

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第4883015号
(P4883015)

(45) 発行日 平成24年2月22日(2012.2.22)

(24) 登録日 平成23年12月16日(2011.12.16)

(51) Int.Cl.		F I			
G06F 21/22	(2006.01)		G06F 9/06		660G
G06F 21/24	(2006.01)		G06F 12/14		520B
			G06F 12/14		530B

請求項の数 17 (全 30 頁)

(21) 出願番号	特願2008-10188 (P2008-10188)	(73) 特許権者	000002185
(22) 出願日	平成20年1月21日(2008.1.21)		ソニー株式会社
(65) 公開番号	特開2009-169893 (P2009-169893A)		東京都港区港南1丁目7番1号
(43) 公開日	平成21年7月30日(2009.7.30)	(74) 代理人	100093241
審査請求日	平成21年3月23日(2009.3.23)		弁理士 官田 正昭
		(74) 代理人	100101801
			弁理士 山田 英治
		(74) 代理人	100086531
			弁理士 澤田 俊夫
		(74) 代理人	100095496
			弁理士 佐々木 榮二
		(72) 発明者	上田 健二郎
			東京都港区港南1丁目7番1号 ソニー株式会社内

最終頁に続く

(54) 【発明の名称】 情報処理装置、ディスク、および情報処理方法、並びにプログラム

(57) 【特許請求の範囲】

【請求項1】

ディスクに記録されたアプリケーションプログラムの利用制御を行なう情報処理装置であり、

前記アプリケーションプログラムを利用した処理を実行するアプリケーション実行部と

、
前記アプリケーションプログラムの提供主体であるコンテンツオーナーの無効化情報を記録した証明書リポケーションリスト(CRL)を参照して、前記アプリケーションプログラムの正当性を示す証明書としてディスクに記録されるアプリケーション証明書に記録されたコンテンツオーナー識別子が、前記証明書リポケーションリスト(CRL)に含まれるか否かを検証し、含まれている場合には、

前記ディスクの記録コンテンツの正当性を示す証明書としてディスクに記録されているコンテンツ証明書に格納されたコンテンツ証明書タイムスタンプと、前記証明書リポケーションリスト(CRL)に格納されたCRLタイムスタンプを取得して、両タイムスタンプの比較を行い、前記コンテンツ証明書タイムスタンプとCRLタイムスタンプとの時間的な前後関係を検証するデータ検証部と、

前記コンテンツ証明書タイムスタンプが、前記CRLタイムスタンプ以降の日時データを有する場合、前記アプリケーション実行部におけるアプリケーションプログラムの利用処理を禁止または制限するアプリケーション制御部と、

を有することを特徴とする情報処理装置。

【請求項 2】

前記コンテンツ証明書タイムスタンプは、コンテンツ証明書の発行主体による署名生成日時を示す日時情報であり、

前記 C R L タイムスタンプは、前記アプリケーション証明書の失効日時、すなわち前記アプリケーション証明書に記録されたコンテンツオーナーの無効化日時を示す日時情報であることを特徴とする請求項 1 に記載の情報処理装置。

【請求項 3】

前記アプリケーション制御部は、

前記アプリケーション実行部が、ディスクもしくは情報処理装置に記録された識別情報を取得する処理を禁止する処理を実行することを特徴とする請求項 1 に記載の情報処理装置。

10

【請求項 4】

前記識別情報は、

(a) ディスク固有の識別情報であるメディア ID (P M S N)、

(b) ディスクのタイトル単位で設定されるボリューム ID、

(c) ディスク記録コンテンツの正当性を示すコンテンツ証明書の識別情報としてのコンテンツ証明書 ID、

(d) 情報処理装置の識別情報であるデバイスバイディング ID、

上記 (a) ~ (d) いずれかの識別情報であることを特徴とする請求項 3 に記載の情報処理装置。

20

【請求項 5】

前記アプリケーション制御部は、

前記アプリケーション実行部が、ディスクに記録されたコンテンツの再生またはコピーまたは外部出力する処理を禁止または制限する処理を実行することを特徴とする請求項 1 に記載の情報処理装置。

【請求項 6】

前記アプリケーション制御部は、

前記アプリケーション実行部が、ネットワークを介して外部サーバに接続する処理を禁止または制限する処理を実行することを特徴とする請求項 1 に記載の情報処理装置。

【請求項 7】

前記アプリケーション制御部は、

前記アプリケーション実行部が、ディスク記録データの読み取りまたは利用処理を行なうプログラム実行部に対する A P I 呼び出し処理を禁止または制限する処理を実行することを特徴とする請求項 1 に記載の情報処理装置。

30

【請求項 8】

前記データ検証部は、さらに、

前記アプリケーション証明書をディスクから読み出して第 1 の署名検証を実行し、

さらに、前記アプリケーションプログラムの正当性を示す証明書としてディスクに記録されたルート証明書を含むデータに対する署名を有するデータをディスクから読み出して第 2 の署名検証を実行し、

40

前記アプリケーション制御部は、

前記データ検証部における第 1 および第 2 の署名検証処理において、検証が失敗した場合に、前記アプリケーション実行部におけるアプリケーションプログラムの利用処理を禁止または制限することを特徴とする請求項 1 に記載の情報処理装置。

【請求項 9】

情報処理装置において、ディスクに記録されたアプリケーションプログラムの利用制御を行なう情報処理方法であり、

前記情報処理装置のデータ検証部が、前記アプリケーションプログラムの提供主体であるコンテンツオーナーの無効化情報を記録した証明書リボケーションリスト (C R L) を参照して、前記アプリケーションプログラムの正当性を示す証明書としてディスクに記録

50

されるアプリケーション証明書に記録されたコンテンツオーナー識別子が、前記証明書リポーションリスト（CRL）に含まれるか否かを検証し、含まれている場合には、

前記ディスクの記録コンテンツの正当性を示す証明書としてディスクに記録されているコンテンツ証明書に格納されたコンテンツ証明書タイムスタンプと、前記証明書リポーションリスト（CRL）に格納されたCRLタイムスタンプを取得して、両タイムスタンプの比較を行い、前記コンテンツ証明書タイムスタンプとCRLタイムスタンプとの時間的な前後関係を検証するデータ検証ステップと、

前記情報処理装置のアプリケーション制御部が、前記コンテンツ証明書タイムスタンプが、前記CRLタイムスタンプ以降の日時データを有する場合、前記アプリケーションプログラムの利用処理を禁止または制限するアプリケーション制御ステップと、

を実行することを特徴とする情報処理方法。

【請求項10】

前記コンテンツ証明書タイムスタンプは、コンテンツ証明書の発行主体による署名生成日時を示す日時情報であり、

前記CRLタイムスタンプは、前記アプリケーション証明書の失効日時、すなわち前記アプリケーション証明書に記録されたコンテンツオーナーの無効化日時を示す日時情報であることを特徴とする請求項9に記載の情報処理方法。

【請求項11】

前記アプリケーション制御ステップは、

アプリケーション実行部が、ディスクもしくは情報処理装置に記録された識別情報を取得する処理を禁止する処理を実行することを特徴とする請求項9に記載の情報処理方法。

【請求項12】

前記識別情報は、

(a) ディスク固有の識別情報であるメディアID（PMSN）、

(b) ディスクのタイトル単位で設定されるボリュームID、

(c) ディスク記録コンテンツの正当性を示すコンテンツ証明書の識別情報としてのコンテンツ証明書ID、

(d) 情報処理装置の識別情報であるデバイスバイディングID、

上記(a)～(d)いずれかの識別情報であることを特徴とする請求項11に記載の情報処理方法。

【請求項13】

前記アプリケーション制御部は、

アプリケーション実行部が、ディスクに記録されたコンテンツの再生またはコピーまたは外部出力する処理を禁止または制限する処理を実行することを特徴とする請求項9に記載の情報処理方法。

【請求項14】

前記アプリケーション制御ステップは、

アプリケーション実行部が、ネットワークを介して外部サーバに接続する処理を禁止または制限する処理を実行することを特徴とする請求項9に記載の情報処理方法。

【請求項15】

前記アプリケーション制御ステップは、

アプリケーション実行部が、ディスク記録データの読み取りまたは利用処理を行なうプログラム実行部に対するAPI呼び出し処理を禁止または制限する処理を実行することを特徴とする請求項9に記載の情報処理方法。

【請求項16】

前記データ検証ステップは、さらに、

前記アプリケーション証明書をディスクから読み出して第1の署名検証を実行し、

さらに、前記アプリケーションプログラムの正当性を示す証明書としてディスクに記録されたルート証明書を含むデータに対する署名を有するデータをディスクから読み出して第2の署名検証を実行するステップであり、

10

20

30

40

50

前記アプリケーション制御ステップは、

前記データ検証ステップにおける第1および第2の署名検証処理において、検証が失敗した場合に、前記アプリケーション実行部におけるアプリケーションプログラムの利用処理を禁止または制限するステップであることを特徴とする請求項9に記載の情報処理方法。

【請求項17】

情報処理装置において、ディスクに記録されたアプリケーションプログラムの利用制御を行なわせるプログラムであり、

前記情報処理装置のデータ検証部に、前記アプリケーションプログラムの提供主体であるコンテンツオーナーの無効化情報を記録した証明書リポーションリスト(CRL)を参照して、前記アプリケーションプログラムの正当性を示す証明書としてディスクに記録されるアプリケーション証明書に記録されたコンテンツオーナー識別子が、前記証明書リポーションリスト(CRL)に含まれるか否かを検証させ、含まれている場合には、

前記ディスクの記録コンテンツの正当性を示す証明書としてディスクに記録されているコンテンツ証明書に格納されたコンテンツ証明書タイムスタンプと、前記証明書リポーションリスト(CRL)に格納されたCRLタイムスタンプを取得して、両タイムスタンプの比較を実行させるデータ検証ステップと、

前記情報処理装置のアプリケーション制御部に、前記コンテンツ証明書タイムスタンプが、前記CRLタイムスタンプ以降の日時データを有する場合、前記アプリケーションプログラムの利用処理を禁止または制限させるアプリケーション制御ステップと、

を実行させることを特徴とするプログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、情報処理装置、ディスク、および情報処理方法、並びにプログラムに関する。さらに、詳細には情報記録媒体に記録されたコンテンツや識別情報(ID)の読み取り制御や利用制御を行う情報処理装置、ディスク、および情報処理方法、並びにプログラムに関する。

【背景技術】

【0002】

コンテンツの記録媒体としてDVD(Digital Versatile Disc)、Blu-ray Disc(登録商標)などのディスクが利用されている。例えば映画コンテンツなどがディスク(例えばROMディスク)に記録されてユーザに提供されるが、これらのディスク記録コンテンツは、多くの場合、その作成者あるいは販売者に著作権、頒布権等が保有されたコンテンツである。このようなコンテンツについては例えば許可のないコピー(複製)等を防止するための利用制御がなされる。

【0003】

利用制御の形態としては様々な形態があるが、例えば、著作権保護技術を規定しているAACS(Advanced Access Content System)の規定では、ディスク記録コンテンツの利用に際して、メディアIDなどのID情報をディスクから読み取らせて、読み取りIDの確認やID情報を利用した鍵生成など実行させてコンテンツ利用制御を行なう構成としている。

【0004】

例えば、ディスクには、以下のような識別情報(ID)が記録されている。

(a) ディスク固有の識別情報であるメディアID(PMSN(Pre-recorded Media Serial Numberと呼ばれる場合もある)、

(b) ディスクのタイトル単位で設定されるボリュームID、

(c) ディスク記録コンテンツに対応して設定されたコンテンツ証明書の識別情報としてのコンテンツ証明書ID、

例えばこれらの識別情報(ID)がディスクに記録されている。

【 0 0 0 5 】

再生装置は、ディスクから例えば上記 (a) ~ (c) の少なくともいずれかの識別情報 (I D) を読み取り、所定のシーケンスに従った処理、例えば I D を利用した鍵生成やコンテンツ復号などによりコンテンツ利用を行なう。さらに、上記の各種識別情報 (I D) をサーバに送信し、サーバにおける I D 確認に基づいて、サーバから様々な付加コンテンツやサービスデータなどを受領することが行なわれる場合もある。

