グループウェアと
ネットワークサービス 40−8
（２００１．５．２５）

Java Cardを用いた ソフトウェアライセンスの管理方法の提案

菅原 陽子 *　　小宅 宏明 *　　岡田 謙一 *

慶應義塾大学大学院 理工学研究科 開放環境科学専攻

近年，ソフトウェアの違法コピーは増加傾向にあり，CD-R などの大容量リムーバブルメディアの低価格化や，インターネットの普及に伴って, 今後も増加してゆくと予想されている. また，ソフトウェアはディジタルデータであり，品質を劣化させることなく無数にコピーを作成することが可能である．ソフトウェア制作者は著作権保護のために様々な方法をとっているものの，効果が上がらないものが殆んどである． また，コンピュータが急速に普及してきたことにより，どこへ行ってもコンピュータが利用できるようになった．それに伴って, 出先でコンピュータを操作する機会も多くなってきている．そのような場合に, いつでも自分用にカスタマイズされた環境でソフトウェアが利用できれば, 作業効率の向上につながると考えられる. 本研究では,IC カード上に Java の実行環境を実装した Java Card を用いてソフトウェアのライセンス管理を行うことにより，確実にユーザーのライセンスを認証できるようにすること及びソフトウェアがインストールされている端末に関わらず, 常に自分用にカスタマイズされた環境でソフトウェアを利用できるようにすることを目的としたライセンス管理方法を提案し, 実装した.

The proposal of the management method of a software license using JavaCard

Yoko Sugawara * , Hiroaki Ohya * , Kenichi Okada * ,

It is expected that the illegal copy of software is increasing and increases also from now on in recent years in connection with the reduction in the price of mass remover bull media, such as CD-R, and the spread of the Internet. Moreover, software is digital data, and it is possible to create a copy innumerably, without degrading quality. It is almost which the effect of that to which the software producer has taken various methods because of copyright protection does not go up.Moreover, when the computer had spread quickly, the computer could be used wherever it might go.In connection with it, an opportunity to operate a computer on the way also increases.In such a case, if software can be used in the environment always customized for itself, it will be thought that it leads to the improvement in working efficiency.By this research, by performing license management of software using Java Card which mounted execution environment of Java on the integrated circuit card, it was not concerned with the terminal with which the thing for which it enables it to attest a user's license certainly, and software are installed, but the license management method aiming at enabling it to use software was proposed and mounted in the environment always customized for itself.

1　はじめに

ここ数年，ソフトウェアの違法コピーは世界的に増加傾向にあり，CD-R などの大容量リムーバブルメディアの低価格化や，インターネットの普及に伴って, 今後

* 慶應義塾大学大学院 理工学研究科 開放環境科学専攻
Science-and-engineering graduate course
opening environmental science speciality, Keio University

も増加してゆくと予想されている.

ソフトウェアはディジタルデータであり，品質を劣化させることなく無数にコピーを作成することが可能である．このため，ソフトウェアの流通は通常の「物」の流通とはかなり性質が異なっている.にも関わらず,現在の著作権やソフトウェアの流通,配布システムは「物」のそれを元にして作られているため，様々な点で問題を引き起こしている.

ソフトウェア制作者は著作権保護のために様々な方法をとっているものの，効果が上がらないものが殆んどであり，効果的なものであっても，プライバシーの点から批判が多かったりと，なかなか実用に適したものは作られていない．ソフトウェアメーカーの中には,違法コピーによる損失を見越して高めの価格設定を行うところもあり，ソフトウェアの著作権を保護することは，正規ユーザーの権利を保護することにも繋がる.

また，コンピュータが急速に普及してきたことにより，どこへ行ってもコンピュータが利用できるようになった．それに伴って,出先でコンピュータを操作する機会も多くなってきている．そのような場合に,いつでも自分用にカスタマイズされた環境でソフトウェアが利用できれば,作業効率の向上につながると考えられる.

本研究では,IC カード上に Java の実行環境を実装した Java Card を用いてソフトウェアのライセンス管理を行うことにより，確実にユーザーのライセンスを認証できるようにすること及びソフトウェアがインストールされている端末に関わらず,常に自分用にカスタマイズされた環境でソフトウェアを利用できるようにすることを目的としたライセンス管理方法を提案し,実装した.

2 Java Cardとは

Java Card とは，Java の実行環境を実装した IC カードであり，以下のような特徴がある.

