All rights are reserved and copyright of this manuscript belongs to the authors. This manuscript has been published without reviewing and editing as received from the authors: posting the manuscript to SCIS 2010 does not prevent future submissions to any journals or conferences with proceedings.

SCIS 2010 The 2010 Symposium on Cryptography and Information Security
Takamatsu, Japan, Jan. 19-22, 2010
The Institute of Electronics, Information and Communication Engineers

ディジタル動画像配信サービスにおけるアクセス制御方式
An Access Control Method for Digital Video Distribution

今泉 祥子 * 阿部 淑人 * 藤吉 正明 † 貴家 仁志 †
Shoko IMAIZUMI Yoshito ABE Masaaki FUJIYOSHI Hitoshi KIYA

あらまし 本稿では，ネットワークを介したディジタル動画像の有料配信サービスにおいて，著作権や未成年ユーザの保護を目的としたアクセス制御方式を提案している．提案法は，ユーザが視聴を許諾された品質，または，年齢に応じた 1 つの鍵を，ただ 1 つの管理鍵（マスターキー）から従属的に生成し，ユーザに配送する．また，異なる品質，年齢での再生を許諾された他のユーザに対しても，同様にマスターキーから従属的に生成された異なる 1 つの鍵を配送する．これによって，課金に応じた品質で画像を配信する動画像の有料配信において，品質に応じたアクセス制御が可能となる．また，映画のレイティングシステムを始め，視聴可能年齢が制限された動画像コンテンツに対応したアクセス制御が可能となっている．さらに，提案法では，複数ユーザが不正に鍵を共有することにより，許諾された品質，または，コンテンツ範囲以上の再生を企てる結託攻撃に対しても検討されており，結託攻撃が不可能であることが示されている．

キーワード 動画像　アクセス制御　鍵生成　ハッシュ関数　著作権保護　レイティングシステム

1 まえがき

ネットワークを介した情報通信の一般化によるディジタル画像通信の増加に伴い，画像の保護に関して様々な研究がなされている [1–12]．本稿では，ディジタル動画像 [13–15] を対象に，効率的な暗号鍵生成方法を用いたアクセス制御方式を提案する．

近年，通信路や通信端末の多様化により，異なった品質での画像再生が求められている．例えば，テレビジョン放送におけるフレームレートは，ワンセグ放送で 15 fps，高精細度テレビジョン放送で 30 fps，60 fps などのように多様である．有料配信の場合，課金の額は再生されるコンテンツの品質ごとに異なるため，フレームレートを考慮したアクセス制御が要求される．

また，映画のレイティングシステムに代表されるように，コンテンツにはその視聴に年齢制限がかけられる作品も多くなっている．例えば，日本の映画では，あらゆる年齢層が鑑賞できる G，12 歳未満の鑑賞には保護者の助言・指導が適当とされる PG12，15 歳未満は鑑賞禁止である R-15，および，18 歳未満は鑑賞禁止である R-18 の 4 つに区分される．有料配信サービスには，レイティングシステムに対応するアクセス制御も要求される．

著者らは，これまで JPEG 2000 (以降 JP2 と略) [16,17] で符号化された静止画像に対するアクセス制御の研究を行なってきた [10–12]．これらの研究は，JP2 の特長であるスケーラビリティを考慮し，SNR，解像度，色数に関して，ユーザが許諾された品質でのみ再生するためにアクセス制御を行なうものである．これらの特長は，種々の冗長性を排除した点にあり，1 つの静止画像へのアクセス制御において，必要な符号化列はただ 1 つ，管理鍵（マスターキー）は制御対象となるスケーラビリティ数に寄るが，対象が 2 つの場合は小さい方のスケーラビリティの階層数と同数まで低減されている．また，複数のユーザがそれぞれの鍵を不正に共有して，許諾された品質より高い品質で再生することを企てる結託攻撃についても十分な耐性を有する．

本稿では，制御対象が 1 つの場合に有効な，JP2 符号化画像に対するアクセス制御法 [8] の特長を保持したまま，動画像に拡張した手法を提案する．提案法は，1 つの動画像コンテンツに対して，1 つのシーケンスと 1 つのマスターキーとで，様々なフレームレートでの再生を可能とするアクセス制御を可能とする．また，動画像コンテンツのレイティングシステムに基づくアクセス制御についても同様に，1 つのマスターキーで実現する．さ

