(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2009-199629
(P2009-199629A)
(43)公開日　平成21年9月3日(2009.9.3)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/24	(2006.01)	G06F	12/14	520A	5B017
G06F 21/00	(2006.01)	G06F	12/14	520F	5B082
G06F 21/20	(2006.01)	G06F	15/00	330Z	5B285
G06F 12/00	(2006.01)	G06F	15/00	330D	
		G06F	12/00	537A	

審査請求 有　請求項の数 2　OL　（全 16 頁）

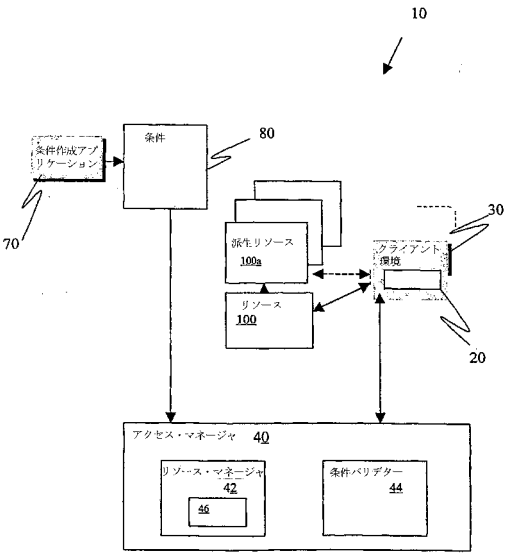
(21)出願番号　特願2009-137820 (P2009-137820)
(22)出願日　平成21年6月9日 (2009.6.9)
(62)分割の表示　特願2003-504586 (P2003-504586)の分割
原出願日　平成14年6月7日 (2002.6.7)
(31)優先権主張番号　60/296,113
(32)優先日　平成13年6月7日 (2001.6.7)
(33)優先権主張国　米国 (US)
(31)優先権主張番号　60/296,117
(32)優先日　平成13年6月7日 (2001.6.7)
(33)優先権主張国　米国 (US)
(31)優先権主張番号　60/296,118
(32)優先日　平成13年6月7日 (2001.6.7)
(33)優先権主張国　米国 (US)

(71)出願人　500470703
コンテントガード　ホールディングズ　インコーポレイテッド
ＣｏｎｔｅｎｔＧｕａｒｄ　Ｈｏｌｄｉｎｇｓ，　Ｉｎｃ．
アメリカ合衆国　１９８０３　デラウェア州　ウィルミントン　スイート　２００－エム　フォーク　ロード　１０３
(74)代理人　100079049
弁理士　中島　淳
(74)代理人　100084995
弁理士　加藤　和詳
(74)代理人　100085279
弁理士　西元　勝一

最終頁に続く

(54)【発明の名称】保護されたリソースの使用を管理する装置及び方法

(57)【要約】
【課題】広範なリソースについて、許可および保護の双方を統合してリソースへのアクセスを管理する方法および装置を提供する。
【解決手段】保護されたリソース（１００）へアクセスする権利は、条件に基づく。条件は、リソースおよびリソース状態の双方に関連づけられ、それによってリソースのライフサイクルの様々な段階でリソースを保護する。保護されたリソースの全体のライフサイクルに関連づけられた条件は、データ構造、規則のセット、または言語（４４）を含む文法を使用して表現可能である。
【選択図】図１



【特許請求の範囲】
【請求項１】
保護されたリソースの使用形態を特定する使用権と、少なくとも一つのアクセス中条件を含む条件と、によって管理される前記保護されたリソースの使用を、管理する装置であって、
前記使用権に基づいて許可された使用のために、前記保護されたリソースへのアクセスを許可する、アクセスマネージャと、
前記アクセスマネージャが、前記許可された使用のために前記保護されたリソースへのアクセスを許可した後に、前記保護されたリソースの使用を制御する、リソースマネージャと、
を含み、
前記保護されたリソースの使用を制御することは、
前記保護されたリソースを、前記許可された使用のための一つ以上の派生リソースへと変換し、
前記アクセス中条件が満たされている限り、前記一つ以上の派生リソースの使用を許可し、
前記アクセス中条件の一つが満足されなくなった場合、前記一つ以上の派生リソースの使用を終了する、
ことを含む、
装置。
【請求項２】
保護されたリソースの使用形態を特定する使用権と、少なくとも一つのアクセス中条件を含む条件と、によって管理される前記保護されたリソースの使用を、アクセスマネージャと、リソースマネージャとを備える装置によって管理する方法であって、
前記アクセスマネージャは、前記使用権に基づいて許可される使用のために、前記保護されたリソースへのアクセスを許可し、
前記リソースマネージャは、前記アクセスマネージャが、前記許可された使用のための前記保護されたリソースへのアクセスを許可した後に、前記保護されたリソースの使用を制御する、
ことを含み、
前記保護されたリソースの使用を制御することは、
前記保護されたリソースを、前記許可された使用のための一つ以上の派生リソースへと変換し、
前記アクセス中条件が満たされている限り、前記一つ以上の派生リソースの使用を許可し、
前記アクセス中条件の一つが満足されなくなった場合、前記一つ以上の派生リソースの使用を終了する、
ことを含む、方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、条件を確認することによってリソースのアクセスおよび使用を管理する方法、並びにそれと共に使用される条件に関する。
【０００２】
（著作権表示）

【背景技術】

【０００３】
電子手段、特にインターネットを介して広範囲に頒布されるディジタル作品（即ち、コンピュータによって読み取り可能な形式の文書または他のコンテンツ）に関して、差し迫った最も重要な問題の１つは、現在、ディジタル作品が頒布および使用される間、コンテンツ・オーナーが知的所有権を実施する能力を欠いていることである。この問題を解決する努力は、これまで「知的所有権マネジメント（Ｉｎｔｅｌｌｅｃｔｕａｌ Ｐｒｏｐｅｒｔｙ Ｒｉｇｈｔｓ Ｍａｎａｇｅｍｅｎｔ（ＩＰＲＭ））」、「ディジタル所有権マネジメント（Ｄｉｇｉｔａｌ Ｐｒｏｐｅｒｔｙ Ｒｉｇｈｔｓ Ｍａｎａｇｅｍｅｎｔ（ＤＰＲＭ））」、「知的財産マネジメント（Ｉｎｔｅｌｌｅｃｔｕａｌ Ｐｒｏｐｅｒｔｙ Ｍａｎａｇｅｍｅｎｔ（ＩＰＭ））」、「権利マネジメント（Ｒｉｇｈｔｓ Ｍａｎａｇｅｍｅｎｔ（ＲＭ））」、および「電子著作権マネジメント（Ｅｌｅｃｔｒｏｎｉｃ Ｃｏｐｙｒｉｇｈｔ Ｍａｎａｇｅｍｅｎｔ（ＥＣＭ））」と呼ばれてきたが、ここでは集約的に「ディジタルライツ・マネジメント（Ｄｉｇｉｔａｌ Ｒｉｇｈｔｓ Ｍａｎａｇｅｍｅｎｔ（ＤＲＭ））」と呼ぶことにする。ＤＲＭシステムを達成するには、考慮すべき多くの問題が存在する。たとえば、認証、許可、アカウンティング、支払いおよび金融決済、権利指定、権利確認、権利実施、および文書保護の問題が考慮されなければならない。参照によってここに開示が組み込まれる特許文献１、特許文献２、特許文献３、特許文献４、特許文献５は、これらの問題に取り組んでいるＤＲＭシステムを開示している。

