コンテンツ保護の柔軟化を実現した開放型超流通基盤

穴澤健明† 武村浩司†† 常広隆司††† 長谷部高行†††† 畠山卓久†††††

†日本コロムビア ††三洋電機 †††日立 ††††富士通研 †††††富士通

ファイル交換ソフトウェアが普及し，著作権侵害などの面で問題になる中，DRM (Digital Rights Management)への期待が高まっている。これに応えるためには，利用者間でのコピーなどの2次流通を扱うことの出来る超流通，コンテンツ保護の柔軟性ならびにコンテンツをメディアで持ち回る操作性などを実現する完全開放型DRM間相互運用方式の提供が重要である。本稿ではこれらを想定したコンテンツ保護に関する技術的要件についてまずふれ，それらの要件を満足する方式であるUDAC-MB (Universal Distribution with Access Control - Media Base)の概要，その安全性の解析ならびに実施例について述べる。

Open Superdistribution Infrastructure Realizing the Tenacity of the Content Protection

Tekeaki Anazawa†, Hiroshi Takemura††, Takashi Tsunehiro†††, Takayuki Hasebe†††† and Takahisa Hatakeyama†††††

†Nippon Columbia ††Sanyo †††Hitachi ††††Fujitsu Laboratory †††††Fujitsu

Universal Distribution with Access Control – Media Base (UDAC-MB) is an open infrastructure to tenaciously protect highly value-added digital content superdistributed. If the spread of file exchange pirating eventually make it possible for remote users to share and make instant bulk copies of digital content, DRM (Digital Rights Management) mechanisms such as UDAC-MB become important. In this paper, we present requirements on such a content protection, UDAC-MB method that satisfies the requirements, security analysis on it and its application examples.

1. はじめに

情報ネットワークのブロードバンド化とファイル交換ソフトウェアの普及が進み，遠隔地間でのディジタルコンテンツ大量瞬時複製を全ての人々が容易に実行できる時代が到来したときに対策がなければ，インターネット上での著作権保護の問題がさらに悪化するとの指摘が各所でなされている。この問題は，本来なら人々の裕福な情報交換を促進するはずの超流通(注)の発展をも意識的に阻害する要因として働く。

利用者間でのコピーなどの2次流通をも扱うことが可能な超流通においてコンテンツ保護機能を確保し，阻害要因を排除するためには，コンテンツの配信，複製，移動，再生時のセキュリティ上の要件やポリシーを明らかにし，それらを満足する相互接続仕様およびセキュリティ評価基準に従ったDRM (Digital Rights Management)(注2)を導入する必要がある。その上で，コンテンツ流通関係者間の責任の範囲を明確にし，不正発生時や破られた場合の対策等を盛り込んだセキュリティ管理が技術的な面でも適切に運営されることによって

(注) 森亮一筑波大学名誉教授が1983年に無体物などの流通方式として提唱した。超流通ではコンテンツ・情報の再流通まで取り扱うことができ，コピーも流通として対応できる。「所有すること」と「使用すること」のどちらにも，あるいは両方にも課金でき，情報提供者の権利と利用者の利便性を同時に保証する。権利を守るためには，外部からの電子的および機械的攻撃に耐える保護容器と暗号による防御機構が必要とした。

(注2) 著作権などのディジダルコンテンツに関わる権利を保護する技術，機能あるいは機能を提供するシステム。そのシステム内部でコンテンツ利用許可条件を管理し，これに従って動作する。

はじめて，超流通ビジネスの推進に対しコンテンツホルダーをはじめとする各方面からの支持が得られるようになる。

2. 超流通コンテンツ保護の要件

まず，コンテンツ超流通ビジネスの運営におけるコンテンツ保護の要件を含めたセキュリティ要件を示すとともに若干の検討を加える。

2.1. 超流通の定義とセキュリティ要件

筑波大学の森亮一名誉教授は「超流通」の定義[1][10]に次の項目を挙げている。

（1）利用者は暗号化コンテンツをほぼ無料で入手
（2）コンテンツ提供者は課金を含む利用許可条件を指定可能
（3）利用者はそのために面倒な手続きを必要としない

ここで(2)は本稿で言及するコンテンツ保護（利用許可条件強制）に関する要件である。(3)に関しては，コンテンツとその利用許諾情報をユーザがメディアで持ち回る従来からのメディアベースの操作性を実現すること，あるいは再生システムがネットワークに接続されていない場合でも，利用許可条件付きコンテンツを再生可能にすることなどによって達成される。

超流通ビジネスのセキュリティ要件にはさらに次のようなものがある。

（4）SSL（Secure Socket Layer）[8]によるサーバ認証などを用いた電子商取引のセキュリティ
（5）電子透かしによる不正アクセス検出
（6）ディジタル署名によるコンテンツの原本性維持

これらの項目はそれぞれ異なるセキュリティ技術で実現され，高い安全性を維持する必要がある場合には一般に暗号技術を利用する。

2.2. 想定する脅威と対抗手段

動画や音楽などの高価値コンテンツを保護してネットワークで流通させるビジネスにおける脅威とその対抗手段を脅威の主体ごとに表-1に示す。

脅威の主体の第一は機器の利用者であり，例えば再生機器や記録メディアの利用者が機器を解析し，機器内部のDRMから秘密情報を取り出そうとする脅威がある。これに対してはDRMを実現する機器やソフトウェアをTRM（Tamper Resistant Module：耐攻撃モジュール）化する必要がある。またコンテンツ保護機構において，送信者偽装による再送攻撃(replay attack)などのなりすましは無限のコンテンツ不正コピーにつながるため，十分な対処が必要である。さらに第二，第三の脅威の主体として網(配信ネットワーク）の利用者やDRMの製造者自身を想定する必要がある。

