様式 C-19

科学研究費補助金研究成果報告書

平成２２年　６月　４日現在

研究種目：基盤研究（Ｂ）
研究期間：2007～2009
課題番号：19300005
研究課題名（和文）高水準なポリシー記述を可能にするアクセス制御機能

研究課題名（英文）An Access Control Mechanism to Allow High-level Policy Description

研究代表者　加藤　和彦
（KATO KAZUHIKO）
筑波大学・大学院システム情報工学研究科・教授
研究者番号：90224493

研究成果の概要（和文）：
本研究では，オペレーティングシステムにおけるセキュリティ・ポリシー記述の容易化を目指して，カーネルレベルで動作する新しいアクセス制御機構に関する研究を行った．ポリシーの記述方式としてフェーズやクラス階層に基づく方式について研究し，それに基づくアクセス制御を実施する保護機構の研究開発を行った．その結果，直感的なポリシー記述が可能になったほか，ポリシーの記述量を大幅に削減できることが分かった．

研究成果の概要（英文）
We have carried out the research on a in-kernel new access control mechanism for simplifying the process of describing security policies in operating systems. We introduced the concept of phase and class hierarchy into the policy description language and developed the protection mechanism for enforcing such policies, allowing intuitive and small description of security policies.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
２００７年度	5,400,000	1,620,000	7,020,000
２００８年度	4,400,000	1,320,000	5,720,000
２００９年度	3,900,000	1,170,000	5,070,000
年度			
年度			
総　計	13,700,000	4,110,000	17,810,000

研究分野：オペレーティングシステム
科研費の分科・細目：情報学・ソフトウェア
キーワード：セキュア OS，アクセス制御，ポリシー記述

１．研究開始当初の背景

これまでにオペレーティングシステム（OS）のセキュリティ機能を高める機能として，さまざまなアクセス制御機能が提案され，それらの一部はセキュア OS と呼ばれる，セキュリティ機能を大幅に高めることを意図して設計されたシステムとして提供されている．multilevel security，mandatory access control，role-based access control，type enforcement 等は，セキュリティを高める代表的なアクセス制御機能であり，そのよ

うな機能を組み込んだセキュア OS の例として，PitBull，Trusted Solaris，Virtual Vault，SELinux 等がある．セキュア OS は，複数ユーザ間のアクセス制御を厳格，かつ，きめ細やかに設定することによって，ユーザおよびユーザプロセスの動作に必要な資源アクセス権限を最小限に抑制することを可能にする．このようなシステムは，システム内部でのアクセス制御を統制する上で有効であることに加え，ネットワーク経由のアクセスによる，システムの脆弱性や設定の不具合を突く攻撃に対しても有効性があるとされ，LAN やインターネットに接続されたサーバシステムのセキュリティ向上にも役立つことが期待されてきた．

前述のセキュア OS の中でも SELinux は，米国 National Security Agency によって開発された本格的なセキュア OS 機能を持ち，Linux のオープンソース・コミュニティに提供され，RedHat や Fedora Core 等の有力ディストリビューションにも含まれ，高い普及度を有するにも拘わらず，実際には広く利用されるに至っていないのが実情である．その最大の理由は，設定が大変に煩雑であり，専門知識を有する技術者であっても，管理者が求めるアクセス制御ポリシーを正しく記述するのは容易でなく，またポリシーが正しく設定されていることを確認すること，あるいは，修整することが大変に困難であるためと言われている．

研究代表者らもこれまでにセキュア OS 機能の一種である，SoftwarePot システム[1]の開発を行ってきた．SoftwarePot システムでは，ファイルシステムを含むアプリケーションの実行環境を仮想的に封じ込めて，アプリケーションを実行するユーザの環境とは隔離すると共に，アクセス制御ポリシーで指定した限定されたファイルのみについてのみ，ユーザの環境へのアクセスを許すことを可能とした．その実装は，OS カーネルの改変もアプリケーションの改変も必要としない，透明性の高いミドルウェアとして実現された．SoftwarePot システムにおいても，問題はアクセス制御ポリシーの記述にあった．同システムでは基本的に，アプリケーションを封じ込めた仮想実行環境内のファイルシステムとユーザ環境のファイルシステムの間で，共有が必要となるマッピング関係を記述すればよく，ポリシーの記述は簡略化されているが，それでもなお，エンドユーザが記述するのはあまりに煩雑であり，また，システム管理者が記述する場合でも，アプリケーションに関する専門の知識が必要であり，容易ではなかった．