1. 異なるメーカーのカード間でもアプリケーションの互換性が保たれる
   ‘Java” という名称が示す通り,Java Card はその上で動作するアプリケーションに対して同一の動作環境を提供する．つまり，カードに依存せずにアプリケーションが動作する.
2. 必要に応じてアプリケーションの追加,削除が可能である
   従来の IC カードでは，新規にアプリケーションを追加,削除することは不可能であり,カードの機能を変更するためにはユーザーから IC カードを回収し,再発行した後に再配布を行う必要があった.Java Card ではカード発行後にアプリケーションを追加,削除でき,インターネット経由でアプリケーションをインストールすることも可能である.
3. アプリケーションを複数搭載可能である
   従来の IC カードには,アクセス権によって複数のコマンドを管理できるものもあった．Java Card はこれとは異なり,アプリケーションはすべて VM 上で実行されるため，アプリケーション相互の独立性が保証されており，完全なマルチアプリケーションを実現している．item 通常の Java 開発環境を利用できる
   通常の Java 開発環境とアプリケーション開発ツールを利用して,カードベンダー以外でもアプリケーションの開発が可能である.このため，IC チップごとに異なるアセンブラ言語を用いてアプリケーションを開発していた従来の環境と比べて,開発者の確保が容易になると同時に，開発コストを下げることができる.

Java Card 上で実行されるアプリケーションはアプレットと呼ばれ,プログラムとして機能するだけでなく，データを内部に格納することができる．アプレットは AID(Applet ID) によって一意に識別される.

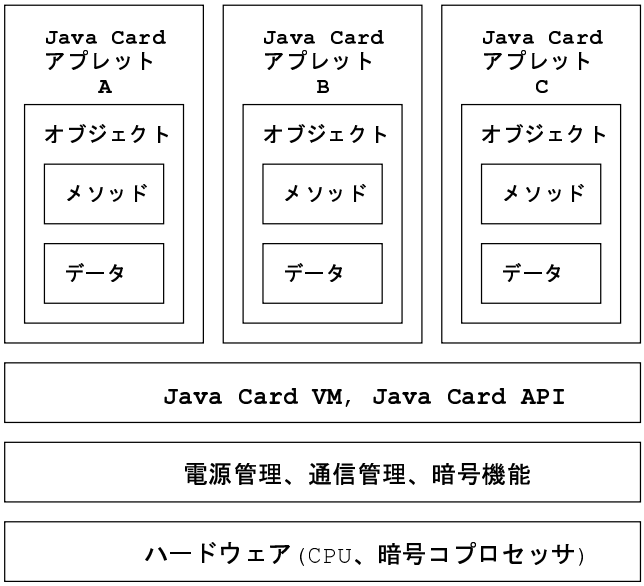

図 1: Java Card の構造

3 提案

本提案では，Java Card を利用してソフトウェアのライセンスを認証することにより，ソフトウェアの著作権保護を行う．

提案の概要を図 2 に示す．本提案では, ソフトウェアを実際に処理を行う部分 (ここでは”アプリケーション”と呼ぶ) とライセンス, 設定情報を格納する部分に分離し，ライセンスと設定情報を Java Card のアプレットに保存する．一つのソフトウェアに対して一つのアプレットが存在し, アプレット同士は AID によって一意に識別されるので，Java Card 内でアプレットが競合することはない．

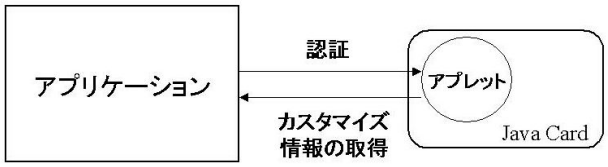

図 2: 提案の概要

アプリケーションはアプレットを認証し，認証が成功すれば，アプレットから設定に関する情報を読み込む．

3.1 ライセンスの携帯

我々が提案するライセンスの管理方法では，ライセンスは Java Card に格納されて持ち歩くことができる．ライセンスを持っているユーザーはソフトウェアがインストールされている環境では, どこでもそのソフトウェアを利用することができる．逆にライセンスを持っていないユーザーは, ソフトウェアがイストールされている環境でも, そのソフトウェアを利用することはできない．

3.2 設定情報の携帯

ユーザーによるアプリケーションの設定情報は，カード内のアプレットに保存される．このため，ユーザーは外出先でも普段と同じ設定でアプリケーションを利用することができる．

3.3 配布形態

従来の方式では，ソフトウェアの配布とライセンスの配布は必ずしも明確に区別されているとは言い難かったが，本提案ではこれらを完全に分離する．すなわち, アプリケーションの配布とライセンスの配布は完全に別の作業として行われ, アプリケーションとライセンスの両方を持っているユーザーのみが，実際にアプリケーションを利用できることになる．

