

(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有權機關
國際事務局



(43) 国際公開日
2007年8月16日(16.08.2007)

PCT

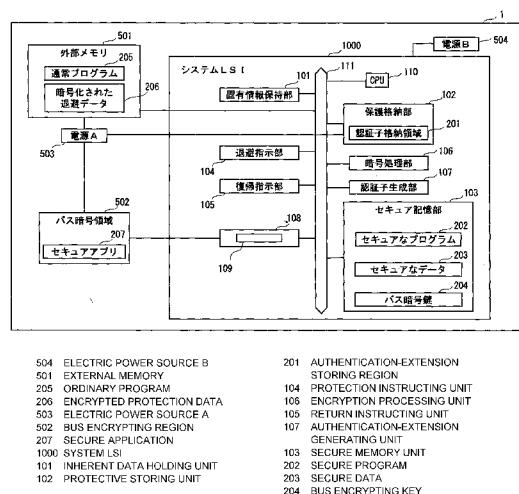
(10) 国際公開番号
WO 2007/091492 A1

- | | | |
|--|-----------------------------|--|
| (51) 国際特許分類:
<i>G09C 1/00</i> (2006.01)
<i>H04L 9/10</i> (2006.01) | <i>H04L 9/32</i> (2006.01) | (72) 発明者; および
(75) 発明者/出願人(米国についてのみ): 伊藤 孝幸 (ITO, Takayuki). 井藤 好克 (ITO, Yoshikatsu). |
| (21) 国際出願番号: | PCT/JP2007/051804 | (74) 代理人: 中島 司朗, 外(NAKAJIMA, Shiro et al.); 〒5310072 大阪府大阪市北区豊崎三丁目 2 番 1 号淀川 5 番館 6 F Osaka (JP). |
| (22) 国際出願日: | 2007 年 2 月 2 日 (02.02.2007) | |
| (25) 国際出願の言語: | 日本語 | (81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW. |
| (26) 国際公開の言語: | 日本語 | |
| (30) 優先権データ:
特願2006-028580 2006 年 2 月 6 日 (06.02.2006) JP | | |
| (71) 出願人(米国を除く全ての指定国について): 松下電器産業株式会社 (MATSUSHITA ELECTRIC INDUSTRIAL CO.,LTD.) [JP/JP]; 〒5718501 大阪府門真市大字門真 1006 番地 Osaka (JP). | | |

[繰葉有]

(54) Title: SECURE PROCESSING DEVICE, METHOD AND PROGRAM

(54) 発明の名称: セキュア処理装置、方法、プログラム



(57) Abstract: A secure processing device used for a built-in apparatus or the like is provided with a power saving mode. The secure processing device calculates a hash value of the secure data subjected to protection when shifting to the power saving mode. The calculated hash value is stored in a protective storing unit in the secure processing device in which memory data are not vanished in the power saving mode. The secure processing device encrypts the secure data, stores so encrypted secure data in an external memory, and shifts to the power saving mode. When the secure processing device returns to an ordinary mode, the secure processing device decrypts the encrypted data stored in the external memory. The secure processing device calculates a hash value of the decrypted data and compares the same with the hash value stored in the protective storing unit. If the hash values are consistent with each other, the secure processing device stores the decrypted data in the protective storing unit. If the hash values are inconsistent with each other, the secure processing device discards the decrypted data or the encrypted data stored in the outer memory.

(57) 要約: 組み込み機器等に用いられ、省電力モードを備えるセキュア処理装置であって、省電力モードへの移行時に、退避させる対象となるセキュアなデータのハッシュ値を計算する。計算したハッシュ値を、省電力モード時においても記憶内容が消失しないセキュア処理装置内部の保護格納部に格納する。セキュアなデータを暗号化して外部メモリに記憶させ、省電力モードへ移行する。通常電力モードへ復帰する時に、外部メモリに記憶させ

[續著有]



(84) 指定国(表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

添付公開書類:
— 国際調査報告書

明細書

セキュア処理装置、方法、プログラム

技術分野

[0001] 本発明は、秘匿すべき保護データを安全に処理するための機構を有し、通常電力モードおよび省電力モードにより動作することができるセキュア処理装置に関し、特に、通常電力モードと省電力モードとの切り替えの前後において、保護データを安全に外部メモリへ退避させ、また、省電力モードからの復帰を安全に行うための技術に関する。

背景技術

[0002] 音楽データなどに代表されるコンテンツにかかるデータが不正に複製されたり、コンテンツを再生するためのプログラムが不正に改ざん等されると、著作権者等の不利益となる。そのため、著作権者等にとっては、これらの高い価値を有するデータにかかる処理が安全に行われることが望ましい。

この要望に応えるため、秘匿すべき保護データを用いた処理を安全に実行することができるセキュア処理装置が提供されている。

[0003] セキュア処理装置としては、例えば、セキュアメモリを内部に含んだ集積回路がある。このセキュアメモリは、外部からの不正アクセスを防止する機構を有している。具体的には、この集積回路では、セキュアメモリにアクセスすることができるのは、集積回路内部のCPUのみである。そして、集積回路内部のCPUの動作モードがセキュアモードのときに限り、CPUは、セキュアメモリにアクセスすることができる。

[0004] このように、セキュア処理装置は、秘匿すべき保護データを保持する記憶領域にアクセスすることができる主体およびアクセスできる機会を制限することで、データの秘匿を実現している。

ところで、セキュア処理装置には、動作モードとして、通常電力モードおよび省電力モードを切り換えて動作するものがある。省電力モードで動作している間、セキュア処理装置は、電源の供給が制限され、また、CPUをスリープモードに移行させる等、機能の一部を制限することで、消費電力を小さくして動作する。省電力モードを備えた

セキュア処理装置は、例えば、バッテリー駆動により動作する携帯機器等で用いられる。こうすることで、携帯機器は、音楽データ等の秘匿すべき保護データを用いた処理を、セキュア処理装置により安全に行いつつ、動作時間を長くすることができる。

[0005] また、セキュア処理装置の、外部からの不正アクセスを防止する機構を有している記憶領域は、CPUによる高速アクセスを可能にするため、通常、揮発性のメモリが用いられる。そのため、セキュア処理装置が省電力モードに移行すると、上記記憶領域に保持されているデータが消失する。したがって、音楽データや音楽再生用の重要なプログラム等が上記記憶領域でのみ保持されている場合、セキュア処理装置が省電力モードに移行するたびに、当該データやプログラムが消失することになる。

[0006] この場合、セキュア処理装置を組み込んだ機器のユーザにとって不都合が生じることがある。

具体的に、セキュア処理装置を組み込んだ携帯機器のユーザが音楽データを再生している場合を例に、上述したユーザの不都合を説明する。携帯機器が音楽データを再生している途中に、携帯機器が省電力モードに移行したとする。この後、省電力モードから復帰して、音楽データの続きを再生しようとしても、上記記憶領域の音楽データが消失している。そのため、再度、上記記憶領域に音楽データが読み込まれるまでユーザが待たされたり、音楽データの再生位置等の情報が消失して音楽データの先頭からしか再生できないなどの望ましくない事態が生じることがある。

[0007] そこで、セキュア処理装置を省電力モードへ移行させる際に、上記記憶領域に保持されているデータを、セキュア処理装置の外部にある外部メモリに退避させる技術が従来用いられている。そして、セキュア処理装置を省電力モードから復帰させる際に、外部メモリに退避させたデータを、上記記憶領域に再設定する。これにより、セキュア処理装置は、省電力モード移行前後の処理を継続して行うことができ、ユーザの不都合が発生しないようにすることができる。

[0008] ただし、この技術を用いる場合、セキュア処理装置に異常なデータが再設定されると、セキュア処理装置が暴走する可能性がある。そのため、外部メモリへのデータの退避と、セキュア処理装置へのデータの再設定は、異常なく行われることが望ましい。

この課題を解決するため、下記の特許文献1には、正常な手順で外部メモリへのデータの退避が行えるようにすることを目的とする技術が開示されている。具体的には、まず、省電力モードへの移行を開始すると、キーワードをレジスタに設定する。次に、外部メモリへデータを退避させる前に、キーワードとレジスタの内容とが一致するか判断し、一致する場合にデータの退避を実行する。

- [0009] この技術によると、セキュア処理装置が暴走等により、キーワードをレジスタに設定する処理を飛ばして省電力モードに移行する処理を実行しようとしたとしても、キーワードとレジスタの内容とが一致しないので、異常終了する。

特許文献1: 日本国特許公開公報 特開平5-143478号公報

発明の開示

発明が解決しようとする課題

- [0010] 上記特許文献1の技術を用いると、異常な手順で省電力モードへ移行する事態を防ぐことができる。すなわち、暴走等によりセキュア処理装置が省電力モードへ移行するのを回避できる。したがって、外部メモリへ退避するデータを適切なものとすることはできる。

しかし、特許文献1記載の技術を用いたとしても、退避したデータが改ざんされたり破損したりすると、省電力モードから復帰するときに、セキュア処理装置に、異常なデータが再設定されることとなる。すなわち、省電力モードからの復帰が安全に行われないという問題がある。例えば外部メモリに退避させたデータが改ざんされて、不正なプログラム等がセキュア処理装置に再設定されて実行される可能性がある。その結果、例えば上記記憶領域のデータを外部に出力させるような処理が行われて、秘匿すべき保護データが暴露されるなどの事態が発生しうる。

- [0011] そこで、本発明は、省電力モードを備えるセキュア処理装置において、秘匿すべき保護データを外部メモリへ安全に退避し、かつ、外部メモリへ退避させたデータをセキュア処理装置に安全に再設定することを可能とする技術を提供することを目的とする。

課題を解決するための手段

- [0012] 上記課題を解決するため、本発明のセキュア処理装置は、動作モードとして、通常

電力モードと、省電力モードとを切り換えて動作し、前記通常電力モード時には、秘匿すべき保護データに係る処理を少なくとも実行し、前記省電力モード時には、前記保護データを、外部メモリにおいて安全に保持するセキュア処理装置であって、データの暗号化および復号化を行う暗号処理部と、データの内容に依存して定まり、当該データよりもデータサイズが小さい認証子を生成する生成部と、自装置外部からの不正アクセスを防止する機構を有し、前記省電力モード時において、記憶内容が消失するメモリにより構成され、前記保護データを記憶するためのセキュア記憶部と、前記通常電力モードまたは前記省電力モードのいずれの動作時であっても記憶内容を保持する機構、および、自装置外部からの不正アクセスを防止する機構を有し、前記セキュア記憶部よりも記憶容量が小さい保護格納部と、前記省電力モードへの移行時に、前記保護データに基づいて、前記生成部に第1認証子を生成させ、生成された当該第1認証子を前記保護格納部に格納させるとともに、前記保護データを前記暗号処理部に暗号化させ、得られた暗号化データを前記外部メモリに記憶させるよう制御する移行制御部と、前記通常電力モードへの復帰時に、前記外部メモリに記憶された前記暗号化データを前記暗号処理部に復号化させ、得られた復号化データに基づいて、前記生成部に第2認証子を生成させる認証子生成制御部と、生成された前記第2認証子と、前記保護格納部に格納されている前記第1認証子とが一致するか否かを判断する判断部と、一致しないと判断されると、前記復号化データの前記セキュア記憶部への書き込みを禁止し、一致すると判断されると、前記復号化データを前記セキュア記憶部へ書き込む復帰制御部とを備えることを特徴とする。

発明の効果

- [0013] 上述の構成を備えるセキュア処理装置は、省電力モードへの移行時に、保護データに基づいて第1認証子を生成する。また、通常電力モードへの復帰時に、セキュア記憶部に再設定する対象となるデータに基づいて第2認証子を生成し、第2認証子と、省電力モードへの移行時に生成した第1認証子とを比較することで、外部メモリに退避させたデータの再設定を行うか否かを制御するという技術的特徴を有している。
- [0014] 生成部により生成される認証子は、生成の元となるデータに依存して定まる。したがって、セキュア処理装置は、第1認証子と第2認証子とを比較することにより、セキュア

記憶部に再設定する対象となるデータが、外部メモリに退避させたデータと同一か否かを判断することができる。

同一であれば、データをセキュア記憶部に再設定する。同一でなければ、退避させたデータが、改ざん等により、異常なデータになっていると推定できるので、当該データをセキュア記憶部に書き込まない。

- [0015] こうすることで、セキュア処理装置は、異常なデータを再設定しないですみ、外部メモリへ退避させたデータを、安全に再設定することができる。

また、セキュア処理装置は、外部メモリへデータを退避させる際に、暗号化部により、退避にかかるデータを暗号化する。そして、暗号化したデータを外部メモリへ退避させる。したがって、セキュア処理装置は、秘匿すべき保護データを安全に外部メモリに退避させることができる。

- [0016] また、上述の構成において、生成部は、認証子を生成する対象となるデータよりもデータサイズが小さい認証子を生成するので、認証子を格納する保護格納部は、セキュア記憶部よりもメモリ領域を小さくできる。

したがって、上述の構成を備えるセキュア処理装置は、秘匿すべき保護データを安全に処理しつつ、省電力化を実現し、さらに、装置の大型化を避けることができる。例えば、セキュア処理装置が集積回路の場合、回路の大型化を避けることができる。そのため、小型化の要請が強い集積回路において、上述の技術的特徴を有するセキュア処理装置を容易に実現することができる。

- [0017] ところで、セキュア処理装置が高速で所定の処理を行うには、重要なデータを記憶するセキュア記憶部の記憶容量が十分ではない場合がある。この場合は、重要なプログラムなどのデータを所定の暗号鍵を用いて暗号化する。この暗号鍵を、以下、バス暗号鍵という。セキュア処理装置は、バス暗号鍵を安全に保持する。また、バス暗号鍵を用いて暗号化したデータを、外部の記憶領域に記憶させる。この外部の記憶領域を、以下、バス暗号領域といふ。

- [0018] このような構成により、セキュア処理装置は、セキュア記憶部の記憶容量が十分ではない場合も、秘匿すべき保護データを用いて安全に処理を行うことができる。

しかし、省電力モードへの移行時に、セキュア処理装置において保持しているバス

暗号鍵が消失してしまうと、バス暗号領域のデータを復号するための鍵が無くなり、処理を再開できなくなる。

[0019] ここで、セキュア処理装置が、例えば装置に固有な情報等の、変化しない情報に基づいて、1のバス暗号鍵をいつでも生成することができ、これによって生成されたバス暗号鍵を用い続けるとする。この場合、確かに、省電力モードへ移行してバス暗号鍵が消失したとしても、再度、同一のバス暗号鍵を生成することができるので、通常電力モードへの復帰後、再度生成したバス暗号鍵を用いて、バス暗号領域のデータを復号化することはできる。

[0020] しかし、バス暗号領域のデータを復号するためのバス暗号鍵がいつまでも同じであると、不正者がバス暗号領域のデータを解析する等により、バス暗号鍵が解読され、バス暗号領域に保持されている重要なデータが暴露されるおそれがある。そのため、バス暗号鍵は、隨時変更されることが望ましい。

このように、セキュア処理装置が1のバス暗号鍵を用い続けないことを前提とすると、セキュア処理装置は、省電力モードへの移行後、通常電力モードへ復帰したときに、バス暗号鍵が消失していると、バス暗号領域のデータを用いた処理を再開できなくなる。そのため、再度、バス暗号領域にデータを書き込む等の不要な処理が必要となる。

[0021] この問題に対処すべく、バス暗号領域において保持されている重要なデータについても、省電力モードへの移行後、通常電力モードへの復帰時に、上述のセキュア記憶部のデータと同様に、処理の継続等を可能とすることが望ましい。

