(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6437433号
(P6437433)
(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 9/08 (2006.01)　　H04L 9/00 601C
H04L 9/32 (2006.01)　　H04L 9/00 675A
A61M 5/168 (2006.01)　　A61M 5/168

請求項の数 21　(全 35 頁)

(21)出願番号　特願2015-521119(P2015-521119)
(86)(22)出願日　平成25年7月9日(2013.7.9)
(65)公表番号　特表2015-531184(P2015-531184A)
(43)公表日　平成27年10月29日(2015.10.29)
(86)国際出願番号　PCT/IB2013/055626
(87)国際公開番号　WO2014/009876
(87)国際公開日　平成26年1月16日(2014.1.16)
審査請求日　平成28年6月21日(2016.6.21)
(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　フレデリク・ネフテル
スイス国ＣＨ－１００５ローザンヌ．シュマン．デ・ベレヴュ３６
(72)発明者　クリスチャン・グリジス
スイス国ＣＨ－１００４ローザンヌ．アヴェニュ　ドゥ　セヴェリン２８
最終頁に続く

(54)【発明の名称】医療デバイスとその遠隔デバイスの間の保護された通信

(57)【特許請求の範囲】
【請求項１】
その間を安全に無線で通信するために共に適合した第１のデバイスおよび第２のデバイスを含む医療システムであって、
ここで第１のデバイスは、第２のデバイスへのおよび第２のデバイスからの通信を伝送しそして受信するための第１の通信モジュール、ならびに、第２のデバイスとの通信を確立するためおよび／または第２のデバイスと安全に通信するために使用される少なくとも１つの必須の情報を含むメモリ、を含む医療デバイスであり、
ここで第２のデバイスは、第１のデバイスを制御するために適合した遠隔制御装置であり、前記第２のデバイスは、第１のデバイスへのおよび第１のデバイスからの通信を伝送しそして受信するための第２の通信モジュール、入力手段、電子装置接続手段、ならびに、第２の通信モジュール、入力手段および電子装置接続手段に接続されたプロセッサを含み、
前記システムはさらに、第２のデバイスの電子装置接続手段に物理的および電子的に接続されるように適合したセキュリティトークンを含み、
ここでセキュリティトークンは、第１のデバイスと第２のデバイスとの間で安全に情報を交換することを可能にする少なくとも１つの必須情報を含むメモリを含み、
ここで第１のデバイスは１つだけのセキュリティトークンと対になり、そしてここで、少なくとも１つの必須の情報は、第１の通信モジュールと第２の通信モジュールとの間の無線通信を確立するために使用されるペアリングデータであり、

ここで、前記少なくとも１つの必須の情報の少なくとも一部は、セキュリティトークンに接続された第２のデバイスだけが第１のデバイスを管理および／または監視することができるように、そして、セキュリティトークンがこの第２のデバイスから取り外されるとすぐに、この第２のデバイスがもはや第１のデバイスを管理および／または監視することができないように、第２のデバイスとは共有されない、
上記医療システム。
【請求項２】
保護されたトークンがもはや第２のデバイスとは接続されていないとき、第２のデバイスが、第１のデバイスへのおよび第１のデバイスからの通信を伝達も受信もできない、請求項１に記載のシステム。
【請求項３】
前記ペアリングデータは、第１のデバイス（１、７）のアドレス、少なくとも部分的なリンク鍵、少なくとも部分的な長期鍵、および／または少なくとも部分的な短期鍵である、請求項１または２に記載のシステム。
【請求項４】
必須の情報は、読み出しのみが可能で必須の情報は修正できないセキュリティトークン（４、６、８）のメモリ（１０）の一部分に記憶される、請求項１～３のいずれか１項に記載のシステム。
【請求項５】
トークン（４、６、８）のメモリ（１０）は秘密鍵を含み、そして第１のデバイス（１、７）のメモリは対応づけられた公開鍵を含む、請求項１～４のいずれか１項に記載のシステム。
【請求項６】
第１のデバイス（１、７）のメモリは秘密鍵を含み、そしてトークン（４、６、８）のメモリ（１０）は対応づけられた公開鍵を含む、請求項１～５のいずれか１項に記載のシステム。
【請求項７】
秘密鍵は、セキュリティトークン（４、６、８）の安全な部分に、トークンだけが前記秘密鍵を読み出し、かつ／または使用することができるようにして記憶される、請求項５に記載のシステム。
【請求項８】
セキュリティトークン（４、６、８）は、第２のデバイス（３）による秘密鍵のアクセスを防止する、請求項７に記載のシステム。
【請求項９】
少なくとも１つの必須の情報は：
－　特定の時点にトークン（４、６、８）および／または第２のデバイス（３）内で動作させることができるまたは動作させないアプリケーションおよび／またはソフトウェアのリスト、
－　アプリケーションの完全性および／またはオペレーションシステムおよび／または医療アプリケーションのアップグレードバージョンを、少なくともブート時に調べるために使用されるデータ、および／または
－　患者の識別名および／または身体の特性、
である、請求項１～８のいずれか１項に記載のシステム。
【請求項１０】
第２のデバイス（３）は、少なくとも１つの必須情報が一時的に記憶されるメモリを含む、請求項１～９のいずれか１項に記載のシステム。
【請求項１１】
前記第１のデバイス（１、７）は、第１のデバイスと第２のデバイスとの間で交換されるデータを暗号化するためのおよび／または復号するための、暗号化手段を含む、請求項１～１０のいずれか１項に記載のシステム。

【請求項１２】
少なくとも１つの必須情報は、セキュリティトークン（４、６、８）のメモリ内に秘密に保持され、そしてセキュリティトークン（４、６、８）は、第１のデバイスと第２のデバイスとの間で交換されるデータを暗号化するためのおよび／または復号するための、暗号化手段を含む、請求項１～１１のいずれか１項に記載のシステム。
【請求項１３】
セキュリティトークン（４、６、８）は、少なくとも１つの暗号鍵を生成する鍵生成器が動作中であるプロセッサを含む、請求項１～１２のいずれか１項に記載のシステム。
【請求項１４】
セキュリティトークン（４、６、８）は、第２のデバイス（３）と第１のデバイス（１、７）との間の自動的かつ確実なペアリングプロセスを、ペアリングプロセスの間に別のデバイスから見えるようにならずに、可能にするように構成される、請求項１～１３のいずれか1項に記載のシステム。
【請求項１５】
セキュリティトークン（４、６、８）は、一度だけ第１のデバイスと対にされ、そしてセキュリティトークン（４、６、８）は、別のデバイスとはもう一度対にすることはできない、請求項１～１４のいずれか１項に記載のシステム。
【請求項１６】
セキュリティトークン（４、６、８）のメモリは、セキュリティトークン（４、６、８）により書き込み可能かつ読み出し可能であるが、他のデバイスによっては書き込み不可能かつ読み出し不可能である部分を含む、請求項１～１５のいずれか１項に記載のシステム。
【請求項１７】
セキュリティトークン（４、６、８）は、特定のペアリングプロセス、データを保護するための暗号化鍵、第２のデバイスの完全性を調べるための完全性試験、ループバック機構、またはホストおよび安全なオペレーションシステムの、少なくとも１つである、保護された処理手段（５）を、さらに含む、請求項１～１６のいずれかに記載のシステム。
【請求項１８】
セキュリティトークン（４、６、８）は、スマートカード、ＳＩＭカード、ＳＤカード、またはＳＤＩＯカードである、請求項１～１７のいずれか１項に記載のシステム。
【請求項１９】
セキュリティトークン（４、６、８）は、さらに、血糖測定手段、加速度計、表示手段、または入力手段の、少なくとも１つを含む、請求項１～１７のいずれかに記載のシステム。
【請求項２０】
その間を安全に無線で通信するために共に適合した第１のデバイスおよび第２のデバイスを含む医療システムであって、
ここで第１のデバイスは、第２のデバイスへのおよび第２のデバイスからの通信を伝送しそして受信するための第１の通信モジュール、ならびに、第２のデバイスとの通信を確立するためおよび／または第２のデバイスと安全に通信するために使用される少なくとも１つの必須の情報を含むメモリ、を含む医療デバイスであり、
ここで第２のデバイスは、第１のデバイスを制御するために適合した遠隔制御装置であり、前記第２のデバイスは、第１のデバイスへのおよび第１のデバイスからの通信を伝送しそして受信するための第２の通信モジュール、入力手段、電子装置接続手段、ならびに、第２の通信モジュール、入力手段および電子装置接続手段に接続されたプロセッサを含み、
前記システムはさらに、第２のデバイスの電子装置接続手段に取り外し可能に結合されるように適合したセキュリティトークンを含み、
ここでセキュリティトークンは、第１のデバイスと第２のデバイスとの間で安全に情報を交換することを可能にする少なくとも１つの必須情報を含むメモリを含み、

ここで第１のデバイスは１つだけのセキュリティトークンと対になり、そしてここで、少なくとも１つの必須の情報は、第１の通信モジュールと第２の通信モジュールとの間の無線通信を確立するために使用されるペアリングデータを含み、
ここで、少なくとも１つの必須の情報は、第２のデバイスが、（ｉ）セキュリティトークンが現在第２のデバイスに接続されており、かつ（ｉｉ）秘密データが成功裏に認証されていた場合にのみ、第１のデバイスと通信できるように、第２のデバイスとはけっして共有されない秘密データを、さらに含む、
上記医療システム。
【請求項２１】
ペアリングプロセスが、以下の工程：
第１のデバイスとセキュリティトークンとの間の少なくとも１つの必須の情報を共有する工程；
セキュリティトークンを第２のデバイスの電子的接続手段に接続する工程；
第１のデバイスと第２のデバイスを接続するために、セキュリティトークンのメモリ中に収納されたペアリングデータを使用する工程；および
接続を認証する工程；
を含み、
ここで、認証工程は、セキュリティトークンおよび第１のデバイスにより実行される、請求項１～２０のいずれか１項に記載のシステムの使用。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、それだけには限らないが、送達デバイス（例えば、インスリンポンプ）、および／または無線センサ（例えば、連続グルコース計）、および／または埋込み可能デバイス、および／またはサンプリングデバイスなどの医療デバイスの遠隔制御に関する。
【背景技術】
【０００２】
最新技術
パッチポンプのように軽量かつ小型であるインスリンポンプのような一部の医療デバイスを制御するには、遠隔制御装置が必要とされるが、その理由は、ポンプ自体の上に設置されている表示装置の内容を患者が見ることは非常に困難なことになりうるからである。今日、大部分のポンプが専用の、メーカ独自の遠隔制御装置を使用しており、これは、この遠隔制御装置によって生じうるすべての不都合、すなわち：
・　装置を入れるためのポケットを、速く簡単に手が届く安全な場所に見つけること、
・　自分の遠隔制御装置を忘れないこと、
・　装置を充電することを思い出す、または予備電池を持っていること、
・　落下、または日光もしくは砂に曝すような、あらゆる「悪い」外部条件による装置の劣化を防止すること
を伴う別のデバイスを持ち歩くことを表す。
【０００３】
別の専用のデバイスを使用しないようにする１つの方法は、それだけには限らないが、既に患者が所持しているはずの、遠隔操作機能を組み込むために必要なすべての能力を有する血糖計または携帯電話などの既存のデバイスに、遠隔制御機能を組み込むことである。
【０００４】
この目的に携帯電話を使用することは、非常に魅力的であるが、インスリンポンプにプログラムするのに携帯電話を使用できるようにする前に対処しなければならない多くのセキュリティの側面をもたらす。確保されなければならない重要なセキュリティ機能の中には：
・　使用者に表示されるデータの完全性、

・　インスリンポンプに送られる命令の完全性、
・　患者の治療パラメータ、ならびに輸注履歴およびイベントのログを記憶するデータベースの完全性および保護、
・　医療デバイスをその遠隔制御装置と確実に対にすること、
・　あらゆる時点でのソフトウェアの応答性（例えば：別のソフトウェアに焦点がある間に警報を発すること、他のタスクがＭＣＵなどのリソースを過負荷状態にしている間に使用者要求を処理する能力など）、
がある。
【０００５】
無線通信を保護するのに、最新技術のデバイスでは、無保護または不十分な保護でデバイスが秘密を共有する認証プロセスを使用する。この認証プロセスでは、携帯電話で使用されているようなスマートカードを使用することができ、また米国特許出願（特許文献１、２、３および４）には、信頼された第三者機関として使用される、および／または認証プロセスのために使用されるトークンを含む医療デバイスが開示されている。具体的には、前記トークンは、トークンを有する患者が、関連づけられた医療デバイスを有する患者であることを証明するのに使用される。さらに、前記製品のすべてが、医療デバイスを操作するためのデータをハッカーが見つけることができるような方法で、その暗号化鍵を交換し、かつ／または標準的なペアリングプロセスを使用する。
【先行技術文献】
【特許文献】
【０００６】
【特許文献１】米国特許出願公開第２０１０／０４５４２５号
【特許文献２】米国特許出願公開第２００５／２０４１３４号
【特許文献３】米国特許出願公開第２００８／１４０１６０号
【特許文献４】米国特許出願公開第２０１１／１９７０６７号
【発明の概要】
【発明が解決しようとする課題】
【０００７】
本出願は、Ｄｅｂｉｏｔｅｃｈの名前で２０１２年１０月２６日に出願されたＰＣＴ／ＩＢ２０１２／０５５９１７の優先権、およびＤｅｂｉｏｔｅｃｈの名前で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。これら出願の開示全体を参照によって本明細書に組み入れる。
【０００８】
本発明の目的は、医療デバイスとその遠隔制御装置の間の通信を保護するための堅牢な環境を提供することである。本明細書では、「通信を保護すること」という表現は：
－　遠隔制御装置と医療デバイスの間のデータ交換が適正である、および／または
－　前記データは、許可された操作者（例えば、使用者とも呼ばれる患者）から送信されている、および／または
－　使用されるデバイスは適正なデバイスである、および／または
－　前記データは適正に受信されている、
ことを保証するために使用されるすべての手段として理解されたい。
【課題を解決するための手段】
【０００９】
したがって、通信を保護するために、前記手段では、データ、アプリケーションまたはオペレーティングシステムの完全性を調べること、および／またはデータを暗号化すること、および／または安全に対にすること、および／または操作者の身元を調べることができる。この趣旨で本発明は、医療デバイスおよび遠隔制御装置からなる医療アセンブリを含み、前記保護手段は：
－　遠隔制御装置に挿入される（あるいはプラグ接続される）追加のマイクロコントローラ（ＭＣＵ）、

