1. DRMにおける脆弱性について

奈良先端科学技術大学院大学情報科学研究科
山口　英　sugurusec@is.naist.jp

（独）科学技術振興機構 社会技術研究開発センター
金野 和弘　konnok@ristex.jst.go.jp

はじめに

近年のアクセスラインの低廉化に伴い，オフィスだけでなく家庭でも広帯域インターネット接続が一般化した．広帯域インターネット接続は，多様化したネットワークサービスを産み出し，その利用は急速な広がりをみせている．ネットワークサービスの対象は，従来からのBtoB型だけではなく，BtoC型のサービスも急激に拡大している．この変化は，経済活動を取り巻く空間的・時間的制約を劇的に低減させ，経済社会に大きな便益を与え，また，新たなビジネスチャンスを産み出してきた．まさに，2000年に策定されたe-Japan戦略が希求した高度情報通信ネットワーク社会が登場したといえる．特に，インターネットを用いた電子商取引（e-Commerce）を拡大させてきた点が特徴的であるとまとめてもよいだろう．

さらに，ここ1，2年で拡大してきた新たなネットワークサービスがある．いわゆる直接コンテンツ提供を行うサービスで，映像や音楽などを記録した素材を提供するものや，音楽や映像のライブ中継（live feed）を供給するものが代表的である．これらの取引をd-Commerceと呼ぶ研究者もいる[1)]．これらのサービスは，e-Commerceと同様に，BtoB型とBtoC型での取り組みの両面で展開している．たとえば，BtoB型のサービスでは，プロダクション間での映像素材の交換や，放送事業者間での番組の相互提供，さらには，映画館に対するディジタル映画の供給などが試みられている．またBtoC型では，インターネットでの音楽ダウンロード販売が典型的な事例といえよう．またストリーミング技術を利用して，各種映像をオンラインで提供するサービスも広がりつつある．たとえば，国内大手ISPが広帯域アクセスサービス購入者に対して提供している，アニメ映画やスポーツ映像サービスは，その典型例といえよう．

このようなd-Commerceの取り組みは，1つの大きな弱点がある．それは，d-Commerceによってやりとりされるものがディジタルデータという点だ．取引されるデータに対して何の保護策も施さなければ，元々のデータは複製され，不当に流通してしまう可能性がある．これにより本来データ利用者から回収することができた対価を得ることができず，結果としてデータの権利保有者の機会損失を生じさせてしまう．その典型例が，ファイル交換型P2Pを利用した音楽や映像データの交換・利用による著作権侵害事案である．また，データの無断改変による，コンテンツ制作者の権利侵害も問題だ．このため，早急に何らかのコンテンツ保護機構の実装が必要というのは，コンテンツ提供者にとっては共通認識となっている．

この保護策として生まれてきたのが，いわゆるDRM（Digital Rights Management）であり，各コンテンツについて，参照，複製，廃棄，改変などを管理するための基盤技術である．コンテンツ提供にDRMを適用することで，適切な権限を持ったユーザのみがコンテンツにアクセスすることを保証できるようになる．さらに，DRMをより汎用的に捉え，ネットワーク環境に分散して配置された情報資源に対する汎用のアクセス管理技術とみなすこともできる．DRMは，これまでにコンテンツおよび情報機器の供給者や研究者を中心として精力的な研究開発が進められ，実証・実用の段階まで取り組みが進められてきた．

さらに，DRMがこれまで対象としてきたコンテンツは，主に画像，映像，音楽など主に商業コンテンツであるが，今後は文書などのネットワーク上を流通するあらゆるディジタル・コンテンツがDRMによる管理対象となると予想されている．

しかし，残念ながら，既存のDRMが実際のネットワークサービスに広く適用される状況にはなっていない．これまでのDRM実現の取り組みは，コンテンツ保護の技術的課題解決が中心的であった．しかしコンテンツ提供

を取り巻く法律的あるいは経済的な側面についての議論が十分に行われておらず，その議論に基づいた適切な機能を実現したDRMが提供されているわけではない．このため，コンテンツの権利保有者にとって，DRM利用に積極的になれない状況を産み出していると考えられる．このような状況を放置することは，将来のコンテンツ流通が促進されないだけでなく，権利保有者にとって現時点での機会損失，権利侵害の問題を解決できない．

ここに示した問題は，DRMの新たな脆弱性，あるいは，DRMをめぐる社会的リスクと考えることができる．今後のIT利活用の広がりを考慮した場合，この問題を解決することは重要である．

