（ 続紙 1 ）

京都大学	博士（情報学）	氏名	近藤　誠一
論文題目	ロールベースアクセス制御拡張モデルと 異種分散システム適用における設計・評価に関する研究		

（論文内容の要旨）

官庁，企業等の組織体における機密情報漏えい防止，コンプライアンス対応として，アクセス制御管理が重要視されている．組織体で定められたアクセス制御ポリシを実践するため，ロールベースアクセス制御(RBAC)モデルが主流となっている．RBACモデルを大規模異種分散環境に適用する際の課題として，以下の点に注目した．

(1) 利用者，アクセス制御対象の変化を，広域に分散された個別システムへ速やかに反映．

(1-1) 人事異動，組織変更等の利用者，アクセス制御対象の変化への迅速な対応．

(1-2) 行為実行後のログを，過去のアクセス権変化と整合性をとった監査．

(1-3) ITシステム／非ITシステムが混在するシステムへの反映．

(2) 種々の異なるRBACモデルを適用したシステム共通の総合的な定量的リスク解析．

(3) (2)の評価をシステム構築前の設計段階で行う手法の確立．

これらの課題解決のため，本研究では，以下の提案と評価を行った．

(1) 大規模企業向けRBAC拡張モデル

大規模企業特有の組織構造の変化への対応を迅速に行うために，アクセス制御情報を集約して全体統合を行う以下の3種類の拡張モデルを提案した．

(1-1) ルールベース階層組織RBACモデル

人事システムと連動した運用管理効率化を実現するため，日本式の階層型組織情報をロールから独立させた構成とし，組織構造を要素とするルールを実行時に解釈するモデルを提案した．その結果，一般的な企業構造であるセキュリティ管理部門と人事部門の操作範囲を一致させ，人事異動時の運用コスト削減を図った．また，本モデルを採用した実システムを用いて実行時のルール解釈のオーバヘッドを測定し，応答時間，スループットの差異が5%以内で，実用上問題ないことを示した．

(1-2) 世代管理RBACモデル

情報漏えい防止対策として，行為実施前のユーザ認証・アクセス制御と，行為実施後のログの監視・監査・分析の整合性をとったアイデンティティ・アクセス管理方式について示した．RBACモデルを構成する各情報の変更履歴を利用した多バージョン並行制御による世代管理RBACモデルを新たに提案し，それを用いた監査ログトラッキング手法について示した．世代管理の方式として，ディレクトリ変更時に静的に作成する方式と，変更履歴をもとに参照トランザクションが必要とする部分のみ，動的に生成する方式を示した．(1-1)で与えたユーザ情報とセキュリティ情報を分離して論理式で関連づける階層組織RBACモデルを採用することにより，頻繁に人事異動が行われる企業，官公庁等の組織において，継続的なログの監査を行う場合に有用であることを示した．

(1-3) 代替ユーザRBACモデル

RBACモデルの入退室管理装置，キャビネット等の非ITシステムへの適用と，ICカードに代表される認証デバイスを利用した企業情報セキュリティへの適用モデルを示し

た．提案した代替ユーザを付加したRBACモデルでは，運用，セキュリティの問題で更新頻度の少ないシステムに対して，変更管理を局所化することを可能とした．また，代替ユーザを導入することによって新たに生じる実ユーザと代替ユーザの設定制約の自動化，実ユーザを用いたログの鑑査の実現方式を示した．これらの方式は，一般の動的職責分掌のセッション設定，ログ監査のためのアイデンティティの変更履歴管理に応用することが可能である．

(2) RBAC拡張モデルの異種分散システム適用における定量的リスク評価手法

さまざまなRBAC拡張モデルを適用したシステムに共通な定量的評価基盤を定め，具体的なシステム固有の情報を代入して比較評価できる手法を考案した．評価基準として，ポリシに違反している時間に注目し，総合的な角度でこの時間の評価を可能とした．さらに，セキュリティ違反，機会損失，システム管理コストをトップ事象として作成した故障木を用いた企業レベルでの総合的な定量的解析手法を提案した．実システム性能測定データをもとに，(a) RBAC拡張モデル，およびプラットフォームの選択，(b) 提案モデルの優位性の提示，(c) 許容時間を考慮した解釈に効果があることを示した．

(3) RBAC拡張モデルの異種分散システム適用におけるモデル駆動設計手法

(2)で提案した実システム評価に加えて，システム開発の上流段階において，脅威となる時間に注目した設計手法を提案した．RBACモデルの構成要素まで細分化してその動作と時間情報を与えることによって，遅延によって生じる脅威時間を設計段階で評価可能とした．シミュレーション可能なRBAC性能評価モデルを定義し，(1-2)で提案した世代管理RBACシステムを題材に，提案した方式を用いた解析を行い，実システム性能測定データをもとに，シミュレーション結果を加えて，(a) RBAC拡張モデル，およびプラットフォームの選択，(b) セキュリティ違反，機会損失の許容範囲内でのスケジュール設計に効果があることを示した．

（続紙 ２ ）

（論文審査の結果の要旨）

本論文は大規模組織体を対象とした統制型のアクセス制御管理を扱っている．アクセス制御はセキュリティ分野における中核の技術であり，また，コンプライアンス対応として必須の項目であることを考えると，本論文の対象である技術の適用範囲は広い．

大規模企業向けロールベースアクセス制御(RBAC)拡張モデルでは，人事異動等の変化に対して迅速に対応する組織階層を利用したルールベースアクセス制御モデル，行為実行履歴と過去のアクセス権を照合した監査を実現するアクセス制御情報の世代管理モデル，IT/非ITシステム混在システムでのアクセス権の同期に有効な代替ユーザを導入したモデルといった新たなRBAC拡張モデルを提案している．これらは，RBACモデルを適用した実際のシステムにおいて抽出された課題に着目して考案した実用性の高いものである上に，新規性の高いものである．また，実システムに適用して良好な結果を残しており，提案モデルの有効性を具体的に示した点も評価できる．

RBAC拡張モデルの異種分散システム適用における定量的リスク評価手法では，新たにポリシ違反の時間的脅威を評価尺度とした総合的な定量的解析手法を提案しており，異なるモデル間の比較，および異なるモデルを組み合わせたシステムの評価に有用であるという点で評価できる．また，具体的な方式として，故障木を利用した企業レベルでの総合的なリスク評価方式を与えており，提案手法の有効性を示した点も評価できる．

RBAC拡張モデルの異種分散システム適用におけるモデル駆動設計手法では，設計時に時間的脅威の評価を行うためのシミュレーション可能な手法の提案を行っている．本方式は，RBACモデルの構成要素とその動的振る舞いを同時に定義して時間的脅威を設計時に評価可能とした点で，新規性が高いものである．さらに，UMLに実時間プロファイルを加えたモデル駆動設計手法を提案して市販ツールにてシミュレーション可能であることを実践的に示し，設計コストの低減，誤りの混入回避などに対する有効性を示した点も評価できる．

このように，本論文は，大規模組織体を対象とした統制型のアクセス制御管理に関し，新たなロールベースアクセス制御拡張モデルと異種分散システム適用における設計・評価手法の提案を行ったものであり，アクセス制御管理の実システムにおける課題を抽出しその解決法を新たに提案し有効性を検証した点で研究の新規性と有用性が高く評価される．

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２３年４月１８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．