称号及び氏名	博士（工学）　川橋　裕
学位授与の日付	平成 25 年 3 月 31 日
論　　文　　名	「組織内ネットワークにおけるネットワーク運用管理技法に関する研究」
論文審査委員	主査　戸出　英樹
	副査　吉岡　理文
	副査　宮本　貴朗

論文要旨

インターネットおよびイントラネットを構成するネットワーク技術は，階層モデルを採用している．端末間や端末とサーバ間の通信で，通信内容を指す情報は，物理層からアプリケーション層までを，フレーム，パケットおよびデータなどの形式で相互に交換される．したがって，ユーザ利用およびアプリケーション開発では，各層の仕組みや状況を把握，理解する必要がない．しかし，ユーザが理解する障害は「つながらない」と体感することから始まる．そのため，ネットワーク運用管理には，各層における問題の切り分けなど，様々な面での技能を必要とする．

1990年代半ばより，全世界でインターネットを利用した教育，産業，ビジネスおよび研究が著しく発展してきた．ネットワークにおいては，メトロネットワークや拠点間接続，トンネル技術および経路制御などが急激に進歩し，複雑化している．コンピュータシステムにおいても，クラウドなどネットワーク技術を前提とした仕組みが同じく複雑化している．近年はサービスの分野で，セキュリティ，プライバシ，フォレンジックおよびポリシのように，ネットワーク運用管理全体が複雑なしがらみによって構成されるようになった．

本来,ネットワーク運用管理の困難さは,一方でユーザの利便性を確保しつつ,他方で機密性,耐障害性（事前防御と事後対応）などの完全性を高めるための程度問題に帰結する．一般的に,ビジネスや行政分野では,制限事項を増やすことで業務要員の利便性を低減させている．しかし,学術研究機関などでは研究教育業務に支障を来すため,制限事項に頼らず運用管理を支援するシステムと，支援する体制が必要となる．

上記の支援システムに関する例として，近年では事前防御が困難で，事後対応でもリスクを回避し難い問題が2つ顕在化している．1つ目はP2P(Peer to Peer)ファイル共有ソフトウェア利用による著作権侵害であり，2つ目はDoS(Denial of Service:サービス妨害）攻撃である．前者は政府機関や民間機関によって，交換するファイルの多くが違法コンテンツであると判明している．後者は攻撃対象のリソース枯渇を狙う手法である．これらは正規の手順に沿っているため検知と対応が困難とされている．

前述の支援体制に関する例として，運用管理に従事する管理者の不足があげられる．運用管理には，知識や技術に偏らず，これらを技能として総合的に習得，発揮する人材が必要である．しかし，総合的な技能は運用管理の経験によって習得できるため，知識や技術を積み重ねた上で，より現実に近いシミュレーションや演習を実現する支援システムと運用体制が必要である．

本研究は，上記の運用管理支援システムと運用管理人材育成支援システムの 2 部より構成される．第 2 章と第 3 章では，新たな運用管理支援システムとして，それぞれファイル共有ソフトウェア利用検出システムと，DoS 攻撃に対する透過型防御システムについて述べる．さらに第 4 章では，運用管理人材育成支援システムとして，実際の運用管理を演習形式で実施する環境と運用法について述べる．これらは筆者らが全国の学術機関に対して実施してきた情報危機管理コンテストや，文部科学省の先導的 IT(Information Technology)スペシャリスト育成推進事業の一環で始めた IT 危機管理演習で活用され，現在も継続している．

以下に，各章における要旨を述べる．

第2章では，トラヒックパターンに基づくファイル共有ソフトウェア利用検出システムについて述べる．

ファイル共有ソフトウェア利用を検出する手法には，一般的にクローリング型とゲートウェイ型，およびパケットキャプチャ型がある．前者の2つにおいては，調査に大規模なシステム導入が必要な点や，シグネチャを継続的に解析し提供する必要性，およびスループット低下の懸念などがある．したがって，本研究ではパケットモニタ型を採用する．ファイル共有ソフトウェアの多くは，膨大な数の通信相手先(ピア)を必要とするか，初期のピアやファイルの所在をインデックス化して固定する形態に大別される．既存研究では，WinnyやShareなど挙動が顕著なファイル共有ソフトウェアに限定して検出するとともに，Skypeなど有用なファイル共有ソフトウェアを誤検知する場合が多い．

