(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第6438113号
(P6438113)

(45)発行日　平成30年12月12日(2018.12.12)　(24)登録日　平成30年11月22日(2018.11.22)

(51)Int.Cl.		F I		
H04L 9/32	(2006.01)	H04L	9/00	675A
G09C 1/00	(2006.01)	G09C	1/00	640E
G06F 21/33	(2013.01)	G06F	21/33	

請求項の数 41　(全 46 頁)

(21)出願番号	特願2017-504163 (P2017-504163)
(86)(22)出願日	平成27年7月29日 (2015.7.29)
(65)公表番号	特表2017-524301 (P2017-524301A)
(43)公表日	平成29年8月24日 (2017.8.24)
(86)国際出願番号	PCT/US2015/042743
(87)国際公開番号	WO2016/019064
(87)国際公開日	平成28年2月4日 (2016.2.4)
審査請求日	平成30年7月26日 (2018.7.26)
(31)優先権主張番号	14/447,514
(32)優先日	平成26年7月30日 (2014.7.30)
(33)優先権主張国	米国(US)
(31)優先権主張番号	14/470,590
(32)優先日	平成26年8月27日 (2014.8.27)
(33)優先権主張国	米国(US)

早期審査対象出願

(73)特許権者　511224896
マスター　ロック　カンパニー　エルエルシー
アメリカ合衆国．５３１５４　ウィスコンシン，オーク　クリーク，ダヴリュ．フォレスト　ヒル　アヴェニュー　１３７
(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

最終頁に続く

(54)【発明の名称】認証のための無線鍵管理

(57)【特許請求の範囲】

【請求項１】

ロック装置をスリープ機能から覚醒させるステップと、

前記ロック装置により、前記ロック装置を前記スリープ機能から覚醒させることに応じて、前記ロック装置に対応する一意の識別子をブロードキャストするステップと、

移動装置において、前記一意の識別子を受信するステップと、

前記移動装置において、前記ロック装置に要求を送信するステップであって、前記ロック装置に前記要求を送信することは、前記一意の識別子がユーザプロファイルに関係付けられることを決定することに基づくステップと、

前記ロック装置により、前記移動装置にセキュリティチャレンジを送信するステップと、

前記移動装置により、前記チャレンジに対するレスポンス及び暗号化されたユーザプロファイルを前記ロック装置に送信するステップであって、前記レスポンスは前記移動装置及び前記ロック装置の両方に記憶されているアクセス鍵と共に生成されるデータを含み、前記ユーザプロファイルはサーバ及び前記ロック装置に記憶されている秘密鍵を使用して前記サーバにより暗号化されるステップと、

前記ロック装置により、前記チャレンジに対する前記レスポンスを検証するステップであって、前記レスポンスは前記アクセス鍵を使用して検証されるステップと、

前記ロック装置により前記レスポンスを検証することに応じて、前記移動装置からのデータの正当性を確認するステップであって、前記データの正当性を確認することは、

暗号化されたユーザプロファイルを復号することであって、前記ユーザプロファイルは前記秘密鍵を使用して復号されること、及び
復号されたユーザプロファイルを検証することを含むステップと、
前記ロック装置により、前記データの正当性を確認することに応じて、前記要求により特定される前記ロック装置のアクションを開始するステップであって、前記アクションは前記ロック装置をアンロックするために前記ロック装置の物理ロックコンポーネントをアクティブ化することを含むステップと
を含む、認証の方法。
【請求項２】
復号されたユーザプロファイルを検証するステップは、前記秘密鍵及び前記ユーザプロファイルに基づいてメッセージ認証コード（ＭＡＣ）の正当性を確認することを含む、請求項１に記載の方法。
【請求項３】
前記移動装置により、前記移動装置のタイムスタンプを送信するステップを更に含み、前記移動装置からの前記データの正当性を確認するステップは、前記ロック装置により維持される時間と前記タイムスタンプとを比較することによって、前記タイムスタンプを検証することを更に含む、請求項１に記載の方法。
【請求項４】
復号されたユーザプロファイルを検証するステップは、前記ロック装置により維持される時間を使用して、前記ユーザプロファイルのアクセススケジュールを比較することを更に含み、前記アクセススケジュールは前記移動装置が前記ロック装置にアクセスできる時間を特定する、請求項３に記載の方法。
【請求項５】
前記ロック装置により、前記タイムスタンプを前記ロック装置により維持される時間と比較することによって、前記移動装置が信頼できる装置であるかどうかを決定するステップを更に含む、請求項３に記載の方法。
【請求項６】
前記チャレンジは、前記移動装置と前記ロック装置との間の通信セッションに対応する一意のセッション識別子を含む、請求項１に記載の方法。
【請求項７】
前記ユーザプロファイルはＣＣＭモード暗号化アルゴリズムに基づいて前記サーバにより暗号化され、前記秘密鍵は１２８ビットの長さを有する、請求項１に記載の方法。
【請求項８】
前記一意の識別子が前記ユーザプロファイルに関係付けられていることを決定することは、
前記一意の識別子を前記移動装置におけるユーザプロファイルのリストと比較することであって、前記ユーザプロファイルのリストは前記ユーザプロファイルを含み、且つ前記リストの中のユーザプロファイルの各々が少なくとも１つロック装置に関係付けられていること、及び
前記一意の識別子が前記ユーザプロファイルの識別子情報と一致することを決定すること
を含む、請求項１に記載の方法。
【請求項９】
前記移動装置は、ユーザプロファイル生成処理の間に前記サーバから前記暗号化されたユーザプロファイル及びアクセス鍵を受信する、請求項１に記載の方法。
【請求項１０】
前記ロック装置及び移動装置の各々は、ブルートゥースプロトコル、近距離無線通信プロトコル、ＺｉｇＢｅｅプロトコル、及び無線自動識別（ＲＦＩＤ）プロトコルの少なくとも１つを使用して無線でデータを送信するように構成される、請求項１に記載の方法。
【請求項１１】

無線トランシーバと、
メモリと、
電子的に制御可能なロック機構と、
プロセッサと
を備え、前記プロセッサは、
前記メモリに秘密鍵を記憶することであって、前記秘密鍵は電子ロック装置に関する第１のコードに関係付けられていること、
前記メモリにアクセス鍵を記憶することであって、前記アクセス鍵は前記電子ロック装置に関する第２のコードに関係付けられていること、
前記トランシーバを介して、移動装置から要求を受信すること、
前記電子ロック装置をスリープ機能から覚醒させること、
前記無線トランシーバを介して、前記スリープ機能から覚醒することに応じて、前記電子ロック装置に対応する一意の識別子をブロードキャストすること、
前記トランシーバを介して、前記移動装置にセキュリティチャレンジを送信すること、
前記アクセス鍵を使用して、前記チャレンジに対するレスポンスを検証することであって、前記レスポンスは前記移動装置から受信され、前記レスポンスは前記移動装置により記憶されている前記アクセス鍵のコピーと共に生成されるデータを含むこと、
前記レスポンスを検証することに応じて、前記移動装置からのデータの正当性を確認することであって、前記データの正当性を確認することは、
暗号化されたユーザプロファイルを復号することであって、前記ユーザプロファイルは前記秘密鍵を使用して復号され、前記ユーザプロファイルはサーバにより記憶されている前記秘密鍵のコピーと共に前記サーバにより暗号化されていること、及び
復号されたユーザプロファイルを検証することを含むこと、並びに
前記データの正当性を確認することに応じて、前記要求により特定される前記電子ロック装置のアクションを開始すること
を行うように構成される、電子ロック装置。
【請求項１２】
前記アクションを開始することは、前記ロック装置のセキュアデータ記憶装置へのアクセスを提供することを含む、請求項１１に記載の電子ロック装置。
【請求項１３】
前記ロック装置の前記セキュアデータ記憶装置へのアクセスを提供することは、
前記秘密鍵を使用して前記ロック装置により、前記セキュアデータ記憶装置のデータを復号し、且つ復号されたセキュアデータ記憶装置のデータを前記移動装置に送信すること、又は
前記秘密鍵を使用して前記ロック装置により、前記移動装置から受信した追加データを暗号化し、且つ暗号化された追加データを前記セキュアデータ記憶装置に記憶すること
を含む、請求項１２に記載の電子ロック装置。
【請求項１４】
前記アクションは、前記ロック装置の物理ロックコンポーネントをアクティブ化することを含む、請求項１１に記載の電子ロック装置。
【請求項１５】
復号されたユーザプロファイルを検証することは、前記秘密鍵及び前記ユーザプロファイルに基づいてメッセージ認証コード（ＭＡＣ）の正当性を確認することを含む、請求項１１に記載の電子ロック装置。
【請求項１６】
前記データの正当性を確認することは、前記移動装置のタイムスタンプと前記電子ロック装置により維持される時間を比較することによって、前記タイムスタンプを検証することを更に含む、請求項１１に記載の電子ロック装置。
【請求項１７】
復号されたユーザプロファイルを検証することは、前記ロック装置により維持される時

間を使用して、前記ユーザプロファイルのアクセススケジュールを比較することを更に含み、前記アクセススケジュールは前記移動装置が前記ロック装置にアクセスできる時間を特定する、請求項１６に記載の電子ロック装置。

【請求項１８】

前記無線トランシーバは、ブルートゥーストランシーバ、近距離無線通信トランシーバ、ＺｉｇＢｅｅトランシーバ、及び無線自動識別（ＲＦＩＤ）トランシーバの少なくとも１つを含む、請求項１１に記載の電子ロック装置。

【請求項１９】

前記第１のコード及び前記第２のコードは、前記電子ロック装置に対して一意である同じコードである、請求項１１に記載の電子ロック装置。

【請求項２０】

前記電子ロック装置に電力を供給するように構成されるバッテリを更に備える、請求項１１に記載の電子ロック装置。

【請求項２１】

前記電子ロック装置の位置に基づいて位置情報を提供するように構成されるＧＰＳ装置を更に備え、前記プロセッサは、前記トランシーバを介して、前記移動装置に前記位置情報を送信するように更に構成される、請求項１１に記載の電子ロック装置。

【請求項２２】

移動装置において、物理ロックコンポーネントと前記物理ロックコンポーネントのロック及びアンロックを制御するように構成される回路とを備えるロック装置からロック識別子を受信するステップであって、前記ロック識別子は前記ロック装置に関係付けられているステップと、

前記移動装置により、前記ロック識別子を前記移動装置における一組のロック識別子と比較することによって前記ロック識別子が前記移動装置におけるユーザプロファイルに関係付けられることを決定するステップであって、前記ユーザプロファイルはロック識別子に関係付けられ且つサーバ及び前記ロック装置により記憶されているロック鍵を使用して前記サーバにより認証及び暗号化され、前記ユーザプロファイルはユーザ鍵を含むステップと、

前記移動装置により、前記ロック識別子に関係付けられる前記ユーザプロファイルを前記ロック装置に送信するステップと、

前記ロック装置により、前記ユーザプロファイルを復号して、復号されたユーザプロファイルを生成するステップであって、前記ユーザプロファイルは前記ロック鍵を使用して復号され且つ検証されるステップと、

前記ロック装置により、前記移動装置にセキュリティコードを送信するステップと、

前記移動装置により、暗号化されたコマンドを生成するステップであって、前記暗号化されたコマンドは前記セキュリティコードを含み且つ前記ユーザプロファイルの前記ユーザ鍵を使用して暗号化されるステップと、

前記移動装置により、前記暗号化されたコマンドを前記ロック装置に送信するステップと、

前記ロック装置により、前記移動装置からの前記暗号化されたコマンドの正当性を確認するステップであって、前記暗号化されたコマンドの正当性を確認することは、

前記復号されたユーザプロファイルから取得した前記ユーザ鍵を使用して前記暗号化されたコマンドを復号して、復号されたコマンドを生成すること、

前記セキュリティコードが有効であるかどうかを決定すること、及び

前記ユーザ鍵を使用して前記復号されたコマンドを認証することを含むステップと、

前記ロック装置により、前記コマンドの正当性を確認することに応じて、前記コマンドにより特定される前記ロック装置のアクションを開始するステップと

を含む、方法。

【請求項２３】

前記ロック装置をスリープ機能から覚醒させるステップと、

前記ロック装置により、前記ロック識別子をブロードキャストするステップであって、前記ロック識別子は前記ロック装置を前記スリープ機能から覚醒させることに応じてブロードキャストされるステップと
を更に含む、請求項２２に記載の方法。
【請求項２４】
前記移動装置により、前記移動装置のタイムスタンプを送信するステップを更に含み、前記移動装置からの前記暗号化されたコマンドの正当性を確認するステップは、前記ロック装置により維持される時間と前記タイムスタンプを比較することによって前記タイムスタンプを検証することを更に含む、請求項２２に記載の方法。
【請求項２５】
前記ユーザプロファイルを検証するステップは、前記ロック装置により維持される時間を使用して、前記ユーザプロファイルのアクセススケジュールを比較することを更に含み、前記アクセススケジュールは前記移動装置が前記ロック装置にアクセスできる時間を特定する、請求項２４に記載の方法。
【請求項２６】
前記ロック装置により、前記タイムスタンプを前記ロック装置により維持される時間と比較することによって、前記移動装置が信頼できる装置であるかどうかを決定するステップを更に含む、請求項２４に記載の方法。
【請求項２７】
前記セキュリティコードはシーケンス番号である、請求項２２に記載の方法。
【請求項２８】
前記セキュリティコードは、前記セキュリティコードの最初の使用の後の既定の時間量、前記セキュリティコードに関与するコマンドの既定の数、前記セキュリティコードに関与するトランザクションの既定の数、又は前記セキュリティコードに関与する通信セッションの既定の数の少なくとも１つのに対して有効である、請求項２２に記載の方法。
【請求項２９】
前記暗号化されたコマンドの正当性を確認するステップは、前記コマンドがユーザプロファイルの許可によって可能とされるかどうかを決定するステップを更に含む、請求項２２に記載の方法。
【請求項３０】
前記コマンドの正当性を確認することに応じて開始される前記ロック装置のアクションは、前記ロック装置の前記物理ロックコンポーネントをアクティブ化することを含む、請求項２２に記載の方法。
【請求項３１】
前記ロック装置により、前記ロック装置の前記物理ロックコンポーネントをアクティブ化した後で、前記ロック識別子をブロードキャストするステップと、
前記移動装置により、前記ユーザプロファイルを前記ロック装置に送信するステップと、
前記ロック装置により、新しいセキュリティコードを前記移動装置に送信するステップと、
前記移動装置により、前記新しいセキュリティコードを含む暗号化されたコマンドを送信するステップと
を更に含む、請求項３０に記載の方法。
【請求項３２】
前記サーバにより、ユーザの信頼できる装置から１つ以上のユーザプロファイルの第１の組を含む前記ユーザの特定の移動装置の選択を受信するステップと、
前記サーバにより、前記特定の移動装置における前記ユーザの全てのユーザプロファイルを除去するステップと、
前記サーバにより、全てのユーザプロファイルの除去が成功したかどうかを前記ユーザに通知するステップと、

全てのユーザプロファイルの除去が失敗したことに応じて、前記サーバにより、除去が成功しなかった前記ユーザの前記特定の移動装置におけるユーザプロファイルごとに鍵交換コマンドを生成し且つこうしたロック識別子を含む全ての信頼できる装置に送信するステップであって、前記鍵交換コマンドは元のロック鍵を使用して暗号化された前記ロック装置に関係付けられる新しいロック鍵を含み、前記鍵交換コマンドの正当性を確認することに応じて開始される前記ロック装置の前記アクションは前記新しいロック鍵を復号し且つ前記ロック装置に記憶することを含むステップと、

前記サーバにより、前記新しいロック鍵を前記ロック装置に記憶することに成功したことを確認するステップと、

前記サーバにより、信頼できる装置に更新されたユーザプロファイルを送信するステップであって、前記更新されたユーザプロファイルは前記新しいロック鍵を使用して前記サーバにより認証され且つ暗号化され、且つ前記更新されたユーザプロファイルは新しいユーザ鍵を含むステップと

を更に含む、請求項２２に記載の方法。

【請求項３３】

前記サーバにより、ユーザの前記移動装置から取り消すためにゲストユーザの１つ以上の特定のユーザプロファイルの選択を受信するステップと、

前記サーバにより、前記ゲストユーザの移動装置から前記１つ以上の特定のユーザプロファイルを除去するステップと、

前記サーバにより、全ての特定のユーザプロファイルの除去が成功したかどうかを前記ユーザに通知するステップと、

全ての特定のユーザプロファイルの除去が失敗したことに応じて、前記サーバにより、除去が成功しなかった前記ゲストユーザの前記移動装置における特定のユーザプロファイルごとに鍵交換コマンドを生成し且つこうしたユーザプロファイルを含む全ての信頼できる装置に送信するステップであって、前記鍵交換コマンドは元のロック鍵を使用して暗号化された前記ロック装置に関係付けられる新しいロック鍵を含み、前記鍵交換コマンドの正当性を確認することに応じて開始される前記ロック装置の前記アクションは前記新しいロック鍵を復号し且つ前記ロック装置に記憶することを含むステップと、

前記サーバにより、前記新しいロック鍵を前記ロック装置に記憶することに成功したことを確認するステップと、

前記サーバにより、信頼できる装置に更新されたユーザプロファイルを送信するステップであって、前記更新されたユーザプロファイルは前記新しいロック鍵を使用して前記サーバにより認証され且つ暗号化され、且つ前記更新されたユーザプロファイルは新しいユーザ鍵を含むステップと

を更に含む、請求項２２に記載の方法。

【請求項３４】

無線トランシーバと、

メモリと、

電子的に制御可能なロック機構と、

プロセッサと

を備え、前記プロセッサは、

前記メモリにロック識別子及びロック鍵を記憶することであって、前記ロック識別子及び前記ロック鍵は電子ロック装置に関係付けられていること、

前記トランシーバを介して、前記ロック識別子をブロードキャストすること、

前記トランシーバを介して、移動装置から暗号化されたユーザプロファイルを受信すること、

前記暗号化されたユーザプロファイルを認証及び復号することであって、前記暗号化されたユーザプロファイルは前記ロック鍵を使用して認証及び復号され、前記ユーザプロファイルはサーバにより記憶されている前記ロック鍵のコピーと共に前記サーバにより暗号化され且つユーザ鍵を含むこと、

前記トランシーバを介して、前記移動装置にセキュリティコードを送信すること、
前記トランシーバを介して、前記移動装置から暗号化されたコマンドを受信すること、
前記暗号化されたコマンドの正当性を確認することであって、前記暗号化されたコマンドの正当性を確認することは、
前記復号されたユーザプロファイルからの前記ユーザ鍵を使用して前記暗号化されたコマンドを復号して、復号されたコマンドを生成すること、
前記セキュリティコードが有効であるかどうかを決定すること、及び
前記ユーザ鍵を使用して前記復号されたコマンドを認証することを含むこと、並びに
前記コマンドの正当性を確認することに応じて、前記コマンドにより特定される前記電子ロック装置のアクションを開始すること
を行うように構成される、電子ロック装置。
【請求項３５】
前記コマンドは、前記ロック装置の物理ロックコンポーネントをアクティブ化することを含む、請求項３４に記載の電子ロック装置。
【請求項３６】
データの正当性を確認することは、前記移動装置のタイムスタンプと前記電子ロック装置により維持される時間を比較することによって、前記タイムスタンプを検証することを更に含む、請求項３４に記載の電子ロック装置。
【請求項３７】
前記ユーザプロファイルを検証することは、前記電子ロック装置により維持される時間を使用して、前記ユーザプロファイルのアクセススケジュールを比較することを更に含み、前記アクセススケジュールは前記移動装置が前記電子ロック装置にアクセスできる時間を特定する、請求項３６に記載の電子ロック装置。
【請求項３８】
前記セキュリティコードはシーケンス番号である、請求項３４に記載の電子ロック装置。
【請求項３９】
前記セキュリティコードは、限定された時間フレーム又は限定された使用回数の少なくとも１つに対して有効である、請求項３４に記載の電子ロック装置。
【請求項４０】
前記プロセッサは、
前記電子ロック装置をスリープ機能から覚醒させること、
前記トランシーバを介して、前記スリープ機能から覚醒することに応じて、前記ロック識別子をブロードキャストすること
を行うように更に構成される、請求項３４に記載の電子ロック装置。
【請求項４１】
前記電子ロック装置の位置に基づいて位置情報を提供するように構成されるＧＰＳ装置を更に備え、前記プロセッサは、前記トランシーバを介して、前記移動装置に前記位置情報を送信するように更に構成される、請求項３４に記載の電子ロック装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本願は、認証のための無線鍵管理用の方法、システム及びコンピュータ可読媒体に関する。
（関連出願の相互参照）
本願は、２０１４年7月３０日に出願され、“Ｗｉｒｅｌｅｓｓ　Ｋｅｙ　Ｍａｎａｇｅｍｅｎｔ　ｆｏｒ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ”と題された米国特許出願第１４／４４７，５１４号、及び２０１４年8月２７日に出願され、“Ｗｉｒｅｌｅｓｓ　Ｋｅｙ　Ｍａｎａｇｅｍｅｎｔ　ｆｏｒ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ”と題された米国特許出願第１４／４７０，５９０号の利益及び優先権を主張する国際出願である。米国特許出

願第１４／４４７，５１４号及び第１４／４７０，５９０号の全体が参照によりここに組み込まれる。

【背景技術】

【０００２】

近年、電子ロックが商業的に利用可能になってきている。このような電子ロックは、無線接続（例えば、Ｗｉ－Ｆｉ等）を介してユーザ装置により制御することができる場合がある。しかしながら、このような電子ロックとインターフェース接続するために使用される通信はあまり安全ではないことが多く、そのため不正なユーザがロックを制御し得る危険が増加している。

