

(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関  
国際事務局



(43) 国際公開日  
2006年11月30日 (30.11.2006)

PCT

(10) 国際公開番号  
WO 2006/126686 A1

(51) 国際特許分類:

G06F 21/22 (2006.01) G09C 1/00 (2006.01)  
G06F 12/14 (2006.01) H04L 9/14 (2006.01)  
G06F 21/24 (2006.01)

(21) 国際出願番号:

PCT/JP2006/310584

(22) 国際出願日:

2006年5月26日 (26.05.2006)

(25) 国際出願の言語:

日本語

(26) 国際公開の言語:

日本語

(30) 優先権データ:

特願2005-153478 2005年5月26日 (26.05.2005) 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).

(72) 発明者; および

(75) 発明者/出願人(米国についてのみ): 金村孝一 (KANE-MURA, Kouichi).

(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6F Osaka (JP).

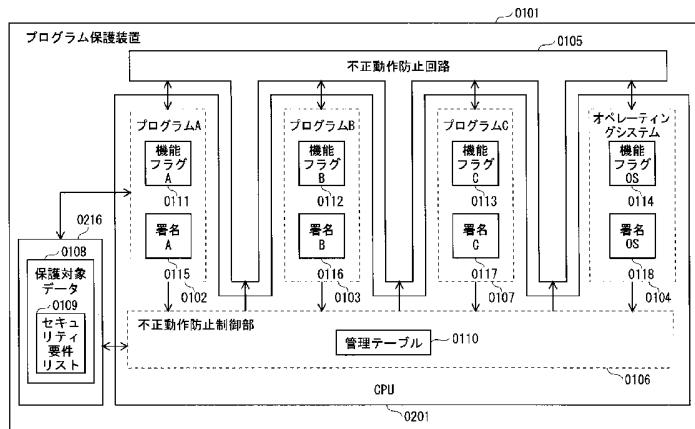
(81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(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),

[続葉有]

(54) Title: DATA PROCESSING DEVICE

(54) 発明の名称: データ処理装置



0101...PROGRAM PROTECTION DEVICE  
0105...UNLAWFUL ACTION PREVENTING CIRCUIT  
0102...PROGRAM A  
0111...FUNCTION FLAG A  
0115...SIGNATURE A  
0103...PROGRAM B  
0112...FUNCTION FLAG B  
0116...SIGNATURE B  
0107...PROGRAM C  
0113...FUNCTION FLAG C  
0117...SIGNATURE C  
0104...OPERATING SYSTEM  
0114...FUNCTION FLAG OS  
0118...SIGNATURE OS  
0108...PROTECTION TARGET DATA  
0109...SECURITY REQUIREMENT LIST  
0106...UNLAWFUL ACTION PREVENTING CONTROL UNIT  
0110...MANAGEMENT TABLE

(57) Abstract: Provided is a data processing device capable of preventing the data to be handled by each program from being unlawfully used by another program irrespective of the quality of the program. Included are a CPU (0201) for executing the program, and an unlawful action preventing circuit (0105) for preventing the data to be used by each program from being unlawfully accessed by another program. An unlawful action preventing control unit (0106) for acting in a protection mode to control the unlawful action preventing circuit (0105) decides it, on the basis of a function flag assigned to a program B (0103) to act in an ordinary mode, whether or not a memory area can be used by a program A (0102) to act in the ordinary mode, and sets, if the memory area is used, the unlawful action preventing circuit (0105) so that the memory area may be used by the program B (0103).

[続葉有]

WO 2006/126686 A1



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

---

(57) 要約: プログラムの品質によらず、各プログラムが取り扱うデータが、他のプログラムにより不正使用されるのを防ぐことができるデータ処理装置を提供する。 プログラムを実行するCPU0106と、各プログラムが使用するデータを他のプログラムが不正アクセスするのを防止する不正動作防止回路0105とを備え、保護モードで動作し不正動作防止回路0105を制御する不正動作防止制御部0106が、通常モードで動作するプログラムA0102が使用しているメモリ領域について、通常モードで動作するプログラムB0103に割り当てられた機能フラグに基づき、前記メモリ領域の使用可否を判定し、使用させる場合にプログラムB0103に当該メモリ領域が使用できるよう不正動作防止回路0105に設定する。

## 明細書

### データ処理装置

#### 技術分野

- [0001] 本発明は、複数プロセスの連携動作により保護データを処理するデータ処理装置に関し、特に、保護データに対する不正処理を防ぐ技術に関する。

#### 背景技術

- [0002] 近年、音楽や映画などのコンテンツを再生するコンテンツ再生装置など多くのデジタル家電に、著作権保護のためのデータの暗号化、復号の機能(特許文献1～3、非特許文献1～2参照)や、販売後における新機能の追加及びバグ修正などのためのプログラム更新機能などが実装されてきている。

特許文献1:特開平2-155034号公報

特許文献2:特開平4-102920号公報

特許文献3:特開2001-318787号公報

非特許文献1:Lie, D., Thekkath, C. A., Mitchell, M., Lincoln, P., Boneh, D., Mitchell, J. C. and Horowitz, M.: Architectural Support for Copy and Tamper Resistant Software, In Proceedings of the 9th Inte'l Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS-IX), pages 169-177, November 2000.

非特許文献2:E. Suh, D. Clarke, B. Gassend, M. van Dijk, and S. Devadas. The AEGIS processor architecture for tamper evident and tamper resistant processing. Technical Report LCS-TM461, Massachusetts Institute of Technology, February 2003.

#### 発明の開示

##### 発明が解決しようとする課題

- [0003] 前述の暗号化、復号などデータに対する処理はプログラム自身の管理下で行っており、前記データが他のプログラムにより漏洩させられることはない。

しかしながら、暗号化データを復号する復号プログラムと、復号後のデータを再生するプレーヤプログラムとの間でデータを連携処理するような場合には、当該データを複数のプログラムから使用できるようにする必要があるので、前述の更新機能を悪用されて不正なプログラムが導入されると、当該不正なプログラムによって前記データが漏洩されてしまうという問題が生じうる。

- [0004] 上記問題に鑑み、本発明は、各プログラムが取り扱うデータを連携処理するような場合にも、当該データの漏洩を防ぐことができるデータ処理装置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

- [0005] 上記課題を解決するために、本発明は、プログラムに従って動作するプロセッサを備え、前記プログラムの実行単位であるプロセスが動作する通常モードと前記プロセスの動作が抑制される保護モードを切り替えて動作するデータ処理装置であって、通常モードにおいて、第1プロセスの処理対象データに対して、前記第1プロセスによるアクセスを許可し、他のプロセスによるアクセスを禁止するアクセス禁止手段と、通常モードにおいて、前記第1プロセスから、第2プロセスの呼び出しを指示する呼出命令を検出する検出手段と、前記呼出命令が検出されると、通常モードから保護モードに切り替える切替手段と、保護モードにおいて、前記第2プロセスが、前記処理対象データについての使用権限を有しているか否かを判断する判断手段と、保護モードにおいて、前記第2プロセスが使用権限を有していると判断される場合に、前記アクセス禁止手段に対して、前記第2プロセスが前記通常モードにおいて、前記処理対象データに対しアクセスすることが許可されるように制御する制御手段とを備える。

### 発明の効果

- [0006] 本発明のデータ処理装置は、上述の構成を備えることにより、第1プロセスが、第2プロセス以外のプロセスに知られないよう第2プロセスにデータを受け渡すことができ、通常モードで動作する他のプロセスによってデータが漏洩されるのを防ぐことができる。

また、上述の構成を備えることにより、第2のプログラムが更新されて機能が変更され

、処理対象データの使用権限を失った場合においても前記判断手段がそれを検知し、前記制御手段で情報漏洩を防止できる。

- [0007] また、前記アクセス禁止手段は、メモリと、プロセス毎の前記メモリ内でアクセスを許可する領域を示す管理情報を、保護モードにおいてのみ書き換え可能に保持する保持部と、通常モードで動作するプロセスを、前記管理情報に従って前記メモリにアクセスさせるアクセス制限部とを含み、前記制御手段は、前記判断手段により使用権限があると判定された場合に、第2プロセスの管理情報に、前記メモリ上で前記対象データが保持されている領域へのアクセスを許可する情報を追加することとしてもよい。
- [0008] この構成によれば、前記管理情報の書き換えを保護モードである場合に制限するので、通常モードで動作する他のプロセスにより、前記管理情報をデータの漏洩が可能なよう不正に書き換えられるのを防ぐことができる。
- また、前記保持部が保持する前記管理情報は、前記メモリ中のアドレスと、アドレスに対応する鍵とを対応づけた情報を一以上含み、前記アクセス制限部は、前記メモリのアドレスを含む前記メモリへのアクセス要求を取得する取得部と、前記アクセス要求に含まれるアドレスが、前記管理情報に含まれるか否かを判定するアドレス判定部と、含まれると判定された場合に、前記アクセス要求が書込要求であれば、書き込むデータを前記アドレスに対応する鍵で暗号化して前記アドレスで示される領域に書込み、前記アクセス要求が読み出要求であった場合には、前記メモリの前記アドレスから読み出したデータを、前記アドレスに対応する鍵を用いて復号して出力するアクセス実行部とを含むこととしてもよい。
- [0009] この構成によれば、プロセス毎に定められているアドレス毎の鍵で前記メモリにデータを暗号して記録し、暗号して記録されたデータを復号して読み出すので、他のプロセスによって、前記データが適切に使用されるのを防ぐことができる。
- ここで、メモリへのアクセス要求には、前記メモリからデータを読み出す読み出要求や、前記メモリへのデータの書込要求の他、使用を要望する前記メモリの領域の使用許可要求や、他のプロセスが使用許可されているメモリの領域を、自プロセスでも使用するための共有設定要求などが含まれるものとする。

- [0010] また、前記データは、プロセスのコードであることとしてもよい。  
この構成によれば、プロセスのコードが、漏洩するのを防ぐことができる。  
また、各プロセスには、個別のプロセス識別子が割り当てられ、前記保持部が保持する前記管理情報は、前記メモリ中のアドレスと、前記アドレスへのアクセスが許可されているプロセス識別子とを対応付けた情報を一以上含み、前記アクセス制限部は、前記メモリのアドレスを含む前記メモリへのアクセス要求を取得する取得部と、アクセス要求に含まれるアドレスと、アクセス要求したプロセスに割り当てられたプロセス識別子とを対応付けた情報が、前記管理情報に含まれるか否かを判定するアドレス判定部と、含まれると判定された場合に、アクセス要求したプロセスを、前記メモリの前記アドレスにアクセスさせるアクセス実行部とを含むこととしてもよい。
- [0011] この構成によれば、メモリへのアクセス要求があっても、前記メモリの前記アドレスへのアクセスを、前記管理情報に含まれるアクセス要求されたアドレスに対応するプロセス識別子で示されるプロセスのみに制限するので、他のプロセスにより前記データが漏洩されるのを防ぐことができる。  
また、前記データには、一以上のデータ処理方法それぞれについて実行を許可するか否かを示すセキュリティ要件情報が割り当てられ、プロセスそれぞれには、一以上のデータ処理方法それを実行可能か否かを示す機能情報が割り当てられ、前記呼出命令は、一以上のデータ処理方法のいずれかを示す処理特定情報を含み、前記判断手段は、前記セキュリティ要件情報が前記処理特定情報により示されるデータ処理方法の実行を許可しておりかつ第2プロセスの機能情報が、前記処理特定情報により示されるデータ処理方法の実行が可能であることを示す場合に、前記使用権限があると決定することとしてもよい。
- [0012] この構成によれば、前記データ連携が要求されているデータを、当該データに割り当てられたセキュリティ要件情報により許可され、かつ、第2プロセスの機能情報が実行可能であることを示しているデータ処理方法による処理に限定し、データの漏洩の可能性を低減することができる。  
また、前記切替手段は、前記通常モードから前記保護モードへと切り替える場合に、前記通常モードで動作しているプロセスのコンテキストを前記メモリに退避し、前記

保護モードから前記通常モードへと切り替える場合に、次に前記通常モードで動作するプロセスのコンテキストを前記メモリから復帰させることとしてもよい。

- [0013] この構成によれば、コンテキストの退避、復帰の処理実行を、保護モードである場合に限定できるので、通常モードで動作するプロセスによって、コンテキストに対し不正な操作がされ、データが漏洩されるのを防ぐことができる。

また、前記第1プロセス及び前記第2プロセスは、それぞれが動作している間に割り込み又は例外が発生した場合に、その割り込み又は例外を処理する割込処理又は例外処理を含み、前記データ処理装置は、さらに、割り込み又は例外が発生した場合に、実行されるべき処理を示すベクタテーブルを、保護モードにおいてのみ書き換え可能に保持するベクタテーブル保持手段と、動作するプロセスが、前記第1プロセスから前記第2プロセスへと切り替わる前に、保護モードにおいて前記ベクタテーブルを、前記通常モードにおいて割り込み又は例外が発生した際に第2プロセスの割込処理又は例外処理を実行するよう書き換えるベクタテーブル書換手段とを含むこととしてもよい。

- [0014] この構成によれば、ベクタテーブルの変更を、保護モードである場合に限定できるので、通常モードで動作するプロセスによって、ベクタテーブルに対し不正な書換操作がされることにより、不正なプロセスが実行され、データが漏洩されるのを防ぐことができる。

また、前記判断手段は、さらに、プロセスから前記メモリにおける領域の使用要求を受け付ける使用要求受付部と、使用要求されたアドレスが、既に使用されているか否かを判定する使用判定部と、使用されていなかった場合に、使用要求したプロセスの、前記アドレスに格納を要望するデータについての使用権限の有無を判定する権限判定部と、前記権限判定部により使用権限があると判定された場合に、使用要求したプロセスの管理情報に、前記アドレスで示される領域へのアクセスを許可する情報を登録する管理情報登録部とを含むこととしてもよい。

- [0015] この構成によれば、プロセスからの要求に従い、使用を要求したプロセスのみが、要求したメモリの領域を使用できるように、管理情報を生成し、他のプロセスによって、前記領域に記憶されるデータが漏洩されるのを防ぐことができる。

また、前記管理情報登録部は、前記権限判定部により使用権限があると判定された場合に、鍵を生成し、前記アクセスを許可する情報として、前記アドレスと生成した鍵とを対応付けた情報を使用要求した前記プロセスの管理情報に追加することとしてもよい。

- [0016] この構成によれば、要求されるごとに毎に生成する鍵を、管理情報に追加することができる。

アドレス毎に異なる鍵を用いることなどとすれば、同じ鍵を用いる頻度が少なくなり鍵が解読される確率を低下させることができる。

また、前記データ処理装置は、さらに、前記プロセスに係るデバッグを行うデバッグ手段を含み、前記切替手段は、さらに、前記通常モードに切り替える場合に、前記デバッグ手段を有効化し、前記保護モードに切り替える場合に、前記デバッグ手段を無効化することとしてもよい。

- [0017] この構成によれば、保護モードにおけるデバッグを禁止し、保護モードにおける処理内容を、解析されるのを防ぐことができる。

本発明のデータ処理方法は、プログラムに従って動作するプロセッサを備え、前記プログラムの実行単位であるプロセスが動作する通常モードと前記プロセスの動作が抑制される保護モードを切り替えて動作するデータ処理装置に用いられるデータ処理方法であって、通常モードにおいて、第1プロセスの処理対象データに対して、前記第1プロセスによるアクセスを許可し、他のプロセスによるアクセスを禁止するアクセス禁止ステップと、通常モードにおいて、前記第1プロセスから、第2プロセスの呼び出しを指示する呼出命令を検出する検出ステップと、前記呼出命令が検出されると、通常モードから保護モードに切り替える切替ステップと、保護モードにおいて、前記第2プロセスが、前記処理対象データについての使用権限を有しているか否かを判断する判断ステップと、保護モードにおいて、前記第2プロセスが前記使用権限を有していると判断される場合に、前記アクセス禁止手段に対して、前記第2プロセスが前記通常モードにおいて、前記処理対象データに対しアクセスすることが許可されるように制御する制御ステップとを含む。

- [0018] 本発明のコンピュータプログラムは、プログラムに従って動作するプロセッサを備え

、前記プログラムの実行単位であるプロセスが動作する通常モードと前記プロセスの動作が抑制される保護モードを切り替えて動作するデータ処理装置に用いられるコンピュータプログラムであって、通常モードにおいて、第1プロセスの処理対象データに対して、前記第1プロセスによるアクセスを許可し、他のプロセスによるアクセスを禁止するアクセス禁止ステップと、通常モードにおいて、前記第1プロセスから、第2プロセスの呼び出しを指示する呼出命令を検出する検出ステップと、前記呼出命令が検出されると、通常モードから保護モードに切り替える切替ステップと、保護モードにおいて、前記第2プロセスが、前記処理対象データについての使用権限を有しているか否かを判断する判断ステップと、保護モードにおいて、前記第2プロセスが前記使用権限を有していると判断される場合に、前記アクセス禁止手段に対して、前記第2プロセスが前記通常モードにおいて、前記処理対象データに対しアクセスすることが許可されるように制御する制御ステップとを含む。

- [0019] この構成によれば、第1プロセスが、第2プロセス以外のプロセスに知られないよう第2プロセスにデータを受け渡すことができ、通常モードで動作する他のプロセスによってデータが漏洩されるのを防ぐことができる。  
また、上述の構成を備えることにより、第2のプログラムが更新されて機能が変更され、処理対象データの使用権限を失った場合においても前記判断ステップによりそれを検知し、前記制御ステップによって情報漏洩を防止できる。
- [0020] 本発明の集積回路は、プログラムに従って動作するプロセッサを備え、前記プログラムの実行単位であるプロセスが動作する通常モードと前記プロセスの動作が抑制される保護モードを切り替えて動作する集積回路であって、通常モードにおいて、第1プロセスの処理対象データに対して、前記第1プロセスによるアクセスを許可し、他のプロセスによるアクセスを禁止するアクセス禁止手段と、通常モードにおいて、前記第1プロセスから、第2プロセスの呼び出しを指示する呼出命令を検出する検出手段と、前記呼出命令が検出されると、通常モードから保護モードに切り替える切替手段と、保護モードにおいて、前記第2プロセスが、前記処理対象データについての使用権限を有しているか否かを判断する判断手段と、保護モードにおいて、前記第2プロセスが前記使用権限を有していると判断される場合に、前記アクセス禁止手段に対し

て、前記第2プロセスが前記通常モードにおいて、前記処理対象データに対しアクセスすることが許可されるように制御する制御手段とを備える。

[0021] この構成によれば、第1プロセスが、第2プロセス以外のプロセスに知られないよう第2プロセスにデータを受け渡すことができ、通常モードで動作する他のプロセスによってデータが漏洩されるのを防ぐことができる。

また、上述の構成を備えることにより、第2のプログラムが更新されて機能が変更され、処理対象データの使用権限を失った場合においても前記判断手段がそれを検知し、前記制御手段で情報漏洩を防止できる。

### 図面の簡単な説明

[0022] [図1]本発明に係るプログラム保護装置の構成の主要部を模式的に示す図である。

[図2]本発明に係るプログラム保護装置のハードウェア構成を示す図である。

[図3]鍵レジスタの構成を示す図である。

[図4]保護対象データの構成を示す図である。

[図5]プログラムを記録するファイルの構成を模式的に示す図である。

[図6]プログラムを記録するファイルの構成を模式的に示す図である。

[図7]プログラム保護装置のソフトウェア構成を示す図である。

[図8]管理テーブルの構成を示す図である。

[図9]管理テーブルの構成を示す図である。

[図10]不正動作防止制御処理を示すフローチャートである。

[図11]状態切替動作A及びBの処理を示すフローチャートである。

[図12]プログラムXからの要求に対する不正動作防止制御部の処理を示すフローチャートである。

[図13]プログラムの全体動作を示すフローチャートである。

[図14]プログラムの全体動作を示すフローチャートである(図13の続き)。

[図15]プログラム保護装置の動作を示すフローチャートである。

[図16]プログラム保護装置の動作中のRAMの状態を示す。

[図17]プログラム保護装置の動作中の管理テーブルの状態を示す。

[図18]プログラム保護装置の動作中の管理テーブルの状態を示す。

[図19]プログラム保護装置の動作中の管理テーブルの状態を示す。

[図20]プログラムの機能フラグがセキュリティ要件を満たすか否かを判定する処理を示すフローチャートである。

[図21]プログラム保護装置におけるプログラムの動作を示すフローチャートである。

[図22]変形例に係るプログラム保護装置の構成を示すブロック図である。

[図23]変形例に係るIDレジスタの構成を示す図である。

### 符号の説明

- [0023] 0101 プログラム保護装置
- 0102 プログラムA
- 0103 プログラムB
- 0104 オペレーティングシステム(OS)
- 0105 不正動作防止回路
- 0106 不正動作防止制御部
- 0107 プログラムC
- 0108 保護対象データ
- 0109 セキュリティ要件リスト
- 0110 管理テーブル
- 0201 CPU
- 0202 RAM
- 0203 不揮発メモリ
- 0204 バス暗号回路
- 0205 鍵レジスタ
- 0206 保護メモリ
- 0207 アクセス制限回路
- 0208 状態切替回路
- 0209 デバッガI/F
- 0210 バス
- 0216 蓄積メディア

- 0219 ベクタテーブル
- 0221 不揮発メモリ
- 0401 セキュリティカーネル
- 0402 プログラムA用割り込み管理部
- 0403 プログラムB用割り込み管理部
- 0404 OS用割り込み管理部
- 0405 BIOS
- 0406 プログラムC用割り込み管理部

### 発明を実施するための最良の形態

[0024] <第1実施形態>

#### <1. 概要>

図1は、プログラム保護装置0101の構成の主要な部分を模式的に示した図である。

。

プログラム保護装置0101は、図1に示すように、CPU0201と、不正動作防止回路0105と、蓄積メディア0216とを含んで構成される。

[0025] CPU0201は、プログラムを実行するプロセッサである。

不正動作防止回路0105は、CPU0201により実行されるプログラムの不正実行及びプログラム間の不正アクセスを防ぐための機構を備えた回路である。

蓄積メディア0216は、CPU0201により実行されるプログラムが扱う、コンテンツや個人情報などの機密情報である保護対象データ0108を、暗号化した状態で記憶している。

[0026] CPU0201上で実行されるプログラムには、一例として図1に示すようにオペレーティングシステム(OS)0104、プログラムA0102、プログラムB0103、プログラムC0107、不正動作防止制御部0106等がある。

不正動作防止制御部0106は、プログラムA0102、プログラムB0103、プログラムC0107その他の各プログラムとOS0104のそれぞれから、メモリ領域の使用要求を取得して使用可否を判定し、使用させる場合には不正動作防止回路0105を制御し

て、要求元のプログラムが要求する様態でのみ、当該メモリ領域の使用をさせる。

- [0027] オペレーティングシステム(OS)0104は、プログラムA0102、プログラムB0103、プログラムC0107その他のプログラム(図示せず)を動作させる基本ソフトウェアである。