本稿では，これまでのDRMを構成する基本技術を概観し，DRMを巡る社会的リスクとは何かを明らかにする．さらに，この問題解決への取り組みのあり方について私見を述べる．

DRMとは

DRMはDigital Rights Managementの略であり，「ディジタル著作権管理」もしくは「ディジタル権利管理」などと訳される．

その定義は，論者によってさまざまである．たとえば「ディジタルデータの著作権を保護する技術で...音声，映像ファイルにかけられる複製の制限技術が有名だが，画像ファイルの電子透かしも含まれる」[2]，「著作者ないし配信者が配信条件，利用条件，利用端末を指定して，的確な著作権利用を実現するもの」[3]などである．

対象となるコンテンツの範囲もまたさまざまである．現時点で実装されている多くのDRMが想定しているコンテンツとは，楽曲，静止画像（たとえば写真，イラスト），動画像（映画，TV番組），テキスト（雑誌記事，小説）などを指す．これらは主に商業目的で商品として流通・販売される．

さらに，一般的にDRMが対象とするコンテンツは，ネットワーク上で流通・交換されるあらゆるディジタルデータのうち，信憑性の確保や権利保護が必要なものという特徴を持つ．このため，上記の商用コンテンツ群だけでなく，電子商取引でやりとりされる契約書などの重要文書，インターネット上で公開されている政府刊行物や公文書，企業のIR情報などもDRMの対象に含まれると考えることができる．

◆DRMの目的

DRMの主目的として次の3つがある．

第1に，コンテンツ制作者やコンテンツ提供者が保持する著作権および著作隣接権を保護するためである．権利保持者の意図を無視した改変や引用は同一性保持権等を侵害する可能性があり，これを防止するためにDRMが有効である．たとえば，コンテンツを流通させる際に，配信条件，利用条件，利用端末を詳細に設定し，コンテンツ利用者の利用を制限・監視することにより諸権利を保護する．

第2に，権利保持者の投資インセンティブを阻害するのを防ぐためである．権利保持者はコンテンツを制作・流通する際に相応の「投資」を行っており，その投資回収を阻害されることで投資インセンティブが低下する可能性がある．そのため，DRMによって違法複製や違法販売を防止する必要がある．

第3に，意思決定に重大な影響を及ぼすコンテンツの信憑性を保証するためである．もし改竄されるなど信憑性が保証されないコンテンツに基づいて意思決定がなされれば，重大な損失を生み出す可能性がある．さらに意思決定者が事前にその可能性を認識すればコンテンツの利用を忌避し，その結果，経済活動を萎縮させるかもしれない☆1．これは電子商取引市場の発展にとって阻害要因となり得る．市場取引において，情報の信憑性はいわゆる社会資本（social capital）であり，この社会資本が失われれば市場は成立しない．それゆえDRMが果たす役割はきわめて重大である．DRMはこれらのコンテンツの信憑性を保証することを通じて，個々の意思決定者ばかりでなく社会的にも不可欠な社会基盤を提供する．

上記の3点以外にもDRMの役割はいくつかある．たとえば顧客情報の効率的収集や情報漏洩対策である．前者は利用状況や転々流通過程に関する情報を収集し，その情報をフィードバックすることによってマーケティング戦略に役立つ．後者は，企業組織内の重要情報に対してDRMを利用することによって，監視体制の強化や抑止効果が期待できる．

◆主なDRM技術

これまで実装されているDRMで利用されている基本技術は以下のものがある．

暗号化／認証技術

コンテンツ利用者の認証機能と，利用者ごとに暗号化されたコンテンツを提供するための暗号鍵管理機能は，多くのDRMの基本機能として用意されている．

コンテンツ供給側では，顧客管理システムの一部としてDRMが実装されるのが一般的である．

一方，利用者側に実装されるDRMの場合，通常の暗

☆1　これを，経済学では萎縮効果（chilling effect）と呼ぶ．

号化機能とは異なり，以下の 2 点の技術が必要となる．

(1) 利用者による復号鍵漏洩の問題に対処するために，各利用者に対して供給されるコンテンツ復号に用いられる鍵を利用者から秘匿した状態で管理し，コンテンツの復号を実施する機構．

