6G−2

不正なホストの攻撃に対処するモバイルエージェントのセキュリティ機構*

長谷川 信†　天野 憲樹†　二木 厚吉†

北陸先端科学技術大学院大学 情報科学研究科‡

1 はじめに

近年注目されているモバイルエージェントは，携帯端末との連携によるモバイルバンキングなどに利用が期待されているが，その実用化にあたりセキュリティ問題が最大の障害となる．このようなモバイルエージェントのセキュリティ問題は大別すると，不正なエージェントによるホストへの攻撃と不正なホストによるエージェントへの攻撃がある [1].

本研究では，モバイルエージェントの自律性を活かした**柔軟な自己暗号・復号化**により不正なホストの攻撃からエージェントの情報を保護するセキュリティ機構を提案する．

2 背景

モバイルエージェントはその実行環境を提供するホストから，盗み見，内部解析，改竄などの攻撃を受ける可能性がある [2].

これらの攻撃に対する代表的なセキュリティ技術として，エージェントの情報を**暗号鍵**と呼ばれるパラメータを用いて暗号化する技術がある．この技術には，**秘密鍵暗号方式**と**公開鍵暗号方式**の2種類があり，前者は鍵の安全な配送の問題，後者は暗号・復号化の計算負荷が大きくなるといった問題がある．

モバイルエージェントは，ネットワーク上の複数のホストを巡回すると考えられる．このとき，モバイルエージェントに実行環境を提供するホストは，計算資源が豊富なサーバやワークステーションだけではなく，リソースが制限される携帯端末なども考えられる．また，エージェントの持つ情報は，全てのホストに公開するものとは限らない．

モバイルエージェントと携帯端末の連携によるモバイルバンキングなど，商用ベースの実用に耐え得るモバイルエージェントの実現には，計算負荷が小さく，ホストの信用度に応じた柔軟なセキュリティ機構が求められる．

3 本研究のアプローチ

このような背景をふまえて本研究では，以下のアプローチにより不正なホストによる盗み見や内部解析といった攻撃から，エージェントの持つ秘密情報の保護を実現する．

- モバイルエージェントに暗号・復号化機構を導入
- エージェントのセキュリティポリシに基づく秘密情報の柔軟な自己暗号・復号化

モバイルエージェント自身が暗号・復号化機構を内蔵することにより，移動先のホストに依存しない暗号技術が利用できるといった利点が得られる．つまり比較的計算負荷が小さい暗号アルゴリズムを使用することができる．しかし，暗号方式が知られてしまうと，簡単に復号化されてしまうという問題がある．これについては，3.2節で述べる．

また，エージェントの持つセキュリティポリシに基づき，暗号・復号化する秘密情報を柔軟に選択することで，必要な秘密情報だけの公開が可能になる．このように，必要な秘密情報だけを暗号・復号化する方式は計算負荷の減少につながる．

3.1 モバイルエージェントの構成

本研究では，ベースレベルとメタレベルからなる二層構造で，モバイルエージェントを構成する（図1）．

ベースレベルは，移動機構，アプリケーションロジックなどから構成される．一方メタレベルは，暗

---

*A Security Mechanism of Mobile Agents against Attack of Malicious Hosts

†Makoto HASEGAWA(makoto-h@jaist.ac.jp), Noriki AMANO,Kokichi FUTATUGI

‡School of Information Science, Japan Advanced Institute of Science and Technology

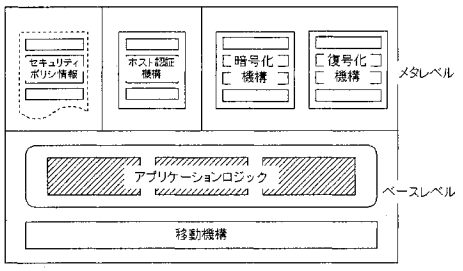

図 1: モバイルエージェントの構成

号・復号化機構，ホスト認証機構，セキュリティポリシ情報などから構成する．

このような二層構造でモバイルエージェントを実現することにより，メタレベルの柔軟な変更や再利用が可能となる．

3.2 暗号・復号化機構の難読化

秘密情報は，暗号方式を知られてしまうと簡単に復号化されてしまう．そこで，メタレベルの暗号・復号化機構は，移動先のホストに解析されないように難読化する必要がある．同様に，ホスト認証機構，セキュリティポリシ情報なども難読化する．

本研究で用いる難読化手法は以下である．

- メタレベルの機構はセルと呼ぶ実行可能な最小単位のモジュールに分割
- 時間軸と空間軸の両方にセルを分散
- セルのインタリーブおよびマルチスレッド化
- ダミーセルの挿入

具体的には，難読化するメタレベルを複数のセルに分割し，主記憶のアドレスのなかに分散配置する．ダミーセルを含む複数のセルはマルチスレッド化しインタリーブして実行する．

3.3 セキュリティポリシに基づく柔軟な自己暗号・復号化

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として定義し，モバイルエージェントに内蔵させる．

セキュリティポリシには，

- 秘密情報とその重要度
- 巡回対象のホスト情報とその信頼度

このホストの信頼度と秘密情報の重要度に基づき，エージェントは秘密情報を柔軟に暗号・復号化する．

4 モバイルエージェントの動作

本研究で提案したセキュリティ機構を備えたモバイルエージェントの一連の動作は以下のようになる．

- ユーザのホスト上で，秘密情報を暗号化し移動する．
- 移動先のホストに対し認証を行う．認証に失敗した場合次のホストに移動し，成功した場合ホストに秘密情報を開示．
- ホストが要求する秘密情報がセキュリティポリシに合致するなら，要求された秘密情報だけ復号化し，目的となる処理を実行する．合致しない場合は次のホストに移動する．
- 処理の終了とともに，再び秘密情報を暗号化し，次のホストに移動する．

5 まとめと今後の予定

本研究では，柔軟な自己暗号・復号化により不正なホストの攻撃に対処するモバイルエージェントのセキュリティ機構を提案した．

また，本研究で提案したセキュリティ機構を，JAVA ベースのモバイルエージェントシステム AgentSpace[3] 上に実装し，モバイルバンキングエージェントなどの作成を予定している．

参考文献

[1] David M. Chess.:Security Issues in Mobile Code System, LNCS 1419, Springer(1998), p.1-14.

[2] 岩井俊弥, 栗山健, 文武, 溝口文雄.:耐タンパ・移動エージェントの調査研究, 第 18 回 IPA 技術発表会, 1999.

[3] 佐藤一郎.:AgentSpace 高階モーバイルエージェントシステム, 電子情報通信学会技術研究報告, Vol 97, No627, pages41-48, 電子情報通信学会,1998.