平成 13 年度

学士学位論文

動画像 MPEG-4 における暗号適用方式

The code application method in MPEG-4

1020257　　植田　洋加

指導教員　　清水　明宏

2001 年 2 月 8 日

高知工科大学 情報システム工学科

要 旨

動画像 MPEG-4 における暗号適用方式

植田　洋加

モバイルフォンの爆発的な普及から市場が飽和状態にある現在，携帯端末の動画配信サービスが新たなサービスとして期待を集めている．その中で，MPEG-4 は携帯端末のような低処理能力，且つ低ビットレートでも再生可能な動画符号化方式として注目され，MPEG-4 を利用したコンテンツが数多く提供されるようになってきた．

本研究では，商用目的で作成された MPEG-4 に対する著作権保護を目的とした暗号適用方式を提案し，そのセキュリティの確保と処理速度の向上を両立することを目指す．MPEG-4 の特徴から，シーン記述である BIFS，BIFS と各メディアオブジェクトとの中間的役割を果たす OD に対しての暗号適用方式を提案する．BIFS,OD は制御部分に当たり，他のビデオやオーディオのオブジェクトに比べ非常に小容量であるため，効率的な暗号適用を行うことができる．

キーワード　MPEG-4　BIFS　OD　暗号化

Abstract

The code application method in MPEG-4

Hiroka UETA

Recently, it is saturated though mobilephone is being popularized explosively. Such present condition, distributing service for video of a personal digital assistant attracts expectation as new service. It pays attention to MPEG-4 because even a low throughtput and low bitrate like a personal digital assistant can regenerate. And it is coming to be provided abundantly.

In this research, I proposes the code application method which aimed at the protection of contents toward MPEG-4 made on business. And I aim at improvement of processing speed and guaranteed its security. BIFS and OD are encripted for MPEG-4. BIFS composes a scene. OD has the middle-role of BIFS and a media object. BIFS and OD control in MPEG-4, and they are very small capacity compared with other objects. Therefore, this system can perform efficient encryption.

key words MPEG-4 BIFS OD Encryption

目次

図目次

表目次

第 1 章

はじめに

1999 年に開始された携帯電話からインタネットにアクセスできるサービスにより，ブラウジングできる電話，ブラウザフォンが爆発的に普及し，現在モバイル EC(Electronic Commerce:電子商取引）市場は拡大，発展してきている．

さらにインタネットの普及率もそれに伴って年々増加の傾向にある．PC を利用してのインタネット利用率が伸び悩むのとは対照的に，ブラウザフォンでのインタネット利用が利用開始からわずか 2 年間で約 12 倍にもなっている [1]．この状況から見ても，わが国の IT(Information Technology:情報技術) 革命はモバイルによってなされたといっても過言ではない．

しかし，モバイル端末でデータをやり取りする場合，PC に比べ，その端末の処理能力やネットワークの伝送率において大きく見劣りし，音楽や静止画を扱ってもその容量に制限がされていた．

近年，無線ネットワーク技術の進歩により，これまでの数倍から数十倍のデータ伝送率が実現されつつある．更に，モバイルのような処理能力の低い端末で処理が可能な画像圧縮方式の開発により，音楽，静止画データ配信の高速化だけでなく，動画像のリアルタイム配信までが現実になっている．

画像や音楽などのデジタルコンテンツそのものが課金の対象になるというモバイル EC 市場の特性を考えた時，動画像配信の実用化は，モバイル EC 市場を更なる拡大へと導く十分な要素になりうると考えられる．現在，インタネット上の動画像や音声配信はユーザを限定しない一般的な放送システムであるのに対し，モバイルで動画像を商品として活用するためには，ユーザを限定した動画像の秘匿性の確保，著作権の保護を第一に考慮せねばならない．

本研究では，商用目的で作成された動画像に対する著作権保護を目的とした暗号適用方式を提案し，そのセキュリティの確保と処理速度の向上を両立する．つまり，モバイル等が扱う動画像に対して，暗号をかけることによりコンテンツを保護し，作成元であるコンテンツプロバイダが安心してコンテンツを配信できる環境を整え，次世代携帯電話向けコンテンツ配信サービスを健全に成長させる一翼を担うことを目的としている．

動画像については，近年モバイルのような処理能力の低い端末に配信することを目的として開発された動画像圧縮方式である MPEG-4 を研究対象とする．

セキュリティ向上をはかる上で，動画像全てに暗号をかけるとセキュリティは確保されたものになるが処理量が膨大になり，モバイル端末上では処理に負荷がかかりうる．そこで，MPEG-4 の圧縮アルゴリズムを利用し，一部に暗号化をかけることによって，全体を暗号化できるような暗号適用方式を提案した．このことにより，ネットワークへの負荷を軽減させる事ができ，ファイルの伝送速度の向上という利点も生まれる．

本論文の以下の部分では，まず，上に示したように現在モバイル端末に動画配信用に採用されている MPEG-4 についての概要を第二章で述べる．そして，その MPEG-4 での特徴を利用した暗号適用方式の提案を，従来の動画像における暗号適用方式を例に挙げると共に問題点を掲示したものを第三章で行う．第三章での提案による考察を第四章で行う．第五章では今後の課題について述べ，最後に第六章で本論文のまとめとする．

第 2 章

MPEG-4(Moving Picture Experts Group phase4)

携帯端末への動画配信サービスが始まる中で，MPEG-4 に注目が集められている．ここでは，その MPEG-4 のしくみを述べると共に，現在での動画配信サービス状況についても説明する．

2-1 では MPEG-4 における特徴，2-2 では各オブジェクトを合成する働きをするシーン記述について，2-3 では各オブジェクトの内部制御を行うオブジェクトデスクリプタについて述べる．また，2-4 では現在の携帯端末における MPEG-4 の状況について述べる．

2.1 動画像 MPEG-4

以下では概要について述べる．ビデオ，オーディオ，システムにおいては付録にて記載する．

2.1.1 概要

MPEG-4 のエンコーダ，デコーダは高効率符号化，高エラー耐性といった特徴を備えている．また低ビットレート (5Kbps) から高ビットレート（15Mbps）までをカバーし，自然映像・音声，合成画像・音響，テキスト・グラフィックスの符号化方式も規定，有線・無線伝送にも対応した規格である．

MPEG-1/2 では画面全体を一括して符号化するのに対し，MPEG-4 では画面を任意の

画像ごとに符号化する．符号化前に，画面を人物，音声，背景，BGM などに分離する．分離する方法，手順などは規格外である．これらの構成要素はオブジェクトと呼ばれ，それぞれのオブジェクトに適した符号化を行うことにより，効率のよい圧縮を行うことができる．また，映像や音声の符号化だけでなく，CG(Computer Graphics) やテキスト，人工音声 (TTS:Text to Speech) を自然画像や自然音声と組み合わせるなど，ユーザカスタマイズに沿った機能も有している．