(2) 権限を与えられてない利用者によるコンテンツの複写・漏洩を阻止するために，復号結果を安全に管理し，不正な複写を阻止する機構．

この技術的要件により，現在利用可能な DRM は，独立したコンポーネントとして構成されるのではなく，コンテンツ利用アプリケーションと一体化した形で実装されている．たとえば，Adobe 社の Acrobat，Microsoft 社の WMT 等は，それぞれ文書，映像素材に対する DRM 機能を持っているが，コンテンツ利用アプリケーションと一体化されて実装されている．

電子透かし技術

一般に電子透かし技術とは，著作権情報などのメタ情報をコンテンツの中に安全に埋め込む技術である．ファイルの形態で流通されるコンテンツにおいて，著作権情報や複製回数制限などを管理するために，この技術は広く使われている．コンテンツ供給側によって安全に埋め込まれたメタ情報は，専用のアプリケーションによってアクセスすることができ，利用者側では著作権情報の表示や，メタ情報に基づいて不正複製や改善防止処理を実施する．この機能は，現在急速に広がりつつある音楽コンテンツのダウンロード販売において一般的に用いられている．

耐タンパー技術

耐タンパー技術を用いて，コンテンツから容易にコンテンツデータ自体や利用者の個人情報などを読み取りや書き換えができないようにする．やはり既存の DRM では，専用の閲覧ソフトウェアを使うことによりユーザの操作を制限し，画面に表示するために一時的に復号化されたデータを電子的に読み出されることを防止する．

脆弱性の原点：DRM の経済性とリスク

複数の技術を組み合わせ，コンテンツ保護を実現する DRM は，これまで多くの提案と実装が行われてきた．しかしながら，その社会展開は限定的であり，コンテンツ供給側が DRM 利用に積極的になれない現状が厳然と存在している．この問題は，DRM をめぐる新たな社会的リスクの存在を浮き彫りにしている．それは，DRM の経済性とリスクについて，合理的な適応方法が見出されていないことに起因する．

◆情報財問題

先に述べたように，DRM が対象とするコンテンツは，一般にディジタル化可能な情報すべてであり，特に信憑性の確保や権利保護が必要なものである．

Varian[4] によれば，「あらゆるデータのうち，ディジタル化可能なもの」を「情報財」と呼び，情報財は以下の 3 つの特性を備えていると主張した．

(1) 制作のための初期コストは大きいが，再生産（複製）コストはほぼゼロである．

(2) 流通コストがほぼゼロである．

(3) 非競合性（non-rivalry）と非排除性（non-excludability）を具備している．

これらの特性は，以下に挙げる 2 つの「情報財問題」を生み出す．

コンテンツ利用許諾料金の回収が困難である

複製コストがほぼゼロであるため，生産者以外の者がコスト負担をすることなく容易に複製可能である．加えて，料金を支払わない者を利用から排除するための監視および強制コストがきわめて大きいため，DRM 技術が導入されていない下では，効果的な排除は経済的に不可能である．そのため，事前的投資を回収することが困難であり，それを予測する生産者の投資インセンティブは低下する．結果的として，社会全体に供給されるコンテンツ量が減少し，かつその質も低下すると推測される．

権利侵害が容易で，かつその違法コンテンツが瞬時にかつ広範囲に流布される

ディジタル・コンテンツは，質を損ねることなく複製や改変が容易であるため，権利者や権利保持者に無断で，かつコストをほとんどかけることなく権利侵害が可能である．加えて，金銭的コスト，時間ともにほぼゼロで，ネットワークを介した流通・取引が実現可能であるため，きわめて短時間でかつ広範に伝搬させることが可能である．

この情報財問題に対して，DRM は技術的には解決方法を与えるのは明らかである．

◆ DRM をめぐるトレードオフ

一方，DRM の導入コストと，権利保護強度の間にはトレードオフ関係が存在することに注目しなければならない．

導入コストの 1 つの要素は，ユーザ側でのコストである．権利保護強度の高い DRM は複数の技術を組み合わせて実現され，多くの場合専用のソフトウェアとして実装される．利用者側に専用ソフトウェアを導入する段階で，大きなコスト負担が必要となるとすると，ユーザが

そのソフトウェアの利用を忌避し，需要減退を引き起こす場合がある．実際，この問題を回避するために，現在利用可能なDRMを実装したシステムでは，ユーザ側で利用される閲覧ソフトは無料で配布し，供給側で用いられるシステム構築にコスト負担を要求するものが大部分である．

導入コストのもう1つの要素は，供給側でのシステム構築コストである．強固なDRMシステムを構築するためには，高度な技術を利用する必要があるが，同時に高性能なシステムが必要になり，そのシステムの運用に十分なコストをかけることが不可欠である．一般に，強固な保護システムを構築しようとすればするほど，供給側システム構築コストは上昇する．

