(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2019-176441
(P2019-176441A)
(43)公開日　令和1年10月10日(2019.10.10)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/32	(2006.01)	H04L	9/00	675B	2E250
E05B 49/00	(2006.01)	E05B	49/00	J	5J104
H04L 9/08	(2006.01)	H04L	9/00	675D	
		H04L	9/00	601F	

審査請求 未請求　請求項の数 7　OL　（全 15 頁）

(21)出願番号　特願2018-66095(P2018-66095)
(22)出願日　平成30年3月29日(2018.3.29)

（特許庁注：以下のものは登録商標）
1．ＺＩＧＢＥＥ

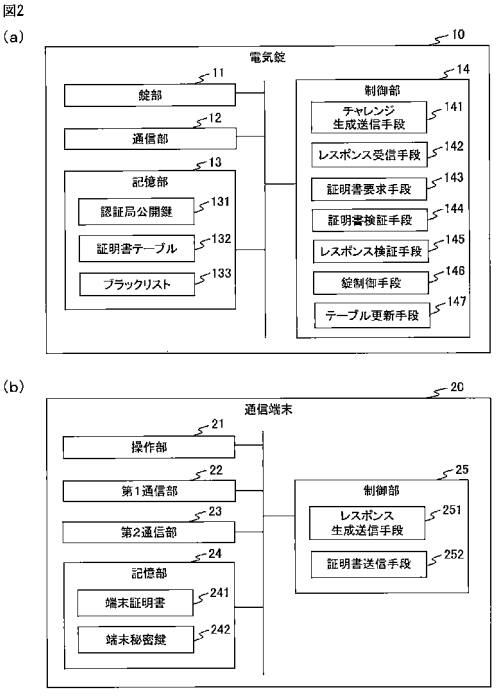
(71)出願人　000108085
セコム株式会社
東京都渋谷区神宮前一丁目５番１号
(74)代理人　100099759
弁理士　青木　篤
(74)代理人　100123582
弁理士　三橋　真二
(74)代理人　100114018
弁理士　南山　知広
(74)代理人　100180806
弁理士　三浦　剛
(72)発明者　下村　武史
東京都三鷹市下連雀八丁目１０番１６号
セコム株式会社内

最終頁に続く

(54)【発明の名称】電気錠

(57)【要約】　（修正有）
【課題】錠の施解錠の制御要求を受けてから錠の制御までのレスポンスタイムを短くし、バッテリへの負荷を軽減できる電気錠を提供する。
【解決手段】錠の施解錠を制御する電気錠は、認証局公開鍵１３１を記憶した記憶部１３と、チャレンジを生成して通信端末に送信するチャレンジ生成送信手段１４１と、通信端末から端末証明書ＩＤとチャレンジに対するレスポンスとを受信するレスポンス受信手段１４２と、受信した証明書ＩＤに対応する端末公開鍵が記憶部に記憶されていない場合、端末証明書の送信要求を通信端末に送信する証明書要求手段１４３と、通信端末から受信し正当であると検証した端末証明書が有する端末公開鍵を当該端末証明書の証明書ＩＤと対応付けて記憶部に記憶する証明書検証手段１４４と、記憶部に記憶されている端末公開鍵を用いて、受信したレスポンスが正当なレスポンスであると検証した場合、錠を制御する錠制御手段１４６と、を有する。
【選択図】図２

図2



【特許請求の範囲】
【請求項１】
通信端末と通信して錠の施解錠を制御する電気錠であって、
少なくとも認証局の認証局公開鍵を記憶した記憶部と、
前記通信端末から受信した錠の施解錠の制御要求に応じてチャレンジを生成して前記通信端末に送信するチャレンジ生成送信手段と、
前記通信端末から前記認証局により発行された端末証明書の証明書ＩＤと前記チャレンジに対するレスポンスとを受信するレスポンス受信手段と、
前記受信した証明書ＩＤに対応する端末公開鍵が前記記憶部に記憶されていない場合に前記端末証明書の送信要求を前記通信端末に送信する証明書要求手段と、
前記送信要求に応じて前記通信端末から送信された前記端末証明書を受信し、当該端末証明書が正当であるか否かを前記認証局公開鍵を用いて検証し、正当な端末証明書が有する端末公開鍵を当該端末証明書の証明書ＩＤと対応付けて前記記憶部に記憶させる証明書検証手段と、
前記レスポンスが正当か否かを、前記受信した証明書ＩＤに対応する端末公開鍵を用いて検証するレスポンス検証手段と、
前記レスポンスが正当な場合、前記制御要求に従って前記錠の施解錠を制御する錠制御手段と、を有する電気錠。
【請求項２】
前記記憶部は、前記錠の制御を禁止する端末証明書の証明書ＩＤを記したリスト情報を更に記憶し、
前記錠制御手段は、前記受信した証明書ＩＤが前記リスト情報に記されている場合、前記錠を制御しない、請求項１に記載の電気錠。
【請求項３】
前記リスト情報に登録された証明書ＩＤと対応付けて記憶された前記端末公開鍵を、前記記憶部から消去する消去手段を有する、請求項２に記載の電気錠。
【請求項４】
前記記憶部に記憶された前記端末公開鍵のうち、前記レスポンスが正しいと検証されたタイミングが古い端末公開鍵であるほど優先して前記記憶部から消去する消去手段を有する、請求項１～３のいずれか一項に記載の電気錠。
【請求項５】
前記証明書検証手段は、前記正当な端末証明書の有効期間を当該端末証明書の証明書ＩＤと対応付けて前記記憶部に更に記憶させ、
前記有効期間が終了している証明書ＩＤに対応付けて記憶されている端末公開鍵を前記記憶部から消去する消去手段を有する、請求項１～４のいずれか一項に記載の電気錠。
【請求項６】
前記端末証明書は、前記通信端末が属する端末グループを識別するグループＩＤを有し、
前記証明書検証手段は、前記正当な端末証明書が有するグループＩＤを、当該端末証明書の証明書ＩＤに対応付けて前記記憶部に更に記憶させ、
正当な前記レスポンスとともに受信された証明書ＩＤに対応するグループＩＤと異なるグループＩＤに対応付けて記憶された前記端末公開鍵を前記記憶部から消去する消去手段を有する、請求項１～５のいずれか一項に記載の電気錠。
【請求項７】
電源ＯＦＦ状態から電源ＯＮ状態に移行するとき、前記記憶部に記憶された全ての端末公開鍵を消去する消去手段を有する、請求項１～６のいずれか一項に記載の電気錠。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、電気錠に関する。

