を参照しながら、第二サーバ証明書を用いてオートロック式ドア７０が解錠されるまでの動作について説明する。図７に示されるように、制御装置６０の記憶部６３には、ルート証明書が記憶される。ルート証明書には第二の公開鍵が含まれる。ルート証明書は、例えば、管理端末３０の端末制御部３２によって生成され、端末通信部３１によって制御装置６０に送信されることで記憶部６３に記憶される。ルート証明書は、制御装置６０の製造時に製造設備により記憶部６３に記憶されてもよい。

[0078] まず、居住者は、施設８０へ到着するとオートロック式ドア７０の近くへ移動し、上記アプリを実行中の第二情報端末５０の第二操作受付部５１へオートロック式ドア７０を解錠するための所定の解錠操作を行う。第二操作受付部５１は、解錠操作を受け付ける（Ｓ３６）。

[0079] 第二操作受付部５１によって解錠操作が受け付けられると、第二情報処理部５３は、第二サーバ証明書を第二通信部５２に制御装置６０へ送信させる。つまり、第二通信部５２は、第二サーバ証明書を制御装置６０へ送信する（Ｓ３７）。なお、第二通信部５２は、局所通信ネットワークを通じた無線通信により、第二サーバ証明書を制御装置６０へ送信する。この無線通信は、例えば、Ｂｌｕｅｔｏｏｔｈ（登録商標）などの通信規格に基づく近距離無線通信である。

[0080] 制御装置６０の通信部６１は、第二サーバ証明書を受信する。制御部６２は、受信された第二サーバ証明書に含まれる第二署名を、記憶部６３に記憶されたルート証明書に含まれる第二の公開鍵を用いて検証する（Ｓ３８）。制御部６２は、第二署名の検証に成功した場合に、第二サーバ証明書に含ま

れている利用条件の判定を行う（Ｓ３９）。上述のように、利用条件は、例えば、時期的な条件であり、制御部６２は、時期的な条件が満たされるか否かを判定する。制御部６２は、時期的な要件が満たされると判定した場合に、第二サーバ証明書に含まれる第三の公開鍵を用いてセッション鍵を生成する（Ｓ４０）。制御部６２は、生成したセッション鍵を第三の公開鍵で暗号化し、暗号化されたセッション鍵を通信部６１に第二情報端末５０へ送信させる（Ｓ４１）。

[0081] 第二情報端末５０の第二通信部５２は、暗号化されたセッション鍵を受信する。第二情報処理部５３は、第三の秘密鍵を用いてセッション鍵を復号し、セッション鍵を用いた暗号化通信により、解錠指令を第二通信部５２に制御装置６０へ送信させる（Ｓ４２）。

[0082] 制御装置６０の通信部６１は、解錠指令を受信する。制御部６２は、受信された解錠指令に基づいてオートロック式ドア７０を解錠する（Ｓ４３）。制御部６２は、具体的には、オートロック式ドア７０に制御信号を送信することによりオートロック式ドア７０を解錠する。なお、第二情報端末５０は、同様の動作シーケンスに基づいて、オートロック式ドア７０の施錠を行うこともできる。

[0083] このように、情報処理システム１０においては、管理端末３０は、第二サーバ証明書及び第二ルート証明書を用いて、安全に第二情報端末５０にオートロック式ドア７０の解錠権限を付与することができる。

[0084] ［変形例］

上記実施の形態では、利用条件がサーバ証明書（第一サーバ証明書または第二サーバ証明書）に含まれたが、利用条件は、サーバ証明書とは別に安全な方法で通信端末２０から制御装置６０へ送信されてもよい。例えば、図４でステップＳ２８よりも後に、セッション鍵を用いた暗号通信によって、利用条件が管理端末３０の第一署名と共に第一情報端末４０から制御装置６０へ送信されてもよい。また、図７でステップＳ４１よりも後にセッション鍵を用いた暗号化通信によって利用条件が管理端末３０の第二署名と共に第二

情報端末５０から制御装置６０へ送信されてもよい。このように、サーバ証明書と利用条件を分けることにより、サーバ証明書の再発行をしなくても利用条件を柔軟に追加または変更することが可能となる。

[0085] また、上記実施の形態では、制御装置６０は、オートロック式ドア７０などの施設８０内の空間への人の出入りを制限する機器を制御したが、物品の出入りを制限する機器を制御してもよい。例えば、制御装置６０は、宅配ボックス、コインロッカー、または、貸金庫などの扉を施錠及び解錠する電気錠を制御してもよい。つまり、制御装置６０は、空間に対する物品または人の出入りを制限する機器を制御すればよい。

[0086] また、情報処理システム１０は、空間に対する物品または人の出入りを制限する機器だけでなく、照明機器及び空調機器などの家電機器の制御を特定の人にのみ許可する場合にも適用できる。

[0087] ［効果等］

以上説明したように、情報処理システム１０は、空間に対する物品または人の出入りを制限する機器の制限を解除するために用いられる。情報処理システム１０は、第一情報端末４０、管理端末３０、及び、制御装置６０を備える。第一情報端末４０は、第一の秘密鍵及び第一の公開鍵がされた第一記憶部４４と、第一の公開鍵を管理端末３０へ送信する第一通信部４２とを有する。管理端末３０は、第二の秘密鍵及び第二の公開鍵が記憶された端末記憶部３３と、第一情報端末４０から第一の公開鍵を受信する端末通信部３１と、受信された第一の公開鍵に対する第一署名を第二の秘密鍵を用いて生成し、第一の公開鍵、及び、第一署名を含む第一サーバ証明書を示す二次元コードを発行する端末制御部３２とを有する。第一情報端末４０は、管理端末３０によって発行された二次元コードを読み取る読取部４６と、読取部４６が読み取った二次元コードにより、第一サーバ証明書を取得する第一情報処理部４３を有する。第一通信部４２は、取得された第一サーバ証明書を制御装置６０へ送信する。制御装置６０は、第二の公開鍵を含むルート証明書が記憶された記憶部６３と、第一情報端末４０から第一サーバ証明書を受信す

る通信部６１と、受信された第一サーバ証明書に含まれる第一署名を記憶部６３に記憶されたルート証明書に含まれる第二の公開鍵を用いて検証し、検証に成功した場合に機器の制限を解除する制御部６２とを有する。なお、空間は、例えば、施設８０内の任意の閉空間である。

[0088] このような情報処理システム１０は、第一サーバ証明書を示す二次元コードの提示を要件として、比較的安全に物品または人の出入りの制限を解除することができる。

