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

特許第4502002号
(P4502002)

(45)発行日　平成22年7月14日(2010.7.14)　(24)登録日　平成22年4月30日(2010.4.30)

(51)Int.Cl.		F I		
G06F 21/24	(2006.01)	G06F	12/14	520D
G06F 21/00	(2006.01)	G06F	12/14	540A
G06Q 50/00	(2006.01)	G06F	15/00	330Z
G06Q 30/00	(2006.01)	G06F	17/60	142
G06Q 10/00	(2006.01)	G06F	17/60	302E

請求項の数 3　(全 25 頁)　最終頁に続く

(21)出願番号　特願2007-329670 (P2007-329670)
(22)出願日　平成19年12月21日 (2007.12.21)
(65)公開番号　特開2009-151605 (P2009-151605A)
(43)公開日　平成21年7月9日 (2009.7.9)
審査請求日　平成21年8月25日 (2009.8.25)

(73)特許権者　000005496
富士ゼロックス株式会社
東京都港区赤坂九丁目７番３号
(74)代理人　100075258
弁理士　吉田　研二
(74)代理人　100096976
弁理士　石田　純
(72)発明者　筧　るみ子
東京都港区赤坂九丁目７番３号　富士ゼロックス株式会社内
(72)発明者　鈴木　敏克
東京都港区赤坂九丁目７番３号　富士ゼロックス株式会社内

最終頁に続く

(54)【発明の名称】情報利用制御システムおよび情報利用制御装置

(57)【特許請求の範囲】
【請求項１】
それぞれ、自身が管理する利用者からの登録要求に応じて、制御対象情報の利用を制御するための利用制御情報を当該制御対象情報と関連付けて自身の記憶手段に登録し、自身が管理する利用者からの制御対象情報に対応する利用情報の発行要求を受けると、当該制御対象情報と関連付けて前記自身の記憶手段に登録されている利用制御情報に基づき、当該制御対象情報を利用するための利用情報を前記利用者に提供する第１および第２の情報利用制御装置を含み、
前記第１の情報利用制御装置は、自身が管理する利用者からの登録要求に応じて、前記第２の情報利用制御装置で用いられる利用制御情報の一覧を前記利用者に提供し、前記一覧の中から利用制御情報の選択を受け付け、当該選択された利用制御情報を、当該利用制御情報が適用される制御対象情報と関連付けて前記第２の情報利用制御装置に送る第１の情報処理手段を有し、
前記第２の情報利用制御装置は、前記第１の情報処理手段から前記制御対象情報と関連付けられた利用制御情報を受け取り、当該利用制御情報を当該制御対象情報と関連付けて前記自身の記憶手段に登録する第２の情報処理手段を有し、
さらに、
前記第２の情報処理手段は、前記制御対象情報と関連付けられた利用制御情報を受け取ると、当該制御対象情報を暗号化するために自身が生成した第２の暗号鍵を前記第１の情報処理手段に送るとともに、当該第２の暗号鍵に対応する第２の復号鍵を当該制御対象情

報と関連付けて前記第２の情報利用制御装置の記憶手段に登録し、
前記第１の情報処理手段は、前記第２の情報処理手段から送信された前記第２の暗号鍵と、前記制御対象情報を暗号化するために自身が生成した第１の暗号鍵とを前記登録要求元の利用者に提供するとともに、前記第１の情報利用制御装置で用いられる前記制御対象情報の利用制御情報と、前記第１の暗号鍵に対応する第１の復号鍵とを、当該制御対象情報と関連付けて前記第１の情報利用制御装置の記憶手段に登録し、
前記制御対象情報は、前記登録要求元の利用者の情報処理装置において前記第１の暗号鍵と前記第２の暗号鍵とのそれぞれを用いて別々に暗号化され、
前記第１の情報利用制御装置は、前記第１の暗号鍵と前記第２の暗号鍵とのそれぞれを用いて別々に暗号化された制御対象情報に対応する利用情報の発行要求を、自身が管理する利用者から受けると、当該制御対象情報と関連付けて自身の記憶手段に登録されている利用制御情報に基づき、当該制御対象情報と関連付けられた第１の復号鍵を含む利用情報を前記発行要求元の利用者に提供する第１の提供手段を有し、
前記第２の情報利用制御装置は、前記第１の暗号鍵と前記第２の暗号鍵とのそれぞれを用いて別々に暗号化された制御対象情報に対応する利用情報の発行要求を、自身が管理する利用者から受けると、当該制御対象情報と関連付けて自身の記憶手段に登録されている利用制御情報に基づき、当該制御対象情報と関連付けられた第２の復号鍵を含む利用情報を前記発行要求元の利用者に提供する第２の提供手段を有する、
ことを特徴とする情報利用制御システム。

【請求項２】
自身が管理する利用者からの登録要求に応じて、制御対象情報の利用を制御するための利用制御情報を当該制御対象情報と関連付けて記憶手段に登録する登録手段と、
自身が管理する利用者からの制御対象情報に対応する利用情報の発行要求を受けると、当該制御対象情報と関連付けて前記記憶手段に登録されている利用制御情報に基づき、当該制御対象情報を利用するための利用情報を前記利用者に提供する提供手段と、
自身が管理する利用者からの登録要求に応じて、他の情報利用制御装置で用いられる利用制御情報の一覧を前記利用者に提供し、前記一覧の中から利用制御情報の選択を受け付け、当該選択された利用制御情報を、当該利用制御情報が適用される制御対象情報と関連付けて前記他の情報利用制御装置に送る情報処理手段であって、前記他の情報利用制御装置は、自身が管理する利用者からの登録要求に応じて、制御対象情報の利用を制御するための利用制御情報を当該制御対象情報と関連付けて自身の記憶手段に登録し、自身が管理する利用者からの制御対象情報に対応する利用情報の発行要求を受けると、当該制御対象情報と関連付けて前記自身の記憶手段に登録されている利用制御情報に基づき、当該制御対象情報を利用するための利用情報を前記利用者に提供する装置である、情報処理手段と
、
を有し、
さらに、
前記他の情報利用制御装置は、前記制御対象情報と関連付けられた利用制御情報を受け取ると、当該制御対象情報を暗号化するために自身が生成した第２の暗号鍵を前記情報処理手段に送るとともに、当該第２の暗号鍵に対応する第２の復号鍵を当該制御対象情報と関連付けて前記他の情報利用制御装置の記憶手段に登録し、
前記情報処理手段は、前記他の情報利用制御装置から送信された前記第２の暗号鍵と、前記制御対象情報を暗号化するために自身が生成した第１の暗号鍵とを前記登録要求元の利用者に提供するとともに、自身で用いられる前記制御対象情報の利用制御情報と、前記第１の暗号鍵に対応する第１の復号鍵とを、当該制御対象情報と関連付けて自身の前記記憶手段に登録し、
前記制御対象情報は、前記登録要求元の利用者の情報処理装置において前記第１の暗号鍵と前記第２の暗号鍵とのそれぞれを用いて別々に暗号化され、
前記提供手段は、前記第１の暗号鍵と前記第２の暗号鍵とのそれぞれを用いて別々に暗号化された制御対象情報に対応する利用情報の発行要求を、自身が管理する利用者から受

けると、当該制御対象情報と関連付けて自身の前記記憶手段に登録されている利用制御情報に基づき、当該制御対象情報と関連付けられた第１の復号鍵を含む利用情報を前記発行要求元の利用者に提供する、

ことを特徴とする情報利用制御装置。

【請求項３】

自身が管理する利用者からの登録要求に応じて、制御対象情報の利用を制御するための利用制御情報を当該制御対象情報と関連付けて記憶手段に登録する登録手段と、

自身が管理する利用者からの制御対象情報に対応する利用情報の発行要求を受けると、当該制御対象情報と関連付けて前記記憶手段に登録されている利用制御情報に基づき、当該制御対象情報を利用するための利用情報を前記利用者に提供する提供手段と、

自身が管理する利用者からの登録要求に応じて、制御対象情報の利用を制御するための利用制御情報を当該制御対象情報と関連付けて自身の記憶手段に登録し、自身が管理する利用者からの制御対象情報に対応する利用情報の発行要求を受けると、当該制御対象情報と関連付けて前記自身の記憶手段に登録されている利用制御情報に基づき、当該制御対象情報を利用するための利用情報を前記利用者に提供する他の情報利用制御装置から、制御対象情報と関連付けられた、前記他の情報利用制御装置が管理する利用者により選択された利用制御情報を受け取り、当該利用制御情報を当該制御対象情報と関連付けて当該情報利用制御装置の記憶手段に登録する情報処理手段と、

を有し、

さらに、

前記情報処理手段は、前記制御対象情報と関連付けられた利用制御情報を前記他の情報利用制御装置から受け取ると、当該制御対象情報を暗号化するために自身が生成した第２の暗号鍵を前記他の情報利用制御装置に送るとともに、当該第２の暗号鍵に対応する第２の復号鍵を当該制御対象情報と関連付けて自身の前記記憶手段に登録し、

前記他の情報利用制御装置は、前記情報処理手段から送信された前記第２の暗号鍵と、前記制御対象情報を暗号化するために自身が生成した第１の暗号鍵とを前記登録要求元の利用者に提供するとともに、前記他の情報利用制御装置で用いられる前記制御対象情報の利用制御情報と、前記第１の暗号鍵に対応する第１の復号鍵とを、当該制御対象情報と関連付けて前記他の情報利用制御装置の記憶手段に登録し、

前記制御対象情報は、前記登録要求元の利用者の情報処理装置において前記第１の暗号鍵と前記第２の暗号鍵とのそれぞれを用いて別々に暗号化され、

前記提供手段は、前記第１の暗号鍵と前記第２の暗号鍵とのそれぞれを用いて別々に暗号化された制御対象情報に対応する利用情報の発行要求を、自身が管理する利用者から受けると、当該制御対象情報と関連付けて自身の前記記憶手段に登録されている利用制御情報に基づき、当該制御対象情報と関連付けられた第２の復号鍵を含む利用情報を前記発行要求元の利用者に提供する、

ことを特徴とする情報利用制御装置。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、情報利用制御システムおよび情報利用制御装置に関する。

【背景技術】

【０００２】

セキュリティポリシーを用いてコンテンツの利用を制御するデジタル著作権管理（DRM: Digital Rights Management）システムが知られている。

【０００３】

特許文献１には、第１の組織のデジタルコンテンツやデジタルサービスなどのリソースが、そのリソースへのアクセスを第２の組織の要求者に提供する方法が記載されている。当該方法では、第１の組織の第１の管理者は、第１の信用情報を第２の組織の第２の管理

