(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6632887号
(P6632887)
(45)発行日　令和2年1月22日(2020.1.22)　(24)登録日　令和1年12月20日(2019.12.20)

(51)Int.Cl.		F I		
E05B 49/00	(2006.01)	E05B	49/00	J
G06F 21/31	(2013.01)	G06F	21/31	
G06Q 50/16	(2012.01)	G06Q	50/16	300

請求項の数 58　(全 30 頁)

(21)出願番号　特願2015-557302 (P2015-557302)
(86)(22)出願日　平成26年1月15日 (2014.1.15)
(65)公表番号　特表2016-510371 (P2016-510371A)
(43)公表日　平成28年4月7日 (2016.4.7)
(86)国際出願番号　PCT/CA2014/050022
(87)国際公開番号　WO2014/124529
(87)国際公開日　平成26年8月21日 (2014.8.21)
審査請求日　平成28年11月2日 (2016.11.2)
(31)優先権主張番号　61/765,618
(32)優先日　平成25年2月15日 (2013.2.15)
(33)優先権主張国・地域又は機関
米国 (US)

前置審査

(73)特許権者　515222539
キーカフェ　インク.
カナダ国　Ｖ６Ｂ　５Ｃ６　ブリティッシュコロンビア州　バンクーバー　ウォーター　ストリート　２００－３７５
(74)代理人　100083806
弁理士　三好　秀和
(74)代理人　100095500
弁理士　伊藤　正和
(74)代理人　100111235
弁理士　原　裕子
(74)代理人　100195257
弁理士　大渕　一志
(74)代理人　100153877
弁理士　大森　拓

最終頁に続く

(54)【発明の名称】鍵交換の管理のための方法及びシステム

(57)【特許請求の範囲】
【請求項１】
鍵アクセス場所において１つ以上の鍵を含む鍵セットの交換を容易にする方法であって、
一意の鍵識別子を取得するために前記鍵セットに取り付けられる鍵トークンをスキャンするステップと、
クライアント装置から場所データを受信することにより前記鍵アクセス場所を識別するステップであって、前記鍵アクセス場所は、前記鍵セットが交換され得る複数の鍵アクセス場所の１つであるステップと、
前記鍵アクセス場所におけるビンに前記鍵セットを割り当てるステップと、
前記ビン及び前記鍵アクセス場所を前記鍵セットと関係付けるステップと、
前記鍵セットに対するアクセス規則を受信するステップであって、前記アクセス規則は承認されたパーティを識別するステップと、
前記鍵アクセス場所を前記承認されたパーティに公開するステップと、
前記クライアント装置を介して、前記承認されたパーティから前記鍵セットに対するアクセス要求を受信するステップであって、前記アクセス要求はユーザ認証情報を提供するステップと、
前記承認されたパーティに関係付けられる認証情報のセットに対して前記アクセス要求において提供された前記ユーザ認証情報を検証することにより前記アクセス要求を認証するステップと、

前記アクセス要求が認証されると、前記鍵セットの提示のためのアクセス命令を送信するステップと
を含む、方法。
【請求項２】
前記クライアント装置の場所を決定するステップを含み、前記アクセス要求を認証するステップは、前記クライアント装置の場所を前記鍵セットに関係付けられる前記鍵アクセス場所と比較することを更に含む、請求項１に記載の方法。
【請求項３】
前記場所データは、ＧＰＳデータ、モバイルネットワーク場所データ、装置識別データ、及びユーザデータ入力の１つ以上を含む、請求項１又は２に記載の方法。
【請求項４】
ＧＰＳデータ、モバイルネットワーク場所データ、装置識別データ、及びユーザデータ入力の１つ以上を、前記クライアント装置から受信することにより前記クライアント装置の場所を決定するステップを含む、請求項１～３のいずれか１項に記載の方法。
【請求項５】
前記アクセス規則は承認アクセス期間を含み、前記方法は前記アクセス要求の時間を識別するステップを含み、前記アクセス要求を認証するステップは前記アクセス要求の時間を前記承認アクセス期間と比較することを含む、請求項１～４のいずれか１項に記載の方法。
【請求項６】
前記鍵セットに対する複数のアクセス規則を受信するステップを含み、前記アクセス規則の各々が承認されたパーティ及び対応する承認アクセス期間を識別する、請求項１～５のいずれか１項に記載の方法。
【請求項７】
前記対応する承認アクセス期間の既定時間内に前記承認されたパーティの各々に前記鍵アクセス場所を公開するステップを含む、請求項６に記載の方法。
【請求項８】
前記鍵アクセス場所において前記鍵トークンのスキャンを開始することにより、正しい鍵セットの提示を検証するステップを含む、請求項１～７のいずれか１項に記載の方法。
【請求項９】
前記鍵セットの提示のためのアクセス命令を送信するステップは、前記鍵セットに関係付けられるビン番号を前記クライアント装置に送信することを含む、請求項１～８のいずれか１項に記載の方法。
【請求項１０】
前記ビンは制御及び処理装置により制御可能であり、前記鍵セットの提示のためのアクセス命令を送信するステップは、前記鍵セットをアクセス可能にするための信号を前記制御及び処理装置に送信することを含む、請求項１～９のいずれか１項に記載の方法。
【請求項１１】
前記鍵トークンから前記鍵セットの前記鍵識別子を読み取るために前記ビンにおけるスキャナを起動することにより、要求された鍵セットが前記ビンにあることを検証するステップを含む、請求項１～１０のいずれか１項に記載の方法。
【請求項１２】
前記鍵識別子はＵＲＬを含む、請求項１～１１のいずれか１項に記載の方法。
【請求項１３】
前記ＵＲＬは、前記鍵セットに割り当てられる一意の識別情報にリンクされる、請求項１２に記載の方法。
【請求項１４】
前記識別情報は、数字、名前又は他の英数字の列を含む、請求項１３に記載の方法。
【請求項１５】
前記鍵識別子は、前記鍵セットに取り付けられる鍵チェイン上に符号化される、請求項

１～１４のいずれか１項に記載の方法。
【請求項１６】
前記鍵識別子は、前記鍵チェインにおけるＮＦＣタグに符号化される、請求項１５に記載の方法。
【請求項１７】
１つ以上の鍵交換所において鍵セットの鍵トークンを周期的にスキャンするステップと、周期的なスキャンからの情報に基づいて、ビン及び前記鍵アクセス場所と前記鍵セットの関係付けを更新するステップとを含む、請求項１～１６のいずれか１項に記載の方法。
【請求項１８】
前記鍵アクセス場所を前記承認されたパーティに公開するステップは、前記承認されたパーティによってアクセス可能なＥメールアカウント又はユーザアカウントページに前記鍵アクセス場所を送信することを含む、請求項１～１７のいずれか１項に記載の方法。
【請求項１９】
前記鍵セットが前記承認されたパーティに提示されること及び前記鍵セットが鍵アクセス場所に引き渡されることの１つ以上に応じて、前記鍵セットに関係付けられる鍵管理者への通知を自動的に生成するステップを含む、請求項５に記載の方法。
【請求項２０】
前記鍵セットが特定の時間までに前記承認されたパーティに提示されていない場合、前記鍵セットに関係付けられる鍵管理者への通知を自動的に生成するステップを含む、請求項５に記載の方法。
【請求項２１】
前記承認アクセス期間の開始の既定時間前に前記承認されたパーティへの通知を自動的に生成するステップを含む、請求項１９又は２０に記載の方法。
【請求項２２】
前記鍵セットが前記承認されたパーティに提示されることに応じて、前記鍵管理者への通知を自動的に生成するステップを含む、請求項２１に記載の方法。
【請求項２３】
前記鍵セットに関係付けられる管理ユーザから前記承認されたパーティへの前記通知に関するコンテンツを受信するステップと、前記承認されたパーティへの前記通知に前記コンテンツを含めるステップとを含む、請求項２２に記載の方法。
【請求項２４】
１つ以上の事前購入された物品、クーポン、又は前記鍵交換所に地域的な商品若しくはサービスに対する他の申し出を前記承認されたパーティに自動的に提供するステップを含む、請求項１７に記載の方法。
【請求項２５】
住居におけるサービスに対するユーザ要求、物件予約、反復性のアクセス要求、及び承認されたサードパーティシステムによる要求の１つ以上に応じて、前記アクセス規則を自動的に生成するステップを含む、請求項１～２４のいずれか１項に記載の方法。
【請求項２６】
複数の鍵アクセス場所の１つにおいて１つ以上の鍵を含む鍵セットの非同期的な交換を容易にするシステムであって、
前記鍵に取り付けられる鍵トークン上に符号化される一意の鍵識別子を受信し、
クライアント装置から場所データを受信することにより前記鍵アクセス場所を決定し、であって、前記鍵アクセス場所は、前記鍵セットが交換され得る複数の鍵アクセス場所の１つであり、
前記鍵アクセス場所におけるビンを前記鍵セットに割り当て、
前記ビン及び前記鍵アクセス場所を前記鍵セットと関係付け、
前記鍵セットに対するアクセス規則であって、承認されたパーティを識別するアクセス規則を受信又は生成し、
前記鍵アクセス場所を前記承認されたパーティに公開し、

前記鍵セットに対するアクセス要求であってユーザ認証情報を提供するアクセス要求を、前記クライアント装置を介して前記承認されたパーティから受信し、
前記承認されたパーティに関係付けられる認証情報のセットに対して前記アクセス要求において提供された前記ユーザ認証情報を検証することにより前記アクセス要求を認証し、且つ
前記アクセス要求が認証されると、前記鍵セットの提示のためのアクセス命令を前記承認されたパーティに送信する
ように構成される鍵交換サーバを備える、システム。
【請求項２７】
前記鍵交換サーバは、前記クライアント装置の場所を決定し、前記クライアント装置の場所を前記鍵セットに関係付けられる前記鍵アクセス場所と比較することを含むステップにより前記アクセス要求を認証するように構成される、請求項２６に記載のシステム。
【請求項２８】
前記場所データは、ＧＰＳデータ、モバイルネットワーク場所データ、装置識別データ、及びユーザデータ入力の１つ以上を含む、請求項２６又は２７に記載のシステム。
【請求項２９】
前記鍵交換サーバは、ＧＰＳデータ、モバイルネットワーク場所データ、装置識別データ、及びユーザデータ入力の１つ以上を前記クライアント装置から受信することにより前記クライアント装置の場所を決定するように構成される、請求項２６～２８のいずれか１項に記載のシステム。
【請求項３０】
前記アクセス規則は承認アクセス期間を含み、前記鍵交換サーバは前記アクセス要求の時間を識別し、前記アクセス要求の時間を前記承認アクセス期間と比較することを含むステップにより前記アクセス要求を認証するように構成される、請求項２６～２９のいずれか１項に記載のシステム。
【請求項３１】
前記鍵交換サーバは、前記鍵セットに対する複数のアクセス規則を受信又は生成するように構成され、前記アクセス規則の各々が承認されたパーティ及び対応する承認アクセス期間を識別する、請求項２６～３０のいずれか１項に記載のシステム。
【請求項３２】
前記鍵交換サーバは、前記対応する承認アクセス期間の既定時間内に前記承認されたパーティの各々に前記鍵アクセス場所を公開するように構成される、請求項３１に記載のシステム。
【請求項３３】
前記鍵アクセス場所において複数のビンを含む鍵キャビネットサブシステムを備える、請求項２６～３２のいずれか１項に記載のシステム。
【請求項３４】
前記複数のビンの各々が１つの鍵及び鍵チェインの組み合わせを受け入れるように適合される、請求項３３に記載のシステム。
【請求項３５】
前記鍵キャビネットサブシステムは制御及び処理装置を備え、前記鍵交換サーバは、前記鍵セットを前記承認されたパーティにアクセス可能にするための信号を前記制御及び処理装置に送信することにより前記鍵セットの提示のためのアクセス命令を送信するように構成される、請求項３３又は３４に記載のシステム。
【請求項３６】
前記鍵キャビネットサブシステムは前記ビンにおいてスキャナを備え、前記鍵交換サーバは、要求された鍵セットが前記ビンにあることを検証するために前記鍵セットの前記鍵識別子を読み取るために前記スキャナを起動させる信号を前記制御及び処理装置に送信するように構成される、請求項３５に記載のシステム。
【請求項３７】

前記鍵交換サーバは、前記鍵セットのスキャンから前記鍵識別子を受信して、前記承認されたパーティに提示される前記鍵セットが正しい鍵セットであることを前記鍵識別子から検証するように構成される、請求項２６～３６のいずれか１項に記載のシステム。

【請求項３８】

前記鍵交換サーバは、前記鍵セットに関係付けられるビン番号を前記クライアント装置に送信することにより前記鍵の提示のためのアクセス命令を送信するように構成される、請求項２６～３７のいずれか１項に記載のシステム。

【請求項３９】

前記鍵セットに関係付けられる前記鍵識別子はＵＲＬを含む、請求項２６～３８のいずれか１項に記載のシステム。

【請求項４０】

前記鍵識別子は、鍵チェイン上に視認可能な一意の識別情報にリンクされる、請求項３９に記載のシステム。

【請求項４１】

前記鍵トークンは、前記鍵セットに取り付けられる鍵チェイン上に位置する、請求項２６～４０のいずれか１項に記載のシステム。

【請求項４２】

前記鍵識別子はＮＦＣタグに符号化される、請求項２６～４１のいずれか１項に記載のシステム。

【請求項４３】

前記ＮＦＣタグは、金属フォブにおける凹所に埋め込まれる、請求項４２に記載のシステム。

【請求項４４】

前記ＮＦＣタグは、アンチメタル層により前記金属フォブの金属から分離され、エポキシ層により金属の凹所に固定される、請求項４３に記載のシステム。

【請求項４５】

前記鍵交換サーバは、前記鍵セットに対する複数のアクセス規則を処理するように構成され、前記アクセス規則の各々が承認されたパーティ及び対応する承認アクセス期間を識別する、請求項２６～４４のいずれか１項に記載のシステム。

