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

特許第4810608号
(P4810608)

(45)発行日　平成23年11月9日(2011.11.9)　(24)登録日　平成23年8月26日(2011.8.26)

(51)Int.Cl.		F I		
G06F 21/24	(2006.01)	G06F	12/14	560A
G06F 12/00	(2006.01)	G06F	12/14	530P
		G06F	12/00	537A
		G06F	12/00	520G

請求項の数 20　(全 16 頁)

(21)出願番号	特願2009-509446 (P2009-509446)
(86)(22)出願日	平成19年5月14日 (2007.5.14)
(65)公表番号	特表2009-537043 (P2009-537043A)
(43)公表日	平成21年10月22日 (2009.10.22)
(86)国際出願番号	PCT/KR2007/002361
(87)国際公開番号	WO2007/133035
(87)国際公開日	平成19年11月22日 (2007.11.22)
審査請求日	平成20年11月11日 (2008.11.11)
(31)優先権主張番号	60/799,652
(32)優先日	平成18年5月12日 (2006.5.12)
(33)優先権主張国	米国 (US)
(31)優先権主張番号	10-2007-0043573
(32)優先日	平成19年5月4日 (2007.5.4)
(33)優先権主張国	韓国 (KR)

(73)特許権者　503447036
サムスン　エレクトロニクス　カンパニー　リミテッド
大韓民国キョンギ－ド，スウォン－シ，ヨントン－ク，マエタン－ドン　４１６
(74)代理人　100070150
弁理士　伊東　忠彦
(74)代理人　100091214
弁理士　大貫　進介
(74)代理人　100107766
弁理士　伊東　忠重

最終頁に続く

(54)【発明の名称】乱数を用いて権利オブジェクトの保安用ファイル識別子を生成して活用する装置および方法

(57)【特許請求の範囲】

【請求項１】

保存装置から権利オブジェクトを識別するためのファイル識別子のリストを受信する受信部と、

所定の乱数を生成して、前記生成された乱数を前記受信されたファイル識別子の権利オブジェクト識別子に対するハッシュ値と結合して保安用ファイル識別子を生成する保安用ファイル識別子生成部、および

前記生成された保安用ファイル識別子を前記保存装置に伝送する伝送部と、を含む、乱数を用いて権利オブジェクトの保安用ファイル識別子を生成して活用する装置。

【請求項２】

前記保安用ファイル識別子は、固定された長さを有する、請求項１に記載の乱数を用いて権利オブジェクトの保安用ファイル識別子を生成して活用する装置。

【請求項３】

権利オブジェクトを識別するための保安用ファイル識別子リストを生成する保安用ファイル識別子リスト生成部と、

前記保安用ファイル識別子リストに含まれた第１保安用ファイル識別子を代替するための第２保安用ファイル識別子をホストから受信する受信部、および

前記受信した第２保安用ファイル識別子で前記第１保安用ファイル識別子を代替して代替された第２保安用ファイル識別子の権利オブジェクト状態を変更する権利オブジェクト管理部と、を含む、乱数を用いて権利オブジェクトの保安用ファイル識別子を生成して活

用する装置。
【請求項４】
前記保安用ファイル識別子は、前記ホストで生成した所定の乱数と前記権利オブジェクトの権利オブジェクト識別子に対するハッシュ値の結合からなり、固定された長さを有する、請求項３に記載の乱数を用いて権利オブジェクトの保安用ファイル識別子を生成して活用する装置。
【請求項５】
前記権利オブジェクト状態は、活性化状態および非活性化状態のうち何れか１つである、請求項３に記載の乱数を用いて権利オブジェクトの保安用ファイル識別子を生成して活用する装置。
【請求項６】
保安用ファイル識別子リスト生成部は、前記権利オブジェクトの状態が活性化状態である保安用ファイル識別子で前記保安用ファイル識別子リストを生成する、請求項５に記載の乱数を用いて権利オブジェクトの保安用ファイル識別子を生成して活用する装置。
【請求項７】
保安用ファイル識別子リスト生成部は、前記権利オブジェクトの状態が非活性化状態である保安用ファイル識別子で前記保安用ファイル識別子リストを生成する、請求項５に記載の乱数を用いて権利オブジェクトの保安用ファイル識別子を生成して活用する装置。
【請求項８】
前記権利オブジェクト管理部は、前記権利オブジェクトの状態が非活性化である場合、前記保安用ファイル識別子リストから前記ホストのＩＤを参照して前記権利オブジェクトの状態を変更する、請求項７に記載の乱数を用いて権利オブジェクトの保安用ファイル識別子を生成して活用する装置。
【請求項９】
前記保安用ファイル識別子リスト生成部によって生成された前記保安用ファイル識別子リストを前記ホストに伝送する伝送部をさらに含む、請求項３に記載の乱数を用いて権利オブジェクトの保安用ファイル識別子を生成して活用する装置。
【請求項１０】
保存装置から権利オブジェクトを識別するためのファイル識別子のリストを受信部によって受信する受信段階と、
所定の乱数を生成して、前記生成された乱数を前記受信されたファイル識別子の権利オブジェクト識別子に対するハッシュ値と結合して、保安用ファイル識別子を保安用ファイル識別子生成部によって生成する保安用ファイル識別子生成段階、および
前記生成された保安用ファイル識別子を前記保存装置に伝送部によって伝送する伝送段階をと、含む、乱数を用いて権利オブジェクトの保安用ファイル識別子を生成して活用する方法。
【請求項１１】
前記保安用ファイル識別子は、固定された長さを有する、請求項１０に記載の乱数を用いて権利オブジェクトの保安用ファイル識別子を生成して活用する方法。
【請求項１２】
権利オブジェクトを識別するための保安用ファイル識別子リストを保安用ファイル識別子リスト生成部によって生成する保安用ファイル識別子リスト生成段階と、
前記保安用ファイル識別子リストに含まれた第１保安用ファイル識別子を代替するための第２保安用ファイル識別子をホストから受信部によって受信する受信段階、および
前記受信した第２保安用ファイル識別子で前記第１保安用ファイル識別子を代替して、代替された前記第２保安用ファイル識別子の権利オブジェクト状態を権利オブジェクト管理部によって変更する権利オブジェクト管理段階と、を含む、乱数を用いて権利オブジェクトの保安用ファイル識別子を生成して活用する方法。
【請求項１３】
前記第２保安用ファイル識別子は、前記ホストで生成した所定の乱数と前記権利オブジ