【背景技術】
【０００２】
近年、玄関の扉などの錠を、近接したスマートフォンなどの通信端末と無線通信することにより解錠制御を行う電気錠が提案されている。このような電気錠では、通信端末の公開鍵を用いて通信端末との間で安全な通信を行い通信端末の認証および解錠制御を行う。例えば、特許文献１には、認証局が発行した公開鍵証明書の端末公開鍵を用いてチャレンジレスポンス認証を行い電気錠の解錠を制御する方式が開示されている。
【先行技術文献】
【特許文献】
【０００３】
【特許文献１】特開２０１６－１１１７０４号公報
【発明の概要】
【発明が解決しようとする課題】
【０００４】
しかしながら、特許文献１に記載されている電気錠では、解錠制御を行うごとに、通信端末から送信された公開鍵証明書が信頼できる認証局から発行されたものであることを検証するための証明書検証処理と、電気錠が送信したチャレンジに署名して返信されたレスポンスが正当であることを検証するための署名データ検証処理との２種類の検証処理を行う必要がある。これらの検証処理では、公開鍵暗号方式を用いるため計算負荷が増大し、解錠までに要する時間（レスポンスタイム）が長くなったり、電気錠の電池寿命が短くなるといった問題があった。また、施錠要求に対する施錠においても同様の問題が生じる。
【０００５】
本発明の目的は、錠の施解錠の制御要求を受けてから錠の施解錠を制御（施錠または解錠）するまでのレスポンスタイムを短くし、バッテリへの負荷を軽減できる電気錠を提供することである。
【課題を解決するための手段】
【０００６】
かかる課題を解決するための本発明の一つの態様によれば、通信端末と通信して錠の施解錠を制御する電気錠が提供される。かかる電気錠は、少なくとも認証局の認証局公開鍵を記憶した記憶部と、通信端末から受信した錠の施解錠の制御要求に応じてチャレンジを生成して通信端末に送信するチャレンジ生成送信手段と、通信端末から認証局により発行された端末証明書の証明書ＩＤとチャレンジに対するレスポンスとを受信するレスポンス受信手段と、受信した証明書ＩＤに対応する端末公開鍵が記憶部に記憶されていない場合に端末証明書の送信要求を通信端末に送信する証明書要求手段と、送信要求に応じて通信端末から送信された端末証明書を受信し、当該端末証明書が正当であるか否かを認証局公開鍵を用いて検証し、正当な端末証明書が有する端末公開鍵を当該端末証明書の証明書ＩＤと対応付けて記憶部に記憶させる証明書検証手段と、レスポンスが正当か否かを、受信した証明書ＩＤに対応する端末公開鍵を用いて検証するレスポンス検証手段と、レスポンスが正当な場合、前記制御要求に従って錠の施解錠を制御する錠制御手段と、を有する。
【０００７】
この電気錠において、記憶部は、錠の制御を禁止する端末証明書の証明書ＩＤを記したリスト情報を更に記憶し、錠制御手段は、受信した証明書ＩＤがリスト情報に記されている場合、錠を制御しないことが好ましい。
【０００８】
この電気錠において、リスト情報に登録された証明書ＩＤと対応付けて記憶された端末公開鍵を、記憶部から消去する消去手段を有することが好ましい。
【０００９】
この電気錠において、記憶部に記憶された端末公開鍵のうち、レスポンスが正しいと検証されたタイミングが古い端末公開鍵であるほど優先して記憶部から消去する消去手段を有することが好ましい。

【００１０】
この電気錠において、証明書検証手段は、正当な端末証明書の有効期間を当該端末証明書の証明書ＩＤと対応付けて記憶部に更に記憶させ、有効期間が終了している証明書ＩＤに対応付けて記憶されている端末公開鍵を記憶部から消去する消去手段を有することが好ましい。
【００１１】
この電気錠において、端末証明書は、通信端末が属する端末グループを識別するグループＩＤを有し、証明書検証手段は、正当な端末証明書が有するグループＩＤを、当該端末証明書の証明書ＩＤに対応付けて記憶部に更に記憶させ、正当なレスポンスとともに受信された証明書ＩＤに対応するグループＩＤと異なるグループＩＤに対応付けて記憶された端末公開鍵を記憶部から消去する消去手段を有することが好ましい。
【００１２】
この電気錠において、電源ＯＦＦ状態から電源ＯＮ状態に移行するとき、記憶部に記憶された全ての端末公開鍵を消去する消去手段を有することが好ましい。
【発明の効果】
【００１３】
本発明に係る電気錠によれば、錠の施解錠の制御要求を受けてから錠の施解錠を制御（施錠または解錠）するまでのレスポンスタイムを短くし、バッテリへの負荷を軽減することが可能となる。
【図面の簡単な説明】
【００１４】
【図１】本発明の一実施形態に係る電気錠システム１の全体構成図である。
【図２】電気錠システム１における電気錠１０および通信端末２０の構成図である。
【図３】証明書テーブルおよび端末証明書の構造の一例を示す図である。
【図４】電気錠１０による解錠制御処理を示すフローチャートである。
【図５】図４における証明書テーブルの更新処理を示すフローチャートである。
【図６】通信端末２０による解錠要求処理を示すフローチャートである。
【００１５】
以下、本発明を、住居、民泊の物件、レンタル倉庫などの施設への入場を規制するため設置された電気錠を管理する電気錠システムに適用した一実施形態について添付の図面を参照しつつ説明する。ただし、本発明は図面または以下に記載される実施形態には限定されないことを理解されたい。
【００１６】
図１は、本発明の一実施形態に係る電気錠システム１の全体構成図である。図１に示すように、電気錠システム１は、電気錠１０、通信端末２０および管理サーバ３０を有する。電気錠１０と通信端末２０との間は近距離通信によって接続され、通信端末２０と管理サーバ３０との間は無線通信や広域通信網などを有する通信網９０を介して接続される。
電気錠１０は、施設への入場を規制するため施設の入口の扉などに設置され、施解錠を制御するマイクロコントローラなどの情報処理装置を有する。電気錠１０は、通信端末２０から解錠要求を受信したとき、通信端末２０の公開鍵（端末公開鍵）を用いて通信端末２０が解錠権限を有する正当な通信端末であると認証すると解錠する。
通信端末２０は、施設の利用者によって所持され、利用者が電気錠１０の解錠要求などの操作を行うのに用いるスマートフォン、タブレットなどの携帯型情報処理端末である。図１に示すように、一つの通信端末２０－１が複数の電気錠１０－１および１０－２の解錠権限を有してもよく、一つの電気錠１０－２に対して複数の通信端末２０－１および２０－２が解錠権限を有してもよい。
管理サーバ３０は、電気錠システム１を管理するデータベースサーバ、ウェブサーバなどの情報処理装置であり、電気錠システム１に関するデータベースの管理、通信端末２０の端末公開鍵に対応する公開鍵証明書（端末証明書）の発行、失効した端末証明書を示すブラックリスト（リスト情報）の管理などを行う。次に、これらの装置の構成について詳

述する。

【００１７】

図２（ａ）は、電気錠システム１における電気錠１０の構成図である。

図２（ａ）に示すように、電気錠１０は、錠部（錠）１１、通信部１２、記憶部１３および制御部１４を有し、図示しないバッテリからの電力供給によって動作する。

【００１８】

錠部１１は、制御部１４から受信した解錠／施錠指示に従ってモータを駆動することにより解錠／施錠動作を実行する。なお、錠部１１は、電気錠１０とは別個の装置でもよく、この場合、有線／無線通信で接続された電気錠１０から解錠／施錠指示を受信する。