【 0 0 0 6 】

なお、ディスクに記録された上記 (a) ~ (c) ではなく、
(d) 再生装置対応の識別情報であるデバイスバイディング I D 、
が利用される場合もある。デバイスバイディング I D は、再生装置固有の識別情報として再生装置内のメモリに記録され、ディスク格納コンテンツの利用、後発データのサーバからの取得、再生装置のハードディスクなどの記憶部に格納された後発データの利用などに際して、例えば再生装置の確認処理としての I D 確認や、鍵生成、コンテンツ復号などの処理に利用される。

10

【 0 0 0 7 】

上記 (a) ~ (d) の識別情報 (I D) を読み取ってコンテンツの再生やコピー処理、あるいはサーバからのデータ取得処理などを行なうためには、所定のプログラムを再生装置において実行することが必要である。プログラムはディスク格納コンテンツに対応して作成されるプログラムである場合が多く、コンテンツとともにディスクに記録され、再生装置は、プログラムをディスクから読み取って実行する。

20

【 0 0 0 8 】

このようなプログラムは、例えば J a v a (登録商標) を利用した簡易プログラムとして作成され、例えばコンテンツ所有者や提供者 (コンテンツオーナー) において、あるいはその委託によって作成されることが多い、従って、不正なプログラムが混在する可能性もある。

【 0 0 0 9 】

不正なプログラムは、ディスクに記録された識別情報 (I D) を不正に取得してコンテンツを不正に利用し、またサーバからのサービスデータの不正取得を行うといった不正な処理に利用される可能性がある。

【 0 0 1 0 】

図 1 を参照して現状の A A C S 規定におけるコンテンツ利用制御構成の概要について説明する。図 1 には、コンテンツ 1 2 1 を格納したディスク (メディア) 1 2 0 、ディスク記録コンテンツを提供するコンテンツオーナー 1 1 0 、コンテンツ管理処理を行なうライセンス管理部 1 3 0 を示している。ライセンス管理部 1 3 0 は例えば A A C S 規定に従ったコンテンツ利用管理を行なう A A C S L A (L i c e n s i n g A d m i n i s t r a t o r) によって運営される。

30

【 0 0 1 1 】

ディスク 1 2 0 には、コンテンツ 1 2 1 の他、前述した識別情報 (I D) 1 2 2 が記録されている。識別情報 (I D) 1 2 2 としては、

- (a) ディスク固有の識別情報であるメディア I D (P M S N) 1 2 6 、
 - (b) ディスクのタイトル単位で設定されるボリューム I D 1 2 7 、
 - (c) ディスク記録コンテンツに対応して設定されたコンテンツ証明書の識別情報としてのコンテンツ証明書 I D 1 2 8 、
- これらの I D 情報が含まれる。

40

【 0 0 1 2 】

ディスク 1 2 0 には、コンテンツ 1 2 1 が正当なコンテンツ、すなわちライセンス管理部 (A A C S L A) 1 3 0 によって認定された正当コンテンツであることを証明するためのコンテンツ証明書 1 2 3 が記録される。コンテンツ証明書 1 2 3 はディスク 1 2 0 に記録されるコンテンツ 1 2 1 に対応してその正当性を証明するデータとしてライセンス管理部 1 3 0 の管理下で発行されディスク 1 2 0 に記録される。

50

【 0 0 1 3 】

コンテンツ証明書 1 2 3 は、ライセンス管理部 1 3 0 内にその詳細を示すように、ルート証明書ハッシュ値を記録し、これらの記録ハッシュ値に対して、ライセンス管理部 (A A C S L A) 1 3 0 の秘密鍵による電子署名が付与された構成を持つ。ルート証明書 1 2 4 はディスク 1 2 0 に記録され、その構成は、図のコンテンツオーナー 1 1 0 内に示すように、コンテンツオーナーの公開鍵に対して、コンテンツオーナーの秘密鍵で署名を設定した構成を持つ。

【 0 0 1 4 】

このディスクに記録されたコンテンツ 1 2 1 を再生する再生装置は、コンテンツ証明書に設定された署名検証を実行して、コンテンツ証明書の正当性が確認されたことを条件としてコンテンツ 1 2 1 の利用が許容される。このように、コンテンツに関しては、厳格に正当性の確認が実行されることになる。

10

【 0 0 1 5 】

しかし、さらに、ディスク 1 2 0 にはディスク記録アプリケーション 1 2 5 が記録される場合がある。このディスク記録アプリケーション 1 2 5 は、例えばコンテンツ 1 2 1 の再生処理、その他の処理に利用されるプログラムである。具体的には、コンテンツ利用ユーザに対して、サービスデータをサーバから提供するためのアプリケーションなどである。ディスク 1 2 0 に記録された識別情報 (I D) 1 2 2 をサーバに送信することで、サーバからサービスデータを取得するために実行するプログラムなどである。

【 0 0 1 6 】

このディスク記録アプリケーション 1 2 5 は、図のコンテンツオーナー 1 1 0 内に示すように、コンテンツオーナーが提供するアプリケーションに対して、コンテンツオーナーの秘密鍵で署名を設定した構成を持つ。

20

【 0 0 1 7 】

ディスク 1 2 0 に記録されたディスク記録アプリケーション 1 2 5 を利用する再生装置は、コンテンツオーナーの公開鍵を適用して、ディスク記録アプリケーション 1 2 5 に設定された署名検証を行なうことで、アプリケーションの正当性を確認してアプリケーションを実行することになる。

【 0 0 1 8 】

しかし、このディスク記録アプリケーション 1 2 5 は、コンテンツオーナー 1 1 0 が独自に作成可能であり、第三者による監視がなされていない。前述したように、コンテンツについてはコンテンツに対応してライセンス管理部 1 3 0 が発行するコンテンツ証明書 1 2 3 によって、その正当性を確認できるが、ディスク記録アプリケーション 1 2 5 はこのように第三者による正当性の確認ができないデータであり、コンテンツオーナー 1 1 0 が不正なアプリケーションを作成してしまう可能性が否定できない。

30

【 0 0 1 9 】

前述したように不正なアプリケーションを利用することで、ディスク 1 2 0 に記録された識別情報 (I D) 1 2 2 を不正に取得してコンテンツ 1 2 1 を不正に利用し、またサーバからのサービスデータの不正取得を行うといった不正な処理に利用される可能性がある。

40

【 発明の開示 】

【 発明が解決しようとする課題 】

【 0 0 2 0 】

本発明は、例えば上記の問題点を鑑みてなされたものであり、ディスクに記録されたコンテンツや識別情報の不正な読み取りや、利用を防止する情報処理装置、ディスク、および情報処理方法、並びにプログラム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 】

【 0 0 2 1 】

本発明の第 1 の側面は、

ディスクに記録されたアプリケーションプログラムの利用制御を行なう情報処理装置で

50

あり、

前記アプリケーションプログラムを利用した処理を実行するアプリケーション実行部と

、
前記アプリケーションプログラムの提供主体であるコンテンツオーナーの無効化情報を記録した証明書リボケーションリスト（CRL）を参照して、前記アプリケーションプログラムに対応する証明書としてディスクに記録されるアプリケーション証明書に記録されたコンテンツオーナー識別子が、前記証明書リボケーションリスト（CRL）に含まれるか否かを検証し、含まれている場合には、

前記ディスクの記録コンテンツに対応する証明書としてディスクに記録されているコンテンツ証明書に格納されたコンテンツ証明書タイムスタンプと、前記証明書リボケーションリスト（CRL）に格納されたCRLタイムスタンプを取得して、両タイムスタンプの比較を実行するデータ検証部と、

前記コンテンツ証明書タイムスタンプが、前記CRLタイムスタンプ以降の日時データを有する場合、前記アプリケーション実行部におけるアプリケーションプログラムの利用処理を禁止または制限するアプリケーション制御部と、

を有することを特徴とする情報処理装置にある。

【0022】

さらに、本発明の情報処理装置の一実施態様において、前記コンテンツ証明書タイムスタンプは、コンテンツ証明書の発行主体による署名生成日時に対応する日時情報であり、前記CRLタイムスタンプは、前記アプリケーション証明書の失効日時、すなわち前記アプリケーション証明書に記録されたコンテンツオーナーの無効化日時に対応する日時情報であることを特徴とする。

【0023】

さらに、本発明の情報処理装置の一実施態様において、前記アプリケーション制御部は、前記アプリケーション実行部が、ディスクもしくは情報処理装置に記録された識別情報を取得する処理を禁止する処理を実行することを特徴とする。

【0024】

さらに、本発明の情報処理装置の一実施態様において、前記識別情報は、
（a）ディスク固有の識別情報であるメディアID（PMSN）、
（b）ディスクのタイトル単位で設定されるボリュームID、
（c）ディスク記録コンテンツに対応して設定されたコンテンツ証明書の識別情報としてのコンテンツ証明書ID、
（d）情報処理装置の識別情報であるデバイスバイディングID、
上記（a）～（d）いずれかの識別情報であることを特徴とする。

【0025】

さらに、本発明の情報処理装置の一実施態様において、前記アプリケーション制御部は、前記アプリケーション実行部が、ディスクに記録されたコンテンツの再生またはコピーまたは外部出力する処理を禁止または制限する処理を実行することを特徴とする。

【0026】

さらに、本発明の情報処理装置の一実施態様において、前記アプリケーション制御部は、前記アプリケーション実行部が、ネットワークを介して外部サーバに接続する処理を禁止または制限する処理を実行することを特徴とする。

【0027】

さらに、本発明の情報処理装置の一実施態様において、前記アプリケーション制御部は、前記アプリケーション実行部が、ディスク記録データの読み取りまたは利用処理を行なうプログラム実行部に対するAPI呼び出し処理を禁止または制限する処理を実行することを特徴とする。

【0028】

さらに、本発明の情報処理装置の一実施態様において、前記データ検証部は、さらに、前記アプリケーション証明書をディスクから読み出して第1の署名検証を実行し、さらに

10

20

30

40

50

、前記アプリケーションプログラムに対応する証明書としてディスクに記録されたルート証明書を含むデータに対する署名を有するルート証明書対応データをディスクから読み出して第2の署名検証を実行し、前記アプリケーション制御部は、前記データ検証部における第1および第2の署名検証処理において、検証が失敗した場合に、前記アプリケーション実行部におけるアプリケーションプログラムの利用処理を禁止または制限することを特徴とする。

【0029】

さらに、本発明の第2の側面は、
コンテンツと、

前記コンテンツに対応する証明データであり、コンテンツ証明書の発行主体による署名生成日時に対応するタイムスタンプを記録したコンテンツ証明書と、

アプリケーションプログラムと、

前記アプリケーションプログラムに対応する証明書であるアプリケーション証明書を記録し、

前記アプリケーションプログラムを実行しようとする再生装置において、

前記アプリケーションプログラムの提供主体であるコンテンツオーナーの無効化情報を記録した証明書リボケーションリスト(CRL)に、前記アプリケーション証明書に記録されたコンテンツオーナー識別子が含まれている場合、

前記コンテンツ証明書に格納されたコンテンツ証明書タイムスタンプと、前記証明書リボケーションリスト(CRL)に格納されたCRLタイムスタンプとの比較を行い、前記コンテンツ証明書タイムスタンプが、前記CRLタイムスタンプ以降の日時データを有する場合、アプリケーションプログラムの利用処理を禁止または制限することを可能としたディスクにある。

【0030】

さらに、本発明の第3の側面は、

情報処理装置において、ディスクに記録されたアプリケーションプログラムの利用制御を行なう情報処理方法であり、

データ検証部が、前記アプリケーションプログラムの提供主体であるコンテンツオーナーの無効化情報を記録した証明書リボケーションリスト(CRL)を参照して、前記アプリケーションプログラムに対応する証明書としてディスクに記録されるアプリケーション証明書に記録されたコンテンツオーナー識別子が、前記証明書リボケーションリスト(CRL)に含まれるか否かを検証し、含まれている場合には、

前記ディスクの記録コンテンツに対応する証明書としてディスクに記録されているコンテンツ証明書に格納されたコンテンツ証明書タイムスタンプと、前記証明書リボケーションリスト(CRL)に格納されたCRLタイムスタンプを取得して、両タイムスタンプの比較を実行するデータ検証ステップと、

アプリケーション制御部が、前記コンテンツ証明書タイムスタンプが、前記CRLタイムスタンプ以降の日時データを有する場合、前記アプリケーションプログラムの利用処理を禁止または制限するアプリケーション制御ステップと、

を有することを特徴とする情報処理方法にある。

【0031】

さらに、本発明の情報処理方法の一実施態様において、前記コンテンツ証明書タイムスタンプは、コンテンツ証明書の発行主体による署名生成日時に対応する日時情報であり、前記CRLタイムスタンプは、前記アプリケーション証明書の失効日時、すなわち前記アプリケーション証明書に記録されたコンテンツオーナーの無効化日時に対応する日時情報であることを特徴とする。

