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

特許第5026670号
(P5026670)

(45)発行日　平成24年9月12日(2012.9.12)　(24)登録日　平成24年6月29日(2012.6.29)

(51)Int.Cl.		F I		
G06F 21/22	(2006.01)	G06F	21/22	110J
G06F 21/24	(2006.01)	G06F	21/22	110K
G06F 1/00	(2006.01)	G06F	21/24	163G
G06Q 50/10	(2012.01)	G06F	21/24	167A
		G06F	1/00	370E

請求項の数 17　(全 16 頁)　最終頁に続く

(21)出願番号	特願2004-563434 (P2004-563434)
(86)(22)出願日	平成15年11月21日 (2003.11.21)
(65)公表番号	特表2006-512658 (P2006-512658A)
(43)公表日	平成18年4月13日 (2006.4.13)
(86)国際出願番号	PCT/IB2003/005725
(87)国際公開番号	WO2004/059451
(87)国際公開日	平成16年7月15日 (2004.7.15)
審査請求日	平成18年11月20日 (2006.11.20)
(31)優先権主張番号	02080568.5
(32)優先日	平成14年12月30日 (2002.12.30)
(33)優先権主張国	欧州特許庁 (EP)

(73)特許権者　590000248
コーニンクレッカ　フィリップス　エレクトロニクス　エヌ　ヴィ
オランダ国　５６２１　ベーアー　アインドーフェン　フルーネヴァウツウェッハ　1
(74)代理人　100087789
弁理士　津軽　進
(74)代理人　100114753
弁理士　宮崎　昭彦
(74)代理人　100122769
弁理士　笛田　秀仙
(74)代理人　100124224
弁理士　▲高▼▲橋▼　理恵

最終頁に続く

(54)【発明の名称】承認領域における分割された権利

(57)【特許請求の範囲】

【請求項１】

複数の機器からなるシステムにおいて、コンテンツに対するアクセスを当該コンテンツの使用権利に基づいて制御する方法であって、前記使用権利は複数の部分的権利からなり、前記部分的権利の各々は前記コンテンツの異なる使用のうちの１つに対応し、当該方法は、署名手段によって前記複数の部分的権利の各々に個別に署名して複数の署名のセットを提供し、前記署名の各々が前記複数の部分的権利のうちの１つに対応し、前記複数の部分的権利のうちの少なくとも１つを、対応する署名と共に、他の部分的権利から独立して、前記複数の機器のうちの１つの機器から他の機器へ転送可能である、方法。

【請求項２】

前記部分的権利の各々は、アクセス及び行使されるべき部分的権利に対応する署名の確認後にアクセス及び行使される、請求項１に記載の方法。

【請求項３】

前記部分的権利のうちの１つは、レンダリング権利、転送権利、オファー権利、派生著作物権利及び利用権のうちの１つからなる、請求項１又は請求項２に記載の方法。

【請求項４】

前記部分的権利のうちの少なくとも１つは限られた回数のみ行使可能である請求項１から請求項３のいずれか一項に記載の方法。

【請求項５】

前記複数の機器の１つが、前記部分的権利及びその交付者がいずれも無効とされていな

いかを、当該部分的権利を行使する前に確認する、請求項１から請求項４のいずれか一項に記載の方法。
【請求項６】
前記複数の機器からなる前記システムが承認領域(Authorized Domain)を構成する、請求項１から請求項５のいずれか一項に記載の方法。
【請求項７】
少なくとも１つの部分的権利が、当該部分的権利が保護されるべき程度を示す保護レベルを含む、請求項１から請求項６のいずれか一項に記載の方法。
【請求項８】
部分的権利が保護されるべき程度を示す保護レベルが、当該部分的権利の種類に基づいて決定される、請求項１から請求項６のいずれか一項に記載の方法。
【請求項９】
前記システム中の少なくとも１つの機器が、
別の機器が適合性を有し取消しを受けていないことを確認し、
少なくとも一つの部分的権利と、前記承認領域の識別情報、前記別の機器の識別情報並びに前記部分的権利の期間及び有効性に関する情報との組み合わせからなる情報に署名し、
署名された前記組み合わせを前記別の機器に転送する、
請求項６に記載の方法。
【請求項１０】
前記システム中の少なくとも１つの機器が、
別の機器が適合性を有し取消しを受けていないことを確認し、
少なくとも１つの部分的権利に署名し、
署名された前記部分的権利を前記別の機器に転送する、
請求項６に記載の方法。
【請求項１１】
前記別の機器が異なる承認領域（Authorized Domain）のメンバである、請求項９に記載の方法。
【請求項１２】
署名された前記組み合わせを前記別の機器に転送する前に、前記少なくとも１つの機器が、前記別の機器が準拠機器であるかを確認する、請求項１１に記載の方法。
【請求項１３】
前記少なくとも１つの機器中の転送された部分的権利が、当該少なくとも１つの機器により、無効にされるか又は削除される、請求項１１に記載の方法。
【請求項１４】
前記使用権利が特定の部分的権利のオファー権利を含み、前記オファー権利は、署名された前記特定の部分的権利を、要求に応じて、前記コンテンツのプロバイダから、当該オファー権利を前記プロバイダに送信した機器とは別の機器へ直接転送する約束を含み、前記プロバイダは、前記オファー権利を受信すると、署名された前記特定の部分的権利を前記別の機器へと供給する、請求項６に記載の方法。
【請求項１５】
複数の機器からなり、コンテンツに対するアクセス制御を当該コンテンツの使用権利に基づいて実行するクライアントシステムであって、前記使用権利は複数の部分的権利からなり、前記部分的権利の各々は前記コンテンツの異なる使用のうちの１つに対応し、前記部分的権利の各々は個別に署名されて複数の署名のセットが提供され、前記署名の各々は、前記複数の部分的権利のうちの１つに対応し、前記クライアントシステムは、前記署名の各々を個別に確認し、前記複数の部分的権利のうちの少なくとも１つを、対応する署名と共に、他の部分的権利から独立して、前記複数の機器のうちの１つの機器から他の機器へ転送可能であるクライアントシステム。
【請求項１６】
コンテンツに対するアクセス制御を当該コンテンツの使用権利に基づいて実行するサー

