3U－7

エージェントを用いた侵入検出システムIDAの情報収集戦略

浅香 緑[†*]　情報処理振興事業協会 技術センター
大森 康正[‡]　上越教育大学
掛本 喜嗣[§]　日本総合研究所

1　はじめに

情報処理振興事業協会で開発中の侵入検出システムIDA(Intrusion Detection Agent system)では、モーバイルエージェントによってネットワーク上のターゲットシステムから侵入検出のための情報を収集する。モーバイルエージェントはサーバの制御を受けずに自律的にネットワークを移動して侵入を追跡する。モーバイルエージェントは侵入を追跡すると同時にネットワーク上に分散したターゲットから、侵入に関連した情報のみを整理して収集してサーバへ報告する。これによりサーバへの通信、解析の負荷を減らすことが可能になる。本論文では、複数のモーバイルエージェントが効率良くネットワーク上を移動し情報を収集する方法を提案する。

2　IDAの構成

IDAでは各ターゲット上で侵入につながる可能性がある事象（痕跡）が発生しているか観察し、痕跡を検出した場合さらにそれに関連した情報のみ収集して侵入であるかどうか判断するという侵入検出モデルを提案した[1]。IDAでは情報収集するための処理を各ターゲットに移動させ、システムログから必要な情報のみを収集するというモーバイルエージェントモデルを採用している。これらに基づきIDAは、情報を収集するモーバイルエージェント（情報収集エージェント）、ネットワーク上の各ターゲットで痕跡を検出するセンサー、情報収集エージェントが集めた情報から侵入を解析するマネージャから構成される。またこれら以外にネットワーク経由の侵入を追跡するためのモーバイルエージェント（追跡エージェント）がある（図1）。

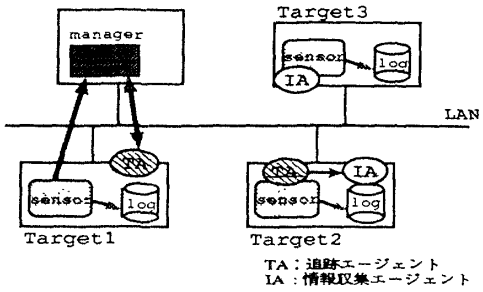

図 1: IDAの全体図

IDAの動作は、(1)各ターゲットシステム上のセンサーが痕跡を検出したらマネージャに報告する。(2)マネージャはそのターゲットシステムに追跡エージェントを派遣する。(3)ターゲットに到達した追跡エージェントは、情報収集エージェントを起動する。(4)情報収集エージェントは情報収集のためのタスクを実行する。(5)追跡エージェントは情報収集エージェントを起動した後、侵入を追跡する。すなわち痕跡がネットワークを経由したユーザにより引き起こされているか調べる。そうである場合、その発信元のホストへ自動的に移動する。(6)到達したターゲットシステムでも同様に情報収集エージェントを起動し、自らは侵入を追跡する。侵入源を突き止めた場合、それ以上移動できない場合、あるいは他の追跡エージェントがその侵入を追跡している場合、追跡エージェントはマネージャに戻る。(7)情報収集エージェントは情報収集のためのタスクが終了した後、追跡エージェントの動きと独立にマネージャに戻り、集めた情報をマネージャに報告する。これをもとにマネージャは侵入が起きているかどうか解析する。

3　掲示板

IDAではエージェント同志の情報の交換のために、情報の書き込みや読み込みが可能な掲示板を利

The Strategy of Gathering Information for IDA
[†]Midori Asaka, Information-technology Promotion Agency, Japan
[‡]Yasumasa Oomori, Joetsu University of Education
[§]Yoshitugu Kakemoto, The Japan Research Institute
*情報数理研究所より出向中

用する。掲示板には各ターゲット上で追跡エージェントが利用するものと、マネージャ上で情報を書き込み、侵入を解析するためのものとがある。

追跡エージェントは、痕跡が残されたターゲットシステムから追跡を開始するが、痕跡を残したユーザが途中のターゲットシステムでも痕跡を残している場合、他の追跡エージェントが起動されて、すでに侵入を追跡している可能性もある。これを避けるために、追跡エージェント同志が掲示板を介して情報を交換し、他のエージェントによって追跡されている侵入はそれ以上追跡しないようにする。

