特集

音楽コンテンツの超流通とセキュリティ

Superdistribution and the Security of Music Content

あらまし

インターネットを用いたメジャー系音楽配信が日米を始めとして多様な形でサービスされており，日本ではPHS（簡易型携帯電話）を用いた音楽配信サービスも始まっている。富士通ではこうした音楽を始めとする高価値コンテンツの超流通を想定したセキュリティ基盤技術としてUDAC（Universal Distribution with Access Control）を提供している。ブロードバンド化とコンテンツ交換アプリケーションの普及が更に進み，遠隔間でのディジタルコンテンツ大量瞬間複製がすべての人々に容易に実施できる時代が来れば，ますますオープンで柔靭（じゅうじん）性の高いコンテンツ保護技術として，UDACのような仕組みが重要になる。

本稿ではUDACを核としてサービスを実現した「ケータイdeミュージック」およびこのサービスとPCとの相互運用方式を紹介する。本方式の高い柔靭性が評価され，ヒット曲がCD販売前に配信されたことはこの成果の一つである。

Abstract

Major record companies now provide various Electronic Music Distribution (EMD) services over the Internet. In Japan, EMD services have been started through mobile phone networks. Fujitsu provides its Universal Distribution with Access Control (UDAC) as a security infrastructure for superdistributed, highly value-added content, for example, music belonging to a major record company. As a result of UDAC, the hit chart was recently distributed by EMD before being distributed on CD. If the spread of broadband networks and remote file exchange applications eventually make it possible for remote users to share and make instant bulk copies of digital content, mechanisms such as UDAC that can provide open, flexible, and strong content protection technology are expected to become more important. This paper introduces a UDAC-based service called “Keitaide-Music” (music on your mobile) and describes how the interoperability between mobiles supporting Keitaide-Music and PCs can be realized.

畠山卓久（はたけやま　たかひさ）
開発企画統括部計画部 所属
現在，UDACの企画に従事。

丸山秀史（まるやま　ひでふみ）
開発企画統括部情報アプライアンス開発部 所属
現在，UDACおよびストリーム配信の企画・開発に従事。

千葉哲央（ちば　てつひろ）
開発企画統括部情報アプライアンス開発部 所属
現在，DRMおよびストリーム配信の企画・開発に従事。

ま え が き

インターネットを用いた音楽配信が日米を始めとして多様な形でサービスされており，日本ではPHSを用いた配信も始まっている。また，ナップスターやグヌーテラのような遠隔コンテンツ交換アプリケーションが著作権の面から問題視され，コンテンツ保護技術に対するコンテンツホルダ（レコード会社など）の要求も高まっている。富士通ではこうした状況に応えるべく，音楽を始めとする高価値コンテンツの超流通(注)を想定したセキュリティ基盤技術としてUDAC（Universal Distribution with Access Control）を提供している。

本稿ではUDACを核としてサービスを実現した「ケータイdeミュージック」およびこのサービスとPC（パーソナルコンピュータ）との相互運用を実現するPCソリューションを紹介する。

音楽超流通の要件とUDAC

UDACではディジタルコンテンツの超流通を想定し，コンテンツホルダからのコンテンツ保護要件を満足する機構を持つ。また，コンテンツの超流通を実際に行うに当たっての脅威を独自に想定し，それらの脅威も加味した上で，想定したすべての脅威に向けての対策をUDACに盛り込んでいる。

● 超流通の要件

筑波大学の森亮一名誉教授は「超流通」の定義[1]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

(1)に関しては，暗号化したディジタルコンテンツを復号鍵の配信と分離して配信するようにすれば，ブロードバンドの時代には必然的に実現される。(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。

(2)に関しては，超流通のセキュリティ要件の一項目であり，UDAC技術の一つであるUDAC-MB（Universal Distribution with Access Control - Media Base）を用いて実現することができる。

なお，超流通のセキュリティ要件にはUDAC-MBで満足する遠隔コンテンツ利用制御以外に次のようなものがある。

(1) SSL（Secure Socket Layer）などを用いた電子商取引のセキュリティ
(2) 電子透かしによる不正アクセス検出
(3) ディジタル署名によるコンテンツの完全性維持

