[解説]

アクセス制御技術とその最新動向

A Brief Review on Access Control Technologies

情報セキュリティ大学院大学 情報セキュリティ研究科　　橋　本　正　樹
Graduate School of Information Security Institute of Information Security　Masaki HASHIMOTO

要　旨

アクセス制御技術は，暗号技術と並び，最も伝統的で重要な情報セキュリティを支える要素技術である．アクセス制御技術は，機密性・完全性・可用性のいずれの保護にも関係する為，これを洗練し，情報セキュリティを担保する為の研究が半世紀近く前から継続的に行なわれている．本稿では，アクセス制御技術の理論と実装について簡単に解説し，セキュリティポリシモデル，ポリシ記述言語，ポリシ検証手法，アクセス制御メカニズムに整理して，近年の研究動向と今後の課題についてまとめる．

キーワード

アクセス制御，セキュリティポリシモデル，ポリシ記述言語，ポリシ検証手法，アクセス制御メカニズム

1. はじめに

アクセス制御技術は，情報セキュリティを支える最も基礎的な要素技術のひとつであり，機密性・完全性・可用性のいずれの保護にも関係する．この為，アクセス制御機能を TCB（Trusted Computing Base）としての OS から上位層に提供し，情報セキュリティを担保する為の研究が半世紀近く前から継続的に行われており，初期の研究成果は，TCSEC[1]にみることができる．また，近年では，ISO/IEC10181-3[2]として，高度に抽象化されたアクセス制御システムのモデルが標準化されている．本稿では，アクセス制御技術の理論と実装について概説し，その後，その主要な構成要素として，セキュリティポリシモデル，セキュリティポリシ記述言語，セキュリティポリシ検証技術，アクセス制御メカニズムについて，それぞれ近年の研究動向を紹介し，今後の課題について述べる．

2. アクセス制御技術の理論と実装

アクセス制御においては，ある情報システム S が取りうる保護状態の集合を P，認可された保護状態の集合を Q とした時，S の保護状態が Q である時に，S はセキュアであると考える．逆に，S の保護状態が P–Q（P のどの要素も Q の要素と異なる）の保護状態となった時，S はセキュアではないと考える．この保護状態は，情報システムが変化する時，合わせて変化するものであると考える．例えば，あるコマンドが情報システムを変化させる時，保護状態の遷移が起こる．状態遷移後の保護状態は帰納的に定めるのが通例で，すなわち，認可された保護状態から許可された権限による操作によって状態遷移が発生した時，遷移後の保護状態も認可されたものであると考えるのが一般的である．

アクセス制御マトリクスモデル[3][4][5]は，この理論的基礎を最も単純明快に表現するモデルで，元々OS 研究とデータベース研究の双方から検討が進

められてきたものである．これは，名前の通り，マトリクスを用いて許可する権限を定義し，情報システムの保護状態を記述する．例えば，ある保護状態をアクセス制御マトリクスに記述するには，表側にアクセス主体となるシステム要素(プロセス等)を，表頭にアクセス対象となるシステム要素（ファイル等）を羅列し，各セルに当該アクセス主体がアクセス対象に対して許可された権限を設定・記述すれば良い．

アクセス制御マトリクスモデルの実装に関しては，幾つかの課題があることが知られている．一つ目は，典型的な情報システムにおいて，アクセス主体とアクセス対象の数が膨大である為，マトリクスのサイズも合わせて大きくなることである．二つ目は，ほとんどのセルが，空白か同じ内容となることで，三つ目は，単純なアクセス主体やアクセス対象の追加・削除がマトリクス全体に大きな影響を与えることもある為，この操作を慎重に，場合によっては複雑なコードで実現する必要があることである．これらの課題を解決する為に，数多くの研究が非常に古くから行われており，例えば，第 6 章で紹介する ACL 方式や Capability 方式は，最も伝統的で強力なアクセス制御マトリクスの実装方式であろう．

3. セキュリティポリシモデル

情報システムは，その用途に応じて様々な水準の機密性・完全性・可用性を必要とする為，この特性を反映した様々なセキュリティポリシモデルが従来から研究されてきた．主要な類型は，機密性保護型，完全性保護型に加え，これらの混成型で，各類型の代表的なセキュリティポリシモデルは，機密性保護型として Bell-LaPadula モデル[6]，完全性保護型として Biba Integrity モデル[7]と Clark-Wilson モデル[8]，混成型として Chinese Wall モデル[9]と RBAC モデル[10], [11]などがある．以下に，近年の代表的なセキュリティポリシモデルの研究例を示す．

