

知能ソフトウェアに基づくグローバルな通信セキュリティに関する研究

Research on Global Communication Security based on Wisdom Software

溝口 文雄 (Mizoguchi Fumio)

東京理科大学・理工学部・教授



研究の概要

本研究では WAN(Wide Area Network)および無線 LAN やセンサチップ等を含む利用に対する知能的ソフトウェアに基づく安全な通信基盤の構築を行う。具体的には各計算機およびチップ上で動作する監視機構を設け、その監視機構が互いに協調することで不正侵入の検知および排除を実現する超分散セキュリティソフトウェアを設計する。

研究分野：総合領域

科研費の分科・細目：情報学・計算機システム・ネットワーク

キーワード：セキュアネットワーク

1. 研究開始当初の背景・動機

インターネット世界は、利用人口の巨大化、通信・計算機処理の高速化、そして無線 LAN などの汎用化に伴い、利便性・有用性が急速に向上している。しかしながら、コンピュータウイルスやクラッキングなどの危険性および被害も拡大しているため通信の信頼性は低下している。

2. 研究の目的

本研究では、LAN(Local Area Network)だけでなく WAN(Wide Area Network)レベルを対象とするほか、無線通信に基づくセンサチップ等を含む利用に対して、知能的ソフトウェアに基づく安全な通信基盤の構築を行う。具体的には、各計算機およびチップ上で動作する監視機構を設け、その監視機構が互いに協調する超分散セキュリティソフトウェアを設計する。さらに、多数のセンサを用いたヒューマンセキュリティなど、その通信の安全性を背景とする新たなネットワークサービスの創出を行う。

3. 研究の方法

各セキュリティソフトウェアの設計および実装は東京理科大学溝口研究室のワークステーション上で実施を行った。各種カメラセンサを含むセンサネットワーク関連の研究開発は同大学情報メディアセンター内で実施した。また、株式会社ウイズダムテックの協力により、多拠点間の通信およびセキュリティ実験を実施した他、プロトタイプの配布および評価実験を実施した。

4. 研究の主な成果

本研究では、最初に WAN レベルにおける超分散および情報共有処理を大規模に行うための言語開発を行った。本言語は、NAT 等で寸断されたプライベートネットワーク間の透過的な通信を可能にするミドルウェアを開発し、組み込みを行うことで、WAN レベルでの情報共有を可能にした。

次に、通信セキュリティとして、各種 OS ごとに、計算機上のプロセスを監視するソフトウェア、および、パケットレベルを解析するソフトウェアを開発した。そして、本解析ソフトウェアを用いたセキュリティソフトウェアを上記言語により実装を行うことで、監視ソフトウェア間の分散・協調処理を実現した。これにより、WAN レベルにおける不正侵入の検知および侵入経路の追跡を可能にした。本ソフトウェアに動的なモニタリングを用いたファイルバックアップシステムの設計と実装を行うことで、ファイルの自己修復機能を備えることに成功した。これにより、不正侵入等によりファイルの改ざんが行われたとしても、不正侵入の検知が行われた段階で、本セキュリティシステムの追跡により不正侵入処理の追跡が行われ、ファイルの修復が自動的に行うことが可能となった。また、本自己修復機能を応用することにより、ネットワークを介した特定ファイルの追跡も実現している。これは、Winny 等のファイル共有ツールを悪用した情報漏洩により機密情報や個人情報流出しても、その流出先を特定することができることを意味する。

その他、侵入パターンおよび個人情報ルールを導出するデータマイニングソフトウェア、無線通信に対する伝播損失情報を応用した位置認識が可能なソフトウェア、ヒューマンセキュリティシステム、そしてヒューマンサポートシステムを開発した。さらにセンサチップ群を用いたセキュアな相互協調システムの設計を実施するとともに、設計した言語の開発環境の構築、WAN レベルにおける情報共有を実現するための NAT 越え通信に対する検証等を行った。

以下に本課題における代表となる研究成果を列挙する。

○ WAN レベルにおける超分散および情報共有処理を大規模に行うための言語開発

WAN レベルにおける分散処理および情報共有を大規模に行うための言語 WMAL(WAN Multi Agent Language)