【発明の概要】

【０００３】

認証のための無線鍵管理用の方法、システム及びコンピュータ可読媒体が開示される。一実施形態は、認証の方法に関する。方法は、移動装置により、製品への要求を送信するステップと、製品により、移動装置へのセキュリティチャレンジを送信するステップと、移動装置により、チャレンジに対するレスポンス及び暗号化ユーザプロファイルを製品に送信するステップであって、レスポンスは、移動装置及び製品の両方に記憶されるアクセス鍵と共に生成されるデータを含み、ユーザプロファイルは、サーバ及び製品に記憶される秘密鍵を使用してサーバにより暗号化されるステップと、製品により、チャレンジに対するレスポンスを検証するステップであって、レスポンスはアクセス鍵を使用して検証されるステップと、製品により、レスポンスを検証することに応じて、移動装置からのデータの正当性を確認するステップとを含む。データの正当性を確認するステップは、暗号化ユーザプロファイルを復号するステップであって、ユーザプロファイルは秘密鍵を使用して復号されるステップと、復号ユーザプロファイルを検証するステップとを含む。方法は、製品により、データの正当性を確認することに応じて、要求により特定される製品のアクションを開始するステップを更に含む。

【０００４】

一実施形態は、認証の方法に関する。方法は、移動装置により、ロック装置への要求を送信するステップと、ロック装置により、移動装置へのセキュリティチャレンジを送信するステップと、移動装置により、チャレンジに対するレスポンス及び暗号化ユーザプロファイルをロック装置に送信するステップであって、レスポンスは、移動装置及びロック装置の両方に記憶されるアクセス鍵と共に生成されるデータを含み、ユーザプロファイルは、サーバ及びロック装置に記憶される秘密鍵を使用してサーバにより暗号化されるステップと、ロック装置により、チャレンジに対するレスポンスを検証するステップであって、レスポンスはアクセス鍵を使用して検証されるステップと、ロック装置により、レスポンスを検証することに応じて、移動装置からのデータの正当性を確認するステップとを含む。データの正当性を確認するステップは、暗号化ユーザプロファイルを復号するステップであって、ユーザプロファイルは秘密鍵を使用して復号されるステップと、復号ユーザプロファイルを検証するステップとを含む。方法は、ロック装置により、データの正当性を確認することに応じて、要求により特定されるロック装置のアクションを開始するステップを更に含み、アクションはロック装置をアンロックするためにロック装置の物理ロックコンポーネントをアクティブ化することを含む。

【０００５】

別の実施形態は、電子ロック装置に関する。電子ロック装置は、電子ロック装置に電力を供給するように構成されるバッテリと、無線トランシーバと、メモリと、電子的に制御可能なロック機構と、プロセッサとを備える。プロセッサは、メモリに秘密鍵を記憶し、秘密鍵は電子ロック装置に関する第１のコードに関係付けられ、メモリにアクセス鍵を記憶し、アクセス鍵は電子ロック装置に関する第２のコードに関係付けられ、トランシーバを介して、移動装置から要求を受信し、トランシーバを介して、移動装置へのセキュリティチャレンジを送信し、アクセス鍵を使用して、チャレンジに対するレスポンスを検証し、レスポンスは移動装置から受信され、レスポンスは移動装置に記憶されるアクセス鍵の

コピーと共に生成されるデータを含み、レスポンスを検証することに応じて、移動装置からのデータの正当性を確認するように構成される。データの正当性を確認することは、暗号化ユーザプロファイルを復号することであって、ユーザプロファイルは秘密鍵を使用して復号され、ユーザプロファイルはサーバにより記憶されている秘密鍵のコピーと共にサーバにより暗号化されること、及び復号ユーザプロファイルを検証することを含む。プロセッサは、データの正当性を確認することに応じて、要求により特定される電子ロック装置のアクションを開始するように更に構成される。

【０００６】

別の実施形態は、システムに関する。システムは、製品に関する秘密鍵を取得し、秘密鍵は製品に関する一意のコードに関係付けられ、製品に関するアクセス鍵を取得し、アクセス鍵は製品に関する一意のコードに関係付けられ、秘密鍵を使用して、製品に関するユーザプロファイルを暗号化し、ユーザプロファイル及び一意のコードは移動装置により提供され、一意のコードはユーザプロファイルと製品を関係付け、秘密鍵及びアクセス鍵は一意のコードを使用して取得され、暗号化ユーザプロファイル及びアクセス鍵を移動装置に提供し、ユーザプロファイルは製品に関するアクセスデータを含むように構成される１つ以上のプロセッサを備える１つ以上のサーバを含む。

【０００７】

別の実施形態は、システムに関する。システムは、ロック装置に関する秘密鍵を取得し、秘密鍵はロック装置に関する一意のコードに関係付けられ、ロック装置に関するアクセス鍵を取得し、アクセス鍵はロック装置に関する一意のコードに関係付けられ、秘密鍵を使用して、ロック装置に関するユーザプロファイルを暗号化し、ユーザプロファイル及び一意のコードは移動装置により提供され、一意のコードはユーザプロファイルとロック装置を関係付け、秘密鍵及びアクセス鍵は一意のコードを使用して取得され、暗号化ユーザプロファイル及びアクセス鍵を移動装置に提供し、ユーザプロファイルはロック装置に関するアクセスデータを含むように構成される１つ以上のプロセッサを備える１つ以上のサーバを含む。

【０００８】

別の実施形態は、電子ロック装置に関する。ロック装置は、無線トランシーバ、メモリ、電子的に制御可能なロック機構、プロセッサ、及び前記電子ロック装置の位置を決定するように構成される位置決定回路を含む。プロセッサは、１つ以上の時間における電子ロック装置の位置を示す１つ以上の位置データアイテムを受信し、１つ以上の位置データアイテムをメモリに記憶し、無線トランシーバを介してメモリから移動装置に１つ以上の位置データアイテムを送信するように構成される。

【０００９】

別の実施形態は、１つ以上の位置データアイテムに対する要求をロック装置に送信し、且つロック装置からセキュリティチャレンジを受信するように構成される１つ以上のプロセッサを含む移動装置に関する。１つ以上のプロセッサは、チャレンジに対するレスポンス及び暗号化ユーザプロファイルをロック装置に送信するように更に構成される。レスポンスは、移動装置及びロック装置の両方に記憶されているアクセス鍵と共に生成されるデータを含み、ユーザプロファイルはサーバ及びロック装置に記憶されている秘密鍵を使用してサーバにより暗号化され、ロック装置はレスポンスを検証し且つデータの正当性を確認するように構成される。１つ以上のプロセッサは、ロック装置から１つ以上の位置データアイテムを取得し、１つ以上の位置データアイテムはロック装置の位置決定回路により生成されたものであり、各々が１つ以上の時間におけるロック装置の位置を示すように更に構成される。１つ以上のプロセッサは、１つ以上の位置データアイテムにより示される１つ以上の位置を示す地図インターフェースを生成するように更に構成される。

【００１０】

更に別の実施形態は、ロック装置の位置決定回路を使用して、１つ以上の時間におけるロック装置の位置を示す１つ以上の位置データアイテムを生成するステップを含む方法に関連する。方法は、移動装置により、１つ以上の位置データアイテムに対する要求をロッ

ク装置に送信するステップと、ロック装置により、セキュリティチャレンジを移動装置に送信するステップとを更に含む。方法は、移動装置により、チャレンジに対するレスポンス及び暗号化ユーザプロファイルをロック装置に送信するステップを更に含む。レスポンスは移動装置及びロック装置の両方に記憶されているアクセス鍵と共に生成されるデータを含み、ユーザプロファイルはサーバ及びロック装置に記憶されている秘密鍵を使用してサーバにより暗号化される。方法は、ロック装置により、チャレンジに対するレスポンスを検証するステップを更に含み、レスポンスはアクセス鍵を使用して検証される。方法は、ロック装置により、レスポンスを検証することに応じて、移動装置からのデータの正当性を確認するステップを更に含む。正当性を確認するステップは、暗号化ユーザプロファイルを復号するステップであって、ユーザプロファイルは秘密鍵を使用して復号されるステップと、復号ユーザプロファイルを検証するステップとを含む。方法は、データの正当性を確認することに応じて、ロック装置から移動装置に１つ以上の位置データアイテムを送信するステップを更に含む。

【００１１】

更に別の実施形態は、認証の方法に関する。方法は、移動装置において、ロック装置からロック識別子を受信するステップであって、ロック識別子はロック装置に関係付けられているステップと、移動装置により、ロック識別子を移動装置における一組のロック識別子と比較することによってロック識別子が移動装置におけるユーザプロファイルに関係付けられることを決定するステップであって、ユーザプロファイルはロック識別子に関係付けられ且つサーバ及びロック装置により記憶されているロック鍵を使用してサーバにより認証及び暗号化され、ユーザプロファイルはユーザ鍵を含むステップと、移動装置により、ロック識別子に関係付けられるユーザプロファイルをロック装置に送信するステップと、ロック装置により、ユーザプロファイルを復号して、復号されたユーザプロファイルを生成するステップであって、ユーザプロファイルはロック鍵を使用して復号され且つ検証されるステップと、ロック装置により、移動装置にセキュリティコードを送信するステップと、移動装置により、暗号化されたコマンドを生成するステップであって、暗号化されたコマンドはセキュリティコードを含み且つユーザプロファイルのユーザ鍵を使用して暗号化されるステップと、移動装置により、暗号化されたコマンドをロック装置に送信するステップと、ロック装置により、移動装置からの暗号化されたコマンドの正当性を確認するステップであって、暗号化されたコマンドの正当性を確認することは、復号されたユーザプロファイルから取得したユーザ鍵を使用して暗号化されたコマンドを復号すること、セキュリティコードが有効であるかどうかを決定すること、及びユーザ鍵を使用して復号されたコマンドを認証することを含むステップと、ロック装置により、コマンドの正当性を確認することに応じて、コマンドにより特定されるロック装置のアクションを開始するステップとを含む。

【００１２】

別の実施形態は、電子ロック装置に関する。装置は、無線トランシーバと、メモリと、電子的に制御可能なロック機構と、プロセッサとを備え、プロセッサは、メモリにロック識別子及びロック鍵を記憶し、ロック識別子及びロック鍵は電子ロック装置に関係付けられており、トランシーバを介して、ロック識別子をブロードキャストし、トランシーバを介して、移動装置から暗号化されたユーザプロファイルを受信し、暗号化されたユーザプロファイルを認証及び復号し、暗号化されたユーザプロファイルはロック鍵を使用して認証及び復号され、ユーザプロファイルはサーバにより記憶されているロック鍵のコピーと共にサーバにより暗号化され且つユーザ鍵を含み、トランシーバを介して、移動装置にセキュリティコードを送信し、トランシーバを介して、移動装置から暗号化されたコマンドを受信し、暗号化されたコマンドの正当性を確認し、暗号化されたコマンドの正当性を確認することは、復号されたユーザプロファイルからユーザ鍵を使用して暗号化されたコマンドを復号すること、セキュリティコードが有効であるかどうかを決定すること、及びユーザ鍵を使用して復号されたコマンドを認証することを含み、且つコマンドの正当性を確認することに応じて、コマンドにより特定される電子ロック装置のアクションを開始する

ように構成される。
【００１３】
別の実施形態はロック装置へのアクセスを共有することに関する。方法は、サーバにより、ユーザの移動装置から、ユーザの移動装置に記憶されている一組のロック識別子からゲストユーザの移動装置と共有するためにロック装置に関係付けられるロック識別子の選択を受信するステップと、サーバにより、ユーザの移動装置からゲストユーザプロファイル要求を受信するステップと、サーバにより、ゲストユーザプロファイル要求及びゲストユーザ鍵に基づいて認証され且つ暗号化されたゲストユーザプロファイルを生成するステップであって、認証され且つ暗号化されたゲストユーザプロファイルはロック装置に関係付けられるロック鍵を使用して暗号化され、認証され且つ暗号化されたゲストユーザプロファイルはゲストユーザ鍵を含むステップと、ゲストユーザの移動装置がゲストユーザプロファイルにアクセスできるとサーバが決定する場合、サーバにより、ユーザの移動装置から、ユーザの移動装置における一組のユーザからのゲストユーザの選択を受信するステップと、サーバにより、ゲストユーザの移動装置に認証され且つ暗号化されたゲストユーザプロファイル及びゲストユーザ鍵を送信するステップと、サーバにより、ゲストユーザの移動装置における一組のロック識別子にロック識別子を追加するステップと、ゲストユーザの移動装置がゲストユーザプロファイルにアクセスできないとサーバが決定する場合、サーバにより、リンク及びコードを含むメッセージを生成し且つゲストユーザの移動装置に送信するステップと、サーバにより、ゲストユーザの移動装置においてユーザプロファイルへのアクセスを許可するためにリンクが使用されたことを決定するステップと、サーバにより、ゲストユーザの移動装置においてコードが入力されたことを決定するステップと、サーバにより、ゲストユーザの移動装置に認証され且つ暗号化されたゲストユーザプロファイル及びゲストユーザ鍵を送信するステップと、サーバにより、ゲストユーザの移動装置における一組のロック識別子にロック識別子を追加するステップとを含む。
【００１４】
上記の概要は、単なる例示であって、如何なる限定も意図していない。例示の態様、実施形態、及び上記の特徴に加えて、以下の図面及び詳細な説明を参照して更なる態様、実施形態及び特徴が明らかになるであろう。
【図面の簡単な説明】
【００１５】
本開示の上記の及び他の特徴は、添付の図面と併せて、以下の説明及び添付の請求項からより完全に明らかになるであろう。こうした図面は本開示に従う複数の実装のみを描いているので、その範囲を制限すると見なされるべきではなく、本開示は、添付の図面の使用を介して更なる具体性及び詳細が記載されることが理解される。
【図１】一実施形態による、認証のための無線鍵管理のためのシステムのブロック図である。
【図１Ｂ】一実施形態による、例示的な電子ロック装置の図である。
【図２】一実施形態による、製品及びユーザ装置を構成するための処理のフロー図である。
【図３】一実施形態による、ユーザ装置により製品と相互作用するための処理のフロー図である。
【図４】一実施形態による、本明細書に開示の技術を実装するための装置のブロック図である。
【図５】一実施形態による、本明細書に開示の技術を実装するためのユーザ装置のブロック図である。
【図６】一実施形態による、本明細書に開示の技術を実装するためのサーバのブロック図である。
【図７】一実施形態による、本明細書に開示の技術を実装するための製品のブロック図である。
【図８】一実施形態による、製品に関する位置データを決定し、選択的に、（複数の）決

定された位置を示すマッピングインターフェースを生成するための処理のフロー図である。
【図９】一実施形態による、ユーザ装置により製品と相互作用するための処理のフロー図である。
【図１０】一実施形態による、特定のユーザ装置からユーザプロファイルを除去するための処理のフロー図である。
【図１１】一実施形態による、ゲストユーザの装置からゲストユーザプロファイルを除去するための処理のフロー図である。
【図１２】一実施形態による、ロックへのゲストユーザアクセスを許可するための処理のフロー図である。
【図１３】別の実施形態による、製品及びユーザ装置を構成するための処理のフロー図である。
【図１４】別の一実施形態による、本明細書に開示の技術を実装するための製品のブロック図である。
【図１５Ａ】一実施形態による、ユーザ装置により製品と相互作用するためのデータフロー処理のデータフロー図である。
【図１５Ｂ】一実施形態による、ユーザ装置により製品と相互作用するためのデータフロー処理のデータフロー図である。図１５は、可読性のために第１の部分図１５Ａと第２の部分図１５Ｂとに分けられている。
【００１６】
本明細書に記載の主題の１つ以上の実装の詳細は、添付の図面及び以下の記載の中で説明される。本主題の他の特徴、態様、及び利点が、記載、図面、及び請求項から明らかになるであろう。
【００１７】
様々な図面における同様の参照番号及び記号は同様の要素を示す。例示の実施形態を詳細に記載する詳細な説明に入る前に、本願は記載の中で説明される又は図面に示される詳細又は方法に限定されないことが理解されるべきである。また、用語は単に説明を目的としており、限定と見なされるべきではないことが理解されるべきである。
【発明を実施するための形態】
【００１８】
以下の詳細な説明では、その一部を形成する添付の図面が参照される。図面において、同様の記号は、文脈上それ以外を示す場合を除いて、典型的には同様の構成要素を識別する。詳細な説明、図面及び請求項に記載の例示的な実施形態は、限定することを意図していない。本明細書に提示された主題の精神又は範囲から逸脱することなく、他の実施形態が利用されてもよく、他の変更が行われてもよい。本明細書に概略的に記載され且つ図面に例示された本開示の態様は、広範な異なる構成で配置され、置換され、結合され、且つ設計され得る。これらの全ては明確に考慮され、本開示の一部とされる。
【００１９】
本明細書には認証のための無線鍵管理の技術が記載されている。本明細書の開示によれば、サーバを利用する認証スキーム及び少なくとも２つの鍵を使用する暗号化スキームを介してユーザ装置（例えば、携帯電話、ラップトップ、タブレット装置等）と製品（例えば、南京錠、ドアロック、金庫等の電子ロック装置）との間の無線通信に追加のセキュリティが提供される。ユーザ装置が製品の動作を制御又は管理するように構成される状況では、開示された認証及び暗号化システムの使用は、製品が有効に制御されていることを確実にするために望ましい。本開示の中で、実施形態は、携帯電話のユーザ装置及び電子ロック装置の製品を参照して検討される。しかしながら、本開示は、携帯電話及び電子ロック装置を使用する実装に限定されず、他のタイプのユーザ装置及び製品を利用する実施形態も本開示の範囲内である。
【００２０】
一部の例示の実施形態によれば、開示されたやり方は、２つの鍵を使用する暗号化に基

づいている。一方の鍵（例えば、秘密鍵）が製品（電子ロック装置）及びサーバ（管理システム）において既知であり／保存されている。他方の鍵（例えば、アクセス鍵）がロック及びユーザ装置（携帯電話）において既知であり／保存されている。秘密及びアクセス鍵は共にロック／製品に固有のものである。このようにして、秘密及びアクセス鍵は、単一のロック／製品に一意に関連する。秘密鍵は、ロック／製品へのユーザのアクセス権を決定するために使用され得るファイル（例えば、ユーザプロファイル）を暗号化するために使用されてもよい。例えば、このようなアクセス権は、ユーザがいつロック／製品にリモートでアクセスすることができるか又はユーザがいつ装置を他のやり方で制御（例えば、電子ロック装置をロック又はアンロック）できるかを定義してもよい。アクセス鍵は、ロック／製品との通信を開始するのにユーザ装置により使用可能であり、ユーザ装置とロック／製品との間のチャレンジ・レスポンス交換の一部として使用されてもよい。

【００２１】

また、本明細書で検討される鍵は、データが有効であり、対応する鍵の他の保有者から来たものであることを認証するために使用されてもよい。このようなデータの完全性及びソースの認証／真正性は、（例えば、秘密鍵又はアクセス鍵を使用して）送信されたデータのＭＡＣ（メッセージ認証コード）を計算することによって行われてもよい。従って、本明細書で更に検討されるように、サーバがユーザプロファイルを暗号化すると、暗号化されたプロファイルを受信する装置（例えば、ロック装置）は、ＭＡＣが正しいことを確認するために秘密鍵のコピーを使用してもよい。同様に、ロックがデータを送信しているとき、それは秘密鍵を使用して、サーバにより確認されるＭＡＣを計算してもよく（データがサーバに向けられている場合）、サーバは秘密鍵を使用してＭＡＣを確認してもよい。代替的に、本明細書で検討される任意の通信は暗号化されていなくてもよく（例えば、平文パケット等）、ＭＡＣは送信されたデータに対して計算され且つ送信されたデータと共に含まれてもよい。次に、ＭＡＣは、データが正当なソースから送信されていることを確認するためのセキュリティ手段として使用されてもよい。更に、ロック及び移動装置が通信しているとき、各々はアクセス鍵のコピーを使用してＭＡＣを計算してもよく、各装置はデータを検証し、且つアクセス鍵を使用してソースを認証してもよい。従って、ＭＡＣのこのような使用は、データが適切なソース（即ち、サーバ、移動装置、又はロック）から来ていること、及びデータが有効であることも確実にすることができる。

【００２２】

一部の例示の実施形態によれば、手段は、（例えば、製造段階の間に）２つの鍵をロックに記憶せずに、２つの鍵を使用してユーザ装置（例えば、携帯電話）と製品（例えば、ロック）との間の安全な通信を可能にし得る。一部のこのような実施形態では、一方の鍵（例えば、ロック鍵）が製品（電子ロック装置）及びサーバ（管理システム）において知られ／記録されており、他方の鍵（例えば、ユーザ鍵）がユーザ装置（携帯電話）において知られ／記録されているが、製品においては知られ／記録されていない。ロック鍵は先に検討された秘密鍵と類似又は同等であってもよく、ユーザ鍵は先に検討されたアクセス鍵と類似又は同等であってもよい。ロック鍵及びユーザ鍵は共にロック／製品に固有のものであってもよい。このように、ロック鍵及びユーザ鍵は、単一のロック／製品に一意に関連してもよい。ユーザ装置は、ロック識別子を受信し、それをユーザ装置上の１つ以上のユーザプロファイルに関係付けられるロック識別子のリストと比較してもよい。一致が見つかると、ユーザ装置は、関係付けられるユーザプロファイルを製品に送信してもよい。ユーザプロファイルはユーザ鍵を含む。製品は、プロファイルを復号し、セキュリティコードをユーザ装置に送信してもよい。ユーザ装置は、暗号化コマンドを生成し且つ送信してもよい。暗号化コマンドは、ユーザ鍵を使用して暗号化され、セキュリティコードを含む。製品は、ユーザ鍵及びセキュリティコードを使用して暗号化コマンドの正当性を確認し、コマンドの正当性が確認されると仮定すれば、コマンドにより特定されるアクション（例えば、物理ロックコンポーネントをアンロックすること）を開始してもよい。一部のこのような実施形態は、図９から１５Ｂに関して以下により詳細に検討される。

