(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2008-33594
(P2008-33594A)
(43)公開日　平成20年2月14日(2008.2.14)

(51)Int.Cl.		F I		テーマコード（参考）
G06K 17/00	(2006.01)	G06K 17/00	F	5B011
G06F 21/06	(2006.01)	G06F 12/14	560E	5B017
G06F 1/26	(2006.01)	G06F 1/00	335C	5B018
G06F 12/16	(2006.01)	G06F 12/16	340M	5B058
		G06K 17/00	E	

審査請求 未請求　請求項の数 7　ＯＬ　（全 23 頁）　最終頁に続く

(21)出願番号　特願2006-205714 (P2006-205714)
(22)出願日　平成18年7月28日 (2006.7.28)

(71)出願人　000002185
ソニー株式会社
東京都港区港南１丁目７番１号
(74)代理人　100082131
弁理士　稲本　義雄
(72)発明者　村岡　如竹
東京都品川区北品川６丁目７番３５号　ソニー株式会社内

Ｆターム(参考)　5B011 DA06　EA06　GG02　JB01
5B017 AA07　BB03　CA14
5B018 GA07　LA01　MA24　QA12
5B058 CA15　CA22　CA27　KA27　KA31

(54)【発明の名称】データ記憶装置、電力制御方法、並びに、通信装置

(57)【要約】
【課題】耐タンパ性を物理的に向上させる。
【解決手段】主電源１４がオフされている場合に、電池３５１が電池ソケット３５２から取り外されたとき、主電源１４または電池３５１によりコンデンサ３５５に蓄積されている電力が、タンパ監視回路１０５－１乃至１０５－６、電池電圧検知器３５８、および、記憶部１０３に供給される。電池電圧検知器３５８は、入力端子Ｔ１１への入力電圧が所定の閾値以下になった状態が所定の時間継続した場合、出力端子Ｔ１２からの出力電圧をHighからLowレベルに変化させ、スイッチ３５９をオフし、記憶部１０３への電力の供給を停止させる。これにより、記憶部１０３のRAMのデータが消去される。本発明は、リーダライタに適用できる。
【選択図】図１０

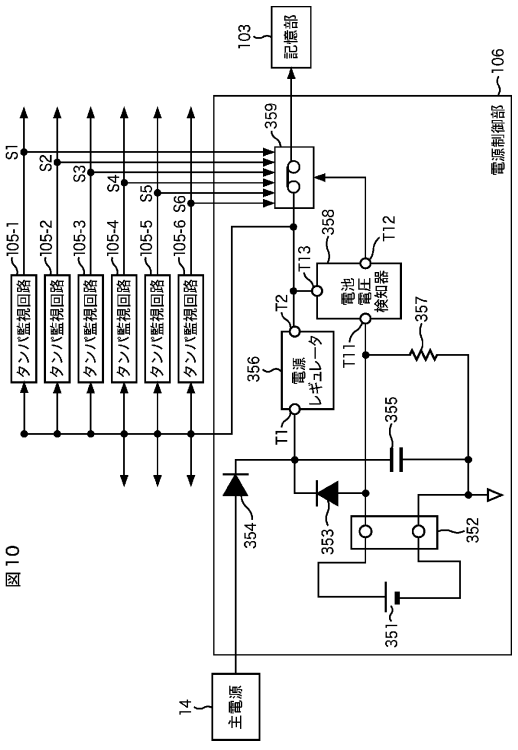


図10

【特許請求の範囲】
【請求項１】
メモリ、および、前記メモリに格納されているデータに対する不正行為を監視する監視手段を有するデータ記憶装置において、
前記監視手段に電力を供給する第１の電源と、
前記第１の電源から前記監視手段に電力が供給されている場合に充電され、前記第１の電源から前記監視手段への電力の供給が停止された場合、前記監視手段に電力を供給する蓄電手段と
を含むデータ記憶装置。
【請求項２】
前記メモリは、揮発性であり、
前記第１の電源は、さらに、前記メモリに電力を供給する
請求項１に記載のデータ記憶装置。
【請求項３】
前記蓄電手段は、さらに、前記第１の電源から前記メモリへの電力の供給が停止された場合、前記メモリに電力を供給し、
前記第１の電源から前記メモリへの電力の供給が停止されてから所定の時間が経過した場合、前記蓄電手段からの前記メモリへの電力の供給を停止させる電力供給制御手段を
さらに含む請求項２に記載のデータ記憶装置。
【請求項４】
前記第１の電源は、前記監視手段に電力を供給する第２の電源がオフされた場合に前記監視手段に電力を供給するバックアップ電源であり、
前記蓄電手段は、前記第１の電源または前記第２の電源により充電される
請求項１に記載のデータ記憶装置。
【請求項５】
前記第１の電源は電池であり、前記蓄電手段はコンデンサである
請求項１に記載のデータ記憶装置。
【請求項６】
メモリ、および、前記メモリに格納されているデータに対する不正行為を監視する監視手段を有するデータ記憶装置の電力制御方法において、
電源から前記監視手段に電力が供給されている場合に蓄電手段を充電し、
前記電源から前記監視手段への電力の供給が停止された場合、前記蓄電手段から前記監視手段に電力を供給する
電力制御方法。
【請求項７】
非接触ICカード機能を有する装置と通信を行う通信装置であって、前記非接触ICカード機能を有する装置から読み出したデータを格納するメモリ、および、前記メモリに格納されているデータに対する不正行為を監視する監視手段を有する通信装置において、
前記監視手段に電力を供給する電源と、
前記電源から前記監視手段に電力が供給されている場合に充電され、前記電源から前記監視手段への電力の供給が停止された場合、前記監視手段に電力を供給する蓄電手段と
を含む通信装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、データ記憶装置、電力制御方法、および、通信装置に関し、特に、耐タンパ性を物理的に向上させるようにしたデータ記憶装置、電力制御方法、および、通信装置に関する。
【背景技術】
【０００２】

近年、筐体の開放や破壊などのタンパ行為を監視する監視回路を設け、メモリに記憶されているデータを保護する装置が普及してきている（例えば、特許文献１参照）。

【０００３】

そのような装置においては、主電源がオフの状態においても、タンパ行為の監視が行われるように、監視回路用にバッテリなどのバックアップ電源が設けられる場合がある。

【０００４】

【特許文献１】特開２００５－５６４３９号公報

【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、監視回路用にバックアップ電源を設けた場合、バックアップ電源が取り外され、監視回路の動作を停止させられた上で、データの盗聴や改ざんが行われる恐れがある。

【０００６】

本発明は、このような状況に鑑みてなされたものであり、耐タンパ性を物理的に向上させるようにするものである。

【課題を解決するための手段】

【０００７】

本発明の第１の側面のデータ記憶装置は、メモリ、および、前記メモリに格納されているデータに対する不正行為を監視する監視手段を有するデータ記憶装置であって、前記監視手段に電力を供給する第１の電源と、前記第１の電源から前記監視手段に電力が供給されている場合に充電され、前記第１の電源から前記監視手段への電力の供給が停止された場合、前記監視手段に電力を供給する蓄電手段とが設けられている。

【０００８】

前記メモリは、揮発性であり、前記第１の電源には、さらに、前記メモリに電力を供給させるようにすることができる。

【０００９】

前記蓄電手段には、さらに、前記第１の電源から前記メモリへの電力の供給が停止された場合、前記メモリに電力を供給させ、前記第１の電源から前記メモリへの電力の供給が停止されてから所定の時間が経過した場合、前記蓄電手段からの前記メモリへの電力の供給を停止させる電力供給制御手段をさらに設けることができる。

【００１０】

前記第１の電源は、前記監視手段に電力を供給する第２の電源がオフされた場合に前記監視手段に電力を供給するバックアップ電源であり、前記蓄電手段は、前記第１の電源または前記第２の電源により充電されるようにすることができる。

【００１１】

前記第１の電源は電池であり、前記蓄電手段はコンデンサであるようにすることができる。

【００１２】

本発明の第１の電力制御方法は、メモリ、および、前記メモリに格納されているデータに対する不正行為を監視する監視手段を有するデータ記憶装置の電力制御方法であって、電源から前記監視手段に電力が供給されている場合に蓄電手段を充電し、前記電源から前記監視手段への電力の供給が停止された場合、前記蓄電手段から前記監視手段に電力を供給する。

【００１３】

本発明の第２の側面の通信装置は、非接触ICカード機能を有する装置と通信を行う通信装置であって、前記非接触ICカード機能を有する装置から読み出したデータを格納するメモリ、および、前記メモリに格納されているデータに対する不正行為を監視する監視手段を有する通信装置において、前記監視手段に電力を供給する電源と、前記電源から前記監視手段に電力が供給されている場合に充電され、前記電源から前記監視手段への電力の供

給が停止された場合、前記監視手段に電力を供給する蓄電手段とが設けられている。

【００１４】

本発明の第１の側面においては、電源から監視手段に電力が供給されている場合に蓄電手段が充電され、前記電源から前記監視手段への電力の供給が停止された場合、前記蓄電手段から前記監視手段に電力が供給される。

【００１５】

本発明の第２の側面においては、電源から監視手段に電力が供給されている場合に蓄電手段が充電され、前記電源から前記監視手段への電力の供給が停止された場合、前記蓄電手段から前記監視手段に電力が供給される。

【発明の効果】

【００１６】

本発明の第１の側面または第２の側面によれば、メモリに格納されているデータに対する不正行為を監視する監視手段に電力を供給することができる。また、本発明の第１の側面または第２の側面によれば、耐タンパ性を物理的に向上させることができる。

【発明を実施するための最良の形態】

【００１７】

以下に本発明の実施の形態を説明するが、本発明の構成要件と、明細書または図面に記載の実施の形態との対応関係を例示すると、次のようになる。この記載は、本発明をサポートする実施の形態が、発明の詳細な説明に記載されていることを確認するためのものである。従って、発明の詳細な説明中には記載されているが、本発明の構成要件に対応する実施の形態として、ここには記載されていない実施の形態があったとしても、そのことは、その実施の形態が、その構成要件に対応するものではないことを意味するものではない。逆に、実施の形態が構成要件に対応するものとしてここに記載されていたとしても、そのことは、その実施の形態が、その構成要件以外の構成要件には対応しないものであることを意味するものでもない。