本提案ではソフトウェアに関する配布は自由であり, 実際の利用に際して権利を認証するという方式をとっている．

1. アプリケーションの配布
   アプリケーションの配布とライセンスの配布を切り離したことにより，アプリケーションの配布は, 内容を変更しない限り, 基本的に自由に行うことができる．
2. ライセンスの配布
   ライセンスの配布は，アプレットの配布によって行われる. アプレットはネットワークを通じてインストールすることもできる．ただし，配布の際には安全性が保証されている必要がある．

3.4 Java Card の利用

本研究ではライセンス及び設定情報を携帯するためのメディアとして Java Card を利用している．Java Card を使うことには次のような利点がある．

- アプレットの追加・削除によってライセンスの配布, 回収を行うことができる．
- Java のセキュリティ機能を使うことができる．
- 開発環境及び人材の確保が容易である．

他のメディアとして，メモリースティックなどのリムーバブル・メディアも考えられる. こういったメディアは記憶容量が大きいという利点があるものの，外部から自由に読み書きできるので，認証に適さないという問題がある．

また，従来の IC カードでは，次のような問題がある．

- カード発効後のアプリケーションの追加, 削除が行えない．
- アプリケーション同士が完全に独立ではない．
- カード メーカー間でデバイスの互換性がない

- アプリケーションの開発はカードごとに異なるアセンブリ言語を用いて行わなければならないので，人材の確保や開発環境の整備が難しい．

3.5 想定される利用方法

本システムを利用することで，このようなサービスが可能になると考えられる．

1. 複数のライセンスをまとめて管理する
   OP(Open Platform) を用いることにより，複数のアプレットをまとめて，一つの単位として扱うことができる．幾つかのアプリケーションが一つのパッケージを構成するソフトウェアに関しては，ソフトウェアのパッケージをアプレットのセキュアドメインに対応挿せることにより，一つのアプレットに認証を代行させたり，アプレット間で情報の共有を行うための API である SIO(S harable InterfaceObject) を用いて，ユーザーに関する情報をアプレット間で共有することもできる．
2. ライセンスに期限を設定する
   アプレットはプログラムであり，内部で簡単な処理を行うことができる．アプレットに日付の計算をさせることにより，ライセンスに期限を設けることができる．

4 実装

本システムは Java クラスライブラリという形式をとっており，個々のアプリケーションにおける実装に関しては，アプリケーション開発者が各々に行う必要がある．

4.1 実装環境

実装にあたり IC カードリーダを接続した PC と Java Card を用意した．IC カードリーダの制御には，OCF(OpenCard Framework) を用いた．

4.2 認証

平文パスワードによる認証は盗聴の危険性があるため，本システムではチャレンジ&レスポンス方式による認証を用いた．具体的には，アプリケーション側でランダムな配列を生成してアプレットに送信する．アプレットはこれとパスワードからハッシュ値を生成し，アプリケーションに返す．アプリケーションも内部で同様の処理を行い，アプレットから返ってきたハッシュ値と自身で求めたハッシュ値を比較することで認証を行う．

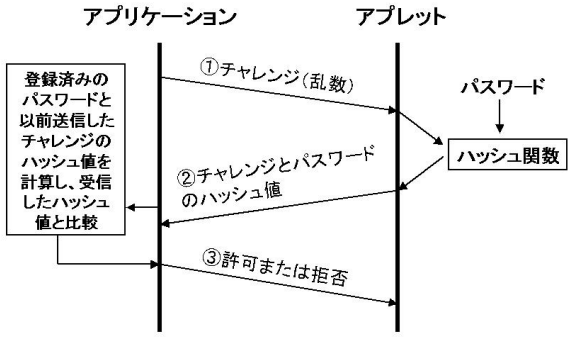

図 3: チャレンジ&レスポンス方式の認証

4.3 実装例

Sun Microsystems の提供する JDK1.3 に付属しているサンプルプログラム' NotePad' に作成したクラスライブラリを実装した．アプレットには認証に用いるパスワードと，ユーザー個人のカスタマイズの情報として，署名 (電子署名ではない) を保存できるようにした．

アプリケーションはカードリーダを監視しており，アプレットが認証されている状態でのみ，利用可能になっている．カードが抜かれるとアプリケーションは使用できない状態になり，カードを挿入すると再び使用できるようにした．

5 考察

提案したシステムのについて定性的に考察する．

5.1 カードリソースの問題

一つのアプレットに保存できるデータの量は極めて少なく (100 バイト程度)、アプリケーションの設定を保存するには不十分であるという問題がある．これに関しては，各 IC カードベンダーの動向を見る限り，いずれ解決されると思われる.RAM のサイズは Java Card の仕様では 512Byte であるが，4KB 程度の RAM を実

