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

特許第6284882号
(P6284882)

(45)発行日　平成30年2月28日(2018.2.28)　(24)登録日　平成30年2月9日(2018.2.9)

(51)Int.Cl.		F I		
H04L 9/08	(2006.01)	H04L	9/00	601A
G06F 21/70	(2013.01)	H04L	9/00	601C
A61B 5/0215	(2006.01)	G06F	21/70	
A61B 5/00	(2006.01)	A61B	5/02	610F
		A61B	5/00	C

請求項の数 26　(全 23 頁)　最終頁に続く

(21)出願番号　特願2014-537799 (P2014-537799)
(86)(22)出願日　平成24年10月26日 (2012.10.26)
(65)公表番号　特表2015-501593 (P2015-501593A)
(43)公表日　平成27年1月15日 (2015.1.15)
(86)国際出願番号　PCT/IB2012/055917
(87)国際公開番号　WO2013/061296
(87)国際公開日　平成25年5月2日 (2013.5.2)
審査請求日　平成27年10月13日 (2015.10.13)
(31)優先権主張番号　11187121.6
(32)優先日　平成23年10月28日 (2011.10.28)
(33)優先権主張国　欧州特許庁 (EP)
(31)優先権主張番号　12175498.0
(32)優先日　平成24年7月9日 (2012.7.9)
(33)優先権主張国　欧州特許庁 (EP)

(73)特許権者　511280951
デバイオテック・ソシエテ・アノニム
スイス国ＣＨ－１００４ローザンヌ．セヴェリン２８．“ル　ポルティック”アヴェニュ　ドゥ　イムブル
(74)代理人　100127926
弁理士　結田　純次
(74)代理人　100140132
弁理士　竹林　則幸
(72)発明者　ステファン・プロエンネッケ
スイス国ＣＨ－１００４ローザンヌ．アヴェニュ　ドゥ　セヴェリン２８．デバイオテック・ソシエテ・アノニム

最終頁に続く

(54)【発明の名称】医療用デバイスとその遠隔デバイスの間のセキュアな通信

(57)【特許請求の範囲】

【請求項１】

無線通信をセキュアにするための医療用システムであって、

無線通信手段、

接続ポート、

前記無線通信手段に接続されたプロセッサ

を備える遠隔制御装置（３）と、

前記遠隔制御装置（３）の無線通信手段と無線通信するよう適合された無線通信手段、

セキュアな内部メモリ

を備える医療用デバイス（１、７）と、

前記遠隔制御装置（３）の接続ポートに接続されるように設計され；セキュアなメモリをさらに備えるＭＣＵ（４、４ａ、４ｂ、４ｃ、６）と

を備え、

ここで、少なくとも１つの医療用デバイス（１、７）は、ただ１つのＭＣＵ（４、４ａ、４ｂ、４ｃ、６）と排他的にペアリングされ、

前記医療用デバイス（１、７）および前記ＭＣＵ（４、４ａ、４ｂ、４ｃ、６）は、前記医療用デバイス（１、７）と前記遠隔制御装置（３）の間のデータの通信をセキュアにするセキュアな処理手段（５）を備え、

前記ＭＣＵ（４、４ａ、４ｂ、４ｃ、６）は、前記遠隔制御装置（３）が前記セキュアな処理手段（５）にアクセスしないような形で、そのセキュアなメモリ内に前記セキュア

な処理手段（５）を保つ、
上記医療用システム。
【請求項２】
前記医療用デバイス（１、７）のセキュアな内部メモリおよびそのＭＣＵ（４、４ａ、４ｂ、４ｃ、６）のセキュアなメモリがさらに、無線通信構成の少なくとも一部を含む、請求項１に記載の医療用システム。
【請求項３】
前記医療用デバイスのセキュアな内部メモリまたは前記ＭＣＵのセキュアなメモリのみが、暗号機構または認証手順のために使用される鍵を含む、請求項１に記載の医療用システム。
【請求項４】
前記ＭＣＵのメモリがさらに、前記遠隔制御装置と前記医療用デバイスの間でペアリングを開始するために前記遠隔制御装置によって使用されるリンク鍵を保存する、請求項１に記載の医療用システム。
【請求項５】
前記医療用デバイスが、別のＭＣＵとペアリングすることができない、請求項１に記載の医療用システム。
【請求項６】
前記ＭＣＵが前記遠隔制御装置に接続される前に、前記医療用デバイスとそのＭＣＵがペアリングされる、請求項１に記載の医療用システム。
【請求項７】
前記医療用デバイスと前記遠隔制御装置の間のペアリングの前に、前記医療用デバイスとそのＭＣＵがペアリングされる、請求項１に記載の医療用システム。
【請求項８】
前記遠隔制御装置（３）は、表示手段および入力手段の少なくとも１つを備える、請求項１に記載の医療用システム。
【請求項９】
前記セキュアな処理手段（５）が、認証手順を処理するよう設計される、請求項１に記載の医療用システム。
【請求項１０】
前記セキュアな処理手段（５）が、新しい医療用デバイスまたは新しいＭＣＵとの新しいペアリング処理を防ぐよう設計される、請求項１に記載の医療用システム。
【請求項１１】
前記セキュアな処理手段が、前記無線通信のセキュア化および前記無線通信の開始の少なくとも１つのための追加の鍵を生成する暗号機構を使用する、請求項１に記載の医療用システム。
【請求項１２】
前記ＭＣＵが、前記無線通信のデータの暗号化を行うよう構成されたプロセッサを含む、請求項１に記載の医療用システム。
【請求項１３】
前記ＭＣＵが、前記無線通信のデータの復号を行うよう構成されたプロセッサを含む、請求項１に記載の医療用システム。
【請求項１４】
前記ＭＣＵ（４、４ａ、４ｂ、４ｃ、６）は、汎用集積回路カード、スマート・カード、またはＳＩＭカード、またはＳＤカードである、請求項１に記載の医療用システム。
【請求項１５】
前記ＭＣＵ（４、４ａ、４ｂ、４ｃ、６）の前記セキュアなメモリは、前記ＭＣＵ（４、４ａ、４ｂ、４ｃ、６）の内部で実行され遠隔制御装置（３）とインタフェースするアプリケーションを備える、請求項１に記載の医療用システム。
【請求項１６】

アプリケーションは、遠隔制御装置（３）の内部メモリにロードされ、前記遠隔制御装置（３）の内部で実行されている、請求項１に記載の医療用システム。
【請求項１７】
前記ＭＣＵ（４、４ａ、４ｂ、４ｃ、６）は、前記アプリケーションの完全性を確認するための認証手段を備える、請求項１５に記載の医療用システム。
【請求項１８】
前記ＭＣＵのメモリがさらに、前記遠隔制御装置によって読み取ることができないデータを含むセキュアな情報を保存する、請求項１に記載の医療用システム。
【請求項１９】
前記遠隔制御装置によって読み取ることができないデータが、暗号機構によって使用される鍵、認証機構によって使用される鍵、他の鍵および他の情報の少なくとも１つである、請求項１８に記載の医療用システム。
【請求項２０】
前記遠隔制御装置が、テレコム・オペレータのＳＩＭカードを受け取るよう構成された第２の接続ポートを含む、請求項１に記載の医療用システム。
【請求項２１】
前記遠隔制御装置が、制御されている環境および制御されていない環境を示すためのモバイル仮想化ディスプレイを含む、請求項１に記載の医療用システム。
【請求項２２】
前記遠隔制御装置が、ホスト・オペレーティング・システムによって実行され、前記制御されている環境が、医療用オペレーティング・システムである、請求項２１に記載の医療用システム。
【請求項２３】
前記医療用デバイスおよびそのＭＣＵが各々、ループバック機構を実行するよう構成されたコンピュータ指令によって運用される、請求項１に記載の医療用デバイス。
【請求項２４】
前記ＭＣＵが、前記医療用デバイス専用である、請求項１に記載の医療用システム。
【請求項２５】
ループバック機構を持つ、請求項１～２４のいずれか１項に記載の医療用システム（４、４ａ、４ｂ、４ｃ、６）の使用であって：
前記医療用デバイス（１、７）によって行われる、
医療用デバイス（１、７）のセキュアなメモリに肯定応答でなければならないパラメータを書き込む工程と、
チャレンジを生成する工程と、
一時鍵Ｋｓ１を使用することによって前記パラメータを暗号化する工程と、
振動、音、ＬＥＤ、または患者に知らせる他の任意の方法によって、医療用デバイス（１、７）および遠隔制御装置（３）はループバック・モードであることをユーザに示す工程と、
暗号化したパラメータを遠隔制御装置（３）に送信する工程と、
遠隔制御装置（３）によって行われる、
暗号化したパラメータをＭＣＵ（４、４ａ、４ｂ、４ｃ、６）に送信する工程と、
ＭＣＵ（４、４ａ、４ｂ、４ｃ、６）によって行われる、
暗号化されたパラメータおよびチャレンジを受信して、ＭＣＵ（４、４ａ、４ｂ、４ｃ、６）のセキュアなメモリ領域に書き込む工程と、
鍵Ｋｓ１を使用することによってパラメータを復号する工程と、
復号したパラメータおよびチャレンジを遠隔制御装置（３）のメモリに送信する工程と、
遠隔制御装置（３）によって行われる、
復号されたパラメータを「概要」ページに表示する工程と、
ユーザに、ユーザの認証手段を入力することを促す工程と、