者に発行する。この第１の信用情報には、第２の管理者が第１の管理者に代わって第２の信用情報を要求者に発行することができるというポリシーが含まれる。第２の管理者は、発行された第１の信用情報を含む第２の信用情報を要求者に発行する。要求者はリソースへのアクセスを要求し、その要求に発行された第１および第２の信用情報を含める。リソースは、発行された第１の信用情報が第１の管理者を第２の管理者に結びつけ、発行された第２の信用情報が第２の管理者を要求者に結びつけるものであることを検証する。したがってリソースは、要求が、第１の管理者から第２の管理者を経由して要求者に委任された権限に基づくものであることを確認することができる。

【０００４】

特許文献２には、利用法ごとの利用条件と、暗号化著作物データの復号鍵を利用法ごとに異なるチケット鍵により再暗号化した利用秘密情報とを、当該暗号化著作物データとともにカプセル化するデジタル著作物流通システムが記載されている。

【０００５】

【特許文献１】特開２００６－２５４４６４号公報

【特許文献２】特開２０００－４８０７６号公報

【発明の開示】

【発明が解決しようとする課題】

【０００６】

ところで、それぞれ、自身が管理する利用者からの要求に応じて、制御対象情報の利用を制御するための利用制御情報を当該制御対象情報と関連付けて記憶し、自身が管理する利用者からの制御対象情報に対応する利用情報の要求を受けると、当該制御対象情報と関連付けて記憶されている利用制御情報に基づき、当該制御対象情報を利用するための利用情報を利用者に提供する複数の情報利用制御装置が設けられている場合に、特定の情報利用制御装置により管理される利用者が、その他の情報利用制御装置により管理される利用者に利用可能な制御対象情報を作成することを可能にしたいという要望がある。

【０００７】

本発明は、特定の情報利用制御装置により管理される利用者が、その他の情報利用制御装置により管理される利用者に利用可能な制御対象情報を作成することを可能にする情報利用制御システムおよび情報利用制御装置を提供することを目的とする。

【課題を解決するための手段】

【０００８】

本発明に係る情報利用制御システムは、それぞれ、自身が管理する利用者からの要求に応じて、制御対象情報の利用を制御するための利用制御情報を当該制御対象情報と関連付けて自身の記憶手段に登録し、自身が管理する利用者からの制御対象情報に対応する利用情報の要求を受けると、当該制御対象情報と関連付けて前記自身の記憶手段に登録されている利用制御情報に基づき、当該制御対象情報を利用するための利用情報を前記利用者に提供する第１および第２の情報利用制御装置を含み、前記第１の情報利用制御装置は、自身が管理する利用者からの要求に応じて、前記第２の情報利用制御装置で用いられる利用制御情報の一覧を前記利用者に提供し、前記一覧の中から利用制御情報の選択を受け付け、当該選択された利用制御情報を、当該利用制御情報が適用される制御対象情報と関連付けて前記第２の情報利用制御装置に送る第１の情報処理手段を有し、前記第２の情報利用制御装置は、前記第１の情報処理手段から前記制御対象情報と関連付けられた利用制御情報を受け取り、当該利用制御情報を当該制御対象情報と関連付けて前記自身の記憶手段に登録する第２の情報処理手段を有する、ことを特徴とする。

【０００９】

本発明の一態様では、前記第２の情報処理手段は、前記制御対象情報と関連付けられた利用制御情報を受け取ると、当該制御対象情報を保護するための第２の保護用情報を前記第１の情報処理手段に送るとともに、当該第２の保護用情報に対応する第２の保護解除用情報を当該制御対象情報と関連付けて前記第２の情報利用制御装置の記憶手段に登録し、前記第１の情報処理手段は、前記第２の情報処理手段からの前記第２の保護用情報と、前

記制御対象情報を保護するための第１の保護用情報とを前記要求元の利用者に提供するとともに、前記第１の情報利用制御装置で用いられる前記制御対象情報の利用制御情報と、前記第１の保護用情報に対応する第１の保護解除用情報とを、当該制御対象情報と関連付けて前記第１の情報利用制御装置の記憶手段に登録し、前記第１の情報利用制御装置は、自身が管理する利用者からの、前記第１および第２の保護用情報を用いて保護された制御対象情報に対応する利用情報の要求を受けると、当該制御対象情報と関連付けて自身の記憶手段に登録されている利用制御情報に基づき、当該制御対象情報と関連付けられた第１の保護解除用情報から得られる、当該制御対象情報の保護を解除するための情報を含む利用情報を前記利用者に提供する第１の提供手段を有し、前記第２の情報利用制御装置は、自身が管理する利用者からの、前記第１および第２の保護用情報を用いて保護された制御対象情報に対応する利用情報の要求を受けると、当該制御対象情報と関連付けて自身の記憶手段に登録されている利用制御情報に基づき、当該制御対象情報と関連付けられた第２の保護解除用情報から得られる、当該制御対象情報の保護を解除するための情報を含む利用情報を前記利用者に提供する第２の提供手段を有する。

【００１０】

本発明に係る情報利用制御装置は、自身が管理する利用者からの要求に応じて、制御対象情報の利用を制御するための利用制御情報を当該制御対象情報と関連付けて記憶手段に登録する登録手段と、自身が管理する利用者からの制御対象情報に対応する利用情報の要求を受けると、当該制御対象情報と関連付けて前記記憶手段に登録されている利用制御情報に基づき、当該制御対象情報を利用するための利用情報を前記利用者に提供する提供手段と、自身が管理する利用者からの要求に応じて、他の情報利用制御装置で用いられる利用制御情報の一覧を前記利用者に提供し、前記一覧の中から利用制御情報の選択を受け付け、当該選択された利用制御情報を、当該利用制御情報が適用される制御対象情報と関連付けて前記他の情報利用制御装置に送る情報処理手段であって、前記他の情報利用制御装置は、自身が管理する利用者からの要求に応じて、制御対象情報の利用を制御するための利用制御情報を当該制御対象情報と関連付けて自身の記憶手段に登録し、自身が管理する利用者からの制御対象情報に対応する利用情報の要求を受けると、当該制御対象情報と関連付けて前記自身の記憶手段に登録されている利用制御情報に基づき、当該制御対象情報を利用するための利用情報を前記利用者に提供する装置である情報処理手段と、を有することを特徴とする。

【００１１】

本発明に係る情報利用制御装置は、自身が管理する利用者からの要求に応じて、制御対象情報の利用を制御するための利用制御情報を当該制御対象情報と関連付けて記憶手段に登録する登録手段と、自身が管理する利用者からの制御対象情報に対応する利用情報の要求を受けると、当該制御対象情報と関連付けて前記記憶手段に登録されている利用制御情報に基づき、当該制御対象情報を利用するための利用情報を前記利用者に提供する提供手段と、自身が管理する利用者からの要求に応じて、制御対象情報の利用を制御するための利用制御情報を当該制御対象情報と関連付けて自身の記憶手段に登録し、自身が管理する利用者からの制御対象情報に対応する利用情報の要求を受けると、当該制御対象情報と関連付けて前記自身の記憶手段に登録されている利用制御情報に基づき、当該制御対象情報を利用するための利用情報を前記利用者に提供する他の情報利用制御装置から、制御対象情報と関連付けられた、前記他の情報利用制御装置が管理する利用者により選択された利用制御情報を受け取り、当該利用制御情報を当該制御対象情報と関連付けて当該情報利用制御装置の記憶手段に登録する情報処理手段と、を有することを特徴とする。

【発明の効果】

【００１２】

請求項１に記載の発明によれば、特定の情報利用制御装置により管理される利用者が、その他の情報利用制御装置により管理される利用者に利用可能な制御対象情報を作成することが可能となる。

【００１３】

請求項２に記載の発明によれば、特定の情報利用制御装置により管理される利用者と、その他の情報利用制御装置により管理される利用者とに利用可能な、保護された制御対象情報を作成することが可能となる。

【００１４】

請求項３に記載の発明によれば、特定の情報利用制御装置により管理される利用者が、その他の情報利用制御装置により管理される利用者に利用可能な制御対象情報を作成することが可能となる。

【００１５】

請求項４に記載の発明によれば、特定の情報利用制御装置により管理される利用者が、その他の情報利用制御装置により管理される利用者に利用可能な制御対象情報を作成することが可能となる。

【発明を実施するための最良の形態】

【００１６】

以下、本発明の実施の形態を図面に従って説明する。

【００１７】

［第１の実施の形態］

図１は、本実施の形態に係る情報利用制御システム１の構成の一例を示すブロック図である。図１において、情報利用制御システム１は、２つの情報利用制御装置１０，２０を含む。情報利用制御装置１０，２０は、互いに通信可能に接続される。情報利用制御装置１０，２０は、それぞれ、自身が管理する利用者からの要求に応じて、制御対象情報の利用を制御するための利用制御情報を当該制御対象情報と関連付けて記憶し、自身が管理する利用者からの制御対象情報に対応する利用情報の要求を受けると、当該制御対象情報と関連付けて記憶されている利用制御情報に基づき、当該制御対象情報を利用するための利用情報を利用者に提供するものである。

【００１８】

情報利用制御装置１０，２０の各々は、一つの態様では、ハードウェア資源とソフトウェアとの協働により実現され、例えばコンピュータである。具体的には、情報利用制御装置１０，２０の各々の機能は、記録媒体に記録された情報利用制御プログラムがメインメモリに読み出されてＣＰＵ（Central Processing Unit）により実行されることによって実現される。上記情報利用制御プログラムは、ＣＤ－ＲＯＭ等のコンピュータ読み取り可能な記録媒体に記録されて提供されることも可能であるし、データ信号として通信により提供されることも可能である。ただし、情報利用制御装置１０，２０の各々は、ハードウェアのみにより実現されてもよい。また、情報利用制御装置１０，２０は、それぞれ、物理的に１つの装置により実現されてもよいし、物理的に複数の装置により実現されてもよい。

【００１９】

具体的な一態様では、情報利用制御装置１０，２０はサーバコンピュータであり、以下の説明では、情報利用制御装置を「サーバ」と称する。

【００２０】

一つの態様では、サーバ１０および２０は、互いに異なる組織に設けられるものか、または互いに異なる組織により管理されるものである。互いに異なる組織とは、例えば、異なる会社、同一会社内の異なる部署などである。また、別の態様では、一方のサーバは社内向けにサービスを提供するものであり、他方のサーバは社外向けにサービスを提供するものである。

【００２１】

サーバ１０は、利用者記憶部１１、記憶部１２、登録部１３、および提供部１４を有する。

【００２２】

利用者記憶部１１は、サーバ１０により管理される利用者を識別するための識別情報（以下、「利用者ＩＤ」と称す）を記憶する。図２には、利用者記憶部１１の記憶内容の一

例が示されている。

【００２３】

記憶部１２は、制御対象情報の利用を制御するための利用制御情報を当該制御対象情報と関連付けて記憶する。例えば、記憶部１２は、制御対象情報の利用を制御するための利用制御情報と、当該制御対象情報を識別するための識別情報とを互いに関連付けて記憶する。

