(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5973583号
(P5973583)
(45)発行日　平成28年8月23日(2016.8.23)　(24)登録日　平成28年7月22日(2016.7.22)

(51)Int.Cl.　F I
G06F 21/57 (2013.01)　G06F 21/57

請求項の数 21　(全 15 頁)

(21)出願番号	特願2014-537150 (P2014-537150)
(86)(22)出願日	平成24年10月16日 (2012.10.16)
(65)公表番号	特表2014-531088 (P2014-531088A)
(43)公表日	平成26年11月20日 (2014.11.20)
(86)国際出願番号	PCT/US2012/060412
(87)国際公開番号	WO2013/059189
(87)国際公開日	平成25年4月25日 (2013.4.25)
審査請求日	平成27年3月11日 (2015.3.11)
(31)優先権主張番号	13/277,063
(32)優先日	平成23年10月19日 (2011.10.19)
(33)優先権主張国	米国(US)

(73)特許権者　502208397
グーグル　インコーポレイテッド
アメリカ合衆国　カリフォルニア州　９４０４３　マウンテン　ビュー　アンフィシアター　パークウェイ　１６００
(74)代理人　110001195
特許業務法人深見特許事務所
(72)発明者　エリック・アール・ノーサップ
アメリカ合衆国・ワシントン・９８１０３・シアトル・ノース・フォーティース・ストリート・１１７

審査官　岸野　徹

最終頁に続く

(54)【発明の名称】コンピュータセキュリティを増強する防御技術

(57)【特許請求の範囲】
【請求項１】
第１の権限レベルに関連付けられた第１の記述子テーブルを初期化するステップと；
第２の記述子テーブルのためにランダムな位置を生成するステップであって、前記ランダムな位置は、オペレーティングシステムカーネルではないソフトウェアプロセスがハードウェアプロセッサに関連付けられたコマンドを使用しても決定できない位置である、ステップと；
前記ランダムな位置で前記第２の記述子テーブルを初期化するステップであって、前記第２の記述子テーブルが、前記第１の権限レベルとは異なる第２の権限レベルに関連付けられ、前記第１の記述子テーブルおよび前記第２の記述子テーブルが、前記ハードウェアプロセッサに関連付けられ、前記オペレーティングシステムカーネルによって初期化され、前記第１の権限レベルが読み取り専用であって、前記第２の権限レベルが読み書きである、ステップと；
記述子テーブルアドレス要求に応答して、前記第１の記述子テーブルに関連付けられたメモリアドレスを提供するステップであって、前記記述子テーブルアドレス要求が、前記ソフトウェアプロセスの少なくとも１つによって提供される、ステップと；
前記少なくとも１つのソフトウェアプロセスによる前記第１の記述子テーブルに対する更新要求に応答して、前記オペレーティングシステムカーネルが前記更新要求が有効または信頼できると決定したことに応答して前記第２の記述子テーブルを更新するステップであって、前記第２の記述子テーブルの前記位置は、前記少なくとも１つのソフトウェアプ

ロセスに公開されない、ステップと；
を備える、コンピュータ実施方法。
【請求項２】
前記第２の記述子テーブルを更新するステップは、前記第１の記述子テーブルを更新させる、請求項１に記載のコンピュータ実施方法。
【請求項３】
前記第１の記述子テーブルおよび前記第２の記述子テーブルは、割り込み記述子テーブルを含む、請求項１または２に記載のコンピュータ実施方法。
【請求項４】
前記第１の記述子テーブルおよび前記第２の記述子テーブルは、グローバル記述子テーブルを含む、請求項１～３のいずれか１項に記載のコンピュータ実施方法。
【請求項５】
前記記述子テーブルアドレス要求は、グローバル記述子テーブル格納命令、または割り込み記述子テーブル格納命令を含む、請求項１～４のいずれか１項に記載のコンピュータ実施方法。
【請求項６】
前記第１の記述子テーブルに含まれるデータは、前記第２の記述子テーブルに含まれるデータと等しい、請求項１～５のいずれか１項に記載のコンピュータ実施方法。
【請求項７】
前記ソフトウェアプロセスは、マルウェアまたはコンピュータウィルスを含む、請求項１～６のいずれか１項に記載のコンピュータ実施方法。
【請求項８】
コンピュータ可読プログラムであって、実行時、
第１の権限レベルに関連付けられた第１の記述子テーブルを初期化するステップと；
第２の記述子テーブルのためにランダムな位置を生成するステップであって、前記ランダムな位置は、オペレーティングシステムカーネルではないソフトウェアプロセスがハードウェアプロセッサに関連付けられたコマンドを使用しても決定できない位置である、ステップと；
前記ランダムな位置で前記第２の記述子テーブルを初期化するステップであって、前記第２の記述子テーブルが、前記第１の権限レベルとは異なる第２の権限レベルに関連付けられ、前記第１の記述子テーブルおよび前記第２の記述子テーブルが、前記ハードウェアプロセッサに関連付けられ、前記オペレーティングシステムカーネルによって初期化され、前記第１の権限レベルが読み取り専用であって、前記第２の権限レベルが読み書きである、ステップと；
記述子テーブルアドレス要求に応答して、前記第１の記述子テーブルに関連付けられたメモリアドレスを提供するステップであって、前記記述子テーブルアドレス要求が、前記ソフトウェアプロセスの少なくとも１つによって提供される、ステップと；
前記少なくとも１つのソフトウェアプロセスによる前記第１の記述子テーブルに対する更新要求に応答して、前記オペレーティングシステムカーネルが前記更新要求が有効または信頼できると決定したことに応答して前記第２の記述子テーブルを更新するステップであって、前記第２の記述子テーブルの前記位置は、前記少なくとも１つのソフトウェアプロセスに公開されない、ステップと；
を含む動作を前記ハードウェアプロセッサに実行させるコンピュータ可読プログラム。
【請求項９】
前記第２の記述子テーブルを更新するステップは、前記第１の記述子テーブルを更新させる、請求項８に記載のコンピュータ可読プログラム。
【請求項１０】
前記第１の記述子テーブルおよび前記第２の記述子テーブルは、割り込み記述子テーブルを含む、請求項８または９に記載のコンピュータ可読プログラム。
【請求項１１】

