氏名	朝倉　義晴
学位の種類	博士（応用情報科学）
学位記番号	博情第７号
学位授与年月日	平成２２年３月２４日
学位授与の要件	学位規則第４条第１項該当（課程博士）
論文題目	情報システムにおけるアクセス制御ポリシー設計手法の研究
論文審査委員	（主査）教授　中本　幸一
	（副査）教授　白川　功
	（副査）教授　力宗　幸男

学位論文の要旨

近年，ウィルスや悪意あるアプリケーションからコンピュータ上の情報やコンピュータシステムを保護するために，セキュリティ技術の重要性がますます高まっている．このような技術として，アクセス制御とリソース使用量制御が挙げられる．アクセス制御は，サブジェクト（例えば，プロセス）にオブジェクト（例えば，ファイル）へのアクセスのための適切な特権を認可することで，サブジェクトによるオブジェクトへの操作（例えば，読み込み）を制御する技術である．リソース使用量制御は，プロセス毎の使用可能なリソース量（例えば，メモリ量）を制御する技術である．アクセス制御やリソース使用量制御は，アクセスの可否やリソースの使用の可否の判断基準となる規則（ポリシーと呼ぶ）に従い動作する．

アクセス制御を適切に運用するためには，ポリシーを適切に設計する必要がある．しかしシステム管理者が，多くのサブジェクト，オブジェクト，操作に関して適切なアクセス制御ポリシーを設計することは容易ではない．本研究では，ポリシーの設計を容易にするために，ロールベースアクセス制御（RBAC）のモデルの 1 つであるロールグラフを拡張した拡張ロールグラフを提案した．RBAC では，オブジェクトにアクセスするための特権をロールに関連付け，サブジェクトにロールを割り当てることで，アクセスを制御する．ロールグラフは，ノードがロールを表し，辺がロールの継承関係を表す，有向非循環グラフであり，ロールの階層構造（ロール階層，ポリシーに相当する）を表現するモデルである．ロールグラフは推移簡約であり，冗長な辺や冗長な特権を持たないため，RBAC の運用フェーズにおけるロール階層の記述手段に適している．しかし，ロールの集合に対してグラフの形状が一意に定まるためにロール階層の多様性がなく，ロール階層を設計するときの記述手段には適していない．拡張ロールグラフは，ロールの集合に対して多様なグラフの形状をとることができるため，RBAC の設計フェーズにおけるロール階層の記述手段に適しており，ポリシーの設計を容易にできる．

本研究ではさらに，拡張ロールグラフ間の等価関係を定義し，任意の拡張ロールグラフ

は等価なロールグラフに変換可能であることを，拡張ロールグラフを等価なロールグラフに変換する等価変換アルゴリズムを示すことで証明した．等価変換アルゴリズムを用いることで，拡張ロールグラフを用いてロール階層を設計し，等価なロールグラフに変換した後にコンピュータに適用できる．この手法により，RBAC の設計フェーズと運用フェーズに適したロール階層の記述手段を利用できる．

一度ロール階層を設計した後でも，コンピュータの運用環境が変化（サブジェクトやオブジェクトの追加，削除などの変化）した場合，ロール階層を再設計しなければならない．本研究ではロール階層の再設計を容易にするために，次の 2 点の研究を行った．

まず 1 点目として，ロールグラフで記述されたロール階層が任意の等価な拡張ロールグラフに変換できることを証明した．この証明により，ロール階層を任意の等価な拡張ロールグラフに変換した後に，拡張ロールグラフを用いてロール階層を容易に再設計できることが保証される．

次に 2 点目として，分散システムに属するコンピュータ上のロール階層の再設計を容易にするために，拡張ロールグラフ間の拡張関係を定義し，拡張関係を維持しながら拡張ロールグラフを変換する拡張変換操作を定義した．分散システム内のオブジェクトへのアクセスを RBAC で制御する場合，各コンピュータ上に定義されたロールを適切にマッピングする必要がある．そして，運用環境の変化によりロール階層を再設計した場合，ロールのマッピングが適切に維持されるかを確認しなければならない．この確認は，ロール階層の設計者にとって大きな負荷となる．拡張変換操作を用いることで，ロールのマッピングが適切に維持されるかを確認することなくロール階層の再設計が可能となり，ロール階層の設計者の負荷を軽減することができる．

セキュリティ技術の実システムへの適用として，本研究では X サーバにアクセス制御機能とリソース使用量制御機能を付加したセキュリティ強化型 X サーバを開発した．アクセス制御機能により，悪意ある X クライアントによる不正な X リソースへのアクセスを禁止できる．また，リソース使用量制御機能により，悪意ある X クライアントによるメモリの大量消費を防ぐことができ，他の X クライアントの動作を妨害することを防ぐことができる．これらの技術により，X サーバや X クライアントに対する攻撃を防ぎ，コンピュータの安定動作を実現する．

さらに，本研究成果の実システムへの応用事例について述べた．本研究の成果を活用することで，ポリシーの設計，再設計を容易にできる．

論文審査の結果の要旨

近年，ウィルスや悪意あるアプリケーションによる攻撃は増加傾向にある．これらの脅威からコンピュータ上の情報やコンピュータシステムを保護するために，セキュリティ技術の重要性がますます高まっている．これらの攻撃からコンピュータ上の情報やコンピュータシステムを保護するための技術として，アクセス制御が挙げられる．アクセス制御は，オブジェクト（例えば，ファイル）にアクセスするための適切な特権をサブジェクト（例えば，プログラム）に認可することで，サブジェクトによるオブジェクトへの操作（例えば，読み込み）を制御するものであり，これを制御するルールをアクセス制御ポリシーと呼ぶ．情報システムのアクセス制御ポリシーを正しく設計することはそのセキュリティ管理上大きな課題である．

本研究はアクセス制御ポリシーを利用者が正しくかつ容易に設計するために，アクセス制御ポリシーのモデル化とそのモデルを用いたアクセス制御ポリシーの設計手法を提案している．博士論文の 4 章，5 章で提案設計手法の根幹をなすアクセス制御ポリシーのモデル化とそれに対する変形操作の意味を定義している．こうしたモデルを用いたコンピュータの援用により，正しいアクセス制御ポリシーを容易に設計することができる．また 6 章にて，複数の情報システムから構成される分散システムにおいて，上述のモデルを利用して，情報システム間のアクセス制御ポリシーの対応付けを自動で管理する手法を述べている．アクセス制御の管理が難しい分散システムで正しくアクセス制御ポリシーを管理することは煩瑣であり，本手法はこの問題を解決する手段を与えている．7 章において，上記のアクセス制御技術を実際に GUI プログラムに適用し，その有効性を評価した．さらに 8 章にて，本研究成果を容易に利用できるようにするためのグラフエディタの機能を説明し，一般利用者によるこのモデルの利用が容易であることを提示している．さらに実際の情報システムでのユースケースを 3 例あげ，本手法の具体的適用方法に言及している．

作られたアクセス制御ポリシーそのものが正しいかどうかを調べることは難しいため，本研究のアプローチは極めて実践的であるということができる．また，実際の情報システムへの適用化研究も進めることも期待でき，本博士論文の実用面での価値も大きいということができる．

以上を総合して本審査委員会は，本論文が博士（応用情報科学）の学位授与に値するものと全員一致で判定した．