(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第5453167号
(P5453167)

(45)発行日　平成26年3月26日(2014.3.26)　(24)登録日　平成26年1月10日(2014.1.10)

(51)Int.Cl.　F I
H04L 9/10 (2006.01)　H04L 9/00 621A
G06F 1/00 (2006.01)　G06F 1/00 370E

請求項の数 7　(全 9 頁)

(21)出願番号　特願2010-114873(P2010-114873)
(22)出願日　平成22年5月19日(2010.5.19)
(65)公開番号　特開2011-244227(P2011-244227A)
(43)公開日　平成23年12月1日(2011.12.1)
審査請求日　平成24年7月24日(2012.7.24)

(73)特許権者　000005108
株式会社日立製作所
東京都千代田区丸の内一丁目６番６号
(74)代理人　110000350
ポレール特許業務法人
(72)発明者　等々力　直之
神奈川県秦野市堀山下１番地　株式会社日立製作所　エンタープライズサーバ事業部内
(72)発明者　内藤　倫典
神奈川県横浜市西区みなとみらい二丁目３番３号　日立情報通信エンジニアリング株式会社内

最終頁に続く

(54)【発明の名称】暗号機能の識別装置

(57)【特許請求の範囲】
【請求項１】
情報処理装置のＡＣ電源からの給電を受けて動作する電子部品を搭載し、該情報処理装置に対して着脱可能な電子ユニットにおいて、
情報処理装置で扱われるデータを暗号化及び復号化するための暗号化復号キーを保持する暗号機能と、
該暗号機能を有効又は無効に設定する制御手段と、
電池と、
該電池からの給電を受け、該暗号機能の該設定に応じて該制御手段の出力信号の状態を保持する信号保持器と、
該信号保持器の出力に従って所定の通報信号を出力する通報手段と、
を有することを特徴とする電子ユニットにおける暗号機能の識別装置。
【請求項２】
前記暗号機能として、情報処理装置で扱われるデータを暗号化及び復号化するための暗号化復号キーを保持するセキュリティチップを有し、更に
該セキュリティチップが有効又は無効かの現在の設定状態を示す管理情報を格納するメモリと、
外部からの操作によって、該セキュリティチップを有効又は無効にするため設定が行われるレジスタを有する、前記制御手段としての制御マイコンを有し
前記信号保持器は、該メモリに格納される該管理情報の設定に応じて、該制御マイコンの