【0032】

さらに、本発明の情報処理方法の一実施態様において、前記アプリケーション制御ステップは、アプリケーション実行部が、ディスクもしくは情報処理装置に記録された識別情報を取得する処理を禁止する処理を実行することを特徴とする。

【0033】

さらに、本発明の情報処理方法の一実施態様において、前記識別情報は、

- (a) ディスク固有の識別情報であるメディアID (PMSN)、
 - (b) ディスクのタイトル単位で設定されるボリュームID、
 - (c) ディスク記録コンテンツに対応して設定されたコンテンツ証明書の識別情報としてのコンテンツ証明書ID、
 - (d) 情報処理装置の識別情報であるデバイスバインディングID、
- 上記(a)～(d)いずれかの識別情報であることを特徴とする。

【0034】

さらに、本発明の情報処理方法の一実施態様において、前記アプリケーション制御部は、アプリケーション実行部が、ディスクに記録されたコンテンツの再生またはコピーまたは外部出力する処理を禁止または制限する処理を実行することを特徴とする。

【0035】

さらに、本発明の情報処理方法の一実施態様において、前記アプリケーション制御ステップは、アプリケーション実行部が、ネットワークを介して外部サーバに接続する処理を禁止または制限する処理を実行することを特徴とする。

【0036】

さらに、本発明の情報処理方法の一実施態様において、前記アプリケーション制御ステップは、アプリケーション実行部が、ディスク記録データの読み取りまたは利用処理を行なうプログラム実行部に対するAPI呼び出し処理を禁止または制限する処理を実行することを特徴とする。

【0037】

さらに、本発明の情報処理方法の一実施態様において、前記データ検証ステップは、さらに、前記アプリケーション証明書をディスクから読み出して第1の署名検証を実行し、さらに、前記アプリケーションプログラムに対応する証明書としてディスクに記録されたルート証明書を含むデータに対する署名を有するルート証明書対応データをディスクから読み出して第2の署名検証を実行するステップであり、前記アプリケーション制御ステップは、前記データ検証ステップにおける第1および第2の署名検証処理において、検証が失敗した場合に、前記アプリケーション実行部におけるアプリケーションプログラムの利用処理を禁止または制限するステップであることを特徴とする。

【0038】

さらに、本発明の第4の側面は、情報処理装置において、ディスクに記録されたアプリケーションプログラムの利用制御を行なわせるプログラムであり、

データ検証部に、前記アプリケーションプログラムの提供主体であるコンテンツオーナーの無効化情報を記録した証明書リボケーションリスト(CRL)を参照して、前記アプリケーションプログラムに対応する証明書としてディスクに記録されるアプリケーション証明書に記録されたコンテンツオーナー識別子が、前記証明書リボケーションリスト(CRL)に含まれるか否かを検証させ、含まれている場合には、

前記ディスクの記録コンテンツに対応する証明書としてディスクに記録されているコンテンツ証明書に格納されたコンテンツ証明書タイムスタンプと、前記証明書リボケーションリスト(CRL)に格納されたCRLタイムスタンプを取得して、両タイムスタンプの比較を実行させるデータ検証ステップと、

アプリケーション制御部に、前記コンテンツ証明書タイムスタンプが、前記CRLタイムスタンプ以降の日時データを有する場合、前記アプリケーションプログラムの利用処理を禁止または制限させるアプリケーション制御ステップと、

を有することを特徴とするプログラムにある。

【0039】

なお、本発明のプログラムは、例えば、様々なプログラム・コードを実行可能な汎用シ

10

20

30

40

50

システムに対して、コンピュータ可読な形式で提供する記憶媒体、通信媒体によって提供可能なプログラムである。このようなプログラムをコンピュータ可読な形式で提供することにより、コンピュータ・システム上でプログラムに応じた処理が実現される。

【0040】

本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。なお、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

【発明の効果】

【0041】

本発明の一実施例によれば、ディスクに記録されたアプリケーションプログラムの提供主体であるコンテンツオーナーの無効化情報を記録した証明書リポケーションリスト(CRL)を参照して、アプリケーション証明書に記録されたコンテンツオーナー識別子が、証明書リポケーションリスト(CRL)に含まれるか否かを検証し、含まれている場合に、コンテンツ証明書に格納されたタイムスタンプと、証明書リポケーションリスト(CRL)のタイムスタンプの比較を実行して、コンテンツ証明書タイムスタンプが、CRLタイムスタンプ以降の日時データを有する場合、アプリケーション実行部におけるアプリケーションプログラムの利用処理を禁止または制限する構成とした。本構成により、無効化される前のアプリケーションは利用制限を行わず、無効化された後のアプリケーションに対してのみ利用制限を行なう構成が実現される。

【発明を実施するための最良の形態】

【0042】

以下、図面を参照しながら本発明の情報処理装置、ディスク、および情報処理方法、並びにプログラムの詳細について説明する。

【0043】

図2を参照して、本発明の構成の概要について説明する。図2には、先に図1を参照して説明したと同様、コンテンツ221を格納したディスク(メディア)220、ディスク記録コンテンツを提供するコンテンツオーナー210、コンテンツ管理処理を行なうライセンス管理部230を示し、さらに、新たに、認証局(BDA-CA)240を示している。ライセンス管理部230は例えばAACSR規定に従ったコンテンツ利用管理を行なうAACSLA(Licensing Administrator)によって運営される。

【0044】

なお、本実施例ではディスク220として、BD(Blu-ray Disc(登録商標))、具体的にはROM型のBDであるBD-ROMディスクについて説明する。なお、実施例ではBD-ROMを適用した例を説明するが、BD-ROMの適用例は一例であり、その他の種類のメディアであっても本発明の適用は可能である。

【0045】

ディスク220には、コンテンツ221の他、先に図1を参照して説明したと同様、識別情報(ID)222が記録されている。識別情報(ID)222としては、

- (a) ディスク固有の識別情報であるメディアID(PMSN)226、
 - (b) ディスクのタイトル単位で設定されるボリュームID227、
 - (c) ディスク記録コンテンツに対応して設定されたコンテンツ証明書の識別情報としてのコンテンツ証明書ID228、
- これらのID情報が含まれる。

【0046】

再生装置は、ディスクから例えば上記(a)~(c)の少なくともいずれかの識別情報(ID)を読み取り、所定のシーケンスに従った処理、例えばIDを利用した鍵生成やコンテンツ復号などによりコンテンツ利用を行なう。さらに、上記の各種識別情報(ID)をサーバに送信し、サーバにおけるID確認に基づいて、サーバから様々な付加コンテン

10

20

30

40

50

ツやサービスデータなどを受領することが行なわれる場合もある。

【 0 0 4 7 】

なお、ディスクに記録された上記 (a) ~ (c) ではなく、
 (d) 再生装置対応の識別情報であるデバイスバイディング I D、
 が利用される場合もある。デバイスバイディング I D は、再生装置固有の識別情報として再生装置内のメモリに記録され、ディスク格納コンテンツの利用、後発データのサーバからの取得、再生装置のハードディスクなどの記憶部に格納された後発データの利用などに際して、例えば再生装置の確認処理としての I D 確認や、鍵生成、コンテンツ復号などの処理に利用される。

【 0 0 4 8 】

ディスク 2 2 0 には、コンテンツ 2 2 1 が正当なコンテンツ、すなわちライセンス管理部 (A A C S L A) 2 3 0 によって管理された正当コンテンツであることを証明するためのコンテンツ証明書 (C o n t e n t C e r t) 2 2 3 が記録される。コンテンツ証明書 2 2 3 はディスク 2 2 0 に記録されるコンテンツ 2 2 1 に対応してその正当性を証明するデータとしてライセンス管理部 2 3 0 の管理下で発行されディスク 2 2 0 に記録される。

【 0 0 4 9 】

コンテンツ証明書 2 2 3 は、図 2 に示すライセンス管理部 2 3 0 内にその詳細を示すように、ルート証明書の構成データによって生成されたハッシュ値であるルート証明書ハッシュを記録し、これらの記録ハッシュ値に対して、ライセンス管理部 (A A C S L A) 2 3 0 の秘密鍵による電子署名が付与された構成を持つ。

【 0 0 5 0 】

また、ディスク 2 2 0 に記録されるルート証明書 (B D - J R o o t C e r t) 2 2 4 は、図 2 に示すコンテンツオーナー 2 1 0 内にその詳細を示すように、コンテンツオーナーの公開鍵と、コンテンツオーナーの公開鍵に対してコンテンツオーナーの秘密鍵で生成した署名を含むデータ構成を持ち、ディスク 2 2 0 に記録されるディスク記録アプリケーション 2 2 5 に対応する証明書としてディスク 2 2 0 に記録される。

【 0 0 5 1 】

ディスク 2 2 0 に記録されたコンテンツ 2 2 1 を再生する再生装置は、コンテンツ証明書 2 2 3 に設定された署名の検証を実行して、コンテンツ証明書 2 2 3 の正当性を確認し、この正当性確認を条件としたコンテンツ 2 2 1 の利用を行う。このように、コンテンツに関しては、厳格に正当性の確認が実行されることになる。

【 0 0 5 2 】

さらに、ディスク 2 2 0 にはディスク記録アプリケーション (B D - J a p p l i c a t i o n) 2 2 5 が記録される。このディスク記録アプリケーション 2 2 5 は、例えばコンテンツ 2 2 1 の再生処理やコピー処理、その他の処理、例えば、サービスデータを外部のサーバから受領するためのアプリケーションなどである。ディスク記録アプリケーション 2 2 5 は、図 2 に示すコンテンツオーナー 2 1 0 内に詳細を示すように、コンテンツオーナーが提供するアプリケーションに対して、コンテンツオーナーの秘密鍵で署名を設定した構成を持つ。

【 0 0 5 3 】

このディスク記録アプリケーション 2 2 5 は、ディスク 2 2 0 に記録された識別情報 2 2 2 の読み取りを直接実行することができないので、別のプログラムに識別情報 (I D) 2 2 2 の読み取りを依頼して、別のプログラムによってディスクから読み取られた識別情報 (I D) 2 2 2 を受領する。

【 0 0 5 4 】

図 3 を参照して、ディスク 2 2 0 に記録された識別情報 (I D) 2 2 2 の読み取り処理例について説明する。ディスク記録アプリケーション 2 2 5 は、再生装置 3 0 0 のアプリケーション実行部 3 0 1 において実行される。ディスク記録アプリケーション 2 2 5 は例えば J a v a (登録商標) プログラムであり、この場合、アプリケーション実行部 3 0 1

10

20

30

40

50

は、例えば、Java（登録商標）プログラムを実行するバーチャルマシン（BD - J Virtual Machineと呼ばれる）によって構成される。

【0055】

アプリケーション実行部301において実行するアプリケーションは、ディスク220に記録された識別情報222の読み取りを直接実行することはできないので、識別情報222の読み取りを実行するプログラムにID読み取りを依頼する。図3に示すAACSLレイヤ（ID情報取得プログラム実行部）302がディスク220に記録された識別情報222の読み取りを直接実行する。AACSLレイヤ302は、AACSL規定に従ったシーケンスに従ってデータ処理を実行するデータ処理部である。

【0056】

アプリケーション実行部301の実行するアプリケーションは、AACSLレイヤ（ID情報取得プログラム実行部）302に対してAPI（Application Programming Interface）呼び出しを実行する。このAPIは、ディスク220に記録された識別情報222の読み取りを行なわせる関数からなるAPIである。

【0057】

AACSLレイヤ（ID情報取得プログラム実行部）302は、アプリケーション実行部301からのAPI呼び出しに応じて、ディスク220に記録された識別情報222の読み取りを実行し、読み取った識別情報222をアプリケーション実行部301に提供することになる。その後、アプリケーション実行部301において実行されているアプリケーションは、取得した識別情報を利用してコンテンツの利用やサービスデータの取得、例えば取得識別情報（ID）をサーバに送信し、コンテンツのコピー許可情報や、その他のサービス情報などを受領するといった処理を行なう。

