研究速報

低演算量鍵生成手法を用いたマルチメディアコンテンツの多重階層型アクセス制御方式

Multiple Level Access Control Method for Hierarchical Multimedia Content Using Low-complexity Key Generating Schemes

正会員　今泉祥子[†]，正会員　藤吉正明[††]，正会員　貴家仁志[††]

Shoko Imaizumi[†], Masaaki Fujiyoshi[††] and Hitoshi Kiya[††]

Abstract　We propose an efficient method of access control for hierarchical multimedia content. The proposed method simultaneously controls access to each medium contained in multimedia content and to each entity which is hierarchically organized in an individual medium. Even though this method achieves such fine control, it does not increase the computational complexity for key derivation. In our method, a service provider manages only a single key to control access to one multimedia content regardless of the number of media and the depth of hierarchy in each medium. The single managed key is not delivered to any user.

キーワード：鍵生成　ハッシュ連鎖　巡回シフト　マルチメディア　階層構造

1. ま え が き

通信路や再生端末の多様化に伴い，コンテンツ配信サービスでは，ある権利を有するユーザに対して，その権利に応じた品質でコンテンツを提供することが求められている．この要求に対応するため，コンテンツの品質は階層化され，階層ごとに暗号化される．本論文では，マルチメディアコンテンツを構成する複数のメディア，および，各メディアの品質尺度を対象として，同時にアクセス制御を施すための低演算量かつ高効率な暗号鍵生成法を提案する．

暗号化に基づくアクセス制御では，ハッシュ連鎖[1]を用いることにより，サービス事業者が管理する鍵（以降，管理鍵と呼ぶ）およびユーザが受信する鍵（以降，配送鍵と呼ぶ）の個数を削減する方法が検討されている[2)〜5)]．複数のメディアから構成されるマルチメディアコンテンツについて，個々のメディアの品質尺度に階層構造を設定して，アクセス制御を施すための研究が行われた[6)]．しかし，この方式[6)]は，複数ユーザが互いの鍵を共有することで，許諾されていない高品質での不正再生を企てる，結託攻撃に対して耐性をもたない．また，制御対象となるメディアの個数の増加に伴い，管理鍵および配送鍵の個数もそれぞれ増加する．この問題に対して，暗号鍵の生成に再帰型ハッシュ連鎖を用いることにより，メディアの個数に関わらず，管理鍵を1個とする暗号鍵生成方式が提案された[7)]．しかし，この方式[7)]では，マルチメディアコンテンツを構成する複数のメディアのうち，一つのメディアの品質尺度にしか階層構造を設定できない．また，再帰型ハッシュ連鎖の導入により，ハッシュ演算量が増加する．

そこで本論文では，個々のメディアに，品質尺度に基づく階層構造を設定可能な，マルチメディアコンテンツのアクセス制御方式を提案する．提案法は，結託攻撃に対して耐性を有し，管理鍵は1個のみである．さらに，巡回シフトの導入により，暗号鍵生成にかかる演算量の増加を回避している．また，従来法[2)〜7)]では，最高品質での再生を許諾されたユーザに管理鍵を配送していたのに対して，提案法では管理鍵が配送されることはない．

2. 想定する階層構造

マルチメディアコンテンツを対象としたアクセス制御において，制御対象は，画像，音声，テキストなどのメディアであり，メディアごとにアクセスの可否を制御する．本論文ではさらに，品質尺度（例えば，解像度，ビットレートなど）に基づく階層構造を各メディアに設定し，その階層に対しても，同時にアクセス制御を施すことを想定する．

2011年5月27日受付，2011年10月14日再受付，2011年12月12日採録
†千葉大学 大学院融合科学研究科
（〒263–8522 千葉県千葉市稲毛区弥生町 1–33, TEL 043-290-3450）
††首都大学東京 システムデザイン学部
（〒191–0065 東京都日野市旭ヶ丘 6–6, TEL 042-585-8454）
†Graduate School of Advanced Integration Science, Chiba University
(1–33 Yayoicho, Inage-ku, Chiba-shi, Chiba 263–8522 Japan)
††Faculty of System Design, Tokyo Metropolitan University
(6–6 Asahigaoka, Hino-shi, Tokyo 191–0065 Japan)

