コンピュータセキュリティ　18－26
(2002.　7.　19)

デジタルコンテンツ保護用鍵管理方式
－木構造パターン分割方式の一般化検討－

中野 稔久† 松崎 なつめ† 館林 誠†

†松下電器産業株式会社 マルチメディア開発センター

〒571-8501 大阪府門真市大字門真 1006

E-mail: †{tnakano, matuzaki, tatebaya}@isl.mei.co.jp

あらまし 映画や音楽などのコンテンツを保護するために，記録媒体には，暗号化されたコンテンツと，復号のための鍵情報が記録される．一方，コンテンツの扱いを許可された機器だけに復号のためのデバイス鍵が与えられ，記録媒体に記録された鍵情報から，暗号化コンテンツを復号する復号鍵の導出を可能とする．しかし，ある特定の機器では，デバイス鍵を与えられていても復号鍵を導出できないように鍵情報は生成される．

このように，記録媒体を利用して機器の無効化を実現する鍵管理方式が提案されており，その一手法である木構造を用いた鍵管理方式は，記録媒体に記録する鍵情報のサイズが機器の総数に比例せず，その対数に比例することから，そのサイズを小さくできる特徴がある．

我々は，SCIS2002 において，木構造を用いた鍵管理方式の一手法であり，従来方式に比べて機器の無効化を効率的に行う「木構造パターン分割方式」を提案した．ここでは，木構造の分木数に対応したビット数の「ノード無効化パターン」を定義し，その「ノード無効化パターン」の全ビットパターンに対してデバイス鍵を割り当てている．

本稿では，デバイス鍵を割り当てるノード無効化パターンに自由度を持たせて一般化を図った「一般化木構造パターン分割方式」を示して，その方式の評価を行う．

キーワード 著作権保護，木構造，鍵管理，無効化

Key Management System for Digital Content Protection
－Generalized Tree Pattern Division Scheme－

Toshihisa NAKANO† Natsume MATSUZAKI† and Makoto TATEBAYASHI†

†Multimedia Development Center, Matsushita Electric Industrial Co., Ltd.

1006 Kadoma, Kadoma City, Osaka 571-8501, Japan

E-mail: †{tnakano, matuzaki, tatebaya}@isl.mei.co.jp

Abstract In this paper, we present and evaluate the scheme named "Generalized Tree Limited Pattern Division Scheme" which generalized [1]. This scheme is one of the tree-based key management systems for digital content protection. In [1], "Node Revocation Pattern (NRP)" is defined, and the device keys are assigned to every possible patterns of NRP for each node. In the present scheme, we generalize [1] by assigning device keys to a subset of possible patterns of NRP.

Keyword Digital Content protection, Tree structure, Key management, Revocation

1. はじめに

近年，デジタル処理，蓄積，通信技術の発展に伴い，映画，音楽などの著作物であるコンテンツをデジタル化して，デジタル光ディスク等の大容量記録媒体（パッケージメディア）に記録してユーザに提供するシステムが普及している．また，デジタル化したコンテンツを放送し，これを受信したユーザが，そのコンテンツを記録型デジタル光ディスク等の記録媒体に記録し，これを再生機器で再生して楽しむというシステムも普及してきている．

こうしたシステムにおいては，通常，コンテンツを不正なコピーから保護するためにコンテンツは暗号化されて記録される．また，正規の再生機器や記録機器には，コンテンツ保護条項を遵守するという条件の下でのみ，暗号化されたコンテンツを復号するための鍵が与えられる．以下，この機器が内蔵する鍵を「デバイス鍵」という．

しかし，何らかの事故や事件により，あるデバイス鍵が不正者に暴露されると，上記コンテンツ保護条項を遵守しない機器が出現する可能性がある．このような場合，著作権者は暴露されたデバイス鍵では，次から提供するコンテンツを扱えないようにしたいと考える．以下，これを「鍵無効化」，あるいは「機器の無効化」という．

その鍵無効化を実現する一手法として，記録媒体を利用した鍵管理方式が提案されている[1-2,6]．一方で，鍵無効化を行う時に，記録媒体に記録する鍵データの容量が機器の総数に比例せず，その対数に比例することから，木構造を用いた鍵管理方式も数多く提案されている[1-5]．木構造を用いた鍵管理方式では，各機器が持つデバイス鍵の共有関係を，木構造を用いて表現しており，木構造の最下位層に各機器が割り当てられる．そして，各機器には，その割り当てられた最下位層から，最上位層に至る経路上に存在する複数のデバイス鍵のうち，適当なデバイス鍵が選択されて与えられる．これらの方式の評価は，機器の総数，及び無効化する機器数に対して，主に以下の3つの指標により行われる．