出力信号の状態を保持する、請求項１の暗号機能の識別装置。
【請求項３】
前記信号保持器と前記通報手段との間にスイッチを備え、該スイッチが閉じられたときに該信号保持器の出力によって前記通報手段は該所定の通報信号を出力する、請求項１又は２のいずれかの項記載の暗号機能の識別装置。
【請求項４】
前記電子ユニットは該情報処理装置の電子部品を搭載するマザーボードであり、該信号保持器には、該電池から及び該マザーボードの外に設置された補助電源から給電され、該マザーボードが該情報処理装置から脱状態にある時、該補助電源からの給電はオフとなる、請求項１又は３のいずれかの項記載の暗号機能の識別装置。
【請求項５】
前記メモリは、該セキュリティチップが有効なときの設定値と、該セキュリティチップが無効な時の設定値と、該セキュリティチップの現在の設定値とを管理する、セキュリティ設定テーブルを記憶する、請求項２記載の暗号機能の識別装置。
【請求項６】
前記通報手段はＬＥＤであり、該電子ユニットが該情報処理装置から脱状態にある時、前記信号保持器の出力に応じて該ＬＥＤは発光する、請求項１乃至５のいずれかの項記載の暗号機能の識別装置。
【請求項７】
前記信号保持器はフリップフロップであり、該フリップフロップは、該制御マイコンが設定した、該セキュリティチップの現在の設定値と同じ状態を保持する、請求項２記載の暗号機能の識別装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、暗号機能の識別装置に係り、特に、情報処理装置で扱われるデータが暗号化されているか否かを識別する暗号機能の識別装置に関する。
【背景技術】
【０００２】
サーバなどの情報処理装置の情報セキュリティに関して、情報処理装置が保有する暗号化されたデータと、情報処理装置内のマザーボード上に実装された暗号化されたデータを復号するためのセキュリティチップ(副処理装置)とを組み合わせて、該当するセキュリティチップが実装されたマザーボードを実装した情報処理装置でなければ暗号化されたデータを読み出すことのできない暗号機能を使用して、情報セキュリティを高める技術が実用化されている。例えば、情報処理装置においてハードディスク（ＨＤ）に記憶するデータのセキュリティを確保するために、マザーボード上に暗号キーを格納するセキュリティチップを持ち、セキュリティチップの暗号キーを用いてハードディスクのデータを暗号化及び復号化する方法が知られている。この種の技術として、特許文献１には、データ処理装置のＨＤとの間でデータの送受信を行うインタフェースボードに暗号キーを生成するキー生成部を設け、生成したキーを自己の記憶部に記憶して、データ処理装置の電源が投入されている間だけ保持することが開示されている。
【０００３】
ところで、情報処理装置内のマザーボードが故障した場合、そのマザーボード（旧マザーボード）は新しいマザーボードに保守交換される。すると、暗号化復号キーを保持するセキュリティチップもマザーボードの交換に伴って変わってしまう。この場合、旧マザーボードの基で暗号化されたデータ（例えばＨＤに記憶されたデータ）と、その暗号化データを復号するためのセキュリティチップを組み合わせた暗号機能は変わっているので、新マザーボードではその暗号化データを復旧することが困難である。
【先行技術文献】
【特許文献】

【０００４】
【特許文献１】特開２００３－１９５７５８公報
【発明の概要】
【発明が解決しようとする課題】
【０００５】
故障した旧マザーボードを新マザーボードに交換する保守作業時に、旧マザーボードが暗号化されているのか否かを識別し、保守対象の情報処理装置が当該暗号機能を使用している場合には、暗号化された情報処理装置を復旧するための特別な保守手順を行う必要がある。この特別な保守手順を行うとなると、保守作業はさらに手間取る。また、保守員が旧マザーボードを情報処理装置から取り外すと、そのマザーボードの電源がオフとなるので、当該ボードの暗号機能が有効か否か識別できないという問題がある。
【０００６】
本発明の目的は、ＡＣ電源オフの時でも暗号機能を搭載した交換可能な電子ユニットの暗号機能の有効性を識別することにある。
具体的には、情報処理装置から暗号機能を搭載したマザーボードを取り外してＡＣ電源がオフになった時でも、当該暗号機能が有効か無効かの識別を可能とすることにある。
【課題を解決するための手段】
【０００７】
本発明は、好ましくは、情報処理装置のＡＣ電源からの給電を受けて動作する電子部品を搭載し、該情報処理装置に対して着脱可能な電子ユニットにおいて、情報処理装置で扱われるデータを暗号化及び復号化するための暗号化復号キーを保持する暗号機能と、該暗号機能を有効又は無効に設定する制御手段と、電池と、該電池からの給電を受け、該暗号機能の該設定に応じて該制御手段の出力信号の状態を保持する信号保持器と、該信号保持器の出力に従って所定の通報信号を出力する通報手段と、を有することを特徴とする電子ユニットにおける暗号機能の識別装置として構成される。
【０００８】
好ましい例において、前記暗号機能として、情報処理装置で扱われるデータを暗号化及び復号化するための暗号化復号キーを保持するセキュリティチップを有し、更に該セキュリティチップが有効又は無効かの現在の設定状態を示す管理情報を格納するメモリと、外部からの操作によって、該セキュリティチップを有効又は無効にするため設定が行われるレジスタを有する、前記制御手段としての制御マイコンを有し
前記信号保持器は、該メモリに格納される該管理情報の設定に応じて、該制御マイコンの出力信号の状態を保持する。
【０００９】
また、好ましくは、前記信号保持器と前記通報手段との間にスイッチを備え、該スイッチが閉じられたときに該信号保持器の出力によって前記通報手段は該所定の通報信号を出力する。
また、好ましくは、前記電子ユニットは該情報処理装置の電子部品を搭載するマザーボードであり、該信号保持器には、該電池から及び該マザーボードの外に設置された補助電源から給電され、該マザーボードが該情報処理装置から脱状態にある時、該補助電源からの給電はオフとなる。
【００１０】
また、好ましくは、前記メモリは、該セキュリティチップが有効なときの設定値と、該セキュリティチップが無効な時の設定値と、該セキュリティチップの現在の設定値とを管理する、セキュリティ設定テーブルを記憶する。
また、好ましくは、前記通報手段はＬＥＤであり、該電子ユニットが該情報処理装置から脱状態にある時、前記信号保持器の出力に応じて該ＬＥＤは発光する。
また、好ましくは、前記信号保持器はフリップフロップであり、該フリップフロップは、該制御マイコンが設定した、該セキュリティチップの現在の設定値と同じ状態を保持する。

