

(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2013年5月23日(23.05.2013)



(10) 国際公開番号

WO 2013/073335 A1

- (51) 国際特許分類:
H04L 9/08 (2006.01) H04L 9/32 (2006.01)
- (21) 国際出願番号: PCT/JP2012/077066
- (22) 国際出願日: 2012年10月19日(19.10.2012)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願 2011-251734 2011年11月17日(17.11.2011) JP
- (71) 出願人: ソニー株式会社 (SONY CORPORATION)
[JP/JP]; 〒1080075 東京都港区港南1丁目7番1号 Tokyo (JP).
- (72) 発明者: 小林 義行 (KOBAYASHI, Yoshiyuki); 〒1080075 東京都港区港南1丁目7番1号 ソニー株式会社内 Tokyo (JP). 久野 浩 (KUNO, Hiroshi); 〒1080075 東京都港区港南1丁目7番1号 ソニー株式会社内 Tokyo (JP). 林 隆道 (HAYASHI, Takamichi); 〒1080075 東京都港区港南1丁目7番1号 ソニー株式会社内 Tokyo (JP).
- (74) 代理人: 宮田 正昭, 外 (MIYATA, Masaaki et al.); 〒1040032 東京都中央区八丁堀三丁目25番9号 KSKビル西館8階 特許業務法人 大同特許事務所 Tokyo (JP).

- (81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.
- (84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

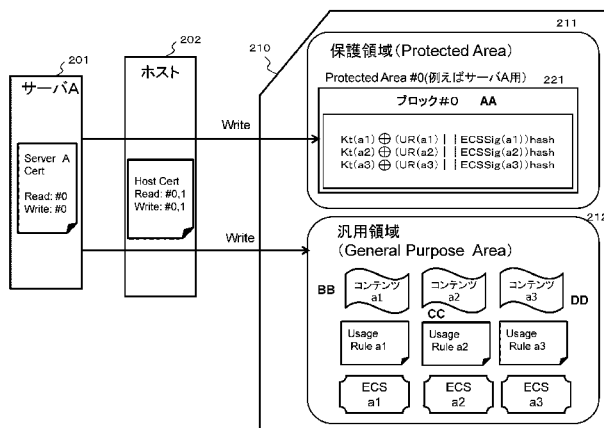
添付公開書類:

— 国際調査報告 (条約第21条(3))

(54) Title: INFORMATION PROCESSING DEVICE, INFORMATION STORAGE DEVICE, INFORMATION PROCESSING SYSTEM, AND INFORMATION PROCESSING METHOD, AS WELL AS PROGRAM

(54) 発明の名称: 情報処理装置、情報記憶装置、情報処理システム、および情報処理方法、並びにプログラム

[図19]



201 Server A
202 Host
211 Protected Area
212 General Purpose Area
221 Protected Area #0 (for example, for server A)
AA Block #0
BB Content a1
CC Content a2
DD Content a3

(57) Abstract: Provided are a device and method which effectively prevent unauthorized use of content. When performing decryption processing of encrypted content, a converted encryption key, which is converted data for an encryption key which is applied to decryption of encrypted content recorded upon a medium, is read in order to perform computation processing for the converted encryption key so as to perform acquisition processing for the encryption key. The converted encryption key is a converted encryption key that is generated by performing computation on the encryption key and an electronic signature, which is configuration data for an encrypted content signature file which is set in accordance with the encrypted content. A playback device acquires the electronic signature, which is the configuration data for the encrypted content signature file recorded upon the medium, in order to perform computation processing in which the acquired electronic signature is applied so as to perform acquisition processing for the encryption key. The electronic signature is set as an electronic signature for data which includes configuration data for the encrypted content and the encryption key.

(57) 要約:

[続葉有]

WO 2013/073335 A1



コンテンツの不正利用を効果的に防止する装置、方法を提供する。暗号化コンテンツの復号処理に際して、メディアに記録された暗号化コンテンツの復号に適用する暗号鍵の変換データである変換暗号鍵を読み出し、変換暗号鍵に対する演算処理を実行して暗号鍵の取得処理を実行する。変換暗号鍵は、暗号鍵と、暗号化コンテンツに対応して設定された暗号化コンテンツ署名ファイルの構成データである電子署名との演算によって生成された変換暗号鍵であり、再生装置は、メディアに記録された暗号化コンテンツ署名ファイルの構成データである電子署名を取得し、取得した電子署名を適用した演算処理を実行して暗号鍵の取得処理を実行する。電子署名は、暗号化コンテンツの構成データおよび暗号鍵を含むデータに対する電子署名として設定される。

明 細 書

発明の名称：

情報処理装置、情報記憶装置、情報処理システム、および情報処理方法、並びにプログラム

技術分野

[0001] 本開示は、情報処理装置、情報記憶装置、情報処理システム、および情報処理方法、並びにプログラムに関する。特に、コンテンツの不正利用を防止する情報処理装置、情報記憶装置、情報処理システム、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] 例えば映画や音楽などのコンテンツは、DVD (Digital Versatile Disc) や、Blu-ray Disc (登録商標)、あるいはフラッシュメモリなど、様々なメディア、あるいはインターネット等のネットワーク、あるいは放送波などを介してユーザに提供される。ユーザは、例えばPC、携帯端末、BDプレーヤ等の記録再生装置、テレビなど様々な情報処理装置を利用して、コンテンツの再生を行うことができる。

[0003] しかし、これらユーザに提供される音楽データ、画像データ等の多くのコンテンツは、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ている。従って、コンテンツ提供者は、ユーザにコンテンツを提供する場合、所定のコンテンツ利用制限が行う場合が多い。

[0004] デジタル記録装置および記録媒体によれば、例えば画像や音声を劣化させることなく記録、再生を繰り返すことが可能であり、不正コピーコンテンツのインターネットを介した配信や、いわゆる海賊版ディスクの流通など不正コピーコンテンツの利用が蔓延しているといった問題が発生している。

このようなデータの不正なコピーを防ぐため、デジタル記録装置および記録媒体に違法なコピーを防止するための様々な技術が実用化されている。

[0005] 例えば、コンテンツ暗号化処理はその1つの態様である。暗号化データを

復号するために用いる鍵が、コンテンツ利用権であるライセンスを受けた再生装置のみに与えられる。ライセンスは、例えば不正コピーを行わない等の所定の動作規定に従うように設計された再生装置に対して与えられる。一方、ライセンスを受けていない再生装置は、暗号化されたデータを復号するための鍵を有していないため、暗号化データの復号を行うことができない。

[0006] しかしながら、このようなコンテンツの暗号化を実行しても、不正なコンテンツ利用が行われてしまうという現状がある。

具体的なコンテンツの不正利用の一例について説明する。

コンテンツサーバが、ユーザ機器、例えば記録再生機器や、PC、あるいは携帯端末等のユーザ機器に対して暗号化コンテンツを配信する構成を想定する。

[0007] コンテンツサーバが、ユーザ機器に対して暗号化コンテンツを配信する場合、コンテンツサーバは、

(a) 暗号化コンテンツ

(b) 暗号化コンテンツの暗号化および復号に適用する暗号鍵

これらの各データを例えばネットワークを介してユーザ機器に配信する。

[0008] 例えば同じ映画等の同一コンテンツを多数のユーザ機器に提供する場合、コンテンツサーバの実行する処理態様としては、例えば以下の2つの処理態様がある。

(A) ユーザ機器各々に対して、個別の異なる暗号鍵を適用して異なる暗号化コンテンツを生成して提供する。

(B) 複数のユーザ機器に対して、同一の暗号鍵で暗号化した同じ暗号化コンテンツを生成して提供する。

[0009] コンテンツの不正利用を防止するための安全性を考慮した場合、上記(A)の処理は有効である。

しかし、上記(A)の処理を行うためには、多数のユーザ各々に対して、個別の暗号鍵を設定して個別の暗号化コンテンツを生成する処理が必要となり、暗号鍵の生成、管理、暗号化コンテンツの生成処理等、コンテンツを配

信するユーザ数に応じてサーバの処理負荷が増大するという問題が発生する。

[0010] 従って、多くの場合上記（B）の処理、すなわち、同一コンテンツについては、同一の暗号鍵で暗号化した同じ暗号化コンテンツを生成して、複数のユーザに提供する処理が行われることが多い。

例えば、あるタイトルのコンテンツに対して、1つの暗号鍵（＝タイトルキー）を設定し、この1つのタイトルキーを適用して同一の暗号化コンテンツを生成して、

（a）暗号化コンテンツ、

（b）タイトルキー

これらのデータセットを、多数のユーザに配信するものである。

このような処理を行うことで、コンテンツサーバの処理負荷は削減される。

。

[0011] なお、以下、コンテンツのタイトル単位で設定される暗号鍵を「タイトルキー」として説明する。

なお、タイトルキーは、そのタイトルの暗号化コンテンツの暗号化と復号処理に適用される。

[0012] しかし、このように、多数のユーザに同一のデータセット、すなわち、

（a）暗号化コンテンツ

（b）タイトルキー

これらの同一のデータの組み合わせを配信すると、一部の「不正ユーザ」によって以下のような処理が行われる可能性がある。

[0013] （１）「不正ユーザ」が、サーバから受信したタイトルキーを読み出して、読み出したタイトルキーを不特定多数のユーザに対して公開する。

あるいは、

（２）「不正ユーザ」が、ある暗号化コンテンツAに対応するタイトルキーAを使用して、全く別のコンテンツBを暗号化して、

（X）タイトルキーA、

(Y) タイトルキー A で暗号化した暗号化コンテンツ B、
これらの組み合わせデータを不特定多数のユーザに配信する。
このような不正が実行される可能性がある。

[0014] 例えば上記 (1) の処理が行われると、不正公開されたタイトルキーを取得した多数のユーザによって、そのタイトルキーを利用して暗号化されたコンテンツが不正に利用される。

また、上記 (2) の処理が行われると、上記の「不正ユーザ」の生成した不正なデータセット、すなわち、

(X) タイトルキー A、
(Y) タイトルキー A で暗号化した暗号化コンテンツ B、
これらを「不正ユーザ」から取得することで、多数のユーザによって、暗号化コンテンツ B が不正に利用されてしまうことになる。

結果として、本来の正規なデータセット、すなわち、
暗号化コンテンツ B、
暗号化コンテンツ B に対応するタイトルキー B、
これらのデータセットを正規に購入するユーザが減少し、著作権者や頒布権者の利益が著しく損なわれることになる。

[0015] さらに、具体的な不正処理例について説明する。

コンテンツサーバが、以下の (1) ~ (3) の暗号化コンテンツ (C) とタイトルキー (K t) のデータセットを保持しているものとする。

(1) (K t 1 1, C 1 1)

(2) (K t 1 2, C 1 2)

(3) (K t 1 3, C 1 3)

ただし、

C n n は、コンテンツファイル

K t n n は、コンテンツの暗号化に使用したタイトルキー
である。

(K t 1 1, C 1 1) は、タイトルキー (K t 1 1) と、タイトルキー (

K t 1 1) によって暗号化されたコンテンツ (C 1 1) のデータセットである。

[0016] 例えば、ある「不正ユーザU x」が、上記の3つのデータセット

(1) (K t 1 1, C 1 1)

(2) (K t 1 2, C 1 2)

(3) (K t 1 3, C 1 3)

これらを総て購入したとする。

この購入処理自体は、「不正ユーザU x」の持つユーザ機器、例えばP Cとコンテンツサーバとの所定の正当な購入手続に従って行われたものとする。

「不正ユーザU x」は、ユーザ機器であるP Cの例えばハードディスク等のメディアに上記の(1)～(3)のデータセットを記録する。

[0017] 「不正ユーザU x」は、P C等のユーザ機器P Cのハードディスク等のメディアから上記の(1)～(3)のデータセットを読み出し、一旦、すべての暗号化コンテンツをそれぞれのタイトルキーで復号し、以下のデータを得る。

タイトルキー：K t 1 1, K t 1 2, K t 1 3

復号コンテンツ：C 1 1, C 1 2, C 1 3

なお、正当な再生機器において、正規のコンテンツ再生プログラムを利用する場合にはタイトルキーを外部に読み出すことはできないが、P C等の装置に不正プログラムをインストールするなどの方法によって、タイトルキー自体が読み出されてしまう可能性があり、タイトルキーの読み出しを完全に防止することは困難であるというのが現状である。

[0018] さらに、「不正ユーザU x」は、

復号コンテンツ：C 1 1～C 1 3を連結したデータ、

C 1 1 | | C 1 2 | | C 1 3

を生成し、

この連結データをタイトルキー：K t 1 1で暗号化する。

すなわち、以下のデータセット、

(K t 1 1, C 1 1 | | C 1 2 | | C 1 3)

を生成し、このデータセットを、ネットワークを介して不正に流通、例えば安い価格で販売、あるいは無償で多くのユーザに提供するといったことを行う。

[0019] このような処理が行われると、

多くの一般ユーザは、上記の「不正ユーザU x」から、上記の不正作成データセット、すなわち、

(K t 1 1, C 1 1 | | C 1 2 | | C 1 3)

上記の不正データセットを取得することが可能となる。

このデータセットは、

(a) タイトルキーK t 1 1で暗号化された暗号化コンテンツ

(b) タイトルキーK t 1 1、

これらのデータセットによって構成されており、

正規のコンテンツ提供者からユーザに提供されるデータセットコンテンツと同一のデータ構成を有している。

[0020] そのため、ライセンスを持つ正当なコンテンツ再生プログラムを持つ正当な再生機器は、タイトルキーK t 1 1を利用して、何ら問題なく暗号化コンテンツ [C 1 1 | | C 1 2 | | C 1 3] を復号、再生してしまうことができる。

結果として、正規なコンテンツ購入が行われることなく、不正利用が蔓延し、C 1 1～C 1 3等のコンテンツを正規に購入するユーザが減少により、正当権利者の利益が損なわれることになる。

[0021] さらに具体化して説明する。例えば、あるドラマなど、1話～12話の12タイトルからなるシリーズコンテンツにおいて、

1話 = (K t 0 1, C 0 1)

2話 = (K t 0 2, C 0 2)

3話 = (K t 0 3, C 0 3)

：

1 2 話 = (K t 1 2, C 1 2)

上記のように各話単位で、コンテンツの購入単位を設定としているとする

。

[0022] このような場合に、ある 1 人の「不正ユーザ」が 1 話～1 2 話の 1 2 タイトルのシリーズ全てを購入して、1 話～1 2 話のコンテンツ：C 0 1～C 1 2 を連結して、1 話対応のタイトルキー：K t 0 1 で再暗号化したデータセット、すなわち、

(K t 0 1, C 0 1 || C 0 2 || C 0 3 . . . || C 1 2)

を生成して、ネットワーク上で公開してしまう。あるいは不正に販売するといった処理を行う。

[0023] このような場合、多数のユーザ機器において、「不正ユーザ」の生成した不正データセット、

(K t 0 1, C 0 1 || C 0 2 || C 0 3 . . . || C 1 2)

を取得して再生、利用してしまうといったことが可能となる。

例えば、上記の 1 2 話の各々の 1 話単位の正規価格が ¥ 2, 0 0 0 であるとする。

この場合、1 2 話全話を購入すると、

1 2 × ¥ 2, 0 0 0 = ¥ 2 4, 0 0 0

である。

[0024] 上記の「不正ユーザ」は、上記の不正データセット、

(K t 0 1, C 0 1 || C 0 2 || C 0 3 . . . || C 1 2)

を、例えば ¥ 6, 0 0 0 で販売する。この場合、多くのユーザがこの安いコンテンツを購入してしまい、結果として、正規なコンテンツ販売が阻害され、本来の著作権者や販売権者の利益、権利が侵害されることになる。

[0025] 上記の例の他、ある 1 つのコンテンツ C 1 1 に対応して設定されたタイトルキー K t 1 1 を、その他の無関係の様々なコンテンツ C x x の暗号化に利用して、

(K t 1 1, C x x)

コンテンツ、C x xを様々なコンテンツとすることが可能であり、無制限にすべてのコンテンツを1つのタイトルキーで復号、再生することが可能となるという問題が発生する。

すなわち、平文コンテンツの再生を禁止した再生機器を作成したとしても、上記の不正なデータセットの利用により、正規購入コンテンツと同様の復号、再生が可能になってしまう。

[0026] さらに「不正ユーザ」は、タイトルキーのすげかえ、再暗号化をサービスとして立ち上げることも可能となり、あたかもオーソライズされたサーバのごとく振舞える。

[0027] このように、コンテンツの暗号化処理という対策のみでは、コンテンツの不正利用を防止することが困難になっている。

[0028] 暗号化処理と異なるコンテンツ不正利用排除手法として、再生装置にコンテンツの改ざん検証を実行させる手法がある。この手法を適用することで、例えば不正コンテンツの流通過程において、コンテンツに何等かの変更（改ざん）が行われた場合にその改ざんコンテンツの利用を停止させることができる。

[0029] 具体的には、コンテンツ再生を実行するユーザ装置において、コンテンツの改ざんの有無検証処理を実行させて、コンテンツに改ざんがないことが確認された場合にのみコンテンツ再生を許容し、改ざんがあることが判明した場合には、コンテンツの再生を実行しない構成とする制御構成である。

[0030] 例えば、特許文献1（特開2002-358011号公報）には、再生予定のコンテンツファイルからハッシュ値を計算し、予め容易された照合用ハッシュ値、すなわち正当なコンテンツデータに基づいて予め計算済みの照合用ハッシュ値との比較を実行し、新たに算出したハッシュ値が照合用ハッシュ値と一致した場合には、コンテンツの改ざんは無いと判定して、コンテンツの再生処理に移行する制御構成を開示している。

[0031] しかし、このようにハッシュ値をコンテンツに基づいて算出する処理を実

行する場合、ハッシュ値算出の元データとしてのコンテンツデータの容量が大きい場合、計算に要する処理負荷、処理時間が多大なものとなる。昨今では動画像データの高品質化が進み、1コンテンツあたり、数GB～数十GBのデータ量を持つ場合が多くなっている。このような大容量データに基づくコンテンツのハッシュ値算出処理を、コンテンツ再生を実行するユーザ機器に行わせることは、ユーザ機器に求められるデータ処理能力が過大になるという問題、さらに、コンテンツの検証に要する時間が長くなり、コンテンツ再生処理が効率的に行われないという問題が発生する。

[0032] また、特許文献2（特許第4576936号）には、情報記録媒体の格納コンテンツの細分化データとして設定されたハッシュユニット各々についてのハッシュ値をコンテンツハッシュテーブルに記録してコンテンツとともに情報記録媒体に格納した構成を開示している。

[0033] この開示構成によれば、コンテンツ再生を実行する情報処理装置は、ランダムに選択した1つ以上のハッシュユニットに基づいてハッシュ値照合処理を実行する。本構成によりコンテンツのデータ量にかかわらず、少ないデータ量のハッシュユニットに基づくハッシュ値の算出、照合処理が可能となり、コンテンツ再生を実行するユーザ機器における効率的なコンテンツ検証が可能となる。

[0034] しかし、特許文献2に記載の構成は、情報記録媒体の格納コンテンツに対する処理を前提としている。この開示構成は、例えば情報記録媒体の製造時にコンテンツとともにハッシュ値も併せて記録できる場合には利用可能であるが、例えばサーバからのダウンロードコンテンツに対して適用することは困難であるという問題がある。

[0035] また、上記の特許文献1、特許文献2は、いずれもコンテンツの改ざん検証に重点をおいており、改ざんのない不正コピーコンテンツの流通に対しては、何ら制御することができないという問題がある。

このように、従来技術としてのコンテンツの暗号化や、改ざん検証処理は、不正コピーコンテンツの流通や、コンテンツ暗号鍵の漏えいに対して、十

分な防止効果を奏していないというのが現状である。

先行技術文献

特許文献

[0036] 特許文献1：特開2002-358011号公報

特許文献2：特許第4576936号

発明の概要

発明が解決しようとする課題

[0037] 本開示は、例えば上記問題点に鑑みてなされたものであり、コンテンツの不正利用の効果的な防止を実現する情報処理装置、情報記憶装置、情報処理システム、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

[0038] 本開示の第1の側面は、

暗号化コンテンツおよび暗号化コンテンツの復号に適用する暗号鍵を格納する記憶部を有し、

前記記憶部は、前記暗号鍵を前記暗号化コンテンツに対応して設定された暗号化コンテンツ署名ファイルの構成データである電子署名との演算によって生成された変換暗号鍵を格納し、

前記電子署名は、前記暗号化コンテンツの構成データおよび前記暗号鍵を含むデータに対する電子署名であり、

前記記憶部から前記暗号化コンテンツを読み出して復号処理を実行する再生装置に、前記変換暗号鍵に対する電子署名の適用演算による暗号鍵取得を行わせることを可能とした情報記憶装置にある。

[0039] さらに、本開示の情報記憶装置の一実施態様において、前記変換暗号鍵は、前記暗号化コンテンツに対応して設定される利用制御情報と、前記電子署名との連結データに対するハッシュ値と、前記暗号鍵との排他的論理和演算結果である。

- [0040] さらに、本開示の情報記憶装置の一実施態様において、前記記憶部は、アクセス制限の設定された保護領域を有し、前記変換暗号鍵を、前記保護領域に格納した構成である。
- [0041] さらに、本開示の情報記憶装置の一実施態様において、前記情報記憶装置は、前記保護領域に対するアクセス要求装置から受領した証明書に基づいて、前記保護領域に対するアクセス可否を判定するデータ処理部を有する。
- [0042] さらに、本開示の情報記憶装置の一実施態様において、前記記憶部は、アクセス制限の設定された保護領域と、アクセス制限のない汎用領域を有し、前記変換暗号鍵を、前記保護領域に格納し、前記暗号化コンテンツと、前記暗号化コンテンツ署名ファイルを、前記汎用領域に格納した構成である。
- [0043] さらに、本開示の情報記憶装置の一実施態様において、前記電子署名は、前記暗号化コンテンツの構成データおよび前記暗号鍵、さらに、前記暗号化コンテンツ署名ファイルの構成データを含むデータに対する電子署名である。
- [0044] さらに、本開示の情報記憶装置の一実施態様において、前記電子署名は、前記暗号化コンテンツ署名ファイルの構成データである前記暗号化コンテンツ署名ファイルの発行日時情報を含むデータに対する電子署名である。
- [0045] さらに、本開示の第2の側面は、
メディアに記録された暗号化コンテンツの復号および再生処理を実行するデータ処理部を有し、
前記データ処理部は、
前記暗号化コンテンツの復号処理に際して、前記メディアに記録された前記暗号化コンテンツの復号に適用する暗号鍵の変換データである変換暗号鍵を読み出し、該変換暗号鍵に対する演算処理を実行して暗号鍵の取得処理を実行し、
前記変換暗号鍵は、
前記暗号鍵を前記暗号化コンテンツに対応して設定された暗号化コンテンツ署名ファイルの構成データである電子署名との演算によって生成された変

換暗号鍵であり、

前記データ処理部は、

前記メディアに記録された暗号化コンテンツ署名ファイルの構成データである電子署名を取得し、取得した電子署名を適用した演算処理を実行して暗号鍵の取得処理を実行する情報処理装置にある。

[0046] さらに、本開示の情報処理装置の一実施態様において、前記電子署名は、前記暗号化コンテンツの構成データおよび前記暗号鍵を含むデータに対する電子署名である。

[0047] さらに、本開示の情報処理装置の一実施態様において、前記変換暗号鍵は、前記暗号化コンテンツに対応して設定される利用制御情報と、前記電子署名との連結データに対するハッシュ値と、前記暗号鍵との排他的論理和演算結果であり、前記データ処理部は、前記メディアに記録された暗号化コンテンツ署名ファイルの構成データである電子署名と、前記メディアに記録された利用制御情報を取得し、取得したデータを適用した演算処理を実行して暗号鍵の取得処理を実行する。

[0048] さらに、本開示の情報処理装置の一実施態様において、前記データ処理部は、前記メディアに記録された暗号化コンテンツ署名ファイルの構成データである電子署名に対する署名検証処理を実行し、該署名検証処理に成功し、前記暗号化コンテンツ署名ファイルの正当性を確認したことを条件として、前記暗号鍵の取得処理を行う。

[0049] さらに、本開示の第3の側面は、

メディアに記録する暗号化コンテンツと、該暗号化コンテンツの復号に適用する暗号鍵の変換データである変換暗号鍵を出力するデータ処理部を有し、

前記データ処理部は、

前記暗号化コンテンツに対応して設定された暗号化コンテンツ署名ファイルの構成データである電子署名であり、前記暗号化コンテンツの構成データおよび前記暗号鍵を含むデータに対する電子署名と、前記暗号鍵の演算処理

により、前記変換暗号鍵を生成する情報処理装置にある。

[0050] さらに、本開示の情報処理装置の一実施態様において、前記データ処理部は、前記暗号化コンテンツに対応して設定される利用制御情報と、前記電子署名との連結データに対するハッシュ値と、前記暗号鍵との排他的論理和演算を実行して前記変換暗号鍵を生成する。

[0051] さらに、本開示の第4の側面は、

情報処理装置において実行する情報処理方法であり、

データ処理部が、メディアに記録された暗号化コンテンツの復号処理に際して、復号に適用する暗号鍵の変換データである変換暗号鍵を読み出し、該変換暗号鍵に対する演算処理を実行して暗号鍵の取得処理を行うデータ処理ステップを実行し、

前記変換暗号鍵は、

前記暗号鍵を前記暗号化コンテンツに対応して設定された暗号化コンテンツ署名ファイルの構成データである電子署名との演算によって生成された変換暗号鍵であり、

前記データ処理部は、前記データ処理部ステップにおいて、

前記メディアに記録された暗号化コンテンツ署名ファイルから前記電子署名を取得し、取得した電子署名を適用した演算処理を実行して暗号鍵の取得処理を実行する情報処理方法にある。

[0052] さらに、本開示の第5の側面は、

情報処理装置において実行する情報処理方法であり、

データ処理部が、メディアに記録する暗号化コンテンツと、該暗号化コンテンツの復号に適用する暗号鍵の変換データである変換暗号鍵を出力するデータ処理ステップを実行し、

前記データ処理ステップにおいて、

前記暗号化コンテンツに対応して設定された暗号化コンテンツ署名ファイルの構成データである電子署名であり、前記暗号化コンテンツの構成データおよび前記暗号鍵を含むデータに対する電子署名と、前記暗号鍵の演算処理

により、前記変換暗号鍵を生成する情報処理方法にある。

[0053] さらに、本開示の第6の側面は、

情報処理装置において情報処理を実行させるプログラムであり、

データ処理部に、メディアに記録された暗号化コンテンツの復号処理に際して、復号に適用する暗号鍵の変換データである変換暗号鍵の読み出し処理と、該変換暗号鍵に対する演算処理による暗号鍵の取得処理を行うデータ処理ステップを実行させ、

前記変換暗号鍵は、

前記暗号鍵を前記暗号化コンテンツに対応して設定された暗号化コンテンツ署名ファイルの構成データである電子署名との演算によって生成された変換暗号鍵であり、

前記データ処理部ステップにおいて、

前記メディアに記録された暗号化コンテンツ署名ファイルから前記電子署名の取得処理と、取得した電子署名を適用した演算処理による暗号鍵の取得処理を実行させるプログラムにある。

[0054] さらに、本開示の第7の側面は、

情報処理装置において情報処理を実行させるプログラムであり、

データ処理部に、メディアに記録する暗号化コンテンツと、該暗号化コンテンツの復号に適用する暗号鍵の変換データである変換暗号鍵を出力するデータ処理ステップを実行させ、

前記データ処理ステップにおいて、

前記暗号化コンテンツに対応して設定された暗号化コンテンツ署名ファイルの構成データである電子署名であり、前記暗号化コンテンツの構成データおよび前記暗号鍵を含むデータに対する電子署名と、前記暗号鍵の演算処理により、前記変換暗号鍵を生成させるプログラムにある。

[0055] なお、本開示のプログラムは、例えば、様々なプログラム・コードを実行可能な情報処理装置やコンピュータ・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、情報処理装置やコンピュータ・システム上でプログラムに応じた処理が実現される。

[0056] 本開示のさらに他の目的、特徴や利点は、後述する本開示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

[0057] 本開示の一実施例の構成によれば、コンテンツの不正利用を効果的に防止する装置、方法が実現される。

具体的には、暗号化コンテンツの復号処理に際して、メディアに記録された暗号化コンテンツの復号に適用する暗号鍵の変換データである変換暗号鍵を読み出し、変換暗号鍵に対する演算処理を実行して暗号鍵の取得処理を実行する。変換暗号鍵は、暗号鍵と、暗号化コンテンツに対応して設定された暗号化コンテンツ署名ファイルの構成データである電子署名との演算によって生成された変換暗号鍵であり、再生装置は、メディアに記録された暗号化コンテンツ署名ファイルの構成データである電子署名を取得し、取得した電子署名を適用した演算処理を実行して暗号鍵の取得処理を実行する。電子署名は、暗号化コンテンツの構成データおよび暗号鍵を含むデータに対する電子署名として設定される。

この暗号化コンテンツ署名ファイルの署名データを変換暗号鍵の構成データとすることで、鍵の掛け替え処理などによるコンテンツ不正利用を防止することが可能となる。

図面の簡単な説明

[0058] [図1]コンテンツ提供処理および利用処理の概要について説明する図である。

[図2]メモ리카ードに記録されたコンテンツの利用形態について説明する図である。

[図3]メモ리카ードの記憶領域の具体的構成例について説明する図である。

[図4]ホスト証明書 (Host Certificate) について説明する図である。

[図5]サーバ証明書 (Server Certificate) について説明する図である。

[図6]メモ리카ードの記憶データの具体的構成例とアクセス制御処理の一例について説明する図である。

[図7]コンテンツの不正利用を防止するための本開示の情報処理システムの全体構成について説明する図である。

[図8]コンテンツの不正利用を防止するために適用するデータの各装置間の流れについて説明する図である。

[図9]暗号化コンテンツ署名ファイル (ECSファイル) の構成例について説明する図である。

[図10]暗号化コンテンツ署名ファイル (ECSファイル) の構成例について説明する図である。

[図11]暗号化コンテンツ署名ファイル (ECSファイル) に含まれるECS発行装置証明書の構成例について説明する図である。

[図12]ECS発行装置証明書リボケーションリストの構成例について説明する図である。

[図13]暗号化コンテンツ署名ファイル (ECSファイル) の生成処理とデータ構成の概要について説明する図である。

[図14]暗号化コンテンツ署名ファイル (ECSファイル) の生成とコンテンツ提供、利用処理シーケンスについて説明するシーケンス図である。

[図15]暗号化コンテンツ署名ファイル (ECSファイル) の生成とコンテンツ提供、利用処理シーケンスについて説明するシーケンス図である。

[図16]暗号化コンテンツ署名ファイル (ECSファイル) に記録された日時データを適用したコンテンツ提供可否判定処理の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17]暗号化コンテンツ署名ファイル (ECSファイル) に記録された日時

データを適用したコンテンツ提供可否判定処理の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18]暗号化コンテンツ署名ファイル（ECSファイル）に記録された日時データを適用したコンテンツ再生可否判定処理の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19]メモリカードに対するサーバのデータ記録処理の一例について説明する図である。

[図20]メモリカードの記録データに対するホストの読み取り処理の一例について説明する図である。

[図21]メモリカードに対する記録データの構成例について説明する図である。

[図22]メモリカードに対する記録データの構成例について説明する図である。

[図23]メモリカードの汎用領域に記録される利用制御情報の記録データの構成例について説明する図である。

[図24]すげ替え処理による不正なコンテンツ利用例について説明する図である。

[図25]すげ替え処理による不正なコンテンツの記録処理例について説明するフローチャートを示す図である。

[図26]すげ替え処理によって記録した不正コンテンツの再生が実行できないことを説明するフローチャートを示す図である。

[図27]すげ替え処理による不正なコンテンツ利用例について説明する図である。

[図28]すげ替え処理による不正なコンテンツの記録処理例について説明するフローチャートを示す図である。

[図29]すげ替え処理によって記録した不正コンテンツの再生が実行できないことを説明するフローチャートを示す図である。

[図30]暗号化コンテンツ署名ファイル（ECSファイル）に記録されたプロ

ック識別子と利用制御情報ファイルに記録されたブロック識別子について説明する図である。

[図31]暗号化コンテンツ署名ファイル（ECSファイル）に記録されたブロック識別子と利用制御情報ファイルに記録されたブロック識別子を適用したコンテンツ提供可否判定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32]ECS発行装置証明書からのブロック識別子読み出し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33]暗号化コンテンツ署名ファイル（ECSファイル）に記録されたブロック識別子と利用制御情報ファイルに記録されたブロック識別子を適用したコンテンツ再生可否判定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34]情報処理装置のハードウェア構成例について説明する図である。

[図35]メモリカードとしての情報処理装置のハードウェア構成例について説明する図である。

発明を実施するための形態

[0059] 以下、図面を参照しながら本開示の情報処理装置、情報記憶装置、情報処理システム、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。なお、説明は以下の項目に従って行う。

1. コンテンツ提供処理および利用処理の概要について
2. メモリカードの構成例と利用例について
3. 保護領域に対するアクセス許容情報を持つ証明書について
4. 各装置の証明書を適用したメモリカードに対するアクセス処理例について
5. 暗号化コンテンツ署名（ECS）発行装置を利用したコンテンツ提供システムについて
6. ECSファイルの構成例について
7. ECS発行装置証明書リボケーションリストの構成について

8. 暗号化コンテンツ署名ファイル（ECSファイル）の生成処理について

9. ECSファイル、ECS発行装置証明書の日時情報を適用した処理について

10. 暗号鍵とECS発行装置署名との関連づけ構成について

11. 暗号化コンテンツ署名（ECS）ファイルに記録したブロック識別子の適用処理について

12. 各装置のハードウェア構成例について

13. 本開示の構成のまとめ

[0060] [1. コンテンツ提供処理および利用処理の概要について]

以下、図面を参照しながら本開示の情報処理装置、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。

[0061] まず、図1以下を参照して、コンテンツ提供処理および利用処理の概要について説明する。

図1には、左から、

(a) コンテンツ提供装置

(b) コンテンツ記録再生装置（ホスト）

(c) コンテンツ記録メディア

これらの例を示している。

[0062] (c) コンテンツ記録メディアはユーザがコンテンツを記録して、コンテンツの再生処理に利用するメディアである。ここでは例えばフラッシュメモリ等の情報記憶装置であるメモリカード31を示している。

なお、以下の実施例では、コンテンツ提供装置が提供するコンテンツは暗号化コンテンツである例を代表例として説明するが、本開示の構成は、提供コンテンツが暗号化コンテンツである場合に限らず、暗号化されていない平文コンテンツである場合にも適用可能である。

[0063] ユーザは、例えば音楽や映画などの様々なコンテンツをメモリカード31に記録して利用する。これらのコンテンツには例えば著作権の管理対象とな

るコンテンツ等、利用制御対象となるコンテンツが含まれる。

[0064] 利用制御対象となるコンテンツとは、例えば無秩序なコピーやコピーデータ配布等が禁止されたコンテンツや、利用期間が制限されたコンテンツ等である。なお、メモリカード31に対して、利用制御コンテンツを記録する場合、そのコンテンツに対応する利用制御情報（Usage Rule）が合わせて記録される。

利用制御情報（Usage Rule）には、例えば許容されるコンテンツ利用期間や許容されるコピー回数などのコンテンツ利用に関する情報が記録される。

コンテンツ提供装置は、コンテンツに併せてコンテンツ対応の利用御情報を提供する。

[0065] （a）コンテンツ提供装置は、音楽や映画等のコンテンツの提供元である。図1には、一例として、放送局11と、コンテンツサーバ12をコンテンツ提供装置として示している。

放送局11は、例えばテレビ局であり、様々な放送コンテンツを地上波や衛星を介した衛星波に載せてユーザ装置〔（b）コンテンツ記録再生装置（ホスト）〕に提供する。

コンテンツサーバ12は、音楽や映画等のコンテンツをインターネット等のネットワークを介して提供するサーバである。

[0066] ユーザは、例えば（c）コンテンツ記録メディアであるメモリカード31を（b）コンテンツ記録再生装置（ホスト）に装着し、（b）コンテンツ記録再生装置（ホスト）自体の受信部、あるいは、コンテンツ記録再生装置（ホスト）に接続された受信装置を介して、放送局11やコンテンツサーバ12の提供するコンテンツを受信してメモリカード31に記録することができる。

[0067] （b）コンテンツ記録装置（ホスト）は、（c）コンテンツ記録メディアであるメモリカード31を装着して、（a）コンテンツ提供装置である放送局11やコンテンツサーバ12から受信したコンテンツをメモリカード31

に記録する。

[0068] (b) コンテンツ記録再生装置（ホスト）としては、例えばDVDプレーヤなど、ハードディスクやDVD、BD等のディスクを備えた記録再生専用器（CE機器：Consumer Electronics機器）21がある。さらに、PC22や、スマートフォン、携帯電話、携帯プレーヤ、タブレット端末などの携帯端末23などがある。これらはすべて(c) コンテンツ記録メディアであるメモリカード31を装着可能な装置である。

[0069] ユーザは、記録再生専用器21、PC22、携帯端末23などを利用して、放送局11やコンテンツサーバ12から音楽や映画等のコンテンツを受信し、メモリカード31に記録する。

[0070] メモリカード31に記録されたコンテンツの利用形態について図2を参照して説明する。

情報記憶装置であるメモリカード31は、例えばPC等のコンテンツ再生器に対して着脱可能な記録メディアであり、コンテンツ記録を実行した機器から自由に取り外して、その他のユーザ機器に装着することが可能である。