【００１９】

通信部１２は、通信端末２０と近距離通信を行う通信インターフェイスであり、ＢＬＥ（Bluetooth（登録商標） Low Energy）、ＺｉｇＢｅｅ、ＩＥＥＥ８０２．１１、Ｚ－Ｗａｖｅなど、通信端末２０が有する無線通信規格の少なくとも一つに準ずる。例えば、ＢＬＥに準ずる場合、通信部１２は、１回／秒など定期的に電気錠１０の錠識別情報（電気錠ＩＤ）などを有するアドバタイズ信号を周囲にブロードキャストし、このアドバタイズ信号に応答して通信接続を要求してきた通信端末２０と通信接続する。以下、電気錠１０と通信端末２０との間の通信はＢＬＥに準ずるものとして説明する。

【００２０】

記憶部１３は、電気錠１０上で実行されるコンピュータプログラムのコードおよびデータを記憶し、ＲＡＭ、ＲＯＭ、ＥＰＲＯＭおよび／またはフラッシュメモリなどの任意の記憶装置を有する。記憶部１３に記憶されるコードおよびデータは、製造時に予め記憶されたり、可搬記憶媒体、通信部１２、操作部（図示せず）などを介して提供されて記憶させることができる。

記憶部１３は、認証局公開鍵１３１、証明書テーブル１３２およびブラックリスト１３３を記憶する。

【００２１】

認証局公開鍵１３１は、端末証明書を発行する認証局としての機能を有する管理サーバ３０の公開鍵であり、通信端末２０から受信した端末証明書が管理サーバ３０によって発行された正当なものであるか否かを検証するのに用いられる。端末証明書を発行する管理サーバ３０が複数ある場合、複数の認証局公開鍵１３１を、管理サーバ３０を識別する認証局ＩＤに対応付けて記憶してもよい。認証局公開鍵１３１は、電気錠１０の工場出荷時や施設への設置時などに記憶部１３に予め記憶される。なお、記憶部１３は、認証局公開鍵１３１の代わりに、管理サーバ３０が発行した認証局公開鍵が記された認証局証明書を記憶してもよい。

【００２２】

証明書テーブル１３２は、通信端末２０から受信し認証局公開鍵にて正当なものであると検証された端末証明書が有する端末公開鍵と、当該端末証明書の証明書ＩＤと、を少なくとも対応付けて記憶するテーブルである。

図３（ａ）は、証明書テーブル１３２の構造の一例を示す図である。図３（ａ）に示すように、証明書テーブル１３２は、通信端末２０から受信し認証局公開鍵にて検証された端末証明書が有する端末公開鍵、有効期間およびグループＩＤと、後述する検証最新度と、を有する証明書情報を、当該端末証明書の証明書ＩＤに対応付けて記憶するテーブルである。

証明書ＩＤは、管理サーバ３０から通信端末２０に対して発行された端末証明書を電気錠システム１で一意に識別するＩＤである。端末証明書を発行する管理サーバ３０が複数ある場合、管理サーバ３０ごとに一意に割り当てられた証明書ＩＤと電気錠システム１において管理サーバ３０を一意に識別する認証局ＩＤとを併せて証明書ＩＤとしてもよい。

端末公開鍵は、通信端末２０が記憶する端末秘密鍵２４２と対となる公開鍵であり、チャレンジレスポンス認証で電気錠１０がレスポンスの正当性を認証するのに用いられる。

有効期間は、端末証明書２４１の有効期間を終了日時または開始および終了日時などで

示し、通信端末２０が端末公開鍵によって電気錠１０を解錠できる期間を示す。
グループＩＤは、端末証明書２４１の発行対象である通信端末２０が属するグループを電気錠システム１において一意に識別するＩＤである。ここで、グループとは、例えば家族や団体などのように、特定の電気錠１０に対して解錠が許可された複数の人々からなる集団のことをいう。例えば、ホテルの一部屋に同時に複数の利用者が宿泊する場合、当該利用者が所持する通信端末２０の端末証明書２４１には、同じグループＩＤが付与される。後述するように、新たなグループＩＤが記された端末証明書２４１を有する通信端末２０からの解錠要求の認証が成功すると、電気錠１０は、証明書テーブル１３２から既存のグループＩＤに対応する証明書情報を消去する。これにより、既存のグループＩＤが示すグループに属する通信端末２０は、電気錠１０の解錠を行えなくすることができる。なお、図３（ａ）において“－”で示されるグループＩＤは、管理者や清掃員など有効期間内であればグループに関係なく解錠が許可される利用者の通信端末２０に対して付与される。
検証最新度は、証明書テーブル１３２から証明書情報を消去する際に参照される情報であり、後述するように検証最新度が低い証明書情報が優先的に消去される。
【００２３】
ブラックリスト１３３は、失効した端末証明書の証明書ＩＤを記したリストであり、管理サーバ３０によって更新される。電気錠１０は、管理サーバ３０と通信可能な場合は管理サーバ３０から直接、そうでない場合は管理サーバ３０から通信端末２０を経由して、ブラックリスト１３３を受信して記憶部１３に記憶する。
【００２４】
制御部１４は、プロセッサおよび周辺回路を有し、当該プロセッサは、記憶部１３に記憶されたコンピュータプログラムのコードを実行することによって電気錠１０が行う種々の動作を実現する。記憶部１３および制御部１４は、半導体メモリとプロセッサとが一体化されたマイクロコントローラを有してもよい。制御部１４は、錠部１１に解錠／施錠指示を送信して錠部１１の解錠／施錠を制御し、通信部１２を介して通信端末２０とデータの送受信を行う。
制御部１４は、コンピュータプログラムにより実現される動作の機能モジュールとして、チャレンジとして乱数を生成して通信端末２０に送信するチャレンジ生成送信手段１４１と、チャレンジに対して通信端末２０から送信されたレスポンスおよび証明書ＩＤを受信するレスポンス受信手段１４２と、通信端末２０に端末証明書を送信するよう要求する証明書要求手段１４３と、通信端末２０から受信し正当であると検証した端末証明書の情報を証明書テーブル１３２に記憶する証明書検証手段１４４と、通信端末２０から受信したレスポンスを検証するレスポンス検証手段１４５と、レスポンス検証手段１４５の検証結果に従って錠部１１の解錠を制御する錠制御手段１４６と、証明書テーブル１３２から所定の証明書情報を消去し検証最新度を更新するテーブル更新手段（消去手段）１４７と、を有する。各手段の動作については、後の電気錠１０による解錠制御処理の説明にて詳述する。
【００２５】
図２（ｂ）は、電気錠システム１における通信端末２０の構成図である。
図２（ｂ）に示すように、通信端末２０は、操作部２１、第１通信部２２、第２通信部２３、記憶部２４および制御部２５を有する。
【００２６】
操作部２１は、データの入出力が行われるタッチパネル、ボタン、マイクなどを有する利用者とのユーザインターフェイスである。
【００２７】
第１通信部２２は、電気錠１０と近距離通信を行う通信インターフェイスであり、電気錠１０が通信端末２０との近距離通信に用いる無線通信規格に準じた通信を行う。第１通信部２２は、周囲の装置から発信されるアドバタイズ信号をスキャンし、所望の電気錠１０の電気錠ＩＤを有するアドバタイズ信号を発信する電気錠１０を見つけると、この電気

