Web アプリケーションにおける ユーザ権限によるアクセス制御のテスト

2004MT021 早川 さやか　　2004MT056 蒔田 沙織
指導教員　蜂巣 吉成

1　はじめに

アクセス制御機能を持つ Web アプリケーションの増加に伴い，アクセス制御に関わるセキュリティの問題が顕在化してきた．Web アプリケーションの各ページは全て独立しているので，URL を指定することによってあらゆるページに遷移することが可能となる．そのため，Web アプリケーションにおけるアクセス制御のテストでは，すべてのページに対する網羅的なテストが必要となり，テストに多くのコストがかかってしまう．

本研究の目的は，アクセス制御に関するテストのコストを削減することである．これを実現するために，アクセス制御のテストのためのテスト基準を提案する．また，この基準に従ってテストケースを生成することにより，テストケースの数を削減することができることを示す．

本研究は，以下のように進める．

1. Web アプリケーションの例として卒業論文題目登録システムの設計
2. アクセス制御に関するテストについての考察
3. アクセス制御のテスト基準の提案

なお，早川さやかは主に Web アプリケーションのテスト手法を，蒔田沙織は主にテストシーケンス生成を担当した．

2　関連研究

ページ生成プログラムに対する従来のテスト手法には，Web アプリケーションのページ間の遷移にもとづく，ページ網羅，遷移網羅，パス網羅のためのテスト自動化手法がある [1]．この手法は Web アプリケーションの各ページに対して仕様を記述し，その仕様中のリンクおよびフォームによる，ページ間遷移をもとにテストシーケンスを生成し，Canoo Web テストをもちいて自動実行する．ページの仕様からテスト自動実行がおこなえる点で他の手法に比べて容易にテストがおこなえるが，ページ間の直接的な遷移しか考慮していないのでアクセス制御のテストが十分におこなえない．

3　Web アプリケーションにおけるアクセス制御のテスト基準

本章では，テスト対象の Web アプリケーションの前提およびアクセス制御のテストに関する基準について述べる．

3.1　Web アプリケーションに関する前提

本研究で対象としている Web アプリケーションは以下の条件を満たしているものとする．

1. MVC モデルに従って設計されている
2. 遷移要素は動的に生成されない
3. 権限情報はセッションで管理されている
4. 1 度に 2 つ以上の権限を持たない

近年開発されている多くの Web アプリケーションはこれらの条件を満たしており，テスト支援の対象として一般的なものである．

3.2　アクセス制御のテスト

Web アプリケーションは各ページでアクションを実行することにより，次のページへ遷移する．権限はそのアクションが実行されたときにセッション変数として保持される．アクセス制御はそのセッション変数に保持された権限の情報をもとに，各ページまたはアクションで行なわれる．

Web アプリケーションのアクセス制御が正しくおこなわれているかテストするには，権限操作アクションが正しく動作しているか，閲覧不可能なページが閲覧不可能であるかを確認すべきである．

これらのテストをおこなうためには，遷移関係だけではなく，閲覧不可能なページへの遷移も考えてテストシーケンスを生成する必要がある．

3.3　アクセス制御に関するテスト基準

我々は，アクセス制御のテストを網羅的におこなうための，テストシーケンスを生成する基準を定めた．テストすべき遷移を通る経路を求めるための基準と，その経路によって到達したページからアクセス制御の確認をするためのページとアクションを求めるための基準に従ってテストシーケンスを生成する．

＜経路に関する基準＞

1. Web アプリケーションのいずれかの初期ページからの最短経路 [権限操作アクション網羅]
2. Web アプリケーションの全ての初期ページから到達する全ての経路 [権限操作アクションに対するパス網羅]

権限情報を操作するアクションの動作がそれまでの経路に依存しない場合，そのアクションに行き着くまでの経路によって付加される権限情報に変化がない．この場合，権限を操作するアクションを網羅することによって十分なアクセス制御のテストが可能である．したがって，権限操作アクションまでの経路は初期ページからの最短経路で十分である．

権限情報を操作するアクションの動作がそれまでの経路に依存する場合，そのアクションに行き着くまでの経路によって付加される権限情報が異なる可能性がある．そこで，権限操作アクションに対するパス網羅による全て

