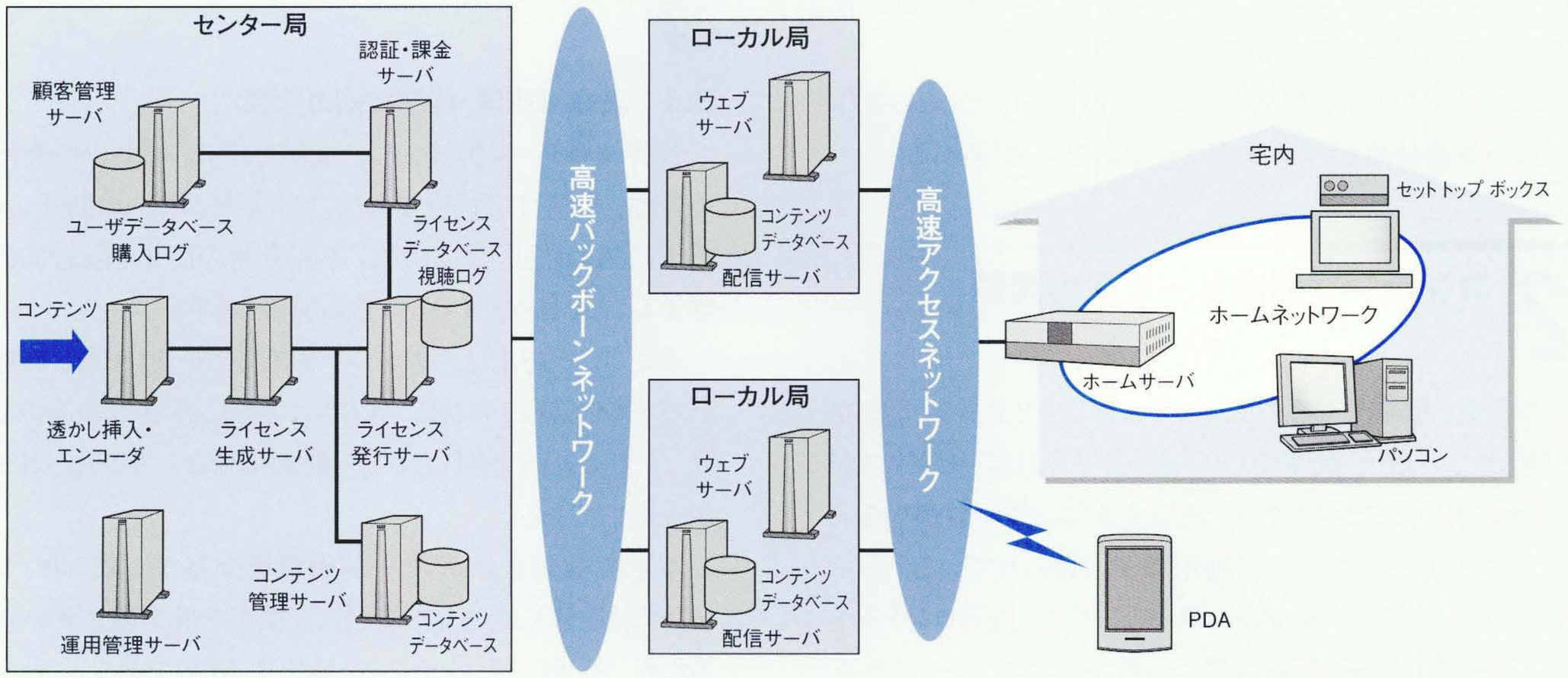
コンテンツ配信ソリューションにおける著作権管理・保護技術

Digital Technology for Rights Management in Content Distribution

岡山 祐孝 *Masataka Okayama*　　森野 東海 *Harumi Morino*



注:略語説明　PDA(Personal Digital Assistant)

著作権管理・保護を中心としたコンテンツ配信システム例

有料コンテンツを配信するコンテンツ配信システムでは，ライセンス生成サーバで暗号化されたコンテンツが，コンテンツ管理サーバで管理され，配信サーバから各端末に配信される。暗号化に使用されたかぎは，利用条件とともにライセンスとしてライセンス発行サーバで管理される。端末で暗号化されたコンテンツを利用する場合，ライセンス発行サーバからライセンスを取得してコンテンツを復号する。

ブロードバンドネットワークの普及により，映像や音楽を中心とした大容量コンテンツの配信サービスが立ち上がりつつある。コンテンツ配信サービスを定着させるためには，ユーザーの購買意欲をそそるような，魅力あるコンテンツを流通させることが不可欠である。また，ディジタルコンテンツは画質が劣化することなく容易に複製できるので，不正コピーや不正利用などの著作権侵害から確実にコンテンツを保護し，コンテンツの著作権保有者が安心してコンテンツを提供することができる環境が必須となる。