【００２４】

上記制御対象情報は、利用制御の対象である情報であり、例えば文書、動画、静止画、音声等のコンテンツである。制御対象情報は、一つの態様では電子データであるが、紙に記載された情報など、電子データ以外の形態の情報であってもよい。なお、以下の説明では、制御対象情報を「コンテンツ」と称する。

【００２５】

一つの態様では、コンテンツは、暗号化などにより保護される。この態様では、記憶部１２は、コンテンツを復号化するための情報など、コンテンツの保護を解除するための保護解除用情報を、当該コンテンツと関連付けて記憶してもよい。

【００２６】

上記利用制御情報は、コンテンツの利用を制御するための情報であり、例えば、コンテンツの利用が許可される条件または範囲を示す情報、コンテンツの利用に対する制限を示す情報などである。具体的には、利用制御情報は、コンテンツの利用が許可される、利用者、期間、回数、あるいは操作、またはこれらの組み合わせを示す情報を含む。例えば、利用制御情報は、どの利用者がどのような操作をいつからいつまでの期間内に行えるか等が記述された情報である。利用制御情報は、例えばセキュリティポリシーと呼ばれるものであり、以下の説明では利用制御情報を「ポリシー」と称する。

【００２７】

記憶部１２は、例えば、ポリシーを管理するポリシーテーブルと、コンテンツとポリシーとの関連付けを管理する関連付けテーブルとを有する。

【００２８】

図３は、サーバ１０のポリシーテーブルの一例を示す図である。図３の例では、ポリシーテーブルには、ポリシー毎に、当該ポリシーを識別するための識別情報であるポリシーＩＤと、当該ポリシーの内容とが互いに関連付けて記録されている。各ポリシーは、コンテンツの利用が許可される１以上の利用者または利用者のグループを示す情報と、利用者またはグループ毎に規定される当該利用者またはグループに与えられる利用条件、利用権限、または許可内容を示す利用条件情報とを含む。利用条件情報は、例えば、利用が許可される期間である有効期間を示す情報や、許可される操作を示す情報などを含む。

【００２９】

図４は、サーバ１０の関連付けテーブルの一例を示す図である。図４の例では、関連付けテーブルには、コンテンツ毎に、当該コンテンツを識別するための識別情報であるコンテンツＩＤと、当該コンテンツの利用を制御するためのポリシーのポリシーＩＤとが互いに関連付けて記録されている。

【００３０】

登録部１３は、サーバ１０が管理する利用者からの要求に応じて、コンテンツの利用を制御するためのポリシーを当該コンテンツと関連付けてサーバ１０の記憶部１２に登録する。具体的には、登録部１３は、サーバ１０により管理される利用者から記憶部１２に登録すべき情報を受け付け、当該情報を記憶部１２に登録する。例えば、登録部１３は、記憶部１２に登録すべき情報を、サーバ１０に接続されたパーソナルコンピュータ（ＰＣ）等の利用者が使用する装置（以下、「利用者装置」と称す）１００から受け付け、当該情報を記憶部１２に登録する。

【００３１】

登録部１３は、利用者から当該利用者を認証するための認証情報を受け取り、当該認証情報に基づいて利用者の認証を行い、当該認証が成功した場合に、当該登録部１３の機能

を上記利用者に提供する。例えば、登録部１３は、利用者から利用者ＩＤを受け取り、当該利用者ＩＤが利用者記憶部１１に登録されている場合に、当該登録部１３の機能を提供し、登録されていない場合には、当該登録部１３の機能を提供しない。

【００３２】

一つの態様では、登録部１３は、利用者からポリシーを受け付け、当該ポリシーを当該ポリシーのポリシーＩＤと関連付けてポリシーテーブルに登録する。また、登録部１３は、利用者からコンテンツＩＤとポリシーＩＤとを受け付け、当該コンテンツＩＤと当該ポリシーＩＤとを互いに関連付けて関連付けテーブルに登録する。コンテンツＩＤは、当該コンテンツＩＤで識別されるコンテンツに含められる。コンテンツが暗号化などにより保護される態様では、例えば、登録部１３は、関連付けの際、コンテンツを保護するための保護用情報（例えば暗号鍵）を利用者に提供し、コンテンツの保護を解除するための保護解除用情報（例えば復号鍵）をコンテンツＩＤと関連付けて関連付けテーブルに登録し、利用者は、保護用情報を用いてコンテンツを保護（例えば暗号化）する。

【００３３】

上記ポリシーテーブルへのポリシーの登録と、関連付けテーブルへの関連付けの登録とは、別々の利用者または利用者装置により行われてもよいし、同一の利用者または利用者装置により行われてもよい。

【００３４】

提供部１４は、サーバ１０が管理する利用者からのコンテンツに対応する利用情報の要求を受けると、当該コンテンツと関連付けて記憶部１２に登録されているポリシーに基づき、当該コンテンツを利用するための利用情報を上記利用者に提供する。例えば、提供部１４は、サーバ１０に接続された利用者装置１００からコンテンツに対応する利用情報の要求を受けると、記憶部１２を参照し、当該コンテンツに対応するポリシーに基づき、当該コンテンツを利用するための利用情報を利用者装置１００に提供する。

【００３５】

提供部１４は、利用者から当該利用者を認証するための認証情報を受け取り、当該認証情報に基づいて利用者の認証を行い、当該認証が成功した場合に、当該提供部１４の機能を上記利用者に提供する。例えば、提供部１４は、利用者から利用者ＩＤを受け取り、当該利用者ＩＤが利用者記憶部１１に登録されている場合に、当該提供部１４の機能を提供し、登録されていない場合には、当該提供部１４の機能を提供しない。

【００３６】

上記利用情報は、例えば、コンテンツの利用を可能にするための情報、コンテンツの利用に必要な情報、コンテンツに対する利用条件または利用権限を示す情報などである。利用情報は、例えばライセンスと呼ばれるものであり、以下の説明では利用情報を「ライセンス」と称する。

【００３７】

ライセンスの具体例としては、例えば下記（ａ１）～（ａ３）が挙げられる。

（ａ１）ライセンスは、コンテンツの利用を許可する旨を示す情報を含む。この場合、利用者装置１００は、ライセンスを受けたとき、利用者にコンテンツの利用を許可し、そうでないときには、利用者にコンテンツの利用を許可しない。ここで、上記「コンテンツの利用」は、コンテンツに対する複数種類の操作のうち、特定の一部の操作であってもよい。例えば、利用者装置１００は、ライセンスの有無に関わらずコンテンツの閲覧を許可し、ライセンスを受けたときに限りコンテンツの印刷を許可してもよい。

（ａ２）ライセンスは、利用が許可される期間、回数、操作など、利用条件を示す情報を含む。この場合、利用者装置１００は、当該利用条件に従う範囲内で、利用者にコンテンツの利用を許可する。例えば、利用者装置１００は、複数種類の操作のうち、利用が許可される操作に限って、コンテンツの操作を可能にする。

（ａ３）ライセンスは、保護されたコンテンツの保護を解除するための保護解除用情報（例えば復号鍵）を含む。この場合、利用者装置１００は、当該保護解除用情報を用いて、コンテンツの保護を解除する。例えば、暗号化されたコンテンツを復号化する。

【００３８】
一つの態様では、提供部１４は、要求に係るコンテンツに対応するポリシーに基づき、要求者からの利用者ＩＤで識別される利用者にコンテンツの利用が許可されるか否かを判断し、許可されると判断された場合に、当該利用者に対する利用条件を含むライセンスを要求者に提供する。なお、提供部１４は、利用者に対する利用条件の一部または全部について、利用条件が満たされているか否かを判断し、満たされていると判断された場合にライセンスを要求者に提供してもよい。例えば、提供部１４は、有効期間内の利用か否かを判断し、有効期間内の利用であると判断された場合に、許可される操作を示すライセンスを要求者に提供してもよい。
【００３９】
サーバ２０は、利用者記憶部２１、記憶部２２、登録部２３、および提供部２４を有する。以下、利用者記憶部２１、記憶部２２、登録部２３、および提供部２４について説明するが、これらは上記サーバ１０のものと同様であるので、詳しい説明については省略する。
【００４０】
利用者記憶部２１は、サーバ２０により管理される利用者を識別するための識別情報（利用者ＩＤ）を記憶する。図５には、利用者記憶部２１の記憶内容の一例が示されている。
【００４１】
記憶部２２は、コンテンツの利用を制御するためのポリシーを当該コンテンツと関連付けて記憶する。
【００４２】
登録部２３は、サーバ２０が管理する利用者からの要求に応じて、コンテンツの利用を制御するためのポリシーを当該コンテンツと関連付けてサーバ２０の記憶部２２に登録する。例えば、登録部２３は、記憶部２２に登録すべき情報を、サーバ２０に接続された利用者装置２００から受け付け、当該情報を記憶部２２に登録する。
【００４３】
提供部２４は、サーバ２０が管理する利用者からのコンテンツに対応するライセンスの要求を受けると、当該コンテンツと関連付けて記憶部２２に登録されているポリシーに基づき、当該コンテンツを利用するためのライセンスを上記利用者に提供する。例えば、提供部２４は、サーバ２０に接続された利用者装置２００からコンテンツに対応するライセンスの要求を受けると、記憶部２２を参照し、当該コンテンツに対応するポリシーに基づき、当該コンテンツを利用するためのライセンスを利用者装置２００に提供する。
【００４４】
さらに、本実施の形態では、サーバ１０，２０は、それぞれ以下のように構成されている。
【００４５】
サーバ１０は、当該サーバ１０が管理する利用者からの要求に応じて、他のサーバ２０で用いられるポリシーの一覧を上記利用者に提供し、当該一覧の中からポリシーの選択を受け付け、当該選択されたポリシーを、当該ポリシーが適用されるコンテンツと関連付けて他のサーバ２０に送る情報処理部１５を有する。
【００４６】
例えば、情報処理部１５は、利用者装置１００からポリシーの一覧の要求を受けると、サーバ２０用のポリシーの一覧を利用者装置１００に提供し、当該一覧の中からのポリシーの選択を利用者装置１００から受け付け、当該選択されたポリシーを、当該ポリシーが適用されるコンテンツと関連付けてサーバ２０に送る。
【００４７】
また、例えば、情報処理部１５は、利用者からのポリシーの選択を受け付けると、当該選択されたポリシーと、当該ポリシーが適用されるコンテンツのコンテンツＩＤとをサーバ２０に送る。ここで、情報処理部１５は、利用者からコンテンツのコンテンツＩＤを受

