2000年度日本オペレーションズ・リサーチ学会
秋季研究発表会

情報セキュリティ管理へのエージェントベースアプローチの試み

01203740 新潟国際情報大学 杉野 隆 SUGINO Takashi

1. 情報セキュリティ管理の重要性

情報ネットワークが企業活動，消費者活動のインフラになるに従い，情報ネットワークシステムの脆弱性が指摘されてきている。特に，TCP/IP にもとづく情報ネットワークシステムは，オープンシステムを特徴とするため，セキュリティ上の脆弱性を避けられない。

最近郵政省から発表された中間報告書[1]では，ネットワーク社会における脅威を，①情報ネットワークシステム，②情報システム，③社会システムそれぞれに対する脅威に分類している。①には，盗聴，改ざん・破壊，偽造が含まれ，②には利用不能攻撃，コンピュータウイルス，メール爆弾，不正アクセス，なりすまし，内部者による脅威，ホームページ改ざんなど，③にはソーシアルエンジニアリング，暴露・漏洩，プライバシ・著作権などの権利侵害を列挙している。セキュリティ被害を発生させないためのセキュリティ保護対策として，報告書では，技術的方策のみでは不十分であり，社会的側面から制度的方策，組織的対策法体系的方策を含めた総合的な対策を検討する必要があると指摘している。本発表では，この分類に従えば特に制度的方策あるいは企業組織における行動面に視点を当てて検討する。

また，去る 3 月に日本情報処理開発協会から発表された調査結果[2]をみると，情報セキュリティ管理についての問題点がいくつも浮かび上がってくる。経営理念に基づくセキュリティポリシを定めていない企業割合が 43.5%，セキュリティ管理者を定めていない企業数が 62.2%に及んでいる。また，不正アクセス対策についての従業員教育，コンピュータウイルス対策についての教育を特に実施していないという回答が 81.5%，70.0%と非常に高い。この調査は，1999 年末に実施されたものであり，本年 1 月下旬から2月にかけての中央官庁を代表に発生した不正アクセス，ホームページ改ざん事件の後の変化を捉えていないが，一時的なフィーバ後に元に戻るという日本企業の習性からすると，現在も同様に状況にあるかもしれない。

組織の認識，意思決定，組織構成員の行動によって組織のセキュリティ行動が支配される。組織を多数の自立主体が相互依存関係をもつシステムとして把握し，その活動を情報セキュリティ活動の側面から分析する。また，適切な管理行動への指針を見出したい。

2. 情報セキュリティ管理へのエージェントベースモデルの提案

これまでの組織と異なり，オープンネットワークをインフラとした組織運営を行う場合には，組織の拘束力が弱いため，いわゆる組織事故が発生しやすくなるのではないか。また，情報セキュリティ事故もこのような組織事故の一種と思われる。ここで組織事故とは，Reason[3]のいうように社会的，組織的，工学的，人的要因から事故が発生するという立場をとる。このような因果関係をエージェントベースモデルとして構築し，シミュレーションに

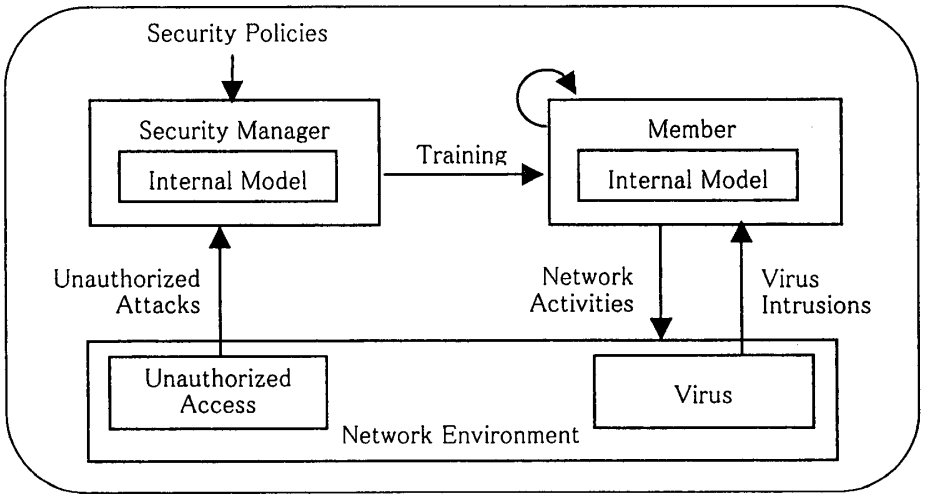

Figure 1 An Agent-based Model of Information Security Management

© 日本オペレーションズ・リサーチ学会. 無断複写・複製・転載を禁ず.