の経路に関するテストが必要である．
＜テスト対象に関する基準＞

1. 他のグループのページ，他のグループへ遷移するアクション 1 つずつ [グループ網羅]
2. 他のグループのページ，他のグループへ遷移するアクション全て [ページ・アクション網羅]

それぞれのグループのアクセス制御がグループ内のページやアクションに対してアクセス制御が同じ方法でおこなわれている場合，テスト対象となるグループ内の全てのページとアクションでアクセス制御が正しくおこなわれていることは容易に確認できる．他のグループの任意のページとアクションが閲覧できないことを確かめることによってそのグループのアクセス制御を確認することができる．
逆にグループ内のページやアクションに対してアクセス制御の方法が異なる場合，ページ・アクション網羅にしたがって全てのページとアクションをテストしなければそれぞれのアクセス制御が正しくおこなわれていることを確認できない．

4 テストシーケンス生成

テストシーケンスを生成する手順は, 以下の流れで行う．

- ページ遷移モデルとグループ仕様からテストシーケンス生成
  1. Web アプリケーションの初期ページから，権限操作アクションによって権限情報が変更されて遷移したページ (アクセス制御テストページ) までの経路を求める．
  2. アクセス制御テストページから，そのグループが閲覧不可能なページへの遷移を 1 の経路に加える．

4.1 ページ遷移モデル

ページ遷移モデルとは，テストシーケンス生成のためにページ間の遷移関係を明確にし，アクションとそれによって変化する権限情報を遷移のラベルとして表現したモデルである．
ページ遷移モデルの例を図 1 に示す．この例では，ページ login からページ A に遷移する際，アクション A1 が実行され，group1 の権限が付加されることを示している．

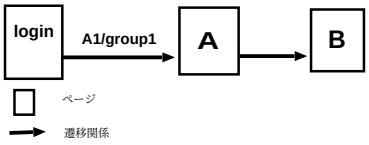

図 1　ページ遷移モデルの例

4.2 グループ仕様

グループ仕様とは，アクセス制御されているグループの種類とそのグループに属するページ名とアクション名が記されたものである．アクセス制御されるグループごとに分けることで，グループごとに遷移可能なページやアクション，遷移不可能なページやアクションがわかり，アクセス制御のテストが可能になる．

4.3 テストシーケンス生成アルゴリズム

テストシーケンスは，ページ遷移モデルとグループ仕様で生成することができる．また，権限操作アクションによって，権限の情報が変更された後のページから他のグループへの遷移をテストする必要があり，そのページに到達するための経路を求める必要がある．そのための手順を以下に示す．

4.3.1 アクセス制御テストページまでの到達経路

＜権限操作アクション網羅の場合＞

1. Web アプリケーションの初期ページのうち一つをテストシーケンスのスタートページとして定める．
2. スタートページから権限アクションを実行して次のページに遷移するまでの最短経路を求める．
3. 求められた最短経路が，到達経路になる．

＜権限操作アクションに対するパス網羅の場合＞

1. Web アプリケーションの全ての初期ページをテストシーケンスのスタートページとする．
2. スタートページから，権限アクションを実行して次のページまでのすべての到達経路を求める．
3. 求められた全ての経路が，到達経路になる．

4.3.2 アクセス制御の確認方法

1. アクセス制御テストページまでの到達経路の基準によって，アクセス制御テストページまでの到達経路を決める．
2.
   - グループ網羅の場合
     アクセス制御テストページから，そのページを閲覧できるグループが閲覧不可能な他のグループのどれか 1 つのページとアクションへの遷移をテストする．(テスト対象となる各グループの 1 つのページとアクションは，そのグループの先頭のページとアクションとする．)
   - ページ・アクション網羅の場合
     アクセス制御テストページから，そのページを閲覧できるグループが閲覧不可能な他のグループの全てのページとアクションへの遷移をテストする．
3. 求められた到達経路とテスト対象のページとアクションからテストシーケンスを生成する．