[0089] また、例えば、二次元コードは、パスワードによって暗号化された第一サーバ証明書を示す。第一情報端末４０は、パスワードの入力操作を受け付ける第一操作受付部４１を備える。第一情報処理部４３は、発行された二次元コードを読み取り、かつ、入力されたパスワードを用いた復号処理を行うことにより、第一サーバ証明書を取得する。

[0090] このような情報処理システム１０は、暗号化された第一サーバ証明書を示す二次元コードの提示と、パスワードの入力とを要件として、比較的安全に物品または人の出入りの制限を解除することができる。

[0091] また、例えば、端末制御部３２は、パスワードの設定操作を受け付ける操作受付部２１を備える通信端末２０によって送信された、パスワードを含む二次元コードの発行要求が端末通信部３１によって受信された場合に、二次元コードを発行し、発行した二次元コードを端末通信部３１に通信端末２０へ送信させる。

[0092] このような情報処理システム１０は、通信端末２０のユーザ（上記実施の形態の訪問者）に対して、物品または人の出入りの制限を解除する権限を付与することができる。

[0093] また、例えば、端末制御部３２は、通信端末２０によって送信された二次元コードの発行要求が端末通信部３１によって受信された場合に、二次元コードを発行し、発行した二次元コードを端末通信部３１に通信端末２０へ送信させる。第一情報処理部４３は、発行された二次元コードであって通信端末２０が有する表示部２５に表示された二次元コードを読取部４６で読み取

り、かつ、第一操作受付部４１より入力されたパスワードを用いた復号処理を行うことにより、第一サーバ証明書を取得する。

[0094] このような情報処理システム１０は、通信端末２０の表示部２５に表示された二次元コードを読み取ることにより、物品または人の出入りの制限を解除することができる。

[0095] また、例えば、情報処理システム１０は、さらに、第二情報端末５０を備える。第二情報端末５０は、第三の秘密鍵及び第三の公開鍵が記憶された第二記憶部５４と、第三の公開鍵を管理端末３０へ送信する第二通信部５２とを有する。管理端末３０の端末通信部３１は、第二情報端末５０から第三の公開鍵を受信する。端末制御部３２は、受信された第三の公開鍵に対する第二署名を第二の秘密鍵を用いて生成し、第三の公開鍵、及び、第二署名を含む第二サーバ証明書を、端末通信部３１に第二情報端末５０へ送信させる。第二情報端末５０の第二通信部５２は、管理端末３０から第二サーバ証明書を受信し、受信した第二サーバ証明書を制御装置６０へ送信する。制御装置６０の通信部６１は、第二情報端末５０から第二サーバ証明書を受信する。制御部６２は、受信された第二サーバ証明書に含まれる第二署名を記憶部６３に記憶されたルート証明書に含まれる第二の公開鍵を用いて検証し、検証に成功した場合に機器の制限を解除する。

[0096] このような情報処理システム１０は、第二情報端末５０のユーザ（上記実施の形態の居住者）に対して、物品または人の出入りの制限を解除する権限を付与することができる。

[0097] また、例えば、第一情報端末４０、及び、制御装置６０は、同一の施設８０に設置される。機器は、施設８０の共同玄関に設けられたオートロック式ドア７０である。機器の制限の解除とは、オートロック式ドア７０を解錠することである。

[0098] このような情報処理システム１０は、第一サーバ証明書を示す二次元コードの提示を要件として、オートロック式ドア７０を解錠することができる。

[0099] また、情報処理方法は、空間に対する物品または人の出入りを制限する機

器の制限を解除するために用いられる情報処理システム１０が実行する情報処理方法である。情報処理方法は、第一情報端末４０が第一の公開鍵を管理端末３０へ送信し、管理端末３０が第一情報端末４０から第一の公開鍵を受信する第一通信ステップＳ１１と、管理端末３０が、受信された第一の公開鍵に対する第一署名を第二の秘密鍵を用いて生成し、第一の公開鍵、及び、第一署名を含む第一サーバ証明書を示す二次元コードを発行する発行ステップＳ１５～Ｓ１７と、第一情報端末４０が、発行された二次元コードを読み取ることにより、第一サーバ証明書を取得する取得ステップＳ２１～Ｓ２３と、第一情報端末４０が取得された第一サーバ証明書を制御装置６０へ送信し、制御装置６０が第一情報端末から第一サーバ証明書を受信する第二通信ステップＳ２４と、制御装置６０が、受信された第一サーバ証明書に含まれる第一署名を記憶部６３に記憶されたルート証明書に含まれる第二の公開鍵を用いて検証し、検証に成功した場合に機器の制限を解除する制御ステップＳ２５～Ｓ３０とを含む。

[0100] このような情報処理方法は、第一サーバ証明書を示す二次元コードの提示を要件として、比較的安全に物品または人の出入りの制限を解除することができる。

[0101] また、情報処理プログラムは、上記情報処理方法をコンピュータに実行させるためのプログラムである。

[0102] このような情報処理プログラムは、第一サーバ証明書を示す二次元コードの提示を要件として、比較的安全に物品または人の出入りの制限を解除することができる。

[0103] （その他の実施の形態）

以上、実施の形態について説明したが、本発明は、上記実施の形態に限定されるものではない。

[0104] 例えば、上記実施の形態において、情報処理システムは、複数の装置によって実現された。この場合、情報処理システムが備える構成要素（特に、機能的な構成要素）は、複数の装置にどのように振り分けられてもよい。また

、情報処理システムは、単一の装置として実現されてもよい。例えば、情報処理システムは、通信端末、管理端末、第一情報端末、第二情報端末、及び、制御装置のいずれかに相当する単一の装置として実現されてもよい。

[0105] また、上記実施の形態において、特定の処理部が実行する処理を別の処理部が実行してもよい。また、複数の処理の順序が変更されてもよいし、複数の処理が並行して実行されてもよい。

[0106] また、上記実施の形態において、各構成要素は、各構成要素に適したソフトウェアプログラムを実行することによって実現されてもよい。各構成要素は、ＣＰＵまたはプロセッサなどのプログラム実行部が、ハードディスクまたは半導体メモリなどの記録媒体に記録されたソフトウェアプログラムを読み出して実行することによって実現されてもよい。

[0107] また、各構成要素は、ハードウェアによって実現されてもよい。例えば、各構成要素は、回路（または集積回路）でもよい。これらの回路は、全体として１つの回路を構成してもよいし、それぞれ別々の回路でもよい。また、これらの回路は、それぞれ、汎用的な回路でもよいし、専用の回路でもよい。

