文脈に基づくアクセス権限制御による情報操作と機器操作の制御

Access Control with Filtering Information and Operating Devices based on a Context-Aware Security Model

城戸 聡 †, 飯島 正 ‡
Satoshi Kido†, and Tadashi Iijima‡
† 慶應義塾大学大学院 理工学研究科
‡ 慶應義塾大学　理工学部
†Graduate School of Science and Technology, Keio Univ.
‡Faculty of Science and Technology, Keio Univ.

要旨

アクセス権限制御技術は，情報へのアクセスだけではなく，機器操作へも適用できる．情報の「読み」／「書き」操作だけではなく，機器に対するどのような操作を許可するかを規定することもアクセス権限制御の枠組みに含めることができる．一方で，特定の情報への操作も単純な「読み」と「書き」だけではなく，一部にモザイクを掛けて可視性を制限するような加工操作もありうる．更に，近年では，ウェアラブル端末の普及から，利用者の位置や時間といった文脈に基づいてアクセス制御を扱うことも注目されている．しかし，文脈に基づくアクセス制御の必要性は，ウェアラブル端末の利用時に限らず，より一般の状況での，より複雑化したアクセス制御の必要性も向上してきている．そこで，筆者らは，オブジェクト指向ペトリネットに基づいて文脈を表現するセキュリティモデルの構築を進めている．ここでは，筆者らが構築中のである，文脈に基づくセキュリティモデルについて報告する．

1. はじめに

本報告におけるアクセス制御モデルでは，特に，複数のデータ管理組織にまたがって分散されている情報にアクセスすることを想定している．従来，単一のデータベースにアクセスするのであれば，そのFacade としてのデータベース管理システムにアクセス制御モデルを組み込んでおくことで，アクセス制御を実現していた．しかし，情報資源が分散・管理される近年では，それを前提とすることが必ずしも有効ではなくなってきている．近年のアプリケーションソフトウェアは複数のデータ管理組織に対してアクセスしなければならず，組織間を移動する情報の一貫性を保たなければならない．そこで本報告では，分散した複数の情報資源へのアクセス制御を，抽象化し外部化することで共通的なフレームワークを構築することを試みている．もちろん，このモデルではアプリケーションソフトウェア側だけでアクセス制御ポリシーを強制することはできないので，情報資源側とアプリケーションソフトウェア側で協調してポリシーを順守するアクセス制御を成立させることになる．そこで本報告では，個別にプロセス表現を与えて協調動作させることができるモデルである，オブジェクト指向ペトリネットを文脈表現として採用している．

次節では，本報告で想定している具体的事例から，文脈を意識したアクセス制御 (Context-Aware Access Control: CxAC と略す) [1]，更には，文脈を意識した権限制御 (Context-Aware Authorization Control) の必要性を示す [1]．続く第 3 節では，nets-within-nets 意味論に基づくオブジェクト指向ペトリネットについて解説する．第 4 節では，CxAC の一つのサブクラスとして，ロールに基づくアクセス制御モデル (Role-Based Access Control: RBAC) [2] に文脈を取り入れた文脈指向ロールベースアクセス制御 (権限制御) モデルとモデルの適用例を示し，第 5 節においてその提案モデルのポリシー強制系の詳細設計に関して述べる．第 6 節では関連研究との比較を行い，本提案モデルの一般性を示す．

2. 具体的な想定事例

この節では，センサ情報の加工度合いによるアクセス制御例と機器操作への権限制御例に関して紹介する．一つ目の想定事例として，センサ情報の加工度合いによるアクセス権限制御を取り上げる．近年，監視カメラによる映像や交通系 IC カードから読み取られるデータなどのセンサ情報ビッグデータに対し，PPDM(Privacy Preserving Data Mining) というようなプライバシ保護を加えたデータ分析の必要性が認識されてきている．実際に，認知症高齢者介護施設にでは，監視カメラは介護活動を支援する一

[1] ここでは，情報へのアクセス制御と，通常，より一般性が高いとされる権限制御の間で特に区別を設けることはしない．機器操作の権限を有することを機器へのアクセスが許可されていると表現することもある．

手段としての有効性が認められているが，その監視によってプライバシが侵害されているとする考えも存在する．監視カメラに限らずセンサネットワークが普及すれば，セキュリティとプライバシに関する同様の議論が起こることは避けられない．現在でもプライバシ情報の利用と保護のバランスを取る方法の模索が続けられている．