プログラムA0102、プログラムB0103、プログラムC0107は、任意の処理を実行するアプリケーションプログラムである。本実施形態では、一例として、プログラムA0102が、コンテンツである保護対象データ0108の復号を行うプログラムであり、プログラムB0103は、コンテンツの再生を行うプレーヤープログラムであり、プログラムA0102とプログラムB0103は、コンテンツを処理する際に連携動作するものとする。

- [0028] プログラムA0102は、保護対象データ0108である暗号化されたコンテンツを復号し、復号済みの当該コンテンツをプログラムB0103に再生させる。プログラムA0102は、プログラムB0103を呼び出すための呼出命令を含んでおり、CPU0201は前記呼出命令を検出すると、不正動作防止回路0105に後述する保護モードを示す状態切替指示を行う。不正動作防止回路0105は、前記状態切替指示に基づき、保護モードへと切り替えて、処理を実行する。

前記呼出命令は、コンテンツの出力、コピー、移動、特殊再生、デジタル出力などのデータ処理方法を示す情報を含むものとする。

また、不正動作防止制御部0106が前記保護モードにおいて不正動作防止回路0105を制御することにより、例えば、プログラムC0107が、前記コンテンツを不正に使用したり、コンテンツを破壊するようなことを妨げている。

- [0029] 以下、プログラム保護装置0101の動作について、詳細に説明する。

## <2. 構成>

### <2. 1. ハードウェア構成>

プログラム保護装置0101のハードウェア構成について、図面を用いて説明する。

プログラム保護装置0101は、図2に示すように、相互にバス0210を介して接続されるCPU0201、不揮発メモリ0203、バス暗号回路0204、鍵レジスタ0205、アクセス制限回路0207、状態切替回路0208、デバッガI/F0209、蓄積メディア0216、不揮発メモリ0221と、バス暗号回路0204に接続するRAM0202と、アクセス制限回

路0207に接続する保護メモリ0206を含んで構成される。

- [0030] プログラム保護装置0101は、具体的には、マイクロプロセッサ、ROM、RAMなどから構成されるコンピュータシステムである。前記ROMには、コンピュータプログラムが記憶されており、前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、プログラム保護装置0101は、その機能を達成する。
- CPU0201は、RAM0202、保護メモリ0206上に記憶されるプログラムを実行するマイクロプロセッサである。
- [0031] 状態切替回路0208は、CPU0201から、前記通常モードと前記保護モードとのいずれかを選択的に示す状態切替指示を受けつけて、デバッガIF0209、鍵レジスタ0205、アクセス制限回路0207を、当該状態切替指示に対応するモードに切り替える。
- 保護モードは、セキュリティの高い特定のプログラムのみが動作するモードであり、通常モードは、その他のプログラムが動作するモードである。
- [0032] 状態切替回路0208は、受信した前記状態切替指示が保護モードを示す場合には、デバッガI/F0209に対し保護モードを示す状態信号A0211を出力してデバッガI/F209を無効化し、鍵レジスタ0205に対し保護モードを示す状態信号B0217を出力し、アクセス制限回路0207に対し保護モードを示す状態信号C0218を出力する。
- [0033] また、状態切替回路0208は、受信した前記状態切替指示が通常モードを示す場合には、デバッガI/F0209に対し通常モードを示す状態信号A0211を出力し、鍵レジスタ0205に対し通常モードを示す状態信号B0217を出力し、アクセス制限回路0207に対し通常モードを示す状態信号C0218を出力する。また、状態切替回路0208は必要に応じてベクターテーブル0219の変更を行う。状態を切り替える動作、ベクターテーブル0219の変更については後述する。
- [0034] なお、状態切替の詳細は発明者らによる出願、特開2005-11336号公報などに開示されている。
- アクセス制限回路0207は、バス0210と保護メモリ0206の接続を制御する回路であり、状態切替回路0208から受け取る状態信号Cが通常モードを示す場合には、バ

ス0210と保護メモリ0206との接続を遮断し、保護モードを示す場合には、バス0210と保護メモリ0206を接続する。よって、通常モードで動作するプログラムは、保護メモリ0206内のデータにアクセスすることはできない。

- [0035] デバッガI/F0209は、プログラム保護装置0101外のプログラムデバッガを接続可能なインターフェイスであり、CPU0201と接続されている。

デバッガI/F0209は、状態切替回路0208から通知される状態信号Aが、通常モードを示す場合に、前記プログラムデバッガとCPU0201とを接続し、状態信号Aが保護モードを示す場合に、プログラムデバッガとCPU0201との接続を切断する。

- [0036] また、状態信号Aが通常モードを示す場合であっても、デバッガI/F0209の設定を変更することにより、プログラムデバッガとCPU0201との接続を強制的に切断状態にすることも可能である。

鍵レジスタ0205は、アクセス要求されたアドレスに対応する暗号鍵をバス暗号回路0204に出力する回路である。

- [0037] 鍵レジスタ0205は、図3に示すように、アドレスと命令用バス暗号鍵との対応を示す命令用鍵情報テーブル0305と、アドレスとデータ用バス暗号鍵との対応を示すデータ用鍵情報テーブル0306とを保持しており、バス暗号回路0204からアドレス信号0301を取得して、アドレス信号0301が示すアドレスに対応づけられている命令用バス暗号鍵信号0302と、データ用バス暗号鍵信号0303とをバス暗号回路0204に出力する。

- [0038] ここで、命令用鍵情報テーブル0305は、命令用鍵情報T0311、T0312、T0313…を含み、各命令用鍵情報は、アドレスと命令用バス暗号鍵との対応を示しており、データ用鍵情報テーブル0306は、データ用鍵情報T0321、T0322、T0323…を含み、各データ用鍵情報は、アドレスとデータ用バス暗号鍵との対応を示している。

- [0039] 鍵レジスタ0205の設定の変更は、状態切替回路0208が 출력する状態信号Bが保護モードを示すときのみ変更可能であり、不正動作防止制御部0106によって、バス0210を介して通知される設定信号0304を用いて変更される。

RAM0202は、バス暗号回路0204と接続されているメモリ装置である。

バス暗号回路0204は、鍵レジスタ0205から通知される鍵を用いて、当該鍵に対

応付けられたメモリアドレスに入出力するコードやデータの暗号化や復号を行う。

- [0040] これにより、バス0210とRAM0202との間でやり取りされるコードやデータは、バス暗号回路0204で暗号化及び復号される。

また、バス暗号回路0204は、CPU0201が命令フェッチのためにRAM0202にアクセスしているのか、データアクセスのためにアクセスしているのかを検知し、同一物理アドレスへの命令フェッチの場合には命令用バス暗号鍵を用い、データアクセスの場合にはデータ用バス暗号鍵を用いて、コードやデータの暗号化、復号を行う。

- [0041] 不揮発メモリ0203は、ファイルA0212、ファイルB0213、ファイルC0214、ファイルOS0215、BIOS0405、ファイルS0220を記憶している。

ここで、前記ファイルのデータ構造について、ファイルA0212のデータ構造を例に、図5を用いて説明する。

ファイルA0212は、コード暗号鍵0710、プログラムA0102のコード0711、署名A0115、機能フラグA0111を含む。

- [0042] コード暗号鍵0710は、プログラムAのコード0711を暗号化するために用いた鍵(KC\_A)である。

コード暗号鍵0710は、公開鍵暗号アルゴリズムで暗号化されている。

コード暗号鍵0710を暗号化する際に用いられた公開鍵に対応する秘密鍵は、不正動作防止制御部0106が保持する。

- [0043] プログラムAのコード0711には、プログラムA0102が行う処理が記述されており、CPU0201によって実行される。

プログラムAのコード0711は、コード暗号鍵0710で暗号化されている。

署名A0115は、プログラムAのコード0711を暗号化したベンダの署名が格納されている。

- [0044] 署名A0115を用いてプログラムAのコード0711の正当性、完全性を検証できる。

機能フラグA0111は、プログラムA0102が、機能0714、0715、0716、0717、0718…を備えているか否か示すフラグである。

本実施形態では、機能フラグは、プログラムがファイル出力、コピー、移動、特殊再生、デジタル出力の各機能を備えているかを示すものとする。

- [0045] 機能フラグは、例えば、5ビットのデータであり、各ビットに、ファイル出力機能、コピー機能、移動機能、特殊再生機能、デジタル出力機能が割り当てられる。即ち、ファイル出力と、移動の機能を備える場合の、機能フラグは、2進数表現で10100となり、デジタル出力機能のみ備える場合には、2進数表現で00001となる。プログラムA0102の機能フラグA0111は、2進数表現で00000であり、すべての機能を備えていないことを示している。
- [0046] ファイルB0213のデータ構造は図5に示し、ファイルC0214、ファイルOS0215のデータ構造は図6に示している。ファイルB0213、ファイルC0214、ファイルOS0215は、ファイルA0212と同様の構成を備えるので、説明は省略する。  
ただし、ファイルC0214の機能フラグC0113は、ファイル出力機能0734を備えることを示し、ファイルOS0215の機能フラグOS0114はファイル出力機能0744、コピー機能0745、移動機能0746を備えることを示している。
- [0047] 不揮発メモリ0221は、例外および割り込みハンドラのアドレスを示すベクターテーブル0219を記憶しているメモリ装置である。  
プログラム保護装置0101において、CPU0201は、割り込みや例外の発生を検知した場合に、ベクターテーブル0219を参照して、次に実行するハンドラの位置を取得する。
- [0048] ベクターテーブル0219に格納されている各種例外および割り込みに対応するハンドラのアドレスは、状態切替回路0208のみが変更可能であり、保護モードにおいて動作するソフトウェアのみが、状態切替回路0208に対しふベクターテーブル0219の設定内容の変更を依頼することができる。  
蓄積メディア0216は、コンテンツや個人情報などの機密情報である保護対象データ0108を、暗号化した状態で記憶する。
- [0049] 保護対象データ0108は、図4に示すように、データ0701、データ暗号鍵0702、セキュリティ要件リスト0109、署名データ0708を含む。  
データ0701は、保護対象となるデータであり、データ暗号鍵0702を用いて暗号化されている。但し、データ0701は必ずしも暗号化されている必要はない。  
データ暗号鍵0702は、公開鍵暗号アルゴリズムで暗号化されており、暗号化する

際に用いられた公開鍵に対応する秘密鍵は、不正動作防止制御部0106が保持しているので、不正動作防止制御部0106のみが復号可能である。

- [0050] セキュリティ要件リスト0109は、セキュリティ要件0703、0704、0705、0706、0707…を含む。

セキュリティ要件リストは、例えば、各ビットがセキュリティ要件を示す5ビットのデータであり、各ビットは、ファイル出力機能、コピー機能、移動機能、特殊再生機能、デジタル出力機能に対応し、ビット値が1の場合にはその機能が可能であることを示し、ビット値が0である場合にはその機能が不可能であることを示す。

- [0051] ファイル出力と、移動の機能が可能な場合のセキュリティ要件リストは2進数表現で10100となり、デジタル出力機能のみ可能な場合は、2進数表現で00001となる。

ここで、データ0701に対するセキュリティ要件0703、0704、0705、0706、0707は、すべて不可能となっている。

署名データ0708は、セキュリティ要件リスト0109に対する署名データであり、当該署名データを用いることにより、セキュリティ要件リスト0109の正当性を検証することができる。

## <2. 2. ソフトウェア構成>

次に、プログラム保護装置0101のソフトウェア構成について、図面を用いて説明する。

- [0052] プログラム保護装置0101のCPU0201上で動作するプログラムは、図7に示すように、OS用割り込み管理部0404を含むオペレーティングシステム(OS)0104、プログラムA用割り込み管理部0402を含むプログラムA0102、プログラムB用割り込み管理部0403を含むプログラムB0103、プログラムC用割り込み管理部0406を含むプログラムC0107、セキュリティカーネル0401、不正動作防止制御部0106、BIOS0405を含んで構成される。

- [0053] BIOS0405は、不揮発メモリ0203に記憶されており、プログラム保護装置0101における電源投入時などに、通常モードでCPU0201により実行される。

BIOS0405は、ハードウェアの基本的な設定を行った後、OS0104をRAM0202にロードする。本実施形態では、BIOS0405は、OS0104のみをロードすることとし

ているが、更にプログラムA0102、B0103、C0107をロードすることとしてもよい。

[0054] OS0104は、一般的なオペレーティングシステムの機能を持つOSであり、起動した後に、プログラムA0102、プログラムB0103、プログラムC0107を順に起動する。

また、OS0104に含まれるOS用割り込み管理部0404は、OS0104が動作している時に発生する割り込みや例外を処理するハンドラを含む。

[0055] プログラムA0102、プログラムB0103、プログラムC0107は、OS0104上で動作する汎用的な処理を行うプログラムであり、保護対象データ0108を取り扱う。

プログラムA0102に含まれる割り込み管理部0402は、プログラムA0102が動作している時に発生する割り込みや例外を処理するハンドラを含む。

[0056] 同様に、プログラムB0103に含まれる割り込み管理部0403、プログラムC0107に含まれる割り込み管理部0403は、プログラムB0103、C0107それぞれが動作している時に発生する割り込みや例外を処理するハンドラを含む。

プログラムA0102、プログラムB0103、プログラムC0107、OS0104は、通常モードで動作するソフトウェアであり、それぞれRAM0202にロードされ、CPU0201により実行される。セキュリティカーネル0401は、保護モードにおけるシステム制御を行うソフトウェアであり、保護メモリ0206にロードされて、CPU0201により実行される。

[0057] セキュリティカーネル0401は、保護モードにおいて発生した割り込み及び例外をハンドリングし、ハンドリングした当該割り込み及び例外に対する処理を実行する。

保護モードにおけるベクタテーブル0219の内容は、通常モードから保護モードへの切替直前に、状態切替部0206によって、割り込み及び例外発生時にCPU0201がセキュリティカーネル0401内のハンドラを実行するよう書き換えられる。

[0058] セキュリティカーネル0401は、不正動作防止制御部0106に制御主体を移す。

不正動作防止制御部0106による不正動作防止制御処理が終了すると、セキュリティカーネル0401に制御主体が戻り、セキュリティカーネル0401は、状態切替回路0208に対し、通常モードへの移行のための状態切替依頼を出力する。

不正動作防止制御部0106は、不正動作防止回路0105を制御してOS0104等を含むプログラムの不正動作を防止する。

[0059] 不正動作防止制御部0106は、保護モードで動作するプログラムであり、保護メモリ

0206にロードされて、CPU0201により実行される。よって、保護メモリ0206にアクセス権限のない、通常モードで動作するプログラムから、セキュリティカーネル0401、および不正動作防止制御部0106へのアクセスはできない。

不正動作防止制御部0106は、前記不正動作防止回路0105を制御するためのデータである管理テーブル0110を管理している。

(管理テーブル)

ここで、管理テーブル0110について、図8、図9を用いて説明する。

[0060] 管理テーブル0110は、プログラムのデータ及びコード領域の保護のための管理データ群であり、図8に示すデータ領域管理情報テーブル群0501、コード領域管理情報テーブル群0502と、図9に示すセキュリティ要件管理情報テーブルT0310、プログラム管理情報テーブルT0410およびカレントプログラム管理テーブル0503を含む。

[0061] データ領域管理情報テーブル群0501、コード領域管理情報テーブル群0502、セキュリティ要件管理情報テーブルT0310、プログラム管理情報テーブルT0410、カレントプログラム管理テーブル0503は、保護メモリ0206に記憶される。

プログラム保護装置0101に電源が投入された時には、各管理テーブル0110の内容は空である。

[0062] 不正動作防止制御部0106は、後述するプログラム登録処理において、プログラムA0102、プログラムB0103、プログラムC0107についてOS0104が行う登録要求に従い、コード領域管理情報テーブル群とプログラム管理情報テーブルの内容を登録又は更新する。

不正動作防止制御部0106は、後述するデータ領域保護設定処理において、他のプログラムから成される保護設定要求に従ってデータ領域管理情報テーブル群の内容を登録又は更新し、後述するデータ領域共有設定において、他のプログラムから成される共有設定要求に従ってセキュリティ要件管理情報テーブルの内容を登録又は更新する。

(プログラム管理情報テーブルT0410)

プログラム管理情報テーブルT0410は、プログラム管理情報T0411、T0412、T0

413、T0414…を含む。

- [0063] 各プログラム管理情報は、プログラム管理情報識別子、コードアドレス、プログラム識別子、共有プログラム識別子、機能フラグを含む。
- プログラム管理情報識別子は、プログラム管理情報を識別するための識別子であり、不正動作防止制御部0106が、当該プログラム管理情報を登録する時に、既に使用されている値と重複しない値を割り当てる。
- [0064] コードアドレスは、各プログラム管理情報が管理対象とするアドレス領域である。
- プログラム識別子は、前記アドレス領域にロードされるコードを含むプログラムの識別子であり、予め、各プログラムに対し割り振られている。
- 共有プログラム識別子は、前記アドレス領域のコードを共有するプログラムの識別子である。
- [0065] 機能フラグは、前記アドレス領域のコードに対し、ファイル出力、コピー、移動、特殊再生、デジタル出力の各機能が許可されているか否かを示すフラグである。
- 機能フラグは、例えば、5ビットのデータであり、各ビットに、ファイル出力機能、コピー機能、移動機能、特殊再生機能、デジタル出力機能が割り当てられる。
- 即ち、ファイル出力と、移動とが許可されている場合の、機能フラグは、2進数表現で10100となり、デジタル出力機能のみが許可されている場合には、2進数表現で00001となる。
- (コード領域管理情報テーブル群)
- コード領域管理情報テーブル群0502は、プログラム用コード領域管理情報テーブルT0210、T0220、T0230…を含み、プログラム用コード領域管理情報テーブルは、プログラム毎に生成されたものである。
- [0066] プログラム識別子がP1であるプログラムについて生成されるプログラムP1用コード領域管理情報テーブルT0210は、コード領域管理情報T0211、T0212、T0213…を含み、データ領域管理情報は、コード領域識別子、コードアドレス、コード暗号鍵を含む。
- コード領域識別子は、コード領域管理情報を識別するための識別子であり、不正動作防止制御部0106が、当該コード領域管理情報を生成する時に、既に使用されて

いる値と重複しない値を割り当てる。

- [0067] コードアドレスは、コード領域管理情報が管理対象とするアドレス領域である。  
コード暗号鍵は、前記アドレス領域で示されるメモリ領域に保持されたコードを暗号化、復号するための鍵であり、コードアクセスの際に用いられる。  
(データ領域管理情報テーブル群)  
データ領域管理情報テーブル群0501は、データ領域管理情報テーブルT0110、T0120、T0130…を含む。
- [0068] データ領域管理情報テーブルは、プログラム毎に生成されたものであり、データ領域識別子、データアドレス、データ暗号鍵を含む。  
データ領域識別子は、各データ領域管理情報を識別するための識別子である。  
データアドレスは、各データ領域管理情報が管理対象とするアドレス領域である。  
データ暗号鍵は、前記アドレス領域で示されるメモリ領域に保持されたデータを暗号化、復号するための鍵であり、データアクセスの際に用いられる。  
(セキュリティ要件管理情報テーブル)  
セキュリティ要件管理情報テーブルT0310は、データ領域管理情報テーブル群0501に含まれる各データ領域管理情報に対するセキュリティ要件を管理するためのテーブルであり、複数のセキュリティ要件管理情報T0311、T0312、T0313、T0314…を含む。
- [0069] セキュリティ要件管理情報は、セキュリティ要件管理情報識別子、データアドレス、生成プログラム識別子、共有プログラム識別子、セキュリティ要件を含む。  
セキュリティ要件管理情報識別子は、セキュリティ要件管理情報を識別するための識別子である。  
データアドレスは、セキュリティ領域管理情報が管理対象とするアドレス領域である。  
。
- [0070] 生成プログラム識別子は、物理メモリ上の前記アドレス領域について、最初にデータ設定を行ったプログラムの識別子である。  
共有プログラム識別子は、物理メモリ上の前記アドレス領域について、当該メモリ領域を共有するプログラムを識別するための識別子である。

セキュリティ要件は、前記データアドレスにより示される、物理メモリ上の前記アドレス領域に保持されるデータの保護方法を定める。

- [0071] 前記セキュリティ要件は、本実施形態では、機能フラグと同じ構造を持つものとし、例えば、5ビットのデータであり、各ビットに、ファイル出力機能、コピー機能、移動機能、特殊再生機能、デジタル出力機能の実行可否が割り当てられる。

即ち、ファイル出力と、移動とが実行許可されている場合の、機能フラグは、2進数表現で10100となり、デジタル出力のみ実行許可されている場合には、2進数表現で00001となる。

(カレントプログラム管理テーブル0503)

カレントプログラム管理テーブル0503には、現在動作中のプログラムの識別子が記憶される。

### <3. ソフトウェア動作>

次に、プログラム保護装置0101上で動作するソフトウェアによる処理の流れについて説明する。

- [0072] まず、ソフトウェア全体の処理フローについて、図21を用いて説明する。

プログラム保護装置0101に対し電源が投入されると、BIOS0405が起動する(ステップS2011)。

BIOS0405は、プログラム保護装置0101のハードウェアについての基本的な設定を行った後、OS0104をRAM0202にロードする(ステップS2012)。

- [0073] OS0104は、不正動作防止制御部0106に対し、自プログラムであるOS0104についての後述する登録処理を行い(ステップS2020)、プログラムA0102についての後述する登録処理を行い(ステップS2021)、プログラムB0103についての登録処理を行い(ステップS2022)、プログラムC0107についての登録処理を行う(ステップS2023)。

- [0074] 登録処理が成されると、不正動作防止制御部0106は、OS0104、プログラムA0102、プログラムB0103、プログラムC0107からのメモリ保護などの各要求について、処理することが可能となる。

次に、OS0104は、登録処理が成功したプログラムA0102、B0103、C0107を順

に起動する(ステップS2031)。

- [0075] ここで、プログラムA0102、プログラムB0103、プログラムC0107が、OS0104上で動作を開始する。

次に、OS0104は、不正動作防止制御部0106に対し、自プログラム内で使用するデータ領域の後述する保護設定を行う(ステップS2040)。

同様に、プログラムA0102は、不正動作防止制御部0106に対し、自プログラム内で使用するデータ領域の後述する保護設定を行い(ステップS2041)、プログラムB0103は、不正動作防止制御部0106に対し、自プログラムが使用するデータ領域の保護設定を行い(ステップS2042)、プログラムC0107は、不正動作防止制御部0106に対し、自プログラムが使用するデータ領域の保護設定を行う(ステップS2043)。

次に、プログラムA0102は、必要ある場合に、不正動作防止制御部0106に対し、他プログラムと使用するデータ領域を共有するための後述するデータ領域共有設定を行う(ステップS2051)。