【００１８】

本発明の第１の側面のデータ記憶装置（例えば、図１の制御モジュール１３）は、第１に、メモリ（例えば、図５のRAM１７１）、および、前記メモリに格納されているデータに対する不正行為を監視する監視手段（例えば、図５のタンパ監視回路１０５－１乃至１０５－６）を有するデータ記憶装置であって、前記監視手段に電力を供給する第１の電源（例えば、図１０の電池３５１）と、前記第１の電源から前記監視手段に電力が供給されている場合に充電され、前記第１の電源から前記監視手段への電力の供給が停止された場合、前記監視手段に電力を供給する蓄電手段（例えば、図１０のコンデンサ３５５）とを備える。

【００１９】

本発明の第１の側面のデータ記憶装置は、第２に、前記蓄電手段は、さらに、前記第１の電源から前記メモリへの電力の供給が停止された場合、前記メモリに電力を供給し、前記第１の電源から前記メモリへの電力の供給が停止されてから所定の時間が経過した場合、前記蓄電手段からの前記メモリへの電力の供給を停止させる電力供給制御手段（例えば、図１０の電池電圧検知器３５８）をさらに備える。

【００２０】

本発明の第２の側面のデータ記憶装置は、第３に、前記第１の電源は、前記監視手段に電力を供給する第２の電源（例えば、図１の主電源１４）がオフされた場合に前記監視手段に電力を供給するバックアップ電源であり、前記蓄電手段は、前記第１の電源または前記第２の電源により充電される。

【００２１】

本発明の第１の側面の電力制御方法は、メモリ（例えば、図５のRAM１７１）、および、前記メモリに格納されているデータに対する不正行為を監視する監視手段（例えば、図５のタンパ監視回路１０５－１乃至１０５－６）を有するデータ記憶装置（例えば、図１の制御モジュール１３）の電力制御方法において、電源（例えば、図１０の電池３５１）

から前記監視手段に電力が供給されている場合に蓄電手段（例えば、図１０のコンデンサ３５５）を充電し、前記電源から前記監視手段への電力の供給が停止された場合、前記蓄電手段から前記監視手段に電力を供給する。

【００２２】

本発明の第２の通信装置（例えば、図１のリーダライタ１）は、非接触ICカード機能を有する装置（例えば、図１のICカード２）と通信を行う通信装置であって、前記非接触ICカード機能を有する装置から読み出したデータを格納するメモリ（例えば、図５のRAM１７１）、および、前記メモリに格納されているデータに対する不正行為を監視する監視手段（例えば、図５のタンパ監視回路１０５－１乃至１０５－６）を有する通信装置において、前記監視手段に電力を供給する電源（例えば、図１０の電池３５１）と、前記電源から前記監視手段に電力が供給されている場合に充電され、前記電源から前記監視手段への電力の供給が停止された場合、前記監視手段に電力を供給する蓄電手段（例えば、図１０のコンデンサ３５５）とを備える。

【００２３】

以下、図を参照して、本発明の実施の形態について説明する。

【００２４】

図１は、本発明を適用したリーダライタの一実施の形態を示すブロック図である。本発明を適用したリーダライタ１は、アンテナ１１、RFドライブ基板１２、制御モジュール１３、および、主電源１４を含むように構成される。

【００２５】

RFドライブ基板１２は、アンテナ１１を介して、非接触式のICカード２との間で、単一の周波数の搬送波を使用した、電磁誘導による近接通信を行う。RFドライブ基板１２が使用する搬送波の周波数としては、例えば、ISM（Industrial Scientific Medical）バンドの13.56MHzなどを採用することができる。また、近接通信とは、通信する装置どうしの距離が、数10cm以内となって可能となる通信を意味し、通信する装置（の筐体）同士が接触して行う通信も含まれる。

【００２６】

制御モジュール１３は、ICカード２を利用したサービスを実現するための処理を実行し、適宜、サービスで使用されるデータを、アンテナ１１およびRFドライブ基板１２を介して、ICカード２に書き込んだり、ICカード２から読み出したりする。また、制御モジュール１３は、複数の種類のサービスの処理を並行して実行することが可能である。すなわち、例えば、電子マネーサービス、プリペイドカードサービス、各種の交通機関の乗車カードサービスなど、非接触式のICカードを利用した複数のサービスを、１台のリーダライタ１により提供することができる。

【００２７】

主電源１４は、RFドライブ基板１２および制御モジュール１３の動作に必要な電力を供給する。

【００２８】

図２は、制御モジュール１３の外観の構成の例を示す断面図である。

【００２９】

制御モジュール１３においては、直方体の筐体３１内に、メイン基板３２、および、保護基板３３乃至３６が設けられている。メイン基板３２は、筐体３１の高さ方向のほぼ中央付近に配置されている。保護基板３３乃至３６は、それぞれ、筐体３１の面３１Ａ乃至面３１Ｄの内面とほぼ同じ形状および面積の基板であり、筐体３１の面３１Ａ乃至面３１Ｄの内面に取り付けられている。また、図示されていないが、筐体３１の残りの２面にも、保護基板３３乃至３６と同様に、各面の内面とほぼ同じ形状および面積の保護基板が取り付けられている。すなわち、保護基板３３乃至３６および図示せぬ２枚の保護基板の合計６枚の保護基板が筐体３１の内面のほぼ全面を覆うように、かつ、メイン基板３２を囲むように配置されている。なお、図２においては、筐体１３の内面と各保護基板との間に所定の間隔が設けられているが、各保護基板を筐体３１内の内面に接するように配置する

ようにしてもよい。

【００３０】

メイン基板３２は、CPU（Central Processing Unit）１０１（図５）、RAM１７１（図５）などの制御モジュール１３の処理を行うための各部品が搭載されている。

【００３１】

６枚の保護基板は、図８などを参照して後述するように、メイン基板３２上に設けられているRAM１７１に格納されているデータに対して盗聴や改ざんなどの不正行為を行うために、筐体３１を開放したり、破壊するなどのタンパ行為を検出するために設けられている基板である。

【００３２】

図３および図４は、保護基板３３の構成の例を示している。図３は、図２においてメイン基板３２側となる保護基板３３の面３３Ａの構成の例を示し、図４は、図２において筐体３１側となる保護基板３３の面３３Ａの構成の例を示している。

【００３３】

保護基板３３の形状は、上述したように、筐体３１の面３１Ａの内面とほぼ同じ大きさおよび形状の長方形である。保護基板３３の面３３Ａのほぼ中央には、コネクタ４１Ｂが設けられている。また、面３３Ａのコネクタ４１Ｂ以外の部分において、面３３Ａの長さまたは幅に対して十分細い電線５１Ａが、面３３Ａの長さまたは幅に対して十分狭い間隔で、長さ方向が面３３Ａの縦方向とほぼ平行となり、面３３Ａのほぼ全面を覆うように配線されている。さらに、面３３Ｂにおいて、面３３Ｂの長さまたは幅に対して十分細い電線５１Ｂが、面３３Ｂの長さまたは幅に対して十分狭い間隔で、長さ方向が面３３Ａ電線５１Ａの長さ方向とほぼ直交する面３３Ｂの横方向とほぼ平行となり、面３３Ｂのほぼ全面を覆うように配線されている。また、電線５１Ａと電線５１Ｂとは、貫通ビア５２および５３により接続されることにより、１本の電線を構成している。すなわち、面３３Ａと面３３Ｂの両面を合わせて、保護基板３３のほぼ全面にほぼ格子状に１本の電線が配線されている。

【００３４】

なお、以下、適宜、電線５１Ａと電線５１Ｂとを合わせて、電線５１と称する。

【００３５】

図示および詳細な説明は省略するが、保護基板３３以外の他の５枚の保護基板についても、保護基板３３と同様に、各基板の両面を合わせて、各基板のほぼ全面にほぼ格子状に１本の電線が配線されている。すなわち、筐体３１の各面の長さまたは幅に対して十分細い電線が、筐体３１の各面の長さまたは幅に対して十分狭い間隔で筐体３１のほぼ全面を覆うように配線されている。従って、筐体３１に穴を開けるなどの破壊行為が行われた場合、筐体３１のほぼ全面を覆っている電線の一部がほぼ確実に断線される。

【００３６】

なお、各保護基板において、電線をできる限り細くし、隣接する電線の間隔をできる限り狭くするようにすることが望ましい。

【００３７】

図２に戻り、メイン基板３２と保護基板３３とは、コネクタ４１Ａおよび４１Ｂにより電気的に接続されており、メイン基板３２と保護基板３４とは、コネクタ４２Ａおよび４２Ｂにより電気的に接続されており、メイン基板３２と保護基板３５とは、コネクタ４３Ａおよび４３Ｂにより電気的に接続されており、メイン基板３２と保護基板３６とは、コネクタ４４Ａおよび４４Ｂにより電気的に接続されている。また、図示されていない２枚の保護基板についても、図示せぬコネクタを用いて、メイン基板３２と電気的に接続されている。すなわち、筐体３１の各面を開放しようとした場合、筐体３１の内面に取り付けられている保護基板とメイン基板３２とが電気的に切断されるようになされている。