以下に MPEG-4 の特性を示す．

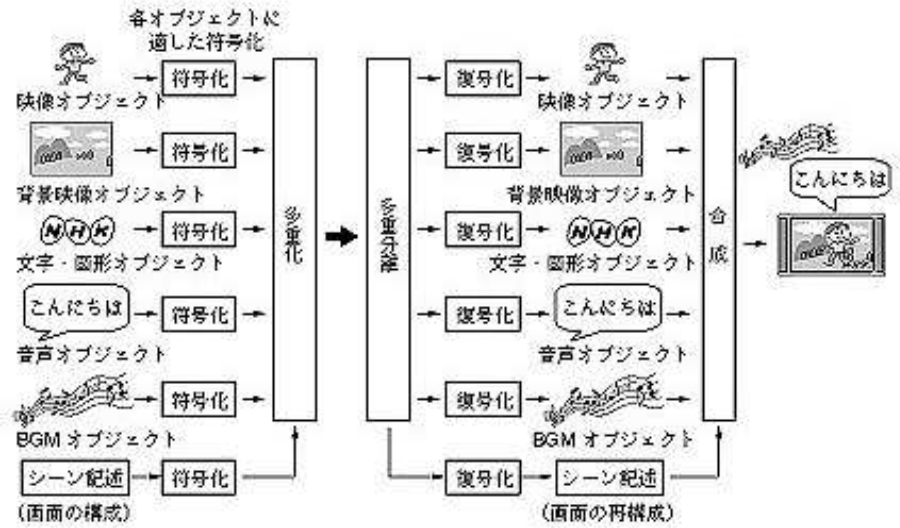

図 2.1　MPEG-4 の特性

図のように各オブジェクトに分割し，符号化したものと，制御/管理する役割を果たす図の下位部分にある，シーン記述を加え，多重化して配送する．受信者側では送信者から送られた多重化されたオブジェクトを分離，復号し，シーン記述により合成する．シーン記述の詳細は 2-2 で述べる．

2.2　シーン記述

シーンとは閲覧者に掲示される画面の構成を意味する．MPEG-1/2 ではシーンという概念はなく，一つの画像/音声として扱ってきた．故に矩形形状のビデオ符号化のみを扱ってきた．しかし，MPEG-4 では任意形状のオブジェクトが符号化できるという特徴から，シーンを構成し，扱うことが可能となった. その仕組みを下に示す.

図 2.2　MPEG-4

この画像を構成するためのシーンの構成は以下のようになる.

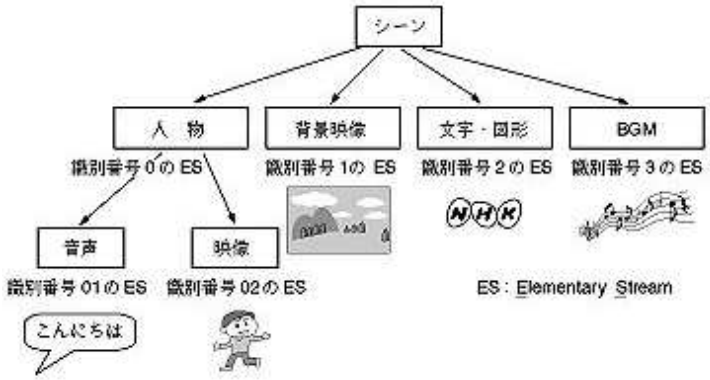

図 2.3　シーン構成

MPEG-4 ではオブジェクトの表示方法や特性を指定するためのシーン記述言語として BIFS(Binary Format for Scenes) を規格化されている.

BIFS では以下の操作を定義している．

- オブジェクトのグループ化
- オブジェクトの時間的・空間的位置の指定
- 属性値の選択
- その他の変形

このように，BIFS は各オブジェクトの制御的役割を果たす．また，加工等もこの部分で行う．

BIFS の配信は予め，シーン全体を配信しておき，シーンの削除，追加等の変更があった場合にその都度 BIFS パケットを送信するというものである．その都度送るということは，変更したシーンを含めたシーン全体を送るのではなく，変更したい部分のみを送るだけなので，容量はシーン全体から比較するとより小容量となる．もちろん，シーン全体を変えたい場合にはシーン全体の BIFS を送る必要がある．また，シーンの変更がなければ BIFS は送ることはなく，字幕や，ニュースのテロップなどを使って表示する場合には比較的連続に BIFS パケットを配送する事になる．

BIFS は WWW(World Wide Web) で用いられている VRML（Virtual Reality Modeling Language）を基に作成されたものである．VRML とは異なった点で，2D 画像の中に 3D 画像を組み込む等 VRML よりも複雑なシーンを構成することが可能である．また，バイナリ形式での記述と規定されている．バイナリ形式での記述とはデータ量の削減を図るためである．このように，MPEG-4 では伝送データを削減し，携帯端末など低ビットレートかつ，低処理能力のものに対して，あらゆる技術が取り入れられている．

2.3　オブジェクトデスクリプタ

各メディアオブジェクト，BIFS，制御情報の符号化表現などを個別に格納して運ぶデータ・ストリームを ES（Elementary Stream）という．この ES を定義，識別するものが OD（Object Descriptor）である．OD は各オブジェクトや BIFS を制御するが，OD 自体も制

御する働きを有する．OD に含まれる情報にはデータフォーマットやデータへのポインタなどがある．また．動画配信する際に一番最初に配信する OD を IOD(Initial OD) といい，IOD は BIFS と OD を制御する．

BIFS と OD，各メディアオブジェクトはそれぞれ個別のものとして扱われる．つまり，BIFS には各オブジェクトを再生するストリームについての情報が含まれず，OD には各オブジェクトに関する構成は含まれない [2]．

