

(19) 日本国特許庁(JP)

(12) 公表特許公報(A)

(11) 特許出願公表番号

特表2017-522467
(P2017-522467A)

(43) 公表日 平成29年8月10日(2017.8.10)

(51) Int.Cl. F I テーマコード(参考)
E O 5 B 49/00 (2006.01) E O 5 B 49/00 K 2 E 2 5 O

審査請求 未請求 予備審査請求 未請求 (全 24 頁)

(21) 出願番号 特願2016-566608 (P2016-566608)
(86) (22) 出願日 平成27年6月18日 (2015. 6. 18)
(85) 翻訳文提出日 平成28年12月28日 (2016. 12. 28)
(86) 国際出願番号 PCT/EP2015/001233
(87) 国際公開番号 W02015/197179
(87) 国際公開日 平成27年12月30日 (2015. 12. 30)
(31) 優先権主張番号 00951/14
(32) 優先日 平成26年6月23日 (2014. 6. 23)
(33) 優先権主張国 スイス(CH)

(71) 出願人 503300339
レジック・アイデントシステムズ・アクチ
エンゲゼルシャフト
スイス, シーエイチー8620 ベツィ
コン, ビンザッカーシュトラッセ 41
(74) 代理人 100107456
弁理士 池田 成人
(74) 代理人 100162352
弁理士 酒巻 順一郎
(74) 代理人 100123995
弁理士 野田 雅一
(74) 代理人 100148596
弁理士 山口 和弘

最終頁に続く

(54) 【発明の名称】 電子アクセス制御デバイス及びアクセス制御方法

(57) 【要約】

電子アクセス制御デバイス(1)は、直接ワイヤレス通信リンク(3)を介して移動デバイス(2)と第1の無線周波数帯域でワイヤレスデータ交換を実行するための無線通信モジュール(11)を備える。アクセス制御デバイスは、移動デバイスから受信したアクセスキーを使用してアクセス制御信号を発生するためワイヤレス無線通信モジュールに接続されたコントローラ(12)を有する。電子アクセス制御デバイスは、第1の無線周波数帯域とは異なる第2の無線周波数帯域の無線周波数を使用して、規定の近さ(P)の移動デバイスを検出するための近接検出装置(13)をさらに備える。コントローラは、近接検出装置に接続され、移動デバイスが電子アクセス制御デバイスの規定の近さに検出される場合にだけ、無線通信モジュールを制御して移動デバイスとの直接ワイヤレス通信リンクを確立する。

【選択図】 図1

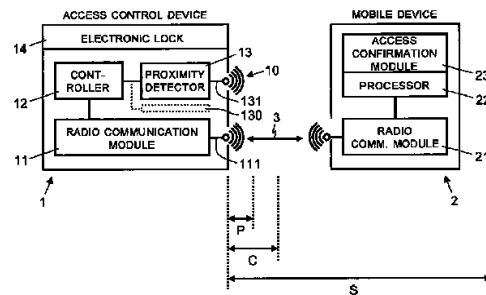


Fig. 1

【特許請求の範囲】**【請求項 1】**

無線通信モジュール(11)と移動デバイス(2)との間の直接ワイヤレス通信リンク(3)を介して前記移動デバイス(2)と第1の無線周波数帯域でワイヤレスデータ交換を実行するように構成されている無線通信モジュール(11)と、

前記ワイヤレス無線通信モジュール(11)に接続され、前記移動デバイス(2)から前記直接ワイヤレス通信リンク(3)を介して前記無線通信モジュール(11)によって受信されたアクセスキーを使用してアクセス制御信号を発生するように構成されているコントローラ(12)と

を備える、電子アクセス制御デバイス(1)であって、

前記電子アクセス制御デバイス(1)が、前記第1の無線周波数帯域とは異なる第2の無線周波数帯域の無線周波数を使用して前記電子アクセス制御デバイス(1)の規定の近さ(P)の前記移動デバイス(2)の存在を検出するように構成されている近接検出装置(13)をさらに備え、

前記コントローラ(12)は、前記近接検出装置(13)に接続され、且つ前記移動デバイス(2)が前記無線通信モジュール(11)へ前記アクセスキーを送信することを可能にするために、前記電子アクセス制御デバイス(1)の前記規定の近さ(P)に前記近接検出装置(13)によって前記移動デバイス(2)を検出したとき、前記無線通信モジュール(11)を制御して、前記移動デバイス(2)との前記直接ワイヤレス通信リンク(3)を確立するようにさらに構成されている、

電子アクセス制御デバイス(1)。

【請求項 2】

前記無線通信モジュール(11)が、数メートルの、特に10メートルまでの距離にわたる近距離(S)通信リンク(3)を介して前記移動デバイス(2)と前記ワイヤレスデータ交換を実行するように構成されており、前記近接検出装置(13)が、数センチメートルの、特に10センチメートルまでの距離内に前記電子アクセス制御デバイス(1)にごく近接(P)する前記移動デバイス(2)の前記存在を検出するように構成されている、請求項1に記載の電子アクセス制御デバイス(1)。

【請求項 3】

前記近接検出装置(13)が、RFIDリーダを備え、電磁場パルス(10)を放出し、前記電磁場パルス(10)の放出中に戻り信号を検出し、前記戻り信号を使用して前記移動デバイス(2)の前記存在を検出することによって、前記移動デバイス(2)の前記存在を検出するように構成されている、請求項1又は2に記載の電子アクセス制御デバイス(1)。

【請求項 4】

前記無線通信モジュール(11)が、Bluetoothトランシーバを備え、前記コントローラ(12)が、前記Bluetoothトランシーバを制御して、Bluetooth接続プロセスを実行することによって前記移動デバイス(2)との前記直接ワイヤレス通信リンク(3)を確立するようにさらに構成されている、請求項1～3のいずれか一項に記載の電子アクセス制御デバイス(1)。

【請求項 5】

前記コントローラ(12)が、前記Bluetoothトランシーバを制御して、スレープとしてBluetoothペリフェラルモードで動作している前記移動デバイス(2)との前記直接ワイヤレス通信リンク(3)を確立するためのマスタとしてBluetoothセントラルモードで動作するように、且つ応答に失敗したとき、前記Bluetoothトランシーバを制御して、前記マスタとして前記Bluetoothセントラルモードで動作している前記移動デバイス(2)により確立された前記直接ワイヤレス通信リンク(3)を有するためのスレープとして前記Bluetoothペリフェラルモードで動作するようにさらに構成されている、請求項4に記載の電子アクセス制御デバイス(1)。

10

20

30

40

50

【請求項 6】

前記無線通信モジュール(11)が、Bluetooth Low Energy トラシーバを備える、請求項 4 又は 5 に記載の電子アクセス制御デバイス(1)。

【請求項 7】

前記コントローラ(12)が、前記無線通信モジュール(11)を制御して、実行可能なアクセス確認モジュール(23)を前記移動デバイス(2)へ送信するようにさらに構成されており、前記実行可能なアクセス確認モジュール(23)が、前記移動デバイス(2)のプロセッサ(22)を制御して、確認命令を前記移動デバイス(2)のユーザから受信し前記確認命令に応じて確認メッセージを前記アクセス制御デバイス(1)の前記無線通信モジュール(11)へ送信するように、前記移動デバイス(2)から前記確認メッセージを受信するように、且つ前記確認メッセージをさらに使用して前記アクセス制御信号を発生するように構成されている、請求項 1 ~ 6 のいずれか一項に記載の電子アクセス制御デバイス(1)。

10

【請求項 8】

前記実行可能なアクセス確認モジュール(23)が、前記移動デバイス(2)の前記プロセッサ(22)を制御して、前記移動デバイス(2)の指紋センサ及び前記移動デバイス(2)のグラフィカルユーザインターフェースのうち少なくとも一方を介して前記移動デバイス(2)の前記ユーザから前記確認命令を受信するようにさらに構成されている、請求項 7 に記載の電子アクセス制御デバイス(1)。

20

【請求項 9】

前記実行可能なアクセス確認モジュール(23)が、前記移動デバイス(2)の前記プロセッサ(22)を制御して、前記確認メッセージに前記アクセスキーを含ませるようにさらに構成され、前記コントローラ(12)が、前記アクセス制御信号を発生するために前記確認メッセージから前記アクセスキーを得るようにさらに構成されている、請求項 7 又は 8 に記載の電子アクセス制御デバイス(1)。

【請求項 10】

前記コントローラ(12)は、前記無線通信モジュール(11)を制御して、前記無線通信モジュール(11)の受信信号強度が 1 メートルの前記アクセス制御デバイス(1)からの前記移動デバイス(2)の最大距離(C)を示す規定のしきい値を満足する場合にだけ、前記実行可能なアクセス確認モジュール(23)を前記移動デバイス(2)へ送信するように、且つ前記確認メッセージの前記受信信号強度に拘わらず前記アクセス制御信号を発生するようにさらに構成されている、請求項 7 ~ 9 のいずれか一項に記載の電子アクセス制御デバイス(1)。

30

【請求項 11】

前記アクセス制御デバイス(1)が、電子錠(14)をさらに備え、前記コントローラ(12)が、前記電子錠(14)に接続されており、前記電子錠(14)を制御するため前記電子錠(14)へ前記アクセス制御信号を供給して、解錠機能を実行するようにさらに構成されている、請求項 1 ~ 10 のいずれか一項に記載の電子アクセス制御デバイス(1)。

