

免疫系の超分散モデリングに基づく情報セキュリティ

5Q-02

～ その2 不正侵入検出への応用 ～ *

溝口 文雄[†] 大和田 勇人[†] 西山 裕之[†]

東京理科大学 理工学部[‡]

1 はじめに

本論文では免疫系の柔軟な構造に類似したセキュリティ技術の開発のために、不正侵入とウイルス感染に対処する方法を提案する。これは免疫系のもつ自己・非自己の認識メカニズムを応用する。計算機セキュリティに免疫系の概念を用いた研究として、Forrest らによって侵入検知とファイルの保護が行われているが [1], それぞれの機能は独立しているため、互いの機能が協調して効率的に侵入者を追い詰めるようなシステムとはなっていない。

免疫系では侵入者の排除と侵入者により汚染（「非自己」化）された「自己」の排除を行うべく、B 細胞、T 細胞と呼ばれる 2 種類の免疫細胞が存在する [4]。これに対し本研究では、ネットワークを介した入力監視を B 細胞プロセス、その入力により操作・実行されたファイルの監視を T 細胞プロセスとして、各免疫細胞プロセスを定義する。それぞれの免疫細胞プロセスは独立して不正侵入および汚染されたファイルを「非自己」として検出し、検出後は互いに協調して「非自己」の存在を排除する。本システムの実装には [3] で設計された言語 AIL を用いることで、各免疫系プロセスの動的な生成・削除および各プロセスの並行実行とプロセス間通信を実現している。これにより、外部からの全てのアクセスおよびファイル操作に対して動的に対応する免疫系のセキュリティシステムを構築している。

2 システム構成

人間における免疫システムでは骨髄 (Bone marrow) から B 細胞が、そして胸腺 (Thymus) から T 細胞が生成される。これらの免疫細胞は、ウイルスや細菌などの「抗原」が体のあらゆる部分から侵入した場合に備え、体内を常時巡回している。これに対してネットワークセ

キュリティにおいては、不正侵入者やコンピュータウイルスなどの「抗原」は、ネットワークケーブルという唯一の通路を介して侵入してくる。そのため計算機を守るためには、その計算機と接続されている通路の監視を行い、その通路を介して発せられた命令により操作・実行が行われたファイルのみを監視すればよい。ここで、これらの 2 つの監視機構は本システムの実装に用いる言語 AIL に組み込まれている [3] ため、各々の免疫細胞プロセス以外に必要なプロセスは次の通りとなる。

- B 細胞生成プロセス (骨髄プロセス)

ネットワークの監視により新たな外部からの接続を認識したならば、その接続先からの入力を監視する B 細胞プロセスを生成するためのプロセス。このとき生成される B 細胞プロセスには、ネットワーク監視機構との通信路が付加され、以後、その接続先からの入力情報を受信することになる。

- T 細胞生成プロセス (胸腺プロセス)

ファイルの監視により操作・実行を認識し、B 細胞プロセスによりそれが外部からの入力によるものと判定されたならば、その操作・実行されているファイルを監視する T 細胞プロセスを生成するためのプロセス。生成されたプロセスにはファイル操作の監視機構との通信路が設けられる。なお、このプロセスでは T 細胞プロセスが監視している実行ファイルが新たにファイルの操作・実行を行った場合も同様にして T 細胞プロセスを生成する。

- 「非自己」判定プロセス

侵入検知においては、分析したトレースとデータベース内のパターンを比較することにより、異常な振舞いを含んでいるものを認識する方法が提案されている [1]。本研究ではこの方法を拡張し、判定プロセスに帰納学習器を複数備えることで、データベース内におけるパターンの動的な生成を実現する [2]。これにより、本システムでは既に与えられたパターンルールを基に「非自己」の判定を行い、システムの稼働中における情報収集により、新たな

*Information security based on distributed modeling of immunology ~Part 2: Application to intrusion detection~

