審査の結果の要旨

論文提出者氏名　アブデュラハマン　エム．エス．アルハルビ

本論文は，「ENHANCED TECHNIQUES FOR DETECTION, PRIVACY PRESERVATION, AND ARCHITECTURE IN INTRUSIONS DETECTION SYSTEMS（侵入検知システムの検出能力・プライバシ保護・アーキティクチャ強化技術）」と題し，現在の侵入検知システム（IDS）の問題点の解決およびIDSの応用について論じたものである．現在のIDSの多くには，低い検知率，高いフォールスアラーム率，ユーザのプライバシ侵害，分散IDSにおいてIDS間通信の安全性が保証されない，などの問題がある．本研究ではこれらの潜在的な問題を明らかにし，それらの解決法を提案している．さらに，セキュリティプロトコルの保護に対するIDSの応用について論じている．論文の構成は「Introduction」を含め６章からなる．

第1章は「Introduction（序論）」で，本研究の背景を明らかにした上で，研究の動機と目的について言及している．

第2章は「Intrusion Detection and Alarm Reduction（侵入検知およびアラーム削減）」と題し，IDSに関する大きな技術的課題として，アラートの管理を取り上げている．膨大なアラートから真のアラームを特定し，高い確率で侵入検知を行うことはIDS普及のための基本的な課題となっている．本章では，パターン検知にデータマイニングの手法を用い，それまでのアラームの振る舞いに基づいて，フォールスアラーム率を減少させる方法を提案している．

第3章は「IDS Users' Privacy（IDSユーザのプライバシ保護）」と題し，IDSを用いる際に問題となるユーザのプライバシ保護について論じている．IDSはユーザの行動についてのデータを収集・解析することにより，コンピュータネットワークを保護しているが，収集したデータはユーザのプライバシの脅威となり得る．本章では，IDSシステムに，暗号技術に基づく匿名性失効可能な匿名技術を導入することにより，IDS監視下にあるネットワークのユーザのプライバシを保護する方法を提示している．

第4章は「Distributed Intrusion Detection System Architecture（分散侵入検知システムアーキティクチャ）」と題し，多様なIDSを含む分散IDSシステムにおける情報セキュリティの問題について論じている．このようなシステムにおいて個々のIDSが持つデータを保護し，不正なコマンドが実行されないようにするために，本章では，個々のIDSが相互に安全な通信を行える新しいアーキティクチャを提案している．

第５章は「Security Protocols Dynamic Protection as an Application of IDS（IDSの応用としてのセキュリティプロトコルの動的保護）」と題し，アノマリーIDS（正常な状態との差を検知するIDS）の応用として，セキュリティの動的解析に基づいたセキュリティプロトコルの検証方法を提案している．従来，セキュリティプロトコルの評価としては主として形式的（数理的）検証方法が用いられている．この方法はオフラインの状況でセキュリティプロトコルの静的評価を行うものであるが，本章では，アノマリーIDSの応用として，セキュリティの動的解析に基づいたセキュリティプロトコル検証方法を提案している．この方法は様々の侵入検知手法を用いて，セキュリティプロトコル実行時における変則的な振る舞いを自動的に検知しようというものであり，新たなセキュリティプロトコル検証方式として期待される．

最後に第6章は「 Conclusion（結論）」で，本研究の総括を行い，併せて将来展望について述べている．

以上これを要するに，本論文では，IDS の基本的課題に対し，有効な解決策を提示するとともに，IDS 技術の新たな応用を示したものであり，電子情報学，特に情報セキュリティ工学上貢献するところが少なくない．

よって本論文は博士（情報理工学）の学位請求論文として合格と認められる．