DRMの有効性

Digital Rights Management

text：加畑健志

国内のADSL加入者は500万人を超え、多くの人が10メガ超の世界に足を踏み入れている。この状況を見ると、インターネット上の映画や音楽を鑑賞するというライフスタイルが定着してもよさそうなものだが、「インターネット上にはおもしろいコンテンツがない」という言葉が聞かれるのが現状だ。何がインターネットをこのような状況にしているのか？ 大きな原因の1つとして、インターネットでコンテンツビジネスを展開すると、コンテンツが不正利用されるのではないかと映画会社、レコード会社が感じていることがあげられる。そこで、現在、DRMと呼ばれるコンテンツマネージメント技術が注目されている。DRMはどのようにしてブロードバンドでのコンテンツ流通を加速させようとしているのだろうか？　この技術の全貌から答えを見つけていきたい。

ウィンドウズ98とデジタルミレニアム著作権法がDRMに光をあてる

1998年、この年はDigital Rights Management（DRM）という言葉が大きく注目される1年となった。その背景としてはウィンドウズ98の発売によって、インターネットが急激に普及したこと、それにともなってMP3などの音楽データがインターネット上に公開され、社会的問題になったことなどが考えられる。またデジタルコンテンツを持つ企業がインターネットを市場として認識した時期であるのも大きな理由だ。さらに米国でのデジタルミレニアム著作権法（DMCA）の施行（1998年10月28日）により、複製を防ぐ機能を持った著作物をコピーすることも、それをコピーするための機器を売買することも違法となり、デジタルコンテンツを取り巻く情勢が大きく変化したこともDRMがクローズアップされた一因と言える（日本国内では、同じような規制をもうけた「著作権法および不当競争防止法の改正」が1999年10月1日に施行されている）。

もちろん、1998年だけでなく、現在に至るまで注目されているDRMだが、その全体像というといまひとつ見えてこない感がある。その理由は、DRMが一般的にデジタル化されたコンテンツにかかわるさまざまな権利を守りながら、それを配信できるようにする技術の“総称”とされているため、カバーする範囲が非常に広いからだ。まず、DRM誕生以前の著作権保護技術の歴史をさかのぼることで、この把握しにくい技術の実像にせまってみたい。

DRMはユーザーや機器の認証、配布技術などを巻き込んでいる

コピーガードという言葉を聞いたことのある人は少なくないだろう。もちろん、このコピーガード、つまりコピーを防ぐ技術やニーズは、インターネットが普及する以前から存在していた。有名なものでは、今でも使われているビデオテープのコピーガードがあげられるだろう。ただし、アナログメディア全盛の時代ではコピーによる劣化が必ず発生したこと、さらにそれを配布する効率的な方法がなかったなどの理由で、現在ほど大きな問題にはなっていなかった。

では、「プログラム」という簡単に複製でき、劣化もなくコピーできるデジタルデータを扱うコンピューターの世界では、この

コピーガードはどのように発展してきたのだろうか。プログラムがテープやフロッピーディスクに記録されていたころ、それ自体をアナログコピーしてしまえば誰でも使えてしまうので、プログラムメーカーはさまざまな知恵をしぼってそれに対抗しようとしていた。その技術のなかにはフロッピーディスクの回転数を変えないと読み込めないようなフォーマットとそれに対応するデバイスドライバーを独自に開発して自社ソフトでないと読み込めないようにしたものや、ソフト自体はコピーできるものの、「ドングル」と呼ばれる、認証キーを書き込んだ機器をプリンターポートなどに装着し、それがないと起動しないという仕組みを作ったメーカーもあった。

では、これらのインターネット以前のコピーガード技術とDRMはどこが違うのか？それはDRMが単純に著作物の複製を防ぐだけでなく、ユーザーや機器の認証、配布技術などの大きな枠組みを必要とするものだという点で、大きく違ってくるのだ。

