再帰型ハッシュ連鎖を用いたディジタルコンテンツのアクセス制御方式

An Access Control Method Using Recursive Hash Chains for Digital Content

今泉祥子 †,‡ Shoko IMAIZUMI　藤吉正明 ‡ Masaaki FUJIYOSHI　貴家仁志 ‡ Hitoshi KIYA

新潟県工業技術総合研究所 †
Industrial Research Institute of Niigata Prefecture
首都大学東京大学院　システムデザイン研究科 ‡
Graduate School of System Design, Tokyo Metropolitan University

1　まえがき

本稿では，鍵管理・配送の観点から効率的な暗号鍵生成法を用いた，ディジタルコンテンツのアクセス制御方式を提案する．提案法は，鍵生成に，再帰型ハッシュ連鎖を導入することで，サービス事業者が管理する鍵（管理鍵）とユーザが受信する鍵（配送鍵）の個数をいずれも 1 つとする．また，複数のユーザが互いの鍵を共有し，不正な高品質再生を企てる結託攻撃について考慮する．

2　想定するアクセス制御

ディジタルコンテンツのアクセス制御は，コンテンツ単位，解像度単位，フレーム単位など様々である．提案法は，ある 1 つの制御対象に対して階層性を設定し，複数の制御対象に対して同時にアクセス制御を施す．階層性が設定された制御対象は，図 1 に示すとおり，

$$\mathcal{A} \subset \mathcal{B} \subset \mathcal{C} \subset \mathcal{U} \tag{1}$$

の階層関係を有する必要がある．

3　再帰型ハッシュ連鎖による暗号鍵生成法

ある動画像を想定し，フレームレートに 120，60，30，15 fps（図 1 における集合 $\mathcal{U},\mathcal{C},\mathcal{B},\mathcal{A}$ に対応）の階層性を設定する．このとき，フレームレート，音声，文字に対して同時にアクセス制御を施す例を図 2 に示す．同図における鍵 $K_{\text{f\_rate }0}$ は，120 fps のみで再生されるフレーム集合 $\mathcal{C}^c$ に対する鍵であり，$K_{\text{f\_rate }0}$ が管理鍵となる．同様に，鍵 $K_{\text{f\_rate }1}$ は 15 fps，30 fps で非再生となる 60 fps の集合 $\mathcal{B}^c$，鍵 $K_{\text{f\_rate }2}$ は 15 fps で非再生の 30 fps の集合 $\mathcal{A}^c$，鍵 $K_{\text{f\_rate }3}$ は 15 fps の集合 $\mathcal{A}$ に対する鍵である．鍵 $K_{\text{f\_rate }i}$ は，管理鍵 $K_{\text{f\_rate }0}$ を初期値として，

$$K_{\text{f\_rate }i} = H^i\left(K_{\text{f\_rate }i}\right), \quad i = 1,2,3 \tag{2}$$

の単純なハッシュ連鎖（単純ハッシュ連鎖）により，図 2 の黒矢印の順に，従属的に生成される．

一方，図 2 における鍵 K_{sound}，K_{char} は，それぞれ音声，文字に対する鍵である．同図の例では，$K_{\text{f\_rate }0}$ または $K_{\text{f\_rate }1}$ を受信した，すなわち，120 fps または 60 fps での再生を許諾されたユーザは，音声に対する鍵を得ることができる．また，$K_{\text{f\_rate }0}$，$K_{\text{f\_rate }1}$ または $K_{\text{f\_rate }2}$ の鍵を受信し，30 fps 以上での再生を許諾されたユーザは，文字に対する鍵を得られる．これらの鍵 K_{sound}，K_{char} は，

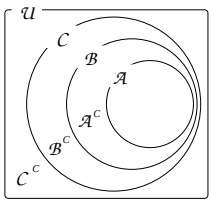

図 1　制御対象の階層条件．

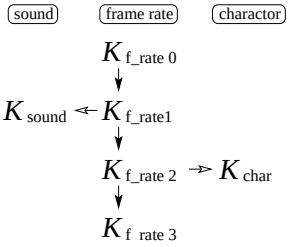

図 2　再帰型ハッシュ連鎖を用いた提案手法．

表 1　管理鍵・配送鍵の個数と結託攻撃耐性の比較．

	提案法	文献 [1]
管理鍵	1	X
配送鍵	1	1
結託攻撃耐性	有	無

$$\begin{aligned} K_{\text{sound}} &= H\left(K_{\text{f\_rate }1} \oplus K_{\text{f\_rate }2}\right) \\ &= H\left(K_{\text{f\_rate }1} \oplus H\left(K_{\text{f\_rate }1}\right)\right) \end{aligned} \tag{3}$$

$$\begin{aligned} K_{\text{char}} &= H\left(K_{\text{f\_rate }2} \oplus K_{\text{f\_rate }3}\right) \\ &= H\left(K_{\text{f\_rate }2} \oplus H\left(K_{\text{f\_rate }2}\right)\right) \end{aligned} \tag{4}$$

のとおり，算出されたハッシュ値を再度用いることで，すなわち，再帰型ハッシュ連鎖（図 2 の白矢印）を用いることで生成される．なお，本稿では，再帰型ハッシュ連鎖の実現に排他的論理和を用いている．

以上より，120 fps，60 fps を許諾されたユーザは音声・文字付，30 fps を許諾されたユーザは文字付での再生が可能となる．このとき，ユーザに対する配送鍵の個数は，いずれの場合も 1 つである．さらに，再帰型ハッシュ連鎖の導入は，鍵の削減だけでなく，結託攻撃耐性を与える．

4　評価

提案法の効果を，管理鍵・配送鍵の個数と結託攻撃耐性について，単純ハッシュ連鎖のみを用いたアクセス制御方式（文献 [1]）と比較することにより評価する．1 つのコンテンツに対する制御対象の個数を X 個とした場合について比較した結果を表 1 に示す．ここで，図 2 では，制御対象がフレームレート，音声，文字であることから $X = 3$ となる．同表より，提案法の有効性が示された．

5　あとがき

本稿では，再帰型ハッシュ連鎖による効率的な暗号鍵生成法を用いたディジタルコンテンツのアクセス制御方式を提案した．提案法は，管理鍵・配送鍵の個数をいずれもただ 1 つとし，かつ，結託攻撃耐性を有する．

今後の課題として，認証技術や電子透かしへの応用を検討する．

参考文献

[1] M. Fujiyoshi, S. Imaizumi, and H. Kiya: “Encryption of composite multimedia contents for access control,” IEICE Trans. Fundamentals, E90-A, 3, 2007.