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。

● コンテンツホルダを始めとする各業界の要件

音楽コンテンツ配信システムに対するコンテンツホルダの要求はSDMI（Secure Digital Music Initiative）の仕様[2]としてまとめられており，配信を受け，再生するPCや携帯電話はこれに準拠しなければならないものとされている。またレコード店舗など既存流通チャネルとの協調の一環として暗号化コンテンツのディスク記録媒体を用いた流通やKIOSK端末への配信との連携なども考慮しておく必要がある。

さらに配信サービス運営上の要件として，ライセンス（コンテンツ復号鍵）配信時の回線切断への対処が要求される。

● 実際の脅威と各セキュリティ対策

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策を脅威の主体ごとに**表-1**に示す。

表-1 高価値コンテンツ流通時の脅威と対策

主体	攻撃（脅威）		対抗手段
機器の利用者	機器内部解析・露呈		1 機器・ソフトのTRM化
	なりすまし	機器の偽装	2 TRM認証
		再送攻撃（Replay）	3 TRM認証で共有した一時的な鍵で暗号化
網または機器の利用者	認証局またはTRM種別の秘密鍵推定		4 CRLによる鍵更新
	TRM種別の秘密鍵または一時的な秘密鍵露呈		5 TRM個別鍵でコンテンツ復号鍵を暗号化
製造者	鍵情報漏洩		6 CRLによるTRM停止
PCの利用者	ソフトウェアTRM解析		7 コンテンツ保護レベル制御

(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。

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。これに対してはコンテンツの移動や復号・再生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。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）の利用者および機器（TRM）の製造者自身を想定する必要がある。

また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を用いてコンテンツ保護を実現することも考えられる。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がソフトウェアTRMを信頼する場合，第四の脅威として，脆弱（ぜいじゃく）なソフトウェアTRMが破られたのち，偽装され，これを信頼したハードウェアTRMにも不正な復号・再生許諾情報が格納されるという事態が想定される。

これらの脅威に対する各対抗手段については後述するが，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（じゅうじん）（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。さらに各TRM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TRM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する必要がある。セキュリティ評価基準ではTRM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。

保護コンテンツの超流通方式：UDAC-MB

UDACは以上のすべての要件を想定した技術であり，その中でUDAC-MBは保護コンテンツのオンライン配信・移動・再生の際のシステム間相互運用を目的として策定した方式および仕様である。

● UDAC-MBの概要

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である。

UDAC-MBの基本サービスモデルを**図-1**に示す。UDAC-MBでは各TRM製造者は配信サービス参入に当たって機器種別ごとにTRM種別公開鍵を生成し，認証局に提出する。認証局ではこの種別公開鍵に認証局の秘

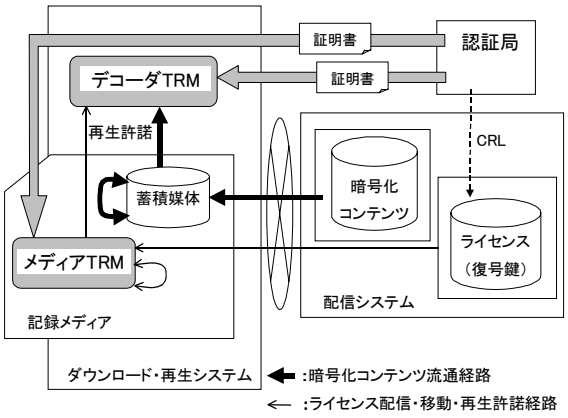

図-1　UDAC-MB基本サービスモデル
Fig.1-UDAC-MB basic service model.