装したチップの開発も行われている．あるいは，もっと根本的な解決策として，ネットワーク上のリソースを参照するという方法もある．その場合, アプレット内にはリソースの URL や (必要ならば) ユーザーのアカウントなどの情報を保存しておけばいいので，それほど情報量は多くならないと思われる．

5.2 複数のライセンスへの対応

同じソフトウェアのライセンスを複数持つことができない問題がある．これは，一枚のカードに同一のアプレット ID をもつアプレットをインストールできないことに起因する. あるソフトウェアのライセンスを二つ持っていたとすると，それらは同じアプレット ID をもっていることになる．アプレット ID はアプレットを一意的に識別するための番号なので，同一のアプレット ID をもつアプレットを Java Card にインストールすることはできない．同一ネットワーク上に同じ IP アドレスを持つホストが複数あってはならないのと似ている．

同一のソフトウェアのライセンスを複数持つことは, 一見不自然ではあるが，ないとは言えない．例えば, 個人としてもともとソフトウェアのライセンスを持っていて, 会社等でもう一つのライセンスを配布される場合なども考えられる．

こういった問題に対処するには，一つのアプレットに複数の設定情報を保存できるようにするしかないと思われる. システムをそのように構築する場合, カードに必要とされるリソースはライセンスの数だけ多くなる. また，ソフトウェアがアプレットを認証する際に, どのライセンスに対して認証を行うのかを選択する必要があり，ユーザーにそのための操作を要求することになる. 現段階では，カードリソースが不足しなければ，実現は可能である．

6 まとめと今後の課題

本研究において、セキュリティ及び携帯性に優れ, アプリケーションの削除と追加が自由に行えることから,Java Card を利用したソフトウェアのライセンス管理方法提案した. 本システムには以下の特徴がある．

ライセンスと設定情報の携帯
: ソフトウェアのライセンスとユーザーごとのカスタマイズ設定を Java Card アプレットに保存することにより，ユーザーはどこでも自分用の設定でソフトウェアを使用できる．

ソフトウェアの配布方法
: ソフトウェア使用時に認証が行われるため，ソフトウェア本体は無料で, 幾つでも配布することができる．したがって，違法コピーは発生しない．

提案に基づく実装を行った結果, ソフトウェアのライセンス管理に関して有効なシステムであると考えられる．

今後は, ライセンスを格納するアプレット部分を安全に配布する方法について検討を行ってゆきたい．

参考文献

[1] JAVA CARD テクノロジー
http://www.sun.co.jp/software/consumer-embedded/card/ 21, Jan, 2001.

[2] JAVA CARD TECHNOLOGY
http://java.sun.com/products/javacard/index.html
18, Jan, 2001.

[3] Java Card 2.1.1 Technology Datasheet
http://java.sun.com/products/javacard/datasheet.html
20, Jan, 2001.

[4] GemXpresso RAD 211
http://www.gemplus.fr/developers/products/gemxpresso_rad211
18, Jan, 2000.

[5] GemXpresso RAD210
http://www.gemplus.com/products/microprocessor/gemxpresso2
18, Jan, 2000.

[6] JavaCard Forum
http://www.javacardforum.org/ 16, Jan, 2000.

[7] Java Card のセキュリティ
http://www.toshiba.co.jp/tech/review/1999/07/a07/index_j.htm
20, Feb, 2000.

[8] Java Card Special Interest Group
http://www.post1.com/home/shuming/

[9]
http://www.gemplus.fr/developers/products/gemxpresso_rad211/index.htm
, 18, Jan, 2000.

[10] GemXpresso RAD210

http://www.gemplus.com/products/microprocessor/gemxpresso211.htm,
18, Jan, 2000.

[11] JavaCard Forum
http://www.javacardforum.org/ 16, Jan, 2000.

[12] Java Card のセキュリティ

http://www.toshiba.co.jp/tech/review/1999/07/a07/index_j.htm,
20, Feb, 2000.

[13] Java Card Special Interest Group
http://www.post1.com/home/shuming/

[14] Java Card World

http://www.cp8.bull.net/sct/uk/world/index_java.html

[15]
http://pcweb.mycom.co.jp/news/2000/05/29/17.html
23, Jan, 2001.

[16] 黒葛祐介ディジタル・コンテンツの電子商取引について
オフィス・オートメーション 第 40 回全国大会予稿集, 127–130, 1999.

[17] 松沢茂, 山光忠, 小池博, 荒井達郎サイバー社会を切り開くディジタルコンテンツの世界 ディジタルコンテンツの管理・流通を支える情報システム 日立評論, Vol.81, No.7, 447–452, July. 1999.