チャレンジ、パラメータ、および入力した前記認証手段を使用することによってこれらのパラメータの受け入れを確認する肯定応答チケットを構築する工程と、
遠隔制御装置（３）のセキュアなメモリ領域にチケットを書き込む工程と、
前記チケットをＭＣＵ（４、４ａ、４ｂ、４ｃ、６）に送信する工程と、
ＭＣＵ（４、４ａ、４ｂ、４ｃ、６）によって行われる、
前記チケットを受信し、ＭＣＵ（４、４ａ、４ｂ、４ｃ、６）のセキュアなメモリ領域に書き込む工程と、
一時鍵Ｋｓ２を使用することによって前記チケットを暗号化する工程と、
前記暗号化したチケットを遠隔制御装置（３）に返送する工程と、
遠隔制御装置（３）によって行われる、
暗号化したチケットを医療用デバイス（１、７）に送信する工程と、
医療用デバイス（１、７）によって行われる、
予想されるチケットを計算する工程と、
遠隔制御装置（３）から来る肯定応答チケットを受信し、復号し、検証する工程とを含み、
チケットが検証されるとき、ループバック・プロセスは閉じており、医療用デバイス（１、７）は更新されたパラメータを使用することが可能である、
上記医療用システムの使用。

【請求項２６】

ユーザの認証手段はＰＩＮコードであってもよいし、指紋読み取り装置または網膜読み取り装置などを使用してもよい、請求項２５に記載のループバック機構の使用。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、限定するものではないが、送達デバイス（たとえばインスリン・ポンプ）および／または無線センサ（たとえば持続血糖測定器）および／または埋め込み型デバイスおよび／またはサンプリング・デバイスなどの医療用デバイスの遠隔制御装置（ｒｅｍｏｔｅ　ｃｏｎｔｒｏｌ）に関する。

【背景技術】

【０００２】

パッチ・ポンプのような軽量かつ小型のインスリン・ポンプなどいくつかの医療用デバイスを制御するために、遠隔制御装置が必要とされる。その理由は、ポンプそれ自体に配置されたディスプレイの内容を患者が見るのは非常に困難なものとなり得るからである。現在、ポンプの大部分は、メーカ独自の専用の遠隔制御装置を使用している。このことは、別のデバイスを、それにより生じる可能性がある以下のようなあらゆる欠点と共に携行することを表す。すなわち：

・ポケットを見つけて、すばやく簡単にアクセスできる安全な場所に入れること。
・遠隔制御装置を忘れないこと
・充電について考えること、または予備のバッテリを持つこと
・落下、または日光もしくは砂にさらされることのようなあらゆる外部の「悪」条件によるその劣化を防止すること。

【０００３】

別の特定のデバイスの使用を防止する１つの方法は、患者が常に携行しなければならない既存のデバイスに遠隔制御装置機能を組み込むことであるである。この既存のデバイスは、限定するものではないが、血糖測定器または携帯電話などであり、遠隔制御装置機能を組み込むために必要とされるすべての機能を有する。

【０００４】

この目的で携帯電話を使用することは、非常に魅力的であるが、インスリン・ポンプをプログラムするために携帯電話を使用することを可能にする前に、セキュリティ上の多数の側面に対処しなければならない。確保しなければならない重要なセキュリティ機能には

、以下のものがある：
・ユーザに対して表示されるデータの完全性
・インスリン・ポンプに送信されるコマンドの完全性
・患者の治療パラメータならびに注入履歴およびイベントのログを収納するデータベースの完全性および保護。
・医療用デバイスとその遠隔制御装置をセキュアにペアリングすること。
・いつでもソフトウェアの応答性があること（たとえば：別のソフトウェアにフォーカスがあるときにアラームを発する、他のタスクがＭＣＵのようなリソースに負荷をかけすぎているときにユーザ要求を処理する能力、など）。

【０００５】
本出願は、Ｄｅｂｉｏｔｅｃｈの名義で２０１１年１０月２８日に出願されたＥＰ１１１８７１２１．６の優先権およびＤｅｂｉｏｔｅｃｈの名義で２０１２年７月９日に出願されたＥＰ１２１７５４９８．０の優先権の利益を主張するものであり、これらの開示全体は、参照により本明細書に組み込まれる。

【発明の概要】
【発明が解決しようとする課題】
【０００６】
本発明の目的は、医療用デバイスとその遠隔制御装置の間の通信をセキュアにする（ｓｅｃｕｒｅ）ための堅牢な環境を提供することである。本明細書では、「通信をセキュアにする」という表現は、遠隔制御装置と医療用デバイスの間のデータ交換が正常であることを確実にするために使用されるあらゆる手段として理解されなければならず、前記データは、許可されたオペレータ（たとえば、ユーザとも呼ばれる患者）によって適切なデバイスを使用して送信され、適切に受信されている。前記手段は、データまたはアプリケーションもしくはオペレーティング・システムの完全性の確認、暗号化プロセス、ペアリング・プロセス、オペレータの身元の検証などであってよい。この趣旨で、本発明は、ループバック・プロセスおよび／または仮想化プラットフォームを組み込んだ前記遠隔制御装置（または医療用デバイスに属する追加のマイクロコントローラ）を使用する医療用アセンブリ（前記医療用デバイスとその遠隔制御装置とを備える）および／または追加のマイクロコントローラ（ＭＣＵ）を使用する前記アセンブリを備えることができ、このＭＣＵは、遠隔制御装置に挿入され（あるいはプラグ接続され）、セキュアな（ｓｅｃｕｒｅｄ）データを含むことができ、かつ／または暗号機構を使用して前記医療用デバイスと通信することができる。前記３つの異なる手段（ＭＣＵ、ループバック、仮想化）を使用することによって、セキュリティを実質的に改善することが可能になるが、前記手段のうち１つまたは２つだけを使用することも可能である。

【０００７】
前記医療用アセンブリは、限定するものではないが、送達デバイスおよび／または無線センサおよび／または埋め込み型デバイスおよび／またはサンプリング・デバイスおよび／または血糖測定モニタなどの少なくとも１つの医療用デバイスを管理および／または監視することができる遠隔制御装置を備えることができる。

【０００８】
前記医療用デバイスは、遠隔制御装置を用いた無線通信を可能にする通信手段と、前記通信をセキュアにする鍵情報を含むセキュアな内部メモリとを備える。前記医療用デバイスは、ただ１つのマイクロコントローラ（ＭＣＵ）とペアリングされ、このＭＣＵは、セキュアなメモリを備え、前記鍵情報も含む。前記ＭＣＵは、遠隔制御装置にプラグ接続されるように設計される。

【課題を解決するための手段】
【０００９】
外部マイクロコントローラを使用する一実施形態では、医療用デバイスと遠隔制御装置の間のセキュアな通信を確立するのに適した前記アセンブリは、：
・前記医療用デバイスとの無線通信を可能にする通信手段、

・追加のマイクロコントローラ（ＭＣＵ）をプラグ接続するための接続手段；
・表示手段（場合により）、
・少なくとも１つの入力手段、
・通信手段、接続手段、（場合により、表示手段）、および入力手段に接続された少なくとも１つのプロセッサ；
を備える遠隔制御装置と：
・前記遠隔制御装置との無線通信を可能にする通信手段、
・セキュアな内部メモリ；
を備える医療用デバイスと：
・前記遠隔制御装置に接続することができ；セキュアなメモリをさらに備えるＭＣＵと；
を備え、
ここで、少なくとも１つの医療用デバイスは、ただ１つのＭＣＵと排他的にペアリングされ；
前記医療用デバイスの内部メモリおよび前記ＭＣＵのセキュアなメモリは、通信をセキュアにするための鍵情報を含む。

【００１０】

本明細書では、マイクロコントローラ（ＭＣＵ）は、遠隔制御装置に挿入された集積チップであってもよいし、または遠隔制御装置にプラグ接続された外部デバイスであってもよい。一般に、ＭＣＵは、ＣＰＵと、ＲＡＭと、何らかの形態のＲＯＭと、Ｉ／Ｏポートと、タイマとを含む。他の構成要素を含むコンピュータまたは遠隔制御装置とは異なり、マイクロコントローラ（ＭＣＵ）は、非常に特殊なタスク向けに、たとえば特定のシステムを制御するように、設計されている。その結果、ＭＣＵは単純化および小型化することが可能であり、これによって、製造コストを削減する。さらに、前記ＭＣＵは、遠隔制御装置の性能を改善するために（遠隔制御装置の）ＯＳが使用することができる別のＣＰＵおよびメモリをもたらすのではなく、他の機能、特に追加のセキュリティ機能をもたらす。遠隔制御装置のＭＣＵとＣＰＵは別物であり、異なるタスクを有する。本発明では、ＭＣＵは、ＭＣＵがさまざまな遠隔制御装置と共に使用できるように、遠隔制御装置から完全に独立している。前記ＭＣＵは、スマート・カード、Ｓｉｍカード、ＳＤＩＯカード（Ｓｅｃｕｒｅ　Ｄｉｇｉｔａｌ　Ｉｎｐｕｔ　Ｏｕｔｐｕｔ）などのＳＤカードであってもよい。本明細書では、発明者らは、以下の用語、すなわち：外部マイクロコントローラまたは追加のマイクロコントローラまたはＭＣＵを区別せずに（ｉｎｄｉｆｆｅｒｅｎｔｌｙ）使用することができる。

【００１１】

好ましい一実施形態では、前記医療用デバイスおよび前記ＭＣＵは、無線通信構成を含むセキュアなメモリを備える。このようにして、前記デバイスおよび前記ＭＣＵは、良好な構成を事前に認識している。特に、前記ＭＣＵは、遠隔制御装置を医療用デバイスに接続するために、および前記通信を保護するために使用される鍵情報を含むことができる。

【００１２】

したがって、前記ＭＣＵはただ１つの医療用デバイスとペアリングされ、前記ＭＣＵは遠隔制御装置に挿入される。このようにして、前記ＭＣＵを含む遠隔制御装置のみが、前記医療用デバイスを管理および／または監視することができる。また、患者は、前記ＭＣＵが挿入されている遠隔制御装置が、医療用デバイスを管理および／または監視することが可能な単一の遠隔制御装置であることを知っていながら、遠隔制御装置を変更することができる。