密鍵を用いてディジタル署名を施し，TRM種別公開鍵の証明書を生成する。TRM製造者はこの証明書の発行を受け，自身が製造するTRMに埋め込む必要がある。

UDAC-MBでは暗号化コンテンツの流通とは別個にライセンス（コンテンツ復号鍵）を安全に配信・移動し，デコーダTRMに再生許諾するためのプロトコルを規定している。移動されたライセンスは移動元からは強制的に削除される。図中の記録メディアはUDAC-MBを実装したメモリカードなどの記録媒体を示し，記録メディア内部のメディアTRM内でUDAC-MBのライセンス処理を実行する。またデコーダTRMはコンテンツの復号機能を持ち，復号した結果は再生システムに渡される。

万が一，TRM内の鍵の一つを破られた場合やTRMの不正が明らかになった場合は，認証局からCRL（Certificate Revocation List：証明書失効リスト）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，提示したTRM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。

証明書とCRLおよび暗号アルゴリズムはPKIX｛Public Key Infrastructure（X.509）｝準拠のものを採用した。[3]

コンテンツホルダに指定された次のアクセス条件はライセンス内に埋め込まれた状態で配信され，TRM間で交換される。

（1）　ACm

メディアアクセス条件。記録メディア内で強制するアクセス条件。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。デコーダ内で強制するアクセス条件。再生可能期限，再生可能時間，そのほかを含む。

（3） CRL

証明書失効リスト。認証局の署名を持つ。秘密鍵を破られるなどした証明書の利用停止を指定するのに用いる。一つのTRMが持つすべての証明書が停止されればそのTRMは停止される。

また，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。

● 各対抗手段

表-1の各脅威に対する具体的な対抗手段を以下に説明する。

【TRM】

表-1に示した対抗手段1としての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，アクセス制御情報などの書換えができない構造。

（2） 電流や電磁波の漏れからの秘密情報盗難を防止するメタル層，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）。

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。

【TRM認証】

対抗手段2としてのTRM認証は認証対象のTRMに埋め込まれたTRM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，認証元（配信システムまたはメディア）と認証されるTRM（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。

【ライセンス（復号鍵）の安全な転送】

対抗手段3および5として，再生ライセンスは，**図**-2に示すように，TRM認証で共有したセッション鍵およびTRM個別公開鍵を用いて暗号化してから，転送先TRM