【発明の効果】
【００１１】
本発明によれば、ＡＣ電源オフ時に暗号機能を搭載した交換可能な電子ユニットの暗号機能の有効性を識別することが可能である。
【図面の簡単な説明】
【００１２】
【図１】本発明の実施形態による情報処理装置における暗号機能の識別装置の構成を示すブロック図。
【図２】セキュリティチップを用いたデータの暗号化処理を説明するためのフローチャート。
【図３】実施形態によるＡＣ電源オンからの初期化処理を示すフローチャート。
【図４】実施形態によるセキュリティ設定テーブルの構成を示す図。
【図５】実施形態による暗号化管理情報の設定動作を示すフローチャート。
【図６】実施形態による暗号機能の有効性の識別動作を示すフローチャート。
【発明を実施するための形態】
【００１３】
以下、図面を参照して、本発明の実施形態について説明する。
図１は、情報処理装置における暗号機能の識別装置の構成を示す。
図1において、サーバなどの情報処理装置は、所定のＯＳ（Operating System）で動作する複数のプロセッサやメモリ（図示せず）、ハードディスクドライブ（ＨＤＤ）５０を備えて構成される。一般にこれらのプロセッサやメモリ等の電子部品はプリント基板（図示せず）に搭載され、さらに複数のプリント基板はマザーボード１０に搭載される。マザーボード１０はその外に配置された電源３１に接続され、ＡＣオンされると直ちに給電を開始する補助電源３１１と、利用者の操作により給電する主電源３１２に接続される。補助電源３１１及び主電源３１２は、マザーボード１０に搭載された電子部品にＡＣ電源を供給する。
【００１４】
情報処理装置で処理されてＨＤＤ５０に記憶されるデータのセキュリティを確保するために暗号機能が設けられる。暗号機能は、暗号復号キーを格納するセキュリティチップ２１と、セキュリティチップ２１が有効か否かを示す管理情報（セキュリティの設定テーブル（図４参照））を記憶する不揮発メモリ２２と、不揮発メモリ２２に対するセキュリティ設定情報などの管理情報の読出し書き込み制御を行う制御マイコン２３により構成される。制御マイコン２３はレジスタを有し、入力装置などの外部からの操作によりその内容を変更して設定することができる。なお、制御マイコン２２は、ＨＤＤ５０に対するデータのＩ／Ｏ制御を兼ねることもある。
【００１５】
図４に示すように、セキュリティ設定テーブル４０は、セキュリティチップ２１が有効なときの設定値４０２と、セキュリティチップ２１が無効なときの設定値４０３と、現在の設定値４０１を保管する。セキュリティチップ２１に暗号化復号キーが設定されるとき（即ちセキュリティチップ２１が有効なとき）には、現在の設定値４０１に有効時の設定値４０２が格納される。一方、暗号化復号キーが設定されないとき（即ちセキュリティチップ２１が無効なとき）には、無効時の設定値４０３が格納される。
現在の設定値４０１の設定や変更は、保守員が入力装置から制御マイコン２３のレジスタの内容を設定又は変更するときの操作の一環として、行うことができる。
【００１６】
本実施例に特徴的な事項として、マザーボード１０には、保守員によるマザーボード１０の引き抜き、或いは電源の故障や給電ラインの断線等により補助電源３１１がオフしても、暗号機能が有効か否か（セキュリティチップ２１が有効か無効か）を保持して管理する構成が搭載される。即ち、マザーボード１０には、主電源３１２に接続され、主電源３１２を受けてリセット信号を出力するリセットＩＣ１２と、そのリセット端子ＲＳＴにリ