* 新潟県工業技術総合研究所，〒 950–0915 新潟県新潟市中央区鐙西 1–11–1, Industrial Research Institute of Niigata Prefecture, 1–11–1 Abumi-nishi, Chuo-ku, Niigata-shi, Niigata 950–0915 Japan, shoko.imaizumi@m.ieice.org
† 首都大学東京システムデザイン学部情報通信システムコース，〒 191–0065 東京都日野市旭ヶ丘 6–6, Department of Information and Communication Systems, Tokyo Metropolitan University, 6–6 Asahigaoka, Hino-shi, Tokyo 191–0065 Japan

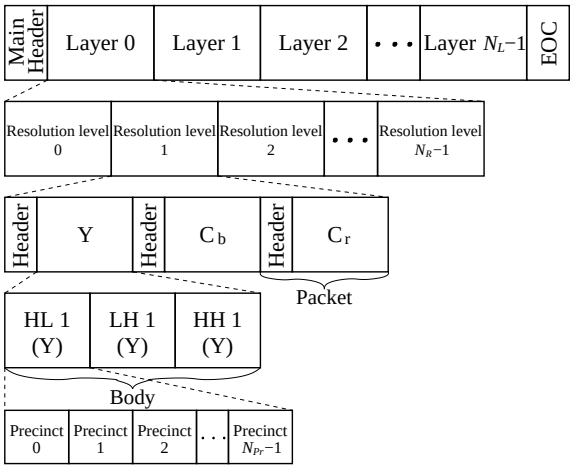


図 1: カラー画像に対する JP2 符号化列の構成例（プログレッション順序：LRCP）.

らに，提案法では，上述した結託攻撃が不可能である．

2 JP2 符号化画像のアクセス制御

本節では，提案法の基礎となる JP2 符号化画像のアクセス制御法 [8] の説明ため，JP2 符号化列の構成とその階層性を要約し，この文献 [8] におけるアクセス制御方式を述べる．

2.1 JP2 符号化列の概要

JP2 では，複数あるスケーラビリティの種類に対して優先順位を与える．この優先順位は，符号化列中のデータ単位である JP2 パケットの構成順序，すなわちプログレッション順序として表現される [16]．パケットの構成順序を決定するのは，レイヤ (L)，解像度レベル (R)，コンポーネント (C)，プレシンクト (P) の 4 つのスケーラビリティである．プログレッション順序には，LRCP，RLCP，RPCL，PCRL，CPRL の 5 種類があり，それぞれ先頭の要素から順に優先される．

図 1 は，原画像がカラー画像の場合に，プログレッション順序に LRCP を選択し，色表現として YC_bC_r を使用した JP2 符号化列の例である．同図において，N_L，N_R はレイヤおよび解像度レベルの階層数を，N_{Pr} はプレシンクトの数をそれぞれ示している．符号化列はまず，レイヤスケーラビリティに沿って，SNR の低いレイヤから順に構成される．各レイヤは解像度レベルの情報を有しており，解像度レベルの情報には色コンポーネントの情報が含まれる．カラー画像の場合，個々の色コンポーネントが JP2 パケットとなる．さらに，各色コンポーネントは HL など離散ウェーブレット変換のサブバンドの情報を有し，各サブバンドはプレシンクトから構成される．なお，プレシンクトは非階層的スケーラビリティである．

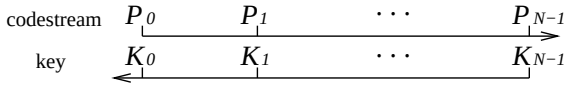


図 2: 文献 [8] におけるアクセス制御.

