ID ベース署名に基づくコンテンツ編集制御システム

藤本 竜矢 †1　岩村 惠市†1　稲村 勝樹†2

概要：コンテンツ編集の可否のみの制御が可能である従来の著作権保護技術とは異なり，編集内容毎の制御を可能にした新たな著作権保護方式を提案する．本方式は電子署名を用いることで一つのコンテンツ内の部分コンテンツに対して，変更・削除・追加といった編集制御に加え，部分コンテンツの他コンテンツへの流用や，コンテンツ間の合成を著作者の意志に基づいて制御することが可能である．また、署名方式に ID ベース署名を用いることで認証局による公開鍵証明書の発行も不要となる．本方式は，Youtube などの消費者生成メディアのようなインターネット上のコンテンツ保護に適している．また，様々な攻撃に対する安全性についても評価を行う．

キーワード：編集制御，電子署名，集約署名，ID ベース署名

Copyright Protection Scheme to Realize Edit Control based on ID-based signature

Tatsuya Fujimoto†1　Keiichi Iwamura†1　Masaki Inamura†2

Abstract: We propose a new copyright protection technology enables various types of editing suitable for editable contents, in contrast to the conventional copyright protection technology enables only availability of editing. Our proposed scheme can control diversion of partial contents to the other contents and composition of contents, in addition to control of change, deletion and addition of partial contents in one contents using digital signature based on author's intention. Additionally, public key certificate by a Certificate Authority is not required because we used ID-based signature. This scheme is effective in contents on the latest Internet like consumer generated media such as Youtube. We also evaluate the security of our proposed scheme against various attacks.

Keywords: Edit Control, Digital Signature, Aggregate Signature, ID-based signature

1. はじめに

近年，インターネットの普及により消費者自身によりコンテンツの生成・流通が行われている．これを消費者生成メディア(CGM:Consumer Generated Media)と呼び，Youtube[1]，CLIP[2]などのサービスが代表的である．この CGM において，コンテンツが著作者の意図に反する二次利用をされる可能性がある．CGM 上のコンテンツに対する著作権保護技術として CC(Creative commons)，Rights Manager などが挙げられるが，これらはコンテンツが二次利用される際にコンテンツ全体に対する編集の可否のみの制御が可能である．加えて，CC はコンテンツの二次利用に関する許諾をライセンスマークで表示するが，それを保証する技術的な手段を持たない。さらに，柔軟性のあるコンテンツ保護をするために，我々は以下のような著作権保護技術を提案する．

- CC ライセンスで表現した編集許諾を技術的に保証する手段を与える．
- CC ライセンスで表現できないコンテンツに関する二次利用の際のより詳細な編集許諾を事前に設定可能にする．
- コンテンツを二次利用する著作者は，著作者の ID によって署名を検証でき，自らも ID によって設定した部分コンテンツに対する権利を主張できる．

上記に対して，2 番目の要件のみを実現する著作権保護技術が提案されている[4]．これにより，一つのコンテンツ内における部分コンテンツの変更・追加・削除に関する制御と，他コンテンツ間における部分コンテンツの流用制御とコンテンツ間の合成制御が可能となった．しかし，[4]に示された著作権保護技術は電子署名として BLS 署名が用いているため,その検証には公開鍵証明書が必要となる．コンテンツ作成者が多数存在する CGM サービスにおいては公開鍵証明書の必要ない ID ベース署名が適している．そこで，本稿ではこれまで実現された編集制御を ID ベース署名に基づいて構成することにより 3 番目の要件を実現する．さらに，[4]ではオリジナルコンテンツの著作者が編集可とした部分コンテンツは，それを二次利用する著作者により編集禁止へ変更が可能であった．すなわち，編集は許諾するが設定状態の変更を認めないという制御は行われていなかった．CC ライセンスでは編集を許可するが，その状態変更を認めないという設定が存在する．そこで，本

†1 東京理科大学
Tokyo University of Science
†2 東京電機大学
Tokyo Denki University

稿ではオリジナルコンテンツの著作者が設定した編集可の条件を, 二次利用後のコンテンツに引き継ぐ制御も実現し, CC ライセンスで設定した編集許諾を技術的に実現する, すなわち 1 番目の要件を実現する.