表-1　高価値コンテンツ流通時の脅威と対抗手段

<table>
<tr><th>主体</th><th colspan="2">脅威（攻撃）</th><th colspan="2">対抗手段</th></tr>
<tr><td rowspan="3">記録メディアや機器の利用者</td><td colspan="2">内部DRM解析・露呈</td><td colspan="2">1)DRMのTRM化</td></tr>
<tr><td rowspan="2">なりすまし</td><td>受信側偽装</td><td rowspan="2" colspan="2">2)受信側DRM認証により共有した一時的な鍵で暗号化</td></tr>
<tr><td>送信側偽装
再送攻撃
(Replay)</td></tr>
<tr><td rowspan="5">上記および網利用者</td><td colspan="2">DRM種別の秘密鍵または一時的な秘密鍵露呈</td><td colspan="2">3)DRM個別鍵でコンテンツ保護情報を暗号化</td></tr>
<tr><td colspan="2">通信切断偽装</td><td colspan="2">4)DRM間ログ比較</td></tr>
<tr><td colspan="2">認証局またはDRM種別の秘密鍵推定</td><td rowspan="3">5)CRL投入</td><td>鍵更新</td></tr>
<tr><td rowspan="2">製造者</td><td colspan="2">不正製品製造</td><td rowspan="2">特定DRMの停止</td></tr>
<tr><td colspan="2">鍵情報漏洩</td></tr>
<tr><td>PCの利用者</td><td colspan="2">ソフトウェアTRM解析</td><td colspan="2">6)コンテンツ保護レベル制御</td></tr>
</table>

PCの場合にはソフトウェアの解析を困難にしたソフトウェアTRMを用いてDRMを実現することが考えられる。しかし，現状のPCで実現されているソフトウェアTRMはハードウェアTRMに比較すれば保護強度は格段に低い。このためハードウェアTRM化されたDRMとソフトウェアTRM化されたDRMが共存するシステムにおいて，前者が後者を信頼する場合，第四の脅威の主体であるPC利用者に脆弱なソフトウェアTRMが破られたのち，DRMが偽装され，これを信頼したハードウェアTRM化DRMからも秘密情報を流してしまうという事態が想定される。

これらの脅威と各対抗手段については3.3.に

詳述するが，実際の脅威に対抗するに当たっては，コンテンツ流通ビジネスのリスクとコストに見合うTRM化手段，暗号アルゴリズムおよび認証方式の選択が必要である。これらの適切な組合せによって，柔靭（柔軟で強力）なコンテンツ保護セキュリティを維持し，保護・配信システム全体を正常に運営し続けることが可能になる。さらにDRMに必要なレベルのセキュリティを維持していくためには，各DRM製造者に対し，証明書発行の交換条件として遵守を義務付けたセキュリティ評価基準を提供し，DRM認定作業を実施する必要がある。セキュリティ評価基準ではDRMへの実装を必須とするセキュリティ対策などが列挙されている。

2.3. 異機種DRM間相互運用の要件

コンテンツ超流通にかかわる記録メディアや配信・再生システムを開発，製造，運営する立場からは，コンテンツ保護基盤がそれにより構築された超流通システムへの参加を抑制するようなものではなく，その柔靭性を維持しつつも異機種DRM間相互接続に関しては完全にオープンな形態をとることを求められる。これに関しては具体的には次のような要件がある。

（1）ライセンスのみの追加購入と移動

技術的には暗号化コンテンツとライセンス（コンテンツ復号鍵＋利用許可条件）を分離してそれぞれ単独で購入，複製あるいは移動できること。これにより，ROM媒体による暗号化コンテンツ先行配布や利用者間での暗号化コンテンツコピー，キャッシュサーバへの暗号化コンテンツ分散蓄積が可能となり，ネットワークの負荷削減および分散の効果により，利用者からみたコンテンツ流通の高速化すなわち超流通が可能となる。

（2）ハードウェアTRM内処理のみでの保護

ハードウェアTRM内ですべての認証，暗号および復号の処理を実行する強力なコンテンツ保護とシンプルな相互接続仕様。

（3）不正の局所封印

万が一，コンテンツ保護が破壊された場合でも，不正の影響が広がらないこと。またこれにより旧システム破壊時にも，新システムへの影響を防止し，柔軟なシステム交代が可能となること。

（4）完全開放型DRM間相互接続仕様

完全にオープンな異機種DRM間相互接続仕様が存在し，不正の影響が拡散する要因となる秘密鍵の接続者間事前交換などが必要ないこと。

3. UDAC-MB：DRM間相互運用基盤

UDAC（ユーダック）-MB (Universal Distribution with Access Control - Media Base)は以上の要件を満足することを可能にした保護コンテンツオンライン配信・移動・再生の際のDRM間相互運用方式であり，仕様である。UDAC-MBはコンテンツのアクセス制御を遠隔においても強制する技術基盤でもある。

3.1. サービスモデル

UDAC-MBの基本サービスモデルを図-1に示す。モデル上，DRMは配信システム，記録メディアおよびコンテンツ再生システムの内部に存在し，それぞれをサーバDRM，メディアDRMおよびデコーダDRMと呼ぶ。これらのうち，メディアDRMとデコーダDRMにはTRM化が必要である。

TRM化が必要なDRMの製造者は配信サービス参入に当たって機器種別ごとにDRM種別公開鍵と秘密鍵のペアを生成し，公開鍵のみを認証局(CA: Certification Authority)に提出する。認証局ではこの種別公開鍵に認証局の秘密鍵を用いてディジタル署名を施し，DRM種別公開鍵の証明書を生成，発行する。DRMの製造者

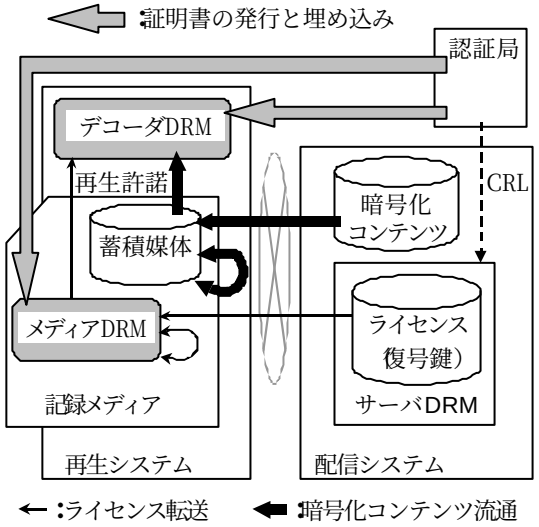

図-1　UDAC-MB基本サービスモデル

は，この証明書を自身が製造するDRMに埋め込む。

UDAC-MBでは暗号化コンテンツの流通方式については特定しておらず，ライセンス（コンテンツ復号鍵＋利用許諾鍵）を安全に記録メディア内のメディアDRMに配信・移動し，またデコーダDRMに再生許諾するためのプロトコルを規定している。メディアDRMはライセンスを正当に格納し，移動されたライセンスを移動元から強制的に削除する機能を持つ。またデコーダDRMはメディアDRMから再生許諾を受け，コンテンツを復号する機能を持つ。復号した結果は再生システムに渡される。

