安全なソフトウェア流通システムの構築と運用評価

佐々木茂彦† 桂林浩 谷口慎一郎 京嶋仁樹 田丸恵理子 大澤隆

ssasaki@crl.fujixerox.co.jp†

富士ゼロックス(株) 総合研究所

259-01 神奈川県足柄上郡中井町境 430 グリーンテクなかい
TEL:0465(80)2193　　FAX:0465(81)8971

1 はじめに

近年のパーソナルコンピュータ(PC)の発展と普及はめざましい。インターネットも PC 同様に、急速に発展し普及しつつある。PC とインターネット環境の普及に伴い、デジタル化されたコンテンツの流通に要するコストは非常に小さくなり、文書、画像、プログラム、各種データ等、多種多様なデジタルコンテンツが大量に流通するようになった。

当社も最近の PC 化の波に乗り、従来の自社システムから PC 環境に移行しつつある。これに伴い、ネットワーク上で流通するシェアウェア/フリーソフトと言われる比較的小規模なアプリケーションが、社内の一部で利用されるようになった。シェアウェア/フリーソフトは、有用なものが多く、PC 環境上の作業の効率化に不可欠である。しかし、シェアウェア/フリーソフトの利用は社内の一部の範囲にとどまり、一般的に利用されることはなかった。

なぜならば、シェアウェア/フリーソフトは、様々な流通経路で多数のタイトルが流通しており、必要な機能を持つ製品を探すのは容易ではないという問題があった。また、各々の使用許諾条件が細かく異なり、作者に直接交渉しなくてはならない場合がほとんどであったため、個々のオフィスワーカが必要なソフトウェアを探し出し、使用許諾取得処理をするには負担が大きすぎるという問題があったためである。

これらの問題を解決し、シェアウェア/フリーソフトの展開を促進するため、本研究において PC 用のシェアウェアとフリーソフトを対象としたライセンス管理システム、「ソフトウェアライセンス管理システム(SLM システム)」の構築を行い、社内の PC 環境の改善をはかった。

構築した SLM システムにより、流通を妨げることなく、オフィスワーカに整理された形で製品情報を提供し、容易に使用許諾取得処理を行うことが可能となった。また副次効果として、SLM システムが持つ利用履歴の捕捉機能により、ウィルスが侵入した場合の感染経路の追跡が可能となった。

2 流通モデルとセキュリティ技術

2-1　超流通モデル

デジタルコンテンツの流通コストが小さいことを活用した流通モデルとして、1983年に森が提案した「超流通モデル」という概念がある[1]。これは、デジタル知財の流通における著作者の権利の保護と、利用に基づく課金に関するモデルである。

情報供給者(プロバイダ)が直接ユーザにデジタルコンテンツを配布することを1次流通といい、ユーザの手に渡ったデジタルコンテンツが、プロバイダの手を介さずユーザによりコピーされて他ユーザに流通することを2次流通という。

従来の流通モデルにおいては、2次流通は不正コピーであり、プロバイダの利益を損なう行為であった。しかし、超流通モデルにおいては、課金がコンテンツの利用時に行われるため、2次流通はプロバイダの利益を損ねるどころか、むしろ流通を促進する行為となる。つまり、超流通モデルは、2次流通の防止コストがかからないばかりか、2次流通によって流通コストを大幅に低減できる大きな利点を持つ。

しかし、現在市場で実際に運用されている、2次流通を許す、デジタルコンテンツの流通システムは、悪意のユーザの不正を完全に防ぐことはできない[2]。2次流通を許す流通モデルをビジネスとして成立させるためには、悪意のユーザの不正を防止できるセキュリティ機能が不可欠である。

2-2　DDSA 技術

当社で開発したセキュリティ技術のひとつに Digital Document Security Architecture (DDSA)技術がある。この技術は、公開鍵暗号技術とブロック慣用暗号技術を用いて構成されており、超流通モデルにおいて、悪意のユーザの不正を防止できる[3]。そこで、この DDSA 技術を使って、SLM システムの構築を行った。まず、DDSA 技術について簡単に概要を説明する(図1)。