2.2 JP2 符号化画像に対するアクセス制御法 [8]

ここで，JP2 符号化画像のアクセス制御法の 1 つである文献 [8] の手法について説明する．文献 [8] は，制御対象が 1 つの場合に有効な手法である．

2.2.1 JP2 符号化列の暗号化

文献 [8] の手法は，JP2 パケット単位に暗号処理を施す．ある JP2 符号化列のパケット数を N とし，各パケットを P_i $(i = 0,1,\ldots,N-1)$，各パケットに対する暗号鍵を K_i $(i = 0,1,\ldots,N-1)$ とする．ここで，P_0 は最上位パケット，P_{N-1} は最下位パケットを表す．ただし，図 1 において，最上位パケット P_0 は，レイヤ 0，解像度レベル 0 の Y 成分パケットに，最下位パケット P_{N-1} は，レイヤ N_L-1，解像度レベル N_R-1 の C_r 成分パケットにそれぞれ相当する．各暗号鍵 K_i は，

$$\begin{aligned} K_i &= H^{(N-1)-i}(K_{N-1}) \\ &= H\left(H^{(N-1)-i-1}(K_{N-1})\right), \\ & \qquad i = N-2,\ldots,1,0 \end{aligned} \tag{1}$$

によって K_{N-1} をマスターキーとして，下位パケットに対応する鍵から順に従属的に生成される（図 2）．ここで，$H(\cdot)$ は一方向性ハッシュ関数であり，$H^y(x)$ は x に対して再帰的に y 回ハッシュ値を求めることを意味する．すなわち，

$$H^1(x) = H(x), \tag{2}$$

$$H^2(x) = H(H(x)) \tag{3}$$

である．したがって，あるパケット P_i に対する鍵 K_i は，式 (1) を用いて，1 つ下位のパケット P_{i-1} に対する鍵 K_{i-1} のハッシュ値として求められ，この K_i を用いて P_i が暗号化される．以上のように，マスターキー K_{N-1} から従属的に生成された鍵 K_i を用いて，最下位パケット P_{N-1} から順次暗号化される．

2.2.2 JP2 符号化列の暗号解除

暗号化された JP2 符号化列は公開される．パケット P_J（J は $N-1$ 以下の任意の整数）以上の上位パケットの暗号解除を許諾されたユーザは，P_J に対する鍵 K_J を受信する．ユーザは，

$$K_i = H^{J-i}(K_J), \quad i = J-1,\ldots,1,0 \tag{4}$$

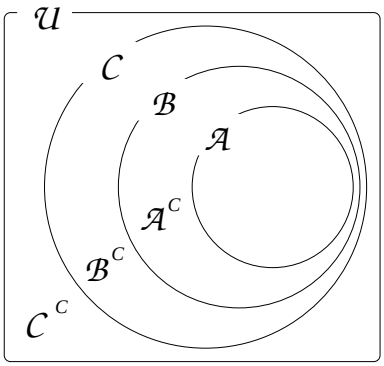


図 3: 提案法におけるアクセス制御対象の相互関係.

によって，P_J より上位のパケットに対する鍵 K_i ($i = 0, 1, \ldots, J-1$) を K_{J-1} から順に従属的に生成し，暗号を解除する．したがって，K_0 を受信したユーザは最低品質で，K_{N-1} を受信したユーザは最高品質で，それぞれ画像を再生することとなる．

次節で述べる提案法は，文献 [8] の暗号鍵生成法を応用して，動画像に対するアクセス制御に拡張させたものである．

3 提案法

ユーザ要求に応じたディジタル動画像 [13–15] の再生のため，個々のユーザに対応する鍵をマスターキーから従属的に生成し，配送する，新しいアクセス制御方式を提案する．提案法に要するマスターキーおよび配送鍵は，いずれの場合も 1 つである．以下では，まず，提案する動画像のアクセス制御法について説明する．次に，提案法の具体例として，フレームレートに基づくアクセス制御，および，レイティングシステムに対応したコンテンツ単位でのアクセス制御について述べる．さらに，提案法では結託攻撃が不可能であることを述べる．

3.1 提案法の原理

提案法でアクセス制御対象とする動画像の単位は，フレーム，チャプター，コンテンツなど様々である．ただし，その相互関係は，図 3 に示すとおり，

$$\mathcal{A} \subset \mathcal{B} \subset \mathcal{C} \subset \mathcal{U} \tag{5}$$