【請求項 12】

前記コントローラ(12)が、前記アクセス制御信号を反映しているアクセスステータスを規定するように、且つ前記無線通信モジュール(11)を制御して、前記移動デバイス(2)へ前記アクセスステータスを送信するようにさらに構成されている、請求項 1 ~ 11 のいずれか一項に記載の電子アクセス制御デバイス(1)。

40

【請求項 13】

第 2 の無線周波数帯域の無線周波数を使用して電子アクセス制御デバイス(1)の規定の近さ(P)の移動デバイス(2)の存在を前記電子アクセス制御デバイス(1)の近接検出装置(13)によって検出するステップ(S1)と、

前記電子アクセス制御デバイス(1)の前記規定の近さ(P)に前記近接検出装置(13)によって前記移動デバイス(2)を検出したとき、前記電子アクセス制御デバイス(

50

1)の無線通信モジュール(11)を制御して、前記第2の無線周波数帯域とは異なる第1の無線周波数帯域でワイヤレスデータ交換のための直接ワイヤレス通信リンク(3)を前記移動デバイス(2)と確立するステップ(S2)と、

前記直接ワイヤレス通信リンク(3)を介して前記移動デバイス(2)からアクセスキーを前記電子アクセス制御デバイス(1)の前記無線通信モジュール(11)によって受信するステップ(S3)と、

前記移動デバイス(2)から受信した前記アクセスキーを使用してアクセス制御信号を前記電子アクセス制御デバイス(1)において発生するステップ(S5)とを含む、アクセス制御方法。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、電子アクセス制御デバイス及びアクセス制御方法に関する。詳細には、本発明は、移動デバイスとの直接ワイヤレスデータ交換のための無線通信モジュールを備えている電子アクセス制御デバイス、及び移動デバイスから受信したアクセスキーを使用してアクセス制御信号を発生するためのワイヤレス無線通信モジュールに接続されているコントローラに関する。

【背景技術】

【0002】

長年にわたって、アクセス制御システムは、受動RFIDトランスポンダ(無線周波数識別子(Radio Frequency Identifier))に関連して使用されてきている。これらのアクセス制御システムは、ビルディング又は部屋などのアクセスを制御されている領域、又は自動販売機の商品などのアクセスを制御された物品、等へのアクセスを制御するために、RFIDトランスポンダからのアクセス権又は少なくともユーザ識別子をワイヤレス方式で読み取るためのRFIDリーダを含んでいた。能動RFIDベースの通信インターフェース、いわゆるNFCインターフェース(近距離無線通信(Near Field Communication))を含んでいる携帯無線電話機(セルラフォン)の到来で、RFIDカード、 dongle、等の形態の受動RFIDトランスポンダよりはむしろ、アクセス権のキャリアとしてこのような携帯電話機を使用することが可能になってきている。NFCインターフェースを用いると、例えば、ドア又は門に取り付けられている又は近くのアクセス制御デバイスの対応するNFCインターフェースの近くの領域の携帯電話機の物理的な存在にアクセス制御を結び付けることが可能である。言い換えると、NFCインターフェースの短い通信範囲は、ユーザの携帯電話機がアクセスしようとしているドア又は門から遠い距離にあってはならないことを必要とし、携帯電話機が正当なユーザに所有されている限り、正当なユーザの携帯電話機に記憶されているアクセス権に基づいて、無許可の人間が誤って所与のアクセスを行うことを起き難くさせている。しかしながら、すべてのタイプ及びブランドの携帯電話機が、NFCインターフェース又は他のRFIDベースの通信能力を備えているわけではない。それにも拘らず、GSM(登録商標。以下同じ)(グローバルシステムフォーモバイルコミュニケーション(Global System for Mobile Communication))又はUMTS(ユニバーサル携帯電話システム(Universal Mobile Telephone System))などのセルラ電話ネットワークにアクセスするために使用されている移動無線通信モジュールに加えて、携帯電話機のうちのいくつかのタイプ及びブランドは、ローカルワイヤレス通信リンク又は直接ワイヤレス通信リンクを確立するための他の無線ベースの通信モジュールを含んでいる。例えば、このような無線ベースの通信モジュールは、WLAN(ワイヤレスローカルエリアネットワーク(Wireless Local Area Network))及び、例えば、10~100メートルのNFCインターフェースよりもはるかに大きい通信範囲を有しているBluetooth(登録商標。以下同様)通信インターフェースを含んでいる。このような他の無線に基づく通信モジュールがアクセス制御デバイスとアクセス権を交換するために使用され

10

20

30

40

50

てもよいが、正当なユーザ又は少なくともそのユーザの携帯電話がアクセス制御デバイスの拡張した通信範囲内に位置するという理由だけで、許可されていないユーザが誤ってアクセスすることがあるというリスクがある。

【0003】

FR2981823は、自動車始動動作を実行するために自動車に組み込まれているアクチュエータデバイスに関する識別デバイスを認証するために方法を記載している。認証セッションでは、識別デバイスは、識別デバイスとアクチュエータデバイスとの間で認証データを交換することによって認証されている。認証セッション中には、交換認証データの第1の部分が、Bluetoothを使用して通信され、一方で認証データの第2の部分が、磁気誘導を介して交換される。アクチュエータでは、認証データの2つの部分が、10

【0004】

米国特許出願公開第2012/154115号は、位置追跡システムにおけるアクセスを制御するための方法を記載している。移動タグが部屋に入ると、移動タグは、位置更新手続きを実行し、位置追跡システムのノードにリンクされるようになり、室内でそれ自体の位置を更新している。位置更新に応じて、位置追跡システムの位置追跡装置は、室内のアクセス制御デバイスへ起動信号を送信して、移動タグのアクセス権について取り決めるため移動タグとの通信接続の確立を開始している。ある実施形態では、アクセス制御デバイスは、近接センサを備えることができ、近接センサは、アクセス権の取り決めに続いて、アクセス制御デバイスが実際にアクセスを承認する又は拒否する前に、移動タグのごく近接を検出している。20

【0005】

米国特許出願公開第2014/049361号は、電子錠に関係するリーダデバイスと通信している移動デバイスを含んでいる電子システムを記載している。移動デバイス及びリーダデバイスは、例えば、Bluetoothを介して相互に通信し、クレデンシャル、安全なデータ、及び位置情報を交換している。ある実施形態では、電子錠は、適切なクレデンシャルを有する移動デバイスがごく近接範囲内であるときに電子錠を自動的に解錠するごく近接範囲能力をやはり含むことができる。

【発明の概要】

【0006】

先行技術の欠点のうちの少なくともいくつかを持たない電子アクセス制御デバイス及びアクセス制御方法を提供することが、この発明の目的である。特に、NFCインターフェースを有する移動デバイスに限定されないだけでなく、NFCベースのアクセス制御の長所のうちの少なくともいくつかをそれにも拘らず共有する電子アクセス制御デバイス及びアクセス制御方法を提供することが、本発明の目的である。30

【0007】

本発明によれば、これらの目的は、独立請求項の特徴を介して達成される。加えて、さらに有利な実施形態は、従属請求項及び明細書に従う。

【0008】

電子アクセス制御デバイスは、無線通信モジュールと、ワイヤレス無線通信モジュールに接続されているコントローラとを備えている。無線通信モジュールは、無線通信モジュールと移動デバイスとの間の直接ワイヤレス通信リンクを介して移動デバイスと第1の無線周波数帯域でワイヤレスデータ交換を実行するように構成されている。コントローラは、移動デバイスから直接ワイヤレス通信リンクを介して無線通信モジュールによって受信されたアクセスキーを使用してアクセス制御信号を発生するように構成されている。40

【0009】

本発明によれば、上に述べた目的は、電子アクセス制御デバイスが、近接検出装置をさらに備えていることで特に達成される。近接検出装置は、第1の無線周波数帯域とは異なる第2の無線周波数帯域の無線周波数を使用して電子アクセス制御デバイスの規定の近さの移動デバイスの存在を検出するように構成されている。コントローラは、近接検出装置50

に接続され、電子アクセス制御デバイスの規定の近さに近接検出装置によって移動デバイスを検出したとき、無線通信モジュールを制御して、移動デバイスとの直接ワイヤレス通信リンクを確立するようにさらに構成されている。

【0010】

アクセス制御デバイスの規定の近さに移動デバイスの存在を検出することは、移動デバイスがその規定の近さ内に実際に位置するという条件にアクセスを限定することを可能にしている。従って、移動デバイスのタイプ又はブランド及び移動デバイスがサポートする無線通信モジュールの種類に拘わらず、ユーザは、(認証されたアクセスキーが移動デバイスに記憶されていることが与えられると)アクセスするためにアクセス制御デバイスの規定の近さに移動デバイスを置くことを常に要求されるであろう。

10

【0011】

ある実施形態では、無線通信モジュールは、数メートルの、特に10メートルまでの距離にわたる近距離通信リンクを介して移動デバイスとワイヤレスデータ交換を実行するように構成されている。近接検出装置は、数センチメートルの、特に10センチメートルまでの距離内で電子アクセス制御デバイスにごく近接する移動デバイスの存在を検出するように構成されている。

