

(19) 日本国特許庁(JP)

(12) 公表特許公報(A)

(11) 特許出願公表番号

特表2017-500624
(P2017-500624A)

(43) 公表日 平成29年1月5日(2017.1.5)

(51) Int.Cl.	F I	テーマコード (参考)
G06F 21/62 (2013.01)	G06F 21/62 345	5J104
H04L 9/10 (2006.01)	H04L 9/00 621A	
G06F 21/72 (2013.01)	G06F 21/72 ZEC	
G06F 21/44 (2013.01)	G06F 21/44	

審査請求 未請求 予備審査請求 未請求 (全 48 頁)

(21) 出願番号 特願2016-523290 (P2016-523290)
 (86) (22) 出願日 平成26年10月15日 (2014.10.15)
 (85) 翻訳文提出日 平成28年6月7日 (2016.6.7)
 (86) 国際出願番号 PCT/EP2014/072156
 (87) 国際公開番号 W02015/055738
 (87) 国際公開日 平成27年4月23日 (2015.4.23)
 (31) 優先権主張番号 13188787.9
 (32) 優先日 平成25年10月15日 (2013.10.15)
 (33) 優先権主張国 欧州特許庁 (EP)

(71) 出願人 516109200
 ワン ドロップ ダイアグノスティクス
 エスエーアールエル
 スイス, シーエイチ-2000 ヌーシ
 ャテル, ルー ド ラ マラディエール
 71シー
 (74) 代理人 100107456
 弁理士 池田 成人
 (74) 代理人 100162352
 弁理士 酒巻 順一郎
 (74) 代理人 100123995
 弁理士 野田 雅一
 (74) 代理人 100148596
 弁理士 山口 和弘

最終頁に続く

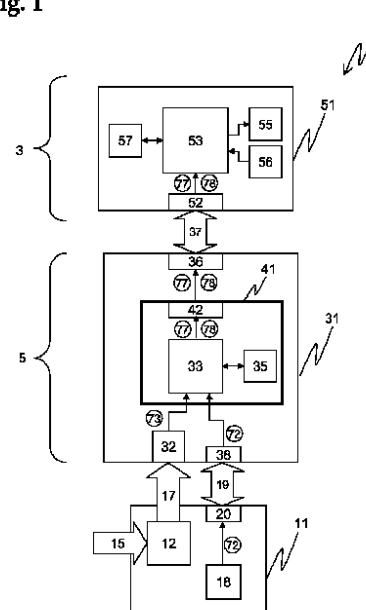
(54) 【発明の名称】 診断検査アッセイの分析結果へのアクセスを保護及び制御するシステム及び方法

(57) 【要約】

リーダユニット(31)は、1つ又は複数の診断検査(13)を1つ又は複数の生理学的試料(15)に対して実行できるアッセイユニット(11)と動作可能に接続されるように構成され、また、リーダユニットと動作可能に接続されたアッセイユニットで実行される診断検査の検査生データ(73)を取得するように構成される(32、36)。リーダユニットは、検査生データ又は当該検査生データ由来のデータを含む入力データをロック鍵データ(75)で暗号化するように構成された暗号化モジュール(33)を備える。リーダユニットは、入力データではなく暗号化されたデータ(77)へのアクセスを提供するように構成される。

【選択図】 図1

Fig. 1



【特許請求の範囲】**【請求項 1】**

リーダユニット(31)であって、1つ又は複数の診断検査(13)を1つ又は複数の生理学的試料(15)に対して実行できるアッセイユニット(11)と動作可能に接続されるように構成され、さらに、該リーダユニット(31)と動作可能に接続されたアッセイユニットで実行される診断検査の検査生データ(73)を取得するように構成された(32、36)リーダユニット(31)において、

データ保護モジュール(41)であって、該データ保護モジュール(41)は、前記検査生データを取得し一時的に格納し、前記検査生データを分析結果データ(74)に変換し、前記分析結果データをロック鍵データ(75)によって暗号化されたデータ(77)へと暗号化し(33)、前記暗号化されたデータを出力インタフェース(42)に提供するように構成されており、前記保護モジュールは、前記モジュール内に格納されたデータ(73、74)へのアクセスを防止するように構成された改竄防止モジュールである、データ保護モジュール(41)を備えることを特徴とする、リーダユニット(31)。

10

【請求項 2】

前記保護モジュール(41)は、前記ロック鍵データ(75)を第2レベル鍵データ(82)により暗号化されたロック鍵データ(84)へと暗号化し、前記暗号化されたロック鍵データを前記出力インタフェース(42)に提供するように構成されていることを特徴とする、請求項1に記載のリーダユニット。

20

【請求項 3】

診断デバイスであって、請求項1又は2に記載のリーダユニット(31)、1つ又は複数の診断検査(13)を1つ又は複数の生理学的試料(15)に対して実行できるアッセイユニット(11)、及び/又は評価ユニット(51)を備え、

前記アッセイユニットと前記リーダユニットとは永久的に又は取り外し可能に、動作可能に互いに接続され、

前記リーダユニットは、前記アッセイユニットで実行される診断検査の検査生データ(73)を取得するように構成され、

前記評価ユニットと前記リーダユニットは永久的に又は取り外し可能に、動作可能に互いに接続され(37、28、52)、

前記評価ユニットは、データ(77、78、84)を前記リーダユニットから受信し、前記データの少なくとも一部を認証鍵データ(79)を使用して復号化し、分析結果データ(74)を取得するために前記復号化された出力データを使用するように構成されている、診断デバイス。

30

【請求項 4】

請求項1又は2に記載の1つ又は複数のリーダユニット(31、31')と、

1つ又は複数の診断検査(13)を1つ又は複数の生理学的試料(15)に対して実行できる1つ又は複数のアッセイユニット(11、11')であって、該アッセイユニットは前記リーダユニットに動作可能に接続されるように構成されており、前記リーダユニットは前記アッセイユニットで実行された診断検査の検査生データ(73)を取得するように構成されている、1つ又は複数のアッセイユニット(11、11')と、

40

1つ又は複数の評価ユニット(51)であって、該評価ユニットは、前記リーダユニットに動作可能に接続され、前記リーダユニットからデータ(77、78、84)を受信し、前記データの少なくとも一部を認証鍵データ(79)を使用して復号化し、分析結果データ(74)を取得するために前記復号化された出力データを使用するように構成されている、1つ又は複数の評価ユニット(51)と、

を備える、診断システム。

【請求項 5】

評価ユニット(51)は、暗号化されたデータ(77、84)を復号化するように構成されているデータ処理モジュール(53)を備えることを特徴とする、請求項4に記載の診断システム。

50

【請求項 6】

評価ユニット (5 1) に動作可能に接続された 1 つ若しくは複数の認証ユニット (1 0 0) 及び / 又は

通信ネットワーク (1 0 4) を介して前記評価ユニットに接続された 1 つ若しくは複数の遠隔認証サーバ (1 1 0) によって特徴づけられており、

前記認証ユニット及び / 又は遠隔認証サーバは、特定の条件が満たされると、前記認証鍵データ (7 9) を前記評価ユニットに提供するように構成されているか、或いは

前記認証ユニット及び / 又は遠隔認証サーバは、暗号化されたデータ (7 7 、 8 4) を前記評価ユニットから受信し、特定の条件が満たされると前記暗号化されたデータの一部又はすべてを復号化し、前記復号化されたデータ (8 0 、 8 0 ') を前記評価ユニットに提供するように構成されている、請求項 4 又は 5 に記載の診断システム。

10

【請求項 7】

1 つ又は複数の診断検査 (1 3) を 1 つ又は複数の生理学的試料 (1 5) に対して実行することができる検査モジュール (1 2) を有する 1 つ又は複数のアッセイユニット (1 1 、 1 1 ') と、

請求項 1 ~ 4 のいずれか一項に記載のリーダユニット (3 1) と、
を備える、診断キット。

【請求項 8】

ユーザ (3) のアッセイユニット (1 1) の分析結果 (7 3 、 7 4) へのアクセスを制御する方法であって、

20

a) 並行して複数の診断検査 (1 3) を 1 つ又は複数の生理学的試料 (1 5) に対して実施するように構成されたアッセイユニット (1 1) を用意するステップと、

b) 前記アッセイユニットから前記複数の診断検査の分析結果の完全なデータセット (7 3 、 7 4) を読み出すステップと、

c) 分析結果の前記完全なデータセットをロック鍵データ (7 5) によって暗号化するステップと、

d) 分析結果の前記暗号化された完全なデータセット (7 7) を前記ユーザに提供するステップと、

e) 前記ユーザに認証手段を提供するステップであって、該認証手段は、前記ユーザが、分析結果の前記暗号化された完全なデータセット内に存在するような分析結果の前記完全なデータセットの特定の認証されたサブセット (7 3 a 、 7 4 a) へのアクセス権を得ることを可能にするが、分析結果の前記完全なデータセットの他の部分へのアクセス権を得ることを可能にしない、ステップと、
を含む、方法。

30

【請求項 9】

前記認証手段は、認証鍵データ (7 9) であり、該認証鍵データ (7 9) は、分析結果の前記暗号化された完全なデータセット (7 7) の特定の部分を復号化することにより、前記復号化されたデータ (8 0) が分析結果の前記完全なデータセット (7 3 、 7 4) の前記特定の認証されたサブセット (7 3 a 、 7 4 a) に対応することを可能にすることを特徴とする、請求項 8 に記載の方法。

40

【請求項 10】

前記認証手段は、前記ユーザが認証ユニット (1 0 0) 又は遠隔認証サーバ (1 1 0) から認証鍵データ (7 9) を受信することを可能にする認証データであり、前記認証鍵データは、分析結果の前記暗号化された完全なデータセット (7 7) の特定の部分を復号化することにより、前記復号化されたデータ (8 0) が分析結果の前記完全なデータセット (7 3 、 7 4) の前記特定の認証されたサブセット (7 3 a 、 7 4 a) に対応することを可能にすることを特徴とする、請求項 8 に記載の方法。

【請求項 11】

ステップ c) において、分析結果の前記完全なデータセット (7 3 、 7 4) の異なるサブセット (7 3 . 1 、 7 3 . 2 、 . . . 、 7 4 . 1 、 7 4 . 2 、 . . .) は、異なるロッ

50

ク鍵 (75.1、75.2、...) によって、暗号化されたデータの異なるサブセット (77.1、77.2) へと暗号化され、

前記異なるロック鍵 (75.1、75.2、...) は共に前記ロック鍵データ (75) を成し、前記暗号化されたデータの異なるサブセット (77.1、77.2) は共に分析結果の前記暗号化された完全なデータセット (77) を成す、
ことを特徴とする、請求項 8 ~ 10 のいずれか一項に記載の方法。

【請求項 12】

ステップ c) での暗号化は非対称暗号化アルゴリズムにより行なわれ、前記ロック鍵は前記非対称暗号化アルゴリズム用の公開鍵 (75.1、75.2、...) であることを特徴とする、請求項 11 に記載の方法。

10

【請求項 13】

前記認証手段は、前記非対称暗号化アルゴリズムのプライベート鍵であり、前記非対称暗号化アルゴリズムのプライベート鍵は共に前記認証鍵データを成すものであり、

前記プライベート鍵は、分析結果の前記暗号化された完全なデータセットのサブセットを復号化することを可能にするものであり、前記暗号化された完全なデータセットの前記復号化されたデータサブセット (80.1、80.2、...) は分析結果の前記完全なデータセット (73、74) の前記特定の認証されたサブセット (73a、74a) に対応する、

ことを特徴とする、請求項 12 に記載の方法。

【請求項 14】

20

ステップ c) での暗号化は対称暗号化アルゴリズムにより行なわれ、前記ロック鍵は前記対称暗号化アルゴリズム用の秘密鍵 (75.1、75.2、...) であることを特徴とする、請求項 11 に記載の方法。

【請求項 15】

前記認証手段は、前記ロック鍵データ (75) の特定の鍵 (79.1、79.2、...) であり、該特定の鍵 (79.1、79.2、...) は共に前記認証鍵データ (79) を成すものであり、

前記特定の鍵 (79.1、79.2、...) は、分析結果の前記暗号化された完全なデータセット (77) のサブセット (77.1、77.2、...) を復号化することを可能にするものであり、前記暗号化された完全なデータセットの前記復号化されたデータサブセット (80.1、80.2、...) は分析結果の前記完全なデータセット (73、74) の前記特定の認証されたサブセット (73a、74a) に対応する、

30

ことを特徴とする、請求項 14 に記載の方法。

【請求項 16】

ステップ c) 後、前記ロック鍵データ (75) は、非対称暗号化アルゴリズム用の 1 つ又は複数の公開鍵 (82.1、82.2、...) を使用して、前記非対称暗号化アルゴリズムによって暗号化されたロック鍵データ (84) へと暗号化され、

前記 1 つ又は複数の公開鍵 (82.1、82.2、...) は共に第 2 レベル鍵データ (82) を成す、

ことを特徴とする、請求項 14 に記載の方法。

40

【請求項 17】

分析結果の前記暗号化された完全なデータセット (77) は認証ユニット (100) 又は遠隔認証サーバ (110) へと提供され、

前記認証手段は認証データであり、該認証データは、前記ユーザが前記認証ユニット又は前記遠隔認証サーバに対して、

前記暗号化されたデータの特定の部分を復号化することにより、前記復号化されたデータ (80) が分析結果の前記完全なデータセット (73、74) の前記特定の認証されたサブセット (73a、74a) に対応するようにすること、

前記復号化されたデータを前記ユーザに提供すること、

を実行させるように命令することを可能にすることを特徴とする、請求項 8 に記載の方法

50

。

【請求項 18】

ステップ I I) / ステップ c) における暗号化の前に、前記データセットの前記異なるサブセットは、前記ユーザに提供されるプライバシー鍵データ (8 6) により暗号化されることを特徴とする、請求項 17 に記載の方法。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、診断システム用の分析ユニット (assay unit : アッセイユニット)、読み取りユニット (reader unit : リーダユニット)、診断デバイス、及び診断キットから分析結果データを取得し処理する診断システム、並びに分析結果へのアクセスを制御する方法に関する。

10

【背景技術】

【0002】

今日、例えば、体液等の生理学的試料は多種多様な生化学的分析物に関して分析することができる。正確な医学診断は、健康状態及び疾患の特定、モニタリング、予後、及びコンパニオン診断等の医療処置の重要な部分である。医学診断システムが使用される2つの主な状況、すなわち、専用の医療検査室及びいわゆるポイントオブケア (P o C) 検査がある。

【0003】

20

本明細書の文脈における用語「生理学的試料」は、血液、尿、便、若しくは組織等の患者から得られた生物学的物質、又はかかる生物学的物質を基に後に分析するために準備された試料のいずれかである、あらゆる液体物質、固体物質、又は気体状物質を包含するものとする。

【0004】

一般に、医療検査室で使用される検査室用診断デバイスにより多種多様な分析能力が提供される。例えば、I l l u m i n a 及び A f f y m e t r i x から販売されるデバイスは、デオキシリボ核酸 (D N A) 及びリボ核酸 (R N A) の分子診断を行う。R o c h e 及び A b b o t t により販売されているような臨床用分析器は、免疫化学 (抗体ベースの検出) 及び臨床化学 (小化学分子の検出) 用の検査を行う。例えば B e c k m a n C o u l t e r から販売されるようなデバイスは体液中の細胞を計数することができる。

30

【0005】

このような診断デバイスは、高感度で正確、且つ柔軟であり、高い処理量を提供する。しかし、診断デバイスは、高価であり、また操作によく訓練された人員を必要とするという不利点も有する。このため、このような診断デバイスは主に病院検査室及び中央医療検査室で使用され、病院検査室及び中央医療検査室では診断デバイスが最も効率的に使用され得る。しかし、かかるデバイスは患者の生理学的試料を必要とするため、当該試料は分析が行なわれる医療検査室へ移送されなければならない。その結果、分析結果は数時間後又は数日後にしか入手できない。

【0006】

40

ますます多くの数の診断検査がポイントオブケアで、患者の近くで例えば、医療現場、病院の救急処置室、救急車、又はさらには患者の身辺で行なわれる。ポイントオブケア診断デバイスは多くの場合携帯型で、分析結果を迅速に (数分以内) 得ることができる。ポイントオブケア診断デバイスの使用は通常、診断検査が普通の医療関係者又は患者自身により実施することができるようにはるかに簡単である。

【0007】

最も一般に普及したポイントオブケア診断デバイスは、ラテラルフローイムノアッセイストリップ検査を実行する。このような検査は、妊娠、H I V、マラリア、インフルエンザ検査等の多種多様な診断指標に利用できる。対応するデバイスは多数の製造業者、例えば、S w i s s P r e c i s i o n D i a g n o s t i c s、A l e r e、B a y e

50

r、及びSiemensから提供される。ラテラルフロー検査は通常、1つ又は2つの分析物の検出及び定性的検出、例えば、明瞭な色調の変化に限定される。

【0008】

アリーアトリアージメータプロ(Aleré Triage Meter Pro)システムは、消耗カートリッジ形態のアッセイユニット及び再利用可能卓上リーダの形態の評価デバイスから構成された免疫化学システムである。カートリッジは、3タンパク質心臓パネル(ミオグロビン、CK-MB、及びトロポニンI)等のバイオマーカのパネル及び薬物スクリーニングパネルを検出するために利用可能である。したがって、このようなカートリッジによって3つの分析物について試料を同時に検査できる。バイオマーカの新しいパネル毎に新しい検査カートリッジが必要とされる。Aleréのエポック(epoc)システム及びAbottのアイ-スタット(i-STAT)システムは、血液ガス、電解質、及び代謝産物のパネルを測定できるカートリッジを有する。Abottのアイ-スタットシステムについては、1つの心臓バイオマーカ(トロポニンI、CK-MB、又はBNP)を測定するカートリッジが利用可能である。これらのデバイスは高感度で正確である。主な制限は、検査室用診断マシンに比べると、検査する分析物毎の価格が高いことである。別の不利点は、利用可能な検査カートリッジの種類が限られていることである。

10

【0009】

新規のバイオセンサシステムによって、ポイントオブケア診断用途において多数の分析物のマルチプレックス検出が可能になる。このようなデバイスは高度で統合的な分析能力を持つため、検査室用診断デバイスの能力に匹敵する。