【００１３】

別の実施形態では、遠隔制御装置は、少なくとも２つの医療用デバイスを管理および／または監視する。この場合、前記２つの医療用デバイスは、ただ１つのＭＣＵとペアリングすることができ、あるいは、各医療用デバイスはそれ自体のＭＣＵとペアリングされる。

【００１４】

一実施形態では、前記ＭＣＵは、前記医療用アセンブリを医療用サーバと接続するための鍵情報を含む。この実施形態では、医療用アセンブリは、遠隔制御装置のデータ通信手段を使用することができる。したがって、前記ＭＣＵは、限定するものではないが、ユーザ認証、暗号化パラメータなどの、医療用アセンブリと医療用サーバの間の通信をセキュアにするためのすべての情報を含むことができる。

【００１５】

一実施形態では、ＭＣＵは、医療用デバイスによって送信される少なくとも１組のデータまたは遠隔デバイスまたは他のデバイスから提供される他の組のデータを、セキュアなメモリに収納することができる。別の実施形態では、前記データは暗号化され、遠隔デバイスまたは医療用デバイスに収納されるが、ＭＣＵ（または医療用デバイス）のみが、前記データを復号するための鍵を含む。

【００１６】

遠隔制御装置が仮想プラットフォームを使用する一実施形態では、遠隔制御装置は、
・少なくとも１つのゲスト・オペレーティング・システム（ｇＯＳ）用のハードウェア構成要素をエミュレートするホスト・オペレーティング・システム（ｈＯＳ）と、
・いずれも制御されていない環境で使用するように設計され、限定するものではないが、カレンダーまたは連絡先のような一般的な機能を処理する第１のｇＯＳと、
・いずれも制御されている環境で使用するように設計された、医療用デバイスのための遠隔制御装置の機能を処理する医療用オペレーティング・システム（ｍＯＳ）とを備える仮想化プラットフォームを組み込む。前記ｍＯＳは、特定のｇＯＳであってもよい。

【００１７】

本明細書では、「ホスト・オペレーティング・システム」という表現は、ＲＡＭ、Ｆｌａｓｈ、ＵＡＲＴ、Ｗｉｆｉなどのすべての遠隔制御装置周辺機器を単独で管理しこれらを共有することが可能な拡張ハイパーバイザなどの、できる限り機能の少ない（ｔｈｉｎ）オペレーティング・システムとして理解されなければならない。ｈＯＳは一般的な機能を扱わず、その目的は、医療用デバイスに送信されるコマンドをセキュアにすることである。

【００１８】

一実施形態では、（上記に記載されているような）ＭＣＵは遠隔制御装置にプラグ接続されるが、前記ホスト・オペレーティング・システムは、前記ＭＣＵの周辺機器を管理および共有することはできない。

【００１９】

好ましい一実施形態では、前記ｈＯＳは、単に標準的なハイパーバイザにとどまらない。前記ｈＯＳは、できる限り機能は少ないが、（制御されない環境または制御されている環境で実行されている）何らかのアプリケーションを拒否するまたは何らかの優先度を与えるために、何らかのオペレーティング・プロセス（複数可）を含む。

【００２０】

本明細書では、「ゲスト・オペレーティング・システム」という表現は、一般的な機能（電話、データ送信、カレンダーなど）または特定のオペレーティング・システム（医療用オペレーティング・システムなど）を処理する標準的なオペレーティング・システム（限定するものではないが、Ａｎｄｒｏｉｄ、ＡｐｐｌｅのｉＯＳなど）として理解されなければならない。前記異なるゲスト・オペレーティング・システムは、同じ遠隔制御装置上で強固に分離して（ｉｎ　ｓｔｒｏｎｇ　ｉｓｏｌａｔｉｏｎ）共存してもよい。

【００２１】

本明細書では、「制御されている環境」は、以下の空間と理解されなければならない：
・意図されたアプリケーションの応答性が決定論的である
・ソフトウェア・パッケージおよびオペレーティング・システムのリストおよびバージョンが既知であり、ユーザによる変更が可能である
・ハードウェア構成要素へのアクセスが制御および保証されている
・ハードウェア構成要素（ＣＰＵ、メモリ、ＲＦリンクなど）の応答性が決定論的であ

る
・所定の最小帯域幅は、常に、ハードウェア構成要素（たとえば：ＣＰＵ、ネットワークＲＦリンクなど）にアクセスすることが保証されている
・少なくとも１つの医療用アプリケーションおよび／またはｍＯＳが実行および収納されている
制御されている環境と制御されていない環境は完全に分離されている。

【００２２】
その結果、制御されていない環境では、ハードウェアと制御されている環境との間の相互作用が把握できない。有利には、制御されている環境内にあるゲスト・オペレーティング・システムまたはアプリケーション（限定するものではないが、医療用オペレーティング・システムおよび／または医療用アプリケーションなど）が、他のものよりも優先される。それによって、ホスト・オペレーティング・システムは、本出願によって引き起こされる混乱を回避するために、制御されていない環境で実行されているアプリケーションをブロックすることを決定する。ホスト・オペレーティング・システムは、制御されている環境または制御されていない環境からのどのアプリケーションが画面上でフォーカスを得るか決定することもできる。

【００２３】
一実施形態では、本発明による遠隔制御装置は携帯電話である。任意の適切なＯＳ、たとえばＡｎｄｒｏｉｄを使用することができる。遠隔制御装置は、医療用デバイスと組み合わせて使用される。有利には、遠隔制御装置の機能は、インスリン・ポンプの遠隔制御装置向けに設計される。

【００２４】
外部ＭＣＵを使用する一実施形態では、前記ＭＣＵは、ｈＯＳの完全性を認証および確保するためにも使用される。

【００２５】
医療用アセンブリの一実施形態では、前記アセンブリは、有利には、両方の物体（たとえばインスリン・ポンプおよび遠隔制御装置）の間にループバック機構を備える。

【００２６】
本明細書では、ループバック機構は、ユーザによって入力されたデータの単純な確認ではない。ループバック機構は、医療用デバイスによって受信されたデータを確認することを可能にする。そのため、ユーザは、コマンドを（入力手段によって）入力し、そのコマンドを、セキュアな通信を介して医療用デバイスに送信する。前記機構により、コマンドを起動する前に、医療用デバイスは、受信したコマンドがユーザによって送信されたコマンドかどうか、確認を求めなければならない。ユーザが医療用デバイスに対して確認すると、コマンドが起動される。有利には、セキュリティを改善するために、ユーザは、コマンドを確認するためにＰＩＮコードを入力しなければならない。

【００２７】
ループバック機構のセキュリティおよび医療用デバイスへの接続性は、有利には、スマート・カードまたはＳＩＭカードまたはＳＤカードなどのような、遠隔制御装置の中への追加の保護されたＭＣＵを使用することによって保護することができる。

【発明の効果】

【００２８】
本発明は、具体的には以下の利点を提供する：
－　本発明はまた、応答性、完全性、およびセキュリティが低レベル・オペレーティング・システム・アーキテクチャのコア設計によって確保される制御されている環境を提供する。
－　提案する解決策はセキュアな環境を提供し、このセキュアな環境は、たとえば、患者が望まない追加の数回の注入をプログラムすることのように、治療法を変更することによって正常な使用法を模倣しうる望ましくないアプリケーションを防止することができる。

－　スマート・カードとして遠隔制御装置から独立したＭＣＵを使用することによって、ペアリング・プロセス中に別のデバイスから見えることなく、遠隔制御装置を自動的およびセキュアに医療用デバイスと接続することが可能になる。
－　携帯電話のような異なる遠隔制御装置に挿入またはプラグ接続されうるＭＣＵを使用することによって、問題（バッテリ電力低下、遠隔制御装置の失念または喪失など）が発生した場合に、遠隔制御装置の変更が可能になる。
－　ループバック・プロセスを使用することによって、医療用デバイス（たとえばインスリン・ポンプ）内でプログラムされた値がユーザの予想する遠隔制御装置上の値に対応することを確実にすることが可能になる。
－　ループバック・プロセスの終了時に、ユーザは、好ましくはＰＩＮコード（ユーザのみが知っている）を遠隔制御装置上で入力することによって、その値に対して肯定応答する。前記ＰＩＮコードを使用することによって、適切なユーザによって確認が承認されることが確実になる。
－　仮想プラットフォームを使用することによって、医療用アプリケーションまたはｍＯＳが優先権を持っており、セキュアに実行されることが確実になる。
－　ｈＯＳは、何らかの周辺機器（ＭＣＵ、ＬＥＤ、画面の一部、振動子など）が医療用アプリケーションおよび／またはｍＯＳのみによって使用されることを確実にする。

【００２９】
本発明について、以下の図によって示される例を用いて、以下でより詳細に説明する：

【図面の簡単な説明】

【００３０】
【図１】本発明による遠隔制御装置（３）のディスプレイを示す図である。この図は仮想化プラットフォームを含む。
【図２】本発明の好ましい一実施形態、すなわち遠隔制御装置（３）と医療用デバイス（１）とを備えるアセンブリの、全体的なアーキテクチャを示す図である。
【図３】本発明によるループバック機構を示す図である。
【図４】ＭＣＵを使用する、本発明によるループバック機構を示す図である。
【図５】スマート・カードなどのＭＣＵ（４）を内部に備える遠隔制御装置（３）と通信する医療用デバイス（１）を示す図である。
【図６】ＭＣＵ（６）にプラグ接続された遠隔制御装置（３）と通信する医療用デバイス（１）を示す図である。
【図７】スマート・カードなどの別のＭＣＵ（４）を内部に備えるＭＣＵ（６）にプラグ接続された遠隔制御装置（３）と通信する医療用デバイス（１）を示す図である。
【図８】スマート・カードなどの２つのＭＣＵ（４ａ、４ｂ）を内部に備えるＭＣＵ（６）にプラグ接続された遠隔制御装置（３）と通信する２つの医療用デバイス（１、７）を示す図である。
【図９】スマート・カードなどの２つのＭＣＵ（４ａ、４ｂ）を内部に備える遠隔制御装置（３）と通信する２つの医療用デバイス（１、７）を示す図である。
【図１０】スマート・カードなどの単一のＭＣＵ（４ｃ）を内部に備える遠隔制御装置（３）と通信する２つの医療用デバイス（１、７）を示す図である。