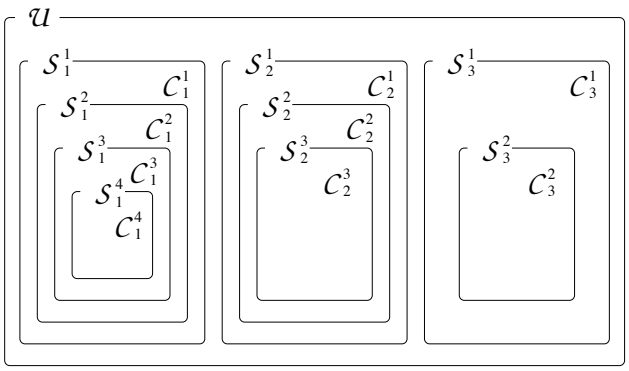


図 1 マルチメディアコンテンツ $\mathcal{U}$ の例．メディアの個数は 3 個（$X = 3$）．各メディア $\mathcal{S}_1^1$，$\mathcal{S}_2^1$，$\mathcal{S}_3^1$ の階層構造は 4 層，3 層，2 層（$N_1 = 4$，$N_2 = 3$，$N_3 = 2$）
An example of multimedia content $\mathcal{U}$. The number of media is $X = 3$ and the depths of each scalable hierarchy in media $\mathcal{S}_1^1$, $\mathcal{S}_2^1$, and $\mathcal{S}_3^1$ are $N_1 = 4$, $N_2 = 3$, and $N_3 = 2$, respectively.

X 個のメディア $\mathcal{S}_i^1$ $(i = 1, 2, \ldots, X)$ から構成されるマルチメディアコンテンツ $\mathcal{U}$ を仮定する．メディア $\mathcal{S}_i^1$ ごとに，品質尺度に基づき N_i 層の階層構造を設定する．このとき，マルチメディアコンテンツ $\mathcal{U}$ と個々のメディア $\mathcal{S}_i^1$ はそれぞれ，

$$\mathcal{U} = \{\mathcal{S}_1^1, \mathcal{S}_2^1, \ldots, \mathcal{S}_X^1\} \tag{1}$$

$$\mathcal{S}_i^1 \supset \mathcal{S}_i^2 \supset \cdots \supset \mathcal{S}_i^{N_i}, \qquad i = 1, 2, \ldots, X \tag{2}$$

と表される．上式 (1)，(2) を満たすマルチメディアコンテンツ $\mathcal{U}$ の例を**図 1** に示す．同図において，マルチメディアコンテンツ $\mathcal{U}$ は，3 個のメディア $\mathcal{S}_1^1$，$\mathcal{S}_2^1$，$\mathcal{S}_3^1$ から構成され（$X = 3$），各メディアはそれぞれの品質尺度に基づき，式 (2) を満たすような階層構造が設定されている（$N_1 = 4$，$N_2 = 3$，$N_3 = 2$）．また，図 1 の補集合 $\mathcal{C}_i^{n_i}$ の関係は次式で与えられる．

$$\mathcal{C}_i^{n_i} = \begin{cases} \mathcal{S}_i^{n_i} - \mathcal{S}_i^{n_i+1}, & n_i = 1, 2, \ldots, N_i - 1 \\ \mathcal{S}_i^{n_i}, & n_i = N_i \end{cases}$$
$$i = 1, 2, \ldots, X \tag{3}$$

ここで，図 1 におけるメディア $\mathcal{S}_1^1$ を動画像とし，階層構造がフレームレートに基づいて設定された例を用いて，上述の階層構造を補足する．**図 2** では，4 種類のフレームレート（$N_1 = 4$），15 fps（同図 (a)），30 fps （同図 (b)），60 fps （同図 (c) ）および 120 fps （同図 (d) ）を仮定している．同図において，影部フレームが再生されるフレームである．このとき，図 1 における集合 $\mathcal{S}_1^1$ は，フレームレートが最も高い 120 fps のフレーム集合である．続いて，60 fps のフレーム集合が $\mathcal{S}_1^2$，30 fps のフレーム集合が $\mathcal{S}_1^3$，15 fps のフレーム集合が $\mathcal{S}_1^4$ となる．したがって，これらの集合は，式 (2) の関係を満たしている．