【0058】

なお、本実施例では、ディスクに記録された識別情報222を利用する例について説明するが、前述したように、

再生装置対応の識別情報であるデバイスバイディングID、

が利用される場合もある。デバイスバイディングIDは、再生装置固有の識別情報として再生装置内のメモリに記録され、ディスク格納コンテンツの利用、後発データのサーバからの取得、再生装置のハードディスクなどの記憶部に格納された後発データの利用などに際して、例えば再生装置の確認処理としてのID確認や、鍵生成、コンテンツ復号などの処理に利用される。以下では、ディスクに記録された識別情報222を利用する例について説明するが、再生装置対応の識別情報であるデバイスバイディングIDを再生装置のメモリから読み取って利用する場合も、以下に説明する識別情報222の読み取り処理と同様の処理として実行される。

【0059】

識別情報の読み取りや利用処理において問題となるのは、前述したように、アプリケーション実行部301において実行するアプリケーション、すなわちディスク記録アプリケーション225が不正なプログラムである可能性があることである。例えば識別情報222を不正に取得しようとして生成された不正プログラムである可能性もあることである。

【0060】

そこで、本発明の構成では、このような不正処理を防止するため、ディスク220に、さらにアプリケーション証明書（AACSL On-line Cert）251と、ルート証明書対応署名データ（AACSL On-line Sig）252を記録している。

【0061】

アプリケーション証明書（AACSL On-line Cert）251は、認証局（BDA - CA）240が発行する証明書であり、コンテンツオーナーの公開鍵に対して、認証局（BDA - CA）240の秘密鍵による署名データが設定された構成である。

【0062】

ルート証明書対応署名データ（AACSL On-line Sig）252は、コンテンツオーナー210が生成する署名データであり、ルート証明書224を含むデータに対し

10

20

30

40

50

て、コンテンツオーナーの秘密鍵を適用して生成される署名データである。

【0063】

図4を参照して、アプリケーション証明書(AACS Online Cert)251と、ルート証明書対応署名データ(AACS Online Sig)252の各々のデータ構成例について説明する。

【0064】

アプリケーション証明書(AACS Online Cert)251は、例えば以下のデータ構成を持つ。

データ長：アプリケーション証明書の全体データのデータ長(4バイト)、

証明書バージョン：アプリケーション証明書のバージョン情報(4バイト)、

コンテンツオーナーID：ディスク記録アプリケーションを提供したコンテンツオーナーの識別子(4B)、

コンテンツオーナー公開鍵：ディスク記録アプリケーションを提供したコンテンツオーナーの公開鍵、

署名：認証局(BDA-CA)の秘密鍵を適用して生成されたアプリケーション証明書に対する署名、

これらのデータからなる。

【0065】

なお、署名は、アプリケーション証明書251の構成データ(データ長~コンテンツオーナー公開鍵)に対して生成される署名であり、認証局(BDA-CA)の公開鍵を適用した署名検証により、アプリケーション証明書251が改竄されているか否かを確認することができる。

【0066】

一方、ルート証明書対応署名データ(AACS Online Sig)252は、図に示すように

データ長：ルート証明書対応署名データの全体データのデータ長(4バイト)、

署名バージョン：ルート証明書対応署名データのバージョン情報(4バイト)、

署名：ディスク記録アプリケーションを提供したコンテンツオーナーの秘密鍵を適用して生成されたルート証明書224と、ルート証明書対応署名データ252の構成データ(データ長, 署名バージョン)に対する署名、

【0067】

なお、署名は、ルート証明書224と、ルート証明書対応署名データ252の構成データ(データ長, 署名バージョン)に対して生成される署名であり、コンテンツオーナーの公開鍵を適用した署名検証により、ルート証明書224と、ルート証明書対応署名データ252が改竄されているか否かを確認することができる。

【0068】

アプリケーション証明書251と、ルート証明書対応署名データ252の発行構成について図5を参照して説明する。

【0069】

図5には、

(a)本発明に従った追加構成、

(b)既存構成、

これら(a), (b)の構成を示している。

(b)既存構成は、従来構成として説明した図1と、本発明の構成として説明した図2に示す構成のいずれにも共通に存在する構成である。すなわち、ディスクに記録されたディスク記録アプリケーション225と、ルート証明書224の構成である。

【0070】

ディスク記録アプリケーション225は、ディスク記録アプリケーション225を提供しているコンテンツオーナーの秘密鍵を適用した署名が設定されている。

【0071】

10

20

30

40

50

ルート証明書 224 は、図 2 を参照して説明したように、ディスク記録アプリケーション 225 を提供しているコンテンツオーナーの公開鍵に対して、コンテンツオーナーの秘密鍵で署名を設定した構成を持つ。

この構成は、従来構成として説明した図 1 と、本発明の構成として説明した図 2 に示す構成のいずれにも共通に存在する構成である。

【0072】

一方、図 5 の上段に示す (a) 本発明に従った追加構成は、従来構成として説明した図 1 には存在せず、本発明の構成として説明した図 2 に示す構成にのみ存在する追加構成である。

【0073】

まず、ルート証明書対応署名データ (AACS Online Sig) 252 は、コンテンツオーナー 210 が生成する署名データであり、ルート証明書 224 を含むデータに対して、コンテンツオーナーの秘密鍵を適用して生成される署名データである。このルート証明書対応署名データ (AACS Online Sig) 252 に設定された署名検証を実行することで、ルート証明書 224 とルート証明書対応署名データ 252 との改竄検証が可能となる。

【0074】

アプリケーション証明書 (AACS Online Cert) 251 は、認証局 (BDA-CA) 240 が発行する証明書であり、コンテンツオーナーの公開鍵に対して、認証局 (BDA-CA) 240 の秘密鍵による署名データが設定された構成である。この署名検証により、アプリケーション証明書 251 の改竄検証が可能であり、アプリケーション証明書 251 に格納されたコンテンツオーナー公開鍵は正当な鍵データであることが確認可能となる。

【0075】

改竄検証によってアプリケーション証明書 251 が改竄のない正当なデータであることが確認された場合に、アプリケーション証明書 251 に格納されたコンテンツオーナー公開鍵を取得して、取得したコンテンツオーナー公開鍵を適用して、ルート証明書対応署名データ (AACS Online Sig) 252 に設定された署名の検証を行なう。この署名検証により、ルート証明書 224 とルート証明書対応署名データ 252 とが改竄のない正当なデータであることを確認する。

【0076】

さらに、コンテンツオーナー公開鍵により、ディスク記録アプリケーション 225 に設定された署名検証も行ない、ディスク記録アプリケーション 225 の改竄検証を行う。

【0077】

このようなシーケンスとすることで、図 5 に示すように、

[認証局 240]、

[アプリケーション証明書 (AACS Online Cert) 251]、

[ルート証明書対応署名データ (AACS Online Sig) 252]

[ディスク記録アプリケーション (BD-J application) 225]

これらの構成およびデータが、一連の関係を有することになる。

【0078】

コンテンツオーナーの提供するディスク記録アプリケーション 225 を実行しようとする再生装置は、上述のデータ、すなわち、

[アプリケーション証明書 (AACS Online Cert) 251]、

[ルート証明書対応署名データ (AACS Online Sig) 252]

これらのデータに設定された署名検証を実行する。

【0079】

この署名検証によって、アプリケーション証明書 251、ルート証明書対応署名データ 252、ルート証明書 224 に改竄のないことが確認された場合には、ディスク記録アプリケーション 225 の実行を許容し、例えば、図 3 を参照して説明したシーケンスに従っ

10

20

30

40

50

たディスクに記録された識別情報 2 2 2 の取得を許容する。しかし、署名検証によって、アプリケーション証明書 2 5 1、ルート証明書対応署名データ 2 5 2、ルート証明書 2 2 4 に改竄のないことが確認されなかった場合には、ディスク記録アプリケーション 2 2 5 の実行を許可しない設定とする。

【 0 0 8 0 】

あるいは、ディスク記録アプリケーション 2 2 5 の実行機能の一部を停止させるといった処理を行なう。具体的には、識別情報 2 2 2 の取得および識別情報 2 2 2 を利用した処理を不可とする制御や、ネット接続を不可とする制御や、コンテンツのコピーを不可とする制御などを行なう。なお、識別情報 2 2 2 の取得を許容しない設定とする場合には、先に図 3 を参照して説明した A P I の使用を禁止する処理によって実現される。

10

【 0 0 8 1 】

図 6 に示すフローチャートを参照して再生装置のデータ処理部において実行する処理シーケンスについて説明する。

【 0 0 8 2 】

まず、ステップ S 1 0 1 においてアプリケーション証明書 (A A C S O n - l i n e C e r t) をディスクから読み取り、アプリケーション証明書 (A A C S O n - l i n e C e r t) に設定された署名の検証を行なう。ステップ S 1 0 2 において、アプリケーション証明書の署名検証が成功したか否か、すなわち、署名検証によりアプリケーション証明書が改竄のない正当な証明書であることが確認されたか否かを判定する。

【 0 0 8 3 】

20

先に図 4 等を参照して説明したようにアプリケーション証明書 (A A C S O n - l i n e C e r t) は、認証局 (B D A - C A) が発行する証明書であり、コンテンツオーナーの公開鍵に対して、認証局 (B D A - C A) の秘密鍵による署名データが設定された構成である。この署名検証により、アプリケーション証明書の改竄の有無についての検証が可能であり、例えば、アプリケーション証明書に格納されたコンテンツオーナー公開鍵が正当な鍵データであるか否かを確認することが可能となる。

【 0 0 8 4 】

ステップ S 1 0 2 において、アプリケーション証明書の署名検証が失敗、すなわち、アプリケーション証明書が改竄のない正当な証明書であることが確認されなかったと判定した場合は、ステップ S 1 1 2 に進む。ステップ S 1 1 2 では、ディスクに記録されたディスク記録アプリケーションの使用の禁止または制限を行なう。具体的には、例えば、

30

- (1) ディスク記録アプリケーションの利用可能な A P I を限定する。
- (2) ネットワーク接続の禁止、
- (3) ディスク記録コンテンツの再生禁止、
- (4) ディスク記録コンテンツのコピー禁止、
- (5) ディスク記録アプリケーションの利用禁止、

例えば上記 (1) ~ (5) のいずれかまたは組み合わせによるアプリケーションの利用制限処理を行なう。その後、ステップ S 1 1 3 において、許容された範囲でのアプリケーションの利用処理を行なう。

【 0 0 8 5 】

40

一方、ステップ S 1 0 2 において、アプリケーション証明書の署名検証が成功、すなわち、アプリケーション証明書が改竄のない正当な証明書であることが確認された場合は、ステップ S 1 0 3 に進む。

【 0 0 8 6 】

ステップ S 1 0 3 では、ルート証明書対応署名データ (A A C S O n - l i n e S i g) をディスクから読み取り、ステップ S 1 0 4 において、アプリケーション証明書に格納されたコンテンツオーナー公開鍵を適用して、ルート証明書対応署名データの署名検証を行う。この署名検証に適用する鍵は、ステップ S 1 0 2 において正当性の確認されたアプリケーション証明書に格納されたコンテンツオーナー公開鍵である。

【 0 0 8 7 】

50

先に図4等を参照して説明したようにルート証明書対応署名データは、コンテンツオーナーが生成する署名データであり、ディスクに記録されたルート証明書を含むデータに対して、コンテンツオーナーの秘密鍵を適用して生成される署名データである。このルート証明書対応署名データ(AACS On-line Sig)に設定された署名検証を実行することで、ルート証明書とルート証明書対応署名データとの改竄検証が可能となる。

【0088】

ステップS105において、ルート証明書対応署名データの署名検証が成功したか否か、すなわち、署名検証によりルート証明書とルート証明書対応署名データが改竄のない正当なデータであることが確認されたか否かを判定する。ステップS105において、ルート証明書とルート証明書対応署名データが改竄のない正当なデータであることが確認されなかった場合は、ステップS112に進む。ステップS112では、ディスクに記録されたディスク記録アプリケーションの使用の禁止または制限を行なう。具体的には、前述したように、例えば、

- (1) ディスク記録アプリケーションの利用可能なAPIを限定する。
- (2) ネットワーク接続の禁止、
- (3) ディスク記録コンテンツの再生禁止、
- (4) ディスク記録コンテンツのコピー禁止、
- (5) ディスク記録アプリケーションの利用禁止、

例えば上記(1)～(5)のいずれかまたは組み合わせによるアプリケーションの利用制限処理を行なう。その後、ステップS113において、許容された範囲でのアプリケーションの利用処理を行なう。

