

免疫系の超分散モデリングに基づく情報セキュリティ ～その1 表現言語の設計～*

5Q-01

溝口 文雄† 西山 裕之† 大和田 勇人†

東京理科大学 理工学部‡

1 はじめに

計算機セキュリティにおける重要なものを外部の危険から守るという考え方とは、ウィルスや寄生生物などから体を保護する自然界の免疫システムに類似している。このような考え方から、Forrest らはセキュリティシステムの構築に免疫の概念を取り入れており、不正侵入の検知や複数の検知器によるファイルの保護に成功している[1]。このようなシステムの実現には、検知器間の分散的な制御や通信、および、膨大な情報に対する処理が必要となるが、このことは[1]の論文では言及されておらず、システムの実装方法など検討されていない。また、このシステムでは単体の計算機のみを対象とし、ローカルなネットワーク全体の保護は行っていない。

これに対して本研究では免疫系に存在する多様な情報を処理するために、大量のメッセージを処理するための言語 AIL (Active Immunology Language) を設計する。これはすでに我々が開発したマルチエージェント言語 MRL[3] を免疫系に適用したものである。これにより、免疫系の分散処理に基づく情報処理が AIL により表現でき、免疫系の実験データに対応するシミュレーションが可能となる。なお、本言語 AIL を用いたセキュリティソフトウェアは、[2] を参照されたい。

2 免疫系のセキュリティへの応用

免疫システムを簡単に述べると、体内における「自己」と「非自己」などの区別を行い、「非自己」を排除する機構のことである[4]。ここで、「非自己」な存在の排除は、図 1 のように「B 細胞」「T 細胞」と呼ばれる 2 種類の細胞群を中心に処理が行われている。「B 細胞」とは、ウィルスなどの「抗原」と呼ばれる非自己な蛋白質を認識することで、その「抗原」と反応して排除する分子である「抗体」を分泌する細胞である。「B 細胞」の

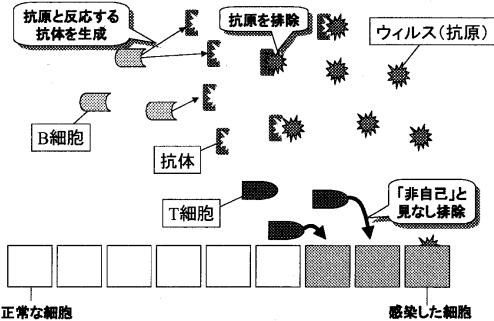


図 1: 免疫システム

大きな特徴として、一度認識した「抗原」を記憶する能力があり、再認識がなされることで短時間に大量の「抗体」を生産することができる点である（二次免疫反応）。これに対し、「T 細胞」とは「抗原」により変質させられた「自己」の細胞を「非自己」と見なし、排除する細胞である。双方の細胞は刺激し合うことで互いの活性化を計り、「抗原」の侵入により変質させられた細胞、および「抗原」自身を効率的に排除を行う。

このように、免疫システムは二段階のメカニズムに分かれており、2 種類の細胞群が超並列分散的に、かつ互いに協調しながら、外部からの「抗原」により変質された「自己」の部分と、元凶である「抗原」そのものを「非自己」として排除している。

これを計算機セキュリティに適用すると、「自己」とは正規のユーザーからのアクセスや正規に作成されたファイルとなり、「非自己」のうち、「B 細胞」により排除される「抗原」は不正侵入によるアクセスや侵入したウィルスであり、「T 細胞」により削除されるべき変質された「自己」とは、不正に作成、変更されたファイルに該当する。これにより、互いの細胞が協調することで、不正侵入によるアクセスを認識した場合は、そのアクセスにより操作されたファイルの削除・修正を行い、不正に操作されたファイルを認識したのならば、その操作を行ったアクセスを「抗原」と見なせばよい。さらに、二次免疫反応の特徴を取り入れることで、2 度目の以降の不正侵入は、侵入した段階で排除することが可能となる。

*Information security based on distributed modeling of immunology ~ Part 1: Design of representation language ~