- デバイス鍵サイズ：機器がデバイス鍵を記憶するために必要なメモリの容量
- 鍵情報サイズ：記録媒体に記録する鍵データの容量．
- 管理デバイス鍵サイズ：鍵管理センタが全てのデバイス鍵を管理するための必要なメモリの容量．

我々は，SCIS2002において，木構造を用いた鍵管理方式の一手法である，木構造パターン分割方式[1]を提案した．[1]は，それまでに提案されている[2,4-5]に比べて，記録媒体上の鍵情報サイズを小さくすることができる方式である．また，[3]に比べると記録媒体上の鍵情報サイズは大きくなるが，[3]ほど機器内のデバイス鍵サイズを大きくする必要がない方式である．[1]では，あるノードの子孫に無効化すべき鍵が存在するノードを「無効化ノード」と定義し，さらに，あるノードの子ノードが無効化ノードであるか否かを表現した「ノード無効化パターン」を定義している．そして，ノードごとに，ノード無効化パターンの全パターンに対して，対応するデバイス鍵を割り当てている．

本稿では，デバイス鍵を割り当てるノード無効化パターンをその全パターンに限定せず，デバイス鍵を割り当てるパターンに自由度を持たせて[1]を一般化した「一般化木構造パターン分割方式」を示して，その方式の評価を行う．

本稿の構成は，2章で著作権保護のためのシステム仮定を示し，3章で一般化木構造パターン分割方式について説明する．4章では，一般化木構造パターン分割方式に対するデバイス鍵サイズ，鍵情報サイズ，及び管理デバイス鍵サイズの評価を行い，最後に，5章で本稿をまとめる．

2. 著作権保護のためのシステム仮定

本章では，本稿におけるコンテンツ保護システムに必要な構成要素について，パッケージメディアを用いたシステムを例に説明して，図2.1にその構成図を示す．したがって，以下では，「機器」を「再生機器」と表現する．また，コンテンツの暗号方式についても説明する．

＜構成要素＞

- 鍵管理センタ：
  再生機器に与えるべきデバイス鍵を生成して，予め各再生機器に複数のデバイス鍵を配布する．また，コンテンツを暗号化するためのコンテンツ鍵を生成して，特定の再生機器のみがそのコンテンツ鍵を獲得できるような鍵情報も合わせて生成する．デバイス鍵，及びコンテンツ鍵の生成および保管は安全に行われると仮定する．
- コンテンツ供給者：
  鍵管理センタよりコンテンツ鍵と鍵情報を受取り，そのコンテンツ鍵を用いてコンテンツを暗号化して，鍵情報と共に暗号化されたコンテンツをパッケージメディアに記録してユーザに提供する．
- 再生機器：
  複数のデバイス鍵を保有して，これを用いてコンテンツ供給者から提供されたパッケージメディアの暗号化されたコンテンツを復号して再生する．ここでは，普及した民生機器を想定し，多く（1億以上）の再生機器の存在を仮定する．

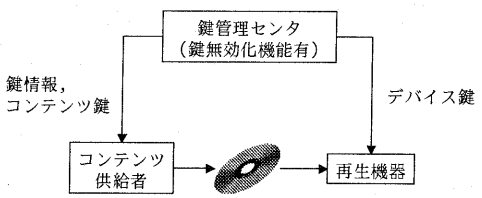

図 2.1 記録媒体を利用した著作権保護システム

＜コンテンツ暗号方式＞

大容量の映画，音楽などの著作物であるコンテンツを配送する場合，コンテンツ供給者は，以下のような階層的暗号方式を用いる．

- コンテンツ毎に決定されるコンテンツ鍵を用いてコンテンツを暗号化する．この結果を暗号化コンテンツという．
- 再生機器が持つデバイス鍵を用いて，上記コンテンツ鍵を暗号化する．この結果を暗号化コンテンツ鍵という．図 2.1 における鍵情報とは，複数の暗号化コンテンツ鍵の集合である．

3. 一般化木構造パターン分割方式

本章では，本稿の提案方式である「一般化木構造パターン分割方式」について説明する．提案方式は，木構造を用いた鍵管理方式の一手法である木構造パターン分割方式[1]を一般化したものである．