錠１０に対して通信接続を要求して当該電気錠１０と通信接続する。
【００２８】
第２通信部２３は、通信網９０を介して管理サーバ３０と通信を行う通信インターフェイスであり、ＩＥＥＥ８０２．１１、Ｗ－ＣＤＭＡ、ＣＤＭＡ２０００またはＬＴＥなどの無線通信規格により通信網９０に接続する。そして、第２通信部２３は、接続した通信網９０を介して、専用回線やインターネットなどにより通信網９０に接続された管理サーバ３０とＳＳＬ／ＴＬＳ、ＩＰＳｅｃなどの通信プロトコルにより安全な通信を行う。
【００２９】
記憶部２４は、通信端末２０上で実行されるコンピュータプログラムのコードおよびデータを記憶し、ＲＡＭ、ＲＯＭ、ＥＰＲＯＭなどの任意の半導体メモリを有することができる。また、記憶部２４は、フラッシュメモリ、磁気記憶装置、光学記憶装置などの任意の記憶装置を有してもよい。記憶部２４に記憶されるコードおよびデータは、製造時に予め記憶させられたり、フラッシュメモリ、磁気記憶媒体、光学記憶媒体などの可搬記憶媒体、操作部２１、第２通信部２３などを介して記憶される。
記憶部２４は、端末証明書２４１および端末秘密鍵２４２を記憶する。なお、一つの通信端末２０が複数の電気錠１０の解錠権限を有する場合、電気錠１０ごとに端末証明書２４１および当該端末証明書２４１に対応する端末秘密鍵２４２を記憶する。
【００３０】
端末証明書２４１は、電気錠１０が記憶する認証局公開鍵１３１に対応する認証局（管理サーバ３０）から、端末秘密鍵２４２に対応する端末公開鍵に対して電子署名されることにより、発行された公開鍵証明書である。端末証明書２４１は、管理サーバ３０によって、通信端末２０が電気錠１０の解錠権限を有する正当な通信端末であることを確認されたとき、管理サーバ３０によって発行される。例えば、施設の利用前に、利用者が、操作部２１により管理サーバ３０が運営する証明書発行サイトにアクセスするなどして、通信端末２０で生成された端末公開鍵や利用者の情報などを有する証明書発行要求を管理サーバ３０に送信する。管理サーバ３０は、証明書発行要求を受信したとき、当該利用者が施設の利用条件を満たしていることを確認した上で端末証明書を発行し、通信端末２０に送信する。通信端末２０は、管理サーバ３０から受信した端末証明書を記憶部２４の端末証明書２４１として記憶する。端末証明書の発行については、後の管理サーバ３０の説明にて詳述する。
図３（ｂ）は、端末証明書の構造の一例を示す図である。図３（ｂ）に示すように、端末証明書２４１は、証明書ＩＤ、認証局ＩＤ、電気錠ＩＤ、端末公開鍵、有効期間、グループＩＤおよび署名を有する。また、端末証明書２４１は、通信端末ＩＤなどの他の情報を有してもよく、ＩＴＵ－ＴにおけるＰＫＩの規格Ｘ．５０９などに準じてもよい。
【００３１】
証明書ＩＤは、管理サーバ３０によって発行された端末証明書２４１に一意に割り当てられる端末証明書２４１を識別する情報である。
認証局ＩＤは、端末証明書２４１を発行した認証局である管理サーバ３０を電気錠システム１において一意に識別するための情報である。なお、端末証明書を発行する管理サーバ３０が一つである場合は、省略してもよい。
電気錠ＩＤは、端末証明書２４１の発行対象の通信端末２０が解錠権限を有する電気錠１０を、電気錠システム１において一意に識別する錠ＩＤである。
端末公開鍵、有効期間およびグループＩＤについては、前述の電気錠１０の証明書テーブル１３２の説明で詳述した通りである。
署名は、管理サーバ３０が、証明書ＩＤ、認証局ＩＤ、電気錠ＩＤ、端末公開鍵、有効期間およびグループＩＤなどの端末証明書２４１の各情報を署名対象として生成した電子署名であり、例えば、署名対象の各情報をＳＨＡ－２、ＳＨＡ－３などのハッシュ関数を用いて変換したハッシュ値を、管理サーバ３０の認証局秘密鍵を用いてＲＳＡ、ＥＣＤＳＡなどの公開鍵暗号方式で暗号化した値である。
【００３２】

端末秘密鍵２４２は、公開鍵暗号方式において端末証明書２４１が有する端末公開鍵と対となる秘密鍵であり、通信端末２０が、管理サーバ３０に端末証明書２４１の発行を要求する際に、管理サーバ３０に送信する端末公開鍵とともに生成して記憶部２４に記憶する。この端末秘密鍵２４２は、チャレンジレスポンス認証においてチャレンジに対するレスポンスを生成するのに用いられる。

【００３３】

制御部２５は、プロセッサおよび周辺回路を有し、当該プロセッサは、記憶部２４に記憶されたコンピュータプログラムのコードを実行することによって通信端末２０が行う種々の動作を実現する。記憶部２４および制御部２５はマイクロコントローラを有してもよい。制御部２５は、操作部２１を介して利用者とデータの入出力を行い、第１通信部２２を介して電気錠１０とデータの送受信を行い、第２通信部２３を介して管理サーバ３０とデータの送受信を行う。

制御部２５は、コンピュータプログラムにより実現される動作の機能モジュールとして、電気錠１０から受信したチャレンジに対するレスポンスを生成して証明書ＩＤとともに送信するレスポンス生成送信手段２５１と、電気錠１０から受信した証明書要求に対して端末証明書２４１を送信する証明書送信手段２５２と、を有する。各手段の動作については、後の通信端末２０による解錠要求処理の説明にて詳述する。

【００３４】

管理サーバ３０（図示せず）は、通信網９０を介して通信端末２０と通信する通信インターフェイスである通信部と、任意の記憶装置を有し管理サーバ３０上で実行されるコンピュータプログラムが用いるコードおよびデータを記憶する記憶部と、プロセッサを有し記憶部に記憶されたコンピュータプログラムを実行して管理サーバ３０が行う種々の動作を実現する制御部と、を有する。

管理サーバ３０は、施設、施設の利用者、施設の電気錠１０、利用者の通信端末２０およびその解錠権限などに関する情報をデータベースとして記憶部に記憶して管理し、情報の登録、変更、削除などを行う。このデータベースは、管理サーバ３０とは別個のデータベースサーバに記憶されてもよい。

