(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2017-118447
(P2017-118447A)
(43)公開日　平成29年6月29日(2017.6.29)

| (51)Int.Cl. | | F I | | | テーマコード（参考） |
|---|---|---|---|---|---|
| H04L 9/32 | (2006.01) | H04L | 9/00 | 675B | 5J104 |
| H04L 9/08 | (2006.01) | H04L | 9/00 | 601F | |
| G06F 21/60 | (2013.01) | G06F | 21/60 | 320 | |
| G06F 21/64 | (2013.01) | G06F | 21/64 | | |

審査請求 未請求　請求項の数 14　ＯＬ　（全 51 頁）

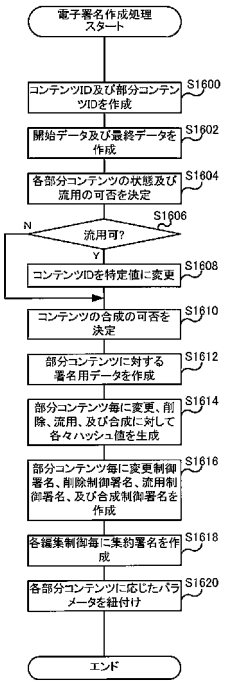
(21)出願番号　特願2015-254787 (P2015-254787)
(22)出願日　平成27年12月25日 (2015.12.25)

(71)出願人　000125370
学校法人東京理科大学
東京都新宿区神楽坂一丁目３番地
(74)代理人　100079049
弁理士　中島　淳
(74)代理人　100084995
弁理士　加藤　和詳
(74)代理人　100099025
弁理士　福田　浩志
(72)発明者　岩村　恵市
東京都新宿区神楽坂一丁目３番地　学校法人東京理科大学内
(72)発明者　稲村　勝樹
東京都新宿区神楽坂一丁目３番地　学校法人東京理科大学内

最終頁に続く

(54)【発明の名称】管理局装置、著作権保護装置、編集装置、検証装置、管理プログラム、著作権保護プログラム、編集プログラム、及び検証プログラム

(57)【要約】
【課題】コンテンツ間及びコンテンツ内の双方の編集を考慮した著作権の保護を行う。
【解決手段】複数の部分コンテンツから構成されるコンテンツの編集を電子署名によって制御するシステムにおいて、部分コンテンツに対して前記部分コンテンツの流用を制御する電子署名を生成する生成部と、前記部分コンテンツが含まれるコンテンツに対して前記電子署名を集約した集約署名を設定する設定部と、を備えた著作権保護装置。
【選択図】図１６



【特許請求の範囲】
【請求項１】
複数の部分コンテンツから構成されるコンテンツの編集を電子署名によって制御するシステムにおいて、
検査した部分コンテンツが予め定められた条件を満たした場合に、前記部分コンテンツと前記部分コンテンツを検証する鍵を特定する情報とに対して電子署名を生成する生成部
を備えた管理局装置。
【請求項２】
複数の部分コンテンツから構成されるコンテンツの編集を電子署名によって制御するシステムにおいて、
部分コンテンツに対して前記部分コンテンツの流用を制御する電子署名を生成する生成部と、
前記部分コンテンツが含まれるコンテンツに対して前記電子署名を集約した集約署名を設定する設定部と、
を備えた著作権保護装置。
【請求項３】
複数の部分コンテンツから構成されるコンテンツの編集を電子署名によって制御するシステムにおいて、
部分コンテンツに対して編集を許可する場合、編集を許可する第１鍵を用いて電子署名を生成して前記第１鍵を特定する情報を公開し、編集を不許可とする場合、編集を不許可とする第２鍵を用いて電子署名を生成して前記第２鍵を特定する情報を公開する生成部
を備えた著作権保護装置。
【請求項４】
複数の部分コンテンツから構成されるコンテンツの編集を電子署名によって制御するシステムにおいて、
部分コンテンツに対して前記部分コンテンツが含まれるコンテンツの合成を制御する電子署名を生成する生成部と、
前記コンテンツに対して前記電子署名を集約した集約署名を設定する設定部と、
を備えた著作権保護装置。
【請求項５】
複数の部分コンテンツから構成されるコンテンツの編集を電子署名によって制御するシステムにおいて、
１つの部分コンテンツに対して複数の著作者の各々が行った修正を制御する電子署名を生成する生成部と、
前記部分コンテンツまたは前記部分コンテンツが含まれるコンテンツに対して前記電子署名を集約した集約署名を設定する設定部と、
を備えた著作権保護装置。
【請求項６】
複数の部分コンテンツから構成されるコンテンツの編集を電子署名によって制御するシステムにおいて、
電子署名が設定された部分コンテンツまたは当該部分コンテンツを含むコンテンツに対して変更、追加、削除、流用、及び合成のうち少なくとも１つを含む編集を行う編集部と、
前記編集部が行った編集に応じて前記部分コンテンツに設定された前記電子署名を差し替えて集約署名の設定を更新する設定部と、
を備えた編集装置。
【請求項７】
複数の部分コンテンツから構成されるコンテンツの編集を電子署名によって制御するシステムにおいて、
部分コンテンツまたはコンテンツに対して変更、追加、削除、流用、及び合成のうち少

なくとも１つを含む編集に関する署名の検証を行う検証部と、
前記検証部の検証結果に応じて不正な編集が行われたコンテンツを検出する検出部と、
を備えた検証装置。
【請求項８】
複数の部分コンテンツから構成されるコンテンツの編集を電子署名によって制御するシステムにおける管理局装置として、
コンピュータにより、
検査した部分コンテンツが予め定められた条件を満たした場合に、前記部分コンテンツと前記部分コンテンツを検証する鍵を特定する情報とに対して電子署名を生成する、
ことを含む処理を行わせる管理プログラム。
【請求項９】
複数の部分コンテンツから構成されるコンテンツの編集を電子署名によって制御するシステムにおける著作権保護装置として、
コンピュータにより、
部分コンテンツに対して前記部分コンテンツの流用を制御する電子署名を生成し、
前記部分コンテンツが含まれるコンテンツに対して前記電子署名を集約した集約署名を設定する、
ことを含む処理を行わせる著作権保護プログラム。
【請求項１０】
複数の部分コンテンツから構成されるコンテンツの編集を電子署名によって制御するシステムの著作権保護装置として、
コンピュータにより、
部分コンテンツに対して編集を許可する場合、編集を許可する第１鍵を用いて電子署名を生成して前記第１鍵を特定する情報を公開し、編集を不許可とする場合、編集を不許可とする第２鍵を用いて電子署名を生成して前記第２鍵を特定する情報を公開する、
ことを含む処理を行わせる著作権保護プログラム。
【請求項１１】
複数の部分コンテンツから構成されるコンテンツの編集を電子署名によって制御するシステムの著作権保護装置として、
コンピュータにより、
部分コンテンツに対して前記部分コンテンツが含まれるコンテンツの合成を制御する電子署名を生成し、
前記コンテンツに対して前記電子署名を集約した集約署名を設定する、
ことを含む処理を行わせる著作権保護プログラム。
【請求項１２】
複数の部分コンテンツから構成されるコンテンツの編集を電子署名によって制御するシステムにおける著作権保護装置として、
コンピュータにより、
１つの部分コンテンツに対して複数の著作者の各々が行った修正を制御する電子署名を生成し、
前記部分コンテンツまたは前記部分コンテンツが含まれるコンテンツに対して前記電子署名を集約した集約署名を設定する、
ことを含む処理を行わせる著作権保護プログラム。
【請求項１３】
複数の部分コンテンツから構成されるコンテンツの編集を電子署名によって制御するシステムにおける編集装置として、
コンピュータにより、
電子署名が設定された部分コンテンツまたは当該部分コンテンツを含むコンテンツに対して変更、追加、削除、流用、及び合成のうち少なくとも１つを含む編集を行い、
行った編集に応じて前記部分コンテンツに設定された前記電子署名を差し替えて集約署

名の設定を更新する、
ことを含む処理を行わせる編集プログラム。
【請求項１４】
複数の部分コンテンツから構成されるコンテンツの編集を電子署名によって制御するシステムの検証装置として、
コンピュータに、
部分コンテンツまたはコンテンツに対して変更、追加、削除、流用、及び合成のうち少なくとも１つを含む編集に関する署名の検証を行い、
検証結果に応じて不正な編集が行われたコンテンツを検出する、
ことを含む処理を行わせる検証プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、管理局装置、著作権保護装置、編集装置、検証装置、管理プログラム、著作権保護プログラム、編集プログラム、及び検証プログラムに関する。
【背景技術】
【０００２】
ネットワークの発達した現代において、コンテンツの流通が盛んに行われるようになってきている。近年では、誰でもがコンテンツ提供者として、インターネットで流通させることができる消費者生成メディア（ＣＧＭ：Consumer Generated Media）または利用者生成コンテンツ（ＵＧＣ：User Generated Content）という概念が発生している。ＣＧＭまたはＵＧＣ（以降、ＣＧＭと総称する）サービスのサイト例としてYouTube（登録商標）が代表的である。ＣＧＭにおいては、インターネット上に公開されたコンテンツ（著作物）を２次利用して新たなコンテンツを作るマッシュアップと呼ばれるコンテンツ制作が頻繁に行われている。一方、現在の著作権保護技術としては代金などを支払ったユーザのみがコンテンツを視聴できるようにする視聴制御や、コンテンツのコピー回数やコピー機能自体を制限するコピー制御が一般的である。しかしながらこれらの制御方法は、コンテンツの２次利用が頻繁に行われるＣＧＭサービスに対しては不適当である。なぜならば、自分が制作したコンテンツを広く見てほしいという著作者の希望に対して視聴制御は無意味であり、コピー制御はコンテンツの２次利用を妨げる。それに対して、ＣＧＭサービスに必要な著作権保護技術はコンテンツの編集を前提としたものであり、著作者が公開したコンテンツを２次利用させる際、その著作者の著作権を守る権利継承や編集制御と呼ばれる技術と考えられる。
【０００３】
権利継承とは、あるコンテンツが２次利用された時、２次コンテンツの中に元コンテンツの著作者の権利を正当に示すことである。これによって、著作者は自分のコンテンツが２次利用されても、自分の著作権が守られつつ自分のコンテンツが視聴されることになるため、自分が制作したコンテンツを広く見てほしいという希望が達成される。
【０００４】
また、編集制御とは著作者が制作したコンテンツに対して、２次利用できる範囲を制御するための技術である。編集制御は、著作者が自分のコンテンツを２次利用されたくない、または編集できる部分をある範囲内のみに制限したいという場合に有効である。
【０００５】
権利継承及び編集制御の二つの技術が揃って、コンテンツの２次利用が正当に促進されると考えられる。
【０００６】
これらの二つの技術については、電子署名を用いて実現する技術が提案されている（例えば、非特許文献１～３及び特許文献１参照）。権利継承に関しては、１次コンテンツの著作者とそれを利用する２次コンテンツの著作者との関係を示す署名を導入して順序関係を表現し、複数の署名を固定長の署名に集約することによって、１回の検証で第三者がそ

の署名の正当性を判断することができる。すなわち，署名順序が隣接する署名者間の前後において、後者が自分の署名対象となるメッセージと前者の署名対象となるメッセージの両方に対して署名し、この署名を順次合成していくことで順序付きアグリゲート署名を構成する。この手法は、この隣接署名者間の手順を１対多に拡張し、その関係を積み重ねることで木構造表記型のアグリゲート署名に拡張されている。

【０００７】

しかし、この手法はコンテンツの構成を署名に反映させるためのものであるため、これによって編集を制御することはできない。すなわち、著作者の意図しない編集を禁止することはできない。

【０００８】

編集制御については事前に設定した電子署名によってコンテンツの編集（部分コンテンツの削除・変更・追加）を制御可能にする。すなわち、著作者がコンテンツ制作後に編集の可否に応じてコンテンツを複数の部分コンテンツに分割し、部分コンテンツ毎に編集の可否を示す電子署名を事前設定し、署名を１つに集約する。以降、編集を制御するために部分コンテンツに設定する署名を編集制御署名と呼ぶ。編集を許可する部分コンテンツの編集制御署名は公開することによって集約した署名から削除して差し替えられるようにし、編集を許可しない部分コンテンツの編集制御署名は秘匿して差し替えられなくすることで、編集の可否を制御することができる。さらに、空データという制御用のデータを用いて、部分コンテンツの追加も制御可能にしているので、著作者は自分の意図しない編集を防ぐことができる。

【先行技術文献】

【非特許文献】

【０００９】

【非特許文献１】稲村勝樹、斉藤旭、岩村恵市、“拡張墨塗り署名を用いたコンテンツ編集事前制御システム”、電気学会論文誌、c133(4),802-815,2013.

【非特許文献２】稲村勝樹、斉藤旭、岩村恵市、“新しい改装表記型アグリゲート署名を用いたコンテンツ引用過程表記手法”、情報処理学会論文誌、Vol.53,No.92267-2278,Sep S2012.

【非特許文献３】佐野達彦、柿崎淑郎、稲村勝樹、岩村恵市、“コンテンツ二次利用に適した編集制御可能な電子署名システム”、CSS2011,302-3,2011,10.

【特許文献】

【００１０】

【特許文献１】国際公開２０１５／０４５１７３号

【発明の概要】

【発明が解決しようとする課題】

【００１１】

しかしながら、従来技術では、１つのコンテンツ内の編集のみを前提としており、複数のコンテンツ間の編集を想定していない。例えば、コンテンツＡの部分コンテンツをコンテンツＢに流用しようとする場合は想定していないため、コンテンツＡの部分コンテンツは自由にコンテンツＢに流用される。

【００１２】

さらに、従来技術では、部分コンテンツの流用を考慮していないため、部分コンテンツの設定が編集禁止でも、流用した人がその部分コンテンツに対して自由に編集（変更・削除・追加）に関する設定を変更することができる。すなわち、部分コンテンツに関する編集制御設定が流用先で維持されないという問題が発生する。

【００１３】

さらに、従来技術では、１つのコンテンツ内であっても編集が繰り返されると編集の整合性が維持できないか、全制御状態が維持できない場合が生じた。すなわち、従来技術では追加は追加用の制御署名によって制御され、削除は空データへの置き換えではなく実際の削除であったため、全制御状態を維持するとコンテンツ内における部分コンテンツの構

成が一定でなくなる。そのため、編集の整合性が維持できない場合が生じた。また、削除を空データへの変更とすると変更可能＝削除可能となるため、変更不可かつ削除可や変更可かつ削除不可などの制御状態が設定できない。

【００１４】

また、従来技術では、複数のコンテンツ間の編集を考慮していないため、例えばあるコンテンツに他のコンテンツからの部分コンテンツを流用した場合、どの部分コンテンツが元のコンテンツのもので、どの部分コンテンツが他のコンテンツのものかを区別できない。すなわち、コンテンツ自体を識別できない。

【００１５】

また、従来技術では複数のコンテンツ間の合成に関する制御も想定していなかった。そのため、部分コンテンツを全て流用禁止にできたとしても、コンテンツ自体が他のコンテンツに合成されれば、全ての部分コンテンツを流用したことと同じことになる。

【００１６】

さらに、コンテンツ自体の使用の可否も制御できなかった。すなわち、公開されたコンテンツが編集禁止かつ合成禁止でも、そのまま用いるのであれば自由に使用可能である。

【００１７】

また、従来技術では、電子署名によって１つのコンテンツ内の編集を制御するが、どのように部分コンテンツとその著作者（電子署名を検査する鍵）をバインドするかについては考慮されていなかった、また、複数のコンテンツを想定していないため、コンテンツ自体の著作者のバインドについても考慮されていなかった。すなわち、部分コンテンツまたはコンテンツと各著作者の対応を保証する技術は示されていなかった。基本的に著作者がその部分コンテンツまたはコンテンツに対する署名を生成するため、著作者を偽れると署名も偽れる可能性がある。

【００１８】

さらに、以上を全て電子署名だけで実現する手法については考慮されていなかった。例えば前述のコンテンツの使用制御は従来のコピー制御技術を用いれば実現できるが、従来のコピー制御は電子署名だけでは実現できない。

【００１９】

最後に、従来技術では、特定のアグリゲート（Aggregate）署名を用いて構成されており、ＩＤベース署名などの種々の電子署名によって構成できるか示されていない。

【００２０】

本発明は、上記問題に鑑みてなされたものであり、コンテンツ間及びコンテンツ内の双方の編集を考慮した著作権の保護を行うことができる管理局装置、著作権保護装置、編集装置、検証装置、管理プログラム、著作権保護プログラム、編集プログラム、及び検証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】

【００２１】

本発明の管理局装置は、複数の部分コンテンツから構成されるコンテンツの編集を電子署名によって制御するシステムにおいて、検査した部分コンテンツが予め定められた条件を満たした場合に、前記部分コンテンツと前記部分コンテンツを検証する鍵を特定する情報とに対して電子署名を生成する生成部を備える。

【００２２】

また、本発明の著作権保護装置は、複数の部分コンテンツから構成されるコンテンツの編集を電子署名によって制御するシステムにおいて、部分コンテンツに対して前記部分コンテンツの流用を制御する電子署名を生成する生成部と、前記部分コンテンツが含まれるコンテンツに対して前記電子署名を集約した集約署名を設定する設定部と、を備える。

【００２３】

また、本発明の著作権保護装置は、複数の部分コンテンツから構成されるコンテンツの編集を電子署名によって制御するシステムにおいて、部分コンテンツに対して編集を許可する場合、編集を許可する第１鍵を用いて電子署名を生成して前記第１鍵を特定する情報

を公開し、編集を不許可とする場合、編集を不許可とする第２鍵を用いて電子署名を生成して前記第２鍵を特定する情報を公開する生成部を備える。

【００２４】

また、本発明の著作権保護装置は、複数の部分コンテンツから構成されるコンテンツの編集を電子署名によって制御するシステムにおいて、部分コンテンツに対して前記部分コンテンツが含まれるコンテンツの合成を制御する電子署名を生成する生成部と、前記コンテンツに対して前記電子署名を集約した集約署名を設定する設定部と、を備える。

【００２５】

また、本発明の著作権保護装置は、複数の部分コンテンツから構成されるコンテンツの編集を電子署名によって制御するシステムにおいて、１つの部分コンテンツに対して複数の著作者の各々が行った修正を制御する電子署名を生成する生成部と、前記部分コンテンツまたは前記部分コンテンツが含まれるコンテンツに対して前記電子署名を集約した集約署名を設定する設定部と、を備える。

【００２６】

また、本発明の編集装置は、複数の部分コンテンツから構成されるコンテンツの編集を電子署名によって制御するシステムにおいて、電子署名が設定された部分コンテンツまたは当該部分コンテンツを含むコンテンツに対して変更、追加、削除、流用、及び合成のうち少なくとも１つを含む編集を行う編集部と、前記編集部が行った編集に応じて前記部分コンテンツに設定された前記電子署名を差し替えて集約署名の設定を更新する設定部と、を備える。

【００２７】

また、本発明の検証装置は、複数の部分コンテンツから構成されるコンテンツの編集を電子署名によって制御するシステムにおいて、部分コンテンツまたはコンテンツに対して変更、追加、削除、流用、及び合成のうち少なくとも１つを含む編集に関する署名の検証を行う検証部と、前記検証部の検証結果に応じて不正な編集が行われたコンテンツを検出する検出部を備える。

【００２８】

また、本発明の管理プログラムは、複数の部分コンテンツから構成されるコンテンツの編集を電子署名によって制御するシステムにおける管理局装置として、コンピュータにより、検査した部分コンテンツが予め定められた条件を満たした場合に、前記部分コンテンツと前記部分コンテンツを検証する鍵を特定する情報とに対して電子署名を生成する、ことを含む処理を行わせるものである。

【００２９】

また、本発明の著作権保護プログラムは、複数の部分コンテンツから構成されるコンテンツの編集を電子署名によって制御するシステムにおける著作権保護装置として、コンピュータにより、部分コンテンツに対して前記部分コンテンツの流用を制御する電子署名を生成し、前記部分コンテンツが含まれるコンテンツに対して前記電子署名を集約した集約署名を設定する、ことを含む処理を行わせるものである。

【００３０】

また、本発明の著作権保護プログラムは、複数の部分コンテンツから構成されるコンテンツの編集を電子署名によって制御するシステムの著作権保護装置として、コンピュータにより、部分コンテンツに対して編集を許可する場合、編集を許可する第１鍵を用いて電子署名を生成して前記第１鍵を特定する情報を公開し、編集を不許可とする場合、編集を不許可とする第２鍵を用いて電子署名を生成して前記第２鍵を特定する情報を公開する、ことを含む処理を行わせるものである。

【００３１】

また、本発明の著作権保護プログラムは、複数の部分コンテンツから構成されるコンテンツの編集を電子署名によって制御するシステムの著作権保護装置として、コンピュータにより、部分コンテンツに対して前記部分コンテンツが含まれるコンテンツの合成を制御する電子署名を生成し、前記コンテンツに対して前記電子署名を集約した集約署名を設定