【請求項４６】

前記鍵交換サーバは、前記対応する承認アクセス期間の既定時間内に前記承認されたパーティの各々に前記鍵アクセス場所を公開するように構成される、請求項４５に記載のシステム。

【請求項４７】

前記鍵交換サーバは、１つ以上の鍵交換所において鍵セットの鍵トークンのスキャンを周期的に引き起こし、周期的なスキャンからの情報に基づいて、ビン及び前記鍵アクセス場所と前記鍵セットの関係付けを更新するように構成される、請求項２６～４６のいずれか１項に記載のシステム。

【請求項４８】

前記鍵交換サーバは、前記承認されたパーティによってアクセス可能なＥメールアカウント又はユーザアカウントページに前記鍵アクセス場所を送信することにより前記承認されたパーティに前記鍵アクセス場所を公開するように構成される、請求項２６～４７のいずれか１項に記載のシステム。

【請求項４９】

前記鍵セットが前記承認されたパーティに提示されること及び前記鍵セットが鍵アクセス場所に引き渡されることの１つ以上に応じて、前記鍵セットに関係付けられる鍵管理者への通知を生成するように構成される通知生成器を備える、請求項２６～４８のいずれか１項に記載のシステム。

【請求項５０】

前記鍵セットが特定の時間までに前記承認されたパーティに提示されていない場合、前

記通知生成器は、前記鍵セットに関係付けられる前記鍵管理者への通知を自動的に生成するように構成される、請求項４９に記載のシステム。
【請求項５１】
通知を生成するように構成される通知生成器を備え、前記通知生成器は、前記承認アクセス期間の開始の既定時間前に前記承認されたパーティへの通知を自動的に生成するように構成される、請求項３０に記載のシステム。
【請求項５２】
前記鍵交換サーバは、前記鍵セットが前記承認されたパーティに提示されることに応じて、前記承認されたパーティへの通知を自動的に生成するように構成される通知生成器を備える、請求項２６～４９のいずれか１項に記載のシステム。
【請求項５３】
前記鍵交換サーバは、前記鍵セットに関係付けられる管理ユーザから前記承認されたパーティへの前記通知に関するコンテンツを受信して記憶し、前記承認されたパーティへの前記通知に前記コンテンツを含めるように構成される、請求項５２に記載のシステム。
【請求項５４】
前記鍵交換所に地域的な商品若しくはサービスに対するクーポン又は他の申し出を前記承認されたパーティに自動的に送信するように構成される、請求項４７に記載のシステム。
【請求項５５】
前記鍵交換サーバは、住居におけるサービスに対するユーザ要求、物件予約、反復性のアクセス要求、及び承認されたサードパーティシステムによる要求の１つ以上に従ってシステム要求からアクセス規則を生成するように構成される、請求項２６～５４のいずれか１項に記載のシステム。
【請求項５６】
インターフェースアプリケーションが前記鍵キャビネットサブシステムにプッシュされ、前記インターフェースアプリケーションは、前記鍵キャビネットサブシステムが前記鍵交換サーバとインターフェース接続することを可能にするための命令を含む、請求項３３～３５のいずれか１項に記載のシステム。
【請求項５７】
前記インターフェースアプリケーションへの更新が前記鍵キャビネットサブシステムにプッシュされる、請求項５６に記載のシステム。
【請求項５８】
鍵アクセス場所において１つ以上の鍵を含む鍵セットの交換を容易にする方法であって、
前記鍵セットに取り付けられる鍵トークン上に符号化される一意の鍵識別子を受信するステップと、
クライアント装置から場所データを受信することにより前記鍵アクセス場所を決定するステップであって、前記鍵アクセス場所は、前記鍵セットが交換され得る複数の鍵アクセス場所の１つであるステップと、
前記鍵アクセス場所におけるビンを前記鍵セットに割り当てるステップと、
前記ビン及び前記鍵アクセス場所を前記鍵セットと関係付けるステップと、
前記鍵アクセス場所を承認されたパーティに公開するステップと、
前記クライアント装置を介して、前記承認されたパーティからの前記鍵セットに対するアクセス要求を受信するステップであって、前記アクセス要求はユーザ認証情報を提供するステップと、
前記鍵セットに関係付けられるアクセス規則を取得するステップであって、前記アクセス規則は承認されたパーティのための承認アクセス期間を識別するステップと、
前記承認されたパーティに関係付けられる認証情報のセットに対して前記アクセス要求において提供された前記ユーザ認証情報を検証することにより前記アクセス要求を認証して、前記アクセス要求が前記承認アクセス期間内に行われることを検証するステップと、

前記アクセス要求が認証されると、前記ビンを開錠するためのアクセス命令を鍵キャビネットコントローラに送信するステップと
を含む、方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本明細書に記載の技術は、鍵の交換を処理するための方法及びシステムに関する。
（関連出願の参照）
本出願は、２０１３年２月１５日に提出され且つ“ＭＥＴＨＯＤＳ　ＡＮＤ　ＳＹＳＴＥＭＳ　ＦＯＲ　ＭＡＮＡＧＥＭＥＮＴ　ＯＦ　ＫＥＹ　ＥＸＣＨＡＮＧＥＳ”と題された米国出願第６１／７６５，６１８号からの優先権を主張する。米国のために、本出願は、２０１３年２月１５に提出され且つ“ＭＥＴＨＯＤＳ　ＡＮＤ　ＳＹＳＴＥＭＳ　ＦＯＲ　ＭＡＮＡＧＥＭＥＮＴ　ＯＦ　ＫＥＹ　ＥＸＣＨＡＮＧＥＳ”と題された米国出願第６１／７６５，６１８号の米国特許法第１１９条による利益を主張し、これはあらゆる目的のためにここでの参照により本明細書に組み込まれる。
【背景技術】
【０００２】
場合によっては、鍵の掛かった物件へのアクセスを１人以上の個人に提供する必要がある。例えば、物件内の宿泊を手配したゲストがアクセスを要求する場合がある。また、家族、友人、物件管理人、宅配便業者、配達員又はサービス提供者（例えば、掃除人、犬の散歩代行者、建築請負人、不動産仲介業者、花屋等）が、アクセスを要求する場合もある。また、人々は、車両、保存装置、又は他のタイプの鍵を掛けられている物件へのアクセスを要求する場合もある。個人が物件に入るために物件の鍵を持っている人物に会うことができない場合、その個人に物件へのアクセスを提供することは困難であり得る。
【０００３】
鍵が物件の外側に隠されており、アクセスを必要とする個人は鍵を見つけるための指示を受けることがある。場合によっては、鍵は建物の外側の鍵付きの箱に保存されている。一般的に、鍵付きの箱はキーパッドロックを有している。鍵付きの箱に関するピンコードを持っている全ての個人がいつでも鍵を取得するために鍵付きの箱を開くことができるので、鍵付きの箱は安全性の問題を有している。更に、鍵付きの箱は、建物に入るための別個のキーフォブ、アクセスカード又は建物の鍵を一般的に必要とする分譲マンション等の複合物件に対しては実現不可能であり得る。
【０００４】
鍵は、物件に入るために個人に会うことができる隣人又は他の第三者に与えられることもある。この解決法は、特定の時間に特定の場所で個人に会うことができる人物がいるということに依存している。このようなイベントを調整するロジスティックは、特に、個人の到着時刻が常に予想できるとは限らないので、負担になり得る。
【０００５】
上記の問題を解決する方法及びシステムに対する一般的な願望がある。特に、個人に鍵又は鍵のセットへのアクセスを提供するための方法及びシステムに対する願望がある。複合建築を含む市街地の物件、車両、保存ユニット及び他の鍵を必要とする物件へのアクセスを提供するために使用するのが好都合な方法及びシステムに対する願望がある。
【０００６】
関連技術の上記の例示及びそれに関連する限定は例示目的であり、排他的ではないことが意図されている。明細書を読み且つ図面を観察すれば関連技術の他の例示が当業者には明らかとなろう。
【発明の概要】
【０００７】
本明細書に記載の技術は、多数の側面を有する。これらは、限定ではないが、物件へアクセスするための鍵を交換する方法、個人への鍵の供給を調整するためのコンピュータシ

ステム、鍵を保存して利用可能にするための装置、及び個人への鍵の供給を容易にするためのシステムを含む。

【０００８】

１つの態様は、鍵にアクセスする場所で鍵の交換を容易にする方法を提供する。この方法は「非同期的」であり、即ち、鍵にアクセスする場所で個人に鍵を利用可能にするための予備ステップが、個人が鍵へのアクセスを取得するのと同時に発生する必要がないことを意味してもよい。方法は、鍵において符号化される一意の鍵識別子又は鍵に取り付けられる装置を取得するためにスキャンするステップ、鍵にアクセスする場所でビン（ｂｉｎ）に鍵を割り当てるステップ、鍵及び鍵にアクセスする場所を識別子と関係付けるステップとを含む。鍵に対するアクセス規則が管理ユーザから受信され、アクセス規則は承認されたパーティ及び承認されたアクセス期間を識別する。鍵にアクセスする場所は、承認されたパーティに公開される。鍵に対するアクセス要求が、クライアント装置を介して承認されたパーティから受信される。アクセス要求はユーザ認証情報を提供する。アクセス要求は、承認されたパーティに関係付けられる認証情報のセットに対してアクセス要求において提供されるユーザ認証情報を検証し、アクセス要求の時間を承認されたアクセス期間と比較することにより認証される。認証は、個人の識別位置を識別子に関係付けられる鍵アクセス場所と比較することを更に含む。アクセス要求が認証されると、鍵の提示に対するアクセス命令が送信される。

【０００９】

別の態様は、鍵アクセス場所で鍵をスキャンするスキャナから（例えば、クライアント装置において又は鍵保存装置において）識別子を受信することにより提示される鍵の検証を提供する。