【0012】

さらなる実施形態では、近接検出装置は、RFIDリーダを備えており、電磁場パルスを放出し、電磁場パルスの放出中に戻り信号を検出し、戻り信号を使用して移動デバイスの存在を検出することによって、移動デバイスの存在を検出するように構成されている。従って、近接検出装置は、電磁場内の移動デバイスの物理的な存在によって引き起こされる電磁場の変化に単に基づいて移動デバイスの存在を検出するように構成されている - 移動デバイスは、その目的のために何らかの対応する通信構成を装備する必要がない。

20

【0013】

ある実施形態では、無線通信モジュールは、Bluetoothトランシーバを備えており、コントローラは、Bluetoothトランシーバを制御して、Bluetooth接続プロセスを実行することによって、移動デバイスとの直接ワイヤレス通信リンクを確立するようにさらに構成されている。例えば、無線通信モジュールは、Bluetooth Low Energyトランシーバを備えている。

【0014】

別の実施形態では、コントローラは、Bluetoothトランシーバを制御して、スレーブとしてBluetoothペリフェラルモードで動作している移動デバイスとの直接ワイヤレス通信リンクを確立するためのマスタとしてBluetoothセントラルモードで動作させるように、且つ応答に失敗したとき、Bluetoothトランシーバを制御して、マスタとしてBluetoothセントラルモードで動作している移動デバイスにより確立された直接ワイヤレス通信リンクを有するためのスレーブとしてBluetoothペリフェラルモードで動作させるようにさらに構成されている。

30

【0015】

さらなる実施形態では、コントローラは、無線通信モジュールを制御して、実行可能なアクセス確認モジュールを移動デバイスへ送信するようにさらに構成されている。実行可能なアクセス確認モジュールは、移動デバイスのプロセッサを制御して、確認命令を移動デバイスのユーザから受信し、確認命令に応じて確認メッセージをアクセス制御デバイスの無線通信モジュールへ送信するように構成されている。コントローラは、移動デバイスから確認メッセージを受信するように、且つ確認メッセージをさらに使用してアクセス制御信号を発生するようにさらに構成されている。

40

【0016】

ある実施形態では、実行可能なアクセス確認モジュールは、移動デバイスのプロセッサを制御して、移動デバイスの指紋センサ及び/又は移動デバイスのグラフィカルユーザインターフェースを介して移動デバイスのユーザから確認命令を受信するようにさらに構成されている。

50

【0017】

さらなる実施形態では、実行可能なアクセス確認モジュールは、移動デバイスのプロセッサを制御して、確認メッセージにアクセスキーを含ませるようにさらに構成されており、コントローラは、アクセス制御信号を発生させるため確認メッセージからアクセスキーを得るようにさらに構成されている。

【0018】

別の一実施形態では、コントローラは、無線通信モジュールを制御して、無線通信モジュールの受信信号強度が1メートルのアクセス制御デバイスからの移動デバイスの最大距離を示す規定のしきい値を満足する及び/又は超える場合にだけ、実行可能なアクセス確認モジュールを移動デバイスへ送信するように、且つ確認メッセージの受信信号強度に拘わらずアクセス制御信号を発生するようにさらに構成されている。

10

【0019】

ある実施形態では、コントローラは、無線通信モジュールを制御して、電子アクセス制御デバイスの規定の近さ内に近接検出装置による移動デバイスを検出したとき、及び無線通信モジュールによって示された(ような移動デバイスの)受信信号強度が、アクセス制御デバイスからの移動デバイスの規定の最大距離、例えば、0.5又は1メートルの規定の最大距離を示す規定のしきい値を満足することを検証したときのみ、移動デバイスとの直接ワイヤレス通信リンクを確立するように構成されている。これは、移動デバイスがアクセス制御デバイスに実際に近い、すなわちアクセス制御デバイスからの最大距離内であることを検証されることで、ユーザがもう1つの対象を使用して近接検出装置をトリガする場合において、セキュリティを維持することを可能にする。

20

【0020】

ある実施形態では、アクセス制御デバイスは、電子錠をさらに備えており、コントローラは、電子錠に接続されており、電子錠を制御するため電子錠へアクセス制御信号を供給して、解錠機能を実行するように、例えば、ドア又は門などの入口を解錠するようにさらに構成されている。

【0021】

別の一実施形態では、コントローラは、アクセス制御信号を反映しているアクセスステータスを規定するように、且つ無線通信モジュールを制御して、移動デバイスへアクセスステータスを送信するようにさらに構成されている。

30

【0022】

電子アクセス制御デバイスに加えて、本発明は、アクセス制御方法にもやはり関する。アクセス制御方法は、第2の無線周波数帯域の無線周波数を使用して、電子アクセス制御デバイスの規定の近さの移動デバイスの存在を電子アクセス制御デバイスの近接検出装置によって検出するステップを含む。本方法は、電子アクセス制御デバイスの規定の近さに近接検出装置によって移動デバイスを検出したとき、電子アクセス制御デバイスの無線通信モジュールを制御して、第2の無線周波数帯域とは異なる第1の無線周波数帯域でワイヤレスデータ交換のための直接ワイヤレス通信リンクを移動デバイスと確立するステップを含む。引き続いて、電子アクセス制御デバイスの無線通信モジュールは、直接ワイヤレス通信リンクを介して移動デバイスからアクセスキーを受信し、移動デバイスから受信したアクセスキーを使用してアクセス制御信号を電子アクセス制御デバイスにおいて発生する。

40

【0023】

本発明のさらなる態様は、電子アクセス制御デバイスに関し、無線通信モジュールと移動デバイスとの間の直接ワイヤレス通信リンクを介して移動デバイスとワイヤレスデータ交換を実行するように構成されている無線通信モジュールと;ワイヤレス無線通信モジュールに接続されており、移動デバイスから直接ワイヤレス通信リンクを介して無線通信モジュールによって受信されたアクセスキーを使用してアクセス制御信号を発生するように構成されているコントローラと;容量センサを使用して電子アクセス制御デバイスへの規定の近さにユーザの存在を検出するように構成されている近接検出装置とを備えており、以

50

て、コントローラは、それぞれ、近接検出装置又はその容量センサに接続されており、無線通信モジュールを制御して、電子アクセス制御デバイスの規定の近さに近接検出装置によるユーザを検出したとき、及び無線通信モジュールにより示された受信信号強度が、アクセス制御デバイスからの移動デバイスの規定の最大距離を示す規定のしきい値を満足することを検証したとき、移動デバイスとの直接ワイヤレス通信リンク確立するようにさらに構成されている。例えば、コントローラは、無線通信モジュールを制御して、ユーザが電子アクセス制御デバイスから3又は5センチメートルまでの規定の近さに検出される場合で、且つ移動デバイスの受信信号強度が、無線通信モジュールによって示されているように、アクセス制御デバイスから0.5又は1メートルの移動デバイスの最大距離を示す規定のしきい値以上である場合にだけ、移動デバイスとの直接ワイヤレス通信リンクを確立するように構成されている。例えば、容量センサは、ドアハンドルに接続されている又は近くに配置されており、ユーザの近接は、ユーザがドアハンドルの近くに自身の手を保持すると検出される。

【0024】

本発明は、例として図面を参照して、より詳細に説明されるであろう。

【図面の簡単な説明】

【0025】

【図1】無線通信モジュール及び無線ベースの近接検出装置を有する電子アクセス制御デバイスを概略的に示すブロック図である。

【図2】電子アクセス制御デバイス、アクセス権サーバ、及び移動デバイスを有するアクセス制御システムを概略的に示すブロック図である。

【図3】電子アクセス制御のためのステップの例示的なシーケンスを示す流れ図である。

【図4】電子アクセス制御デバイスと移動デバイスとの間の直接ワイヤレス通信リンクを確立するためのステップの例示的なシーケンスを示す流れ図である。

【図5】移動デバイスから電子アクセス制御デバイスへアクセスキーを送信するためのステップの例示的なシーケンスを示す流れ図である。

【発明を実施するための形態】

【0026】

図1～図5では、参照番号1は、電子アクセス制御デバイスを指している。電子アクセス制御デバイス1は、1つ若しくは複数のバッテリー又はデバイスに接続されている外部電源によって電力を供給される1つ又は複数の回路及びモジュールを備えている。

【0027】

図1の実施形態に概略的に図示されているように、電子アクセス制御デバイス1は、ビルディング、自動車、又は部屋などのアクセスを制御された領域への、ドア、門、等などの入口を施錠し解錠するための電子/電動錠14を備えている。アクセス制御信号に応じて、電子錠14は、1つ又は複数のバー又はボルトを駆動させて、アクセスを制御された領域への入口を施錠する又は解錠する。電子錠14は、共通の筐体又は別々の筐体に電子アクセス制御デバイス1の残りの構成要素とともに実装されている。当業者は、用途に応じて、例えば、自動販売機の品物へのアクセスを制御するために、電子アクセス制御デバイス1又は電子錠14は、それぞれ、それに応じてアクセスを阻止する又は認可するように、例えば、自動販売機を解錠する又は自動販売機に品物を入れる若しくは自動販売機から品物を取り出せるように構成されている。