日立製作所は，ユーザーが正規に購入したコンテンツを，いつでもどこでも，ユーザーが所有する複数の端末で利用できる，新しいコンセプトの著作権管理・保護(DRM:Digital Rights Management)技術の研究開発を推進している。そのコンセプトは，コンテンツの著作権を保護しつつコンテンツを利用し，その対価を支払うユーザーの利便性向上をねらいとするものである。日立製作所は，このDRM技術と動画対応電子透かし技術を組み合わせた統合ソリューション化も推進している。

1 はじめに

ADSL(Asymmetric Digital Subscriber Line)やFTTH(Fiber to the Home)といったブロードバンド回線の急速な家庭への普及により，映像や音楽を中心とした大容量コンテンツ(情報内容)を家庭に配信できるネットワーク環境が整いつつある。さらに，コンテンツの圧縮技術やストリーミング技術など配信技術の進展と相まって，高品質を維持したまま家庭へコンテンツを配信できるようになってきた。

このような状況の中で，コンテンツをユーザー端末に配信し，ユーザーからコンテンツの利用料(視聴料)を徴収することを

基本のビジネスモデルとする，有料コンテンツ配信サービスが立ち上がりつつある。このコンテンツ配信サービスを成功させる条件の一つとして，ユーザーの購買意欲をそそるような，魅力あるコンテンツを，多く流通させることがあげられる。つまり，コンテンツホルダから，いかに多くのコンテンツを集められるかがポイントになる。

一方，現在のコンテンツ配信環境では，コンテンツの著作権者が安心してコンテンツを提供することができる著作権保護機構が十分に確立していない。このため，コンテンツの著作権者の多くは，不正コピーや不正利用に代表される著作権侵害について懸念しているのが実情である。

ここでは，コンテンツ配信サービスに必要不可欠となる著作権管理・保護技術と，そのソリューションについて述べる。

2 コンテンツ配信サービスの課題

コンテンツ配信サービスは，今後の新しいビジネスとして有望視されているが，収益性という観点から見れば，ビジネスがまだ地に着いたばかりである。流通するコンテンツ数が少ないので，ユーザーのコンテンツ利用機会が限られているからである。流通コンテンツが少ない理由としては，既存コンテンツを二次利用する際の権利処理の煩雑さや，コンテンツの不正コピー・不正利用による著作権侵害のおそれなどがあげられる。

前者は例えば，テレビ放送番組をインターネット上に配信する場合に起こる問題である。通常，テレビ番組には，番組制作者，原作者，脚本家，出演者，作詞家，作曲者，演奏者などが所有する著作権などの諸権利が存在する。テレビ放送番組は，コンテンツ配信サービスの有力コンテンツと目されている。しかし，これをインターネットに配信するためには，各権利者に利用許諾を取り付ける必要があり，それには膨大な労力を必要とする。これに対応して，総務省が中心となって，コンテンツ流通の円滑化に向けた権利クリアランスシステムに関する取り組みを行っており[1]，コンテンツの二次利用も考慮した取引ルールの整備が期待される。

後者は，実際にコンテンツをインターネット上に配信した場合に起こる問題である。コンテンツを配信する際，著作権管理・保護機構が十分でないと，ネットワーク上での盗聴や成り済ましによる不正取得，端末上での不正コピーや不正利用などによる，いわゆる海賊版が横行しやすい。海賊版が横行すると，著作権者（コンテンツホルダー）に支払われるべき著作権料の回収が困難となる。その結果，コンテンツホルダーはコンテンツ提供に消極的になり，流通コンテンツが不足する。これを回避するためには，暗号技術や認証技術を応用した著作権管理・保護技術が必須となる。

コンテンツ配信サービスビジネスは，配信されたコンテンツの利用料を，ユーザーが支払うことで成り立つ。言いかえると，ユーザーがコンテンツを利用しないと，ビジネスとしては成立しない。そのため，ユーザーがコンテンツを利用しやすい環境を整備することも必要である。一般的に，著作権保護とユーザーの利便性は対極に位置するが，この両者を両立させ，バランスよく充実させることが，コンテンツ流通を促進する重要課題である。

3 著作権管理・保護技術

3.1 著作権管理・保護技術の分類

著作権管理・保護技術は，文字どおりコンテンツの著作権を管理，保護する技術であり，(1) 不正コピーの防止，(2) 不正流通の防止，および(3) 不正利用の防止を統合的に管理することを目的とするものである（**表1**参照）。

不正コピー防止は，コンテンツが端末からテレビなどの外部デバイスや記録メディアに出力される際に必須となるものであり，すでに規格化されたコピー制御機構などで実施されるのが一般的である。

