2B-1

随伴者の有無に基づく動的アクセス権設定

森田 陽一郎†，中江 政行†，小川 隆一†
日本電気 (株) インターネットシステム研究所†

1. はじめに

近年，部門内に限らず，複数の部門にまたがったプロジェクトや，拠点間での遠隔会議などの場面で，アドホックにファイルサーバなどを共有して，ユーザ同士で情報共有を行いたいというニーズが高まっている．

その実現手法として，我々は，頻繁に生滅やメンバ変動を繰り返すユーザグループ (アドホックグループ) に対応できるアクセス権ポリシ (CBAC ポリシ) を定義し，このポリシに指定されたタイミングで FW (ファイアウォール) などのアクセス制御機器のルール (ACL) を設定・変更する動的 ACL 設定方式 [2] を提案した．

しかし，本方式を用いたアクセス制御システムでは，制御対象となるユーザ本人の属性 (コンテキスト) しか条件として参照しないため，誰と誰が出会ったか，どのようなユーザの組み合わせで集まったかなどの条件に基づく，より動的な制御を行うことはできなかった．

そこで，本方式を拡張し，アクセス制御対象ユーザを含めた複数のユーザのコンテキストを条件として CBAC ポリシに記述することで，ユーザ間の関係や，ユーザ集合の状態をトリガとした，より動的なアクセス制御を可能とする手法を提案する．

本稿では，アドホックグループのアクセス権記述モデルである CBAC モデル，および本モデルに基づく動的 ACL 設定方式を応用したアクセス制御方式である随伴者制御方式のポリシ記述と動作について述べる．

2. コンテキストによるアクセス権設定

2.1.CBAC モデル

CBAC は，ユーザの所属・位置などのアドホックグループを特徴づけるユーザ属性 (コンテキスト) を条件として用いてユーザ集合を定義するよう，RBAC [1] を拡張したポリシモデルである (図 1).

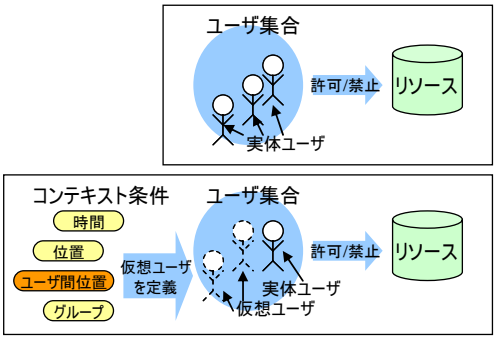

図 1: CBAC と RBAC の比較

Dynamic Security Provisioning Based on the Existence of Attendants
† Yoichiro MORITA, Masayuki NAKAE, Ryuichi OGAWA, Internet Systems Research Labs., NEC Corp.

CBAC ポリシの基本構造

```
<CBAC effect="E">
  <context>
    <group>G</group>
    <location>L</location>
    <time>T</time>
  </context>
  <resource>R</resource>
</CBAC>
```

従来方式における L の基本構造

```
<location>
  <place>P</place>
</location>
```

拡張方式における L の基本構造

```
<location>
  <place>P</place>
  <attendant>A</attendant>
</location>
```

図 2: CBAC ポリシの基本構造と拡張

CBAC ポリシは，コンテキスト条件で定義されたユーザ集合が，リソースにアクセス可能かどうかを，記述することになる．ユーザ集合が変化する場合，RBAC では，ユーザ集合を再定義するため管理者によるポリシ変更が必要となるが，CBAC では，ポリシ変更をしなくても，仮想ユーザごとのコンテキスト情報を外部から受け取り，コンテキスト条件に合致する実体ユーザを逐次更新する．

2.2.CBAC ポリシ

CBAC ポリシの基本構造は，コンテキスト条件 (G，L，T) と，リソース (R) と，アクセス可否 (E) からなる (図 2). コンテキスト条件は，グループ (G)，位置 (L)，時間 (T) からなり，これらの条件によって，R へのアクセスについて，E で指定された制御を行う対象となるユーザ集合を定義している．拡張前の CBAC ポリシでは，L に指定する内容として，「会議室」などの静的な場所 (P) のみを用いていた．今回，L の指定として，P 以外に，随伴者 (A) (以下，随伴条件) を利用できるよう拡張した．

拡張前の CBAC ポリシでは，例えば，会議室にいるユーザからのアクセスを許可し，会議室にいないユーザからのアクセスを拒否するような制御は可能であったが，会議室にいるユーザのうち，ユーザ A がいる間は，同じく会議室にいるユーザ B，C からのアクセスを許可し，ユーザ A がいなくなると，ユーザ B，C からのアクセスを拒否するような制御は不可能であった．

拡張後の CBAC ポリシでは，他のユーザのコンテキストをコンテキスト条件に用いることができる．すなわち，従来方式では，ユーザ A，B，C がいる場合，ユーザ A のアクセス制御の条件としてユーザ A のコンテキスト，ユーザ B のアクセス制御の条件としてユーザ B のコンテキストのように CBAC ポリシを記述していたが，拡張方式では，ユーザ A のアクセス制御の条件として，ユーザ A，B，C のコンテキストを CBAC ポリシに記述して，そのコンテキスト間の関係に基づいてアクセス制御を行うことができる．