【0028】

図1に示されているように、電子アクセス制御デバイス1は、無線通信モジュール11、コントローラ12、及び無線ベースの近接検出装置13をさらに備えている。コントローラは、通信モジュール11及び無線ベースの近接検出装置13に電氣的に接続されている。

【0029】

無線通信モジュール11は、無線通信モジュール11と移動デバイス2との間の直接ワイヤレス通信リンク3をわたり、移動デバイス2とのワイヤレスデータ交換を実行するよ

10

20

30

40

50

うに構成されている。「直接」という用語は、直接ワイヤレス通信リンク3が、無線通信モジュール11と移動デバイス2との間に、ルータ、リピータ、ゲートウェイ、有線ネットワーク、基地局、等などの中間の構成要素を含んでいないことを示すためである。無線通信モジュール11は、数メートルの近距離Sをわたり、特に、5、10、又は20メートルまでの距離をわたりワイヤレスデータ交換を実行するように構成されている。ある実施形態では、無線通信モジュール11は、Bluetoothトランシーバ、具体的には、Low Energy Bluetoothトランシーバを備えている。無線通信モジュール11は、(超高周波数(Ultra High Frequency)UHF)マイクロ波を使用して、2.4~2.485GHzの周波数帯域で動作するように構成されている。代替実施形態では、無線通信モジュール11は、IEEE802.11標準に基づき、例えば、2.4GHz~5GHzの周波数帯域で動作するWLAN通信モジュールを備えている。

10

【0030】

コントローラ12は、コンピュータプログラムコードを有するプログラマブルマイクロプロセッサ、フィールドプログラマブルゲートアレイ、特定用途向け集積回路、及び/又は後でより詳細に説明するような様々な機能を実行するように構成されている別の電子回路を備えている。

【0031】

無線に基づいた近接検出装置13は、電子アクセス制御デバイス1の規定の近さPに、具体的には、例えば、アクセス制御デバイス1の感度パラメータを設定することによって調節可能な、5、10、又は15センチメートルまでの距離範囲内にごく近接Pする移動デバイス2の存在を検出するように構成されている。近接検出装置13は、電磁場パルス10を放出することによって、電磁場パルス10の放出中に戻り信号を検出し、戻り信号を使用して移動デバイス2の存在を検出することによって、移動デバイス2の存在を検出するように構成されている。基本的に、近接検出装置13は、移動デバイス2の存在によって引き起こされるような近接検出装置13により放出された電磁場10の変化を検出することによって移動デバイス2の存在を検出するように構成されている。具体的には、近接検出装置13は、アンテナ131が規定の電磁場パルス10を放出している間のアンテナ131での戻り信号を測定し、出願人の名前での欧州特許第1723575号又は欧州特許第2437403号の特許に開示されているような減衰、増幅、及び/又は周波数のシフトを戻り信号において決定しており、特許の全体の内容は、援用によって本明細書中に組み込まれている。ある実施形態では、近接検出装置13は、RFIDリーダ(無線周波数識別子)、例えば、ISO18092、ISO21481、ISO15693、及び/又はISO14443に従ったRFIDリーダを備えている。近接検出装置13は、(高周波数(High Frequency)HF)無線波を使用して、RFIDシステムのキャリア周波数、例えば、6.78MHz、13.56MHz、又は27.12MHz(若しくは13.56MHzの別の高調波)で動作するように構成されている。

20

30

【0032】

従って、無線に基づいた近接検出装置13は、無線通信モジュール11とは異なる、すなわち低い周波数帯域を使用している。図1に明確に示されているように、無線に基づいた近接検出装置13及び無線通信モジュール11は、アクセス制御デバイス1の2つの別個の(無線に基づいた通信)モジュールであり、各々がそれ自体のトランシーバ回路及びそれ自体のアンテナ111、131を持っている。無線に基づいた近接検出装置13及び無線通信モジュール11は、2つの異なり且つ別々の通信ユニットであり、例えば、各々が異なる集積回路(チップ)に実装されており、2つの異なり且つ別々の通信チャネルを有するアクセス制御デバイス2を形成している。

40

【0033】

移動デバイス2は、移動無線電話機(すなわち、セルラフォン)、タブレット若しくはノートブックコンピュータ、コンピュータ型腕時計、又は別の移動通信デバイスとして実装されている。図1に概略的に図示されているように、移動デバイス2は、無線通信モジ

50

ジュール 2 1 及びこれに接続されているプログラマブルプロセッサ 2 2 を備えている。無線通信モジュール 2 1 は、直接ワイヤレス通信リンク 3 を介してアクセス制御デバイス 1 の無線通信モジュール 1 1 とデータを交換するように構成されている。

【 0 0 3 4 】

図 2 に示されているように、アクセス制御システム 1 0 0 は、1 つ又は複数の電子アクセス制御デバイス 1 及び通信ネットワーク 4 を介して電子アクセス制御デバイス 1 に接続されているアクセス権サーバ 5 を備えている。実装形態によっては、通信ネットワーク 4 は、LAN (ローカルエリアネットワーク (Local Area Network))、別の有線ネットワーク、WLAN (ワイヤレス LAN)、及び / 又は GSM (Global system for Mobile Communication) 又は UMTS ネットワーク (Universal Mobile Telephone System) などの別の移動無線ネットワークを含んでおり、インターネットを含むことができる。

10

【 0 0 3 5 】

アクセス権サーバ 5 は、アクセスキーを移動デバイス 2 へ送信するように、且つアクセスキー及び / 又は復号キーを電子アクセス制御デバイス 1 へ送信するように構成されている 1 つ又は複数のプロセッサを有する 1 つ又は複数の動作可能なコンピュータを備えている。ある実施形態では、アクセス権サーバ 5 又はそのコンピュータ / プロセッサは、それぞれ、実行可能なアクセス確認モジュール 2 3 を移動デバイス 2 及び / 又は電子アクセス制御デバイス 1 へ送信するようにさらに構成されている。或いは、実行可能なアクセス確認モジュール 2 3 は、上に述べたような移動無線ネットワークを含んでいる遠距離通信ネットワーク 6 を介してアプリケーションサーバ 7 によって移動デバイス 2 へ送信されている。

20

【 0 0 3 6 】

実行可能なアクセス確認モジュール 2 3 は、それぞれの移動デバイス 2 のプロセッサを制御し、その結果、移動デバイス 2 がより詳細に後で説明するような様々な機能を実行するように構成されているコンピュータプログラムコードを備えている。ある実施形態では、実行可能なアクセス確認モジュール 2 3 は、いわゆるアプレットとして実装されており、仮想マシン用の解釈可能なコンピュータプログラムコード、例えば、Java 仮想マシン (Java は Sun Microsystems, Inc. による登録商標である。以下同様) 上でランするように構成されている Java コードを備えている。

30

【 0 0 3 7 】

下記の段落では、図 3 ~ 図 5 を参照して説明しているものは、アクセス制御デバイス 1、移動デバイス 2、及びアクセス権サーバ 5 の機能モジュールによって実行される電子アクセス制御のためのステップの可能なシーケンスである。

【 0 0 3 8 】

準備ステップ S 0 では、アクセス権サーバ 5 は、アクセス制御デバイス 1 によって制御されており、アクセスを制御されている状態の領域にアクセスするためのアクセスキーを移動デバイス 2 へ転送する。アクセスキーは、例えば、トランスポート層セキュリティ (Transport Layer Security) (TLS)、セキュアソケット層 (Secure Sockets Layer) (SSL)、又は安全なデータ通信用の他の暗号化プロトコルを介して、安全に転送される。ある実施形態では、アクセスキーは、NFC インターフェース、Bluetooth インターフェース、又は Bluetooth ビーコンを介して移動デバイス 2 へ転送される。例えば、移動デバイス 2 へアクセスキーを送信するために、それぞれ、NFC 端末が、ホテルの受付のカウンタ若しくはデスクに据え付けられている、又は Bluetooth 端末 (インターフェース) 若しくは Bluetooth ビーコンが、ホテルの受付領域に据え付けられている。実施形態及び構成によっては、アクセス権サーバ 5 は、それぞれのアクセス制御デバイス 1 へ、アクセスキー又はアクセスキーを検証するための暗号化エレメントをさらに転送する。或いは、アクセスキー又は暗号化エレメントは、それぞれ、移動デバイス 2 へ転送される前にアクセ

40

50

ス制御デバイス1に記憶される。例えば、アクセスキーは、暗号化された秘密（例えば、秘密アクセス認証コード）であり、アクセス制御デバイス1は、秘密を検証するために秘密復号キーを使用する。

【0039】

ある実施形態では、アクセス権サーバ5は、上に述べた実行可能なアクセス確認モジュール23を移動デバイス2へさらに転送する。さらなる実施形態では、アクセスキーは、実行可能なアクセス確認モジュール23の一部として移動デバイスへ転送される。

【0040】

例えば、ホテルアプリケーションの場合では、アクセスキー及び適用可能である場合には実行可能なアクセス確認モジュール23は、受付でのチェックイン手続き中に移動デバイス2へ送信される。