[0071] すなわち、図2に示すように、

(1) 記録処理

(2) 再生処理

これらの処理を実行する。

なお、記録または再生の一方のみを実行する機器もある。

また、記録と再生各処理の実行機器は同一であることは必須ではなく、ユーザは自由に記録機器と再生機器を選択して利用することができる。

[0072] なお、多くの場合、メモリカード31に記録された利用制御コンテンツは暗号化コンテンツとして記録されており、記録再生専用器21やPC22、携帯端末23等のコンテンツ再生装置は、所定のシーケンスに従った復号処理を実行した後、コンテンツ再生を行う。

また、コンテンツに対応して設定される利用制御情報（Usage Rule）に記録された利用許容態様で再生処理などを行う。

(b) コンテンツ記録再生装置（ホスト）には、利用制御情報（U s a g e R u l e）に従ったコンテンツ利用やコンテンツの復号処理を実行するためのプログラム（ホストアプリケーション）が格納されており、コンテンツ再生はこのプログラム（ホストアプリケーション）に従って実行する。

[0073] [2. メモリカードの構成例と利用例について]

次に、コンテンツの記録メディアとして利用されるフラッシュメモリ等のメモリカードの構成例と利用例について説明する。

メモリカード31の記憶領域の具体的構成例を図3に示す。

メモリカード31の記憶領域は、図3に示すように、

(a) 保護領域（P r o t e c t e d A r e a）51、

(b) 汎用領域（G e n e r a l P u r p o s e A r e a）52、

これら2つの領域によって構成される。

[0074] (b) 汎用領域（G e n e r a l P u r p o s e A r e a）52はユーザの利用する記録再生装置によって、自由にアクセス可能な領域であり、コンテンツやコンテンツ対応の利用制御情報（U s a g e R u l e）、その他の一般のコンテンツ管理データ等が記録される。

この汎用領域（G e n e r a l P u r p o s e A r e a）52は、例えばサーバやユーザの記録再生装置によって自由にデータの書き込みや読み取りを行うことか可能な領域である。

[0075] 一方、(a) 保護領域（P r o t e c t e d A r e a）51は、自由なアクセスが許容されない領域である。

保護領域（P r o t e c t e d A r e a）51は複数の区分領域としてのブロック（＃0，＃1，＃2・・・）に分割され、各ブロック単位でアクセス権が設定される。

[0076] 例えば、ユーザの利用する記録再生装置、あるいはネットワークを介して接続されるサーバ等によってデータの書き込みあるいは読み取りを行おうとする場合、メモリカード31のデータ処理部が、メモリカード31に予め格納されたプログラムに従って、各装置に応じてブロック単位で読み取り（R

ead) または書き込み (Write) の可否を決定する。

[0077] メモリカード31は、予め格納されたプログラムを実行するためのデータ処理部や認証処理を実行する認証処理部を備えており、メモリカード31は、まず、メモリカード31に対してデータの書き込みまたは読み取りを実行しようとする装置との認証処理を行う。

[0078] この認証処理の段階で、相手装置、すなわちアクセス要求装置から公開鍵証明書等の装置証明書を受信する。

たとえばアクセス要求装置がサーバである場合は、サーバの保有するサーバ証明書 (Server Certificate) を受信し、その証明書に記載された情報を用いて、保護領域 (Protected Area) 51の各ブロック (区分領域) 単位でアクセスが許容されるか否かを判定する。

[0079] また、アクセス要求装置がホスト装置、例えばコンテンツ記録再生を実行するユーザ機器としての記録再生装置 (ホスト) である場合は、記録再生装置 (ホスト) の保有するホスト証明書 (Host Certificate) を受信し、その証明書に記載された情報を用いて、保護領域 (Protected Area) 51の各ブロック (区分領域) のアクセスが許容されるか否かを判定する。

[0080] このアクセス権判定処理は、図3に示す保護領域 (Protected Area) 51内のブロック (図に示す領域 #0, #1, #2...) 単位で行われる。メモリカード31は、ブロック単位で許可された処理 (データの読み取り/書き込み等の処理) のみをサーバやホストに実行させる。

[0081] メディアに対する読み取り/書き込み制限情報 (PAD Read/PAD Write) は、例えば、アクセスしようとする装置、例えばコンテンツサーバ、あるいは記録再生装置 (ホスト) 単位で設定される。これらの情報は各装置対応のサーバ証明書 (Server Certificate) や、ホスト証明書 (Host Certificate) に記録される。

なお、以下において「Certificate」は、簡略化して「Cer

t」として記載する。

[0082] このように、メモリカード31は、メモリカード31に予め格納された規定のプログラムに従って、サーバ証明書（Server Cert）や、ホスト証明書（Host Cert）の記録データを検証して、アクセス許可のなされた領域についてのみアクセスを許容する処理を行う。

[0083] [3. 保護領域に対するアクセス許容情報を持つ証明書について]

次に、サーバやユーザ装置であるホスト機器（＝記録再生装置）が、上述したメモリカード31の保護領域（Protected Area）51に対するアクセスを行う場合に、メモリカードに提示が必要となる証明書の構成例について図4、図5を参照して説明する。

[0084] 上述したように、メモリカード31は、メモリカード31に対してデータの書き込みまたは読み取りを実行しようとする装置との認証処理を行う。この認証処理の段階で、相手装置、すなわちアクセス要求装置から公開鍵証明書等の装置証明書（たとえばサーバ証明書（Server Cert）やホスト証明書（Host Cert））を受信し、その証明書に記載された情報を用いて、保護領域（Protected Area）51の各区分領域のアクセスを許容するか否かを判定する。

[0085] この認証処理に利用される装置証明書の一例として、図1に示す記録再生専用器21、PC22、携帯端末23等のユーザ機器（ホスト機器）に格納されるホスト証明書（Host Cert）の構成例について図4を参照して説明する。

[0086] ホスト証明書（Host Cert）は、例えば、公開鍵証明書発行主体である認証局によって各ユーザ機器（ホスト機器）に提供される。例えば、ホスト証明書（Host Cert）は、認証局がコンテンツ利用処理を認めたユーザ機器（ホスト機器）に対して発行するユーザ機器の証明書であり、公開鍵等を格納した証明書である。ホスト証明書（Host Cert）は、認証局秘密鍵によって署名が設定され、改ざんの防止されたデータとして構成される。

[0087] なお、装置証明書は、例えば、装置製造時に装置の種類などの装置確認に基づいて予め装置内のメモリに格納することが可能である。ユーザの購入後、取得する場合は、装置と認証局あるいはその他の管理局との所定のシーケンスに従った装置種類や利用可能なコンテンツの種類等の確認処理を行って、各装置に対して発行し装置内のメモリに格納する構成としてもよい。

[0088] なお、メモリカード31の保護領域に対するアクセスを行うサーバは、ホスト証明書と同様の構成を持つサーバ公開鍵とメモリカードのアクセス許容情報が記録されたサーバ証明書（S e v e r C e r t）を保持する。

[0089] 図4に認証局が各ホスト機器（ユーザ機器）に提供するホスト証明書（H o s t C e r t）の具体例を示す。

ホスト証明書（H o s t C e r t）には、図4に示すように、以下のデータが含まれる。

- (1) タイプ情報
- (2) ホストID（ユーザ機器ID）
- (3) ホスト公開鍵（H o s t P u b l i c K e y）
- (4) 保護領域アクセス権情報（メディアの保護領域に対する読み取り／書き込み制限情報（P A D R e a d／P A D W r i t e））
- (5) その他の情報
- (6) 署名（S i g n a u r e）

[0090] 以下、上記（1）～（6）の各データについて説明する。

- (1) タイプ情報

タイプ情報は、証明書のタイプやユーザ機器のタイプを示す情報であり、例えば本証明書がホスト証明書であることを示すデータや、機器の種類、例えばPCであるとか、音楽再生プレーヤであるといった機器の種類などを示す情報が記録される。

[0091] (2) ホストID

ホストIDは機器識別情報としての機器IDを記録する領域である。

- (3) ホスト公開鍵（H o s t P u b l i c K e y）

ホスト公開鍵 (Host Public Key) はホスト機器の公開鍵である。ホスト機器 (ユーザ機器) に提供される秘密鍵とともに公開鍵暗号方式に従った鍵ペアを構成する。

- [0092] (4) 保護領域アクセス権情報 (メディアの保護領域に対する読み取り／書き込み制限情報 (PAD Read/PAD Write))

保護領域アクセス権情報は、コンテンツを記録するメディア、例えば図3に示すメモリカード31の記憶領域中に設定される保護領域 (PDA: Protected Area) 51内のデータ読み取り (Read) や、書き込み (Write) が許容されたブロック (区分領域) 単位の情報が記録される。

アクセス権は、保護領域内のブロック (区分領域) 単位のアクセス権として記録される。

- [0093] (5) その他の情報、(6) 署名 (Signature)

ホスト証明書には、上記 (1) ~ (4) の他、様々な情報が記録され、(1) ~ (5) の情報に対する署名データが記録される。

署名は、認証局の秘密鍵によって実行される。ホスト証明書に記録された情報、例えばホスト公開鍵を取り出して利用する場合には、まず認証局の公開鍵を適用した署名検証処理を実行して、ホスト証明書の改ざんがないことを確認し、その確認がなされたことを条件として、ホスト公開鍵等の証明書格納データの利用が行われることになる。

- [0094] 図4は、メモリカードの保護領域に対するユーザ機器 (ホスト機器) のアクセス許容情報を記録したホスト証明書であるが、例えばメモリカードにコンテンツを提供するコンテンツ提供サーバなど、保護領域に対するアクセスが必要となるサーバに対しては、図4に示すホスト証明書と同様、メモリカードの保護領域に対するアクセス許容情報を記録した証明書 [サーバ証明書 (例えばサーバ公開鍵を格納した公開鍵証明書)] が提供される。

- [0095] サーバに提供されるサーバ証明書 (Server Cert) の構成例について図5を参照して説明する。なお、以下ではサーバは、図1に示すコン

テンツ提供装置のすべて、すなわち放送局 11 やコンテンツサーバ 12 等、ユーザ装置に対してコンテンツを提供する装置を含むものとして説明する。

[0096] サーバ証明書 (Server Cert) は、例えば、公開鍵証明書発行主体である認証局によって例えば、コンテンツ提供を行うコンテンツサーバ等の装置に提供される。例えば、サーバ証明書 (Server Cert) は、認証局がコンテンツ提供処理を認めたサーバに対して発行するサーバの証明書であり、サーバ公開鍵等を格納した証明書である。サーバ証明書 (Server Cert) は、認証局秘密鍵によって署名が設定され、改ざんの防止されたデータとして構成される。

[0097] 図 5 に認証局が各コンテンツサーバに提供するサーバ証明書 (Server Cert) の具体例を示す。

サーバ証明書 (Server Certificate) には、図 5 に示すように、図 4 を参照して説明したホスト証明書と同様、以下のデータが含まれる。

- (1) タイプ情報
- (2) サーバ ID
- (3) サーバ公開鍵 (Server Public Key)
- (4) メディアに対する読み取り／書き込み制限情報 (PAD Read / PAD Write)
- (5) その他の情報
- (6) 署名 (Signature)

[0098] これらの各情報は、図 4 を参照して説明した情報と同様の情報であり、詳細な説明は省略する。

なお、「(4) メディアに対する読み取り／書き込み制限情報 (PAD Read / PAD Write)」

は、各サーバ単位で、メモリカード 31 の保護領域 51 のブロック (区分領域) 単位のアクセス権 (データ読み取り (Read) / 書き込み (Write) 許容情報) が記録される。

[0099] なお、サーバ証明書に記録された情報、例えばサーバ公開鍵を取り出して利用する場合には、まず認証局の公開鍵を適用した署名検証処理を実行して、サーバ証明書の改ざんがないことを確認し、その確認がなされたことを条件として、サーバ公開鍵等の証明書格納データの利用が行われることになる。

[0100] [4. 各装置の証明書を適用したメモリカードに対するアクセス処理例について]

図4、図5を参照して説明したように、サーバやホスト機器（記録再生器等のユーザ機器）がメモリカード31の保護領域（Protected Area）51のブロックに対してアクセスを行う場合には、図4や図5に示すような証明書をメモリカードに提示することが必要となる。

メモリカードは、図4や図5に示す証明書を確認して、図3に示すメモリカード31の保護領域（Protected Area）51の各ブロック単位のアクセス可否を判定する。

[0101] ホスト機器は、例えば図4を参照して説明したホスト証明書（Host Certificate）を保持し、コンテンツの提供等を行うサーバは、図5を参照して説明したサーバ証明書（Server Certificate）を保持している。

[0102] これらの各装置が、メモリカードの保護領域（Protected Area）に対するアクセスを行う場合には、各装置が保有している証明書をメモリカードに提供してメモリカード側の検証に基づくアクセス可否の判定を受けることが必要となる。

[0103] 図6を参照して、メモリカードに対するアクセス要求装置がサーバである場合と、記録再生装置等のホスト機器である場合のアクセス制限の設定例について説明する。

[0104] 図6には、左から、メモリカードに対するアクセス要求装置であるサーバA61、サーバB62、ホスト機器63、メモリカード70を示している。

サーバA61、サーバB62は、例えば、メモリカード70に対する記録

コンテンツである暗号化コンテンツ（Con 1, Con 2, Con 3 . . . ）を提供する。

これらのサーバは、さらに、暗号化コンテンツの復号用に鍵であるタイトルキー（K t 1, K t 2 . . . ）、コンテンツに対応する利用制御情報（U s a g e R u l e : U R 1, U R 2 . . . ）を提供する。

[0105] ホスト機器63は、メモリカード70に格納されたコンテンツの再生処理を行う装置である。

ホスト機器63は、メモリカード70の汎用領域（General Purpose Area）90に記録された暗号化コンテンツ（Con 1, Con 2, Con 3 . . . ）と利用制御情報（Usage Rule : U R 1, U R 2 . . . ）を読み取る。さらに、保護領域（Protected Area）80のブロック（区分領域）81, 82からコンテンツ復号処理に適用するタイトルキー（K t 1, K t 2 . . . ）を読み取って、タイトルキーによる復号処理を実行して利用制御情報（Usage Rule）に従ったコンテンツ利用を行う。

[0106] メモリカード70は、保護領域（Protected Area）80と、汎用領域（General Purpose Area）90を有し、暗号化コンテンツ、利用制御情報（Usage Rule）等は汎用領域（General Purpose Area）90に記録される。

コンテンツ再生に際して必要とする鍵であるタイトルキーは保護領域（Protected Area）80に記録される。

[0107] 先に図3を参照して説明したように、保護領域（Protected Area）80は、複数のブロック（区分領域）に区分されている。

図6に示す例では、

ブロック#0（Protected Area#0）81、

ブロック#1（Protected Area#1）82、

これらの2つのブロックのみを示している。

保護領域（Protected Area）80には、この他にも多数の

ブロックが設定される。

[0108] ブロックの設定態様としては様々な設定が可能である。

図6に示す例では、

ブロック#0 (Protected Area#0) 81は、サーバA 61専用のブロック、すなわち、サーバA 61の提供コンテンツの復号用のタイトルキーを格納する領域としている。

ブロック#1 (Protected Area#1) 82は、サーバB 62専用のブロック、すなわち、サーバB 62の提供コンテンツの復号用のタイトルキーを格納する領域としている。

[0109] このような設定において、例えばコンテンツの提供サーバA 61は、提供コンテンツの復号に必要となるタイトルキーを、ブロック#0 (Protected Area#0) 81に記録する。

この場合、サーバA 61のサーバ証明書 (Server Certificate) に記録される書き込み許容領域情報 (PAD Write) は、ブロック#0 (Protected Area#0) に対する書き込み (Write) 許可が設定された証明書として構成される。

なお、図に示す例では、書き込み (Write) の許容されたブロックに対しては、読み取り (Read) についても許容された設定として示している。

[0110] またサーバB 62は、提供コンテンツの復号に必要となるタイトルキーを、ブロック#1 (Protected Area#1) 82に記録する。

この場合、サーバB 62のサーバ証明書 (Server Certificate) に記録される書き込み許容領域情報 (PAD Write) は、ブロック#1 (Protected Area#1) 82に対する書き込み (Write) 許可が設定された証明書として構成される。

[0111] また、ブロック#0, #1に記録されたタイトルキーを読み取ってコンテンツ再生を実行する再生装置であるホスト機器63の保持するホスト証明書 (Host Certificate) は、ブロック#0, #1に対する読

み取り (Read) 許可が設定された証明書として構成される。

[0112] この例では、ホスト証明書 (Host Certificate) には、ブロック # 0, # 1 に対する書き込み (Write) 許可は設定されない。

ただし、コンテンツ削除時に、削除コンテンツに対応するタイトルキーの削除が可能な設定とするため、削除処理については許可する設定としてもよい。

また、その他の処理において、ホスト機器 63 が保護領域に対するデータ書き込みが必要となる場合は、ホスト証明書 (Host Certificate) に書き込み (Write) 許可を設定してもよい。

[0113] メモリカード 70 のデータ処理部は、コンテンツを提供するサーバや、コンテンツを利用するホストなどのアクセス要求装置から保護領域 (Protected Area) 80 に対するアクセス要求を受信すると、各装置の装置証明書を参照して、各ブロック単位のアクセス許容情報を確認して各ブロックに対するアクセスを許可するか否かを判定する。

[0114] メモリカード 70 は、アクセス要求装置からのデータ書き込みや読み取り要求の入力に応じて、書き込みあるいは読み取り要求データの種別を判別し、データ書き込み先あるいは読み取り先としてのブロック (# 0, # 1, # 2 . . .) を選別する。

[0115] アクセス制御情報は、図 4、図 5 を参照して説明したように、各アクセス要求装置の証明書 (サーバ証明書、ホスト証明書など) に記録され、メモリカードは、アクセス要求装置から受領した証明書について、まず署名検証を行い、証明書の正当性を確認した後、証明書に記載されたアクセス制御情報、すなわち、以下の情報を読み取る。

読み取り許容領域情報 (PAD Read)、

書き込み許容領域情報 (PAD Write)、

これらの情報に基づいて、アクセス要求装置に対して認められた処理のみを許容して実行する。

[0116] [5. 暗号化コンテンツ署名 (ECS) 発行装置を利用したコンテンツ

提供システムについて]

先に図1を参照して説明したように、ユーザ装置に提供されるコンテンツはコンテンツ提供装置から提供される。しかし、このコンテンツ提供装置自身が、不正なコピーコンテンツを配信する場合もある。以下では、このようなサーバの不正処理など、ユーザ装置以外の構成による不正についても防止可能とした構成について説明する。

[0117] 図7を参照して、コンテンツの不正利用を防止するための本開示の情報処理システムの全体構成について説明する。

図7には、情報処理システムの全体構成例を示している。図7には以下の4種類の装置を階層構成として示している。

(A) ライセンス発行装置 (L A) 101

(B) 暗号化コンテンツ署名 (E C S) 発行装置 (E n c r y p t e d C o n t e n t S i g n a t u r e I s s u e r) 102-1~n

(C) コンテンツ提供装置 (C o n t e n t S e r v e r) 103-1~m

(D) ユーザ装置 (コンテンツ再生装置) 104-1~f

[0118] 図7に示す (C) コンテンツ提供装置 (C o n t e n t S e r v e r) 103-1~mは、図1に示す放送局11、コンテンツサーバ12等に対応する。

また、図7に示す (D) ユーザ装置 (コンテンツ再生装置) 104-1~fは、図1に示す記録再生専用器21、PC22、携帯端末23等のユーザ装置に対応する。

[0119] (C) コンテンツ提供装置 (C o n t e n t S e r v e r) 103-1~mは、コンテンツサーバや放送局、さらにはコンテンツを格納したディスク等のメディアを提供するメディア提供会社などコンテンツを送信する装置や、メディアに対するコンテンツ記録を実行する装置など、様々な情報処理装置を含む。これらは多数存在する。

[0120] (D) ユーザ装置 (コンテンツ再生装置) 104-1~fは、コンテンツ

提供装置 (Content Server) 103-1~mからコンテンツ、例えば映画、音楽、その他の様々なコンテンツをインターネットや放送波、あるいはディスク等のメディアを介して受信、または読み出して再生処理を実行する装置である。具体的にはPC、携帯端末、DVDプレーヤ、BDプレーヤ、テレビなどコンテンツ再生可能な様々な種類の情報処理装置が含まれる。

[0121] (B) 暗号化コンテンツ署名 (ECS) 発行装置 (Encrypted Content Signature Issuer) 102-1~nは、(C) コンテンツ提供装置 (Content Server) 103-1~mの提供するコンテンツに対応する暗号化コンテンツ署名ファイル (ECSファイル: Encrypted Content Signature File) を生成する。

[0122] (C) コンテンツ提供装置 (Content Server) 103-1~mは、例えば、新たな映画コンテンツなどのコンテンツをユーザ装置104に提供する場合、そのコンテンツに対応する暗号化コンテンツ署名ファイル (ECSファイル) の生成依頼を、暗号化コンテンツ署名 (ECS) 発行装置 (Encrypted Content Signature Issuer) 102に対して行う。

[0123] (B) 暗号化コンテンツ署名 (ECS) 発行装置 (Encrypted Content Signature Issuer) 102-1~nは、この依頼に応じて、暗号化コンテンツ署名ファイル (ECSファイル) を生成して、(C) コンテンツ提供装置 (Content Server) 103に提供する。

なお、この暗号化コンテンツ署名ファイル (ECSファイル) の具体的な構成と生成処理については後段で詳細に説明する。

[0124] (C) コンテンツ提供装置 (Content Server) 103は、(B) 暗号化コンテンツ署名 (ECS) 発行装置 (Encrypted Content Signature Issuer) 102から暗号化コン

テンツ署名ファイル（ＥＣＳファイル）を受領し、これを、暗号化コンテンツに併せて（Ｄ）ユーザ装置（コンテンツ再生装置）１０４に提供する。

[0125] （Ｄ）ユーザ装置（コンテンツ再生装置）１０４は、コンテンツの再生を行う前に、暗号化コンテンツ署名ファイル（ＥＣＳファイル）の署名検証処理を行い、この署名検証処理の成立が確認された場合にのみ、コンテンツの復号、再生が許容される。

なお、ユーザ装置（コンテンツ再生装置）１０４には、暗号化コンテンツ署名ファイル（ＥＣＳファイル）の署名検証を条件としてコンテンツの復号、再生を実行するシーケンスに従った再生処理プログラムが格納されており、この再生処理プログラムに従って暗号化コンテンツ署名ファイル（ＥＣＳファイル）の署名検証等のコンテンツ再生可否判定処理と、コンテンツ再生が実行されることになる。

例えば、暗号化コンテンツ署名ファイル（ＥＣＳファイル）の署名検証が成功しなかった場合は、コンテンツの再生は禁止される。

[0126] （Ａ）ライセンス発行装置（ＬＡ）１０１は、（Ｂ）暗号化コンテンツ署名（ＥＣＳ）発行装置（Ｅｎｃｒｙｐｔｅｄ Ｃｏｎｔｅｎｔ Ｓｉｇｎａｔｕｒｅ Ｉｓｓｕｅｒ）１０２－１～ｎに対して、ＥＣＳファイルの発行許可証としてのライセンスを提供する。

[0127] （Ａ）ライセンス発行装置（ＬＡ）１０１は、予め既定したライセンス発行シーケンスにしたがって、（Ｂ）暗号化コンテンツ署名（ＥＣＳ）発行装置（Ｅｎｃｒｙｐｔｅｄ Ｃｏｎｔｅｎｔ Ｓｉｇｎａｔｕｒｅ Ｉｓｓｕｅｒ）１０２－１～ｎの正当性を確認し、正当であると確認された場合に、暗号化コンテンツ署名（ＥＣＳ）発行装置に対して、ライセンスを発行する。

[0128] なお、ライセンスは、具体的には、例えばライセンス発行装置（ＬＡ）１０１の秘密鍵による署名が付与された公開鍵証明書である。公開鍵証明書には、暗号化コンテンツ署名（ＥＣＳ）発行装置（Ｅｎｃｒｙｐｔｅｄ Ｃｏｎｔｅｎｔ Ｓｉｇｎａｔｕｒｅ Ｉｓｓｕｅｒ）１０２の公開鍵が格納さ

れる。なお、この公開鍵証明書に格納される公開鍵に対応する秘密鍵も併せて (A) ライセンス発行装置 (L A) 101 から、暗号化コンテンツ署名 (E C S) 発行装置 (E n c r y p t e d C o n t e n t S i g n a t u r e I s s u e r) 102 に提供される。

[0129] 次に、図8を参照して、

(A) ライセンス発行装置 (L A) 101、
(B) 暗号化コンテンツ署名 (E C S) 発行装置 (E n c r y p t e d C o n t e n t S i g n a t u r e I s s u e r) 102、
(C) コンテンツ提供装置 (C o n t e n t S e r v e r) 103、
これらの3者間で実行される処理について説明する。

[0130] 図8には、

(A) ライセンス発行装置 (L A) 101、
(B) 暗号化コンテンツ署名 (E C S) 発行装置 (E n c r y p t e d C o n t e n t S i g n a t u r e I s s u e r) 102、
(C) コンテンツ提供装置 (C o n t e n t S e r v e r) 103、
これらの3つの装置と、各装置において実行する代表的な処理を示す図である。

[0131] ライセンス発行装置 (L A) 101の実行する処理は、処理 (A 1)、(A 2)

として示している。

ライセンス発行装置 (L A) 101は以下の処理を実行する。

処理 (A 1) 暗号化コンテンツ署名 (E C S) 発行装置102に対して、使用期限 (E x p i r a t i o n D a t e) 付のE C S発行装置証明書 (E C S I s s u e r C e r t i f i c a t e) を提供する。

処理 (A 2) コンテンツ提供装置103に対して、E C S発行装置証明書リボケーションリスト (E C S I s s u e r K e y R e v o c a t i o n L i s t) を提供する。

[0132] 暗号化コンテンツ署名 (E C S) 発行装置102の実行する処理は、処理

(B1)、(B2)

として示している。

暗号化コンテンツ署名(ECS)発行装置102は以下の処理を実行する。

処理(B1)暗号化コンテンツ署名ファイル(ECSファイル: Encrypted Content Signature File)を生成、

処理(B2)コンテンツ提供装置103に対して、暗号化コンテンツ署名ファイル(ECSファイル: Encrypted Content Signature File)を提供、

[0133] コンテンツ提供装置103の実行する処理は、処理(C1)、(C2)として示している。

コンテンツ提供装置103は以下の処理を実行する。

処理(C1)暗号化コンテンツ署名(ECS)発行装置102に対して、ECSファイル生成用データを提供する。例えば、コンテンツハッシュリスト集合、タイトルキーのハッシュ値、ブロック識別子等を提供する。

処理(C2)ECSファイルを利用したコンテンツ提供可否判定処理、

[0134] [6. ECSファイルの構成例について]

次に、暗号化コンテンツ署名(ECS)発行装置102の生成するECSファイルの構成例について説明する。

図9にECSファイルと、ECSファイルの構成データとしても設定されるECS発行装置証明書のデータ構成例を示す。

ECSファイルは、暗号化コンテンツ署名(ECS)発行装置102において生成するファイルであり、コンテンツ提供装置103から受領するコンテンツハッシュリスト集合、タイトルキーのハッシュ値、ブロック識別子等を構成データとして格納したファイルである。

[0135] 図9(A)に示すように、ECSファイルは、

(1) コンテンツハッシュリスト集合(Hash List Collections)

(2) ECS発行日時 (ECS Issue Date)

(3) ブロック識別子 (PAD Block Number)

(4) ECS発行装置署名 (Signature by ECS Issuer)

(5) ECS発行装置証明書 (ECS Issuer Certificate)

(6) コンテンツブロックテーブル (Stored Content Block Table)

これらのデータを含むファイルである。

[0136] (1) コンテンツハッシュリスト集合 (Hash List Collections) は、コンテンツ提供装置 (Content Server) 103が生成して、暗号化コンテンツ署名 (ECS) 発行装置102が受領するデータである。ユーザ装置に提供するコンテンツ、具体的にはユーザ装置において再生される例えば映画等のコンテンツに基づいて生成されるコンテンツの構成データに基づいて生成されるハッシュ値とその属性情報 (ハッシュ値生成元のコンテンツブロックの位置等を示すオフセット、レングスなどの情報) を含むデータである。

[0137] (2) ECS発行日時 (ECS Issue Date) は、暗号化コンテンツ署名 (ECS) 発行装置102においてECSファイルを生成した日時情報である。

この日時情報は、例えば、(4) ECS発行装置署名 (ECS Signature) の生成日時に対応する。

[0138] (3) ブロック識別子 (PAD Block Number) は、コンテンツ提供装置 (Content Server) 103から、暗号化コンテンツ署名 (ECS) 発行装置102に通知されるデータであり、コンテンツ提供装置103がユーザ装置104に対して提供したコンテンツに対応する暗号鍵であるタイトルキーを格納したメディアの保護領域のブロックの識別子である。これは、コンテンツ提供装置103が利用可能なメディアの保護

領域におけるブロックの識別子である。

先に、図3、図6等を参照して説明したように、コンテンツ提供装置の利用可能なメディアの保護領域のブロックは予め設定されており、これらのアクセス許容ブロック情報が記録される。

[0139] (4) ECS発行装置署名 (ECS Signature)

ECS発行装置署名 (ECS Signature) は、ECS発行装置の電子署名である。

署名対象データは、コンテンツハッシュリスト集合、ECS発行日時、ブロック識別子、さらに、タイトルキー (ハッシュ値) 等の構成データとなる。

[0140] (5) ECS発行装置証明書 (ECS Issuer Certificate)

ECS発行装置証明書 (ECS Issuer Certificate) は、ECS発行装置102に対応する公開鍵証明書であり、図9 (B) に示すように、ECS発行装置102の公開鍵等が格納されている。この構成については後述する。

[0141] (6) コンテンツブロックテーブル (Stored Content Block Table)

コンテンツブロックテーブル (Stored Content Block Table) は、上記のコンテンツハッシュリスト集合 (Hash List Collections) に、複数のコンテンツに対応するハッシュリストが記録されている場合に、各ハッシュリストとコンテンツの対応情報を記録したフィールドとして設定される。

[0142] 次に、図9 (B) に示すECS発行装置証明書 (ECS Issuer Certificate) のデータ構成について説明する。

ECS発行装置証明書 (ECS Issuer Certificate) は、ライセンス発行装置 (LA) 101が生成し、ECS発行装置102に提供される。ECS発行装置102は、ECS発行装置証明書 (ECS

I s s u e r C e r t i f i c a t e) の生成に必要となるデータをライセンス発行装置 (L A) 1 0 1 に提供して、E C S 発行装置証明書 (E C S I s s u e r C e r t i f i c a t e) の生成を依頼する。

[0143] ライセンス発行装置 (L A) 1 0 1 は、この依頼に応じて E C S 発行装置証明書 (E C S I s s u e r C e r t i f i c a t e) を生成する。

図 9 (B) に示すように、E C S 発行装置証明書は、

- (1) E C S 証明書識別子 (E C S C e r t i f i c a t e I D)
- (2) ブロック識別子開始番号 (S t a r t P A D B l o c k N u m b e r)
- (3) ブロック識別子範囲 (P A D B l o c k N u m b e r C o u n t e r)
- (4) 発行装置証明書使用期限 (E x p i r a t i o n D a t e)
- (5) E C S 発行装置公開鍵 (E C S I s s u e r P u b l i c K e y)
- (6) L A 署名 (S i g n a t u r e b y L A)

これらのデータを含むファイルである。

[0144] (1) E C S 証明書識別子 (E C S C e r t i f i c a t e I D) は、この E C S 証明書の識別子である。

(2) ブロック識別子開始番号 (S t a r t P A D B l o c k N u m b e r) は、E C S 発行装置 1 0 2 が、コンテンツ提供装置 1 0 3 に対して許容可能なメディアの保護領域のアクセス許容ブロックの開始番号である。

(3) ブロック識別子範囲 (P A D B l o c k N u m b e r C o u n t e r) は、E C S 発行装置 1 0 2 が、コンテンツ提供装置 1 0 3 に対して許容可能なメディアの保護領域のアクセス許容ブロックの開始番号からの範囲を示す情報である。

[0145] (4) 発行装置証明書使用期限 (E x p i r a t i o n D a t e) は、この発行装置証明書の使用期限情報である。

(5) ECS発行装置公開鍵 (ECS Issuer Public Key) は、ECS発行装置の公開鍵である。

(6) LA署名 (Signature by LA) は、図7、図8に示すライセンス発行装置 (LA) の電子署名である。ECS発行装置証明書の上記構成データ (1) ~ (5) に基づいて生成される電子署名である。

[0146] 図10は、ECSファイルのシンタックス、
図11は、ECS発行装置証明書のシンタックス、
を示す図である。

なお、ECS発行装置証明書に記録される、

(2) ブロック識別子開始番号 (Start PAD Block Number)

(3) ブロック識別子範囲 (PAD Block Number Counter)

これらの2つのデータは、前述したように、ECS発行装置102が、コンテンツ提供装置103に対して許容可能なメディアの保護領域のアクセス許容ブロックを示す情報である。

具体的には、例えば、

ブロック識別子開始番号 $\leq N \leq$ ブロック識別子開始番号 + ブロック識別子範囲

を満たす、すべてをブロック識別子として設定したのと同等である。

[0147] また、

ブロック識別子開始番号 = 0 x F F F F F F F F

と設定されていた場合は、

メディアの保護領域の全ブロックがアクセス許容ブロックであることを示す。

[0148] なお、図9~図11を参照して説明した例は、ECSファイルがECS発行装置証明書を含む構成として説明したが、ECSファイルにECS発行装置証明書を含めず、ECSファイルと、ECS発行装置証明書を個別のファ

イルとして構成してもよい。

[0149] [7. E C S 発行装置証明書リボケーションリストの構成について]

次に、図 1 2 を参照して、E C S 発行装置証明書リボケーションリストの構成について説明する。

[0150] E C S 発行装置証明書リボケーションリスト (E C S I s s u e r K e y R e v o c a t i o n L i s t) は、先に図 8 を参照して説明したように、ライセンス発行装置 (L A) 1 0 1 が発行するリストである。このリストは、例えばコンテンツ提供装置 1 0 3 において利用される。

[0151] ライセンス発行装置 (L A) 1 0 1 は、不正であると判定された E C S 発行装置の公開鍵を格納した E C S 発行装置証明書 (図 9 (B) 参照) を無効化し、無効化した E C S 発行装置 (具体的には、E C S 発行装置証明書) の識別子 (I D) を登録したリストとして、E C S 発行装置証明書リボケーションリストを生成する。

図 1 2 に示すように、E C S 発行装置証明書リボケーションリストは、以下のデータを格納している。

- (1) バージョン (V e r s i o n)
- (2) エントリ数 (N u m b e r o f e n t r i e s)
- (3) リボーク (無効化) された E C S 発行装置証明書の I D
- (4) リボーク (無効化) された E C S 発行装置証明書のリボーク日時
- (5) ライセンス発行装置 (L A) 1 0 1 の電子署名

これらのデータを格納している。

[0152] (5) ライセンス発行装置 (L A) 1 0 1 の電子署名は (1) ~ (4) のデータに対する署名である。

なお、E C S 発行装置証明書リボケーションリストは、不正な E C S 発行装置が新たに発見された場合には、その E C S 発行装置の I D を追加して更新した新しいバージョンのリストが逐次、発行され、コンテンツ提供装置 1 0 3 に提供される。

[0153] [8. 暗号化コンテンツ署名ファイル (E C S ファイル) の生成処理に

ついて]

次に、図 1 3 を参照して暗号化コンテンツ署名ファイル（ECS ファイル）の生成処理について説明する。

[0154] 暗号化コンテンツ署名ファイル（ECS ファイル）は、コンテンツ提供装置（Content Server）103 からの生成依頼に基づいて、暗号化コンテンツ署名（ECS）発行装置（Encrypted Content Signature Issuer）102 が生成する。

[0155] コンテンツ提供装置（Content Server）103 が、例えば、新たな映画コンテンツなどのコンテンツをユーザ装置 104 に提供する場合、そのコンテンツに対応する暗号化コンテンツ署名ファイル（ECS ファイル）の生成依頼を、暗号化コンテンツ署名（ECS）発行装置（Encrypted Content Signature Issuer）102 に対して行う。

[0156] 暗号化コンテンツ署名（ECS）発行装置（Encrypted Content Signature Issuer）102 は、この依頼に応じて、暗号化コンテンツ署名ファイル（ECS ファイル）を生成して、コンテンツ提供装置（Content Server）103 に提供する。

[0157] 図 1 3 は、この暗号化コンテンツ署名ファイル（ECS ファイル）の生成処理において、コンテンツ提供装置（Content Server）103 と暗号化コンテンツ署名（ECS）発行装置（Encrypted Content Signature Issuer）102 の実行する処理を説明する図である。

[0158] コンテンツ提供装置（Content Server）103 は、新たな暗号化コンテンツ署名ファイル（ECS ファイル）の生成依頼を行う場合、図 1 3 に示すように、

コンテンツ 181 の構成データ（コンテンツブロック）に基づいて生成したハッシュ値を含むコンテンツハッシュリスト集合（Hash List Collections）183 を生成する。

[0159] なお、コンテンツハッシュリスト集合 (Hash List Collections) 183は、ユーザ装置104に提供する暗号化コンテンツの構成データ (コンテンツブロック) に基づいて生成したハッシュ値を格納したコンテンツハッシュリスト集合として生成される。