以上述べたように，これまでのセキュア OS の研究で，さまざまなアクセス制御機能の提案と実装は行われてきたものの，実際に実用に供しようとすると，アクセス制御ポリシーの記述の煩雑さがボトルネックとなり，その機能を有効に活用できないことが問題となっている．またこの煩雑さのために，セキュア OS はもっぱらサーバシステムのための機能となっている．クライアントシステム，エンドユーザ・システムにおいては，既知のウィルスパターンをシステム内から発見するウィルス検知ソフトウェアが主として使われているのが実情で，エンドユーザ用 OS の本格的なアクセス制御機能の研究が十分になされているとは言い難い．

２．研究の目的

本研究では，アクセス制御ポリシーを可能な限り簡便に記述することを目的とした，セキュア OS の新しいアクセス制御機能の研究開発を行う．本研究は次の三点の着想に基づく．

(1) これまでの一般 OS およびセキュア OS におけるアクセス制御機能では，システムはクローズであることを仮定し，閉じたシステム空間内のドメインと資源間のアクセス関係を制御することにより行っていた．本研究では，システムはオープンであることを仮定し，インターネット上で定義される資源と，インターネット上で定義されるドメインが，たまたま一つのコンピュータシステム内で関係を持ち，アクセス制御が行われると考える．ファイルが新たに生成されたり，インターネットや外部ストレージからシステム内にファイルが取り入られるときには，付帯状況から可能な推論をシステムが行い，自動的なアクセス制御設定を行う．

(2) アクセス制御ポリシーを高水準に記述することを可能にするために，ファイル概念を一般化し，仮想化・抽象化されたオブジェクトとして扱う．すなわち，仮想的にすべてのファイルを，属性名と属性値のペアの集合によって構成されたオブジェクトとして扱う．このとき，複数ファイルやディレクトリを仮想的なオブジェクトとして扱うことも可能とする．さらに，オブジェクトを要素として，generalization, aggregation 等の関係を用いて複合的なオブジェクトを定義することも検討する．同様に，アクセスを行う主体となるユーザやユーザプロセスもオブジェクトとして仮想化する．これらの仮想化・抽象化によって，OS 内のアクセス制御ポリシーの記述を高水準に行うことが可能となる．アクセス制御ポリシーは，アクセス主体オブジェクトと，アクセス対象オブジェクトとを問い合わせ式によって選択し，それらの間に成立

する関係（読み出し権，書き出し権，実行権等）を宣言的に記述することによって定義できることを目指す．

(3) 第三に，以上のような機能を，現行の OS 環境と互換性を保つように設計・実現する．すなわち，現行の OS やアプリケーションソフトウェアは，従来のファイルと同様に資源アクセスを行うが，OS カーネル内では，前述の仮想的なオブジェクトとしての取り扱いとして記述されたアクセス制御ポリシーに基づき，アクセス制御が行われる．

３．研究の方法

本研究では，アクセス制御のポリシーを容易にかつ正しく記述できるようにするために，データベース，プログラミング言語処理系，オペレーティングシステムのそれぞれの技術を組み合わせた手法を用いる．平成 19 年度では，(1)データベースの機能を応用した仮想オブジェクトの概念による属性管理，(2)プログラミング言語処理系の技術を応用したプログラマブルなアクセス制御機能の２つについてそれぞれ以下のように研究を進める．

(1) 仮想オブジェクトの概念による属性管理

アクセス制御のポリシーを高水準で記述できるようにするためには，ポリシー記述に用いるプリミティブを高水準化する必要がある．本研究ではデータベースの技術を応用して，OS のファイルシステムに仮想オブジェクトの概念を導入し，ファイルなどのオブジェクトに対して高水準の属性を設定できるようにすることで，ポリシー記述に用いるプリミティブの高水準化を実現する．

① 仮想オブジェクトの提供

従来のアクセス制御ポリシーの記述では，アクセスの対象となるファイル等のオブジェクトを指定するために，主にファイル名やパス名などオブジェクトの物理的な格納場所に依存した形式を用いている．この結果，本来アクセスの可否を決定する基準となるオブジェクトの内容や性質とは直接関係の無い情報（格納場所）を元に記述しなければならず，記述が直感的ではない．また，OS によるオブジェクトの管理の仕方に関する専門的な知識が必要になる．