証明書とおよび暗号アルゴリズムはPKIX{Public Key Infrastructure（X.509)} [3]準拠のものを利用する。

3.2. 利用許可条件(ACm, ACp)

コンテンツホルダに指定された利用許可条件は次のようなアクセス条件として，復号鍵とともにライセンス内に埋め込まれた状態で配信され，またDRM間で転送される。

（1） ACm

メディアアクセス条件(Media Access Condition)。記録メディア内で強制する利用許可条件。再生許諾可能回数，移動可能回数，コンテンツ保護レベル，そのほかを含む。

（2） ACp

デコーダアクセス条件(Decoder Access Condition)。デコーダ内で強制する利用許可条件。再生可能期限，再生可能時間，そのほかを含む。

複製可能回数の指定はその回数分の数の移動可能ライセンスを配信することで実現できる。

3.3. 各対抗手段

表-1の各脅威に対するUDAC-MBの具体的な対抗手段を説明する。

3.3.1. TRM化

表-1に示した対抗手段1)としてのTRMはコンテンツ復号鍵や各システム内部で持つ秘密鍵な

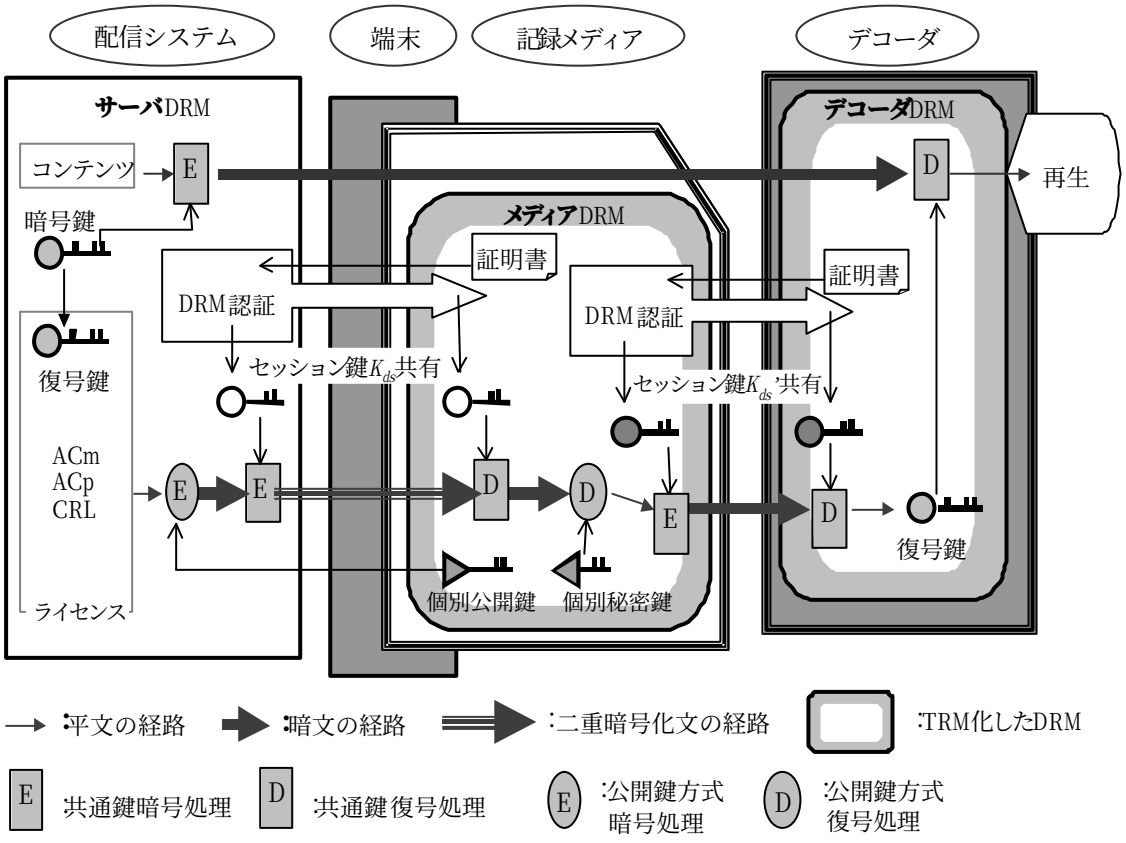

図-2 ライセンス転送プロトコル概要

どの秘密情報を安全にDRM内部で維持する機構であり，それらの鍵に係わる処理をDRM内部でのみ処理し，決して外部に漏らさない機能を持つ。TRMにはハードウェアTRM（保護容器）とソフトウェアTRMがある。

ハードウェアTRM化には例として次のような処置が必要になる。

(1) 外部端子から秘密情報（秘密鍵）の読出し，書換えや制御ファーム，ログ情報，利用許可条件などの書換えができない構造。

(2) 回路パターン読み出し防止のためのメタル層，特殊コーティングなどによる覆い。

(3) 解析困難な極微細化（最先端の微細化技術を用いる）。

(4) サイドチャネル攻撃など，電流や電磁波の漏れからの秘密情報盗難を防止する機構。

ソフトウェアTRMは解析困難なソフトウェアであり，例えば次のような処置が必要になる。

・暗号化したソフトウェアを実行の瞬間のみ復号。

・平文化されたときに解析しにくい構造。

3.3.2. DRM認証とライセンス転送

対抗手段2)としてのDRM認証は認証対象のDRMに埋め込まれたDRM種別公開鍵の証明書を用いてチャレンジレスポンス方式で行われる。またこの認証の結果，ライセンス転送元（配信システムまたはメディア）と認証された転送先DRM（メディアまたはデコーダ）とでセッション鍵（一時的な暗号鍵）が秘密裏に共有される。DRM認証プロトコルの安全性に関しては3.5.で詳述する。

ライセンスは，図-2に示すように，DRM認証で共有したセッション鍵およびDRM個別公開鍵を用いて暗号化してから，転送先DRMに送信される。DRM個別公開鍵は製造したメディアDRM一個一個に割り当てられる。