ェクトの権利オブジェクト識別子に対するハッシュ値の結合からなり、固定された長さを有する、請求項１２に記載の乱数を用いて権利オブジェクトの保安用ファイル識別子を生成して活用する方法。
【請求項１４】
前記権利オブジェクト状態は、活性化状態および非活性化状態のうち何れか１つである、請求項１２に記載の乱数を用いて権利オブジェクトの保安用ファイル識別子を生成して活用する方法。
【請求項１５】
保安用ファイル識別子リスト生成段階は、前記権利オブジェクトの状態が活性化状態である保安用ファイル識別子で前記保安用ファイル識別子リストを生成する、請求項１４に記載の乱数を用いて権利オブジェクトの保安用ファイル識別子を生成して活用する方法。
【請求項１６】
保安用ファイル識別子リスト生成段階は、前記権利オブジェクトの状態が非活性化状態である保安用ファイル識別子で前記保安用ファイル識別子リストを生成する、請求項１４に記載の乱数を用いて権利オブジェクトの保安用ファイル識別子を生成して活用する方法。
【請求項１７】
前記権利オブジェクト管理段階は、前記権利オブジェクトの状態が非活性化の場合、前記保安用ファイル識別子リストから前記ホストのＩＤを参照して前記権利オブジェクトの状態を変更する、請求項１６に記載の乱数を用いて権利オブジェクトの保安用ファイル識別子を生成して活用する方法。
【請求項１８】
前記保安用ファイル識別子リストを前記ホストに伝送する段階をさらに含む、請求項１２に記載の乱数を用いて権利オブジェクトの保安用ファイル識別子を生成して活用する方法。
【請求項１９】
保存装置から権利オブジェクトを識別するためのファイル識別子のリストを受信部によって受信する受信段階と、
所定の乱数を生成して、前記生成された乱数を前記受信されたファイル識別子の権利オブジェクト識別子に対するハッシュ値と結合して保安用ファイル識別子を保安用ファイル識別子生成部によって生成する保安用ファイル識別子生成段階、および
前記生成された保安用ファイル識別子を前記保存装置に伝送部によって伝送する伝送段階と、を含む、乱数を用いて権利オブジェクトの保安用ファイル識別子を生成して活用する方法を実行するためのコンピュータプログラムを保存するコンピュータ判読可能保存媒体。
【請求項２０】
権利オブジェクトを識別するための保安用ファイル識別子リストを保安用ファイル識別子リスト生成部によって生成する保安用ファイル識別子リスト生成段階と、
前記保安用ファイル識別子リストに含まれた第１保安用ファイル識別子を代替するための第２保安用ファイル識別子をホストから受信部によって受信する受信段階、および
前記受信した第２保安用ファイル識別子で前記第１保安用ファイル識別子を代替して、代替された前記第２保安用ファイル識別子の権利オブジェクト状態を権利オブジェクト管理部によって変更する権利オブジェクトの管理段階と、を含む、乱数を用いて権利オブジェクトの保安用ファイル識別子を生成して活用する方法を実行するためのコンピュータプログラムを保存するコンピュータ判読可能保存媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、乱数を用いて権利オブジェクトの保安用ファイル識別子を生成して活用する装置および方法に関するものであって、より詳細には、ホストと保安用マルチメディアカ

ードとの間で権利オブジェクトを移動したり使用したりするときに保安用ファイル識別子を用いて権利オブジェクトの状態を非活性化状態に変更することで権利オブジェクトを保護して効率的に管理する装置および方法に関するものである。

【背景技術】

【０００２】

現在、ホスト（Ｈｏｓｔ）と保安用マルチメディアカード（Ｓｅｃｕｒｅ Ｒｅｍｏｖａｂｌｅ Ｍｅｄｉａ、以下ＳＲＭと称する）との間で権利オブジェクト（Ｒｉｇｈｔ Ｏｂｊｅｃｔ）を移動したり使用したりするときに利用されるファイル識別子（Ｆｉｌｅ Ｉｄｅｎｔｉｆｉｅｒ、以下ＦＩＤと称する）は、著作権発給者（Ｒｉｇｈｔ Ｉｓｓｕｅｒ）が権利オブジェクトを発行する時に指定した識別子の権利オブジェクト識別子（Ｒｉｇｈｔ Ｏｂｊｅｃｔ Ｉｄｅｎｔｉｆｉｅｒ、以下ＲＯＩＤと称する）を特定の長さでハッシュ（Ｈａｓｈ）して作られることができる。

【０００３】

デジタル著作権管理（Ｄｉｇｉｔａｌ Ｒｉｇｈｔｓ Ｍａｎａｇｅｍｅｎｔ、以下ＤＲＭと称する）において前述したＲＯＩＤは「固有の（ｇｌｏｂａｌｌｙ ｕｎｉｑｕｅ）」という仮定あるが、現実的にこれを保障する方法はない。

【０００４】

特にＲＯＩＤは、発給者によって長さが一定ではないこともあるので、管理の効率上ＳＲＭに保存される権利オブジェクトに対して固定された長さのＦＩＤを生成する時ＲＯＩＤのハッシュ値（２０Ｂｙｔｅ）を利用するのが一般的であるが、ＦＩＤに対する固有性が低くなってＦＩＤ間の衝突が生じる問題点がある。

【０００５】

他にも、ＳＲＭのファイル管理システムに依存して既存ＦＩＤと重複しないように別途の規則に従ってＦＩＤを生成する方法があるが、ＦＩＤだけでは該当権利オブジェクトのＲＯＩＤとの関連性を把握することができなくＲＯＩＤとＦＩＤを連結する別途のメカニズムを必要とする問題点がある。

【発明の開示】

【発明が解決しようとする課題】

【０００６】

本発明は、乱数（ｒａｎｄｏｍ ｎｕｍｂｅｒｓ）を用いて権利オブジェクトの保安用ファイル識別子（Ｓｅｃｕｒｅ Ｆｉｌｅ Ｉｄｅｎｔｉｆｉｅｒ、以下ＳＦＩＤと称する）を生成することによって権利オブジェクトのＦＩＤに対する固有性を高め、効率的に権利オブジェクトを非活性化することにその目的がある。

