ソフトウェアの配布方法に関する一考察
– ソフトウェアプロテクションの観点から –

2004MT050 近藤 洋介　　2004MT101 鈴木 徳宏
指導教員　真野 芳久

1　はじめに

近年、様々な方法でソフトウェアが世の中に配布され、利用されている。その中でもオンライン上や店頭で販売されているソフトウェアを不正に使おうとする攻撃者がおり、問題となっている。また既存のソフトウェア配布サイトでは、そのような攻撃者からの対策がほとんどなされていない。

そこで我々はソフトウェアプロテクションの観点から、ソフトウェアの有効な配布システムを検討した。

個々のプロテクション技術だけではなく、ソフトウェアの配布システムの枠組の中で既存の技術や新しいアイデアなどを組合せ、プロテクションに有効なシステムを検討していこうという方針である。そして、最終的にシステム全体で安全なソフトウェアの配布を実現することが目標である。

2　関連研究

本研究に関連した技術やソフトウェア配布における現状をこの章で述べる。

2.1　既存のソフトウェア配布サイト

現在ソフトウェアを配布するサイトは世の中に数多く存在し様々な種類のフリーソフトウェア、シェアウェアがいつでも手軽に入手できるようになっている。またそれらのサイトは全ての掲載ソフトウェアにウィルスチェックを行っているが、ソフトウェアのプロテクションについてほとんど対策がなされていない。

2.2　脅威

既存のソフトウェア配布サイトには様々な脅威が存在しておりそれらは互いに関連している。既存のソフトウェア配布サイトについての脅威の関連を図 1 に示す。

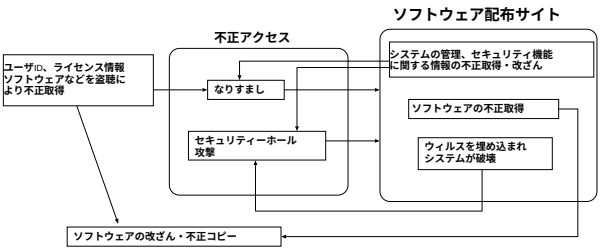

図 1　ソフトウェア配布サイトにおける脅威の関連

2.3　プロテクション技術

本研究で利用するプロテクション技術には次のようなものがある。

- 電子透かし、フィンガープリンティング (指紋)
- 暗号技術
- 認証技術
- ライセンスキー (キーファイル、ドングル)
- ウィルスチェック

2.4　ソフト電池 [6]

ソフトウェアの課金制度を実現するシステムである。対応ソフトウェアはソフト電池とセットになって動作し、様々な課金モデルが実現できる。ユーザはソフト電池化されたソフトウェアを使用する場合、ソフトウェア、ソフトウェアランタイムプログラムをダウンロードし、インストールする。ソフトウェアランタイムプログラムとは、ソフト電池化されたソフトウェアの電池の有無の確認や電池を消費、充電などの働きを制御するソフト電池マネージャ、電池メータなどが格納されているソフト電池を管理するプログラムである。

またソフトウェア開発者がソフト電池を利用するには、ソフト電池マネージャを動作させるためのソフト電池 API 関数をソースコードに組み込む作業が必要である。ソフト電池 API 関数はソフト電池 SDK というソフト電池ライブラリやツール群を含む開発キットに対応しており、関数をソースコードに記述すると対応するライブラリから関数を呼び出す仕組みである。ソフト電池の仕組みを図 2 に示す。

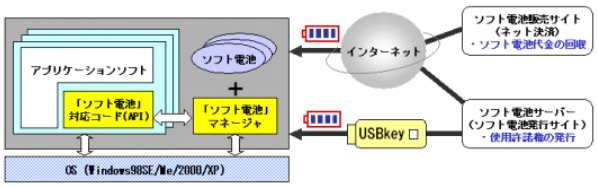

図 2　ソフト電池システムの概要 ([6] より)