この転送方式は，ライセンスの配信，ライセンスのメディアDRM間移動およびメディアDRMからデコーダDRMへの再生許諾に用いられる。なお，特に図中にはないが，メディアDRM間移動プロトコルは配信プロトコルと同じである。

DRM認証はライセンス転送先のDRMのみを認証する一方向認証である。転送元に入った時点ですでに保護が破られ平文化したコンテンツについては対処の方法がなく，転送元を逆認証してもビジネスリスクの縮小には結びつかないためである。

DRM個別公開鍵によるライセンス暗号化は，対抗手段3)として，特定のDRM種別公開鍵がやぶられた場合でも，そのDRMだけを識別して停止することを可能にしている。

3.3.3. 再転送時のDRM間ログ比較

特に無線をベースにした携帯電話網を経由した配信サービスでは，コンテンツのダウンロード中に利用者の意図しない通信の中断が発生する確立も高い。攻撃の主体はこの事情を利用し，ライセンスを正しく受信したにもかかわらず，通信切断を装いライセンス配信の要求を繰り返すことで，不正に複数のライセンスを入手しようと試みる可能性がある。この脅威に対抗する手段がない場合，配信する側からみると，実際に通信切断がおこっているかもしれず，ライセンスが届いた証拠もなく，課金をするからには確実にライセンスを届ける必要があり，ユーザクレームを回避するためにもライセンスを再送しつづけることになりかねない。

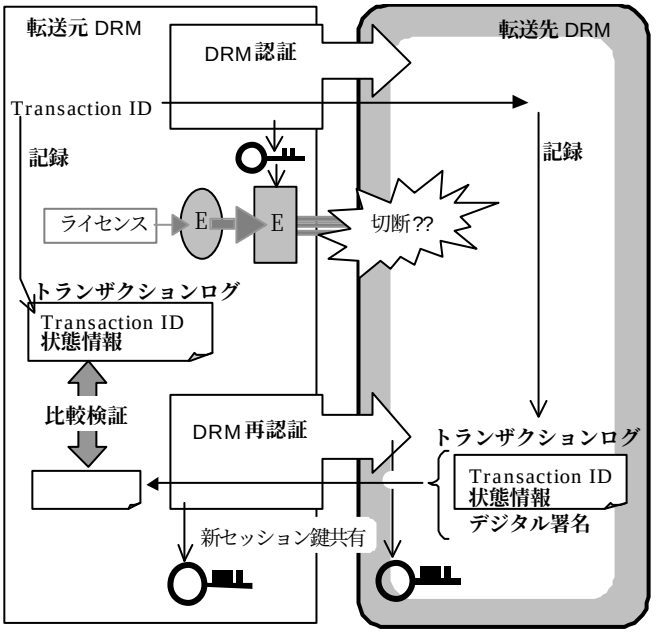

図-3　ライセンス再転送時のログ比較

このような攻撃に対しても，表-1の対抗手段4)として示したように，通信切断後の再接続要求時にライセンス転送元と転送先のトランザクションログを比較することで，転送先にライセンスが届いたかどうかを確認し，通信切断偽装攻撃を防止しつつ，ユーザへの課金を確実にすることが可能になる。図-3にライセンス再転送時のログ比較の手順を示す。

再接続にあたっては転送元がメディアなどの転送先DRMを再認証し，新たなセッション鍵を共有する。その際，転送先のトランザクションログがディジタル署名付で転送元に送信される。このログ内の状態情報が転送元DRMのトランザクションログの内容と比較され，ライセンス転送が失敗したことを確認できて初めて，ライセンスが転送先DRMに再送される。

3.3.4. CRL（証明書失効リスト）

CRLは対抗手段5)として利用する。万が一，DRM内の鍵の一つが破られた場合やDRMの不正が明らかになった場合は，認証局からCRL（Certificates Revocation List）が配信システムに発行される。CRL発行以降に配信されるライセンスについては，CRLで指定された証明書を提示しても，指定されたDRM内への配信・移動や再生許諾を拒否される仕組みとなっている。これにより，不正の局所封印を実現し，また旧システムのセキュリティ崩壊時にもその影響を局所封印することで，新システムへの柔軟な交代が可能となる。

CRLは認証局が発行するが，ライセンス転送時にライセンスとともにセッション鍵で暗号化されて，転送先メディアに強制的に送信され，メディアDRM内でも指定された証明書の失効が実行される。CRLは，対応する秘密鍵を破られるなどした公開鍵の証明書を利用停止にし，鍵を更新するのに用いられる。一つのDRMが持つすべての証明書が停止されればそのDRMへのライセンス転送が完全に停止される。

CRLもPKIX準拠[3]のものを用いる。

3.3.5. コンテンツ保護レベル制御

対抗手段6)として，ソフトウェアTRMに頼った保護（レベル1）とハードウェアTRMによってすべてのセキュリティホールを埋めた保護（レベル2）をDRMのTRM化レベルとして区別し，さらにACmで指定されたコンテンツ保護レベルに従い，レベルの低いDRMへのライセンス格納を制限する必要がある。このコンテンツ保護レベル制御の基本方針を図-4に示す。

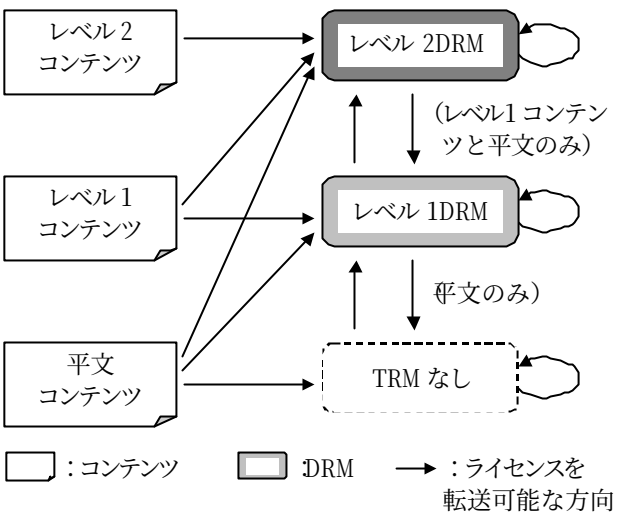

図-4　コンテンツ保護レベルによるアクセス制御

レベル1コンテンツのライセンスはレベルが1以上のDRMのすべてに格納することが可能であるが，レベル2コンテンツのライセンスはレベル2以上のDRMにしか格納することができない。

