コンテンツ保護技術

ネットワークと情報セキュリティ11

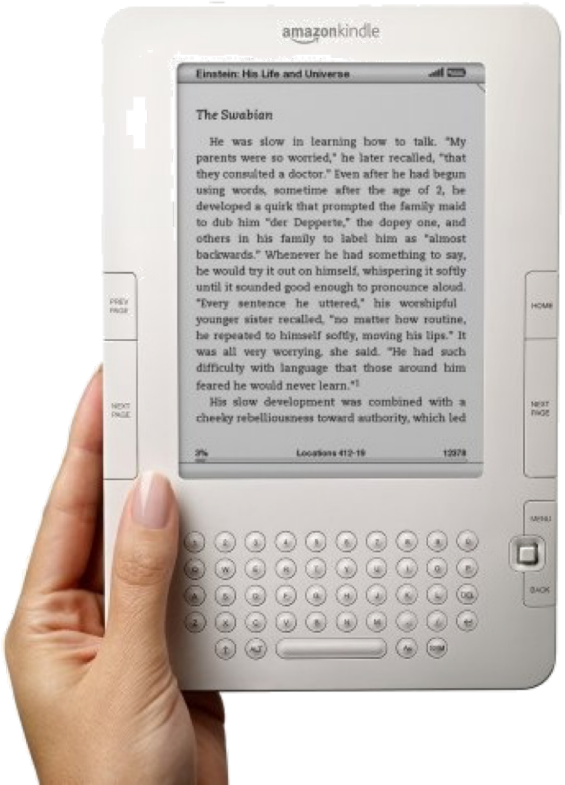
菊池　浩明

CONTENTS

- 電子書籍と著作権
- 電子透かし
- DVDと放送型暗号

電子書籍

- ipat, kindle, reader
- 新聞電子版，EBI，ケータイ小説



なぜ，日本の出版社は出遅れたか？

- 理由1. ePubは縦書きに対応していないから.
- 理由2. アップルが販売価格の3割を売買手数料として取ってしまうから．街の本屋が潰れてしまう.
- 理由3. 電子化したら…

答) 著作権が守られないから

- 2015年12月3日
  - 発売前の漫画雑誌をアップロード・著作権侵害と電子出版権侵害で再逮捕
  - 「週刊少年マガジン」に連載中の「七つの大罪」の誌面をWebサイト「RED HAWK」に掲載することを企て，「週刊少年ジャンプ」に連載中の「ONE PIECE」，「BLEACH」を雑誌の発売前に、デジタル化し、画像ファイルを権利者に無断でサーバコンピュータにアップロード

http://www2.accsjp.or.jp/criminal/2015/1181.php

Winnyによる被害総額は100億円

- コンピュータソフトウェア著作権協会（ACCS）2006年コンテンツ実態調査
  - 21万Winnyユーザ
  - 61万個の音楽ファイル(4.4億円相当）
  - 61万個のビジネスソフト(19.5億円相当)
  - 117万個のゲーム(51.3億円相当)
  - 18万個のアニメーション (17.2億円相当）

不正ソフトウェア総額トップ5

順位	国	不正額 [Mドル]		不正コピー率	
		2013	2017	2013	2017
1	米国	$9,737	$8,612	18 %	15%
2	中国	$8,767	$6,842	74%	66%
3	インド	$2,911	$2,474	60%	56%
4	ブラジル	$2,851	$1,665	50%	46%
5	フランス	$2,685	$1,996	36%	32%
11	日本	$1,349	$982	19%	$16%
番外	ジョージア	$40	$22	90%	81%
	モルドバ	$57	$35	90%	83%
平均				43% (+1%)	

出典 BSA 2013 グローバルソフトウェア調査
（86か国，22,000人ユーザ調査）

プロテクト破り DeCSS

- CSS (Contents Scrambling System)
  - 松下＆東芝の提案したDVD暗号化方式
  - 40bit共通鍵暗号（マスタ鍵，ディスク鍵，タイトル鍵）
  - 1999 ノルウェイの高校生(Jon Johansen)が公開

http://www-2.cs.cmu.edu/~dst/DeCSS/Gallery/

DeCSS開発者

- Jon Lech Johansen
  - 15歳でdeCSSを開発
  - 2002年ノルウェー検察当局は著作権法違反として起訴
  - 2003年無罪判決
- なぜか罪を問われなかったのか？

http://nanocr.eu/

著作権保護法

- 知的財産権
  - 工業所有権（特許，実用新案）
  - 著作権（文化的な著作物）
- 著作権
  - 著作物：論文，小説，楽曲，歌詞，絵画，地図，写真，映画，ゲームソフト，プログラム，
  - 登録不要（著作物を創作したら権利発生），
  - 著作者の**死後50年**まで保護
- 著作者の権利
  - 著作者人格権： 公表権，同一性保持権
  - 著作権（財産権）： 複製権，上映権，公衆送信権，譲渡権

著作物を自由に使える例

私的利用のための複製	第30条	自分自身や家族など限られた範囲内で作る複製.
図書館などでの複製	第31条	図書館の利用者に対する複製
学校における複製	第35条	教育者と授業を受けるものは授業目的での複製. 試験問題(36条), 教科書(33条).
非営利目的の演奏会	第38条	料金を取らない上映, 演奏.

それって違法？

- Q1. 宿題にウェブサイトの文書や写真を無断
- Q2. 文化祭でゲームセンターを開いた.
- Q3. 教育目的で有料ソフトをコピーしてインストールした.
- Q4. アカデミック割引ソフトを卒業後も使った.
- Q5. 無料配布のパンフレットにキャラクター画像を使用.
- Q6. バンコクで極安ソフトウェアを購入した.

