

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第5246602号
(P5246602)

(45) 発行日 平成25年7月24日(2013.7.24)

(24) 登録日 平成25年4月19日(2013.4.19)

(51) Int. Cl.		F I	
GO 1 R	29/08 (2006.01)	GO 1 R	29/08 Z
GO 1 R	29/10 (2006.01)	GO 1 R	29/08 D
GO 6 K	17/00 (2006.01)	GO 1 R	29/10 E
HO 4 B	5/02 (2006.01)	GO 6 K	17/00 B
		GO 6 K	17/00 F

請求項の数 7 (全 11 頁) 最終頁に続く

(21) 出願番号	特願2009-545408 (P2009-545408)	(73) 特許権者	000004237
(86) (22) 出願日	平成20年12月9日(2008.12.9)		日本電気株式会社
(86) 国際出願番号	PCT/JP2008/072325		東京都港区芝五丁目7番1号
(87) 国際公開番号	W02009/075262	(74) 代理人	100130029
(87) 国際公開日	平成21年6月18日(2009.6.18)		弁理士 永井 道雄
審査請求日	平成23年9月7日(2011.9.7)	(74) 代理人	100166338
(31) 優先権主張番号	特願2007-319686 (P2007-319686)		弁理士 関口 正夫
(32) 優先日	平成19年12月11日(2007.12.11)	(74) 代理人	100152054
(33) 優先権主張国	日本国(JP)		弁理士 仲野 孝雅
		(72) 発明者	久門 亨
			日本国東京都港区芝五丁目7番1号 日本電気株式会社内
		(72) 発明者	山下 哲孝
			日本国東京都港区芝五丁目7番1号 日本電気株式会社内

最終頁に続く

(54) 【発明の名称】 電磁波測定方法及び装置

(57) 【特許請求の範囲】

【請求項1】

通信機器と非接触で通信を行う被測定機器から発生する漏洩電磁波を測定する電磁波測定装置であって、

前記被測定機器の漏洩磁界発生部からの漏洩電磁波を受信するアンテナ部と、

前記通信機器と前記被測定機器の漏洩磁界発生部とが重ならないように位置調整を行い、且つ、前記アンテナ部が前記被測定機器の漏洩磁界発生部と重なるように位置調整を行う位置調整部と、

前記被測定機器が処理を実行していることを検出する検出部と、

前記検出部からの信号に基づき前記アンテナ部の受信信号から漏洩電磁波を測定する測定部と、

を備えた電磁波測定装置。

【請求項2】

前記位置調整部は、前記被測定機器、前記通信機器及び前記アンテナ部をそれぞれ独立に位置調整することを特徴とする請求項1に記載の電磁波測定装置。

【請求項3】

前記検出部は、前記通信機器と前記被測定機器との通信を制御する制御装置からの通信を観測し、前記制御装置からの通信を指示する信号に基づいて前記被測定機器の処理の実行を検出することを特徴とする請求項1又は2に記載の電磁波測定装置。

【請求項4】

10

20

前記検出部は、前記通信機器と前記被測定機器との通信を示す信号に基づき前記被測定機器の処理の実行を検出することを特徴とする請求項 1 又は 2 に記載の電磁波測定装置。

【請求項 5】

前記検出部は、前記通信機器と前記被測定機器との通信用電磁波の強度変化に基づいて前記被測定機器の処理の実行を検出することを特徴とする請求項 1 又は 2 に記載の電磁波測定装置。

【請求項 6】

前記検出部は、前記位置調整部に前記被測定機器が設置されたことを検出することによって前記被測定機器の処理の実行を検出することを特徴とする請求項 1 又は 2 に記載の電磁波測定装置。

10

【請求項 7】

通信機器と非接触で通信を行う被測定機器から発生する漏洩電磁波を測定する電磁波測定方法であって、

前記通信機器と前記被測定機器の漏洩磁界発生部とが重ならないように位置調整を行い、
前記被測定機器の漏洩磁界発生部からの漏洩電磁波を受信するアンテナ部が前記被測定機器の漏洩磁界発生部と重なるように位置調整を行い、

前記被測定機器が処理を実行していることを検出し、

検出された信号に基づき前記アンテナ部からの受信信号から漏洩電磁波を測定する電磁波測定方法。

20

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、電磁波を測定する電磁波測定方法及び装置、特に、非接触型 IC カード等の被測定機器の処理過程で発生する漏洩電磁波を測定するのに好適な電磁波測定方法及び装置に関するものである。