本研究では，ピア数とインデックス先の特定に加えて，TCP(Transmission Control Protocol)送信ポート番号の連続性やUDP(User Datagram Protocol)送信ポート番号の同一性などを指標として採用する．同一の端末内でさまざまなアプリケーションが稼働する場合，OS（Operating System）上で規定された短命ポート（Ephemeral Port）により送信元ポートが選定される．このため，同一端末内での複数アプリケーション利用を区別できる．これは，冒頭に示した階層構造

の中で，アプリケーション層とネットワーク層のみでファイル共有ソフトウェアの挙動を捉えるだけでなく，他の層を含めてトラヒックをパターン化することが，誤検知を回避するだけでなく，さまざまなファイル共有ソフトウェア利用の検出に役立っている．

上記を提案手法として，和歌山大学の対外線利用下で実験した結果，全15種類のファイル共有ソフトウェアを検出し，Skypeを誤検知しなかった．

続いて第3章では，ソースアドレスルーティングによるDoS攻撃等への防御システムについて述べる．

DoS攻撃によるサービス妨害は，近年業務妨害だけでなく，脅迫や詐欺などの事件として多発している．これはDoS攻撃の検知と回避が困難であることに起因する．既存研究では，DoS攻撃を受けるサーバでの検知手法や，ACL(Access Control List)による回避策が検討されてきた．しかし，一般アクセスを保持しつつACL機能を十全に提供するには，相当なハードウェア要件が求められる．

本研究では，サーバごとにDoS攻撃と認定する閾値を変更し，ACLではなく送信元IP(Internet Protocol)アドレスを用いた経路制御によって，対外接続部で統括して防御するシステムを提案した．冒頭に示した階層構造では，上位になるほど一般的に処理の負荷が高くなる．経路制御はACL機能より下位で実装されているため，DoS攻撃への耐性が高いといえる．一方で，本来経路制御は宛先IPアドレスに対して実施されるため，攻撃対象のサーバを指定しては，一般アクセスも遮断することになる．提案システムでは，送信元IPアドレスに対して経路制御を施し，DoS攻撃と認定されたアクセスのみをnullデバイスや他のIPアドレスに転送することで，負荷を低減しつつ一般アクセスを保護している．

上記に加えて，提案システムでは，転送先に代理応答サーバを指定することで，DoS攻撃の一種であるF5リロード攻撃に対して攻撃認定されたことを通知する．これは提案システムで設定した閾値によるfalse-positiveを改善する機能である．そのため，代理応答サーバはTCPパケットによるリクエストをステートレスに応答し，返信内容を簡素化することで負荷を低減している．さらに，本提案システムはブリッジ型で構築しているため，既存のネットワーク構成を変更することなく導入が可能である．

本研究では，本提案システムの動作を実験環境下で検証した．和歌山大学の日中平均である6,000pps(毎秒パケット数)の状況下で，50,000ppsのDoS攻撃(SYN Flood)を発生させた場合の一般アクセス(HTTP,DNS)の保護，および攻撃対象サーバと本提案システムの負荷について，良好な結果が得られた．さらに，代理応答サーバの返信能力として，DoS攻撃(リロード攻撃)に対して，5,000ppsまで完全に返信することを確認した．当該機能はfalse-positiveの把握と改善に対して有効であり，攻撃認定の閾値周辺にある一般アクセスへの対応に十分な能力であるといえる．

第4章では，運用管理人材育成支援システムと同システムの運用法について述べる．

2010年以降，日本では日本版CTF(Capture The Flag)として，互いに侵入と防御を競うイベントが増えつつある．しかし，ネットワーク運用管理では，すべての障害が攻撃に起因するとは限らない．故障，ユーザの設定や使い方のミス，複合的な要因で単一の障害が発生する場合などがある．運用管理に必要な技能には，原因の特定に必要な切り分け手法によって上記を判定することや，原状回復を確認できること，およびユーザとの適切な情報交換など多様な能力が求められ