センサ情報のプライバシ保護策として「情報の加工」(filtering) が考えられる．これにより，監視カメラの生映像をそのまま表示，録画するのではなく，映像から人の存在を感知し，人が在室しているかどうかという情報のみをモニタ画面に表示したり，赤外線サーモグラフィによって映像を加工することができる．しかし，こうした「情報の加工」により，情報の有用性に悪影響が生じる可能性もある．上記の例で言えば，認知症高齢者介護施設において，緊急時での被介護者救助の際も監視カメラを活用できなくなってしまう．こうした状況に陥った場合，被介護者の救助，ないしは避難を迅速に進めるため，介護側は加工されていない情報，つまり監視カメラの生映像にアクセスできるようにしなければならない．つまり，これまでの多くモデルが対象としてきた電子文書へのアクセス制御とは異なり，センサ情報へのアクセス制御では，情報の加工度合いを，状況に応じて動的に変更できる制御モデルが求められている．

二つ目の想定事例として，機器操作への権限制御を取り上げる．センサのような機器の操作権限では，電子文書情報へのアクセス制御とは異なり,「読み」／「書き」操作以外の権限も制御する必要がある．例えば，監視カメラの映像であれば，表示，停止，編集，ズームイン，ズームアウト等が挙げられる．しかし，これらの操作権限が常に利用者に付与されることは必ずしも有効ではない．コンビニエンスストアに設置されている防犯カメラの場合，顔認証機能が備わっているものも少なくないが，顔認証によって個人を特定する行為を，防犯カメラを設置している店舗の従業員ができてしまってはプライバシ問題が生じてしまう．一方，犯罪捜査等の特別な状況下では防犯カメラの映像の解析 (顔認証システムによる個人の特定等) を行わなければならない．よって，単にアクセス権限制御と言っても，情報へのアクセスだけではなく，機器操作へも適用することを想定し，情報の「読み」／「書き」操作だけではなく，機器に対するどのような操作を許可するかを規定することもアクセス権限制御の枠組みに含める必要がある．

以上のような想定事例において，電子文書情報を対象とした従来のアクセス制御モデル (RBAC など) を単純に適用した場合では，情報加工という条件付けや，機器操作への権限制御が困難である．そこで本報告では，筆者らが構築を続けている文脈に基づくアクセス制御モデル Context-Aware Access Control (CxAC) [1] を，センサ情報の情報加工や機器操作への権限制御 (Authorization Control) にまで拡張したモデルを提案している．

3. オブジェクト指向ペトリネット

本研究では，オブジェクト指向ペトリネットを，文脈を表現するモデルとして用いている．オブジェクト指向ペトリネットとは，オブジェクト指向概念に基づいてモジュール性を取り入れたペトリネットの拡張モデルであり，多くのものが提案されている．ここでは，nets-within-nets 意味論に基づく参照ネット (Reference Net) [3] の考え方を採用している．このモデルの例を示す (図 1)．

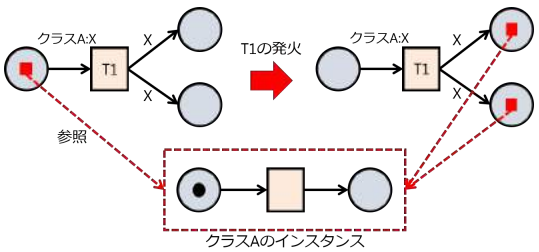


図 1: オブジェクト指向ペトリネットの例

参照ネットにおけるトークンには，単純トークン (Black Token)，参照トークン (Reference Token) という種類がある．単純トークンは，通常の P/T ネット (Place/Transition ネット) におけるトークンであり，プレースに存在する単純トークンはトークン数で示される．一方，参照トークンは，別のシステムを表現するサブネットへの参照 (reference) を持つトークンである．ここで，参照トークンを持つ側のネットをシステムネットと呼び，参照トークンが参照しているサブネットをオブジェクトネットと呼ぶ．参照トークンがトランジションの発火によってコピーされることもあるが，その際は，あくまで共通のオブジェクトネットへの参照がコピーされる点に注意されたい．

複数のオブジェクトネットで構成されるシステムは階層的に表現されるが，その場合，あるオブジェクトネットもまた，より下位のサブペトリネットから見れば相対的にシステムネットに相当する．混乱