2.5　レンタルアプリケーション

レンタルアプリケーションとはアプリケーションソフトウェアのサービスをインターネットを通じて顧客に提供する技術である。そのようなサービスを提供する事業者を ASP (Application Service Provider) という。ユーザは Web ブラウザを使って、ASP の保有するサーバにインストールされたアプリケーションソフトウェアを利用する。

3　ソフトウェアレンタルシステムの設計

この章ではソフトウェアプロテクションの観点からソフトウェアの配布システムを設計する。また、我々が提案する配布システムではソフトウェアをレンタルする形で利用するので、システム名をソフトウェアレンタルシステムとしそのな設計図を図 3 に示す。

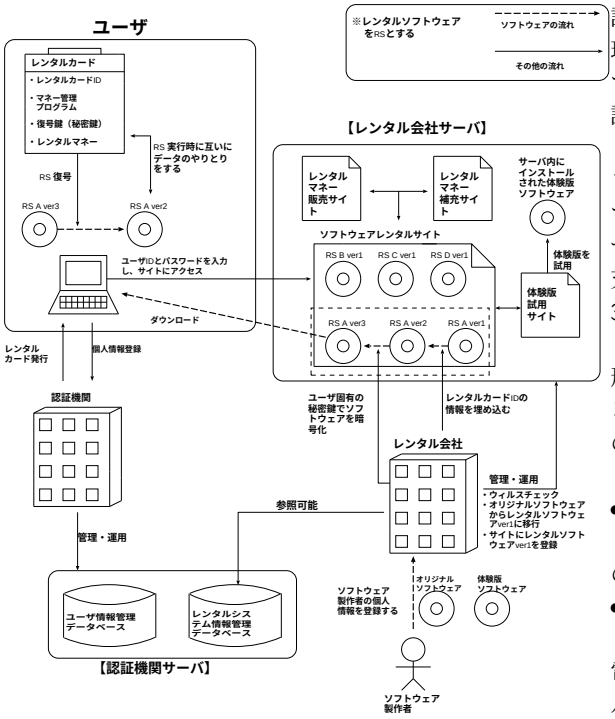

図 3　ソフトウェアレンタルシステムの設計図

以下に図 3 で登場する各オブジェクトの本研究での役割を述べる。

3.1　ユーザ

ユーザは基本的に個人のユーザを想定する。それはレンタルカード (3.4 節参照) とユーザが 1 対 1 で対応しており、企業や団体よりもソフトウェアレンタルシステムに適していると判断したためである。また、レンタルソフトウェア (3.5 節参照) の不正利用を防ぐためユーザにレンタルカードを所持させている。

3.2　認証機関

認証機関はユーザの個人情報、ソフトウェアをレンタルするための情報をデータベースで管理する。また社会的に信頼された機関である。ソフトウェアレンタルシステム内での認証機関の必要性を以下に示す。

- ユーザの登録した情報が正しいかどうかを正確に確認するため
- 登録された個人情報の不正利用や流出を防ぐため
- レンタル会社が悪意を持っていないことを証明するため
- ユーザの情報を認証機関で管理することによって、ユーザがすべてのレンタル会社で同一のユーザ ID、パスワード、レンタルカードを使用可能にするため

また、本研究ではユーザ ID はユーザを判別するための一意の文字列であり、パスワードはユーザ ID を証明する任意の文字列であると定義する。

3.3　レンタル会社

ソフトウェアを貸し出すためのサイトを作成し運営する団体である。レンタル会社は社会的信用を得るため認証機関に認定されているものとする。レンタル会社が管理するものにはソフトウェアレンタルサイト、レンタルマネー販売サイト、レンタルマネー補充サイト、体験版試用サイト、各種ソフトウェアがある。

ソフトウェアレンタルサイトは、ユーザがレンタルソフトウェアをダウンロードするサイトである。レンタルマネー販売サイト、レンタルマネー補充サイトは、ユーザがレンタルカードにレンタルマネー (3.4 節参照) を補充するサイトである。

3.4　レンタルカード

単体で演算機能を持ち合わせており、USB ドングルの形態をしていることとする。ユーザがソフトウェアをレンタルするための情報が格納されており、ソフトウェアの不正利用を防ぐ目的で作成した。以下にレンタルカードに格納されているものを示す。