以下に BIFS，OD，各メディアオブジェクトの関係を示す．

2.3　オブジェクトデスクリプタ

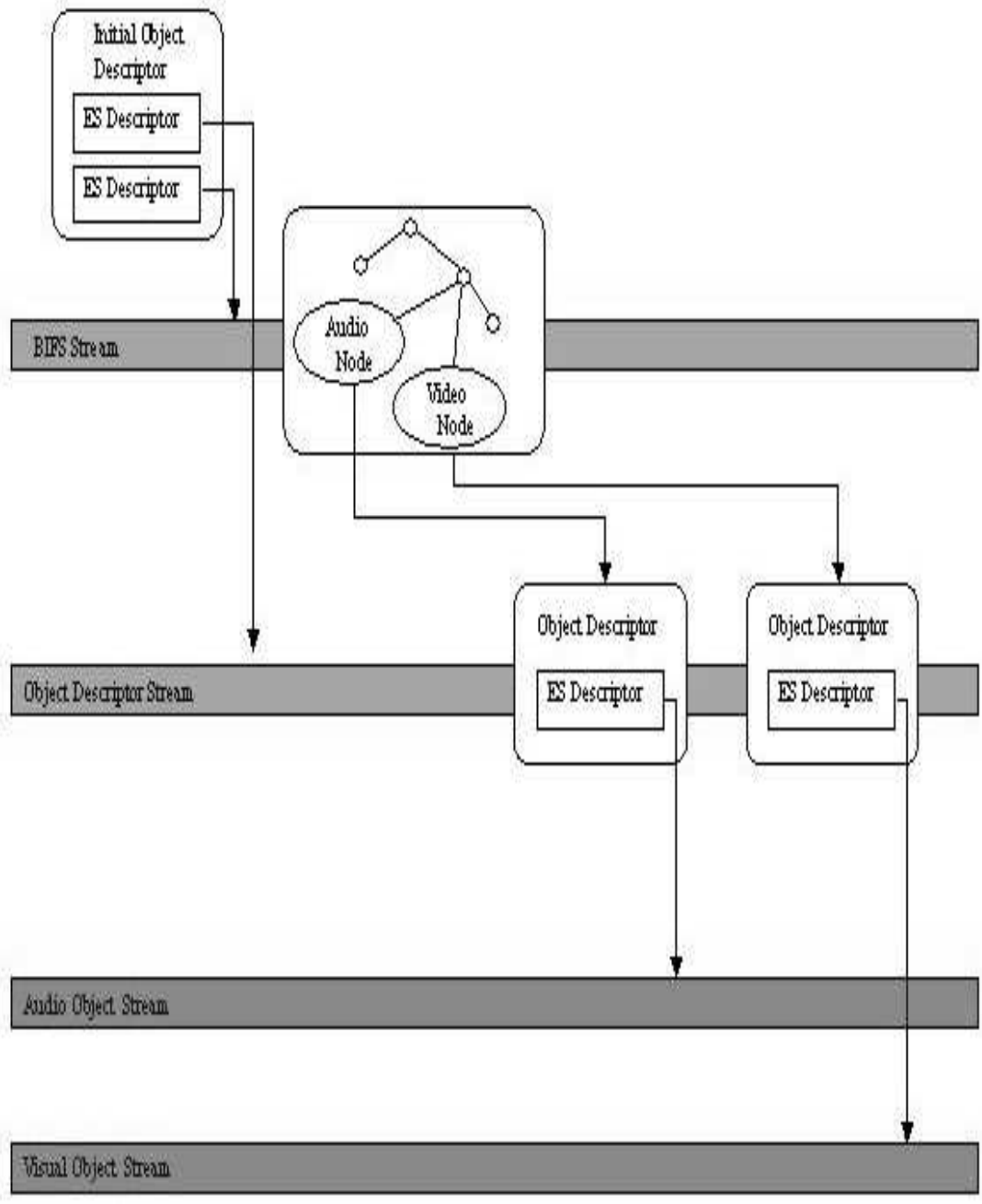

図 2.4　BIFS,OD, 各メディアオブジェクト

2.4　現在の携帯端末における MPEG-4

現在の携帯電話における動画像配信サービスを以下に示す.

会社名	動画配信サービス名	Video	Audio	System
NTTDocomo	i-motion	MPEG-4	AMR	ASF
KDDI	ezmovie	MPEG-4	MP3/QCELP	MP4

上に示すように現在，携帯端末では MPEG-4 が用いられている．携帯端末で用いられている MPEG-4 はシンプルプロファイルと呼ばれる，MPEG-1/2 同様，ビデオオブジェクト，オーディオオブジェクトが 1 つずつしか存在せず，BIFS を用いないものであるのが現状である．BIFS を用いたものはコアプロファイル，メインプロファイルと呼ばれるものである．現在は動画配信が始まったばかりで，MPEG-4 の特徴を十分に生かせていないが，これからビデオ 1 ＋オーディオ 1 の普及が進むにつれ，多ビデオ＋多重化音声の要望も高まってくると考えられる．そうすると，BIFS を用いたコアプロファイルや，メインプロファイルも携帯端末で採用され，その普及も増加してくると考えられる．

BIFS を用いた例で考える．現在のコンテンツでも存在するニュースを想定すると，音声の切り替えがユーザの希望により随時行われ，また，解説者の映像を削除し，背景のみを閲覧する事も可能である．さらに，スポーツ観戦においては，ユーザの閲覧したい部分のみ拡大し，閲覧できる．

第 3 章

暗号適用方式の提案

本章では第二章で述べた MPEG-4 における効率的な暗号適用方式の提案を行う．初めに従来の動画像への暗号適用方式を述べる．その後，MPEG-4 の符号化方式に適した暗号適用方式を述べる．

3.1 動画像への暗号適用

以下では，従来の動画像への暗号適用を挙げると共にその問題点も列挙する．

3.1.1 アナログ画像への暗号適用

従来の動画像への暗号適用はスクランブル技術と呼ばれる方式で行われている．これは信号を攪拌し，放送内容を分からなくするものである．しかし，スクランブル技術は安全性が少なく，暗号強度が低いために簡単に解読される解読される危険性がある．また，スクランブル技術の目的は受信契約を行った正当な受信者だけに提供することであり，その利用価値は放送会社の受信料収入を確保する事にあるので，従来の厳密な意味での「暗号」とは異なり，要求される秘匿性，安全性の面で大きく異なったものになっている．さらに MPEG などのディジタルの符号化方式に対して，圧縮率の低下などの効率的な適用が困難であるという問題点がある．

3.1.2　ディジタル画像 (MPEG) への暗号適用

MPEG は，一つ一つのフレームを圧縮せず，動き予測[*1]をすることによりデータ量を減らすとともに，高画質を維持している．MPEG への暗号化では，これらの特徴を利用し，I フレーム，P フレームを作成する際の I フレームとの差分などに暗号を適用する．しかし，画像という比較的容量の大きいものに暗号化を行う事に変わりはなく，全体暗号を施すよりは効率的だが，携帯端末への実装を考慮すると，処理に負荷がかかりすぎる問題点がある．

