

著作権保護と著作物再利用システムの検討

武井英明 森保健治

NTTソフトウェア研究所

{htake, moriyasu}@slab.ntt.co.jp

2 Y - 8

1.はじめに

デジタル著作物の著作権保護には trusted systems [1]と呼ばれる耐タンパ装置を用いたシステムが提案されているが一般的な普及には至っておらず、電子情報流通活性化という目的における著作権保護問題解決の緊急性から、より汎用的な普及性の高い著作権保護システムが望まれている。また特にデジタルデータは、カット&ペーストに象徴されるように、他のデータの引用・流用により作られることが多く、上記著作権保護システムには著作物を簡単に再利用できる機能も求められている。本稿ではこれを実現するシステム RINS を提案する。

2.著作権保護システム：RINS

著作権保護にはある種の制約が含まれるが、それは他人の「利用」における制約であり、利用しやすさと制約との両立をはかることがシステム構築における課題となる。この課題に対し、ある単純なしくみで解決を試みる。

2-1.しくみ

「データ」を「実体」と「使用権」に分離し、データはユーザから隠す。

これがそのしくみである。典型的には、実体は「暗号データ」であり、使用権は「復号鍵」である。このしくみには以下の3つの主な利点がある。

- ・著作権保護  
データの代わりに（暗号化されている）実体を定期的に記録することで記録時の安全性を確保する。データの利用には使用権が必要であり、システムはユーザに使用権の購入等の手続きを強制できる。
- ・流通性が向上  
実体をコピーされても著作権上の脅威にはならず、むしろ電子情報の利点を生かした活発な流通を期待できる。
- ・使用権をユーザが携帯可能  
使用権は一般にサイズが小さく、ユーザの携帯装置に格納も可能である。ユーザが一度手続きすればマシンを問わず使用可能になるシステムも構築可能になる。

2-2.実現のためのファイルシステム

上記しくみの実現にあたり、復号化等はファイルシステム(FS)で暗黙に行い、ユーザはデータを今までと同じように扱えるのが望ましい。そこで、FS に新たに「暗号属性」を各ファイルに設定可能にする。暗号属性は例えば以下の項目を持つ。

- ・暗号の種類（暗号してない/アルゴリズムの種類）
  - ・復号鍵の場所
- 暗号属性が設定されているファイルは上でいう実体に対応する。このファイルのリードには2種類ある。
- ・通常のリード  
そのまま（暗号化されたまま）OS に渡す。
  - ・復号リード  
暗号属性からアルゴリズムと復号鍵の場所を特定し、

それらの情報を使ってファイルを復号化してから OS に渡す。

2-3.使用権（復号鍵）の管理

ユーザの勝手なコピーを防止するなど厳重な管理が要求されるため、耐タンパなハードに記録する。IC カードにすれば使用権の携帯性を損なうことはない。なお安全な鍵配送に関しては Infoket[2]等が実現されている。

2-4.利用時のデータ保護

記録・流通においてデータは暗号化されるので安全だがデータの利用時にはアプリケーション(APP)にデータが生で渡る。そこで APP からのデータ流出防止が課題となる。

・ trusted systems (TS)

典型的な TS では、耐タンパなハード上で置き換え困難な OS を走らせ信頼できる APP のみを動作可能とすることでこの課題の克服を図っている。しかし 1)新しいシステム導入が必要で、2)APP が限定される、等の問題で一般的な普及には至っていない。

そこで、以下のシステムを考える。

・ OS による APP 管理

基本的に既存のコンピュータシステムを流用する。違いは OS が、保護すべきデータを渡した APP の動作を制限する点である。具体的な制限は以下ようになる。

OS は保護すべきデータを渡したプロセスに対し、以後すべてのデバイス・プロセスへの出力を禁止する。但し画像、音声出力はこの限りでない。

この OS の制限により APP からの情報流出は最小限になったと考え、任意の APP を動作可能とする（図1）。

2-5.考察

OS の改造や情報流出を意図した APP によって著作権が侵害される可能性がある。これらの欠点にもかかわらず TS の普及前に本システムの導入を主張する主な理由は以下である。

- ・上記のような著作物流通のしくみの利点を広く享受してもらおう。
- ・テキストを手でうつすなど、ディスプレイやスピーカからの情報流出は本システムの対象外とする。
- ・OS の改造は一般に困難である。

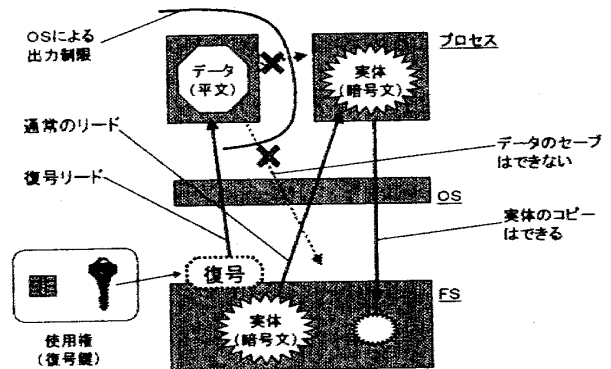


図1: 利用時のデータ保護

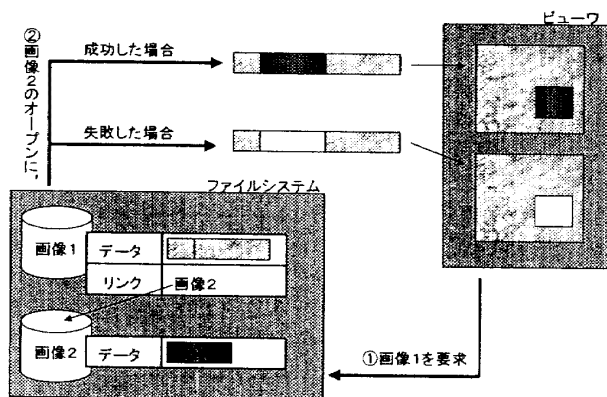


図2:リンクファイルのオープン

### 3 RINS における再利用機能

上記のような著作物の流通性が高い著作権保護システム RINS が普及すれば、それらの著作物を引用・流用した新たな著作物の作成要求が高まることは必定である。本章では RINS における著作物再利用機能について考える。