本稿の構成として, 2 章では本方式の編集を制御に用いる署名方式として ID ベース署名に基づく集約署名について説明し, 3 章では提案方式の概要について説明する. また, 4 章からは提案方式のアルゴリズムについて説明し, 5 章ではその安全性と実用性について説明し, 6 章をまとめとする.

2. ID ベース署名に基づく集約署名

楕円曲線上において双線形性の特徴を持つペアリングと呼ばれる関数を利用する ID ベース署名[6]が実現可能であることが示された. この ID ベース署名を基にした ID ベース集約署名が提案されている[7]. これは, 署名サイズが一定のまま 2 つ以上の署名を 1 つの署名へと集約することが可能である. 本節ではその方式について説明する.

ここで, $L = \{u_{i_1}, \cdots, u_{i_t}\}$を集約署名に参加する署名者の集合, $J = \{i_1, \cdots, i_t\}$を集約署名に参加する署名者のシンボルの集合とすると, 集約署名は以下のように構成される.

2.1 準備

生成元 $g \in \mathbb{G}_1$ と $s \in Z_p$ から秘密鍵発行センターは $g_{pub} = sg$を計算し, sをマスター秘密鍵とする.

2.2 鍵生成

一方向性ハッシュ関数$H_1: \{0,1\}^* \to \mathbb{G}_2$を定義する. 署名者 u_jのユーザ ID 情報をID_jとした時, TA は$Q_{ID_j} = H_1(ID_j)$を計算し, $d_{ID_j} = sQ_{ID_j}$を$u_j \in L$の秘密鍵として発行する.

2.3 署名作成

一方向性ハッシュ関数$H_2: \{0,1\}^* \to \mathbb{G}_2$を定義する. m_jを署名対象となる平文とした時, 署名者は$r_j \in Z_p$を選び, $U_j = r_j g$を計算する. その後, $h_j = H_2(ID_j, m_j, U_j)$を計算し, $V_j = d_{ID_j} + r_j h_j$ を生成する. m_j に対する署名を $\sigma_j =< U_i, V_j >$とする. 署名作成後すべての署名者のV_jを集め $V = \sum V_j \ (j \in J)$を計算し, 集約署名を$\sigma =< U_{i_1}, \cdots, U_{i_t}, V >$とする.

2.4 検証

検証者に$g, g_{pub}, U_{i_1}, \cdots, U_{i_t}, V, m_{i_1}, \cdots, m_{i_t}, ID_{i_1}, \cdots, ID_{i_t}$を集め, $Q_{ID_j} = H_1(ID_j)$, $h_j = H_2(ID_j, m_j, U_j)$ を計算し, $e(g, V) = \prod e(g_{pub}, Q_{ID_j}) e(U_j, h_j) \ (j \in J)$が成り立つかを判定する.

3. 提案方式の概要

本節では提案方式の概要を示す. 提案方式のコンテンツおよび部分コンテンツの構造と編集制御方式は, 基本的に従来方式[4][5]の構成と同様である.

3.1 コンテンツの構造

各著作者は一つ以上の部分コンテンツを含むコンテンツを作成し公開する. 一つのコンテンツはコンテンツの開始位置を表すデータ(開始データ), 最低一つ以上の部分コンテンツ, そしてコンテンツの最終位置を表すデータ(最終データ)から構成される. また, 各著作者は著作者 ID を持ち, 各コンテンツにはコンテンツ ID, 各部分コンテンツには部分コンテンツ ID を設定する.

例えば, コンテンツ A_{ij} は著作者 ID_{ij} によって作成され, コンテンツ ID を IC_{ij} とする. コンテンツ A_{ij} は図 1 のように m 個の部分コンテンツ A_{ij1}～A_{ijm} から構成され, 開始データと最終データとしてそれぞれ A_{ij0}, A_{ijm+1} を持つとする. 部分コンテンツ A_{ij0}～A_{ijm+1} は部分コンテンツ ID を I_{ij0}～I_{ijm+1} を持つ.

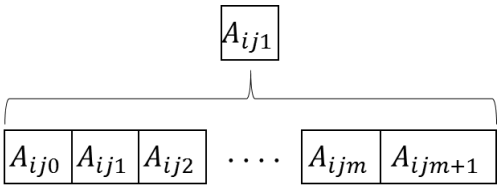

図 1　コンテンツの構造

3.2 部分コンテンツの構造

部分コンテンツは実データ空データの 2 種類のデータからなる. 実データは内容を持つ部分コンテンツであり, 実際に表示されるコンテンツの一部となる. また, 空データは追加と削除に対応できる空の部分コンテンツであり, 実際には表示されない制御データである. 開始データと最終データは共に制御データである. 図 1 において A_{ij1}～A_{ijm} の内, 実データ以外の部分は空データに設定される. また, 各データは識別子によって識別される.