- **レンタルカード ID**

レンタルカード ID は、レンタルカードをユーザ固有のものとするための情報である。

- **マネー管理プログラム、レンタルマネー**

マネー管理プログラムは、ソフト電池におけるソフト電池マネージャの仕組みを利用したものである。レンタルマネーを消費、補充する際にその演算をするプログラムである。また、レンタルマネーはソフト電池における電池に相当する。消費量はソフトウェアごとに決まっており、全てのソフトウェアに対応している。

マネー管理プログラムとレンタルマネーをレンタルカードの中に格納することによって、ユーザはどのコンピュータからでもソフトウェアを使用することができる。

- **復号鍵**

復号鍵にはキーファイルを用いる。レンタルソフトウェアを復号するために使用する。

本研究では、共通鍵暗号方式を採用するので、秘密裡にユーザに復号鍵を渡す必要がある。レンタルカードをユーザに郵送することで鍵の盗聴の危険性をなくすことが可能になる。

またこれらの情報はレンタルカードの中に格納することによって改ざんや盗聴などの脅威から耐性を持たせている。

3.5　ソフトウェア

ソフトウェアレンタルシステムでは、ソフトウェアを次の場合に分類している。

- **オリジナルソフトウェア**

プロテクション技術が施される前のオリジナルソフトウェア。この段階でソフトウェア製作者の判断によりソフトウェアに著作権を主張するための電子透かしを埋め込む。またソフトウェア製作者は身元が確かな企業や団体や個人と定義する。

- **レンタルソフトウェア ver.1**

オリジナルソフトウェアにマネー管理プログラムを呼び出す関数、レンタル会社の指紋、レンタルカード ID を識別する関数を埋め込んだもの。レンタル会社の指紋

を埋め込むことによって、不正配布されたレンタルソフトウェアを発見した場合にどのレンタル会社からダウンロードされたものか特定することができる。

- **レンタルソフトウェア ver.2**

レンタルソフトウェア ver.1 にレンタルカード ID の情報を埋め込み、ユーザ固有のレンタルカードと対応させたもの。それによって復号後のソフトウェアを不正コピーされ配布されても対応したレンタルカードがなければ使用できないので、不正利用に対して耐性を持つことができる。また、レンタルカード ID の情報はユーザの指紋となる。

- **レンタルソフトウェア ver.3**

レンタルソフトウェア ver.2 をユーザ固有の秘密鍵によって暗号化したもの。それによって、盗聴などが原因でレンタルソフトウェアが流出した場合、復号鍵を持たない者にはレンタルソフトウェアが使用不可である。また、なりすましによる不正利用も防ぐことができる。

- **体験版ソフトウェア**

体験版ソフトウェアはオリジナルソフトウェアに機能制限を加えたものである。体験版ソフトウェアが改ざんされ機能制限などが外され不正利用されることを防ぐため、本研究ではレンタルアプリケーションの仕組みを利用しユーザにソフトウェア自体を渡さないことにしている。

このようにオリジナルソフトウェアに新たな機能を加る作業は、すべてレンタル会社が行なう。

4 ソフトウェアレンタルシステムの検討

この章では、3 章で設計したソフトウェアレンタルシステムについて既存のソフトウェア配布サイトとソフト電池システムをそれぞれプロテクションの観点から比較検討していく。

4.1 既存のソフトウェア配布サイトとの比較検討

この節では既存の配布サイトの脅威に対してソフトウェアレンタルシステムがどのような対策を立てているかを比較検討する。

4.1.1 製作者と運営者間における脅威と対策

■コンピュータウィルス 既存の配布サイト、ソフトウェアレンタルシステムともにウィルスチェックを行なっている。

■ソフトウェアの不正利用 配布サイト、ソフトウェアレンタルシステムともに運営者側が悪意を持っている場合には、ソフトウェアを不正利用される可能性がある。

そのため、ソフトウェアレンタルシステムでは、認証機関が社会的に信頼できると証明したレンタル会社のみを想定している。

4.1.2 ユーザと運営者間の通信における脅威と対策

■ユーザ ID とパスワードの盗聴 既存の配布サイト、ソフトウェアレンタルシステムともにユーザ ID とパスワードの情報を通信経路で盗聴される可能性がある。その情報を利用することでなりすましなどの脅威が考えられ、不正アクセスされることが考えられる。また不正アクセスによって、正当なライセンスを持たない者にソフトウェアがダウンロードされ不正利用される恐れがある。