【0089】

一方、ステップS105において、ルート証明書とルート証明書対応署名データが改竄のない正当なデータであることが確認された場合は、ステップS106に進む。ステップS106では、サーバまたはディスクから証明書リボケーションリスト(CRL: Certificate Revocation List)を取得して取得した証明書リボケーションリスト(CRL)の署名検証処理を行なう。

【0090】

証明書リボケーションリスト(CRL)は、発行済みの証明書中、既に無効化された証明書についての情報を格納したリストである。例えばアプリケーション証明書などの公開鍵を格納した公開鍵証明書に格納された公開鍵が無効なものであることを示すリストであり、無効化された証明書の証明書識別子や証明書の発行先の識別情報などを登録したリストである。この証明書リボケーションリスト(CRL)は、逐次、更新され、最新のリストが証明書発行主体の管理サーバから取得可能であり、またディスクに記録されてユーザに提供される。なお、証明書リボケーションリスト(CRL)にはバージョン情報が設定され、新旧の判別が可能な構成となっている。

【0091】

証明書リボケーションリスト(CRL)には、証明書発行主体の秘密鍵による署名が設定されており、証明書発行主体の公開鍵による署名検証により改竄検証が可能なデータ構成となっている。ステップS106では、証明書リボケーションリスト(CRL)の署名検証を行なう。ステップS107において、証明書リボケーションリスト(CRL)の署名に失敗した場合は、不正なCRLである可能性があり、ステップS106に戻り、新たな証明書リボケーションリスト(CRL)をサーバから取得して、取得した証明書リボケーションリスト(CRL)について署名検証を行なう。

【0092】

ステップS107において、証明書リボケーションリスト(CRL)の署名に成功し、証明書リボケーションリスト(CRL)の正当性が確認された場合、ステップS108に進む。

【0093】

ステップS108では、再生装置のメモリに格納されている証明書リボケーションリス

10

20

30

40

50

ト(CRL)のバージョンと、サーバまたはディスクから取得した署名検証を実行した証明書リボケーションリスト(CRL)のバージョンを比較し、サーバまたはディスクから取得した署名検証を実行した証明書リボケーションリスト(CRL)が、再生装置に格納されている証明書リボケーションリスト(CRL)より新しいと判断された場合は、ステップS109において、サーバまたはディスクから取得し署名検証を実行した証明書リボケーションリスト(CRL)を再生装置のメモリに格納する。

【0094】

ステップS110では、アプリケーション証明書からコンテンツオーナーID読み取り、署名検証を実行した証明書リボケーションリスト(CRL)の記録データと照合する。

【0095】

ステップS111において、アプリケーション証明書に記録されたコンテンツオーナーIDがCRLリストに記録されていないと判断された場合は、ステップS113に進み、許容された範囲でのアプリケーションの利用処理を行なう。この場合、基本的に制限のないアプリケーション利用処理が可能となる。すなわち、先に図3を参照して説明した識別情報の取得および利用処理などが制限無く実行することが可能となる。

【0096】

一方、ステップS111において、アプリケーション証明書に記録されたコンテンツオーナーIDがCRLリストに記録されていると判断された場合は、ステップS112に進み、ディスクに記録されたディスク記録アプリケーションの使用の禁止または制限を行なう。具体的には、前述したように、例えば、

- (1) ディスク記録アプリケーションの利用可能なAPIを限定する。
- (2) ネットワーク接続の禁止、
- (3) ディスク記録コンテンツの再生禁止、
- (4) ディスク記録コンテンツのコピー禁止、
- (5) ディスク記録アプリケーションの利用禁止、

例えば上記(1)~(5)のいずれかまたは組み合わせによるアプリケーションの利用制限処理を行なう。その後、ステップS113において、許容された範囲でのアプリケーションの利用処理を行なう。

【0097】

なお、アプリケーションの利用に際しては、先に図2を参照して説明したように、ディスク記録アプリケーション225には、コンテンツオーナーの署名が設定されており、コンテンツオーナーの公開鍵を適用した署名検証を行なって署名検証に成功、すなわち、ディスク記録アプリケーション225が改竄のない正当なアプリケーションデータであることを確認し、この確認がなされたことを条件としてアプリケーション利用を行なう。

【0098】

このように、本発明の構成では、先に図5を参照して説明したように、

[認証局240]、

[アプリケーション証明書(AACS On-line Cert)251]、

[ルート証明書対応署名データ(AACS On-line Sig)252]

[ディスク記録アプリケーション(BD-J application)225]

これらの構成およびデータを関連付け、コンテンツオーナーの提供するディスク記録アプリケーションを、第三者、すなわち認証局の管理下に設定することを可能とし、ディスク記録アプリケーションを利用しようとする再生装置に、図6に示すフローに従った処理を実行させて、ディスク記録アプリケーション225の厳格な正当性確認を可能とし、アプリケーション証明書(AACS On-line Cert)や、ルート証明書対応署名データ(AACS On-line Sig)の署名検証に失敗した場合は、ディスク記録アプリケーション225の実行機能の少なくとも一部を停止させるアプリケーション実行機能の制限処理を行なう構成とした。

【0099】

具体的には、メディアID(PMSN)などのディスクに記録された識別情報の取得や

10

20

30

40

50

利用処理を不可とする制御や、ネット接続を不可とする制御、コンテンツのコピーを不可とする制御などを行なう。

【0100】

先に、図3を参照して説明したように、ディスク220に記録された識別情報222の読み取りなどの処理を行なうのは、ディスク記録アプリケーション自体ではなく、図3に示すAACSLレイヤ(ID情報取得プログラム実行部)302である。先に説明したようにAACSLレイヤはAACSL規定に従ったシーケンスに従ってデータ処理を実行する。

【0101】

アプリケーションは、このAACSLレイヤに対して様々な処理の依頼が可能であり、様々な処理に対応して設定されたAPIの呼び出しを実行する。AACSLレイヤはAPI呼び出しに応じたデータ処理、例えば前述した識別情報の読み取り処理などを実行し、処理結果をアプリケーション実行部に提供する。

10

【0102】

図6を参照して説明したように、本発明の再生装置では、ディスクに記録されたデータであるアプリケーション証明書(AACSON-line Cert)や、ルート証明書対応署名データ(AACSON-line Sig)などの署名検証に失敗した場合、アプリケーションの処理を制限する構成としている。アプリケーションの処理を制御する構成例について図7を参照して説明する。図7には、ディスク220と、再生装置300を示している。

【0103】

20

再生装置300は、アプリケーション実行部301、AACSLレイヤ302、さらに、データ検証部351、アプリケーション制御部352を有する。アプリケーション実行部301と、AACSLレイヤ302は図3を参照して説明したアプリケーション実行部301と、AACSLレイヤ302に対応する。

【0104】

データ検証部351は、図6に示すフローにおけるステップS101~S110の処理を実行する。すなわち、ディスクに記録されたデータであるアプリケーション証明書(AACSON-line Cert)251や、ルート証明書対応署名データ(AACSON-line Sig)252などの署名検証、CRLの記録データの検証処理などを実行し、その検証結果をアプリケーション制御部352に通知する。

30

【0105】

アプリケーション制御部352は、データ検証部351におけるデータ検証の結果に応じて、アプリケーションの制御を行なう。すなわち、具体的には、前述したように、例えば、

- (1) ディスク記録アプリケーションの利用可能なAPIを限定する。
- (2) ネットワーク接続の禁止、
- (3) ディスク記録コンテンツの再生禁止、
- (4) ディスク記録コンテンツのコピー禁止、
- (5) ディスク記録アプリケーションの利用禁止、

例えば上記(1)~(5)のいずれかまたは組み合わせによるアプリケーションの利用制限処理を行なう。

40

【0106】

アプリケーション実行部301は、ディスク220に記録されたディスク記録アプリケーション(BD-J application)225を読み出して実行する。アプリケーションは、AACSLレイヤ302に対して様々な処理を実行させる関数からなるAPIの呼び出しを行なう。しかし、このAPI処理に対して、アプリケーション制御部352は、データ検証部351におけるデータ検証の結果に応じて、制御を行い、API呼び出しをAACSLレイヤ302に入力する処理を禁止する。

【0107】

このアプリケーション制御部352によるAPI制御により、アプリケーションの様々

50

な処理の実行が禁止される。具体的には前述の(1)~(5)のいずれかの処理または複数の処理が禁止される。なお、アプリケーションにおける禁止処理や許容処理は様々な設定が可能である。

【0108】

アプリケーション実行部301は、処理に応じたAPI呼び出しをAACSLレイヤ302に対して実行する。具体的には、

メディアID(PMSN)226の読み出し処理をAACSLレイヤに対して実行させるAPI、

ボリュームID227の読み出し処理をAACSLレイヤに対して実行させるAPI、

コンテンツ証明書ID228の読み出し処理をAACSLレイヤに対して実行させるAPI、

さらに、

ディスク記録コンテンツの再生、コピー、外部出力処理のための許容情報の提供をAACSLレイヤに対して実行させるAPI、

ネット接続や、ディスク記録コンテンツと再生装置の記憶部(ハードディスクやフラッシュメモリなど)に格納されたコンテンツとのバインド処理による再生などの様々な処理、あるいは処理許可情報の出力をAACSLレイヤに対して実行させるAPI、

このような各種の処理に応じて設定されるAPIを利用した処理依頼をAACSLレイヤ302に対して実行するが、アプリケーション制御部352によるAPI制御により、アプリケーションの様々な処理の実行を選択的に禁止することが可能となる。

【0109】

なお、前述したように、ディスクに記録された識別子ではなく、再生装置のメモリに記録された再生装置対応の識別情報であるデバイスバイディングIDが利用される場合もあり、この場合もディスクに記録された識別子の利用と同様の処理態様として実行可能である。デバイスバイディングIDは、再生装置固有の識別情報として再生装置内のメモリに記録され、ディスク格納コンテンツの利用、後発データのサーバからの取得、再生装置のハードディスクなどの記憶部に格納された後発データの利用などに際して、例えば再生装置の確認処理としてのID確認や、鍵生成、コンテンツ復号などの処理に利用される。

【0110】

このように、本発明の構成によれば、

ディスクに記録されるアプリケーションを提供するコンテンツオーナーの公開鍵を格納し、認証局の署名を設定したアプリケーション証明書(AACSON-lineCert)と、

ルート証明書を含むデータに対してコンテンツオーナーの署名を設定したルート証明書対応署名データ(AACSON-lineSig)、

これらのデータをディスクに記録する構成とし、

アプリケーションを実行しようとする再生装置に、図6に示すフローに従ってアプリケーション証明書(AACSON-lineCert)の署名検証を行い、アプリケーション証明書(AACSON-lineCert)の正当性を確認させ、正当性の確認されたアプリケーション証明書からコンテンツオーナー公開鍵を取得して、取得したコンテンツオーナー公開鍵を適用して、ルート証明書対応署名データ(AACSON-lineSig)の署名検証を行い、ルート証明書の正当性確認を行なわせる構成とし、これらの署名検証に失敗した場合は、アプリケーションの利用の禁止または制限を行なう構成とした。

【0111】

この構成によりコンテンツオーナーの提供するアプリケーションが、第三者機関としての認証局の管理下に置かれることになり、不正なアプリケーションの蔓延、不正アプリケーションの使用による識別情報の不正取得や利用、あるいはコンテンツの不正利用を防止することが可能となる。

【 0 1 1 2 】

[証明書リボケーションリスト (C R L) のタイムスタンプを適用した処理例]

次に、ディスクに記録されるアプリケーション証明書 (A A C S O n - l i n e C e r t) の無効化情報を格納した証明書リボケーションリスト (C R L) に、アプリケーション証明書 (A A C S O n - l i n e C e r t) の失効日時、すなわち、ディスクに記録されるアプリケーションの提供主体であるコンテンツオーナーの無効化日時に対応する日時情報を記録し、さらに、図 2 に示すライセンス管理部 (A A C S - L A) 2 3 0 の発行するコンテンツ証明書 (C o n t e n t C e r t i f i c a t e) にもライセンス管理部 (A A C S - L A) が署名を生成した日時情報を示すタイムスタンプを設定する構成とした例について説明する。

10

【 0 1 1 3 】

ディスク記録アプリケーションを実行しようとする再生装置は、

(a) コンテンツ証明書のタイムスタンプ、

(b) 証明書リボケーションリスト (C R L) のタイムスタンプ、

これらの 2 つのタイムスタンプの比較を実行し、

コンテンツ証明書のタイムスタンプが、証明書リボケーションリスト (C R L) のタイムスタンプ以降の日時データである場合に、ディスク記録アプリケーションの使用の禁止または制限を行なう。