け取って当該コンテンツＩＤをサーバ２０に送ってもよいし、コンテンツＩＤを生成し、当該コンテンツＩＤを利用者に渡すとともにサーバ２０に送ってもよい。

【００４８】

一方、サーバ２０は、サーバ１０の情報処理部１５から、上記コンテンツと関連付けられたポリシーを受け取り、当該ポリシーを当該コンテンツと関連付けてサーバ２０の記憶部２２に登録する情報処理部２５を有する。

【００４９】

例えば、情報処理部２５は、情報処理部１５から、利用者により選択されたポリシーと、当該ポリシーが適用されるコンテンツのコンテンツＩＤとを受け取り、当該ポリシーとコンテンツＩＤとを互いに関連付けて記憶部２２に登録する。

【００５０】

なお、サーバ１０および２０の各々が、情報処理部１５および２５を有してもよい。すなわち、サーバ１０がサーバ２０と同様の機能を有し、サーバ２０がサーバ１０と同様の機能を有してもよい。

【００５１】

また、図１の例では、２つのサーバが示されているが、サーバは複数であればよく、３つ以上のサーバが設けられてもよい。

【００５２】

３つ以上のサーバが設けられる場合、あるサーバは、当該サーバの利用者からの要求に応じて、他の複数のサーバ用のポリシーの一覧を上記利用者に提供し、当該一覧の中からポリシーの選択を受け付け、当該選択されたポリシーを、当該ポリシーが適用されるコンテンツと関連付けて、当該ポリシーに係る他のサーバに送ってもよい。すなわち、１つのサーバ１０に対して、サーバ２０と同様のサーバが複数存在してもよい。

【００５３】

また、３つ以上のサーバが設けられる場合、あるサーバは、他の複数のサーバから、コンテンツと関連付けられたポリシーを受け取って、自身の記憶部に登録してもよい。すなわち、１つのサーバ２０に対して、サーバ１０と同様のサーバが複数存在してもよい。

【００５４】

一つの態様では、サーバ１０は、他のサーバ用のポリシーを記憶する他サーバ用ポリシー記憶部１６を有する。そして、情報処理部１５は、利用者からの要求に応じて、他サーバ用ポリシー記憶部１６に予め記憶されている他のサーバ用のポリシーの一覧を利用者に提供する。この態様では、サーバ１０は、例えば、通信等により他のサーバから当該他のサーバ用のポリシーの提供を受け、当該他のサーバ用のポリシーを他サーバ用ポリシー記憶部１６に登録する。サーバ１０は、例えば、他のサーバと信頼関係を結んだときに、当該他のサーバからポリシーの提供を受ける。サーバ１０は、適当なタイミングで他のサーバから当該他のサーバ用のポリシーの提供を受けて、他サーバ用ポリシー記憶部１６の記憶内容を更新してもよい。

【００５５】

図６には、サーバ１０の他サーバ用ポリシー記憶部１６の記憶内容の一例が示されている。図６の例では、他のサーバ２０，２０－１，２０－２，・・・毎に、当該サーバ用のポリシーのポリシーＩＤと、当該ポリシーの内容とが関連付けて記録されている。なお、上記サーバ２０－１，２０－２，・・・は、サーバ２０と同様のものである。

【００５６】

別の態様では、情報処理部１５は、利用者からの要求に応じて、他のサーバから当該他のサーバ用のポリシーの提供を受け、当該提供されたポリシーの一覧を利用者に提供する。

【００５７】

また、一つの態様では、サーバ２０は、他のサーバ１０等に提供される当該サーバ２０用のポリシーのポリシーＩＤと、当該ポリシーの内容とを互いに関連付けて記憶する他サーバ提供ポリシー記憶部２６を有する。この態様では、サーバ１０は、利用者により選択

されたポリシーのポリシーＩＤをサーバ２０に送る。例えば、サーバ１０は、利用者により選択されたポリシーのポリシーＩＤと、当該ポリシーが適用されるコンテンツのコンテンツＩＤとをサーバ２０に送り、サーバ２０は、当該コンテンツＩＤとポリシーＩＤとを互いに関連付けて記憶部２２の関連付けテーブルに登録する。サーバ２０において、選択されたポリシーＩＤに対応するポリシーの内容は、他サーバ提供ポリシー記憶部２６から取得される。

【００５８】

図７には、サーバ２０の他サーバ提供ポリシー記憶部２６の記憶内容の一例が示されている。図７の例では、他のサーバに提供されるポリシーのポリシーＩＤと、当該ポリシーの内容とが関連付けて記録されている。

【００５９】

また、一つの態様では、情報処理部１５は、登録部１３に含まれる。すなわち、登録部１３が、情報処理部１５の機能を有する。当該一つの態様における一態様では、登録部１３は、利用者からの要求に応じて、自サーバ１０で用いられるポリシーの一覧（例えば記憶部１２のポリシーテーブルに登録されているポリシーの一覧）と、他のサーバで用いられるポリシーの一覧を利用者に提供する。そして、登録部１３は、利用者からポリシーの選択を受け、選択されたポリシーが自サーバ１０用であった場合には、当該ポリシーを当該ポリシーが適用されるコンテンツと関連付けて記憶部１２に登録し、選択されたポリシーが他のサーバ用であった場合には、当該ポリシーを当該ポリシーが適用されるコンテンツと関連付けて、当該ポリシーの提供元のサーバに送る。別の態様では、登録部１３は、利用者からサーバの指定を受け、指定されたサーバ用のポリシーの一覧を利用者に提供する。具体的には、登録部１３は、サーバ１０の指定を受けた場合にはサーバ１０用のポリシーの一覧を利用者に提供し、サーバ２０の指定を受けた場合にはサーバ２０用のポリシーの一覧を利用者に提供する。

【００６０】

また、一つの態様では、情報処理部１５は、利用者からポリシーの選択を受けると、当該ポリシーを当該ポリシーが適用されるコンテンツと関連付けて他のサーバに送るとともに、当該コンテンツと関連付けて、サーバ１０で用いられる当該コンテンツのポリシーを記憶部１２に登録する。ここで、上記サーバ１０で用いられる当該コンテンツのポリシーは、要求者により指定されるものであってもよいし、予め決められたポリシーであってもよい。予め決められたポリシーとしては、例えば、当該要求者に当該コンテンツの利用を許可するポリシーが挙げられる。当該一つの態様における一態様では、情報処理部１５は、要求者により選択された他のサーバ用のポリシーまたはそのポリシーＩＤと、サーバ１０用のポリシーまたはそのポリシーＩＤとを含む新たなポリシーを作成し、当該新たなポリシーを記憶部１２に登録する。上記予め決められたポリシーや、上記新たなポリシーに含められるサーバ１０用のポリシーは、予め他のサーバ毎に設定されていてもよい。

【００６１】

また、一つの態様では、情報処理部２５は、情報処理部１５からコンテンツと関連付けられたポリシーを受け取ると、当該コンテンツを保護するための第２の保護用情報を情報処理部１５に送るとともに、当該第２の保護用情報に対応する第２の保護解除用情報を当該コンテンツと関連付けて記憶部２２に登録する。例えば、情報処理部２５は、コンテンツと関連付けられたポリシーを受け取ると、当該コンテンツを暗号化するための第２の暗号情報（例えば暗号鍵）を情報処理部１５に送るとともに、当該第２の暗号情報に対応する第２の復号情報を当該コンテンツと関連付けて記憶部２２に登録する。

【００６２】

一方、情報処理部１５は、上記情報処理部２５からの上記第２の保護用情報と、上記コンテンツを保護するための第１の保護用情報とを要求者に提供するとともに、サーバ１０で用いられる当該コンテンツのポリシーと、上記第１の保護用情報に対応する第１の保護解除用情報とを、当該コンテンツと関連付けてサーバ１０の記憶部１２に登録する。例えば、情報処理部１５は、情報処理部２５から受け取った第２の暗号情報と、コンテンツを

暗号化するための第１の暗号情報（例えば暗号鍵）とを要求者に提供するとともに、サーバ１０用の当該コンテンツのポリシーと、第１の暗号情報に対応する第１の復号情報とを、当該コンテンツと関連付けて記憶部１２に登録する。

【００６３】

要求者またはその利用者装置１００は、情報処理部１５から上記第１および第２の保護用情報を受けると、当該第１および第２の保護用情報を用いてコンテンツを保護し、保護コンテンツを生成する。例えば、要求者またはその利用者装置１００は、第１および第２の暗号情報を用いてコンテンツを暗号化し、暗号コンテンツを生成する。

【００６４】

提供部１４は、サーバ１０が管理する利用者からの、上記第１および第２の保護用情報を用いて保護されたコンテンツに対応するライセンスの要求を受けると、当該コンテンツと関連付けて記憶部１２に登録されているポリシーに基づき、当該コンテンツと関連付けられた第１の保護解除用情報から得られる、当該コンテンツの保護を解除するための情報を含むライセンスを上記利用者に提供する。例えば、提供部１４は、サーバ１０が管理する利用者からの暗号コンテンツに対応するライセンスの要求を受けると、当該暗号コンテンツと関連付けて記憶部１２に登録されているポリシーに基づき、当該暗号コンテンツと関連付けられた第１の復号情報から得られる、当該暗号コンテンツを復号化するための情報（例えば復号鍵）を含むライセンスを上記利用者に提供する。

【００６５】

要求者またはその利用者装置１００は、提供部１４から上記ライセンスを受けると、当該ライセンスに含まれる保護を解除するための情報を用いて保護コンテンツの保護を解除して、元のコンテンツを復元する。例えば、要求者またはその利用者装置１００は、ライセンスに含まれる復号化するための情報を用いて暗号コンテンツを復号化して、元のコンテンツを復元する。

【００６６】

また、提供部２４は、サーバ２０が管理する利用者からの、上記第１および第２の保護用情報を用いて保護されたコンテンツに対応するライセンスの要求を受けると、当該コンテンツと関連付けて記憶部２２に登録されているポリシーに基づき、当該コンテンツと関連付けられた第２の保護解除用情報から得られる、当該コンテンツの保護を解除するための情報を含むライセンスを上記利用者に提供する。例えば、提供部２４は、サーバ２０が管理する利用者からの暗号コンテンツに対応するライセンスの要求を受けると、当該暗号コンテンツと関連付けて記憶部２２に登録されているポリシーに基づき、当該暗号コンテンツと関連付けられた第２の復号情報から得られる、当該暗号コンテンツを復号するための情報（例えば復号鍵）を含むライセンスを上記利用者に提供する。

【００６７】

要求者またはその利用者装置２００は、提供部２４から上記ライセンスを受けると、当該ライセンスに含まれる保護を解除するための情報を用いて保護コンテンツの保護を解除して、元のコンテンツを復元する。例えば、要求者またはその利用者装置２００は、ライセンスに含まれる復号化するための情報を用いて暗号コンテンツを復号化して、元のコンテンツを復元する。

