(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4680187号
(P4680187)
(45)発行日　平成23年5月11日(2011.5.11)　(24)登録日　平成23年2月10日(2011.2.10)

(51)Int.Cl.　　F I
A61N 1/37 (2006.01)　　A61N 1/37
A61B 5/00 (2006.01)　　A61B 5/00 102D
A61B 5/00 102C

請求項の数 31　(全 18 頁)

(21)出願番号　特願2006-517513 (P2006-517513)
(86)(22)出願日　平成16年6月22日 (2004.6.22)
(65)公表番号　特表2007-524456 (P2007-524456A)
(43)公表日　平成19年8月30日 (2007.8.30)
(86)国際出願番号　PCT/US2004/019902
(87)国際公開番号　WO2005/000397
(87)国際公開日　平成17年1月6日 (2005.1.6)
審査請求日　平成19年6月20日 (2007.6.20)
(31)優先権主張番号　10/601,763
(32)優先日　平成15年6月23日 (2003.6.23)
(33)優先権主張国　米国(US)

(73)特許権者　505003528
カーディアック　ペースメイカーズ，　インコーポレイテッド
アメリカ合衆国　５５１１２－５７９８
ミネソタ，　セントポール，　ハムライン　アベニュー　ノース　４１００
(74)代理人　100078282
弁理士　山本　秀策
(74)代理人　100062409
弁理士　安村　高明
(74)代理人　100113413
弁理士　森下　夏樹

最終頁に続く

(54)【発明の名称】埋め込み可能な医療装置のための安全な遠隔測定

(57)【特許請求の範囲】
【請求項１】
埋め込み可能な医療装置（ＩＭＤ）と外部装置（ＥＤ）との間で遠隔測定チャンネルを介して安全な通信を行うことを可能にする方法であって、
該方法は、
該遠隔測定チャンネルを介した該ＥＤと該ＩＭＤとの間の通信を制限する遠隔測定インターロックを実装することであって、該遠隔測定インターロックがリリースされていない場合、該ＩＭＤから該ＥＤへのデータの送信を可能にする該遠隔測定チャンネルを介したデータ通信セッションが確立されることが可能であるが、該遠隔測定インターロックがリリースされない限り、該ＥＤによる該ＩＭＤのプログラミングが実行されることが可能でない、ことと、
該ＩＭＤに物理的に近いことを必要とする短距離通信チャンネルを介してイネーブル・コマンドを該ＩＭＤに送信することによって、該遠隔測定インターロックをリリースすることと、
該ＥＤが、該ＩＭＤにより所有されていることが期待されている暗号化キーの使用の証拠を示すメッセージを該ＩＭＤから受信した場合、該ＥＤに対して該ＩＭＤを認証することと、
該ＩＭＤが、該ＥＤにより所有されていることが期待されている暗号化キーの使用の証拠を示すメッセージを該ＥＤから受信した場合、該ＩＭＤに対して該ＥＤを認証することと、

該ＩＭＤおよび該ＥＤが互いに認証された後にのみ、該遠隔測定チャンネルを介した該ＩＭＤと該ＥＤとの間のデータ通信セッションが生じることを可能にすることと
を包含する、方法。
【請求項２】
前記データ通信セッションの間、前記ＥＤと前記ＩＭＤとの間の通信を暗号化することをさらに包含する、請求項１に記載の方法。
【請求項３】
データ通信セッションが終了した後に、前記遠隔測定インターロックが再起動され、該遠隔測定インターロックが再びリリースされるまで、前記遠隔測定チャンネルを介した通信を制限する、請求項１に記載の方法。
【請求項４】
前記遠隔測定インターロックがリリースされるまで、前記ＥＤと前記ＩＭＤとの間の通信が生じることが可能でない、請求項１に記載の方法。
【請求項５】
前記遠隔測定チャンネルは、遠距離場無線周波数通信リンクである、請求項１に記載の方法。
【請求項６】
前記遠隔測定チャンネルは、インターネットリンクを含む、請求項１に記載の方法。
【請求項７】
前記短距離通信チャンネルは、前記ＩＭＤと別の装置との間の誘導通信リンクである、請求項１に記載の方法。
【請求項８】
前記短距離通信チャンネルは、前記ＩＭＤ内のスイッチであり、該ＩＭＤは、磁石によって起動され、該磁石は、該ＩＭＤと該磁石との間の距離が所定の距離よりも短くなるように該ＩＭＤの近くに保持されており、それによって、前記遠隔測定インターロックをリリースする、請求項１に記載の方法。
【請求項９】
前記ＥＤと前記ＩＭＤとは、公開キー暗号化方法を用いて互いに認証され、
この認証は、
該ＥＤが、該ＩＭＤにより所有されていることが期待されている対応するプライベートキーを有する公開キー用いて第１のメッセージを暗号化し、該暗号化された第１のメッセージを該ＩＭＤに前記遠隔測定チャンネルを介して送信し、その応答として、該第１のメッセージに由来するメッセージを該ＩＭＤから受信し、それにより、該メッセージが、該ＩＭＤによる該対応するプライベートキーの所有の証拠を示す場合、該ＥＤに対して該ＩＭＤを認証することと、
該ＩＭＤが、該ＥＤにより所有されていることが期待されている対応するプライベートキーを有する公開キー用いて第２のメッセージを暗号化し、該暗号化された第２のメッセージを該ＥＤに該遠隔測定チャンネルを介して送信し、その応答として、該第２のメッセージに由来するメッセージを該ＥＤから受信し、それにより、該メッセージが、該ＥＤによる該対応するプライベートキーの所有の証拠を示す場合、該ＩＭＤに対して該ＥＤを認証することと
によって達成される、請求項１に記載の方法。
【請求項１０】
認証のために前記ＩＭＤまたは前記ＥＤによって送られた、前記第１のメッセージに由来する前記メッセージは、該第１のメッセージを含み、認証のために該ＩＭＤまたは該ＥＤによって送られた、前記第２のメッセージに由来する該メッセージは、該第２のメッセージを含む、請求項９に記載の方法。
【請求項１１】
前記第１のメッセージは、前記ＥＤによって生成された乱数を含み、前記第２のメッセージは、前記ＩＭＤによって生成された乱数を含む、請求項９に記載の方法。

【請求項１２】
前記第１のメッセージは、前記ＥＤの識別コードを含み、前記第２のメッセージは、前記ＩＭＤの識別コードを含む、請求項９に記載の方法。
【請求項１３】
前記ＩＭＤによって送信され、前記第１のメッセージに由来する前記メッセージは、該ＥＤの前記公開キーを用いて暗号化され、前記ＥＤによって送信され、前記第２のメッセージに由来する該メッセージは、該ＩＭＤの該公開キーを用いて暗号化される、請求項９に記載の方法。
【請求項１４】
前記ＩＭＤによって送信される、前記第１のメッセージに由来する前記メッセージは、前記第２のメッセージを含む、請求項９に記載の方法。
【請求項１５】
前記データ通信セッションの間、前記ＥＤと前記ＩＭＤとの間の通信を秘密キー暗号化方法を用いて暗号化することをさらに包含し、該秘密キーデータ通信セッションは、該ＥＤまたは該ＩＭＤのいずれか一方が、該ＥＤまたは該ＩＭＤの他方に、該他方の公開キーによって暗号化された秘密セッションキーを送信することによって確立される、請求項９に記載の方法。
【請求項１６】
前記ＥＤまたは前記ＩＭＤのいずれか一方がセッションのインスティゲータとして指定され、該ＥＤまたは該ＩＭＤの他方がセッションの受信者として指定され、該ＥＤと該ＩＭＤは、公開キー暗号化方法を用いて互いに認証され、
この認証は、
該インスティゲータが、該受信者により所有されていることが期待されている対応するプライベートキーを有する公開キーを用いて第１のメッセージを暗号化することであって、該第１のメッセージは、該インスティゲータの識別コードと乱数R_Aとを含み、該インスティゲータが、前記遠隔測定チャンネルを介して該受信者に該暗号化された第１のメッセージを送信する、ことと、
該受信者が、該受信者のプライベートキーを用いて該第１のメッセージを解読し、該第１のメッセージ内に含まれている該識別コードを使用して、該インスティゲータによって所有されていることが期待されている対応するプライベートキーを有する公開キーをルックアップし、該インスティゲータの該公開キーを用いて第２のメッセージを暗号化することであって、該第２のメッセージは、該受信者の識別コードと該乱数R_Aと第２の乱数R_Bとを含む、ことと、
該受信者が、該遠隔測定チャンネルを介して該インスティゲータに該暗号化された第２のメッセージを送信することと、
該インスティゲータが、該第２のメッセージの暗号化に使用された該公開キーに対応する該インスティゲータのプライベートキーを用いて該第２のメッセージを解読し、該第２のメッセージがR_Aを含むことを検証し、それによって該受信者を認証することと、
該インスティゲータが、該第２のメッセージに由来する第３のメッセージを該受信者の該公開キーを用いて暗号化することであって、該第３のメッセージは、該乱数R_Bを含む、ことと、
該インスティゲータが、該遠隔測定チャンネルを介して該受信者に該暗号化された第３のメッセージを送信することと、
該受信者が、該第３のメッセージの暗号化に使用された該公開キーに対応する該受信者のプライベートキーを用いて該第３のメッセージを解読し、該第３のメッセージがR_Bを含むことを検証し、それによって該インスティゲータを認証することと
によって達成される、請求項１に記載の方法。
【請求項１７】
前記データ通信セッションの間、前記インスティゲータと前記受信者との間の通信を秘密キー暗号化方法を用いて暗号化することをさらに包含し、該秘密キーデータ通信セッシ