【００２３】

図１を参照すると、一実施形態による、認証のための無線鍵管理のためのシステム１００のブロック図が示されている。システム１００は、少なくとも１つユーザ装置１０２、サーバ１０４、及び製品１０６を含む。例示的な実施形態では、ユーザ装置１０２は、移動装置（例えば、携帯電話）であり、製品１０６は電子ロック装置である。一般に、ユーザ装置１０２は、製品１０６の動作を少なくとも部分的に管理するように構成される。例えば、携帯電話は、電子ロック装置の機能をアンロック、ロック、及び他のやり方で管理するために使用されてもよい。ユーザ装置１０２は、このような製品管理（例えば、プロセッサ１０２、メモリ１０２ｂ、タイマ１０２ｃ、トランシーバ１０２ｄ及び１０２ｅ、ユーザ入力装置１０２ｆ等）に必要なコンポーネントを含む。プロセッサ１０２は、任意の市販のプロセッサであってもよく、１つ以上のプロセッサを表してもよく、汎用プロセッサ又は特定用途向け集積回路として実装されてもよい。メモリ１０２ｂは、プロセッサ１０２のメモリ（例えば、キャッシュ）、ＲＡＭ、又は他の記憶装置（フラッシュメモリ、ハードディスク記憶装置等）を含んでもよい。タイマ１０２ｃは、ユーザ装置１０２に対する時間値を維持するように構成される。例えば、タイマ１０２ｃは、プロセッサ１０２のクロックであってもよく、又は装置１０２の任意の他の時間管理回路であってもよい。タイマ１０２ｃによって維持される時間値は、（例えば、製品１０６と時間を同期する際、ロギング用にイベントに関連するタイムスタンプを提供する際等）本明細書で更に検討される安全な通信に使用されてもよい。トランシーバ１０２ｄ及び１０２ｅは、異なるプロトコルの通信のために様々なタイプのトランシーバを含んでもよい。一実施形態では、トランシーバ１０２ｄは、セルラネットワークを介してサーバ１０４と通信するためのセルラコンポーネントを含む。一実施形態では、トランシーバ１０２ｄは、インターネット又は他のネットワークを介してサーバ１０４と通信するための有線又は無線（例えば、Ｗｉ－Ｆｉ）コンポーネントを含む。無線トランシーバ１０２ｄは、製品１０６と通信するように構成される。一実施形態では、無線トランシーバ１０２ｄは、製品１０６とのブルートゥース（登録商標）接続を確立するためのブルートゥースコンポーネントを含む。ユーザ装置１０２は、（例えば、プロセッサ１０２及びメモリ１０２ｂを介して）ユーザ装置上で実行するように構成される管理アプリケーションの使用を介して製品１０６を管理することができる。例えば、アプリが携帯電話に（即ち、ユーザ装置１０２のメモリ１０２ｂに）インストールされてもよく、アプリは無線接続を通じて（無線トランシーバ１０２ｄを介して）電子ロック装置（即ち、製品１０６）を構成及び制御するために使用されてもよい。ユーザが装置１０２、サーバ１０４、製品１０６及び装置で実行中の任意のアプリケーションと相互作用することを可能にするために、１つ以上のユーザ入力装置１０２ｆ（例えば、タッチスクリーン、ボタン、スピーカ、ディスプレイ、キーボード）がユーザ装置１０２に含まれてもよい。

【００２４】

製品１０６が電子ロック装置等のロック装置である実施形態では、典型的には電子ロック装置の論理を提供するためのプロセッサ１０６ａ及び高電流負荷（例えば、プロセッサにより制御可能な電動ロック機構１０６ｇ）を含む。高電流負荷は、以下で検討される１つ以上のロック機構１０６ｇ（例えば、シャックル、ピン、メモリ等）を含んでもよい。また、電子ロック装置は、プロセッサと並列に高電流負荷に電力を供給するためのバッテリ１０６ｄ及びコンデンサを含んでもよい。電子ロック装置は、ユーザが装置（例えば、キーパッド、タッチスクリーン、タッチセンサ領域、ダイヤル、組み合わせ錠インターフェース、ボタン、キーホール等）を管理するために、１つ以上の物理的及び／又はデジタルインターフェース１０６ｅを含んでもよい。電子南京錠の回路（例えば、プロセッサ１０６ａ）は、バッテリ１０６ｄが高電流負荷１０６ｇを駆動している間、（一部の実施形態ではバッテリではなく）コンデンサによりプロセッサに電力が供給されるように構成されてもよい。一実施形態では、回路は、本明細書で検討される安全な通信に使用可能な製品の時間値を維持するように構成されるタイマ１０６ｃも含む。一実施形態では、電子ロック装置は、電子ロック装置の位置を提供するために使用され得るＧＰＳ受信機等の位置決定回路１０６ｈを含む。様々な実装において、位置決定回路１０６ｈは、無線トランシ

ーバ１０６ｆの一部又はそれから離れていてもよい。一実施形態では、電子ロック装置は、電子組み合わせ又はキーパッド南京錠等の電子南京錠である。他の実施形態では、電子ロック装置は、限定されないが、電子ドアロック又はキーパッド装置（例えば、キーパッドデッドボルト）、電子金庫（例えば、小型文書金庫、電子鍵金庫等）、電子箱錠又は埋め込み錠又は他のタイプの戸棚錠、電子自動アクセサリロック（例えば、カプラロック、ヒッチピンロック、トレーラロック等）、及び／又はハンドル又は自動車用のドアロック、自転車、オートバイ、スクータ、ＡＴＶ及び／又はスノーモービル等の他の電動若しくは非電動車両用の車両ロック（例えば、ホイールロック又はイグニションロック）、収納チェスト、電子ロック付きケース（例えば、文書ケース又は小型貴重品用のケース）、電子ケーブルロック（例えば、コンピュータ装置を固定等するためのアラーム対応ケーブルロック）、安全目的でアクセスを保護するための（例えば、電気工事が行われている間に電気制御ボックスを保護するための）安全ロックアウト／タグアウト、電子ロック付きのロッカー、及び／又は電子手荷物ロックであってもよく、又はそれらを含んでもよい。一実施形態では、ロック装置は、（例えば、メモリ等に記憶されている）セキュアデータへのアクセスを提供し又はセキュアデータを記憶するように構成される。例えば、物理ロックコンポーネントを含むのではなく（又は物理ロックコンポーネントに加えて）、ロック機構１０６ｇは、セキュアメモリを含んでもよい（例えば、メモリ１０６ｂは暗号化ハードドライブ等を含んでもよい）。このようなロック装置は、本明細書で検討される認証技術に基づいて（例えば、無線トランシーバ１０６ｆを介して）通信を行ってもよい。例えば、認証時に、ロック装置は、記憶されている秘密鍵を使用して、メモリ１０６ｂに記憶されているセキュアコンテンツを復号してもよい。次に、復号されたコンテンツは（例えば、無線トランシーバ１０６ｆを介して）別の装置に提供されてもよい。一実施形態では、電子ロック装置は、（例えば、ユーザのタッチに基づいて、ユーザの動作に基づいて等）ユーザの存在を検出するように構成されるタッチ検出装置及び／又は近接検出装置を含む。

【００２５】

図１Ｂを参照すると、一実施形態による電子ロック装置１００ｂの例が示されている。電子ロック装置１００ｂは、典型的には、１つ以上のロック機構（例えば、ロック機構１０６ｇ）を含む。例えば、電子ロック装置は、シャックル１６０、インターフェース１６２を含んでもよい。一実施形態では、インターフェース１６２は、本明細書で更に検討されるように、ユーザのタッチに応じて、電子ロック装置１００ｂを覚醒させるように構成されるタッチセンサを含む。一実施形態では、インターフェース１６２は、本明細書で更に検討されるように、近接ユーザの検出に応じて、電子ロック装置１００ｂを覚醒させるように構成される近接センサを含む。一実施形態では、インターフェース１６２は、ユーザが（例えば、シャックル１６０を解除するため等）ロックにコードを入力することを可能にするように構成される機械式ダイヤルを含む。様々な処理及び機械コンポーネント１６４が、電子ロック装置１００ｂのケース１６６内に組み込まれてもよい。例えば、処理及び機械コンポーネント１６４は、図１の製品１０６を参照して検討される１つ以上のコンポーネント（例えば、プロセッサ１０６ａ、メモリ１０６ｂ、タイマ１０６ｃ、バッテリ１０６ｄ、無線トランシーバ１０６ｆ、ロック機構１０６ｇ等）を含んでもよい。

【００２６】

再び図１を参照すると、例示的な実施形態では、製品１０６は、１つ以上の無線技術（例えば、無線周波数、無線自動識別（ＲＦＩＤ）、Ｗｉ－Ｆｉ、ブルートゥース、ＺｉｇＢｅｅ（登録商標）、近距離無線通信（ＮＦＣ）等）による通信のための無線トランシーバ１０６ｆを含む。例えば、無線トランシーバ１０６ｆは、（例えば、無線トランシーバ１０２ｄを介して）ユーザ装置１０２とのブルートゥースに基づく接続を確立するように構成されるブルートゥーストランシーバであってもよい。従って、本明細書で検討される電子ロック装置は、無線トランシーバを介して、ロックへの組み合わせ式入力又はキーパッド入力以外の、別のユーザインターフェース装置（例えば、ユーザ装置１０２のユーザ入力装置１０２ｆ、サーバ１０４のネットワークインターフェース１０４ｅ等）を使用し

てロック又はアンロックされるように備えられてもよい。例えば、無線で電子ロック装置をロック／アンロック／制御するために無線通信が使用されてもよい（例えば装置をロック又はアンロックするために携帯電話上のアプリケーションが使用されてもよい）。また、一実施形態では、製品１０６の回路は、別の装置との物理的接続を確立するために使用可能な入力／出力ポート（例えば、ＵＳＢポート、ＣＯＭポート、ネットワークポート等）も含む。例えば、このような物理的接続は、製品１０６をプログラムするか又は製品１０６と通信するために製造業者により使用されてもよい。

【００２７】

サーバ１０４は、一般に、ユーザ装置１０２と通信して、認証鍵及び暗号化機能を提供するためのコンポーネント（例えば、プロセッサ１０４ａ、メモリ１０４、ネットワークインターフェース１０４ｅ等）を含む。サーバ１０４とユーザ装置１０２との間の通信は、直接的であってもよく、又は中間ネットワーク（例えば、インターネットネットワーク、セルラネットワーク等）を介してであってもよい。例えば、ネットワークインターフェース１０４ｅは、サーバ１０４が装置１０２のトランシーバ１０２ｄとの接続を確立することを可能にするように構成される物理ネットワークコンポーネント（例えば、ネットワークカード等）を含んでもよい。一実施形態では、ネットワークインターフェース１０４ｅからの通信はセルラインターフェースを介してルーティングされて、サーバ１０４がセルラネットワークを介して装置１０２と通信することを可能にする。一実施形態では、ネットワークインターフェース１０４ｅは、サーバ１０４が装置１０２とのインターネットに基づく通信を確立することを可能にする。サーバ１０４は、１つのサーバ（物理的又は仮想サーバ）であってもよく、又は複数のサーバを含んでもよい。サーバ１０４は、認証及び暗号化のために使用される鍵（例えば、秘密鍵、アクセス鍵等）を生成して保存するように構成される１つ以上のサービスを含んでもよい。一実施形態では、メモリ１０４の様々なモジュールは、サーバ１０４の異なる機能を提供する。例えば、デバイスインターフェースモジュール１０４ｃは、ユーザ装置１０２との通信を確立して管理するために使用されてもよい。セキュリティモジュール１０４ｄは、セキュリティ関連機能（例えば、鍵を生成し且つ保存すること、ユーザプロファイルを暗号化すること等）のために使用されてもよい。セキュリティモジュール１０４ｄの出力がデバイスインターフェースモジュール１０４ｃに提供されてもよく、その結果、デバイスインターフェースモジュールは装置１０２にセキュリティ関連データを伝達してもよい。一実施形態では、アクセス鍵及び暗号化ユーザプロファイルが、デバイスインターフェースモジュール１０４ｃの要求に応じてセキュリティモジュール１０４ｄにより提供されてもよい。アクセス鍵及び暗号化ユーザプロファイルを受信すると、デバイスインターフェースモジュール１０４ｃは、アクセス鍵及び暗号化ユーザプロファイルをユーザ装置１０２に（例えば、ネットワークインターフェース１０４ｅからセルラネットワークを介して）送信してもよい。このように、ユーザ装置１０２は、セキュリティモジュール１０４ｄに直接的にアクセスしない。一実施形態では、デバイスインターフェースモジュール１０４ｃ及びセキュリティモジュール１０４ｄは、２つの別個のサーバ１０４に設置される。

【００２８】

以下の検討には、電子ロック装置（即ち、製品１０６）及び移動装置（即ち、ユーザ装置１０２）を有する実施形態が記載されている。ロックが製造されるとき、又はその直後、２つの鍵（秘密鍵及びアクセス鍵）が生成されて、ロックと連携され得る。例えば、秘密鍵及びアクセス鍵は、それぞれがロックに関する一意のシリアルＩＤ又は他の識別番号に関連付けられてもよく、ロックのメモリに記憶されてもよい。一実施形態では、一方又は両方の鍵が一意の及び／又はランダム生成の鍵である。一実施形態では、（例えば、サーバ１０４により）製品を表す一意のコードが生成され、この一意のコードはロックを対応する鍵に結び付けるために使用され得る。例えば、このような一意のコードは、ユーザがロック及び移動装置を適切に構成できるように、ロックの製品包装に固定されてもよい。一実施形態では、別個の一意のコードがセキュリティ及びアクセス鍵の各々に提供され、一意のコードの各々が、製造業者により各セキュリティ又はアクセス鍵に関係付けられ

てもよい。一実施形態では、サーバ１０４は、秘密鍵及びアクセス鍵も生成する。例えば、サーバ１０４は、製造工程の間にアクセスされ得る鍵生成サービスを提供してもよい。鍵は任意の生成アルゴリズムに従って生成されてもよい。しかしながら、秘密鍵及びアクセス鍵は、一般的には、互いから導出されない。生成した後、秘密鍵のみがサーバ１０４及びロックに保存される。秘密鍵は移動装置に送信されない。しかしながら、アクセス鍵は、ロック及び移動装置の両方に提供されてもよい。

【００２９】

ユーザがロックを獲得すると、ユーザは、ロックをその鍵に結び付けるために使用される一意のコードを使用してロック及びユーザの移動装置の両方を構成してもよい。図２を参照すると、一実施形態による、製品及びユーザ装置を構成するための処理２００のフロー図が示されている。代替的な実施形態では、より少ない、追加の、及び／又は異なるステップが実行されてもよい。また、フロー図の使用は、行われるステップの順序に関して限定することを意図していない。

【００３０】

一意のコードが取得される（２０２）。例えば、ユーザは、一意のコードを取得するために包含された製品包装を参照してもよく、ユーザは他のやり方で（例えば、製造業者ウェブサイト、電話等を介して）一意のコードを取得するために製造業者に接触してもよい。次に、ロックをユーザと関係付けるために、一意のコードは管理サーバに提供される（２０４）。例えば、ユーザは移動装置で実行中のアプリケーションのユーザインターフェースに一意のコードを入力してもよく、次に移動装置は一意のコードをサーバに送信する。このような例示では、ユーザは、管理サーバにより提供され且つ移動装置上のブラウザアプリケーションを介してアクセスされるフロントエンドインターフェース内で一意のコードを入力してもよい。代替的に、ユーザは、移動装置を使用して、一意のコードを取得し且つ送信するためにロックの包装をスキャンしてもよい。例えば、一意のコードは、バーコード、ＱＲコード（登録商標）、光学コード等により符号化されてもよく、移動装置のカメラは一意のコードをスキャンして決定するために使用されてもよい。移動装置から一意のコードを受信することに応じて、サーバは秘密鍵及びアクセス鍵を（例えば、要求に応じて）取得し又は新たに生成することができ、次に秘密鍵及びアクセス鍵は一意のコードに関係付けられてもよい。

【００３１】

次に、サーバはユーザプロファイルを生成してもよく（２０６）、これは一意のコードに関係付けられてもよい。ユーザプロファイルがまだ存在していない場合、新しいプロファイルを生成するために、デフォルト値、又は移動装置を介してユーザにより提供された値が使用されてもよい。例えば、ユーザは、移動装置のアプリケーションにプロファイルデータを入力してもよく、移動装置は一意のコードと共にサーバにプロファイルデータを送信する。ユーザがプロファイルを既に作成している場合、サーバは、その代わりに移動装置を介してユーザにより提供される新しい値でユーザプロファイルを更新してもよい。

【００３２】

一般に、ユーザプロファイルは、上記の実施形態におけるロックである製品の動作に関連するデータを含む１つ以上のファイルを含んでもよい。例えば、ユーザプロファイルは、ロックがいつアクセス（アンロック、ロック等）され得るかのユーザスケジュールを含んでもよい。スケジュールは、対応する許可ごとに、例えば、曜日により、開始時間（時間、分等）及び終了時間（時間、分等）を含むロックアクセス許可を特定してもよい。例えば、スケジュールは、電子ロックが移動装置を介してアンロックされ得る時間間隔を特定してもよい。別の例示として、スケジュールは、典型的な相互作用が起こると予想される時間周期、及びこうした時間周期に基づいて決定され得る信頼レベルを特定してもよい。従って、予想される時間周期内に送信されるアンロック要求は、予想外の／非典型的な時間に送信される要求よりもロックによって信頼されてもよい。また、移動装置は、スケジュールを自動的に調節してもよい。例えば、移動装置は、ロックとのユーザの相互作用のログ／記録を取ってもよく、ユーザの予想されるアクションに基づいてスケジュールを

設定してもよい。一実施形態では、（例えば、製造業者等により）デフォルトユーザスケジュールが設定される。更に、典型的にはユーザスケジュールのリストは、ユーザが多くの構成オプションの１つから選択することを可能にするように提供されてもよい。このように、製造業者は、様々な推奨動作設定をユーザに提供してもよい。また、ユーザは、スケジュールをカスタマイズして、所望のスケジュールに調整してもよい。

【００３３】

ユーザプロファイルは、ロックのモデル／シリアル番号及びどのようなタイプのアクセスがそのユーザに利用可能であるかを更に特定してもよい。例えば、このようなアクセスは、とりわけ、ロックのソフトウェア／ハードウェアバージョン情報を読み取ること、ロックのソフトウェアを更新すること、ロックのシャックル状態を読み取ること、ロックすること、アンロックすること、解除すること、時間／クロックの値を読み取る／設定すること、バッテリレベルを読み取ること、イベント関連データ（例えば、フラグ、カウンタ等）を読み取る／消去すること、ロックのログを読み取ること、ロックのキーパッドコードを読み取る／設定する／リセットすること、ロック用の通信データ（例えば、送信状態、送信電力レベル、チャネル情報、アドレス情報等）を読み取ること、ロック用に記憶されたデフォルト値（例えば、デフォルト解除時間、デフォルトアンロック時間）を読み取る／設定することを含んでもよい。また、ユーザプロファイルは、プロファイル用の開始時間及び取り消し日／時間（即ち、プロファイルが有効であり始めるとき及びプロファイルが満了してもはや有効ではなくなるとき）を特定してもよい。ユーザプロファイルは、ロック用の最大解除／アンロック時間を提供してもよい。ユーザプロファイルは、対応する移動装置の信頼レベルの指示（例えば、移動装置により提供された時間値／タイムスタンプが信頼できるかどうか）を提供してもよい。ロックは、装置の信頼レベルに基づいて所定の機能を許可する又は無効にするように構成されてもよい。信頼レベルは、ユーザがアクセスを有する又は有さない独立許可として記憶されてもよい（例えば、信頼レベルは、ロック、移動装置又はサーバ等のソフトウェアにより管理／調節されてもよい）。例えば、高信頼装置のみがロックのファームウェアを更新する又は所定の設定を変更することが可能であってもよい。更に、ロックは、信頼レベル及び時間値を計算に入れるセキュリティアルゴリズムを有してもよい。例えば、装置がより頻繁にロックとの相互作用を成功させると、ロックは装置に対する信頼レベルを増加（又は調節）してもよい。しかしながら、時間値がロックの維持時間との同期外であり又は認証が失敗する場合、ロックは装置に対する信頼レベルを低下（又は調節）してもよい。移動装置により提供される時間値はロックにより維持される時間値と比較されてもよく、２つの時間の間の近接度は装置に対する信頼レベルを示すために使用されてもよい（例えば、２つの時間が同期するのに近いほど、信頼レベルは高くなる等）。信頼レベルが所定の閾値を下回る場合、ロックは移動装置との相互作用を中断又は制限してもよい。また、信頼レベルは、先に検討されたスケジュールに基づいてもよい。例えば、移動装置は、装置がロックにアクセスしている時間、及びその時間がスケジュールにより定義された所定の時間周期内に入るかどうかに基づいてより信頼されている又はあまり信頼されていないと見なされてもよい。また、移動装置により提供される時間値は、ロックのクロックを移動装置のそれと同期するために使用されてもよく、又は認証された通信の間に他のやり方で使用されてもよい。検討された任意のプロファイルアイテムは、デフォルト値（例えば、製造業者のデフォルト）又はユーザ提供値を有してもよい。プロファイルは上記のデータに限定されず、追加データが含まれてもよい。また、プロファイルは、後で取得するためにサーバに記憶されてもよい。

【００３４】

ユーザ（例えば、ロックの所有者）に対してプロファイルを生成することに加えて、ユーザは、友人、家族、同僚等と共有される追加のゲストプロファイルを作成することを望む場合がある（２０８）。このように、ユーザは、ゲストプロファイルに基づいて、ロックへのアクセスを別の人物に許可してもよい。そうするために、ユーザは、（複数の）追加の人物用に（移動装置を使用して）所望のプロファイル値を入力してもよい。ユーザのプロファイルの作成と同様に、ゲストプロファイルデータは、サーバに送信されて、以下

で更に検討されるように処理されてもよい。ゲストプロファイルデータは、ユーザが自身のプロファイルを最初に生成するときと同時に又は別に（例えば、後の時間に）サーバに送信されてもよい。移動装置は、ユーザに提供されるプロファイルのタイプ（例えば、所有者とゲスト）を区別する情報を含む。

【００３５】

少なくとも１つのプロファイルが生成された後で、ユーザはロックの所有者として特定のロックに関係付けられる。一部の実施形態では、関係付けは、（例えば、ステップ２０４で）サーバに提供された一意のコードのみに基づいてもよい。一実施形態では、一意のコードを提供した後で、移動装置は、一意のコードを使用して、ロックの製造業者のサーバ又はデータベースからロックに関連する追加情報（例えば、シリアルＩＤ、モデル番号等）を自動的に取得してもよい。代替的な実施形態では、シリアルＩＤ、モデル番号又は他のコードは、ユーザにより（例えば、製品包装等を参照することにより）提供されてもよく、このような追加データは、ユーザをロックと関係付ける際に一意のコードと共に利用されてもよい。一部の実施形態では、ユーザをロックと関係付ける前にユーザの追加認証が要求されてもよく、このような認証は移動装置を介して提供されてもよい。