する、ことを含む処理を行わせるものである。
【００３２】
また、本発明の著作権保護プログラムは、複数の部分コンテンツから構成されるコンテンツの編集を電子署名によって制御するシステムにおける著作権保護装置として、コンピュータにより、１つの部分コンテンツに対して複数の著作者の各々が行った修正を制御する電子署名を生成し、前記部分コンテンツまたは前記部分コンテンツが含まれるコンテンツに対して前記電子署名を集約した集約署名を設定する、ことを含む処理を行わせるものである。
【００３３】
また、本発明の編集プログラムは、複数の部分コンテンツから構成されるコンテンツの編集を電子署名によって制御するシステムにおける編集装置として、コンピュータにより、電子署名が設定された部分コンテンツまたは当該部分コンテンツを含むコンテンツに対して変更、追加、削除、流用、及び合成のうち少なくとも１つを含む編集を行い、行った編集に応じて前記部分コンテンツに設定された前記電子署名を差し替えて集約署名の設定を更新する、ことを含む処理を行わせるものである。
【００３４】
また、本発明の検証プログラムは、複数の部分コンテンツから構成されるコンテンツの編集を電子署名によって制御するシステムの検証装置として、コンピュータに、部分コンテンツまたはコンテンツに対して変更、追加、削除、流用、及び合成のうち少なくとも１つを含む編集に関する署名の検証を行い、検証結果に応じて不正な編集が行われたコンテンツを検出する、ことを含む処理を行わせるものである。
【発明の効果】
【００３５】
本発明によれば、コンテンツ間及びコンテンツ内の双方の編集を考慮した著作権の保護を行うことができる。
【図面の簡単な説明】
【００３６】
【図１】電子署名について説明するための説明図である。
【図２】集約署名（アグリゲート署名）について説明するための説明図である。
【図３】編集制御技術について説明するための説明図である。
【図４】権利継承技術について説明するための説明図である。
【図５】編集制御技術における部分コンテンツ、コンテンツ及び、制御署名、集約署名の関係について説明するための説明図である。
【図６】編集制御技術における正当な編集と不正な編集について説明するための説明図である。
【図７】編集制御技術におけるコンテンツの検証の原理について説明するための説明図である。
【図８】第１実施形態の著作権保護システムの一例の構成を示す構成図である。
【図９】第１実施形態におけるコンテンツの構造の一例を示す図である。
【図１０】第１実施形態の端末装置、管理局装置、及び検証装置の一例の構成を示したブロック図である。
【図１１】第１実施形態の部分コンテンツの一例を示す図である。
【図１２】図１１に示した部分コンテンツにより構成されるコンテンツの一例を示す図である。
【図１３】部分コンテンツの状態推移を説明する図である。
【図１４】第１実施形態の端末装置で実行される著作権保護処理の一例を表すフローチャートである。
【図１５】第１実施形態の管理局で実行される管理処理の一例を表すフローチャートである。
【図１６】第１実施形態の端末装置で実行される著作権保護処理における電子署名作成処

理の一例を表すフローチャートである。
【図１７】第１実施形態の端末装置で実行される編集処理の一例を表すフローチャートである。
【図１８】第１実施形態の検証装置で実行される検証処理の一例を表すフローチャートである。
【図１９】第１実施形態の端末装置で実行される編集処理における編集制御処理の一例を表すフローチャートである。
【図２０】第１実施形態の端末装置で実行される編集処理における合成・権利継承処理の一例を表すフローチャートである。
【図２１】第２実施形態の端末装置で実行される著作権保護処理における電子署名作成処理の一例を表すフローチャートである。
【図２２】第２実施形態の端末装置で実行される編集処理における編集制御処理の一例を表すフローチャートである。
【図２３】第２実施形態の検証装置で実行される検証処理の一例を表すフローチャートである。
【発明を実施するための形態】
【００３７】
まず、本発明の前提となる電子署名を用いた権利継承技術及び編集技術について説明する。
【００３８】
電子署名とは、著作権保護技術に用いられる要素技術の一つであり、偽造が難しく、改竄の検知が可能である。例えば、図１に示すようにコンテンツを制作して送信する送信者（著作者）は、ハッシュ関数を用いて制作したコンテンツＡをハッシュ値ｈに変換する。秘密鍵ｓを用いてハッシュ値ｈから電子署名である署名ａを得る。送信者は、署名ａとコンテンツＡとを送信する。
【００３９】
図１に示すように、送信されたコンテンツＡに改竄がない場合、署名ａ及びコンテンツＡを受信した受信者（コンテンツの正当性を検証する検証者）は、秘密鍵ｓに対応する公開鍵ｖを用いた署名ａからハッシュ値ｈを得る。また、コンテンツＡをハッシュ関数を用いてハッシュ値ｈに変換する。署名ａから得られたハッシュ値ｈと、コンテンツＡから変換されたハッシュ値ｈとが一致するため、受信したコンテンツＡが正当なコンテンツであるとの検証結果が得られる。
【００４０】
一方、図１に示すように、送信されたコンテンツＡが改竄された場合、署名ａ及びコンテンツＡを受信した受信者は、秘密鍵ｓとに対応する公開鍵ｖを用いた署名ａからハッシュ値ｈを得る。また、改竄されたコンテンツＡをハッシュ関数を用いてハッシュ値ｈ’（ｈ’≠ｈ）に変換する。署名ａから得られたハッシュ値ｈと、コンテンツＡから変換されたハッシュ値ｈ’とが一致しないため、受信したコンテンツＡが正当なコンテンツではない、すなわち改竄されたとの検証結果が得られる。
【００４１】
このような電子署名において集約署名（アグリゲート署名）と呼ばれる技術がある。集約署名とは、複数人の署名者（著作者）が、それぞれが制作した異なるコンテンツに対して行った署名を一つに集約した署名のことである。集約署名によれば、一つの署名で署名者全員の署名をまとめて検証することができる。また、集約署名によれば、一人でも署名を検証するための検証鍵やコンテンツの内容が異なれば検証に失敗し、コンテンツが改竄されたことがわかる。
【００４２】
例えば、図２に示すように、著作者Ａが制作したコンテンツＡから、署名鍵Ａを用いて署名Ａを得る。同様に、著作者Ｂが制作したコンテンツＢから、署名鍵Ｂを用いて署名Ｂを得、さらに著作者Ｃが制作したコンテンツＣから、署名鍵Ｃを用いて署名Ｃを得る。

【００４３】
そして、コンテンツＡ、コンテンツＢ、及びコンテンツＣを合成等した場合、各コンテンツに対応する個々の署名を用いずとも、全ての署名を集約した署名ＡＢＣを用いることにより、全てのコンテンツの署名（Ａ、Ｂ、及びＣ）を一括して検証することができる。
【００４４】
まず、編集制御技術について説明する。編集制御技術は上述したように、著作者が制作したコンテンツに対して、２次利用できる範囲を制御する技術である。図３に示した例では、「頭部の形状」というコンテンツには、「ヘアスタイル」及び「表情」の２つの部分コンテンツが含まれている。また、「体のデザイン」というコンテンツには、「体型」及び「ポーズ」の２つの部分コンテンツが含まれている。また、「服のデザイン」というコンテンツには、「衣装」及び「靴」の２つの部分コンテンツが含まれている。編集制御技術によれば、これら各部分コンテンツ毎に、編集を許可（「可」）するか否か（「否」）を、著作者が事前に制御（設定）することができる。図３に示した例では、「体型」及び「衣装」というコンテンツは編集が許可されていないが、他のコンテンツについては、他の著作者による編集が可能であり、当該コンテンツを用いて２次以降の著作物の作成が可能であることが示されている。
【００４５】
編集制御技術の基本原理について説明する。
【００４６】
オリジナルのコンテンツＡのデータは、複数の部分コンテンツのデータにより構成される。例えば、図５に示した例では、コンテンツＡは、部分コンテンツ$A_1$～$A_6$により構成されている。部分コンテンツ$A_1$～$A_6$の各々に対応して、編集に関する制御を行うための電子署名である制御署名$\sigma_1$～$\sigma_6$が設定される。編集制御技術では、編集を許可する部分コンテンツに対応する制御署名のみを公開する。さらに、コンテンツＡに対して制御署名$\sigma_1$～$\sigma_6$を集約した集約署名σが設定される。集約署名σは、部分コンテンツの編集が行われた際、対応する制御署名について編集内容に応じて減算または加算を行う。
【００４７】
例えば、上述した編集制御技術の例（図３参照）に適用した場合、部分コンテンツ$A_1$～$A_6$はそれぞれ、「ヘアスタイル」、「表情」、「体型」、「ポーズ」、「衣装」、及び「靴」に対応する。部分コンテンツ$A_3$の「体型」及び部分コンテンツ$A_5$の「衣装」については、編集（ここでは、削除）が許可されていないため、図６に示すように、削除用の公開署名は、制御署名$\sigma_1$、$\sigma_2$、$\sigma_4$、及び$\sigma_6$が設定される。一方、削除用に用意する削除用集約署名は、図６に示すように全ての制御署名（$\sigma_1$～$\sigma_6$）を集約した集約署名が設定される。
【００４８】
図６には、この状態で、正当な編集を行う場合の例として部分コンテンツ$A_4$の「ポーズ」を削除した場合、及び不正な編集を行う場合の例として部分コンテンツ$A_3$の「体型」を削除した場合を示している。
【００４９】
部分コンテンツの削除を行う場合、削除用公開署名を参照し、削除した部分コンテンツに対応する制御署名を削除用集約署名から削除する。
【００５０】
図６に示した例では、正当な編集を行った場合、削除用公開署名に部分コンテンツ$A_4$に対応する制御署名$\sigma_4$が含まれるため、当該制御署名$\sigma_4$を削除用集約署名σから削除する。一方、不正な編集を行った場合、削除用公開署名に部分コンテンツ$A_3$に対応する制御署名$\sigma_3$が含まれていないため、当該制御署名$\sigma_3$を削除用集約署名σから削除することができない。正当か不正にかかわらず、編集を行った編集者は、編集済みのコンテンツ及び削除用集約署名σを公開する。
【００５１】
正当な編集が行われたか否か、すなわち編集済みのコンテンツについて正当であるか否

かについては、検証を行うことにより判定することができる。

【００５２】

当該検証は、編集済みのコンテンツと検証鍵を用いて、ペアリング関数により編集者の発行した集約署名を検証することにより行われる。

【００５３】

図７に示すように正当な編集を行った場合は、編集済みのコンテンツは部分コンテンツ$A_1$～$A_3$、$A_5$、及び$A_6$が含まれているため、当該コンテンツから得られるハッシュ値は、ハッシュ値$h_1$～$h_3$、$h_5$、$h_6$を含む。また、削除用集約署名σ（＝$\sigma_1+\sigma_2+\sigma_3+\sigma_5+\sigma_6$）も$A_1$～$A_3$、$A_5$、及び$A_6$に対応する署名$\sigma_1$～$\sigma_3$、$\sigma_5$、$\sigma_6$を含む。ペアリング関数ｅはコンテンツに対応する集約署名σと、コンテンツから得られるハッシュ値$h_j$の対応が正しければ検証鍵$v_j$と検証鍵の生成元ｇを用いて下記（１）式が成立するため、正当な編集が行われた正当なコンテンツであると判定することができる。

【００５４】

【数１】

$$e(g,\sigma)=\Pi e\left(gv_i,h_j\right) \quad \cdots(1)$$

一方、図７に示すように不正な編集を行った場合は、編集済みのコンテンツは部分コンテンツ$A_1$、$A_2$、及び$A_4$～$A_6$が含まれているため、当該コンテンツから得られるハッシュ値は、ハッシュ値$h_1$、$h_2$、及び$h_4$～$h_6$を含む。また、削除用集約署名σ（＝$\sigma_1+\sigma_2+\sigma_3+\sigma_4+\sigma_5+\sigma_6$）は全部分コンテンツに対応する$\sigma_1$～$\sigma_6$を含む。この場合、コンテンツから得られるハッシュ値と、コンテンツに対応する集約署名とが正しく対応しないため、上記（１）式が成立しないため、不正な編集が行われた不正なコンテンツであると判定することができる。

【００５５】

なお、ここでは編集の具体例として編集の種類が削除の場合について具体的に説明したが、編集の種類が変更または追加の場合は、新規の部分コンテンツに対応する制御署名を作成し、作成した制御署名を集約署名に加算する。

【００５６】

一方、権利継承技術について説明する。上述したように、権利継承技術とは、１次著作者が制作したコンテンツを利用して制作した２次以降の著作者の新しいコンテンツの中において、１次著作者の権利が保証される技術である。

【００５７】

図４に示した例では、著作者Ａが制作した頭部の形状、著作者Ｂが制作した体のデザイン、及び著作者Ｃが制作した服のデザインを用いて著作者Ｄがキャラクタの正面画を制作し、著作者Ｅが背面画を制作した場合、著作者Ａ～Ｃは、１次著作者にあたり、著作者Ｄ、Ｅは２次著作者にあたる。さらに、当該キャラクタを使用して著作者Ｆが動画を制作した場合、著作者Ｆは、３次著作者にあたる。さらに、当該動画、著作者Ｇが制作した音楽、及び著作者Ｈが制作した声を組み合わせてアニメーション作品を著作者Ｉが制作した場合、著作者Ｉは、著作者Ａ～Ｃが制作したコンテンツから見ると、４次著作者にあたる。

【００５８】

ここで、著作者Ａ～Ｃ各々の権利（著作権）は、２次～４次著作物のいずれにおいても保護される必要がある。また、１つの作品、例えば図４に示した例では、アニメーション作品において、著作者Ａ～Ｊ、全員の関係を表現する必要がある。これらを満たす技術を権利継承技術という。

【００５９】

１次著作者Ａ～Ｃと２次著作者Ｄの関係を例に説明すると、著作者Ａ～Ｃが各々のコンテンツに対するハッシュ値$h_A$～$h_C$に対して各々の署名鍵$s_A$～$s_C$を用いて、署名$\sigma_A$～$\sigma_C$を生成する。著作者Ｄは合成したキャラクタに対するハッシュ値$h_D$を生成し、

1次著作者の署名$\sigma_A$～$\sigma_C$を用いて下記（２）式の署名を生成する。

【００６０】

【数２】

$$\sigma_D = \sigma_A + \sigma_B + \sigma_C + s_D(h_A + h_B + h_C + h_D) \quad \cdots(2)$$

これは、$s_D h_A$～$s_D h_D$を１つの署名とみなせば前述の集約署名となっているが、２次著作者Ｄが１次著作者Ａ～Ｃのコンテンツのハッシュ値とその合成コンテンツのハッシュ値に自らの署名鍵$s_D$を用いて署名をしていることからその関係を示すことができる。

この場合、検証は著作者Ｄの２次コンテンツに関わるハッシュ値$h_A$～$h_D$と著作者Ａ～Ｄの検証鍵$\nu_A$～$\nu_D$を用いて下記（３）式が成り立つことによって、権利継承署名$\sigma_D$が著作者Ａ～Ｄ間の関係を表すことが検証できる。下記（３）式は権利継承署名$\sigma_D$が検証鍵$\nu_D$をもつ著作者を２次著作者として、検証鍵$\nu_A$をもつ著作者のコンテンツ（のハッシュ値$h_A$）と、検証鍵$\nu_B$をもつ著作者のコンテンツ（のハッシュ値$h_B$）と、検証鍵$\nu_C$をもつ著作者のコンテンツ（のハッシュ値$h_C$）とから構成されていることを示す。

【００６１】

【数３】

$$e(g, \sigma_D) = e(\nu_D, h_D)e(\nu_D + \nu_A, h_A)\, e(\nu_D + \nu_B, h_B)e(\nu_D + \nu_C, h_C) \quad \cdots(3)$$

本発明は、このような電子署名を用いた権利継承技術及び編集制御技術に対する従来技術に生じる下記の問題を解決する。

【００６２】

（２）編集制御に関する従来技術は１つのコンテンツ内における編集（変更・追加・削除）のみを対象としており、他のコンテンツへの部分コンテンツの流用の可否を制御することができない。

【００６３】

（４）従来技術は複数のコンテンツ間の編集を考慮していないため、部分コンテンツを流用された場合、流用された部分コンテンツの編集制御に関する設定を維持することができない。

【００６４】

（３）部分コンテンツの追加・削除・変更を繰り返すと、コンテンツの構成が変化するか、変更可かつ削除不可や、変更不可かつ削除可等の状態を設定することができない。

【００６５】

（４）コンテンツ自体を識別することができないため、コンテンツの合成や使用自体を制御することができない。

【００６６】

（５）部分コンテンツと各種署名のバインドとを保証する技術が示されておらず、上記を実現する技術を電子署名だけで実現することができない。

【００６７】

（６）特定の署名を前提としており、ＩＤベース署名などを含む種々の電子署名での構成法が示されていない。

【００６８】

以下、図面を参照して本発明の実施形態を詳細に説明する。

［第１実施形態］

まず、本実施形態の著作権保護システムの構成について説明する。

【００６９】

図８に示すように、本実施形態の著作権保護システム１０は、端末装置１２$_1$～１２$_W$

と、管理局装置１４と、検証装置１６と、を備える。なお、本実施形態では、具体例として、ｗ個の端末装置１２（著作者及び編集者）を示したが、ｗの数は２以上であればよく、特に限定されるものではない。以下では、端末装置$１２_{1}$～$１２_{W}$を総称する場合は、端末装置１２という。

【００７０】

端末装置１２、管理局装置１４、及び検証装置１６は、ネットワーク１９を介して、互いに各種データの授受が可能に接続されている。

【００７１】

本実施形態の著作権保護システム１０は、端末装置１２を操作する著作者が作成したコンテンツの著作権を保護するシステムである。著作権保護システム１０は、著作者の著作権を保護するために、著作者の意図に反する編集を抑制することを目的として、著作者の意図に反した不正な編集が行われたコンテンツ（不正なコンテンツ）を検出する。

【００７２】

なお、本実施形態の著作権保護システム１０は、違反処理（不正な編集）が行われることによって正当なコンテンツが不正なコンテンツとされることが防止されるものではない。しかしながら、基本的にコンテンツの編集は、編集元となるコンテンツをコピーしたものに対して行われるため、元のコンテンツには影響しない。一方、違反処理によって不正コンテンツとなると、ネットワーク１９等に公開しても誰も視聴できないコンテンツとなるため、違反処理をした著作者のみが不利益をこうむることになり、故意に違反処理をするメリットはない。そのため、本実施形態の著作権保護システム１０によれば、違反処理が行われることそのものを防止せずとも、著作権を保護することができる。

【００７３】

端末装置１２は、著作者または編集者が使用する装置である。本実施形態では、複数の著作者によって制作されたコンテンツの合成も対象とするため、編集者という言葉は使用せず、著作者と総称するか、またはｉ次著作者という。ｉは後述するようにコンテンツの構造によって定まる。

【００７４】

ｉ次著作者は、あるコンテンツの制作及び編集に係り、自分が設定可能なコンテンツの編集制御署名を設定する。本実施形態では簡略化のため、あるコンテンツを図９に示すように木構造によって表し、一番深い部分にいる著作者を１次著作者とし、木の高さをｎ－１としたとき、ルートとなっている著作者をｎ次著作者と呼ぶ。よって、オリジナルコンテンツを持つ著作者でもｎ次著作者によって利用された場合はｎ－１次著作者と呼ばれる。ｉ次著作者は自分が制作または編集した部分に対して編集制御署名を設定でき、ｉ－１次以前の著作者が定めた編集制御署名に関して編集が許可されている場合のみ編集が可能である。

【００７５】

図９に示した例では、$Ａ_{11}$～$Ａ_{16}$を複数の１次著作者が制作した１次コンテンツとし、それを組み合わせて２次著作者が２次コンテンツ$Ａ_{21}$、$Ａ_{22}$を制作し、最後に３次著作者が完成形となるコンテンツ$Ａ_{31}$を制作した場合を示している。ここでは、２次著作者は各１次著作者が定めた編集制御署名の設定に従って編集を行い、３次著作者は各１次及び２次著作者が定めた編集制御署名の設定に従って編集を行う。

【００７６】

なお、各コンテンツは必ず異なる著作者によって制作されているとは限らず、例えば$Ａ_{11}$と$Ａ_{12}$は同一著作者であってもよい。

【００７７】

本実施形態において、端末装置１２は、当該端末装置１２を使用するｉ次著作者のｉの位置に応じて、本発明の著作権保護装置及び編集装置の少なくとも一方の機能を有する。

【００７８】

検証装置１６は、コンテンツが正当な電子署名を有しているか、すなわち、コンテンツが正当であるか否かを検証する機能を有する。なお、以下では、検証を行うものを便宜上

「検証者」と称するが、本実施形態では検証装置１６が後述する検証プログラムを実行することにより、検証者として機能する。

【００７９】

例えば、検証装置１６をコンテンツ再生機器等に持たせることにより、正当な電子署名を有さないコンテンツは再生できない著作権保護システム１０を構築することができる。

【００８０】

また、検証装置１６は端末装置１２の中に含ませることをもできる。端末装置１２が編集装置である場合、コンテンツは検証装置１６によってその正当性を検証され、それが正当であった場合に編集が行われる。

【００８１】

管理局装置１４は、著作者が制作したコンテンツを構成する部分コンテンツと、当該著作者との紐付けを行う機能を有する。以下、管理局装置１４を簡略化して管理局１４という。

【００８２】

管理局１４は、著作者が制作したコンテンツを構成する部分コンテンツと他のコンテンツとの類似度を検査することにより、当該部分コンテンツのオリジナル性を検査する。管理局１４は、当該部分コンテンツがオリジナルであると認めた場合に著作者を確認して、当該部分コンテンツに対して管理局署名を行う。本実施形態の著作権保護システム１０では、管理局署名のない部分コンテンツを不正と判定する。