2.3.ポリシエンジン

ポリシエンジンは，コンテキスト情報源を用いて，アクセス制御情報 (ACL) を生成・設定する． 拡張後の CBAC ポリシを解釈する際には，ユーザの位置情報の変化をコンテキスト情報源から取得し，関係する CBAC ポリシを特定する． その後，その CBAC ポリシに指定されたグループに含まれるユーザと，随伴者に含まれるユーザの位置関係に基づいて，ACL を生成・設定する．

3. 随伴者制御システム

拡張した CBAC ポリシを用いた動的 ACL 設定方式の応用例として，ユーザが誰と一緒にいるか (随伴者の有無) によって，動的にアクセス権設定を行う随伴者制御方式について説明する．

利用シーンとして，商談もその場で行う展示場を想定する． 展示用端末で資料を見せる際，顧客によってはすぐに重要な資料を見せて販促につなげたいが，情報漏洩を防ぐためには一般の顧客には一般向け資料以外は見せないようにしたいと考えられる． そこで，営業担当のみの場合や営業担当と重要顧客が一緒にいる場合は重要資料と一般資料の両方へのアクセスを許可し，顧客のみで営業担当がいない場合や営業担当がいても一般顧客も一緒にいる場合は，重要資料へのアクセスを拒否して一般資料へのアクセスのみを許可するようなアクセス制御が必要である．

このようなアクセス制御を行うために，展示端末の場所にいるユーザの組み合わせについて，コンテキスト条件として随伴条件を用いて表現する (図 3)． ここでは，展示用端末付近のユーザ集合 (以下，展示端末のユーザ) を U，展示場の営業担当を A，重要な顧客を B，一般の顧客を C，一般資料を R1，重要資料を R2 と置く． このアクセス制御を行う CBAC ポリシは，それぞれ以下のように表現できる． CBAC ポリシ p1 は，一般顧客 C が一緒にいると，展示端末のユーザ U から，重要資料 R2 へのアクセスを拒否する (図 4)． p2 は，営業担当 A，重要顧客 B，一般顧客 C のうち誰かが一緒にいると，展示端末のユーザ U から，一般資料 R1 へのアクセスを許可する． p3 は，営業担当 A が一緒にいれば，展示端末のユーザ U から，重要情報 R2 へのアクセスを許可する． どのポリシの随伴条件にも合致しない場合 (default) は，あらゆる資料へのアクセスを拒否する．

ポリシエンジンは，ポリシ解釈の際，随伴条件の判定のため，ユーザの位置を比較する． 今回試作したシステムでは，アクティブ型 RFID タグと RFID リーダ (センサ) による位置情報を用いて，比較している． RFID センサをコンテキスト情報源の 1 つとし，位置情報に変化があれば，位置に関するコンテキスト情報が更新され，ポリシエンジンに通知される．

```
<CBAC effect="deny">
  <context>
    <group>展示端末のユーザU</group>
    <location>
      <place>展示スペースP</place>
      <attendant>一般顧客C</attendant>
    </location>
    <time>展示期間T</time>
  </context>
  <resource>重要資料R2</resource>
</CBAC>
```

図 4: CBAC ポリシ p1 の概要

ポリシエンジンは，上記 3 つ (p1〜p3) の CBAC ポリシに記述された，アクセス対象のユーザの位置と，随伴者のユーザの位置との，一致の有無を発火条件として，CBAC ポリシを解釈する． 本システムでは，ユーザ A，B，C の位置を比較することで，展示端末のユーザにどのユーザが含まれているかを判断し，適切なアクセス制御を実現する．より具体的には，位置に変化があったユーザに関係するポリシを解釈し，その発火条件が満たされた場合，そのポリシに基づく ACL を生成し，ポリシの順に設定する (図 3)．図 3 の例では，p1 から順に条件の評価が行われるため，例えば，時刻 t2 から t3 へ状態が変化した場合，営業担当 A が一緒にいることによってアクセス許可されていた重要情報 R2 (図 3 ①) について，一般顧客 C が加わることによって，重要情報 R2 へのアクセス拒否 (図 3 ②) が設定され，ACL としては，② が先に評価されるため，R2 へのアクセスは拒否される．

これにより，展示端末付近のユーザの組み合わせが時刻経過とともに頻繁に変化しても，これに追随した動的なアクセス制御が実現できる．

4. おわりに

アドホックグループのアクセス権を表現できる CBAC モデルに，ユーザ間の位置関係を記述できるよう拡張を行った． また，この拡張を利用した，随伴者制御システムについて述べた．

参考文献

[1] R. Sandhu et al., “Role-Based Access Control Models”, IEEE Computer, v. 29, n. 2, 1996, pp. 38-47.

[2] 森田 他, “安全なアドホック情報共有のための動的 ACL 設定方式”, FIT 2004, pp. 233-234

CBAC ポリシ pn					t1		t2		t3		t4		t5		時刻 tn
	随伴条件	アクセス権			A∧C		A∧B		A∧B∧C		B		−		ユーザの組み合わせ
		アクセス元	アクセス先	可否	R1	R2	R1	R2	R1	R2	R1	R2	R1	R2	アクセス先リソース
p1	C	U	R2	×		×				× ②					ポリシ解釈によって生成・設定される ACL (上から順に評価・適用)
p2	A∨B∨C	U	R1	○	○		○		○		○				
p3	A	U	R2	○		○		○①		○					
default	*	*	*	×	×	×	×	×	×	×	×	×	×	×	

図 3: CBAC ポリシとポリシ解釈