【００３６】

次に、管理サーバは取得したプロファイルデータを検証してもよい。取得したプロファイルデータを検証するために、管理サーバは、データの完全性を確実にするためにプロファイルに巡回冗長検査（ＣＲＣ）を行ってもよい。また、他のデータ検証方法が利用されてもよい。例えば、例示的な実施形態では、秘密鍵を使用して、メッセージ認証コード（ＭＡＣ）（例えば、鍵付きハッシングメッセージ認証コード（ＨＭＡＣ））が生成され且つデータ完全性の検証に使用されてもよい。本開示の範囲は所定のデータ完全性確認方法に限定されない。次に、サーバは、プロファイルデータを暗号化プロファイル（例えば、暗号文）に変換するために、秘密鍵を使用してプロファイルデータを暗号化することができる。プロファイルは、任意の既知の暗号化標準に従って暗号化されてもよい。例示的な実施形態では、プロファイルは、ＣＣＭモード（暗号ブロック連鎖ＭＡＣによるＮＩＳＴ／ＦＩＰＳカウンタモード暗号化）に基づくアルゴリズムを使用して暗号化され、暗号鍵として使用される秘密鍵は１２８ビット長を有する。従って、サーバはユーザプロファイルを暗号化し、また秘密鍵を使用してＭＡＣを生成してもよい。代替的に、異なる鍵で暗号化を行ってＭＡＣを生成する等、他の標準も使用され得る。

【００３７】

一実施形態では、本明細書で検討される管理サーバは、管理サーバのグループの中の１つである。このような実施形態では、第１の管理サーバが移動装置との通信を処理するように構成されてもよく、第２の管理サーバがセキュリティ機能（例えば、鍵の記憶、鍵の生成、暗号化／復号化処理等）を処理するように構成されてもよい。このように、第１のサーバは、移動装置から通信を受信してもよく、セキュリティ機能が要求されると第２のサーバと通信してもよい。例えば、第１のサーバは、第１のサーバが最初に受信したプロファイルデータを暗号化するために、第２のサーバが提供するサービスを要求してもよい。次に、第２のサーバは、暗号化データを暗号化して第１のサーバに提供し、それは次に暗号化データを移動装置に送信してもよい。他のサーバ構成も想定される。

【００３８】

暗号化した後、暗号化プロファイルは、サーバから移動装置に送信される（２１０）。また、サーバは、対応するアクセス鍵を移動装置に送信する（２１０）。例示的な実施形態では、アクセス鍵は、１２８ビット長を有する。アクセス鍵は、（例えば、ステップ２０２－２０４で検討されたように）一意のコードを使用してサーバにより決定され得る。次に、受信した暗号化プロファイル及びアクセス鍵は、ロックと移動装置の関係付けを完了するために、移動装置のメモリに記憶される。次に、ユーザは、自身の移動装置を使用してロックと相互作用してもよい（２１２）。

【００３９】

ゲストプロファイルが生成された状況において、一部の実施形態では、サーバは、ユー

ザプロファイルに対して行われる同様のセキュリティ手続きを行ってもよい。例えば、ゲストプロファイルは、秘密鍵を使用して記憶され且つ暗号化されてもよい。一部の実施形態では、ゲストプロファイルの場合、サーバは、暗号化ゲストプロファイルを暗号化して送信する前に、最初にゲストに通知を送信してもよい。例えば、サーバは、ユーザがゲストプロファイルを設定したときに、ユーザが提供した情報（例えば、Ｅメールアドレス、電話番号等）に基づいてゲストに通知Ｅメール又はテキスト／ＳＭＳメッセージ／警告を送信してもよい。次に、通知を受信すると、ゲストは、ユーザが作成した自身のプロファイルをアクティブ化してもよい。例えば、通知は、（例えば、Ｅメール又はメッセージ内に）クリックされるアクティベーションリンク又はゲストが提供することを要求されるコードを含んでもよい。また、ゲストは、本明細書で検討される管理アプリケーションをインストールし、アクティベーションコードを使用してゲストプロファイルをアクティブ化するためにアプリケーションを使用してもよい。管理アプリケーションをアクティブ化及びインストールすると、サーバは、暗号化ゲストプロファイル及びアクセス鍵を生成して、管理アプリケーションを介してゲストの移動装置に送信し得る。暗号化ゲストプロファイル及びアクセス鍵を受信した後で、各々はゲストの装置をロックと関係付けるためにゲストの移動装置に記憶されてもよい。次に、ゲストは、自身の移動装置を使用してロックと相互作用してもよい（２１２）。

【００４０】

プロファイルが構成された後で、ユーザ（又はゲスト）は、移動装置を介して無線でロックと相互作用してもよい。例えば、ユーザは、ロック、アンロック、又はロックの設定を調節等してもよい。一実施形態では、ロックは覚醒し／近接ユーザの存在を検出し、相互作用処理を開始してもよい。例えば、ロックは近接検出機能を含んでもよく、又はユーザは能動的にロック（例えば、ロックのタッチセンサの場所、物理的ボタン等）にタッチしてもよく、又はユーザの移動装置はロックを覚醒させるために共通チャネルで信号を送信してもよい。ロックは、覚醒されると、ユーザの移動装置と接続しようとし得る。例えば、ロックは、そのモデル及びシリアル番号情報（又は他の一意のロックＩＤ情報）をブロードキャストして、移動装置からの応答を待ってもよい。移動装置は、ロック情報を受信して、それを管理アプリケーションにより維持されるプロファイルと比較し得る。例えば、管理アプリケーションは、一度に複数の異なるロック用のプロファイルを維持し得る。一致が見つかると（例えば、プロファイルがその特定のタイプのロック用に見つかると）、認証手続きが開始されて一致したプロファイルを検証してもよい。プロファイルが検証され、ユーザがその特定の時間に（即ち、プロファイルのスケジュールデータに基づいて）アクセスを有し、且つユーザの時間／装置が信頼できる場合、ユーザは、ロックをアンロックして、ロックとの他の相互作用を行ってもよい。また、認証の後で、必要に応じて、ロックの時間及び移動装置の時間が同期されてもよい。

【００４１】

図３を参照すると、一実施形態による、ユーザ装置と製品との相互作用を行うための例示の処理のフロー図３００が示されている。代替的な実施形態では、より少ない、追加の、及び／又は異なるステップが実行されてもよい。また、フロー図の使用は、行われるステップの順序に関して限定することを意図していない。

【００４２】

一部の実施形態では、ロックは、低電力スタンバイ又はスリープ状態から覚醒されてもよい（３０２）。例えば、ロックはユーザにより接触されてもよく、又はユーザの近接が自動的に検出されてもよい。スタンバイ／スリープ状態は、ロックが完全に動作可能な覚醒状態にある場合よりも少ない電力（例えば、バッテリ電力）を使用し得る。一部の実施形態では、ロックは、常に完全機能状態にあってもよく、スタンバイ／スリープ状態から覚醒されなくてもよい。

【００４３】

ロックは、一意のＩＤ（例えば、そのモデル及び／又はシリアル番号から形成される識別子）をブロードキャストすることによって、そのタイプ情報をアドバタイズしてもよい

（３０４）。ロックと装置との間の通信は、任意のタイプの無線通信プロトコルを介して行われてもよい。一実施形態では、移動装置及びロックはブルートゥース接続を介して通信する。別の実施形態では、移動装置及びロックはＷｉ－Ｆｉ接続を介して通信する。別の実施形態では、移動装置及びロックはＺｉｇＢｅｅ接続を介して通信する。別の実施形態では、移動装置及びロックはＮＦＣ接続を介して通信する。更に、移動装置とロックとの間で伝達される任意のデータ（例えば、送信されるパケット）は、任意の既知のセキュリティプロトコル（例えば、ＷＥＰ、ＷＰＡ、ユーザ／製造業者パスワード等）に従って更に保護されてもよい。一実施形態では、移動装置とロックとの間で送信されるデータは、アクセス鍵を使用して暗号化される。この実施形態では、移動装置及びロックの両方は、それぞれが記憶されたアクセス鍵のコピーを有するので、データを暗号化及び復号することができる。受信したデータを復号すると、移動装置及びロックの両方は、例えば、復号データに対してＭＡＣ確認スキームを使用して、ＣＲＣ検査を実行すること等によって、復号データの完全性を更に確実にしてもよい。また、このようなＭＡＣ確認スキームは、データが適切なソース（即ち、ＭＡＣを生成するために使用される鍵の他の保有者等）から発信されたことを移動装置及びロックが検証することを可能にする。

【００４４】

ユーザ装置は、ロックの情報（例えば、ロックのＩＤ）を受信し且つ確認する（３０６）。一実施形態では、移動装置がロックに関係付けられているかどうか（例えば、ロックのＩＤに対応するプロファイルが存在するかどうか）を決定するために、ロックのＩＤは移動装置に記憶されているプロファイルのリストと比較される。一致するプロファイルが見つからない場合、ユーザは、ロックを秘密鍵に結び付ける一意のコードを使用して、（例えば、プロセッサ２００を介して）プロファイルを作成するように促されてもよい。ロックに関するプロファイルが見つかる場合、ユーザ装置は、ロックに要求（例えば、アンロック要求等）を送信してもよく、要求に従う前に認証手続きが開始され得る。

【００４５】

ロックは、チャレンジを生成して、チャレンジをユーザ装置に送信する（３０８）。一実施形態では、ロックは、チャレンジとしてロング乱数を生成する。別の実施形態では、ロックは、通信セッションによって異なるデータを生成する（例えば、各通信セッションごとにチャレンジとして一意の数（セッション識別子）が生成されてもよい）。一実施形態では、チャレンジは平文として移動装置に送信される。しかしながら、別の実施形態では、チャレンジはアクセス鍵を使用して暗号化されてもよい。移動装置は、（先に検討された構成の間にサーバから受信した）アクセス鍵及びセキュリティアルゴリズムを使用してチャレンジに対するレスポンス（例えば、ロングレスポンス）を計算する（３１０）。一実施形態では、移動装置は、アクセス鍵を使用して、レスポンス及びレスポンスと共に送信されるＭＡＣを生成する。一部の実施形態では、移動装置とロックとの間の通信は、逐次同定（例えば、パケット又はメッセージの逐次同定）に基づいて更に保護される。例えば、逐次同定によって、移動装置は、受信したパケットごとに特定の順番に従うフィールドを送信してもよい。次に、ロックは、既知の順番に対して受信したパケットを検証してもよい。このような既知の順番は、ロックにより事前決定され又は生成されてもよく、また通信中にロックにより移動装置に提供されてもよい。従って、このシーケンシングは、上記の１つ以上の他の方法と共に使用されてもよく（例えば、既定の初期シーケンスフィールド値と共にセッション識別子が使用されてもよい）、又はシーケンシングはそれ自身により使用されてもよい（例えば、ロックは、接続時にシーケンスフィールドの初期値を提供してもよい）。一実施形態では、接続時に、移動装置はロックから初期シーケンス番号を受信し、ロックは後で受信したメッセージが受信したメッセージごとに１つ増分された初期番号を含むことを検証する。ロックは、受信したメッセージがアクセス鍵を使用して暗号化され及び／又はそれから計算されるＭＡＣを含むことを更に検証してもよい。

【００４６】

次に、移動装置は、レスポンス及び（先に検討された秘密鍵を使用してサーバにより暗号化された）対応する暗号化プロファイルをロックに送信し得る（３１２）。一実施形態

では、移動装置は、移動装置のクロックに基づいて現在のタイムスタンプも送信する。ロックは、秘密鍵及びアクセス鍵の両方を記憶しているので、こうした鍵を使用して移動装置から受信したデータを認証してもよい。一実施形態では、ロックは、チャレンジに対するレスポンスが正しいことを検証し、且つＭＡＣを検証するためにアクセス鍵を使用する（３１４）。一実施形態では、ロックは、プロファイルを受け入れて復号しようとする前にレスポンスが検証されることを要求する。チャレンジ・レスポンス処理の遂行が成功すると、ロックは、受信したデータの正当性を確認することができる。ロックは秘密鍵を使用して暗号化プロファイルを復号することができ、ロックは、復号が成功したこと及びデータが実際に正しいソースから来たこと（例えば、暗号化プロファイルがサーバ等により生成されたこと）を確実にするために（例えば、秘密鍵又は他の確認スキームから生成されたＭＡＣを使用して、例えば、ＣＲＣ検査を行って）復号プロファイルデータのデータの正当性を確認してもよい。また、ロックは、（例えば、復号プロファイルに含まれるスケジュール情報を参照することによって）その検証された時間にプロファイルがアクセスを有することを確実にしてもよい。移動装置がタイムスタンプを送信した実施形態では、ロックは、タイムスタンプをロックの現在の時間と比較することによってタイムスタンプを検証してもよい。レスポンス及び復号プロファイルの各々が検証される場合、ロックは、移動装置の要求に従って、対応するアクションを開始してもよい（３１６）。先に検討されたタイムスタンプを利用する実施形態では、受信したタイムスタンプは、ロックにより維持される時間から閾値量の時間内であることが要求されてもよい。この例示では、ロックは、要求されるとそのシャックルをアンロックできる。

【００４７】

ロックが（そのメモリにセキュアデータを記憶するように）デジタルロック装置として構成される別の実施形態では、ロックは、ロックに記憶されているコンテンツを復号するために秘密鍵のコピーを使用してもよい。従って、このようなロック装置に対して所定のデータを取得又は記憶するように移動装置から要求が受信される場合、このようなデータの転送が要求に応じて開始されてもよい。例えば、移動装置がデータを記憶することを要求し、認証中に提供された対応する暗号化プロファイルがこのようなアクションを許可し、先に検討された認証が成功した場合、移動装置は、ロック装置へのデータの送信に進んでもよい（またロック装置はこのようなデータを受信してもよい）。次に、ロック装置は、受信したデータをそのメモリに記憶してもよい。受信したデータがまだ暗号化されていない場合、ロック装置は、秘密鍵を使用して記憶されるデータを暗号化してもよぃ。別の例示として、移動装置がデータを取得することを要求し、認証中に提供された対応する暗号化プロファイルがこのようなアクションを許可し、先に検討された認証が成功した場合、ロックは、要求されたデータを復号して移動装置に送信してもよい。代替的に、ロックは暗号化データを送信してもよく、次に移動装置は復号のために（同様に秘密鍵のコピーを記憶している）サーバと通信してもよい。また、任意の典型的なデータ相互作用（例えば、データの削除、ファイルのリネーム、データのコピー、データの整理等）がデジタルロック装置によりサポートされてもよく、これは対応するユーザプロファイルにおいて特定されるアクセスのタイプに基づいてもよい。

【００４８】

また、追加のセキュリティ関連機能が本明細書で検討されるサーバにより実装されてもよい。例えば、アクセス鍵又は秘密鍵が漏洩した場合、ユーザのサーバのオペレータは（モバイルアプリケーションを介して）保護措置を開始してもよい。例えば、ユーザは、新しい鍵のペアを生成するように要求してもよい。一実施形態では、サーバは、新しく生成された秘密鍵及び古いアクセス鍵から成る新しい鍵のペアを生成して、（先に検討されたプロファイルの暗号化と同様に）古い秘密鍵を使用して新しい鍵のペアを暗号化することができる。次に、サーバは、移動装置と通信して、鍵のペア交換要求をキューに入れてもよい。ユーザが複数の装置又はゲストプロファイルを有する場合、ユーザは、鍵のペア交換要求がキューに入れられている１つ以上の特定の装置を選択してもよい。移動装置によるロックとの次のアクセスの試行時に、先に検討されたチャレンジ・レスポンスシーケン

スが開始されてもよい。しかしながら、要求されたアクションは「鍵交換要求」であり得る。チャレンジ・レスポンス送信の一部として、移動装置は、暗号化された新しい鍵のペアを含んでもよい。例えば、移動装置は、レスポンスを送信してから、暗号化された新しい鍵のペアを送信してもよい。レスポンスの確認後、ロックは、古い秘密鍵を使用して暗号化された新しい鍵のペアを復号して、データを検証してもよい。成功すると、ロックは、復号された新しい鍵のペアから新しい秘密鍵にアクセスして、次に、将来の相互作用で使用されるように新しい秘密鍵を記憶してもよい。秘密鍵を更新することに加えて、秘密鍵を使用する同様のチャレンジ・レスポンス交換及び暗号化を介して他の機能が提供されてもよい。一実施形態では、「鍵交換要求」を送信する代わりに、移動装置は、秘密鍵で暗号化される新しいファームウェアバージョンと共に「ファームウェア更新要求」を送信してもよい。認証が成功すると、ロックは、新しいファームウェアの復号に進み、次に、そのファームウェアを新しいバージョンに更新してもよい。

【００４９】

また、本明細書で検討される任意の装置（例えば、ユーザ装置、製品、サーバ）が、その動作に関連するオーディット・トレールを生成するように構成されてもよい。例えば、ログは、ユーザ装置及び製品の相互作用を介して発生するイベントを詳述するように形成されてもよい。これは、とりわけ、サーバ対ユーザ装置イベント（例えば、暗号化プロファイルの送信、新しい鍵のペア要求の送信等）、ユーザ装置対製品イベント（例えば、アンロック要求の送信／応答、認証の成功及び失敗時のロギング等）、装置のみのイベント（例えば、アプリケーションエラーのロギング、電子ロック装置のシャックル状態のロギング等）を含んでもよい。本開示の範囲は、特定のログフォーマットに限定されない。

【００５０】

一実施形態では、ロックは、ＧＰＳ装置／受信機等の位置決定回路を更に備えてもよく、移動装置との相互作用の間に移動装置にその位置情報（例えば、ＧＰＳ座標）を送信してもよい。次に、位置情報は、最後に知られていたロックの場所として（例えば、ロック用に作成されたプロファイル内等に）移動装置により記憶されてもよい。また、移動装置の管理アプリケーションは、提供された位置情報に基づいて、ロックの最後に知られていた場所が地図上に表示され得るように地図機能を備えてもよい。代替的に、管理アプリケーションは、位置情報がサードパーティの地図アプリケーションにエクスポートされることを可能にしてもよい。こうした位置機能は、ユーザが自身の移動装置上で管理アプリケーションを開き、次に、最後に知られていた場所（例えば、ＧＰＳ座標）が提供されたときにロックがどこに位置しているかを示す地図を観ることを可能にしてもよい。更に、ナビゲーション指示又は他の機能が、ユーザをロックに案内するために提供されてもよい。代替的な実施形態では、移動装置は、ＧＰＳ装置を含んでもよい。このように、移動装置は、ロック及びサーバとの相互作用の間にその位置情報を記録してもよい。

【００５１】

本明細書で検討される任意の実施形態において、装置は、メモリ、処理及び通信ハードウェアを有する１つ以上のコンピュータ装置を含む処理サブシステムの一部を形成してもよい。装置（例えば、サーバ、ユーザ装置、製品）は単一の装置又は分散装置であってもよく、装置の機能はハードウェアにより及び／又は非一時的なコンピュータ可読記憶媒体におけるコンピュータ命令として行われてもよく、機能は様々なハードウェア又はコンピュータに基づくコンポーネントに分散されてもよい。図４を参照すると、本明細書で検討される任意の装置を表し得る装置４００が示されている。また、装置４００は、本明細書で検討される技術及び方法を実装するために使用されてもよい。例えば、装置４００は、ユーザ装置１０２の処理コンポーネント（例えば、携帯電話の処理コンポーネント）を含んでもよい。別の例示として、装置４００は、サーバ１０４の処理コンポーネントを含んでもよい。別の例示として、装置４００は、製品１０６の処理コンポーネント（例えば、電子ロック装置の処理コンポーネント）を含んでもよい。更に、装置４００は、本開示の技術を実装するために、本明細書で検討される計算（例えば、処理２００及び３００等に関連する計算）を行って、他の装置と通信し、データを暗号化及び復号し、データを認証

等するために必要な信号を生成するように構成されてもよい。

【００５２】

装置４００は、典型的には、メモリ４０４に結合される少なくとも１つのプロセッサ４０２を含む。プロセッサ４０２は、任意の市販のＣＰＵであってもよい。プロセッサ４０２は、１つ以上のプロセッサを表してもよく、汎用プロセッサ、特定用途向け集積回路（ＡＳＩＣ）、１つ以上のフィールド・プログラマブル・ゲート・アレイ（ＦＰＧＡ）、デジタル信号プロセッサ（ＤＳＰ）、一群の処理コンポーネント、又は他の適切な電子処理コンポーネントとして実装されてもよい。メモリ４０４は、装置４００の主記憶装置を含むランダム・アクセス・メモリ（ＲＡＭ）装置、及び任意の補助レベルのメモリ、例えば、キャッシュメモリ、不揮発性又はバックアップメモリ（例えば、プログラム可能又はフラッシュメモリ）、読み出し専用メモリ等を含んでもよい。更に、メモリ４０４は、別の場所に物理的に設置されるメモリ記憶装置、例えば、プロセッサ４０２内の任意のキャッシュメモリ及び、例えば、大容量記憶装置等に記憶される仮想メモリとして使用される任意の記憶容量を含んでもよい。また、装置４００は、トランシーバ４０６も含み、これは他の装置と通信するために必要な任意の追加のネットワークコンポーネント又は送信機（例えば、Ｗｉ－Ｆｉネットワークコンポーネント、ブルートゥースコンポーネント、ＺｉｇＢｅｅコンポーネント、ＮＦＣコンポーネント等）も含む。例えば、装置４００が電子ロックを含む実施形態では、トランシーバ４０６は、ユーザの移動装置と通信するように構成されるブルートゥーストランシーバであってもよい。別の例示として、装置４００がサーバを含む実施形態では、トランシーバ４０６は、移動装置と通信するためにサーバをネットワークに結合するように構成されるネットワークインターフェースであってもよい。別の例示として、装置４００が移動装置を含む実施形態では、トランシーバ４０６は、サーバと通信するように構成されるＷｉ－Ｆｉ又はセルラトランシーバを含み、トランシーバ４０６は、製品（例えば、電子ロック装置）と通信するように構成されるブルートゥースコンポーネントを更に含んでもよい。