【００８３】

すなわち、攻撃者（不正な編集を行う者）が既存の部分コンテンツまたは既存の部分コンテンツを少し修正した部分コンテンツに対して管理局署名を得ようとしても管理局の検査によりオリジナルでないとされる。そのため、このような部分コンテンツは管理局署名を得ることができず、また、管理局署名の偽造もできない。

【００８４】

以上のように、本実施形態の著作権保護システム１０では、正当な管理局署名のない部分コンテンツは不正コンテンツとされるため、当該部分コンテンツへの著作者の紐付けが確実なものとなる。

【００８５】

なお、管理局１４が行う部分コンテンツの類似度の検査方法は特に限定されず、既存の手法を用いることができる。例えば、部分コンテンツが画像である場合は、画像類似検索技術により容易に実現することができる。

【００８６】

本実施形態の端末装置１２、管理局１４、及び検証装置１６は、同様の構成である。図１０に示すように、端末装置１２、管理局装置１４、及び検証装置１６の各々は、制御部２０、記憶部２８、表示部駆動部３０、表示部３２、操作入力検出部３４、操作部３６、及びインターフェース部３８を備えている。

【００８７】

制御部２０、記憶部２８、表示部駆動部３０、操作入力検出部３４、及びインターフェース部３８は、システムバスやコントロールバス等のバス３９を介して相互に情報等の授受が可能に接続されている。

【００８８】

制御部２０は、ＣＰＵ（Central Processing Unit）２２、ＲＯＭ（Read Only Memory）２３、及びＲＡＭ（Random Access Memory）２４を備えている。ＣＰＵ２２は、端末装置１２全体の動作を制御する。ＲＯＭ２３には、ＣＰＵ２２で使用される各種の処理プログラム等が予め記憶されている。ＲＡＭ２４は、各種データを一時的に記憶する機能を有している。

【００８９】

端末装置１２の場合、ＲＯＭ２３には、著作権保護プログラム及び編集プログラムが予め記憶されており、ＣＰＵ２２が当該著作権保護プログラム及び編集プログラムプログラ

ムをＲＯＭ２３から読み出してＲＡＭ２４に展開し、当該著作権保護プログラム及び編集プログラムプログラムを実行する。著作権保護プログラムを実行する場合は、端末装置１２が著作権保護装置として機能し、制御部２０が、本発明の端末装置における生成部及び設定部として機能する。また、編集プログラムを実行する場合は、端末装置１２が編集装置として機能し、制御部２０が、本発明の端末装置における編集部及び設定部として機能する。

【００９０】

また、管理局１４の場合、ＲＯＭ２３には、管理プログラムが予め記憶されており、ＣＰＵ２２が当該管理プログラムをＲＯＭ２３から読み出してＲＡＭ２４に展開し、当該管理プログラムを実行する。これにより、制御部２０が、本発明の管理局装置における検査部及び生成部として機能する。

【００９１】

また、検証装置１６ＲＯＭ２３には、検証プログラムが予め記憶されており、ＣＰＵ２２が当該検証プログラムをＲＯＭ２３から読み出してＲＡＭ２４に展開し、当該検証プログラムを実行する。これにより、制御部２０が、本発明の検証装置における検証部及び検出部として機能する。

【００９２】

記憶部２８は、各種データを記憶する。本実施形態では、端末装置１２及び検証装置１６の各々に応じた種類の鍵（詳細後述）が記憶される。記憶部２８の具体例としては、不揮発性のメモリ等が挙げられる。

【００９３】

インターフェース部３８は、無線通信または有線通信により、ネットワーク１９を介して、他の装置との間で各種情報の通信を行う。

【００９４】

表示部駆動部３０は、表示部３２への各種情報の表示を制御する。操作入力検出部３４は、操作部３６に対する操作状態を検出することにより、著作者が操作部３６により行った入力について検出する。操作部３６は、著作者がコンテンツの制作や編集、編集制御に関する指示等を行うために用いられる。本実施形態では操作部３６は、例えば、タッチパネル、タッチペン、複数のキー、及びマウス等を含んでいる。なお、操作部３６０をタッチパネルとする場合は、表示部３２と同一としてもよい。

【００９５】

なお、管理局装置１４及び検証装置１６については、表示部駆動部３０、表示部３２、操作入力検出部３４、及び操作部３６は必須の構成ではない。

【００９６】

次に、本実施形態の著作権保護システム１０の作用について説明する。本実施形態の著作権保護システム１０では、電子署名として、ＢＬＳ署名を用いている。そのため、まずＢＬＳ署名について説明する。

【００９７】

Boneh, Lynn, Shachamにより、ペアリング関数ｅを利用することで、楕円曲線上の演算においてＧＤＨ（Gap Diffie-Hellman）問題に基づく電子署名方式が実現できることが示され、ＢＬＳ署名方式の提案が行われた。

【００９８】

ＢＬＳ署名を基に、署名対象となるメッセージが各署名者で全て異なっている電子署名を集約し、署名サイズが署名者数に依存せずに一定値以下とすることを可能としたアグリゲート署名方式が提案されている。

【００９９】

下記（４）式を署名の作成が可能な署名者のグループとして定義し、さらに、下記（５）式を実際にアグリゲート署名の作成に参加した署名者のグループとして定義する。

【０１００】

【数４】

$$U = \{u_1 \ldots, u_n\} \quad \cdots(4)$$
$$L = \{u_{i1}, \ldots, u_{it}\} \subseteq U \quad \cdots(5)$$

さらに下記（６）式を、上記アグリゲート署名へ参加した署名者を示す符号(ｕ$_{k}$のｋに相当)の全員分の集合とする。

【０１０１】

【数５】

$$J = \{i_i, \quad \ldots, i_{it}\} \quad \cdots(6)$$

この場合、アグリゲート署名は以下の通りに構成される。

【０１０２】

鍵として、署名者の署名鍵及び署名を検証するための検証鍵を生成する。

【０１０３】

ｇ∈Ｇ$_{1}$を生成元とする。署名者ｕ$_{i}$∈Ｕについてｘ$_{i}$∈Ｚ$_{p}$を選び、ｖ$_{i}$＝ｘ$_{i}$ｇを計算する。なお、全ての署名者の署名鍵は各々異なるものとする。ｘ$_{i}$を署名者ｕ$_{i}$の署名鍵、ｖ$_{i}$を署名者ｕ$_{i}$の検証鍵とする。Ｇ$_{1}$及びＧ$_{2}$は、位数ｐの乗法巡回群である。

【０１０４】

まず、署名者ｕ$_{i}$の署名ｘ$_{i}$から電子署名を作成する。一方向性ハッシュ関数Ｈを下記（７）式のように定義する。

【０１０５】

【数６】

$$H : \{0, 1\}^* \rightarrow G_2 \quad \cdots(7)$$

ｍ$_{j}$をアグリゲート署名の作成に参加する署名者ｕ$_{j}$∈Ｌの署名の対象となるメッセージとしたとき、署名者ｕ$_{j}$∈Ｌはｈ$_{j}$＝Ｈ（ｍ$_{j}$）を計算する。σ$_{j}$をｍ$_{j}$に対する署名者ｕ$_{j}$の電子署名とすると、下記（８）式により、電子署名σ$_{j}$が得られる。

【０１０６】

【数７】

$$\sigma_j = x_j h_j \quad \cdots(8)$$

次に電子署名σ$_{i}$を集約した集約署名σを作成する。アグリゲート署名の作成に参加する全ての署名者の電子署名σ$_{j}$を集め、下記（９）式を計算する。

【０１０７】

【数８】

$$\sigma = \Sigma\sigma_j \quad (j \in J) \quad \cdots(9)$$

（ｍ$_{i 1}$、・・・、ｍ$_{i t}$、Ｌ、σ）をメッセージとアグリゲート署名の組とする。

【０１０８】

ある電子署名が正当に作成された集約署名σであるか否かを判定する場合は、検証鍵ｖ$_{i}$を用いて検証を行う。検証者に（ｍ$_{i 1}$、・・・、ｍ$_{i t}$、Ｌ、σ）及びｇが与えられ、さらに、Ｌから検証に必要となる全ての検証鍵ｖ$_{i}$（ｊ∈Ｊ）が得られたとき、検証者は全てのｍ$_{j}$からｈ$_{j}$＝Ｈ（ｍ$_{j}$）を計算し、ペアリング関数を用いて下記（１０）式を判定式として用い、当該判定式が成り立つかの判定を行う。

【０１０９】

【数９】

$$e(g,\sigma)=\Pi e(v_j,h_j)\ (j\in J) \qquad \cdots(10)$$

このとき、電子署名が正しく作成されている（正当である）場合、検証における判定式（上記（１０）式）の左辺は下記（１１）式で表される。また、右辺は、下記（１２）式で表される。

【０１１０】

【数１０】

$$e(g,\sigma)=e(g,\Sigma x_j h_j)=\Pi e(g,x_j h_j)=\Pi e(g,h_j)^{x_j} \qquad \cdots(11)$$

$$\Pi e(v_j,h_j)=\Pi e(x_j g,h_j)=\Pi e(g,h_j)^{x_j} \qquad \cdots(12)$$

上記（１１）式及び（１２）式から分かるように、右辺と左辺とが同じ値になり、判定式（上記（１０）式）が成り立つ。

【０１１１】

一方、電子署名が正しく作成されていない（不正である）場合、右辺と左辺とが同じ値にならず、判定式（上記（１０）式）が成り立たたない。

【０１１２】

従って、判定式（上記（１０）式）が成り立つ場合は、電子署名が正当であり、成り立たない場合は、電子署名が不正であると判定することができる。

【０１１３】

次に、本実施形態の著作権保護システム１０における部分コンテンツとコンテンツの構成、及びこれらに対する著作者の紐付け方法について説明する。

【０１１４】

著作者は著作者を識別するための著作者ＩＤを有し、著作者が制作した各コンテンツにはコンテンツＩＤが設定され、各部分コンテンツにも部分コンテンツＩＤが設定される。例えば、図９に示したコンテンツの場合、$A_{11}$は著作者$ID_{11}$によって制作されたコンテンツであり、そのコンテンツＩＤを$IC_{11}$とする。$A_{11}$はｍ個の部分コンテンツ$A_{111}$～$A_{11m}$によって構成され、$A_{111}$の前には開始データが置かれ、$A_{11m}$の後には最終データが置かれる。$A_{111}$～$A_{11m}$には各々部分コンテンツＩＤとして$I_{111}$～$I_{11m}$が設定されている。

【０１１５】

図１１には、本実施形態における部分コンテンツの一例を示す。著作者は、制作した部分コンテンツを、図１２に例示したコンテンツの形式で公開する。図１２は、具体例とし、ｍ＝４として著作者$ID_{11}$が制作したコンテンツ$IC_{11}$の構成例を示している。

【０１１６】

本実施形態では、実データ、空データ、開始データ、及び最終データの４種類のデータが存在する。実データと空データを合わせて部分コンテンツと呼ぶ。実データは、コンテンツを構成する基本的なデータであり、表示機器が表示の対象とするデータである。一方、空データは、追加が予定されている部分コンテンツや削除した部分コンテンツに替わって置かれるデータであり、空データは追加や削除を制御するための制御データとして扱われる。制御データは、表示機器が表示対象としないデータである。

【０１１７】

開始データはコンテンツの開始位置に置かれ制御データとして扱われる。また、最終データはコンテンツの最終位置に置かれ制御データとして扱われる。コンテンツは開始データと、一つ以上の部分コンテンツと、最終データと、によって構成される。各データの種類は、予め定められた識別子（図１１、識別子参照）によって区別される。なお、当該識別子をどのように設定するかについては、特に限定されるものではない。

【０１１８】
図１２に示した例では、全部分コンテンツの著作者ＩＤ$_1$に著作者ＩＤ$_{11}$が設定され、コンテンツＩＤにはＩＣ$_{11}$が設定された状態を示している。部分コンテンツＩＤがＩ$_{110}$のデータは開始データ、Ｉ$_{111}$、Ｉ$_{113}$、及びＩ$_{114}$のデータは実データ、Ｉ$_{112}$のデータは空データ、及びＩ$_{115}$のデータは最終データを表す。
【０１１９】
部分コンテンツには、当該部分コンテンツを制作した著作者を識別するための著作者ＩＤ（以降、著作者ＩＤ$_1$という）が紐付けされている。この紐付けは、上述したように管理局１４が部分コンテンツと著作者ＩＤ$_1$の連接のハッシュ値に対して署名を行うことにより保証される。なお、部分コンテンツのうち、実データではない制御データは管理局署名を有さなくてもよい。
【０１２０】
実データ及び空データには、後述する署名検証のため、著作者ＩＤ$_1$の他に、各種パラメータと紐付けされている。図１１及び図１２に示すように、各種パラメータは、コンテンツＩＤ（ＩＣ）、部分コンテンツＩＤ（Ｉ）、データの識別子（開、実、空、及び終）を含む。また、各種パラメータは、後述する編集を制御するための各種編集制御署名（$\sigma_k$、$\tau_k$、$\chi_k$、$\delta_k$、$\zeta_k$）または署名用ハッシュ値（$h_k$）、編集不可とした著作者を識別するための著作者ＩＤ（以降、著作者ＩＤ$_2$という）、著作者ＩＤ$_1$を保証する管理局署名（μ）、及び流用可否情報や署名回数等その他の情報を含む。
【０１２１】
図１１及び図１２では部分コンテンツのヘッダ部に各種パラメータを設定して部分コンテンツやコンテンツと種々のパラメータとの紐付けを行う場合を示すが、これらは上書きや変更が可能である。ただし、攻撃者がこれらのデータを不正に変更すると、著作者ＩＤ$_1$に関しては上述の仕組みによって、それ以外は後述のアルゴリズムにより署名の整合性が合わなくなることにより不正が検出される。
【０１２２】
なお、部分コンテンツやコンテンツへの種々のパラメータの紐付け方法は各データのヘッダ部への設定に限定されるものではなく、各種紐付け情報をまとめて管理するディレクトリなどを用意し、各部分コンテンツまたはコンテンツ毎に管理していてもよい。または、電子透かし等によって紐付けを行ってもよい。
【０１２３】
また、開始データと最終データには後述する各種編集制御の集約署名や権利継承署名等のコンテンツ単位で設定される情報と紐付けされている。開始データにはコンテンツ単位の各種検証情報が紐付けされている。図１２に示すように、本実施形態の開始データは、コンテンツＩＤ、部分コンテンツＩＤ、識別子に加えて、各種編集制御の集約署名σ、τ、χ、δ、及び権利継承署名ζ等と紐付けされている。本実施形態の最終データには、コンテンツの使用条件及び使用制御署名λが紐付けされている。これらのパラメータもすべて上書きや変更が可能である。ただし、上記は紐付けの一例であって、開始データと最終データへ紐付ける情報の対応は上記に限定されるわけではない。例えば、開始データまたは最終データに全ての情報を紐付けてもよい。
【０１２４】
図１２に示した例では、部分コンテンツＩＤがＩ$_{111}$、Ｉ$_{112}$、及びＩ$_{113}$のデータは後述する変更制御署名$\sigma_k$が公開されているため変更可であり、部分コンテンツＩＤがＩ$_{114}$のデータは変更制御署名$\sigma_k$の代わりに署名用ハッシュ値ｈと著作者ＩＤ$_2$が公開されているため変更不可であることを表している。また、部分コンテンツＩＤがＩ$_{111}$とＩ$_{114}$のデータは後述する削除制御署名$\tau_k$の代わりに署名用ハッシュ値ｈと著作者ＩＤ$_2$が公開されているため削除不可、部分コンテンツＩＤがＩ$_{112}$とＩ$_{113}$のデータは削除制御署名$\tau_k$が公開されているため削除可であることを表している。また、部分コンテンツＩＤがＩ$_{111}$とＩ$_{112}$のデータは後述する流用制御署名$\chi_k$が公開されていないため流用不可、部分コンテンツＩＤがＩ$_{113}$とＩ$_{114}$のデータは流用制

御署名$\chi_k$が公開されているため流用可（流用可の場合コンテンツＩＤは特定値が設定され、ここではＩＣ$_{00}$と表記する）であることを表している。また、全部分コンテンツの合成制御署名$\delta_k$が公開されているためコンテンツの合成が可であり、空データを除く全部分コンテンツは管理局署名μを有し、署名回数は０、すなわち初めての署名であることを表している。

【０１２５】

次に、上述した部分コンテンツの各種編集制御について説明する。本実施形態の著作権保護システム１０で行われる編集制御の種類は、上述したように、変更、追加、削除、流用、合成、及び使用が挙げられる。

【０１２６】

まず、変更制御及び追加制御について説明する。

【０１２７】

本実施形態の著作権保護システム１０では、追加は空データから実データへの変更として扱うため、追加の場合における編集制御は変更制御に含まれる。各部分コンテンツに対して変更制御と削除制御を独立に設定することによって、著作権保護システム１０では、部分コンテンツの変更可かつ削除不可、及び変更不可かつ削除可という制御を実現することができる。例えば、コンテンツが各コマを部分コンテンツとする四コマ漫画の場合、各コマの変更を認める場合、四コマ漫画であるためには各部分コンテンツを変更可かつ削除不可とする制御を行うことができる。また、コンテンツが動画等において、画面（画像）の隅に表示される著作権クレジットを１つの部分コンテンツとする場合、見やすくするために著作権クレジットを削除または非表示にしてもよいが、変更はできないとする、変更不可かつ削除可とする制御を行うことができる。

【０１２８】

変更制御署名$\sigma_k$とは、変更用定数と部分コンテンツ及び検証に必要なパラメータのハッシュ値に対して行った署名である。変更可の場合、変更制御署名$\sigma_k$は公開され、変更不可の場合、変更制御署名$\sigma_k$は公開されずに、代わりに、そのときの署名用ハッシュ値と変更不可と設定した著作者のＩＤが著作者ＩＤ$_2$として公開される。空データに対して変更可と設定すれば、当該空データは実データに変更することが可能になる。一方、空データに対して変更不可と設定すれば、削除状態が固定される。

【０１２９】

削除制御署名$\tau_k$とは、削除用定数と部分コンテンツ及び検証に必要なパラメータのハッシュ値に対して行った署名である。削除可の場合、削除制御署名$\tau_k$は公開され、削除不可の場合、削除制御署名$\tau_k$は公開されずに、代わりに、そのときの署名用ハッシュ値と削除不可と設定した著作者のＩＤが著作者ＩＤ$_2$として公開される。空データの削除は空データへの置き換えであり、空データを削除不可としても変更可であればその状態は固定されないため、空データに対する削除制御は意味がない。よって、空データは変更可であれば削除可、変更不可であれば削除不可にのみ設定可能とする。

【０１３０】

変更集約署名σは上記変更制御署名$\sigma_k$をＢＬＳ署名に従って集約したものである。削除集約署名τは上記削除制御署名$\tau_k$をＢＬＳ署名に従って集約したものである。集約署名は「開始位置署名＋部分コンテンツの編集制御署名群＋最終位置署名」の構成を持つ。本実施形態の著作権保護システム１０では、開始位置署名と最終位置署名とは常に非公開である。これによって、部分コンテンツが１つで編集不可でもその編集制御署名がそのまま集約署名として公開されることはなく、開始位置署名と最終位置署名と不可分の形で公開される。コンテンツ毎に集約署名は紐づけられて公開され、集約署名を付与せず公開されたコンテンツは不正コンテンツとして扱われる。

【０１３１】

署名を行う際、部分コンテンツＩＤまたはコンテンツＩＤにはその部分コンテンツまたはコンテンツを特定する本来のＩＤに加えて、著作回数に関する情報も含む。これは同一著作者が同一コンテンツに対して署名した場合、区別がつくようにするためである。例え

ば、図９においてＩＣ$_{11}$（Ａ$_{21}$）を著作者ＩＤ$_{11}$が制作し、次に著作者ＩＤ$_{11}$が著作者ＩＤ$_{21}$としてＡ$_{21}$を作る場合再びＩＣ$_{11}$に署名するが、この場合２回目の署名であるため回数を更新して署名内容を変更して署名する。

【０１３２】

検証者は部分コンテンツが変更可であれば、その部分コンテンツの変更制御署名用ハッシュ値を計算し、管理局署名μを検査してその著作者ＩＤ$_1$の検証鍵で集約署名の検証を行う。

【０１３３】

変更不可であれば、公開された署名検査用ハッシュ値とその部分コンテンツの整合を確認し、合えば著作者ＩＤ$_2$の検証鍵で集約署名の検証を行う。ただし、部分コンテンツが空データで変更不可（すなわち、削除不可）の場合は、その空データと削除制御署名検査用ハッシュ値との整合を確認し、整合すれば著作者ＩＤ$_2$の検証鍵で削除集約署名の検証を行う。それ以外の場合は、部分コンテンツと署名用ハッシュ値が整合しなくとも著作者ＩＤ$_2$の検証鍵で集約署名の検証を行う。

【０１３４】

以上より、本実施形態の著作権保護システム１０では、編集可と設定できるのはその部分コンテンツを制作した著作者（著作者ＩＤ$_1$）のみであり、それ以降の著作者（著作者ＩＤ$_2$）は編集可の場合に限り、その状態を編集不可に変更することができる。これにより本実施形態の著作権保護システム１０では、編集不可の部分コンテンツを編集可とする不正な編集は行えない。