そこで、前記セキュア処理装置は、さらに、バス暗号鍵を用いて暗号化したデータを、外部の記憶領域であるバス暗号領域に保持させ、前記バス暗号領域に保持されているデータを用いて安全に処理を行うものであり、前記セキュア記憶部は、さらに、前記バス暗号鍵を記憶し、前記移行制御部は、前記省電力モードへの移行時に、前記セキュア記憶部に記憶されている前記バス暗号鍵を暗号化し、暗号化されたバス暗号鍵を前記外部メモリに記憶させるよう制御するバス暗号鍵退避制御部を含み、前記復帰制御部は、前記外部メモリに記憶された前記暗号化されたバス暗号鍵を復号化するバス暗号鍵復号化制御部と、前記バス暗号鍵復号化制御部により復号化さ

れたバス暗号鍵を、前記セキュア記憶部へ書き込むバス暗号鍵再設定部を含むこととしてもよい。

[0022] このような構成により、バス暗号領域のデータについても、省電力モードへの移行の前後において、処理の継続等を行うことができるので、通常電力モードへの復帰後、処理を再開するまでの時間を短くすることができる。

なお、上記のようにバス暗号領域およびバス暗号鍵を用いるセキュア処理装置は、処理を高速化するために、所定の回路やレジスタ等を用いて実現されることがある。

[0023] 具体的には、前記セキュア処理装置は、前記バス暗号鍵を保持し、前記省電力モードへの移行が完了すると、保持内容が消失するバス暗号鍵設定レジスタと、前記バス暗号鍵設定レジスタに保持されているバス暗号鍵を用いて、前記バス暗号領域へ出力するデータの暗号化、および、前記バス暗号領域から出力されるデータの復号化を行うバス暗号回路を含み、前記セキュア記憶部が記憶している前記バス暗号鍵は、前記バス暗号鍵設定レジスタに保持されている前記バス暗号鍵と同一であり、前記バス暗号鍵再設定部は、前記バス暗号鍵復号化制御部により前記復号化されたバス暗号鍵を、前記バス暗号鍵設定レジスタに保持させるという構成を有していてもよい。

[0024] このような構成により、バス暗号領域を用いた処理を、安全かつ高速に行うことができる。

さらに、上述のバス暗号領域を用いた処理を行う場合、安全性をより高めるには、例えば重要なデータ1つ1つに対し、異なるバス暗号鍵を用いることが望ましい。仮に1のバス暗号鍵が解読されたとしても、他のバス暗号鍵を用いたデータは暴露されないためである。

[0025] 上述の技術は、例えば、バス暗号回路とバス暗号鍵設定レジスタとの組を複数備え、重要なデータ1つ1つを、バス暗号回路とバス暗号鍵設定レジスタとの組のそれぞれに対応させることで実現できる。ただし、この場合、バス暗号鍵設定レジスタが複数あるので、セキュア処理装置が省電力モードへ移行する際に、複数のバス暗号鍵設定レジスタに保持されている各バス暗号鍵を読み出そうとすると、バス暗号鍵を保持しているレジスタの特定やバス暗号鍵の読み出し等の処理を要する。そのため、省電

力モードへの移行が遅れたり、また、省電力モードへの移行が完了するまでに、バス暗号鍵の外部メモリへの退避が間に合わないおそれがある。

- [0026] そこで、前記セキュア処理装置は、前記バス暗号鍵設定レジスタと、前記バス暗号回路とからなる組を複数備え、前記バス暗号鍵設定レジスタと前記バス暗号回路とかなる組のそれぞれは、前記バス暗号領域に保持されているデータそれぞれと対応しており、前記セキュア記憶部は、前記バス暗号鍵設定レジスタそれぞれが保持している複数のバス暗号鍵それぞれと同一のバス暗号鍵を記憶しており、前記バス暗号鍵退避制御部は、前記省電力モードへの移行時に、前記セキュア記憶部により記憶されている複数の前記バス暗号鍵を前記暗号化し、暗号化された複数のバス暗号鍵を前記外部メモリに前記記憶させ、前記バス暗号鍵復号化制御部は、複数の前記バス暗号鍵を前記復号化し、前記バス暗号鍵再設定部は、復号された前記複数の前記バス暗号鍵を、前記セキュア記憶部へ書き込むこととしてもよい。
- [0027] 上述の構成によると、セキュア記憶部は、バス暗号鍵設定レジスタに保持されている複数のバス暗号鍵と同一のバス暗号鍵をそれぞれ保持している。そのため、セキュア処理装置は、省電力モードへの移行時に、バス暗号鍵を退避させるバス暗号鍵設定レジスタの特定や探索等を行うことなく、バス暗号鍵等の外部メモリへの退避を行うことができる。したがって、省電力モードへの移行時に、外部メモリへのデータの退避が間に合わない等のおそれを回避することができる。
- [0028] ところで、消費電力をより低下させたい場合は、省電力モード時において、必要な電源の供給を少なくすることが望ましい。
- そこで、前記保護格納部は、不揮発性のメモリにより構成されることとしてもよい。
- 上述の構成によると、保護格納部は電源電圧を供給しなくとも記憶内容を保持するので、保護格納部に揮発性メモリを用いる場合と比べると、セキュア処理装置の消費電力を低下させることができる。
- [0029] 一方、セキュア処理装置の安全性を高めたい場合には、保護格納部を以下の構成とすることもできる。
- すなわち、前記保護格納部は、揮発性のメモリであり、前記省電力モード時においても電力が供給される構成を有することとしてもよい。

仮に、何らかの不正な解析手段により、保護格納部に記憶されている認証子が暴露されてしまうとする。この場合、認証子に基づいて、元のデータが不正者に推定されたり、暴露されたのと同一の認証子が生成部により生成されるように、不正なデータを不正者が作成するおそれがある。

- [0030] このようなおそれに対し、上述の構成を備えるセキュア処理装置によると、保護格納部は、揮発性のメモリであるため、省電力モード時には記憶内容を保持する。そして、セキュア処理装置の電源がオフになると、保護格納部の記憶内容が消失する。そのため、セキュア処理装置が電源オフの場合に、保護格納部が解析されて認証子が不正に暴露されるのを防ぐことができる。また、耐タンパ性などの対策をとる必要もない。
- [0031] すなわち、簡易な構成で、不正な解析に対するセキュア処理装置の安全性を高めることができる。

また、生成部による認証子の生成方法に関連して、セキュア処理装置の安全性をより高めるには、以下の構成としてもよい。

すなわち、前記生成部は、データの内容に基づいて、ハッシュ関数によりハッシュ値を算出し、前記生成部が生成する前記認証子とは、前記算出されたハッシュ値であることとしてもよい。

- [0032] ハッシュ関数とは、あるデータから固定長の擬似乱数を生成する関数である。メッセージダイジェスト関数ともいう。ハッシュ関数により生成された値は、ハッシュ値と呼ばれる。ハッシュ関数は、不可逆な一方方向関数を含むため、算出されたハッシュ値から、元のデータを推測するのが困難という特徴がある。また、ハッシュ関数は、あるデータとハッシュ値が等しい別のデータを容易に生成できないという特徴も有する。
- [0033] したがって、上述の構成によると、仮に保護格納部に記憶されている認証子が暴露されたとしても、認証子を生成する元となったデータ、すなわち秘匿すべき保護データが推測されるのを困難にすることができます。また、暴露された認証子が生成されるように、不正者が不正なデータを作成し、外部メモリに記憶させるのも困難となる。

ここで、外部メモリへ退避したデータと、外部メモリから再設定する対象となるデータとが異なる場合、すなわち、外部メモリへ退避したデータが改ざん等されている場合

に、セキュア処理装置の安全性を高めるために、以下の構成とすることもできる。

[0034] すなわち、前記復帰制御部は、前記判断部により一致しないと判断されると、前記外部メモリに記憶された前記暗号化データを消去する消去部と、前記暗号処理部により復号化された前記復号化データを破棄する破棄部とを含むこととしてもよい。

上述の構成によると、改ざん等がなされたおそれのある異常なデータをセキュア処理装置および外部メモリから完全に消去するので、このような異常なデータを誤ってセキュア処理装置が実行するおそれをなくすことができる。

[0035] また、外部メモリに退避させた保護データが改ざんされているにせよ、改ざんされていないにせよ、セキュア処理装置が通常電力モードに復帰した後においても、外部メモリに退避させたデータをそのまま外部メモリに残しておくことは望ましくない。不正な解析等によって保護データが解読されるおそれがあるからである。

そこで、前記セキュア処理装置は、前記通常電力モードへの復帰時に、前記外部メモリに記憶された前記暗号化データを消去するデータ消去部を含むこととしてもよい。

[0036] これにより、外部メモリにデータを退避させる期間を最小限にすることができる、不正者が外部メモリの暗号化データにアクセスしたり、不正な解析を行うおそれを小さくすることができる。

一方、外部メモリに退避させた保護データを、不正に利用されないようにするには、以下の構成とすることもできる。

[0037] すなわち、前記セキュア処理装置は、さらに、自装置を識別する情報である装置固有情報を保持する固有情報保持部を含み、前記暗号化部は、前記保持されている装置固有情報に基づいた暗号鍵を用いて、前記暗号化および前記復号化を行うこととしてもよい。

上述の構成によると、外部メモリに退避されるデータは、装置固有情報に基づいて暗号化されたデータである。すなわち、外部メモリに退避されるデータは、暗号化を行った装置のみが、復号化することができる。

[0038] したがって、外部メモリに退避されたデータが他の装置に読み込まれて不正に解析される等の不正行為を困難にすることができる。

上述の構成において、セキュア処理装置の安全性の観点からは、以下の構成にすることが望ましい。

すなわち、前記固有情報保持部は、自装置外部からの不正アクセスを防止する機構を有していることとしてもよい。

[0039] これにより、固有情報保持部から装置固有情報が不正に漏洩するおそれが小さくなる。したがって、暗号化されたデータの復号がより困難になるので、セキュア処理装置の安全性を、より一層、高めることができる。

ところで、上述の構成では、外部メモリへデータを退避させる際、暗号化を行う前のセキュア記憶部のデータに基づいて、生成部により第1認証子を生成している。しかし、生成部が認証子を生成するタイミングは、これに限られるものではない。

[0040] したがって、本発明のセキュア処理装置は、動作モードとして、通常電力モードと、省電力モードとを切り換えて動作し、前記通常電力モード時には、秘匿すべき保護データに係る処理を少なくとも実行し、前記省電力モード時には、前記保護データを、外部メモリにおいて安全に保持するセキュア処理装置であって、データの暗号化および復号化を行う暗号処理部と、データの内容に依存して定まり、当該データよりもデータサイズが小さい認証子を生成する生成部と、自装置外部からの不正アクセスを防止する機構を有し、前記省電力モード時において、記憶内容が消失するメモリにより構成され、前記保護データを記憶するためのセキュア記憶部と、前記通常電力モードまたは前記省電力モードのいずれの動作時であっても記憶内容を保持する機構、および、自装置外部からの不正アクセスを防止する機構を有し、前記セキュア記憶部よりも記憶容量が小さい保護格納部と、前記省電力モードへの移行時に、前記保護データを前記暗号処理部に暗号化させ、得られた暗号化データを前記外部メモリに記憶させるとともに、前記暗号化データに基づいて、前記生成部に第1認証子を生成させ、生成された当該第1認証子を前記保護格納部に格納させる移行制御部と、前記通常電力モードへの復帰時に、前記外部メモリに記憶された前記暗号化データに基づいて、前記生成部に第2認証子を生成させる認証子生成制御部と、生成された前記第2認証子と、前記保護格納部に格納されている前記第1認証子とが一致するか否かを判断する判断部と、一致しないと判断されると、前記外部メモリに記憶さ

れた前記暗号化データを前記セキュア記憶部へ書き込むための処理を制限し、一致すると判断されると、前記暗号化データを前記暗号処理部に復号化させ、得られた復号化データを前記セキュア記憶部へ書き込む復帰制御部とを備えることを特徴としてもよい。

[0041] また、上述の構成において、前記復帰制御部は、前記判断部により一致しないと判断されると、前記暗号化データの前記暗号処理部による復号化を実行しないことで、前記制限を行うこととしてもよい。

上述の構成によると、セキュア処理装置は、生成部により生成された第2認証子と第1認証子とを比較し、比較結果に応じて、外部メモリに記憶された暗号化データを復号化するか否かを制御する。すなわち、セキュア処理装置は、負荷の大きい復号化処理が行われる前に、外部メモリに退避されたデータが異常なデータであるかを判断する。

[0042] 外部メモリに退避されたデータが異常である場合には、復号化処理を行わないとすることでセキュア処理装置の処理負荷を軽減できる。また、異常なデータを検出した時に、異常なデータに対する対策にかかる処理、例えば異常終了などを迅速に行うことができる。

また、上述の構成においても、外部メモリに退避させたデータを、セキュア処理装置が通常電力モードに復帰した後もそのまま外部メモリに残しておくことは望ましくない。

[0043] そこで、前記復帰制御部は、前記判断部により一致しないと判断されると、前記外部メモリに記憶された前記暗号化データを消去する消去部を含むこととしてもよい。

上述の構成によると、改ざん等のおそれのある異常なデータを外部メモリから消去することができるので、このような異常なデータを誤ってセキュア処理装置が実行するおそれなくすことができる。

[0044] また、本発明は、動作モードとして、通常電力モードと、省電力モードとを切り換えて動作し、前記通常電力モード時には、秘匿すべき保護データに係る処理を少なくとも実行し、前記省電力モード時には、前記保護データを、外部メモリにおいて安全に保持するセキュア処理装置において用いられる、情報処理方法であって、前記セ

キュア処理装置は、自装置外部からの不正アクセスを防止する機構を有し、前記省電力モード時において、記憶内容が消失するメモリにより構成され、前記保護データを記憶するためのセキュア記憶部と、前記通常電力モードまたは前記省電力モードのいずれの動作時であっても記憶内容を保持する機構、および、自装置外部からの不正アクセスを防止する機構を有し、前記セキュア記憶部よりも記憶容量が小さい保護格納部とを有し、前記情報処理方法は、データの暗号化および復号化を行う暗号処理ステップと、データの内容に依存して定まり、当該データよりもデータサイズが小さい認証子を生成する生成ステップと、前記セキュア処理装置が前記省電力モードへ移行する時に、前記セキュア記憶部に記憶されている前記保護データに基づいて、前記生成ステップの実行により第1認証子を生成し、生成された当該第1認証子を前記保護格納部に格納させるとともに、前記保護データを前記暗号処理ステップの実行により暗号化し、得られた暗号化データを前記外部メモリに記憶させるよう制御する移行制御ステップと、前記セキュア処理装置が前記通常電力モードへ復帰する時に、前記外部メモリに記憶された前記暗号化データを前記暗号処理ステップの実行により復号化し、得られた復号化データに基づいて、前記生成ステップの実行により第2認証子を生成するよう制御する認証子生成制御ステップと、生成された前記第2認証子と、前記保護格納部に格納されている前記第1認証子とが一致するか否かを判断する判断ステップと、前記判断ステップにおいて一致しないと判断されると、前記復号化データの前記セキュア記憶部への書き込みを禁止し、一致すると判断されると、前記復号化データを前記セキュア記憶部へ書き込む復帰制御ステップとを含むこととしてもよい。

[0045] また、本発明は、動作モードとして、通常電力モードと、省電力モードとを切り換えて動作し、前記通常電力モード時には、秘匿すべき保護データに係る処理を少なくとも実行し、前記省電力モード時には、前記保護データを、外部メモリにおいて安全に保持するセキュア処理装置の動作を制御する制御プログラムであって、前記セキュア処理装置は、自装置外部からの不正アクセスを防止する機構を有し、前記省電力モード時において、記憶内容が消失するメモリにより構成され、前記保護データを記憶するためのセキュア記憶部と、前記通常電力モードまたは前記省電力モードのい