【００３８】

なお、制御モジュール１３には、図示した以外にも、RFドライブ基板１２および主電源１４と電気的に接続するためのコネクタなどが設けられる。

【００３９】
図５は、図１の制御モジュール１３の機能的構成を示すブロック図である。制御モジュール１３は、CPU１０１、メモリアクセス制御部１０２、記憶部１０３、リセット回路１０４、タンパ監視回路１０５－１乃至１０５－６、および、電源制御部１０６を含むように構成される。また、メモリアクセス制御部１０２は、スイッチ１４１、スクランブル鍵変更指令器１４２、乱数出力器１４３、および、バススクランブル器１４４を含むように構成される。さらに、バススクランブル器１４４は、スクランブル鍵保持部１５１、および、アドレスバススクランブル回路１５２を含むように構成される。また、スクランブル鍵保持部１５１は、スクランブル鍵バッファ１６１、および、内部メモリ１６２を含むように構成される。さらに、記憶部１０３は、RAM（Random Access Memory）１７１および不揮発性メモリ１７２を含むように構成される。
【００４０】
CPU１０１とアドレスバススクランブル回路１５２とは、バス幅がｎビットのアドレスバス１２１を介して相互に接続され、アドレスバススクランブル回路１５２と記憶部１０３とは、アドレスバス１２１と同じｎビットのバス幅のアドレスバス１２２を介して相互に接続されている。また、CPU１０１と記憶部１０３は、バス幅がmビットのデータバス１２３を介して、相互に接続されている。
【００４１】
CPU１０１は、所定のプログラムを実行することにより、ICカード２を利用したサービスを実現するための処理を実行する。また、CPU１０１は、各サービスに対応したプログラムを並行して実行することができる。換言すれば、CPU１０１は、複数のサービスの処理を並行して実行することができる。
【００４２】
CPU１０１は、各サービスで使用するデータを、記憶部１０３のRAM１７１または不揮発性メモリ１７２に書き込んだり、記憶部１０３のRAM１７１または不揮発性メモリ１７２から読み出したりする。なお、以下、適宜、記憶部１０３のRAM１７１または不揮発性メモリ１７２にデータを書き込むことを、単に、記憶部１０３にデータを書き込むと表現し、記憶部１０３のRAM１７１または不揮発性メモリ１７２からデータを読み出すことを、単に、記憶部１０３からデータを読み出すと表現する。
【００４３】
CPU１０１は、記憶部１０３にデータを書き込む場合、データの論理的な書き込み位置を表す論理アドレスを示す論理アドレス信号を、アドレスバス１２１を介してアドレスバススクランブル回路１５２に供給するとともに、書き込むデータを含み、データの書き込みの指令を示す書き込み信号を、データバス１２３を介して記憶部１０３に供給する。また、CPU１０１は、記憶部１０３からデータを読み出す場合、データの論理的な読み出し位置を表す論理アドレスを示す論理アドレス信号を、アドレスバス１２１を介してアドレスバススクランブル回路１５２に供給するとともに、データの読み出しの指令を示す読み出し信号を、データバス１２３を介して記憶部１０３に供給する。
【００４４】
メモリアクセス制御部１０２は、CPU１０１の記憶部１０３へのアクセスを制御する。
【００４５】
メモリアクセス制御部１０２に含まれる個々の構成要素のうち、スイッチ１４１は、ユーザがスクランブル鍵の変更を指令する場合に押下される。スイッチ１４１は、ユーザにより押下された場合、押下されたことを示す信号をスクランブル鍵変更指令器１４２に供給する。
【００４６】
スクランブル鍵変更指令器１４２は、スイッチ１４１が押下された場合、スクランブル鍵の変更の指令を乱数出力器１４３に供給する。また、スクランブル鍵変更指令器１４２は、タンパ監視回路１０５－１乃至１０５－６から出力される監視信号に基づいて、筐体３１の破壊や開放などのタンパ行為を検出した場合、スクランブル鍵の変更の指令を乱数

出力器１４３に供給する。

【００４７】

乱数出力器１４３は、スクランブル鍵変更指令器１４２からスクランブル鍵の変更の指令を示す信号が供給された場合、ｎビットのビット列からなる疑似乱数を生成し、生成した疑似乱数をスクランブル鍵としてスクランブル鍵バッファ１６１に出力する。

【００４８】

バススクランブル器１４４は、CPU１０１から供給される論理アドレス信号により示される論理アドレスを、記憶部１０３に実際にアクセスする物理アドレスに変換する処理を行う。

【００４９】

バススクランブル器１４４に含まれる個々の構成要素のうち、スクランブル鍵保持部１５１は、乱数出力器１４３から供給された疑似乱数をスクランブル鍵として保持する。具体的には、スクランブル鍵保持部１５１のスクランブル鍵バッファ１６１が、乱数出力器１４３から供給された疑似乱数をスクランブル鍵として保持するとともに、スクランブル鍵を内部メモリ１６２に供給し、記憶させる。内部メモリ１６２は、フラッシュメモリなどの不揮発性メモリ、または、電池などによりバックアップされたRAMなどにより構成され、主電源１４がオフされた状態においても、スクランブル鍵を保持し続ける。また、スクランブル鍵バッファ１６１は、主電源１４がオフされた状態からオンされた場合、内部メモリ１６２に記憶されているスクランブル鍵を読み出し、保持する。さらに、スクランブル鍵バッファ１６１は、主電源１４がオンされてから、内部メモリ１６２からのスクランブル鍵の読み出しが完了するまでの間、リセット指令信号をリセット回路１０４に供給する。

【００５０】

アドレスバススクランブル回路１５２は、スクランブル鍵バッファ１６１に保持されている鍵を用いて、CPU１０１から供給された論理アドレス信号により示される論理アドレスにスクランブルをかけることにより、論理アドレスを実際に記憶部１０３にアクセスする物理アドレスに変換する。換言すれば、アドレススバスクランブル回路１５２は、入力された論理アドレスにスクランブルをかけることにより、その論理アドレスに対して、物理アドレスを割り当てる。アドレスバススクランブル回路１５２は、アドレスバス１２２を介して、変換後の物理アドレスを示す物理アドレス信号を記憶部１０３に供給する。

【００５１】

記憶部１０３に含まれる個々の構成要素のうち、RAM１７１は、各サービスのデータや個人情報などの機密性の高いデータを格納する。RAM１７１に格納されているデータは、電源制御部１０６からの電力により保持され、電源制御部１０６からの電力の供給が停止された場合、消去される。

【００５２】

不揮発性メモリ１７２は、例えば、フラッシュメモリ、EEPROM（Electrically Erasable and Programmable Read Only Memory）、HDD（Hard Disk Drive）、MRAM（Magnetoresistive Random Access Memory，磁気抵抗メモリ）、FeRAM（Ferroelectric Random Access Memory，強誘電体メモリ）、または、OUM（Ovonic Unified Memory）などにより構成され、機密性の低いデータが格納される。

【００５３】

RAM１７１および不揮発性メモリ１７２は、CPU１０１から書き込み信号が供給された場合、アドレスバススクランブル回路１５２から供給された物理アドレス信号により示されるRAM１７１または不揮発性メモリ１７２上の物理アドレスに、書き込み信号に含まれるデータを書き込む。また、RAM１７１および不揮発性メモリ１７２は、CPU１０１から読み出し信号が供給された場合、アドレスバススクランブル回路１５２から供給された物理アドレス信号により示されるRAM１７１または不揮発性メモリ１７２上の物理アドレスからデータを読み出し、読み出したデータを、データバス１２３を介して、CPU１０１に供給する。

【００５４】
リセット回路１０４は、スクランブル鍵バッファ１６１からリセット指令信号が供給されている間、CPU１０１にリセット信号を供給し、CPU１０１の状態を初期化する。
【００５５】
タンパ監視回路１０５－１乃至１０５－６は、図８などを参照して後述するように、筐体３１の破壊や開放などのタンパ行為を監視し、監視結果を示す監視信号を電源制御部１０６およびスクランブル鍵変更指令器１４２に供給する。
【００５６】
なお、以下、タンパ監視回路１０５－１乃至１０５－６を個々に区別する必要がない場合、単に、タンパ監視回路１０５と称する。
【００５７】
電源制御部１０６は、図１０などを参照して後述するように、主電源１４からの電力の供給を受け、制御モジュール１３の各部への電力の供給を制御する。また、電源制御部１０６は、制御モジュール１３に対するタンパ行為が検出された場合、記憶部１０３への電力の供給を停止することにより、RAM１７１のデータを消去させる。
【００５８】
図６は、乱数出力器１４３の機能的構成を示すブロック図である。乱数出力器１４３は、乱数生成器２０１、および、スイッチ２０２を含むように構成される。
【００５９】
乱数生成器２０１は、Ｌ１ビットのシフトレジスタを有するLFSR(Linear Feedback Shift Register, リニアフィードバックシフトレジスタ)型乱数発生器２１１、Ｌ２ビットのシフトレジスタを有するLFSR型乱数発生器２１２、および、EXOR回路２１３を含むように構成される。
【００６０】
LFSR型乱数発生器２１１，２１２は、シフトレジスタの所定のビットの値の排他的論理和をフィードバック値としてシフトレジスタに入力する周知のLFSRの原理により構成される。乱数生成器２０１は、LFSR型乱数発生器２１１，２１２により生成される２つの異なるM系列の疑似乱数の排他的論理和をEXOR回路２１３によりビット毎に取ることにより、Gold系列の疑似乱数を生成する。なお、乱数生成器２０１が備えるLFSR型乱数発生器２１１，２１２の個数は、２個に限定されるものではなく、３個以上とすることも可能である。
【００６１】
スイッチ２０２は、スクランブル鍵変更指令器１４２からスクランブル鍵の変更の指令を示す信号が入力された場合、オンとなり、乱数生成器２０１により生成されたGold系列の疑似乱数を示すビット列が、スイッチ２０２を介してスクランブル鍵バッファ１６１に出力される。
【００６２】
図７は、バススクランブル器１４４の機能的構成の詳細を示すブロック図である。
【００６３】
スクランブル鍵バッファ１６１は、シリアル入力およびパラレル入出力のｎビットのシフトレジスタなどにより構成され、乱数出力器１４３からシリアル信号により供給された疑似乱数をスクランブル鍵として保持する。
【００６４】
アドレスバススクランブル回路１５２は、アドレスバス１２１を介してCPU１０１から供給される論理アドレス信号により示されるビットA1乃至Anからなるnビットの論理アドレスと、スクランブル鍵バッファ１６１に保持されているビットK1乃至Knからなるnビットのスクランブル鍵との排他的論理和を、EXOR回路２５１－１乃至２５１－ｎによりビット毎に取ることにより、論理アドレスをビットSA1乃至SAnからなるｎビットの物理アドレスに変換する。アドレスバススクランブル回路１５２は、アドレスバス１２２を介して、変換後の物理アドレスを示す物理アドレス信号を記憶部１０３に供給する。