本研究では，オブジェクトの内容や性質に基づいたアクセス制御を記述できるようにするために，仮想的に全てのオブジェクトを属性名と属性値のペアで決定されたオブジェクトとして扱い，アクセス制御とファイルの指定を統合しておこなえるようにする．ファイルやディレクトリも仮想的なオブジェクトとして扱えるようにすることで，従来のファイル名やパス名といった物理的な制約にとらわれず，より高水準な概念でアクセス可能なオブジェクトの集合を指定できる．また，物理的制約にとらわれない方式で記述することにより，新たに作成したオブジェクトに対するアクセス制御やオブジェクトが移動・コピーされたときの対応を容易にする．

② オブジェクトの属性管理

アクセス制御の記述は一般に，あるサブジェクト(主体)がオブジェクト(対象)にアクセスすることを許可するかどうかといった形式で記述をおこなう．従来の OS ではこの主体や対象の単位がプロセスやユーザ，ファイルといった抽象化はされているものの，一般ユーザからみると OS がプリミティブとして提供している極めて低レベルな概念を用いており，これが記述の難しさの要因となっていると考えられる．

本研究では，アクセス制御のポリシーを，より人間が理解しやすい抽象概念で記述できるようにするために，サブジェクトやオブジェクトに対して従来よりも高水準な抽象概念による属性を設定できるようにする．例えばファイルであれば，作成した人やソフトウェアの名前，それぞれが所属する組織名，その所属組織の属性（創業年，従業員数，上場の有無など）など，人間が一般社会において信頼性を判断する基準となる情報を生かして，直感的に可否を判断しやすい形式で記述できるようにすることを目指す．本機構では，ファイルなどの永続的オブジェクトに対して対応する属性を管理して保存し，アクセス制御機構からの問い合わせに答えてアクセスの可否を判断するための情報を提供する．オブジェクト指向データベースやアクティブデータベースの技術を応用して，大量の問い合わせに対しても効率よく処理する機構を実現し，アクセス制御によるオーバーヘッドを抑える．

(2) プログラマブルなアクセス制御機能

新しいポリシー記述手法の導入を容易にするために，プログラミング言語処理系の技術を応用して，記述されたポリシーを実際に実施(enforce)するアクセス制御機構をプログラマブルにする．言語処理系の機能を用いることにより，以下の機能を実現する．

① 交換可能なアクセス制御機構

従来の OS ではアクセス制御を実施する機構は C 言語などの低レベルな言語で記述されることが多く，機能拡張や新しい方式の導入にはカーネルレベルで動作するプログラムの書き換えが必要となり，アクセス制御機能の交換をおこなうことは容易ではない．従来からも拡張可能 OS の研究において，SPIN

における Modula-3 など高級言語で書かれたプログラムをカーネル内に組み込む仕組みは多数提案されているが，その仕組みは一般的なものにとどまっており，アクセス制御機構への適用手法について具体的に言及したものは少ない．

本研究では，アクセス制御機構に焦点を絞って高級言語をカーネル内に導入することを目的として，言語処理系に最低限必要となる機能やカーネル側とのインターフェイス設計などについて研究をおこなう．具体的には関数型言語の ML をベースとして使用し，以下に述べるポリシー記述や安全性検証をおこない易くする．アクセス制御機構の実装に限って言語処理系のランタイムを用いることにより，既存のカーネルの修正を最小限にしてオーバーヘッドを抑え，実用的に使える交換可能なアクセス制御機構を実現する．

② 高水準なポリシー記述方式

高級言語で記述したアクセス制御機構を用いて，アクセス制御の記述を容易におこなえるポリシー記述言語の設計をおこなう．ポリシー記述言語の設計にあたっては，従来のセキュア OS が想定しているクローズドな環境ではなく，インターネットのようなオープンな環境を想定して，わかりやすい抽象度で記述できる方式を設計する．具体的には，プログラムやファイルなどのオブジェクトに関して，従来の OS の user や role といった抽象概念だけではなく，そのオブジェクトを作成した人や企業の具体的な名前や所属，オブジェクトの性質（例えばプライベートな写真，企業秘密が格納されたファイル，身元不明のプログラム）など，現実社会で馴染みのあるわかりやすい抽象概念を導入して，直感的にポリシーを記述できるようにする．例えば「作成したユーザの所属組織が同じ場合にはアクセスを許可」といった指定の仕方や，「インターネットからダウンロードした作者不明のプログラムからは，読み込みアクセスのみ許可する」などの高水準でのポリシー記述を可能にする．

