アクセスコントロール技術の動向と将来課題

千葉　直子　　大嶋　嘉人　　中嶋　良彰
ＮＴＴ情報流通プラットフォーム研究所

1　はじめに

リソースの参照や変更等のアクションを、許可されたユーザのみに制限するためのアクセスコントロール技術は、これまでに多くの技術開発が行なわれてきた。近年、インターネットサービスの普及と共に、社内システム等で用いられてきた従来型のアクセスコントロール機構では、不十分な点が明らかになり、新しい技術の検討が進められている。

本稿では、アクセスコントロール技術の動向と今後の課題について述べる。

2　アクセス制御情報の管理方式の動向

アクセス制御情報とは、どのようなアクセスが許可・拒否されるべきかを定義したアクセス可否の判断規則であり、「アクション(アクセス対象リソースと動作種別)に関する条件」、「アクセス者に関する条件」、「その他環境的条件」の組合せ及びその許可・拒否によって表される。ここでは、主に「アクセス者に関する条件」の記述方式に着目し、その動向について述べる。

①ID ベース
- 個々のアクセス者に対して権限の付与を行なう最も古典的な方法。

[例] “ID=001”は、ファイル A を参照でき、“ID=002”は、ファイルAを参照及び変更できる。

②ロールベース
- アクセス者を所属や役職等の「ロール」によって分類すると共に、権限をロールに対して付与する方法。アクセス者と権限の管理を分離することにより、個々の ID ごとに権限を管理するよりも、ユーザの追加や削除が容易。(図 1)

[例] “ID=001”と“ID=002”は、“ロール=課長”を持つ。“ロール=課長”はファイル B の実行ができる。

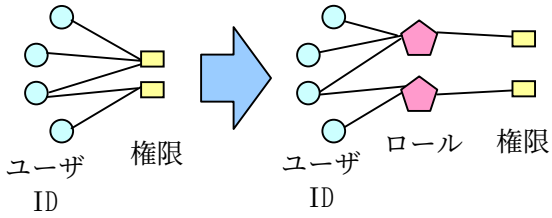

図 1: ID ベースとロールベース

③動的属性ベース
- 短期間に変動し得るアクセス者の特徴(属性)に対しても権限を付与可能とし、よりダイナミックな権限管理を行なう方法。

[例] アクセス者の「累積購入額」属性が 10 万円を超えたら、お得意様サービスを利用可能とする。

3　インターネット上のサービスにおけるアクセスコントロール

近年のインターネットの爆発的な普及に伴い、インターネット上で実現されるサービスに対する様々なセキュリティ課題が明らかになってきている。特に、ユーザの多様化に伴ない、ユーザごとにサービスの利用権限をより厳密に管理するアクセスコントロール技術は、インターネット上でより安全かつ利便性の高いサービスを実現するうえで必須である。例えば、学生限定の情報提供サービスや、年齢によって提供するメニューを変える EC サービス等のサービスにおいては、資格の有無によるアクセスコントロールが必要である。

イントラネット等で用いられている従来のアクセスコントロール機構では、リソース管理者は、ユーザ(アクセス者)の ID を識別し、その ID をもとにロールや属性をリソース管理者自身の DB 等から取得し、制御を行なう。ユーザの母集団が固定的なイントラネット等では、ユーザが事前登録をして、管理者がユーザに ID を付与したり、ユーザに付随する属性情報を集中

“A Survey of Access Control Techniques”
Naoko Chiba, Yoshihito Oshima, Yoshiaki Nakajima
NTT Information Sharing Platform Laboratories

的に管理したりすることは、十分に実施可能であった。

ところが、インターネット上のサービスでは、サービス提供者とユーザは多対多であり、その関係も動的に変化することから、従来のアクセスコントロール機構では以下のような問題が顕著になる。

(A) アカウント管理
- ユーザは、個々のサービスごとにユーザ登録・ログインを要求され、面倒である
- サービス提供者は、アクセスしてくるユーザ全てのアカウント管理を行わなければならず、負担である

(B) 属性の集中管理
- ユーザは、個々のサービスごとに必要な属性を登録しなければならず面倒である
- サービス提供者は、ユーザが登録した属性の確かさを確認、かつこれらを管理する必要がある

上記で挙げたような問題を解決する手段として、以下のような技術が開発されつつある。

(A) アカウント管理
- Liberty Alliance や Passport 等のシングルサインオン(SSO)技術により、ログインの煩雑さやユーザアカウントの管理コスト等は解消されつつある。

(B) 属性の集中管理
- X.509 の属性証明書や、SAML(Security Assertion Markup Language)の属性証明技術により、第三者が管理する属性の安全な入手と利用が可能になりつつある。

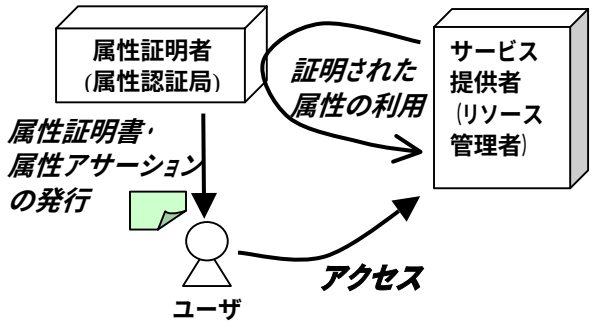

図 2: 第三者の発行する属性証明情報の利用

さらに、SAML と組合せて利用する XACML (eXtensible Access Control Markup Language)等、Web サービスでアクセスコントロールを行なうためのポリシ(ルール)を記述する言語仕様の標準化も進んできている。

4 今後の課題

上記のように、技術開発は進展してきているものの、残された課題は多い。今後解決すべき課題を以下に述べる。

(A) アカウント管理

SSO 技術でも、依然としてサービス提供者ごとにユーザアカウントを作成し、管理する負担は解消されていないため、各サービス提供者のアカウント管理負担を軽減する仕組みが必要である。

(B) 属性の集中管理

属性の確認を第三者が集中的に行ない、その結果を流通させる仕組みが出来たとしても、誰が発行した、どのような属性を、どのように利用すれば良いのかといった知識や判断が難しい。全体的な方法論の整備や、例えば、「○○属性認証局を信頼する」といった単純なトラストポイントの指定ではなく、「○○属性認証局が発行した、△△に関する属性証明情報を信頼する」といったことなど、より柔軟な信頼関係を構成する必要がある。

また、属性の利用に関して、ユーザの属性をサービスの権限に結び付ける部分は、サービス提供者が個々に手動で行なう場合が多いので、今後、属性と権限のマッピングを自動化・簡素化する仕組みが必要になると考えられる。

[参考文献]

- “XML-Based Security Services TC (SSTC) Security Assertion Markup Language”, http://www.oasis-open.org/committees/security/
- ” OASIS eXtensible Access Control Markup Language TC”, http://www.oasis-open.org/committees/xacml/