ョンは、該インスティゲータが、該受信者の公開キーにより暗号化された秘密セッションキーを、該受信者に送信することによって確立される、請求項１６に記載の方法。
【請求項１８】
前記秘密セッションキーは、前記インスティゲータによって送信される前記第３のメッセージ内に含められる、請求項１７に記載の方法。
【請求項１９】
埋め込み可能な医療装置（ＩＭＤ）と外部装置（ＥＤ）との間で遠隔測定チャンネルを介して安全な通信を行うことを可能にする方法であって、
該方法は、
遠隔測定インターロックを実装することであって、該遠隔測定インターロックは、該ＩＭＤに物理的に近いことを必要とする短距離通信チャンネルを介してイネーブル・コマンドを該ＩＭＤに送信することによってリリースされる、ことと、
該遠隔測定インターロックがリリースされるまで、該遠隔測定チャンネルを介した該ＩＭＤと該ＥＤとの間のデータ通信を制限することであって、該遠隔測定インターロックがリリースされていない場合、該ＩＭＤから該ＥＤへのデータの送信を可能にする該遠隔測定チャンネルを介したデータ通信セッションが確立されることが可能であるが、該遠隔測定インターロックがリリースされない限り、該ＥＤによる該ＩＭＤのプログラミングが実行されることが可能でない、ことと、
該ＥＤが、該遠隔測定チャンネルを介して第１のメッセージを該ＩＭＤに送信し、その応答として、該ＩＭＤにより所有されていることが期待されている秘密キーによって暗号化され、該第１のメッセージに由来するメッセージを受信した場合に、該ＥＤに対して該ＩＭＤを認証することと、
該ＩＭＤが、該遠隔測定チャンネルを介して第２のメッセージを該ＥＤに送信し、その応答として、該ＥＤにより所有されていることが期待されている秘密キーによって暗号化され、該第２のメッセージに由来するメッセージを受信した場合に、該ＩＭＤに対して該ＥＤを認証することと
を包含する、方法。
【請求項２０】
前記遠隔測定チャンネルを介したデータ通信セッションが終了した後に、前記遠隔測定インターロックが再起動され、該遠隔測定インターロックが再びリリースされるまで、該遠隔測定チャンネルを介した通信を制限する、請求項１９に記載の方法。
【請求項２１】
前記遠隔測定インターロックがリリースされるまで、前記遠隔測定チャンネルを介した前記ＥＤと前記ＩＭＤとの間の通信が生じることが可能でない、請求項１９に記載の方法。
【請求項２２】
前記短距離通信チャンネルは、前記ＩＭＤと別の装置との間の誘導通信リンクである、請求項１９に記載の方法。
【請求項２３】
前記短距離通信チャンネルは、前記ＩＭＤ内のスイッチであり、該ＩＭＤは、磁石によって起動され、該磁石は、該ＩＭＤと該磁石との間の距離が所定の距離よりも短くなるように該ＩＭＤの近くに保持されており、それによって、前記遠隔測定インターロックをリリースする、請求項１９に記載の方法。
【請求項２４】
埋め込み可能な医療装置（ＩＭＤ）と外部装置（ＥＤ）との間で遠隔測定チャンネルを介して安全な通信を行うことを可能にする方法であって、
該方法は、
該ＥＤが、該ＩＭＤにより所有されていることが期待されている暗号化キーの使用の証拠を示すメッセージを該ＩＭＤから受信した場合、該ＥＤに対して該ＩＭＤを認証することと、

該ＩＭＤが、該ＥＤにより所有されていることが期待されている暗号化キーの使用の証拠を示すメッセージを該ＥＤから受信した場合、該ＩＭＤに対して該ＥＤを認証することと、

該ＩＭＤと該ＥＤとの間の通信を制限することであって、該ＥＤが該ＩＭＤに対して認証されていない場合、該ＩＭＤから該ＥＤへのデータの送信を可能にする前記遠隔測定チャンネルを介したデータ通信セッションが確立されることが可能であるが、該ＥＤが該ＩＭＤに対して認証されない限り、該ＥＤによる該ＩＭＤのプログラミングが実行されることが可能でない、ことと

を包含する、方法。

【請求項２５】

前記ＥＤと前記ＩＭＤとは、公開キー暗号化方法を用いて互いに認証され、

この認証は、

該ＥＤが、該ＩＭＤにより所有されていることが期待されている対応するプライベートキーを有する公開キー用いて第１のメッセージを暗号化し、該暗号化された第１のメッセージを該ＩＭＤに前記遠隔測定チャンネルを介して送信し、その応答として、該第１のメッセージに由来するメッセージを該ＩＭＤから受信し、それにより、該メッセージが、該ＩＭＤによる該対応するプライベートキーの所有の証拠を示す場合、該ＥＤに対して該ＩＭＤを認証することと、

該ＩＭＤが、該ＥＤにより所有されていることが期待されている対応するプライベートキーを有する公開キー用いて第２のメッセージを暗号化し、該暗号化された第２のメッセージを該ＥＤに該遠隔測定チャンネルを介して送信し、その応答として、該第２のメッセージに由来するメッセージを該ＥＤから受信し、それにより、該メッセージが、該ＥＤによる該対応するプライベートキーの所有の証拠を示す場合、該ＩＭＤに対して該ＥＤを認証することと

によって達成される、請求項２４に記載の方法。

【請求項２６】

前記ＥＤと前記ＩＭＤとは、秘密キー暗号化方法を用いて互いに認証され、

この認証は、

該ＥＤが、該遠隔測定チャンネルを介して第１のメッセージを該ＩＭＤに送信し、その応答として、該ＩＭＤにより所有されていることが期待されている秘密キーによって暗号化され、該第１のメッセージに由来するメッセージを受信した場合に、該ＥＤに対して該ＩＭＤを認証することと、

該ＩＭＤが、該遠隔測定チャンネルを介して第２のメッセージを該ＥＤに送信し、その応答として、該ＥＤにより所有されていることが期待されている秘密キーによって暗号化され、該第２のメッセージに由来するメッセージを受信した場合に、該ＩＭＤに対して該ＥＤを認証することと

によって達成される、請求項２４に記載の方法。

【請求項２７】

埋め込み可能な医療装置（ＩＭＤ）と外部装置（ＥＤ）との間で遠隔測定チャンネルを介して安全な通信を行うことを可能にする方法であって、

該方法は、

該ＩＭＤが、該ＥＤにより所有されていることが期待されている暗号化キーの使用の証拠を示すメッセージを該ＥＤから受信した場合、該ＩＭＤに対して該ＥＤを認証することと、

該ＥＤと該ＩＭＤとの間の通信を制限することであって、該ＥＤが該ＩＭＤに対して認証されていない場合、該ＩＭＤから該ＥＤへのデータの送信を可能にする前記遠隔測定チャンネルを介したデータ通信セッションが確立されることが可能であるが、該ＥＤが該ＩＭＤに対して認証されない限り、該ＥＤによる該ＩＭＤのプログラミングが実行されることが可能でない、ことと

