

(19)日本国特許庁(JP)

## (12)特許公報(B2)

(11)特許番号  
特許第7001524号  
(P7001524)

(45)発行日 令和4年1月19日(2022.1.19)

(24)登録日 令和3年12月28日(2021.12.28)

(51)国際特許分類		F I			
H 0 4 L	9/32 (2006.01)	H 0 4 L	9/32	2 0 0 B	
E 0 5 B	49/00 (2006.01)	E 0 5 B	49/00	J	
H 0 4 L	9/08 (2006.01)	H 0 4 L	9/08	F	

請求項の数 6 (全15頁)

(21)出願番号	特願2018-66095(P2018-66095)	(73)特許権者	000108085 セコム株式会社 東京都渋谷区神宮前一丁目5番1号
(22)出願日	平成30年3月29日(2018.3.29)	(74)代理人	100099759 弁理士 青木 篤
(65)公開番号	特開2019-176441(P2019-176441 A)	(74)代理人	100123582 弁理士 三橋 真二
(43)公開日	令和1年10月10日(2019.10.10)	(74)代理人	100114018 弁理士 南山 知広
審査請求日	令和3年1月19日(2021.1.19)	(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
		(72)発明者	伊藤 忠彦

最終頁に続く

(54)【発明の名称】 電気錠

## (57)【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、を有し、  
 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、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】

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1～5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】

【文献】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】

10

20

30

40

50

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、バッテリー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。

10

【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。

20

【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。

30

【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と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。

40

【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、バッテリー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。

50

【図 2】電気錠システム 1 における電気錠 1 0 および通信端末 2 0 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 1 0 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 2 0 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。

10

【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 1 0、通信端末 2 0 および管理サーバ 3 0 を有する。電気錠 1 0 と通信端末 2 0 との間は近距離通信によって接続され、通信端末 2 0 と管理サーバ 3 0 との間は無線通信や広域通信網などを有する通信網 9 0 を介して接続される。電気錠 1 0 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 1 0 は、通信端末 2 0 から解錠要求を受信したとき、通信端末 2 0 の公開鍵（端末公開鍵）を用いて通信端末 2 0 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 2 0 は、施設の利用者によって所持され、利用者が電気錠 1 0 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 2 0 - 1 が複数の電気錠 1 0 - 1 および 1 0 - 2 の解錠権限を有してもよく、一つの電気錠 1 0 - 2 に対して複数の通信端末 2 0 - 1 および 2 0 - 2 が解錠権限を有してもよい。

20

管理サーバ 3 0 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 2 0 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 1 0 の構成図である。

図 2 ( a ) に示すように、電気錠 1 0 は、錠部（錠）1 1、通信部 1 2、記憶部 1 3 および制御部 1 4 を有し、図示しないバッテリーからの電力供給によって動作する。

30

【0018】

錠部 1 1 は、制御部 1 4 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 1 1 は、電気錠 1 0 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 1 0 から解錠 / 施錠指示を受信する。

【0019】

通信部 1 2 は、通信端末 2 0 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 )、Z i g B e e、I E E E 8 0 2 . 1 1、Z - W a v e など、通信端末 2 0 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 1 2 は、1 回 / 秒など定期的に電気錠 1 0 の錠識別情報（電気錠 I D）などを有するアダプティブ信号を周囲にブロードキャストし、このアダプティブ信号に応答して通信接続を要求してきた通信端末 2 0 と通信接続する。以下、電気錠 1 0 と通信端末 2 0 との間の通信は BLE に準ずるものとして説明する。

40

【0020】

記憶部 1 3 は、電気錠 1 0 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 1 3 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 1 2、操作部（図示せず）などを介して提供されて記憶させ

50

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。

10

#### 【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。

20

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。

30

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。

40

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

50

動作を実現する。記憶部 1 3 および制御部 1 4 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 1 4 は、錠部 1 1 に解錠 / 施錠指示を送信して錠部 1 1 の解錠 / 施錠を制御し、通信部 1 2 を介して通信端末 2 0 とデータの送受信を行う。