ソフトウェアレンタルシステムでは、仮にユーザ ID とパスワードが流出し不正にダウンロードされたとしてもレンタルカードがなければ、ソフトウェアを復号することができないのでソフトウェアを不正に利用することができない。

■ライセンスデータの盗聴 既存の配布サイトでは、シリアルナンバーなどのライセンスデータが盗聴される可能性がある。ライセンスデータの流出により、正当なライセンスを持たない者にソフトウェアを不正利用される危険性が考えられる。

ソフトウェアレンタルシステムでは、ライセンスデータをレンタルカードに格納して、ユーザに郵送しているので通信経路上で盗聴される危険性はない。

■ソフトウェアの盗聴 既存の配布サイト、ソフトウェアレンタルシステムともにソフトウェアのダウンロード中に盗聴される可能性がある。それによってソフトウェアを不正利用される恐れがある。

ソフトウェアレンタルシステムでは、仮に盗聴されたとしてもレンタルカードがなければ、ソフトウェアを復号することができないのでソフトウェアを不正利用することができない。

4.1.3 ダウンロード後のソフトウェアにおける脅威と対策

■ソフトウェアの不正利用 既存の配布サイトでは、ダウンロード後のソフトウェアプロテクションに関しては、製作者に任せられているので、ソフトウェアが改ざんされたりライセンス数以上の不正コピーをされる可能性がある。また、ダウンロードした体験版を解析し、機能制限などを外すことによって不正利用する可能性も考えられる。

ソフトウェアレンタルシステムでは、ソフトウェアを使用するためにレンタルカードが必要なのでダウンロードした後のソフトウェアを自分が所有する他の機器にコピーすることは問題ない。だがソフトウェア自身を不正に解析、改ざんされレンタルカードがなくても使用できるようにされる危険性がある。

■不正な二次配布 既存の配布サイトでは、ダウンロード後のソフトウェアを不正に二次配布される恐れがある。正当なライセンスを手に入れることや改ざんにより機能制限を外した後のソフトウェアを二次配布されると、正当なライセンスを持たない者に広くソフトウェアが不正利用されてしまう可能性がある。

ソフトウェアレンタルシステムでは、仮に、復号後のソフトウェアを不正に二次配布されたとしてもレンタルカードがなければソフトウェアを使用することができない。だが、ソフトウェア自身を不正に解析、改ざんされレンタルカードがなくても使用できるようにされる危険性がある。

■ライセンスデータの不正利用　既存の配布サイトでは、入手後のライセンスデータを不正に複製、配布される危険性がある。またライセンスデータを不正に解析することによって新たなライセンスキーを作製し、悪用することが考えられる。

ソフトウェアレンタルシステムでは、ライセンスデータであるユーザ固有の復号鍵とレンタルカード ID はレンタルカードの中に格納してあるので、ライセンスデータの不正な解析、複製、配布に対して耐性を持たせている。

4.2　ソフト電池との比較検討

ソフトウェアプロテクションの観点からソフト電池を見ると、不正コピーや不正配布に関しては耐性を持つことができるが、ソフトウェア自体が改ざんされソフト電池がなくても実行させるように書き換えられる恐れがある。レンタルソフトウェアシステムについても復号後のレンタルソフトウェアに対して改ざんされる恐れがある点では同様である。