3.1. 言葉の定義

- 木構造

  再生機器が他の再生機器とデバイス鍵を共有する関係を，「木構造」を用いて表現する．木構造は，ノードとパスにより構成される．
- ノード

  木構造における各節を「ノード」という．
- パス

  ノードとノードは「パス」により連結されている．また，1 つのノードから下に派生するパスの数を，その木構造の「分木数」という．
- 親ノード

  あるノードから上に伸びる 1 つのパスにより連結されているノードを，そのノードの「親ノード」いう．
- 子ノード

  あるノードから下に派生した複数のパスにより連結されているノードを，そのノードに「子ノード」という．
- ルート

  木構造における最上位層に位置する（親ノードが存在しない）ノードを，特に「ルート」という．
- リーフ

  木構造における最下位層に位置する（子ノードが存在しない）ノードを，特に「リーフ」という．リーフには，1 対 1 で再生機器が割り当てられる．
- レイヤ（番号）

  木構造におけるノードの位置する各層を「レイヤ」と表現し，レイヤの上位から順に 0，1，･･･と番号を付与する．これを「レイヤ番号（Layer Number：LN)」という．
- 相対ノード番号

  同一レイヤに存在する複数のノードに対して，木構造の左側から順に 0，1，･･･と番号を付与する．これを「相対ノード番号（Relative Node Number：RNN)」という．
- 無効化ノード

  あるノードの子孫に，無効化すべき鍵を持つ再生機器が割り当てられたリーフが存在する場合，そのノードを「無効化ノード」という．
- ノード無効化パターン

  あるノードの子ノードが無効化ノードであるか否かを，「0」あるいは「1」で表現する．無効化ノードでない場合を「0」，無効化ノードである場合を「1」とし，それらの値を木構造の左側から順に連結したものを「ノード無効化パターン（Node Revocation Pattern：NRP)」という．

3.2. デバイス鍵を割り当てるNRPのサブセット

本稿では，NRP のハミング重み w に着目して，$w \le w_{max}$ を満たす NRP に対してのみ，デバイス鍵を割り当てるものとする．本稿で提案する「一般化木構造パターン分割方式」は，この w_{max} を新たなパラメータとして導入したところに特徴がある．ただし，n を木構造の分木数とした場合，w_{max} は，$0 < w_{max} < n$ を満たす整数とする．なお，[1]は $w_{max} = n - 1$ の場合に相当する．

3.3. 木構造に対するデバイス鍵の割り当て

システムの準備フェーズとして，鍵管理センタは木構造を構築して，各ノードにデバイス鍵を次のように割り当てる．リーフを除く各ノードに対して，$w \le w_{max}$ を満たす NRP に対してデバイス鍵をそれぞれ割り当て，各リーフには，NRP=「00･･･0」（オール 0）に対応するデバイス鍵を 1 つ割り当てる．ここでは，割り当てたデバイス鍵を識別するための Index 情報として，LN，RNN，NRP を，それぞれのデバイス鍵に付与するものとする．

ただし，$w_{max}=n-1$の場合は，あるレイヤのノードの NRP=「01…1」（$w=n-1$）に対応するデバイス鍵①と，その左端の子ノードの NRP=「00…0」（オール0）に対応するデバイス鍵②は，同一の再生機器をカバーすることになる．したがって，$w_{max}=n-1$の条件下では，デバイス鍵①と，デバイス鍵②のどちらか一方だけ割り当てればよい．図 3.1 に，その具体例を示す．

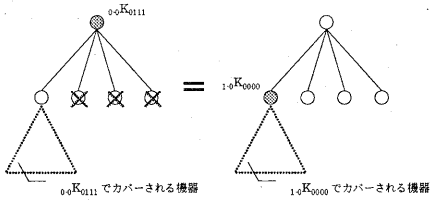

図 3.1 デバイス鍵が同一機器をカバーする例

次に，図 3.2 に，4 分木で $w_{max}=1$ とした場合の LN0／RNN0，LN1／RNN3 に割り当てられるデバイス鍵の具体例を示し，図 3.3 に，同じく 4 分木で $w_{max}=3$ とした場合の LN0／RNN0，LN1／RNN3 に割り当てられるデバイス鍵の具体例を示す．ただし，図 3.3 に示す具体例は[1]に対応する．

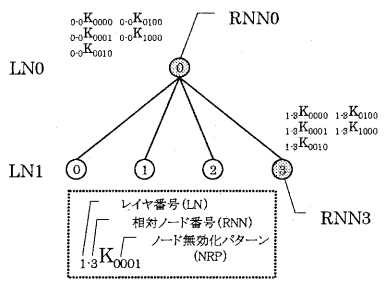

図 3.2 木構造に対するデバイス鍵の割り当て ($w_{max}=1$)