教育機関における複製

- 著作権法35条1項で規定される条件
  - （1）営利を目的としない教育機関であること
  - （2）教育を担当している教員等やその授業を受ける者が複製すること
  - （3）公表された著作物であること
  - （4）授業の過程における使用を目的とすること
  - （5）必要と認められる限度内であること
  - （6）著作物の種類・用途、複製の数・態様に照らして著作権者の利益を不当に害しないこと

	現行	改正著作権法 (2018/5/25改正)
35条1項	授業目的の **複製**OK	授業目的の複製，公衆送信，公の伝達 OK
35条2項	授業目的の **同時公衆送信**OK	上記の公衆送信においては補償金を支払う
35条3項		同時公衆送信については支払い不要

ディジタル著作権管理
Digital Right Management (DRM)

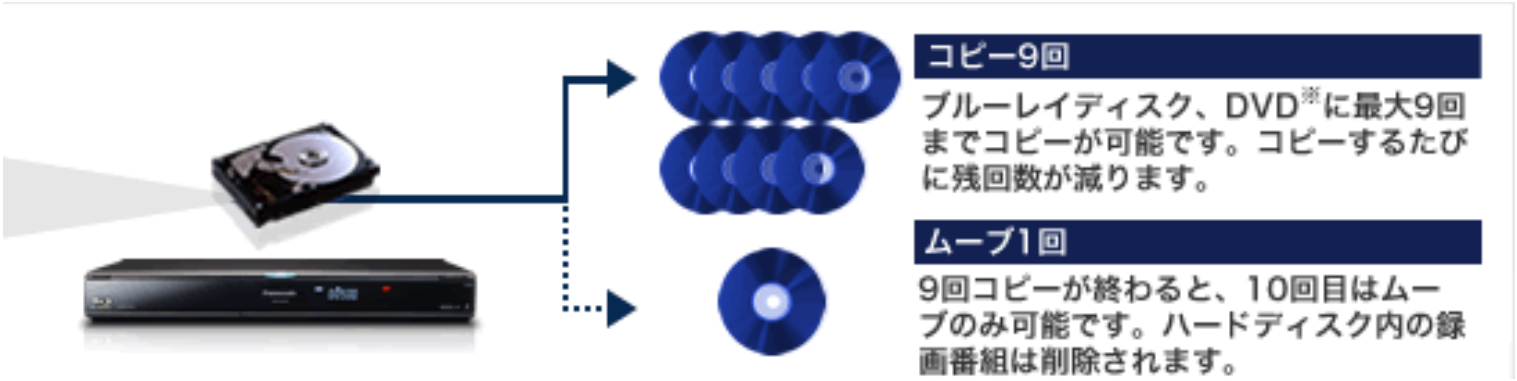
技術	開発	対象	備考
CSS	東芝，パナソニック	DVD-Video	アクセス制御技術
AACS	AACS	BD-ROM	
CPRM	インテル，IBM，東芝，パナソニック	DVD-R, RAM, RW, SDメモリー	
B-CAS	パナソニック	地上波ディジタル	機器認証
FairPlay	Apple	iPod, iPhone	

2種類のDVD

- 三菱化学メディア
  - DHR47JP50YB
  - データ用DVD-R 4.7GB 16倍速対応 50枚
  - 1,780円
- 三菱化学メディア
  - VHR12DP50H5
  - 録画用DVD-R 120分 1-8倍速 CPRM対応 50枚
  - 1,980円

ダビング10

- 2008年7月4日運用開始
  - ディジタル放送の私的利用規定
  - 従来:　　ムーブ1回
  - ダビング10:　コピー9回＋ムーブ1回



http://panasonic.jp/diga/info/index.html

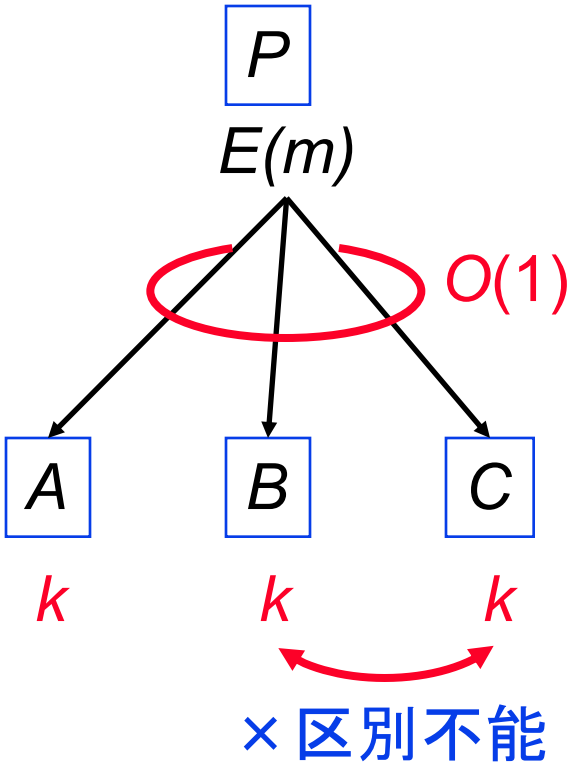
著作権保護対策

- 1. 専用アプリ
  - ipad, kindle, ebi-reader
- 2. コピー制御技術
  - CPRM
- 3. 情報ハイディング
  - 電子透かし