部分コンテンツの先頭には図 2 のようにコンテンツ ID、オリジナルコンテンツの著作者 ID(aID)、部分コンテンツ ID、識別子、変更制御署名・削除制御署名もしくは署名用ハッシュ値と bID, 流用制御署名, 合成制御署名, オリジナルコンテンツ著作者が設定した各編集の許否設定 $p_\sigma, p_\tau, p_\chi, p_\delta$, 状態制御署名, 管理局署名など検証に必要な様々なパラメータが紐付けされている. ここで, bID は編集可を編集不可へと変更した著作者の ID である. また, 管理局署名は, コンテンツがオリジナルと認められたときにのみコンテンツ管理局(CAC)が紐付けされたデータ(部分コンテンツと aID の連結した値のハッシュ値)に対して署名したものである. 管理局の署名のない部分コンテンツは不正なコンテンツとして再生機器により検知・削除され

る仕組みにより実現される．その他の署名については次節以降で述べる．

<table>
<tr><td colspan="2">コンテンツID</td><td colspan="2">著作者 aID</td><td rowspan="9">メッセージ</td></tr>
<tr><td colspan="2">部分コンテンツID</td><td colspan="2">識別子</td></tr>
<tr><td colspan="2">変更制御署名orハッシュ値</td><td>bID</td><td>p_σ</td></tr>
<tr><td colspan="2">削除制御署名orハッシュ値</td><td>bID</td><td>p_τ</td></tr>
<tr><td colspan="3">流用制御署名</td><td>p_χ</td></tr>
<tr><td colspan="3">合成制御署名</td><td>p_δ</td></tr>
<tr><td colspan="4">状態制御署名</td></tr>
<tr><td colspan="4">管理局署名</td></tr>
<tr><td colspan="4">その他</td></tr>
</table>

図 2　部分コンテンツの構造

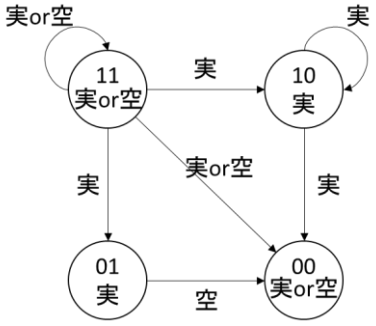

図 3　部分コンテンツの状態遷移

3.3 部分コンテンツの編集

部分コンテンツの変更・削除・追加を制御するため，変更制御署名・削除制御署名を定義する．ここで，追加は空データから実データへの変更で，削除は実データから空データへの変更であるが，削除は変更とは独立に制御する．これは，部分コンテンツの変更は許可するが削除は禁止する，削除は許可するが変更は禁止する場合に対応するためである．

部分コンテンツの変更・削除制御署名はその編集を許可する場合に公開され，禁止する場合は署名を秘匿し，署名用ハッシュ値と共に禁止に設定した著作者 ID(bID)を公開する．

コンテンツ内のすべての部分コンテンツ，開始データ，最終データそれぞれについて変更制御署名と削除集約署名を生成する．そのうち開始データと最終データの署名は秘密に保存される．また，すべての変更制御署名・削除制御署名を元に各集約署名を生成する．各集約署名はコンテンツと紐付けされ公開される．各集約署名のないコンテンツは不正コンテンツとする．

各部分コンテンツの状態は図 3 に示すように 4 状態で表すことが可能である。図 3 では変更可・削除可を(11)，変更可・削除不可を(10)，変更不可・削除可を(01)，変更不可・削除不可を(00)で表しており，その下の状態を表す「実」，「空」はそれぞれ実データと空データを表している．また，遷移を表す「実」，「空」はそれぞれ実データへの変更と空データへの変更を表す．これらの状態遷移により部分コンテンツの状態を制御可能である．ここで，空データは実データのみに変更可能であるが，置き換え後の実データは変更・削除の可否を新たに設定する必要がある．そのため，空データは変更可・削除可と変更不可・削除不可の二種類の状態が設定可能である．