【００６５】
図８は、図５のタンパ監視回路１０５－１の回路構成の例を示す図である。タンパ監視回路１０５－１は、保護基板３３上の電線５１および抵抗３０１、抵抗３０２、抵抗３０３、p型のMOSFET（Metal Oxide Semiconductor Field Effect Transistor）３０４、比較電圧源素子３０５、および、電圧比較器３０６を含むように構成される。
【００６６】
MOSFET３０４のゲートは、点Ａ、コネクタ４１Ａ，４１Ｂ、および、電線５１を介して、抵抗３０１の一端に接続され、点Ａを介して、抵抗３０２の一端に接続されている。MOSFET３０４のソースは、点Ｂを介して、抵抗３０３の一端、および、電圧比較器３０６のプラス端子に接続されている。MOSFET３０４のドレインは、抵抗３０２の一端であって、MOSFET３０４のゲートに接続されている一端とは異なる一端、および、比較電圧源素子３０５のマイナス端子に接続されるとともに、接地されている。すなわち、タンパ監視回路１０５－１は、MOSFET３０４のドレインが接地されたソースフォロワ回路により構成される。
【００６７】
また、抵抗３０１の一端であって、電線５１に接続されている一端とは異なる一端は、コネクタ４１Ｂ，４１Ａを介して、電源制御部１０６、および、抵抗３０３の一端であって、点Ｂに接続されている一端とは異なる一端に接続されている。比較電圧源素子３０５のプラス端子は、電圧比較器３０６のマイナス端子に接続されている。電圧比較器３０６の出力端子は、点Ｓ１を介して、図５の電源制御部１０６およびスクランブル鍵変更指令器１４２に接続されている。
【００６８】
抵抗３０２の値は、抵抗３０１の値と比較して十分大きな値を持つ。従って、点Ａの電圧、すなわち、MOSFET３０４のゲート電圧は、電源制御部１０６からの入力電圧とほぼ同じ値まで引き上げられ、MOSFET３０４のソース電圧は、ゲート電圧とほぼ同じ電圧となるように追従するので、点Ａと点Ｂはほぼ同じ電圧となる。従って、電圧比較器３０６のプラス端子には、電源制御部１０６からの入力電圧とほぼ等しい電圧が入力される。比較電圧源素子３０５は、電源制御部１０６からの入力電圧の約半分の電圧を電圧比較器３０６のマイナス端子に入力する。電圧比較器３０６から出力される監視信号の電圧は、マイナス端子よりプラス端子に入力される電圧の方が高い場合、プラス端子とマイナス端子との電圧の差分を増幅した値となり、プラス端子よりマイナス端子に入力される電圧の方が高い場合、ほぼ０Ｖとなる。
【００６９】
ここで、図９を参照して、タンパ監視回路１０５－１の動作の例について説明する。図９は、制御モジュール１３の筐体３１の面３１Aに対して、開放や破壊などのタンパ行為が行われた場合の点Ａ、点Ｂおよび点Ｓ１の電圧の変化の例を示す図である。なお、時刻ｔ１は、タンパ行為が行われた時刻を示す。
【００７０】
時刻ｔ１以前の異常が発生していない状態においては、上述したように、点Ａと点Ｂの電圧は、電源制御部１０６からの入力電圧とほぼ等しくなる。従って、電圧比較器３０６のプラス端子の電圧、すなわち、点Ｂの電圧が、マイナス端子の電圧、すなわち、比較電圧源素子３０５の電圧より高くなるため、電圧比較器３０６の出力電圧、すなわち、点Ｓ１の電圧は、プラス端子とマイナス端子との電圧の差分を増幅した正の値となる。
【００７１】
時刻ｔ１において、制御モジュール１３の筐体３１の面３１Ａが開放され、コネクタ４１Ａとコネクタ４１Ｂとが分離されたり、面３１Ａに対して、穴を開けるなどの破壊行為が行われ、電線５１に断線が生じた場合、電源制御部１０６とMOSFET３０４のゲートとの間が断線され、点Ａの電圧はほぼ０Ｖとなる。これに伴い、図９に示されるように、点Ｂの電圧もほぼ０Ｖとなり、電圧比較器３０６のマイナス端子の電圧がプラス端子の電圧より高くなるため、電圧比較器３０６の出力電圧、すなわち、点Ｓ１の電圧は、ほぼ０Ｖと

なる。

【００７２】

従って、タンパ監視回路１０５－１から出力される監視信号に基づいて、筐体３１の開放や破壊などのタンパ行為を検出することができる。

【００７３】

なお、タンパ監視回路１０５－２乃至１０５－６も、タンパ監視回路１０５－１と同様の構成を有しており、その説明は繰り返しになるので省略するが、タンパ監視回路１０５－１と同様に、タンパ監視回路１０５－２乃至１０５－６からの監視信号に基づいて、筐体３１の開放や破壊などのタンパ行為を検出することができる。

【００７４】

従って、タンパ監視回路１０５－１乃至１０５－６からの監視信号の電圧を監視することにより、筐体３１の全ての面に対する開放や破壊などのタンパ行為を確実に検出することができる。

【００７５】

なお、以下、タンパ監視回路１０５－２は、保護基板３４上の電線を含み、タンパ監視回路１０５－３は、保護基板３５上の電線を含み、タンパ監視回路１０５－４は、保護基板３５上の電線を含み、タンパ監視回路１０５－５および１０５－６は、図２に図示されていない筐体３１の２面にそれぞれ対応する保護基板上の電線を含むものとする。

【００７６】

図１０は、図５の電源制御部１０６の回路構成の例を示す図である。電源制御部１０６は、主電源１４のバックアップ電源である電池３５１、電池ソケット３５２、ダイオード３５３，３５４、コンデンサ３５５、電源レギュレータ３５６、抵抗３５７、電池電圧検知器３５８、および、スイッチ３５９を含むように構成される。

【００７７】

電池３５１は、電池ソケット３５２に装着された状態において、正極が、電池ソケット３５２を介して、逆流防止用のダイオード３５３のアノード、抵抗３５７の一端、および、電池電圧検知器３５８の入力端子Ｔ１１に接続され、負極が、電池ソケット３５２を介して、コンデンサ３５５の一端、および、抵抗３５７の一端であって、電池３５１の正極に接続されている一端とは異なる一端に接続されるとともに、接地されている。ダイオード３５３のカソードは、逆流防止用のダイオード３５４のカソード、コンデンサ３５５の一端であって、電池３５１の負極に接続されている一端とは異なる一端、および、電源レギュレータ３５６の入力端子Ｔ１に接続されている。ダイオード３５４のアノードは、主電源１４に接続されている。

【００７８】

電源レギュレータ３５６の出力端子Ｔ２は、電池電圧検知器３５８の電源端子Ｔ１３、スイッチ３５９の一端、CPU１０１、メモリアクセス制御部１０２、リセット回路１０４、および、タンパ監視回路１０５－１乃至１０５－６に接続されている。電池電圧検知器３５８の出力端子Ｔ１２は、スイッチ３５９の図示せぬ電圧検知端子に接続されている。スイッチ３５９の一端であって、電源レギュレータ３５６の出力端子Ｔ２に接続されている一端とは異なる一端は、記憶部１０３に接続されている。また、スイッチ３５９の図示せぬ電圧検知端子が、点Ｓ１乃至Ｓ６を介して、タンパ監視回路１０５－１乃至１０５－６に接続されている。

【００７９】

電源レギュレータ３５６は、ダイオード３５４を介して、主電源１４から入力される電圧、または、ダイオード３５３を介して、電池３５１から入力される電圧を所定の電圧に変換し、ほぼ一定の電圧を出力端子Ｔ２から出力する。出力端子Ｔ２から出力された電圧は、CPU１０１、メモリアクセス制御部１０２、リセット回路１０４、タンパ監視回路１０５－１乃至１０５－６、電池電圧検知器３５８、および、スイッチ３５９を介して、記憶部１０３に供給される。すなわち、主電源１４または電池３５１からの電力が、電源レギュレータ３５６により、その電圧が安定化されて、CPU１０１、メモリアクセス制御部

１０２、リセット回路１０４、タンパ監視回路１０５－１乃至１０５－６、電池電圧検知器３５８、および、記憶部１０３に供給される。従って、主電源１４または電池３５１のいずれか一方からの電力の供給が停止されても、CPU１０１、メモリアクセス制御部１０２、リセット回路１０４、タンパ監視回路１０５－１乃至１０５－６、電池電圧検知器３５８、および、記憶部１０３に安定化された電力が供給される。

【００８０】

また、コンデンサ３５５は、主電源１４または電池３５１により電力が供給されている場合、主電源１４または電池３５１により所定の電圧に充電される。そして、主電源１４および電池３５１からの電力の供給が停止された場合、コンデンサ３５５に蓄えられた電力が、電源レギュレータ３５６を介して、CPU１０１、メモリアクセス制御部１０２、リセット回路１０４、タンパ監視回路１０５－１乃至１０５－６、電池電圧検知器３５８、および、スイッチ３５９を介して、記憶部１０３に供給される。コンデンサ３５５は、例えば、スーパーキャパシタ（電気二重層キャパシタ）により構成され、CPU１０１、メモリアクセス制御部１０２、リセット回路１０４、タンパ監視回路１０５－１乃至１０５－６、電池電圧検知器３５８、および、記憶部１０３に所定の時間（例えば、３０～４０分）以上の電力の供給が可能な蓄電容量を持つ。

