Vol.2013-SPT-7 No.2
2013/11/11

“Formal Definitions for Usable Access Control Rule Sets From Goals to Metrics” の紹介

葛野 弘樹[1,a)]

概要：本稿では，Beckerle らが SOUPS 2013 において発表した研究 [1] を紹介する．システムリソースに対するアクセス制御を適切に行うためには，アクセス制御ルールセットの理解が必要であるが，アクセス制御ルールセットの作成と管理は難しい．Beckerle らは，これらの課題を解決するために，ユーザブルアクセス制御ルールセット（Usable Access Control Rule Sets）を提案し，1）アクセス制御ポリシの反映，2）簡単な理解と管理，が可能と述べており，ユーザブルアクセス制御ルールセットが満たす 6 つの目標とその形式的な定義，そして，2 つのユーザスタディから効果的なアクセス制御が可能なことを示した．

Summary Report of “Formal Definitions for Usable Access Control Rule Sets From Goals to Metrics”

1. はじめに

Beckerle らは，アクセス制御機構は，(a) リソースへのアクセス権は，認可されたユーザのみ与えられる, (b) リソースへのアクセス権は，認可されたユーザに与えられないことはない, ことを保証するとしている．アクセス制御機構で用いるアクセス制御ポリシおよびポリシを記述するアクセス制御ルールセットは複雑であり，管理や誤りの把握が難しくなる．そこで，Beckerle らは，ユーザブルアクセス制御ルールセットを提供し，(i) ユーザブルアクセス制御ルールセットはアクセス制御ポリシ ((a),(b) を満たす) を反映する，(ii) ユーザブルアクセス制御ポリシは容易に理解・管理する，ことを目的としている．

2. 事前調査

Beckerle らの研究では，まず，7 名の異なる組織のシステム管理者にアクセス制御ルールセットの管理における課題についての調査を行い，その結果を 6 つにまとめている．

- (G1) ルールセットは認可されていないアクセスは拒否しなければならない
- (G2) ルールセットは認可されたアクセスは許可しなければならない
- (G3) 冗長なルールは削除する必要がある
- (G4) 矛盾するルールは削除する必要がある
- (G5) 大規模ルールセットより簡潔ルールセットが良い
- (G6) ルールセットは管理者がユーザをルールセットから容易に追加削除できるよう管理できるようデザインされていた方がよい

3. ユーザブルアクセス制御の目標

事前調査で得られた課題を整理し，ユーザブルアクセス制御が満たすべき 6 つの目標をあげている．

- *(G1)* リソース所有者の許可しか認めない
- *(G2)* リソース所有者の許可は全て認める
- *(G3)* ルールセット内のルールは他のルールによりカバーされるべきではない
- *(G4)* ルールセット内の二つのルールが不一致になるべきではない
- *(G5)* ルールセットの要素数は最小限とする
- *(G6)* システム変更時の維持管理は最小限とする

4. ユーザブルアクセス制御の形式的定義

定義 4.1 要素．W を全要素，E をシステム S の全要素，B をシステム上のグループの所有者とし，$W \supseteq E$, $W \supseteq B$ とする．

[1] セコム株式会社 IS 研究所
Intelligent Systems Laboratory, SECOM Co., Ltd., Mitaka, Tokyo, 181–8528, Japan
[a)] h-kuzuno@secom.co.jp

定義 4.2 属性．$\mathring{A}$ を全属性，A を $\mathring{A}$ の部分集合とする．

定義 4.3 オブジェクト．O を全てのオブジェクト，D をシステム上の全ての集合とし，$O \supseteq D \supseteq H$ とする．

定義 4.4 アクセス判定．アクセス判定結果は $Z = \{-1, 1\}$，-1 はアクセス拒否，1 はアクセス許可とする．

定義 4.5 ルールとルールセット．ルールセットは $R = (r_1, \ldots, r_n)$, ルールは $r_i = (A_i, H_i, z_i)$ とする．

定義 4.6 システム．システムは $S = (B, E, D, R) \in p(W) \times p(W) \times p(O) \times (p(\mathring{A}) \times p(D) \times Z)^n$ とする．

定義 4.7 属性抽出関数 f_A．要素 w の全ての属性 A_w を返す関数を $f_A : W \to p(\mathring{A}), w \mapsto f_A(w) := A_w$ とする．

定義 4.8 アクセス判定関数 $f_{request}$.

$$f_{req}(A_w, H_w, i) := \begin{cases} z_{default} & if\ (i > n), \\ z & if\ A_w \supseteq A_i, H_w \subseteq H_i \\ & .(A_i), H_i, z_i) = r_i, \\ f_{req}(A_w, H_w, i_1) & else. \end{cases}$$

n はルールセット R のルール数，$i \in N, i \leq i$，$z_{default}$ はルールが存在しない場合のルール．

定義 4.9 所有者の意図（Owners' Intention）．

$$f_{intended}(w, H) := \begin{cases} 1 & if\ B\ wants\ f_{request}(w, H) = 1, \\ -1 & else \end{cases}$$