－　遠隔制御装置に組み込むことができる仮想化プラットフォーム、または医療デバイスに属する追加のマイクロコントローラ、
－　特定のループバックプロセス、
－　完全性を調べる方法、
－　特定のペアリングプロセス、
－　秘密を生成および／または共有する方法、
とすることができる。前記別個の各手段を使用することにより、セキュリティを実質的に改善することが可能になるが、前記手段のうちの１つまたは２つだけを使用することもまた可能である。

【００１０】

前記遠隔制御装置は、それだけには限らないが、送達デバイス、および／または無線センサ、および／または埋込み可能デバイス、および／またはサンプリングデバイス、および／または血糖監視、．．．などの、少なくとも１つの医療デバイスを操作および／または監視するのに使用することができる。好ましくは、前記遠隔制御装置の設計は、容易に可搬式になることが可能であり、かつ軽量、可動で、ポケット内で着用可能、．．．とすることができる。

【００１１】

前記医療デバイスは、前記遠隔制御装置との無線通信を可能にする無線手段と、前記通信を確立および／または保護するための鍵情報を含む内部メモリとを含む。好ましくは、前記医療デバイスは、前記鍵情報（例えば、リンク鍵、暗号鍵、ハッシュ）をやはり含むメモリを含む、１つだけのマイクロコントローラ（ＭＣＵ）と対にされる。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。本明細書では、「～にプラグ接続する」は、「～に挿入する」または「～と接続する」に置き換えることがある。遠隔制御装置とＭＣＵの間の通信は、無線接続でも有線接続でも、接触してもしなくても行うことができる。

【００１２】

したがって、医療デバイスでは、遠隔制御装置にプラグ接続することができるＭＣＵを使用する。保護された通信を医療デバイスと遠隔制御装置の間に確立するのに適している前記アセンブリは：

・　遠隔制御装置であって：
　○　前記医療デバイスとの無線通信を可能にする通信手段、
　○　追加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、入力手段、および任意選択の表示手段に接続される少なくとも１つのプロセッサ
を含む遠隔制御装置と、
・　医療デバイスであって：
　○　前記遠隔制御装置との無線通信を可能にする通信手段、
　○　メモリ
を含む医療デバイスと、
・　前記遠隔制御装置に接続されるように設計されたＭＣＵと
を含み；前記ＭＣＵはさらに、メモリを含むことができる。

【００１３】

前記医療デバイスのメモリ、および前記ＭＣＵのメモリは、通信を確立および／または保護するための鍵情報の少なくとも一部分を含む。前記鍵情報は、共有秘密の少なくとも一部分を含む。少なくとも１つの医療デバイスは、１つだけのＭＣＵと排他的に対にされる。一実施形態では、医療デバイスとＭＣＵの間でのペアリングは、患者に使用されるのに先立って対にされる。

【００１４】

一実施形態では、ＭＣＵと遠隔制御装置の間の接続は無線通信によって行われる。

【００１５】

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る集積チップ、または遠隔制御装置にプラグ接続される外部デバイスとすることができる。一般にＭＣＵは、ＣＰＵ、ＲＡＭ、何らかの形のＲＯＭ、Ｉ／Ｏポート、およびタイマを含む。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、非常に限定された（例えば特定のシステムを制御する）タスク用に設計される。そのため、ＭＣＵは簡略化および縮小することができ、これにより製造コストが削減される。ＭＣＵはまた、開封明示シール、ロック、改ざん応答スイッチおよび抹消スイッチのような、そのメモリ内容を保護するための特殊な機能を組み込むこともできる。さらに、前記ＭＣＵは、遠隔制御装置の性能を向上させるために（遠隔制御装置の）ＯＳが使用することができる別のＣＰＵおよびメモリが付いて来ないが、他の機能を、具体的にはさらなるセキュリティを、具体的には、ペアリングプロセスまたは他のプロセスによって生成された共有秘密の少なくとも一部分が付いて来る。遠隔制御装置のＭＣＵとＣＰＵは異なっており、異なるタスクを有する。本発明では、ＭＣＵは、別々の遠隔制御装置でＭＣＵを使用することができるような方法で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（保護デジタル入出力）などのＳＤカード、内部または外部ドングルとすることができる。本明細書では、次の用語：内部もしくは外部マイクロプロセッサ、追加のマイクロプロセッサまたはＭＣＵ、を差別せずに使用することがある。

【００１６】

一実施形態では、前記医療デバイスおよび前記ＭＣＵは、無線通信構成（リンクキー、医療デバイスのアドレス（例えば、ブルートゥースアドレス）、．．．）を含むメモリを含む。このようにして、前記デバイスおよび前記ＭＣＵには、適切な構成があらかじめ分かる。特に、前記ＭＣＵは、遠隔制御装置を医療デバイスに接続するために、また前記通信を保護するために使用される鍵情報（例えば、リンクキー、．．．）を、それが無保護で（例えば、ブルートゥースによって）与えられる必要がなくなるように、または使用者（例えば、患者）が、遠隔制御装置を医療デバイスと対にする特定のタスクを実施しなくてもよくなるように、含むことができる。

【００１７】

好ましくは、医療デバイスは１つだけのＭＣＵと対にされ、前記ＭＣＵは遠隔制御装置に挿入される；そのようにして、前記ＭＣＵを含む遠隔制御装置だけが前記医療デバイスを操作および／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、医療デバイスを操作および／または監視することができるただ一つの遠隔制御装置であることを知りながら、遠隔制御装置を変更することもできる。

【００１８】

一実施形態では、遠隔制御装置は、少なくとも２つの医療デバイスを操作および／または監視する。この場合、前記医療デバイスは、１つだけのＭＣＵと対にされてよく、あるいは、それぞれの医療デバイスは、それ自体のＭＣＵと対にされる。

【００１９】

一実施形態では、前記ＭＣＵは、前記医療アセンブリを医療サーバと接続するための鍵情報（患者識別名、医療サーバの識別名およびアドレス、暗号化鍵、．．．）を含む。この実施形態では、医療アセンブリは、受信データを医療サーバに送信するのに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、１つまたはそれ以上の医療デバイスと医療サーバの間の通信を確立し保護するための、それだけには限らないが、使用者確認、暗号化パラメータ、．．．などのすべての情報を含むことができる。

【００２０】

一実施形態では、ＭＣＵは、そのメモリ内に、医療デバイスから送信された少なくとも一組のデータ、または遠隔デバイスもしくは別のデバイスから供給された別の組のデータ

を記憶することができる。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デバイス内に記憶されるが、ＭＣＵ（または医療デバイス）だけが前記データを復号するための鍵を含む。

【００２１】

さらなるセキュリティのために、前記鍵情報は、製造者、医師、介護者または薬剤師によって生成され、患者に使用されるのに先立って前記メモリ内に記録される。

【００２２】

遠隔制御装置で仮想化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）のハードウェア部材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、

・　無制御の環境で使用されるようにすべてが設計されている、それだけには限らないが、カレンダ、連絡先などの共通機能を操作する第１のｇＯＳと、

・　制御された環境内で使用されるようにすべてが設計されている医療デバイス用遠隔制御機能を操作する医療オペレーティングシステム（ｍＯＳ）と、

を含む仮想化プラットフォームを内蔵する。前記ｍＯＳは特定のｇＯＳでありうる。

【００２３】

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、フラッシュ、ＵＡＲＴ、ＷｉＦｉ、．．．などのすべての遠隔制御周辺装置を単独で操作および共有すべき、強化ハイパーバイザなどの可能な限り薄いオペレーティングシステムとして理解されたい。ｈＯＳは、共通機能を操作せず、その目的は、医療デバイスに送信されたコマンドを保護することである。

【００２４】

一実施形態では、ＭＣＵ（上記で見つけられたようなもの）が遠隔制御装置にプラグ接続されるが、前記ｈＯＳは、必ずしも前記ＭＣＵの周辺装置を操作および共有しない。一実施形態では、ＭＣＵは、各オペレーティングシステムの完全性を調べるための手段またはデータを含む。

【００２５】

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、共通機能（電話をかける、データを送信する、カレンダ、．．．）を操作する標準的オペレーティングシステム（それだけには限らないが、アンドロイド、ＡｐｐｌｅのｉＯＳ、．．．など）として、または特別のオペレーティングシステム（医療オペレーティングシステムなど）として理解されたい。前記別個の各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に互いに強く分離して共存することができる。

【００２６】

本明細書では、「制御された環境」という表現は：

・　意図されたアプリケーションの応答性が決定的である、

・　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は分かっており、使用者が変更することができない、

・　ハードウェア部材へのアクセスが制御され保証される、

・　ハードウェア部材（ＣＰＵ、メモリ、ＲＦリンクなど）の応答性が決定的である、

・　ハードウェア部材（例えば、ＣＰＵ、ネットワークＲＦリンクなど）にアクセスするために、所定の最小帯域幅が常に保証される、

・　少なくとも１つの医療アプリケーションおよび／またはｍＯＳが動作され記憶される、

空間として理解されたい。制御された環境および無制御の環境は、完全に分離される。

【００２７】

好ましい実施形態では、前記ｈＯＳは標準的ハイパーバイザを越える。前記ｈＯＳは、可能な限り薄いが、一部のアプリケーション（無制御の環境または制御された環境で動作する）を拒絶するための、または医療ＯＳにいくつかの優先権を与えるためのいくつかの動作プロセスを含む。したがって、ｈＯＳは、制御された環境が起動されたときに、また

は制御された環境のすべてまたは一部のアプリケーションが動作中であるときに、無制御の環境内で動作するアプリケーションのすべてまたは一部を止めることができる。例えば、ｈＯＳは、電話がメッセージを受信した場合でも医療アプリケーションだけを表示する。

【００２８】

結論として、無制御の環境には、ハードウェアと制御された環境との間の対話に対する可視性がない。有利なことに、制御された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（それだけには限らないが、医療オペレーティングシステムおよび／または医療アプリケーション）は、他のものに対して優先権を有する。それによって、ホストオペレーティングシステムは、無制御の環境内で動作するアプリケーションを、このアプリケーションによって引き起こされるいかなる摂動も回避するために、阻止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また、制御された、または無制御の環境からのどのアプリケーションが画面上に焦点するかを決定することができる。

【００２９】

一実施形態では、本発明による遠隔制御装置は、携帯電話（例えば、スマートフォン）である。適切な任意のＯＳを使用することができる（例えば、アンドロイド）。遠隔制御装置は、医療デバイスと一緒に使用される。有利には、遠隔制御機能は、インスリンポンプの遠隔制御用に設計される。

【００３０】

上述のように、前記ＭＣＵはまた、ｈＯＳの完全性を認証もしくは保証するために、または他のものに対して優先権を有するアプリケーションのリストを記憶するために、またはどれかのアプリケーションが動作中である、もしくは動作中でないときに、または特定の条件が満たされたときに実行する様々なシナリオを記憶するために、使用することもできる。

【００３１】

医療アセンブリの別の実施形態では、前記アセンブリは有利なことに、少なくとも２つの対象物（例えば、インスリンポンプおよび遠隔制御装置）の間のループバック機構を含む。ループバックの一般的概念は、メッセージまたは信号が、それが出発したところに最後に行き着く（すなわちループ）バックするための機構である。

【００３２】

本明細書では、ループバック機構は、使用者によって入力されたデータの単純な確認ではない。例えば、標準的なループバック機構は、使用者にコマンドを確認したかどうかを尋ねるデバイスで使用される。この標準的な場合では、ループバックは使用者とデバイスの間にある。

【００３３】

この新規のループバック機構では、遠隔制御装置から送信され医療デバイスで受信されるデータを確認することが可能になる。したがって、使用者は遠隔において（入力手段を用いて）コマンドを入力し、遠隔制御装置はこれを、保護された通信によって医療デバイスへ送出する。前記機構により、コマンドが起動される前に医療デバイスは、受信されたコマンドが使用者から送信されたコマンドであるかどうかの確認を求めなければならない。医療デバイスは、遠隔制御装置によって表示されるデータを遠隔制御装置に送信する。前記データは、呼掛け（ｃｈａｌｌｅｎｇｅ）または暗号化データ、または他のものでありうる。使用者が医療デバイスに確認すると、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、使用者は、コマンドを確認するのにＰＩＮコードを入力しなければならない。

【００３４】

ループバック機構のセキュリティ、および医療デバイスとの接続性は、有利には、スマートカードまたはＳＩＭまたはＳＤカード．．．のような保護された追加のＭＣＵを遠隔制御装置の中に使用することによって保護することができ、このＭＣＵは、ループバックのデータを暗号化または復号することができる。

【００３５】
遠隔制御装置またはＭＣＵ（例えば、外部ドングル）または医療デバイスは、情報を患者に安全に送信するための追加手段（例えば、ＬＥＤ、バイブレータ、表示手段、．．．）を含むことができる。例えば、外部ＭＣＵは、それ自体の表示手段でデータを表示することができる。
【００３６】
本発明は、以下の優位点のうちの少なくとも１つを示す：
－　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、制御された環境を提供する。
－　提案の解決策は、例えば、患者が望まないいくつかの追加輸注をプログラムするような、治療を変更することによって正常な使用法を模倣することもできるいかなる望ましくないアプリケーションも防止できる、保護された環境を提供する。
－　スマートカードのように遠隔制御装置から独立しているＭＣＵを使用することにより、遠隔制御装置を医療デバイスと自動的かつ確実に接続することが、ペアリングプロセス時に別のデバイスから見えるようにならずに可能になる。
－　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することができるＭＣＵを使用することにより、もし問題（電池電力低下、遠隔制御装置を忘れるか失う、．．．）があれば遠隔制御装置を変えることが可能である。この場合、使用者は、自分の医療デバイスを保持し、新しい遠隔制御装置を介してその医療デバイスに安全にアクセスすることができ、ＭＣＵは、遠隔制御装置メモリに記録されたデータのプライバシーを確保することができる。
－　ループバックプロセスを使用することにより、医療デバイス（例えば、インスリンポンプ）にプログラムされた値が、使用者に期待される値に一致することが遠隔制御装置によって確実になりうる。
－　ループバックプロセスの最後に、使用者はその値を、好ましくはＰＩＮコード（使用者だけが知っている）を遠隔制御装置で入力することによって確認する。前記ＰＩＮコードを使用することにより、適正な使用者によって確認が承認されることが確実になる。
－　仮想化プラットフォームを使用することにより、医療アプリケーションまたはｍＯＳが優先すること、および安全に動作することが確実になる。
－　ｈＯＳは、いくつかの周辺装置（ＭＣＵ、ＬＥＤ、画面の一部、バイブレータ、．．．）が医療アプリケーションおよび／またはｍＯＳによってのみ使用されることを保証する。
【００３７】
本発明について、以下の図に示された例を用いてより詳細に以下で論じる。
【図面の簡単な説明】
【００３８】
【図１】仮想化プラットフォームを含む本発明による遠隔制御装置（３）の表示装置を示す図である。
【図２】本発明の好ましい実施形態の全体アーキテクチャ、すなわち遠隔制御装置（３）および医療デバイス（１）を含むアセンブリを示す図である。
【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（４）などのＭＣＵを内部に含む遠隔制御装置（３）と通信する医療デバイス（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）と通信する医療デバイス（１）を示す図である。
【図７】スマートカード（４）などの別のＭＣＵを内部に含むＭＣＵ（６）にプラグ接続された遠隔制御装置（３）と通信する医療デバイス（１）を示す図である。
【図８】スマートカード（４ａ、４ｂ）などの２つのＭＣＵを内部に含むＭＣＵ（６）にプラグ接続された遠隔制御装置（３）と通信する２つの医療デバイス（１、７）を示す図