セットＩＣ１２が接続されそのクロック端子に制御マイコン２３が接続され、また補助電源３１１にダイオード１４１を介して接続されるフリップフロップ１１と、ダイオード１４２を介してフリップフロップ１１に給電する電池１３と、フリップフロップ１１の出力端子１１１に接続されるスイッチ１５、及びスイッチ１５の一端に抵抗１６を介して接続される発光ダイオード（ＬＥＤ）１７が搭載される。フリップフロップ入力端子Ｄにはフリップフロップ出力反転信号がそのまま接続されている。

【００１７】

フリップフロップ１１には、補助電源３１１からダイオード１４１を介して給電される他に、電池１３からダイオード３１１を介して給電されているので、制御マイコン２３の出力信号に応じて、その状態を保持する。即ち、フリップフロップ１１はセキュリティチップ２１が有効か無効かの状態を保持する。保守員によってスイッチ１５が閉じられると、フリップフロップ１１の保持状態に応じて、出力信号１１１がＬＥＤ１７を発光させる。保守員は、ＬＥＤ１７の発光状態を観て、セキュリティチップ２１の有効性を判断することができる。

【００１８】

次に、図２を参照して、本発明の前提となる、セキュリティチップを用いたデータの暗号化処理について説明する。

まず、最初にセキュリティチップ２１を有効化する（Ｓ２００）。即ち、情報処理装置の保守員が入力装置（図示せず）を操作して、制御マイコン２３が有するレジスタの内容を設定し、制御マイコン２３がセキュリティチップ２１と通信が行えるようする。

【００１９】

その後、情報処理装置のプロセッサが有するＯＳ上で暗号化ソフトウェアを実行し、所定の暗号化アルゴリズムに従ってＨＤＤ５０に格納されたデータを暗号化する(Ｓ２０１）。更に暗号化ソフトウェアは、暗号化されたデータの暗号化復号キーを生成して（Ｓ２０２）、そのキーをセキュリティチップ２１に格納する(Ｓ２０３）。

このように、本発明の前提となる暗号機能は、制御マイコン２３のレジスタの設定を変更することによって、セキュリティチップ２１の有効又は無効を切り替えて、セキュリティチップが有効化されている時のみデータを暗号化することができる。

【００２０】

次に図３を参照して、ＡＣ電源オンからの初期化処理について説明する。

電源３１のＡＣがオンされると、補助電源３１１の給電を開始される（Ｓ３００）。その後、主電源３１２がオンされると、主電源３１２を受けたリセットＩＣ１２はフリップフロップ１１のＲＳＴ端子に対してリセット信号１２１を出力して（Ｓ３０２）、フリップフロップ１１をリセットする（Ｓ３０３）。リセットされたフリップフロップ１１の出力信号１１１はＬｏｗになる。