【発明を実施するための形態】

【００３１】
追加のマイクロコントローラ（ＭＣＵ）の使用
限定するものではないが図５～１０に示される好ましい一実施形態では、医療用デバイス（１、７）と遠隔制御装置（３）の間で保護された通信を確立するのに適した医療用アセンブリは、：
・前記医療用デバイス（１、７）との無線通信（２）を可能にする通信手段、
・追加のマイクロコントローラ（ＭＣＵ）（４、６）をプラグ接続するための接続手段、
・表示手段（場合により）、

・少なくとも１つの入力手段、
・通信手段、接続手段、表示手段、および入力手段に接続された少なくとも１つのプロセッサ；
を備える遠隔制御装置（３）と：
・前記遠隔制御装置（３）との無線通信（２）を可能にする通信手段、
・セキュアな内部メモリ；
を備える医療用デバイス（１、７）と：
・前記遠隔制御装置（３）に接続することができ；セキュアなメモリをさらに備えるＭＣＵ（４、４ａ、４ｂ、４ｃ、６）と；を備え、
ここで、少なくとも１つの医療用デバイス（１、７）は、ただ１つのＭＣＵ（４、４ａ、４ｂ、４ｃ、６）と排他的に対にされ；
前記医療用デバイス（１、７）の内部メモリおよび前記ＭＣＵ（４、４ａ、４ｂ、４ｃ、６）のセキュアなメモリは、通信をセキュアにするための鍵情報を含む。

【００３２】
前記医療用デバイス（１、７）は、（限定するものではないが、インスリン・ポンプなどの）送達デバイスおよび／または（患者の生理的特性を測定することができる）無線センサおよび／または埋め込み型デバイスおよび／またはサンプリング・デバイスであってよい。

【００３３】
遠隔制御装置（３）のプロセッサは、遠隔制御装置の主要なコンピューティング・ユニットである。このプロセッサは、遠隔制御装置のオペレーティング・システム（ＯＳ）（または複数のオペレーティング・システムＯＳ）を実行しているプロセッサであり、ＲＡＭ、Ｆｌａｓｈ、ＵＡＲＴ、Ｗｉｆｉなどの遠隔制御装置（３）のすべての周辺機器にアクセスすることができる。

【００３４】
ＭＣＵ（４、４ａ、４ｂ、４ｃ、６）もプロセッサを含み、このプロセッサは、それ自体のオペレーティング・システムおよびコードを実行する。しかし、そのプロセッサは、ＭＣＵ（４、４ａ、４ｂ、４ｃ、６）の内部周辺機器（暗号化エンジン、通信インタフェースなど）のみにアクセスすることができる。（限定するものではないが、スマート・カードなどの）ＭＣＵ（４、４ａ、４ｂ、４ｃ、６）のプロセッサは、遠隔制御装置（３）の周辺機器にアクセスすることができない。２つのデバイス（ＭＣＵ（４、４ａ、４ｂ、４ｃ、６）と遠隔制御装置（３））間の相互作用のみは、通信リンクを介して行われる。したがって、遠隔制御装置（３）のプロセッサとＭＣＵ（４、４ａ、４ｂ、４ｃ、６）のプロセッサは、互いから独立している。したがって、前記ＭＣＵ（４、４ａ、４ｂ、４ｃ、６）は、異なる遠隔制御装置にプラグ接続され、完全なセキュリティを確保することができる。

【００３５】
一実施形態では、遠隔制御装置（３）はまた、ＢＧＭ（血糖モニタ）モジュールの形態をとる別のプロセッサを有する。しかし、このプロセッサは、通信リンクを介して遠隔制御装置（３）のみと相互作用する。

【００３６】
図５に示される一実施形態では、医療用デバイス（１）は遠隔制御装置（３）と通信する。前記遠隔制御装置（３）は、（限定するものではないが、スマート・カードまたはＳＩＭカードなどの）ＭＣＵ（４）を内部に備え、ＭＣＵ（４）は、前記医療用デバイス（１）のみとペアリングされる。前記遠隔制御装置（３）と前記医療用デバイス（１）の間の通信（２）は、前記スマート・カード（４）によって起動または実行されるセキュアな処理手段（５）によりセキュリティ保護される（ｓｅｃｕｒｉｓｅｄ）。

【００３７】
一実施形態では、遠隔制御装置（３）は携帯電話であり、ＭＣＵ（４）は電話オペレータのすべてのデータおよびアプリケーションならびにペアを形成し医療用デバイス（１、

７）とセキュア通信するためのすべてのデータおよびアプリケーションを含むｓｉｍカードである。一実施形態では、前記遠隔制御装置（３）は、以降で開示される仮想化プラットフォームを備える。別の実施形態では、前記携帯電話は、２つの異なる接続手段、すなわちテレコム・オペレータのＳＩＭカードをプラグ接続するための第１の接続手段と、医療用デバイスとペアリングされたＭＣＵをプラグ接続するための別の接続手段とを備える。

【００３８】

一実施形態では、前記ＭＣＵ（４、４ａ、４ｂ、４ｃ、６）は、前記医療用アセンブリと医療用サーバ（たとえばテレメディシン（ｔｅｌｅｍｅｄｉｃｉｎｅ））の間の通信をセキュアにするための鍵情報を含む。このようにして、何らかのデータは医療用サーバにセキュアに送信することができ、医療用サーバにおいて、前記データは、分析されてもよいし、または収納されてもよい。

【００３９】

図６に示される一実施形態では、医療用デバイス（１）は、遠隔制御装置（３）と通信する。前記遠隔制御装置（３）はＭＣＵ（６）にプラグ接続され、ＭＣＵ（６）は前記医療用デバイス（１）のみとペアリングされる。前記遠隔制御装置（３）と前記医療用デバイス（１）の間の通信（２）は、前記ＭＣＵ（６）によって起動または実行されるセキュアな処理手段（５）によりセキュアにされる。

【００４０】

一実施形態では、ＭＣＵ（６）は、前述したすべての要素と他の手段とを備える外部デバイスと見なされてもよいし、またはそのような外部デバイスであってもよい。たとえば、前記ＭＣＵ（６）は、限定するものではないが血糖測定手段などのセンサを備えてもよく、このようにして前記ＭＣＵ（６）はまた、血糖モニタリングのように使用されてもよい。

【００４１】

一実施形態では、前記ＭＣＵ（６）は、遠隔制御装置に依存することなく医療用デバイスとセキュア通信するための通信手段を備えることができる。この実施形態では、遠隔制御装置は、携帯電話であってもよく、有利には、その表示手段に使用される。

【００４２】

図７に示される一実施形態では、医療用デバイス（１）は、遠隔制御装置（３）と通信する。前記遠隔制御装置（３）は第１のＭＣＵ（６）にプラグ接続され、前記第１のＭＣＵ（６）は、（スマート・カードまたはｓｉｍカードのような）第２のＭＣＵ（４）を内部に備える。前記第２のＭＣＵ（４）は、前記医療用デバイス（１）のみとペアリングされる。前記遠隔制御装置（３）と前記医療用デバイス（１）の間の通信（２）は、前記第１のＭＣＵ（６）および／または前記第２のＭＣＵ（４）によって起動または実行されるセキュアな処理手段（５）によりセキュアにされる。一実施形態では、前記ＭＣＵ（６）は、限定するものではないが血糖測定手段などのセンサを備え、このようにして前記ＭＣＵ（６）はまた、血糖モニタリングのように使用されてもよい。

【００４３】

図８および９に示される一実施形態では、２つの医療用デバイス（１、７）は遠隔制御装置（３）と通信する。たとえば、第１の医療用デバイス（１）はインスリン・ポンプ（１）であり、第２の医療用デバイス（７）は持続血糖測定器（７）である。各医療用デバイスは、それ自体のＭＣＵ（４ａ、４ｂ）のみとペアリングされる。図８に示される実施形態は、第１のＭＣＵ（６）にプラグ接続された遠隔制御装置（３）を開示する。前記第１のＭＣＵ（６）は、第２のＭＣＵおよび第３のＭＣＵ（４ａ、４ｂ）を挿入するための２つの異なる接続手段を備える。図９に示される実施形態は、第１のＭＣＵ（６）を必要とすることなく２つの異なるＭＣＵ（４ａ、４ｂ）を挿入するための２つの異なる接続手段を内部に備える遠隔制御装置（３）を開示する。第２のＭＣＵ（４ａ）（または第３のＭＣＵ（４ｂ））は、第１の医療用デバイス（１）（または第２の医療用デバイス（７））との無線通信（２）構成を含むセキュアなメモリを備える。前記第２のＭＣＵ（４ａ）

は第１の医療用デバイス（１）のみとペアリングされ、前記第３のＭＣＵ（４ｂ）は第２の医療用デバイス（７）のみとペアリングされる。実施形態では、より多くのＭＣＵと医療用デバイスとを備えてもよい。

【００４４】

図１０に示される一実施形態では、２つの医療用デバイス（１、７）は、遠隔制御装置（３）と通信するが、１つのＭＣＵ（４ｃ）がプラグ接続される。この実施形態では、前記ＭＣＵ（４ｃ）は前記２つの医療用デバイス（１、７）とペアリングされ、前記２つの医療用デバイス（１、７）との無線通信（２）構成を含む少なくとも１つのセキュアなメモリを備える。

