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

特許第5122468号
(P5122468)

(45)発行日　平成25年1月16日(2013.1.16)　(24)登録日　平成24年11月2日(2012.11.2)

(51)Int.Cl.　　F I
G06F 21/10 (2013.01)　　G06F 21/22 110N
H04L 9/08 (2006.01)　　H04L 9/00 601B
H04L 9/00 601E

請求項の数 10　(全 15 頁)

(21)出願番号　特願2008-536080 (P2008-536080)
(86)(22)出願日　平成18年10月17日 (2006.10.17)
(65)公表番号　特表2009-512085 (P2009-512085A)
(43)公表日　平成21年3月19日 (2009.3.19)
(86)国際出願番号　PCT/FR2006/002328
(87)国際公開番号　WO2007/045756
(87)国際公開日　平成19年4月26日 (2007.4.26)
審査請求日　平成21年10月13日 (2009.10.13)
(31)優先権主張番号　0510566
(32)優先日　平成17年10月17日 (2005.10.17)
(33)優先権主張国　フランス(FR)

(73)特許権者　501263810
トムソン　ライセンシング
Ｔｈｏｍｓｏｎ　Ｌｉｃｅｎｓｉｎｇ
フランス国，　９２１３０　イツシー　レ　ムーリノー，　ル　ジヤンヌ　ダルク，　１－５
１－５，　ｒｕｅ　Ｊｅａｎｎｅ　ｄ’Ａｒｃ，　９２１３０　ＩＳＳＹ　ＬＥＳ　ＭＯＵＬＩＮＥＡＵＸ，　Ｆｒａｎｃｅ
(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】デジタルデータを記録し、セキュアに配信する方法、アクセス装置及びレコーダ

(57)【特許請求の範囲】
【請求項１】
マルチメディアコンテンツを表すデジタルデータを受信してセキュアに記録する方法であって、
幾つかの機器のアイテムを有し、そのドメインの全ての機器に固有の識別子により定義される予め決定されたセキュアなドメインに属するレコーダ／レシーバによりセキュアなディスクに前記デジタルデータを記録するステップと、
前記レコーダ／レシーバのドメイン識別子をセキュアなディスクに記録して、このドメインを、前記マルチメディアコンテンツのコピーが許可されるドメインとして定義するステップとを含み、
前記ディスクは、記録可能なメディアのデータプロテクションシステムによりセキュアにされ、前記ドメイン識別子は、あるドメインにおいてデータプロテクションシステムにより定義され、
当該方法は、前記記録可能なメディアのデータプロテクションシステムに従って前記セキュアなディスクからディスクキーを取得する事前のステップを更に含み、
前記記録可能なメディアの前記データプロテクションシステムに従って前記記録されたデジタルデータがタイトルキーによりスクランブルされた場合、前記ドメイン識別子は前記ディスクキーにより暗号化され、
前記タイトルキーは、前記記録可能なメディアのデータプロテクションシステムに従って前記ディスクキーにより暗号化される、方法。

【請求項２】
前記マルチメディアコンテンツに付属する複製権を前記セキュアなディスクに記録するステップを更に含み、
前記複製権は、前記マルチメディアコンテンツが自由にコピー可能であるか、前記マルチメディアコンテンツが決定されたドメインでのみコピー可能であるか、又は前記マルチメディアコンテンツがコピー不可能であるかを定義する、
ことを特徴とする請求項１記載の受信及びセキュアに記録する方法。
【請求項３】
マルチメディアコンテンツを表すデジタルデータをセキュアに配信する方法であって、
記録可能なメディアのデータプロテクションシステムに従ってレコーダ／レシーバからセキュアなディスクにマルチメディアコンテンツを表すデジタルデータを受信し、記録するステップと、前記記録ステップは、請求項１又は２記載の受信及びセキュアに記録する方法により実行され、
ある識別子により定義される特定のセキュアなドメインの識別子を記憶する手段を有する前記特定のセキュアなドメインにアクセスする装置から、あるドメインにおけるデータプロテクションシステムに従って、前記特定のセキュアなドメインにおいて、前記記録されたデジタルデータをセキュアに供給するステップとを含み、
前記供給ステップは、
前記セキュアなディスクで、前記アクセス装置により決定されたセキュアなドメインの識別子を読取るステップと、
前記セキュアディスクで読取られた識別子を、前記アクセス装置の記憶手段に記憶される識別子と比較するステップと、
前記セキュアディスクで読取られた識別子が前記アクセス装置の記憶手段に記憶された識別子に一致しないとき、前記デジタルデータの第一の動作モードを許可するように、前記デジタルデータを前記アクセス装置により供給するステップと、
前記セキュアなディスクで読取られた識別子が前記アクセス装置の記憶手段に記憶された識別子に一致するとき、前記デジタルデータの第二の動作モードを許可するように、前記デジタルデータを前記アクセス装置により供給するステップと、を含むセキュアな配信方法。
【請求項４】
前記デジタルデータの第一の動作モードを許可するように前記デジタルデータが供給されるとき、前記供給ステップは、適切なプロトコルに従って前記アクセス装置により前記デジタルデータをスクランブリングし、前記マルチメディアコンテンツのコピーを禁止し、前記デジタルデータが前記アクセス装置により読取られている間にのみ前記特定のセキュアなドメインに属する表示装置での前記マルチメディアコンテンツの表示を許可するステップを含む、
請求項３記載のセキュアな配信方法。
【請求項５】
前記デジタルデータの第二の動作モードを許可するように前記デジタルデータが供給されるとき、前記供給ステップは、
前記セキュアなディスクにプリレコードされる複製権を前記アクセス装置により読取るステップと、
前記マルチメディアコンテンツに付属する複製権を前記セキュアディスクで読取るステップと、前記複製権は、前記マルチメディアコンテンツが自由にコピー可能であるか、マルチメディアコンテンツが予め決定されたドメインでのみコピー可能であるか、又は前記マルチメディアコンテンツがコピー不可能であるかを定義し、
前記セキュアなディスクで読取られた複製権に従って定義されたプロトコルに従い、前記アクセス装置により前記デジタルデータをスクランブリングするステップと、
を含む請求項３又は４記載のセキュアな配信方法。
【請求項６】