- [0076] 同様に、プログラムB0103は、必要ある場合に、不正動作防止制御部0106に対し、他プログラムと使用するデータ領域を共有するためのデータ領域共有設定を行い(ステップS2052)、プログラムC0107は、必要ある場合に、不正動作防止制御部0106に対し、他プログラムと使用するデータ領域を共有するためのデータ領域共有設定を行う(ステップS2053)。

- [0077] これにより、複数のプログラムが、保護されているメモリ領域を共有できるようになる。以後、OS0104は、必要に応じ、動作させるカレントのプログラムを切り替え(ステップS2061)、カレントのプログラムは、自プログラムが行うべき処理を実行する(ステップS2062)。

- [0078] 以下、ステップS2021におけるプログラム登録処理、ステップS2041における保護設定処理、ステップS2051におけるデータ領域の共有設定処理、ステップS2061におけるプログラム切替処理について、説明する。

上述のステップS2020、ステップS2021、ステップS2022、ステップS2023、ステップS2040、ステップS2041、ステップS2042、ステップS2043、ステップS2051

、ステップS2052、ステップS2053は、全て、図10～12で示す基本の処理フローに従い実行される。

- [0079] 以下、ステップS2020～S2023については、ステップS2021を例として説明し、ステップS2040～S2043については、ステップS2041を例として説明し、ステップS2051～S2053については、ステップS2051を例として説明する。

また、ステップS2021～S2053の各処理の実行は、一度に限らず、必要に応じて隨時実行するものとする。

### <3. 1. プログラム登録処理>

図21におけるステップS2021は、OS0104が、プログラムAについての情報を、不正動作防止制御部0106に登録する処理である。

- [0080] 図11、図12に示したプログラムXは、当該フローチャートに従い動作するプログラムを示しており、本実施形態では、プログラムA0102、プログラムB0103、プログラムC0107、OS0104のいずれかである。ここでは、OS0104が、プログラムXに該当し、OS用割込み管理部0404が、プログラムX用割込み管理部に該当し、OS0104が、プログラムAについての登録を要求するものとする。

- [0081] プログラムXは、まず、プログラムXについて予め指定されている、RAM0202上のデータ領域に、プログラムAを登録するための登録要求を書き込む。

前記登録要求には、図5に示した、登録されるプログラムであるプログラムAのコードを暗号化する際に用いられた鍵(コード暗号化)、プログラムの署名データ、機能フラグが含まれる。さらに、前記登録要求には、プログラムのロードアドレス情報が含まれる。

- [0082] 鍵は公開鍵暗号アルゴリズムによって暗号化されており、鍵の暗号化に用いる公開鍵に対応する秘密鍵は不正動作防止制御部0106に格納されている。

秘密鍵は不正動作防止制御部0106の外部に漏洩しないよう対策が施される。

プログラムの署名データは、プログラムの正当性、完全性を検証するために用いられる。

- [0083] プログラムのロードアドレス情報は、登録されるプログラムがロードされているアドレス領域である。

プログラムXは、プログラムAの登録要求を要因とするソフトウェア割り込みを発生させ(ステップS0801)、プログラムX用割り込み管理部に制御を移す。

次に、プログラムX用割り込み管理部は、プログラムXが発生させたソフトウェア割り込みの要因を調査し、前記登録要求を所定の前記データ領域から読み出し、割り込みの種別を確認する(ステップS0802)。ここで、プログラムX用割り込み管理部は、前記割り込みの種別が、プログラムAについての登録要求を要因とするソフトウェア割り込みであったことを確認する。

- [0084] 次に、プログラムX用割り込み管理部は、前記登録要求を共有メモリに格納する(ステップS0803)。

ここで、前記共有メモリは、通常モードと保護モードとの通信に用いる、RAM0202内の所定のメモリ領域である。

ここで、プログラム保護装置0101の動作状態を、通常モードから保護モードへ切り替えるための状態切替動作Aを実行する。

- [0085] 状態切替動作Aについては、図11(a)を用いて説明する。

プログラムXは、ここでは、OS0104である。

プログラムX用割り込み管理部は、状態切替回路0208に対し、保護モードへの状態切替依頼を行う(ステップS1700)。

状態切替回路0208は、CPU内の状態を予め定められているRAM0202内のプログラムXが管理するデータ領域に格納する(ステップS1701)。

- [0086] 状態切替回路0208は、状態切替依頼元であるプログラムXのコンテキストを、RAM0202においてプログラムXが使用するよう予め定められている領域に退避する。

状態切替回路0208は、保護モードを示す状態信号A0211を出力し、デバッガI/F0209を無効化する(ステップS1702)。

次に、状態切替回路0208は、CPU内部状態のクリアを行う(ステップS1703)。

- [0087] 次に、状態切替回路0208は、保護モードを示す状態信号B0217を出力し、鍵レジスタ0205の設定を変更する(ステップS1704)。

ここで、鍵レジスタ0205は、バス0210を介して通知される設定信号0304を用いて命令用鍵情報テーブル0305とデータ用鍵情報テーブル0306を変更できるようにす

る。

[0088] 次に、状態切替回路0208は、保護モードを示す状態信号C0218を出力し、アクセス制限回路0207の設定を変更し(ステップS1705)、アクセス制限回路0207は、バス0210から保護メモリ0206へのアクセスを開放状態にする。

開放状態とは、バス0210から保護メモリ0206へのアクセスが許可された状態を示す。

[0089] 次に、状態切替回路0208は、割り込みおよび例外発生時にCPU0201がセキュリティカーネル0401内のハンドラを実行するようベクタテーブル0219の設定を変更する(ステップS1706)。

状態切替回路0208は、前回保護モードから通常モードに切り替える直前に保護メモリ0206に格納していたコンテキストをCPUに復帰させる(ステップS1707)。

[0090] 次に、状態切替回路0208は、セキュリティカーネル0401に制御を移す(ステップS1708)。プログラム保護装置0101は保護モードとなり、状態切替動作Aは終了する。

次に、セキュリティカーネル0401は、不正動作防止制御部0106に制御を移す(ステップS0815)。

[0091] 次に、不正動作防止制御部0106は、共有メモリから前記要求を取得する(ステップS0806)。ここでは、前記要求は、前記登録要求である。

次に、不正動作防止制御部0106は、不正動作防止制御処理(ステップS0807)を実行する。

ここで、前記要求が前記登録要求である場合の不正動作防止制御処理(ステップS0807)の詳細について、図10を用いて説明する。

[0092] 不正動作防止制御部0106は、前記要求がいずれの要求であるかを判定する(ステップS600)。

前記要求が登録要求であるので(ステップS600:登録)、ステップS0612へと分岐する。

次に、不正動作防止制御部0106は、セキュリティ要件管理情報テーブルT0310とプログラム管理情報テーブルT0410を用い、プログラムのロードアドレス情報によつ

て示されているコードアドレス領域が、未使用領域であるかどうかを判定する(ステップS0612)。

[0093] 未使用領域である場合(ステップS0612のYES)、不正動作防止制御部0106は、プログラムの署名と機能フラグの署名の検証を行う(ステップS0613)。

署名検証結果がOKであった場合(ステップS0613のYES)、不正動作防止制御部0106は、新規のコード領域管理情報テーブルとデータ領域管理情報テーブルを生成する(ステップS0614)。

[0094] 次に、管理テーブルの更新として、プログラム管理情報テーブルT0410の更新とコード領域管理情報テーブルの更新を行う(ステップS0615)。

プログラム管理情報テーブルT0410の更新において、不正動作防止制御部0106は、固有のプログラム識別子を生成した後、プログラム管理情報の追加を行う。

コード領域管理情報テーブルの更新において、不正動作防止制御部0106は、コード暗号鍵の復号化とコード領域管理情報の追加を行う。

[0095] 次に、不正動作防止制御部0106は、処理結果を生成する。

処理結果は、管理テーブルの更新(ステップS0615)時に生成したプログラム識別子を含む。コードアドレス領域が未使用領域でなかった場合(ステップS0612のNO)と署名検証に失敗した場合(ステップS0613のNO)には、処理に失敗した原因を処理結果に含める。ここで生成した処理結果を、共有メモリに格納する(ステップS0808)。

[0096] 次に、不正動作防止制御部0106は、セキュリティカーネル0401に制御を移す(ステップS0816)。

ここで、セキュリティカーネル0401、状態切替部0208、プログラムX用割り込み管理部が、状態切替動作Bを実行することにより、保護モードから通常モードへ切り替える(ステップS0809)。

[0097] ここで、状態切替動作Bについて、図11(b)を用いて説明する。

ここで、プログラムXは、前述のように、OS0104である。

セキュリティカーネル0401は、状態切替回路0208に対し、通常モードを示す状態信号C0218を出力することにより、状態切替を依頼する(ステップS1710)。

状態切替回路0208は、CPUのコンテキストを保護メモリ0206に格納する(ステップS0817)。

[0098] アクセス制限回路0207は、状態信号C0218を受け付けて、バス0210から保護メモリ0206へのアクセスを遮断状態にする。

遮断状態とは、バス0210から保護メモリ0206へアクセスできない状態を示す。

状態切替回路0208は、状態信号B0217を制御し、鍵レジスタ0205の設定を変更する(ステップS1713)。

[0099] ここで、鍵レジスタ0205は、バス0210を介して通知される設定信号0304を用いて命令用鍵情報テーブル0305とデータ用鍵情報テーブル0306を変更できないようにする。

状態切替回路0208は、CPU内部状態のクリアを行う(ステップS1714)。

状態切替回路0208は、ベクタテーブル0219の設定変更を行う(ステップS1715)

。ここで、状態切替回路0208は、割り込みおよび例外発生時にCPU0201がプログラムX用割り込み管理部に含まれるハンドラを実行するよう設定する。

[0100] ベクタテーブル0219は各々の割り込み管理部に含まれるハンドラを実行するよう設定される。どの割り込み管理部に含まれるハンドラを実行するよう設定するかは、不正動作防止制御部0106が状態切替回路0208に指示することができる。

次に状態切替回路0208は、状態信号A0211を制御してデバッガI／F0209を有効にする(ステップS1716)。

[0101] なお、不正動作防止制御部0106が前もって状態切替回路0208にデバッガI／F0209を有効にしないよう指示している場合、状態切替回路0208は、ステップS1716をスキップし、デバッガI／F0209を有効にしない。

ここで、状態切替回路0208は、プログラムXのコンテキストを復帰させ(ステップS1717)、次に状態切替回路0208は、プログラムX用割り込み管理部に制御を移し(ステップS1718)、プログラム保護装置0101は通常モードとなり、状態切替動作Bは終了する。

[0102] 次に、プログラムX用割り込み管理部は、共有メモリから前記処理結果を取得する(ステップS0811)。

次に、プログラムX用割り込み管理部は、処理結果をプログラムXが管理するデータ領域に格納(ステップS0812)した後、ソフトウェア割り込みからリターンする(ステップS0813)。

### <3. 2. データ領域の保護設定処理>

図21におけるステップS2041は、プログラムAが不正動作防止制御部0106に対し、使用するメモリ領域の保護設定を要求する処理である。

- [0103] 以下、保護設定の処理について、前述のプログラム登録処理と異なる部分を中心に、説明する。

ここでは、プログラムXは、プログラムA0102であるものとする。

まず、プログラムXは、自プログラムについて予め指定されているRAM0202上のデータ領域である共有メモリに、データアドレスとセキュリティ要件とを含むデータ領域保護設定要求を書き込む。

- [0104] 前記データアドレスは、プログラムXがデータ領域として使用を要望するメモリ領域の先頭アドレスと末尾アドレスとを含む。

前記セキュリティ要件は、プログラムXが前記データアドレスに格納するデータに対し設定を要望する保護属性であり、セキュリティ要件リスト0109と同様のデータ構造を持つ。例えば、前記セキュリティ要件は、5ビットのデータであり、各ビットに、ファイル出力機能、コピー機能、移動機能、特殊再生機能、デジタル出力機能の実行可否が割り当てられる。なお、前記セキュリティ要件は、セキュリティ要件リスト0109である場合もある。

- [0105] 不正動作防止制御部0106は、ステップS0802において、前記データ領域保護設定要求を取得する。

ステップS0803～S0806までは、プログラム登録処理と同様である。

ステップS0807の詳細である図10のステップS0600における判定で、不正動作防止制御部0106は、前記処理要求が、データ領域の保護設定要求であると判定し(ステップS0600の保護)、ステップS0602に移行する。

- [0106] 不正動作防止制御部0106は、前記データ領域保護設定要求に含まれるデータアドレスが、セキュリティ要件管理情報テーブルT0310中のセキュリティ要件管理情報

として登録されているか否かを判定し(ステップS0602)、登録されていなければ、未使用領域であると決定し、登録されていれば、未使用領域でないと決定する。

未使用領域であった場合(ステップS0602のYES)、セキュリティ要件管理情報テーブルT0310およびデータ領域管理情報テーブル群0501を更新する(ステップS0603)。

- [0107] セキュリティ要件管理情報テーブルT0310の更新において、不正動作防止制御部0106は、要求元のプログラムに対応するデータ領域管理情報テーブルに、前記先頭アドレス及び前記末尾アドレスをデータアドレスとした新規セキュリティ要件管理情報を追加する。

また、不正動作防止制御部0106は、前記新規セキュリティ要件管理情報におけるデータ暗号鍵には、乱数値を生成して登録する。

- [0108] 次に、不正動作防止制御部0106は、データ領域管理情報テーブルの更新された情報を不正動作防止回路0105に設定する(ステップS0604)。

具体的には、不正動作防止制御部0106は、更新された情報の不正動作防止回路0105への設定として、前記新規セキュリティ要件管理情報のデータアドレスと、データ暗号鍵との組を、不正動作防止回路0105のデータ用鍵情報テーブル0306に追加する。

- [0109] また、ステップS0602において、受け取ったデータアドレス領域が既に他のプログラムによって確保されている場合には(ステップS0602のNO)、不正動作防止制御部0106は、管理テーブルの更新(ステップS0603)、およびデータ領域設定の変更(ステップS0604)の処理を行わず、ステップS0808に移行する。

不正動作防止制御部0106は、処理結果を共有メモリに格納する(ステップS0808)。

- [0110] 処理結果には、正常終了、データアドレス領域が他のプログラムにより確保されている等のエラー要因などを含める。
- 以降の処理は、前述のプログラム登録処理と同様である。

### <3. 3. データ領域共有設定処理>

図21におけるステップS2051は、プログラムAが不正動作防止制御部0106に対

し、使用するメモリ領域の共有設定を要求する処理である。

- [0111] 以下、データ領域共有設定処理について、前述のプログラム登録処理と異なる部分を中心に説明する。なお、プログラムXは、プログラムA0102である。

まず、プログラムXは、自プログラムについて予め指定されているRAM0202上のデータ領域である共有メモリに、データアドレスとセキュリティ要件とを含むデータ領域共有設定要求及び署名A0115を書き込む。

- [0112] 前記データアドレスは、プログラムXがデータ領域として共有を要望するメモリ領域の先頭アドレスと末尾アドレスとを含み、前記セキュリティ要件は、ファイルA0212の機能フラグA0111の情報を含む。

署名A0115は、不正動作防止制御部0106により、機能フラグA0111の正当性の確認に用いられる。不正動作防止制御部0106は、ステップS0802において、前記データ領域共有設定要求を取得する。

- [0113] ステップS0803～S0806までは、プログラム登録処理と同様である。

ステップS0807の詳細である図10のステップS0600における判定で、処理要求が、データ領域の共有設定要求であると判定する(ステップS0600の共有)。

不正動作防止制御部0106は、ステップS0802において、RAM0202上の共有メモリから前記データ領域共有設定要求を取得し、ステップS0632において、前記データ領域共有設定要求に含まれるデータアドレスが、セキュリティ要件管理情報テーブルT0310中のセキュリティ要件管理情報として登録されているか否かを判定し、登録されている場合(ステップS0632のYES)、不正動作防止制御部0106は前記データ領域共有設定要求の妥当性判断を行う(ステップS0633)。

- [0114] 妥当性判断は、具体的には、共有を要求しているプログラムに対応するプログラム管理情報に含まれる機能フラグが、妥当性判断の対象となっているセキュリティ要件管理情報のセキュリティ要件を満たすかどうかによって判断される。

また、前記セキュリティ要件の正当性についても、前記共有メモリに書き込まれた署名を用いて確認する。

- [0115] 妥当であると判断した場合(ステップS0633のYES)、不正動作防止制御部0106は、セキュリティ要件管理情報テーブルT0310と要求元のプログラム用のデータ領

域管理情報テーブルの更新を行う(ステップS0634)。

不正動作防止制御部0106は、セキュリティ要件管理情報テーブルT0310の更新において、具体的には、対象となるデータ領域に対応するセキュリティ要件管理情報の共有プログラム識別子に共有を要求しているプログラムの識別子を書き込む。

- [0116] 要求しているプログラムの識別子は、カレントプログラム管理テーブル0503に格納されている識別子を用いる。

また、要求しているプログラムが指定しているセキュリティ要件が、既存のセキュリティ要件より厳しい場合、要求しているプログラムが指定しているセキュリティ要件を、対象となるデータ領域に対応するセキュリティ要件管理情報のセキュリティ要件として追加する。

- [0117] ここで、要求しているプログラムが指定しているセキュリティ要件が既存のセキュリティ要件より厳しい場合は、セキュリティ要件はセキュリティ要件リスト0109と同様のデータ構造をしていることから、セキュリティ要件が既存のものより多い場合を指す。

さらに、データ領域管理情報テーブルの更新において、不正動作防止制御部0106は、要求元のプログラム用のデータ領域管理情報テーブルにデータ領域管理情報を追加する。

- [0118] ここで、追加するデータ領域管理情報のデータアドレスには、要求されたアドレス領域を設定し、データ暗号鍵には、共有対象となるデータ領域の暗／復号に用いている暗号鍵を設定する。

次に、不正動作防止制御部0106は、データ保護設定の変更を行う(ステップS0635)。

- [0119] 具体的には、不正動作防止制御部0106が、ステップS0634で更新したデータ領域管理情報テーブルの更新内容を不正動作防止回路0105に反映し、正常終了を示す処理結果を生成する。

また、ステップS0632において、登録されていないと判断した場合(ステップS0632のNO)、および設定が妥当でないと判断した場合(ステップS0633のNO)、不正動作防止制御部0106は、エラーを示す処理結果を生成する。

- [0120] 次に、不正動作防止制御部0106は、生成した処理結果を共有メモリに格納する(

ステップS0808)。

処理結果には、正常終了、データアドレス領域が他のプログラムにより確保されている等のエラー要因などを含める。

以降の処理は、前述のプログラム登録処理と同様である。

#### <3. 4. プログラム切替処理>

図21におけるステップS2061は、プログラムA0102が、不正動作防止制御部0106に対し、カレントのプログラムを切り替えるよう要求し、その要求に対する処理である。

- [0121] 以下、プログラム切替処理について、前述のプログラム登録処理と異なる部分を中心説明する。

なお、プログラムXは、プログラムA0102であり、プログラムB0103への切替を要求するものとする。

まず、プログラムXは、自プログラムについて予め指定されているRAM0202上のデータ領域である共有メモリに、切替を希望するプログラムの識別子を含む切替要求と、切替を希望するプログラムに対して伝達を希望する引数データとを書き込む。

- [0122] プログラムX用割り込み管理部は、ステップS0802において、前記プログラム切替要求を取得する。

ステップS0803～S0806までは、プログラム登録処理と同様である。

ステップS0807の詳細である図10のステップS0600における判定で、処理要求が、プログラム切替要求であると判定する(ステップS0600の切替)。

- [0123] 不正動作防止制御部0106は、ステップS0802において、RAM0202から前記切替要求を取得し、更に、引数データの取得を行う(ステップS0621)。引数データは、切替元のプログラムから切替先のプログラムへ伝達される情報であり、コマンドなどが含まれる。

不正動作防止制御部0106は、取得した引数データを保護メモリ0206に格納する。

- [0124] RAM0202における引数データの格納位置は予め決められており、不正動作防止制御部0106は予め知っている。

なお、引数データの位置は固定である必要はなく、切替要求に含むこととしてもよい。

次に、不正動作防止制御部0106は、カレントプログラム管理テーブルの更新を行う(ステップS0622)。

- [0125] ここで、カレントプログラム管理テーブルの内容を切替先のプログラムの識別子に変更する。

次に、不正動作防止制御部0106は、不正動作防止回路0105の設定を変更する(ステップS0623)。

不正動作防止制御部0106は、鍵レジスタ0205に記憶されている命令用鍵情報テーブルの内容と、データ用鍵情報テーブルの内容を消去し、データ領域管理情報テーブル群0501に含まれる切替先のプログラムに対応するデータ領域管理情報テーブル中の各データ領域管理情報に記憶されているデータアドレスと、データ暗号鍵との組を、不正動作防止回路0105のデータ用鍵テーブルに書き込む。

- [0126] また、コード領域管理情報テーブル群0502に含まれる切替先のプログラムに対応するコード領域管理情報テーブル中の各コード領域管理情報に記憶されているコードアドレスと、コード暗号鍵との組を、不正動作防止回路0105の命令用鍵情報テーブル0305に書き込む。

次に、不正動作防止制御部0106は、予め保護メモリ0206に格納しておいた引数データを切替先のプログラムが管理するRAM0202に格納する(ステップS0624)。

- [0127] 次に、不正動作防止制御部0106は、切替先のプログラムへの分岐指示を含む処理結果を生成し、当該処理結果を共有メモリに格納する(ステップS0808)。

このように、不正動作防止制御部0106は、引数データを保護メモリを介して他のプログラムに受け渡すことができる。

そのため、不正動作防止制御部0106は、OS0104を含むプログラムから他のプログラムへのデータの受け渡しを依頼された場合、依頼元のプログラムと依頼先のプログラム以外のプログラムへ、そのデータが漏洩しないように受け渡しを行うことが可能となる。

- [0128] 例えば、プログラムA0102がプログラムB0103を関数として呼び出す場合で、プロ

グラムB0103がプログラムA0102のデータ領域を共有していない場合において、引数データの受け渡しを安全に行うことができる。

また、プログラムA0102がOS0104のシステムコールを呼び出す場合も同様に引数データの受け渡しを安全に行うことができる。

#### <4. 全体動作>

プログラム保護装置0101によるプログラムの切替処理(プログラムA0102からプログラムB0103への切替処理)を例として、全体動作について、図13、図14に示すフローチャートを用いて説明する。