また，120 fps のフレーム集合 $\mathcal{S}_1^1$ のうち，120 fps 時のみ再生されるフレームの集合が $\mathcal{C}_1^1$，60 fps のフレーム集合 $\mathcal{S}_1^2$ のうち，120 fps または 60 fps 時のみ再生されるフレームの集合が $\mathcal{C}_1^2$，30 fps のフレーム集合 $\mathcal{S}_1^3$ のうち，15 fps 時には再生されないフレームの集合が $\mathcal{C}_1^3$ となる．これらの関係は式 (3) のとおりである．なお，15 fps のフレーム集合 $\mathcal{S}_1^4$ は，式 (3) に示すとおり，$\mathcal{C}_1^4$ に等しい．このようなメディア S_1^1 に対する暗号化処理は，フレーム集合 $\mathcal{C}_1^1$，$\mathcal{C}_1^2$，$\mathcal{C}_1^3$，$\mathcal{C}_1^4$ をそれぞれ単位データとして，単位データごとに施される．

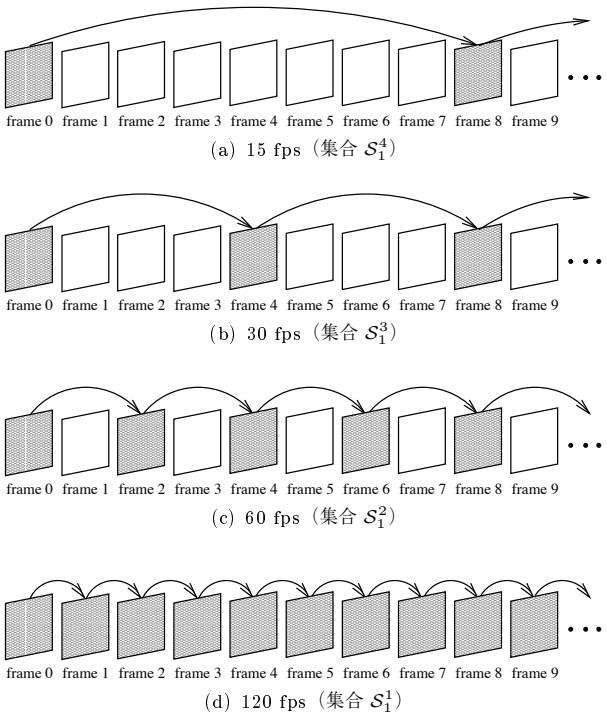


図 2 各フレームレートにおける動画像再生（影部フレームを再生）
Decoding of a video stream at each frame rate (The shaded frames are decoded).

3. 提 案 法

各メディアに，品質尺度に基づく階層構造を設定可能とする，マルチメディアコンテンツのアクセス制御方式において，管理鍵を 1 個のみとし，かつ，演算量の増加を回避する暗号鍵生成法および暗号解除鍵生成法について説明する．

図 1 のマルチメディアコンテンツについて，具体的な例を**図 3** に示す．図 3 において，全体集合 $\mathcal{U}$ は，あるマルチメディアコンテンツを示しており，動画像，音声，テキストの 3 個のメディアから構成されている（$X = 3$）．これら 3 個のメディアのうち，集合 $\mathcal{S}_1^1$ は動画像であり，図 2 に示す，120 fps（集合 $\mathcal{S}_1^1$），60 fps（集合 $\mathcal{S}_1^2$），30 fps（集合 $\mathcal{S}_1^3$），15 fps（集合 $\mathcal{S}_1^4$）のフレームレートで再生可能である．集合 $\mathcal{S}_2^1$ は音声であり，256 kbps（集合 $\mathcal{S}_2^1$），128 kbps（集合 $\mathcal{S}_2^2$），64 kbps（集合 $\mathcal{S}_2^3$）のビットレートでの再生が可能である．また，集合 $\mathcal{S}_3^1$ はテキスト情報である．テキスト情報は，会話に関する字幕全般（以降，サブタイトルと呼ぶ，集合 $\mathcal{S}_3^1$），または，会話を別の言語に