よって確認しようとするものである。

想定したネットワーク環境を説明する。組織体(企業)は社内にネットワークを持ち，インターネットに接続されている。組織構成員(Member)は社内外を問わず，電子メール/WWW/FTP などをアプリケーションとして利用している。組織体にはセキュリティ管理者(Security Manager)が配置されており，ネットワークシステムの監視，構成員へのサポートを行っている。セキュリティ管理者は経営者あるいはその部門の上司から指示されたセキュリティポリシを運用指針としてセキュリティ管理活動を行っている。図1にモデルの概要を示す。

3. 情報セキュリティ管理行動のエージェントベースモデル

システム要素として，セキュリティ管理者，組織構成員をエージェントとする。システム環境としてインターネットを設定し，セキュリティ脅威としては，不正アクセス(Unauthorized Access)とコンピュータウイルス(Virus Intrusion)を想定する。セキュリティ管理者は，セキュリティポリシの規定に従い，アクセスログの定期点検と構成員のセキュリティ教育を実施することを管理業務とする。セキュリティ管理者が，定期的にアクセスログを検査することにより不正アクセスの事実に気付き，然るべき対処を行っていれば，セキュリティ被害を未然に防止できる。また，定期的にセキュリティ教育を構成員に行うことにより，構成員のセキュリティ意識を向上させる。これらの管理行動は，セキュリティ意識の低下によって妨げられることがある。構成員は，ある確率でネットワークを利用するが，その利用に応じてウイルスの侵入を受け感染する。セキュリティ意識が十分にあればこの侵入を発見し駆除できるが，低下していると，気付かずに他の構成員にウイルスを感染させてしまう。教育を受けることによりセキュリティ意識を向上できるが，構成員は他の構成員との相互作用に支配された結果としてセキュリティ行動を取る。

4. シミュレーション結果の一例

モデルの構築とシミュレーションは，構造計画研究所で開発されたエージェントベースシミュレータを利用して行っている。図2にシミュレーション結果の一例を示す。

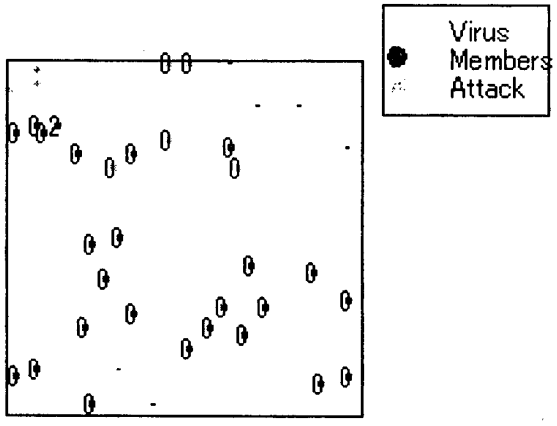

Figure 2 Distribution of Agents

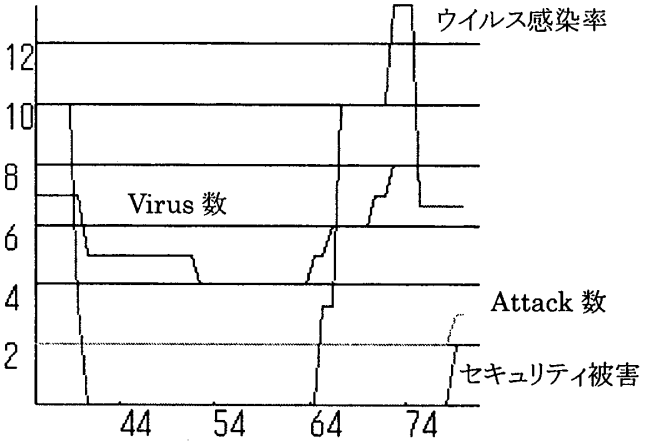

Figure 3 Transition of Agent Model

5. 今後の課題

本研究は着手したばかりであり，モデルも未だ単純過ぎる。今後，より現実的なモデルに詳細化し，またエージェントの内部モデルを適切なものに，最適化アルゴリズムを導入していきたい。

エージェントベースシミュレータ(ABS)を無償供与していただいた構造計画研究所に謝意を示します。

参考文献

[1]郵政省　情報通信利用に係るセキュリティ保護に関する検討会中間報告書－ネットワーク社会の脆弱性の克服に向けて－，平成12年 6 月。

[2]日本情報処理開発協会 「情報セキュリティに関する調査」集計結果，平成 12 年3月。

[3]Reason, James (塩見弘監訳/高野研一，佐相邦英訳)　組織事故，日科技連出版社，1999 年。

© 日本オペレーションズ・リサーチ学会．無断複写・複製・転載を禁ず．