2R−4

ネットワークにおける暗号化されたソフトウエアの流通に関する研究*

榊原 裕之　武藤 康史　関 一則　松下 温†　慶應義塾大学 理工学部‡

1 はじめに

近年の有料衛星放送の実現は、既に確立されつつある暗号技術の今後の応用例として非常に注目されている。我々はこの概念をさらに発展させ、ソフトウエアを暗号化 [1] させた形で流通させることによって、著作権を保護しながらこれらのソフトウエアをコンピュータネットワーク上で流通させるためのシステムを提案する。現在のソフトウエアの流通形態は生産者の販売網による正規の流通経路と既に購入したユーザ間でのコピーによる不正な流通経路という2つの大きな流通形態があり、後者の流通経路は不正な経路ではあるがその流通能力は正規の経路の能力を凌ぐ。我々のシステムでは、この能力を利用してユーザー間のコピーによる流通を正規の流通経路とするようなシステムである。

2 ソフトウエアとプロテクト

2.1 コピープロテクト

従来はソフトの不正利用を防ぐためにコピープロテクトという複製を作れないようにする機構を含んだソフトが多く存在した。

コピープロテクトは、フロッピーディスクを媒体とするソフトに主にかけられており、簡単に再現できないような特殊なフォーマットをフロッピーの一部に施してこれをチェックしてマスターかコピーかを判別していた。その種類は多く、複数のプロテクトを組み合わせて強力なプロテクトをかけた商品も登場した。[2]

コピープロテクトを外すツールとして、バックアップツールというものが市販されていたが著作権侵害の問題から、現在は有名量販店ではイメージの悪化を懸念してほとんど販売していない。

2.2 コピープロテクトの問題点

コピープロテクトの問題点としては,“バックアップがとれない”,“プロテクトを強力にすると実行時に時間的ロスが出る場合がある”, 等が挙げられる。上記の理由から現在のビジネスソフトの多くはソフトにプロテクトをかけないで流通している。しかし、ソフトにプロテクトをかけない場合は, “不正利用のリスクを見込んだ高めの価格設定”, という問題が生じる。

3 新しいソフトの流通形態

前述のソフトの保護に関する諸問題を解決するような流通形態として“レンタル”の概念を取り入れ、利用時間に応じて課金するたシステムを提案する。ソフトの複製は可能で自由にできるが、利用するときはソフトの管理者(ソフトウエアサーバーと呼ぶ)に申請をしないと利用できないという方法である。ソフトウエアサーバは各地域ごとに配置され、ソフトに関する各種サービス(レンタル、課金情報等)にたずさわる。図1に全体像を示す。

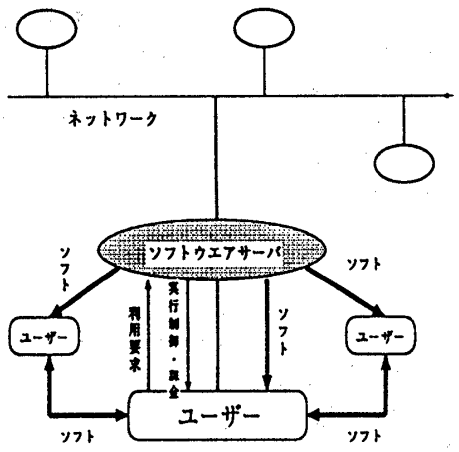

図 1: システムの概要

3.1 ソフトウエアサーバー

ソフトウエアサーバーはネットワーク管理者が各地域(会社、学校等)に設置し、ソフトウエアの流通、利用課金に関する管理を局地的に行なうサービスセンターである。ソフトの使用はここに通信で申請することにより可能となり、利用状況がユーザーから“管理プロセス”を通じて送られてくる。

*A study of a distribution system of encrypted software on the computer network
†Hiroyuki Sakakibara, Yasushi Mutoh, Kazunori Seki, Yutaka Matsushita
‡Faculty of Science and Technology, Keio University

3.2 管理プロセス

管理プロセスはネットワーク管理会社が無料配布するソフトで、ソフトウエアサーバーとユーザー間の通信を行ない、アプリケーションソフトの実行は管理プロセスを通じて行なわれる。