である。
【図９】スマートカード（４ａ、４ｂ）などの２つのＭＣＵを内部に含む遠隔制御装置（３）と通信する２つの医療デバイス（１、７）を示す図である。
【図１０】スマートカード（４ｃ）などの単一のＭＣＵを内部に含む遠隔制御装置（３）と通信する２つの医療デバイス（１、７）を示す図である。
【図１１】ＭＣＵ（８）の包含物（ｃｏｎｔａｉｎｅｄ）を示す図である。
【図１２】スマートカード（４ｂ）などの別のＭＣＵを内部に含む外部ＭＣＵ（６）にプラグ接続された遠隔制御装置（３）と通信する２つの医療デバイス（１、７）を示す図である。
【図１３】ペアリングデバイス（１６）を示す図である。
【図１４】共有できる少なくとも１つの秘密を示す図である。
【図１５】分離可能な、小型遠隔制御装置として使用可能な外部ＭＣＵ（６）を示す図である。
【図１６】第１の表示手段（１８）および少なくとも１つの保護された表示手段（１９）を含む遠隔制御装置（３）を示す図である。
【図１７】本発明によるセッション鍵生成を示す図である。
【発明を実施するための形態】
【００３９】
以下の詳細な説明では、説明の一部分を成し、デバイス、システムおよび方法のいくつかの実施形態が例示的に示されている添付の図面を参照する。他の実施形態が企図され、かつ本開示の範囲および趣旨から逸脱することなく作られる可能性があることを理解されたい。したがって、以下の詳細な説明は限定的な意味で解釈されるべきではない。
【００４０】
本明細書で用いられているすべての科学用語および技術用語は、特にことわらない限り、当技術分野で一般に用いられている意味を有する。本明細書で提示された定義は、本明細書で頻繁に用いられる特定の用語を理解しやすくするものであり、本開示の範囲を限定するものではない。
【００４１】
本明細書および添付の特許請求の範囲では、「ａ」、「ａｎ」および「ｔｈｅ」の単数形は、内容で特に明示されない限り、複数の指示物を有する実施形態を包含する。
【００４２】
本明細書では、「ｈａｖｅ（有する）」、「ｈａｖｉｎｇ（有する）」、「ｉｎｃｌｕｄｅ（含む）」、「ｉｎｃｌｕｄｉｎｇ（含む）」、「ｃｏｍｐｒｉｓｅ（備える、含む）」、「ｃｏｍｐｒｉｓｉｎｇ（備える、含む）」などは、それらの制限を設けない意味で用いられ、一般には「含んでいるが、それだけには限らない」を意味する。
【００４３】
本明細書および添付の特許請求の範囲では、「または」という用語は、内容で特に明示されない限り、「および／または」を含む意味で一般に用いられる。
【００４４】
本明細書および添付の特許請求の範囲では、「ノード」という用語は、以下の用語を置き換えるのに使用されることがある：医療デバイス、医療サーバ、ＢＧＭ（血糖計）、ＣＧＭ（連続グルコースモニタ）、遠隔制御装置、携帯電話、．．．。
【００４５】
本明細書および添付の特許請求の範囲では、「ＭＣＵ」という用語は、以下の用語を参照するのに使用されることがある：ドングル、内部ＭＣＵまたは外部ＭＣＵ。
【００４６】
本発明は、独立請求項において記述され特徴づけられており、従属請求項には本発明の他の特徴が記載される。
【００４７】
追加マイクロコントローラ（ＭＣＵ）の特徴

好ましい実施形態では、医療デバイス（１、７）と遠隔制御装置（３）の間に通信を確立し保護するのに適している医療アセンブリは：
・　遠隔制御装置（３）であって：
　○　前記医療デバイス（１、７）との無線通信（２）を可能にする通信手段、
　○　追加マイクロコントローラ（ＭＣＵ）（４、６、８）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、入力手段、および任意選択の表示手段に接続される少なくとも１つのプロセッサ
を含む遠隔制御装置と、
・　医療デバイス（１、７）であって：
　○　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、
　○　メモリ
を含む医療デバイスと、
・　前記遠隔制御装置（３）に接続されるように設計されたＭＣＵ（４、６、８）と
を含み；前記ＭＣＵ（４、６、８）はさらに、メモリを含む；
前記医療デバイス（１、７）のメモリ、および前記ＭＣＵ（４、６、８）のメモリは、通信を確立し保護するための鍵情報を含む。

【００４８】

前記医療デバイス（１、７）は、送達デバイス（それだけには限らないが、インスリンポンプなど）、および／または無線センサ（これは患者の生理学的特性を測定することができる）、および／または埋込み可能デバイス、および／またはサンプリングデバイスとすることができる。

【００４９】

一実施形態では、少なくとも１つの医療デバイス（１、７）は、１つだけのＭＣＵ（４、６、８）と排他的に対にされる。前記鍵情報は、医療デバイスおよび／またはＭＣＵの安全なメモリ内にすべてまたは一部を記憶することができる。一実施形態では、ＭＣＵは、ＭＣＵを別の医療デバイスと対にすることができなくなるように、一度だけ対にされる。

【００５０】

前記遠隔制御装置は、前記ＭＣＵにプラグ接続するための接続手段を含む電話、血糖計、または他の携帯型デバイスとすることができる。

【００５１】

遠隔制御装置（３）のプロセッサは、この遠隔制御装置の主計算ユニットである。これは、遠隔制御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）を動作させるものであり、ＲＡＭ、フラッシュ、ＵＡＲＴ、Ｗｉｆｉなどのすべての遠隔制御装置（３）の周辺装置にアクセスすることができる。

【００５２】

ＭＣＵ（４、４ａ、４ｂ、４ｃ、６、８）はまた、それ自体のオペレーティングシステムおよびコードを動作させるプロセッサも含む。このプロセッサは、ＭＣＵ（４、４ａ、４ｂ、４ｃ、６、８）の内部周辺装置（暗号エンジン（ｃｒｙｐｔｏ　ｅｎｇｉｎｅ）、通信インターフェース、鍵生成器など）にアクセスすることができる。ＭＣＵ（４、４ａ、４ｂ、４ｃ、６、８）のプロセッサは、遠隔制御装置（３）の周辺装置のすべてまたは一部にはアクセスできないことがある。２つのデバイス（ＭＣＵ（４、４ａ、４ｂ、４ｃ、６、８）と遠隔制御装置（３））の間の対話だけが、通信リンクを介してデータを交換する。遠隔制御装置（３）のプロセッサとＭＣＵ（４、４ａ、４ｂ、４ｃ、６、８）のプロセッサは、互いに独立している。遠隔制御装置（３）は、ＭＣＵ内に記憶されているデータへのアクセスが限定されているか、またはアクセスすることができない。したがって、前記ＭＣＵ（４、４ａ、４ｂ、４ｃ、６、８）は、別個の遠隔制御装置にプラグ接続し

、全体のセキュリティを確保することができる。
【００５３】
前記ＭＣＵ（４、４ａ、４ｂ、４ｃ、６、８）は、汎用集積回路カード（スマートカード、ＳＩＭカード、ＳＤカード、ＳＤＩＯカード、．．．）とすること、または他の、遠隔制御装置にプラグ接続されるかもしくは挿入されるように、または少なくとも遠隔制御装置（３）の接続手段に接続されるように設計されている、外部デバイスとすることができる。
【００５４】
図１１に開示されている一実施形態では、ＭＣＵ（４、４ａ、４ｂ、４ｃ、６、８）は、中央処理ユニット（ＣＰＵ）（９）と、遠隔制御装置に接続されるように設計された接続手段（１７）と、少なくとも１つのメモリ（１０）とを含み、このメモリはいくつかの（例えば４つの）個別部分：
－　ＣＰＵおよび他のデバイス（例えば、ＭＣＵがプラグ接続されている遠隔制御装置）によって書き込み可能かつ読み出し可能である第１の部分（１１）、
－　ＣＰＵによって書き込み可能かつ読み出し可能であるが、他のデバイスによっては書き込み可能で読み出し不可能である第２の部分（１２）、
－　ＣＰＵによって書き込み可能かつ読み出し可能であるが、他のデバイスによっては書き込み不可能で読み出し可能である第３の部分（１３）、および
－　ＣＰＵによって書き込み可能かつ読み出し可能であるが、他のデバイスによっては書き込み不可能かつ読み出し不可能である第４の部分（１４）、
を含むことができる。
【００５５】
図５に示された一実施形態では、医療デバイス（１）は遠隔制御装置（３）と通信する。前記遠隔制御装置（３）は、もとから前記医療デバイス（１）と対にすることができるＭＣＵ（４）と接続される。前記遠隔制御装置（３）と前記医療デバイス（１）の間の通信（２）は、前記ＭＣＵ（４）および／または前記医療デバイスによって起動または実行される保護された処理手段（５）により、確立され保護される。前記メモリは、医療デバイスまたは医療サーバとの通信を確立し保護するための全情報（鍵情報）を収容する。
【００５６】
一実施形態では、鍵情報は、特定の時点にＭＣＵ内および／または遠隔制御装置（３）内で動作させることができる、またはできないアプリケーションおよび／またはソフトウェアのリストを含む。前記ソフトウェアまたはアプリケーションのいくつかは、医療アプリケーションまたは他の特定のアプリケーションが遠隔制御装置（３）またはＭＣＵ（４）内で使用中の場合に同時に動作することを許可することも、または停止することもできる。遠隔制御装置が仮想マシンを含む場合、ハイパーバイザは、医療ＯＳが使用されるときに、または特定の医療アプリケーションが動作中であるときに、前記リストを使用して無許可のアプリケーションおよび／またはソフトウェアを起動または停止（キル）する。前記ＭＣＵ（４）は、特定の条件が満たされたときに実行予定のシナリオのリストを含むことができる。
【００５７】
図６は、遠隔制御装置にプラグ接続された外部ＭＣＵ（６）を示す。前記ＭＣＵ（６）は、ＣＰＵ、メモリ（１０）および接続手段（１７）を含み、かつハウジングを含むことができる。前記メモリは、医療デバイスまたは医療サーバとの通信を保護するための全情報を含む。前記医療デバイスは、もとから前記外部ＭＣＵ（６）と対にすることができる。前記遠隔制御装置（３）と前記医療デバイス（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保護された処理手段（５）により、確立され保護される。前記医療デバイスはまた、前記保護された処理手段のすべてまたは一部を使用することもできる。
【００５８】
図５と図６の間の相違はＭＣＵである。第１のもの（図５）は、遠隔制御装置（３）の

中に少なくとも一時的に挿入される、（スマートカードのような）内部ＭＣＵ（４）である。第２のもの（図６）は、遠隔制御装置（３）に少なくとも一時的にプラグ接続される、（ドングルのような）外部ＭＣＵ（６）である。その設計により、外部ＭＣＵ（６）は、後で開示する他の機能および手段を含むことができる。

【００５９】

保護された処理手段（５）は：

－　特定のペアリングプロセス、および／または

－　データを保護するための暗号化鍵、および／または

－　遠隔制御装置の完全性を調べるための完全性試験、および／または

－　特定のループバック機構、および／または

－　ホストおよび安全なオペレーティングシステム

を使用することができる。

【００６０】

保護された処理手段（５）は、通信を確立し保護するための鍵情報を必要とする。これは、リンク鍵、アドレス（アドレスブルートゥース、．．．）、暗号化鍵、共有秘密、ハッシュ、．．．でありうる。

【００６１】

一実施形態では、ＭＣＵ（４、６、８）は、その保護されたメモリ内に保護された処理手段（５）を、前記遠隔制御装置（３）が前記保護された処理手段（５）にアクセスしないように保持する。一実施形態では、医療デバイスはまた、（例えば）暗号化通信を処理するための前記保護された処理手段を含む。

【００６２】

一実施形態では、保護された処理手段（５）は：

・　少なくとも１つの非対称鍵対および／または対称鍵を生成する非対称鍵暗号法機構、

・　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法機構、

・　暗号ハッシュ機構

を使用することができる。

【００６３】

前記非対称鍵暗号法機構は、このアルゴリズム：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のうちの少なくとも１つを使用することができる。

【００６４】

ペアリングプロセス

本発明の一部分では、ブルートゥースプロトコル（「クラッシック」ブルートゥースまたはブルートゥースローエネルギーなど）および／または他の無線通信プロトコル（長距離または短距離インターフェース）を使用できる、特定のペアリングプロセスを開示する。具体的には、遠隔制御装置と医療デバイスの間のペアリングは、ＭＣＵが既に少なくとも１つの医療デバイスと対にされており（少なくともＭＣＵは、少なくとも１つの医療デバイスのペアリング情報を含む）、使用者による特定のペアリング操作を必要としないので、使用者にやさしい。加えて、ペアリング情報は使用者には見えず、これは、ペアリング情報が盗まれる、または第三者によって使用される可能性がなく、かつ医療デバイスがもはやペアリングプロセスのためにアクセス可能になりえないことを意味し、このことがデバイスを、ペアリングプロセスによって生じる無許可接続、および電池の過剰消耗から

守る。

【００６５】

本明細書では、新規のペアリングプロセスの利点、および標準的ブルートゥースペアリングプロセスとの相違について説明する。しかし、新規のプロセスおよび製品は、ブルートゥースプロトコルに限定されない。

【００６６】

ブルートゥースペアリングは一般に、デバイス使用者によって手動で開始される。ブルートゥースペアリングプロセスは通常、２つのデバイスがまだ対にされていないときに、最初に起動される。したがって、１つのデバイスがもう一方のデバイスから接続要求を受ける。ブルートゥースペアリングが行われうるようにするには、パスワードが２つのデバイス間で交換されなければならない。このパスワード、すなわちより適正に呼ばれるときの「合鍵」は、両方のブルートゥースデバイスによって共有されるコードである。この「合鍵」は、ブルートゥースパイプとは別の通信パイプ（通常これは、使用者によって表示され入力される）を使用することによって、交換されなければならない。これは、両方の使用者が互いに対になることに同意したことを保証するために使用される。しかし、ハッカーがこのプロセスを見るか、または聴いた場合、ハッカーは、デバイスへの接続を遮断し、デバイスに命令することもできる。標準的なペアリングプロセスの終わりに、リンク鍵が生成され、両方のデバイスで共有されると共に、対にされたデバイス間で通信を確立するために使用される。ブルートゥースローエネルギーでは、リンク鍵よりむしろ短期鍵および／または長期鍵を使用するが、本明細書を簡単にするために、リンク鍵という用語も短期鍵または長期鍵の代わりに用いられる。