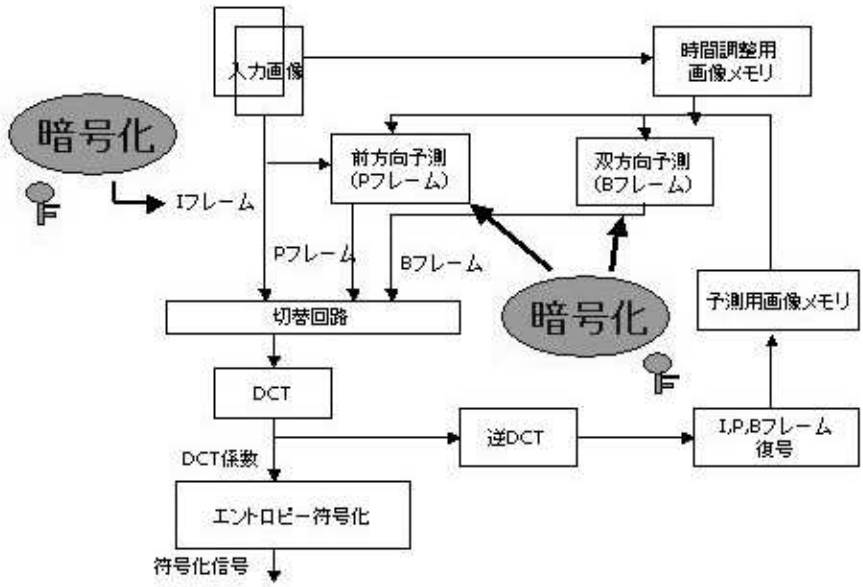

図 3.1　MPEG 暗号化

3.2　MPEG-4 における暗号適用方式の提案

以下では，本研究における暗号適用方式の詳細を述べる．

[*1] 前後のフレームの差分データのみ抽出して符号化する方法

3.2.1　BIFS の暗号化－１－

先に説明したように，MPEG-4 における BIFS は時間的，空間的な制御を果たす意味でも最も重要な役割をしている．よって，この BIFS に対して暗号適用を行う．　BIFS が規定されている System Part において，BIFS の欠落による補償は一切されていない．したがって，第三者にとっての暗号化データはデータの欠落と同等の現象と考えられ，第三者からのデータ盗聴を BIFS の暗号化によって保護できる事を示す．また，正規ユーザに対する BIFS データの欠落，遅延による補償方式 [12] が現在提案されている．

BIFS は他の各メディアオブジェクト同様，データ容量を削減するために符号化を行う．そこで，暗号化箇所が 2 箇所考えられる．一つは符号化前，もう一つは符号化後である．

ここでは，便宜的に MPEG-4 エンコーダによって符号化される前のテキスト形式の BIFS をテキスト型 BIFS と呼び，テキスト型 BIFS が MPEG-4 エンコーダによって符号化された後のバイナリ形式の BIFS をバイナリ型 BIFS をいうことにする．

テキスト型 BIFS の暗号化

まず，符号化前の暗号化について示す．

BIFS は前述で述べたように VRML の拡張である．以下に BIFS の記述を示す．

```
Group {
        children [
                Transform {
                        translation -2 0 0
                        rotation 1 1 0 45
                                children [
                                        Shape {
                                                appearance Appearance {
                                                        texture ImageTexture {
                                                                url 2
                                                        }
                                                } geometry Box {
                                                        size 2 2 2
                                                }
                                        }
                                ]
                }
        ]
}
```

図 3.2　BIFS 表記

シーンはツリー状に配置されたさまざまなノードの集合として表現され，ノードの種類も決まっている．このように，BIFS で定められた形式で記述されたテキストファイル以外のファイルは，エンコードする際に MPEG-4 エンコーダがエラーファイルとみなし，符号化することができない．つまり，テキスト型 BIFS 全体に暗号を適用てしまうと，BIFS の記述形式が崩れてしまい，エンコードすることができなくなってしまう．このことより，テキスト型 BIFS への暗号適用は，BIFS の記述形式を崩さないようファイルに記述されたパラメータのみ，例えば動画の配置を示す座標の値や，再生タイミングを示す時間の値などになされなければならない．

図においては,「translation」（配置位置）,「rotation」（回転）,「size」（拡大，縮小）,「url」（貼り付ける画像，または音声の URL．OD とのポインタ）の右の値を暗号化することになる．

ここで問題となるのが，第三者にとって BIFS に記述されている詳細なパラメータは不明

確だが，どのような要素が記述されているかは閲覧できるので，動画像の大まかな構成が分かってしまう事である．つまり，図において，貼り付ける画像と「BOX」をグループ化している事が分かる．このテキスト型 BIFS のパラメータのみ暗号化された動画像を閲覧する際，何かが再生されているにも関わらず，何かは分からない，例えば位置を表示画面外に配置している場合，再生はしているが暗転の状態が続くという現象が考えられる．図では，「translation -2 0 0」は x,y,z 座標が (-2, 0, 0) へ配置指示を行っているところだが，この配置位置を（500,1000,800）など十分に値を取ることで画面外へと配置することである．しかし，このテキスト型 BIFS への暗号適用の場合，BIFS の記述形式に熟知している者であれば，パラメータの予測を立てて標準のサイズに容易に書き換えられてしまう可能性がある．つまり，暗号化箇所が限定されており，容易に暗号化が行うことができるだけに，簡単に復号されてしまうといった問題点がある．

バイナリ型 BIFS への暗号化

次に符号化後のバイナリ型 BIFS への暗号化について示す.

MPEG-4 エンコーダにより符号化されたバイナリ型 BIFS は，テキストファイルから冗長性をとり除いたバイナリデータの羅列であるため，MPEG-4 デコーダを用いてデコードをしなければ，人間には理解できない．そして，MPEG-4 システムにおいてバイナリ型 BIFS をデコードした後は，その記述に基づいた動画の再生のみであるため，伝送直前に暗号化，伝送直後に復号を行うと，バイナリ型 BIFS 全体に暗号化を施しても正規ユーザにとって何の支障も起こらない．一方，暗号の鍵を知らない第三者は暗号化されたバイナリ型 BIFS を受信した場合，それをそのまま MPEG-4 デコーダでデコードしようとしても無意味なファイルが生成されるだけで，動画像を見ることができない.

このバイナリ型 BIFS への暗号適用の場合，バイナリデータを加工して正規のデータを生成することは，実質全てのデータパターンを総当りしなければならず，不可能である．考えられる攻撃方法としては，BIFS の記述パターンを全て総当りし，それぞれをエンコードし

てバイナリファイルを生成して試さなくてはならない．これは，BIFS のパラメータのみの総当りで推測可能なテキスト型 BIFS の暗号化とは異なり，その BIFS に記述されている要素や構成についても全てのパターンを総当りしなければならず，総当り攻撃に対する十分な保証を得られるものである．

さらに符号化を行う際，上位ノード，下位ノードによって符号化後のサイズが変化するが，符号化前，約 650Byte の BIFS が符号化後，約 50Byte となっている．このサイズであるとあまり暗号，復号時間に大きな変化は見られないが，より複雑であり，容量の多い BIFS となると，符号化後に暗号をかけることが，効率のよい暗号適用となる．したがって，符号化後のバイナリ型 BIFS 全体に対して暗号化を行う．

3.2.2　BIFS の暗号化－２－

BIFS には大きく分けて二つ存在する．一つはシーン全体を表すもので，もう一つは追加，削除など一部変更を行うものである．シーン全体を表す BIFS については全体 BIFS, 変更を行う BIFS については変更 BIFS として次に述べる．先に，全体 BIFS における暗号化を述べ，次に変更 BIFS の暗号化について述べる．

