ソフトウェアの権利保護のための個人認証プロトコル

5U-7

---モラル向上効果を持つ認証プロトコル---

小林俾史（埼玉工業大学），山本和明(IPA)

論文要旨

パーソナルコンピュータにおいて，ソフトウェアの権利保護は社会的にも技術的にも大きな問題であるが，技術的な対策は非常に難しく効果も十分でない．最終的にはソフトウェアなどの知的生産物（無体財産）に対する社会的な評価の形成や個人のモラルの向上を待つほかないというのが現実である．

本稿では，ソフトウェアの権利保護のための個人認証プロトコルを提案する．このプロトコルは，簡易なハードウェアに基礎をおいたソフトウェアによる個人認証を行うもので，非常に広汎な分野に適用可能である．従来は技術的な対策では困難であると見られていたソフトウェア（知的財産）に対するモラルの向上を図るという重要な副次効果を期待できる．

1．はじめに

パーソナルコンピュータにおいてソフトウェアの権利保護は非常に大きな問題であり，技術的対策である保護方式をめぐって様々な立場の対立が激しく，その解決は不可能のように見える［1］．情報処理振興事業協会技術センターでは，昭和60年度に面接調査を中心に広範な対象の実態調査を行った［2］，［3］．簡単にまとめると，現在採用されている保護方式はかえって問題の解決には多くの課題を生み出すという結果になっており，事態をむしろ混乱させる結果に終わっていると言えよう．ソフトウェアの権利保護の問題の本質は，＜守る＞技術対策という問題というより，むしろ守る対象＝ソフトウェアの質が問題であるといえる．つまり，守るに値するソフトウェアの質，サービスの内容そのものが本質的な問題であり，その本質を回避したところで技術対策や法的な対策を先行させたところに事態を紛糾させた原因があると想定される．したがって，この問題の解決策は必ずしも一つの方式を採用すれば解決できるといった単純なものではなく，当面は保護対策を構じる側の要求（費用と強度）に応じたさまざまな対策が当面要請されているといえよう．

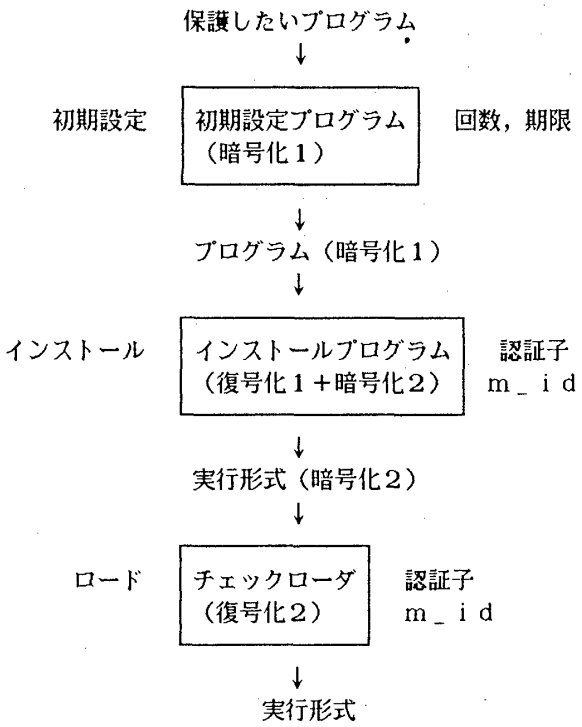
パーソナルコンピュータのソフトウェアは，まだビジネスとして未熟な段階にあり，ソフトウェアに関する社会習慣や通念，モラルなどの未形成な段階にある．そこで本稿では，モラル形成によい効果を持つ認証プロトコルを提案する．

2．システムの概要

本システム「ユーザ認証システムＵＡＭＩＳ」は，プログラムの権利保護を行う手法としてプログラムの実行時にユーザの認証を行うものであり，認証されたユーザが特定の計算機でのみ使用できるという目的を実現する．ＵＡＭＩＳは，「ユーザ認証およびモラル向上型システム（User Authentication and Moral Improvement System）」の略である．

本システムは，まず保護したいプログラムに対して使用回数と使用期限の制約条件を組み込む初期設定ができる．そのプログラムをインストールするときに，ユーザ固有の認証子と計算機の番号を元に一方向性関数で鍵を作成し，その鍵で暗号化してＯＳに組み込む．実行時は，その認証子をチェックし計算機の番号と併用して鍵を作成し，復号化する．このときに用いられる暗号系は共通鍵暗号である．