【 0 1 1 4 】

コンテンツ証明書のタイムスタンプが、証明書リボケーションリスト (C R L) のタイムスタンプより前の日時データである場合には、ディスク記録アプリケーションの使用の禁止または制限を行なわない。ただし、前述の署名検証、すなわち、アプリケーション証明書 (A A C S O n - l i n e C e r t) と、ルート証明書対応署名データ (A A C S O n - l i n e S i g) の署名検証に失敗した場合は、ディスク記録アプリケーションの使用の禁止または制限を行なう。

20

【 0 1 1 5 】

本実施例において利用される証明書リボケーションリスト (C R L) 、コンテンツ証明書のデータ構成および再生装置における処理の概要について図 8 を参照して説明する。

【 0 1 1 6 】

図 8 にはディスク 4 0 0 、再生装置 3 0 0 を示している。ディスク 4 0 0 には、コンテンツ証明書 (C o n t e n t C e r t i f i c a t e) 4 0 1 と、アプリケーション証明書 (A A C S O n - l i n e C e r t) 4 0 2 のみを示しているが、その他、図 2 を参照して説明したと同様のコンテンツや識別情報 (I D) などのデータが記録されている。

30

【 0 1 1 7 】

コンテンツ証明書 (C o n t e n t C e r t i f i c a t e) 4 0 1 は、先に図 2 を参照して説明したように、ディスクに記録されるコンテンツが正当なコンテンツ、すなわちライセンス管理部 (A A C S L A) によって管理された正当コンテンツであることを証明するためのデータである。コンテンツ証明書 4 0 1 はディスク 4 0 0 に記録されるコンテンツに対応してその正当性を証明するデータとしてライセンス管理部の管理下で発行されディスク 4 0 0 に記録される。

40

【 0 1 1 8 】

先に図 2 を参照して説明した例では、コンテンツ証明書 (C o n t e n t C e r t i f i c a t e) は、ルート証明書の構成データによって生成されたハッシュ値であるルート証明書ハッシュを記録し、記録ハッシュ値に対してライセンス管理部 (A A C S L A) の秘密鍵による電子署名が付与された構成であったが、本実施例において利用するコンテンツ証明書 4 0 1 は、図 8 に示すように、さらにタイムスタンプを記録データとした構成を持つ。

【 0 1 1 9 】

このタイムスタンプは、ライセンス管理部 (A A C S - L A) がコンテンツ証明書 (C

50

Content Certificate) 401に対する署名を生成した日時情報を示す。すなわち、コンテンツ証明書(Content Certificate) 401の発行日時に相当する。署名は、コンテンツ証明書に含まれるルート証明書ハッシュとタイムスタンプを含むデータに対して実行される。従って、タイムスタンプの改竄を行えば署名検証に失敗し、改竄がなされたことが発覚することになる。

【0120】

一方、アプリケーション証明書(AACS On-line Cert) 402は、図8には省略して示してあるが、先に、図4を参照して説明したと同様の構成であり、以下のデータ構成を持つ。

データ長：アプリケーション証明書の全体データのデータ長(4バイト)、
証明書バージョン：アプリケーション証明書のバージョン情報(4バイト)、
コンテンツオーナーID：ディスク記録アプリケーションを提供したコンテンツオーナーの識別子(4B)、
コンテンツオーナー公開鍵：ディスク記録アプリケーションを提供したコンテンツオーナーの公開鍵、
署名：認証局(BDA-CA)の秘密鍵を適用して生成されたアプリケーション証明書に対する署名、
これらのデータを記録した証明書である。

【0121】

再生装置300は、ディスク記録アプリケーションを実行する前に、先に図6のフローを参照して説明したように、サーバまたはディスクから証明書リポケーションリスト(CRL) 391を取得して、証明書リポケーションリスト(CRL)に、アプリケーション証明書に記録されたコンテンツオーナーIDが含まれるか否かを検証して、含まれている場合は、ディスク記録アプリケーションの使用の禁止または制限を行なう。

【0122】

本実施例では、ディスクに記録されるアプリケーション証明書(AACS On-line Cert) 402の無効化情報を格納した証明書リポケーションリスト(CRL) 391に、アプリケーション証明書(AACS On-line Cert) 402の失効日時であり、アプリケーション証明書に記録されたコンテンツオーナーの無効化日時を示すタイムスタンプを設定した構成としている。すなわち証明書リポケーションリスト(CRL) 391は、ディスクに記録されるアプリケーションの提供主体であるコンテンツオーナーの無効化日時に対応する日時情報を示すタイムスタンプを設定した構成としている。

【0123】

なお、証明書リポケーションリスト(CRL) 391は、逐次更新されるデータであり、先に図6のフローを参照して説明したように、再生装置は、ディスクまたはサーバからより新しい、証明書リポケーションリスト(CRL) 391を取得して、取得した証明書リポケーションリスト(CRL) 391を再生装置300のメモリ(NVRAM) 371に格納して利用する。

【0124】

再生装置300のデータ検証部351は、図8に示すステップS201において、
(a) コンテンツ証明書のタイムスタンプ、
(b) 証明書リポケーションリスト(CRL)のタイムスタンプ、
これらの2つのタイムスタンプの比較を実行する。
このタイムスタンプ比較処理において、
コンテンツ証明書のタイムスタンプが、証明書リポケーションリスト(CRL)のタイムスタンプ以降の日時データである場合には、再生装置のアプリケーション制御部が、ディスク記録アプリケーションの使用の禁止または制限を行なう。

【0125】

コンテンツ証明書のタイムスタンプが、証明書リポケーションリスト(CRL)のタイ

10

20

30

40

50

ムスタンプより前の日時データである場合には、ディスク記録アプリケーションの使用の禁止または制限を行なわない。ただし、前述の署名検証、すなわち、アプリケーション証明書(AACS On-line Cert)や、ルート証明書対応署名データ(AACS On-line Sig)の署名検証に失敗した場合は、ディスク記録アプリケーションの使用の禁止または制限を行なう。

【0126】

本実施例では、逐次更新される証明書リポケーションリスト(CRL)のタイムスタンプによって、コンテンツオーナーの無効化、すなわちコンテンツオーナーの提供するディスク記録アプリケーションの無効化日時を確認し、この無効化日時以降のタイムスタンプを持つコンテンツ証明書が記録されたディスクのアプリケーションについては利用の禁止または制限を行ない、無効化日時以前のタイムスタンプを持つコンテンツ証明書が記録されたディスクのアプリケーションについては、アプリケーション証明書や、ルート証明書対応署名データの署名検証に成功した場合は、使用の禁止や制限を行なわない設定とした処理例である。

10

【0127】

本実施例に対応する再生装置の処理シーケンスについて図9に示すフローチャートを参照して説明する。図9に示すフローチャートにおいて、ステップS101～S113の処理は、図6を参照して説明した処理と同様のステップであり、本実施例では、ステップS301、ステップS302の処理が新たに追加される。

【0128】

以下、各ステップの処理について説明する。なお、ステップS101～S113の処理については図6を参照して説明した処理と同様のステップであり、簡略化して説明する。

20

【0129】

ステップS101においてアプリケーション証明書(AACS On-line Cert)をディスクから読み取り、アプリケーション証明書(AACS On-line Cert)に設定された署名の検証を行なう。

ステップS102において、アプリケーション証明書の署名検証が成功したか否か、すなわち、署名検証によりアプリケーション証明書が改竄のない正当な証明書であることが確認されたか否かを判定する。

【0130】

ステップS102において、アプリケーション証明書の署名検証が失敗、すなわち、アプリケーション証明書が改竄のない正当な証明書であることが確認されなかったと判定した場合は、ステップS112に進む。ステップS112では、ディスクに記録されたディスク記録アプリケーションの使用の禁止または制限を行なう。具体的には、例えば、

- (1) ディスク記録アプリケーションの利用可能なAPIを限定する。
- (2) ネットワーク接続の禁止、
- (3) ディスク記録コンテンツの再生禁止、
- (4) ディスク記録コンテンツのコピー禁止、
- (5) ディスク記録アプリケーションの利用禁止、

例えば上記(1)～(5)のいずれかまたは組み合わせによるアプリケーションの利用制限処理を行なう。その後、ステップS113において、許容された範囲でのアプリケーションの利用処理を行なう。

30

40

【0131】

一方、ステップS102において、アプリケーション証明書の署名検証が成功、すなわち、アプリケーション証明書が改竄のない正当な証明書であることが確認された場合は、ステップS103に進む。

【0132】

ステップS103では、ルート証明書対応署名データ(AACS On-line Sig)をディスクから読み取り、ステップS104において、アプリケーション証明書に格納されたコンテンツオーナー公開鍵を適用して、ルート証明書対応署名データの署名検

50

証を行う。この署名検証に適用する鍵は、ステップS 1 0 2において正当性の確認されたアプリケーション証明書に格納されたコンテンツオーナー公開鍵である。

【 0 1 3 3 】

ステップS 1 0 5において、ルート証明書対応署名データの署名検証が成功せず、ルート証明書とルート証明書対応署名データが改竄のない正当なデータであることが確認されなかった場合は、ステップS 1 1 2に進む。ステップS 1 1 2では、ディスクに記録されたディスク記録アプリケーションの使用の禁止または制限を行なう。具体的には、前述したように、例えば、

- (1) ディスク記録アプリケーションの利用可能なAPIを限定する。
- (2) ネットワーク接続の禁止、
- (3) ディスク記録コンテンツの再生禁止、
- (4) ディスク記録コンテンツのコピー禁止、
- (5) ディスク記録アプリケーションの利用禁止、

例えば上記(1) ~ (5)のいずれかまたは組み合わせによるアプリケーションの利用制限処理を行なう。その後、ステップS 1 1 3において、許容された範囲でのアプリケーションの利用処理を行なう。

【 0 1 3 4 】

一方、ステップS 1 0 5において、ルート証明書とルート証明書対応署名データが改竄のない正当なデータであることが確認された場合は、ステップS 1 0 6に進む。ステップS 1 0 6では、サーバまたはディスクから証明書リボケーションリスト(CRL: Certificate Revocation List)を取得して取得した証明書リボケーションリスト(CRL)の署名検証処理を行なう。

【 0 1 3 5 】

証明書リボケーションリスト(CRL)は、発行済みの証明書中、既に無効化された証明書についての情報を格納したリストであり、本実施例では、ディスク記録アプリケーションを提供している無効化されたコンテンツオーナーIDと、コンテンツオーナーの無効化日時、すなわちコンテンツオーナーの提供するディスク記録アプリケーションの無効化日時を示すタイムスタンプが記録された構成を持つ。なお証明書リボケーションリスト(CRL)にはバージョン情報が設定され、新旧の判別が可能な構成となっている。

【 0 1 3 6 】

証明書リボケーションリスト(CRL)には、証明書発行主体の秘密鍵による署名が設定されており、証明書発行主体の公開鍵による署名検証により改竄検証が可能なデータ構成となっている。ステップS 1 0 6では、証明書リボケーションリスト(CRL)の署名検証を行なう。ステップS 1 0 7において、証明書リボケーションリスト(CRL)の署名に失敗した場合は、不正なCRLである可能性があり、ステップS 1 0 6に戻り、新たな証明書リボケーションリスト(CRL)をサーバから取得して、取得した証明書リボケーションリスト(CRL)について署名検証を行なう。

【 0 1 3 7 】

ステップS 1 0 7において、証明書リボケーションリスト(CRL)の署名に成功し、証明書リボケーションリスト(CRL)の正当性が確認された場合、ステップS 1 0 8に進む。

【 0 1 3 8 】

ステップS 1 0 8では、再生装置のメモリに格納されている証明書リボケーションリスト(CRL)のバージョンと、サーバまたはディスクから取得した署名検証を実行した証明書リボケーションリスト(CRL)のバージョンを比較し、サーバまたはディスクから取得した署名検証を実行した証明書リボケーションリスト(CRL)が、再生装置に格納されている証明書リボケーションリスト(CRL)より新しいと判断された場合は、ステップS 1 0 9において、サーバまたはディスクから取得し署名検証を実行した証明書リボケーションリスト(CRL)を再生装置のメモリに格納する。

【 0 1 3 9 】

10

20

30

40

50

ステップS 1 1 0では、アプリケーション証明書からコンテンツオーナーID読み取り、署名検証を実行した証明書リボケーションリスト(CRL)の記録データと照合する。

