6G-6　モバイルエージェントのセキュリティ機構フレームワーク*

村田真一†　渡部卓雄††　天野憲樹††

†北陸先端科学技術大学院大学 / (株)富士通北陸システムズ

††北陸先端科学技術大学院大学

1 はじめに

本研究の目的は，不正なホスト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のセキュリティ問題には，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がある[1]．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)は考慮されていない[2]．このため，エージェントの情報が，移動先のホストにより盗み見，改竄される危険性がある．

本研究では，ネットワーク上の複数のホストを巡回する Java ベースの電子商取引エージェントを対象とする．そのためのセキュリティ機構を，クラスライブラリ，巡回パターン，セキュリティマネージャ等からなるアプリケーションフレームワークとして実現する．セキュリティ機構では，不正なホストの攻撃のうち，電子商取引エージェントが保持する情報（価格情報，個人情報，電子決済情報等）が盗み見されることを防ぐ．提案するフレームワークを用いることにより，エージェントへのセキュリティ機構の組み込みが容易になる．また，エージェントのアプリケーションロジックとセキュリティに関するコードを分離でき，セキュリティポリシーの柔軟な設定，変更も可能となる．

2 想定する巡回パターン

ネットワーク上の仮想店舗と電子商取引を行うモバイルエージェント（電子商取引エージェント）を考える．電子商取引エージェントは，エージェントを生成したユーザのホストを出発した後，複数の仮想店舗を巡回し，ユーザの代わりに，商品リストの獲得，価格交渉，電子決済処理を行う．本研究では，電子商取引エージェントをネットワーク上の巡回パターンで以下のように分類する．

1. 巡回後決済エージェント
2. 巡回中決済エージェント
3. 巡回交渉エージェント

巡回後決済エージェントは，巡回により各店舗の情報を入手した後で一旦ユーザのホストに戻り，次に巡回済の店舗から決済対象を決定し，決済に向う．巡回中決済エージェントは，巡回中に目的の店舗が見つかった時点で決済を行う．巡回交渉エージェントは，巡回により各店舗の情報を入手した後で一旦ユーザのホストに戻り，次に巡回済の店舗から交渉対象を決定し，交渉に向かう．これらの巡回パターンは，フレームワークの一部として実現する．

3 セキュリティ機構

電子商取引エージェントの巡回パターンごとにセキュリティ要件を整理し，各パターンに必要なセキュリティ機能をフレームワークとして実現する．また，保護対象となるエージェントの秘密情報にはセキュリティポリシーを定義し，フレームワークにセキュリティポリシーの監視機能を設けることで，セキュアな電子商取引エージェントを実現する．

3.1 セキュリティ要件

複数のホストを巡回する電子商取引エージェントでは，不正なホストの盗み見に対し，次の２つのセキュリティ要件を考慮しなければならない．

1. ネットワーク上のどのホストに情報を公開するか
2. どの様な手法で情報を保護するか

要件１については，電子商取引エージェントが保持する情報を，以下のように分けて考える．

---

*Towards a Security Framework for Mobile Agents against Malicious Hosts

†Shinichi MURATA, smurata@jaist.ac.jp / s-murata@fjh.se.fujitsu.co.jp, JAIST / FUJITSU HOKURIKU SYSTEMS LIMITED

††Takuo WATANABE,Noriki AMANO, {takuo,n-amano}@jaist.ac.jp, JAIST

- 全てのホストに公開する情報
- 特定のホスト（仮想店舗）にだけ公開する情報
- 仮想店舗以外の，特定のホストにだけ公開する情報
- エージェントを作成したユーザのホスト以外は，全てのホストに対して秘密にすべき情報

要件2は，電子商取引エージェントが保持する情報を特定のホストにだけ公開するための手法であり，以下の手法に分けて考える．

- エージェントの生成者と移動先のホストとで共有する共通鍵で暗号化
- 移動先のホストの公開鍵で暗号化
- SET プロトコルを応用する

これら2つのセキュリティ要件の組み合わせは，保護対象であるエージェントの秘密情報ごとに適用すべきものが異なる．また，エージェントの処理内容や利用方法にも依存するため，セキュリティ機構は柔軟なカスタマイズが可能でなければならない．

3.2 秘密情報の保護手法

電子商取引エージェントが電子決済に必要な秘密情報を保持してネットワーク上を巡回すると，不正なホストにより秘密情報を盗み見されてしまう危険性がある．このため本研究では，電子商取引エージェントの機能を，ネットワーク巡回機能，秘密情報管理機能の2つに分け，それぞれを巡回エージェント，秘密情報管理エージェントとして分離することにより，不正なホストの盗み見に対処する．巡回エージェントは，ネットワーク上の複数の仮想店舗を巡回するが，秘密情報管理エージェントは，ユーザのホストに留まり移動しない．図1に示す様に，巡回エージェントは，仮想店舗のあるホストに移動した後，決済を行う時点で，秘密情報管理エージェントに秘密情報を依頼する．秘密情報管理エージェントは，要求された秘密情報に暗号化等の適切な処理を施し，巡回エージェントに送る．このエージェント間通信は，フレームワークによって秘密情報管理エージェントに組み込まれるセキュリティマネージャを経由する．セキュリティマネージャは，秘密情報アクセスに関するエージェント間通信が，ポリシーファイルから読み込んだセキュリティポリシーに違反しないことを監視する．

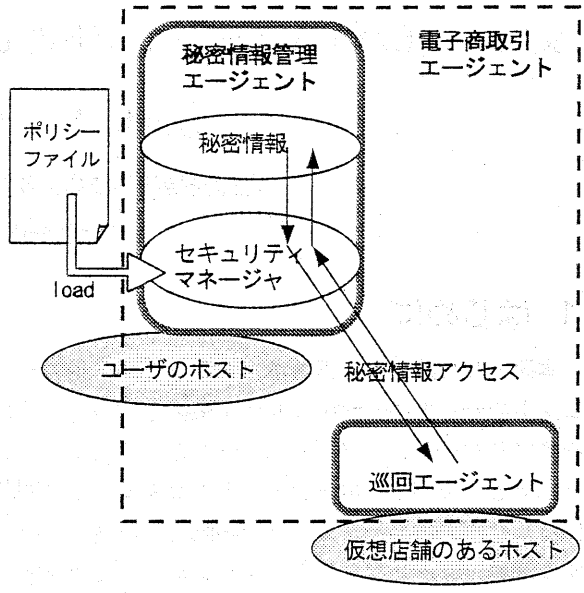

図1秘密情報の保護機構

3.3 セキュリティポリシー

本研究では，秘密情報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，外部のポリシーファイルに定義する．これにより，セキュリティポリシーに関する記述をエージェントのアプリケーションロジックと分離する．

ポリシーファイルには，保護対象となる秘密情報の識別子と，その情報に適用するセキュリティポリシーの組み合わせを記述する．秘密情報ごとにセキュリティポリシーを設定することでポリシーの柔軟な設定が可能であり，ポリシーファイルの内容を変更することで，エージェントの処理内容や利用方法に合わせてセキュリティポリシーをカスタマイズできる．

4 今後の方針

本研究の今後の方針であるが，1)ポリシーファイルに定義するセキュリティポリシーの記述方法，および 2)セキュリティマネージャの詳細についてそれぞれ検討し，プロトタイプの実装，評価を行う．

参考文献

[1] David M. Chess.:Security Issues in Mobile Code Systems, Lecture Notes in Computer Science Vol.1419,Springer(1998), p.1-14.

[2]本位田真一，飯島正，大須賀昭彦.:エージェント技術，共立出版，1999.