この導入コストと権利保護強度の間にトレードオフ関係が存在する状況で，適切な水準のシステムをどのように構築するかを合理的に判断する手法が確立していない．このため，供給者側では，あえてDRMシステムを構築してネットワークを介したコンテンツ供給をするよりも，旧来型の媒体を利用したコンテンツ供給を選択する傾向が強まる．これは，利用者側での投資インセンティブを低下させる効果を持ち，一層DRMの導入を忌避することになる．また旧来型媒体によるコンテンツ流通で発生している権利侵害問題は解決することがなく，悪化の一途をたどる状況を引き起こす．

この状況は，我が国における音楽コンテンツの流通現場において観測される状況に等しい．すなわち，権利保護機能をまったく持たない旧来型媒体である音楽CDで供給される音楽コンテンツは，不正複製され，ネットワーク環境で広範に普及される．一方，音楽供給側では，DRMに対応したかたちのダウンロード型音楽販売を，その導入コストの高さから始めていない状況にある．また，一部の音楽供給会社では，独自システムを構築して音楽のダウンロード販売を始めたが，その再生に特別のソフトウェアあるいはハードウェアが必要であり，利用者側での導入コストから普及が進まない状況にある．このために，音楽CDによる供給で発生している問題は，まったく解決されることなく放置されている状況にある．

◆ DRMを巡る社会的リスク

コンテンツ流通において情報財問題を発生させないためには，DRMの構築が効果的であることは先に述べた．また，多種多様なコンテンツについて，多くのビジネス領域で流通を促進させることを考えると，DRMは1つの社会基盤として成立する必要がある．一方，DRMを社会基盤として成立させるためには，コンテンツを扱うすべての経済主体に対して課されるリスクを明らかにし，各リスクについて適切に対応する（対策を実施する）必要がある．

情報財問題の議論から，各主体は次のような具体的なリスクを被る可能性がある．

コンテンツ制作者は権利侵害リスクや許諾料回収リスクを，コンテンツ供給者は著作隣接権等の権利侵害リスクや投資回収リスクを，そしてコンテンツ利用者は入手したコンテンツの信憑性が保証されないならば利用リスクや訴訟リスクをそれぞれ抱え得る．各々がリスクを抱えた結果，コンテンツの制作，供給，利用を控え，コンテンツ市場およびコンテンツを利用する経済社会の発展に対する阻害要因となる．つまり，ここには社会的リスクが存在することになる．この社会的リスクとしては，以下の3つが考えられる．

コンテンツ流通リスク

第三者によるコンテンツの改変・改竄の可能性があるならば，ネットを介したコンテンツの流通量が縮小する可能性がある．自分が作成したコンテンツもしくは自分宛のコンテンツデータが無断改変されることで損害を被る可能性があるならば，コンテンツのやりとりを躊躇するであろう．ネットワーク上で経済活動に従事する者の多くがこのような心理になれば，全体の流通量が萎縮する可能性が高い．このとき，ネットワークを介したコンテンツ流通自体が重大な社会的リスクとなる．これを「コンテンツ流通リスク」と呼ぶ．

コンテンツ利用リスク

実際にコンテンツを利用する時点でも真偽性が問題となる可能性がある．ネットワークを介して取得したコンテンツを重要な意思決定の根拠として活用する際には真偽性の確保が不可欠である．DRM技術が導入されていない，もしくは十分でないためにコンテンツの利用が減退したり，虚偽のコンテンツの利用によって損害を被ることが予測されたりするならば，これもまた社会的リスクとなり得る．これを「コンテンツ利用リスク」と呼ぶことができる．真偽性と第三者による改変を防止するDRM技術は，このような社会的リスクを低減させるためにきわめて重要な役割を果たすと考える．

権利侵害リスク

コンテンツを利用する際，ユーザ自身が無意識に権利を侵害する恐れがある．たとえば，コンテンツにメタ情報が付加されていないために著作権情報を獲得できないことが原因となり得る．意図せぬ権利侵害によって提訴されるかもしれず，訴訟リスクもしくは「権利侵害リスク」と呼ぶことができる．権利侵害リスクによって，社会全体の制作活動が阻害され，コンテンツの総量を減少

