博士請求論文審査要旨

情報セキュリティ大学院大学
情報セキュリティ研究科

論文題目　：　直観主義論理の意味論に基づく統合セキュリティモデル
申請者　：　森住哲也
審査委員会　：　主査　教授　辻井重男
副査　教授　田中英彦
副査　教授　板倉征男
副査　教授　有田正剛

Ⅰ．論文内容の要旨

本論文は、オープン・イノベーションやダイナミック・コラボレーション、あるいはＳＮＳなどが進展する情報ネットワーク社会環境の中で、ネットワーク化された統合データベースにおける隠れチャンネル（covert channel）による情報漏洩という深刻化する課題に対して、データベース群の有用性・効率性の低下を極小化しつつ、情報漏洩を防ぐことを目的として、直観主義論理に基づく隠れチャンネルの検出法を提案したものである。

データベースにおける隠れチャンネルとは、いくつかのアクセス主体を列、読み書きされる情報（ファイルなど）を行とし、読み出し権限と書き込み権限の有無を要素とする行列において、各主体が許可された権限に従って、読み出し、書き込みを行ったとき、あるファイルの中身を、読み出し権限のない主体が読めてしまうような情報漏洩経路を意味している。１つの組織内だけでデータベースを利用している場合には、隠れチャンネルがあったとしても深刻な問題として認識されない場合も多いし、そもそも、日本では、従来、情報漏洩に対して高い関心は払われなかった。しかし、冒頭に述べたように、例えば、ライバル企業とも情報交流が行われる環境下では、情報漏洩の極小化は企業などの存亡に関わる課題となっている。

データベースにおける隠れチャンネル問題は、１９８０年代から研究されてきた研究課題である。海外では、米国を中心に、軍における機密保護の観点からの Bell and Lapadura モデルを始めとして、Chinese Wall モデルや Take and Grant モデルなどが提案されてきた。他方、我が国では、一般にはこの問題に対する関心は低かったが、１９８０年代後半、本論文申請者の森住らは、いち早く本問題の重要性を認識し、ＡＴＲにおいて研究を開始した。その後、申請者は、日本におけるこの分野の数少ない研究者として東工大、中央大の辻井研究室との共同研究や総務省の情報セキュリティプロジェクトを主導して、多くの業績を挙げ論文を発表してきた。そして、ここ数年のいわゆる Web 2.0 時代の潮流を背景に、申請者は、企業などの組織間にまたがる統合データベースにおける情報漏洩問題に取り組んできた。

本論文は「直観主義論理の意味論に基づく統合セキュリティモデル」と題し１２章から成っている。

第１章「緒論」では、本研究の背景、概要、及び経緯などを説明している。

第２章「covert channel とセキュリティモデルの位置づけ」は、本論文全般の導入部に当たり、データベースにおける情報漏洩や情報改竄の経路となる covert channel を定義した上で、Bell and LaPadula モデル、X.５００ディレクトリのアクセス制御モデル、Chinese Wall モデル、Take-Grant モデル、及び Role

Based Access Control(RBAC)モデルなどの従来型セキュリティモデルを示し、それらが、競合、役割、所有、階層という単体概念に対応するモデルであると述べ、統合データベース時代のモデルとしては柔軟性に欠ける事を示している。

第３章「データベースにおける covert channel」では、アクセス行列における covert channel の経路、及びその総数などについて分析すると共に、具体的事例として、関係データベース、及びＸＭＬデータベースにおいて covert channel が引き起こされるメカニズムを明らかにしている。

第４章「モデルの統合と５つの特性」では、異なるコミュニティにあっても柔軟にかつ効率的に作動する作動するアクセス制御のあり方について考察し、個々のアクセス要求に関する covert channel を分析し、局所的に矛盾がある場合には、それを無くすようなフィルタをかけるという手法を提案している。

第５章「確定記述によるセキュリティモデルの記述」では、セキュリティモデルの記述を可能な限り一般化するために、論理式の記述方式を確定記述の方法によって、統一的に記述することを提案している。この形式と直観主義論理によって、アクセス要求における不確定項を条件付で確定項に置き換え、最終的には真、あるいは偽の真理値という結論が得られることを示している。