【００６８】

なお、サーバ１０により管理される各利用者について、当該利用者にサーバ１０のどのような機能の提供が認められるか、すなわちサーバ１０に対する利用権限が設定されてもよい。同様に、サーバ２０により管理される各利用者について、当該利用者にサーバ２０のどのような機能の提供が認められるか、すなわちサーバ２０に対する利用権限が設定されてもよい。

【００６９】

以下、本実施の形態に係る情報利用制御システム１の動作を、保護コンテンツの作成、サーバ１０によるライセンスの発行、サーバ２０によるライセンスの発行、およびポリシーの無効化に分けて具体的に説明する。

【００７０】
（保護コンテンツの作成）
図８は、保護コンテンツの作成処理の一例を示すシーケンス図であり、図９は、保護コンテンツの作成におけるサーバ１０の動作の一例を示すフローチャートであり、図１０は、保護コンテンツの作成におけるサーバ２０の動作の一例を示すフローチャートである。以下、図８～１０を参照して、保護コンテンツの作成処理の一例を説明する。
【００７１】
サーバ１０と他のサーバ２０，２０－１，２０－２，・・・とは、予め信頼関係を構築し、サーバ１０は、他のサーバ２０等から当該他のサーバ用のポリシーの提供を受けておく。
【００７２】
利用者装置１００は、利用者ＩＤを含むポリシーリスト取得要求をサーバ１０に送る（Ｓ１０１）。ここで、利用者装置１００は、利用者から利用者ＩＤの入力を受け付けてもよいし、予め利用者装置１００に記憶されている利用者ＩＤを読み出してもよい。
【００７３】
サーバ１０は、利用者装置１００から上記ポリシーリスト取得要求を受けると（Ｓ１１）、当該ポリシーリスト取得要求に含まれる利用者ＩＤが利用者記憶部１１に登録されているか否かを判断する（Ｓ１２）。
【００７４】
利用者ＩＤが登録されていないと判断された場合（Ｓ１２：ＮＯ）、サーバ１０は、ポリシーリスト提供不可を示す情報を利用者装置１００に返す（Ｓ１３）。
【００７５】
一方、利用者ＩＤが登録されていると判断された場合（Ｓ１２：ＹＥＳ）、例えば利用者ＩＤが「ユーザ１１」であった場合、サーバ１０は、記憶部１２のポリシーテーブルに登録されている自サーバ用のポリシーのリストと、他サーバ用ポリシー記憶部１６に登録されている他サーバ用のポリシーのリストとを利用者装置１００に返す（Ｓ１４）。
【００７６】
利用者装置１００は、上記ポリシーの一覧を画面上に表示させ、当該画面上で利用者からポリシーの選択を受け付ける（Ｓ１０２）。ここで、画面上では、例えば、ポリシーＩＤとポリシーの内容とが互いに関連付けられて表示される。
【００７７】
ついで、利用者装置１００は、保護対象のコンテンツのコンテンツＩＤを生成し、当該コンテンツＩＤを保護対象のコンテンツに埋め込む（Ｓ１０３）。
【００７８】
そして、利用者装置１００は、上記選択されたポリシーのポリシーＩＤと、上記生成されたコンテンツＩＤとを含む第１暗号鍵発行要求をサーバ１０に送る（Ｓ１０４）。
【００７９】
サーバ１０は、利用者装置１００から上記第１暗号鍵発行要求を受けると（Ｓ１５）、当該第１暗号鍵発行要求に含まれるポリシーＩＤに基づき、選択されたポリシーが自サーバ１０により管理されるものか、他のサーバで管理されるものかを判断する（Ｓ１６）。
【００８０】
選択されたポリシーが自サーバ１０により管理されるものであると判断された場合、サーバ１０は、保護対象のコンテンツを暗号化するための第１暗号鍵（例えば公開鍵）を生成する（Ｓ１７）。そして、サーバ１０は、第１暗号鍵発行要求に含まれるコンテンツＩＤと、第１暗号鍵発行要求に含まれるポリシーＩＤと、上記生成された第１暗号鍵に対応する第１復号鍵とを互いに関連付けて記憶部１２に登録し（Ｓ１８）、上記第１暗号鍵を利用者装置１００に発行する（Ｓ１９）。
【００８１】
利用者装置１００は、サーバ１０から上記第１暗号鍵を受けると、当該第１暗号鍵を用いて保護対象のコンテンツを暗号化して、保護コンテンツを作成する。

【００８２】
一方、選択されたポリシーが他のサーバにより管理されるものであると判断された場合、サーバ１０は、選択された他のサーバ用のポリシーまたはそのポリシーＩＤと、サーバ１０用の所定のポリシーまたはそのポリシーＩＤとを含む新規ポリシーを作成する（Ｓ２０）。ここでは、サーバ１０は、選択された他のサーバ用のポリシーＩＤを包含し、かつ要求者（作成者）に対してコンテンツの利用を許可する新規ポリシーを作成する。また、ここでは、サーバ２０用のポリシーＩＤ「ポリシー２Ａ」のポリシーが選択されたものとする。
【００８３】
そして、サーバ１０は、上記作成された新規ポリシーのポリシーＩＤと、当該新規ポリシーの内容と、第１暗号鍵発行要求に含まれるコンテンツＩＤとを含む第２暗号鍵発行要求を、選択されたポリシーの提供元のサーバ（ここではサーバ２０）に送る（Ｓ２１）。
【００８４】
サーバ２０は、サーバ１０から上記第２暗号鍵発行要求を受けると（Ｓ４１）、保護対象のコンテンツを暗号化するための第２暗号鍵（例えば公開鍵）を生成する（Ｓ４２）。そして、サーバ２０は、第２暗号鍵発行要求に含まれる、コンテンツＩＤ、ポリシーＩＤ、およびポリシーの内容、並びに第２暗号鍵に対応する第２復号鍵を互いに関連付けて記憶部２２に登録する（Ｓ４３）。例えば、記憶部２２のポリシーテーブルには、図１１に示されるように、新規ポリシーのポリシーＩＤ「ポリシー１３」と、当該新規ポリシーの内容と、第２復号鍵（不図示）とが、互いに関連付けられて登録される。記憶部２２の関連付けテーブルには、図１２に示されるように、保護対象のコンテンツのコンテンツＩＤ「コンテンツ１３」と、新規ポリシーのポリシーＩＤ「ポリシー１３」とが互いに関連付けられて登録される。なお、図１１に示されるように、新規ポリシーのうち、サーバ１０で用いられる部分については、記憶部２２に登録されなくてもよいし、サーバ１０からサーバ２０に送られなくてもよい。
【００８５】
ついで、サーバ２０は、上記生成された第２暗号鍵をサーバ１０に発行する（Ｓ４４）。
【００８６】
サーバ１０は、サーバ２０から第２暗号鍵を受けると（Ｓ２２）、保護対象のコンテンツを暗号化するための第１暗号鍵（例えば公開鍵）を生成し（Ｓ２３）、保護対象のコンテンツのコンテンツＩＤと、新規ポリシーのポリシーＩＤと、新規ポリシーの内容と、第１暗号鍵に対応する第１復号鍵を互いに関連付けて記憶部１２に登録する（Ｓ２４）。例えば、記憶部１２のポリシーテーブルには、図１３に示されるように、新規ポリシーのポリシーＩＤ「ポリシー１３」と、当該新規ポリシーの内容と、第１復号鍵（不図示）とが、互いに関連付けられて登録される。記憶部１２の関連付けテーブルには、図１４に示されるように、保護対象のコンテンツのコンテンツＩＤ「コンテンツ１３」と、新規ポリシーのポリシーＩＤ「ポリシー１３」とが互いに関連付けられて登録される。
【００８７】
ついで、サーバ１０は、当該サーバ１０により作成された第１暗号鍵と、サーバ２０により作成された第２暗号鍵とを利用者装置１００に発行する（Ｓ２５）。
【００８８】
利用者装置１００は、上記サーバ１０から発行された第１暗号鍵および第２暗号鍵を用いて、保護対象のコンテンツをそれぞれの暗号鍵で別々に暗号化し、上記第１復号鍵または第２復号鍵により復号可能な保護コンテンツを生成する（Ｓ１０５）。
【００８９】
（サーバ１０によるライセンスの発行）
図１５は、サーバ１０によるライセンスの発行処理の一例を示すシーケンス図であり、図１６は、ライセンスの発行におけるサーバ１０の動作の一例を示すフローチャートである。以下、図１５，１６を参照して、サーバ１０によるライセンスの発行処理の一例を説

明する。
【００９０】
保護コンテンツを利用しようとする利用者は、利用者装置１００に（具体的には保護コンテンツを利用するためのアプリケーションソフトに）、保護コンテンツを起動させる。
【００９１】
利用者装置１００は、利用者から保護コンテンツの起動指示を受け付けると、当該保護コンテンツから当該コンテンツのコンテンツＩＤを抽出し、コンテンツＩＤおよび利用者ＩＤを含むライセンス発行要求をサーバ１０に送る（Ｓ１１１）。この場合、利用者装置１００は、利用者から利用者ＩＤの入力を受け付けてもよいし、予め利用者装置１００に記憶されている利用者ＩＤを読み出してもよい。
【００９２】
サーバ１０は、利用者装置１００からライセンス発行要求を受けると（Ｓ５１）、当該ライセンス発行要求に含まれる利用者ＩＤが利用者記憶部１１に登録されているか否かを判断する（Ｓ５２）。
【００９３】
利用者ＩＤが登録されていないと判断された場合（Ｓ５２：ＮＯ）、サーバ１０は、ライセンス発行不可を示す情報を利用者装置１００に返す（Ｓ５３）。
【００９４】
一方、利用者ＩＤが登録されていると判断された場合（Ｓ５２：ＹＥＳ）、サーバ１０は、ライセンス発行要求に含まれるコンテンツＩＤが記憶部１２に登録されているか否かを判断する（Ｓ５４）。
【００９５】
コンテンツＩＤが登録されていないと判断された場合（Ｓ５４：ＮＯ）、サーバ１０は、ライセンス発行不可を示す情報を利用者装置１００に返す（Ｓ５３）。
【００９６】
一方、コンテンツＩＤが登録されていると判断された場合（Ｓ５４：ＹＥＳ）、サーバ１０は、記憶部１２において当該コンテンツＩＤと関連付けられているポリシーに基づき、要求者に対するライセンス発行処理を行う。
【００９７】
具体的には、サーバ１０は、上記コンテンツＩＤと関連付けられたポリシーに基づき、上記ライセンス発行要求に含まれる利用者ＩＤで識別される利用者が、コンテンツの利用が許可されている利用者か否かを判断する（Ｓ５６）。
【００９８】
許可されていない利用者であると判断された場合には（Ｓ５６：ＮＯ）、サーバ１０は、ライセンス発行不可を示す情報を利用者装置１００に返す（Ｓ５３）。
【００９９】
一方、許可されている利用者であると判断された場合には（Ｓ５６：ＹＥＳ）、サーバ１０は、上記ポリシーにおいて当該利用者に設定されている利用条件情報と、ライセンス発行要求に含まれるコンテンツＩＤに関連付けられた第１復号鍵とを含むライセンスを生成し（Ｓ５７）、当該ライセンスを利用者装置１００に発行する（Ｓ５８）。
【０１００】
（サーバ２０によるライセンスの発行）
図１７は、サーバ２０によるライセンスの発行処理の一例を示すシーケンス図であり、図１８は、ライセンスの発行におけるサーバ２０の動作の一例を示すフローチャートである。以下、図１７，１８を参照して、サーバ２０によるライセンスの発行処理の一例を説明する。
【０１０１】
保護コンテンツを利用しようとする利用者は、利用者装置２００に（具体的には保護コンテンツを利用するためのアプリケーションソフトに）、保護コンテンツを起動させる。
【０１０２】