20

【0010】

GyrosのラボオンCD(Lab-on-a-CD)システム及びAdvanced Liquid Logicのデジタルマイクロ流体システムは、卓上分析器を用いて1度に100以上の分析物を検出できる。さまざまな生化学的分析物を検出するためのその他のバイオセンシング手法は、例えば、米国特許第5719324号、国際公開第2002/048701号、米国特許第4020830号、国際公開第89/009938号、米国特許第4945045号、及び米国特許第5641640号で提供される。

【0011】

医学診断デバイスは通常、再利用可能測定デバイス及び消耗部品(検査ユニット又は試薬)からなる。特定の診断検査を実施したいユーザは、所望の分析能力を有する診断デバイスを選択する。例えば、自分の血液中の血糖値を知りたい真性糖尿病患者は、再利用可能血糖測定器及び消耗血糖検査片を備える専用の診断システムを使用することができる。

30

【0012】

評価デバイスが異なる診断検査を実行できる場合、ユーザは対応する消耗アッセイユニットを選択しなければならない。例えば、心筋梗塞について検査したいユーザは、アリーアトリアージ(Aleré Triage)メータ(評価デバイス)及びカードイオ3パネル(Cardio 3 Panel)カートリッジ(アッセイユニット)を使用して、3つの心臓バイオマーカについて検査することができる。さらなる心臓バイオマーカ等の他の分析物について検査したいユーザは、必要とする診断検査を行うことが可能な他の検査カートリッジを選択しなければならない。

40

【0013】

消耗アッセイユニットの費用は主として、実際の製造費用だけで決まるものではなく、一方では製造業者が回収すべき研究開発費用と、他方では、国及び/又は保険会社等の間で通常異なる、特定の分析物についての特定の診断検査で適用可能な健康保険還付金とによって決まるものである。したがって、特定のアッセイユニットの購入価格は、消耗アッセイユニットによって測定できる分析物の数及び種類等の分析能力に依存する。

【0014】

このようなアッセイユニットの購入価格を介して費用を回収するアプローチは、1つの分析物又はいくつかの分析物を測定可能な消耗アッセイユニットには有効である。

50

【0015】

分析物の組み合わせは、心臓バイオマーカー又は薬物乱用スクリーニングのための組み合わせ検査のような日常的に一緒に必要とされる検査でのみ利用可能である。したがって、通常はほんのいくつかの異なる診断組み合わせ検査が利用可能である。

【0016】

購入価格でのアプローチでは、再利用可能な評価デバイス及び消耗アッセイユニットを備えたポイントオブケア診断に使用される場合、上述のような広範でマルチプレックスな能力を提供する診断システムには最適な解決策を提供しない。例えば、同時に100分析物を検査できる診断システムの利用は桁違いの費用がかかる。その理由は、購入価格は当該100分析物の検査の研究開発費用及び還付金に依存するからであるが、消耗アッセイユニットの製造費用は、はるかに診断能力が低いアッセイユニットと同等である。

10

【0017】

医学診断システムはますますデータ通信ネットワークに統合され、病院、医療現場、中央検査室、患者の家、さらには救急車又は救助ヘリ等の移動ユニット間のデータ交換を可能にする。電子健康管理システムと通信することができる医学診断システムは、検査結果の注文、請求、較正、及び電子カルテとの同期といった種々のメリットをさらに提供する。しかしながら、このような用途すべてにおいて、慎重に扱うべき個人的医療データの守秘義務が問題となる。

【0018】

米国特許出願公開第2002/0161606号、米国特許出願公開第2005/0055240号、及び米国特許第6018713号は、中央臨床検査室から診断検査を注文するシステムについて記述する。当該システムは、クライアント端末及び中央検査室の遠隔サーバに基づく。ユーザは患者情報を入力し、中央検査室で実施する診断検査を選択して注文する。診断検査の結果報告はクライアント端末に送信できる。行なわれる検査は自動で健康保険会社に請求できる。ある種のロジスティクス面での利点を有するものの、開示されるシステムは依然として、診断検査を実施するために中央検査室のよくある問題、すなわち、試料を検査室に輸送しなければならないという必要性を有する。

20

【0019】

欧州特許第1776919号は、契約ベースのバイオセンサモニタリングシステムについて開示している。システムにより、契約が有効なときにだけ再利用可能な測定デバイス及び消耗検査片を使用したバイオセンサ測定を行うことを可能にする。測定デバイスは、遠隔サーバに測定デバイスの識別子コード及びROM回路識別子コードを伝達し、そのことによって契約が有効であることを確認し、測定デバイスに診断検査を行わせることが可能である。

30

【0020】

国際公開第99/022236号は、セルラネットワークベースの血糖検査片の較正方法を提案している。携帯電話に接続された測定デバイスは、検査片で実施した診断検査の結果を評価し、検査片の結果及び識別コードを遠隔サーバに伝達する。遠隔サーバは、検査片に対応付けられた較正データを携帯電話に送信し、次いで携帯電話が最終的な検査結果を算出する。開示されるシステムは検査結果の機密を保護しない。

40

【0021】

米国特許出願公開第2004/0181528号は、ポイントオブケアデバイスの在庫管理システムを示す。電子システムは、複数のポイントオブケア診断デバイスをその有効期限、消費時間、室温保管時間について追跡し、在庫を補充するために追加のデバイスの注文を管理する。開示されるシステムは、在庫管理及び診断デバイスが既に使用可能でなくなったときの在庫補充に限定される。

【0022】

国際公開第02/100261号は、ポイントオブケア生体外血液分析のためのシステムについて記載している。システムは、バイオセンシング検査を行うことができる改造スマートカードをベースにする。スマートカードはスマートカードリーダーに挿入され、スマ

50

ートカードリーダーは、アナログ出力信号を測定し、アナログ信号をデジタル信号に変換し、当該デジタル生データを汎用コンピュータデバイスに送信して、分析結果を生成する。開示されるシステムは、改造スマートカードをベースにしたバイオセンサに限定され、汎用コンピュータを用いて分析結果を生成できるにすぎない。

【0023】

分析結果を含む慎重に扱うべき個人健康管理データへの無許可の又は不正なアクセスは、主要な安全面及び機密面での懸念材料である。

【0024】

米国特許出願公開第2012/0029303号は、無線、有線、又はネットワークを介して通信できる遠隔患者デバイス及び診断デバイスを備える仮想健康診断システムについて開示している。診断デバイス、例えば、カメラは診断結果、例えば、画像を生成し、当該結果データを遠隔患者デバイスに送信し、遠隔患者デバイスはデータを暗号化し暗号化されたデータを患者記録サーバへと送信する。診断デバイスを使用する医療関係者は診断データへのアクセス権を有する。システムの目的は、リアルタイム遠隔仮想健康診断を提供することである。

10

【0025】

米国特許第7039810号では、1つ又は複数の埋込み型医療デバイスが、埋込み型医療デバイスをプログラムすることを可能にするローカルコンピュータ(「プログラマ」と無線通信する。プログラマは遠隔エキスパートデータセンタへの暗号化されたデータ通信を提供する。

20

【0026】

米国特許出願公開第2005/065890号は、例えば、航空機のメディアプレーヤのために、又はセットトップボックスを介して等、映画等のメディアコンテンツを確実に配信する方法について開示している。一実施形態では、メディアコンテンツデータ(例えば、映画)はコンテンツ鍵により暗号化される。このコンテンツ鍵は、各認証メディアプレーヤの特定のメディアプレーヤの公開鍵により再び暗号化される。あらゆるメディアプレーヤのために何度も暗号化されたコンテンツ鍵は、暗号化されたコンテンツデータと共に配信される。各認証メディアプレーヤは、それ自身の特有の公開鍵により予め暗号化されたコンテンツ鍵は復号化できるが、他の暗号化されたコンテンツ鍵は復号化できない。このことによって、各レシーバのために個々の安全なデータ媒体を製造することを必要とせず、また遠隔認証サーバとの交信も必要とせずに、同一の保護されたメディアコンテンツデータセットを多数の認証レシーバに確実に配信することができる。別の変形例では、メディアコンテンツデータはいくつかのデータ区分に分割される。各区分では2つ以上のコピーが用意され、各区分のコピーは独自のフィンガープリントを有する。これらの区分はすべて、異なるコンテンツ鍵で暗号化される。各認証メディアプレーヤに対して、完全なメディアコンテンツを表す独自の区分の組み合わせが提供され、対応する個々のコンテンツ鍵セットは認証メディアプレーヤの公開鍵で暗号化される。暗号化メディアコンテンツは、認証メディアプレーヤすべての暗号化コンテンツ鍵セットすべてと一緒に配信される。いったん復号化されると、完全なメディアコンテンツデータセットは、独自のフィンガープリントを有する。その結果、コンテンツの違法コピーは特定のメディアプレーヤまで遡ることができる。開示された変形例すべてにおいて、同一の保護されたコンテンツが配信され、多数の所定の認証受信者にアクセス可能になる。アクセス可能とされたコンテンツも受信者リストも当該プロセスでは変更できない。

30

40

【0027】

国際公開第02/01271号は、電子文書の異なるセクションを選択的に暗号化及び復号化する方法について開示しており、当該方法により、認証ユーザグループに文書の異なるセクションへの選択的アクセスレベルを提供することを可能にする。あるアクセスレベルを有するグループのユーザはこのレベルのプライベート鍵を知り、文書のこの特定のアクセスレベルに対応する公開鍵で予め暗号化されたセクションにアクセスできる。異なるアクセスレベルのセクションは複雑であってもよい。したがって、第1のアクセスレベ

50

ルのセクションのうち、第2のアクセスレベルの特定のサブセクションは第2の公開鍵で暗号化され、次いで、暗号化されたサブセクションを含む完全なセクションが第1の公開鍵で暗号化される。暗号化コンテンツの異なるセクションと特定のアクセスレベルに対応するユーザグループの割当ては不変である。

【0028】

ポイントオブケア用途でのマルチプレックス診断検査の費用効率の高い使用を可能にする診断システムへの一般的な必要性があるため、このようなマルチプレックス診断検査の利点は完全に活かされ得る。

【発明の目的】

【0029】

本発明の全体的な目的は、上述及びその他の問題の1つ又は複数を克服する、有利な診断システム及び診断デバイス並びに診断検査の結果を保護し、当該データへのアクセスを制御する方法を提供することである。

【0030】

本発明のさらなる目的は、本発明のこのような診断システム及びデバイスにおいて使用するための有利なリーダユニット及びアッセイユニットを提供することである。

【0031】

特に、本発明の診断システムは、すべての診断検査の結果すべてを強制的にユーザが受け取ることなく、ポイントオブケア用途でのマルチプレックス診断検査能力を備えた医療診断技術の使用を可能にすべきである。ユーザは、ユーザがどの分析結果を実際に受け取りたいかを予め、検査中、及び/又は検査後に選択できることが有利である。

【0032】

さらに、本発明の診断システム並びにデータ保護及びアクセス制御方法により、診断検査の柔軟な支払い又は契約モデルを可能にすべきである。

【0033】

本発明の別の目的は、消耗アッセイユニットの簡略化された分配及び在庫管理、改善された広範な製造業者の品質管理、並びにユーザにとって向上した安全性レベルである。

【0034】

本発明の診断システム及びアクセス制御方法によって患者データの守秘義務を常に確実にすべきである。

【0035】

これらの及びその他の目的は、独立請求項による診断システム、診断デバイス、リーダユニット、診断キット、及び方法によって実質的に達成される。さらなる有利な実施形態は従属請求項及び本明細書から得られる。

【発明の概要】

【0036】

本発明によれば、上記の目的は特に、1つ又は複数の診断検査を1つ又は複数の生理学的試料に対して実行し、診断検査の結果を測定し、対応するデジタル測定生データを生成し、その後、場合によっては、補助データ(例えば、センサの較正データ)の助けを借りて、当該生データを分析結果データ(例えば、血清中の特定の分析物の濃度)へと処理し、当該結果データを暗号化して、結果データをユーザが可逆的にアクセスできないようにし(データがロックされる)、ユーザの適切な認証の後、当該暗号化結果データの一部又はすべてに選択的にアクセス可能にすることができる診断システムによって達成される。

【0037】

本明細書の文脈においては、用語「暗号化されたデータ」、「ロックされたデータ」、及び「保護データ」は、特定の暗号鍵による暗号化によりロックされたデータは、復号化鍵を知らない認証されていない人によるロック解除/アクセスから保護されているため、本質的に同義であると理解されるべきである。

【0038】

10

20

30

40

50

ユーザの認証レベルは、ユーザが分析結果にアクセスする権限が与えられた診断検査に対応する。復号化され、ロック解除された分析結果データは次いで、所期の医療目的に使用できる。したがって、本発明の診断システムはユーザに、どの診断検査を実施するかを選択肢ではなく、当該検査のどの分析結果を実際に知りたいか又はアクセスしたいかを選択肢を与える。特別な利点は、ユーザの決定が最終的なものではないということである。ユーザは後にさらなる結果をロック解除したい場合がある。これらの検査結果へのアクセスが得られていれば、このことは分析結果の品質に対するいかなるマイナスの影響も与えることなく可能である。すなわち、最初の段階で、分析結果がすべて取得され、保護データとして格納されるが、アッセイユニットの概ね一時的な結果は、信頼性を持ってアッセイユニットから当該結果を読み取ることが可能な制限された有効期間を有する。

10

【0039】

暗号化前に測定生データから分析結果データに処理することに代えて、分析結果データへの処理は後で生データを復号化した後にのみ可能であるように、測定生データは直接暗号化されてもよい。

【0040】

小型な診断チップ又は類似のマルチプレックス診断検査アッセイデバイスは、多数の試薬及びセンサを組み込んでよい。さらなる試薬及びセンサを組み込むことによる診断チップへのさらなる分析能力の追加により、最小限の限界費用が生じる。したがって、このような診断システムのユーザは、このような診断チップを有するアッセイユニットを最小限の前払い価格で購入することができ、また必要な分析結果だけを購入することができるため、追加の診断チップの必要性がなくなり、検査費用全体が下がる。したがって、購入価格は、アッセイユニットそれ自体の費用ではなく、購入された分析結果に依存することができる。

20

【0041】

アッセイユニットは1つの生理学的試料に対して1つの診断検査のみ、又は異なる患者の多数の生理学的試料に対して1種類の診断検査を実施できるように実現することもできるという点に留意すべきである。しかし、このような場合、本発明の診断システムの利点の一部は活用できるが、一部は完全に活用できない。

【0042】

さらに、幅広いアッセイユニットが提供される診断システム又は非常に高価な診断検査の支払いプロセスの簡略化への適合性を確実にするために、単一の診断検査アッセイユニットを有することが有用であり得る。

30

【0043】

特に有利な実施形態では、本発明のリーダユニットは、より古い種類のアッセイユニットの結果を読み出すことが可能であり、以て旧バージョン互換性を確保するように実現されてもよい。

【0044】

ユーザは、対応する暗号化されたデータセットを復号化し、したがってロック解除するために必要な手段を備えることによって、例えば、復号化に必要な鍵データを提供することによって、又は、対応する暗号化されたデータを診断システムのセキュア領域で復号化させ、ここでロック解除された使用可能な分析結果データをユーザに送達することによって、特定の分析結果にアクセスすることが可能になる。その他の、依然として暗号化されているデータセットは、情報内容がアクセス不能でありユーザにはロックされているため、ユーザに知られているとしても保護されたままである。

40

【0045】

診断検査はすべて実際に実施されたため、ロック解除された分析結果は、さらに使用するために暗号化されたデータセットの形態で格納してもよく、先の任意の時点でアクセス可能にしてもよい。したがって、本発明の診断システムは、後の時点でも特定の診断検査を使用可能にする可能性を提供する。例えば、既に使用可能な診断検査の結果が、さらに検査しなければならない特定の可能な診断を示唆する場合にのみ、特定の診断検査が重要

50

となり得る。

【0046】

任意の認証手段なしでもアッセイユニットを分配することさえも可能になるが、その場合、購入価格は本質的に基本的な製造費用及び流通費用をまかないさえすれば良いため、非常に低く選択することができる。その後、認証手段は別途配布することができる。

【0047】

このようなアプローチによって、さらに、最大保管期間の終了によるアッセイユニットの所有者の潜在的な金銭的損失が低下する。より少ない数の異なる種類のアッセイユニットが必要とされるため、在庫に保管されるアッセイユニットの総数を減らすことができ、このことにより、機械設備に関わる金額も減少する。

10

【0048】

本明細書の文脈における用語「ユーザ」又は「ユーザ領域」は、本発明の診断デバイスを操作する患者又は医療関係者等の人間だけを意味するのではない。用語「ユーザ」又は「ユーザ領域」は、ユーザの事実上の制御下にある診断システムのあらゆる部分、例えば、本発明の診断システムの少なくとも一時的に一部であるラップトップコンピュータ、タブレットコンピュータ、又はスマートフォン等の補助コンピュータデバイスもさらに包含する。このように、診断システムのユーザ領域内のデータは主に、ユーザに知られていると考えなければならず、ユーザに知られていない鍵によりロックされ、暗号化された場合にのみ、無許可使用から保護される。

【0049】

20

本発明の診断システムの「セキュア部分」又は「セキュア領域」とは、ユーザが制限なしで完全にはアクセス可能でない診断システムの1つ又は複数の部分である。例えば、まだ暗号化されていない測定生データ及び分析結果データの処理に関連し、また測定データの後の暗号化に関連するすべての電子部品は、改竄の恐れがないように実現可能である。当該改竄の恐れがない電子部品のセキュア領域内のデータへの無許可アクセスは、相当な時間及び労力並びに悪意のある意図を以てしてのみ可能である。

【0050】

このような電子部品の保護は、例えば、合成樹脂に埋め込むことによる、又は改竄の恐れがないように回路を特別に設計することによる電子回路の機械的保護を含むさまざまな手段によって行うことができる。対応する技術及びアプローチは先行技術から、特に電子小売り支払いシステム等との関係において公知である。