バシステムであって、前記使用権利は複数の部分的権利からなり、前記部分的権利の各々は前記コンテンツの異なる使用のうちの１つに対応し、前記サーバシステムは、前記複数の部分的権利の各々に個別に署名する署名手段を有し、前記サーバシステムは、前記複数の部分的権利のうちの少なくとも１つが、対応する署名と共に、他の部分的権利から独立して、１つの機器から他の機器へ転送可能であるように、個別に署名された部分的権利を、複数の署名された部分的権利のセットにまとめる、サーバシステム。

【請求項１７】

コンテンツに対するアクセス制御を当該コンテンツの使用権利に基づいて実行する機器であって、前記使用権利は複数の部分的権利からなり、前記部分的権利の各々は前記コンテンツの異なる使用のうちの１つに対応し、前記部分的権利の各々は個別に署名されて複数の署名のセットが提供され、前記複数の部分的権利のうちの少なくとも１つを、対応する署名と共に、他の部分的権利から独立して、他の機器へ転送可能である機器。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、機器の組を含むシステム内において、コンテンツ項目へのアクセスを管理する方法であって、少なくとも１つの使用権利をコンテンツ項目と関連付ける工程を含む方法に関するものである。

【０００２】

本発明はまた、機器の組を含み、コンテンツ項目と関連付けられた使用権利を取り扱う手段を有し、コンテンツ項目へのアクセス管理を実行するように構成されたクライアントシステムにも関するものである。

【０００３】

本発明はさらに、コンテンツ項目へのアクセス管理を実行するように構成され、さらに少なくとも１つの使用権利をコンテンツ項目と関連付けるサーバーシステムにも関するものである。

【０００４】

本発明はまた、使用権利を担持する信号にも関するものである。

【０００５】

本発明はさらに、コンテンツ項目へのアクセス管理を実行するように構成され、コンテンツ項目と関連付けられた使用権利を取り扱うことのできる機器にも関するものである。

【背景技術】

【０００６】

テレビその他のコンテンツは、ますますデジタル化してきている。また、デジタルコンテンツは、互いに通信できるものであることが多い機器間において、容易に転送が可能である。このことは、コンテンツへのアクセスがもはや１つの機器に限定されておらず、何らかの（ホーム）ネットワークに接続されたいずれの機器からもコンテンツへのアクセスが可能であるような、ユーザーフレンドリなシステムを末端ユーザーに与える。

【０００７】

一方、このことは、コンテンツの所有者に対しては、自分のコンテンツが無制限にコピーまたは転送されるという脅威をもたらす。デジタル著作権管理（ｄｉｇｉｔａｌ　ｒｉｇｈｔｓ　ｍａｎａｇｅｍｅｎｔ；ＤＲＭ）システムは、コンテンツへのアクセスを防止および制限するように設計される。無制限のコピーを防止するため、コンテンツのデジタル転送に対して厳しい規則を課したいと考えることの多いコンテンツの所有者にとっては、ＤＲＭシステムによるコンテンツ保護は、消費者世帯へのデジタルコンテンツの頒布を受諾するための重要な条件である。

【０００８】

ＣＰＴＷＧ（Ｃｏｐｙ　Ｐｒｏｔｅｃｔｉｏｎ　Ｔｅｃｈｎｉｃａｌ　Ｗｏｒｋｉｎｇ　Ｇｒｏｕｐ；コピー防止テクニカルワーキンググループ；http://www.cptwg.org）、ＤＶＢ（Ｄｉｇｉｔａｌ　Ｖｉｄｅｏ　Ｂｒｏａｄｃａｓｔｉｎｇ；デジタルビデオ放送；

http://www.dvb.org）、およびＴＶ－Ａｎｙｔｉｍｅ（http://www.tv-anytime.org）のような、いくつかのフォーラムでは、消費者が自己のホームネットワークに接続された機器から価値の高いデジタルコンテンツにアクセスする際に、いかにして確実にそのコンテンツを不正に再配信できないようにするかということについて、議論が行われている。

【０００９】

ＤＶＢ－ＣＰＴ（Ｃｏｐｙ　Ｐｒｏｔｅｃｔｉｏｎ　Ｔｅｃｈｎｉｃａｌ　ｍｏｄｕｌｅ；コピー防止テクニカルモジュール）、およびＴＶ－ＡｎｙｔｉｍｅのＲＭＰ（Ｒｉｇｈｔｓ　Ｍａｎａｇｅｍｅｎｔ　ａｎｄ　Ｐｒｏｔｅｃｔｉｏｎ；著作権管理および保護）における最近の議論では、上記の問題は、承認領域（Ａｕｔｈｏｒｉｚｅｄ　Ｄｏｍａｉｎ；ＡＤ）という題目の下で扱われている。ＡＤ内においては、消費者はコンテンツにアクセスし、そのコンテンツを配信する自由を有しているのと同時に、領域間でコンテンツが無制限にデジタルコピーされることを防止する、厳しいインポート規則およびエクスポート規則の導入により、コンテンツの所有者およびサービスプロバイダの権利も保護されているという意味で、ＡＤは、コンテンツプロバイダの関心と消費者の関心との双方を尊重したものである。

【００１０】

ＤＶＢ－ＣＰＴグループは、ＡＤを、ＤＶＢ－ＣＰＣＭ（Ｃｏｐｙ　Ｐｒｏｔｅｃｔｉｏｎ　ａｎｄ　Ｃｏｐｙ　Ｍａｎａｇｅｍｅｎｔ；コピー防止およびコピー管理）に準拠した機能的単位の組であって、コンテンツおよびコンテンツフォーマットの流通を管理するものであると定義した。ＡＤは、著作権保護されたコンテンツの承認された使用についての、信任環境を表す。ＡＤは、潜在的に非接続とされているかもしれない、ユーザーのホームネットワークのいくつかのセグメントからなっていてもよい。これには、携帯機器の一時的な接続や、携帯可能な媒体による、異なる複数のネットワークセグメント（動作時間が重複しないセグメントであるかもしれない）の仮想的な「接続」が含まれる。

【００１１】

ＡＤは、そのＡＤ内において適正に取得されたコンテンツへの制限のない単純なアクセスを、消費者に提供する。消費者は、その領域に、機器、権利、およびコンテンツを追加できることを期待する。消費者はまた、どこからでも、いつでも、かつ自分が持つ機器のそれぞれにおいて、自分のコンテンツにアクセスできることを期待する。加えて、このことは、携帯機器や、ホテルの部屋のテレビのような家庭外の端末についても当てはまるかもしれない。さらに、たとえば世帯間でユーザーが変わるために、領域へのユーザーの追加および領域からのユーザーの除外があり得る。また、たとえば、滞在中の友人であるため、または公正な使用規定のためという理由で、コンテンツへのアクセス手段を有することを期待するユーザーもいるかもしれない。