制御部 1 4 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 2 0 に送信するチャレンジ生成送信手段 1 4 1 と、チャレンジに対して通信端末 2 0 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 1 4 2 と、通信端末 2 0 に端末証明書を送信するよう要求する証明書要求手段 1 4 3 と、通信端末 2 0 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 1 3 2 に記憶する証明書検証手段 1 4 4 と、通信端末 2 0 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 1 4 5 と、レスポンス検証手段 1 4 5 の検証結果に従って錠部 1 1 の解錠を制御する錠制御手段 1 4 6 と、証明書テーブル 1 3 2 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） 1 4 7 と、を有する。各手段の動作については、後の電気錠 1 0 による解錠制御処理の説明にて詳述する。

#### 【 0 0 2 5 】

図 2 ( b ) は、電気錠システム 1 における通信端末 2 0 の構成図である。

図 2 ( b ) に示すように、通信端末 2 0 は、操作部 2 1、第 1 通信部 2 2、第 2 通信部 2 3、記憶部 2 4 および制御部 2 5 を有する。

#### 【 0 0 2 6 】

操作部 2 1 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。

#### 【 0 0 2 7 】

第 1 通信部 2 2 は、電気錠 1 0 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 1 0 が通信端末 2 0 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 2 2 は、周囲の装置から発信されるアダプタイズ信号をスキャンし、所望の電気錠 1 0 の電気錠 ID を有するアダプタイズ信号を発信する電気錠 1 0 を見つけると、この電気錠 1 0 に対して通信接続を要求して当該電気錠 1 0 と通信接続する。

#### 【 0 0 2 8 】

第 2 通信部 2 3 は、通信網 9 0 を介して管理サーバ 3 0 と通信を行う通信インターフェイスであり、IEEE 8 0 2 . 1 1、W - C D M A、C D M A 2 0 0 0 または L T E などの無線通信規格により通信網 9 0 に接続する。そして、第 2 通信部 2 3 は、接続した通信網 9 0 を介して、専用回線やインターネットなどにより通信網 9 0 に接続された管理サーバ 3 0 と S S L / T L S、I P S e c などの通信プロトコルにより安全な通信を行う。

#### 【 0 0 2 9 】

記憶部 2 4 は、通信端末 2 0 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、R A M、R O M、E P R O M 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 2 4 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 2 4 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 2 1、第 2 通信部 2 3 などを介して記憶される。

記憶部 2 4 は、端末証明書 2 4 1 および端末秘密鍵 2 4 2 を記憶する。なお、一つの通信端末 2 0 が複数の電気錠 1 0 の解錠権限を有する場合、電気錠 1 0 ごとに端末証明書 2 4 1 および当該端末証明書 2 4 1 に対応する端末秘密鍵 2 4 2 を記憶する。

#### 【 0 0 3 0 】

端末証明書 2 4 1 は、電気錠 1 0 が記憶する認証局公開鍵 1 3 1 に対応する認証局（管理サーバ 3 0）から、端末秘密鍵 2 4 2 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 2 4 1 は、管理サーバ 3 0 によって、通信端末 2 0 が電気錠 1 0 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 3 0 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

10

20

30

40

50

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。

10

20

30

40

50

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

10

20

30

40

50

に記憶されているか否かを確認し ( S 4 0 4 )、まだ記憶されていない場合 ( S 4 0 4 の N o )、通信端末 2 0 に端末証明書の送信要求を送信して証明書 I D に対応する端末証明書を送信するよう要求する ( S 4 0 5 )。

要求した端末証明書を通信端末 2 0 から受信すると ( S 4 0 6 の Y e s )、証明書検証手段 1 4 4 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 ( S 4 0 7 )、有効期間以内であれば ( S 4 0 7 の Y e s )、認証局公開鍵 1 3 1 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 3 0 から発行された正当なものであるか否かを検証する ( S 4 0 8 )。

#### 【 0 0 4 0 】

証明書検証手段 1 4 4 は、受信した端末証明書が管理サーバ 3 0 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 ( S 4 0 9 の Y e s )、証明書検証手段 1 4 4 は、端末証明書が有する端末公開鍵、有効期間、グループ I D などの証明書情報を当該端末証明書の証明書 I D と対応付けて記憶部 1 3 の証明書テーブル 1 3 2 に記憶し ( S 4 1 0 )、レスポンスの検証 ( S 4 1 2 ) を行う。