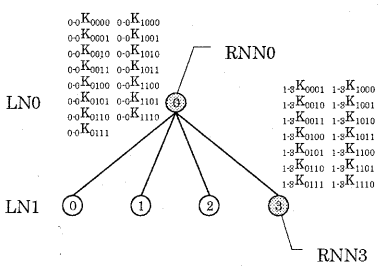

図 3.3 木構造に対するデバイス鍵の割り当て ($w_{max}=3$)

3.4. 再生機器に対するデバイス鍵の割り当て

次に，システムの準備フェーズとして，木構造のリーフに位置する各再生機器に，デバイス鍵を次のように割り当てる．そのリーフからルートに至るパス上に存在するノードに割り当てられている全てのデバイス鍵のうち，その再生機器が無効化されているときの NRP に対応するデバイス鍵を除く鍵（パス上に位置するノードが「0」と表現される NRP に対応するデバイス鍵）を割り当てる．

図 3.4 に，高さ 2 の 4 分木の木構造を示し，$w_{max}=1$ の場合の LN2／RNN0 に位置する再生機器に割り当てられるデバイス鍵の具体例を示す．

まず，LN0／RNN0 に割り当てられた全てのデバイス鍵のうち，LN1／RNN0 が「0」と表現される NRP に対応するデバイス鍵（NRP=「0xxx」：x は「0」，あるいは「1」の任意であるが，そのハミング重み w は $w\leq 1$）が再生機器に割り当てられる．同様に，LN1／RNN0 に割り当てられた全てのデバイス鍵のうち，LN2／RNN0 が「0」と表現される NRP に対応するデバイス鍵（NRP=「0xxx」）が再生機器に割り当てられる．

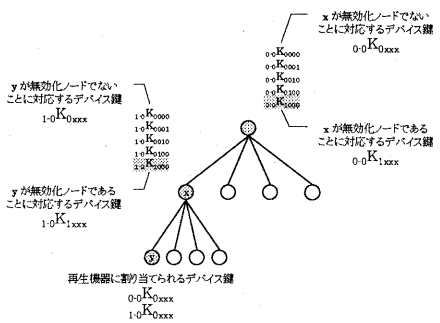

図 3.4 再生機器に対するデバイス鍵の割り当て

3.5. コンテンツ鍵の暗号化に使用するデバイス鍵の選択

システムの運用フェーズでは，鍵管理センタが生成する鍵情報（暗号化コンテンツ鍵の集合）は以下の手順により生成される．

(1) 無効化する再生機器が存在する場合，その再生機器が位置するリーフを指定する．

(2) 木構造において，(1)で指定したリーフから，ルートに至るパス上に位置するノードを全て無効化ノードにする．

(3) 木構造における各ノードを，上位から下位，同じレイヤの場合は左から右の順に，全てのノードをチェックしていき，そのノードが無効化ノ

ードであれば，そのノードを，デバイス鍵を選択するノードの候補として記憶する．さらに，無効化ノードの NRP のハミング重み w が w_{max} よりも大きい場合は，その無効化ノードの子ノードもデバイス鍵を選択するノードの候補として記憶する．

(4) (3)で候補として記憶したノードのうち，その NRP のハミング重み w が w_{max} 以下のノードに対して，その NRP に対応するデバイス鍵を，コンテンツ鍵を暗号化するための鍵として選択する．

(5) コンテンツ鍵を，(4)で選択した複数のデバイス鍵でそれぞれ独立に暗号化し，複数の暗号化コンテンツ鍵からなる鍵情報を生成する．

図 3.5 に，4 分木の木構造を示し，さらに $w_{max}=1$ として，LN2／RNN3，LN2／RNN12 に位置する再生機器が無効化されているとする．このときの，コンテンツ鍵の暗号化に使用するデバイス鍵の選択方法を具体例を用いて説明する．