前記第１の記述子テーブルおよび前記第２の記述子テーブルは、グローバル記述子テーブルを含む、請求項８～１０のいずれか１項に記載のコンピュータ可読プログラム。
【請求項１２】
前記記述子テーブルアドレス要求は、グローバル記述子テーブル格納命令、または割り込み記述子テーブル格納命令を含む、請求項８～１１のいずれか１項に記載のコンピュータ可読プログラム。
【請求項１３】
前記第１の記述子テーブルに含まれるデータは、前記第２の記述子テーブルに含まれるデータと等しい、請求項８～１２のいずれか１項に記載のコンピュータ可読プログラム。
【請求項１４】
前記ソフトウェアプロセスが、マルウェアまたはコンピュータウィルスを含む、請求項８に記載のコンピュータ可読プログラム。
【請求項１５】
データを記憶するためのメモリと；
第１の権限レベルに関連付けられた第１の記述子テーブルを初期化するステップと、
第２の記述子テーブルのためにランダムな位置を生成するステップであって、前記ランダムな位置は、オペレーティングシステムカーネルではないソフトウェアプロセスが１つまたは複数のハードウェアプロセッサに関連付けられたコマンドを使用しても決定できない位置である、ステップと、
前記ランダムな位置で前記第２の記述子テーブルを初期化するステップであって、前記第２の記述子テーブルが、前記第１の権限レベルとは異なる第２の権限レベルに関連付けられ、前記第１の記述子テーブルおよび前記第２の記述子テーブルが、前記１つまたは複数のハードウェアプロセッサに関連付けられ、オペレーティングシステムカーネルによって初期化され、前記第１の権限レベルが読み取り専用であって、前記第２の権限レベルが読み書きである、ステップと、
記述子テーブルアドレス要求に応答して、前記第１の記述子テーブルに関連付けられたメモリアドレスを提供するステップであって、前記記述子テーブルアドレス要求が、ソフトウェアプロセスの少なくとも１つによって提供される、ステップと、
前記少なくとも１つのソフトウェアプロセスによる前記第１の記述子テーブルに対する更新要求に応答して、前記オペレーティングシステムカーネルが前記更新要求が有効または信頼できると決定したことに応答して前記第２の記述子テーブルを更新するステップであって、前記第２の記述子テーブルの前記位置は、前記少なくとも１つのソフトウェアプロセスに公開されない、ステップと、
を含む動作を実行するように動作可能な１つまたは複数のハードウェアプロセッサと；
を備える、システム。
【請求項１６】
前記第２の記述子テーブルを更新するステップは、前記第１の記述子テーブルを更新させる、請求項１５に記載のシステム。
【請求項１７】
前記第１の記述子テーブルおよび前記第２の記述子テーブルは、割り込み記述子テーブルを含む、請求項１５または１６に記載のシステム。
【請求項１８】
前記第１の記述子テーブルおよび前記第２の記述子テーブルは、グローバル記述子テーブルを含む、請求項１５～１７のいずれか１項に記載のシステム。
【請求項１９】
前記記述子テーブルアドレス要求は、グローバル記述子テーブル格納命令、または割り込み記述子テーブル格納命令を含む、請求項１５～１８のいずれか１項に記載のシステム。
【請求項２０】
前記第１の記述子テーブルに含まれるデータは、前記第２の記述子テーブルに含まれる

データと等しい、請求項１５～１９のいずれか１項に記載のシステム。
【請求項２１】
前記ソフトウェアプロセスは、マルウェアまたはコンピュータウィルスを含む、請求項１５～２０のいずれか１項に記載のシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
本明細書は、コンピュータセキュリティに関する。
【背景技術】
【０００２】
コンピュータシステムは、敵対的なソフトウェアアプリケーションまたはプロセス(例えば、マルウェア、ウィルスなど)によって危険にさらされる可能性がある。敵対的なソフトウェアアプリケーションは、オペレーティングシステムカーネルに、敵対的なソフトウェアアプリケーションによって指定されるメモリ位置にデータを書き込ませる。例えば、敵対的なソフトウェアアプリケーションは、オペレーティングシステムに関連する欠陥および/または脆弱性を悪用することができ、オペレーティングシステムカーネルに、カーネルに関連する命令を変更させる(例えば、ユーザもしくは他のソフトウェアがセキュリティ対策を回避することを可能にする、または、ユーザまたはソフトウェアの不正アクセスを許可するバックドアを挿入する)ことができる。別の例として、敵対的なソフトウェアアプリケーションは、オペレーティングシステムカーネルに、中央処理装置(CPU)またはオペレーティングシステムによって使用される様々なデータ構造またはテーブル(例えば、割り込み記述子テーブル、グローバル記述子テーブルなど)に格納されたデータを変更させることができる。加えて、敵対的なソフトウェアアプリケーションは、CPUに関連するコマンドを使用して、CPUまたはオペレーティングシステムに関連するリソース(例えば、割り込み記述子テーブルまたはグローバル記述子テーブル)の位置を決定するために、オペレーティングシステムに関連する欠陥および/または脆弱性を悪用することができる。例えば、敵対的なソフトウェアアプリケーションは、CPUに割り込み記述子テーブルのアドレスを提供させるために、SIDT命令を使用することができる。
【発明の概要】
【発明が解決しようとする課題】
【０００３】
本明細書は、コンピュータセキュリティを改善するための防御技術に関連する技法を説明する。システムは、記述子テーブル(例えば、割り込み記述子テーブルまたはグローバル記述子テーブル)を初期化することができ、記述子テーブルを異なるメモリ位置にマッピングすることができる。記述子テーブルの1つのマッピングは、読み書き権限に関連付けられてよく、記述子テーブルの第2のマッピングは、読み取り専用権限に関連付けられてよい。システムは、読み取り専用記述子テーブル(例えば、第2のマッピング)のアドレスを、CPUに提供することができる。CPUが、記述子テーブルの値を返すためにコマンドを受信すると、CPUは、読み取り専用記述子テーブルのアドレスを提供することができる。オペレーティングシステムカーネルが、記述子テーブルを更新するために有効な命令(例えば、敵対的なソフトウェアアプリケーションからの命令と対照的に、信頼できるプロセスから、またはオペレーティングシステムからの命令)を受信すると、オペレーティングシステムカーネルは、記述子テーブルにアクセスすることができ、記述子テーブルの値を更新することができる。
【課題を解決するための手段】
【０００４】
全体的に、本明細書に記載の主題の1つの革新的な態様は、第1の記述子テーブル、および記述子テーブルの第2のマッピングを初期化するアクションであって、記述子テーブルの第1のマッピングが、第1の権限レベルに関連付けられ、記述子テーブルの第2のマッピングが、第1の権限レベルとは異なる第2の権限レベルに関連付けられ、第1の記述子テー