3.3 ソフトの実行制御

実行制御はレンタルを行なう場合に最も重要な要素となる。実行制御の基本的な形式は次の三つが挙げられる。

制御無し 無料配布に関するソフト (情報も含む) は、無制御で管理される。

信号による制御 管理プロセスとソフトの間で一定時間間隔で信号のやりとりを行なう。さらに、管理プロセスがソフトウエアサーバーに信号のやりとりの状況を逐次報告することによりソフトウエアサーバーは利用状況を把握する。ソフトには管理プロセスへの通信に関するプログラムが付加される。信号の内容は、毎回変化させれば安全性は高まる (関数に初期値を与える等)。

暗号による制御 ソフトを暗号化して流通させる。利用者は管理プロセスを通じて、暗号を解く復号化鍵をソフトウエアサーバから借りてくる。ソフトを復号化して使用可能となる。鍵の貸し出し状況を把握することにより、ユーザーの利用状況を把握する。暗号の処理速度を考慮し、暗号化する部分を分けても良い。

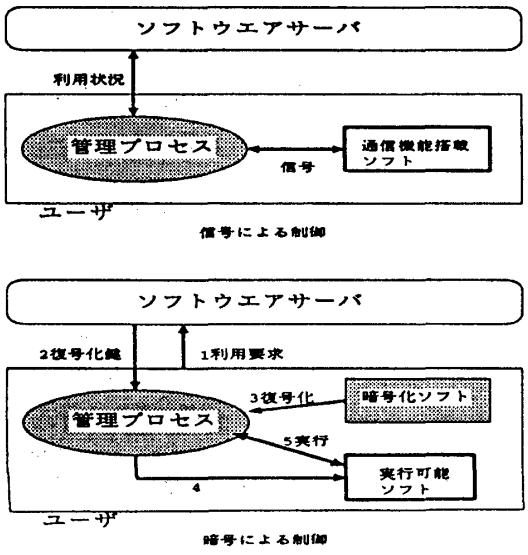

図 2: 制御方式

実際には信号による制御と暗号による制御の併用が安全性の面では望ましい。

4 システムの利点

流通時間と経路の短縮が実現されるのでユーザーは使いたい時にいつでも希望のソフトが使用できる。それに伴い、流通面でのコストダウンがはかられる。さらにソフトウエアの著作権の保護が可能なので、従来のように不正コピーによる損を見込んでの価格設定よりも低価格化が可能になる。現在では正規ユーザーの把握は、葉書による返信により行なうのが主流のようだが、ソフトの流通状況はソフトウエアサーバーを通じて把握できるのでこれが簡単になり、Version の管理も容易になる。

ソフトの利用量に応じた課金方法という妥当な使用料の支払方法が可能になるので利用の手軽さにより多くのソフトを試用して、自分に最適なものを選ぶことができる。さらに、個人ユーザーが自己開発のソフトを流通させることもできるのでソフトウエア業界の質の向上が期待される, 等が利点として挙げられる。

5 課題点

ネットワーク全般にいえることであるが、その性質上、過失、故意、事故等によるシステムの異常時に多くのユーザーのソフトが使用できなくなる可能性がある。管理プロセスとソフトウエアサーバー間で、情報のやりとりを行ないこれに基づいて実行の制御を行なうので、特に注意しなくてはならない。また、ソフトが改変してしまうこともあり、改変したソフトが流通する可能性がある。改変に関してはデジタル署名を応用すれば検出は可能であるが、改変したソフトの流出は避けたい。また、コンピューターウイルスに対する防御も考慮しなければならない。

暗号をソフトに用いた場合、処理速度の問題が挙げられる。暗号鍵、メモリアクセスなどによるソフトの解読に対する防御は最も熟慮しなければならないポイントである。メモリアクセスによるソフトの解読の防止は、現在では OS の関係上完全に防ぐのは困難であり、これらをふまえたシステムの構築が必要である。

参考文献

[1] 辻井重男, 笠原正雄, "暗号と情報セキュリティ", 培風館, 1990

[2] 技術開発室, "ザ プロテクト 3、上・下", 秀和トレーディング, 1992