利用者装置２００は、利用者から保護コンテンツの起動指示を受け付けると、当該保護コンテンツから当該コンテンツのコンテンツＩＤを抽出し、コンテンツＩＤおよび利用者ＩＤを含むライセンス発行要求をサーバ２０に送る（Ｓ１２１）。この場合、利用者装置２００は、利用者から利用者ＩＤの入力を受け付けてもよいし、予め利用者装置２００に記憶されている利用者ＩＤを読み出してもよい。

【０１０３】

サーバ２０は、利用者装置２００からライセンス発行要求を受けると（Ｓ６１）、当該ライセンス発行要求に含まれる利用者ＩＤが利用者記憶部２１に登録されているか否かを判断する（Ｓ６２）。

【０１０４】

利用者ＩＤが登録されていないと判断された場合（Ｓ６２：ＮＯ）、サーバ２０は、ライセンス発行不可を示す情報を利用者装置２００に返す（Ｓ６３）。

【０１０５】

一方、利用者ＩＤが登録されていると判断された場合（Ｓ６２：ＹＥＳ）、サーバ２０は、ライセンス発行要求に含まれるコンテンツＩＤが記憶部２２に登録されているか否かを判断する（Ｓ６４）。

【０１０６】

コンテンツＩＤが登録されていないと判断された場合（Ｓ６４：ＮＯ）、サーバ２０は、ライセンス発行不可を示す情報を利用者装置２００に返す（Ｓ６３）。

【０１０７】

一方、コンテンツＩＤが登録されていると判断された場合（Ｓ６４：ＹＥＳ）、サーバ２０は、記憶部２２において当該コンテンツＩＤと関連付けられているポリシーに基づき、要求者に対するライセンス発行処理を行う。

【０１０８】

具体的には、サーバ２０は、上記コンテンツＩＤと関連付けられたポリシーに基づき、上記ライセンス発行要求に含まれる利用者ＩＤで識別される利用者が、コンテンツの利用が許可されている利用者か否かを判断する（Ｓ６６）。

【０１０９】

許可されていない利用者であると判断された場合には（Ｓ６６：ＮＯ）、サーバ２０は、ライセンス発行不可を示す情報を利用者装置２００に返す（Ｓ６３）。

【０１１０】

一方、許可されている利用者であると判断された場合には（Ｓ６６：ＹＥＳ）、サーバ２０は、上記ポリシーにおいて当該利用者に設定されている利用条件情報と、ライセンス発行要求に含まれるコンテンツＩＤに関連付けられた第２復号鍵とを含むライセンスを生成し（Ｓ６７）、当該ライセンスを利用者装置２００に発行する（Ｓ６８）。

【０１１１】

例えば、記憶部２２のポリシーテーブルが図１１に示されるとおりであり、記憶部２２の関連付けテーブルが図１２に示されるとおりである場合において、ライセンス発行要求に含まれるコンテンツＩＤが「コンテンツ１３」であった場合には、サーバ２０は次のように動作する。

【０１１２】

サーバ２０は、図１２の関連付けテーブルから、コンテンツＩＤ「コンテンツ１３」と関連付けられているポリシーＩＤ「ポリシー１３」を特定する。そして、サーバ２０は、図１１のポリシーテーブルから、ポリシーＩＤ「ポリシー１３」のポリシーを取得する。このポリシーには、ポリシーＩＤ「ポリシー２Ａ」のポリシーを参照すべき旨が記述されているので、サーバ２０は、他サーバ提供ポリシー記憶部２６から、ポリシーＩＤ「ポリシー２Ａ」のポリシーを取得する。そして、サーバ２０は、当該ポリシーＩＤ「ポリシー２Ａ」のポリシーに基づいて、ライセンス発行処理を行う。例えば、図７を参照すると、ライセンス発行要求に含まれる利用者ＩＤが「ユーザ２５」であった場合、当該利用者ＩＤは当該ポリシーに記述されていないので、サーバ２０は、ライセンス発行不可を示す情

報を利用者装置２００に送る。一方、ライセンス発行要求に含まれる利用者ＩＤが「ユーザ２１」であった場合、当該利用者ＩＤは当該ポリシーに記述されているので、サーバ２０は、当該利用者ＩＤに対応する利用条件情報「有効期間：無期限／許可操作：閲覧」を含むライセンスを利用者装置２００に発行する。

【０１１３】

（ポリシーの無効化）

図１９は、ポリシーの無効化処理におけるサーバ１０の動作の一例を示すフローチャートであり、図２０は、ポリシーの無効化処理におけるサーバ２０の動作の一例を示すフローチャートである。以下、図１９，２０を参照して、ポリシーの無効化処理の一例を説明する。

【０１１４】

サーバ１０は、当該サーバ１０の管理者等から、無効化対象のポリシーのポリシーＩＤを含む無効化要求を受け付ける（Ｓ７１）。

【０１１５】

ついで、サーバ１０は、記憶部１２を参照し、当該無効化要求に含まれるポリシーＩＤで識別されるポリシーに、他のサーバ用のポリシーが含まれているか否かを判断する（Ｓ７２）。

【０１１６】

他のサーバ用のポリシーが含まれていないと判断された場合（Ｓ７２：ＮＯ）、サーバ１０は、記憶部１２のポリシーテーブルに登録されている当該ポリシーＩＤのポリシーを無効化する（Ｓ７３）。これにより、記憶部１２において当該ポリシーＩＤと関連付けられているコンテンツが無効化される。例えば、図１４を参照すると無効化要求に含まれるポリシーＩＤが「ポリシー１１」であった場合、記憶部１２においてポリシーＩＤ「ポリシー１１」のポリシーが無効化され、記憶部１２において当該ポリシーと関連付けられているコンテンツＩＤ「コンテンツ１１」のコンテンツが無効化され、以降、当該コンテンツに対応するライセンスは発行されなくなる。

【０１１７】

一方、他のサーバ用のポリシーが含まれていると判断された場合（Ｓ７２：ＹＥＳ）、サーバ１０は、記憶部１２のポリシーテーブルに登録されている当該ポリシーＩＤのポリシーを無効化するとともに（Ｓ７４）、当該ポリシーの提供元である他のサーバに対し、当該ポリシーＩＤのポリシーの無効化を通知する（Ｓ７５）。ここでは、サーバ１０は、ポリシーＩＤ「ポリシー１３」を含む無効化要求を受け、図１３のポリシーテーブルと図６のテーブルとを参照し、当該ポリシーＩＤ「ポリシー１３」のポリシーに含まれるポリシーＩＤ「ポリシー２Ａ」のポリシーの提供元であるサーバ２０に対し、ポリシーＩＤ「ポリシー１３」のポリシーの無効化を通知したものとする。

【０１１８】

サーバ２０は、上記ポリシーＩＤ「ポリシー１３」のポリシーの無効化の通知を受けると（Ｓ８１）、記憶部２２のポリシーテーブルに登録されている当該ポリシーＩＤ「ポリシー１３」のポリシーを無効化する（Ｓ８２）。これにより、記憶部２２において当該ポリシーＩＤ「ポリシー１３」と関連付けられたコンテンツＩＤ「コンテンツ１３」のコンテンツが無効化される。これにより、以降、サーバ１０により管理される利用者に対しても、サーバ２０により管理される利用者に対しても、当該コンテンツに対応するライセンスは発行されなくなる。この場合において、無効化されたポリシーＩＤ「ポリシー１３」に含まれているポリシーＩＤ「ポリシー２Ａ」のポリシーや、当該ポリシーＩＤ「ポリシー２Ａ」のポリシーと関連付けられているコンテンツに対しては、影響が及ばない。

【０１１９】

［第２の実施の形態］

以下、第２の実施の形態に係る情報利用制御システムについて説明する。なお、上記第１の実施の形態に係る情報利用制御システムと共通する部分については、同一の符号を付し、説明を省略する。

【０１２０】
本実施の形態では、サーバ１０やその利用者等により、他のサーバから提供された他のサーバ用のポリシーに基づき、他のサーバ用のポリシーを含むポリシーが予め作成され、記憶部１２に登録される。例えば、他のサーバ用のポリシーと、自サーバ１０用のポリシーとを含むポリシーが予め作成され、記憶部１２に登録される。このポリシーの作成は、いつ行われてもよい。
【０１２１】
図２１は、本実施の形態における記憶部１２のポリシーテーブルの一例を示す図である。図２１の例では、ポリシーテーブルには、サーバ１０用のポリシーのみを含むポリシー（ポリシーＩＤ「ポリシー１１」や「ポリシー１２」のポリシー）の他に、サーバ２０用のポリシーとサーバ１０用のポリシーを含むポリシー（ポリシーＩＤ「ポリシー１４」や「ポリシー１５」のポリシー）が登録されている。ポリシーＩＤ「ポリシー１４」のポリシーは、サーバ２０用のポリシーＩＤ「ポリシー２Ａ」のポリシーを含んでおり、ポリシーＩＤ「ポリシー１５」のポリシーは、サーバ２０用のポリシーＩＤ「ポリシー２Ｂ」のポリシーを含んでいる。
【０１２２】
以下、本実施の形態における情報利用制御システムの動作を、保護コンテンツの作成およびポリシーの無効化に分けて説明する。なお、ライセンスの発行については、第１の実施の形態と同様である。
【０１２３】
（保護コンテンツの作成）
図２２は、保護コンテンツの作成におけるサーバ１０の動作の一例を示すフローチャートであり、図２３は、保護コンテンツの作成におけるサーバ２０の動作の一例を示すフローチャートである。以下、図２２，２３を参照して、保護コンテンツの作成処理の一例を説明する。
【０１２４】
サーバ１０は、利用者装置１００から利用者ＩＤを含むポリシーリスト取得要求を受けると（Ｓ２１１）、当該ポリシーリスト取得要求に含まれる利用者ＩＤが利用者記憶部１１に登録されているか否かを判断する（Ｓ２１２）。
【０１２５】
利用者ＩＤが登録されていないと判断された場合（Ｓ２１２：ＮＯ）、サーバ１０は、ポリシーリスト提供不可を示す情報を利用者装置１００に返す（Ｓ２１３）。
【０１２６】
一方、利用者ＩＤが登録されていると判断された場合（Ｓ２１２：ＹＥＳ）、サーバ１０は、記憶部１２のポリシーテーブルに登録されているポリシーのリストを利用者装置１００に返す（Ｓ２１４）。
【０１２７】
そして、サーバ１０は、利用者装置１００から、利用者により選択されたポリシーのポリシーＩＤと、保護対象のコンテンツのコンテンツＩＤとを含む第１暗号鍵発行要求を受けると（Ｓ２１５）、当該第１暗号鍵発行要求に含まれるポリシーＩＤに基づき、選択されたポリシーが他サーバ用のポリシーを含むか否かを判断する（Ｓ２１６）。
【０１２８】
選択されたポリシーが他サーバ用のポリシーを含まないと判断された場合（Ｓ２１６：ＮＯ）、サーバ１０は、第１暗号鍵を生成し（Ｓ２１７）、コンテンツＩＤと、ポリシーＩＤと、第１暗号鍵に対応する第１復号鍵とを互いに関連付けて記憶部１２に登録し（Ｓ２１８）、上記第１暗号鍵を利用者装置１００に発行する（Ｓ２１９）。
【０１２９】
一方、選択されたポリシーが他サーバ用のポリシーを含むと判断された場合（Ｓ２１６：ＹＥＳ）、サーバ１０は、選択されたポリシーのポリシーＩＤと、当該ポリシーの内容と、第１暗号鍵発行要求に含まれるコンテンツＩＤとを含む第２暗号鍵発行要求を、選択