4.3.3 アクセス制御テストページのアクションによるテストの種類

4.3 節で述べた生成アルゴリズムによって生成されるテストシーケンスを形式化する．テストシーケンスは以下の 3 種類を考察する必要がある．

- 権限が付加されたときに，他のグループのページとアクションは閲覧不可能であるか
- 権限が破棄されたときに，アクセス制御されている全てのページとアクションが閲覧不可能であるか

- 権限が変更されたときに，変更後のページから他のグループのページとアクションは閲覧不可能であるか

4.3.4 テストシーケンス

以上のことにより生成されるテストシーケンスは以下のようになる．また，それぞれの基準によって，テストシーケンスは異なる．

- P：ページの集合
- A：アクションの集合 ($a_i \in A$)
- G：グループの集合
- S：スタートページの集合 ($s_i \in S$)
- T：遷移要素の集合 ($t_i \in T$)
- P^{g_i}：グループ g_i が閲覧不可能なページの集合 ($g_i \in G$，$P^{g_i} \subset P$，$p_j^{g_i} \in P^{g_i}$)
- A^{g_i}：グループ g_i に遷移しないアクションの集合 ($g_i \in G$，$A^{g_i} \subset A$，$a_j^{g_i} \in A^{g_i}$)
- T^{g_i}：グループ g_i の権限付加する遷移，グループ g_i の権限破棄する遷移，グループ g_i の権限変更する遷移の集合
- $p_i \rightsquigarrow_{short} p_j$：$p_i$ から p_j に到達する最短経路 (p_i，$p_j \in P$)
- $p_i \rightsquigarrow p_j$：p_i から p_j に到達する経路 (p_i，$p_j \in P$)
- $p_i \xrightarrow{T_j} p_k$：$p_i$ から t_j によって p_k に遷移 (p_i，$p_k \in P$，$t_j \in T$)

＜権限操作アクション網羅とグループ網羅＞

$\forall g_i \in G$，$\forall t_k^{g_i} \in T^{g_i}$ に対して次の式で表現される経路がテストシーケンスとなる．

- $s_0 \rightsquigarrow_{short} p_j \xrightarrow{t_k^{g_i}} p_l \rightarrow p_0^{g_i}$
- $s_0 \rightsquigarrow_{short} p_j \xrightarrow{t_k^{g_i}} p_l \rightarrow a_0^{g_i}$

＜権限操作アクション網羅とページ・アクション網羅＞

$\forall g_i \in G$，$\forall t_k^{g_i} \in T^{g_i}$，$\forall p_m^{g_i} \in P^{g_i}$，$\forall a_m^{g_i} \in A^{g_i}$ に対して次の式で表現される経路がテストシーケンスとなる．

- $s_0 \rightsquigarrow_{short} p_j \xrightarrow{t_k^{g_i}} p_l \rightarrow p_m^{g_i}$
- $s_0 \rightsquigarrow_{short} p_j \xrightarrow{t_k^{g_i}} p_l \rightarrow a_m^{g_i}$

＜パス網羅とグループ網羅＞

$\forall g_i \in G$，$\forall s_j \in S$，$\forall t_l^{g_i} \in T^{g_i}$ に対して次の式で表現される経路がテストシーケンスとなる．

- $s_j \rightsquigarrow p_k \xrightarrow{t_l^{g_i}} p_m \rightarrow p_0^{g_i}$
- $s_j \rightsquigarrow p_k \xrightarrow{t_l^{g_i}} p_m \rightarrow a_0^{g_i}$

＜パス網羅とページ・アクション網羅＞

$\forall g_i \in G$，$\forall s_j \in S$，$\forall t_l^{g_i} \in T^{g_i}$，$\forall p_n^{g_i} \in P^{g_i}$，$\forall a_n^{g_i} \in A^{g_i}$ に対して次の式で表現される経路がテストシーケンスとなる．

- $s_j \rightsquigarrow p_k \xrightarrow{t_l^{g_i}} p_m \rightarrow p_n^{g_i}$
- $s_j \rightsquigarrow p_k \xrightarrow{t_l^{g_i}} p_m \rightarrow a_n^{g_i}$

権限操作アクションに対するパス網羅では，初期ページからアクセス制御テストページまでの任意の経路を求める必要があるが，遷移がループしている場合，その経路は無限となってしまう．そこでループに関しては，以下のルールに従って経路を求める．