システムの概要を図示すると次のようになる．



（注）ｍ＿ｉｄは，計算機固有の番号を表す．

User Authentication Protocol for Software Protection
Hitoshi Kobayashi, Kazuaki Yamamoto
Saitama Institute of Technology, Information-Technology Promotion Agency

２．システムの機能

本プログラムは次の４つのプログラムから構成される．

１）初期設定プログラム
２）インストールプログラム（組み込みプログラム）
３）チェックローダ
４）ユーティリティ

３．１　初期設定プログラム

プログラムは，作成時に簡単な暗号化を施して流通させる．初期設定プログラムにより，保護したいプログラムは使用回数，使用期限などの制約条件をプログラムに組み込める．プログラムはインストールプログラムによってＯＳに組み込まないかぎり，直接は実行できないように「トラップ（罠）」をしかけてある．

３．２　インストールプログラム

インストールプログラムでは，まず与えられたユーザ名などの識別子と計算機固有の番号（製造番号）から，一方向性関数を元に内部でのみ使用する鍵を生成する．この鍵を使って保護するプログラムを暗号化し，ＯＳに組み込む．この暗号化によって特定の計算機の上でのみ動作し，かつユーザの識別子が一致した場合のみ動作することが保証される．

３．３　チェックローダ

チェックローダはユーザ認証を行い，かつ内部で認証子と計算機固有の番号から一方向性関数を用いて解読の鍵を生成する．その鍵を用いてプログラムを復号化しながらロードして実行する．このチェックローダは，認証ができた段階で使用回数の更新や有効期限の確認を行う．

３．４　ユーティリティ

ユーティリティは，使用回数や有効期限の表示，変更などを行う．このユーティリティはプログラムを保護する立場で用いられるもので，通常のユーザが使用するものではない．

４．システムの特長

本システムでは，特定のユーザが特定の計算機においてのみプログラムを実行できる，という保護を行う．このシステムでは，まず使用回数や使用期間などの制約条件を組み込めること，特定の計算機においてのみ実行できるという最も厳しい保護形態を実現する．ただしこれらの制約条件は使用する目的に応じて緩和することができる．要約すると，この認証手順の特長は使用回数の制約，使用期限の制限を組み込むということだけでなく，使用するユーザを制限し，また実行できる計算機をも制限することが可能である．これらの制限のすべてを実際に用いる必要はなく，選択的に用いることもできる．さらに認証子として名前を用いることにより，不正にコピーされたプログラムを使うときに他人の名前を用いなければならないという制限のため，他の人にこの認証の過程を「見られることは恥しい」という意味で，モラルを刺激できる効果を持たせられる．

５．今後の課題

本システムの中心となるアルゴリズムは，以下の三点である．本システムは現在開発中であり，妥当なスピードと強度について評価を行う予定である．

［認証のための一方向性関数］

一方向性関数としては，１）鍵を固定したＤＥＳアルゴリズム，２）ハッシング関数，３）指数関数（離散的対数問題に帰着）の三種類を作成し，処理時間を比較する．

［共通鍵暗号系］

暗号化１および暗号化２の暗号系としては，次のものを扱う．１）排他的論理和，２）多表式暗号，３）ＤＥＳ暗号の三種類を作成し，処理時間の比較を行う．

暗号化は簡単な（処理速度が現実的な）もの使用する．

［モラルを刺激する方法］

いずれにしても技術的な対策として，保護技術は必ずしも一律に対処することは，現時点では困難である．しかも社会的なコンセンサスを形成する方向でこのモラル向上の副次効果を得られるプロトコルは有望であろう．

［参考文献］

[1] 山本，松本：ソフトウェア保護システム要件解明への二つのアプローチ，情報処理振興事業協会技術センター第四回技術発表会論文集，pp.176-181(1985)．
[2] 松本，山本：ソフトウェア保護システムへの要件の分析，情報処理学会第32回全国大会 7R-6 (1986)．
[3] 情報処理振興事業協会：技術センター報告書 60-063 パーソナルコンピュータにおけるソフトウェア保護技術の動向とシステムの要件 (1986)．