著作権を支える技術

慶應義塾大学
環境情報学部
中村　修

コンテンツ保護に関連した技術

- Copy Protection/Copy Once
- DRM
- Digital Watermarks

Copy Protection

- アナログメディアのコピー防止技術
  - マクロビジョン／カラーストライプ
  - CGMS-A(Copy Generation management System-Analog)
- デジタルメディアのコピー防止技術
  - CD関連のコピー防止技術
  - DVD関連のコピー防止技術、CSS(Content Scramble System)など
  - DTCP(Digital Transmission Content Protection

マクロビジョン

- Macrovision社が開発したコピーガードシステム
- ビデオデッキに搭載されているAGC(Automatic Gain Control:輝度入力信号の自動調整機能）を誤動作させる。（テレビにはこの機能は入っていない）
- DVDデッキなどでも、この信号を発見すると録画停止になるものもある。
- カラーストライプと呼ばれるカラーバースト信号をビデオ信号に付加する手法も用いられている。
- 業務用などAGC機能をオフにできるものだとコピーできる

CGMS-A

- CGMS-A(Copy Generation Management System - Analog)
- EIAJ(電子情報技術産業協会）の規格 (CPR-1204)
- VBI(Vertical Blanking Interval)にIDを畳み込む方法
- 世代管理(Copy once）などの制御をおこなえる
- ビデオデッキ間の制御なので、非対応のものには効果なし
- 接続ケーブル上での信号除去に弱い

CD関連

- データCDには多種多様なものがある。
  - セクター操作方式
    - Alpha-ROM, TAGES, Bleem, RingPROTECH, SafeDisc, etc
  - 暗号化による方式
    - ROOT, DiskGuard, LaserLock, etc
- オーディオCD
  - CCCD
    - イスラエルのMidbartech社が開発
    - AVEX社で有名
    - Redbook規格違反
    - 普通のプレイヤーなどでも再生できない場合がある

DVD関連のコピーガード

- CSS(Contents Scramble System)
  - 松下などが開発したコピープロテクション
  - 多くのDVD-VIDEOが採用
  - コンテンツを暗号化、鍵を書き込めない領域に保存
- CPRM(Content Protection for Recordable Media)
  - 書き込めない、変更できないエリアBCA(Burst Cutting Area)に、メディアに依存したID
  - このIDを使ってコンテンツを暗号化
  - CPRM対応の再生器機が必要

DVD関連（続き）

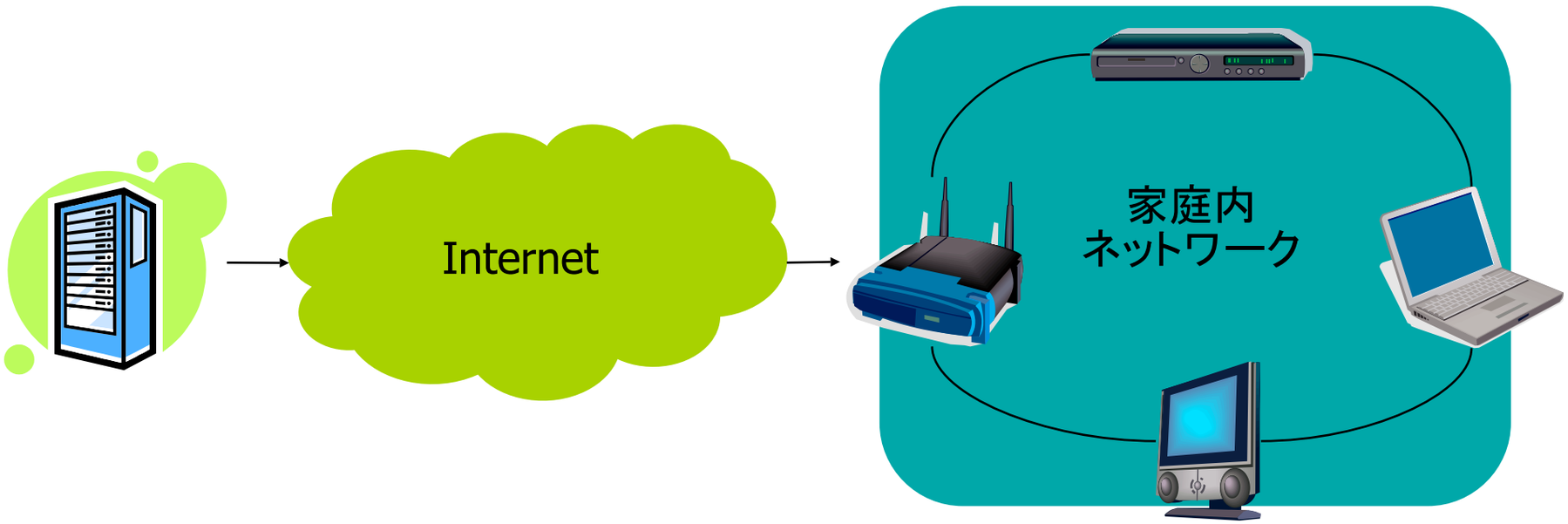
- ARccOS
  - Sonyが開発したコピープロテクション
  - DVD内のセクターを意図的に操作しコピー防止
- RipGuard
  - Macrovision社が開発
  - ARccOSと類似技術

ITU-T FG-IPTVにおけるセキュリティ議論

- FG-IPTVにて提出された要求条件
  - 機器認証
  - ユーザ認証
  - ドメイン管理
  - アクセスコントロール
  - コピープロテクション
  - プライバシ保護
  - DoS攻撃，ウィルス
  - 不正利用者のトレース

IP放送におけるセキュリティ問

- 前提条件
  - ネットワーク上に存在する様々な機器
    - STB，PC，情報家電，ルータなど
    - →それぞれの機器が情報の送受信をできる



考えられる脅威

- なりすまし
  - プロバイダ
    - 悪意のある第三者が正規のプロバイダのフリをしてユーザにコンテンツを配信
  - ユーザ
    - 悪意のある第三者が正規のユーザのフリをしてコンテンツを受信
- 盗聴，改ざん
  - 途中経路において通信内容を盗聴

B-CAS(1/5)

- BS-Conditional Access Systems(B-CAS)社が運営
  - 対象：
    - 地上デジタル放送，BSデジタル放送，110度CSデジタル放送など
- B-CASカードを対応受信機に挿すことによって利用

写真：
(カード)http://www.b-cas.co.jp/about.html
(デッキ) http://pc.watch.impress.co.jp/docs/2003/0303/kai21.htm

B-CASカードスロット(左)

B-CAS(2/5)

- 用途
  - BS，地上デジタル受信契約確認
    - 平成16年4月より開始
  - 契約内容確認
    - 有料コンテンツ放送，PPV，自動表示メッセージ，データ放送など
- コピーコントロール
  - 1回のみ録画可能
  - 平成16年4月より開始