不正流通防止は，コピー制御機構が万が一破られ，コンテンツが違法に流通した場合に，損害を最小限に食い止めるため，不正流通コンテンツを摘出するものである。これを実現する一つの手段として，「電子透かし技術」があげられる。これは，電子透かしを用いてコンテンツの著作権情報や購入ユーザーを特定する情報をコンテンツに埋め込んでおき，インターネットに流通するコンテンツに対して，透かしを検出することにより，不正流通コンテンツの摘出を行うものである。

不正利用防止は，コンテンツを購入したユーザーが，購入時に指定されたコンテンツの利用条件に反して利用することを防御することであり，言いかえると，ユーザーのコンテンツ利

表1 著作権管理・保護技術の分類

著作権管理・保護技術は，目的別に，(1) 不正コピー防止，(2) 不正流通防止，および (3) 不正利用防止に分類できる。

	項　目	実現手段	
著作権管理・保護ソリューション	不正コピー防止	DTCP（IEEE1394），CSS（DVD），CPRM（DVD-RAM），HDCP（DVI）など	電子透かし，耐タンパ，暗号，認証，PKI
	不正流通防止	電子透かしを応用した不正流通コンテンツの摘出	
	不正利用防止	電子透かし，認証，暗号を応用したコンテンツ利用権管理	

注：略語説明
DTCP（Digital Transmission Content Protection）
CSS（Content Scrambling System）
CPRM（Content Protection for Recordable Media）
DVD-RAM（Digital Versatile Disc Random Access Memory）
HDCP（High-Bandwidth Digital Content Protection）
DVI（Digital Visual Interface）
PKI（Public Key Infrastructure）

用権を管理することである。

日立製作所は，著作権保護とユーザーの利便性を両立させる，新しいコンセプトのコンテンツ利用権管理技術の研究開発に取り組んでいる。その概要について以下に述べる。

3.2 コンテンツ利用権管理の考え方

コンテンツ配信モデルとして超流通配信[2)]をベースとしており，コンテンツは暗号化されていて，自由に流通する。つまり，コンテンツはどのような流通経路をたどってもよく，また，暗号化コンテンツのコピーも自由である。ユーザーは，コンテンツを利用するときに，暗号化コンテンツを復号するために必要な復号かぎと，コンテンツの利用条件を含んだライセンスを購入し，利用条件に従って利用する。このモデルで著作権保護を実現するためには，ライセンスに含まれる復号かぎの秘匿性や，利用条件の強制が条件となる。

コンテンツ配信ビジネスでは，ライセンスを正規に購入したユーザーに，安全かつ正確に配信することが重要であるが，その一方で，ユーザーの利便性を損ねることがないようにしなければならない。そのためには，以下のような要件を満たすコンテンツ利用権管理が重要である。

(1) ユーザーが所有する複数の端末での利用

正規に購入したコンテンツは，ユーザーが所有する複数の端末，例えばパソコンやセットトップボックス，PDA(Personal Digital Assistant)など，さまざまな端末で利用できることが望ましい。端末ごとにライセンスを購入することになれば，ユーザーにとって割高感はぬぐいきれない。ユーザーは，いつでもどこでもコンテンツを利用できることが重要である。

(2) 同じ端末で複数のサービス利用

サービスごとに違う端末が必要になると，コンテンツごとに端末を変えるなどの操作が必要となり，不便である。このような状況を避けるためにも，同じ端末で複数のサービスを利用できることが望ましい。しかし，ライセンスの管理をしないと，利用したいコンテンツのライセンスの所在がわからなくなる。このようなことを考えると，購入したライセンスを集中的に管理する必要がある。

3.3 ライセンス管理

ユーザーが所有する複数の端末でライセンスを共有して使用するために，ライセンス発行サーバでライセンスを管理する。端末で利用するときは，ライセンスそのものではなく，ライセンスに含まれる利用条件を制限し，一時的に生成されるライセンス(一時ライセンス)を取得して利用する。一時ライセンスを取得するときには，ネットワーク上での盗聴や成り済まし，改ざんを防ぐために，一時ライセンスを受け渡しする機器・モジュール間で，相互認証と暗号化通信を行う。また，ユーザーがコンテンツを利用している間は，一時ライセンスを端末に保持しておく必要がある。このため，端末にはユーザーがアクセスできない耐タンパ領域(ライセンスモジュール)を設け(**図1**参照)，一時ライセンスをその領域に格納して管理する。また，暗号化コンテンツを復号し，再生を行うデコーダモジュールでも，コンテンツかぎや暗号化されてないコンテンツデータを扱うためには，耐タンパな仕組みが必要となる。

