様式Ｃ－１９

科学研究費助成事業（科学研究費補助金）研究成果報告書

平成 24 年 6 月 20 日現在

機関番号：32721
研究種目：基盤研究(B)
研究期間：2009～2011
課題番号：21300016
研究課題名（和文）
SOA の健全な発展を支える先進的共通アクセス制御アーキテクチャの研究
研究課題名（英文）
Advanced access control architecture to support healthy development of SOA
研究代表者
田中 英彦（TANAKA HIDEHIKO）
情報セキュリティ大学院大学・情報セキュリティ研究科・教授
研究者番号：60011102

研究成果の概要（和文）：本研究では、情報システムのアクセス制御を OS によって保護される共通機構で実現するアーキテクチャを開発した。このアーキテクチャは、アクセス制御を厳密且つ安全に行う共通の仕組みを提供することを目的としており、OS とアプリケーションの協調によるアクセス制御機構を実現した上で、その機構の利用を強制化する。提案アーキテクチャの主要な構成要素は、ポリシー記述言語と認可判定機構、アクセス制御機構で、本研究では、Linux を対象に各種実装と評価実験を行い、その有効性を実証した。

研究成果の概要（英文）：
In this research, we developed an architecture to realize a common access control mechanism protected by OS. This architecture is intended to provide a common mechanism to perform safely and strict access control by the coordination of applications and OS, and to force the use of that mechanism. The main components of the architecture are an authorization decision mechanism, policy description language and mandatory access control mechanism. We performed various experiments for implementation and evaluation on Linux OS and demonstrated its effectiveness.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
平成 21 年度	3,700,000	1,110,000	4,810,000
平成 22 年度	5,000,000	1,500,000	6,500,000
平成 23 年度	3,700,000	1,110,000	4,810,000
年度			
年度			
総　計	12,400,000	3,720,000	16,120,000

研究分野：総合領域
科研費の分科・細目：情報学／計算機システム・ネットワーク
キーワード：ディペンダブルコンピューティング、アクセス制御、セキュリティ

１．研究開始当初の背景

近年、SQL インジェクションに代表されるような、個別アプリケーションの脆弱性を狙った情報システムに対する攻撃が蔓延している。そして、この種の攻撃における最大の問題点は、その対策が場当たり的な継ぎ接ぎ方式であることにある。本研究は、その根本的な対策に繋がる方式を提案するものである。

これまでのセキュリティ対策は、情報システムにおける基盤として重要で、且つ、幅広く利用されるソフトウェア、例えば、OS 等のプラットフォームや、Web サーバ、DB といった汎用アプリケーションに対するもの

が中心であった。これらのソフトウェアは、世界中のユーザが様々な分野で利用することで脅威にさらされると同時に、世界的ブランドと多大なコストによって大規模に開発されることで洗練され、常に発生しうるセキュリティホールへの対策方法がようやく確立されてきたといえる。

しかし、それらが一定のセキュリティレベルを保てるようになった今、今度はそれらをベースに構築される個別アプリケーションの弱点が浮き彫りなってきた。「情報システムのセキュリティレベルは最弱点に引きずられる」等の表現があるように、まさに個別アプリケーションが現在の情報システムにおける弱点となりつつある。

すなわち、個別アプリケーションのセキュリティ確保の問題は、なによりそれらが個別に構築される点にある。個別であるということは、そのセキュリティレベルは、開発者もしくはベンダに依存することとなり、個別アプリケーションの実装方式、もしくは一部のミドルウェア機能に依存することで、共通のセキュアプラットフォームが確立されていないことが問題点であると考える。

昨今の情報システムは、Web サービスに代表されるように、ネットワーク経由で接続された複数アプリケーションが連携処理を行うものが中心である。従って、個別アプリケーションのセキュリティ対策を汎用的に実現する仕組みが必要であるにも関わらず、現状では実装者に依存した対策となっており、個別アプリケーションの脆弱性を狙う情報システムに対する攻撃への根本的な対策となっていない。