【００５３】

一般に、実施形態を実装するために実行されるルーチンは、オペレーティングシステムの一部又は特定のアプリケーション、モジュール、又は一連の命令として実装されてもよい。所定の実施形態において、装置４００は、本明細書に記載の認証のための無線鍵管理に必要な各動作を機能的に実行するように構築される１つ以上のモジュールを含む。モジュールを含む本明細書の記載は、装置の態様の構造的独立性を強調しており、動作の１つの分類及び装置の責任を例示している。装置の動作の所定の実施形態のより詳細な記載は、図１－３を参照してこの節に記載されている。類似の動作全体を実行する他の分類も本願の範囲内であると理解される。モジュールは、典型的には、コンピュータの様々なメモリ及び記憶装置において様々な時間に設定された１つ以上の命令であって、コンピュータの１つ以上のプロセッサにより読み取られ且つ実行されると、開示された実施形態の要素を実行するのに必要な動作をコンピュータに行わせる１つ以上の命令を含む。更に、様々な実施形態が完全に機能するコンピュータ及びコンピュータシステムとの関連で記載されており、当業者であれば、様々な実施形態が様々な形態のプログラム製品として配布されることが可能であり、これは実際に配布させるために使用される特定のタイプのコンピュータ可読媒体に関わらず等しく適用されることを理解するであろう。

【００５４】

図５を参照すると、一実施形態による、本明細書に開示の技術を実装するためのユーザ装置５００のブロック図が示されている。例えば、ユーザ装置５００は、本明細書で検討される移動装置に対応してもよい。一実施形態では、ユーザ装置５００は携帯電話である。別の実施形態では、ユーザ装置５００はラップトップコンピュータである。別の実施形態では、ユーザ装置５００はタブレットコンピュータである。別の実施形態では、ユーザ装置５００はデスクトップコンピュータである。一般に、ユーザ装置５００は、処理回路５０２を含み、これはプロセッサ５０２ａ、メモリ５０２ｂ、及びタイマ５０２ｃを含んでもよい。プロセッサ５０２ａは、市販のプロセッサ又は本明細書で検討される任意のプ

ロセッサ（例えば、（複数の）プロセッサ４０２等）であってもよい。メモリ５０２ｂは、本明細書で検討される任意のメモリ及び／又は記憶装置コンポーネントを含む。例えば、メモリ５０２ｂは、ＲＡＭ及び／又はプロセッサ５０２ａのキャッシュを含んでもよい。また、メモリ５０２ｂは、ユーザ装置５００に対してローカル又はリモートの１つ以上の記憶装置（例えば、ハードドライブ、フラッシュドライブ、コンピュータ可読媒体等）を含んでもよい。

【００５５】

メモリ５０２ｂは、ユーザ装置に関して本明細書に開示の技術を実装するように構成される様々なソフトウェアモジュールを含む。例えば、メモリ５０２ｂは、メモリ５０２ｂの他のモジュールにより要求されるアクセス鍵を記憶し且つ提供するように構成されるアクセス鍵モジュール５０４を含む。アプリケーションモジュール５０６は、本明細書で検討される管理アプリケーションを提供するように構成される。例えば、ユーザ装置５００が携帯電話である実施形態では、アプリケーションモジュール５０６は、サーバ及び／又は製品とインターフェース接続するために使用され得る携帯電話アプリに対応するソフトウェアを含む。アプリケーションモジュール５０６は、サーバ及び製品との相互作用を含むプロファイル生成処理を管理するように構成されるプロファイルモジュール５０８を含んでもよい。例えば、ユーザは、アプリケーションモジュール５０６により提供されるアプリケーションによって（例えば、ユーザ入力装置５０２ｆを介して）ユーザ装置５００と相互作用してもよい。ユーザは、サーバに（例えば、トランシーバ５０２ｄを介して）送信される１つ以上の製品に対応する１つ以上のプロファイルを作成してもよい。サーバは、ユーザプロファイルを暗号化し、本明細書で検討されるユーザ装置５００に、暗号化ユーザプロファイル、アクセス鍵、ＭＡＣ等をプロファイリングしてもよい。また、アプリケーションモジュールは、本明細書で検討される無線トランシーバ５０２ｅを介して製品（例えば、電子ロック装置）と相互作用してもよい。レスポンスモジュール５１０は、製品により送信されたチャレンジに対するレスポンスを生成するために必要とされるセキュリティアルゴリズムを含んでもよい。更に、レスポンスモジュール５１０は、暗号化／復号及びＭＡＣ認証アルゴリズムを含んでもよく、これらは安全な通信の間にアプリケーションモジュール５０６によりアクセスされてもよい。メモリ５０２ｂはタイマ５０２ｃを更に含んでもよく、これは本明細書に記載されるように使用されるデバイス時間を維持するためのプロセッサ５０２ａのクロックコンポーネントを含んでもよい。

【００５６】

一部の実装では、メモリ５０２ｂは、製品（例えば、ロック装置）から取得した位置データに基づいて１つ以上の地図インターフェースを生成するために使用され得る地図モジュール５１２を含んでもよい。このような実装は、図８を参照して以下に記載されている。

【００５７】

ユーザ装置５００は、（ユーザ装置１０２のトランシーバ１０２ｄ及びトランシーバ１０２ｅ等に対応し得る）トランシーバ５０２ｄ及び無線トランシーバ５０２ｅを更に含み、これらは様々な通信回路を含む。例えば、一実施形態では、トランシーバ５０２ｄはセルラコンポーネント及び／又はＷｉ－Ｆｉコンポーネントを含み、無線トランシーバ５０２ｅはブルートゥースコンポーネント等を含んでもよい。ユーザ入力装置５０２ｆは、ユーザ装置５００との相互作用のために１つ以上のユーザ入力装置を含んでもよい。例えば、ユーザ入力装置５０２ｆは、１つ以上のボタン、タッチスクリーン、ディスプレイ、スピーカ、キーボード、スタイラス入力、マウス、トラックパッド等）を含んでもよい。

【００５８】

図６を参照すると、一実施形態による、本明細書に開示の技術を実装するためのサーバ６００のブロック図が示されている。サーバ６００は、１つ以上の物理的又は仮想サーバ／サーバスライス等を含む。例えば、サーバ６００は、（複数の）サーバ１０４対応してもよい。一般に、サーバ６００は、ユーザ装置（例えば、ユーザ装置５００等）と相互作用するように構成される。サーバ６００は、処理回路６０２を含んでもよい。処理回路６

０２は、プロセッサ６０２ａ及びメモリ６０２ｂを含む。例として、プロセッサ６０２ａは、任意の市販のプロセッサ、例えば、サーバ処理チップ、仮想プロセッサ等を含んでもよい。メモリ６０２ｂは、本明細書で検討される任意のメモリ及び／又は記憶装置コンポーネントを含む。例えば、メモリ６０２ｂは、ＲＡＭ及び／又はプロセッサ６０２ａのキャッシュを含んでもよい。また、メモリ６０２ｂは、任意の大容量記憶装置（例えば、ハードドライブ、フラッシュドライブ、コンピュータ可読媒体等）を含んでもよい。

【００５９】

メモリ６０２ｂは、アクセス鍵モジュール６０４及びセキュリティ鍵モジュール６０６を含んでもよい。アクセス鍵モジュール６０４及びセキュリティ鍵モジュール６０６は、それぞれアクセス鍵及びセキュリティ鍵を安全に記憶するように構成されてもよい。アクセス及びセキュリティ鍵は、本明細書で検討される製品に対応してもよい。例として、アクセス鍵モジュール６０４及びセキュリティ鍵モジュール６０６は、鍵のデータベースに対応してもよく、このような鍵を記憶し且つ取得するように構成されるソフトウェアを含んでもよい。プロファイルモジュール６０８は、（例えば、ユーザ及びゲストプロファイル生成、記憶、及びユーザ装置との通信の処理を管理するために）製品と相互作用するように構成されるソフトウェアを含む。また、プロファイルモジュール６０８はセキュリティモジュール６１０と相互作用してもよく、これは本明細書で検討されるセキュリティアルゴリズムを含んでもよい。例えば、セキュリティモジュール６１０は、アクセス鍵、セキュリティ鍵、暗号／復号データを生成し、データに基づいてＭＡＣを生成し、プロファイルモジュール６０８にこのようなデータを提供するように構成されてもよい。一実施形態では、セキュリティモジュール６１０のセキュリティ機能及びアクセス鍵モジュール６０４及びセキュリティモジュール６１０は、プロファイルモジュール６０８とは別のサーバ６００に設けられる。この実施形態では、本明細書で検討される技術を実装するために必要に応じて、プロファイルモジュール６０８がセキュリティ機能にアクセスして鍵を取得するように、様々なサービスが適切なサーバにより提供されてもよい。また、一部の実施形態では、サーバ６００は、製品（例えば、製品１０６）と相互作用するように構成される。例えば、製造工程の間、サーバ１０６は、対応する製品に記憶されるアクセス鍵及びセキュリティ鍵を提供してもよい。

【００６０】

一部の実装では、メモリ６０２ｂは、製品（例えば、ロック装置）から取得した位置データに基づいて１つ以上の地図インターフェースを生成するために使用され得る地図モジュール６１２を含んでもよい。このような実装は、図８を参照して以下に記載されている。

【００６１】

図７を参照すると、一実施形態による、本明細書に開示の技術を実装するための製品７００のブロック図が示されている。例えば、製品７００は本明細書で検討されるロックであってもよい。一般に、製品７００は処理回路７０２を含み、これはプロセッサ７０２ａ、メモリ７０２ｂ及び（本明細書に記載のように使用される製品時間を維持するために、プロセッサ７０２ａのクロックコンポーネントを含み得る）タイマ７０２ｃを含んでもよい。プロセッサ７０２ａは、市販のプロセッサ又は本明細書で検討される任意のプロセッサ（例えば、（複数の）プロセッサ４０２等）であってもよい。メモリ７０２ｂは、本明細書で検討される任意のメモリ及び／又は記憶装置コンポーネントを含む。例えば、メモリ７０２ｂは、ＲＡＭ及び／又はプロセッサ７０２ａのキャッシュを含んでもよい。また、メモリ７０２ｂは、１つ以上の大容量記憶装置（例えば、ハードドライブ、フラッシュドライブ、コンピュータ可読媒体等）を含んでもよい。

【００６２】

メモリ７０２ｂは、製品（例えば、電子ロック装置等）に関して本明細書に開示の技術を実装するように構成される様々なソフトウェアモジュールを含む。例えば、メモリ７０２ｂは、アクセス鍵モジュール７０４、セキュリティ鍵モジュール７０６、セキュリティモジュール７０８、及び制御モジュール７１０を含んでもよい。アクセス鍵モジュール７

０４及びセキュリティ鍵モジュール７０６は、製品の対応するアクセス鍵及びセキュリティ鍵をそれぞれ記憶するように構成される。メモリ７０２ｂの他のモジュールは、アクセス鍵モジュール７０４及びセキュリティ鍵モジュール７０６と相互作用してもよい。例えば、製品に関するセキュリティアルゴリズム（例えば、暗号化／復号アルゴリズム、ＭＡＣ生成／検証アルゴリズム等）が、例えば、ユーザ装置に送信されるチャレンジを生成するときに、アクセス鍵モジュール７０４からアクセス鍵を取得してもよい。別の例示として、セキュリティモジュール７０８は、セキュリティ鍵を取得してユーザ装置から受信した暗号化ユーザプロファイルを復号するためにセキュリティ鍵モジュール７０８にアクセスしてもよい。制御モジュール７１０は、製品に関して本明細書に開示の技術を実装するためにメモリ７０２ｂの他のモジュールと相互作用するように構成されるソフトウェアを含む。例えば、製品７００がロックである実施形態では、覚醒後、制御モジュール７１０は、（無線トランシーバ７０２ｄを介して）ユーザ装置とペアリング／通信することを試行してもよい。また、制御モジュール７１０は、製品７００のためのオペレーティングシステム（例えば、組み込みオペレーティングシステム、ファームウェア等）ソフトウェアを含んでもよい。別の例示として、制御モジュール７１０は、セキュリティモジュール７０８にユーザプロファイルにアクセスするように要求して、取るべきアクションを決定するように要求してもよい。ユーザプロファイルの許可及び要求に基づいて、制御モジュール７１０は、要求アクションを取るべきかどうかを決定してもよい。例えば、制御モジュール７１０は、要求（例えば、ロックに対するアンロック要求等）に応じて製品７００（例えば、ロック機構７０２ｆ）の機械（及び電子）コンポーネントを制御するために必要な信号を生成してもよい。別の例示として、制御モジュール７１０は、ロックのシャックルをアンロックするために、ロックとユーザの物理相互作用を制御するためにロック機構７０２ｆとインターフェース接続してもよい（例えば、制御モジュール７１０はダイヤルインターフェース、キーコードインターフェース、ボタン、タッチインターフェース等から入力を受信してもよい）。

【００６３】

一部の実施形態では、製品７００は、１つ以上の時間における製品７００の１つ以上の位置を決定し得るグローバルポジショニングシステム（ＧＰＳ）装置／受信機等の位置決定回路７０２ｇを含んでもよい。一部のこのような実施形態では、メモリ７０２ｂは、位置決定回路７０２ｇから位置データを受信して、１つ以上の時間における製品７００の位置又は場所を示すデータを記憶するように構成される位置追跡モジュール７１２を含んでもよい。このような実施形態は、図８を参照して以下に記載されている。

【００６４】

無線トランシーバ７０２ｄは、別の装置（例えば、ユーザ装置５００、サーバ６００等）と無線通信するために通信ハードウェア（例えば、ブルートゥースコンポーネント、無線周波コンポーネント、ＮＦＣコンポーネント、ＺｉｇＢｅｅコンポーネント、ＲＦＩＤコンポーネント、Ｗｉ－Ｆｉコンポーネント等）を含む。一部の実施形態では、製品７００は、製品に電力を提供するためのバッテリ７０２ｅを含む。製品７００がロックである実施形態では、（複数の）ロック機構７０２ｆは、本明細書で検討される１つ以上の物理的及び／又は電子ロック機構（例えば、ピン、シャックル、ダイヤル、ボタン、シャフト、キーホール等）を含む。例えば、（複数の）ロック機構７０２ｆがロック機構１０６ｇに対応してもよい。

【００６５】

一部の実施形態では、製品（例えば、ロック装置）は、位置決定回路（例えば、ＧＰＳ受信機）を含み、ロックに関する位置情報を生成し且つ記憶してもよい。次に図８を参照すると、例示的な実施形態による、製品に関する位置データを収集し且つ移動装置の地図インターフェース上に位置データを表示するための処理８００のフロー図が示されている。処理８００は地図インターフェースを提供することを例示しているが、一部の実施形態では、移動装置／（複数の）サーバが地図インターフェースを生成せずに、製品は、ロック装置に関する位置データを生成／受信し、データを記憶し、及び／又は移動装置及び／

又は１つ以上のサーバにデータを送信し得ることが理解されるべきである。

【００６６】

製品は、１つ以上の時間における製品の位置を示す１つ以上の位置データアイテムを生成し及び／又は受信してもよい（８０２）。一部の実施形態では、位置データアイテムは、ＧＰＳ受信機等の位置決定回路により生成されてもよく、製品の１つ以上のプロセッサに送信されてもよい。位置データアイテムは、メモリに記憶されてもよい（８０４）。

【００６７】

製品は、移動装置にデータを送信する要求を受信してもよい。一部の実施形態では、要求は、製品からの位置データを特に要求してもよい。他の実施形態では、要求は接続要求であってもよく、製品は移動装置との接続の成功に応じて位置データを送信してもよい。一部の実施形態では、製品は、移動装置に位置データを提供する前に移動装置からのデータの正当性を確認してもよい（８０６）。一部のこのような実施形態では、データの確認は、例えば、図２及び３を参照して先に記載されたのと同様の処理を使用して行われてもよい（例えば、チャレンジを送信し、チャレンジに対するレスポンスを検証し、秘密鍵を使用してデータの正当性を確認する等）。製品は、位置データアイテムを移動装置に送信してもよい（８０８）。一部の実施形態では、製品は、データが確認される場合にのみ移動装置に位置データアイテムを送信してもよい。

【００６８】

移動装置は、製品から（複数の）位置データアイテムを取得してもよい（８１０）。一部の実施形態では、移動装置は、地図インターフェースを生成するのに使用される位置及び／又は時間パラメータをユーザから取得してもよい（８１２）。例えば、位置パラメータは、地図インターフェースに表示された位置が制限されるべきである１つ以上の位置領域（例えば、建物、地理的領域等）を特定してもよい。このような実装では、位置パラメータは、地図インターフェースの現在の設定（例えば、地理的焦点及び／又はズームレベル）に基づいてもよい。時間パラメータは、結果に関係付けられる時間を制限してもよい。例えば、一部の実施形態では、ユーザは、製品の知られている最後の場所だけを見たいという要望を示してもよい。一部の実施形態では、ユーザは、この１週間の間の位置だけを見たいかもしれない。移動装置は、（例えば、地図インターフェースを生成する前に）位置及び／又は時間パラメータに基づいて（複数の）位置データアイテムをフィルタリングしてもよい（８１４）。例えば、パラメータを充足しないアイテムは、地図インターフェース内に表示されるデータのセットから除去されてもよい。

【００６９】

移動装置は、１つ以上の位置データアイテム（例えば、フィルタリングされたアイテム）により示される１つ以上の位置を示す地図インターフェースを生成してもよい（８１６）。一部の実装では、移動装置は、建物、関心の有る地点、及び／又は他の地図要素を含む、レンダリングされた地図インターフェース全体を生成するように構成されてもよい。一部の実装では、移動装置は、カスタム位置点の追加／オーバレイを許可する地図インターフェース等、サードパーティにより生成される地図インターフェース上のオーバレイとして位置情報を示してもよい。地図インターフェースは、移動装置のディスプレイに送信されてもよい。一部の実装では、（複数の）位置データアイテムが１つ以上のサーバに送信されてもよい（８１８）。例えば、１つの実装では、移動装置は、製品の知られている最後の位置を示すように構成されてもよく、（複数の）サーバにより管理されるインターフェースは、ユーザが指定された時間フレーム上で複数の異なる位置を見ることを可能にしてもよい。

【００７０】

図９から１５Ｂを概略的に参照すると、例示の実施形態による、ユーザ装置（例えば、移動装置）を使用して、ロック装置等の製品との相互作用の際に使用される更なる実施形態が示されている。一部の実施形態では、以下に検討される特徴は、（例えば、製造段階の間に）製品にユーザ鍵を（例えば、恒久的に）記憶せずに、ユーザ装置と製品との間の安全な通信を可能にするために使用されてもよい。例えば、ユーザ鍵は、ユーザ装置から

製品に伝達され、（通信セッションの間に）一時的に記憶及び使用されてもよい。本開示の様々な実装により、図１から８を参照して先に検討された特徴は、図９から１５Ｂを参照して以下に検討される実施形態により利用されてもよく、逆の場合も同じであることが理解されるべきである。

【００７１】

特に図９を参照すると、一実施形態による、ユーザ装置と製品との相互作用を行うための例示の処理のフロー図９００が示されている。代替的な実施形態では、より少ない、追加の、及び／又は異なるステップが実行されてもよい。また、フロー図の使用は、行われるステップの順序に関して限定することを意図していない。一部の実施形態では、下記のロック鍵は先に検討された秘密鍵と類似又は同等であってもよく、下記のユーザ鍵は先に検討されたアクセス鍵と類似又は同等であってもよい。

【００７２】

一部の実施形態では、ロックは、低電力スタンバイ又はスリープ状態から覚醒されてもよい（９０２）。例えば、ロックはユーザにより接触されてもよく（例えば、ロック上のボタンが押されてもよい）、又は（ＮＦＣセンサ等の近接センサを使用して）ユーザの接近が自動的に検出されてもよい。スタンバイ／スリープ状態は、ロックが完全に動作可能な覚醒状態にある場合よりも少ない電力（例えば、バッテリ電力）を使用し得る。一部の実施形態では、ロックは、常に完全機能状態にあってもよく、スタンバイ／スリープ状態から覚醒されなくてもよい。一部の実施形態では、低電力スリープ状態から覚醒すると、ロックは、ロックに関係付けられる一意のロック識別子（例えば、そのモデル及び／又はシリアル番号から形成される識別子）をブロードキャスト又はアドバタイズしてもよい。

【００７３】

ユーザ装置は、ロック識別子を受信する（９０４）。一実施形態では、移動装置がロックに関係付けられているかどうか（例えば、ロック識別子に対応するプロファイルが存在するかどうか）を決定するために、ロック識別子は移動装置に記憶されている一組のロック識別子のリストと比較される。例えば、各ユーザプロファイルは、ユーザプロファイルに関係付けられるユーザがアクセスの許可を有するロックを識別するロック識別子のリストを有してもよい。一致するプロファイルが見つからない場合、ユーザは、ロックをロック鍵に結び付ける一意のコードを使用して、（例えば、プロセッサ２００を介して）プロファイルを作成するように促されてもよい。ロックに関するプロファイルが見つかる場合、ユーザ装置は、プロファイルをロックに送信してもよい（９０６）。プロファイルは、少なくとも１つのロック識別子（従って、ロック）に関係付けられ、サーバ及びロックにより記憶されるロック鍵を使用してサーバにより認証及び暗号化される。一部の実施形態では、ロック鍵は、サーバ及びロックにだけ記憶されており、ユーザの移動装置には記憶されていなくてもよい。ロック鍵がハッキングされる場合、鍵はその１つのロックにおいてだけ使用することができ、それをロックから取り出すことはその過程でロックを破壊し得る。ロック鍵は、ロック鍵に関係付けられるロックの１人以上のユーザ（例えば、全てのユーザ）のプロファイルを認証及び暗号化／復号するために使用されてもよい。プロファイルはユーザ鍵を含む。