【０００４】
たとえば、特許文献２は、ディジタル文書の頒布を規制するシステムを開示している。各々のレンダリングデバイスは、それに関連づけられたリポジトリを有する。使用トランザクション・ステップの所定のセットが、文書に関連づけられた使用権を実施するため、リポジトリによって使用されるプロトコルを定義する。使用権は文書コンテンツと一緒に存続する。使用権は、コンテンツ使用の様々な方法、たとえば、閲覧のみ、一回の使用、頒布などを指定する。使用権に従ってコンテンツへのアクセスを許す前に、事前条件、たとえば料金の支払い、アイデンティティの証明、または他の条件を要求可能である。一度、事前条件が満足されると、コンテンツへのアクセスが付与される。条件付きアクセスの概念は、アクセス制御アプリケーションでも良く知られている。たとえば、ログイン名およびパスワードを入力すると、ネットワーク・リソースへのアクセスが付与されることは知られている。

【０００５】
条件付きアクセスの概念は、アクセス制御およびＤＲＭシステムの双方の基礎である。典型的な事前条件、即ち、アクセスを付与する条件は、許可されるユーザのリスト、および所与のリソースへのアクセス権利並びに条件のセットを定義する。所与のリソースに関連づけられた事前条件は、或るユーザに関連づけられたリソースとして定義できる。これは、「役割ベース」のアクセス制御として知られる。更に、事前条件は、「規則ベース」のアクセス制御として知られるプロセスで、規則によって定義できる。事前条件の双方のタイプは、アクセス制御リストとして表現される。アクセス制御リストは、或る言語またはデータ構造の中で定義されたリソースまたは規則のセットである。

【０００６】
条件付きアクセスは、典型的には、大部分のシステムによって、許可プロセスとして実現される。その場合、本人（たとえば、人、システム、またはプロセス）は、或る条件が満足および／または確認された後に、保護されたリソースへのアクセスを許される。

【先行技術文献】
【特許文献】
【０００７】
【特許文献１】米国特許第５，５３０，２３５号
【特許文献２】米国特許第５，６３４，０１２号
【特許文献３】米国特許第５，７１５，４０３号

【特許文献４】米国特許第５，６３８，４４３号
【特許文献５】米国特許第５，６２９，９４０号
【発明の概要】
【課題を解決するための手段】
【０００８】
本発明の第１の態様は、リソースのシステムにおいて、保護されたリソースの使用を管理する方法である。この方法は、保護されたリソースおよび本人に関連づけられた事前条件が満足されたとき、保護されたリソースへの本人によるアクセスを付与し、保護されたリソースおよび本人に関連づけられたアクセス中条件が満足される間、保護されたリソースへの本人によるアクセスの継続を許可し、終了イベントが起こったとき、保護されたリソースへの本人によるアクセスを終了することを含む。終了イベントは、アクセス中条件から区別される事後条件の満足、またはアクセス中条件の満足を継続できないことのいずれかであり得る。
【０００９】
本発明の第２の態様は、リソースのシステムにおいて、保護されたリソースの使用を管理する方法である。この方法は、保護されたリソースへのアクセスを得るために満足されなければならない事前条件を準備し、前記保護されたリソースへのアクセスを継続するために満足されなければならないアクセス中条件を準備することを含む。前記保護されたリソースがアクティブでないとき、前記事前条件が満足されるまで前記事前条件を実施し、前記事前条件が満足されたとき、前記保護されたリソースをアクティブにして前記アクセス中条件を実施する。
【００１０】
本発明の第３の態様は、保護されたリソースを管理するシステムの中で、保護されたリソースを制御するため、保護されたリソースに条件を関連づけるように構成された条件指定である。この指定は、条件が関連づけられる被保護リソースを示すリソース表示、条件に関してリソースのステータスを示す状態変数、および状態変数の値をデバイスから得ることができる方法を示すメソッド指定を含む。
【図面の簡単な説明】
【００１１】
【図１】好ましい実施形態のコンピュータ・アーキテクチャのブロック図である。
【図２】従来のアクセス制御モデルの状態の略図である。
【図３】好ましい実施形態の状態の略図である。
【図４】好ましい実施形態の許可プロセスのフローチャートである。
【図５】好ましい実施形態の条件の略図である。
【図６】好ましい実施形態の条件状態の略図である。
【発明を実施するための形態】
【００１２】
本発明は、好ましい実施形態および添付の図面を使用して説明される。
【００１３】
異なったタイプのリソースは、許可されない使用からそれらを保護するため、異なったタイプの条件および異なったメカニズムを必要とする。出願人は、保護およびコミットメントの双方の条件を含むように従来の事前条件を拡張し、それによって、そのような条件を表現および実施する柔軟なメカニズムを実現した。
【００１４】
好ましい実施形態において、条件は、保護されたリソースの全体のライフサイクルの一部分である。これは、条件がアクセス許可の前に評価されるだけでなく、リソースの実際の消費の間でも評価されることを意味する。更に、条件は、保護されたリソース、および保護されたリソースの状態の双方に関連づけられる。条件を、保護されたリソースの様々な状態に関連づけることは、異なったタイプのリソースを保護する柔軟な方法を、コンテンツ・オーナーまたはサービス・プロバイダへ提供する。リソースは、ディジタル・コン

テンツ、ハードウェア、ソフトウェア・プログラム、メモリ空間、商品、サービス（ウェブ・サービスを含む）、時間、料金、使用権、またはライセンスとなり得る。

【００１５】

使用権は、使用の方法を指定する。たとえば、使用の方法は、指定された方法で指定された期間、或るアイテムを使用する能力を含むことができる。更に、使用権は、転移権、たとえば頒布権を指定可能である、他人への使用権の付与または使用権の派生を許可できる。