[0160] コンテンツ提供装置 (Content Server) 103は、生成したコンテンツハッシュリスト集合 (Hash List Collections) 183を暗号化コンテンツ署名 (ECS) 発行装置 (Encrypted Content Signature Issuer) 102に提供する。

[0161] さらに、コンテンツ181の暗号化に適用する暗号鍵であるタイトルキー182、またはタイトルキーのハッシュ値も暗号化コンテンツ署名 (ECS) 発行装置 (Encrypted Content Signature Issuer) 102に提供する。

[0162] コンテンツハッシュリスト集合 (Hash List Collections) 183は、ユーザ装置に提供するコンテンツ、具体的にはユーザ装置において再生される例えば映画等のコンテンツに基づいて生成されるコンテンツの構成データに基づいて生成されるハッシュ値とその属性情報を含むデータである。

なお、属性情報には、例えばハッシュ値を算出したコンテンツブロックの位置情報等の属性情報などが含まれる。

[0163] 暗号化コンテンツ署名 (ECS) 発行装置 (Encrypted Content Signature Issuer) 102は、図13に示すステップS11において、コンテンツ提供装置 (Content Server) 103から受信したデータと、ECSファイルの構成データ、具体的には、例えば、

コンテンツハッシュリスト集合、

ECS発行日時、

ブロック識別子、

タイトルキー（ハッシュ）、

これらのデータに対する署名を生成する。

[0164] 署名データの生成は、暗号化コンテンツ署名（ECS）発行装置（Encrypted Content Signature Issuer）102の保持する秘密鍵を適用して署名を生成する。例えばECDSAアルゴリズムに従った署名生成を行う。

[0165] 生成した署名は、図13に示すように、暗号化コンテンツ署名ファイル（ECSファイル）の構成データとして設定される。

先に図9を参照して説明したように、暗号化コンテンツ署名（ECS）発行装置（Encrypted Content Signature Issuer）102の生成する暗号化コンテンツ署名ファイル（ECSファイル）200は、以下のデータを構成データとして有する。

（1）コンテンツハッシュリスト集合（Hash List Collections）

（2）ECS発行日時（ECS Issue Date）

（3）ブロック識別子（PAD Block Number）

（4）ECS発行装置署名（Signature by ECS Issuer）

（5）ECS発行装置証明書（ECS Issuer Certificate）

（6）コンテンツブロックテーブル（Stored Content Block Table）

これらのデータを含むファイルである。

[0166] [9. ECSファイル、ECS発行装置証明書の日時情報を適用した処理について]

次に、ECSファイル、ECS発行装置証明書の日時情報を適用した処理について説明する。

（1）ECS発行装置102が生成し、コンテンツ提供装置に提供される

ECS ファイル、

(2) ライセンス発行装置 (LA) 101 が生成し、ECS 発行装置 10 に提供される ECS 発行装置証明書、

これらには、図 9 を参照して説明したように、様々な日時情報が記録される。

[0167] 例えば、ECS ファイルには、

ECS 発行日時 (ECS Issue Date)
が記録される。

また、ECS 発行装置証明書には、

発行装置証明書使用期限 (Expiration Date)
が記録される。

[0168] コンテンツ提供装置 103 は、これらの ECS ファイルと ECS 発行装置証明書に記録された日時情報や、先に図 12 を参照して説明した ECS 発行装置証明書リボケーションリストを適用して、ユーザ装置 104 に対するコンテンツ提供処理の可否判定処理を実行する。

[0169] また、コンテンツ提供装置 103 からコンテンツを受領するユーザ装置においても、ECS ファイルと ECS 発行装置証明書に記録された日時情報や、先に図 12 を参照して説明した ECS 発行装置証明書リボケーションリストを適用して、ユーザ装置 104 におけるコンテンツ再生の可否判定処理を実行する。

以下、これらの処理について説明する。

[0170] まず、図 14、図 15 に示すシーケンス図を参照して、暗号化コンテンツ署名ファイル (ECS ファイル) の生成とコンテンツ提供、利用処理シーケンスについて説明する。

図 14 には、左から、

ライセンス発行装置 101、

暗号化コンテンツ署名 (ECS) 発行装置 102、

コンテンツ提供装置 103、

これらの各装置を示し、ステップS 1 1 1、S 1 2 1～S 1 2 8の各処理を時系列処理として示している。

これらの各処理ステップについて説明する。

[0171] ステップS 1 1 1

ステップS 1 1 1は、ライセンス発行装置1 0 1が、暗号化コンテンツ署名(E C S)発行装置1 0 2に対してライセンス(E C S発行装置証明書)を発行する処理である。

[0172] 先に図8他を参照して説明したように、ライセンス発行装置1 0 1は、暗号化コンテンツ署名(E C S)発行装置1 0 2に対して、E C Sファイルの発行許可証としてのライセンス、すなわちE C S発行装置証明書を提供する。

ライセンス発行装置(L A)1 0 1は、予め既定したライセンス発行シーケンスにしたがって、暗号化コンテンツ署名(E C S)発行装置1 0 2の正当性を確認し、正当であると確認された場合に、暗号化コンテンツ署名(E C S)発行装置に対して、E C S発行装置証明書を発行する。

[0173] E C S発行装置証明書は、図9 (B)を参照して説明したデータ構成を有する公開鍵証明書である。E C S発行装置証明書には、暗号化コンテンツ署名(E C S)発行装置(E n c r y p t e d C o n t e n t S i g n a t u r e I s s u e r)1 0 2の公開鍵が格納される。なお、このE C S発行装置証明書に格納される公開鍵に対応する秘密鍵も併せて(A)ライセンス発行装置(L A)1 0 1から、暗号化コンテンツ署名(E C S)発行装置(E n c r y p t e d C o n t e n t S i g n a t u r e I s s u e r)1 0 2に提供される。

[0174] ステップS 1 2 1～S 1 2 4は、図1 3を参照して説明した暗号化コンテンツ署名ファイル(E C Sファイル)の生成処理のシーケンスである。

この処理は、コンテンツ提供装置1 0 3が、例えば新たなコンテンツをユーザ装置に提供する場合に、その新たなコンテンツに対応する暗号化コンテンツ署名ファイル(E C Sファイル)を取得するために、各提供コンテンツ

に応じて逐次実行される。

この処理は、暗号化コンテンツ署名（ECS）発行装置102と、コンテンツ提供装置103との間で実行される。

[0175] まず、ステップS121において、コンテンツ提供装置103は、暗号化コンテンツ署名ファイル（ECSファイル）作成に必要なデータを生成する。

具体的には、図13を参照して説明した、

コンテンツハッシュリスト集合（Hash List Collections）183の生成処理などを実行する。

[0176] 前述したように、コンテンツハッシュリスト集合（Hash List Collections）は、ユーザ装置に提供するコンテンツ、具体的にはユーザ装置において再生される例えば映画等のコンテンツに基づいて生成されるコンテンツの構成データに基づいて生成されるハッシュ値とその属性情報を含むデータである。

属性情報には、例えばハッシュ値を算出したコンテンツブロックの位置情報等の属性情報などが含まれる。

[0177] なお、コンテンツ提供装置103は、コンテンツの暗号化および復号処理に適用するタイトルキー、あるいはタイトルキーのハッシュ値も、暗号化コンテンツ署名（ECS）発行装置102への提供データとして生成する。

[0178] 次に、コンテンツ提供装置103は、ステップS122において、生成データを暗号化コンテンツ署名（ECS）発行装置102に送信して、暗号化コンテンツ署名ファイル（ECSファイル）の生成および送信要求を行う。

[0179] 次に、ステップS123において、暗号化コンテンツ署名（ECS）発行装置102は、コンテンツ提供装置103から受信したデータに対する署名生成処理を行う。

すなわち、図13を参照して説明したステップS11の署名生成処理を実行する。

[0180] さらに、先に図9（A）を説明したデータ構成を持つ暗号化コンテンツ署

名ファイル（ECSファイル）を生成し、ステップS124において、生成した暗号化コンテンツ署名ファイル（ECSファイル）をコンテンツ提供装置103に送信する。

[0181] 先に図9（A）を参照して説明したように、暗号化コンテンツ署名ファイル（ECSファイル）には、

ECSファイルは、

（1）コンテンツハッシュリスト集合（Hash List Collections）

（2）ECS発行日時（ECS Issue Date）

（3）ブロック識別子（PAD Block Number）

（4）ECS発行装置署名（Signature by ECS Issuer）

（5）ECS発行装置証明書（ECS Issuer Certificate）

（6）コンテンツブロックテーブル（Stored Content Block Table）

これらのデータが含まれる。

[0182] 暗号化コンテンツ署名ファイル（ECSファイル）を受信したコンテンツ提供装置103は、ステップS125において、暗号化コンテンツ署名ファイル（ECSファイル）を適用したコンテンツ提供が許容されるか否かのコンテンツ提供可否判定処理を実行する。

ステップS126において、コンテンツ提供が許容されると判定した場合は、ステップS127においてユーザ装置に対するコンテンツ提供処理を実行する。

ステップS126において、コンテンツ提供が許容されないと判定した場合は、ステップS128に進み、コンテンツ提供処理を中止する。

なお、ステップS125～S128の処理については、図16以下を参照して、後段でさらに詳細に説明する。

[0183] 次に、図 15 を参照して、コンテンツ提供装置 103 からユーザ装置 104 に対するコンテンツの提供と、ユーザ装置 104 におけるコンテンツ再生シーケンスについて説明する。

図 15 には、左から、
コンテンツ提供装置 103、
ユーザ装置 104、
これらを示している。

[0184] まず、コンテンツ提供装置 103 は、ステップ S 131 において、ユーザ装置に、

- (1) 暗号化コンテンツ
- (2) 暗号化コンテンツ署名ファイル (ECS ファイル)
- (3) タイトルキー

これらのデータを送信する。

[0185] なお、ステップ S 131 の処理の前処理として、例えばユーザ装置 104 からコンテンツ提供装置 103 に対するコンテンツ送信要求が実行されているものとする。コンテンツ提供装置 103 は、ユーザ装置からのリクエストに応じたコンテンツを提供する。

[0186] なお、ステップ S 131 においてコンテンツ提供装置 103 の送信する、

- (1) 暗号化コンテンツ

は、コンテンツに対応して設定される上記の「(3) タイトルキー」で暗号化されたコンテンツである。

また、

- (2) 暗号化コンテンツ署名ファイル (ECS ファイル)

は、上記の (1) 暗号化コンテンツに対応して生成されたファイルであり、先に図 9 を参照して説明した暗号化コンテンツ署名ファイル (ECS ファイル) の構成データを格納している。

[0187] ユーザ装置 104 は、これらのデータを受信し、例えばハードディスク等のメディアに格納する。

その後、コンテンツの再生処理を実行する際に、図 15 に示すステップ S 132 以下の処理を実行する。

- [0188] ユーザ装置 104 は、ステップ S 132 において、再生対象コンテンツに対応する暗号化コンテンツ署名ファイル（ECS ファイル）を読み出して、暗号化コンテンツ署名ファイル（ECS ファイル）を適用してコンテンツ再生が許容されるか否かのコンテンツ再生可否判定処理を実行する。

ステップ S 133 において、コンテンツ再生が許容されると判定した場合は、ステップ S 134 においてコンテンツ再生処理を実行する。

ステップ S 133 において、コンテンツ再生が許容されないと判定した場合は、ステップ S 135 に進み、コンテンツ再生処理を中止する。

なお、ステップ S 132～S 135 の処理については、図 18 を参照して、後段でさらに詳細に説明する。

- [0189] 次に、図 14 を参照して説明したコンテンツ提供装置におけるステップ S 125 | S 128 の処理、すなわち、暗号化コンテンツ署名ファイル（ECS ファイル）を適用したコンテンツ提供可否判定処理の詳細シーケンスについて図 16、図 17 に示すフローチャートを参照して説明する。

- [0190] 図 16 に示すフローチャートのステップ S 151 の前処理として、コンテンツ提供装置は、暗号化コンテンツ署名ファイル（ECS ファイル）発行装置から受信した暗号化コンテンツ署名ファイル（ECS ファイル）に設定された ECS 発行装置署名を適用した署名検証を実行する。

この署名検証が成立し、暗号化コンテンツ署名ファイル（ECS ファイル）の正当性が確認され場合は、さらに、暗号化コンテンツ署名ファイル（ECS ファイル）に格納された ECS 発行装置証明書の署名検証を実行する。これらの 2 つの署名検証が成立したことを条件としてステップ S 151 以下の処理を行う。

- [0191] 上記 2 つの署名検証の少なくともいずれかが成立しなかった場合は、暗号化コンテンツ署名ファイル（ECS ファイル）または ECS 発行装置証明書の正当性が確認されないため、ステップ S 151 以下の処理は実行されない

。この場合はコンテンツ提供処理も実行しないことになる。

[0192] 暗号化コンテンツ署名ファイル（ECSファイル）と、ECS発行装置証明書の2つの署名検証が成立し、暗号化コンテンツ署名ファイル（ECSファイル）とECS発行装置証明書の正当性が確認された場合、コンテンツ提供装置は、ステップS151の処理を実行する。

[0193] コンテンツ提供装置は、

暗号化コンテンツ署名ファイル（ECSファイル）の記録データであるECS発行日時（ECS Issue Date）を読み出す。さらに、

ECS発行装置証明書の記録データであるECS発行装置証明書使用期限（Expiration Date）を読み出す。

さらに、これらの日時情報を比較し、

ECS発行装置証明書使用期限（Expiration Date）がECS発行日時（ECS Issue Date）より前であるか否かを判定する。

ECS発行装置証明書使用期限（Expiration Date）がECS発行日時（ECS Issue Date）より前である場合（Yes）は、ステップS156に進み、暗号化コンテンツの配布を停止する。

[0194] 前でない場合（No）は、ステップS152に進み、ステップS153以下において暗号化コンテンツ署名ファイル（ECSファイル）とECS発行装置証明書に記録された日時情報（タイムスタンプ）を適用したコンテンツ提供可否判定処理を開始する。

[0195] ステップS153では、ECS発行装置証明書使用期限（Expiration Date）と、コンテンツ提供装置の持つ時間クロックあるいは信頼できる時間情報提供サーバから取得した実時間とを比較する。

ECS発行装置証明書使用期限（Expiration Date）が、実時間より1日以上前であれば、ステップS156に進み、コンテンツ提供処理を中止する。

[0196] 一方、ECS発行装置証明書使用期限（Expiration Date

）が、実時間より１日以上前でなければ、ステップＳ１５４に進む。

ステップＳ１５４では、ＥＣＳ発行日時（ＥＣＳ Issue Date）と、コンテンツ提供装置の持つ時間クロックあるいは信頼できる時間情報提供サーバから取得した実時間とを比較する。

ＥＣＳ発行日時（ＥＣＳ Issue Date）が、実時間より１日以上前であれば、ステップＳ１５６に進み、コンテンツ提供処理を中止する。

[0197] 一方、ＥＣＳ発行日時（ＥＣＳ Issue Date）が、実時間より１日以上前でなければ、ステップＳ１５５に進む。

[0198] 次に、ステップＳ１５５以下において実行するリボケーションリストを適用したコンテンツ提供可否判定処理について、図１７に示すフローチャートを参照して説明する。

なお、コンテンツ提供装置は、予め図１２を参照して説明したＥＣＳ発行装置公開鍵リボケーションリストを取得しているものとする。例えばライセンス発行装置（ＬＡ）１０１から取得可能である。

[0199] コンテンツ提供装置は、ステップＳ１６１において、ＥＣＳ発行装置証明書からＥＣＳ証明書識別子を取得し、この識別子（ＩＤ）がＥＣＳ発行装置公開鍵リボケーションリストに登録されているか否かを判定する。

登録されていない場合（Ｎｏ）は、ＥＣＳ発行装置証明書は無効化（リボーク）されておらず有効であることが確認され、この場合は、ステップＳ１６４に進み、コンテンツ提供処理を実行する。

[0200] 一方、ステップＳ１６１において、ＥＣＳ証明書識別子（ＩＤ）がＥＣＳ発行装置公開鍵リボケーションリストに登録されていると判定した場合（Ｙｅｓ）、この場合は、ステップＳ１６２に進む。

[0201] ステップＳ１６２では、ＥＣＳ発行装置公開鍵リボケーションリストに登録されているそのＥＣＳ発行装置証明書が無効化（リボーク）された日時、すなわち、

リボーク日時と、

暗号化コンテンツ署名ファイル（ＥＣＳファイル）の記録データであるＥ

CS発行日時 (ECS Issue Date) と、

これらの2つの日時データを比較する。

- [0202] 暗号化コンテンツ署名ファイル (ECSファイル) の記録データであるECS発行日時 (ECS Issue Date) がリボーク日時より前である場合 (Yes) は、ステップS164に進み、コンテンツの提供処理を実行する。

これは、リボーク以前の正当なECS発行装置証明書に基づく処理であると判断できるためである。

- [0203] 一方、ステップS162において、暗号化コンテンツ署名ファイル (ECSファイル) の記録データであるECS発行日時 (ECS Issue Date) がリボーク日時より前でない場合 (No) は、ステップS163に進み、コンテンツの提供処理を停止する。

これは、リボーク後の不当なECS発行装置証明書に基づく処理であると判断できるためである。

- [0204] 次に、図18に示すフローチャートを参照して、先に図14のステップS132～S135を参照して説明したユーザ装置104における暗号化コンテンツ署名ファイル (ECSファイル) を適用したコンテンツ再生許容判定処理の詳細について説明する。

- [0205] なお、ユーザ装置は、図18に示すステップS171以前に、コンテンツ提供装置から受信した暗号化コンテンツ署名ファイル (ECSファイル) に設定されたECS発行装置署名を適用した署名検証を実行する。

この署名検証が成立し、暗号化コンテンツ署名ファイル (ECSファイル) の正当性が確認され場合は、さらに、暗号化コンテンツ署名ファイル (ECSファイル) に格納されたECS発行装置証明書の署名検証を実行する。これらの2つの署名検証が成立したことを条件としてステップS171以下の処理を行う。

- [0206] 上記2つの署名検証の少なくともいずれかが成立しなかった場合は、暗号化コンテンツ署名ファイル (ECSファイル) またはECS発行装置証明書

の正当性が確認されないので、ステップS 1 7 1 以下の処理は実行されない。
この場合はコンテンツ再生処理も実行しないことになる。

[0207] 暗号化コンテンツ署名ファイル（ECSファイル）と、ECS発行装置証明書の2つの署名検証が成立し、暗号化コンテンツ署名ファイル（ECSファイル）とECS発行装置証明書の正当性が確認された場合、ユーザ装置は、ステップS 1 7 1 の処理を実行する。

[0208] ステップS 1 7 1 において、ユーザ装置は、
暗号化コンテンツ署名ファイル（ECSファイル）の記録データであるECS発行日時（ECS Issue Date）を読み出す。さらに、
ECS発行装置証明書の記録データであるECS発行装置証明書使用期限（Expiration Date）を読み出す。

さらに、これらの日時情報を比較し、
ECS発行装置証明書使用期限（Expiration Date）がECS発行日時（ECS Issue Date）より前であるか否かを判定する。

前である場合（Yes）は、ステップS 1 7 5に進み、コンテンツの復号、再生処理を実行しない。

これは、すでに有効期限の切れたECS発行装置証明書であることが確認されたからである。

[0209] 一方、ステップS 1 7 1 において、ECS発行装置証明書使用期限（Expiration Date）がECS発行日時（ECS Issue Date）より前でない場合（No）は、ステップS 1 7 2に進み、ステップS 1 7 3以下においてリボケーションリストを適用したコンテンツ提供可否判定処理を実効する。

[0210] なお、ユーザ装置は、予め図12を参照して説明したECS発行装置公開鍵リボケーションリストを取得しているものとする。例えばライセンス発行装置（LA）101から取得可能である。

[0211] ユーザ装置は、ステップS 1 7 3において、ECS発行装置証明書からE

ＣＳ証明書識別子を取得し、この識別子（ＩＤ）がＥＣＳ発行装置公開鍵リボケーションリストに登録されているか否かを判定する。

登録されていない場合（Ｎｏ）は、ＥＣＳ発行装置証明書は無効化（リボーク）されておらず有効であることが確認され、この場合は、ステップＳ１７６に進み、コンテンツ再生処理を実行する。

[0212] なお、コンテンツ再生処理の開始前に、さらに、暗号化コンテンツの復号に適用するタイトルキーの取得や生成処理、さらに、暗号化コンテンツ署名ファイルに含まれるコンテンツハッシュリストを適用したハッシュ値照合処理を実行する。ハッシュ値照合において照合が成立し、コンテンツの改ざんのないことが確認された場合にコンテンツの再生が許容されることになる。

[0213] 一方、ステップＳ１７３において、ＥＣＳ証明書識別子（ＩＤ）がＥＣＳ発行装置公開鍵リボケーションリストに登録されていると判定した場合（Ｙｅｓ）、この場合は、ステップＳ１７４に進む。

[0214] ステップＳ１７４では、ＥＣＳ発行装置公開鍵リボケーションリストに登録されているそのＥＣＳ発行装置証明書が無効化（リボーク）された日時、すなわち、

リボーク日時と、

暗号化コンテンツ署名ファイル（ＥＣＳファイル）の記録データであるＥＣＳ発行日時（ＥＣＳ Ｉｓｓｕｅ Ｄａｔｅ）と、

これらの２つの日時データを比較する。

[0215] 暗号化コンテンツ署名ファイル（ＥＣＳファイル）の記録データであるＥＣＳ発行日時（ＥＣＳ Ｉｓｓｕｅ Ｄａｔｅ）がリボーク日時より前である場合（Ｙｅｓ）は、ステップＳ１７６に進み、コンテンツの再生処理を実行する。

これは、リボーク以前の正当なＥＣＳ発行装置証明書に基づく処理であると判断できるためである。

[0216] 一方、ステップＳ１７３において、暗号化コンテンツ署名ファイル（ＥＣＳファイル）の記録データであるＥＣＳ発行日時（ＥＣＳ Ｉｓｓｕｅ Ｄ

a t e) がリボーク日時より前でない場合 (N o) は、ステップ S 1 7 5 に進み、コンテンツの再生処理を停止する。

これは、リボーク後の不当な E C S 発行装置証明書に基づく処理であると判断できるためである。

[0217] [1 0. 暗号鍵と E C S 発行装置署名との関連づけ構成について]

次に、暗号鍵と E C S 発行装置署名との関連づけ構成について説明する。

先に、図 3、図 6 を参照して説明したように、ユーザ装置 1 0 4 では、例えばフラッシュメモリから構成されるメモリカード等にコンテンツ等を記録して利用する。

[0218] 図 3 を参照して説明したように、メモリカード 3 1 の記憶領域は、

(a) 保護領域 (P r o t e c t e d A r e a) 5 1、

(b) 汎用領域 (G e n e r a l P u r p o s e A r e a) 5 2、

これら 2 つの領域によって構成される。

[0219] (b) 汎用領域 (G e n e r a l P u r p o s e A r e a) 5 2 はユーザの利用する記録再生装置によって、自由にアクセス可能な領域であり、コンテンツやコンテンツ対応の利用制御情報 (U s a g e R u l e)、その他の一般のコンテンツ管理データ等が記録される。

この汎用領域 (G e n e r a l P u r p o s e A r e a) 5 2 は、例えばサーバやユーザの記録再生装置によって自由にデータの書き込みや読み取りを行うことが可能な領域である。

[0220] 一方、(a) 保護領域 (P r o t e c t e d A r e a) 5 1 は、自由なアクセスが許容されない領域である。

保護領域 (P r o t e c t e d A r e a) 5 1 は複数の区分領域としてのブロック (# 0, # 1, # 2 . . .) に分割され、各ブロック単位でアクセス権が設定される。

[0221] 例えば、ユーザの利用する記録再生装置、あるいはネットワークを介して接続されるサーバ等によってデータの書き込みあるいは読み取りを行おうとする場合、メモリカード 3 1 のデータ処理部が、メモリカード 3 1 に予め格

納されたプログラムに従って、各装置に応じてブロック単位で読み取り（Read）または書き込み（Write）の可否を決定する。

[0222] メモリカード31は、予め格納されたプログラムを実行するためのデータ処理部や認証処理を実行する認証処理部を備えており、メモリカード31は、まず、メモリカード31に対してデータの書き込みまたは読み取りを実行しようとする装置との認証処理を行う。

[0223] この認証処理の段階で、相手装置、すなわちアクセス要求装置から公開鍵証明書等の装置証明書を受信する。

たとえばアクセス要求装置がサーバである場合は、図5を参照して説明したサーバの保有するサーバ証明書（Server Certificate）を受信し、その証明書に記載された情報を用いて、保護領域（Protected Area）51の各ブロック（区分領域）単位でアクセスが許容されるか否かを判定する。

[0224] また、アクセス要求装置がホスト装置、例えばコンテンツ記録再生を実行するユーザ装置としての記録再生装置（ホスト）である場合は、図4を参照して説明した記録再生装置（ホスト）の保有するホスト証明書（Host Certificate）を受信し、その証明書に記載された情報を用いて、保護領域（Protected Area）51の各ブロック（区分領域）のアクセスが許容されるか否かを判定する。

[0225] このアクセス権判定処理は、図3に示す保護領域（Protected Area）51内のブロック（図に示す領域#0，#1，#2・・・）単位で行われる。メモリカード31は、ブロック単位で許可された処理（データの読み取り／書き込み等の処理）のみをサーバやホストに実行させる。

[0226] ユーザ装置104がメディアを装着してコンテンツ提供装置103から受信するコンテンツを記録する場合のデータ記録構成例について、図19を参照して説明する。

図19には、コンテンツ提供装置としてのサーバA201がユーザ装置としてのホスト202に装着されたメモリカード210に、暗号化コンテンツ

を提供して記録する処理例を示している。

メモ리카ード210は、

保護領域 (Protected Area) 211、

汎用領域 (General Purpose Area) 212、

これらを有している。

[0227] コンテンツ提供装置としてのサーバA201は、暗号化コンテンツ提供処理に際して、提供コンテンツの暗号化および復号に適用するタイトルキーを保護領域 (Protected Area) の所定ブロックに記録する。

[0228] サーバA201は、先に図5を参照したサーバ証明書 (Server Certificate) を保有している。

まず、サーバA201は、メモ리카ード210との相互認証処理を実行する。その際にメモ리카ード210に対してサーバ証明書を出力する。

メモ리카ード210は、サーバA201から受信したサーバ証明書に記録された保護領域アクセス権情報を確認する。

この確認処理において、サーバA201がブロック#0のアクセス権 (書き込みの権利) を有していることが判定された場合にのみ、サーバA201はメモ리카ード210に設定された保護領域211のブロック#0に対するデータ書き込みが可能となる。

[0229] 図に示すように、サーバA201は、提供コンテンツの復号に適用するタイトルキーを保護領域 (Protected Area) 211のブロック#0, 221に格納する。

なお、保護領域には、タイトルキー自体をそのまま格納せず、

(a) 利用制御情報 (UR: Usage Rule) と、

(b) 図9を参照して説明したECSファイルの構成データであるECS発行装置署名 (Signature by ECS Issuer)

これら (a)、(b) の連結データのハッシュ値と、

タイトルキーKtとの排他的論理和演算結果を格納する。

[0230] 例えばコンテンツ(a1)に対するタイトルキー: Kt(a1)は、以下

のタイトルキー変換データとして保護領域に格納する。

$Kt(a1) (+) (UR(a1) || ECSSig(a1)) hash$

ただし、

$UR(a1)$: コンテンツ $a1$ に対応する利用制御情報

$ECSSig(a1)$: コンテンツ $a1$ に対応する ECS ファイルの構成データである ECS 発行装置署名 (Signature by ECS Issuer)

また、演算子としての記号、

$(+)$: 排他的論理和演算

$||$: データの連結を意味し、 $a || b$ はデータ a とデータ b の連結データを意味する。

$hash$: ハッシュ値を意味し、 $(a || b) hash$ は、データ a とデータ b の連結データのハッシュ値を意味する。

[0231] 図 19 に示す例では、サーバ A は、メモ리카ードの汎用領域 (General Purpose Area) 212 に、以下のコンテンツと利用制御情報と ECS ファイルを記録する。

コンテンツ : $Con(a1)$ 、 $Con(a2)$ 、 $Con(a3)$ 、

上記コンテンツに対応する利用制御情報 (Usage Rule) : $UR(a1)$ 、 $UR(a2)$ 、 $UR(a3)$ 、

上記コンテンツに対応する ECS ファイル (ECS File) : $ECS(a1)$ 、 $ECS(a2)$ 、 $ECS(a3)$ 、

これらのコンテンツと利用制御情報と ECS ファイルのセットを記録する。

[0232] さらに、サーバ A は、メモ리카ードの保護領域 (Protected Area) 211 のブロック #0, 221 に以下のデータを記録する。

コンテンツ対応のタイトルキーと、

コンテンツ対応の利用制御情報 (Usage Rule) と ECS 発行装置署名 ($ECSSig$) の連結データのハッシュ値との排他的論理和 (XO

R) 演算結果

$$K_t(a_1) (+) (UR(a_1) || ECSSig(a_1)) hash$$

$$K_t(a_2) (+) (UR(a_2) || ECSSig(a_2)) hash$$

$$K_t(a_3) (+) (UR(a_3) || ECSSig(a_3)) hash$$

[0233] なお、図19には、サーバA201の処理例を示しているが、例えば異なるサーバBは、サーバBの提供コンテンツ(b_x)に対応するタイトルキーの格納領域として許容された保護領域(Protected Area)の所定ブロック、例えば、ブロック#1にサーバBの提供コンテンツに同様のタイトルキー変換データ、例えば、

$$K_t(b_x) (+) (UR(b_x) || ECSSig(b_x)) hash$$

上記データを格納する。

[0234] 図20には、コンテンツを利用するユーザ装置(ホスト)202とコンテンツ等を格納したメモリカード210を示している。

[0235] ユーザ装置(ホスト)202は、先に図4を参照したホスト証明書(Host Certificate)を保有している。

まず、ユーザ装置(ホスト)202は、メモリカード210との相互認証処理を実行する。その際にメモリカード210に対してホスト証明書を出力する。

メモリカード210は、ユーザ装置(ホスト)202から受信したホスト証明書に記録された保護領域アクセス権情報を確認する。

この確認処理において、ユーザ装置(ホスト)202がブロック#0のアクセス権(読み取りの権利)を有していることが判定された場合にのみ、ユーザ装置(ホスト)202はメモリカード210に設定された保護領域211のブロック#0からのデータ読み取りが可能となる。

[0236] これらの相互認証およびアクセス権が確認された後、ユーザ装置(ホスト)202は、コンテンツの利用に際して以下の処理を実行する。

まず、メモリカードの汎用領域(General Purpose Area)212から利用対象コンテンツ:Con(x_y)と、対応する利用制

御情報：UR (x y)、ECSファイル：ECS (x y) 取得する。

- [0237] 次に、利用制御情報：UR (x y) を参照して、利用対象コンテンツ：Con (x y) のタイトルキーの格納された保護領域のブロックがいずれのブロックであるかを確認する。

利用制御情報：UR (x y) には、利用対象コンテンツ：Con (x y) のタイトルキーの格納されたブロックの識別子が記録されている。

- [0238] 保護領域 2 1 1 のタイトルキー格納ブロックが特定されると、そのブロックの記録データの読み出し処理を行う。

例えば、選択ブロックから、以下のデータを読み出す。

$$Kt(x y) (+) (UR(x y) || ECSSig(x y)) hash$$

- [0239] 次に、汎用領域 2 1 2 から読み出した

利用制御情報：UR (x y) と、

ECSファイル：ECS (x y) に格納されたECS発行装置署名 (ECSSig (x y))

これらの連結処理とハッシュ値算出処理を行う。

すなわち、

$$(UR(x y) || ECSSig(x y)) hash$$

上記を算出する。

この算出結果を、

P (x y) とする。

- [0240] その後、以下の計算を行うことでタイトルキーKt (x y) を得る。

$$[\text{ブロックからの読み出しデータ (タイトルキー変換データ)}] (+) P(x y)$$

$$= (Kt(x y) (+) (UR(x y) || ECSSig(x y)) hash) (+) P(x y)$$

$$= (Kt(x y) (+) (UR(x y) || ECSSig(x y)) hash) (+) (UR(x y) || ECSSig(x y)) hash$$

$$= K_t(x, y)$$

このような計算処理によってタイトルキー $K_t(x, y)$ を取得し、取得したタイトルキーによって暗号化コンテンツを復号して利用する。

[0241] メモリカードの記録データの例について図 21 を参照して説明する。

図 21 には、2つの異なるサーバ、サーバ A とサーバ B がメモリカードに対して書き込むデータの例を示している。

サーバ A は、メモリカードの保護領域のブロック # 0 に対するアクセス権を有している。

サーバ B は、メモリカードの保護領域のブロック # 1 に対するアクセス権を有している。

[0242] 各サーバはユーザ装置としてのホスト機器に装着されたメモリカードに対してコンテンツ他のデータを記録する。

サーバ A の提供コンテンツを、 $Con(a1)$ 、 $Con(a2)$ 、 $Con(a3)$ とする。

サーバ B の提供コンテンツを、 $Con(b1)$ 、 $Con(b2)$ とする。

[0243] 図 21 に示すように、

サーバ A は、メモリカードの汎用領域 (General Purpose Area) に、以下のデータを記録する。

コンテンツ : $Con(a1)$ 、 $Con(a2)$ 、 $Con(a3)$

上記コンテンツに対応する利用制御情報 (Usage Rule) : $UR(a1)$ 、 $UR(a2)$ 、 $UR(a3)$ 、

上記コンテンツに対応する ECS ファイル (ECS File) : $ECS(a1)$ 、 $ECS(a2)$ 、 $ECS(a3)$ 、

[0244] さらに、サーバ A は、メモリカードの保護領域 (Protected Area) のブロック # 0 に以下のデータを記録する。

上記コンテンツの復号に適用するタイトルキー : $K_t(a1)$ 、 $K_t(a2)$ 、 $K_t(a3)$ の変換データ、

$K_t(a1)(+)(UR(a1) || ECSSig(a1)) has$

h

K t (a 2) (+) (U R (a 2) | | E C S S i g (a 2)) h a s

h

K t (a 3) (+) (U R (a 3) | | E C S S i g (a 3)) h a s

h

これらのデータを記録する。

[0245] 一方、サーバBは、メモ리카ードの汎用領域 (G e n e r a l P u r p o s e A r e a) に、以下のデータを記録する。

コンテンツ : C o n (b 1) 、 C o n (b 2)

上記コンテンツに対応する利用制御情報 (U s a g e R u l e) : U R (b 1) 、 U R (b 2) 、

上記コンテンツに対応するECSファイル (E C S F i l e) : E C S (b 1) 、 E C S (b 2) 、

[0246] さらに、サーバBは、メモ리카ードの保護領域 (P r o t e c t e d A r e a) のブロック # 1 に以下のデータを記録する。

上記コンテンツの復号に適用するタイトルキー : K t (b 1) 、 K t (b 2) の変換データ、

K t (b 1) (+) (U R (b 1) | | E C S S i g (b 1)) h a s
h

K t (b 2) (+) (U R (b 2) | | E C S S i g (b 2)) h a s
h

これらのデータを記録する。

[0247] 各サーバが、メモ리카ードの保護領域 (P r o t e c t e d A r e a) のブロック内にデータを記録する場合には、メモ리카ードは、前述したサーバ証明書の記録に基づくアクセス権確認を実行し、ブロックに対する書き込み権の確認を行い、アクセス権が確認された場合にのみ、データ書き込みが実行される。

[0248] 図 2 2 には、

サーバAとサーバBが、メモリカードの保護領域のブロック#0に対するアクセス権を有し、

サーバCとサーバDが、メモリカードの保護領域のブロック#1に対するアクセス権を有する場合におけるデータ記録例を示している。

[0249] サーバAは、メモリカードの汎用領域 (General Purpose Area) に、以下のデータを記録する。

コンテンツ : Con (a1)、Con (a2)、Con (a3)

上記コンテンツに対応する利用制御情報 (Usage Rule) : UR (a1)、UR (a2)、UR (a3)、

上記コンテンツに対応するECSファイル (ECS File) : ECS (a1)、ECS (a2)、ECS (a3)、

さらに、サーバAは、メモリカードの保護領域 (Protected Area) のブロック#0に以下のデータを記録する。

上記コンテンツの復号に適用するタイトルキー : Kt (a1)、Kt (a2)、Kt (a3) の変換データ、

Kt (a1) (+) (UR (a1) || ECSSig (a1)) has h

Kt (a2) (+) (UR (a2) || ECSSig (a2)) has h

Kt (a3) (+) (UR (a3) || ECSSig (a3)) has h

これらのデータを記録する。

[0250] サーバBは、メモリカードの汎用領域 (General Purpose Area) に、以下のデータを記録する。

コンテンツ : Con (b1)、Con (b2)

上記コンテンツに対応する利用制御情報 (Usage Rule) : UR (b1)、UR (b2)、

上記コンテンツに対応するECSファイル (ECS File) : ECS

(b 1)、ECS (b 2)、

[0251] さらに、サーバBは、メモ리카ードの保護領域 (Protected Area) のブロック # 0 に以下のデータを記録する。

上記コンテンツの復号に適用するタイトルキー : K t (b 1)、K t (b 2) の変換データ、

K t (b 1) (+) (U R (b 1) || E C S S i g (b 1)) h a s h

K t (b 2) (+) (U R (b 2) || E C S S i g (b 2)) h a s h

これらのデータを記録する。

[0252] サーバCは、メモ리카ードの汎用領域 (General Purpose Area) に、以下のデータを記録する。

コンテンツ : C o n (c 1)

