

(続紙 1)

京都大学	博士 (情報学)	氏名	大平 健司
論文題目	インターネット接続の低管理コストな運用に関する研究		
(論文内容の要旨) 本論文は、インターネットが重要な社会インフラとして利活用されている社会の現状を踏まえ、管理を分散し低コスト化しつつインターネット接続の可用性、到達性、安全性を向上させるための運用技術を提案しているもので、全5章から構成されており、それぞれの章の内容は以下の通りである。 第1章では序論として、本研究の背景と目的および全体の構成と各章の概要について説明している。 第2章では、インターネット接続を信頼関係のない他者に安全に提供できるようにするための、みあこネット方式と呼ぶ公衆無線インターネット接続サービス方式を提案し、評価考察を行っている。みあこネット方式では、公衆無線インターネット接続サービスにおける利用者認証の管理者と基地局の管理者の役割を分離し、基地局提供に伴う管理上の負担を軽減することで、自発的な無線インターネット接続サービスの提供を促しインターネットに接続できるところが広がるという意味での可用性の向上を実現している。 第3章では、家庭のような中小規模のネットワークが、複数の上流ISPとの接続を持つことで、負荷分散や耐障害性向上を図る技術である、複数アドレス型サイトマルチホーミングについて論じている。送信元アドレス依存経路制御を用いて、ホストによる送信元アドレス選択を経路選択に反映させることで、ISPが実施する流入フィルタリングの回避という課題を解決するアーキテクチャを提案し、実装上の複雑度を増やすことなくマルチホーミングによる冗長化・頑健化の利益を享受できるようにして到達性を向上させている。さらに、運用者の管理コストを低減するために、動的な送信元アドレス依存経路制御のためのサイト外経路広告プロトコル、およびサイト内でのIPアドレスの自動割り当てのプロトコルを提案し、評価考察を行っている。 第4章では、インターネット接続において未知の脆弱性を衝いた攻撃活動（ゼロデイ攻撃）が深刻化し対策が管理者の負担となっている状況を踏まえ、実ユーザのいないシステムを用いて攻撃を追跡・解析し攻撃対象などを特定する手法であるハニーポットについて論じ、広範な攻撃に対応可能な見破られにくいハニーポットを低管理コストで構築し運用する方法を提案している。提案方式では、攻撃状況に応じて待受け設定を自動的に変更し、またハニーポットが攻撃者により乗っ取られた場合でも観測・制御系ネットワークへの侵入を防ぐことで、管理者の負担とリスクを軽減している。これにより、ハニーポットを分散して設置することで広域での攻撃活動状況を低コストに把握できるようになり、インターネット接続の安全性の向上に貢献している。 第5章では結論として、第2章から第4章の各章で得られた結論と今後の課題について述べ、「インターネット接続の低管理コストな運用」の観点からの評価と今後の展望について述べている。			

注) 論文内容の要旨と論文審査の結果の要旨は1頁を38字×36行で作成し、合わせて、3,000字を標準とすること。

論文内容の要旨を英語で記入する場合は、400～1,100 wordsで作成し
審査結果の要旨は日本語500～2,000字程度で作成すること。

(続紙 2)

(論文審査の結果の要旨)

様々なサービスがインターネットに依存し、いつでも確実にインターネットに接続できることが求められつつある。本論文はインターネット接続の運用にかかる管理コストに着目し、「どこでも使えること(可用性)」「相手まで確実に届くこと(到達性)」「セキュリティ上の懸念なく使えること(安全性)」のそれぞれを、管理コストを増大させることなく向上させることを目的としている。具体的には、可用性について「公衆無線インターネット接続サービスみあこネット」を、到達性について「IPv6サイトマルチホーミングによる冗長化」を、安全性について「ハニーポットによるゼロデイ攻撃の早期検出」をそれぞれ題材として取り上げ、管理コストを分散化させることで導入時の初期コストや運用上の維持コストを削減する運用技術を提案している。

「公衆無線インターネット接続サービス」の研究においては、公衆無線インターネットの運用をセキュリティと管理コストの観点からモデル化して分類した点、ならびに、VPNを用いて利用者認証とアクセス提供の責任を分離することで、セキュリティを担保しつつ管理コストを分散し無線基地局設置者の負担を最小限にした、「みあこネット方式」を提案した点に独創性がある。提案方式に基づくサービスは、NPOによる実証実験を経て、現在は本学などで実際に広く利用されるようになっている点についても評価できる。

「IPv6サイトマルチホーミングによる冗長化」の研究では、家庭やSOHOなどの中小規模のネットワークにおいても、商用ISPが提供する一般的なインターネット接続を複数束ねることで、耐障害性や経路最適性の向上、さらには負荷分散をエンドホスト主導で行うことができるマルチホーミングのアーキテクチャを提案している点が注目される。提案アーキテクチャならびにその運用のための技術は、次世代インターネットプロトコルIPv6の家庭などへの普及そのものにも寄与する可能性があり、将来性を評価できる。

「ハニーポットによるゼロデイ攻撃の早期検出」の研究においては、ハニーポットを簡素化しその導入と運用にかかる管理上のコストとリスクを軽減するという着眼が、従来研究にはないユニークなものである。本提案方式の実装は2006年3月から現在まで京都大学および協力機関に分散して設置されている。その運用を通じ長期にわたって対象不明な攻撃活動を捕捉できており、提案方式の有効性が実証されている点も評価できる。

インターネットが重要な社会インフラとして利活用されている今日、インターネット接続の可用性・到達性・安全性の向上と運用にかかるコストの低減との相反する要求に対し、管理コストをエンドホストに近い側に分散させるというアプローチで、実応用に即した具体的な課題に対してその解決のための運用技術を示している点は意義深い。よって本論文は博士(情報学)の学位論文として価値あるものと認める。

また、平成22年6月9日に実施した論文内容とそれに関連した試問の結果、合格と認めた。

注)論文審査の結果の要旨の結句には、学位論文の審査についての認定を明記すること。
更に、試問の結果の要旨(例えば「平成 年 月 日論文内容とそれに関連した口頭試問を行った結果合格と認めた。」)を付け加えること。

Webでの即日公開を希望しない場合は、以下に公開可能とする日付を記入すること。
要旨公開可能日： 年 月 日以降