「Rights Description」「Rights Enforcement」がコアになる技術

DRMは著作権を守る技術だという説明を見かけることがある。確かに、それは間違いではないが、あまりにも大雑把すぎてわかりにくいのではないだろうか。たとえばウィンドウズメディアプレイヤーがDRM対応と言われても、何がどこで動いていてDRM対応になっているのかすぐにはわからない。これを理解するためには「Rights Description」「Rights Enforcement」と呼ばれる2つの技術に注目すればわかりやすいだろう。

「Rights Description」は権利を持っている人（プロバイダー、ライセンサーなどと呼ばれる）がその権利を買った人（ユーザー）に、その権利をどのように使っていいかを記述するための技術で、たとえばそのコンテンツを「1回しか見られない」「1か月間だけ使用できる」など、プロバイダーとユーザーの間で交わされた契約の内容や条件を表すために使われる。「Rights Description」によって記述された権利や条件はコンテンツ自身のデータに埋め込むことも可能だが、ライセンスキーと呼ばれる別のデータに埋め込み、個別に提供されることが一般的だ。

もう1つの技術「Rights Enforcement」はコンテンツもしくはライセンスキーのデータに、「Rights Description」によって埋め込まれた情報を読み取って、その契約に違反しない範囲での利用を許可する技術だ。ウィンドウズメディアプレイヤーがDRM対応と謳っているのは、コンテンツやライセンスキーに記述された各種の権利を読み取って侵害しないように再生できる「Rights Enforcement」を実装しているからなのだ。

5つのステップでデジタルコンテンツを保護

DRMが利用する技術は大きく「Rights Description」と「Rights Enforcement」に分類できると説明したが、それでは具体的にどのようなフローで著作権管理をしていくのかを説明しよう。大きく分けると

1. パッケージング
2. ディストリビューション
3. ライセンシング
4. キーディストリビューション
5. プレイヤー

の5つのステップが考えられる。

まず「パッケージング」とは配布したいコンテンツをデジタル化し、さらに権利をライセンスキーのデータに埋め込む作業だ。「ディストリビューション」とは「パッケージング」されたコンテンツを配布すること。「ライセンシング」とは権利を埋め込まれたライセンスキーを管理用の場所（サーバー）に格納すること。そして「キーディストリビューション」とはライセンスキーを配布する作業となる。最後に「プレイヤー」によって入手したコンテンツとライセンスキーを組み合わせる。それぞれのステップで利用する技術は言うまでもなく「Rights Description」と「Rights Enforcement」のどちらか（または両方）に属しているのだが、それらの使われ方は次ページでフローの全体図を示しながら説明する。

■デジタルコンテンツを取り巻く状況の変化

1994年	1995年	1996年	1997年	1998年	1999年	2001年
米ソフト著作権保護団体BSA、不正コピーにより米ソフト業界が93年に被った損害は128億ドルと発表	米政府、ネットワーク上の知的所有権保護のために、著作権法改正を要求する報告書を発表	世界知的所有権機関（WIPO）、電子化情報などを保護対象とする条約改正で合意	経済協力開発機構（OECD）、暗号技術に関する政策指針を決定 ドイツ、インターネット利用の法的枠組みとなる「情報通信サービスの枠組みの規制に関する法律案」（マルチメディア法案）を可決 米商務省がネットスケープコミュニケーションズ、マイクロソフトに対し128ビット暗号化技術に対応したサーバー製品の出荷を許可	米国でデジタルミレニアム法成立 ウィンドウズ98発売。インターネットが爆発的に普及する。	MP3をインターネット上で公開していた少年が摘発される。日本ではじめての事例	1977年から米政府の標準として採用されていた暗号方式DESに変わり、より強力な新暗号方式AESが採用される

著作権表示を埋め込む「パッケージング」

「パッケージング」を行うためにはまずコンテンツをデジタル化する必要がある。アナログコンテンツをデジタル化することをデジタルエンコードするといい、デジタルエンコードする方法にはイメージであればスキャナーから取り込む、音楽やビデオであればキャプチャーなどの方法があり、それぞれ各種のソフトウェアが発売されている。このようにしてデジタルエンコードしたデータを、「Rights Description」技術を持ったパッケージマネージャーと呼ばれるソフトを使って元のデータが改ざんされないように暗号化したり、著作権表示などの各種データを埋め込んだりするまでが「パッケージング」の作業だ。

