免疫型超分散ネットワークセキュリティシステムに関する研究（0221059）

Research of Super Distributed Network Security System based on Immune System

西山裕之　東京理科大学理工学部
Hiroyuki Nishiyama　Faculty of Science and Technology, Tokyo University of Science

平石広典　東京理科大学情報メディアセンター、株式会社ウィズダムテック
Hironori Hiraishi　Information Media Center, Tokyo University of Science, WisdomTex Inc.

研究期間　平成 14 年度～平成 16 年度

概要

本研究ではネットワークに接続された計算機およびその情報を守るために、人間の免疫系における免疫細胞の機能を免疫細胞エージェントとして計算機ネットワーク上で実現することにより、不正侵入の検知および排除を可能にするセキュリティシステムに関する研究を行った。本エージェントはネットワークに流れ込む情報や計算機内の処理情報を個別に監視しており、各エージェントが協調することにより、従来のセキュリティソフトウエアでは検知困難な不正侵入の検知や追跡を可能にする。また本システムは、帰納学習器を中心とするデータマイニングを用いることで侵入パターンの自己生成を可能とし、未知な侵入への対応を図る他、管理者が侵入経路等を容易に特定可能とするために、侵入の痕跡データを視覚的に表示可能なツールも設計した。

Abstract

We design a network security system using an analogy of natural world immunology. We adopt an immune mechanism that distinguishes self or non-self and cooperation among immune cells of the system. This system implements each immune cell as an agent. These agents can detect and reject intrusion by cooperating with each other.

研究内容及び研究成果

不正侵入者を検知し排除するシステムはネットワークセキュリティの中でもっとも重要な研究課題の一つである。しかしながら、従来のシステムでは予め与えられた侵入パターンのルールベースに基づくものがほとんどであり、未知な不正侵入に対しては対応することが不可能であった。また、不正侵入を検知できたとしても、その侵入者の特定のアクセス過程のみを認識できただけであり、その侵入により改竄されたファイルや実行されたプロセスなどを把握することは困難であった。このような問題に対し本研究では、人間の持つ免疫機構に着目し、体内に入り込むウイルスや病原菌を排除し、これらにより汚染された部分を排除するシステムをネットワーク計算機上で実現する。具体的には、ネットワークを介して流れ込む情報や各計算機内で活動中のプロセス等を個別に監視する機構を持ち、分散的に機能している各監視機構が協調することで不正侵入の検知と排除を効率的に行うネットワークセキュリティシステムを開発する。不正侵入の排除としては、本システムを導入するネットワーク内における不正侵入者のすべてのアクセスと処理中のプロセスを強制的に終了させるとともに、それらの情報を視覚化するソフトウエアも開発し、ネットワーク管理者による不正侵入者の侵入経路や処理内容の認識を容易にする。不正侵入の検知においては、既に把握されている侵入パターンのルールベースを用いるとともに、一度行われた不正侵入や可能となりうる侵入パターンを予め用意する機構を取り入れ、未知な不正侵入へも対応可能とする。これは、本セキュリティシステムの一つの機能として開発するデータマイニングソフトウエアにより、これまでの侵入パターンおよび侵入における痕跡データ等から、新たな侵入パターンに対応するルールを自己生成することにより可能とする。

以上を実現するために、本研究では次の３つのソフトウエアの開発を行った。

１．不正侵入を検知および排除する超分散ネットワークセキュリティソフトウエア
２．侵入パターンルールを導出するデータマイニングソフトウエア
３．侵入経路および不正処理内容を視覚的に表示する GUI ソフトウエア

1. 不正侵入を検知および排除する超分散ネットワークセキュリティソフトウエア

超分散ネットワークセキュリティソフトウエアを実現するために、本研究では分散処理および情報共有を大規模に行うための言語 JMAL(Java Multi Agent Language)の開発を行った他、ネットワーク監視ツールおよびプロセス監視ツールの開発を行い、それらの言語および各ツールを統合的に用いることにより、免疫系セキュリティツールの実装を行った。本セキュリティツールでは、ネットワークからのアクセスを個別に監視する機能を B 細胞エージェント、プロセスの処理内容を個別に監視する機能を T 細胞エージェントとして定義する。これらのエージェントは動的に生成され個別に監視対象の情報を収集することから、ネットワーク計算機全体の振る舞いをリアルタイムに監視可能である。また、各免疫細胞エージェントは互いに情報共有を行うことで、単体の情報では検知が困難な不正侵入の協調的な検知を実現する。さらに、異なる計算機間の免疫細胞エージェント間で情報共有を行うことにより、ネットワーク全体に対するユーザごとの振る舞いを監視エージェント群のグループとして表現することができる。

2. 侵入パターンルールを導出するデータマイニングソフトウエア

我々の所属する研究組織では、既に機械学習システムを開発しているが、これは汎用システムとして設計されている。ここで、扱うログのデータ形式は、時間情報やプロセスの関連情報、ユーザ情報、そしてメッセージ情報などがリスト構

造などの論理表現として表されている。しかしながら、従来の関係データベースでは論理表現を行うのに十分で簡潔な表現力に欠けるなどの問題が存在してきた。そこで、本研究では、論理表現からなるデータベースを実現する方法として、XML データベースを利用する帰納学習アルゴリズムを設計した。XML データベースのための ILP システムの設計により、progol のような ILP システムを XML で表現し、それを XML データベース上で実現することにより、データの取り扱いの容易さ、自然な記述形式、メモリに関する問題等を解決することができる。さらに本研究では、学習ツールにおけるルール生成アルゴリズムの処理を計算機群による並列処理を可能とするための分散システムを設計し、JMAL 言語により実装した。また、効率的な分散処理を実現するために、言語開発において設計した計算機状況およびネットワーク内の情報量を計測するツールを応用し、タスクを割り当てる際に最も適した計算機への割り当てを可能にした。