3.4 コンテンツ利用の手順

コンテンツを利用するための手順は以下のとおりである。

(1) 相互認証・かぎ交換

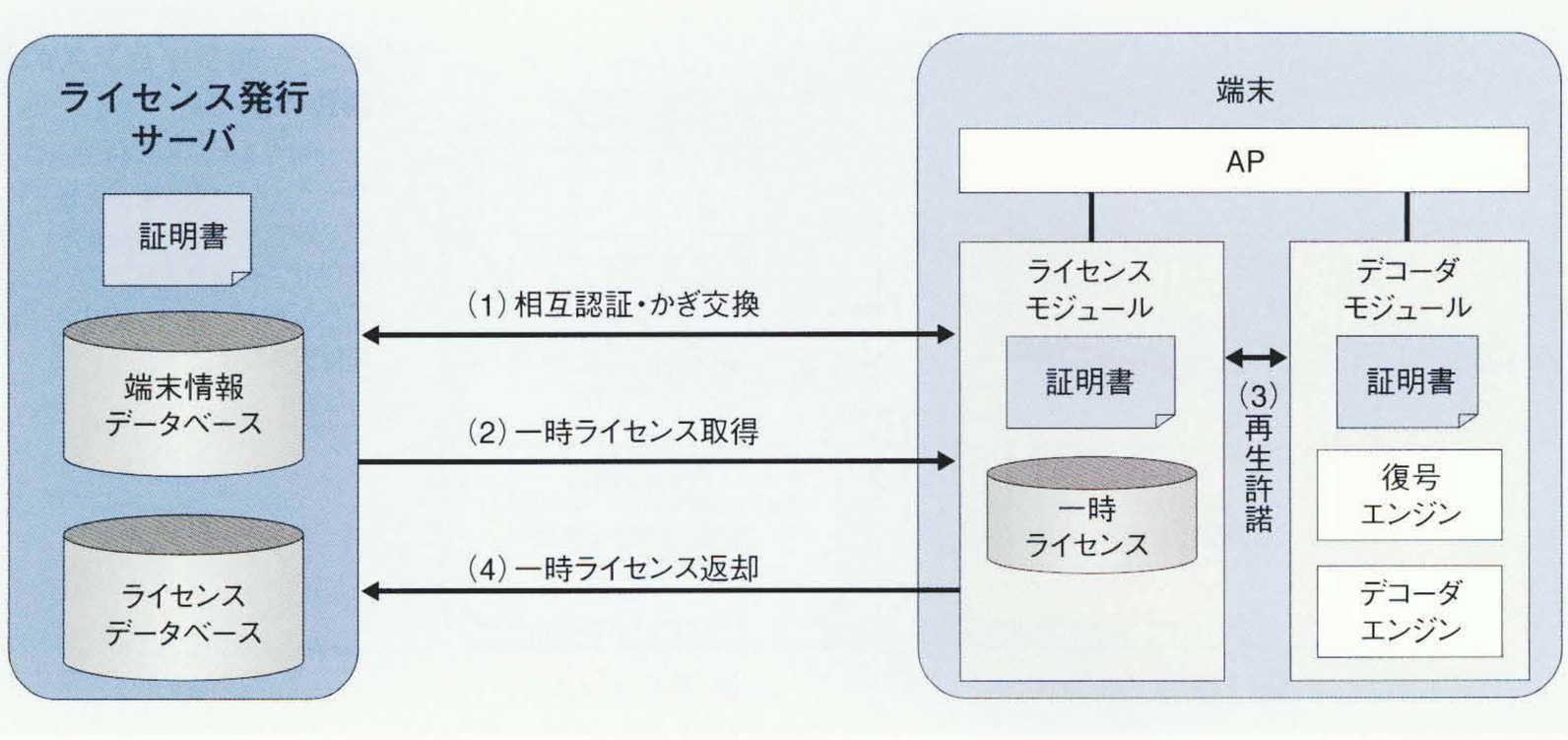
一時ライセンスを安全に配信するために，相互認証・かぎ交換から始める。この手順はPKI(公開かぎ暗号方式)をベースとしており，認証局(CA:Certification Authority)から発行された証明書を用いて，端末とライセンス発行サーバの間で相互認証を行う。ライセンス発行サーバでは，あらかじめ一時ライセンスを発行できる端末の情報を管理しておく。相互認証を行うときには，端末情報を用いて一時ライセンスの取得要求のあった端末に，一時ライセンスを発行できるかどうかの確認も行う。

認証が済むと，証明書に含まれている公開かぎを用いてかぎを交換する。一時ライセンスを配信するときに暗号化するためのかぎ(共通かぎ)を，端末の耐タンパ領域であるライセンス

図1 ライセンスの管理方法

ライセンスを端末に格納するのではなく，利用時に端末で一時ライセンスを取得し，終了後にこれを返却することにより，他の端末での利用が可能となる。

注:略語説明
AP(Application)