【０００７】

本発明の目的は、以上で言及した目的に制限されず、言及されていないまた他の目的は次の記載から当業者に明確に理解できるであろう。

【課題を解決するための手段】

【０００８】

前記目的を達成するために本発明の実施形態による乱数を用いて権利オブジェクトのＳＦＩＤを生成して活用する装置は、保存装置から権利オブジェクトを識別するためのファイル識別子のリストを受信する受信部と、所定の乱数を生成して、前記生成された乱数を前記受信されたファイル識別子の権利オブジェクト識別子に対するハッシュ値と結合して保安用ファイル識別子を生成する保安用ファイル識別子生成部、および前記生成された保安用ファイル識別子を前記保存装置に伝送する伝送部と、を含む。

【０００９】

前記目的を達成するために本発明の他の実施形態による乱数を用いて権利オブジェクトのＳＦＩＤを生成して活用する装置は、権利オブジェクトを識別するための保安用ファイル識別子リストを生成する保安用ファイル識別子リスト生成部と、前記保安用ファイル識別子リストに含まれた第１保安用ファイル識別子を代替するための第２保安用ファイル識別子をホストから受信する受信部、および前記受信した第２保安用ファイル識別子で前記

第１保安用ファイル識別子を代替して代替された第２保安用ファイル識別子の権利オブジェクト状態を変更する権利オブジェクト管理部と、を含む。

【００１０】

前記目的を達成するために本発明の実施形態による乱数を用いて権利オブジェクトのＳＦＩＤを生成して活用する方法は、保存装置から権利オブジェクトを識別するためのファイル識別子のリストを受信する受信段階と、所定の乱数を生成して、前記生成された乱数を前記受信されたファイル識別子の権利オブジェクト識別子に対するハッシュ値と結合して保安用ファイル識別子を生成する保安用ファイル識別子生成段階、および前記生成された保安用ファイル識別子を前記保存装置に伝送する伝送段階をと、含む。

【００１１】

前記目的を達成するために本発明の他の実施形態による乱数を用いて権利オブジェクトのＳＦＩＤを生成して活用する方法は、権利オブジェクトを識別するための保安用ファイル識別子リストを生成する保安用ファイル識別子リスト生成段階と、　前記保安用ファイル識別子リストに含まれた第１保安用ファイル識別子を代替するための第２保安用ファイル識別子をホストから受信する受信段階、および前記受信した第２保安用ファイル識別子で前記第１保安用ファイル識別子を代替して、代替された前記第２保安用ファイル識別子の権利オブジェクト状態を変更する権利オブジェクト管理段階と、を含む。

【００１２】

その他実施形態の具体的な内容は詳細な説明および図に含まれている。

【発明の効果】

【００１３】

前記したような本発明の乱数を用いて権利オブジェクトの保安用ファイル識別子を生成して活用する装置によれば次のような効果が１つあるいはそれ以上ある。

【００１４】

権利オブジェクトのファイル識別子に対する固有性が増加する長所がある。

【００１５】

また、特定のホストが非活性化状態に変更した権利オブジェクトは、該当権利オブジェクトのＳＦＩＤを認識しているホストのみアクセスが可能で、非活性化された権利オブジェクトは他のホストから隠匿されることによって、ＳＲＭに保存された権利オブジェクトに対する活性化および非活性化実行が安全な長所もある。

【００１６】

さらに、ＳＲＭに保存された権利オブジェクトに対する活性化および非活性化の実行費用が低いので、権利オブジェクトの移動だけではなく、使用（再生）のようなリアルタイム処理を要するプロセスにも権利オブジェクトの活性化および非活性化の機能が使用可能であり、これは権利オブジェクトの使用において既存の「ｌｏｃｋ／ｕｎｌｏｃｋ」機能に比べて保安性が高まる長所がある。

【発明を実施するための最良の形態】

【００１７】

本発明の利点、特徴、およびそれらを達成する方法は、添付される図面と共に詳細に後述される実施形態を参照すれば明確になるであろう。

【００１８】

しかし、本発明は、以下で開示される実施形態に限定されるものではなく、互いに異なる多様な形態で具現されることが可能である。本実施形態は、単に本発明の開示が完全になるように、本発明が属する技術分野で通常の知識を有する者に対して発明の範疇を完全に知らせるために提供されるものであり、本発明は、請求項の範囲によってのみ定義される。

【００１９】

なお、明細書全体にかけて同一の参照符号は同一の構成要素を指すものとする。

【００２０】

以下、本発明の実施形態による乱数を用いて権利オブジェクトのＳＦＩＤを生成して活

用する装置および方法を説明するための構成図または処理フローチャートに対する図を参考にして本発明について説明する。

【００２１】

この時、フローチャートの各ブロックとフローチャートの組み合わせはコンピュータプログラムインストラクションにより実行可能なのが理解できるであろう。

【００２２】

これらコンピュータプログラムインストラクションは、汎用コンピュータ、特殊用コンピュータまたはその他のプログラマブルデータプロセッシング装備のプロセッサーに搭載されうるので、コンピュータまたはその他のプログラマブルデータプロセッシング装備のプロセッサーを通じて実行されるそのインストラクションがフローチャートのブロックで説明された機能を行う手段を生成するように機構を作れる。

【００２３】

これらコンピュータプログラムインストラクションは特定方式で機能を具現するためにコンピュータまたはその他のプログラマブルデータプロセッシング装備を指向できるコンピュータ利用可能またはコンピュータ判読可能メモリに保存されることも可能なので、そのコンピュータ利用可能またはコンピュータ判読可能メモリに保存されたインストラクションはフローチャートのブロックで説明された機能を行うインストラクション手段を内包する製造品目を生産することも可能である。

【００２４】

コンピュータプログラムインストラクションは、コンピュータまたはその他のプログラマブルデータプロセッシング装備上に搭載することも可能なので、コンピュータまたはその他のプログラマブルデータプロセッシング装備上で一連の動作段階が実行されてコンピュータで実行されるプロセスを生成し、コンピュータまたはその他のプログラマブルデータプロセッシング装備を行うインストラクションはフローチャートのブロックで説明された機能を実行するための段階を提供することも可能である。