#### 3-1.例

以下は再利用の端的な例である。画像1は画像2を内部に張り込んでいる。画像2の使用権を持つ A 氏が画像1を見る場合、期待通り画像2が張り込まれた画像1を見ることができる。画像2の使用権を持たない B 氏が見る画像1には画像2が張り込まれていない。

#### 3-2. FS による実現

この種の機構は、例えば WWW におけるリンクのように、個々の APP ベースで対処可能だが、ここでは FS レベルでの実現を考える。その主な理由は以下である。

- ・著作権は画像、テキスト、その他さまざまなファイル形式で発生する。
- ・APP はリンクの存在を意識する必要がないので、既存の APP を流用可能であり、APP の作成は容易である。

#### 3-3.再利用システムの実現

ファイル形式に依存させないためにはリンク情報をファイルデータ内に埋め込む必要がある。ファイルに付随する「リンク属性」を設ける必要がある。もちろん、リンク属性はリンクの数に応じて複数個になる。リンク属性は例えば以下の項目を持つ。

- ・リンク先ファイル名
- ・リンク元におけるリンク先の挿入位置
- ・リンク先ファイルの展開後のサイズ
- ・リンク先ファイルの中で展開する場所（一部分しか使わないかもしれないので）
- ・展開できないときの対処法（0 でパディング/購入を促す文句を表示）

このリンク属性によってバイナリベースのリンクが可能になる。

#### 3-4.再び例

先ほどの例を使う(図2)。まずビューワは画像1を開くことを FS に要求する。FS はまず画像1のリンクをチェックし設定されている場合はリンク先の画像2を開こうとする。画像2を開く鍵がない等でこれに失敗した場合、FS は指定された対処をとる。成功した場合、FS は画像2を画像1の指定位置に挿入し、ビューワは正しい画像1を得る。結局ビューワは画像1がリンクで構成されて

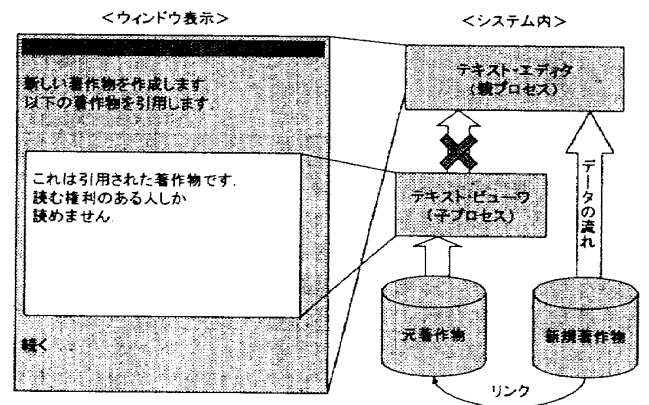


図3:再利用著作物作成時のAPP構成

いることを知らない。

#### 3-5.再利用著作物作成時のAPP構成例

当然だが、再利用著作物の作成時にも利用した著作物の著作権が保護される必要がある。作成のための APP は図3のような構成になる。既存エディタは流用できない。このとき、ユーザは全部の文書を（あたかもリンクがないかのように）眺めることができるが、リンク先の文書の編集はできない。リンク先のデータは子プロセス内で閉じているからである。

#### 3-6.考察

3-5 の制約は、APP がデータ全体を知る必要があるファイル形式を扱うときに問題となる。つまり元の著作物データと新規作成データが互いに干渉するデータ形式のとき問題となる。例えばテキストは OK だが、JPEG や GIF は問題となる。これにはリンク情報を FS から APP に与えるサービスとビューワの専用化によって対処可能と考えられる。

### 4.付随的な話題

#### ・改竄検知

メッセージ認証子によって実体の認証機能を付加することもできる。

#### ・勝手なリンクの防止

WWW での経験から、リンクによるファイルオープン制限するといったオプションも必要かもしれない。

### 5.おわりに

本稿では現行システムからの移行が容易な著作権保護・著作物再利用システム RINS を提案した。本システムは著作物の不正利用を防止しつつ再利用をするための機能を提供する。

RINS の普及によって、著作物ファイルに関して従来一般的であった発行元からの一元配布のみならず配布先からの再配布という新たな流通経路の創出が期待される。著作物へのリンク機構によって、著作物の直接利用だけでなく再利用という新たな利用形態の創出が期待される。著作物の使用権は利用者毎への付与が可能であり、著作物の提供者は利用者毎の厳密な管理を、利用者はマシンを問わない利用可能性を、それぞれ期待できる。

### 参考文献

- [1] Mark Stefik: Trusted Systems (邦訳) 電子取引のセキュリティ, 日経サイエンス, 27, No.7, pp52-56, 1997
- [2] 明石・森保・寺内: インターネットを用いた情報流通プラットフォーム: Infoket-I, NTT R&D, 46, No.2, pp107-114, 1997.