読取られた複製権が前記予め決定されたドメインでのみ前記マルチメディアコンテンツのコピーを許可するとき、前記供給するステップは、適切なプロトコルに従って前記アクセス装置により前記デジタルデータをスクランブリングし、前記予め決定されたドメインに属する機器でのみ前記マルチメディアコンテンツのコピー及び表示を許可する、
請求項５記載のセキュアな配信方法。
【請求項７】
前記複製権が前記マルチメディアコンテンツのコピーを禁止するとき、前記供給ステップは、適切なプロトコルに従って前記アクセス装置により前記デジタルデータをスクランブリングし、前記マルチメディアコンテンツのコピーを禁止し、前記デジタルデータが前記アクセス装置により読み取られる間、前記予め決定されたドメインに属する表示装置でのみ前記マルチメディアコンテンツの表示を許可する、
請求項５記載のセキュアな配信方法。
【請求項８】
前記複製権が前記マルチメディアコンテンツの自由なコピーを許可するとき、前記供給ステップは、適切なプロトコルに従って前記アクセス装置により前記デジタルデータをスクランブリングし、任意の機器での前記マルチメディアコンテンツのコピー及び表示を許可する、
請求項５記載のセキュアな配信方法。
【請求項９】
特定のセキュアなドメインにアクセスする装置であって、
記録可能なメディアのデータプロテクションシステムによりセキュアにされたディスクに記録されているマルチメディアコンテンツを表すデジタルデータを読取り、予め決定されたセキュアなドメインの識別子が、あるドメインにおいてデータプロテクションシステムにより定義されている場合に、セキュアなディスクで、前記予め決定されたセキュアなドメインの識別子を読み取る読取手段と、
当該アクセス装置が属する特定のドメインの識別子を記憶する手段と、
前記記憶手段に記憶された識別子を前記セキュアなディスクで読取られた識別子と比較し、ディスクキーを使用してドメイン識別子を復号する手段と、
前記セキュアなディスクで読取られた識別子が当該アクセス装置の前記記憶手段に記憶された識別子に一致しないとき、前記デジタルデータの第一の動作モードを許可するように、前記デジタルデータを供給し、前記セキュアなディスクで読取られた識別子が当該アクセス装置の記憶手段に記憶された識別子に一致するとき、前記デジタルデータの第二の動作モードを許可するように、前記デジタルデータを供給する手段とを含み、
前記記録可能なメディアのデータプロテクションシステムに従って前記セキュアなディスクからディスクキーを取得し、前記ディスクキーを使用して前記ドメイン識別子を復号する暗号／復号手段と、
前記ディスクキーを使用して前記セキュアなディスクに記録された前記デジタルデータをデスクランブル可能なスクランブリング／デスクランブリング手段と、を更に含むアクセス装置。
【請求項１０】
幾つかの機器のアイテムを有するセキュアなドメインであって、前記ドメインの全ての機器に固有の識別子により定義されるセキュアなドメインに属するレコーダ／レシーバであって、
当該レコーダ／レシーバは、マルチメディアを表すデジタルデータを、記録可能なメディアのデータプロテクションシステムによりセキュアにされたディスクに記録し、
当該レコーダ／レシーバは、当該レコーダ／レシーバのドメイン識別子があるドメインにおいてデータプロテクションシステムにより定義されている場合に、前記ドメイン識別子を前記セキュアディスクに記録し、このドメインを、前記マルチメディアコンテンツのコピーが許可される唯一のドメインとして定義し、
当該レコーダ／レシーバは、前記記録可能なメディアのデータプロテクションシステム

に従って前記セキュアなディスクからディスクキーを取得し、前記記録可能なメディアのデータプロテクションシステムに従ってタイトルキーにより前記デジタルデータをスクランブルし、前記タイトルキーは、前記記録可能なメディアのデータプロテクションシステムに従って前記ディスクキーにより暗号化され、前記ディスクキーを使用して前記識別子を暗号化し、前記スクランブルされたデジタルデータ及び前記暗号化された識別子を記録する、レコーダ／レシーバ。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、マルチメディアコンテンツを表すデジタルデータを記録、表示及びセキュアに配信する方法に関する。

【背景技術】

【０００２】

マルチメディアの違法なコピーを回避するため、文献ＪＰ２００１／１９５８２６は、それぞれの機器に固有の識別子であって、他の機器の識別子とは異なる識別子を記憶するメモリを有する機器を開示している。この機器は、それぞれの記録に関して記憶媒体にデジタルデータとそれ自身の識別子を記憶するように構成される。デジタルデータを読取る前に、その識別子を記憶媒体で読取られた識別子と比較し、記憶媒体に記憶されている識別子がその識別子に一致するときにのみデジタルデータを表示する。

【０００３】

この機器は、所有権を監視するが、デジタルデータが固有の機器でのみ表示されるのを可能にする。

【０００４】

デジタルデータに付着する所有権を監視しつつ、デジタルデータのより広い配信を可能にするため、コンテンツスクランブリングシステム（ＣＳＳ）システムのようなデータプロテクション方法により、セキュアＤＶＤに記録されるデジタルデータを保護することが知られている。