3.4 部分コンテンツの流用

部分コンテンツは，他のコンテンツの一部として使用することも可能である．これを流用と呼び，流用を制御するために流用制御署名を定義する．部分コンテンツの流用を許可する場合，流用制御署名を公開する．

オリジナルコンテンツは 1 つの ID を持つため，各部分コンテンツの流用制御署名は同じコンテンツ ID を含んでいる．そこで流用の検知はコンテンツ ID の整合性により行う．しかし，部分コンテンツを流用して作成したコンテンツは，異なるコンテンツ ID を持つ部分コンテンツにより構成される．そのため，コンテンツ内の部分コンテンツがオリジナルコンテンツ ID かどうかを検証する必要がある．そこで，オリジナルコンテンツ著作者は流用を許可する部分コンテンツのコンテンツ ID を定数 0 に設定する．これにより，コンテンツ内のすべての部分コンテンツはオリジナルコンテンツ ID もしくは定数 0 を持つことになる．

流用制御署名は aID の鍵で検証されるため，aID のみが流用制御署名を設定可能であり，編集制御署名とは異なり，部分コンテンツを流用した著作者は署名を変更できない．一方流用されたコンテンツの編集制御は前節により可能である．しかし，部分コンテンツが流用不可のとき，部分コンテンツを編集する場合，署名内のコンテンツ ID を変えずに編集する必要がある．

3.5 コンテンツの合成

複数のコンテンツを順序付けて並べ一つのコンテンツとすることをコンテンツの合成と呼び，合成によって生成されたコンテンツを合成コンテンツと呼ぶ．合成コンテンツは，構造データ(コンテンツの繋がりを表す制御データ)と合成コンテンツを構成している複数のコンテンツから成る．

コンテンツの合成を制御するため，合成制御署名を定義する．合成制御署名はすべての部分コンテンツに持たせ，集約署名を生成する．コンテンツの合成を許可する場合，部分コンテンツのすべての合成制御署名を公開する．

また，二つのコンテンツ同士を合成後に他のコンテンツの合成を禁止することが可能である．このとき，合成に用

いたコンテンツからそれぞれ最低一つ以上の部分コンテンツを編集し，合成制御署名を更新する必要がある．更新後の合成制御署名は秘匿し，合成集約署名のみを公開する．各制御用署名は独立して設定されるため，合成コンテンツの部分コンテンツは 4.2 により編集可能である。しかし，合成制御署名は部分コンテンツが編集されたときに再び生成しなくてはならない．

一方，このように合成可を合成不可に変更せず単純にコンテンツ同士を合成する場合は，著作者は構造データを変更するだけでよい．以上がこれまでに提案されている．

3.6 編集条件の保持

従来方式では，二次利用者が編集の可否を前の著作者の許可の範囲(禁止を許可へ変更できない)を超えずに変更可能である．しかし，CC ライセンスの Share Alike のようにオリジナルコンテンツの著作者が編集制御とは別にコンテンツの設定を変更して欲しくない場合がある．そこで，このような編集条件の保持のため状態制御署名を導入する．状態制御署名はオリジナルコンテンツの編集許否の設定値$(p_\sigma, p_\tau, p_\chi, p_\delta)$を元にそれぞれ編集毎に作成され，すべての部分コンテンツに持たせる．また，集約署名を生成する．各部分コンテンツの状態制御署名は秘匿し，状態集約署名は必ずオリジナルコンテンツの著作者 aID の鍵により検証される．状態集約署名のないコンテンツは不正コンテンツとする．また，他の既存方式と同様に部分コンテンツの先頭に紐付けされている．

4. ID ベース署名に基づくコンテンツ編集制御システム

本章では提案方式の具体的なアルゴリズムについて示す．

4.1 オリジナルコンテンツ作成時

4.1.1 準備・鍵生成

$g \in G_1$を生成元とし，乱数$s \in Z_p^*$を選択し，ID_{ij}と bit 列$b_{ij} \in \{0,1\}$を元に公開鍵$Q_{ij} = H_1(ID_{ij}, b_{ij})$を計算し，$d_{ij} = sQ_{ij} = sH_1(ID_{ij}, b_{ij})$を発行する．$d_{ij}$を$ID_{ij}$の秘密鍵とする．また、$g_{pub} = sg$を公開する．