ブルおよび第2の記述子テーブルが、ハードウェアプロセッサに関連付けられ、オペレーティングシステムカーネルによって初期化されるアクションと、記述子テーブルアドレス要求に応答して、第1の記述子テーブルに関連付けられたメモリアドレスを提供するアクションであって、記述子テーブル要求が、ソフトウェアプロセスによって提供されるアクションと、更新要求に応答して、第2の記述子テーブルを更新するアクションとを含む方法で具体化されてよい。

【０００５】

本明細書に記載の主題の別の革新的な態様は、記述子テーブルを初期化するアクションであって、記述子テーブルが、オペレーティングシステムカーネルによって初期化され、ハードウェアプロセッサに関連付けられるアクションと、記述子テーブルに関連付けられた権限レベルを第1の権限レベルに変更するアクションと、更新要求に応答して、記述子テーブルに関連付けられた権限レベルを第2の権限レベルに変更するアクションであって、第2の権限レベルが、第1の権限レベルよりも高いアクションと、記述子テーブルが第2の権限レベルに関連付けられている間に、記述子テーブルを更新するアクションであって、更新要求に基づくアクションと、記述子テーブルを更新した後に、記述子テーブルに関連付けられた権限レベルを第1の権限レベルに変更するアクションであって、オペレーティングシステムカーネルが、記述子テーブルに関連付けられた権限レベルを変更するステップとを含む方法で具体化されてよい。

【０００６】

本明細書に記載の主題の特定の実施形態は、以下の利点の1つまたは複数の実現するように実施され得る。例えば、ネットワークおよびコンピュータセキュリティは、敵対的なソフトウェアアプリケーションまたはマルウェアがCPUおよび/またはOSカーネルによって使用されるデータ構造(例えば、割り込み記述子テーブルおよびグローバル記述子テーブル)にアクセスすること、またはこれを変更することを防止することによって、増強され得る。加えて、オペレーティングシステムは、記述子テーブルの意図しない上書きが低減または防止され得るため、より容易にデバッグされ得る。

【０００７】

本明細書に記載の主題の1つまたは複数の実施形態の詳細は、添付図面および以下の説明に記載される。主題の他の特徴、態様、および利点は、説明、図面、および特許請求の範囲から明らかになるであろう。

【図面の簡単な説明】

【０００８】

【図１】コンピュータセキュリティを改善するための例示的なシステムを示す図である。

【図２】コンピュータセキュリティを改善するための例示的なプロセスのフローチャートである。

【図３】コンピュータセキュリティを改善するための例示的なプロセスのフローチャートである。

【発明を実施するための形態】

【０００９】

様々な図面中の同様の参照番号および名称は、同様の要素を示す。

【００１０】

図1は、コンピュータセキュリティを改善するための例示的なシステム100を示す。システム100は、CPU102、記述子テーブルレジスタ104、記述子テーブル106、記述子テーブルの第1のマッピング107、エイリアス記述子テーブル108、メモリマップ110、オペレーティングシステムカーネル112、およびソフトウェアプロセス114を含む。CPU102は、様々なタイプのコンピュータプロセッサであってよい。例えば、CPU102は、x86プロセッサ、x86互換プロセッサ、またはx86プロセッサの64ビット系列(64 bit descendant) (例えば、Intel Core2またはAMD Opteron)であってよい。他のCPUが使用されてもよい。

【００１１】

CPU102は、関連する記述子テーブル106のメモリアドレスを格納する記述子テーブルレ

ジスタ104(「DTレジスタ」)を含むことができる。例えば、CPU102は、割り込み記述子テーブルのメモリアドレスを格納する割り込み記述子テーブルレジスタを含むことができる。図1は、単一のDTレジスタ104を示しているが、CPU102は、様々な記述子テーブル106に対応する複数のDTレジスタ104を含むことができる。例えば、割り込み記述子テーブルレジスタに加えて、CPU102は、グローバル記述子テーブルに関連付けられたメモリアドレスを格納するグローバル記述子テーブルレジスタを含むことができる。DTレジスタ104は、物理メモリアドレスまたは仮想メモリアドレスを格納することができる。

【００１２】

DTレジスタ104に格納される値は、オペレーティングシステムカーネル112によってプログラムされ得る。例えば、システム100の初期化中(例えば、ブート時)、オペレーティングシステムカーネル112は、エイリアス記述子テーブル108に関連付けられたメモリアドレス(例えば、仮想メモリアドレス)を格納することができる。いくつかの実施形態では、DTレジスタ104に格納される値は、初期化以外のときにプログラムされてよい。

【００１３】

メモリマップ110は、どのようにメモリが編成されるかを記述する、CPU102に関連付けられたメモリ管理モジュール(例えば、仮想メモリマップ)であってよい。例えば、メモリマップ110は、メモリサイズ、オペレーティングシステムの使用のために予約されたメモリの領域、および/または、ソフトウェアプロセス114によって使用またはアクセスされ得るメモリの領域を記述する情報を含むことができる。加えて、メモリマップ110は、メモリアドレスが、読み取り専用権限または読み書き権限のどちらに関連付けられているのかを指定するために使用されてよい。例えば、オペレーティングシステムカーネル112は、記述子テーブル106またはエイリアス記述子テーブル108に関連付けられた権限を変更するために、メモリマップ110を変更することができる。加えて、メモリマップ110は、論理/仮想メモリアドレスを物理メモリアドレスに翻訳するために、CPU102、またはCPU102に関連付けられたメモリマネージャによって使用されてよい。

【００１４】

記述子テーブル106は、例えば、様々なソフトウェアルーチンまたはデータ構造に関連付けられたメモリアドレス、メモリセグメント記述子、CPUに関連付けられた特権レベル(例えば、「コールゲート」)を変更するためのメカニズム、および他のデータを含むことができる。例えば、記述子テーブル106は、割り込みベクタテーブルを実装するために使用され得る割り込み記述子テーブルであってよい。いくつかの実施形態では、割り込み記述子テーブルは、割り込みハンドラに関連付けられたメモリアドレスを含み、割り込みハンドラは、割り込み(例えば、ハードウェア割り込み、ソフトウェア割り込み、および/またはプロセッサ例外(まとめて「割り込み」と呼ばれる))を、それらがトリガされるときに処理するソフトウェアプロセスまたはルーチンであってよい。例えば、割り込み記述子テーブルは、タイマ割り込みに対応するテーブル内の位置に、割り込みハンドラ(T0_Int_Handler)に関連付けられたメモリアドレスを格納することができる。タイマ割り込みがトリガされると、オペレーティングシステムは、割り込み記述子テーブルにアクセスすることができ、T0_Int_Handlerがタイマ割り込みに応答して実行されるべきであることを決定する。