【背景技術】

30

【0002】

一般に、電子機器はその動作の過程において電磁波を発生する。この電磁波は無線通信等を目的として意図的に発生する電磁波とは異なり、非意図的に漏洩する電磁波であり、この漏洩電磁波を解析することによって処理中の情報を解析可能であることが知られている。

【0003】

非特許文献 1 には、これを応用して暗号機能付きの接触型 IC カード又は携帯端末等の暗号を実装した装置において、暗号処理中に装置から発生する漏洩電磁波を測定することで秘密情報を解析する方法が記載されている。

【0004】

40

電磁波解析では、暗号装置内の CPU 又は LSI 等において実行する処理命令やオペランドにより変化する電流変化に依存して発生する電磁波を 1 回もしくは複数の入出力の異なる処理に対して測定解析することで、暗号アルゴリズム、処理タイミング、及び秘密鍵等の推定が可能である。

【0005】

通常、接触型 IC カード又はその他の暗号を実装した暗号モジュールに対する電磁波解析では、暗号が実装される CPU 又は LSI 等のデバイス上に電磁波プローブをかざすことで、対象のデバイスから漏洩する電磁波を測定している。

【非特許文献 1】Karine Gandolfi, Christophe Mourtel, and Francis Olivier, "Electromagnet IC Analysis: Concrete Results," In the Proceedings of the Works

50

hop on Cryptograph I C Hardware and Embedded Systems 2001 (CHES 2001), LNCS 2162 Paris, France, May 2001, pp 251-261.

【発明の開示】

【発明が解決しようとする課題】

【0006】

リーダライタと被接触ICカードとの通信時もしくは被接触ICカードへの電力供給時には電磁波が用いられ、非接触型ICカードの漏洩電磁波を測定する際にはその時の被接触ICカードからの漏洩磁界を測定する。このため、解析対象であるICカード上に搭載されているICチップから漏洩する電磁波を測定する際にリーダライタとの通信に利用される電磁波も同時に測定してしまい、解析対象である被接触ICカード上のICチップから漏洩する電磁波を正確に測定することは困難である。また、漏洩電磁波を測定する場合には、非接触型ICカード上での暗号処理動作等のタイミングを把握することが困難であった。

10

【0007】

本発明の典型的な目的は、被測定機器の通信に利用される電磁波の影響を軽減でき、測定対象から漏洩する電磁波を正確に測定することが可能な電磁波測定方法及び装置を提供することにある。

【課題を解決するための手段】

【0008】

本発明の典型的な電磁測定装置は、通信機器と非接触で通信を行う被測定機器から発生する漏洩電磁波を測定する電磁波測定装置であって、前記被測定機器の漏洩磁界発生部からの漏洩電磁波を受信するアンテナ部と、前記通信機器と前記被測定機器の漏洩磁界発生部とが重ならないように位置調整を行い、且つ、前記アンテナ部が前記被測定機器の漏洩磁界発生部と重なるように位置調整を行う位置調整手段と、前記被測定機器が処理を実行していることを検出する検出手段と、前記検出手段からの信号に基づき前記アンテナ部の受信信号から漏洩電磁波を測定する測定手段とを備える。

20

【0009】

また、本発明の典型的な電磁測定方法は、通信機器と非接触で通信を行う被測定機器から発生する漏洩電磁波を測定する電磁波測定方法であって、

前記通信機器と前記被測定機器の漏洩磁界発生部とが重ならないように位置調整を行い

30

、前記被測定機器の漏洩磁界発生部からの漏洩電磁波を受信するアンテナ部が前記被測定機器の漏洩磁界発生部と重なるように位置調整を行い、

前記被測定機器が処理を実行していることを検出し、

検出された信号に基づき前記アンテナ部からの受信信号から漏洩電磁波を測定する電磁波測定方法である。

【0010】

本願は、2007年12月11日に出願された特願2007-319686号に基づき、優先権の利益を主張するものである。そして、特願2007-319686号の内容は本願の明細書の内容に含まれる。

40

【発明の効果】

【0011】

本発明によれば、被測定機器からの漏洩電磁波を測定する際に被測定機器とアンテナの位置調整等、通常の通信に用いられる電磁波を測定しないように位置調整を行うことにより、被測定機器からの漏洩電磁気を正確に検出することができる。また、被測定機器の処理状態を通信機器の動作や測定波形の変動等から判断することにより好ましいタイミングで電磁波を測定することができる。