上記コンテンツに対応する利用制御情報 (Usage Rule) : U R (c 1)、

上記コンテンツに対応するECSファイル (ECS File) : E C S (c 1)、

[0253] さらに、サーバCは、メモ리카ードの保護領域 (Protected Area) のブロック # 1 に以下のデータを記録する。

上記コンテンツの復号に適用するタイトルキー : K t (c 1) の変換データ、

K t (c 1) (+) (U R (c 1) || E C S S i g (c 1)) h a s h

これらのデータを記録する。

[0254] サーバDは、メモ리카ードの汎用領域 (General Purpose Area) に、以下のデータを記録する。

コンテンツ : C o n (d 1)、C o n (d 2)

上記コンテンツに対応する利用制御情報 (Usage Rule) : U R

(d 1)、UR (d 2)、

上記コンテンツに対応するECSファイル (ECS File) : ECS (d 1)、ECS (d 2)、

[0255] さらに、サーバDは、メモリカードの保護領域 (Protected Area) のブロック# 1に以下のデータを記録する。

上記コンテンツの復号に適用するタイトルキー: Kt (d 1)、Kt (d 2) の変換データ、

Kt (d 1) (+) (UR (d 1) || ECSSig (d 1)) hash

Kt (d 2) (+) (UR (d 2) || ECSSig (d 2)) hash

これらのデータを記録する。

[0256] なお、コンテンツ再生を実行するユーザ装置 (ホスト) は、再生対象コンテンツを汎用領域から選択した場合、そのタイトルキーの格納されている保護領域のブロックを特定することが必要となる。

このブロック特定情報は、各コンテンツに対応する利用制御情報 (UR) から取得する。

[0257] 図23を参照して利用制御情報の利用例について説明する。図23 (a) に、メモリカードの汎用領域 (General Purpose Area) に記録されたコンテンツa 1に対応する利用制御情報 (Usage Rule) a 1の具体例を示す。

[0258] 利用制御情報 (Usage Rule) には、

- (1) ブロック識別子 (# 0)
- (2) タイトルキー識別子 (a 1)
- (3) ECSファイル識別子 (a 1)

これらのデータが記録される。

[0259] (1) ブロック識別子は、

この利用制御情報 (Usage Rule) UR - (a 1) の対応コンテ

ンツ：C o n (a 1) に対するタイトルキーK t (a 1) の格納ブロックを示す情報である。

本例ではブロック識別子＝# 0であり、

コンテンツ再生を実行するユーザ装置（ホスト機器）は、ブロック# 0を選択可能となる。

[0260] (2) タイトルキー識別子は、

ブロック# 0に格納された多数のタイトルキーのどのタイトルキーが、この利用制御情報（U s a g e R u l e）U R (a 1) の対応コンテンツ：C o n (a 1) に対するタイトルキーであるかを示す情報である。

本例では、タイトルキー識別子＝a 1であり、

タイトルキーK t (a 1) が選択可能となる。

[0261] (3) E C Sファイル識別子（a 1）は、

コンテンツ（a 1）に対応するE C Sファイルを識別するための情報である。

[0262] ユーザ装置（ホスト）は、利用制御情報：U R (a 1) を参照して、利用対象コンテンツ：C o n (a 1) のタイトルキーの格納された保護領域のブロックがいずれのブロックであるかを確認し、そのブロックから、以下のデータを読み出す。

K t (a 1) (+) (U R (a 1) | | E C S S i g (a 1)) h a s h

[0263] 次に、汎用領域から読み出した

利用制御情報：U R (a 1) と、

E C Sファイル：E C S (a 1) に格納されたE C S発行装置署名（E C S S i g (x y) ）

これらの連結処理とハッシュ値算出処理を行う。

すなわち、

P (a 1) = (U R (a 1) | | E C S S i g (a 1)) h a s h

上記を算出する。

その後、以下の計算を行うことでタイトルキー $K_t(x y)$ を得る。

$$\begin{aligned}
 & \left[\text{ブロックからの読み出しデータ (タイトルキー変換データ)} \right] (+) P \\
 & (x y) \\
 & = (K_t(a 1) (+) (UR(a 1) || ECSSig(a 1)) hash) (+) P(a 1) \\
 & = (K_t(a 1) (+) (UR(a 1) || ECSSig(a 1)) hash) (+) (UR(a 1) || ECSSig(a 1)) hash) \\
 & = K_t(a 1)
 \end{aligned}$$

このような計算処理によってタイトルキー $K_t(a 1)$ を取得し、取得したタイトルキーによって暗号化コンテンツを復号して利用する。

[0264] このように、メモ리카ードの保護領域に記録するタイトルキーは、利用制御情報 (UR) と EC S 発行装置署名 (ECSSig) との連結データのハッシュ値との排他的論理和 (XOR) 演算結果として格納される。

このような処理を行うことで、EC S 発行装置署名 (ECSSig) に適用する EC S 発行装置の署名鍵 (秘密鍵) の漏えいが発生した場合にもコンテンツの不正利用を防止することが可能となる。

[0265] 例えば、コンテンツ提供サーバやユーザ装置が、漏えいした EC S 発行装置の署名鍵 (秘密鍵) を適用した不正処理、具体的には、暗号化コンテンツのすげ替え処理などによるコンテンツ不正利用を防止可能となる。

[0266] なお、すげ替えとは、例えば、あるコンテンツ (C 1) に対応するタイトルキー ($K_t 1$) を利用して他のコンテンツ (C 2)、(C 3)、(C 4)・・・の暗号化を施してユーザに提供する処理などである。

このような処理を行うと、タイトルキー ($K_t 1$) を有するユーザ装置では、その他のコンテンツ (C 2)、(C 3)、(C 4)・・・を正規購入することなく、復号、再生することが可能となる。

[0267] メモ리카ードの保護領域に記録するタイトルキーを、利用制御情報 (UR) と EC S 発行装置署名 (ECSSig) との連結データのハッシュ値との排他的論理和 (XOR) 演算結果として格納することで、上記のようなすげ

替えを防止することができる。

[0268] このすげ替え防止効果について図24以下を参照して説明する。

図24は、

(a) コンテンツ (C1) に対応する正当なデータ格納構成

(b) コンテンツ (C1) に対応するタイトルキー (Kt1) を利用してコンテンツ (C2) を暗号化したすげ替えデータのデータ格納構成を示している。

[0269] 図24 (a) に示す正当データ格納構成では、

メモ리카ードの汎用領域に、

(a1) コンテンツ (C1) に対する正当なタイトルキー (Kt1) で暗号化された暗号化コンテンツ (C1 (Kt1))

(a2) コンテンツ (C1) に対する正当な利用制御情報 (UR1)

(a3) コンテンツ (C1) に対する正当な暗号化コンテンツ署名ファイル (ECSファイル: ECS1 (C1, Kt1))

[0270] なお、ECSファイルには、ECS発行装置署名 (ECSSig) が格納されており、このECS発行装置署名 (ECSSig) は、先に、図13を参照して説明したように、コンテンツ (C1) のハッシュリスト集合と、タイトルキー (Kt1) のハッシュ値を含むデータに基づいて生成された電子署名を含む。この署名データの生成元データを明示するため、ECSファイルは、ECS1 (C1, Kt1) として記載している。

[0271] また、図24 (a) に示す正当データ格納構成では、

メモ리카ードの保護領域のブロックNに、タイトルキー (Kt1) の変換データ、すなわち、以下のデータが記録される。

Kt1 (+) (UR1 || ECS1Sig) hash

ただし、

UR1 : コンテンツ1に対応する利用制御情報

ECS1Sig : コンテンツ1に対応するECSファイルの構成データであるECS発行装置署名 (Signature by ECS Issue

r)

また、演算子としての記号、

(+) : 排他的論理和演算

| | : データの連結を意味し、 $a \mid b$ はデータ a とデータ b の連結データを意味する。

hash : ハッシュ値を意味し、 $(a \mid b) \text{ hash}$ は、データ a とデータ b の連結データのハッシュ値を意味する。

[0272] 例えば、悪意のあるコンテンツ提供サーバは、このコンテンツ (C 1) のタイトルキー (K t 1) を他のコンテンツ (C 2) に対する暗号鍵として利用して、ユーザに提供する。

この不正コンテンツ配信の結果、メモリカードには、図 2 4 (b) に示す「すげ替えデータ」が格納される。

[0273] 図 2 4 (b) に示す「すげ替えデータ」格納構成では、

メモリカードの汎用領域に、

(b 1) コンテンツ (C 2) に対する不正なタイトルキー (K t 1) で暗号化された不正暗号化コンテンツ (C 2 (K t 1))

(b 2) コンテンツ (C 2) に不正に対応付けた利用制御情報 (U R 1)
[= コンテン (C 1) 対応の利用制御情報 (U R 1)]

(b 3) コンテンツ (C 2) に対応させて不正に生成した暗号化コンテンツ署名ファイル (E C S 2 [= E C S 2 (C 2, K t 1)]

[0274] なお、不正な E C S ファイル : E C S 2 に格納される E C S 発行装置署名 (E C S S i g) は、コンテンツ (C 2) のハッシュリスト集合と、コンテンツ (C 1) 対応のタイトルキー (K t 1) のハッシュ値を含むデータに基づいて、漏えいした E C S 発行装置の署名鍵 (秘密鍵) によって生成した電子署名を含む。この署名データの生成元データを明示するため、E C S ファイルは、E C S 2 (C 2, K t 1) として記載している。

[0275] また、図 2 4 (b) に示す「すげ替えデータ」格納構成では、

メモリカードの保護領域のブロック N に、タイトルキー (K t 1) の変換

データ、すなわち、以下のデータが記録される。

$K_{t1} (+) (UR1 || ECS1Sig) hash$

[0276] この図24(b)に示す「すげ替えデータ」の記録処理シーケンスについて図25に示すフローチャートを参照して説明する。

なお、この図25に示す処理は、既に、図24(a)に示すコンテンツ(C1)に対応する正当なデータセットを格納したメモリカードを利用して実行され、メモリカードの保護領域のブロックNに対するアクセス権としてデータ読み取り処理の権利を有する装置、例えばコンテンツ提供サーバやユーザ装置によって実行される処理である。

[0277] まず、ステップS201において、新たなコンテンツC2を用意する。

次に、ステップS202において、メモリカードの汎用領域に記録されたコンテンツ(C1)の利用制御情報(UR1)から、「ブロック識別子」及び「タイトルキー識別子」を取得し、これらの取得情報に基づいて、保護領域の所定ブロック、すなわちタイトルキー格納ブロックから、正当なコンテンツ(C1)に対応する以下のタイトルキー変換データを読み出す。

$K_{t1} (+) (UR1 || ECS1Sig) hash$

なお、 $ECS1Sig = Sign(ECS署名鍵, M)$

$M = \text{コンテンツC1のコンテンツハッシュリスト集合} || K_{t1} \text{ハッシュ値}$

である。

[0278] 次に、ステップS203において、汎用領域から読み出した正当なコンテンツ(C1)に対応する利用制御情報(UR1)とECSファイル(ECS1(C1, K_{t1}))の連結データのハッシュ値を算出し、算出結果と、保護領域から読み出した上記のタイトルキー変換データとの排他的論理和演算(XOR)を実行してコンテンツ(C1)に対応する正当なタイトルキー(K_{t1})を取得する。

すなわち、

$K_{t1} = (\text{保護領域からの読み出しデータ}) (+) (\text{汎用領域からの読み$

出しデータ)

$$= K_{t1} (+) (UR1 || ECS1Sig) hash (+) (UR1 || ECS1Sig) hash$$

上記式に従ってタイトルキー (K_{t1}) を取得する。

なお、(+) は排他的論理和演算 (XOR) を意味する。

[0279] 次に、ステップ S204 において、ステップ S203 で取得したタイトルキー (K_{t1}) を適用して新たなコンテンツ C2 の暗号化を実行する。

暗号化コンテンツ C2 (K_{t1}) を生成する。

[0280] 次に、ステップ S205 において、暗号化コンテンツ C2 (K_{t1}) をメモ리카ードの汎用領域に記録する。

[0281] 次に、ステップ S206 において、コンテンツ C2 から生成したコンテンツハッシュリスト集合及び K_{t1} ハッシュ値に対する暗号化コンテンツ署名 $ECS2Sig$ を生成する。以下の署名データである。

$$ECS2Sig = Sign(ECS \text{ 署名鍵}, M)$$

ただし、

$M = \text{コンテンツ C2 のコンテンツハッシュリスト集合} || K_{t1} \text{ ハッシュ値}$

である。

なお、署名生成には漏えいした暗号化コンテンツ署名発行装置の署名鍵 (秘密鍵) を適用する。

[0282] 最後にステップ S207 において、ステップ S206 で不正に生成した ECS 署名 ($ECS2Sig(C2, K_{t1})$) を含む ECS ファイルを生成してメモ리카ードの汎用領域に記録する。

[0283] この図 25 に示す一連の処理によって図 24 (b) に示す「すげ替えデータ」の記録処理が終了する。

このようなすげ替え処理によって、コンテンツ C2 を、異なるコンテンツ (C1) のタイトルキー (K_{t1}) を適用して暗号化されたコンテンツ C2 (K_{t1}) が生成される。

なお、本例では、不正記録コンテンツ C 2 (K t 1) に対応する利用制御情報として、コンテンツ C 1 の利用制御情報 (U R 1) をそのまま利用するものとする。

[0284] 次に、図 2 4 (b) に示す「すげ替えデータ」を利用してコンテンツ C 2 を再生するユーザ装置の処理について、図 2 6 に示すフローチャートを参照して説明する。

まず、ステップ S 2 2 1 において、ユーザ装置は、メモリカードの汎用領域から再生予定の暗号化コンテンツ C 2 (K t 1) と、このコンテンツに対して生成された ECS ファイル (ECS 2 (C 2, K t 1)) を読み出す。

[0285] 次にステップ S 2 2 2 において、メモリカードの汎用領域からコンテンツ C 2 に対応付けて記録されている利用制御情報 (U R 1) からタイトルキーの格納ブロックを示すブロック識別子を読み取る。

前述したように、本例では、不正記録コンテンツ C 2 (K t 1) に対応する利用制御情報として、コンテンツ C 1 の利用制御情報 (U R 1) をそのまま利用する。

[0286] 先に図 2 3 を参照して説明したように、利用制御情報 (U R) には、タイトルキーを格納したブロック識別子、タイトルキー識別子等が記録されている。

ステップ S 2 2 2 では、コンテンツ C 1 の利用制御情報 (U R 1) からブロック識別子、タイトルキー識別子を読み取る。

このブロック識別子、タイトルキー識別子は、コンテンツ C 1 に対する正当なタイトルキー K t 1 の格納されたブロックと、そのブロックに格納されたタイトルキーに対応する識別子である。

したがって、読み取りデータは、コンテンツ C 1 に対するタイトルキー変換データ、すなわち、

$$K t 1 (+) (U R 1 || ECS 1 S i g) h a s h$$

となる。

[0287] 次に、ステップ S 2 2 3 において、汎用領域から読み出した利用制御情報

(U R 1) とコンテンツ C 2 に対応して不正に生成した E C S ファイル (E C S 2 (C 2, K t 1)) の連結データのハッシュ値を算出し、算出結果と、保護領域から読み出した上記のタイトルキー変換データとの排他的論理和演算 (X O R) を実行してコンテンツ C 2 に対応する復号用のタイトルキー K t 2 の取得を試みる。

ここでは、K t 2 = K t 1 となるタイトルキー K t 2 が得られればタイトルキーの取得に成功したことになる。

[0288] すなわち、以下の式に従ってタイトルキー算出処理を試みる。

K t 2 = (保護領域からの読み出しデータ) (+) (汎用領域からの読み出しデータ)

= K t 1 (+) (U R 1 | | E C S 2 S i g) h a s h (+) (U R 1 | | E C S 1 S i g) h a s h

上記タイトルキー算出式に従ってタイトルキー (K t 2) の取得を試みる。

なお、(+) は排他的論理和演算 (X O R) を意味する。

[0289] しかし、上記タイトルキー算出式において、

E C S 2 S i g ≠ E C S 1 S i g

であるため、

上記算出式によってえられる値 : K t 2 は、K t 1 とは異なる値、すなわち、

K t 2 ≠ K t 1

となる。

[0290] この結果、ユーザ装置は、コンテンツ C 2 の暗号化に適用したタイトルキー K t 1 を取得することはできず、コンテンツ C 2 の復号、再生は失敗する。ステップ S 2 2 4 の処理である。

[0291] また、ステップ S 2 2 5 において、ユーザ装置は、予め規定された再生シーケンスに従って、汎用領域から読み出した E C S ファイルに含まれる E C S 発行装置署名 (E C S S i g) の検証処理を実行する。

以下の式に従って署名検証処理を行う。

$Verify(ECS \text{ 発行装置公開鍵}, ECS2Sig, M)$

ただし、

$Verify(k, S, M)$ は、データ M に対する電子署名 S を検証鍵 k を用いて検証する処理を示す。

$M = \text{コンテンツ} C2 \text{ のコンテンツハッシュリスト集合} || Kt2 \text{ ハッシュ}$ である。

$Kt2$ は、ステップ $S223$ で算出した値を利用することになる。

[0292] ECS ファイルに格納した $ECS2Sig$ は、図 25 に示すフローのステップ $S206$ において生成した不正な署名であり、以下のデータである。

$ECS2Sig = Sign(ECS \text{ 署名鍵}, M)$

ただし、

$M = \text{コンテンツ} C2 \text{ のコンテンツハッシュリスト集合} || Kt1 \text{ ハッシュ}$ 値である。

[0293] このように、

署名検証に適用するデータ M は、 $Kt2$ ハッシュ値を含むデータであるのに対して、

ECS ファイルに格納された署名データ $ECS2Sig$ は、 $Kt1$ ハッシュを含む M に対して生成されている。

従って、このステップ $S225$ における署名検証は失敗する。図 26 のステップ $S226$ に記載の通りである。

[0294] このように、ユーザ装置は、図 24 (b) に示す「すげ替えデータ」を適用してコンテンツ $C2$ の復号、再生を行おうとしても、

コンテンツ $C2$ の復号に失敗、

ECS ファイルの署名検証に失敗、

これらの結果となり、結果としてコンテンツ $C2$ を利用することはできない。

[0295] 図24～図26を参照して説明した処理例は、コンテンツC1のタイトルキーK_t1を適用して、新たなコンテンツC2の暗号化と復号を試みた処理例であった。

次に、図27以下を参照して、コンテンツC1に対応する正しい利用制御情報(U_R1)を不正に改ざんして、新たな利用制御情報(U_R2)を生成した不正処理を行う場合の例について説明する。

利用制御情報には、例えば、コンテンツの利用期間情報やコピー制限情報などが記録されており、この利用制御情報の書き換えによって、利用可能期限を延長するといった不正が行われる可能性がある。

[0296] 図27は、先に説明した図24と同様、

(a) コンテンツ(C1)に対応する正当なデータ格納構成

(b) コンテンツ(C1)に対応するタイトルキー(K_t1)を利用してコンテンツ(C2)を暗号化したすげ替えデータのデータ格納構成を示している。

[0297] 図24(a)に示す正当データ格納構成では、

メモ리카ードの汎用領域に、

(a1) コンテンツ(C1)に対する正当なタイトルキー(K_t1)で暗号化された暗号化コンテンツ(C1(K_t1))

(a2) コンテンツ(C1)に対する正当な利用制御情報(U_R1)

(a3) コンテンツ(C1)に対する正当な暗号化コンテンツ署名ファイル(ECSファイル:ECS1(C1, K_t1))

[0298] なお、ECSファイルには、ECS発行装置署名(ECS_{sig})が格納されており、このECS発行装置署名(ECS_{sig})は、先に、図13を参照して説明したように、コンテンツ(C1)のハッシュリスト集合と、タイトルキー(K_t1)のハッシュ値を含むデータに基づいて生成された電子署名を含む。この署名データの生成元データを明示するため、ECSファイルは、ECS1(C1, K_t1)として記載している。

[0299] また、図27(a)に示す正当データ格納構成では、

メモ리카ードの保護領域のブロックNに、タイトルキー（ K_{t1} ）の変換データ、すなわち、以下のデータが記録される。

$K_{t1} (+) (UR1 || ECS1Sig) hash$

ただし、

UR1：コンテンツ1に対応する利用制御情報

ECS1Sig：コンテンツ1に対応するECSファイルの構成データであるECS発行装置署名（Signature by ECS Issuer）

また、演算子としての記号、

（+）：排他的論理和演算

||：データの連結を意味し、 $a || b$ はデータaとデータbの連結データを意味する。

hash：ハッシュ値を意味し、 $(a || b) hash$ は、データaとデータbの連結データのハッシュ値を意味する。

[0300] 例えば、悪意のあるコンテンツ提供サーバやユーザ装置は、このコンテンツ（C1）の利用制御情報（UR1）の書き換えを行う。

この不正処理の結果、メモ리카ードには、図27（b）に示す「すげ替えデータ」が格納される。

[0301] 図27（b）に示す「すげ替えデータ」格納構成では、

メモ리카ードの汎用領域に、

（b1）コンテンツ（C1）に対する不正生成したタイトルキー（ K_{t2} ）で暗号化された不正暗号化コンテンツ（ $C1(K_{t2})$ ）

（b2）コンテンツ（C1）に対応させて不正に生成した利用制御情報（UR2）

（b3）コンテンツ（C1）に対応させて不正に生成した暗号化コンテンツ署名ファイル（ $ECS2 [= ECS2(C1, K_{t2})]$ ）

[0302] なお、不正なECSファイル：ECS2に格納されるECS発行装置署名（ECS Sig）は、コンテンツ（C1）のハッシュリスト集合と、不正生

成したタイトルキー（ $K_t 2$ ）のハッシュ値を含むデータに基づいて、漏えいしたECS発行装置の署名鍵（秘密鍵）によって生成した電子署名を含む。この署名データの生成元データを明示するため、ECSファイルは、ECS2（ C_1 ， $K_t 2$ ）として記載している。

[0303] また、図27（b）に示す「すげ替えデータ」格納構成では、

メモ리카ードの保護領域のブロックNに、タイトルキー（ $K_t 1$ ）の変換データ、すなわち、以下のデータが記録される。

$K_t 1 (+) (UR1 || ECS1Sig) hash$

[0304] この図27（b）に示す「すげ替えデータ」の記録処理シーケンスについて図28に示すフローチャートを参照して説明する。

なお、この図28に示す処理は、既に、図27（a）に示すコンテンツ（ C_1 ）に対応する正当なデータセットを格納したメモ리카ードを利用して実行され、メモ리카ードの保護領域のブロックNに対するアクセス権としてデータ記録処理の権利を有する装置、例えばコンテンツ提供サーバやユーザ装置によって実行される処理である。

[0305] まず、ステップS241において、コンテンツ C_1 対応の利用制御情報UR1を汎用領域から読み出して、例えば利用期限情報などの書き換え等の改ざんを行い不正な利用制御情報（UR2）を生成する。

[0306] 次に、ステップS242において、メモ리카ードの汎用領域に記録されたコンテンツ（ C_1 ）の利用制御情報（UR1）から、「ブロック識別子」及び「タイトルキー識別子」を取得し、これらの取得情報に基づいて、保護領域の所定ブロック、すなわちタイトルキー格納ブロックから、正当なコンテンツ（ C_1 ）に対応する以下のタイトルキー変換データを読み出す。

$K_t 1 (+) (UR1 || ECS1Sig) hash$

なお、 $ECS1Sig = Sign(ECS署名鍵, M)$

$M = \text{コンテンツ} C_1 \text{のコンテンツハッシュリスト集合} || K_t 1 \text{ハッシュ値}$

である。

[0307] 次に、ステップS 2 4 3において、汎用領域から読み出した正当なコンテンツ（C 1）に対応する利用制御情報（UR 1）とECSファイル（ECS 1（C 1，K t 1））の連結データのハッシュ値を算出し、算出結果と、保護領域から読み出した上記のタイトルキー変換データとの排他的論理和演算（XOR）を実行してコンテンツ（C 1）に対応する正当なタイトルキー（K t 1）を取得する。

すなわち、

$K t 1 = (\text{汎用領域からの読み出しデータ}) (+) (\text{保護領域からの読み出しデータ})$

$= (UR 1 || ECS 1 Sig) hash (+) K t 1 (+) (UR 1 || ECS 1 Sig) hash$

上記式に従ってタイトルキー（K t 1）を取得する。

なお、（+）は排他的論理和演算（XOR）を意味する。

[0308] さらに、コンテンツC 2の暗号化と復号に適用するタイトルキーK 2を以下の式に従って算出する。

$K t 2 = (K t 1 (+) (UR 1 || ECS 1 Sig) hash (+) (UR 2 || ECS 1 Sig) hash$

[0309] 次に、ステップS 2 4 4において、ステップS 2 4 3で生成したタイトルキーK t 1を適用してコンテンツC 1（K t 1）を復号し、さらに、ステップS 2 4 3で生成した新たなタイトルキーK t 2を適用してコンテンツC 1暗号化してアンゴウカコンテンツC 1（K t 2）を生成する。

[0310] 次に、ステップS 2 4 5において、暗号化コンテンツC 2（K t 2）をメモ리카ードの汎用領域に記録する。

[0311] 次に、ステップS 2 4 6において、コンテンツC 1から生成したコンテンツハッシュリスト集合及びK t 2ハッシュ値に対する暗号化コンテンツ署名ECS 2 Sigを生成する。以下の署名データである。

$ECS 2 Sig = Sign (ECS \text{署名鍵}, M)$

ただし、

$M = \text{コンテンツ } C_1 \text{ のコンテンツハッシュリスト集合} \parallel K_{t2} \text{ ハッシュ値}$

である。

なお、署名生成には漏えいした暗号化コンテンツ署名発行装置の署名鍵（秘密鍵）を適用する。

[0312] 次に、ステップS247において、ステップS246で不正に生成したECS署名（ $ECS2Sig(C_1, K_{t1})$ ）を含むECSファイルを生成してメモ리카ードの汎用領域に記録する。

最後に、ステップS248において、ステップS241で生成した利用制御情報UR2を汎用領域に記録する。

この図28に示す一連の処理によって図27(b)に示す「すげ替えデータ」の記録処理が終了する。

このようなすげ替え処理によって、コンテンツC1に対して不正に生成した利用制御情報（UR2）が対応づけられる。なお、コンテンツC1は新たなタイトルキーKt2によって暗号化されて記録される。

[0313] 次に、図27(b)に示す「すげ替えデータ」を利用してコンテンツC1を再生するユーザ装置の処理について、図29に示すフローチャートを参照して説明する。

まず、ステップS261において、ユーザ装置は、メモ리카ードの汎用領域から再生予定の暗号化コンテンツC1（Kt2）と、このコンテンツに対して生成されたECSファイル（ $ECS2(C_1, K_{t2})$ ）を読み出す。

[0314] 次にステップS262において、メモ리카ードの汎用領域からコンテンツC1に対応付けて不正に生成した新たな利用制御情報（UR2）からタイトルキーの格納ブロックを示すブロック識別子、タイトルキー識別子を読み取る。

このブロック識別子、タイトルキー識別子は、改ざん前の正当な利用制御情報（UR1）のままに設定されている。

すなわち、このブロック識別子、タイトルキー識別子は、コンテンツC1

に対する正当なタイトルキー $K_t 1$ の格納されたブロックと、そのブロックに格納されたタイトルキーに対応する識別子である。

したがって、読み取りデータは、コンテンツ $C 1$ に対するタイトルキー変換データ、すなわち、

$$K_t 1 (+) (UR 1 || ECS 1 Sig) hash$$

となる。

- [0315] 次に、ステップ $S 2 6 3$ において、汎用領域から読み出した不正に生成した利用制御情報 ($UR 2$) と不正に生成した ECS ファイル ($ECS 2 (C 1, K_t 2)$) の連結データのハッシュ値を算出し、算出結果と、保護領域から読み出した上記のタイトルキー変換データとの排他的論理和演算 (XOR) を実行してコンテンツ $C 1$ に対応する復号用のタイトルキー $K_t 3$ の取得を試みる。

ここでは、 $K_t 3 = K_t 2$ となるタイトルキー $K_t 3$ が得られればタイトルキーの取得に成功したことになる。

- [0316] ステップ $S 2 6 3$ では、以下の式に従ってタイトルキー算出処理を試みる。

$$K_t 3 = (\text{保護領域からの読み出しデータ}) (+) (\text{汎用領域からの読み出しデータ})$$

$$= K_t 1 (+) (UR 1 || ECS 1 Sig) hash (+) (UR 2 || ECS 2 Sig) hash$$

上記タイトルキー算出式に従ってタイトルキー ($K_t 3$) を生成する。

なお、 $(+)$ は排他的論理和演算 (XOR) を意味する。

- [0317] しかし、上記タイトルキー算出式において、

$K_t 2$ は得られない。

上記算出式によってえられる値： $K_t 3$ は、 $K_t 1$ とも $K_t 2$ とも異なる値、すなわち、

$$K_t 3 \neq K_t 2$$

$$K_t 3 \neq K_t 1$$

となる。

[0318] この結果、ユーザ装置は、コンテンツC1の再暗号化に適用したタイトルキーK_{t2}を取得することはできず、コンテンツC1の復号、再生は失敗する。ステップS264の処理である。

[0319] また、ステップS265において、ユーザ装置は、予め規定された再生シーケンスに従って、汎用領域から読み出したECSファイルに含まれるECS発行装置署名(ECS_{sig})の検証処理を実行する。

以下の式に従って署名検証処理を行う。

$Verify(ECS\text{発行装置公開鍵}, ECS2\text{Sig}, M)$

ただし、

$Verify(k, S, M)$ は、データMに対する電子署名Sを検証鍵kを用いて検証する処理を示す。

M=コンテンツC1のコンテンツハッシュリスト集合||K_{t3}ハッシュである。

K_{t3}は、ステップS263で算出した値を利用することになる。

[0320] ECSファイルに格納したECS2_{sig}は、図28に示すフローのステップS246において生成した不正な署名であり、以下のデータである。

$ECS2\text{Sig} = Sign(ECS\text{署名鍵}, M)$

ただし、

M=コンテンツC1のコンテンツハッシュリスト集合||K_{t2}ハッシュ値

である。

[0321] このように、

署名検証に適用するデータMは、K_{t3}ハッシュ値を含むデータであるのに対して、

ECSファイルに格納された署名データECS2_{sig}は、K_{t2}ハッシュを含むMに対して生成されている。

従って、このステップS265における署名検証は失敗する。図29のス

テップ S 2 6 6 に記載の通りである。

[0322] このように、ユーザ装置は、図 2 7 (b) に示す「すげ替えデータ」を適用してコンテンツ C 1 の復号、再生を行おうとしても、
コンテンツ C 1 の復号に失敗、
E C S ファイルの署名検証に失敗、
これらの結果となり、結果としてコンテンツ C 1 を利用することはできない。

[0323] このように、メモ리카ードの保護領域に記録するタイトルキーを、
利用制御情報 (U R) と E C S 発行装置署名 (E C S S i g) との連結データのハッシュ値との排他的論理和 (X O R) 演算結果として格納することで、E C S 発行装置署名 (E C S S i g) に適用する E C S 発行装置の署名鍵 (秘密鍵) の漏えいが発生した場合にもコンテンツの不正利用を防止することが可能となる。

[0324] 例えば、コンテンツ提供サーバやユーザ装置が、漏えいした E C S 発行装置の署名鍵 (秘密鍵) を適用した不正処理、具体的には、暗号化コンテンツの暗号鍵のすげ替え処理や、利用制御情報の改ざんなどによるコンテンツ不正利用を防止可能となる。

[0325] [1 1 . 暗号化コンテンツ署名 (E C S) ファイルに記録したブロック識別子の適用処理について]

次に、暗号化コンテンツ署名 (E C S) ファイルに記録したブロック識別子 (P A D B l o c k N u m b e r) の適用処理について説明する。

[0326] 先に、図 9 を参照して説明したように、暗号化コンテンツ署名 (E C S) ファイルには、ブロック識別子 (P A D B l o c k N u m b e r) が記録される。

ブロック識別子 (P A D B l o c k N u m b e r) は、図 1 3 を参照して説明したように、コンテンツ提供装置 (C o n t e n t S e r v e r) 1 0 3 から、暗号化コンテンツ署名 (E C S) 発行装置 1 0 2 に通知されるデータであり、コンテンツ提供装置 1 0 3 がユーザ装置 1 0 4 に対して提

供したコンテンツに対応する暗号鍵であるタイトルキーを格納したメディアの保護領域のブロックの識別子である。これは、コンテンツ提供装置 103 が利用可能なメディアの保護領域におけるブロックの識別子である。

先に、図 3、図 6 等を参照して説明したように、コンテンツ提供装置の利用可能なメディアの保護領域のブロックは予め設定されており、これらのアクセス許容ブロック情報が記録される。

[0327] また、このブロック識別子 (P A D B l o c k N u m b e r) に対応する情報は、図 9 を参照して説明したように E C S 発行装置証明書にも記録される。

先に、図 9 を参照して説明したように、

(a) ブロック識別子開始番号 (S t a r t P A D B l o c k N u m b e r)

(b) ブロック識別子範囲 (P A D B l o c k N u m b e r C o u n t e r)

である。

[0328] (a) ブロック識別子開始番号 (S t a r t P A D B l o c k N u m b e r) は、E C S 発行装置 102 が、コンテンツ提供装置 103 に対して許容可能なメディアの保護領域のアクセス許容ブロックの開始番号である。

(b) ブロック識別子範囲 (P A D B l o c k N u m b e r C o u n t e r) は、E C S 発行装置 102 が、コンテンツ提供装置 103 に対して許容可能なメディアの保護領域のアクセス許容ブロックの開始番号からの範囲を示す情報である。

[0329] さらに、先に図 23 を参照して説明したように、ブロック識別子は、コンテンツ対応の利用制御情報 (U R) にも記録される。利用制御情報 (U R) に記録されるブロック識別子は、コンテンツに対応するタイトルキーを格納したブロックを示すブロック識別子である。

[0330] 図 30 に、

暗号化コンテンツ署名（ECS）ファイル、

利用制御情報（UR）、

これらに記録されたブロック識別子と保護領域のタイトルキー格納ブロック（図に示す例ではブロックk）との対応関係を示す。

[0331] 図30に示すように、メモ리카ードの汎用領域にはコンテンツに対応する、

暗号化コンテンツ署名（ECS）ファイル、

利用制御情報（UR）、

これらのデータが格納される。

また、保護領域のブロックkには、

コンテンツに対応するタイトルキーの変換データ、すなわち、

$K_t (+) UR || ECSSig) hash$

が格納される。

[0332] ユーザ装置に対して、コンテンツを提供するコンテンツ提供装置は、自己の有するホスト証明書（図5参照）に記録された保護領域アクセス権情報としてのブロック識別子と、ECS発行装置証明書中のブロック識別子としての書き込み許容ブロック領域情報とを比較する。

この比較結果に応じて、コンテンツ提供の可否を判定する。

[0333] また、コンテンツ再生を行うユーザ装置は、利用制御情報中のブロック識別子とECSファイル中のブロック識別子とを比較する。

この比較結果に応じて、コンテンツ再生の可否を判定する。

[0334] まず、コンテンツ提供サーバにおけるブロック識別子を利用したコンテンツ提供の可否判定シーケンスについて図31に示すフローチャートを参照して説明する。

[0335] なお、図31に示すフローチャートのステップS401の前処理として、コンテンツ提供装置は、暗号化コンテンツ署名ファイル（ECSファイル）発行装置から受信した暗号化コンテンツ署名ファイル（ECSファイル）に設定されたECS発行装置署名を適用した署名検証を実行する。

この署名検証が成立し、暗号化コンテンツ署名ファイル（ECSファイル）の正当性が確認され場合は、さらに、暗号化コンテンツ署名ファイル（ECSファイル）に格納されたECS発行装置証明書の署名検証を実行する。これらの2つの署名検証が成立したことを条件としてステップS401以下の処理を行う。

[0336] 上記2つの署名検証の少なくともいずれかが成立しなかった場合は、暗号化コンテンツ署名ファイル（ECSファイル）またはECS発行装置証明書の正当性が確認されないので、ステップS401以下の処理は実行されない。この場合はコンテンツ提供処理も実行しないことになる。

なお、暗号化コンテンツ署名ファイル（ECSファイル）に格納されるコンテンツハッシュリスト集合の元データであるコンテンツハッシュは、暗号化コンテンツのハッシュまたは暗号化前のコンテンツのハッシュ、いずれの設定としてもよい。

[0337] 暗号化コンテンツ署名ファイル（ECSファイル）と、ECS発行装置証明書の2つの署名検証が成立し、暗号化コンテンツ署名ファイル（ECSファイル）とECS発行装置証明書の正当性が確認された場合、コンテンツ提供装置は、ステップS401の処理を実行する。

コンテンツ提供装置は、まず、ステップS401において、ECSファイル内のECS発行装置証明書を読み出して、ECS発行装置証明書に記録されたブロック識別子情報を読み出す。

[0338] このステップS401の処理の詳細について、図32に示すフローを参照して説明する。

ステップS421において、ECS発行装置証明書内のブロック識別子開始番号（Start PAD Block Number）を読み出す。

ブロック識別子開始番号（Start PAD Block Number）は、ECS発行装置102が、コンテンツ提供装置103に対して許容したメディアの保護領域のアクセス許容ブロックの開始番号である。

[0339] 次に、ステップS422において、ECS発行装置証明書内のブロック識

別子開始番号 (Start PAD Block Number) が $0 \times F F F F F F F F$ であるか否かを判定する。

なお、ブロック識別子開始番号 (Start PAD Block Number) が $0 \times F F F F F F F F$ である場合は全ブロックに対するアクセス許容が設定された状態に対応する。