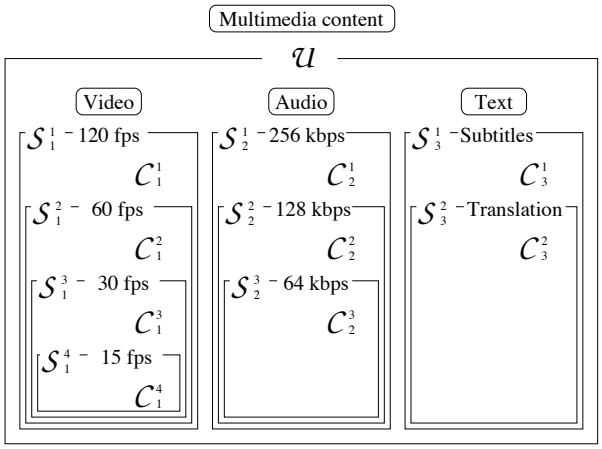


図 3 図 1 に示すマルチメディアコンテンツの具体例
A practical example of multimedia content shown in Fig. 1.

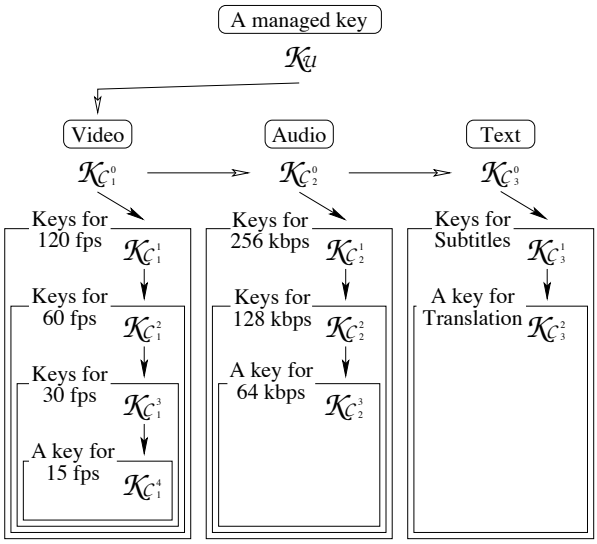


図 4 暗号鍵生成アルゴリズム．白矢印は巡回シフト，黒矢印はハッシュ連鎖
Key generating algorithm. White arrows represent cyclic shifts and black arrows represent hash chains.

翻訳した字幕のみ（以降，翻訳と呼ぶ，集合 $\mathcal{S}_3^2$）の再生が選択できる．このように，提案法は，メディアの種類だけでなく，各メディアの品質尺度に基づく階層に対しても同時にアクセス制御を実現するものである．

3.1 暗号鍵生成法

図 3 のマルチメディアコンテンツに対応した暗号鍵生成アルゴリズムを**図 4** に示す．図 4 において，例えば，$K_{\mathcal{C}_2^1}$ は図 3 に示す音声の単位データ $\mathcal{C}_2^1$ に，$K_{\mathcal{C}_3^2}$ はテキストの単位データ $\mathcal{C}_3^2$ に，それぞれ対応する暗号鍵である．ここで，$K_{\mathcal{U}}$ が提案法における唯一の管理鍵であり，いずれの単位データに対しても暗号鍵として用いられない．

まず，管理鍵 $K_{\mathcal{U}}$ に対して，左回りの 1 ビット巡回シフトを施したものを，動画像に対する初期鍵 $K_{\mathcal{C}_1^0}$ とする．次に，$K_{\mathcal{C}_1^0}$ に再度左回りの 1 ビット巡回シフトを施したものを音声に対する初期鍵 $K_{\mathcal{C}_2^0}$，さらに $K_{\mathcal{C}_2^0}$ に同様の巡回シフトを施したものを $K_{\mathcal{C}_3^0}$ とする．上述の関係は，

$$K_{\mathcal{C}_i^0} = K_{\mathcal{U}} << i, \qquad i = 1,2,3 \tag{4}$$

と表される．ここで，$a << b$ は，a に対して左回りに b ビットの巡回シフトを施すことを意味する．図 4 において，左回りの 1 ビット巡回シフトは白矢印で示されている．