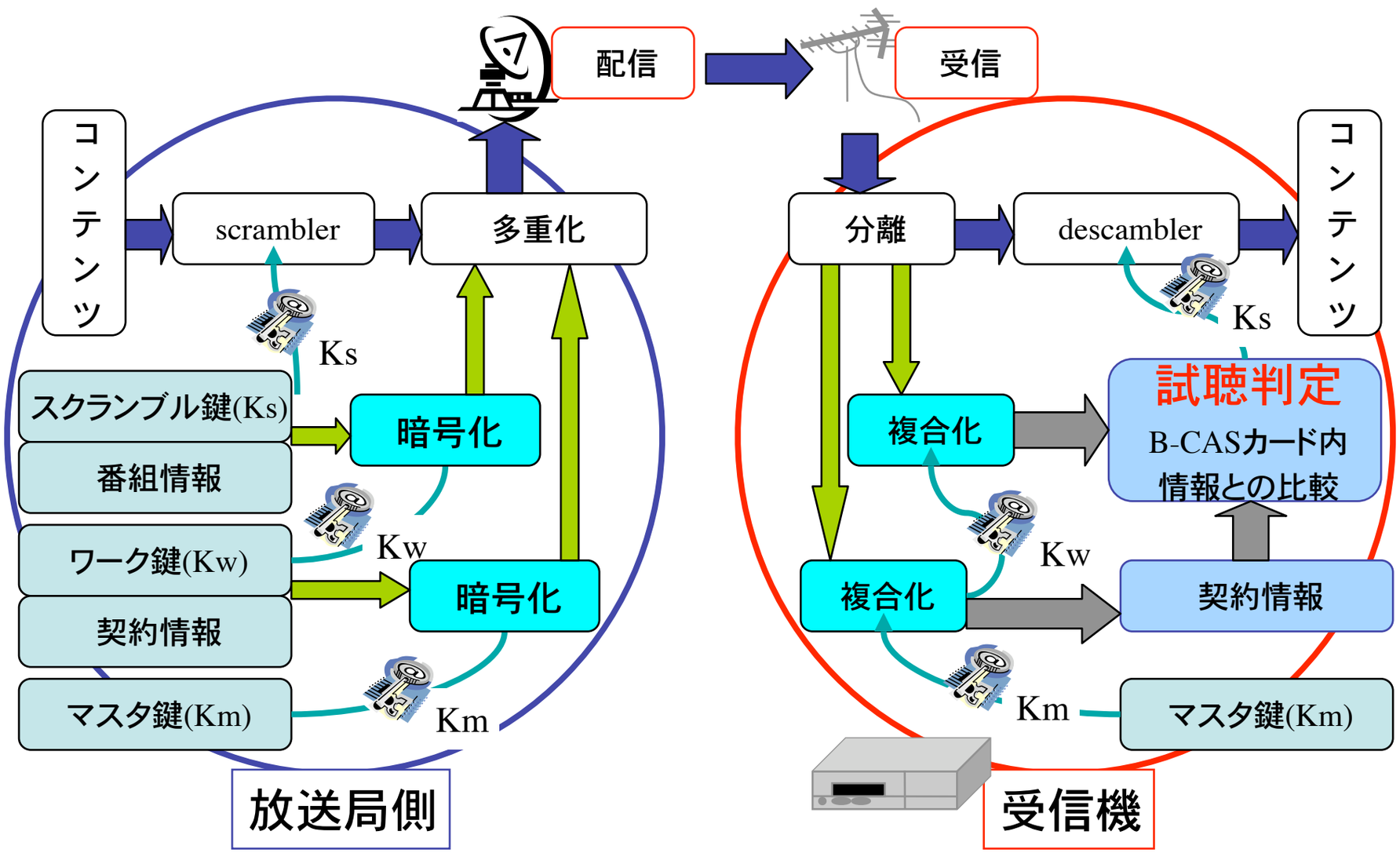
B-CAS(3/5)

- 3種類の鍵を使用
  - Ks(スクランブル鍵)
    - 信号にスクランブルをかける
    - 数秒おきに変更される
    - 共通ECM
  - Kw(ワーク鍵)
    - Ksを送る為のスクランブル鍵
    - 共通ECM
  - Km(マスタ鍵)
    - Kwを送る為の鍵
    - 個別契約情報の伝送用鍵
    - 個別EMM

B-CAS(4/5)

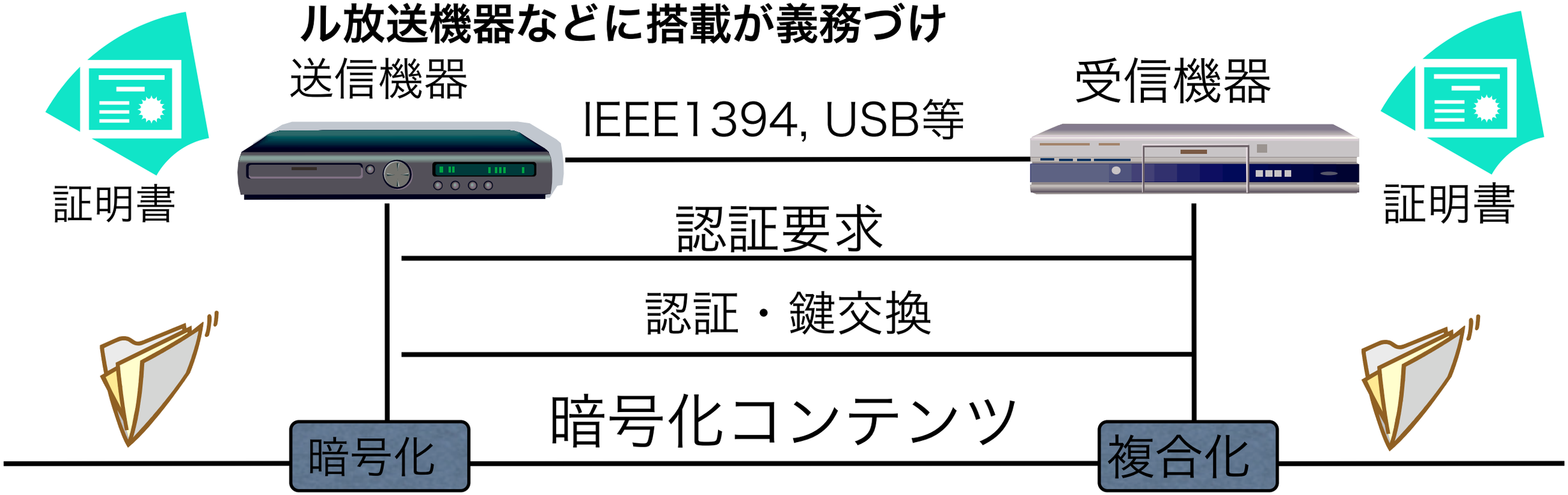
- ECM(Entitlement Control Message)
  - スクランブル解除の際に用いる関連情報のうち以下のものを扱う
    - 鍵情報(スクランブル鍵)
    - スクランブル機能の制御(有効化／無効化)
- EMM(Entitlement Management Message)
  - 契約情報や暗号を解くための鍵情報(ワーク鍵)など
  - 契約情報に応じたスクランブル鍵解除が可能
    - PPV(Pay Per View)などに利用される

B-CAS(5/5)