【００１６】

好ましい実施形態は、保護されたリソースの使用または消費の前、間、および後で、条件を確認および認証有効化する。条件は、条件状態として表され、各々の条件の現在の状態および履歴は、ログされて後で使用可能である。「状態変数」は、可能的にダイナミックな条件を追跡する。状態変数は、リソースまたは他のダイナミックな条件のステータスを表す値を有する変数である。状態変数は追跡可能であり、状態変数の値は条件の中で使用可能である。たとえば、使用権は、リソースとして、コンテンツを閲覧する権利であり得、条件は、使用権が行使されるとき他のユーザがネットワークへログインされないようにできる。この例では、適切な状態の値が、他のユーザがログインされていることを示すとき、条件は、もはや満足されず、コンテンツを閲覧不可能であるか、閲覧が終了する。

【００１７】

図１は、好ましい実施形態のコンピュータ・アーキテクチャ１０を示す。条件８０は、後で詳細に説明され、アイテムの頒布者、コンテンツ・サービス・プロバイダ、企業マネージャ、またはリソース、たとえばディジタル・コンテンツへのアクセスを制御したいと望む他の当事者に関連づけられた作成アプリケーション７０で準備可能である。条件８０を指定するためには、文法、たとえばＸｒＭＬ（商標）を使用可能である。しかし、条件８０は、任意の方法で指定可能である。ユーザは、ユーザに関連づけられたコンピュータまたは他のデバイスを含むクライアント環境３０内でオペレーションを行う。ソフトウェア・アプリケーション２０、たとえばレンダリング・エンジンまたは他のアプリケーションを、クライアント環境３０へインストール可能である。アクセス・マネージャ４０は、以下で説明するように、保護されたリソース１００および派生リソース１００ａへのアクセスを制御する。

【００１８】

アクセス・マネージャ４０、即ち、好ましい実施形態におけるコンピュータデバイスは、リソース１００および派生リソース１００ａへのアクセスのセキュリティ面を処理する。具体的には、アクセス・マネージャ４０は、署名、たとえば暗号署名、またはメッセージの他の識別特性を、知られた方法で確認および認証有効化することによって、メッセージを認証できる。アクセス・マネージャ４０は２つの主なコンポーネント、即ち、リソース・マネージャ４２および条件確認器（バリデター）４４を含む。リソース・マネージャ４２は、リソースの登録、リソースの変換、およびリソースの終了に責任を有する。「変換」とは、リソース１００から派生リソース１００ａを派生することを意味する。たとえば、リソースが、画像などを表す暗号化ファイルである場合、派生リソース１００ａは、平文画像自身およびその画像を保持するメモリのアドレスを含むことができる。リソースの登録の間、画像を保持するメモリ・アドレスは、リソース・マネージャ４２のリソース・リポジトリ４６によって記録され、そのメモリ、すなわち派生リソース１００ａへのアクセスは、追跡可能である。更に、追跡マーク（たとえば透かし模様）を画像の中へ挿入し、いつでもそれを追跡可能である。

【００１９】

条件バリデター４４は、設定条件をモニタし、システムの現在の状態を管理する。条件バリデター４４は、以下で詳細に説明するように、リソース・マネージャ４６と交信し、派生リソース１００ａを規制する。現在のシステム状態が、もはや有効ではないとき、条件バリデター４４は、以下で詳細に説明するように、全ての派生リソース１００ａを削除する（使用不能にする）か、派生リソース１００ａの使用が、もはや許されないことをア

プリケーション２０に通知するようにリソース・マネージャ４２に要求する。

【００２０】

保護されたリソース１００へのアクセスは、条件８０に基づく。このタイプの条件は、アクセス条件または「事前条件」と呼ばれる。しかし、条件をリソース１００、およびリソース１００の状態に関連づけることによって、リソース１００のライフサイクルの様々な段階で、リソース１００を保護することが可能になる。リソース１００は、ユーザがアクセスを付与される前、アクセスが付与される時、リソース１００の実際の使用の間、およびリソース１００の使用の後で、保護可能である。保護されたリソースの全体のライフサイクルに関連づけられる条件８０は、言語、たとえばＸｒＭＬ（商標）、データ構造、規則のセットを含む文法を使用することによって、表現可能である。好ましい実施形態は、条件を表現する言語としてＸｒＭＬ（商標）を使用する。

【００２１】

リソース１００を保護するため、リソース１００それ自身、または有形であれ無形であれ他のリソースへ、条件８０を課すことができる。それらのリソースは、保護されたリソース１００がアクセスおよび使用される実行環境を作り上げているリソース、たとえばクライアント環境３０のアプリケーション２０を含む。

【００２２】

条件８０は、本人としてアクセスを付与され、保護されたリソース１００を使用するユーザまたはユーザ・グループのアイデンティティとなり得る。条件８０の例は、ＸｒＭＬ（商標）言語の表現として以下で説明される。例Ａは、保護されたディジタル・コンテンツ「ＸｒＭＬブック」を「閲覧」する権利を付与された本人「エドガー」に関連づけられた条件を表す。例Ｂは、本人のグループ、即ち、保護されたディジタル作品「ＸｒＭＬブック」を印刷する権利を付与されたカテゴリ「コンテンツガード従業員」に入る全ての人に関連づけられた条件を表す。

例Ａ：

```
＜ライセンス＞
  ＜インベントリ＞
    ＜ディジタル作品　ライセンス部分ＩＤ＝"ＸｒＭＬブック"／＞
    ＜キーホルダ　ライセンス部分ＩＤ＝"エドガー"／＞
  ＜／インベントリ＞
  ＜付与＞
    ＜キーホルダ　ライセンス部分ＩＤＲｅｆ＝"エドガー"／＞
    ＜閲覧／＞
    ＜ディジタル作品　ライセンス部分ＩＤＲｅｆ＝"ＸｒＭＬブック"／＞
  ＜／付与＞
＜／ライセンス＞
```

例Ｂ：

```
＜ライセンス＞
  ＜インベントリ＞
    ＜ディジタル作品　ライセンス部分ＩＤ＝"ＸｒＭＬブック"／＞
  ＜／インベントリ＞
  ＜付与＞
    ＜ｆｏｒＡｌｌ　ｖａｒＮａｍｅ＝"コンテンツガード従業員"／＞
    ＜本人　ｖａｒＲｅｆ＝"コンテンツガード従業員"／＞
    ＜印刷／＞
    ＜ディジタル作品　ライセンス部分ＩＤＲｅｆ＝"ＸｒＭＬブック"／＞
  ＜／付与＞
＜／ライセンス＞
```