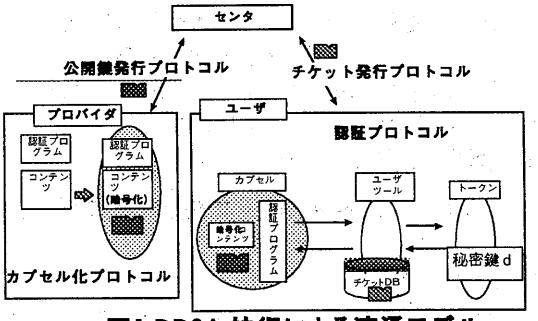

図1 DDSA 技術による流通モデル

DDSA 技術を用いたシステムでは、主に暗号鍵情報

を管理するセンタが存在する。あらかじめ、センタからすべてのユーザにトークンが配布される。トークンは、ユーザID、秘密鍵情報など各ユーザの固有情報と、コンテンツの利用履歴などの課金情報を保持するメディアである。トークン内の情報へのアクセスは、トークンを所持する正当なユーザであっても制限され、直接トークン内の情報にアクセスすることはできない。この制限によって、トークンの複製、トークン内の情報の改変など、悪意のユーザの攻撃から保護される。

プロバイダ(シェアウェア/フリーソフトの作者)が制作したデジタルコンテンツは暗号化され、認証プログラムコードを付加されて、ユーザに提供される。これをカプセルという。カプセルは、暗号化されているのでそのまま利用することはできない。利用するためには、アクセスチケットが必要となる。アクセスチケットとは、トークン毎にカスタマイズされたデジタル鍵データで、カプセルに組み込まれた認証プログラムにより、コンテンツの利用の可否を決定するために使われる。アクセスチケットは、ユーザの要求に応じてセンタから発行される。また、アクセスチケットに、利用できる期間の設定をすることもできる。

アクセスチケットは、デジタルデータであり、容易にコピー可能だが、指定されていないカプセルの利用に用いることはできない。また、指定されたトークンがないと利用できない。つまり、カプセルおよびトークンと、それらに対応するアクセスチケットの3つをそろえることで、カプセルを復号しコンテンツを利用することが可能となる。

利用時に行われるカプセルの復号処理と復号されたコンテンツは、ユーザが直接アクセスできないよう保護されるため、ユーザは暗号化されていない、生のコンテンツを入手することはできない。また、復号処理時にトークン内に履歴が記録されるため、後でトークンより履歴情報を回収することにより、利用履歴を捕捉することができる。

コンテンツ利用料の課金は、アクセスチケットの発行履歴、またはカプセル復号処理時のコンテンツ利用履歴の記録に基づきセンタが行う。

以下に、DDSA 技術の特長をまとめる。

1. カプセル、トークン、アクセスチケットの3つがそろうことにより、コンテンツを利用することができる。
2. カプセルを公開しても、不正に利用されない。
3. アクセスチケットを公開しても安全である。
4. 利用期間を制限したアクセスチケットをつくれる。
5. ユーザから生のコンテンツが見えない。
6. 利用履歴の記録ができる。

3 ソフトウェアライセンス管理システム

3-1 コンテンツ

今回対象にしたコンテンツである、シェアウェアとフリーソフトの特徴について簡単に説明する。

シェアウェアは、ネットワークや雑誌の付録により、入手は対価なしで可能である。しかし、使用するためには対価の支払いが義務づけられているソフトウェアのことである。無料で試用可能だが、試用では期間や機能に制限がある場合が多い。

フリーソフトとは、シェアウェア同様ネットワークや雑誌の付録を介して流通し、無償で使用できるソフトウェアのことである。使用許諾条件は各ソフトごとまちまちである。

シェアウェアとフリーソフトは一般に市販されるパッケージソフトに比較して、バージョンアップの頻度が高い傾向にある。シェアウェアのバージョンアップは、無償でできる場合と有償の場合がある。

コンテンツは、インターネット[4]や Nifty serve、CDROM 付書籍等[5]から収集し、ソフトウェアの著作権者に電子メールで使用許諾を求めた。許諾が得られたものについて、SLM システムのコンテンツとして採用し、カプセル化した。