全体 BIFS の暗号化

全体 BIFS はそのシーンに関連した各メディアオブジェクトが伝送される前に配送する必要があることを先に述べた．また，動画配信の際，初めの全体 BIFS は他のオブジェクトも含め，一番初めに伝送される必要があり，もし，欠落や遅延が起こってしまうと，全体 BIFS が伝送されるまで暗転になってしまうという現象が考えられる．よって，各メディアオブジェクトはそのままのデータであるにも関わらず，全体のシーンを表すためのオブジェクトが暗号化されているために動画データとして成り立たないことになる．

したがって，どのシーンにおいても全体 BIFS によってシーンを構成することから全体 BIFS に対して全てのデータを暗号化する．逆に全体 BIFS を一つでも暗号化を行わない部

分が存在すると，そのシーンのみ閲覧できることとなる．もし，そのシーンが長時間変更しない場合は，第三者に動画の内容を秘匿できないことになる．

変更 BIFS の暗号化

変更 BIFS は全体 BIFS に対して，変更を行うものであり，変更事項のみを記述したものである．第三者にとってこのデータだけでは動画を再生することが不可能だが，変更をする際にオブジェクトの時間的，空間的な部分の一部をさらしてしまう事になる．そのため，何度も変更 BIFS が送る事を想定すると，過去のシーン情報が漏洩してしまうことになり，シーン全体が分かってしまう可能性が出てくる．

したがって，この変更 BIFS に対しても暗号適用を行うこととする．また，変更 BIFS の配送回数が多数にのぼる場合を想定すると，このデータも全てにおいて暗号適用を行うことによってより保護強度を高める．

3.2.3　BIFS の暗号化における問題点

BIFS のみの暗号化であると，OD の情報より，各オブジェクトの情報が第三者に漏洩してしまう．オブジェクトの情報が既知であるということは，構成パターンが推測しやすく，類似データが容易に作成される可能性があるという問題点が挙げられる．さらにオブジェクト数が少ない場合も同様に類似データが作成容易である問題点もある．

3.2.4　OD の暗号化

ここでは，OD に対する暗号適用についてその有効性を述べる．

OD は前述で示したように，BIFS がシーンを構成する際，その構成要素であるオブジェクトと BIFS 内で記述されているオブジェクト識別子との関連付けを行うという，各メディアオブジェクトと BIFS との中間的役割を果たす．OD の記述を以下に示す．

OD の表記は図に示すように，オブジェクトを識別するための ID，ES の ID が付加され

```
UPDATE OD [
        {
        objectDescriptorID 2
        es_descriptor {
                es_Number 1
                fileName Angelika.h263
                streamData 15
                decConfigDescr {
                        streamType 5
                        bufferSizeDB 256000
                        specificInfo H263
                }
                alConfigDescr {
                        useAccessUnitEndFlag TRUE
                        useRandomAccessPointFlag TRUE
                        useTimeStampsFlag TRUE
                        timeStampResolution 1000
                        timeStampLength 10
                }
        }
    }
]
```

図 3.3　OD 表記

ている．したがって，BIFS 同様，MPEG-4 における制御的役割を果たし，この部分がないと，再生できない．

OD の暗号化を行うことにより，第三者はオブジェクトの関連付けが不可能となる．よって，各オブジェクトと BIFS のノードとの関連付けを総当りによって自ら行わなければならない．また，デコードに必要なリソースも含まれている事から，この情報がなければ，復号できない事を示す．したがって，第三者は一つのオブジェクトに対して，全ての符号化方式を試さなければならず，リアルタイム配信など時間的制約のあるものは特に，実時間での復号は困難である．

OD は他のオブジェクトとは異なり，符号化を行わず伝送する．そのため，一部，全ての暗号化の両方が行う事ができる．OD は BIFS 同様，容量が少なく，オプショナルな情報も付加しうるので，OD も全体に暗号化を行う．

次に OD の暗号化部分について示す.

IOD の暗号化

動画配信の際，セッションの開始に IOD を配信する事を先に示した．IOD の記述を下に示す.

```
InitialObjectDescriptor {
        objectDescriptorID 1
        ODProfileLevelIndication 1
        sceneProfileLevelIndication 1
        audioProfileLevelIndication 2
        visualProfileLevelIndication 1
        graphicsProfileLevelIndication 1
        esdescr [
                ES_Descriptor {
                        es_id 1
                        muxInfo muxInfo {
                                fileName "exe.od"
                                maxAhead 1
                                streamFormat BIFS
                                }
                        decConfigDescr DecoderConfigDescriptor {
                                objectTypeIndication 0xFF
                                ...
                                avgBitrate 0
                                }
                ......
```

図 3.4　IOD 表記

IOD の表記を見れば分かるが，OD とほぼ変わらない．制御する箇所だけが相違点である．OD は各オブジェクトを制御するのに対し，IOD は BIFS，OD を制御する．そのため，この部分に対しても全体に暗号を適用する．第三者にとって，このデータに暗号化が行われていると，OD のみならず，BIFS のストリームの情報も未知であるため，コンテンツ提供者にとって有効であるといえる．しかし，この部分での暗号化のみであると，BIFS，OD の識別 ID は 16 ビット長，並びに 1 つの MPEG-4 セッション内で重複を許されないので，総当りを行う事で容易に復号できてしまう．そこで，他の部分に対しても暗号適用を行う事に

より，安全性を高める．

IOD 以外の OD の暗号化

OD は BIFS 同様，変更があった場合には，変更箇所のみ伝送する．したがって，この部分に対しても全体に暗号化を行う．全体を示す OD の暗号化はもちろんのこと，変更を示す OD も変更 BIFS に対しての理由同様，変更が多い場合ほど，OD の情報を第三者から防ぐ必要があるためである．

3.2.5　OD の暗号化における問題点

OD のみへの暗号適用を考えた場合，オブジェクトの種類が偏っている場合は符号化方式が限定されるため，BIFS の情報からオブジェクトの情報が予測できる．したがって，容易に類似データが作成可能であるといった問題点がある．また，オブジェクト数が少ない場合も総当り数が少なくなり，類似データ作成が容易であるという問題点も挙げられる．

3.2.6　提案における暗号適用方式

以上の事から，本研究における暗号適用方式は，BIFS，OD の全てに暗号化を行う．２つ同時に暗号化を行うことにより，BIFS のみの暗号化では懸念される脆弱性を，OD にも暗号を適用することでより安全性を高めた．