30

【0051】

診断検査プロセスを、i) 診断検査を実施すること、及びii) 診断結果をアクセス可能にすることに分けられる本発明の基本発明原理から、多数の異なる診断検査を単一の試料に対して実行する能力を有するアッセイユニットに適切な購入価格で、実際に当該アッセイユニットを販売する必要なしに、多数の異なる診断検査を単一の試料に対して実行することが可能なアッセイユニットを使用することが可能である。ユーザは、ユーザが権限を与えられた特定のグループの診断検査の結果へのアクセス権を得るだけであるため、その他の診断検査は、実際に実施はされたが、ロックされ、ユーザがアクセスできないようになっているため、アッセイユニットの購入価格に関しては無視できる。

40

【0052】

本発明の診断システムでは、例えば、同時に患者の血液試料を100の異なるバイオマーカに関して分析することができるアッセイユニットを使用することができる。しかしながら、アッセイユニットは、3つの特定のバイオマーカ、例えば、心筋梗塞の診断に関連するミオグロビン、CK-MB、及びトロポニンIの分析結果へのアクセスのみを可能とする認証手段と共に分配してもよい。したがって、購入価格はこれら3つの診断検査によって設定され、先行技術のようにすべての分析結果をユーザが利用できる場合に必要となるよりもはるかに低く設定できる。

【0053】

まったく同じ種類のアッセイユニットを、他のパネルのバイオマーカ、又は単一のバイ

50

オマーカのみ認証手段と共に販売することもできる。唯一の違いは、認証手段、したがって、ユーザが予め権限が与えられる診断検査及びユーザがアクセス可能になる分析結果の種類である。

【0054】

より少ない種類の異なるアッセイユニットが必要とされるため、ユニットそれ自体は、いくつかの異なるアッセイユニットが製造されなければならない場合に可能であるよりもはるかに多い数で製造可能である。その結果低下した製造費用は、アッセイユニットにさらに異なる検査を追加するための追加製造費用も補う。

【0055】

本発明の診断システムは、一体型単一デバイスとして、又は少なくとも使用中に、例えば電子インタフェース、データ接続等により動作可能に接続される2つ以上の別個のユニット若しくはデバイスを有するシステムとして実現できる。診断システムの一部のユニット及び部品は、遠隔設置されていてもよい。

10

【0056】

本発明の特定の有利な変形例では、本発明の診断システムは、1つ又は複数の診断検査を1つ又は複数の生理学的試料に対して実行することが可能な1つ又は複数のアッセイユニットと、(1つ又は複数の)アッセイユニットが動作可能に接続でき、(1つ又は複数の)アッセイユニットからの診断検査信号又は測定生データを読み出すことが可能な再利用可能リーダユニットとを備える。

【0057】

アッセイユニットは有利には、1回限り使用可能な消耗部品として提供され、使用後に処分される。したがって、特に、生理学的試料物質と接触するか、又は接触し得るすべての要素は有利には、使い捨てアッセイユニットの一部である。

20

【0058】

他方では、リーダユニットは有利には、より高価な電子部品及び/又は診断検査の品質に悪影響を与えることなく2度以上使用可能なその他の部品を備える再利用可能デバイスである。

【0059】

リーダユニットはさらに、アッセイユニットに用意された、例えば、メモリチップ又は1次元若しくは2次元バーコードに格納されたさらなるデータを読み取ってもよい。このようなデータとしては、ユーザが読み取り、対応するインタフェース手段、例えば、キーボードにより手動でリーダユニットに入力される英数字データも挙げられ得る。さらなるデータをアッセイユニットそれ自体に提供する代わりに、当該データの一部又はすべてが、アッセイユニットが包装されるパッケージ、又は印刷カード若しくは印刷紙、チップカード等の同封のデータ媒体に付与されてもよい。

30

【0060】

アッセイユニットのデータ媒体は、データ及び鍵を記憶するための不揮発性メモリを収容する認証集積回路を用いて実装され得る。認証は例えば、チャレンジレスポンスメッセージを使用するホスト-スレーブシステムに基づくことができる。このような集積回路は、Atmel、NXP、Maxim、Texas Instruments等のいくつかの製造業者から入手可能である。認証集積回路は、標準に基づくアルゴリズムを使用して強力で手頃な暗号化によるセキュリティをもたらす。

40

【0061】

当該さらなるデータは、診断検査の結果を評価するのに必要な校正データ、バッチ番号、アッセイユニットの種類、タイムスタンプ、独自のアッセイユニット識別子等の補助データを含んでもよい。当該さらなるデータは、分析結果データの一部又はすべてにユーザをアクセス可能にする認証データをさらに含んでもよい。

【0062】

リーダユニットは、データを暗号化することによって、測定生データ又は測定生データから得られた分析結果データへのアクセスを防止するように構成されている。所望により

50

、さらなるデータの一部又はすべてもまた暗号化してもよく、又は普通テキストのままであってよい。

【0063】

少なくとも、暗号化分析結果データのみが例えば、電子インタフェースを介して外部から取得されるように、リーダユニットは診断システムのセキュア領域に属していなければならない。

【0064】

所望により、悪意のあるユーザが、接続が電子インタフェースである場合に特に重要となり得るが、アクセイユニットに直接アクセスすることによって本発明の保護機構を回避することが不可能であるように、アクセイユニットとリーダユニットとの機能的接続をセキュアなものとするのもまた可能である。このような場合、アクセイユニットもまたセキュア領域に属する。

10

【0065】

次いで、暗号化されたデータは、リーダユニットに動作可能に接続された診断システムの評価ユニットに提供される。評価ユニットは診断システムのユーザ領域に属し、有利には、ユーザの特定の保護されロックされたデータへのアクセスを可能にすることを含むデータの処理を行う。評価ユニットは例えば、ソフトウェアが提供され、コンピュータデバイスの既に存在するハードウェア、例えば、CPU、メモリ及びデータ記憶手段、電子インタフェース、ディスプレイ、キーボード等を利用して必要なタスクを実施することを可能にする標準コンピュータデバイスとして実現されてもよい。

20

【0066】

さらなるセキュリティレベルを提供するために、評価デバイスがそのタスクを実施することを可能にするソフトウェアは有利には、リーダユニット及び/又はアクセイユニットが評価ユニットに接続されている場合にのみ動作する。したがって、リーダユニット又はアクセイユニットはハードウェア鍵、いわゆる dongle として機能してもよい。或いは、必要なソフトウェア又はその必須部分は評価ユニットそれ自体ではなく、リーダユニット又はアクセイユニットのメモリモジュールに格納されてもよい。例えば、リーダユニット又はアクセイユニットは、ソフトウェアが格納された専用のフラッシュメモリユニットを備えてもよく、専用のフラッシュメモリユニットは、評価ユニットに接続されると記憶容量として現れてもよい。

30

【0067】

特定のソフトウェア要素をアクセイユニットに提供することは、新しい種類のアクセイユニットは必要なソフトウェア要素をもたらすことができるため、評価ユニット又はリーダユニットの手動でのソフトウェアアップデートが必要でなくなるというさらなる利点を有する。

【0068】

データは、リーダユニットから、例えば、USB、RS232等のバスインタフェース、光ファイバ接続、又はブルートゥース(Bluetooth(登録商標))、WLAN、IRインタフェース等の無線通信リンク、又は別の適切なデータリンク等の適切なデータインタフェースを介して評価に転送することができる。データ転送は、例えば、携帯型メモリデバイス(例えば、スマートカード、フラッシュメモリデバイス及びカード、書込み可能CD-ROM)にデータを一時的に格納し、後に携帯型メモリデバイスを評価ユニットに機能的に接続することによって手動で行うこともできる。

40

【0069】

評価ユニット、例えば、コンピュータデバイスは、暗号化されたデータの管理、認証データの取得、利用可能な認証手段に基づくデータの復号化、分析結果へのデータ処理、遠隔システムとの通信、データ格納等の種々のタスクを実行することを可能にする手段を備える。

【0070】

評価ユニットは、ロックされた分析結果の安全性を損なうことなく公共領域で行うこと

50

が可能な診断システムのタスク及び機能の少なくとも一部を実施する。特別又は特殊なハードウェアはデータ処理を含むこれらタスク及び機能に必要なとされないため、これらのタスクのために普通のコンピュータデバイスを使用することは、ユーザが既にコンピュータデバイスを利用可能であるか又は比較的安価で得ることができるため、ハードウェア費用全体を低減できるという利点を有する。

【0071】

他方では、本発明の診断システムのリーダユニットは有利には、アッセイユニットから測定生データ又は分析結果データを取得し、当該データを暗号化により保護するのに必要な最小限のハードウェア及びソフトウェアのみを備える。

【0072】

本発明の他の実施形態では、リーダユニットの機能及び評価ユニットの機能の一部又はすべては単一の診断デバイスに統合される。

【0073】

或いは、アッセイユニット及びリーダユニットが分離可能でない一体型診断デバイスが提供できる。診断検査の構成及び対応する読み出しエレクトロニクスの検出技術が完全に統合され、別個の再利用可能部分として容易に実現できない場合に一体型診断デバイスは特に有利となり得る。

【0074】

しかし、アッセイユニット、リーダユニット、及び/又は評価ユニットが別個のユニットとして実現されるか、又は一体型デバイスに部分的に組み合わされるかという問題は本発明ではそもそも重要ではない。このような一体化が好ましいかそうでないかは主に、関係する診断検査技術及び必要な費用に依存する。かなり製造費用が高いアッセイユニットについては、エレクトロニクスの一部部品、又はさらには暗号化及び/若しくはデータ処理エレクトロニクスを含むエレクトロニクスの全体が消耗アッセイユニットの一部であるかどうかは経済的観点からまったく重要ではなくなり得る。さらに、将来、電子部品がさらに安価でエネルギー効率がより高く、さらに小型になると想定しなければならない。これらはすべて一体化アプローチに好ましい。

【0075】

評価ユニットは単純にリーダユニットの場所に配置できる。しかし、必要なデータ接続はさらに、より長距離に渡って、例えば、通信ネットワークとして確立されてもよい。したがって、評価ユニットは異なる部屋に配置されても、又はさらに遠くでもよい。

【0076】

使用可能な診断検査の、保護されロックされた結果へのアクセス権を得るのに必要な認証手段は、メモリチップに格納される認証データの形態で、又は印刷された1次元若しくは2次元バーコードとして、又は評価デバイスに手動で入力しなければならないアッセイユニットに印刷された英数字コードとして提供されてもよい。認証データは独自の、特別なアッセイユニットエンティティのためだけの機能であり、これによって認証手段の起こり得る誤用を防ぐことが有利である。

【0077】

認証手段は直接アッセイユニットに設けられるか、又は別個のユニット、例えば認証データを含む同封のスマートカード、又は単にバーコード若しくは英数字コードが印刷された1枚の紙に設けられてもよい。

【0078】

分析結果の保護は、診断検査の結果へのアクセスを制御し、不正な行為を防止するために重要である。有利なアプローチでは、リーダユニット及びアッセイユニットはホストコントローラ及びセキュアオーセンティケータの手段と通信する。リーダユニットのホストコントローラは、アッセイユニットのセキュアオーセンティケータに乱数(challenge; チャレンジ)を送信し、レスポンスを受信する。このレスポンスはリーダユニットにより評価されて、アッセイユニットが本物であることを確定する。このような方法は当業者に公知であり、データ及び鍵を記憶するための不揮発性メモリを含んだ認証集積回路を使用

10

20

30

40

50

して実装され得る。認証は例えば、チャレンジレスポンスメッセージを使用するホスト-スレーブシステムに基づることができる。このような集積回路は、既に上で説明したようにいくつかの製造業者から入手可能である。

【0079】

リーダユニットがアッセイユニットを本物として確認すると、アッセイユニットは、アッセイユニットのメモリモジュールに格納された暗号化規則を、リーダユニットのセキュアメモリモジュールに転送する。セキュアメモリは、一致規則を読み出すために暗号化規則を復号化することを可能にするプライベート鍵を含む。一致規則が取得されると、個々の測定生データが個々の診断検査に割り当てられ、アッセイユニットの分析結果がコンパイルされる。次に、分析結果データセットを暗号化し、最終的にこの保護されロックされた形態でユーザに提供される。これらのステップすべては、リーダユニットのセキュア領域、例えば、専用の改竄防止電子回路で実施される。

10

【0080】

一変形例において、当該一致規則は、検査素子識別子及びそれらの対応する分析物識別子のリストを含み、当該リストは、多数の取得された生データを並列して実施された特定の診断検査へと一致させるために必要とされる。換言すれば、一致規則は、検査素子の測定生データを分析結果リストに変換するために必要とされる。例えば、マトリックス状に配置された多数の分析物のための検査素子を有する光学的に検出されるアッセイユニットの場合、一致規則により、どの検査素子がどの検出される分析物に対応するかを知ることを可能にする。

20

【0081】

一致規則は、同一の一致規則を有するアッセイユニットのグループ又は個々のアッセイユニットが異なる暗号化規則を含むような暗号化形態でアッセイユニットに提供されることが有利である。これは、例えば、特定の規則に従ってデータを並べ替えることによって、例えば、暗号化前の一致規則のデータセットを可逆的に変えることにより達成できる。結果として、同一の一致規則に対して暗号化規則データセットが異なる。

【0082】

より有利な変形例では、一致規則及び/又は暗号化規則は時間の経過と共に変更される。例えば、新しい一致規則をもたらす検査素子位置の新しいセットは、アッセイユニットの新しいバッチ毎に生成され得る。或いは、又は加えて、一致規則はバッチ毎、又はさらには個々のアッセイユニット毎に異なる暗号化規則(上記参照)に変換してもよい。対応する暗号化規則は例えば、アッセイユニットのメモリモジュールに格納される。最も必然的なアプローチは、新しく製造されたアッセイユニット毎に新しい一致規則を生成することであろう。

30

【0083】

代替的変形例では、アッセイユニットに格納された一致規則は、データベースレコードの識別子に対応し、データベースはリーダユニットのセキュアメモリに格納されている。データベースレコードは、生データを生データが表す分析結果に一致させるのに必要な情報を含む。データベースレコードは例えば、検査素子識別子と対応する分析物識別子との一致リストを含んでもよい。この方法は、アッセイユニットのデータ媒体に必要なメモリ量を最小限にし、メモリ要件をリーダユニットに移すという利点を有する。さらに別の代替策は、データベースレコードをセキュアチャネルでリーダユニットへと送信して、セキュア遠隔データベースにデータベースを格納することである。

40

【0084】

さらに別の実施形態においては、データベースレコードは暗号化形態で提供されてもよい。適切なデータベースレコードの識別子に加えて、次いで、一致規則は、対応するデータベースレコードを復号化することを可能にする復号化鍵を含む。

【0085】

さらなる実施形態では、暗号化規則は検査素子の配列に直接組み込むことができる。特定の検査素子は、診断検査目的で使用する代わりに、暗号化規則を格納するデータ媒体と

50

して使用することが可能である。生データを測定するリーダユニットは次いで、これらの検査素子を読み取り、暗号化規則を取得する。

【0086】

このような保護方法のメリットは、分析結果が保護され、認証されたユーザによってしか修正できないということである。別のメリットは、本物のアッセイユニットのみを使用して、正確な生データ及び対応する分析結果を取得できることである。さらに別のメリットは、本物のリーダユニットのみを使用して、正確な生データ及び対応する分析結果を取得することである。認可された本物のリーダユニット及びアッセイユニットのみが、迅速で正確、厳密、微細なダイナミックレンジの大きい分析結果を提供するのにその能力を最大限まで使用される。

10

【0087】

不法ユーザはアッセイユニットの一致規則を復号化しようと試みるが、このようなタスクには、同一のアッセイユニットが大量に必要となり、また極端に時間がかかり、自明でなく、桁違いの費用がかかる。一致規則及び検査素子位置は規則的に変わることで、またユーザはどのアッセイユニットが同一の一致規則を含むか認識できないことによりこのタスクは実質上不可能となっている。

【0088】

分析結果の購入、又はより正確には既に存在するが保護されている分析結果へのアクセス権を購入することを可能とするために、改竄防止リーダユニットは電子クレジットユニットメモリを備えることができる。電子クレジットユニットメモリは、遠隔支払い承認サーバを有するリーダユニットに一時的に接続し同期することにより補充できる。分析結果を購入するために、クレジットメモリのカウンタは、クレジットユニットの対応する量だけ減る。この実施形態は、クレジットメモリにクレジットユニットを補充する短い時間を除いてオンラインアクセスが必要とされないという利点を有する。使用前に補充されなければならない、したがって前払いモデルに基づくクレジットメモリの代わりに、使ったクレジットユニットを記録し、クレジット残高を遠隔支払い承認サーバと定期的に同期させ、遠隔支払い承認サーバが次にインボイスを発行するか、又は使用したクレジットユニット分を料金請求することも可能である。このようなアプローチを組み合わせることもできる。

20

【0089】

本発明の別の有利な実施形態において、認証手段をアッセイユニットに完全に組み込む代わりに、認証手段を遠隔認証サーバと組み合わせて実現することもまた可能である。本実施形態では、評価ユニットは、遠隔認証サーバへの少なくとも一時的なアクセスを必要とする。次に、使用可能な分析結果データへのアクセスをロック解除するのに必要な認証データは、遠隔認証サーバによりユーザに提供される。

30

【0090】

本発明の有利な一変形例では、リーダユニットは検査測定生データ又は分析結果データをそれぞれ、対称暗号化アルゴリズムにより暗号化する。秘密鍵暗号化としても知られている対称暗号化アルゴリズムは、関係する通信相手にのみ知られる共有秘密鍵に基づき、暗号化及び復号化のために同じ鍵を使用する。例としては、AES、ブローフィッシュ (Blowfish)、CAST5、DES、IDEA、RC2、RC4、RC6、サーペント (Serpent)、トリプルDES (Triple DES)、トゥーフイッシュ (Twofish) 等である。暗号化アルゴリズムを使用する代わりに、暗号化されるデータと等しい長さのバイナリ鍵をデータにmod 2加算できる。このようなアプローチは、より長い鍵を暗号化アルゴリズムとして必要とするが、よりセキュアで高速である。暗号化されるデータセットは特に長くはないため、鍵もまた特に長くない。

40

【0091】

後の段階で特定の分析結果の選択的ロック解除を可能にするために、診断検査 T_1 、 T_2 、 \dots 、 T_n の異なる分析結果に対応する異なるデータセット D_1 、 D_2 、 \dots 、 D_n は、異なる鍵 A_1 、 A_2 、 \dots 、 A_n により個々に暗号化される。鍵は、使用直前に生成