モジュールとライセンス発行サーバで共有する。この共通かぎを用いて一時ライセンスの暗号化通信を行うことで，盗聴や成り済まし，改ざんを防ぐことができる。

(2) 一時ライセンス取得

ユーザーがコンテンツを利用するとき，端末(ライセンスモジュール)でライセンス発行サーバから一時ライセンスを取得し，耐タンパモジュールに格納する。このとき，一時ライセンスは，上記(1)で共有した共通かぎを用いて暗号化され，送信される。また，ネットワーク障害などでライセンス発行サーバとの接続が切断されても，一時ライセンス取得が再開できる仕組みを設けている。

(3) コンテンツ再生

実際にコンテンツを利用するときは，コンテンツを再生するデコーダモジュールで，ライセンスモジュールからコンテンツかぎと再生条件を含む再生許諾を受信する。その後，暗号化コンテンツを復号し，再生条件に従って再生する。再生許諾の受信時に，そのデータが汎用のバスを経由し，盗聴，改ざんされる可能性もある。そのため，ライセンスモジュールとデコーダモジュールで認証を行ったうえで，かぎ交換で共通かぎを共有して暗号化を行い，コンテンツかぎの秘匿性を保つ。

(4) 一時ライセンス返却

コンテンツ利用を終えればライセンス発行サーバに一時ライセンスを返却する。このような操作により，ユーザーが所有する他の端末でも，一時ライセンスを取得してコンテンツを利用することができる。このときも，上記(1)で共有した共通かぎで暗号化して送信する。共通かぎが，すでにライセンス発行サーバとライセンスモジュールで破棄されている場合は，再び相互認証・かぎ交換を行う。また，障害が発生した場合には，一時ライセンス取得と同様に，返却が再開できる仕組みを設けている。

3.5 一時ライセンスの利用条件

ライセンスに含まれる利用条件には，再生回数，期限などがある。例えば，10回再生という利用条件のライセンスがあり，端末から3回再生の要求があると，ライセンスは再生回数を7にし，利用条件3回の一時ライセンスを発行する(**図2**参照)。そのとき，端末側で2回しか再生しなければ，その一時ライセンスをライセンス発行サーバに返却し，残りの1回分の利用条件をライセンスの利用条件に併合させ，再生回数を8にする。このように，消費していない一時ライセンスを返却することで，ユーザーは，購入した権利をむだなく利用することができる。

3.6 ホームサーバによるライセンス一括管理

ユーザーが複数の配信事業者のサービスを利用している場合，購入したコンテンツの一時ライセンスは，各配信事業者のライセンス発行サーバに接続して取得することになる。そのため，宅内にホームサーバを設置し，各配信事業者から購入したライセンスをホームサーバで一括管理する(**図3**参照)。これにより，端末をホームサーバに接続さえすれば，購入したすべてのライセンスの一覧が取得でき，一時ライセンスの取得が可能となる。また，端末情報の登録もホームサーバに一度行うだけで済むので，ユーザーの利便性が損なわれることはない。

また，ダウンロード型のサービスでは，ダウンロードしたコンテンツをホームサーバに蓄積しておき，実際の端末での利用では，ストリーミングでリアルタイムに配信すれば端末のハードディスクが必要なくなり，いっそう安価な端末を提供することができる。

ホームサーバは配信事業者のライセンス発行サーバの代行として動作することになり，ライセンスを管理するためには，耐タンパ領域が必須となる。

4 著作権管理・保護ソリューション

日立製作所は，上記のコンテンツ利用権管理技術と電子透かし技術を統合し，ユーザー認証・課金システムと連携させた著作権管理・保護ソリューションの構築に取り組んでいる(17ページの図参照)。

