不正なホストの盗み見からモバイルエージェントを保護するセキュリティ機構の提案と実装

村田 真一

北陸先端科学技術大学院大学 情報科学研究科

2001 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, アプリケーションフレームワーク, 電子商取引, セキュリティポリシー, 不正なホスト.

1 セキュリティ問題

本研究の目的は，不正なホストの盗み見からモバイルエージェントを守るためのセキュリティ機構を考案し，それをアプリケーションフレームワークとして実現することにある．モバイルエージェントとは，ネットワーク上のホスト間を移動し，移動先のホスト上でタスクを実行するプログラムである．モバイルエージェントは，プログラムの内部状態を保持したままホスト間を移動できるため，柔軟なアプリケーションの作成が可能である．しかし，モバイルエージェントを実用的なシステムで使用するためには，信頼性とセキュリティの問題を解決しなければならない．このうちセキュリティの問題は，1) 不正なエージェントが移動先のホストを攻撃する問題，2) 不正なホストがエージェントを攻撃する問題に分けることができる．既存のモバイルエージェントシステムでは，1) を考慮しているものはあるが，2) に対する有効な対処手法は確立されていない．2) のセキュリティ脅威としては，盗み見や改竄などの攻撃が想定されるが，本研究では，エージェントの秘密情報が不正なホストにより盗み見される問題を扱う．

モバイルエージェントの適用分野として期待されているものの１つに電子商取引がある．電子商取引にモバイルエージェントを用いれば，エージェントがユーザの代わりに情報収集，電子決済，価格交渉などを行うことが可能である．しかし，決済情報や個人情報などをモバイルエージェントに持たせると，これらの秘密情報が不正なホストにより盗み見される危険性がある．このため，電子商取引では，不正なホストの盗み見に対処することが重要である．本研究では，モバイルエージェントのアプリケーションとして，ネット

ワーク上の仮想店舗を巡回してユーザの代わりに電子商取引を行うエージェント（電子商取引エージェント）を対象とする．

2　本研究のセキュリティ機構

既に，不正なホストのセキュリティ脅威に対するモバイルエージェントのセキュリティ手法が幾つか提案されているが，盗み見の脅威に対する有効な対処手法は確立されていない．これは，モバイルエージェントが移動先のホスト上で実行されるためであり，移動先のホストは，エージェントのプログラムコードやインスタンス変数の値などを知る必要がある．ユーザがエージェントの情報を暗号化したとしても，移動先のホストがそれを復号化できなければならないため，盗み見には対処できない．このため，本研究では，エージェントの秘密情報をエージェント本体と分離し，秘密情報へのアクセスを制限することで盗み見に対処する．ユーザのホスト上で秘密情報を管理するエージェントを秘密情報管理エージェント，秘密情報を持たずにネットワーク上を巡回するエージェントを巡回エージェントと呼ぶ．巡回エージェントは，決済時などの秘密情報が必要になった時点で秘密情報管理エージェントに要求を送る．秘密情報管理エージェントはその要求を受け取り，アクセス権を持つ巡回エージェントだけに秘密情報を返す．秘密情報へのアクセス権は，以下の項目によって判別される．

- 巡回エージェントが実行されている移動先のホスト
- 巡回エージェントが通信している仮想店舗の識別子
- 巡回エージェントの実行フェーズ
- アクセスの種類
- 巡回エージェントの識別子

3　アプリケーションフレームワーク

提案するセキュリティ機構では，巡回エージェントが秘密情報を持たずにネットワーク上を巡回するため，不正なホストは秘密情報を盗み見することができない．しかし，巡回エージェントは，秘密情報が必要になる度に秘密情報管理エージェントに要求を送る必要がある．また，秘密情報管理エージェントは，秘密情報へのアクセス権を持つ巡回エージェントを見分けなければならない．更に，これらのエージェント間のネットワーク通信は，暗号化プロトコルなどを用いて安全に行われなければならない．このため，エージェントのプログラムコードは煩雑になり易く，セキュリティ機能を正しく実装することは難しい．本研究では，この問題に対処するために，セキュリティ機構を電子商取引エージェントのアプリケーションフレームワークとして実現した．アプリケーションフレームワー

クを用いることにより，盗み見に対するセキュリティ機能を持った電子商取引エージェントを容易に作成できる．アプリケーションフレームワークは，電子商取引エージェントの雛型，セキュリティマネージャ機能，データストア機能，セキュリティ機能のクラスライブラリから構成される．エージェントの雛型には，セキュリティ機構やネットワーク上の巡回パターンが組み込まれている．セキュリティマネージャとは，秘密情報管理エージェントに組み込まれ，巡回エージェントからの要求が正しいアクセス権を持っているかどうかを監視する機能である．データストアとは，巡回エージェントに組み込まれ，秘密情報管理エージェントとのセキュアなエージェント間通信をサポートする機能である．これらのセキュリティ機能は，雛型クラスを継承することで，それぞれの電子商取引エージェントに組み込まれる．

電子商取引エージェントの秘密情報を守るためには，情報の公開先，情報の保護手法の２つのセキュリティ要件を考慮する必要がある．この２つのセキュリティ要件の組み合わせは，秘密情報毎に異なり，また，アプリケーションの処理内容や利用方法にも依存する．このため，アプリケーションフレームワークでは，秘密情報毎に適用するセキュリティ要件をセキュリティポリシーとして外部ファイルに XML を用いて定義する．これにより，セキュリティ機構の柔軟な設定およびカスタマイズが可能になる．

4　実験・考察

実装したアプリケーションフレームワークを用いて，３つの電子商取引エージェントの例題アプリケーションを作成した．この例題アプリケーションは，それぞれが異なるネットワーク上の巡回パターンを実装したものである．保護すべき秘密情報は巡回パターン毎に異なり，また，秘密情報毎に保護手法が異なるため，３つの例題はそれぞれ異なる秘密情報を異なる手法で保護している．本アプリケーションフレームワークを用いることで，異なる巡回パターンを持つ電子商取引エージェントを容易に作成でき，アプリケーション毎に異なる秘密情報を少ないコード量で不正なホストの盗み見から保護できた．今後の課題としては，改竄などの盗み見以外のセキュリティ問題への対応や，電子商取引以外の分野への応用が挙げられる．