50

され2度目は使用されない、1回限り使用するためのランダム鍵であることが好ましい。暗号化前に、データセット D_1 、 D_2 、 \dots 、 D_n は所望により、追加のメタデータにより展開できる。当該メタデータは、診断検査番号、アッセイユニットID、リーダユニットID等のその他の有用なデータを含む。暗号化されたデータ AD_1 、 AD_2 、 \dots 、 AD_n はリーダユニットから評価ユニットに転送され、後に使用するために評価ユニットに格納される。

【0092】

秘密鍵 A_1 、 A_2 、 \dots 、 A_n はさらに、追加メタデータと組み合わせて拡張鍵データセット A^*_1 、 A^*_2 、 \dots 、 A^*_n にすることもでき、当該メタデータは、診断検査番号、アッセイユニットID、リーダユニットID等の他の有用なデータを含む。拡張鍵データセットは次に、公開鍵暗号化としても知られる非対称暗号化アルゴリズムによる2度目の暗号化が行なわれる。

10

【0093】

このような非対称暗号化アルゴリズムの例は、RSA、ディフィーヘルマン(Diffie-Hellman)、デジタルシグネチャアルゴリズム(Digital Signature Algorithm)、エルガマル(ElGamal)、ECDSA、XTRである。このような非対称暗号化では、受信者のみが知るプライベート鍵Bによって、受信者がデータを解除できるが、プライベート鍵Bに対応付けられた公開鍵Cはデータを送信したい潜在的な通信相手に利用可能となり、当該通信相手はデータを暗号化できるが復号化できないようにする。暗号化されるデータセットがさらに大きい場合、データを秘密鍵(有利には1回限り使用するランダム鍵)及び対称暗号化アルゴリズムを使用して暗号化し、次に秘密鍵自体を公開鍵及び非対称暗号化アルゴリズムを使用して暗号化することによって、非対称暗号化を対称暗号化と組み合わせてもよい。暗号化された秘密鍵は次に、暗号化されたデータセットと一緒に送信できる。

20

【0094】

本発明の診断システムでは、外部から捏造公開鍵が提供されることによる改竄リスクを避けるために、公開鍵は有利には、アッセイユニット又はリーダユニット等のセキュア領域内に既に格納されて提供されるべきである。

【0095】

公開鍵Cを用いた暗号化の後、暗号化鍵データ CA^*_1 、 CA^*_2 、 \dots 、 CA^*_n は遠隔認証サーバへと転送される。暗号化鍵データはリーダユニットに格納されることが有利であり、又は評価ユニットに格納されることがより有利であり、そこで暗号化鍵データは対応する暗号化されたデータ AD_1 、 AD_2 、 \dots 、 AD_n と一緒に格納され得る。暗号化鍵データすべてを送信する代わりに、必要とされる分析結果に属する鍵のみを遠隔認証サーバに送信してもよい。

30

【0096】

遠隔認証サーバでは鍵データが一時的に格納される。次に、ユーザは、例えば、クレジットカード払い、料金の請求、インボイスの発行、前払いバウチャの換金等によって、1つ又は複数の診断検査、例えば検査 T_2 、 T_7 、及び $T_{3,4}$ の分析結果にアクセスするための認証手段を購入して当該診断検査をロック解除できる。対応する遠隔電子支払い技術は当業者によく知られている。アッセイユニットが特定の診断検査について予め使用可能になっている場合、アッセイユニットID等の対応する独自の識別手段によって、遠隔サーバは必要な認証データ情報をローカルデータベースから取得できる。

40

【0097】

支払い取引が適切に完了するか、又はアッセイユニットIDの認証情報がデータベースから取り出されると、認証サーバは使用可能な暗号化鍵データ CA^*_2 、 CA^*_7 、 $CA^*_{3,4}$ をプライベート鍵Bにより復号化する。必要な診断検査に対応する復号化された鍵 A^*_2 、 A^*_7 、 $A^*_{3,4}$ は次いで、評価ユニットに送り返され、評価ユニットにて鍵を使用して使用可能な暗号化されたデータ AD_2 、 AD_7 、 $AD_{3,4}$ をアクセス可能な分析結果 D_2 、 D_7 、 $D_{3,4}$ に復号化する。

50

【0098】

本発明の上述の変形例は、遠隔サーバ上の慎重に扱うべき患者データ等への不正アクセスができないように、結果データは遠隔サーバに転送されないが、情報内容を有していない鍵データのみが遠隔サーバに転送されるという利点を有する。

【0099】

本発明の別の変形例において、リーダユニットは、検査測定生データ又は診断結果データDを公開鍵Cを使用して直接非対称暗号化アルゴリズムで暗号化し、暗号化されたデータCDを遠隔サーバに転送し、遠隔サーバにて暗号化されたデータCDは認証を行った後復号化され、アクセス可能なデータDとして評価ユニットに戻される。このような解決策においては、通信ネットワークをモニタしている可能性のある外部の人間からデータの秘密性を確実なものとするために、診断デバイスと遠隔認証サーバとのデータ接続が暗号化されることが有利である。

10

【0100】

このような場合に遠隔認証サーバについてもデータの秘密性を確実なものとするために、分析結果データDは、遠隔認証サーバに知られていない追加秘密ユーザ鍵Eを用いてリーダユニットにより暗号化できる。これらの暗号化されたデータEDは公開鍵Cで暗号化され、これらの二重暗号化されたデータCEDは遠隔認証サーバに送信される。秘密ユーザ鍵Eは、ユーザが選択したパスワード又はリーダユニットにより生成されユーザに提供される1回限りのランダム鍵に基づくことができる。

20

【0101】

遠隔認証サーバはそのプライベート鍵Bでデータセットの暗号化を1レベル復号化でき、次にまだ暗号化されているデータEDをユーザに戻す。しかし、遠隔認証サーバは鍵Eを利用できないため、遠隔認証サーバシステムそれ自体はデータEDにアクセスできない。したがって、第三者が遠隔サーバへの無許可の又は不正なアクセスを取得してもデータ機密は確保される。データEDが評価ユニットに戻されると、ユーザは秘密鍵Eにより暗号化の第2レベルを解除できる。診断検査結果Dは最終的にユーザがアクセス可能となる。

【0102】

完全なデータを遠隔認証サーバに転送することは、将来引き続き利用可能であることを確実なものとするために、またバックアップ策として、結果を遠隔地で格納できるというさらなる利点をもたらす。

30

【0103】

既に上で簡潔に述べたように、遠隔認証サーバを介してアクセスが可能である本発明の実施形態では、特定の診断検査又は特定の診断検査のパネルが予め使用可能なアッセイユニットの分配が特に有利である。必要なアクセスデータを単一のアッセイユニットそれぞれに格納するか又は各アッセイユニットにこのような認証データの追加媒体を設ける代わりに、対応する独自のアッセイユニットIDを製造中に記録し、予め使用可能な診断検査の認証データをローカルデータベースに格納する。したがって、認証手順は、暗号化鍵データ又は暗号化分析結果データと一緒にアッセイユニットIDを評価ユニットから遠隔認証サーバへ転送すること、予め使用可能な診断検査の鍵又は分析結果を復号化すること、及び復号化されたデータをユーザに戻すことからなる。

40

【0104】

本発明の特に有利な実施形態では、異なるレベルの認証を実施できる。第1レベルの認証は例えば、特定の分析結果が特定の規定値範囲内にある場合にのみ情報へのアクセスを提供できる。その後、ユーザインタフェースは分析結果が規定値範囲内にあるか又は範囲外にあるかについてそれぞれ診断検査を強調できる。このことは、例えば、問題となり得る健康状態を示唆できる。ユーザがさらに特定の結果を見たい場合、ユーザはその後、分析結果へのフルアクセスを提供する第2レベルの認証を購入できる。本発明の本変形例は、複数の分析物を迅速に精査し、患者の健康状態全体を確認するのに特に有用であり得る。

50

【0105】

本発明の診断システムのさらなる利点は、アッセイユニットの特定のバッチ又はそれらに含まれる検査の一部が、例えば生産上の問題により、誤った結果を出しやすい可能性があるとして後で分かった場合に、リコール手順は遠隔認証サーバを介してまとめて行うことができるということにより与えられる。例えば、認証手順は、診断検査を実施する前にアッセイユニットが認証ユニットによって、例えばアッセイユニットIDを転送することにより予め登録されなければならないように、設定してもよい。対応するIDが、リコールされたアッセイユニットのセットに属する場合、警告メッセージがユーザに与えられ、アッセイユニットを使用せず、製造業者へ返送するように要求する。

【0106】

同じ手順を使用して、最大有効期間に到達したアッセイユニットの使用を防止するか、又は過失によるアッセイユニットの2度目の使用を防止してもよい。診断検査が前述の警告にもかかわらず実施された場合、問題の深刻さに応じて適切な対策をとってもよい。分析結果へのアクセスが拒否されてもよく、又は分析結果にユーザが受け取ったことを確認しなければならない警告メッセージが付随してもよい。

【0107】

別の利点は、偽造アッセイユニットの予防である。認可された製造業者から製造されていないアッセイユニットは必要な品質基準を満たしていない場合がある。しかし、ユーザがこのような認可されていない製品であるか見分けるのは困難である場合があり、製造業者は、自社が製造していない製品に対して責任を負うというリスクに晒され得る。認可されたアッセイユニットはすべて製造中に登録され得るため、認可されていないアッセイユニットは容易に識別できる。

【0108】

本発明の別の利点は、分析結果は例えば病院内のネットワーク上で共有でき、遠隔の認証されたユーザがアクセスできることである。次に、例えば、病室内の専用の評価ユニットから、又は認証された遠隔アクセスデバイスから、例えば、担当医師のオフィス内の計算デバイスで分析結果にアクセスするか、選択するか、見るか、又は購入できる。分析結果を測定した後に分析結果を暗号化することによって、患者の個人データの機密を保護することが可能である。

【0109】

このようなアプローチの変形例では、評価ユニットは、リーダユニットから受信した保護され、ロックされたデータ及び/又はロック解除された分析結果データを遠隔記憶サーバに格納できる。このような遠隔記憶サーバは、特定のユーザ又はユーザのグループが操作する専用のサーバであってもよい。或いは、遠隔記憶サーバは第三者によって操作される遠隔認証サーバと組み合わせて実現されてもよい。後者の場合、遠隔記憶サーバは有利には、診断検査すべての既にロック解除されたデータを格納できるが、所望により、データはユーザの秘密鍵により暗号化されてもよい。

【0110】

このような変形例は、バックアップを含む適切な長期間データ記憶を確実にでき、分析データは、既に存在する結果データの確認のためであれ、又はさらなる分析結果へのアクセス権の購入のためであれ、医師のオフィス内のコンピュータ等の遠隔アクセスデバイスによってより便利にアクセスできるため、特に有利である。

【0111】

追加の分析結果を購入するために遠隔サーバへの接続を必要としない本発明の診断システムのさらに別の実施形態では、スマートカードデバイス等の改竄防止認証ユニットは、秘密鍵B及び予め入れられたクレジットユニットカウンタを含む。認証ユニットはリーダユニットに、若しくは例えば、標準スマートカードリーダにスマートカードを接続する場合は評価ユニットに動作可能に接続されるか、又はアッセイユニットに一時的若しくは永久的に一体化されてもよい。リーダユニットは、認証デバイスに格納されたプライベート鍵Bに対応する公開鍵Cを使用し、遠隔認証サーバに関して上述されたアプローチと同様

10

20

30

40

50

にして、公開鍵 C で間接的又は直接的に結果データ D を暗号化する。したがって、暗号化されたデータ A D 及び暗号化秘密鍵 C A は、評価ユニット又は暗号化されたデータ C D に提供される。ユーザが分析結果を購入するか又は見たい場合、暗号化鍵 C A 又は暗号化されたデータ C D はそれぞれ、要求される診断検査結果についての情報と一緒に認証デバイスに送信される。認証デバイスはそれに従ってクレジットユニットカウントを減らし、プライベート鍵 B でデータを復号化し、復号化されたデータ A 又は D を評価ユニットに戻す。

【 0 1 1 2 】

このような実施形態のさらなる変形例では、リーダユニットは公開鍵のセットの 1 つを使用して分析結果を暗号化し、暗号化した分析結果を評価ユニットに提供する。リーダユニットの公開鍵に対応するプライベート鍵のセットは改竄防止認証デバイスに格納される。ユーザが分析結果を購入するか又は見たい場合、評価ユニットは、認証デバイスからのデータを復号化するのに必要な対応するプライベート鍵を要求する。認証によりクレジットユニットカウントを減らし、要求されたプライベート鍵を提供する。公開鍵 / プライベート鍵の各対は 1 度しか使用してはならない。評価ユニットは、プライベート鍵を使用して分析結果を復号化し、分析結果をユーザに提供する。

10

【 0 1 1 3 】

公開鍵とプライベート鍵の対の対応関係により、認証デバイスそれ自体の真偽を証明する。プライベート鍵セットは認証ユニットに既に存在していなければならないが、公開鍵セットは、アッセイユニットと一緒に既に提供されているか、又は認証デバイスの独自の識別子に基づいて信頼できる遠隔サーバからダウンロードされるか、又は予めインストールされたローカルデータベースに提供されている。後者 2 つの可能性は、1 番目の場合には、認証デバイスが特定のアッセイユニットと組み合わせられたときにのみ機能するため、特に有利である。

20

【 0 1 1 4 】

本実施形態の別の変形例は、各分析結果に対して単一の公開鍵及び別個のプライベート鍵を用いる細粒度アクセス制御暗号化を用いることである。プライベート鍵は認証デバイスに格納され、公開鍵はリーダユニットに格納される。この例では、分析結果はリーダユニットの公開鍵を使用して暗号化でき、特定の分析結果はその後、スマートカードのプライベート鍵を使用して復号化できる。細粒度アクセス制御に使用される技術はいくつかある。このような技術の 1 つは、属性ベース暗号化である。

30

【 0 1 1 5 】

さらに別の変形例においては、暗号化分析結果はリーダユニットから認証デバイスへ転送され、認証デバイスで安全に格納される。

【 0 1 1 6 】

さらなる別の実施形態では、秘密鍵が、リーダユニット及び / 又は評価ユニット及び / 又は遠隔サーバに提供される。リーダユニットは秘密鍵を使用して分析結果データを暗号化する。ユーザが分析結果を購入するか又は見たい場合、評価ユニットは秘密鍵を使用して分析結果を復号化し、ユーザに提供できる。暗号化分析結果はリーダユニットから、各々が秘密鍵を有する遠隔記憶サーバ及び遠隔アクセスデバイスに送信できる。単純ではあるが、この方法は、秘密鍵がユーザに対して秘密とされアクセス不能である限り安全である。本実施形態は、製造業者が秘密鍵をリーダユニット、評価ユニット等に提供することをさらに必要とする。或いは、秘密鍵は標準セキュアデータ転送技術を使用してリーダユニットからサーバ及び他の遠隔アクセスデバイスに送信できる。

40

【 0 1 1 7 】

本発明の別の変形例において、センサデータはアッセイユニットから選択的に読み出される。ユーザは所望の分析結果を選択できる。リーダユニットは、センサから選択された分析結果を取得するために必要とされるデータのみを読み出すことができる。この変形例は、ユーザが診断検査前に、どの分析結果が必要か知っている場合に有用であり得る。しかし、本変形例は、一部のセンサデータは読み取られないため、一部の必要となり得る分

50

析結果は不可逆的に消されるという不利点を有し得る。

【0118】

本発明は、添付の特許請求の範囲で述べられる特徴の1つ若しくは複数、並びに/又は次の特徴の1つ若しくは複数及びそれらの組み合わせを含み得る。

【0119】

本発明のリーダユニットの有利な実施形態は、1つ又は複数の診断検査を1つ又は複数の生理学的試料に対して実行できるアッセイユニットと動作可能に接続されるように構成され、リーダユニットと動作可能に接続されたアッセイユニットで実行される診断検査の検査生データを取得するように構成されている。リーダユニットは、検査生データを取得し、一時的に格納し、当該検査生データを分析結果データに変換し、当該分析結果データをロック鍵データによって暗号化されたデータへと暗号化し、当該暗号化されたデータを出力インタフェースに提供するように構成されたデータ保護モジュールを備える。保護モジュールは、モジュール内に格納されたデータへのアクセスを防止するように構成された改竄防止モジュールである。したがって、保護モジュール及びリーダユニットは全体で暗号化されたデータへのアクセスを提供するが、分析結果データへのアクセスは提供しない。

10

【0120】

保護モジュールは、暗号化を実施するための暗号化モジュールを備えることが有利である。

【0121】

本発明のリーダユニットの当該前述の実施形態の別の有利な変形例では、リーダユニットは第2のデータインタフェースから補助データを受信するように構成されている。

20

【0122】

本発明のリーダユニットの当該前述の実施形態の別のさらなる有利な変形例では、保護モジュールは、ロック鍵データを第2レベル鍵データにより暗号化されたロック鍵データへと暗号化し、当該暗号化されたロック鍵データを出力インタフェースに提供するように構成されている。したがって、保護モジュール及びリーダユニットは全体で暗号化されたロック鍵データへのアクセスを提供するが、ロック鍵データへのアクセスは提供しない。

【0123】

本発明のリーダユニットの当該前述の実施形態の別のさらに別の有利な変形例では、リーダユニットは第1のデータインタフェースにデータを提供するように構成されている。

30

【0124】

本発明の診断デバイスの有利な実施形態は、上述のような本発明のリーダユニットと、1つ又は複数の診断検査を1つ又は複数の生理学的試料に対して実行することができるアッセイユニットとを備える。アッセイユニット及びリーダユニットは永久的に又は取り外し可能に、動作可能に互いに接続され、リーダユニットは、アッセイユニットで実行される診断検査の検査生データを取得するように構成されている。或いは、又は加えて、診断デバイスは、リーダユニットと永久的又は取り外し可能に、動作可能に互いに接続され、リーダユニットからデータを受信し、認証鍵データを使用して当該データの少なくとも一部を復号化し、復号化された出力データを使用して分析結果データを取得するように構成された評価ユニットを備える。