4.1.2 署名生成

著作者ID_{ij}は部分コンテンツの変更・削除・流用の可否，コンテンツの合成の可否，そして作成する部分コンテンツのID(ここではI_{ij1}~I_{ijk}~I_{ijm}とする)を定め，以下を行う．

(1)コンテンツの先頭及び最後につける制御データ$A_{ij0}{}^*$，$A_{ijm+1}{}^*$を作成する．また，それに対する署名α_{ij}, β_{ij}を変更・削除・流用それぞれについて作成する．ここでr_{ij}は著作者ID_{ij}が生成した乱数である．

$$\begin{cases} A_{ij0}{}^* = IC_{ij} \parallel I_{ij0} \parallel d \\ A_{ijm+1}{}^* = IC_{ij} \parallel I_{ijm+1} \parallel d \end{cases}$$

$$\begin{cases} \alpha_{ij} = r_{ij} H(IC_{ij} \parallel I_{ij0} \parallel H(A_{ij0}{}^*) \parallel r) \\ \beta_{ij} = r_{ij} H(IC_{ij} \parallel I_{ijm+1} \parallel H(A_{ijm+1}{}^*) \parallel r) \end{cases}$$

(2)部分コンテンツA_{ijk}(空データの場合d)元に，制御データ$A_{ijk}{}^*$を作成する．

$$A_{ijk}{}^* = IC_{ij} \parallel I_{ijk} \parallel A_{ijk}$$

(3)編集毎に異なる定数p,rを元にハッシュ値を生成する．編集を許可する場合p=1，許可しない場合p=0とする．

$$h_{ijk} = H(IC_{ij} \parallel I_{ijk} \parallel H(A_{ijk}{}^*) \parallel p \parallel r)$$

(4)部分コンテンツ毎に編集制御署名を以下のように作成する．

変更制御署名: $\sigma_{ijk} = r_{ij} h_{ijk}$
削除制御署名: $\tau_{ijk} = r_{ij} h_{ijk}$
流用制御署名: $\chi_{ijk} = r_{ij} h_{ijk}$
合成制御署名: $\delta_{ijk} = r_{ij} h_{ijk}$

(5)編集(変更・削除・流用・合成)の許否を示す設定値p_x $(p_\sigma, p_\tau, p_\chi, p_\delta)$を用いてハッシュ値を生成し，状態制御署名を作成する．編集許否の変更を許可する場合p=1，許可しない場合p=0とする．状態制御署名は各編集について作成する．

$$h_{ijk} = H(IC_{ij} \parallel I_{ijk} \parallel H(A_{ijk}{}^*) \parallel p \parallel p_x \parallel r)$$

状態制御署名: $\omega_{ijk} = r_{ij} h_{ijk}$

(6)コンテンツに対する署名を作成する．

変更集約署名: $\sigma_{ij} = (\alpha_{ij} + \sum \sigma_{ijk} + \beta_{ij}) + d_{ij},\ U_{ij} = r_{ij} g$
削除集約署名: $\tau_{ij} = (\alpha_{ij} + \sum \tau_{ijk} + \beta_{ij}) + d_{ij},\ U_{ij} = r_{ij} g$
流用集約署名: $\chi_{ij} = (\alpha_{ij} + \sum \chi_{ijk} + \beta_{ij}) + d_{ij},\ U_{ij} = r_{ij} g$
合成集約署名: $\delta_{ij} = (\alpha_{ij} + \sum \delta_{ijk} + \beta_{ij}) + d_{ij},\ U_{ij} = r_{ij} g$
状態集約署名: $\omega_{ij} = (\alpha_{ij} + \sum \omega_{ijk} + \beta_{ij}) + d_{ij},\ U_{ij} = r_{ij} g$

状態制御署名は各編集(変更・削除・流用・合成)について部分コンテンツに付加する．また，部分コンテンツは，図 2 のように検証に必要な各種のパラメータ(各アグリゲート署名，編集を許可する場合は編集制御署名，許可しない場合は(4)のハッシュ値と許可しないと設定した著作者 bID=aID)と紐付されている．

4.2 部分コンテンツの編集および流用

著作者 ID_{ab} が，コンテンツ A_{ij} の部分コンテンツ A_{ijk} を編集(変更・削除・追加・流用)し，コンテンツ A_{abk} とする場合を考える．著作者 ID_{ab} は以下の手順でコンテンツを編集する．