る．

筆者らは，2006年より情報危機管理コンテストと称して，全国の学術機関より参加チームを募って，上記技能の必要性を体感できる環境システムを構築，運用してきた．当該コンテストは，2009年より最優秀チームに経済産業大臣賞が授与されている．さらに，本提案システムは，2007年より文部科学省の「先導的ITスペシャリスト育成推進事業」における「IT-Keys：社会的ITリスク軽減のための情報セキュリティ技術者・管理者育成」のIT危機管理演習に採用され，現在も当該演習実施を継続している．

本提案システムでは，シナリオ方式を採用しており，提案システムを運用する運営側と，参加者や受講者など障害に対応する参加側が存在する．運営側は，攻撃を含むさまざまな要因で障害が発生するよう事前に設計，検証した環境下で，攻撃や苦情連絡を実施する．

運用管理の人材育成システムは，教育支援システムと近似する．シナリオ方式によって演習の流れを制御し，対応できない，対応が間違った参加側に対して，適切な対応修正を施す．一方で，開催ごとにシナリオを新規構築には負担がかかる．さらに，実施には大規模な設備が必要であり，参加側に会場まで来場させるには予算も必要となる．本提案システムでは，2009年よりASP(Application Service Provider)形式を採用し，コンテスト予選と演習において導入，実施している．

本研究では，本提案システムが他の類似のイベントと比較した定性評価と，コンテストや演習の実施を継続している実績から，他に類を見ない有効な運用管理人材育成システムであることを検証する．

第5章では，本研究で得られた結果を総括するとともに，今後の取り組むべき課題について整理する．

審査結果の要旨

本論文は，ネットワーク運用管理支援と同運用管理の人材育成支援において，レイヤモデルに基づき支援の内容を充実させることを目的として，検知が困難なアプリケーションや防御が困難な攻撃への対応と，遠隔利用で実際の運用管理に近似した演習環境について研究したものであり，以下の成果を得ている．

(1)　著作権侵害や利用制限の対象となる多様なファイル共有ソフトウェアが P2P（Peer-to-Peer）ネットワークを形成する初動を，従来の検知手法で採用されているパケット単位ではなく上位層であるフロー単位で捉えることにより，正しく判別する検知システムを提案・実装した．実ネットワーク環境において、現在研究されている最大数のファイル共有ソフトウェアの種類に対し，有用なファイル共有ソフトウェアと区別しつつ正しく判別できることを実証した．

(2)　インターネット上で提供する各種サービスを妨害する DoS(Denial of Service)攻撃について，これを上位層で遮断する従来手法に対し，下位層である経路制御によってパケットを破棄あるいは転送することで DoS 攻撃への高い耐性を有する対処システムを提案・実装した．新たに誤検知を修正するための代理応答機能を加えることで，運用管理上の問題点も解消した．さらに，代理応答機能の実行により，DoS 攻撃によるパケット数が収束するという事実を明らかにした．

(3)　事故前提社会に対応する情報セキュリティ技術者や管理者を育成することを目的として，地理的に分散した大学や組織などからの遠隔利用を可能にすることで演習会場や設備規模による制限を回避しつつ，競技形式の中で上記育成のための教育指導を実現することができる運用支援フレームワークを構築した．また，本フレームワークに対し，継続的な実施・運用の実績を通してその有用性を明らかにした．

以上の諸成果は，レイヤモデルを広く捉えることによって，さまざまな障害への事前防御と事後対応を可能とするための重要な知見を与えるとともに，運用管理に必要な，幅広い知識と技能を習得する人材育成についても有益な環境を提供したものであり，本分野の学術的・産業的な発展に貢献するところ大である．また，申請者が自立して研究活動を行うのに必要な能力と学識を有することを証したものである．