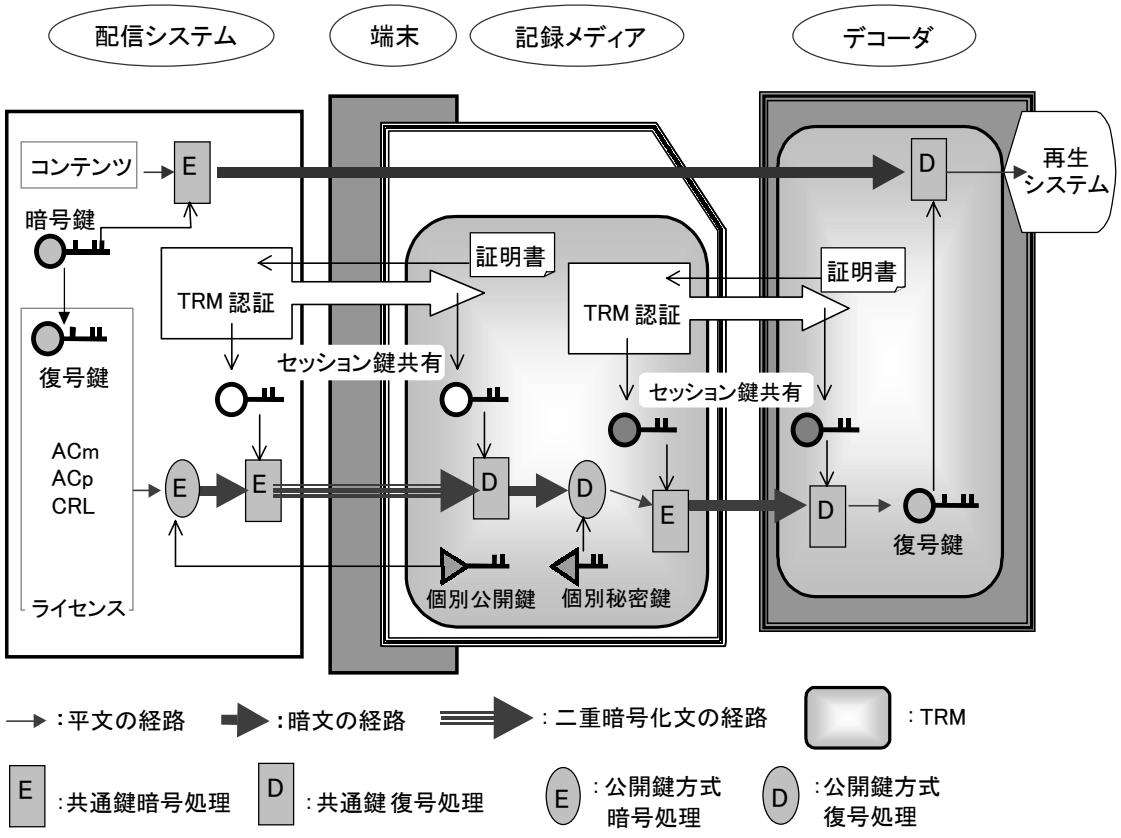

図-2 ライセンスの安全な基本転送方式

Fig.2-Basic secure transformation of license.

に送信される。TRM個別公開鍵は製造した機器一個一個またはソフトウェアのインストールごとに割り当てられる。

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TRM間移動およびメディアTRMからデコーダTRMへの再生許諾に用いられる。

なお，図中にはないが，移動のプロトコルは配信のプロトコルと同じである。

【アクセス制御】

アクセス条件，ACm，ACp，CRLは復号鍵とともにライセンスとして暗号化されて配信され，またTRM間を移動する。各TRM内ではその情報に基づいたアクセス制御を実行する。このうちCRLは表-1の対抗手段4，6として利用することができる。

また，対抗手段7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TRMのレベルとして区別し，さらにACmに指定されたコンテンツ保護レベルに従い，レベルの低いTRM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**-3に示す。

レベル1コンテンツのライセンスはレベルが1以上のTRM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TRMにしか格納することができない。

【暗号アルゴリズム】

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，TRM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。

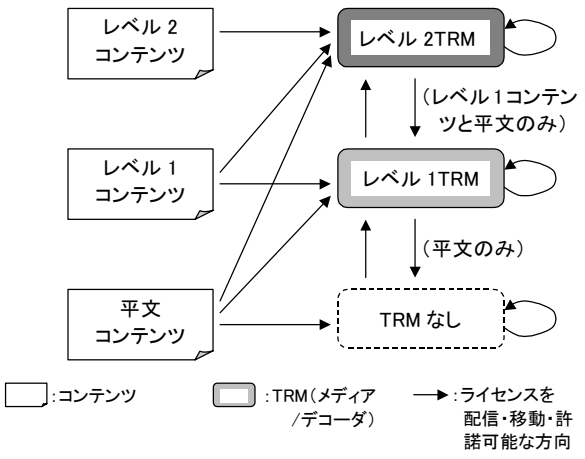

図-3　コンテンツ保護レベルによるアクセス制御
Fig.3-Access control by content protection level.

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）性能が高い。

●　暗号化コンテンツ形式：SCDF

UDACでは前述の超流通定義の(1)で示される要件を実現するため，暗号化コンテンツ形式として定義したSCDF（超流通コンテンツ形式：Super Content Distribution Format）を利用する。SCDFには音楽だけでなく，動画，画像，プログラムそのほかの保護したいマルチメディアデータを複数格納することができる。

SCDFにはコンテンツホルダのディジタル署名が付加され，コンテンツの完全性確認も可能である。

●　特徴のまとめ

以上をまとめると，UDAC-MBは次のような特徴を持つ。

(1)　技術的には暗号化コンテンツを自由に流通可能

(2)　ライセンス（コンテンツ復号鍵＋アクセス制御情報）のみを購入・移動可能

(3)　ハードウェアTRM内に閉じてすべての暗号処理を実行する強力なコンテンツ保護

(4)　不正の影響が広がらない柔軟なシステム交代が可能（CRL投入や保護レベル制御を利用）

(5)　完全にオープンなコンテンツ保護相互運用仕様

(6)　TRMメーカによる自律的な鍵生成と管理

ケータイdeミュージック

●　UDAC-MBを適用した音楽配信サービス

UDAC-MBとSCDFを適用した携帯端末向け音楽コンテンツ配信方式はDDIポケット（株）の音楽配信サービス“SoundMarket”で最初に実装された。このサービスは世界初の携帯電話向け音楽配信サービスとして2000年11月30日から稼働している。

