【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】平成30年9月6日(2018.9.6)

【公表番号】特表2017-524301(P2017-524301A)
【公表日】平成29年8月24日(2017.8.24)
【年通号数】公開・登録公報2017-032
【出願番号】特願2017-504163(P2017-504163)
【国際特許分類】
*Ｈ０４Ｌ　9/32　(2006.01)*
*Ｇ０９Ｃ　1/00　(2006.01)*
*Ｇ０６Ｆ　21/33　(2013.01)*
【ＦＩ】
Ｈ０４Ｌ　9/00　６７５Ａ
Ｇ０９Ｃ　1/00　６４０Ｅ
Ｇ０６Ｆ　21/33

【手続補正書】
【提出日】平成30年7月26日(2018.7.26)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【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。