またこの段階で、人間の目には見えないが、ある処理を行うことで情報を取り出せるようにする“電子透かし”という方法を用いることもある。この電子透かしはデータの一部だけを取り出したり、画像などであれば色や解像度を変更したりしても消えないようになっているので、誰かが一部だけを取り出して利用しようとしても、元々どこのデータだったかということを追跡しやすくなるというわけだ。

ここまでの処理を行ったデータを“パッケージされたコンテンツ”と呼ぶのだが、このデータはファイルの形式を採る場合もあればDVDなどの物理メディアに記録される場合もある。

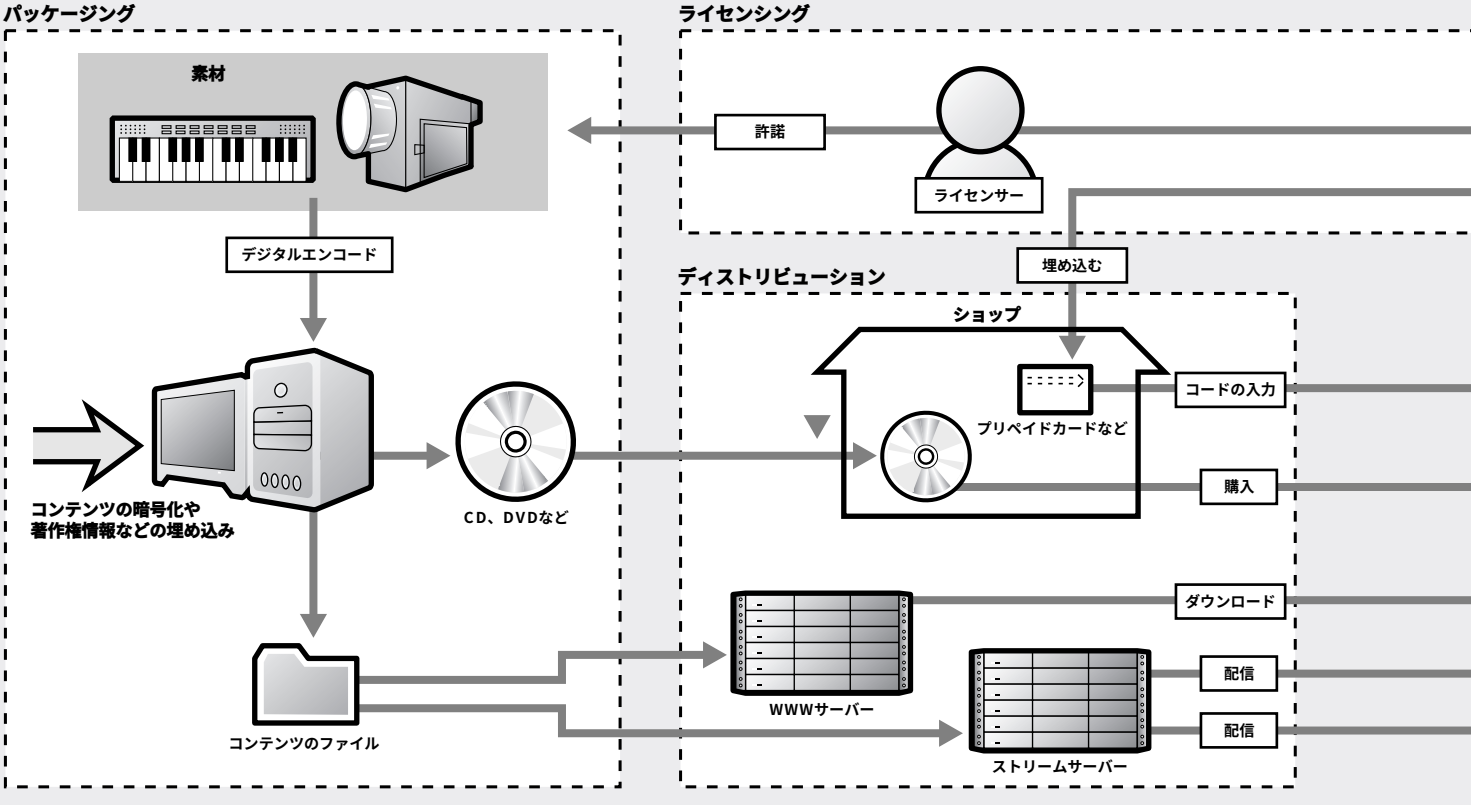
P2Pが注目される「ディストリビューション」

“パッケージされたコンテンツ”はユーザーに配布しなければならないのだが、そのままでは暗号化されているので、ユーザーはそれを再生できない。そのためプロバイダーにとっては、そのコンテンツをいくらコピーされても問題にならない。これらのコンテンツはインターネット経由であればウェブサイトからダウンロードさせる、ストリーミングサーバーからストリーミング配布するなどが考えられ、電子メールの添付ファイルという方法もあるのだが、最近注目されているのはP2Pを利用する方法だ。ただ、インターネット経由でなければ配布できないわけではなく、たとえばDVDに記録させたものを店頭などで配布して、「その内容を見たければ暗号化を解くライセンスキーを入手してください」というビジネス展開も可能になる。

クリアリングハウスを中心とした「ライセンシング」

「ライセンシング」では、コンテンツを利用するためのライセンスキーをユーザーからのリクエストに応じて配布できるようにする。この機能を持つ場所をライセンスク

■DRMが運用されるフィールド



PKIのフロー

リアリングハウスと呼び、ここではコンテンツごとの利用条件に応じたライセンスキーが生成される。

このライセンスキーにはコンテンツの暗号化を解くための鍵も含まれているので、ユーザーはライセンスキーの提供を受けて初めてコンテンツを利用できるようになるというわけだ。ライセンスキーのフォーマットはプレイヤーによって異なり、コンピューターで利用される場合は、パスワードだけというもっとも単純なパターンから、最近ではこのフォーマットにXMLファイルを使った認証モデルを使うパターンも増えてきている。