【００３５】

また、管理サーバ３０は、通信端末２０からの証明書発行要求に応じて端末証明書を発行し、当該通信端末２０に送信する認証局の機能を有する。具体的には、通信端末２０において端末秘密鍵および端末公開鍵の鍵ペアが生成され、生成された端末公開鍵と通信端末２０の端末ＩＤなどとを有する証明書発行要求（ＣＳＲ）が管理サーバ３０に送信される。通信端末２０から証明書発行要求を受信すると、管理サーバ３０は、データベースを参照し、証明書発行要求が有する端末ＩＤに対して解錠が許可された電気錠１０に関する情報を検索する。管理サーバ３０の記憶部のデータベースには、端末ＩＤ、電気錠ＩＤ、有効期間、グループＩＤなどの解錠権限に関する情報が紐付けられて記憶されている。これらの情報は、所定の施設利用サービスの加入手続きに応じて管理者などにより登録されるものとする。管理サーバ３０は、データベースを検索した結果、端末ＩＤに対して解錠権限を有する電気錠１０に関する電気錠ＩＤ、有効期間、グループＩＤなどの情報と、証明書発行要求が有する端末公開鍵と、を用いて端末証明書を発行する。端末証明書の発行に際し、管理サーバ３０は認証局秘密鍵を用いる。この認証局秘密鍵は、公開鍵暗号方式における秘密鍵であり、電気錠１０の記憶部１３に記憶される認証局公開鍵１３１と対をなす。なお、一つの端末ＩＤについて複数の電気錠１０の情報がある場合は、電気錠１０ごとに端末証明書を発行する。この場合、通信端末２０が複数の電気錠１０のそれぞれに対応する証明書発行要求を送信し、各証明書発行要求に対応する端末証明書を管理サーバ３０が発行する。しかし、これに限らず、一つの証明書発行要求から当該複数の電気錠１０の端末証明書をそれぞれ発行してもよい。管理サーバ３０における認証局機能は、別個の認証局サーバによって実現されてもよい。

【００３６】

さらに、管理サーバ３０は、電気錠１０の解錠権限を有しなくなった通信端末２０の証

明書ＩＤを登録したブラックリストを管理する。管理サーバ３０は、通信端末２０の紛失や盗難、施設の利用中止などにより失効した端末証明書の証明書ＩＤをブラックリストに追加する。そして、管理サーバ３０は、電気錠１０と通信可能な場合、ブラックリストの更新後、数時間ごと～数日ごとなど定期的に、および／または電気錠１０からのブラックリストの要求時などに、通信網（図示せず）を介してブラックリストを電気錠１０に直接送信してもよい。また、管理サーバ３０は、電気錠１０と通信可能でない場合、通信網９０を介して通信端末２０にブラックリストを一旦送信しておき、通信端末２０が電気錠１０と通信する際に当該通信端末２０からブラックリストを電気錠１０に送信してもよい。

【００３７】

図４は、電気錠１０による解錠制御処理を示すフローチャートである。以下、図４を参照しつつ、電気錠１０の制御部１４による解錠制御処理について詳述する。電気錠１０では、通信端末２０から解錠要求を受信すると、以下の解錠制御処理が開始される。

【００３８】

通信端末２０から解錠要求を受信すると、制御部１４のチャレンジ生成送信手段１４１は、チャレンジとして乱数を生成して通信端末２０に送信し（Ｓ４０１）、レスポンス受信手段１４２は、送信したチャレンジに対するレスポンスと端末証明書の証明書ＩＤとを通信端末２０から受信する（Ｓ４０２のＹｅｓ）。

制御部１４は、受信した証明書ＩＤが記憶部１３のブラックリスト１３３に登録されているか否かを照合し（Ｓ４０３）、登録されている場合（Ｓ４０３のＹｅｓ）、解錠失敗を通信端末２０に送信して（Ｓ４１７）解錠制御処理を終了する。

【００３９】

証明書ＩＤがブラックリスト１３３に登録されていない場合（Ｓ４０３のＮｏ）、証明書要求手段１４３は、証明書ＩＤに対応付けられた証明書情報が既に証明書テーブル１３２に記憶されているか否かを確認し（Ｓ４０４）、まだ記憶されていない場合（Ｓ４０４のＮｏ）、通信端末２０に端末証明書の送信要求を送信して証明書ＩＤに対応する端末証明書を送信するよう要求する（Ｓ４０５）。

要求した端末証明書を通信端末２０から受信すると（Ｓ４０６のＹｅｓ）、証明書検証手段１４４は、現在時刻が受信した端末証明書が有する有効期間以内か否かを確認し（Ｓ４０７）、有効期間以内であれば（Ｓ４０７のＹｅｓ）、認証局公開鍵１３１を用いて端末証明書の署名を検証することにより、端末証明書が管理サーバ３０から発行された正当なものであるか否かを検証する（Ｓ４０８）。

【００４０】

証明書検証手段１４４は、受信した端末証明書が管理サーバ３０によって発行された正当なものであると検証された場合（Ｓ４０９のＹｅｓ）、証明書検証手段１４４は、端末証明書が有する端末公開鍵、有効期間、グループＩＤなどの証明書情報を当該端末証明書の証明書ＩＤと対応付けて記憶部１３の証明書テーブル１３２に記憶し（Ｓ４１０）、レスポンスの検証（Ｓ４１２）を行う。

現在時刻が端末証明書の有効期間以内でない場合（Ｓ４０７のＮｏ）、または受信した端末証明書が正当なものでない場合（Ｓ４０９のＮｏ）、証明書検証手段１４４は、解錠失敗を通信端末２０に送信して（Ｓ４１８）解錠制御処理を終了する。

【００４１】

受信した証明書ＩＤに対応付けられた証明書情報が既に証明書テーブル１３２に記憶されている場合（Ｓ４０４のＹｅｓ）、レスポンス検証手段１４５は、現在時刻が、当該証明書情報の有効期間以内であれば（Ｓ４１１のＹｅｓ）、レスポンスの検証を行う（Ｓ４１２）。

レスポンスの検証のため、レスポンス検証手段１４５は、証明書テーブル１３２に証明書ＩＤに対応付けて記憶されている端末公開鍵を用いて通信端末２０から受信したレスポンスを復号し、通信端末２０に送信したチャレンジのハッシュ値を求め、復号したレスポンスとチャレンジのハッシュ値とが等しければ、受信したレスポンスは、送信したチャレンジに対する正しいレスポンスであると決定する（Ｓ４１３のＹｅｓ）。このとき、レス

ポンス検証手段１４５が用いる暗号方式およびハッシュ関数は、通信端末２０がチャレンジからレスポンスを生成するのに用いるものに対応し、予め定められるか、通信端末２０から受信した端末証明書などによって示されてもよい。

【００４２】

受信したレスポンスが正しければ（Ｓ４１３のＹｅｓ）、錠制御手段１４６は、錠部１１に解錠指示を送信して錠部１１を解錠するよう制御して（Ｓ４１４）解錠成功を通信端末２０に送信し（Ｓ４１５）、テーブル更新手段１４７により証明書テーブル１３２の更新を行って（Ｓ４１６）、解錠制御処理を終了する。テーブル更新手段１４７による証明書テーブル１３２の更新処理（Ｓ４１６）については、後で詳述する。