10

現在時刻が端末証明書の有効期間以内でない場合 ( S 4 0 7 の N o )、または受信した端末証明書が正当なものでない場合 ( S 4 0 9 の N o )、証明書検証手段 1 4 4 は、解錠失敗を通信端末 2 0 に送信して ( S 4 1 8 ) 解錠制御処理を終了する。

#### 【 0 0 4 1 】

受信した証明書 I D に対応付けられた証明書情報が既に証明書テーブル 1 3 2 に記憶されている場合 ( S 4 0 4 の Y e s )、レスポンス検証手段 1 4 5 は、現在時刻が、当該証明書情報の有効期間以内であれば ( S 4 1 1 の Y e s )、レスポンスの検証を行う ( S 4 1 2 )。

20

レスポンスの検証のため、レスポンス検証手段 1 4 5 は、証明書テーブル 1 3 2 に証明書 I D 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 2 0 から受信したレスポンスを復号し、通信端末 2 0 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 ( S 4 1 3 の Y e s )。このとき、レスポンス検証手段 1 4 5 が用いる暗号方式およびハッシュ関数は、通信端末 2 0 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 2 0 から受信した端末証明書などによって示されてもよい。

30

#### 【 0 0 4 2 】

受信したレスポンスが正しければ ( S 4 1 3 の Y e s )、錠制御手段 1 4 6 は、錠部 1 1 に解錠指示を送信して錠部 1 1 を解錠するよう制御して ( S 4 1 4 ) 解錠成功を通信端末 2 0 に送信し ( S 4 1 5 )、テーブル更新手段 1 4 7 により証明書テーブル 1 3 2 の更新を行って ( S 4 1 6 )、解錠制御処理を終了する。テーブル更新手段 1 4 7 による証明書テーブル 1 3 2 の更新処理 ( S 4 1 6 ) 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 I D と対応付けて証明書テーブル 1 3 2 に記憶された有効期間以内でない場合 ( S 4 1 1 の N o )、または受信したレスポンスが正しくない場合 ( S 4 1 3 の N o )、レスポンス検証手段 1 4 5 は、解錠失敗を通信端末 2 0 に送信して ( S 4 1 7 ) 解錠制御処理を終了する。

40

#### 【 0 0 4 3 】

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 1 4 7 による証明書テーブル 1 3 2 の更新処理 ( 図 4 における S 4 1 6 ) について詳述する。

#### 【 0 0 4 4 】

テーブル更新手段 1 4 7 は、記憶部 1 3 の証明書テーブル 1 3 2 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 1 3 2 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 ( S 5 0 1 の Y e s )、証明書テーブル 1 3 2 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 ( S 5 0 2 )。例えば、テーブル更新手段 1 4 7 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

50

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)。

10

【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。

20

【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から発信されるアダプタイズ信号のスキャンを開始する。制御部25は、アダプタイズ信号を受信すると(S601のYes)、受信したアダプ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が記憶されている場合(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)。

30

アダプタイズ信号を受信しない場合(S601のNo)、受信したアダプ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、他のアダプタイズ信号をスキャンする(S601)。

40

【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

50

R S A、E C D S A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（S 6 0 7）。レスポンス生成送信手段 2 5 1は、チャレンジの送信元の電気錠 1 0の電気錠 I Dを有する端末証明書 2 4 1の証明書 I Dを、生成したレスポンスとともに電気錠 1 0に送信する（S 6 0 8）。

電気錠 1 0から端末証明書の送信要求を受信すると（S 6 0 9の Y e s）、証明書送信手段 2 5 2は、電気錠 1 0の電気錠 I Dを有する端末証明書 2 4 1を電気錠 1 0に送信する（S 6 1 0）。端末証明書の送信（S 6 1 0）後、または端末証明書の送信要求を受信しない場合（S 6 0 9の N o）、制御部 2 5は、電気錠 1 0から解錠成功/失敗を受信すると（S 6 1 1の Y e s）、受信した解錠成功/失敗に従って、電気錠 1 0の解錠成功/失敗を操作部 2 1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（S 6 1 2）処理を終了する。解錠成功/失敗を受信しない場合（S 6 1 1の N o）、制御部 2 5は、S 6 0 9の処理に戻る。