【００２１】

フリップフロップ１１がリセットされた後、制御マイコン２３は、不揮発メモリ２２に保管されたセキュリティ設定テーブル４０の内容を読み込み（Ｓ３０４）、現在の設定値４０１を判別する（Ｓ３０５）。判別の結果、現在の設定値４０１が、セキュリティチップが有効な時の設定値４０２と同一の場合は制御マイコン２３からパルス信号を１回出力する（Ｓ３０６，Ｓ３０７）。一方、現在の設定値４０１が、セキュリティチップが無効な時の設定値４０３と同一の場合は、初期化処理を終了する。

この初期化処理によって、フリップフロップ１１の出力信号１１１は現在の出力状態と同じ状態を保つことができる。

【００２２】

次に、図５を参照して、暗号化管理情報の設定動作について説明する。

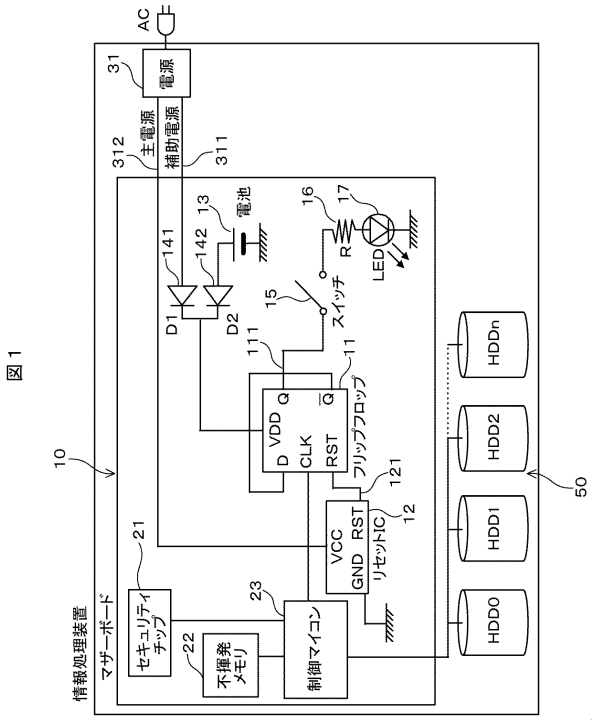
保守員が入力装置より制御マイコン２３のレジスタ設定を操作し、セキュリティチップの有効又は無効の設定を変更する（Ｓ５００）。例えば、セキュリティチップを有効にするために、セキュリティ設定テーブルの現在設定値４０１を「有効」状態に変更するように入力装置から操作する。すると、制御マイコン２３は不揮発メモリ２２に保持されたセキ