10

【0041】

ステップS1では、アクセス制御デバイス1又はその近接検出装置13は、それぞれ、アクセス制御デバイス1の規定の近さPに（ごく近接して）移動デバイス2の存在を検出する。この目的で、移動デバイス2のユーザは、それぞれ、アクセス制御デバイス2又はその近接検出装置13のアンテナ131の規定の近さの（ごく近接する）範囲Pへと移動デバイス2を物理的に移動させる又は置く。

【0042】

ステップS2では、それぞれ、アクセス制御デバイス1又はその近接検出装置13の規定の近さPに（ごく近接して）移動デバイス2を検出したとき、アクセス制御デバイス1のコントローラ12は、無線通信モジュール11を制御して移動デバイス2との直接ワイヤレス通信リンク3を確立する。

20

【0043】

図4に図示されている実施形態において、ステップS21では、アクセス制御デバイス1又はそのコントローラ12は、それぞれ、無線通信モジュール11を制御して直接ワイヤレス通信リンク3を確立するためのマスタとして動作する。具体的には、コントローラ12は、Bluetoothセントラルモードに無線通信モジュール11のBluetoothトランシーバを設定する。

【0044】

ステップS22では、無線通信モジュール11は、接続プロセスを実行する：具体的には、Bluetoothトランシーバは、Bluetooth接続プロセスを開始し、Bluetoothスレーブをスキャンする。上手くいった場合には、アクセス制御デバイス1及び移動デバイス2又はそれらの無線通信モジュール11、21は、それぞれ、Bluetoothペアリング型接続として直接ワイヤレス通信リンク3を確立する。当業者なら理解するように、Bluetooth（BT）を用いると、接続の確立は、先のペアリングプロセスを使用する、ところが、Bluetooth Low Energy（BLE）は、ペアリングプロセスを含まない。

30

【0045】

別の方法では、コントローラ12は、無線通信モジュール11を制御して、直接ワイヤレス通信リンク3を移動デバイス2に確立させるためのスレーブとして動作させることによりステップS23に進む。具体的には、コントローラ12は、Bluetoothペリフェラルモードに無線通信モジュール11のBluetoothトランシーバを設定する。

40

【0046】

ステップS24では、移動デバイス2又はその無線通信モジュール21は、それぞれ、接続プロセスを実行する：具体的には、移動デバイス2のBluetoothトランシーバは、Bluetooth接続プロセスを開始し、Bluetoothスレーブをスキャンする。上手くいった場合には、移動デバイス2及びアクセス制御デバイス1又はそれらの無線通信モジュール11、21は、それぞれ、Bluetoothペアリング型接続として直接ワイヤレス通信リンク3を確立し、ステップS3へ進む。

50

【 0 0 4 7 】

別の方法では、ステップ S 2 5 において、アクセス制御デバイス 2 は、例えば、プロセスを繰り返す前に、移動デバイス 2 の通信モジュール 2 1 が起動されるべきであることをユーザに示すエラーメッセージを表示する。さらなる実施形態では、移動デバイス 2 がそれぞれのアクセス制御デバイス 1 と関係付けられることが可能な場合において、アクセス制御デバイス 1 は、類似のエラーメッセージを移動デバイス 2 のユーザへ送るようにアクセス権サーバ 5 に要求する。

【 0 0 4 8 】

ある実施形態では、多様性を大きくするために、それぞれ、アクセス制御デバイス 1 又はその近接検出装置 1 3 の規定の近さ P に（ごく近接して）移動デバイス 2 を検出したとき、アクセス制御デバイス 1 のコントローラ 1 2 は、アクセス制御デバイス 1 に実装されている様々なタイプの無線通信モジュールから移動デバイス 2 との直接ワイヤレス通信リンク 3 を確立するための好ましい無線通信モジュールを選択するように構成されている。具体的には、コントローラ 1 2 は、上に説明したような Bluetooth トランシーバ若しくは WLAN 通信モジュール、又は例えば、上に説明した近接検出装置 1 3 の RFID リードに実装されている NFC インターフェースを選択するように構成されている。実施形態又は構成によっては、好ましい無線通信モジュールの選択は、アクセス制御デバイス 1 に記憶されている選択表を使用して、又はプログラマブル選択ルールに従ってコントローラ 1 2 によって実行され、アクセス制御デバイス 1 が移動デバイス 2 との直接ワイヤレス通信リンク 3 を確立するための無線通信モジュールを選択する優先順位又は順番を規定する。

10

20

【 0 0 4 9 】

ステップ S 3 では、一旦、直接ワイヤレス通信リンク 3 が、それぞれ移動デバイス 2 とアクセス制御デバイス 1 との間又はその無線通信モジュール 1 1、2 1 間で設定されると、移動デバイス 2 又はその無線通信モジュール 2 1 は、それぞれ、アクセス制御デバイス 1 へ直接ワイヤレス通信リンク 3 を介してアクセスキーを転送する。具体的には、アクセス確認モジュール 2 3 が、実行され、移動デバイス 2 のプロセッサ 2 2 を制御して、アクセス制御デバイス 1 へアクセスキーを転送する。アクセス確認モジュール 2 3 の実行は、直接ワイヤレス通信リンク 3 が移動デバイス 2 とアクセス制御デバイス 1 又はアクセス制御デバイスのそれらの無線通信モジュール 1 1、2 1 との間でそれぞれ設定されると 1 回トリガされる。ある実施形態では、アクセス確認モジュール 2 3 の実行は、移動デバイス 2 へ直接ワイヤレス通信リンク 3 を介して実行要求を送信しているアクセス制御デバイス 1 によってトリガされる。

30

【 0 0 5 0 】

図 5 に図示されているように、ステップ S 3 3 では、移動デバイス 2 又はアクセス確認モジュール 2 3 は、アクセス制御デバイス 1 へアクセスキーを転送する前に、確認命令を移動デバイスのユーザに要求し受信する。実施形態によっては、アクセス確認モジュール 2 3 は、ユーザに対するグラフィカルユーザインターフェース、例えば、「キャンセル」及び「ok」ボタンを生成し、移動デバイス 2 のディスプレイ上に表示して、アクセス制御デバイス 1 によって制御されている領域への目的とするアクセスを確認する。ある実施形態では、ユーザは、アクセスコード又はパスワードなどの認証情報を入力することを要求される。代替で又は加えて、アクセス確認モジュール 2 3 は、移動デバイス 2 の指紋センサを使用して、ユーザから肯定確認を受信する。

40

【 0 0 5 1 】

ステップ S 3 4 では、ユーザが、例えば、「ok」ボタンを上手く押すこと及び/又は指紋センサによって要求された確認命令を入力した場合には、アクセス確認モジュール 2 3 は、アクセスキーを含んでいる確認メッセージを生成する。確認メッセージ及び従ってアクセスキーは、アクセス制御デバイス 1 へ直接ワイヤレス通信リンク 3 を介して移動デバイス 2 から転送される。

【 0 0 5 2 】

50

ステップS 3 5では、アクセス制御デバイス1又はそのコントローラ1 2は、それぞれ、直接ワイヤレス通信リンク3を介して無線通信モジュール1 1から確認メッセージを受信する。コントローラ1 2は、移動デバイス1から受信した確認メッセージからアクセスキーを抽出する。

【0053】

任意選択的なステップS 3 0、S 3 1、S 3 2は、アクセス確認モジュール2 3が移動デバイス2にプリロードされずプレインストールされていない実施形態/シナリオにおいて適用可能であるが、移動デバイス2がアクセス制御デバイス1の規定の近さに(ごく近接して)検出されると動的にロードされインストールされる。図5に図示されている実施形態では、コントローラ1 2は、受信信号強度インジケータ(Received Signal Strength Indicator)(RSSI)が、アクセス制御デバイス1から離れた規定の近い範囲C、例えば、アクセス制御デバイス1の距離パラメータの設定によって調節可能な、例えば、0.5メートル、1メートル、又は2メートルのアクセス制御デバイス1からの移動デバイス2の最大距離に対応する、それぞれ、移動デバイス2又はその無線通信モジュール2 1の信号強度を示すかどうかを検査する。RSSI値が設定した信号強度しきい値よりも大きく、且つ移動デバイス2が従ってアクセス制御デバイス1から離れた規定の近い範囲C内に位置する場合には、ステップS 3 1では、コントローラ1 2は、無線通信モジュール1 1を使用して、移動デバイス2へ直接ワイヤレス通信リンク3を介してアクセス確認モジュール2 3を転送する。

10

【0054】

ステップS 3 2では、移動デバイス2のプロセッサ2 2は、アクセス確認モジュール2 3を受信し実行する。アクセス確認モジュール2 3は、構成及び/又は実施形態に応じて、例えば、確認ボタンを押すこと及び/又は指紋センサ上に指を置くことをユーザに求めるそれぞれの要求を移動デバイス2のディスプレイ上に表示することによって、確認命令を移動デバイス2のユーザに要求する。

20

【0055】

ステップS 3 3では、アクセス確認モジュール2 3は、例えば、グラフィカルユーザインターフェース及び/又は指紋センサを介して確認命令を移動デバイス2のユーザから受信する。確認が肯定的である場合、例えば、ユーザが「ok」ボタンを押した又は指紋センサがユーザの指紋を正当であると読み取り検証した場合には、アクセス確認モジュール2 3は、例えば、アクセス権サーバ5から以前に受信したような暗号化された形態のアクセスキーを含んでいる肯定的確認メッセージを生成する。