ずれの動作時であっても記憶内容を保持する機構、および、自装置外部からの不正アクセスを防止する機構を有し、前記セキュア記憶部よりも記憶容量が小さい保護格納部とを有し、前記制御プログラムは、データの暗号化および復号化を行う暗号処理ステップと、データの内容に依存して定まり、当該データよりもデータサイズが小さい認証子を生成する生成ステップと、前記セキュア処理装置が前記省電力モードへ移行する時に、前記セキュア記憶部に記憶されている前記保護データに基づいて、前記生成ステップの実行により第1認証子を生成し、生成された当該第1認証子を前記保護格納部に格納させるとともに、前記保護データを前記暗号処理ステップの実行により暗号化し、得られた暗号化データを前記外部メモリに記憶させるよう制御する移行制御ステップと、前記セキュア処理装置が前記通常電力モードへ復帰する時に、前記外部メモリに記憶された前記暗号化データを前記暗号処理ステップの実行により復号化し、得られた復号化データに基づいて、前記生成ステップの実行により第2認証子を生成するよう制御する認証子生成制御ステップと、生成された前記第2認証子と、前記保護格納部に格納されている前記第1認証子とが一致するか否かを判断する判断ステップと、前記判断ステップにおいて一致しないと判断されると、前記復号化データの前記セキュア記憶部への書き込みを禁止し、一致すると判断されると、前記復号化データを前記セキュア記憶部へ書き込む復帰制御ステップとを含むこととしてもよい。

- [0046] また、本発明は、動作モードとして、通常電力モードと、省電力モードとを切り換えて動作し、前記通常電力モード時には、秘匿すべき保護データに係る処理を少なくとも実行し、前記省電力モード時には、前記保護データを、外部メモリにおいて安全に保持するセキュア処理装置において用いられる、情報処理方法であって、前記セキュア処理装置は、自装置外部からの不正アクセスを防止する機構を有し、前記省電力モード時において、記憶内容が消失するメモリにより構成され、前記保護データを記憶するためのセキュア記憶部と、前記通常電力モードまたは前記省電力モードのいずれの動作時であっても記憶内容を保持する機構、および、自装置外部からの不正アクセスを防止する機構を有し、前記セキュア記憶部よりも記憶容量が小さい保護格納部とを有し、前記情報処理方法は、データの暗号化および復号化を行う暗号

処理ステップと、データの内容に依存して定まり、当該データよりもデータサイズが小さい認証子を生成する生成ステップと、前記セキュア処理装置が前記省電力モードへ移行する時に、前記保護データを前記暗号処理ステップの実行により暗号化し、得られた暗号化データを前記外部メモリに記憶させるとともに、前記暗号化データに基づいて、前記生成ステップの実行により第1認証子を生成し、生成された当該第1認証子を前記保護格納部に格納させるよう制御する移行制御ステップと、前記セキュア処理装置が前記通常電力モードへ復帰する時に、前記外部メモリに記憶された前記暗号化データに基づいて、前記生成ステップの実行により第2認証子を生成するよう制御する認証子生成制御ステップと、生成された前記第2認証子と、前記保護格納部に格納されている前記第1認証子とが一致するか否かを判断する判断ステップと、前記判断ステップにおいて一致しないと判断されると、前記外部メモリに記憶された前記暗号化データを前記セキュア記憶部へ書き込むための処理を制限し、一致すると判断されると、前記暗号化データを前記暗号処理部ステップの実行により復号化し、得られた復号化データを前記セキュア記憶部へ書き込むよう制御する復帰制御ステップとを含むこととしてもよい。

[0047] また、本発明は、動作モードとして、通常電力モードと、省電力モードとを切り換えて動作し、前記通常電力モード時には、秘匿すべき保護データに係る処理を少なくとも実行し、前記省電力モード時には、前記保護データを、外部メモリにおいて安全に保持するセキュア処理装置の動作を制御する制御プログラムであって、前記セキュア処理装置は、自装置外部からの不正アクセスを防止する機構を有し、前記省電力モード時において、記憶内容が消失するメモリにより構成され、前記保護データを記憶するためのセキュア記憶部と、前記通常電力モードまたは前記省電力モードのいずれの動作時であっても記憶内容を保持する機構、および、自装置外部からの不正アクセスを防止する機構を有し、前記セキュア記憶部よりも記憶容量が小さい保護格納部とを有し、前記制御プログラムは、データの暗号化および復号化を行う暗号処理ステップと、データの内容に依存して定まり、当該データよりもデータサイズが小さい認証子を生成する生成ステップと、前記セキュア処理装置が前記省電力モードへ移行する時に、前記保護データを前記暗号処理ステップの実行により暗号化し、得られ

た暗号化データを前記外部メモリに記憶させるとともに、前記暗号化データに基づいて、前記生成ステップの実行により第1認証子を生成し、生成された当該第1認証子を前記保護格納部に格納させるよう制御する移行制御ステップと、前記セキュア処理装置が前記通常電力モードへ復帰する時に、前記外部メモリに記憶された前記暗号化データに基づいて、前記生成ステップの実行により第2認証子を生成するよう制御する認証子生成制御ステップと、生成された前記第2認証子と、前記保護格納部に格納されている前記第1認証子とが一致するか否かを判断する判断ステップと、前記判断ステップにおいて一致しないと判断されると、前記外部メモリに記憶された前記暗号化データを前記セキュア記憶部へ書き込むための処理を制限し、一致すると判断されると、前記暗号化データを前記暗号処理部ステップの実行により復号化し、得られた復号化データを前記セキュア記憶部へ書き込むよう制御する復帰制御ステップとを含むこととしてもよい。

[0048] これにより、上述した制御プログラムを、ネットワークを通して頒布等により流通させることができる。

図面の簡単な説明

[0049] [図1]組み込み機器1のハードウェア構成を示す機能ブロック図。

[図2]組み込み機器1がシステムLSI1000によって音楽データを安全に再生する処理を示すフローチャート。

[図3]システムLSI1000が省電力モードと通常電力モードとの切り替えを制御する処理の概要を示すフローチャート。

[図4]CPU110がセキュア記憶部103に記憶されているデータを外部メモリ501に安全に退避させる処理を示すフローチャート。

[図5]外部メモリ501に退避されているデータをCPU110がセキュア記憶部103に安全に再設定する処理を示すフローチャート。

符号の説明

[0050] 1 組み込み機器

101 固有情報保持部

102 保護格納部

- 103 セキュア記憶部
- 104 退避指示部
- 105 復帰指示部
- 106 暗号処理部
- 107 認証子生成部
- 108 バス暗号回路
- 109 バス暗号鍵設定レジスタ
- 110 CPU
- 111 内部バス
- 501 外部メモリ
- 502 バス暗号領域
- 503 電源A
- 504 電源B
- 1000 システムLSI

発明を実施するための最良の形態

[0051] 1. 1 概要

以下、本発明のセキュア処理装置について、実施の一形態を説明する。

1. 1. 1 セキュア処理装置の概要

本実施形態では、セキュア処理装置がシステムLSI1000の場合を想定して説明する。また、システムLSI1000は、組み込み機器1に含まれているとする。システムLSI1000は、少なくとも、秘匿すべき保護データにかかる処理を行う構成要素については、外部からの不正なアクセスを防止する機構が設けられている。

[0052] 1. 1. 2 組み込み機器1の概要

なお、組み込み機器1は、具体的には、例えば、音楽データ等の再生が可能な携帯機器である。組み込み機器1は、MP3(MPEG-1 Audio Layer-3)、AAC(Advanced Audio Coding)、WMA(Windows(登録商標) Media Audio)などの音声ファイルフォーマットの音楽データを再生する。音楽データは、SDメモリカード等の外部のフラッシュメモリに記憶されている。

[0053] 著作権保護に配慮した音楽データの利用を可能にするために、組み込み機器1は、SD-Audioに対応している。SD-Audioとは、SDメモリカードに著作権保護を施して音楽データを記録するSD応用規格(application format)である。

著作権保護を実現するため、SDメモリカードに記録されている音楽データは、暗号化されている。暗号化された音楽データを再生するには、音楽データを復号する必要がある。復号化された音楽データは、不正に複製等されないようにする必要があるので、組み込み機器1は、システムLSI1000によって当該音楽データの再生処理を安全に行う。

[0054] 1. 1. 3 システムLSI1000の概要

システムLSI1000は、秘匿すべき保護データを用いた処理を行うためのセキュア記憶部103を有している。

また、システムLSI1000は、通常電力モードと省電力モードとを切り換えて動作する。

[0055] 省電力モードで動作している間、システムLSI1000においては、セキュア記憶部103には電力が供給されず、記憶内容が消失する。そのため、システムLSI1000は、省電力モードへ移行する際に、セキュア記憶部103のデータを、システムLSI1000の外部にある外部メモリ501に退避させる。また、システムLSI1000は、省電力モードから通常電力モードへ復帰する際に、外部メモリ501に退避させたデータを、セキュア記憶部103に安全に再設定する。

[0056] 以下、セキュア記憶部103のデータを外部メモリ501に安全に退避させ、また、外部メモリ501に退避させたデータをセキュア記憶部103に安全に再設定することを特徴とする本発明のセキュア処理装置の一例であるシステムLSI1000について、具体的に説明する。

1. 2 構成

まず、組み込み機器1およびシステムLSI1000の構成を具体的に説明する。

[0057] 図1は、組み込み機器1のハードウェア構成を示す機能ブロック図である。

図1に示すように、組み込み機器1は、システムLSI1000と、外部メモリ501と、バス暗号領域502と、電源A503と、電源B504とを含む。

1. 2. 1 システムLSI1000

システムLSI1000は、固有情報保持部101と、保護格納部102と、セキュア記憶部103と、退避指示部104と、復帰指示部105と、暗号処理部106と、認証子生成部107と、バス暗号回路108と、バス暗号鍵設定レジスタ109と、CPU110とからなるハードウェア構成を含む。システムLSI1000の各構成要素は、内部バス111によってそれぞれ接続されている。

- [0058] 上述のシステムLSI1000の各構成要素は、システムLSI1000の内部に含まれており、システムLSI1000の外部からの不正アクセスを防止する機構を有している。

1. 2. 2 外部メモリ501

外部メモリ501は、システムLSI1000の外部に設けられた揮発性のメモリであり、著作権保護やセキュリティ面から見て重要度の低いデータと、システムLSI1000から退避させるデータとを記憶する。

- [0059] 外部メモリ501は不正アクセスを防止する機構を有しておらず、外部メモリ501に記憶されているデータは、さまざまな機器からアクセスされうる。また、外部メモリ501は、図示するように、電源A503と接続されている。組み込み機器1が動作している間、外部メモリ501には電源A503から電力が供給されている。そのため、組み込み機器1が動作している間、外部メモリ501の記憶内容は消失しない。

- [0060] 外部メモリ501が記憶するデータ等を具体的に説明すると、図示するように、外部メモリ501は、通常プログラム205や、暗号化された退避データ206などを記憶する。

通常プログラム205は、例えば、組み込み機器1全体の処理を制御するためのプログラムであり、CPU110により随時参照され、実行される。暗号化された退避データ206は、システムLSI1000が省電力モードへ移行する際に、システムLSI1000から外部メモリ501へと退避させるデータである。このデータは、システムLSI1000の暗号処理部106により暗号化されている。外部メモリ501には、これら以外にも、通常プログラム205などが処理のために用いるデータ等を記憶する。

- [0061] なお、通常プログラム205は、著作権保護を要する音楽データ等と比べると、セキュリティ面から見た場合にそれほど重要ではなく、また、組み込み機器1全体の動作を制御するものであるため比較的データサイズが大きい。そのため、セキュア記憶部10

3ではなく外部メモリ501において記憶することとする。

なお、暗号化された退避データ206は、より高いセキュリティを確保するためには、システムLSI1000が省電力モードから通常電力モードへと復帰した後、速やかに外部メモリ501から削除されることが望ましい。

[0062] 1. 2. 3 バス暗号領域502

バス暗号領域502は、システムLSI1000の外部に設けられた揮発性のメモリであり、著作権保護やセキュリティ面から見て重要度の高いデータが記憶される。図示するように、バス暗号領域502は、電源A503と接続され、電源A503から電力が供給されている。そのため、組み込み機器1が動作している間、バス暗号領域502の記憶内容は消失しない。

[0063] バス暗号領域502は、セキュア記憶部103の記憶容量が十分でない等の問題により、システムLSI1000のセキュア記憶部103に格納しきれないデータをシステムLSI1000の外部で安全に保持するために用いられる。なお、バス暗号領域502は、さまざまな機器からアクセスされうるため、バス暗号領域502には、安全にデータが保持されるようにするため、バス暗号回路108により暗号化されたデータが記憶される。バス暗号回路108が暗号化に用いる鍵を、バス暗号鍵と言う。

[0064] 本実施形態では、バス暗号領域502には、図示するように、セキュアアプリ207などが記憶される。セキュアアプリ207は、バス暗号回路108により暗号化されている。セキュアアプリ207は、著作権保護を実現するためのプログラムであり、具体的には、音楽データの権利情報を用いた処理や音楽データを復号するための復号鍵を用いた処理などを安全に行うためのものである。

[0065] バス暗号領域502に保持されているセキュアアプリ207は、CPU110により読み出され、バス暗号回路108でバス暗号鍵を用いて復号化がなされる。CPU110は、復号化処理がなされたプログラムを実行して上述の著作権保護を実現するための処理を行う。

1. 2. 4 電源A503

電源A503は、図示するように、外部メモリ501、バス暗号領域502、システムLSI1000内部の保護格納部102に電力を供給し続ける電源である。電池等として実装さ

れる。電源A503は、システムLSI1000が省電力モードであれ通常電力モードであれ、上述の外部メモリ501、バス暗号領域502、保護格納部102に電力を供給する。

[0066] 1. 2. 5 電源B504

電源B504は、図示するように、システムLSI1000に電力を供給する電源である。ただし、電源B504は、システムLSI1000が通常電力モードで動作している場合にのみ電力を供給し、システムLSI1000が省電力モードである場合には電力を供給しない電源である。電源B504は、組み込み機器1の外部バッテリー等として実装される。

[0067] なお、電源A503は、システムLSI1000が省電力モード時において、所定のデータを保持するためにメモリ等に電力を供給するものである。CPU110等を含み、プログラム等を実行するシステムLSI1000に電力を供給する電源B504と比べると、電源A503がメモリ等に供給するのに必要な電力は少なくて済む。そのため、電源A503は、一般的には電源B504より小容量の電源であり、例えばコンデンサなどの、着脱不可のバッテリーとして実装される。

[0068] 1. 2. 6 固有情報保持部101

次に、システムLSI1000の内部に含まれる各構成要素について説明する。

固有情報保持部101は、システムLSI1000に固有の固有情報を記憶する。固有情報とは、例えばシステムLSI1000を識別するための識別子(ID)などである。

固有情報がシステムLSI1000に固有であることを利用した処理を行う場合を考慮して、固有情報保持部101は、記憶している固有情報が消去されたり書き換えられたりされるのが困難となるような実装で実現されることが望ましい。例えば、固有情報保持部101は、マスクROM(Read Only Memory)やヒューズである。

[0069] 1. 2. 7 保護格納部102

保護格納部102は、認証子を格納するための認証子格納領域201を有し、後述する認証子生成部107が生成する認証子を、認証子格納領域201において格納する。認証子については、認証子生成部107とともに後述する。