③ ポリシーの安全性検証

記述したアクセス制御のポリシー自身に欠陥が無いか検証する手法について研究をおこなう．従来のアクセス制御ポリシーの記述では，高度な知識を持った専門家が低レベルのプリミティブを駆使して記述をおこなうが，複雑なポリシーを正しく記述することはソフトウェアを正しく記述することと同等以上に困難な作業である．また，ポリシーは宣言的に書かれることが多く，その内容を理論的に検証することは難しい．本研究では，アクセス制御のポリシーを記述するためのポリシー記述言語を比較的限られた機能でも実現可能なドメイン特定言語として定義し，言語処理系の技術を用いて静的な検証をおこなえるようにする．これにより，ポリシー自体の問題によりセキュリティホールが生じるという事態を理論的に回避することを可能にしつつ，ポリシー記述が容易で現実的に利用可能なアクセス制御機構を提供することを目指す．本手法の設計は，主に研究代表者（加藤）が中心となっておこなう．研究代表者は，SoftwarePot の研究を通じてポリシー記述の難しさやその要因について精通しているほか，データベースや言語処理系の知識を持ち合わせている．一方，研究分担者（品川）はアクセス制御機構の実装に精通しており，設計したポリシー記述言語をカーネル内で実施可能にする手法について担当する．両者が連携して設計・実装をおこなうことにより，記述が容易で検証可能なアクセス制御方式をカーネル内で安全かつ効率よく実現することが可能となり，理論と実践の両面で研究を進められる．

平成２０年度以降は，(1)仮想オブジェクト管理とアクセス制御のカーネル内での統合と，(2)実証実験による有効性検証の 2 つについて研究を行う．

(1) 仮想オブジェクト管理とアクセス制御のカーネル内での統合

１９年度に開発したアクセス制御と仮想オブジェクト管理をそれぞれカーネル内に組み込んで動作させ，OS・データベース・言語処理系の機能をお互いに連携させながら，安全に効率よく実行させる手法に関して研究をおこなう．

① 仮想オブジェクト管理機構のカーネル内への統合仮想オブジェクト管理機構をカーネル内に導入するにあたり，既存の OS との互換性を保ちながら実現する手法について研究をおこなう．既存の OS はファイルシステムを用いてオブジェクトをファイルとして管理しており，詳細な属性を管理や仮想オブジェクトの実現のための機能は提供していない．本研究では既存のファイルシステムに機能を追加する形で属性管理や仮想オブジェクトの機能を実現するが，その際従来のアプリケーションが仮想オブジェクトのインターフェイスを使用せずに，通常のファイルとしてアクセスをおこなっても正しく動作するように，互いの機能を連携させる必要がある．本研究では，オブジェクト管理機構をカーネル内に密接に統合することにより，既存のファイルシステムの機能と仮想オブジェクト管理の機能を確実に同期させて，両者の共存を可能にする．また，アクセス制御実施時における大量の問い合わせを効率よく処理できるようにするために，カーネル内におけるオブジェクトのキャッシュ機構などに本研究の手法を統合し，アクセス制御の

オーバーヘッドを実用的な範囲に抑える手法を研究する．
② プログラマブルなアクセス制御機構のカーネル内への統合
アクセス制御機構はカーネル内で動作するため，制御プログラム自体の欠陥によりカーネルの安全性が脅かされることを防ぐ必要がある．これまでもカーネル内で拡張コードを安全に動作させる仕組みとして，Modula-3, PCC, BPF, Cyclone など様々な言語が用いられてきたが，ML をカーネルで動作させる試みはあまりなされていない．
本研究では ML の特長を生かしながらカーネル内でアクセス制御機構のコードを安全に動作させる仕組みについて研究をおこなう．アクセス制御の実施に必要な最小限のランタイムのみをカーネル内で動作させることにより，実行時オーバーヘッドを低減させつつ言語処理系としての検証可能性は保ち，拡張性と安全性・速度の両立を図る．
③ 仮想オブジェクト管理とアクセス制御の連携
カーネル内で仮想オブジェクトの概念に基づいたポリシーを実施できるようにするために，アクセス制御機構が仮想オブジェクトにアクセスするためのインターフェイスを設計・実装して，お互いに連携可能なことを確認する．
(2)実証実験による有効性検証
実際にアクセス制御機構を動作させて有効性を確認する．・ アクセス制御機構の有効性検証実際にデスクトップ OS として導入し，Web ブラウザやメーラによるインターネットとのファイルのやり取り，Office 系ソフトウェアによるファイルの閲覧・編集，デジタルカメラで撮影した画像ファイルの取り込み・編集・送信など，一般にデスクトップ PC で頻繁におこなわれる様々な状況を想定した実験をおこない，不必要にアクセスが制限される false positive が発生しないかどうか検証する．また，実際の攻撃を想定した攻撃プログラムを作成し，不正アクセスを確実に防止できること，すなわち false nevative が発生しないことを確認する．
・ ポリシー記述方式の有効性検証
ポリシー記述の容易さについて比較検証をおこなう．具体的には，同じアクセス制御を本研究の方式と SELinux の両方で記述したポリシーを作成し，両者のポリシーの記述量や必要とされる専門知識などの観点から比較をおこなう．また，言語処理系を用いた理論的検証の有効性を確認し，ポリシーを正しく記述することが容易にできるかどうか検証する．