を包含する、方法。

【請求項２８】
埋め込み可能な医療装置（ＩＭＤ）と外部装置（ＥＤ）との間で遠隔測定チャンネルを介して安全な通信を行うことを可能にするシステムであって、
該システムは、
該遠隔測定チャンネルを介した該ＥＤと該ＩＭＤとの間の通信を制限する遠隔測定インターロックを実装する手段であって、該遠隔測定インターロックがリリースされていない場合、該ＩＭＤから該ＥＤへのデータの送信を可能にする該遠隔測定チャンネルを介したデータ通信セッションが確立されることが可能であるが、該遠隔測定インターロックがリリースされない限り、該ＥＤによる該ＩＭＤのプログラミングが実行されることが可能でない、手段と、
該ＩＭＤに物理的に近いことを必要とする短距離通信チャンネルを介してイネーブル・コマンドを該ＩＭＤに送信することによって、該遠隔測定インターロックをリリースする手段と、
該ＥＤが、該ＩＭＤにより所有されていることが期待されている暗号化キーの使用の証拠を示すメッセージを該ＩＭＤから受信した場合、該ＥＤに対して該ＩＭＤを認証する手段と、
該ＩＭＤが、該ＥＤにより所有されていることが期待されている暗号化キーの使用の証拠を示すメッセージを該ＥＤから受信した場合、該ＩＭＤに対して該ＥＤを認証する手段と、
該ＩＭＤおよび該ＥＤが互いに認証された後にのみ、該遠隔測定チャンネルを介した該ＩＭＤと該ＥＤとの間のデータ通信セッションが生じることを可能にする手段と
を備えている、システム。
【請求項２９】
埋め込み可能な医療装置（ＩＭＤ）と外部装置（ＥＤ）との間で遠隔測定チャンネルを介して安全な通信を行うことを可能にするシステムであって、
該システムは、
該ＩＭＤに対し物理的に近いことを必要とする短距離通信チャンネルを介してイネーブル・コマンドを該ＩＭＤに送信することによってリリースされる遠隔測定インターロックを実装する手段と、
該遠隔測定インターロックがリリースされるまで、該遠隔測定チャンネルを介した該ＥＤと該ＩＭＤとの間のデータ通信を制限する手段であって、該遠隔測定インターロックがリリースされていない場合、該ＩＭＤから該ＥＤへのデータの送信を可能にする該遠隔測定チャンネルを介したデータ通信セッションが確立されることが可能であるが、該遠隔測定インターロックがリリースされない限り、該ＥＤによる該ＩＭＤのプログラミングが実行されることが可能でない、手段と、
該ＥＤが、該遠隔測定チャンネルを介して第１のメッセージを該ＩＭＤに送信し、その応答として、該ＩＭＤにより所有されていることが期待されている秘密キーによって暗号化され、該第１のメッセージに由来するメッセージを受信した場合に、該ＥＤに対して該ＩＭＤを認証する手段と、
該ＩＭＤが、該遠隔測定チャンネルを介して第２のメッセージを該ＥＤに送信し、その応答として、該ＥＤにより所有されていることが期待されている秘密キーによって暗号化され、該第２のメッセージに由来するメッセージを受信した場合に、該ＩＭＤに対して該ＥＤを認証する手段と
を備えている、システム。
【請求項３０】
前記短距離通信チャンネルは、前記ＩＭＤと別の装置との間の誘導通信リンクである、請求項２９に記載のシステム。
【請求項３１】
前記短距離通信チャンネルは、前記ＩＭＤ内のスイッチであり、該ＩＭＤは、磁石によって起動され、該磁石は、該ＩＭＤと該磁石との間の距離が所定の距離よりも短くなるよ

うに該ＩＭＤの近くに保持されており、それによって、前記遠隔測定インターロックをリリースする、請求項２９に記載のシステム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、心臓ペースメーカや埋め込み可能な電気的除細動器／除細動器等の埋め込み可能な医療装置に関する。より詳細に述べれば、本発明は遠隔測定データをその種の装置から送信するためのシステムと方法に関する。

【背景技術】

【０００２】

ペースメーカや電気的除細動器／除細動器等の心臓リズム管理装置を含む、埋め込み可能な医療装置（ＩＭＤ）は、通常、無線周波数遠隔測定リンクを介して外部プログラマと呼ばれる外部装置とデータを通信する能力を有する。その種の外部プログラマの１つの用途は、埋め込み可能な医療装置の動作パラメータをプログラムすることである。たとえばペースメーカの、ペーシング・モードやそのほかの動作特性は、一般に埋め込みの後にこの方法で修正される。近代的な埋め込み可能装置は、両方向通信のための能力も含んでおり、その結果、埋め込まれた装置からプログラマへ情報を送信することができる。埋め込み可能装置から一般に遠隔測定されるデータは、種々の動作パラメータや生理学的データであり、後者は、リアルタイムで収集されるか、以前のモニタリング動作からストアされる。

【０００３】

外部プログラマは、一般に誘導リンクを介してＩＭＤと通信するべく構成されている。外部プログラマ内のコイル・アンテナとＩＭＤが誘導結合され、その結果、２つの結合されたコイルの共振周波数に対応する無線周波数の搬送波形を変調することによってデータを送信することができる。誘導リンクは、外部装置のコイル・アンテナがＩＭＤに、通常は数インチ内まで近接することを必要とする短距離通信チャンネルである。別のタイプの遠隔測定システムは、フラウンホーファ領域の電磁放射あるいは別のタイプのデータ・リンク、たとえば電話回線またはネットワーク（インターネットを含む）等を使用してより大きな距離にわたって通信することができる。その種の長距離遠隔測定は、埋め込み可能な装置が遠隔地のモニタリング・ユニットへデータを送信すること、あるいは遠隔地からそれをプログラムすることができる。このように長距離遠隔測定は、医師が部屋を隔てて、さらには国までも隔てて患者をモニタし、患者の継続管理を行うことを可能にする。

【０００４】

【特許文献１】米国特許第４，５６２，８４１号

【発明の開示】

【発明が解決しようとする課題】

【０００５】

しかしながら埋め込み可能な医療装置のための長期遠隔測定は、短距離遠隔測定には存在しない特殊な問題をもたらす。誘導リンク等の短距離通信チャンネルを介した埋め込み可能な装置は、外部装置が患者の近くにあることを必要し、そのため医師には、誰の埋め込み可能な装置のプログラムが行われているかがわかり、患者には、埋め込み可能な装置のプログラムと、それからのデータの受信を誰が行っているかがわかる。これに対して長距離遠隔測定は、その種の物理的な近接を必要とせず、医師が誤った装置を不用意にプログラムする可能性を与える。フラウンホーファ領域の電磁放射もしくは何らかの種類のネットワークを介する通信は、意図していないユーザによる通信の傍受も可能にし、その患者のプライバシ問題を浮揚させる。悪意のあるユーザが、長距離遠隔測定システムを使用して埋め込み済み装置の再プログラムを試みることも考えられる。本発明は、これらの問題に注目した長距離遠隔測定を提供するためのシステムと方法である。

【課題を解決するための手段】

【０００６】

本発明は、遠隔測定チャンネルを介した埋め込み可能な医療装置（ＩＭＤ）と外部装置（ＥＤ）の間の安全な通信を可能にするための方法とシステムに関係する。一実施態様においては、遠隔測定インターロックが具体化され、それが遠隔測定チャンネルを介したＥＤとＩＭＤの間の任意の通信を制限する。遠隔測定インターロックは、ＩＭＤに対する物理的な近接を必要とする短距離通信チャンネルを介し、ＥＤがＩＭＤに対してイネーブル・コマンドを送信するときにリリースされる。別の実施態様においては、ＩＭＤとＥＤが互いに対して認証された後に限って、ＩＭＤとＥＤの間において遠隔測定チャンネルを介したデータ通信セッションを生じさせることができる。ＩＭＤは、ＥＤが、ＩＭＤによる所有が期待されている暗号化キーの使用の証拠を示すＩＭＤからのメッセージを受信するときにＥＤに対して認証され、ＥＤは、ＩＭＤが、ＥＤによる所有が期待されている暗号化キーの使用の証拠を示すＥＤからのメッセージを受信するときにＩＭＤに対して認証される。