【００２３】

条件８０は、或る特性、たとえば或る資格、または権利、たとえばセキュリティ許容度

を所有していなければならない本人の条件となり得る。例Ｃは、本人が管理者のバッジを所有していなければならない条件を表す。

例Ｃ：

```
＜ライセンス＞
  ＜インベントリ＞
    ＜ディジタル作品　ライセンス部分ＩＤ＝"ＸｒＭＬブック"／＞
    ＜キーホルダ　ライセンス部分ＩＤ＝"エドガー"／＞
  ＜／インベントリ＞
  ＜付与＞
    ＜ｆｏｒＡｌｌ　ｖａｒＮａｍｅ＝"誰でも"／＞
    ＜本人　ｖａｒＲｅｆ＝"誰でも"／＞
    ＜所有特性／＞
    ＜バッジ＞
    ＜資格＞管理者＜／資格＞
    ＜／バッジ＞
    ＜閲覧／＞
    ＜ディジタル作品　ライセンス部分ＩＤＲｅｆ＝"ＸｒＭＬブック"／＞
  ＜／付与＞
＜／ライセンス＞
```

【００２４】

条件８０は、保護されたアイテムへアクセスする時間間隔の条件となり得る。下記の例Ｄは、本人としてのキーホルダ「エドガー」が、２００２年5月２９日の前、および２００３年5月２９日の後では、コンテンツ「ＸｒＭＬブック」を閲覧できない条件を表す。

例Ｄ：

```
＜ライセンス＞
  ＜インベントリ＞
    ＜ディジタル作品　ライセンス部分ＩＤ＝"ＸｒＭＬブック"／＞
    ＜キーホルダ　ライセンス部分ＩＤ＝"エドガー"／＞
  ＜／インベントリ＞
  ＜付与＞
    ＜キーホルダ　ライセンス部分ＩＤＲｅｆ＝"エドガー"／＞
    ＜閲覧／＞
    ＜ディジタル作品　ライセンス部分ＩＤＲｅｆ＝"ＸｒＭＬブック"／＞
    ＜有効期間＞
      ＜前でない＞２００２－０５－２９Ｔ００：００：００＜／前でない＞
      ＜後でない＞２００３－０５－２９Ｔ００：００：００＜／後でない＞
    ＜／有効期間＞
  ＜／付与＞
＜／ライセンス＞
```

【００２５】

条件８０は、本人またはコンテンツにアクセスするために使用されるリソースの物理的ロケーションに関連させることができる。下記の例Ｅは、現在米国にいる人は、誰でもコンテンツ「ＸｒＭＬブック」を印刷できる条件を表す。

例Ｅ：

```
＜ライセンス＞
  ＜インベントリ＞
    ＜ディジタル作品　ライセンス部分ＩＤ＝"ＸｒＭＬブック"／＞
  ＜／インベントリ＞
  ＜付与＞
    ＜ｆｏｒＡｌｌ　ｖａｒＮａｍｅ＝"誰でも"／＞
```

```
      ＜本人　ｖａｒＲｅｆ＝"誰でも"／＞
      ＜印刷／＞
      ＜ディジタル作品　ライセンス部分Ｉｄ＝"ＸｒＭＬブック"／＞
      ＜地域＞
        ＜国＞米国＜／国＞
      ＜／地域＞
    ＜／付与＞
  ＜／ライセンス＞
```

【００２６】

条件８０は、本人がアクセスに対して支払わなければならない料金を指定できる。下記の例Ｆは、３．１０ドルの料金を支払えば、誰でもコンテンツ「ＸｒＭＬブック」を印刷できる条件を表す。下記の例Ｇは、各々の印刷について３．１０ドルの料金を支払えば、誰でもコンテンツ「ＸｒＭＬブック」を印刷できる条件を表す。下記の例Ｈは、１時間の閲覧時間ごとに１０．００ドルを支払えば、誰でもコンテンツ「ＸｒＭＬブック」を閲覧できる条件を表す。

例Ｆ：

```
  ＜ライセンス＞
    ＜インベントリ＞
      ＜ディジタル作品　ライセンス部分ＩＤ＝"ＸｒＭＬブック"／＞
    ＜／インベントリ＞
    ＜付与＞
      ＜ｆｏｒＡｌｌ　ｖａｒＮａｍｅ＝"誰でも"／＞
      ＜本人　ｖａｒＲｅｆ＝"誰でも"／＞
      ＜印刷／＞
      ＜ディジタル作品　ライセンス部分Ｉｄ＝"ＸｒＭＬブック"／＞
      ＜料金＞
        ＜一律支払い＞
        ＜レート通貨＝"米国ドル"＞３．１０＜／レート＞
        ＜／一律支払い＞
        ＜ｔｏ＞
        ＜ａｂａ＞
        ＜金融機関＞１２３４５６７８９＜／金融機関＞
        ＜アカウント＞９８７６５４３２１＜／アカウント＞
        ＜／ａｂａ＞
        ＜／ｔｏ＞
      ＜／料金＞
    ＜／付与＞
  ＜／ライセンス＞
```

例Ｇ：

```
  ＜ライセンス＞
    ＜インベントリ＞
      ＜ディジタル作品　ライセンス部分ＩＤ＝"ＸｒＭＬブック"／＞
    ＜／インベントリ＞
    ＜付与＞
      ＜ｆｏｒＡｌｌ　ｖａｒＮａｍｅ＝"誰でも"／＞
      ＜本人　ｖａｒＲｅｆ＝"誰でも"／＞
      ＜印刷／＞
      ＜ディジタル作品　ライセンス部分ＩＤＲｅｆ＝"ＸｒＭＬブック"／＞
      ＜料金＞
        ＜使用当たりの支払い＞
```

```
        ＜レート通貨＝"米国ドル"＞３．１０＜／レート＞
        ＜／使用当たりの支払い＞
        ＜／料金＞
      ＜／付与＞
  ＜／ライセンス＞
```