【００２５】

また、各ブロックは特定の論理的機能を行うための１つ以上の実行可能なインストラクションを含むモジュール、セグメントまたはコードの一部を示すことができる。

【００２６】

また、いくつの代替実行例では、ブロックで言及された機能が順序を外れて発生することも可能であるということに注目せねばならない。

【００２７】

例えば、連続して図示されている２つのブロックは、実質的に同時に行われてもよく、またはそのブロックが時々該当する機能によって逆順に行われてもよい。

【００２８】

以下、添付した図面を参照して本発明の望ましい実施形態について詳細に説明する。

【００２９】

図１は、本発明の実施形態によるＳＦＩＤの構成示す図である。

【００３０】

本発明の実施形態によるＳＦＩＤ１００は、ＳＲＭで権利オブジェクトを識別するために使用するＦＩＤであって、ＲＯＩＤのハッシュ値１１０と該当権利オブジェクトを設置するホストが生成した乱数１２０を結合して固定された長さで生成される。

【００３１】

本発明の実施形態によるＳＦＩＤは、該当権利オブジェクトを生成したホストのみ知ることが出来るため保安の側面で様々な長所を提供し、これは後述する。

【００３２】

図２は、本発明の実施形態による乱数を用いて権利オブジェクトのＳＦＩＤを生成して活用する装置の構成を示すブロック図である。

【００３３】

本発明の実施形態による乱数を用いて権利オブジェクトのＳＦＩＤを生成して活用する

装置２００の構成は、保存装置から権利オブジェクトを識別するためのＦＩＤのリストを受信する受信部２１０、所定の乱数を生成して生成された乱数の受信を受けたＦＩＤのＲＯＩＤに対するハッシュ値と結合して固定された長さのＳＦＩＤを生成する保安用ファイル識別子生成部２２０、生成されたＳＦＩＤを保存装置に伝送する伝送部２３０および権利オブジェクトの移動、設置、削除およびコピーのうち何れか１つの作業のために保存装置に該当作業を要請して各部を制御する制御部２４０を含む。

【００３４】

ここで保存装置は、ＳＲＭ、保安機能がある所定の保存所を内蔵したＰＣや携帯電話、ＰＤＡ、ＭＰ３プレーヤおよびＰＭＰのうち少なくとも１つを含む意味であり、本発明では保存装置としてＳＲＭを使用する実施形態を説明する。

【００３５】

参考までに、図２に図示された装置はマルチメディアデータを実行するＰＣ、携帯電話、ＰＤＡ、ＭＰ３プレーヤおよびＰＭＰのようなホストに含まれることができる。

【００３６】

図３は、本発明の他の実施形態による乱数を用いて権利オブジェクトのＳＦＩＤを活用する装置の構成を示すブロック図である。

【００３７】

本発明の他の実施形態による乱数を用いて権利オブジェクトのＳＦＩＤを活用する装置３００は、権利オブジェクトを識別するためのＳＦＩＤリストを生成する保安用ファイル識別子リスト生成部３１０、ＳＦＩＤリストに含まれた第１　ＳＦＩＤを代替するための第２　ＳＦＩＤをホストから受信する受信部３２０、受信した第２　ＳＦＩＤで第１　ＳＦＩＤを代替して、代替された第２　ＳＦＩＤの権利オブジェクト状態を変更する権利オブジェクト管理部３３０、保安用ファイル識別子リスト生成部３１０で生成された保安用ファイル識別子リストをホストに送信する送信部３４０および各部を制御する制御部３５０を含む。

【００３８】

参考までに、図３に図示された装置３００は、ＳＲＭ、保安機能がある所定の保存所を内蔵したＰＣや携帯電話、ＰＤＡ、ＭＰ３プレーヤおよびＰＭＰのような保存装置に含まれ得、前述したように本発明では保存装置としてＳＲＭを用いた実施形態を説明する。

【００３９】

本発明の実施形態による図２から図３で図示された構成要素はソフトウェア、ＦＰＧＡ（Ｆｉｅｌｄ　Ｐｒｏｇｒａｍｍａｂｌｅ　Ｇａｔｅ　Ａｒｒａｙ）またはＡＳＩＣ（Ａｐｐｌｉｃａｔｉｏｎ　Ｓｐｅｃｉｆｉｃ　Ｉｎｔｅｇｒａｔｅｄ　Ｃｉｒｃｕｉｔ）のようなハードウェア構成要素を意味し、ある機能を果たす。

【００４０】

しかし、構成要素はソフトウェアまたはハードウェアに限定される意味ではなく、各構成要素はアドレッシングできる保存媒体にあるように構成されることもでき、１つまたはそれ以上のプロセッサーを再生させるように構成されることもできる。

【００４１】

したがって、実施形態での構成要素は、ソフトウェアの構成要素、オブジェクト指向ソフトウェアの構成要素、クラスの構成要素およびタスク構成要素のような構成要素と、プロセス、関数、属性、プロシーザ、サブルーチン、プログラム　コードのセグメント、ドライバ、ファームウェア、マイクロコード、回路、データ、データベース、データ構造、テーブル、アレイ、および変数を含む。