【００１２】

一方、コンテンツプロバイダは、コンテンツのやりとり、とりわけインターネットでの再配信を介したやりとりに対して、強い制限を要求する。したがって、コンテンツに関する権利は、明確に規定され、保護されるべきである。たとえば、テレビシステムの領域において、コンテンツ権（有料テレビの場合にはＥＣＭとも呼ばれる）は、そのコンテンツに関して何が許可されているかを記述しており、使用権利（有料テレビの場合にはＥＭＭとも呼ばれる）は、ある人物に特定のコンテンツ権を使用する権限を付与しており、さらにあるユーザーがそのコンテンツで何を行うことを許可されているかを記述していてもよい。

【００１３】

使用権利の例としては、コンテンツを再生する権利、子コピーを作成する権利等が挙げられる。

【００１４】

コンテンツ権と使用権利とのいずれも、暗号鍵も含んでいてもよい。

【００１５】

ホームネットワークにおけるＤＲＭの利用に関するより広範な概説については、Ｆ．Ｌ

．Ａ．Ｊ．Ｋａｍｐｅｒｍａｎ、Ｓ．Ａ．Ｆ．Ａ．ｖａｎ　ｄｅｎ　Ｈｅｕｖｅｌ、Ｍ．Ｈ．Ｖｅｂｅｒｋｔ、Ｄｉｇｉｔａｌ　Ｒｉｇｈｔｓ　Ｍａｎａｇｅｍｅｎｔ　ｉｎ　Ｈｏｍｅ　Ｎｅｔｗｏｒｋｓ（ホームネットワークにおけるデジタル著作権管理）、フィリップス・リサーチ、オランダ、ＩＢＣ　２００１　ｃｏｎｆｅｒｅｎｃｅ　ｐｕｂｌｉｃａｔｉｏｎ、第Ｉ巻、第７０－７７頁を参照されたい。

【００１６】

コンテンツ権および使用権利は、いくらかの価値を代表するものであり、望まれない複製や非承認の生成から保護されるべきであることは明らかである。このことは、不正変更防止ソフトウェアおよび／またはハードウェアによってのみ取扱いが可能な、暗号化された安全な通信と、これらの権利の安全な記憶とを利用して行うことが可能である。

【００１７】

コンテンツ権は、個人のものとされていないので、コンテンツと共に転送されることも、異なる種々のサーバーによりオファー（提供）されることもあり得る。

【００１８】

しかしながら、使用権利は個人ごとのものとされている。ビジネスモデルまたは保護戦略に応じて、使用権利は、機器、ＣＤ等の媒体、ＡＤ、または特定の人物に拘束され得る。不正変更防止の取扱いの要求は、たとえば機器間や旅行時において、使用権利を自由に使用または転送することを困難にする。

【００１９】

よりよい１つの解決策は、デジタル署名を用いて使用権利を保護することである。使用権利は、よく知られた公開鍵署名技術を用いて、コンテンツプロバイダその他の権限を有するコンテンツ源によって署名される。かかる解決策においては、コンテンツプロバイダは、秘密鍵と公開鍵とのペアを有している。秘密鍵は、公開の権利に署名を加える処理において必要とされる。秘密鍵は、コンテンツプロバイダにより、完全に秘密に保持される。公開の権利の完全性を保護する署名の有効性は、対応の公開鍵を用いて確認することができる。使用権利はデジタル署名によって保護されているので、不正変更防止環境外においても、使用権利が許可され得る。

【００２０】

コンテンツへの不正なアクセスを防止するために、使用権利の証明は、権限を有するコンテンツ源に由来するものであることが（公開鍵を用いて）確認できた場合にのみ、（準拠）機器によって認められるべきである。加えて、証明を認める前に、その証明が、その権利のものとして意図されたＡＤに属するか否か、または、人物ベースのＡＤの場合には、対応の人物が存在するか否か等、他の条件が確認されてもよい。

【００２１】

デジタル使用権利の中には、たとえばあるコンテンツ片を３回のみ再生してよい権利や、そのコンテンツを他の領域へ２回のみ転送してよい権利等、限られた回数のみ使用可能なものもあり得る。この態様は、使用権利自体が、その使用権利が利用されるごとに始動させられる、何らかの計数機構または取消機構を含んでいることを要する。

【発明の開示】

【発明が解決しようとする課題】

【００２２】

しかしながら、使用権利への計数機構の実装に起因する変更は、署名を無効化してしまう。署名は、信任された第三者によってのみ計算可能であり、このことが不利であることは明白である。

【００２３】

加えて、使用権利は、別の領域またはユーザーに対して１回のみコンテンツを転送してよい権利も含み得る。かかる転送権利は、使用後に取り消される必要がある。かかる転送権利の取消しまたは削除もまた、残りの使用権利の署名を無効化してしまう。

