平成24年度　情報工学コース卒業研究報告要旨

高倉 研究室	氏　　名	三　木　太　一
卒業研究題目	IPv6アドレス監視システムを用いたネットワーク異常の早期検知手法	

IPv6においては，プロトコルの仕様に起因する様々なセキュリティ問題が指摘されている．セキュリティインシデントに対処するためには，IPアドレスの定期的な付け替えを考慮し，どの端末がどの時間にどのIPアドレスを使っていたかを的確に特定する技術が今まで以上に重要となっている．名古屋大学ではこの問題に向け，Monetと呼ばれる追跡・監視システムを構築している．しかし，Monetが取得するデータは膨大なものであり，ネットワークにおいて異常なパケットが存在することを見つけたいという目的を持っているネットワーク管理者にとって，この大量のデータから実際にそのようなセキュリティインシデントに繋がる恐れがある異常なパケットを探し出すことは大きなコストがかかるのが現状である．

そこで，本研究ではMonetが収集した情報を統合し，異常なパケットを検知し，ネットワーク管理者に提示することで，ネットワークの異常を早期に察知し易くなるよう支援する手法を提案した（図1）．本研究では，IPv6におけるネットワーク上の脅威として，IPv6アドレス取得の妨害，ルータへのなりすましによるMan-In-The-Middle攻撃を取り上げて，異常検知手法を提案した．これらの攻撃は，危険性の極めて高い攻撃となりうる一方，簡単に実現できるためIPv6ネットワークの安全性に影響を及ぼすことが懸念されている．

提案手法に対する評価実験を行うために，実際に名古屋大学ネットワークのL3スイッチが処理するパケットからMonetが取得した，1ヶ月分のデータに加え，実験用に被害者ノードと攻撃者ノードからなるネットワークを構築し，被害者ノードを妨害するプログラムを実行することにより得たデータを用いて提案手法を評価した．その結果，名古屋大学ネットワークおよび実験用ネットワークにおいて被害者ノードを妨害するパケットを検知することができた．本研究では過去のデータを対象に実験を行ったが，リアルタイムでMonetのデータを監視することで，より早期にネットワーク管理者へ攻撃者ノードの存在を知らせる機能の導入及び本研究で取り上げなかった脅威にも対応し，検知できるようにすることが今後の課題である．

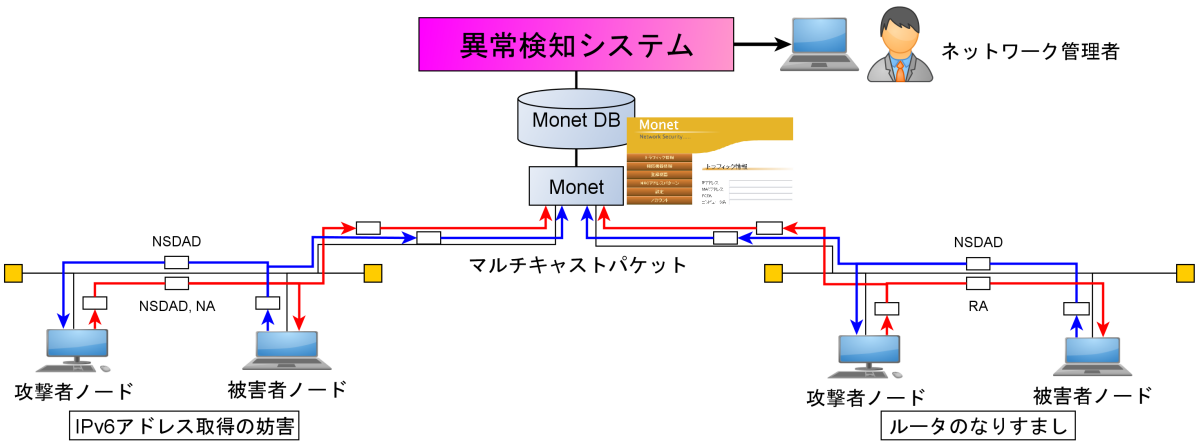

図1：Monetデータを利用した異常通信検知