以下では図 4 でソフト電池とソフトウェアレンタルシステムにおいての違いを示した後、更にその詳細を述べる。

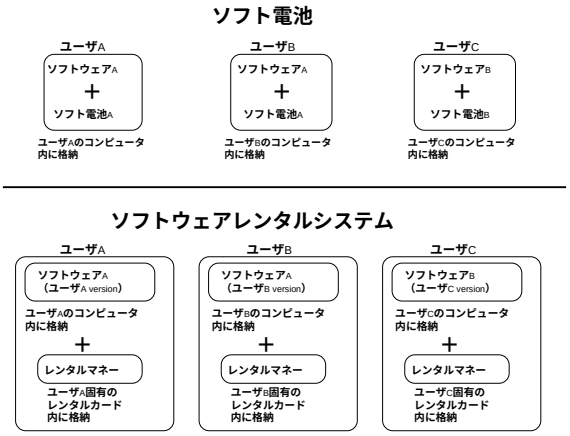

図 4　ソフト電池との相異点の比較

■ソフト電池　ソフト電池では、ソフト電池とソフトウェアが 1 対 1 で対応しておりどのユーザに対しても同じ組合せとなっている。つまりユーザは、ソフトウェアと同じ数のソフト電池を必要とするので柔軟な課金制度を実現することができる。しかし、ソフト電池を他のソフトウェアに使用することができないので、ソフト電池が余る場合も予想される。

また、ソフト電池とソフトウェアは同じコンピュータ内に格納される必要があるので、他のコンピュータでソフトウェアを使用するためには、再びソフトウェアとソフト電池をインストールする必要がある。

■ソフトウェアレンタルシステム　ソフトウェアレンタルシステムでは、レンタルマネーとレンタルソフトウェアが 1 対多で対応している。すべてのレンタルソフトウェアに対してレンタルマネーが使用できるのでソフト電池と違いレンタルマネーが余ることがなくなる。

またレンタルソフトウェアとユーザが 1 対 1 で対応しており、レンタルソフトウェアがユーザ固有のものとなっている。固有のものとすることによって、不正に配布されたときに、耐性を持つことができる。

レンタルカードにレンタルマネーを格納することによって、レンタルソフトウェアがインストールされているどのコンピュータでも使用することが可能となる。

5　おわりに

本研究ではソフトウェアの不正利用に対する耐性をソフトウェアレンタルシステムという限定されたある一定の条件の中で高めようと試みた。そこで我々が定義した条件の中で認証技術、暗号技術、電子透かし、フィンガープリンティング、レンタルアプリケーション、レンタルカードの仕組みを組み合わせた。その結果 2.2 節で述べた脅威に対して既存の配布サイトより強い耐性を得ることができると考えられる。

またソフトウェアレンタルシステムで配布されるレンタルソフトウェアが不正利用されるには次の場合が考えられる。

場合 1　レンタルカードとレンタルソフトウェアが流出
場合 2　レンタルカードとユーザ ID、パスワードが流出
場合 3　レンタルソフトウェアが流出し、改ざん

レンタルカードは複製が困難であり、レンタルカードとレンタルソフトウェアが 1 対 1 で対応していることから場合 1、2 が起こる可能性は低いと予想される。それに比べ場合 3 が起こる可能性は高い。

今後の課題は、上記の場合についての対策や今までに述べた短所を検討し、更にシステムの耐性を高めることである。また具体的な組込みアルゴリズムなどの更に詳しい検討が必要である。

参考文献

[1] Kracker's, BEAMZ：クラッカー・プログラム大全, データハウス (2003).

[2] 佐々木ら: インターネット時代の情報セキュリティ-暗号と電子透かし, 共立出版 (2000).

[3] John Viega, Gary McGraw：Building Secure Software, オーム社 (2006).

[4] 土居範久監修, 佐々木良一ら編: 情報セキュリティ事典, 共立出版 (2003).

[5] Christian S. Collberg, Clark Thomborson：Watermarking, Tamper-Proofing, and Obfuscation - Tools for Software Protection, IEEE Tr. on SE, Vol.28, No.8, pp.735-746 (Aug.2002).

[6] Paltiosoft：ソフト電池, http://www.paltio.co.jp/soft-denchi/

[7] フリーソフトウェア財団：GNU オペレーティング・システム, http://www.gnu.org/home.ja.html

[8] 特許庁：標準技術集, http://www.jpo.go.jp/shiryou/index.htm