氏名	石橋勇人（いしばしはやと）
学位(専攻分野)	博士（情報学）
学位記番号	論情博第35号
学位授与の日付	平成14年7月23日
学位授与の要件	学位規則第4条第2項該当
学位論文題目	オープンアクセスシステムにおける不正アクセス防止方式に関する研究
論文調査委員	（主査）教授 金澤正憲　教授 髙橋豊　教授 北野正雄

論文内容の要旨

コンピュータおよび情報ネットワークの進歩は目覚しく，スーパーコンピュータから携帯型パソコンに至るまで，コンピュータはネットワークに接続されているのが通常である。さらに，インターネットにより世界中のコンピュータとの通信が可能な状態になっている。

大学のキャンパスにおいては，教育・研究活動を円滑に遂行するため，教職員から学生までの利用者が自由にアクセスできるための手段を提供したオープンシステム，あるいは，オープンスペースに設置されて誰でも接続できる情報コンセントを用意することが不可欠である。利用者がこのようなコンピュータネットワークを利用するに際して，単にネットワークへの接続性やQoS（Quality of Service）が保証されるだけでは不十分であり，セキュリティの確保が喫緊の課題となっている。

本論文では，オープンアクセスシステムでの利用者の認証機構，悪意のある利用者による不正なアクセスの試みをシステム的に防止する機構，および，電子メールにおける送信者詐称を防止する機構を提案し，実装して運用に供し，その有効性を明らかにしたものであり，全体で6章からなっている。

第1章は，本論文の序論であり，キャンパスネットワークにおけるオープンシステムの必要性とセキュリティ上の問題点について説明している。

第2章では，情報コンセントにおけるセキュリティについて今までに考案された方式について説明し，多数のコンピュータに対する管理上の問題点，悪意の利用者によるセキュリティの脆弱性，伝送効率の低下などの問題点を指摘している。

第3章では，コンピュータを情報コンセントに接続する際に，各コンピュータに与えられた識別子（IPアドレス，MACアドレス）を偽って情報（パケット）を発信するという不正アクセスを取り上げ，2つの識別子に情報コンセントハブのポート番号を導入した3つ組を導入し，これに利用者認証サーバにより許可された利用者のみの接続を許可することにより，不正が不可能である方式を提案している。これをLANAシステムとして実装し，チェックなどのためのオーバーヘッドを測定し，実用上問題がないことを確認している。

第4章では，教員，職員，学生などの身分によりアクセス制御を異なるようにするため，利用者認証でアクセス権に基づきIEEE802.1QによるVLANのタギング機能を利用した方式を提案している。これをLANA2システムとして実装し，LANA2での所要時間（オーバーヘッド）が極めて小さいことを確認するとともに，運用に供して有効であることを実証している。

第5章では，アプリケーションレベルの不正アクセスであるメールの送信者詐称問題をとりあげ，各種認証サーバ（利用者認証，IPアドレス保持機能）を導入することにより，詐称されたメールのヘッダ部に利用者の正規のメールアドレスを付加することで詐称を実際上防止できる方式を提案するとともに，実際のシステムで運用して3年以上経過し，有効性を検証している。この方式は，利用者側のソフトウェアを変更する必要がなく，オーバーヘッドも実用上問題ない範囲であることを確認している。

第6章は結論であり，本論文で得られた知見を述べている。

論文審査の結果の要旨

本論文は，コンピュータネットワークサービスへ様々な利用者がアクセスするために使用するオープンアクセスシステムにおける不正アクセス防止の方式を提案し，実際のシステムにインプリメントし，業務レベルの運用を行い，その有効性を明らかにしたものであり，得られた成果は以下のようにまとめられる。

(1) オープンアクセスシステムでは，利用者の認証に加えて，悪意のある利用者による不正なアクセスの試みをシステム的に防止する機構が特に重要である。事前に登録された正規の利用者のみがオープンアクセスシステムの情報コンセントへ接続でき，かつ，IPアドレスとMACアドレスの偽造による不正アクセスに対して，IPとMACアドレスおよびポート番号の3つ組による管理方式を提案した。さらに，LANAシステムとして実現し，様々な利用者が立ち代り入れ替わり情報コンセントを利用してもセキュリティが保たれることが明らかになった。

(2) 利用者の属性によってネットワークへのアクセス権が異なるのが通常である。利用者認証で判明するアクセス権に基づき，最近のスイッチングハブに標準的に装備されているIEEE802.1Qに則ったVLANタギング機能を利用した方式を提案した。上述の3つ組の考え方において，VLAN識別子をポート番号に相当する識別子として利用し，この結果，各パケット単位に利用者を識別できる方式を考案している。即ち，パケットレベルにおいて利用者ごとの柔軟な制御が可能となり，LANシステムを拡張したLANA2システムとして実現し，運用され，有効性・実用性を明らかにした。

(3) アプリケーションレベルの不正アクセスとしては，電子メールが大きな問題であり，その一つとして発信者詐称問題がある。発信される電子メールをIPフィルタにより，必ず認証サーバ（利用者認証，IPアドレス保持機能）を経由させ，認証された利用者と電子メールの差出人欄とをチェックし，詐称されている場合は，メールヘッダに正規の利用者情報として付加する方式を提案している。実際の大規模なメールシステムに実装し，1年以上運用を行い，有効性・実用性を明らかにするとともに，メールクライアントに修正を加える必要がないことを確認した。

以上のように，本論文は，自由な接続が特徴のインターネットにおいて最近大きな社会的問題となってきたオープンアクセスシステムにおける不正アクセスの防止方式において先駆的研究であり，理論的発展に貢献するとともに，実用技術を開発したものであり，学術上，実際上寄与するところが少なくない。

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14年5月23日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。