【０１３５】

各部分コンテンツの状態の設定として変更可かつ削除可をその順に従って状態（１１）とし、変更不可かつ削除不可を状態（００）とすれば、各部分コンテンツの状態を（１１）～（００）の４状態で表せる。この場合、状態は図１３に示す推移が可能である。図１３において「部」は実データと空データを含む部分コンテンツ、「実」は実データ、「空」は空データを示し、各状態を設定できる部分コンテンツを示す。

【０１３６】

また、基本的には同じ状態の推移、または１を０にする状態推移は可能であるが、編集不可の場合、編集制御署名が公開されないことから０を１にする状態推移はできない。すなわち、部分コンテンツの編集に関する条件は、部分コンテンツの状態が（００）以外の状態の場合で、図１３に示した矢印の方向への編集に限られる。

【０１３７】

上述の編集制御を行うことにより、本実施形態の著作権保護システム１０では、従来技術の編集制御では実現できなかった以下の制御を実現することができる。

【０１３８】

本実施形態の著作権保護システム１０では、部分コンテンツの追加・削除・変更を繰り返してもコンテンツの構成が変化しないため、変更不可かつ削除可や、変更可かつ削除不可等の制御状態を設定することができる。すなわち、本実施形態の著作権保護システム１０では、追加は追加制御署名によって制御されず、予め設定した空データを実データに変更する変更制御署名$\sigma_k$によって制御される。

【０１３９】

また本実施形態の著作権保護システム１０では、削除は実際に部分データを削除するのではなく実データから空データへの変更によって制御するが、削除制御署名$\tau_k$を用いて変更制御署名$\sigma_k$と別に制御することから削除可と変更可が同義（削除可＝変更可）ではない個別の設定が可能であり、コンテンツの構成が変化しない。

【０１４０】

次に、流用制御について説明する。

【０１４１】

部分コンテンツの流用制御とは、あるコンテンツを構成する部分コンテンツに対する、他のコンテンツにおける使用の可否に関する制御を指す。よって、流用に関しても電子署

名を導入し、以下のように制御する。

【０１４２】

流用制御署名χとは流用用定数と部分コンテンツ及び検証に必要なパラメータのハッシュ値に対して行った署名である。流用の可否については流用可否情報によって示す。流用可の場合、流用制御署名$\chi_k$は公開され、流用不可の場合、非公開としてもよい。流用集約署名χは流用制御署名$\chi_k$をＢＬＳ署名に従って集約したものである。

【０１４３】

基本的に一つのコンテンツを構成する部分コンテンツのコンテンツＩＤは統一する。すなわち、各種編集制御署名にはコンテンツＩＤを設定する部分があり、一つのコンテンツでは同じコンテンツＩＤを用いて署名用ハッシュ値が作成される。よって、あるコンテンツに別のコンテンツからの部分コンテンツを流用するとコンテンツＩＤが整合せず、流用であることが検出できる。

【０１４４】

ただし、流用可とする部分コンテンツのコンテンツＩＤはオール０等の特定の値（特定値）が定まっているとする（以降、これを無設定という）。図１２に示した例では、部分コンテンツ$I_{113}$と$I_{114}$は流用可の部分コンテンツであるので、その流用制御署名$\chi_k$はコンテンツＩＤを$IC_{00}$とした特定値で計算する。これにより、コンテンツの各部分コンテンツが複数のコンテンツからの流用であっても、流用されて来た部分コンテンツは流用可の設定がされているためそのコンテンツＩＤは特定値$IC_{00}$とみなされる。そのため、そのコンテンツ本来のコンテンツＩＤを識別することができる。なお、当該無設定は、他の制御署名に対しても設定してもよい。

【０１４５】

また、部分コンテンツの流用可否はその部分コンテンツの著作者のみが設定でき、部分コンテンツを流用する著作者はその流用可否に何の権限も持たない。よって、流用制御署名$\chi_k$の検証は常に著作者$ID_1$の鍵によってのみ行われる。

【０１４６】

また、流用した部分コンテンツの編集に関する状態は、図１３に示したように、状態の維持または、１を０とする状態変更が可能である。ただし、コンテンツＡに対して異なる著作者が新たな部分コンテンツを追加・変更する場合、流用可でなければコンテンツＡのコンテンツＩＤを設定して流用制御署名$\chi_k$を生成する。

【０１４７】

また、検証側ではまず流用可とされた（コンテンツＩＤが特定値の）部分コンテンツ及び流用集約署名χを著作者$ID_1$の検証鍵で検証し、それが合えば次に編集制御に関する検証を上述したように行う。

【０１４８】

以上より、流用不可設定の部分コンテンツが１つでも存在すると、変更または追加する部分コンテンツはコンテンツＩＤを同じにするか無設定にしなければ、不正編集とみなされる。

【０１４９】

よって、流用不可設定の部分コンテンツが１つでも存在する場合は、異なるコンテンツＩＤをもつコンテンツを作成することができない。すなわち、全てのコンテンツは編集が行われてもそのコンテンツＩＤを識別することができる。コンテンツＩＤがそのコンテンツの著者に関する情報を含む（例えば、コンテンツＩＤの前半が著作者ＩＤで後半が作品番号等）場合、コンテンツ単位で設定される開始位置署名や最終位置署名を検査する検証鍵が特定される。

【０１５０】

次に、コンテンツ間の合成制御について説明する。

【０１５１】

コンテンツの合成とは２つのコンテンツを定めた順序に並べて１つのコンテンツにする処理である。合成処理によって生成されるコンテンツを合成コンテンツと呼ぶ。合成コン

テンツは合成コンテンツの構成等を示す構造データ（合成コンテンツに対する制御データであり、コンテンツの並び順等を示す）と、コンテンツ群とからなる。構造データと異なる合成等を行うと検出されるが、コンテンツの著作者による署名が施されていてもよい。

【０１５２】

本実施形態の著作権保護システム１０では、１つの各部分コンテンツはコンテンツ合成を制御する以下の合成制御署名$\delta_k$を持つ。

【０１５３】

ここでは分かり易くするため、映像コンテンツのような時系列的なコンテンツの合成を例として、前合成制御署名$\delta_{kf}$と後合成制御署名$\delta_{kb}$を設定して説明する。なお、映像コンテンツに字幕コンテンツ等を加える場合では、コンテンツの前後ではなく時系列的に同時と考えられるため上下方向の合成といえるが、この場合、上合成制御署名及び下合成制御署名を加えればよく種々の合成に対応することができる。また、合成制御署名$\delta_k$を集約した合成集約署名$\delta$をＢＬＳ署名に従って生成し公開する。前合成制御署名$\delta_{kf}$と後合成制御署名$\delta_{kb}$も編集制御署名の一種であるが、以降では分かりやすくするため区別して合成制御署名と呼ぶ。

【０１５４】

前(後)合成制御署名$\delta_{kf(b)}$とは、時系列的に前(後)方にあるコンテンツ（以降、前コンテンツまたは後コンテンツと呼ぶ）との合成を制御するもので、前（後）合成用定数と部分コンテンツ及び検証に必要なパラメータのハッシュ値に対して行われた署名である。合成可の場合、合成制御署名$\delta_k$は公開され、合成不可の場合、合成制御署名$\delta_k$は公開されない。

【０１５５】

すなわち、コンテンツの生成時にそのコンテンツを合成不可とする場合、各部分コンテンツに対する合成制御署名と合成集約署名を作成後、合成制御署名を非公開にする。その場合、合成制御署名が公開されていない（以降、合成不可設定と呼ぶ）部分コンテンツを含むコンテンツを合成しようとしても、その部分コンテンツの著作者$ID_1$による合成制御署名がなければ合成できない。ただし、その部分コンテンツが変更可・削除可であれば合成不可が設定された部分コンテンツを全て変更・削除すれば合成可となるが、それは別のコンテンツを作ったことと等価であり、合成不可が設定された部分コンテンツを含むコンテンツの合成はできない。ただし、コンテンツが合成不可設定であってもその一部の部分コンテンツを流用可とする場合、その部分コンテンツは流用制御署名とともに合成制御署名も公開する。この場合、その部分コンテンツのみを残せば合成できるが、これはその部分コンテンツを流用したことと等価になる。また、合成制御署名は編集制御署名と独立に設定されるため、合成不可でも編集可であれば編集可能である。

【０１５６】

次に、合成可設定（全部分コンテンツの合成制御署名が全て公開された）されたコンテンツＡの後にコンテンツＢを合成してその関係を固定する場合は、以下のようになる。まず、著作者$ID_A$によるコンテンツＡと著作者$ID_B$によるコンテンツＢの部分コンテンツを著作者$ID_C$が少なくとも１つ編集してコンテンツＡ’とコンテンツＢ’を作る。コンテンツＡ’にはコンテンツＢ’の各部分コンテンツに対して後合成集約署名（未編集の部分コンテンツの著作者$ID_A$による合成制御署名と、編集した部分コンテンツの著作者$ID_C$による合成制御署名からなる）を生成し、コンテンツＢ’にはコンテンツＡ’の各部分コンテンツと著作者$ID_C$の部分コンテンツに対して前合成集約署名を生成し、編集した部分コンテンツの合成制御署名を非公開とする。この場合、コンテンツＤをコンテンツＡ’とＢ’の間に合成しようとしても、コンテンツＡ’の全合成制御署名（編集された部分コンテンツの制御署名）が揃わないためコンテンツＤは正当な前合成制御署名を生成できない（コンテンツＡ’内の編集された部分コンテンツが変更・削除可であれば、それを変更・削除すれば合成可となるが、これば元々のコンテンツＡを使った合成と等価であるので、著作者の意図に反しない）。コンテンツＤの後合成制御署名も同様である。

【０１５７】

合成後に合成不可とする場合は、前述のように部分コンテンツの編集を伴う必要がある。なぜならば、合成可のコンテンツを何も変えずに合成不可とするために公開されている各部分コンテンツの合成制御署名を非公開としても、元のコンテンツは合成可であるため、元の合成制御署名を再利用すれば合成不可としたコンテンツが合成可となるためである。また、部分コンテンツを編集する場合、合成の設定は同じでも、部分コンテンツの内容が異なるため合成制御署名$\delta_k$及び合成集約署名$\delta$を毎回更新する必要がある。

【０１５８】

さらに、「合成可のコンテンツを合成後に、合成不可とする制御には部分コンテンツの編集を伴う必要がある」としているが、各コンテンツに空データがあれば、それを合成不可・削除不可・変更不可に変更すれば、見かけ上のコンテンツは何も編集されていなくても合成後に合成不可とすることが可能である。ただし、その空データを置き換えて合成可にすると、検証において合成に対する不正編集ではなく、部分コンテンツに対する不正編集として検出される。

【０１５９】

また、合成不可とした著作者は合成制御署名$\delta_k$を持たない部分コンテンツの著作者であるため、著作者$ID_2$はなくてもよい。基本的に１つのコンテンツに対して合成不可制御は１度しか行わないため、合成制御署名$\delta_k$を持たない部分コンテンツの著作者は特定される。複数の部分コンテンツが合成制御署名$\delta_k$を持たない場合、それが同一著作者でなければ不正コンテンツとされる。

【０１６０】

また、合成可のコンテンツを合成不可とせずに合成を行うだけであれば、構造データを変更するだけでよい。検証側では各コンテンツが構造データに記述されている側の合成が可であることを確認し、正しければ合成コンテンツと認める。

【０１６１】

次に、使用制御について説明する。本実施形態の著作権保護システム１０では、コンテンツの使用を制御するための使用制御署名λをコンテンツに紐付ける。使用制御署名λとは、使用用定数と使用条件と検証に必要なパラメータのハッシュ値に対して行った署名である。この署名は集約されずに公開される。必ず著作者$ID_1$の鍵で検証されるので、１つのコンテンツに対して使用条件を設定できるのは著作者$ID_1$のみであり、使用条件と整合しない場合は全て使用不可となる。

【０１６２】

使用条件は使用の可否などの他により細かな使用状況も設定できる。例えば、署名検証が整合していればその使用条件は正当であるため、そこに記述されている条件（使用者や使用環境の設定等）に使用者が整合しているかを検査し、整合していれば使用を許可する。

【０１６３】

例えば、使用条件が使用不可であれば再生機器または編集機器はそのコンテンツの再生または編集を行わない。他のコンテンツと無理に合成しても、コンテンツ単位で使用制御を検証するため、正当な再生機器・編集機器はそのコンテンツを使用しない。また、使用条件として正当な証明書をもつ再生機器であることが条件の場合、正当な再生機器または編集機器は証明書が入力されなければ、そのコンテンツを使用しない。また、使用制御署名λがない場合も使用不可となる。

【０１６４】

以上の編集制御を行う本実施形態の著作権保護システム１０における、権利継承技術すなわち、コンテンツ間の関係の記述について説明する。

【０１６５】

コンテンツの合成によって各コンテンツの著作者間に関係が生じるが、合成可の場合は合成制御署名$\delta_k$が公開されている。そのため、本実施形態の著作権保護システム１０では、合成制御署名$\delta_k$を用いて従来技術と同様に権利継承署名ζを構成すれば、コンテンツ合成に関する編集制御と権利継承とを同時に実現することができる。

【０１６６】
従来の権利継承署名技術では、公開された合成制御署名$\delta_k$を用いるという制限を設けておらず、権利継承専用の署名をコンテンツ毎に作成して構成していた。よって、合成を変更するときは新たなコンテンツに対する権利継承専用の署名を生成して構成しなおす、すなわち署名全体を作り直す必要があった。
【０１６７】
一方、本実施形態の著作権保護システム１０では、編集制御署名（合成制御署名$\delta_k$）を利用することにより、合成制御署名$\delta_k$が公開されていれば変更が可能であるため署名の抜き差しによって権利継承署名$\zeta$を容易に再構成することができる。
【０１６８】
例えば、図９の例で$ID_{21}$が$A_{11}$～$A_{14}$を合成後、例えば$A_{13}$を$A_{17}$に変える場合、$A_{12}$～$A_{14}$が合成可の設定であれば１から署名を構成しなくても、$A_{13}$の合成制御署名$\delta_{13}$を$A_{17}$の合成制御署名$\delta_{17}$に差し替えることによって更新ができる。ただし、図９において$A_{22}$を$A_{21}$（の$A_{14}$）の後に合成しているが、$A_{12}$と$A_{13}$の間に$A_{22}$を合成してもコンテンツの権利関係は同じ（図９の例では$ID_{31}$が$A_{21}$と$A_{22}$を用いているという関係は同じ）であるため、権利継承署名$\zeta$に関しては同じものになる。
【０１６９】
以上の編集制御施術及び権利継承技術を行う本実施形態の著作権保護システム１０の具体的なアルゴリズムを以下に説明する。なお、以下の３つの前提条件を付ける。
【０１７０】
前提条件１として、公開鍵基盤（ＰＫＩ：Public Key Infrastructure）は整備されており、認証局（ＣＡ：Certification Authority)により全ての署名者とその検証鍵の紐付けは保証されるとする。
【０１７１】
前提条件２として、各署名者に発行されている鍵ペア以外に、新たな鍵ペアの発行は行われないとする。
【０１７２】
前提条件３として、アグリゲート署名作成中において、署名者間の通信は安全に行われ、作成中の中間情報を第三者が入手することは不可能であるとする。
【０１７３】
なお、以下の例では記述を簡単にするために各種パラメータを統一的に用いているが、以下に限定される必要はなく、必要最小限のパラメータのみを用いて構成しても良い。
【０１７４】
まず鍵を生成する。$g \in G_1$を生成元とする。ｉ次でｊ番目に位置する署名者を$ID_{ij}$として、$ID_{ij}$は署名鍵$s_{ij} \in Z_p^*$（全ての署名者の署名鍵（秘密鍵）は各々異なるものとする）を持つ。それに対する検証鍵$v_{ij} = s_{ij} g$を公開する。
【０１７５】
本実施形態の著作権保護システム１０の端末装置１２では、著作者がコンテンツを制作して部分コンテンツに分割する、または、部分コンテンツを制作してコンテンツを構成した後、著作者の指示に応じて、図１４に示した著作権保護処理を実行する。著作権保護処理は、端末装置１２のＲＯＭ２３に記憶されている著作権保護プログラムをＣＰＵ２２が実行することにより行われる。
【０１７６】
ステップＳ１４００で端末装置１２の制御部２０は、部分コンテンツを管理局１４へ提出する。本実施形態の、著作権保護システム１０では、制作したコンテンツを公開する前に、管理局署名を得るために部分コンテンツを管理局１４へ提出する。なお、部分コンテンツに対する管理局署名を得るために管理局１４へ部分コンテンツを提出する方法は特に限定されない。部分コンテンツ毎に、管理局１４へ送信してもよいし、当該部分コンテンツを含むコンテンツ全体を管理局１４へ送信してもよい。また、部分コンテンツを管理局

１４へ提出するタイミングも、特に限定されるものではなく、当該部分コンテンツを含むコンテンツの公開前であればよい。例えば、電子署名（各種編集署名）を作成した後であってもよい。

【０１７７】

端末装置１２が提出した部分コンテンツ（コンテンツ）を受信した管理局１４は、図１５に示した管理処理を実行する。管理処理は、管理局１４のＲＯＭ２３に記憶されている管理プログラムをＣＰＵ２２が実行することにより行われる。

【０１７８】

ステップＳ１５００で管理局１４の制御部２０は、部分コンテンツのオリジナル性を検査する。上述したように検査方法は特に限定されず、例えば、画像検索により類似画像の有無を検出してもよい。

【０１７９】

次のステップＳ１５０２で管理局１４の制御部２０は、部分コンテンツがオリジナル性を有しているか否かを判定する。オリジナル性の有無の判定方法は特に限定されないが、例えば、上記の場合では、類似画像が検出されなかった場合にオリジナル性を有していると判定する。オリジナル性を有していない場合、否定判定となりステップＳ１５０４へ移行する。

【０１８０】

ステップＳ１５０４で管理局１４の制御部２０は、オリジナル性を有していないことを端末装置１２に出力した後、本管理処理を終了する。なお、オリジナル性を有していない場合の処理は特に限定されるものではなく、例えば、管理局署名を発行しない旨を端末装置１２に通知してもよい。また、オリジナル性を有していない場合は、そのまま本管理処理を終了してもよい。

【０１８１】

一方、部分コンテンツがオリジナル性を有している場合、肯定判定となりステップＳ１５０６へ移行する。ステップＳ１５０６で管理局１４の制御部２０は、上述したように管理局署名μを生成する。なお、上述したように、管理局署名μは、少なくとも実データである部分コンテンツ毎に生成される。

【０１８２】

次のステップＳ１５０８で管理局１４の制御部２０は、生成した管理局署名μを端末装置１２に出力した後、本管理処理を終了する。

【０１８３】

一方、端末装置１２では、上述したようにステップＳ１４００で部分コンテンツを管理局へ提出した後、ステップＳ１４０２へ移行する。

【０１８４】

ステップＳ１４０２で端末装置１２の制御部２０は、管理局署名μを取得したか否かを判定する。上述したように、部分コンテンツがオリジナル性を有していないと管理局署名μが取得できない。コンテンツに含まれる実データの部分コンテンツのうち、管理局署名μが取得できない部分コンテンツが一つでもあった場合、否定判定となり本著作権保護処理を終了する。一方、全ての部分コンテンツについて管理局署名μを取得した場合、肯定判定となりステップＳ１４０４へ移行する。

【０１８５】

ステップＳ１４０４で端末装置１２の制御部２０は、図１６に示した電子署名作成処理を実行する。なお、ここでは、電子署名作成処理の説明に当たり簡略化のため合成を１つの署名（合成制御署名$\delta_k$）で制御するが、前合成や後合成または上合成や下合成等、種々の合成を実現する場合、合成制御署名$\delta_k$の種類を増やせばよい。

【０１８６】

ステップＳ１６００で制御部２０は、コンテンツＩＤ及び部分コンテンツＩＤを作成する。著作者$ID_{ij}$が制作したコンテンツ$A_{ij}$のコンテンツＩＤを$IC_{ij}$とし、$A_{ij}$の$m_{ij}$個の部分コンテンツ$A_{ijk}$（$k=1$、…、$m_{ij}$）に対する部分コンテンツ

ＩＤを$I_{ijk}$とする。なお、$ID_{ij}$は各著作者が本来もつＩＤとすることができる。そのＩＤを著作者の位置に応じて$ID_{ij}$として扱ってもよい。なお、コンテンツＩＤは重複を避けるためにコンテンツ毎に全て異なり、著作者を特定できるものとする（例えば、$IC_{ij}$の前半部分が$ID_{ij}$と等しい等）。

【０１８７】

次のステップＳ１６０２で制御部２０は、開始データ及び最終データを作成する。制御データの内容をｄとして、開始データ$A_{ij0}{}^{*}$と最終データ$A_{ijm+1}{}^{*}$を下記（１３）式を用いて作成する。さらに、開始データ$A_{ij0}{}^{*}$と最終データ$A_{ijm+1}{}^{*}$に対する開始位置署名$\alpha_{ij}$と最終位置署名$\beta_{ij}$、及び使用制御署名$\lambda_{ij}$を下記（１４）式を用いて作成する。ただし、ｒは処理に応じて定められる定数であり、変更の場合はｒｃ、削除の場合はｒｄ、合成の場合はｒｓ、流用の場合はｒｔ、及び使用の場合はｒｕとする。よって、変更・削除・流用・合成に対して$\alpha_{ij}$と$\beta_{ij}$とは異なる。使用制御署名λにおけるａｗは使用条件を表す。