【００４５】

上記で説明した実施形態では、１つまたは２つの医療用デバイスを使用するが、本発明はその実施形態に限定されるものではなく、本発明は、１つまたはそれ以上の医療用デバイスと、１つまたはそれ以上のＭＣＵとを有することができる。

【００４６】

一実施形態では、ペアリングは、販売の前に（たとえ工場で）、または遠隔制御装置（３）内のＭＣＵ（４、４ａ、４ｂ、４ｃ、６）をプラグ接続する前に、直接実行することができる。

【００４７】

一実施形態では、前記ＭＣＵおよび／または医療用デバイスは、新しいペアリング要求を許容することはできない。

【００４８】

一実施形態では、前記医療用デバイス（１、７）および／または前記ＭＣＵ（４、４ａ、４ｂ、４ｃ、６）は、セキュア・ブート・プロセスおよび／またはセキュア・フラッシュ・プロセスおよび／または暗号機構などのセキュアな処理手段（５）を備え、前記セキュアな処理手段（５）は、少なくとも遠隔制御装置の完全性をチェックする、かつ／または前記医療用デバイス（１、７）と前記遠隔制御装置（３）の間のデータのセキュアな通信（２）を管理する。

【００４９】

したがって、前記ＭＣＵ（４、４ａ、４ｂ、４ｃ、６）は、限定するものではないが、遠隔制御装置（３）のオペレーティング・システムおよび／またはｈＯＳおよび／またはアプリケーションなど、遠隔制御装置（３）の完全性を確保するために使用することができる。この完全性を確保するための一般的な方法は、セキュア・ブートまたはセキュア・フラッシュを使用することである。これは、遠隔制御装置（３）のブート中に、または定期的な間隔で、モニタリング・システムを介して完全性チェックを実行する機能である。

【００５０】

たとえば、セキュア・ブート・プロセスを使用する一実施形態では：遠隔制御装置（３）上で実行されているソフトウェアが偶然に（ハードウェアの故障）または意図的に（攻撃者、マルウェア）修正されていないことを確実にするために、セキュア・ブートの機構を使用する。遠隔制御装置（３）がオンにされるとき、そのプロセッサによって実行される第１のコードは、遠隔制御装置（３）の内部ストレージ（フラッシュメモリ）の内容の署名を計算し、この署名の有効性を検証するルーチンである。署名が有効であると検証されると、そのプロセッサは、その通常のＯＳ始動手順を継続する。それ以外の場合、システムは始動しない。署名の検証がＭＣＵ（４、４ａ、４ｂ、４ｃ、６）を使用して実行され、これによって、機密（鍵）が露出されないことが確実になることに留意することが重要である。

【００５１】

別の例として、セキュア・フラッシュ・プロセスを使用する一実施形態では：ユーザが、遠隔制御装置ＯＳのより新しいバージョンを利用できることが望ましい。同様に、遠隔制御装置（３）のソフトウェアを不正ソフトウェアで更新することを防止するために、書き込まれるべき新しいソフトウェアは署名されなければならない。遠隔制御装置（３）が

（たとえば、電源ボタンを長く押すことによって）更新モードで開始されると、プロセッサは第１のルーチンを実行する。この第１のルーチンは、新しいソフトウェアのイメージをダウンロードし、その署名を計算し、それを検証してから、既存のソフトウェアに上書きする。この場合も、署名の検証がＭＣＵ（４、４ａ、４ｂ、４ｃ、６）を使用して実行され、これによって、機密（鍵）が露出されないことが確実になることに留意することが重要である。

【００５２】

したがって、上記で示した一実施形態では、前記ＭＣＵ（４、４ａ、４ｂ、４ｃ、６）が存在することによって、破損したソフトウェアによるｈＯＳの置き換えが回避される。

【００５３】

一実施形態では、ＭＣＵ（４、４ａ、４ｂ、４ｃ、６）は、医療用デバイス（１、７）への無線接続を可能にする、（限定するものではないが：通信構成、公開鍵、秘密鍵、暗号プロセスなどの）鍵情報も含むことができ、医療用デバイス（１、７）も前記鍵情報を部分的または完全に知っている。前記鍵情報がなければ、医療用デバイス（１、７）に接続することは不可能である。この特徴は、医療用デバイス（１、７）が発見できないブルートゥース通信を使用することによって、説明することができる。遠隔制御装置（３）は、標準的なペアリング・プロセスを使用せずにブルートゥース接続を開始するために、リンク鍵を必要とする。この特殊な場合では、リンク鍵をＭＣＵ（４、４ａ、４ｂ、４ｃ、６）に読み込み、次にブルートゥース通信層に転送することができ、この層は接続をじかに要求することが可能である。

【００５４】

一実施形態では、前記セキュアな処理手段（５）は：

－　少なくとも１つの非対称鍵ペアおよび／または対称鍵を生成する非対称鍵暗号機構；

－　少なくとも１つの対称鍵および／または非対称鍵を生成する対称鍵暗号機構

－　暗号学的ハッシュ機構

を使用することができる。

【００５５】

前記非対称鍵暗号機構は、このアルゴリズムのうち少なくとも１つを使用することができる：Ｂｅｎａｌｏｈ、Ｂｌｕｍ－Ｇｏｌｄｗａｓｓｅｒ、Ｃａｙｌｅｙ－Ｐｕｒｓｅｒ、ＣＥＩＬＩＤＨ、Ｃｒａｍｅｒ－Ｓｈｏｕｐ、Ｄａｍｇａｒｄ－Ｊｕｒｉｋ、ＤＨ、ＤＳＡ、ＥＰＯＣ、ＥＣＤＨ、ＥＣＤＳＡ、ＥＫＥ、ＥｌＧａｍａｌ、ＧＭＲ、Ｇｏｌｄｗａｓｓｅｒ－Ｍｉｃａｌｉ、ＨＦＥ、ＩＥＳ、Ｌａｍｐｏｒｔ、ＭｃＥｌｉｅｃｅ、Ｍｅｒｋｌｅ－Ｈｅｌｌｍａｎ、ＭＱＶ、Ｎａｃｃａｃｈｅ－Ｓｔｅｒｎ、ＮＴＲＵＥｎｃｒｙｐｔ、ＮＴＲＵＳｉｇｎ、Ｐａｉｌｌｉｅｒ、Ｒａｂｉｎ、ＲＳＡ、Ｏｋａｍｏｔｏ－Ｕｃｈｉｙａｍａ、Ｓｃｈｎｏｒｒ、Ｓｃｈｍｉｄｔ－Ｓａｍｏａ、ＳＰＥＫＥ、ＳＲＰ、ＳＴＳ、Ｔｈｒｅｅ－ｐａｓｓ　ｐｒｏｔｏｃｏｌ、またはＸＴＲ。

【００５６】

一実施形態では、前記ＭＣＵのセキュアなメモリは秘密鍵を含み、前記医療用デバイスのセキュアな内部メモリは適切な公開鍵を含む。

【００５７】

遠隔制御装置（３）と医療用デバイスの間のペアリングは、以下の工程を含む：

・遠隔制御装置（３）内での前記ＭＣＵ（４、４ａ、４ｂ、４ｃ、６）の挿入、

・前記ＭＣＵ（４、４ａ、４ｂ、４ｃ、６）は、（前記ＭＣＵ（４、４ａ、４ｂ、４ｃ、６）のセキュアなメモリに含まれる）無線通信構成を使用して、医療用デバイスを遠隔制御装置（３）と接続する、

・前記医療用デバイス（１、７）は、（前記医療用デバイス（１、７）のセキュアなメモリに含まれる）前記無線通信構成を使用して、遠隔制御装置（３）と接続される、

・有利には、前記ＭＣＵ（４、４ａ、４ｂ、４ｃ、６）および前記医療用デバイス（１、７）は、暗号機構を使用してプラグ接続を認証する。

したがって、医療用デバイス（１、７）および遠隔制御装置（３）は、強制的に医療用デバイス（１、７）を他のデバイスに見えるようにする標準的なペアリング・プロセスを使用しない。

【００５８】

一実施形態では、前記ＭＣＵ（４、４ａ、４ｂ、４ｃ、６）は、前記遠隔制御装置（３）が前記セキュアな処理手段（５）にアクセスしないような形で、そのセキュアなメモリ内に前記セキュアな処理手段（５）を保つ。

【００５９】

一実施形態では、医療用デバイスも、医療用デバイスのセキュアなメモリと遠隔デバイスの間のデータの暗号化された通信を管理する前記セキュアな処理手段を備える。

【００６０】

ホスト・オペレーティング・システム（ｈＯＳ）の使用

限定するものではないが好ましい一実施形態では、ここで図１に注意を向けると、遠隔制御装置（３）のモバイル仮想化プラットフォームの使用は、遠隔制御装置（３）（たとえばスマートフォン）を、（たとえば医療用デバイス（１、７）を制御するための）制御されている環境と（たとえば汎用タスクのための）制御されていない環境に分割する可能性を提供する。仮想化プラットフォームは、仮想マシン・アプリケーションを介して定義することができる。

【００６１】

以下のアーキテクチャは、本発明による仮想化プラットフォームの非限定的な例を説明する（図１を参照されたい）：

・１つまたはいくつかのゲストＯＳ（図１では、２つのゲストＯＳのみが示されている）に対するハードウェア構成要素をエミュレートするホスト・オペレーティング・システム（ＯＳ）。