#### 【 0 0 5 0 】

以上説明してきたように、本発明に係る電気錠 1 0は、通信端末 2 0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 1 3 2に記憶しておき、二回目以降は、証明書テーブル 1 3 2に端末公開鍵が記憶されていれば当該通信端末 2 0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 1 0は、処理能力が低くバッテリー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、バッテリーへの負荷を軽減してバッテリーの寿命を延ばすことができる。特に、スマートロックなどと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。

#### 【 0 0 5 1 】

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 1 0の記憶部 1 3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 3 0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 1 3 2に記憶させられる可能性がある。その場合、不正に電気錠 1 0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 1 0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 1 0のバッテリーから電力が供給されない状態（電源 O F F 状態）からバッテリーから電力が供給された状態（電源 O N 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 1 3 2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 1 0の記憶部 1 3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 1 0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 1 0は、電源 O F F 状態になったり、証明書テーブル 1 3 2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。

#### 【 0 0 5 2 】

上記実施形態では、利用者が通信端末 2 0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 2 0の解錠要求処理が開始されたが、通信端末 2 0が、G P Sなどの位置取得部（図示せず）により通信端末 2 0の位置情報を取得して電気錠 1 0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 1 0が解錠制御処理において電気錠 1 0から通信端末 2 0に送信した解錠成功/失敗（図 4の S 4 1 5、S 4 1 7、S 4 1 8）を、通信端末 2 0が受信して操作部 2 1を介して解錠成功/失敗を利用者に通知した（図 6の S 6 1 1、S 6 1 2）が、代替または追加として、電気錠 1 0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 1 0から通信端末 2 0に送信されない場合、通信端末 2 0は、解錠要求処理において電気錠 1 0に

10

20

30

40

50

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

10

20

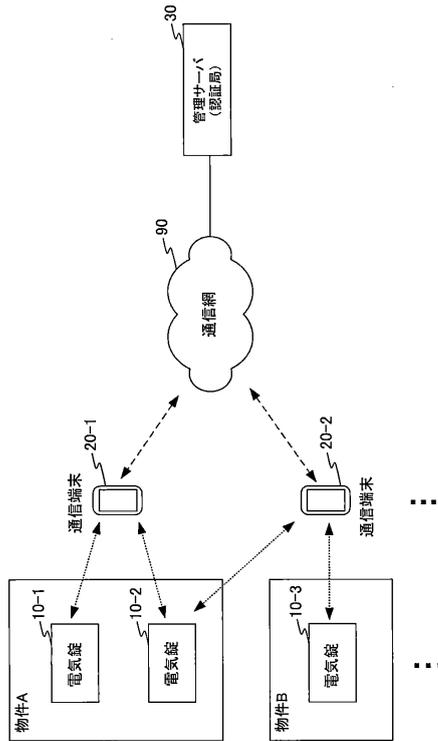
30

40

50

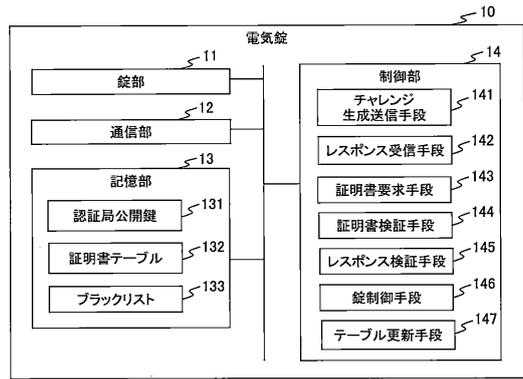
【 図面 】  
【 図 1 】

図1

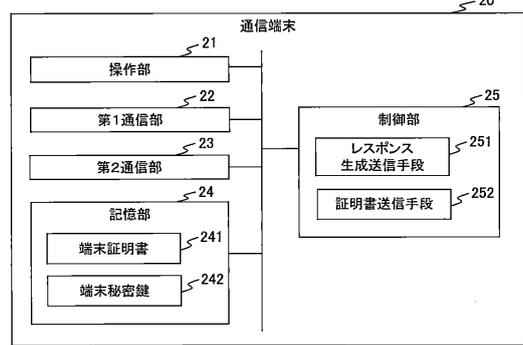


【 図 2 】

図2  
(a)



(b)



【 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
...	...	...	...	...