【図面の簡単な説明】

【0012】

【図1】本発明に係る電磁波測定装置の第1の実施形態を示すブロック図である。

50

【図 2】図 1 の実施形態の電磁波測定部の構成を示す斜視図である。

【図 3】本発明による第 2 の実施形態の電磁波測定部の構成を示す斜視図である。

【図 4】本発明に係る電磁波測定装置の第 3 の実施形態を示すブロック図である。

【図 5】本発明に係る電磁波測定装置の第 4 の実施形態を示すブロック図である。

【図 6】本発明に係る電磁波測定方法を示すフローチャートである。

【図 7】本発明に係る電磁波測定装置の第 5 の実施形態を示すブロック図である。

【符号の説明】

【 0 0 1 3 】

1 0	電磁波測定部	
1 1	位置調整部	10
1 2	アンテナ部	
1 3	非接触型 I C カード	
1 4	I C カードリーダライタ	
1 5	I C チップ	
2 0	トリガ生成部	
2 1	通信用電磁波	
2 2	漏洩電磁波	
3 0	測定器	
4 0	P C	
4 1	U S B ケーブル	20
1 1 2	アンテナ位置調整部	
1 1 3	非接触型 I C カード位置調整部	
1 1 4	I C カードリーダライタ位置調整部	
1 1 5	非接触型 I C カード固定部	

【発明を実施するための最良の形態】

【 0 0 1 4 】

次に、本発明を実施するための典型的な実施形態 (exemplary embodiment) について、図面を参照して詳細に説明する。

【 0 0 1 5 】

(第 1 の実施形態)

図 1 は本発明に係る電磁波測定装置の第 1 の実施形態を示すブロック図である。電磁波測定装置は、電磁波測定部 1 0、トリガ生成部 2 0、測定器 3 0 を備えている。

【 0 0 1 6 】

非接触型 I C カード 1 3 は漏洩電磁波を測定する測定対象の被測定機器である。I C カードリーダライタ 1 4 は非接触型 I C カード 1 3 と非接触で通信を行う通信機器である。

【 0 0 1 7 】

本実施形態では、非接触型 I C カード 1 3 と I C カードリーダライタ 1 4 間で非接触で通信を行う際に非接触型 I C カード 1 3 の電磁波発生部 (I C チップ) から漏洩する漏洩電磁波を測定する例を説明する。

【 0 0 1 8 】

電磁波測定部 1 0 は、位置調整部 1 1、アンテナ部 1 2 を備えている。非接触型 I C カード 1 3、I C カードリーダライタ 1 4 は、電磁波測定時に電磁波測定部 1 0 内に挿入して固定され、電磁波測定後に取り出しが可能となっている。図 1 では、電磁波測定時に非接触型 I C カード 1 3、I C カードリーダライタ 1 4 が挿入された状態の構成を示している。位置調整部 1 1 は、詳しく後述するように非接触型 I C カード 1 3、アンテナ部 1 2、I C カードリーダライタ 1 4 の位置調整を行う。図 1 では電磁波測定部 1 0 内に非接触型 I C カード 1 3 と I C カードリーダライタ 1 4 が納められているが、これら非接触型 I C カード 1 3 と I C カードリーダライタ 1 4 は測定対象である。

【 0 0 1 9 】

位置調整部 1 1 は、非接触型 I C カード 1 3 上に搭載されている I C チップから漏洩す

る電磁波を測定するためICチップの真上もしくは真下等の近傍へとアンテナ部12の位置調整を行う。また、位置調整部11は、非接触型ICカード13とICカードリーダー14との通信が可能で、アンテナ部12で受信する非接触型ICカード13上のICチップからの漏洩電磁波に影響を与えないように非接触型ICカード13とICカードリーダー14との位置調整を行う。

【0020】

トリガ生成部20はICカードリーダー14の動作もしくは通信状態から非接触型ICカードのICチップにて処理が実行されていることを検出し、トリガ信号を生成する。このトリガ信号は測定器30に送信され、トリガ信号のタイミングで漏洩電磁波の測定を行う。