・制御されていない環境において汎用タスク（たとえば：カレンダー、連絡先、ウェブ・ブラウジング、電話通信、エンターテインメントなど）を処理する１つのゲストＯＳ

・制御されている環境において医療用デバイスとの相互作用を処理する１つのゲストＯＳ

【００６２】

有利には、ｈＯＳは、できる限り機能が少ないが、いくつかの先行するオペレーティング・プロセスを統合しており、最低レベルのオペレーティング・システム・アーキテクチャに存在する。ホスト・オペレーティング・システムは単純なハイパーバイザではない。実際には、ホスト・オペレーティング・システムは、さまざまなセキュリティ・タスクと制御タスクとをさらに含む。したがって、ホスト・オペレーティング・システムは、アクティビティを管理、協調させ、遠隔制御装置のリソースを共有し、アプリケーションの実行ならびに／または遠隔制御装置（３）のドライバおよび／もしくは周辺機器の使用を拒否および／または許可することを決定する。このようにして、悪意のあるソフトウェアは、ドライバおよび／または限定するものではないが上記で説明したようなＭＣＵなどの周辺機器にアクセスできないので、セキュリティは改善される。

【００６３】

したがって、このアーキテクチャを使用することによって、制御されている環境は、常に、医療用デバイスと交換したコマンド／情報を妨害または修正または生成するための悪意のあるあらゆるアプリケーションを防止するために、遠隔制御装置の完全な制御を有する。そのような悪意のあるアプリケーションの一般的な動作は、注入のプログラミングを模倣するために、ユーザのＰＩＮコードを盗むことである。

【００６４】

一実施形態では、この制御されている環境が認証され、その完全性は、上記で説明したＭＣＵを用いてチェックされる。遠隔制御装置のブート時には、安全チェックは前記ＭＣＵによって行われる。このチェックは、完全性を確認し、ｈＯＳおよび場合によりｍＯＳを認証するべきである。

【００６５】

このアーキテクチャに加えて、特殊なモニタリング・プログラムを実施して、制御されている環境で実行されているすべてのタスクをチェックすることができ、これによって、許可されたアプリケーションの特定のリストに含まれていないアプリケーションを無効にすることができる。この特定のモニタリングはまた、前記ＭＣＵによって制御することができる。前記モニタは、アプリケーションによって使用される実行時間を測定し、アラームをトリガすることによって、アクティビティの過負荷が疑われることをユーザに示すことが可能な場合がある。

【００６６】

一実施形態では、前記ｈＯＳは、前記ＭＣＵに含まれている、および／または起動されている、および／または実行されている。

【００６７】

一実施形態では、前記ｍＯＳは、前記ＭＣＵに含まれている、および／または起動されている、および／または実行されている。

【００６８】

一実施形態では、前記ｍＯＳおよび／または前記ｈＯＳは前記ＭＣＵに含まれている。前記ＭＣＵを遠隔制御装置に挿入すると、ＭＣＵは、遠隔制御装置上に前記ｍＯＳおよび／またはｈＯＳをインストールする。

【００６９】

一実施形態では、制御されている環境内での処理は、視覚的インジケータおよび／または音声インジケータおよび／またはＬＥＤのような他のインジケータ（振動子など）を使用して知らせることができ、これによって、現在のアプリケーションは制御されていない環境ではなく制御されている環境で実行されていることがユーザに知らされる。例として、現在のアプリケーションが制御されている環境にいるとき、緑色のＬＥＤがオンに切り替えられ、次に、制御されていない環境にユーザが戻ると、緑色のＬＥＤがオフに切り替えられることを想像することができる。また、制御されている環境にユーザがいるときＬＥＤがオフであり、制御されていない環境にユーザが戻るとＬＥＤが赤色になる「反対の」使用事例を有してもよい。

【００７０】

別の実施形態では、ｈＯＳは、画面の一部を、制御されている環境で実行されているアプリケーションに予約することができる。このようにして、ｍＯＳのみがこの空間に何かを表示することができ、制御されていない環境で実行されているアプリケーションまたは他のｇＯＳは、この空間を使用することはできない。

【００７１】

したがって、ユーザは、ｍＯＳのアプリケーションが実行されていることまたは実行されていないことがわかる。実際には、前記インジケータがユーザに正しく通知しない場合、医療用デバイスを制御しようとするまたはユーザを誤った方向に導こうとするのは、間違いなく悪意のあるアプリケーションである。

【００７２】

ループバック機構の使用

次の段落は、ループバック機構を備える本発明の好ましい一実施形態に関する。この特徴は、本発明によるアセンブリと患者が読むまたは入力する情報との間のセキュアなブリッジを確保するために、これまで開示したアーキテクチャまたは類似のレベルのセキュリティが遠隔制御装置の内部に設けられることを考慮に入れることによって、医療用デバイスと遠隔制御装置の間のセキュア通信を提供することができる。図３および４は、本発明による遠隔制御装置（３）によるループバック機構の使用を示す。

【００７３】

ループバックとは、医療用デバイス（１、７）上で実行されるコマンドが、そのパラメータと共に、オペレータによって要求されており（認証）、オペレータの希望に対応する（完全性）ことを確実にする機構である。より正確には、この機構は、最初に、遠隔制御装置（３）と医療用デバイス（１、７）の間で伝送される情報が偶然に（メモリの故障、

通信干渉）または随意的に（攻撃者、マルウェア）変更されていないことを確実なものにする。そのうえ、この機構は、コマンドがユーザによって要求されていることを確実なものにする。これらの２つの機能は、限定するものではないが、以下のタスクなどによって達成される：

－　コマンドが、そのパラメータと共に、遠隔制御装置（３）によって医療用デバイス（１、７）に伝送される。

－　医療用デバイス（１、７）が、コマンドおよびそのパラメータに基づいてチャレンジを生成し、それを遠隔制御装置（３）に返す。

－　遠隔制御装置（３）が、チャレンジから情報を抽出して、それを確認のためにユーザに対して表示する。この情報は、医療用デバイス（１、７）によって受信されるコマンドおよびそのパラメータを含む。

－　ユーザは、本人のみが知っているＰＩＮを入力することによって承認および確認を知らせる。遠隔制御装置（３）は、ＰＩＮおよびチャレンジそのものを使用してチャレンジへのレスポンスを生成する。

－　このレスポンスは医療用デバイス（１、７）に送信され、医療用デバイス（１、７）によって検証される。コマンドは、チャレンジのレスポンスが正しい場合のみ、実際に実行し始める。

【００７４】

この機構は、チャレンジ・レスポンスの特定のインスタンスの場合のみユーザの使用するＰＩＮが検証されるという点において、標準的な「ログイン」機構と異なる。このようにして、各コマンドはユーザによって検証されなければならず、したがって、悪意のあるアプリケーションは、ユーザがＰＩＮコードを入力した直後に新しいコマンドを送信することはできない。そのうえ、ユーザはＰＩＮコードを知る唯一の人物なので、別の人物が適切な遠隔制御装置または他のデバイスを用いて誤ってまたは意図的にコマンドを送信することはできない。

【００７５】

この機構はまた、ユーザに示され承認が要求される情報はターゲット・デバイスによって返される情報であるという点で、「本当によろしいですか（Ａｒｅ　ｙｏｕ　ｓｕｒｅ？）」機構を用いてユーザに対して要求されたコマンドを繰り返すだけとも異なる。何らかの改変が行われた場合、この返された値は、当初ユーザが入力した情報とは自動的に異なる。

【００７６】

前記確認は遠隔デバイスによって自動的に処理されず、したがって、悪意のあるアプリケーションは、前記確認を制御することができない。送信されたコマンドを確認するためのＰＩＮコードを知るユーザのみによって確認が許可されることが、極めて重要である。

【００７７】

好ましくは、セキュアな直接パイプが、医療用デバイスのメモリと表示される値を含む遠隔制御装置上のセキュアなバッファとの間に作成される。次に、遠隔制御装置（３）上の許可されたアプリケーションが、その値を表示し、ユーザ認証を記録し、これを使用して戻り値が構築され、この戻り値が医療用デバイスに返送される。このセキュアなパイプは、追加のＭＣＵの内部にある情報を使用して開始することができる。

【００７８】

医療用デバイス上でプログラムしたいパラメータの定義をユーザが終了すると、セキュアなパイプが開く。医療用デバイスがそれらのパラメータを使用することを可能にするためにユーザがそれらのパラメータを承認すると、セキュアなパイプが閉じる。

【００７９】

本発明によるループバック・プロセスは、好ましくは、以下の要素の実装を必要とする：

・医療用デバイス内のセキュアなメモリ領域

・医療用デバイスのセキュアなメモリ領域と遠隔制御装置の間のデータの暗号化された

通信を管理する、医療用デバイス内のセキュアなプロセス。
・遠隔制御装置内のセキュアな表示メモリ領域
・医療用デバイスと遠隔制御装置のセキュアな表示メモリ領域との間のデータの暗号化された通信を管理する、遠隔制御装置内のセキュアなプロセス。
・セキュアな表示メモリ領域から遠隔制御装置のディスプレイにデータを転送し、ユーザの肯定応答チケットを構築する、遠隔制御装置上での許可されたセキュアなプロセス。
これらの異なる要素のアーキテクチャが図２に示されている。

【００８０】

医療用デバイスが、１組のパラメータを受信すると、ループバック・プロセスが開始され、それにより、治療法のセットアップまたはアラーム設定のようなセキュリティ機構が変更される。

【００８１】

追加のＭＣＵを使用しない一実施形態では、医療用アセンブリ（少なくとも１つの医療用デバイスおよび１つの遠隔制御装置）は、
・セキュアなメモリ領域を含むことができる、前記医療用デバイス内のメモリと、
・前記セキュアなメモリ領域と遠隔デバイスの間のデータの暗号化された通信を管理する、前記医療用デバイス内のセキュアな処理手段（５）と、
・遠隔制御装置内のセキュアなメモリ領域と、
・医療用デバイスと前記メモリ領域の間のデータの暗号化された通信を管理する、遠隔制御装置内のセキュアな処理手段（５）と、
・セキュアなメモリ領域から遠隔制御装置のディスプレイにデータを転送し、ユーザの肯定応答チケットを構築する、遠隔制御装置上での許可されたセキュアな処理手段（５）とを備える。