(a) エラーによる元のページへの遷移を辿らない．

(b) 遷移先が一つしかないページへの戻る遷移を辿らない．

(c) ログアウトなどにより，セッションを破棄する遷移を辿らない．

5 適用例

5.1 卒業論文題目登録システム

提案したテスト方法を実際におこなうために，Web アプリケーション開発の一例として，卒業論文題目登録システムの設計をおこなった．

本システムにおける権限の種類とそれぞれの権限で閲覧可能なページおよび利用可能なアクションを**表 1** に示す．また，ページ遷移モデルを**図 2** に示す．

5.2 テストシーケンスの適用例

4 章で述べたテストシーケンス生成方法に従ってテストシーケンスを生成した．以下に，group1 のそれぞれの基準の場合のテストシーケンスの数を示す．

＜権限操作アクション網羅とグループ網羅＞

$(s_0 \rightsquigarrow_{short} p_j \xrightarrow{t_k^{g_i}} p_l \rightarrow p_0^{g_i}) + (s_0 \rightsquigarrow_{short} p_j \xrightarrow{t_k^{g_i}} p_l \rightarrow a_0^{g_i})$

$= 14$ 通り

＜権限操作アクション網羅とページ・アクション網羅＞

$(s_0 \rightsquigarrow_{short} p_j \xrightarrow{t_k^{g_i}} p_l \rightarrow p_m^{g_i}) + (s_0 \rightsquigarrow_{short} p_j \xrightarrow{t_k^{g_i}} p_l \rightarrow a_m^{g_i})$

$= 72$ 通り

＜パス網羅とグループ網羅＞

$(s_j \rightsquigarrow p_k \xrightarrow{t_l^{g_i}} p_m \rightarrow p_0^{g_i}) + (s_j \rightsquigarrow p_k \xrightarrow{t_l^{g_i}} p_m \rightarrow a_0^{g_i})$

$= 712$ 通り

＜パス網羅とページ・アクション網羅＞

$(s_j \rightsquigarrow p_k \xrightarrow{t_l^{g_i}} p_m \rightarrow p_n^{g_i}) + (s_j \rightsquigarrow p_k \xrightarrow{t_l^{g_i}} p_m \rightarrow a_n^{g_i})$

$= 2882$ 通り

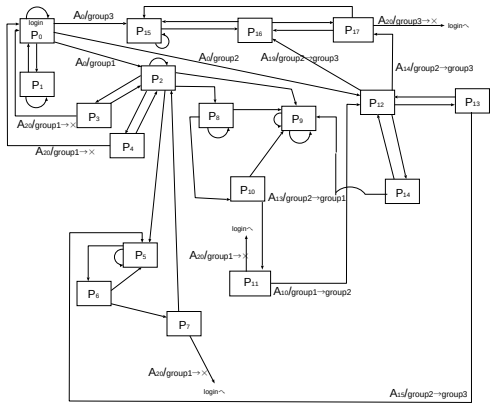

図 2　ページ遷移モデル

表 1　グループ仕様

権限の種類	ページ名	アクション名
group1	P_2,P_3,P_4,P_5,P_6, P_7,P_8,P_9,P_{10},P_{11}	A_2,A_3,A_4,A_5,A_6, A_7,A_8,A_9,A_{10}
group2	P_{12},P_{13},P_{14}	A_{11},A_{12},A_{13}, A_{14},A_{15},A_{19}
group3	P_{15},P_{16},P_{17}	A_{16},A_{17},A_{18}

6　考察

6.1　基準の確認

アクセス制御のテストは，経路に関する基準およびテスト対象ページに関する基準によって削減することができた．最も少ないテストシーケンスでアクセス制御が正しくおこなわれていることを確認するためには以下のことを確認する必要がある．

- 経路に依存するかどうかは一般には確認できないが，単体テストによって経路に依存していないことが確認されている Web アプリケーションにはテスト基準として使用できる．
- グループのアクセス制御がグループ内のページやアクションに対して同様におこなわれていることは，ページやアクションのプログラムの中の権限情報の制御方法を確認すればよい．フレームワーク設定ファイルやアクションの中で制御している場合は，グループ内のアクセス制御が異なる可能性がある．
- エラー処理によるループのあとに権限情報が操作されないことは，エラー処理のアクションのプログラムの中で権限情報を保持しているセッション変数が変更されていないことを確認すればよい．