させる可能性がある．

以上のリスクが生じる結果，コンテンツの絶対量の減少とともにインターネットを介したコンテンツ利用の減退を招き，社会的便益が減少する可能性がある．インターネットが重要インフラとして位置づけられる以上，このようなリスクが存在する状況下でのコンテンツ利用は社会的リスクとみなすことができる．それゆえ DRM はコンテンツにかかわる社会的リスクを低減させるツールとして重要な役割を果たすといえる．

◆問題解決に向けて

ここまで述べてきたように，高度情報通信ネットワーク社会におけるコンテンツ流通を促進させ，同時にコンテンツ利用における社会的リスクを低減させるための重要なツールとして，DRM のポテンシャルを示してきた．しかしながら，DRM だけでは，これらの問題を解決できるわけではない．本質的に問題を解決するためには，DRM を含めた技術，ディジタル・コンテンツに関連する法制度，コンテンツ利用における契約，利用者の教育・啓発活動の 4 つの要素について，バランスある発展が実現されなければならない．これら 4 要素がバランスよく整備されることで，安全かつ安心なコンテンツ流通基盤が成立する．

まず，法制度については，物的資産やアナログ・コンテンツを前提とした著作権や著作隣接権を，ディジタル・コンテンツにも馴染むよう追加・改正が必要である．現在の著作権制度は，新たに表面化したディジタル・コンテンツ特有の問題に対処するべく修正・追加を繰り返しているが，必ずしも対処しきれているとはいえない．将来的にはディジタル・コンテンツを前提とした新たな法制度を抜本的に再構築する必要があるかもしれない．

契約は，基本的に法制度が対処しきれていない部分について当事者間でのコンテンツ取り扱いの具体を補完する意味で重要である．コンテンツによっては，そのコンテンツにかかわる利害関係が複雑になるものが多数存在する．これらのコンテンツをネットワーク流通可能にするためには，契約のテンプレート化などの取り組みも必要になろう．また，契約は別の重要な役割を果たす．我が国の（狭義の）コンテンツ産業では，厳格な契約を締結せず慣例追従や口約束による緩やかな契約関係を築く傾向が強い．このため，業界内の地位や交渉力が契約内容に如実に反映された取引関係が維持されてきた傾向がある．このような関係は，コンテンツ産業の発展を阻害する要因となると指摘されている．曖昧さを可能な限り排除した契約を初期時点で締結することは，各当事者の権利や利益を保護する意味でも，また再交渉や契約締結にかかる無駄な取引コストを削減する意味でも有効であると考える．

教育・啓発活動は，コンテンツ利用者のモラルを向上させ，公正・公平な「コンテンツ利用文化」を醸成させ，コンテンツの不正利用，不正流通の発生を抑止することにある．教育・啓発活動は短期的にはコスト上昇を招くが，長期的には確実にコンテンツ利用におけるリスク管理コストの圧縮を達成する．

おわりに

本稿では，インターネットを介した広義のコンテンツ流通における具体的なリスクと，社会的リスクを概観し，そのリスク低減に DRM が果たす役割を述べた．現在実装されている DRM は，高度な技術を利用しており，これらのリスクを低減させる能力を持つ．しかしながら，現在の DRM はコンテンツ流通で積極的に利用されているわけではない．これは，DRM を構築するための導入コストとそれによって得られる便益，すなわち権利保護強度の間に存在するトレードオフの関係を解明し，適切な水準の DRM を構築するための指針を得ることができていないことに起因すると考えられる．

また，コンテンツ流通を取り巻く社会的リスクを低減し，コンテンツ流通を促進するためには，DRM の高度化を追求するのみでは不十分である．DRM を含む技術領域における高度化はもちろんのことながら，ディジタル・コンテンツ流通に適応した法制度の整備，明確な契約締結の一般化，コンテンツ利用者の教育・啓発活動が必要である．これら 4 要素（技術，法制度，契約，教育・啓発活動）のバランスある進展が，コンテンツ流通の促進には不可欠である．

謝辞　本研究は，社会技術研究開発センター ミッション・プログラム II「高度情報社会の脆弱性の解明と解決」の研究として行われたものである．

参考文献

1）東倉洋一他：情報セキュリティと法制度，丸善ライブラリ 368（2005）．
2）IT 用語辞典 E-words，http://www.e-words.com/
3）牧野二郎：ディジタル著作権概論，UFJ 総合研究所芸術・文化政策センター「Arts Policy & Management」，No.20, pp.1-5（2003）．
4）Varian, H. R.：Markets for Information Goods, The Author's Home page, University of California Berkeley（1998）．

（平成 17 年 5 月 8 日受付）