【0140】

ステップS 1 1 1において、アプリケーション証明書に記録されたコンテンツオーナーIDがCRLリストに記録されていないと判断された場合は、ステップS 1 1 3に進み、許容された範囲でのアプリケーションの利用処理を行なう。この場合、基本的に制限のないアプリケーション利用処理が可能となる。すなわち、先に図3を参照して説明した識別情報の取得および利用処理などが制限無く実行することが可能となる。

【0141】

一方、ステップS 1 1 1において、アプリケーション証明書に記録されたコンテンツオーナーIDがCRLリストに記録されていると判断された場合は、ステップS 3 0 1に進む。

【0142】

ステップS 3 0 1では、先に図8を参照して説明したタイムスタンプ比較処理を実行する。すなわち、

- (a) コンテンツ証明書のタイムスタンプ、
 - (b) 証明書リボケーションリスト(CRL)のタイムスタンプ、
- これらの2つのタイムスタンプの比較を実行する。

【0143】

ステップS 3 0 2で、コンテンツ証明書のタイムスタンプが、証明書リボケーションリスト(CRL)のタイムスタンプ以降の日時データであることが確認された場合は、ディスクまたはディスクに記録されたアプリケーションは、コンテンツオーナーが無効化された後に製造されたディスクまたは記録されたアプリケーションであると判断し、ステップS 1 1 2に進み、ディスクに記録されたディスク記録アプリケーションの使用の禁止または制限を行なう。具体的には、前述したように、例えば、

- (1) ディスク記録アプリケーションの利用可能なAPIを限定する。
- (2) ネットワーク接続の禁止、
- (3) ディスク記録コンテンツの再生禁止、
- (4) ディスク記録コンテンツのコピー禁止、
- (5) ディスク記録アプリケーションの利用禁止、

例えば上記(1)～(5)のいずれかまたは組み合わせによるアプリケーションの利用制限処理を行なう。その後、ステップS 1 1 3において、許容された範囲でのアプリケーションの利用処理を行なう。

【0144】

一方、ステップS 3 0 2において、コンテンツ証明書のタイムスタンプが、証明書リボケーションリスト(CRL)のタイムスタンプより前の日時データであることが確認された場合は、ディスクまたはディスクに記録されたアプリケーションは、コンテンツオーナーが無効化される前に製造されたディスクまたはディスクに記録されたアプリケーションであると判断し、ディスク記録アプリケーションの使用の禁止または制限を行なうことなくステップS 1 1 3に進み、アプリケーション利用を可能とする。

【0145】

なお、先に図2を参照して説明したように、ディスク記録アプリケーション225には、コンテンツオーナーの署名が設定されており、コンテンツオーナーの公開鍵を適用した署名検証を行なって署名検証に成功、すなわち、ディスク記録アプリケーション225が改竄のない正当なアプリケーションデータであることを確認し、この確認がなされたことを条件としてアプリケーション利用を行なう。

【0146】

このように、本実施例の構成では、再生装置300のデータ検証部において、

- (a) コンテンツ証明書のタイムスタンプ、
- (b) 証明書リボケーションリスト(CRL)のタイムスタンプ、

10

20

30

40

50

これらの2つのタイムスタンプの比較を実行し、コンテンツ証明書のタイムスタンプが、証明書リボケーションリスト(CRL)のタイムスタンプ以降の日時データである場合には、再生装置のアプリケーション制御部が、ディスク記録アプリケーションの使用の禁止または制限を行ない、コンテンツ証明書のタイムスタンプが、証明書リボケーションリスト(CRL)のタイムスタンプより前の日時データである場合には、前述の署名検証、すなわち、アプリケーション証明書(AACS Online Cert)や、ルート証明書対応署名データ(AACS Online Sig)の署名検証に成功している場合はディスク記録アプリケーションの使用の禁止または制限を行なわない構成とした。

【0147】

この構成により、コンテンツオーナーが無効化される前のアプリケーションについてまで利用制限が行なわれてしまう弊害を排除することが可能となる。

10

【0148】

以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、特許請求の範囲の欄を参酌すべきである。

【0149】

また、明細書中において説明した一連の処理はハードウェア、またはソフトウェア、あるいは両者の複合構成によって実行することが可能である。ソフトウェアによる処理を実行する場合は、処理シーケンスを記録したプログラムを、専用のハードウェアに組み込まれたコンピュータ内のメモリにインストールして実行させるか、あるいは、各種処理が実行可能な汎用コンピュータにプログラムをインストールして実行させることが可能である。例えば、プログラムは記録媒体に予め記録しておくことができる。記録媒体からコンピュータにインストールする他、LAN(Local Area Network)、インターネットといったネットワークを介してプログラムを受信し、内蔵するハードディスク等の記録媒体にインストールすることができる。

20

【0150】

なお、明細書に記載された各種の処理は、記載に従って時系列に実行されるのみならず、処理を実行する装置の処理能力あるいは必要に応じて並列的あるいは個別に実行されてもよい。また、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

30

【産業上の利用可能性】

【0151】

以上、説明したように、本発明の一実施例によれば、ディスクに記録されたアプリケーションプログラムの提供主体であるコンテンツオーナーの無効化情報を記録した証明書リボケーションリスト(CRL)を参照して、アプリケーション証明書に記録されたコンテンツオーナー識別子が、証明書リボケーションリスト(CRL)に含まれるか否かを検証し、含まれている場合に、コンテンツ証明書に格納されたタイムスタンプと、証明書リボケーションリスト(CRL)のタイムスタンプの比較を実行して、コンテンツ証明書タイムスタンプが、CRLタイムスタンプ以降の日時データを有する場合、アプリケーション実行部におけるアプリケーションプログラムの利用処理を禁止または制限する構成とした。本構成により、無効化される前のアプリケーションは利用制限を行わず、無効化された後のアプリケーションに対してのみ利用制限を行なう構成が実現される。

40

【図面の簡単な説明】

【0152】

【図1】現状のAACS規定におけるコンテンツ利用制御構成の概要について説明する図である。

【図2】本発明の一実施例に係るアプリケーション利用制御を実現するための構成について説明する図である。

【図3】ディスクに記録された識別情報(ID)の読み取り処理例について説明する図で

50

ある。

【図4】アプリケーション証明書(AACS On-line Cert)と、ルート証明書対応署名データ(AACS On-line Sig)各々のデータ構成例について説明する図である。

【図5】アプリケーション証明書と、ルート証明書対応署名データの発行構成について説明する図である。

【図6】再生装置のデータ処理部において実行する処理シーケンスについて説明するフローチャートを示す図である。

【図7】アプリケーションの処理を制御する構成例について説明する図である。

【図8】タイムスタンプを持つコンテンツ証明書と証明書リボケーションリスト(CRL)を利用した処理例について説明する図である。 10

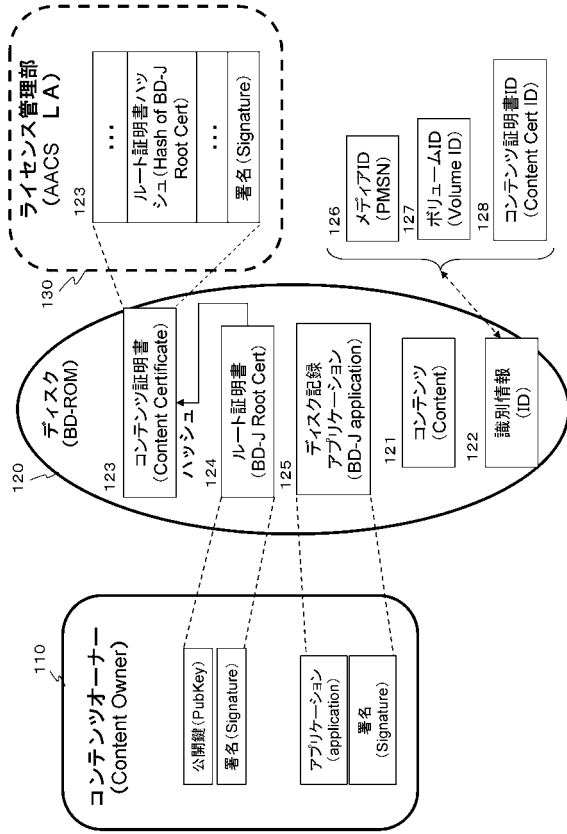
【図9】再生装置のデータ処理部において実行する処理シーケンスについて説明するフローチャートを示す図である。

【符号の説明】

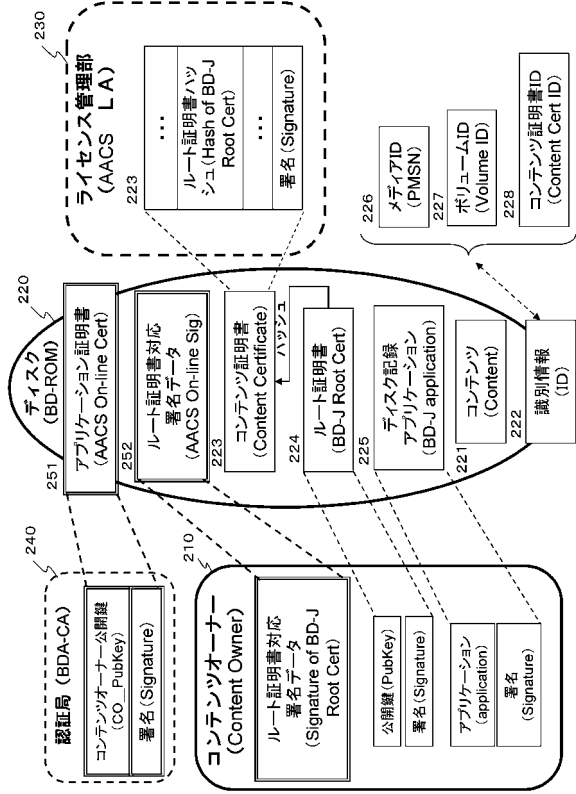
【0153】

110	コンテンツオーナー	
120	ディスク	
121	コンテンツ	
122	識別情報(ID)	
123	コンテンツ証明書	20
124	ルート証明書	
125	ディスク記録アプリケーション	
126	メディアID(PMSN)	
127	ボリュームID	
128	コンテンツ証明書ID	
130	ライセンス管理部	
210	コンテンツオーナー	
220	ディスク	
221	コンテンツ	
222	識別情報(ID)	30
223	コンテンツ証明書(Content Cert)	
224	ルート証明書(BD-J Root Cert)	
225	ディスク記録アプリケーション(BD-J application)	
226	メディアID(PMSN)	
227	ボリュームID	
228	コンテンツ証明書ID	
230	ライセンス管理部	
240	認証局(BDA-CA)	
251	アプリケーション証明書(AACS On-line Cert)	
252	ルート証明書対応署名データ(AACS On-line Sig)	40
300	再生装置	
301	アプリケーション実行部(BD-J VM)	
302	AACSレイヤ	
351	データ検証部	
352	アプリケーション制御部	
371	メモリ	
391	証明書リボケーションリスト(CRL)	
400	ディスク	
401	コンテンツ証明書(Content Cert)	
402	アプリケーション証明書(AACS On-line Cert)	50