● ケータイdeミュージックの目的

ケータイdeミュージックの主要な目的は新たな音楽流通市場の創出である。

現状のインターネット音楽配信市場ではコンテンツ保護が不十分であり，コンテンツホルダから高価値コンテンツが提供されにくい状況となっている。この状況に対し，以下の問題解決による新たな音楽流通市場の創出を目指した。

(1) UDAC-MBの適用によって音楽コンテンツの配信・流通で強力なコンテンツ保護を実現し，そのことが高価値コンテンツ（最新ヒット曲など）の積極的な配信につながる。

(2) 携帯端末へのオンデマンド配信により，利用者がいつでもどこででも好きな音楽を購入し，聴くことが可能な環境の実現。

● ケータイdeミュージック技術規格の標準化

情報・家電・通信メーカ間でのケータイdeミュージックによるシステム間相互運用を目的として，以下の5社が中心となってケータイdeミュージックコンソーシアムを設立した。

・三洋電機株式会社
・株式会社日立製作所
・日本コロムビア株式会社
・株式会社PFU
・富士通株式会社

ケータイdeミュージックのシステム間相互運用仕様は「ケータイdeミュージック技術規格書[5]」としてこのコンソーシアムで規格化されている。

● 配信システム

“SoundMarket”音楽配信サービスで構築した配信システムの概要を**図-4**に示す。このサービスではコンテンツ送信時の通信速度と通信料を考慮してPHS（最大通信速度64 kbps）での配信となった。図中のアミ掛け部分は富士通，（株）富士通インフォソフトテクノロジおよび（株）PFUが開発・構築した。

(1) 配信対象コンテンツ

UDAC-MBは配信対象コンテンツの形式を限定してはいないが，今回のサービスでは配信対象音楽コンテンツの圧縮形式をMP3（MPEG1 Audio Layer 3）とした。