【００１５】

メモリマップ110を使用して、記述子テーブル106は、様々な権限レベルに関連付けられ得る。例えば、記述子テーブル106は、読み取り専用権限を有することができ、読み取り専用権限は、記述子テーブル106および記述子テーブル106に格納された値が変更されるのを防止する。加えて、記述子テーブル106は、読み書き権限を有することができ、読み書き権限は、記述子テーブル106および記述子テーブル106に格納された値が変更されることを許可する。記述子テーブル106に関連付けられた権限レベルは、オペレーティングシステムカーネル112によって変更され得る。例えば、オペレーティングシステムカーネル112は、記述子テーブル106の権限を読み書きから読み取り専用に変更するために、メモリマップ110を使用することができる。

【００１６】
記述子テーブル106は、様々な物理メモリアドレスに配置されてよい。例えば、記述子テーブル106は、オペレーティングシステムカーネル112またはCPU102によって、ランダムなメモリアドレスに作成されてよい。加えて、記述子テーブル106は、固定されたメモリアドレスに作成されてよい。加えて、記述子テーブル106は、メモリマップ110によって、物理メモリ位置から仮想メモリ位置にマッピングされてよい(例えば、マップ記述子テーブル107)。マップ記述子テーブル107は、記述子テーブル106に戻って指すことができ、マップ記述子テーブル107に含まれる値は、記述子テーブル106に含まれる値を反映することができる。例えば、記述子テーブル106に含まれる値が変更された場合、マップ記述子テーブル107も、変更された値を反映するように更新される。

【００１７】
記述子テーブル106は、メモリマップ110を使用して、第2のアドレスにマッピングされてよい(例えば、エイリアス記述子テーブル108)。例えば、記述子テーブル106は、記述子テーブル106に関連付けられた物理メモリアドレスを指す第2の仮想アドレスにマッピングされてよい。マップ記述子テーブル107と同様に、エイリアス記述子テーブル108に含まれる値は、記述子テーブル106(および、マップ記述子テーブル107)に含まれる値を反映することができる。

【００１８】
記述子テーブル106、マップ記述子テーブル107、およびエイリアス記述子テーブル108は、異なる権限に関連付けられてよい。例えば、記述子テーブル106およびマップ記述子テーブル107は、読み書き権限に関連付けられてよく、エイリアス記述子テーブル108は、読み取り専用権限に関連付けられてよい。加えて、記述子テーブル106、マップ記述子テーブル107、およびエイリアス記述子テーブル108に関連付けられた権限レベルは、オペレーティングシステムカーネル112によって変更されてよい。例えば、オペレーティングシステムカーネル112は、エイリアス記述子テーブル108に関連付けられた権限レベルを読み取り専用であるように設定することができ、記述子テーブル106に関連付けられた権限レベルを読み書きであるように設定することができる。エイリアス記述子テーブル108は、CPUおよび/またはオペレーティングシステムカーネル112によってアクセスされ得る。いくつかの実施では、システム100は、マップ記述子テーブル107および/またはエイリアス記述子テーブル108を含まない。

【００１９】
CPU102は、記述子テーブル106のメモリアドレスを提供させる命令を含むことができる。例えば、CPU102は、DTレジスタ104に格納された値を返させる命令(例えば、SDT命令)を含むことができる。いくつかの実施形態では、SDT命令は、割り込み記述子テーブルに関連付けられたメモリアドレスを返す割り込み記述子テーブル格納命令(Store Interrupt Descriptor Table instruction)(SIDT)、または、グローバル記述子テーブルに関連付けられたメモリアドレスを返すグローバル記述子テーブル格納命令(Store Global Descriptor Table instruction)(SGDT)であってよい。命令は、オペレーティングシステムカーネル112によって使用されてよい。ソフトウェアアプリケーションまたはプロセス114は、オペレーティングシステム内の欠陥または脆弱性を悪用する可能性があり、オペレーティングシステムカーネル112にSDT命令を発行させる可能性がある。

【００２０】
オペレーティングシステムカーネル112は、任意の適切なタイプのオペレーティングシステムカーネルであってよい。オペレーティングシステムカーネル112は、CPUのリソース、および/または、システム100に関連する他のハードウェアリソースを管理することができる。オペレーティングシステムカーネル112は、システム100上で実行されるソフトウェアプロセス114と相互作用することができる。例えば、オペレーティングシステムカーネル112は、ソフトウェアプロセス112から命令を受信することができ、ソフトウェアプロセス114の代わりに、CPU102、および/または、システム100に関連するハードウェアリソースと相互作用することができる(例えば、データポートまたは周辺デバイスとデータを交

換することができる)。

【００２１】

ソフトウェアプロセス114は、オペレーティングシステムカーネル112と相互作用する1つまたは複数のソフトウェアアプリケーションまたはプロセスであってよい。いくつかの実施形態では、ソフトウェアプロセス114は、CPU102に、記述子テーブル106に関連付けられたメモリアドレスを提供させることができる。例えば、ソフトウェアプロセス114は、CPU102に、割り込み記述子テーブルに関連付けられたDTレジスタ104に格納された値を返させるために、SIDT命令を使用する。

【００２２】

図2は、コンピュータセキュリティを改善するための例示的なプロセス200のフローチャートである。プロセス200は、(202で)記述子テーブルを生成し、初期化することによって開始する。例えば、CPU102が(例えば、ブート時に)初期化されると、オペレーティングシステムカーネル112、または、オペレーティングシステムカーネル112に関連するファームウェアは、記述子テーブル106を作成し、初期化することができる。ファームウェアまたはオペレーティングシステムカーネル112は、割り込みがトリガされると実行されるソフトウェアルーチン(例えば、「割り込みハンドラ」)に関連付けられたメモリ位置を含めるために、記述子テーブル106の値を更新する。オペレーティングシステムカーネル112は、記述子テーブル106を、第1の仮想メモリアドレス(例えば、マップ記述子テーブル107)にマッピングすることができる。オペレーティングシステムカーネル112は、初期化された記述子テーブル116の第2のマッピング(例えば、エイリアス記述子テーブル108)を作成することができる。オペレーティングシステムカーネル112は、マップ記述子テーブル107およびエイリアス記述子テーブル108を、異なる仮想メモリアドレスに配置することができる。例えば、オペレーティングシステムカーネルは、マップ記述子テーブル107を第1の仮想メモリアドレスに配置するようメモリマップ110を使用することができ、エイリアス記述子テーブル108を、第1の仮想メモリアドレスとは異なる第2の仮想メモリアドレスにマッピングするようメモリマップ110を使用することができる。いくつかの実施形態では、オペレーティングシステムカーネル112は、マップ記述子テーブル107およびエイリアス記述子テーブル108を、ランダムなメモリ位置に作成する。いくつかの実施形態では、マップ記述子テーブル107は、含まれず、使用されない。

