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

2005－DPS－122（24）
2005－CSEC－28（24）
2005／3／22

コンテキストアウェアな認可機構における効率的なポリシ構成方式の提案

柴田 賢介† 大嶋 嘉人† 荒金 陽助† 金井 敦†

† 日本電信電話株式会社 NTT 情報流通プラットフォーム研究所

あらまし 近年，価値ある電子的な情報を保護するための技術として，アクセス制御の重要性が高まっており，情報の提供可否の判断を行なう認可はその核となる技術である．著者らは，認可の際に利用者のおかれている状況 (コンテキスト) を考慮することが重要であると考え，これに基づいて情報資源の利用をダイナミックに制御可能な認可機構の開発を行なっている．本稿では，コンテキストアウェアな認可機構における効率的な認可ポリシ構成方式を提案する．本方式は，コンテキストの変化に応じて継続的に行なわれる認可のためのポリシ（継続認可ポリシ）を自動生成することにより，ポリシ記述コストを軽減すると共に，継続認可ポリシを構成する条件数を必要最小限に抑えることにより，システム負荷を軽減することを特徴としている．

キーワード 認可，アクセス制御，コンテキストアウェアネス，認可ポリシ，情報利用制御

A Method of Effective Policy Construction for Context-Aware Authorization

Kensuke Shibata† Yoshihito Oshima† Yosuke Aragane† Atsushi Kanai†

† NTT Information Sharing Platform Laboratories, NTT Corporation

Abstract In recent years access control system becomes more important to protect the valuable information. Authorization is the core component of access control. Along with the multiplicity of environment for the information usage, the context would become the important factor for authorization. So we develop context-aware authorization platform which enables dynamic access control. In this paper, we propose a method of policy construction for context-aware authorization platform. Context-aware authorization needs continuity during information usage because of the variability of context. Since our platform generates the policy for continuous authorization automatically, this method saves the policy description cost. Our method also reduces the load of authorization system because it cuts down the number of conditions in the policy for continuous authorization.

Keywords Authorization, Access Control, Context Awareness, Authorization Policy, Information Usage Control

1 はじめに

1.1 コンテキストアウェアネスと認可

価値ある情報を保護するため，当該情報へのアクセスや利用を制御するためのアクセス制御技術の重要性が高まっている．特に企業においては機密情報，顧客情報といった重要な情報を管理しており，これらの情報は適切な利用者に対してのみアクセスが許可されるべきである．このアクセス制御技術の中核を成しているのが，情報の提供可否を判断する認可であり，アクセス制御を行なうシステム上では，認可の結果に基づいて，情報の利用を制御している．現在は，XACML[1] に見られるように，人やリソースの特徴を示す属性に基づいて情報の利用可否を判断する認可が主流となっている．

一方，HCI(Human Computer Interaction) の分野においては，コンテキストアウェアアプリケーションに関する研究開発が進められている．コンテキストアウェアアプリケーションとはセンサから取得した情報 (利用者の現在位置や天気など) や，現存する情報 (利用者の予定表や時刻など) を基に，利用者に応じて，最適なサービスを提供するものであり，例えば，位置情報を基にした観光案内や，屋内での電話の転送サービスが実現されている [2]，[3]．

1.2 コンテキストアウェアな認可

現在，モバイル，ワイヤレス技術の発達により，情報の利用環境が多様化しており，さまざまな状況で情報が利用されている．よって認可を行なう際には，情報の利用を要求している利用者に対して当該

情報を提供するのに適切な属性 (資格，所属など) を有するか否かを判断するだけではなく，利用者のおかれている状況が情報の提供に適切であるか否かを考慮した認可が必要と考えられる．

我々は特に情報を保護するという観点から，情報提供時に利用者のおかれている状況を決定する要因として,「利用者に提供されている情報資源を入手したり，これに影響を与えうるような，利用者の周囲にいる人や機器から形成される状況」が重要であると捉えている．このようなコンテキストを特に近隣コンテキストと呼ぶ．近隣コンテキストとして，以下の例が挙げられる．

