ISS-P-254

属性管理とセキュリティレベルの多重化について

関　陽介† 松浦　健二†† 佐野　雅彦†† 上田　哲史††
† 徳島大学　知能情報工学科　　†† 徳島大学　情報化推進センター

1. はじめに

徳島大学では教育・業務等に利用する複数のシステムを，SAML をベースにしたオープンソースである Shibboleth[1]を用いることで学内構成員向けシングルサインオンを実現し，認証基盤を統一することで利用者や管理者の負荷軽減を図っている．本研究では本学の個人属性情報の管理と Shibboleth のセキュリティ強化をとりあげ，実運用に寄与する拡張機能に関する設計上の方針を検討する．

2. 問題点について

(1)大学組織では多くの場合，構成員に関する ID やパスワード，所属等の属性を一元的に管理(以下，「人事管理基盤」と呼ぶ)[2]している． Shibboleth は認証に加え，属性を元に認可制御を行うため，その判断基準となる属性の登録が必要である．しかし，本学は併任等で基準となる所属等の属性が未登録の場合があり，認可制御に必要な情報が不十分なケースが発生する．

(2)Shibboleth 認証は一般的な認証方式と同じくアカウント入力(ID,PW)を要求する．つまり，単一の認証方式ではアカウントが漏れた場合，その漏洩に対する堅守性はないため，不正アクセスされる可能性は避けられない．そのため，運用面での回避，認証・認可制御の見直しなど，多角的にセキュリティ強度を高める対策を検討する必要性が求められる．

3. 解決案とシステム設計

(1) 人事管理基盤とは別に，自由に登録可能な付加属性管理原(以下，「拡張認可 DB」と呼ぶ)を用意する．これは人事管理基盤の構成員データと紐付いており，構成員の所属等の属性を補完する位置づけである．

設計としては，拡張認可 DB を MySQL などのオープンソースで構築し，Shibboleth の参照先に登録することで，対象システムへ構成員に関する属性とそれに紐付く登録情報を渡す．属性の登録権限は，各組織に属する総務課等の事務担当に付与することで，人事異動に伴う属性変更に，柔軟に対応させたい．拡張認可 DB に登録する UI は WebDAV を採用し，組織形態に従った階層化構造を設計することで，登録範囲を所属単位に制限する．担当者が登録用ファイル(csv 形式を想定)を所属毎に決められた場所に保存することで，拡張認可 DB に反映させる．

(2)IC カードを用いた多重認証方式を採用する．アカウントが漏洩しても物理トークンである IC カードを保有していない限り，不正アクセスされる危険は軽減される．多重認証は利便性とのトレードオフであるため，その適用範囲は人事給与システムや高い機密性が求められる特定の領域など，重要性が高いものに限られるべきである．そこで，特定のシステムや領域を利用する利用者に対して，人事管理基盤や拡張認可 DB に登録された属性を判断基準として多重認証を実現する．

設計としては，IdP に x.509 規格に準拠した証明書認証を実装する．利用者にアカウントと IC カード内に記録された証明書を要求することで，アカウント漏洩に対する対策となる．また，IdP が取得する属性を元に認証方式(単一/多重認証)を提供することで，属性単位のセキュリティ強化が可能となる．(図1)

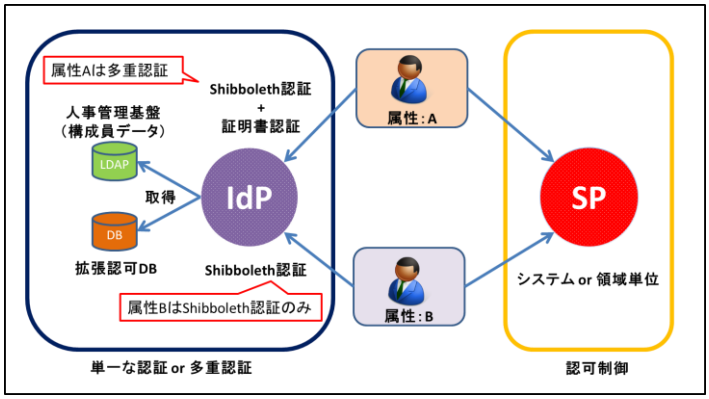

図1. 拡張認可 DB と多重認証

4. 今後の方針

現設計では多重認証を実現するため，利用者すべてに基準となる属性が必要となる．今後は IdP がシステムを基準の 1 つと判断し，①「Shibboleth 認証・認可」，②「属性を基準とする多重認証」，③「システムを基準とする多重認証」と，適用する認証方式を複数用意することで，本研究で提供するシステムの利便性を高めたい．また実運用を視野に入れ，拡張認可 DB や証明書の登録ポリシー等の検討も進めたい．

参考文献

[1]藤原 翔一郎，古村 隆明，岡部 寿男「プライバシー保護に考慮した Shibboleth における属性交換の拡張」，情報処理学会研究報告，2006-QAI-21(1)

[2] 松平拓也， 笹原禎也， 高田良宏， 東昭考， 二木恵，森 祥寛「大学における Shibboleth を利用した統合認証基盤の構築」， 情報処理学会論文誌，Vol.52，No2，pp703-713，2011