【０００５】

しかし、この方法によれば、セキュアＤＶＤに記録されたデジタルデータは、許可されたドライブにより読取ることができるが、コピー又は複製することができない。

【０００６】

さらに、文献“SmartRight Technical white paper, Version 1.7, January 2003, Thomson”に記載される登録商標“SmartRight”による方法、及び文献“xCP: eXtensible Content Protection. 2003. IBM”及び文献“xCP Cluster Protocol, IBM Presentation to Copy Protection Technical Working Group, July 18, 2002”に記載される登録商標“eXtensible Content Protection”による方法のような、あるドメインにおけるデータプロテクション方法が知られている。これらの方法は、同じドメインに属する機器によってのみデコードすることができる暗号化プロトコルに従って、デジタルデータがスクランブルされるのを可能にする。正しく暗号化されたデジタルデータは、あるドメインに属する機器によってのみ提供されるか、又はコピー／複製される。

【０００７】

しかし、このデジタルデータは、このドメインへのアクセスを有さない人物と共有することができない。したがって、このデジタルデータを友人又は知人と共有することができない。

【０００８】

また、米国特許文献２００４／０２３０５３２から特に知られるものは、デジタルデータコピーマネージメントシステムであり、同一のレコーダによりデジタルデータの１以上の複製／コピーを可能にするが、別のレコーダによる複製を禁止する。

【０００９】

このシステムは、インターネットネットワーク介してアクセスすることができるサーバ

、及びユーザ向けに意図される特定のレコーダ／ドライバを有する。それぞれの記録に関して、それぞれのレコーダ／ドライブは、それに固有の識別子、ＤＶＤの識別子及びＤＶＤで読取られるコンテンツの識別子をサーバに送信されるように構成される。このサーバは、データベース、レコーダにより受信される識別子を登録する手段、そのデータベースに記憶される識別子とレコーダにより受信される識別子とを比較して、レコーダにより送出された識別子がデータベースに既に記憶されている識別子に対応するかがチェックされる。

【発明の開示】

【発明が解決しようとする課題】

【００１０】

しかし、このシステムは、複雑であり、大量のデータを含むデータベースの管理を必要とする。

【００１１】

本発明の目的は、デジタルデータに付着する所有権を監視しつつ、デジタルデータの所定の程度の共有を可能にする、デジタルデータをセキュアに配信する方法を提案することにある。

【課題を解決するための手段】

【００１２】

上記目的を達成するため、本発明は、マルチメディアコンテンツを表すデジタルデータを受信してセキュアに記録する方法であって、幾つかの機器のアイテムを有し、そのドメインの全ての機器に固有の識別子により定義される予め決定されたセキュアなドメイン（secured domain）に属するレコーダ／レシーバによりセキュアディスク（secured disk）に前記デジタルデータを記録するステップ、レコーダ／レシーバのドメイン識別子をセキュアディスクに記録して、マルチメディアコンテンツの複製／コピーが許可されるドメインとして、このドメインを定義するステップを含み、本方法は、セキュディスクからディスクキーを取得する事前のステップを含み、ドメイン識別子は、前記ディスクキーにより暗号化され、記録されたデジタルデータは、タイトルキーによりスクランブルされ、前記タイトルキーは、前記ディスクキーにより暗号化される。

【００１３】

特定の実施の形態によれば、受信及び記録方法は、マルチメディアコンテンツに付着する複製権をセキュアディスクに記録するステップを含み、この複製権は、マルチメディアコンテンツが自由に複製可能／コピー可能であるか、マルチメディアコンテンツが決定されたドメインでのみ再生可能／コピー可能であるか、又はマルチメディアコンテンツが再生可能／コピー可能であるかを定義する。

【００１４】

また、本発明は、第二の態様によれば、マルチメディアコンテンツを表すデジタルデータをセキュアに配信する方法に関し、以下のステップを含む。レコーダ／レシーバからセキュアディスクにマルチメディアコンテンツを表すデジタルデータを受信し、記録するステップ。記録ステップは、上述された受信及び記録方法により実行される。特定のセキュアなドメインの識別子を記憶する手段を有する特定のセキュアなドメインにアクセスする装置から、ある識別子により定義される特定のセキュアなドメインにおいて、前記記録されたデジタルデータをセキュアに供給するステップ。供給ステップは、以下のステップを有する。

【００１５】

セキュアディスクで、アクセス装置により決定されたセキュアなドメインの識別を読取るステップ。セキュアディスクで読取られた識別子をアクセス装置の記憶手段に記憶される識別子と比較するステップ。セキュアディスクで読取られた識別子がアクセス装置の記憶手段に記憶された識別子に一致しないとき、デジタルデータの第一の動作モードを認可するように、デジタルデータをアクセス装置により供給するステップ。セキュアディスクで読取られた識別子がアクセス装置の記憶手段に記憶された識別子に一致するとき、デジ

タルデータの第二の動作モードを認可するように、デジタルデータをアクセス装置により供給するステップ。

【００１６】

特定の実施の形態によれば、配信方法は、以下の特性のうちの１以上を有する。デジタルデータの第一の動作モードを認可するように、デジタルデータが供給されるとき、供給ステップは、適切なプロトコルに従ってアクセス装置によりデジタルデータをスクランブリングし、マルチメディアコンテンツの複製／コピーを禁止し、デジタルデータがアクセス装置により読取られている間にのみ特定のドメインに属する表示装置でのマルチメディアコンテンツの表示を認可するステップ。第二の動作モードを認可するようにデジタルデータが供給されるとき、供給ステップは、以下のステップをも有する。セキュアディスクに前もって記録された複製権をアクセス装置により読取るステップ。マルチメディアコンテンツに付着する複製権をセキュアディスクで読取るステップ。複製権は、マルチメディアコンテンツが自由に複製可能／コピー可能であるか、マルチメディアコンテンツが予め決定されたドメインでのみ複製可能／コピー可能であるか、又はマルチメディアコンテンツが複製可能／コピー可能でないかを定義する。セキュアディスクで読取られた複製権に従って定義されたプロトコルに従い、アクセス装置によりデジタルデータをスクランブリングするステップ。読取られた複製権が決定されたドメインのみにおけるマルチメディアコンテンツの複製／コピーを許可するとき、供給するステップは、適切なプロトコルに従ってアクセス装置によりデジタルデータをスクランブリングし、決定されたドメインに属する機器でのみマルチメディアコンテンツの複製／コピー及び表示を認可する。複製権がマルチメディアコンテンツの複製／コピーを禁止するとき、供給ステップは、適切なプロトコルに従ってアクセス装置によりデジタルデータをスクランブリングし、マルチメディアコンテンツの複製／コピーを禁止し、デジタルデータがアクセス装置により読み取られる間、決定されたドメインに属する表示装置でのマルチメディアコンテンツの表示のみを認可する。複製権がマルチメディアコンテンツの自由な複製／コピーを認可するとき、供給ステップは、適切なプロトコルに従ってアクセス装置によりデジタルデータをスクランブリングし、任意の機器でのマルチメディアコンテンツの複製／コピー及び表示を認可する。本方法は、リモートサーバから前記レコーダ／レシーバにマルチメディアコンテンツに付着された複製権を送信するステップを含む。送信ステップは、複製権を記録するステップの前のステップである。本方法は、識別子及び複製権を暗号化するステップを含み、前記暗号化ステップは、記録ステップの前のステップである。