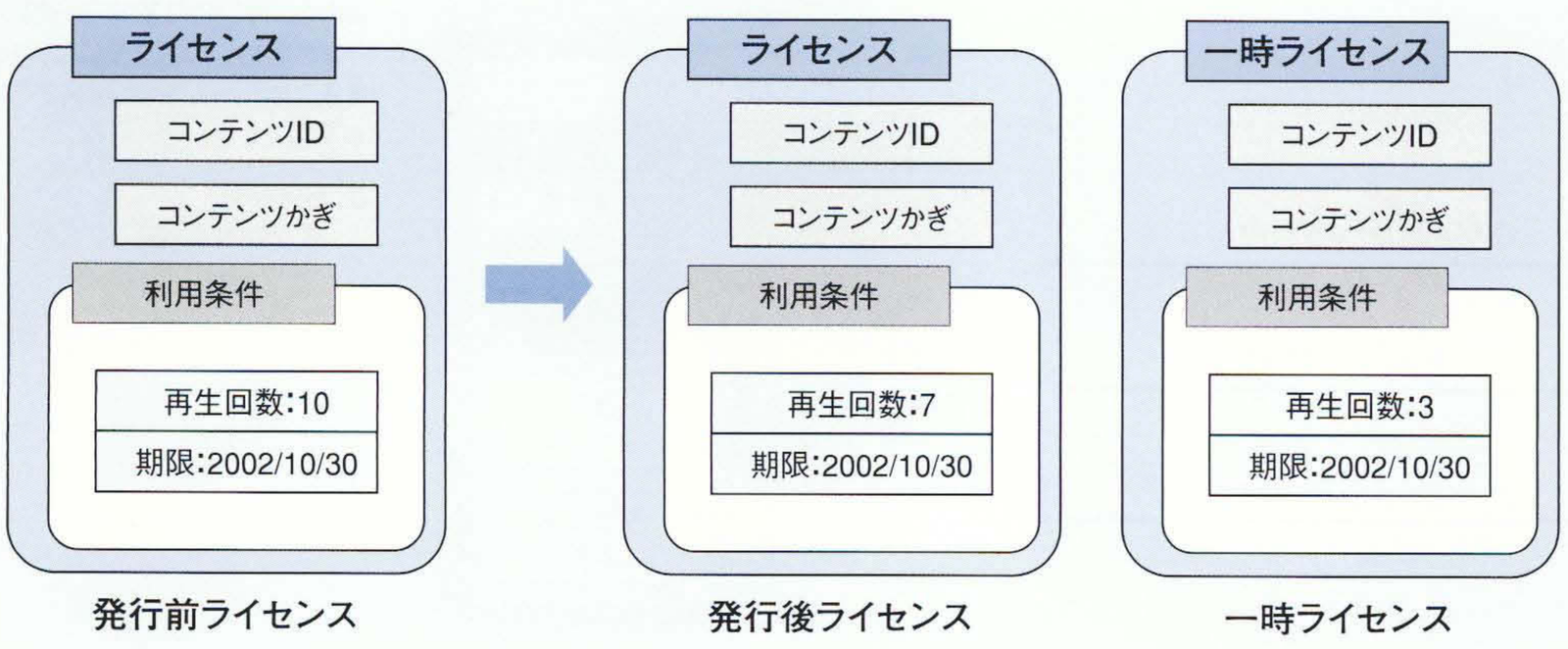


図2 一時ライセンスの利用条件の例

一時ライセンスの利用条件では，ライセンスの利用条件を超えない範囲で設定する。消費しなかった利用条件は，一時ライセンスを返却することにより，ライセンスの利用条件に併合される。