のない限り，最上位ネットに限らず，隣り合う階層のネット間の関係を，システムネットとオブジェクトネットと称することとする．

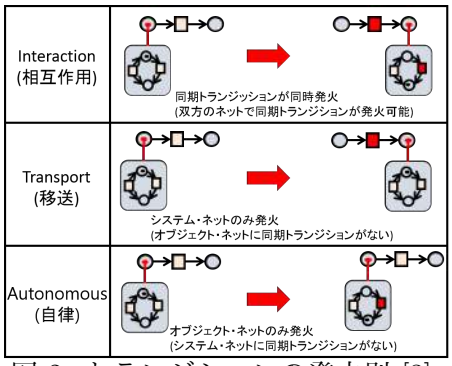


図 2: トランジションの発火則 [3]

システムネットとオブジェクトネットの間では，一部のトランジションの発火が同期的に行われる．オブジェクト指向ペトリネットの発火則「Interaction(相互作用)」により，同期発火が行われるには，全ての同期トランジションが発火可能な状態である必要がある．こうした発火のメカニズムから，nets-within-net 意味論，およびその拡張に基づくオブジェクト指向ペトリネットにおいては，(a)interaction(相互作用)，(b)transport(移送)，(c)autonomous(自律)，という 3 通りの発火則が考えられる (図 2)．

4. 文脈指向ロールベースアクセス制御モデル

文脈を意識したアクセス制御モデル (CxAC) には，そのベースとなるアクセス制御モデルと，具体的にどのような状況を取り扱うかで，2 つの観点からサブクラスが考えられる．ここでは，ベースとなるアクセス制御モデルに RBAC(Role-Based Access Control) を採用し，データに対する操作を従来の「電子文書情報の読み書き」をベースとしたものから,「情報の加工」や「機器操作の権限制御」にまで拡張した制御モデルである，文脈指向ロールベースアクセス制御モデルを提案する．

4.1.Role-Based Access Control: RBAC

一般に，権限制御を含むアクセス制御は，主体–操作–対象の 3 つの組のうち，許可されている組の集合で表現できる．中でもロールベースアクセス制御モデルは，情報にアクセスする主体ごとにアクセス権限を定義するのではなく，ロールすなわち役割に基づいて主体を分類し，ロールごとにアクセス権限を定義するものであり，現在，広く使われている．ロールごとに分類することで大幅にアクセス権限の定義数を減らすことができ，またロールへ継承階層を導入することで管理の容易性を一層進めることができる [4]．これに基づき，例えば認知症高齢者介護施設の場合であれば，介護職員の一人一人にアクセスと操作の権限を定義するのではなく，介護福祉士，監視員，パート職員，医療関係者といった役割ごとに，アクセス権限を定義することになる (図 3)．このような継承階層に構造化することで，より体系化し記述量を減らすことができ，ポリシーの保守性を向上させることができる．

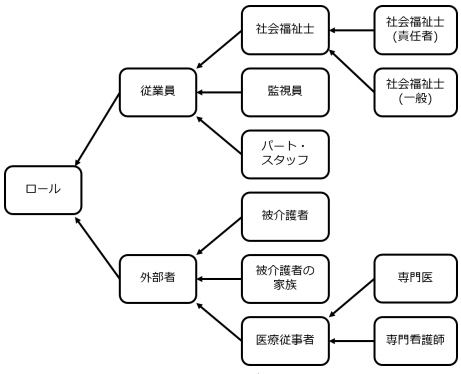


図 3: ロールの継承階層例

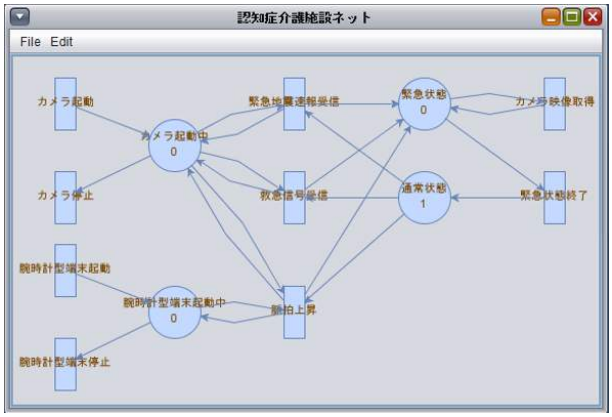
また，ロールは主体表現の一形態であるが，本研究では資源表現と操作表現も重要である．電子文書情報の読み書きをベースとしたアクセス制御だけでなく，情報加工や機器操作の権限制御にまで拡張する必要があるからである．そこで本研究では，資源もロールと同様に，加工度合いごとの継承階層で構造化させることにしている．しかし，資源の場合，全ての加工が全順序で表せられるとは限らない．例えば，電子カルテに記載されている氏名，年齢，住所に関する情報をそれぞれ，イニシャル，年代，都道府県などのように加工できるとする．その際，年齢を加工しない場合と住所を加工しない場合では加工度合いに優劣を付けることができない．つまり，ロールとは異なり単純な継承階層ではなく，半順序集合であることを考慮に入れる必要がある．一方，操作表現に関しては，多様な操作の体系化や，それを組み合わせた複合操作の定義が重要となる．