[0108] また、本発明の全般的または具体的な態様は、システム、装置、方法、集積回路、コンピュータプログラムまたはコンピュータ読み取り可能なＣＤ－ＲＯＭなどの記録媒体で実現されてもよい。また、本発明の全般的または具体的な態様は、システム、装置、方法、集積回路、コンピュータプログラム及び記録媒体の任意な組み合わせで実現されてもよい。

[0109] 例えば、本発明は、上記実施の形態の通信端末、管理端末、第一情報端末、第二情報端末、または、制御装置として実現されてもよい。

[0110] また、本発明は、上記実施の形態の情報処理システムなどのコンピュータが実行する情報処理方法として実現されてもよい。また、本発明は、情報処理方法をコンピュータに実行させるためのプログラムとして実現されてもよい。本発明は、このようなプログラムが記録されたコンピュータ読み取り可能な非一時的な記録媒体として実現されてもよい。

[0111] また、本発明は、汎用の情報端末を、上記実施の形態の管理端末、第一情報端末、または、第二情報端末として機能させるためのアプリケーションプログラムとして実現されてもよい。本発明は、このようなアプリケーションプログラムが記録されたコンピュータ読み取り可能な非一時的な記録媒体として実現されてもよい。

[0112] また、本発明は、既存のシステムに第一情報端末を追加することで情報処理システムを構築する方法として実現されてもよい。

[0113] その他、各実施の形態に対して当業者が思いつく各種変形を施して得られる形態、または、本発明の趣旨を逸脱しない範囲で各実施の形態における構成要素及び機能を任意に組み合わせることで実現される形態も本発明に含まれる。

符号の説明

[0114] １０ 情報処理システム
２０ 通信端末
２１ 操作受付部
２２ 通信部
２３ 情報処理部
２４ 記憶部
２５ 表示部
３０ 管理端末
３１ 端末通信部
３２ 端末制御部
３３ 端末記憶部
４０ 第一情報端末
４１ 第一操作受付部
４２ 第一通信部
４３ 第一情報処理部
４４ 第一記憶部

４５　第一表示部

４６　読取部

５０　第二情報端末

５１　第二操作受付部

５２　第二通信部

５３　第二情報処理部

５４　第二記憶部

５５　第二表示部

６０　制御装置

６１　通信部

６２　制御部

６３　記憶部

７０　オートロック式ドア（機器）

８０　施設

８１　共用部

８２　専有部

請求の範囲

[請求項1] 空間に対する物品または人の出入りを制限する機器の前記制限を解除するために用いられる情報処理システムであって、

第一情報端末、管理端末、及び、制御装置を備え、

前記第一情報端末は、

第一の秘密鍵及び第一の公開鍵が記憶された第一記憶部と、

前記第一の公開鍵を前記管理端末へ送信する第一通信部とを有し、

前記管理端末は、

第二の秘密鍵及び第二の公開鍵が記憶された端末記憶部と、

前記第一情報端末から前記第一の公開鍵を受信する端末通信部と、

受信された前記第一の公開鍵に対する第一署名を前記第二の秘密鍵を用いて生成し、前記第一の公開鍵、及び、前記第一署名を含む第一サーバ証明書を示す二次元コードを発行する端末制御部とを有し、

前記第一情報端末は、

前記管理端末によって発行された前記二次元コードを読み取る読取部と、

前記読取部が読み取った前記二次元コードにより、前記第一サーバ証明書を取得する第一情報処理部を有し、

前記第一通信部は、取得された前記第一サーバ証明書を前記制御装置へ送信し、

前記制御装置は、

前記第二の公開鍵を含むルート証明書が記憶された記憶部と、

前記第一情報端末から前記第一サーバ証明書を受信する通信部と、

受信された前記第一サーバ証明書に含まれる前記第一署名を前記記憶部に記憶された前記ルート証明書に含まれる前記第二の公開鍵を用いて検証し、検証に成功した場合に前記機器の前記制限を解除する制御部とを有する

情報処理システム。

[請求項2] 前記二次元コードは、パスワードによって暗号化された前記第一サーバ証明書を示し、

前記第一情報端末は、前記パスワードの入力操作を受け付ける第一操作受付部を備え、

前記第一情報処理部は、発行された前記二次元コードを読み取り、かつ、入力された前記パスワードを用いた復号処理を行うことにより、前記第一サーバ証明書を取得する

請求項１に記載の情報処理システム。

[請求項3] 前記端末制御部は、前記パスワードの設定操作を受け付ける操作受付部を備える通信端末によって送信された、前記パスワードを含む前記二次元コードの発行要求が前記端末通信部によって受信された場合に、前記二次元コードを発行し、発行した二次元コードを前記端末通信部に前記通信端末へ送信する

請求項２に記載の情報処理システム。

[請求項4] 前記端末制御部は、通信端末によって送信された前記二次元コードの発行要求が前記端末通信部によって受信された場合に、前記二次元コードを発行し、発行した二次元コードを前記端末通信部に前記通信端末へ送信させ、

前記第一情報処理部は、発行された前記二次元コードであって前記通信端末が有する表示部に表示された前記二次元コードを前記読取部で読み取ることにより、前記第一サーバ証明書を取得する

請求項１～３のいずれか１項に記載の情報処理システム。

[請求項5] 前記情報処理システムは、さらに、第二情報端末を備え、

前記第二情報端末は、

第三の秘密鍵及び第三の公開鍵が記憶された第二記憶部と、

前記第三の公開鍵を前記管理端末へ送信する第二通信部とを有し、

前記管理端末の前記端末通信部は、前記第二情報端末から前記第三の公開鍵を受信し、

前記端末制御部は、受信された前記第三の公開鍵に対する第二署名を前記第二の秘密鍵を用いて生成し、前記第三の公開鍵、及び、前記第二署名を含む第二サーバ証明書を、前記端末通信部に前記第二情報端末へ送信させ、

前記第二情報端末の前記第二通信部は、前記管理端末から前記第二サーバ証明書を受信し、受信した前記第二サーバ証明書を前記制御装置へ送信し、

前記制御装置の前記通信部は、前記第二情報端末から前記第二サーバ証明書を受信し、

前記制御部は、受信された前記第二サーバ証明書に含まれる前記第二署名を前記記憶部に記憶された前記ルート証明書に含まれる前記第二の公開鍵を用いて検証し、検証に成功した場合に前記機器の前記制限を解除する