【００２３】

記述子テーブルに関連付けられた権限レベルは、(203で)更新される。例えば、オペレーティングシステムカーネル112は、エイリアス記述子テーブル108に関連付けられた権限レベルを、読み取り専用であるように設定することができ、記述子テーブル106およびマップ記述子テーブル107に関連付けられた権限レベルを、読み書きであるように設定することができる。いくつかの実施形態では、オペレーティングシステムカーネル112は、記述子テーブル106、マップ記述子テーブル107、およびエイリアス記述子テーブル108に関連付けられた権限レベルを、メモリマップ110を使用して設定する。

【００２４】

オペレーティングシステムカーネルは、(204で)DTレジスタを更新する。例えば、オペレーティングシステムカーネル112は、エイリアス記述子テーブル108に関連付けられたメモリアドレス(例えば、エイリアス記述子テーブル108に関連付けられた仮想メモリアドレス)を格納するために、DTレジスタ104を更新することができる。

【００２５】

プロセス200は、(206で)記述子テーブルに関連付けられたメモリアドレスを返すための命令を受信することによって継続することができる。例えば、CPU102は、オペレーティングシステムカーネル112またはソフトウェアアプリケーション114から、SDT命令を受信することができる。いくつかの実施形態では、SDT命令は、SIDT命令またはSGDT命令である。

【００２６】

命令に応答して、CPUは、(208で)DTレジスタに格納されたメモリアドレスを返す。例え

ば、SDT命令に応答して、CPU102は、204でDTレジスタ104に格納されたエイリアス記述子テーブル108に関連付けられたメモリアドレスを供給することができる。エイリアス記述子テーブル108のメモリアドレスは、CPU102によって返されるが、敵対的なソフトウェアアプリケーション114は、エイリアス記述子テーブル108が読み取り専用権限に関連付けられているため、この情報を悪用することができない。敵対的なソフトウェアアプリケーション114が、記述子テーブル106にデータを書き込むために、208で返されたエイリアス記述子テーブル108のメモリアドレスを使用することを試みる場合、オペレーティングシステムカーネル112またはメモリマップ110は、エラー(例えば、権限違反)を生成し、敵対的なソフトウェアアプリケーションがデータを記述子テーブル106に書き込むのを防止する。したがって、敵対的なソフトウェアアプリケーションは、記述子テーブル106の値または内容を変更することができない。

【００２７】

代わりに、プロセス200は、(210で)記述子テーブルに格納されたデータを更新するための命令を受信することができる。例えば、オペレーティングシステムカーネル112は、記述子テーブル106が更新されるべきであるという命令を受信することができる。いくつかの実施形態では、オペレーティングシステムカーネル112は、オペレーティングシステム機能(例えば、ハードウェアマネージャ)から、記述子テーブルを更新するための命令を受信することができる。

【００２８】

命令に応答して、オペレーティングシステムカーネルは、(212で)記述子テーブルを更新することができる。例えば、オペレーティングシステムカーネル112は、読み書き権限に関連付けられたマップ記述子テーブル107にアクセスすることができ、マップ記述子テーブル107内の特定のエントリに関連付けられた値を更新することができる。マップ記述子テーブル107は、記述子テーブル106のマッピングであるため、記述子テーブル106およびエイリアス記述子テーブル108に含まれた値は、更新される。いくつかの実施形態では、オペレーティングシステムカーネル112は、記述子テーブル106にアクセスし、記述子テーブル106内の値を更新する。

【００２９】

図3は、コンピュータセキュリティを改善するための例示的なプロセス300のフローチャートである。プロセス300は、(302で)記述子テーブルを初期化することによって開始する。例えば、オペレーティングシステムカーネル112は、記述子テーブル106(例えば、割り込み記述子テーブルまたはグローバル記述子テーブル)を作成することができ、適切なデータ値(例えば、割り込みハンドラに関連付けられたメモリアドレス、または、様々なメモリセグメントに関連付けられた特性)を含めるために、記述子テーブル106を初期化することができる。いくつかの実施形態では、オペレーティングシステムカーネル112は、ブート時に記述子テーブル106を初期化する。オペレーティングシステムカーネル112は、記述子テーブル106に関連付けられた権限を、読み取り専用であるように変更することができる。

【００３０】

オペレーティングシステムカーネル112は、(303で)DTレジスタを更新することができる。例えば、オペレーティングシステムカーネル112は、記述子テーブル106に関連付けられたメモリアドレスを、DTレジスタ104内に格納することができる。

【００３１】

プロセス300は、(304で)記述子テーブルに関連付けられたメモリアドレスを提供するための命令を受信することによって継続することができる。例えば、CPU102は、オペレーティングシステムカーネル112またはソフトウェアアプリケーション114からSDT命令を受信することができる。いくつかの実施形態では、SDT命令は、SIDT命令またはSGDT命令である。命令に応答して、CPUは、(306で)DTレジスタに格納されたメモリアドレス(例えば、記述子テーブル106のメモリアドレス)を返す。記述子テーブル106のメモリアドレスは、CPU102によって返されるが、敵対的なソフトウェアアプリケーション114は、記述子テーブ

ル106が読み取り専用権限に関連付けられているため、この情報を悪用することができない。敵対的なソフトウェアアプリケーション114が、記述子テーブル106にデータを書き込むことを試みる場合、オペレーティングシステムカーネル112またはメモリマップ110は、権限違反を生成する。したがって、敵対的なソフトウェアアプリケーションは、記述子テーブル106の値または内容を変更することができない。