【０１８８】

【数１１】

$$A_{ij0}{}^{*} = IC_{ij} \| I_{ij0} \| d, \quad A_{ijm+1}{}^{*} = IC_{ij} \| I_{ijm+1} \| d \qquad \cdots(13)$$

【０１８９】

【数１２】

$$\alpha_{ij} = s_{ij} H\left(IC_{ij} \| I_{ij0} \| H\left(A_{ij0}{}^{*}\right) \| r\right)$$
$$\beta_{ij} = s_{ij} H\left(IC_{ij} \| I_{ijm+1} \| H\left(A_{ijm+1}{}^{*}\right) \| r\right)$$
$$\lambda_{ij} = s_{ij} H\left(IC_{ij} \| aw \| ru\right) \qquad \cdots(14)$$

次のステップＳ１６０４で制御部２０は、各部分コンテンツの状態及び流用の可否を決定する。各部分コンテンツに状態（００）～（１１）及び流用の可否を決定する。なお、本電子署名作成処理において編集の可否の決定方法は特に限定されず、著作者の指示に応じて可否を決定すればよい。

【０１９０】

なお、各部分コンテンツの状態は、空データの状態は（００）か（１１）のみとする。また、署名回数は０とする。以降、部分コンテンツＩＤは署名回数を連接したものとする。

【０１９１】

次のステップＳ１６０６で制御部２０は各部分コンテンツが流用可であるか否かを判定する。流用不可である場合、否定判定となりステップＳ１６１０へ移行する。一方、流用可である場合、肯定判定となりステップＳ１６０８へ移行する。

【０１９２】

ステップＳ１６０８で制御部２０は、上記ステップＳ１６００で作成したコンテンツＩＤを特定値（ここでは０）に変更する。

【０１９３】

次のステップＳ１６１０で制御部２０は、コンテンツの合成の可否を決定する。

【０１９４】

次のステップＳ１６１２で制御部２０は、部分コンテンツに対する署名用データを作成する。具体的には、部分コンテンツ$A_{ijk}$（追加用空データｄも含む）に対する署名用データ$A_{ijk}{}^{*}$を下記（１５）式を用いて作成する。ただし、$A_{ijk}$の流用を許可する場合、$IC_{ij}=0$とする。

【０１９５】
【数１３】

$$A_{ijk}{}^{*} = IC_{ij} \| I_{ijk} \| A_{ijk} \qquad \cdots(15)$$

次のステップＳ１６１４で制御部２０は、部分コンテンツ毎に変更、削除、流用、及び合成の各々に対してハッシュ値ｈ$_{k}$を生成する。具体的には、制御部２０は、上記ステップで設定した状態に応じて定数ｒを使い分けて、下記（１６）式を用いて、変更、削除、流用、及び合成に対して各々ハッシュ値ｈ$_{k}$を生成する。ただし、ｒは変更ではｒｃ、削除ではｒｄ、流用ではｒｔ、及び合成ではｒｓとなる。
【０１９６】
【数１４】

$$h_{ijk} = H\left(IC_{ij} \| I_{ijk} \| H\left(A_{ijk}{}^{*}\right) \| r\right) \qquad \cdots(16)$$

上記（１６）式により得られるハッシュ値ｈ$_{ijk}$は処理毎に異なる値となる。
【０１９７】
次のステップＳ１６１６で制御部２０は、部分コンテンツ毎に変更制御署名σ$_{ijk}$、削除制御署名τ$_{ijk}$、流用制御署名χ$_{ijk}$、及び合成制御署名δ$_{ijk}$の各々を生成する。具体的には、下記（１７）式を用いて変更制御署名σ$_{ijk}$を生成する。また、下記（１８）式を用いて削除制御署名τ$_{ijk}$を生成する。また、下記（１９）式を用いて流用制御署名χ$_{ijk}$を生成する。また、下記（２０）式を用いて合成制御署名δ$_{ijk}$を生成する。
【０１９８】
【数１５】

$$\text{変更制御署名}: \sigma_{ijk} = s_{ij} h_{jjk} \qquad \cdots(17)$$

$$\text{削除制御署名}: \tau_{ijk} = s_{ij} h_{jjk} \qquad \cdots(18)$$

$$\text{流用制御署名}: \chi_{ijk} = s_{ij} h_{jjk} \qquad \cdots(19)$$

$$\text{合成制御署名}: \delta_{ijk} = s_{ij} h_{jjk} \qquad \cdots(20)$$

次のステップＳ１６１８で制御部２０は、各編集制御毎に集約署名を作成する。具体的には、下記（２１）式を用いて変更集約署名σ$_{ij}$を生成する。また、下記（２２）式を用いて削除制御署名τ$_{ij}$を生成する。また、下記（２３）式を用いて流用制御署名χ$_{ij}$を生成する。また、下記（２４）式を用いて合成制御署名δ$_{ij}$を生成する。ただし下記（２１）式～（２４）式においてα$_{ij}$及びβ$_{ij}$は編集処理毎に異なる値である。
【０１９９】
【数１６】

$$\text{変更集約署名}: \sigma_{ij} = \alpha_{ij} + \sum_{k} \sigma_{ijk} + \beta_{ij} \qquad \cdots(21)$$

$$\text{削除集約署名}: \tau_{ij} = \alpha_{ij} + \sum_{k} \tau_{ijk} + \beta_{ij} \qquad \cdots(22)$$

$$\text{流用集約署名}: \chi_{ij} = \alpha_{ij} + \sum_{k} \chi_{ijk} + \beta_{ij} \qquad \cdots(23)$$

$$\text{合成集約署名}: \delta_{ij} = \alpha_{ij} + \sum_{k} \delta_{ijk} + \beta_{ij} \qquad \cdots(24)$$

次のステップＳ１６２０で制御部２０は、各部分コンテンツに応じて、上記ステップで使用した各パラメータを例えば図１１のように部分コンテンツに紐付けた後、本電子署名作成処理を終了して、著作権保護処理のステップＳ１４０６（図１４参照）へ移行する。

【０２００】

なお、開始データまたは最終データの場合は、使用条件、使用制御署名λ、各集約署名（$\sigma_{ij}$、$\tau_{ij}$、$\chi_{ij}$及び$\delta_{ij}$）等のコンテンツ単位の署名検証に必要なパラメータを紐付ける。ここではコンテンツの合成はまだ行われないので権利継承署名は生成しないが、合成コンテンツを初めから生成する場合は、複数のコンテンツを上記のように独立に生成し、後述の合成処理を行った後、権利継承署名をつけることもできる。

【０２０１】

ステップＳ１４０６で端末装置１２の制御部２０は、紐付けられた電子署名とともに制作したコンテンツを出力（公開）した後、本著作権保護処理を終了する。

【０２０２】

次に、このようにして著作者により制作されたコンテンツに対して、行われる編集処理について説明する。

【０２０３】

本実施形態の著作権保護システム１０では、公開されたコンテンツを取得し、当該コンテンツに対して編集を行う場合に、図１７に示した編集処理を実行する。編集処理は、端末装置１２のＲＯＭ２３に記憶されている編集プログラムをＣＰＵ２２が実行することにより行われる。

【０２０４】

なお、編集処理のステップＳ１７００、Ｓ１７０２、及びＳ１７０６の各処理は、上述した著作権保護処理（図１４参照）のステップＳ１４００、Ｓ１４０２、及びＳ１４０６の各処理にそれぞれ対応しており、著作権保護処理のステップＳ１４０４に代わりステップＳ１７０５Ａ～Ｓ１７０５Ｆの処理を実行する他は同様の処理であるため、ここでは、ステップＳ１７０５Ａ～Ｓ１７０５Ｆの処理についてのみ説明する。なお、新しい部分コンテンツを生成せず、部分コンテンツの削除及びコンテンツの合成のみを行う場合は、ステップＳ１７００及びＳ１７０２の処理は省略することができる。

【０２０５】

編集を行う場合、端末装置１２の制御部２０は、まずＳ１７０５Ａで図１８に示す検証処理（詳細後述）を行い、そのコンテンツが正しく構成されていない場合は、否定判定となり本編集処理を終了する。一方、そのコンテンツが正しく構成されている場合、肯定判定となり、ステップＳ１７０５Ｂへ移行し、ステップＳ１７０５Ｂで図１９に示した編集制御処理（詳細後述）を実行する。編集制御処理が終了すると、さらに次のステップＳ１７０５Ｃでコンテンツに対する合成・権利継承処理を行うかを判定し、行わない場合、否定判定となりステップＳ１７０６へ移行する。一方、合成・権利継承処理を行う場合、肯定判定となりステップＳ１７０５Ｄへ移行し、ステップＳ１７０５Ｄで図２０に示した合成・権利継承処理（詳細後述）を行う。ステップＳ１７０５Ｅで端末装置１２の制御部２０は、処理を継続するか否かを判定し、処理を継続しない場合は、ステップＳ１７０６へ移行する。一方処理を継続する場合は肯定判定となりステップＳ１７０５Ｆへ移行する。ステップＳ１７０５Ｆで端末装置１２の制御部２０は、編集制御処理を行うか否か判定し、編集処理を行う場合、肯定判定となりステップＳ１７０５Ｂに戻り、編集制御処理を繰り返す。一方、編集処理を行わない場合、すなわち合成・権利継承処理を行う場合、否定判定となりステップＳ１７０５Ｄに戻り、合成・権利継承処理を繰り返す。　なお、ステップＳ１７０５Ｂの編集制御処理とステップＳ１７０５Ｄの合成・権利継承処理は、順不同で連続して行うことが可能である。また、端末装置１２が編集専用装置の場合、Ｓ１７０５Ａの処理は省略される。

【０２０６】

ステップＳ１７０５Ｂの編集制御処理（図１９参照）について説明する。ここでは、著作者$ID_{ij}$が作成したコンテンツ$A_{ij}$の部分コンテンツ$A_{ijk}$（空データを含む）

を著作者ＩＤ$_{ab}$が作成した部分データＡ$_{abk}$（空データを含む）に変更する場合を考える。ただし、編集処理はステップＳ１７０５Ａで管理局署名及び、使用条件、コンテンツＩＤ、流用判定、編集判定、合成判定、権利継承判定などが正当である場合に行われるので、上記判定は正当であるという前提のもと行われる。

【０２０７】

まず、ステップＳ１９００で部分コンテンツを流用するかどうかを判定する。流用する場合、肯定判定となりステップＳ１９０２へ移行し、その部分コンテンツをコピーして他のコンテンツの編集処理に移動する。一方、流用しない場合、否定判定となりステップＳ１９０４へ移行する。流用するかどうかの決定方法は特に限定されず、著作者の指示に応じて可否を決定すればよい。

【０２０８】

次に、ステップＳ１９０４で制御部２０は、部分コンテンツＡ$_{ijk}$に対して対象とする編集（変更、削除、追加）が可能であるか否かを判定する。すなわち、対象とする編集に関する編集制御署名が公開されており、制御署名及び集約署名の検証が成功した場合に、編集が可能であると判定する。編集が可能ではない場合、否定判定となり本編集制御処理を終了する。

【０２０９】

次に、ステップＳ１９０６で制御部２０は、部分コンテンツＡ$_{ijk}$に対して変更を行う場合、実データＡ$_{abk}$を準備し、Ａ$_{ijk}$を削除する場合空データｄを準備し、追加を行う場合、空データｄに対して追加する実データＡ$_{abk}$を準備する。

【０２１０】

次のステップＳ１９０８で制御部２０は、差し替える部分コンテンツＡ’$_{abk}$の変更、削除、追加、流用（合成に関しては後述の合成処理で定めた状態に従う）に関する状態を決定する。なお、空データの状態は（００）か（１１）のみとし、流用してきた部分コンテンツの場合、前の状態を超えない（編集不可を編集可としない）状態に決定する。

【０２１１】

次のステップＳ１９１０で制御部２０は、差し替えた部分コンテンツに対する署名用データＡ’$_{abk}$*及び署名用ハッシュ値ｈ’$_{abk}$を生成する。具体的には、制御部２０は、処理に応じて定数ｒを使い分けて下記（２５）式により、署名用データＡ’$_{abk}$*及び署名用ハッシュ値ｈ’$_{abk}$を生成する。

ただし、ｒは処理に応じて定まる定数であり、変更の場合はｒｃ、削除の場合はｒｄ、流用の場合ｒｔ、及合成の場合はｒｓとする。また、ＩＣ$_{ij}$は流用を認めない場合は変更しない。一方、流用を認める場合、ＩＣ$_{ij}$＝０とする。Ｉ$_{ijk}$は部分コンテンツの識別番号であれば変更され、コンテンツ中の位置情報であれば変更しない。

【０２１２】

【数１７】

$$A'_{abk}{}^{*} = IC_{ij} \| I_{ijk} \| A'_{abk}, \quad h'_{abk} = H\left(IC_{ij} \| I_{ijk} \| H(A_{abk}{}^{*}) \| r\right) \quad \cdots(25)$$

上記（２５）式により得られるハッシュ値ｈ’$_{abk}$は処理毎に異なる値となる。

【０２１３】

次のステップＳ１９１２で制御部２０は、差し替えた部分コンテンツの変更制御署名σ’$_{abk}$、削除制御署名τ’$_{abk}$、流用制御署名χ’$_{abk}$、及び合成制御署名δ’$_{abk}$の各々を生成する。具体的には、下記（２６）式を用いて変更制御署名σ’$_{abk}$を生成する。また、下記（２７）式を用いて削除制御署名τ’$_{abk}$を生成する。また、下記（２８）式を用いて流用制御署名χ’$_{abk}$を生成する。また、下記（２９）式を用いて合成制御署名δ’$_{abk}$を生成する。なお、流用してきた部分コンテンツである場合は、流用制御署名χ’$_{abk}$は前のものを用いる。

【０２１４】

【数１８】

$$\text{変更制御署名}:\sigma'_{abk} = s_{ab}h'_{abk} \quad \cdots(26)$$
$$\text{削除制御署名}:\tau'_{abk} = s_{ab}h'_{abk} \quad \cdots(27)$$
$$\text{流用制御署名}:\chi'_{abk} = s_{ab}h'_{abk} \quad \cdots(28)$$
$$\text{合成制御署名}:\delta'_{abk} = s_{ab}h'_{abk} \quad \cdots(29)$$

次のステップＳ１９１４で制御部２０は、各編集制御毎に集約署名を作成する。具体的には、下記（３０）式を用いて変更集約署名σ$_{ij}$を生成する。また、下記（３１）式を用いて削除集約署名τ$_{ij}$を生成する。また、下記（３２）式を用いて流用集約署名χ$_{ij}$を生成する。また、下記（３３）式を用いて合成集約署名δ$_{ij}$を生成する。

【０２１５】

【数１９】

$$\text{変更集約署名}:\sigma'_{ij} = \sigma_{ij} - \sigma_{jjk} + \sigma'_{abk} \quad \cdots(30)$$
$$\text{削除集約署名}:\tau'_{ij} = \tau_{ij} - \tau_{jjk} + \tau'_{abk} \quad \cdots(31)$$
$$\text{流用集約署名}:\chi'_{ij} = \chi_{ij} - \chi_{jjk} + \chi'_{abk} \quad \cdots(32)$$
$$\text{合成集約署名}:\delta'_{ij} = \delta_{ij} - \delta_{jjk} + \delta'_{abk} \quad \cdots(33)$$

次のステップＳ１９１６で制御部２０は、差し替えた部分コンテンツに、上記パラメータを紐付けた後、本編集制御処理を終了する。具体的には、差し替えた部分コンテンツの編集を許可する場合、編集の種類に応じた編集制御署名を紐付ける。一方、編集不可の場合署名用ハッシュ値と不可とした著作者ＩＤ$_2$を紐付ける。ただし、合成制御署名δ’$_{abk}$には著作者ＩＤ$_2$は不要である。また、各種制御署名検証に必要なパラメータを部分コンテンツに紐付ける。

【０２１６】

次に、図１７におけるステップＳ１７０５Ｄの合成・権利継承処理（図２０参照）について説明する。ここでは、ｉ＋１次著作者ＩＤ$_{i+1\,j}$がｉ次コンテンツを用いて新しいコンテンツを作る場合の合成処理を例に説明する。なお、合成を行ったコンテンツの順序等は構造データに記述される。

【０２１７】

ステップＳ２０００で制御部２０は、合成が可能であるか否かを判定する。具体的には、著作者ＩＤ$_{i+1\,j}$がコンテンツＡ$_{ia}$とＡ$_{ib}$とを合成したい場合、Ａ$_{ia}$及びＡ$_{ib}$の全部分コンテンツの合成制御署名δ$_k$が公開されており、合成集約署名δの検証が成功した場合（合成可能の場合）に、合成が可能であると判定する。合成が可能ではない場合、否定判定となり本合成・権利継承処理を終了する。一方、合成が可能な場合、肯定判定となりステップＳ２００２へ移行する。

【０２１８】

ステップＳ２００２で制御部２０は、合成するコンテンツ（コンテンツＡ$_{ia}$とＡ$_{ib}$）の状態（合成可か不可）を新たに決定する。

【０２１９】

次のステップＳ２００４で制御部２０は、今回合成により得られたコンテンツの関係を固定するか（例えば、コンテンツＡ$_{ia}$とＡ$_{ib}$の間に他のコンテンツの合成を許可する）か否かを判定する。関係を固定しない、すなわち合成を許可する場合、ステップＳ２００８へ移行する。一方、関係を固定して合成を許可しない場合、ステップＳ２００６へ移行する。

【０２２０】

ステップＳ２００６で制御部２０は、コンテンツＡ$_{ia}$とＡ$_{ib}$の中の部分コンテンツ

$A_{iak}$が前記編集処理によって編集済みであれば、その部分コンテンツの合成制御署名$\delta'_{iak}$を用いて下記（３４）式のように合成集約署名$\delta_{ia}$と$\delta_{ib}$を更新する。なお、$A_{iak}$の合成制御署名$\delta'_{iak}$は公開しない。

【０２２１】

【数２０】

$$\delta'_{iaj}=s_{i+1j}H(IC_{ia}\|I_{iaj}\|H(A_{iaj}{}^{*})\|rs)$$
$$\delta'_{ia}=\delta_{ia}-\sum_{k}\delta_{iak}+\sum_{k}\delta_{ibk}+\delta'_{iak}$$
$$\delta'_{ib}=\delta_{ib}-\sum_{k}\delta_{ibk}+\sum_{k}\delta_{iak}-\delta_{iaj}+\delta'_{iak}$$

･･･(34)

次のステップＳ２００８で制御部２０は、権利継承署名ζを生成する。具体的には、著作者$ID_{i+1j}$が下位階層のコンテンツ$A_{i1}$～$A_{im}$を合成した場合、合成コンテンツ$A_{i+1j}$に対して、下記（３５）式を用いて、権利継承署名$\zeta_{i+1j}$を生成して公開する。ここで、$h_{i+1j}$は$A_{i+1j}$に対するハッシュ値、$\zeta_{ik}$（ｋ＝１、・・・、ｍ）は$A_{ik}$に対する権利継承署名$h_{ik}$は$\zeta_{ik}$を生成する場合に用いた署名用ハッシュ値である。ただし、オリジナルコンテンツに関する権利継承署名を、$\zeta_{ik}=\Sigma\delta_{ikj}$（合成可のため公開されている）とする。

【０２２２】

【数２１】

$$\zeta_{i+1j}=s_{i+1j}h_{i+1j}+\sum\zeta_{ij}+s_{i+1j}\sum h_{ij}$$ ･･･(35)

さらに、合成コンテンツ$A_{i+1j}$を構成するコンテンツ$A_{ia}$が合成可であり、それを合成可のコンテンツ$A_{ib}$に変更する場合、下記（３６）式を用いて権利継承署名$\zeta'_{i+1j}$を生成して更新する。なお、コンテンツ$A_{ia}$の削除のみを実行する場合は、コンテンツ$A_{ib}$に関する加算を行わない。また、合成のみを行い権利継承処理を行わない場合、ステップＳ２００８は省略することができる。

【０２２３】

【数２２】

$$\zeta'_{i+1j}=\zeta_{i+1j}-\zeta_{ia}+\zeta_{ib}-s_{i+1j}h_{ia}+s_{i+1j}h_{ib}$$ ･･･(36)

このように、本実施形態の著作権保護システム１０では、従来技術と異なり、従来技術では考慮されていなかった合成コンテンツの制御を実現することができる。

【０２２４】

次のステップＳ２０１０で制御部２０は、コンテンツの合成に合わせて構造データを作成・更新し、権利継承署名$\zeta'_{i+1j}$を付加した後、本合成・権利継承処理を終了する（権利継承処理を行わなかった場合、$\zeta'_{i+1j}$は付加しない）。

【０２２５】

次に、検証装置１６で行われる検証処理について説明する。図１７では端末装置１２に検証装置１６の機能を持たせ、ステップＳ１７０５Ａでこれから述べる検証処理後に編集制御処理に移行するとしたが、ステップＳ１７０５Ｂで行われる編集制御処理及びＳ１７０５Ｄで行われる合成・権利継承処理において全ての処理を対象としない場合（例えば変更のみ行う場合）、対象とする処理に関連する最小限の検証のみ行い他の処理（削除、追