30

【0056】

ステップS 3 4では、移動デバイス2のプロセッサ2 2は、無線通信モジュール2 1を使用して、アクセス制御デバイス1へ直接ワイヤレス通信リンク3を介して確認メッセージ、従ってアクセスキーを転送する。

【0057】

ステップS 3 5では、コントローラ1 2は、受信した確認メッセージからアクセスキーを抽出する。

【0058】

図3に図示されているように、ステップS 4では、コントローラ1 2は、移動デバイス2から受信したアクセスキーを検査し検証する。実施形態によっては、コントローラ1 2は、受信したアクセスキーを復号し、アクセス制御デバイス1に記憶されている検証キーと復号したアクセスキーとを比較する。アクセスキーを検証するための様々な暗号法機能及びアルゴリズムがあり、異なるレベル及びタイプのアクセス権、例えば、許可されたアクセス日付及び/又は時間枠が、特定のアクセスキーと関係付けられてもよいことを、当業者なら理解するであろう。いずれにせよ、ステップS 0~S 4は、アクセス権サーバ5とアクセス制御デバイス1との間のアクセスキーのエンドツーエンド暗号化又は秘密アクセス認証を提供する。

40

【0059】

50

任意選択的なステップS 4 1では、アクセスキーが適正に検証され得なかった場合には、コントローラ1 2は、無線通信モジュール1 1を使用して、移動デバイス2へ直接ワイヤレス通信リンク3を介してエラーメッセージを転送する。

【0060】

任意選択的なステップS 4 2では、移動デバイス2のプロセッサ2 2は、エラーメッセージを受信し、例えば、移動デバイス2のディスプレイにエラーメッセージを表示する及び/又は移動デバイス2上で警報音を発生することによって移動デバイス2上にエラーメッセージを表示する。

【0061】

ステップS 5では、受信したアクセスキーの肯定的な検証に応じて、コントローラ1 2は、例えば、電気信号又はデータ値の形態のアクセス制御信号を発生する。実施形態及び/又は構成によっては、アクセス制御信号は、施錠コマンドと異なり区別可能である解錠コマンドを表している。

【0062】

ステップS 5 0では、コントローラ1 2は、例えば、電子錠1 4に接続された又はアクセス可能な電気信号回線又はデータレジスタを介して、電子錠1 4にアクセス制御信号を適用する。

【0063】

ステップS 5 1では、コントローラ1 2からのアクセス制御信号に応じて、電子錠1 4は、解錠機能を実行する、例えば、電子錠1 4は、ドア、門、等を機械的に解錠するためにパー又はボルトを駆動して、アクセスを制御された領域、例えば、ビルディング又はホテルの部屋などの部屋への入口を通るアクセスに許可を与える。

【0064】

任意選択的なステップS 5 2では、電子錠1 4は、例えば、電気信号又はデータ値の形態の解錠確認信号又は解錠ステータス信号をコントローラ1 2へ返す。

【0065】

ステップS 6では、コントローラ1 2は、アクセス制御信号に対応し反映するアクセスステータスを決定し規定する。例えば、アクセスステータスは、解錠コマンドに対応している「開」状態、又は施錠コマンドに対応している「閉」状態を示す。任意選択的なステップS 5 2を含んでいる実施形態では、コントローラ1 2は、電子錠1 4からの解錠確認信号又は解錠ステータス信号を使用してアクセスステータスを確認し規定する。

【0066】

任意選択的なステップS 6 1では、コントローラ1 2は、無線通信モジュール1 1を使用して、移動デバイス2へ直接ワイヤレス通信リンク3を介して、アクセスステータスを含んでいるアクセスステータスメッセージを転送する。

【0067】

任意選択的なステップS 6 2では、移動デバイス2のプロセッサ2 2は、アクセスステータスメッセージを受信し、移動デバイス2のディスプレイ上にアクセスステータスを表示する。

【0068】

さらなる態様では、近接検出装置1 3は、追加で又は代替として、電子アクセス制御デバイス1までの規定の近さPの、例えば、0～5センチメートル、例えば、2～3センチメートル又は2～5センチメートルの規定の近さPのユーザの存在を検出するように構成されている容量センサ1 3 0を備えている。具体的には、容量センサ1 3 0は、電子アクセス制御デバイス1までの規定の近さPのユーザの手の存在を検出するように構成されている。例えば、容量センサ1 3 0は、CypressからのCapsense MBR3センサ(CapsenseはCypress Semiconductor Corp.の登録商標である)、例えば、Capsense MBR3センサCY8CMBR3108である。例えば、容量センサ1 3 0は、金属ドアハンドルに又はドアハンドル又はアクセスを制御された領域への入口のマークされた領域の近くに配置されたアンテナに電氣的

10

20

30

40

50

に接続されている。この実施形態では、コントローラ 12 は、それぞれ、近接検出装置 13 又は容量センサ 130 に接続され、電子アクセス制御デバイス 1 の規定の近さ P に近接検出装置 13 によってユーザを検出したとき、無線通信モジュール 11 を制御して、移動デバイス 2 との直接ワイヤレス通信リンク 3 を確立するようにさらに構成されている。コントローラ 12 は、直接ワイヤレス通信リンク 3 を確立するための追加の第 2 の条件として、移動デバイス 2 の受信信号強度が、無線通信モジュール 11 によって示されているように、移動デバイス 2 がアクセス制御デバイス 1 から規定の最大距離内であることを示す規定のしきい値を満足することを検査し検証するようにさらに構成されている。例えば、ユーザが電子アクセス制御デバイス 1 から 0 ~ 5 センチメートルの規定の近さに検出される場合で、且つ移動デバイス 2 の受信信号強度が、無線通信モジュール 11 によって示されているように、アクセス制御デバイス 1 から 0 . 5 又は 1 メートルの移動デバイス 2 の最大距離を示す規定のしきい値以上である場合にだけ、コントローラ 12 は、無線通信モジュール 11 を制御して、移動デバイス 2 との直接ワイヤレス通信リンク 3 を確立するように構成されている。

10

20

30

40

【 0 0 6 9 】

ある実施形態では、2 つ以上のアクセス制御デバイス 1 は、1 つの無線通信モジュール 11 を共有している。例えば、ホテルのシナリオでは、2 つの隣り合っているホテルの部屋のアクセス制御デバイス 1 は、2 つのアクセス制御デバイス 1 の（ドア側に装着されている）筐体の外に、例えば、（天井側の筐体内の）2 つのアクセス制御デバイス 1 までほぼ等距離又は少なくとも類似の距離で天井に設置されている共通無線通信モジュール 11 に接続されている。外部無線通信モジュール 11 は、それぞれアクセス制御デバイス 1 又はそのコントローラ 12 に有線接続を介して接続されている。ステップ S 2 を参照して上に説明したように、電子アクセス制御デバイス 1 のうちの 1 つの規定の近さ P 内に近接検出装置 13 によって移動デバイス 2 を検出したとき、その電子アクセス制御デバイス 1 のそれぞれのコントローラ 12 は、外部無線通信モジュール 11 を制御して、移動デバイス 2 との直接ワイヤレス通信リンク 3 を確立する。その目的で、コントローラ 12 は、検出信号を外部無線通信モジュール 11 へ送信する。或いは、外部無線通信モジュール 11 は、アクセス制御デバイス 1 からの検出信号に拘わらず、移動デバイス 2 との直接ワイヤレス通信リンク 3 を確立し、一方で、検出信号は、規定の近さ P 内に移動デバイス 1 を効果的に検出した特定のアクセス制御デバイス 1 を外部無線通信モジュール 11 が同定することを可能にする。引き続いて、図 3 及び図 5 を参照して上に説明したように、動作はステップ S 3 に続く。代替のシナリオ及び構成では、外部無線通信モジュール 11 は、2 つ以上のアンテナ 131 を有し、以てアンテナ 131 の各々が、それぞれ異なるドア又はその電子錠 14 に関係付けられている 1 つのアクセス制御デバイス 1 に有線接続を介して接続されている。この代替構成では、移動デバイス 2 が、それぞれ電子アクセス制御デバイス 1 又は特定のアンテナ 131 の規定の近さ P 内に近接検出装置 13 によって検出されたアンテナ 131 に基づいて、コントローラ 12 は、開けられるべき電子錠 14 を決定する。外部無線通信モジュール 11 と移動デバイスとの間の通信は、上に説明したように行われる。

【 0 0 7 0 】

明細書では、コンピュータプログラムコードが特定の機能モジュールに関係付けられており、ステップのシーケンスが特定の順序で提示されてきているが、しかしながら、当業者は、発明の範囲から乖離せずに、コンピュータプログラムコードが別なふうに構造化されてもよく、且つステップのうちの少なくともいくつかの順序が変更されてもよいことを理解するであろうことに留意されたい。

