修士論文の和文要旨

大学院情報システム学研究科　博士前期課程　情報システム運用学専攻		
氏　名	向坂 真一	学籍番号 0552032
論文題目	論理・時間・地図情報を統合的に視覚化した 内部ネットワーク監視システム	

要　旨

近年コンピュータネットワークの普及に伴い大学や企業のネットワークも大規模化した．この傾向は無線LANの普及などによってさらに進んでいる．その一方でウィルスや不正アクセス，情報漏洩が社会問題になっている．そのため各計算機にファイアウォールやウィルス対策ソフトの導入が進んでいる．しかしながら内部ネットワークにセキュリティ対策を取っていない計算機やウィルス定義ファイルを更新していない計算機の混入，未知の攻撃を受ける可能性があるため，内部ネットワーク監視が行われている．

従来よく研究されてきた広域監視とは異なり，内部ネットワーク監視は内部ネットワークから外部ネットワークへの攻撃を最も危険な攻撃として警戒している．その監視手法は侵入検知システム(IDS)のログ等を見ることである．IDSのログには攻撃ではないものまで記録されているが，異常時には急激に増えることが多く，時間あたりの攻撃量をカウントすることで早期に発見できる．また，ログでは計算機を論理情報であるIPアドレスとして表現するが，それは実際の計算機の位置とは異なる．これらの対応関係は対応表を見たり経験を使ったりして解決しているのが現状である．

このように実際のネットワーク管理では論理情報・時間情報・地図情報の情報を用いて判断している．そこでこの三種類の情報を統合的に視覚化することにより管理者の負荷を低減させるだけでなく，今まで発見できなかった異常を発見し，経験の浅い新しい管理者も適切に判断できるようになると考えられる．

また，論理情報には内部ネットワークだからできるポートスキャンによるネットワーク調査の結果を組み合わせることで攻撃の有効性を適切に判断できると考えた．これらの条件を満たすように，立方体の内面に論理・時間・地図情報を配置し，それらの関係も視覚化した．また，実際の管理ではgrepコマンド等による様々なフィルタリングによって必要な情報を選別しているためフィルタリングのための対話性が必要である．そのためGUI，CUIの両方で操作できるシステムにした．

このシステムを電気通信大学情報基盤センターで実際に運用した．ボットネット，FTPへの攻撃等の監視に効果があった例を挙げた．さらにハニーネット監視へ応用した例も挙げた．

本システムを他の内部ネットワーク監視システムと比較を行った．地図情報との統合，ネットワーク調査結果の利用，対話的なフィルタリングにおいて優れているが，使用できるネットワーク規模に制限がある．

この大規模内部ネットワーク監視システムは更に発展させることによってハニーポットの視覚化以外に企業の内部ネットワーク監視やISPにおける監視，無線LANの監視に応用できると考えられる．