４．研究成果

本研究では，まず仮想オブジェクトの概念による属性管理として，(1)仮想オブジェクトの提供，(2)オブジェクトの属性管理，について研究を行った．
(1)の仮想オブジェクトの提供については，Linux カーネル内で動作するカーネルモジュールとして実装した．ファイルごとに属性情報を格納したうえで，カーネル内のアクセス制御機構でこれらの属性情報にアクセスし，あらかじめ設定したポリシーと照らし合わせることで，ファイルの物理的な場所にとらわれず，仮想的なオブジェクトとみなした状態でのアクセス制御をおこなうことが出来るようになった．
(2)のオブジェクトの属性管理に関しては，例えばプログラムの作成者・メーカーといった情報を付与することによって，ソフトウェアのインストールを安全に行うためのポリシーを従来の方式よりも容易に記述して実施することができるようになった．属性情報の付与に関しては，手動で設定する方式のほかに，パッケージ管理システムで管理している情報の応用や，電子証明などの方式を組み合わせて，ある程度自動的に設定を行う方式を検討した．
プログラマブルなアクセス制御機能に関しては，(1)交換可能なアクセス制御機構，(2)高水準なポリシー記述方式，(3)ポリシーの安全性検証，について研究を行った．
(1)の交換可能なアクセス制御機構については，当初はアクセス制御機構のベースとして関数型言語の ML を使う予定であったが，カーネル内で動作させるのに適当な処理系の実装を用意することが難しかったため，独自のバイトコードを用いたアクセス制御専用の仮想マシンを実装した．この仮想マシンでは，命令セットを最小限のものに絞ったほか，設計を注意することでカーネル内でも安全に動作させられるようになっている．
(2)の高水準なポリシー記述方式に関しては，オブジェクト指向の概念を導入したクラス階層型のポリシー記述方式を導入することにより，直感的なポリシー記述が可能になったほか，実際にインターネットサーバに対してポリシー記述を行うことにより，複数のポリシーをまとめることによってポリシーの行数を削減する効果が得られることを確認した．また，実行時のフェーズを用いたポリシー記述方式や，ファイル名の接頭辞を用いたアクセス制御方式などにより，更にポリシー記述量の削減や直感的なポリシー記述力が向上することを確認した．
(3)のポリシーの安全性検証に関しては，ポリシーを記述するための専用言語をドメイン特定言語として定義し，パーサー生成器である ANTLR を用いて，(1)で設計・実装した仮想マシン向けバイトコードへ変換するア

プローチを取った．これにより，実際にポリシーを静的に検証する段階には至ってはいないのものの，将来的な静的検証に向けた足がかりを実現することが出来た．

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計１件）
[1] 品川 高廣，忠鉢 洋輔，河野 健二，加藤 和彦．実行時のフェーズを用いたセキュリティポリシー簡略化．情報処理学会論文誌：コンピューティングシステム，第 2 巻，第 2 号，166-177 頁，2009 年 6 月．（査読有）

〔学会発表〕（計２件）
[1] 横川 晃，品川 高廣，加藤 和彦．クラス階層型セキュリティポリシーによるアクセス制御．情報処理学会研究報告(2009-OS-112)，2009 年並列/分散/協調処理に関する『仙台』サマー・ワークショップ（SWoPP 仙台 2009），情報処理学会，仙台，2009 年 8 月 6 日．
≪最優秀学生発表賞受賞≫

[2] 大宮 正大，品川 高廣，加藤 和彦．ファイル名の接頭辞を用いた簡易アクセス制御．コンピュータシステム・シンポジウム(ComSys2007)，東京，2007 年 11 月 27 日．

６．研究組織
(1)研究代表者
加藤　和彦（KATO KAZUHIKO）
筑波大学・大学院システム情報工学研究科・教授
研究者番号：90224493
(2)研究分担者
品川　高廣（SHINAGAWA TAKAHIRO）
筑波大学・大学院システム情報工学研究科・講師
研究者番号：40361745
(3)連携研究者
なし