3.4. 暗号アルゴリズムの選択

UDAC-MBの基本方式としては，暗号アルゴリズムを特定しないが，現在，DRM認証，コンテンツ暗号化，ライセンス暗号化および署名に用いている暗号アルゴリズムは，共通鍵方式としては鍵長112ビットのTriple DES，公開鍵方式としては鍵長163ビットの楕円曲線暗号[4]を用いている。企業が2002年に10億円を投じて解読を試みた場合，前者は約2×10^{15}年を要し，セキュリティ強度が鍵長1,024ビットのRSA（Rivest，Shamir，Adelman）暗号アルゴリズムに匹敵する後者は約5×10^{5}年を要すると予測されている。

つぎの二つの理由から，現時点では公開鍵暗号方式としてRSAではなく，楕円曲線暗号を用いている。

(1) 楕円曲線暗号は同じセキュリティ強度のRSAに比較し，鍵の長さが数分の一で済み，高速処理が可能。

(2) 楕円曲線暗号はRSAに比較し，セキュリ

ティ強度が高くなるほど（鍵のビット長が長くなるほど）計算量の観点からの優位性が増す。

3.5. プロトコルの安全性の検証

本節ではUDAC-MBのライセンス転送プロトコルの安全性をNeedhamらが提唱した認証プロトコル解析手法[5]を用いて検証する。検証にあたっては次の記法を用いる。

- P *believes* X：主体PがXを信用しているか，又はPがXを信用する権限を与えられている。PはXが真であるかのようにふるまうことにもなる。
- P *sees* X：PがXを認知する。Xを含むメッセージがXに送信されれば，（復号などのあと）PはXを読み，Xを反復することも可能。
- P *said* X：Pが1回"X"と言及した。Pはある時点でXを含むメッセージを送信したことを示す。それがいつの時点かは不明であるが，PがXを信用していることが認知されたことを示す。
- *fresh(X)*：式Xが新規(fresh)であること，すなわち今回のプロトコル実行以前にXが送出されていないことを示す。
- $\{X\}_K$：式XがキーKで暗号化されていることを示す。
- $\overset{K}{\mapsto} P$：Pは公開鍵Kを所有する。対応する秘密鍵はP以外が知ることはできない。
- $P \overset{K}{\leftrightarrow} Q$：PとQは共有鍵$K$を情報交換のために利用できる。鍵$K$は適切なものであり，PとQ以外には決して発見できない。

3.5.1. DRM認証プロトコル

D (Destination)と命名したDRMが管理する種別公開鍵をK_dとして，ライセンスをS (Source)と命名したDRMからDへ転送することを想定する。UDAC-MBにおいて，ライセンス転送のためにSがDを認証する手順は，解析に必要な情報のみで表現すると次のようにシンプルなものになる。

$$Message\ 1\quad D \rightarrow S:\ K_d$$

$$Message\ 2\quad S \rightarrow D:\{K_{sd}\}_{K_d}$$

$$Message\ 3\quad D \rightarrow S:\{K_{ds}\}_{K_{sd}}$$

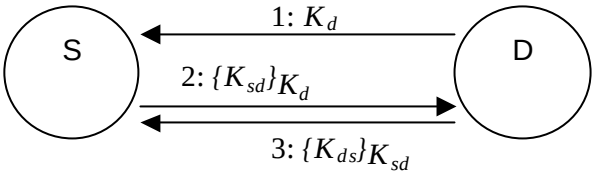

図-5　DRM認証プロトコル

ここでK_{sd}はSが，またK_{ds}はDが秘密裏に生成する乱数であり，ともにSとDで一時的に共有する鍵として利用することを目的とする。

3.5.2. プロトコルの理想化

Needhamの手法に習い，プロトコルを理想化(idealization)すると次のようになる。

$$Message\ 1\quad D \rightarrow S:\ \overset{K_d}{\mapsto} D$$

$$Message\ 2\quad S \rightarrow D:\{S \overset{K_{sd}}{\leftrightarrow} D\}_{K_d}$$

$$Message\ 3\quad D \rightarrow S:\{S \overset{K_{ds}}{\leftrightarrow} D\}_{K_{sd}}$$

ここでMessage 2ではK_{sd}が，またMessage 3ではK_{ds}がS及びDで共有され，他の主体が知ることはできないことを期待した表現とした。

3.5.3. 初期条件

このプロトコルを利用するにあたっての初期条件は次のとおりである。

$$D\ believes\ \overset{K_d}{\mapsto} D \qquad (2)$$

$$S\ believes\ \overset{K_d}{\mapsto} D \qquad (3)$$

$$S\ believes\ fresh(K_{sd}) \qquad (4)$$

$$D\ believes\ fresh(K_{ds}) \qquad (5)$$

ここで(2)は公開鍵K_dに対応する秘密鍵がTRM化されたDに秘密裏に埋め込まれることによって実現する。(3)は，Message 1としてK_dが認証局で認証された証明書の形式で送信され，その署名をSが確認することにより成立する。(4)および(5)はK_{sd}およびK_{ds}がそれぞれSおよびDによって十分に安全な乱数として生成されれば成立する。

3.5.4. 解析

Message 2が正しくDに到達した場合，「公開鍵による暗号を用いた式確認」の公準

(postulate)により，次の状態が得られる。

$$D \text{ sees } S \overset{K_{sd}}{\leftrightarrow} D \qquad (6)$$

この式はMessage 2を送信し，この状態の要因を作ったSから見ると次のことを意味する。

$$S \text{ believes } D \text{ sees } S \overset{K_{sd}}{\leftrightarrow} D \qquad (7)$$

さらに(7)はK_{sd}がK_dにより暗号化された状態で送信され，Sは初期条件(3)によりD以外にはこれが発見できないことを信じていることから，次のことを意味する。

$$S \text{ believes } S \overset{K_{sd}}{\leftrightarrow} D \qquad (8)$$

(8)の状態でのMessage 3の結果，公準の一つである「共有鍵で暗号化したメッセージの意義規則(*message-meaning rule*)」より，次の状態が得られる。

$$S \text{ believes } D \text{ said } S \overset{K_{ds}}{\leftrightarrow} D \qquad (9)$$