【００７４】

ロックは、プロファイルを受信して、ロック鍵を使用してプロファイルを復号及び認証する。一実施形態では、ロックはセキュリティコードを生成する（９０８）。一部の実施形態では、セキュリティコードは、シーケンス番号又は逐次同定（例えば、パケット又はメッセージの逐次同定）であってもよい。例えば、逐次同定によって、移動装置は、受信したパケット又はコマンドごとに特定の順番に従うフィールドを送信してもよい。次に、ロックは、既知の順番に対して受信したパケットを検証してもよい。一実施形態では、移動装置はロックから初期シーケンス番号を受信し、ロックは後で受信したメッセージが受信したメッセージごとに１つ増分された初期番号を含むことを検証する。

【００７５】

一部の実施形態では、セキュリティコードは、限定された時間フレームの間だけ有効で

あってもよい。例えば、一部の実施形態では、セキュリティコードは、コードの最初の使用の後で、特定の時間量の間だけ有効であってもよい。一部の実施形態では、セキュリティコードは、所定数のコマンド、トランザクション、及び／又は通信セッションに対してだけ有効であってもよい。一部のこのような実施形態では、セキュリティコードは、単一のコマンド又は単一の通信セッションに対してだけ使用されるが、その後再び使用されてなくてもよい。

【００７６】

このような既知の順番は、ロックにより事前決定され又は生成されてもよく、また通信中にロックにより移動装置に提供されてもよい。従って、このシーケンシングは、上記の１つ以上の他の方法と共に使用されてもよく（例えば、既定の初期シーケンスフィールド値と共にセッション識別子が使用されてもよい）、又はシーケンシングはそれ自身により使用されてもよい（例えば、ロックは、接続時にシーケンスフィールドの初期値を提供してもよい）。ロックは、受信したメッセージがユーザ鍵を使用して暗号化され及び／又はそれから計算されるＭＡＣを含むことを更に検証してもよい。

【００７７】

次に、移動装置は、セキュリティコードを含み且つユーザ鍵を使用して暗号化される暗号化コマンドを生成してロックに送信し得る。シーケンス番号などの特定のコマンド及び／又は通信セッションに一意であるセキュリティコードと組み合わせて、ユーザ鍵を使用して通信を認証及び暗号化／復号することは、通信のリプレイ、スニフィング、及び改竄を防ぐのに役立ち得る。一実施形態では、移動装置は、移動装置のクロックに基づいて現在のタイムスタンプも送信する。一部の実施形態では、セキュリティコードは、ユーザ認証ＭＡＣの生成に含まれ、暗号化コマンドには含まれない。

【００７８】

ロックは、暗号化コマンドの正当性を確認することができる（９１２）。一部の実施形態では、ロックは、復号ユーザプロファイルから取得したユーザ鍵を使用して暗号化コマンドを復号し、セキュリティコードが有効であるかどうかを決定し、及び／又はユーザ鍵を使用して復号コマンドを認証することによって暗号化コマンドの正当性を確認する。一部の実施形態では、ロック及び移動装置は共に、セキュリティコードフィールドが予想通りであること検証してもよく、接続時に予想の初期状態を確立してもよい。また、一部の実施形態では、サーバは、それが生成された製品をロック鍵に結び付けるためのコードを生成してもよい。一部の実施形態では、コードは（例えば、包装内に固定される指示シート上のラベルとして）ロックと共に出荷されてもよいまた、先に検討されたように、サーバは、攻撃者がシリアル番号を推測して、まだ棚に有るロックへのアクセスを所有しようとすることを防ぐために、製品コードとは異なり得るロック用の一意の識別子（例えば、シリアル識別子）を生成してもよい。

【００７９】

一部の実施形態では、セキュリティコードは、ユーザ認証ＭＡＣ等の通信セッション用に別のコードを生成する際に使用されてもよい。一部のこのような実施形態では、セキュリティコードは、まず第１にロックから移動装置に送信されてもよい。また、セキュリティコードは、移動装置からロックに送信される第１の暗号化コマンドに含まれてもよい。後続の通信において、セキュリティコードは含まれてもよく又は含まれなくてもよい。ロックは、後続の通信においてユーザ認証ＭＡＣを検証してもよく、ＭＡＣを検証することによって、ロックは同様にセキュリティコードを間接的に検証している。従って、一部の実施形態では、セキュリティコードは、１つ以上のメッセージ／コマンドのペイロードには含まれなくてもよい。

【００８０】

また、一部の実施形態では、ロックは、（例えば、復号プロファイルに含まれるスケジュール情報を参照することによって）その検証された時間にプロファイルがアクセスを有することを確実にしてもよい。移動装置がタイムスタンプを送信した実施形態では、ロックは、タイムスタンプをロックの現在の時間と比較することによってタイムスタンプを検

証してもよい。先に検討されたタイムスタンプを利用する実施形態では、受信したタイムスタンプは、ロックにより維持される時間から閾値量の時間内であることが要求されてもよい。一実施形態では（例えば、ユーザプロファイル許可により許可される場合）、ロックの時間を同期又は更新するために移動装置からのタイムスタンプが使用されてもよい。

【００８１】

プロファイル及びコマンドの両方が検証される場合、ロックは、移動装置の要求に従って、対応するアクションを開始してもよい（９１４）。一実施形態では、ロックは、物理ロックコンポーネントをアクティブ化することができる。一実施形態では、物理ロックコンポーネントをアクティブ化した後で、ロックはそのロック識別子をブロードキャストし、移動装置はユーザプロファイルを送信し、ロックは新しいセキュリティコードを送信し、移動装置は新しいセキュリティコードを含む別の暗号化コマンドを送信する（例えば、状態を読み込む、時間を同期する、データを監査する、構成を修正する等）。

【００８２】

図１０を参照すると、一実施形態による、特定のユーザ装置からユーザプロファイルを除去するための例示の処理のフロー図１０００が示されている。代替的な実施形態では、より少ない、追加の、及び／又は異なるステップが実行されてもよい。また、フロー図の使用は、行われるステップの順序に関して限定することを意図していない。特定のユーザ装置からユーザプロファイルを除去する処理は、例えば、特定のユーザ装置が無くなるか、盗まれるか、又はそれ以外にユーザに所持されていない場合に第三者がロックへのアクセスを有することを防ぐために使用されてもよい。

【００８３】

一実施形態では、サーバは、ユーザの信頼できる装置から特定のユーザ装置の選択を受信してもよい（１００２）。一部の実施形態では、サーバは、ユーザプロファイルを除去する要求が受信された装置が認証データを装置から受信することによって信頼できることを決定してもよい。例えば、ユーザは、装置上のアプリケーション及び／又はサーバによりホスティングされるフロントエンドインターフェースにアクセスし、ユーザ名及びパスワード等の認証データを使用してアカウントにログインするために装置を使用してもよい。次に、ユーザは、選択された特定のユーザ装置が無くなったことの指示を提供してもよい。

【００８４】

一実施形態では、サーバは、特定のユーザ装置上のユーザのプロファイルの全てを除去してもよい（１００４）。一部の実施形態では、サーバは、無くなった装置で実行中のアプリケーションにコマンドを送信することによってプロファイルを除去してもよい。次に、無くなった装置で動作中のアプリケーションは、装置からユーザプロファイルデータを除去してもよい。

【００８５】

サーバは、ユーザのプロファイルの除去に成功したかどうかをユーザに通知してもよい。ユーザのプロファイルの全ての除去に成功した場合、処理は終了する（１０１６）。この場合、鍵はまだ安全であると見なされてもよく、鍵の交換は開始されなくてもよい。一部の実施形態では、鍵交換コマンドは、全てのプロファイルの除去が成功した場合であっても送信されてもよい。例えば、一部の実施形態では、プロファイル／鍵を交換することは、無くなった装置からプロファイルを除去することが成功した場合であってもデフォルトレスポンスであってもよい。

【００８６】

一部の実施形態では、無くなった装置からプロファイルを除去する動作が成功しない場合がある。例えば、電話はオンラインでなくてもよい（例えば、オフにされていてもよく、ネットワーク接続が無効にされていてもよく、又はネットワークアクセスの無い場所に居てもよい）。一実施形態では、全てのユーザプロファイルの除去が失敗することに応じて、サーバは、除去が成功しなかった特定の移動装置上のユーザプロファイルごとに鍵交換コマンドを生成して、除去が成功しなかったユーザプロファイルに関係付けられるロッ

ク識別子を含む全ての信頼できる装置に送信する（１０１０）。鍵交換コマンドは、サーバにより元のロック鍵を使用して暗号化されたロックに関係付けられる新しいロック鍵を含む。無くなった又は盗まれた移動装置はロックへのアクセスを得てロックの全ての信頼できるユーザに影響を与えるために使用され得るので、一部の実施形態では、信頼できる各ユーザは、信頼できる装置を介して鍵交換をもたらす能力を有してもよい。一実施形態では、信頼できる装置がロックを訪問すると、ロックと相互作用する処理（例えば、処理９００）が行われ、ロックにより鍵交換コマンドが受信され、正当性が確認され、且つ開始される。一部の実施形態では、ロック内でどれくらい迅速に鍵交換が行われるかは、どのくらいユーザが心配しているか及びロックの地理的分布の要因であってもよい。ユーザは、誰かが古い電話を使用する脅威を取り除くためにできるだけ早く全てのロックを訪問してもよく、又はそれはロックが通常の使用で訪問されると経時的に行われ得る。他のユーザに鍵交換コマンドを送信する能力は、他人がロックを訪問してユーザのためにロック鍵を変更することを可能にする。一部の実施形態では、鍵交換コマンドは、（例えば、ロックの無線トランシーバを使用して）ロックに直接送信されてもよい。一実施形態では、サーバは、新しいロック鍵をロックに記憶することに成功したことを確認する（１０１２）。一実施形態では、サーバは、信頼できる装置に更新されたユーザプロファイルを送信する（１０１４）。交信されたユーザプロファイルは新しいロック鍵を使用するサーバにより認証され且つ暗号化されてもよく、更新されたユーザプロファイルは新しいユーザ鍵を含んでもよい。

【００８７】

図１１を参照すると、一実施形態による、ゲストユーザの装置からゲストユーザプロファイルを除去するための例示の処理のフロー図１１００が示されている。代替的な実施形態では、より少ない、追加の、及び／又は異なるステップが実行されてもよい。また、フロー図の使用は、行われるステップの順序に関して限定することを意図していない。ゲストユーザの特定のユーザプロファイルを除去する処理は、例えば、ユーザによりゲストに以前に与えられていたロックへのアクセスを取り消すために使用されてもよい。

【００８８】

一実施形態では、サーバは、ユーザの移動装置から取り消すためにゲストユーザの１つ以上の特定のユーザプロファイルの選択を受信する（１１０２）。一部の実施形態では、選択を受信する前に、移動装置は、（例えば、ユーザ名及びパスワード等、ユーザから認証情報を受信することによって）最初に認証されてもよい。一実施形態では、サーバは、ゲストユーザの移動装置から１つ以上の特定のユーザプロファイルを除去してもよい（１１０４）。一部の実施形態では、サーバは、ゲストユーザの全ての移動装置から１つ以上の特定のユーザプロファイルを除去してもよい（１１０４）。

【００８９】

一実施形態では、サーバは、特定のユーザプロファイルの除去に成功したかどうかをユーザに通知してもよい（１１０６）。ユーザのプロファイルの全ての除去に成功した場合、処理は終了する（１０１６）。一部の実施形態では、鍵交換コマンドは、全てのプロファイルの除去が成功した場合であっても送信されてもよい。

【００９０】

一部の実施形態では、ユーザプロファイルの除去は、（例えば、ゲスト装置がオフラインであるか又はそれ以外に到達不能であるため）失敗する場合がある。一実施形態では、全てのユーザプロファイルの除去が失敗することに応じて、サーバは、除去が成功しなかったゲストユーザの移動装置上の特定のユーザプロファイルごとに鍵交換コマンドを生成して、除去が成功しなかった特定のユーザプロファイルに関係付けられるロック識別子を含む全ての信頼できる装置に送信する（１０１０）。鍵交換コマンドは、サーバにより元のロック鍵を使用して暗号化されたロックに関係付けられる新しいロック鍵を含む。ゲストユーザはまだロックへのアクセスを得ていて、特定のユーザプロファイルが除去されない場合にロックの全ての信頼できるユーザに影響を与えるので、一部の実施形態では、信頼できる各ユーザは、信頼できる装置を介して鍵交換をもたらす能力を有してもよい。一

実施形態では、信頼できる装置がロックを訪問すると、ロックと相互作用する処理（例えば、処理９００）が行われ、ロックにより鍵交換コマンドが受信され、正当性が確認され、且つ開始される。一実施形態では、サーバは、新しいロック鍵をロックに記憶することに成功したことを確認する（１１１２）。一実施形態では、サーバは信頼できる装置に更新されたユーザプロファイルを送信し、ここで、更新されたユーザプロファイルは新しいロック鍵を使用してサーバにより認証され且つ暗号化され、且つ更新されたユーザプロファイルは新しいユーザ鍵を含む（１１１４）。

【００９１】

一部の実施形態では、ゲスト装置からプロファイルを取り消すために鍵交換を使用することの代わりに又はそれに加えて、ブラックリストが利用されてもよい。例えば、アクセスが取り消される１つ以上のゲスト装置の一意の及び／又は持続的識別子が、禁止装置のブラックリストに加えられて（複数の）ロック内に記憶されてもよい。このような方法は、新しい鍵／ユーザプロファイルを再配布せずにアクセス制御を可能にしてもよい。しかしながら、一部の例では、ゲストユーザが能動的にアクセス取り消しを回避しようとしている場合、ユーザはゲスト装置をオフラインに維持して、鍵を取得しようとする場合がある。このような場合、鍵及びユーザプロファイルを置換する方がより安全であり得る。一部の実施形態では、セキュリティレベルを高めるために、鍵交換手続きと組み合わせてブラックリストが利用されてもよい。

【００９２】

図１２を参照すると、一実施形態による、ロックへのゲストユーザアクセスを許可するための例示の処理のフロー図１２００が示されている。代替的な実施形態では、より少ない、追加の、及び／又は異なるステップが実行されてもよい。また、フロー図の使用は、行われるステップの順序に関して限定することを意図していない。

【００９３】

一実施形態では、サーバは、ユーザの移動装置から、ユーザの移動装置に記憶されている一組のロック識別子からゲストユーザと共有するための１つ以上のロックに関係付けられる１つ以上のロック識別子の選択を受信する（１２０２）。一部の実施形態では、選択は、アクセスを許可するユーザの１つ以上のユーザプロファイルに関係付けられるロックリストからであってもよい。

【００９４】

一実施形態では、サーバは、ユーザの移動装置からゲストユーザプロファイル要求を受信する（１２０４）。一部の実施形態では、ゲストユーザプロファイル要求は構成されてもよく、ゲストプロファイル要求を構成することは、ロックがゲストによりいつアクセスされ得るかを定義するゲストユーザスケジュールデータ、満了するとゲストユーザプロファイルが無効になるゲストユーザプロファイルの満了時間を設定する取り消しデータ、及び／又は移動装置により維持される時間が信頼できるかどうかの指示を修正することを含んでもよい。一部の実施形態では、ゲストプロファイルの１つ以上のこうした特徴及び／又は他の特徴は、ゲストアクセスを許可するユーザにより構成可能であってもよい。

【００９５】

一実施形態では、サーバは、ゲストユーザプロファイル要求及びゲストユーザ鍵に基づいて認証され且つ暗号化されたゲストユーザプロファイルを生成する（１２０６）一部の実施形態では、認証され且つ暗号化されたゲストユーザプロファイルは、共有されるロックに関係付けられるロック鍵を使用して暗号化され、認証され且つ暗号化されたゲストユーザプロファイルはゲストユーザ鍵を含む。一部の実施形態では、ゲストユーザ鍵は、ゲストユーザプロファイルの中に、移動装置により読み取ることができるように記憶される。ゲストユーザ鍵は、個人ゲストユーザごとに一意に生成される。これは、ゲストユーザが別のユーザの鍵を使用することを防ぐ。

【００９６】

サーバは、ゲストユーザの移動装置がゲストユーザプロファイルにアクセスできるかどうかを決定してもよい（１２０８）。一部の実施形態では、サーバは、ゲストユーザが登

録ユーザであるかどうか及び／又はゲストユーザの移動装置にインストールされたロックと相互作用するために使用されるアプリケーションを有するかどうかを決定してもよい。

【００９７】

一実施形態では、ゲストユーザの移動装置がゲストユーザプロファイルにアクセスできる（例えば、ゲストユーザが登録ユーザであり及び／又はゲストユーザの移動装置にアプリケーションがインストールされている）とサーバが決定する場合、サーバは、ユーザの移動装置からゲストアクセスを許可するユーザの移動装置における（例えば、一組の登録ユーザからの）ゲストユーザの選択を受信する（１２１０）。一部の実施形態では、ゲストユーザの選択は、移動装置におけるゲストユーザの検索からであってもよい。一実施形態では、サーバは、選択を受信した後でゲストユーザの移動装置にゲストユーザプロファイル及びゲストユーザ鍵を送信する（１２１２）。一実施形態では、サーバは、ゲストユーザの移動装置上の一組のロック識別子にゲストユーザプロファイルに関係付けられるロック識別子を追加する。

【００９８】

一実施形態では、ゲストユーザアクセスの移動装置がゲストユーザプロファイルにアクセスできない（例えば、ゲストユーザが登録ユーザではなく及び／又はゲストユーザの移動装置にアプリケーションがインストールされていない）ことを決定すると、サーバはメッセージを生成して、ゲストユーザの移動装置に送信する。一部の実施形態では、メッセージは、（複数の）ロック鍵へのアクセスを許可するために使用されるコード、及び／又はゲストユーザがコードを入力し及び／又はアプリケーション及び／又はゲストプロファイルをダウンロードし得る認証リソース（例えば、ウェブページ）へのリンクを含んでもよい。一部の実施形態では、メッセージはＥメール又はＳＭＳ／テキストであってもよい。一部の実施形態では、リンクは、アクティベーションリンクであってもよい。一部の実施形態では、コードは、招待コード又は承認コードであってもよい。

【００９９】

一実施形態では、サーバは、ゲストユーザの移動装置においてユーザプロファイルへのアクセスを許可するためにリンクが使用されたことを決定する（１２１８）。一部の実施形態では、リンクはゲストユーザが移動装置にアプリケーションをダウンロードすることを許可してもよく、ユーザはリンクされたリソースにおいて及び／又はダウンロードされたアプリケーションを介して新しいゲストアカウントを作成するための登録情報を入力してもよい。一部の実施形態では、サーバは、ゲストユーザの移動装置が今のところユーザプロファイルにアクセスできることを決定する。一実施形態では、サーバは、ゲストユーザの移動装置においてコードが入力されたことを決定する（１２２０）。一実施形態では、サーバは、ゲストユーザの移動装置にゲストユーザプロファイル及びゲストユーザ鍵を送信する（１２１２）。一実施形態では、サーバは、ゲストユーザの移動装置上の一組のロック識別子にゲストユーザプロファイルに関係付けられるロック識別子を追加する（１２１４）。

【０１００】

図１３を参照すると、一実施形態による、製品及びユーザ装置を構成するための処理１３００のフロー図が示されている。代替的な実施形態では、より少ない、追加の、及び／又は異なるステップが実行されてもよい。また、フロー図の使用は、行われるステップの順序に関して限定することを意図していない。

【０１０１】

ロック識別子が取得される（１３０２）。例えば、ユーザは、ロック識別子を取得するために包含された製品包装を参照してもよく、ユーザは他のやり方で（例えば、製造業者ウェブサイト、電話等を介して）ロック識別子を取得するために製造業者に接触してもよい。ユーザが登録ユーザである場合、ユーザは、ロック識別子を取得及び／又は入力する前にユーザの移動装置上のアプリケーションを開き及び／又はアプリケーションにログインしてもよい。ユーザが登録されていない場合、ユーザは、新しいアカウントを作成して、それを管理サーバに登録してもよい。一部の実施形態では、ユーザは、ユーザの移動装

置にアプリケーションをダウンロードして、アプリケーションを介してアカウントを作成してもよい。一部の実施形態では、ユーザは、（例えば、移動装置上のブラウザアプリケーションを介して）サーバから移動装置に提供されるフロントエンドインターフェースを介してアカウントを作成してもよい。

【０１０２】

次に、ロック識別子は、ロックをユーザと関係付けるために、管理サーバに提供される（１３０４）。例えば、ユーザは移動装置で実行中のアプリケーションのユーザインターフェースにロック識別子を入力してもよく、次に移動装置はロック識別子をサーバに送信する。このような例示では、ユーザは、管理サーバにより提供され且つ移動装置上のブラウザアプリケーションを介してアクセスされるフロントエンドインターフェース内でロック識別子を入力してもよい。代替的に、ユーザは、移動装置を使用して、ロック識別子を取得し且つ送信するためにロックの包装をスキャンしてもよい。例えば、ロック識別子は、バーコード、ＱＲコード、光学コード等により符号化されてもよく、移動装置のカメラが一意のコードをスキャンして決定するために使用されてもよい。移動装置からロック識別子を受信することに応じて、サーバはロック鍵及びユーザ鍵を（例えば、要求に応じて）取得し又は新たに生成することができ、次にロック鍵及びユーザ鍵はロック識別子に関係付けられてもよい。一部の実施形態では、サーバは、例えば、ロック識別子を有効な識別子であることが知られている一組の識別子と比較することによって、ロック識別子（例えば、製品コード）が有効であることを検証してもよい。

【０１０３】

次に、サーバはユーザプロファイルを生成してもよく（１３０６）、これはロック識別子に関係付けられてもよい。ユーザプロファイルがまだ存在していない場合、新しいプロファイルを生成するために、デフォルト値、又は移動装置を介してユーザにより提供された値が使用されてもよい。例えば、ユーザは、移動装置のアプリケーションにプロファイルデータを入力してもよく、移動装置はロック識別子と共にサーバにプロファイルデータを送信する。ユーザがプロファイルを既に作成している場合、サーバは、その代わりに移動装置を介してユーザにより提供される新しい値でユーザプロファイルを更新してもよい。