[0340] ステップ S 4 2 2 において、ブロック識別子開始番号 (Start PAD Block Number) が $0 \times F F F F F F F F$ であると判定した場合は、ステップ S 4 2 3 に進み、メディアの保護領域に設定された前ブロックをアクセス許容ブロックとみなす。

[0341] 一方、ステップ S 4 2 2 において、ブロック識別子開始番号 (Start PAD Block Number) が $0 \times F F F F F F F F$ でないと判定した場合は、ステップ S 4 2 4 に進む。

ステップ S 4 2 4 では、ECS 発行装置証明書内のブロック識別子範囲情報 (PAD Block Number Counter) を読みだす。

ブロック識別子範囲 (PAD Block Number Counter) は、ECS 発行装置 1 0 2 が、コンテンツ提供装置 1 0 3 に対して許容可能なメディアの保護領域のアクセス許容ブロックの開始番号からの範囲を示す情報である。

[0342] 次のステップ S 4 2 5 ~ S 4 2 8 の処理は、ブロック識別子を示す変数 I を 0 から順次、1, 2, 3... とインクリメントして実行する繰り返しルーチンである。

まずステップ S 4 2 5 において

変数: $I = 1$ とする。

[0343] 次に、ステップ S 4 2 6 において、ブロック識別子開始番号 (Start PAD Block Number) + I をブロック識別子リスト (PAD Block Number List) に追加する。

[0344] 次に、ステップ S 4 2 7 において、

$I = I + 1$

とする。

[0345] 次に、ステップS 4 2 8において、I がブロック識別子範囲情報（P A D B l o c k N u m b e r C o u n t e r）と等しいか否かを判定する。

等しければ、処理を終了する。等しくなければ、ステップS 4 2 6に戻り、処理を繰り返す。

この処理に従って、図3 1に示すフローのステップS 4 0 1の処理が行われる。

[0346] ステップS 4 0 1では、E C S発行装置証明書内のブロック識別子開始番号（S t a r t P A D B l o c k N u m b e r）と、ブロック識別子範囲情報（P A D B l o c k N u m b e r C o u n t e r）を適用して、E C S発行装置証明書において規定されたアクセス許容範囲を算出しこれをアクセス許容ブロック識別子リストとして設定する。

[0347] 次に、ステップS 4 0 2において、ステップS 4 0 1で生成したアクセス許容ブロック識別子リストに、暗号化コンテンツ署名（E C S）ファイルの記録データとして記載されたブロック識別子（P A D B l o c k N u m b e r）が含まれるか否かを判定する。

[0348] 含まれていなければ、ステップS 4 0 5に進み、ユーザ装置に対するコンテンツ提供処理は実行しない。

一方、含まれている場合は、ステップS 4 0 3に進む。

[0349] ステップS 4 0 3では、暗号化コンテンツ署名（E C S）ファイルの記録データとして記載されたブロック識別子（P A D B l o c k N u m b e r）が、利用制御情報（U R）に記録されたブロック識別子と一致するか否かを判定する。

一致しなければ、ステップS 4 0 5に進み、ユーザ装置に対するコンテンツ提供処理は実行しない。

一方、一致した場合は、ステップS 4 0 4に進み、ユーザ装置に対するコンテンツ提供を実行する。

[0350] このように、コンテンツ提供装置は、

(a) 暗号化コンテンツ署名 (ECS) ファイルに記録されたブロック識別子 (PAD Block Number) が、ECS 発行装置証明書に記録されたアクセス許容ブロックの範囲内であること、

(b) 暗号化コンテンツ署名 (ECS) ファイルに記録されたブロック識別子 (PAD Block Number) が、利用制御情報 (UR) に記録されたブロック識別子に一致すること、

これら (a)、(b) の条件を満足するか否かを判定し、満足する場合にのみ、ユーザ装置に対するコンテンツ提供を実行する。

[0351] 次に、図 33 に示すフローチャートを参照して、コンテンツ再生処理を実行するユーザ装置におけるブロック識別子の適用処理について説明する。

[0352] なお、ユーザ装置は、図 33 に示すステップ S 4 5 1 以前に、コンテンツ提供装置から受信した暗号化コンテンツ署名ファイル (ECS ファイル) に設定された ECS 発行装置署名を適用した署名検証を実行する。

この署名検証が成立し、暗号化コンテンツ署名ファイル (ECS ファイル) の正当性が確認され場合は、さらに、暗号化コンテンツ署名ファイル (ECS ファイル) に格納された ECS 発行装置証明書の署名検証を実行する。これらの 2 つの署名検証が成立したことを条件としてステップ S 4 5 1 以下の処理を行う。

[0353] 上記 2 つの署名検証の少なくともいずれかが成立しなかった場合は、暗号化コンテンツ署名ファイル (ECS ファイル) または ECS 発行装置証明書の正当性が確認されないので、ステップ S 4 5 1 以下の処理は実行されない。この場合はコンテンツ再生処理も実行しないことになる。

[0354] 暗号化コンテンツ署名ファイル (ECS ファイル) と、ECS 発行装置証明書の 2 つの署名検証が成立し、暗号化コンテンツ署名ファイル (ECS ファイル) と ECS 発行装置証明書の正当性が確認された場合、ユーザ装置は、ステップ S 4 5 1 の処理を実行する。

[0355] ステップ S 4 5 1 は、先にサーバ提供装置の処理として説明した図 31 に

示すフローのステップS401の処理と同様の処理である。すなわち、図32に示すフローを参照して詳細を説明したように、ECS発行装置証明書内のブロック識別子開始番号（Start PAD Block Number）と、ブロック識別子範囲情報（PAD Block Number Counter）を適用して、ECS発行装置証明書において規定されたアクセス許容範囲を算出しこれをアクセス許容ブロック識別子リストとして設定する。

[0356] 次に、ステップS452において、ステップS451で生成したアクセス許容ブロック識別子リストに、暗号化コンテンツ署名（ECS）ファイルの記録データとして記載されたブロック識別子（PAD Block Number）が含まれるか否かを判定する。

[0357] 含まれていなければ、ステップS455に進み、コンテンツ再生処理は実行しない。

一方、含まれている場合は、ステップS453に進む。

[0358] ステップS453では、暗号化コンテンツ署名（ECS）ファイルの記録データとして記載されたブロック識別子（PAD Block Number）が、利用制御情報（UR）に記載されたブロック識別子と一致するか否かを判定する。

一致しなければ、ステップS455に進み、コンテンツ再生処理は実行しない。

一方、一致した場合は、ステップS454に進み、コンテンツ再生を実行する。

[0359] なお、コンテンツ再生処理の開始前に、さらに、暗号化コンテンツの復号に適用するタイトルキーの取得や生成処理、さらに、暗号化コンテンツ署名ファイルに含まれるコンテンツハッシュリストを適用したハッシュ値照合処理を実行する。ハッシュ値照合において照合が成立し、コンテンツの改ざんのないことが確認された場合にコンテンツの再生が許容されることになる。

[0360] このように、コンテンツ再生を実行するユーザ装置は、

(a) 暗号化コンテンツ署名 (ECS) ファイルに記録されたブロック識別子 (PAD Block Number) が、ECS 発行装置証明書に記録されたアクセス許容ブロックの範囲内であること、

(b) 暗号化コンテンツ署名 (ECS) ファイルに記録されたブロック識別子 (PAD Block Number) が、利用制御情報 (UR) に記録されたブロック識別子に一致すること、

これら (a)、(b) の条件を満足するか否かを判定し、満足する場合にのみ、コンテンツ再生を実行する。

[0361] [12. 各装置のハードウェア構成例について]

最後に、図34を参照して、上述した処理を実行する各装置のハードウェア構成例について説明する。

図34は、図7、図8に示すユーザ装置104、コンテンツ提供装置103、暗号化コンテンツ署名発行装置102、ライセンス発行装置101のいずれにも適用可能な情報処理装置のハードウェア構成例を示している。

[0362] CPU (Central Processing Unit) 701は、ROM (Read Only Memory) 702、または記憶部708に記憶されているプログラムに従って各種の処理を実行するデータ処理部として機能する。例えば、上述した各フローチャートに従った処理を実行する。RAM (Random Access Memory) 703には、CPU 701が実行するプログラムやデータなどが適宜記憶される。これらのCPU 701、ROM 702、およびRAM 703は、バス704により相互に接続されている。

[0363] CPU 701はバス704を介して入出力インタフェース705に接続され、入出力インタフェース705には、各種スイッチ、キーボード、マウス、マイクロホンなどよりなる入力部706、ディスプレイ、スピーカなどよりなる出力部707が接続されている。CPU 701は、入力部706から入力される指令に対応して各種の処理を実行し、処理結果を例えば出力部707に出力する。

[0364] 入出力インタフェース705に接続されている記憶部708は、例えばハードディスク等からなり、CPU701が実行するプログラムや各種のデータを記憶する。通信部709は、インターネットやローカルエリアネットワークなどのネットワークを介して外部の装置と通信する。

[0365] 入出力インタフェース705に接続されているドライブ710は、磁気ディスク、光ディスク、光磁気ディスク、あるいはメモリカード等の半導体メモリなどのリムーバブルメディア711を駆動し、記録されているコンテンツや鍵情報等の各種データを取得する。例えば、取得されたコンテンツや鍵データを用いて、CPUによって実行する再生プログラムに従ってコンテンツの復号、再生処理などが行われる。

[0366] 図35は、情報記憶装置であるメモリカードのハードウェア構成例を示している。

CPU (Central Processing Unit) 801は、ROM (Read Only Memory) 802、または記憶部807に記憶されているプログラムに従って各種の処理を実行するデータ処理部として機能する。例えば、上述の各実施例において説明したサーバやホスト機器との通信処理やデータの記憶部807に対する書き込み、読み取り等の処理、記憶部807の保護領域811の区分領域単位のアクセス可否判定処理等を実行する。RAM (Random Access Memory) 803には、CPU801が実行するプログラムやデータなどが適宜記憶される。これらのCPU801、ROM802、およびRAM803は、バス804により相互に接続されている。

[0367] CPU801はバス804を介して入出力インタフェース805に接続され、入出力インタフェース805には、通信部806、記憶部807が接続されている。

[0368] 入出力インタフェース805に接続されている通信部804は、例えばサーバやホストとの通信を実行する。記憶部807は、データの記憶領域であり、先に説明したようにアクセス制限のある保護領域 (Protected

Area) 811、自由にデータ記録読み取りができる汎用領域 (General Purpose Area) 812を有する。

[0369] なお、上述した実施例では、コンテンツ提供装置が提供するコンテンツは暗号化コンテンツである例を代表例として説明したが、本開示の構成は、提供コンテンツが暗号化コンテンツである場合に限らず、暗号化されていない平文コンテンツである場合にも適用可能である。なお、コンテンツが平文コンテンツである場合、上述の実施例で説明したタイトルキーは既知のデータ列、例えばオール0の値からなるキーデータであるものとして、上述した暗号化コンテンツの提供処理と同様の処理を行うことができる。

[0370] [13. 本開示の構成のまとめ]

以上、特定の実施例を参照しながら、本開示の実施例について詳解してきた。しかしながら、本開示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開示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。本開示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。

[0371] なお、本明細書において開示した技術は、以下のような構成をとることができる。

(1) 暗号化コンテンツおよび暗号化コンテンツの復号に適用する暗号鍵を格納する記憶部を有し、

前記記憶部は、前記暗号鍵を前記暗号化コンテンツに対応して設定された暗号化コンテンツ署名ファイルの構成データである電子署名との演算によって生成された変換暗号鍵を格納し、

前記電子署名は、前記暗号化コンテンツの構成データおよび前記暗号鍵を含むデータに対する電子署名であり、

前記記憶部から前記暗号化コンテンツを読み出して復号処理を実行する再生装置に、前記変換暗号鍵に対する電子署名の適用演算による暗号鍵取得を行わせることを可能とした情報記憶装置。

[0372] (2) 前記変換暗号鍵は、前記暗号化コンテンツに対応して設定される利

用制御情報と、前記電子署名との連結データに対するハッシュ値と、前記暗号鍵との排他的論理和演算結果である前記（１）に記載の情報記憶装置。

（３）前記記憶部は、アクセス制限の設定された保護領域を有し、前記変換暗号鍵を、前記保護領域に格納した構成である前記（１）または（２）に記載の情報記憶装置。

（４）前記情報記憶装置は、前記保護領域に対するアクセス要求装置から受領した証明書に基づいて、前記保護領域に対するアクセス可否を判定するデータ処理部を有する前記（３）に記載の情報記憶装置。

[0373] （５）前記記憶部は、アクセス制限の設定された保護領域と、アクセス制限のない汎用領域を有し、前記変換暗号鍵を、前記保護領域に格納し、前記暗号化コンテンツと、前記暗号化コンテンツ署名ファイルを、前記汎用領域に格納した構成である前記（１）～（４）いずれかに記載の情報記憶装置。

（６）前記電子署名は、前記暗号化コンテンツの構成データおよび前記暗号鍵、さらに、前記暗号化コンテンツ署名ファイルの構成データを含むデータに対する電子署名である前記（１）～（５）いずれかに記載の情報記憶装置。

（７）前記電子署名は、前記暗号化コンテンツ署名ファイルの構成データである前記暗号化コンテンツ署名ファイルの発行日時情報を含むデータに対する電子署名である前記（６）に記載の情報記憶装置。

[0374] （８） メディアに記録された暗号化コンテンツの復号および再生処理を実行するデータ処理部を有し、

前記データ処理部は、

前記暗号化コンテンツの復号処理に際して、前記メディアに記録された前記暗号化コンテンツの復号に適用する暗号鍵の変換データである変換暗号鍵を読み出し、該変換暗号鍵に対する演算処理を実行して暗号鍵の取得処理を実行し、

前記変換暗号鍵は、

前記暗号鍵を前記暗号化コンテンツに対応して設定された暗号化コンテン

ツ署名ファイルの構成データである電子署名との演算によって生成された変換暗号鍵であり、

前記データ処理部は、

前記メディアに記録された暗号化コンテンツ署名ファイルの構成データである電子署名を取得し、取得した電子署名を適用した演算処理を実行して暗号鍵の取得処理を実行する情報処理装置。

[0375] (9) 前記電子署名は、前記暗号化コンテンツの構成データおよび前記暗号鍵を含むデータに対する電子署名である前記(8)に記載の情報処理装置。

(10) 前記変換暗号鍵は、前記暗号化コンテンツに対応して設定される利用制御情報と、前記電子署名との連結データに対するハッシュ値と、前記暗号鍵との排他的論理和演算結果であり、前記データ処理部は、前記メディアに記録された暗号化コンテンツ署名ファイルの構成データである電子署名と、前記メディアに記録された利用制御情報を取得し、取得したデータを適用した演算処理を実行して暗号鍵の取得処理を実行する前記(8)または(9)に記載の情報処理装置。

(11) 前記データ処理部は、前記メディアに記録された暗号化コンテンツ署名ファイルの構成データである電子署名に対する署名検証処理を実行し、該署名検証処理に成功し、前記暗号化コンテンツ署名ファイルの正当性を確認したことを条件として、前記暗号鍵の取得処理を行う前記(8)～(10)いずれかに記載の情報処理装置。

[0376] (12) メディアに記録する暗号化コンテンツと、該暗号化コンテンツの復号に適用する暗号鍵の変換データである変換暗号鍵を出力するデータ処理部を有し、

前記データ処理部は、

前記暗号化コンテンツに対応して設定された暗号化コンテンツ署名ファイルの構成データである電子署名であり、前記暗号化コンテンツの構成データおよび前記暗号鍵を含むデータに対する電子署名と、前記暗号鍵の演算処理

により、前記変換暗号鍵を生成する情報処理装置。

(13) 前記データ処理部は、前記暗号化コンテンツに対応して設定される利用制御情報と、前記電子署名との連結データに対するハッシュ値と、前記暗号鍵との排他的論理和演算を実行して前記変換暗号鍵を生成する前記(12)に記載の情報処理装置。

[0377] さらに、上記した装置およびシステムにおいて実行する処理の方法や、処理を実行させるプログラムも本開示の構成に含まれる。

[0378] 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。

[0379] 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に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。

産業上の利用可能性

[0380] 以上、説明したように、本開示の一実施例の構成によれば、コンテンツの不正利用を効果的に防止する装置、方法が実現される。

具体的には、暗号化コンテンツの復号処理に際して、メディアに記録された暗号化コンテンツの復号に適用する暗号鍵の変換データである変換暗号鍵

を読み出し、変換暗号鍵に対する演算処理を実行して暗号鍵の取得処理を実行する。変換暗号鍵は、暗号鍵と、暗号化コンテンツに対応して設定された暗号化コンテンツ署名ファイルの構成データである電子署名との演算によって生成された変換暗号鍵であり、再生装置は、メディアに記録された暗号化コンテンツ署名ファイルの構成データである電子署名を取得し、取得した電子署名を適用した演算処理を実行して暗号鍵の取得処理を実行する。電子署名は、暗号化コンテンツの構成データおよび暗号鍵を含むデータに対する電子署名として設定される。

この暗号化コンテンツ署名ファイルの署名データを変換暗号鍵の構成データとすることで、鍵の掛け替え処理などによるコンテンツ不正利用を防止することが可能となる。

符号の説明

- [0381] 1 1 放送局
- 1 2 コンテンツサーバ
- 2 1 記録再生専用器
- 2 2 P C
- 2 3 携帯端末
- 3 1 メモリカード
- 5 1 保護領域 (P r o t e c t e d A r e a)
- 5 2 汎用領域 (G e n e r a l P u r p o s e A r e a)
- 6 1 サーバ A
- 6 2 サーバ B
- 6 3 ホスト
- 6 4 サーバ C
- 6 5 サーバ D
- 7 0 メモリカード
- 8 0 保護領域 (P r o t e c t e d A r e a)
- 8 1 ブロック # 0

- 8 2 ブロック # 1
 - 9 0 汎用領域 (General Purpose Area)
 - 1 0 1 ライセンス発行装置
 - 1 0 2 暗号化コンテンツ署名 (E C S) 発行装置
 - 1 0 3 コンテンツ提供装置
 - 1 0 4 ユーザ装置
 - 1 8 1 コンテンツ
 - 1 8 2 タイトルキー
 - 1 8 3 コンテンツハッシュリスト集合
- 2 0 1 コンテンツ提供装置 (サーバ)
- 2 0 2 ユーザ装置 (ホスト)
- 2 1 0 メモリカード
 - 2 1 1 保護領域 (Protected Area)
 - 2 1 2 汎用領域 (General Purpose Area)
- 2 2 1 ブロック # 0
- 7 0 1 C P U
- 7 0 2 R O M
- 7 0 3 R A M
- 7 0 4 バス
- 7 0 5 入出力インタフェース
- 7 0 6 入力部
- 7 0 7 出力部
- 7 0 8 記憶部
- 7 0 9 通信部
- 7 1 0 ドライブ
- 7 1 1 リムーバブルメディア
- 8 0 1 C P U
- 8 0 2 R O M

803 RAM

804 バス

805 入出力インタフェース

806 通信部

807 記憶部

811 保護領域 (Protected Area)

812 汎用領域 (General Purpose Area)

請求の範囲

- [請求項1] 暗号化コンテンツおよび暗号化コンテンツの復号に適用する暗号鍵を格納する記憶部を有し、
- 前記記憶部は、前記暗号鍵を前記暗号化コンテンツに対応して設定された暗号化コンテンツ署名ファイルの構成データである電子署名との演算によって生成された変換暗号鍵を格納し、
- 前記電子署名は、前記暗号化コンテンツの構成データおよび前記暗号鍵を含むデータに対する電子署名であり、
- 前記記憶部から前記暗号化コンテンツを読み出して復号処理を実行する再生装置に、前記変換暗号鍵に対する電子署名の適用演算による暗号鍵取得を行わせることを可能とした情報記憶装置。
- [請求項2] 前記変換暗号鍵は、
- 前記暗号化コンテンツに対応して設定される利用制御情報と、前記電子署名との連結データに対するハッシュ値と、前記暗号鍵との排他的論理和演算結果である請求項1に記載の情報記憶装置。
- [請求項3] 前記記憶部は、アクセス制限の設定された保護領域を有し、
- 前記変換暗号鍵を、前記保護領域に格納した構成である請求項1に記載の情報記憶装置。
- [請求項4] 前記情報記憶装置は、
- 前記保護領域に対するアクセス要求装置から受領した証明書に基づいて、前記保護領域に対するアクセス可否を判定するデータ処理部を有する請求項3に記載の情報記憶装置。
- [請求項5] 前記記憶部は、アクセス制限の設定された保護領域と、アクセス制限のない汎用領域を有し、
- 前記変換暗号鍵を、前記保護領域に格納し、
- 前記暗号化コンテンツと、前記暗号化コンテンツ署名ファイルを、前記汎用領域に格納した構成である請求項1に記載の情報記憶装置。
- [請求項6] 前記電子署名は、前記暗号化コンテンツの構成データおよび前記暗

号鍵、さらに、前記暗号化コンテンツ署名ファイルの構成データを含むデータに対する電子署名である請求項 1 に記載の情報記憶装置。

[請求項7] 前記電子署名は、前記暗号化コンテンツ署名ファイルの構成データである前記暗号化コンテンツ署名ファイルの発行日時情報を含むデータに対する電子署名である請求項 6 に記載の情報記憶装置。

[請求項8] メディアに記録された暗号化コンテンツの復号および再生処理を実行するデータ処理部を有し、

前記データ処理部は、

前記暗号化コンテンツの復号処理に際して、前記メディアに記録された前記暗号化コンテンツの復号に適用する暗号鍵の変換データである変換暗号鍵を読み出し、該変換暗号鍵に対する演算処理を実行して暗号鍵の取得処理を実行し、

前記変換暗号鍵は、

前記暗号鍵を前記暗号化コンテンツに対応して設定された暗号化コンテンツ署名ファイルの構成データである電子署名との演算によって生成された変換暗号鍵であり、

前記データ処理部は、

前記メディアに記録された暗号化コンテンツ署名ファイルの構成データである電子署名を取得し、取得した電子署名を適用した演算処理を実行して暗号鍵の取得処理を実行する情報処理装置。

[請求項9] 前記電子署名は、前記暗号化コンテンツの構成データおよび前記暗号鍵を含むデータに対する電子署名である請求項 8 に記載の情報処理装置。

[請求項10] 前記変換暗号鍵は、

前記暗号化コンテンツに対応して設定される利用制御情報と、前記電子署名との連結データに対するハッシュ値と、前記暗号鍵との排他的論理和演算結果であり、

前記データ処理部は、

前記メディアに記録された暗号化コンテンツ署名ファイルの構成データである電子署名と、

前記メディアに記録された利用制御情報を取得し、取得したデータを適用した演算処理を実行して暗号鍵の取得処理を実行する請求項 8 に記載の情報処理装置。

[請求項11]

前記データ処理部は、

前記メディアに記録された暗号化コンテンツ署名ファイルの構成データである電子署名に対する署名検証処理を実行し、

該署名検証処理に成功し、前記暗号化コンテンツ署名ファイルの正当性を確認したことを条件として、前記暗号鍵の取得処理を行う請求項 8 に記載の情報処理装置。

[請求項12]

メディアに記録する暗号化コンテンツと、該暗号化コンテンツの復号に適用する暗号鍵の変換データである変換暗号鍵を出力するデータ処理部を有し、

前記データ処理部は、

前記暗号化コンテンツに対応して設定された暗号化コンテンツ署名ファイルの構成データである電子署名であり、前記暗号化コンテンツの構成データおよび前記暗号鍵を含むデータに対する電子署名と、前記暗号鍵の演算処理により、前記変換暗号鍵を生成する情報処理装置。

[請求項13]

前記データ処理部は、

前記暗号化コンテンツに対応して設定される利用制御情報と、前記電子署名との連結データに対するハッシュ値と、前記暗号鍵との排他的論理和演算を実行して前記変換暗号鍵を生成する請求項 12 に記載の情報処理装置。

[請求項14]

情報処理装置において実行する情報処理方法であり、

データ処理部が、メディアに記録された暗号化コンテンツの復号処理に際して、復号に適用する暗号鍵の変換データである変換暗号鍵を

読み出し、該変換暗号鍵に対する演算処理を実行して暗号鍵の取得処理を行うデータ処理ステップを実行し、

前記変換暗号鍵は、

前記暗号鍵を前記暗号化コンテンツに対応して設定された暗号化コンテンツ署名ファイルの構成データである電子署名との演算によって生成された変換暗号鍵であり、

前記データ処理部は、前記データ処理部ステップにおいて、

前記メディアに記録された暗号化コンテンツ署名ファイルから前記電子署名を取得し、取得した電子署名を適用した演算処理を実行して暗号鍵の取得処理を実行する情報処理方法。

[請求項15]

情報処理装置において実行する情報処理方法であり、

データ処理部が、メディアに記録する暗号化コンテンツと、該暗号化コンテンツの復号に適用する暗号鍵の変換データである変換暗号鍵を出力するデータ処理ステップを実行し、

前記データ処理ステップにおいて、

前記暗号化コンテンツに対応して設定された暗号化コンテンツ署名ファイルの構成データである電子署名であり、前記暗号化コンテンツの構成データおよび前記暗号鍵を含むデータに対する電子署名と、前記暗号鍵の演算処理により、前記変換暗号鍵を生成する情報処理方法。

[請求項16]

情報処理装置において情報処理を実行させるプログラムであり、

データ処理部に、メディアに記録された暗号化コンテンツの復号処理に際して、復号に適用する暗号鍵の変換データである変換暗号鍵の読み出し処理と、該変換暗号鍵に対する演算処理による暗号鍵の取得処理を行うデータ処理ステップを実行させ、

前記変換暗号鍵は、

前記暗号鍵を前記暗号化コンテンツに対応して設定された暗号化コンテンツ署名ファイルの構成データである電子署名との演算によって

生成された変換暗号鍵であり、

前記データ処理部ステップにおいて、

前記メディアに記録された暗号化コンテンツ署名ファイルから前記電子署名の取得処理と、取得した電子署名を適用した演算処理による暗号鍵の取得処理を実行させるプログラム。

[請求項17]

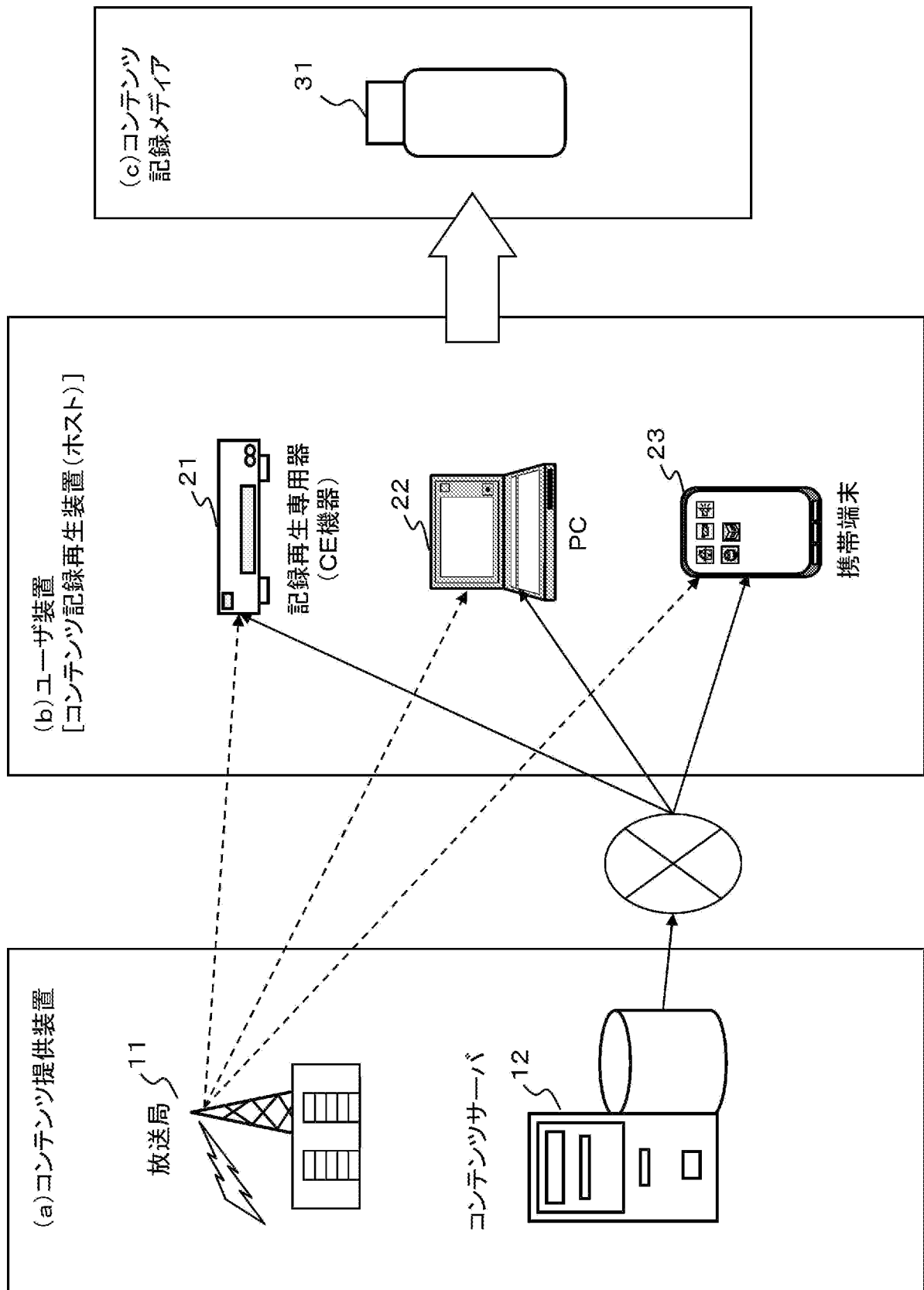
情報処理装置において情報処理を実行させるプログラムであり、

データ処理部に、メディアに記録する暗号化コンテンツと、該暗号化コンテンツの復号に適用する暗号鍵の変換データである変換暗号鍵を出力するデータ処理ステップを実行させ、

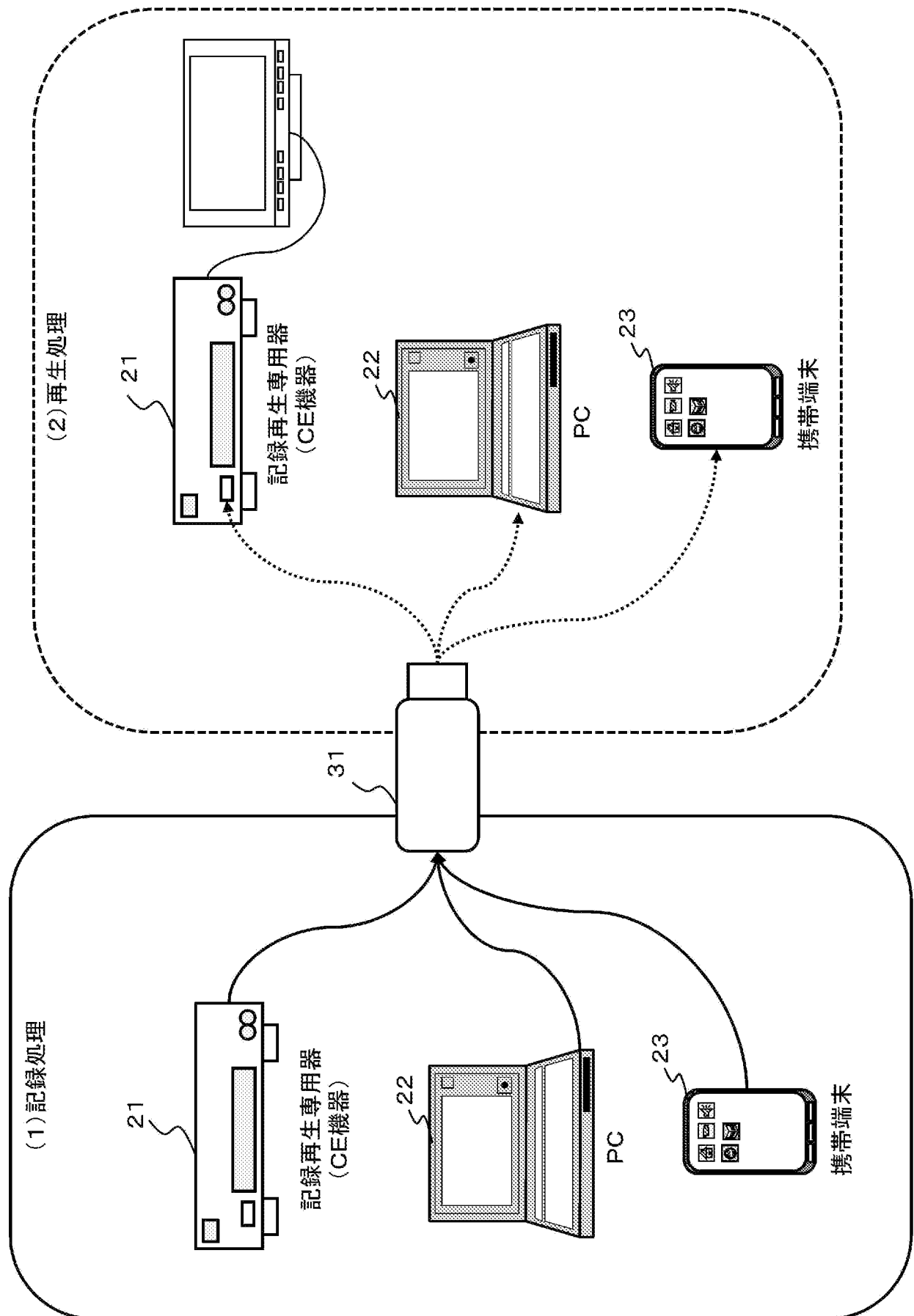
前記データ処理ステップにおいて、

前記暗号化コンテンツに対応して設定された暗号化コンテンツ署名ファイルの構成データである電子署名であり、前記暗号化コンテンツの構成データおよび前記暗号鍵を含むデータに対する電子署名と、前記暗号鍵の演算処理により、前記変換暗号鍵を生成させるプログラム。

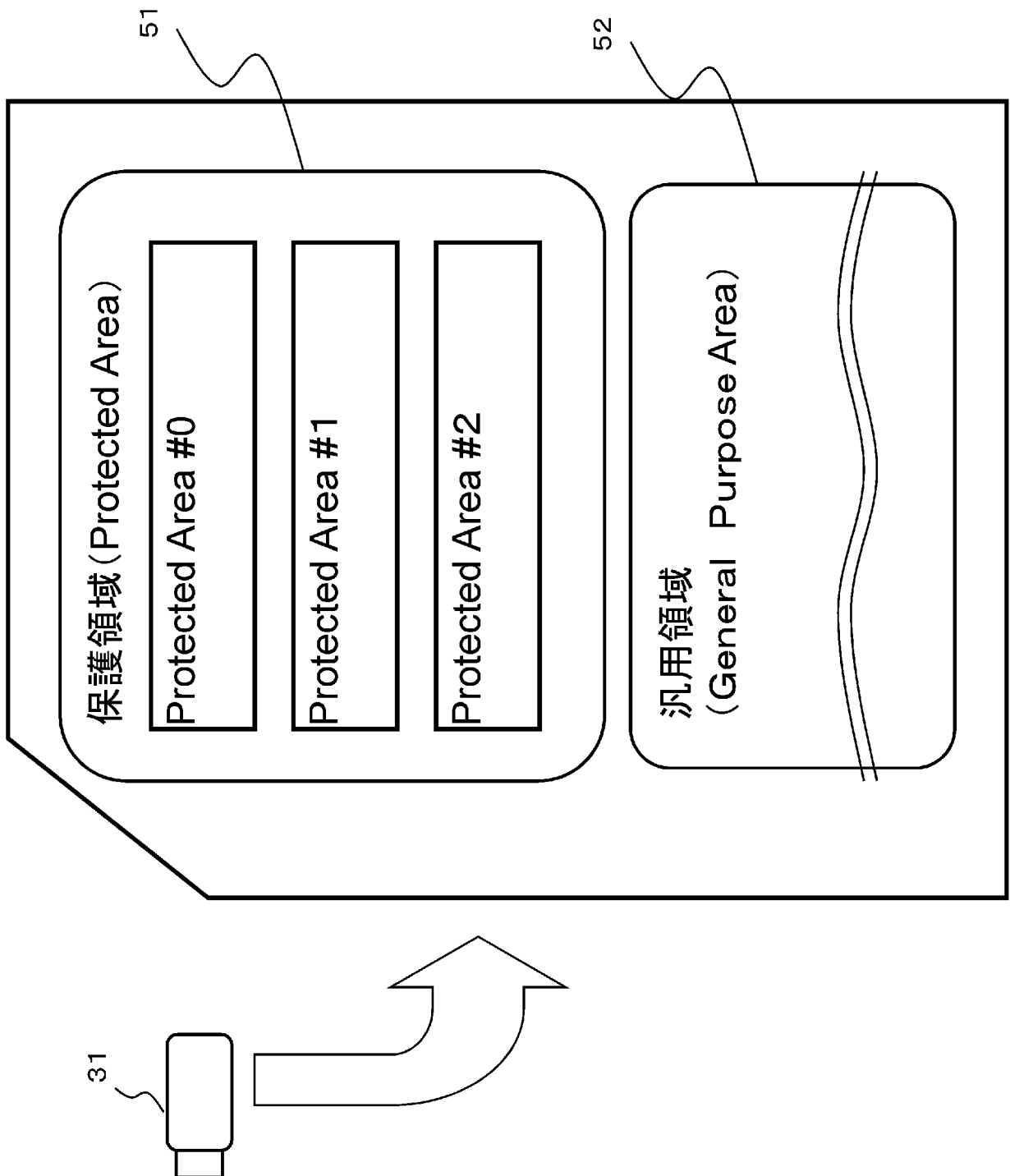
[図1]