請求項１～３のいずれか１項に記載の情報処理システム。

[請求項6] 前記第一情報端末、及び、前記制御装置は、同一の施設に設置され、

前記機器は、前記施設の共同玄関に設けられたオートロック式ドアであり、

前記機器の前記制限の解除とは、前記オートロック式ドアを解錠することである

請求項１～３のいずれか１項に記載の情報処理システム。

[請求項7] 空間に対する物品または人の出入りを制限する機器の前記制限を解除するために用いられる情報処理システムが実行する情報処理方法であって、

第一の秘密鍵及び第一の公開鍵が記憶された第一記憶部を有する第一情報端末と、

第二の秘密鍵及び第二の公開鍵が記憶された端末記憶部を有する管理端末と、

前記第二の公開鍵を含むルート証明書が記憶された記憶部を有する制御装置とを備え、

前記情報処理方法は、

前記第一情報端末が前記第一の公開鍵を前記管理端末へ送信し、前記管理端末が前記第一情報端末から前記第一の公開鍵を受信する第一通信ステップと、

前記管理端末が、受信された前記第一の公開鍵に対する第一署名を前記第二の秘密鍵を用いて生成し、前記第一の公開鍵、及び、前記第一署名を含む第一サーバ証明書を示す二次元コードを発行する発行ステップと、

前記第一情報端末が、発行された前記二次元コードを読み取ることにより、前記第一サーバ証明書を取得する取得ステップと、

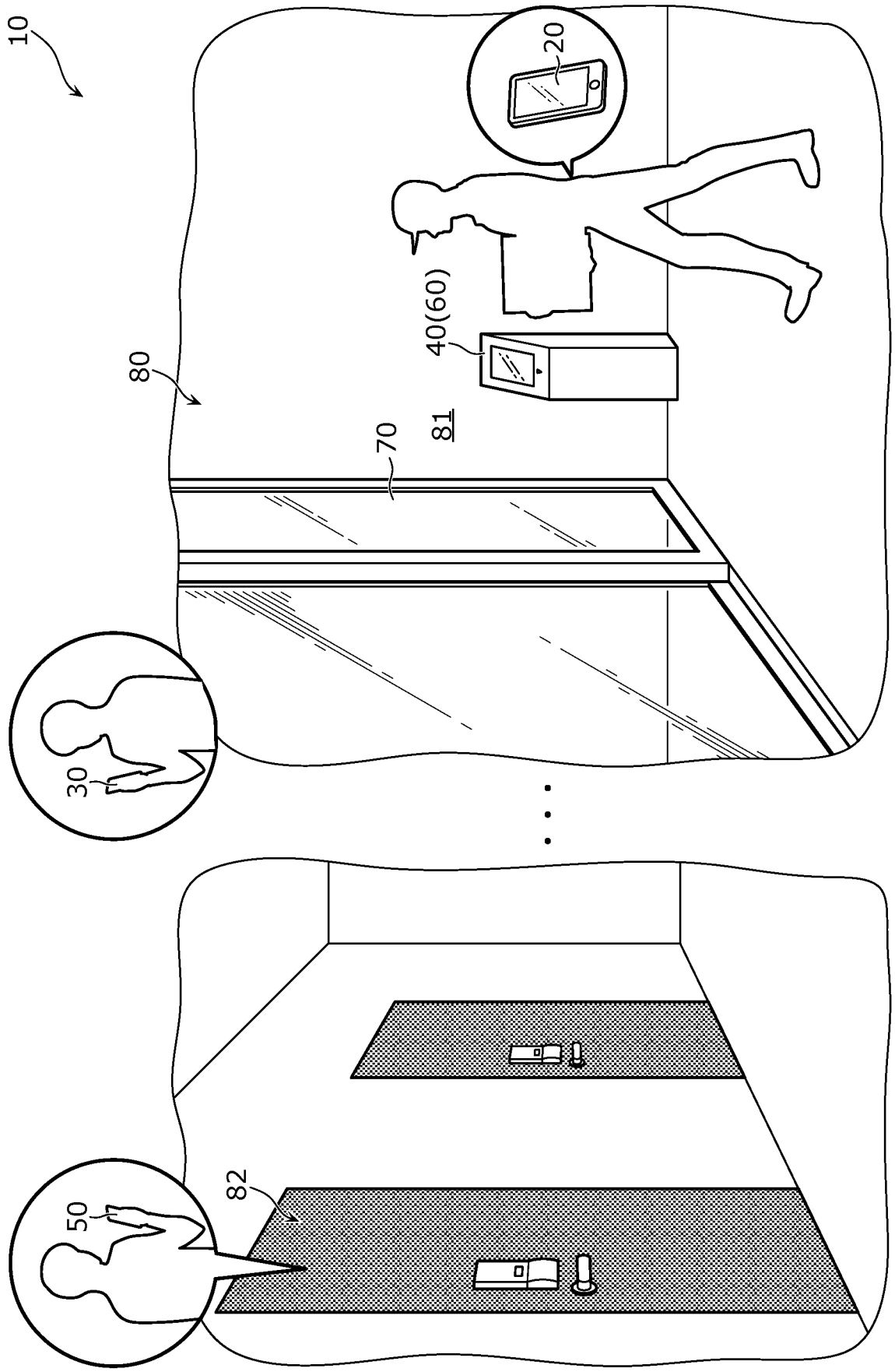
前記第一情報端末が取得された前記第一サーバ証明書を前記制御装置へ送信し、前記制御装置が前記第一情報端末から前記第一サーバ証明書を受信する第二通信ステップと、

前記制御装置が、受信された前記第一サーバ証明書に含まれる前記第一署名を前記記憶部に記憶された前記ルート証明書に含まれる前記第二の公開鍵を用いて検証し、検証に成功した場合に前記機器の前記制限を解除する制御ステップとを含む