まず，手順(1)に従い，無効化する再生機器が位置するリーフ(LN2／RNN3，LN2／RNN12)を指定する．次に，手順(2)に従い，該当するノードを無効化ノードにする（図中の「×」マークが無効化ノードである)．さらに，手順(3)より，デバイス鍵を選択するノードの候補を決定する．その候補は，LN0／RNN0，LN1／RNN0，LN1／RNN1，LN1／RNN2，LN1／RNN3 の 5 つのノードである．手順(4)より，候補である 5 つのノードのうち，そのノードの NRP のハミング重み w が $w \le w_{max}=1$ であるノードから，その NRP に対応するデバイス鍵を選択する．LN0／RNN0 の NRP は NRP=「1001」$(w=2)$ であるためデバイス鍵を選択せず，LN1／RNN0 からはデバイス鍵 $_{1\cdot0}K_{0001}$，LN1／RNN1 からはデバイス鍵 $_{1\cdot1}K_{0000}$，LN1／RNN2 からはデバイス鍵 $_{1\cdot2}K_{0000}$，LN1／RNN3 からはデバイス鍵 $_{1\cdot3}K_{1000}$ をそれぞれ選択する．最後に，手順(5)に従い，選択したデバイス鍵でコンテンツ鍵を暗号化する．

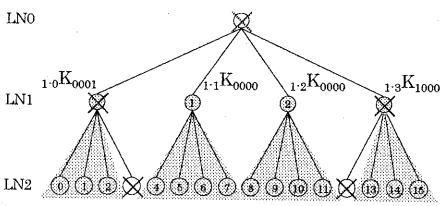

図 3.5 暗号化に使用するデバイス鍵の選択

3.6. 復号に使用するデバイス鍵の選択

システムの運用フェーズでは，各再生機器は，自身が持つ複数のデバイス鍵から，どのデバイス鍵を用いて暗号化コンテンツ鍵を復号するのかを決定する必要がある．その方法としては，例えば，全てのデバイス鍵で，全ての暗号化コンテンツ鍵を復号する方法や，暗号化コンテンツ鍵に，復号に使用すべきデバイス鍵の情報（暗号化に使用したデバイス鍵の Index 情報）を付与する方法などが考えられる．ただし，本稿では復号に使用するデバイス鍵の決定方法については言及しない．

4. 一般化木構造パターン分割方式の評価

本章では，NRP のハミング重みの上限である w_{max} を導入した，一般化木構造パターン分割方式の評価を行う．具体的には，木構造の分木数を n，高さを h，デバイス鍵を割り当てる NRP のハミング重みの上限を w_{max} として，デバイス鍵サイズ（再生機器が持つデバイス鍵の数，number of Device Key for Playback device：DKP）と，鍵情報サイズ（暗号化コンテンツ鍵の数，number of Encrypted Content Key：ECK）と，管理デバイス鍵サイズ（鍵管理センタが管理するデバイス鍵の総数，number of Device Key for key management Center：DKC）を求める．

4.1. デバイス鍵サイズの評価式

再生機器が持つデバイス鍵の数 DKP は，以下の式で与えられる．

$$\begin{aligned} DKP &= h\times\textstyle\sum_{j=0}^{w_{max}} C_{n-1}^{j}+1 && (0<w_{max}<n-2)\\ DKP &= h\times\textstyle\sum_{j=0}^{w_{max}} C_{n-1}^{j}+1-h && (n-2\le w_{max}<n) \end{aligned} \quad (1)$$

＜導出＞

再生機器が持つデバイス鍵の数 DKP の導出を以下に示す．各ノードに割り当てられているデバイス鍵のうち，各再生機器に割り当てられるデバイス鍵は，リーフを除くレイヤ毎に $\sum_{j=0}^{w_{max}} C_{n-1}^{j}$ 個である．これは，n ビットの NRP のうち，デバイス鍵を配布する再生機器の祖先に当たるノードの NRP を「0」に固定して，残りの $n-1$ ビットに対して，重みを 0～w_{max} まで変化させたときの，組み合わせの数の総和である．さらに，リーフには，そのリーフ固有のデバイス鍵が 1 つ割り当てられるため，再生機器が持つデバイス鍵の数 DKP は，

$$DKP = h\times\textstyle\sum_{j=0}^{w_{max}} C_{n-1}^{j}+1 \quad (2)$$

となる．

一方，$w_{max}=n-1$ の場合は，あるレイヤのノードの NRP=「01…1」（$w=n-1$）に対応するデバイス鍵①と，

その左端の子ノードのNRP=「00…0」(オール0)に対応するデバイス鍵②は，同一の再生機器をカバーすることになるため，どちらか一方だけを割り当てればよい．[1]では，ルートを除く各ノードにデバイス鍵①が割り当てられ，デバイス鍵②は割り当てられないので，式(2)に比べて h 個だけデバイス鍵の数を少なくすることができる．さらに，$w_{\max}=n-2$ では，デバイス鍵①に代えてデバイス鍵②が割り当てられるため，$w_{\max}=n-1$ と，$w_{\max}=n-2$ の条件下では，再生機器が持つデバイス鍵の数は同じ値となる．