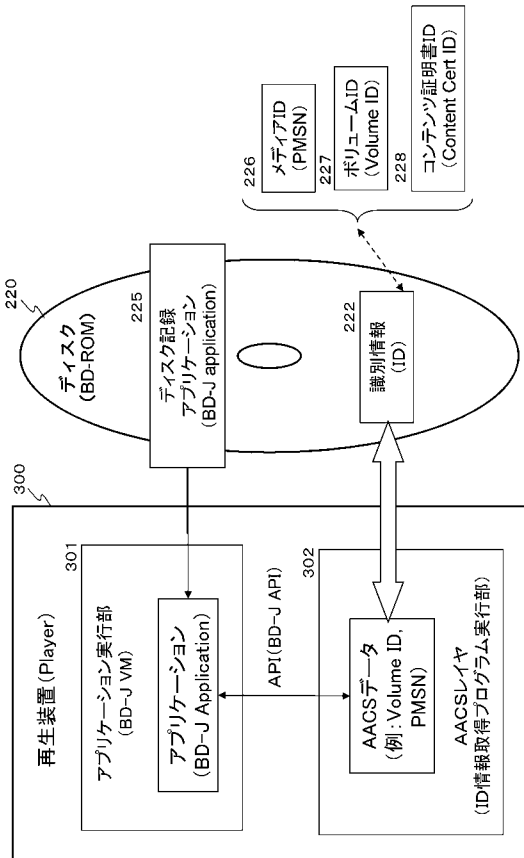
【図 1】



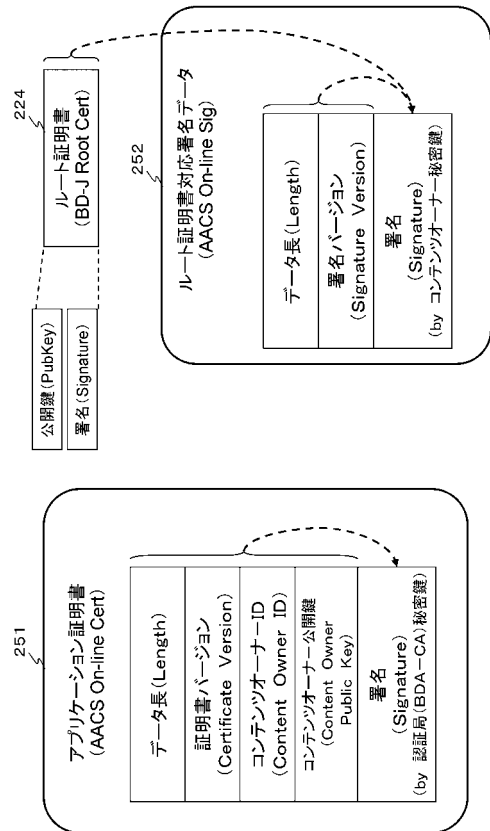
【図 2】



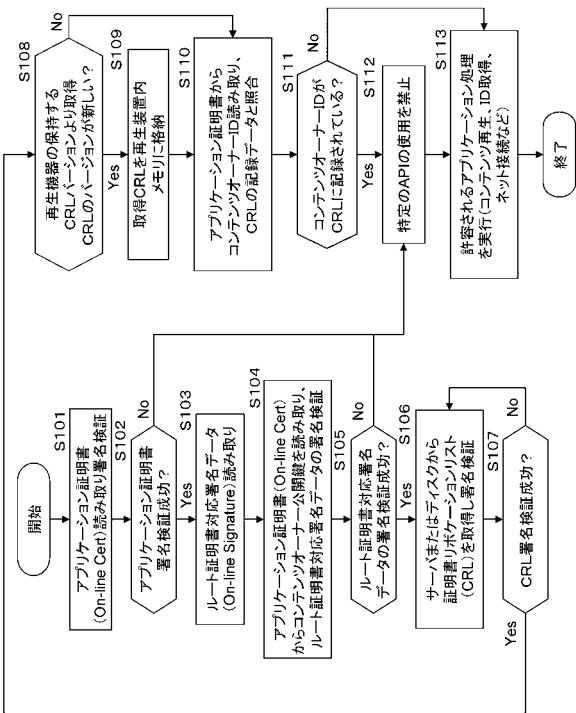
【図 3】



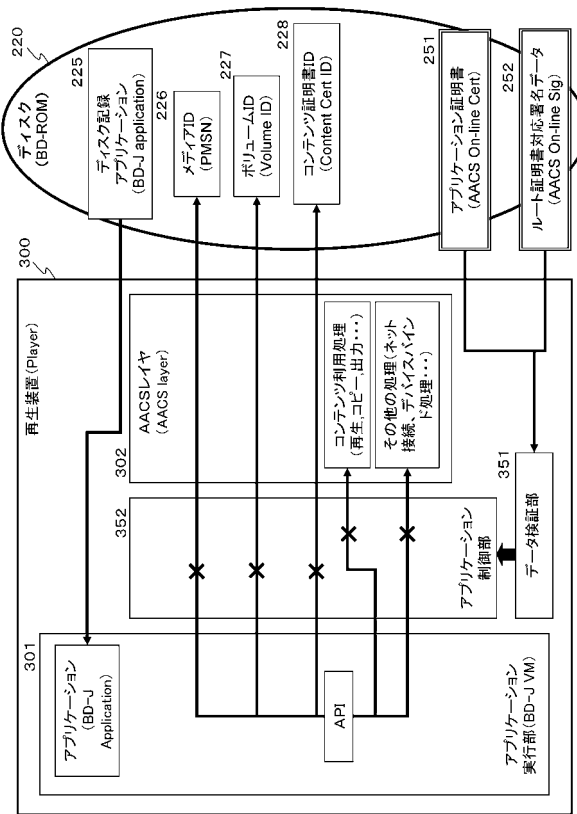
【図 4】



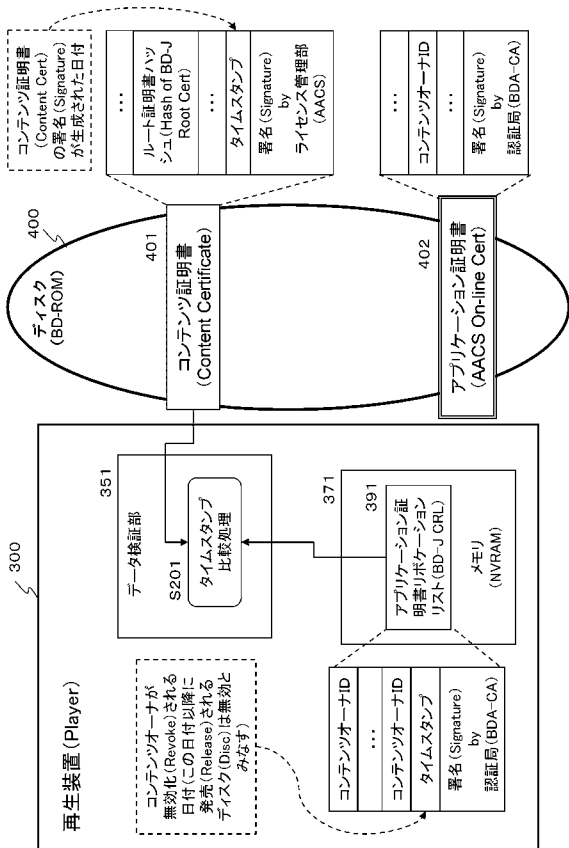
【図6】



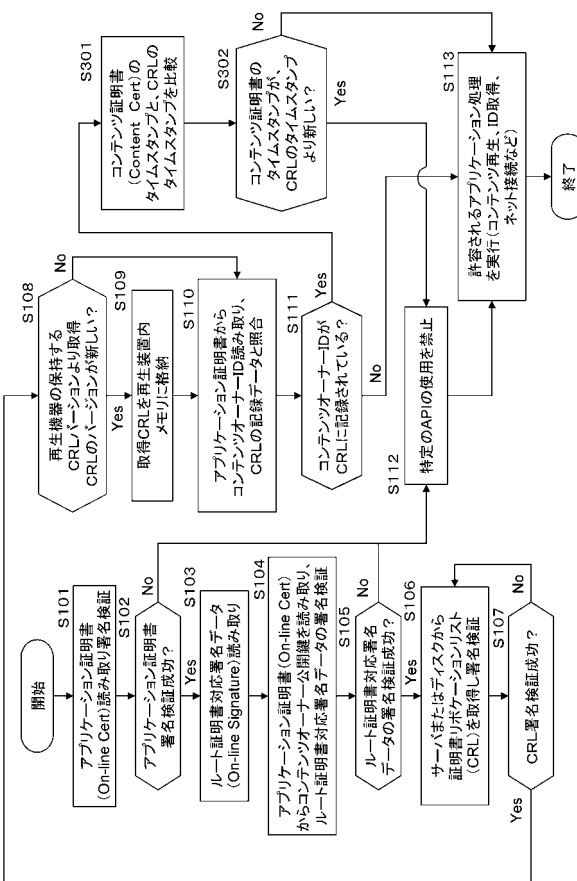
【図7】



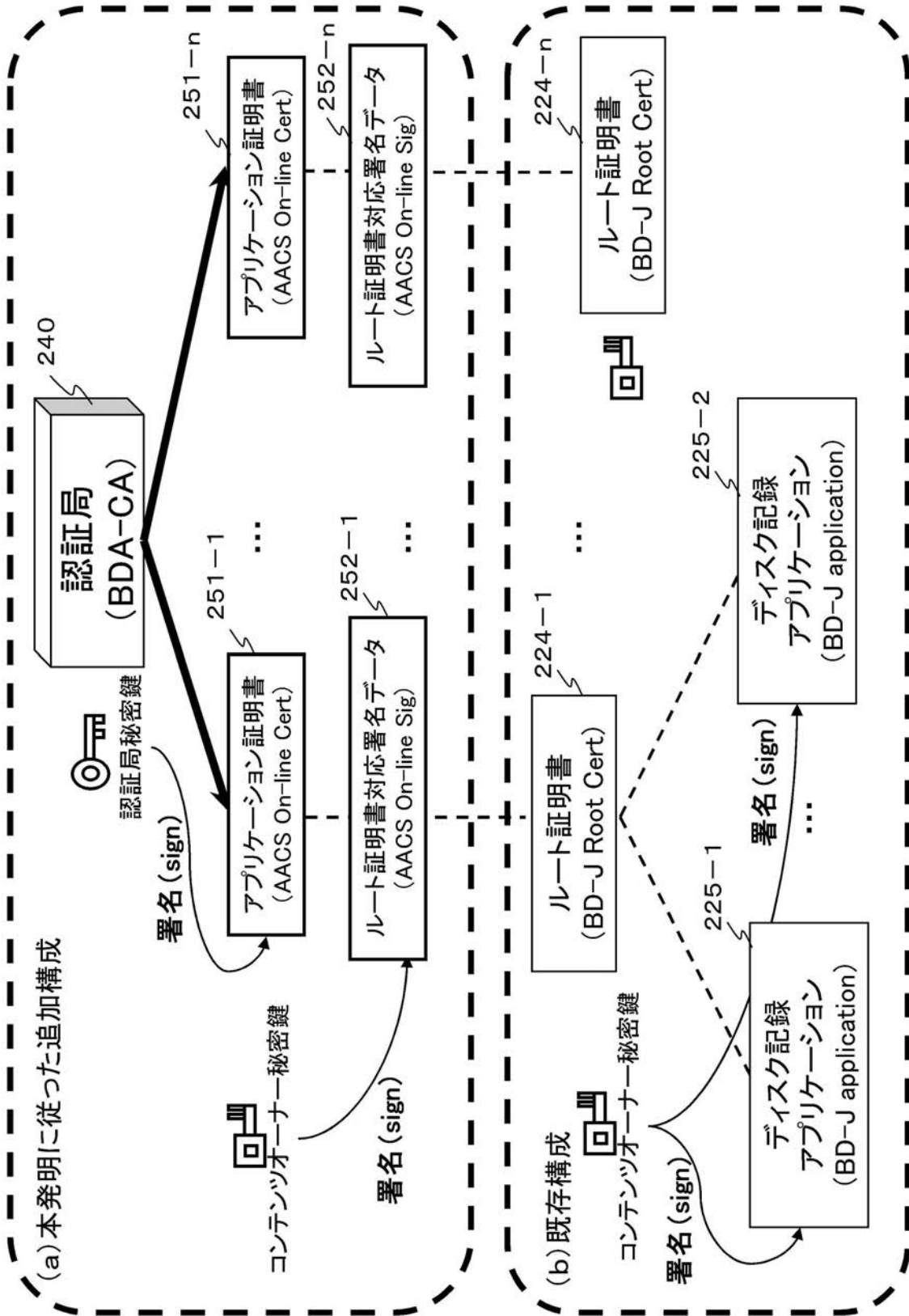
【図8】



【図9】



【 図 5 】



フロントページの続き

- (72)発明者 大石 丈於
東京都港区港南1丁目7番1号 ソニー株式会社内
- (72)発明者 村松 克美
東京都港区港南1丁目7番1号 ソニー株式会社内
- (72)発明者 加藤 元樹
東京都港区港南1丁目7番1号 ソニー株式会社内
- (72)発明者 小林 義行
東京都港区港南1丁目7番1号 ソニー株式会社内

審査官 和田 財太

- (56)参考文献 特開2007-150587(JP,A)
特開2007-128366(JP,A)
特開2006-221629(JP,A)
特開2005-124097(JP,A)
特開2007-157308(JP,A)
国際公開第2006/085647(WO,A1)
特開2006-050355(JP,A)
特開2005-328198(JP,A)

(58)調査した分野(Int.Cl., DB名)

G06F 21/22 - 21/24