4.2.Context-Aware Access Control (CxAC) の適用事例

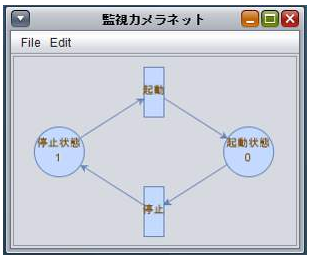
CxAC では，アクセス者と情報資源のそれぞれの振る舞い (ワークフロー) を文脈としてそれぞれオブジェクト指向ペトリネットによって表現し，協調動作を行う場合はトランジション間の同期によって表現する．つまり，強制すべきポリシーをオブジェクト指向ペトリネットに変換し，他のペトリネットとの同期関係を定義することによって，アクセス者にポリシーに従った振る舞いを強制する．

以下に 2 つの適用事例を示す．まず一つ目に認知症高齢者介護施設における監視カメラ映像の情報加

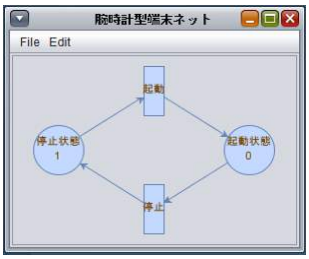
工による制御例を示す．日本の軽犯罪法第一条二十三項には「正当な理由がなくて人の住居、浴場、更衣場、便所その他人が通常衣服をつけないでいるような場所をひそかにのぞき見た者」は違法とあり，被介護者の安全確保や緊急時の救助支援という「正当な理由」がある場合は監視カメラを設置することが可能である．しかし，プライバシに関する苦情が生じる可能性もあり，寝室や浴室等の高度なプライバシ保護が必要な場所に監視カメラを設置することが現状難しい．そこで，浴室・寝室に設置された監視カメラの映像に対して，通常時は映像を加工 (在室，空室という情報のみを監視員に提示) し，緊急時のみ，加工されていない映像を監視員に提示することでプライバシ保護を図ることとする．ここでの緊急時とは，気象庁からの緊急地震速報を受信した時，被介護者からの救急信号を受信した時，または腕時計型ウェアラブル端末によって取得した被介護者の脈拍が危険値を超えた時，としている．この文脈をオブジェクト指向ペトリネットで図 4 に表現した．



(a) 認知症介護施設のシステムネット

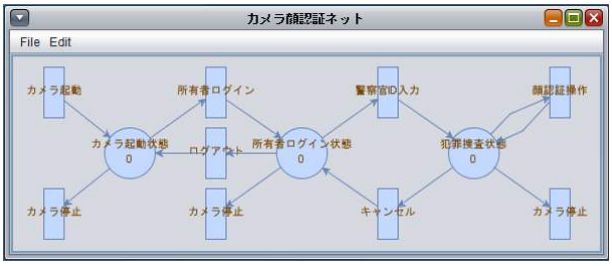


(b) 監視カメラのネット

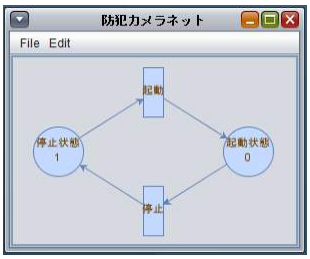


(c) 腕時計型端末のネット

図 4: 情報加工による制御例の文脈



(a) コンビニエンスストアのシステムネット



(b) 防犯カメラのネット

図 5: 機器操作に対する権限制御例の文脈

次にコンビニエンスストアに設置されている防犯カメラの顔認証操作の権限を状況に応じて動的に変更する例を取り上げる．近年の犯罪捜査においてコンピュータやセンサ機器に存在する情報を収集，解析するデジタル・フォレンジックスが一般化されてきている．一方で，操作対象となった人物のプライバシ保護の問題も生じており，デジタル・フォレンジックスとプライバシ保護の両立が求められている．そこで，この例題では，カメラの所有者と警察の了承を得た状態を犯罪捜査状態とし，この犯罪捜査状態にのみ顔認証という操作を可能にすることでプライバシ保護を図ることとする．この文脈をオブジェクト指向ペトリネットで図 5 に表現した．また，本報告で提案しているモデルが，実際の機器操作においても権限制御が可能かどうかを確認するため，Phidgets のアクチュエータを用いた実証実験も行っている．