【００４２】

構成要素と該当構成要素のうちから提供される機能はさらに小さい数の構成要素に結合したり追加的な構成要素でさらに分離したりすることができる。

【００４３】

図２に図示された装置２００のうち受信部２１０はＳＲＭから権利オブジェクトを識別するためのＳＦＩＤのリストを受信する。

【００４４】
ここでＳＦＩＤのリストはＳＲＭに保存された権利オブジェクトの状態が活性化状態である権利オブジェクトのＳＦＩＤで構成されている。
【００４５】
また、権利オブジェクトの状態とは、権利オブジェクトが活性化（ｅｎａｂｌｅ）状態および非活性化（ｄｉｓａｂｌｅ）状態のうち何れか１つの状態であることを意味し、権利オブジェクトの状態に対しては図３で詳細に後述する。
【００４６】
一方、保安用ファイル識別子生成部２２０は、所定の乱数を生成して、生成された乱数を受信部２１０で受信したＳＦＩＤのＲＯＩＤに対するハッシュ値と結合して、固定された長さのＳＦＩＤを生成する。
【００４７】
例えば、受信部２１０で受信したＳＦＩＤのＲＯＩＤに対するハッシュ値が２０ｂｙｔｅであり、保安用ファイル識別子生成部２２０で生成した乱数が８ｂｙｔｅであれば、保安用ファイル識別子生成部２２０で生成されるＳＦＩＤは２８ｂｙｔｅで固有性が高まり、ＲＯＩＤに対するハッシュ値で権利オブジェクトを速く検索するのが可能である。
【００４８】
さらに、該当ＳＦＩＤを生成したり認識しているホストだけが該当ＳＦＩＤを解釈したりすることができるので保安性を強化することができる。
【００４９】
一方、制御部２４０は、ホストからＳＲＭに権利オブジェクトを移動、設置、削除およびコピーのうち何れか１つの作業時、ＳＲＭに該当作業を要請する。
【００５０】
ここで、移動（ｍｏｖｅ）は、原本装置（ｓｏｕｒｃｅ　ｄｅｖｉｃｅ）から目標装置（ｔａｒｇｅｔ　ｄｅｖｉｃｅ）に権利オブジェクトを移動させることで、権利オブジェクトの移動中には該当権利オブジェクトが２つの装置に同時に存在することができるが、目標装置への権利オブジェクトの移動が完了すれば該当権利オブジェクトは原本装置に残っていることができなく、ただ目標装置にだけ存在しなければならない。
【００５１】
さらに、設置（ｉｎｓｔａｌｌ）は、権利オブジェクトをホストやＳＲＭのような装置でコンテンツと接続して使用できるように保存して処理する過程であり、削除（ｄｅｌｅｔｅ）は、原本装置から目標装置に権利オブジェクトの移動完了時に原本装置に該当権利オブジェクトが存在しないように削除することを意味する。
【００５２】
また、コピー（ｃｏｐｙ）は、１つの権利オブジェクトが使用可能な状態で２つ以上の装置に存在する状態を意味する。
【００５３】
図３に図示された装置３００のうち保安用ファイル識別子リスト生成部３１０は権利オブジェクトを識別するためのＳＦＩＤリストを生成する。
【００５４】
この時、保安用ファイル識別子リスト生成部３１０で生成されるＳＦＩＤリストは権利オブジェクトの状態が活性化状態である場合のみリストで生成することができ、これとは反対に権利オブジェクトの状態が非活性化状態である場合のみリストで生成することができる。
【００５５】
ここで権利オブジェクトの状態が活性化状態であるということは、権利オブジェクトを使用できる状態を意味することで、所定の条件を満たす装置とプロセスによって権利オブジェクトの活性化状態を非活性化状態に変更することができる。
【００５６】
また、権利オブジェクトが非活性化状態であるということは、権利オブジェクトを使用

できない状態を意味するものであり、活性化状態に変更されない限りプロセスが終了したり電源が遮断されたりしても解除されない状態であり、所定の条件を満たす装置とプロセスによって権利オブジェクトの非活性化状態を活性化状態に変更することができる。

【００５７】

この時、ＳＲＭに保存された権利オブジェクトに対する活性化／非活性化の可否はそれぞれの状態をビットで設定（例えば１と０）することで具現することができ、様々な方法で権利オブジェクトに対する活性化／非活性化状態を示すことができる。

【００５８】

一方、権利オブジェクト管理部３３０は、ホストからＳＲＭに権利オブジェクトが移動する時、設置する権利オブジェクトの空間を確保して該当空間にＳＦＩＤを記録する。

【００５９】

さらに、権利オブジェクト管理部３３０は、ＳＲＭからホストに権利オブジェクトが移動する時、移動する権利オブジェクトの状態を非活性化状態に変更し、受信部３２０で受信した第２　ＳＦＩＤ（移動しようとする権利オブジェクトを非活性化するためにホストで生成した新たなＳＦＩＤ）で第１　ＳＦＩＤ（既に存在した該当権利オブジェクトのＳＦＩＤ）を代替する。

【００６０】

図４は、本発明の実施形態によるホストがＳＲＭからＳＦＩＤリストを読み取る過程を示す図である。

【００６１】

参考までに、ＳＲＭはＡ、Ｂ、Ｃ、Ｄ、Ｅ、ＧおよびＨという権利オブジェクトを保存しており、権利オブジェクトＡ、Ｃ、Ｄ、ＦおよびＨは活性化した状態であり、権利オブジェクトＢ、ＥおよびＧは所定のホストによって既に非活性化されている状態であると仮定する。

【００６２】

先に、ホストはＳＲＭにＳＦＩＤリストの伝達を要請する（Ｓ４０１）。

【００６３】

Ｓ４０１の後、ＳＲＭは活性化された権利オブジェクトのＳＦＩＤリストを生成してホストにこれを伝送する（Ｓ４０２）。

【００６４】

この時、ＳＲＭには権利オブジェクトＡ、Ｃ、Ｄ、ＦおよびＨが活性化された状態で保存されており、権利オブジェクトＢ、ＥおよびＧは所定のホストによって既に非活性化されている状態である。

【００６５】

ここで、所定のホストは図４に図示されたホストになり得、図４に図示されていない他のホストになりうる。

【００６６】

すなわち、ある権利オブジェクトの状態が活性化状態から非活性化状態に変更された時、これを実行したホストもＳＦＩＤリストの要請だけで非活性化された権利オブジェクトを認識することができなく、非活性化された権利オブジェクトは該当権利オブジェクトのＳＦＩＤを認識しているホストのみが別途のプロセスを通して認識可能である。