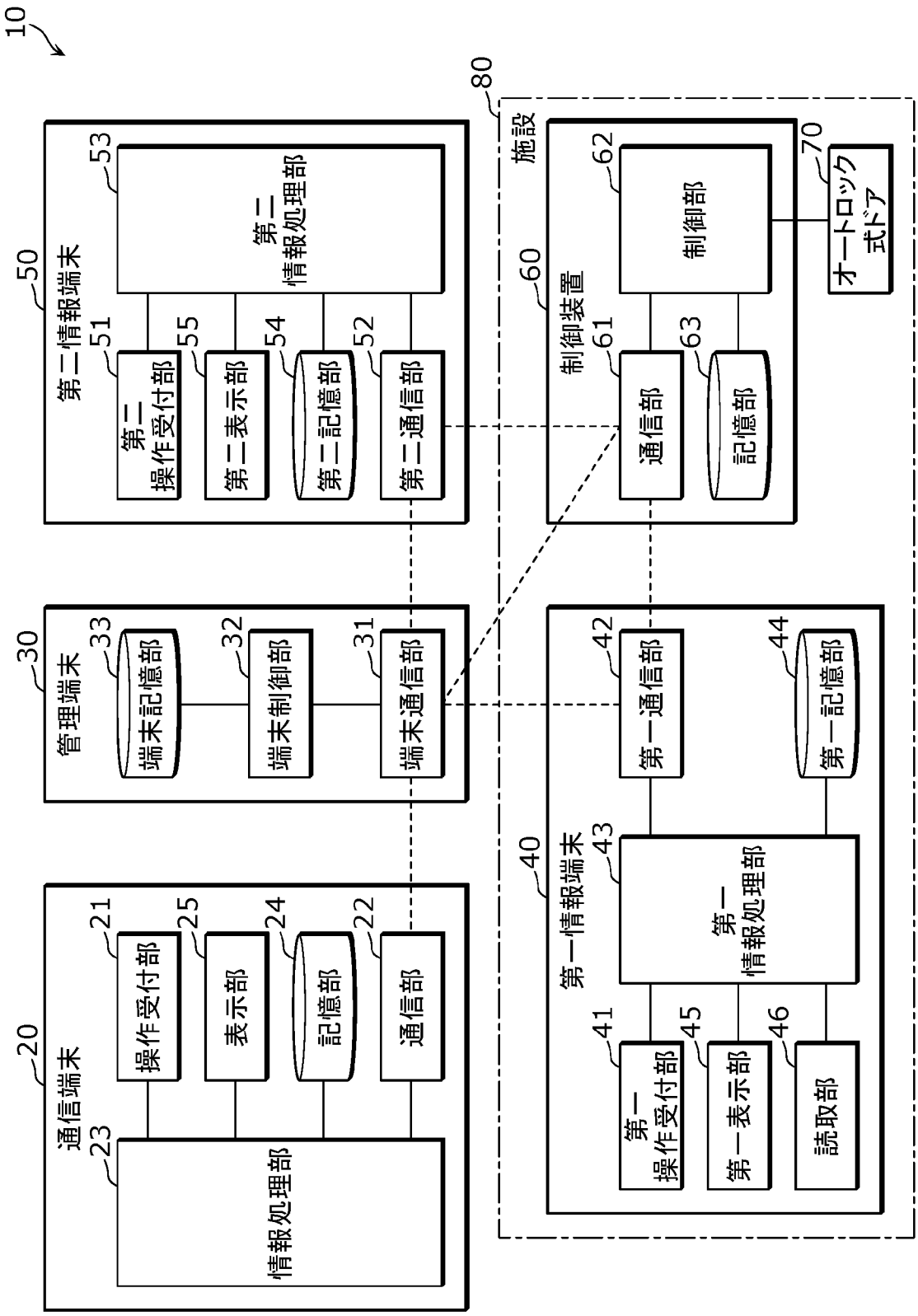
情報処理方法。

[請求項8] 請求項７に記載の情報処理方法をコンピュータに実行させるためのプログラム。

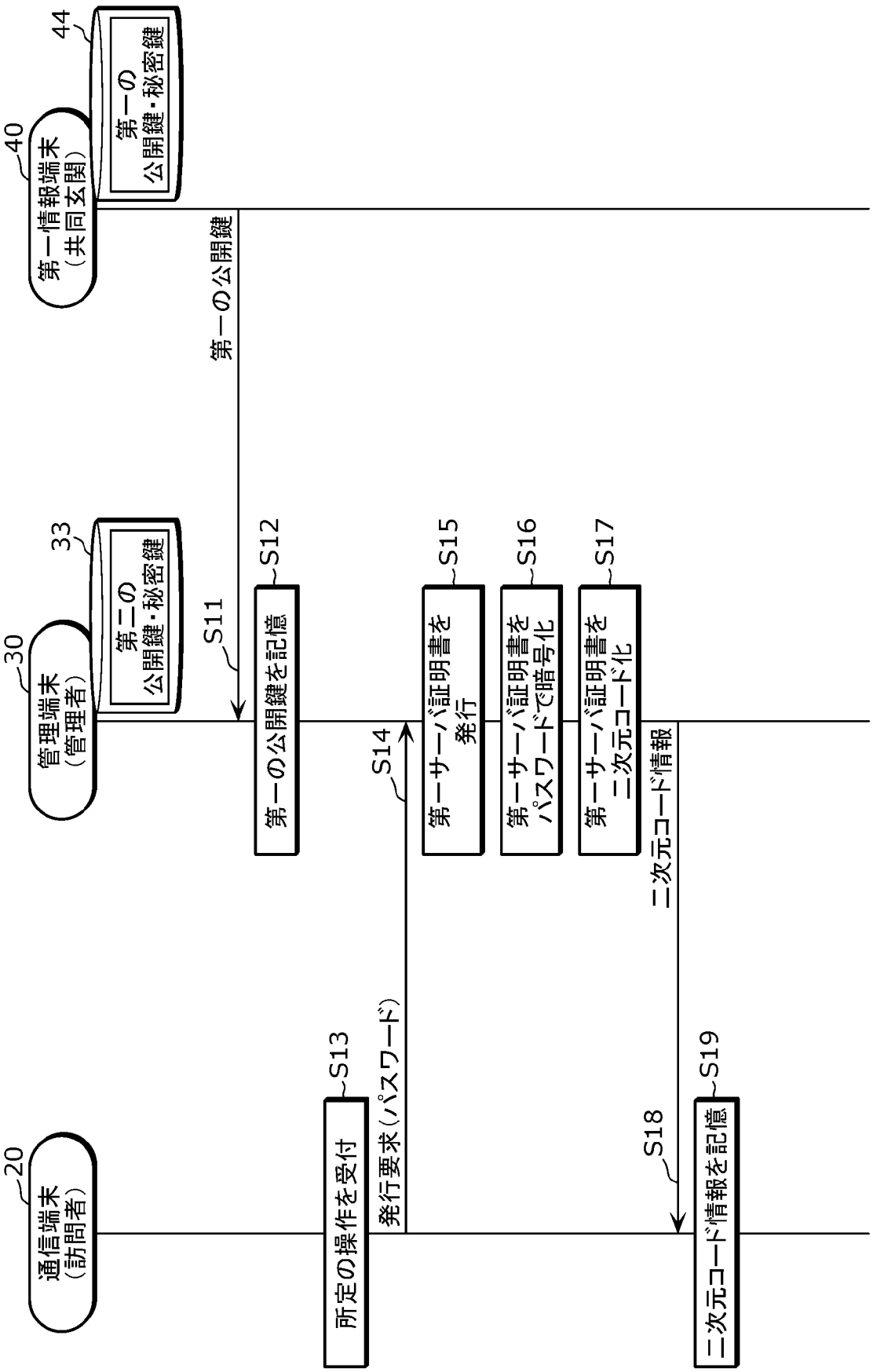
[図1]