3-2 設計方針

以上説明したコンテンツの特性を考慮し、以下の方針で SLM システムを設計した。

1. シェアウェアとフリーソフトの製品情報の検索閲覧環境を提供し、容易にユーザが希望するソフトウェアを入手できるようにする。
2. 頻繁に生じるバージョンアップについて、簡単な操作で対応できるようにする。
3. シェアウェア料金の支払処理を集中管理して、ユーザの事務処理の負担を軽減する。
4. シェアウェアについて、試用と本利用の区別を設け、使用許諾条件を遵守できるようにする。
5. ウィルス混入等の不測の事態に備えるために、ソフトウェアのインストールと利用の履歴が把握できるようにする。

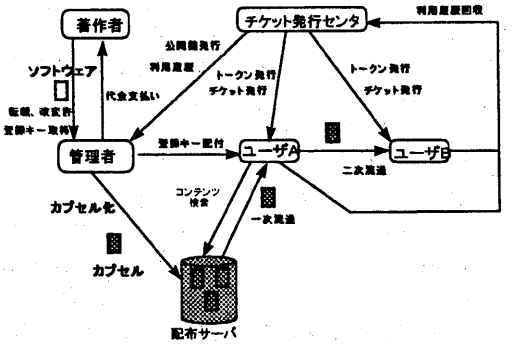

図2 ソフトウェアライセンス管理システム概略

この方針で構築した SLM システムの概略図を図2に示す。チケット発行センタは、ユーザにアクセスチケットを発行するセクションで、チケット発行サーバと履歴回収サーバで構成される。配布サーバは、ユーザに製品情報を提供し、カプセルを配布する機能(1次流通)を持ち、WWW 技術で構築された。

ユーザには、チケット発行センタからトークンが、各々に配布される。また、チケットの管理、コンテンツの利用(復号処理)、履歴情報管理を支援するアプリケ

ーションである、ユーザツールが各ユーザの PC にインストールされる。

以下に、各セクションについて説明を行う。

3-3 チケット発行センタ

チケット発行センタは、WindowsNT3.51上の WWW サーバ(MS IIS2.0)とデータベースシステム (Oracle WG Server7.2)で構築された、チケット発行サーバと履歴回収サーバより構成される。

チケット発行サーバは、ユーザツールからの要請に応えて、アクセスチケットを発行するサーバである。チケット発行/取得の通信は HTTP(Hyper Text Transport Protocol)を用いて行われる。HTTP を採用した理由は、ファイアーウォールを乗り越えられる場合が多く、また汎用性が高いためである。

SLM システムで、コンテンツを利用すると、その履歴がトークンの中に記録される。履歴回収サーバは、この履歴記録を回収するサーバである。ユーザが明示的に履歴回収の指示をユーザツールに与えることにより、履歴回収サーバへ履歴データが送付される。利用履歴情報は管理者に送られ、課金処理に用いられる。

3-4 配布サーバ

コンテンツを配布(1次流通)する配布サーバは、ユーザが WWW ブラウザを用いて、コンテンツを検索したり、ダウンロードすることができるように、Windows NT3.51 上の WWW サーバ(MS IIS2.0)を用いて、実装された。

コンテンツのタイトル名と内容の説明文を対象とした全文検索機能と、カテゴリ分別による検索機能を持ち、ユーザが望む機能を持つコンテンツを探し出すのを支援した。また、チケットの発行履歴データより利用ランキング表を表示し、人気の高いコンテンツを知ることができる機能を設けた。

また、推薦ソフトのページを設け、利用者の推薦文を掲載した。これにより、コンテンツの探索や口コミ情報による流通を促進できるようにした。

3-5 管理者

管理者は、SLM システム全体の管理を行う。基本業務は、(1)フリーソフト/シェアウェアの作者との使用許諾交渉、(2)ソフトウェアのカプセル化と配布サーバへの登録、(3)チケット発行履歴に基づく課金処理、(4)作者から送付された登録キーのユーザーへの配付、の4つである。SLM システムに対するクレーム対応も行った。

3-6 ユーザの環境

SLM システムが提供するサービスを利用できる PC 環境は、MS Windows 95または Windows NT3.51が搭載された IBM 互換 PC である。ユーザ環境は、トークンとユーザツールで構成される。