【００３２】

代わりに、プロセス300は、(308で)記述子テーブルに格納されたデータを更新するための命令を受信することができる。例えば、オペレーティングシステムカーネル112は、記述子テーブル106が更新されるべきであるという命令を受信することができる。いくつかの実施形態では、オペレーティングシステムカーネル112は、オペレーティングシステム機能(例えば、ハードウェアマネージャ)から命令を受信することができる。

【００３３】

命令に応答して、オペレーティングシステムカーネルは、(310で)記述子テーブルに関連付けられた権限レベルを変更することができる。例えば、オペレーティングシステムカーネル112は、記述子テーブル106に関連付けられた権限レベルを、読み取り専用から読み書きに変更することができる。

【００３４】

記述子テーブルに関連付けられた権限レベルが更新された後、記述子テーブルは、(312で)更新されてよい。例えば、オペレーティングシステムカーネル112は、記述子テーブル106内の特定のエントリに関連付けられた値を更新することができる。記述子テーブルが更新された後、記述子テーブルに関連付けられた権限レベルは、(314で)変更されてよい。例えば、記述子テーブル106が、新しい値を含むように更新された後、オペレーティングシステムカーネルは、記述子テーブルに関連付けられた権限レベルを、読み取り専用であるように変更することができる。

【００３５】

本明細書に記載の主題および動作の実施形態は、本明細書で開示される構造およびそれらの構造的等価物を含む、デジタル回路網で、もしくは、コンピュータソフトウェア、ファームウェア、もしくはハードウェアで、または、それらの1つもしくは複数の組み合わせで実現されてよい。本明細書に記載の主題の実施形態は、1つまたは複数のコンピュータプログラムとして、すなわち、データ処理装置によって実行するための、または、データ処理装置の動作を制御するための、コンピュータ記憶媒体上に符号化されたコンピュータプログラム命令の1つまたは複数のモジュールとして実施されてよい。代わりに、または加えて、プログラム命令は、データ処理装置によって実行するための適切な受信装置に伝送するための情報を符号化するために生成された、人工的に生成された伝播信号、例えば、機械生成された電気、光、または電磁信号上に符号化されてよい。コンピュータ記憶媒体は、コンピュータ可読記憶媒体、コンピュータ可読記憶基板、ランダムまたはシリアルアクセスメモリアレイもしくはデバイス、または、それらの1つもしくは複数の組み合わせであってよく、または、それらに含まれてよい。さらに、コンピュータ記憶媒体は、伝播信号ではないが、コンピュータ記憶媒体は、人工的に生成された伝播信号内に符号化されたコンピュータプログラム命令の発信元または宛先であってよい。コンピュータ記憶媒体は、また、1つまたは複数の別個の物理的構成要素または媒体(例えば、複数のCD、ディスク、または他の記憶デバイス)であってよく、またはそれらに含まれてよい。

【００３６】

本明細書に記載の動作は、1つもしくは複数のコンピュータ可読記憶デバイスに格納された、または、他の発信元から受信したデータに対してデータ処理装置によって実行される動作として実施されてよい。

【００３７】

「データ処理装置」という用語は、例として、プログラム可能プロセッサ、コンピュータ、システムオンチップ、または、上記の複数もしくは組み合わせを含む、データを処理するためのすべての種類の装置、デバイス、および機械を包含する。装置は、特定目的の

論理回路網、例えば、FPGA(フィールドプログラマブルゲートアレイ)またはASIC(特定用途向け集積回路)を含むことができる。装置は、ハードウェアに加えて、問題のコンピュータプログラムのための実行環境を作成するコード、例えば、プロセッサファームウェア、プロトコルスタック、データベース管理システム、オペレーティングシステム、クロスプラットフォーム実行時環境、仮想マシン、または、それらの1つもしくは複数の組み合わせを構成するコードを含むこともできる。装置および実行環境は、ウェブサービス、分散コンピューティングおよびグリッドコンピューティングインフラストラクチャのような、様々な異なるコンピューティングモデルインフラストラクチャを実現することができる。

【００３８】

(プログラム、ソフトウェア、ソフトウェアアプリケーション、スクリプト、またはコードとしても知られる)コンピュータプログラムは、コンパイルされたまたは翻訳された言語、宣言型または手続き型言語を含む、任意の形式のプログラミング言語で書かれてよく、スタンドアロンプログラムとして、または、モジュール、構成要素、サブルーチン、オブジェクト、もしくは、コンピューティング環境で使用するのに適した他のユニットとして、を含む、任意の形態で展開されてよい。コンピュータプログラムは、ファイルシステム内のファイルに対応してもよいが、対応する必要はない。プログラムは、他のプログラムまたはデータを保持するファイルの一部(例えばマークアップ言語文書に格納された1つまたは複数のスクリプト)内に、問題のプログラム専用の単一のファイル内に、または、複数の連携ファイル(例えば、1つもしくは複数のモジュール、サブプログラム、もしくはコードの一部を格納するファイル)内に格納されてよい。コンピュータプログラムは、1つのコンピュータ上で、または、1つのサイトに配置される、もしくは、複数のサイトにわたって分散され、通信ネットワークによって相互接続される複数のコンピュータ上で実行されるように展開されてよい。

【００３９】

本明細書に記載のプロセスおよび論理フローは、入力データに対して動作し、出力を生成することによってアクションを実行するために、1つまたは複数のコンピュータプログラムを実行する1つまたは複数のプログラム可能プロセッサによって実行されてよい。プロセスおよび論理フローは、特定目的の論理回路網、例えば、FPGA(フィールドプログラマブルゲートアレイ)またはASIC(特定用途向け集積回路)によって実行されてもよく、装置は、このような特定目的の論理回路網として実施されてよもよい。

【００４０】

コンピュータプログラムの実行に適したプロセッサは、例として、汎用および専用マイクロプロセッサの両方、ならびに、任意の種類のデジタルコンピュータの任意の1つまたは複数のプロセッサを含む。一般に、プロセッサは、読み取り専用メモリもしくはランダムアクセスメモリ、またはその両方から、命令およびデータを受信することになる。コンピュータの必須要素は、命令にしたがってアクションを実行するためのプロセッサ、ならびに、命令およびデータを格納するための1つまたは複数のメモリデバイスである。一般に、コンピュータは、また、データを格納するための1つまたは複数の大容量記憶デバイス、例えば、磁気、光磁気ディスク、または光ディスクを、これらからデータを受信する、もしくはこれらにデータを転送する、またはその両方を行うために、含むことになり、または、これらに作動的に結合されることになる。しかしながら、コンピュータは、このようなデバイスを有する必要はない。さらに、コンピュータは、別のデバイス、例えば、数例を挙げると、携帯電話、パーソナルデジタルアシスタント(PDA)、携帯オーディオもしくはビデオプレイヤ、ゲームコンソール、全地球測位システム(GPS)受信機、または、携帯用記憶デバイス(例えば、ユニバーサルシリアルバス(USB)フラッシュドライブ)内に埋め込まれてよい。コンピュータプログラム命令およびデータを格納するのに適したデバイスは、例として、半導体メモリデバイス、例えば、EPROM、EEPROM、およびフラッシュメモリデバイス、磁気ディスク、例えば、内蔵ハードディスクまたはリムーバブルディスク、光磁気ディスク、ならびに、CD-ROMおよびDVD-ROMディスクを含む、すべての形態の