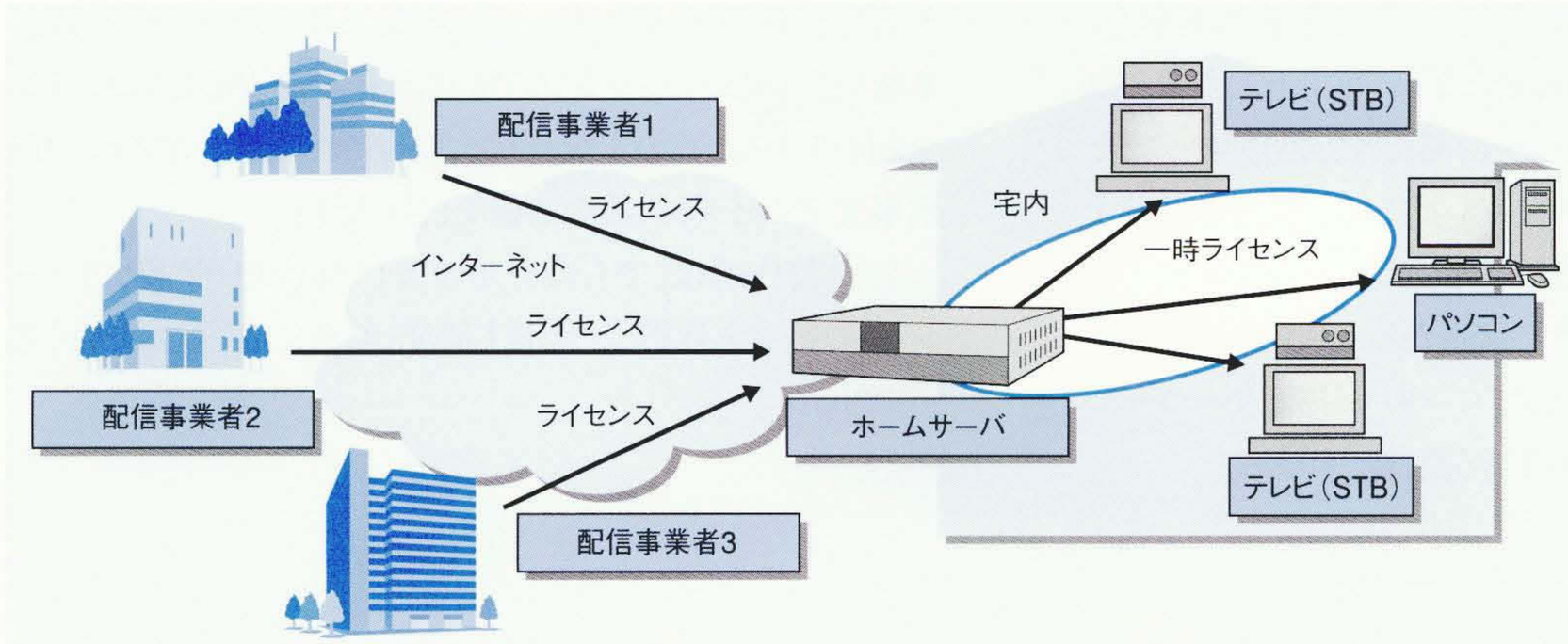


図3 ホームサーバでのライセンス管理の仕組み

ホームサーバでライセンスを一括管理し，端末では，ホームサーバから一時ライセンスを取得して利用する。

注：略語説明
STB(Set-Top Box)

4.1 コンテンツ利用権管理と電子透かしの統合

配信するコンテンツには，その著作権情報やコンテンツに関連する情報を電子透かしで挿入し，不正行為の抑止をねらう。たとえ，コンテンツが不正に流通したとしても，インターネットに流通するコンテンツから透かしを検出することにより，不正流通コンテンツの摘出を行い，著作権者の権利を保護することができる。

コンテンツ利用権管理は，ユーザーが購入したコンテンツの利用権をサーバで管理し，端末からの利用要求に応じて，暗号化通信で一時ライセンスを逐一送信する。端末では，受信した一時ライセンスを耐タンパ領域で管理し，不正利用を防止する。

コンテンツ利用権管理と電子透かしは互いを補完し合う関係にあり，これらを統合することで，さらに堅ろうな著作権管理・保護システムを実現することができる。

4.2 ユーザー認証・課金システムとの連携

コンテンツ利用権管理では，ユーザーがコンテンツを購入することは，コンテンツのライセンスを購入することに等しい。また，ユーザーが所有する複数の端末でのコンテンツ利用を実現するために，ユーザー情報と端末情報を管理する。したがって，コンテンツ利用権管理は，ユーザー認証・課金システムと密接な関係にある。このソリューションでは，ユーザー認証・課金システムも含めたトータルソリューションを提供する。

4.3 著作権管理・保護ソリューションを構成するブロードバンド端末

ユーザーがコンテンツを利用する際，端末で暗号化コンテンツを復号することになる。復号した後のコンテンツは，コピーすると自由に利用することができる。このため，端末では，復号かぎを含む一時ライセンスを厳重に管理するだけでなく，復号した後のコンテンツも同様に，厳重に管理，処理しなければならない。これを怠ると，ライセンスによる利用権管理は意味のないものとなる。

日立製作所は，著作権管理・保護ソリューションを構築するうえで重要となる，ブロードバンド端末の研究・開発にも取り組んでいる(**図4**参照)。VLIW(Very Long Instruction Word)アーキテクチャを採用したメディアプロセッサを開発し，ブロードバンド端末にこれを搭載する。このメディアプロセッサは30GOPS(Giga Operations per Second)の性能を誇るビデオ処理DSP(Digital Signal Processor)であり，多様なアプリケーションに対応する。暗復号エンジン，圧縮映像のデコード機能，動画対応電子透かし検出機能も装備する。したがって，コンテンツ利用権管理の枠組みで配信される暗号化