【００８２】

プロセスは、好ましくは、以下の工程を含む：
・医療用デバイス内の組み込みソフトウェアによって行われる、
・医療用デバイスのメモリに肯定応答されなければならないパラメータを書き込む工程
・一般にチャレンジという名前である、ランダムな情報を生成する工程
・医療用デバイスと遠隔制御装置の間でセキュアなパイプを開く工程
・振動、音、ＬＥＤ、または患者に知らせる他の任意の方法のような手段によって、医療用デバイスおよび遠隔制御装置はループバック・モードであることをユーザに示す工程。
・ＫＰと呼ばれる暗号化鍵および遠隔制御装置へのチャレンジを使用することによって暗号化されたパラメータを送信する工程。
・遠隔制御装置内のソフトウェア・エンティティ１によって行われる、
・暗号化されたパラメータおよびチャレンジを受信して、遠隔制御装置のセキュアなメモリ領域に書き込む工程。
・遠隔制御装内のソフトウェア・エンティティ２によって行われる、
・ＫＰに対応する鍵である、ＫＲＣと呼ばれる鍵を使用することによってパラメータを復号する工程。これらの鍵は、対称であってもよいし、非対称であってもよい。許可されたアプリケーションは、対応する正しい鍵ＫＲＣを有することによって検証される。
・復号されたパラメータを「概要」ページに表示する工程。
・ユーザのＰＩＮコードを入力する工程。
・チャレンジ、鍵ＫＲＣ、および入力したＰＩＮコードを使用することによってこれらのパラメータの受け入れを確認する肯定応答チケットを構築する工程。
・遠隔制御装置（３）のセキュアなメモリ領域にチケットを書き込む工程。
・遠隔制御装置内のソフトウェア・エンティティ１によって行われる、
・このチケットを医療用デバイスに送信する工程。
・医療用デバイス内の組み込みソフトウェアによって行われる、
・予想されるチケットを計算する工程

・遠隔制御装置から来る肯定応答チケットを受信し検証する工程。
このプロセスは図３に示されている。チケットが検証されるとき、ループバック・プロセスは閉じており、医療用デバイス（１、７）は更新されたパラメータを使用することが可能である、この基本プロセスは、セキュアなパイプのセキュリティを改善するために、より磨きをかけてもよいし、より複雑なスキームの一部であってもよい。

【００８３】
一実施形態では、ユーザの動作を模倣するまたはＰＩＮ情報を傍受するアプリケーションを防止するために、遠隔制御装置デバイス上のランダム配列表示を使用しながら、このＰＩＮを入力してもよい。たとえば、ＰＩＮコードがユーザによって入力されるたびに異なるランダムな順序で、数字（０から９のうち５個）を表示する。

【００８４】
別の実施形態では、限定するものではないが、指紋読み取り装置または網膜読み取り装置などの別の認証手段によって、ＰＩＮを変更することができる。認証手段は、ユーザのみが知っているまたは所有していなければならない。

【００８５】
一実施形態では、前記ソフトウェア・エンティティ１と前記ソフトウェア・エンティティ２は、同じソフトウェア・エンティティであり、または、ソフトウェア・エンティティ１は遠隔制御装置（３）内の組み込みソフトウェアであってよく、ソフトウェア・エンティティ２は遠隔制御装置（３）内の許可されたアプリケーションであってよい。別の実施形態では、前記ソフトウェア・エンティティ１は上記で定義したホスト・オペレーティング・システムによって実行されており、ソフトウェア・エンティティ２は上記で説明した医療用オペレーティング・システムによって実行されている。

【００８６】
送信されたデータを暗号化する方法および前記チケットを生成する方法がいくつかあることは、当業者には理解されよう。本発明は、送信されたデータを暗号化するまたは前記チケットを生成する特定の方法に限定されない。

【００８７】
追加のＭＣＵを含む一実施形態では、プロセスは、好ましくは以下の工程を含む：
・医療用デバイス内の組み込みソフトウェアによって行われる：
・医療用デバイスのメモリに肯定応答でなければならないパラメータを書き込む工程
・チャレンジを生成する工程
・一時鍵Ｋｓ１を使用することによって前記パラメータを暗号化する工程
・振動、音、ＬＥＤ、または患者に知らせる他の任意の方法のような手段によって、医療用デバイスおよび遠隔制御装置はループバック・モードであることをユーザに示す工程。
・暗号化したパラメータを遠隔制御装置に送信する工程
・遠隔制御装置内で組み込みソフトウェアによって行われる、
・暗号化したパラメータをＭＣＵに送信する工程。
・ＭＣＵ内で組み込みソフトウェアによって行われる、
・暗号化されたパラメータおよびチャレンジを受信して、ＭＣＵのセキュアなメモリ領域に書き込む工程。
・鍵Ｋｓ１を使用することによってパラメータを復号する工程。
・復号したパラメータおよびチャレンジを遠隔制御装置のメモリに送信する工程
・遠隔制御装置内で組み込みソフトウェアによって行われる、
・復号されたパラメータを「概要」ページに表示する工程。
・ユーザに、ＰＩＮコードを入力することを促す工程。
・チャレンジ、パラメータ、および入力したＰＩＮコードを使用することによってこれらのパラメータの受け入れを確認する肯定応答チケットを構築する工程。
・遠隔制御装置のセキュアなメモリ領域にチケットを書き込む工程。
・前記チケットをＭＣＵに送信する工程

・ＭＣＵ内で組み込みソフトウェアによって行われる、
・前記チケットを受信し、ＭＣＵのセキュアなメモリ領域に書き込む工程
・一時鍵Ｋｓ２を使用することによって前記チケットを暗号化する工程
・前記暗号化したチケットを遠隔制御装置に返送する工程
・遠隔制御装置内で組み込みソフトウェアによって行われる、
・暗号化したチケットを医療用デバイスに送信する工程。
・医療用デバイス内の組み込みソフトウェアによって行われる、
・予想されるチケットを計算する工程
・遠隔制御装置から来る肯定応答チケットを受信し、復号し、検証する工程。
このプロセスは図４に示されている。チケットが検証されるとき、ループバック・プロセスは閉じており、医療用デバイスは更新されたパラメータを使用することが可能である。この基本プロセスは、セキュアなパイプのセキュリティを改善するために、より磨きをかけてもよいし、より複雑なスキームの一部であってもよい。

【００８８】
一実施形態では、遠隔制御装置内の前記組み込みソフトウェアは、上記で定義したホスト・オペレーティング・システムによって実行されており、ＭＣＵ内の前記組み込みソフトウェアは、上記で説明した医療用オペレーティング・システムによって実行されている。

【００８９】
一実施形態では、チャレンジも暗号化されてよい。

【００９０】
一実施形態では、鍵Ｋｓ１およびＫｓ２は、非対称鍵ペアまたは対称鍵であってもよいし、またはハッシング機構を使用してもよい。

【００９１】
一実施形態では、鍵Ｋｓ１とＫｓ２が同じである。

【００９２】
一実施形態では、鍵Ｋｓ１とＫｓ２は異なる。

【００９３】
一実施形態では、ユーザは、ＰＩＮコードを入力して、ループバック機構への参加（ｅｎｔｒａｎｃｅ）を確認しなければならず、そのようなＰＩＮコードはランダムに表示される配列上に入力される。

【００９４】
別の実施形態では、医療用デバイスは、患者の生理的特性を測定することができる少なくとも１つのセンサと、前記センサによって観察される第１の症状をリアル・タイムで認識するための診断手段と、前記診断手段が前記第１の症状を検出した場合に患者に警告するアラーム手段とを備える。このようにして、医療用デバイスは、遠隔制御装置によって監視され、遠隔制御装置にアラームを送信することができる。

【００９５】
一実施形態では、遠隔制御装置は、アラームが送信された場合にユーザの位置を特定するためのＧＰＳを備える。前記医療用アセンブリは、前記診断手段が前記第１の症状を検出した場合、または／および患者が自分ですることができない場合に、遠隔制御装置内のアプリケーションを起動して、患者の位置を特定し、前記位置特定を医療センターまたは他の人物に送信することができる。また、前記医療用アセンブリは、前記診断手段が前記第１の症状を検出した場合、または／および患者が自分ですることができない場合に、遠隔制御装置内のアプリケーションを起動して、生理的特性のデータを医療センターまたは他の人物に送信することができる。

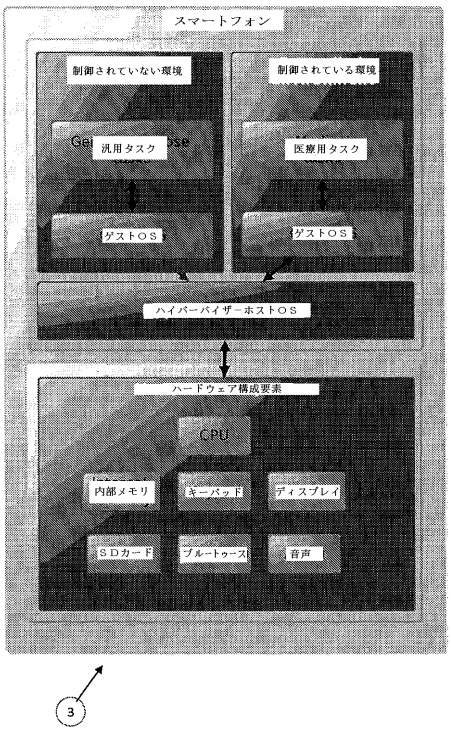
【００９６】
本発明は、当然のことながら、これまでに説明した図示の例に限定されない。