10

【0021】

測定器30はアンテナ部12の受信信号から非接触型ICカード上のICチップから漏洩する電磁波を測定し、測定データを格納し、測定データの表示等を行う。測定器30は例えば、オシロスコープやスペクトラムアナライザである。図示しない電磁波解析部では、測定器30で測定された漏洩電磁波に基づき、例えば、上記非特許文献1等に記載された電磁波解析方法を用いて電磁波解析を行う。

【0022】

図2は電磁波測定部10を立体的に示す斜視図である。位置調整部11は非接触型ICカード位置調整部113、アンテナ位置調整部112、ICカードリーダー位置調整部114から成っている。本実施形態では、非接触型ICカード位置調整部113は電磁波測定部10の上部に設置されている。アンテナ部12及びアンテナ位置調整部112は、非接触型ICカード13とICカードリーダー14との間に配置されている。

20

【0023】

非接触型ICカード位置調整部113は非接触型ICカード13をX、Y方向に移動させて位置調整を行う。アンテナ位置調整部112はアンテナ部12をX、Y、Z方向及び図中の矢印で示すアンテナ部12の軸回りの方向に回転させて位置調整を行う。ICカードリーダー位置調整部114はICカードリーダー14をX、Y、Z方向に移動させて位置調整を行う。

【0024】

ここで、図2に示すようにX方向は横方向、Y方向は縦方向、Z方向は高さ方向とする。また、アンテナ位置調整部112にはアンテナ部12の一端部が固定されており、図2に示すようにアンテナ部12はアンテナ位置調整部112によりその軸回りの方向に回転することが可能である。アンテナ部12をその軸回りの方向に回転させることで指向性を持たせている。

30

【0025】

本実施形態では、非接触型ICカード13は電磁波測定部10の上面に設置された非接触型ICカード位置調整部113により固定されている。非接触型ICカード位置調整部113は、非接触型ICカード13をX方向及びY方向(縦方向及び横方向)に位置調整する機能を有しており、非接触型ICカード13の位置を所望の位置に調整固定することが可能である。

40

【0026】

ICカードリーダー14は電磁波測定部10の床面に設置されたICカードリーダー位置調整部114により固定されている。ICカードリーダー位置調整部114は電磁波測定部10の床面上にてXYZ方向(縦横高さ方向)にICカードリーダー14を自由に調整する機能を有しており、ICカードリーダー14を所望の位置に調整固定することができる。

【0027】

アンテナ部12は電磁波測定部10の側面に設置されたアンテナ位置調整部112により固定されている。アンテナ位置調整部112は電磁波測定部10の側面にてアンテナ部12を自由に位置を調整可能である。即ち、アンテナ位置調整部112はアンテナ部12

50

をXYZ方向（横方向（奥行き方向）、縦方向、高さ方向）に調整する機能を有している。また、上述のようにアンテナ位置調整部112はアンテナ部12をその軸回りの方向に回転させる機能を有しており、アンテナ部12の位置と向きを自由に調整固定することができる。

【0028】

本実施形態では、非接触型ICカード13上のICチップ15からの漏洩電磁波22を測定する場合には、位置調整部11のICカードリーダライタ位置調整部114、非接触型ICカード位置調整部113、アンテナ位置調整部112を用いて手動又は自動で位置調整を行う。以下、図6のフローチャートを用いて電磁波測定方法について説明する。

【0029】

例えば、まず、ステップS11に示すように、ICカードリーダライタ位置調整部114を用いてICカードリーダライタ14を所定位置に固定する。次いで、非接触型ICカード位置調整部113を用いて非接触型ICカード13上のICチップ15がICカードリーダライタ14の上部と重ならないように非接触型ICカード13の位置調整を行う。その後、ステップS12に示すように、アンテナ位置調整部112を用いてICチップ15の真下にアンテナ部12が位置するように、即ち、図2に示すようにアンテナ部12と非接触型ICカード13のICチップ15とが重なり合うように位置調整を行う。

【0030】

ここで、自動で位置調整を行う場合には、ステップS11において、例えば、ICカードリーダライタ14の信号（ICカードリーダライタ14と非接触型ICカード13との通信を示す信号）を図示しない観測装置で観測しながら、非接触型ICカード13とICカードリーダライタ14との通信が確立する位置にICカードリーダライタ位置調整部114と非接触型ICカード位置調整部113でICカードリーダライタ14と非接触型ICカード13との位置調整を行う。