【００１０】

他の態様は、上記の方法を実装するためのシステムを提供する。

【００１１】

上記の例示の態様及び実施形態に加えて、図面を参照することにより及び以下の詳細な記載を吟味することにより更なる態様及び実施形態が明らかとなろう。図面の簡単な説明

図面を参照して、例示の実施形態が示される。本明細書に開示の実施形態及び図面は限定ではなく例示と見なされることが意図されている。

【図面の簡単な説明】

【００１２】

【図１】一実施形態により個人間の鍵交換を処理するためのシステムのコンポーネントを示す。

【図２】一実施形態により管理ユーザが鍵へのアクセス権を割り当てるための方法を示すフローチャートである。

【図３】一実施形態により鍵引き渡し（ｄｒｏｐ－ｏｆｆ）において実行され得る方法を示すフローチャートである。

【図４】一実施形態により鍵へのアクセスを個人に提供するために鍵引き取り（ｋｅｙ　ｐｉｃｋ－ｕｐ）において実行され得る方法を示すフローチャートである。

【図５】別の実施形態により鍵へのアクセスを個人に提供するために鍵引き取り（ｋｅｙ　ｐｉｃｋ－ｕｐ）において実行され得る方法を示すフローチャートである。

【図６Ａ】一実施形態による鍵交換アプリケーションのグラフィカルユーザインターフェースの例示のスクリーンショットである。

【図６Ｂ】一実施形態による鍵交換アプリケーションのグラフィカルユーザインターフェースの例示のスクリーンショットである。

【図６Ｃ】一実施形態による鍵交換アプリケーションのグラフィカルユーザインターフェースの例示のスクリーンショットである。

【図７Ａ】一部の実施形態で使用され得る鍵トークンを含む鍵チェインを示す。

【図７Ｂ】一部の実施形態で使用され得る鍵トークンを含む鍵チェインを示す。

【図７Ｃ】一部の実施形態で使用され得る鍵トークンを含む鍵チェインを示す。

【図７Ｄ】一部の実施形態で使用され得る鍵トークンを含む鍵チェインを示す。
【図８】鍵のセットを保存するための例示のキャビネットを示す。
【図９】ユーザに通知するための例示の方法を示す。
【発明を実施するための形態】
【００１３】
以下の記載を通じて、より完全な理解を当業者に提供するための詳細が説明される。しかしながら、本開示を不必要に不明確にするのを避けるために周知の要素は詳細には示されず又は記載されない場合がある。従って、説明及び図面は、限定ではなく例示の意味で考慮されるべきである。
【００１４】
本明細書に記載の実施形態において、鍵交換システム及び方法は、鍵交換ネットワークにおける多数の場所にわたる個人間での鍵の交換を容易にするために提供される。本明細書で用いられる「物件（ｐｒｏｐｅｒｔｙ）」とは、任意の鍵の掛けられる不動産、保管場所、商用、車両用又は人物がアクセスを認められたい若しくは得たい他の物件のことを言う。本明細書で用いられる「鍵」又は「複数の鍵」とは、物件にアクセスするために１つ以上の錠を作動させるために使用され得る任意の道具又は装置又はそれらのセットのことを言う。鍵は、例えば、家の鍵、キーフォブ、鍵カード、車の鍵、１つ以上の錠に鍵を掛ける若しくは開錠するために使用され得るデジタル若しくはモバイル装置等を含む。「鍵セット」は、鍵識別子に直接又は間接的に関係付けられる１つ以上の鍵の組である。単一の鍵は、鍵セットの一例である。鍵識別子は、観念的に一意である。鍵セットは、１つ以上の物件への鍵を含んでもよい（例えば、鍵のセットは、建物にアクセスするための鍵、建物のアパートにアクセスするための鍵及び車の鍵を含んでもよい）。
【００１５】
鍵交換システムは、１つ以上の鍵のセットが承認された個人によるアクセスのために保持される鍵交換所を含む。コンピュータシステムは、鍵交換所で保持される鍵のセット及び鍵のセットが解放され得る時間及び人物を決定する規則を記録する。コンピュータシステムは、鍵のセットを受け取ろうとする個人を認証するためのステップを実行してもよい。
【００１６】
以下は、このようなシステムがどのように用いられるかの非限定的な例示である。所有者が一度に数日間にわたり旅行者にアパートを貸し出す場合を検討する。アパートの鍵を渡すために特定の場所及び時間に旅行者に会うための手配をする代わりに、所有者は、鍵のセットが安全に保存される鍵交換所にアパートの鍵のセットを預け入れする。鍵が鍵交換所で引き渡されると、鍵を検証するための１つ以上のステップが行われてもよい。また、所有者は、旅行者を識別する情報及び旅行者が鍵のセットにアクセスする権利を与えられる時間を特定する規則を鍵交換システムのコンピュータシステムに提供する。こうしたステップは、旅行者の到着の前の任意の時間に所有者の都合で行われてもよい。
【００１７】
適切な時間に、鍵交換システムは、鍵交換所の場所を旅行者に自動的に通知してもよい。鍵交換所は、例えば、アパートの地域の喫茶店等のビジネスにホスティングされてもよい。許可された時間内に、旅行者は、鍵交換所から鍵のセットを要求することが可能であり、その後アパートにアクセスすることができる。以下に記載されるように、旅行者の認証及びアパートの鍵のセットの解放は、様々な程度に自動化されてもよい。旅行者は、鍵のセットを鍵交換所に最終的に戻し得る。
【００１８】
上記の非限定的な例示に記載されるシステムは、アパート又は他の物件のための鍵が所有者と旅行者とが対面して会う必要なく交換できるという利点を有することが理解され得る。更に、このようなシステムは、所有者が旅行者のクレジットカード又は他の支払い情報へのアクセスを要求しないやり方でアパート又は他の物件の使用に対する支払いを選択的に管理することができる。一部の実施形態では、所有者及び旅行者は、スマートフォン

又はタブレットコンピュータ等のネットワーク接続された携帯型装置によってシステムと相互作用することができる。このようなシステムは、各々に所望の安全性を提供しつつ、所有者及び旅行者の両者によって非常に容易に使用することができる。

【００１９】

好ましくは、鍵識別子は機械読み取り可能である。特定の実施形態において、鍵識別子は、鍵に符号化され又はその中に埋め込まれ、又は例えば、鍵チェインによって、鍵に又は鍵のセットに物理的に取り付けられる装置である。「鍵トークン」は、鍵識別子を読み取るためにスキャンされ得る物理的構造である。鍵トークンは、任意の適切な技術を用いて読み取り可能であってもよい。例えば、鍵トークンは、ＮＦＣ（ｎｅａｒ　ｆｉｅｌｄ　ｃｏｍｍｕｎｉｃａｔｉｏｎ）タグ、選択的にスキャン可能なバーコード（ＵＰＣコード又はＱＲコード（登録商標）等）、鍵に又は鍵に取り付けられたタグに印付けられた一連の記号（例えば、文字、数字及び／又は他の記号）を含んでもよい。観念的に、各鍵セットは、それが属する物件と鍵セットを関係付けることを非承認のパーティに可能にする人間読み取り可能な印を有さない。

【００２０】

１つの有益且つ新規な実施形態において、鍵トークンは鍵チェインに設けられる。鍵チェインは、金属フォブ及びチェイン又は鍵セットの鍵にフォブを結合するための他のアタッチメントを含む。フォブは、フォブの金属における凹所内の非金属材料に埋め込まれるＮＦＣタグを含む。例えば、ＮＦＣタグは、近くの金属の存在に関わらずＮＦＣタグの読み取りを可能にする絶縁層を含む粘着層により凹所に付着されてもよい。このような絶縁層を含むＮＦＣタグは、「アンチメタル（ａｎｔｉ－ｍｅｔａｌ）」ＮＦＣタグとして市販されている。タグは、プラスチック又はエポキシ等の層により覆われてもよい。ＮＦＣタグの近くの金属の存在は、一般的に、ＮＦＣタグの正確なスキャンに干渉する。しかしながら、上記のような凹所に埋め込まれたＮＦＣタグは、凹所の上でＮＦＣタグに接近して位置するＮＦＣスキャナにより容易に読み取られ得ることが分かっている。

【００２１】

例示の鍵チェイン４００が、図７Ａから７Ｄに示される。鍵チェイン４００は、その一つの表面に凹所４０４を有する金属フォブ４０２を有する。ＮＦＣタグ４０６が、タグ４０６とフォブ４０２の金属本体との間の絶縁層４０８と共に凹所４０４に付けられる。エポキシ又はプラスチック等の層４１０がタグ４０６を覆う。ロゴ、会社名又は他の印４１２がフォブ４０２に付けられてもよい。一意のシリアル番号又は他の一意の人間読み取り可能な識別情報４１４がフォブ４０２に印付けられてもよい。

【００２２】

ＮＦＣタグには、鍵識別子として一意のＵＲＬが埋め込まれてもよい。一意のシリアル番号（又は鍵チェイン名）が、符号化又は製造プロセスの間にＮＦＣタグ又は鍵チェインに印刷されてもよい。シリアル番号は、鍵交換を管理するために使用されるコンピュータシステム（例えば、下記の鍵交換サーバデータベース）における一意のＵＲＬにリンクされてもよい。

【００２３】

鍵交換システムにおけるこのようなキーフォブの使用は、以下を含む様々な利点を有する。即ち、１）金属フォブは、パーティ間の鍵の連続的な使用及び転送並びに保存ビンの硬質壁との物理的接触を要求する鍵交換システムのために十分な耐久性を有し得る。即ち、他の表面と接触し得るフォブのほとんどの表面は耐久性金属である。２）金属鍵チェインは特定の鍵保持装置と協調するように成形されてもよい。一部の実施形態では、金属は磁性金属を含んでもよく、鍵保持装置は磁性により鍵チェインの全体又は一部を保存場所に保持してもよい。３）金属フォブの凹所に非金属材料と共にアンチメタルＮＦＣタグを固定することは、このような金属フォブでＮＦＣタグを使用することを可能にする。４）ＮＦＣタグは鍵チェイン及び鍵識別子がスマートフォンにより検出されることを可能にし、クライアント装置との双方向性及び鍵交換システムの大量流通を可能にする。５）ＮＦＣタグのスマートフォン双方向性と併せて、鍵識別子としてＵＲＬを埋め込むことは、シ

ステムの大量流通を支援する広範な情報的及び商業的可能性を可能にする。６）リンクされたシリアル番号（又は名前）を含むことは、スキャナが利用できなくても、ユーザが多数の鍵セットのチェインを視覚的に区別して、所望の鍵セットを識別することを可能にする。

【００２４】

鍵交換システムは、承認されたユーザを有するコンピュータシステムを含む。ユーザは、任意の適切なやり方でコンピュータシステムに認証されてもよい。例えば、ユーザは、ユーザ名／パスワード認証を用いてコンピュータシステムにログオンしてもよい。任意の適切な認証方法が使用されてもよい。異なるユーザが、任意の特定の鍵のセットに関連して異なる権利を有してもよい。あるユーザ（例えば、物件所有者又は物件管理者）が、特定の鍵のセットに関連して管理者権限を有してもよい（そのユーザは「鍵管理者」と呼ばれてもよい）。管理者権限は、他人によるその鍵のセットへのアクセスを鍵管理者に承認させてもよい。

【００２５】

コンピュータシステムは、鍵セット及び鍵管理者により鍵セットに関係付けられる許可を記録するデータベースを保持する。このようなデータベースは、様々な異なるやり方で実装されてもよい。例えば、一実施形態では、各鍵セットが物件に関係付けられ、鍵管理者により与えられるアクセス権が物件に関係付けられる。このような実施形態では、アクセス権は、鍵セットと間接的に関係付けられる。他の実施形態では、データベースは、（鍵識別子によって）アクセス権が各鍵セットに直接的に関係付けられるように構築される。いずれの場合も、鍵管理者は、鍵交換所に保持されている鍵セットを解放するための条件を示すアクセス規則を追加することができる。鍵管理者は、典型的には、このようなアクセス規則を追加／修正及び消去するための権利を有する。規則がどのような形式を取っても、またデータベースに対してどのような特定の配置が選択されても、コンピュータシステムは、鍵セットに関係付けられる鍵トークンから鍵識別子を与えられると、その鍵識別子に直接的に又は間接的に関係付けられる規則にアクセスして、その規則に基づいて特定の個人が鍵セットへのアクセスを与えられるかどうかを決定するように構成される。

【００２６】

鍵管理者の利便性のため、システムは、名前を異なる物件及び／又は異なる鍵セットに関係付けることを鍵管理者に許可してもよい。例えば、物件がジュネーブにあるアパートである場合、鍵管理者は「ジュネーブアパート」という名前を物件及び／又はその鍵セットに関係付けることを選んでもよく、物件がボートである場合、鍵管理者は「ボート」という名前を物件及び／又はその鍵セットに関係付けることを選んでもよい。

【００２７】

ある個人から別の個人への鍵の物理的な転送が、鍵交換センター又は鍵アクセス場所において実行される。鍵交換センターは、鍵を引き渡す及び引き取るのに好都合な任意の場所に位置してもよい。例えば、鍵交換センターは、喫茶店又はコーヒーショップ、レストラン、コンビニエンスストア、ロビー、ショッピングセンター、空港、公共輸送ハブ、マリーナ、駐車場ビル及び駐車場等にあってもよい。

【００２８】

一部の実施形態では、各鍵交換センターは、鍵トークンを読み取ることができるスキャナを含む。スキャナは、鍵保存装置に組み込まれてもよく、又は適切に装備されたネットワーク接続されたコンピュータ又はハンドヘルド装置により別に提供されてもよい。鍵交換センターの各々において、鍵トークンは鍵セットの引き渡し及び引き取り時にスキャンされる。鍵トークンをスキャンすることにより、鍵識別子が読み取られる。次に、鍵識別子は、鍵交換センターから鍵交換ネットワークにおいて全ての鍵セットの場所を追跡する鍵交換サーバに中継される。

【００２９】

鍵交換サーバは、各鍵セットがその予期される場所に有るかどうかを検証してもよい。また、鍵交換サーバは、鍵交換センターにおいて個人が鍵セットを引き取ることを承認さ

れるかどうかを検証してもよい。アクセス要求が行われ且つ個人が鍵セットを引き取ることを承認されることが決定された場合、鍵交換サーバは、承認された個人が鍵セットへのアクセスを有することを可能にするように鍵交換センターにおいて装置に命令を提供する。また、鍵交換サーバは、スキャンされたトークンの鍵識別子を受信して、次に鍵セットの保存のために鍵交換センターにおける装置に命令を提供し、且つサーバにおける鍵に関係付けられる鍵の場所を更新することにより、鍵交換センターにおける鍵セットの引き渡しを調整してもよい。

【００３０】

図１は、鍵交換ネットワークにおける個人間で鍵セットの交換を処理するための例示的なシステム１００を示す。代表的な個人１０２、１０４及び１０６及び代表的な鍵１０３、１０５及び１０７が図１に示される。本明細書における説明のために、個人１０２は、１つ以上の鍵セットに対してアクセス権を割り当てる特権を有する管理ユーザである。個人１０４、１０６は、個人１０２等の管理ユーザにより鍵セットの１つへのアクセスが与えられ得るゲストユーザである。ユーザ１０２は、選択的に、他の鍵セットに関してはゲストユーザであってもよい。

【００３１】

システム１００は、鍵セットの場所を追跡して、管理ユーザ１０２と１人以上のゲストユーザ１０４、１０６との間等の個人間における鍵転送を調整するように構成される鍵交換サーバ１０８を含む。管理ユーザ１０２は、鍵セットに対するアクセス権を与えるために鍵交換サーバ１０８と通信してもよい。ゲストユーザ１０４、１０６は、鍵セットへのアクセスを要求するために鍵交換サーバ１０８と通信してもよい。

【００３２】

個人１０２、１０４及び１０６と鍵交換サーバ１０８との間の相互作用は、個人により使用されるクライアント装置１１２に表示される鍵交換インターフェースを介して処理されてもよい。クライアント装置は、鍵交換サーバ１０８と通信するように構成される任意の装置であり得る。例えば、クライアント装置は、パーソナルコンピュータ、端末、キオスク、又は鍵キャビネット若しくは他の装置と統合されるネットワーク接続型コントローラを含んでもよい。場合によって、クライアント装置は、タブレットコンピュータ、ラップトップコンピュータ又はスマートフォン等のモバイル装置を含んでもよい。特定の実施形態では、全てのユーザが同じタイプのアカウントを有していて単一の統合型インターフェースを利用してもよいが、インターフェース内では、一部の鍵セットに関しては管理特権を有しており一部の他の鍵セットに関してはゲスト特権のみを有していてもよい。

【００３３】

鍵交換サーバ１０８が鍵セットの場所を追跡して鍵セットに割り当てられたアクセス権を管理することを可能にするために、鍵交換ネットワークにおける各鍵セットに一意の鍵識別子が割り当てられる。鍵識別子は、鍵トークンに符号化されてもよい。例えば、図１の実施形態において、鍵１０３の一意の鍵識別子は、鍵１０３に取り付けられた鍵チェイン１０３ＡにおけるＮＦＣ（Ｎｅａｒ　Ｆｉｅｌｄ　Ｃｏｍｍｕｎｉｃａｔｉｏｎ）タグ１０３Ｂに符号化されてもよい。図１における鍵チェイン１０３Ａには１つだけの代表する鍵１０３が取り付けられるように示されているが、複数の鍵がチェイン１０３Ａに取り付けられてもよいことが理解されるべきである。例えば、物件がマンションのユニットである場合、そのユニットへのアクセスを得るために必要な全ての鍵、例えば共通物件に対するキーフォブ及びそのユニットへの家の鍵が鍵チェイン１０３Ａに取り付けられてもよい。鍵セットが複数の鍵を含む一部の実施形態では、鍵セットの一部であるべき全ての鍵が存在することをシステムが検証することができるように、トークンが選択的に各鍵に取り付けられ又は埋め込まれてもよい。