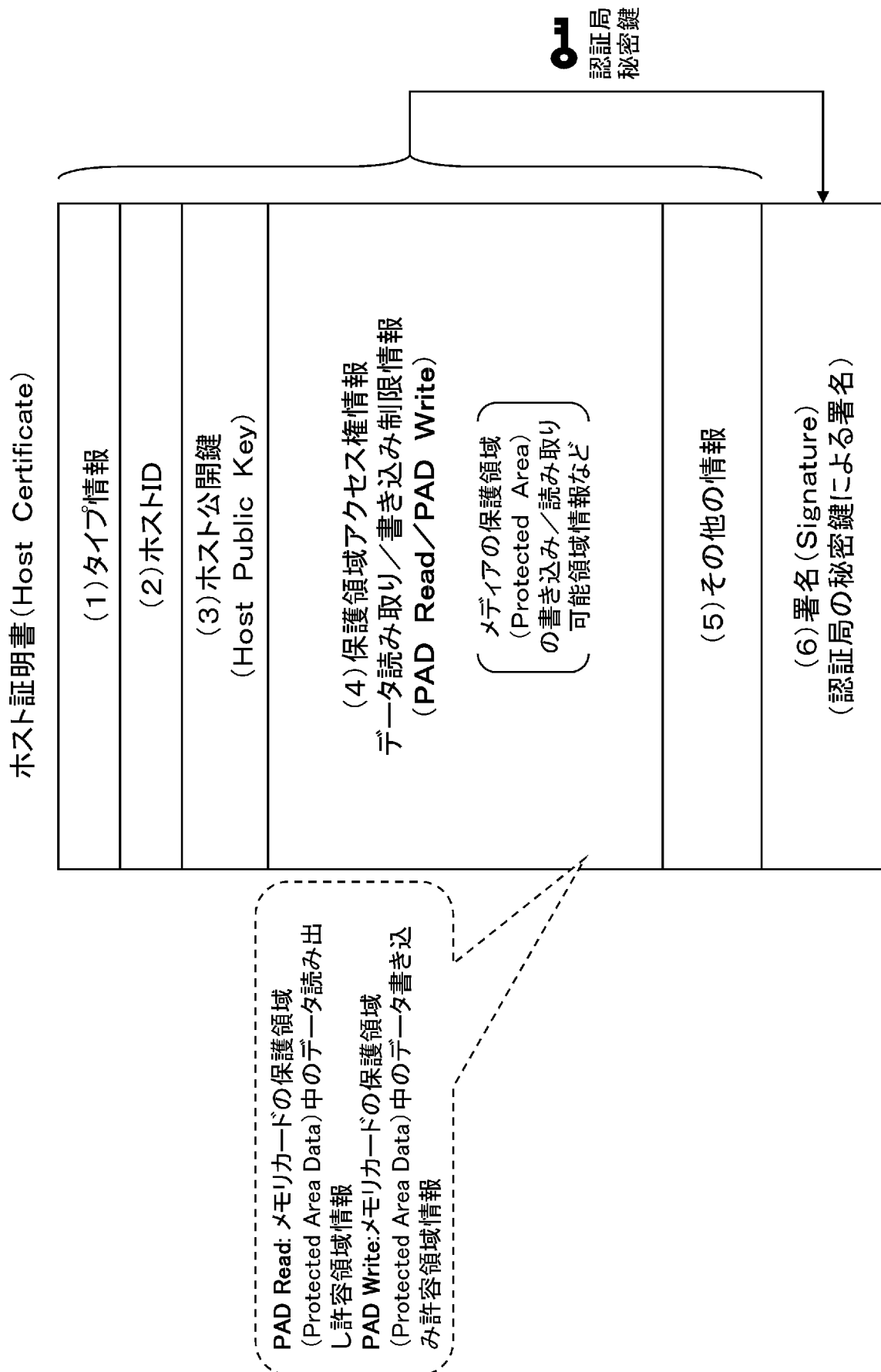
[図2]



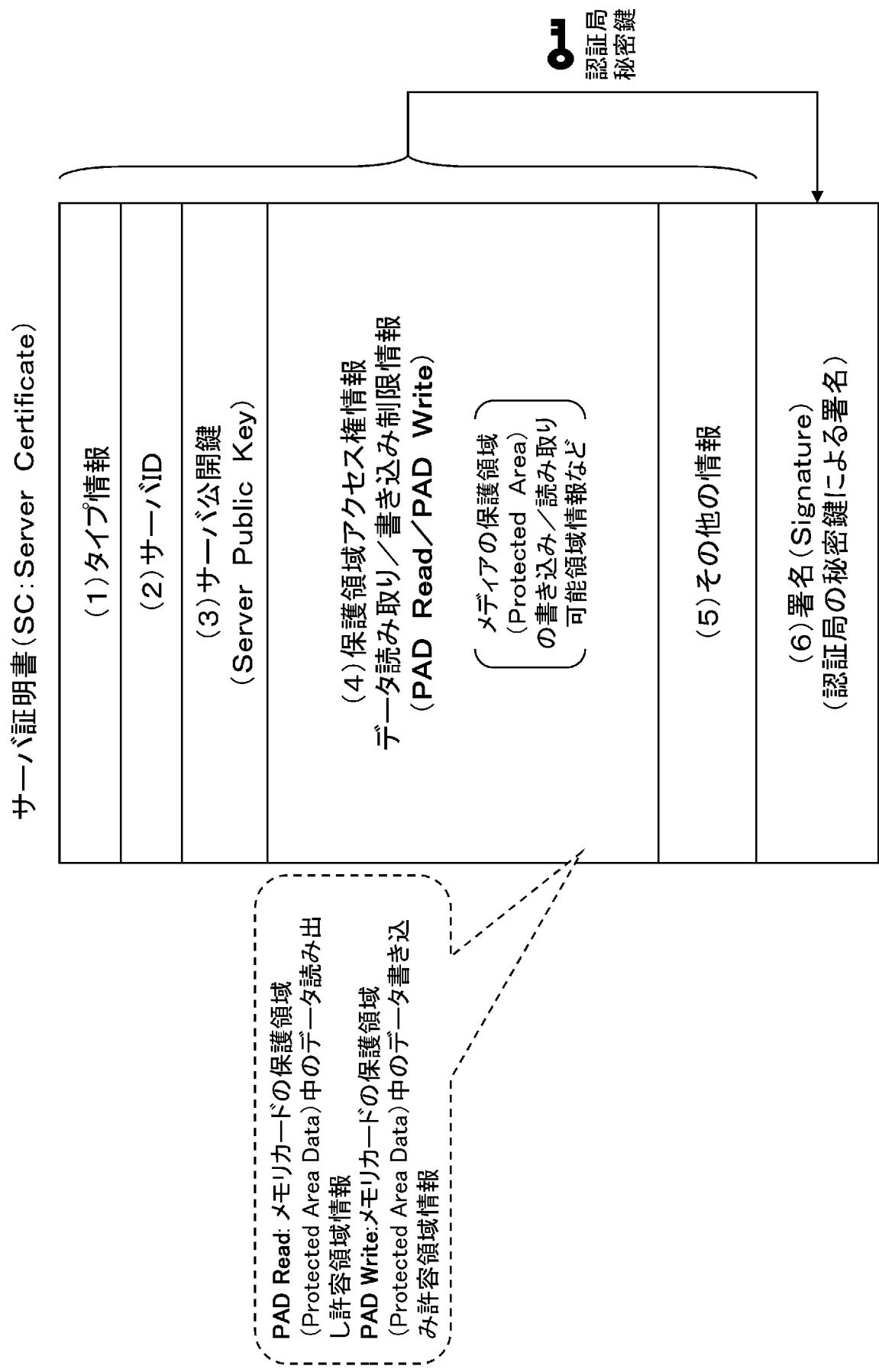
[図3]



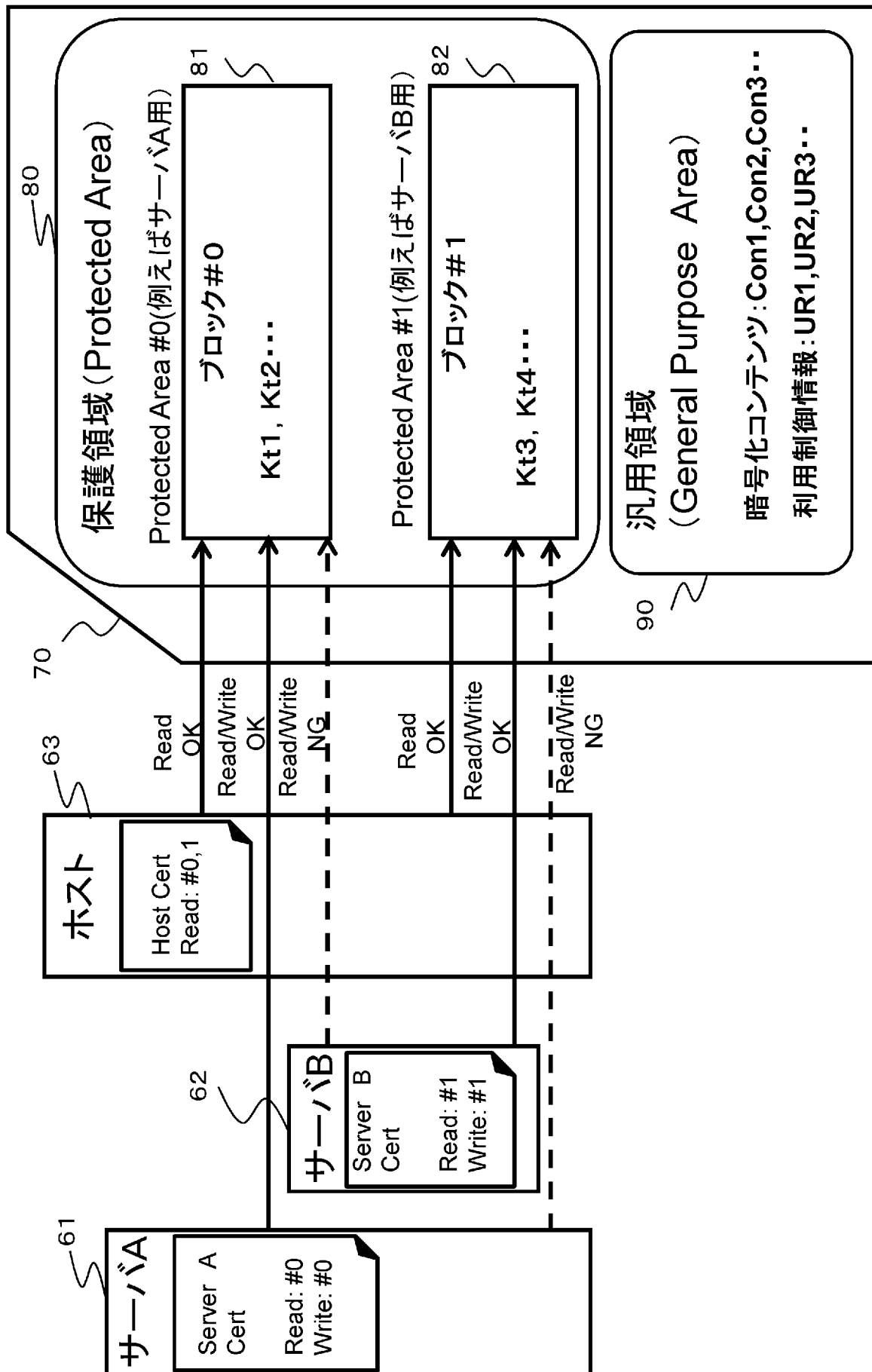
[図4]



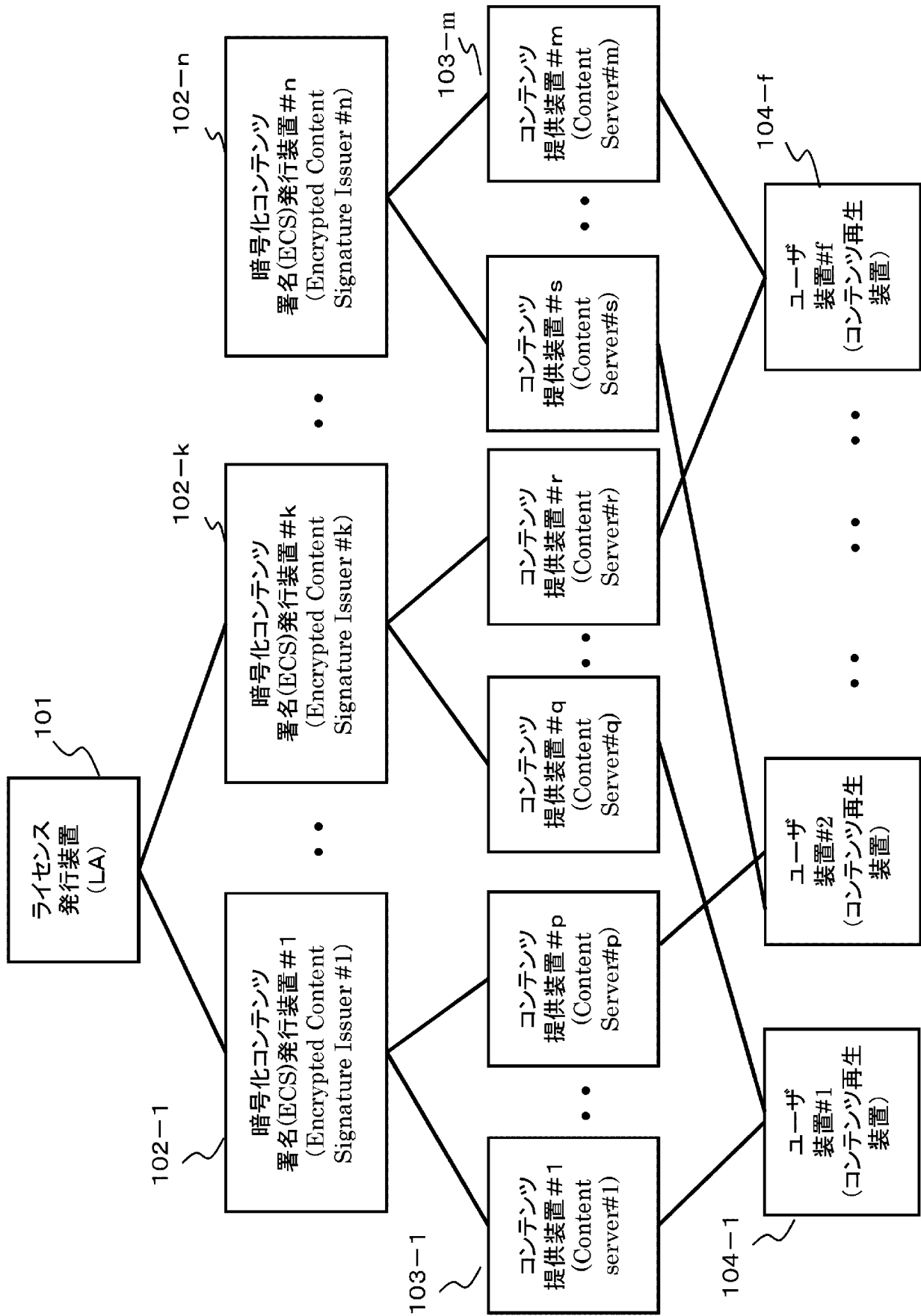
[図5]



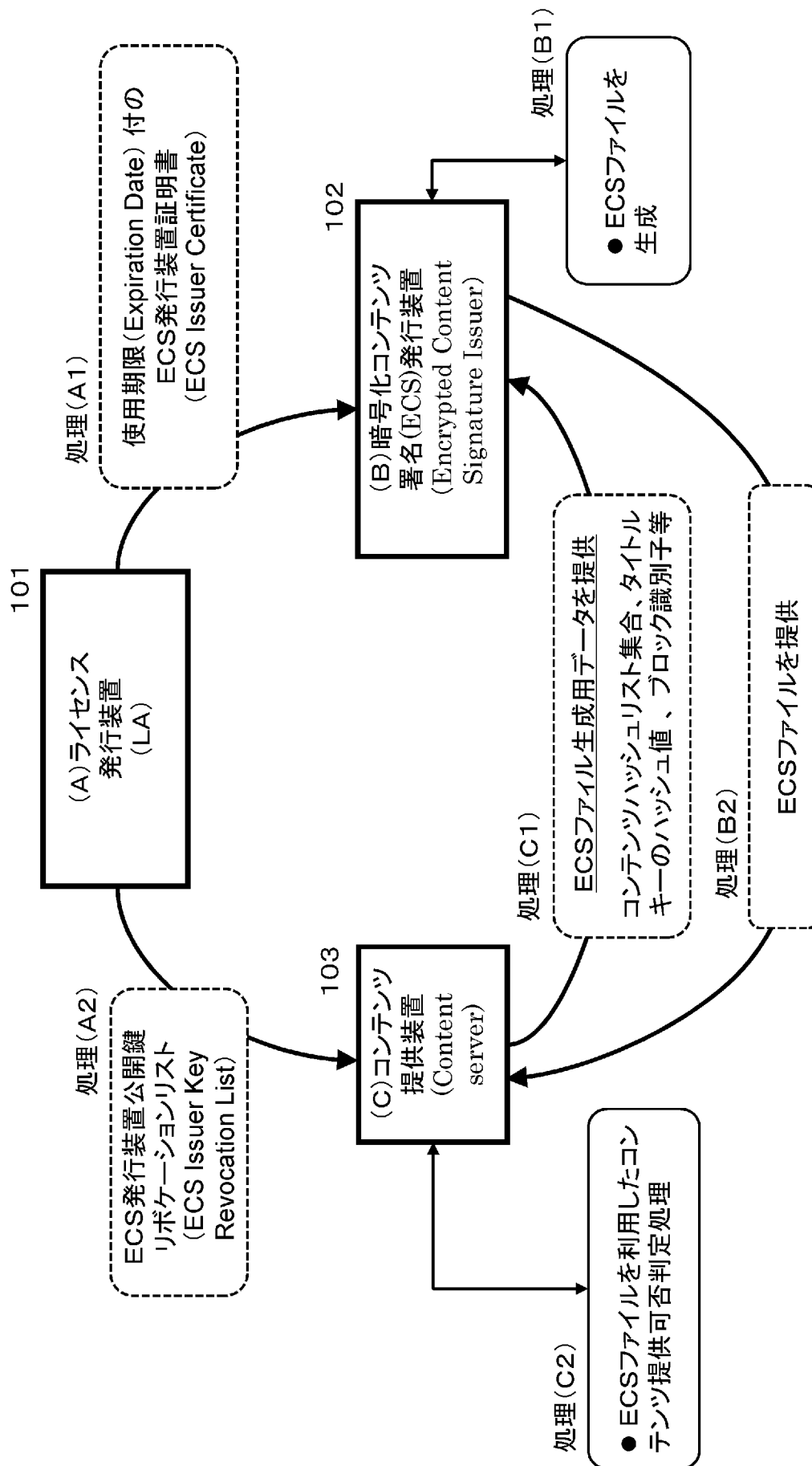
[図6]



[図7]



[図8]



[図9]

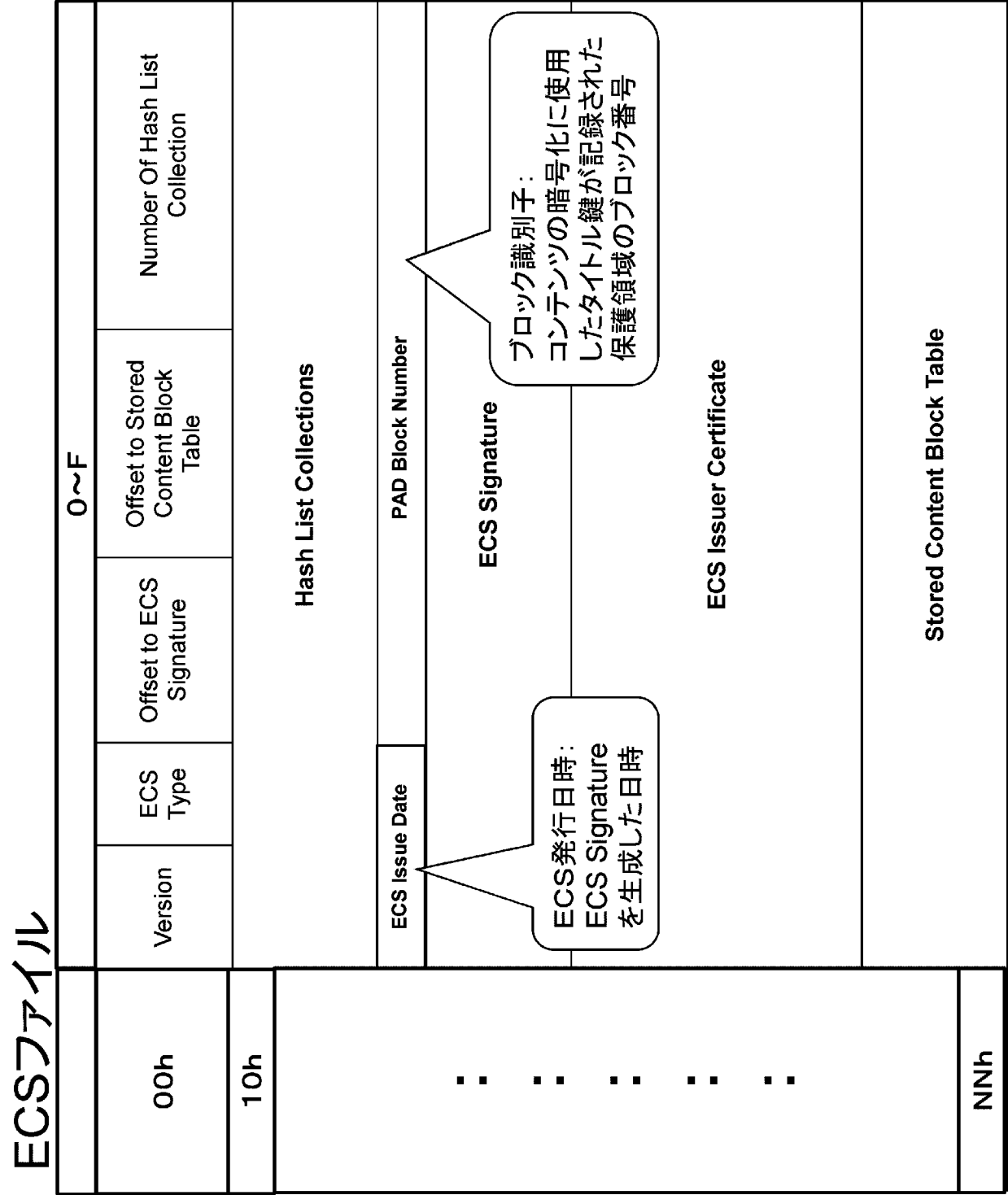
(B) ECS 発行装置証明書

ECS証明書識別子 (ECS Certificate ID)
ブロック識別子開始番号 (Start PAD Block Number)
ブロック識別子範囲 (PAD Block Number Counter)
発行装置証明書使用期限 (Expiration Date)
ECS発行装置公開鍵 (ECS Issuer Public Key)
LA署名 (Signature by LA)

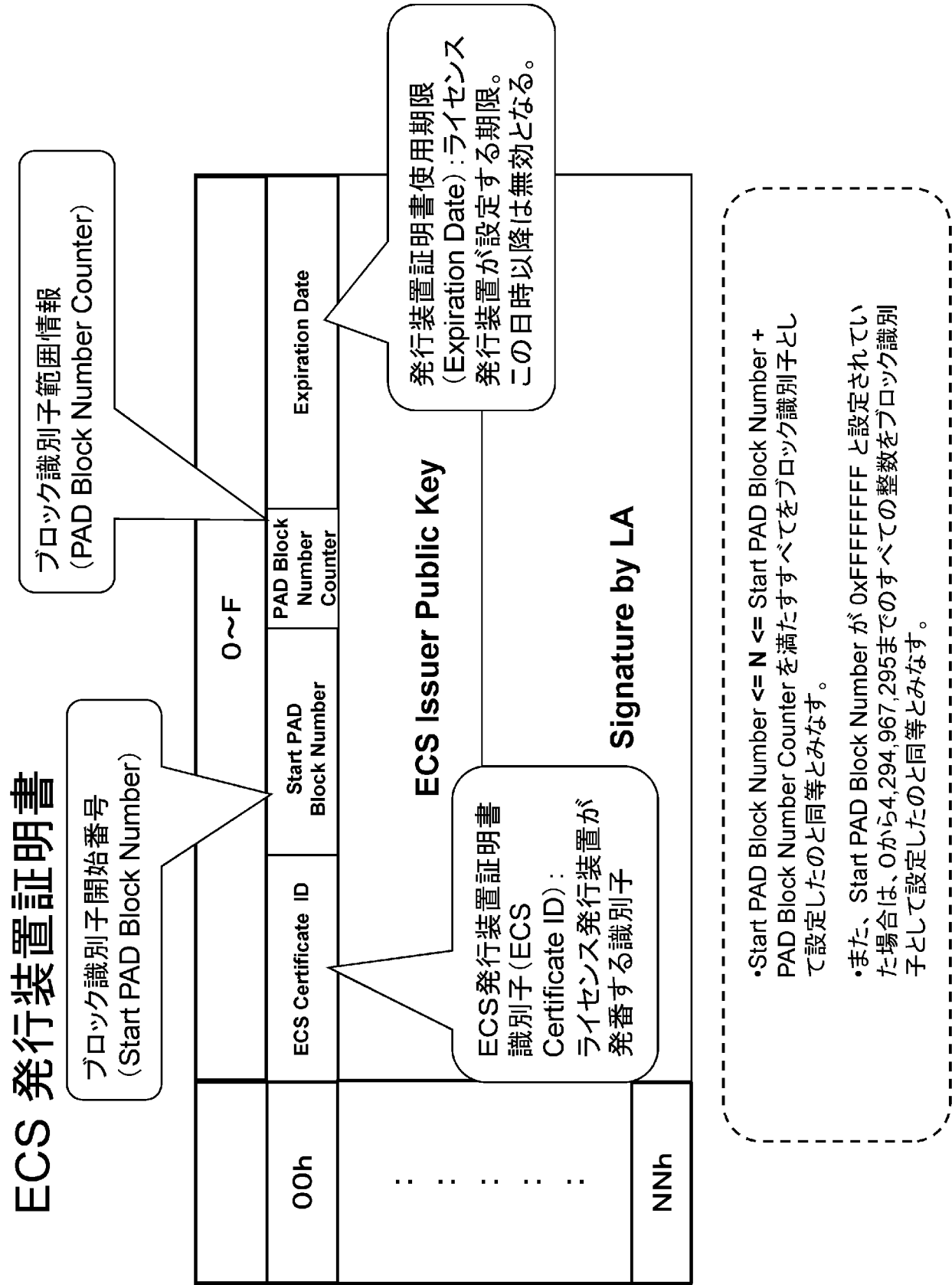
(A) ECSファイル

コンテンツハッシュリスト集合 (Hash List Collections)
ECS発行日時 (ECS Issue Date)
ブロック識別子 (PAD Block Number)
ECS発行装置署名 (Signature by ECS Issuer)
ECS発行装置証明書 (ECS Issuer Certificate)
コンテンツブロックテーブル (Stored Content Block Table)

[図10]



[図11]

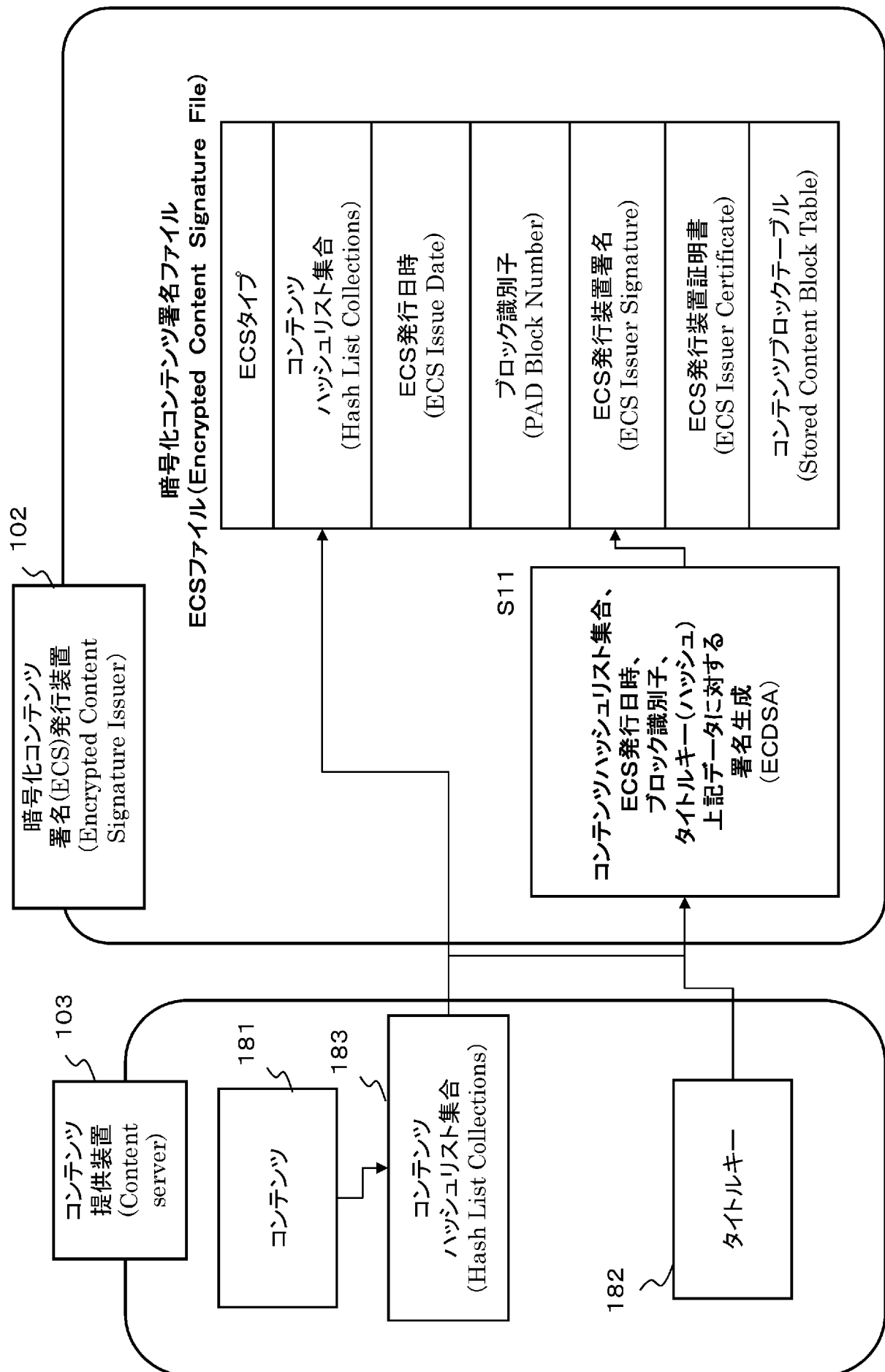


[図12]

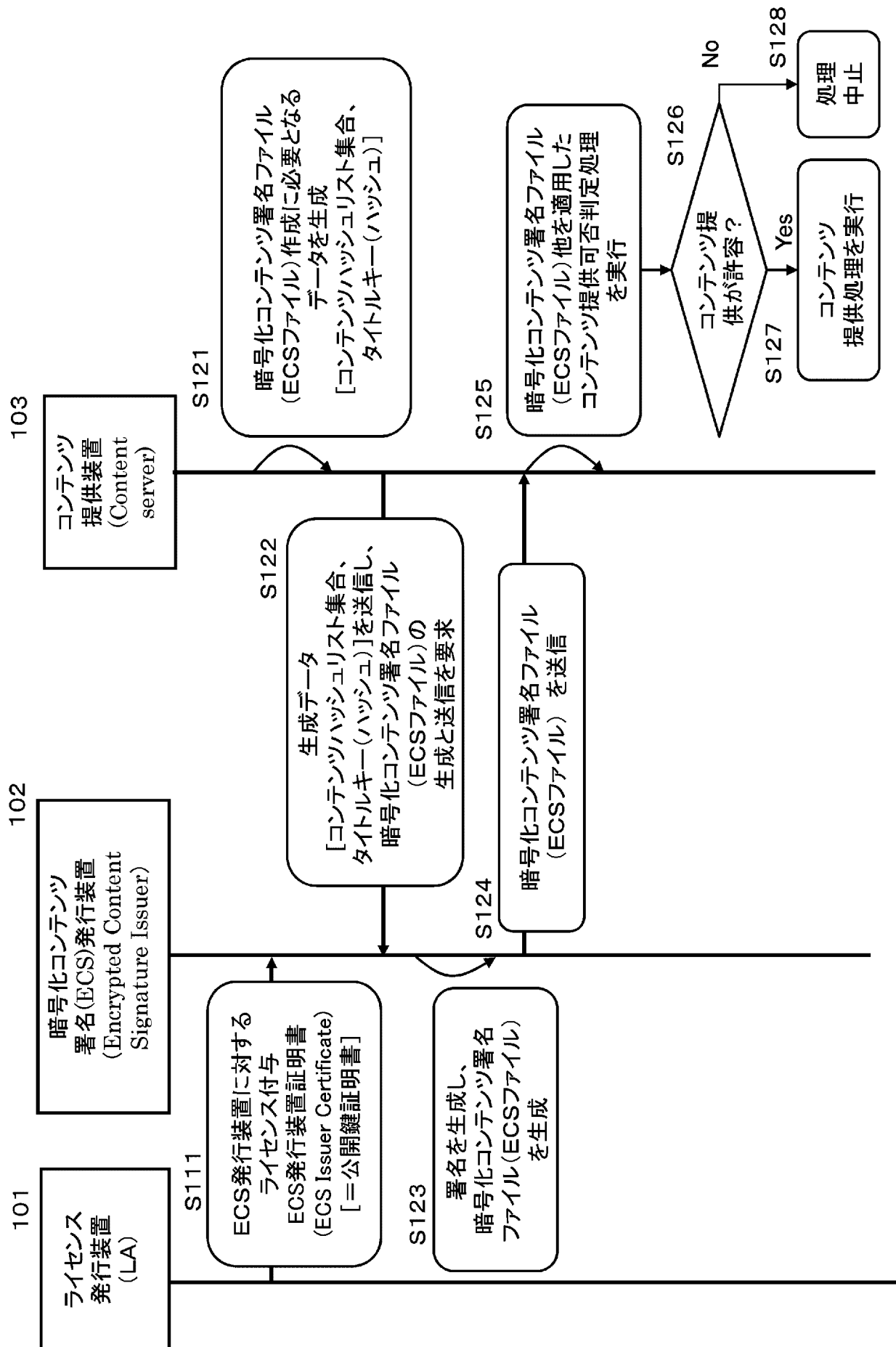
ECS発行装置証明書（公開鍵）リボケーションリスト
(ECS Issuer Key Revocation List)

バージョン (Version)	
エントリ数 (Number of entries)	
リボークECS発行装置証明書識別子 #1 (Revoked ECS Issuer Certificate ID #1)	リボーク日時 #1 (Revoked Date #1)
...	
リボークECS発行装置証明書識別子 #N (Revoked ECS Issuer Certificate ID #N)	リボーク日時 #N (Revoked Date #N)
LA署名 (Signature by LA)	