【００２４】

本発明の１つの目的は、デジタル署名を無効化することなく、使用権利の取扱いを可能

とする方法を提供することである。
【課題を解決するための手段】
【００２５】
この目的は、冒頭の段落で述べた方法であって、使用権利を一組の部分的権利に分解する工程と、その分解の後に、その一組の部分的権利の各々に個別に署名して、対応の署名を結果として得る工程とをさらに含む方法によって、達成される。
【００２６】
この方法は、使用権利が、全体としてではなく、基本的な断片ごとに署名されるようになるという利点を有する。たとえば、別の領域にコンテンツを転送する権利と、特定のＡＤ内においてコンテンツを１回再生する権利とが、それぞれ個別に署名され得る。部分的権利が使用または転送される際には、その部分的権利はデジタル署名されたままであり、残りの部分的権利もまたデジタル署名されている。
【００２７】
本発明に係る上記の方法の１つの実施形態が、請求項２に記載されている。
【００２８】
システム内の機器は、使用権利全体へのアクセスを要さずに、上記のような部分的権利にアクセスし、その有効性を確認することができる。その後、その権利は、有効性が正しく確認できた後に行使され得る。
【００２９】
本発明に係る上記の方法の１つの実施形態が、請求項４に記載されている。
【００３０】
この形態では、いくつかの部分的権利は、限られた回数のみ行使可能であり、このことは、コンテンツ項目がアクセスされ得る回数の管理を可能とする。権利が１回のみ行使可能なものである場合には、かかる権利の取消し、削除、または使用済の権利としての即座のマーキングが、個別に行われ得るという利点がある。
【００３１】
本発明に係る上記の方法の１つの実施形態が、請求項５に記載されている。
【００３２】
この形態では、機器は、権利の行使前にその権利の取消しを確認することができ、それにより、古い権利の使用に対するロバスト性を向上させることができる。
【００３３】
領域内の不正変更防止機器を調べることのできるこの確認動作は、信頼性の高い権利の取消しを可能とする。
【００３４】
本発明に係る上記の方法の１つの実施形態が、請求項６に記載されている。
【００３５】
複数機器のシステムは、たとえば上記に述べたようにして、たとえば１つの世帯をなすメンバーに属する機器の領域、または、機器間もしくはそれら機器の所有者間において何らかの他の関係を有する領域といった、領域を構成し得る。各人物は、領域に入ることまたは出ることを許されていてもよい。ユーザーは、たとえば個人のスマートカードによって識別され得る。
【００３６】
本発明に係る上記の方法の１つの実施形態が、請求項９に記載されている。
【００３７】
この形態では、領域内の少なくとも１つの機器が、部分的権利の１つと、その機器自体ならびに／もしくは別の機器または領域の識別情報を含む情報、および有効性に関する情報（期間、タイプ）との組合せに、自己の署名を加え、その後、この権利を別の機器（別の領域の一部、または別の領域を代表するものであるかもしれない）に転送することを許されている。
【００３８】

このことは、履歴、再分配チャネル、および転送された権利の当初の交付者のトラッキングを行うことを可能とするという利点を有する。

【００３９】

同様に、請求項１０に記載されているように、装置は、自己を制限して部分的権利のみに署名することを許されていてもよい。

【００４０】

本発明に係る上記の方法の１つの実施形態が、請求項１２に記載されている。

【００４１】

権利を転送する機器は、その権利を受け取る機器の適合性を確認することを要求されていてもよい。権利を転送する機器はまた、その権利を受け取る機器が取消しを受けていないかどうかを、第三者に問い合わせてもよい。権利を受け取る機器も、送信元の機器に対して類似の確認動作を行ってもよい。

【００４２】

本発明に係る上記の方法の１つの実施形態が、請求項１３に記載されている。

【００４３】

別の機器に権利を転送する機器は、部分的権利をローカルにおいて取消しまたは削除してもよい。

【００４４】

本発明に係る上記の方法の１つの実施形態が、請求項１４に記載されている。

【００４５】

この形態では、コンテンツプロバイダからのオファーを表す、オファー権利と呼ばれる使用権利のタイプが導入される。オファー権利は、要求を受けて、署名された使用権利を、コンテンツプロバイダから、より後の段階で指定される第三者に直接転送する約束を含んでいてもよい。このことは、コンテンツプロバイダによる権利の使用の有効性確認を可能としながら、オファー権利の所有者が、より後の段階で使用権利を「転送」することを可能とする。オファー権利と転送時点との間の最小遅延または最大遅延といった、追加の制約が導入されてもよい。

【００４６】

上記の第三者は、別の領域であってもよいが、その領域の一部ではないまたは常にその領域の一部であるとは限らないユーザーが所有する機器の１つであってもよい。第三者はまた、他者が所有する機器であってもよいが、たとえば滞在中、旅行中、またはホテルの部屋において、転送の所有者によって現在使用されている機器であってもよい。

【００４７】

本発明の別の１つの目的は、冒頭の段落で述べたようなクライアントシステムであって、使用権利が、個別に署名された部分的権利の組であり、当該クライアントシステムが、それら部分的権利を、個別に確認して個別に取り扱うように構成されているクライアントシステムを提供することである。

【００４８】

本発明のさらに別の１つの目的は、冒頭の段落で述べたようなサーバーシステムであって、使用権利を一組の部分的権利に分解する手段を有し、その分解の後に、一組のそれら部分的権利の各々に個別に署名するように構成された署名部をさらに有し、個別に署名された部分的権利をまとめて１つの組とするように構成されたサーバーシステムを提供することである。

【００４９】

本発明のさらに別の１つの目的は、冒頭の段落で述べたような信号であって、使用権利が、個別に署名された部分的権利に分割されている信号を提供することである。

【００５０】

本発明のさらに別の１つの目的は、冒頭の段落で述べたような機器であって、各々がデジタル署名を有する部分的権利に分割されている、使用権利を取り扱うように構成された機器を提供することである。