以下では提案における実装について示す．

3.2　MPEG-4 における暗号適用方式の提案

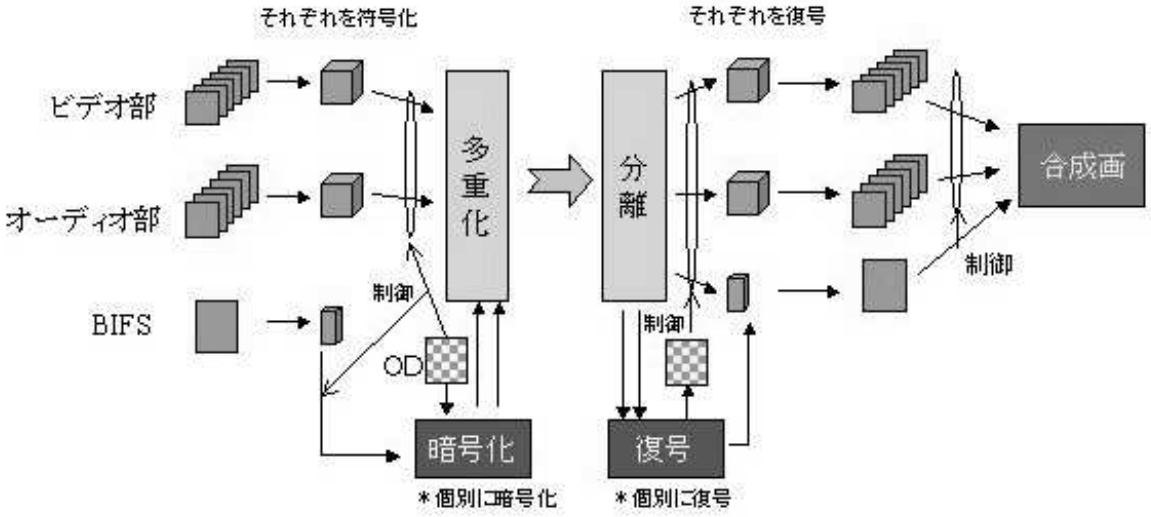

図 3.5　暗号適用方式の提案

手順

BIFS，OD に対して送信側で暗号化が行われた事を前提に，受信端末における動画再生の様子を下に示す.

1. IOD の受信
2. IOD の復号
   (a) BIFS，OD の情報が既知となる
3. BIFS，OD の受信
4. BIFS，OD の復号
   (a) シーン構成が既知となる
   (b) シーンに含まれる種類や数が既知となる
   (c) 各オブジェクトとの関連付けが可能となる
5. 各メディアオブジェクトの受信
6. BIFS，OD，各メディアオブジェクトより再生

3.2.7 暗号方式

ネットワーク上での暗号方式には公開鍵暗号方式と，共通鍵暗号方式の２つが存在する．本研究では動画像という比較的容量の大きいものに対しての暗号適用，並びにストリーミング配信等，リアルタイムでの動画像表示を想定した時に高速処理が必要であることから，共通鍵暗号を用いる．鍵配送に関しては，公開鍵暗号方式による配送など，セキュアな状態で鍵配送を行われるものとする．

共通鍵暗号方式には代表的なものとして，DES(Data Encryption Standard), FEAL(Fast data Encipherment ALgorithm) などが挙げられる．DES はハードウェアでの実現を想定して設計された暗号方式であり，ビット単位での処理によるデータ乱数化を行っていることからソフトウェアでの実現には不向きであることが言える．携帯電話等の比較的処理能力の低い端末においての暗号化/復号を行うためにはハードウェアでなはく，ソフトウェアでの実装を実現しなければならない．そこで，ソフトウェアでの実装に適した，FEAL を今回の暗号方式として提案する．

プログラム

実証実験の際，使用すべく FEAL-8 プログラムを作成した．仕様は以下の通りである．

- プログラム言語は C を用いた．C 言語は構造化された制御構造を持っているので，作業の手順化，明確化が容易であるからである．
- 受信端末側のプログラム搭載量を削減するため，暗号化，復号プログラムを個別に作成した．
- BIFS をバイナリ型で暗号化を行う事より，プログラムはバイナリ型での入出力を可能とした．
- 復号時間計測のための掲示を行う．

- キーボードによる入出力データ，パスワードの指定を行う

このプログラムを実証実験にて搭載する予定である．

現在の仕様は上でも示した通り，キーボードによるファイルの指定，パスワードの入力だが，実証実験では，MPEG-4 エンコーダ，デコーダに直接組み込む事とする．したがって，BIFS ファイルである「*.bif」，OD ファイルである「*.od」を自動認識し，ユーザのパスワードによって，復号を行うように改良を進める．

図 3.6　現在のプログラム

図 3.7　改良後のプログラム

第 4 章

暗号適用方式の考察

ここでは，これまで提唱してきた本研究の暗号適用方式についての考察を行う．考察は，研究背景，目的に照らし合わせ，以下について考察する．

- 動画像の安全性
- 正規ユーザの負荷

4.1 動画像の安全性

提案では，BIFS 並びに OD の全体に対して暗号化を行う事で，BIFS のみの暗号化における脆弱性を，OD へ暗号を適用することで補う，また，逆に対しての意味でも有効性があることを論じた．

これに対する不正ユーザの攻撃方法だが，　BIFS の暗号化により，第三者は復号のために，パスワードの総当り，バイナリ型データの総当り，暗号化データの入れ替えが考えられる．さらに，OD の暗号化により，第三者は復号のために，パスワードの総当り，暗号化データの入れ替えが考えられる．

今回適用する共通鍵暗号方式 FEAL の耐久度を破る総当り攻撃は論外とし，BIFS の暗号化，OD の暗号化のどちらにおいても，パスワードの総当りによる復号を行う事はないという前提で考察する．また，BIFS の暗号化において，バイナリ型データの総当による復号を行う事もないという前提で考察を進める．

以上の前提を踏まえ，一番現実的な攻撃方法として脅威となりうるのが，BIFS への暗号化，OD への暗号化のどちらにおいも，暗号化データのすり替えであると考えられる．

4.1.1　IOD の耐性

提案の中で暗号化の手順を示したが，受信者は動画配信と同時に暗号化データを受信する事になるため，復号できなければ，それ以降の BIFS，OD を含める各メディアオブジェクトの情報が未知となる．もし，暗号化が行われている事が分かると，IOD は BIFS，OD を制御している事より，BIFS，OD のストリームを総当りすることになる．この時，第三者にとって，ストリームの識別 ID が 16 ビット長より，2^{16} の計算をしなければならない．また，ID の重複は許されないので次の ID を識別するためには，$2^{16}-1$ の計算を行う必要がある．

4.1.2　BIFS，OD の耐性

OD への暗号化に対しては，オブジェクト数とオブジェクトの種類を推測することで求められるが，特筆すべきは BIFS への暗号化で，OD により脆弱性を失った BIFS 暗号化により，BIFS のパラメータだけでなく，要素，構成の決定も憶測で行わなければならず，実質無限の組合せが存在し，安全性を確保しているといえる．

さらに，任意形状のオブジェクトを扱う上で，最も時間がかかるものが合成である．正規ユーザにとっても端末に負荷のかかるものである，透過度情報などの計算を総当りの際一つ一つ計算していくのは不可能である．

これらのことから，IOD，BIFS，OD への暗号化は有効であるといえる．

4.2　正規ユーザの負荷

コンテンツ保護のため，暗号化を行うことより，正規ユーザの負荷は受信端末側で復号処理として行われる処理量を示す．復号が合成，再生時間に間に合えば，暗号適用に問題がないといえる．