【００８１】

電池電圧検知器３５８は、入力端子Ｔ１１に入力される電圧、すなわち、電池３５１により抵抗３５７に印加される電圧を検知することにより、電池３５１の取り外しを検出する。電池電圧検知器３５８は、入力端子Ｔ１１の電圧が所定の閾値以下になった場合、内部の図示せぬカウンタを用いて時間の計測を開始し、入力端子Ｔ１１の電圧が閾値以下の状態が所定の時間継続した場合、出力端子Ｔ１２の電圧をHighレベル（例えば、５V）からLowレベル（例えば、０V）に変化させる。

【００８２】

スイッチ３５９は、タンパ監視回路１０５－１乃至１０５－６からの監視信号、および、電池電圧検知器３５８の出力信号の電圧のうち１つでも所定の閾値以下になった場合、オフされ、電源制御部１０６から記憶部１０３への電力の供給が停止される。

【００８３】

ここで、図１１を参照して、電源制御部１０６の動作の例を説明する。図１１は、主電源１４がオフされており、かつ、タンパ監視回路１０５－１乃至１０５－６によりタンパ行為が検出されていない状態において、電池３５１が電池ソケット３５２から取り外された場合の電池電圧検知器３５８の端子Ｔ１１，Ｔ１２、および、電源制御部１０６から記憶部１０３への出力電圧の変化の例を示す図である。なお、時刻ｔ１１は、電池３５１が電池ソケット３５２から取り外された時刻を示す。

【００８４】

時刻ｔ１１以前の電池３５１が取り付けられた状態においては、電池３５１により、電池電圧検知器３５８の入力端子Ｔ１１に正の電圧が入力され、出力端子Ｔ１２からHighレベルの電圧がスイッチ３５９に入力される。また、タンパ監視回路１０５－１乃至１０５－６によりタンパ行為が検出されておらず、タンパ監視回路１０５－１乃至１０５－６から正の電圧がスイッチ３５９に入力されているため、スイッチ３５９はオンの状態となり、電源レギュレータ３５６の出力端子Ｔ２から出力された電力が、スイッチ３５９を介して、記憶部１０３に供給される。また、このとき、電源レギュレータ３５６の出力端子Ｔ２から出力された電力は、CPU１０１、メモリアクセス制御部１０２、リセット回路１０４、タンパ監視回路１０５－１乃至１０５－６、および、電池電圧検知器３５８にも供給される。

【００８５】

時刻ｔ１１において、電池３５１が電池ソケット３５２から取り外された場合、電池電圧検知器３５８の入力端子Ｔ１１に入力される電圧が、ほぼ０Ｖとなり、電池電圧検知器３５８は、内部のカウンタを用いて、時間の計測を開始する。また、コンデンサ３５５が放電を開始し、コンデンサ３５５に蓄積されている電力が、電源レギュレータ３５６を介

して、CPU１０１、メモリアクセス制御部１０２、リセット回路１０４、タンパ監視回路１０５－１乃至１０５－６、および、電池電圧検知器３５８に供給される。

【００８６】

時刻ｔ１１において電池電圧検知器３５８が時間の計測を開始してから、所定の時間Ｔａが経過した時刻ｔ１２において、電池電圧検知器３５８は、出力端子Ｔ１２の電圧をHighレベルからLowレベルに変化させる。これにより、スイッチ３５９がオフされ、記憶部１０３への電力の供給が停止される。これにより、記憶部１０３のRAM１７１に記憶されているデータが消去される。

【００８７】

なお、時刻ｔ１２以降も、CPU１０１、メモリアクセス制御部１０２、リセット回路１０４、タンパ監視回路１０５－１乃至１０５－６、および、電池電圧検知器３５８には、電源レギュレータ３５６を介して、コンデンサ３５５から電力が継続して供給される。従って、電池３５１が取り外されても、タンパ監視回路１０５－１乃至１０５－６によるタンパ行為の監視が継続して行われる。

【００８８】

なお、電池電圧検知器３５８は、時間Ｔａの間に電池３５１が取り付けられ、入力端子Ｔ１１に入力される電圧が、所定の閾値を超えた場合、内部のカウンタによる時間の計測を停止する。従って、時間Ｔａを適切に設定することにより、主電源１４をオフした状態においても、RAM１７１のデータを消去させることなく、電池３５１を交換することができる。なお、電池３５１の交換を考慮しなくてもよい場合、時間Ｔａを設けずに、時刻ｔ１１において、スイッチ３５９をオフするようにしてもよい。

【００８９】

次に、図１２乃至図１４を参照して、リーダライタ１の処理を説明する。

【００９０】

まず、図１２のフローチャートを参照して、リーダライタ１により実行されるスクランブル鍵生成処理について説明する。なお、この処理は、例えば、ユーザが、スイッチ１４１を押下したとき開始される。

【００９１】

ステップＳ１において、乱数出力器１４３は、疑似乱数を出力する。具体的には、スイッチ１４１は、押下されたことを示す信号をスクランブル鍵変更指令器１４２に供給する。スクランブル鍵変更指令器１４２は、スクランブル鍵の変更の指令を示す信号をスイッチ２０２に供給し、スイッチ２０２をオンさせる。乱数生成器２０１は、リーダライタ１の主電源１４がオンになっている間、常に疑似乱数を生成しており、スイッチ２０２がオンされることにより、スイッチ２０２を介して、乱数生成器２０１からスクランブル鍵バッファ１６１への疑似乱数の出力が開始される。スイッチ２０２は、乱数生成器２０１から疑似乱数がｎビット出力されたとき、オフとなる。

【００９２】

ステップＳ２において、バススクランブル器１４４は、スクランブル鍵を設定し、スクランブル鍵生成処理は終了する。具体的には、スクランブル鍵バッファ１６１は、乱数出力器１４３から供給されたｎビットのビット列からなる疑似乱数をスクランブル鍵として内部のレジスタに保持する。また、スクランブル鍵バッファ１６１は、内部メモリ１６２にスクランブル鍵を供給し、記憶させる。すなわち、スクランブル鍵が内部メモリ１６２にバックアップされる。

【００９３】

これにより、簡単に、各制御モジュール１３に対して、それぞれ値が異なり、かつ、予測が困難なスクランブル鍵を設定することができる。なお、このスクランブル鍵設定処理は、例えば、リーダライタ１を工場から出荷する前に行われる。

【００９４】

次に、図１３のフローチャートを参照して、リーダライタ１により実行されるメモリアクセス制御処理を説明する。なお、この処理は、例えば、リーダライタ１の主電源１４が

オンされたとき開始される。

【００９５】

ステップＳ３１において、スクランブル鍵バッファ１６１は、リーダライタ１の主電源１４がオンされることにより、リセット回路１０４へのリセット指令信号の供給を開始する。

【００９６】

ステップＳ３２において、リセット回路１０４は、CPU１０１へのリセット信号の供給を開始し、CPU１０１をリセットする。これにより、CPU１０１の状態が初期化される。

【００９７】

ステップＳ３３において、スクランブル鍵バッファ１６１は、内部メモリ１６２に保持されているスクランブル鍵を読み出す。スクランブル鍵バッファ１６１は、読み出したスクランブル鍵を内部のレジスタに保持する。

【００９８】

ステップＳ３４において、スクランブル鍵バッファ１６１は、リセット回路１０４へのリセット指令信号の供給を停止する。これに伴い、リセット回路１０４は、CPU１０１へのリセット信号の供給を停止し、CPU１０１は、プログラムの実行を開始する。

【００９９】

ステップＳ３５において、CPU１０１は、データを書き込むかを判定する。CPU１０１は、実行中のプログラムにおいて、次の処理がデータの書き込みを行う処理でない場合、データを書き込まないと判定し、処理はステップＳ３６に進む。

【０１００】

ステップＳ３６において、CPU１０１は、データを読み出すかを判定する。CPU１０１は、実行中のプログラムにおいて、次の処理がデータの読み出しを行う処理でない場合、データを読み出さないと判定し、処理はステップＳ３５に戻る。

【０１０１】

その後、ステップＳ３５において、データを書き込むと判定されるか、ステップＳ３６においてデータを読み出すと判定されるまで、ステップＳ３５およびＳ３６の処理が繰り返し実行される。

【０１０２】

ステップＳ３５においてCPU１０１は、実行中のプログラムにおいて、次の処理がデータの書き込みを行う処理である場合、データを書き込むと判定し、処理はステップＳ３７に進む。

【０１０３】

ステップＳ３７において、CPU１０１は、データの書き込みを指令する。具体的には、CPU１０１は、データの論理的な書き込み位置を表す論理アドレスを示す論理アドレス信号を、アドレスバス１２１を介してアドレスバススクランブル回路１５２に供給するとともに、書き込むデータを含み、データの書き込みの指令を示す書き込み信号を、データバス１２３を介して記憶部１０３に供給する。

【０１０４】

ステップＳ３８において、アドレスバススクランブル回路１５２は、論理アドレスを物理アドレスに変換する。具体的には、アドレスバススクランブル回路１５２は、論理アドレス信号により示される論理アドレスとスクランブル鍵バッファ１６１に保持されているスクランブル鍵との排他的論理和をビット毎に取り、論理アドレスにスクランブルをかけることにより、論理アドレスを物理アドレスに変換する。アドレスバススクランブル回路１５２は、変換後の物理アドレスを示す物理アドレス信号を、アドレスバス１２２を介して記憶部１０３に供給する。

【０１０５】

ステップＳ３９において、記憶部１０３は、データを書き込む。具体的には、RAM１７１または不揮発性メモリ１７２は、物理アドレス信号に示されるRAM１７１または不揮発性メモリ１７２上の物理アドレスに、CPU１０１から供給された書き込み信号に含まれる

データを書き込む。これにより、CPU１０１から連続した論理アドレスへのデータの書き込みが指令されても、実際には、ランダムに配置されるようにRAM１７１または不揮発性メモリ１７２にデータが書き込まれるため、RAM１７１または不揮発性メモリ１７２に格納されているデータの内容を解析したり、改ざんしたりすることが困難となる。

