モバイルエージェントの セキュリティに関する研究

能登研究室　　渡部彩（26083）

1　はじめに

現在エージェント技術は、コンピュータとネットワークインフラを柔軟に融合する技術として、主にビジネス分野への応用研究を中心に実用化が進められている。

本研究では、次世代の通信パラダイムとして注目を集めているモバイルエージェントの仕組み・現状を理解し、不正なアクセスからモバイルエージェントを保護することを考える。ここでの主なセキュリティの方法として、アクセス制限、暗号化・復号化のシステムを中心にして考える。

2　モバイルエージェント

モバイルエージェントとは、コンピュータ間を移動しながら計算処理を継続していく自律的なプログラムで、プログラムのコードとプログラムの実行状態が一緒に移動先に転送されるソフトウェアである。主な特徴として以下の 5 つが挙げられる。

- 自律性：外部からデータを取り入れ、内部の状態に従って、各自の意思決定機構に沿って行動する
- 協調性：互いに通信し、情報を交換し合うことによって、協調的に動作する
- 適応性：外部の環境の変化に追随し、適切な行動規則やインタフェースを用いて処理を行う
- 移動性：ネットワーク上のホスト間を移動しながら処理を行う
- 局所性：システム全体の情報を持つことはなく、局所的な情報のみで動作する

3　モバイルエージェントの攻撃・防御

エージェントが移動先のホスト上で不正な処理を実行したり、また逆に、移動先のホストでエージェントが攻撃されることも考えられる。そこでモバイルエージェントのセキュリティとして、以下の 2 つが挙げられる。

不正なエージェントによるホストへの攻撃・防御

- 情報の盗み見、ファイルへの不正使用や削除などの攻撃
- 情報の暗号化、アクセス制御などの対策

不正なホストによるエージェントへの攻撃・防御

- 情報を盗み見、コード・データを改竄するなどの攻撃
- 情報の暗号化、秘密情報を持たせないなどの対策

4　提案するシステム

本研究では、主に不正なシステムからモバイルエージェントを保護するプログラムを考えるために、まずそれぞれ移動先のホストから攻撃を受けないようにモバイルエージェントでアクセス許可を交渉するシステムを考える。次にアクセス可能になったら、モバイルエージェントに秘密情報を持たせる。この時に秘密情報を鍵 A によって暗号化する。移動後に鍵 B によって復号化し、秘密情報が見れるようにする。流れを図 1 に示す。

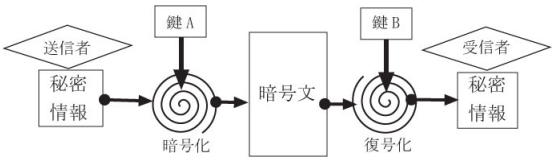

図 1: 暗号化・復号化の流れ

5　シミュレーション

本研究では、まずモバイルエージェントのセキュリティで不可欠な暗号化・復号化の流れに関して，簡単なプログラムを C 言語により作成し、シミュレーションした。方法・結果を以下に示す。

5.1　暗号化・復号化

暗号化

まずパスワード（ローマ字の大小文字のみ）を入力し数字に置き換える。これをパスキーと呼ぶ。次に情報文（ローマ字の大小文字のみ）を入力し数字に置き換える。これを情報キーと呼ぶ。この 2 つのキーを利用して、暗号化の処理を行う。暗号化の処理方法は、パスキーを情報キーにランダムに足していき、足した結果を暗号文とし、出力する。

復号化

まず暗号化した文を入力し、パスワードによって元の情報文に戻るようにする。復号化の処理方法は、暗号文をパスキーで引いていく。引いた結果が情報キーと同じになるので、それを元の情報文に戻す。

問題点として、違うパスワードを入力しても情報文が出るが、元の情報文と異なったものになるため、パスワードが違うときには、エラー文が出るように修正する必要がある。

5.2　モバイルエージェントへの適用

暗号化・復号化の 2 つをモバイルエージェント内に持たせ、移動先との交渉でアクセス可能とする。

結果として、まずモバイルエージェントが移動先とのアクセスを交渉成立させ、移動先で攻撃を受けないようにする。次に移動前に、パスキーを「berry」、情報文を「MobileAgentSecurity」と入力し、暗号文を出力する。暗号文は「412020273707322523392250232146201438 43」とランダムな数字に変換される。移動後、パスキーと暗号文を入力する。暗号文が元の情報文に出力できた。

6　おわりに

より発展した暗号化・復号化のシステムは、秘密鍵・公開鍵が必要である。本研究では、このシステムを知る前に暗号化・復号化の流れを理解するために、独自で簡単なシミュレーションをした。

今後の課題として、移動中に秘密情報を奪うことが可能かどうかシミュレーションする。仮に奪えたとしても秘密情報を見られなければよい。既存するモバイルエージェントのセキュリティを調べて比較し、問題点を改善するシステムを考察する必要がある。