40

【0125】

本発明のこのような診断デバイスの有利な変形例では、評価ユニットは、暗号化されたデータを復号化するように構成されたデータ処理モジュールを備える。

【0126】

本発明の当該診断デバイスの別の有利な変形例では、評価ユニットは、データ出力モジュール、例えば、ディスプレイ若しくはプリンタ、及び/又はデータ入力モジュール、例えば、キーボード若しくはトラックパッド、及び/又は複合データ入力/出力モジュール、例えばタッチスクリーンを備える。

【0127】

50

本発明の診断システムの有利な実施形態は、上述のような本発明の1つ又は複数のリーダユニットと、1つ又は複数の診断検査を1つ又は複数の生理学的試料に対して実行でき、アッセイユニットで実行された診断検査の検査生データを取得するように構成されたリーダユニットに動作可能に接続されるように構成されている、1つ又は複数のアッセイユニットと、リーダユニットに動作可能に接続され、リーダユニットからデータを受信し、当該データの少なくとも一部を認証鍵データを使用して復号化し、分析結果データを取得するために復号化された出力データを使用するように構成された1つ又は複数の評価ユニットとを備える。

【0128】

評価ユニットは、暗号化されたデータを復号化するように構成されたデータ処理モジュールを備えることが有利である。

10

【0129】

評価ユニットは、データ出力モジュール、例えば、ディスプレイ若しくはプリンタ、及び/又はデータ入力モジュール、例えば、キーボード若しくはトラックパッド、及び/又は複合データ入力/出力モジュール、例えばタッチスクリーンを備えてもよい。

【0130】

本発明の診断システムのある有利な変形例では、1つ若しくは複数の認証ユニットは、評価ユニットに動作可能に接続され、及び/又は1つ若しくは複数の遠隔認証サーバは、通信ネットワークを介して評価ユニットに接続される。認証ユニット及び/又は遠隔認証サーバは、特定の条件が満たされると、認証鍵データを評価ユニットに提供するように構成されている。

20

【0131】

本発明の診断システムのある有利な変形例では、1つ若しくは複数の認証ユニットは、評価ユニットに動作可能に接続され、及び/又は1つ若しくは複数の遠隔認証サーバは、通信ネットワークを介して評価ユニットに接続される。認証ユニット及び/又は遠隔認証サーバは暗号化されたデータを評価ユニットから受信し、特定の条件が満たされると暗号化されたデータの一部又はすべてを復号化し、復号化されたデータを評価ユニットに提供するように構成されている。

【0132】

本発明の診断システムの当該変形例の両方において、満たされなければならない特定の条件とは、特定の認証データの認証ユニット及び/又は遠隔認証サーバへの提供である。

30

【0133】

本発明の診断キットは、1つ又は複数の診断検査を1つ又は複数の生理学的試料に対して実行することが可能な検査モジュールを有する1つ又は複数のアッセイユニットと、上述のような本発明のリーダユニットとを備える。

【0134】

完全なデータセットのうち、ユーザが権限を与えられたデータのサブセットへのユーザのアクセスを制御する、特にマルチプレックスアッセイユニットの分析結果へのユーザのアクセスを制御する本発明の方法の有利な変形例は、I) 完全なデータセットを用意するステップと、II) 完全なデータセットをロック鍵データにより暗号化するステップと、III) 暗号化されたデータセットをユーザに提供するステップと、IV) ユーザが、暗号化されたデータセットのユーザが権限を与えられたデータのサブセットに対応する部分へのアクセス権は得るが、暗号化されたデータセットの他の部分へのアクセス権は得ないことを可能にする認証手段をユーザに提供するステップと、を含む。

40

【0135】

アッセイユニットの分析結果へのユーザのアクセスを制御する当該方法の特に有利な変形例では、本方法は、a) 並行して複数の診断検査を1つ又は複数の生理学的試料に対して実施するように構成されたアッセイユニットを用意するステップと、b) 当該アッセイユニットから当該複数の診断検査の分析結果の完全なデータセットを読み出すステップと、c) 分析結果の完全なデータセットをロック鍵データによって暗号化するステップと、

50

d) 分析結果の暗号化された完全なデータセットをユーザに提供するステップと、e) ユーザが、分析結果の暗号化された完全なデータセット内に存在するような分析結果の完全なデータセットの特定の認証されたサブセットへのアクセス権は得るが、分析結果の完全なデータセットの他の部分へのアクセス権は得ないことを可能にする認証手段をユーザに提供するステップとを含む。

【0136】

本発明のこのような方法のある有利な変形例では、認証手段は認証鍵データであり、該認証鍵データは暗号化されたデータ、すなわち、分析結果の暗号化された完全なデータセットの特定の部分を復号化することを可能にするため、復号化されたデータはデータの認証されたサブセット、すなわち、分析結果の完全なデータセットのうち特定の認証されたサブセットに対応する。

10

【0137】

本発明のこのような方法の別の有利な変形例では、認証手段は認証データであり、該認証データはユーザが認証ユニット又は遠隔認証サーバから認証鍵データを受信することを可能にし、認証鍵データは、暗号化されたデータ、すなわち、分析結果の暗号化された完全なデータセットの特定の部分を復号化することを可能にするため、復号化されたデータは、データの認証されたサブセット、すなわち、分析結果の完全なデータセットのうち特定の認証されたサブセットに対応する。

【0138】

本発明の当該方法において、ステップII) / ステップc) では、データセットの異なるサブセット、すなわち、分析結果の完全なデータセットの異なるサブセットは、共にロック鍵データを成す異なるロック鍵を用いて、共に暗号化されたデータ、すなわち、分析結果の暗号化された完全なデータセットを成す暗号化されたデータの異なるサブセットへと暗号化されることが有利である。

20

【0139】

ステップII) / ステップc) の暗号化は非対称暗号化アルゴリズムを用いて行うことができ、ロック鍵は非対称暗号化アルゴリズムのための公開鍵であり得る。

【0140】

非対称暗号化を用いる本方法の特に有利な変形例では、認証手段は、共に認証鍵データを成す非対称暗号化アルゴリズムのプライベート鍵であり、当該プライベート鍵は、暗号化されたデータのサブセットを復号化すること、すなわち、分析結果の暗号化された完全なデータセットのサブセットを復号化して、暗号化された完全なデータセットの復号化されたデータサブセットが、認証されたデータのサブセットに対応すること、すなわち、分析結果の完全なデータセットの特定の認証されたサブセットに対応すること、を可能にする。

30

【0141】

或いは、ステップII) / ステップc) の暗号化は対称暗号化アルゴリズムを用いて行うことができ、ロック鍵は対称暗号化アルゴリズムのための秘密鍵であり得る。

【0142】

対称暗号化を用いる本方法の特に有利な一変形例では、認証手段は、共に認証鍵データを成すロック鍵データの特定の鍵であり、当該特定の鍵は、暗号化されたデータのサブセットを復号化すること、すなわち、分析結果の暗号化された完全なデータセットのサブセットを復号化して、暗号化された完全なデータセットの復号化されたデータサブセットが、認証されたデータのサブセットに対応すること、すなわち、分析結果の完全なデータセットの特定の認証されたサブセットに対応すること、を可能にする。

40

【0143】

対称暗号化を用いる本方法の別の特に有利な変形例では、ステップII) / ステップc

50

後、ロック鍵データは、共に第2レベル鍵データを成す非対称暗号化アルゴリズム用の1つ又は複数の公開鍵を使用して、非対称暗号化アルゴリズムによって暗号化されたロック鍵データへと暗号化される。

【0144】

本方法のこのような変形例では、暗号化されたロック鍵データをユーザに提供できる。或いは、又は加えて、暗号化されたロック鍵データは認証ユニット又は遠隔認証サーバに提供でき、認証手段は認証データであり得て、該認証データは、ユーザが認証ユニット又は遠隔認証サーバに対して、

暗号化されたロック鍵データの特定の部分を復号化することにより、復号化されたロック鍵データは、暗号化されたデータのサブセットを復号化することができるロック鍵に対応し、暗号化されたデータの復号化されたデータサブセットは、認証されたデータのサブセットに対応するようにすること、

復号化されたロック鍵データをユーザに提供すること、
を実行させるように命令することを可能にする。

【0145】

上述のような本発明の基本方法のさらに別の有利な変形例では、暗号化されたデータ、すなわち分析結果の暗号化された完全なデータセットは認証ユニット又は遠隔認証サーバに提供される。認証手段は認証データであり得て、該認証データは、ユーザが認証ユニット又は遠隔認証サーバに対して、

暗号化されたデータの特定の部分を復号化することにより、復号化されたデータがデータの認証されたサブセット、すなわち、分析結果の完全なデータセット(73、74)の特定の認証されたサブセット(73a、74a)に対応するようにすること、

復号化されたデータをユーザに提供すること、

を実行させるように命令することを可能にする。特に有利な変形例では、ステップII) / ステップc)における暗号化の前に、データセットの異なるサブセットは、ユーザに提供されるプライバシー鍵データにより暗号化される。

【0146】

上述のような本発明の方法において、ステップII) / ステップc)で暗号化される完全なデータセットは、アッセイユニットの分析結果データ又はアッセイユニットの検査生データを含む。データの認証されたサブセットは、認証された分析結果、又はさらに認証された分析結果へと処理できる認証された検査生データを含む。

【0147】

上述のような本発明の方法において、認証手段はアッセイユニット又はアッセイユニットに対応付けられたデータ媒体に提供される。

【図面の簡単な説明】

【0148】

本発明のさらなる完全な理解を促すために、ここで添付の図面を参照する。これらの参照は、本発明を限定するものと解釈すべきではなく、単なる例示を意図するものである。

【図1】アッセイユニット、リーダユニット、及び評価ユニットを有する本発明の診断システムの有利な実施形態の概略図である。

【図2】図1に示す診断システムの実施形態における検査結果データの読み出しの概略図である。

【図3】診断検査が実施され、結果が測定及び処理され、その後暗号化によりロックされ、潜在的なさらなる使用のために保護された結果がユーザに提供されるプロセスの一部を説明するフローチャートである。

【図3A】生データを分析結果に処理する有利な変形例を説明するフローチャートである(ステップS15)。

【図4】予め認証された診断検査についての、ロックされ保護された結果へのアクセスが可能になるプロセスの一部を説明するフローチャートである。

【図5】別途認証が購入された診断検査についての、ロックされ保護された結果へのアク

10

20

30

40

50

セスが可能になるプロセスの一部を説明するフローチャートである。

【図 6】本発明の診断システムの別の有利な実施形態の概略図である。

【図 7】図 6 に示す診断システムの実施形態における検査結果データの読み出しの概略図である。

【図 8】アッセイユニット及びリーダユニットが複合デバイスとして実現される、本発明の診断システムのさらなる有利な実施形態の概略図である。

【図 9】評価ユニット及びリーダユニットが複合デバイスとして実現される、本発明の診断システムのさらに別の有利な実施形態の概略図である。

【図 10】(a) 1つの評価ユニットを共有する2つのリーダユニットを有する本発明の診断システムと、(b) 2つのアッセイユニットに同時に動作可能に接続され得るリーダユニットを有する本発明の診断システムを概略的に示す。

【図 11】遠隔認証サーバ及び一般的な通信ネットワーク上で通信するその他のエンティティを有する診断システムの概略図である。

【図 12】分析結果を選択し、購入し、見るための例示的インタフェースの概略図である。

【図 13】分析結果の購入を確定するための例示的インタフェースの概略図である。

【図 14】分析結果の購入を確定するための別の例示的インタフェースの概略図である。

【図 15】分析結果を表示するための例示的インタフェースの概略図である。

【図 16】分析結果を遡って購入するか又は見ることを可能にする分析結果データのデータベースのための例示的インタフェースの概略図である。

【図 17】分析結果を保護し、購入し、見る手順を説明するフローチャートである。

【図 18】検査データをサーバに転送する手順を説明するフローチャートである。

【図 19】サーバデータベースに格納される分析結果を購入するか又は見る手順を説明するフローチャートである。

【発明の実施形態の説明】

【0149】

例として本明細書に開示される実施形態の特定の態様を以下にまとめた。これらの態様はただ単に、読者に、本明細書で開示及び/又は特許請求される任意の実施態様がとり得る特定の形態の概略を示すために提示されており、またこれらの態様は本開示の範囲を制限することを意図していないことを理解すべきである。実際に、本明細書で開示及び/又は特許請求される任意の実施態様は、以下で述べられていない場合がある種々の態様も包含できる。

【0150】

同一であるか又は少なくとも機能面が同一である構成要素は、以下で同一又は少なくとも類似の参照番号で示される。

【0151】

機能的に接続されたアッセイユニット 11、リーダユニット 31、及び評価ユニット 51 を備えた本発明の診断システム 1 の有利な実施形態を図 1 に概略的に示す。

【0152】

有利には消耗ユニットとして実現されるアッセイユニット 11 は、用意された生理学的試料 15 に 1 つ又は複数の診断検査を実施できる検査モジュール 12 を備える。メモリモジュール 18 は、分析結果は含まない、アッセイユニットに関する補助データ、例えば、アッセイユニット ID 番号、ロット番号、製造日、有効期限、アッセイユニットの種類、その他の仕様、校正データ、暗号化一致規則等のさまざまな追加データ 72 を格納することを可能にする。さらに、当該データ 72 は、例えば、アッセイユニットが予め認証された 1 組の診断検査へのアクセスを可能にする認証データを含んでもよく、したがって当該分析結果を別途購入する必要がない。加えて、データ 72 はさらに、例えば、タイムスタンプ、エラーメッセージ、プロトコル、患者データ等の実施された診断検査に特有のデータを含んでもよいが、それ自体の結果は含まない。

【0153】

10

20

30

40

50

メモリモジュール18のデータ72は、アクセイユニットのデータインタフェース20とリーダユニットのデータインタフェース38との接続により確立されたデータ接続19を介してリーダユニットがアクセスできる。データ接続は、パラレルデータバス又はシリアルデータバス、例えば、USB又はイーサネット(Ethernet)(登録商標)として実現され得る。その他の可能性としては、無線アクセス手段、例えば、近距離無線通信、例えば、RFID技術等、又は無線プロトコル、例えば、ブルートゥース/IEEE-802.15、WLAN/IEEE-802.11等、それだけでなく光通信手段、例えば、IRデータ転送インタフェース等がさらに挙げられる。

【0154】

メモリモジュール18は、永久的に又は一時的にデジタルデータを格納することを可能にする任意の最新技術、例えば、フラッシュメモリチップにより実現できる。リーダユニットはメモリモジュールに格納されたデータへのフルアクセス権を有してもよく、又はアクセスは有利には、例えば、「スマートカード」チップとして実現され得るメモリモジュールそれ自体によって制御されてもよい。

10

【0155】

アクセイユニットが基づく技術の種類に応じて、接続が単なる結果の読み出しのためだけに必要であるように、診断検査が実施されてから、アクセイユニットはリーダユニットに取り外し可能に接続される。このことは、診断検査がかなりの時間を必要とするか、若しくは特別な環境で実施されなければならない場合、又はいくつかのアクセイユニットが並行して診断検査を行う場合に有利であり得る。その他の場合では、アクセイユニットがリーダユニットに接続されている間に診断検査を実施することがより有利であり得る。

20

【0156】

リーダユニットはまた、アクセイユニットに電力を供給するか、又は制御ユニット(図示せず)若しくは例えばリーダユニット31に統合され得る制御モジュール若しくは評価ユニット51にデータインタフェースを提供することにより、アクセイユニット11の操作を制御可能にする等の補助機能を有してもよい。

【0157】

アクセイユニット11は取り外し可能に動作可能にリーダユニット31に接続されると、リーダユニットのセンサモジュール32によって、リーダユニットは診断検査の結果17を読み出すことができる。例えば、センサモジュールは、例えば、電極対のアナログ電圧信号等の検査信号、又はセンサモジュール32の受光器(例えば、カメラ)から見えるため光学情報を測定してもよい。センサ信号は次いで、デジタル形態の検査生データ73に変換される。アナログ電圧信号17は例えば、AD変換器によって検査生データを表すデジタル出力値に変換できる。検査生データはさらに、CCDチップ等から読み取ることが可能なデジタルデータであってもよい。

30

【0158】

図1に示す診断システムの実施形態における検査結果データの読み出しの可能なアプローチを図2で概略的に示す。生理学的試料15は検査モジュールのいくつかの検査素子12.1、. . .、12.nに提供され、各素子は1つの特定の診断検査を実施できる。次に、検査素子の出力信号17.1、. . .、17.nは、センサモジュール32のセンサ素子32.1、. . .、32.nにより測定される。センサ素子32.1、. . .、32.nはそれぞれ、対応する診断検査の生データ73.1、. . .、73.nの1つのセットを用意する。生データのすべてのセットは共に検査生データ73を成す。

40

【0159】

本発明の診断システムに使用可能なアクセイユニットは、先行技術から公知の種々の技術、例えば、検査片、顕微鏡スライド、マイクロ流体チップ、マイクロチップ、カートリッジ、コンパクトディスク、マルチウェルプレート等で実現できる。アクセイユニットは、種々の分析物を測定することが可能な異なる検査素子を含んでもよい。分析物は例えば、タンパク質、核酸、細胞、小分子、気体、電解質、又は病原体(例えば、細菌、ウイルス、プリオン)等であり得る。適用される診断技術に応じて、アクセイユニットはさらに

50

、診断検査を実施するのに必要なさまざまな試薬、補助システム、マイクロポンプ、マイクロプロセッサ等を備えてもよい。しかし、このような診断技術の種類は、アッセイユニットが、リーダユニットの適切なセンサモジュールにより読み出されてデジタル形態に変換できる形態で診断検査結果を提供できる限り、本発明の原理には重要でない。光学的手段、機械的手段、電気的手段、又は化学的手段等の種々の変換機構が使用できる。

【0160】

用語「検査素子」、「検査モジュール」、「センサモジュール」、及び「検査生データ」は広い意味で理解されなければならない。例えば、アッセイユニットが、分析物の量が検査片の特定のレイの特定の色に対応する検査片技術に基づく場合、検査片の光学情報は光センサ又はセンサモジュールにより検出され、デジタル形態の検査生データに変換される。一体型センサを有するより複雑なアッセイユニットの場合、当該センサは、マルチピンプラグの複数の電気接点にアナログ電気信号を提供できる。センサモジュールは当該信号を測定し、対応するデジタル検査生データを生成する。より複雑なアッセイユニットは、データ処理能力を備えてもよく、検査生データをリーダユニットに直接提供できる。