【００６７】

したがって、安全な接続を確立するには、デバイスは、隠された方法で秘密を共有する必要がある。この共有された秘密は、医療デバイスおよびその遠隔制御装置だけに知られている必要がある。このような共有秘密を前もって両方のデバイスに組み入れることによって、秘密情報を交換する必要がなくなる。それでも、患者が自分の遠隔制御装置を変更する場合には、それまでの遠隔制御装置は、別の新しいデバイスと秘密を共有することができず、したがって、新しいデバイスは医療デバイスと接続することができない。

【００６８】

本発明により、遠隔制御装置と医療デバイスの間の通信は完全に保護され、共有された秘密は、医療デバイスと、いくつかの遠隔制御装置（旧および新）の間で移転可能である医療デバイスのＭＣＵとによって、安全に保持される。さらに、医療デバイス（１、７）は、他のデバイスによっては決して見つけることができず、前記ＭＣＵがなければデバイスと接続することもできない。

【００６９】

さらなるセキュリティのために、医療デバイスとＭＣＵの間のペアリングは、患者に使用されるのに先立って、または少なくともＭＣＵを遠隔制御装置の中にプラグ接続するのに先立って、行われる。有利なことに、前記ペアリング（医療デバイス／ＭＣＵ）は、ペアリングデバイスを用いて行うことができるだけであり、かつ／または前記ペアリングは、製造者、医師、介護者または薬剤師によって行うことができる。前記ペアリングにより、少なくとも１つの秘密が生成され、医療デバイス（１）に、また対にされたＭＣＵ（４、６、８）に、安全な方法で記憶される。例えば、ペアリングデバイスが要求された場合に、ペアリングプロセスは有線通信を介して行われてもよい。

【００７０】

医療デバイス（１）は、医療デバイスが標準的なブルートゥースプロトコルによって見つからない場合でも、ＭＣＵが、第三者によってハッキングされる可能性のある機密情報を交換することなく前記医療デバイスとの通信を確立できるように、ＭＣＵ（４、６、８）のメモリに記憶できるアドレス（例えば、ブルートゥースアドレス）を有する。

【００７１】

したがって、ＭＣＵと医療デバイスの間のペアリングにより、秘密のすべてまたは一部

を共有することが可能になる。このペアリング中、リンク鍵の少なくとも一部分が生成され、医療デバイスおよびＭＣＵのメモリに記憶される。前記リンク鍵は、共有秘密（例えば、暗号化鍵、．．．）、および医療デバイスのブルートゥースアドレスを含むことができる。前記リンク鍵は、この後の無線通信を確立するのに要求される。

【００７２】

遠隔制御装置は、前記医療デバイスが見つからない場合でも遠隔制御装置を医療デバイスと対にすることができるように、ＭＣＵ（４、６、８）の中に記憶された前記リンク鍵を読み出すことができる。したがって、遠隔制御装置（３）は、標準のペアリングプロセスを用いなくても接続（例えば、ブルートゥース接続）を開始することができる。次に、遠隔制御装置は前記パラメータを、接続を直接確立することができるブルートゥース通信層まで転送する。

【００７３】

ＭＣＵは、使用者が使用するのに先立って医療デバイスとすでに対にされているので、患者は、リンク鍵を知っている前記ＭＣＵ（４、６、８）を自分の遠隔制御装置の中にプラグ接続しなければならないだけであり、医療アセンブリはすぐに使用できる。

【００７４】

有利なことに、リンク鍵は、ＭＣＵ（８）のメモリの第３の部分（１３）に記憶されている。前記第３の部分（１３）は、ＣＰＵによって書き込み可能かつ読み出し可能であるが、他のデバイスによっては書き込み不可能で読み出し可能である。したがって、リンク鍵は遠隔制御装置によって読み出すことができるが、前記遠隔制御装置は、そのリンク鍵を変更することはできない。言い換えれば、ＭＣＵをもう一度対にすることができない。

【００７５】

上記で開示されたように、ペアリングデバイス（１６）を使用してペアリングプロセスを実施することができる。前記ペアリングデバイス（１６）は２つの接続手段を含み、一方が医療デバイス接続用であり、他方がＭＣＵ接続用である。使用者が医療デバイスおよびＭＣＵをペアリングデバイス（１６）にプラグ接続すると、ペアリングプロセスを実施することができる。このペアリングデバイスにより、医療デバイスおよびＭＣＵは、その秘密（例えば、リンク鍵、．．．）を実際に安全に共有することができる。ペアリングデバイスは、ＭＣＵと医療デバイスの間の安全なデータ交換を行うための有線通信手段を備えてもよい。ペアリングデバイスはまた、それを数回プラグ引抜きおよびプラグ接続することができるので、いくつかの遠隔制御装置で使用することもできる。

【００７６】

一実施形態では、前記ＭＣＵおよび／または医療デバイスは、新規のペアリング要求を受け入れることができない。

【００７７】

この独特のペアリングプロセスにより、医療デバイスは、容易および安全に遠隔制御装置に接続される。ＭＣＵと医療デバイスが対にされた後、遠隔制御装置は、ＭＣＵ内に記憶されたパラメータ（例えば、リンク鍵）を読み出し、それを使用しなければならない。

【００７８】

ＭＣＵ（４、６、８）と医療デバイス（１、７）の間のペアリングは、以下の工程を含む：

・　ＭＣＵ（４、６、８）および医療デバイス（１、７）を提供する工程。

・　前記ＭＣＵ（４、６、８）と前記医療デバイス（１、７）の間の通信を可能にする手段を提供する工程。

・　ＭＣＵ（４、６、８）と医療デバイス（１、７）の間で少なくとも１つの秘密を共有する工程。

【００７９】

前記少なくとも１つの秘密には、医療デバイスアドレス、リンク鍵および／または他の鍵が含まれうる。

【００８０】

前記鍵情報のすべてまたは一部を共有する前記手段（例えば、ペアリングデバイス）には、入力手段、有線接続部、表示手段、および／またはペアリングプロセスを実施するための手段（アプリケーションなど）が含まれうる。

【００８１】

遠隔制御装置（３）と医療デバイスの間のペアリングでは、以下の工程を含む：

・　医療デバイス（１、７）、遠隔制御装置（３）、および前記医療デバイス（１、７）とすでに対にされているＭＣＵ（４、６、８）を提供する工程。

・　前記ＭＣＵ（４、６、８）を前記遠隔制御装置（３）の中にプラグ接続する工程。

・　前記ＭＣＵ（４、６、８）のメモリおよび前記医療デバイスのメモリに含まれているペアリングデータを使用して、医療デバイスを遠隔制御装置（３）と接続する工程。

【００８２】

有利なことに、前記ＭＣＵ（４、６、８）および前記医療デバイス（１、７）は、接続を認証するための暗号機構、ならびにセッション鍵または他の鍵を生成する手段を使用することができる。

【００８３】

一実施形態では、医療デバイスは、前記ＭＣＵを一時的に接続してペアリングプロセスを実施する接続手段を含むことができる。

【００８４】

遠隔制御装置と医療デバイスの間の通信を保護する

本明細書では、ペアリングプロセスを安全に実施できるようにする安全なペアリングプロセスを上に開示している。このプロセスは単独で使用することができるが、さらなるセキュリティを付加するには、データが安全に交換されなければならない。

【００８５】

遠隔制御装置と医療デバイスの間の通信を保護するために、医療デバイスは、少なくとも１つの暗号化鍵データおよび／またはループバック機構を使用することができる。

【００８６】

暗号化鍵：

上に開示されているように、ＭＣＵ（４、６、８）のメモリは、医療デバイス（１、７）との安全な通信を可能にするために、鍵情報を含むことができ（それだけには限らないが：通信構成、公開鍵、秘密鍵、暗号法プロセス、リンク鍵、．．．など）、この医療デバイスもまた、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、医療デバイス（１、７）に接続すること、および／またはデータを暗号化／復号することは不可能である。

【００８７】

一実施形態では、前記鍵情報は、遠隔制御装置（３）および医療デバイス（１、７）が暗号化データを交換し、かつ／または送信側を認証できるように、少なくとも１つの暗号鍵を含む。前記少なくとも１つの暗号鍵は、非対称鍵および／または対称鍵とすることができる。そのように、所与のデータはＭＣＵまたは遠隔制御装置によって暗号化されるが、医療デバイス（１、７）は、前記データを復号することができる。逆に、医療デバイス（１、７）は、遠隔制御装置（３）に暗号化データを送信することができ、前記暗号化データは、ＭＣＵまたは遠隔制御装置によって復号することができる。

【００８８】

鍵生成器は、少なくとも１つの暗号化鍵を生成し、この鍵は、ＭＣＵのメモリおよび／または医療デバイスのメモリに記録される。さらなるセキュリティのために、前記少なくとも１つの暗号化鍵は秘密に保持され、ＭＣＵと医療デバイスの間だけで共有されなければならない。

【００８９】

一実施形態では、少なくとも１つの暗号鍵は非対称鍵である。鍵生成器は、ＭＣＵのメモリに記憶される秘密鍵と、医療デバイスのメモリに記憶されることになる公開鍵とを生成する。前記秘密鍵は、遠隔制御装置またはＭＣＵで使用することができるが、前記公開

鍵は医療デバイスだけで使用される。したがって、前記ＭＣＵのメモリは秘密鍵を含み、前記医療デバイスのメモリはその適合する公開鍵を含む。有利なことに、前記公開鍵は、医療デバイスによって秘密に保持され、他のデバイスとは、またはブルートゥースを介しては、決して共有されない。

【００９０】

一実施形態では、ＭＣＵが遠隔制御装置から取り外されると（そのＭＣＵを含む前記遠隔制御装置を使用した後に）、遠隔制御装置が前記秘密鍵を使用できないように、したがって遠隔制御装置が医療デバイスと通信できないように、ＭＣＵは秘密を保持し、かつ前記秘密鍵を遠隔制御装置と共有しない。有利なことに、前記秘密鍵は、ＭＣＵのメモリの第２または第４の部分（１２、１４）に記憶され、したがって秘密鍵は、他のデバイスによって読み出し可能にすることができない。具体的な事例で、秘密鍵が第４の部分（１４）にだけ記憶されている場合、その秘密鍵は他のデバイスによって書き換え可能にすることができない。医療デバイスによって使用される公開鍵は、好ましくは医療デバイスによって秘密にしておかなくてはならない。それでもハッカーが前記公開鍵を見つけた場合、このハッカーは、遠隔制御装置から送信さたデータ（例えば、治療、命令、．．．）を復号するだけである。これは、ハッカーが秘密鍵（ＭＣＵのメモリに記憶されている）を見つけた場合よりも危険性が少ない。その理由は、こちらの具体的な事例では、ハッカーが遠隔制御をシミュレーションし、患者治療計画（例えば、インスリン送達、．．．）を変更することもできるからである。

【００９１】

一実施形態では、鍵生成器は、少なくとも２つの非対称鍵（ＡおよびＢ）を生成する。秘密鍵ＡはＭＣＵに記憶され、その適合する公開鍵Ａは医療デバイスに記憶される。秘密鍵Ａは、遠隔制御装置および／またはＭＣＵで使用することができ、公開鍵Ａは医療デバイスだけで使用される。秘密鍵Ｂは医療デバイスに記憶され、その適合する公開鍵ＢはＭＣＵに記憶される。公開鍵Ｂは、遠隔制御装置および／またはＭＣＵで使用することができ、秘密鍵Ｂは医療デバイスだけで使用される。したがって、この実施形態では、医療デバイスは公開鍵Ａおよび秘密鍵Ｂを含み、ＭＣＵは公開鍵Ｂおよび秘密鍵Ａを含む。前記公開鍵Ｂおよび前記秘密鍵Ａは、ＭＣＵのメモリの読み出し不可能な部分（書き込み可能または書き込み不可能な部分内にある）に記憶することができる。したがって、通信は完全に保護され、送信側は認証される。実際、公開鍵Ａを用いて復号可能であるメッセージを医療デバイスが受信した場合、医療デバイスには督促者（ｅｘｐｅｄｉｔｏｒ）（遠隔制御装置）が分かり、逆も同様であり、公開鍵Ｂを用いて復号可能であるメッセージを遠隔制御装置が受信した場合、遠隔制御装置には督促者（医療デバイス）が分かる。２つの非対称鍵を使用することにより、送信側を認証することが可能になる。

【００９２】

一実施形態では、ＭＣＵ（８）のＣＰＵは、共有されることになる少なくとも１つの暗号化鍵を生成する鍵生成器を含む。前記ＣＰＵ（９）はまた、暗号化エンジン．．．などの他の機能を含むこともできる。例えば、図１４に開示されているように、ＭＣＵ（８）は、少なくとも１つの秘密を生成するように生成器が実行されるＣＰＵ（９）を含む。この秘密は、鍵情報（リンク鍵、暗号化鍵、ハッシュ、．．．）のすべてまたは一部とすることができる。図１４では、２つの秘密が生成され、両方がＭＣＵ（８）のメモリ（１０）に記憶される。秘密１および秘密２は同一にする、同類にする、または別個にすることができる。秘密１はＭＣＵのメモリ（１０）内に保持され、秘密２は医療デバイス（１）と共有される。この事例では、秘密１は、ＭＣＵのメモリの第２および第４の（好ましい）部分に記憶することができ、秘密２は、ＭＣＵのメモリの第１または第３の部分に記憶することができる。したがって、秘密２は、医療デバイスに送出されるように読み出すことができる。次に、秘密２はＭＣＵのメモリ（１０）から削除することができる。例えば、公開鍵Ａは、ＭＣＵのメモリの第１の部分に記憶することができる。その理由は、前記秘密は医療デバイスへ送信されなければならず、その後、前記秘密を所与のデバイス（例えば、後述のペアリングデバイス）において削除することが好ましいからである。リンク

鍵は削除してはならないので、ＭＣＵのメモリの第３の部分に記憶することができる。このプロセスは、遠隔制御装置を用いて、または図１３に示されるペアリングデバイス（１６）のような特定のデバイスを用いて、実施することができる。