【発明を実施するための最良の形態】

【０００７】

本発明は、埋め込み済み装置の悪意のある、あるいは不用意な再プログラムの可能性に対して保護する埋め込み可能な医療装置のための長距離遠隔測定に関係する。別の側面においては、このシステムは、データ送信の機密性の維持も提供する。この種の患者の安全と機密性の確保は、３つの別々のテクニックを使用して達成することができる：すなわち、データの暗号化、遠隔測定セッションにおける関係者の認証、遠隔測定インターロックである。

【０００８】

１．暗号化／解読

暗号化とは、メッセージがそのメッセージを解読する特別なキーの所有なしに読むことが不可能な方法でメッセージをエンコードするために使用される暗号方法のアルゴリズムを言う。メッセージの暗号化は、そのメッセージに対する暗号化関数を適用することによって行われる。その暗号化関数は、暗号方法のアルゴリズムと暗号化キーによって定義される。以下の説明や参照図面においては、その種の暗号化されたメッセージをＥ（ｍ，ｋ）として示す。Ｅは暗号化関数、ｍは暗号化未済メッセージ、ｋはそのメッセージの暗号化に使用されるキーである。メッセージの解読は、解読キーｋを使用して逆関数Ｄを暗号化済みメッセージｍに適用することを伴い、Ｄ（ｍ，ｋ）と表される。

【０００９】

暗号化キーと解読キーは、使用されている暗号方法のアルゴリズムのタイプによって同一のこともあれば、異なることもある。秘密キー暗号方法においては、通信している両方の関係者が単一の秘密キーを共有し、それがメッセージの暗号化と解読の両方に使用される。したがって、秘密キー暗号化関数Ｅによってキーｋを用いて暗号化されたメッセージｍは、解読関数Ｄを同一のキーｋとともに適用することによって復元される：

ｍ＝Ｄ（Ｅ（ｍ，ｋ），ｋ）

秘密キー暗号方法のアルゴリズムのよく知られている例としては、ＤＥＳ（データ暗号化標準）、ＡＥＳ（米国暗号化標準）、トリプルＤＥＳ、ブローフィッシュが挙げられる。

【００１０】

これに対して公開キー暗号化方法では暗号化キーと解読キーが異なる。公開キー暗号化方法を使用して安全なメッセージを送信するためには、送信者が受信者の公開キーを用いてメッセージを暗号化するが、これはすべての認証済み送信者に知られており、また広く公開されて誰もがメッセージを送信できるようになっている。その後そのメッセージは、そのメッセージの暗号化に使用された公開キーに対応するプライベートキーによってのみ解読が可能であり、このプライベートキーは、メッセージの受信者によって保持され、ほかの誰とも共有されない。したがって、公開キー暗号化関数Ｅによって公開キーｋ１を用いて暗号化されたメッセージは、対応するプライベートキーｋ２とともに解読関数Ｄを適用することによって復元される：

ｍ＝Ｄ（Ｅ（ｍ，ｋ１），ｋ２）

安全な両方向通信セッションにおける各関係者は、そのためそれぞれ独自のプライベートキーを所有し、かつ相手の公開キーを知っていなければならない。公開キー暗号化方法のアルゴリズムのよく知られた例にＲＳＡがある。

【００１１】

公開キーもしくは秘密キー暗号化方法のいずれを使用しても安全にデータを送信することができるが、公開キー暗号化方法のアルゴリズムははるかに演算集約的となる。この理由から、埋め込み可能な装置と外部装置の間における実際のデータ通信のためには、秘密キー暗号化方法を使用する方が通常は好ましい。しかしながら後述するように、認証のために公開キー暗号化方法を使用して、データ通信に使用される秘密キーの送信を使用することができる。

【００１２】

２．認証

認証は、通信セッションにおける関係者が高い信頼性をもって互いを識別できるメカニズムまたはプロトコルを言う。認証プロトコルは、秘密キーまたは公開キー暗号化方法を使用して具体化され、埋め込み可能な医療装置（ＩＭＤ）と外部装置（ＥＤ）の互いを認証する。ＩＭＤとＥＤの間における遠隔測定チャンネルを介したデータ通信セッションは、ＩＭＤとＥＤが互いに対して認証された後に限って許可される。公開キーまたは秘密キーの暗号化方法のいずれかによる認証を用いて、ＩＭＤは、ＥＤが、ＩＭＤによる所有が期待されている暗号化キーの使用の証拠を示すメッセージをＩＭＤから受信するときにＥＤに対して認証され、ＥＤは、ＩＭＤが、ＥＤによる所有が期待されている暗号化キーの使用の証拠を示すメッセージをＥＤから受信するときにＩＭＤに対して認証される。

【００１３】

秘密キー暗号化方法による認証においては、ＥＤが遠隔測定チャンネルを介して第１のメッセージをＩＭＤに送信し、それに応答して、ＩＭＤによる所有が期待されている秘密キーによって暗号化されたその第１のメッセージから誘導されたメッセージを受信するとき、ＩＭＤがＥＤに対して認証される。続いてＩＭＤが遠隔測定チャンネルを介して第２のメッセージをＥＤに送信し、それに応答して、ＥＤによる所有が期待されている秘密キーによって暗号化されたその第２のメッセージから誘導されたメッセージを受信すると、ＥＤがＩＭＤに対して認証される。

【００１４】

公開キー暗号化方法を使用する認証プロトコルは次のように機能する。ＥＤが、ＩＭＤによる所有が期待されている対応するプライベートキーを有する公開キーを用いて第１のメッセージを暗号化し、その暗号化した第１のメッセージを、遠隔測定チャンネルを介してＩＭＤに送信し、それに応答してＩＭＤから、ＩＭＤによる対応するプライベートキーを所有している証拠を示す、第１のメッセージから誘導されたメッセージを受信すると、ＩＭＤがＥＤに対して認証される。またＥＤは、ＩＭＤが、ＥＤによる所有が期待されている対応するプライベートキーを有する公開キーを用いて第２のメッセージを暗号化し、その暗号化した第２のメッセージを、遠隔測定チャンネルを介してＥＤに送信し、それに応答してＥＤから、ＥＤによる対応するプライベートキーを所有している証拠を示す、第２のメッセージから誘導されたメッセージを受信すると、ＩＭＤに対して認証される。第１と第２のメッセージから誘導されるメッセージは、ＥＤとＩＭＤのための識別コード等の識別データとともにそれぞれ第１と第２のメッセージを含むこともできる。それぞれのための別々の送信に代えて、第１のメッセージから誘導されたメッセージと第２のメッセージを、結合されたメッセージとしてＩＭＤが送信してもよい（つまり、ＩＭＤによって送信される第１のメッセージから誘導されたメッセージが第２のメッセージを含む）。一実施形態においては、第１と第２のメッセージがＥＤとＩＭＤによって生成された乱数をそれぞれ含む。その場合、第１と第２のメッセージから誘導されたメッセージは、それぞれの乱数自体もしくはそれから誘導された数を含む（たとえば、その乱数を１インクリメントした数）。一方の関係者を他方に対して認証する応答の機密性を維持するために、第

１と第２のメッセージから誘導され、それぞれＩＭＤとＥＤによって送信されるメッセージを、それぞれＥＤとＩＭＤの公開キーを使用して暗号化してもよい。

【００１５】

３．遠隔測定インターロック

前述したとおり、暗号化方法のテクニックを、ＩＭＤとＥＤの相互に対する認証と、安全なデータの送信の両方に使用することができる。しかしながらあらゆる暗号化方法のテクニックは、秘密に保たれる秘密キーまたはプライベートキーに依存する。長距離遠隔測定に関して患者に追加の安全性を提供するために、ここで遠隔測定インターロックと呼んでいるテクニックが採用される。遠隔測定インターロックは、ＥＤとＩＭＤの間における長距離遠隔測定リンクを介した任意の通信を、インターロックがリリースされるまで制限するテクニックである。遠隔測定インターロックは、ＩＭＤに対する物理的な近接を必要とする短距離通信チャンネルを介して、ＩＭＤにイネーブル・コマンドを送信することによってリリースされる。一実施形態においては、インターロックがリリースされるまでいかなる情報の送信も許可されない。これは、より安全な実施形態である。第２の実施形態においては、限られた情報が許可されるが、装置のプログラミングは許可されない。この実施形態は、患者がインターロックをリリースする必要を伴わずに遠隔地における患者のモニタリングをサポートすることができる。