10

【0161】

完全な並列検出の代わりに、信号17.1、. . .、17.nを、1つだけの又は少数のセンサ素子により順次測定することもまた可能である。センサ素子としてのデジタルカメラは、同時にすべての検査素子の画像を受信することもでき、このデジタル画像は検査生データ73を形成する。この場合、別個の検査生データ17.1、. . .は、画像内の対応する検査素子の位置により規定される。順次診断検査を実施することもまた可能であり得る。本発明を実施するために、満たされなければならない唯一の条件は、異なる検査素子12.1、. . .、12.nの結果は検査生データ73全体とは明確に分離可能でなければならないということであり、或いは、好適なデータ処理により検査生データ73全体から別個の分析結果74.1、. . .、74.nを得ることができなければならない。明らかに、1つのみの単一の診断検査を実施することを目的としているアッセイユニットの場合、この条件は常に満たされる。

20

【0162】

リーダユニット31は、検査生データ73及び追加データ72を取得する改竄防止保護モジュール41を備える。データをロックし、ユーザ又は評価ユニットそれぞれに対してデータをアクセス不能なものとするために、保護モジュールは、上で詳細に説明されるような検査生データ73を暗号化できる暗号化モジュール33を備える。暗号化を必要としない特定のデータは、普通テキストデータ78として暗号化モジュールにより転送され得る。

30

【0163】

任意選択的な揮発性及び/又は不揮発性メモリモジュール35は暗号化モジュールに接続され、一時的にデータを格納することを可能にする。メモリ能力を直接暗号化モジュールに統合することもまた可能である。

【0164】

暗号化モジュール33は、すべての機能が配線によって接続された集積回路として、又はメモリモジュールに格納されて提供できるプログラムを実施するマイクロプロセッサとして、又は両方の組み合わせとして実現され得る。

40

【0165】

暗号化モジュールはさらに、検査生データを分析結果データに変換するために使用されてもよく、又は別の変換モジュールを使用してもよい(図示せず)。

【0166】

暗号化されたデータ77及び普通テキストデータ78のデータは改竄防止モジュール41の出力インタフェース42に提供される。データは、出力インタフェース42から、リーダユニット31のデータインタフェース36、データ接続37、及び評価ユニットのデータインタフェース52を介して診断デバイスの評価ユニット51に送信でき、評価ユニット51で受信できる。このデータ接続については、上でさらに論じられているようなア

50

ッセイユニット 1 1 とリーダユニット 3 1 との間のデータ接続 1 9 と同じ能力が利用できる。

【 0 1 6 7 】

リーダユニット 3 1 は、本発明の診断システム 1 のセキュア領域 5 に属する。換言すると、ユーザ又は任意の他の外部の人が、ユーザに明示的に提供されていないリーダユニット内部の任意のデータへのアクセス権を有することを意図しない。リーダユニット 3 1 又は少なくとも保護モジュール 4 1 は改竄の恐れがないように実現される。したがって、ユーザ又は任意の第三者は、暗号化前に、アクセス可能であるように意図されていないデータ、すなわち、まだ暗号化されていない検査生データ又は分析結果データにアクセスできるべきではない。先行技術で公知である、電子回路を無許可アクセス又は操作から保護するためのいくつかの技術及びアプローチがある。

10

【 0 1 6 8 】

診断システム 1 の評価ユニット 5 1 は、データ処理モジュール 5 3 を備える。データ処理モジュール 5 3 は、認証された分析結果データへのアクセス権を得、当該データを後で評価し、最終的にはユーザに使用可能な結果を提供するために実施しなければならないさまざまなタスクを実行することができる。データ処理モジュールは、対応するプログラムコードを実施できるマイクロプロセッサ又は CPU であることが有利である。

【 0 1 6 9 】

評価ユニット 5 1 は、診断システムのユーザ領域 3 に属するが、これはユーザが主として評価ユニットに存在する任意のデータへのアクセス権を有することを意味する。

20

【 0 1 7 0 】

評価ユニット 5 1 は、ユーザに情報を提示することを可能にするデータ出力モジュール 5 5 を備えてもよい。データ出力モジュールは例えば、ディスプレイ、内蔵型プリンタユニット、又は単に状態情報を示すいくつかの LED として実現され得る。さらに、評価ユニットは、ユーザが手動でデータを入力するか又は評価ユニットに命令を与えることを可能にするデータ入力モジュール 5 6 を備えてもよい。データ入力モジュールは例えば、いくつかのキー若しくはボタンを備えてもよく、又は完全なキーボード、データ出力モジュール、及びデータ入力モジュールはさらに、例えばタッチスクリーンの形態で組み合わせられてもよい。

【 0 1 7 1 】

評価ユニットは、本発明の診断システムで使用するための専用の特別なデバイスであってもよい。しかし、評価ユニットの本質的にすべての必要な及び任意選択的なハードウェア要素は、デスクトップパーソナルコンピュータ、ラップトップコンピュータ、タブレット、スマートフォン等の標準計算デバイスにおいて利用可能であるため、評価ユニットは有利には、種々のタスクを実施するための適切なソフトウェアを装備したこのような計算デバイスで実現される。例えば、診断システムにおいて使用するための専用の基本評価ユニットと、例えば基本ユニットの遠隔制御を可能にするか又は基本ユニットの能力を高める、基本ユニットに接続された追加コンピュータデバイスとの 2 つ以上の接続されたデバイスによって、評価ユニットを実現することもまた可能であってもよい。

30

【 0 1 7 2 】

本発明の診断システムにおいて起こり得る典型的な動作及び事象の流れを、図 3、3 A、4、及び 5 のフローチャートで概略的に説明する。

40

【 0 1 7 3 】

ステップ S 1 1 では、ユーザは適切なアッセイユニットを選択し、所定のプロトコルの後に診断検査を生理学的試料に実施する。次にアッセイユニットをリーダユニットに接続し S 1 2、アッセイユニット検査素子の出力信号を測定する S 1 3。得られた検査生データを読み出し S 1 4、診断検査すべてについての分析結果へと処理する S 1 5。次のステップ S 1 6 では、分析結果を次に暗号化によりロックすることにより、ユーザのアクセスから保護する。暗号化されたデータをリーダユニット又は評価ユニットのいずれかに格納する S 1 7。ここでシステムは状態 A にある。

50

【 0 1 7 4 】

ステップ S 1 5 の特に有用な変形例を図 3 A のフローチャートに記す。リーダユニットのセキュア領域内のホストコントローラ（図示せず）は、アッセイユニットのセキュアオーセンティケータ（図示せず）と通信する。リーダユニットのホストコントローラは、アッセイユニットのセキュアオーセンティケータにチャレンジを送信し、レスポンスを受信する。リーダユニットは、アッセイユニットのセキュアオーセンティケータからのレスポンスが本物であるかどうかを評価する。アッセイユニットが本物であれば、リーダユニットはアッセイユニットから暗号化規則を受信する。

【 0 1 7 5 】

ここから以下の操作が診断システムのセキュア領域で実施される。復号化アルゴリズムはプライベート鍵及び暗号化規則を入力として受け取り、一致規則を生成する。変換アルゴリズムは、生データ及び一致規則を入力として受け取り、分析結果を生成する。

【 0 1 7 6 】

保護機能は次いで、格納されたプライベート鍵（セキュア領域内）又は格納された公開鍵（必ずしもセキュア領域にある必要はない）を使用して分析結果を暗号化する。このステップは図 3 のステップ S 1 6 に対応する。

【 0 1 7 7 】

暗号化により保護された分析結果の取扱い（格納、ロック解除等）は次に、セキュア領域外で実施できる。

【 0 1 7 8 】

アッセイユニットが、対応する認証データを例えばアッセイユニットのメモリモジュール内に備えた予め認証されたアッセイユニットである場合、対応する認証データはリーダユニットを介して評価ユニットにより自動で取り出される S 2 1。認証データを使用して、暗号化されたデータの認証された分析結果に対応する部分が復号化され S 2 2、ユーザに提供される S 2 3。ここでシステムは状態 B にある。

【 0 1 7 9 】

ここで、ユーザがさらなる保護されロックされた分析データにアクセスしたい場合、又はアッセイユニットが事前の認証なしで分配された場合、ユーザは所望の分析結果を選択し S 3 1、例えば製造業者から必要なアクセス手段を購入する S 3 2。アクセス手段を受け取ると、新たに認証されたデータは復号化 / ロック解除され S 3 3、対応する分析結果はユーザに提供される S 3 4。

【 0 1 8 0 】

アッセイユニット 1 1、リーダユニット 3 1、及び評価ユニット 5 1 を有する本発明の診断システム 1 の別の有利な実施形態を図 6 に示す。システムは、検査モジュール 1 2 及びセンサモジュール 3 2 の両方がアッセイユニット 1 1 の一部であり、一体型モジュール 1 4 の形態で実現される点で図 1 のシステムとは異なる。検査生データ 7 3 は、データ接続 1 9 を介して追加データ 7 2 と一緒にリーダユニット 3 1 に提供される。

【 0 1 8 1 】

一体型検査及びセンサモジュール 1 4 を図 7 に概略的に示す。これは、診断検査素子及び得た信号を測定するセンサ素子が完全に統合された分析デバイスの典型的なケースである。

【 0 1 8 2 】

リーダユニット 3 1 の改竄防止保護モジュール 4 1 では、検査生データ 7 3 はデータ処理ユニット 3 4 により分析結果データ 7 4 へと処理される。次に、当該分析データ 7 4 は暗号化モジュール 3 3 に提供され、暗号化モジュール 3 3 で分析データ 7 4 は暗号化によりロックされ、メモリモジュール 4 0 に格納される。その後、評価ユニットは、メモリモジュール 4 0 から保護モジュール 4 1 の出力インタフェース 4 2 を介して暗号化されたデータ 7 7 及び普通テキストデータ 7 8 を読み取ることができる。メモリモジュール 4 0 は、暗号化モジュール 3 3 及び評価ユニットの動作を分離できるという利点を提供する。メモリモジュールは例えば、暗号化モジュールがデータ 7 7、7 8 を格納する不揮発性フラ

10

20

30

40

50

ッシュメモリとして実現されてもよい。次に、評価ユニットは先の任意の時点で当該データにアクセスできる。したがって、リーダユニットは、まだ評価ユニットに動作可能に接続されていないなくてもアッセイユニットのデータを読み取って暗号化でき、さらにはいくつかの異なるアッセイユニットの結果を読み取り、ロックし、格納することもできる。次いで、評価ユニットは、メモリモジュール40からデータ77、78をダウンロードするのに十分な短時間、リーダユニットに接続されさえすればよい。

【0183】

リーダユニットと評価ユニットとの直接ライブデータ通信を確立する代わりに、メモリモジュール40を、SDカード、USBメモリスティック等の取り外し可能に取り付けられるフラッシュメモリデバイスの形態で実現することもまた可能である。メモリデバイス40にデータを書き込んだ後、メモリデバイス40はユーザによりリーダユニットから取り外され、その後データを読み取る評価デバイスに接続される。しかし、それでもなお、このようなアプローチは本発明ではデータ接続37である。データ保護を確実にするために、このような実施形態では、例えば暗号化されていない分析結果等のデータは、保護モジュール内に留まるべきメモリに一切格納すべきではない。

10

【0184】

アッセイユニット11及びリーダユニット31が単一の一体型診断デバイスとして実現される診断システムの別の有利な変形例を図8に示す。一体型検査/センサモジュール14は試料15に診断検査を実施し、検査生データ73を保護モジュール41の暗号化モジュール33に提供し、暗号化モジュール33はデータを暗号化する。普通テキストデータ78と同様に暗号化されたデータ77を暗号化モジュール33のメモリモジュール35に一時的に格納できる。ロックされたデータ77及びさらなるデータ78は出力インタフェース42を介して評価ユニット51から要求され得る。

20

【0185】

図示される実施形態は、より複雑なアッセイユニットに特に有利であり、リーダユニット部分の電子要素33、35、36の追加コストは製造費用全体に対して重要ではない。

【0186】

単一のデバイスに組み合わされるリーダユニット31及び評価ユニット51を有する本発明の診断システム1の別の変形例を図9に示す。図示される実施形態は、小型独立デバイスとして特に有利である。

30

【0187】

示されるアッセイユニット11は、図6に示したものと同一のものである。リーダユニット及び評価ユニットの要素並びにリーダユニット及び評価ユニットの関係は、先に論じられた実施形態に類似している。図9の単一のデバイスは、セキュア領域5とユーザ領域3の両方を備え、セキュア領域、すなわち、改竄防止保護モジュール41内に存在する任意のデータは、保護モジュール41の内部出力インタフェース42のリーダユニット31により提供される場合を除いて、外部5からアクセス可能ではない。

【0188】

ここまで示した実施形態では、1つの評価ユニットが、それ自体が1つのアッセイユニットに動作可能に接続されている1つのリーダユニットに動作可能に接続されていた。しかし、本発明は他の組み合わせもさらに包含する。例えば、診断システムは、図10(a)に概略的に示すように1つの共通の評価ユニット51に動作可能に接続された2つ以上のリーダユニット31、31'を備えてもよい。このような実施形態により、診断システムの容易で費用効率の高いグレードアップを可能とする。さらに、追加の評価ユニットの必要なしに異なる種類のリーダユニットを例えば、特定の種類のアッセイユニットの種類のために使用することが可能である。

40

【0189】

同様に、例えば、図10(b)に示されるような同時に2つ以上のアッセイユニット11、11'と動作可能に接続する手段を有するリーダユニット31を提供することが可能である。したがって、このようなリーダユニットは2つ以上のアッセイユニットの並列動

50

作又は読み出しを可能にし、このことによりスループットを増加させる。或いは、リーダユニットは異なる種類のアクセユニット用の接続手段を備えてもよい。

【0190】

本発明の診断システム1の特に有利な変形例を図11に概略的に示す。本発明の診断システムにおいて使用するためのリーダユニット31の図示される例示的实施形態は、アクセユニットを取り外し可能に取り付けることができる第1のスロットをケーシングの側壁に備える。加えて、認証ユニットを取り外し可能に挿入できる第2のスロットはカバーに設けられる。図11では、アクセユニット11は第1のスロットに挿入された状態で示されており、スマートカードの形態の認証ユニットは第2のスロットに挿入されている。2つの追加の消耗アクセユニット11'が後に使用するために準備されている。

10

【0191】

リーダユニット31はデータ接続37(例えば、USB接続又はWLAN接続)を介して評価ユニット51に接続される。所与の例における評価ユニット51は、評価ユニットの機能を遂行するために、適切なプログラムを実施できる標準コンピュータデバイス、すなわち、ディスプレイ及びキーボードを有するデスクトップコンピュータである。

【0192】

認証ユニットの機能のための異なるアプローチがさらに上で論じられている。認証スマートカード100は例えば、特定の診断検査に割り当てられたクレジットユニットの量に応じて当該検査の結果にアクセスすることを可能にするクレジットユニットを含んでもよい。或いは、認証スマートカード100は、ユーザが特定の事前に認証された検査結果にアクセスすることを可能にする認証データを含んでもよい。リーダユニットと接続する代わりに、認証手段はさらに、評価ユニットと接続されてもよい。

20

【0193】

評価ユニット51は、一般的な通信ネットワーク104に接続される105。用語「通信ネットワーク」は、専用のワイヤに基づくか又は無線リンクを介したインターネット、モバイルネットワーク、VPN接続等のセキュアチャネル等である、ある場所から他の場所へのデータ通信を可能にする任意のリンクを含むと理解されなければならない。通信ネットワークへのリンクは例えば、電話回線、DSL又はケーブルモデム、セルラーリンク、無線リンク、イーサネット等により実現してもよい。

【0194】

遠隔認証サーバ110もまた、通信ネットワーク104に接続される105'。遠隔認証サーバの機能は上でさらに論じられている。例えば、評価デバイス51は、評価ユニットの認証レベルに応じて、復号化されたロック鍵又はその一部を受け取るために暗号化されたロック鍵を認証サーバ110に伝達できる。

30

【0195】

通信ネットワーク104に接続された遠隔支払い承認サーバ115により、ユーザ又はユーザの評価ユニットはそれぞれ、認証手段を購入することができる。次いで、このような認証手段(クレジットユニット、認証データ等)により、ユーザはさらなる分析結果にアクセスできる。

【0196】

遠隔アクセスデバイス102及び遠隔記憶サーバ103もまた、遠隔操作で分析結果にアクセスするか又は分析結果を格納するために、評価デバイス51と通信できる。

40

【0197】

遠隔認証サーバ110、遠隔支払い承認サーバ115、遠隔アクセスデバイス102、及び遠隔記憶サーバ103は、2つ以上の評価ユニットと共に動作できる。図11では、第2の概略的评价ユニット51'はネットワーク104に接続され、異なるユーザの制御下にあってもよい。

【0198】

分析結果を選択し、購入し、見るための例示的グラフィカルユーザインタフェース(GUI)を図12に示す。このようなGUIは、評価ユニットとして機能するコンピュータ

50

デバイス、又は専用の評価ユニットのディスプレイ、又はさらには遠隔アクセスデバイス上で実行されるソフトウェアにより実現され得る。

【0199】

インタフェースは、さまざまな種類の分析結果（例えば、小分子、タンパク質、DNA、細胞、ウイルス、細菌）を特定する項目を含んでもよい。ユーザは、多数のロックされた分析結果を測定してデータベースにインポートするために、さまざまな仕様及び分析能力を有する種々のアッセイをリーダユニットに挿入できる。

【0200】

次に、ユーザは購入するか又は見るために1つ又は複数の分析結果を選択してもよい。例えば、ユーザはチェックボックス又はその他のアプローチを使用して分析結果を選択できる。塗りつぶされたチェックボックスは、アクセス認証が事前に購入されたか又はアクセスがアッセイユニットとバンドルされて提供される分析結果に対応してもよい。チェックマークは、購入するために選択した分析結果に対応できる。場合により利用可能な分析結果は例えば、適用パネル（例えば、心臓マーカ、ウイルス、炎症マーカ）としてグループ分けできる。