- [0129] プログラムA0102は、保護対象データ0108であるコンテンツの復号を行った後、復号されたコンテンツの再生を依頼するために、プログラムA0102に対し予め決められたデータ領域に、プログラムBへの引数データを含む処理要求を書き込んで、プログラムB0103に切り替えるためにソフトウェア割り込みを発生させ、プログラムA用割り込み管理部0402に制御を移す(ステップS0901)。
- [0130] プログラムA用割り込み管理部0402は、前記データ領域から前記引数データを取得し、また、割り込みの種別がプログラムB0103へ切り替えるためのソフトウェア割り込みであったことを確認する(ステップS0902)。  
次に、プログラムA用割り込み管理部0402は、プログラムB0103へ切り替える旨の要求と引数データを共有メモリに格納する(ステップS0903)。
- [0131] 次に、プログラムA用割り込み管理部0402、状態切替回路0208、セキュリティカーネル0401は、前述の状態切替動作Aを実行し、通常モードから保護モードへ切り替える(ステップS0905)。  
次に、ステップS0905において、制御主体となったセキュリティカーネル0401は、不正動作防止制御部0106に制御を移す(ステップS0907)。
- [0132] 次に、不正動作防止制御部0106は、共有メモリから、ステップS0903で格納された前記要求と前記引数データを取得する(ステップS0908)。  
次に、不正動作防止制御部0106は、前記要求がプログラムB0103への切り替え要求であることから、プログラムの切替処理が必要であることを判断し、前述したプログラムの切替処理0602の処理を行う(S0909)。

[0133] 不正動作防止制御部0106は、切替処理の結果を共有メモリに格納する(ステップS0910)。

次に、不正動作防止制御部0106は、セキュリティカーネルに制御を移す(ステップS0911)。

ここで、セキュリティカーネル0401、状態切替回路0208及びOS用割り込み管理部0404が前述の状態切替動作Bを実行し、保護モードから通常モードへ切り替える(ステップS0913)。また、プログラムの切替にはオペレーティングシステムの処理が必要なので、通常モードに復帰後、OS用割り込み管理部0404に制御を移す。

[0134] 次に、OS用割り込み管理部0404は、共有メモリから処理結果を取得し(ステップS0915)、OS0104に制御を移す(ステップS0916)。

次にOS0104は、プログラムA0102からプログラムB0103への切替処理を行う(ステップS0917)。ここで、OS0104は、プログラムコンテキストの切替などの処理を行う。

[0135] 次に、OS0104は、プログラムB0103への切替を不正動作防止制御部0106に依頼するために、OS用割り込み管理部0404に制御を移す(ステップS0918)。

次に、OS用割り込み管理部0404は、プログラムB0103への切替要求を共有メモリに格納する(ステップS0919)。

[0136] ここで、ステップS0921～ステップS0929は、ステップS0905～ステップS0913までと同様の処理であるので、説明を省略する。

ただし、切替先のプログラムはOS0104ではなく、プログラムB0103であるので、プログラムB用割り込み管理部0403に制御が移る。

次に、プログラムB用割り込み管理部0403は、共有メモリから処理結果を取得する(ステップS0931)。

[0137] 次にプログラムB用割り込み管理部0403は、処理結果をプログラムB0103が管理するデータ領域に格納(ステップS0932)した後、ソフトウェア割り込みからリターンする(ステップS0933)。

その後、プログラムB0103は、データ処理を行う(ステップS0934)。

<5. コンテンツ復号処理を例とした補足説明>

プログラム保護装置0101において、暗号化コンテンツである保護対象データ0108の復号処理を行うプログラムA0102と、復号されたコンテンツを再生するプレーヤーであるプログラムBとが、連係して動作する場合について、データの変化を中心に、図15～図20に示す図を用いて補足説明する。

- [0138] また、保護対象データへのアクセス権を保持していないプログラムC0107が、保護対象データへアクセスした場合の動作についても説明する。

図16は、プログラム保護装置0101動作中のRAM0202の状態を示す。

プログラムA0102、プログラムB0103、プログラムC0107、OS0104のコードは、それぞれコード暗号鍵KC\_A、KC\_B、KC\_C、KC\_OSによって暗号化されて不揮発メモリ0203に格納されている。

- [0139] 不揮発メモリ0203に格納されているBIOS0405は、ファイルA0212、ファイルB0213、ファイルC0214、ファイルOS0215をRAM0202にロードする。

その結果、プログラムA0102のコード領域(定数も含まれる)1201は、1000番地から1100番地にロードされる。

- [0140] プログラムB0103、プログラムC0107、OS0104も同様に、それぞれ2000～2100、3000～3100、4000～4100番地にロードされる。

また、蓄積メディア0216に格納されている保護対象データ0108は、8000～9000番地の保護対象データ領域1210にロードされる。

なお、保護対象データ0108は、必ずしもBIOS0405がロードする必要はなく、その他のプログラムがロードしてもよい。

- [0141] その後、BIOS0405は、不正動作防止制御部0106にプログラム登録依頼をする。不正動作防止制御部0106は、プログラムの登録処理0601に従って、各プログラムを登録する。

その結果、図17～図19に示すように、管理テーブル0110内に、データ領域管理情報テーブルT0500、T0600、T0700、T0800、コード領域管理情報テーブルT0900、T1000、T1100、T1200、およびプログラム管理情報テーブルT1300、セキュリティ要件管理情報テーブルT1400が生成される。

- [0142] なお、ここではBIOS0405がプログラムA0102、プログラムB0103、プログラムC0

107をロード／登録しているが、BIOS0405がOS0104のみをロード／登録した後、OS0104がプログラムA0102、プログラムB0103、プログラムC0107をロード／登録してもよい。

プログラム登録処理0601の管理テーブルの更新(ステップS0615)で、プログラム管理情報T1301～T1304がプログラム管理情報テーブルT1300に追加される。

- [0143] プログラムA0102およびプログラムB0103の機能フラグ0111および0112において、ファイル出力機能は無しであるので、プログラム管理情報T1301およびT1302の機能フラグはファイル出力機能無しとなる。

また、プログラムC0107およびOS0104の機能フラグ0113および0114は、ファイル出力機能は有りであるので、プログラム管理情報T1303およびT1304の機能フラグはファイル出力機能有りとなる。

- [0144] なお、ここではファイル出力機能のみに着目しているが、その他の機能についても同様に扱われる。

プログラム登録処理0601の管理テーブルの更新(ステップS0615)で、プログラムA用コード領域管理情報テーブルT0900には、コード領域管理情報T0901とT0902が追加される。

- [0145] コード領域管理情報T0901において、コード領域識別子として“A\_C0”、コードアドレスとして“1000～1099”、コード暗号鍵として“KC\_A”が設定される。

ここで、不正動作防止制御部0106は、ファイルA0212に格納されているコード暗号鍵0710を秘密鍵で復号化する。コード領域管理情報T0902において、コード領域識別子として“未定義領域”、コードアドレスとして“定義領域以外”、コード暗号鍵として“KC\_RA”が設定される。

- [0146] ここで、“定義領域以外”とは、プログラムA用コード領域管理情報テーブルT0900に登録されているコード領域管理情報T0902以外のコード領域管理情報で定義されているコードアドレス領域以外の領域を意味し、この領域には、コード暗号鍵としてKC\_RAが用いられる。

KC\_RAは、不正動作防止制御部0106が生成した乱数値である。なお、他のコード領域管理情報テーブルT1000、T1100、T1200も図16に示すように、同様に

設定される。

[0147] 図15は、プログラム保護装置0101の動作を示すフローチャートである。

本フローチャートは、プログラムA～Cが連携動作しようとし、プログラムCがセキュリティ要件違反により停止する場合を示している。

なお、図15では、各割り込み管理部0402、0403、0404、0406の動作は省略している。以下、図15にしたがってプログラム保護装置0101の動作を説明する。

[0148] プログラムA0102は、プログラムAのデータ領域1202を使用可能にするために不正動作防止制御部0106に対しデータ保護設定を依頼する(ステップS1101)。

ここで、プログラムA0102は、1500～1599番地までのデータ領域をプログラムA0102のみアクセス可能な状態で確保するよう不正動作防止制御部0106に依頼をする。

[0149] プログラムA0102は、ステップS0801～ステップS0813と同様の動作を行い、データ保護設定を行う。

以下、データ保護設定の依頼は同様の動作で行われるものとする。

その結果、プログラムA用データ領域管理情報テーブルT0500にデータ領域管理情報T0501が追加されると共に、セキュリティ要件管理情報テーブルT1400にセキュリティ要件管理情報T1401が追加される。

[0150] このとき、不正動作防止制御処理(ステップS0807)において、不正動作防止制御部0106は、データ領域の保護設定処理0603を行う。

データ領域管理情報T0501のデータ暗号鍵KD\_A1は、不正動作防止制御部が生成した乱数値である。

次にプログラムA0102は、保護対象データ領域1210のデータを取り扱えるように設定を行う(ステップS1102)。

[0151] 保護対象データ領域1210に格納されている保護対象データ0108内のデータ0701はデータ暗号鍵0702で暗号化されているので、データ0701をデータ暗号鍵0702で復号化しなければプログラムA0102はデータ0701を使用できない。

ここでは、バス暗号回路0204で復号化するものとする。

そこで、プログラムA0102は、不正動作防止制御部0106に対し、データ領域設定

要求を行う。

- [0152] データ領域設定要求には、保護対象データ領域1210のアドレスとセキュリティ要件が含まれる。

ここで、プログラムA0102は、セキュリティ要件として、保護対象データ0108に含まれるセキュリティ要件リスト0109を用いるように不正動作防止制御部0106に指示する。

- [0153] 不正動作防止制御部0106は、図12に示す(ステップS0801)から(ステップS081 3)までの処理を行う。

不正動作防止制御処理(ステップS0807)において、不正動作防止制御部0106は、データ領域保護設定処理0603と同様の処理を行う。

ただし、未使用領域であるかどうかを確かめる処理(ステップS0602)の後、図20のフローチャートに示す、プログラムAの機能フラグが保護対象データ0108のセキュリティ要件リスト0109記載のセキュリティ要件を満たすかどうかの確認を行う処理が追加される。

- [0154] もし、セキュリティ要件を満たしていないければ不正動作防止制御処理を終了する。

ここで、セキュリティ要件を満たすかどうかの確認において、不正動作防止制御部0106は、まずセキュリティ要件リストの正当性確認を行う(ステップS1801)。

セキュリティ要件リストが正当でないと判断した場合(ステップS1801のNO)、不正動作防止制御処理を終了する。

- [0155] ここで、不正動作防止制御部0106は、署名データ0708を用い、セキュリティ要件リスト0109の正当性の確認を行う。

次に、不正動作防止制御部0106は、セキュリティ要件と機能フラグの比較を行う(ステップS1802)。

ここで、不正動作防止制御部0106は、正当性を確認したセキュリティ要件リスト0109とプログラム管理情報T1301に含まれるプログラムAの機能フラグを比較し、セキュリティ要件を満たしているかどうかの確認、および、セキュリティ要件管理情報テーブルT1400に含まれる生成したプログラムがプログラムAであるセキュリティ要件管理情報のセキュリティ要件がセキュリティ要件リスト0109を満たしているかどうかの確

認を行う。

- [0156] セキュリティ要件を満たしていないと判断された場合(ステップS1802のNO)、不正動作防止制御処理を終了する。

セキュリティ要件管理情報テーブルT1400に含まれる他のデータ領域のセキュリティ要件がセキュリティ要件リスト0109を満たしているかどうか確認することで、保護対象データ0108のセキュリティ要件を満たしていないデータ領域からデータが漏洩することを防止することができる。

- [0157] 次に、不正動作防止制御部0106は、データ暗号鍵0702の復号化を行った後(ステップS1803)、データ領域管理情報テーブルの更新(ステップS0603)を行う。

ここで、不正動作防止制御部0106は、プログラムA用データ領域管理情報テーブルT0500にデータ領域管理情報T0502を追加すると共に、セキュリティ要件管理情報テーブルT1400にセキュリティ要件管理情報T1402を追加する。

- [0158] データ領域管理情報T0502のデータ暗号鍵には、データ暗号鍵0702が格納される。

図17では、データ暗号鍵0702は、“KD\_S”と示されている。

次にプログラムA0102は、1600～1699番地までのデータ領域をセキュリティ要件リスト0109に基づくセキュリティ要件で確保するよう不正動作防止制御部0106に依頼をする(ステップS1103)。

- [0159] ここで、セキュリティ要件リスト0109には、保護対象データ0108はファイル出力禁止である旨の情報が含まれている。

ここで、不正動作防止制御部0106は、要求されたセキュリティ要件が、プログラムA0102が既に生成しているすべてのデータ領域のセキュリティ要件と同等かもしくは厳しいものであるかをセキュリティ要件管理情報テーブルT1400を用いて確認する。

- [0160] もし、要求されたセキュリティ要件が、既に生成しているすべてのデータ領域のセキュリティ要件と同等かもしくは厳しいものでなければ、管理情報の追加は行わない。

要求されたセキュリティ要件が、既に生成しているすべてのデータ領域のセキュリティ要件と同等かもしくは厳しいものであると、プログラムA用データ領域管理情報テーブルT0500にデータ領域管理情報T0503が追加されると共に、セキュリティ要件管

理情報テーブルT1400にセキュリティ要件管理情報T1403が追加される。

- [0161] 次に、プログラムA0102は、保護対象データ0108を保護対象データ領域1210から読み出し、保護対象データ0108の処理を行う(ステップS1105)。処理結果は、プログラムAのデータ領域1203に格納される。
- 次に、プログラムA0102は、プログラムA0102からプログラムB0103への切替処理を行う(ステップS1106)。
- [0162] ここで切替処理は、図13及び図14のステップS0901～ステップS0933の処理を行う。
- 切替処理(ステップS1106)が実行される以前、不正動作防止制御部0105には、プログラムA用コード領域管理情報テーブルT0900およびプログラムA用データ領域管理情報テーブルT0500の情報が設定されている。
- [0163] 切替処理(ステップS1106)が実行されると、不正動作防止制御部0105には、プログラムB用コード領域管理情報テーブルT1000およびプログラムB用データ領域管理情報テーブルT0600の情報が設定される。
- ここで、動作中のプログラムに合わせた鍵が鍵レジスタに設定されるように、不正動作防止制御部0105を構成している鍵レジスタ0205の命令用鍵情報テーブル0305に各コード領域管理情報テーブルの設定が反映され、データ用鍵情報テーブル0306に各データ領域管理情報テーブルの設定が反映される。
- [0164] このように、プログラム保護装置0101がプログラムA0102からプログラムB0103への切替処理(ステップS1106)を行い、プログラムA0102がロードされている領域を暗／復号する鍵を変更するので、プログラムB0103によるプログラムA0102の不正実行を防止することができる。
- 例えば、プログラムB0103の動作中にコード暗号鍵KC\_Aで暗号化されてRAM0202に格納されているプログラムAのコード領域1201(1000～1099番地に配置されている)に分岐する場合、コード領域1201のコードはコード暗号鍵KC\_RBを用いて復号化される。
- [0165] 鍵KC\_Aで暗号化されているコードを鍵KC\_RBで復号してもコードは正しく復号されないため、正しくCPU0201は実行することができず、プログラムB0103による

プログラムA0102の不正実行を防止することができる。

また、同様にプログラムB0103の動作中にプログラムAのデータ領域1202にアクセスしたとしてもデータ暗号鍵が異なるので、意味のあるデータは取得できない。

[0166] また、プログラム保護装置0101がプログラムA0102からプログラムB0103への切替処理(ステップS1106)を行うことで、割り込みおよび例外が発生した場合にはプログラムB用割り込み管理部0403に含まれるハンドラが実行される。

そのため、割り込みおよび例外によって、プログラムB0103以外のプログラムに制御を奪われることがない。

[0167] 次に、プログラムB0103は、プログラムBのデータ領域1205を使用可能にするために不正動作防止制御部0106に対しデータ保護設定を依頼する(ステップS1107)。

ここで、プログラムB0103は、2500～2599番地までのデータ領域をプログラムB0103のみアクセス可能な状態で確保するよう不正動作防止制御部0106に依頼をする。

[0168] その結果、プログラムB用データ領域管理情報テーブルT0600にデータ領域管理情報T0601が追加されると共に、セキュリティ要件管理情報テーブルT1400にセキュリティ要件管理情報T1404が追加される。

次に、プログラムB0103は、データ領域1203をプログラムAと共有するためにデータ保護設定を行う(ステップS1108)。

[0169] ここで、プログラムB0103は、1600～1699番地までのデータ領域1203をファイルへの出力不可を示すセキュリティ要件で確保するよう不正動作防止制御部0106に依頼をする。

データ領域1203は、既にプログラムA0102によって確保されているので、データ領域を共有することとなる。

[0170] プログラム保護装置0101は、図12に示すステップS0801～ステップS0813と同様の処理を行う。

ここで、コード・データ保護設定(ステップS0807)において、不正動作防止制御部0106は、図10に示すデータ領域共有設定処理0604を行う。

データ領域共有設定処理0604において、不正動作防止制御部0106は、要求されているデータ領域がセキュリティ要件管理情報テーブルT1400に存在するかどうかを確かめる(ステップS0632)。

- [0171] 不正動作防止制御部0106は、セキュリティ要件管理情報T1403の存在を確認できる。

次に不正動作防止制御部0106は、プログラムBのプログラム管理情報T1302に含まれる機能フラグが、要求されているデータ領域のセキュリティ要件管理情報T1403に含まれるセキュリティ要件を満たすかどうかを確かめる。

- [0172] ここでは、共有対象のデータ領域1203のセキュリティ要件はファイル出力不可であるのに対し、プログラムB0103の機能フラグはファイル出力不可能であるので、妥当であると判断される。

その結果、セキュリティ要件管理情報T1403に含まれる共有プログラム識別子にプログラムBの識別子が設定される。

- [0173] プログラムB0103がデータ領域1203に要求するセキュリティ要件は、ファイルへの出力不可であり、これは既存のセキュリティ要件と等しいので、セキュリティ要件管理情報T1403のセキュリティ要件は変更しない。

次に管理テーブルの更新(ステップS0634)が行われ、プログラムB用データ領域管理情報テーブルT0600にデータ領域管理情報T0602が追加される。

- [0174] データ領域管理情報T0602のデータ暗号鍵は、プログラムA用データ領域管理情報T0503と同様の鍵が設定される。

次にデータ保護設定の変更(ステップS0635)が行われ、鍵レジスタ0205の設定が変更される。

その結果、プログラムB0103からもプログラムAのデータ領域1203の参照が可能となる。

- [0175] 次に、プログラムB0103は、データ領域1203のデータを用いて処理を行う(ステップS1109)。

次にプログラム保護装置0101は、プログラムBからCへの切替処理を行う(ステップS1110)。

次に、プログラムC0107は、プログラムCのデータ領域1207を使用可能にするために不正動作防止制御部0106に対しデータ保護設定を依頼する(ステップS1111)。

- [0176] ここで、プログラムC0107は、3500～3599番地までのデータ領域をプログラムCのみアクセス可能な状態で確保するよう不正動作防止制御部0106に依頼をする。その結果、プログラムC用データ領域管理情報テーブルT0700にデータ領域管理情報T0701が追加されると共に、セキュリティ要件管理情報テーブルT1400にセキュリティ要件管理情報T1405が追加される。

- [0177] 次に、プログラムC0107は、データ領域1203をプログラムA0102と共有するためにデータ保護設定を行う(ステップS1112)。
- ここで、プログラムC0107は、1600～1699番地までのデータ領域1203をファイルへの出力可を示すセキュリティ要件で確保するよう不正動作防止制御部0106に依頼をする。

- [0178] 共有メモリの設定(ステップS1108)と同様に不正動作防止制御部0106は、データ領域共有設定処理0604を行う。

共有メモリの設定(ステップS1112)は、共有メモリの設定(ステップS1108)と異なり、共有メモリの設定は失敗する。

データ領域共有設定処理0604における、要求の妥当性判断(ステップS0633)で妥当でないと判断されるからである。

- [0179] より具体的には、不正動作防止制御部0106は、セキュリティ要件管理情報T1403のセキュリティ要件をプログラム管理情報T1303の機能フラグが満たすかどうかの確認を行う。

セキュリティ要件がファイル出力不可であるのに機能フラグが出力可能であるので、不正動作防止制御部0106は、データ領域1203のセキュリティ要件をプログラムCが満たしていないと判断し(ステップS0633のNO)、不正動作防止制御部0106は、不正動作防止制御処理を終了する。

#### <6. 変形例>

なお、本発明を上記の実施の形態に基づいて説明してきたが、本発明は、上記の

実施の形態に限定されないのはもちろんである。以下のような場合も本発明に含まれる。

(1) 第1実施形態において、コード暗号鍵0710等のコード暗号鍵は、公開鍵暗号アルゴリズムで暗号化されているとしていたが、これに限るものではない。

[0180] それぞれのコード暗号鍵を共通鍵暗号方式で暗号化してもよく、この場合、暗号化する際に用いた共通鍵は不正動作防止制御部0106が保持する。また、プログラムは必ずしも暗号化する必要はない。その場合、コード暗号鍵0710はNULL鍵とする。また、コード暗号鍵0710は、プログラムAのコード0711を暗号化する際に用いたアルゴリズム情報を含むことができる。

[0181] また、データ暗号鍵0702についても、データ暗号鍵0702を共通鍵暗号方式で暗号化してもよく、この場合、暗号化する際に用いた共通鍵は不正動作防止制御部0106が保持する。

また、データ0701を暗号化しない場合、データ暗号鍵0702はNULL鍵とする。

[0182] また、データ暗号鍵0702は、データ0701を暗号化する際に用いたアルゴリズム情報を含むことができる。

(2) 上述の実施形態では、不正動作防止回路0105を用いて、RAM0202へのアクセスを制限していたが、これに限らず、RAM0202へのアクセスを、プログラム単位で制限することができる他の回路、方法等を用いてもよい。

[0183] 例えば、図22に示すように、不正動作防止回路0105に代えて、不正動作防止回路2105を用いてもよい。

不正動作防止回路2105は、RAM0202に記憶させるコード、データに対し暗号化、復号を行うのに代えて、RAM0202へのアクセスを、プログラムIDを用いて制限する。

[0184] 不正動作防止回路2105は、鍵レジスタに代えてIDレジスタ2205を備え、バス暗号回路に代えてバス接続許可回路2204を備える。

IDレジスタ2205は、図23に示すように、アドレスと命令用バス接続IDとの対応を示す命令用ID情報テーブル2305と、アドレスとデータ用バス接続IDとの対応を示すデータ用ID情報テーブル2306とを保持しており、バス接続許可回路2204からアド

レス信号2301を取得して、アドレス信号2301が示すアドレスに対応づけられている命令用バス接続ID2302と、データ用バス接続ID2303とをバス接続許可回路2204に出力する。

[0185] ここで、命令用ID情報テーブル2305は、命令用ID情報T2311、T2312、T2313…を含み、各命令用ID情報は、アドレスと命令用バス接続ID暗号鍵との対応を示しており、データ用ID情報テーブル2306は、データ用ID情報T2321、T2322、T2323…を含み、各データ用ID情報は、アドレスとデータ用バス接続IDとの対応を示している。

[0186] この変更に伴い、不正動作防止制御部0106が管理する管理テーブル0110の内容は、上述の実施形態で説明したものに代えて、不正動作防止回路2105に設定するためのIDに関する情報とする。

