社団法人　情報処理学会　研究報告
IPSJ SIG Technical Report

2005－DSM－38（9）
2005／8／5

インターネットにおける組織間システム連携時のアクセス制御に関する考察

市川本浩[†,††]　河合栄治[†]
藤川和利[†]　砂原秀樹[†]

近年，インターネットは普及と接続環境の整備に伴い利用環境の社会的な基盤としての役割が増しつつある．基盤化に伴い多様な利用形態が増しつつある．利用形態の多様化や変化に伴い従来ではあまり考慮されていなかったサービスの提供や利用およびリソースの共有や交換におけるポリシー等の策定とシステムの一部として反映の必要性が生じつつある．ポリシーの異なる組織間のアクセスにおいても異なるポリシーの提示および許諾や制御等がシステムの一部として求められつつある．本稿では組織間のネットワークやネットワークを介したシステム間のアクセス制御に関する考察を行い必要とされるアクセス制御についての議論を行う．

A consideration of the access control for the interorganizational system coalition in the Internet

Motohiro Ichikawa,[†,††] Eiji Kawai,[†] Kazutoshi Fujikawa[†]
and Hideki SUNAHARA[†]

In recent years, the Internet is increasing a role of the social infrastructure with maintaining of spread and communication environment. Various usages are increasing with the infrastructure. Currently, necessity is arising for system offering the service of decision of the policy with diversification and change of usages. The system is increasing needs to be designed with different protocol and consent of a policy, the control in access during organizations. In this paper, we discuss the access control needed by acting consideration about the access control during organizations network federation.

1. はじめに

インターネット接続環境の整備[1)2)]に伴い，社会的な基盤としての性格を帯びつつある．これに伴いテレワークと呼ばれる在宅勤務，モバイルワーク，サテライトオフィスといった利用形態が増えつつあり，多様な利用形態の増加や期待が増しつつある[1)]．しかしながら，企業通信網の利用上または利用を妨げる問題点[1)]として，「セキュリティ対策の確立が困難」「ウィルス感染に不安」「従業員のセキュリティ意識が低い」等が挙げられている．1980年9月にOECD理事会より勧告された「プライバシー保護と個人データの国際流通についてのガイドライン」に基づいた個人情報保護基本法制[3)]への対応ならびに考慮も必要とされつつある．

これらの状況を背景に低コストで効率的な運用や一貫したセキュリティ対策等を目的として，通信系や情報系システムを中心に集約的に管理する論理統合と呼ばれる流れが進行しつつある．

通信系では，システムの運用方針(ポリシー)[4)5)]や提供および利用サービス達成目標合意(Service Level Agreement)[6)]を定め適切にシステムへ対応および適用させる為，IETFとDesktop Management Task Force (DMTF)によるPolicy Framework WG[7)~11)]やResource Allocation Protocol Working Group[12)~13)]を中心として提案規格化されている．

Quality of Service (QoS)領域を中心に多様なシステム間の制御運用ポリシーを対象にHASHMANIら[15)]によるポリシー管理，江端ら[16)17)]や加藤[18)]によるポリシー適用や配布等の研究および提案が行われている．

情報系では，いわゆるオープンシステムを中心に1980年代中頃よりNIS NetInfo Kerberos/LDAP等の技術や考え方により認証や管理情報の統合が行われて来た．1980年代前半にまとめられた主に軍用用途(DoD5200.28-STD Trusted Computer System Evaluation Criteria)を主体とし形成されたISO/IEC

† 奈良先端科学技術大学院大学 情報科学研究科
Graduate School of Information Science, Nara Institute of Science and Technology
†† 株式会社 エーティエル システムズ
ATL Systems, Inc.

15408 の品質評価基準に基づく Trusted OS やその考え方を取り入れた Secure OS を基にアプリケーション・サーバーや利用機器のセキュリティ対策を目的としてプロセス間の関係について拡張し Mandatory Access Control (MAC) と呼ばれる考え方により運用ポリシーをシステム全体に適用し制御する仕組みが提案実装されつつある．

以上の概観に基づき本稿では，システム間のアクセス制御について議論する．ここでシステム間のアクセス制御とは，異なるポリシーに基づいた管理単位間のインターネット関連技術によるシステムを利用したサービスやリソースの連携や交換におけるアクセス制御とする．第 2節では現状の問題点について述べ，第 3節では第 2節で述べた問題点について考察し，第 4節では考察に基づいた指針を示し，第 5節でまとめる．