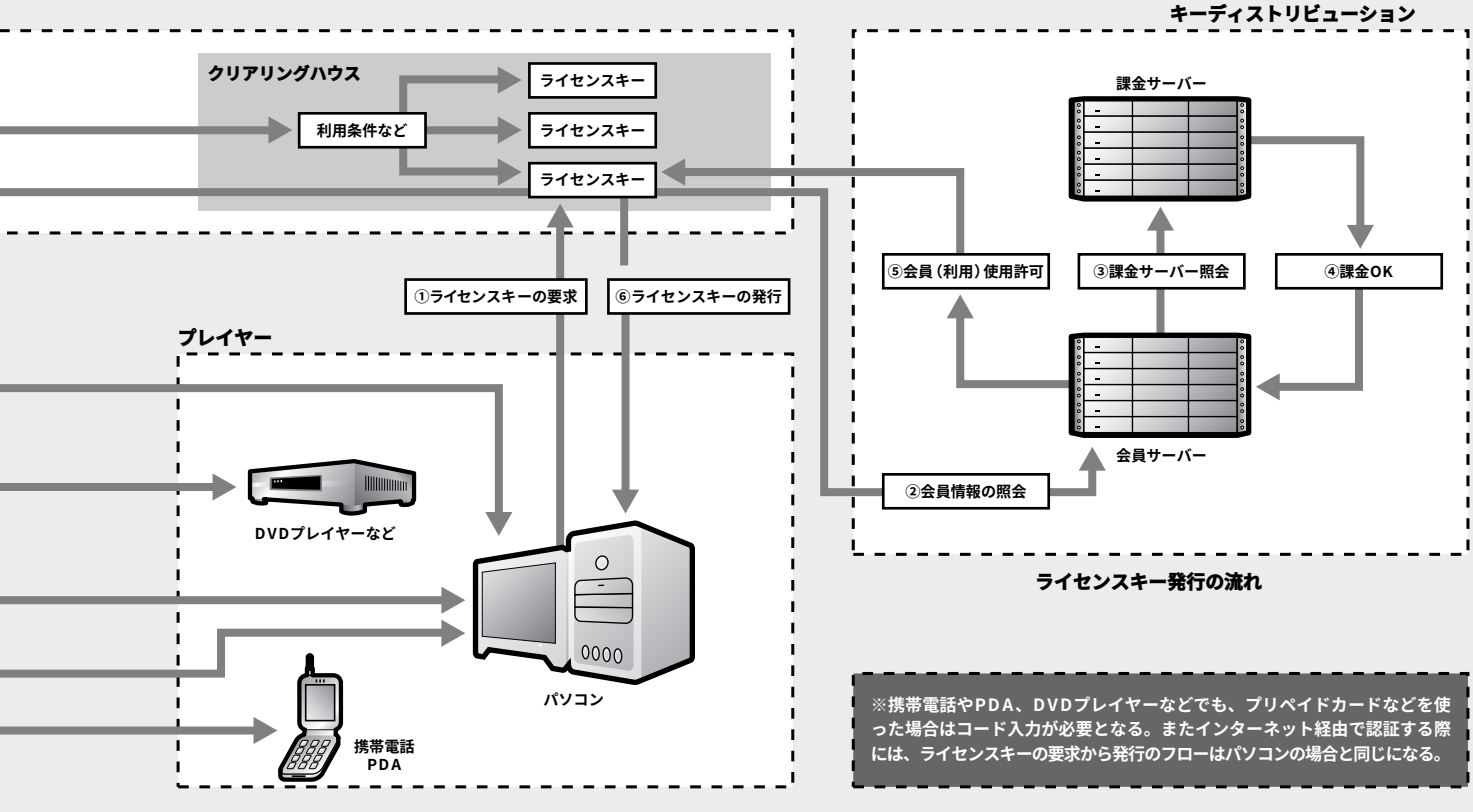
課金、会員サーバーも巻き込んだ「キーディストリビューション」

ユーザーがコンテンツを入手し、それを見るためのプレイヤーにセットするとライセンスキーが要求されるのだが、このライセンスキーを入手するステップが「キーディストリビューション」だ。この「キーディストリビューション」には“明示的”なものと“暗黙的”なものがあり、明示的なものとはユーザー名とパスワードをユーザーに問い掛けるもので、暗黙的なものはマイクロソフトのパスポートのようにOSレベルで自動的にユーザー名やパスワードを答えてしまうものだ。コンピューターを使わない場合、たとえばデジタル衛星放送の場合はセットトップボックスに装着されているICカードなどに記憶されているライセンスキーを使う場合もある。またあらかじめ購入したプリペイドカードの番号を入力することもキーディストリビューションの一形態だと言ってもいいだろう。この場合はクリアリングハウスからあらかじめライセンスキーがそのカードに“配布”されていると考えればいいわけだ。

一般的にはこの「キーディストリビューション」の段階で課金が行われる。実際にはクリアリングハウスがライセンスキーを配布していいかどうかを判断するわけではなく、課金サーバーや会員サーバーが別にあり、ユーザーから送信された個人（課金）データをクリアリングハウスとの間でやり取りし、問題がなければライセンスキーを発行するという仕組みになっている。

「プレイヤー」の機能は“再生”だけではない

ユーザーが入手したコンテンツとライセンスキーを元に再生を行う機器やソフトが「プレイヤー」なのだが、これは必要に応じて著作権表示や許された再生条件を表示する機能も持っていなければいけない。ライセンスキーが「コピー禁止」と指定していれば、そのプレイヤーはコンテンツの再生環境を提供するだけでなく、コピーもできないようにする機能を実装している必要がある。