以上より，再生機器が持つデバイス鍵の数 DKP は，

$$DKP=h\times\sum_{j=0}^{w_{\max}}C_{n-1}^{j}+1 \qquad (0<w_{\max}<n-2)$$
$$DKP=h\times\sum_{j=0}^{w_{\max}}C_{n-1}^{j}+1-h \qquad (n-2\le w_{\max}<n)$$

となり，式(1)が導かれる．

■

4.2. 鍵情報サイズの評価方法

記録媒体に記録する鍵情報は，図3.5に示す通り，有効な再生機器をカバーする部分木のルートに割り当てられたデバイス鍵でコンテンツ鍵を暗号化した，暗号化コンテンツ鍵の集合である．したがって，暗号化コンテンツ鍵の数は，有効な再生機器をカバーする部分木の数と等しいため，以下では，部分木の数を求めることで，鍵情報サイズを求める．

ここでは，2種類の部分木の定義を行い，その部分木に無効化すべき再生機器が発生した場合の振る舞い（分割の法則）と，分割されて増加する部分木の増加量と，次に無効化すべき再生機器が発生するルールについて以下に示す．

- Complete Tree：$CT(L)$
  部分木のルートのNRPがNRP=「00…」(オール0)で，かつ，ルートの位置するレイヤがLである部分木．
- Revoked Tree：$RT_w(L)$
  部分木のルートのNRPがNRP=「00…」以外で，かつ，ルートの位置するレイヤがLである部分木．ただし，w はそのルートのNRPのハミング重みとする．

まず，$CT(L)$ に無効化すべき再生機器が1台発生すると，この部分木は，$RT_1(L)$，$RT_1(L+1)$，…，$RT_1(h-1)$ の $h-L$ 個の部分木に分割される．この時の部分木の増加量は $(h-L-1)$ 個である．

次に，$RT_w(L)$ に無効化すべき再生機器が1台発生すると，$w<w_{\max}$ の場合，この部分木は，$RT_{w+1}(L)$，$RT_1(L+1)$，…，$RT_1(h-1)$ の $h-L$ 個の部分木に分割される．この時の部分木の増加量も同様に $(h-L-1)$ 個である．一方，$w=w_{\max}$ の場合，この部分木は，$RT_1(L+1)$，$RT_1(L+2)$，…，$RT_1(h-1)$ の $(h-L-1)$ 個の RT と，$(n-w-1)$ 個の $CT(L+1)$ に分割される．この時の部分木の増加量は $(h-L+n-w-3)$ 個である．

以上より，最も部分木の数が増加する無効化すべき再生機器の発生パターンは以下の通りである．

$n-w\le 2$ となる木構造においては，無効化すべき再生機器が発生する優先順位を，部分木の高さが同一の場合は，

$$CT>RT_1>RT_2>\cdots>RT_{w_{\max}} \tag{3}$$

とする．ただし，部分木の高さが異なる場合は，最も高い部分木を優先する．

一方，$n-w>2$ となる木構造においては，無効化すべき再生機器が発生する優先順位を，部分木の高さが同一の場合は，

$$CT>RT_1>RT_2>\cdots>RT_{w_{\max}-1} \tag{4}$$

とする．ただし，部分木の高さが異なる場合は，最も高い部分木を優先する．さらに，部分木 $RT_{w_{\max}}$ については，他の部分木との高さの差が，$n-w-2$ よりも小さければ，その優先順位を，

$$RT_{w_{\max}}>CT \tag{5}$$

とする．

上記ルールにしたがって，無効化すべき再生機器が発生した場合，無効化台数に対する鍵情報サイズが最大値となる．

4.3. 管理デバイス鍵サイズの評価式

鍵管理センタが管理するデバイス鍵の総数 DKC は，以下の式で与えられる．

$$DKC=(n^h-1/n-1)\times\sum_{j=0}^{w_{\max}}C_n^j+n^h \qquad (0<w_{\max}<n-2)$$
$$DKC=(n^h-1/n-1)\times\sum_{j=0}^{w_{\max}}C_n^j+n^h-((n^{h+1}-1/n-1)-1) \qquad (n-2\le w_{\max}<n) \tag{6}$$