【0031】

その後、ステップS12において、アンテナ部12の信号を図示しない観測装置で観測しながら、アンテナ位置調整部112によりアンテナ部12の信号が最大となるようにアンテナ部12の位置調整を行う。なお、自動で位置調整を行う場合には、プログラム制御等を用いて各部の位置調整を制御する制御手段、或いは各位置調整部を駆動するモータ等の駆動手段等が必要である。

【0032】

位置調整が終了すると、ステップS13において、トリガ生成部20により非接触型ICカードのICチップ15で処理が実行されていることが検出され、トリガ信号が測定器30に送信される。ステップS14に示すように、測定部30はトリガ信号のタイミングで非接触型ICカード13のICチップ15からの漏洩電磁波の測定を行う。

【0033】

本実施形態では、このように非接触型ICカード13、ICカードリーダライタ14、及びアンテナ部12の位置調整を行うことで、通信用電磁波21の影響を極力抑えながらICチップ15からの漏洩電磁波22を正確に測定することが可能となる。また、非接触型ICカード13、ICカードリーダライタ14、アンテナ部12を自由に位置調整することができるため、ICチップ15の位置が異なる様々なICカードにも対応することができる。

【0034】

更に、ICカードリーダライタ14の動作もしくは通信状態から非接触型ICカード13のICチップ15にて処理が実行されていることを検出するため、非接触型ICカード13のICチップ15が動作する好ましいタイミングで漏洩電磁波を測定することが可能となる。

【0035】

（第2の実施形態）

図3は本発明の第2の実施形態を示す斜視図である。図3は図2と同様に電磁波測定部

10

20

30

40

50

10を立体的に示すものである。図3では図2と同一部分には同一符号を付している。装置構成は図1と同様である。図2との違いは非接触型ICカード位置調整部113を電磁波測定部10の内部に設置した点である。それに伴い、アンテナ部12及びアンテナ位置調整部112が非接触型ICカード13の上部に配置されている。それ以外の構成は図2の構成と同様である。

【0036】

非接触型ICカード位置調整部113、アンテナ位置調整部112、ICカードリーダライタ位置調整部114の各位置調整や漏洩磁界の測定は図2の説明と同様に行う。本実施形態では、図2と同様に通信用電磁波41の影響を極力抑えながらICチップ15からの漏洩電磁波42を測定することが可能となる。また、ICチップ15の位置が異なる様

10

【0037】

(第3の実施形態)

図4は本発明に係る電磁波測定装置の第3の実施形態を示すブロック図である。図4では図1と同一部分には同一符号を付している。図1との違いは制御装置となるPC(パーソナルコンピュータ)40が設けられており、ICカードリーダライタ14はPC40とUSBケーブル41により接続されている点である。PC40は非接触型ICカード13とICカードリーダライタ14との通信制御を行う。その他の構成や動作は図1の実施形態と同様である。

【0038】

トリガ生成部20はUSBケーブル41の通信状況を観測し、PC40からICカードリーダライタ14への非接触型ICカード13との通信開始コマンドが送信された場合には、測定器30に対して電磁波の測定と格納するためのトリガ信号を送信する。測定器30は、トリガ信号に基づき非接触型ICカード13上のICチップ15が動作するタイミングで漏洩電磁波を測定することができる。

20

【0039】

電磁波測定部10としては図2或いは図3の構成が採用され、位置調整部11の構成も図2或いは図3の説明と同様である。本実施形態ではPC40からの通信開始コマンドに基づいてトリガ信号を作成するため、ICチップ15からの漏洩電磁波を正確に測定することが可能となる。

30

【0040】

(第4の実施形態)

図5は本発明の第4の実施形態を示すブロック図である。図5では図1と同一部分には同一符号を付している。図1或いは図4との違いは、トリガ生成部20がアンテナ部12にて受信した電磁波波形をもとにトリガ信号を生成する点である。その他の構成や動作は図1、図4と同様である。

【0041】

本実施形態では、トリガ生成部20はアンテナ部12の受信信号から非接触型ICカード13とICカードリーダライタ14との通信もしくは電力供給に用いられる電磁波を測定部30を介して検出する。その際、ICカードリーダライタ14と非接触型ICカード13間の電磁波は、両者の通信が実施されている時と実施されていない時で通信用電磁波21の強度が異なる。