これら三つのメディアの各単位データ $\mathcal{C}_i^{n_i}$ に対する暗号鍵 $K_{\mathcal{C}_i^{n_i}}$ $(n_i = 1,2,\ldots,N_i, \quad i = 1,2,3)$ は，式 (4) で生成された $K_{\mathcal{C}_i^0}$ から，一方向性ハッシュ関数 $H()$ を用いて，

$$K_{\mathcal{C}_i^{n_i}} = H^{n_i}\left(K_{\mathcal{C}_i^0}\right) = H^{n_i-1}\left(H\left(K_{\mathcal{C}_i^0}\right)\right), \quad n_i = 1,2,\ldots,N_i, \qquad i = 1,2,3 \tag{5}$$

により従属的に生成される．ここで，$H^b(a)$ は，a に対してハッシュ演算を b 回施す，ハッシュ連鎖 [1] を意味している．ハッシュ連鎖は，図 4 において，黒矢印で示されている．

このように，提案法は，巡回シフトの導入によりハッシュ演算の回数を増加させることなく，一つの管理鍵から各単位データに対する暗号鍵を生成可能である．一方，再帰型ハッシュ連鎖 [7] では，算出されたハッシュ値（ハッシュ演算の出力）を新たなハッシュ連鎖に対する入力として再度用いるため，ハッシュ演算回数が増加する．また，提案法は，あらゆる結託攻撃に対して耐性を考慮している．図 4 に示すとおり，各メディアを関連付ける暗号鍵 $K_{\mathcal{C}_1^0}$，$K_{\mathcal{C}_2^0}$，$K_{\mathcal{C}_3^0}$ は，いずれの単位データにも割り当てられず，各メディアは，見かけ上，それぞれ独立な暗号鍵で暗号化される．これにより，複数ユーザが互いの暗号鍵を共有し，組合せても，許諾されていない単位データに対する暗号鍵を生成することはできない．このように，提案法は，許諾されていないメディア，および，許諾されていない高品質での不正再生を防いでいる．なお，演算量の観点から巡回シフトを用いているが，本アルゴリズムの実現は，巡回シフトの利用に限定されるものではない．また，シフト量を一定（上述の例では，左回りに 1 ビット）とすることにより，変数の増加を回避している．

