6U-05

巡回エージェントによるキャンパスネットワークの管理支援*

石黒 貴純† 星野 良将† 能登 正人†

神奈川大学工学部‡

1 はじめに

21世紀のネットワーク社会を迎えるにあたって，情報セキュリティがいかに重要であるかについては，すでに言い尽くされてると言ってよいかも知れない．何か1つの対策をとって安心してしまっている場合も見受けられる．たとえば，ファイアウォールを設置して，それで情報セキュリティ対策は万全と考えている人もいると思われる．ファイアウォールは適切な設定をして，保守しなければ役には立たないし，それだけで万全と言うわけでもない[1].

現在，多くの大学において研究環境のみならず事務を含めたキャンパスネットワークの整備が進められている．本研究では巡回エージェントを用いて，キャンパスネットにおける異なったセキュリティポリシー環境において，全てのセキュリティ機能を向上させる（支援）方法を提案する．

2 セキュリティポリシー

セキュリティポリシーとは，組織内のセキュリティに関する基本的な方針や行動指針の事をいう．特にインターネットを活用している場合，セキュリティに関して配慮するのは言うまでもない．ただし，セキュリティとはある一定の状態を指すものではなく，組織によって目指すところはまちまちである．ファイアウォールでも，どのようなパケットを通過させどのようなパケットを遮断するかは，運用時に柔軟な設定が可能で，この時設定のよりどころとなるのが，その組織のセキュリティポリシーである．どのようなネットワークアプリケーションの利用を許すかといったところから，組織内のユーザをアクセス権限ごとにグループ分けするなどセキュリティ対策には，さまざまなアプローチがあり，汎用的な正解というものはない．組織が必要とするネットワークの利用法や，組織内にあるリソースの量や質，そして業務内容に影響を受けるからである．セキュリティポリシーは，こうした複雑な要素を総合的に利用して策定される．そして，これに基づいてネットワーク環境を構成する個々の要素それぞれに適切な設定を行いながら，そのポリシーを維持，運用していく．もちろん，セキュリティポリシーは不変ではありえない．新しいネットワークアプリケーションの出現や，新たなセキュリティ侵害手法の登場などを受けて，刻々変化し続けるものである．

3 キャンパスネットワーク

各キャンパス内の全学部・全事務部門をATMスイッチをバックボーンに統合し，学内全体を有機的に統合する．これにより教育・研究のあらゆる分野において情報交換をスムーズにに行える環境を提供する．ワークステーションまたはパソコンをサーバとして採用し，分散処理を行い，利用者はパソコンなどを端末としてネットワーク介し，これらに接続する．また，全学の利用者を一元統合する統合サーバを置き，利用者は1つのIDで簡単にキャンパスネットワークの全てのサービスを受けられ，インターネットなどの広域ネットワークと接続し，国内・国外の大学や研究機関との通信が可能である．

4 巡回エージェント

エージェントとは，代理人という意味で使われる用語であり，人間に代わって自律的に仕事するソフトウェアは全てエージェントと呼ぶことが可能である．エージェントを特徴づける概念としては以下のようなものがある．但し必ずしも全て揃う必要はないと考えられている[2][3].

- 自律性
  自らの目標を達成するために，自らの意思決定原理／機構に基づいて，その行動や内部状態を制御する．
- 適応性
  個々あるいは共同で，経験を通して自らの能力を高めていく．
- 協調性
  人間や他のエージェントと相互作用して，目標達成のために共同作業する．
- 運動性
  環境に対して受動的に応答するだけでなく，

*Use of Patrolling Agents in Campus Network Management Support

†Takazumi Ishiguro, Yoshimasa Hoshino and Masato Noto

‡Faculty of Engineering, Kanagawa University

目標達成に必要となる処理や作業に対して，能動的に参加する．

- 代理性
  ユーザから一定の権限を与えられ，ユーザの代理としてその権限を行使する．
- 反応性
  環境（物理世界，ユーザ，ネットワークなど）を認識し，その状態に即した振舞いや行動を行う．
- 移動性
  ネットワーク上のホストからホストへ移動できる．

これらの性質をもち，さらにWeb上を自由に動き回り巡回するシステムを巡回エージェントと呼ぶことにする．

5 サーバチェック

5.1 使用するエージェント

本研究では目的に応じ，「セキュリティチェックエージェント」と「取得エージェント」の2つのエージェントを使用する．簡単な動きを図1に示す．

- セキュリティチェックエージェント ： Web上を巡回して，サーバの検索とセキュリティチェックを行う．セキュリティのチェック項目に対して対策がたててある場合に，IPアドレスを記憶して取得エージェントに伝達する．
- 取得エージェント ： セキュリティチェックエージェントによってセキュリティが良しとされたサーバのIPアドレスを譲り受け，サーバに赴きソースコードからセキュリティの情報を取得する．

5.2 チェック項目

以下の項目についてチェックを行う．

- 管理者権限の奪取が行えるか否かのチェック
- パスワードが奪えるか否かのチェック
- 改竄等が行えるか否かのチェック
- すでに攻撃されてるか否かのチェック
- 情報が奪えるか否かのチェック

5.3 チェックの流れ

1. まず仮想サーバを構築しあらかじめセキュリティホールを作っておく．
2. セキュリティチェックエージェントでまずセキュリティチェックを行う．そこでIPアドレスを取得し，取得エージェントに送る．

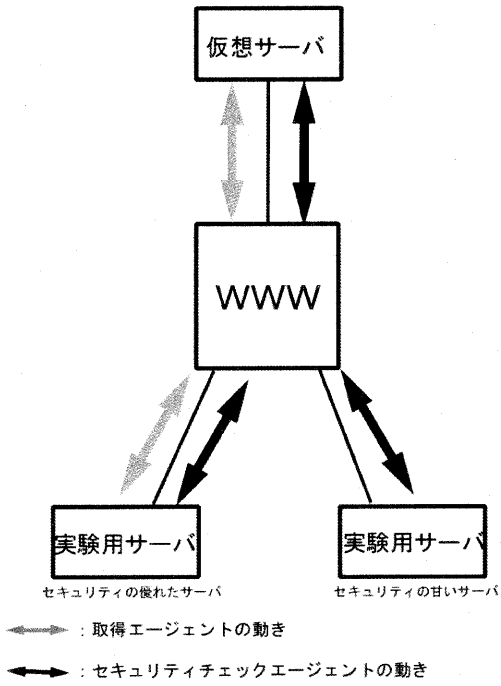

図 1: 実験の流れ

3. 取得エージェントは送られてきたIPアドレスに赴き，ソースからセキュリティコードを取得して，仮想サーバに持ち帰る．
4. 持ち帰られたセキュリティコードを仮想サーバのソースに書き込んで，新たに取得したセキュリティをサーバに組み込む．

6 おわりに

本研究では，仮想サーバをあげそれについてのセキュリティチェックを行い，仮想サーバのセキュリティの機能を向上させるための実験を行った．今後は，セキュリティの評価方法を決め，より高度なキャンパスネットワークのセキュリティ機能を確立させることが必要である．

参考文献

[1] セキュリティ研究会：インターネットセキュリティがわかる，技術評論社 (2000).

[2] 岩井俊弥：Javaモバイル・エージェント，SRC (1998).

[3] David Flanagan : JAVAプログラムクイックリファレンス，オライリー・ジャパン (1998).