また、IDレジスタ2205の設定は、状態切替回路0208が出力する状態信号Bが保護モードを示すときのみ、バス0210により通知される設定信号2304を用いて変更することができる。

[0187] RAM0202は、バス接続許可回路2204と接続されているメモリ装置である。

バス接続許可回路2204は、IDレジスタ2205から通知されるデータ用バス接続ID、コード用バス接続IDと、現在動作中のプログラム固有のIDとを比較し、一致する場合に、当該アドレスで示されるメモリ領域へのアクセスを許可する。前述の現在動作中のプログラム固有のIDは、カレントプログラム管理テーブルT0503に設定されているカレントプログラムの固有のIDである。

[0188] これにより、コードやデータが、バス0210とRAM0202との間でやり取りされるか否かをバス接続許可回路2204により制御することができる。

また、バス接続許可回路2204は、CPU0201上で動作するプログラムが命令フェッチのためにRAM0202にアクセスしているのか、データアクセスのためにアクセスしているのかを検知し、同一物理アドレスへの命令フェッチの場合には命令用バス接続IDを用い、データアクセスの場合にはデータ用バス接続IDを用いる。

[0189] (3) 上記の実施形態では、プログラム単位で、コード領域、データ領域、セキュリティ要件、プログラムの管理情報、メモリの共有など情報の管理や、実行単位の切替を

行っていたが、これに限らず、プロセス、スレッドなど他の単位毎に行ってもよい。この場合、通常モードや保護モードのそれぞれで連携動作するプロセスやスレッドは、互いに異なるプログラムに含まれるプロセスやスレッドではなく、同一のプログラムの別プロセスや別スレッドであってもよい。(4)上記の各装置は、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクユニット、ディスプレイユニット、キーボード、マウスなどから構成されるコンピュータシステムである。前記RAM又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、各装置は、その機能を達成する。ここで、コンピュータプログラムは、所定の機能を達成するために、コンピュータに対する指令を示す命令コードが複数個組み合わされて構成されたものである。

[0190] (5)上記の各装置を構成する構成要素の一部又は全部は、1個のシステムLSI(Large Scale Integration:大規模集積回路)から構成されているとしてもよい。システムLSIは、複数の構成部を1個のチップ上に集積して製造された超多機能LSIであり、具体的には、マイクロプロセッサ、ROM、RAMなどを含んで構成されるコンピュータシステムである。前記RAMには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、システムLSIは、その機能を達成する。これらは個別に1チップ化されても良いし、一部又は全てを含むように1チップ化されても良い。

[0191] ここでは、LSIとしたが、集積度の違いにより、IC、システムLSI、スーパーLSI、ウルトラLSIと呼称されることもある。

また、集積回路化の手法はLSIに限るものではなく、専用回路又は汎用プロセサで実現してもよい。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リコンフィギュラブル・プロセッサーを利用して良い。

[0192] さらには、半導体技術の進歩又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、その技術を用いて機能ブロックの集積化を行ってもよい。バイオ技術の適応等が可能性としてありえる。

(6) 上記の各装置を構成する構成要素の一部又は全部は、各装置に脱着可能なICカード又は単体のモジュールから構成されているとしてもよい。前記ICカード又は前記モジュールは、マイクロプロセッサ、ROM、RAM、などから構成されるコンピュータシステムである。前記ICカード又は前記モジュールは、上記の超多機能LSIを含むとしてもよい。マイクロプロセッサが、コンピュータプログラムに従って動作することにより、前記ICカード又は前記モジュールは、その機能を達成する。このICカード又はこのモジュールは、耐タンパ性を有するとしてもよい。

- [0193] (7) 本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータ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。

また、本発明は、前記コンピュータプログラム又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コンピュータプログラム又は前記デジタル信号であるとしてもよい。

- [0194] また、本発明は、前記コンピュータプログラム又は前記デジタル信号を、電気通信回線、無線又は有線通信回線、インターネットを代表とするネットワーク、データ放送等を経由して伝送するものとしてもよい。

また、本発明は、マイクロプロセッサとメモリとを備えたコンピュータシステムであって、前記メモリは、上記コンピュータプログラムを記憶しており、前記マイクロプロセッサは、前記コンピュータプログラムに従って動作するとしてもよい。

- [0195] また、前記プログラム又は前記デジタル信号を前記記録媒体に記録して移送することにより、又は前記プログラム又は前記デジタル信号を前記ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。

(8) 上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。

#### <7. 用語についての補足説明>

前記データ処理装置は、プログラム保護装置0101に相当する。

- [0196] 前記検出手段は、CPU0201及び状態切替部0208に相当する。
- 前記アクセス手段は、不正動作防止制御回路0105及びRAM0202及び保護メモリ0206及びアクセス制限回路0207に相当する。
- 前記切替手段は、状態切替部0208に相当する。
- 前記判定手段は、不正動作防止制御部0106に相当する。
- [0197] 前記制御手段は、不正動作防止制御部0106及びセキュリティカーネル0401に相当する。
- 前記メモリは、RAM0202に相当する。
- 前記保持部は、鍵レジスタ0205に相当する。
- 前記アクセス制限部は、不正動作防止制御部0106及びセキュリティカーネル0401及び不正動作防止制御回路0105及びRAM0202及び保護メモリ0206及びアクセス制限回路0207に相当する。
- [0198] 前記アクセス制限部における前記取得部は、RAM0202と、不正動作防止回路0205と、セキュリティカーネル0401と、不正動作防止制御部0106に相当する。
- 前記アドレス判定部は、鍵レジスタ0205とバス暗号回路0204に相当する。
- 前記アクセス実行部は、バス暗号回路0204に相当する。
- 前記管理情報追加部は、不正動作防止制御部0106に相当する。
- [0199] 前記ベクタテーブル保持手段は、不揮発メモリ221に相当する。
- 前記ベクタテーブル書換手段は、不正動作防止制御部0106に相当する。
- 前記使用要求受付部は、バス暗号回路0204に相当する。
- 前記使用判定部は、バス暗号回路0204に相当する。
- 前記権限判定部は、不正動作防止制御部0106に相当する。
- [0200] 前記管理情報登録部は、不正動作防止制御部0106に相当する。
- 前記デバッグ手段は、デバッガI/F0209に相当する。
- 前記強制無効化手段は、CPU0201に相当する。
- ### 産業上の利用可能性
- [0201] 本発明のプログラム保護装置は、機能追加、不具合修正などのためにプログラムの更新が可能なデジタル家電などとして使用され、家電製品を扱う業者などにより、生

産、使用、販売等される。

## 請求の範囲

- [1] プログラムに従って動作するプロセッサを備え、前記プログラムの実行単位であるプロセスが動作する通常モードと前記プロセスの動作が抑制される保護モードを切り替えて動作するデータ処理装置であつて、  
　　通常モードにおいて、第1プロセスの処理対象データに対して、前記第1プロセスによるアクセスを許可し、他のプロセスによるアクセスを禁止するアクセス禁止手段と、  
　　通常モードにおいて、前記第1プロセスから、第2プロセスの呼び出しを指示する呼出命令を検出する検出手段と、  
　　前記呼出命令が検出されると、通常モードから保護モードに切り替える切替手段と、  
　　保護モードにおいて、前記第2プロセスが、前記処理対象データについての使用権限を有しているか否かを判断する判断手段と、  
　　保護モードにおいて、前記第2プロセスが前記使用権限を有していると判断される場合に、前記アクセス禁止手段に対して、前記第2プロセスが前記通常モードにおいて、前記処理対象データに対しアクセスすることが許可されるように制御する制御手段と  
　　を備えることを特徴とするデータ処理装置。
- [2] 前記アクセス禁止手段は、  
　　メモリと、  
　　プロセス毎の前記メモリ内でアクセスを許可する領域を示す管理情報を、保護モードにおいてのみ書き換え可能に保持する保持部と、  
　　通常モードで動作するプロセスを、前記管理情報に従って前記メモリにアクセスさせるアクセス制限部と、  
　　を含み、  
　　前記制御手段は、前記判断手段により使用権限があると判定された場合に、第2プロセスの管理情報に、前記メモリ上で前記対象データが保持されている領域へのアクセスを許可する情報を追加する  
　　ことを特徴とする請求項1に記載のデータ処理装置。

- [3] 前記保持部が保持する前記管理情報は、前記メモリ中のアドレスと、アドレスに対応する鍵とを対応付けた情報を一以上含み、  
前記アクセス制限部は、  
前記メモリのアドレスを含む前記メモリへのアクセス要求を取得する取得部と、  
前記アクセス要求に含まれるアドレスが、前記管理情報に含まれるか否かを判定するアドレス判定部と、  
含まれると判定された場合に、前記アクセス要求が書込要求であれば、書き込むデータを前記アドレスに対応する鍵で暗号化して前記アドレスで示される領域に書き込み、前記アクセス要求が読み出要求であった場合には、前記メモリの前記アドレスから読み出したデータを、前記アドレスに対応する鍵を用いて復号して出力するアクセス実行部と  
を含むことを特徴とする請求項2に記載のデータ処理装置。
- [4] 前記データは、プロセスのコードである  
ことを特徴とする請求項2に記載のデータ処理装置。
- [5] 各プロセスには、個別のプロセス識別子が割り当てられ、  
前記保持部が保持する前記管理情報は、前記メモリ中のアドレスと、前記アドレスへのアクセスが許可されているプロセスを示すプロセス識別子とを対応付けた情報を一以上含み、  
前記アクセス制限部は、  
前記メモリのアドレスを含む前記メモリへのアクセス要求を取得する取得部と、  
アクセス要求に含まれるアドレスと、アクセス要求したプロセスに割り当てられたプロセス識別子とを対応付けた情報が、前記管理情報に含まれるか否かを判定するアドレス判定部と、  
含まれると判定された場合に、アクセス要求したプロセスを、前記メモリの前記アドレスにアクセスさせるアクセス実行部と  
を含むことを特徴とする請求項2に記載のデータ処理装置。
- [6] 前記データには、一以上のデータ処理方法それぞれについて実行を許可するか否かを示すセキュリティ要件情報が割り当てられ、

プロセスそれぞれには、一以上のデータ処理方法それぞれを実行可能か否かを示す機能情報が割り当てられ、

前記呼出命令は、一以上のデータ処理方法のいずれかを示す処理特定情報を含み、

前記判断手段は、前記セキュリティ要件情報が前記処理特定情報により示されるデータ処理方法の実行を許可しておりかつ第2プロセスの機能情報が、前記処理特定情報により示されるデータ処理方法の実行が可能であることを示す場合に、前記使用権限があると決定する

ことを特徴とする請求項1に記載のデータ処理装置。

- [7] 前記切替手段は、前記通常モードから前記保護モードへと切り替える場合に、前記通常モードで動作しているプロセスのコンテキストを前記メモリに退避し、  
前記保護モードから前記通常モードへと切り替える場合に、次に前記通常モードで動作するプロセスのコンテキストを前記メモリから復帰させる  
ことを特徴とする請求項1に記載のデータ処理装置。

- [8] 前記第1プロセス及び前記第2プロセスは、それぞれが動作している間に割り込み又は例外が発生した場合に、その割り込み又は例外を処理する割込処理又は例外処理を含み、  
前記データ処理装置は、さらに、  
割り込み又は例外が発生した場合に、実行されるべき処理を示すベクタテーブルを、保護モードにおいてのみ書き換え可能に保持するベクタテーブル保持手段と、  
動作するプロセスが、前記第1プロセスから前記第2プロセスへと切り替わる前に、保護モードにおいて前記ベクタテーブルを、前記通常モードにおいて割り込み又は例外が発生した際に第2プロセスの割込処理又は例外処理を実行するよう書き換えるベクタテーブル書換手段と  
を含むことを特徴とする請求項7記載のデータ処理装置。

- [9] 前記判断手段は、さらに、  
プロセスから前記メモリにおける領域の使用要求を受け付ける使用要求受付部と、  
使用要求されたアドレスが、既に使用されているか否かを判定する使用判定部と、

使用されていなかった場合に、使用要求したプロセスの、前記アドレスに格納を要望するデータについての使用権限の有無を判定する権限判定部と、  
前記権限判定部により使用権限があると判定された場合に、使用要求したプロセスの管理情報に、前記アドレスで示される領域へのアクセスを許可する情報を登録する管理情報登録部と  
を含むことを特徴とする請求項1に記載のデータ処理装置。

- [10] 前記管理情報登録部は、前記権限判定部により使用権限があると判定された場合に、鍵を生成し、前記アクセスを許可する情報として、前記アドレスと生成した鍵とを対応付けた情報の組を使用要求した前記プロセスの管理情報に追加することを特徴とする請求項9に記載のデータ処理装置。
- [11] 前記データ処理装置は、さらに、  
前記プロセスに係るデバッグを行うデバッグ手段を含み、  
前記切替手段は、さらに、前記通常モードに切り替える場合に、前記デバッグ手段を有効化し、前記保護モードに切り替える場合に、前記デバッグ手段を無効化することを特徴とする請求項1記載のデータ処理装置。
- [12] プログラムに従って動作するプロセッサを備え、前記プログラムの実行単位であるプロセスが動作する通常モードと前記プロセスの動作が抑制される保護モードを切り替えて動作するデータ処理装置に用いられるデータ処理方法であつて、  
通常モードにおいて、第1プロセスの処理対象データに対して、前記第1プロセスによるアクセスを許可し、他のプロセスによるアクセスを禁止するアクセス禁止ステップと  
、  
通常モードにおいて、前記第1プロセスから、第2プロセスの呼び出しを指示する呼出命令を検出する検出ステップと、  
前記呼出命令が検出されると、通常モードから保護モードに切り替える切替ステップと、  
保護モードにおいて、前記第2プロセスが、前記処理対象データについての使用権限を有しているか否かを判断する判断ステップと、  
保護モードにおいて、前記第2プロセスが前記使用権限を有していると判断される

場合に、前記アクセス禁止手段に対して、前記第2プロセスが前記通常モードにおいて、前記処理対象データに対しアクセスすることが許可されるように制御する制御ステップと

を含むことを特徴とするデータ処理方法。

- [13] プログラムに従って動作するプロセッサを備え、前記プログラムの実行単位であるプロセスが動作する通常モードと前記プロセスの動作が抑制される保護モードを切り替えて動作するデータ処理装置に用いられるコンピュータプログラムであって、  
通常モードにおいて、第1プロセスの処理対象データに対して、前記第1プロセスによるアクセスを許可し、他のプロセスによるアクセスを禁止するアクセス禁止ステップと  
、

通常モードにおいて、前記第1プロセスから、第2プロセスの呼び出しを指示する呼出命令を検出する検出ステップと、

前記呼出命令が検出されると、通常モードから保護モードに切り替える切替ステップと、

保護モードにおいて、前記第2プロセスが、前記処理対象データについての使用権限を有しているか否かを判断する判断ステップと、

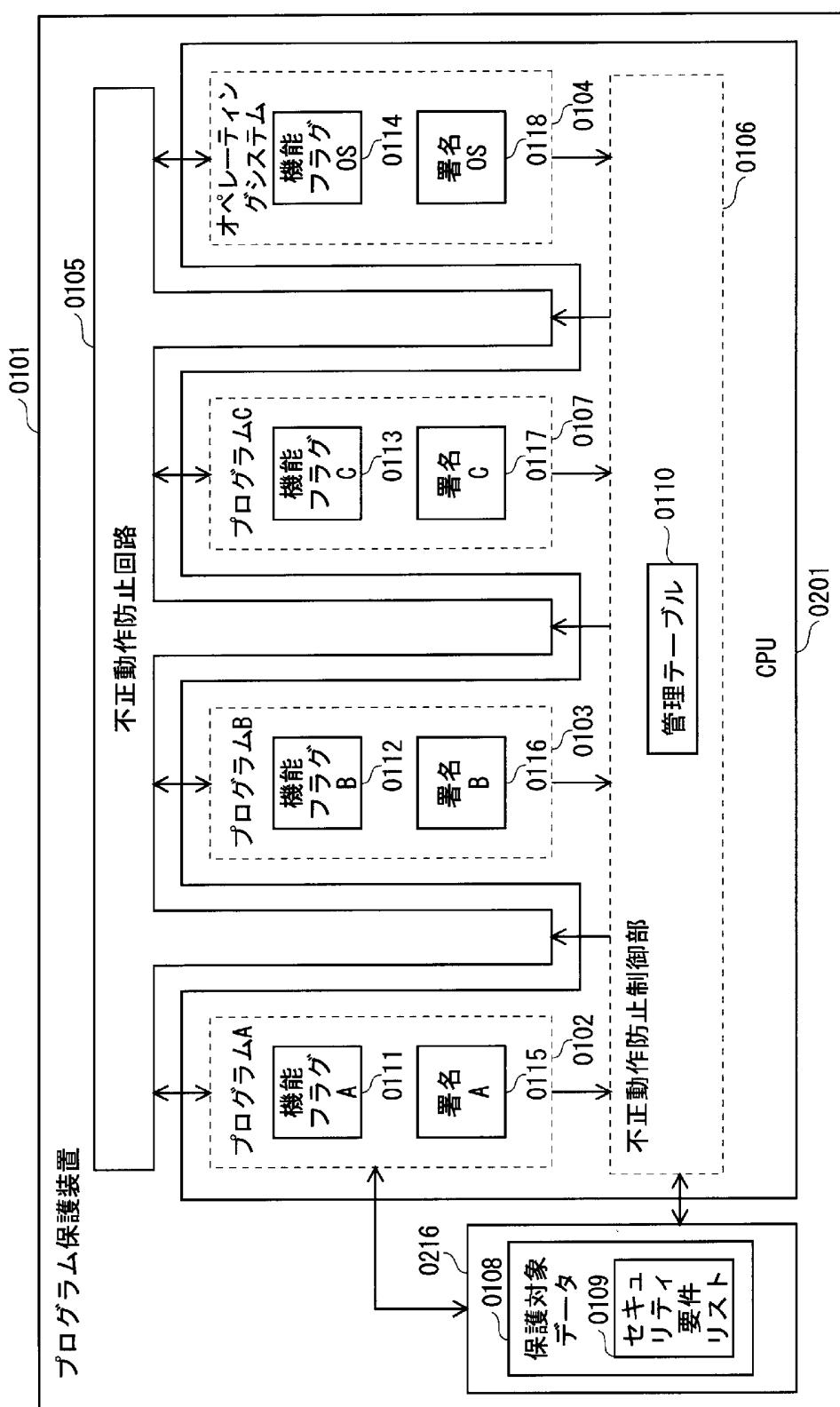
保護モードにおいて、前記第2プロセスが前記使用権限を有していると判断される場合に、前記アクセス禁止手段に対して、前記第2プロセスが前記通常モードにおいて、前記処理対象データに対しアクセスすることが許可されるように制御する制御ステップと

を含むことを特徴とするコンピュータプログラム。

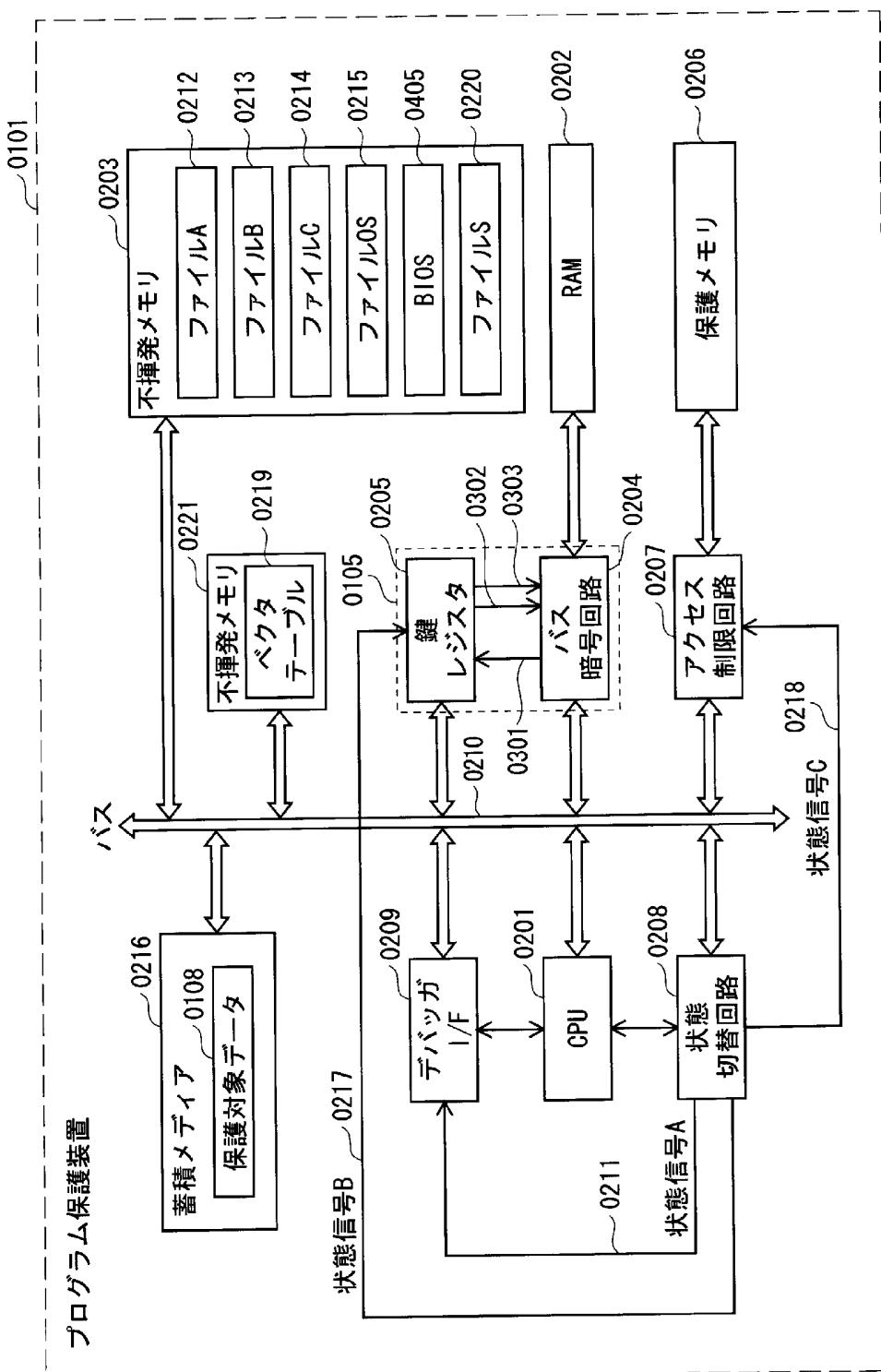
- [14] プログラムに従って動作するプロセッサを備え、前記プログラムの実行単位であるプロセスが動作する通常モードと前記プロセスの動作が抑制される保護モードを切り替えて動作する集積回路であって、  
通常モードにおいて、第1プロセスの処理対象データに対して、前記第1プロセスによるアクセスを許可し、他のプロセスによるアクセスを禁止するアクセス禁止手段と、  
通常モードにおいて、前記第1プロセスから、第2プロセスの呼び出しを指示する呼出命令を検出する検出手段と、