5. アーキテクチャ

本報告で提案する CxAC のアーキテクチャとして，オブジェクト指向ペトリネットの状態遷移の表現方法，セキュリティポリシーの記述，ポリシー判定エンジンの構成，文脈推論のためのルールエンジンに関して説明する．

オブジェクト指向ペトリネットでは，2 階層以上を持つことによって，個別の組織のみならず，複数組織にまたがったワークフローや，その中を動くアクター (情報にアクセスする主体)，情報資源 (アク

セスされる対象) の個別の振る舞い (状態遷移) を表現することができる．本研究では，文脈をトランジションの発火系列で表現し，発火可能な発火系列の集合を文脈パターンとしている．トランジションの発火系列を正規表現で記述することで，正規表現によるパターンマッチングを行うことができ，複雑な状態遷移に基づく状況判断を可能にしている．

本研究では，セキュリティポリシーの記述として，基本的にはプログラミング言語 Scala による内部 DSL を利用し，自然言語表現からポリシー判定エンジンの入力に必要な XML 表現に変換させている．プログラミング言語 Scala は関数型言語であるため，より自然言語に近いセキュリティポリシー記述を可能にしている．更に，この内部 DSL では，形態素解析によって英語だけでなく日本語の自然言語表現にも対応させているため，プログラミングの知識がない現場の業務担当者であってもポリシーの編集や内容確認が容易になっている．

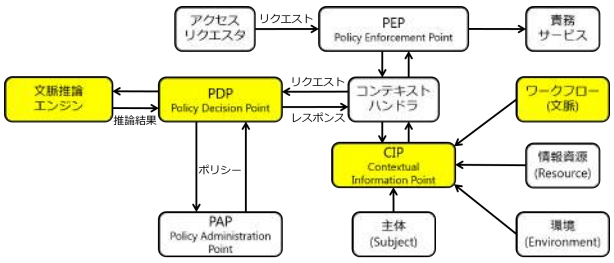


図 6: 提案モデルのアーキテクチャ

CxAC のポリシー判定エンジンの構成は，OASIS により標準化作業が進められている XACML(eXtensible Access Control Markup Language) [5] のアーキテクチャをベースとしている．Sun Microsystems の XACML2.0 実装 [6] を元に実装を行った．前述のセキュリティポリシーの表現も XACML に準じている．本報告におけるアクセス制御モデルのアーキテクチャを図 6 に示す．権限の判定を行う PDP(Policy Decision Point)，アクセス制御を実施する PEP(Policy Enforcement Point) および，ポリシーの管理を行う PAP(Policy Administration Point) をそれぞれ別のサーバーとして独立させ，柔軟性を持たせている．通信規格としてリアルタイムの双方向通信が可能な Web Socket を採用している．

文脈推論には，ルールエンジン Hammurabi [7] を用いている．CxAC では，ポリシー判定の過程でルールエンジンに文脈情報，つまり発火系列を推論させ，得られた文脈情報を基にパーミッションを与える構造になっている．Hammurabi はある問題に対して適用できる離散ルールの集合で成り立っており，断片的または不十分な条件入力であっても対応できる柔軟性がある．また，プログラミング言語 Scala で記述されているため，Java との親和性が高く，内部 DSL の記述にも適している．文脈推論のためのルールエンジンとして Hammurabi を採用することで，ポリシー判定エンジン全体の柔軟性と可読性を向上させている．

6. 関連研究との比較

RBAC との比較に加え，CxAC と同じく状況に応じたアクセス制御が可能な，オートマトンによるアクセス制御モデル (Security Automata Integrated XACML) との比較を行う．XACML を拡張したモデルである Security Automata Integrated XACML (以下 SA) [8] は，数学的に抽象化されたワークフローモデルで状態遷移を記述できるモデルで，非決定性有限オートマトンと似た構造を持つ．初期状態があり，イベントによって状態が遷移する．SA では，オートマトンが XACML の状況判断の不足を補っており，主体や資源の状態変化に応じて判定を下すセキュリティポリシーを持っているため，状態変化に応じたアクセス制御を可能にしている．

