6G－2

移動型プログラムを用いた分散システム管理における セキュリティ機構の設計と試作

松永 繁樹＊　石田 慶樹＊＊　牛島 和夫＊

＊ 九州大学大学院システム情報科学研究科　＊＊ 九州大学大型計算機センター

1. はじめに

現在、ネットワーク環境における新しいプログラムとして、移動型プログラムの研究が進んでいる。これはネットワークを経由して目的の計算機に移動し、指示されている作業をその計算機の資源だけを用いて行うプログラムであり、モバイルエージェントとも呼ばれている[1]。現在まで移動型プログラムの応用として、分散した計算機システムの管理作業支援を考え、研究を進めている[2]。

移動型プログラム処理系を様々な分野で応用し利用していくには、移動型プログラム固有の危険性を回避するためのセキュリティ機構が必要である。既存の移動型プログラム処理系では、セキュリティ機構が未実装であったり、利用者自身による導入に依存している。本研究では、移動型プログラム固有の危険性を明らかにし、それぞれの危険性について分類を行った。次に、危険性回避に必要なセキュリティ機構の設計を行い、我々の研究室で研究開発を行っている移動型プログラム処理系 MaLio に実装した。

2. 移動型プログラム

2.1 性質

移動型プログラムは次の性質を持つ。

移動性: 目的の計算機に、作業に必要な情報を持って移動し、その計算機上の資源を用いて作業を行う。

自律性: 様々な情報を判断し行動することができる。

協調性: 相互に通信し、情報を交換しながら作業することができる。

2.2 MaLio

我々の研究室で研究開発を行っている移動型プログラム処理系 MaLio(MAlio is reLocatable and Interchangeable Object system)[3] の概要を述べる。

MaLio は、Java 言語を用いて実装した。Java 言語はプラットフォーム非依存のアプリケーションを開発可能である。分散した計算機システムには様々な機種の計算機が接続されており、管理作業支援への応用を考える場合、この Java 言語の特徴は有効である。

MaLio は、移動部・管理部・実行部から構成される。

移動部 行わせたい作業毎に作成する部分。作成者はそれぞれの目的に合わせ、作業内容・作業対象・判断基準の3つを記述し、移動部の基本クラスを継承させて移動部をインスタンスとして作成する。動作中は次の2種類の情報を所持し、計算機間を移動する。

- 作業を行うに当たって必要なデータ
- 内部状態 (実行時の変数や得られた結果)

管理部 作成者から受け取った移動部を実行部に渡し、実際に作業を開始させる部分。作成者の計算機にだけ置く。

実行部 被作業対象となる計算機にあらかじめ置いておく部分。移動してきた移動部を受け入れ、移動部に記述されている作業内容を逐次解釈して実行する。

3. 移動型プログラム特有の危険性とその分類

移動型プログラムを悪用した攻撃は、移動型プログラムの特徴をもとに4つに分類できる。

①ネットワーク上を移動するという特徴を悪用した攻撃

- 移動部の改竄: ネットワーク上を移動中の移動部が、"攻撃を行うもの"に改竄される危険性がある。
- 移動部の破壊: ネットワーク上を移動中の移動部が破壊され、作業が妨害される危険性がある。
- 発信元の詐称: 攻撃者が移動部を作成し、発信元をその計算機システムの管理者だと偽ることにより、攻撃を行う移動部を侵入させる危険性がある。
- リプレイ攻撃: ある計算機へ移動している移動部を複製し、それを再送することで、同じ処理を行う移動部をその計算機に送りつけることができる。移動部が行う処理が、ある時刻に限定されるべきものであった場合、別の時刻にその処理が再度行われることとなり、障害が発生する危険性がある。

②作業対象の計算機を利用している者が移動型プログラムの異常動作に気付きにくいという特徴を悪用した攻撃

- 攻撃プログラムの作成: 計算機システムに攻撃を行う移動部が作成され、障害が引き起こされる危険性がある。
- 過負荷による使用不能: 移動部が同一の計算機に大量に進入し作業することで、計算機の資源が食い尽くされ、計算機が使用不能に陥る危険性がある。

③秘密情報を持って移動するという特徴を悪用した攻撃

- 移動部の解析: 移動部が所持する情報が盗聴され解析されることにより、秘密情報が漏洩する危険性がある。

④移動型プログラム間の相互通信能力という特徴を悪用した攻撃

- 通信の改竄: 移動型プログラムの行う通信が改竄され、移動型プログラムの作業が妨害される危険性がある。
- 通信の盗聴: 移動型プログラムの行う通信が盗聴されることにより秘密情報が漏洩する危険性がある。

Design and Trial Implementation of Security Mechanism for Distributed System Administration Using Mobile Agent.

Shigeki Matsunaga*, Yoshiki Ishida** and Kazuo Ushijima*

*Graduate School of Information Science and Electrical Engineering, Kyushu University.