【発明を実施するための最良の形態】
【００５１】
以下、本発明の上記およびその他の側面を、例として、図面を参照してさらに説明する。図面全体に亘って、同一の参照番号は、類似または対応の特徴を示している。図中に示されている特徴のいくつかは、典型的にはソフトウェア内に実装されるものであり、それ自体が、ソフトウェアモジュールまたはオブジェクトといったような、ソフトウェア的存在を示している。
【００５２】
図１は、ホームネットワークシステム１００を概略的に示している。このようなシステムは、典型的には、たとえばラジオ受信機、チューナー／デコーダ、ＣＤプレーヤー、１対のスピーカー、テレビ、ＶＣＲ、テープデッキ、パソコン等といった、複数の機器を含む。これらの機器は、通常、相互接続されて、１つの機器（たとえばテレビ）が、別の機器（たとえばＶＣＲ）を制御できるようにされている。たとえばチューナー／デコーダまたはセットトップボックス（ＳＴＢ）といったような１つの機器が、通常は中央機器であり、その他の機器に対して中央制御を行う。
【００５３】
コンテンツ１３０は、典型的には、音楽、歌、動画、テレビ番組、画像、プログラミング案内情報等のものを含み、たとえば、ＰＣ１０６、住宅用ゲートウェイ、またはセットトップボックス１０１を介して受信される。コンテンツ源としては、ブロードバンドのケーブルネットワークへの接続、インターネット接続、衛星から地上へのデータ送信等があり得る。セットトップボックス１０１またはシステム１００内のその他のいずれの機器も、適当な大きさのハードディスク等の記憶媒体Ｓ１を備えていてもよく、それにより、受信したコンテンツの記録およびその後の再生が可能となる。記憶媒体Ｓ１は、セットトップボックス１０１が接続された何らかの種類のパーソナルデジタルレコーダ（ＰＤＲ）であってもよく、たとえばＤＶＤ＋ＲＷレコーダであってもよい。コンテンツはまた、コンパクトディスク（ＣＤ）またはデジタルバーサタイルディスク（ＤＶＤ）といったような担体１２０に記憶されて、システム１００に供給されてもよい。その後、コンテンツは、ネットワーク１１０を介してレンダリングのためのシンクに転送されてもよい。
【００５４】
シンクは、たとえば、テレビのディスプレイ１０２、携帯型表示機器１０３、携帯電話１０４、および／またはオーディオ再生機器１０５であってもよい。コンテンツ項目がレンダリングされる際の厳密な手法は、機器のタイプおよびコンテンツのタイプに依存する。たとえば、ラジオ受信機内においては、レンダリング処理は、オーディオ信号を生成する工程と、それらの信号をスピーカーに供給する工程とを含む。テレビ受像機については、レンダリング処理は、一般的には、オーディオ信号とビデオ信号とを生成する工程と、それらの信号をディスプレイ画面とスピーカーとに供給する工程とを含む。他のタイプのコンテンツについても、類似の適当な処理が行われなくてはならない。レンダリング処理はさらに、受信した信号の解読またはスクランブル解除、オーディオ信号とビデオ信号との同期化等といった動作を含んでいてもよい。
【００５５】
ある一定の条件下においては、パソコン１０６も、コンテンツ源、記憶媒体、および／またはシンクとして動作し得る。
【００５６】
携帯型表示機器１０３および携帯電話１０４は、ベースステーション１１１を用いて（たとえば、ＢｌｕｅｔｏｏｔｈまたはＩＥＥＥ８０２．１１ｂを用いて）、ネットワーク１１０に無線接続されている。その他の機器は、従来型の有線接続を用いて接続されている。機器１０１から１０６同士のトランスアクションを可能とするため、異なる機器同士がメッセージおよび情報を交換し、相互制御を行うことを可能とする、いくつかの相互運用性規格が利用可能である。１つのよく知られた規格は、２０００年１月に発行された、ＨＡＶｉ（Ｈｏｍｅ　Ａｕｄｉｏ／Ｖｉｄｅｏ　Ｉｎｔｅｒｏｐｅｒａｂｉｌｉｔｙ；ホ

ーム・オーディオ／ビデオ相互運用性）規格、バージョン１．０であり、この規格は、アドレスhttp://www.havi.orgにおいて、インターネット上で入手可能である。他のよく知られた規格としては、Ｄ２Ｂ（ｄｏｍｅｓｔｉｃ　ｄｉｇｉｔａｌ　ｂｕｓ；ドメスティックデジタルバス）規格、ＩＥＣ１０３０に記述されている通信プロトコル、およびＵｎｉｖｅｒｓａｌ　Ｐｌｕｇ　ａｎｄ　Ｐｌａｙ（ユニバーサル・プラグ・アンド・プレイ；http://www.upnp.org）が挙げられる。

【００５７】

ホームネットワーク内の機器１０１から１０６がコンテンツの無許可のコピーを作成しないよう保証することが、重要であることが多い。この保証を行うため、典型的にはデジタル著作権管理（ＤＲＭ）システムと呼ばれる、セキュリティ体制が必要である。そのようなシステムは、典型的には権利を利用するものである。異なるタイプの権利として、コンテンツ権と使用権利とがある。

【００５８】

コンテンツ権は、そのコンテンツに関して何が許可されているかを記述しており、使用権利は、ある人物に特定のコンテンツ権を使用する権限を付与しており、さらにあるユーザーがそのコンテンツで何を行うことを許可されているかを記述していてもよい。

【００５９】

使用権利の例としては、コンテンツを再生する権利、子コピーを作成する権利等が挙げられる。

【００６０】

コンテンツ権と使用権利とのいずれも、暗号鍵も含んでいてもよい。

【００６１】

権利の安全な処理および記憶は、不正変更防止モジュール１０８内において行われ得る。この不正変更防止モジュール１０８は、たとえば中央コントローラ１０１内に配されていてもよい。

【００６２】

図２は、従来技術によって、使用権利がどのように署名され得るかを示している。使用権利は、たとえばレンダリング権利、転送権利、派生的業務の権利、または実用権利を含み得る。期間または回数に関して、有効性が制限された権利もある。この例では、使用権利２０１は、ユーザーが特定のコンテンツ片に対して再生権利を有することを指定するレンダリング権利２０２と、ユーザーが一定量のコンテンツを別の領域にちょうど２回だけ転送する権利を有することを指定する転送権利２０３とを含んでいてもよい。ここでの署名処理は、秘密鍵と公開鍵とのペアの存在に基づいた、よく知られた公開鍵暗号化を利用している。秘密鍵は、その秘密鍵を用いてメッセージに署名しそのメッセージが真正であることを認証した当事者によって、秘密に保たれており、対応の公開鍵は、そのメッセージが確かに署名されたものであり、その送信元の当事者によって署名された後に変更されていないものであることを確認するために、任意の第三者に分配され使用され得る。

【００６３】

この例では、秘密鍵／公開鍵ペア生成器２１０が、使用権利の交付者のために、秘密鍵２１１と公開鍵２１２とのペアを生成している。この交付者は、ここではＰと記すコンテンツプロバイダ自身であってもよい。Ｐは、使用権利２０１の署名処理２１３において、その秘密鍵２１１を用いて、署名２０４を計算する。使用権利２０１と署名２０４との組合せは、検知されない不正変更の危険を伴わずに記憶および転送が可能である、署名された使用権利２０５を構成する。任意の第三者は、公開鍵２１２を用いて、メッセージ２０５が真正のものであるか否かを確認する確認手続き２１４を行うことができる。その回答は、出力２１５として入手可能である。

【００６４】

しかしながら、権利の交付者のみがそのような使用権利２０１に署名することができるので、この組に含まれる権利を、個別に削除または取扱いすることはできない。かかる個別の削除または取扱いは、署名２０４を無効化するからである。安全な環境による保護外