【００１７】

また、本発明は、第三の態様によれば、特定のセキュアなドメインにアクセスする装置に関し、当該アクセス装置は、以下を有する。セキュアディスクに記録されているマルチメディアコンテンツを表すデジタルデータを読取る手段。この読取手段は、セキュアディスクで決定されたセキュアなドメインの識別子を読み取るために適する。当該アクセス装置が属する特定のドメインの識別子を記憶する手段。記憶手段に記憶された識別子をセキュアディスクで読取られた識別子と比較し、ディスクキーを使用してドメイン識別子を復号する手段。セキュアディスクで読取られた識別子が当該アクセス装置の記憶手段に記憶された識別子に一致しないとき、デジタルデータの第一の動作モードを認可するように、デジタルデータを供給し、セキュアディスクで読取られた識別子が当該アクセス装置の記憶手段に記憶された識別子に一致するとき、デジタルデータの第二の動作モードを認可するように、デジタルデータを供給する手段。また、当該アクセス装置は、以下を有する。セキュアディスクからディスクキーを取得し、ディスクキーを使用してドメイン識別子を復号する暗号／復号手段。前記ディスクキーを使用してセキュアディスクに記録されたデジタルデータをデスクランブル可能なスクランブリング／デスクランブリング手段。

【００１８】

また、本発明は、第四の態様によれば、幾つかの機器のアイテムを有するセキュアなドメインであって、前記ドメインの全ての機器に固有の識別子により定義されるセキュアなドメインに属するレコーダ／レシーバに関し、当該レコーダ／レシーバは、マルチメディ

アを表すデジタルデータをセキュアディスクに記録し、当該レコーダ／レシーバは、レコーダ／レシーバのドメイン識別子をセキュアディスクに記録して、このドメインを、マルチメディアコンテンツの複製／コピーが認可される唯一のドメインとして定義する。当該レコーダ／レシーバは、セキュアディスクからデジタルデータを取得し、前記ディスクキーにより暗号化されているタイトルキーによりデジタルデータをスクランブルし、ディスクキーを使用して識別子を暗号化し、前記スクランブルされたデジタルデータ及び前記暗号化された識別子を記録する。

【００１９】

特定の実施の形態によれば、当該レコーダ／レシーバは、以下の特性の１以上を有する。マルチメディアコンテンツに付着する複製権を記録するのに適する。複製権は、マルチメディアコンテンツが自由に複製可能／コピー可能であるか、マルチメディアコンテンツが決定されたドメインのみにおいて複製可能／コピー可能であるか、マルチメディアコンテンツが複製不可能／コピー不可能であるか、を定義する。マルチメディアコンテンツに付着する複製権は、マルチメディアコンテンツの許可される複製回数を含む。

【００２０】

本発明は、例として、図面を参照しながら与えられる以下の説明を読んで良好に理解されるであろう。

【発明を実施するための最良の形態】

【００２１】

本発明に係る方法が実現されるシステム２は、図１及び図２で例示される。このシステム２は、ＤＶＤレコーダ又はＤＶＤドライブの何れかを有し、異なるユーザに属し、ＤＶＤを交換する可能性があるＩＴ機器のアイテムのセットに関する。機器のアイテムは、異なるセキュアなドメイン間で分配される。

【００２２】

１つのセキュアなドメインに属する機器のアイテムは、このドメインを表す同一の識別子及びドメインのキーをメモリにそれぞれ有する。このドメインにおける機器は、ネットワークを介して、このドメインのキーによりスクランブルされるデジタルデータを伝達する。このセキュアなドメインに属さない機器、又は別のセキュアなドメインに属する機器は、このネットワークを伝達されるスクランブルされたデータ、又はネットワークにおける機器でセキュアにされるスクランブルされたデータを読取ることができない。

【００２３】

図１において分かるように、システム２は、レシーバ装置６に、インターネットネットワークのようなディストリビューションネットワーク８を介して、デジタルデータを供給するコンテンツプロバイダ４を有する。

【００２４】

コンテンツプロバイダ４は、データベース１２にリンクされるマルチメディアサーバ１０を有する。

【００２５】

データベース１２は、たとえばオーディオ、ビデオ又は原文データの系列、若しくはソフトウェアをセットアップするために使用されるコンピュータデータファイルのような、マルチメディアコンテンツを表すデジタルデータを記憶する。