例Ｈ：

```
  ＜ライセンス＞
    ＜インベントリ＞
      ＜ディジタル作品　ライセンス部分ＩＤ＝"ＸｒＭＬブック"／＞
      ＜／インベントリ＞
    ＜付与＞
    ＜ｆｏｒＡｌｌ　ｖａｒＮａｍｅ＝"誰でも"／＞
    ＜本人　ｖａｒＲｅｆ＝"誰でも"／＞
    ＜閲覧／＞
    ＜ディジタル作品　ライセンス部分ＩＤＲｅｆ＝"ＸｒＭＬブック"／＞
      ＜料金＞
        ＜時間ベース支払い＞
        ＜レート通貨＝"米国ドル"＞１０．００＜／レート＞
        ＜ｐｅｒ＞ＰＴ１Ｈ＜／ｐｅｒ＞
        ＜フェーズ＞ＰＴ１０Ｍ＜／フェーズ＞
        ＜／時間ベース支払い＞
        ＜ｔｏ＞
        ＜ａｂａ＞
        ＜金融機関＞１２３４５６７８９＜／金融機関＞
        ＜アカウント＞９８７６５４３２１＜／アカウント＞
        ＜／ａｂａ＞
        ＜／ｔｏ＞
      ＜／料金＞
    ＜／付与＞
  ＜／ライセンス＞
```

【００２７】

下記の例Ｉは、誰でもコンテンツを印刷できるが、印刷の前に、印刷権の行使が追跡サービスによって追跡される条件を表す。

例Ｉ：

```
  ＜ライセンス＞
    ＜インベントリ＞
      ＜ディジタル作品　ライセンス部分ＩＤ＝"ＸｒＭＬブック"／＞
      ＜キーホルダ　ライセンス部分ＩＤ＝"エドガー"／＞
    ＜／インベントリ＞
    ＜付与＞
      ＜ｆｏｒＡｌｌ　ｖａｒＮａｍｅ＝"誰でも"／＞
      ＜本人　ｖａｒＲｅｆ＝"誰でも"／＞
      ＜印刷／＞
      ＜ディジタル作品　ライセンス部分ＩＤＲｅｆ＝"ＸｒＭＬブック"／＞
      ＜追跡レポート＞
        ＜状態リファレンス＞
          ＜ｕｄｄｉ＞
          ＜サービスキー＞
          ＜ｕｕｉｄ＞．．．＜／ｕｕｉｄ＞
          ＜／サービスキー＞
```

＜／ｕｄｄｉ＞
＜サービス・パラメータ＞
＜／サービス・パラメータ＞
＜／状態リファレンス＞
＜／追跡レポート＞
＜／付与＞
＜／ライセンス＞

【００２８】

更に、条件８０は、リソース１００が消費されるシステムの条件となり得る。たとえば、条件８０は、システムが、許可されたセキュリティ・メカニズムまたは他の特定のハードウェアまたはソフトウェアを有するか、特定最大数のユーザだけがログオンされることを要求可能である。

【００２９】

条件８０は、リソース１００、たとえばコンテンツが存在するリポジトリまたは他のデバイスを指定できる。条件８０は、本人が、保護されたリソース１００を使用する前に獲得しなければならない承認表示に関連させることができる。条件８０は、リソース１００の使用前または使用後に通知を要求可能である。条件８０は、保護されたリソース１００または他のリソースに関連した以前の権利を指定できる。更に、他の条件８０、たとえば条件の確認方法に、条件８０を課すことができる。

【００３０】

もちろん、条件８０は、上記の例に限定されず、事前条件、アクセス中の条件、および事後条件として、保護されたリソース１００に関連づけられる任意の制限、義務、または要件となり得る。更に、上記の例はＸｒＭＬ（商標）を使用して表現されたが、条件はＸｒＭＬに限定されず、任意の方法で表現可能である。

【００３１】

図５は、好ましい実施形態に従った条件８０を概略的に示す。条件８０は、暗黙的または明示的に表されることのできるリソース表示４２を含む。たとえば、前記の例Ａにおいて、リソース表示４２は、「ディジタル作品」要素の属性「ライセンス部分ＩＤ」によって示される。更に、条件８０は、状態変数４４、およびどのようにして状態変数４４の値を得ることができるかを示すメソッド指定４６を含む。メソッド指定４６は、状態変数４４の値が記憶されているロケーション（たとえば、条件を管理する遠隔のサーバ）、条件が管理されるサーバと通信するための通信プロトコル、および値を得るために必要なパラメータ（たとえばサービス・パラメータなど）を含むことができる。代替的に、メソッドはシステムの中でハードコード可能であり、またメソッド指定４６は省略可能である。

【００３２】

前述したように、状態変数４４は条件８０のステータスを表す。所与の権利に対する全ての状態変数４４の集合は、ここでは「権利状態」と呼ばれる。各々の状態変数４４は、本人、権利、およびリソースについて、任意の時点で対応する値を有する。条件８０の全ての状態変数４４の集合は、ここでは単に「条件状態」と呼ばれる。図６は、条件８０、および条件８０の状態変数４４の現在値５２を含む条件状態５０を示す。メソッド指定５６は、状態変数４４の現在値５２を得るために使用されるメソッドを示し、可能性として、その値が得られるソース、信任状のディジタル署名、リクエストのセッションＩＤ、および他の適切な情報を含む。注意すべきは、メソッド指定５６は、メソッド指定４６に対して冗長であると考えられることができ、単にその繰り返しであり得る。しかし、幾つかの場合には、値５２を実際に得るために使用されるメソッド指定５６は、条件８０での使用を暗示されるメソッド指定４６とは異なることができる。

【００３３】

権利について条件８０を表すため条件状態５０を使用することは、条件８０を確認するプロセスを簡単にする。なぜなら、条件８０を確認するために必要な全ての情報へ、容易にアクセスできるからである。条件状態５０は、対応する条件８０が評価および確認され

るとき、常に構成されて使用される。各々の条件状態５０は、状態変数４４の値５２を確認するために必要な全ての情報を含むことができる。認証された本人および保護されたリソース１００に関連づけられた所与の権利に対する条件状態５０の集合は、ここでは「システム状態」と呼ばれる。

【００３４】

認証された本人は、システムによって処理されたユーザである。システムはそのユーザの真正性を認証有効化し、たとえば、ユーザがユーザ名およびパスワードを使用して成功裏にログインしたとき、そのユーザは、認証された本人または正当な「本人」になる。「システム状態」の概念を使用することによって、権利の所与のセットに対する条件８０は、本人が、保護されたリソース１００にアクセスすることを許される必要システム状態のセットとして定義される。認証された本人が、保護されたリソース１００のアクセスを望むとき、システム状態は、「オリジナル状態」から「許可状態」へ変化する。