配信
受信
コンテンツ
scrambler
多重化
分離
descambler
コンテンツ
Ks
Ks
スクランブル鍵(Ks)
暗号化
番組情報
Kw
Kw
ワーク鍵(Kw)
暗号化
契約情報
Km
Km
マスタ鍵(Km)
放送局側
複合化
試聴判定
B-CASカード内
情報との比較
複合化
契約情報
マスタ鍵(Km)
受信機

DTCP(1/2)

- Digital Transmission Content Protection
  - IEEE1394，USBなどにおける伝送系著作権保護技術
  - DTLA社が発行した証明書を各機器が保持
    - 証明書の相互検証
    - 認証・鍵交換
    - M6暗号鍵の共有
  - 国内の家庭ネットワーク(IEEE1394, USB等)対応デジタル放送機器などに搭載が義務づけ



DTCP(2/2)

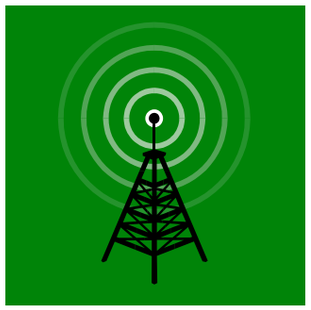
- DTCPの持つその他の機能
  - SRM(System Renewability Message)
    - 無効化すべき機器の一覧を共有する仕組み
    - 無効化リストに記載されると通信が拒絶される
  - 無制限コピー防止
    - AVストリームを受信可能な受信デバイス数の上限を策定

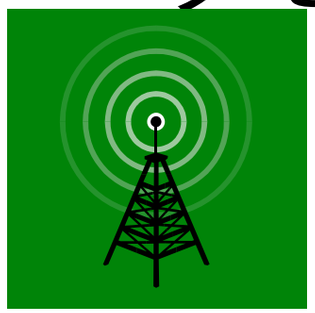
ダビング10(1/2)

- デジタル放送のコピー制御
  - 2004年4月
    - BSデジタル放送と地上デジタル放送にコピーワンスを導入
      - コピー制御信号CCI(Copy Control Information)を導入
      - 「1回だけ録画は可能だが，ダビングはできない」
      - HDDからDVDに移動(mv)する際に失敗，コンテンツを失うトラブルから利用者の不満が高まる

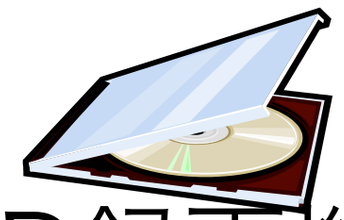
ダビング10(2/2)

ダビング10





- コピーワン



DVD録画機

×

HDD録画機

move

copy

(9回まで)

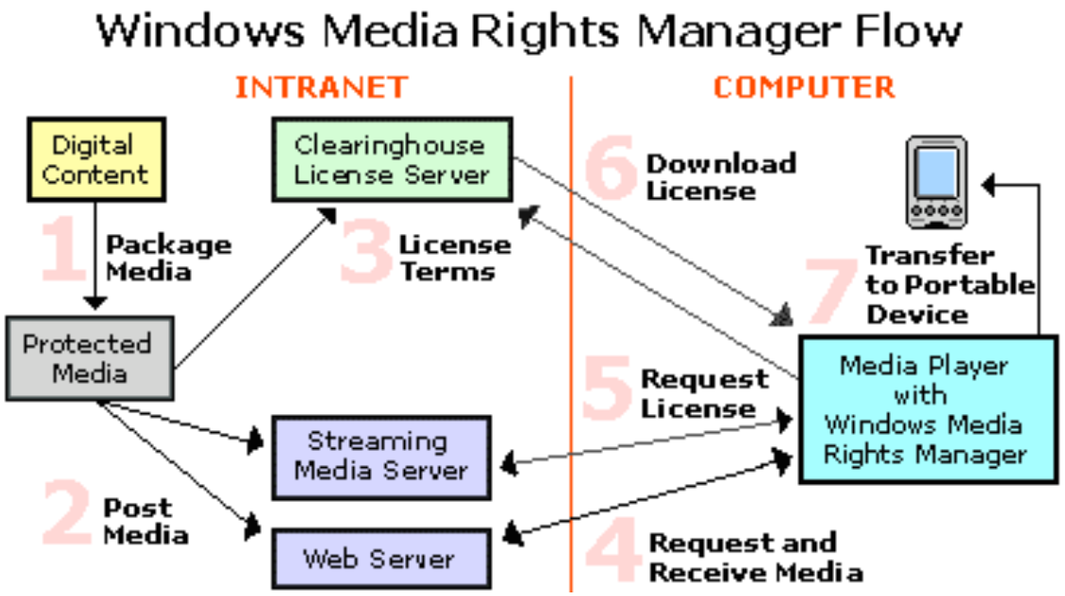
move

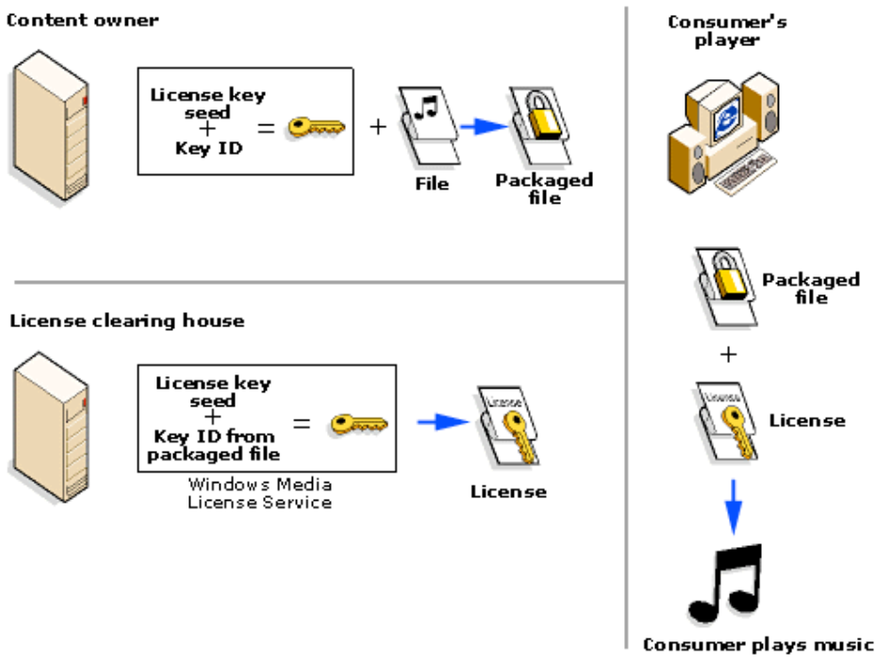
HDD録画機

主要DRM

- WMRM
  - Microsoft
- FairPlay
  - Apple Computer
- OpenMG
  - SONY
- DNAS
  - SONY
- Helix DRM
  - Real Networks