3. 侵入経路および不正処理内容を視覚的に表示する GUI ソフトウエア

不正侵入が検知された場合の対処として、上記の免疫系セキュリティツールによる侵入者の実行プロセスの排除の他、その不正侵入者の振舞いの内容をネットワーク管理者が視覚的に認識するためのビジュアルツールの開発を行った。本ツールはハイパボリックツリーの表示形式、および三次元グラフィックスを用いることにより一度に大量の痕跡データの全貌を確認することが可能な機能を想定するとともに、マウス操作などによって必要とされる情報を容易に引き出すための GUI を備え付ける。本ソフトウエアを用いることにより、ネットワーク管理者は管理するネットワーク全域における侵入者の痕跡の調査を簡易に行うとともに、その侵入経路などの追跡を視覚的に認識することが可能となる。これにより、ネットワークから流れ込む情報と計算機の内部情報（プロセスレベルの振舞い）の双方を監視し、互いの情報を一つの画面で表示可能な視覚化ツールの設計および実装を行った。本ツールでは単体の計算機だけでなく、複数台の計算機間の通信状況も視覚化を行うことにより、不正侵入における経路追跡を可能にした。また、不正侵入により生成されたプロセス情報も追跡結果として表示可能であることから、不正侵入後の対応も容易となる。

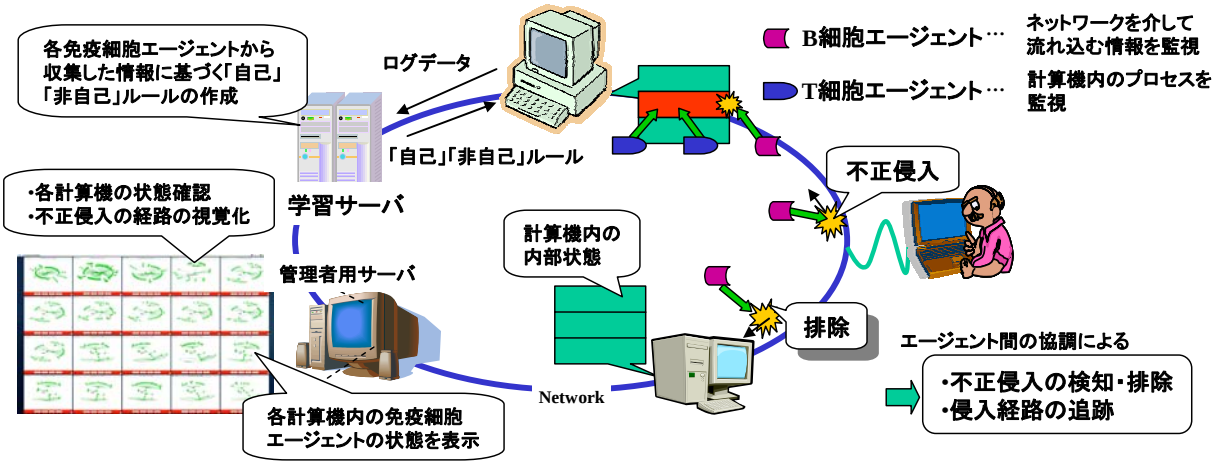

図１　本システムの使用イメージ

以上のように本研究では３つのソフトウエアを開発し、人間の免疫系における免疫細胞の振舞いを免疫細胞エージェントとしてネットワーク計算機内で実現し、不正侵入およびその痕跡を免疫細胞エージェント間の協調により検知および排除することに成功した（図１参照）。また、帰納学習ツールを組み合わせることで、一度経験した不正侵入に対する即応的な検知を実現するなど、免疫系における二次免疫反応と同様の機能を実現した。さらに、不正侵入に対する視覚化ツールを導入することにより、各免疫細胞の振舞いや不正侵入の追跡を視覚的に確認できるようになった他、ネットワーク管理者が組織内の計算機状況の確認や通信状況の把握を容易に行うことを可能にした。また、未知な不正侵入を受けた場合でも、「非自己」ルールに定義された侵入パターンと同様の不正侵入に関しては、免疫細胞エージェント間の協調により侵入の段階で排除が実現できた。「非自己」ルールが存在しない場合でも、帰納学習ツールにより作成した「自己」ルールにより「自己」以外の存在として認識され、視覚化ツールとの協調により確認および排除が可能となっている。

誌上発表リスト

[発表 1] 西山 裕之、山崎 航、溝口 文雄、“並列論理プログラミングに基づくマルチエージェント言語 MRL”、コンピュータソフトウエア、Vol. 20, No. 1, pp. 36-50 (2003. 1)

[発表 2] Hiroyuki Nishiyama and Fumio Mizoguchi, “Design and Implementation of Security System Based on Immune System”, Software Security - Theories and Systems, Lecture Notes in Computer Science, Hot Topics, No.2609, Springer-Verlag, pp.234-248 (2003. 2).

[発表 3] 溝口文雄、西山裕之、“免疫系によるネットワークセキュリティ”、コンピュータソフトウエア、Vol.20,No.3,pp.88-94, (2003.5).

報道発表リスト

[報道 1] “無線 LAN 室外からの侵入阻止：理科大がソフト、電波強度で識別”、日経産業新聞、2004. 3. 19.

[報道 2] “ネット侵入・ウイルス検知で新手法：人工知能ソフト多数掲載、免疫細胞の仕組み応用”、日経産業新聞、2004.4.15.