一方、現在時刻が、受信した証明書ＩＤと対応付けて証明書テーブル１３２に記憶された有効期間以内でない場合（Ｓ４１１のＮｏ）、または受信したレスポンスが正しくない場合（Ｓ４１３のＮｏ）、レスポンス検証手段１４５は、解錠失敗を通信端末２０に送信して（Ｓ４１７）解錠制御処理を終了する。

【００４３】

図５は、図４における証明書テーブルの更新処理を示すフローチャートである。以下、図５を参照しつつ、テーブル更新手段１４７による証明書テーブル１３２の更新処理（図４におけるＳ４１６）について詳述する。

【００４４】

テーブル更新手段１４７は、記憶部１３の証明書テーブル１３２が満杯になりこれ以上記憶できない場合、すなわち、証明書テーブル１３２に記憶されている証明書情報の数が記憶可能な上限数に達した場合（Ｓ５０１のＹｅｓ）、証明書テーブル１３２に記憶されている証明書情報のうち優先順位の低い証明書情報を消去する（Ｓ５０２）。例えば、テーブル更新手段１４７は、優先順位の低い証明書情報として、ブラックリストに登録されている証明書ＩＤに対応する証明書情報を消去したり、有効期間が過ぎた証明書情報を消去したり、証明書テーブル１３２において最も低い検証最新度を有する証明書情報から消去する。これらの消去は、この順序で行うことが好ましいが、任意の組合せおよび順序で行うことができ、一つまたは複数の証明書情報を消去できる。

【００４５】

優先順位の低い証明書情報を消去した（Ｓ５０２）後、または証明書テーブル１３２に記憶されている証明書情報の数が記憶可能な上限数に達しない場合（Ｓ５０１のＮｏ）、テーブル更新手段１４７は、通信端末２０から受信した証明書ＩＤに対応するグループＩＤが、証明書テーブル１３２に記憶されている既存のグループＩＤのいずれとも異なる新規のグループＩＤであるか否かを判定する（Ｓ５０３）。新規のグループＩＤである場合（Ｓ５０３のＹｅｓ）、テーブル更新手段１４７は、既存のグループＩＤを有する証明書情報を証明書テーブル１３２から消去する（Ｓ５０４）。

【００４６】

既存のグループＩＤを有する証明書情報を消去した（Ｓ５０４）後、または受信した証明書ＩＤに対応するグループＩＤが新規のグループＩＤでない場合（Ｓ５０３のＮｏ）、テーブル更新手段１４７は、証明書テーブル１３２において、解錠が許可された端末証明書の証明書ＩＤに対応する証明書情報の検証最新度を最も高くし（Ｓ５０５）、その他の証明書情報には、元の検証最新度が高い証明書情報から順に、最も高い検証最新度に続く連続値を付け直し（Ｓ５０６）、証明書テーブル１３２の更新処理を終了する。例えば、証明書テーブル１３２に検証最新度が高い順に検証最新度０～５を有する証明書情報が記憶されており、検証最新度３を有する証明書情報に対応する通信端末２０が解錠を許可され、検証最新度１を有する証明書情報が消去された場合、検証最新度３の証明書情報は最も高い検証最新度０に更新され、残りの検証最新度０、２、４、５の証明書情報は、検証最新度の高い方から順に連続する検証最新度１、２、３、４に更新される。

【００４７】

図６は、通信端末２０による解錠要求処理を示すフローチャートである。以下、図６を参照しつつ、通信端末２０の制御部２５による解錠制御処理について詳述する。例えば、

利用者が通信端末２０上で解錠を要求する解錠アプリを起動したとき、以下の解錠要求処理が開始される。

【００４８】

通信端末２０の制御部２５は、解錠要求処理を開始すると、第１通信部２２により周囲の電気錠１０から発信されるアドバタイズ信号のスキャンを開始する。制御部２５は、アドバタイズ信号を受信すると（Ｓ６０１のＹｅｓ）、受信したアドバタイズ信号が有する電気錠ＩＤを記憶部２４に記憶された端末証明書２４１が有する電気錠ＩＤと照合する（Ｓ６０２）。受信した電気錠ＩＤを有する端末証明書２４１が記憶されていれば（Ｓ６０２のＹｅｓ）、制御部２５は、この電気錠ＩＤを操作部２１の画面上に解錠可能な電気錠リストとして表示する（Ｓ６０３）。なお、記憶部２４に電気錠ＩＤに対応付けて電気錠１０の名称が記憶されている場合、電気錠１０の名称をリストで表示してもよい。利用者が表示された電気錠リストから解錠する電気錠１０を操作部２１により選択して解錠を指示すると（Ｓ６０４のＹｅｓ）、制御部２５は、解錠を指示された電気錠ＩＤに対応する電気錠１０に対して通信接続を要求するとともに解錠要求を送信する（Ｓ６０５）。

アドバタイズ信号を受信しない場合（Ｓ６０１のＮｏ）、受信したアドバタイズ信号が有する電気錠ＩＤを有する端末証明書２４１が記憶部２４に記憶されていない場合（Ｓ６０２のＮｏ）、または利用者により電気錠１０の解錠指示が行われない場合（Ｓ６０４のＮｏ）、制御部２５は、他のアドバタイズ信号をスキャンする（Ｓ６０１）。

【００４９】

解錠要求を送信した（Ｓ６０５）後、解錠要求の送信先の電気錠１０からチャレンジが送信されるのを待ち（Ｓ６０６のＮｏ）、チャレンジを受信すると（Ｓ６０６のＹｅｓ）、レスポンス生成送信手段２５１は、受信したチャレンジのハッシュ値をＳＨＡ－２、ＳＨＡ－３などのハッシュ関数を用いて求め、求めたハッシュ値を端末秘密鍵２４２を用いてＲＳＡ、ＥＣＤＳＡなどの公開鍵暗号方式で暗号化することにより、チャレンジに署名を施したレスポンスを生成する（Ｓ６０７）。レスポンス生成送信手段２５１は、チャレンジの送信元の電気錠１０の電気錠ＩＤを有する端末証明書２４１の証明書ＩＤを、生成したレスポンスとともに電気錠１０に送信する（Ｓ６０８）。

電気錠１０から端末証明書の送信要求を受信すると（Ｓ６０９のＹｅｓ）、証明書送信手段２５２は、電気錠１０の電気錠ＩＤを有する端末証明書２４１を電気錠１０に送信する（Ｓ６１０）。端末証明書の送信（Ｓ６１０）後、または端末証明書の送信要求を受信しない場合（Ｓ６０９のＮｏ）、制御部２５は、電気錠１０から解錠成功／失敗を受信すると（Ｓ６１１のＹｅｓ）、受信した解錠成功／失敗に従って、電気錠１０の解錠成功／失敗を操作部２１の画面や音声、バイブレーションなどの鳴動などにより利用者に通知して（Ｓ６１２）処理を終了する。解錠成功／失敗を受信しない場合（Ｓ６１１のＮｏ）、制御部２５は、Ｓ６０９の処理に戻る。