【００３５】

一度、システムが許可状態になると、本人は、許可されたオペレーションについて、保護されたリソース１００にアクセス可能である。多くの場合、保護されたリソース１００へ実際にアクセスするのは、認証された本人自身ではない。たとえば、アクセスは他の認証された本人、たとえばレンダリング・アプリケーション、サービスなどへ委任可能である。保護されたリソース１００がアクセスされて消費される間、最初のアクセスを付与するための事前アクセス条件８０のセットは、もはや継続されるアクセスを許可する場合に適用できないことがある。更に、保護されたリソース１００の消費は、リソースを一時的、即ち、派生されたリソース１００ａのセットへ変換し、オリジナル・リソースの上に課されたアクセス条件８０も、リソース１００ａから適用することはできない。リソース１００および派生リソース１００ａを、それらがアクセスされている間に保護するため、好ましい実施形態は、以下で詳細に説明する「アクセス中条件」と呼ばれる許可および保護概念を使用する。

【００３６】

従来のシステムにおいて、リソースは２つの状態の１つの状態にある。図２で示されるように、リソース１００がアクティブでないとき、システムは、事前条件が満足されるまで、オリジナル状態１０２にある。事前条件が満足された時点で、リソース１００はアクティブになり、システムは、許可またはアクティブ状態１０４へ入る。リソースに対する制御を増進するため、好ましい実施形態は、「オリジナル状態」および「許可状態」に加えて、２つの追加状態を定義する。図３で示されるように、保護されたリソース１００の使用またはアクセスの間に、システム状態は、次の状態を経て変化する。即ち、オリジナル状態１０２、許可状態１０４、使用状態１０６、および終了状態１０８である。各々の状態について、次の状態へ移行するか、同じ状態の中で継続するため、満足されなければならない条件８０を定義できる。図１に関して説明したように、条件８０は、必要なユーザ・インタフェースおよび編集能力を含む作成アプリケーション７０を使用して定義および準備可能である。許可状態へ入るために満足されなければならない条件８０は「事前条件」と呼ばれる。リソース１００の使用中に満足されなければならない条件８０は「アクセス中条件」と呼ばれ、使用の終了時に必要な条件８０は「事後条件」と呼ばれる。条件バリデター４４は、各々の状態に必要な条件８０を呼び出すことができる。

【００３７】

アクセス中条件は、オリジナル・リソース１００および派生リソース１００ａが、認証された本人によってアクセスおよび消費されている間、オリジナル・リソース１００から、それ自身および派生リソース１００ａへ転移する条件８０である。たとえば、もしリソース１００が、許可された動作「閲覧」の間にクライアント環境３０のスクリーン上に表示される文書であれば、派生リソース１００ａは、文書からのデータを含むメモリ、文書のプレゼンテーション・フォーマット、および表示されたウィンドウを含むことができる。派生リソース１００ａの全ては、アクセス中条件のセットによって保護されるであろう。言い換えれば、本人は、アクセス中条件が満足される限りでのみ、派生リソース１００

ａへのアクセスを有する。アクセス中条件は、他の条件８０と同じようにして定義できる。

【００３８】

他の例は、アプリケーション、たとえばアプリケーション２０、または他のユーザが、保護されたリソース１００であるサービスをリクエストする場合である。一度、リクエストが許可されると、そのサービスを実行するアプリケーションは派生リソースとして考えられ、サービスが実行されている間、アクセス中条件のセットに従う。アクセス中条件は、派生リソースがもはや使用されなくなるか、システム状態が許可されなくなるまで、システム状態を継続的に変更する。一度、リクエストされた動作が、強制的または任意的に終了すると、アクセス中条件によって保護された全ての派生リソース１００ａは削除（または使用不能に）され、システム状態は事後アクセス条件のセットによって最終状態へ転移する。

【００３９】

リソースの使用またはアクセスの後または間の条件８０は、変化してもよいし変化しなくてもよい。状態が変化しない条件は、「ステートレス（ｓｔａｔｅｌｅｓｓ）条件」と呼ばれ、リソースの使用の後または間に変化する条件は、「ステートフル（ｓｔａｔｅｆｕｌ）条件」と呼ばれる。事前条件８０は、通常、ステートレス条件８０であり、保護された文書へのアクセスを制御するために使用される。アクセス中条件および事後条件は、通常、ステートフル条件８０である。それらは、保護されたリソース１００のライフタイムを制御するために使用される。（たとえば、保護されたリソース１００は、ネットワークへログインされたユーザの数が特定の数を一度超過すると、もはやアクセスされることはできない。）保護されたリソース１００の異なった段階に関連づけられた条件８０のこれらの拡張タイプを使用することによって、好ましい実施形態は、保護されたリソース１００の使用を許可し、リソース１００が使用されている間にリソース１００を保護および追跡するメカニズムを提供する。

【００４０】

図３に示されるように、また図１を参照すると、好ましい実施形態に従ったシステムは、３つの段階を経て進行する。アクセス許可段階３０２は、アクセス・マネージャ４０が、事前条件が満足されたことを確認することによって、許可された動作について、保護されたリソース１００のアクセスを、認証された本人に許可する段階である。リソース保護段階３０４は、アクセス・マネージャ４０が、アクセス中条件が満足されたままであることを確認することによって、リソース１００および派生リソース１００ａが使用されている間、それらのリソースを保護する段階である。動作終了段階３０６は、事後アクセス条件が満足されるか、アクセス中条件が満足されるのを終了したとき、アクセス・マネージャ４０が、所与の動作について、保護されたリソース１００および派生リソース１００ａの使用を終了する段階である。

【００４１】

同じリソース１００について多数のアクセスが与えられる再帰的な状況では、事後条件は、次のサイクルの事前条件と同じである場合がある。そのような場合、無限ループの状況を防止するため、非静止パラメータを使用可能である。たとえば、時間依存条件、または外部実体、たとえば人間の介在によって修正または強制される条件である。

【００４２】

アクセス許可は、許可されたオペレーションについて、保護されたリソース１００にアクセスする権利を、認証された本人に付与する。図４は、好ましい実施形態に従ったアクセス許可手順を示し、ステップ４００で、認証された本人、オペレーション、および保護されたリソース１００に関連づけられた条件８０のリストに基づいて、現在のシステム状態を収集することを含む。各々の状態条件５０は、アクセス・マネージャ４０によって、ローカル・システムまたは遠隔システム、デバイス、アプリケーション、リポジトリ、またはサービスから得ることができる。ステップ４００の結果はオリジナル状態である。ステップ４０２では、事前条件における各々の状態変数４４の現在値５２が、アクセス・マネ