保護格納部102は、例えば揮発性のメモリであり、図示するように、電源A503と接続されている。電源A503から電力の供給を受けているので、システムLSI1000が

省電力モードであるか否かにかかわらず、記憶内容が消失しない。また、保護格納部102は、セキュア記憶部103またはバス暗号領域502に格納されたプログラムに含まれる命令コードでのみアクセス可能な領域であり、外部からの不正なアクセスから保護されている。

- [0070] 認証子のデータサイズは、セキュア記憶部103に記憶されているデータのデータサイズよりも小さいので、後述するセキュア記憶部103と比較して、保護格納部102は、記憶容量が少ない。例えば、セキュア記憶部103の1/1000～1/100程度の記憶容量を有している。そのため、セキュア記憶部103と比較して、必要なメモリ領域が少ない。

1. 2. 8 セキュア記憶部103

セキュア記憶部103は、秘匿すべき保護データの処理等をCPU110が行うために用いられるメモリである。

- [0071] セキュア記憶部103は、揮発性のメモリであり、システムLSI1000の外部からアクセスすることができないハードウェア構成を有している。
- このようなハードウェア構成は、例えば、通常モードとセキュアモードとを切り換えて動作するCPU110と、セキュア記憶部103とで実現できる。詳細に説明すると、セキュア記憶部103は、物理的に分離されたメモリ空間であり、システムLSI1000の外部からアクセスできず、セキュアモードで動作しているCPU110のみがアクセス可能である、という構成にすることでこのようなハードウェア構成を実現できる。

- [0072] なお、本実施形態では、機密性が保証されるべきデータが、セキュア記憶部103に記憶される。これらのデータが暴露されるとデータの権利者等の不利益になるためである。具体的には、同図に示すように、セキュア記憶部103には、セキュアなプログラム202、セキュアなデータ203、バス暗号鍵204が記憶される。

ここで、セキュアなプログラム202は、システムLSI1000の処理を制御するプログラムである。例えば、著作権管理がなされている音楽データを復号化して再生するためのプログラムや、システムLSI1000が省電力モードへ移行するときに、セキュア記憶部103に記憶されているデータを外部メモリ501に退避させる処理を実行するためのプログラムなどがセキュアなプログラム202に含まれる。なお、セキュアなプログラム2

02のうち、省電力モード移行時にセキュア記憶部103に記憶されているデータを外部メモリ501に退避させる処理を実行するためのプログラムは、予めシステムLSI1000内部の不揮発性のROM(Read Only Memory)に格納されていることとする。そして、システムLSI1000が動作を開始したときに、ROMから読み出されてセキュア記憶部103にセキュアなプログラム202として記憶されることとする。なお、このROMは、システムLSI1000の内部に含まれるため、システムLSI1000の外部からの不正アクセスから保護されている。また、セキュアなデータ203は、例えば、暗号化のなされていない音楽データである。

[0073] セキュアなプログラム202が暴露されると、プログラムが改ざんされて、音楽データの再生回数の制限が無効にされる等の不正な処理が可能なプログラムが作成されるおそれがある。また、セキュアなデータ203が暴露されると、不正に複製がなされうる。そのため、これらプログラムやデータは、機密性が保証されるべきものであるといえる。

なお、バス暗号鍵204については、バス暗号回路108およびバス暗号鍵設定レジスタ109とともに詳しく説明する。

[0074] 上述の通り、セキュア記憶部103は、外部からアクセスすることができないハードウェア構成を有しているため、セキュア記憶部103に記憶されるデータは、機密性が保証される。また、固有情報保持部101、保護格納部102も、上述のセキュア記憶部103と同様のハードウェア構成を有し、外部からアクセスすることができない。

また、セキュア記憶部103は、システムLSI1000が省電力モードで動作している間、電力が供給されず、記憶内容が消失する。

[0075] 1. 2. 9 退避指示部104

退避指示部104は、システムLSI1000が通常電力モードから省電力モードに移行すべきであることを検知する。検知すると、セキュア記憶部103に記憶されているデータを外部メモリ501に退避させる指示を、CPU110に通知する。

なお、組み込み機器1は、図示しない操作部材がユーザにより押下されたり、操作指示を示す信号を受信したりすることで、ユーザの操作がなされたと検出する検出機構を有している。組み込み機器1は、システムLSI1000が通常電力モードにより動作

している時においては、ユーザの操作が所定時間以上検出されないと、システムLSI1000を省電力モードに移行させる。また、組み込み機器1は、システムLSI1000が省電力モードにより動作している時においては、ユーザの操作を検出することでシステムLSI1000を通常電力モードへと復帰させる。

[0076] 詳細に説明すると、システムLSI1000が通常電力モードの時において、上記検出機構が所定時間以上ユーザの操作を検出しなかったとき、組み込み機器1は、システムLSI1000を省電力モードへ移行させるための移行制御信号を退避指示部104へ出力する。退避指示部104は、この移行制御信号を受け付けることで、システムLSI1000が通常電力モードから省電力モードへ移行すべきことを検知する。

[0077] また、組み込み機器1は、システムLSI1000が省電力モードで動作している時に、上記検出機構によりユーザの操作を受け付けると、システムLSI1000を通常電力モードへと復帰させるために、電源B504からシステムLSI1000への電力の供給を再開する。システムLSI1000への電力の供給が再開されると、組み込み機器1は、復帰指示部105に対して、復帰制御信号を出力する。

[0078] 1. 2. 10 復帰指示部105

復帰指示部105は、復帰制御信号を受け付けることで、システムLSI1000が省電力モードから通常電力モードへと復帰すべきであることを検知する。検知すると、外部メモリ501に退避されているデータをセキュア記憶部103に安全に再設定させる処理の実行をCPU110に指示する。

[0079] 詳細に説明すると、システムLSI1000は、外部メモリ501に退避されているデータをセキュア記憶部103に安全に再設定するための復帰プログラムを記憶している。この復帰プログラムは、例えばシステムLSI1000の外部からの不正アクセスを防止する機構を有している不揮発性メモリに記憶されており、システムLSI1000が省電力モードにより動作している間も消失しない。

[0080] システムLSI1000を通常電力モードへと復帰させるために、電源B504からシステムLSI1000への電力の供給が再開され、復帰指示部105が復帰制御信号を受け付けると、復帰指示部105は、上記復帰プログラムをメモリから読み出し、読み出した復帰プログラムをセキュア記憶部103に記憶させる。そして、復帰指示部105は、CPU

110に、セキュア記憶部103に記憶されている復帰プログラムの実行を開始するよう指示する。

[0081] なお、外部メモリ501に退避されているデータをセキュア記憶部103に安全に再設定させる処理については、後述する。また、上記復帰プログラムは、不正な改ざんから保護されていることが望ましい。改ざん等がなされると、例えば一部の認証等の処理が省略され、外部メモリ501に退避されているデータをセキュア記憶部103に再設定する処理が安全に行われなくなる可能性があるためである。

[0082] 1. 2. 11 暗号処理部106

暗号処理部106は、CPU110の指示に従って、入力されたデータやプログラムの暗号化処理、および、復号化処理を行う。暗号処理部106は、システムLSI1000の外部からの不正アクセスを防止する機構を有している。そのため、暗号処理部106が暗号化処理または復号化処理を行うための鍵や、暗号化または復号化処理中の間データなどをシステムLSI1000の外部の不正者が不正に取得することはできない。

[0083] なお、暗号化や復号化に用いるアルゴリズムとしては、共通鍵方式のAES(Advanced Encryption Standard)や、公開鍵方式のRSA(Rivest Shamir Adleman)などが一例として挙げられるが、これらに限られない。

1. 2. 12 認証子生成部107

認証子生成部107は、CPU110の指示に従って、入力されたデータやプログラムから、認証子を生成する。ここで、認証子とは、入力されたデータやプログラムを要約した値である。

[0084] 認証子は、システムLSI1000の省電力モード移行時に外部メモリ501に退避されるデータと、通常電力モードへの復帰時にセキュア記憶部103に再設定するデータとが同一であるかを判断するために用いられる。

そのため、認証子生成部107は、少なくとも、入力されたデータやプログラムに依存した値、望ましくは、一意に求まる値を生成すべきである。また、外部メモリ501に退避させたデータが改ざん等されていないことを保証するために、認証子生成部107は、あるデータと認証子の値が等しい別のデータが容易に生成できないような方法で

認証子を生成することが望ましい。さらに、似たデータから近い値の認証子が生成されないこと、また、生成される認証子の値に偏りがないことが望ましい。

- [0085] そのため、本実施形態では、認証子生成部107は、入力されたデータやプログラムのハッシュ値を計算し、計算されたハッシュ値を認証子としている。ハッシュ値計算のアルゴリズムは、例えばSHA-1などを用いることとするが、これに限らない。

1. 2. 13 バス暗号回路108

バス暗号回路108は、バス暗号鍵設定レジスタ109を含んでいる。バス暗号鍵設定レジスタ109は、バス暗号鍵を格納するレジスタである。バス暗号鍵は、CPU110が、セキュア記憶部103に記憶されているセキュアなプログラム202を実行することにより決定される。バス暗号回路108は、バス暗号領域502に書き込むプログラム等を、まず、バス暗号鍵設定レジスタ109に設定されたバス暗号鍵を用いて暗号化する。暗号化した後、バス暗号領域502にセキュアアプリ207などとして記憶させる。また、バス暗号回路108は、バス暗号領域502に保持されている暗号化されたプログラムやデータを読み出して、バス暗号鍵を用いて復号化する。

- [0086] なお、バス暗号領域502には、暗号化されたデータが格納されているが、バス暗号領域502は、さまざまな機器からアクセスされうるため、暗号化に用いたバス暗号鍵が固定だと、バス暗号領域502に記憶されているデータが解析等されることにより、暗号化に用いているバス暗号鍵が暴露されるおそれがある。そのため、バス暗号鍵は、隨時変更されることが望ましい。バス暗号鍵が変更されると、バス暗号回路108は、バス暗号鍵設定レジスタ109の記憶内容を更新する。

- [0087] また、バス暗号鍵設定レジスタ109に保持されているバス暗号鍵は、セキュア記憶部103においてもバス暗号鍵204として記憶される。バス暗号鍵が変更されるたびに、変更後のバス暗号鍵が、バス暗号鍵設定レジスタ109とセキュア記憶部103に上書きされる。

なお、バス暗号鍵変更のタイミングとしては、例えば組み込み機器1に電源が投入された時や、セキュアなプログラム202が動作を開始した時など様々なものが考えられる。このとき、セキュアなプログラム202の初期動作として、セキュアなプログラム202の実行開始時刻等を用いて鍵を生成するなどとすればよい。

[0088] また、バス暗号回路108や、バス暗号鍵を格納しているバス暗号鍵設定レジスタ109等は、システムLSI1000の内部に含まれ、システムLSI1000の外部から不正アクセスできない。バス暗号領域502に記憶されている暗号化されたデータは、システムLSI1000によって読み出され、システムLSI1000の内部でしか復号化できないため、復号化後のデータはシステムLSI1000のみが利用することができる。

[0089] 1. 2. 14 CPU110

CPU110は、セキュア記憶部103やバス暗号領域502や外部メモリ501などに記憶されているプログラムに従って、システムLSI1000の動作を制御する。

CPU110は、動作モードとして通常モードとセキュアモードとを備え、通常モードとセキュアモードとを切り換えて動作する。セキュアモードで動作している時に限り、CPU110は、セキュア記憶部103や保護格納部102や固有情報保持部101などのシステムLSI1000内部のメモリへアクセスできる。また、セキュアモードで動作している時に限り、暗号処理部106やバス暗号回路108を用いて、機密性が保証されるべきデータに関する処理を行う。つまり、システムLSI1000では、機密性が保証されるべきデータを用いた処理が行われる際に、システムLSI1000内部の各構成要素にアクセス可能な主体および時期を、CPU110がセキュアモードで動作している時に限定している。こうすることで、システムLSI1000は、外部からの不正アクセスを防止する。

例えば、CPU110は、動作モードをセキュアモードに切り換えてから、暗号化された音楽データをSDメモリカードから読み出して復号化し、再生する処理や、省電力モードへの移行時にセキュア記憶部103のデータ等を外部メモリ501に安全に退避させる処理や、通常電力モードへの復帰時に、外部メモリ501に退避させたデータをセキュア記憶部103に安全に再設定する処理などを行う。

[0090] 1. 2. 15 内部バス111

内部バス111は、図示するように、システムLSI1000内部の各構成要素を互いに接続する。

1. 2. 16 その他の構成要素

なお、組み込み機器1には、ユーザの操作を受け付ける操作受付部や、SDメモリカード等のフラッシュメモリを着脱できるようにするためのインターフェース等を備えるが、

本発明の特徴部分ではないので、図1には図示せず、説明を省略する。

[0091] 1. 3 動作

次に、本発明のセキュア処理装置の動作を説明する。

まず、システムLSI1000が音楽データを安全に再生する処理を「1. 3. 1 音楽データの再生処理」で説明する。

次に、システムLSI1000が、省電力モードへの移行時にセキュア記憶部103に記憶されているデータ等を外部メモリ501に安全に退避させる処理と、通常電力モードへの復帰時に外部メモリ501に退避させたデータを安全にセキュア記憶部103に再設定する処理とを、「1. 3. 2 電力モード切り替え時の処理」「1. 3. 3 退避時の処理」「1. 3. 4 復帰時の処理」で説明する。

[0092] 1. 3. 1 音楽データの再生処理

以下、組み込み機器1がシステムLSI1000によって音楽データを安全に再生する処理を説明する。なお、音楽データは、暗号化処理がされており、SDメモリカードに記憶されているものとする。

また、システムLSI1000は、バス暗号領域502に記憶されているセキュアアプリ207によって、SDメモリカードから音楽データを取得する。また、セキュアなプログラム202によって、音楽データの復号化を行い、復号化された音楽データをセキュア記憶部103に記憶させることとする。また、セキュア記憶部103に記憶される音楽データの再生も、セキュアなプログラム202によって行うこととする。

[0093] 以下、具体的に説明すると、組み込み機器1は、ユーザから音楽データの再生を指示する操作を受け付けると、システムLSI1000により音楽データの再生処理を開始する。

図2は、組み込み機器1がシステムLSI1000によって音楽データを安全に再生する処理を示すフローチャートである。

[0094] 図2に示すように、システムLSI1000のCPU110は、バス暗号領域502に記憶されているセキュアアプリ207を実行することにより、組み込み機器1に接続されたSDメモリカードから、暗号化された音楽データを取得する(ステップS201)。

CPU110は、セキュア記憶部103からセキュアなプログラム202を読み出す。CPU

110は、セキュアなプログラム202を実行することで、暗号化された音楽データを復号するための復号鍵を算出する。算出された復号鍵を用いて、暗号化された音楽データを復号化する(ステップS202)。なお、音楽データ等の、暗号化されたコンテンツを復号するための復号鍵の算出方法は、従来から広く用いられており、本発明の特徴部分ではないため詳細な説明を省略する。

- [0095] CPU110は、セキュアなプログラム202を実行することにより復号化された音楽データを、セキュア記憶部103に記憶させる(ステップS203)。

CPU110は、セキュア記憶部103に記憶されている復号化された平文音楽データを再生する(ステップS204)。

CPU110は、全ての音楽データをSDメモリカードから取得したか否かを判断し(ステップS205)、取得したのであれば(ステップS205:YES)、処理を終了し、取得したのでなければ(ステップS205:NO)、ステップS201の処理に戻って、音楽データの取得、復号化、再生処理を繰り返し行う(ステップS201、S202、S203、S204)。