【００１６】

遠隔測定インターロックを具体化する１つの方法は、短距離通信チャンネルとして誘導リンクを使用することである。前述したように、伝統的な埋め込み可能な医療装置は、非常にレンジの短い（わずか数インチ）誘導遠隔測定リンクを有している。この遠隔測定インターロックの実装においては、ＩＭＤハードウエアが、長距離遠隔測定インターロックをリリースするために誘導的に交換されるキーを伴う誘導リンクが確立されることを必要とする。一実施形態においては、遠隔測定インターロックのリリースが数十分の後にタイムアウトし、セッションを継続するために再び装置の上で誘導ワンドを振ることが必要となる。別の実施形態においては、現在の遠隔測定セッションの終了まで遠隔測定インターロックが満了しない。

【００１７】

遠隔測定インターロックを具体化する別の方法は、磁石がＩＭＤの近くに保持されているときに遠隔測定インターロックがリリースされるように、短距離通信チャンネルとして磁石の静磁界を使用する。この実施形態は、ＩＭＤが誘導遠隔測定システムを装備していない場合に必要になると考えられる。その場合には、医師またはそのほかの、患者によって信頼されている者に、埋め込み可能な医療装置の上で磁石を振り、プログラミングをイネーブルすることが求められることになる。これにおいてもインターロックのリリースが、所定短時間後、もしくは現在の遠隔測定セッションの終了時に満了する。

【００１８】

これらのインターロック・テクニックは、いずれも、患者と物理的に非常に近接した者によってのみインターロックがリリース可能であることから、遠隔地のハッカーからの悪意のあるプログラミングを抑止することができる。またこれらのインターロック・テクニックは、有効なユーザによる不用意なプログラミングも抑止することができる。医師またはそのほかの認証されたユーザが偶発的に誤った装置を用いて遠隔測定セッションを立ち上げることが考えられるため（長距離遠隔測定は、医師のプログラマのレンジ内における複数の患者の存在を許可することになる）、誘導ワンドもしくは磁石を装置の上で振らなければプログラミングをイネーブルできないことは、医師が偶発的に誤った装置をプログラミングすることを防止する。

【００１９】

４．安全なデータ通信セッション

認証と遠隔測定インターロックのリリースが行われた後は、ＩＭＤとＥＤは、相手が詐称者でないとの知識の下にそれぞれの装置を用いて長距離遠隔測定リンクを介したデータ通信に進むことができる。しかしながらそのデータ通信セッションの間にデータが平文で

送信されると、傍受者がデータを傍受し、患者のプライバシを危険にさらしかねない。したがって、データ通信セッションの間は、ＥＤとＩＭＤの間における通信の一部もしくは全部を暗号化することが望ましい。すべに述べたように、秘密キー暗号化は、公開キー暗号化よりはるかに演算集約的でなく、比較的大量のデータの送信には好ましい。秘密キー暗号化方法が認証に使用される場合には、ＥＤとＩＭＤは、データ送信用に同一の秘密キーを使用することができる。公開キー暗号化方法が認証に使用される場合には、データ通信のために秘密キー暗号化方法を使用することが可能であり、それにおいてはＥＤまたはＩＭＤのいずれか一方が、ＥＤまたはＩＭＤのいずれか他方に対して、当該他方の公開キーにより暗号化した秘密セッションキーを送信する。その後、両方の関係者がこの秘密セッションキーを使用してデータを暗号化することができる。

【００２０】

４．ハードウエア例の説明

図１は、遠隔測定コンポーネント、すなわち埋め込み可能な医療装置１と、２つの代表的な外部装置２、３のブロック図である。これらの装置のそれぞれは、ディジタル・データの処理のためのマイクロプロセッサまたはそのほかのタイプのコントローラを有し、それぞれ１０、２０、３０として示されている。それぞれの装置内のコントローラによって実行されるソフトウエアまたはファームウエアは、種々の通信アルゴリズムやプロトコルを実装でき、それには前述した暗号化、認証、遠隔測定インターロック・スキームが含まれる。受信されるデータと送信されるデータは、変調された搬送波信号またはベースバンド信号のいずれかの受信と送信のために、それぞれの装置内のコントローラにインターフェースされる。それぞれの受信機には、搬送波信号またはベースバンド信号からディジタル・データを抽出するために復調器またはデコーダが組み込まれている。またそれぞれの送信機には、ディジタル・データを用いて搬送波信号を変調するため、あるいはベースバンド信号をエンコードするために変調器またはエンコーダが組み込まれている。それぞれの装置によって送信されるデータは、ディジタル・データであり、特定タイプのデータ・リンク内におけるベースバンド・データとして、あるいは変調された搬送波信号として直接送信することができる。いずれの場合においても、データは、情報の１ないしは複数のビットを表す記号の形式で送信される。たとえば、オン‐オフ振幅シフト・キーイングにおいては、それぞれのパルスが１またはゼロのいずれかを表す。別の変調方法（たとえば、Ｍ‐ａｒｙ変調テクニック）は、より多くの数のビットを表す記号を使用する。

【００２１】

外部装置２、３のそれぞれは、通常、埋め込み可能な装置１の再プログラムやそれからのダウンロードをともに行うことができる外部プログラマである。外部装置３は、誘導リンクを介した短距離遠隔測定のために設計された装置を表すことが意図されており、それにおいてはコイルＣ３が、埋め込み可能な装置の受信機１５と送信機１４とインターフェースする対応するコイルＣ１との誘導リンクのために、受信機３５と送信機３４にインターフェースする。コイルＣ３は、通常、埋め込み可能な装置の近くに位置決めするためにワンド内に組み込まれ、コイルＣ１は、通常、埋め込み可能な装置のケースの内側の周囲に巻き付けられる。外部プログラマと心臓ペースメーカのための誘導リンク遠隔測定システムの一例は、ブロックウエイほかに対して発行され、カーディアック・ペースメーカズ・インク（Ｃａｒｄｉａｃ　Ｐａｃｅｍａｋｅｒｓ，Ｉｎｃ．）に譲渡された特許文献１に述べられており、その開示は、参照によりこれに援用されている。外部装置２は、フラウンホーファ領域の無線送信またはネットワーク経由のいずれかを用いて実装される長距離遠隔測定リンクを介して埋め込み可能な装置１と通信する装置を示すことが意図されている。長距離遠隔測定リンクを介して装置間におけるデータの送受を行うため、埋め込み可能な装置１内のコントローラとデータ受信機１１およびデータ送信機１２がインターフェースされ、外部装置２内のコントローラとデータ受信機２１およびデータ送信機２２がインターフェースされる。フラウンホーファ領域の無線リンクの場合には、埋め込み可能な装置１と外部装置２の受信機／送信機のペアが、それぞれアンテナＡ１、Ａ２とインターフェースされる。長距離遠隔測定がネットワークを介して実装される場合には、外部装

置２の受信機／送信機のペアは、ネットワーク接続にインターフェースされることになるが、埋め込み可能な装置１は、ネットワーク接続を伴う中継器ユニットとワイヤレスでインターフェースされることになろう。

【００２２】

また埋め込み可能な装置１には、磁気的に作動されるスイッチＳ１とそれに関連付けされたプルアップ抵抗Ｒ１が備えられており、それがコントローラ１０とインターフェースされている。この実施形態においては、遠隔測定インターロックが、コイルＣ１、Ｃ３によって構成される誘導リンクを介して外部装置３から送信されたコマンドによってリリースされるか、あるいは外部マグネットＭ１の近接によるスイッチＳ１の作動が使用されて遠隔測定インターロックがリリースされる。別の実施形態においては、埋め込み可能な装置が、おそらくは遠隔測定インターロックをリリースするために、１つのタイプの短距離通信チャンネルだけ、つまり磁気的に作動されるスイッチだけ、または誘導リンク遠隔測定システムだけしか有していないこともある。遠隔測定インターロックをリリースするための別のタイプの短距離通信チャンネルも可能であり、それには容量性リンクまたは物理的に取り付けられたスイッチを用いて実装される短距離遠隔測定システムが含まれる。

【００２３】

５．特定の実施形態の例

前述したとおり、本発明に従った、埋め込み可能な医療装置のために安全な長距離遠隔測定を提供するシステムは次のうちの任意の１つまたは全部を含むことができる：すなわち（１）短距離通信チャンネルを介してリリースされる遠隔測定インターロック、（２）外部装置と埋め込み可能な装置が互いを識別することができる認証プロトコル、（３）患者のプライバシを確保する長距離遠隔測定通信の暗号化である。以下は、これらの特徴を組み込むスキームの例の説明である。