SLM システムでは、トークンに IC カードを採用した。IC カードは耐タンパー性にすぐれ、可搬性も良好な媒体である。各ユーザの PC には、IC カードにアクセスするために、シリアルポートを介して PC と接続できる IC カードドライブを接続した。トークンには、秘密鍵情報の他にアクセスチケットや利用履歴情報も記録される。SLM システム開始時に、あらかじめ各ユーザの秘密鍵情報を書き込んだ IC カードおよび IC カードドライブを各ユーザに配布した。

ユーザツールとは、SLM システムを利用するために必要なアプリケーションである。ユーザツールには以下の機能がある。

1. トークンの管理
   PC と IC カードドライブの通信を管理する。ユーザがトークンの正当な所持者であることを確認するために、暗証番号による認証を行う。
2. アクセスチケットの管理
   チケットの発行依頼、チケットの取得、チケットの閲覧、コピー、削除等の管理を行う。カプセルの復号時には、認証プログラムにチケットを渡す。
3. 利用履歴情報の管理
   利用履歴を記録し、必要に応じて履歴をセンタへ送付する。

システム開始時に、ユーザが各自ユーザツールを自分の PC にインストールできるよう、ユーザツールのインストールキットは、配布サーバで公開し、WWW ブラウザでダウンロードできるよう手配した。

3-7 システム運用

SLM システムにおいて、ユーザがコンテンツを検索、入手して利用し、プログラムの作者に料金が支払われるまでの流れに沿って、システム運用について説明する。

まず、ユーザは WWW ブラウザで配布サーバに接続し、望むコンテンツを検索する。希望するコンテンツがみつかったら自分の PC にそのコンテンツのカプセルをダウンロードする。また、配布サーバからダウンロードしなくても、知人から直接カプセルをコピー(2次流通)してもらってもよい。

カプセルとは、MS-Windows95/NT 上の win32環境の実行形式(EXE)ファイル内の実行コードを暗号化し、アクセスチケット認証、暗号化された実行コードの復号を行うプログラムコード(認証プログラム)を付加したものである。カプセルもまた実行形式ファイルである。

カプセルを実行すると、まず付加された認証プログラムが実行される。認証プログラムは、ユーザツールと通信を行い、対応するチケットが保持されているか確認する。保持されていない場合、チケット取得処理に自動的に入る。

PC の画面には、チケット取得処理ウィンドウが現れる。ウィンドウには、対応するコンテンツの名称と、チケットの種別が表示される。チケットの種別には、試用と本利用チケットの2種類がある。これはシェアウェアの試用と本利用に対応したもので、フリーソフトには試用チケットはない。

試用チケットは、ソフトウェアを試しに使ってみるためのもので、利用できる期間が制限されるが、利用料を

支払う必要はない。本利用チケットは利用料を支払って利用するためのもので、期間の制限はない。

試用期間が切れた後に、試用チケットを再取得して、不正利用することは、チケット発行センタが蓄積しているチケット発行履歴を用いて防止している。チケット紛失対策のため、最初にとった試用チケットの再発行は可能だが、試用終了日は更新されないようにした。この仕組みにより使用許諾条件通りの運用ができる。

チケット取得ウィンドウで試用か本利用のどちらのチケットを取得するか選択すると、自動的にユーザツールがチケット発行サーバにアクセスし、チケットを取得する。取得したチケットはユーザツールで確認することができる。

チケットが取得されていた状態で、カプセルを実行すると、認証プログラムは、チケットが保持する鍵情報とトークン内の秘密鍵情報から、ユーザツールを介して復号鍵情報を取得し、カプセル内の暗号化部分を復号し、メモリ上に元のコンテンツのイメージを生成し実行する。ユーザからは、これらの処理は意識されることなく、普通の実行ファイルと同様に扱うことができる。

本利用チケットの発行記録に基づいて、利用料をシェアウェアの作者の指定した決済手段で送金した。シェアウェアには、利用料を支払うと、試用時の制限を解除する登録キーを送ってくる制度をとるものが少なくない。料金支払い担当者が受け取ったこれらの登録キーは、本利用チケットを取得したユーザに転送した。