ージャ４０によって収集される。現在値５２は、レコード、たとえばＸＭＬ文書の中へアセンブル可能である。レコードを構成するために使用される情報は、認証可能である（たとえば、本人またはリソース１００の認証）。ステップ４０４では、事前条件がレコードに対して評価、即ち、実施される。たとえば、事前条件の各々の状態変数４４について現在値５２を含むレコードに記憶された情報は受け入れられ、および／または様々な処理、たとえば、レコードの署名の確認または全ての事前条件値の再評価を受けることができる。もし実施が成功すれば、リソース１００および派生リソース１００ａは、ステップ４０６で許可状態へ入る。

【００４３】

事前アクセス条件のセットを認証有効化（発効）するとき条件バリデター４２によって使用されるメソッドに依存して、許可プロセスは、「任意」プロセスまたは「強制」プロセスに分類可能である。前述したレコードに記憶された状態変数４４の値を受け入れるプロセスは「任意」プロセスと呼ばれ、それらの値を問題にするシステムは「強制」プロセスと呼ばれる。強制プロセスでは、保護されたリソース１００および全ての派生リソース１００ａは、事前条件、アクセス中条件、または事後条件を含む条件８０が満足されることができないと、直ちに使用不能にされる。リソース１００または派生リソース１００ａが使用不能（または無効）にされると、アプリケーション２０は、もはや保護されたリソース１００にアクセスすることはできない。任意プロセスでは、アプリケーション２０は、条件８０が満足されないと無効になることを通知される。したがって、アプリケーション２０が、保護されたリソース１００および派生リソース１００ａを使用不能にする責任を有する。使用不能にするかどうかの意思決定は、自動的または人間の介入によって行われることができる。実施ステップ４０４は、システムを、そのオリジナル状態から許可状態（ステップ４０６）または拒絶状態（ステップ４０４）のいずれかへ変更する。許可状態では、保護されたリソース１００が、リクエストした本人またはその委任された本人へ発行され、アクセス中条件が実施を開始される。アクセス中条件は、リソース１００の柔軟な制御を提供するため事前条件から区別されることに注意されたい。

【００４４】

前述したように、リソースの保護は、アクセス中条件のセットを実施することによって、最初の保護されたリソース１００および派生リソース１００ａの双方を保護する。アクセス許可状態から返却された許可状態は、許可された動作の間に実施されるべきアクセス中条件のリストを含む。強制システムでは、全ての派生リソース１００ａは、それが生成および使用されるとき、リソース・マネージャ４２のリソース・リポジトリ４６を使用して登録可能である。もしアクセス中条件が無効になれば、リソース・マネージャ４２は、アプリケーション２０によって、保護されたリソース１００および派生リソース１００ａへのアクセスを不能にする。

【００４５】

他のタイプのシステム、たとえば「追跡システム」では、追跡オブジェクト、たとえば特殊マークまたはＩＤが、リソースの登録および変換の間に、派生リソース１００ａの中へ挿入される。これは、リソース保護コンポーネントによるリソースの追跡を可能にする。挿入マークは、派生リソース１００ａを処理するアプリケーションへトランスペアレント、明らかなフォーマットにできる。追跡システムは、強制システムまたは任意システムのいずれかであり得る。

【００４６】

許可された動作の終了は、事後条件のセット（もし存在すれば）を実行する。事後条件の実行は、システム状態を永続的に変更し、リソース１００への次のアクセス・リクエストに影響を与える。たとえば、もし事後条件が、行使限度に達した後のリソース１００へのアクセスの除去であれば、限度に到達したとき、リソース１００は削除されるか、アクセスを不能にするか禁止する他のアクションが取られる。動作の終了は、リソースの終了を含むことができる。動作が終了されつつあるとき、その動作が終了を強制されているか、またはアプリケーションが任意的に動作を終了しているかどうかを問わず、リソース・

マネージャ４２は、派生リソース１００ａを削除（使用不能に）できる。派生リソース１００ａの削除（または使用不能）は、リソース１００の保護プロセスで重要である。条件バリデター４４は、保護されたリソース１００の使用をコミット、制約し、事後条件のセットを実施する。条件バリデター４４は、もしリソース１００が、システム状態の変化の結果として無効になれば、保護されたリソース１００を無効（使用不能）にするであろう。

【００４７】

好ましい実施形態は、様々なデバイス、たとえばパーソナル・コンピュータ、サーバ、ワークステーション、ＰＤＡ、シンクライアントなどを利用可能である。たとえば、クライアント環境は、ハンドヘルドデバイス、たとえば携帯電話またはＰＤＡとなり得る。様々な通信チャネルを使用可能である。更に、様々な機能を１つのデバイスに集積可能である。開示された機能デバイスおよびモジュールは、明瞭性を目的として機能ごとに区分されている。しかし、様々な機能を、ハードウェアおよび／またはソフトウェア・モジュールおよびデバイスとして、どのようにでも結合または分離可能である。様々な機能モジュールおよびデバイスは、別個または組み合わせた有用性を有する。

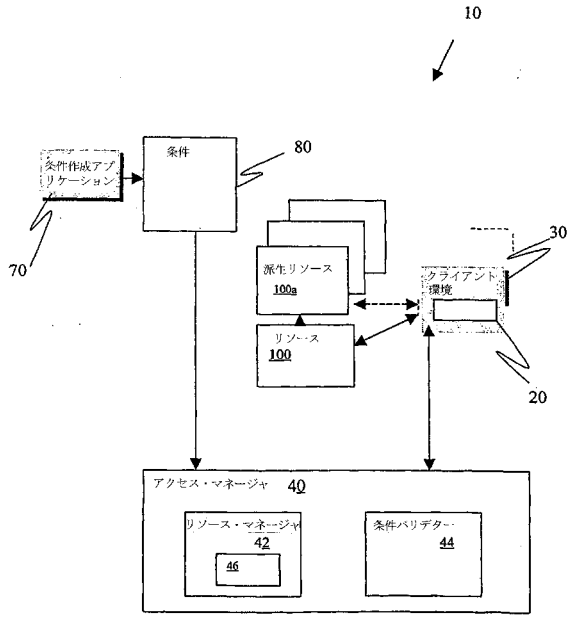
【００４８】

様々なレコード、メッセージ、要素、および、それらの部分は、同じデバイスまたは異なったデバイスに記憶可能である。様々なリンク、リファレンス、指定などは、要素を関連づけるために使用可能である。任意のタイプのリソースへのアクセスを制御可能である。状態変数の値を追跡するため、任意のメカニズムを使用可能である。