【００６７】

結局、ＳＲＭが伝送したＳＦＩＤリストにはＡ、Ｃ、Ｄ、ＦおよびＨだけが存在するためホストは該当権利オブジェクトにのみアクセスすることができる。

【００６８】

図５は、本発明の実施形態によるホストからＳＲＭに権利オブジェクトを移動する時ＳＦＩＤの活用を示す図である。

【００６９】

参考までに、ＳＲＭには権利オブジェクトＡ、ＢおよびＣが存在し、ホスト１０は「権利オブジェクトＤ」をＳＲＭに設置しようとすると仮定する。

【００７０】
先に、ホスト１０は、ＳＲＭに「権利オブジェクトＤ」の設置を要請する（Ｓ５０１）。
【００７１】
この時、ホスト１０は、ＳＲＭに設置しようとする「権利オブジェクトＤ」のための所定の乱数を生成して、生成された乱数を「権利オブジェクトＤ」のＲＯＩＤに対するハッシュ値と結合して、固定された長さの「ＳＦＩＤ　Ｄ」を生成してＳＲＭに伝達する。
【００７２】
Ｓ５０１の後、ＳＲＭは「権利オブジェクトＤ」を設置する空間を確保した後、該当空間に「ＳＦＩＤ　Ｄ」を記録して、作業が成功的に実行されればこれをホスト１０に知らせる（Ｓ５０２）。
【００７３】
この時、ホスト１０以外の他のホスト２０がＳＦＩＤリストの伝達を要請する場合、ホスト２０は権利オブジェクトＡ、ＢおよびＣを認識することができる。
【００７４】
Ｓ５０２後、ホスト１０は該当「権利オブジェクトＤ」をＳＲＭに伝送する（Ｓ５０３）。
【００７５】
Ｓ５０３の後、ＳＲＭは、「権利オブジェクトＤ」を受信して「ＳＦＩＤ　Ｄ」で確保された空間に保存して、権利オブジェクトＤの設置が成功的に実行されればこれをホスト１０に知らせる（Ｓ５０４）。
【００７６】
この時、ホスト１０以外の他のホスト２０がＳＦＩＤリストの伝達を要請する場合、他のホスト２０は権利オブジェクトＡ、Ｂ、ＣおよびＤを認識することができる。
【００７７】
図６は、本発明の実施形態によるＳＲＭからホストに権利オブジェクトを移動する時ＳＦＩＤの活用を示す図である。
【００７８】
参考までに、ＳＲＭに権利オブジェクトＡ、Ｂ、ＣおよびＤが存在してホスト１０は「権利オブジェクトＤ」をＳＲＭから移動しようとすると仮定し、図４に図示された過程を通してＳＲＭのＳＦＩＤリストを既に受信した状態であると仮定する。
【００７９】
先に、ホスト１０は、ＳＲＭに「権利オブジェクトＤ」の移動を要請する（Ｓ６０１）。
【００８０】
この時、ホスト１０は、所定の乱数を生成して、生成された乱数を「権利オブジェクトＤ」のＲＯＩＤに対するハッシュ値と結合して、固定された長さの新しい「ＳＦＩＤ　Ｘ」を生成した後、ＳＦＩＤリストから得た「権利オブジェクトＤ」の「ＳＦＩＤ　Ｄ」と「権利オブジェクトＤ」を非活性化するための「ＳＦＩＤ　Ｘ」を「権利オブジェクトＤ」の移動要請時に伝送する。
【００８１】
参考までに、この時点までは他のホスト２０がＳＲＭに接続してＳＦＩＤリストを要請すると、他のホスト２０が受信したＳＦＩＤリストには権利オブジェクトＡ、Ｂ、ＣおよびＤが存在する。
【００８２】
Ｓ６０１の後、ＳＲＭはホスト１０から「ＳＦＩＤ　Ｄ」と「ＳＦＩＤ　Ｘ」を受信して、「ＳＦＩＤ　Ｄ」を有する権利オブジェクトである「権利オブジェクトＤ」を調べて権利オブジェクトの状態を非活性化状態に設定して該当権利オブジェクトの「ＳＦＩＤ　Ｄ」を「ＳＦＩＤ　Ｘ」で代替した後、「権利オブジェクトＤ」をホスト１０に伝送する（Ｓ６０２）。

【００８３】
参考までに、この時点以後から他のホスト２０がＳＲＭに接続しても、ホスト２０はＳＲＭから「ＳＦＩＤ　Ｘ」を有する「権利オブジェクトＤ」を認識できないが、その理由は「ＳＦＩＤ　Ｘ」を有する「権利オブジェクトＤ」の状態が非活性化状態であるからである。
【００８４】
また、この時点で移動プロセスが非正常的に終了するとしても、権利オブジェクトの状態が非活性化状態であるため、コピーされた状態で２つ以上の装置で同一の権利オブジェクトを使用する状況を防止することができる。
【００８５】
参考までに、非活性化状態に変更された「権利オブジェクトＤ」とは、該当「ＳＦＩＤ　Ｘ」を認識しているホストまたは後述する図８に図示された別途のプロセスを用いて該当「権利オブジェクトＤ」を非活性化したホスト主体のみがアクセス可能である。
【００８６】
仮に、非正常的終了以後に「ＳＦＩＤ　Ｘ」を認識しているホスト１０と再び接続される場合、Ｓ６０２以後の過程が実行される。
【００８７】
Ｓ６０２の後、ホスト１０は、ＳＲＭから該当「権利オブジェクトＤ」の伝送を受けてＳＲＭに「権利オブジェクトＤ」の削除を要請するが、この時ホスト１０は該当「権利オブジェクトＤ」の「ＳＦＩＤ　Ｘ」を伝送する（Ｓ６０３）。
【００８８】
Ｓ６０３の後、ＳＲＭは「ＳＦＩＤ　Ｘ」を生成したホストであるホスト１０だけに非活性化された「権利オブジェクトＤ」のアクセスを許容して、要請に応じて「権利オブジェクトＤ」を削除した後、その結果をホスト１０に知らせる（Ｓ６０４）。
【００８９】
Ｓ６０４の後、ホスト１０はＳＲＭで「権利オブジェクトＤ」が削除されたことを確認した後、移動プロセスを終了する。
【００９０】
図７は、本発明の実施形態によるＳＲＭに保存された権利オブジェクトの使用のためＳＦＩＤの活用を示す図である。
【００９１】
参考までに、ＳＲＭに権利オブジェクトＡ、Ｂ、ＣおよびＤが存在し、ホスト１０は権利オブジェクトＤを使用（再生）しようとし、図４に図示された過程によりＳＲＭのＳＦＩＤリストを既に受信した状態であると仮定する。
【００９２】
先に、ホスト１０は、ＳＲＭにコンテンツ再生のための該当「権利オブジェクトＤ」の権利暗号化キー（Ｒｉｇｈｔｓ　Ｅｎｃｒｙｐｔｉｏｎ　Ｋｅｙ、以下ＲＥＫと称する）を要請する（Ｓ７０１）。
【００９３】
この時、ホスト１０は、所定の乱数を生成して、生成された乱数を「権利オブジェクトＤ」のＲＯＩＤに対するハッシュ値と結合して、固定された長さの新たな「ＳＦＩＤ　Ｚ」を生成した後、ＳＦＩＤリストから得た「権利オブジェクトＤ」の「ＳＦＩＤ　Ｄ」と「権利オブジェクトＤ」を非活性化するための「ＳＦＩＤ　Ｚ」をＳＲＭに伝送する。
【００９４】
Ｓ７０１の後、ＳＲＭはホスト１０から「ＳＦＩＤ　Ｄ」と「ＳＦＩＤ　Ｚ」を受信して、「ＳＦＩＤ　Ｄ」に該当する「権利オブジェクトＤ」を検索して、「権利オブジェクトＤ」の既存「ＳＦＩＤ　Ｄ」を「ＳＦＩＤ　Ｚ」で代替する。
【００９５】
Ｓ７０１の後、ＳＲＭは「ＳＦＩＤ　Ｚ」で代替された「権利オブジェクトＤ」を非活性化した後にＲＥＫをホスト１０に伝送する（Ｓ７０２）。