ライセンスキー発行の流れ

※携帯電話やPDA、DVDプレイヤーなどでも、プリペイドカードなどを使った場合はコード入力が必要となる。またインターネット経由で認証する際には、ライセンスキーの要求から発行のフローはパソコンの場合と同じになる。

PKIとシングルサインオンがDRMをより強力にする

DRMを構築、利用するためにはさまざまな技術が必要であることは以上で述べたとおりだが、そのなかでも公開鍵を配布するための仕掛けである“PKI（Public Key Infrastructure）”とユーザー認証の煩雑さを解消する“シングルサインオン（Single Sign On）”は非常に重要な技術だ。

デジタルデータの改ざん防止や原本証明などを行うためには、この“データが本物である”と証明するデジタル署名が必要になる。デジタル署名は元のデータから計算されるある値（「ダイジェスト」と呼ばれることが多い）を、署名を行う人が持つ秘密鍵で暗号化して、公開鍵とともに元のデータに添付してユーザーに送る。ユーザー側では署名を行った人の公開鍵で暗号を復元し、それが元データから計算された値と一致するかどうかをチェックすることで“データが本物である”と確認する。ただし、その公開鍵が本当に署名を行った人のものかどうかがわからなければ意味がない。そこで、PKIを使うと、その人のデジタル署名と公開鍵に、信頼のある別の機関からの署名を加えることで、“その署名が本物だ”と証明できるのだ。

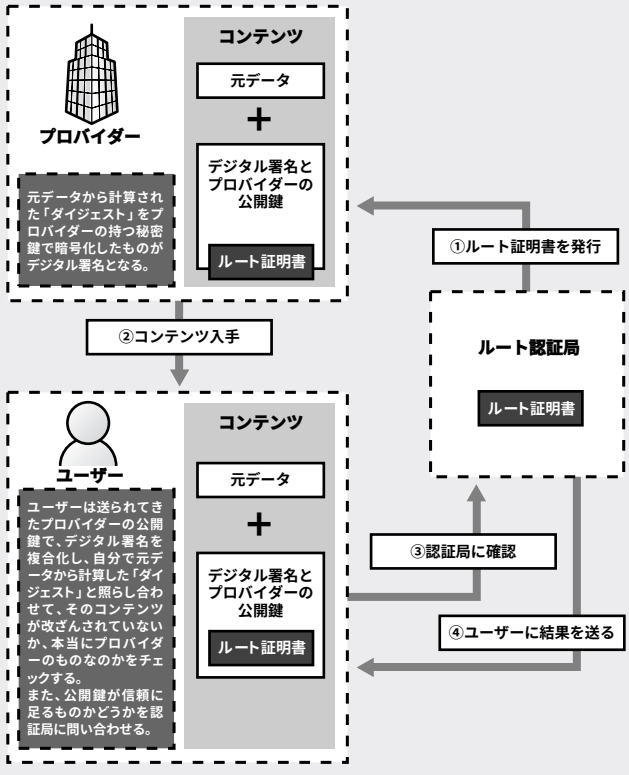
この方法はユーザーがライセンスキーを取得する際にも使われ、具体的にはプロバイダーが受け取った署名からルート証明書と呼ばれる大元締めの証明書を取り出し、ルート認証局にそれを送り、ルート認証局はそれを検証して正しいかどうかをチェックし、その結果を返すというものだ（下図参照）。

次に、シングルサインオンとはキーディストリビューションの際に重要になってくる技術だ。複数のサービスからコンテンツやライセンスキーを受け取る場合にそれぞれに対応したユーザー名とパスワード、証明書などを管理しなければならないのはユーザーにとって煩雑すぎる。これを解決するためには1つのサービスやOSに認証されればあとの証明は自動的に行ってくれるという技術を使う必要があり、それを実現するのがシングルサインオンなのだ。代表的なシングルサインオンにはマイクロソフトのパスポートやサンなどが推進しているリバティーアライアンスなどがある。