【００９３】

別の実施形態では、生成器は医療デバイス内で実行される。別の実施形態では、医療デバイスおよびＭＣＵは、それ自体の生成器を実行し少なくとも部分的な鍵情報を生成し、この鍵情報は、ＭＣＵと医療デバイスの間で少なくとも部分的に共有することができる。

【００９４】

一実施形態では、上述の生成器は、ペアリングデバイス（１６）のような特定のデバイスによって起動または実行される。

【００９５】

生成器は、製造者、医師、介護者または薬剤師が起動させることができる。

【００９６】

鍵生成プロセスの間または後に、患者の特徴、薬物、治療、投薬計画、治療セキュリティ制限、．．．などの他の情報を、ＭＣＵおよび／または医療デバイスのメモリに記録することができる。

【００９７】

一実施形態では、本明細書に記載された医療デバイスとの少なくとも１つの通信を保護するために、１つの方法は以下の工程を含む：

－　秘密鍵および適合した公開鍵を含む非対称鍵を生成する工程。

－　前記秘密鍵をＭＣＵの安全なメモリに記憶する工程。

－　前記適合させた公開鍵を医療デバイスのメモリに記憶する工程。

－　前記秘密鍵を用いてデータＡを暗号化する工程、または前記公開鍵を用いてデータＢを暗号化する工程。

－　前記暗号化データＡを医療デバイスに伝送する工程、または前記暗号化データＢを遠隔制御装置へ伝送する工程。

－　前記公開鍵を使用してデータＡを復号する工程、または前記秘密鍵を使用してデータＢを復号する工程。

【００９８】

前記鍵交換は有線通信で行い、患者に使用されるのに先立って、ペアリングデバイスによって起動させることができる。鍵生成は、ＭＣＵで起動させた、またはＭＣＵ内で実行された鍵生成器によって行うことができる。

【００９９】

非対称鍵はいくつかの資源を使用し、対称鍵を使用することが好ましい。したがって、非対称鍵は、セッション通信の開始時、また対称鍵を（セッション鍵として）使用した後に使用することができる。前記対称鍵は、一時的に使用すること、および定期的に変更することができる。

【０１００】

一実施形態では、本明細書に記載された医療デバイスとの少なくとも１つの通信を保護するために、１つの方法は以下の工程を含む：

－　遠隔制御装置と医療デバイスの間に第１の通信を確立する工程。

－　医療デバイスで交渉値Ｖｍを生成する工程。

－　前記交渉値Ｖｍを遠隔制御装置まで伝送する工程。

－　前記交渉値ＶｍをＭＣＵまで伝送する工程。

－　ＭＣＵでセッション鍵Ｋｓおよび交渉値Ｖｒｃを計算する工程。

－　前記秘密鍵を使用して、ＭＣＵで少なくともセッション鍵および／または前記交渉値Ｖｒｃを暗号化する工程。

－　前記暗号化データを遠隔制御装置まで伝送する工程。

－　前記暗号化データＶｒｃを医療デバイスまで伝送する工程。

－　前記公開鍵を使用して、医療デバイスで前記暗号化データを復号する工程。

【０１０１】
医療デバイスは、セッション鍵もまた計算することができる。前記セッション鍵は、秘密にしておくことも、ＭＣＵで生成されたセッション鍵と照合するために使用することもできる。医療デバイスは、前記暗号化データおよび／または前記公開鍵を使用して認証を確認することができる。
【０１０２】
図１７に示される一実施形態では、トークンを一方が含む２つの別個のノード間の少なくとも１つの通信を保護するために、１つの方法が以下の工程を含む：
－　２つの別個のノード：すなわち１および２を提供する工程。前記ノード１は、暗号化鍵１、鍵生成器、および暗号化エンジンを含むことができる。前記ノード２は、暗号化鍵２、鍵生成器、および暗号化エンジンを含むことができる前記トークンに接続する手段を含む。
－　第１のノードで第１の通信を開始する工程。
－　第１のノードで値Ｖ１を生成する工程。
－　鍵１（任意選択）を用いて前記値Ｖ１を暗号化する工程。
－　前記（暗号化）値Ｖ１を第２のノードまで伝送する工程。
－　前記（暗号化）値Ｖ１をトークンまで伝送する工程。
－　鍵２（任意選択）を用いて前記値Ｖ１を復号する工程。
－　トークンで値Ｖ２を生成する工程。
－　値Ｖ１およびＶ２を使用して、トークンでセッション鍵１を生成する工程。
－　鍵２（任意選択）を用いて前記値Ｖ２を暗号化する工程。
－　前記（暗号化）値Ｖ２を第２のノードまで伝送する工程。
－　前記（暗号化）値Ｖ２を第１のノードまで伝送する工程。
－　鍵１（任意選択）を用いて前記値Ｖ２を復号する工程。
－　値Ｖ１およびＶ２を使用して、第１のノードでセッション鍵２を生成する工程。
【０１０３】
セッション鍵１および２は、暗号化データを安全に認証および交換するために同一でなければならない。第１のノードは医療デバイスまたは医療サーバとすることができ、第２のノードは遠隔制御装置とすることができる。トークンはＭＣＵ内にあってよい。暗号化鍵は、非対称鍵または対称鍵とすることができる。暗号化鍵１は公開鍵とし、暗号化鍵２は秘密鍵とすることができる。場合により、第１のノードおよび／または第２のノードは、通信が現在安全に行われていることを視覚、音声表示、および／またはバイブレータによって患者に知らせることができる。
【０１０４】
第１のノードで不正なトークンと接続しようとする場合には、暗号化鍵により、前記トークンは値Ｖ１を正しく復号することができない。その結果、このトークンは、セッション鍵２と異なるセッション鍵１を生成し、このトークンは、前記第１のノードとデータを交換することができない。
【０１０５】
したがってこのプロセスにより、前記ＭＣＵと前記医療デバイスは、無線通信の際にいかなる鍵も決して交換しない。一実施形態では、前記セッション鍵は、前記セッション鍵を使用して復号および暗号化するための暗号化エンジンを含むトークン内に、秘密に保持される。別の実施形態では、前記トークンは、セッション鍵を第２のノードと共有し（トークンは、鍵２も秘密に保持すること、または共有することができる）、前記第２のノードは、前記セッション鍵を用いて復号または暗号化するための暗号化エンジンを含む。
【０１０６】
ループバック機構
次の段落は、ループバック機構を含む本発明の実施形態に関する。この機能は、本発明によるアセンブリと、患者によって読み出された、または入力された情報との間に保護されたブリッジを確保するために、これまでに開示されたアーキテクチャ、または同様なレ

ベルのセキュリティが遠隔制御装置内部に用意されることを考慮に入れることによって、医療デバイスと遠隔制御装置の間に安全な通信を実現することができる。図３および図４は、本発明による遠隔制御装置（３）を用いたループバック機構の使用を示す。

【０１０７】

このループバックは、医療デバイス（１、７）において実行されるコマンドが、そのパラメータと共に、操作者から要求されたこと（認証）、かつ操作者の要望に対応すること（完全性）を保証する機構である。より正確には、この機構はまず、遠隔制御装置（３）と医療デバイス（１、７）の間で伝送された情報が、事故（メモリ不良、通信障害）によって、または故意に（攻撃者、マルウェア）変更されていないことを保証する。さらに、この機構は、コマンドが確かに使用者から要求されたことを保証する。これらの２つの機能は、それだけには限らないが以下のようなタスクによって実現される：

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

－　医療デバイス（１、７）は、コマンドおよびそのパラメータに基づく呼掛けを生成し、それを遠隔制御装置（３）へ返す。

－　遠隔制御装置（３）は、呼掛けから情報を抽出し、確認のためにそれを使用者に表示する。外部ＭＣＵ（表示装置を含む）を使用する一実施形態では、前記情報は、外部ＭＣＵの表示手段によって表示することができる。この情報は、医療デバイス（１、７）で受信されたコマンドおよびそのパラメータを含む。

－　使用者は、自分が承認および確認したことを、自分だけが知っているＰＩＮを入力することによって知らせる。遠隔制御装置（３）は、呼掛けに対する応答を、ＰＩＮおよび呼掛け自体を使用して生成する。

－　応答は、医療デバイス（１、７）まで伝送され、医療デバイスによって検証される。コマンドは、呼掛けの応答が正しい場合に限り、実際に実行し始める。

【０１０８】

この機構は、使用者によって使用されるＰＩＮが、呼掛け－応答の特定のインスタンスについてのみ検査するという意味で、標準的な「ログイン」機構とは異なる。このように、各コマンドは使用者によって検査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では、使用者がＰＩＮコードを入力したすぐ後に、新しいコマンドを送信することができなくなる。さらに、この使用者がＰＩＮコード（任意選択）を知っている唯一の人であるので、別の人が適正な遠隔制御装置を用いて、または間違いで、もしくは意図的に別のデバイスを用いて、コマンドを送信することはできない。

【０１０９】

この機構はまた、使用者に示され、使用者の承認が要求される情報が、目標デバイスから返される情報であるという意味で、要求されたコマンドを使用者に対し「確かですか？」機構によって繰り返すことだけとも異なる。何らかの変更が行われた場合には、この返された値は、使用者によって初めに入力された情報とは自動的に異なることになる。

【０１１０】

前記確認は遠隔制御装置によって自動的に処理されず、そのため、悪意のあるアプリケーションで前記確認を制御することはできない。確認は、使用者によってのみ認可されることがきわめて重要である。一実施形態では、送信されたコマンドを確認するのにループバック機構でＰＩＮコードを使用し、使用者だけが前記ＰＩＮコードを知っている。

【０１１１】

好ましくは、直接保護されたパイプが、医療デバイスのメモリと、表示された値を含む遠隔制御装置の保護されたバッファとの間に作成される。次に、遠隔制御装置（３）上の認証されたアプリケーションがその値を表示し、かつ使用者認証を記録し、この使用者認証は、医療デバイスに返送される戻り値を構築するのに使用される。この保護されたパイプは、追加のＭＣＵの内部にある鍵情報を使用することによって始動させることができる。

【０１１２】

保護されたパイプは、使用者が医療デバイスでプログラムしたいパラメータを使用者が定義し終わったときに開く。保護されたパイプは、医療デバイスがパラメータを使用できるようにするために使用者がそのパラメータを確認したときに閉じられる。

【０１１３】

本発明によるループバックプロセスは、以下の要素を実施することを含む。

・　医療デバイス内の保護されたメモリ領域。

・　医療デバイスの保護されたメモリ領域から遠隔制御装置までの間のデータの暗号化通信を管理する、医療デバイスにおける保護されたプロセス。

・　遠隔制御装置内の保護された表示メモリ領域。

・　医療デバイスから遠隔制御装置の保護された表示メモリ領域までの間の暗号化通信を管理する、遠隔制御装置による保護されたプロセス。

・　保護された表示メモリからのデータを遠隔制御装置の表示装置まで転送し、使用者の確認チケット（ａｃｋｎｏｗｌｅｄｇｅｍｅｎｔ　ｔｉｃｋｅｔ）を構築する、遠隔制御装置による保護および認証されたプロセス。

これらの様々な要素のアーキテクチャは図２に示されている。

【０１１４】

ループバックプロセスは、医療デバイスが、治療のセットアップ、または警報設定のような任意のセキュリティ機能を変更する１組のパラメータを受信したときに開始される。

【０１１５】

図３に示される、追加のＭＣＵを使用しない一実施形態では、医療アセンブリ（少なくとも１つの医療デバイスおよび１つの遠隔制御装置）は：

○　保護されたメモリ領域を含むことができる、前記医療デバイス内のメモリ、

○　前記保護されたメモリ領域と遠隔デバイスの間でデータの暗号化通信を管理する、前記医療デバイス内の保護された処理手段（５）、

○　遠隔制御装置内の保護されたメモリ領域、

○　医療デバイスと前記メモリ領域の間でデータの暗号化通信を管理する、遠隔制御装置内の保護された処理手段（５）、

○　保護されたメモリからのデータを遠隔制御装置の表示装置まで転送し、使用者の確認チケットを構築する、遠隔制御装置による保護および認証された処理手段（５）、

を含む。

【０１１６】

この実施形態で追加のＭＣＵを使用しない場合、２つの別個のノードとユーザの間のループバックプロセスは、以下の工程を含むことができる：

・　第２のノードから送信されたコマンドを第１のノードで受信する工程（ｒｅｃｅｉｐｔｉｎｇ）。

・　前記コマンドを第１のノードのメモリに記憶する工程。

・　前記コマンドを第１のノードで暗号化鍵Ａを使用して暗号化する工程。

・　前記暗号化コマンドを第２のノードに送信する工程。

・　第２のノードで前記暗号化コマンドを受信する工程。

・　前記暗号化コマンドを第２のノードで暗号化鍵Ｂを使用して復号する工程。

・　前記コマンドを第２のノードの表示手段によって表示する工程。

・　使用者がコマンドを調べる工程。

・　使用者が前記コマンドを第２のノードの入力手段を使用して検査する工程。

・　前記妥当性検査を第１のノードへ送信する工程。

【０１１７】

前記暗号化鍵ＡおよびＢは、同一とすることも関連づけることもできる。さらなるセキュリティを付加するために、このプロセスはさらに、呼掛け生成、ＰＩＮコード、状態表示、．．．を含むことができる。

【０１１８】

したがって詳細には、このプロセス（図３に示す）は以下の工程を含むことができる：

・　医療デバイス内の埋込みソフトウェアによって行われる工程
　○　医療デバイスのメモリ内で確認されなければならないパラメータを書き込む。
　○　場合により、一般に呼掛けと命名されるランダム情報を生成する。
　○　医療デバイスと遠隔制御装置の間に安全なパイプを開く。
　○　場合により、医療デバイスおよび遠隔制御装置がループバックモードにあることを、振動、音声、ＬＥＤなどの手段、または患者に知らせる任意の方法によって使用者に表示する。
　○　ＫＰと呼ばれる暗号化鍵を使用して暗号化されたパラメータ、および呼掛けを遠隔制御装置へ送信する。
・　遠隔制御装置内のソフトウェアエンティティ１によって行われる工程
　○　遠隔制御装置の保護されたメモリ領域への暗号化パラメータおよび呼掛けを受信し書き込む。
・　遠隔制御装置内のソフトウェアエンティティ２によって行われる工程
　○　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。これらの鍵は、対称または非対称とすることができる。認定されるアプリケーションは、適正な対応鍵ＫＲＣを有することによって妥当性が確認される。
　○　「概要」ページの復号パラメータを表示する。
　○　場合により、使用者のＰＩＮコードを入力する。
　○　これらのパラメータの受入れを、呼掛け、鍵ＫＲＣ、および入力されたＰＩＮコードを使用することによって確認する、確認チケットを構築する。
　○　このチケットを遠隔制御装置の保護されたメモリ領域に書き込む。
・　遠隔制御装置内のソフトウェアエンティティ１によって行われる工程
　○　このチケットを医療デバイスへ返送する。
・　医療デバイス内の埋込みソフトウェアによって行われる工程
　○　場合により、予想されるチケットを計算する。
　○　遠隔制御装置から来る確認チケットを受信および検査する。