- [0096] 1. 3. 2 電力モード切り替え時の処理

図3は、システムLSI1000が省電力モードと通常電力モードとの切り替えを制御する処理の概要を示すフローチャートである。

組み込み機器1が動作を開始し、システムLSI1000が起動すると(ステップS301)、システムLSI1000は、まず、通常電力モードで動作を開始する。

- [0097] 動作を開始すると、システムLSI1000のCPU110は、省電力モード移行時にセキュア記憶部103に記憶されているデータを外部メモリ501に退避させる処理を実行するためのプログラムを、セキュアなプログラム202としてセキュア記憶部103に記憶させる。

システムLSI1000は、省電力モードに移行すべきことを退避指示部104によって検知するまで(ステップS302:NO)、通常電力モードで動作する。

- [0098] 省電力モードへ移行すべきことを退避指示部104が検知すると(ステップS302: YES)、セキュア記憶部103に記憶されているデータを外部メモリ501に退避させる指示が、退避指示部104からCPU110へ通知される。

CPU110は、退避指示部104から上記通知を受け付けると、セキュアなプログラム

202を実行することにより、セキュア記憶部103に記憶されているデータを外部メモリ501に安全に退避させる処理を行う(ステップS303)。このステップS303の処理を、退避時の処理と呼ぶこととする。退避時の処理の詳細は、「1. 3. 3 退避時の処理」で説明する。退避時の処理が実行された後、システムLSI1000は、省電力モードにより動作する。

- [0099] システムLSI1000は、省電力モードにより動作している間、通常電力モードへと復帰すべきであることを復帰指示部105によって検知するまで(ステップS304: NO)、省電力モードで動作する。

通常電力モードへ復帰すべきであることを復帰指示部105が検知すると(ステップS304: YES)、復帰指示部105は、外部メモリ501に退避されているデータをセキュア記憶部103に安全に再設定するための復帰プログラムをシステムLSI1000内の不揮発性メモリから読み出して、セキュア記憶部103に記憶させる。復帰指示部105は、セキュア記憶部103に記憶された上記復帰プログラムの実行をCPU110に指示する。

- [0100] CPU110は、復帰指示部105からの指示を受け付けて、上記復帰プログラムを実行することにより、外部メモリ501に退避されているデータをセキュア記憶部103に安全に再設定する処理を実行する(ステップS305)。このステップS305の処理を、復帰時の処理と呼ぶこととする。復帰時の処理の詳細は、「1. 3. 4 復帰時の処理」で説明する。復帰時の処理が実行された後、システムLSI1000は、通常電力モードで動作し、ステップS302の処理を行う。

- [0101] 1. 3. 3 退避時の処理

ステップS303の、退避時の処理を、詳しく説明する。

図4は、CPU110がセキュア記憶部103に記憶されているデータを外部メモリ501に安全に退避させる処理を示すフローチャートである。

以下、CPU110が退避指示部104から通知を受け付けた後の処理について説明する。

- [0102] CPU110は、まず、セキュア記憶部103に記憶されているセキュアなプログラム202やセキュアなデータ203やバス暗号鍵204など、記憶内容の全てを入力データとし

て、認証子生成部107にハッシュ値を計算させる(ステップS401)。

計算により得られたハッシュ値を保護格納部102の認証子格納領域201に格納する(ステップS402)。

- [0103] CPU110は、セキュア記憶部103に記憶されている全ての記憶内容を、固有情報保持部101に記憶されている固有情報を暗号鍵として用いて暗号処理部106に暗号化させる(ステップS403)。

暗号化が完了したデータを、暗号化された退避データ206として外部メモリ501に記憶させる(ステップS404)。

- [0104] ステップS404の処理が完了した後、CPU110は、電源B504の電力供給を停止する(ステップS405)。こうすることで、システムLSI1000への電力供給が停止して、退避時の処理が完了する。

1. 3. 4 復帰時の処理

ステップS305の、復帰時の処理を、詳しく説明する。

- [0105] 図5は、外部メモリ501に退避されているデータをCPU110がセキュア記憶部103に安全に再設定する処理を示すフローチャートである。

以下、ステップS304の処理、つまりシステムLSI1000が通常電力モードへ復帰すべきことを復帰指示部105が検知した後の処理について説明する。なお、退避指示部104の説明で上述したように、復帰指示部105が検知を行う時には、組み込み機器1により、電源B504からシステムLSI1000への電力の供給が再開されている。

- [0106] まず、復帰指示部105は、検知を行うと、復帰指示部105の説明で上述したように、復帰プログラムをメモリから読み出し、読み出した復帰プログラムをセキュア記憶部103に記憶させる(ステップS501)。復帰指示部105は、CPU110に、復帰プログラムの実行を開始するよう指示する。

CPU110は、復帰指示部105からの指示を受け付けて、復帰プログラムを実行する。以下、復帰プログラムによる処理を説明すると、まず、CPU110は、外部メモリ501に退避させた、暗号化された退避データ206を読み出す。読み出しを終えると、暗号化された退避データ206を、固有情報保持部101に記憶されている固有情報を復号鍵として用いて暗号処理部106に復号化させる(ステップS502)。

[0107] 復号化により得られたデータを入力データとして、認証子生成部107にハッシュ値を計算させる(ステップS503)。

CPU110は、計算により得られたハッシュ値を、保護格納部102の認証子格納領域201に格納されているハッシュ値とを比較して、ハッシュ値が一致するか判断する(ステップS504)。

[0108] 判断の結果、ハッシュ値が一致する場合は(ステップS504:YES)、CPU110は、復帰時の処理を正常終了する(ステップS505)。

判断の結果、ハッシュ値が異なる場合は(ステップS504:NO)、暗号化された退避データ206が改ざんされていると推定できるため、CPU110は復帰時の処理を異常終了する(ステップS506)。このとき、ステップS502において復号化されたデータを破棄する。

[0109] 1. 3. 5 動作についての補足説明

(1) バス暗号鍵についての補足説明

上述の実施例では、バス暗号鍵設定レジスタ109に格納されているバス暗号鍵を、セキュア記憶部103においても記憶している。システムLSI1000が省電力モードに移行する際には、セキュア記憶部103に記憶されているバス暗号鍵204も暗号化されて外部メモリ501に退避される。

[0110] ここで、バス暗号鍵についても退避させる点について、補足説明する。

バス暗号領域502のデータは、上述のように、バス暗号鍵を鍵として用いて暗号化されている。また、上述のように、バス暗号鍵は、隨時、変更されることが望ましい。

ここで、バス暗号鍵を隨時変更することとする。そうすると、システムLSI1000が省電力モードへ移行する際に、バス暗号鍵が消失すると、通常電力モードに復帰した後、もともと用いていたバス暗号鍵が得られなくなり、バス暗号領域502のデータを利用できなくなる。そのため、通常電力モードに復帰した後、バス暗号領域502のデータを用いた処理を継続して行うには、バス暗号領域502に、再度、データを記憶させる等の処理が必要となる。つまり、省電力モードと通常電力モードとが切り換わる前後において、バス暗号領域502のデータを用いた処理を継続して実行できず、終了させるより他ないという問題がある。

[0111] そこで、上述の実施形態のように、バス暗号鍵をも退避させておくと、省電力モードと通常電力モードとが切り換わっても、バス暗号領域502のデータを用いた処理を連続して実行することができる。

また、バス暗号鍵は、セキュア記憶部103においても記憶されているが、必ずしもセキュア記憶部103に記憶させておく必要はない。省電力モードへの移行時に、バス暗号鍵設定レジスタ109から読み出せば、バス暗号鍵を退避させることができる。

[0112] ただし、セキュア記憶部103にバス暗号鍵204として記憶させておくと、省電力モードへ移行する際に、バス暗号鍵設定レジスタ109からバス暗号鍵を読み出さなくてもよいため、外部メモリ501へのデータの退避を高速で行えるという利点がある。

したがって、データを退避させる処理を行いつつシステムLSI1000への供給電力が低下するような場合などにおいて、データの退避が完了する前に電力の供給が停止してデータを消失してしまうなどの危険を低くすることができる。

[0113] また、上述の実施形態では、バス暗号回路108は1つとして説明してきたが、バス暗号領域502においてセキュアアプリ207が複数記憶されている場合、それぞれのセキュアアプリ207ごとに異なる鍵を用いて暗号化や復号化を行うほうが、セキュリティの観点からは好ましい。ある鍵が解析等により暴露されても、その他の鍵を用いているセキュアアプリ207には影響がないからである。

[0114] すなわち、セキュアアプリ207のひとつひとつに、バス暗号回路108とバス暗号鍵設定レジスタ109との組が対応するよう、バス暗号回路108を複数備えることとしてもよい。あるいは、バス暗号鍵設定レジスタ109を複数備えることとしてもよい。

この場合、セキュア記憶部103に、複数のバス暗号鍵を、連続したメモリアドレスによってまとめて記憶させておくと、外部メモリ501へデータを退避させる際、複数のバス暗号鍵設定レジスタ109のそれからバス暗号鍵を読み出すよりも高速でバス暗号鍵の退避を完了することができる。バス暗号鍵設定レジスタ109に格納されているバス暗号鍵は、システムLSI1000から見た場合、仮想メモリ空間において、ばらばらに配置されており、バス暗号鍵を探索する必要があるからである。

(2) 固有情報を用いて暗号化する点についての補足説明

上述の実施例では、システムLSI1000に固有の固有情報を暗号鍵として用いて、

外部メモリ501に退避させるデータの暗号化を行っている。

- [0115] こうすると、システムLSI1000のそれぞれにおいて固有情報が異なるので、それぞれのシステムLSI1000で暗号化のために用いる暗号鍵が異なることになる。そのため、あるシステムLSI1000で暗号化されたデータが、別のシステムLSI1000では復号化されないようにすることができる。

(3) 音楽データの再生処理についての補足説明

なお、図2に示した処理のうち、音楽データの再生を行うステップS201、ステップS202、ステップS203の処理は、システムLSI1000の内部の構成要素、つまりシステムLSI1000の外部からなされる不正アクセスから保護された構成要素でのみ行われる。そのため、音楽データの再生処理を安全に行うことができる。

- [0116] また、暗号化された音楽データを復号化するための復号鍵は、音楽データとともにメモリカードに記録されていることとしてもよい。このとき、復号鍵は、不正に復号鍵が利用されるのを避けるため、暗号化されていることが望ましい。

1. 3. 6 動作の変形例

(1) ハッシュ値の計算タイミングの変形例

省電力モードへの移行時において、認証子生成部107がハッシュ値を計算するタイミングについて、上述の実施例では、セキュア記憶部103に記憶されているデータを暗号処理部106で暗号化する前にハッシュ値を計算することとしている。すなわち、平文のデータに基づいてハッシュ値を計算している。

- [0117] この他にも、まず、セキュア記憶部103に記憶されている平文のデータを暗号処理部106で暗号化し、暗号化により得られたデータに基づいて、認証子生成部107によりハッシュ値を計算することとしてもよい。この場合、通常電力モードへの復帰時においては、CPU110は、まず、暗号化された退避データ206を外部メモリ501から読み出す。次に、暗号化された退避データ206に基づいて、認証子生成部107によりハッシュ値を計算する。計算により得られたハッシュ値が、省電力モードへの移行時に算出したハッシュ値と同一であれば、暗号化された退避データ206を暗号処理部106で復号化してセキュア記憶部103に再設定し、復帰時の処理を正常終了する。ハッシュ値が同一でなければ、暗号化された退避データ206の復号化処理を行わず

に異常終了する。

[0118] このような構成であると、暗号化された退避データ206が改ざんされたか否かを、処理の負荷が大きい復号化を実行する前に改ざん確認することができるので、改ざんチェックを迅速に行うことができる。

なお、上述の実施例で説明したように、平文のデータに基づいてハッシュ値を計算する方法にも利点はある。

[0119] 上記変形例のように、暗号化したデータに基づいてハッシュ値を計算する場合、暗号化して外部メモリ501に書き出した直後から、暗号化したデータに基づいてハッシュ値を計算するまでの間に、外部メモリ501の暗号化データが改ざんされると、改ざんされたデータに基づいてハッシュ値が計算されることとなり、改ざんを検出できないおそれがある。特に、セキュア記憶部103の記憶容量が小さい場合、暗号化したデータをセキュア記憶部103に記憶させつつハッシュ値を計算する処理を行うことが困難な場合もありうる。

[0120] したがって、上記変形例の場合、暗号化したデータのハッシュ値を認証子格納領域201に格納するまで、外部メモリ501への書き出しを行わないことが望ましい。

これに対し、上述の実施例では、ハッシュ値の計算が完了して認証子格納領域201に格納するまでの処理がシステムLSI1000の内部で行われるので、改ざんされたデータに基づいてハッシュ値を計算するような事態は発生しない。

(2) 復帰時の処理が異常終了した場合

なお、復帰時の処理において、異常終了した場合(ステップS506)、システムLSI1000の動作を停止することとしてもよいし、異常終了したことを示す情報を外部に通知したり表示したりしてもよい。

[0121] これにより、不正な改ざんがなされたことを、例えば著作権者等に通知することができる。このとき、システムLSI1000の固有情報をあわせて外部に通知すると、著作権者等は、システムLSI1000を含んでいる組み込み機器1を特定できる。その結果、不正な改ざんがなされた組み込み機器1に対して、コンテンツの再生禁止等の対策をとることができる。

[0122] また、この他にも、ステップS504において、ハッシュ値が一致しないと判断された場

合(ステップS504: NO)、セキュア記憶部103をダミーデータで上書きして、セキュア記憶部103に記憶されているデータを完全に消去してもよい。さらに、外部メモリ501に暗号化された退避データ206が残っていれば、これも同様に消去することとしてもよい。

- [0123] こうすることで、改ざんされたデータを組み込み機器1から完全に消去することができる、過去に改ざんされたデータをCPU110が誤って再び実行するといった危険をなくすことができる。

なお、システムLSI1000を通常電力モードへ復帰させた後において、外部メモリ501に、暗号化された退避データ206が残ったままであると、不正な解析者が外部メモリ501に残っている、暗号化された退避データ206を解析する可能性がある。そのため、ステップS504における判断の結果にかかわらず、ステップS504の処理の後、外部メモリ501の、暗号化された退避データ206を消去することとしてもよい。

(3) 退避時の処理・復帰時の処理

上述の実施例では、退避時の処理は、CPU110がセキュアなプログラム202を実行することにより行っている。また、復帰時の処理は、CPU110が復帰プログラムを実行することにより行っている。

- [0124] この他にも、例えば、退避指示部104や復帰指示部105がCPU110を介さずに直接にシステムLSI1000の各構成要素を制御することとしてもよい。

また、退避指示部104や復帰指示部105の機能を、CPU110が含んでいることとしてもよい。

すなわち、何らかの態様で上述の実施例のような退避時の処理や復帰時の処理を行う機能的構成がシステムLSI1000に備わっていればよく、上述の実施例の構成に限られない。

(4) 暗号化に使用する鍵

セキュア記憶部103の記憶内容を暗号化および復号化するための鍵は、システムLSI1000に固有の固有情報でなくとも、複数のシステムLSI1000のそれぞれに共通する鍵を用いて暗号化等を行ってもよい。

- [0125] また、固有情報のデータ長が長い場合は、暗号化等の処理負荷が大きくなるため、

ハッシュ値をとるなどしてデータ長を縮めた値を、鍵として用いてもよい。

また、固有情報保持部101に記憶されている固有情報でなくとも、セキュアなプログラム202が鍵を生成する処理を行ってもよいし、システムLSI1000の外部から鍵を取得することとしてもよい。例えば、ユーザが入力するデータや、組み込み機器1内の別の領域に記憶されている、何らかの構成要素に固有の情報などを用いることが考えられる。このようにすると、固有情報を持たないシステムLSIに対しても本発明を適用することが出来る。