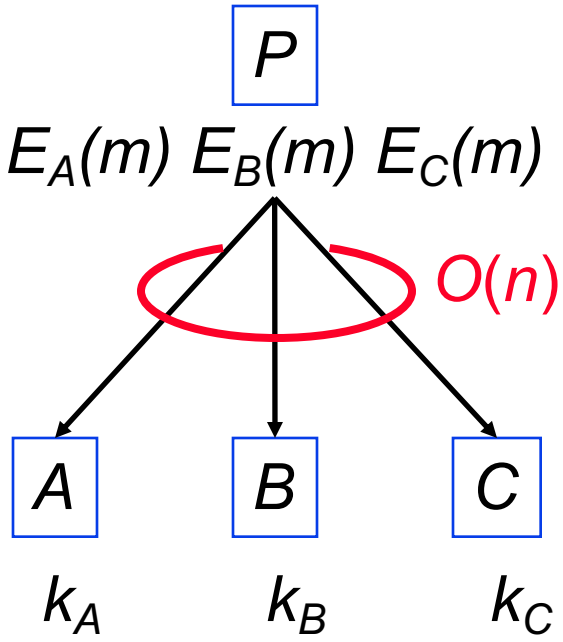
放送型暗号

ナイーブな2方式

- 共通鍵



- 個別鍵

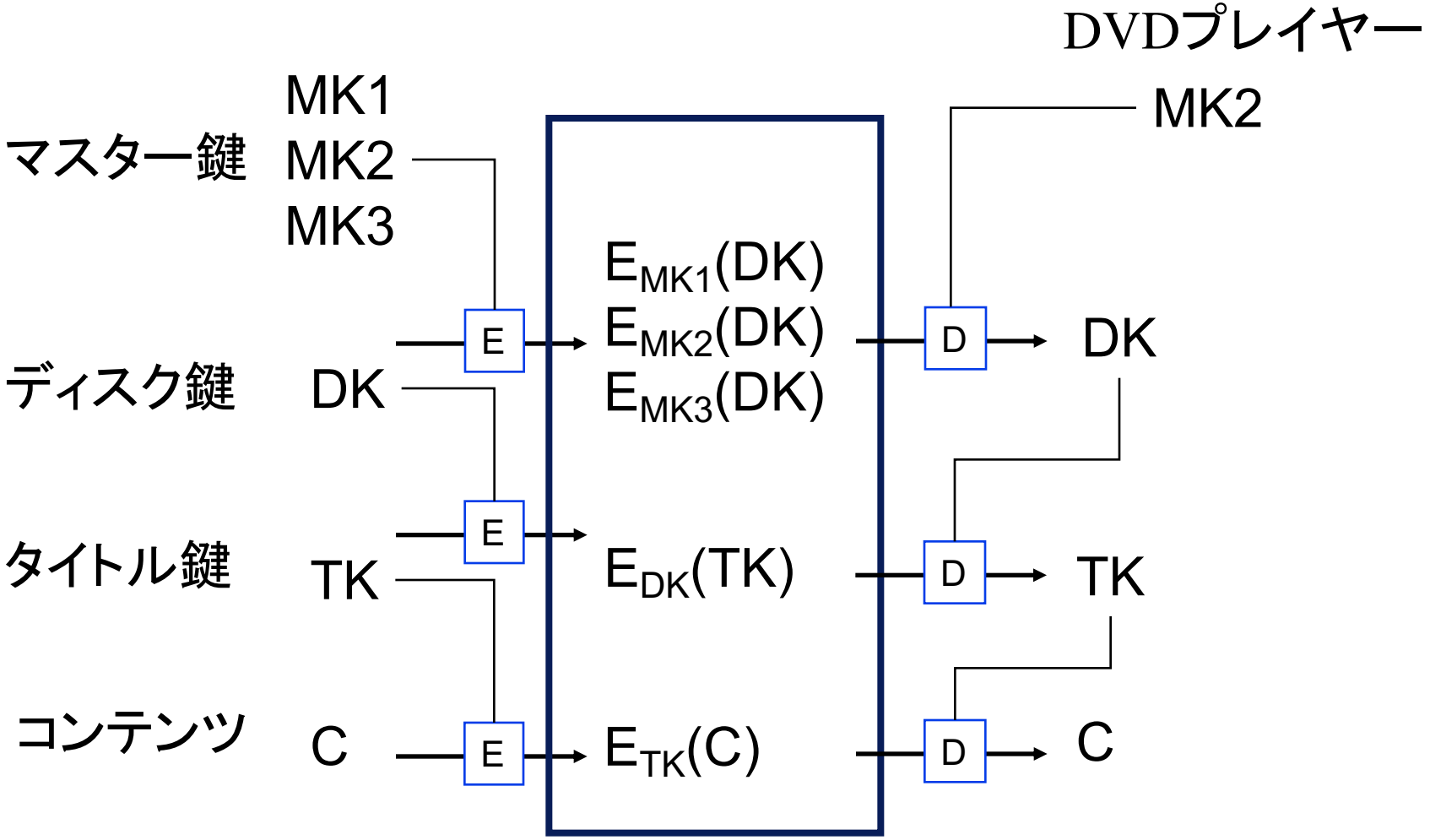


× 個別配信コスト

CPPM/CPRM

- Content Protection for Prerecorded Media/CPRM（Content Protection for Recordable Media）
  - DVDのコピー制御技術
  - プレイヤー: デバイス鍵
  - DVD: メディア鍵