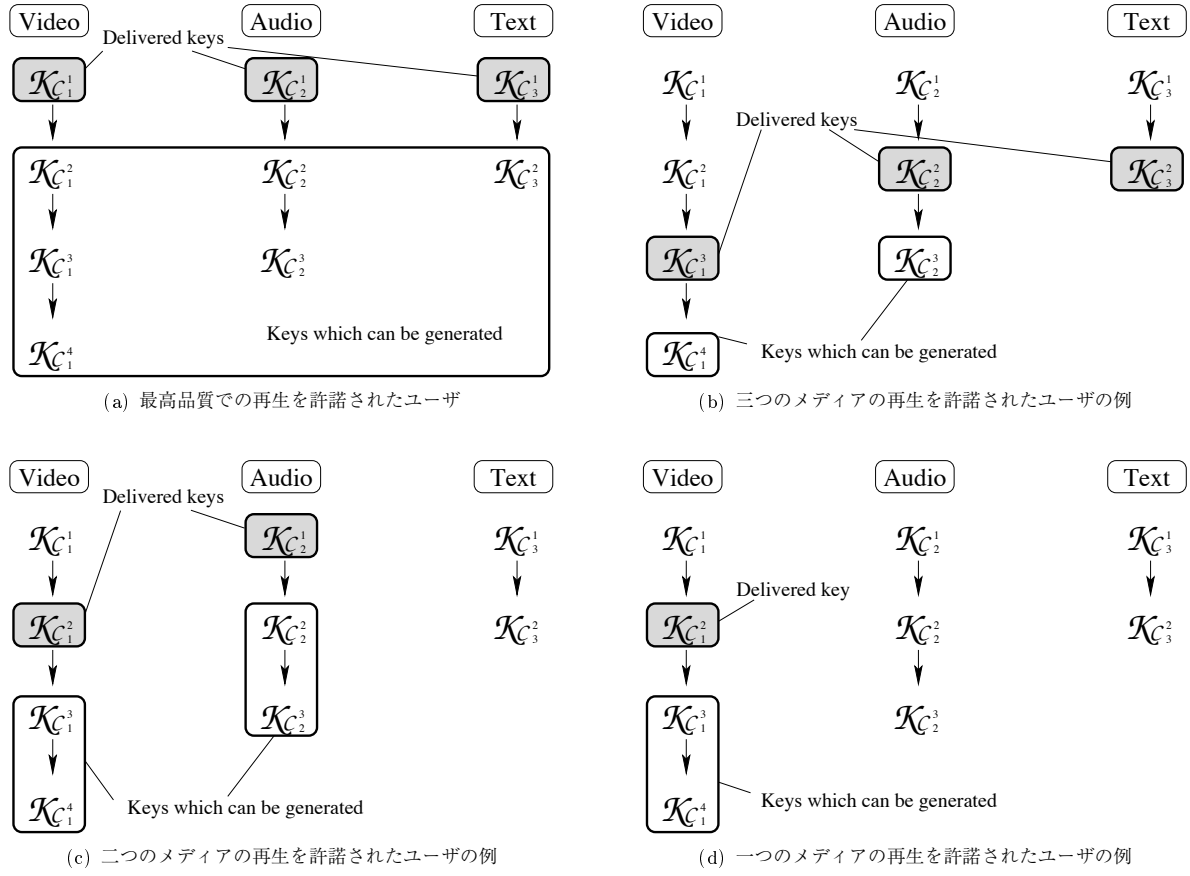
3.2 暗号解除鍵生成法

以下では，各ユーザがその許諾された品質に応じて受信する配送鍵，および，配送鍵から生成される暗号解除のための暗号鍵について，図 4 を例に説明する．

（1） 三つのメディアの再生を許諾されたユーザ

図 3 に示すマルチメディアコンテンツ $\mathcal{U}$ の三つのメディア，すなわち，動画像，音声，テキストの再生を許諾されたユーザについて説明する．

まず，最高品質での再生を許諾されたユーザは，図 3 に示すすべての単位データ $\mathcal{C}_i^{n_i}$ $(n_i = 1,2,\ldots,N_i, \quad i = 1,2,3)$ を再生することができる．このユーザは，**図 5** (a) に示すように，動画像，音声，テキストの各単位データ $\mathcal{C}_1^1$，$\mathcal{C}_2^1$，$\mathcal{C}_3^1$ に対する暗号鍵 $K_{\mathcal{C}_1^1}$，$K_{\mathcal{C}_2^1}$，$K_{\mathcal{C}_3^1}$ を配送鍵として受信する．これら 3 個の配送鍵から，式 (5) を用いて，各メディアを



(a) 最高品質での再生を許諾されたユーザ
(b) 三つのメディアの再生を許諾されたユーザの例
(c) 二つのメディアの再生を許諾されたユーザの例
(d) 一つのメディアの再生を許諾されたユーザの例

図 5 ユーザごとの配送鍵（囲線網掛部）および配送鍵から生成される暗号解除鍵（囲線部）
Delivered keys and derived keys for each user.

構成するすべての単位データに対する暗号鍵を生成する．

また，例えば，動画像を 30 fps，音声を 128 kbps，テキストを翻訳のみの品質で再生許諾されたユーザは，図 5 (b) に示すとおり，$K_{\mathcal{C}_1^3}$，$K_{\mathcal{C}_2^2}$，$K_{\mathcal{C}_3^2}$ を配送鍵として受信する．ここで，式 (5) は，

$$K_{\mathcal{C}_i^{n_i}} = H\left(K_{\mathcal{C}_i^{n_i-1}}\right)$$
$$n_i = 1, 2, \ldots, N_i, \qquad i = 1, 2, 3 \tag{6}$$