WMRM



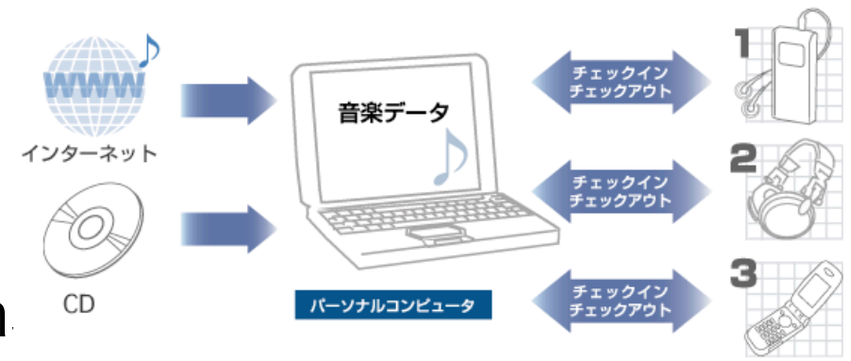


- Microsoft
- WMTのDRM
  - メディアファイルを鍵を使って暗号化
  - 鍵は別個に配布される、暗号化されたライセンス内に格納
  - ライセンスサーバを利用して認証
  - 再生回数、転送可能なデバイスの制限、有効期限などが設定可能
- ユーザの行動
  - メディアファイルをストリーミング/ダウンロードする
  - ユーザはライセンスキーを再生時に取得
    - このときに支払いなどが要求される

http://www.microsoft.com/japan/windows/windowsmedia/wm7/drm/architecture.aspx

MagicGate/OpenMG

- ソニー
- OpenMG
  - パソコン用の専用ハードウエアモジュールと対応ソフトウエアから構成され、音楽コンテンツを暗号化してハードディスクなどに記録
  - SDMI (Secure Digital Music Initiativeに準拠
- MagicGate
  - 半導体メディアと機器の間で認証を行い、認証された場合にのみコンテンツの再生を可能とする



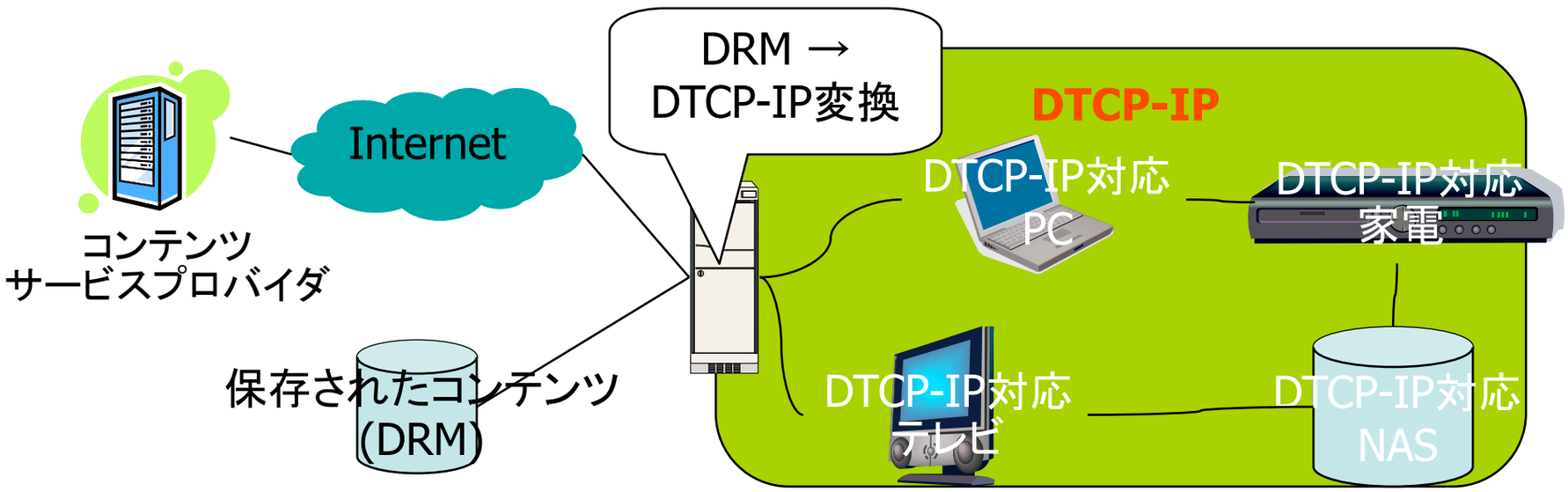
出典：http://www.memorystick.com/jp/m

Helix DRM

- Real Networks
- 2003年1月に発表
  - MCS(Media Commerce Suite)に代わるもの
- 対応フォーマットが多い
  - Real Audio, Real Video, MP3, MPEG4, H.263,など
- XMCL（eXtensible Media Commerce Language）に対応
- RealSystem iQをベース
- ５つのコンポーネント
  - Helix DRM Packager
  - Helix DRM License Server
  - Helix DRM Client
  - Helix Universal Server DRM Plug-in
  - Helix DRM Device Support

DTCP-IP

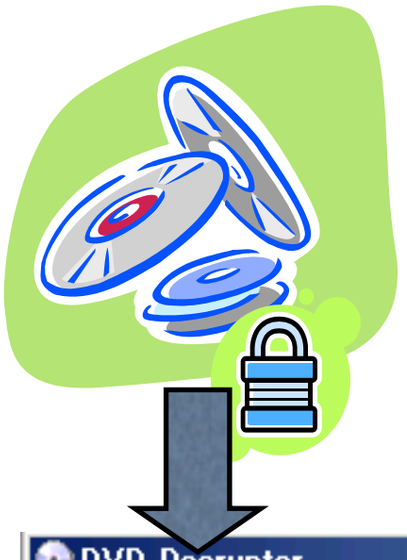
- 主に家庭内LANなどでDRM保護されたコンテンツを伝送するための技術企画
- 登場の背景
  - 多様なDRM技術の登場
    - Windows Media, OpenMG, Helixなどなど
  - 互換性無し
  - →非互換性の問題をカバーする技術が求められるように