追跡エージェントは追跡を始める際、まずターゲット上の掲示板を参照し、自分が追跡しようとしている侵入についての情報が記録されているかどうか調べる。記録されている場合は、追跡をそれ以上続けないでマネージャに戻る。記録されていない場合は、自分がその情報を掲示板に書き込み追跡を続ける。情報としては、プロセスID、ユーザID、およびそのネットワーク接続が確立された時のタイムスタンプ、自分のエージェントID、追跡時のタイムスタンプ、移動先のターゲットシステム名である。これにより同じ侵入を追跡することが避けられる。追跡エージェントがマネージャに持ち帰る情報として、自分の移動ログ、マネージャに戻る理由がある。戻る理由としては、(1)追跡できない、(2)そのターゲットが侵入の発信地、(3)他のエージェントが追跡しているの3種類がある。他の追跡エージェントに追跡を委ねた場合は、その追跡エージェントのID、およびその追跡エージェントが移動したターゲット名も合わせて持ち帰る。

情報収集エージェントが収集した情報から、マネージャは侵入を判断する。判断はマネージャ上の掲示板に記入された情報を評価して行なう。情報収集エージェントは侵入に関連した情報、情報を収集したターゲット名、親の追跡エージェントのID、親追跡エージェントが直前にどこからそのターゲットへやってきたかの情報を持ってマネージャに戻る。情報収集エージェントはマネージャに戻ると、自分の親の追跡エージェントの識別子がついている情報が掲示板に記入されているかどうか調べ、何も掲示板上に情報が書かれていないときは、自ら持ってきた情報を掲示板に記入する。自分の親の追跡エージェントの識別子がついた情報がある場合、親追跡エージェントが自分を起動した直前のターゲットの情報の後に自分の情報をアペンドする。リストをつなぐ時に、マネージャは情報収集エージェントが収集した情報に重み付けし、リストの合成に合わせて再評価し、これの値により侵入かどうか判断し対処する。このように情報収集エージェントは、自分の収集した情報を、侵入容疑者のネットワーク上の移動に沿った形でリストにつなぐ。

追跡エージェントが他の追跡エージェントに追跡を委ねた場合、追跡エージェントは自分が追跡を委ねた追跡エージェントのID、およびそのエージェントの移動先のターゲットシステム名、および追跡を委ねたという情報をマネージャに持ち帰る。マネージャに戻ると追跡エージェントは、自分の情報収集エージェントが収集した情報のリストと、自分が追跡をゆだねた追跡エージェントの情報収集エージェントが収集した情報のリストをアペンドする（図2）。これにより二つの追跡エージェントが分担して収集した情報が合成される。この時マネージャは侵入の再評価を行なう。

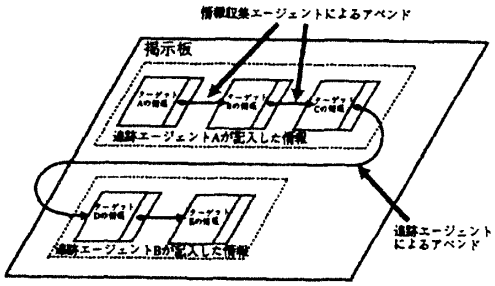

図 2: 掲示板

4 おわりに

IDA は現在 Dartmouth Colledge で開発された Agent Tcl [2] を用いて実装中である。今後は、侵入テストによる評価実験から、適切な情報収集タスクの決定、また各サイトに固有な侵入評価のための情報の重み付けに関する学習機能、暗号化・認証技術を含めたセキュリティ機能の強化を考えている。

参考文献

[1] 浅香緑, “エージェントを応用したネットワークセキュリティ技術の研究,” 成果報告書, 情報処理振興事業協会, 1997

[2] Gray, R., Rus, D. and Kotz., D.: Transportable information agents. Technical Report TR96-278, Department of Computer Science, Dartmouth College (1996)