【００２６】

デジタルデータは、たとえばＭＰＥＧ規格（ＩＳＯ／ＩＥＣ１３８１８－１）に従ってパケット形式でエンコードされる。

【００２７】

データベース１２では、それぞれのマルチメディアコンテンツは、１以上のユーセージ又は複製権に関連され、これらのユーセージ又は権利に従って変動する価格に関連される。

【００２８】

ユーセージ（usage）は、マルチメディアコンテンツのコピー又は複製に付着するプロ

テクションのタイプを識別する。記載される実施の形態の例では、ユーセージは、マルチメディアコンテンツが自由にコピー可能／複製可能であるか、セキュアＤＶＤにコピーすることができるか、又は、セキュアＤＶＤにコピー可能であって、セキュアＤＶＤにコンテンツを記録したレコーダが属するドメインに対応する単一のドメインにおいてコピー可能／複製可能であるかを定義する。

【００２９】

マルチメディアサーバ１０は、デジタルデータをディストリビューションネットワーク８に送出するか、デジタルデータをこのネットワークから受信する手段１４、及びこのデジタルデータをスクランブリングするモジュール１６を有する。

【００３０】

スクランブリングモジュール１６は、ＣＳＳシステムに従ってデータをスクランブリングする。

【００３１】

レシーバ装置６は、コンピュータ又はセットトップボックスである。このレシーバ装置は、ディストリビューションネットワーク８を介してビデオプログラムにアクセスするのを望むユーザの家に通常設けられる。

【００３２】

レシーバ装置６は、たとえば登録商標SmartRightをもつシステムのようなプロテクションシステムによりセキュアにされるドメインに属する。

【００３３】

このセキュアなドメインに属する機器アイテムは、このドメインを表す同一の識別子とドメインの鍵ＤＩＫをメモリにそれぞれ有する。

【００３４】

レシーバ装置６は、プロセッサ１８、暗号／復号モジュール２０、キーボード、スクリーン又はリモートコントロールタイプのユーザインタフェース２２、データを送信又は受信するネットワークインタフェース２４を有する。

【００３５】

プロセッサ１８は、SmartRightデータプロテクションシステムのプロトコル、及び、スクランブリングモジュール１６により使用されるプロテクションシステムに対応するＣＳＳプロテクションシステムのプロトコルを実行する。このため、プロセッサ１８は、特に、レシーバ装置６が属するドメインのマスターキーＭＫ及び識別子ＩＤＤを有する。

【００３６】

インタフェース２４は、リアルタイムのダウンロード（又はストリーミング）することで、すなわちロードしながらコンテンツを視聴するか、又は事前にダウンロードして、オフラインでコンテンツが視聴されるのを可能にすることで、ディストリビューションネットワーク８からデータストリームを受信する。

【００３７】

受信機装置６は、たとえばＤＶＤ－Ｒ、ＤＶＤ－ＲＷ、ＤＶＤ＋Ｒ、ＤＶＤ＋ＲＷ又はＤＶＤ－ＲＡＭタイプのＤＶＤ３０のレコーダ２８にリンクされる。

【００３８】

ＤＶＤ３０は、ＣＳＳプロテクションシステムのプロトコルに従ってセキュアにされるディスクキーのセットで前もって記録されるスタートエリア３２、ストレージエリア３４及びデジタルデータ記録エリア３６を有する。

【００３９】

ストレージエリア３４は、任意のレコーダにより記録されるＤＶＤの特定のエリアである。ＤＶＤ－ＲタイプのＤＶＤについて、ストレージエリア３４は、たとえばＲＭＤフィールド２と呼ばれるフィールドを有する。このフィールドは、文献“DVD Specifications for Recordable Disk for General, Part 1, Physical Specification, version 2.0, Mat 2000”で定義されている。

【００４０】

図２において分かるように、本発明に係るシステム２は、SmartRightプロテクションシステムによりセキュアにされるドメインにアクセスする装置を形成するＤＶＤドライブ４０を有する。このドライブ４０は、チップカード４４を受けるために設計されるチップカードリーダ４２にリンクされる。

【００４１】

ドライブ４０は、ＤＶＤを読取る手段４５、暗号／復号モジュール４８に接続されるマスターキーＭＫ’を記憶する手段４６を有する。

【００４２】

また、ドライブ４０は、スクランブリング／デスクランブリングモジュール５０、及び、たとえば家庭内ネットワーク、イントラネットネットワーク又はインターネットネットワークのようなディストリビューションネットワーク５４を介して、デジタルデータを送出及び受信するネットワークインタフェース５２を有する。

【００４３】

チップカード４４は、セキュアプロセッサ５６を含む。このプロセッサ５６は、ドライブ４０が属するドメインに固有の識別子ＩＤＬ、及びこのドメインの暗号化鍵ＤＯＫをセキュアに記憶する。

【００４４】

プロセッサ５６は、データを比較し、ドライブ４０からのデータを受信し、ドライブ４０にデータを送信し、ランダム数を発生し、それらをSmartRightプロテクションプロトコルに従ってエンコードする。

【００４５】

また、システム２は、テレビジョンタイプの表示装置６０、レコーダ６２及び記憶装置６４を有する。

【００４６】

表示装置６０及びレコーダ６２は、ドライブ４０からデジタルデータを受信するか、記憶装置６４でデジタルデータをサーチするネットワークインタフェース７０，７２をそれぞれ有する。これらは、ドライブ４０と同じセキュアなドメインに属する。

【００４７】

表示装置６０は、デスクランブリングモジュール６６を有する。表示装置は、セキュアプロセッサ５７においてこのドメインの識別子ＩＤＬ及び暗号化鍵ＤＯＫを記憶するチップカード４７を受けるチップカードリーダ４３に接続される。

【００４８】

記憶装置６４は、ディストリビューションネットワーク５４に接続される任意の機器によりアクセスされ、特に、識別子ＩＤＬにより定義されるドメインに属さない機器によりアクセスされる。

【００４９】

図３では、垂直の軸は時間軸を表し、水平軸は、図１及び２に表されるシステムの機器のアイテム間のやりとりを説明する。

【００５０】

第一のステップ１００では、ユーザは、レシーバ装置のユーザインタフェース２２を使用して、ユーザがＤＶＤ３０に記録するのを望む映画又は特定の送信といったビデオ系列を選択する。