4 運用と評価

SLM システムは、富士ゼロックス(株)総合研究所において、1997年2月4日より運用を開始し同年4月に運用を終えた。

約3ヶ月の運用の間に、SLM システムを利用したユーザは260人に達した。登録したコンテンツは153本、アクセスチケットの発行数は1200を超えた。運用前に比較し、シェアウェア/フリーソフトの利用が促進され増加した。これは、SLM システムによってシェアウェア/フリーソフトの社内展開をはばむ問題が解決されたことを示唆する。

運用終了後にユーザを対象にアンケートを行った。それによると、製品情報の提供機能については、好評であった。配布サーバのアクセス履歴によると、利用ランキング表示機能が多数利用されており、ランキング順位を参考にコンテンツをさがすユーザが多かったことがわかった。

料金支払の集中管理機能は正常に動作し、料金支払のユーザの工数低減効果が認められた。試用と本利用がある料金制度も、作者の提示したライセンス通りに運用でき、バージョンアップ対応も正常に行えた。利用履歴の捕捉機能も正常に動作した。幸いなことにコンピュータウィルスの感染事例はなかった。また、システムの不備をついた不正利用は発見されなかった。

アンケートによると、トークン(IC カード)の取扱いに関してはユーザの受容性が低く、トークンの存在や取扱いの手間に不満があることがわかった。また、登録キーが存在するシェアウェアの場合、ユーザが本利用するとき、SLM システムの本利用チケットの取得と登録キーの入力の2つの処理が必要となり、ユーザと管理者双方の作業が煩雑であるなど、いくつかの問題点が判明した。

5 おわりに

SLM システムの構築と運用により、オフィスにおけるコンテンツの利用状況の正確な把握と、自由な流通の両立を可能とした。

また、コンテンツ収集において交渉したシェアウェア/フリーソフトの作者には積極的な人が多く、SLM システムのような法人ユーザが課金処理をまとめて決済する仕組みに賛同的であった。SLM システムは、オフィスワーカおよびソフトウェア作者双方に有益であり、高い効用を持つと思われる。しかし、本利用時にチケットと登録キーが両方必要となり煩雑である問題など改良すべき点も残っている。

今回は、対象コンテンツをシェアウェア/フリーソフトに絞ったシステムを構築した。しかし、流通するデジタルコンテンツは多種多様であり、シェアウェア/フリーソフト以外のコンテンツに対しても、製品情報の入手性と使用許諾取得の煩雑性という問題は同じく存在する。

今後さらに、今回明かになった問題点を改善し、シェアウェア/フリーソフト以外を対象としたデジタルコンテンツのライセンス管理法を模索し、システムの設計、構築、運用実験を進めていく必要がある。

謝辞

本研究を行うにあたり、本システムへのソフトウェアの提供に快く同意してくださったシェアウェアとフリーソフトの作者の皆様に感謝いたします。また、本研究テーマを行う機会を与えてくださった土屋元彦専務、上林憲行主幹研究員、システム開発および有益な助言をいただいた国友修一課長、申吉浩副主任研究員、佐口泰之所員、小林健一所員、小島俊一所員、齊藤和雄所員、鈴木敏克所員、木子健一郎所員、田口正弘所員、システムの運用実験の被験者となった富士ゼロックス総合研究所の方々に感謝します。

参考文献

[1] 森亮一："ソフトウェア・サービスについて", JECC ジャーナル, No.3, pp.16-26(1983)

[2] http://kawahara.k.tsukuba-tech.ac.jp/SdA/OtherServersCom.html
http://infoket.nttprintec.co.jp/
http://softpark.jplaza.com/admin/guide.html
http://www.ibm.co.jp/cd_showcase/
http://mshuttle.sdnet.or.jp
http://www.ntm.co.jp/mitakata/

[3] 申, 小島："デジタル著作物流通の為のアクセス制御スキーム", 信学技報 ISEC97-20, pp65-73, 1997.07.18

[4] http://www.forest.impress.co.jp/win1/index.html
http://www.vector.co.jp/

[5] ベクターデザイン；"フリーソフト&シェアウェア PACK for WIN 1997年前期版"；ベクターデザイン；ISBN4-900952-01-X；1997年