この問題を分析すると、次のような課題が浮き彫りになる。まず、Web サービス等のアプリケーションが持つセキュリティ確保の仕様は、個々のアプリケーションに任され、厳密なアクセス制御機構を持つとは限らない。当然、設計次第では、ある程度に堅牢なアプリケーションを実現可能であるが、標準化されていない以上誰もそれを担保していない。

次に、アプリケーションは、複数の処理要素が TCP/IP 等の標準化された通信手段を使い、アプリケーションレイヤのメッセージングにより処理の受け渡しを行っているのみで、OS 等のプラットフォームにおける厳密なアクセス制御機構を活用することができていない。SELinux 等のセキュア OS においては、特定の Web サービスや DB といった一部の汎用アプリケーションを個別に拡張することで、プラットフォームレイヤとアプリケーションレイヤを統合してアクセス制御しようといった試みが行われているが、それはあくまでアドホックなアプローチであり、プラットフォームと汎用アプリケーションの統一的なアクセス制御の実現にはつながっていない。

２．研究の目的

本研究では、情報システムのアクセス制御を OS によって保護される共通機構で実現するアーキテクチャを開発する。これは、先に指摘した課題を解決するもので、アプリケーションに対し、アクセス制御を厳密且つ安全に行う共通の仕組みを提供することを目的として、OS とアプリケーションの協調によるアクセス制御機構を実現し、その機構の利用を強制化するものである。従って、この研究は大変抜本的なシステム提案であるが、更に、その提供する共通機能は、今後の柔軟な SOA（Service Oriented Architecture）からの要請を先取りして、十分に高機能なアクセス制御機能を実現することを目指している。そのような機能の実現を可能とする所が、この研究の重要なポイントである。

そのための機構は、主にアクセス権記述処理系とその DB 内への設定系、強制アクセス制御機構、認可判定機構、アクセス制御情報 DB、及び、アプリケーションの SVC (Supervisor Call) 履歴モニタから構成される。従来、これらは情報システムの各所で、OS やアプリケーション毎に実装されているため、アクセス権管理は、互いに独立して設定されたものを粗い粒度でマッピングして実現していた。

本研究では、これらを OS 内に一括して取り込むことで、アプリケーションに対してアクセス制御機構の提供と強制を行い、分散処理をも含めた情報システム全体に網羅的で一貫性のあるアクセス制御を適用し、総合的な信頼性向上を実現することで、今後の Web サービス等の発展につなげることを目指す。

この研究では、期間内にこのアーキテクチャの提案と、その実現詳細手法を明らかにすること、更に、そのアクセス権記述が容易に行えることを示すとともに、既存 OS や Web サービス標準への導入手順を明らかにする。すなわち、この研究の具体的な目的と達成内容は以下の通りである。

① 情報システムのアクセス制御機構を汎用的なプラットフォーム技術として OS 内に実装し、アクセス制御情報の統合処理を行うアーキテクチャを提案すること

② SELinux などのセキュア OS が広く使われない原因の一つは、アクセス権記述の困難さにある。従って、今後の広範な分散アプリケーションで、Covert Channel 問題などの対処に必要な状態指定等の細粒度アクセス権設定を、容易に表現する記述系を与えること

③ アクセス権記述を実行形式に直す処理系を実装し、OS 内のアクセス制御情報 DB に安全確実に設定する機構を設計すること
④ 複数アクセス制御情報間の調停アルゴリズムを与え、分散アプリケーションを実現する時に、システム間の調停で必要となる、アクセス制御情報 DB 間の連携機構を設計すること
⑤ 具体的な複数の分散アプリケーションを実験システム上に実現し、提案アーキテクチャの実現性と問題点を評価すること
⑥ 既存 OS と Web サービスに、この機構を埋め込む手順を明らかにすること