において入手可能であった部分的権利も、そのような部分的権利の（不正）コピーに対する管理が存在しないため、高い信頼性で取り消すことはできない。

【００６５】

本発明は、デジタル署名を無効化することなく、使用権利の取扱いを可能とする。

【００６６】

本発明の第１の実施形態では、使用権利２０１は、実質的に個別に署名される部分的権利に分解される。

【００６７】

図３は、本発明に従う、個別に署名された部分的権利の組３３０を示している。この組は、複数の例示的な部分的権利３０１、３１１、３２１（これより多くてもよい）を含んでいる。Ｐの管理下にあるシステム３５０内において、部分的権利が署名される。ここでも、部分的権利３０１に署名する処理３５３において、署名３０２を計算するために、Ｐの秘密鍵３５１が用いられる。同一の署名処理３５６を用いて、部分的権利３１１に対するＰの署名３１２が計算され、以下同様である。これらの署名された権利は、オプションとして他の署名された権利と共に、個別に署名された部分的権利の新たな組３３０を形成する。各部分的権利は、たとえば署名が有効であるか否かを計算する確認処理３５４、３５７、および３６０（出力は、それぞれ３５５、３５８、および３６１）において、システム３４５内で個別に有効性を確認できるものとなる。この有効性確認は、領域内にある、部分的権利へのアクセスが可能な任意の機器によって実行され得る。かかる機器は、権利が交付者によって取り消されていないか、または交付者自身が取消しを受けていないかを、確認してもよい。

【００６８】

部分的権利を１つの組として扱うことにより、通信のサイズおよびトランスアクション回数が最小化され、使用権利とコンテンツ項目との間の概念上の関係は維持される。

【００６９】

オプションとして、権利の組の完全性の確認を可能とするため、個別に署名された部分的権利の全体の組３３０が、処理３７３において、全体として署名されてもよい。署名は、ここでもシステム３６９内において、サービスプロバイダによって行われてもよいが、図３に示すように、別の信任された第三者Ｔによって、鍵ペア生成器３７０により生成されたＴ自身の秘密鍵／公開鍵のペア３７１／３７２を用いて行われてもよい。確認処理３７４は、署名された権利の組３４０が完全な組であるか否かを示す出力回答３７５を与える。

【００７０】

上記の本発明の第１の実施形態の１つの利点は、部分的権利が、署名により個別に保護され、したがって領域内で自由にかつ独立に流通できる点である。そのため、これらの部分的権利は、個別に処理（たとえば取消し）され得る。

【００７１】

この第１の実施形態の１つのバリエーションでは、個別に署名された部分的権利の全体の組は、処理３７３において、その権利の組の受信者（たとえばユーザー）自身の秘密鍵／公開鍵のペア３７１／３７２によって署名されてもよい。その結果は、たとえばその権利の組の交付者へと返送されてもよい。このことは、その権利の全体の組が意図した受信者に到達したことを、交付者が実証できるようにするための、トランスアクションの一部とされ得る。

【００７２】

本発明の第２の実施形態においては、署名された部分的権利のいくつかまたは全部を、１つの領域（送信元領域）から別の領域（受信領域）へと転送することが可能とされる。

【００７３】

図４は、図３に示したような部分的権利に、どのようにして追加情報および署名が追加され、その後署名されて、転送される権利（以下、転送可能な権利と呼ぶ）が形成されるのかを示している。転送可能な権利は、好ましくは、図１のモジュール１０８のような上

記の不正変更防止モジュール内から構成された権利である。この転送可能な権利は、部分的権利３１１を含んでおり、さらに、Ｐによる署名処理３５６によって生成された、いまだ有効な当初の署名３１２を含んでいる。加えて、送信元の領域についての識別子、受信領域についての識別子、転送の理由または目的、転送時間、有効期間に関する情報（ただしこれらに限定されるものではない）を含む、メタデータ４１１が追加される。送信元の領域および受信領域についての識別子としては、それら各々の公開鍵を用いることが好ましい。部分的権利３１１、対応の署名３１２、および追加情報４１１が、一体に構成されて情報４３０とされ、その後、処理４６３において、送信元の領域によって、その送信元の領域の秘密鍵４６１を用いて、署名４３１を形成するように署名がなされる。転送可能な権利４４０は、情報４３０および署名４３１の双方を含んでおり、それらの有効性および真正性は、処理４６４において、任意の第三者によって、送信元の領域の公開鍵４６２を用いて確認されることができる。

【００７４】

図５は、いずれも図１のシステム１００に類似した、２つの領域５００および５５０を示している。この図には、処理５４０において、おそらくは安全な通信を用いて、領域５００の外部へと、さらに別の領域５５０へと転送されている途中の、転送可能な権利４４０が示されている。この転送は、好ましくは、それぞれの領域内の通信機器１０１および５０１が、適合性を有し、取消しを受けていないものとして互いを確認した後に行われる。送信元の領域５００は、転送された権利を、ローカルにおいて取消しまたは削除してもよい。

【００７５】

本発明のこの実施形態は、転送される権利の送信元の領域とターゲット領域との両方を、転送可能な権利に含まれる署名およびメタデータから高い信頼性で取得することができるという、さらなる利点を有する。このことは、コンテンツのトラッキングを可能とする。

【００７６】

本発明の第３の実施形態では、異なる種々のタイプの権利およびそれら権利の取扱いに対する、異なる種々の保護レベルが区別される。

【００７７】

部分的権利の中には、たとえば特定のコンテンツ片を再生するローカルな権利といったような、たとえ暗号化された送信や安全な記憶による保護がなくても、１つの領域内において自由に用いることができる権利がある。これらの権利は、「安全な権利」と呼ばれる。安全な権利は、承認領域（ＡＤ）内において、自由に流通することができる。また、たとえばあるコンテンツ片を１回のみ転送する権利といったような、使用直後に取消しまたは削除を行わなくてはならない権利もある。これらの権利は、「弱い権利」と呼ばれる。弱い権利は、不正な複製や不正変更からの保護を必要とし、かつ、たとえばそれらの権利は限られた回数のみ交付が可能であること等を順守させなくてはならない。たとえば、安全な環境（たとえば、別の領域への権利の転送の処理も行う、おそらくは中央コントローラ内にある不正変更防止モジュール内）による保護外においては弱い権利を許容しないようにすることによって、上記の保護を提供することが可能である。当然ながら、２つ以上の保護レベルを規定することも可能である。