(2) PHS網および課金システムとの関係

端末利用者からのコンテンツおよびライセンスのダウ

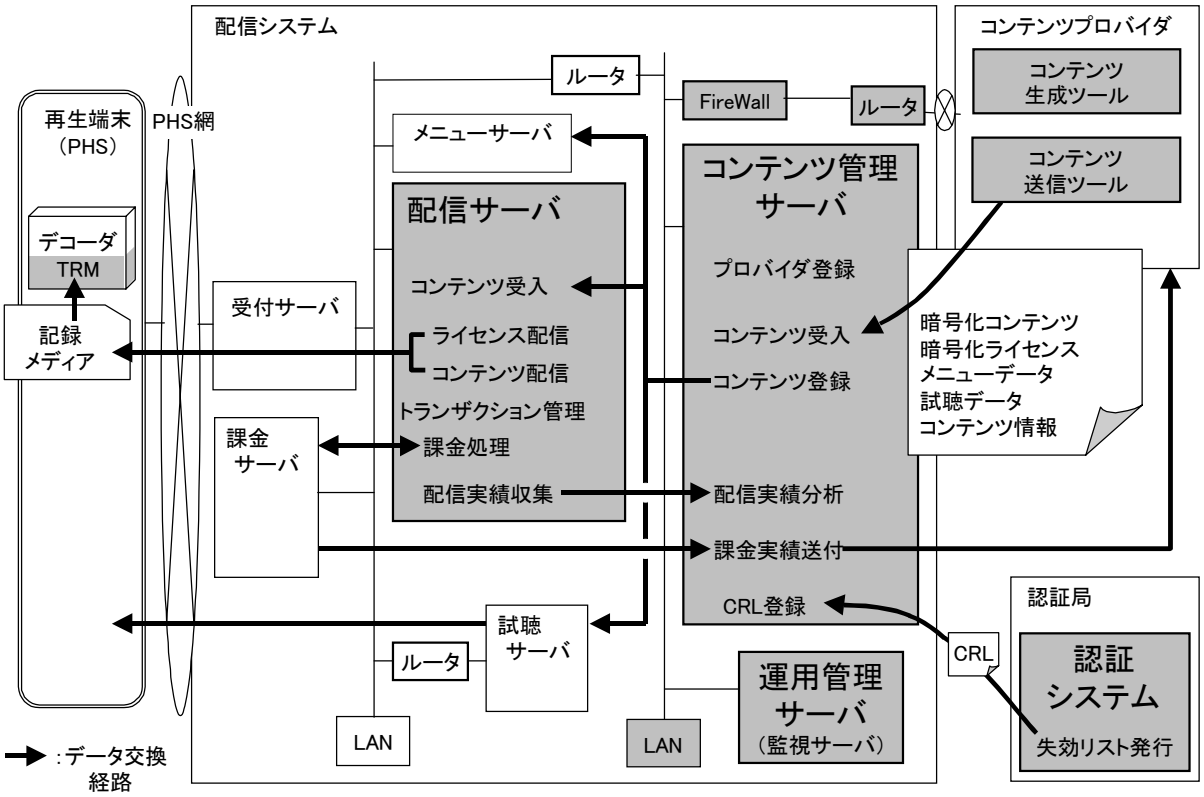

図-4 ケータイdeミュージック配信システムの全体構成
Fig.4-Whole compositions of “Keitaide-music” distribution system.

ンロード要求は音声通話時と異なる受付サーバ（大容量データ通信用のサーバ）で受信し，ここでPIAFS（PHS Internet Access Forum Standard）からTCP/IPに変換されて配信サーバに要求が送られる。

配信サーバは課金トランザクションとUDAC-MBトランザクションとの関係を管理してライセンス配信と課金との整合性を実現している。

(3)　配信システムの構成

配信システムの富士通担当部分は以下のサーバから構成される。

・配信サーバ

暗号化コンテンツ，ライセンスおよびCRLの配信ならびに配信実績情報の収集。

・コンテンツ管理サーバ

暗号化コンテンツ，ライセンスおよびCRLの登録受け入れと配信サーバへの登録ならびに配信実績情報の分析。

・運用管理サーバ

システムを構成する各マシンの監視および運用処理のスケジューリング実行。

(4)　記録メディア，デコーダの停止

万が一，記録メディアあるいはデコーダの秘密鍵が破られたと判断された場合，コンテンツやライセンスの流出によるコンテンツホルダの損害を最小限に食い止めるために，破られた鍵を失効する。

記録メディア，デコーダの鍵を失効させる場合には，認証局から発行されたCRLを配信サーバがライセンス配信時に配信する。配信サーバと記録メディアは配信されたCRLをチェックし配信先メディアや再生許諾先デコーダの鍵が失効されている場合は，ライセンスの配信あるいは再生許諾をエラーで終わらせる。したがって鍵が失効された記録メディアまたはデコーダは，失効後にライセンスあるいはその再生許諾の受信を行うことが不可能となる。

● 配信サーバでのUDAC-MBの適用

本サービスの配信システムにおけるUDAC-MB処理手順例を以下に示す。

(1)　ダウンロード要求コネクション確立

キャリア側サーバからのダウンロード要求を受け付け，課金サーバとの間で課金コネクションを確立する。

(2)　暗号化コンテンツとライセンスの配信

図-2に示した方式により，記録メディアに暗号化コンテンツとライセンスを送信する。その際に，配信サーバが生成したUDAC-MBのトランザクションID（識別子）を課金トランザクションIDと関連させて，DBに登録する。

(3)　ダウンロード要求コネクション閉鎖

課金実績登録を課金サーバに依頼し，配信実績を配信システム内DBに登録する。

● 再生端末（携帯電話・PHS）

配信時にライセンスと暗号化コンテンツが再生端末に差し込まれた記録メディアにダウンロードされ，再生時はそれらが記録メディアからデコーダに送られ，復号されて，再生される。ケータイdeミュージックでは再生端末に挿入可能なUDAC-MB実装記録メディア（レベル2TRM）としてセキュアMMC（Secure Multi MediaCard）を利用する。また，再生端末に内蔵したデコーダ（レベル2TRM）の開発については，暗号関連とハードウェアTRM化を富士通が担当した。