＜導出＞

鍵管理センタが管理するデバイス鍵の総数 DKC の導出を以下に示す．リーフを除く各ノードに割り当てられるデバイス鍵は，$\sum_{j=0}^{w_{\max}}C_n^j$ 個である．これは，n ビットのNRPに対して，重みを0～$w_{\max}$ まで変化させたときの，組み合わせの数の総和である．さらに，リーフには，そのリーフ固有のデバイス鍵が1つ割り当てられるため，鍵管理センタが管理するデバイス鍵の総数 DKC は，

$$DKC=(n^h-1/n-1)\times\sum_{j=0}^{w_{\max}}C_n^j+n^h \tag{7}$$

となる．ただし，$(n^h-1/n-1)$ は，木構造全体からリーフを除いたノードの総数である．

一方，$w_{\max}=n-1$ の場合は，あるレイヤのノードの

NRP=「01…1」($w=n-1$)に対応するデバイス鍵①と，その子ノードのNRP=「00…0」(オール0)に対応するデバイス鍵②は，同一の再生機器をカバーするためデバイス鍵①だけ割り当てればよい．したがって，式(7)に比べてルートを除く各ノードごとに1個ずつデバイス鍵の数を少なくすることができる．さらに，$w_{max}=n-2$では，デバイス鍵①に代えてデバイス鍵②が割り当てられるため，$w_{max}=n-1$と，$w_{max}=n-2$の条件下では，鍵管理センタが管理するデバイス鍵の総数は同じ値となる．

以上より，鍵管理センタが管理するデバイス鍵の総数DKCは，

$$DKC=(n^h-1/n-1)\times\sum_{j=0}^{w_{max}}C_n^j+n^h \quad (0<w_{max}<n-2)$$

$$DKC=(n^h-1/n-1)\times\sum_{j=0}^{w_{max}}C_n^j+n^h - ((n^{h+1}-1/n-1)-1) \quad (n-2\leq w_{max}<n)$$

となり，式(6)が導かれる．ただし，$((n^{h+1}-1/n-1)-1)$は，木構造全体からルートを除いたノードの総数である．■

4.4. 評価結果

ここでは，式(1)，及び式(6)を用いて，与えられた再生機器の総数に対して，必要となるデバイス鍵サイズと，管理デバイス鍵サイズをそれぞれ求める．また，4.2節に示した無効化機器の発生ルールをプログラミングして，与えられた再生機器の総数と，無効化する再生機器数に対する鍵情報サイズを計算機により求める．具体的には，以下の数値例を用いる．

- 再生機器の総数：
  $3^{19}=1{,}162{,}261{,}467$（約10億台）
  $4^{15}=1{,}073{,}741{,}824$（約10億台）
  $5^{13}=1{,}220{,}703{,}125$（約10億台）
- 無効化する再生機器数：
  10,000台

ここでは，鍵情報サイズを算出するために，各コンテンツ鍵はデータ幅128 bitの暗号アルゴリズムで暗号化されているものと仮定して，1つの暗号化コンテンツ鍵を128 bit (=16 byte)として算出している．ただし，実際の運用においては，3.6節に示す通り，Index情報等の何らかの付加情報が必要となるが，ここでは付加情報のサイズは考慮しないものとする．また，デバイス鍵サイズ，及び管理デバイス鍵サイズについても，上記鍵情報サイズと同様に，1つのデバイス鍵を128 bit (=16 byte)として算出している．

3分木を考えた場合，木構造の高さは$h=19$，4分木では$h=15$，5分木では$h=13$の木構造となる．上記パラメータにおいてNRPのハミング重みの上限w_{max}を変化させた場合のデバイス鍵サイズと鍵情報サイズの関係を表4.1と図4.1に示し，w_{max}と管理デバイス鍵サイズの関係を表4.2に示す．

表4.1 デバイス鍵サイズと鍵情報サイズの関係

		デバイス鍵サイズ [KB] (括弧内は[1]に対する割合)	鍵情報サイズ [MB] (括弧内は[1]に対する割合)
3分木	① $w_{max}=1, 2$	0.91 (1.00)	1.63 (1.00)
4分木	② $w_{max}=2, 3$	1.66 (1.00)	1.28 (1.00)
	③ $w_{max}=1$	0.95 (0.57)	1.50 (1.17)
5分木	④ $w_{max}=3, 4$	3.06 (1.00)	1.12 (1.00)
	⑤ $w_{max}=2$	2.25 (0.74)	1.31 (1.17)
	⑥ $w_{max}=1$	1.03 (0.34)	1.42 (1.27)