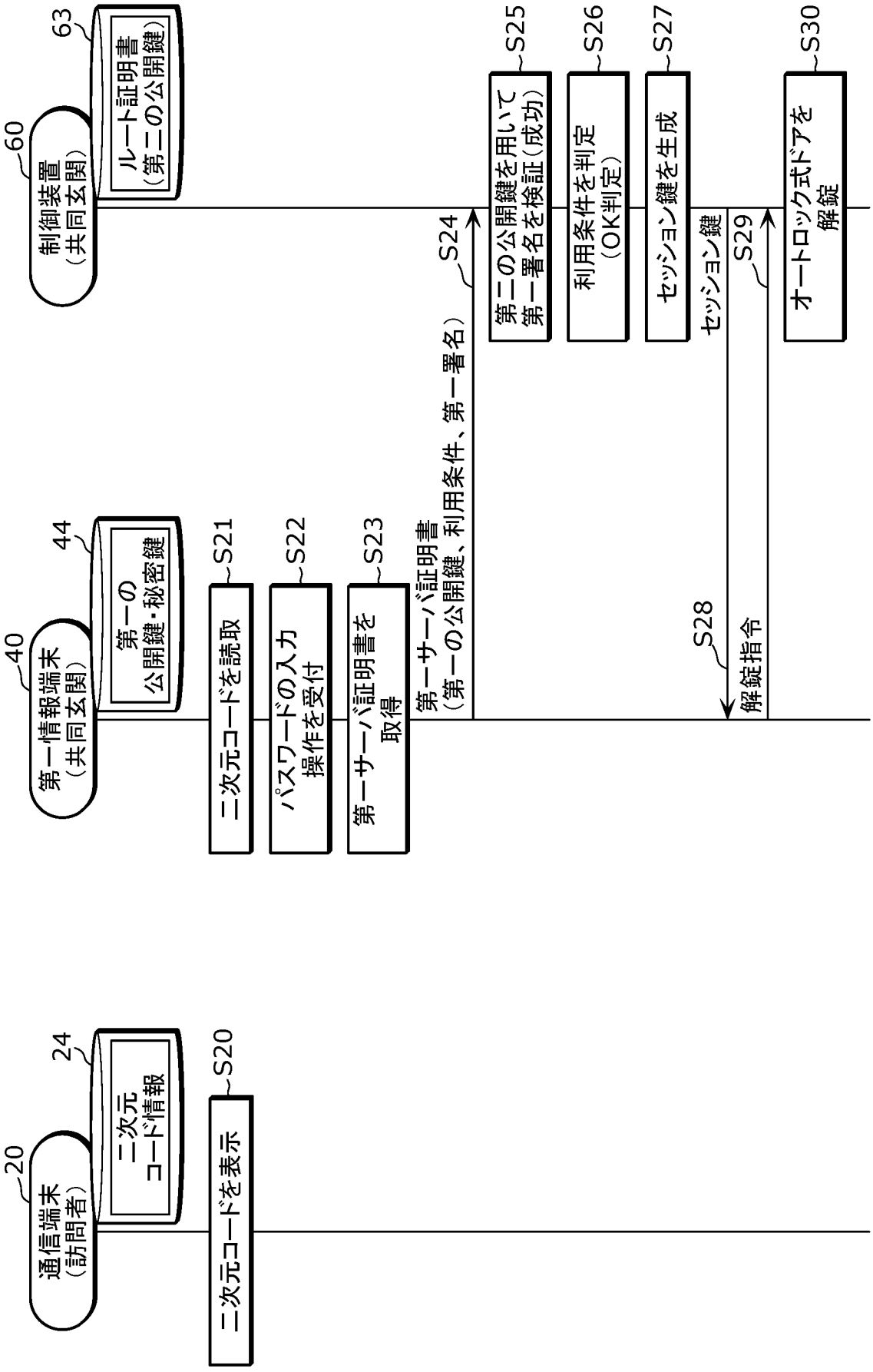
[図2]


10
80
施設
50
第二情報端末
53
第二
情報処理部
51
第二
操作受付部
55
第二表示部
54
第二記憶部
52
第二通信部
60
制御装置
62
制御部
70
オートロック
式ドア
61
通信部
63
記憶部
30
管理端末
33
端末記憶部
32
端末制御部
31
端末通信部
42
第一通信部
44
第一記憶部
40
第一情報端末
43
第一
情報処理部
41
第一
操作受付部
45
第一表示部
46
読取部
20
通信端末
21
操作受付部
25
表示部
24
記憶部
22
通信部
23
情報処理部

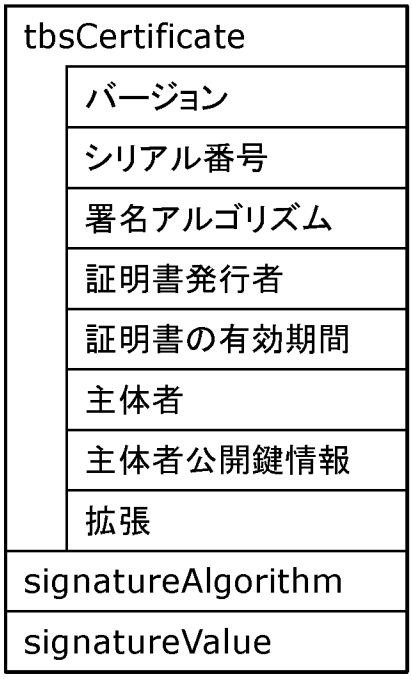
[図3]