の設計および開発を行った。本言語は WMAL トランスレータと通信ミドルウェア LampEye による通信、追跡、検証機構から成り立っており、NAT 越え通信を含む WAN レベルの情報共有を可能にする他、計算機間の情報共有の際の送受信先の情報トレース機能、および情報共有時の計算機間の認証機能を実現している。

○ 自己修復機能を備えた協調型超分散ネットワークセキュリティソフトウェアの開発

本セキュリティソフトウェアでは、ネットワークからのアクセスを個別に監視する機構、プロセスの処理内容を個別に監視する機構を個別のエージェントとして定義する。各エージェントは監視対象の動きをトレースすることで関連するエージェントと情報共有を行い、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、WAN レベルにおける異なる計算機間のエージェント間で情報共有を行うことにより、外部からの侵入はもちろん内部攻撃が行われた際も、その侵入方法や実行内容を詳細に把握することが可能となる。

さらに、本成果の一部である動的なモニタリングを用いたファイルバックアップシステムにおけるハードディスク等に保存されたファイル情報を管理するツールとの協調機能を追加することにより、不正侵入の検知を可能にすると共に、その不正により改竄された部分を特定し自己修復を実現した。さらに、本成果の一部であるファイルアクセスを監視するモニタリング機構と協調することで、ネットワークを介した特定ファイルの移動に対する追跡も実現している。各ソフトウェアの協調は、上記で開発した言語 WLAN により実現している。

5. 得られた成果の世界・日本における位置づけとインパクト

本研究では、従来のセキュリティのように不正侵入に対する検知・排除を行う機能だけではなく、侵入追跡、侵入により改ざんされたファイルの自動修復、さらには、ネットワークを介した情報漏洩に対する追跡を可能にする WAN レベルのセキュリティソフトウェアを開発した。これは、本研究の目標である安全な通信基盤を、本研究で開発した知能的ソフトウェアにより構築できることを意味している。

6. 主な発表論文

(研究代表者は太字、研究分担者には下線)

○ 発表論文・学会発表

・大林 真人, 西山 裕之, 溝口 文雄: TinyMRL: センサネットワークへのマルチエージェント言語の導入によるセキュアな相互協調システム, 電子情報通信学会論文誌, Vol. J89-D, No.8, pp.1764-1776, 2006.

・山崎航, 平石広典, 溝口文雄: 動的なセキュリティポリシーのためのRBACシステムの設計, 情報処理学会論文誌, Vol.47, No.6, pp. 1932-1940, 2006.

・Makoto Obayashi, Hiroyuki Nishiyama and **Fumio Mizoguchi**: Secure Cooperation in a Distributed Robot System using Active RFIDs, International Journal of Artificial Life and Robotics, Vol.10, pp. 29-34, 2006.

・Makoto Obayashi, Hiroyuki Nishiyama and **Fumio Mizoguchi**: Secured Cooperative Multi-Agent System in Limited Resources for Intelligent Sensor Network, The 31st Annual Conference of the IEEE Industrial Electronics Society, pp. 2668-2673, 2005.

・西山 裕之, 溝口 文雄: 自己修復機能を備えた協調型分散ネットワークセキュリティの設計, 日本ソフトウェア科学会第 24 回大会, 6D-2, 2007.9.

・大林 真人, 西山 裕之, 溝口 文雄: 携帯電話アプリケーションによるモバイルなセンサネットワーク構築支援システム, 日本ソフトウェア科学会第 23 回大会, 6A-1, 2006.9.

・西山 裕之, 溝口 文雄: モデル検査を用いた NAT 越え通信ソフトウェア検証の研究, 日本ソフトウェア科学会第 23 回大会, 3C-2, 2006.9.

○ 著書

・溝口 文雄, 西山 裕之: 免疫を持つコンピュータ - 生命に倣うネットワークセキュリティ-, 岩波書店, 総頁数 110, 2006.

ホームページ等

<http://www.wisdomtex.com/>