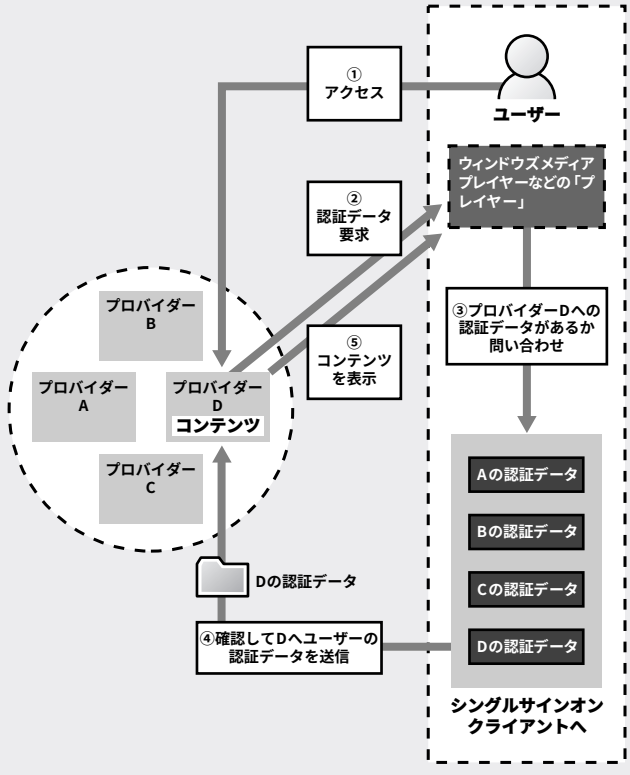
この技術を使うと1回目は認証などの入力が必要になるが、2回目以降はOSレベルで自動的に認証が行われるため、ユーザーにとってはインターネット上のコンテンツが非常に使いやすくなり、またパスワードを忘れるなどのトラブルを未然に防げるようにもなる。

具体的にシングルサインオンの処理の流れを説明すると以下のようになる。あるコンテンツを再生しようとするとプレイ

■署名を使うためのPKIのフロー



■シングルサインオンのフローの一例



ヤーが対応するライセンスキーを捜し、それがなければ自分の持っているキー（OSに組み込まれたユーザー名や証明書など）を使ってそのライセンスキーを取得するためのサーバーに接続し、それらの情報を送信する。そこで、正規のユーザーだと判断されれば、ライセンスキーが自動的にダウンロードされ、再生が始まるという仕組みだ。DRMの本質から考えるとシングルサインオンは必須の機能ではない。しかし実際のDRMを展開する場合にこの機能はなくてはならないものだと考えられる。

「マルチデバイス対応」DRMに残された大きな課題

以上、基本的な仕組みを説明してきたDRMだが、それをさらに使いやすいものにするためには、解決しなければならない問題点がいくつかある。そのなかでも大きいとされているマルチデバイス対応についての問題だ。

CDを購入したユーザーはパソコンでも携帯型プレイヤーでも家のDVDでもそれを再生できるのは当たり前のことだ。しかしインターネットで購入したデジタルコンテンツは、DRMが機能しているために、ほかのパソコンでは再生できない。デスクトップパソコン用とノートパソコン用に別のコンテンツを買う人はいないにもかかわらず現状のDRMでは1つのソースを複数のデバイスで楽しむことができないのだ。

今後インターネット対応ゲーム機やセットトップボックス、さらに動画が使える携帯電話などが普及してくると、これはより大きな問題になるだろう。たとえば携帯電話で映画の予告編を見て、その場で購入して家のパソコンやテレビで視聴できるようになれば便利だが、それを実現するためには現状の“マシンの認証”ではなく「誰が視聴しているのか」という“人間を認証する”方法を大幅に取り入れていく必要がある。この問題はDRMだけのものではなくシングルサインオンにも関係していて、マイクロソフトのパスポートでは生体認証（指紋など）に対応することで人間を認証する方法を採る可能性もあるが、対応しているDRMが同社のリリースしているDRMおよびOSだけであるという点が大きなネックだ。