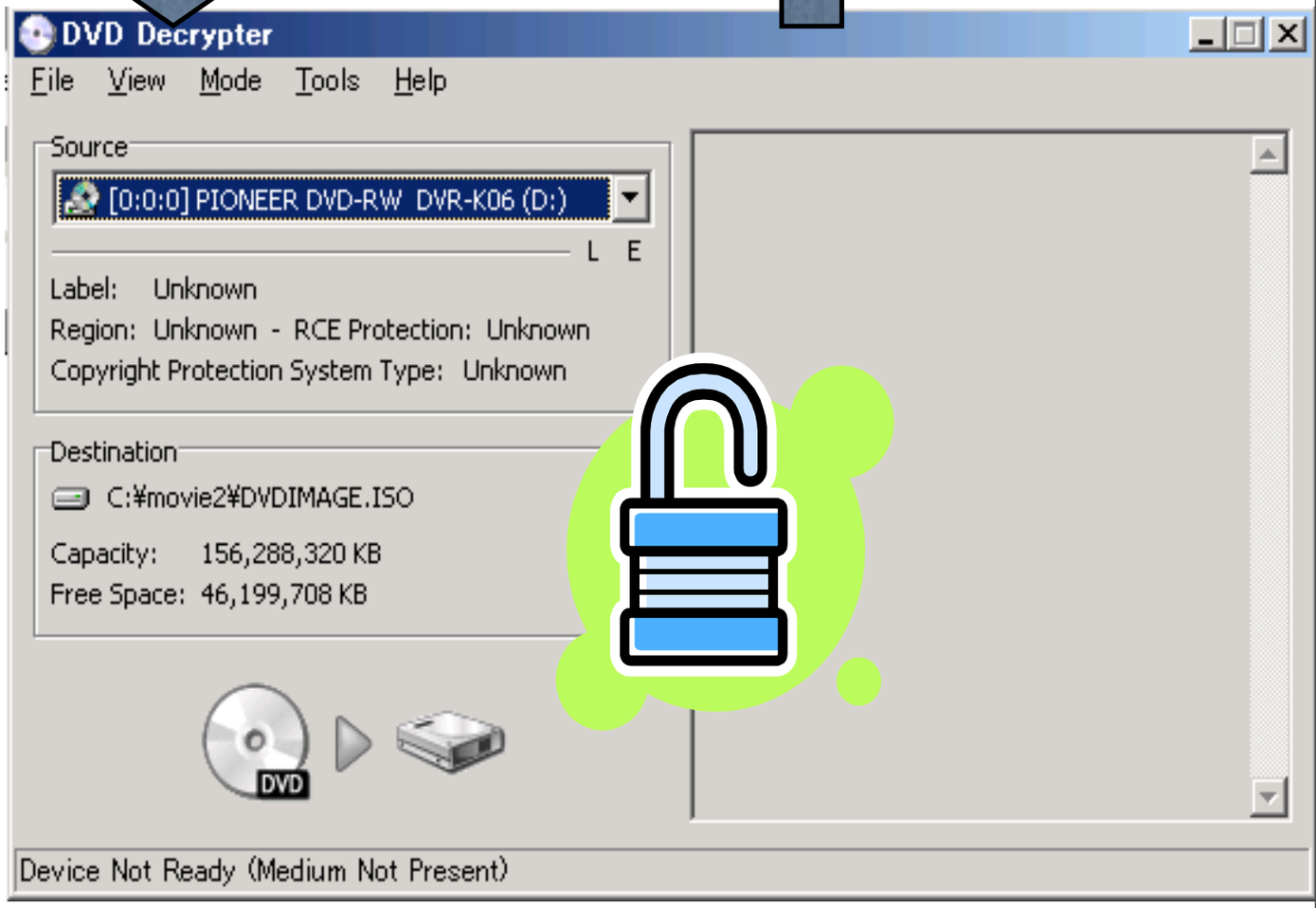


DVDの世界

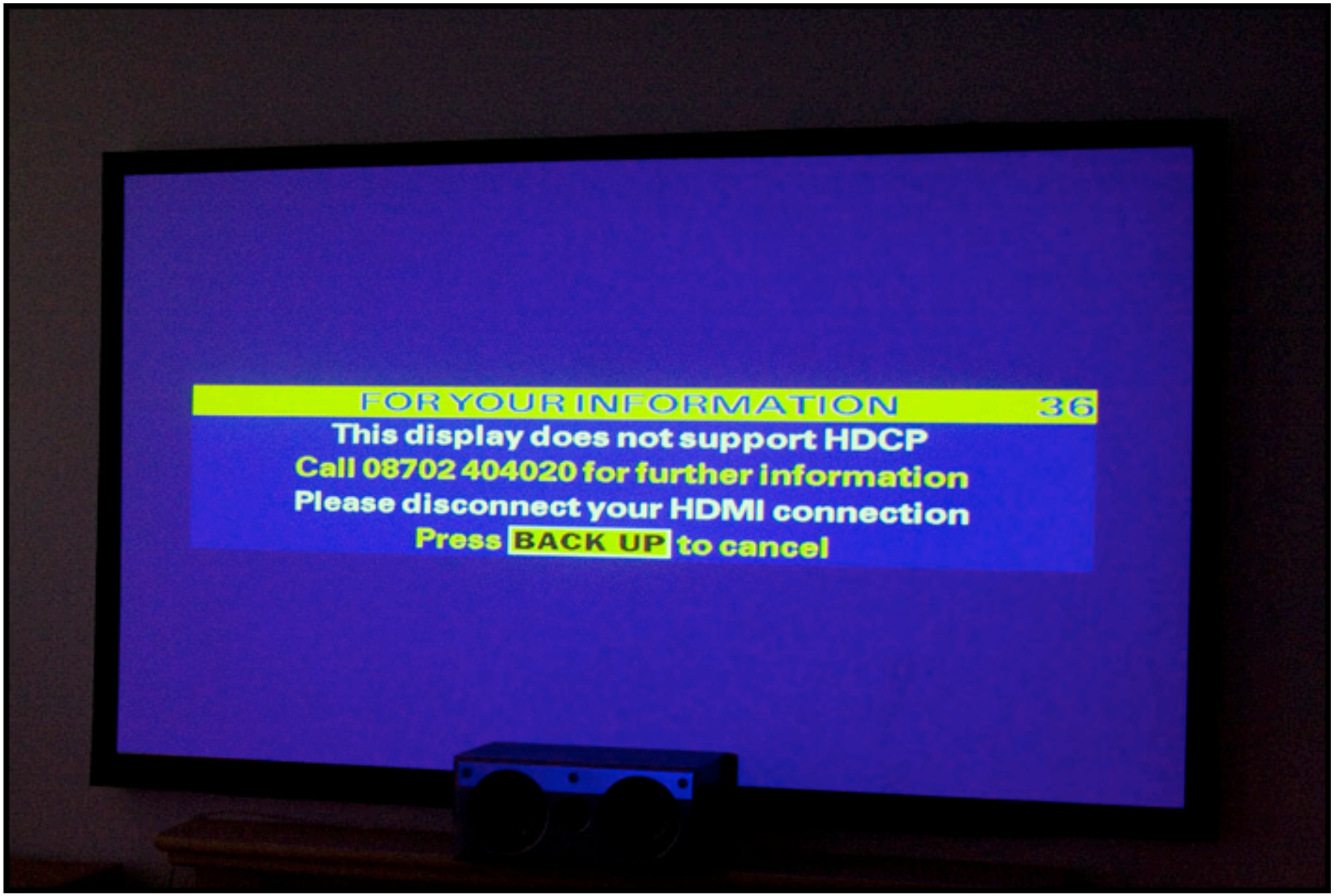
- 解かれた暗号化技術
  - リッピング(RIPPING)
- 海賊版の出現

- ならば・・・
  次世代HDDVD,
  Blu-ray では・・・





HDCP

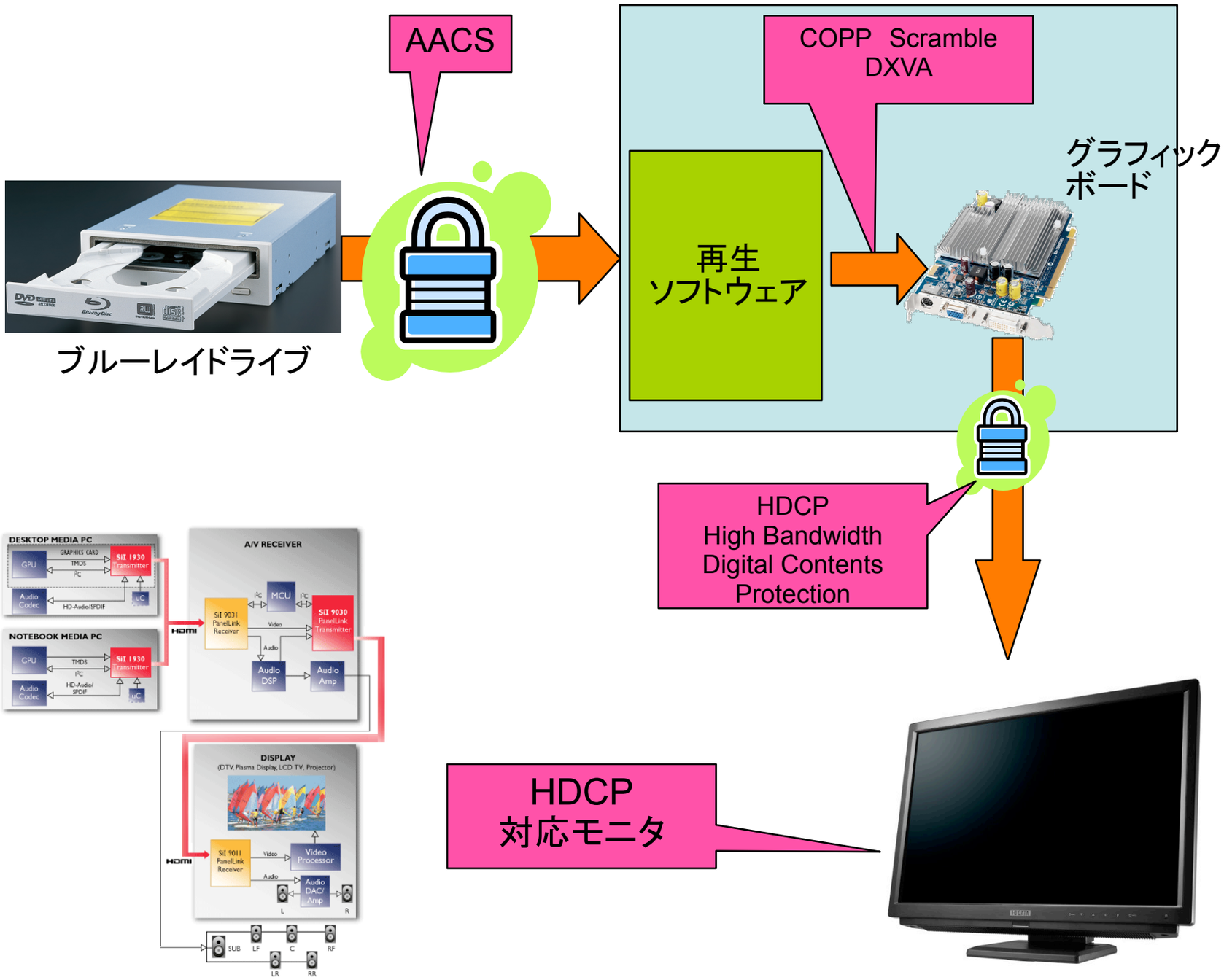

FOR YOUR INFORMATION 36
This display does not support HDCP
Call 08702 404020 for further information
Please disconnect your HDMI connection
Press BACK UP to cancel

こんなメッセージが

- Blu-rayディスクおよびHD DVDは、デジタルコンテンツを保護するためにAACS (Advanced Access Content System) を採用しています。一部のBlu-ray DiscやHD DVDタイトルを再生するには、AACSキーが必要です。AACSキーは違法コピー保護のためにPowerDVDに内蔵されています。AACSキーは時々更新する必要があります。再生しようとするタイトルが新しいAACSキーを必要とする場合は、このエラーメッセージが表示されます。

HDCP

- High-bandwidth Digital Content Protection System
- Intel等が開発、Digital Content Protection, LLCがライセンス管理
- 装置間で鍵を用いた暗号化をおこなう
- DVIやHDMI端子で接続した器機間で使われる（Displayやテレビ等とレコーダー間）


AACS
COPP Scramble
DXVA
再生
ソフトウェア
グラフィック
ボード
ブルーレイドライブ
HDCP
High Bandwidth
Digital Contents
Protection
HDCP
対応モニタ
DESKTOP MEDIA PC
GPU
GRAPHICS CARD
TMDS
I²C
SiI 1930
Transmitter
Audio
Codec
HD-Audio/SPDIF
uC
NOTEBOOK MEDIA PC
A/V RECEIVER
SiI 9031
PanelLink
Receiver
HDMI
MCU
Video
Audio
SiI 9030
PanelLink
Transmitter
Audio
DSP
Audio
Amp
DISPLAY
(DTV, Plasma Display, LCD TV, Projector)
SiI 9011
PanelLink
Receiver
Video
Processor
Audio
DAC/
Amp
L
R
SUB
LF
C
RF
LR
RR

AACS: コンテンツ保護技術

- AACS: Advanced Access Content System
- Device Key
- Media Key (AACS)
- Title Key
- 有効期限(PC)