CSS (Content Scrambling System)



問題点

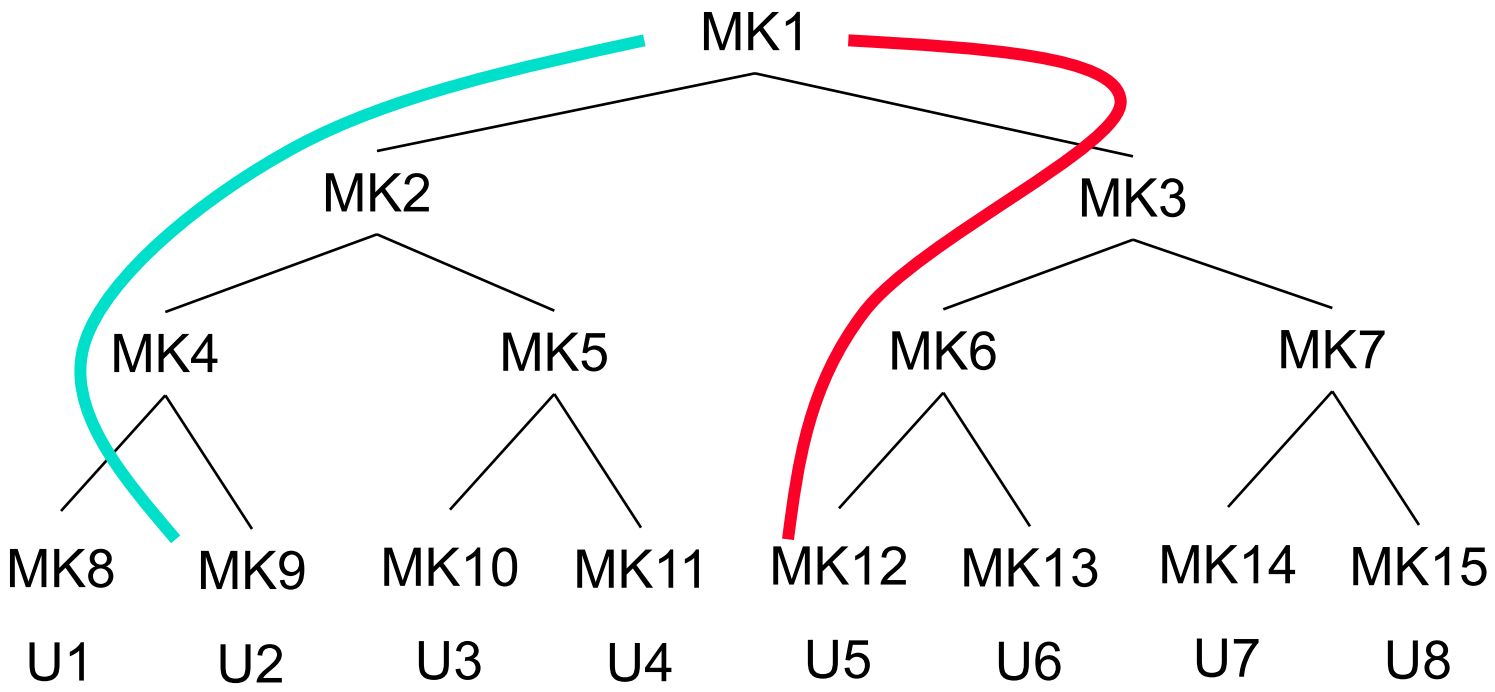
- マスター鍵のどれか一つが漏れても復号を止められない.