10

【0201】

あるグループのチェックボックスがチェックされるか又は塗りつぶされると、チェックマーク状態は背景となる分析結果すべてにも反映され得る。個々の分析結果は、適用パネルを広げ、対応するチェックボックス（「C反応性タンパク質」参照）をチェックすることによってアクセスでき、選択できる。このような下位選択は、ダッシュ付き適用パネル

20

チェックボックスとして表示できる（「炎症マーカ」参照）。

【0202】

データベースで、又はアッセイユニット能力から利用可能ではない適用パネル及び分析結果は無効であると表示され得る（グレー表示）（「薬物スクリーニング」参照）。

【0203】

ユーザは「戻る」矢印を選択して前のインタフェースに戻ってもよい。「注文」矢印により注文インタフェースに進むことができる。

【0204】

図示された実施形態では、インタフェースは特定の分析結果を強調できる。これらの分析結果は背景となる健康状態を示すことができる。例えば、分析物の濃度が健康な基準範囲外にあり得るため、「心臓マーカ」及び「血液」がこのように強調して示される。これら分析物の異常な濃度は、背景となる健康状態又は疾患を示すことができる。例えば、トロポニンTの濃度が健康な基準範囲を上回り得るため、心臓マーカの「トロポニンT」が強調して示され、患者が心臓傷害を受けている可能性があることを示す。

30

【0205】

このようなシステムは、複数の分析物を迅速にスキャンし、患者の健康全般を検査し、潜在的な健康上の問題を特定するのに特に有用であり得る。システムは、ユーザに異なる異常な診断結果も警告できる。ユーザは、これらの強調された分析結果を購入するか又は見るかを決定できる。

【0206】

図13及び図14は、分析結果の購入を確認するための例示的インタフェースの概略図である。ユーザは電子発注書を使用して選択した分析結果を購入でき、クレジットユニットは、リーダユニット又は評価ユニットのユーザクレジット残高から、又はアッセイユニットにバンドルされたクレジットユニットから、又はユーザインボイス情報にアクセスし、遠隔支払いサーバと通信することによりもたらされ得る。

40

【0207】

図13は、ユーザクレジット残高が選択した分析結果へのアクセス権を購入するのに十分である状態を記す。確認インタフェースが現れてもよく、所与の例では、先に図12で示すようなメニュー上にポップアップウィンドウが配置され、ユーザにユーザの現在のユーザクレジット残高、選択した分析結果のクレジットユニットでの価格を知らせ、ユーザ

50

は分析結果の購入を確定又はキャンセルしてもよい。

【0208】

図14は、ユーザクレジット残高が選択した分析結果を購入するのに十分でない場合を記す。ポップアップウィンドウの形態の確認インタフェースは、ユーザにユーザの現在のユーザクレジット残高、選択した分析結果のクレジットでの価格、及びユーザの課金情報を使用した課金額について知らせる。次に、ユーザは対応するボタンを押すことによって、分析結果の購入を確定又はキャンセルできる。

【0209】

図15は、購入した分析結果を表示する例示的インタフェースの概略図である。この例では、購入した適用パネル及びその背景となる分析結果のみが表示される。加えて、この
10
ようなインタフェースに組み込むことができる多くの他の結果、例えば、他のユーザとの比較結果、又はまだ購入されていないか若しくは利用できない分析結果等もあり得る。適用パネルにアクセスして、個々の分析結果を表示してもよい。基準濃度範囲及び分析物濃度等の情報を表示でき、追加情報にアクセスできる。塗りつぶされた適用パネルのチェックボックスは、対応する分析結果がすべて購入されたことを示すことができる。ダッシュ付きの適用パネルのチェックボックスは、対応する分析結果の一部だけが購入されたことを示すことができる。

【0210】

図16は、分析結果データのデータベース及び分析結果を遡って選択するか、購入するか、又は見る機能の例示的インタフェースの概略図である。分析結果は評価ユニット又は
20
遠隔記憶サーバでローカルに格納され得る。ディスプレイは、チップ（アッセイユニット）情報（例えば、チップ証明書、チップ仕様、チップロット番号、チップにバンドルされた分析結果等）、診断検査情報（例えば、検査日、検査時間等）、ユーザ情報（例えば、ユーザ証明書、ユーザ名等）、及びセンサ情報（例えば、分析パネル、センサ生データ、センサ分析結果等）等のいくつかの基準に従ってまとめることができる結果データのデータベースを示すことができる。

【0211】

ユーザは、縦列名等の種々の基準により、又は検索フィルタ項目を使用して分析検査データを分類できる。検査データは、分析結果をさらに見るか又は購入するか選択できる。検査終了時に分析結果が購入もされず見もされなかった場合でも、各検査についての検査
30
データが格納され得る。したがって、ユーザは、いつでも前の検査の検査データを選択でき、分析結果を遡って購入又は見てもよい。

【0212】

図17は、本発明の診断システムにより分析結果を保護し、購入し、見る手順を説明するフローチャートである。分析結果は、上で説明したように測定され、ロックされ、リー
ダユニット、評価ユニット、又はアッセイユニットに格納されている。

【0213】

ユーザは、購入するか又は見るために分析結果を選択してもよいS41。リーダユニット又は評価は、例えば、レジストリを読み込むことにより分析結果が以前に購入されたか
40
確認できるS42。

【0214】

購入されていれば、リーダユニット又は評価ユニットは見るための分析結果をユーザに提供できるS49。

【0215】

購入されていなければ、リーダユニット又は評価ユニットは、分析結果がアッセイユニット仕様から利用可能であるかどうか、すなわち、アッセイユニット、例えば、診断チップが分析物を検出する能力を有するかどうかを判断できるS43。

【0216】

分析結果がアッセイユニット仕様から利用可能でなければ、ユーザは選択した分析結果
50
を取得可能な別の種類のアッセイユニットを使用するように促され得るS45。次に、プ

プロセスは再びステップ S 4 1 から開始され得る。

【 0 2 1 7 】

分析結果がアッセイユニット仕様から利用可能であれば、リーダユニット又は評価ユニットは、選択した分析結果が、アッセイユニットから予め使用可能である分析結果、したがって、認証手段がアッセイユニットとバンドルされて提供された結果に含まれているかを判断できる S 4 4。

【 0 2 1 8 】

選択した分析結果がアッセイユニットから予め使用可能な分析結果に含まれていれば、分析結果を見るためにユーザに提供できる、 S 4 9。

【 0 2 1 9 】

選択した分析結果がアッセイユニットから予め使用可能な分析結果に含まれていなければ、リーダユニット又は評価ユニットは分析結果の価格を確認できる、 S 4 6。このことは、価格のローカルデータベースを使用するか、又は遠隔サーバを価格のデータベースに接続することにより行うことができる。リーダユニット又は評価ユニットは、ユーザクレジット残高が選択した分析結果を購入するのに十分であることを確認できる S 4 7。

【 0 2 2 0 】

ユーザクレジット残高が選択した分析結果を購入するのに十分であれば、ユーザクレジット残高を減らすことができ S 4 8、分析結果をユーザに提供できる、 S 4 9。

【 0 2 2 1 】

ユーザクレジット残高が選択した分析結果を購入するのに十分でなければ、リーダユニット又は評価ユニットはユーザインボイス情報を処理することができ S 4 9、選択した分析結果をユーザに提供することができる、 S 4 9。

【 0 2 2 2 】

図 1 8 は、分析結果データを遠隔記憶サーバに転送する手順を説明するフローチャートである。ロックされた分析結果データ及びさらなるデータは、上で示したように、リーダユニット、評価ユニット、又は診断チップに格納できる S 5 1。

【 0 2 2 3 】

システムは次に、遠隔サーバへの接続が利用可能であることを確認する S 5 2。

【 0 2 2 4 】

遠隔サーバへの接続が利用可能であれば、データを遠隔サーバデータベースに転送できる S 5 3。データはチップ情報、ユーザ情報、及びセンサ情報等の情報を含んでいてもよい。

【 0 2 2 5 】

遠隔サーバへの接続が利用可能でなければ、リーダユニットが接続要求を処理できる S 5 4。接続確立後、データを標準セキュア通信プロトコルを使用してサーバに転送できる。

【 0 2 2 6 】

図 1 9 は、遠隔記憶サーバのデータベースに格納される分析結果を購入するか又は見る手順を説明するフローチャートである。リーダユニット又は評価ユニットは遠隔記憶サーバに接続され得る S 6 1。次に、ユーザは購入するか又は見るために分析結果を選択してもよい S 6 2。サーバは、選択した分析結果が以前に購入されたか確認できる S 6 3。

【 0 2 2 7 】

選択した分析結果が以前に購入されていれば、分析結果をリーダユニット又は評価ユニットに転送でき S 6 4、分析結果をユーザに提供できる S 6 5。

【 0 2 2 8 】

選択した分析結果が以前に購入されていなければ、サーバは分析結果の価格を確認できる S 6 6。次に、サーバはユーザクレジット残高が選択した分析結果を購入するのに十分かを確認できる S 6 7。

【 0 2 2 9 】

ユーザクレジット残高が選択した分析結果を購入するのに十分であれば、ユーザクレジ

10

20

30

40

50

ット残高をそれに従って減らすことができるS 6 8。ユーザクレジット残高が選択した分析結果を購入するのに十分でなければ、ユーザインボイス情報を処理できる、S 6 9。分析結果はその後、リーダユニット又は評価ユニットに転送されS 6 4、ユーザに提供できるS 6 5。

【0230】

上記フローチャートのステップの順序を変更してもセキュアな分析結果を購入し見ることができることが、当業者には容易に明らかであろう。したがって、検査データ及び分析結果を選択し、転送し、購入し、見る手順の順序の変更は本発明の範囲内である。

【0231】

本発明は本明細書に記載される特定の実施形態に範囲が限定されない。実際に、本明細書に記載されているものに加えて、本発明の種々の変形が前述の記述及び添付の図面から当業者に明らかになるであろう。したがって、このような変形は添付の特許請求の範囲に含まれることが意図される。加えて、種々の引用文献が本明細書で引用されており、当該引用文献の開示はそれぞれ、その全文が参照することにより本明細書に組み込まれる。

10

【符号の説明】

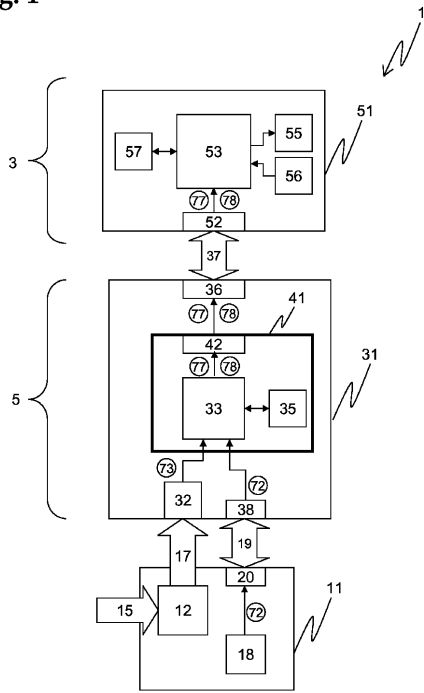
【0232】

1	診断システム	
3	ユーザ、ユーザ領域	
5	セキュア領域	
7	診断デバイス	20
11、11'	アクセイユニット	
12	検査モジュール	
12.1、12.2、...	単一の診断検査の検査素子	
13	診断検査	
14	一体型検査及びセンサモジュール	
15	生理学的試料	
17	診断検査信号	
17.1、17.2、...	単一の診断検査の検査信号	
18	メモリモジュール	
19	データ接続	30
20	データインタフェース	
25	データ媒体	
31	リーダユニット	
32	センサモジュール	
32.1、32.2、...	センサ素子	
33	暗号化モジュール	
34	データ処理モジュール	
35	メモリモジュール	
36	第1のデータインタフェース	
37	データ接続	40
38	第2のデータインタフェース	
39	メモリモジュール	
40	メモリモジュール	
41	保護モジュール	
42	出力インタフェース	
51、51'	評価ユニット	
52	データインタフェース	
53	データ処理モジュール、プロセッサ	
55	データ出力モジュール	
56	データ入力モジュール	50

5 7	メモリモジュール	
7 2	追加データ	
7 3	検査生データ、分析結果の完全なデータセット	
7 3 . 1、7 3 . 2、. . .	単一の診断検査の生データ	
7 3 a	認証された検査生データ、分析結果の完全なデータセットの認証されたサブセット	
7 4	分析結果データ、分析結果全体、分析結果の完全なデータセット	
7 4 a	認証された分析結果、分析結果の完全なデータセットの認証されたサブセット	
7 5	ロック鍵データ	
7 5 . 1、7 5 . 2、. . .	ロック鍵	10
7 7	暗号化されたデータ、分析結果の暗号化された完全なデータセット	
7 7 . 1、7 7 . 2、. . .	暗号化されたデータのサブセット	
7 7 a	アクセス可能な暗号化されたデータ	
7 8	さらなるデータ	
7 9	認証鍵データ	
7 9 . 1、7 9 . 2、. . .	認証鍵	
8 0、8 0 '	復号化されたデータ	
8 0 . 1、8 0 . 2、. . .	復号化されたデータのサブセット	
8 2	第 2 レベル鍵データ	
8 2 . 1、8 2 . 2、. . .	第 2 レベル鍵	20
8 4	暗号化されたロック鍵データ	
8 6	プライバシー鍵データ	
1 0 0	認証ユニット	
1 0 2	遠隔アクセスデバイス	
1 0 3	遠隔記憶サーバ	
1 0 5、1 0 5 '	通信ネットワークへの接続	
1 0 4	通信ネットワーク	
1 1 0	遠隔認証サーバ	
1 1 5	支払い承認サーバ	