【００９６】
この時、他のホスト２０は「ＳＦＩＤ　Ｚ」で代替されて、非活性化された「権利オブジェクトＤ」を認識することができなく、この段階で他のホストはＳＲＭから以前に受信したＳＦＩＤリストがあっても非活性化された「権利オブジェクトＤ」の変更されたＳＦＩＤ、すなわち「ＳＦＩＤ　Ｚ」を知らないためアクセスすることができない。
【００９７】
Ｓ７０２の後、ホスト１０はＲＥＫを受信した後、「権利オブジェクトＤ」を使用（再生）し、以後、「権利オブジェクトＤ」に対する解除（ｒｅｌｅａｓｅ）を要請する（Ｓ７０３）。この時、ホスト１０は権利オブジェクトＤを活性化するためにＳＲＭに「ＳＦＩＤ　Ｚ」を伝送する。
【００９８】
Ｓ７０３の後、ＳＲＭはホストの要請を受信して該当権利オブジェクトを活性化する。
【００９９】
この時、他のホスト２０は新たなＳＦＩＤ、すなわち「ＳＦＩＤ　Ｚ」を付与された「権利オブジェクトＤ」を認識することができる。
【０１００】
参考までに、ＳＲＭで権利オブジェクトの使用（再生）のために権利オブジェクトの状態を活性化状態に変更する時、権利オブジェクトの状態を活性化状態に変更しようとするホストが、以前に該当権利オブジェクトの状態を非活性化状態に変更したホストなのかを確認した後に作業を進行することもできるが、一般的な権利オブジェクトの使用（再生）の場合には、このような段階を必要とせず、ホストとの接続状態が切れてまた再開された場合のようにＳＦＩＤの不法流出が憂慮される状況で使用され得る。
【０１０１】
図８は、本発明の実施形態による非活性化された権利オブジェクトをホストの装置ＩＤで検索して活性化する過程を示す図である。
【０１０２】
参考までに、ＳＲＭに権利オブジェクトＡ、Ｂ、Ｃ、Ｄ、Ｅ、Ｆ、ＧおよびＨが保存されており、権利オブジェクトＡ、Ｃ、Ｄ、ＦおよびＨは活性化状態であり、権利オブジェクトＢ、ＥおよびＧは非活性化状態であると仮定する。
【０１０３】
また、非活性化状態である権利オブジェクトＢおよびＧはホスト１０によって非活性化状態に変更され権利オブジェクトＥはホスト２０によって非活性化状態にそれぞれ変更されたと仮定する。
【０１０４】
先に、ホスト１０は、ＳＲＭに非活性化されたＳＦＩＤリストの伝達を要請する（Ｓ８０１）。
【０１０５】
Ｓ８０１の後、ＳＲＭは非活性化された権利オブジェクトのうち該当権利オブジェクトの状態を非活性化状態に変更したホスト１０のＩＤが記録されている権利オブジェクトを検索してＳＦＩＤリストを生成してホスト１０に伝達する（Ｓ８０２）。
【０１０６】
この時、他のホスト２０はホスト１０によって非活性化された権利オブジェクトＢ、Ｇを認識することができない。
【０１０７】
Ｓ８０２後、ホスト１０は、ホストが非活性化した権利オブジェクトのＳＦＩＤリストを受信し、１つ以上のＳＦＩＤを選択して活性化する。
【０１０８】
Ｓ８０２の後、ホスト１０は「ＳＦＩＤ　Ｂ」をＳＲＭに伝達し「権利オブジェクトＢ」の活性化を要請する（Ｓ８０３）。
【０１０９】

Ｓ８０３の後、ＳＲＭはホスト１０から「ＳＦＩＤ　Ｂ」を受信した後、「ＳＦＩＤＢ」に該当する「権利オブジェクトＢ」の状態を活性化状態に変更して「権利オブジェクトＢ」の装置ＩＤを削除する。

【０１１０】

以後、他のホスト２０は、活性化した権利オブジェクトＢを認識できるようになる。

【０１１１】

参考までに、ＳＦＩＤの使用は、権利オブジェクトの活性化／非活性化を効率的に実行するようにするが、次の２種類場合が生じることもある。

【０１１２】

１）ホスト１０が「ＳＦＩＤ　Ｘ」を紛失した場合、仮にホスト１０が「ＳＦＩＤ　Ｘ」を有する権利オブジェクトを非活性化した以後に「ＳＦＩＤ　Ｘ」を紛失すると、該当権利オブジェクトを活性化する方法がない。

【０１１３】

このような場合のために本発明の実施形態によるＳＲＭに保存される権利オブジェクトは以下のような構成で保存される。

【０１１４】

【表１】

SFID	ビット表示（活性化／非活性化）	装置ID	権利オブジェクト情報

【０１１５】

ここで、ビット表示（Ｂｉｔ　Ｆｌａｇ）は、活性化／非活性化ビット以外に有用なビットフラッグを追加で指定することができ、装置ＩＤは権利オブジェクトの状態を非活性化状態に変更したホスト主体のＩＤを意味する。

【０１１６】

仮に、ホスト１０が非活性化状態に変更した権利オブジェクトのＳＦＩＤを紛失すると、ホスト１０の装置ＩＤと非活性されたＳＦＩＤリストの装置ＩＤを比較して、同一の装置ＩＤを有するＳＦＩＤリストの伝達を受けることができる。

【０１１７】

ホスト１０は、ＳＲＭに保存された非活性化されている権利オブジェクトとホスト１０内の該当権利オブジェクト情報を結合してＳＲＭに保存された権利オブジェクトを活性化したり削除したりするなどの適切な措置をすることができる。

【０１１８】

２）ホスト１０が「ＳＦＩＤ　Ｘ」を外部に流出した場合、仮に、ホスト１０がクラックされる場合、非活性化された権利オブジェクトのＳＦＩＤが外部に公開されて他のホストのアクセスを許容することもできる。

【０１１９】

これを防止するために、ＳＲＭに保存された非活性化状態の権利オブジェクトを活性化状態に変更する時、ホスト主体の装置ＩＤをチェックすることができる。

【０１２０】

例えば、ホスト２０がホスト１０から流出されたＳＦＩＤで、ホスト１０によって非活性化状態に変更された権利オブジェクトにアクセスしょうとする場合、装置ＩＤが異なるため拒否される。