の集合関係であることが条件となる．同図において，$\mathcal{A}$ の $\mathcal{B}$ に関する補集合を $\mathcal{A}^c$，$\mathcal{B}$ の $\mathcal{C}$ に関する補集合を $\mathcal{B}^c$，$\mathcal{C}$ の $\mathcal{U}$ に関する補集合を $\mathcal{C}^c$ と表している．これらの関係を次式にまとめる．

$$\mathcal{A}^c = \mathcal{B} - \mathcal{A}, \tag{6}$$

$$\mathcal{B}^c = \mathcal{C} - \mathcal{B}, \tag{7}$$

$$\mathcal{C}^c = \mathcal{U} - \mathcal{C}, \tag{8}$$

暗号鍵については，集合 $\mathcal{C}^c$ に対する鍵がマスターキーとなる．マスターキーを K_0 とすると，集合 $\mathcal{B}^c$ に対する鍵が K_1，集合 $\mathcal{A}^c$ に対する鍵が K_2，集合 $\mathcal{A}$ に対する鍵が K_3 となり，これらの鍵は次式によって従属的に生成される．

$$K_i = H^i(K_0), \quad i = 1, 2, 3 \tag{9}$$

2.2 節で述べたとおり，$H(\cdot)$ は一方向性ハッシュ関数であり，$H^i(K_0)$ は K_0 に対して再帰的に i 回ハッシュ値を求める．各集合に属するすべての要素は，その集合に割り当てられた同一の鍵で暗号化される．

一方，暗号解除および再生について，全体集合 $\mathcal{U}$ を要求したユーザには，マスターキー K_0 を配送する．K_0 を受信したユーザは式 (9) により，鍵 K_1，K_2，K_3 を生成し，すべての集合に属する要素の暗号を解除し，再生することが可能である．また，集合 $\mathcal{B}$ を要求したユーザには，鍵 K_2 を配送する．ここで，式 (9) は，

$$K_1 = H(K_0) \tag{10}$$

$$K_2 = H(K_1) \tag{11}$$

$$K_3 = H(K_2) \tag{12}$$

と同意である．したがって，このユーザは式 (12) を用いて K_3 を生成し，集合 $\mathcal{B}$ に属する要素の暗号解除と再生が可能である．しかし，$H(\cdot)$ の一方向性によって，鍵 K_2 からは，鍵 K_0 および K_1 は生成できないため，このユーザは要求した集合に属さない要素に対しては，暗号を解除し，再生することはできない．同様のことが，集合 $\mathcal{A}$ または $\mathcal{C}$ を要求したユーザに対しても成り立つ．

3.2 提案法の適用例

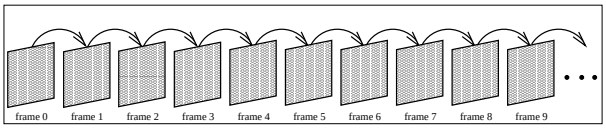
3.1 節で述べた原理を利用した具体的な例を挙げる．ただし，以下に示す例以外においても，提案法は利用可能である．

3.2.1 動画像のフレームレートに基づくアクセス制御

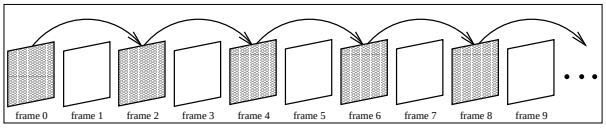
図 4 に，60 fps（同図 (a)），30 fps （同図 (b)），および，15 fps（同図 (c) ）の 3 種類のフレームレートの例を示す．同図において，影部フレームが再生されるフレームである．ここからは，各フレーム集合を図 3 に示す集合に対応づけて説明する．ただし，この例では，3 段階のアクセス制御となるため，集合 $\mathcal{A}$ および $\mathcal{A}^c$ は用いない．

同図において，全体集合 $\mathcal{U}$ はフレームレートが最も高い 60 fps のフレーム集合である．続いて，30 fps のフレーム集合が $\mathcal{C}$，15 fps のフレーム集合が $\mathcal{B}$ となる．したがって，これらの集合は，

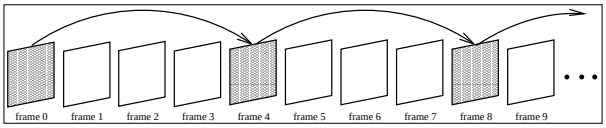
$$\mathcal{B} \subset \mathcal{C} \subset \mathcal{U} \tag{13}$$



(a) 60 fps .



(b) 30 fps .



(c) 15 fps .