【００７８】

ある特定の権利に対する必要最小限の保護を示す１つの可能な方法は、その情報を有するフィールドを追加する方法である。図６は、図３に示した個別に署名された権利の署名済の組３４０に類似の、権利の組の変更例６４０を示している。最も単純な形態では、追加の単一ビットフィールド６０１／６１１が、権利３０１／３１１が安全な記憶内に拘束されなくてはならないか否かを示す。たとえば、権利３０１は、安全な記憶を必要としない再生権利（ビットフィールド６０１内にある例示的なコンテンツは０）であってもよく、一方、権利３１１は、安全な記憶を必要とする権利（ビットフィールド６１１内にある例示的なコンテンツは１）である。必要最小限の保護レベルを示す代替方法としては、権

利のタイプに基づいて取得される保護レベルを機器が決定する方法、または各権利について必要な保護レベルを示した（更新可能な）リストを機器が有している方法が含まれるが、これらに限定されるものではない。

【００７９】

この必要最小限の保護レベルは、その部分的権利がどのように取り扱われるべきかを決定するために利用可能である。

【００８０】

本発明の第４の実施形態では、ユーザー／所有者の近くに配された機器を用いてホームネットワークを拡張（一時的な拡張であるかもしれない）するための、領域外への権利の転送が説明される。この拡張は、部分的権利内での指定またはその他の理由（たとえば公正な使用のため）により、そのコンテンツにアクセスする権限を与えられた、別の所有者の機器への拡張であってもよい。

【００８１】

欧州特許出願第０２０７９３９０．７号（整理番号ＮＬ０２１０６３）には、ある人物が、ホームネットワークの当初の定義外から遠隔で（たとえば旅行中において）、自己の個人的なコンテンツを閲覧または使用することを可能とする、ＡＤの枠組の拡張が記載されている。この出願においては、コンテンツの暗号化、対応の暗号化鍵の安全な記憶、および信任された第三者により生成された署名によって保護される個人のものとされた使用権利により、安全が確保される。

【００８２】

そのような状況においては、使用権利の一部のみを伝送できるようにするのが有利である。かかる伝送は、本発明による個別署名を用いれば可能である。図７は、図１に示すようなシステム１００から、遠隔のホテルのテレビシステム７７０の、たとえば承認されたユーザーの近くにあるテレビ７５２またはオーディオセット７５３への、ゲートウェイ７５１を経由した、転送可能な権利７３１の転送処理７３０を示している。これらの機器は、ホテルの部屋やラウンジ等に置かれ得る。

【００８３】

本発明の第５の実施形態では、転送権利はサービスプロバイダにおいて保持され、所有者は、別の人物または領域に権利を転送すべきことを、そのサービスプロバイダに伝達する。

【００８４】

転送権利の存在を示すために、本願の説明においては、オファー権利が導入されてきた。

【００８５】

このケースでは、許可された数のコピーのみが作成できるようにサービスプロバイダが監視を行うことが可能であるので、不正な複製の防止目的での安全な記憶は必要ではない。

【００８６】

図８は、ホームネットワークシステム１００によるオファー権利の利用を示している。ホームネットワーク外のシステム５５０への使用権利８３１の転送８３０を要求するため、通信処理８２０において、オファー権利８２１がプロバイダ８１０へと送られる。サービスプロバイダは、転送権利を記憶部８１１内に保持していてもよいし、必要なときに生成器８１２を用いて転送権利を生成してもよい。

【００８７】

変更例も可能である。上記の説明において、「含む」および「備える」との語は、他の要素または工程の存在を排除するものではなく、「１つの」との語は複数あることを排除するものではない。また、単一の処理装置その他のユニットが、特許請求の範囲において列挙されたいくつかの手段の機能を果たしてもよい。

【図面の簡単な説明】

【００８８】

【図１】ネットワークを介して相互接続された複数の機器を含むシステムの概略図
【図２】従来技術によるデジタル署名された権利を示した図
【図３】本発明に従い、個別に署名された部分的権利の組を示した図
【図４】本発明に従い、交付者によって転送および署名された権利を示した図
【図５】２つの領域間における上記の権利の転送を示した図
【図６】必要な保護レベルを示すために、それぞれの権利と関連付けられたフィールドを示した図
【図７】ホームネットワーク外の場所への、個別に署名された権利の伝送を示した図
【図８】プロバイダからホームネットワーク外の場所への、使用権利の転送を要求するために用いられる、オファー権利を示した図