これはK_{ds}がK_{sd}により暗号化された状態で送信され，Sは(8)によりD以外にはこれが発見できないことを信じていることから，次のことを意味する。

$$S \text{ believes } S \overset{K_{ds}}{\leftrightarrow} D \qquad (10)$$

また(4)および(9)の結果と一時データ通知(*nonce-notification*)及び新規性(freshness)連動の公準より，次の結果が得られる。

$$S \text{ believes } D \text{ believes } S \overset{K_{ds}}{\leftrightarrow} D \qquad (11)$$

(10)および(11)はそれぞれ，**3.5.3.**の初期条件が満たされることで，この直後にK_{ds}により暗号化されたライセンス情報が転送されるにあたって，転送先DRMへのなりすまし（受信側偽装）および再送攻撃（送信側偽装）に対抗できることを示している。

なお，SSL[8]などの電子商取引の認証プロトコルは一般に双方向の認証機能を想定していることもあり，メッセージの本数も各内容も本方式より冗長なものになる。

4. DRMの実装

UDAC-MBを実際のコンテンツ超流通・再生システムに応用するにあたっての電子商取引のセキュリティとの関係，各DRM実装の方法および実装の評価基準について述べる。

4.1. 電子商取引との関係

SSL[8]などの電子商取引のセキュリティは各システムを管理する利用者間の課金情報を安全に交換することを目的とし，交換した情報が利用者そのものに不正利用されることに対抗する能力はない。しかし，コンテンツ保護のためのライセンス転送にはそうした対抗機能も必須であり，UDAC-MBはこの点も考慮した仕様となっている。図-6にUDAC-MBと電子商取引のセキュリティとの関係をモデルとして示す。

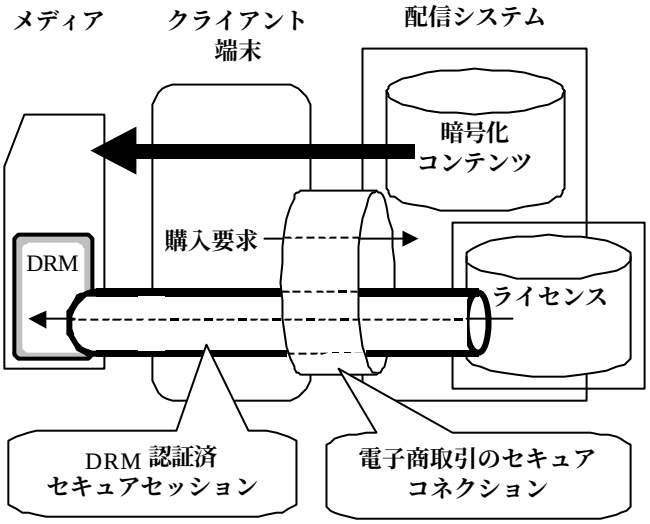

図-6　電子商取引のセキュリティとの関係

UDAC-MBでは**3.3.**で示したように利用者自身の不正利用を防止するために，DRM認証済のセッション鍵をDRM間で共有することによってセキュアセッションを確立する。このセキュアセッションでサーバDRMとメディアDRMの間をダイレクトに連結し，その中でライセンス転送を実行する。このセキュアセッションは配信システムとクライアント端末の間では，課金時の不正に対抗するために，SSLなどを用いた電子商取引のセキュアコネクションの中に確立されねばならない。

このように，コンテンツ保護のセキュリティドメインは電子商取引やプライバシー保護のためのセキュリティドメインとは隔絶されたものでなければならない。

4.2. サーバDRMの実装

ライセンス配信システム内のサーバDRMはファイアウォールなどの運用管理および運営により保護される必要がある。なお，課金やコンテンツ管理も含めたUDAC-MB配信システムの具体的な実装例については，参考文献[12]などにある。

4.3. メディアDRMの実装

UDAC-MB技術を記憶メディアへ適用するためには，ライセンスを安全にその内部のメディアDRMに格納する機構が必要である。このメディアDRMのセキュリティ強度がシステム全体のセキュリティ強度を決定する重要な要素になる。

暗号化コンテンツ自体は技術上，どのような記憶媒体にでも記録することができる。ライセンスを安全に格納する機構と，暗号化コンテンツを記憶する大容量メモリを一体化することでユーザの使い勝手のよい記憶メディアを提供できる。

4.3.1. SECURE MultiMediaCard

セキュアマルチメディアカード（SECURE MultiMediaCard™）はUDAC-MB方式を適用するために，マルチメディアカード（MultiMediaCard™）[11]にメディアDRMコマンドを17件追加したものである。これにより従来のマルチメディアカードと完全な互換性を保ちながら，拡張機能としてのコンテンツ保護機能を利用できる。

携帯電話やポータブル音楽プレーヤに搭載する上で利用者の便から最適な記憶メディアは現在，半導体記憶メディアである。その中で最も小型・軽量な国際標準メディアがマルチメディアカードである。これは記憶素子としてFlash Memoryを使用し，２４×３２×１．４mmの薄型・小型カードでありながら，現在では６４Mバイト以上の記憶容量を持つものまで実現できている。

セキュアマルチメディアカードではマルチメディアカード内部の制御機構を用いてメディアDRMを構築し，その中に暗号関連処理回路，秘匿すべき鍵類，暗号処理にかかわるROMやRAMなどが図-7に示すように配置される。Flash Memory部分は大容量の不揮発性記憶素子であり，現在で64Mバイト程度，1年後には512Mバイトクラスも実現できる。ここは暗号化コンテンツを記憶するために使用することができ，ユーザが自由にアクセスできる領域である。