各社ともこのマルチデバイス対応問題に関しての認識はあるものの、決定的な解決策はまだ提示できずにいる。この状態が長引けばコンテンツホルダーの意欲を萎えさせることにもつながり、ひいてはブロードバンドでのコンテンツビジネスマーケットの立ち上げを遅らせることにつながるかもしれない。結論としてはDRMが利益を生むようになるまでにはもうしばらく時間がかかると思われる。

コンテンツビジネスはDRMで“儲かる”とは限らない

本当にDRMは使われているのだろうか？前出のDMCAが米国で成立した当時、大きな論議が巻き起こった。それはDMCAが消費者の権利を制限するのではないかという議論だ。法案の成立に映画業界や音楽業界の強力なロビー活動があったことはよく知られているが、それはインターネットに代表される新しいメディアでの権益を守ろうとする姿勢とも解釈できる。

一方でこの法案が成立すれば、ユーザーはインターネットでさまざまなコンテンツを入手できるようになり、マーケットも大きくなるという論調も見られたが、すでに法案成立から4年もたっているのに、多くの企業がこのマーケットに参入したものの、ほとんどが利益を出せず撤退を余儀なくされるなど、マーケットが大きくなっているとは言い難い状況だ。

ところが、最近になって日本でも同様だったこの市場に変化が感じられるようになってきた。BBケーブルTVが年内にも開始する本格的なIPベース放送サービスやAllなどによるCDNサービスの充実を見ているとやっとブロードバンドコンテンツマーケットが立ち上がってきたような気さえする。しかし冷静にそこで使われている技術を見ると、DRMがほとんど使われていない（必要がない）ことに気が付くだろう。BBケーブルTVのようにセットトップボックスを使って、Yahoo! BB網の中だけで完結しているサービスなら、無理にDRMのすべてを実装する必要はない。またCATVなどのCDNでは「その加入者なら」見られるコンテンツという制約が付いている。つまりこれらのサービスは for Internetではなく for Intranetというわけだ。

DRMはオープンな環境でデジタルコンテンツの流通を目指しているにもかかわらず、趨勢は閉じたネットワーク内でのサービスが主流になってきている。閉じたネットワークであればDRMに要求されるスペックはぐっと低くなる。場合によっては独自エンコードと独自プレイヤーだけで十分なことさえ考えられる。収益を求めるときDRMを活用するのがいいのか、サービス対象を限定するなどの方法で対応した方がいいのかを冷静に判断する時代がすぐそこに来ているのではないだろうか。

［インターネットマガジン　バックナンバーアーカイブ］ ご利用上の注意

このPDFファイルは、株式会社インプレスR&D（株式会社インプレスから分割）が1994年～2006年まで発行した月刊誌『インターネットマガジン』の誌面をPDF化し、「インターネットマガジン　バックナンバーアーカイブ」として以下のウェブサイト「All-in-One INTERNET magazine 2.0」で公開しているものです。

http://i.impressRD.jp/bn

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容（技術解説、URL、団体・企業名、商品名、価格、プレゼント募集、アンケートなど）は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者（執筆者、写真の撮影者、イラストの作成者、編集部など）が保持しています。
- 著作者から許諾が得られなかった著作物は収録されていない場合があります。
- このファイルやその内容を改変したり、商用を目的として再利用することはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用する際は、出典として媒体名および月号、該当ページ番号、発行元（株式会社インプレスR&D）、コピーライトなどの情報をご明記ください。
- オリジナルの雑誌の発行時点では、株式会社インプレス R&D（当時は株式会社インプレス）と著作権者は内容が正確なものであるように最大限に努めましたが、すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接的および間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

このファイルに関するお問い合わせ先
株式会社インプレスR&D
All-in-One INTERNET magazine 編集部
im-info@impress.co.jp