【０１０６】

その後、処理はステップＳ３５に戻り、ステップＳ３５以降の処理が実行される。

【０１０７】

ステップＳ３６において、CPU１０１は、実行中のプログラムにおいて、次の処理がデータの読み出しを行う処理である場合、データを読み出すと判定し、処理はステップＳ４０に進む。

【０１０８】

ステップＳ４０において、CPU１０１は、データの読み出しを指令する。具体的には、CPU１０１は、データの論理的な読み出し位置を表す論理アドレスを示す論理アドレス信号を、アドレスバス１２１を介してアドレスバススクランブル回路１５２に供給するとともに、データの読み出しの指令を示す読み出し信号を、データバス１２３を介して記憶部１０３に供給する。

【０１０９】

ステップＳ４１において、上述したステップＳ３８の処理と同様に、論理アドレスが物理アドレスに変換され、変換後の物理アドレスを示す物理アドレス信号が、アドレスバス１２２を介して、アドレスバススクランブル回路１５２から記憶部１０３に供給される。

【０１１０】

ステップＳ４２において、記憶部１０３は、データを読み出す。具体的には、RAM１７１または不揮発性メモリ１７２は、物理アドレス信号により示される物理アドレスに記憶されているデータを読み出し、読み出したデータを、データバス１２３を介して、CPU１０１に供給する。

【０１１１】

その後、処理はステップＳ３５に戻り、ステップＳ３５以降の処理が実行される。

【０１１２】

以上のように、各制御モジュール１３に異なるスクランブル鍵を簡単に設定することができるため、たとえ、１台の制御モジュール１３に設定されているスクランブル鍵が解析されたとしても、そのスクランブル鍵を用いて、他の制御モジュール１３のRAM１７１および不揮発性メモリ１７２に記憶されているデータの解析や改ざんをすることができない。従って、データの流出や改ざんの被害を最小限に抑えることができる。

【０１１３】

また、疑似乱数の生成方法およびアドレスのスクランブル方法については、従来の技術をそのまま使用することができ、新たに複雑な回路を設ける必要がなく、スクランブル鍵の変更の指令を入力する以外にユーザの手間も増えないため、簡単にRAM１７１および不揮発性メモリ１７２上のデータのセキュリティを向上させることができる。

【０１１４】

次に、図１４のフローチャートを参照して、リーダライタ１により実行されるタンパ行為監視処理を説明する。なお、この処理は、例えば、工場出荷後に、リーダライタ１の使用が開始されたとき開始される。

【０１１５】

ステップＳ６１において、電池電圧検知器３５８は、電池３５１からの電力の供給が停止されたかを判定する。図１０および図１１を参照して上述したように、電池電圧検知器３５８は、例えば、電池３５１が電池ソケット３５２から取り外され、入力端子Ｔ１１の電圧が所定の閾値を超える状態から閾値以下になった場合、電池３５１からの電力の供給が停止されたと判定し、処理はステップＳ６２に進む。

【０１１６】

ステップＳ６２において、電池電圧検知器３５８は、内部の図示せぬカウンタを用いて

、時間の計測を開始する。

【０１１７】

その後、処理はステップＳ６１に戻り、ステップＳ６１以降の処理が実行される。

【０１１８】

ステップＳ６１において、電池電圧検知器３５８は、入力端子Ｔ１１の電圧が閾値を超えている場合、または、入力端子Ｔ１１の電圧が閾値以下の状態が継続している場合、電池３５１から電力が供給されている、または、電池３５１からの電力の供給が停止された状態が継続していると判定し、処理はステップＳ６３に進む。

【０１１９】

ステップＳ６３において、電池電圧検知器３５８は、電池３５１からの電力の供給が再開されたかを判定する。具体的には、電池電圧検知器３５８は、入力端子Ｔ１１の電圧が閾値以下の状態から閾値を超える状態に変化した場合、電池３５１からの電力の供給が再開されたと判定し、処理はステップＳ６４に進む。

【０１２０】

ステップＳ６４において、電池電圧検知器３５８は、内部の図時せぬカウンタによる時間の計測を停止する。

【０１２１】

その後、処理はステップＳ６１に戻り、ステップＳ６１以降の処理が実行される。

【０１２２】

ステップＳ６３において、電池電圧検知器３５８は、入力端子Ｔ１１の電圧が閾値を超える状態が継続している場合、または、閾値以下の状態が継続している場合、電池３５１から電力が供給されている状態が継続している、または、電池３５１からの電力の供給が停止された状態が継続していると判定し、処理はステップＳ６５に進む。

【０１２３】

ステップＳ６５において、電池電圧検知器３５８は、電池３５１からの電力の供給が停止されてから所定の時間が経過したかを判定する。電池電圧検知器３５８は、内部のカウンタの値が所定の時間以上になっている場合、電池３５１からの電力の供給が停止されてから所定の時間が経過したと判定し、処理はステップＳ６６に進む。

【０１２４】

ステップＳ６６において、電源制御部１０６は、メモリへの電力の供給を停止し、タンパ行為監視処理は終了する。具体的には、電池電圧検知器３５８は、出力端子Ｔ１２の電圧をHighレベルからLowレベルに変化させる。これにより、スイッチ３５９がオフされ、電源レギュレータ３５６から記憶部１０３への電力の供給が停止される。これにより、記憶部１０３のRAM１７１に記憶されているデータが消去される。

【０１２５】

ステップＳ６５において、電池電圧検知器３５８は、内部のカウンタの値が所定の時間未満である場合、電池３５１からの電力の供給が停止されてから所定の時間が経過していない、または、電池３５１からの電力の供給が停止されていないと判定し、処理はステップＳ６７に進む。

【０１２６】

ステップＳ６７において、電源制御部１０６は、筐体３１に対してタンパ行為が行われたかを判定する。具体的には、図８および図９を参照して上述したように、筐体３１の開放や破壊などにより、電源制御部１０６とタンパ監視回路１０５内のMOSFET（図８のタンパ監視回路１０５－１の場合、MOSFET３０４）のゲートとの間が断線された場合、断線されたタンパ監視回路１０５から出力される監視信号の電圧がほぼ０Vになる。電源制御部１０６は、タンパ監視回路１０５－１乃至１０５－６の監視信号の電圧のうち１つでも所定の閾値以下になった場合、筐体３１に対してタンパ行為が行われたと判定し、処理はステップＳ６８に進む。

【０１２７】

ステップＳ６８において、電源制御部１０６は、メモリへの電力の供給を停止する。具

体的には、タンパ監視回路１０５－１乃至１０５－６の監視信号の電圧のうち１つでも所定の閾値以下になることにより、スイッチ３５９がオフされ、電源レギュレータ３５６から記憶部１０３への電力の供給が停止される。これにより、記憶部１０３のRAM１７１に記憶されているデータが消去される。

【０１２８】

ステップＳ６９において、メモリアクセス制御部１０２は、スクランブル鍵を変更し、タンパ行為監視処理は終了する。具体的には、スクランブル鍵変更指令器１４２は、タンパ監視回路１０５－１乃至１０５－６の監視信号の電圧のうち１つでも所定の閾値以下になった場合、スクランブル鍵の変更の指令を示す信号を乱数出力器１４３のスイッチ２０２に供給し、スイッチ２０２をオンさせる。スイッチ２０２がオンされることにより、スイッチ２０２を介して、乱数生成器２０１からスクランブル鍵バッファ１６１への疑似乱数の出力が開始される。スイッチ２０２は、乱数生成器２０１から疑似乱数がｎビット出力されたとき、オフとなる。スクランブル鍵バッファ１６１は、乱数出力器１４３から供給されたｎビットのビット列からなる疑似乱数を新たなスクランブル鍵として内部のレジスタに保持する。また、スクランブル鍵バッファ１６１は、内部メモリ１６２にスクランブル鍵を供給し、記憶させる。

【０１２９】

なお、ステップＳ６９において、アドレスのスクランブルが行われないためスクランブル鍵として用いられることがない、全て０からなる値を強制的にスクランブル鍵に設定するようにしてもよい。

【０１３０】

ステップＳ６７において、筐体３１に対してタンパ行為が行われていないと判定された場合、処理はステップＳ６１に戻り、ステップＳ６１以降の処理が実行される。

【０１３１】

このようにして、例えば、タンパ監視回路１０５－１乃至１０５－６の動作を停止させる目的で電池３５１が取り外されても、タンパ監視回路１０５－１乃至１０５－６が継続して動作するので、制御モジュール１３の耐タンパ性を向上させることができる。また、電池３５１が取り外されてから所定の時間が経過した場合、RAM１７１のデータが消去されるので、耐タンパ性をさらに向上させることができる。

【０１３２】

さらに、筐体３１の開放や破壊などのタンパ行為が確実に検出され、タンパ行為が検出された場合、RAM１７１のデータが消去されるため、さらに耐タンパ性を向上させることができる。

【０１３３】

また、タンパ行為が検出された場合、スクランブル鍵が変更されるため、たとえRAM１７１のデータが消去されなくても、ICE（In-Circuit Emulator）などを用いたRAM１７１上のデータの解析を困難にすることができる。

【０１３４】

なお、以上の説明では、揮発性のメモリであるRAM１７１のデータを保護する例を示したが、例えば、電池３５１の取り外し、筐体の開放や破壊などが検出された場合に、不揮発性のメモリのデータを消去または破壊することにより、不揮発性のメモリのデータを保護するようにすることも可能である。なお、揮発性メモリのデータを消去する場合、不揮発性メモリのデータを消去する場合と比較して、CPU等のプロセッサを動作させる必要がないため、より少ない電力でデータを消去することができる。従って、コンデンサ３５５の容量を低く抑えることができる。