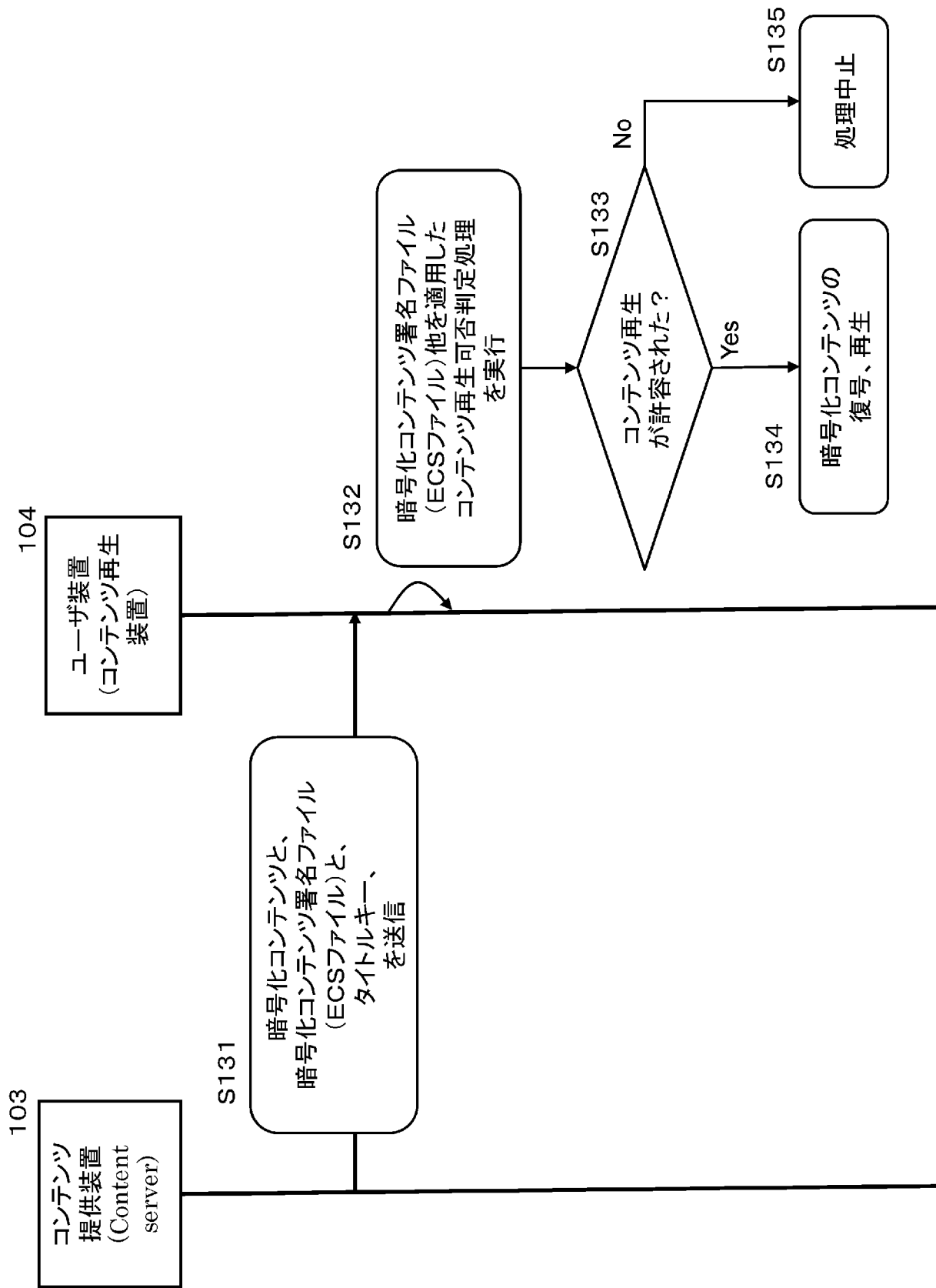
[図13]



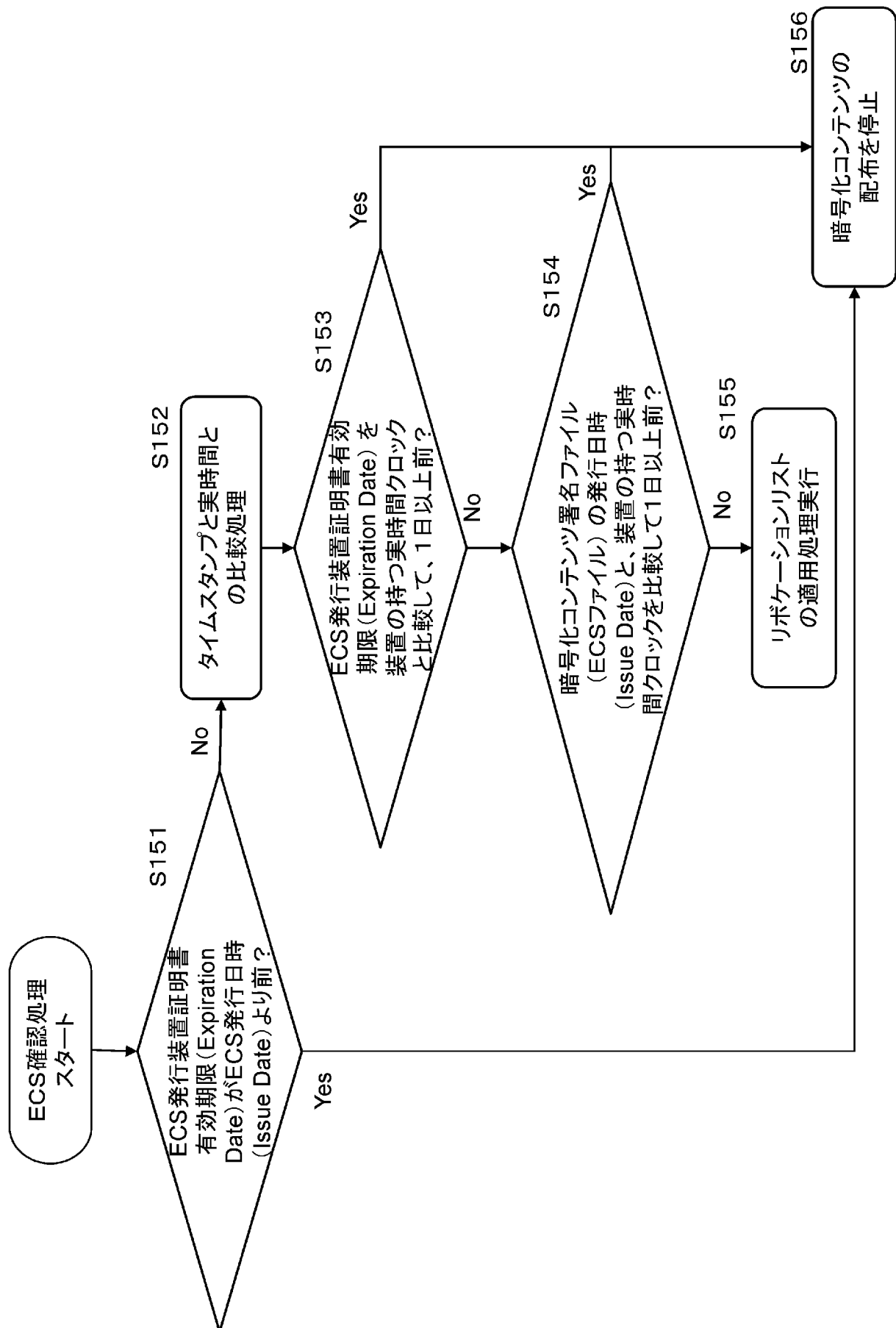
[図14]



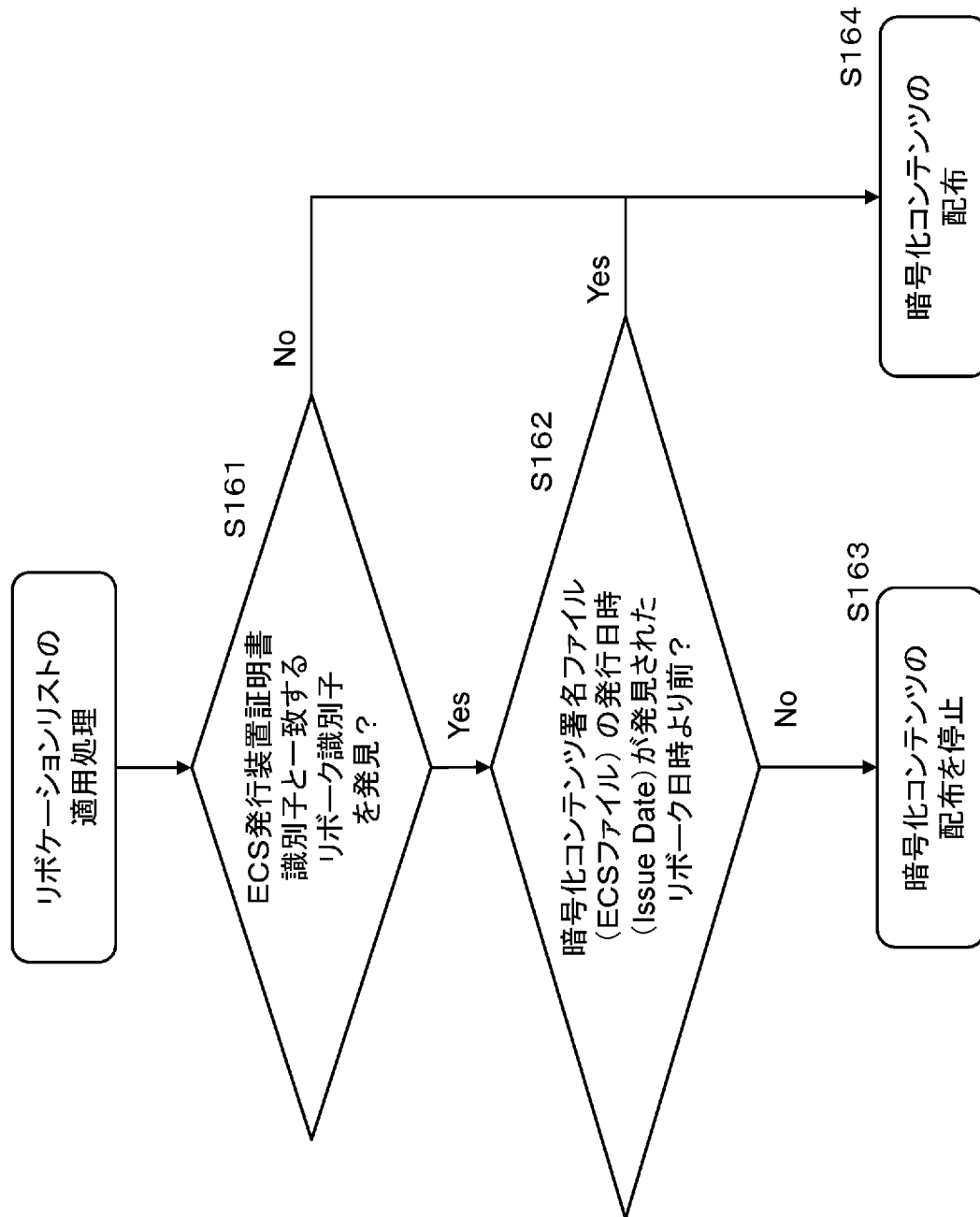
[図15]



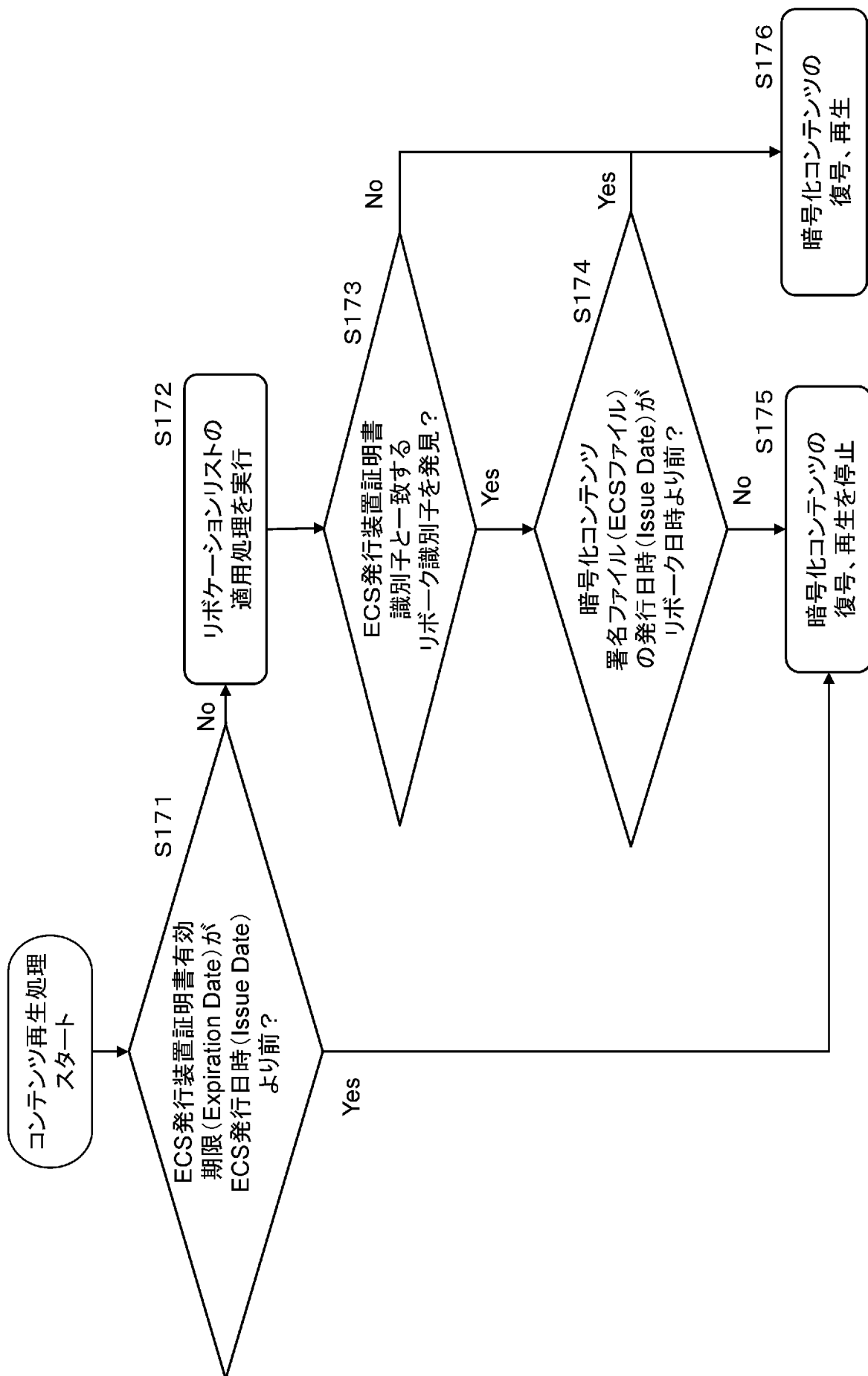
[図16]



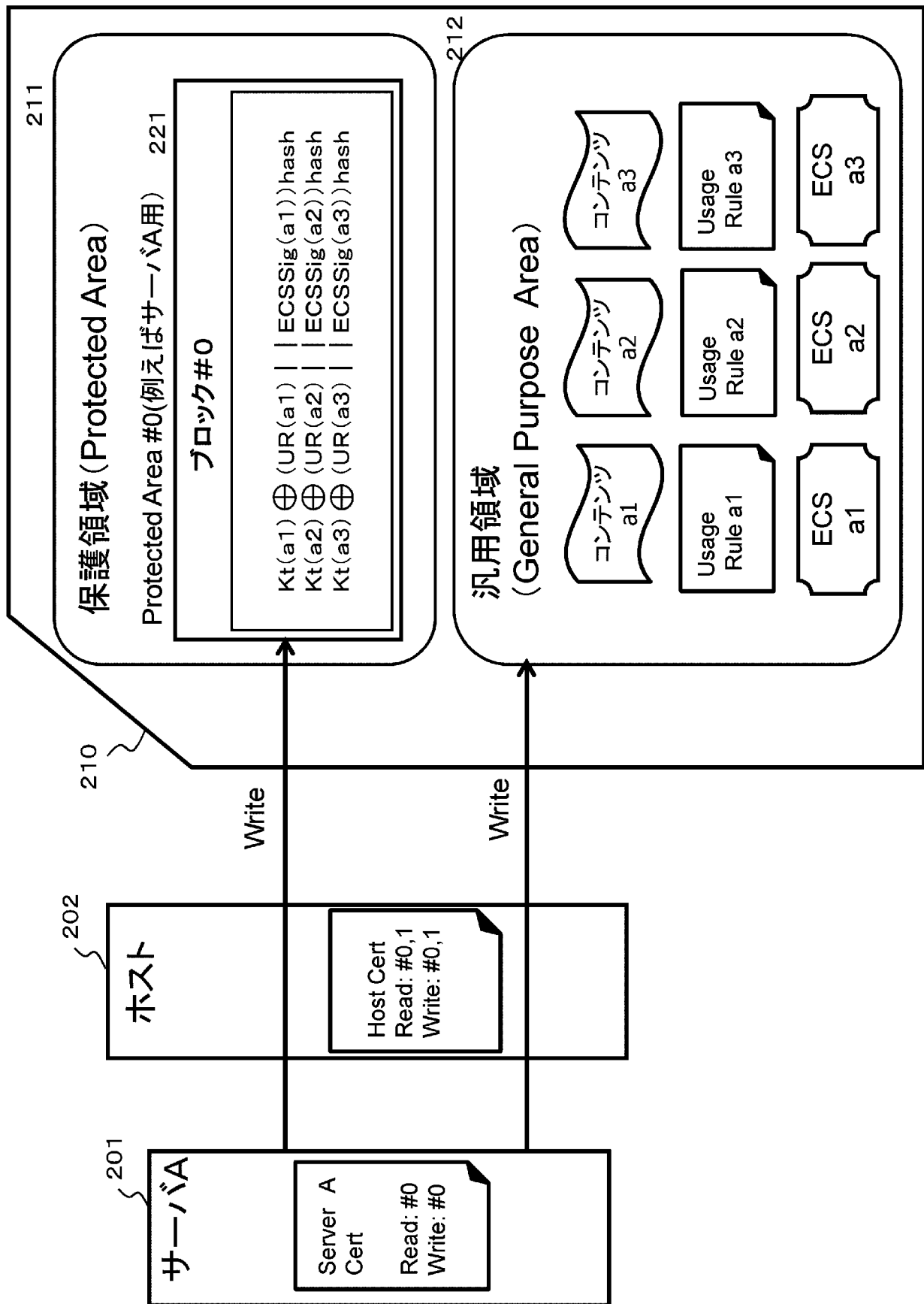
[図17]



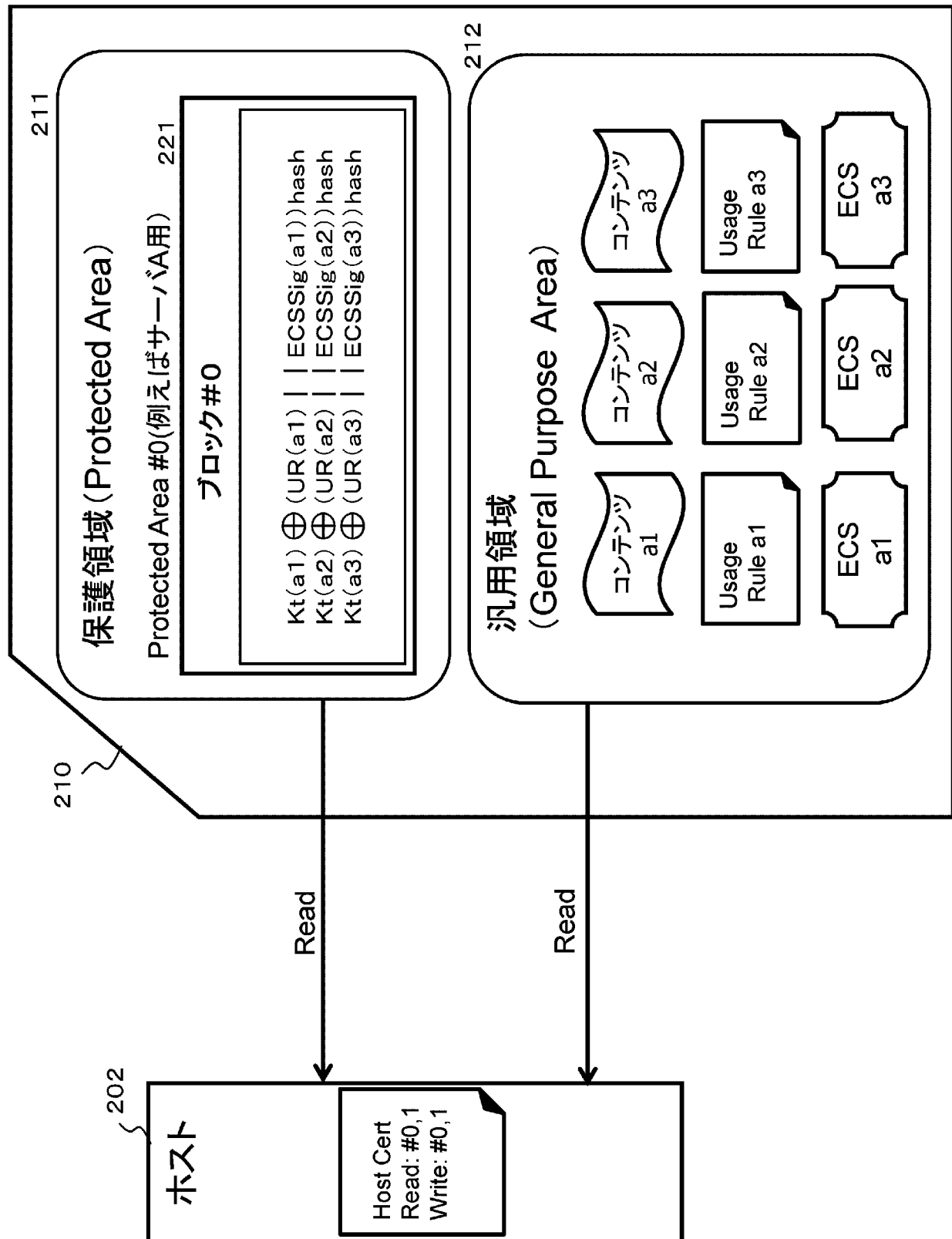
[図18]



[図19]



[図20]



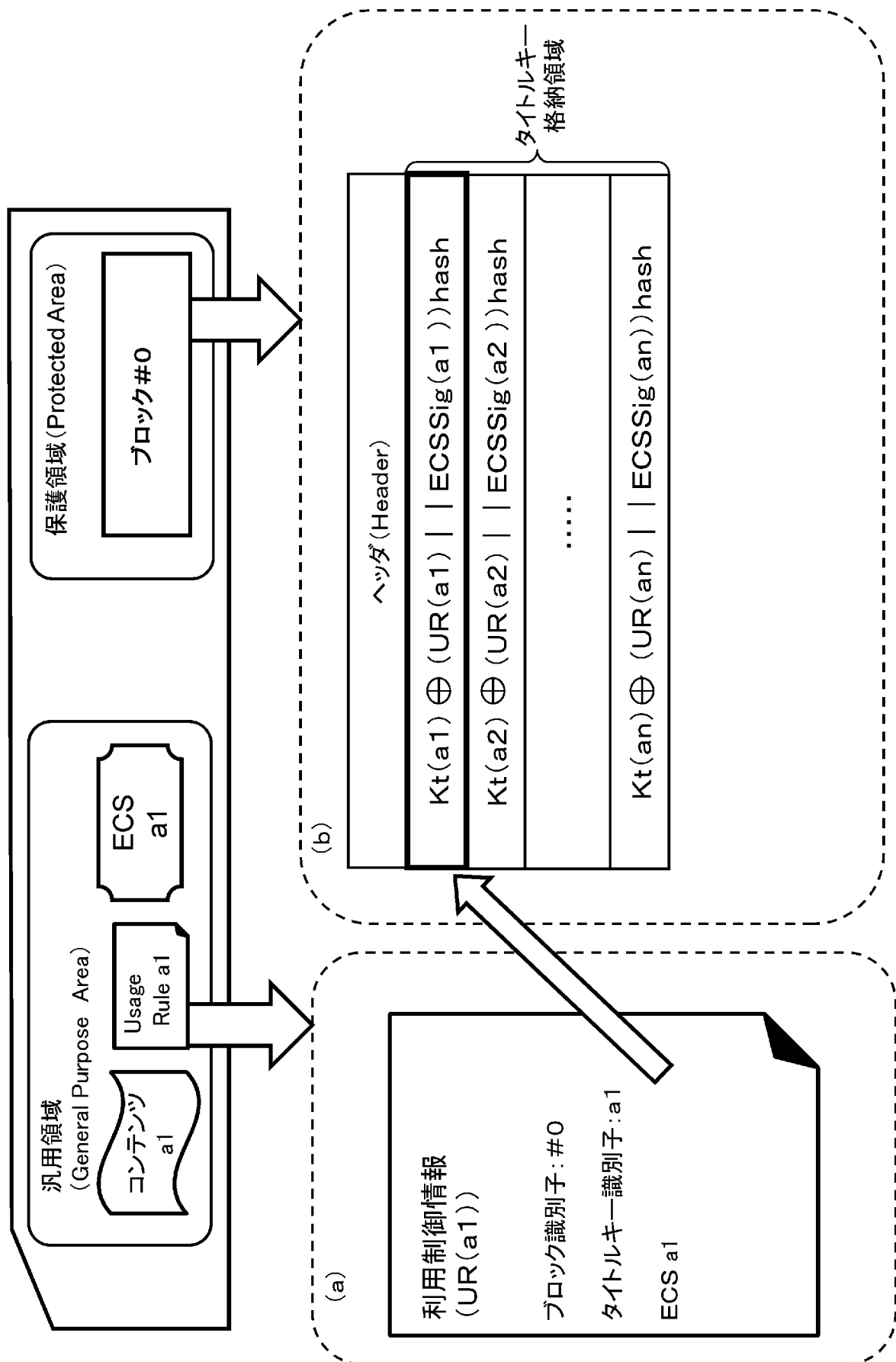
[図21]

	保護領域 (Protected Area)		汎用領域 (General Purpose Area)
	ブロック#0	ブロック#1	
サーバ A	$\text{Kt(a1)} \oplus (\text{UR(a1)} \mid \mid \text{ECSSig(a1)}) \text{hash}$ $\text{Kt(a2)} \oplus (\text{UR(a2)} \mid \mid \text{ECSSig(a2)}) \text{hash}$ $\text{Kt(a3)} \oplus (\text{UR(a3)} \mid \mid \text{ECSSig(a3)}) \text{hash}$	---	Con(a1), UR(a1), ECS(a1) Con(a2), UR(a2), ECS(a2) Con(a3), UR(a3), ECS(a3)
サーバ B	---	$\text{Kt(b1)} \oplus (\text{UR(b1)} \mid \mid \text{ECSSig(b1)}) \text{hash}$ $\text{Kt(b2)} \oplus (\text{UR(b2)} \mid \mid \text{ECSSig(b2)}) \text{hash}$	Con(b1), UR(b1), ECS(b1) Con(b2), UR(b2), ECS(b2)

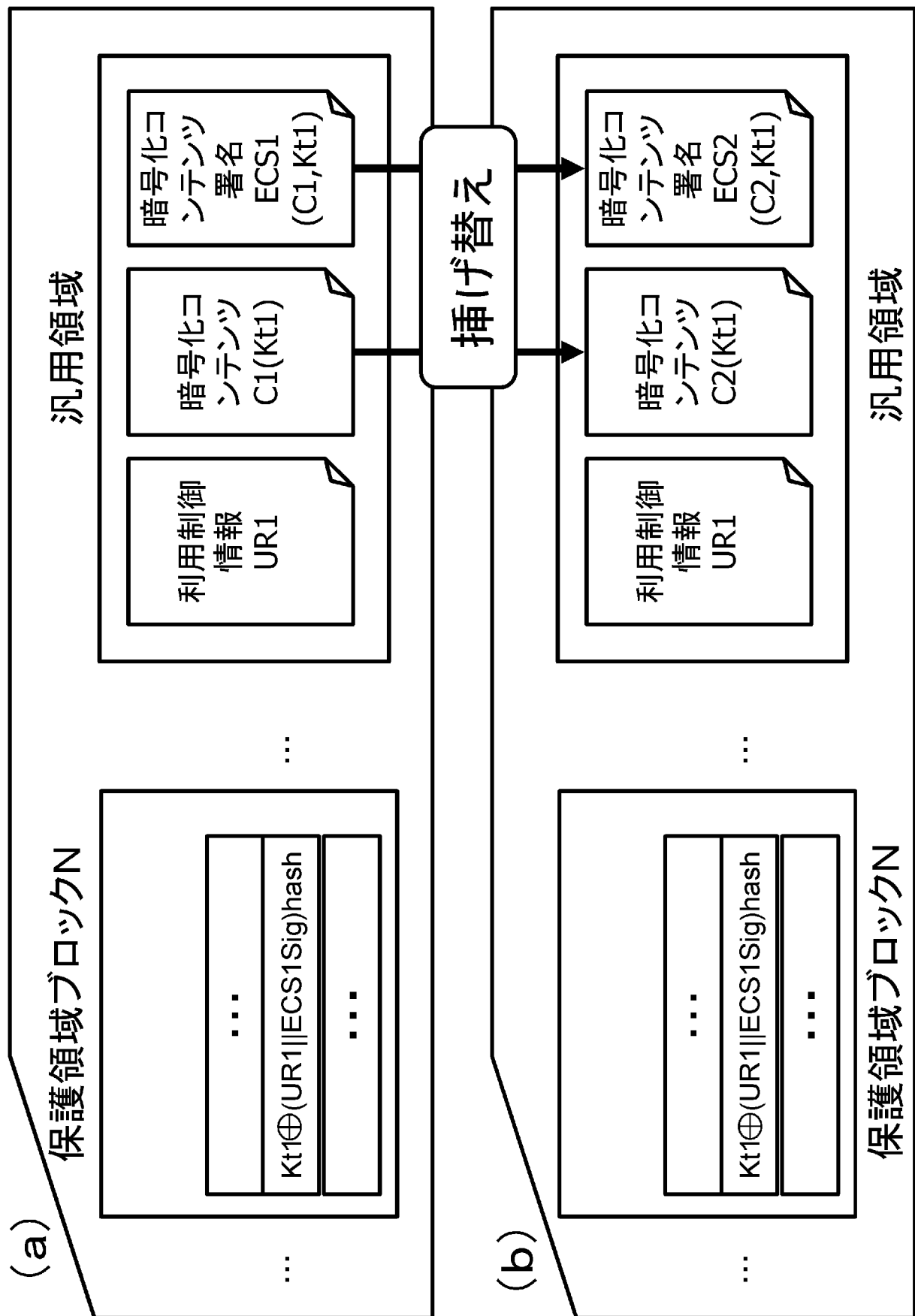
[図22]

	保護領域 (Protected Area)		汎用領域 (General Purpose Area)
	ブロック#0	ブロック#1	
サブ A	$\begin{matrix} \text{Kt(a1)} \oplus (\text{UR(a1)} \mid \text{ECSSig(a1)}) \text{hash} \\ \text{Kt(a2)} \oplus (\text{UR(a2)} \mid \text{ECSSig(a2)}) \text{hash} \\ \text{Kt(a3)} \oplus (\text{UR(a3)} \mid \text{ECSSig(a3)}) \text{hash} \end{matrix}$	---	$\begin{matrix} \text{Con(a1)}, \text{UR(a1)}, \text{ECS(a1)} \\ \text{Con(a2)}, \text{UR(a2)}, \text{ECS(a2)} \\ \text{Con(a3)}, \text{UR(a3)}, \text{ECS(a3)} \end{matrix}$
サブ B	$\begin{matrix} \text{Kt(b1)} \oplus (\text{UR(b1)} \mid \text{ECSSig(b1)}) \text{hash} \\ \text{Kt(b2)} \oplus (\text{UR(b2)} \mid \text{ECSSig(b2)}) \text{hash} \end{matrix}$	---	$\begin{matrix} \text{Con(b1)}, \text{UR(b1)}, \text{ECS(b1)} \\ \text{Con(b2)}, \text{UR(b2)}, \text{ECS(b2)} \end{matrix}$
サブ C	---	$\text{Kt(c1)} \oplus (\text{UR(c1)} \mid \text{ECSSig(c1)}) \text{hash}$	$\text{Con(c1)}, \text{UR(c1)}, \text{ECS(c1)}$
サブ D	---	$\begin{matrix} \text{Kt(d1)} \oplus (\text{UR(d1)} \mid \text{ECSSig(d1)}) \text{hash} \\ \text{Kt(d2)} \oplus (\text{UR(d2)} \mid \text{ECSSig(d2)}) \text{hash} \end{matrix}$	$\begin{matrix} \text{Con(d1)}, \text{UR(d1)}, \text{ECS(d1)} \\ \text{Con(d2)}, \text{UR(d2)}, \text{ECS(d2)} \end{matrix}$

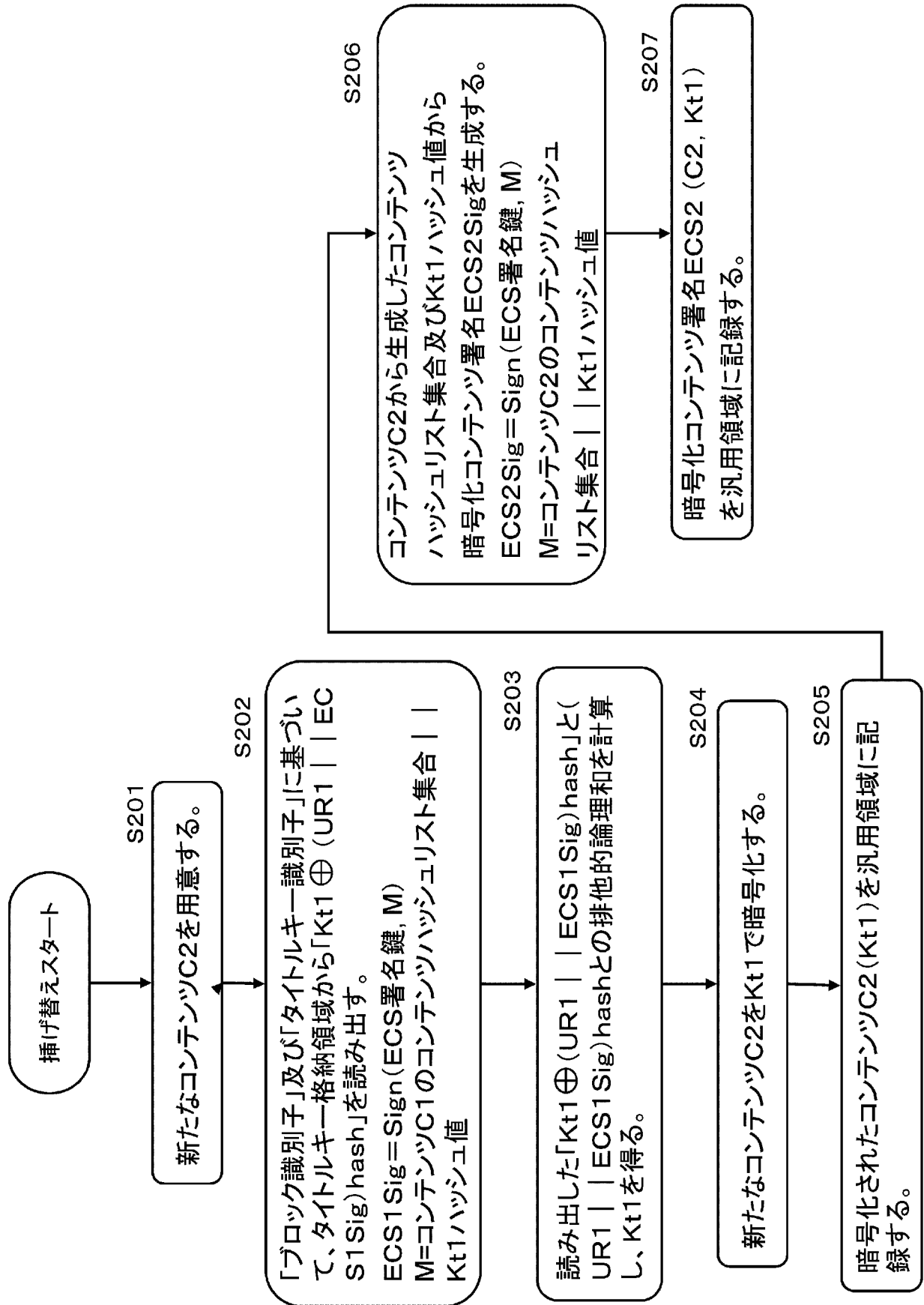
[図23]



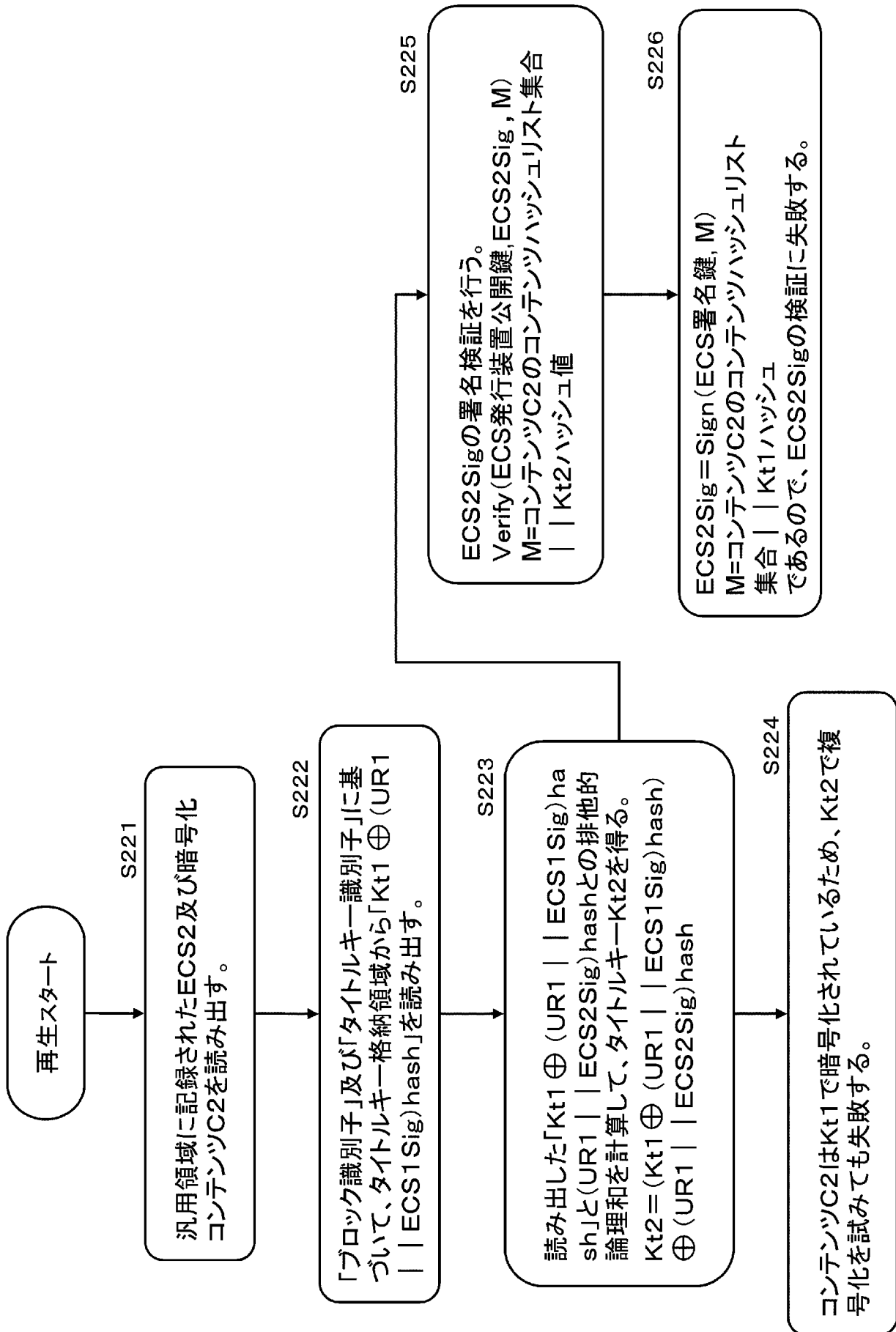
[図24]