前記呼出命令が検出されると、通常モードから保護モードに切り替える切替手段と、  
保護モードにおいて、前記第2プロセスが、前記処理対象データについての使用  
権限を有しているか否かを判断する判断手段と、  
保護モードにおいて、前記第2プロセスが前記使用権限を有していると判断される  
場合に、前記アクセス禁止手段に対して、前記第2プロセスが前記通常モードにおい  
て、前記処理対象データに対しアクセスすることが許可されるように制御する制御手  
段と  
を備えることを特徴とする集積回路。

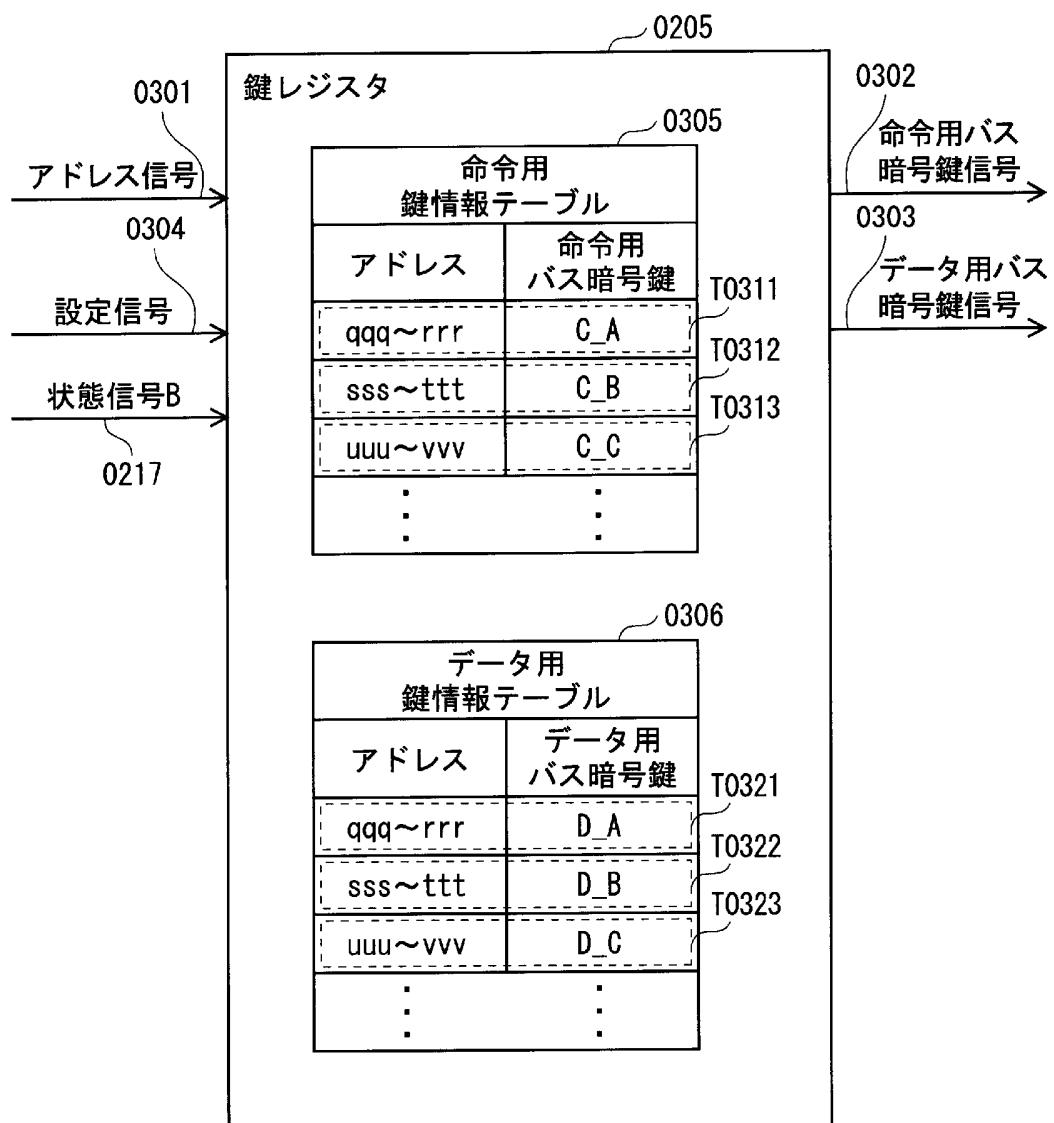
[図1]



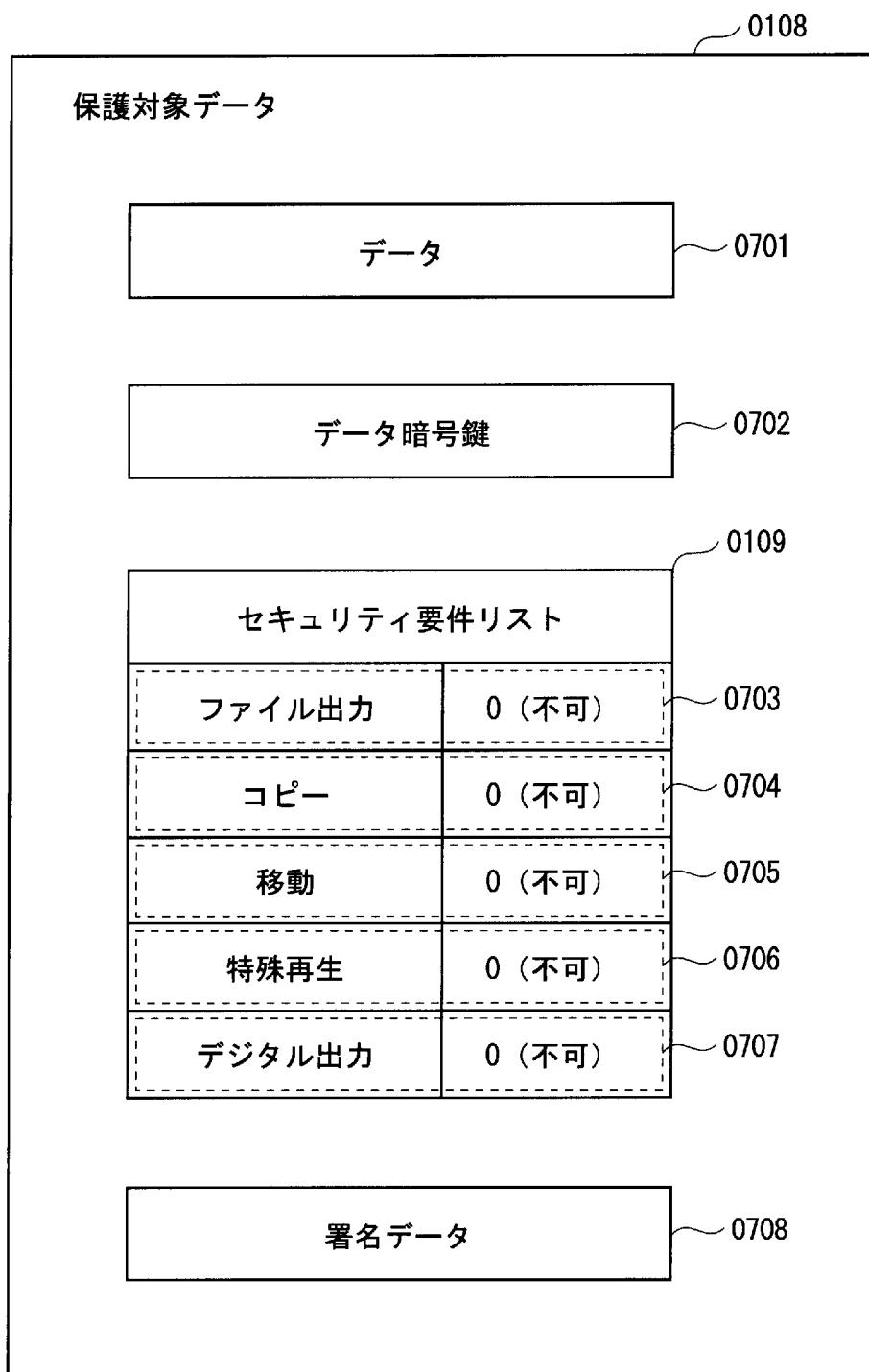
[☒2]



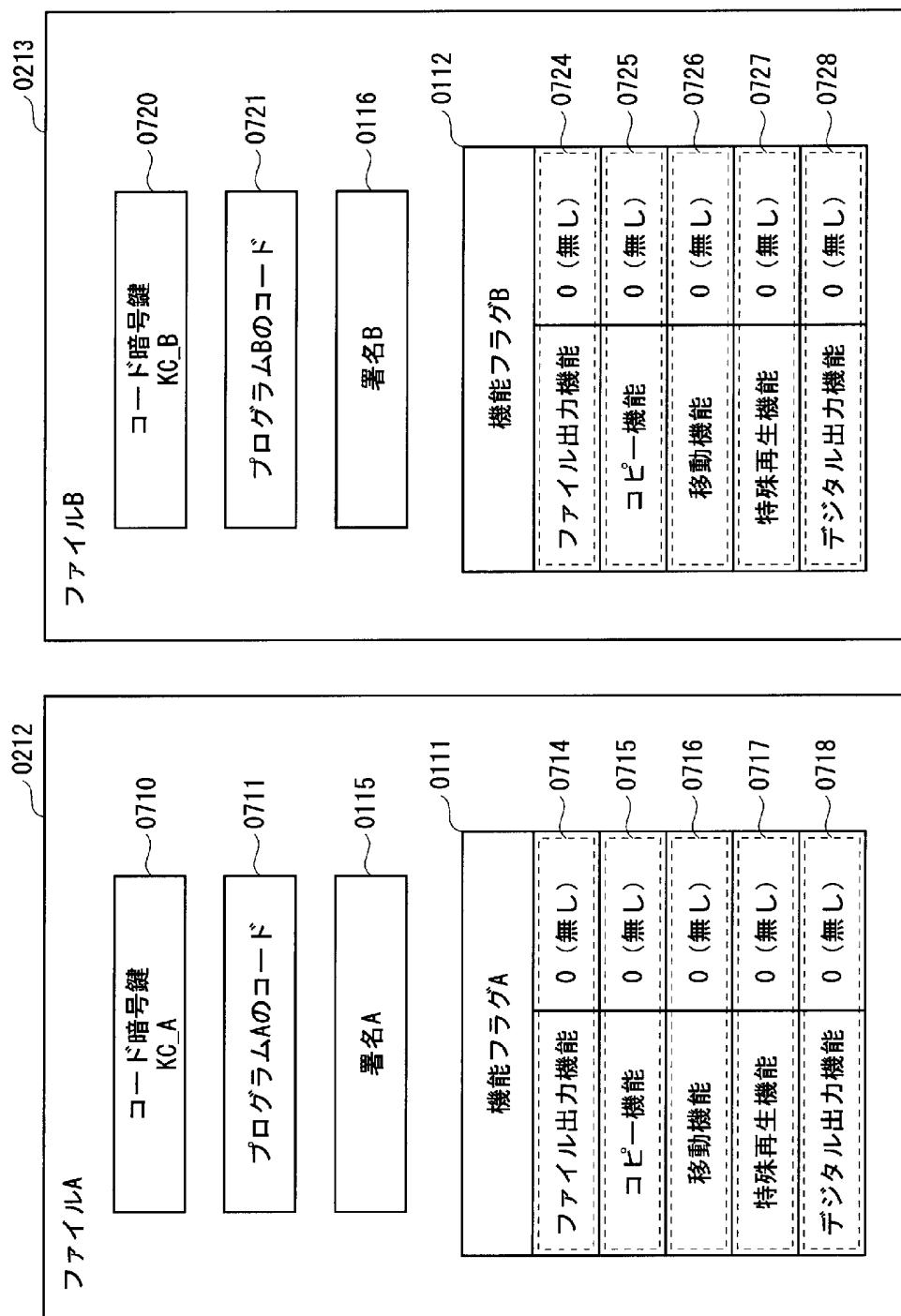
[図3]



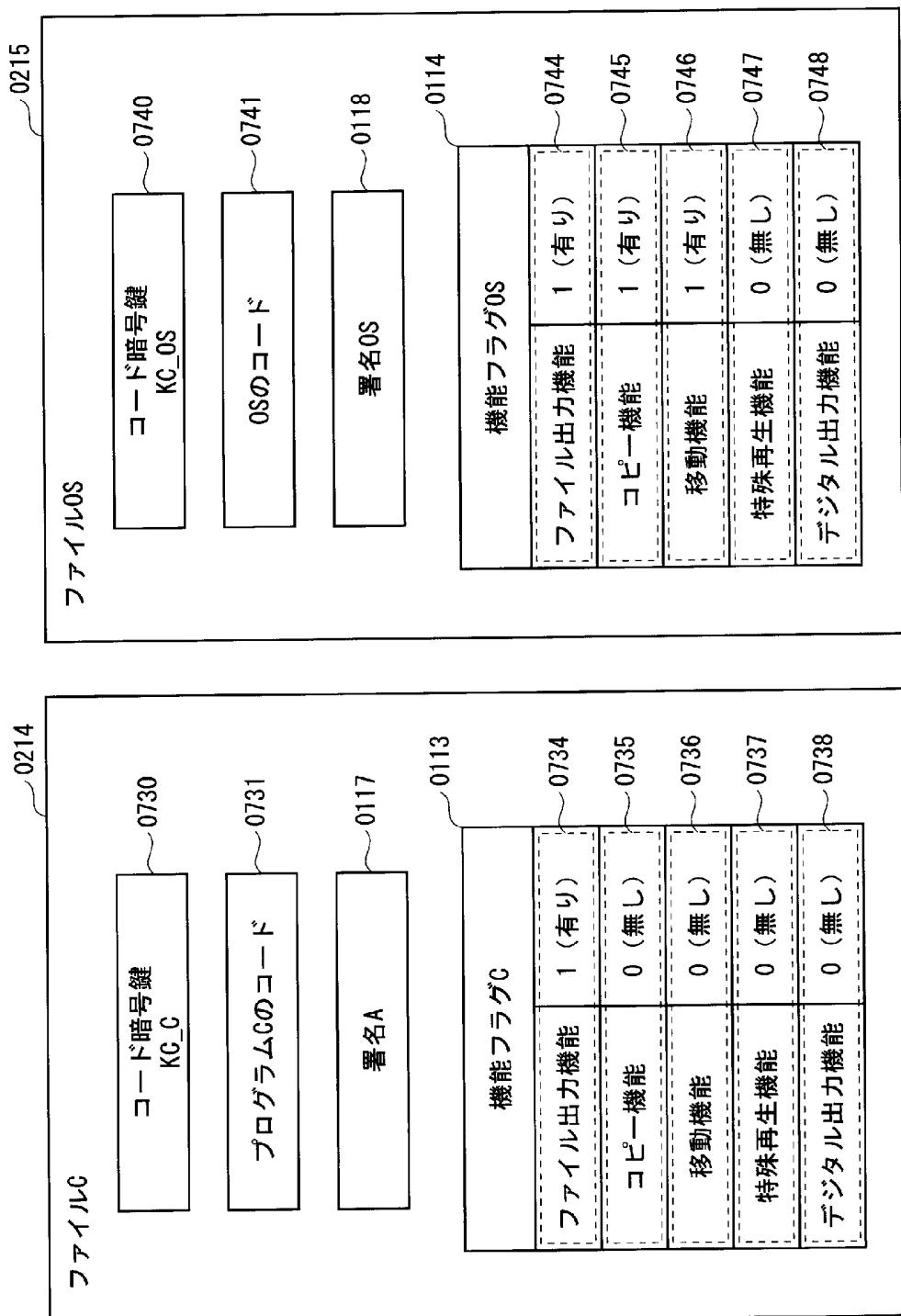
[図4]



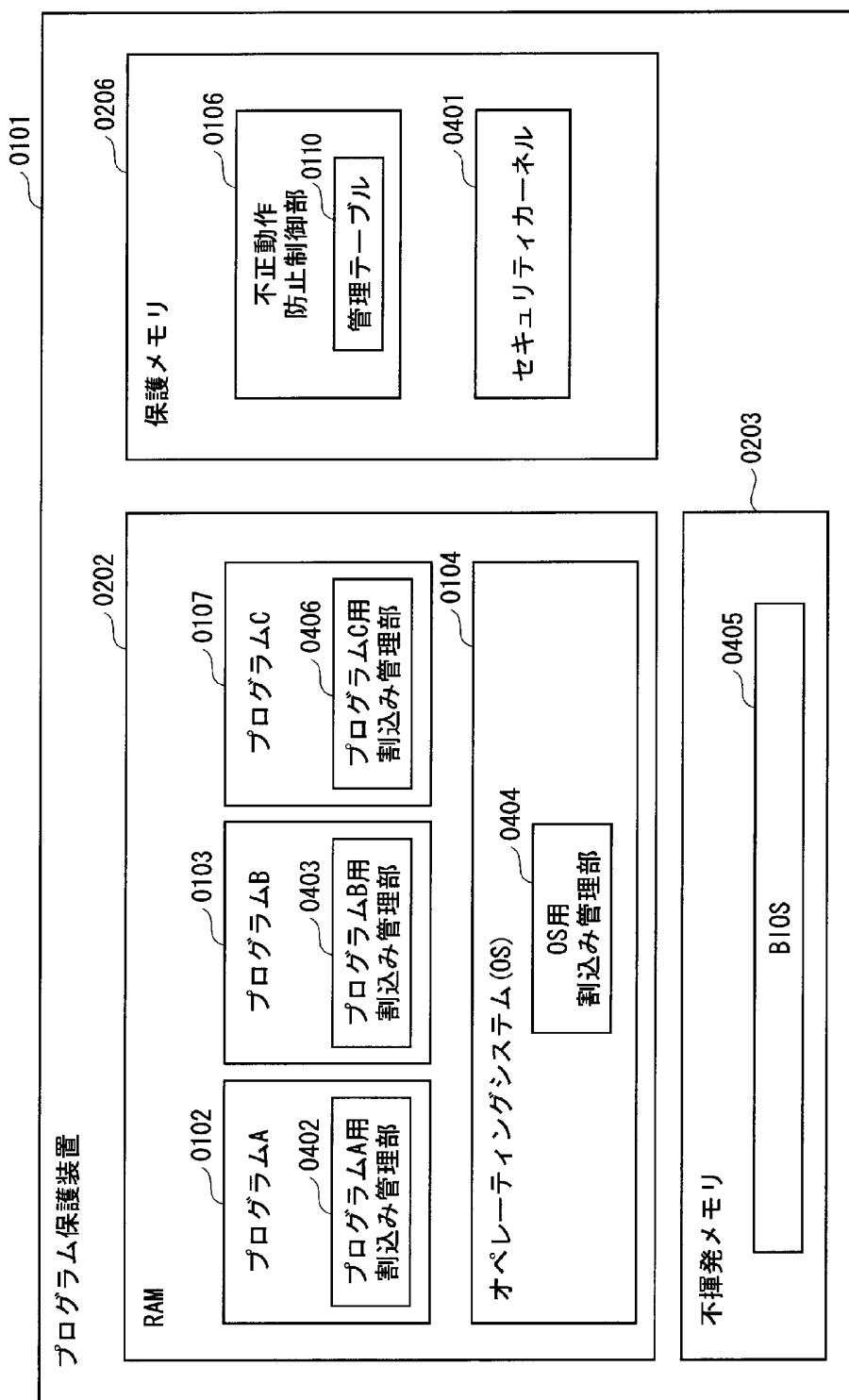
[図5]



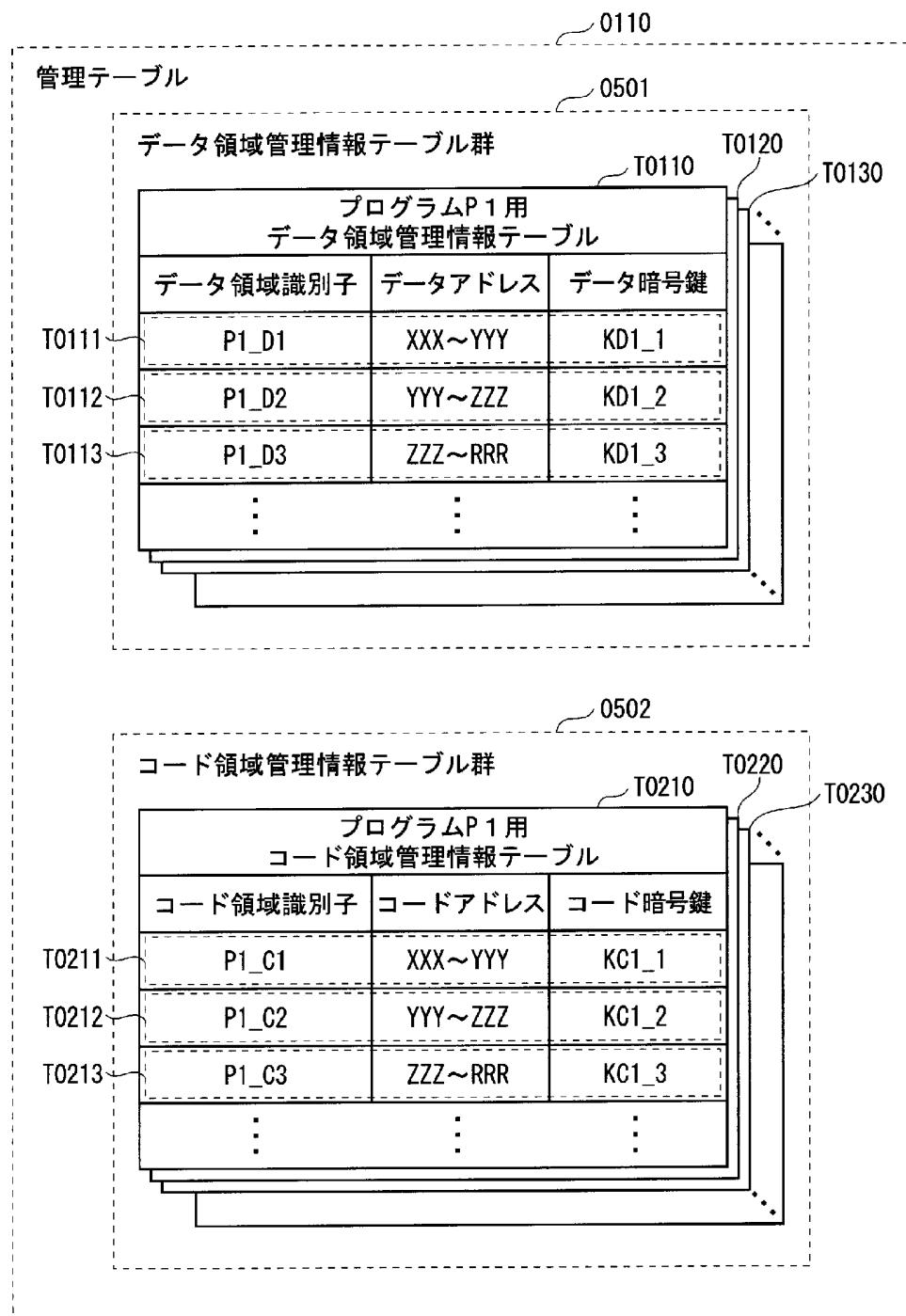
[図6]