2. 問 題 点

通信系を中心に様々なネットワーク・システムの運用ポリシーを統合的に管理制御するため，論理統合の方向へ基盤整備が進められている．情報系では，組織内の認証管理を中心に同様な方向に進みつつある．しかしながら，システム全体として統合的に扱おうとすると幾つかの問題が生じる．組織間や運用ポリシーの異なる管理単位の連携時にデータ管理手法においても問題がある．問題点として大まかに 2 点の項目が挙げられる．

通信系のポリシーは，$P = \{r1, r2, \cdots, rn\}$ と表現されるポリシー規則のならびにより構成されている[7)8)19)]．ポリシー規則は，if 条件 then 動作型である．しかしながら，情報系ではポリシー規則の表とならびにより構成されていることが多い[20)]．ポリシー規則は role[21)] と呼ばれる属性や管理対象に付加されたタグの集合と if 条件 then 動作型の組み合わせとなっている．つまり，管理および制御の考え方が異なる為に通信系の考え方のみではきめ細かな制御が行いにくくかつ情報系の考え方を網羅すると通信系の管理および制御としては過剰となり効率性や運用性が損なわれる．

運用ポリシーの統合的管理や統合集約された管理情報は，透過的な信頼関係を前提とし構築されている．つまり，認証等により信頼関係を得られると収集情報や登録情報について考慮または参照提示用のデータ範囲を限定もしくは別途規定しない限りは透過的に参照や提示可能となってしまう．その際に意図しない情報，たとえばポリシーや管理情報に内部的な情報や個人情報保護基本法制[3)] でのセンシティブな情報が含まれている場合に問題となる．データの参照提示範囲を限定もしくは別途規定した場合，制御情報として不足したり登録情報に重複が生じたりする可能性がある．

3. 問題点に関する考察

本節では，第 2節で挙げた問題点に基づき考察する．

通信系と情報系のポリシーの異なる考え方を統合的に扱おうとする場合，たとえば，不正アクセス検知ならびその対応の領域では，ファイアウォールと Intrusion Detection System (IDS) および Intrusion Prevention System (IPS) の連携として松本ら[24)] によるダイナミックディフェンスや，保理江ら[22)23)] による動的アクセスポリシー制御がある．これらは，あらかじめ決められたポリシーを適用し一定のシナリオに基づく動的な制御を行っている．ダイナミックディフェンスでは，ファイアウォールはいわゆる IETF AAA[25)~28)] での Policy Enforcement Point (PEP) であり，IDS や IPS は Policy Decision Point (PDP) と表せ一方向の関係となっている．保理江らの動的アクセスポリシー制御は，システム内部的にアクセスポリシー制御から得られる検出条件に合わせ動的に適用される縮退と呼ばれるポリシーの状態に遷移させるものであり，拡張アクセスポリシーによる系に閉じた状態遷移の仕組みである．いずれの例も一方向の制御もしくは同一の制御ポリシーに基づいた考え方や仕組みであり，ポリシー管理手法や適用範囲の異なる考え方の単位間の相互連携の想定は考慮されていない．つまり，相互に PEP および PDP が配置され PDP 間の調停（提示，許諾）に基づく制御を前提とする場合，再考が必要と考えることができる．

運用ポリシーの統合的管理や統合集約された管理情報では，集約を行うデータベースとしてディレクトリ・サービスの一種である LDAP を利用する事が多い．LDAP[29)] は，X500 のアクセスモデルを踏襲している．従って，Directory Information Tree (DIT) で構成される識別名 Distinguished Name (DN) 単位のアクセス制御は可能であるが，属性情報の一部のみのきめこまやかな制御は難しい．たとえば，属性情報に制御に必要とされる情報以外にいわゆるセンシティブ情報[3)] が含まれる場合，状況は複雑になってくる．鈴木ら[30)] は PKI で利用される X509v3 での Subject Alternative Name Area における OtherName に格納される Credential となりえる情報の扱いについて指摘を行っている．現状，管理単位が異なっても別途，共通のポリシーを策定し連携を行うのが一般的である．しかしながら，きめ細やかな制御や Sigle Sign-On (SSO) といった認証連携を考える場合に管理の粒度や即時性等の側面で問題となる．したがって，集約された管理情報により，組織間の分散的なアクセス制御や管理ポリシーの異なる場合には，何