図 4: 異なる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）.

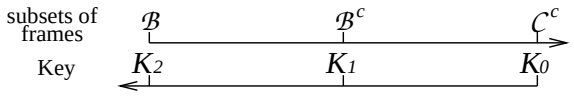


図 5: フレームレートに基づくアクセス制御例.

の関係で示され，提案法の適用条件を満たしている．また，60 fps のフレーム集合 $\mathcal{U}$ のうち，15 fps および 30 fps では再生されないフレーム，すなわち，$2x-1$（x は正の整数）番目のフレーム集合が $\mathcal{C}^c$ ，30 fps で再生されるフレーム集合 $\mathcal{C}$ のうち，15 fps では再生されないフレーム，すなわち，$4x-2$（x は正の整数）番目のフレーム集合が $\mathcal{B}^c$ となる．これらの関係は式 (8)，(7) のとおりである．

提案法では，3.1 節で述べたとおり，$2x-1$ 番目のフレーム集合 $\mathcal{C}^c$ に対する暗号鍵がマスターキー K_0 となり，$4x-2$ 番目のフレーム集合 $\mathcal{B}^c$ に対する鍵が K_1，15 fps のフレーム集合 $\mathcal{B}$ に対する鍵が K_2 となり，これらの鍵は式 (10)，(11) によって従属的に生成される．各集合に属するフレームは，図 5 に示すように，その集合に対応する鍵で暗号化される．

再生に関して，60 fps を要求したユーザには，マスターキー K_0 を配送する．ユーザは式 (10)，(11) によって，鍵 K_1，K_2 を生成し，すべてのフレームの暗号を解除し，再生する．また，15 fps を要求したユーザには，鍵 K_2 を配送する．鍵 K_2 からは，鍵 K_0 および K_1 は生成できないため，このユーザは要求したフレームレート以上の品質で再生することはできない．同様のことが，30 fps を要求したユーザに対しても成立する．

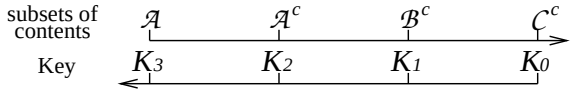


図 6: レイティングシステムにおけるアクセス制御例.

3.2.2 動画像コンテンツのレイティングシステムに基づくアクセス制御

映画に代表されるように，レイティングシステムによる動画像コンテンツの視聴年齢制限が一般的に行われている．本節では，映画コンテンツを例として，レイティングシステムに基づくアクセス制御に提案法を適用する．

1 節で述べたとおり，日本における映画の年齢制限区分は，G，PG12，R-15，および，R-18 の 4 つである．まず，すべてのコンテンツの全体集合 $\mathcal{U}$ において，G 区分のコンテンツ集合を $\mathcal{A}$ とする．次に，G および PG-12 区分の集合を $\mathcal{B}$，G，PG-12 および R-15 区分の集合を $\mathcal{C}$ とする．したがって，これらの集合は式 (5) の関係で示される．図 3 において，PG12 区分のコンテンツ集合は $\mathcal{A}$ の $\mathcal{B}$ に関する補集合 $\mathcal{A}^c$ ，R-15 は $\mathcal{B}$ の $\mathcal{C}$ に関する補集合 $\mathcal{B}^c$，R-18 は $\mathcal{C}$ の $\mathcal{U}$ に関する補集合 $\mathcal{C}^c$ と表される．これらの関係は式 (6)，(7)，(8) に等しい．

この例の場合，R-18 の集合 $\mathcal{C}^c$ に対する暗号鍵がマスターキー K_0 となる．R-15 の集合 $\mathcal{B}^c$ に対する鍵 K_1，PG-12 の集合 $\mathcal{A}^c$ に対する鍵 K_2，G の集合 $\mathcal{A}$ に対する鍵 K_3 は，式 (9) によって従属的に生成される．各集合に属するコンテンツは，図 6 に示すように，その集合に対応する鍵で暗号化される．