【００５１】

レコーダ２８は、ＤＶＤのスタートエリア３２に記録される全てのセキュアなディスクキーを読み取り、このセキュアなディスクキーのセットをレシーバ装置６に送信する。

【００５２】

レシーバ装置６の暗号／復号モジュール２０は、このセキュアなディスクキーのセットとマスターキーＭＫからディスクキーＤＫを取得する。

【００５３】

次いで、レシーバ装置６は、ビデオコンテンツの要求メッセージを構築し、それをマル

チメディアサーバ１０のアドレスに送出する。この要求は、注文されたビデオ系列の識別子、レシーバ装置６の識別子、取得されたディスクキーＤＫ、要求されたユーセージの示唆、及び支払いの指示を含む。

【００５４】

次のステップ１０２では、マルチメディアサーバ１０は、データベース１２において要求されたビデオコンテンツをサーチし、このビデオコンテンツを、タイトルキーを使用してスクランブルし、ＣＳＳプロトコルに従って受信されたディスクキーＤＫを使用してタイトルキーを暗号化する。

【００５５】

ステップ１０４では、マルチメディアサーバ１０は、タイトルキーによりスクランブルされたビデオコンテンツ、ディスクキーＤＫにより暗号化されたタイトルキー、及びユーザにより購入されたユーセージの示唆をレシーバ装置６に送信する。

【００５６】

ステップ１０６の間、レシーバ装置の暗号／復号モジュール２０は、ドメイン情報ＤＩを決定して暗号化する。このドメイン情報ＤＩは、ユーザにより購入されたユーセージ、レシーバ装置が属するドメインの識別子ＩＤＤを有する。

【００５７】

たとえば、ドメイン情報ＤＩは、以下の形式をとる。

ＤＩ＝ＡＥＳ［ＤＤＫ］（ＩＤＤ｜｜ＵＳ）

ここでＡＥＳは暗号化規格である（Advanced Encryption Standard）。

“｜｜”は連結演算子である。

ＤＤＫは、ＡＥＳ暗号化規格に適合される鍵であり、ディスク鍵ＤＫから導出される。たとえば鍵ＤＫの低次のビットで“０”ビットを連結して、ＡＥＳにより要求されるサイズの鍵が取得される。

ＩＤＤは、レシーバ装置のドメインの識別子である。

ＵＳは、ビデオコンテンツに付着するユーセージのSmartRightフォーマットにおけるトランスクリプションである。

【００５８】

ステップ１０８では、レコーダ２８は、スクランブルされたビデオコンテンツをデータ記録エリア３６に記録し、ドメイン情報ＤＩをストレージエリア３４に記録する。

【００５９】

したがって、ユーザは、ＣＳＳ仕様に従ってプロテクトされるビデオコンテンツ、及び、マルチメディアコンテンツが記録されている特定のドメインであって、ＤＶＤが属する特定のドメインを特徴付ける識別子ＩＤＤを含むＤＶＤ３０を有する。

【００６０】

ステップ１１０の間、ユーザは、ダウンロードされたビデオコンテンツを、識別子ＩＤＬにより定義されたドメインにおける機器にとって利用可能にすることを望む。

【００６１】

このため、ＤＶＤ３０は、このドメインに属するドライブ４０に挿入される。ドライブの読取り手段４５は、ＤＶＤのスタートエリア３２における全てのセキュアなディスク鍵、及びＤＶＤのストレージエリア３４に記憶されるドメイン情報ＤＩを記憶する。

【００６２】

ステップ１１２の間、暗号／復号モジュール４８は、（ＣＳＳ仕様の原理に従って）セキュアなディスクキーのセットとドライブ４０に含まれるマスターキーＭＫ’とからディスクキーＤＫを取得する。暗号／復号モジュール４８は、このディスクキーＤＫから、導出される鍵ＤＤＫを推測し、この鍵ＤＤＫを使用して、ドメイン情報ＤＩを復号して、ＤＶＤ３０が記録されたドメインのユーセージＵＳ及び識別子ＩＤＤを取得する。