らかの表明情報に基づいた可否制御の仕組みが必要と考えることができる．

4. 提　　案

本節では，第2節および第3節に基づき，問題解決の方針について述べる．

昨今，Web Service と呼ばれる HTTP による Web ブラウザを利用したサービスと主にシステム間の連携を目的とした SOAP[31] や XML-RPC[32] を利用した RPC サービスがある．Web Service では，HTTP のセッション管理の特性を背景に認証連携を中心とし段階的なオーソリティ (認証，権限・役割，制御) を基本に試みがなされつつある[33)~35)]．これらは，現状，Web コンテンツの連携性による試みのみであるが，前節まで述べてきた事柄に関して補間する仕組みが提案されつつある．本提案では，これらの試みにおいて用いられている OASIS Security Assertion Markup Language (SAML)[36] と呼ばれる XML による広範囲な認証，認可のための仕様を用いてポリシーの異なる組織間のシステム連携時に必要とされるアクセス制御について整理する．整理は，通信系と OS を中心とした情報系における制御点としての PEP と PDP の関係を明らかにする．それぞれの Subject と Object についても整理を行い，連携についての提案を考えている．SAML 仕様の有効性の評価および，仕様の前提として必要とされる信頼関係を保証するための認証の枠組みとの親和性についても評価を行う予定である．

5. ま と め

本稿では，インターネット上でポリシーの異なる組織間のシステム連携時にアクセス制御に必要とされる問題点を明らかにし考察そして解決手法についてかいつまんで述べてきた．今後の取り組みとして，第4節で述べた方針に基づき SAML の仕様に基づき整理し提案，実装，そして，評価を行う予定である．

参 考 文 献

1) 政策統括官 (情報通信担当) 総合政策課情報通信経済室: 平成１６年「通信利用動向調査」の結果, 総務省, (2005).
2) 総務省政策統括官（情報通信担当）総合政策課: 日本のＩＣＴインフラに関する国際比較評価レポート, 総務省, (2005).
3) 内閣府: 個人情報の保護に関する法律, http://www.kantei.go.jp/jp/it/privacy/houseika/hourituan/ .
4) J. Moffett, M. Sloman: Policy Hierarchies for Distributed Systems Management, IEEE Journal on Selected Areas in Communication, Vol. 11 No. 9, pp.1404-1414 (12 1993).
5) P. Flegkas, P. Trimintzios, G. Pavlou, I. Andrikopoulos, F. Cavalcanti: On Policy-based Extensible Hierarchical Network Management in QoS-enabled IP Networks, Proceedings of the IEEE Workshop on Policies for Distributed Systems and Networks (POLICY ’ 01), Bristol, UK, pp. 230-246. (1 2001).
6) Office of Government Commerce (OGC): Information Technology Infrastructure Library (ITIL), Office of Government Commerce (OGC).
7) B. Moore, E. Ellesson, J. Strassner, A. Westerinen: Policy Core Information Model, RFC 3060, (2 2001).
8) B. Moore, Ed.: Policy Core Information Model (PCIM) Extensions, RFC 3460, (1 2003).
9) J. Strassner, B. Moore, R. Moats, E. Ellesson: Policy Core Lightweight Directory Access Protocol (LDAP) Schema, RFC 3703, (2 2004).
10) K. McCloghrie, M. Fine, J. Seligson, K. Chan, S. Hahn, R. Sahita, A. Smith, F. Reichmeyer: Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2), RFC 3159, (8 2001).
11) K. McCloghrie, M. Fine, J. Seligson, K. Chan, S. Hahn, R. Sahita, A. Smith, F. Reichmeyer: Structure of Policy Provisioning Information (SPPI), RFC 3159, (8 2001).
12) D. Durham, Ed., J. Boyle, R. Cohen, S. Herzog, R. Rajan, A. Sastry: The COPS (Common Open Policy Service) Protocol, RFC 2748, (1 2000).
13) K. Chan, J. Seligson, D. Durham, S. Gai, K. McCloghrie, S. Herzog, F. Reichmeyer, R. Yavatkar, A. Smith: COPS usage for Provisioning (COPS-PR), RFC 3084, (3 2001).
14) S. Herzog, Ed., J. Boyle, R. Cohen, D. Durham, R. Rajan, A. Sastry: COPS usage for resource ReSerVation Protocol (COPS-RSVP), RFC 2749, (1 2000).
15) Manzoor HASHMANI, Mikio YOSHIDA, Takeshi IKENAGA, Yuji OIE: Management and Realization of SLA(Service Level Agreement)for Providing Network QoS, Technical Report of IEICE IN2000-103, pp.55-62 (10 2000).
16) T. Ebata, M. Takihiro, S. Miyake, M. Koizumi: Inter-Domain QoS Provisioning and Accounting, INET2000 Proceedings, Internet Society (ISOC), (2000).
17) 江端智一, 滝広眞利, 三宅滋, 小泉稔: QoS 保証対