【０１０４】

一般に、ユーザプロファイルは、上記の実施形態におけるロックである製品の動作に関連するデータを含む１つ以上のファイルを含んでもよい。例えば、ユーザプロファイルは、ロックがいつアクセス（アンロック、ロック等）され得るかのユーザスケジュールを含んでもよい。スケジュールは、対応する許可ごとに、例えば、曜日により、開始時間（時間、分等）及び終了時間（時間、分等）を含むロックアクセス許可を特定してもよい。例えば、スケジュールは、電子ロックが移動装置を介してアンロックされ得る時間間隔を特定してもよい。別の例示として、スケジュールは、典型的な相互作用が起こると予想される時間周期、及びこうした時間周期に基づいて決定され得る信頼レベルを特定してもよい。従って、予想される時間周期内に送信されるアンロック要求は、予想外の／非典型的な時間に送信される要求よりもロックによって信頼されてもよい。また、移動装置は、スケジュールを自動的に調節してもよい。例えば、移動装置は、ロックとのユーザの相互作用のログ／記録を取ってもよく、ユーザの予想されるアクションに基づいてスケジュールを設定してもよい。一実施形態では、（例えば、製造業者等により）デフォルトユーザスケジュールが設定される。更に、典型的にはユーザスケジュールのリストは、ユーザが多くの構成オプションの１つから選択することを可能にするように提供されてもよい。このように、製造業者は、様々な推奨動作設定をユーザに提供してもよい。また、ユーザは、スケジュールをカスタマイズして、所望のスケジュールに調整してもよい。

【０１０５】

ユーザプロファイルは、ロックのモデル／シリアル番号及びどのようなタイプのアクセスがそのユーザに利用可能であるかを更に特定してもよい。例えば、このようなアクセスは、とりわけ、ロックのソフトウェア／ハードウェアバージョン情報を読み取ること、ロ

ックのソフトウェアを更新すること、ロックのシャックル状態を読み取ること、ロックすること、アンロックすること、解除すること、時間／クロックの値を読み取る／設定すること、バッテリレベルを読み取ること、イベント関連データ（例えば、フラグ、カウンタ等）を読み取る／消去すること、ロックのログを読み取ること、ロックのキーパッドコードを読み取る／設定する／リセットすること、ロック用の通信データ（例えば、送信状態、送信電力レベル、チャネル情報、アドレス情報等）を読み取ること、ロック用に記憶されたデフォルト値（例えば、デフォルト解除時間、デフォルトアンロック時間）を読み取る／設定することを含んでもよい。また、ユーザプロファイルは、プロファイル用の開始時間及び取り消し日／時間（即ち、プロファイルが有効であり始めるとき及びプロファイルが満了してもはや有効ではなくなるとき）を特定してもよい。ユーザプロファイルは、ロック用の最大解除／アンロック時間を提供してもよい。ユーザプロファイルは、対応する移動装置の信頼レベルの指示（例えば、移動装置により提供された時間値／タイムスタンプが信頼できるかどうか）を提供してもよい。ロックは、装置の信頼レベルに基づいて所定の機能を許可する又は無効にするように構成されてもよい。信頼レベルは、ユーザがアクセスを有する又は有さない独立許可として記憶されてもよい（例えば、信頼レベルは、ロック、移動装置又はサーバ等のソフトウェアにより管理／調節されてもよい）。例えば、高信頼装置のみがロックのファームウェアを更新する又は所定の設定を変更することが可能であってもよい。更に、ロックは、信頼レベル及び時間値を計算に入れるセキュリティアルゴリズムを有してもよい。例えば、装置がより頻繁にロックとの相互作用を成功させると、ロックは装置に対する信頼レベルを増加（又は調節）してもよい。しかしながら、時間値がロックの維持時間との同期外であり又は認証が失敗する場合、ロックは装置に対する信頼レベルを低下（又は調節）してもよい。移動装置により提供される時間値はロックにより維持される時間値と比較されてもよく、２つの時間の間の近接度は装置に対する信頼レベルを示すために使用されてもよい（例えば、２つの時間が同期するのに近いほど、信頼レベルは高くなる等）。信頼レベルが所定の閾値を下回る場合、ロックは移動装置との相互作用を中断又は制限してもよい。また、信頼レベルは、先に検討されたスケジュールに基づいてもよい。例えば、移動装置は、装置がロックにアクセスしている時間、及びその時間がスケジュールにより定義された所定の時間周期内に入るかどうかに基づいてより信頼されている又はあまり信頼されていないと見なされてもよい。また、移動装置により提供される時間値は、ロックのクロックを移動装置のそれと同期するために使用されてもよく、又は認証された通信の間に他のやり方で使用されてもよい。検討された任意のプロファイルアイテムは、デフォルト値（例えば、製造業者のデフォルト）又はユーザ提供値を有してもよい。プロファイルは上記のデータに限定されず、追加データが含まれてもよい。また、プロファイルは、後で取得するためにサーバに記憶されてもよい。

【０１０６】

ユーザ（例えば、ロックの所有者）に対してプロファイルを生成することに加えて、ユーザは、友人、家族、同僚等と共有される追加のゲストプロファイルを作成することを望む場合がある（１３０８）。このように、ユーザは、ゲストプロファイルに基づいて、ロックへのアクセスを別の人物に許可してもよい。そうするために、ユーザは、（複数の）追加の人物用に（移動装置を使用して）所望のプロファイル値を入力してもよい。ユーザのプロファイルの作成と同様に、ゲストプロファイルデータは、サーバに送信されて、図１２に関連して先に検討されたように処理されてもよい。ゲストプロファイルデータは、ユーザが自身のプロファイルを最初に生成するときと同時に又は別に（例えば、後の時間に）サーバに送信されてもよい。移動装置は、ユーザに提供されるプロファイルのタイプ（例えば、所有者とゲスト）を区別する情報を含む。

【０１０７】

少なくとも１つのプロファイルが生成された後で、ユーザはロックの所有者として特定のロックに関係付けられる。一部の実施形態では、関係付けは、（例えば、ステップ１３０４で）サーバに提供されたロック識別子のみに基づいてもよい。一実施形態では、ロック識別子を提供した後で、移動装置は、ロック識別子を使用して、ロックの製造業者のサ

ーバ又はデータベースからロックに関連する追加情報（例えば、シリアルＩＤ、モデル番号等）を自動的に取得してもよい。代替的な実施形態では、シリアルＩＤ、モデル番号又は他のコードは、ユーザにより（例えば、製品包装等を参照することにより）提供されてもよく、このような追加データは、ユーザをロックと関係付ける際にロック識別子と共に利用されてもよい。一部の実施形態では、ユーザをロックと関係付ける前にユーザの追加認証が要求されてもよく、このような認証は移動装置を介して提供されてもよい。

【０１０８】

一部の実施形態では、管理サーバは、受信したプロファイルデータを検証してもよい。取得したプロファイルデータを検証するために、管理サーバは、データの完全性を確実にするためにプロファイルに巡回冗長検査（ＣＲＣ）を行ってもよい。また、他のデータ検証方法が利用されてもよい。例えば、例示的な実施形態では、ロック鍵を使用して、メッセージ認証コード（ＭＡＣ）（例えば、鍵付きハッシングメッセージ認証コード（ＨＭＡＣ））が生成され且つデータ完全性の検証に使用されてもよい。本開示の範囲は所定のデータ完全性確認方法に限定されない。次に、サーバは、プロファイルデータを認証及び暗号化されたユーザプロファイル（例えば、暗号文）に変換するために、秘密鍵を使用してプロファイルデータを認証及び暗号化することができる。プロファイルは、任意の既知の暗号化標準に従って暗号化されてもよい。また、ユーザプロファイルは対応するユーザ鍵も含む。ユーザ鍵は、（例えば、ステップ１３０２－１３０４で検討されたように）ロック識別子を使用してサーバにより決定され得る。

【０１０９】

暗号化した後、暗号化プロファイルは、サーバから移動装置に送信される（１３１０）。次に、受信した暗号化プロファイル及びユーザ鍵は、ロックと移動装置の関係付けを完了するために、移動装置のメモリに記憶される。次に、ユーザは、自身の移動装置を使用してロックと相互作用してもよい（１３１２）。一部の実施形態では、ユーザは、移動装置上のアプリケーションを使用して、ロック入力をカスタマイズしてもよい。例えば、ユーザは、ロックプロファイルを選択して、限定されないが、ロック名、説明、ＧＰＳ座標、写真、許可されたゲストユーザ等のカスタマイズ情報を提供するために構成を編集してもよい。

【０１１０】

図１４を参照すると、別の実施形態による、本明細書に開示の技術を実装するための製品１４００のブロック図が示されている。例えば、製品１４００は本明細書で検討されるロックであってもよい。一般に、製品１４００は処理回路１４０２を含み、これはプロセッサ１４０２ａ、メモリ１４０２ｂ及び（本明細書に記載のように使用される製品時間を維持するために、プロセッサ１４０２ａのクロックコンポーネントを含み得る）タイマ１４０２ｃを含んでもよい。プロセッサ１４０２ａは、市販のプロセッサ又は本明細書で検討される任意のプロセッサ（例えば、（複数の）プロセッサ４０２等）であってもよい。一実施形態では、プロセッサ１４０２ａは、メモリにロック識別子及びロック鍵を記憶し、トランシーバを介してロック識別子をブロードキャストし、トランシーバを介して移動装置から暗号化ユーザプロファイルを受信し、ロック鍵を使用して暗号化ユーザプロファイルを認証及び復号し、トランシーバを介して移動装置にセキュリティコードを送信し、トランシーバを介して移動装置から暗号化コマンドを受信し、暗号化コマンドの正当性を確認するように構成され、暗号化コマンドの正当性を確認することは、復号されたユーザプロファイルからユーザ鍵を使用して暗号化コマンドを復号すること、セキュリティコードが有効であるかどうかを決定すること、及びユーザ鍵を使用して暗号化コマンドを認証すること、及びコマンドの正当性を確認することに応じて、コマンドによって特定された電子ロック装置のアクションを開始することを含んでもよい。一部の実施形態では、セキュリティコードはシーケンス番号であってもよい。一部の実施形態では、セキュリティコードは、限定された時間の間だけ有効であってもよい。

【０１１１】

メモリ１４０２ｂは、本明細書で検討される任意のメモリ及び／又は記憶装置コンポー

ネントを含む。例えば、メモリ１４０２ｂは、ＲＡＭ及び／又はプロセッサ１４０２ａのキャッシュを含んでもよい。また、メモリ１４０２ｂは、１つ以上の大容量記憶装置（例えば、ハードドライブ、フラッシュドライブ、コンピュータ可読媒体等）を含んでもよい。メモリ１４０２ｂは、製品（例えば、電子ロック装置等）に関して本明細書に開示の技術を実装するように構成される様々なソフトウェアモジュールを含む。例えば、メモリ１４０２ｂは、ロック鍵モジュール１４０６、セキュリティモジュール１４０８、及び制御モジュール１４１０を含んでもよい。ロック鍵モジュール１４０６は、製品の対応するロック鍵を記憶するように構成される。一部の実施形態では、製品１４００は１３００の処理を行い、例えば、ユーザ鍵はユーザプロファイルの一部であり、ユーザ鍵を別々に記憶する必要性は無い。メモリ１４０２ｂの他のモジュールは、ロック鍵モジュール１４０６と相互作用してもよい。例えば、セキュリティモジュール１４０８は、ロック鍵を取得してユーザ装置から受信した暗号化ユーザプロファイルを復号するためにロック鍵モジュール１４０８にアクセスしてもよい。制御モジュール１４１０は、製品に関して本明細書に開示の技術を実装するためにメモリ１４０２ｂの他のモジュールと相互作用するように構成されるソフトウェアを含む。例えば、製品１４００がロックである実施形態では、覚醒後、制御モジュール１４１０は、（無線トランシーバ１４０２ｄを介して）ユーザ装置とペアリング／通信することを試行してもよい。また、制御モジュール１４１０は、製品１４００のためのオペレーティングシステム（例えば、組み込みオペレーティングシステム、ファームウェア等）ソフトウェアを含んでもよい。別の例示として、制御モジュール１４１０は、取るべきアクションを決定するために、セキュリティモジュール１４０８にユーザプロファイル及びコマンドにアクセスするように要求してもよい。ユーザプロファイルの許可及びコマンドに基づいて、制御モジュール１４１０は、コマンドアクションを取るべきかどうかを決定してもよい。例えば、制御モジュール１４１０は、要求（例えば、ロックに対するアンロック要求等）に応じて製品１４００（例えば、ロック機構１４０２ｆ）の機械（及び電子）コンポーネントを制御するために必要な信号を生成してもよい。別の例示として、制御モジュール１４１０は、ロックのシャックルをアンロックするために、ロックとユーザの物理相互作用を制御するためにロック機構１４０２ｆとインターフェース接続してもよい（例えば、制御モジュール１４１０はダイヤルインターフェース、キーコードインターフェース、ボタン、タッチインターフェース等から入力を受信してもよい）。

【０１１２】

一部の実施形態では、製品１４００は、１つ以上の時間における製品１４００の１つ以上の位置を決定し得るグローバルポジショニングシステム（ＧＰＳ）装置／受信機等の位置決定回路１４０２ｇを含んでもよい。一部のこのような実施形態では、メモリ１４０２ｂは、位置決定回路１４０２ｇから位置データを受信して、１つ以上の時間における製品１４００の位置又は場所を示すデータを記憶するように構成される位置追跡モジュール７１２を含んでもよい。

【０１１３】

無線トランシーバ１４０２ｄは、別の装置（例えば、ユーザ装置５００、サーバ６００等）と無線通信するために通信ハードウェア（例えば、ブルートゥースコンポーネント、無線周波コンポーネント、ＮＦＣコンポーネント、ＺｉｇＢｅｅコンポーネント、ＲＦＩＤコンポーネント、Ｗｉ－Ｆｉコンポーネント等）を含む。一部の実施形態では、製品１４００は、製品に電力を提供するためのバッテリ１４０２ｅを含む。製品１４００がロックである実施形態では、（複数の）ロック機構１４０２ｆは、本明細書で検討される１つ以上の物理的及び／又は電子ロック機構（例えば、ピン、シャックル、ダイヤル、ボタン、シャフト、キーホール等）を含む。例えば、（複数の）ロック機構１４０２ｆがロック機構１０６ｇに対応してもよい。

【０１１４】

図１５を参照すると、一実施形態による、ユーザ装置と製品との相互作用を行うための例示のデータフロー処理のデータフロー図が示されている。図１５は、可読性のために第

１の部分図１５Ａと第２の部分図１５Ｂとに分けられている。例示のデータフロー図は、例示の実施形態による、（例えば、図９から１４を参照して）先に検討された１つ以上の機能を行うためにサーバ、モバイルアプリケーション及びロックの間で安全な通信を遂行するために利用され得るデータフローを例示する。

【０１１５】

本明細書における「一実施形態」、「一部の実施形態」又は「実施形態」への参照は、実施形態との関連で記載された特定の機能、構造又は特徴が少なくとも１つの実施形態に含まれることを意味する。本明細書の様々な場所における「一実施形態では」又は「一部の実施形態では」という句の出現は、必ずしも全てが同じ実施形態を参照しているのではなく、他の実施形態を相互に除外する別個の又は代替の実施形態でもない。更に、一部の実施形態により示されているが他の実施形態により示されていない様々な特徴が記載されている場合がある。同様に、一部の実施形態には必須であるが他の実施形態には必須でない様々な要件が記載されている場合がある。

【０１１６】

本開示は、図面を参照して先に記載されている。こうした図面は、本開示のシステム及び方法及びプログラムを実装する特定の実施形態の所定の詳細を示している。しかしながら、図面と共に開示を説明することは、図面に存在し得る何らかの限定を本開示に課すものと解釈されるべきではない。本開示は、その動作を遂行するための任意の機械可読媒体における方法、システム、プログラム製品を考慮している。本開示の実施形態は、既存のコンピュータプロセッサを使用して、又はこの目的若しくは別の目的で組み込まれた専用コンピュータプロセッサにより又は配線化システムにより実装されてもよい。請求項の要素は、“ｍｅａｎｓ　ｆｏｒ”の句を使用して明示的に記載されない限り、米国特許法第１１２条第６段落の規定によって解釈されるべきではない。更に、本開示における要素、コンポーネント又は方法のステップは、要素、コンポーネント又は方法のステップが請求項に明示的に記載されているかどうかに関わらず、公衆に献呈されることを意図していない。

【０１１７】

本開示の範囲内の実施形態は、機械実行可能命令又はそれに記憶されているデータ構造を伝達する又は有する機械可読記憶媒体を含むプログラム製品を含む。このような機械可読媒体は、汎用又は専用コンピュータ又はプロセッサを有する他の機械によりアクセスされ得る任意の利用可能な媒体であり得る。例えば、このような機械可読媒体は、ＲＡＭ、ＲＯＭ、ＥＰＲＯＭ、ＥＥＰＲＯＭ、ＣＤＲＯＭ若しくは他の光学ディスク記憶装置、磁気ディスク記憶装置若しくは他の磁気記憶装置、又は機械実行可能命令若しくはデータ構造の形態にある所望のプログラムコードを伝達若しくは記憶するために使用され得る且つ汎用若しくは専用コンピュータ又はプロセッサを有する他の機械によりアクセスされ得る任意の他の媒体を含み得る。上記の組み合わせも機械可読媒体の範囲内に含まれる。機械実行可能命令は、例えば、汎用コンピュータ、専用コンピュータ、又は専用処理機械に所定の機能又は一群の機能を実行させる命令及びデータを含む。コンピュータ又は機械可読記憶媒体は伝播される信号ではないが（即ち、有形であり非一時的である）、コンピュータ又は機械可読記憶媒体は、人工生成の伝播された信号に符号化されるコンピュータプログラム命令の発信源又は目的地であり得る。

【０１１８】

本開示の実施形態は、例えば、ネットワーク化環境における機械により実行されるプログラムモジュールの形態のプログラムコード等、一実施形態では機械実行可能命令を含むプログラム製品により実装され得る方法のステップの一般的な文脈で記載されている。一般に、プログラムモジュールは、特定のタスクを行う又は特定の抽象データ型を実装するルーチン、プログラム、オブジェクト、コンポーネント、データ構造等を含む。機械実行可能命令、関連データ構造、及びプログラムモジュールは、本明細書に開示の方法のステップを実行するためのプログラムコードの例を表す。このような実行可能命令又は関連データ構造の特定の順序は、このようなステップに記載された機能を実装するための対応す

る動作の例を表す。

【０１１９】

本開示の実施形態は、プロセッサを有する１つ以上のリモートコンピュータへの論理接続を使用してネットワーク化環境で実施されてもよい。論理接続は、限定ではなく例としてここに提示されるローカルエリアネットワーク（ＬＡＮ）及びワイドエリアネットワーク（ＷＡＮ）を含んでもよい。このようなネットワーク環境は、オフィス規模又は企業規模のコンピュータネットワーク、イントラネット及びインターネットでは一般的であり、広範な異なる通信プロトコルを使用してもよい。当業者であれば、このようなネットワークコンピュータ環境が、典型的には、パーソナルコンピュータ、ハンドヘルド装置、携帯電話、マルチプロセッサシステム、マイクロプロセッサに基づく又はプログラム可能消費者家電製品、ネットワークＰＣ、サーバ、ミニコンピュータ、メインフレームコンピュータ等を含む多くのタイプのコンピュータシステムを包含することを理解するであろう。また、本開示の実施形態は、通信ネットワークを介して（配線リンク、無線リンクにより、又は配線若しくは無線リンクの組み合わせにより）結び付けられるローカル及びリモート装置によりタスクが行われる分散コンピュータ環境で実施されてもよい。分散コンピュータ環境では、プログラムモジュールは、ローカル及びリモートメモリ記憶装置の両方に設置されてもよい。

【０１２０】

本開示の一部又はシステム全体を実装するための例示のシステムは、処理装置、システムメモリ、及びシステムメモリから処理装置を含む様々なシステムコンポーネントを結合するシステムバスを含むコンピュータの形態の汎用コンピュータ装置を含んでもよい。システムメモリは、リード・オンリー・メモリ（ＲＯＭ）及びランダム・アクセス・メモリ（ＲＡＭ）を含んでもよい。また、コンピュータは、磁気ハードディスクへの読み書きを行う磁気ハードディスクドライブ、リムーバブル磁気ディスクへの読み書きを行う磁気ディスクドライブ、及びＣＤＲＯＭ又は他の光学媒体等のリムーバブル光学ディスクへの読み書きを行う光学ディスクドライブを含んでもよい。ドライブ及び関連する機械可読媒体は、機械実行可能命令、データ構造、プログラムモジュール、及びコンピュータに関する他のデータの不揮発性記憶を提供する。

【０１２１】

本明細書に提供されるフローチャートは方法のステップの特定の順番を示しているが、こうしたステップの順番は記載のものとは異なってもよいことが理解される。また、２つ以上のステップが同時に又は一部同時に行われてもよい。このような変化は、選択されたソフトウェア及びハードウェアシステムに及び設計者の選択に依存してもよい。全てのこのような変形が本開示の範囲内であることが理解される。同様に、本開示のソフトウェア及びウェブの実装が、様々なデータベース検索ステップ、相関ステップ、比較ステップ及び決定ステップを達成するためのルールベース論理及び他の論理を有する標準プログラミング技術によって達成され得る。また、本明細書及び請求項に用いられる「コンポーネント」という単語は、ソフトウェアコードの１つ以上のライン、及び／又はハードウェア実装、及び／又は手動入力を受け取るための設備を使用する実装を包含することが意図されることに留意されたい。

【０１２２】

本開示の実施形態の先の記載は、例示及び説明の目的で提示されている。網羅的であること又は本開示を開示の厳密な形態に限定することは意図されておらず、上記の教示に照らして修正及び変形が可能であり、又は本開示の実施から獲得されてもよい。実施形態は、当業者が、考えられる特定の用途に適合される様々な修正と共に及び様々な実施形態において本開示を利用できるように、本開示の原理及びその実施の応用を説明するために選択され且つ記載されている。