【００６３】

ステップ１１４の間、ドライブ４０は、ユーセージＵＳ及び識別子ＩＤＤをチップカード４４に送出する。

【００６４】
ステップ１１６の間、チップカードのプロセッサ５６は、ＤＶＤに記録される識別子ＩＤＤはプロセッサ５６が記憶する識別子ＩＤＬに一致するかをチェックする。
【００６５】
ＤＶＤ３０に記憶される識別子ＩＤＤがチップカードの識別子ＩＤＬに一致しない場合、ＤＶＤ３０は、ドライブ４０と同じドメインに属するレコーダにより記録されない。
【００６６】
このケースでは、ステップ１１８の間、チップカードのプロセッサ５６は、一般にＣＷで示される制御ワード、ＬＥＣＭ（Local Entitlement Control Messages）で示される制御メッセージを発生する。制御メッセージＬＥＣＭは、ドメインキーＤＯＫ、ドライブ４０のドメインの識別子ＩＤＬ、インテグリティチェック及びインテグリティの計算によりプロテクトされるユーセージＵＳを使用して復号可能となるように暗号化される制御ワードＣＷを含む。これらの制御メッセージＬＥＣＭは、ドライブ４０と同じドメインに属する機器によってのみ復号される。
【００６７】
識別子ＩＤＤが識別子とは異なるとき、制御メッセージＬＥＣＭに含まれる制御ワードＣＷが超暗号化される（superencrypted）。
【００６８】
SmartRightドメインのプロテクションプロトコルによれば、超暗号化された制御ワードＣＷを含む制御メッセージＬＥＣＭは、これら制御メッセージＬＥＣＭ及び制御メッセージに付属するデジタルデータを受信する任意の機器に対して、ＤＶＤを読み取りしている間にのみ受信されたデジタルデータを表示することができ、コピー又は複製することができないことを示す。
【００６９】
ステップ１２０の間、チップカードのプロセッサ５６は、ドライブ４０に発生された制御メッセージＬＥＣＭ及び制御ワードＣＷを送出する。
【００７０】
ステップ１２２の間、ドライブのスクランブリング／デスクランブリングモジュール５０は、ステップ１１２で取得された鍵ＤＫを使用してＤＶＤのエリア３６に記録されたデジタルデータをデスクランブルする。
【００７１】
ステップ１２４の間、ドライブのスクランブル／デスクランブルモジュール５０は、チップカードのプロセッサ５６により発生された制御ワードＣＷを使用して、ステップ１２２の間にデスクランブルされたデジタルデータをスクランブルする。
【００７２】
ステップ１２６の間、ドライブ４０は、表示装置６０に、ディストリビューションネットワーク５４を介して、制御ワードＣＷを使用してスクランブルされたデジタルデータと、プロセッサ５６により発生された制御メッセージＬＥＣＭとを送信する。
【００７３】
ステップ１２８の間、表示装置６０に接続されるチップカードのプロセッサ５７は、制御メッセージＬＥＣＭを復号し、デスクランブリングモジュール６６は、この装置がネットワーク５４を通して送信されたビデオを表示するように、受信されたデジタルデータをデスクランブルする。
【００７４】
したがって、表示装置６０は、ドライブ４０によりＤＶＤ３０の読み取りと同時にビデオコンテンツを表示する。
【００７５】
また、レコーダ６２は、ディストリビューションネットワーク５４を介して送信された、このデジタルデータへのアクセスを有する。しかし、レコーダ６２は、ユーザの便利さのため、ＤＶＤへのこのデータの複製又はコピーを防止することができる。これは、かか

るコピーが行われる場合、このコピーは、制御ワードＣＷが超暗号化されているために使用不可能であるためである。

【００７６】

このデジタルデータ表示モードは、プロトコル名「視聴のみ“view only”」によりSmartRightプロトコルに知られており、文献“SmartRight Technical white paper, Version 1.7, January 2003, Thomson”に特に記載されている。

【００７７】

識別子ＩＤＤが識別子ＩＤＬに等しいとき、チップカードのプロセッサ５６は、ステップ１３０の間にＤＶＤを記録するときに購入されたユーセージＵＳを分析する。

【００７８】

これらユーセージにより、ビデオコンテンツがあるドメインのみで複製又はコピーされるのを可能にするとき、プロセッサ５６は、ステップ１３２の間に、制御ワードＣＷと、ドメインキーＤＯＫにより暗号化されたこれら制御ワードＣＷを含む制御メッセージＬＥＣＭとを発生する。これにより、これら制御メッセージＬＥＣＭは、ドライブ４０と同じドメイン、すなわち識別子ＩＤＬ＝ＩＤＤのドメインに属し、ドメインキーＤＯＫを含む機器によってのみ復号することができる。

【００７９】

ステップ１３４の間、制御メッセージＬＥＣＭ及び制御ワードＣＷは、ドライブ４０に送信される。

【００８０】

ステップ１３６の間、ＤＶＤで読取られるデジタルデータは、ステップ１２２の間に記載された方法と同じ方法に従ってデスクランブルされる。

【００８１】

ステップ１３８の間、ステップ１３６の間にデスクランブルされたデジタルデータは、ステップ１３２の間に発生された制御ワードＣＷによりスクランブルされる。

【００８２】

ステップ１４０の間、スクランブルされたデジタルデータ及び制御メッセージＬＥＣＭは、ディストリビューションネットワーク５４を介して記憶装置６４に送信され、そこで記録される。

【００８３】

ドライブ４０と同じドメインに属する機器のみが制御メッセージＬＥＣＭを復号し、機器６４に記憶されるデジタルデータを複製／コピー又は表示することができる。

【００８４】

ステップ１３０の間、分析されたユーセージは、デジタルデータが自由にコピー可能／複製可能であることを定義する場合、チップカードのプロセッサ５６は、暗号化されていない制御ワードを含む制御メッセージＬＥＣＭを発生する。

【００８５】

次いで、ステップ１３４～１４０が繰り返される。しかし、このケースでは、任意の機器、更には識別子ＩＤＤ＝ＩＤＬのドメインに属さない機器は、デジタルデータを読み取り、表示又はコピーすることができる。これは、デジタルデータは、セキュアな暗号化鍵によりスクランブルされていないからである。

【００８６】

ステップ１３０の間、デジタルデータが複製可能／コピー可能ではないとプロセッサ５６が判定した場合、プロセッサ５６は、制御メッセージＬＥＣＭ及び超暗号化された制御ワードＣＷを発生し、ステップ１２０～１２８が繰り返される。このケースでは、デジタルデータは、識別子ＩＤＬにより識別されたドメインに属する表示装置により表示可能である。

【００８７】

また、本発明に係る方法は、文献“xCP: eXtensible Content Protection. 2003. IBM”及び“xCP Cluster Protocol, IBM Presentation to Copy Protection T

echnical Working Group, July 18, 2002”に記載される登録商標xCP（eXtensible Content Protection）の方法に従ってプロテクトされるドメインプロテクションシステムで実現することができる。

【００８８】

このドメインプロテクション方法によれば、それぞれのドメイン又は機器のグループは、「クラスタＩＤ」と呼ばれるグループ識別子ＩＤにより定義される。

【００８９】

レコーダは、グループ識別子ＩＤを記憶する手段を有し、ドメイン情報ＤＩを計算するために構成される。この情報ＤＩは、ハッシュ関数を、ＤＶＤのディスクキーＤＫ、グループ識別子ＩＤ、及び、コピーが許可されているか否かに依存して値０又は１を取るコピーインジケータを有する連結されたデータに適用することで得られる。