ュリティ設定テーブル４０内の現在の設定値４０１に、有効な時の設定値を書き込む(Ｓ５０１）。
その後、制御マイコン２３はフリップフロップ１１のＣＬＫ端子に対してパルス信号を1回出力して、フリップフロップ出力信号１１１を反転させる（Ｓ５０２）。この状態で、情報処理装置の暗号機能は有効に設定され、データの暗号化復号化処理が行われる。
【００２３】
その後、保守時に保守員によってマザーボード１０が取り外されて電源３１のＡＣがオフされると、補助電源３１１及び主電源３１２の給電が停止する。そのため、リセットＩＣ１２、制御マイコン２３、不揮発メモリ２２、セキュリティチップ２１の動作は停止する。しかし、フリップフロップ１１には、補助電源３１１からダイオード１４１を介して接続される他に、電池１３からダイオード１４２を介して接続されているので給電が停止されることなく、フリップフロップ１１を駆動し続けることができる。即ち、フリップフロップ１１は、ＡＣ電源オフ時にも、セキュリティ設定テーブル４０内の現在の設定値４０１が変更された（セキュリティが有効に設定されている）旨の信号を保持し続ける。また、フリップフロップ１１の出力信号１１１はスイッチ１５を押下しない限り電流が流れないので、長期間フリップフロップ１１の状態を保持することができる。
【００２４】
次に、図６を参照して、電源のＡＣがオフした時の暗号機能の有効性の識別動作について説明する。
保守員は、マザーボード１０を情報処理装置から取り外した時、マザーボード１０のスイッチ１５を押して（Ｓ６００）、ＬＥＤ１７が点灯しているかを確認する（Ｓ６０１）。このとき、マザーボード１０のセキュリティチップ２１が有効化されていると、フリップフロップ１１の出力端子１１１にＨｉｇｈレベルの信号が出力される。一方、セキュリティチップ２１が無効化されていると、フリップフロップの出力端子１１１にはＬｏｗレベルの信号が出力される。そこで、保守員はＬＥＤ１７の点灯状態を見て、それが点灯している場合は情報処理装置が暗号化されている（セキュリティチップが有効）と判断でき（Ｓ６０３）、ＬＥＤ１７が点灯していない場合は情報処理装置が暗号化されていない（セキュリティチップが無効化）と判断できる（Ｓ６０４）。
【００２５】
以上、本発明の一実施形態について説明したが、本発明は上記実施形態に限定されずに、種々変形、応用して実施し得る。
例えば、図１に示す識別装置の構成においてスイッチ１５は必須ではない。スイッチ１５を要する理由は、保守員がマザーボードを取り外して後々にスイッチをオンにしてフリップフロップ１１の出力信号からＬＥＤ１７の点灯状況を観る。しかし、マザーボードを取り外した直後にＬＥＤの点灯状態を観るような作業要領にしておけば、あえてスイッチを設ける必要はない。この場合でも、電池１３の保持時間はＬＥＤが点灯し続ける。
【００２６】
また、他の変形例として、情報処理装置が暗号化されているか否か（即ち暗号機能の有効性）を保守員に知らせる通知手段としては、ＬＥＤ１７などの光学的手段に限らない。保守員に警報するための特殊な音を発する音発生手段でもよい。更に保守員が保守時に携帯端末装置又はＰＣ（パーソナルコンピュータ）等の装置を携帯している場合には、それらの装置に警報を表示するための特別な信号を送信する無線信号の発信手段でもよい。
【００２７】
また、他の変形例として、上記実施形態では、セキュリティ設定テーブル４０を用いてセキュリティチップの現在の有効性を管理しているが、このテーブルは必ずしも不揮発メモリに記憶しなくてもよい。例えば、制御マイコン内の汎用レジスタに保管してもよい。また他の変形例として、セキュリティ設定テーブルのようなテーブル構成である必要はない。テーブル構成を用いない場合、例えば、制御マイコン内にセキュリティチップの現在の状態を管理するフラグを設け、或いは前記暗号化ソフトウェアの中にその管理フラグを持たせるようにしてもよい。

【００２８】
また他の応用例として、情報処理装置はサーバに限定されないし、交換可能なマザーボードに限定されない。例えば、デジタルカメラで交換可能なプリント基板やメモリチップなどに暗号機能を搭載している場合、或いはデジタルテレビやデジタルビデオに着脱可能に装着されるハードディスクドライブ（ＨＤＤ）やＤＶＤ、メモリカード、プリント基板などに暗号機能を搭載している場合、これらやＨＤＤやＤＶＤ等の電子ユニットに上記実施例と同様の暗号機能の識別装置を搭載することも可能である。
【符号の説明】
【００２９】
１０：マザーボード　２１：セキュリティチップ　２２：不揮発メモリ　２３：制御マイコン　３１：電源　５０：ＨＤＤ
１１：フリップフロップ　１２：リセットＩＣ　１３：電池　１４１，１４２：ダイオード　１５：スイッチ　１６：抵抗　１７：ＬＥＤ
４０：セキュリティ設定テーブル。