1. PC で作業をしている利用者の周りに，ディスプレイに表示された機密情報を見ることができる人が存在する状況
2. 顧客情報が格納されているサーバにアクセス可能なクライアント PC に USB メモリが有効な状態で接続されている状況

我々は，近隣コンテキストを判断の材料として，情報資源の利用をダイナミックに制御可能な認可機構の研究を行なっている．上記 (1) の例では，PC で作業をしている利用者の周りに，他社の社員がいる状況では，利用者に対する機密情報の提供を行なわないといったアクセス制御が想定され，(2) の例においては，クライアント PC に USB メモリが有効な状態で接続されている状況では，外部への持ち出しを禁止されている顧客情報へのアクセスを禁止するといった制御が考えられる．

本稿ではまず，コンテキストアウェアな認可を実現する上で考慮しなければならない 3 つの要件について述べ，そのうち認可ポリシに関する課題について特に注目し，この課題を解決するための手法を提案する．

2 コンテキストアウェアな認可の要件

我々は近隣コンテキストの利用が特に有用であると考えられるアプリケーションを想定し，これらのアプリケーションに対して従来の認可を適用した場合の困難性や，限界について検討した．その結果，コンテキストアウェアな認可を実現するための主な要件として，以下の 3 点を得ることができた．

(1) コンテキストの変動性に対応できること

(2) コンテキストを確実に取得できること

(3) 認可ポリシを容易に記述できること

以下，各項目について説明する．

(1) 従来の認可で対象としていた利用者やリソースの属性は，例えば社員の役職のように，時間の経過によって頻繁にその値が変化するものではなく，静的な情報である．これに対し近隣コンテキストは，1.2 節に例として示した,「周りにいる人」や,「PC に接続されたデバイス」のように，時間の経過によってその値が変化する (変動性をもつ) 動的な情報である．よって，コンテキストアウェアな認可の実現のためには，コンテキストの変動性に対応できる必要がある．

(2) 従来のアクセス制御においては，利用者が提示する属性証明書などを判断材料として，情報の利用制御が行なわれてきた．これに対し，コンテキストに関する情報は，一般的にセンサ等の機器を通して実行時に取得される．従来の認可は,「ある属性を持った人に対して，情報の利用を許可する」というものであるのに対し，コンテキストアウェアネスの概念を認可に導入することにより,「ある状況下にある場合に，情報の利用を停止する，もしくは利用を不許可とする」といった制御が必要となる．つまり,「部外者である」,「資格をもっていない」といった負の意味を持つ属性について，センサを通して確実に取得できることが必要である．

(3) 認可を行なう際には，判断の基準となる認可ポリシが必要である．コンテキストアウェアな認可を行なう場合，認可ポリシの要素としては，従来の認可においても利用されていた，適切な属性を保持しているか否かを判断するための条件に加えて，コンテキストが適切であるか否かを判断するための条件が必要となる．ポリシ記述者が記述しなければならない条件の数が増えることにより，ポリシ記述者の負担はさらに増えることになる．また，コンテキストに対する条件として，その取得に関わるセンサの特定や，センサからの値の取得といった部分も含めてポリシ評価のパラメータとして記述する方法では，ポリシは非常に複雑なものとなってしまう．そこで，ポリシの記述量，複雑さという 2 つの観点から，ポリシ記述者の負担を可能な限り増加させないポリシ記述方式が必要となる．

3　コンテキストアウェアな認可における課題

本稿では，2 章において述べた 3 つの要件のうち，(1) と (3) について注目し，コンテキストの変動性に対応した認可ポリシの構成方式についての検討結果について報告する．本章では，これを実現するための課題について述べる．

3.1　継続認可ポリシ

2 章の (1) において述べたとおり，コンテキストには変動性がある．従来は，静的な属性情報を基に判断を行なっていたため，認可は情報の提供を開始する時にのみ実行されれば十分であった．しかし，コンテキストアウェアな認可を行なう場合，情報の提供開始時には適切な状況であると判断されても，コンテキストの変動性によって提供中に不適切な状況になる可能性があり，認可は情報の提供が終了するまで継続的に実行されなければならない．本稿では，以後，情報を提供開始する際に行なわれる認可を初回認可，情報の提供中に行なわれる認可を継続認可と呼ぶこととする．