不揮発性メモリ、媒体、およびメモリデバイスを含む。プロセッサおよびメモリは、特定目的の論理回路網によって補足されてよく、または、特定目的の論理回路網に組み込まれてよい。

【００４１】

ユーザとの対話を提供するために、本明細書に記載の主題の実施形態は、ユーザに対して情報を表示するためのディスプレイデバイス、例えば、CRT(陰極線管)またはLCD(液晶ディスプレイ)モニタ、ならびに、それによってユーザがコンピュータに入力を提供することができるキーボードおよびポインティングデバイス、例えば、マウスまたはトラックボールを有するコンピュータ上で実施されてよい。同様にユーザとの対話を提供するために、他の種類のデバイスが使用されてよく、例えば、ユーザに提供されるフィードバックは、任意の形態の感覚フィードバック、例えば、視覚フィードバック、聴覚フィードバック、または触覚フィードバックであってよく、ユーザからの入力は、音響、音声、または触覚入力を含む、任意の形態で受信されてよい。加えて、コンピュータは、ユーザによって使用されるデバイスに文書を送信し、デバイスから文書を受信することによって、例えば、ウェブブラウザから受信した要求に応答して、ユーザのクライアントデバイス上のウェブブラウザにウェブページを送信することによって、ユーザと対話することができる。

【００４２】

本明細書に記載の主題の実施形態は、例えば、データサーバとしてバックエンド構成要素を含む、もしくは、例えば、アプリケーションサーバとしてミドルウェア構成要素を含む、または、例えば、クライアントコンピュータとしてフロントエンド構成要素を含む、もしくは、1つもしくは複数のこのようなバックエンド、ミドルウェア、もしくはフロントエンド構成要素の任意の組み合わせを含むコンピューティングシステム内で実施されてよく、クライアントコンピュータは、グラフィカルユーザインタフェースまたはウェブブラウザを有し、グラフィカルユーザインタフェースまたはウェブブラウザを介して、ユーザは、本明細書に記載の主題の実施形態と相互作用することができる。システムの構成要素は、任意の形式または媒体のデジタルデータ通信、例えば、通信ネットワークによって相互接続されてよい。通信ネットワークの例は、ローカルエリアネットワーク(「LAN」)およびワイドエリアネットワーク(「WAN」)、インターネットワーク(例えば、インターネット)、ならびに、ピアツーピアネットワーク(例えば、アドホックピアツーピアネットワーク)を含む。

【００４３】

1つまたは複数のコンピュータのシステムは、動作時にアクションを実行させる、またはシステムにアクションを実行させる、システム上にインストールされたソフトウェア、ファームウェア、ハードウェア、またはそれらの組み合わせを有することによって、特定の動作またはアクションを実行するように構成されてよい。1つまたは複数のコンピュータプログラムは、データ処理装置によって実行されると、装置にアクションを実行させる命令を含むことによって、特定の動作またはアクションを実行するように構成されてよい。

【００４４】

コンピューティングシステムは、クライアントおよびサーバを含むことができる。クライアントおよびサーバは、一般に、互いに離れており、典型的には、通信ネットワークを介して相互作用する。クライアントおよびサーバの関係は、それぞれのコンピュータ上で実行され、互いにクライアント-サーバ関係を有するコンピュータプログラムによって生じる。いくつかの実施形態では、サーバは、(例えば、データを表示させ、クライアントデバイスと対話するユーザからユーザ入力を受信する目的で)データ(例えば、HTMLページ)をクライアントデバイスに送信する。クライアントデバイスで生成されるデータ(例えば、ユーザとの対話の結果)は、サーバでクライアントから受信されてよい。

【００４５】

本明細書は、多くの特定の実施の詳細を含むが、これらは、任意の発明の、または特許請求され得るものの範囲に対する制限として解釈されるべきではなく、特定の発明の特定

の実施形態に固有の特徴の記述として解釈されるべきである。別々の実施形態の文脈で本明細書に記載される特定の特徴は、単一の実施形態で組み合わせて実施されてもよい。逆に、単一の実施形態の文脈で記載される様々な特徴は、複数の実施形態で別々に、または、任意の適切な部分的組み合わせで実施されてもよい。さらに、特徴は、特定の組み合わせで作用するように上述され、そのように当初は特許請求されている場合があるが、特許請求された組み合わせからの1つまたは複数の特徴は、いくつかの場合、組み合わせから削除されてよく、特許請求された組み合わせは、部分的組み合わせ、または部分的組み合わせの変形を対象としてよい。

【００４６】

同様に、動作は、図面中で特定の順序で示されているが、これは、このような動作が図示された特定の順序もしくはシーケンシャルな順序で実行されること、または、所望の結果を達成するために図示されたすべての動作が実行されることを必要とするとして理解されるべきではない。特定の状況では、マルチタスクおよび並列処理が有利であり得る。さらに、上述した実施形態の様々なシステム構成要素の分離は、すべての実施形態でこのような分離を必要とするとして理解されるべきではなく、記載のプログラム構成要素およびシステムは、一般に、単一のソフトウェア製品に一緒に統合されてよく、または、複数のソフトウェア製品にパッケージ化されてよいことが理解されるべきである。