【００２４】

１つの特定の実施形態においては、前述した遠隔測定インターロック・テクニックが、長距離遠隔測定セッションの開始前の安全性を提供するための単独の手段として使用され、暗号化方法による認証プロトコルが使用されず、平文でデータが送信される。別の実施形態においては、長距離遠隔測定セッションの開始のための安全性を提供するために、暗号化方法による認証だけが使用され、遠隔測定インターロックの使用を伴わない。これらの実施形態のいずれにおいても、遠隔測定インターロックのリリースがないか、あるいは暗号化方法による認証がなければ、長距離遠隔測定セッションが完全に防止されるか、特定タイプのデータ送信に限定される。たとえば、遠隔測定インターロックのリリースがないか、あるいは暗号化方法による認証がない場合に長距離遠隔測定を介した埋め込み可能な装置のプログラムを外部装置に許可することは、おそらくは望ましくないが、その場合であっても暗号化を伴うか、あるいはそれを伴わない埋め込み可能な装置からの特定のデータの送信を許可することは可能であろう。別の実施形態においては、暗号化方法による認証と遠隔測定インターロックのいずれも使用されないが、埋め込み可能な装置が公開キーもしくは秘密キー暗号化のいずれかを使用し、長距離遠隔測定リンクを介して特定タイプのデータを外部装置へ送信する。

【００２５】

埋め込み可能な医療装置（ＩＭＤ）と外部装置（ＥＤ）の間における遠隔測定チャンネルを介した安全な通信を可能にするための方法またはシステムの一例の実施形態は、遠隔測定チャンネルを介したＥＤとＩＭＤの間における任意の通信を制限する遠隔測定インターロックを含む。遠隔測定インターロックは、ＩＭＤに対する物理的な近接を必要とする短距離通信チャンネルを介してＩＭＤにイネーブル・コマンドを送信することによってリリースされる。ＩＭＤは、ＩＭＤによって所有することが期待されている暗号化キーの使用の証拠を示すＩＭＤからのメッセージをＥＤが受信すると、ＥＤに対して認証され、ＥＤは、ＥＤによって所有することが期待されている暗号化キーの使用の証拠を示すＥＤからのメッセージをＩＭＤが受信すると、ＩＭＤに対して認証される。その後、ＩＭＤとＥＤが互いに対して認証された後に限り、遠隔測定チャンネルを介したＩＭＤとＥＤの間の

データ通信セッションが許可される。この認証には、公開キーまたは秘密キーの暗号化方法を使用することができる。別の例の実施形態においては、遠隔測定チャンネルを介したＩＭＤとＥＤの間の安全な通信が、ＩＭＤへの物理的な近接を必要とする短距離通信チャンネルを介したＩＭＤへのイネーブル・コマンドの送信によってリリースされる遠隔測定インターロックだけによって提供される。ＩＭＤとＥＤの間における遠隔測定チャンネルを介したデータ通信は、遠隔測定インターロックがリリースされるまで制限される。

【００２６】

別の実施形態においては、ＩＭＤによって所有することが期待されている暗号化キーの使用の証拠を示すＩＭＤからのメッセージをＥＤが受信すると、ＥＤに対してＩＭＤを認証し、ＥＤによって所有することが期待されている暗号化キーの使用の証拠を示すＥＤからのメッセージをＩＭＤが受信すると、ＩＭＤに対してＥＤを認証し、かつＩＭＤがＥＤに対して認証された後に限り、遠隔測定チャンネルを介したＩＭＤとＥＤの間のデータ通信セッションを許可することによって、ＩＭＤとＥＤの間における遠隔測定チャンネルを介した安全な通信が提供される。別の実施形態においては、一方向認証が採用され、その結果、ＩＭＤもしくはＥＤのいずれか一方だけが他方に対して認証されれば、データ通信セッションが許可される。たとえば、ＥＤがあるＩＭＤと通信するときは、ＥＤがそのＩＭＤを認証すれば、それが正しい装置からデータを収集していることがわかる。しかしながら、ＩＭＤは、その状態の変更（再プログラム）をＥＤが試みない限りＥＤを認証する必要がない。ＥＤがデータを読み取るだけである限り、安全性に関する問題はない（ただし、プライバシ問題は存在し得る）。

【００２７】

図２は、遠隔測定インターロックを使用し、秘密キー暗号化方法を用いて認証が行われる実施形態における、外部装置２と埋め込み可能な装置１の間の長距離遠隔測定チャンネルを介した通信セッションを示している。外部装置３からのイネーブル・コマンドによって遠隔測定インターロックがリリースされた後、外部装置２が、キーＫ１を使用する秘密キー暗号化方法のアルゴリズムによって暗号化されたメッセージＭ１を送信する。埋め込み可能な装置１は、そのメッセージを解読してＭ１を獲得し、取り決められた方法（たとえば数Ｍ１の１インクリメント）に従ってＭ１を修正してＭ１*を求め、キーＫ１を用いてＭ１*を暗号化し、埋め込み可能な装置に返すことによって応答する。メッセージを解読してＭ１*を獲得した後、外部装置２は、埋め込み可能な装置１が秘密キーＫ１を所有している証拠を示したことからそれを認証する。同時に埋め込み可能な装置１は、秘密キーＫ１を用いて暗号化したメッセージＭ２を送信する。外部装置２は、そのメッセージを解読してＭ２を獲得し、Ｍ２を修正してＭ２*を求め、キーＫ１を用いてＭ２*を暗号化して埋め込み可能な装置１に返すことによって応答し、それにより外部装置２が認証される。その後、埋め込み可能な装置１は、キーＫ１によって暗号化した秘密セッションキーＳＫを送信する。続いてデータ通信セッションが確保され、その際、いずれかの装置によって秘密セッションキーＳＫを用いてデータが暗号化されて送信される。別の実施形態においては、データ通信セッションの間においても認証のために使用された秘密キーＫ１と同じ秘密キーを使用して装置間のデータの交換が行われる。セッションは、装置の一方がセッション終了信号を送信するまで、あるいはタイムアウトが生じるまで続き、その時点において遠隔測定インターロックが再作動される。

【００２８】

図３は、遠隔測定インターロックを使用し、公開キー暗号化方法を用いて認証が行われる実施形態における、外部装置２と埋め込み可能な装置１の間の長距離遠隔測定チャンネルを介した通信セッションを示している。外部装置３からのイネーブル・コマンドによって遠隔測定インターロックがリリースされた後、外部装置２が、埋め込み可能な装置によって所有されていると考えられている対応するプライベートキーを有するキーＰｕｂＫｅｙ１を使用する公開キー暗号化方法のアルゴリズムによって暗号化されたメッセージＭ１を送信する。埋め込み可能な装置は、ＰｕｂＫｅｙ１に対応するプライベートキーを用いてそのメッセージを解読してＭ１を獲得し、外部装置２によって所有されていると考えら

れている対応するプライベートキーを有する公開キーＰｕｂＫｅｙ２によってＭ１を暗号化し、埋め込み可能な装置に返すことによって応答する。外部装置２は、外部装置２のプライベートキーを用いてそのメッセージを解読してＭ１を得ると、埋め込み可能な装置１が公開キーＰｕｂＫｅｙ１に対応するプライベートキーを所有している証拠が示されたことからそれを認証する。同時に埋め込み可能な装置１は、対応するプライベートキーを有する公開キーＰｕｂＫｅｙ２によって暗号化されたメッセージＭ２を送信する。外部装置２は、ＰｕｂＫｅｙ２に対応するプライベートキーを用いてそのメッセージを解読してＭ２を獲得し、公開キーＰｕｂＫｅｙ１を用いて暗号化されたＭ２を埋め込み可能な装置１に返すことによって応答し、それにより外部装置２が認証される。また外部装置２は、公開キーＰｕｂＫｅｙ１を用いて暗号化された秘密セッションキーＳＫを送信する。それより秘密キー暗号化方法を使用するデータ通信セッションが確保され、いずれかの装置によって秘密セッションキーＳＫを用いてデータが暗号化されて送信される。このセッションは、装置の一方がセッション終了信号を送信するまで、あるいはタイムアウトが生じるまで続き、その時点において遠隔測定インターロックが再作動される。