**Computer Center, Kyushu University.

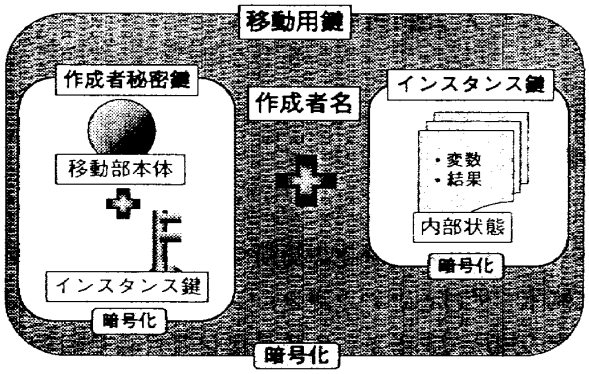

図 1: セキュリティ処理を行った移動部

4. セキュリティ機構の設計

4.1 移動型プログラムに必要なセキュリティ

3章で述べた危険性から計算機システムを守るために、次の4つのセキュリティが必要であると考える。なお、移動型プログラムを管理作業に用いるため、作業対象である計算機の安全は保障されているものとする。

移動部の認証: 発信元の詐称を防ぐために移動部の認証を行う必要がある。これにより行動制限において作成者毎の作業可能範囲を設けることもできる。

移動部の暗号化: 移動部を攻撃を行うものに書き換える改竄を防ぐために、移動部自体を暗号化する必要がある。移動部が所有する秘密情報の漏洩を防ぐためにも、移動部自体を暗号化する必要がある。

行動制限: 過負荷による使用不能に陥ることを防ぐために、移動部の受入数の制限や、負荷の生じる命令を制限する必要がある。また、攻撃を行うプログラムが動作しないよう、システムに障害をもたらす命令を制限する必要がある。リプレイ攻撃を防ぐため、指示する命令に有効期限や再実行禁止期限を設定することも必要である。

通信の暗号化: 移動型プログラムの行う通信が盗聴されることによる秘密情報の漏洩や、通信が改竄されることによる作業の妨害を防ぐため、通信の内容を暗号化する必要がある。

4.2 認証暗号機構

本節では、セキュリティ機構の中でも特に重要な認証暗号機構について説明する。管理部は移動部に次の処理(図1)を行い、移動部を実行部に渡す。

まず共通鍵暗号方式により内部状態をインスタンス鍵で暗号化する。次に移動部本体と、インスタンス鍵の2つを、公開鍵暗号方式における秘密鍵で暗号化する。最後にこれら2つの暗号化されたデータに移動部の作成者名を付け、全体を各実行部が持つ移動型プログラム用の共通鍵（以下移動用鍵とする）で暗号化する。このようにしてセキュリティ処理を行った移動部を作る。

この処理により以下の点が可能となる。

認証: 移動部本体とインスタンス鍵を作成者名から検索した公開鍵で復号化する場合、正しく復号化できるのは作成者の秘密鍵で暗号化したものに限られる。

改竄防止: 移動部は移動型プログラム鍵で暗号化されている。さらに移動部本体は作成者の秘密鍵で暗号化されているため、移動部を"攻撃を行うもの"に改竄することは困難である。

情報の保護: 移動部の作成者名を知ることはできないため、公開鍵を検索できない。このため移動部本体やインスタンス鍵を復号化することができない。移動部本体を復号化できないことから、この移動部の作業内容（命令の有効期限や再実行禁止期限も含む）や作業に必要な秘密情報を知ることはできない。インスタンス鍵を復号化することができないことから、内部状態を知ることができない。

4.3 セキュリティ機構の動作

実行部は移動部を受け入れる際に次の処理を行うことでセキュリティを確保する。

①最大数の検査: 計算機に到着している移動部の数が受入数上限を超えていないかを調べる。超えていなければ移動部を移動用鍵で復号化し受け入れる。

②公開鍵の検索: 復号化した移動部から作成者名を取り出し、その作成者名にあたる公開鍵を検索する。

③複製: 送信されてきた移動部のうち、作成者の秘密鍵で暗号化されている部分を複製する。

④認証: 移動部本体及びインスタンス鍵を②で検索した公開鍵で復号化する。正しく復号化されない場合、発信元の詐称または改竄が行われている可能性がある。

⑤作業内容の検査: 違法な命令やアクセスがないかどうか検査する。

⑥内部状態の復元: 内部状態をインスタンス鍵で復号化し、移動部の復元を完了する。

ここまでの処理で異常や違反があった場合、移動部を破棄し管理部へ報告する。

移動部の実行中は次の処理を行う。

①通信の暗号化: 移動部同士の通信や管理部との通信の内容を暗号化・復号化する。

②行動の記録: 障害発生時の責任追及のため、移動部がどのような作業をしたのか記録を残す。

移動部に記述されている作業を実行部が終え、移動部を次の目標の計算機へ送り出す際は、次の処理を行う。

① 内部状態をインスタンス鍵で暗号化する。

② 移動部を受け入れる際の処理③で複製した部分に、暗号化した内部状態と作者名とを付ける。

③ 移動用鍵で全体を暗号化する。

5. 今後の課題

今回挙げた4つの特徴に基づく攻撃に対するセキュリティ以外に必要なセキュリティがないかを考察する。なお鍵管理も考察する必要がある。また、現在未実装である部分の実装を行う予定である。

参考文献

[1] 飯田一郎, 西ヶ谷岳 :"モバイルエージェントとネットワーク", 情報処理 38 巻 1 号,PP.17-23,1997 年.

[2] 川上貴士, 石田慶樹, 古川善吾, 牛島和夫 :"自律移動型プログラムを用いた計算機管理支援の枠組について", 情報処理学会研究報告,PP.67-72,1997 年.

[3] 古閑直樹, 石田慶樹, 牛島和夫 :"広域分散環境下における移動型プログラム構築環境の実装", 情報処理学会第 56 回全国大会,1J-2,1998 年.