知的エージェントによる
侵入検知支援システムの設計

能登研究室　　玉井理絵 (26103)

1　はじめに

ここ数年で情報通信技術革命は進化し，計算機環境は大きく変化した．簡単にインターネットにアクセスできるようになり，無防備なセキュリティポリシー，好奇心によるツールを使った不正行為を増加させている．リソースやデータへの不正なアクセスを防止するように設計されたシステムのセキュリティ機能は非常に重要であるが，現状ではセキュリティ違反を完全に防ぐことは不可能である．しかし，不正アクセスを発見することは可能である．この分野の研究は侵入検知と呼ばれ，それを発見するシステムを侵入検知システム（Intrusion Detection System: IDS）と呼ぶ．

本研究では，異常検出エージェントおよびアシスタントエージェントを使用し，IDS を使う管理者（administrator）をサポートするエージェントシステムを提案する．

2　侵入検知システム

本研究では IDS をホストベース IDS（HIDS）とし，また検出方法を異常検出としている．管理者が常に監視し続けなくてはならないのは異常検出を判断するためであり，新たな手口の侵入を判断するのは熟練した管理者の経験などが頼りだからである．そこで管理者の判断のふるまいをエージェントに学習させることにより，異常検出の精度を上げ，管理者の負担を軽減しサポートできるようにすることが目的である．

2.1　侵入検知システムの分類

侵入検知の技術は 2 つの主なタイプに分類できる．1 つは不正検出，もう 1 つは異常検出である．異常検出技術は，全ての侵入活動は非定型的な行動であると仮定し，システムの正常状態を確立し，現状のシステム状況も維持する．そしてこれらの 2 つを統計的に比較することで侵入があったかどうかを判定する．侵入ではないが異常な状況を侵入と判断する（false positive problem）ことと，異常状態にはならないが侵入である（false negative problem）ということの閾値を選択することが異常検出では重要である．

2.2　異常検出システム

異常検出システムの主要なアプローチは統計的なアプローチ（まず対象者の profile を作成し，システムが稼働し続けるにつれて侵入者とは異なる profile を生成する）と予想可能なパターン生成アプローチ（過去に発生したイベントから将来起こりうるイベントを予想する）に分けられる．

3　システムの流れ

まず侵入検知には次の式が成り立つ．

重大度=(重要度+致命度)
−(システムの対策+ネットワークの対策)

ここでいう，重要度とは侵入のターゲットが管理者にとって重要であるかどうかの指針を示している．致命度は攻撃の種類を表している．本研究ではエージェントが管理者であるユーザの教育，ふるまいを学習するために,「異常検出エージェント」と「アシスタントエージェント」を提案し，システムの流れを図 1に示す．

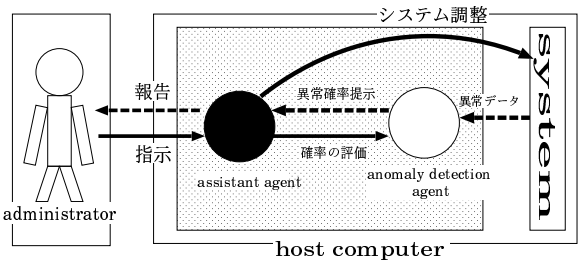

図 1: システムの流れ

1. まず異常検出エージェントはシステムから異常なデータを受け取ると，その侵入（異常）確率をパーセントで提示する．つまり侵入の兆候を 0 から 100 パーセントで判断する．これは侵入重大度式における致命度を判断することに相当する．
2. 次にアシスタントエージェントは侵入のレベルをユーザの学習と異常検出エージェントの提示した確率で判断する．これはユーザのセキュリティポリシーによる侵入対象の重要度を，アシスタントエージェントが異常検出エージェントの提出した致命度の確率と合わせて判断するということである．今までの侵入パターンから推論できるレベル（重大度）の時のユーザの対処と，レベルに対する侵入確率の致命度，重要度を合わせて判断し，侵入に対する対処をユーザに提示する．
3. そしてユーザは，提示された確率，侵入レベル，対処を評価し，その結果をアシスタントエージェントに指示する．アシスタントエージェントは指示をもとに侵入（異常）への対処をし，また確率の評価を異常検出エージェントに伝え，それぞれのエージェントは評価から学習する．

この様にアシスタントエージェントの教育が進めば，ユーザは侵入に対してその報告と提示を確認するだけで，対処はエージェントに任すことができる．

4　おわりに

本システムの利点は管理者であるユーザのセキュリティポリシーを学習するところにあり，確実な侵入と判断されるものだけを扱わないという点にある．

短所としては独立したシステムでなく，あくまでユーザ本位なシステムなことである．そのため，管理者のふるまいを学習するので，管理者が間違えていた場合などは矛盾が生じこのシステムは意味を成さない．また，エージェントの教育に根気が要ることがもっとも困難なことであり，これを改善する必要がある．