第一情報端末
（共同玄関）
40
第一の
公開鍵・秘密鍵
44
第一の公開鍵
管理端末
（管理者）
30
第二の
公開鍵・秘密鍵
33
S11
S12
第一の公開鍵を記憶
S14
S15
第一サーバ証明書を
発行
S16
第一サーバ証明書を
パスワードで暗号化
S17
第一サーバ証明書を
二次元コード化
二次元コード情報
通信端末
（訪問者）
20
所定の操作を受付
S13
発行要求（パスワード）
S18
S19
二次元コード情報を記憶

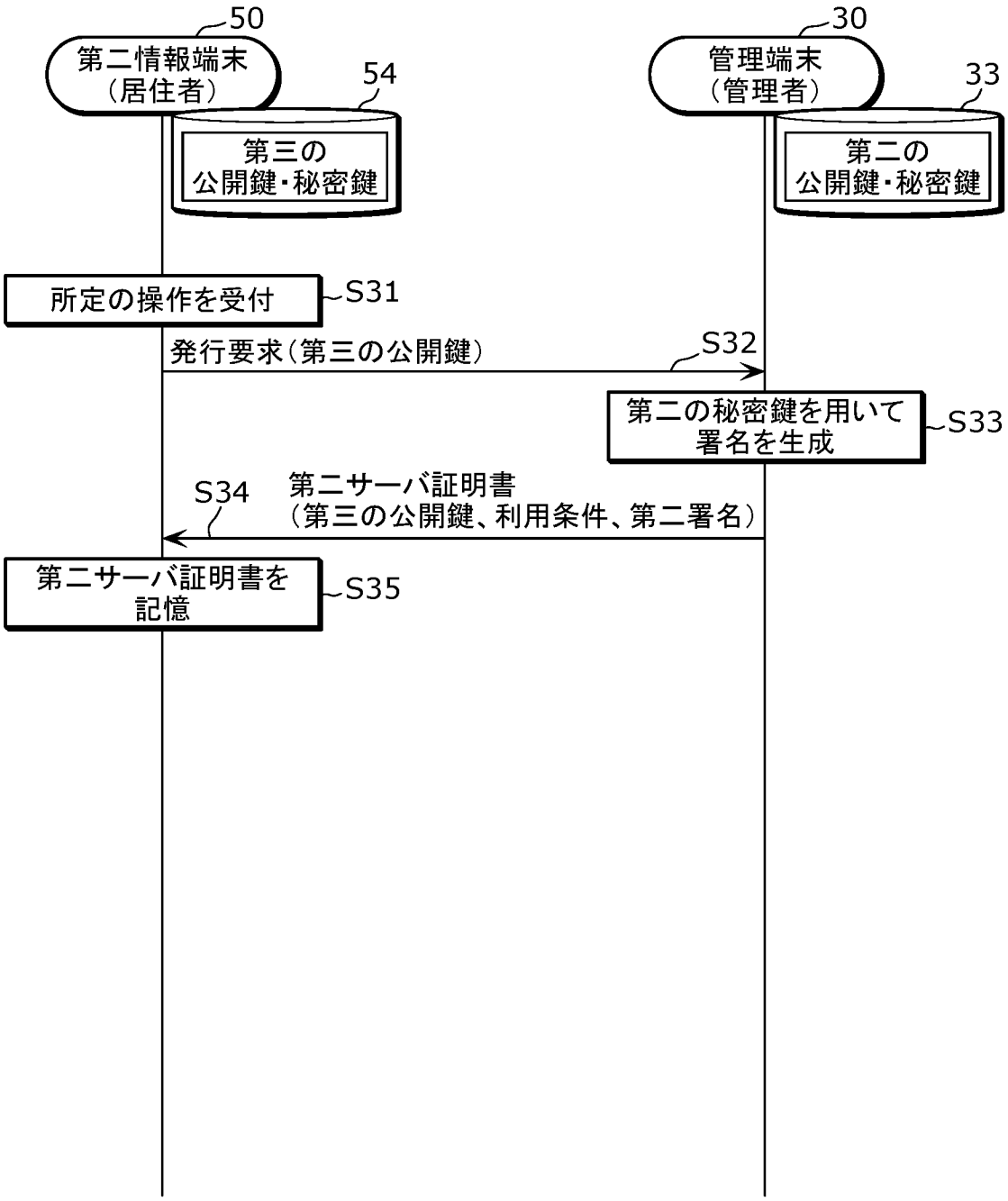
[図4]


通信端末
（訪問者）
20
二次元
コード情報
24
二次元コードを表示
S20
第一情報端末
（共同玄関）
40
第一の
公開鍵・秘密鍵
44
二次元コードを読取
S21
パスワードの入力
操作を受付
S22
第一サーバ証明書を
取得
S23
第一サーバ証明書
（第一の公開鍵、利用条件、第一署名）
S24
制御装置
（共同玄関）
60
ルート証明書
（第二の公開鍵）
63
第二の公開鍵を用いて
第一署名を検証（成功）
S25
利用条件を判定
（OK判定）
S26
セッション鍵を生成
S27
セッション鍵
S28
解錠指令
S29
オートロック式ドアを
解錠
S30