(5) 退避の対象

上記実施例では、セキュア記憶部103の全ての記憶内容を、外部メモリ501に退避させる対象としている。

- [0126] この他にも、外部メモリ501に空き容量がない場合は、特に重要なデータなど、一部のデータのみを退避し、残りを破棄することとしてもよい。

また、セキュア記憶部103の記憶内容のすべてをひとまとめに暗号化したりハッシュ値を計算したりするのではなく、セキュアなプログラム202や、セキュアなデータ203や、バス暗号鍵204などを単位として別々に暗号化やハッシュ値を計算してもよい。この場合、通常電力モードへの復帰時に、それぞれのハッシュ値を用いて改ざん確認を行う必要があるため、ハッシュ値と退避にかかるデータを識別する情報を対応付けて記憶しておく。

- [0127] また、セキュア記憶部103の記憶内容に限らず、例えばシステムLSI1000にあるレジスタの値についても、上述の退避時の処理や復帰時の処理により、外部メモリ501に退避させ、また、レジスタに再設定することとしてもよい。これにより、システムLSI1000の動作状態を、より完全に外部メモリ501に退避させることができ、通常電力モードへの復帰時に、処理の再開を完全に行うことができる。

(6) 退避先

上記実施例では、セキュア記憶部103の記憶内容を、外部メモリ501に退避させることとしている。

- [0128] この他にも、何らかのセキュリティ対策が施されているメモリに退避させれば、より安全性が高まる。

また、退避させるデータを、外部メモリ501のみに限る必要はなく、一部のデータは外部メモリ501に退避させ、その他のデータはバス暗号領域502に退避させるなどとしてもよい。例えば、バス暗号鍵204と、バス暗号鍵設定レジスタ109にバス暗号鍵を設定するためのプログラムを外部メモリ501に退避させ、他のデータをバス暗号領域502に退避させる等とする。この場合、通常電力モードへの復帰時には、まず外部メモリ501からバス暗号鍵204をセキュア記憶部103に再設定する。次に、バス暗号鍵をバス暗号鍵設定レジスタ109に設定してから、バス暗号領域502に退避させていたデータをセキュア記憶部103に再設定する。

[0129] 1. 4 その他の変形例

(1) 電源A503、電源B504

電源A503および電源B504について補足すると、上述の構成に限らず、電源A503と電源B504が同一電源であり、システムLSI1000が省電力モードかそうでないかによって、電力の供給先を制御するとしてもよい。また、電源B504は、システムLSI1000に対して電力を供給することとしているが、組み込み機器1に含まれる他の構成要素に電力を供給することとしてもよい。

(2) 省電力モード、通常電力モードの切り換えの契機

上述の実施例では、組み込み機器1は、ユーザからの操作があるか否かに基づいて、システムLSI1000を省電力モードに移行させ、通常電力モードへ復帰させることとしている。

[0130] この他にも、システムLSI1000が省電力モードへの移行の判断等を行ってもよい。システムLSI1000が省電力モードへの移行の判断等を行う場合、例えば、電源B504から供給される電圧の変化に基づいて、電圧が所定の閾値を下回れば省電力モードへの移行を検知し、所定の閾値を上回れば通常電力モードへの復帰を検知するとしてもよい。

[0131] なお、この場合、電源B504からの電力供給が、システムLSI1000の退避時の処理が完了するまでに途絶えると、データの退避ができなくなる。そのため、退避時の処理が完了するのに必要な時間、電力を供給する予備の電源やコンデンサなどを予め用意してもよい。

また、電源B504の電圧の変化に基づいて、通常電力モードへの復帰を検知する場合、電源B504から電力が供給されていない状態で検知を行うこととなるので、電圧の変化を検出できないおそれがある。そのため、電源B504の電圧の変化を検出して通常電力モードへの復帰を検知する機構に対しては、電源B504とは異なる電源から電力を供給することが望ましい。例えば、電源A503から供給することとしてもよい。

[0132] この他にも、省電力モードへの移行の判断等は、通常プログラム205が制御することとしてもよいし、システムLSI1000に専用のハードウェアにより行っても良いし、退避指示部104や復帰指示部105に判断機能を持たせても良い。

また、復帰指示部105を備えなくとも、例えば、通常電力モードへの復帰の検知を、システムLSI1000の外部の機構により行い、検知時に、外部メモリ501に記憶させておいた復帰プログラムを、CPU110に実行させるよう割り込みをかけることとしてもよい。こうすることで、復帰指示部105そのものを省くことができ、余分なハードウェア構成を省いてシステムLSI1000の集積度を高めることができる。

[0133] また、システムLSI1000内のROMに、復帰プログラムを記憶させておき、通常電力モードからの復帰時にCPU110がROMから直接復帰プログラムを読み出して実行することとしてもよい。この構成によると、セキュア記憶部103に復帰プログラムを記憶させるステップを省略することができるため、より高速に復帰時の処理を実行することができる。このとき、復帰プログラムを、書き換え困難なROMに格納しておくと、復帰プログラム自体の改ざんを防ぐことができる。

(3) メモリ

上述の実施例では、外部メモリ501、バス暗号領域502、保護格納部102は、いずれも揮発性のメモリであるとしたが、省電力モード時においても記憶内容が消失しないのであれば、これに限られない。例えば、不揮発性のメモリや、ハードディスクなどでもよい。なお、不揮発性のメモリやハードディスクを用いると、電力を常時供給しなくとも記憶内容が保持されるので、電源A503は不要となる。

[0134] また、外部メモリ501、バス暗号領域502、保護格納部102は、揮発性のメモリである場合、組み込み機器1の電源がオフであれば記憶内容が消失するので、組み込み

機器1の電源がオフの間にこれらのメモリのデータが解析される等のおそれはなくなる。

また、セキュア記憶部103は、揮発性のメモリであるとしたが、不揮発性のメモリであってもよい。この場合においても、上述の実施例のように、省電力モードへの移行時にセキュア記憶部103の記憶内容を暗号化して外部メモリ501に退避させることで、不正な解析者の攻撃を避けることができる。

- [0135] 具体的に説明すると、セキュア記憶部103が不揮発性のメモリである場合は、システムLSI1000が省電力モード時においてもセキュア記憶部103の記憶内容が消失しない。そのため、省電力モードへの移行の前後において、セキュア記憶部103を用いた処理を継続して行うという点のみを考慮すると、上述の実施例のようにセキュア記憶部103の記憶内容を暗号化して外部メモリ501へ退避させる必要性は大きくなない。
- [0136] しかし、システムLSI1000がセキュア記憶部103を用いた処理を実行している途中でシステムLSI1000が省電力モードに移行すると、処理途中のデータがセキュア記憶部103に残ることとなる。そのため、不正な解析者が、システムLSI1000を省電力モードに移行させて、その間に、セキュア記憶部103の記憶内容を、時間をかけて解析しようと試みる可能性がある。セキュア記憶部103の記憶内容は、通常、機密性を保持すべき、価値の高いデータである。
- [0137] そこで、セキュア記憶部103を不揮発性のメモリとする場合は、システムLSI1000を省電力モードに移行させる時に、上述の実施例のようにセキュア記憶部103の記憶内容を暗号化して外部メモリに退避させるとともに、セキュア記憶部103の記憶内容を消去するとよい。こうすることにより、セキュア記憶部103が不揮発性のメモリである場合に、システムLSI1000がセキュア記憶部103を用いた処理の実行途中でシステムLSI1000を省電力モードに切り換えた上で、処理中のセキュア記憶部103の記憶内容を解析しようとする不正な解析者の攻撃を避けることができる。

(4) ソフトウェアまたはハードウェアによる実装

上記の実施例では、システムLSI1000の各構成要素は、ハードウェアにより実装することを想定しているが、これに限らない。例えば、退避指示部104や復帰指示部

105等を、ソフトウェアにより実装することとしてもよい。例えば、省電力モードへの移行や通常電力モードへの復帰を検知する機能を、セキュアなプログラム202、セキュアアプリ207、通常プログラム205等に持たせ、CPU110が実行することにより、退避指示部104等の機能を実装することができる。

[0138] これにより、ハードウェアリソースを少なくできるので、システムLSI1000の集積度を、さらに高めることができる。

さらに、ソフトウェアとハードウェアとを併用して、省電力モードへの移行等の検知の精度を、より高める構成としてもよい。

要するに、上記実施例の各構成要素を、実現可能な範囲でソフトウェアとして実装すると、必要なハードウェアが減るので回路の集積度が減る。また、ハードウェアとして実装すると、ソフトウェアによる実装と比べて処理を高速化することができる。特に、ユーザの利便性が求められる場合には、退避時の処理や復帰時の処理をハードウェアにより高速化すると有用である。

(5)その他

システムLSIは集積度の違いにより、IC、LSI、スーパーLSI、ウルトラLSIと呼称されることもあるが、システムLSI1000を上記のいずれの集積度で実現した場合も本発明に含まれることは言うまでもない。また、LSI製造後に、プログラムすることが可能なFPGA(Field Programmable Gate Array)や、LSI内部の回路セルの接続や設定を再構成可能なりコンフィギュラブル・プロセッサを利用しても良い。

[0139] さらには、半導体技術の進歩または派生する別技術によりLSIに置き換わる集積回路化の技術が登場すれば、当然、その技術を用いて構成要素の集積化を行ってもよい。バイオ技術の適用等が可能性としてありえる。

本発明は、上記に示す方法であるとしてもよい。また、これらの方法をCPUの処理として実現するプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。

[0140] また、本発明は、前記コンピュータプログラムまたは前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、フレキシブルディスク、ハードディスク、CD-ROM、MO、DVD、DVD-ROM、DVD-RAM、BD(Blu-ray Disc)、半導

体メモリなどに記録したものとしてもよい。また、これらの記録媒体に記録されている前記デジタル信号であるとしてもよい。

[0141] また、これらの実施の形態および変形例の組合せであってもよい。

産業上の利用可能性

[0142] 本発明は、省電力モードと通常電力モードにより動作し、秘匿すべきデータを安全に処理する機構を有するシステムLSI等において、データの安全性を確保しつつ、省電力化と処理の高速化を図ることができる。したがって、これらシステムLSI等を組み込んで著作権にかかるデータの処理を行う機器等において特に有用である。

請求の範囲

- [1] 動作モードとして、通常電力モードと、省電力モードとを切り換えて動作し、前記通常電力モード時には、秘匿すべき保護データに係る処理を少なくとも実行し、前記省電力モード時には、前記保護データを、外部メモリにおいて安全に保持するセキュア処理装置であつて、
データの暗号化および復号化を行う暗号処理部と、
データの内容に依存して定まり、当該データよりもデータサイズが小さい認証子を生成する生成部と、
自装置外部からの不正アクセスを防止する機構を有し、前記省電力モード時において、記憶内容が消失するメモリにより構成され、前記保護データを記憶するためのセキュア記憶部と、
前記通常電力モードまたは前記省電力モードのいずれの動作時であっても記憶内容を保持する機構、および、自装置外部からの不正アクセスを防止する機構を有し、前記セキュア記憶部よりも記憶容量が小さい保護格納部と、
前記省電力モードへの移行時に、前記保護データに基づいて、前記生成部に第1認証子を生成させ、生成された当該第1認証子を前記保護格納部に格納させるとともに、前記保護データを前記暗号処理部に暗号化させ、得られた暗号化データを前記外部メモリに記憶させるよう制御する移行制御部と、
前記通常電力モードへの復帰時に、前記外部メモリに記憶された前記暗号化データを前記暗号処理部に復号化させ、得られた復号化データに基づいて、前記生成部に第2認証子を生成させる認証子生成制御部と、
生成された前記第2認証子と、前記保護格納部に格納されている前記第1認証子とが一致するか否かを判断する判断部と、
一致しないと判断されると、前記復号化データの前記セキュア記憶部への書き込みを禁止し、一致すると判断されると、前記復号化データを前記セキュア記憶部へ書き込む復帰制御部とを備える
ことを特徴とするセキュア処理装置。
- [2] 前記セキュア処理装置は、さらに、バス暗号鍵を用いて暗号化したデータを、外部

の記憶領域であるバス暗号領域に保持させ、前記バス暗号領域に保持されているデータを用いて安全に処理を行うものであり、

前記セキュア記憶部は、さらに、前記バス暗号鍵を記憶し、

前記移行制御部は、前記省電力モードへの移行時に、前記セキュア記憶部に記憶されている前記バス暗号鍵を暗号化し、暗号化されたバス暗号鍵を前記外部メモリに記憶させるよう制御するバス暗号鍵退避制御部を含み、

前記復帰制御部は、前記外部メモリに記憶された前記暗号化されたバス暗号鍵を復号化するバス暗号鍵復号化制御部と、

前記バス暗号鍵復号化制御部により復号化されたバス暗号鍵を、前記セキュア記憶部へ書き込むバス暗号鍵再設定部を含む

ことを特徴とする請求項1記載のセキュア処理装置。

[3] 前記セキュア処理装置は、

前記バス暗号鍵を保持し、前記省電力モードへの移行が完了すると、保持内容が消失するバス暗号鍵設定レジスタと、

前記バス暗号鍵設定レジスタに保持されているバス暗号鍵を用いて、前記バス暗号領域へ出力するデータの暗号化、および、前記バス暗号領域から出力されるデータの復号化を行うバス暗号回路を含み、

前記セキュア記憶部が記憶している前記バス暗号鍵は、前記バス暗号鍵設定レジスタに保持されている前記バス暗号鍵と同一であり、

前記バス暗号鍵再設定部は、前記バス暗号鍵復号化制御部により前記復号化されたバス暗号鍵を、前記バス暗号鍵設定レジスタに保持させる
ことを特徴とする請求項2記載のセキュア記憶装置。

[4] 前記セキュア処理装置は、

前記バス暗号鍵設定レジスタと、前記バス暗号回路とからなる組を複数備え、

前記バス暗号鍵設定レジスタと前記バス暗号回路とからなる組のそれぞれは、前記バス暗号領域に保持されているデータそれぞれと対応しており、

前記セキュア記憶部は、前記バス暗号鍵設定レジスタそれぞれが保持している複数のバス暗号鍵それぞれと同一のバス暗号鍵を記憶しており、

前記バス暗号鍵退避制御部は、前記省電力モードへの移行時に、前記セキュア記憶部により記憶されている複数の前記バス暗号鍵を前記暗号化し、暗号化された複数のバス暗号鍵を前記外部メモリに前記記憶させ、

前記バス暗号鍵復号化制御部は、複数の前記バス暗号鍵を前記復号化し、

前記バス暗号鍵再設定部は、復号された前記複数の前記バス暗号鍵を、前記セキュア記憶部へ書き込む

ことを特徴とする請求項3記載のセキュア処理装置。

[5] 前記保護格納部は、不揮発性のメモリにより構成される

ことを特徴とする請求項1記載のセキュア処理装置。

[6] 前記保護格納部は、揮発性のメモリであり、前記省電力モード時においても電力が供給される構成を有する

ことを特徴とする請求項1記載のセキュア処理装置。

[7] 前記生成部は、データの内容に基づいて、ハッシュ関数によりハッシュ値を算出し、前記生成部が生成する前記認証子とは、前記算出されたハッシュ値であることを特徴とする請求項1記載のセキュア処理装置。

[8] 前記復帰制御部は、前記判断部により一致しないと判断されると、前記外部メモリに記憶された前記暗号化データを消去する消去部と、

前記暗号処理部により復号化された前記復号化データを破棄する破棄部とを含むことを特徴とする請求項1記載のセキュア処理装置。

[9] 前記セキュア処理装置は、前記通常電力モードへの復帰時に、前記外部メモリに記憶された前記暗号化データを消去するデータ消去部を含むことを特徴とする請求項1記載のセキュア処理装置。