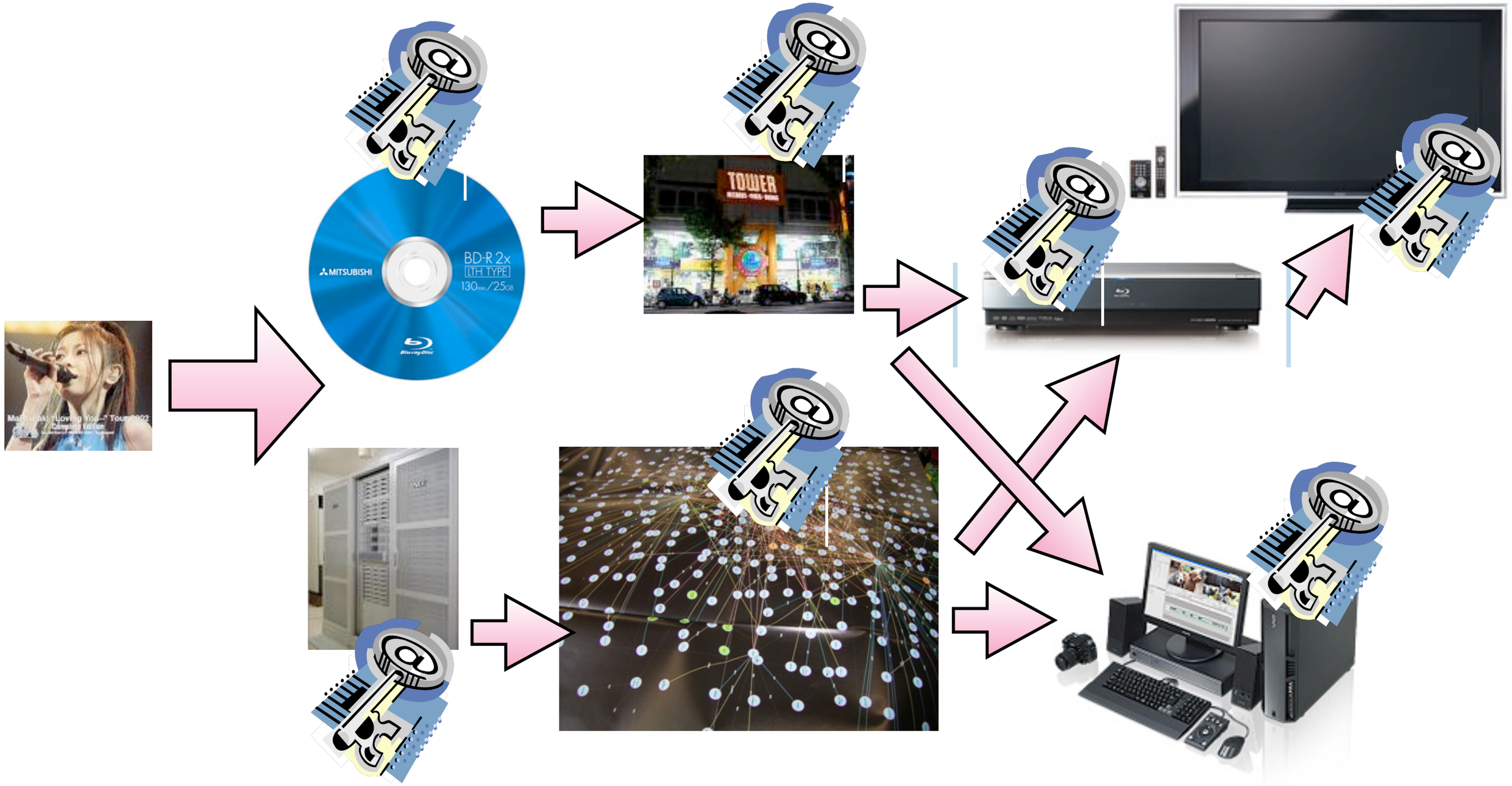
COPP

- Certified Output Protection Protocol
- マイクロソフトが開発
- アプリケーションとGPU間での著作権保護の仕組み
- GPUのドライバとアプリケーション間で暗号鍵を交換
- Windows XP SP2/WM player 10以降でサポート

DXVA2.0

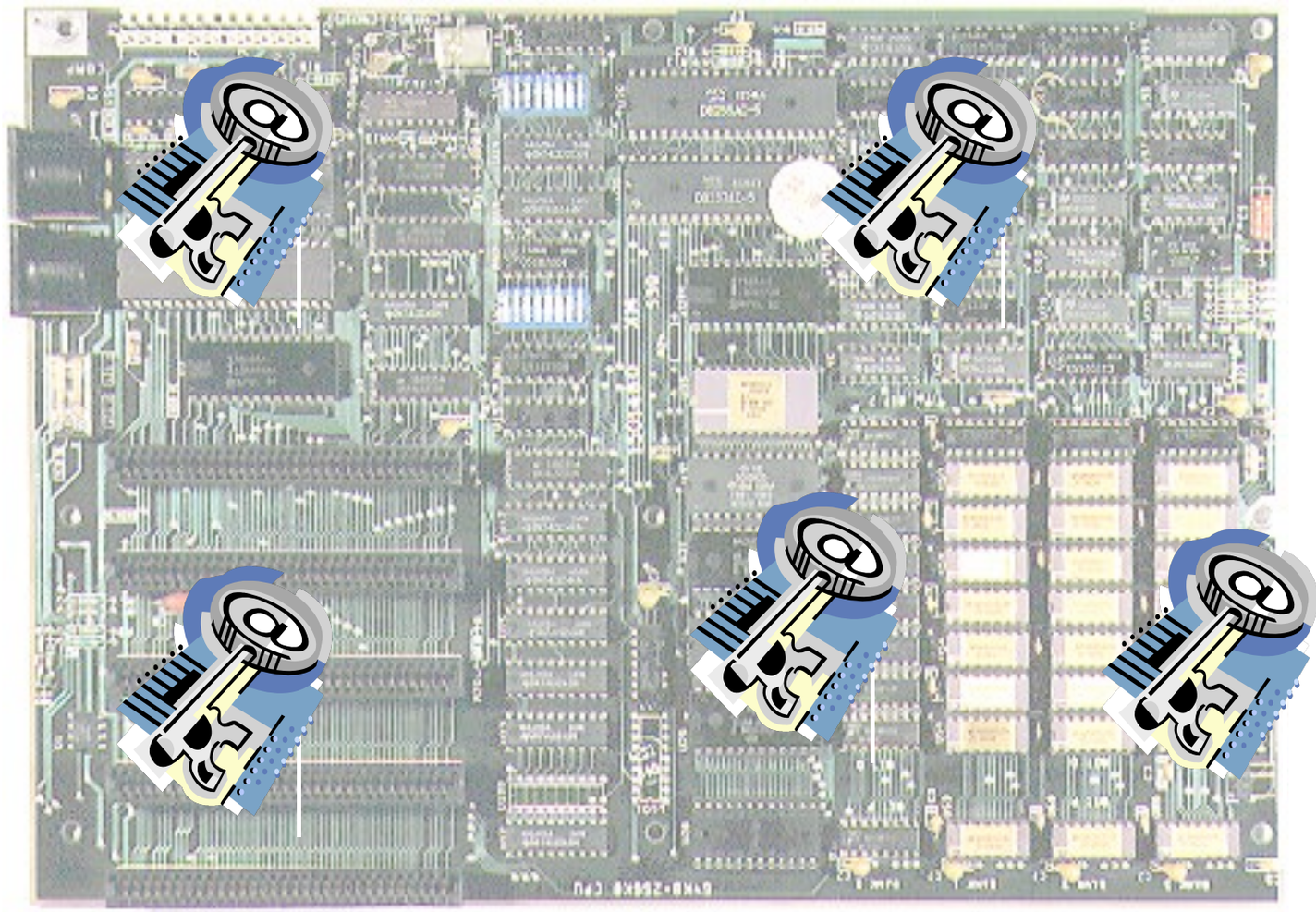
- マイクロソフトが開発
- アプリケーションからディスプレイカードに至プロテクション
- Windows Vista
  - PVP-OPM: Protected Video Path-Output Protection Management
    - ハードウェアの認証等
  - PVP-UAB: Protected Video Path-User Accessible Bus
    - コンピュータ内を流れるコンテンツ情報の暗号化

コンテンツ保護の現状



- メディア・流通・AV器機すべてに鍵を

そして



- コンピュータの中までも。。。。

何から守る？

- 身内以外は、すべて敵！
- 身内とは、
  - メディア制作会社・流通・AV器機ベンダー
  - 身内のハードウェアベンダー
  - OSベンダー・身内のソフトウェアベンダー
- UNIXやインターネットなどのオープンフラットフォームと、その上で活動するフリーのアプリケーションプログラマはすべて敵！？
- コントロールされたコンテンツ流通の世界　v.s