【００４７】

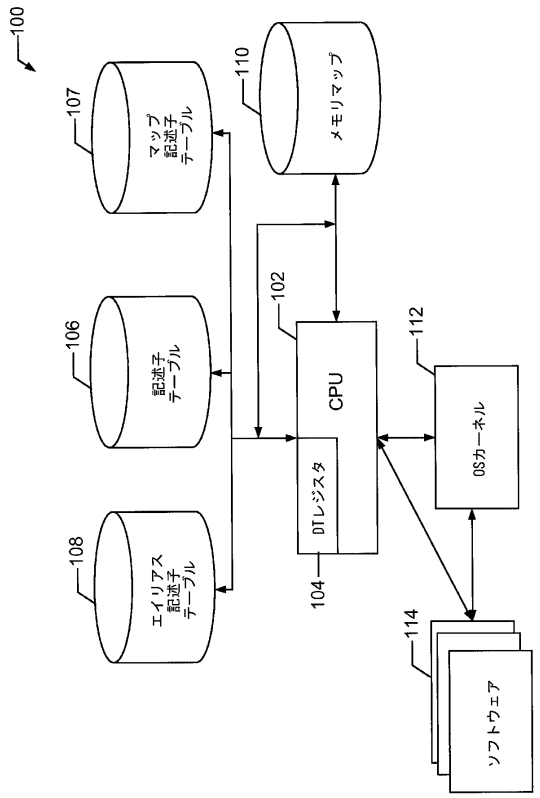
したがって、主題の特定の実施形態を説明してきた。他の実施形態は、以下の特許請求の範囲内である。いくつかの場合、特許請求の範囲に記載のアクションは、異なる順序で実行されてよく、所望の結果を依然として達成することができる。加えて、添付の図面に示されるプロセスは、所望の結果を達成するために、示された特定の順序、またはシーケンシャルな順序を必ずしも必要としない。特定の実施形態では、マルチタスクおよび並列処理が有利であり得る。

【符号の説明】

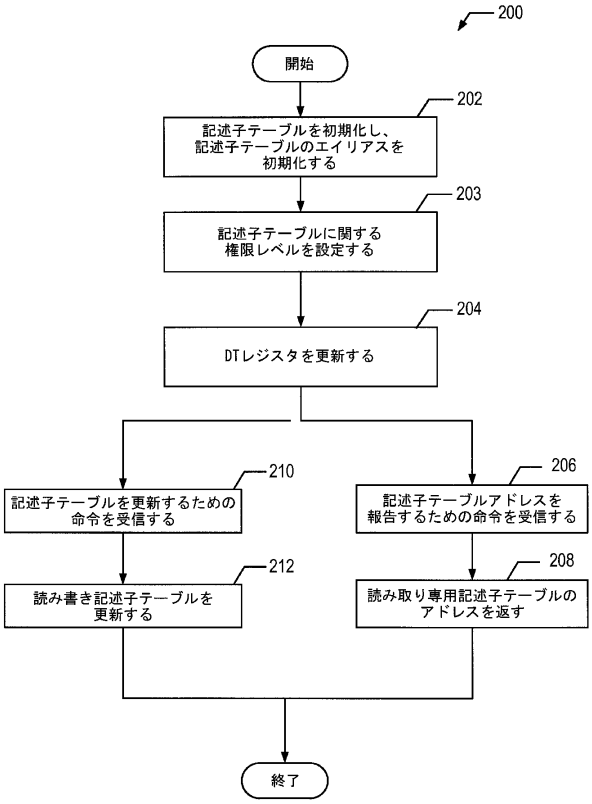
【００４８】

100　システム
102　CPU
104　記述子テーブルレジスタ
106　記述子テーブル
107　記述子テーブルの第1のマッピング
108　エイリアス記述子テーブル
110　メモリマップ
112　オペレーティングシステムカーネル
114　ソフトウェアプロセス

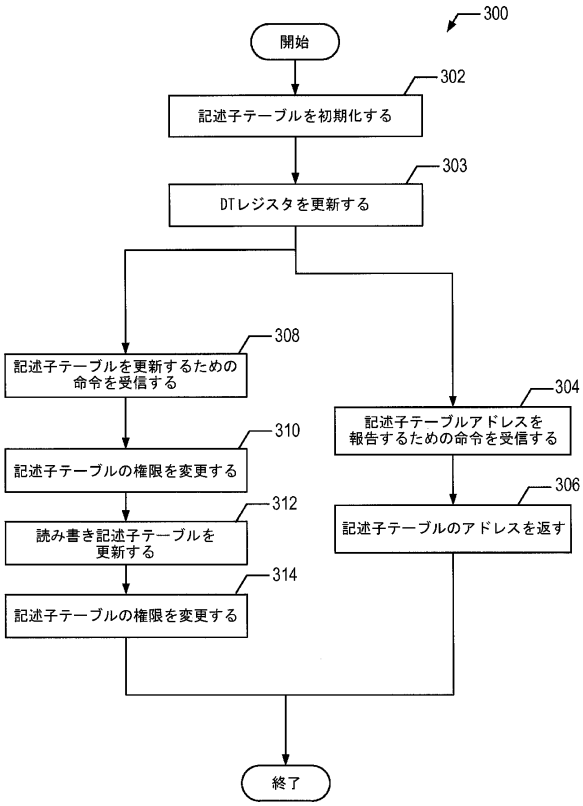
【図１】


100
107
マップ記述子テーブル
110
メモリマップ
102
106
記述子テーブル
CPU
112
OSカーネル
DTレジスタ
108
エイリアス記述子テーブル
104
114
ソフトウェア

【図２】


200
開始
202
記述子テーブルを初期化し、記述子テーブルのエイリアスを初期化する
203
記述子テーブルに関する権限レベルを設定する
204
DTレジスタを更新する
210
記述子テーブルを更新するための命令を受信する
206
記述子テーブルアドレスを報告するための命令を受信する
212
読み書き記述子テーブルを更新する
208
読み取り専用記述子テーブルのアドレスを返す
終了

【図３】


300
開始
302
記述子テーブルを初期化する
303
DTレジスタを更新する
308
記述子テーブルを更新するための命令を受信する
304
記述子テーブルアドレスを報告するための命令を受信する
310
記述子テーブルの権限を変更する
306
記述子テーブルのアドレスを返す
312
読み書き記述子テーブルを更新する
314
記述子テーブルの権限を変更する
終了

フロントページの続き

(56)参考文献 特開２００７－００４６６１（ＪＰ，Ａ）
特開２００５－１２２７１１（ＪＰ，Ａ）
特表２００４－５３１８１９（ＪＰ，Ａ）
特開２０１１－０９０６１２（ＪＰ，Ａ）
特開２００５－０５６４２９（ＪＰ，Ａ）
米国特許出願公開第２０１０／００３１３６０（ＵＳ，Ａ１）
米国特許出願公開第２００７／００６７５９０（ＵＳ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／５７