RBAC モデルは，Role（役割）を中核としたセキュリティポリシモデルで，情報システム内のアクセス制御を実世界の組織構成と各人の責務に合わせて実現し易い為，直感的に理解しやすく，正しく運用すれば最小特権の原則に沿ったアクセス制御を実現可能である為，SELinux や Solaris を始めとした様々な OS で採用が進んでいる．RBAC モデルの近年の研究成果としては，RBAC モデルの形式的な定義と基礎モデルの拡張[12]や，RBAC モデルの標準化・ANSI 標準への採用[13]がある．その他にも，RBAC モデルには，誰がどのように RBAC システム内の様々な関係を設定するべきか，という管理上の課題があるが，これに対しては，ARBAC の諸研究[14],[15]や，管理上の課題に焦点をあてた RBAC モデルの分析がある[16]．また，実際の OS に実装された RBAC モデルについて，そのセキュリティ特性を形式的に検証する方法も提案されている[17]．

TBAC モデル[18]は，Authorization Step (AS) として複数の認可を認可手順としてグループ化し，アクセス主体・アクセス対象・操作内容に加えて，AS 名と AS 内の工程名を指定して認可判定を決定するセキュリティポリシモデルである．TBAC では，AS 毎にサブジェクトに付与するアクセス権限を，その前後関係を考慮しながら逐次有効化・無効化する為，例えば，トランザクションの処理状況に応じて細かなアクセス権限を指定できる．これにより，TBAC は，特定の認可手順を抽象的に構造化し，サブルーチンのように繰り返し利用可能とすることで，ポリシ全体の見通しを向上することができる．

4. セキュリティポリシ記述言語

セキュリティポリシ記述言語は，セキュリティポリシを表現する為のもので，アクセス制御の仕様を記述する言語として見ることができる．近年，セキュリティポリシ記述言語の研究では，述語論理を始めとする数理論理学の知見を応用した研究が行われており，主要な課題は，アクセス権限の委譲・制限・否定等に対する表現力，人間にとっての文法的な明快さ・読み易さ，簡潔で明快な意味論，効率的な認可判定手順，拡張性などがある．以下に，近年の代

表的なセキュリティポリシ記述言語の研究例を示す.

SecPAL[19]は，比較的大規模なシステムで，セキュリティポリシを管理領域毎にモジュール化して構成することを前提とし，分散管理された領域間でアクセス権限の委譲を柔軟に記述する為のセキュリティポリシ記述言語である．SecPAL は，制約論理言語による高レベルなセキュリティポリシ記述言語で，認可判定要求は節の集合に対する問い合わせが成功した時に承認される．SecPAL の文法は自然言語に近く，意味付けは三つの推論ルールから構成されており，否定的なクエリや再帰的な述語，回数を指定可能な権限委譲やその他様々な制限をサポートすることで，多くのセキュリティポリシモデルを汎用的に表現可能である．SecPAL は，クラウド OS である Windows Azure のセキュリティポリシ記述言語として実装する為に，現在も研究が進められている．

Lithium[20]は，論理的な否定を形式的に正しく推論できるセキュリティポリシ記述言語である．Lithium は，一階述語論理を基礎にした高レベル言語で，再帰的な表現を制限することで否定を含んだ推論を実現している．Lithium は，例えば，複数のポリシをマージしてそのアクセス制御仕様を分析する場合に，あるアクセスが未認可であることを形式的に確認できる点で有用であるが，一方で，多くのセキュリティポリシモデルで必要となる，アクセス権限の委譲を簡潔に表現できない課題がある．Lithium には，その文法や一階述語論理の知識がなくとも利用可能とする為に，通常の英文法によってポリシ記述ができるようなフロントエンドも開発されている[21].

5. セキュリティポリシ検証

セキュリティポリシ検証は，セキュリティポリシが特定のアクセス制御に関する仕様を満たすことを検証する為の技術である．近年の情報システムは大規模・複雑化している為，前節で紹介したような言語によるセキュリティポリシの記述量が特に増大する傾向にあり，実現されるアクセス制御仕様を人間が明快に把握できないことが多い．この課題に対処する為に，記述されたセキュリティポリシを容易に解析する為の検証手法が求められており，活発な研究が進められている．以下に近年の代表的なセキュリティポリシ検証の研究例を示す.