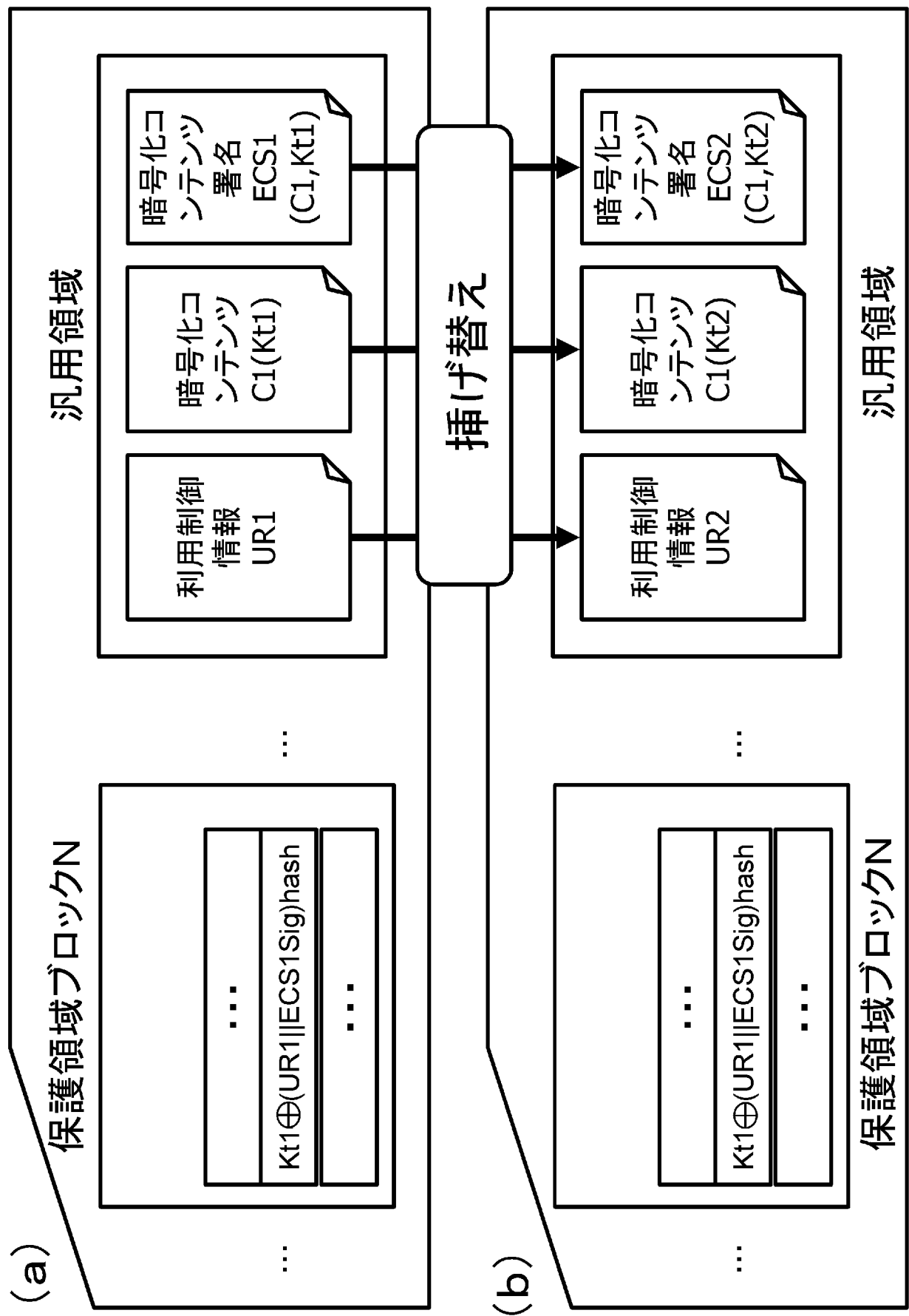
[図25]



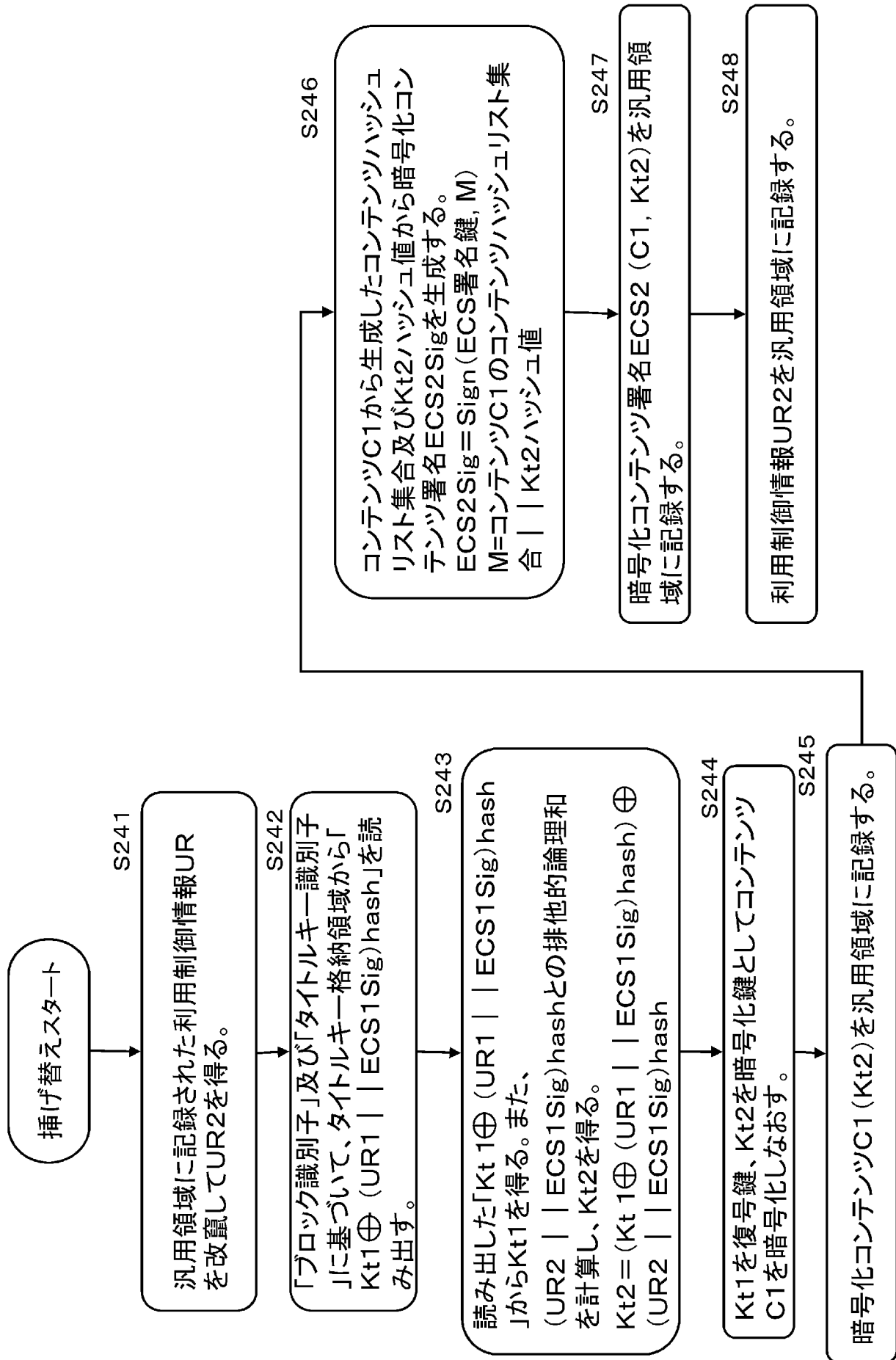
[図26]



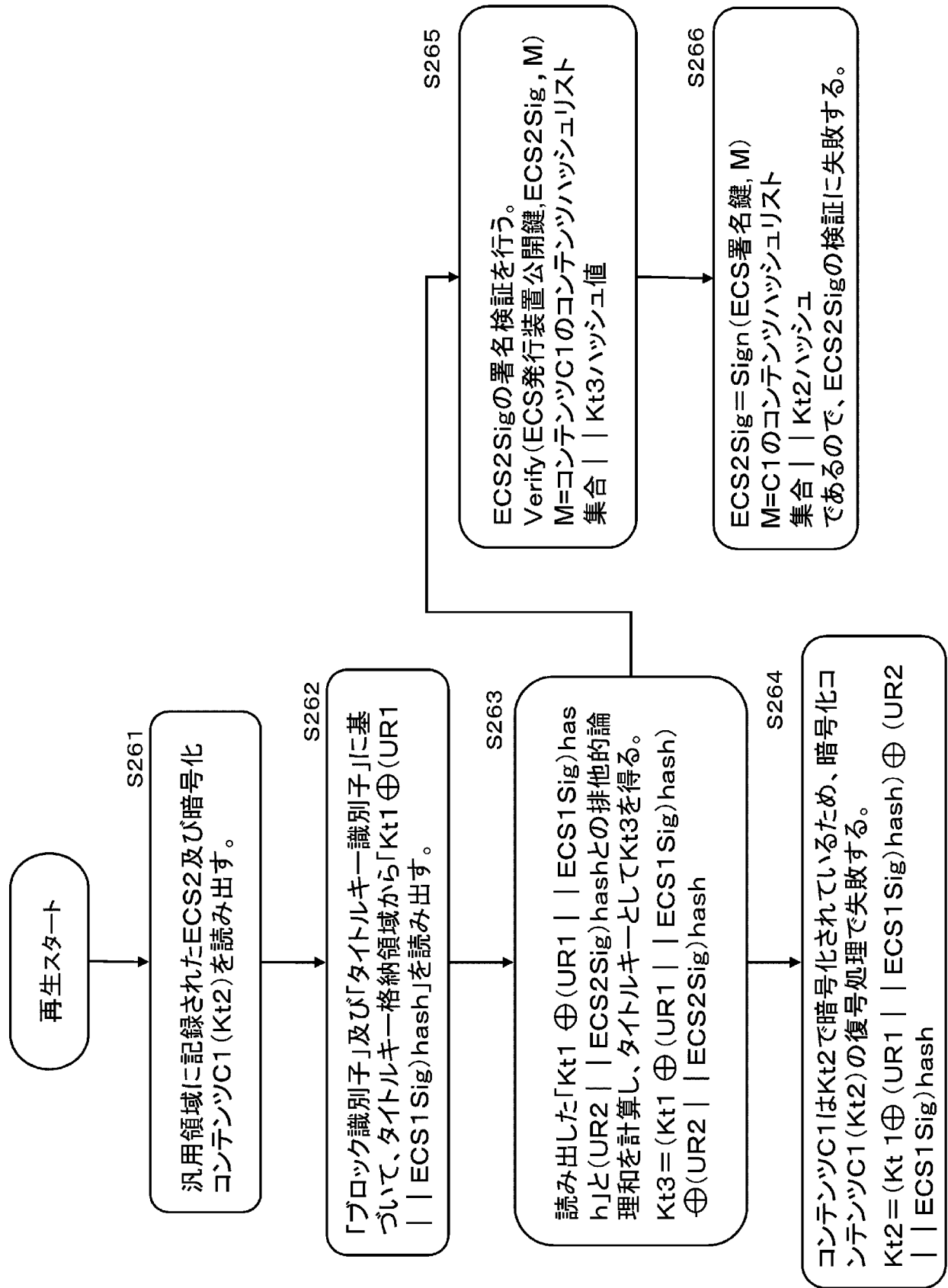
[図27]



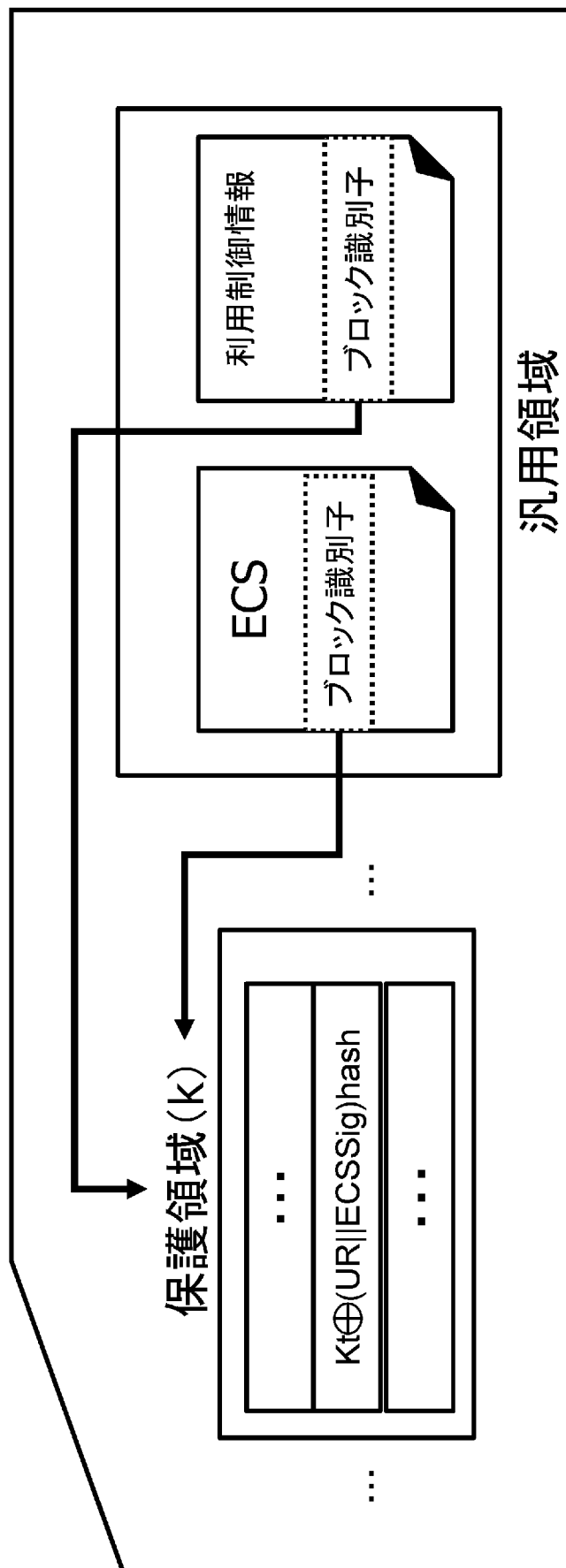
[図28]



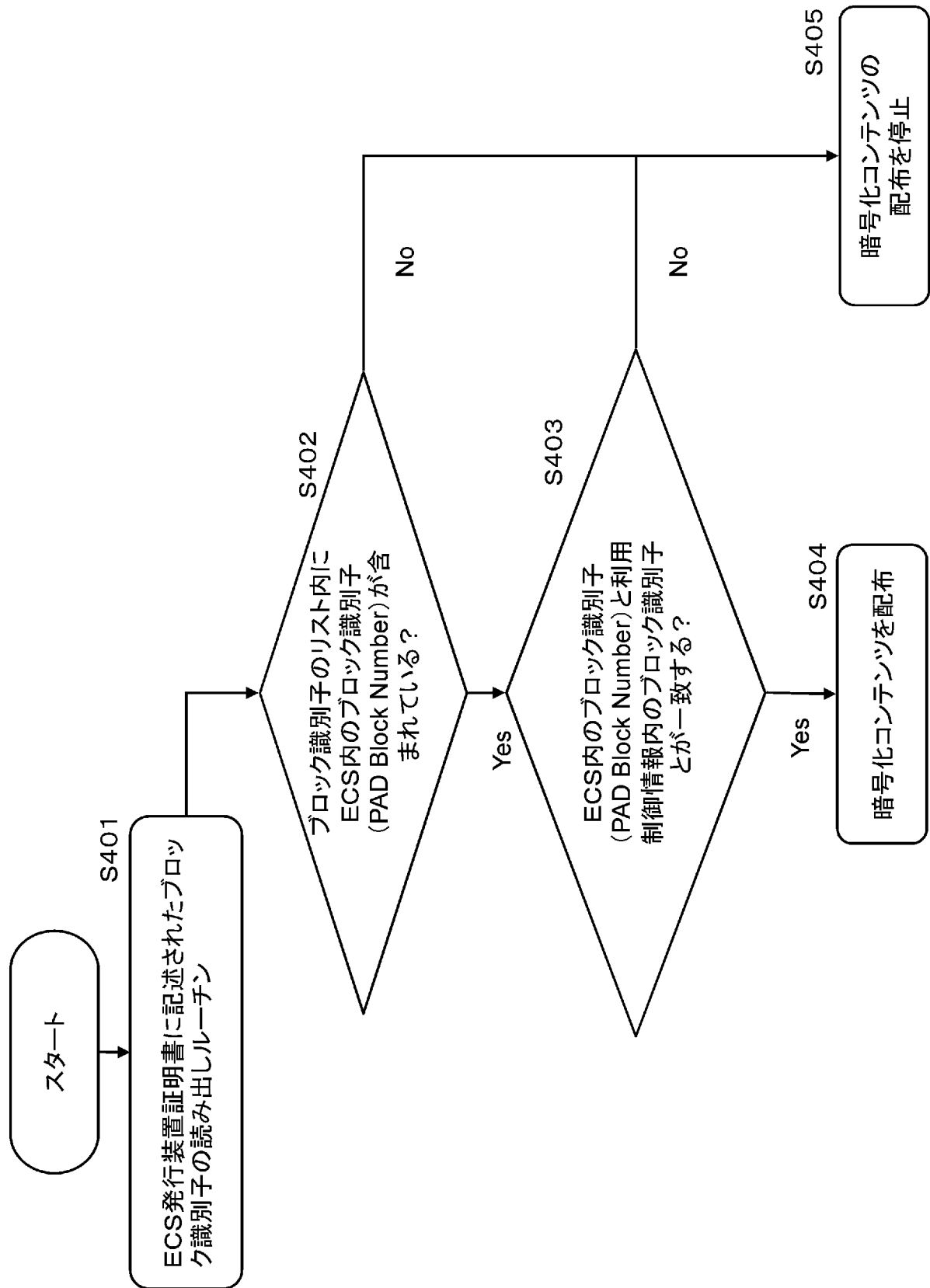
[図29]



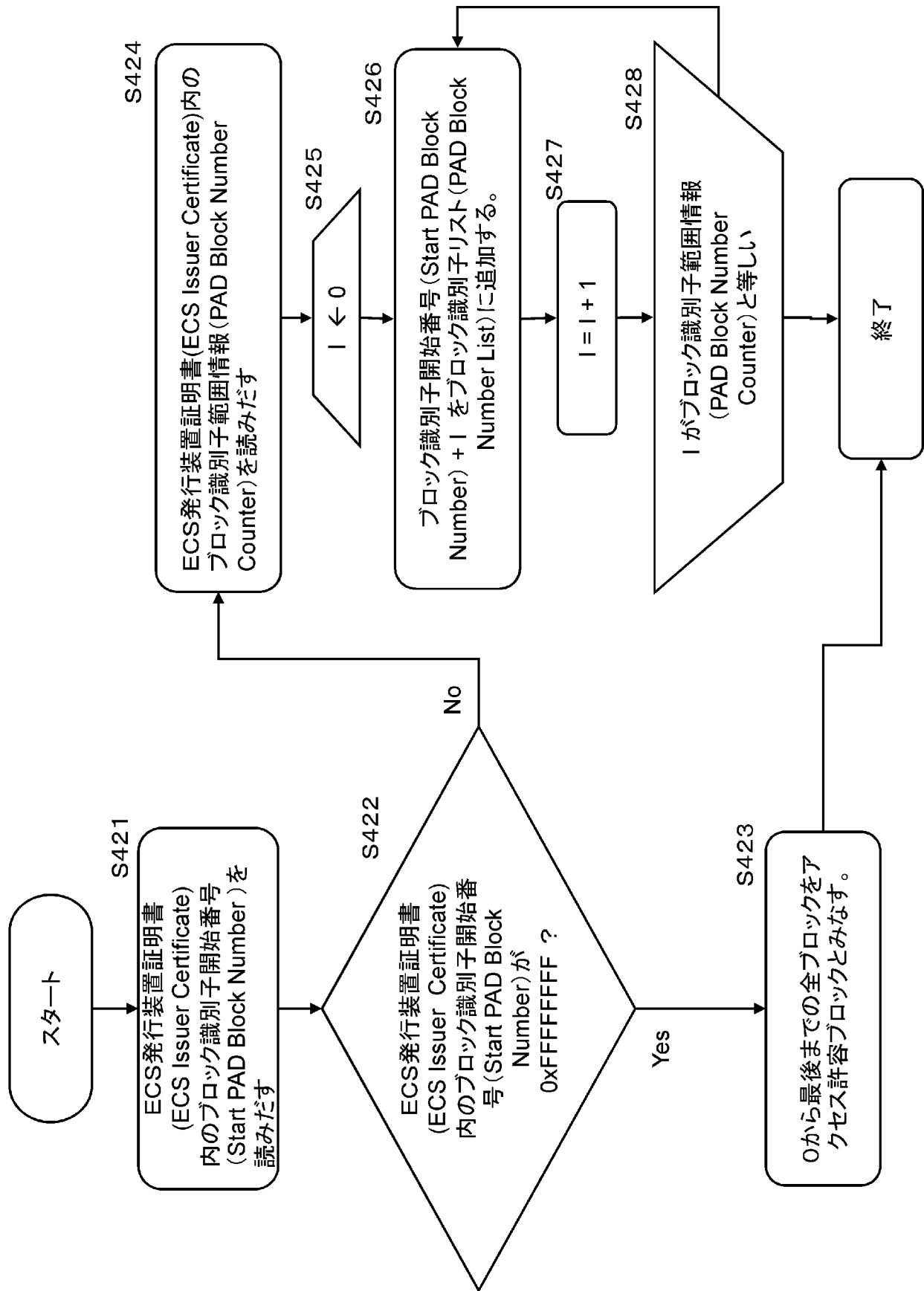
[図30]



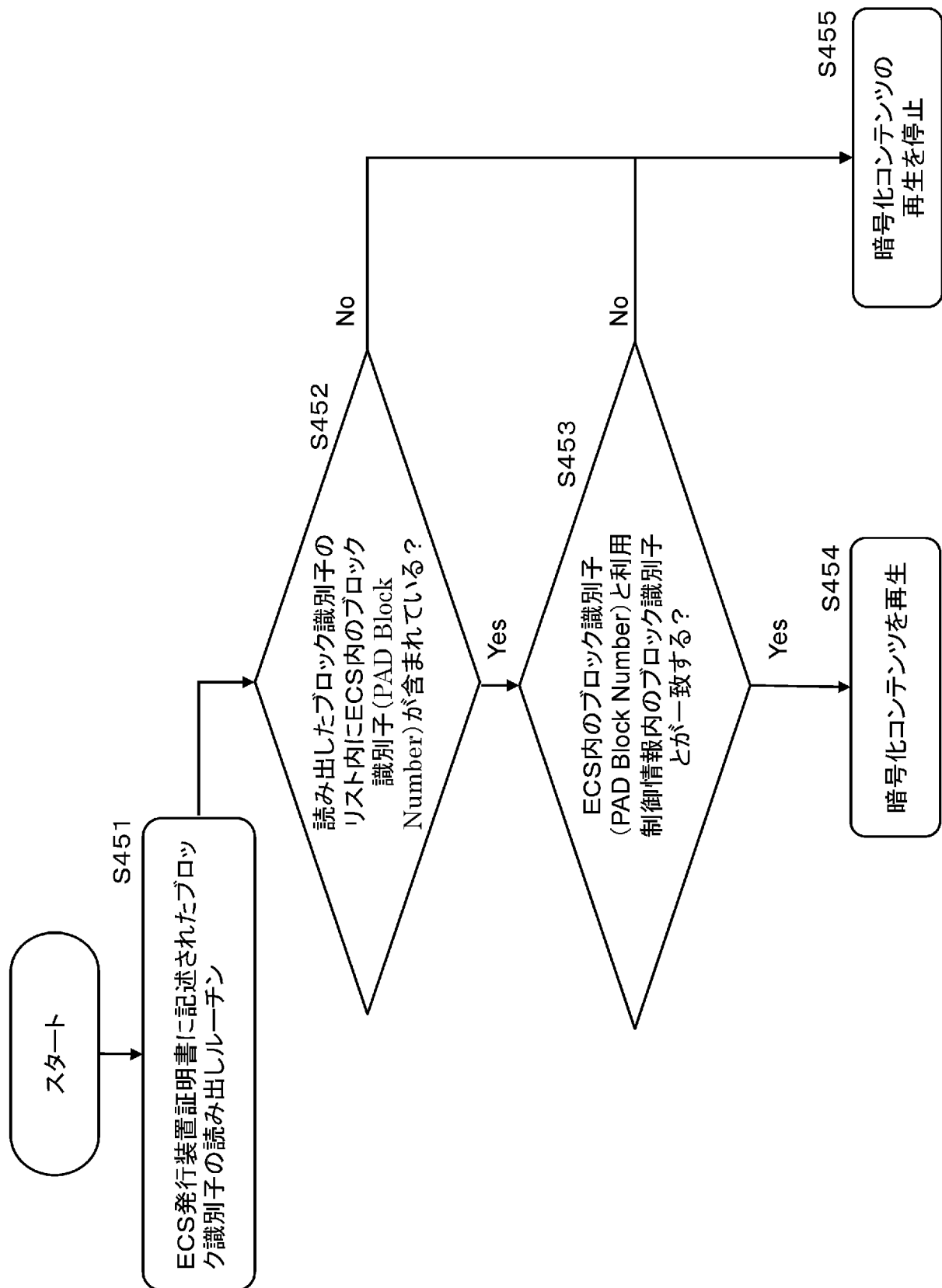
[図31]



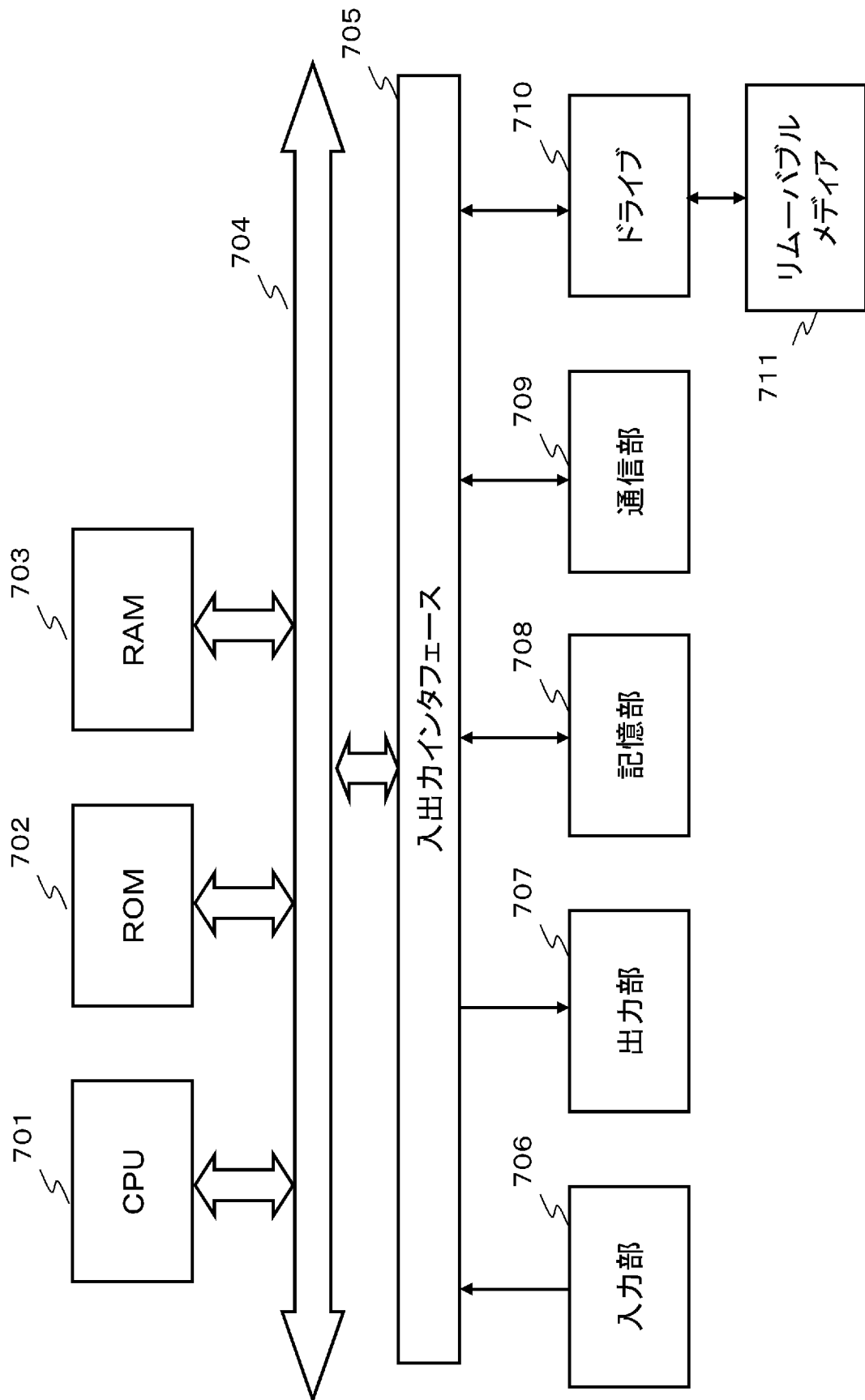
[図32]



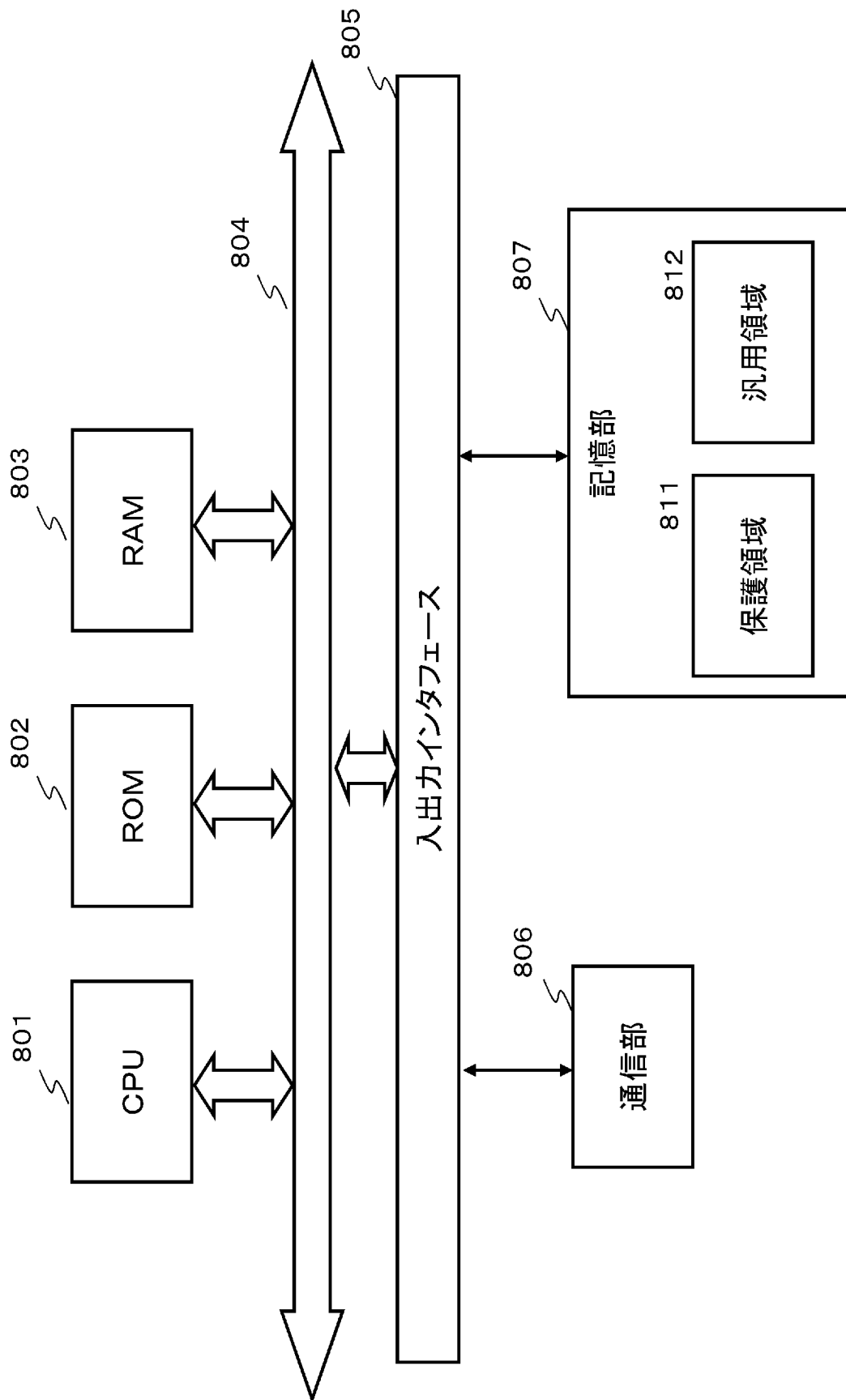
[図33]



[図34]



[図35]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2012/077066

A. CLASSIFICATION OF SUBJECT MATTER

H04L9/08(2006.01) i, H04L9/32(2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L9/08, H04L9/32

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2012

Kokai Jitsuyo Shinan Koho 1971-2012 Toroku Jitsuyo Shinan Koho 1994-2012

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2005-20703 A (Matsushita Electric Industrial Co., Ltd.), 20 January 2005 (20.01.2005), paragraph [0147] & US 2004/0243814 A1 & EP 1624608 A1 & WO 2004/082203 A1 & KR 10-2006-0058047 A & CN 1759559 A & KR 10-1109995 B	1-17
A	JP 2007-124055 A (Nippon Hoso Kyokai), 17 May 2007 (17.05.2007), paragraphs [0052] to [0097] (Family: none)	1-17
A	JP 2007-299475 A (Toshiba Corp.), 15 November 2007 (15.11.2007), paragraphs [0004] to [0007], [0049] to [0057] & US 2008/0063199 A1 & KR 10-2007-0106400 A	1-17

☒ Further documents are listed in the continuation of Box C.☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
08 November, 2012 (08.11.12)Date of mailing of the international search report
20 November, 2012 (20.11.12)Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2012/077066

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2009/124715 A1 (THOMSON LICENSING) , 15 October 2009 (15.10.2009) , page 13, line 21 to page 14, line 6 & JP 2011-530197 A & US 2011/0016311 A1 & EP 2272201 A1 & CN 101981866 A & KR 10-2010-0133410 A	1-17

A. 発明の属する分野の分類（国際特許分類（I P C））

Int.Cl. H04L9/08(2006.01)i, H04L9/32(2006.01)i

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（I P C））

Int.Cl. H04L9/08, H04L9/32

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922-1996年
日本国公開実用新案公報	1971-2012年
日本国実用新案登録公報	1996-2012年
日本国登録実用新案公報	1994-2012年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
A	JP 2005-20703 A（松下電器産業株式会社） 2005.01.20, 段落【0147】 & US 2004/0243814 A1 & EP 1624608 A1 & WO 2004/082203 A1 & KR 10-2006-0058047 A & CN 1759559 A & KR 10-1109995 B	1-17
A	JP 2007-124055 A（日本放送協会） 2007.05.17, 段落【0052】 - 【0097】 （ファミリーなし）	1-17

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日

08.11.2012

国際調査報告の発送日

20.11.2012

国際調査機関の名称及びあて先

日本国特許庁（I S A/J P）

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官（権限のある職員）

金沢 史明

5 S

4538

電話番号 03-3581-1101 内線 3546

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
A	JP 2007-299475 A (株式会社東芝) 2007.11.15, 段落【0004】 - 【0007】, 【0049】 - 【0057】 & US 2008/0063199 A1 & KR 10-2007-0106400 A	1-17
A	WO 2009/124715 A1 (THOMSON LICENSING) 2009.10.15, 13 頁 21 行-14 行 6 行 & JP 2011-530197 A & US 2011/0016311 A1 & EP 2272201 A1 & CN 101981866 A & KR 10-2010-0133410 A	1-17