40

【0042】

この強度の違いを利用し、トリガ生成部20にてアンテナ部12の受信信号レベルが大きくなった時点を非接触型ICカード13の動作状態と判断し、トリガ信号を生成する。そのため、非接触型ICカード13上のICチップ15が動作するタイミングにて漏洩電磁波22を測定することができる。

【0043】

ここで、上述のようにICカードリーダライタ14と非接触型ICカード13上のICチップ15とは重ならないように位置調整を行っているが、アンテナ部12にてICカー

50

ドリーダライタ 14 と非接触型 IC カード 13 間の微弱な通信用電磁波 21 が受信され、そのアンテナ部 12 で受信された通信用電磁波の強度の違いに基づいてトリガ信号を生成する。

【0044】

電磁波測定部 10 は図 2 或いは図 3 の構成とし、位置調整部 11 の構成も図 2 或いは図 3 の説明と同様である。本実施形態では、IC カードリーダライタ 14 と非接触型 IC カード 13 間の通信用電磁波 21 の強度が異なることを利用してトリガ信号を生成するため同様に IC チップ 15 が動作するタイミングで漏洩電磁波 22 を測定することができる。

【0045】

(第 5 の実施形態)

図 7 は本発明の第 5 の実施形態を示すブロック図である。図 7 では図 1 と同一部分には同一符号を付している。図 7 に示す構成が図 1 に示す構成と異なるのは、電磁波測定部と測定器 30 とトリガ生成部 20 とが筐体内に設けられて 1 台の電磁波測定装置 50 として構成されている点である。

【0046】

なお、本発明は、上記実施形態に限定されるものではなく、本発明の要旨の範囲内において種々の変形や変更が可能である。例えば、図 4 では PC 40 と IC カードリーダライタ 14 とを USB ケーブル 41 を用いて接続しているが、観測可能なものであればどのようなものを用いても良い。また、IC カードリーダライタ 14 の制御についても PC に限らず同様の制御可能な装置を用いても構わない。

【0047】

更に、非接触型 IC カード位置調整部 113 内に非接触型 IC カード 13 が設置されたことを検知する機能を有することにより、非接触型 IC カード 13 上の IC チップ 15 が処理を実行していることを検出し、漏洩電磁波の測定のためのトリガ信号とすることもできる。

【0048】

また、本発明の電磁波測定装置は、ハードウェア、ソフトウェア又はこれらの組み合わせにより実現することができる。

【0049】

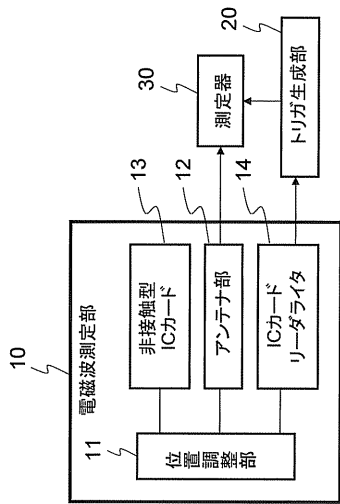
以上、本発明の代表的な実施形態について説明したが、本発明は、本願の請求の範囲によって規定される、その精神または主要な特徴から逸脱することなく、他の種々の形で実施することができる。そのため、前述した各実施形態は単なる例示にすぎず、限定的に解釈されるべきではない。本発明の範囲は特許請求の範囲によって示すものであって、明細書や要約書の記載には拘束されない。さらに、特許請求の範囲の均等範囲に属する変形や変更はすべて本発明の範囲内のものである。