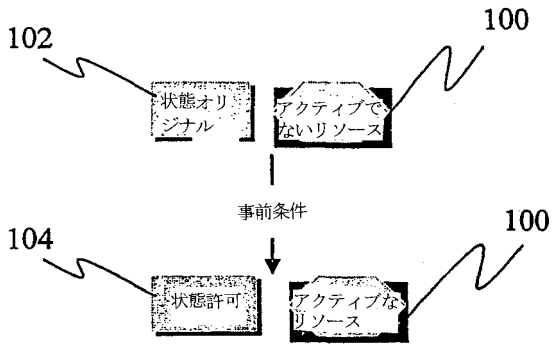
【００４９】

本発明は、好ましい実施形態および例を使用して説明された。しかし、添付のクレイムおよび法的均等物によって規定されるような本発明の範囲から逸脱することなく、様々な修正を行うことができる。

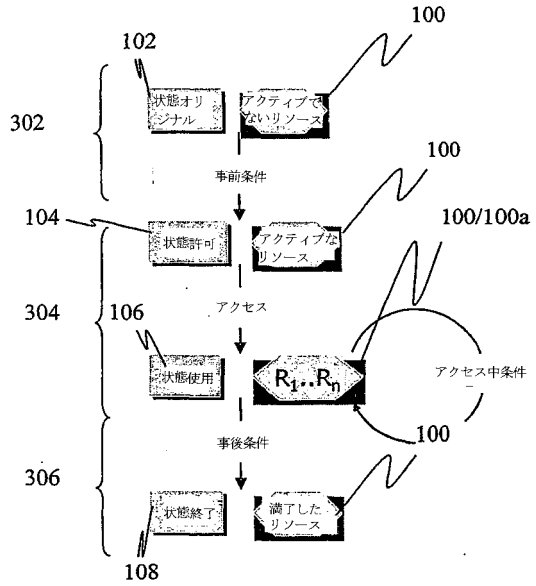
【図１】



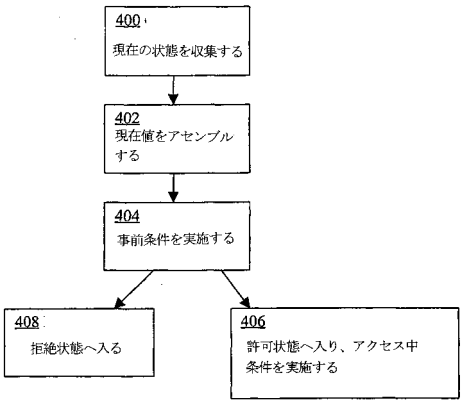
【図２】



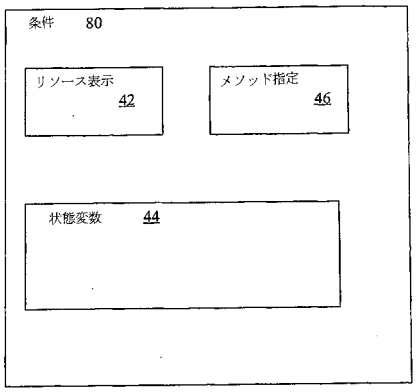
【図３】


100
102
状態オリジナル
アクティブでないリソース
302
事前条件
100
104
状態許可
アクティブなリソース
100/100a
304
106
アクセス
状態使用
$R_1 .. R_n$
アクセス中条件
100
事後条件
306
状態終了
満了したリソース
108

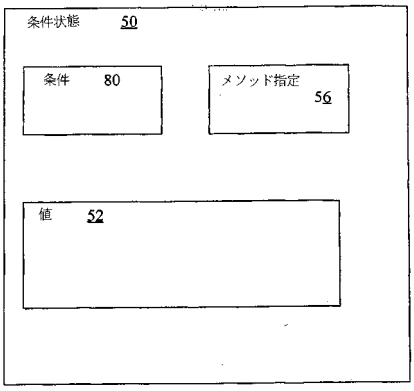
【図４】


400
現在の状態を収集する
402
現在値をアセンブルする
404
事前条件を実施する
408
拒絶状態へ入る
406
許可状態へ入り、アクセス中条件を実施する

【図５】


条件 80
リソース表示 42
メソッド指定 46
状態変数 44

【図６】


条件状態 50
条件 80
メソッド指定 56
値 52

フロントページの続き

(31)優先権主張番号 60/331,623
(32)優先日 平成13年11月20日(2001.11.20)
(33)優先権主張国 米国(US)
(31)優先権主張番号 60/331,624
(32)優先日 平成13年11月20日(2001.11.20)
(33)優先権主張国 米国(US)
(31)優先権主張番号 60/331,625
(32)優先日 平成13年11月20日(2001.11.20)
(33)優先権主張国 米国(US)
(31)優先権主張番号 60/331,621
(32)優先日 平成13年11月20日(2001.11.20)
(33)優先権主張国 米国(US)

(72)発明者 タ、タン
アメリカ合衆国 ９２６４８ カリフォルニア州 ハンティングトン ビーチ ストラットン レーン １８６９４
(72)発明者 デマルティニ、トーマス
アメリカ合衆国 ９０２３０ カリフォルニア州 カルバー シティー グリーン バレー サークル ６４１０ ナンバー１３０
(72)発明者 ファン、ジョセフ、ズィー.
アメリカ合衆国 ９０７０３ カリフォルニア州 セリトス ビーチ ストリート １３４５２
(72)発明者 ラオ、ギラーモ
アメリカ合衆国 ９０５０３ カリフォルニア州 トーランス ローナ ストリート ５５３１
(72)発明者 ングイェン、マイ
アメリカ合衆国 ９６０２１ カリフォルニア州 ブエナ パーク ケンブリッジ アヴェニュー ５６１１
(72)発明者 タダヨン、ビジャン
アメリカ合衆国 ２０８７６ メリーランド州 ジャーマンタウン スコッツベリー ドライブ ２０９２０
(72)発明者 テュウ、ヴィンセント
アメリカ合衆国 ９０５０５ カリフォルニア州 トーランス ニュートン ストリート ４３２８
(72)発明者 トラン、デュク
アメリカ合衆国 ９２６８３ カリフォルニア州 ウエストミンスター サマーウッド ドライブ １４４２２
(72)発明者 ワン、シン
アメリカ合衆国 ９０００７ カリフォルニア州 ロサンジェルス ナンバー８ シュライン プレイス ３００５

Ｆターム(参考) 5B017 AA01 BA06
5B082 EA11 GA11
5B285 AA02 BA09 CA02 CA03 CA06 CA12 CA14 CA16 CA17 CA19
CA33 CA44