【００３４】

管理ユーザ１０２が鍵セット１０３へのアクセス権を制御する特権を有すると仮定する。管理ユーザ１０２は、ゲストユーザ１０４に鍵セット１０３を移動させたい場合、例えば、鍵交換サーバ１０８にこうしたアクセス権を伝達することによりゲストユーザ１０４

にアクセス権を与えてもよい。アクセス権は、ゲストユーザ１０４が鍵セット１０３へのアクセスを有することを許可される期間等、アクセスに対する制限を有してもよい。鍵交換サーバ１０８は、鍵管理者により鍵セットに割り当てられたアクセス規則を記憶するアクセス規則データベース１３４を有する。各アクセス規則は、（直接的又は間接的に）特定の鍵識別子に及び承認されたユーザにリンクされてもよい。

【００３５】

管理ユーザ１０２は、管理ユーザ１０２によって使用されるクライアント装置１１２Ａに提供される管理鍵交換インターフェース１１０を介して鍵交換サーバ１０８にアクセス権を伝達してもよい。クライアント装置１１２Ａは、インターネットを介して鍵交換サーバ１０８と通信してもよい。

【００３６】

管理ユーザ１０２は、鍵セット１０３を所有する場合、承認されたゲストユーザ１０４が後で引き取ることができるように、鍵交換センターに鍵セット１０３を引き渡すことができる。鍵交換センターは、図１に示されるように、鍵セットを保存するために鍵キャビネット又は他の鍵保持装置１２０を有してもよい。特定の実施形態では、鍵セット１０３が鍵交換センターで引き渡されるとき、符号化された一意の鍵識別子を読み取るためにその鍵トークン（例えば、鍵チェイン１０３Ａ）がスキャンされる。鍵１０３は、鍵キャビネット１２０内の利用可能なビン（例えば、ビン１２５Ｃ）に配置される。場合によって（鍵セットが以前のユーザによって鍵交換センターに返却されたばかりである場合等）、鍵セット１０３は、鍵交換センターに既に置かれており、鍵引き渡しは不要である。

【００３７】

一旦鍵セット１０３が鍵交換センターに到着すると、鍵セット１０３の鍵識別子及び鍵セット１０３の場所（例えば、鍵交換センターの場所及び鍵セット１０３が保存される鍵ビンの番号）が鍵交換サーバ１０８に伝達される。鍵交換サーバ１０８は、鍵識別子を場所（及び鍵セットに関連する他の情報）と関係付ける鍵在庫データベース１３３を保持する。鍵交換サーバ１０８は、鍵在庫データベース１３３においてその場所に保持されている鍵セットに対する鍵識別子と場所情報を関係付ける。一部の実施形態では、鍵ビンは、（例えば、鍵在庫データベース１３３を使用することにより、どの鍵ビンが利用可能であるかを決定することができる）鍵交換サーバ１０８により指定されて、鍵交換センターの場所に伝達される。

【００３８】

管理ユーザ１０２により設定されるアクセス規則に従ってゲストユーザ１０４が鍵セット１０３へのアクセスを有することを承認される頃に、鍵交換サーバ１０８は、鍵セット１０３が保持されている鍵交換センターの場所の通知をゲストユーザ１０４に自動的に提供することができる。この通知は、Ｅメール、テキストメッセージ、音声メッセージ、又はゲストユーザの鍵交換アカウントページに現れるメッセージ等の形式で提供されてもよい。通知は、選択的に、鍵交換所の営業時間、及び鍵交換所に行くための方向等の追加の情報を含んでもよい。

【００３９】

鍵セット１０３を取得するために、ゲストユーザ１０４は、鍵セット１０３が置かれている鍵交換センターを訪問して、鍵引き取り要求を鍵交換サーバ１０８に伝達してもよい。この要求は、ゲストユーザ１０４によって使用されるクライアント装置１１２Ｂに提供されるゲスト鍵交換インターフェース１１１を介してゲストユーザ１０４により鍵交換サーバ１０８に伝達されてもよい。ゲストユーザは、ログイン又は他の認証情報の提供を促されてもよい。クライアント装置１１２Ｂは、インターネットを介して鍵交換サーバ１０８と通信してもよい。

【００４０】

鍵引き取り要求のために提供される情報に基づいて、鍵交換サーバ１０８は、アクセス規則データベース１３４を検査して、ゲストユーザ１０４が鍵セット１０３へのアクセスを有することを検証する。ゲストユーザ１０４がそのように承認されていることが決定さ

れると、鍵交換サーバ１０８は、ゲストユーザ１０４が鍵セット１０３へのアクセスを有することを可能にするための命令を鍵交換センターに中継する。一部の実施形態では、この命令は、鍵セット１０３が保存されている鍵キャビネットにおける特定のビンを識別するビン番号の識別性を含む。ビン番号は、鍵交換センターにおいてクライアント装置１１２で受信され得る。それから、鍵交換センターをホスティングするビジネスの従業員等、鍵交換センターで鍵キャビネット１２０へのアクセスを有する人物が、適切なビンを開いて、承認されたゲストユーザ１０４に鍵セット１０３を与えてもよい。

【００４１】

一部の実施形態では、特に鍵を要求するために使用されるクライアント装置１１２Ｂがシステム１００のオペレータによって制御されない場合（例えば、クライアント装置１１２Ｂがゲストユーザのタブレット又は携帯電話である場合）、鍵交換サーバ１０８は、クライアント装置１１２Ｂから場所情報を要求してもよい。場所情報は、例えば、クライアント装置１２２ＢのＧＰＳシステムによって提供されてもよい。鍵交換サーバ１０８は、クライアント装置１１２Ｂから受信した場所情報を鍵交換所の既知の座標と比較してもよく、クライアント装置１１２Ｂから受信した場所情報が鍵交換所の場所と十分に近接して一致する場合にだけ要求された鍵セットの解放をゲストユーザに承認してもよい。

【００４２】

ゲストユーザ１０４に鍵セット１０３を渡す前に、鍵セット１０３は、鍵識別子を読み取るためにスキャンされて、正しい鍵セットが取得されていることを検証してもよい。

【００４３】

一部の実施形態では、鍵セットの解放が自動的に制御される自動鍵保持装置に鍵セットが保存される。例えば、鍵キャビネットのビン又は引き出しを開けること又は鍵の他の提示が、鍵交換サーバ１０８の指示を受けて制御及び処理装置により自動化及び制御されてもよい。自動制御鍵キャビネット又はキオスクが、ユーザ間の鍵交換を処理するために鍵交換センターに設置されてもよい。一部の実施形態では、ホステル、ホテル又は鍵へのアクセスを人物に提供する他の施設のスタッフが居る受付／コンシェルジュデスクを置換するための自動受付システムの一部として鍵交換を管理するように自動制御鍵キャビネットが設置される。

【００４４】

特に、図１に示された実施形態は、鍵セットを含む個々の区画又はビン（例えば、図１のビン１２５Ａ、１２５Ｂ及び１２５Ｃ）の引き出し又はドアの開閉を制御するために制御及び処理装置１２２を有する鍵キャビネットを含む。

【００４５】

鍵交換サーバ１０８から命令を受信すると、制御及び処理装置１２２は、例えば、特定の区画のドアを開け、又はビンの引き出しを滑り出させ、又は分配開口の中へと鍵セットを解放する。ビンの引き出しを開けることにより、ゲストユーザがビンに保存された鍵セットを引き取ることが可能になり、又は管理ユーザ若しくは他のユーザが鍵セットをビンの中に配置することが可能になる。別の実施形態では、自動化キャビネットは、キャビネットが関連するビン又は提示されている鍵セットを機械的に移動させるためにユーザによって鍵セットを置く及び取るための単一の容器を有してもよい。

【００４６】

図１のクライアント装置１１２Ａ、１１２Ｂを含むクライアント装置１１２は、モバイル装置、パーソナルコンピュータ、ラップトップ、タブレット又はインターネットに接続して鍵交換サーバ１０８と通信することが可能な任意の他の装置（特注のコンピュータ端末及びキオスクを含む）含んでもよい。一部の実施形態では、クライアント装置１１２Ｂは、鍵交換所において鍵キャビネット１２０に組み込まれてもよい。

【００４７】

本明細書に記載の一部のステップは、鍵識別子を読み取るために鍵トークンをスキャンすることを含む。例えば、上記のように、鍵トークンは、鍵交換センターにおける鍵セットの引き渡しの間にスキャンされる。また、鍵トークンは、鍵交換センターでの鍵セット

の引き取りの間にスキャンされてもよい。鍵トークンは、符号化された鍵識別子を読み取ることが可能な装置によりスキャンされてもよい。鍵識別子が鍵チェインのＮＦＣタグに符号化される実施形態では、鍵は、例えば、ＮＦＣ使用可能なスマートフォン又はタブレット等のＮＦＣ使用可能装置によりスキャンされてもよい。装置は、鍵交換サーバ１０８に鍵識別子を送信する鍵交換アプリケーションを実行するように構成されてもよい。

【００４８】

図１のシステム１００又はその一部は、本明細書に記載の１つ以上の方法を実装するように構成されてもよい。方法は、図２～５を参照して以下により詳細に記載される。

【００４９】

図２は、一実施形態により管理ユーザが鍵セットにアクセス権を割り当てるための方法１５０を示す。例えば、方法１５０は、管理ユーザ１０２がゲストユーザ１０４に鍵セット１０３（図１）へのアクセスを与えることを可能にするように実行され得る。方法１５０は、管理ユーザが個人に対して新しいアクセス規則を作成することを望む度に繰り返され得る。方法１５０は、図１の鍵交換サーバ１０８のプロセッサにアクセス可能なプログラムメモリに含まれるソフトウェアとして実装されてもよい。プロセッサは、ソフトウェアにより提供されるソフトウェア命令を実行することにより方法を実装する。管理ユーザは、図１の管理鍵交換インターフェースを介してソフトウェアに入力を提供することができる。

【００５０】

方法１５０は、ブロック１５２で、管理ユーザの認証情報を受信することにより開始する。このような認証情報は、例えば、ユーザによって提供されるユーザのアカウント名、Ｅメール及び／又はパスワード１５３を含んでもよい。このような認証情報は、図１のクライアント装置１１２Ａで提供される管理鍵交換インターフェース１１０によりアカウントへのログインページにおいて管理ユーザにより提供されてもよい。管理ユーザの認証情報が鍵交換サーバ１０８により検証された後で、管理ユーザは、パーソナル管理ページ１１４（図１を参照）へのアクセスが提供されてもよい。ここで、管理ユーザは、（インターフェースの表現次第で）管理特権を有する物件、鍵及び／又は鍵識別子のリストを閲覧することができる。また、リストは、各鍵セットの現在の場所（例えば、鍵セットが鍵交換センターに保持されている場合の鍵アクセス場所、又は以前のユーザにより引き取られた場合の鍵セットの最後に知られた所在地）を示してもよい。ブロック１５４において、鍵交換サーバ１０８は、アクセス規則が直接的又は間接的に関係付けられる１つ以上の鍵セットを直接的又は間接的に識別するリスト（例えば、鍵の名前又は識別子１５５）から管理ユーザの選択を受信する。

【００５１】

方法１５０は進んで、ブロック１５６において、選択された鍵セットへのアクセスを有し得る承認されたゲストの識別子１５７、及びブロック１５８において、承認されたゲストがアクセスを有し得る期間１５９の詳細を管理ユーザから受信することにより選択された（複数の）鍵セットに対するアクセス規則を生成する。ゲスト識別子１５７は、Ｅメールアドレス、ユーザアカウント名、電話番号、クレジットカード情報、名前及び住所、又は鍵交換ネットワークにおけるユーザを一意に識別する任意の他の識別子であってもよい。期間１５９は、承認されたゲストが鍵セットへのアクセスを有する（複数の）日及び／又は（複数の）時間を示してもよい（例えば、承認されたゲストは１泊の宿泊を予約しており、２月７日午後３時から２月８日午前１０時の間にアクセスが与えられる）。場合によっては、期間１５９は、反復性の期間（例えば、承認されたゲストは毎月第２月曜日の午後１２時から午後４時の間に鍵へのアクセスを有することを承認される掃除人）を含み、又は期間は無制限であると指定されてもよい。場合によっては、特定のアクセス期間は特定されなくてもよい（即ち、ゲストユーザは、鍵セットが鍵アクセス場所に預けられた後でいつでも鍵セットを受け取る権利が与えられてもよい。

【００５２】

ブロック１５８において承認された期間１５９を割り当てる前に、期間１５９が鍵セッ

トに対して以前に割り当てられたアクセス規則と矛盾するかどうかを決定するために、鍵交換サーバ１０８によって検査が行われてもよい。例えば、異なるゲストユーザが同じ又は重複する期間に同じ鍵セットへのアクセスを既に割り当てられていた場合に、期間１５９は、警告を生成し又は割り当てられない。

【００５３】

ブロック１５６及び１５８において一旦アクセス規則が生成されると、方法１５０は、管理ユーザが同じ又は他の鍵セットに影響を与える更なるアクセス規則を生成することを望む場合に、ブロック１５４に進むことにより繰り返されてもよい。