【０１３５】

また、保護基板を、図３に示されるような単層構造ではなく、多層構造とするようにして、各層に配線のパターンを設けるようにしてもよい。

【０１３６】

さらに、保護基板上の電線の配線パターンは、上述した例に限定されるものではなく、

筐体３１の面の長さまたは幅に対して十分細い電線が、筐体３１の面の長さまたは幅に対して十分狭い間隔で前記筐体のほぼ全面を覆うように配線されるようにすればよい。

【０１３７】

また、必ずしも保護基板上に電線を設ける必要はなく、例えば、筐体３１の内面上に設けたり、筐体の外面と内面との間に設けるようにしてもよい。

【０１３８】

さらに、本発明の実施の形態においては、制御モジュール１３を、主電源１４を用いずに電池３５１のみで動作させるようにすることも可能である。

【０１３９】

また、本発明の実施の形態における電池３５１の取り外しに対する対策は、上述したタンパ監視回路１０５－１乃至１０５－６に限らず、動作させるために電力の供給が必要なタンパ監視回路、例えば、誤動作を目的にした熱による攻撃を監視する温度監視回路などに対して有効である。

【０１４０】

さらに、以上の説明では、保護基板ごとにタンパ監視回路１０５を設けるようにしたが、例えば、複数の保護基板の電線を直列に接続することにより、タンパ監視回路の数を削減するようにしてもよい。

【０１４１】

また、電池３５１の取り外しが検出された場合、タンパ監視回路１０５によりタンパ行為が検出された場合と同様に、スクランブル鍵を変更するようにしてもよい。

【０１４２】

さらに、以上の説明では、Gold系列の疑似乱数をスクランブル鍵に用いる例を示したが、スクランブル鍵に用いる乱数または疑似乱数は上述した例に限定されるものではなく、例えば、LFSRを１個だけ備えたM系列の疑似乱数を用いたり、熱雑音を利用した物理乱数を用いるようにしてもよい。

【０１４３】

また、アドレスにスクランブルをかける方法も上述した例に限定されるものではなく、乱数または疑似乱数により設定されたスクランブル鍵を用いた他の方法を適用するようにしてもよい。

【０１４４】

さらに、以上の説明では、リーダライタ１と通信する相手としてICカード２を例に挙げたが、もちろん、リーダライタ１は、非接触ICカード機能を有する装置、例えば、非接触ICカード機能を有する携帯電話機、携帯情報端末（Personal Digital Assistants）、時計、コンピュータなどと通信することが可能である。

【０１４５】

また、図５のメモリアクセス制御部１０２を、リーダライタ以外の、メモリのデータを読み書きする他の装置に適用することも可能である。

【０１４６】

さらに、本発明の実施の形態は、上述した実施の形態に限定されるものではなく、本発明の要旨を逸脱しない範囲において種々の変更が可能である。

【図面の簡単な説明】

【０１４７】

【図１】本発明を適用したリーダライタの一実施の形態を示すブロック図である。

【図２】図１の制御モジュールの外観の構成の例を示す断面図である。

【図３】図２の保護基板の一つの面の構成の例を示す図である。

【図４】図２の保護基板の他の面の構成の例を示す図である。

【図５】図１の制御モジュールの機能的構成を示すブロック図である。

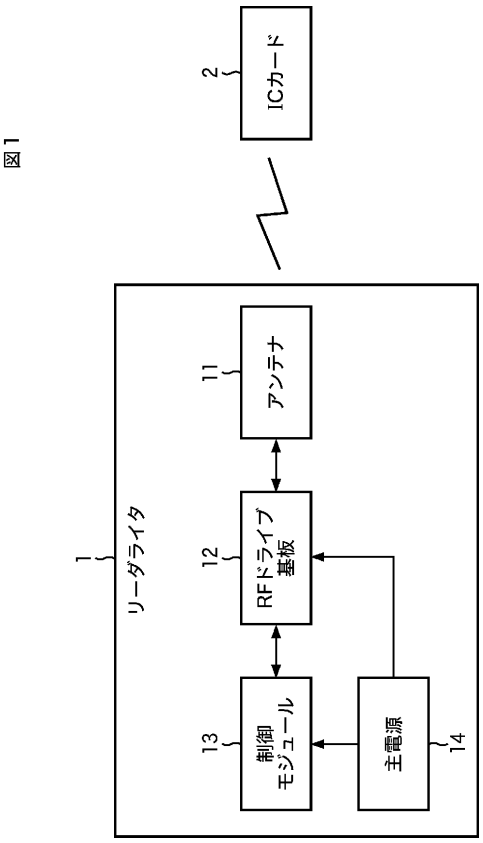
【図６】図５の乱数出力器の機能的構成を示すブロック図である。

【図７】図５のバススクランブル器の機能的構成の詳細を示すブロック図である。

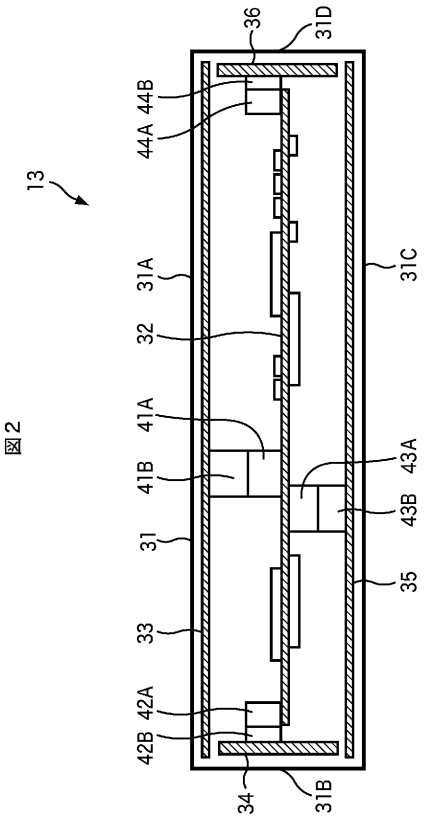
【図８】図５のタンパ監視回路の構成の例を示す図である。

【図９】図５のタンパ監視回路の動作の例を説明するための図である。
【図１０】図５の電源制御部の回路の構成の例を示す図である。
【図１１】図５の電源制御部の動作の例を説明するための図である。
【図１２】図１のリーダライタにより実行されるスクランブル鍵生成処理を説明するためのフローチャートである。
【図１３】図１のリーダライタにより実行されるメモリアクセス制御処理を説明するためのフローチャートである。
【図１４】図１のリーダライタにより実行されるタンパ行為監視処理を説明するためのフローチャートである。
【符号の説明】
【０１４８】
１　リーダライタ，　２　ICカード，　１３　制御モジュール，　１４　主電源，　３１　筐体，　３２　メイン基板，　３３乃至３６　保護基板，　４１乃至４４　コネクタ，　５１　電線，　１０１　CPU，　１０２　メモリアクセス制御部，　１０３　記憶部，　１０５　タンパ監視回路，　１０６　電源制御部，　１４２　スクランブル鍵変更指令器，　１４３　乱数出力器，　１４４　バススクランブル器，　１５１　スクランブル鍵保持部，　１５２　アドレスバススクランブル回路，　１６１　スクランブル鍵バッファ，　１６２　内部メモリ，　１７１　RAM，　１７２　不揮発性メモリ，　２０１　乱数生成器，　２０２　スイッチ，　３０１乃至３０３　抵抗，　３０４　MOSFET，　３０５　比較電圧源素子，　３０６　電圧比較器，　３５１　電池，　３５２　電池ソケット，　３５５　コンデンサ，　３５６　電源レギュレータ，　３５８　電池電圧検知器，　３５９　スイッチ

