耐タンパ・モバイルエージェントを実現する セキュリティ機構の提案と実装

長谷川 信 (010087)

北陸先端科学技術大学院大学 情報科学研究科

2002 年 2 月 15 日

キーワード: モバイルエージェント, セキュリティ, 耐タンパ, アーキテクチャ, アプリケーションフレームワーク.

1 本研究の背景と目的

モバイルエージェントはネットワークを通じて移動し，様々なホスト上でタスクを実行するプログラムである．このようなモバイルエージェントは通信回線の接続状況に影響されにくいといった特長を持つ．実際に携帯電話を用いた情報検索システムにモバイルエージェントを利用したものがあり，携帯電話を用いた電子商取引システムにもモバイルエージェントの利用が期待されている．しかし，その実用化にあたりモバイルエージェントのセキュリティを十分考慮する必要がある．

モバイルエージェントのセキュリティ問題は，1）不正なエージェントによるホストへの攻撃，2）不正なホストによるエージェントへの攻撃に大別される．既存の研究の多くは上記 1 の問題に対してある程度有効な解を与えているが，上記 2 の問題に関しては，概念的・理論的なアプローチに終始しているものが多く，その実用性と有効性に疑問がもたれる．しかし，モバイルエージェントのセキュリティを考慮するうえで，上記 2 の問題を避けて通るわけにはいかない．

特に，モバイルエージェントを用いて電子商取引システムなどを構築する場合，モバイルエージェントに持たせた個人情報をどのように保護するかが非常に重要な問題となる．例えば，モバイルエージェントのデータがエージェントの移動中に盗聴される可能性がある．これには通進路を暗号化することで対処できるが，モバイルエージェントが移動した後，移動先のホスト上で悪意のあるモバイルエージェントなどにデータを不正に取得・改竄される危険性もある．この問題は通進路の暗号化だけでは十分ではなく，アプリケーションレベルにおけるデータの保護機構が必要であることを示唆している．

本研究では，不正なホストによるモバイルエージェントへの攻撃，特に不正な内部解析や盗み見に対する防御機構を持つモバイルエージェント（耐タンパ・モバイルエージェン

ト）を柔軟に構成するためのアーキテクチャを提案する．本研究の目的は新しい暗号化・難読化技術の提案ではない．既存のそれらとうまく融合できるようなモバイルエージェントのアーキテクチャを設計することが最終目標であり，本研究は暗号化・難読化技術の研究と競合するものではなく，それらと相補的な関係に位置づけられる．

2 本研究のアプローチ

上記の背景をふまえて本研究では以下のアプローチをとる．

- モバイルエージェントごとにデータの保護機構（暗号・復号化）を導入
- 保護機構のモジュール化
- モバイルエージェントをメタレベル・アーキテクチャとして構成
- 保護機構の難読化
- モバイルエージェントごとにセキュリティ・ポリシを導入

アプリケーションレベルでモバイルエージェントのデータを保護するには，各モバイルエージェントがその保護機構を持つ必要がある．これにより移動先のホストに依存しない暗号化技術の利用が可能になる．

このような暗号・復号化機構などの保護機構はアプリケーションロジックから分離し独立したモジュールとして実現する．そして，モバイルエージェントはこのモジュール群からなるメタレベル，アプリケーションロジックやエージェントの基本機構などからなるベースレベルの二層構造で構成する．このようなモバイルエージェントのアーキテクチャはメタレベルの変更や再利用により，既存の暗号化技術を柔軟に取り入れ可能とする．

さらに，モジュール化した保護機構を難読化することにより，使用する暗号化方式の解析を困難にする．

また，保護すべきデータに適用するセキュリティ要件をセキュリティポリシとして定義して，各モバイルエージェントに持たせることにより，ホストに公開する情報を柔軟に変更可能とする．

3 実装

本研究では，提案したセキュリティ機構を Java ベースのアプリケーションフレームワークとして実装した．このアプリケーションフレームワークを ART と呼ぶ．そして ART を用いて電子商取引エージェントを作成し，実験を行った．アプリケーションフレームワーク ART は以下の特徴を持つ．

- メタレベル（暗号・復号化モジュール）の柔軟な変更が可能

- 暗号方式として単純なシーザー暗号，BASE64 エンコード方式にもとづく暗号アルゴリズムなどを提供
- 難読化機能としてマルチスレッド化したダミー処理を実現
- セキュリティ・ポリシを外部ファイルとして取り込み可能
- メタレベルとセキュリティ・ポリシを管理するセキュリティマネージャを提供
- 複数の巡回パターンを提供

ART はメタレベルとベースレベルを実現する Java のクラスライブラリからなる．メタレベルはセキュリティ機構を実現するクラス群から構成され，ベースレベルは電子商取引を実現するクラス群から構成される．メタレベルのセキュリティマネージャはセキュリティ・ポリシにもとづき，ベースレベルを暗号・復号化する．ART は既存の暗号化方式を実現するメタレベル・モジュールを複数提供し，これらは柔軟な変更が可能である．

このような ART を用いて作成された電子商取引エージェントは携帯端末などのユーザのホストを出発後，セキュリティマネージャにより秘密情報を暗号・復号化しながら仮想店舗を巡回し，ユーザの代わりに情報収集・電子決済などを行う．実験ではこのようなエージェントの暗号アルゴリズムやセキュリティ・ポリシを変更し，その動作を確かめた．

この実験により，本研究で提案したセキュリティ機構がその柔軟な変更や再利用を可能とすることを示した．こうした ART を用いることで，既存のモバイルエージェントにセキュリティ機構を容易に付加することが可能となる．

4 まとめ

本研究では，耐タンパ・モバイルエージェントを柔軟に構成するためのアーキテクチャを提案し，そのセキュリティ機構を Java ベースのアプリケーションフレームワーク ART として実装した．さらに，ART を用いて電子商取引エージェントを作成し，実験を行った．この実験から提案したアーキテクチャの柔軟性を確認した．

今後の課題としては以下が考えられる．

- セキュリティポリシの記述形式
  本研究では非常に単純な記述形式のセキュリティポリシを用いている．しかし，より柔軟なセキュリティ機構を実現するためには，セキュリティポリシの記述形式について考慮する必要がある．
- セキュリティ機構の難読化技術
  ART で用いた難読化技術は実装が容易で単純なものである．しかし，本研究のセキュリティ機構をより実用的なものにするには，より複雑な難読化技術を用いる必要がある．