【120】

氏　名（本籍）	**鈴　木　真　一（愛 知 県）**
学 位 の 種 類	博　　士（工　　学）
学 位 記 番 号	博　甲　第　3952　号
学位授与年月日	平成 18 年 3 月 24 日
学位授与の要件	学位規則第 4 条第 1 項該当
審 査 研 究 科	システム情報工学研究科
学 位 論 文 題 目	**分散計算環境におけるアクセス制御に関する研究**

主　査	筑波大学教授	理学博士	板　野　肯　三
副　査	筑波大学教授	工学博士	海老原　義　彦
副　査	筑波大学教授	博士（理学）	加　藤　和　彦
副　査	筑波大学助教授	博士（工学）	新　城　　靖
副　査	筑波大学助教授	博士（工学）	満　保　雅　浩
副　査	豊橋技術科学大学助教授	博士（工学）	廣　津　登志夫

論　文　の　内　容　の　要　旨

分散計算環境とは，複数の計算機が LAN（Local Area Network）により結合され，単一の管理者により統一的に管理されている計算環境である。LAN は，ルータにより外部のネットワークに接続されている。このような分散計算環境は，企業や教育現場で広く普及している。

このような分散計算環境においてセキュリティを確保し安全に運用するためには，管理者にとってアクセス制御の設定が重要な仕事になっている。アクセス制御の設定は，センシティブな情報を操作するためミスが許されず，管理者にとって重たい作業になっている。この論文では，この分散環境におけるアクセス制御の問題を分析し，根本的には次の 3 つに起因していると主張している。

(1) IP アドレスとユーザ，または，IP アドレスとサービス（アクセス制御の対象）の対応関係を把握することが困難であること。

(2) アクセス制御リストに基づく方式では，アクセス権限の一時的な変更や委譲に必ず管理者が介在すること。

(3) サービスを提供するプログラムを実行するために，利用者認証と特権（root 権限）が必要であること。

問題 (1)，および，(2) を解決するために，著者は，インターネットで使われている名前サービスである DNS（Domain Name System）のキャッシュ・サーバを利用する方法を提案している。システム管理者は，DNS サーバにアクセス制御のポリシーを記述する。この時，サーバの名前や利用者の名前など文字列でポリシーを記述することができる。著者は，DNS に対して TSIG（Transaction Signature）と呼ばれる標準化された技術を活用することで，利用者の名前を DNS サーバに送る。DNS サーバは，要求に含まれた利用者の文字列を使い，同じく文字列で記述されたポリシーを評価する。このように文字列のレベルでアクセス制御を完遂することで，問題 (1) を解決している。ただし現在は，アクセス制御の対象はルータの外側のサーバに限定されている。問題 (2) については，DNS サーバに，サーバをアクセスするためのケーパビリティを発行させることで解決している。ケーパビリティは，他人に渡すことができるので，管理者の手を煩わ

せることなく一時的にアクセス権を渡すことができる。これは教育現場や協調作業において有効に活用できる。

提案手法は，BIND9 サーバ，Linux カーネル，Linux 上のライブラリを修正することで実現している。実験により，160 台程度のクライアントを含む分散計算環境において実用的な速度で提案手法が実現できることを示している。

問題（3）を解決するために，クライアント・プロセスの権限（UID と GID）をサーバ・プロセスに送り，サーバ・プロセスの権限をクライアント・プロセスのものに変更する仕組みを提案している。サーバ・プロセスは，クライアント･プロセスと同一の権限で動作するので，従来のオペレーティング･システムが持っているアクセス制御の仕組みをそのまま利用することが可能である。従来，権限変更には特権が必要であったが，提案手法ではこれを不要にしている。これにより，サーバを特権なしに安全に利用することが可能になっている。提案手法は，Linux カーネル，inetd スーパーサーバ，PAM モジュール（拡張可能なユーザ認証モジュール）を修正する形で実現している。

審 査 の 結 果 の 要 旨

アクセス制御に DNS を利用している点，および，ケーパビリティに基づくアクセス制御の有効に利用している点が評価できる。権限変更機構は，分散型オペレーティング・システムの軽い実装方式であるとも位置づけることができ，この分野における貢献も認められる。また，現在広く普及しているオペレーティング･システムである Linux において利用可能になっていることから，有用性が高いと言える。

よって，著者は博士（工学）の学位を受けるに十分な資格を有するものと認める。