【図１】

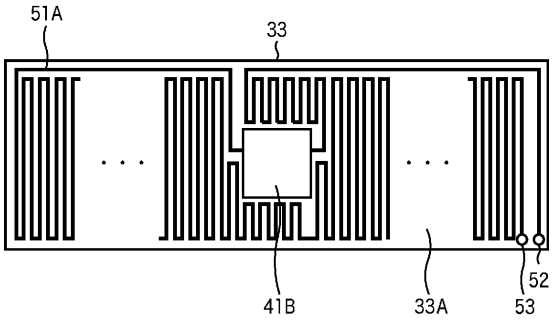


【図２】



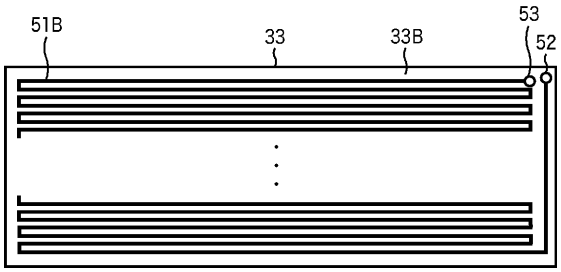
【図３】

図3



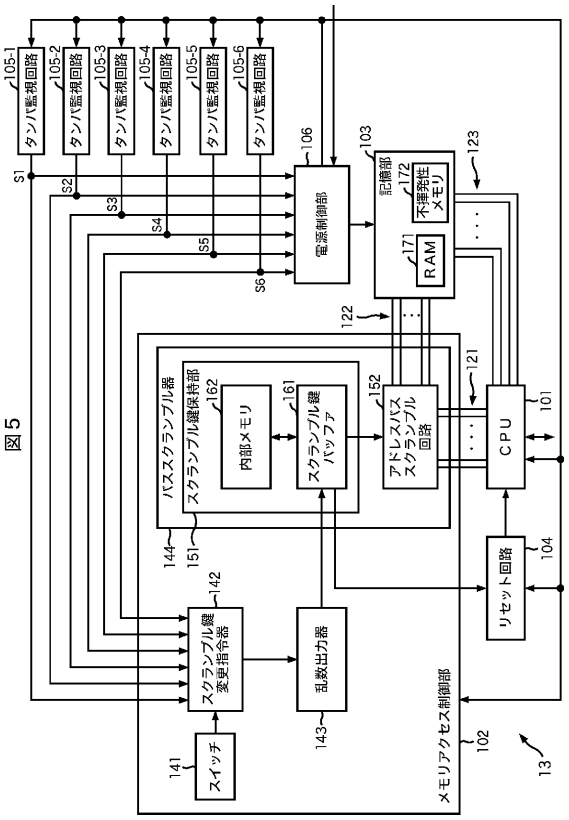
【図４】

図4



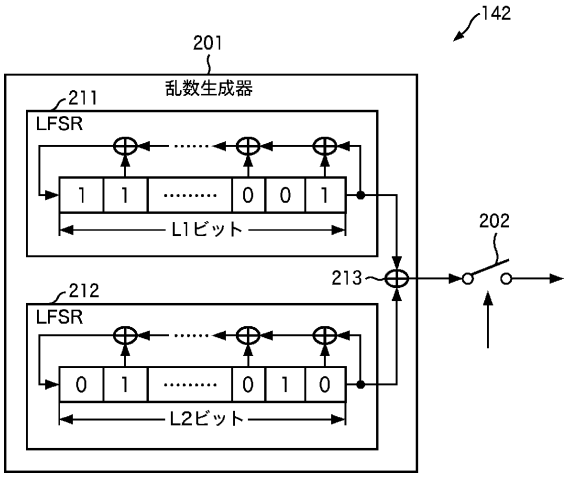
【図５】

図5



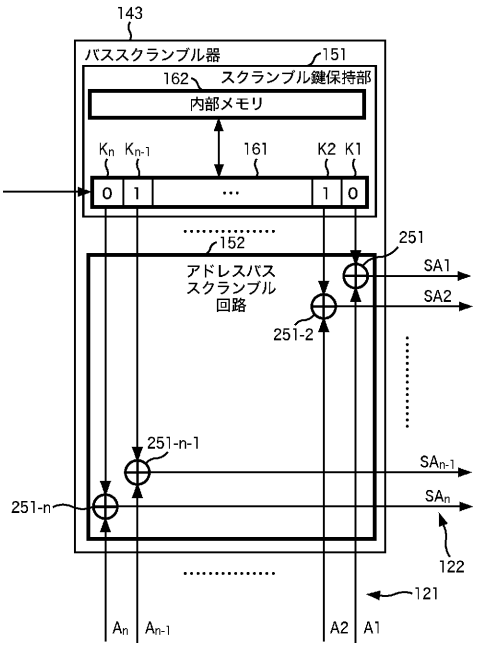
【図６】

図6



【図７】

図7



【図８】

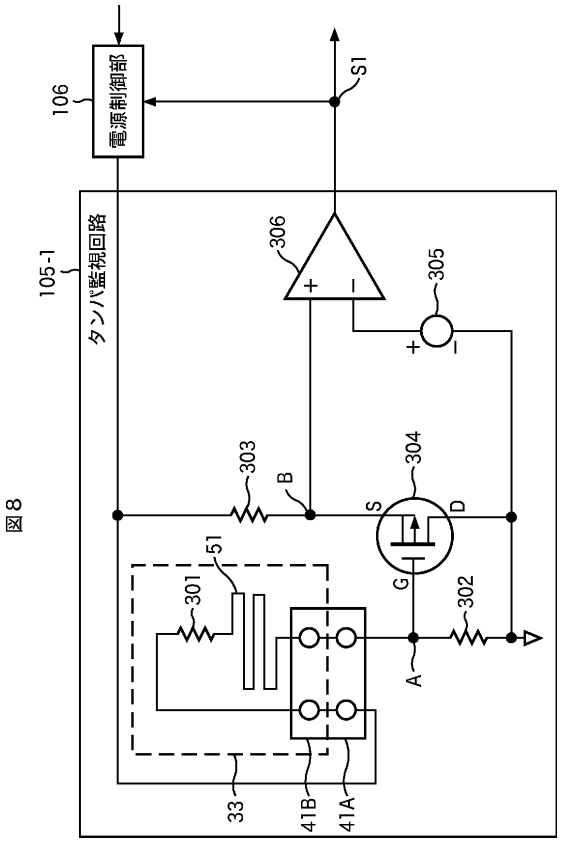


図８

【図９】

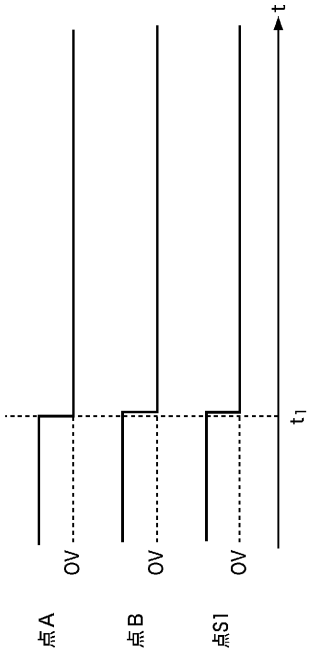


図９

【図１０】

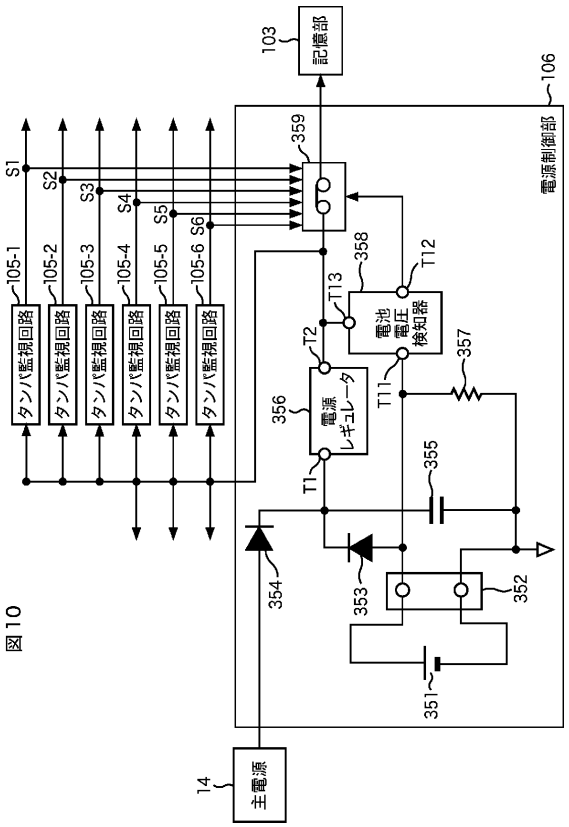


図１０

【図１１】

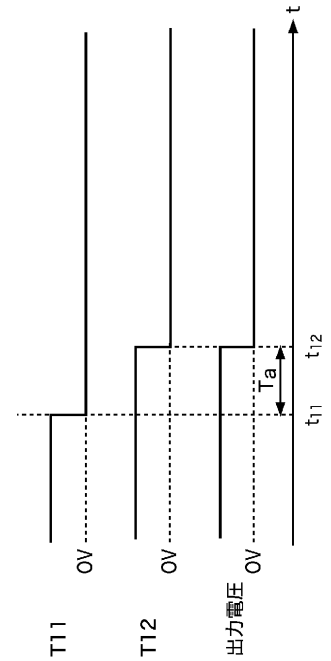
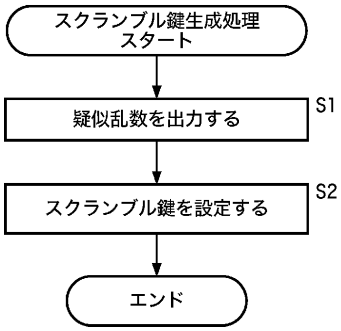
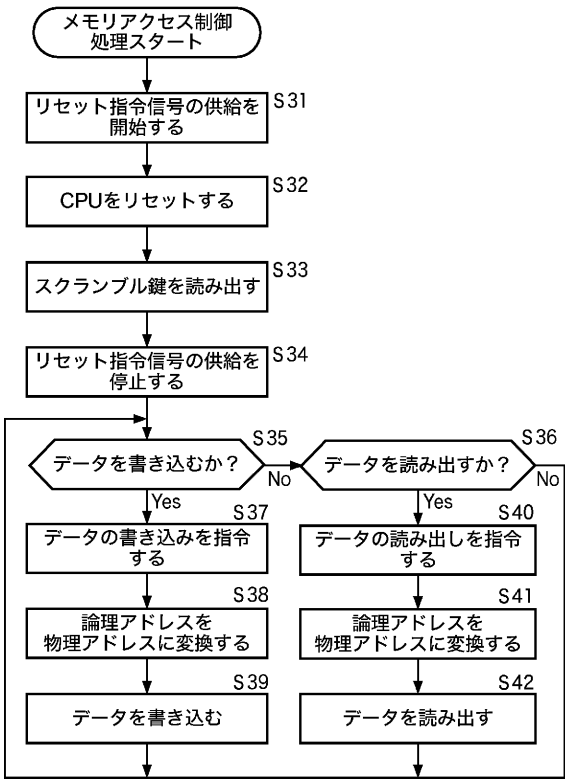


図１１

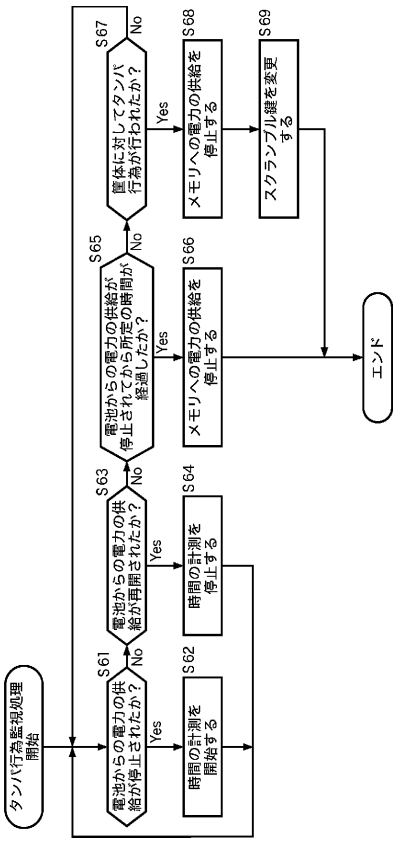
【図１２】
図12



【図１３】
図13



【図１４】
図14



フロントページの続き

(51)Int.Cl.	FI		テーマコード（参考）
	G06K 17/00	S	