【符号の説明】

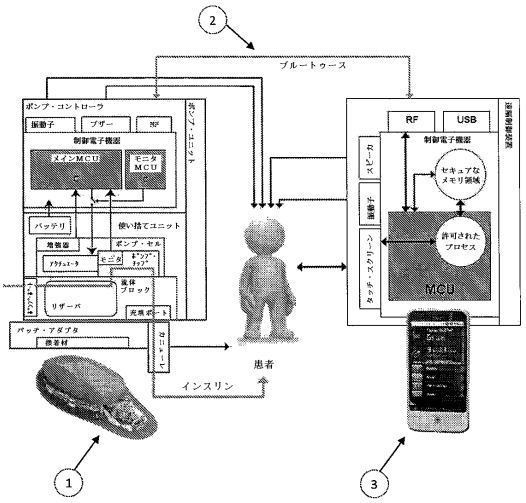
【００９７】

1　医療用デバイス
2　無線通信
3　遠隔制御装置
4、４ａ、４ｂ、４ｃ　（スマート・カードなどの）マイクロコントローラ
5　セキュアな処理手段
6　別のタイプのマイクロコントローラ
7　別の医療用デバイス

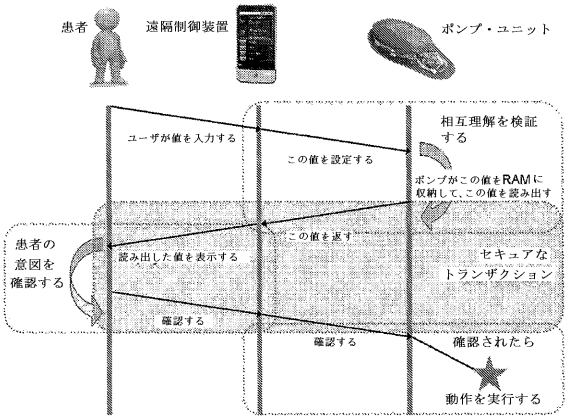
【図１】



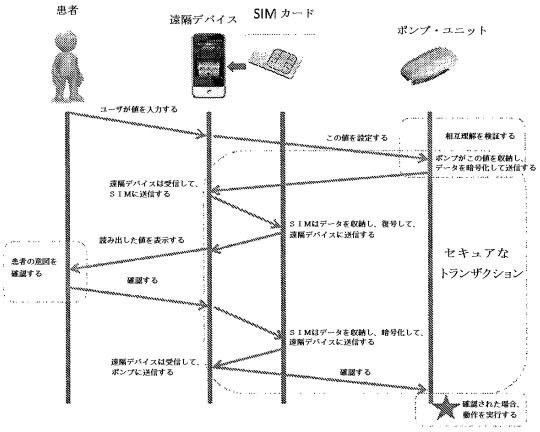
【図２】



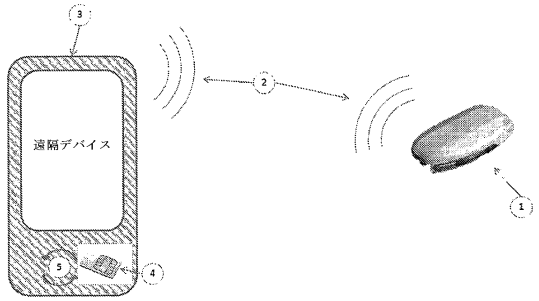
【図３】


患者
遠隔制御装置
ポンプ・ユニット
ユーザが値を入力する
この値を設定する
相互理解を検証する
ポンプがこの値をRAMに収納して、この値を読み出す
この値を返す
患者の意図を確認する
読み出した値を表示する
セキュアなトランザクション
確認する
確認する
確認されたら
動作を実行する

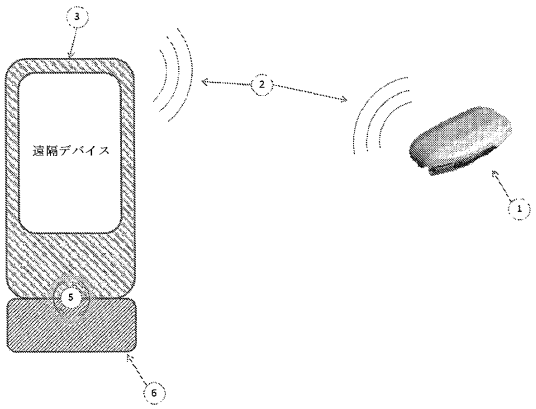
【図４】


患者
遠隔デバイス
SIM カード
ポンプ・ユニット
ユーザが値を入力する
この値を設定する
相互理解を検証する
ポンプがこの値を収納し、データを暗号化して送信する
遠隔デバイスは受信して、ＳＩＭに送信する
ＳＩＭはデータを収納し、復号して、遠隔デバイスに送信する
読み出した値を表示する
患者の意図を確認する
セキュアなトランザクション
確認する
ＳＩＭはデータを収納し、暗号化して、遠隔デバイスに送信する
遠隔デバイスは受信して、ポンプに送信する
確認する
確認された場合、動作を実行する

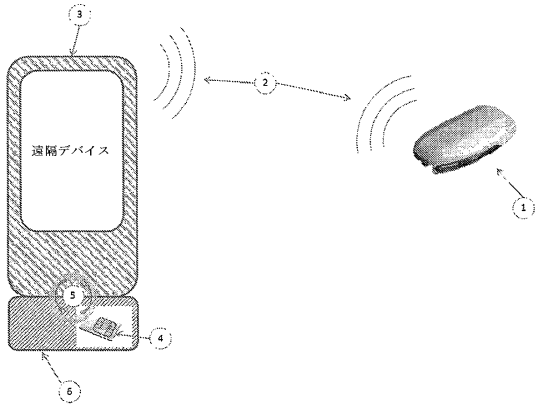
【図５】


3
遠隔デバイス
2
1
5
4

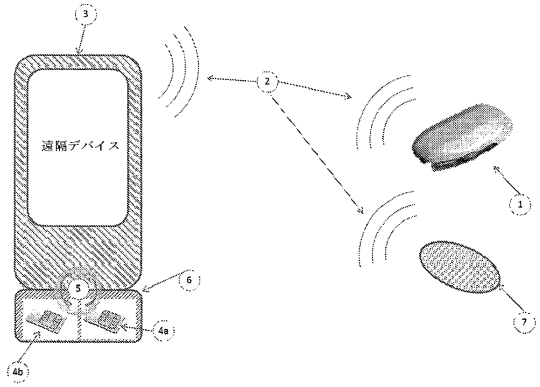
【図６】


3
遠隔デバイス
2
1
5
6

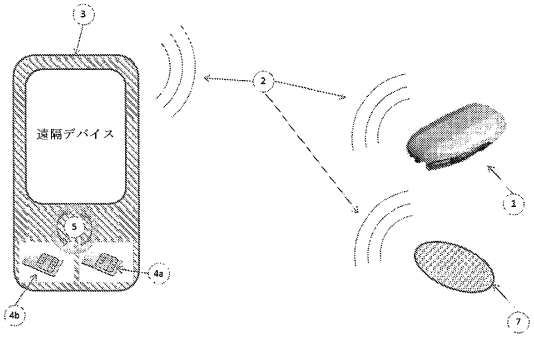
【図７】


3
遠隔デバイス
2
1
5
4
6

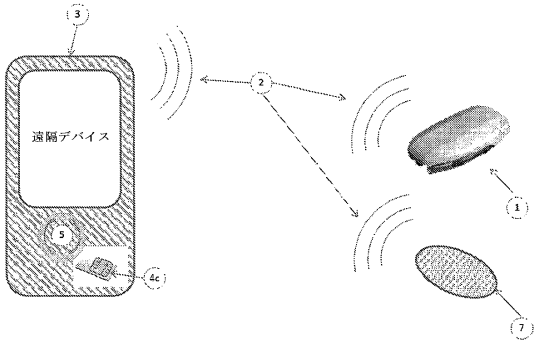
【図８】


3
遠隔デバイス
2
1
5
6
4a
4b
7

【図９】


3
遠隔デバイス
2
1
5
4a
4b
7

【図１０】


3
遠隔デバイス
2
1
5
4c
7

フロントページの続き

(51)Int.Cl. FI
A61B 5/00 102A

(72)発明者 オスカー・フランソワ
スイス国CH－1004ローザンヌ．アヴェニュ ドゥ セヴェリン28．デバイオテック・ソシエテ・アノニム
(72)発明者 フレデリク・ネフテル
スイス国CH－1005ローザンヌ．シュマン．ドゥ・ベルヴュ36

審査官 青木 重徳

(56)参考文献 特表2010－510586（JP，A）
特表2009－530880（JP，A）
特表2011－521581（JP，A）
特開2006－146337（JP，A）
特開平02－195377（JP，A）
特表2010－507928（JP，A）
特開2004－295352（JP，A）
特表2009－522060（JP，A）
中村 雄一，どっちが強い！？ Ｆｅｄｏｒａ ｖｓ．Ｖｉｓｔａ セキュリティ全面対決 Ｐａｒｔ 3，日経Ｌｉｎｕｘ，日本，日経BP社，2007年 7月 8日，第9巻、第7号，ｐ．38－43
Jacob Sorber，et ai.，Plug-n-Trust: Practial Trusted Sensing for mHealth，Proceedings of the 10th international conference on Mobile systems，applications，and services (MobiSys '12)，米国，ACM，2012年 6月25日，pp. 309-322

(58)調査した分野(Int.Cl.，DB名)
H04L 9／08
A61B 5／00
A61B 5／0215
G06F 21／70