放送暗号の原理

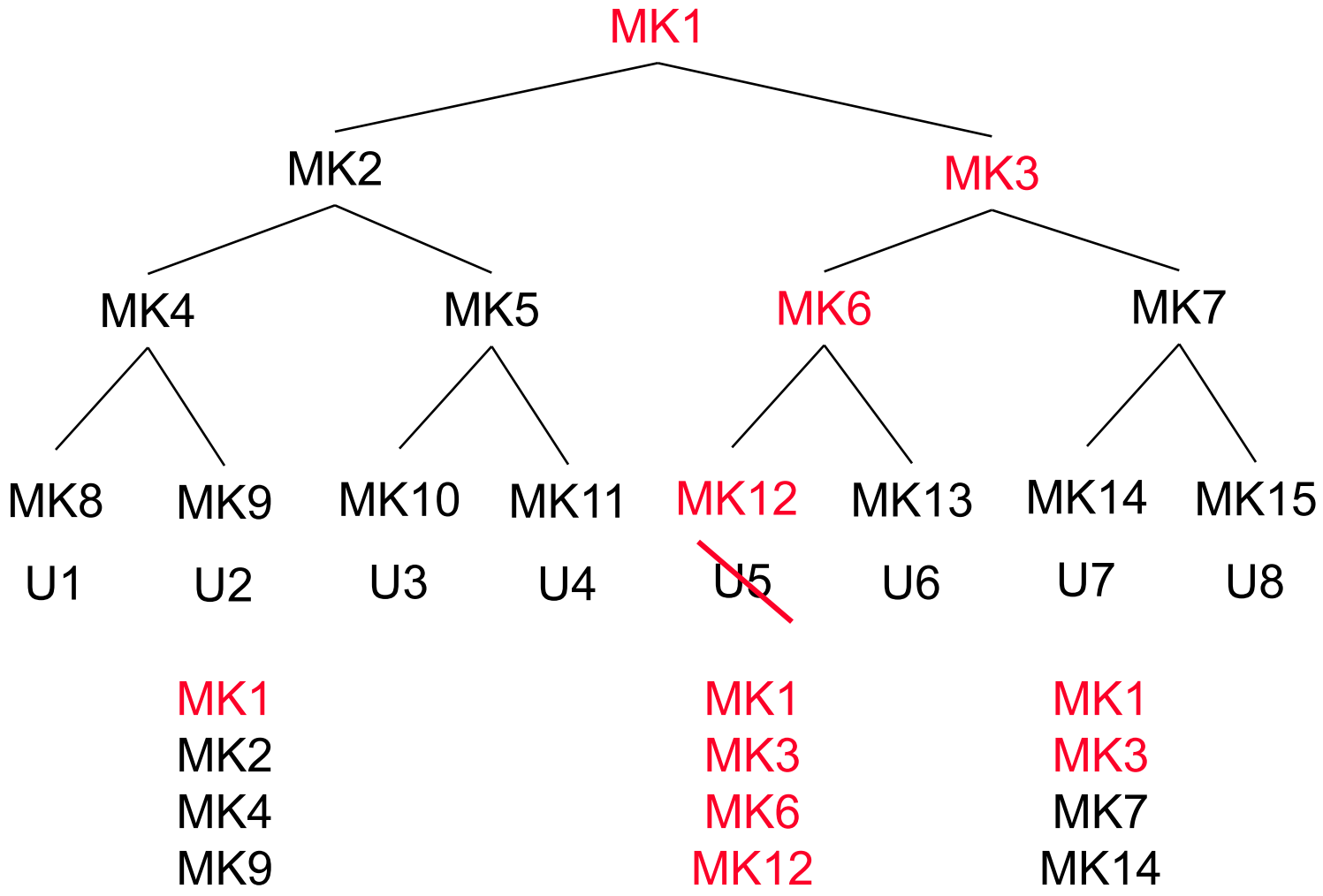
- アイデア
  - 各ユーザ(プレイヤー)に複数の鍵を配布.

U1	U2	U3	
MK1		MK1	
MK2	MK2		
	MK3	MK3	
X	○	○	MK3で暗号化
○	X	○	MK1で暗号化
X	X	○	?

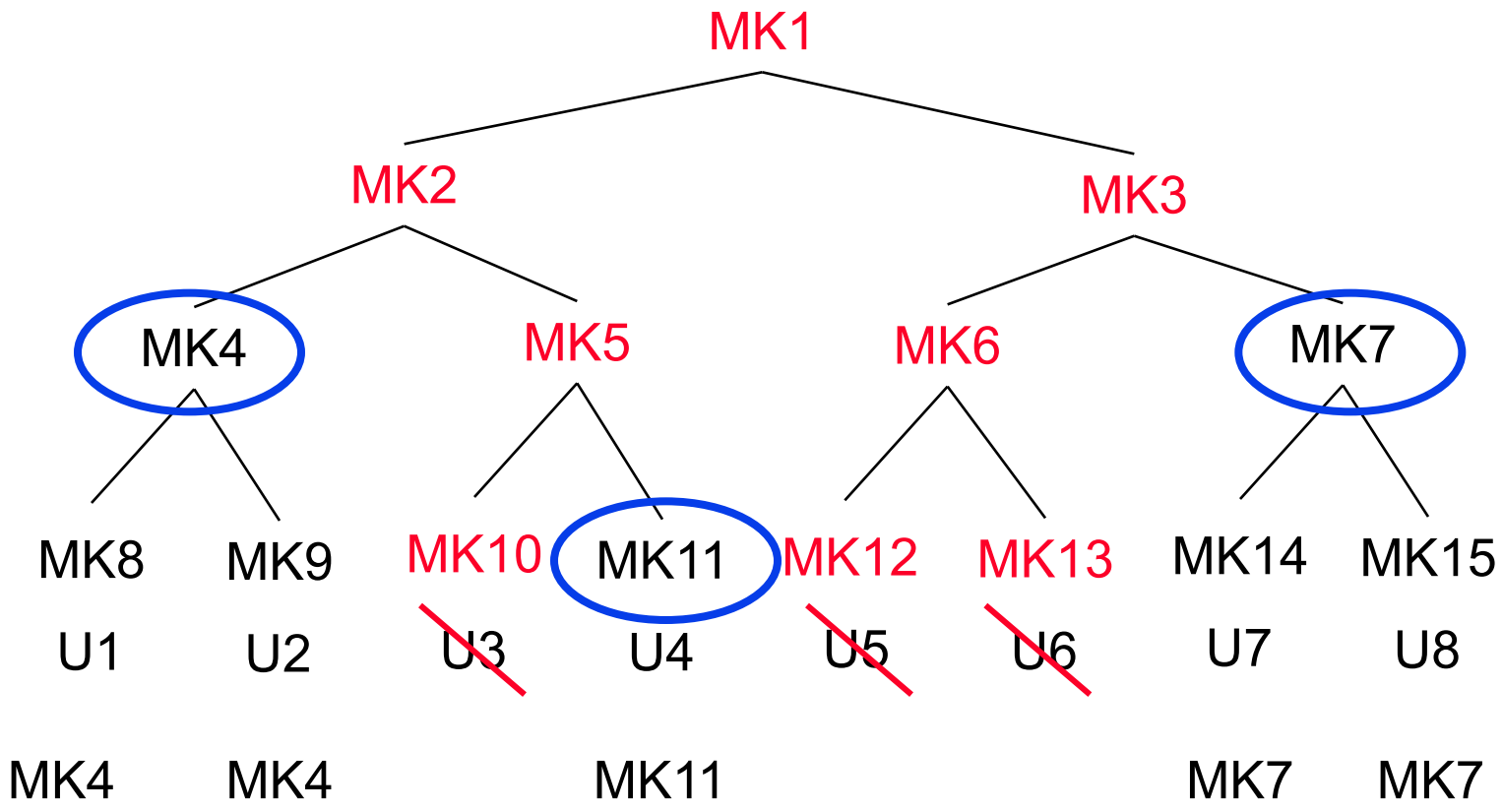
LKH (Logical Key Hierarchy)