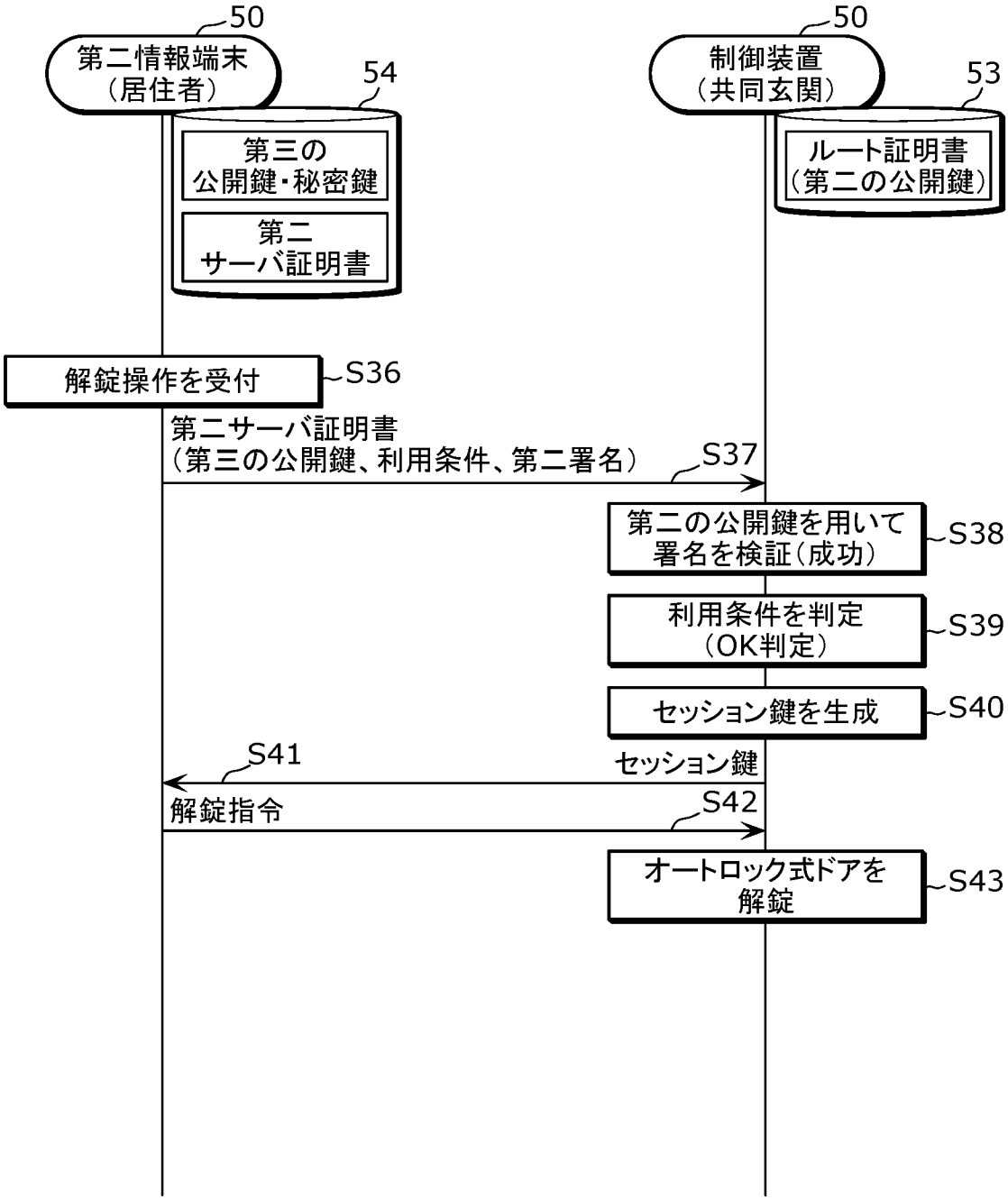
[図5]


tbsCertificate
バージョン
シリアル番号
署名アルゴリズム
証明書発行者
証明書の有効期間
主体者
主体者公開鍵情報
拡張
signatureAlgorithm
signatureValue

[図6]


50
第二情報端末
（居住者）
54
第三の
公開鍵・秘密鍵
30
管理端末
（管理者）
33
第二の
公開鍵・秘密鍵
所定の操作を受付
S31
発行要求（第三の公開鍵）
S32
第二の秘密鍵を用いて
署名を生成
S33
S34
第二サーバ証明書
（第三の公開鍵、利用条件、第二署名）
第二サーバ証明書を
記憶
S35

[図7]


50
第二情報端末
（居住者）
54
第三の
公開鍵・秘密鍵
第二
サーバ証明書
50
制御装置
（共同玄関）
53
ルート証明書
（第二の公開鍵）
解錠操作を受付
S36
第二サーバ証明書
（第三の公開鍵、利用条件、第二署名）
S37
第二の公開鍵を用いて
署名を検証（成功）
S38
利用条件を判定
（OK判定）
S39
セッション鍵を生成
S40
S41
セッション鍵
解錠指令
S42
オートロック式ドアを
解錠
S43

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2022/047605

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32(2006.01)i; ***E05B 49/00***(2006.01)i; ***G06F 21/33***(2013.01)i; ***H04L 9/08***(2006.01)i
FI: H04L9/32 200B; G06F21/33; E05B49/00 L; H04L9/08 F

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L9/32; E05B49/00; G06F21/33; H04L9/08

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 1971-2023
Registered utility model specifications of Japan 1996-2023
Published registered utility model applications of Japan 1994-2023

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 2019-176441 A (SECOM CO., LTD.) 10 October 2019 (2019-10-10) abstract	1-8
A	JP 2019-173523 A (SECOM CO., LTD.) 10 October 2019 (2019-10-10) abstract	1-8
A	JP 2016-148920 A (DAI NIPPON PRINTING CO., LTD.) 18 August 2016 (2016-08-18) paragraphs [0029], [0031]	1-8

☐ 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
02 February 2023	**14 February 2023**
Name and mailing address of the ISA/JP **Japan Patent Office (ISA/JP)** **3-4-3 Kasumigaseki, Chiyoda-ku, Tokyo 100-8915** **Japan**	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/JP2022/047605

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
JP 2019-176441 A	10 October 2019	(Family: none)	
JP 2019-173523 A	10 October 2019	(Family: none)	
JP 2016-148920 A	18 August 2016	(Family: none)	

国際調査報告

国際出願番号
PCT/JP2022/047605

A. 発明の属する分野の分類（国際特許分類（ＩＰＣ））

H04L 9/32(2006.01)i; E05B 49/00(2006.01)i; G06F 21/33(2013.01)i; H04L 9/08(2006.01)i
FI: H04L9/32 200B; G06F21/33; E05B49/00 L; H04L9/08 F

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））

H04L9/32; E05B49/00; G06F21/33; H04L9/08

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２０２３年
日本国実用新案登録公報	１９９６－２０２３年
日本国登録実用新案公報	１９９４－２０２３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 2019-176441 A (セコム株式会社) 10.10.2019 (2019-10-10) [要約]	1-8
A	JP 2019-173523 A (セコム株式会社) 10.10.2019 (2019-10-10) [要約]	1-8
A	JP 2016-148920 A (大日本印刷株式会社) 18.08.2016 (2016-08-18) 段落[0029],[0031]	1-8

☐ 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抵触するものではなく、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
02.02.2023	14.02.2023

名称及びあて先
日本国特許庁(ISA/JP)
〒100-8915
日本国
東京都千代田区霞が関三丁目４番３号

権限のある職員（特許庁審査官）
平井　誠 5S 9071

電話番号 03-3581-1101 内線 3546

国際調査報告
パテントファミリーに関する情報

国際出願番号
PCT/JP2022/047605

引用文献	公表日	パテントファミリー文献	公表日
JP 2019-176441 A	10.10.2019	（ファミリーなし）	
JP 2019-173523 A	10.10.2019	（ファミリーなし）	
JP 2016-148920 A	18.08.2016	（ファミリーなし）	