【 図 1 】

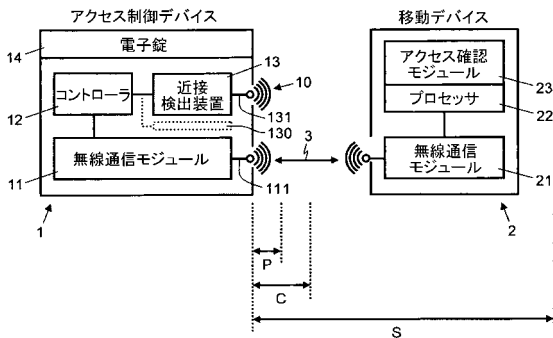


Fig. 1

【 図 2 】

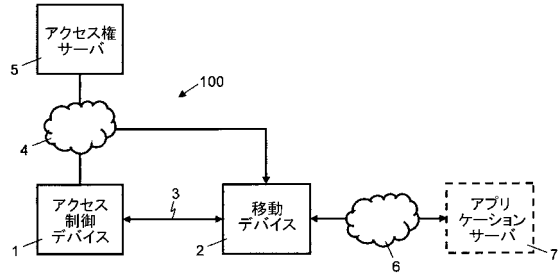


Fig. 2

【 図 3 】

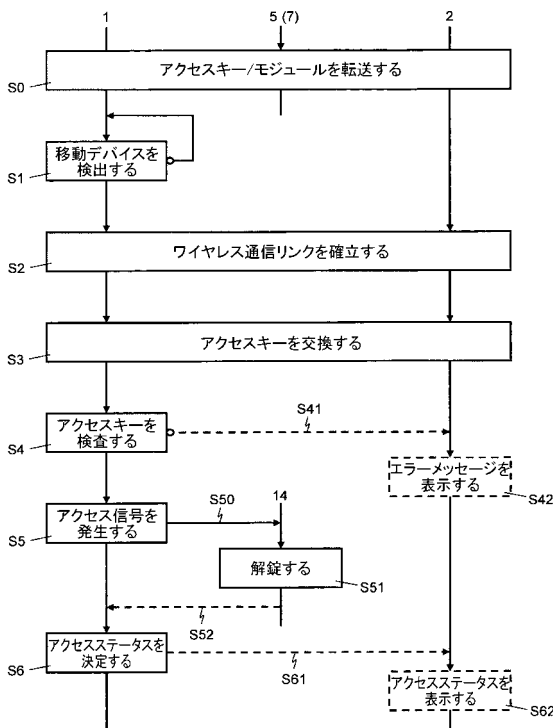


Fig. 3

【 図 4 】

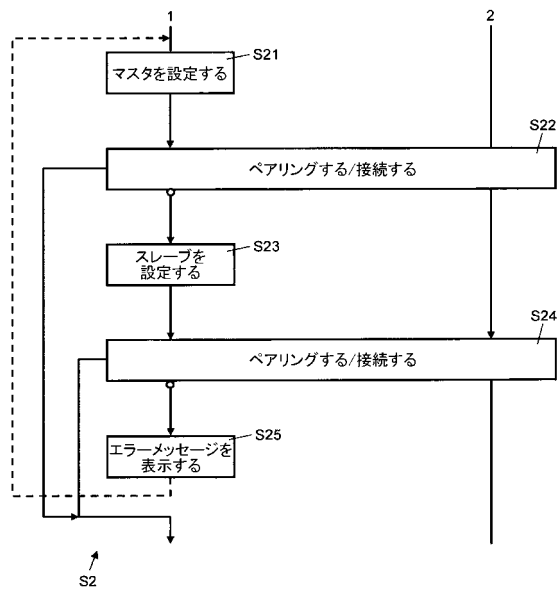


Fig. 4

【 図 5 】

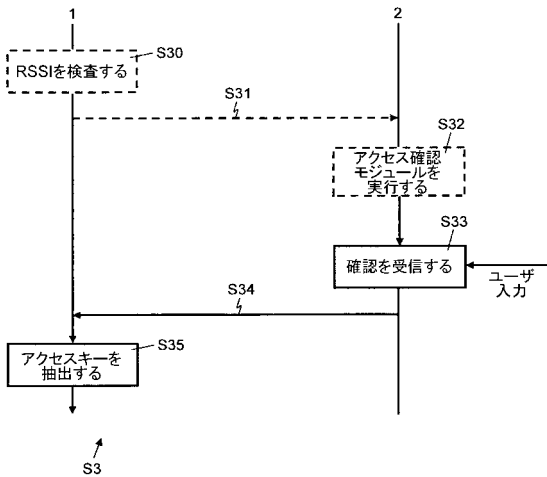


Fig. 5

【 手続 補正書 】

【 提出日 】平成29年1月5日 (2017.1.5)

【 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 】

無線通信モジュール（11）と移動デバイス（2）との間の直接ワイヤレス通信リンク（3）を介して前記移動デバイス（2）と第1の無線周波数帯域でワイヤレスデータ交換を実行するように構成されている無線通信モジュール（11）と、

前記無線通信モジュール（11）に接続され、前記移動デバイス（2）から前記直接ワイヤレス通信リンク（3）を介して前記無線通信モジュール（11）によって受信されたアクセスキーを使用してアクセス制御信号を発生するように構成されているコントローラ（12）と、

前記第1の無線周波数帯域とは異なる第2の無線周波数帯域の無線周波数を使用して前記移動デバイス（2）の存在を検出するように構成されている無線ベースの近接検出装置（13）とを備え、

前記コントローラ（12）は、前記無線ベースの近接検出装置（13）に接続され、前記移動デバイス（2）が前記無線通信モジュール（11）へ前記アクセスキーを送信することを可能にするために、前記無線ベースの近接検出装置（13）によって前記移動デバイス（2）を検出したとき、前記無線通信モジュール（11）を制御して、前記移動デバイス（2）との前記直接ワイヤレス通信リンク（3）を確立するようにさらに構成されている、

電子アクセス制御デバイス(1)において、

前記無線ベースの近接検出装置(13)は、前記移動デバイス(2)が、前記電子アクセス制御デバイス(1)から5センチメートル、10センチメートル、及び15センチメートルのうちの1つまでの距離範囲内に配置されている場合に、前記電子アクセス制御デバイス(1)にごく近接(P)する前記移動デバイス(2)の前記存在を検出するように構成されており、

前記コントローラ(12)が、前記電子アクセス制御デバイス(1)に前記ごく近接(P)する前記移動デバイス(2)を前記無線ベースの近接検出装置(13)によって検出したとき、前記移動デバイス(2)との前記直接ワイヤレス通信リンク(3)を確立するようにさらに構成されていることを特徴とする、

電子アクセス制御デバイス(1)。

【請求項2】

前記無線通信モジュール(11)が、数メートルの、特に10メートルまでの距離にわたる近距離(S)通信リンク(3)を介して前記移動デバイス(2)と前記ワイヤレスデータ交換を実行するように構成されている、請求項1に記載のアクセス制御デバイス(1)。

【請求項3】

前記無線ベースの近接検出装置(13)が、RFIDリーダを備え、電磁場パルス(10)を放出し、前記電磁場パルス(10)の放出中に戻り信号を検出し、前記戻り信号を使用して前記移動デバイス(2)の前記存在を検出することによって、前記移動デバイス(2)の前記存在を検出するように構成されている、請求項1又は2に記載の電子アクセス制御デバイス(1)。

【請求項4】

前記無線通信モジュール(11)が、Bluetoothトランシーバを備え、前記コントローラ(12)が、前記Bluetoothトランシーバを制御して、Bluetooth接続プロセスを実行することによって前記移動デバイス(2)との前記直接ワイヤレス通信リンク(3)を確立するようにさらに構成されている、請求項1～3のいずれか一項に記載の電子アクセス制御デバイス(1)。

【請求項5】

前記コントローラ(12)が、前記Bluetoothトランシーバを制御して、スレーブとしてBluetoothペリフェラルモードで動作している前記移動デバイス(2)との前記直接ワイヤレス通信リンク(3)を確立するためのマスタとしてBluetoothセントラルモードで動作するように、且つ応答に失敗したとき、前記Bluetoothトランシーバを制御して、前記マスタとして前記Bluetoothセントラルモードで動作している前記移動デバイス(2)により確立された前記直接ワイヤレス通信リンク(3)を有するためのスレーブとして前記Bluetoothペリフェラルモードで動作するようにさらに構成されている、請求項4に記載の電子アクセス制御デバイス(1)。

【請求項6】

前記無線通信モジュール(11)が、Bluetooth Low Energyトランシーバを備える、請求項4又は5に記載の電子アクセス制御デバイス(1)。

【請求項7】

前記コントローラ(12)が、前記無線通信モジュール(11)を制御して、実行可能なアクセス確認モジュール(23)を前記移動デバイス(2)へ送信するようにさらに構成されており、前記実行可能なアクセス確認モジュール(23)が、前記移動デバイス(2)のプロセッサ(22)を制御して、確認命令を前記移動デバイス(2)のユーザから受信し前記確認命令に応じて確認メッセージを前記アクセス制御デバイス(1)の前記無線通信モジュール(11)へ送信するように、前記移動デバイス(2)から前記確認メッセージを受信するように、且つ前記確認メッセージをさらに使用して前記アクセス制御信号を発生するように構成されている、請求項1～6のいずれか一項に記載の電子アクセス

制御デバイス(1)。

【請求項8】

前記実行可能なアクセス確認モジュール(23)が、前記移動デバイス(2)の前記プロセッサ(22)を制御して、前記移動デバイス(2)の指紋センサ及び前記移動デバイス(2)のグラフィカルユーザインターフェースのうち少なくとも一方を介して前記移動デバイス(2)の前記ユーザから前記確認命令を受信するようにさらに構成されている、請求項7に記載の電子アクセス制御デバイス(1)。