RBAC-PAT[22]は，ARBAC ポリシを対象として，ある Role を始点にした時の情報流の到達性や可用性，情報システムの区画化，最弱点等を検証することができる．RBAC-PAT は，複数の管理者によってアクセス権限の変更が随時行われるような ARBAC モデルでは，ポリシの分析が困難となる課題に対処している．具体的には，あるユーザに対する特定 Role の到達性・可用性や，Role 間の内包性・最小セット等の関係，不要 Role の発見，オブジェクト間の情報流を検証することができる.

PALMS[23]は，MLS ポリシの形式的な仕様を定義することで，分析対象の MLS ポリシに存在する全情報流を検証することができる．また，二つの MLS ポリシ間の整合性を自動的に検証することができる．PALMS は，Prolog ベースのツールとして実装されており，与えられた MLS ポリシが，*プロパティやシンプルセキュリティコンディション等を満たすこと，アプリケーションの MLS ポリシが，そのホスト OS の MLS ポリシと整合性が取れていること等を検証することができる．PALMS は，MLS ポリシのみを対象としているが，現実の情報システムでは，複数のセキュリティポリシモデルが連携する場合が多い為，MLS ポリシと他のセキュリティポリシモデルが連携する際にも検証可能とするように研究が進められている.

6. アクセス制御メカニズム

アクセス制御メカニズムは，セキュリティポリシ記述言語によって記述された個々のアクセス制御規則を情報システムに強制する為の仕組みである．具体的な実装手法としては，ACL 方式と Capability 方式が従来から存在し[24]，長年 ACL 方式が広く採用されてきたが，最小特権の原則によるアクセス制

御を実現し易い利点がある為，Capability 方式の研究も継続されている．また，セキュリティポリシとの連携に重点を置いた強制アクセス制御機構を既存の OS に追加する為の研究も行われている．以下に，近年の代表的なアクセス制御メカニズムの研究例を示す．

seL4[25]は，L4 マイクロカーネルをベースにセキュリティ拡張を行った研究用 OS で，take-grant モデル[26]を Capability 方式と組み合わせて実装し，各種カーネルオブジェクトに対するアクセス制御を実現している．ここで，L4 のカーネルオブジェクトとは，スレッド，アドレス空間，プロセス間通信，未使用の物理メモリを示す untyped-memory で，これらに対するアクセス権限は Capability を通して授受する仕組みになっている．別の Capability 方式による研究例としては，Capsicum[27]がある．Capsicum は，UNIX の標準 API を拡張する研究用 OS で，Capability を用いることでプロセスやアプリケーションのサンドボックス化を容易且つ細粒度に実現している．Capsicum は，OS からアプリケーション層の区画化を一元的に制御するのではなく，個々のアプリケーションが自身の区画化を容易に実現できるよう OS として支援するという設計思想で研究が進められている．

Flask セキュリティアーキテクチャ（FLSA）[28]は，セキュリティポリシによる決定を強制的に執行するオブジェクトマネージャと，与えられたセキュリティポリシに従ってアクセス可否の決定を下すセキュリティサーバから構成される．各々は，あらかじめ定められたプロトコルに従ってデータ通信を行い，FLSA 全体として参照モニタの役割を果たす．FLSA は，様々なセキュリティポリシモデルを柔軟に実現できることが大きな特徴である．SELinux は FLSA の Linux に対する実装で，その他，SEBSD も FLSA の実装例である．同様の強制アクセス制御機構としては，TrustedBSD MAC Framework[29]が提案されており，FreeBSD や Darwin に実装されている．

7. まとめと今後の課題

アクセス制御技術は，比較的古くから研究が進められてきたもので，最も基礎的な理論は既に確立されている．同時に，情報セキュリティへの要請の変遷に合わせて，継続的にその拡張や応用が求められており，近年では，情報システムの社会基盤化に合わせて，前節までに紹介したような諸研究が進行中である．

今後の課題は，仮想化技術を基礎としたクラウド環境や，スマートフォンを始めとした組み込み環境等，要請されるアクセス制御仕様や，これを実現する為の前提が異なる環境にこれらの成果を応用することである．具体的には，分散システム向けのセキュリティポリシモデルやその記述言語，それを強制する分散アクセス制御メカニズムが求められており，これに向けた研究は，既に各所で検討が進められている．例えば，FLSA の適用範囲を，スタンドアローン・システムの OS 層で捕捉可能な対象から，アプリケーション層や他システムの対象に拡張する為のアクセス制御メカニズム等が研究されている[30][31]．

参考文献

[1] US Department of Defense: Trusted Computer Systems Evaluation Criteria, Technical Report CSC-STD-001-83, DoD Computer Security Center, Fort Meade, MD (1983).

