# 論 文 内 容 の 要 旨

博士論文題目

Computation Theoretic Approaches in Intrusion Detection and Access Control

（侵入検知とアクセス制御における計算理論的アプローチ）

氏 名　王 静

（論文内容の要旨）

本論文では，IDS（侵入検知システム）分割配置問題とHBAC（履歴に基づくアクセス制御）付きプログラムの検証問題という，システムセキュリティにおける二つの課題に取り組んでいる．本研究で用いている共通の方法論は計算理論である．IDS分割配置問題はグラフ理論における特殊なマッチング問題とみなすことができる．一方，HBACプログラムの検証問題の考察には，形式言語理論，とりわけ，有限オートマトンと文脈自由文法の理論を用いている．本論文の具体的内容は以下の通りである．

第２章では，まず，一般化 IDS 分割配置問題が定義されている．この問題を効率良く解くのは困難であるため，工学的見地から単純化 IDS 分割配置問題が導入されている．以降，後者を単に IDS 分割配置問題と呼ぶ．ネットワークに分散配置される個々のIDSをプローブと呼ぶ．IDS分割配置問題とは，ネットワークトポロジーと攻撃シナリオが与えられたとき，IDSの検知能力を落とすことなく，各プローブの負荷の最大値が最小となるように，プローブの個数と各プローブの配置を決定し，攻撃シナリオを各プローブ用に分割する問題である．本論文では次の手順で IDS 分割配置問題が多項式時間可解であることが示されている．まず，IDS分割配置問題を重み付き２分グラフにおけるあるマッチング問題に帰着する．次に，後者を解く多項式時間アルゴリズムを与える．第２章では，関連する問題として，プローブ数最小化IDS分散配置問題がNP完全であることも示されている．

第３章では，Abadi と Fournet が導入した実行履歴に基づくアクセス制御付きプログラムの形式モデルである HBAC プログラムを定義している．そしてまず，HBAC プログラムの表現能力がスタック検査付きプログラムよりも真に大きいこ

とが示されている．次に，HBAC プログラムの検証問題が定義され，本問題が文脈自由言語の空判定問題に帰着できることが示されている．そして，本問題が一般には決定性指数時間完全であること，および，現実的な仮定の下で，多項式時間可解であることも示されている．さらに，検証問題の可解性を示す際に用いた手法を最適化するいくつかの手法が提案されている．これらの最適化法を実装した検証ツールを用いた検証実験により，実用的なHBACプログラムを効率よく検証できることが実証されている．

| 氏　名 | 王　静 |
|---|---|

（論文審査結果の要旨）

本論文では，システムセキュリティにおける重要なテーマである侵入検知技術とアクセス制御技術に関して，計算理論的アプローチから以下のような知見を得ている．

（１）侵入検知システム（IDS と略記）はイントラネット上のトラフィックを監視するネットワーク型と OS へのシステムコール等を監視するホストベース型に分類される．ネットワーク型不正検知 IDS では，ネットワーク上のメッセージ列を監視し，それがあらかじめ作成しておいた攻撃シナリオに適合したら警告を発する．監視のためには一般に複数の IDS が必要である（各々の IDS をプローブと呼ぶ）．本論文では，ネットワークトポロジーと攻撃シナリオが与えられたとき，各プローブの監視のための負荷の最大値が最小となるようなプローブの配置を求める，IDS 分割配置問題を定義している．そして，この問題を重み付き２分グラフにおけるマッチング問題に帰着し，後者に対する効率の良いアルゴリズムを与えることにより，IDS 分割配置問題が多項式時間可解であることを示している．

（２）近年，プログラム言語の実行系に汎用的なアクセス制御機構を包含し，それによってシステム運用の安全性を高めようという，いわゆる language-based security という考え方が注目されている．例えば JVM や C♯ などでは，呼び出し制御スタック中の各メソッドが十分なアクセス権をもつかどうかを動的に判定するスタック検査機構を提供している．Abadi と Fournet は，実行の終了したメソッドに対する検査が行えないというスタック検査の欠点を解決した，実行履歴に基づくアクセス制御法（history-based access control, HBAC）を提案し，C♯上での実装を行っている．本論文では，Abadi と Fournet の HBAC に対応する形式モデル HBAC プログラムを定義し，HBAC プログラムがスタック検査付きプログラムより表現能力が大きいことを示している．次に，HBAC プログラムの検証問題を「与えられたプログラム $P$ と正規言語で指定された検証性質 $\phi$ に対し，$P$ の任意の実行系列が $\phi$ を満たすか」と定義し，この問題が一般には決定性指数時間完全であること，および，妥当な仮定のもとで多項式時

間可解であることを示している．さらに検証ツールを試作し，文脈自由文法の簡単化に基づく on-the-fly 型高速化法により，実用規模のプログラムに対しても効率的に検証が可能であることを実証している．

以上の通り，本論文で提案する手法と得られた結果は，情報セキュリティ，とりわけ，効果的で信頼性の高い侵入検知やアクセス制御を実現するための設計検証技法を与えており，博士（工学）の学位論文として価値あるものと認める．