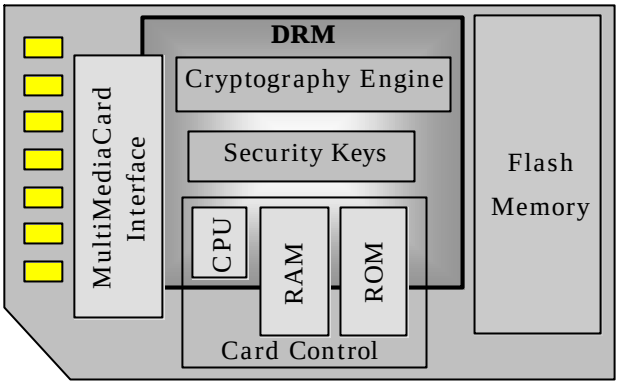

図-7　SECURE MultiMediaCard™構成モデル

4.3.2. その他の記録メディアへの実装

その他，図-8に示すようにメディアDRMをチップ化することにより，多様な記録メディアに搭載し，コンテンツ保護の柔軟性を維持したまま，メディアベースの操作性を実現することができる。

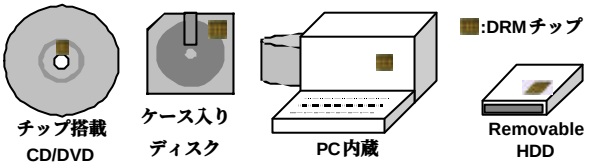

図-8　多様な記録メディアへの実装

4.4. デコーダと再生システム

デコーダの役割は，図-9に示すように，再生時に記録メディアからライセンス（再生許諾）を受け，暗号化コンテンツをACp（デコーダアクセス条件）に従って復号しアナログデータとしてアナログ再生システムに転送することである。デコーダはデコーダDRM，暗号関連処理機能および秘匿すべき鍵情報を維持し，一時的にではあるが平文化されたコンテンツデータまでその内部に出現するため，これをTRM化する必要がある。

再生システムはデコーダと記録メディア装着用のスロットのほか，必要に応じてダウンロードや再生に必要となる各種デバイスを備える。再生システムのCPUは暗号処理等には関与しないが，ダ

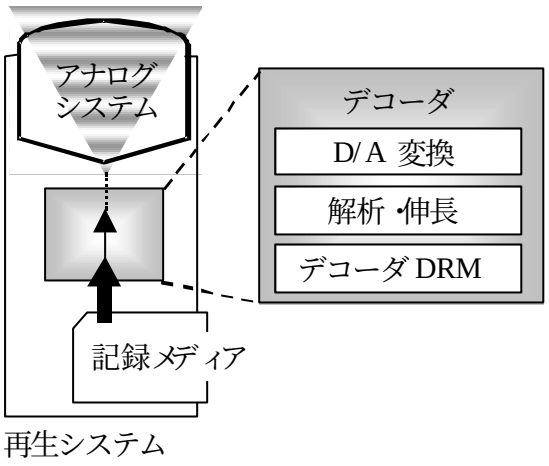

図-9　再生システムとデコーダの関係モデル

ウンロードも可能な場合であれば配信サーバと記録メディアに，再生時であれば記録メディアとデコーダに対して，3.に示した手順に則ったアクセスを行い，これらのシステム間の情報交換を仲介する役割を担う。

再生システムは利用者に対して暗号化コンテンツのコピー機能を提供することもできる。

4.5. ソフトウェアDRM

PCなどではメディアDRMとデコーダDRMをソフトウェアで実現可能であるが，UDAC-MBの異機種間相互運用に参加する場合は，これらにソフトウェアTRM化を施す必要がある。またライセンス受信機能を製品化などするにあたっては，レベル1DRMとしての証明書を取得する必要がある。

なお，ソフトウェアDRMとして音楽コンテンツを扱う場合にはSDMI[2]に準拠した電子透かしチェック機能なども実装する必要がある。

4.6. セキュリティ評価基準

UDAC-MBのDRM製品に証明書を発行するにあたっては，特にDRMのTRM化に関する評価基準を用意する必要がある。認証局はこれに従った製品評価を実施し，これに適合したものにのみ証明書を発行することになる。TRMのセキュリティ評価基準の例としては，参考文献[9]などがある。

5. 実施例と今後の展開

実施例とUDAC-MBの特色を生かした今後の展開について5例を表-2に示すと共に，各例について簡単に説明する。

5.1. PHSへの配信

2000年11月30日，DDIポケット株式会社はサウンドマーケットと呼ぶ携帯電話向け音楽配信サービスを『ケータイde ミュージック』方式で世界に先駆けて開始した。このサービスでは，DRMとしてUDAC-MBを用いた『ケータイde ミュージック技術規格書』[6]に準拠したシステムを採用し，記録メディアとしてはセキュアマルチメディアカードを用いている。現在では音楽，カラオケ，落語，語学教材等32k～128kbpsのMP3で圧縮された約2,000 曲分のコンテンツがダウンロードでき，楽曲のプロモーションにも大きく寄与している。今後，楽曲の拡充，端末，メモリカードの価格の低減，通信速度の高速化，通信料の低減等の様々な改善が想定されるため，ユーザの増加も期待される。

記録メディアに格納されている暗号化コンテンツは端末経由で他の記録メディアにコピーすることができる。コピーを受け取った端末では，そのコンテンツに対応するライセンスのみをダウンロードすることによって再生が可能となる。

暗号化コンテンツ配信の際には，端末内部でダウンロード済サイズを記録しており，通信中断後の再接続では配信サーバにその情報が渡される。これによって，配信サーバはダウンロードが完了していない部分のみの配信を再開することができる。

5.2. KIOSK販売

KIOSK端末としてのPHS内蔵ローカルサーバ付き店頭コピーシステムの展開が試みられている。暗号化コンテンツをこの店頭コピーシステムで入手することにより通信速度の制限を逃れ，ライセンスのみをPHSでダウンロードすることで，利用者は短時間でコンテンツを購入することができる。対応プレーヤーの普及を待って，本格的なサービスとして開始されると考えられる。

5.3. インターネット配信

配信系にインターネットを用いた例であり，『UDAC-MBホスト連携規格書』[7]に準拠して実装したものである。この規格書はSDMI[2]に準拠したDRM間相互接続仕様を規定している。