【０１１９】

チケットが検査されるとループバックプロセスが閉じられ、医療デバイスは、更新されたパラメータを使用することが可能になる。この基本的なプロセスは、保護されたパイプのセキュリティを改善するために、より精緻化することも、より複雑な体系の一部とすることもできる。

【０１２０】

一実施形態では、前記ソフトウェアエンティティ１および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）内の埋込みソフトウェアとし、ソフトウェアエンティティ２は遠隔制御装置（３）内の認証されたアプリケーションとすることもできる。別の実施形態では、前記ソフトウェアエンティティ１は、後で定義されるホストオペレーティングシステムで動作し、ソフトウェアエンティティ２は、後で定義される医療オペレーティングシステムで動作する。

【０１２１】

当技術分野の当業者には、データ送り出しを暗号化するのに、また前記チケットを生成するのに、いくつかの方法があることが理解されよう。本発明は、データ送り出しを暗号化するのに、または前記チケットを生成するのに、特定の方法に限定されない。

【０１２２】

この実施形態で追加のＭＣＵを使用する場合、２つの別個のノードとユーザの間のループバックプロセスは、以下の工程を含むことができる：
・　第２のノードから送信されたコマンドを第１のノードで受信する工程。
・　前記コマンドを第１のノードのメモリに記憶する工程。
・　前記コマンドを第１のノードで暗号化鍵Ａを使用して暗号化する工程。
・　前記暗号化コマンドを第２のノードに送信する工程。

・　第２のノードで前記暗号化コマンドを受信する工程。
・　前記暗号化コマンドをＭＣＵへ送信する工程。
・　ＭＣＵで前記暗号化コマンドを受信する工程。
・　前記暗号化コマンドをＭＣＵで暗号化鍵Ｂを使用して復号する工程。
・　前記コマンドを第２のノードの表示手段によって表示する工程。
・　使用者がコマンドを調べる工程。
・　使用者が前記コマンドを第２のノードまたはＭＣＵ（ＭＣＵが妥当性検査ボタンなどの入力手段を含む外部ＭＣＵである場合）の入力手段を使用して検査する工程。
・　前記妥当性検査を第１のノードへ送信する工程。

【０１２３】

前記暗号化鍵ＡおよびＢは、同一としても（対称）、または関連づけられても（非対称）よい。さらなるセキュリティを付加するために、このプロセスはさらに、呼掛け生成、ＰＩＮコード、状態表示、．．．を含むこともできる。

【０１２４】

したがって詳細には、このプロセス（図４示す）は以下の工程のすべてまたは一部を含むことができる：

・　医療デバイス内の埋込みソフトウェアによって行われる工程：
　○　医療デバイスのメモリ内で確認されなければならないパラメータを書き込む。
　○　場合により、呼掛けを生成する。
　○　一時的な鍵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。
　○　場合により、医療デバイスおよび遠隔制御装置がループバックモードにあることを、振動、音声、ＬＥＤなどの手段、または患者に知らせる任意の方法によって使用者に表示する。一実施形態では、ＭＣＵは、前記情報を使用者に伝える手段（ＭＣＵ上のＬＥＤ、表示手段、バイブレータ、．．．）を含む外部ＭＣＵである。
　○　暗号化されたパラメータおよび／または呼掛けを遠隔制御装置へ送信する。
・　遠隔制御装置内の埋込みソフトウェアによって行われる工程
　○　暗号化パラメータをＭＣＵへ送信する。
・　ＭＣＵ内の埋込みソフトウェアによって行われる工程。
　○　暗号化パラメータおよび呼掛けを受信しＭＣＵのメモリ内に書き込む。
　○　鍵Ｋｓ１を使用することによってパラメータを復号する。
　○　暗号化パラメータおよび呼掛けを遠隔制御装置のメモリへ送信する。
・　遠隔制御装置内の埋込みソフトウェアによって行われる工程
　○　「概要」ページの復号パラメータを表示する。
　○　場合により、使用者にＰＩＮコードを入力することを促す。
　○　これらのパラメータの受入れを、呼掛け（任意選択）、パラメータ、および入力されたＰＩＮコード（任意選択）を使用することによって確認する、確認チケットを構築する。
　○　このチケットを遠隔制御装置のメモリに書き込む。
　○　前記チケットをＭＣＵへ送信する。
・　ＭＣＵ内の埋込みソフトウェアによって行われる工程
　○　前記チケットを受信しＭＣＵの保護されたメモリへ書き込む。
　○　一時的な鍵Ｋｓ２を使用することによって前記チケットを暗号化する。
　○　前記暗号化チケットを遠隔制御装置へ返送する。
・　遠隔制御装置内の埋込みソフトウェアによって行われる工程
　○　暗号化チケットを医療デバイスへ返送する。
・　医療デバイス内の埋込みソフトウェアによって行われる工程
　○　場合により、予想されるチケットを計算する。
　○　遠隔制御装置から来る確認チケットを受信し、復号し、検査する。

【０１２５】

チケットが検査されるとループバックプロセスが閉じられ、医療デバイスは、更新され

たパラメータを使用することが可能になる。この基本的なプロセスは、保護されたパイプのセキュリティを改善するために、より精緻化することも、より複雑な体系の一部とすることもできる。

【０１２６】

一実施形態では、使用者操作を模倣する、またはこの情報を傍受する、いかなるアプリケーションも阻止するために、遠隔制御デバイスによりランダム配列表示を使用しながらＰＩＮを入力することができる。例えば、その数字（０から９の５つ）は、使用者によってＰＩＮコードが入力されなければならないたびに毎回異なるランダムな順序で表示される。別の実施形態では、前記ＰＩＮは、コマンドを検査するために再描画され、入力され、またはコピーされなければならない記号、絵、語、形と置き換えることができ、その意図のすべてが、表示と対話している知的人間がいることを確かめることである。

【０１２７】

別の実施形態では、ＰＩＮは、それだけには限らないが、指紋リーダ、指紋網膜（ｆｉｎｇｅｒｐｒｉｎｔ　ｒｅｔｉｎａｌ）、．．．などの別の認証手段によって変更することができる。この認証手段は、使用者だけに知られている、または所有されている必要がある。

【０１２８】

一実施形態では、遠隔制御装置内の前記埋込みソフトウェアは、後で定義されるホストオペレーティングシステムで動作し、ＭＣＵ内の前記埋込みソフトウェアは、後で定義される医療オペレーティングシステムで動作するか、または起動する。

【０１２９】

ＭＣＵが図４または図５に示されているドングルである場合、および前記ドングルが患者に情報を伝える手段を含む場合、その表示手段によって呼掛けを表示することができる。前記手段により、安全なモード、またはＯＳ、またはループバックモードが進行中であることを患者に知らせることができる。

【０１３０】

一実施形態では、呼掛けも暗号化することができる。

【０１３１】

一実施形態では、鍵Ｋｓ１およびＫｓ２は、非対称鍵対とすることも、対称鍵とすることも、ハッシング機構を使用することもできる。

【０１３２】

一実施形態では、鍵Ｋｓ１とＫｓ２は同じであるか、または異なる。

【０１３３】

一実施形態では、使用者は、ループバック機構の入口を確認するためにＰＩＮコードを入力しなければならないが、このようなＰＩＮコードはランダム表示配列によって入力される。

【０１３４】

一実施形態では、ＭＣＵは外部ＭＣＵであり、このＭＣＵは入力手段を、ＰＩＮコードを前記入力手段によって入力できるようにして、または前記入力手段が指紋リーダ（ｐｒｉｎｔ　ｆｉｎｇｅｒ　ｒｅａｄｅｒ）であるようにして含む。別の実施形態では、前記指紋リーダは遠隔制御装置内にある。

【０１３５】

遠隔制御装置と医療サーバの間の通信を保護する

一実施形態では、前記ＭＣＵ（４、６、８）は、前記医療アセンブリと医療サーバの間の通信（例えば、遠隔医療）を確立および／または保護するための鍵情報を含む。このようにして、データのすべてまたは一部を、前記データを分析または記憶できる医療サーバまで安全に送信することができる。

【０１３６】

本明細書に記載された機能のすべてまたは一部は、遠隔制御装置と医療サーバの間、または医療サーバと医療デバイスの間の通信を確立および／または保護するために使用する

ことができ、その場合この遠隔制御装置はゲートウェイとして使用することができる。
【０１３７】
ＭＣＵの他の特徴
図６、７、８および１２に示されている一実施形態では、外部ＭＣＵ（６）は、（ドングルのような）外部デバイスとみなすことも、外部デバイスとすることもできる。
【０１３８】
一実施形態では、外部ＭＣＵ（６）は単純なドングルとして使用することができ、前記外部ＭＣＵ（６）は、図７に示されるように、内部ＭＣＵ（４）に接続するための追加の接続手段（１５）を含むことができる。この具体的な事例では、ドングル（６）は、遠隔制御装置（３）と内部ＭＣＵ（４）の間の仲介物またはアダプタとして使用することができる。したがって、鍵情報またはプログラムのすべてまたは一部は、必ずしも前記ドングル（６）のメモリに記憶されない。内部ＭＣＵ（４）が、他の鍵情報のすべてまたは一部を収容するために使用されなければならない。例えば、ドングル（６）は、遠隔デバイスで実行されるＯＳ、ｍＯＳ、またはアプリケーションの完全性、または遠隔制御装置（３）にインストールされるソフトウェアの完全性を調べるための鍵情報を含むことができる。内部ＭＣＵ（４）は、リンク鍵、暗号鍵、．．．などの鍵情報を含むことができる。
【０１３９】
さらに、患者が遠隔制御装置を変更した場合（破損または電池故障のために）、また新しい遠隔制御装置がＭＣＵ（４）用の適切な接続手段を備えていない場合には、このドングル（６）を有することが有用である。したがって、この外部ＭＣＵ（６）により、遠隔制御装置（３）が内部ＭＣＵ（４）に接続される。この追加の接続手段により、外部ＭＣＵ（６）と遠隔制御装置（３）の間の有線通信または無線通信を行うことができる。
【０１４０】
前記ＭＣＵ（６）は、前のすべての要素および他の手段、または後述の機能（１５）を含むことができる。
【０１４１】
外部ＭＣＵ（６）は、それだけには限らないが、
－　前記ＭＣＵ（６）もまた血糖監視のように使用できるような血糖測定手段、
－　患者の活動を監視するための加速度計、
などのセンサを含むことができる。
【０１４２】
ＭＣＵ（６）は、患者が２つの別個の表示手段（第１のものが遠隔制御装置に設置され、第２のものがドングルまたは外部ＭＣＵ（６）に設置される）を有するようにして、データを安全に表示するための表示手段を含むことができる。すなわち、第１のものは、医療デバイスをプログラムまたは監視するために使用され、第２のものは、データを確認するために、またはループバックの呼掛けもしくは他の情報のすべてまたは一部を受信および表示するために使用することができる。そのため、遠隔制御装置に必要なセキュリティレベルは最小限にすることができる。というのは、患者は、ＭＣＵ（６）の表示装置に必要な、その情報が完全に保護されているすべての安全関連プログラム変更を、医療デバイスで実施予定のこのようなプログラム変更を確認する前に見直さなければならないことになるからである。
【０１４３】
このような外部ＭＣＵ（６）は、データを安全に設定するための、もしくはＰＩＮコードを入力するための入力手段、または指紋リーダを含むことができる。前記入力手段はまた、送信する前のデータ、またはループバック機構内で使用されるデータを検査するための検査ボタンとすることもできる。
【０１４４】
図１２に示されるように、外部ＭＣＵ（６）は、別のＭＣＵ（４）と接続するための少なくともう１つの接続手段を含むことができる。したがって、外部ＭＣＵ（６）は、もとから医療デバイス（例えば、送達デバイス）と対にすることができ、外部ＭＣＵ（６）

の中にプラグ接続された内部ＭＣＵ（４ｂ）は、別の医療デバイス（例えば、血糖計）と対にすることができる。前記外部ＭＣＵは、第１の医療デバイスの鍵情報を記憶し、前記内部ＭＣＵは、第２の医療デバイスの鍵情報を記憶する。

【０１４５】

外部ＭＣＵが高価な他の手段（１５）（センサ、通信手段、表示手段、．．．のような）を含む場合、単純なドングル（６）（図７に示される）を追加の内部ＭＣＵ（４）と共に使用することが好ましい。医療デバイスは１つのＭＣＵだけと対にされるので、患者が自分の医療デバイスを変更した場合、患者は自分のドングル（６）は保持することができ、対の内部ＭＣＵ（４）－医療デバイス（１）を変更する。

【０１４６】

一実施形態では、前記ＭＣＵ（６）は、遠隔制御装置に依存しないで医療デバイスと安全に通信するための通信手段を含むことができる。この実施形態では、携帯電話とすることができる遠隔制御装置は、有利なことにはその表示手段として使用され、かつ／または前記ＭＣＵに電力供給するために使用される。

【０１４７】

図１５に示される一実施形態では、外部ＭＣＵ（６）は、遠隔制御装置（３）から引き抜き、軽量遠隔制御装置として使用することができる。例えば、前記外部ＭＣＵ（６）が、入力手段（１５）および通信手段（１５）（場合により、電源、表示手段、．．．）を遠隔制御装置なしで含む場合、前記外部ＭＣＵは、医療デバイスを少なくとも部分的に制御することもできる。前記入力手段は、急速投与、および／または一時停止モード、および／または他の送達コマンドもしくはモードを指令するのに使用することができる。

【０１４８】

図８および図９に示される一実施形態では、２つのデバイス（１、７）が遠隔制御装置（３）と通信する。例えば、第１の医療デバイス（１）はインスリンポンプ（１）であり、第２の医療デバイス（７）は連続血糖計（７）である。各医療デバイスは、それ自体のＭＣＵ（４ａ、４ｂ）とだけ対にされる。この実施形態は、図８に示されるように、外部ＭＣＵ（６）にプラグ接続された遠隔制御装置（３）を開示している。前記外部ＭＣＵ（６）は、２つの別個の内部ＭＣＵ（４ａ、４ｂ）を挿入するための２つの別個の接続手段を含む。図９に示される実施形態は、２つの別個の内部ＭＣＵ（４ａ、４ｂ）を挿入するための２つの別個の接続手段を内部に含む遠隔制御装置（３）を開示している。第２のＭＣＵ（４ａ）（または第３のＭＣＵ（４ｂ））は、第１の医療デバイス（１）（または第２の医療デバイス（７））と一緒に鍵情報を含む保護されたメモリを含む。前記第２のＭＣＵ（４ａ）は第１の医療デバイス（１）とだけ対にされ、前記第３のＭＣＵ（４ｂ）は第２の医療デバイス（７）とだけ対にされる。この実施形態は、さらに多くのＭＣＵおよび医療デバイスを含むことができる。