と同意である．式 (6) を用いて，配送鍵 $K_{\mathcal{C}_1^3}$ から $K_{\mathcal{C}_1^4}$ を，$K_{\mathcal{C}_2^2}$ から $K_{\mathcal{C}_2^3}$ を，それぞれ生成する．

以上の手順により，各ユーザは許諾された三つのメディアを許諾された品質で再生することが可能となる．

（2） 二つのメディアの再生を許諾されたユーザ

次に，二つのメディアの再生を許諾されたユーザについて，図 5 (c) を例に説明する．同図は，動画像を 60 fps，音声を 256 kbps の品質で再生することを許諾されたユーザの例である．このユーザは，配送鍵として，二つの暗号鍵 $K_{\mathcal{C}_1^2}$，$K_{\mathcal{C}_2^1}$ を受信する．これらの配送鍵から，式 (6) を用いて，$K_{\mathcal{C}_1^3}$，$K_{\mathcal{C}_1^4}$，$K_{\mathcal{C}_2^2}$，$K_{\mathcal{C}_2^3}$ を従属的に生成する．ただし，図 5 (c) に示すとおり，これらの暗号鍵からテキストに対する暗号鍵を生成することはできない．以上より，二つのメディアに対して再生を許諾されたユーザは，2 個の配送鍵を受け取り，許諾されたメディアを許諾された品質で再生することができる．

（3） 一つのメディアの再生を許諾されたユーザ

三つのメディアのうち，一つのみの再生を許諾されたユーザについて説明する．図 3 において，動画像のみ 60 fps での再生を許諾されたユーザは，図 5 (d) に示すとおり，$K_{\mathcal{C}_1^2}$ を配送鍵として受信する．$K_{\mathcal{C}_1^2}$ から，式 (6) により，$K_{\mathcal{C}_1^3}$，$K_{\mathcal{C}_1^4}$ を従属的に生成する．また，これらの暗号鍵 $K_{\mathcal{C}_1^{n_1}}$ $(n_1 = 2, 3, 4)$ からは，他のメディアに対するいずれの暗号鍵も生成できない．したがって，このユーザは，1 個の配送鍵のみを受け取り，60 fps 以下のフレームレートの品質で，動画像のみを再生可能となる．

このように，複数のメディアから構成され，かつ，個々のメディアに階層構造が設定されたマルチメディアコンテンツのアクセス制御において，提案法は，各ユーザへの配送鍵の個数を，再生許諾されたメディアの個数と同数にしている．

4. 評　価

提案法の有効性を示すため，階層構造を設定可能なメディア，結託攻撃耐性，ハッシュ演算回数，管理鍵・配送鍵の個数，および，管理鍵の配送について，マルチメディアコンテンツに対するアクセス制御の従来法 [6)7)] と比較することにより評価する．

表 1 提案法と従来法 [6)7)] との比較（メディア数：X）．ただし，従来法 [7)] において，階層構造が設定された唯一のメディアを $\mathcal{S}_1^1$ とし，その階層数を N_1 とする．

Comparisons of the proposed method with the conventional methods[6)7)]. Note that a medium with hierarchical structure is $\mathcal{S}_1^1$ and the depth of hierarchy in medium $\mathcal{S}_1^1$ is represented as N_1 in the conventional method[7)].

	提案法	従来法 [6)]	従来法 [7)]
階層構造の設定	複数メディア	複数メディア	単一メディア
結託攻撃耐性	有	無	有
ハッシュ演算回数	$\sum_{i=1}^{X} N_i$	$\sum_{i=1}^{X} N_i$	$N_1 + X - 1$
管理鍵の個数	1	X	1
配送鍵の個数	$1 \sim X$	X	$1 \sim X$
管理鍵の配送	無	有	有

表 1 に，それぞれの方式の特徴を示す．同表より，提案法および従来法 [6)] では，マルチメディアコンテンツの各メディアに階層構造を設定することが可能である．一方，従来法 [7)] では，一つのメディアにしか階層構造を設定できない．また，提案法および従来法 [7)] は，あらゆる結託攻撃に対して耐性を有する暗号鍵生成アルゴリズムとなっているが，従来法 [6)] では耐性が考慮されていないため，複数ユーザによる結託攻撃が可能となっている．