【００５４】

管理ユーザは、取得時に鍵トークン及び鍵識別子によって識別される鍵セットへの管理特権を割り当てられ得る。例えば、物件に関連する鍵交換システムを使用することを望むユーザは、（例えば、ＮＦＣ鍵チェインの形式で）新しい鍵トークンを取得してもよい。アプリケーションを実行するＮＦＣ使用可能なクライアント装置が鍵チェインに取り付けられ、鍵識別子をＮＦＣ鍵チェインから読み取らせて、鍵交換サーバ１０８に送信させることができる。管理ユーザは、クライアント装置におけるインターフェースを介して、自身のユーザ認証情報を提供して、自身が鍵管理者として割り当てられることを要求することができる。次に、鍵交換サーバ１０８は、管理ユーザを鍵識別子と関係付けるために管理ユーザのデータベース１３２（図１を参照）を更新することができる。

【００５５】

鍵識別子を管理ユーザと関係付けるために他の方法が使用され得る。例えば、ユーザは、鍵トークンで見られる一意のシリアル番号を自身のアカウントに入力してもよく、又は鍵交換サービスは、鍵トークンを発送又は提供する前にユーザのアカウントと鍵識別子をリンクしてもよい。次に、鍵識別子は、管理ユーザが物件又はユーザアカウントにおけるアクセス規則を含む他のデータ表現にアクセス規則を追加する又は関係付ける特権を有する鍵セットのリストに追加され得る。

【００５６】

図３は、鍵セットが鍵交換センターに引き渡される度に実行され得る方法２００を示す。例えば、方法２００は、承認されたゲストユーザ１０４（図１）が後で引き取ることができるように、管理ユーザ１０２が鍵交換センターに鍵セット１０３を引き渡すと実行され得る。また、方法２００は、ゲストユーザ１０４が、鍵セットの使用を終えた後で鍵交換センターに鍵セット１０３を返却し／引き渡している場合に実行され得る。方法２００は、図１の鍵交換サーバ１０８のプロセッサにアクセス可能なプログラムメモリに含まれるソフトウェアとして実装され得る。プロセッサは、ソフトウェアにより提供されるソフトウェア命令を実行することにより方法を実装する。

【００５７】

方法２００は、鍵交換センターで鍵トークンをスキャンすることにより開始される。例えば、ユーザが引き渡すための鍵セットを持って鍵交換センターに到着すると、ＮＦＣ使用可能クライアント装置１１２Ｂが、ＮＦＣタグに符号化された鍵識別子を読み取るために鍵トークンを含む鍵チェインにタップされてもよい。この鍵識別子は、クライアント装置１１２Ｂ上の鍵交換アプリケーションによって鍵交換サーバ１０８に送信されてもよい。一部の実施形態では、クライアント装置１１２Ｂは、鍵交換所専用に関係付けられるクライアント装置（スタンドアロン装置又は鍵保存キャビネットに統合されるコントローラ等の装置を含み得る）又はユーザのタブレット若しくはスマートフォン等の携帯型装置のいずれであってもよい。方法２００は、ブロック２０２において、クライアント装置１１２Ｂから鍵識別子２０３を受信する。

【００５８】

ブロック２０４において、方法２００は鍵の場所を識別する。これは、様々なやり方で行われてもよい。例えば、方法２００は、クライアント装置１１２Ｂから場所データ２０５を受信して、このようなデータに基づいて鍵の場所（例えば、鍵交換センターの場所）を決定してもよい。このような場所データ２０５は、ＧＰＳデータ、モバイルネットワー

ク場所データ、及び／又はユーザデータ入力、又は鍵交換サーバ１０８がそのデータベース等の場所にリンクすることができる装置識別データを含んでもよい。

【００５９】

ブロック２０６において、ビン番号２０７が鍵に割り当てられて、鍵を保存するために鍵キャビネット内の利用可能なビンが識別される。ビン番号の割り当ては鍵交換サーバ１０８、制御及び処理装置１２２により実行されてもよく、又は人物が預けられる鍵セットのために利用可能なビンを選択してもよい。ビンの割り当てが鍵交換サーバ１０８によって行われない場合、選択されたビンが鍵交換サーバ１０８に伝達される。

【００６０】

ブロック２０８において、識別された鍵の場所及び割り当てられたビン番号は、ブロック２０２で受信された鍵識別子２０３に関係付けられる。ブロック２０９において、鍵交換サーバ１０８は、鍵セットがビンに配置され得るように、割り当てられたビンを開けさせるための信号を鍵キャビネット１２０の制御及び処理装置１２２に送信する。鍵キャビネット１２０が制御及び処理装置１２２を有さない他の実施形態では、ブロック２０９におけるステップは、鍵交換センターで働く人物がどのビンに鍵を保存すべきかが分かるように、鍵交換センターにおけるクライアント装置に割り当てられたビン番号を送信するステップで、又は鍵交換センターで働く人物が開いたビンに鍵を置いて、その情報がビンセンサを介して又はクライアント装置インターフェースを介して労働者によりサーバに送信されることにより代替されてもよい。

【００６１】

一部の実施形態では、鍵管理者は、例えば、ゲストユーザが鍵セットを引き取った後で、又はゲストユーザが特定の規則に従って鍵セットを引き取る権利を与えられると、選択的な命令又は解放される他の情報をゲストユーザに提供するように促されてもよい。情報は、例えば、鍵セットに関係付けられる物件への地図、物件の手入れの指示等を含んでもよい。一部の実施形態では、システムは、物件等の場所等のシステムで利用可能であり得る情報を含む命令に対してテンプレートを提供する。一部の実施形態では、鍵管理者は、システムが物件のゲストユーザに同じ命令を自動的に提供することができるように、その物件に関する命令のセットを記憶するオプションを有してもよい。

【００６２】

方法２００は、鍵識別子２０３に直接的又は間接的に関係付けられている任意のアクセス規則２１１を受信することによりブロック２１０に進む。アクセス規則の１つに従って鍵セットへのアクセスが与えられているユーザが居て、そのユーザの承認されたアクセス期間の開始が既定時間内である（例えば、あと一日より少ない）場合、方法２００は、承認されたユーザに現在の鍵の場所２１３及び任意の必要とされる引き取り命令又はコード２１５を公開することにより進む。このような引き取り命令又はコード２１５は、鍵引き取り時にシステム又は鍵管理者がゲストユーザを認証することにより生成されてもよい。

【００６３】

方法２００のステップ２１０及び２１２は、他の時間に実行されてもよい。例えば、鍵交換サーバ２０８は、アクセス規則を周期的に読み取り又は処理して、次の承認されたアクセス期間の開始が既定時間内である承認されたユーザに鍵の現在の鍵の場所２１３を公開するように構成されてもよい。例えば、鍵交換サーバ２０８は、承認されたアクセス期間の開始の１日前に、現在の鍵の場所２１３及び引き取り命令又はコード２１５を承認されたユーザに公開するように構成されてもよい。

【００６４】

図４は、一実施形態により鍵セットへのアクセスを個人に提供するために鍵引き取りにおいて実行され得る方法２５０を示すフローチャートである。例えば、方法２５０は、鍵セット１０３（図１）を引き取るためにゲストユーザ１０４が鍵交換センターに到着すると実行され得る。方法２５０は、図１の鍵交換サーバ１０８のプロセッサにアクセス可能なプログラムメモリに含まれるソフトウェアとして実装され得る。プロセッサは、ソフトウェアにより提供されるソフトウェア命令を実行することにより方法を実装する。

【００６５】
方法２５０は、ブロック２５１で、ゲストユーザの認証情報２５３を受信することにより開始する。このような認証情報は、例えば、ユーザによって提供されるユーザのアカウント名、Ｅメール及び／又はパスワード２５３を含んでもよい。このような認証情報は、クライアント装置１１２Ｂ（図１）で提供されるゲスト鍵交換インターフェース１１１のログインページにおいてゲストユーザにより提供されてもよい。認証情報は、追加的に又は代替的に、１つ以上のＰＩＮ（ブロック２５２においてアクセス命令又はコード２１５が提供されるＰＩＮ等）、携帯電話を介した二重認証、又はゲストに関係付けられる一意の識別子を含むＮＦＣタグ等の一意の物理的アクセストークンの提示を含む。

【００６６】
入力されたゲストユーザの認証情報２５３は、鍵交換サーバ１０８がユーザ認証情報データベース１３１（図１を参照）でユーザに関係付けられる認証情報のセットと比較することにより検証されてもよい。ゲストユーザ認証情報を検証した後で、ゲストユーザは、ブロック２５２において、他のアクセス命令又はコード２１５を提供するように促されてもよい。例えば、ゲストユーザは、方法２００（図３）のブロック２１２において、鍵セットに対する引き取りアクセスコード２１５を以前に通知されていてもよい。ゲストユーザは鍵アクセス場所において多くの異なる鍵セットに対するアクセス特権を有し得ると考えられるので、アクセスコード２１５は、どの鍵セットへのアクセスをゲストユーザが要求しているかを鍵交換サーバ１０８が決定するのを支援してもよい。例えば、ゲストユーザは、多くの異なる物権の鍵に対するアクセス権を有する掃除人であってもよい。追加のアクセスコード２１５が要求されず、鍵交換センターにおけるどの鍵セットにゲストがアクセスを希望しているかが不明であれば、ゲストは、アクセスイベントに対して１つの鍵セットを選択するように促されてもよい。

【００６７】
ブロック２５４において、方法２５０は、鍵アクセス要求が行われているクライアント装置１１２Ｂの場所及び時間を識別する。鍵アクセス要求の時間は、例えば、鍵交換サーバ１０８が鍵交換サーバ１０８にアクセス可能なタイミング情報２５７のソースに問い合わせを行うことにより決定されてもよい。クライアント装置の場所は、クライアント装置１１２Ｂから場所データ２５５を受信して、このようなデータに基づいてクライアント装置の場所（例えば、鍵交換センターの場所）を決定することにより識別されてもよい。このような場所データ２５５は、クライアント装置１１２ＢからのＧＰＳデータ、クライアント装置１１２Ｂからのモバイルネットワーク場所データ、クライアント装置１１２Ｂから入力されたユーザデータ、又は鍵交換サーバ１０８がそのデータベースの場所にリンクすることができるクライアント装置１１２Ｂからの装置識別情報、又はボタン、スキャナ又は鍵交換所における設備との他の相互作用を介して達成される物理的存在検証、及び／又は同類を含んでもよい。

【００６８】
ブロック２５６において、ゲストユーザに対する鍵アクセス権を規定する要求された鍵に関する関連アクセス規則２１１が取得される。ブロック２５８において、方法２５０は、ゲストユーザの要求を認証することにより進む。例えば、ブロック２５８において、鍵アクセス要求が承認されたアクセス期間内に行われるかどうかを決定するために、鍵アクセス要求の時間が、アクセス規則に規定される承認されたアクセス期間と比較され得る。更に、ブロック２５８において、ブロック２５４で決定されたクライアント装置１１２Ｂの場所は、要求された鍵セットに対する鍵識別子に関係付けられる鍵アクセス場所と比較されてもよい。これは、鍵セットを引き取るためにゲストユーザが正しい場所に居るかどうかを決定するのに役立ち得る。鍵セットが他の場所に位置しているか、又は鍵アクセス要求が承認されたアクセス期間外に行われている場合、鍵アクセス要求は拒否される。

【００６９】
鍵アクセス要求が認証されると、方法２５０は、クライアント装置１１２Ｂにアクセス命令を送信することによりブロック２６０に進む。例えば、例示の実施形態では、アクセ

ス命令は、鍵セットが保存されるビンのビン番号２０７を含む。ビン番号２０７は、（例えば、図３の方法２００のブロック２０８を参照して先に記載されたように）鍵セットが引き渡された時間又はより最近の鍵在庫のスキャンにおいて要求された鍵セットの鍵識別子に以前に関係付けられていたであろう。鍵キャビネットへのアクセスを有する鍵交換センターの人物は、指定されたビンから要求された鍵セットを取得するためにビンを開けるためのブロック２６０で提供されるアクセス命令を使用することができる。

【００７０】

ブロック２６２において、方法２５０は、鍵セットに対する鍵識別子２０３を受信することにより正しい鍵セットが取得されたことを検証する。例えば、ゲストユーザに鍵セットを渡す前に、鍵セットを取得するためにビンを開けた人物は、鍵チェインのＮＦＣタグに符号化された鍵識別子を読み取るためにＮＦＣ使用可能クライアント装置１１２Ｂに対して鍵チェインをタップしてもよい。この鍵識別子は、クライアント装置１１２Ｂ上の鍵交換アプリケーションによって鍵交換サーバ１０８に送信されてもよい。次に、鍵交換サーバ１０８は、スキャンされた鍵識別子が要求された鍵セットのそれに対応するかどうかを検証してもよい。

【００７１】

図５は、別の実施形態により鍵セットへのアクセスを個人に提供するために鍵引き取りにおいて実行され得る方法３００を示すフローチャートである。例えば、方法３００は、鍵セット１０３（図１）を引き取るためにゲストユーザ１０４が鍵交換センターに到着すると実行され得る。方法３００は、図４の方法２５０に部分的に似ている。類似のステップ又はコンポーネントを記すために同様の参照番号が用いられる。方法３００は、図１の鍵交換サーバ１０８のプロセッサにアクセス可能なプログラムメモリに含まれるソフトウェアとして実装され得る。プロセッサは、ソフトウェアにより提供されるソフトウェア命令を実行することにより方法を実装する。入力は、クライアント装置１１２Ｂ（図１を参照）に表示されるゲスト鍵交換インターフェース１１１を介してソフトウェアに提供され得る。