再生に関して，コンテンツの視聴を要求する 18 歳以上のユーザには，マスターキー K_0 を配送する．ユーザは式 (9) により，鍵 K_1，K_2，K_3 を生成し，任意の集合に所属する，所望するコンテンツの暗号を解除し，再生することが可能となる．また，15 歳未満で集合 $\mathcal{B}$ のコンテンツの視聴を要求するユーザには，鍵 K_2 を配送する．このユーザは，式 (12) により，鍵 K_3 を生成できるが，$H(\cdot)$ の一方向性から，鍵 K_0 および K_1 は生成できない．したがって，このユーザは要求した集合に属するコンテンツのみ視聴可能となる．12 歳未満，18 歳未満のユーザ，すなわち，集合 $\mathcal{A}$，$\mathcal{C}$ の視聴を要求するユーザに対しても，同様のアクセス制御が可能となっている．

3.3 結託攻撃の可能性

複数のユーザが互いの鍵を不正に共有し，正規に許諾された品質より高い品質で再生したり，許諾されていないコンテンツを再生したりすることを結託攻撃という．1 つのフレームやコンテンツなどのアクセス制御対象に対して，2 つ以上の鍵を用いて暗号化処理を施す手法には，結託攻撃される可能性がある [12]．しかしながら，提案法は，3.2.1 節および 3.2.2 節で述べたとおり，1 つ

(a) レベル 0 . (b) レベル 1 . (c) レベル 2 .

図 7: JP2 における解像度レベルの例（画像は Mobile and Calendar）.

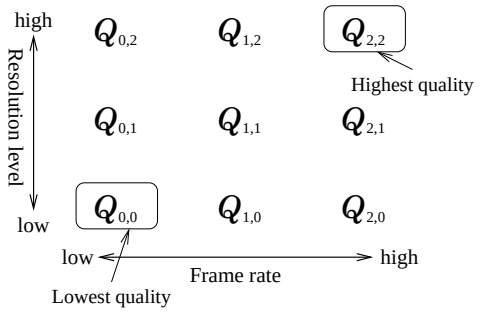


図 8: フレームレートと解像度レベルの関係.

の制御対象に対して，1 つの鍵を用いて暗号化処理を施している．したがって，提案法では，原理的に結託攻撃が生じない．すなわち，提案法は結託攻撃不可能な手法であると言える．

4 アクセス制御対象の拡張

3 節では，フレームレート，コンテンツなど，アクセス制御の対象が 1 つの場合について提案した．ここでは，制御対象を 2 つに拡張した場合について検討する．3 節の提案法は，文献 [8] を基礎とした方式であるが，本節で述べる手法は，著者らの先行研究 [12] に基づいている．

例として，1 つの動画像において，フレームレートと解像度の 2 つの異なる対象を同時に制御することを考える．フレームレートは 3.2.1 節で挙げた 60，30，15 fps，解像度は JP2 [16] における解像度レベル 0–2 の 3 種類とする（図 7）．したがって，本節では動画像符号化方式として Motion JPEG 2000 [15] を仮定するが，スケーラブル符号化が可能な画像符号化方式であれば Motion JPEG 2000 に限定するものではない．

著者らは，1 節で述べたとおり，階層性を有する 2 つの制御対象に同時にアクセス制御を施す方法について，JP2 符号化画像のためのアクセス制御方式として研究してきた [10–12]．文献 [12] は，結託攻撃に対して十分な耐性を有しており，また，冗長性を排除することで，必要なマスターキー数は，2 つの制御対象のうち小さい方の階層数と同数まで低減されている．図 8 の例では，どちらの階層数も 3 であることから，文献 [12] を適用した場合，必要なマスターキーは 3 つとなる．例えば，フレームレート，解像度レベルの階層数それぞれ 5 および 2 の場合，必要なマスターキー数は小さい方の階層数，すなわち，解像度レベルの階層数と同数の 2 つとなる．

このように，動画像に対するアクセス制御対象を 2 つに拡張した場合，著者らの先行研究 [12] を適用することで対応が可能である．ただし，アクセス制御対象が図 3 に示すような階層性を有していることが条件となる．

5 あとがき

本稿では，ディジタル動画像の有料配信サービスにおける，アクセス制御方式を提案した．提案法は制御対象が 1 つの場合において，管理および配送する暗号鍵，各コンテンツのストリームはそれぞれただ 1 つで，ユーザ要求に応じたアクセス制御を可能としている．このことは，鍵とストリームの管理・配送にかかる安全性および容易性を高めるとともに，演算処理量の低減を実現する．さらに，複数ユーザが不正に共有し，正規に許諾されていない品質，年齢制限のコンテンツを再生することを企てる結託攻撃について，提案法の鍵生成方式においては不可能であることを示した．また，アクセス制御対象が 2 つの場合についても考察した．