【０１４９】

図１０に示される一実施形態では、２つの医療デバイス（１、７）が遠隔制御装置（３）と通信するが、１つのＭＣＵ（４ｃ）だけがプラグ接続されている。この実施形態では、前記ＭＣＵ（４ｃ）は、前記２つの医療デバイス（１、７）と対にされ、前記２つの医療デバイス（１、７）と一緒に鍵情報を含む少なくとも１つの保護されたメモリを含む。

【０１５０】

一実施形態では、外部ＭＣＵ（６）は、表示手段および／または入力手段を含む。一部のデータ（例えば、重要なデータ）が外部ＭＣＵの表示手段により表示され、かつ／または入力手段により前記データを、医療デバイスで使用される前に検査することができる。例えば、遠隔制御装置により、医療デバイスに対するコマンドをプログラムすることが可能になり、また外部ＭＣＵにより、前記コマンドを検査することが可能になる。ループバック機構は、前記外部ＭＣＵによって少なくとも部分的に実施することができる。前記表示手段は、呼掛けまたはコマンドを、医療デバイスによって実行する前に表示することができる。

【０１５１】

上述の実施形態では１つまたは２つの医療デバイスを使用しているが、本発明はそうした実施形態に限定されず、本発明は、１つまたはそれ以上の医療デバイス、および１つまたはそれ以上のＭＣＵを有することができる。

【０１５２】

遠隔制御装置

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、電話操作者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。さらに前記ＳＩＭカードは、医療デバイス（１、７）と安全に対になり、かつ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も含む。

【０１５３】

別の実施形態では、前記携帯電話は２つの別個の接続手段を含み、第１のものが電気通信操作者のＳＩＭカードをプラグ接続するため、もう一方が、医療デバイスと対にされたＭＣＵをプラグ接続するためのものである。

【０１５４】

一実施形態では、前記遠隔制御装置はまた、携帯電話およびＢＧＭ、またはＣＧＭへのリンクとしても使用される。前記医療アセンブリは、２つの別個のスマートカードを含む。第１は、電話操作者によって使用されるＳＩＭカードであり、第２のスマートカードは、医療デバイスを制御するために使用される。すべての機能（電話、遠隔制御、ＢＧＭ、ＣＧＭ，．．．）を使用するには、両方のスマートカードが遠隔制御装置の中にプラグ接続されなければならない。しかし前記第１のスマートカードが欠けている場合、遠隔制御装置は、携帯電話として使用することはできないが、医療デバイスを制御すること、およびＢＧＭとして使用することはできる。前記第２のスマートカードが欠けている場合、遠隔制御装置は、医療デバイスを制御するのに使用することはできないが、ＢＧＭ、ＣＧＭおよび／または携帯電話として使用することはできる。両方が欠けている場合は、遠隔制御装置はＢＧＭまたはＣＧＭとしてのみ使用される。

【０１５５】

一実施形態では、前記遠隔制御装置は、安全な情報（例えば：呼掛け、ＰＩＮ、．．．）だけを表示するための第２の表示手段を含む。

【０１５６】

さらなるセキュリティのために、前記遠隔制御装置（３）は、仮想化プラットフォームおよび／または完全性試験を含むことができる。

【０１５７】

完全性試験

一実施形態では、前記医療デバイス（１、７）および／または前記ＭＣＵ（４、６、８）は、安全なブートプロセスおよび／または安全なフラッシュプロセス（ｆｌａｓｈ　ｐｒｏｃｅｓｓ）および／または暗号化機構などの、保護された処理手段（５）を含み、この処理手段は、少なくとも遠隔制御装置の完全性を調べ、かつ／または前記医療デバイス（１、７）と前記遠隔制御装置（３）の間の保護されたデータ通信（２）を管理する。

【０１５８】

したがって、前記ＭＣＵ（４、６、８）を使用して、それだけには限らないが、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、．．．などの完全性を確保することができる。この完全性を確保する典型的な方法は、安全なブートまたは安全なフラッシュを使用することであり、これは完全性検査を遠隔制御装置（３）のブート中に、または監視システムを介して一定間隔で行う機能である。

【０１５９】

例えば、安全なブートプロセスを使用する実施形態：遠隔制御装置（３）で動作するソフトウェアが事故（ハードウェア故障）によって、または故意（攻撃者、マルウェア）に修正されていないことを保証するために、安全なブートの機構が使用される。遠隔制御装置（３）の電源が入れられたとき、そのプロセッサで実行される第１のコードは、遠隔制

御装置（３）内部記憶装置（フラッシュメモリ）の内容のシグネチャを計算し、このシグネチャの妥当性を確認するルーチンである。シグネチャが妥当と確認されると、そのプロセッサは、その正規のＯＳ始動手順を継続する。そうでなければ、システムは始動しない。シグネチャの確認は、秘密（鍵）が公開されないことを保証するＭＣＵ（４、４ａ、４ｂ、４ｃ、６、８）を使用して実施できることに注意することが重要である。

【０１６０】

別の例、安全なフラッシュプロセスを用いる実施形態：本発明者らは、遠隔制御ＯＳのより新しいバージョン（医療サーバからダウンロードできる）を使用者が利用できるようにしたい。同様に、遠隔制御装置（３）のソフトウェアが、認証されていないソフトウェアで更新されないようにするために、書き込み予定の新規のソフトウェアには符号が付けられなければならない。遠隔制御装置（３）が更新モードで始動された場合（例えば、電源ボタンの長押しによって）、プロセッサはまず、新ソフトウェアのイメージをダウンロードし、そのシグネチャを計算し、それを確認するルーチンを、既存のソフトウェアを上書きする前に実行する。再び、シグネチャの確認は、秘密（鍵）が公開されないことを保証するＭＣＵ（４、６、８）を使用して実施できることに注意することが重要である。

【０１６１】

したがって、遠隔制御装置の完全性は、ＯＳおよび／またはアプリケーションの（ハッシュとしての）シグネチャのような鍵情報を秘密にそのメモリに記憶するＭＣＵによって調べることができる。

【０１６２】

一実施形態では、完全性試験が成功の場合、通信が確立される。完全性試験が不成功の場合、ＭＣＵは、ＯＳまたはアプリケーションが破損していることを患者および／またはポンプに知らせるプロセスを起動する。前記ＭＣＵまたは前記医療デバイスは、エラーを表示デバイスによって表示すること、または他の手段（音声、バイブレータ、．．．）によって知らせることができる。

【０１６３】

ホストオペレーティングシステム（ｈＯＳ）を使用する

一実施形態では、モバイル仮想化プラットフォームの遠隔制御装置（３）使用により、遠隔制御装置（３）（例えば、スマートフォン）を、（例えば、医療デバイス（１、７）を制御するための）制御された環境と、（例えば、汎用タスクのための）無制御の環境とに分ける可能性が提供される。この仮想化プラットフォームは、仮想機械アプリケーションによって定義することができる。

【０１６４】

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示す（図１参照）：

・　１つまたはいくつかのゲストＯＳ（図１にはゲストＯＳが２つだけ示されている）に対しハードウェア部材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）。

・　無制御環境内で汎用タスク（例えば：カレンダ、連絡先、ウェブブラウジング、電話連絡、娯楽など）を処理する１つのゲストＯＳ。

・　制御された環境内で医療デバイスとの対話を処理する１つのゲストＯＳ。

【０１６５】

有利には、ｈＯＳは、いくつかの先進のオペレーティングプロセスを組み込みながら可能な限り薄くなっており、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内にある。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、ホストオペレーティングシステムはさらに、様々なセキュリティタスクおよび制御タスクを含む。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し調和させ、遠隔制御装置の資源を共有し、かつアプリケーションを実行すること、および／または遠隔制御装置（３）のドライバおよび／または周辺装置を使用することの拒否および／または許可を決定する。このようにしてセキュリティは、悪意のあるソフトウェアが、それだけには限らないが、上述のようなＭＣＵなどのいかなるドライバおよび／または周辺装置に

もアクセスできないので、改善される。
【０１６６】
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、制御された環境では、医療デバイスと交換されるコマンド／情報を遮断する、または修正する、または生成するいかなる悪意のあるアプリケーションも阻止するように、遠隔制御装置を常に完全に制御している。このような悪意のあるアプリケーションの典型的なアクションは、輸注のプログラミングを模倣するために使用者のＰＩＮコードを盗むことである。
【０１６７】
一実施形態では、上述のようにＭＣＵによって、この制御された環境が認証され、その完全性が調べられる。遠隔制御装置のどのブート時にも、完全性を確認し、かつｈＯｓおよび場合によりｍＯＳを認証することになっている前記ＭＣＵによって、安全検査が行われる。
【０１６８】
このアーキテクチャに加えて、認定されたアプリケーションの特定のリストの中にないアプリケーションがもしあれば不能にできる制御された環境内で、特定の監視プログラムを実施して、動作中であるすべてのタスクを調べることができる。この特定の監視はまた、前記ＭＣＵによって制御することもできる。前記モニタによりまた、アプリケーションによって使用される実行時間を測定すること、ならびにアクティビティの疑わしい過負荷がもしあれば警報を発することで使用者に知らせることが可能になりうる。
【０１６９】
一実施形態では、前記ｈＯＳは、前記ＭＣＵに含まれ、かつ／または前記ＭＣＵで起動され、かつ／または動作する。
【０１７０】
一実施形態では、前記ｍＯＳは、前記ＭＣＵに含まれ、かつ／または前記ＭＣＵで起動され、かつ／または動作する。
【０１７１】
一実施形態では、前記ｍＯＳ、および／または前記ｈＯＳ、および／またはハイパーバイザは、前記ＭＣＵに含まれる。前記ＭＣＵが遠隔制御装置に挿入されたとき、ＭＣＵは、遠隔制御装置に前記ｍＯＳ、および／または前記ｈＯＳ、および／または仮想マシンをインストールする。
【０１７２】
一実施形態では、制御された環境内での処理は、ＬＥＤのような、視覚インジケータおよび／または音声インジケータおよび／または他のインジケータ（バイブレータなど）を使用して知らせることができ、これらのインジケータは、現在のアプリケーションが制御された環境内で動作中であること、または無制御の環境内で動作中であることを使用者に知らせる。例として、現在のアプリケーションが制御された環境内にあるときには緑色のＬＥＤがスイッチオンし、次に、使用者が無制御の環境に戻ったときにはスイッチオフすることを想起することができる。また、使用者が制御された環境内にいるときにはＬＥＤはオフで、使用者が無制御の環境に戻ったときに赤になる、「反対」の使用事例もありうる。
【０１７３】
別の実施形態では、ｈＯＳは、制御された環境内で動作中であるアプリケーションのために画面の一部分を確保しておくことができる。このようにして、ｍＯＳだけがこの場所に何かを表示することができ、無制御の環境内で動作中であるアプリケーションまたは他のｇＯＳは、この場所を使用することができない。
【０１７４】
したがって、使用者には、ｍＯＳのアプリケーションが動作中であるかいないかが分かる。実際、前記インジケータが使用者に正しく通知しない場合には、このアプリケーションは確かに、医療デバイスの制御を奪取しようとする、または使用者を欺こうとする悪意のあるアプリケーションである。

【０１７５】
一実施形態では、ＭＣＵは、ｍＯＳが動作中であるときに動作することができるアプリケーションおよび／またはソフトウェアのリストを含む。ＭＣＵがある、またはない一実施形態では、ＰＩＮコードがｍＯＳおよび／または医療デバイスを起動できるようにする。

【０１７６】
医療アセンブリの他の任意選択の機能
別の実施形態では、医療デバイスは、患者の生理学的特性を測定できる少なくとも１つのセンサと、前記センサによって監視される初期症状をリアルタイムで認識する診断手段と、前記診断手段がもし前記初期症状を検出すれば患者に警報する警報手段とを含む。このようにして、医療デバイスは、遠隔制御装置によって監視すること、および遠隔制御装置に警報を送信することができる。

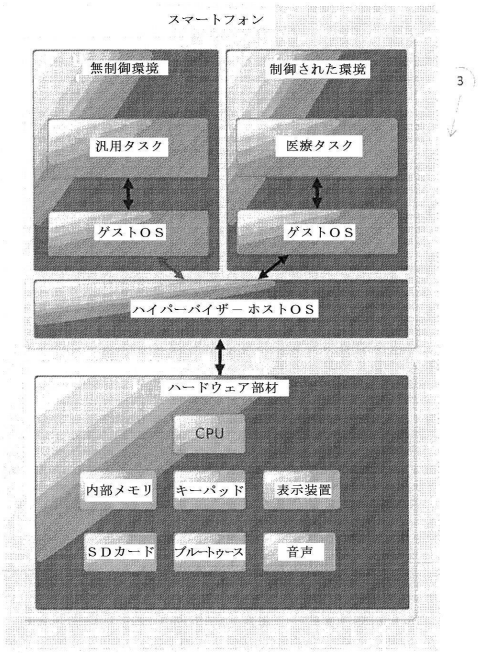
【０１７７】
一実施形態では、遠隔制御装置は、警報が送信された場合に使用者の位置を特定するためのＧＰＳを含む。前記医療アセンブリは、遠隔制御装置内のアプリケーションを起動して、もし前記診断手段で前記初期症状を検出し、または／かつ患者が自分でできない場合には、患者の位置を特定し、前記特定位置を医療センタまたは他の人に送信することができる。また、前記医療アセンブリは、遠隔制御装置内のアプリケーションを起動して、もし前記診断手段で前記初期症状を検出し、または／かつ患者が自分でできない場合には、生理学的特性のデータを医療センタまたは他の人に送信することもできる。