BIFS はデータの構造によって，データ量が変化する．したがって，構造が複雑であれば，容量は大きくなるが，逆に簡易なものであれば，オブジェクトが多くても BIFS の容量は少なくなる．また，BIFS はデータ総量と比較すると，かなりの小容量であることを先に示

した．

さらに，OD は各メディアオブジェクトの数によってデータ量が比例する．したがって，OD の数が多ければ，それだけ正規ユーザに対して，復号時間における負荷がかかる．しかし，オブジェクト一つに対して数バイト程度しか増加しないため，オブジェクトが増加する事によって，合成，再生に影響を及ぼすほど復号に対する負荷はかからないといえる．

今回，FEAL プログラムを作成したが，MPEG-4 ファイルを暗号化した際，総容量約 350KB のデータの復号に要した時間は 189ms であった．バイナリ型の入出力による暗号化より，容量によって復号時間が変化するため，より小容量のものが効率よく暗号化が行う事ができる．また，OD に対しての暗号化も同様のことがいえる．

第 5 章

今後の課題

今後の課題として，今回未検討に終わったオブジェクトの閾値の検討を行う．また，提案した暗号適用方式の実装を行い，実装した提案の安全性，保護強度の実証実験を行う．

5.1　オブジェクトの閾値の検討

今回は，BIFS のみの暗号適用の脆弱性を OD で補うような暗号適用方式を検討したが，これら双方の制御情報を暗号化しても，オブジェクトの数が少ない，かつオブジェクトの種類に偏りがある場合，今回の考察が必ずしも当てはまらない可能性がある．その場合，BIFS・OD への暗号化よりも，従来通り動画像全体，もしくは動画部分を暗号化したほうが，暗号化の処理量，暗号適用の際の保証強度共に有効であると考えられる．

このような可能性を考慮し，今回提案した暗号適用方式と，従来の暗号適用方式の棲み分けを明確にするため，この暗号適用方式の有効適用範囲を定める閾値を，オブジェクト数，オブジェクトの種類に基づいて設定する必要がある．

5.2　実装と実証

実証の際は，以下の 3 つの項目に焦点を当て，実験を行う．

- 正規ユーザの処理量
- 第三者によるあらゆる攻撃への耐性
- オブジェクト数の閾値

5.2.1　正規ユーザの処理量

シミュレータを用い，実際に動画を配信する．また，暗号データの復号にかかる CPU を考慮した復号時間を計測する．

この計測においては，今回提案した BIFS や OD の暗号化ファイルの個別の復号時間はもちろん，動画像全体，動画部分のみという従来の暗号適用方式についてもその復号時間を計測する．

- テキスト型 BIFS への，パラメータ暗号化
- バイナリ型 BIFS への，全体暗号化

- 全体 BIFS への暗号化
- 変更 BIFS への暗号化

- IOD への暗号化
- 全体 OD への暗号化
- 変更 OD への暗号化

- 動画像全体への暗号化
- 動画部分のみへの暗号化

これらの要素に対する復号時間を，100KB 程度の小容量動画ファイルから，数 MB の大容量動画ファイルまでを個別に計測し，処理時間の比例関係を調べ，考察する．

この時求められた復号処理時間は，次に示す暗号強度の保証を検討する際に考慮する．

5.2.2　第三者によるあらゆる攻撃への耐性

BIFS，OD，両方のそれぞれの総当りを行い，復号時間を計測する事により，一つの MPEG-4 ファイルに対しての保護強度を調べる．

- テキスト型 BIFS のパラメータ暗号に対する，総当り攻撃への耐性

- バイナリ型 BIFS の全体暗号に対する，総当り攻撃への耐性
- IOD への全体暗号に対する，総当り攻撃への耐性
- OD への全体暗号に対する，総当り攻撃への耐性

以上のように，暗号化された BIFS，OD に対し，実際に BruteForce ツールによる総当り攻撃で BIFS，OD の生成を試み，一致するまでの平均処理時間を算出し，各暗号化の保証強度を調査する．

復号処理時間の計測と同様に，全ての要素に対する生成までの処理時間を，小容量動画ファイルから大容量動画ファイルまでを個別に計測し，処理時間の比例関係を調べ，考察する．この考察では，前述した復号処理の処理時間の関係と照らし合わせ，モバイルに適した復号処理量と暗号強度を併せ持つ暗号適用方式を検討する．

この時，パスワードクラックに対する保護強度は FEAL に依存し，実証実験では省く．

5.2.3　オブジェクト数の閾値

今後検討する予定のオブジェクトの閾値を，上の二つの実験結果から求める．

また，携帯端末への実装を目的としたネットワークでのエラー耐性を考慮した暗号適用方式の再検討を行う．

第 6 章

おわりに

本研究では，携帯端末などの低処理端末における暗号適用方式の提案を行い，検討した

まず，MPEG-4 における特徴を明らかにし，それに伴った，制御部分の暗号化における提案を行った．その中で，BIFS の特徴上，正規ユーザでなければ復号はほぼ不可能であること，また，OD の暗号化も同時に行う事より，さらなる保護強度を強める事を考察した．また，オブジェクト数が少数であれば，制御する部分も少ないことから，保護強度が低いことより，従来の暗号化の方が有益であることも示した．

現在，前述でも述べた通り，MPEG-4 のアプリケーションは BIFS を用いない，シンプルプロファイルと呼ばれるものがほとんどである．そのため，提案した暗号適用方式は多くは用いられることは少ないと思われる．今後，ネットワーク技術の進歩によりマルチメディアアプリケーションが増えることを考慮すると，この方式の重要性が明確にされると考えられる．