されたポリシーに含まれる他サーバ用のポリシーの提供元のサーバに送る（Ｓ２２１）。ここでは、ポリシーＩＤ「ポリシー１４」のポリシーが選択され、サーバ１０は、当該ポリシーに含まれるポリシーＩＤ「ポリシー２Ａ」のポリシーの提供元であるサーバ２０に対し、第２暗号鍵発行要求を送るものとする。

【０１３０】

サーバ２０は、サーバ１０から上記第２暗号鍵発行要求を受けると（Ｓ２４１）、第２暗号鍵を生成する（Ｓ２４２）。そして、サーバ２０は、第２暗号鍵発行要求に含まれる、コンテンツＩＤ、ポリシーＩＤ、およびポリシーの内容、並びに第２暗号鍵に対応する第２復号鍵を互いに関連付けて記憶部２２に登録する（Ｓ２４３）。例えば、記憶部２２のポリシーテーブルには、選択されたポリシーのポリシーＩＤ「ポリシー１４」と、当該ポリシーの内容と、第２復号鍵とが、互いに関連付けられて登録される。記憶部２２の関連付けテーブルには、保護対象のコンテンツのコンテンツＩＤと、選択されたポリシーのポリシーＩＤ「ポリシー１４」とが互いに関連付けられて登録される。なお、選択されたポリシーのうち、サーバ１０で用いられる部分については、記憶部２２に登録されなくてもよいし、サーバ１０からサーバ２０に送られなくてもよい。

【０１３１】

ついで、サーバ２０は、上記生成された第２暗号鍵をサーバ１０に発行する（Ｓ２４４）。

【０１３２】

サーバ１０は、サーバ２０から第２暗号鍵を受けると（Ｓ２２２）、第１暗号鍵を生成し（Ｓ２２３）、保護対象のコンテンツのコンテンツＩＤと、選択されたポリシーのポリシーＩＤと、選択されたポリシーの内容と、第１暗号鍵に対応する第１復号鍵を互いに関連付けて記憶部１２に登録する（Ｓ２２４）。例えば、記憶部１２のポリシーテーブルには、選択されたポリシーのポリシーＩＤ「ポリシー１４」と、当該ポリシーの内容と、第１復号鍵とが、互いに関連付けられて登録される。記憶部１２の関連付けテーブルには、保護対象のコンテンツのコンテンツＩＤと、選択されたポリシーのポリシーＩＤ「ポリシー１４」とが互いに関連付けられて登録される。

【０１３３】

ついで、サーバ１０は、当該サーバ１０により作成された第１暗号鍵と、サーバ２０により作成された第２暗号鍵とを利用者装置１００に発行する（Ｓ２２５）。

【０１３４】

以上のように、本実施の形態では、他のサーバ用のポリシーの一覧は、他のサーバ用のポリシーとサーバ１０用のポリシーとを含むポリシーの一覧として提供される。このように、他のサーバ用のポリシーの一覧は、そのままの形態で利用者に提供される必要はなく、様々な形態で提供され得る。

【０１３５】

（ポリシーの無効化）

第１の実施の形態では、他サーバ用のポリシーを含むポリシーは、特定のコンテンツのために新規に作成されるものであり、当該１つのコンテンツに対応する。したがって、第１の実施の形態では、他サーバ用のポリシーを含むポリシーを無効化した場合、当該ポリシーに対応する１つのコンテンツが無効化される。

【０１３６】

これに対し、第２の実施の形態では、他サーバ用のポリシーを含むポリシーは、複数のコンテンツに適用可能であるので、１または複数のコンテンツに対応する。したがって、第２の実施の形態では、他サーバ用のポリシーを含むポリシーを無効化した場合、当該ポリシーに対応する１または複数のコンテンツが無効化される。

【０１３７】

なお、ポリシーの無効化処理におけるサーバ１０および２０の動作は、第１の実施の形態と同様である。

【０１３８】

なお、本発明は、上記実施の形態に限定されるものではなく、本発明の要旨を逸脱しない範囲内で種々変更することができる。

【図面の簡単な説明】

【０１３９】

【図１】実施の形態に係る情報利用制御システムの構成の一例を示すブロック図である。

【図２】サーバ１０の利用者記憶部の記憶内容の一例を示す図である。

【図３】サーバ１０のポリシーテーブルの一例を示す図である。

【図４】サーバ１０の関連付けテーブルの一例を示す図である。

【図５】サーバ２０の利用者記憶部の記憶内容の一例を示す図である。

【図６】サーバ１０の他サーバ用ポリシー記憶部の記憶内容の一例を示す図である。

【図７】サーバ２０の他サーバ提供ポリシー記憶部の記憶内容の一例を示す図である。

【図８】保護コンテンツの作成処理の一例を示すシーケンス図である。

【図９】保護コンテンツの作成におけるサーバ１０の動作の一例を示すフローチャートである。

【図１０】保護コンテンツの作成におけるサーバ２０の動作の一例を示すフローチャートである。

【図１１】サーバ２０のポリシーテーブルの一例を示す図である。

【図１２】サーバ２０の関連付けテーブルの一例を示す図である。

【図１３】サーバ１０のポリシーテーブルの一例を示す図である。

【図１４】サーバ１０の関連付けテーブルの一例を示す図である。

【図１５】サーバ１０によるライセンスの発行処理の一例を示すシーケンス図である。

【図１６】ライセンスの発行におけるサーバ１０の動作の一例を示すフローチャートである。

【図１７】サーバ２０によるライセンスの発行処理の一例を示すシーケンス図である。

【図１８】ライセンスの発行におけるサーバ２０の動作の一例を示すフローチャートである。

【図１９】ポリシーの無効化処理におけるサーバ１０の動作の一例を示すフローチャートである。

【図２０】ポリシーの無効化処理におけるサーバ２０の動作の一例を示すフローチャートである。

【図２１】第２の実施の形態における、サーバ１０のポリシーテーブルの一例を示す図である。

【図２２】第２の実施の形態における、保護コンテンツの作成におけるサーバ１０の動作の一例を示すフローチャートである。

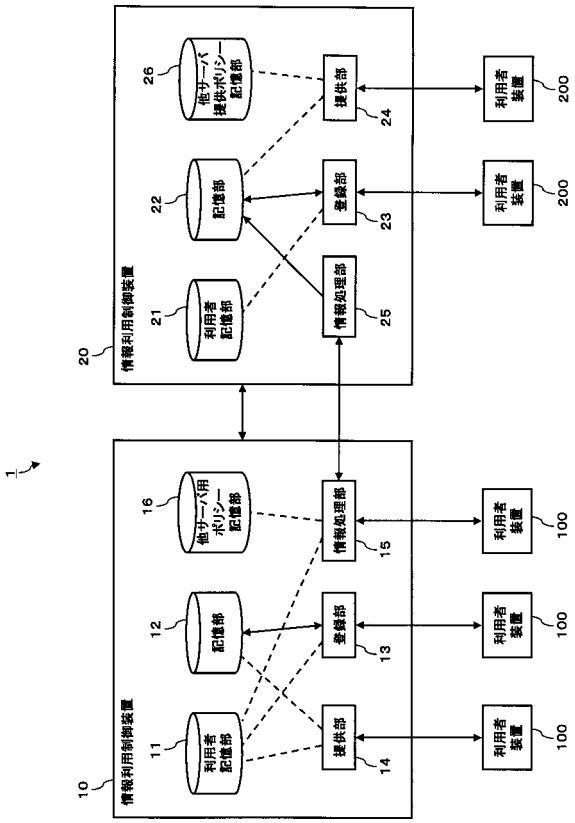
【図２３】第２の実施の形態における、保護コンテンツの作成におけるサーバ２０の動作の一例を示すフローチャートである。

【符号の説明】

【０１４０】

１　情報利用制御システム、１０，２０　情報利用制御装置（サーバ）、１１，２１　利用者記憶部、１２，２２　記憶部、１３，２３　登録部、１４，２４　提供部、１５，２５　情報処理部、１６　他サーバ用ポリシー記憶部、２６　他サーバ提供ポリシー記憶部。

【図１】



【図２】

利用者ID
ユーザ11
ユーザ12
…

【図３】

ポリシーID	許可利用者	有効期間	許可操作
ポリシー11	ユーザ11	無期限	閲覧、編集
	ユーザ12	発行日から1ヶ月	印刷
	…	…	…
ポリシー12	グループ11	2007.9.1 -2007.9.30	閲覧
	…	…	…
…	…	…	…