【００２９】

図４は、図３に例示した認証プロトコルのより詳細な実施形態を使用する通信セッションを示している。ここでは、外部装置２と埋め込み可能な装置が互いの公開認証キーを知っていることを前提としている。インスティゲータ（この実施形態においてはインスティゲータが外部装置２である）が埋め込み可能な装置との認証された長距離遠隔測定セッションの確立を希望するとき、その識別番号ＩＤ２と乱数R_Aを、埋め込み可能な装置の公開キーＰｕｂＫｅｙ１を用いて暗号化することから開始する。意図された受信者を除いてその受信者のプライベートキーを知っているリスナがいないことから、（ほかのリスナがその受信者の公開キーを知っていたとしても）意図された受信者を除くリスナは、この情報を解読できない。受信者装置は、そのプライベートキーを用いてこのメッセージを解読する。続いてインスティゲータの公開キーＰｕｂｋｅｙ２をルックアップし、それを使用して自身の識別番号ＩＤ１、乱数R_A、および第２の乱数R_Bを暗号化する。続いて受信者は、この暗号化した情報をインスティゲータに戻す。インスティゲータのほかにそのインスティゲータのプライベートキーが知られていないことから、インスティゲータを除くリスナは、この情報を解読できない。インスティゲータは応答を受信すると、それが送った乱数R_Aを検証し、意図された装置だけがR_Aを解読し、返すことができたはずであるから、このときそれが通信している埋め込み可能な装置が実際に意図された装置であることがわかる。続いてインスティゲータは、受信者の公開キーＰｕｂＫｅｙ１を用いてR_Bを暗号化し、それを受信者に返す。受信者は、R_Bの受信、解読、検証を行い、正しいプライベートキーの所有者だけがR_Bを解読して返すことができるので、このときインスティゲータが実際にそのプライベートキーの所有者であるとわかる。ここで認証が完了する。この時点においては、通信セッションの両者に、その通信相手が正しいプライベートキーの所有者であることがわかっている。この実施形態においては、認証における両方の関係者によって乱数が使用されており、かつそれらがその都度異なることから、認証済み装置になりすます試みにおいて認証の交換の記録と交換の部分の再送が役立たないことに注意する必要がある。

【００３０】

繰り返すが、公開キー暗号化方法のアルゴリズムは演算コストが高いことから、図４の実施形態においては各セッションの開始時の認証のためにだけ使用されており、暗号化されるメッセージは最小サイズである（通常、数百ビット）。インスティゲータは、公開キーＰｕｂＫｅｙ１を用いて暗号化した秘密セッションキーＳＫを送信し、その結果、秘密キー暗号化方法を使用するデータ通信セッションを行うことができる。この実施形態においては、秘密セッションキーＳＫが、認証の間にR_Bを返すフレームと同じフレーム内において受信者装置に送信される。このようにすれば公開キーの暗号化を使用するフレームの数が１つ減らされる（公開キーの暗号化は演算コストが非常に高い）。特定の実施形態においては、秘密セッションキーＳＫが６４ビットである。６４ビットのキーは、１２８

ビットの公開キーより解読が容易であるが、比較的短い通常の遠隔測定セッションの持続時間にとっては安全性の提供に充分である。データ通信セッションは、装置の一方がセッション終了信号を送信するまで、あるいはタイムアウトが生じるまで続き、その時点において遠隔測定インターロックが再作動される。別の特定の実施形態においては、それぞれの遠隔測定セッションの終了時にセッションキーが満了となり、次のセッション用の新しいキーがランダムに選択される。

【００３１】

データ通信用に秘密キー暗号化方法を使用している場合であっても、埋め込み可能な医療装置にとって、それが送信し、あるいは受信している各メッセージの暗号化または解読が容易でないことがある。現在の心臓リズム管理装置にとって、有意な待ち時間を送信に追加することなくリアルタイムでエレクトログラムを暗号化することは容易でない。したがって一実施形態においては、埋め込み可能な医療装置は、選択的なデータだけを暗号化し、残りのデータは平文で送信する。たとえば、もっとも慎重を要する患者データ（患者の名前、社会保険番号、診断等）を暗号化する。各データ・パケットのヘッダ内の暗号化フラグが、その内容が暗号化されているか否かを表すことができる。

【００３２】

公開キーまたは秘密キーいずれかの認証を用いれば、装置を認証する特定のキーを所有している証拠となる。概して言えば、すべての認証プロトコルは、公開キー暗号化方法の場合であればプライベートキーと同程度、秘密キー暗号化方法の場合であれば秘密キーと同程度に安全であるに過ぎない。この理由から、プライベートキーまたは秘密キーは長くするべきである（たとえば、一実施形態においては１２８ビット）。追加の安全性のためには、プライベートキーまたは秘密キーを、工場において装置内にハード的に接続するか、あるいはその装置によって内部的に生成されるようにして、その後の遠隔測定による読み出しを防止することができる。たとえば、製造間にプライベートキーを装置内にプログラムし、その後その対応公開キーを製品の書類に含めるか、短距離誘導遠隔測定を介して獲得可能とする。医師は、その装置の公開キーをホーム・モニタ、ポータブル中継器、またはプログラマにプログラムすることができる。すべての外部装置は、一意的な公開とプライベート認証キーを有するとともに、製品の書類に公開キーを含める。したがって医師は、多数の外部装置の公開キーを埋め込み可能な装置にプログラムすることができる。別の実施形態においては、埋め込み可能な装置と外部装置の両方が、ＲＳＡアルゴリズムにより、あるいはそのほかの標準的なキーペア生成アルゴリズムを通じて新しい公開キー／プライベートキーのペアをランダムに生成することができる。この実施形態の場合には、安全な短距離誘導遠隔測定を介して医師がコマンドを送ったときに、新しいキーの生成が可能になる。

【００３３】

好ましい実施形態においては、短距離遠隔測定を介した緊急時には常に通信が可能になるように上記の認証スキームが長距離遠隔測定にのみ適用される。たとえば、装置のリセットもしくはそのほかの認証キーが改ざんされる障害の場合に、長距離の認証済み遠隔測定が可能でなくなる。そのような場合においても、認証キーをリセットに短距離遠隔測定が利用可能である必要がある。認証なしに短距離遠隔測定が利用可能となる必要がある別の例として、掛かり付けの医師から離れて旅行中の患者が装置の問い合わせを必要とする場合が挙げられる。

【００３４】

以上、特定の実施形態に関連して本発明を説明してきたが、多くの代用、変形、および修正が当業者には明らかであろう。その種の代用、変形、および修正は、付随する特許請求の範囲に含まれることが意図されている。