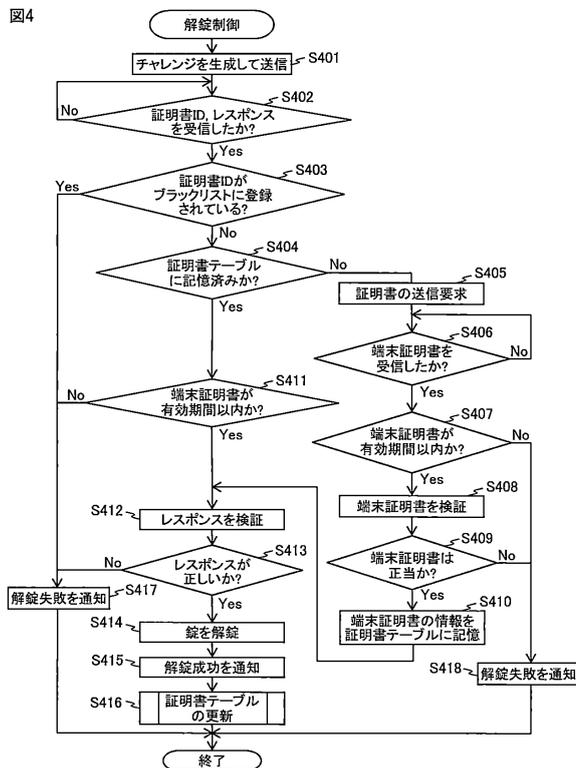
(b)

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



10

20

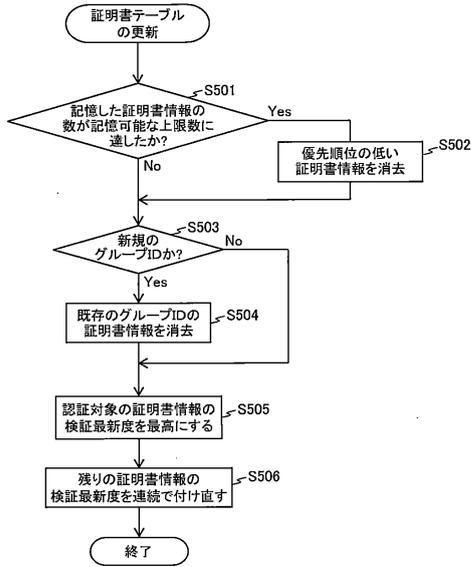
30

40

50

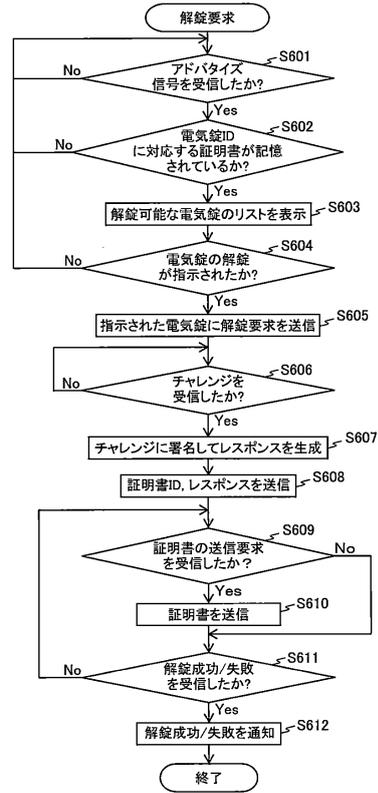
【 図 5 】

図5



【 図 6 】

図6



10

20

30

40

50

## フロントページの続き

東京都三鷹市下連雀八丁目10番16号 セコム株式会社内

審査官 中里 裕正

- (56)参考文献 特開2014-042095(JP,A)  
特開2003-343133(JP,A)  
特開2008-181295(JP,A)  
特開2017-216596(JP,A)  
特表2002-517036(JP,A)  
特開2004-179724(JP,A)  
国際公開第2015/128895(WO,A1)  
特開2007-074393(JP,A)
- (58)調査した分野 (Int.Cl., DB名)  
H04L 9/32  
E05B 49/00  
H04L 9/08