[2] International Organization for Standardization (ISO): Information Technology - Open Systems Interconnection - Security Frameworks in Open Systems - Part 3: Access Control, Technical report, ISO/IEC 10181-3 (1996).

[3] B. Lampson: Protection, Proceedings of the Fifth Princeton Symposium of Information Science and Systems, pp. 437-443 (Mar. 1971); reprinted in Operating Systems Review 8(1), pp. 18-24 (Jan. 1974).

[4] P. Denning: Third Generation Computer Systems, Computing Surveys 3 (4), pp.175-216 (Dec. 1971).

[5] G. Graham and P. Denning: Protection-Principles and Practice, Spring Joint Computer Conference, AFIPS Conference Proceedings 40, pp.417-29 (1972).

[6] Bell, D. and LaPadula, L.: Secure computer systems: mathematical foundations and model, Technical Report M74-244, The MITRE Corporation, Bedford, MA (1973).

[7] Biba, K.J.: Integrity Considerations for Secure Computer Systems, Technical Report MTR-3153, The MITRE Corporation, Bedford, MA (1977).

[8] Clark, D. and Wilson, D.: A comparison of commercial and military computer security models, Proceedings of the IEEE Computer Society Symposium on Security and Privacy, IEEE Computer Society, pp.184-194 (1987).

[9] Brewer, D. and Nash, M.: THE CHINESE WALL SECURITY POLICY, Proceedings of the IEEE Computer Society Symposium on Security and Privacy, IEEE Computer Society, p.206 (1989).

[10] Ferraiolo, D., Cugini, J. and Kuhn, D.: Role-based access control (RBAC): Features and motivations, Proceedings of 11th Annual Computer Security Application Conference, pp.241-48 (1995).

[11] Ferraiolo, D. and Kuhn, R.: Role-Based Access Control, In 15th NIST-NCSC National Computer Security Conference (1992).

[12] Sandhu, R., Coyne, E., Feinstein, H. and Youman, C.: Role-based access control models, Computer, Vol.29, No.2, pp.38-47 (1996).

[13] Ferraiolo, D., Sandhu, R., Gavrila, S., Kuhn, D. and Chandramouli, R.: Proposed NIST standard for role-based access control, ACM Transactions on Information and System Security (TISSEC), Vol.4, No.3, pp.224-274 (2001).

[14] Sandhu, R. and Bhamidipati, V.: Role-based administration of user-role assignment: The URA97 model and its Oracle implementation, Journal of Computer Security, Vol.7, No.4, pp.317-342 (1999).

[15] Sandhu, R., Bhamidipati, V. and Munawer, Q.: The ARBAC97 model for role-based administration of roles, ACM Transactions on Information and System Security (TISSEC), Vol.2, No.1, pp.105-135 (1999).

[16] Crampton, J. and Loizou, G.: Administrative scope: A foundation for role-based administrative models, ACM Transactions on Information and System Security (TISSEC), Vol.6, No.2, pp.201-231 (2003).

[17] Jha, S., Li, N., Tripunitara, M., Wang, Q. and Winsborough, W.: Towards formal verification of role-based access control policies, IEEE Transactions on Dependable and Secure Computing, pp.242-255 (2007).

[18] Thomas, R. K. and Sandhu, R. S.: Task-Based Authorization Controls (TBAC): A Family of Models for Active and Enterprise-Oriented Autorization Management, Proceedings of the IFIP TC11 WG11.3 Eleventh International Conference on Database Security XI: Status and Prospects, London, UK, UK, Chapman & Hall, Ltd., pp.166-181 (1998).

[19] Becker, M., Fournet, C. and Gordon, A.: Design and Semantics of a Decentralized Authorization Language, CSF '07: Proceedings of the 20th IEEE Computer Security Foundations Symposium, Washington, DC, USA, IEEE Computer Society, pp. 3-15

(2007).