【００７２】

方法３００は、鍵キャビネットが、（例えば、鍵キャビネットの引き出し又はビンを開ける及び閉めることにより）鍵キャビネットに保持されている鍵セットへのアクセスを制御する制御及び処理装置１２２を有する場合に実行されてもよい。鍵キャビネット１２０の制御及び処理装置１２２は、インターネットを介して鍵交換サーバ２０８と通信してもよい。方法３００は、方法２００と同様のステップ２５１，２５２，２５４，２５６及び２５８を含む。しかしながら、方法３００は、方法３００のブロック２６４で始めて方法２５０とは異なる。（方法２５０のブロック２６０に従って）クライアント装置１１２Ｂにアクセス命令を送信する代わりに、ブロック２６４において、方法３００は、正しい鍵セットが鍵の識別子に関係付けられるビンに存在していることを検証する。この検証ステップは、鍵ビンに設けられるスキャナにより実装することができ、これはビンに含まれる鍵トークン上のＮＦＣタグをスキャンすることが可能である。例えば、鍵交換サーバ２０８は、識別されたビン（又は鍵識別子２０３を探して鍵キャビネット１２０内の全てのビン）における鍵トークンの鍵識別子２０３を読み取るようにスキャナを起動するための命令を鍵キャビネット１２０の制御及び処理装置１２２に中継してもよい。次に、スキャンされた鍵識別子は、検証のために制御及び処理装置１２２によって鍵交換サーバ２０８に中継される。正しい鍵セットがビンに存在すると決定される場合、次に、ブロック２６８において、鍵交換サーバ２０８は、鍵セットを含むビンを開くか又はそれ以外で鍵セットをアクセス可能にするための命令２６９を制御及び処理装置１２２に送信する。一部の実施形態では、システムは、鍵セットに関連する追加の情報（例えば、鍵交換所から鍵セットが属する物件に至るための方向）を（例えば、Ｅメール、又はテキストメッセージ等によって）鍵セットの受け取り人に自動的に提供する。

【００７３】

方法２５０のブロック２６２及び方法３００のブロック２６４における鍵検証ステップ

は、ゲストユーザに誤った鍵セットが与えられることを防ぐのに役立ち得る。例えば、要求された鍵とは異なる鍵セットがビンに誤って配置されている可能性があり、検証ステップはこのエラーを見つけるであろう。上記の検証ステップは、全ての実施形態に対して必要ではない。所定の実施形態において、検証ステップは省略され、又は何らかの他のやり方で行われる。

【００７４】

鍵交換サーバ１０８は、図１に示されるように、ゲストユーザ及び／又は管理ユーザ等の１人以上のユーザが１つ以上のイベントの通知をいつ受信するかを決定する１つ以上の通知生成器１４０を選択的に実装してもよい。通知は、鍵交換サーバ１０８によって生成されてもよく、及び／又はユーザによって提供される情報からなり又はこのような情報を組み込んでもよい（たとえば、鍵管理者は、ゲストユーザに提供される１つ以上の通知に含まれるコンテンツを提供してもよい。このようなコンテンツは、ユーザインターフェースによってクライアント装置から鍵交換サーバ１０８にアップロード又は入力されてもよい）。

【００７５】

通知生成器は、１つ以上の異なる通知を配布するように構成されてもよい。各通知は、対応する基準に関係付けられてもよい。通知生成器１４０は、通知が配布されるべき場合を識別するために鍵アクセスサーバの１つ以上のデータベースを検索するように構成されてもよい。一部の実施形態では、通知生成器１０４は、通知がいつ誰に対して配布されるべきかを識別するために鍵在庫データベース１３３及び規則データベース１３４等の鍵交換サーバ１０８によりアクセス可能なデータベースを検索するように構成される。例えば、通知生成器１４０は、ゲストユーザ１０４がビン１２５から鍵セット１０３をいつ受信したかを鍵管理者に自動的に通知してもよい。

【００７６】

別の非限定的な例示として、通知生成器１４０は、（鍵セット１０３に関係付けられるアクセス規則から）ゲストユーザ１０４が鍵セット１０３にアクセスし得る最早時間、及びその時間が近いとき（例えば、時間が、１日先、数時間先、又は何らかの他の持続期間だけ先であるとき）を決定してもよく、交換されるべき鍵セット１０３が鍵交換所に（例えば、鍵保持装置１２０のビン１２５に）存在することを検証するために検査してもよい。鍵セット１０３が存在する場合（例えば、鍵在庫データベース１３３により示されるように）、通知生成器１４０は、鍵セット１０３が保持されている鍵交換所においてすぐに鍵セットが利用可能になることを自動的にゲスト１０３に通知してもよい。鍵セット１０３が存在しない場合、通知生成器は、鍵セット１０３がまだ鍵保持装置１２０に配置されていないことを対応する鍵管理者に通知してもよく、一部の実施形態では、鍵管理者が間に合うように鍵交換所に鍵セット１０３を引き渡すのを支援するための情報又は命令を提供してもよい。

【００７７】

通知は、例えば、Ｅメール、テキストメッセージ、音声メッセージ、又はユーザの鍵交換アカウントページに現れるメッセージ等によるものであってもよい。通知生成器１４０は、所定のイベントが発生すると同時に通知を生成してもよく、及び／又はこのようなイベント発生の前に警告する通知を生成してもよい。例えば、通知生成器１４０は、鍵セット１０３が（上記のように）ビン１２５に配置された鍵セット１０３の最早利用可能性より前にゲスト１０４に通知してもよく、又は鍵セット１０３が利用可能になる瞬間までその通知を延期してもよい。以下の例は、後者の手法を用いるが、期限又は他の決定された時間の前に通知を提供するように適合されてもよい。

【００７８】

図９は、通知生成器により実行され得る非限定的な例の通知スケジュール方法４００を示す。ブロック４１０において、通知生成器は、ゲストユーザ１０４が鍵セット１０３にアクセスする許可を有する期間を決定する。これは、時間ベースのアクセス制限に関してアクセス規則データベース１３４を検査することにより実行されてもよい。その期間が開

始すると（即ち、ゲストユーザ１０４が鍵セット１０３にアクセスする許可を取得すると）、通知生成器はブロック４１５に進んで、鍵セット１０３が鍵交換所に（即ち、図１のビン１２５Ｃに）存在するかどうかを決定する。

【００７９】

鍵セット１０３が存在しない場合、通知生成器はブロック４２０に行き、通知生成器の設定に従って、通知を送信して鍵セット１０３に関係付けられる鍵管理者に鍵セット１０３を預けることを思い出させ、ゲストユーザ１０４に鍵セット１０３が預けられていないことを知らせ、又はその両方を行う。そうでなく、鍵セット１０３が存在する場合、通知生成器はブロック４２５に行き、鍵セット１０３が預けられておりアクセス可能であることをゲストユーザ１０４に通知する。

【００８０】

ブロック４２５から、通知生成器１４０は、ブロック４３０に進む。ここで、通知生成器１４０は、鍵セット１０３がいつまでに鍵交換所から除去される予定であるかを決定する。その時間が起きる前に、鍵セット１０３がゲストユーザに提供される場合、通知生成器はブロック４３７に行き、その除去を検出し、その後、ブロック４４５に行き、鍵管理者にその除去を通知する。その時間が起きる前に鍵セット１０３が除去されない場合、通知生成器はブロック４３５に行き、時間の経過が検出され、その後、ブロック４４０に行き、鍵セット１０３が該当する時間までに除去されなかったことを鍵管理者に通知する。鍵セット１０３が後で除去される場合、通知生成器１４０はブロック４３７に行く。

【００８１】

ブロック４４５から、通知生成器はブロック４５０に行き、いつまでに鍵セット１０３がゲストユーザ１０４によって鍵交換所に返却されるようスケジュールされているかを決定する。その時間が起きる前に、鍵セット１０３が鍵交換所に預けられる場合、通知生成器はブロック４６５に行き、その返却を検出し、その後、ブロック４７０に行き、鍵管理者に鍵セット１０３の返却を通知する。鍵セット１０３がその時間が起きる前に返却されない場合、通知生成器はブロック４５５に行き、時間の経過が検出され、その後、ブロック４６０に行き、鍵セット１０３が該当する時間までに除去されなかったことをゲスト１０４に通知する。鍵セット１０３が後で返却される場合、通知生成器１４０はブロック４６５に行く。

【００８２】

通知生成器１４０は、提供される場合、鍵交換サーバ１０８で実行されるソフトウェアで、鍵交換サーバ１０８に組み込まれ又はアクセス可能なハードウェアで、又はソフトウェア及びハードウェアの混合で実装されてもよい。通知生成器１４０は、提供される場合、鍵交換サーバ１０８の他の部分と統合されてもよく、又は別個のコンポーネント又はサブシステムとして実装されてもよい。

【００８３】

図６Ａ、６Ａ及び６Ｂは、一実施形態による鍵交換アプリケーションのグラフィカルユーザインターフェースの例示のスクリーンショットである。図６Ａ及び図６Ｂは、管理ユーザの鍵セットへのアクセス権をゲストユーザに割り当てらるために管理ユーザにより使用され得る管理鍵交換インターフェースの例示的な画面を示す。図６Ｃは、要求された鍵セットが特定の鍵交換センターでの引き取りに利用可能であるという通知をゲストユーザに表示するゲストユーザ鍵交換インターフェースの例示の画面を示す。

【００８４】

鍵セットの預け入れ及び貸し出し並びにそれ以外の鍵交換サーバ１０８との相互作用を支援するために様々なクライアントコンピュータ装置が使用されてもよい。例えば、ＮＦＣ使用可能タブレット又は他の類似の装置が、鍵引き取り／引き渡しを処理するために使用されてもよい。装置は、鍵セットのトークンをスキャンする等の鍵交換センターの機能を実行するアプリケーションを含んでもよい。アプリケーションは、鍵交換所のオペレータに関係付けられる認証情報を用いてサーバ１０８に認証されてもよい。こうした認証情報は、鍵交換所の物理的な場所に関係付けられてもよい。鍵セットを保持又は取得するた

めのビン番号等の情報が、タブレット又は他の装置によって提供されてもよい。

【００８５】

図８は、鍵交換所に提供され得る例示の鍵保存キャビネット５００を示す。キャビネット５００は、この実施形態では、別個のドア５０４によって各々がアクセスされる複数のビン５０２を含む。ドア５０４の各々は、電気制御機構５０６により鍵を掛けて閉じられる。コントローラ５１０は、機構５０６に接続されて、それ故に、ドア５０４に鍵が掛かったままに維持し、又はユーザが対応するビン５０２の中に鍵セットを置く又はビン５０２から鍵セットを除去するために開けることができるようにドア５０４を開錠することができる。

【００８６】

コントローラ５１０は、インターネットによってサーバ（図１に示されるサーバ１０８等）と通信することを可能にする有線又は無線のネットワークインターフェースを有する。例として、コントローラ５１０は、ＷｉＦｉインターフェース又はセルラデータインターフェース等の無線ネットワークインターフェースを含んでもよい。鍵保存キャビネット５００は、コントローラ５１０に電力を供給するための電力供給５１２を含む。一部の実施形態では、電力供給は、電気の幹線等の外部ソースに接続する。他の実施形態では、電力供給はバッテリ及び／又は太陽電池を含む。

【００８７】

鍵トークンをスキャンするスキャナ５１４が各ビン５０２に関係付けられる。スキャナ５１４は、コントローラ５１０とデータ通信を行う。一部の実施形態では、コントローラ５１０は、ゲストユーザが鍵セットの解放を要求することにより又は鍵管理者が鍵セットを引き渡すことにより、鍵交換サーバ１０８と通信するクライアント装置としてコントローラ５１０が使用されることを可能にするユーザインターフェース（図示せず）を含む。保存キャビネット５００は、ユーザに特定のビンを示すためのディスプレイ又は他のシステムを含んでもよい。例えば、ビン番号を表示するように構成されるＬＣＤディスプレイ、各ビン等に関係付けられるＬＥＤ又はＬＣＤである。

【００８８】

本記載を読むと理解されるように、本明細書に記載の鍵交換システム及び方法は、物件所有者又は物件管理者（又は物件の占有者）に多くの利益を提供する。例えば、システム及び方法は、鍵付きの箱を設置し、物件の外に鍵を隠し、又は個人に会うために物理的に現場に居る必要なく、物件の鍵へのアクセスを１人以上の個人に提供するために、物件所有者又は物件管理者（不動産管理会社等）に利便性を提供する。物件所有者又は物件管理者は、鍵交換サーバと通信するスマートフォン等のクライアント装置を介して、各人が鍵へのアクセスを有することができる時間を制限することにより、多くの連続する訪問者に対するアクセス権を制御することができる。これは、物件所有者又は物件管理者が、ゲストに物件を貸し出し又は所定の訪問者（例えば、建築請負人、掃除人、不動産仲介業者、鑑定士等）に一時的なアクセスを与える必要がある場合に便利であってもよい。更に、本明細書に記載のシステム及び方法を用いて、物件所有者又は物件管理者は、同じ物件に対して複数の鍵セットへのアクセス権を与えることができる。例えば、物件所有者又は物件管理者は、物件を借りている現在のゲストに１つの鍵セットを利用可能にし、及び物件の掃除人に別の鍵セットを利用可能にしてもよい。

【００８９】

また、本明細書に記載の鍵交換システム及び方法は、物件へのゲスト又は訪問者に多くの利益を提供する。例えば、こうした鍵交換システム及び方法を用いると、物件を借りているゲストが、ホストの利用可能性と自身の到着時間を調整する必要がない。ゲストは、承認されたアクセス期間及び鍵交換センターの営業時間内でいつでも物件の鍵を取得することができる。また、鍵交換システム及び方法は、訪問を終了した後でゲストが鍵を返却するための利便性を提供する。