†Fumio MIZOGUCHI, Hiroyuki NISHIYAMA and Hayato OHWADA

‡Faculty of Sci. and Tech. Science University of Tokyo

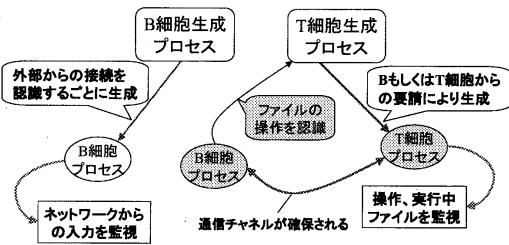


図 2: 各免疫細胞プロセスの生成

3 モデル化

前節で述べた免疫細胞である「B 細胞」と「T 細胞」を、ネットワークセキュリティにおいて実現するためには次のような機構が必要となる。

- (1) 「B 細胞」の役割を担い、外部からの接続を監視するプロセス。
- (2) 「T 細胞」の役割を担い、ファイルに対する操作を監視するプロセス
- (3) 「B 細胞」「T 細胞」の機構を動的に生成・削除するプロセス
- (4) 「非自己」の認識を行うためのプロセス
- (5) 各々の機構間で通信を可能にするプロセス

ここで、ネットワークを介して外部の計算機から接続を受ける場合、外部の計算機の IP アドレスおよびポート番号は各接続ごとに特定される。そのため、(1)「B 細胞」プロセスは接続を受けることで(3)のプロセスにより生成され、生成後は接続元から受信するメッセージの監視を行う。また、その監視によりファイルに対する操作が行われた場合、個々のファイルごとに(2)「T 細胞」プロセスを同様にして生成する(図 2 参照)。これにより、処理すべき情報は各々の免疫細胞プロセスに分散して流れることになる。そして、各々の細胞プロセスは、メッセージの受信もしくはファイルに対する操作を受けることで、(4)の認識プロセスを呼び出し、「非自己」の確認を行う。ここで「非自己」の判定が行われた場合は、不正侵入における接続の切断、もしくは不正に操作されたファイルの削除・修正を行うことになる。さらに、各細胞のプロセス間で(5)の通信を行うことにより、不正侵入が行われた場合は、その侵入者が行ったファイル操作を全て「非自己」へ、逆にファイルの不正操作が行われた場合は、その操作を行った接続を「非自己」へと連鎖的に判断することが可能となる。

4 AIL の設計

以上より、免疫システムに基づくセキュリティモデルを実現するためには、複数プロセスの分散・協調モデリングが不可欠となる。そこで本研究では、並列論理プログラミング言語 KL1に基づいて設計されたマルチエージェント言語 MRL[3]の拡張を行い、本モデルの実現に適用する。MRL は KL1 のもつ同期・非同期制御、ストリーム通信の機能を導入しており、複数プロセスの並行処理やプロセス間通信、およびプロセスの動的な生成・削除を実現できる言語である。本研究では MRL を免疫系セキュリティに適用すべく、次の拡張を行った。

- ネットワークを介して計算機に流れ込む情報を収集する機構の組み込みを行った。この機構では外部からの接続や情報の入力を受けた場合、相手の IP アドレスとポート番号を特定する能力を持つ。
- 計算機内で実行されたファイル名、および実行中のファイル名を監視する機構の組み込みを行った。この機構では、外部からの入力によるファイルの実行、および実行されたファイルからの異なるファイルの実行を認識する。
- 以上の 2 つの機構との通信路を自動生成し、免疫細胞プロセス間とのメッセージの送受信機能を付加した。

以上より、AIL を用いることで免疫系のセキュリティシステムの構築を可能にする [2]。

5 おわりに

本研究では免疫系に存在する多様な情報を処理するために、大量のメッセージを処理する言語 AIL を設計した。AIL は免疫系における情報処理を免疫細胞ごとのプロセス定義により実現し、免疫細胞プロセス間の協調をプロセス間通信により可能にしている。これにより、免疫系の実験データに対応するシミュレーションが実現可能となる。

参考文献

- [1] S. Forrest, S. A. Hofmeyr and A. Somayaji, Computer Immunology, *Communications of the ACM*, Vol. 40, No. 10, 88–96, 1997.
- [2] 溝口文雄、大和田勇人、西山裕之、免疫系の超分散モデリングに基づく情報セキュリティ～その 2 不正侵入検出への応用～、情報処理学会第 60 回全国大会, 2000.
- [3] H. Nishiyama, H. Ohwada and F. Mizoguchi, A Multiagent Robot Language for Communication and Concurrency Control, *International Conference on Multiagent Systems*, 206–213, 1998.
- [4] 多田富雄、免疫の意味論、青土社, 1993.