また，2 章 (3) の説明部分で述べたとおり，認可を行なうためにはポリシを記述する必要がある．つまり，継続認可を行なう場合には，初回認可と継続認可のポリシがそれぞれ必要となる．ここで，継続認可を行なうためのポリシを継続認可ポリシ，これに対して初回認可を行なうためのポリシを初回認可ポリシと呼ぶこととする．また，認可ポリシにおいて適切な属性を保持しているか否かを判断するための条件を属性条件，コンテキストが適切であるか否かを判断するための条件をコンテキスト条件と呼ぶこととする．

3.2　認可ポリシの記述に関する課題

文献 [4] において指摘されているように，ポリシとして定義する内容が増加すると，その記述コスト，管理コストが高くなるという問題がある．コンテキストアウェアな認可を行なうためには，従来の認可ポリシに加えて，コンテキスト条件を記述し，さらに，継続認可ポリシを定義する必要がある．そこで，我々は認可ポリシの記述量に関して以下の 2 点の課題に注目した．

1. コンテキスト条件や，継続認可ポリシをポリシ記述者が記述する場合，認可ポリシの記述量が増加し，ポリシ記述者の負担が増えることになる．
2. ポリシ記述者の記述量を減らすために，初回認可ポリシを継続認可ポリシとして流用する場合，初回認可と同等の認可処理が継続的に実行されることになり，システムに対する負荷が高くなってしまう．

本稿では，上記 2 点のポリシ記述に関する課題を解決するポリシ構成方式を提案し，認可システムのプロトタイピング，ポリシ構成方式の定性的な評価を行なうことにより，今後本方式を実現する場合の効果の見込みについて考察した．

4　コンテキストアウェアな認可を実現するポリシ構成方式

4.1　継続認可ポリシの自動生成

3.2 節において述べた課題を解決するために，本研究では継続認可ポリシを初回認可ポリシから自動生成するというアプローチをとる．初回認可ポリシの属性条件は，静的なパラメータに対する条件であり，情報の提供中には値が変化しないため，継続認可においては判断材料とする必要がない点に着目し，初回認可ポリシの中で情報提供中も動的に値が変わりうるコンテキスト条件のみを抽出する．これにより継続認可ポリシに含まれる条件の数を減少させることが可能となる．

ここで，認可ポリシは 1 つ以上の条件から成り，2 つ以上の場合には各条件は AND，もしくは OR で連結されて条件節を成す．条件とは，パラメータと演算子，そして基準となる値から構成される (例：利用者の所属＝総務課)．条件節は階層的な構造を持つこともある．

4.2　継続認可ポリシの抽出ロジック

図 1 に初回認可ポリシから継続認可ポリシを抽出するための処理手順を示す．本節では，この処理手順について概説する．

(a) まず，初回認可ポリシの属性条件の中で，真とならなかった条件を削除する．初回認可において真

とならなかった属性条件は，継続認可においても偽となるため，判断材料とする必要がない．

(b) 次に，(a) において削除された条件と AND で連結されている条件を削除する．(a) で削除された条件が必ず偽であるため，AND で連結された条件は継続認可において判断材料とする必要がない．

(c) 階層構造を持つ認可ポリシの部分木の中で最も深さが深いものに処理対象を移動し，以下の処理を再帰的に繰り返す．

(h)，(i)，(j)，(k) 処理対象の部分木について 2 種類の判定が行なわれる．対象となる部分木に属性条件が存在し，部分木が OR 連結である場合，その部分木は継続認可においても常に真となるため，部分木の値として真を抽出する．部分木に属性条件が存在しない場合，もしくは部分木が AND 連結である場合には，継続認可においてはコンテキスト条件のみを判断材料とすれば良いため，属性条件を削除する．