(1)コンテンツ A_{ij} の署名が検証成功であることを確認する(4.4 節)．そうでない場合は処理を停止する．

(2)流用が許可されている場合，著作者 ID_{ab} は部分コンテンツを流用できる．

(3)変更・削除・追加が許可されている場合，著作者 ID_{ab} は A_{ijk} を A_{abk} に変更可能である．また，編集の可否を前の著作者の許可の範囲内で変更可能である．ただし，状態制御署名により編集の可否の変更が許可されていない場合は不可とする．

(4)著作者 ID_{ab} は編集後のコンテンツの制御データ $A_{abk}{}^*$を生成し，編集毎に異なる定数 p(図 3 の状態遷移に従う),r を元にハッシュ値を生成する．また，流用が許可されていない場合 IC_{ij} は同じものを使用する．流用が許可されている場合 IC_{ij}=0 とする．

$$A_{abk}{}^* = IC_{ij} \parallel I_{ijk} \parallel A_{abk}$$

$$h_{abk} = H(IC_{ij} \parallel I_{ijk} \parallel H(A_{abk}{}^*) \parallel p \parallel r)$$

(5)著作者 ID_{ab} は A_{abk} の編集制御署名$\sigma_{abk},\tau_{abk},\chi_{abk}$を 4.1 節(4)と同じプロセスで作成し，各集約署名を以下のように更新する．例えば，変更を行ってコンテンツ ID の変更がない場合は変更集約署名の更新のみを行う．ただし，編集の可否を変更しない場合は集約署名の更新は公開されている前の著作者の編集制御署名を用いる．

変更集約署名: $\sigma_{ij} = \sigma_{ij} - \sigma_{ijk} + \sigma_{abk} + d_{ab}$

削除集約署名: $\tau_{ij} = \tau_{ij} - \tau_{ijk} + \tau_{abk} + d_{ab}$

流用集約署名: $\chi_{ij} = \chi_{ij} - \chi_{ijk} + \chi_{abk} + d_{ab}$

編集された部分コンテンツは図 2 のように検証に必要な各パラメータと紐付けされている．

4.3 コンテンツの合成

著作者 ID_{ic} がコンテンツ A_{ia} と A_{ib} を合成する場合を考える．著作者 ID_{ic} は以下の手順でコンテンツ合成を行う．

(1) 著作者 ID_{ic} はコンテンツ A_{ia} と A_{ib} の署名が検証成功であることを確認する(4.4 節).

(2) A_{ia} と A_{ib} が共に合成が許可されている場合，著作者 ID_{ic} はこれらを合成できる．その際，A_{ia} と A_{ib} の合成順序を記録する．

(3)著作者 ID_{ic} が合成後の A_{ia} と A_{ib} の間の合成制御の可否を変更したい場合，A_{ia} と A_{ib} それぞれの部分コンテンツは最低一つ以上編集し，以下のように A_{ia} と A_{ib} の集約署名を更新する．ここで$\delta_{iat},\delta_{ibt}$と$\delta'_{iat},\delta'_{ibt}$はそれぞれ編集前の部分コンテンツの合成制御署名と編集後の部分コンテンツの合成制御署名を表している．ただし，状態制御署名により合成の可否の変更が許可されていない場合は不可とする．

合成集約署名(A_{ia}): $\delta_{ia} = \delta_{ia} - \delta_{iat} + \delta'_{iat} + d_{ic}$

合成集約署名(A_{ib}): $\delta_{ib} = \delta_{ib} - \delta_{ibt} + \delta'_{ibt} + d_{ic}$

以上の編集及び合成は繰り返し行うことが可能である．

4.4 署名検証

コンテンツの署名検証は, コンテンツ利用時に行われる．

(1)始めに各部分コンテンツの管理局署名が正当かを検証する．

(2)合成コンテンツの場合は，構造データを参照し合成コンテンツを各コンテンツに分離する．構造データとコンテンツの構造が一致しない場合不正合成とする．

(3)検証者は各コンテンツの部分コンテンツが正しいコンテンツ ID(コンテンツ ID が 0 の時を除いて統一されている)を持っているかどうかを確認する．

(4)以上が正しく検証できた場合，検証者は各コンテンツが正しく合成されているか aID の公開鍵Q_{aID}(合成の可否が変更されている場合は加えて公開鍵Q_{bID})を用いて以下のように検証する．