応アクティブネットワーク組織間 QoS 制御方式, ネットワーキングアーキテクチャワークショップ資料, (2001).
18) 加藤 優一: ポリシーベースの分散ネットワークにおける QoS の研究, 筑波大学大学院博士課程システム情報工学研究科修士論文, (2004).
19) Damianou, N., N. Dulay, E. Lupu and M. Sloman: The Ponder Policy Specification Language, Workshop on Policies for Distributed Systems and Networks (Policy2001), HP Labs Bristol, 29-31 (01 2001).
20) Matt Bishop: Computer Security (ISBN 0-201-44099-7), Addison-Wesley, Pearson Education, Inc, (2003).
21) David F. Ferraiolo, Ravi Sandhu, Serban Gavrila, D. Richard Kuhn, Ramaswamy Chandramouli: Proposed NIST Standard for Role-Based Access Control, ACM Transactions on Information and System Security, Vol. 4, No. 3, pp.224-274 (08 2001).
22) 保理江 高志, 桝本 圭, 宮本 洋輔, 原田 季栄, 田中 一男: OS カーネルにおける動的アクセス制御, 情報処理学会研究報告, 2003-CSEC-023, Vol.2003 No.126, (12 2003).
23) 保理江 高志: 〔招待論文〕ＯＳカーネルへのＩＤＳ・ＩＰＳ機能拡張　一概念, 実装及び応用について一, 信学技報 CS2004-47, pp.35-42 (09 2004).
24) 松本 直人, 中野 哲也, 長野 邦寿, 伊藤 栄二, 木下 新一, 中村 かおり, 小宮 一郎, 岩井 博樹, 高橋 正和: ダイナミックディフェンスの概要と適用について, Japan Network Security Association Dynamic Defense Working Group, (12 2000).
25) C. de Laat, G. Gross, L. Gommans, J. Vollbrecht, D. Spence: Generic AAA Architecture, RFC 2903, (08 2000).
26) J. Vollbrecht, P. Calhoun, S. Farrell, L. Gommans, G. Gross, B. de Bruijn, C. de Laat, M. Holdrege, D. Spence: AAA Authorization Framework, RFC 2904, (08 2000).
27) J. Vollbrecht, P. Calhoun, S. Farrell, L. Gommans, G. Gross, B. de Bruijn, C. de Laat, M. Holdrege, D. Spence: AAA Authorization Application Examples, RFC 2905, (08 2000).
28) S. Farrell, J. Vollbrecht, P. Calhoun, L. Gommans, G. Gross, B. de Bruijn, C. de Laat, M. Holdrege, D. Spence: AAA Authorization Requirements, RFC 2906, (08 2000).
29) M. Wahl, T. Howes, S. Kille: Lightweight Directory Access Protocol (v3), RFC 2906, (12 1997).
30) セコム IS 研究所: 「サイバーセキュリティ読本」, http://www.secom.co.jp/isl/j/cs_reader/ .
31) World Wide Web Consortium (W3C): XML Protocol Working Group, http://www.w3.org/2000/xp/Group/ .
32) Dave Winer: XML-RPC, http://www.xml-rpc.com/ .
33) Liberty Alliance Project: Liberty Alliance, http://www.projectliberty.org/ .
34) Internet2 Middleware: Shibboleth Project, http://shibboleth.internet2.edu/ .
35) Organization for the Advancement of Structured Information Standards (OASIS): OASIS Web Services Security (WSS) TC, http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss .
36) Organization for the Advancement of Structured Information Standards (OASIS): OASIS Security Services (SAML) TC, http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security .