３．研究の方法

研究は、様々なアクセス条件を柔軟に記述するアクセス権記法と、それに基づいてアクセス制御を強制する機構について、まず単一システムに閉じた環境を対象に設計する。ここで中心となるテーマは、記法の記述力と理解容易性で、細粒度のアクセス制御を簡潔で柔軟に表現できる方式を検討する。また、SELinux の拡張による実験システムを構築して、これらを実証する。次に、この方式を分散処理へ拡張するために、相互に独立して記述・設定したアクセス権記述を、後から必要に応じて調停し、適用すべきアクセス権を設定する方式を設計する。その後は、従来方式からの提案システムへの移行・融合方式、仮想化技術への適用手法などを検討した上で、実験システムに実装し、各種評価と改善を行う。

初年度は、単一システム向けの汎用的なアクセス権記法を設計し、それによって記述されたアクセス権を連携させて、アクセス制御情報 DB を構成する手法を明らかにし、その各種評価を行う。

はじめに、仕様を書くのに適している論理型言語をベースに、多種多様なアクセス条件を汎用的な形式で柔軟に表現可能な、新規のアクセス権記述言語を設計する。

次に、論理型言語で記述されたアクセス権を、アクセス制御情報 DB 内に静的のみならず動的にも設定可能とするために、アクセス権記述の処理系とアクセス制御情報の設定系を具体化し、記述の正しさとアクセス制御情報 DB に対する設定権限の厳密な検査をおこなうことで、記述から設定への安全確実なパスを保証する。また同時に、OS やアプリケーション等のモジュール毎に、個別に記述されたアクセス権を連携させる手法を設計する。

その後、このアクセス権記法とアクセス権記述連携を評価する。評価時は、Web サービスを含む幾つかの主要アプリケーションを例として、アクセス制御情報を実際に構成した上で、SELinux 等で用いられている既存アクセス権記述言語と比較し、十分に記述力が高く、容易な記述が可能であることを実証する。また、その記述を用いて、小規模なアクセス制御情報 DB を構成し、机上実験を行って、適切な粒度、判定計算量、記述力、記述の容易性、検証可能性などを多角的に評価する。また、不正な問い合わせや、意図しないアクセス権制御、サービス停止攻撃など、アクセス制御情報 DB に対して想定できる攻撃を考察し、設計したアクセス権記法とアクセス制御情報 DB が、十分に強固で実用に耐えるものであることを裏付ける。

平成 22 年度は、前年度開発した記法を用いて、単一システム内でアクセス制御を統一的に実行する機構を開発する。また、そのアクセス権記法を拡張して、分散処理を記述・設定する方式を検討する。

はじめに、細粒度のアクセス条件を情報システムの全域で確実に強制するために、従来 ACL（Access Control List）ベースで実現されている Linux のアクセス制御機構を LSM（Linux Security Module）経由で上書きし、ケーパビリティベースのアクセス制御機構を実現する。開発するアクセス制御機構の目的は、初年度に開発したアクセス権記法で設定されたアクセス条件を、漏れなく情報システムに強制することで、その要件は、リソースの参照情報とアクセス権を結合して簡潔に扱うことと、アクセス制御機構が制御対象を確実に捕捉することである。

次に、設計したアクセス制御機構を、初年度に開発したアクセス権記法によるアクセス制御情報 DB と連携する実験システムを構築し、その上で、各種評価を行う。評価項目は、連係動作時におけるアクセス制御機構全体としての判定計算量や設定したアクセス権記述の検証可能性に加えて、ユーザーレベルの強制アクセス制御機構を利用することによる強度と精度への影響で、これらを確認することにより、厳密な階層的防御を確実に実現可能であることを実証する。

また、階層的防御を分散システムでも実現するために、前年度に開発したアクセス権記法を拡張として、分散処理に適用するアクセス権の記述方式を検討する。

最終年度となる平成 23 年度は、前年度までに開発したアクセス制御機構を実装したシステムを複数接続した上で、グローバルな実験システムを構築し、その有効性の検証と安全性の評価を行う。また、本システムの階層的防御手法を基礎とする、新たな適用対象についても考察すると同時に、現実の情報システムに適用するために、既存システムからの移行方法や既存システムとの融合手法、仮