加、流用等）に関する検証は省略してもよい。

【０２２６】

本実施形態の著作権保護システム１０では、検証装置１６（コンテンツの作成や編集処理は行わず、コンテンツの再生のみ行う）が公開されたコンテンツを取得した場合、当該コンテンツを再生等する前に、図１８に示した検証処理を実行する。検証処理は、管理局装置１４のＲＯＭ２３に記憶されている検証プログラムをＣＰＵ２２が実行することにより行われる。

【０２２７】

ステップＳ１８００で検証装置１６の制御部２０は、コンテンツの各部分コンテンツに紐付けられた管理局署名μを上述したように検査し、整合するが否かを判定する。なお、管理局署名μが紐付けられていない場合も、整合しないと判定する。管理局署名μが整合しない部分コンテンツが１つでもある場合は、否定判定となりステップＳ１８２０へ移行する。一方、全ての部分コンテンツの管理局署名μが整合した場合、肯定判定となりステップＳ１８０２へ移行する。

【０２２８】

ステップＳ１８０２で検証装置１６の制御部２０は、検証対象であるコンテンツが合成コンテンツ（合成が行われたコンテンツ）であるか否かを判定する。合成コンテンツではない場合、否定判定となりステップＳ１８０６へ移行する。一方、合成コンテンツの場合、肯定判定となりステップＳ１８０４へ移行する。

【０２２９】

ステップＳ１８０４で検証装置１６の制御部２０は、合成コンテンツを、構造データを用いて各コンテンツに分解する。

【０２３０】

次のステップＳ１８０６で検証装置１６の制御部２０は、コンテンツ毎に、コンテンツを構成する部分コンテンツのコンテンツＩＤが全て一致しているか否かを判定する。なお、部分コンテンツのコンテンツＩＤが無設定の場合は除く。コンテンツＩＤが全て一致しない場合、否定判定となりステップＳ１８２０へ移行する。一方、一致した場合、肯定判定となりステップＳ１８０８へ移行する。なお、ここで構造データとコンテンツの構造とを比較し、一致しない場合、不正合成が行われたと判定してステップＳ１８２０へ移行する。

【０２３１】

ステップＳ１８０８で検証装置１６の制御部２０は、使用条件が正当であるか否かを判定する。具体的には、コンテンツ毎に紐付けられた使用条件ａｗを用いて、上記（１４）式のうち、最下部に示した式を用いてハッシュ値を生成する。さらに、コンテンツＩＤから特定される著作者の検証鍵$\nu_{ij}$を用いて、使用制御署名$\lambda_{ij}$の署名検証を行う。使用制御署名$\lambda_{ij}$は集約署名ではないので通常の署名検証が行われ、整合していれば使用条件が正当であるため、当該コンテンツが使用条件に整合するか否かを検証する。使用条件に整合しない場合、正当ではないため否定判定となりステップＳ１８２０へ移行する。一方、使用条件に整合する場合、正当であるため肯定判定となりステップＳ１８１０へ移行する。

【０２３２】

ステップＳ１８１０で検証装置１６の制御部２０は、コンテンツ毎に、合成集約署名が正当であるか否かを判定する。具体的には、制御部２０は、以下の処理を行う。全ての部分コンテンツの合成制御署名が公開されている場合は合成可であり、合成制御署名が公開されていない部分コンテンツが１つでもある場合は合成不可とし、合成不可と設定している部分コンテンツの著作者を著作者$ＩＤ_{l}$から特定する。その後、上記（１３）式を用いて開始データと最終データとを生成し、処理毎の定数を用いて、上記（１６）式、（２４）式及び（３４）式を用いて各部分コンテンツに対する署名用ハッシュ値$h_{ijk}$を生成する。

【０２３３】

生成された署名用ハッシュ値$h_{ijk}$と開始データまたは最終データに紐付けられた合成集約署名$\delta_{ij}$及びコンテンツＩＤと各部分コンテンツの著作者ＩＤ$_l$から特定される著作者の検証鍵$v_{ij}$を用いて、下記（３７）式が成り立つか否かにより署名の検証を行う。

【０２３４】

【数２３】

$$e(g,\delta_{ij}) = \Pi e(v_{ij},h_{ijk}) \quad \cdots(37)$$

上記（３７）式が成り立たない場合、合成集約署名は不正であるため、ステップＳ１８１０で否定判定となりステップＳ１８２０へ移行する。一方、上記（３７）式が成り立つ場合、合成集約署名は正当であるため、肯定判定となりステップＳ１８１２へ移行する。

【０２３５】

ステップＳ１８１２で検証装置１６の制御部２０は、コンテンツ毎に、権利継承署名$\zeta_{ij}$が正当性であるか否かを判定する。具体的には、制御部２０は、以下の処理を行う。下記（３８）が成り立つか否かにより、構造データに応じて権利継承署名$\zeta_{ij}$が生成されているか否かを検査する。ただし、下記（３８）式の$h_{iijj}$は合成コンテンツに用いられた各階層のコンテンツのハッシュ値であり、$v_{ii+1jj}+v_{iijj}$は$h_{iijj}$に係わる著作者の前後関係を表す検証鍵である。

【０２３６】

【数２４】

$$e(g,\zeta_{ij}) = \Pi e(v_{ii+1jj}+v_{iijj},h_{iijj}) \quad \cdots(38)$$

上記（３８）式が成り立たない場合、権利継承署名$\zeta_{ij}$は不正であるため、ステップＳ１８１２で否定判定となりステップＳ１８２０へ移行する。一方、上記（３８）式が成り立つ場合、権利継承署名$\zeta_{ij}$は正当であるため、肯定判定となりステップＳ１８１４へ移行する。

【０２３７】

ステップＳ１８１４で検証装置１６の制御部２０は、コンテンツ毎に、流用が正当であるか否かを判定する。具体的には、制御部２０は、以下の処理を行う。各部分コンテンツの著作者ＩＤ$_l$を用いて下記（３９）式が成り立つか否かにより流用制御署名及び流用集約署名を検証する。

【０２３８】

【数２５】

$$e(g,\chi_{ij}) = \Pi e(v_{ij},h_{ijk}) \quad \cdots(39)$$

上記（３９）式が成り立たない場合、流用は不正であるため、ステップＳ１８１４で否定判定となりステップＳ１８２０へ移行する。一方、上記（３９）式が成り立つ場合、流用は正当であるため、肯定判定となりステップＳ１８１６へ移行する。

【０２３９】

ステップＳ１８１６で検証装置１６の制御部２０は、コンテンツ毎に、変更及び削除（追加は変更に含まれる）が正当であるか否かを判定する。具体的には、制御部２０は、以下の処理を行う。なお、空データの状態が（０１）または（１０）であれば不正であると判定する。

【０２４０】

まず、部分コンテンツが編集可であれば署名用ハッシュ値を生成し、著作者ＩＤ$_1$の検証鍵を用いて下記（４０）式及び（４１）式が成り立つか否かを検証する。部分コンテンツが実データで変更不可であれば、その実データと公開された変更制御署名用ハッシュ値の整合性とを確認し、空データで変更不可(＝削除不可)であれば、その空データと公開された削除制御署名用ハッシュ値の整合性とを確認する。整合すればその署名用ハッシュ値と著作者ＩＤ$_2$の検証鍵を用いて検査する。それ以外の場合は、部分コンテンツと署名用ハッシュ値が整合していなくても、公開された署名用ハッシュ値と著作者ＩＤ$_2$の検証鍵を用いて検査する。

【０２４１】

【数２６】

$$e(g,\sigma_{ij}) = \Pi e(v_{ij},h_{ijk}) \quad \cdots(40)$$

$$e(g,\tau_{ij}) = \Pi e(v_{ij},h_{ijk}) \quad \cdots(41)$$

上記（４０）式が成り立たない場合、変更が不正であり、上記（４１）式が成り立たない場合、削除が不正である。いずれか一方でも不正である場合、ステップＳ１８１６で否定判定となりステップＳ１８２０へ移行する。一方、上記（４０）式及び（４１）式の両方が成り立つ場合、変更及び削除ともに正当であるため、肯定判定となりステップＳ１８１８へ移行する。

【０２４２】

ステップＳ１８１８で検証装置１６の制御部２０は、検証対象のコンテンツの再生を許可した後、本検証処理を終了する。当該許可により、検証対象のコンテンツの視聴や編集が可能になる。

【０２４３】

一方、上記ステップＳ１８００、及びステップＳ１８０６～Ｓ１８１６の各々において否定判定となった場合に移行するステップＳ１８２０では、検証装置１６の制御部２０は、検証対象のコンテンツの再生を不許可とした後、本検証処理を終了する。従って、この場合は、検証対象のコンテンツの視聴や編集は不可能になる。なお、ステップＳ１８２０の処理に加えて、検査対象のコンテンツが不正なものであることを所定の装置等に報知するようにしてもよい。

【０２４４】

検証処理の具体例について、図９に示した構造のコンテンツを例として説明する。具体例として、コンテンツＡ$_{15}$、Ａ$_{16}$を合成可に設定されたコンテンツとして（Ａ$_{15}$は両側、Ａ$_{16}$はＡ$_{15}$側のみ合成可とする）、それらからＡ$_{22}$が合成されている場合を想定する。

【０２４５】

上記ステップＳ１８００～Ｓ１８０６の処理を行い、各部分データは正当な管理局署名をもち、構造データよりＡ$_{22}$がＡ$_{15}$、Ａ$_{16}$から構成されており、コンテンツＩＤも整合していることを確認する。これらの処理は、コンテンツの著作者の検証鍵を特定する意味がある。整合していなければこのコンテンツは使用不可となるが、整合している場合ステップＳ１８０８に進む。

【０２４６】

次に、ステップＳ１８０８においてコンテンツ毎に使用制御署名の検証を行う。使用条件としてある組織に所属している人のみ使用可能とすれば、そのコンテンツの使用者が検証装置にその組織に属していることを証明するユーザＩＤ及びパスワードなどを入力することによりそのコンテンツは使用可能となる。上記ＩＤやパスワードが入力されないまたは整合しない場合、そのコンテンツは使用不可となる。ここでは、各コンテンツは使用可であるとする。

【０２４７】

次に、ステップＳ１８１０において合成集約署名の検証を行う。まず、Ａ$_{15}$が４つの

部分コンテンツ（各合成制御署名を$\delta_{15i}$とする）からなり、$h_{150}$と$h_{155}$等は合成処理に対する開始位置署名$\alpha_{15}$と最終位置署名$\beta_{15}$の生成に用いたハッシュ値であるとすると、元々の合成集約署名は、下記（４２）式の最上式のようになっている。この場合、上記（３７）式による検証が成功する。すなわち、下記（４２）式の最下式が成立する。ここで、検証鍵はコンテンツＩＤから特定される著作者の鍵を用いる。ただし、$A_{15}$は両側に対して合成可能であるので、前合成に対する集約署名と後合成に関する集約署名を持つ。一般に、前合成集約署名$\delta_{15f}$と後合成集約署名$\delta_{15b}$は開始位置署名$\alpha_{15}$と最終位置署名$\beta_{15}$計算時の乱数が異なるため異なるが、ここでは簡単のため$\delta_{15f}=\delta_{15b}=\delta_{15}$とする。

【０２４８】

【数２７】

$$\delta_{15}=\alpha_{15}+\delta_{151}+\delta_{152}+\delta_{153}+\delta_{154}+\beta_{15}=s_{15}h_{15}$$
$$h_{15}=h_{150}+h_{151}+h_{152}+h_{153}+h_{154}+h_{155}$$
$$e(g,\delta_{15})=e(g,s_{15}h_{15})=e(gs_{15},h_{15})=e(v_{15},h_{15}) \quad \cdots(42)$$

また、合成後にＩＤ$_{22}$がＡ$_{16}$の部分コンテンツＩ$_{163}$をＩ’$_{163}$に変更してＡ$_{15}$とＡ$_{16}$の関係を固定する場合、上記（４２）式は、下記（４３）式のように変更される。ただし、δ’$_{163}$はＩＤ$_{22}$が生成したものであり、公開されない。また、ｈ’$_{163}$の検証には合成不可としたＩＤ$_{22}$（Ｉ’$_{163}$の著作者ＩＤ$_{1}$として公開）の検証鍵が用いられる。Ａ$_{16}$の検証についても同様である。

【０２４９】

【数２８】

$$\delta'_{15}=\delta_{15}-\sum_k\delta_{15k}+\sum_k\delta_{16k}-\delta_{163}+\delta'_{163}=\alpha_{15}+\delta_{161}+\delta_{162}+\delta'_{163}+\delta_{164}+\beta_{15}=s_{15}h'_{15}+s_{16}h'_{16}+\delta'_{163}$$
$$\delta'_{16}=\delta_{16}-\sum_k\delta_{16k}+\sum_k\delta_{15k}+\delta'_{163}=\alpha_{16}+\delta_{151}+\delta_{152}+\delta_{153}+\delta_{154}+\delta'_{163}+\beta_{16}=s_{15}h''_{15}+s_{16}h''_{16}$$
$$h'_{15}=h_{150}+h_{155},\quad h'_{16}=h_{161}+h_{162}+h_{164},\quad h''_{15}=h_{151}+h_{152}+h_{153}+h_{154},\quad h''_{16}=h_{160}+h'_{163}+h_{165}$$
$$e(g,\delta'_{15})=e(g,s_{15}h'_{15}+s_{16}h'_{16}+\delta'_{163})=e(gs_{15},h'_{15})e(gs_{16},h'_{16})e(g,s_{22}h'_{163})$$
$$=e(v_{15},h'_{15})e(v_{16},h'_{16})e(gs_{22},h'_{163})=e(v_{15},h'_{15})e(v_{16},h'_{16})e(v_{22},h'_{163}) \quad \cdots(43)$$

次に、ステップＳ１８１２において権利継承署名の検証を行う。Ａ$_{15}$、Ａ$_{16}$とＡ$_{22}$の各権利継承署名ζ$_{15}$、ζ$_{16}$、及びζ$_{22}$は下記（４４）式で表される。

【０２５０】

【数２９】

$$\zeta_{15}=\sum_k\delta_{15k}=s_{15}h_{15},\quad \zeta_{16}=\sum_k\delta_{16k}=s_{16}h_{16}$$
$$\zeta_{22}=s_{22}h_{22}+\zeta_{15}+\zeta_{16}+s_{22}h_{15}+s_{22}h_{16} \quad \cdots(44)$$

このとき、上記（３８）式の左辺は下記（４５）式のようになる。

【０２５１】

【数３０】

$$\begin{aligned}e(g,\zeta_{22}) &= e(g, s_{22}h_{22} + \zeta_{15} + \zeta_{16} + s_{22}h_{15} + s_{22}h_{16}) \\ &= e(g, s_{22}h_{22})e(g, \zeta_{15} + s_{22}h_{15})e(g, \zeta_{16} + s_{22}h_{16}) \\ &= e(gs_{22}, h_{22})e(g, s_{15}h_{15} + s_{22}h_{15})e(g, s_{16}h_{16} + s_{22}h_{16}) \\ &= e(v_{22}, h_{22})e(g, (s_{15} + s_{22})h_{15})e(g, (s_{16} + s_{22})h_{16}) \\ &= e(v_{22}, h_{22})e(gs_{15} + gs_{22}, h_{15})e(gs_{16} + gs_{22}, h_{16}) \\ &= e(v_{22}, h_{22})e(v_{15} + v_{22}, h_{15})e(v_{16} + v_{22}, h_{16})\end{aligned} \quad \cdots(45)$$

また、構造データからＡ２２に係わる著作者はＩＤ２２だけであり、Ａ２２を構成するＡ１５、Ａ１６に係わる著作者はＩＤ２２とＩＤ１、ＩＤ２２とＩＤ１６であることがわかる。そのため、Ａ２２に係わる全階層のコンテンツとそれに係わる著作者の検証鍵によって構成される上記（３８）式の右辺は下記（４６）式となり、上記（３８）式が成り立つことがわかる。

【０２５２】

【数３１】

$$\prod e(v_{ii+1,jj} + v_{iijj}, h_{iijj}) = e(v_{22}h_{22})e(v_{22} + v_{15}, h_{15})e(v_{22} + v_{16}, h_{16}) \quad \cdots(46)$$

また、Ａ２１とＡ３１の権利継承署名も同様に下記（４７）式のようになり、正しく合成されていれば上記（３８）が成立する。

【０２５３】

【数３２】

$$\begin{aligned}\zeta_{21} &= s_{21}h_{21} + \zeta_{11} + \zeta_{12} + \zeta_{13} + \zeta_{14} + s_{21}(h_{11} + h_{12} + h_{13} + h_{14}) \\ \zeta_{31} &= s_{31}h_{31} + \zeta_{21} + \zeta_{22} + s_{31}(h_{21} + h_{22}) \\ &= s_{31}h_{31} + (s_{22}h_{22} + \zeta_{15} + \zeta_{16} + s_{22}h_{15} + s_{22}h_{16}) + (s_{21}h_{21} + \zeta_{11} \\ &\quad + \zeta_{12} + \zeta_{13} + \zeta_{14} + s_{21}(h_{11} + h_{12} + h_{13} + h_{14}) + s_{31}(h_{21} + h_{22}) \\ &= s_{31}h_{31} + (s_{21} + s_{31})h_{21} + (s_{22} + s_{31})h_{22} + (\zeta_{11} + s_{21}h_{11}) \\ &\quad + (\zeta_{12} + s_{21}h_{12}) + (\zeta_{13} + s_{21}h_{13}) + (\zeta_{14} + s_{21}h_{14}) + (\zeta_{15} + s_{22}h_{15}) + (\zeta_{16} + s_{22}h_{16})\end{aligned} \quad \cdots(47)$$

ここで、ＩＤ３１がＡ１５を自分が制作したＡ’１５に変更する場合、ＩＤ３１は公開されているＡ１５の合成制御署名を権利継承署名ζ２２とζ３１から削除し、Ａ’１５に対する合成制御署名を生成して追加する。ただし、権利継承署名では合成後に合成不可としても隣接コンテンツを対象としないので処理は変わらない。この場合、権利継承署名ζ２２とζ３１は下記（４８）式のように変化する。ただし、ＩＤ３１が元々Ａ１５自体を制作し、さらにＡ２２を制作する場合、Ａ１５はＩＤ３１によって２度署名されることになるため、その際に回数のパラメータは更新され、新たな署名とされる。

【０２５４】

【数３３】

$$\zeta'_{22}=\zeta_{22}-s_{22}h_{22}+s_{31}h'_{22}+(\zeta'_{15}-\zeta_{15})-s_{22}h_{15}+s_{31}h'_{15}$$
$$=s_{31}h'_{22}+\zeta'_{15}+\zeta_{16}+s_{31}h'_{15}+s_{22}h_{16}$$
$$\zeta'_{31}=\zeta_{31}+s_{31}(h'_{31}-h_{31})+(\zeta'_{22}-\zeta_{21})+s_{31}(h'_{22}-h_{22})$$
$$=s_{31}h'_{31}+\zeta_{21}+\zeta'_{22}+_{31}(h_{21}+h'_{22})$$

・・・(48)

次に、ステップＳ１８１４において流用に関する検証を行う。例えば、Ａ$_{15}$の４個の部分コンテンツのうちＡ$_{151}$をＩＤ$_{15}$作の流用不可設定コンテンツ、Ａ$_{152}$をＩＤ$_{15}$作の流用可設定コンテンツ、Ａ$_{153}$をＩＤ$_{16}$作の流用コンテンツ、Ａ$_{154}$をＩＤ$_{17}$が変更した部分コンテンツとする。流用制御署名とその集約署名は下記（４９）式のようになり、上記（３９）式によって以下のように検証される。

【０２５５】

【数３４】

$$\chi_{15}=\alpha_{15}+\chi_{151}+\chi_{152}+\chi_{153}+\chi_{154}+\beta_{15}$$
$$=s_{15}h_{15}+s_{16}h_{153}+s_{17}h_{154},\quad h_{15}=h_{150}+h_{151}+h_{152}+h_{155}$$
$$e(g,\chi_{15})=e(g,s_{15}h_{15}+s_{16}h_{153}+s_{17}h_{154})$$
$$=e(gs_{15},h_{15})e(gs_{16},h_{153})e(gs_{17},h_{154})$$
$$=e(v_{15},h_{15})e(v_{16},h_{153})e(v_{17},h_{154})$$

・・・(49)

最後に、ステップＳ１８１６において各コンテンツの編集集約署名の検証を行う。前例と同様の構成では、Ａ$_{15}$の変更制御署名とその集約署名は下記（５０）式のようになり（α$_{15}$、β$_{15}$、及びｈ$_{15}$は処理毎に異なる）、上記（３８）式によって以下のように検証される。

【０２５６】

【数３５】

$$\sigma_{15}=\alpha_{15}+\sigma_{151}+\sigma_{151}+\sigma_{153}+\sigma_{154}+\beta_{15}=s_{15}h_{15}$$
$$h_{15}=h_{150}+h_{151}+h_{152}+h_{153}+h_{154}+h_{15m}$$
$$e(g,\sigma_{15})=e(g,s_{15}h_{15})=e(gs_{15},h_{15})=\Pi e(v_{15},h_{15k})$$

・・・(50)

また、部分コンテンツＡ$_{154}$が変更可能であり、ＩＤ$_{31}$がＡ’$_{154}$に変更した場合、下記（５１）式のようになる。これは、削除集約署名に関しても同様である。