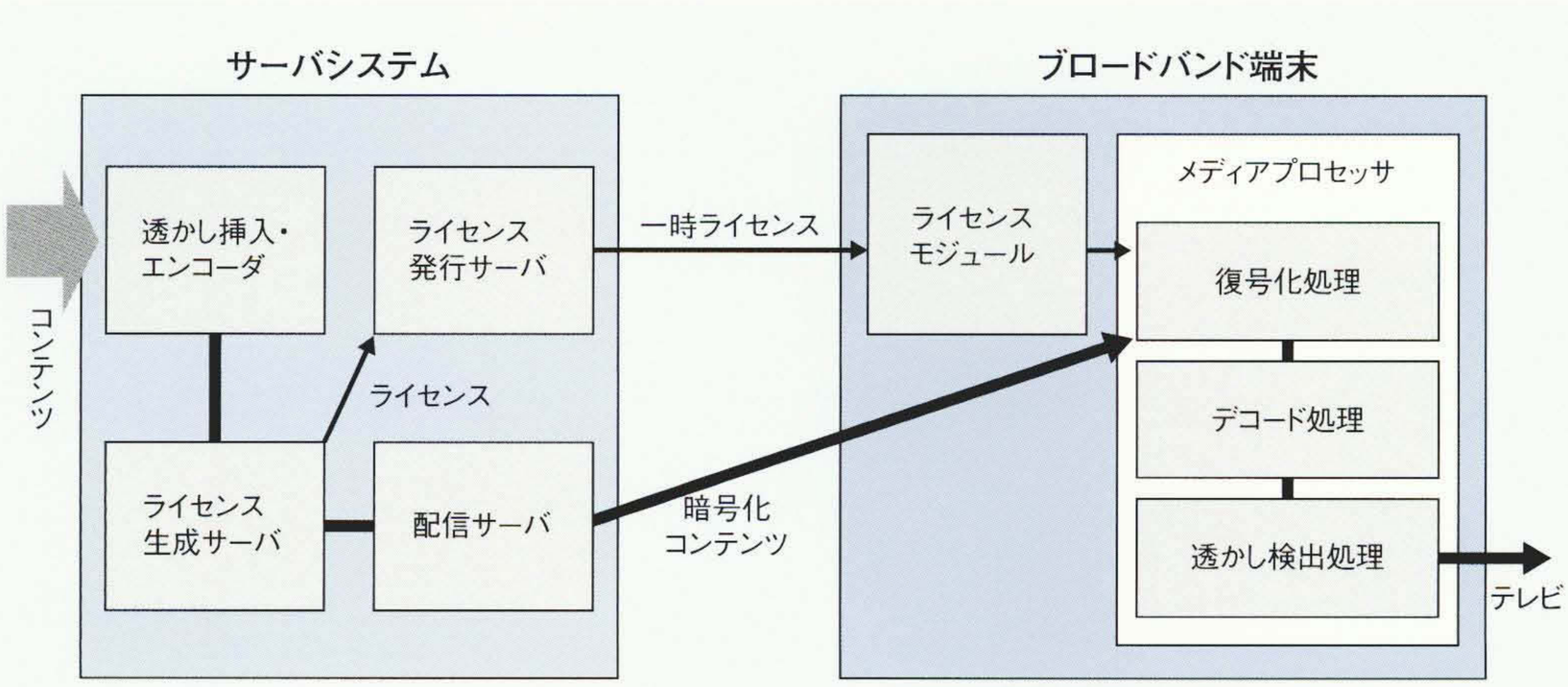


図4 ブロードバンド端末の構成

暗号化されたコンテンツの復号化処理，デコード処理，および透かし検出処理は，すべて一つのメディアプロセッサ内部で行われる。

コンテンツの復号化処理，デコード処理，透かし検出処理が，このメディアプロセッサ一つで可能となる。復号化した後のコンテンツは，このメディアプロセッサ内部だけで処理されることになる。ブロードバンド端末では，テレビにコンテンツを表示する際，アナログ コピー ガード処理を施して出力する。

また，このメディアプロセッサでは透かしの検出も可能であることから，各家庭に設置されるブロードバンド端末一つ一つが，不正流通コンテンツの摘出を行う設備となりえる。

5 おわりに

ここでは，コンテンツ配信サービスが普及し，安心して使えるようにするために必須となる著作権管理・保護技術と，この技術を軸とするソリューションについて述べた。

著作権管理・保護ソリューションによる健全なコンテンツ流通基盤の整備は，コンテンツの権利所有者が安心してコンテンツを提供するための土壌作りである。これにより，コンテンツ配信事業者のビジネス機会は確実に拡大する。

日立製作所は，さらに有用な著作権管理・保護ソリューションの提案を目指し，今後も研究・開発に取り組んでいく考えである。

参考文献

1) 総務省：平成14年版情報通信白書(2002.7)

2) 森，外：歴史的必然としての超流通，情報処理学会超編集・超流通・超管理のアーキテクチャシンポジウム論文集，Vol.94，No.1，pp.67～76(1994)

執筆者紹介

岡山祐孝

1988年日立製作所入社，システム開発研究所 情報サービス研究センタ 第六部 所属
現在，著作権管理・保護ソリューションの研究開発に従事
E-mail：okayama @ sdl. hitachi. co. jp

森野東海

1992年日立製作所入社，システム開発研究所 情報サービス研究センタ 第六部 所属
現在，著作権管理・保護ソリューションの研究開発に従事
電気学会会員
E-mail：morino @ sdl. hitachi. co. jp