10

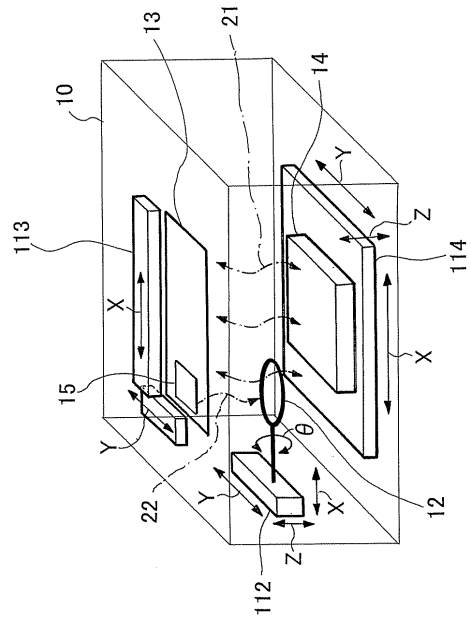
20

30

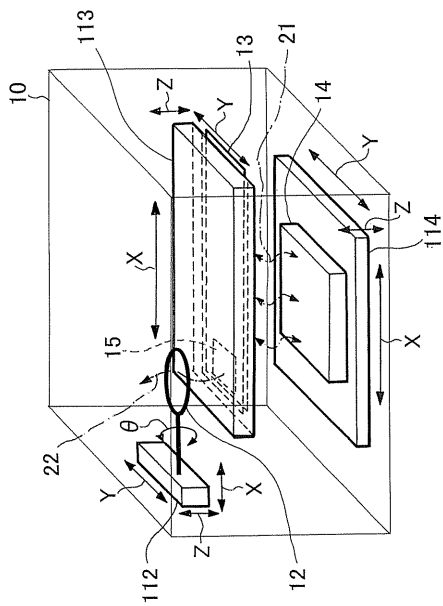
【図1】



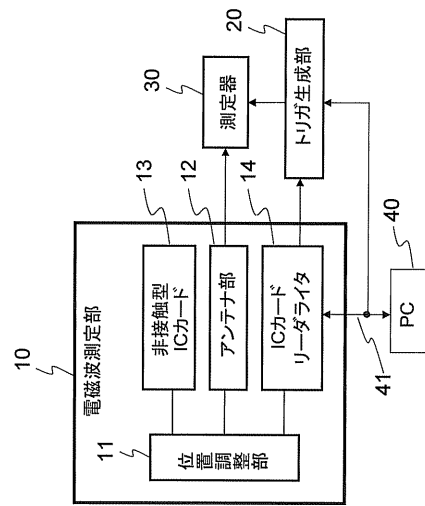
【図2】



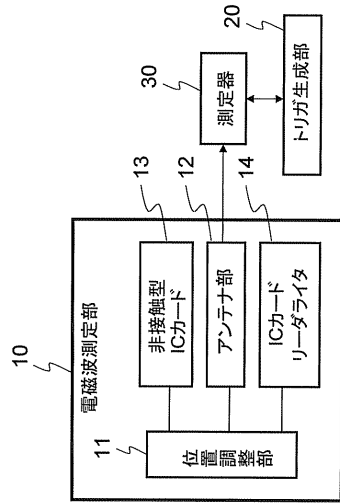
【図3】



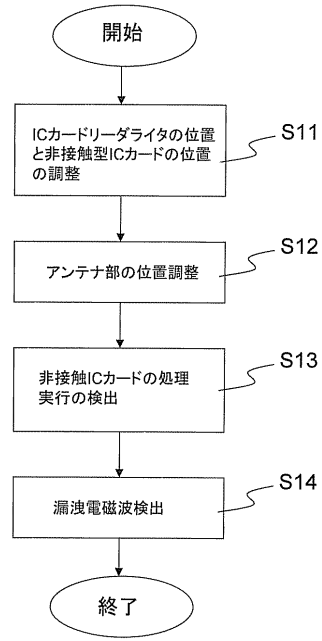
【図4】



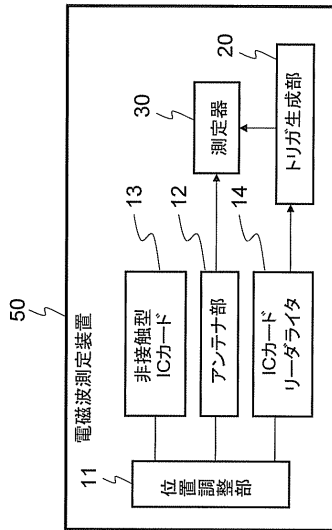
【図5】



【図6】



【図7】



フロントページの続き

(51)Int.Cl.

F I

H 0 4 B 5/02

審査官 吉田 久

(56)参考文献 特開2003-270279(JP,A)
特開2005-121403(JP,A)
特開2002-7969(JP,A)
特開2005-33413(JP,A)
特開2001-24425(JP,A)
特開2000-242746(JP,A)
特開2006-184264(JP,A)
特開2006-18563(JP,A)

(58)調査した分野(Int.Cl., DB名)

G 0 1 R 29/08、29/10
G 0 6 K 17/00、
19/00~19/18
H 0 4 B 5/02