【図１】

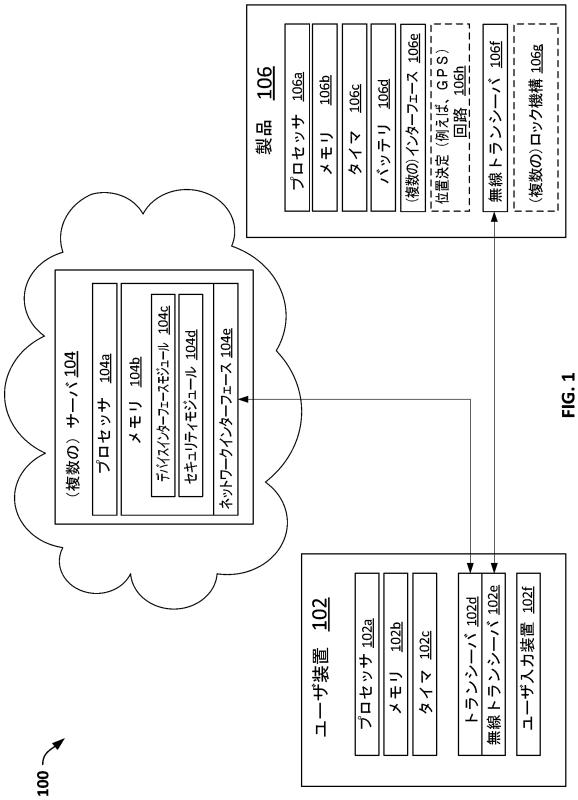

FIG. 1

【図１Ｂ】

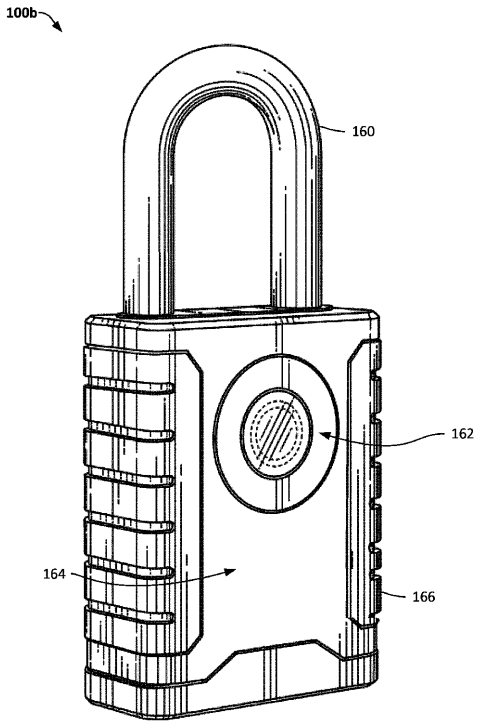

FIG. 1B

【図２】

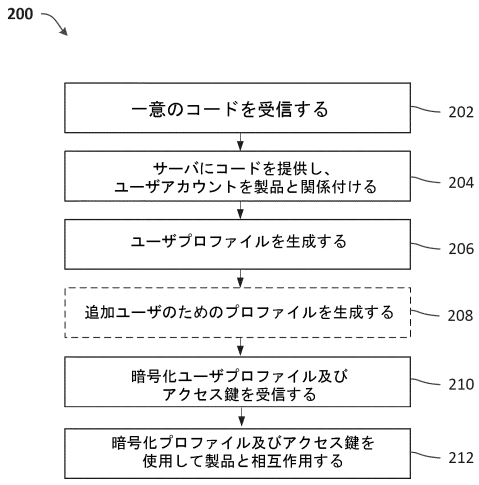

FIG. 2

【図３】

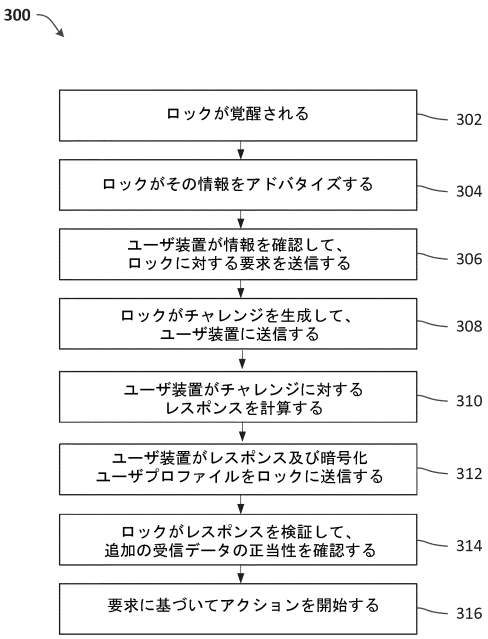

FIG. 3

【図４】

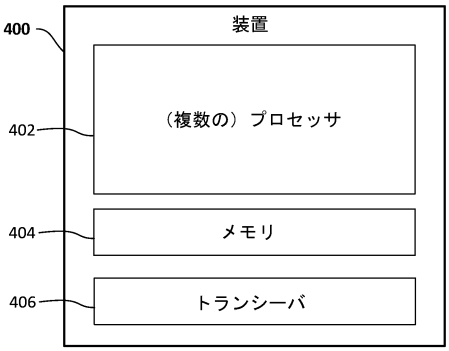

FIG. 4

【図５】

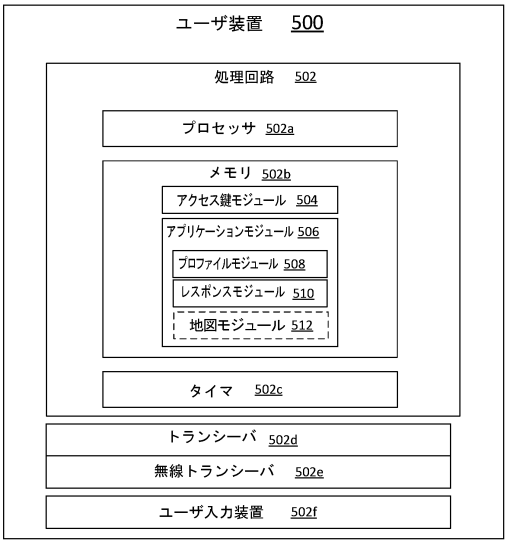

FIG. 5

【図６】

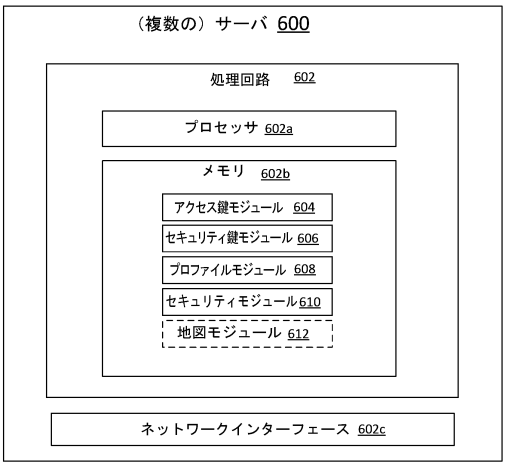

FIG. 6

【図７】

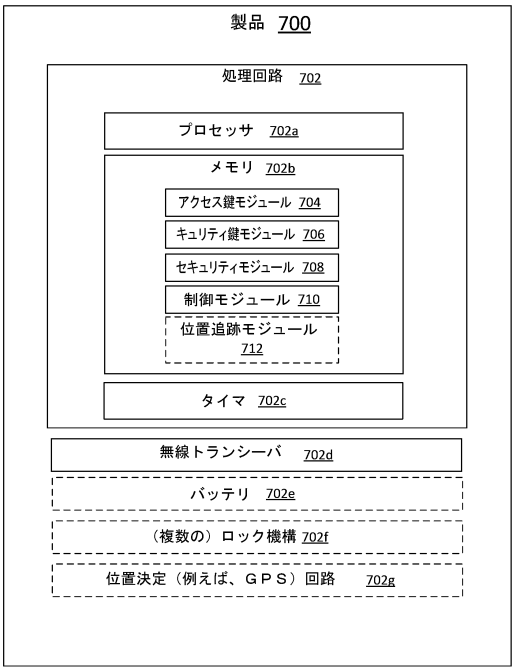

FIG. 7

【図８】

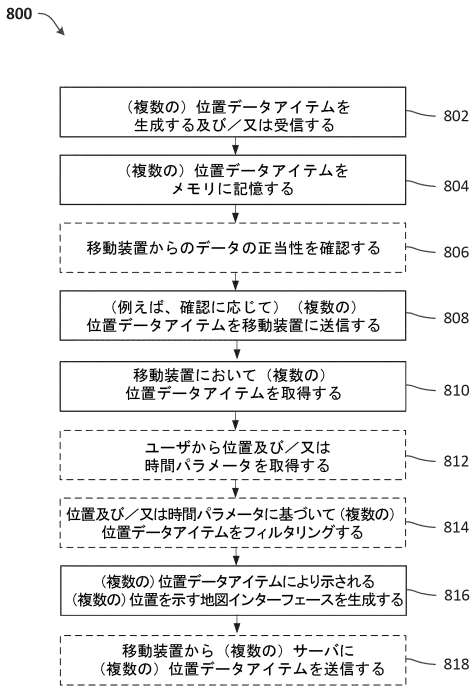

FIG. 8

【図９】

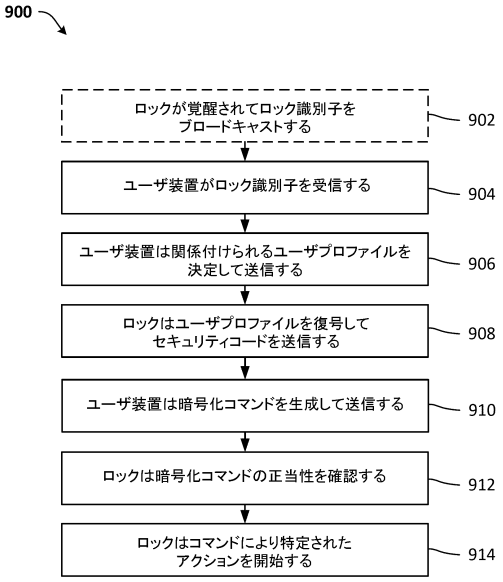

FIG. 9

【図１０】

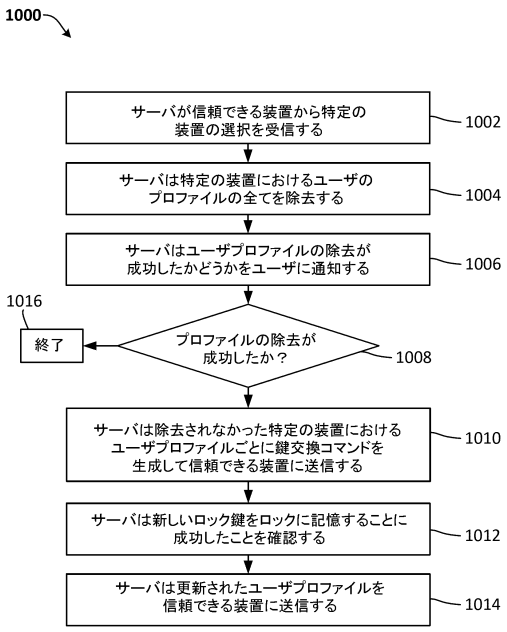

FIG. 10

【図１１】

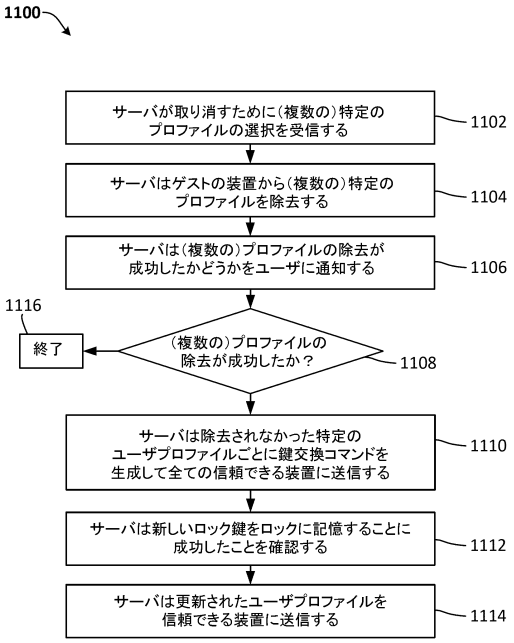

FIG. 11

【図１２】

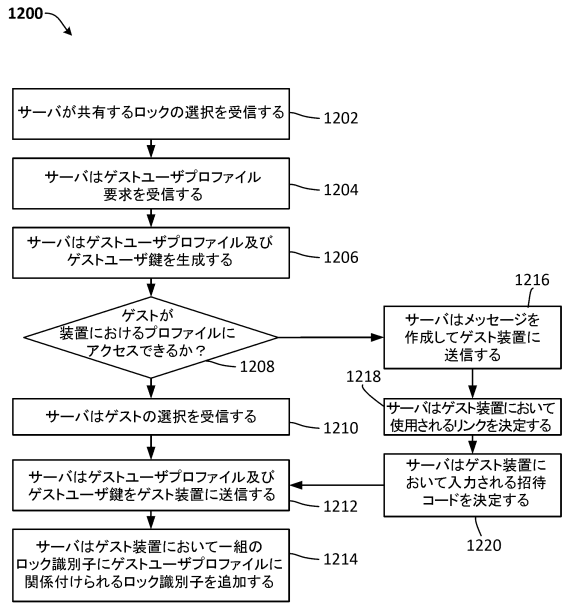

FIG. 12

【図１３】

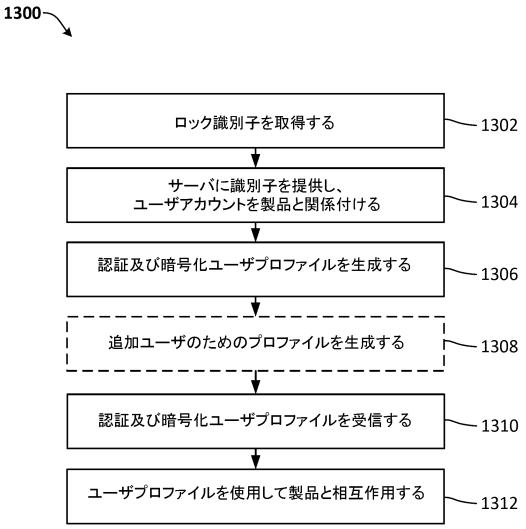

FIG. 13

【図１４】

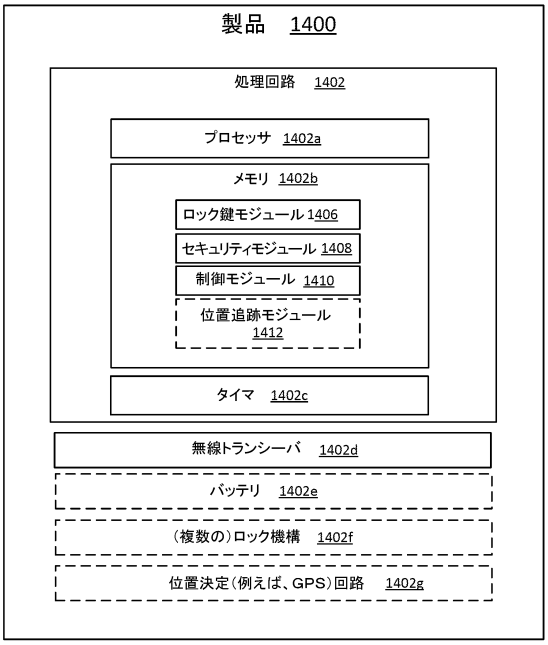

FIG. 14

【図１５Ａ】

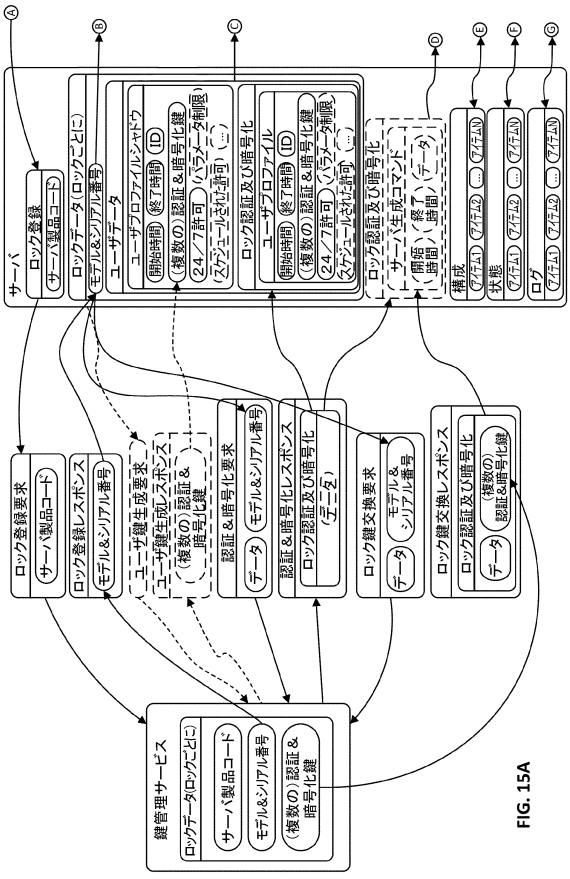

FIG. 15A

【図１５Ｂ】

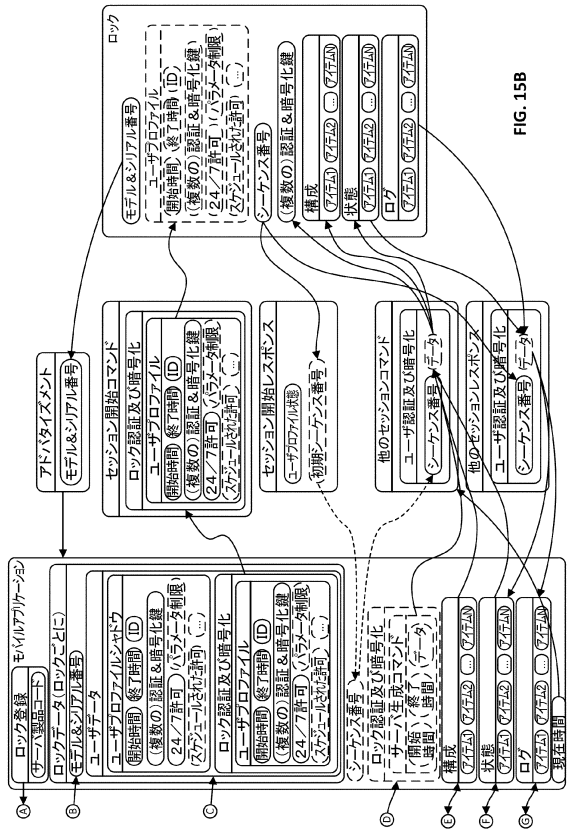
ロック
モデル&シリアル番号
ユーザプロファイル
(開始時間) (終了時間) (ID)
(複数の) 認証&暗号化鍵
(24ノア許可) (パラメータ制限)
(スケジュールされた許可) (...)
シーケンス番号
(複数の) 認証&暗号化鍵
構成
(アイテム) (アイテム) (...) (アイテム)
状態
(アイテム) (アイテム) (...) (アイテム)
ログ
(アイテム) (アイテム) (...) (アイテム)
アドバタイズメント
モデル&シリアル番号
セッション開始コマンド
ロック認証及び暗号化
ユーザプロファイル
(開始時間) (終了時間) (ID)
(複数の) 認証&暗号化鍵
(24ノア許可) (パラメータ制限)
(スケジュールされた許可) (...)
セッション開始レスポンス
ユーザプロファイル状態
初期シーケンス番号
他のセッションコマンド
ユーザ認証及び暗号化
シーケンス番号
データ
他のセッションレスポンス
ユーザ認証及び暗号化
シーケンス番号
データ
モバイルアプリケーション
ロック登録
サーバ識別コード
ロックデータ(ロックごとに)
モデル&シリアル番号
ユーザデータ
ユーザプロファイルシャドウ
(開始時間) (終了時間) (ID)
(複数の) 認証&暗号化鍵
(24ノア許可) (パラメータ制限)
(スケジュールされた許可) (...)
ロック認証及び暗号化
ユーザプロファイル
(開始時間) (終了時間) (ID)
(複数の) 認証&暗号化鍵
(24ノア許可) (パラメータ制限)
(スケジュールされた許可) (...)
シーケンス番号
ロック認証及び暗号化
サーバ生成コマンド
(開始) (終了) (データ)
(時間) (時間)
構成
(アイテム) (アイテム) (...) (アイテム)
状態
(アイテム) (アイテム) (...) (アイテム)
ログ
(アイテム) (アイテム) (...) (アイテム)
現在時間
Ⓐ
Ⓑ
Ⓒ
Ⓓ
Ⓔ
Ⓕ
Ⓖ

FIG. 15B

フロントページの続き

(72)発明者 コンラッド、 ネイサン
アメリカ合衆国 ５３１５４ ウィスコンシン州 オーククリーク ウェスト フォレスト ヒル アベニュー １３７ マスター ロック カンパニー エルエルシー 気付
(72)発明者 チャン、 イ
アメリカ合衆国 ５３１５４ ウィスコンシン州 オーククリーク イースト ビレッジ グリーン コート ７３２
(72)発明者 ステファノビック、 ネマーニャ
アメリカ合衆国 ５３１５４ ウィスコンシン州 オーククリーク ウェスト フォレスト ヒル アベニュー １３７ マスター ロック カンパニー エルエルシー 気付
(72)発明者 バルトゥッチ、 ジョン
アメリカ合衆国 ６００１２ イリノイ州 クリスタルレイク タリスモン ドライブ ８０
(72)発明者 カロウス、 スコット
アメリカ合衆国 ５３１４２ ウィスコンシン州 ケノーシャ ９１スト アベニュー ６１０５

審査官 青木 重徳

(56)参考文献 特表２００８－５１１９２６（ＪＰ，Ａ）
欧州特許出願公開第２７２２８０３（ＥＰ，Ａ１）
米国特許出願公開第２０１２／０２２２１０３（ＵＳ，Ａ１）
米国特許出願公開第２０１２／０２８０７９０（ＵＳ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ ９／３２
Ｇ０６Ｆ ２１／３３
Ｇ０９Ｃ １／００