【００５０】

以上説明してきたように、本発明に係る電気錠１０は、通信端末２０からの解錠要求に対する初回の解錠制御において正当であると検証した端末証明書の少なくとも端末公開鍵を含む証明書情報を証明書テーブル１３２に記憶しておき、二回目以降は、証明書テーブル１３２に端末公開鍵が記憶されていれば当該通信端末２０の端末証明書は正当であるとみなすため、通常では解錠要求の都度行われる端末証明書の検証処理を省略できる。これにより、本発明に係る電気錠１０は、処理能力が低くバッテリ容量が少ない場合であっても、解錠要求を受けてから解錠までのレスポンスタイムを短くでき、バッテリへの負荷を軽減してバッテリの寿命を延ばすことができる。特に、スマートロックなどのように同じ電気錠に対して同じスマートフォンなどによって解錠を繰り返し要求する用途ほど、処理負荷の軽減効果は高くなる。

【００５１】

以上、本発明の好適な実施形態について説明してきたが、本発明はこれらの実施形態に限定されるものではない。例えば、本発明では、検証が成功した端末証明書の端末公開鍵を電気錠１０の記憶部１３に記憶させているため、悪意のある利用者によって、管理サー

バ３０が発行した正規の端末証明書とは異なる不正な端末証明書の端末公開鍵が証明書テーブル１３２に記憶させられる可能性がある。その場合、不正に電気錠１０に記憶された端末公開鍵によってレスポンスが検証されるため、電気錠１０が不正に解錠される恐れがある。これを防止するため、電気錠１０のバッテリから電力が供給されない状態（電源ＯＦＦ状態）からバッテリから電力が供給された状態（電源ＯＮ状態）となったとき、すなわち再起動したときに、証明書テーブル１３２の全ての情報を消去したり利用できない情報であることを示すフラグを付与することが好ましい。

また、電気錠１０の記憶部１３に対する不正なアクセスを物理的に制限するために、電気錠１０の電子基盤を硬質カバーで覆い、開閉スイッチ、近接センサ、遮断センサ、光センサなどにより当該カバーが開けられたと検知すると、電気錠１０は、電源ＯＦＦ状態になったり、証明書テーブル１３２の全ての情報を消去したり、利用できない情報であることを示すフラグを付与することが好ましい。

【００５２】

上記実施形態では、利用者が通信端末２０で解錠を要求する解錠アプリを起動することにより通信端末２０の解錠要求処理が開始されたが、通信端末２０が、ＧＰＳなどの位置取得部（図示せず）により通信端末２０の位置情報を取得して電気錠１０の所定範囲内に入ったと判定すると、解錠要求処理を開始してもよい。

上記実施形態では、電気錠１０が解錠制御処理において電気錠１０から通信端末２０に送信した解錠成功／失敗（図４のＳ４１５、Ｓ４１７、Ｓ４１８）を、通信端末２０が受信して操作部２１を介して解錠成功／失敗を利用者に通知した（図６のＳ６１１，Ｓ６１２）が、代替または追加として、電気錠１０は操作部（図示せず）の画面、ランプ、ブザーなどにより解錠成功／失敗を利用者に通知してもよい。解錠成功／失敗が電気錠１０から通信端末２０に送信されない場合、通信端末２０は、解錠要求処理において電気錠１０に証明書ＩＤおよびレスポンスを送信した（図６のＳ６０８）後、所定期間（数秒間）内に当該電気錠１０から端末証明書の送信要求を受信したか否かを判定する（図示せず）。通信端末２０は、所定期間内に送信要求を受信しなければ解錠要求処理を終了し、所定期間内に送信要求を受信した場合、電気錠１０の電気錠ＩＤを有する端末証明書２４１を電気錠１０に送信して解錠要求処理を終了する（図示せず）。

上記実施形態では、通信端末２０から送信された解錠要求に基づいて、電気錠１０が錠部１１を解錠するよう制御する例を説明したが、本発明はこれに限らず、通信端末２０から送信された施錠要求に基づいて電気錠１０が錠部１１を施錠するよう制御してもよい。すなわち、通信端末２０は解錠要求の場合と同様の処理で施錠要求の処理を行う。また、電気錠１０は、施錠要求を受信した場合、通信端末２０から解錠要求を受信した場合と同様の処理で通信端末２０を認証して錠部１１を施錠する。このように電気錠１０は、受信した錠の施解錠の制御要求（解錠要求または施錠要求）に対して、上記実施形態の処理により通信端末２０を認証し、当該認証が成功したとき錠部１１の施解錠の制御（解錠または施錠）を行う。

以上のように、本発明の範囲内で、実施される形態に合わせて様々な変更を行うことができる。

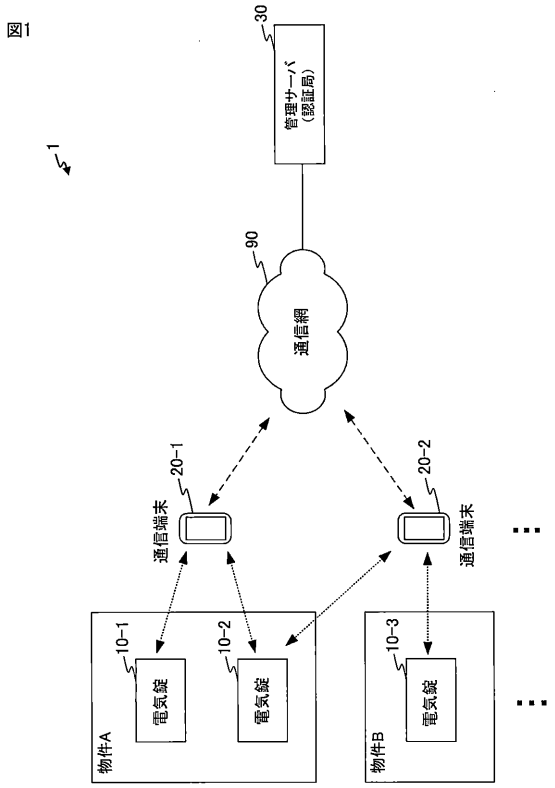
【符号の説明】

【００５３】

１　電気錠システム、１０　電気錠、１１　錠部、１２　通信部、１３　記憶部、１４　制御部、２０　通信端末、２１　操作部、２２　第１通信部、２３　第２通信部、２４　記憶部、２５　制御部、３０　管理サーバ、９０　通信網、１３１　認証局公開鍵、１３２　証明書テーブル、１３３　ブラックリスト、１４１　チャレンジ生成送信手段、１４２　レスポンス受信手段、１４３　証明書要求手段、１４４　証明書検証手段、１４５　レスポンス検証手段、１４６　錠制御手段、１４７　テーブル更新手段、２４１　端末証明書、２４２　端末秘密鍵、２５１　レスポンス生成送信手段、２５２　証明書送信手段