【請求項9】

前記実行可能なアクセス確認モジュール(23)が、前記移動デバイス(2)の前記プロセッサ(22)を制御して、前記確認メッセージに前記アクセスキーを含ませるようにさらに構成され、前記コントローラ(12)が、前記アクセス制御信号を発生するために前記確認メッセージから前記アクセスキーを得るようにさらに構成されている、請求項7又は8に記載の電子アクセス制御デバイス(1)。

【請求項10】

前記コントローラ(12)は、前記無線通信モジュール(11)を制御して、前記無線通信モジュール(11)の受信信号強度が1メートルの前記アクセス制御デバイス(1)からの前記移動デバイス(2)の最大距離(C)を示す規定のしきい値を満足する場合にだけ、前記実行可能なアクセス確認モジュール(23)を前記移動デバイス(2)へ送信するように、且つ前記確認メッセージの前記受信信号強度に拘わらず前記アクセス制御信号を発生するようにさらに構成されている、請求項7～9のいずれか一項に記載の電子アクセス制御デバイス(1)。

【請求項11】

前記アクセス制御デバイス(1)が、電子錠(14)をさらに備え、前記コントローラ(12)が、前記電子錠(14)に接続されており、前記電子錠(14)を制御するため前記電子錠(14)へ前記アクセス制御信号を供給して、解錠機能を実行するようにさらに構成されている、請求項1～10のいずれか一項に記載の電子アクセス制御デバイス(1)。

【請求項12】

前記コントローラ(12)が、前記アクセス制御信号を反映しているアクセスステータスを規定するように、且つ前記無線通信モジュール(11)を制御して、前記移動デバイス(2)へ前記アクセスステータスを送信するようにさらに構成されている、請求項1～11のいずれか一項に記載の電子アクセス制御デバイス(1)。

【請求項13】

感度パラメータを含み、前記距離範囲が、前記感度パラメータを設定することによって調節可能である、請求項1～12のいずれか一項に記載のアクセス制御デバイス(1)。

【請求項14】

前記コントローラ(12)が、前記アクセス制御デバイス(1)に前記ごく近接(P)する前記移動デバイス(2)を検出したとき、前記アクセス制御デバイス(1)に実装されている様々なタイプの無線通信モジュールから前記移動デバイス(2)と前記直接ワイヤレス通信リンク(3)を確立するために前記無線通信モジュール(11)を選択するように構成されている、請求項1～13のいずれか一項に記載のアクセス制御デバイス(1)。

【請求項15】

第2の無線周波数帯域の無線周波数を使用して、移動デバイス(2)が無線通信モジュール(11)から5センチメートル、10センチメートル、及び15センチメートルのうち1つまでの距離範囲内に配置されている場合に、電子アクセス制御デバイス(1)にごく近接(P)する前記移動デバイス(2)の存在を前記電子アクセス制御デバイス(1)の無線ベースの近接検出装置(13)によって検出するステップ(S1)と、

前記電子アクセス制御デバイス(1)に前記ごく近接(P)する前記移動デバイス(2)を前記無線ベースの近接検出装置(13)によって検出したとき、前記電子アクセス制

御デバイス(1)の無線通信モジュール(11)を制御して、前記第2の無線周波数帯域とは異なる第1の無線周波数帯域でワイヤレスデータ交換のための直接ワイヤレス通信リンク(3)を前記移動デバイス(2)と確立するステップ(S2)と、

前記直接ワイヤレス通信リンク(3)を介して前記移動デバイス(2)からアクセスキーを前記電子アクセス制御デバイス(1)の前記無線通信モジュール(11)によって受信するステップ(S3)と、

前記移動デバイス(2)から受信した前記アクセスキーを使用してアクセス制御信号を前記電子アクセス制御デバイス(1)において発生するステップ(S5)とを含む、アクセス制御方法。

【 国際調査報告 】

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2015/001233

A. CLASSIFICATION OF SUBJECT MATTER INV. G07C9/00 ADD.		
According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) G07C B60R		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) EPO-Internal, WPI Data		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2006/098690 A1 (PHONIRO AB [SE]; BLIDING OLLE [SE]; HOERBERG JOHAN [SE]) 21 September 2006 (2006-09-21)	1-4, 6-9, 11, 13
Y	abstract page 4, line 11 - page 7, line 10 page 9, line 31 - page 10, line 13 page 11, line 29 - page 13, line 37 page 15, line 23 - line 37 page 17, line 11 - line 28 page 19, line 4 - page 23, line 13 figures 1,3,6	5, 10, 12
Y	----- US 2003/027526 A1 (HILLYARD JASON [US]) 6 February 2003 (2003-02-06) abstract paragraph [0010] - paragraph [0014] ----- -/--	5
<input checked="" type="checkbox"/> Further documents are listed in the continuation of Box C.		<input checked="" type="checkbox"/> See patent family annex.
* Special categories of cited documents : "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier application or patent but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed		"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family
Date of the actual completion of the international search 7 August 2015		Date of mailing of the international search report 24/08/2015
Name and mailing address of the ISA/ European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016		Authorized officer Van der Haegen, D

1

INTERNATIONAL SEARCH REPORT

International application No

PCT/EP2015/001233

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	EP 1 471 426 A2 (NTT DOCOMO INC [JP]) 27 October 2004 (2004-10-27) paragraph [0015] - paragraph [0017] paragraph [0037] - paragraph [0038] paragraph [0043] -----	10
Y	US 2013/335193 A1 (HANSON PAUL [CA] ET AL) 19 December 2013 (2013-12-19) paragraph [0016] - paragraph [0020] paragraph [0030] - paragraph [0036] paragraph [0091] - paragraph [0097] paragraph [0107] - paragraph [0140] figures 2,7 -----	12
A	WO 2005/086069 A2 (LEGIC IDENTSYSTEMS AG [CH]; PLUESS MARCEL [CH]; KOCH ANDREAS [DE]; HAU) 15 September 2005 (2005-09-15) cited in the application page 1, line 1 - line 10 page 5, line 6 - line 27 -----	3
A	WO 2013/181682 A1 (PHACTUM SOFTWAREENTWICKLUNG GMBH [AT]) 12 December 2013 (2013-12-12) page 1, line 1 - page 2, line 4 page 4, line 26 - line 31 page 5, line 14 - line 29 page 7, line 26 - page 11, line 10 page 13, line 5 - page 23, line 26 -----	7-9

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2015/001233

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2006098690 A1	21-09-2006	DK 2083396 T3	17-12-2012
		DK 201300075 U1	24-05-2013
		DK 201300119 U1	23-08-2013
		DK 201300133 U1	27-09-2013
		EP 1859415 A1	28-11-2007
		EP 2083396 A2	29-07-2009
		EP 2434463 A2	28-03-2012
		US 2007229257 A1	04-10-2007
		US 2009184801 A1	23-07-2009
		US 2010148921 A1	17-06-2010
		US 2014020437 A1	23-01-2014
		US 2014022054 A1	23-01-2014
		WO 2006098690 A1	21-09-2006
US 2003027526 A1	06-02-2003	US 2003027526 A1	06-02-2003
		US 2007190938 A1	16-08-2007
EP 1471426 A2	27-10-2004	CN 1535061 A	06-10-2004
		EP 1471426 A2	27-10-2004
		JP 4602644 B2	22-12-2010
		JP 2004302517 A	28-10-2004
		TW I297997 B	11-06-2008
US 2005021693 A1	27-01-2005		
US 2013335193 A1	19-12-2013	EP 2785939 A1	08-10-2014
		US 2013335193 A1	19-12-2013
		WO 2013078561 A1	06-06-2013
WO 2005086069 A2	15-09-2005	AT 529819 T	15-11-2011
		CA 2557961 A1	15-09-2005
		CN 1926555 A	07-03-2007
		EP 1723575 A2	22-11-2006
		EP 2256662 A2	01-12-2010
		ES 2374551 T3	17-02-2012
		JP 4657283 B2	23-03-2011
		JP 2007526696 A	13-09-2007
		SI 1723575 T1	31-01-2012
		US 2007188326 A1	16-08-2007
		WO 2005086069 A2	15-09-2005
WO 2013181682 A1	12-12-2013	AT 513016 A1	15-12-2013
		CN 104508713 A	08-04-2015
		EP 2856437 A1	08-04-2015
		KR 20150029679 A	18-03-2015
		US 2015119019 A1	30-04-2015
		WO 2013181682 A1	12-12-2013

フロントページの続き

(81)指定国 AP(BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), EA(AM, AZ, BY, KG, KZ, RU, TJ, TM), EP(AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OA(BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG), AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US

(72)発明者 ブルス, マルセル

スイス, 8632 タン, ハリゲイヒシュトラーセ 56

(72)発明者 スチュデルス, ポール

スイス, 8165 オーバーヴェニンゲン, ヒェーブリシュトラーセ 78

Fターム(参考) 2E250 AA04 AA05 AA06 AA21 AA22 BB08 CC12 CC20 CC26 DD06
DD09 FF10 FF23 FF26 FF27 FF36 HH01 JJ03