[†]Fumio MIZOGUCHI, Hayato OHWADA and Hiroyuki NISHIYAMA

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

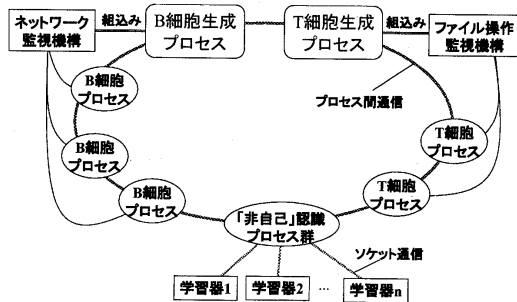


図 1: セキュリティシステムの構成

ルールが生成されることになる。これは、免疫系における二次免疫反応に該当する。なお、帰納学習器は AIL の組み込みではないため、プロセスからのソケット通信を介した外部システムの呼び出しにより実現している。これは、学習を他の計算機上で同時に実行できることを意味する。

以上の各プロセスからなるセキュリティシステムは、図 1 のような構成となる。

3 免疫細胞プロセス間の協調

各免疫細胞プロセスのうち、入力情報を監視する B 細胞プロセスは、一つの外部からの接続に対して一つのみ生成される。これに対して特定ファイルの操作を監視する T 細胞プロセスは、外部から、もしくは T 細胞プロセスが監視しているファイルにより、異なるファイルが操作されることで個別に生成される。ここで、全ての T 細胞プロセスはその生成過程において、必ずいずれかの B 細胞プロセスと関係を持つことになる。例えば、図 2 では、B 細胞プロセスが監視している接続先からファイル A,B,C の操作が行われた場合は、それぞれのファイルを監視する T 細胞プロセス 1,2,3 が生成される。また、ファイル A の操作（実行）中にファイル D が操作された場合、ファイル D を監視するための T 細胞が生成される。これにより、外部の操作により連鎖的に実行された全てのファイル操作を監視できることになり、個々の免疫細胞プロセスは自分の監視を行う対象にたいする情報を受け取ることで、「非自己」判定プロセスに問い合わせることになる。

本システムでは T 細胞プロセスを生成する際、生成元は通信チャネルを新たに開設する。これは、B 細胞プロセスを最上位にして階層的に生成される全ての T 細胞間との通信路が、本システムのプロセス間通信とは独立して構築されることを意味する。これにより、階層的に

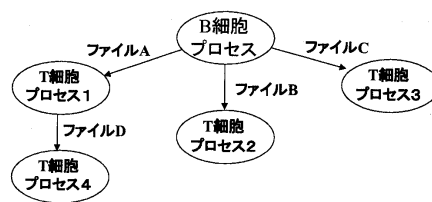


図 2: 免疫細胞プロセスの階層化

構築された免疫細胞プロセスの中で、「非自己」と検知したプロセスが一つの中でも発生すれば、階層間の通信路を介したブロードキャストにより、すべての操作が「非自己」として認識されることになる。例えば、図 2 においてファイル D 操作の監視中に「非自己」の判定が行われたならば、ファイル A,B,C 全ての操作が「非自己」として認識され、さらに、B 操作プロセスの接続先からのアクセスそのものも「非自己」として認識される。これにより、各々のファイル操作は中断・削除され、接続は遮断される。そして、このときの侵入方法およびファイルの操作方法は、「非自己」判定プロセスにおいて記録され、新たな侵入パターンのルール作成に活用される。

以上のように、本システムでは免疫細胞プロセス間の協調により不正侵入の検出と修復を、免疫系のもつ自己・非自己の認識メカニズムを応用することで実現している。

4 おわりに

本研究では、免疫系の柔軟な構造に類似したセキュリティ技術の開発のために、不正侵入とウイルス感染に対処するシステムを構築した。本システムは免疫系のもつ自己・非自己の認識メカニズムを応用することで、自動修復機能をもつセキュリティソフトウェアを構築することを可能としている。

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, 侵入解析用ビジュアルブラウザの設計～ カッコエッグプロジェクト ～, コンピュータセキュリティシンポジウム'99, 135-140, 1999.
- [3] 溝口 文雄, 西山 裕之, 大和田 勇人, 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 ～, 情報処理学会第 60 回全国大会, 2000.
- [4] 多田 富雄, 免疫の意味論, 青土社, 1993.