上記の処理を認可ポリシの階層の根に到達するまで繰り返し，最終的に残ったポリシを継続認可ポリシとして抽出する．

以上のロジックによって，初回認可ポリシに含まれる条件の中で，継続認可において判断結果が自明であるもの，不要となるものを削除し，継続認可の判断材料とすべきコンテキスト条件のみを抽出することが可能となる．上記ロジックにより，継続認可ポリシは初回認可ポリシに比べて条件の数が少なくなり，継続認可に伴うシステムへの負荷を軽減することが可能である．また，上記ロジックは機械的に処理することが可能であり，これを処理する機構を準備することにより，継続認可ポリシを自動生成することが可能となる．よって，ポリシ記述者への負担を軽減することが可能となる．

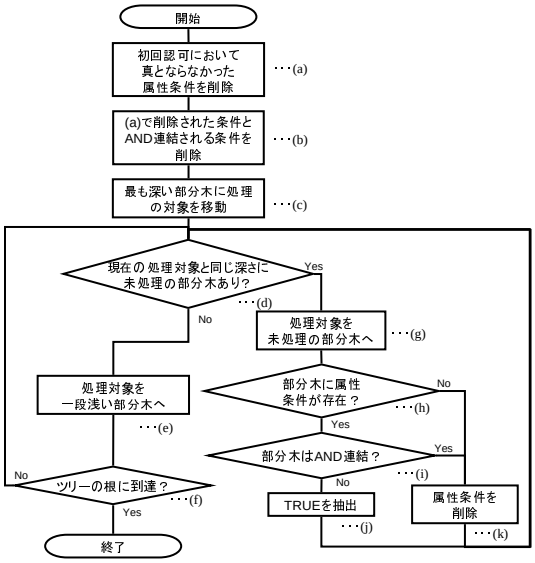

図 1: 継続認可ポリシ抽出処理のフロー

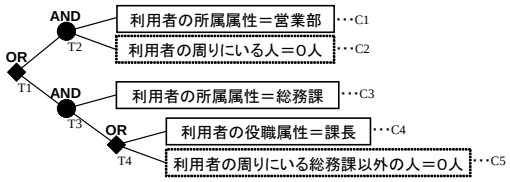

図 2: 初回認可ポリシの例

4.3 継続認可ポリシ抽出の例

図 2 は 4.1 節で述べた，本稿で対象とする認可ポリシの構成例である．ツリーは AND もしくは OR で連結される部分木（T1〜T4）から構成されており，四角で囲まれた部分（C1〜C5）が認可ポリシを構成する条件群となる．条件のうち，実線で囲まれたものは属性条件であり，点線で囲まれたものはコンテキスト条件である．

本節では，図 2 を初回認可ポリシの例として，認可ポリシ抽出の手順を示す．本例においては利用者の所属が総務課であり，役職は一般社員であると想定する．

(a) まず，初回認可の結果に応じて属性条件を削除する．利用者の所属は営業部ではなく，役職は課長ではないため，C1，C4 が削除される．

(b)C1 と AND 連結されている C2 は，継続認可中に C1 が常に偽となるため削除される．

(c) まず最初に T4 に処理対象が移る．

(h)，(i)，(j)，(k)T4 に含まれる条件はすでに C5 のみであるため，C5 が抽出される．

上記の処理を T4 → T2 → T3 → T1 と繰り返す．T2 の条件はすでに削除されて残っていない．T3 は，C3 と C5 が AND 連結された部分木となっているため，(h)〜(k) の処理によって C5 が抽出される．処理対象が T1 に到達したところで，終了条件を満たし，認可ポリシ抽出の処理は終了する．例では最終的に C5 のみが継続認可ポリシとして抽出されることになる．

5 評価

5.1 プロトタイプシステム

提案しているコンテキストアウェアな認可の実現可能性を検証するため，プロトタイプシステムを開発し，実現可能性について検証した．現時点では，継続認可ポリシの自動生成機構については未実装であるが，初回認可，継続認可の実行と近隣コンテキストによる利用制御が可能となっている．