[10] 前記セキュア処理装置は、さらに、

自装置を識別する情報である装置固有情報を記憶する固有情報保持部を含み、

前記暗号化部は、前記固有情報保持部に記憶されている装置固有情報に基づいた暗号鍵を用いて、前記暗号化および前記復号化を行う

ことを特徴とする請求項1記載のセキュア処理装置。

[11] 前記固有情報保持部は、自装置外部からの不正アクセスを防止する機構を有して

いる

ことを特徴とする請求項10記載のセキュア処理装置。

[12] 動作モードとして、通常電力モードと、省電力モードとを切り換えて動作し、前記通常電力モード時には、秘匿すべき保護データに係る処理を少なくとも実行し、前記省電力モード時には、前記保護データを、外部メモリにおいて安全に保持するセキュア処理装置であつて、

データの暗号化および復号化を行う暗号処理部と、

データの内容に依存して定まり、当該データよりもデータサイズが小さい認証子を生成する生成部と、

自装置外部からの不正アクセスを防止する機構を有し、前記省電力モード時において、記憶内容が消失するメモリにより構成され、前記保護データを記憶するためのセキュア記憶部と、

前記通常電力モードまたは前記省電力モードのいずれの動作時であっても記憶内容を保持する機構、および、自装置外部からの不正アクセスを防止する機構を有し、前記セキュア記憶部よりも記憶容量が小さい保護格納部と、

前記省電力モードへの移行時に、前記保護データを前記暗号処理部に暗号化させ、得られた暗号化データを前記外部メモリに記憶させるとともに、前記暗号化データに基づいて、前記生成部に第1認証子を生成させ、生成された当該第1認証子を前記保護格納部に格納させる移行制御部と、

前記通常電力モードへの復帰時に、前記外部メモリに記憶された前記暗号化データに基づいて、前記生成部に第2認証子を生成させる認証子生成制御部と、

生成された前記第2認証子と、前記保護格納部に格納されている前記第1認証子とが一致するか否かを判断する判断部と、

一致しないと判断されると、前記外部メモリに記憶された前記暗号化データを前記セキュア記憶部へ書き込むための処理を制限し、一致すると判断されると、前記暗号化データを前記暗号処理部に復号化させ、得られた復号化データを前記セキュア記憶部へ書き込む復帰制御部とを備える

ことを特徴とするセキュア処理装置。

- [13] 前記復帰制御部は、前記判断部により一致しないと判断されると、前記暗号化データの前記暗号処理部による復号化を実行しないことで、前記制限を行うことを特徴とする請求項12記載のセキュア処理装置。
- [14] 前記セキュア処理装置は、さらに、バス暗号鍵を用いて暗号化したデータを、外部の記憶領域であるバス暗号領域に保持させ、前記バス暗号領域に保持されているデータを用いて安全に処理を行うものであり、
前記セキュア記憶部は、さらに、前記バス暗号鍵を記憶し、
前記移行制御部は、前記省電力モードへの移行時に、前記セキュア記憶部に記憶されている前記バス暗号鍵を暗号化し、暗号化されたバス暗号鍵を前記外部メモリに記憶させるよう制御するバス暗号鍵退避制御部を含み、
前記復帰制御部は、前記外部メモリに記憶された前記暗号化されたバス暗号鍵を復号化するバス暗号鍵復号化制御部と、
前記バス暗号鍵復号化制御部により復号化されたバス暗号鍵を、前記セキュア記憶部へ書き込むバス暗号鍵再設定部を含む
ことを特徴とする請求項12記載のセキュア処理装置。
- [15] 前記セキュア処理装置は、
前記バス暗号鍵を保持し、前記省電力モードへの移行が完了すると、保持内容が消失するバス暗号鍵設定レジスタと、
前記バス暗号鍵設定レジスタに保持されているバス暗号鍵を用いて、前記バス暗号領域へ出力するデータの暗号化、および、前記バス暗号領域から出力されるデータの復号化を行うバス暗号回路を含み、
前記セキュア記憶部が記憶している前記バス暗号鍵は、前記バス暗号鍵設定レジスタに保持されている前記バス暗号鍵と同一であり、
前記バス暗号鍵再設定部は、前記バス暗号鍵復号化制御部により前記復号化されたバス暗号鍵を、前記バス暗号鍵設定レジスタに保持させる
ことを特徴とする請求項14記載のセキュア記憶装置。
- [16] 前記セキュア処理装置は、
前記バス暗号鍵設定レジスタと、前記バス暗号回路とからなる組を複数備え、

前記バス暗号鍵設定レジスタと前記バス暗号回路とからなる組のそれぞれは、前記バス暗号領域に保持されているデータそれぞれと対応しており、

前記セキュア記憶部は、前記バス暗号鍵設定レジスタそれぞれが保持している複数のバス暗号鍵それぞれと同一のバス暗号鍵を記憶しており、

前記バス暗号鍵退避制御部は、前記省電力モードへの移行時に、前記セキュア記憶部により記憶されている複数の前記バス暗号鍵を前記暗号化し、暗号化された複数のバス暗号鍵を前記外部メモリに前記記憶させ、

前記バス暗号鍵復号化制御部は、複数の前記バス暗号鍵を前記復号化し、

前記バス暗号鍵再設定部は、復号された前記複数の前記バス暗号鍵を、前記セキュア記憶部へ書き込む

ことを特徴とする請求項15記載のセキュア処理装置。

[17] 前記復帰制御部は、前記判断部により一致しないと判断されると、前記外部メモリに記憶された前記暗号化データを消去する消去部を含む
ことを特徴とする請求項12記載のセキュア処理装置。

[18] 動作モードとして、通常電力モードと、省電力モードとを切り換えて動作し、前記通常電力モード時には、秘匿すべき保護データに係る処理を少なくとも実行し、前記省電力モード時には、前記保護データを、外部メモリにおいて安全に保持するセキュア処理装置において用いられる、情報処理方法であって、

前記セキュア処理装置は、

自装置外部からの不正アクセスを防止する機構を有し、前記省電力モード時において、記憶内容が消失するメモリにより構成され、前記保護データを記憶するためのセキュア記憶部と、

前記通常電力モードまたは前記省電力モードのいずれの動作時であっても記憶内容を保持する機構、および、自装置外部からの不正アクセスを防止する機構を有し、前記セキュア記憶部よりも記憶容量が小さい保護格納部とを有し、

前記情報処理方法は、

データの暗号化および復号化を行う暗号処理ステップと、

データの内容に依存して定まり、当該データよりもデータサイズが小さい認証子を

生成する生成ステップと、

前記セキュア処理装置が前記省電力モードへ移行する時に、前記セキュア記憶部に記憶されている前記保護データに基づいて、前記生成ステップの実行により第1認証子を生成し、生成された当該第1認証子を前記保護格納部に格納させるとともに、前記保護データを前記暗号処理ステップの実行により暗号化し、得られた暗号化データを前記外部メモリに記憶させるよう制御する移行制御ステップと、

前記セキュア処理装置が前記通常電力モードへ復帰する時に、前記外部メモリに記憶された前記暗号化データを前記暗号処理ステップの実行により復号化し、得られた復号化データに基づいて、前記生成ステップの実行により第2認証子を生成するよう制御する認証子生成制御ステップと、

生成された前記第2認証子と、前記保護格納部に格納されている前記第1認証子とが一致するか否かを判断する判断ステップと、

前記判断ステップにおいて一致しないと判断されると、前記復号化データの前記セキュア記憶部への書き込みを禁止し、一致すると判断されると、前記復号化データを前記セキュア記憶部へ書き込む復帰制御ステップとを含むことを特徴とする情報処理方法。

[19] 動作モードとして、通常電力モードと、省電力モードとを切り換えて動作し、前記通常電力モード時には、秘匿すべき保護データに係る処理を少なくとも実行し、前記省電力モード時には、前記保護データを、外部メモリにおいて安全に保持するセキュア処理装置の動作を制御する制御プログラムであって、

前記セキュア処理装置は、

自装置外部からの不正アクセスを防止する機構を有し、前記省電力モード時において、記憶内容が消失するメモリにより構成され、前記保護データを記憶するためのセキュア記憶部と、

前記通常電力モードまたは前記省電力モードのいずれの動作時であっても記憶内容を保持する機構、および、自装置外部からの不正アクセスを防止する機構を有し、前記セキュア記憶部よりも記憶容量が小さい保護格納部とを有し、

前記制御プログラムは、

データの暗号化および復号化を行う暗号処理ステップと、
データの内容に依存して定まり、当該データよりもデータサイズが小さい認証子を
生成する生成ステップと、

前記セキュア処理装置が前記省電力モードへ移行する時に、前記セキュア記憶部
に記憶されている前記保護データに基づいて、前記生成ステップの実行により第1認
証子を生成し、生成された当該第1認証子を前記保護格納部に格納するとともに、
前記保護データを前記暗号処理ステップの実行により暗号化し、得られた暗号化デ
ータを前記外部メモリに記憶させるよう制御する移行制御ステップと、

前記セキュア処理装置が前記通常電力モードへ復帰する時に、前記外部メモリに
記憶された前記暗号化データを前記暗号処理ステップの実行により復号化し、得ら
れた復号化データに基づいて、前記生成ステップの実行により第2認証子を生成す
るよう制御する認証子生成制御ステップと、

生成された前記第2認証子と、前記保護格納部に格納されている前記第1認証子と
が一致するか否かを判断する判断ステップと、

前記判断ステップにおいて一致しないと判断されると、前記復号化データの前記セ
キュア記憶部への書き込みを禁止し、一致すると判断されると、前記復号化データを
前記セキュア記憶部へ書き込む復帰制御ステップとを含む
ことを特徴とする制御プログラム。

[20] 動作モードとして、通常電力モードと、省電力モードとを切り換えて動作し、前記通
常電力モード時には、秘匿すべき保護データに係る処理を少なくとも実行し、前記省
電力モード時には、前記保護データを、外部メモリにおいて安全に保持するセキュア
処理装置において用いられる、情報処理方法であって、

前記セキュア処理装置は、

自装置外部からの不正アクセスを防止する機構を有し、前記省電力モード時にお
いて、記憶内容が消失するメモリにより構成され、前記保護データを記憶するための
セキュア記憶部と、

前記通常電力モードまたは前記省電力モードのいずれの動作時であっても記憶内
容を保持する機構、および、自装置外部からの不正アクセスを防止する機構を有し、

前記セキュア記憶部よりも記憶容量が小さい保護格納部とを有し、

前記情報処理方法は、

データの暗号化および復号化を行う暗号処理ステップと、

データの内容に依存して定まり、当該データよりもデータサイズが小さい認証子を生成する生成ステップと、

前記セキュア処理装置が前記省電力モードへ移行する時に、前記保護データを前記暗号処理ステップの実行により暗号化し、得られた暗号化データを前記外部メモリに記憶させるとともに、前記暗号化データに基づいて、前記生成ステップの実行により第1認証子を生成し、生成された当該第1認証子を前記保護格納部に格納させるよう制御する移行制御ステップと、

前記セキュア処理装置が前記通常電力モードへ復帰する時に、前記外部メモリに記憶された前記暗号化データに基づいて、前記生成ステップの実行により第2認証子を生成するよう制御する認証子生成制御ステップと、

生成された前記第2認証子と、前記保護格納部に格納されている前記第1認証子とが一致するか否かを判断する判断ステップと、

前記判断ステップにおいて一致しないと判断されると、前記外部メモリに記憶された前記暗号化データを前記セキュア記憶部へ書き込むための処理を制限し、一致すると判断されると、前記暗号化データを前記暗号処理部ステップの実行により復号化し、得られた復号化データを前記セキュア記憶部へ書き込むよう制御する復帰制御ステップとを含む

ことを特徴とする情報処理方法。

[21] 動作モードとして、通常電力モードと、省電力モードとを切り換えて動作し、前記通常電力モード時には、秘匿すべき保護データに係る処理を少なくとも実行し、前記省電力モード時には、前記保護データを、外部メモリにおいて安全に保持するセキュア処理装置の動作を制御する制御プログラムであって、

前記セキュア処理装置は、

自装置外部からの不正アクセスを防止する機構を有し、前記省電力モード時において、記憶内容が消失するメモリにより構成され、前記保護データを記憶するための

セキュア記憶部と、

前記通常電力モードまたは前記省電力モードのいずれの動作時であっても記憶内容を保持する機構、および、自装置外部からの不正アクセスを防止する機構を有し、前記セキュア記憶部よりも記憶容量が小さい保護格納部とを有し、

前記制御プログラムは、

データの暗号化および復号化を行う暗号処理ステップと、

データの内容に依存して定まり、当該データよりもデータサイズが小さい認証子を生成する生成ステップと、

前記セキュア処理装置が前記省電力モードへ移行する時に、前記保護データを前記暗号処理ステップの実行により暗号化し、得られた暗号化データを前記外部メモリに記憶させるとともに、前記暗号化データに基づいて、前記生成ステップの実行により第1認証子を生成し、生成された当該第1認証子を前記保護格納部に格納させるよう制御する移行制御ステップと、

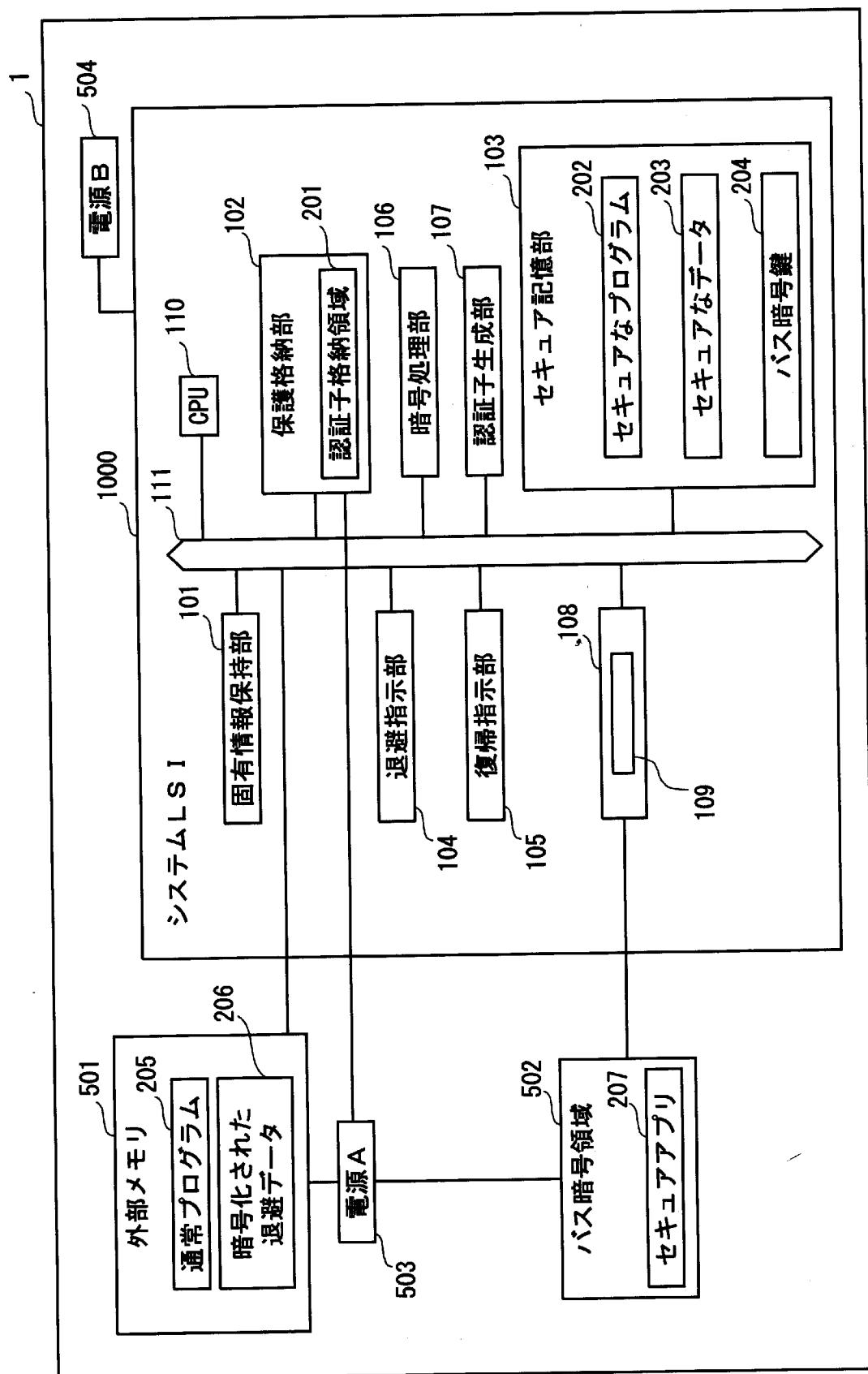
前記セキュア処理装置が前記通常電力モードへ復帰する時に、前記外部メモリに記憶された前記暗号化データに基づいて、前記生成ステップの実行により第2認証子を生成するよう制御する認証子生成制御ステップと、