第６章「直観主義論理によるダイナミックなアクセス制御の記述」では、アクセス主体とアクセスされる客体が持つ５つの属性（競合、所有、プライバシー、役割、階層）を用い、アクセス行列内のレベル２の covert channel 経路に対して、５つの属性に基づいた推論によって covert channel を分析し、情報フィルタを設定する方法を提案し、そのためにはダイナミックな記述が可能な直観主義論理の適用が有効であることを示している。

第７章「統合アクセス制御システムの提案」では、複数のコミュニティにおいて、アクセス制御システムが covert channel を如何に分析し、情報フィルタによって制御するかを示している。

第８章「統合セキュリティモデル‘Community Based Access Control Model‘の提案」では、５つの属性に関する意味論を統合するセキュリティモデルとして‘Community Based Access Control Model`を提案している。このセキュリティモデルにおいて、ネットワーク上の多様な Community に共通的な一般モデルと Community 毎にカストマイズされる特殊モデルを定義している。

第９章「競合属性と階層属性の統合セキュリティモデル」では、Chinese Wall モデルを対象として、第８章で提案したモデル‘Community Based Access Control Model`の有効性を示している。

第１０章「介護・医療システムへの適用と推論機能」では、ＳＮＳを制御する‘Community Based Access Control Model`が介護・医療システムに対して有効であることを示している。

第１１章「covert channel 分析制御のための Access Control Agent System」では、covert channel 分析の計算量を軽減し、異なる組織間での通信時においても常に covert channel を分析できるようにするため、Access Control Agent System を提案している。

第１２章では、本研究で得られた成果を要約している。

以上のように、本論文では、古典論理による隠れチャンネルの数え上げとその禁止と言う対応では、多くの経路が利用不可となって情報利用の有用性を著しく損なうことを示し、排中律を禁止する直観主義論理の採用により、データ利用の効率性、及び、多様なセキュリティポリシーの下での柔軟性を両立させつつ、情報漏洩を防止する方法を世界に先駆けて提案している。本論文は、今後、産学官協力の下にプロジェクトを立ち上げ、実装方法を検討すべき大型研究の理論的基礎と指針を示したものと言える。

Ⅱ. 論文審査結果の要旨

申請者は、１９８０年代後半から略２０年にわたり、一貫して本分野の研究を行い、４編の有査読論文、有査読国際会議論文、３編の著作（分担)、約７０編の発表論文、及び、投稿中査読論文等で成果を発表してきた。この間、申請者は、ＡＴＲにおいて研究を開始した後，東工大、中央大などにおいて多くの大学院学生・卒業研究生を指導しつつ、我が国においては、本分野の数少ない専門家として、研究を推進してきた。平成７年から１１年まで５年間にわたって推進された総務省の情報セキュリティ研究プロジェクトでは､余人を持って変えがたいとして参加を要請され、プロジェクトの活動に貢献した。

これまで、我が国では、一般に、情報漏洩に対する認識が低かったこと、及びデータベースが同一組織内に閉じていたことなどから、本分野の研究は広く注目されるテーマではなかったが、Web2.0、SNS、ダイナミック・コラボレーション、あるいはオープン・イノベーション等のキーワードで表される情報社会においては統合データベースの情報漏洩は企業などの組織の存続にも関わる課題となっている。この際、公開して差し支えない情報は可能な限り流通させると同時に、秘すべき情報の漏洩を防止するために、本論文は本質的貢献を果たすものである。

以上を要するに、本論文は、統合データベースの情報漏洩に対して有効な理論的枠組みと指針を示したものであって、情報学と情報社会の健全な発展に寄与するところが大きい。よって、我々は、本論文が博士（情報学）の学位論文として十分価値あるものと認める。

Ⅲ. 審査経過

本審査委員会は、2008 年 1 月 28 日に論文内容とこれに関連する事項について口述試問を行い、申請者が学位取得にふさわしい知見を持つものと判断した。