本システムは，企業における機密情報の漏洩を防止するために，RFID を利用したコンテキストの検知を行ない，これに基づいて情報の利用制御を行なう．図 3 は本システムの概観を，図 4 はシステムのモジュール構成を示したものである．システムはノート PC と RFID リーダ，RFID タグで構成され，ノート PC は利用者用の端末と認可装置を兼ねている．利用者の周囲にいる人の存在と，その所属を検知するため，企業の建物内に入館する人は全員 RFID タグを保持していることを前提としており，タグに格納されている ID 情報をキーとして属性 DB を検索し，属性情報を取得する．

図 4 を参照してシステム内の動作について説明する．まず，利用者はノート PC に格納されている機密文書ファイルを開く．文書の利用要求は利用制御モジュールから認可制御モジュールへと伝えられ，該当する機密文書ファイルに対応する認可ポリシを検索し，認可のために必要な属性とコンテキストの値をそれぞれ属性 DB，センサ管理モジュールから取得する．認可制御モジュールは収集した情報と認可ポリシを XACML[1] 認可エンジンに渡し，利用可否の判断を行なう．利用を許可すると判断された場合には，利用制御モジュールは利用要求されているファイルをアプリケーションに渡し，利用者は情報を利用することが可能となる．不許可と判断された場合には，利用制御モジュールがディスプレイ上に認可結果ダイアログを表示する．以上が初回認可時の動作である．

継続認可については，RFID リーダにおいて取得しているタグの ID 情報に変動があった場合に発生する．変動はセンサ管理モジュールから認可制御モジュールへ通知され，初回認可と同様に認可処理が行なわれる．利用不許可と判断された場合には，利用停止モジュールを介して情報の利用を一時停止する (現在の実装では該当するアプリケーションのウィンドウを最小化する)．利用停止状態にある情報が，利用許可と判断された場合には，利用停止モジュールは情報の利用停止を解除し，情報の利用を再開する．

図 3: プロトタイプシステムの概観

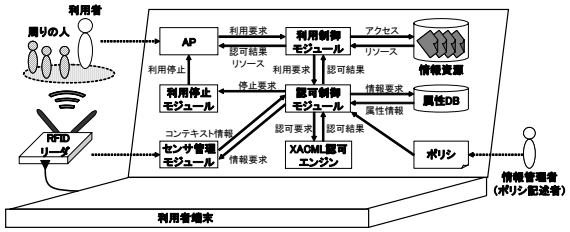

図 4: プロトタイプシステムのモジュール構成

本システムの実装により，初回認可，継続認可の動作を確認することができ，コンテキストアウェアな認可を行なうアプリケーションの実現可能性が示された．

5.2 認可ポリシ自動生成方式の効果

本節では，認可ポリシ自動生成方式の定性的な評価の結果について述べる．コンテキストアウェアな認可を行なうことによる効果があると考えられる 5 種類のアプリケーションを想定し，各アプリケーションについて初回認可ポリシを試行的に記述した．想定したアプリケーションとは，例えば 5.1 節のプロトタイプシステムにおいて題材となっている，企業における機密情報の漏洩対策アプリケーション等である．これらの初回認可ポリシについて 4.2 節で述べた継続認可ポリシの抽出ロジックを適用し，机上で継続認可ポリシを生成した．表 1 は，初回認可ポリシに含まれる条件の数と，抽出ロジックを適用して生成された継続認可ポリシに含まれる条件の数

を示している (数値は 5 種類のアプリケーションの平均値である).