インターネット配信では通常PC上のソフトウェアDRMを用いる。この場合コンテンツ保護

表-2　サービス実施例と今後の展開

サービス形態	PHSへの配信	KIOSK販売	光ディスクによる超流通	インターネット配信	DRMチップ実装光ディスク
流通サービスの主体	DDIポケット (SoundMarket)	KIOSK設置者	スーパーコンテンツ流通	ISP	DigitalJam
DRM	UDAC-MB				
コンテンツの種類	音楽，英会話，落語	カラオケ，他	音楽，他		
販売主体	コンテンツホルダー				
コンテンツ料	100～350円			左に準ずる	未定
試聴料	無料				
コンテンツ料	通信キャリア代行徴収				DigitalJam代行徴収
通信料	13円／分	殆ど発生せず		ISP	殆ど発生せず
DRMの保護	ハードウェアTRM化				
認証局	日本レコード協会／ケータイdeミュージックコンソーシアムコンテンツ担当				左に準ずる
セキュリティ計画書	通信キャリアが作成	左に準ずる			
音声圧縮方式	MP3 32～128Kbps			左記，他方式も可	
流通形態 ライセンス	携帯電話網（64Kpbs）			インターネット	店舗，通信網，他
流通形態 暗号化コンテンツ	携帯電話網（64Kpbs）	既存網から内蔵サーバ経由	光ディスク先行流通		光ディスク先行流通，他
CRL発行機能	○				
試聴方式	PHS音声 (ADPCM)	PHS音声（専用化可能）	光ディスク上に記録	ストリーミング	光ディスク上に記録，他
メディアDRM	SECURE MultiMediaCard				DRM実装ディスク
記録メディア	SECURE MultiMediaCard		光ディスク	左に準ずる	光ディスク
再生システム	携帯型プレーヤー				汎用機，他
サービス開始	‘00年11月30日	実験中	‘01年5月01日	未定	2002年を予定
その他の特徴	CD販売店位置情報案内	KIOSKにPHS端末を内蔵	PCで暗号化コンテンツをコピーして利用	ソフトウェアTRMを併用可	既存CD販売店が参加可能
URL	www.ddipocket.co.jp		www.super-contents.co.jp		www.digitaljam.ne.jp

レベルが低下するため，PCはライセンス交換を仲介するだけにし，メディアDRMを実装した記録メディアにライセンスを直接転送し，再生については半導体メモリオーディオプレーヤーを利用する保護レベル2でのソリューションも提供している。またPCでこれと同等の保護レベルを維持する場合にはハードウェアTRM化したDRMをPC内に実装する必要がある。

5.4. 光ディスクによる超流通

暗号化コンテンツの供給を光ディスクで行う展開例である。暗号化コンテンツを光ディスクからメモリカードにコピーし，ライセンスのみをメモリカード内のメディアDRMに受信することで保護コンテンツの購入を実現する。

5.5. DRMチップ実装光ディスク

光ディスク上にハードウェアTRMで保護されたメディアDRMチップを実装したもので，チップとしては非接触で読み書きが可能なものが想定されている。この展開例はCD販売店等も従来からのコンテンツ流通の流れの中でビジネスに参入

できるという特色を持ち，在庫量の縮減や万引きの防止等にも役立てることができる。

6. おわりに

本稿では，超流通まで想定したコンテンツ保護に関する技術的要件およびそれらの要件を満足する技術であるUDAC-MBの概要について述べ，その安全性を検証し，具体的な実施例についても併せて記述した。

UDAC-MBの実装を行った後，PHS への音楽配信サービスを開始して，本日でちょうど1年になる。セキュリティ上の問題はこれまで発生していないだけでなく，安全なシステムとしてコンテンツホルダより好感をもたれている。超流通等，様々な展開が行えることもその特色として挙げられる。またその強固なコンテンツ保護機能が評価され，ヒット曲のシングルCD発売前配信も実施された。

本稿で紹介した実施例は，特に音楽コンテンツの配信に注目したものであるが，UDAC-MBは動画・画像・文書・プログラムなどの著作権等に関わるすべてのコンテンツに適用することができる。情報ネットワークのブロードバンド化とコンテンツ紹介・交換アプリケーションのインテリジェント化が更に進み，ネットワーク利用者間でのディジタルコンテンツ大量瞬間複製がだれにでも容易にできる時代が到来すれば，ますますオープン性と高い安全性とシステム進化の柔軟性とを兼ね備えた超流通コンテンツ保護技術として，UDAC-MBのような仕組みとその国際標準化が重要になる。

参 考 文 献

[1] 森亮一，河原正治：歴史的必然としての超流通．超編集・超流通・超管理のアーキテクチャシンポジウム，1994年2月．
http://sda.k.tsukuba-tech.ac.jp/SdA/reports/A-50/21894.html

[2] SDMI Portable Device Specification-Part 1-Version 1.0，8 July 1999，SECURE DIGITAL MUSIC INITIATIVE．
http://www.sdmi.org/

[3] Housley, R., Ford, W., Polk, W. and D. Solo, "Internet X.509 Public Key Infrastructure: Certificate and CRL Profile", RFC 2459, January 1999.
http://www.ietf.org/html.charters/pkix-charter.html

[4] SEC1. Elliptic Curve Cryptography. Standards for Efficient Cryptography Group, September, 2000.
http://www.secg.org/

[5] M. Burrows, M. Abadi, Roger Needham: A Logic of Authentication, Twelfth ACM Symposium on Operation Systems, pp. 1-13 (1989).

[6] ケータイdeミュージック・コンソーシアム：ケータイdeミュージック技術規格書Part1：概要．Version 1.0，改訂第一版，2001年5月．
http://www.keitaide-music.org/

[7] ケータイdeミュージック・コンソーシアム：UDAC-MBホスト連携規格書Part 1：概要．Version 0.9，2001年4月．
http://www.keitaide-music.org/

[8] Dierks, Dierks, T., and C. Allen, "The TLS Protocol - Version 1.0," IETF RFC 2246, January 1999.
http://www.ietf.org/html.charters/tls-charter.html

[9] NIST: FIPS PUB 140-1. Federal Information Processing Standards Publication. 1994 January 11. Security Requirement for Cryptographic Modules

[10] Ryoichi Mori, Masaji Kawahara: ``Superdistribution: The Concept and the Architecture", The Trans. of IEICE, Vol. E73. No.7, pp. 1133-1146 (1990)

[11] The MultiMediaCard System Specification Version 3.1, MMCA Technical Commitee, June 2001
http://www.mmca.org/

[12] 畠山卓久，丸山秀史，千葉哲央：音楽コンテンツの超流通とセキュリティ．FUJITSU，Vol.52，No.5，p.473-481，2001年9月．
http://magazine.fujitsu.com/