謝辞

本学情報システム工学科　清水明宏教授には本研究を進める上での御指導，御鞭撻を賜わった．ここに謹んで深謝申し上げる．

ドコモエンジニアリング四国株式会社　林竜也氏には，本研究にあたり，有益な御議論，御助言を頂いた．ここに心から感謝の意を記す．

本学情報システム工学科　島村研究室の修士並びに博士の方々には画像符号化，C 言語において，有益な御議論を頂いた．ここにお礼を申し上げる．

清水研究室学部生　河村智氏，窪内美紀氏をはじめ研究室の方々には，研究途上において有益な御助言を頂いた．諸氏に心より感謝する．

参考文献

[1] http://www.tca.or.jp/

[2] http://leonardo.telecomitalialab.com/icjfiles/mpeg-4_si/

[3] http://www.ics.t.u-tokyo.ac.jp/~nobo/mpeg-4/mpeg-4.html

[4] http://mpeg.telecomitalialab.com/

[5] http://www.pioneer.co.jp/crdl/tech/mpeg/4.html

[6] http://www.nttdocomo.co.jp/index.shtml

[7] http://www.au.kddi.com/

[8] http://www.apple.co.jp/index.html

[9] http://www.strl.nhk.or.jp/TVML/index.html

[10] http://www.strl.nhk.or.jp/publica/dayori-new/index-j.html/

[11] http://www.m4if.org/

[12] 大倉，加藤，田坂，'MPEG-4　BIFS パケットの欠落と補償方式'，電子情報通信学会，2001

[13] 木下　' 動画像情報の暗号化に関する考察'，電子情報通信学会，1997

[14] 岩尾，岩村，安藤，'MPEG-4　IPMP システムへの暗号技術の実装'，情報処理学会，2000

[15] http://ms326.ms.u-tokyo.ac.jp/otobe/

付録 A

MPEG-4

A.1　システム

System Part での構造を下図に示す．まず映像，音声などの各オブジェクト，後述するシーン記述情報がそれぞれの符号化方式で符号化され，ビットストリームが作成される．これをエレメンタリーストリーム（ES : Elementary Stream）という．次に連続する動画像が 1 枚の画面ごとに整理される Sync 層へ渡される．ここではパケットと呼ばれる単位に分割される．これに画面表示する上で必要となる時間管理情報，つまり同期情報が付加され，SL（Sync Layer）パケットとなり，FlexMux，TransMux 層へと渡される．

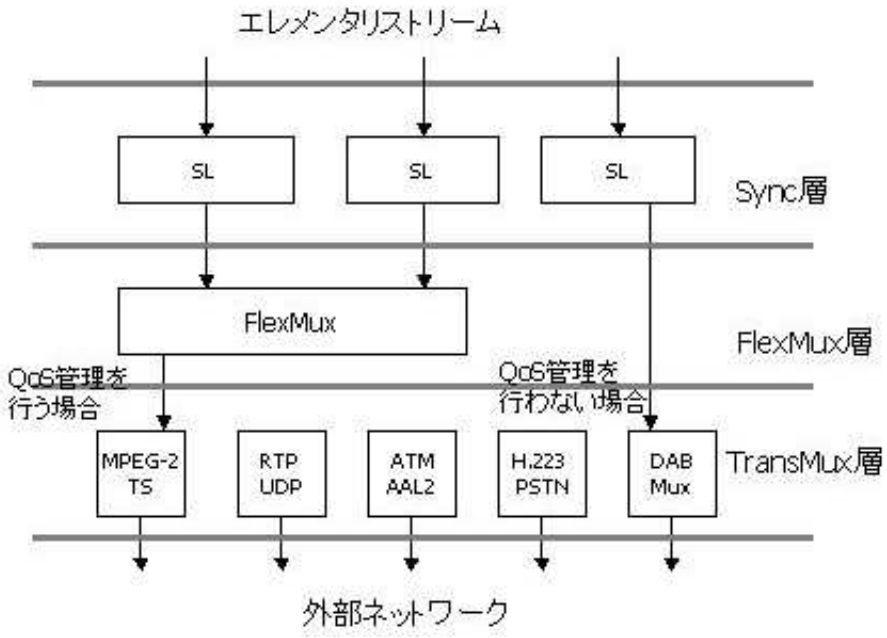

図 A.1　MPEG-4 システム

SL パケット化されたデータは，放送や通信ネットワークへ送られるが，ネットワークの種類により，要求される品質は異なる．電話回線を利用した伝送は数フレーム毎秒程度の品質でも満足されるが，放送に関して言えば，高品質の映像が要求される．したがって，高品質な映像が問われるものは FlexMux 層を通過し，信頼性のあるエラー検出などを行わなければならない．さらに，TransMux 層では，ネットワークに応じてデリバリシステムを選び，伝送する必要がある．利用されるデリバリシステムは MPEG-2 の TS（Transport Stream）や UDP（Use Datagram Protocol），ATM（Asynchronous Transfer Mode）の AAL2，電話回線，DAB(Digital Audio Broadcasting) などが挙げられる．

A.2　ビデオ

ビデオ符号化において，ビデオオブジェクトの時系列を構成する各画面を VOP（Video Object Plane）と呼ぶ．これがビデオ符号化の基本となりうる．VOP は MPEG-1/2 におけるピクチャに相当する．VOP には予測符号化の違いにより，次の 4 種類が存在する．最初の 3 つタイプは MPEG-1/2 における I ピクチャ，P ピクチャ，B ピクチャに相当する．

- I-VOP (フレーム内符号化 VOP) : フレーム内での圧縮を完全に行い，このフレームだけで再生可能である．
- P-VOP (フレーム間順方向予測符号化 VOP) : 直前の I，P フレームを参照して差分を取り，圧縮する．I フレームよりも高圧縮．
- B-VOP (フレーム間双方向予測符号化 VOP) : 前後の I,P フレームを参照して差分を取り，圧縮する．P フレームよりも高圧縮．
- S-VOP (スプライト VOP) : 幾何変換により動画を単一フレームから構成するオブジェクト単位での圧縮を行う．

また，ビデオ部分の基本的な構成はMPEG-1/2と同様，DCT[*1]フレーム内符号化，動き補償[*2]フレーム間符号化である．しかしMPEG-4ビデオ符号化では任意形状の符号化が必要なため，形状符号化のブロックが存在する事が大きな特徴である．またこの形状情報が，動き予測・動き補償・テクスチャ符号器の全てに影響する．

1つのVOPに対するビットストリームは，任意の数のVideo Packetに分割する事が可能である．また，1つのVideo Packetの符号化情報部分には任意の数のマクロブロック符号化情報を格納する事ができる．このことより，1 VOP内のVideo Packet構成に関する自由度が高いといえる．

A.3　オーディオ

MPEG-4のオーディオ部分においても，ビデオ部分同様，低速且つエラーを想定した機能を有する．MPEG-2オーディオとの差を挙げると，従来の周波数分割手法に加え，今までMPEGでは使われていなかったCELP(Code Exited Linear Prediction)やパラメトリック符号化手法が取り入れられたことである．周波数分割手法は高品質のオーディオ符号化に有効な方法だが，低ビットレートや音声に対しての性能が劣る．これに対しCELPは音声に適し，音声符号化標準ではよく使用されるものである．

また，MPEG-4オーディオのカバーする領域は，自然音声，広帯域オーディオの符号化から人工音声までと広範囲に渡ったものである．自然音の音声/オーディオ符号化においては，2kbpsから64kbpsのビットレートが設定される．また，高ビットレートの方式には衛星ディジタル放送の音声符号化方式として採用されたMPEG-2AAC(Advanced Audio Coding)方式が含まれる．合成オーディオに関しては，MIDI(Musical Instrument Digital Interface)に代表される合成音楽（SA : Structured Audio）と，音声合成（TTS : Text-to-Speech）が含まれる．

[*1] Discrete Cosine Transform : 離散コサイン変換．直交変換符号方式の1つである

[*2] Motion Compensation : 二つの連続するフレーム (映像) 間で，データがどの方向へ動いたのかを考慮して圧縮・展開を行う