[ 7]



[図8]



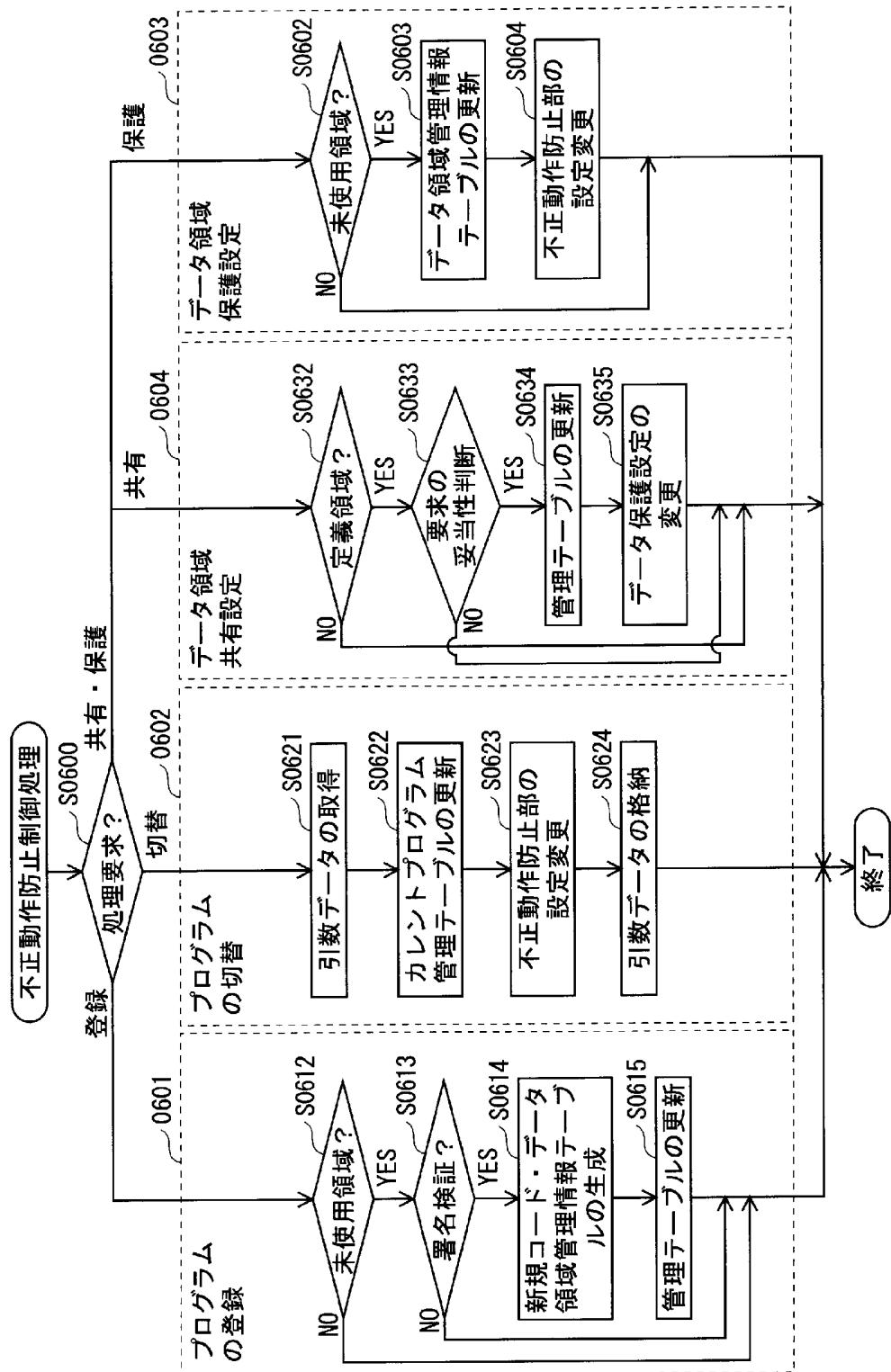
[図9]

セキュリティ要件管理情報テーブル				
セキュリティ要件 管理情報識別子	データアドレス	生成プログラム 識別子	共有プログラム 識別子	セキュリティ要件
1	XXX~YYY	P1	P2、P3	SR1 T0311
2	YYY~ZZZ	P1	P1、P3	SR2 T0312
3	ZZZ~FFF	P1	P1、P2	SR3 T0313
4	AAA~BBB	P2	P1、P2	SR4 T0314
:	:	:	:	カレントプログラム 管理テーブル T0503

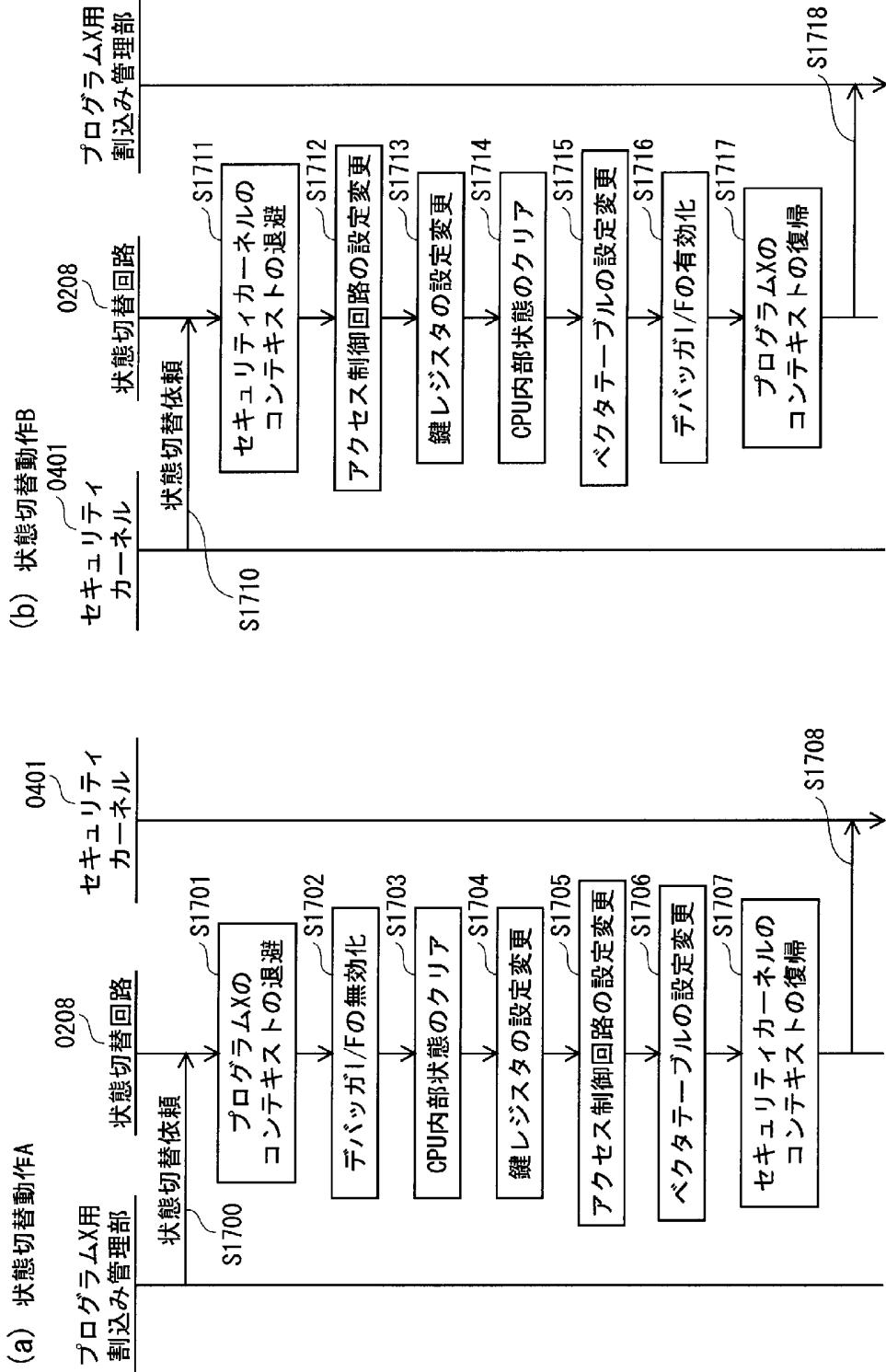
  

プログラム管理情報テーブル				
プログラム管理 情報識別子	コードアドレス	プログラム 識別子	共有プログラム 識別子	機能フラグ
1	XXX~YYY	P1	P2、P3	F1 T0411
2	YYY~ZZZ	P1	P1、P3	F2 T0412
3	ZZZ~FFF	P1	P1、P2	F3 T0413
4	AAA~BBB	P2	P1、P2	F4 T0414
:	:	:	:	:

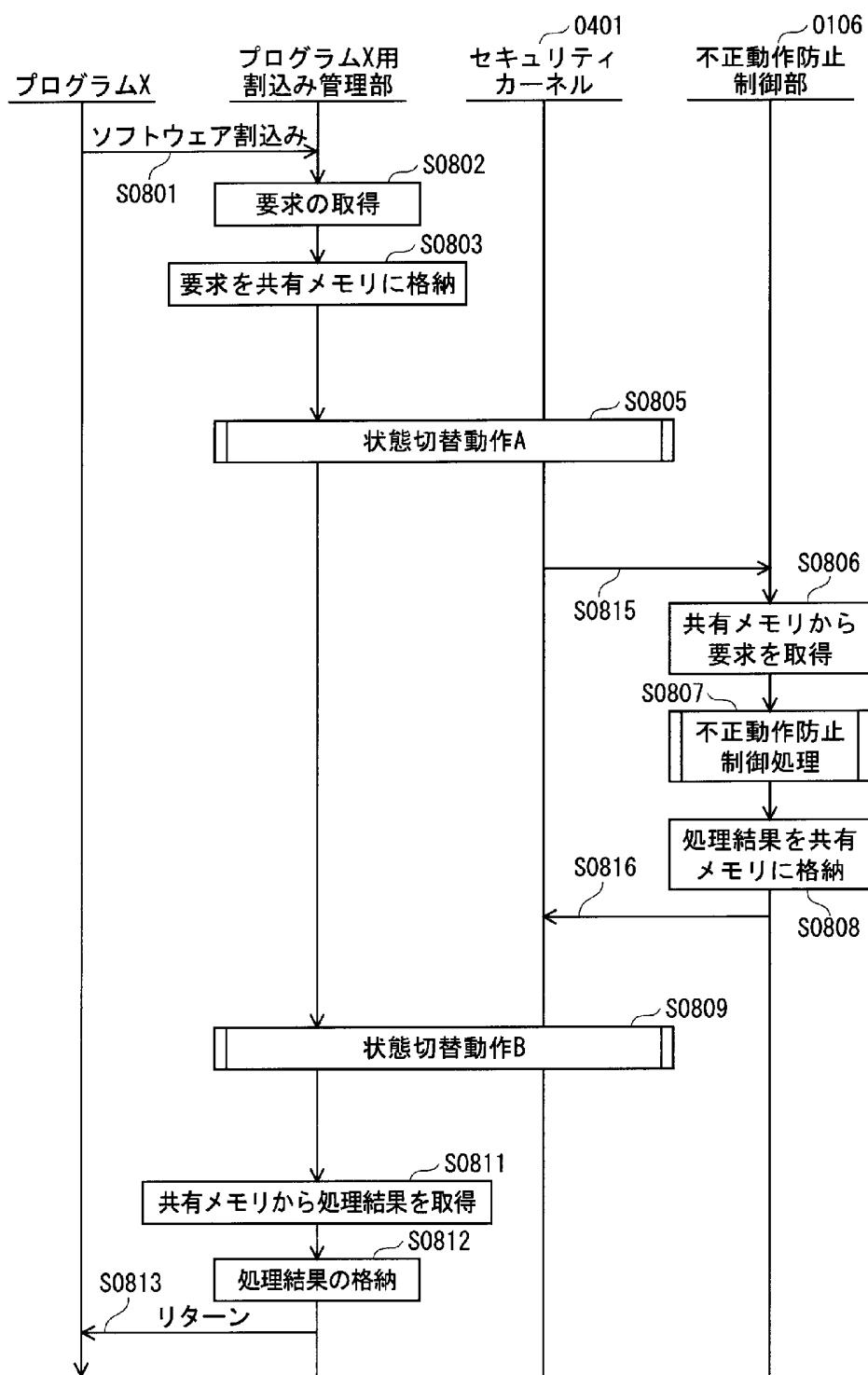
[図10]



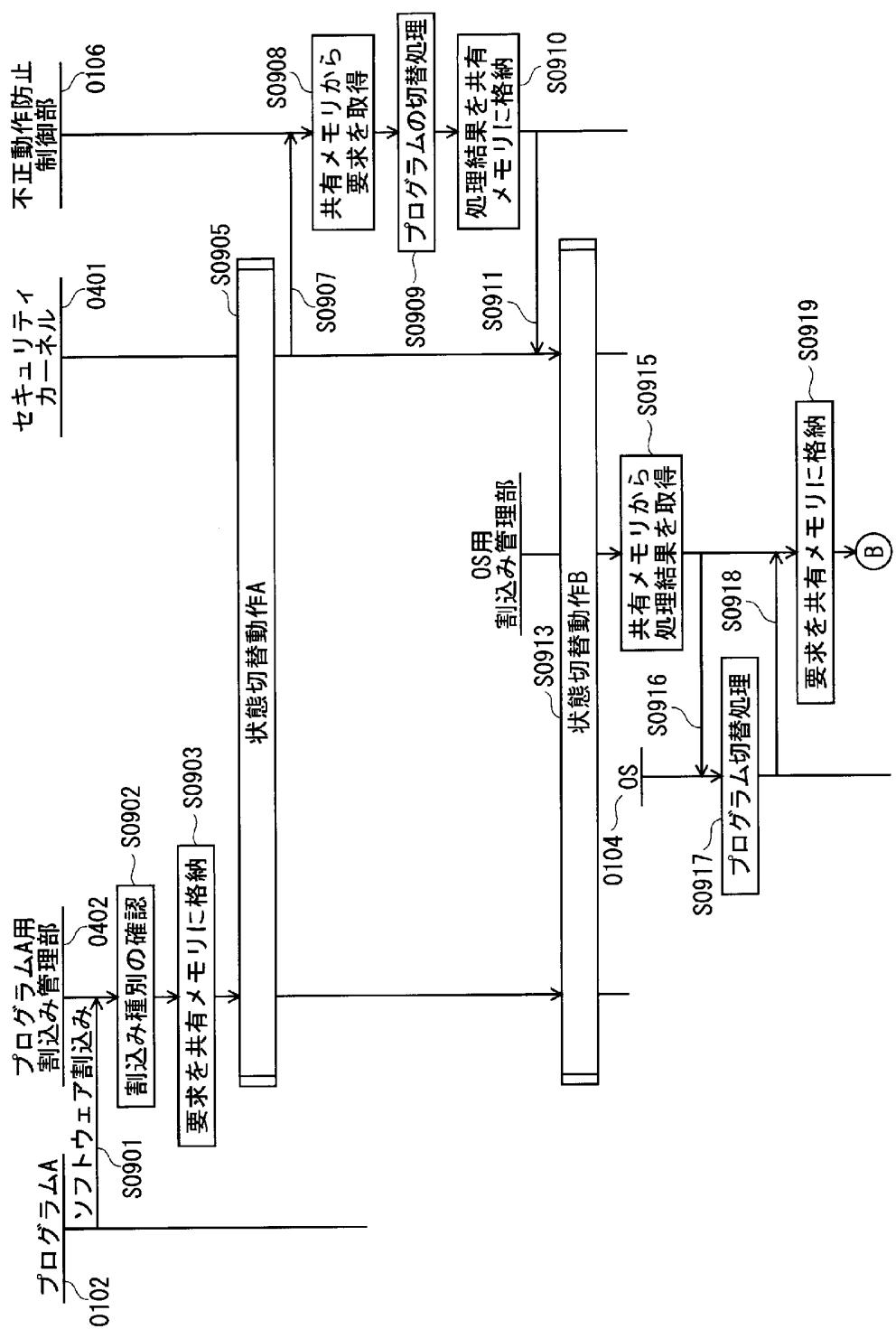
[図11]



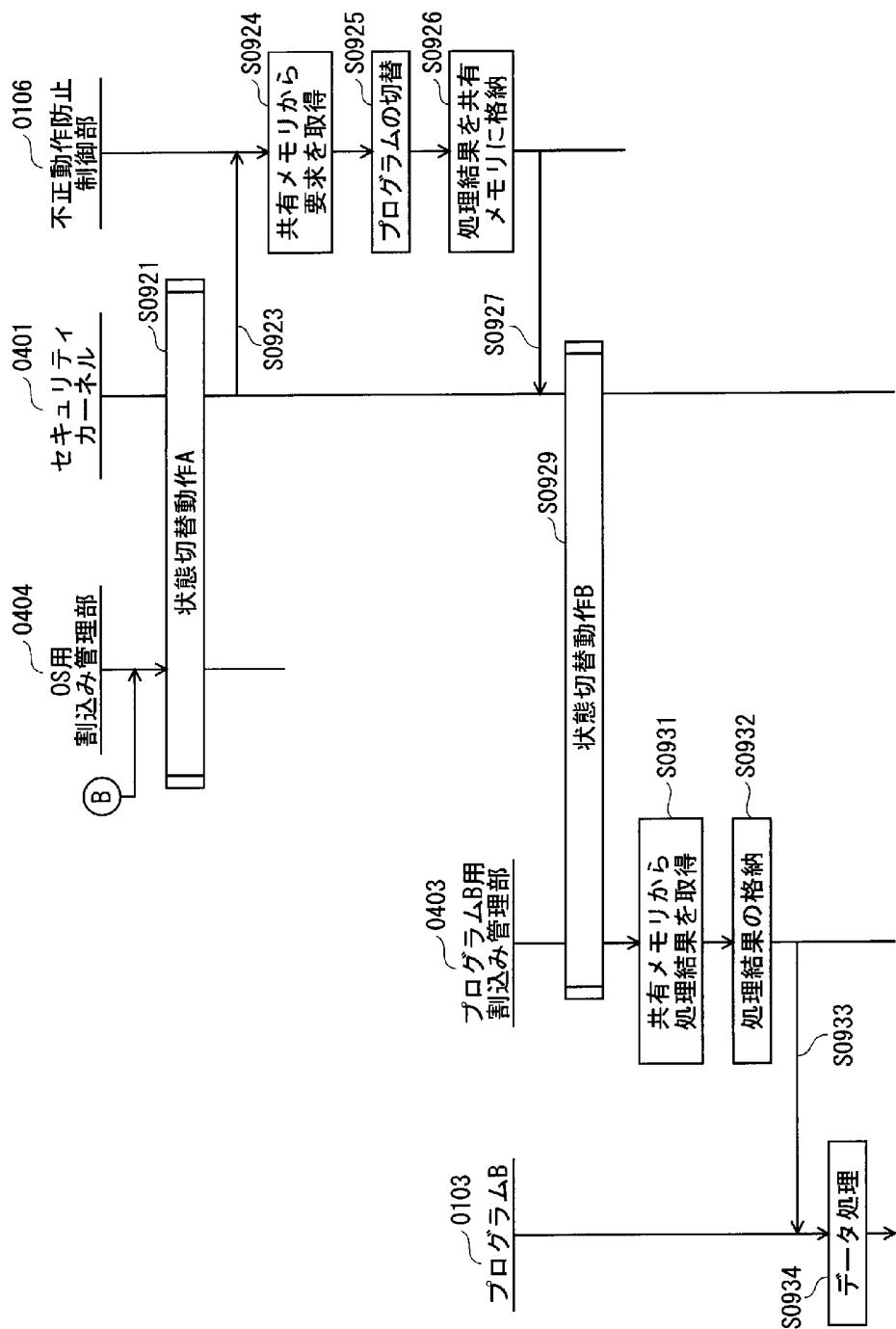
[図12]



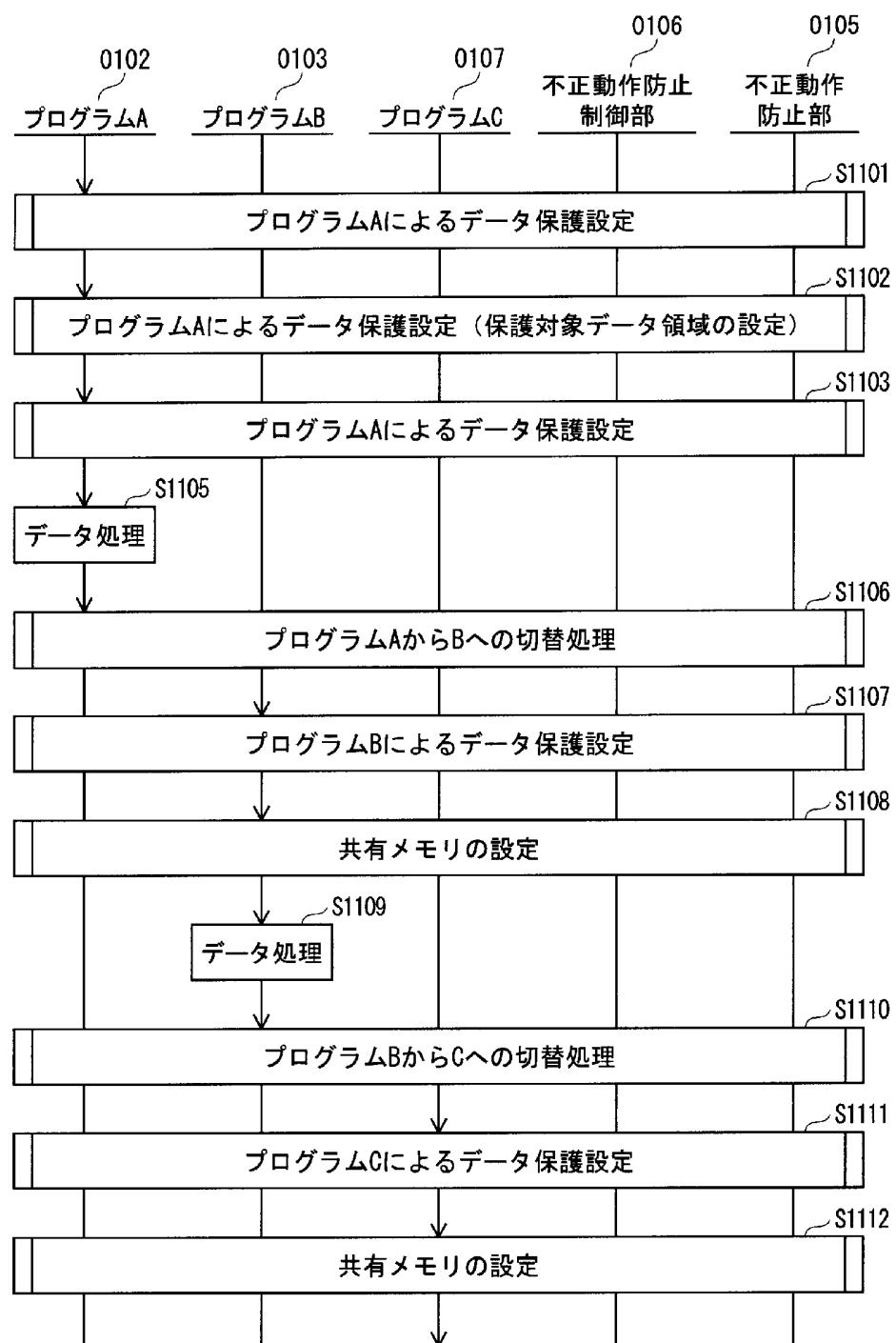
[図13]