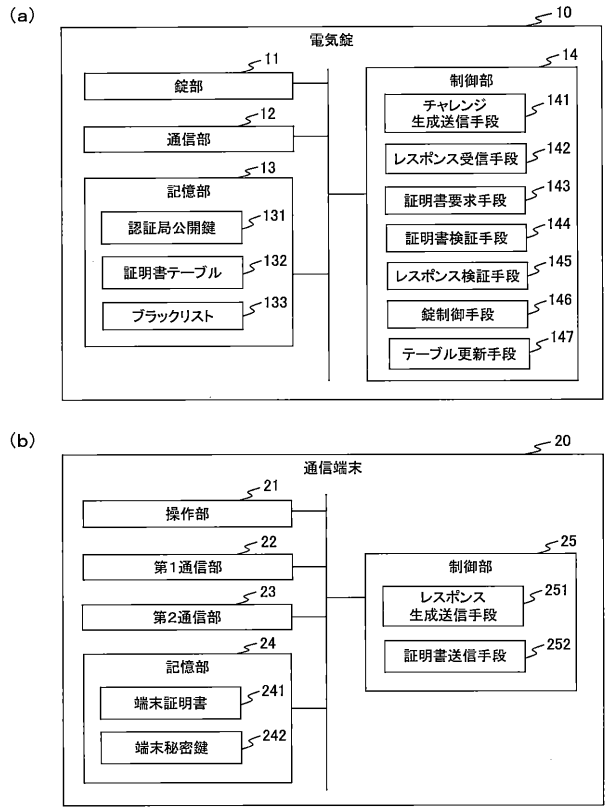
【図１】

図1



【図２】

図2



【図３】

図3

(a)

証明書テーブル

証明書ID	端末公開鍵	有効期間	グループID	検証最新度
001	V	2018/3/10 10:00	A	0
002	W	2018/8/1 10:00	—	2
003	X	2018/3/10 10:00	A	1
004	Y	2018/3/10 10:00	A	3
005	Z	2018/8/1 10:00	—	4
…	…	…	…	…

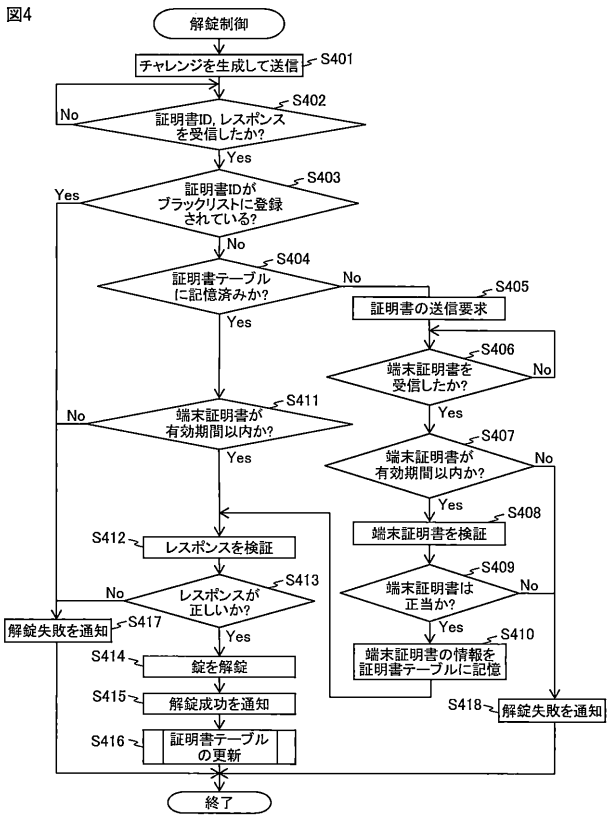
(b)

端末証明書

証明書ID
認証局ID
電気錠ID
端末公開鍵
有効期間
グループID
…
署名

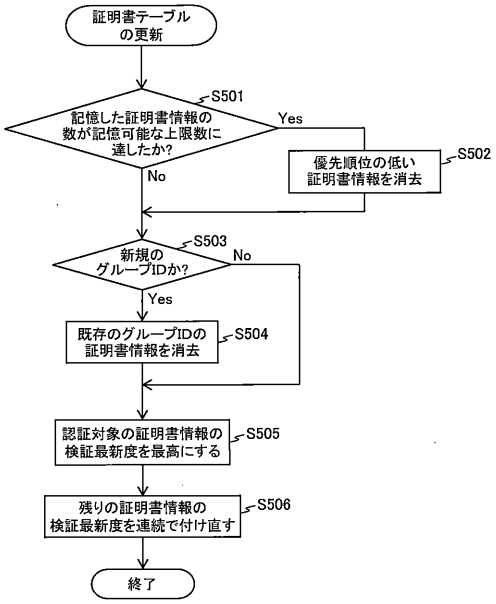
【図４】

図4



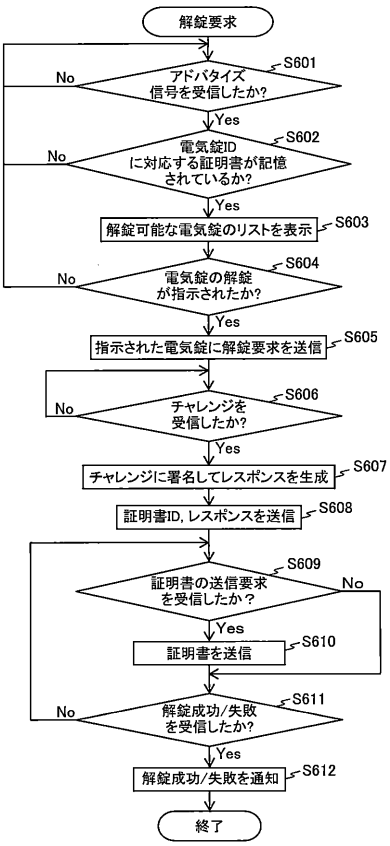
【図５】

図5


証明書テーブル
の更新
S501
記憶した証明書情報の
数が記憶可能な上限数に
達したか?
Yes
No
S502
優先順位の低い
証明書情報を消去
S503
新規の
グループIDか?
No
Yes
S504
既存のグループIDの
証明書情報を消去
S505
認証対象の証明書情報の
検証最新度を最高にする
S506
残りの証明書情報の
検証最新度を連続で付け直す
終了

【図６】

図6


解錠要求
S601
No
アドバタイズ
信号を受信したか?
Yes
S602
No
電気錠ID
に対応する証明書が記憶
されているか?
Yes
S603
解錠可能な電気錠のリストを表示
S604
No
電気錠の解錠
が指示されたか?
Yes
S605
指示された電気錠に解錠要求を送信
S606
No
チャレンジを
受信したか?
Yes
S607
チャレンジに署名してレスポンスを生成
S608
証明書ID, レスポンスを送信
S609
証明書の送信要求
を受信したか?
No
Yes
S610
証明書を送信
S611
No
解錠成功/失敗
を受信したか?
Yes
S612
解錠成功/失敗を通知
終了

フロントページの続き

(72)発明者　伊藤　忠彦
東京都三鷹市下連雀八丁目１０番１６号　セコム株式会社内

Ｆターム(参考) 2E250 AA02 AA06 AA19 BB08 BB29 BB46 DD06 EE10 FF25 FF27
FF36
5J104 AA08 AA16 EA16 KA05 MA01 NA02 NA38