6.2　テストシーケンス削減

本研究で提案するアクセス制御に関するテストについて考察する．アクセス制御が正しくおこなわれているかテストするには, 権限操作アクションが正しく動作しているか，閲覧不可能なページが閲覧不可能であるかを確認しなくてはならない．グループ g_i に対するテストにおける，アクセス制御を考慮したテストシーケンスの最大数は，以下の式で求められる．

(g_i のページ全てに対して，全ての初期ページからの経路の総数) $\times$ ($|P^{g_i}| + |A^{g_i}|$)

しかし，この計算では小規模なシステムのテストでも組合せ爆発を起こしてしまう可能が高い．

本研究で提案した基準に基づいたテストシーケンスでは，その数は以下の式で表される．

＜権限操作アクション網羅とグループ網羅＞

(g_i の権限情報が付加，変更する遷移ラベルの数) $\times$ ($|G| - 1$) $\times$ 2 + (g_i の権限情報が破棄する遷移ラベルの数) $\times$ $|G| \times 2$

＜権限操作アクション網羅とページ・アクション網羅＞

(g_i の権限情報が付加，変更する遷移ラベルの数) $\times$ ($|P^{g_i}| + |A^{g_i}|$) + (g_i の権限情報が破棄する遷移ラベルの数) $\times$ ($|P| + |A|$)

＜パス網羅とグループ網羅＞

{(g_i の権限情報が付加する遷移全てに対して全ての初期ページからの経路の総数) + (g_i の権限情報が変更する遷移全てに対して全ての初期ページからの経路の総数)} $\times$ {($|G| - 1$) + (g_i の権限情報が破棄する遷移全てに対して全ての初期ページからの経路の総数) $\times$ $|G|$} $\times$ 2

＜パス網羅とページ・アクション網羅＞

{(g_i の権限情報が付加する遷移全てに対して全ての初期ページからの経路の総数) + (g_i の権限情報が変更する遷移全てに対して全ての初期ページからの経路の総数)} $\times$ ($|P^{g_i}| + |A^{g_i}|$) + (g_i の権限情報が破棄する遷移全てに対して全ての初期ページからの経路の総数) $\times$ ($|P| + |A|$)

網羅的にテストシーケンスを考えると，任意のページから他のグループのページおよびアクションに対してテストすることが必要となるが，我々の提案手法では，権限情報の変更が起こった後のページから他のグループへのテストを行う．権限情報の変更を行うアクションは Web アプリケーションの総ページ数に比べて非常に少ないため，提案手法により大幅にテストケースを削減することができる．

また，適用例である卒業論文題目登録システムは，HttpUnit などを利用した単体テストによって各アクションに対するテストを十分に行うことができ，また一般的な Web アプリケーションでは統一された方法でアクセス制御を行っているため，一般的な多くのアプリケーションでは，権限操作アクション網羅とグループ網羅によるテストシーケンスで十分だと考えられる．

7　まとめ

本研究では，Web アプリケーション開発の一例として，卒業論文題目登録システムの開発を行った．この卒業論文題目登録システムを例に従来のテスト手法におけるアクセス制御に関してのテストの問題点を考察し, アクセス制御に関するテストのコスト削減をおこなうためのテストシーケンス生成手法を提案した．提案した基準は 6.1 節で述べたことを確認することによって全てを網羅するテストと同等の事を確認することができる。今後の課題として，テストシーケンス自動生成ツールを作成が挙げられる．

謝辞

本研究を進めるにあたり熱心な御指導をいただいた蜂巣吉成先生，野呂昌満先生，沢田篤史先生，渥美紀寿先生，大学院生のみなさまに深く感謝致します．

参考文献

[1] 渥美紀寿，桑原寛明，金子伸幸，山本晋一郎，阿草清滋：高信頼 Web アプリケーションのためのページ生成プログラムのテスト手法，コンピュータソフトウェア,Vol.24,No.4(2007),pp.153-164.