2. U5の失効


MK1
MK2
MK3
MK4
MK5
MK6
MK7
MK8
MK9
MK10
MK11
MK12
MK13
MK14
MK15
U1
U2
U3
U4
U5
U6
U7
U8
MK1
MK2
MK4
MK9
MK1
MK3
MK6
MK12
MK1
MK3
MK7
MK14

3. R={U3, U5, U6}の失効



鍵集合　S = {MK4,MK11,MK7}

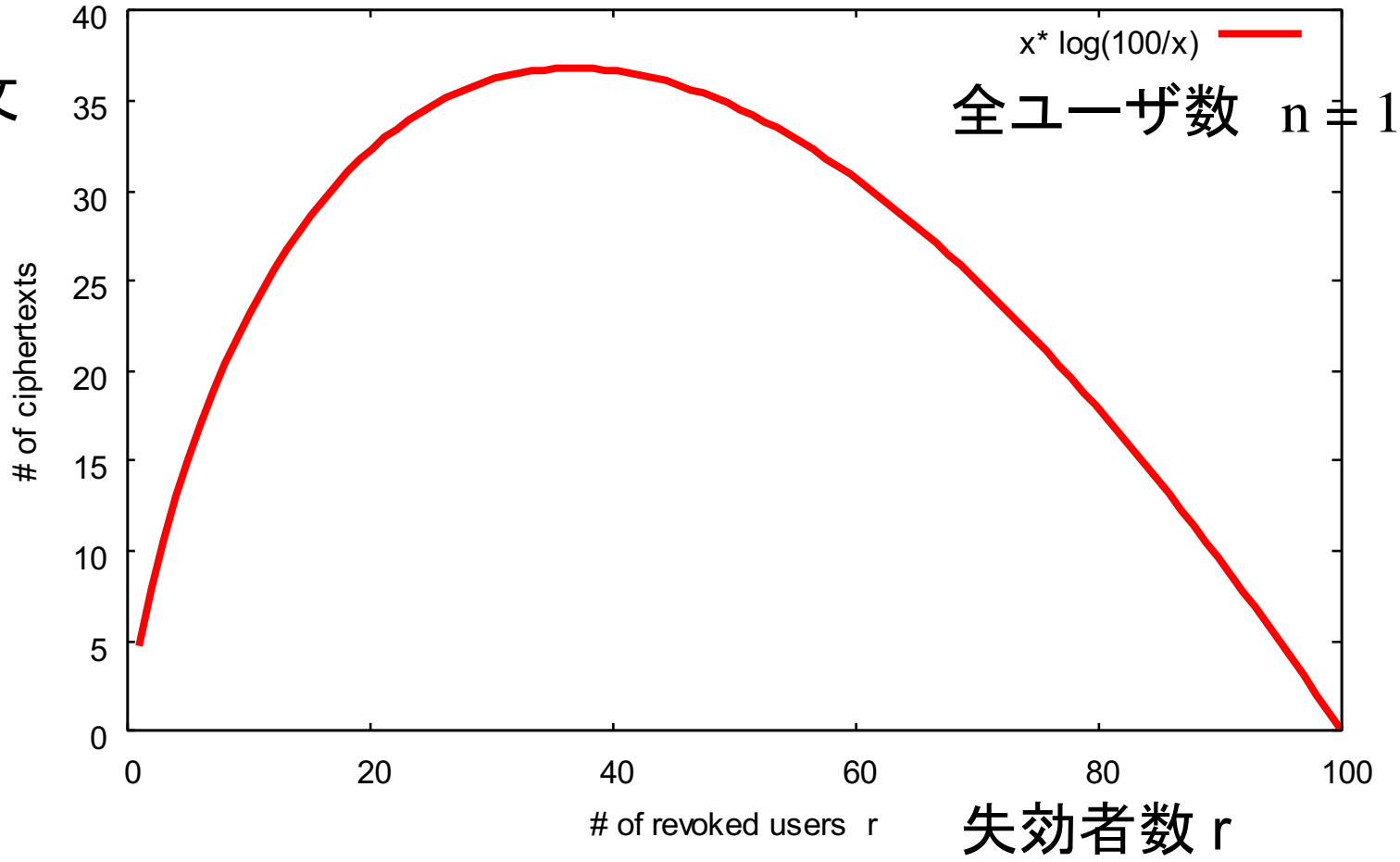
ディスク鍵　$E_4(DK)$, $E_{11}(DK)$, $E_7(DK)$

管理する鍵の数

- ユーザ数 n = 8
- 木の高さ h = 3
  - $n = 2^h$
  - $\log_2 (n) = h$
  - 管理する鍵数: h+1 = 4 [個/ユーザ]
- 失効者数r
  - r=0 の時，暗号文 $E_{MK1}(DK)$ 1個
  - r=1 の時，暗号文 $E_{MK2}(DK)$, $E_{MK7}(DK)$ 2個
  - rの時，？