$$e(g,\delta_{ij}) = \prod e(U_{ij},h_{ijk})e(g_{pub},Q_{ij})$$

(5)合成の検証後，検証者は各コンテンツが正しく流用されているか aID の公開鍵Q_{aID}(流用の可否が変更されている場合は加えて公開鍵Q_{bID})を用いて以下のように検証する．

$$e(g,\chi_{ij}) = \prod e(U_{ij},h_{ijk})e(g_{pub},Q_{ij})$$

(6)検証者はコンテンツが正しく編集(合成・削除・追加)されているか検証する．初めに，空データが変更可・削除可もしくは変更不可・削除不可の状態であるかを確認し，検証者は各編集におけるハッシュ値を生成する．実データが変更制御署名を持たない場合，検証者は生成されたハッシュ値と変更用ハッシュ値が等しいかを検証する．空データが削除制御署名を持たない場合，検証者は生成されたハッシュ値と削除用ハッシュ値が等しいかを検証する．検証者は aID の公開鍵Q_{aID}(変更・削除の可否が変更されている場合は加えて公開鍵Q_{bID}), 生成した部分コンテンツのハッシュ値，署名のない部分コンテンツに付けられたハッシュ値を集め以下の公式が成り立つか検証する．

$$e(g,\sigma_{ij}) = \prod e(U_{ij},h_{ijk})e(g_{pub},Q_{ij})$$

$$e(g,\tau_{ij}) = \prod e(U_{ij},h_{ijk})e(g_{pub},Q_{ij})$$

(7)以上が正しく検証できた場合，各部分コンテンツの状態制御署名を$p_\sigma,p_\tau,p_\chi,p_\delta$の値を元に生成したハッシュ値と aID の公開鍵$Q_{aID}$を用いて以下の式により検証する．正しく検証された場合，p=0(編集の許可を禁止できない)となった部分コンテンツの編集(変更・削除・流用・合成)が許可されているかをそれぞれ検証する．

$$e(g,\omega_{ij}) = \prod e(U_{ij},h_{ijk})e(g_{pub},Q_{ij})$$

以上が正しく検証されたものが正当なコンテンツとして，視聴および二次利用が可能である．

5. 安全性

本方式は信頼できる CAC と再生機器により実現可能である．提案方式の編集制御に用いる署名の安全性は ID ベース署名[6]，ID ベース署名に基づく集約署名[7]の安全性に基づく．

提案方式は，これらの署名方式を用いることでコンテンツの編集制御を行うものである．そのため，提案する編集制御に関して編集違反があった場合にそれを検出できるか，署名の不正編集ができないか重要である．そのため，以下のような項目について考察する．

5.1 部分コンテンツの著作権について

CAC がオリジナルコンテンツのみに管理局署名をつけることで保障される．そのため，部分コンテンツの著作者を偽ることはできない.

5.2 コンテンツの著作権について

コンテンツ ID を統一することで保障される．流用された部分コンテンツはコンテンツ ID が 0 に設定されているため，コンテンツ ID は統一する．また，流用制御署名はコンテンツ ID を元に aID により作成されるため，不正にコンテンツ ID を変えると流用集約署名の検証に失敗する．そのため，コンテンツ ID を不正に変更することができない.

5.3 変更・削除・追加制御の安全性

変更・削除・追加は各部分コンテンツの aID の鍵(変更を禁止した著作者がいる場合 bID を同時に)使用し検証することで制御できる．その上で以下のような状況が考えられる．

5.3.1 変更不可の実データA_{ijk}を実データA_{abk}へ変更した場合

それぞれ実データのハッシュ値は以下のように異なる．

実データA_{ijk}のハッシュ値：

$$h_{ijk} = H(IC_{ij} \| I_{ijk} \| H(A_{ijk}{}^{*}) \| 0 \| r)$$

実データA_{abk}のハッシュ値：

$$h_{abk} = H(IC_{ij} \| I_{ijk} \| H(A_{abk}{}^{*}) \| 0 \| r)$$

そのため，攻撃者が実データA_{ijk}に紐付けられたハッシュ値h_{ijk}と bID の値を不正に変更したとしても，変更集約署名の検証において整合性の不一検出が可能である．また，実データA_{ijk}の変更制御署名は p=0 となっているため，攻撃者は p=1 である変更制御署名を作成できない．また，ハッシュ値は編集毎に異なるため，実データA_{ijk}の他の編集制御署名のハッシュ値を利用することも不可である．そのため，変更集約署名の更新を行うことができず，不正を行うことができない．