想化技術への組み込み手法についても検討する。

次に、これらの諸要素検証の後、実際の情報システムに近い形での総合的な実証と最終的なアーキテクチャの提案を行う。また同時に、既存システムから本システムへの移行を、現実の情報システムに適用するための具体的なステップの切り方や、既存システムとの融合手法、更に、システム間移行を仮想化技術を用いて容易化する手法を検討することで、提案するモデルおよび機能が現実の情報システムに適用可能であり、効果的に動作することを立証する。

この総合的な実証としては、Firewall、IDS、各種サーバ等の構成要素をもつ典型的な情報システム上で様々なインシデントを想定したテストを行ない、提案システムの効果を立証する。また提案した各種手法や機能について、オーバヘッドや遅延を定量的に測定し、結果を分析することで、本手法の有効性を具体的に示すとともに現実的な対策としてまとめあげ、最終提案を行う。

尚、本研究においては、研究代表者である田中英彦を中心にシステムの構想と具体的な設計を行い、それに基づいた詳細なモデルとプロトコルの作成、実装を研究分担者である金美羅と橋本正樹が中心に行う。各種成果物に対する評価と分析、実証実験、さらに最新技術動向との比較検討、対外発表については、研究分担者である辻秀典を中心に行うものとする。また、研究協力者として、博士課程の学生２名と修士課程の学生数名が、各システム実装とその他補助を担当する。

４．研究成果

本研究では、情報システムのアクセス制御を OS によって保護される共通機構で実現するアーキテクチャを開発する。

研究の初年度となる 平成 21 年度は、アクセス制御の根拠となるポリシーについて、汎用的に表現して構成することができるポリシー記述言語を、まずは単一システム向けに設計した。また、それによって表現された複数のアクセス制御規則を連携させてアクセス制御情報 DB を構成する手法を明らかにし、その各種評価を行った。

従来のポリシー記述方式では、ローカル環境の OS や応用に閉じたアクセス制御規則を記述対象としているため、複数の領域間でアクセス権を連携させる場合は、アクセス権同士を相互にマッピングして対応していた。また、個々のアクセス制御規則を独立に記述・羅列するような記述方式であったため、膨大な量のアクセス権を記述すると可読性と保守性が著しく低減する問題もあった。その結果、ポリシーの適用範囲を広げるほどアクセス制御の粒度を粗くせざるを得なくなり、セキュリティインシデント発生時の被害範囲を大きくする要因となっていた。

それに対して、提案したポリシー記述方式では、属性の継承・頻出手続きの構造化といった高レベル記述や、推論規則を用いることで、細粒度のアクセス制御規則を簡潔に表現することを可能とした。さらに、本言語は、アクセス権記述の適用範囲を将来分散処理に拡大する場合に備えて、各アプリケーションのシステムコール呼び出しをモニタして蓄積し、その履歴をプロセス毎の状態同定に用いることで、多種多様なアクセス条件を柔軟・簡潔に表現する汎用的な記述方法となっている。各種の評価実験により、本言語の高記述性が確認された一方で、応答性能の劣化が見られたが、これについては実装方式の工夫により平成 22 年度以降の研究で解決方法を検討した。

研究の二年目となる平成 22 年度は、研究の初年度に開発したセキュリティポリシ記法を用いて、単一システム内のアクセス制御を統一的に実行するためのアクセス制御機構について、Linux を対象に実装方式を検討した。

開発するアクセス制御機構の目的は、初年度に開発したポリシー記法を用いて設定されたアクセス条件を、漏れなく情報システムに強制することで、その要件は、アクセス制御メカニズムがアクセス制御対象を確実に捕捉できることと、アクセス制御メカニズムとアクセス制御情報 DB が正しく連携できることにある。そこで、本研究では、情報システムの各所に対する細粒度アクセス制御を、OS から確実に強制するために、従来 ACL (Access Control List) ベースで実現されている Linux のアクセス制御機構を LSM (Linux Security Module) 経由で上書きし、ケーパビリティベースのアクセス制御機構を実現する方式について検討した。本方式では、アクセス制御メカニズムとアクセス制御情報 DB の連携方法が主要な課題で、平成 22 年度の研究では、カーネルランドにアクセス制御情報 DB を直接埋め込む方式と、ユーザランドにアクセス制御情報 DB を実装し、Linux カーネルとユーザランドのアクセス制御情報 DB が通信する方式の、双方について検討と実験を行った。

