B-7-166

モバイルエージェントによる新しいログ管理方式の検討

A Study on a Log Management by Mobile Agents Technology

小野寺栄吉　　田中英彦
Eikichi Onodera　　Hidehiko Tanaka

情報セキュリティ大学院大学　情報セキュリティ研究科
Institute of Information Security

1. はじめに

組織やシステムのセキュリティ管理を行う上で、高度なログ管理を行うことは欠かせない。またシステムの稼働状況を適切に把握し正常な運用を進めていく上でも、ログの管理を必須である。しかしながら、現在ネットワーク環境上で提供されているサービスは多様であり、それらサービスから様々な形でのログ出力が行われていて、かつ多種多様なサーバを総合的に管理することが要求される現在のログ管理業務は、管理が複雑になりきわめて高度な知識レベルが要求される難易度が高い作業であり、簡易で高度なログ管理方式が要求されている。

本研究では、モバイルエージェント技術を適用させて、ログの管理におけるシステム管理者の負担を軽減し、かつサーバやサービスの種類・行いたい管理業務の変化などに柔軟に対応できるシステム構成を検討して提案する。

2. モバイルエージェント

モバイルエージェント（以下 MA）とは、異なるプラットホーム間をエージェントと呼ばれるプログラムが移動し、移動先でエージェントにより実行の継続を行うことができるというアーキテクチャのことである。MA に明確な定義はないが、本研究では一般に MA における特性とされる 移動性（Mobility）、自律性（Autonomous）、協調性（Cooperative）を活用したログ管理システムを提案するものである。

3. 既存ログ管理方式の概要

複数サーバを効率的に管理する既存のログ管理方式は、大きく以下の 2 種類に分類できる。

（1）ログサーバによる集中管理
　イベント発生ごとに、集中管理するサーバへログが送信される方式である。syslog などで実装されている。

（2）プログラム間通信によるリモート管理
　管理コンソールとログマネージャといった間でプログラム関通信を行い、分散するログを管理する方式。

4. 提案するログ管理方式の概要

MA のアーキテクチャをログ管理に適用することにより、MA によるログの安全な運搬、MA に備えたロジックによるログの適切なサマリ化による通信量の低減、MA にロジックを備えさせることによる様々なサービスへの動的な対応、プログラムを複数エージェントに分割し協調動作させることによるアクセス権配分の適正化などを期待することができる。これを実現させる本提案のシステム構成の構成要素としては、OS に依存しない MA の動作プラットホームとなるエージェント実行環境、ログ管理用に特化した MA、移動能力を必要としないローカルエージェントとして実際のログ入出力を行うエージェントや MA の認証手続きを行うエージェント、MA に改竄が加えられていないことを検証するための認証局、MA やローカルエージェントのロジック（クラス）が不正なものでないことを証明するためのコード証明機関などがある。また、ログ管理手順の概略は、(1)ログ管理用 MA にロジックが判断する元となるコマンドを値として持たせて、インスタンス化する。コマンドは対象となるログの選択やログからのサマリ抽出条件の設定などの機能を実現するための専用命令群である。(2)エージェント実行環境に上記インスタンスをロードし、目的のログ出力側となるサーバに送信を行う。 (3)ログ出力側サーバ上で、MA に付属する証明書を元に改竄のチェック並びにロジックのチェックを行う。(4) MA は自身が持つコマンドを解釈し、適切なログ管理用ローカルエージェントと通信を行いログの抽出などの処理を行う。(5)変更後の値に適切な証明書を添付した上で、送信元ないしは次のプラットホームへと移動を行う。という形となる。

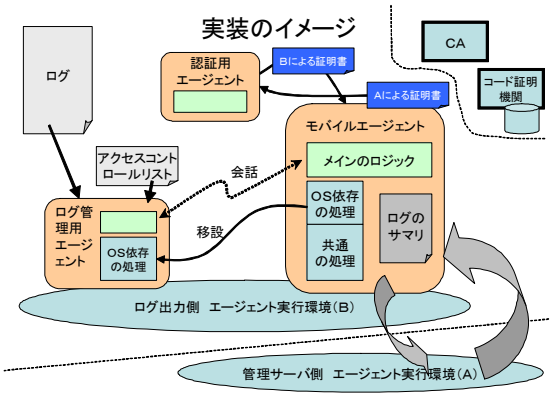

図 1　提案するログ管理システムの構成

5. まとめ

本研究では、多様な OS、多様なサービスなどに対応したログ管理を、簡易かつ高度に行うことのできるシステム構成について検討を行った。現在、提案するシステムのテスト環境として、Java 言語によるモバイルエージェントシステムを作成し、効果測定並びに評価を行っている。

参考文献

[1] The Internet Society, "The BSD syslog protocol" August 2001