【００９０】

レコーダは、ＤＶＤにドメイン情報ＤＩを記録するために構成される。

【００９１】

記録されたＤＶＤを受けるレシーバ装置は、それ自身のドメイン情報ＤＩ’を構成することで、ＤＶＤがそのドメインに記録されているかを判定する。このため、それ自身のドメインの識別子を再使用し、コピーインジケータを許可されたコピーに対応する値に設定し、ＤＶＤで読取られたディスクキーＤＫを再び使用する。

【００９２】

ＤＶＤのドメイン情報ＤＩと、このよう構築されたレシーバ装置のドメイン情報ＤＩ’とが一致する場合、コピーが許可され、レシーバ装置は、このドメインのｘＣＰプロトコルに従ってデジタルデータをデスクランブルし、その後スクランブルする。

【００９３】

ＤＶＤのドメイン情報ＤＩと、このよう構築されたレシーバ装置のドメイン情報ＤＩ’とが一致しない場合、コピーの動作が禁止される。

【００９４】

変形例として、このセキュアな配信方法は、ＣＰＰＭ（Content Protection for Prerecorded Media）システム、ＣＰＲＭ（Content Protection for Recordable Media）システム、ＢＤ ＣＰＳ（Blue ray Disk Copy Protection System）、又はＤＶＤ＋Ｒ／ＤＶＤ＋ＲＷディスク向けＶｉＤｉシステムに従ってセキュアにされるＤＶＤと使用することができる。

【００９５】

変形例として、レコーダは、デジタルデータ及びドメイン識別子のみをＤＶＤに記録し、デジタルデータに付属するユーセージ又は複製権を記録しない。このケースでは、ドライブが識別子を読取るとき、チップカードは、ディスクで識別されたドメインにおけるコピー／複製のみを許可するプロトコルに従って制御ワード及び制御メッセージを発生する。ＤＶＤが識別子を含まないとき、チップカードは、任意の機器によるコピー／複製を防止するプロトコルに従って超暗号化される制御ワード及び制御メッセージを発生する。このケースでは、デジタルデータは、そのドメインに属する表示装置により表示可能である。

【００９６】

変形例として、ＤＶＤは、市販され、マルチメディアコンテンツ及び関連するユーセージを表すデジタルデータを含む形式でプリレコードされる。このＤＶＤの最初のユーセージの前であって、ＤＶＤが機器アイテムにより読取り可能となる前、このＤＶＤは、レコーダが属するドメインの識別子を記録するのに適したレコーダに配置される必要がある。このケースでは、ＤＶＤ又はドライブは、ＤＶＤがドメイン識別子を含むときにのみ動作するように調整される。

【００９７】

有利なことに、このセキュアな配信方法により、友人又は知人とデジタルデータを共有することにおいて所定の自由度が可能となり、このデジタルデータに付属する知的財産権

を保護しつつ、同じドメインにリンクされる機器との共有が可能となる。

【００９８】

有利なことに、マルチメディアコンテンツのコピー／複製が記録されるセキュアディスクは、ダウンロードされたバージョンのマルチメディアコンテンツとドメイン識別子とが記録されているセキュアディスクに記録されている識別子により定義されるドメインにおいてのみ読取られ、表示される。しかし、セキュアディスク、すなわちダウンロードされたバージョンのマルチメディアコンテンツ及びドメイン識別子を含むディスクは、任意のドメインで許可された任意のＣＳＳ表示装置で読取られ、表示される。

【図面の簡単な説明】

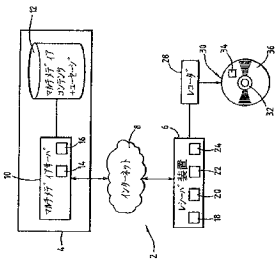
【００９９】

【図１】本発明に係る配信方法を実現可能にするシステムの一部の機能的なブロック図である。

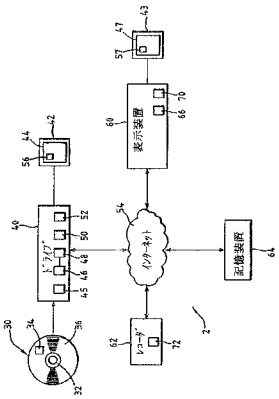
【図２】本発明に係る配信方法を実現可能にするシステムの別の部分の機能的なブロック図である。

【図３】本発明に係る配信方法のステップを説明する図である。

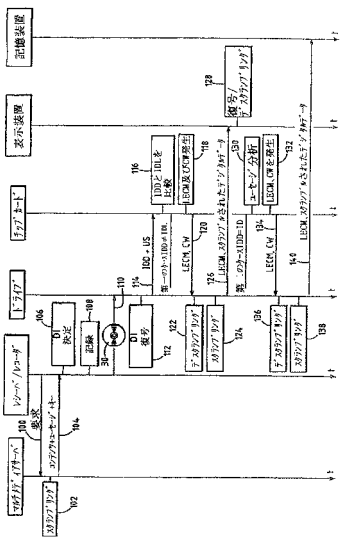
【図１】



【図２】



【図３】



フロントページの続き

(72)発明者　ディアスコール，ジャンールイ
フランス国，３５８３０　ベットン，リュ・デ・シャテニエール　５
(72)発明者　デュラン，アラン
フランス国，３５０００　レンヌ，リュ・ド・ディナン　７９
(72)発明者　ルリエーヴル，シルヴァン
フランス国，３５７６０　モンジェルモン，リュ・デ・アエッテ　３６

審査官　和田　財太

(56)参考文献　米国特許出願公開第２００５／０１６９１１８（ＵＳ，Ａ１）
米国特許出願公開第２００５／００７５９８６（ＵＳ，Ａ１）
国際公開第２００５／０７３８７１（WO，Ａ１）
特表２００５－５２６３３０（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F　21/22-21/24
H04L　9/08