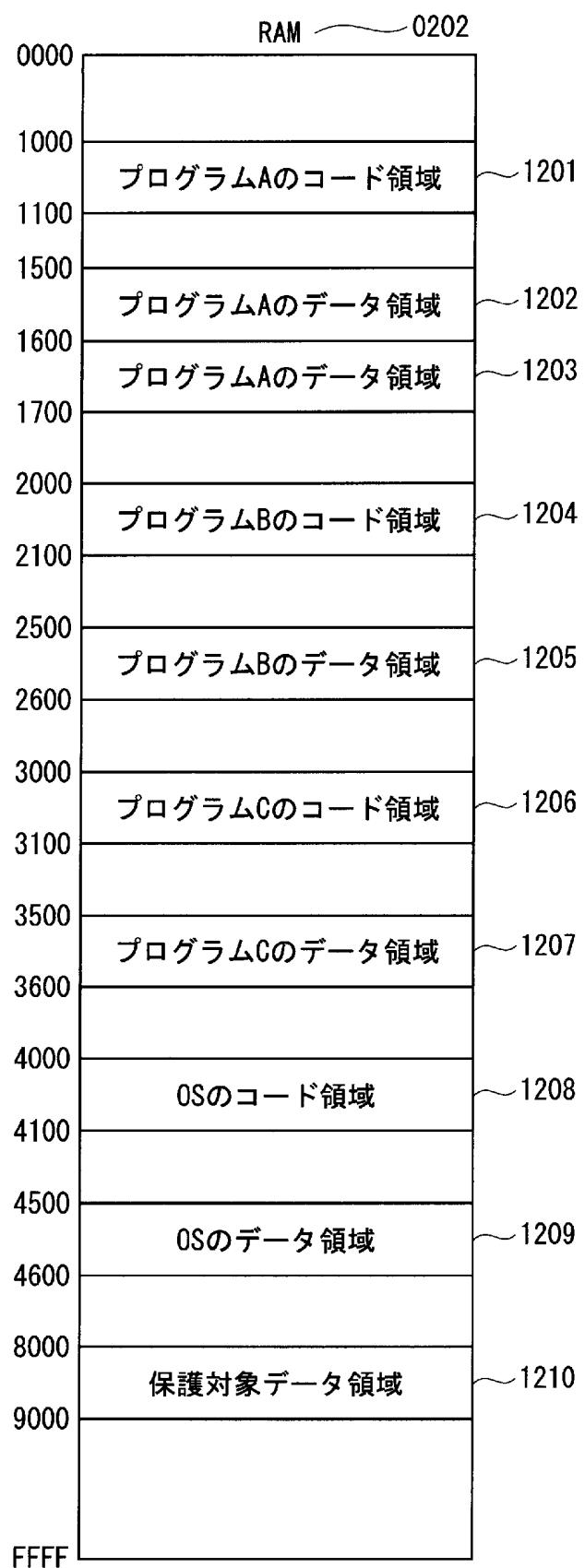
[図14]



[図15]



[図16]



[図17]

データ領域管理情報テーブル		コード領域管理情報テーブル		コード領域管理情報テーブル	
データ領域識別子	データアドレス	コード領域識別子	コードアドレス	コード領域識別子	コードアドレス
A_D0	1500～1599	KD_A1	T0501	A_C0	KC_A
A_D1	8000～8999	KD_S	T0502		
A_D2	1600～1699	KD_A2	T0503	未定義領域	定義領域以外
未定義領域	定義領域以外	KD_RA			KC_RA

データ領域管理情報テーブル		コード領域管理情報テーブル		コード領域管理情報テーブル	
データ領域識別子	データアドレス	コード領域識別子	コードアドレス	コード領域識別子	コードアドレス
B_D0	2500～2599	KD_B1	T0601	B_C0	KC_R3
B_D1	1600～1699	KD_A2	T0602		
未定義領域	定義領域以外	KD_RB		未定義領域	KC_RB

[図18]

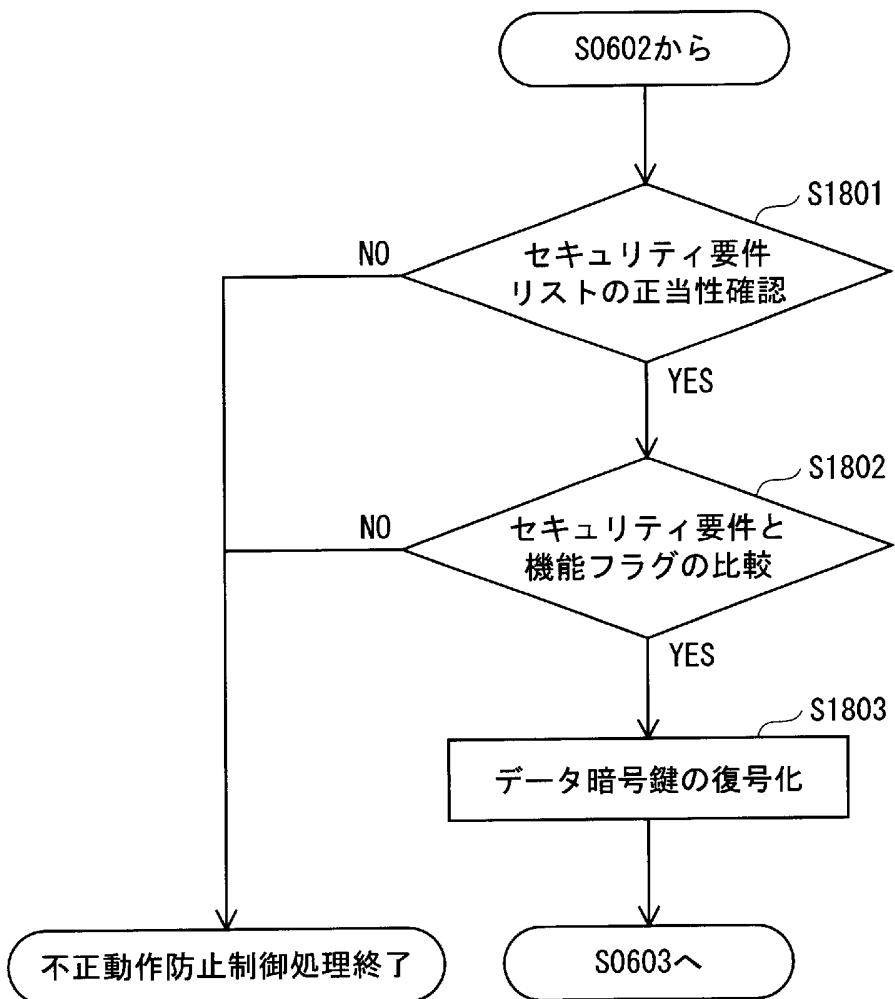
データ領域管理情報テーブル				T0700
プログラムC用 データ領域管理情報テーブル				T1100
コード領域管理情報テーブル				T1200
データ領域 識別子	データ アドレス	データ 暗号鍵	コード 識別子	コード アドレス
C_D0	3500～3599	KD_C1	A_C0	1000～1099
未定義領域	定義領域以外	KD_RB	未定義領域	定義領域以外
				KC_RA

[図19]

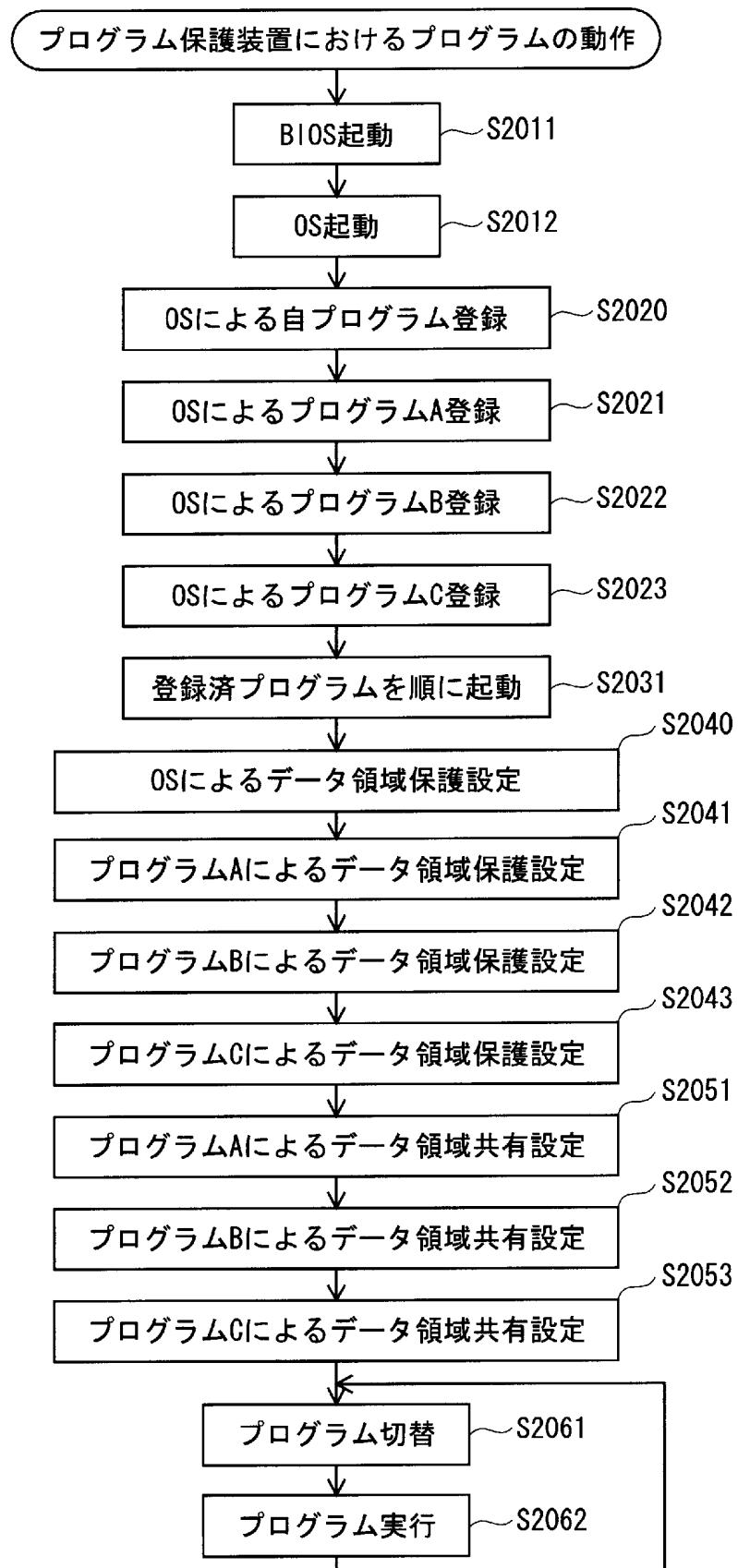
プログラム管理情報テーブル T1300				
プログラム管理 情報識別子	コードアドレス	プログラム 識別子	共有プログラム 識別子	機能フラグ
C1	1000~1099	A	—	ファイル出力機能無し T1301
C2	2000~2099	B	—	ファイル出力機能無し T1302
C3	3000~3099	C	—	ファイル出力機能有り T1303
C4	4000~4099	OS	—	ファイル出力機能有り T1304

セキュリティ要件管理情報テーブル T1400				
セキュリティ要件 管理情報識別子	データアドレス	生成プログラム 識別子	共有プログラム 識別子	セキュリティ要件
D1	1500~1599	A	—	プログラムAのみアクセス可 T1401
D2	8000~8999	A	—	ファイル出力不可 T1402
D3	1600~1699	A	B	ファイル出力不可 T1403
D4	2500~2599	B	—	プログラムBのみアクセス可 T1404
D5	3500~3599	C	—	プログラムCのみアクセス可 T1405
D6	4500~4599	OS	—	OSのみアクセス可 T1406

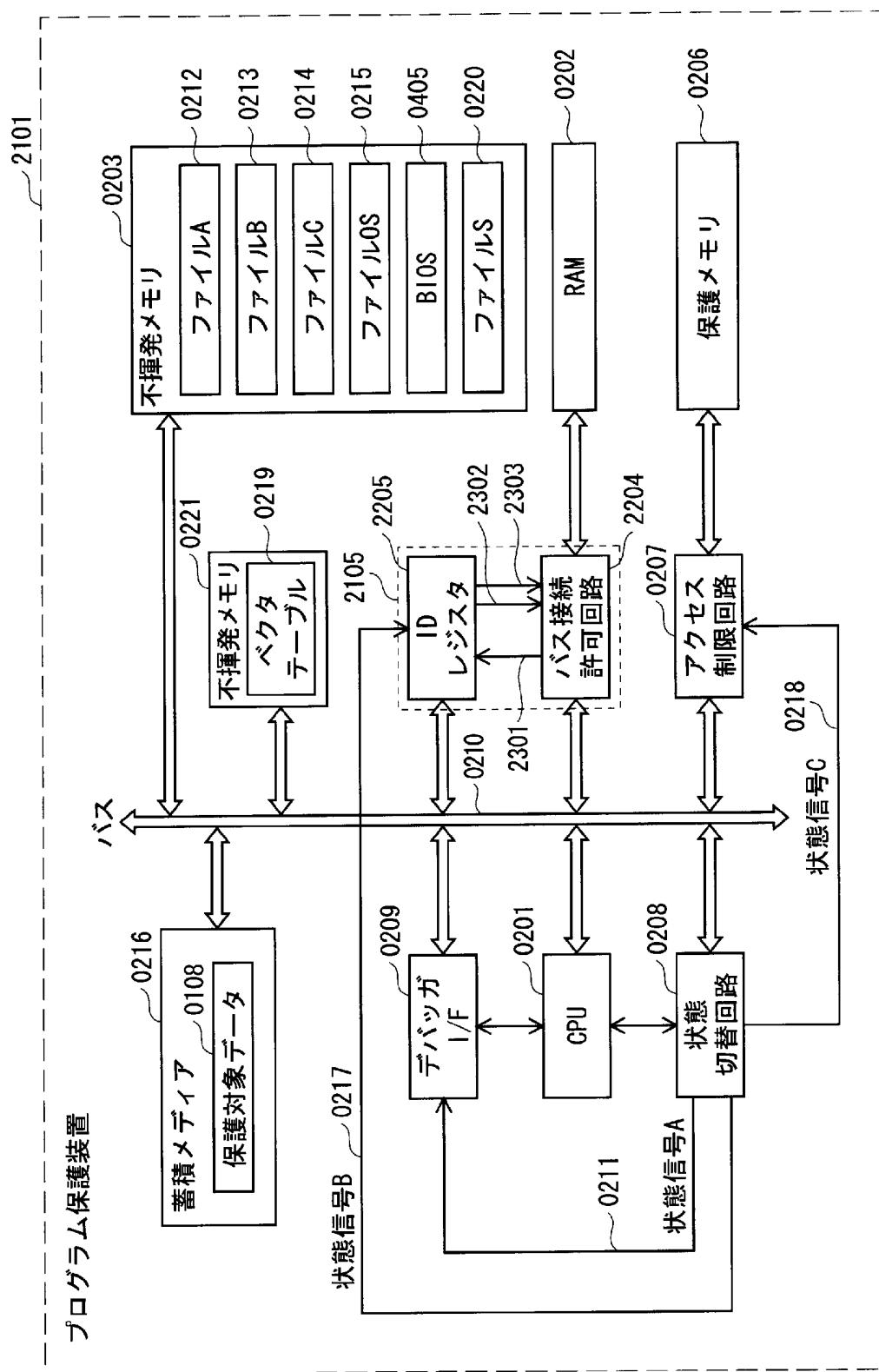
[図20]



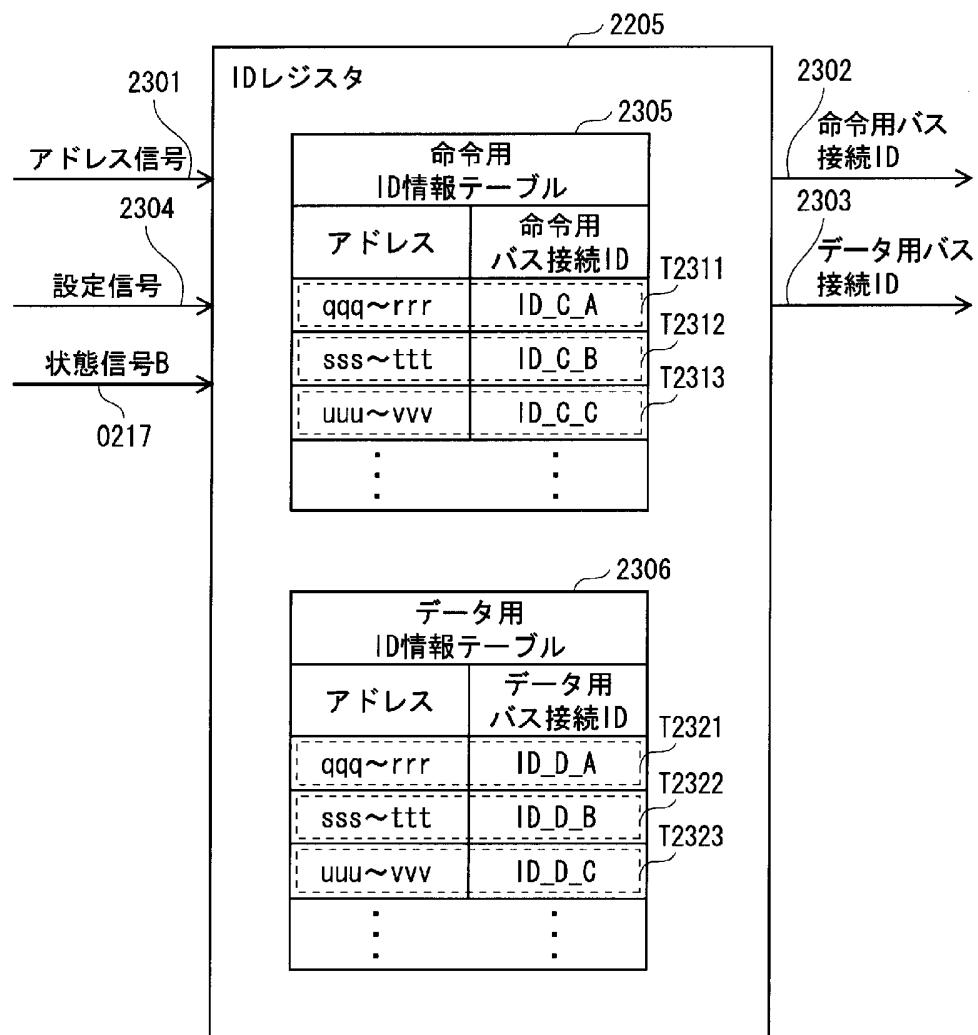
[図21]



[図22]



[図23]



**INTERNATIONAL SEARCH REPORT**

International application No.

PCT/JP2006/310584

**A. CLASSIFICATION OF SUBJECT MATTER**

*G06F21/22(2006.01)i, G06F12/14(2006.01)i, G06F21/24(2006.01)i, G09C1/00 (2006.01)i, H04L9/14(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)  
*G06F21/22, G06F12/14, G06F21/24, G09C1/00, H04L9/14*

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

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2006
Kokai Jitsuyo Shinan Koho	1971-2006	Toroku Jitsuyo Shinan Koho	1994-2006

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

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2002-202720 A (Toshiba Corp.), 19 July, 2002 (19.07.02), Full text; all drawings & US 2003/0126458 A1 & EP 1220079 A2	1-14
A	JP 2001-337864 A (Hitachi, Ltd.), 07 December, 2001 (07.12.01), Abstract & US 2001/0025311 A1	1-14
A	JP 2004-199693 A (Texas Instruments Inc.), 15 July, 2004 (15.07.04), Abstract & US 2003/0140205 A1 & US 2003/0140244 A1 & US 2003/0140245 A1 & EP 1331539 A2 & EP 1329787 A2	1-14

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  
 07 August, 2006 (07.08.06)

Date of mailing of the international search report  
 15 August, 2006 (15.08.06)

Name and mailing address of the ISA/  
 Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

**INTERNATIONAL SEARCH REPORT**

International application No.

PCT/JP2006/310584

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2004-288155 A (ARM Ltd.) , 14 October, 2004 (14.10.04) , <b>Abstract</b> & WO 2004/046924 A1 <b>Abstract</b>	1 - 14

## A. 発明の属する分野の分類（国際特許分類（IPC））

Int.Cl. G06F21/22(2006.01)i, G06F12/14(2006.01)i, G06F21/24(2006.01)i, G09C1/00(2006.01)i, H04L9/14(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. G06F21/22, G06F12/14, G06F21/24, G09C1/00, H04L9/14

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	1971-2006年
日本国実用新案登録公報	1996-2006年
日本国登録実用新案公報	1994-2006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）

## 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 2002-202720 A (株式会社東芝) 2002.07.19, 全文, 全図 & US 2003/0126458 A1 & EP 1220079 A2	1-14
A	JP 2001-337864 A (株式会社日立製作所) 2001.12.07, 要約 & US 2001/0025311 A1	1-14
A	JP 2004-199693 A (テキサス インスツルメンツ インコーポレイ テッド) 2004.07.15, 要約 & US 2003/0140205 A1 & US 2003/0140244 A1 & US 2003/0140245 A1 & EP 1331539 A2 & EP 1329787 A2	1-14
A	JP 2004-288155 A (エイアールエム リミテッド) 2004.10.14, 要 約 & WO 2004/046924 A1, abstract	1-14

□ 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」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「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

07.08.2006

国際調査報告の発送日

15.08.2006

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）

5 S 9071

平井 誠

電話番号 03-3581-1101 内線 3546