【０１７８】
本発明はもちろん、これまで論じた図示の例に限定されない。

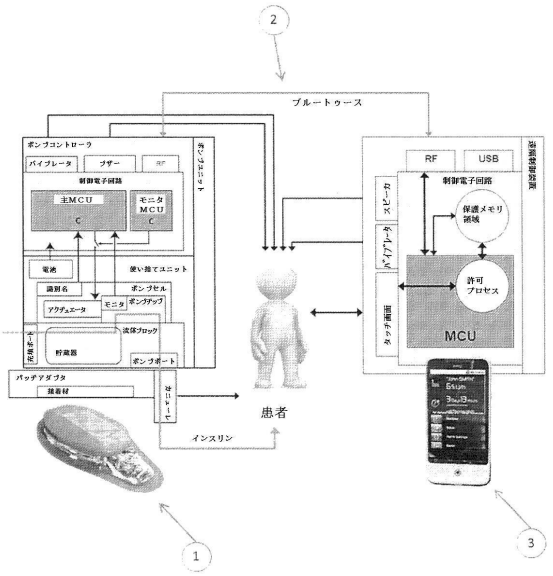
【符号の説明】

【０１７９】
１　医療デバイス
２　無線通信
３　遠隔制御装置
４、４ａ、４ｂ、４ｃ　マイクロコントローラ（スマートカードなど）
５　保護された処理手段
６　外部ＭＣＵ
７　別の医療デバイス
８　マイクロコントローラ
９　ＣＰＵ
１０　マイクロコントローラのメモリ
１１　メモリの第１の部分
１２　メモリの第２の部分
１３　メモリの第３の部分
１４　メモリの第４の部分
１５　外部ＭＣＵの他の手段または機能
１６　ペアリングデバイス（１６）
１７　接続手段
１８　第１の表示手段
１９　第２または安全な表示手段（ＬＥＤ、．．．）

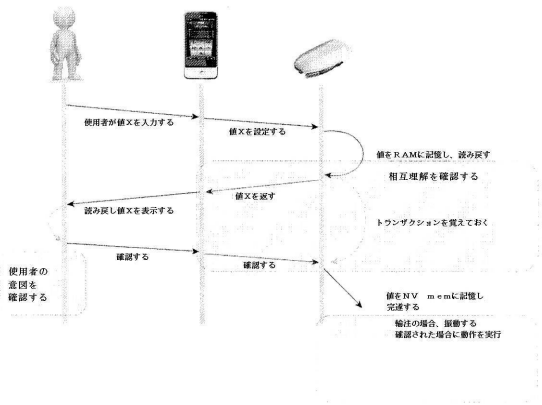
【図１】


スマートフォン
無制御環境
制御された環境
汎用タスク
医療タスク
ゲストOS
ゲストOS
ハイパーバイザー ホストOS
ハードウェア部材
CPU
内部メモリ
キーパッド
表示装置
SDカード
ブルートゥース
音声
3

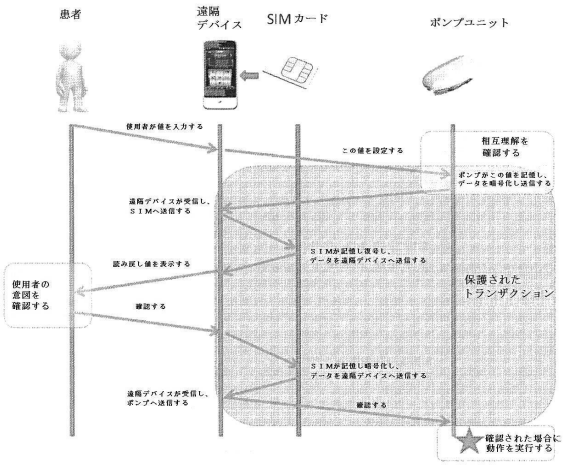
【図２】


2
ブルートゥース
ポンプコントローラ
バイブレータ
ブザー
制御電子回路
主MCU
モニタMCU
電池
使い捨てユニット
識別名
ポンプセル
アクチュエータ
モニタ
ポンプアップ
流体ブロック
貯蔵器
ポンプサポート
パッチアダプタ
接着材
ポンプユニット
RF
USB
スピーカ
バイブレータ
タッチ操作部
制御電子回路
保護メモリ領域
許可プロセス
MCU
患者
インスリン
1
3

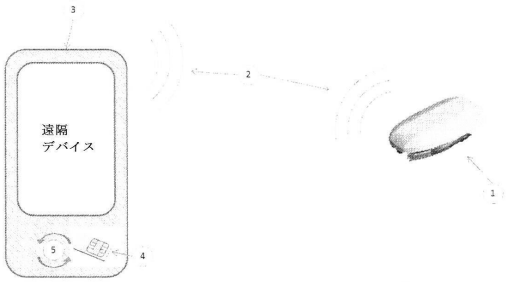
【図３】


使用者が値Xを入力する
値Xを設定する
値をRAMに記憶し、読み戻す
相互理解を確認する
値Xを返す
読み戻し値Xを表示する
トランザクションを覚えておく
確認する
確認する
使用者の意図を確認する
値をNV memに記憶し完遂する
輸注の場合、振動する
確認された場合に動作を実行

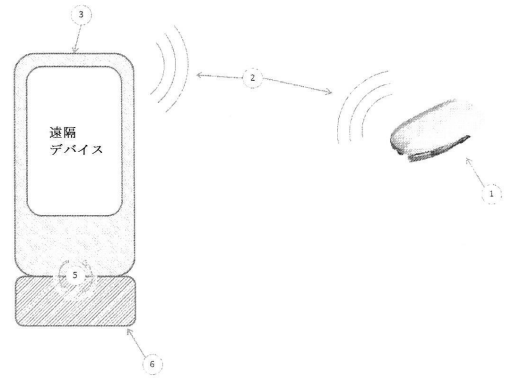
【図４】


患者
遠隔デバイス
SIMカード
ポンプユニット
使用者が値を入力する
この値を設定する
相互理解を確認する
ポンプがこの値を記憶し、データを暗号化し送信する
遠隔デバイスが受信し、SIMへ送信する
SIMが記憶し復号し、データを遠隔デバイスへ送信する
読み戻し値を表示する
使用者の意図を確認する
確認する
保護されたトランザクション
SIMが記憶し暗号化し、データを遠隔デバイスへ送信する
遠隔デバイスが受信し、ポンプへ送信する
確認する
確認された場合に動作を実行する

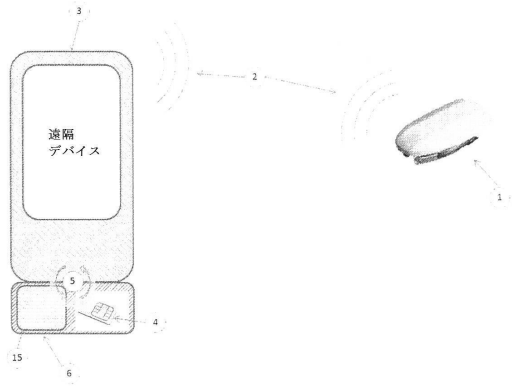
【図５】



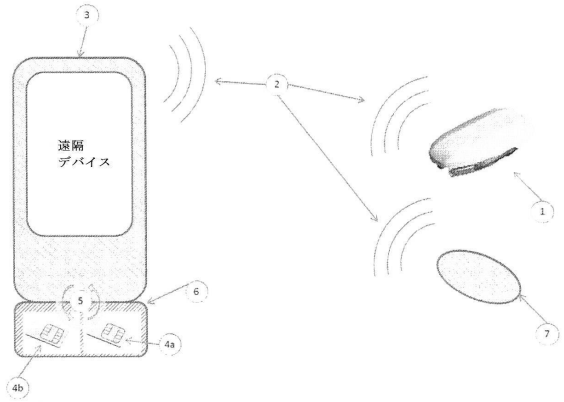
【図６】



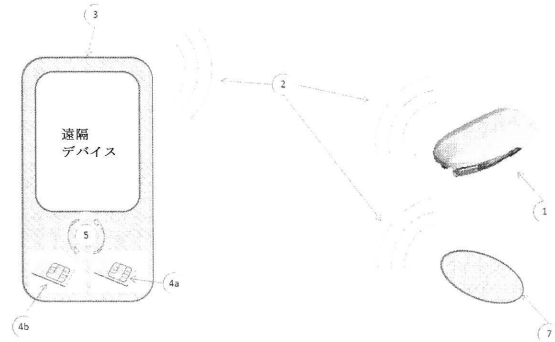
【図７】



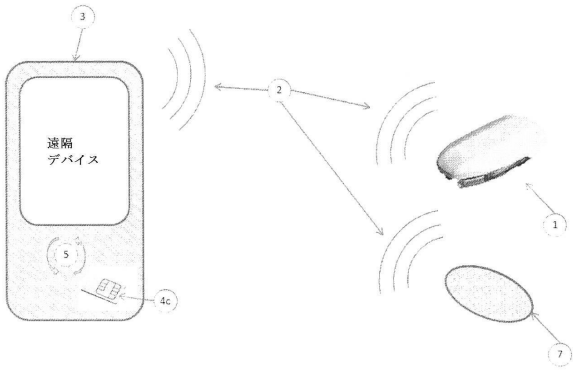
【図８】



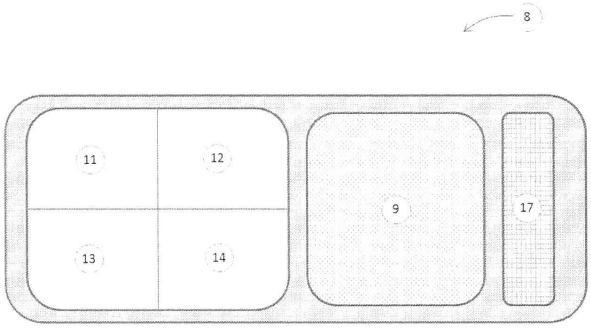
【図９】



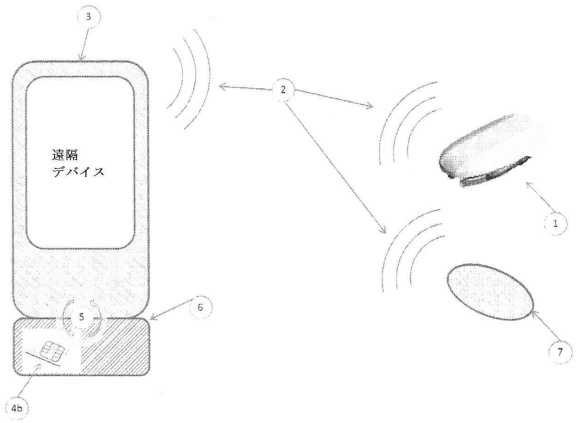
【図１０】



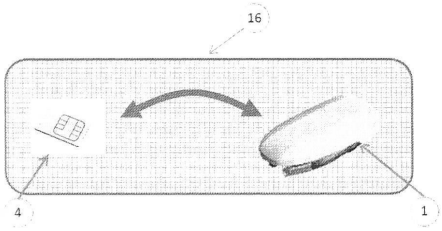
【図１１】



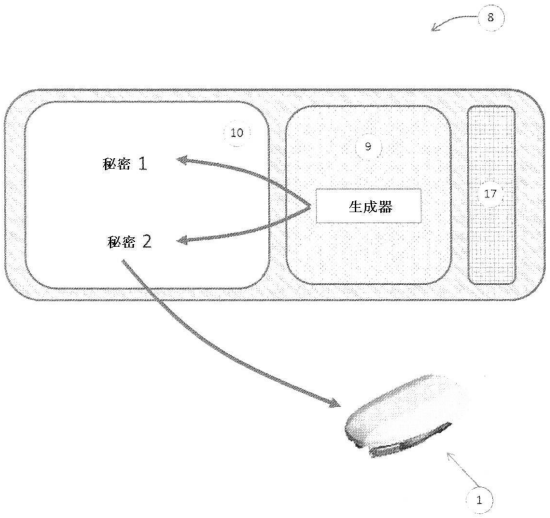
【図１２】



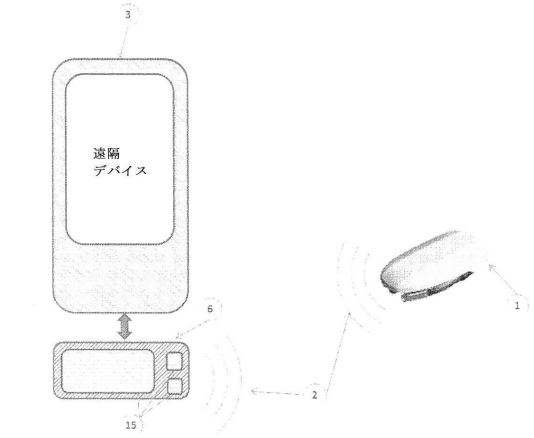
【図１３】



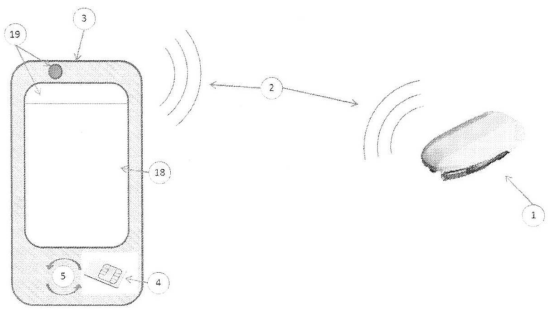
【図１４】



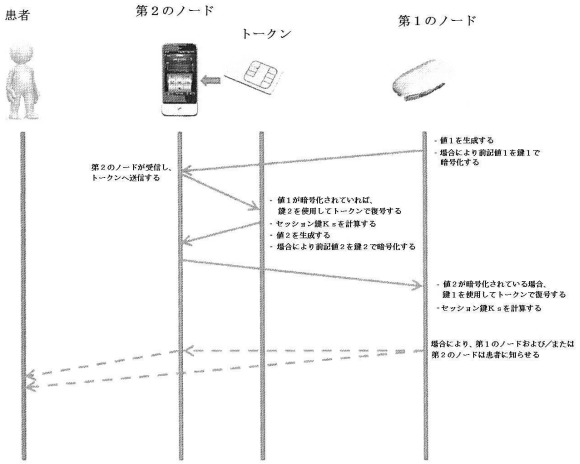
【図１５】



【図１６】



【図１７】



フロントページの続き

(72)発明者　パスカル・ボーアーミースター
スイス国ＣＨ－１００４ローザンヌ．アヴェニュ　ドゥ　セヴェリン２８
(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

審査官　青木　重徳

(56)参考文献　特表２００９－５３０８８０（ＪＰ，Ａ）
特表２０１１－５２１５８１（ＪＰ，Ａ）
特開２００９－１２４４２９（ＪＰ，Ａ）
特開２００３－０２３４３３（ＪＰ，Ａ）
特表２０１０－５０７９２８（ＪＰ，Ａ）
特表２００７－５２４３１２（ＪＰ，Ａ）
特表２０１０－５１０５８６（ＪＰ，Ａ）
岡本　龍明　ほか，シリーズ／情報科学の数学　現代暗号，日本，産業図書株式会社，１９９８年　6月３０日，初版第２刷，ｐ．２０２

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／０８
Ａ６１Ｍ　　５／１６８
Ｈ０４Ｌ　　９／３２