ハッシュ演算回数について，提案法および従来法 [6)] では，各メディアの階層数 n_i $(i = 1, 2, \ldots, X)$ の総和と同数である．一方，従来法 [7)] では，一つのメディアにのみ階層構造を設定できるという制約があるため，表 1 に示す従来法 [7)] の演算回数と他の方式の演算回数との単純な比較はできない．しかし，従来法 [7)] は再帰型ハッシュ連鎖を利用しており，ハッシュ演算回数の削減を優先した拡張を考えた場合でも，ハッシュ演算回数は，提案法より $X - 1$ 回増加する．

さらに，提案法および従来法 [7)] で必要となる管理鍵の個数は，それぞれ 1 個であるのに対して，従来法 [6)] ではメディアの個数と同数，すなわち，X 個の管理鍵が必要となる．また，配送鍵の個数について，提案法および従来法 [7)] では最小で 1 個，最大で X 個である一方，従来法 [6)] では常に X 個の配送鍵が必要となる．なお，従来法 [6)7)] では，最高品質での再生を許諾されたユーザには管理鍵を配送するが，提案法において，管理鍵はいずれのユーザにも配送されない．

以上より，従来法 [6)7)] と比較して，提案法がより有効であることがわかる．

5. むすび

本論文では，個々のメディアに対して，品質尺度に基づく階層構造が設定された，マルチメディアコンテンツのための効率的なアクセス制御方式を提案した．提案法は，メディアの個数および各メディアの階層構造に関わらず，管理鍵を 1 個のみ，配送鍵の個数についても従来法以下としている．この管理鍵は，いずれのユーザにも配送されることがない．また，提案法は，従来法と同様の結託攻撃耐性を有しており，さらに，演算量の増加が回避されるように設計されている．これらの特徴について，従来法との比較により提案法の効果を評価した．

今後の課題として，具体的な演算量の解析，および，個々のメディアにおける複数の品質尺度に階層構造が設定された場合への応用などが挙げられる．

〔文　献〕

1) L. Lamport, “Password authentication with insecure communication,” Communications of the ACM, **24**, 11, pp.770–772 (1981)
2) Y. Wu, D. Ma, and R.H. Deng, “Progressive protection of JPEG 2000 codestreams,” Proc. IEEE Int. Conf. Image Process., pp.3447–3450 (2004)
3) M. Joye and S. Yen, “One-way cross-trees and their applications,” Proc. IACR Int. Conf. Practice and Theory PKC, pp.355–358 (2002)
4) Y. G. Won, T. M. Bae, and Y. M. Ro, “Scalable protection and access control in full scalable video coding,” Proc. IWDW, pp.407–421 (2006)
5) 須賀祐治, 岩村恵市, “DAG における鍵派生方式の枝切り改良方式,” 信学 SCIS, 2C2-4 (2005)
6) M. Fujiyoshi, S. Imaizumi, and H. Kiya, “Encryption of composite multimedia contents for access control,” IEICE Trans. Fundamentals, **E90-A**, 3, pp.590–596 (2007)
7) S. Imaizumi, M. Fujiyoshi, and H. Kiya, “An efficient access control method for composite multimedia content,” IEICE ELEX, **7**, 20, pp.1534–1538 (2010)

今泉 祥子 2011 年，首都大学東京大学院システムデザイン研究科博士後期課程修了．2003 年，文部科学事務官，2005 年，新潟県工業技術総合研究所研究員．2011 年，千葉大学大学院融合科学研究科助教．画像符号化，メディア情報セキュリティの研究に従事．博士（工学）．正会員．

藤吉 正朗 2001 年，埼玉大学大学院理工学研究科博士後期課程修了．同年，東京都立大学大学院工学研究科助手．2007 年，首都大学東京システムデザイン学部助教．画像処理，メディア情報セキュリティの研究に従事．博士（学術）．正会員．

貴家 仁志 1982 年，長岡技術科学大学大学院修士課程修了．同年，東京都立大学助手．2000 年，同大教授．2005 年，首都大学東京システムデザイン学部教授．信号処理，メディア工学，情報セキュリティの研究に従事．工学博士．正会員．フェロー．