比較・評価では，アクセス制御モデルを実際のシステム上へ実装する際に問題となる点を評価基準とする．なお，以下の評価基準は [9] を参考にしている．CxAC，RBAC，SA との比較評価を行った結果を表 1 に示す．また，評価が異なる基準に対していくつか説明を加える．

CxAC と RBAC の比較

Fine-Grained Control

RBAC では，情報の「読み」／「書き」操作の制御を基本としている．一方 CxAC では，情報の加工度合いによるアクセス制御が可能であり，よりきめ細かなセキュリティポリシーを設定することができる．よって，RBAC を Low，CxAC を High としている．

Active / Passive

表 1: 既存アクセス制御モデルとの比較

Criteria	CxAC	RBAC	SA
Complexity	High	Low	High
Understandability	Simple	Simple	Simple
Ease of use	Medium	High	Medium
Applicability	High	Medium	Medium
Groups of Users	Yes	Yes	Yes
Policy Specifications	Yes	Yes	Yes
Policy Enforcement	Yes	Yes	Yes
Fine-Grained Control	High	Low	High
Active / Passive	Active	Passive	Active

RBAC ではパーミッションがポリシーに対して固定的に割り当てられており，ポリシーを編集しない限りパーミッションは変更されない．一方，CxAC では同じ主体，操作，資源を実行する場合であっても文脈によってポリシー強制が行われるため，パーミッションが動的に変更される．よって，RBAC を Passive，CxAC を Active としている．

CxAC と SA の比較

Applicability

SA は状態遷移により状況に応じて動的にアクセス権限を変更できる点で CxAC と類似しているが，Applicability（適用可能性）では評価が異なる．SA では，オートマトンによって各主体・資源の状態遷移は表現できるが，状態遷移を階層構造で構造化できないため，組織間を移動する主体・資源の状態遷移を表現することが難しい．一方，CxAC では，オブジェクト指向概念に基づいたオブジェクト指向ペトリネットを文脈表現として採用しているため，組織内の状態遷移だけでなく，複数組織にまたがった状態遷移の表現にも適している．よって，SA を Medium，CxAC を High としている．

7. まとめ

本研究の目的はアクセス制御モデルの共通的なフレームワークの構築である．本報告では，文脈に基づくアクセス制御モデル CxAC を用いることで，特定の情報への操作も単純な「読み」／「書き」だけでなく，情報の一部にモザイクを掛けて可視性を制限するような加工操作が可能であること，アクセス権限制御技術を機器操作に対する権限制御にまで拡張できることを示した．また，オブジェクト指向ペトリネットを文脈表現として採用することで，状況に応じた細粒度制御を実現し，適用可能性を高めている．一方，本報告で示した例題ではオブジェクト指向ペトリネットの特徴である階層構造化の有用性を十分に示すことができていない．従って今後は，多階層のワークフローに基づくアクセス制御を実現し，共通的なフレームワークとしての有用性の高さを示していく．

参考文献

[1] Tadashi Iijima, Satoshi Kido: “Design and Implementation of a Context-Based Security Model”, Proc. of 11th Joint Conference of Knowledge-based Software Engineering 2014, Sept.17-20, 2014. CCIS-Vol.486, pp.356-370, Springer.

[2] R. S. Sandhu, E. J. Coyne, et al.: “Role-based access control models”, IEEE Computer, vol.29, no.2, pp.38–47, 1996.

[3] Rüdiger Valk: “Object Petri Nets Using the Nets-within-Nets Paradigm”, LNCS 3098, pp.819–848, Springer, 2004.

[4] A.S.M. Kayes, J. Han, and A. Colman: “An Ontology-Based Approach to Context-Aware Access Control for Software Services”, WISE 2013, Part I, LNCS 8180, pp.410–420, 2013.

[5] OASIS Standard: “eXtensible Access Control Markup Language (XACML) 3.0”, 22 January 2013, `http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.pdf`

[6] Sun Microsystems, Inc. (当時): “Sun’s XACML Implementation”, 16 July 2004, `http://sunxacml.sourceforge.net/`

[7] M. Fusco: “Hammurabi - a Scala rule engine”, In Scala Days 2011, Stanford University, California, 2011.

[8] Juan Deng and Ricahrd Brooks, Joachim Taiber: “Security Automata Integrated XACML and Security Validation”, Proc IEEE SOUTHEASTCON 2010, pp338-343, March 2010.

[9] William Tolone, Gail-Joon Ahn, Tanusree Pai, Seng-Phil Hong: “Access Control in Collaborative System”, ACM Computing Surveys, vol.37 Issue 1 pp29-41, March 2005.