【０２５７】

【数３６】

$$\sigma'_{15}=\alpha_{15}+\sigma_{151}+\sigma_{152}+\sigma_{153}+\sigma'_{154}+\beta_{15}=s_{15}h'_{15}+\sigma'_{154}$$
$$h_{15}=h_{150}+h_{151}+h_{152}+h_{153}+h_{15m},\quad \sigma'_{154}=s_{31}h'_{154}$$
$$e(g,\sigma'_{15})=e(g,s_{15}h'_{15}+s_{31}h'_{154})=\Pi e(v_{15},h'_{15k})e(v_{31},h'_{154})$$

・・・(51)

［第２実施形態］

第１実施形態では各種制御署名に対する集約署名を機能毎に分けて構成したが、集約署名を集約してその数を減少させることができる。以下に第１実施形態との相違部分を中心に記述し説明する。ただし、管理局署名及び使用制御署名もηに含ませ集約することもできる。

【０２５８】

鍵の生成については、第１実施形態と同様であり、著作者（署名者）ＩＤ$_{ij}$は署名鍵$s_{ij}\in Z_p^*$を持ち、それに対する検証鍵$v_{ij}=s_{ij}g$を公開する。

【０２５９】

本実施形態の著作権保護システム１０の端末装置１２で行われる著作権保護処理（図１４参照）の全体的な流れは同一であり、著作権保護処理のステップＳ１４０４における電子署名作成処理（図１６参照）の一部が異なっている。図２１に示すように本実施形態の電子署名作成処理では、第１実施形態の電子署名作成処理のステップＳ１６１８の代わりにステップＳ１６１９を実行する他は、各ステップにおいて同一の処理を行う。ここでは第１実施形態と相違するステップＳ１６１９の処理についてのみ説明する。なお、本実施形態の電子署名作成処理では、$\alpha_{ij}$及び$\beta_{ij}$は集約署名毎に必要な分のみ生成する。

【０２６０】

本実施形態の電子署名作成処理のステップＳ１６１９では、下記（５２）式を用いて制御に関する集約署名を集約する。ただし、下記（５２）式において$\alpha_{ij}$及び$\beta_{ij}$は異なる値である。

【０２６１】

【数３７】

$$\text{集約署名：}\ \eta_{ij}=\alpha_{ij}+\sum_k\sigma_{ijk}+\sum_k\tau_{ijk}+\sum_k\chi_{ijk}+\sum_k\delta_{ijk}+\beta_{ij} \qquad \cdots(52)$$

また、本実施形態の著作権保護システム１０の端末装置１２で実行される編集処理(図１７参照）の全体的な流れは同一であり、編集処理のステップＳ１７０５Ａの編集制御処理（図１９参照）及びステップＳ１７０５Ｄの合成・権利継承処理（図２０参照）の一部が異なっているため、各々異なる処理について説明する。

【０２６２】

図２２に示すように本実施形態の編集制御処理では、第１実施形態の編集制御処理のステップＳ１９１４の代わりにステップＳ１９１５を実行する他は、各ステップにおいて同一の処理を行う。

【０２６３】

本実施形態の編集制御処理のステップＳ１９１５では、第１実施形態のステップＳ１９１４と同様にして生成した集約署名により、下記（５３）式を用いて集約署名の集約を更新し、公開する。

【０２６４】

【数３８】

$$\text{集約署名：}\ \eta'_{ij}=\eta_{ij}-\sigma_{ijk}+\sigma'_{abk}-\tau_{ijk}+\tau'_{abk}-\chi_{ijk}+\chi'_{abk}-\delta_{ijk}+\delta'_{abk} \qquad \cdots(53)$$

一方、本実施形態の合成・権利継承処理では、第１実施形態の合成・権利継承処理と同一の処理を行うため、図２０を参照して説明する。

【０２６５】

図２０に示した合成・権利継承処理のうち合成処理に関するステップＳ２０００～Ｓ２００６の各処理については、ステップＳ２００６で集約署名ηに対して上記（３４）式と同様の$\delta_{ijk}$の入れ替えを行う他は、同様の処理を行う。

【０２６６】

一方、合成・権利継承処理のうち権利継承処理に関するステップＳ２００８及びＳ２０１０の各処理については第１実施形態と同様である。

【０２６７】

また、本実施形態の著作権保護システム１０では、端末装置１２や検証装置１６で実行される検証処理の一部が第１実施形態の検証処理（図１８参照）と異なる。図２３に示すように本実施形態の検証処理は、第１実施形態の検証処理のステップＳ１８１０の代わりにステップＳ１８１１を実行する。また、図２３に示すように本実施形態の検証処理では、第１実施形態の検証処理のステップＳ１８１４及びステップＳ１８１６の処理が削除されている。

【０２６８】

なお、その他の各ステップ（処理）については、第１実施形態と同様であるが、管理局署名μ及び使用制御署名λを集約署名ηに含ませた場合は、ステップＳ１８００及びＳ１８０８の処理を省略する。

【０２６９】

ここでは第１実施形態と相違するステップＳ１８１１の処理についてのみ説明する。

【０２７０】

ステップＳ１８１１では、コンテンツ毎に編集及び流用に関して、著作者の検証鍵$\nu_{ij}$を用いて、下記（５４）式が成り立つか否かにより検証を行う。ただし、$h_{ij}$は$\eta_{ij}$に含まれる各種署名に対応するハッシュ値である。ただし、管理局署名μ及び使用制御署名λを集約署名ηに含ませた場合、ηとλも一緒に検証を行う。

【０２７１】

【数３９】

$$e(g,\eta_{ij}) = \prod e(v_{ij}, h_{ijk}) \qquad \cdots(54)$$

上記（５４）式が成り立たない場合、不正であるため、ステップＳ１８１１で否定判定となりステップＳ１８２０へ移行する。一方、上記（５４）式が成り立つ場合、正当であるため、肯定判定となりステップＳ１８１２へ移行する。

【０２７２】

以上より、制御署名に関しては１つまで任意に集約署名を集約できることがわかる。

【０２７３】

これにより、本実施形態の著作権保護システム１０によれば、編集制御に関する検証処理が１度でよくなる。また、図１２に示した開始データや最終データに紐付ける集約署名の数も減少させることができる。

［第３実施形態］

第２実施形態ではコンテンツ及び部分コンテンツの編集制御に関する署名を１つの集約署名にまで減少させた。本実施形態では、権利継承署名も合わせて１つの署名に集約する例を示す。

【０２７４】

すなわち、第２実施形態に示した$\eta_{ij}$を、第１実施形態の合成・権利継承処理（図２０参照）のステップＳ２００８における権利継承署名作成における$\zeta_{ik}$として署名を生成することによって権利継承署名$\zeta_{i+1k}$が実現できる。

【０２７５】

ただし、第１実施形態の合成・権利継承処理では、権利継承署名は公開されている$\zeta_{ik}$のみを用いて構成されるが、第２実施形態に示した$\eta_{ij}$はコンテンツ毎に常に公開されているため、$\zeta_{i+1k}$は常に構成できる。しかし、編集または合成の制御に違反して$\zeta_{i+1k}$を構成すれば、署名が整合しないことは明らかである。

【０２７６】

以上によって、本実施形態の著作権保護システム１０によれば、１つの署名で権利継承

と同時に編集制御を検証できる。

【０２７７】

また、第１実施形態ではコンテンツ単位での権利継承となっているが、本実施形態の著作権保護システム１０では、コンテンツにおける部分コンテンツの数を１つとし、そのコンテンツの合成によってコンテンツを表すようにすることもできる。これにより、部分コンテンツがコンテンツの位置づけとなるため部分コンテンツ単位での権利継承、すなわち部分コンテンツ毎に合成コンテンツの中での位置づけを検証できる。この場合、部分コンテンツは１つでも開始データと最終データを持ち、編集不可の部分コンテンツの集約署名は公開しても制御署名は公開しない。よって、編集制御に違反して編集不可の部分コンテンツを編集可として編集（合成含む）すれば署名が整合せず、変更不可の部分コンテンツに変更しようとしてもオリジナルの著作者である著作者$ＩＤ_1$以外の著作者は、その設定を変更できないことは第１実施形態で説明したとおりであり、権利継承と編集制御を一緒にしても不正な編集はできない。

【０２７８】

それに対して、従来技術において部分コンテンツの編集制御署名を直接用いて権利継承署名を構成する場合が示されるが、この場合、本発明の本質である部分コンテンツの流用・編集が制御されないため任意の流用・編集が行われる。

【０２７９】

すなわち、従来技術では、集約署名ではなく編集制御署名を直接用いているため、編集に関する設定を容易に変更される。例えば編集不可の部分コンテンツの場合、本実施形態の著作権保護システム１０では編集制御署名を公開しないが、用いた部分コンテンツの関係を表すため編集制御署名を直接用いる従来技術では、編集不可の部分コンテンツであっても権利継承に用いる編集制御署名を公開すれば編集可に変更される可能性がある。また、従来技術においては権利継承用の署名を作成しているが、本実施形態の著作権保護システム１０によって編集制御に用いた集約署名を権利継承に転用でき、署名生成の手間や署名保存の手間が削減できる。

［第４実施形態］

上記第１～第３実施形態ではＢＬＳ署名を元に構成したが、ＢＬＳ署名に限定されず、本発明は署名を集約できる方式であれば一般的に構成可能である。本実施形態では、その一例として公開情報であるＩＤを用いて署名を検証可能なＩＤベース署名に基づくＩＤベースアグリゲート署名によって本発明を構成する場合について説明する。アグリゲートとは集約を意味する。

【０２８０】

電子署名として、ＩＤベースアグリゲート署名について説明する。

【０２８１】

下記（５５）式を署名の作成が可能な署名者のグループとして定義し、さらに、下記（５６）式を実際にアグリゲート署名作成に参加した署名者のグループと定義する。

【０２８２】

【数４０】

$$\mathbb{U} = \{u_1, \cdots, u_n\} \quad \cdots(55)$$

$$\mathbb{L} = \{u_{i1}, \cdots, u_{il}\} \quad \cdots(56)$$

さらに、下記（５７）式を、この署名参加者全員の符号とする。

【０２８３】

【数４１】

$$\mathbb{I} = \{i_1, \cdots, i_l\} \quad \cdots(57)$$

この場合、ＩＤベースアグリゲート署名は以下の通りに構成される。

【０２８４】
まず、準備として生成元を
【０２８５】
【数４２】

$$P \in \mathbb{G} \quad \mathbb{G}\text{はペアリング演算が可能な楕円曲線上の点の集合。}$$

とする。
【０２８６】
また、
【０２８７】
【数４３】

$$s \in \mathbb{Z}_q^*$$

を選ぶ。第３者の秘密鍵発行センターＴＡは、$P_{pub}=sP$を計算し、ｓをマスターキーとする。
【０２８８】
鍵の生成は、まず、一方向性ハッシュ関数$H_1$を下記（５８）式のように定義する。
【０２８９】
【数４４】

$$H_1:\{0,1\}^* \rightarrow \mathbb{G}' \quad \mathbb{G}'\text{は位数pの巡回群。} \quad \cdots(58)$$

署名者$u_i$のユーザＩＤ情報を$ID_i$としたとき、秘密鍵発行センターＴＡは下記（５９）式を計算し、下記（６０）式で定義される鍵を発行する。
【０２９０】
【数４５】

$$Q_{ID_i} = H_1(ID_i) \quad \cdots(59)$$
$$d_{ID_i} = sQ_{ID_i} \quad \cdots(60)$$

次に、署名を作成する。まず、一方向性ハッシュ関数$H_2$を下記（６１）式のように定義する。
【０２９１】
【数４６】

$$H_2:\{0,1\}^* \rightarrow \mathbb{G}' \quad \cdots(61)$$

$m_i$を署名対象となる平文としたとき、署名者は、
【０２９２】
【数４７】

$$r_i \in \mathbb{Z}_q^*$$

を選び、$U_i=r_iP$を計算する。その後、$h_i=H_2(ID_i, m_i, U_i)$を計算し、$m_i$に対する電子署名$V_i$を下記（６２）式により計算する。

【０２９３】
【数４８】

$$V_i = d_{ID_i} + r_i h_i \qquad \cdots(62)$$

次に電子署名Ｖ$_i$を集約した集約署名Ｖを作成する。アグリゲート署名作成に参加する全ての参加者の署名Ｖ$_i$を集め、集約署名Ｖを下記（６３）式により計算する。
【０２９４】
【数４９】

$$V = \sum_{i=1}^{n} V_i \qquad \cdots(63)$$

ある電子署名が正当に作成された集約署名Ｖであるか否かを判定する場合、検証者にＰ、Ｐ$_{pub}$、Ｖ、Ｕ$_i$、ｍ$_i$、及びＩＤ$_i$が与えられたとき、検証者は、ｈ$_i$＝Ｈ$_2$（ＩＤ$_i$、ｍ$_i$、Ｕ$_i$）を計算し、下記（６４）式が成立するか判定する。
【０２９５】
【数５０】

$$e(P,V) = \prod_{i=1}^{n} e(P_{pub}, Q_{ID_i}) e(U_i, h_i) \qquad \cdots(64)$$

上記（６４）式は、双線形写像の特性によって下記（６５）式のように展開され、平文の正当性を検証できる。
【０２９６】
【数５１】

$$\begin{aligned} e(P,V) &= e\left(P, \sum_{i=1}^{n} d_{ID_i} + \sum_{i=1}^{n} r_i h_i\right) \\ &= e\left(P, \sum_{i=1}^{n} d_{ID_i}\right) e\left(P, \sum_{i=1}^{n} r_i h_i\right) \\ &= \prod_{i=1}^{n} e\left(P, d_{ID_i}\right) e(P, r_i h_i) \\ &= \prod_{i=1}^{n} e(P_{pub}, Q_{ID_i}) e(U_i, h_i) \end{aligned} \qquad \cdots(65)$$

上記（６２）式～（６４）式は、第１実施形態におけるＢＬＳ署名の説明において上述した（８）式～（１０）式に対応し、上記（６５）式は上記（１１）式及び（１２）式に対応する。よって、第１～第３実施形態における各種署名及び検証式を上記（６２）式～（６４）式の形式に変形すれば、ＩＤベースアグリゲート署名を適用した著作権保護システム１０を構成できることは明らかである。
【０２９７】
以上より、本発明の著作権保護システム１０はＢＬＳ署名やＩＤベース署名等に限定されず、第１実施形態において上記した（８）式～（１０）式または本実施形態において上記した（６２）式～（６４）式のように署名を集約でき、その集約署名を１回の処理で検証できれば種々の電子署名に適用可能であることは明らかである。
［第５実施形態］
１つの部分コンテンツを時系列に複数の著作者によって修正する場合等は、修正部分（元の部分と変更部分の差分）を修正制御によって制御することもできる。この場合、各部分コンテンツは変更制御署名と異なる修正制御署名によって制御される。部分コンテンツの変更は異なる著作者の部分コンテンツへの差し替えであるので１つの署名によって制御

されるが、修正は元の著作者の部分コンテンツに他の著作者による修正部分を加えたものであり複数設定が可能である。ただし、この場合、修正部分はレイヤ構造等によって表現され、元の部分コンテンツが最下層のレイヤ、修正部分がその上のレイヤとなり、修正が加わるためにレイヤが増加する等、その差分が明確に分かる必要がある。

【０２９８】

部分コンテンツ$I_{ijk}$に対する修正制御署名を$\rho_{ijk_t}$（ｔは修正回数を示す）とすると$\rho_{ijk_t}$の署名対象である修正部分を上記（１５）式における$A_{ijk}$として、修正回数を署名回数と同様に部分コンテンツＩＤ に作用させたものを用いて修正制御署名が生成される。修正を許可する場合、修正制御署名は公開され、それ以降の修正を許可しない場合修正制御署名は公開しない。よって、修正制御署名が公開されていないｔ以降の修正は無視される。例えば、修正可否情報（修正可＝１、修正不可＝０ とする）とし、ｔ＝０にあたる最初の部分コンテンツが修正不可であれば、部分コンテンツＩＤの末尾に０が設定され、それを用いて修正制御署名が生成される。よって、その集約署名を下記（６６）式とすれば、後の著作者が修正不可を修正可とするまたはｔ＝１として新たな修正制御署名を生成しても署名が整合しない。ただし、修正集約署名とその著作者ＩＤもその他に記述される。

【０２９９】

【数５２】

$$\rho_{ijk}=\alpha_{ijk}+\sum_{t}\rho_{ijk\_t}+\beta_{ijk} \qquad \cdots(66)$$

また、最初の部分コンテンツが修正可であれば、次の著作者が修正を行い、その修正部に対してｔ＝１として修正制御署名を生成して集約署名を更新する。その修正制御署名が公開されていれば、その後も修正処理は可能であり、修正不可とする場合、修正制御署名を非公開にする。また、集約署名を下記（６７）式のようにすればコンテンツ単位での検証が可能である。

【０３００】

【数５３】

$$\rho_{ij}=\alpha_{ij}+\sum_{k}\sum_{t}\rho_{ijk\_t}+\beta_{ij} \qquad \cdots(67)$$

［第６実施形態］

第１～第４実施形態では変更制御署名と削除制御署名とによって部分コンテンツの変更・削除・追加に関する制御を実現した。

【０３０１】

これに対し本実施形態の著作権保護システム１０では、変更可かつ削除不可や変更不可かつ削除可の制御状態をなくした。この場合、削除制御署名はなしにすることができる。すなわち、部分コンテンツの編集を変更制御署名のみで実現できることは明らかである。

【０３０２】

また、本実施形態の著作権保護システム１０が、第１～第４実施形態に示した制御の一部分だけを必要な署名のみを用いて実現するが、このように実現可能であることは明らかである。

【０３０３】

本実施形態の著作権保護システム１０では、第２及び第３実施形態は制御に関する機能は削減せず、署名の数のみを削減したため、保持または検証する署名数は減少したが、処理の複雑さが増し計算量的な削減は行われていない。それに対して、制御に関する機能を限定することで署名の数と計算量を同時に削減できる。

［第７実施形態］

第１～第５実施形態では記述を簡単にするため、部分コンテンツの変更は１つの変更制御署名によって制御した。しかしながら、変更には様々な変更が考えられる。

【０３０４】

一例として、本実施形態の著作権保護システム１０では、部分コンテンツの面的な一部変更等は変更を許可する部分毎に変更制御署名を設定する、すなわち１つの部分コンテンツに対して許可する変更部分に応じて複数の変更制御署名を設定し、その部分毎に検証を行う。このような場合、１つの部分コンテンツに複数の著作者による署名が紐付けられることになる。

【０３０５】

また、部分コンテンツの変化の度合いなどの深さ方向の変更を制御したい場合はその制限を超えているかどうかを含め検証することができる。すなわち、使用制御における使用条件のような条件（制限）を部分コンテンツ毎に定め、その範囲内であることを検証できるようにすればよい。例えば色の変更の範囲等の場合、部分コンテンツの指定された部分の色情報を確認できる仕組みなどを導入すればよい。

【０３０６】

または初めから部分コンテンツをコンテンツとして構成し、各部分やその範囲に関するものを部分コンテンツとして制御する等も考えられる。

［第８実施形態］

本発明は、暗号技術と組み合わせることにより、コンテンツの不正利用防止と不正編集防止の両立も可能である。

【０３０７】

すなわち、コンテンツは暗号化されランダム化または半開示状態となっており、そのコンテンツを復元できるのは復号鍵を持つ正当な再生機器または編集機器のみとし、正当に復元されたコンテンツに対して本発明を用いて編集を行い、その編集結果を外部に出力するときは再び暗号化または半開示状態の暗号化を行い出力すればよい。

【０３０８】

なお、ここで用いる暗号技術は特に限定されるものではなく、既存の暗号技術を用いることができる。

【０３０９】

これによって、正当なユーザでなければコンテンツを復元できず、かつ編集もできないというシステムが実現できる。

【０３１０】

以上説明したように本発明によれば、コンテンツ間の編集を考慮した著作権の保護を行うことができ、以下の効果が得られる。従来技術において編集とはあるコンテンツ内における部分コンテンツの変更・削除・追加のみを指し、複数回の編集には対応できない場合があったが、本発明は変更・削除・追加に対して従来技術で実現できなかった複数回の編集を実現し、さらに流用と合成及び使用を制御する機能を付加した。よって、本発明における編集は部分コンテンツに対する変更・削除・追加・流用とコンテンツに対する合成・使用を指す。さらに、従来技術で示されていない電子署名とコンテンツまたは部分コンテンツとの紐付け法及び上記編集をすべて電子署名だけで実現する手法を示し、種々の電子署名への拡張することにより、以下の（１）～（６）の効果を実現する。

（１）ある著作者が制作したコンテンツに含まれる部分コンテンツの他のコンテンツへの流用の可否が制御でき、部分コンテンツが著作者の意図に反して勝手に使用されるのを防ぐことができる。