生成された前記第2認証子と、前記保護格納部に格納されている前記第1認証子とが一致するか否かを判断する判断ステップと、

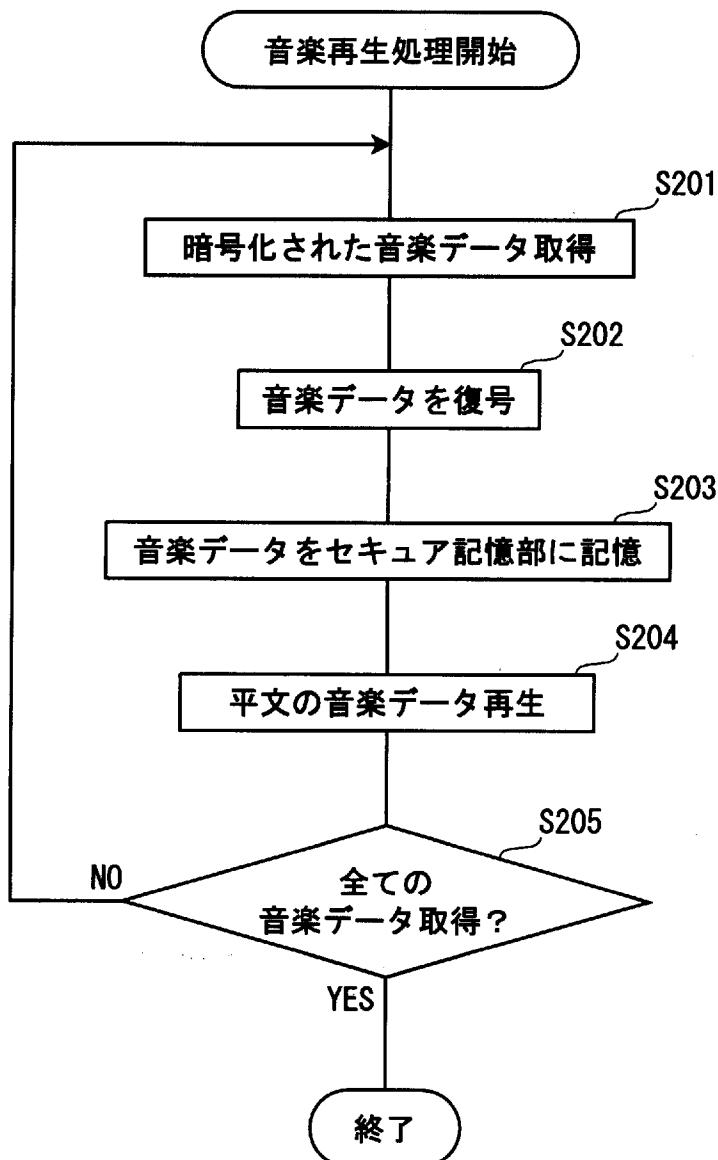
前記判断ステップにおいて一致しないと判断されると、前記外部メモリに記憶された前記暗号化データを前記セキュア記憶部へ書き込むための処理を制限し、一致すると判断されると、前記暗号化データを前記暗号処理部ステップの実行により復号化し、得られた復号化データを前記セキュア記憶部へ書き込むよう制御する復帰制御ステップとを含む

ことを特徴とする制御プログラム。

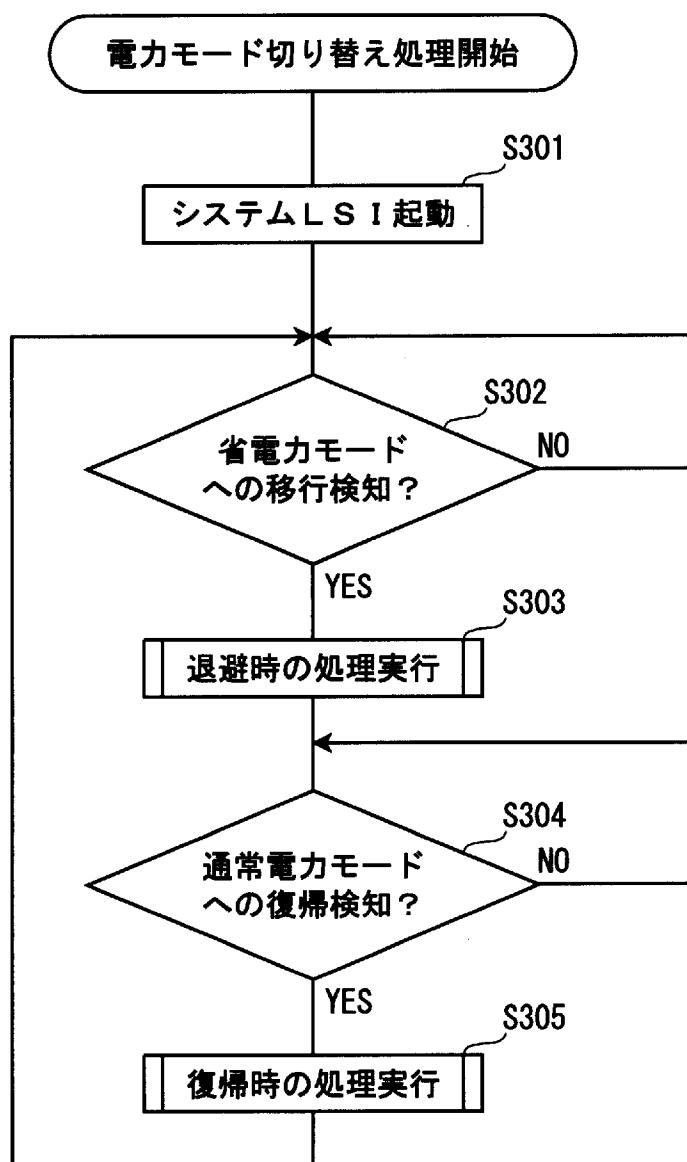
[図1]



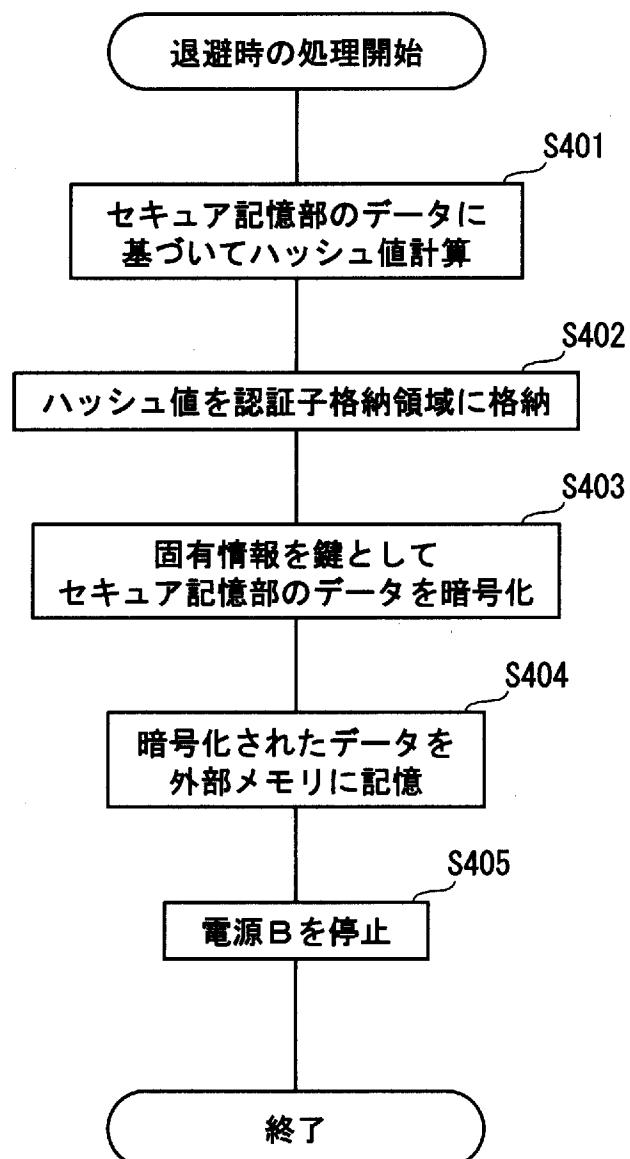
[図2]



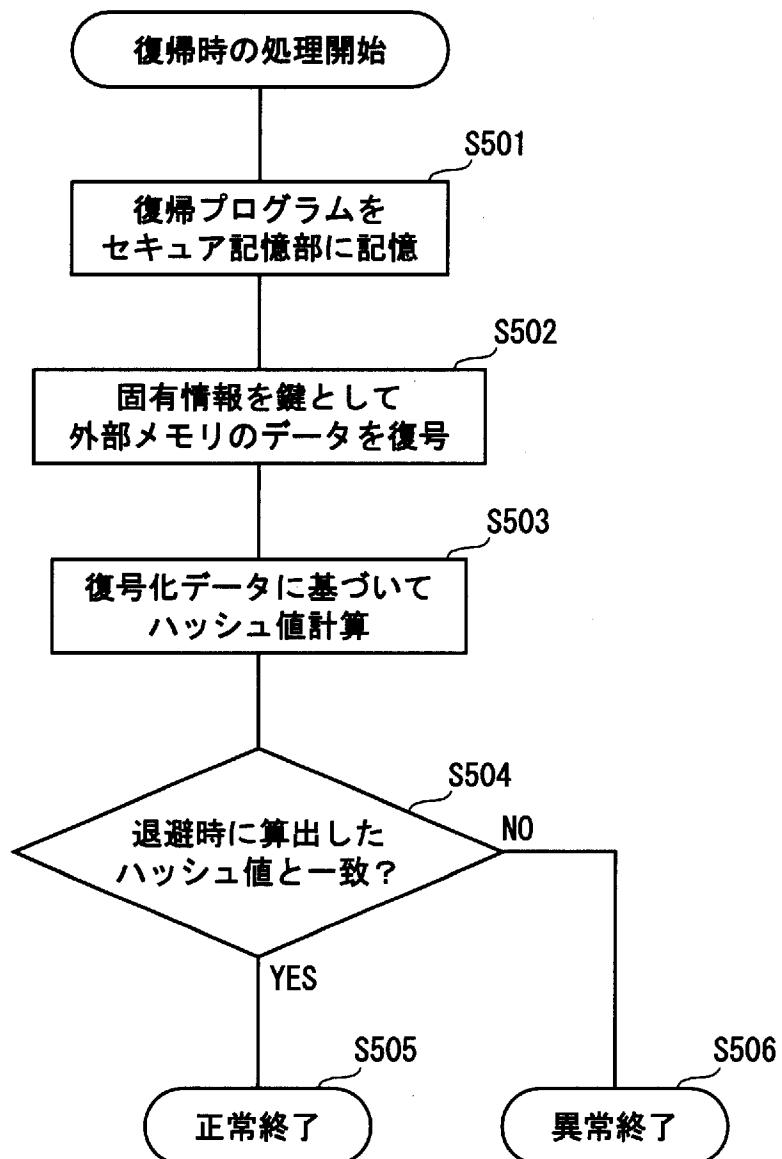
[図3]



[図4]



[図5]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2007/051804

A. CLASSIFICATION OF SUBJECT MATTER

H04L9/32 (2006.01) i, G09C1/00 (2006.01) i, H04L9/10 (2006.01) i

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)

H04L9/32, G09C1/00, H04L9/10

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

<i>Jitsuyo Shinan Koho</i>	<i>1922-1996</i>	<i>Jitsuyo Shinan Toroku Koho</i>	<i>1996-2007</i>
<i>Kokai Jitsuyo Shinan Koho</i>	<i>1971-2007</i>	<i>Toroku Jitsuyo Shinan Koho</i>	<i>1994-2007</i>

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
JSTPlus (JDream2)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2005-189969 A (The CREO Co., Ltd.), 14 July, 2005 (14.07.05), Full text; Figs. 1 to 8 (Family: none)	1-21
A	JP 2003-501747 A (International Business Machines Corp.), 14 January, 2003 (14.01.03), Full text: Figs. 1 to 9 & US 2000/6151664 A1 & WO 2000/075793 A1	1-21
A	JP 05-143478 A (Sharp Corp.), 11 June, 1993 (11.06.93), Full text; Figs. 1 to 3 (Family: none)	1-21

Further documents are listed in the continuation of Box C.

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

"&" document member of the same patent family

Date of the actual completion of the international search
26 February, 2007 (26.02.07)

Date of mailing of the international search report
06 March, 2007 (06.03.07)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

A. 発明の属する分野の分類（国際特許分類（IPC））

Int.Cl. H04L9/32(2006.01)i, G09C1/00(2006.01)i, H04L9/10(2006.01)i

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int.Cl. H04L9/32, G09C1/00, H04L9/10

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922-1996年
日本国公開実用新案公報	1971-2007年
日本国実用新案登録公報	1996-2007年
日本国登録実用新案公報	1994-2007年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

JSTPlus(JDream2)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	JP 2005-189969 A (株式会社クレオ) 2005.07.14, 全文, 図1-8 (ファミリーなし)	1-21
A	JP 2003-501747 A (インターナショナル・ビジネス・マシーンズ・コーポレーション) 2003.01.14, 全文, 図1-9 & US 2000/6151664 A1 & WO 2000/075793 A1	1-21
A	JP 05-143478 A (シャープ株式会社) 1993.06.11, 全文, 図1-3 (ファミリーなし)	1-21

□ C欄の続きにも文献が列挙されている。

□ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

- 「A」特に関連のある文献ではなく、一般的技術水準を示すもの
- 「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
- 「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
- 「O」口頭による開示、使用、展示等に言及する文献
- 「P」国際出願目前で、かつ優先権の主張の基礎となる出願
- 「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
- 「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
- 「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
- 「&」同一パテントファミリー文献

国際調査を完了した日 26.02.2007	国際調査報告の発送日 06.03.2007
国際調査機関の名称及びあて先 日本国特許庁 (ISA/JP) 郵便番号100-8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官（権限のある職員） 金丸 昌司 電話番号 03-3581-1101 内線 3546 5S 3574