研究の最終年度となる平成 23 年度は、前年度までで検討したアクセス制御機構を Linux に実装し、その評価を行った。また、今後、提案方式を仮想化環境や分散環境への拡張・適用する場合に備えた検討を行った。

具体的には、以下の各項により、前年度までに検討したポリシー記述言語とそれによる認可判定機構を Linux カーネルに接続し、細粒度のアクセス制御規則を簡潔に表現・強制するアクセス制御機構を実装した。

① 論理プログラミング言語 XSB を用いたポリシー記述言語の実装と、Linux に与えるアクセス制御規則の仕様
② Linux カーネル内部にある、オリジナル版認可判定関数の実行速度を評価するプログラム
③ ①による認可判定実行速度を評価するプログラム
④ ①による認可判定結果の妥当性を評価するプログラム
⑤ ②-④を組み合わせる事で、オリジナルの認可判定関数と、①による認可判定プロセスの実行について、その速度と妥当性を確認するプログラム
⑥ Linux カーネル・オリジナルの認可判定関数を提案方式による認可判定プロセスに差し替えるための、XSB サーバプロセスおよびカーネルモジュール

また、①-⑥による評価実験によって、提案機構の認可判定に関する妥当性と表現力について、以下の知見を得た。

すなわち、妥当性の評価実験では、アクセス可として判定された問い合わせとアクセス不可として判定された問い合わせで計 99%以上の応答内容が一致したが、一部応答内容が一致しないケースが確認された。この原因は、システム運用時に動的に生成されるコンテキストに対して問い合わせを行ったことによるもので、これについては認可判定時の引数の渡し方に依存するものである。そのため、この解決は認可判定機構の外部で工夫する必要があるが、一方で、元々の Linux の認可判定がポリシーの記述に対して妥当であることを前提とした時、本言語によるポリシー記述とそれに基づいた認可判定自体も妥当であったと言える。従って、この実験結果により、論理プログラミングを基礎とした本言語が、現実のポリシーを論理的に正しく記述することができることを示した。

この応用としては、論理プログラミングの持つ特徴をアクセス制御に適用することで、例えば、変数を用いた問い合わせによりポリシーの検証を柔軟に行い、その検証結果をアクセス制御の条件として記述すること、メタな規則によって新規則の追加方法や既存規則の変更を制御すること、認可判定に利用する引数を認可判定機構が状況に応じて変更することなどが考えられる。

表現力の評価実験では、本言語による記述方式により Linux のポリシーを少ない記述量で構成できることを示したが、これは、アクセス制御規則を定めるのに必要な多くの指定を条件節にまとめたからであり、結果として、各規則に対する条件節の内容が多くなっている。そのため、必要な要素を直接指定している Linux の記述手法の方が、各々の規則を個別に見た場合には内容を直感的に把握しやすい。一方で、本言語の記述手法では、アクセス制御規則を階層化やサブルーチン化によってある程度まとめて記述するため、各々の規則を見た場合の可読性はそれほどよくないが、ポリシー全体としての見通しは向上している。

従って、Linux のポリシー記述手法のような直接要素を指定する表現と、本言語のような変数項と条件節を用いた表現は、双方に異なる特徴があるため、利害得失は利用フェーズに依存すると考えられる。例えば、他の規則と関連性を持たないような少数のアクセス制御規則を厳密に記述していきたいような場合は前者の記述手法が適しているし、様々な認可判定で共有されるアクセス手順が多く存在し、それをまとめて指定したい場合や、アクセス制御規則の総数が膨大になるため、柔軟な構造化が必要な場合には後者の方が適している。