【０１２１】

参考までに、装置ＩＤはこのプロトコル上で伝達されなければならないものではなく、

ホストと保安カードの最初の認証時に交換することができる。

【０１２２】

以上、添付された図面を参照して本発明の実施形態について説明したが、本発明が属する技術分野で通常の知識を有する者は、本発明が、その技術的思想や必須の特徴を変更しない範囲で他の具体的な形態で実施され得るということを理解できるものである。したがって、以上で記述した実施形態はすべての面で例示的なものであり、限定的ではないものと理解しなければならない。

【図面の簡単な説明】

【０１２３】

【図１】本発明の実施形態によるＳＦＩＤの構成を示す図である。

【図２】本発明の実施形態による乱数を用いて権利オブジェクトのＳＦＩＤを生成して活用する装置の構成を示すブロック図である。

【図３】本発明の他の実施形態による乱数を用いて権利オブジェクトのＳＦＩＤを活用する装置の構成を示すブロック図である。

【図４】本発明の実施形態によるホストがＳＲＭからＳＦＩＤリストを読み取る過程を示す図である。

【図５】本発明の実施形態によるホストからＳＲＭに権利オブジェクトを移動する時ＳＦＩＤの活用を示す図である。

【図６】本発明の実施形態によるＳＲＭからホストに権利オブジェクトを移動する時ＳＦＩＤの活用を示す図である。

【図７】本発明の実施形態によるＳＲＭに保存された権利オブジェクトの使用のためＳＦＩＤの活用を示す図である。

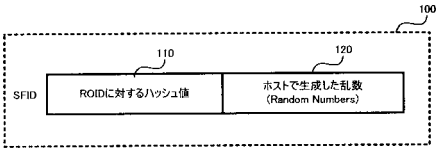
【図８】本発明の実施形態による非活性化された権利オブジェクトをホストの装置ＩＤで検索して活性化する過程を示す図である。

【符号の説明】

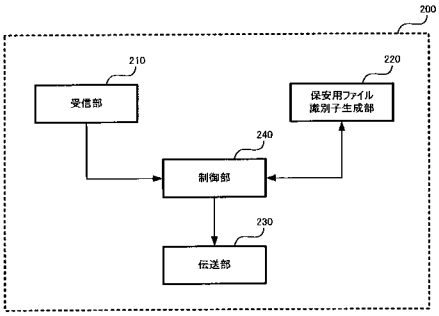
【０１２４】

２１０　受信部
２２０　保安用ファイル識別子生成部
２３０　伝送部
２４０　制御部

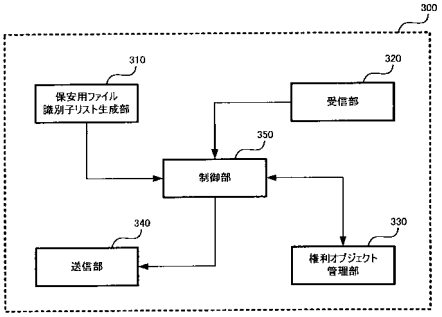
【図１】



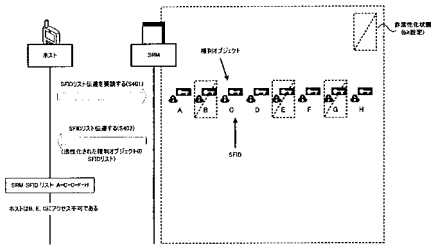
【図２】



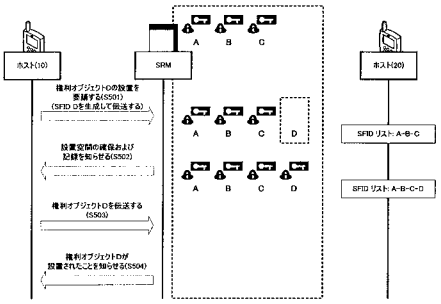
【図３】



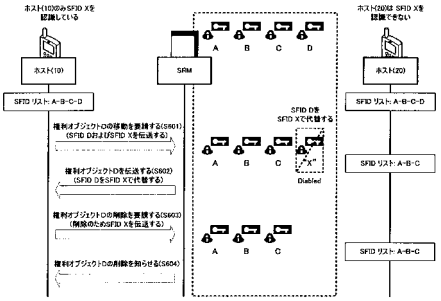
【図４】



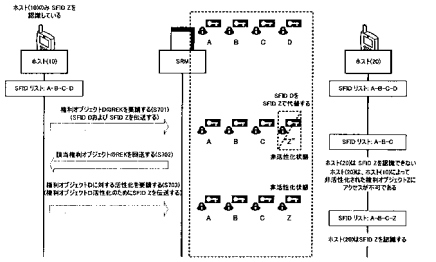
【図５】



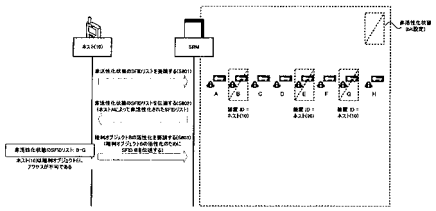
【図６】



【図７】



【図８】



フロントページの続き

(72)発明者 キム，ヨーージン
大韓民国 ４４２－０７０ キョンギード スウォンーシ パルダルーグ インゲードン １１１９ チャーマント・オフィステル ５０７号
(72)発明者 オー，ユンーサン
大韓民国 １３５－２７２ ソウル カンナムーグ ドゴック ２ードン ケポ・ハンシン・アパート ８－７０３号（番地なし）
(72)発明者 シム，サンーギュー
大韓民国 ４４３－３８０ キョンギード スウォンーシ ヨントンーグ ウォンチョンードン ４１９－１７ ホサン・ヴィレッジ １０３－２０２号
(72)発明者 ジョン，キョンーイム
大韓民国 ４６３－０２０ キョンギード ソンナムーシ ブンダンーグ スネードン パークタウン・ロッテ・アパート １２８－９０３号（番地なし）
(72)発明者 キム，ジースー
大韓民国 ４４８－１３０ キョンギード ヨンインーシ スジーグ サンヒョンードン プンサン・アパート １０２－７０１号（番地なし）

審査官 和田 財太

(56)参考文献 特開２００６－１７２４３３（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F 21/24
G06F 12/00