表 1 より明らかなように，比較的規模が小さい初回認可ポリシについては，抽出ロジックによる条件数の削減率は 4 割程度となっているが，初回認可ポリシの規模が大きくなると，図 1 の (a)，(b) において削除される条件の数が多くなり，削減率は 9 割程度となる．よって，本方式は複雑な構造を持つポリシになるほど高い効果が得られることが分かる．

表 1: ポリシ自動生成方式の評価結果

ポリシの規模	初回認可ポリシの条件数	継続認可ポリシの条件数	削減率
小規模	5	2.8	44%
中規模	20	6.4	68%
大規模	100	10.8	89.2%

6 まとめ

6.1 関連研究

本節ではコンテキストを利用した認可と，認可ポリシの簡略化に関する検討について，本研究と類似した研究について述べる．

文献 [5] は，利用者の位置関係をコンテキストとし，サービスを提供するエリアの種別，利用者の役職等の情報，過去のアクセス履歴を基に利用者の信頼度を算出し，サービスの提供可否を決定するアクセス制御機構を提案している．コンテキストを利用したアクセス制御を行なうという点で本研究と類似しているが，本文献ではある時点におけるアクセス制御により，サービスの提供可否を判断するのみであるのに対し，我々は継続的にサービスを提供する場合の認可について検討しているという点で異なる．

文献 [4] では，ネットワークシステムの管理ポリシの記述量が膨大になるという課題を解決することを目的とし，リソースを管理するためのポリシの上位概念として情報の管理者にとって設定しやすい「マスターポリシ」を定義する．このマスターポリシと運用ノウハウなどの情報を用いて個別のポリシを自動生成することにより，ポリシの記述コスト，管理コストを削減している．また，文献 [6] においては，XML 文書をターゲットとし，文書の変換などを行なった場合に，変換後の文書のアクセス制御ポリシーを設定する上で，可能な限り簡略化されたポリシを求める最適化について述べられている．これらの研究はポリシの簡略化を行なうアプローチをとっているという点において類似点が見られるが，本研究では継続的に行なわれる認可に利用するポリシについて検討しているという点で異なる．

6.2 まとめと今後の課題

本研究では，電子的な情報の利用を制御する際に，属性情報だけでなく，利用者を取り巻くコンテキストが情報の提供に適切であるか否かを考慮することが重要であると考え，コンテキストアウェアな認可方式について検討している．本稿では，コンテキストアウェアな認可を行なうプロトタイプシステムの実装により，本方式の実現可能性を示すと共に，コンテキストの変動性から，情報を提供している間の継続的な認可の必要性を指摘し，この継続的な認可に必要となる認可ポリシを自動的に生成する手法を提案した．本手法では，継続的な認可に必須の条件のみで構成されるポリシを生成することにより，システムへの負荷を軽減することを特徴としており，机上の評価において，その有効性を確認した．

5.1 節において述べたプロトタイプシステムでは RFID を利用して利用者の ID 取得，部外者の検出を行なっている．しかし，タグから発信される電波が受信できなかった場合や，悪意を持った人がタグからの電波の発信を妨害した場合に，正確なコンテキストの情報を取得することができない．つまり，2 章の (2) で述べた負の属性を確実に獲得することができていない．今後は，(2) の要件を満たすコンテキストアウェアな認可について検討を進めていく予定である．

参考文献

[1] eXtensible Access Control Markup Language (XACML): http://www.oasis-open.org/.

[2] 上岡英史: コンテクストアウェアネスを用いたアプリケーションの研究動向, 情報処理学会誌, Vol. 44, No. 3, pp. 265–269 (2003).

[3] Dey, A. K., Abowd, G. D. and Salber, D.: A Conceptual Framework and a Toolkit for Supporting the Rapid Prototyping of Context-Aware Applications, *HUMAN-COMPUTER INTERACTION*, Vol. 16, pp. 97–166 (2001).

[4] 菅野政孝, 田中俊介, 坂田祐司, 小熊慶一郎, 白鳥則郎: 情報ネットワークシステムのポリシー制御“ PolicyComputing ”の適用と実装, 情報処理学会論文誌, Vol. 42, No. 02, pp. 126–137 (2001).

[5] 西木健哉, 坂田匡通, 田中英里香: 位置関係に基づく動体認証及びアクセス制御機構, Vol. 2004, No. 66, pp. 79–85 (2004).

[6] 王波, チャットウィチェンチャイソムチャイ, 岩井原瑞穂: XML 文書のアクセス制御ポリシーの簡略化について, 電子情報通信学会技術研究報告, Vol. 104, No. 176, pp. 103–108 (2004).