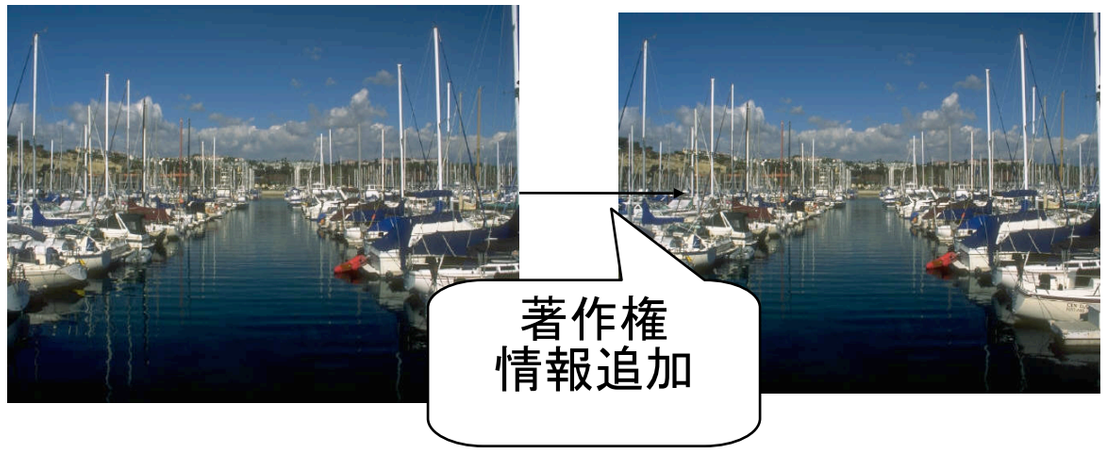
もう１つの考え方

- Copy Protectionではなく、
- Digital Watermarks

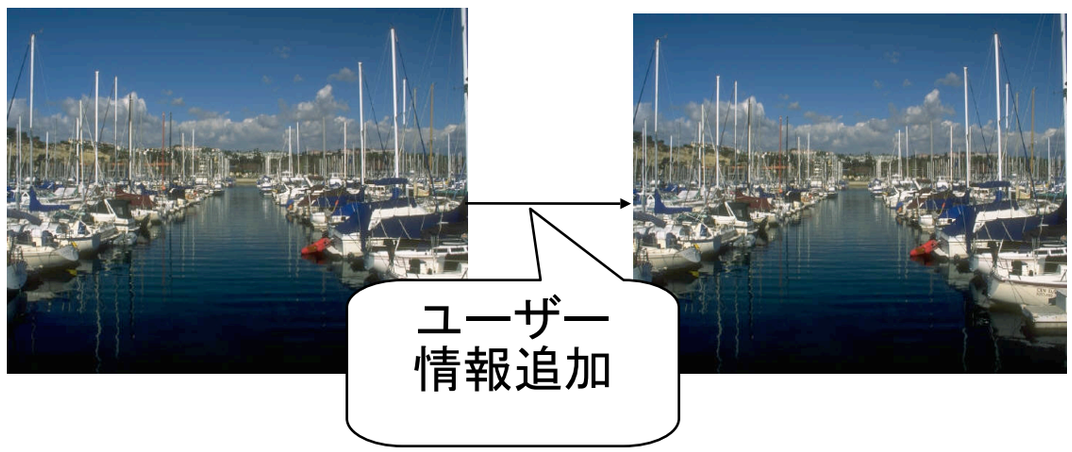
電子透かし(Digital Watermark)

- 可視透かし
  - ロゴや著作権をオリジナルの画像に埋め込む
  - 適合するIDファイルと除去用プログラムで除去可能
- 不可視透かし
  - 目に見えない形でデータを埋め込む

- 著作権保護目的
  - 違法流通の際に著作権の主張を行う

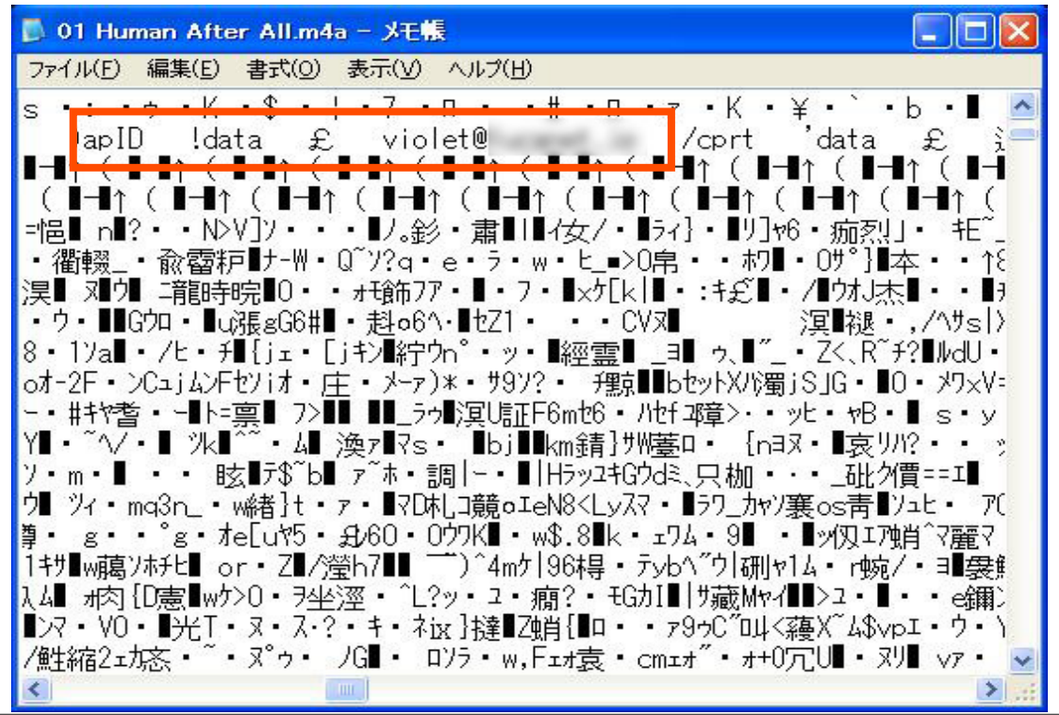


- フィンガープリント
  - ユーザーIDを埋め込むことで違法流通の際に流通者特定を行う



DRMフリーの流れ

- eMusic
  - Basic 30曲/9.99ドル, Plus 50曲/14.99ドル, Premium 75曲/19.99ドル
- iTunes Plus
  - 2007年5月30日サービス開始 1.29ドル/曲
    - 256kbps(DRM有りの場合は128kbps)
  - 2007年10月17日に値下げ 89 - 99セント/曲
  - Apple IDが曲の中にフィンガープリントとして埋め込まれている
    - 流出時に特定できるように
- Amazon MP3
  - 2007年9月25日サービス開始



iTunes Plusで購入された
ファイルの中にあるApple ID

おわりに

- 鍵のかける粒度、鍵の強度
- 鍵にかかるコスト（金、技術、鍵の管理、etc)
- 統制された制御・組織

- すべてを技術で解決するのか？
- 社会システム（法律）によるコンテンツの保護

- 現状は、技術と社会システムが、お互いに反目し合っているように感じる。
- 両者の正しい方向性への合意と協調が必要では？！