[20] Halpern, J. and Weissman, V.: Using first-order logic to reason about policies, ACM Transactions on Information and System Security (TISSEC), Vol.11, No.4, pp.1-41 (2008).

[21] Weissman, V. and Lagoze, C.: Towards a Policy Language for Humans and Computers, Research and Advanced Technology for Digital Libraries (Heery, R. and Lyon, L., eds.), Lecture Notes in Computer Science, Vol.3232, Springer Berlin / Heidelberg, pp.513-525 (2004).

[22] Gofman, M., Luo, R., Solomon, A., Zhang, Y., Yang, P. and Stoller, S.: RBAC-PAT: A Policy Analysis Tool for Role Based Access Control, Tools and Algorithms for the Construction and Analysis of Systems (Kowalewski, S. and Philippou, A., eds.), Lecture Notes in Computer Science, Vol.5505, Springer Berlin / Heidelberg, pp.46-49 (2009).

[23] Guttman, J., Herzog, A., Ramsdell, J. and Skorupka, C.: Verifying information flow goals in security-enhanced Linux, Journal of Computer Security, Vol.13, No.1, pp.115-134 (2005).

[24] Saltzer, J. and Schroeder, M.: The protection of information in computer systems, Proceedings of the IEEE, Issue 9, Vol.63, pp.1278-1308 (1975).

[25] Klein, G., Elphinstone, K., Heiser, G., Andronick, J., Cock, D., Derrin, P., Elkaduwe, D., Engelhardt, K., Kolanski, R., Norrish, M., Sewell, T., Tuch, H. and Winwood, S.: seL4: formal verification of an OS kernel, Proc. of SOSP'09, pp.207-220(2009).

[26] Lipton, R.J. and Snyder, L.: A Linear Time Algorithm for Deciding Subject Security, J. ACM, Vol.24, pp.455-464 (1977).

[27] Watson, R.N.M., Anderson, J., Laurie, B. and Kennaway, K.: Capsicum: practical capabilities for UNIX, Proceedings of the 19th USENIX conference on Security, USENIX Security'10, Berkeley, CA, USA, USENIX Association, pp.3-3 (2010).

[28] Spencer, R., Corporation, S.C., Smalley, S., Loscocco, P., Agency, N.S. and Andersen, M. H.D.: The Flask Security Architecture: System Support for Diverse Security Policies, Proceedings of the 8th USENIX Security Symposium, pp.123-139 (1999).

[29] Watson, R.N.M.: TrustedBSD: Adding Trusted Operating System Features to FreeBSD, Proceedings of the FREENIX Track: 2001 USENIX Annual Technical Conference, Berkeley, CA, USA, USENIX Association, pp.15-28 (2001).

[30] KaiGai, K.: Security Enhanced PostgreSQL (2006).
http://code.google.com/p/sepgsql/.

[31] Macmillan, K., Brindle, J., Mayer, F., Caplan, D., Tang, J. and Technology, T.: Design and implementation of the SELinux policy management server, Proceedings of the Security Enhanced Linux Symposium, pp.1-6 (2006).

（受付日：2016年1月20日）

著者略歴

橋本正樹(はしもと・まさき)　博士(情報学). 2001年, 立命館大学文学部人文総合科学インスティテュート卒業. 学部在籍時より新規法人の立ち上げに参画し, 以降同社にて情報システムの運用管理・監視サービス業務に従事. 2007年, 情報セキュリティ大学院大学情報セキュリティ研究科博士前期課程

修了．2010 年，同博士後期課程修了．2010 年より同助教，2014 年より同准教授．2014 年 4 月からの 1 年間は，英国の Royal Holloway, University of London にある Information Security Group に訪問学術研究員として滞在．専門はアクセス制御，OS セキュリティ．情報処理学会，電子情報通信学会，日本ソフトウェア科学会，IEEE 各会員．電子情報通信学会情報通信システムセキュリティ研究会（ICSS）専門委員，情報処理学会コンピュータセキュリティ研究会（CSEC）運営委員．情報処理学会コンピュータセキュリティシンポジウム 2016（CSS2016）実行委員，NETSAP 2016: The 6th IEEE International Workshop on Network Technologies for Security, Administration and Protection Program Committee 等.