暗号化コスト(暗号化回数)

暗号文数



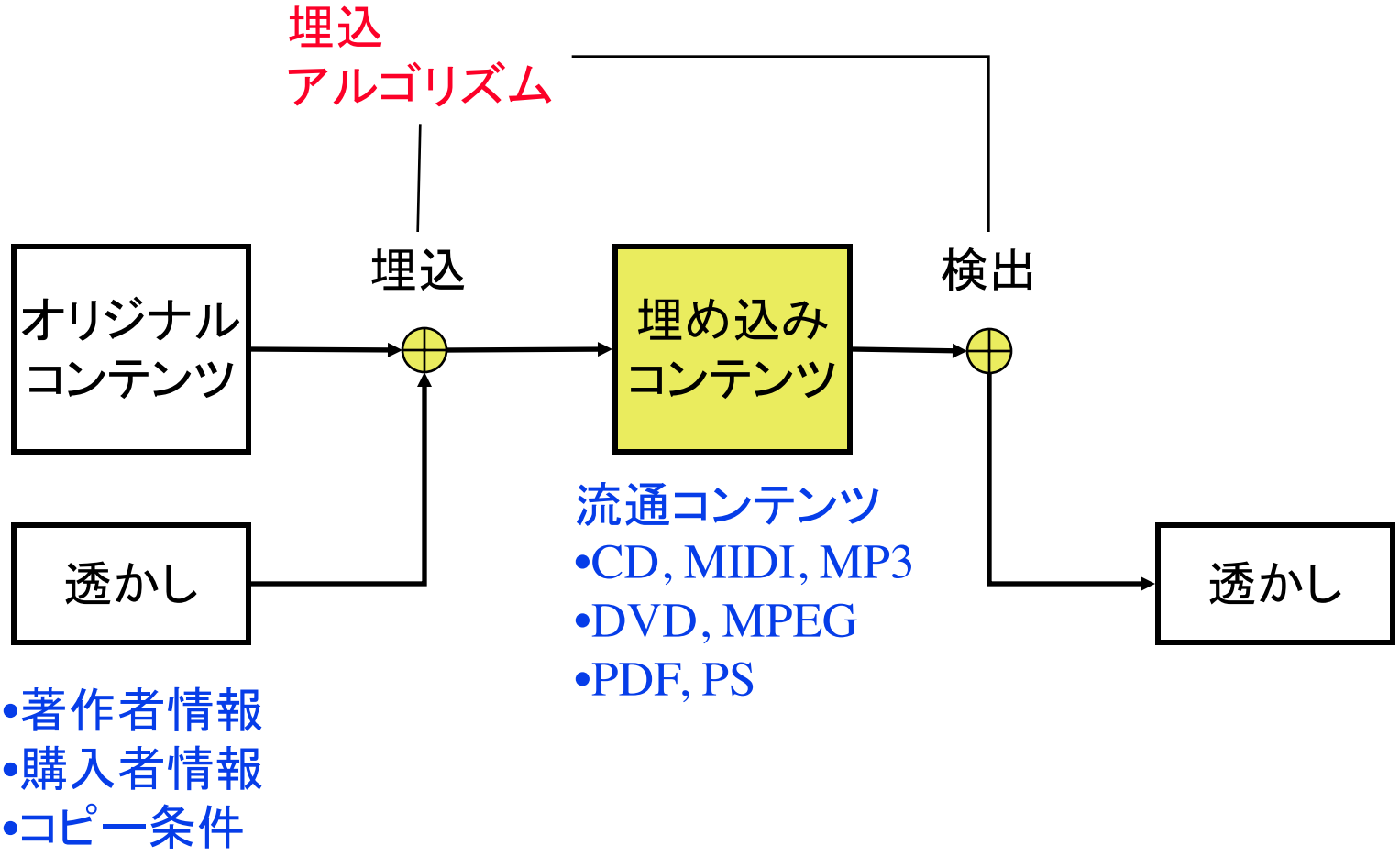
電子透かし

目的

- 1. 著作権保護
  - コンテンツの中に著作者の情報を隠す

- 2. コピー制御
  - コンテンツの中に購入した日や場所や購入者のデータを隠す

情報ハイディングのモデル



情報ハイディングの原理

- 人間の知覚(視覚，聴覚)で認識出来ない領域へ情報を埋め込む
  1. 歪曲法

     意味を変えずにコンテンツを歪ませる．統計量を操作する．
  2. 置換法

     コンテンツの冗長領域を置き換える
  3. ドメイン変換法

     コンテンツを直交変換して，周波数領域に埋め込む

1. LSB置換法

1. 原画像

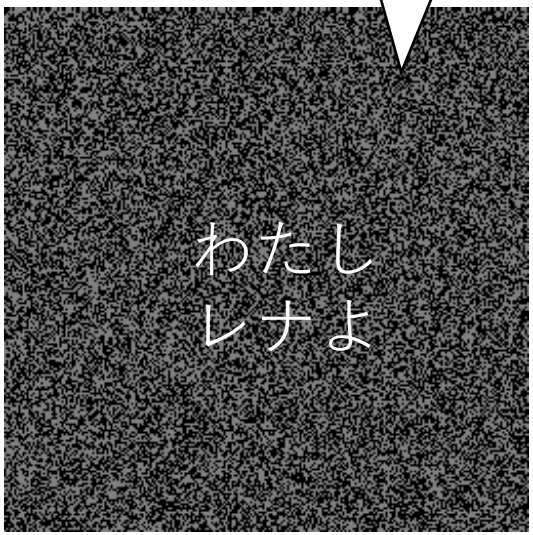
10110010

MSB(最上位ビット)
LSB (最下位ビット)