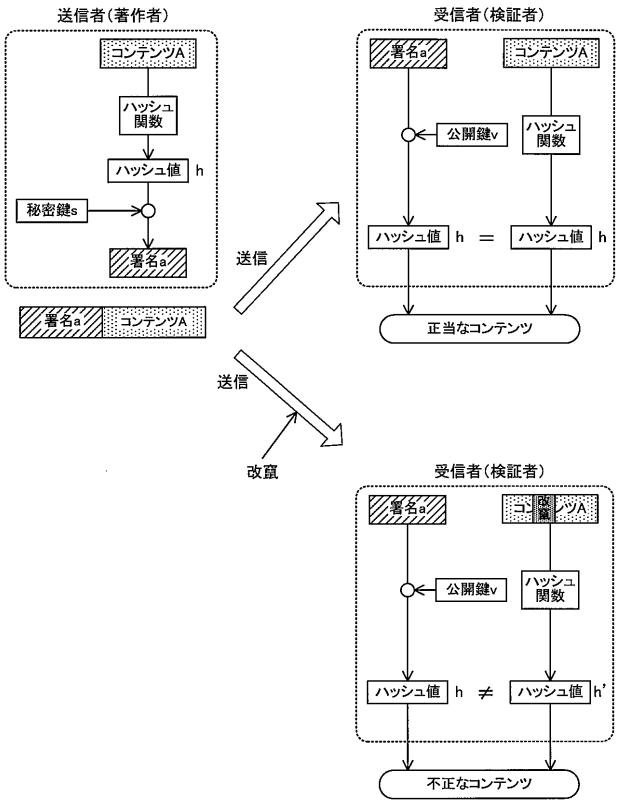
（２）従来技術では、流用された部分コンテンツの編集については著作者が制御できなかったが、流用が許可された部分コンテンツに対しても著作者の意図に従って制御可能にする。

（３）部分コンテンツの追加・削除・変更を繰り返しても、コンテンツの構成が変化せず、変更不可かつ削除可や変更可かつ削除不可などの制御状態を設定できる。

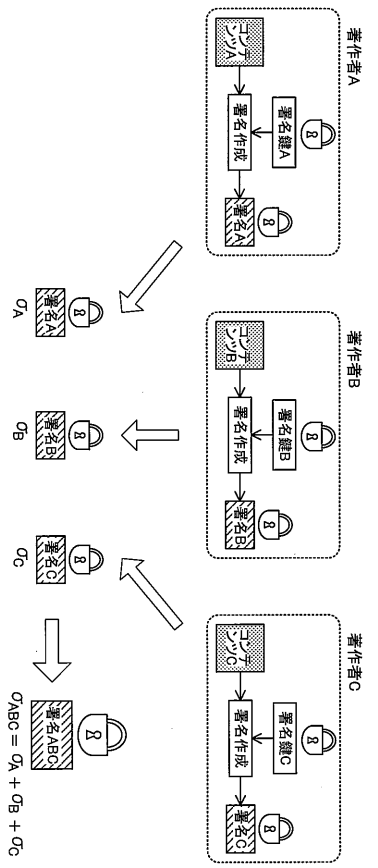
（４）コンテンツを識別可能にし、コンテンツ自体の合成及び使用の制御を可能にする。

すなわち、部分コンテンツの編集制御に加えてコンテンツ単位の編集も可能にする。
（５）部分コンテンツまたはコンテンツとその著作者のバインドを含め、上記を電子署名だけで実現できるシステムが示されることによって、簡易なシステムが構成できる。
（６）特定の電子署名だけでなく、種々の電子署名に対しても拡張できることによりＣＡを必要としないシステム等の広い応用が可能になる。
【符号の説明】
【０３１１】
１０　著作権保護システム
１２　端末装置
１４　管理局装置（管理局）
１６　検証装置

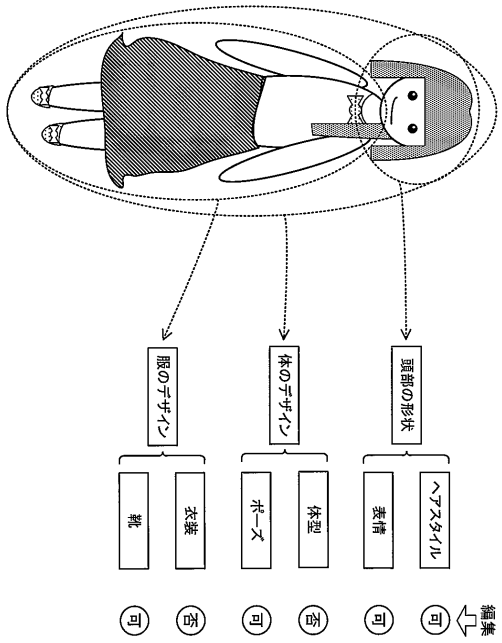
【図１】



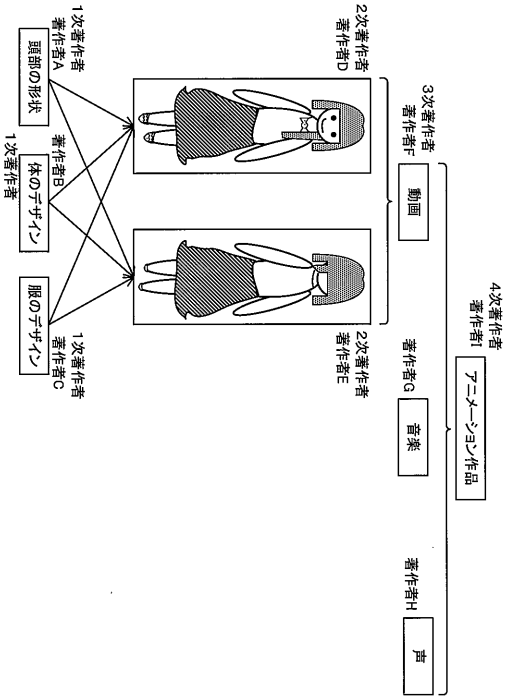

【図２】



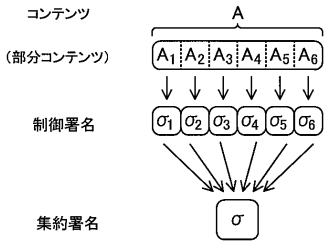
【図３】


頭部の形状
体のデザイン
服のデザイン
ヘアスタイル
表情
体型
ポーズ
衣装
靴
可
否
編集

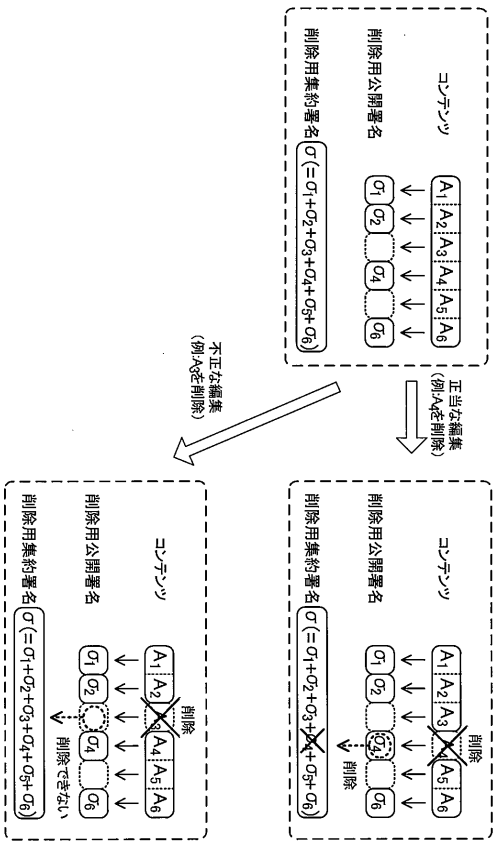
【図４】


アニメーション作品
動画
音楽
声
3次著作者
著作者F
著作者G
著作者H
2次著作者
著作者D
2次著作者
著作者E
1次著作者
著作者A
頭部の形状
著作者B
体のデザイン
1次著作者
著作者C
服のデザイン
4次著作者
著作者I

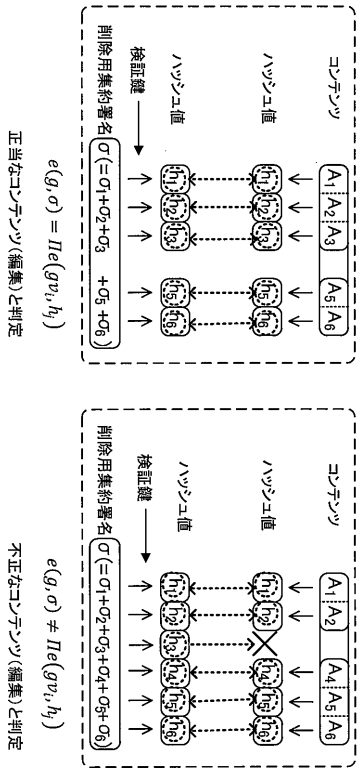
【図５】


コンテンツ
A
(部分コンテンツ)
A1 A2 A3 A4 A5 A6
制御署名
σ1 σ2 σ3 σ4 σ5 σ6
集約署名
σ

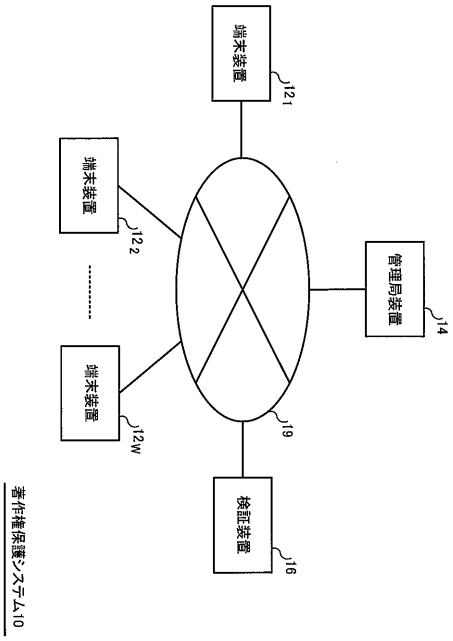
【図６】


コンテンツ
削除用公開署名
削除用集約署名
σ'(=σ1+σ2+σ3+σ4+σ5+σ6)
正当な編集
(例:A4を削除)
不正な編集
(例:A3を削除)
削除
削除できない

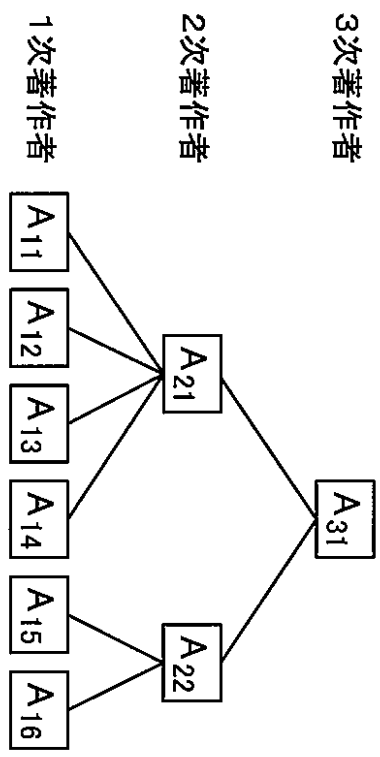
【図７】


コンテンツ
ハッシュ値
検証鍵
削除用集約署名
正当なコンテンツ(編集)と判定
不正なコンテンツ(編集)と判定

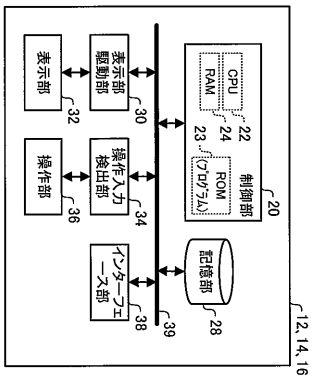
【図８】


端末装置
管理局装置
検証装置
著作権保護システム10

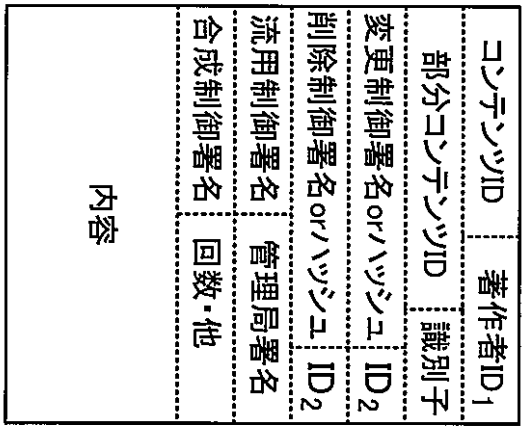
【図９】


3次著作者
2次著作者
1次著作者

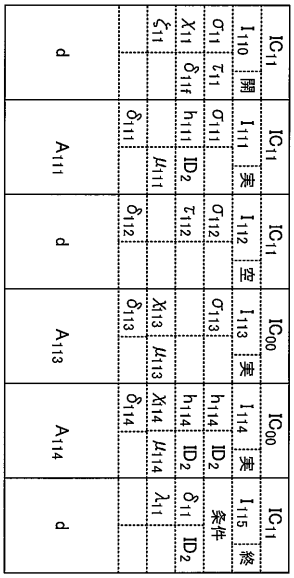
【図１０】


制御部
CPU
RAM
ROM
プログラム
記憶部
表示部駆動部
表示部
操作入力検出部
操作部
インターフェース部

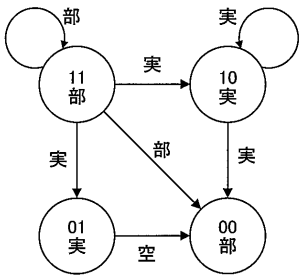
【図１１】



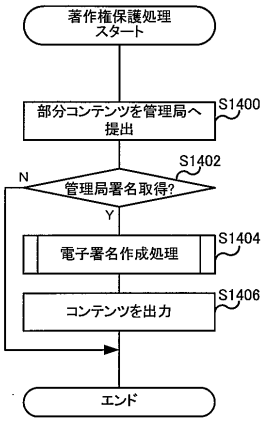

【図１２】



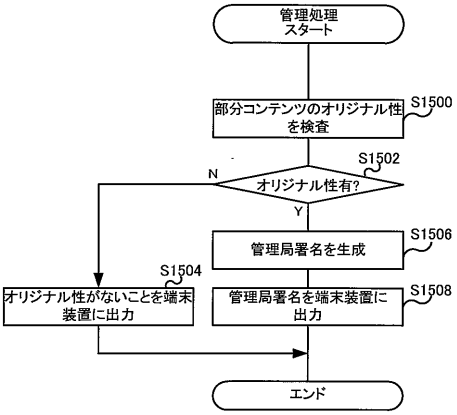

【図１３】



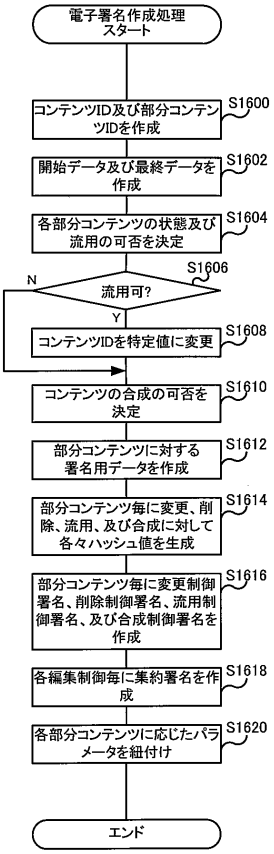

【図１４】



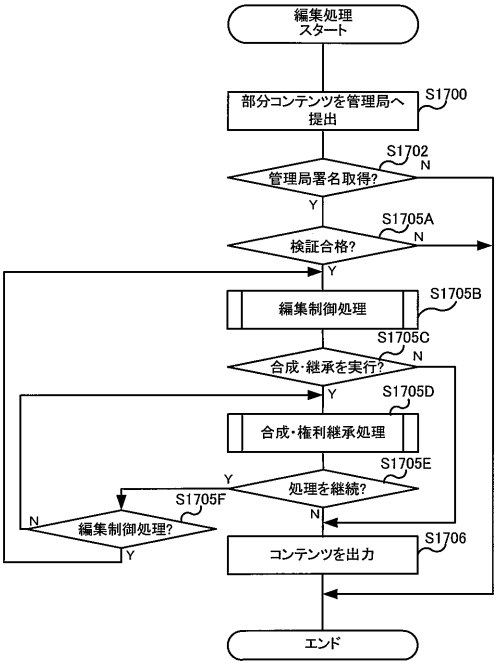

【図１５】



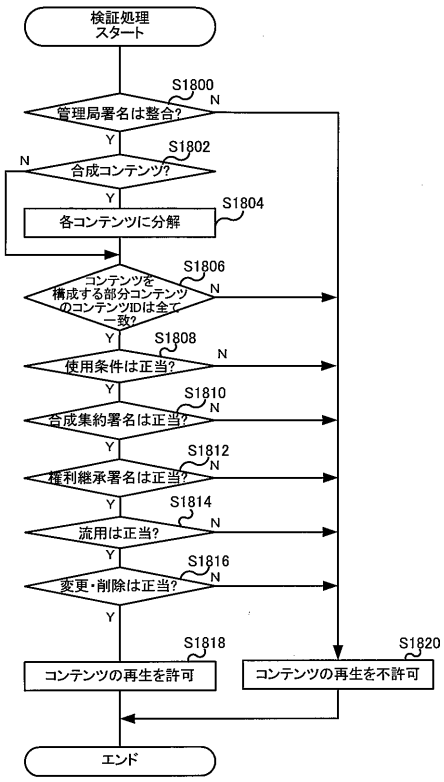
【図１６】



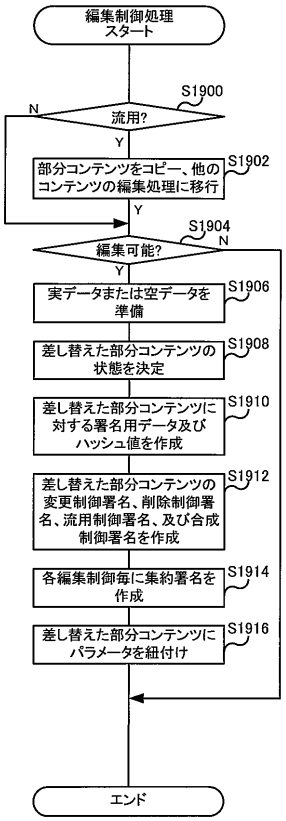

【図１７】



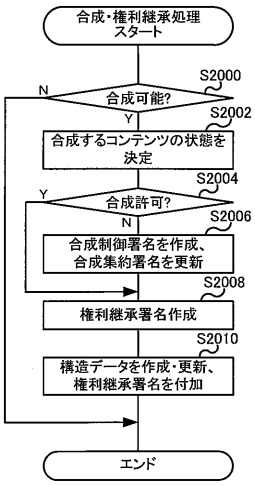

【図１８】



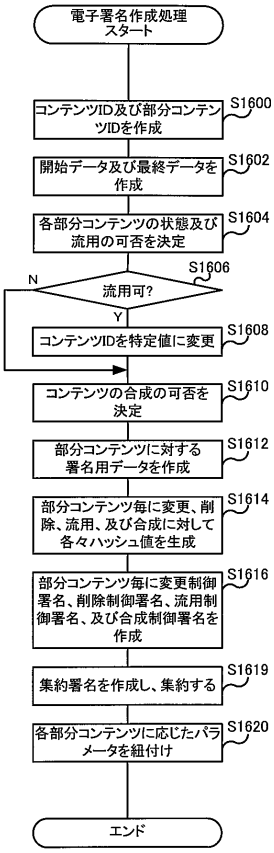

【図１９】



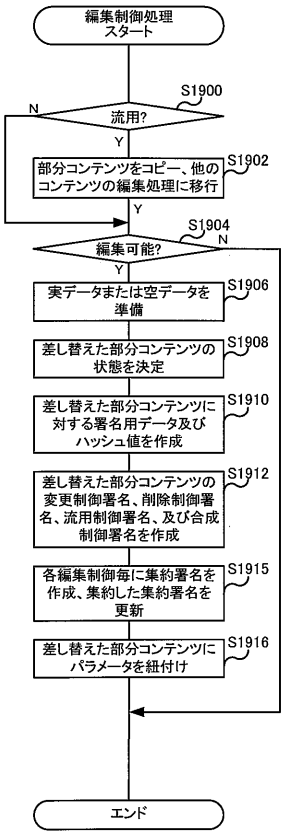
【図２０】



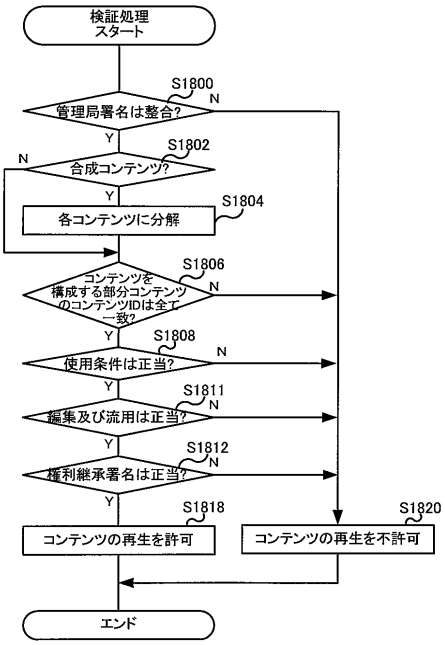

【図２１】




【図２２】




【図２３】



フロントページの続き

Ｆターム(参考) 5J104 AA09 AA12 AA16 AA32 EA04 EA08 EA19 FA00 JA21 LA06
NA02 NA37 NA38 PA14