【００９０】

また、（鍵交換センターのホスティング、管理又は営業のビジネスサービスと引き換え

に鍵交換ネットワークのオペレータ／所有者によりビジネスに提供され得る潜在的直接的な補償に加えて）鍵交換センター（例えば、喫茶店等）の役目をするビジネスが、鍵セットの引き取り又は引き渡しのために到着するユーザによってもたらされるビジネスへの増加した交通量から利益を得てもよい。

【００９１】

鍵交換センターのネットワークにおけるビジネスで購入を行う度に、ユーザがクライアント装置に対する識別及び購入の検証に応じて鍵交換システムにおいて価値又はクレジットを蓄積し得るロイヤルティプログラムをシステムがサポートするように構成される実施形態により、このような歩行者交通の価値が高められ得る。このようなロイヤルティプログラムは、鍵交換プログラムのユーザが鍵交換センターネットワークにおけるビジネスの顧客になることを奨励するであろう。

【００９２】

本明細書に記載のシステムは、容易に拡張可能である。例えば、単一の鍵アクセスサーバ（例えば、１０８）が、多数の鍵アクセス場所を供給してもよい。こうした鍵アクセス場所の一部は、異なってブランド化され、又は公衆に異なって提示されてもよい。一部の実施形態では、異なるクライアントソフトウェア（例えば、鍵セットに対するアクセス規則を管理するためにユーザによって使用されるソフトウェア、又は鍵交換所で使用されるクライアントソフトウェア）は、異なるユーザに対して異なっていてもよい。このような実施形態では、サーバシステム１０８は、異なってブランド化される鍵交換所の範囲で鍵セットを管理してもよい。一部の実施形態では、１つ以上の鍵アクセスサーバ１０８が、多くの鍵キャビネット１２０又は複数の鍵アクセス場所にわたってネットワークに入れられる自動化された鍵交換キオスクにサービス提供するネットワークの一部であってもよい。鍵交換サーバシステムは、鍵アクセスサーバシステム１０８により提供される機能にアクセスするためにプログラマが自身のアプリケーションを書くことを許容するＡＰＩ（ａｐｐｌｉｃａｔｉｏｎ　ｐｒｏｇｒａｍｍｉｎｇ　ｉｎｔｅｒｆａｃｅ）を有してもよい。このようなアプリケーションは、例えば、鍵キャビネット１２０又は自動化された鍵交換キオスクが鍵アクセスサーバ１０８をインターフェース接続することを可能にし、且つクライアント装置が特定の鍵交換機能を実行することを可能にするためのカスタム化インターフェースを提供するアプリケーション、及び鍵アクセス場所において鍵キャビネット１２０又は自動化された鍵交換キオスクの状態を監視するアプリケーションを含んでもよい。カスタムアプリケーション及びそれの更新は、鍵キャビネット又は自動化された鍵交換キオスクに遠隔でプッシュされてもよい。

【００９３】

非限定的な例示として、レンタカー会社が、このようなＡＰＩを利用して、レンタカー場において人間のスタッフが居るモデルから自動化鍵交換システムに移行したい場合があり、物件管理人又は予約会社が、このようなＡＰＩと統合して、地域ビジネスパートナーシップのネットワークを通じて配布される自身のブランド化鍵交換センターへのアクセスを顧客に提供したい場合があり、カーシェアリング会社が、このようなＡＰＩを利用して、車に新しい技術をインストールするのではなく車の鍵を利用するカーシェアリングオプションを提供したい場合があり、ロビー又はフロントデスク／コンシェルジュを有する建物が、このようなＡＰＩを利用して、居住者又はゲストのために自動化受付システムを実装してもよく、又は異なる時間に異なる個人に鍵を割り当てる他のビジネス（例えば、映画館又はトラック運送会社等）が、このようなＡＰＩを利用して、鍵ロジスティックを管理するために鍵管理システムを提供してもよい。

【００９４】

一部の実施形態では、個々のユーザが、自動的にアクセス規則をシステム生成させることを選択してもよい（又は、システムは自動的にアクセス規則を生成するように構成されてもよい）。例えば、システムは、ユーザからのサービス要求に応答してサービスプロバイダが物件にアクセスすることを許可する規則をシステムに自動的に生成させることを人物が希望し得る予約機能を含んでもよい。例えば、鍵セットは、ユーザによって要求され

るクリーニング、買い物、配達、修理又は他のサービスを承認されたプロバイダに自動的に利用可能にしてもよい。別の例示として、レンタカー会社又はレンタルホーム会社等の物件予約会社は、自動的に又は予約が発生すると予約データに基づいて管理ユーザにより承認されるためにアクセス規則が生成されるシステムを構築してもよい。

【００９５】

個々のサービス要求に加えて、進行中のサービス要求が充足されてもよい。非限定的な例として、鍵交換サービスは、小包を仮想住所に配達させるオプションをユーザに提供してもよい。次に、このような小包は、小包が到着するとユーザの鍵へのアクセスを自動的に与えられる配達員によりユーザの家に配達されてもよい。承認は期間限定であってもよい。システムは、鍵セットが時宜に即して返却されない場合に自動警告を提供してもよい。

【００９６】

一部の実施形態では、鍵ビンにおける鍵セットは、鍵交換システムにおける鍵セットの在庫を更新するために鍵交換センターの職員により又は埋め込みセンサによりクライアント装置で周期的にスキャンされてもよい。各ビンは、スキャンにより鍵識別子又はビン識別子のいずれか又は両者が検出されるようにそのビンの識別子を示すスキャン可能識別子を有してもよい。このような周期的在庫スキャンは、鍵配置の干渉又は人為的エラーを制御し、セキュリティ違反を検出し、ユーザのアカウントに公開される更新場所データ又は鍵管理者の安心のための在庫確認を提供するであろう。

【００９７】

一部の実施形態では、システムは、異なる物件にアクセスするための予約をゲストユーザが行うことを可能にする予約サービスを提供してもよい。一部のユーザは、物件を予約したゲストユーザが予約期間の間に予約された物件に対する鍵セットにアクセスすることを許可する規則をシステムに自動的に生成させることを希望する場合がある。システムは、このような規則を自動的に生成するように構成されてもよい。

【００９８】

一部の実施形態では、システムは、物件予約を管理するためにカレンダ及び他のツールを含む。鍵管理者であるユーザは、アクセススケジュールを監視して単一のシステムに統合するためにこのような機能を使用してもよい（こうしたユーザがシステムの外部にあるようにゲストを調達する場合であったとしても）。

【００９９】

本明細書に記載のシステムは異なるビジネスモデルの範囲をサポートして適用され得ることが理解されるべきである。システムは、特定の特徴を供給してこうしたビジネスモデルをサポートしてもよい。例えば、一部の実施形態では、鍵セットを何らかの他の人物に渡すことを希望する所有者又は他の人がシステムのこのような使用の代金を支払ってもよい。このような実施形態では、システムは、交換される鍵セットを引き渡すことを所有者に許可する前に、所有者から支払い（例えば、クレジットカード払いの銀行振込み、デビットカード払い等）を受け取ってもよい。代替的に、システムは、鍵セットの交換が行われる前又は後に自動的に請求してもよい。このような支払い又は請求は、均一料金であってもよく、鍵交換の詳細（対象の受け取り人により引き取られる前にどのくらいの期間、鍵が保持されていたか等）に基づいてもよい。請求が鍵交換の詳細に基づく場合、システムはこのような詳細を自動的に監視してもよい。

【０１００】

一部の実施形態では、システムのユーザは、（例えば、加入料を払って）システムへのアクセスに対して代金を支払ってもよい。場合によっては、ユーザは、鍵管理者になる権利を与えられるために料金を支払ってもよい。料金は、例えば、所定期間の間の加入の形態であってもよい。システムは、ユーザに自動的に請求してもよく、最新の適切な料金を支払っていないユーザからの交換用の鍵セットの受け入れを拒否してもよい。

【０１０１】

本明細書に記載のシステムは、システムのユーザに広告又はクーポンを配達するように

選択的に構成されてもよい。例えば、システムは、鍵セットが関連する物件の地域的な（典型的には鍵交換所に対しても地域的である）ビジネスに関する広告及び／又はクーポンを全ての又は選択された受け取り人に配達してもよい。システムは、鍵交換所が位置する都市若しくは町において又は周辺地域において鍵交換の頃に発生するイベントに関してイベントチケットの申し出を伝達してもよい。

【０１０２】

本明細書に記載のシステムは、物件へのアクセスを予約し且つこのような物件アクセスに対する代金の支払いを人物に許可する予約システムを組み込み又はそれと関係付けられてもよい。システムは、鍵交換に対する料金を含んでもよい。

【０１０３】

一部の実施形態では、システムは、鍵交換センターを管理するビジネスによって提供され且つ鍵交換サービスの予約及び支払いシステムに組み込まれる付加価値サービスの提供及び／又は請求をサポートするように構成されてもよい。非限定的な例示として、鍵の解放前に鍵交換センターがゲストのＩＤを検査又はスキャンするために、到着時に（例えば、喫茶店である鍵交換センターで）ゲストが受け取る飲食料品の事前購入のために、又はビジネスの場所の外側の鍵付きの箱への指定された鍵の配置により営業時間後の鍵引き取りを処理するためのオプションが鍵管理者に提供され得る。更に、ユーザ満足度、鍵在庫スキャンの頻度、平均鍵引き取り回数、付加価値サービスに費やされる顧客の量、及び同類等のサービスレベル及びアクティビティを追跡するためのツールが導入され得る。

【０１０４】

一部の実施形態では、鍵識別子は、鍵交換センターを管理するビジネス又はバウチャーを認めるネットワークに追加される他のビジネスに使用するために鍵管理者により購入されるバウチャーに関係付けられ得る。バウチャーは、旅行体験を高めるために、旅行者等のゲストが使用するために鍵管理者により購入されてもよい。例えば、鍵管理者は、地域の喫茶店に対する所定の金額又は数の飲食料品、地域のアトラクションへのチケット、又は同類を購入して、滞在中に利用するためにそれらを特定の鍵セット及び／又はゲストと関係付けてもよい。クライアント装置が鍵トークンをスキャンして、鍵交換サーバが鍵識別子を受信し、バウチャーを検査し、その場所で所定のバウチャーが引き換え可能であることをクライアント装置に送信すると、このようなバウチャーは引き換えられてもよい。

【０１０５】

異なる実施形態では、支払いは、様々なイベントにより引き起こされる様々な形態で行われてもよい。鍵管理者は鍵交換システムの使用の度に代金を支払ってもよく、この場合、それらは鍵セットの引き取り及び／又は引き渡しごとに請求される。このような請求は、鍵交換インフラストラクチャの時間ベースの利用と請求を合わせるために「夜間料金」を含んでもよい。代替的に、繰り返しの加入料が、パッケージ使用に対して支払われ得る。支払いは、予約、付加価値サービス又はバウチャー購入、サービス要求、物件のゲスト予約、鍵の引き渡し又は引き取り等のシステムにおける異なるイベントにリンクされ得る。

【０１０６】

一部の実施形態では、システムは、鍵管理者が、物理的な鍵以外のアクセス技術に依存する鍵交換システムを介して他の物件を共同管理すること、又は鍵交換システムにおける物件を鍵からデジタル錠技術へと移行させることを可能にするように構成される。このような場合、鍵交換システムは、ａ）物理的な鍵を交換することに依存するシステムをシームレスに代替し得る統合デジタル錠をシステムに提供すること、ｂ）（例えば、ＡＰＩを介して）他のデジタル錠プロバイダと予約システムを統合すること、又はｃ）統合点を提供しない又は提供を拒否するデジタル錠プロバイダの場合、（例えば、低コストのモバイル装置の形式で）鍵管理者が鍵交換センターにおいてデジタル錠へのアクセス権を有するデジタル鍵を保存することを可能にすることにより、このような物件の追加及び移行をサポートしてもよい。クロスプラットフォームで技術に依存しない実施形態は、安全且つ制御された方式で多様な物件へのアクセスをゲストユーザ及び承認されたサービスプロバイ

ダに提供することができる。

【０１０７】

上記は、様々なビジネス機能をサポートする目的で本明細書に記載されたシステムに組み込まれ得る特徴の単なる非限定的な例示に過ぎない。

【０１０８】

コンポーネント（例えば、サーバ、クライアント装置、データベース、ソフトウェアモジュール、プロセッサ、プログラムメモリ、鍵、鍵チェイン、鍵キャビネット、ビン等）が上記で参照される場合、別段の明示がなければ、そのコンポーネントへの参照（「手段」への参照を含む）は、そのコンポーネントの均等物、例示の実施形態における機能を実行する開示の構造と構造的に同等ではないコンポーネントを含む、記載されたコンポーネントの機能を実行する（即ち、機能的に同等である）任意のコンポーネントを含むと解されるべきである。

【０１０９】

多くの例示的態様及び実施形態が先に検討されてきたが、当業者であれば、所定の修正、置換、追加及びサブコンビネーションを認識するであろう。例えば、

・本明細書に記載の実施形態では、鍵識別子は鍵又は鍵セットに取り付けられる鍵チェイン上に符号化される。他の実施形態では、鍵識別子は、鍵に取り付けられる何らかの他のオブジェクトに又は直接鍵自体に符号化されてもよい。

【０１１０】

・特定の実施形態では、一意のシリアル番号が、鍵交換ネットワークで使用される各鍵チェインに印刷され又は彫り込まれてもよい。シリアル番号は、鍵を識別するために使用できるように（鍵チェインをスキャンすることに代えて）、鍵の一意の鍵識別子にリンクされてもよい。例えば、ＮＦＣ使用可能装置が利用可能でない場合、又は鍵を識別するために鍵チェインの目視検査を実行するのがより好都合である場合に、シリアル番号が使用され得る。