● 通信中断時の対処

配信サーバのUDAC-MBトランザクション管理と記録メディアおよび再生端末との連携により，配信処理中に通信が中断した場合でも安全に処理を完了することを可能としている。まず，記録メディアはそのハードウェアTRM内にUDAC-MBトランザクションログを保持しており，かつ，このログは外部からの更新を不可能としている。したがって，ライセンス配信中断に対するユーザクレームに対して不正中断か否かを記録メディアから安全に検出可能である。さらに，再生端末の内部メモリでダウンロード済サイズを保持しており，通信中断後の再接続で配信サーバにそれらの情報が渡される。これにより，配信サーバは対応するUDAC-MBトランザクションについてダウンロードが完了していない部分の配信を安全で確実な課金処理を伴って再開することができる。

PCソリューション

つぎに，UDAC-MBを一般のPCでのコンテンツ利用・操作に適用したPCソリューションの例を二つ説明する。本稿では，ケータイdeミュージックに対応した再生端末（PHSなど）と連携する例と，インターネット配信に対応する例を取り上げた。

なお，PCソリューションのモデルならびにシステム間相互運用仕様は参考文献[6]にまとめられている。

● ケータイdeミュージック連携PCソリューション

PCソリューションは，上述のケータイdeミュージック

システムとの相互運用が可能であり，以下の機能を持つ。

（1） PHSなどの再生端末でダウンロードした楽曲のPCへのバックアップ・リストア

（2） 超流通CD-ROM（後述）との連携

（3） 音楽CD，MP3データのPCからの再生端末への取込み

このPCソリューションは，PCに接続するセキュアMMCリーダライタ，およびそれをサポートするソフトウェアから構成される（**図-5**）。

セキュアMMCの記憶容量は限られており，64 Mバイトの場合，20曲程度ダウンロードすると，容量に不足が生じる。こうした場合に，再生端末から取り出したセキュアMMCをリーダライタに差し込み，購入済の曲の暗号化コンテンツをPCにバックアップすることで，新たな曲をダウンロードできるようになる。

超流通CD-ROMには，SCDF形式の暗号化された音楽コンテンツが多数収録されている。ユーザは気に入った曲をセキュアMMCにコピーし，PHSなどの再生端末でライセンスを購入するだけで，その再生端末で楽しむことができる。この場合は，ライセンスのみのダウンロードとなるので，暗号化コンテンツとライセンスの両方をダウンロードする場合と比べて，楽曲購入が短時間で済むというメリットがある。超流通CD-ROMには各コンテンツの情報や試聴データ（45秒以内）も収録され，PCで閲覧・再生ができる。

インターネットで入手または音楽CDから変換したMP3データファイルをSCDFにカプセル化し，SDMIに準拠した方式でセキュアMMCにチェックアウト（再生ライセンスの移動で，さらに複製や移動をすることはできない）し，PHSなどの再生端末で聴くこともできる。この場合，ユーザは新たにライセンスを購入する必要はない。

● インターネット配信ソリューション

前述のPCソリューションは，PHSなどの再生端末との連携を主体とするものだが，音楽コンテンツをインターネット経由でPCや半導体メモリ・オーディオプレーヤ（セキュアMMCなどの半導体記録媒体を抜き差し可能なまたは内蔵する携帯音楽再生機器）へ配信するソリューションもある。

このソリューションは，インターネット上の音楽配信サイトから暗号化コンテンツおよびレベル1，レベル2コンテンツのライセンスをPCや半導体メモリ・オーディオプレーヤへ配信するものである。レベル2のライセンスは，保護強度の高いセキュアMMCなどのハードウェアTRM内にのみ格納され，レベル1のライセンスは，PC上のソフトウェアTRM内にも格納可能である。