【図１】

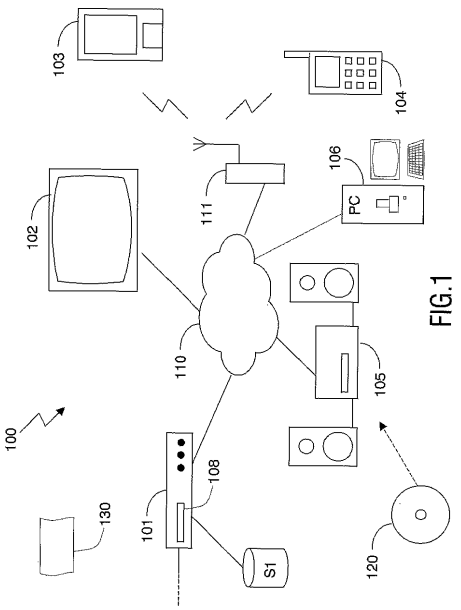

FIG.1

【図２】

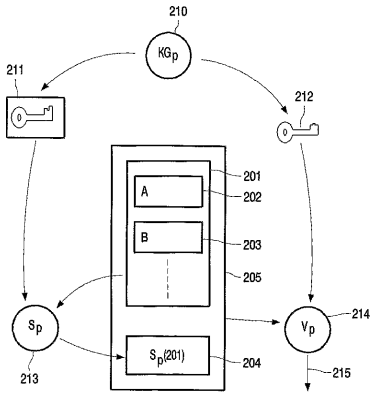

FIG. 2

【図３】

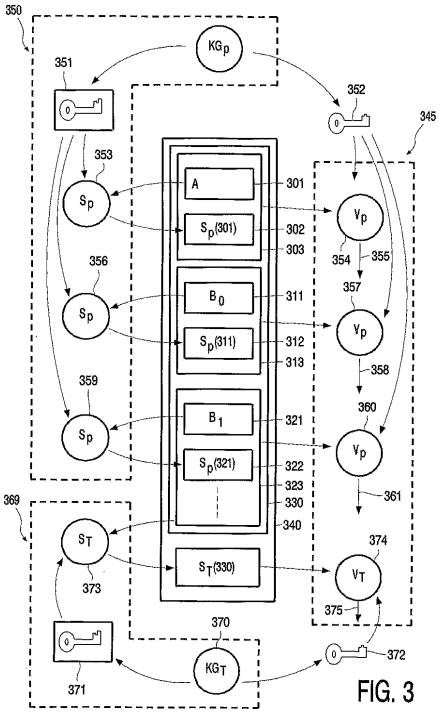

FIG. 3

【図４】

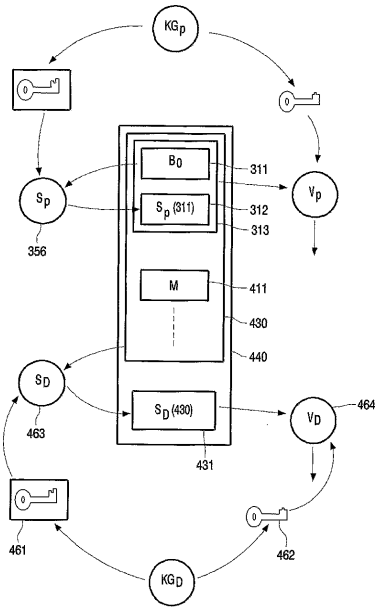

FIG. 4

【図５】

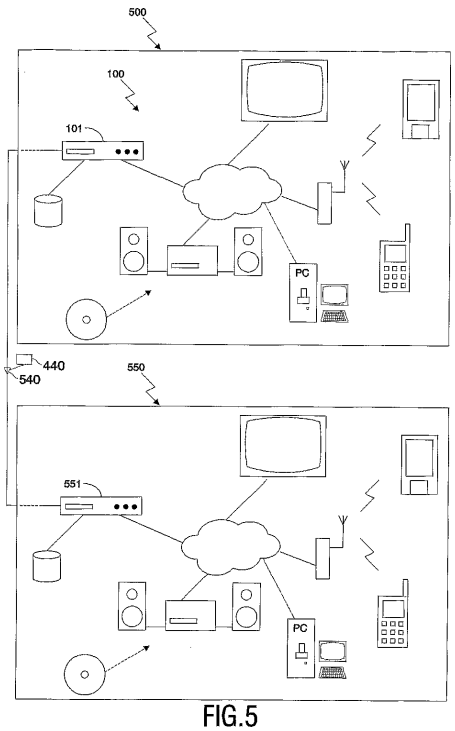

FIG.5

【図６】

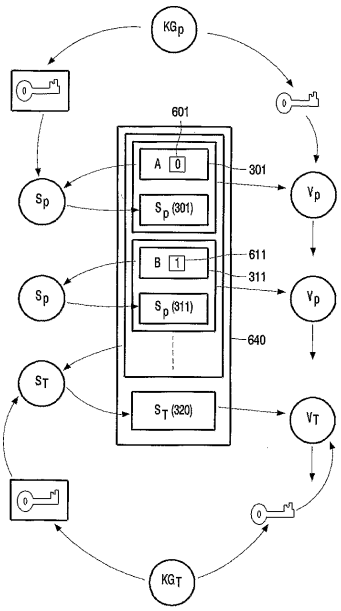

FIG. 6

【図７】

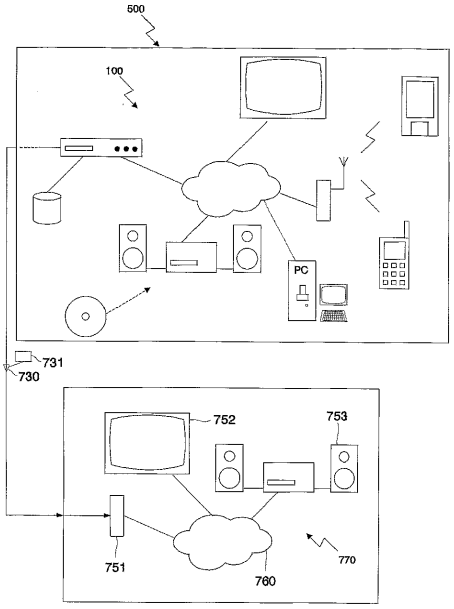

FIG.7

【図８】

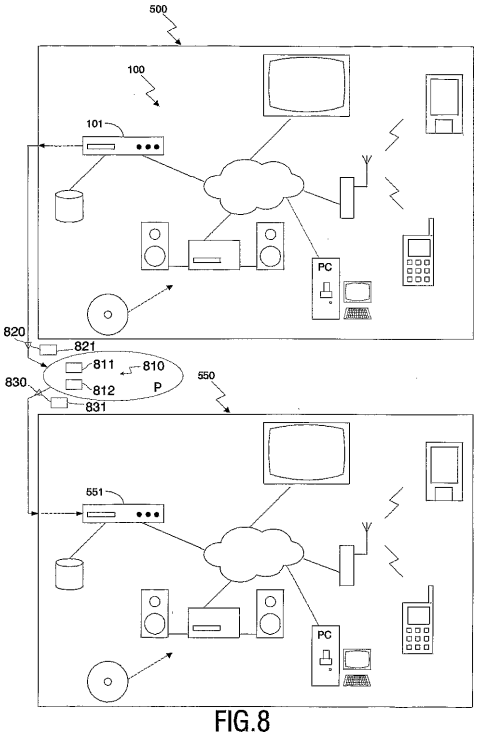

FIG.8

フロントページの続き

(51)Int.Cl. FI
G06F 17/60 142

(72)発明者 カンペルマン フランシスカス エル エイ ジェイ
オランダ国 ５６５６ アーアー アインドーフェン プロフ ホルストラーン 6
(72)発明者 スヒレイエン ヘールト ジェイ
オランダ国 ５６５６ アーアー アインドーフェン プロフ ホルストラーン 6
(72)発明者 ファン デン ヘルフェル セバスティアーン エイ エフ エイ
オランダ国 ５６５６ アーアー アインドーフェン プロフ ホルストラーン 6

審査官 宮司 卓佳

(56)参考文献 特開２００１－０７５８６８（ＪＰ，Ａ）
特開平１０－００３７４５（ＪＰ，Ａ）
特開２００１－２５６４１３（ＪＰ，Ａ）
国際公開第０１／０６３３８７（WO，Ａ１）
特開２００２－３５９６１６（ＪＰ，Ａ）
特開２００１－０９４５５４（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F 21/22
G06F 1/00
G06F 21/24
G06Q 50/10