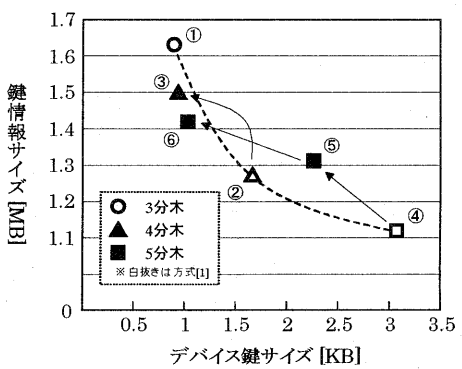

図4.1 デバイス鍵サイズと鍵情報サイズの関係

表4.2 w_{max}と管理デバイス鍵サイズの関係

		管理デバイス鍵サイズ [GB]
3分木	① $w_{max}=1, 2$	74.7
4分木	② $w_{max}=2, 3$	42.7
	③ $w_{max}=1$	136.4
5分木	④ $w_{max}=3, 4$	90.9
	⑤ $w_{max}=2$	45.5
	⑥ $w_{max}=1$	52.0

4.5. 考察

(i)表4.1より，NRPのハミング重みの上限w_{max}を小さくすることで，デバイス鍵サイズを小さくできるが，その反面，鍵情報サイズが大きくなることがわかる．その減少量，あるいは増加量の割合は，4分木の②と③を比較すると，デバイス鍵サイズは約43%減と大幅に削減されているが，鍵情報サイズは約17%増とそれほど増加していない．また，5分木の④と⑥では，デバイス鍵サイズは約66%減と大幅に削減されているが，鍵情報サイズは約27%増とそれほど増加していな

いことがわかる．しかし，図 4.1 より，4 分木の③，及び 5 分木の⑥を，[1]の木構造パターン分割方式の特性（①②④を結ぶ破線で図示）と比較すると，その性能の改善度は僅かであることがわかる．

(ii) 表 4.2 より，管理デバイス鍵サイズを比較すると，[1]の木構造パターン分割方式で最もそのサイズが小さい①に対して，4 分木の③，及び 5 分木の⑥は，それぞれ約 18%減，約 12%減と，そのサイズを削減していることが確認できる．

なお，表 4.1 における $n-w \leq 2$ の条件（①，②，④）は，それぞれ，[1]の木構造パターン分割に対応する．また，表 4.1 より，$n-w \leq 2$ の条件においては，$w_{\max}$ によって鍵情報サイズが変化していない．これは，式(3)に示す通り，上記条件の下では，同一のルールで無効化すべき再生機器が発生するためである．

5. おわりに

本稿では，デバイス鍵を割り当てるノード無効化パターンをその全パターンに限定せず，デバイス鍵を割り当てるパターンに自由度を持たせて[1]を一般化した「一般化木構造パターン分割方式」を示した．さらに，評価式によるデバイス鍵サイズ，及び管理デバイス鍵サイズの算出と，計算機による鍵情報サイズの算出を行った．その結果，デバイス鍵サイズと，鍵情報サイズに関しては，[1]に比べて性能の改善度は僅かであるものの，管理デバイス鍵サイズは，約 18%削減可能であることを示した．

今後の課題は，鍵情報サイズを算出する評価式の導出や，デバイス鍵サイズや，鍵情報サイズ等の特性を大幅に改善することなどが挙げられる．

文　献

[1] 中野 稔久, 大森 基司, 松崎 なつめ, 館林 誠, "デジタルコンテンツ保護用鍵管理方式-木構造パターン分割方式-," 2002 年暗号と情報セキュリティシンポジウム講演論文集, 10C-1, 2002.

[2] 中野 稔久, 大森 基司, 館林 誠, "デジタルコンテンツ保護用鍵管理方式," 2001 年暗号と情報セキュリティシンポジウム講演論文集, 5A-5, 2001.

[3] D.Naor, M.Naor, and J.Lotspiech, "Revocation and Tracing Scheme for Stateless Receivers," *Proceedings of CRYPTO2001*, LNCS2139, pp.41-62, 2001.

[4] D.Wallner, E.Harder, and R.Agee, "Key Management for Multicast: Issues and Architectures," Internet RFC2627, June 1999.

[5] D.McGrew, A.T.Sherman, "Key Establishment in Large Dynamic Groups Using One-way Function Trees," IEEE Transactions on Software Engineering, May 20 1998.

[6] 4C Entity, "CPRM – Introduction and Common Cryptographic Elements," 2000.