5.3.2 変更不可の空データを実データA_{abk}に変更した場合

5.3.1 項において実データA_{ijk}を空データとして考えると同様に安全性が保障される．

5.3.3 削除不可の実データA_{ijk}を削除する場合

5.3.1 項において変更後の実データA_{abk}を空データとし，変更制御署名を削除制御署名，変更集約署名を削除集約署名として考えると同様に安全性が保障される．

また，コンテンツを正しく編集(変更・削除・追加)したとしても，図 3 に含まれない状態を設定された部分コンテンツは不正コンテンツとなる．

5.4 流用制御の安全性

流用は各部分コンテンツの aID の鍵を使用し検証することで制御できる．そのため流用が禁止された部分コンテンツを流用しようとすると，部分コンテンツの流用制御署名は p=0 となっているため，攻撃者は p=1 である流用制御署名を作成できない．また，ハッシュ値は編集毎に異なるため，実データA_{ijk}の他の編集制御署名のハッシュ値を利用することも不可である．そのため，流用集約署名の更新を行うことができず，不正を行うことができない．すなわち流用集約署名の検証において整合性が一致しないため検出が可能である．

5.5 合成制御の安全性

合成不可のコンテンツを不正合成した場合，合成集約署名の検証の際に，部分コンテンツに紐付けられている合成禁止(p=0)と設定した著作者 aID と一致しない．攻撃者が aID を変更した場合には合成集約署名の検証に失敗するため検出が可能となる． また，偽の構造データを作って不正合成を行った場合にも合成集約署名の検証に失敗するため検出が可能となる．

5.6 状態制御の安全性

状態制御は必ず各部分コンテンツの aID の鍵を使用し検証する．加えて，オリジナルコンテンツの編集許否の設定値$(p_\sigma, p_\tau, p_\chi, p_\delta)$を元に検証を行うため，攻撃者が設定値$(p_\sigma, p_\tau, p_\chi, p_\delta)$を改変して編集許否の変更を行った場合，状態集約署名の検証において整合性の不一致により検出が可能である．部分コンテンツの状態制御署名は秘匿されている上，p=0 となっているため署名の偽造は不可である．また，状態制御署名のついていない部分コンテンツは不正なコンテンツとして検知可能である．

6. まとめ

CGM サービスに適した著作権保護方式を提案した．本方式は ID ベース署名，ID ベース集約署名を用いることで認証局による署名者と検証鍵の紐付けが不要となった．また，二次利用する著作者がオリジナルコンテンツの著作者の許可の範囲内で編集の可否を変更ができる従来方式に加え，状態制御署名の導入することでオリジナルコンテンツ著作者は編集の可否を二次利用以降も保存することが可能となった．CC (Creative commons)で既に実現されている著作権保護技術も同時に実現が可能となった．今後は本方式の実装が課題となる．

参考文献

[1] “YouTube”. https://www.youtube.com/, (参照 2016-08-12).

[2] “CLIP”. http://www.clip-studio.com/clip_site/, (参照 2016-08-12).

[3] Inamura, M. Saito, A. Iwamura, K.. A Pre-Control System to Edit Contents with an Extended Sanitizable Signature. IEEE Transactions. 2013, vol. 133, no. 4, p. 802-815.

[4] Iwamura, K. Inamura, M. Koga, K. Kaneda, K.. Content Control Scheme to Realize Right Succession and Edit Control. IEICE Transactions. 2016, vol.J99-D, no. 5, p. 489-500.

[5] Fujimoto, T. Iwamura, K. Inamura, M.. Content Protection Scheme to Realize Edit Control Including Diversion Control and Composition Control. ICETE . 2016, p. 116-123.

[6] Xun, Y.. An Identity-Based Signature Scheme from the Weil Pairing. IEEE Communications Letters. 2003, vol. 7, no. 2, p. 76-78.

[7] Jing, X. Zhenfeng, Z. Dengguo, F.. ID-Based Aggregate Signatures from Bilinear Pairing. CANS, 2005, vol. LNCS3810, p. 110-119.