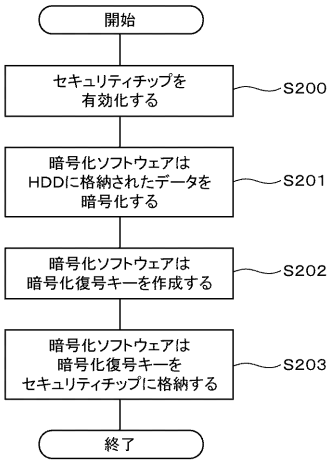
【図１】

図１



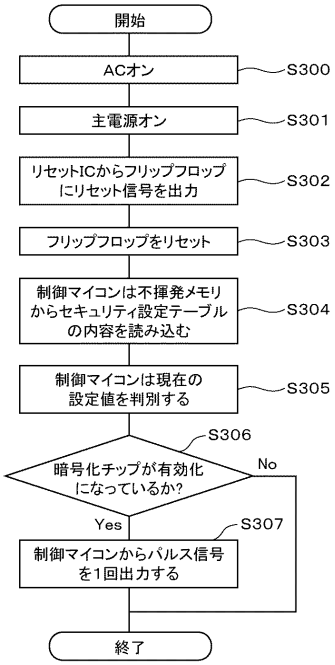
【図２】

図２



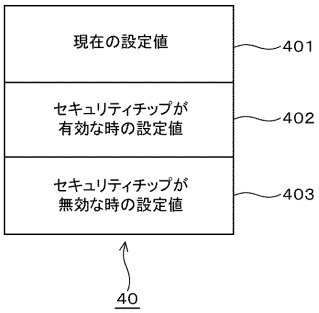
【図３】

図３



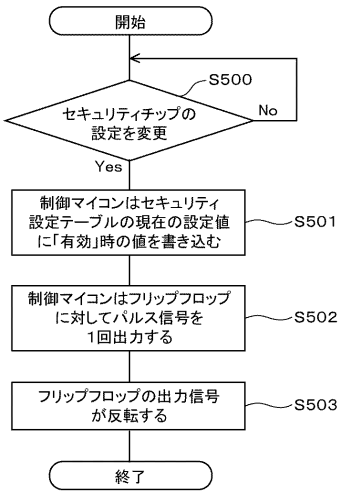
【図４】

図４



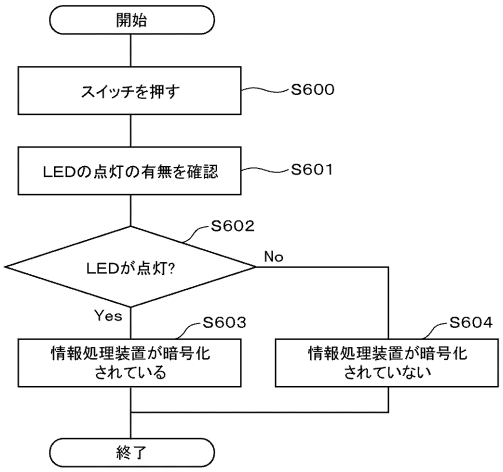
【図５】

図５



【図６】

図６



フロントページの続き

(72)発明者　森田　裕介
神奈川県横浜市西区みなとみらい二丁目３番３号　日立情報通信エンジニアリング株式会社内
(72)発明者　秋葉　正洋
神奈川県秦野市堀山下１番地　株式会社日立製作所　エンタープライズサーバ事業部内
(72)発明者　米田　淳一
神奈川県秦野市堀山下１番地　株式会社日立製作所　エンタープライズサーバ事業部内

審査官　青木　重徳

(56)参考文献　特開２００８－０３５４４９（ＪＰ，Ａ）
特開２００９－２４５０２０（ＪＰ，Ａ）
特開２００７－００５８５５（ＪＰ，Ａ）
特開２００５－２３６６０５（ＪＰ，Ａ）
特開２００６－３１３９７５（ＪＰ，Ａ）
特開２００９－０４４４０７（ＪＰ，Ａ）
特開平０６－０２７８７８（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／１０
Ｇ０６Ｆ　　１／００