なお，半導体メモリ・オーディオプレーヤへのコンテンツ格納方法は，ケータイdeミュージック対応再生端

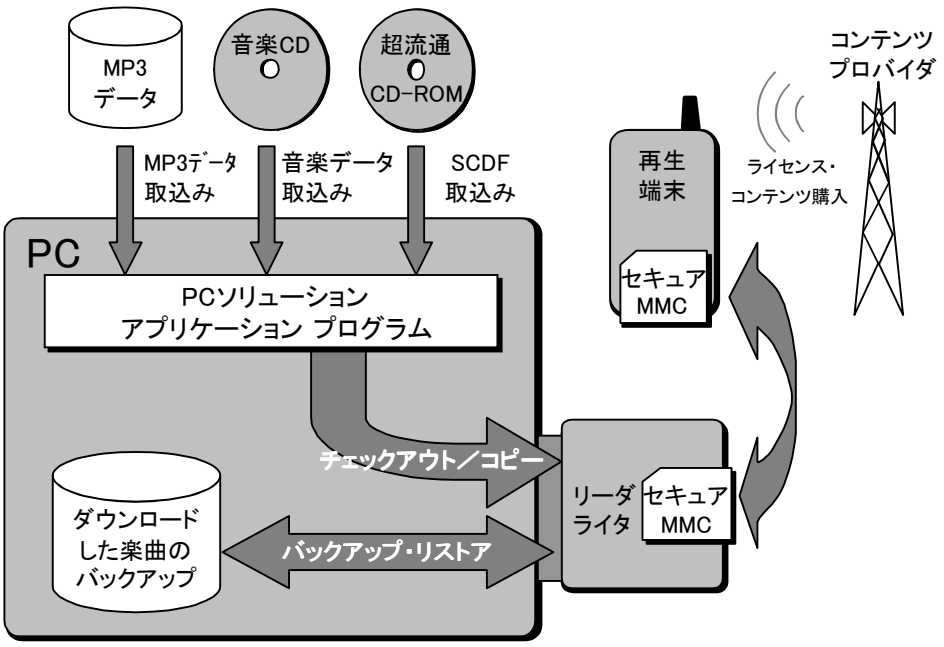

図-5 PCソリューションの例
Fig.5-Example of PC solution.

末への格納方法と互換性があり，セキュアMMCを介して，相互にコンテンツ交換ができる。

応　　用

UDACは更に次のようなシステムに応用できる。

(1)　動画配信システム

動画像のストリーム配信，ダウンロード配信へのUDAC適用により，より高価値のコンテンツを安心して配信することが可能となる。

(2)　文書交換システム

従来のパスワードを用いた文書保護とは異なり，パスワード入力に頼らないユーザの視点での操作性が高いアクセス制御を行うことができる。電子メール，秘密文書管理，オンラインニュースサービスなどに適用可能である。

(3)　静止画アクセス制御

UDACはブロマイドなどの画像ファイルの保護にも応用できる。

(4)　プログラムのライセンス管理

UDACの適用により，プログラムのオンライン販売，期間限定ライセンス販売，試用ライセンスの発行などに当たって，従来方式に比較し，利用の便を損なわずにソフトウェア利用権盗用のリスクを低減することが可能となる。

(5)　AV機器との相互運用

UDAC-MBは映像・音響専用機器などのネットワークに接続しない再生装置への実装も想定した方式である。また，高解像度化が進む最先端の映像機器や周波数帯域が拡大する高級オーディオ機器において，より高いコンテンツ保護強度が求められる場合，ハードウェアTRMに閉じた保護を実現したUDAC-MBを用いれば，これを満足することも可能である。

む　す　び

UDAC-MBを適用した音楽配信サービス“SoundMarket”では，UDACによる強固な著作権保護機能が評価され，ヒット曲のシングルCD発売前配信が実施された。

本稿で紹介したUDAC実装例は，音楽コンテンツの配信に限定されたものであるが，UDACは，動画・画像・文書・プログラムなどの著作権に関わるすべてのコンテンツに適用することができる。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交代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のような仕組みが重要になる。

参 考 文 献

(1)　森亮一ほか：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)　天野大緑ほか：セキュリティ技術．*FUJITSU*，Vol.48，No.2，p.121-128（1997）．

(4)　鳥居直哉ほか：楕円曲線暗号．*FUJITSU*，Vol.50，No.4，p.197-201（1999）．

(5)　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/index_j.html

(6)　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/index_j.html