2. MSBのみ

これを任意の
画像に置き換える
（埋め込み）

3. LSBのみ



LSB置換の例

- 画像
  - サイズ: n x mピクセル
  - I(i, j) : i行j列の画素値 (最大値 Max_i=FF)
  - M=M_0…M_B(2) : 埋め込むメッセージ（画像）
  - K(i,j) : 埋め込み画像の画素値
- 透かしの埋込み
  - K(i+k,j) = I(i+k, j) & FE | M_k (k=1,..,B)
    - » 例) I(0) = 1C, I(1) = 1C, M=2=$10_{(2)}$
      K(0) = 1D, K(1)=1C
  - 下位Lビットに埋込む時: I(i+k, j) & $\overline{(1<<L)}$ | M_k
- 透かしの抽出
  - M_0 = K(0) & FE = 1, M_1 = K(1) & FE= 0

透かしの評価

- 画質の評価
  - SN比 (Peak Signal-to-Noise Ratio)

$$PSNR = 20\log_{10}\frac{MAX_I}{\sqrt{MSE}}$$

  - 平均二乗誤差 MSE(Mean Squared Error)

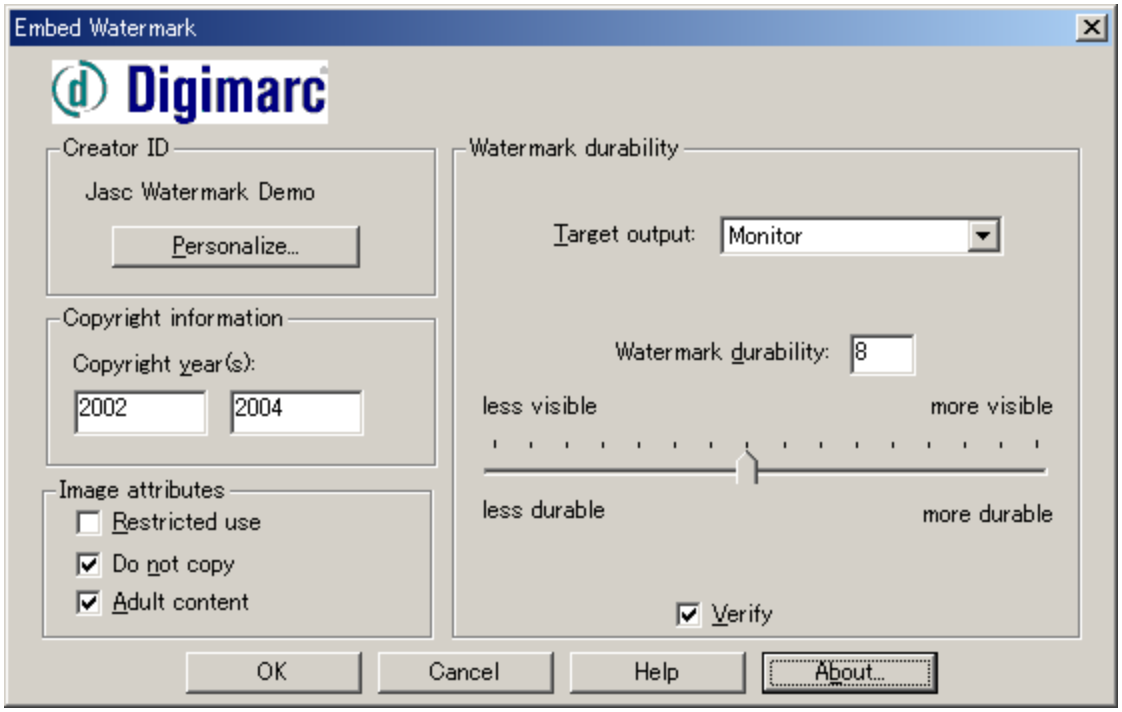
$$MSE = \frac{1}{mn}\sum_i\sum_j (I(i,j) - K(i,j))^2$$

LSB置換の限界

- 攻撃に対する安全性が弱い
  - 透かしを壊す，取り除く.
- 攻撃の種類
  - 変換（回転，縮尺，拡大）
  - ラプラシアン攻撃（ノイズ付加）
  - JPEG攻撃（圧縮率の変化）

2. Digimarkの置換法（原画像）

2. 埋込


Embed Watermark
Digimarc
Creator ID
Jasc Watermark Demo
Personalize...
Copyright information
Copyright year(s):
2002
2004
Image attributes
Restricted use
Do not copy
Adult content
Watermark durability
Target output:
Monitor
Watermark durability:
8
less visible
more visible
less durable
more durable
Verify
OK
Cancel
Help
About...

まとめ

- 知的財産権には，特許などの（　　）権と小説や歌詞を対象とした（　　）権がある．DVDなどをコピーするのは（　　）の範囲内で許されている．
- CSS, CPRMなどの暗号化によるコピー制御の技術を（　　）という．LKHは木構造でデバイス鍵を管理し，不正なデバイスを（　　）する．これを（　　）暗号という．
- 知覚出来ない領域に（　　）者の情報を埋込むことで著作権を保護する技術を電子（　　）という．コピー制御の目的で，（　　）者名を埋め込む．