【図４】

コンテンツID	ポリシーID
コンテンツ11	ポリシー11
コンテンツ12	ポリシー12
…	…

【図５】

利用者ID
ユーザ21
ユーザ22
…

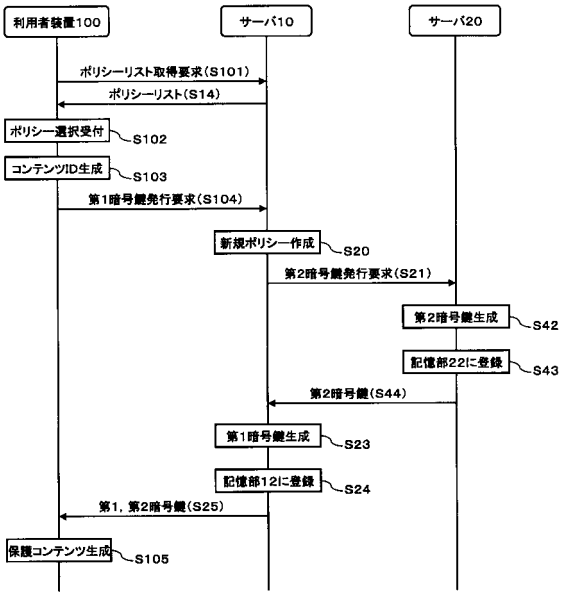
【図６】

サーバ名	ポリシーID	許可利用者	有効期間	許可操作
サーバ20	ポリシー2A	ユーザ21	無期限	閲覧
		ユーザ22	2007.9.1-2008.8.31	印刷
	ポリシー2B	…	…	…
	…	…	…	…
サーバ20－1	…	…	…	…
サーバ20－2	…	…	…	…
…	…	…	…	…

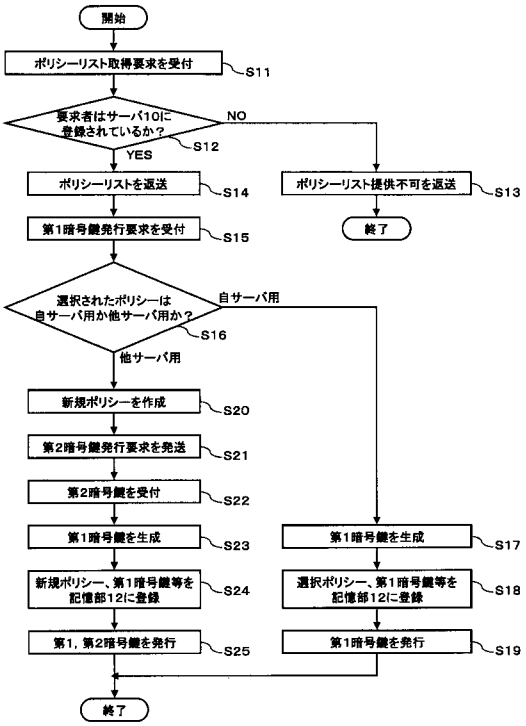
【図７】

ポリシーID	許可利用者	有効期間	許可操作
ポリシー2A	ユーザ21	無期限	閲覧
	ユーザ22	2007.9.1-2008.8.31	印刷
ポリシー2B	…	…	…
…	…	…	…

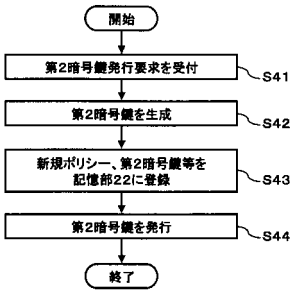
【図８】



【図９】



【図１０】



【図１１】

ポリシーID	許可利用者	有効期間	許可操作
ポリシー21	…	…	…
ポリシー22	…	…	…
…	…	…	…
ポリシー13	ポリシー2Aを参照	−	−

【図１２】

コンテンツID	ポリシーID
コンテンツ21	ポリシー21
コンテンツ22	ポリシー22
…	…
コンテンツ13	ポリシー13

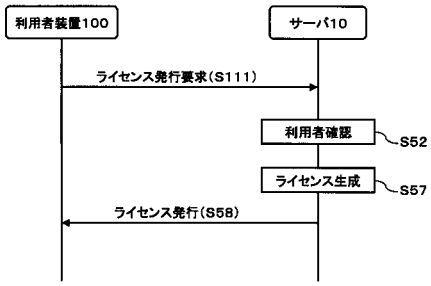
【図１３】

ポリシーID	許可利用者	有効期間	許可操作
ポリシー11	ユーザ11	無期限	閲覧、編集
	ユーザ12	発行日から1ヶ月	印刷
	…	…	…
ポリシー12	グループ11	2007.9.1 -2007.9.30	閲覧
	…	…	…
…	…	…	…
ポリシー13	ユーザ11	無期限	閲覧、編集
	ポリシー2Aを参照	−	−

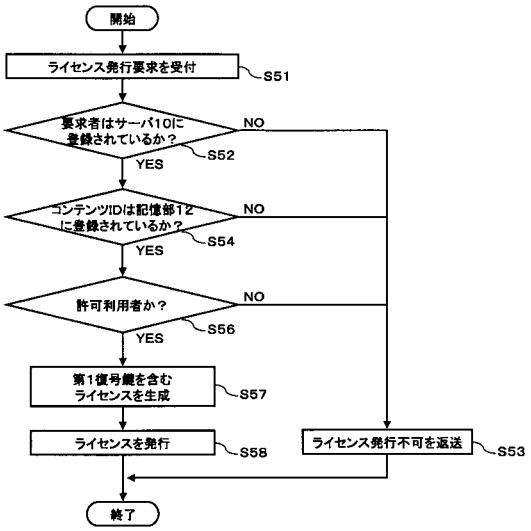
【図１４】

コンテンツID	ポリシーID
コンテンツ11	ポリシー11
コンテンツ12	ポリシー12
…	…
コンテンツ13	ポリシー13

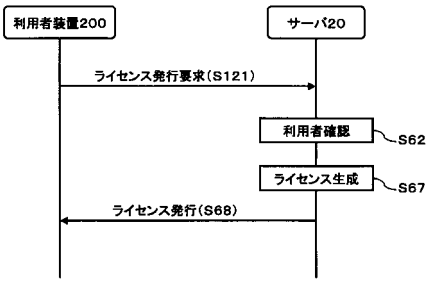
【図１５】



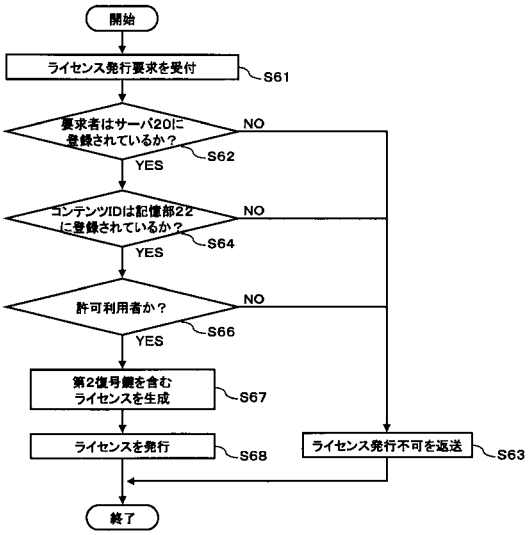
【図１６】



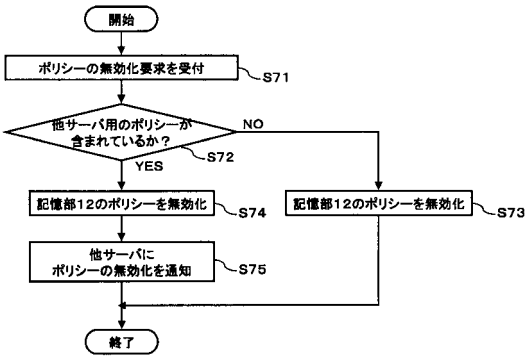
【図１７】



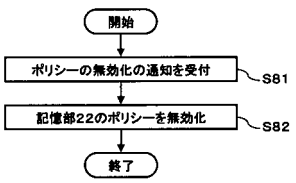
【図１８】



【図１９】



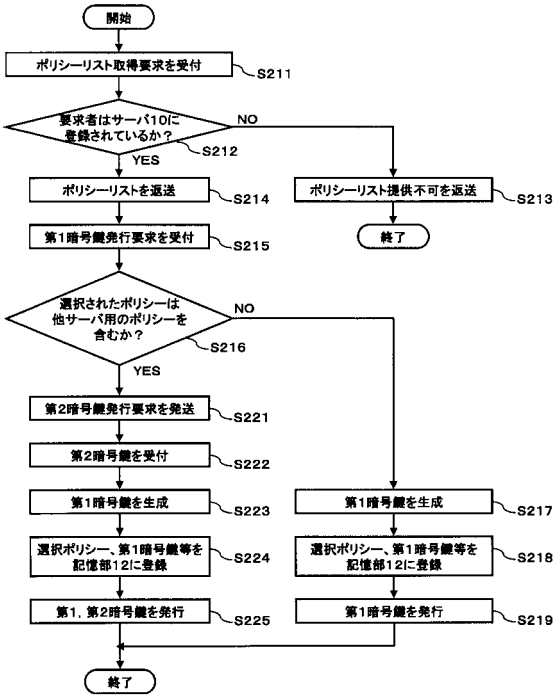
【図２０】



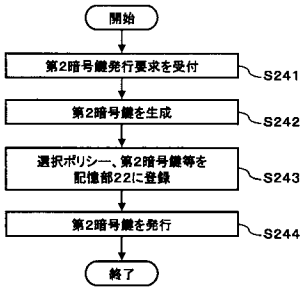
【図２１】

ポリシーID	許可利用者	有効期間	許可操作
ポリシー11	ユーザ11	無期限	閲覧、編集
	ユーザ12	発行日から1ヶ月	印刷
	…	…	…
ポリシー12	グループ11	2007.9.1 -2007.9.30	閲覧
	…	…	…
…	…	…	…
ポリシー14	保護コンテンツ作成者	無期限	閲覧、編集
	ポリシー2Aを参照	−	−
ポリシー15	ユーザ11	発行日から1ヶ月	閲覧
	ポリシー2Bを参照	−	−

【図２２】



【図２３】



フロントページの続き

(51)Int.Cl. F I
H04L 9/08 (2006.01) G06F 17/60 512
H04L 9/00 601B

(72)発明者 中野渡 敬教
東京都港区赤坂九丁目７番３号 富士ゼロックス株式会社内

審査官 高橋 克

(56)参考文献 特開２００３－３２３２２４（ＪＰ，Ａ）
特開２０００－０１０７７７（ＪＰ，Ａ）
特開２００４－３０２８１７（ＪＰ，Ａ）
特開２００５－３３２２４１（ＪＰ，Ａ）
特表２００８－５３９５１８（ＪＰ，Ａ）
特開２００４－０３８６５２（ＪＰ，Ａ）
特開２００１－２７３１３４（ＪＰ，Ａ）
特開平１１－２０３１２５（ＪＰ，Ａ）
特開２００３－０５８６５７（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ ２１
Ｇ０６Ｑ １０／００
Ｇ０６Ｑ ３０／００
Ｇ０６Ｑ ５０／００
Ｈ０４Ｌ ９／０８