【０１１１】

・図１の例示の実施形態では、鍵交換サーバ１０８は、ユーザ認証情報データベース１３１、管理ユーザデータベース１３２、鍵在庫データベース１３３、及びアクセス規則データベースを含む。このようなデータベースが図示のように鍵交換サーバ１０８にある必要はない。他の実施形態では、１つ以上のこうしたデータベースが、鍵交換サーバ１０８にアクセス可能な別のサーバ又は保存装置に提供されてもよい。

【０１１２】

従って、以下の添付の請求項の範囲及び以下に導入される請求項が、例示的に説明された実施形態によって限定されるべきではなく、全体として記載と整合するように最も広く解釈されるべきである。

【図１】

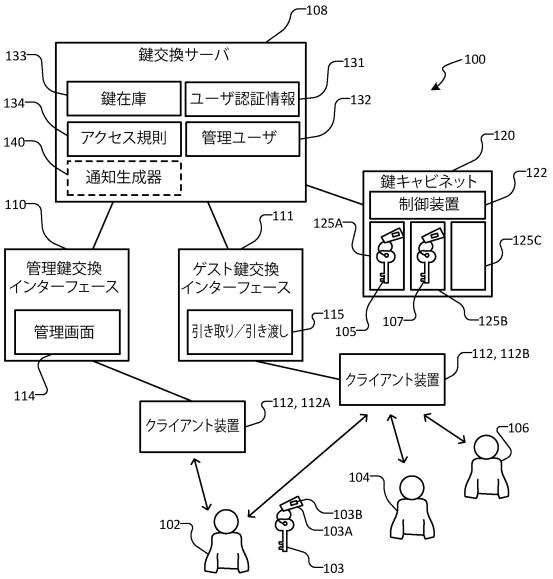

FIG. 1

【図２】

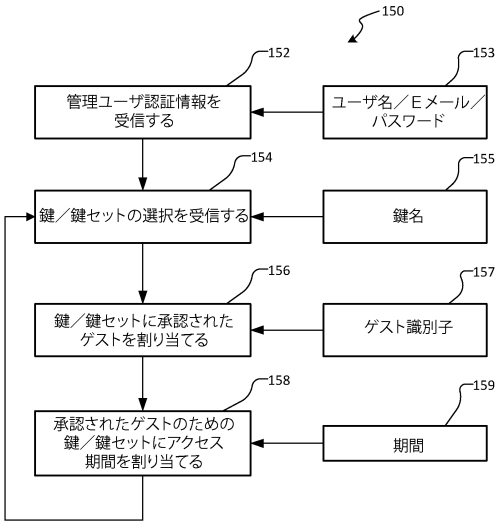

FIG. 2

【図３】

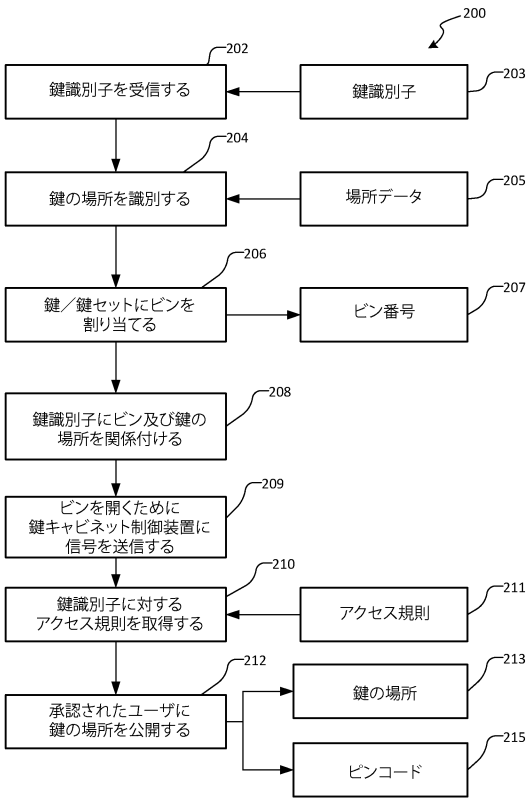

FIG. 3

【図４】

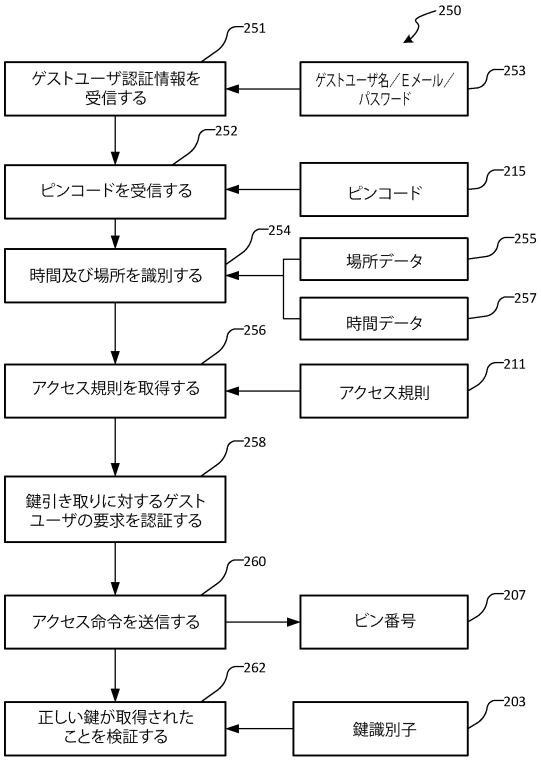

FIG. 4

【図５】

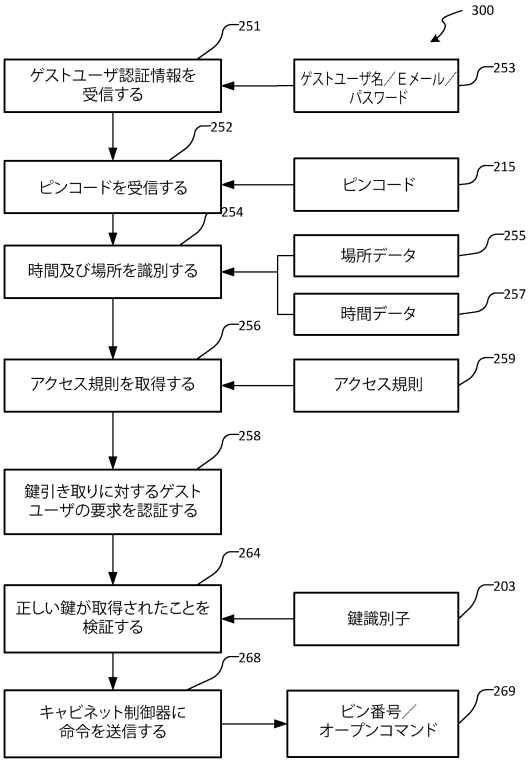

FIG. 5

【図６Ａ】

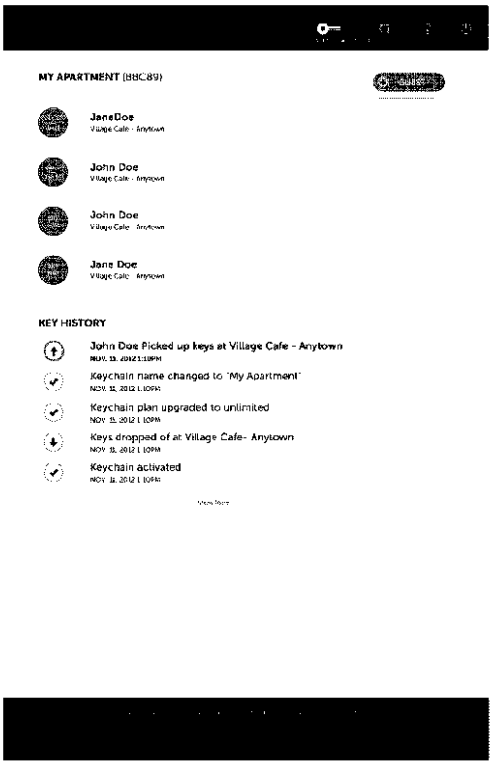

FIG. 6A

【図６Ｂ】

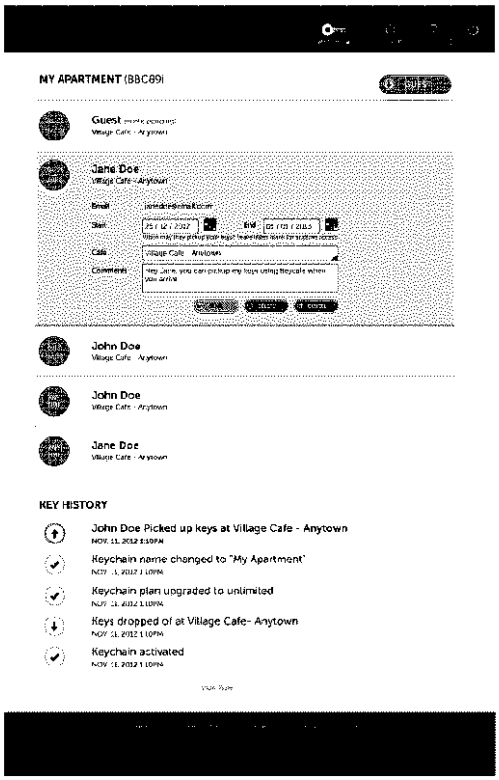

FIG. 6B

【図６Ｃ】

FIG. 6C

【図７Ａ】

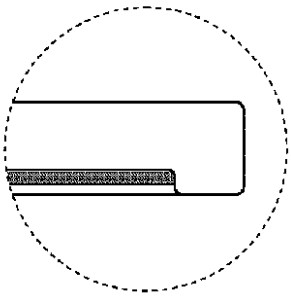

FIG. 7A

【図７Ｂ】

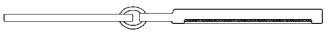

FIG. 7B

【図７Ｃ】

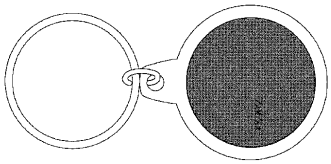

FIG. 7C

【図７Ｄ】

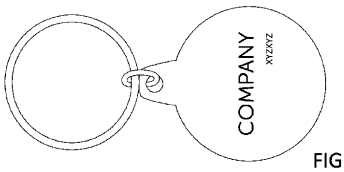

FIG. 7D

【図８】

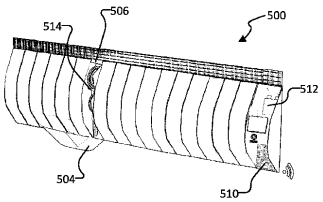

FIG. 8

【図９】

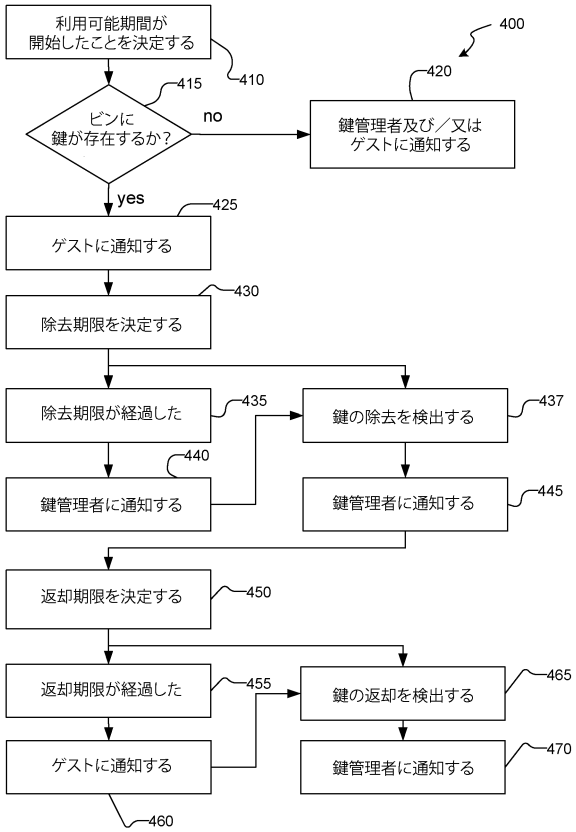

FIG. 9

フロントページの続き

(72)発明者　ブラウン、　クレイトン　カーター
カナダ国　Ｖ６Ｂ　１Ａ１　ブリティッシュコロンビア州　バンクーバー　ウォーター　ストリート　３０４－３３
(72)発明者　クラブ、　ジェイソン　ロバート
カナダ国　Ｖ５Ｗ　１Ｇ１　ブリティッシュコロンビア州　バンクーバー　３７ス　アベニュー　イースト　７８０

審査官　立澤　正樹

(56)参考文献　特開２００５－１８８１９９（ＪＰ，Ａ）
特開２００６－２５７６４３（ＪＰ，Ａ）
米国特許出願公開第２００５／０２４１００３（ＵＳ，Ａ１）
特開２０１０－０９５９１３（ＪＰ，Ａ）
特開２０１１－２４１５６６（ＪＰ，Ａ）
特開２００６－２１９９３４（ＪＰ，Ａ）
特開２００２－１７４０６１（ＪＰ，Ａ）
特開２００２－２４５３１３（ＪＰ，Ａ）
特開２００８－０５９３４９（ＪＰ，Ａ）
特開２００６－３３３４０３（ＪＰ，Ａ）
特開２００２－０１３３２３（ＪＰ，Ａ）
特開２０１０－２７５７７８（ＪＰ，Ａ）
特開２００４－０７６４３９（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｅ０５Ｂ　４９／００
Ｇ０６Ｑ　５０／１６