謝辞

本研究の一部は，科学技術振興事業団（JST）のシーズ発掘試験 A の支援による．

参考文献

[1] 貴家仁志, 今泉祥子, 渡邊修, “マーカコードの発生を考慮した JPEG2000 符号化画像の情報半開示法,” 信学論（D-II）, vol.J86-D-II, no.11, pp.1628–1636, Nov. 2003.

[2] O. Watanabe, A. Nakazaki, and H. Kiya, “A scalable encryption method allowing backward compatibility with JPEG 2000 images,” Proc. IEEE Int. Sympo. Circuits and Sys., pp.6324–6327, Kobe, Japan, May 2005.

[3] 岩村恵市, 林淳一, “JPEG2000 符号化画像のマーカコード発生を回避できる暗号化方式,” 信学論（A）, vol.J90-A, no.11, pp.839–850, Nov. 2007.

[4] R. Grosbois, P. Gerbelot, and T. Ebrahimi, “Authentication and access control in the JPEG 2000 compressed domain, ” Proc. SPIE, vol.4472, pp.95–104, 2001.

[5] B.B. Zhu, M.D. Swanson, and S. Li, “Encryption and authentication for scalable multimedia: current state of the art and challenges,” Proc. SPIE, vol.5601, pp.157–170, 2004.

[6] A. Haggag, M. Ghoneim, J. Lu, and T. Yahagi, “Progressive encryption and controlled access scheme for JPEG 2000 encoded images,” Proc. IEEE Int. Sympo. Intelligent Signal Process. and Comm. Sys., pp.895–898, Yonago, Japan, Dec. 2006.

[7] M. Fujiyoshi, S. Imaizumi, and H. Kiya, “Encryption of composite multimedia contents for access control,” IEICE Trans. Fundamentals, vol.E90-A, no.3, pp.590–596, Mar. 2007.

[8] Y. Wu, D. Ma, and R.H. Deng, “Progressive protection of JPEG 2000 codestreams,” Proc. IEEE Int. Conf. Image Process., pp.3447–3450, Singapore, Oct. 2004.

[9] S. Imaizumi, O. Watanabe, M. Fujiyoshi, and H. Kiya, “Generalized hierarchical encryption of JPEG 2000 codestreams for access control,” Proc. IEEE Int. Conf. Image Process., pp.1094–1097, Genoa, Italy, Sept. 2005.

[10] 今泉祥子, 渡邊修, 藤吉正明, 貴家仁志, “結託攻撃耐性を有する JPEG 2000 の階層性を考慮したアクセス制御型暗号化法,” 信学 SCIS，no . 4F1-5 ，Jan. 2006.

[11] S. Imaizumi, M. Fujiyoshi, Y. Abe, and H. Kiya, “Collusion attack-resilient hierarchical encryption of JPEG 2000 codestreams with scalable access control,” Proc. IEEE Int. Conf. Image Process., pp.II-137–II-140, San Antonio, TX, the U.S., Oct. 2007.

[12] S. Imaizumi, M. Fujiyoshi, and H. Kiya, “Efficient collusion attack-free access control for multidimensionally hierarchical scalability content,” Proc. IEEE Int. Sympo. Circuits and Sys., no.A3L-F-4, pp.505–508, Taipei, Taiwan, R.O.C., May 2009.

[13] ISO/IEC IS 13818-1: “Information technology — Generic coding of moving pictures and associated audio information: System,” 2007.

[14] ISO/IEC IS 14496-10: “Information technology — Coding of audio-visual objects — Part 10: Advanced Video Coding,” 2009.

[15] ISO/IEC IS 15444-3: “Information technology — JPEG 2000 image coding system: Motion JPEG 2000,” 2007.

[16] ISO/IEC IS 15444-1: “Information technology — JPEG 2000 image coding system: Core coding system,” 2004.

[17] ISO/IEC IS 15444-8: “Information technology — JPEG 2000 image coding system: Secure JPEG 2000,” 2007.