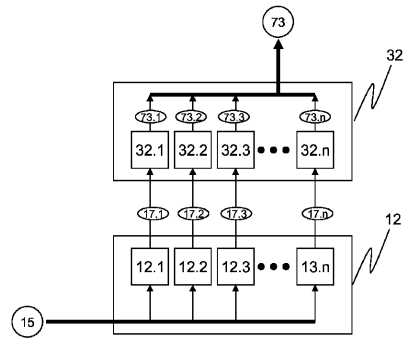
【 図 1 】

Fig. 1



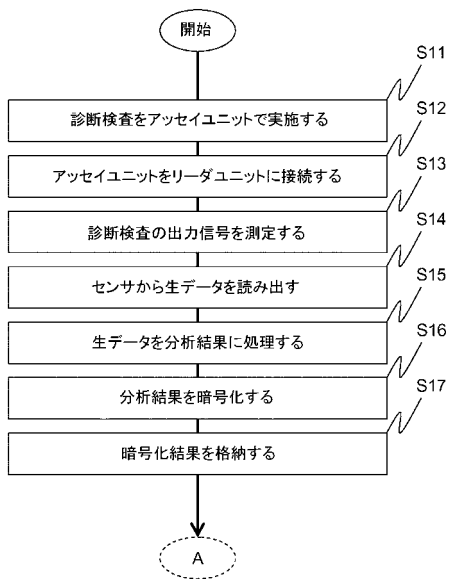
【 図 2 】

Fig. 2



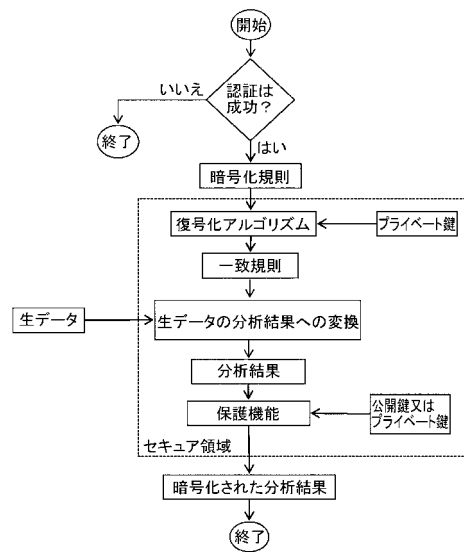
【 図 3 】

Fig. 3



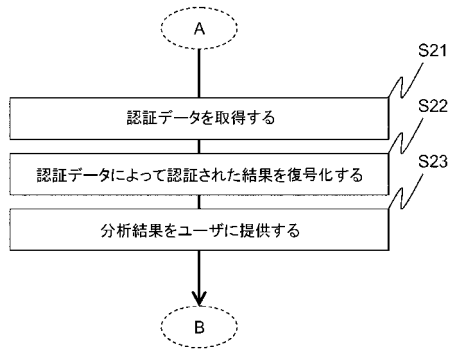
【 図 3 A 】

Fig. 3A



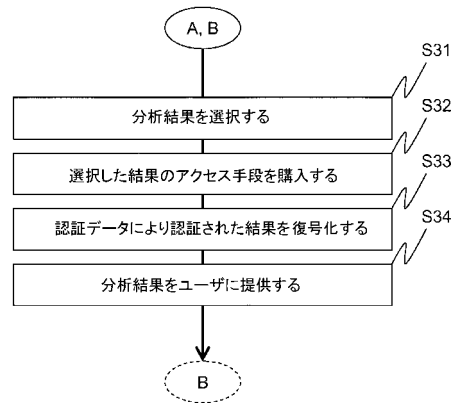
【 図 4 】

Fig. 4



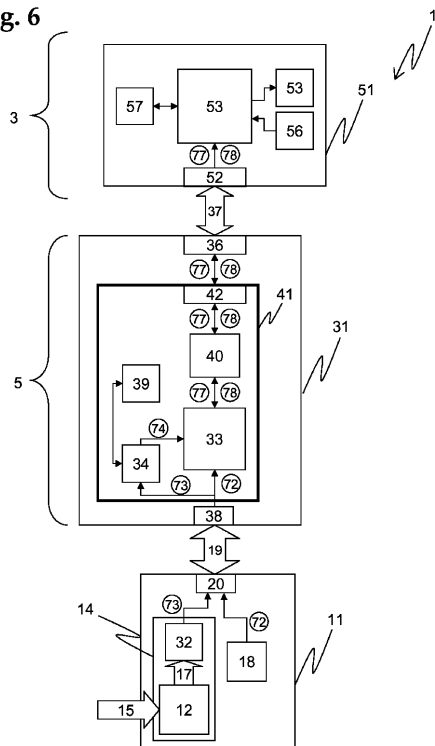
【 図 5 】

Fig. 5



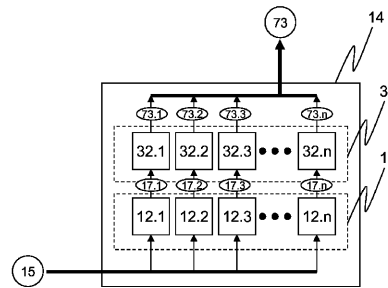
【 図 6 】

Fig. 6



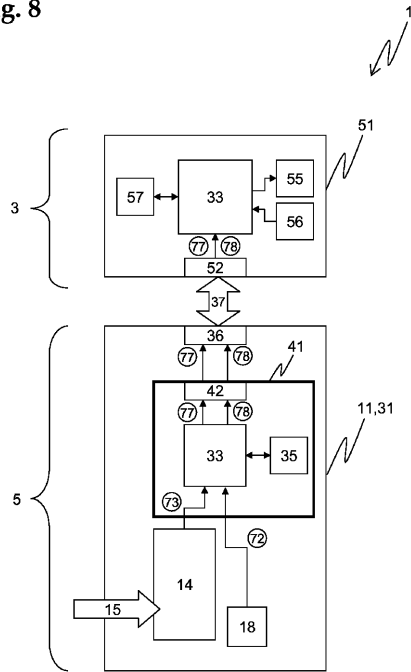
【 図 7 】

Fig. 7



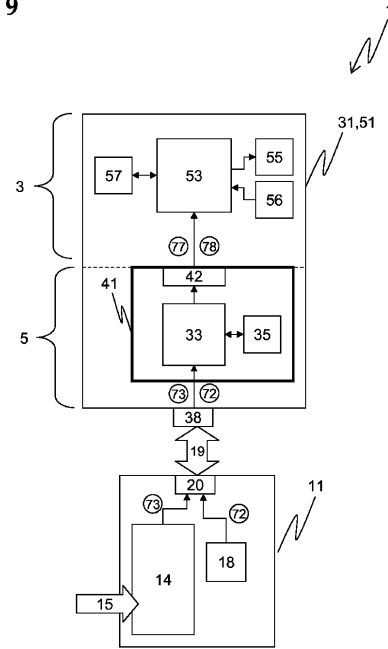
【 図 8 】

Fig. 8



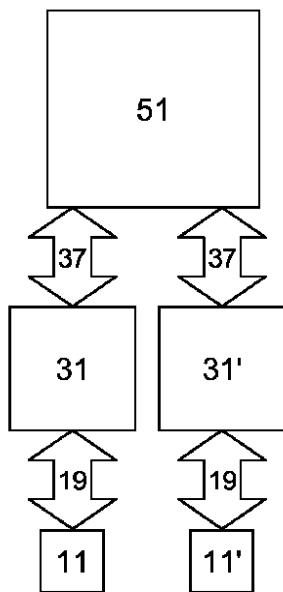
【 図 9 】

Fig. 9



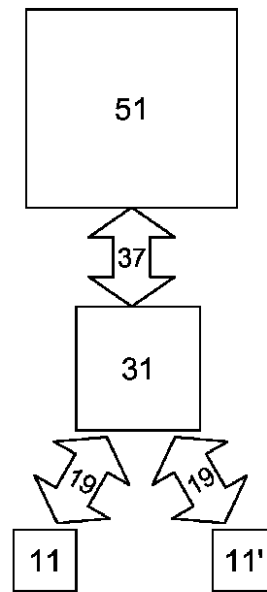
【 図 10 (a) 】

(a)



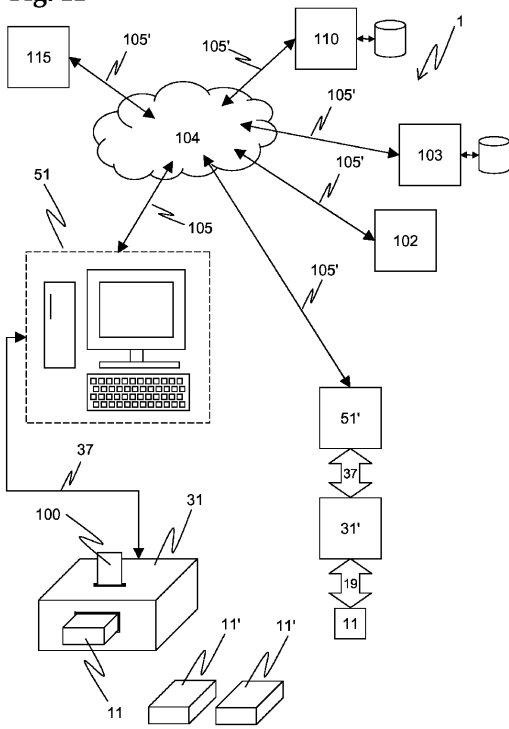
【 図 10 (b) 】

(b)



【 図 1 1 】

Fig. 11



【 図 1 2 】

Fig. 12

戻る	注文する
心臓マーカー	<input checked="" type="checkbox"/>
トロポニンT	<input checked="" type="checkbox"/>
ミオグロビン	<input checked="" type="checkbox"/>
CK-MB	<input checked="" type="checkbox"/>
BNP	<input checked="" type="checkbox"/>
Dダイマー	<input checked="" type="checkbox"/>
性感染症	<input type="checkbox"/>
電解質及び化学物質	<input checked="" type="checkbox"/>
薬物スクリーニング	<input type="checkbox"/>
ウイルス	<input checked="" type="checkbox"/>
血液	<input checked="" type="checkbox"/>
炎症マーカー	<input type="checkbox"/>
インターロイキン-6(IL-6)	<input type="checkbox"/>
C反応性タンパク質(CRP)	<input checked="" type="checkbox"/>
プロカルシトニン(PCT)	<input type="checkbox"/>
急性期血清アミロイドA	<input type="checkbox"/>

【 図 1 3 】

Fig. 13

戻る	注文する
心臓マーカー	<input checked="" type="checkbox"/>
トロポニンT	<input checked="" type="checkbox"/>
ミオグロビン	<input checked="" type="checkbox"/>
CK-MB	<input checked="" type="checkbox"/>
BNP	<input checked="" type="checkbox"/>
Dダイマー	<input checked="" type="checkbox"/>
性感染症	<input type="checkbox"/>
電解質及	<input checked="" type="checkbox"/>
薬物スク	<input type="checkbox"/>
ウイルス	<input checked="" type="checkbox"/>
血液	<input checked="" type="checkbox"/>
炎症マーカー	<input type="checkbox"/>
インターロイキン-6(IL-6)	<input type="checkbox"/>
C反応性タンパク質(CRP)	<input checked="" type="checkbox"/>
プロカルシトニン(PCT)	<input type="checkbox"/>
急性期血清アミロイドA	<input type="checkbox"/>

あなたのクレジット残高は
300クレジットです

選択した分析結果を
67クレジットで購入したいか
ご確認ください

キャンセル OK

【 図 1 4 】

Fig. 14

戻る	注文する
心臓マーカー	<input checked="" type="checkbox"/>
トロポニンT	<input checked="" type="checkbox"/>
ミオグロビン	<input checked="" type="checkbox"/>
CK-MB	<input checked="" type="checkbox"/>
BNP	<input checked="" type="checkbox"/>
Dダイマー	<input checked="" type="checkbox"/>
性感染症	<input type="checkbox"/>
電解質及	<input checked="" type="checkbox"/>
薬物スク	<input type="checkbox"/>
ウイルス	<input checked="" type="checkbox"/>
血液	<input checked="" type="checkbox"/>
炎症マーカー	<input type="checkbox"/>
インターロイキン-6(IL-6)	<input type="checkbox"/>
C反応性タンパク質(CRP)	<input checked="" type="checkbox"/>
プロカルシトニン(PCT)	<input type="checkbox"/>
急性期血清アミロイドA	<input type="checkbox"/>

あなたのクレジット残高は
50クレジットです

選択した分析結果を
67クレジットで購入したいか
ご確認ください

追加の17クレジットのために
あなたの課金情報が
使用されることを
ご確認ください

キャンセル OK

【 図 1 5 】

Fig. 15

← 戻る		注文する →	
心臓マーカー			
トロポニンT		0.15 ng/mL	
ミオグロビン		50 ng/mL	
CK-MB		1.8 ng/mL	
NT-proBNP		45 pg/mL	
Dダイマー		300 ng/mL	
電解質及び化学物質			
ナトリウム		325 mg/dL	
カリウム		18 mg/dL	
尿素		12 mg/dL	
クレアチニン		0.9 mg/dL	
グルコース		80 mg/dL	
pH		7.38	
ウイルス			
血液			
炎症マーカー			
CRP		2 μg/ml	

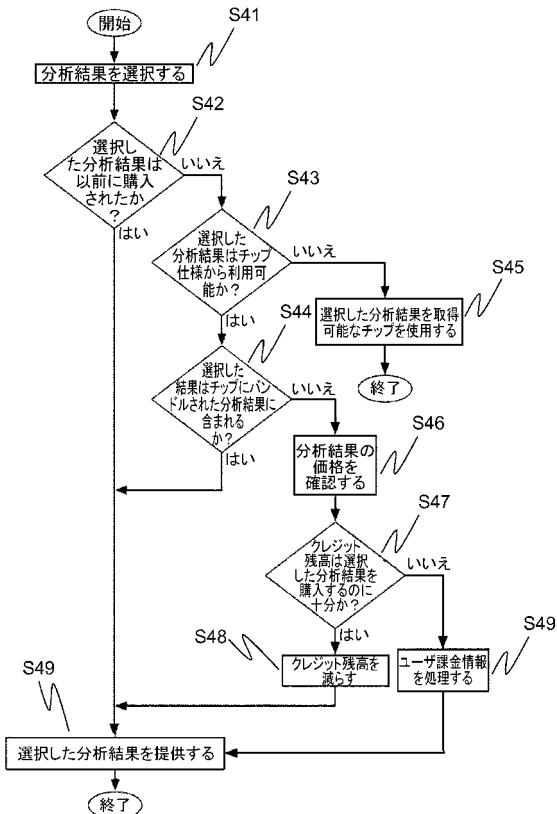
【 図 1 6 】

Fig. 16

検査データのデータベース			
ID	チップ仕様	検査日	ユーザ名
15...	パネル 1	2012/2/2, 20:02	Barbara Mi
15...	パネル 1	2012/2/3, 8:45	Barbara Mi
15...	パネル 1	2012/2/3, 13:15	Barbara Mi
15...	パネル 1	2012/2/3, 19:57	Barbara Mi
15...	パネル 1	2012/2/17, 13:07	Barbara Mi
15...	パネル 1	2012/5/9, 21:14	Barbara Mi
15...	パネル 1	2012/10/1, 10:20	Barbara Mi
58...	パネル 2	2012/1/29, 9:23	Barbara Mi
58...	パネル 2	2012/2/3, 13:28	Barbara Mi
58...	パネル 2	2012/8/13, 15:43	Barbara Mi
23...	パネル 3	2012/1/29, 15:30	Barbara Mi
23...	パネル 3	2012/2/3, 13:00	Barbara Mi
31...	パネル 3	2012/12/10, 23:48	Barbara Mi

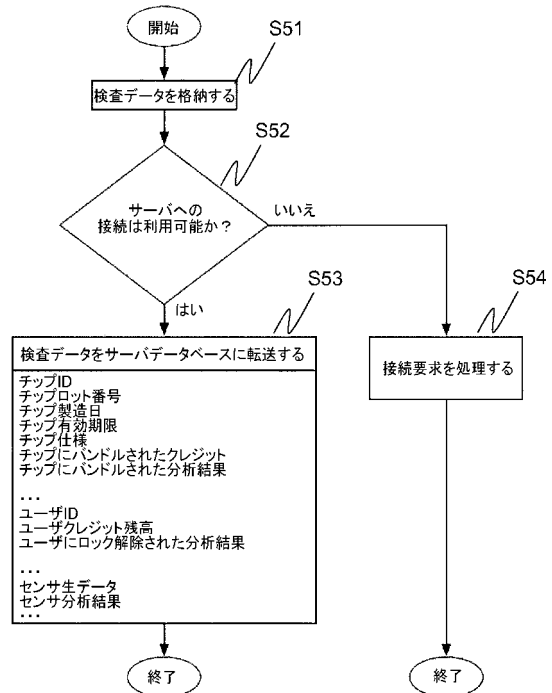
【 図 1 7 】

Fig. 17



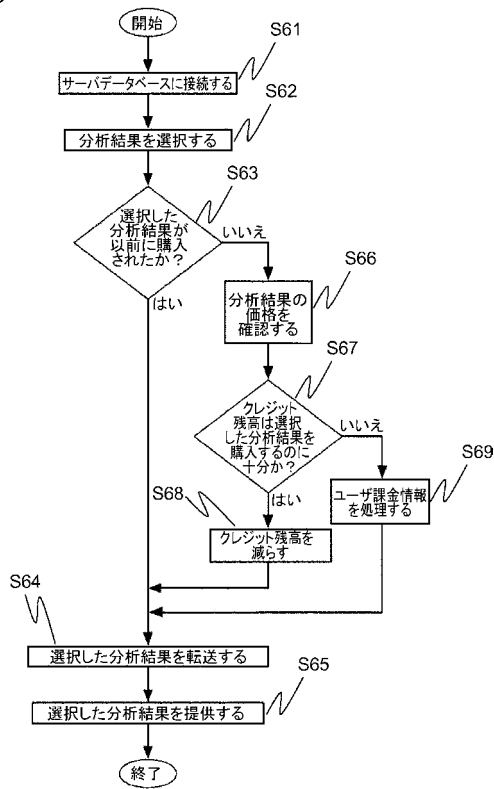
【 図 1 8 】

Fig. 18



【 図 19 】

Fig. 19



【 国際調査報告 】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/EP2014/072156**Box No. II Observations where certain claims were found unsearchable (Continuation of Item 2 of first sheet)**

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:
2. Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:
3. Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of Item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1. As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. As all searchable claims could be searched without effort justifying an additional fees, this Authority did not invite payment of additional fees.
3. As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:
4. No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

- The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.
- The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.
- No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International application No

PCT/EP2014/072156

A. CLASSIFICATION OF SUBJECT MATTER INV. G06F21/62 ADD.		
According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED		
Minimum documentation searched (classification system followed by classification symbols) G06F G01N A61B		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) EPO-Internal, WPI Data		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2012/029303 A1 (SHAYA FAWZI [US]) 2 February 2012 (2012-02-02)	1-7
Y	paragraphs [0007], [0021] - [0034], [0057] - [0061] figure 1	8-18
X	US 7 039 810 B1 (NICHOLS TIMOTHY J [US]) 2 May 2006 (2006-05-02) abstract column 14, line 40 - column 16, line 4 column 16, line 56 - column 18, line 4 column 12, lines 17-34	1-7
Y	WO 02/01271 A1 (KONINKL PHILIPS ELECTRONICS NV [NL]) 3 January 2002 (2002-01-03) the whole document	8-18
	----- -/--	
<input checked="" type="checkbox"/> Further documents are listed in the continuation of Box C. <input checked="" type="checkbox"/> See patent family annex.		
* Special categories of cited documents : *A* document defining the general state of the art which is not considered to be of particular relevance *E* earlier application or patent but published on or after the international filing date *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) *O* document referring to an oral disclosure, use, exhibition or other means *P* document published prior to the international filing date but later than the priority date claimed *T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention *X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone *Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art *Z* document member of the same patent family		
Date of the actual completion of the international search 6 February 2015		Date of mailing of the international search report 13/02/2015
Name and mailing address of the ISA/ European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016		Authorized officer Segura, Gustavo

2

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No

PCT/EP2014/072156

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2005/065890 A1 (BENALOH JOSH D [US]) 24 March 2005 (2005-03-24) paragraphs [0002], [0003] paragraphs [0057] - [0074] -----	8-18
X	US 7 162 451 B2 (BERGER STEFAN [US] ET AL) 9 January 2007 (2007-01-09) column 3, line 10 - line 16 column 6, line 33 - line 46 figures 1,3 -----	8-18

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2014/072156

Patent document cited in search report	Publication date	Patent family member(s)	Publication date	
US 2012029303	A1	02-02-2012	US 2012029303 A1 WO 2012015543 A2	02-02-2012 02-02-2012
US 7039810	B1	02-05-2006	DE 10053894 A1 FR 2800481 A1 JP 4795523 B2 JP 2001217823 A US 7039810 B1	28-06-2001 04-05-2001 19-10-2011 10-08-2001 02-05-2006
WO 0201271	A1	03-01-2002	CN 1471661 A EP 1374009 A2 JP 2004502379 A WO 0201271 A1	28-01-2004 02-01-2004 22-01-2004 03-01-2002
US 2005065890	A1	24-03-2005	US 6886098 B1 US 2005065888 A1 US 2005065889 A1 US 2005065890 A1 US 2005094813 A1 US 2005097062 A1 US 2005097063 A1 US 2005117746 A1 US 2005193210 A1	26-04-2005 24-03-2005 24-03-2005 24-03-2005 05-05-2005 05-05-2005 05-05-2005 02-06-2005 01-09-2005
US 7162451	B2	09-01-2007	AT 484038 T AU 2002312437 A1 CA 2465553 A1 CN 1596521 A EP 1461892 A1 IL 161655 A JP 2005512208 A KR 20040058181 A TW I268078 B US 2003105719 A1 WO 03049359 A1	15-10-2010 17-06-2003 12-06-2003 16-03-2005 29-09-2004 04-05-2009 28-04-2005 03-07-2004 01-12-2006 05-06-2003 12-06-2003

International Application No. PCT/ EP2014/ 072156

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. claims: 1-18

inventions 1.1 and 1.2

1.1. claims: 1-7

securing the data protection module of the reader unit

1.2. claims: 8-18

flexible access to the encrypted data set

フロントページの続き

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

(72)発明者 ジャーヴェイス, ラック
スイス, シーエイチ 2000 ヌーシャテル, ルー ド ラ マラディエール 71シー,
ワン ドロップ ダイアグノスティクス エスエーアールエル

(72)発明者 ジーグラ, ヨルグ
スイス, シーエイチ 2540 グレンヘン, リングシュトラッセ 6
Fターム(参考) 5J104 AA12 NA02 NA37