今後は、これらの成果を仮想化環境や分散環境に適用する方法を検討し、そのために、分散環境においても、階層的防御網による被害局所化を有効に実現するために、アクセス主体と対象をその状態に基づいて細かに分類する新規アクセス制御モデルを設計し、ポリシーの分散管理・配布を含む分散型強制アクセス制御アーキテクチャを提案・実装する。また、本研究で提案したポリシー記述言語を拡張することで、細粒度の分散処理を記述可能とし、同時に、国際標準である SAML モデルや XACML 言語ともマッピング可能な方式を提案する計画である。

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 8 件）

① 橋本正樹、安藤類央、前田俊行、田中英彦、情報セキュリティ向上に向けたOS研究の動向、情報処理学会論文誌 : コンピューティングシステム(ACS) 、査読有 、 Vol.5 、 No.2 、 pp.51-62 、 http://id.nii.ac.jp/1001/00081513/
② 宮本久仁男、田中英彦、特徴データベースを用いない効率的な仮想マシンモニタ検出方式の提案、情報処理学会論文誌、査読有、Vol.52、No.9、pp.2602-2612、http://id.nii.ac.jp/1001/00077492/
③ 三村守、田中英彦、トラフィックパターンを隠すアプリケーションベースVPN

の実現方式、情報処理学会論文誌、査読有、Vol.52、No.9、pp.2775-2787、http://id.nii.ac.jp/1001/00077515/

④ 金子朋子、山本修一郎、田中英彦、アクタ関係表に基づくセキュリティ要求分析手法（SARM）を用いたスパイラルレビューの提案、情報処理学会論文誌、査読有、Vol.52、No.9、pp.2853-2865、http://id.nii.ac.jp/1001/00077508/

⑤ 橋本正樹、金美羅、辻秀典、田中英彦、論理プログラミングを基礎とした認可ポリシ記述言語、情報処理学会論文誌、査読有、Vol.51, No.9、2010 年、pp.1682-1692、http://id.nii.ac.jp/1001/00070341/

⑥ 荒井正人、田中英彦、機密情報共有に有用な情報フロー制御モデルの提案、情報処理学会論文誌、査読有、Vol.51、No.2、2010 年、pp.635–647、http://id.nii.ac.jp/1001/00067985/

⑦ 大久保隆夫、田中英彦、効率的なセキュリティ要求分析手法の提案、情報処理学会論文誌、査読有、Vol.50、No.10、2009 年、pp.2484-2499、http://id.nii.ac.jp/1001/00066497/

⑧ 堀合啓一、今泉隆文、田中英彦、マルウェア亜種の動的挙動を利用した自動分類手法の提案と実装、情報処理学会論文誌、査読有、Vol.50、No.4、2009 年、pp.1321-1333、http://id.nii.ac.jp/1001/00060496/

〔学会発表〕（計 23 件）

① Masaki Hashimoto, Mira Kim, Hidenori Tsuji, Hidehiko Tanaka, Policy Description Language for Dynamic Access Control Models, the 8th IEEE International Symposium on Dependable, Autonomic & Secure Computing, 2009.12.12, Chengdu, China.

② 橋本正樹、金美羅、辻秀典、田中英彦、論理型言語を用いたポリシー記述言語の研究、日本ソフトウェア科学会, DSW09、2009.7.15、函館大沼プリンスホテル.

６．研究組織

(1)研究代表者
田中 英彦（TANAKA HIDEHIKO）
情報セキュリティ大学院大学・情報セキュリティ研究科・教授
研究者番号：60011102

(2)研究分担者
辻 秀典（TSUJI HIDENORI）
情報セキュリティ大学院大学・情報セキュリティ研究科・客員准教授
研究者番号：90398975

(3)研究分担者
金 美羅（KIM MIRA）
情報セキュリティ大学院大学・情報セキュリティ研究科・客員研究員
研究者番号：60387107

(4)研究分担者
橋本 正樹（HASHIMOTO MASAKI）
情報セキュリティ大学院大学・情報セキュリティ研究科・助教
研究者番号：10582158