定義 4.10 システムアクセス判定セット．システムにおけるアクセス判定を $M_{E_{Allow}}$, $M_{E_{Deny}}$, オブジェクトの所有者によるアクセス判定を $M_{E_{Wanted}}$, $M_{E_{Unwanted}}$ とする．

定義 4.11 ワールドアクセス判定セット．システムアクセス判定セットをワールドに一般化した判定を $M_{W_{Allow}}$, $M_{W_{Deny}}$, $M_{W_{Wanted}}$, $M_{W_{Unwanted}}$ とする．

セキュリティとユーザビリティの評価

ユーザブルアクセス制御の目標 $Gi, (1 \leq i \leq 6)$ に定義 4.1 から 4.11 を用い形式的定義を与えている．

- *(S_{G1})* 過剰なアクセス許可，所有者が許可した以上には許可しない．$S_{G1} = M_{E_{Allow}} \setminus M_{E_{Wanted}}$
- *(S_{G2})* 少なすぎるアクセス許可，所有者の許可以上に少なくしない．$S_{G2} = M_{E_{Wanted}} \setminus M_{E_{Allow}}$
- *(S_{G3})* 冗長なルール, $S_{G3} = \{(r_i, r_j).0 \leq i \leq n-1 \wedge i < j \leq n \wedge A_j \supseteq A_i \wedge H_j \subseteq H_i \wedge z_j = z_i\}$
- *(S_{G4})* 矛盾するルール．$S_{G4} = \{(r_i, r_j).0 \leq i \leq n-1 \wedge i < j \leq n \wedge \exists(e,h).(f_A(e) \supseteq A_i, h \subseteq H_i, z) \not\exists (f_A(e) \supseteq A_j, h \subseteq H_j, -z)\}$
- *(S_{G5})* ルールセットの要素数．$S_{G5} = R\ and\ |S_{G5}| := \sum_{(A_i,H_i,Z_i)\in R} |A_i| + |H_i| + 1$
- *(S_{G6})* 将来的な不正なアクセス判定．$S_{G6} = M_{W_{Allow}} \triangle M_{W_{Wanted}} \cup M_{W_{Deny}} \triangle M_{W_{Unwanted}}$

不正なアクセス判定のコスト

$cost_{S_{G1}} = \sum_{d\in X} f_{S_{G1}}(d)$, $X = \{d|(e,d) \in M_{E_{Allow}} \setminus M_{E_{Wanted}}\}$, $cost_{S_{G2}} = \sum_{d\in Y} f_{S_{G2}}(d)$, $Y = \{d|(e,d) \in M_{E_{Wanted}} \setminus M_{E_{Allow}}\}$, $total\ cost = cost_{S_{G1}} + cost_{S_{G2}}$

5. 評価

提案手法の評価をユーザスタディにより行っている．

- 仮説 $H1$：集合，メトリック，基準はユーザが良いルールの提供を補助する．
- 仮説 $H2$：メトリックスコアはポリシからアクセス制御ルールセットに変換する際のランキングに相当する．
- 仮説 $H3$：メトリックスコアはアクセス制御ルールの理解性と管理性を評価する際のランキングに相当する．

ユーザスタディ

ユーザスタディ 1 では，11 名の被験者（IT サポート 4 名，学生 7 名）が，既存のアクセス制御ルールセットの変更，追加，削除を行うにあたり，提案手法のサポートの有無がどのように影響するかをコストとして調査している．ユーザスタディ 2 では，ユーザスタディ 1 で得られたアクセス制御ルールを 4 名の IT サポートの経験と知識により評価しランキング付けする．評価基準は（a）正確なルールセットがアクセス制御ポリシから得られているか，（b）簡単にルールセットが理解し管理できるか，の 2 点である．

評価結果

ユーザスタディ 1 におけるアクセス制御ルールでは，提案手法を用いた場合の方がコストが低い結果が得られたことを示している．ユーザスタディ 2 では，IT サポートより得られたランキングと提案手法により評価したランキングについて，スピアマンの順位相関係数により評価し，仮説に対し高い相関係数が得られたことを示している．

6. 課題と考察

Beckerle らは，研究課題としてユーザスタディで用いたルールセットが小規模である点，被験者が少ない点をあげている．考察として，Beckerle らが定義したユーザブルアクセス制御ルールセットは事前調査を基にしていることから部分的であるとしている．また，ユーザインタフェイスデザインの考慮や所有者の意図の動的な確認，コスト計算の拡張を今後の研究課題としてあげている．

7. まとめ

Beckerle らは，ユーザブルアクセス制御ルールの新たな指標の提案として，事前調査より 6 つの目標を整理し，それらを形式的に定義した．そして，ケーススタディにより，提案手法を用いることで，ユーザブルアクセス制御ルールセットの最適化と管理性の改善が可能なことを示した．

参考文献

[1] Beckerle, M. and Martucci, L. A.: Formal Definitions for Usable Access Control Rule Sets From Goals to Metrics, *The Ninth Symposium On Usable Privacy and Security* (2013).