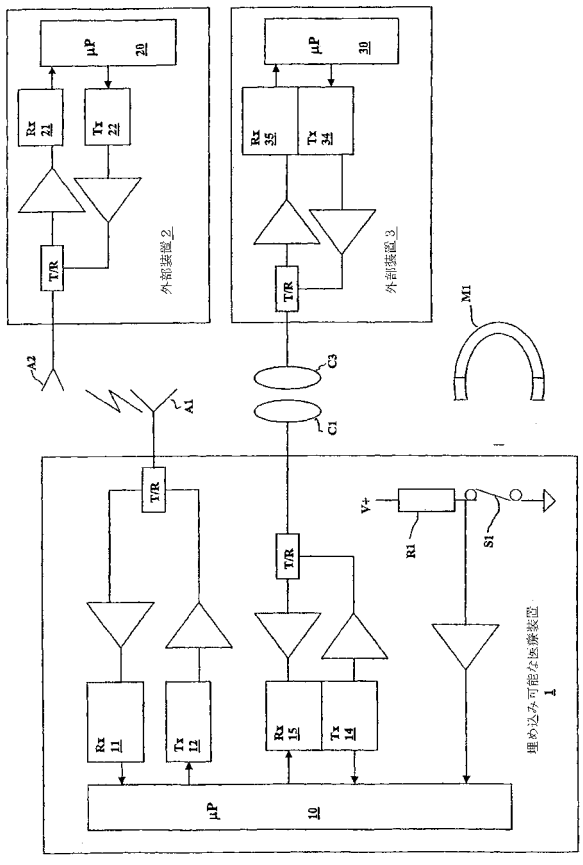
【図面の簡単な説明】

【００３５】

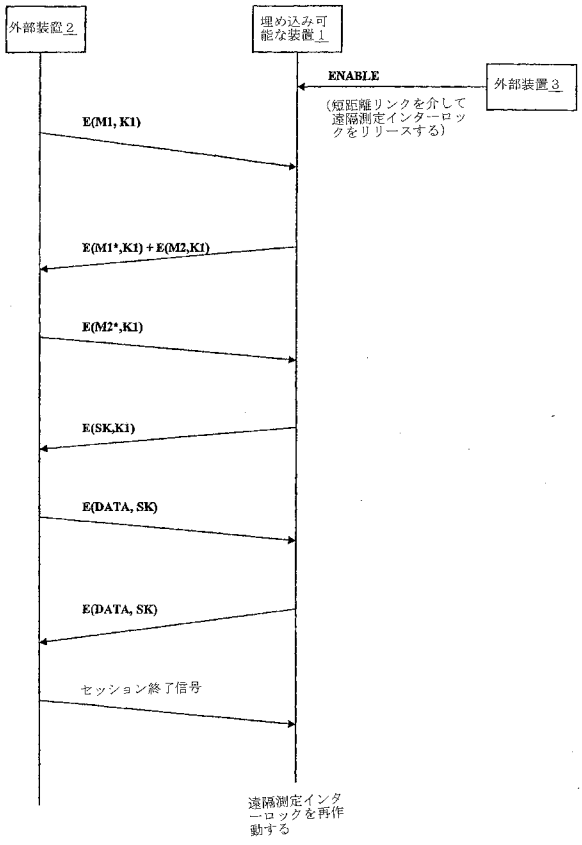
【図１】埋め込み可能な医療装置のための遠隔測定システムの一例を示したブロック図である。

【図２】秘密キー認証プロトコルを例示した説明図である。
【図３】公開キー認証プロトコルを例示した説明図である。
【図４】特定の公開キー認証プロトコルを例示した説明図である。
【符号の説明】
【００３６】
１　埋め込み可能な医療装置；埋め込み可能な装置、２　外部装置、３　外部装置、１０　マイクロプロセッサ；コントローラ、１１　データ受信機、１２　データ送信機、１４　送信機、１５　受信機、２０　マイクロプロセッサ；コントローラ、２１　データ受信機、２２　データ送信機、３０　マイクロプロセッサ；コントローラ、３４　送信機、３５　受信機

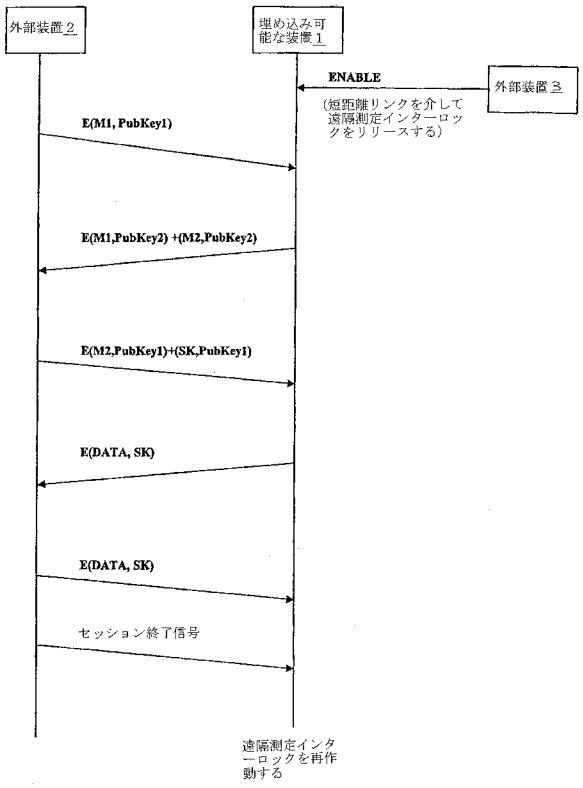
【図１】



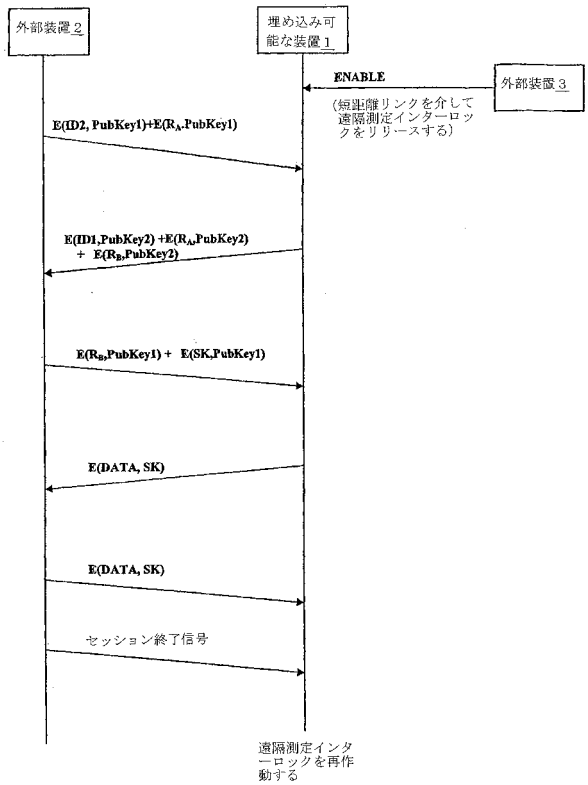
【図２】



【図３】


外部装置２
埋め込み可能な装置１
外部装置３
ENABLE
（短距離リンクを介して遠隔測定インターロックをリリースする）
E(M1, PubKey1)
E(M1,PubKey2) +(M2,PubKey2)
E(M2,PubKey1)+(SK,PubKey1)
E(DATA, SK)
E(DATA, SK)
セッション終了信号
遠隔測定インターロックを再作動する

【図４】


外部装置２
埋め込み可能な装置１
外部装置３
ENABLE
（短距離リンクを介して遠隔測定インターロックをリリースする）
E(ID2, PubKey1)+E(RA,PubKey1)
E(ID1,PubKey2) +E(RA,PubKey2) + E(RB,PubKey2)
E(RB,PubKey1) + E(SK,PubKey1)
E(DATA, SK)
E(DATA, SK)
セッション終了信号
遠隔測定インターロックを再作動する

フロントページの続き

(72)発明者　ボン　アークス，ジェフリー・エイ
アメリカ合衆国・５５４０５・ミネソタ州・ミネアポリス・エマーソン　アベニュ　サウス・２１１５
(72)発明者　コシオル，アラン・ティ
アメリカ合衆国・５５０１４・ミネソタ州・リノ　レイクス・ラフド　グロース　ロード・６６３０
(72)発明者　バンゲ，ジョセフ・イー
アメリカ合衆国・５５１２３・ミネソタ州・イーガン・オーバールック　プレイス・８３２

審査官　大和田　秀明

(56)参考文献　米国特許出願公開第２００３／０１１４８９８（ＵＳ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
A61N　1/37
A61B　5/00

专利名称(译)	用于植入式医疗设备的安全遥测		
公开(公告)号	JP4680187B2	公开(公告)日	2011-05-11
申请号	JP2006517513	申请日	2004-06-22
[标]申请(专利权)人(译)	心脏起搏器股份公司		
申请(专利权)人(译)	心脏起搏器的公司		
当前申请(专利权)人(译)	心脏起搏器的公司		
[标]发明人	ボンアークスジェフリーエイ コシオルアランティ バンゲジョセフイー		
发明人	ボン アークス,ジェフリー·エイ コシオル,アラン·ティ バンゲ,ジョセフ·イー		
IPC分类号	A61N1/37 A61B5/00 A61N1/372 H04L9/32		
CPC分类号	A61B5/0031 A61N1/37223 A61N1/37254 G06F19/3418 G16H40/63 G16H40/67 H04L9/0844 H04L9/3271 H04L2209/88 Y10S128/903		
FI分类号	A61N1/37 A61B5/00.102.D A61B5/00.102.C		
代理人(译)	夏木森下		
审查员(译)	大和田英明		
优先权	10/601763 2003-06-23 US		
其他公开文献	JP2007524456A		
外部链接	Espacenet		

摘要(译)

用于通过遥测信道实现可植入医疗设备（IMD）和外部设备（ED）之间的安全通信的方法和系统。实现遥测互锁以限制ED和IMD之间通过遥测信道进行的任何通信，并通过IMD通过短距离通信信道启用EMD命令，需要物理接近IMD遥测联锁可在发送时释放。作为该遥测互锁的替代或补充，只有在IMD和ED已经相互加密认证之后，才允许IMD和ED之间通过遥测信道的数据通信会话。它可以是。 [选图]图1

【図１】