5Z-5

Shibboleth 認証におけるセキュリティレベルの多重化

関　陽介†　　松浦　健二†　　佐野　雅彦†　　上田　哲史†

徳島大学†

１．はじめに

現在，徳島大学では多くの情報システムを学内構成員向けに提供している．例えば,メールシステムや教務システム，コミュニケーションポータルサイトなど様々な用途に合わせたコンテンツが存在する．これらに対して,各コンテンツを利用者が円滑に利用するためには,必要な情報が効率良くセキュアに運用される情報基盤整備が重要である．そこで,シングルサインオン(=SSO)が各大学で採用されている[1].

さらに,現在，国立情報学研究所が中心となり,複数の大学間での情報システムの共有，相互乗り入れの実現を目指した学認プロジェクトが進められている．本プロジェクトの組織間認証連携には *Shibboleth* と呼ばれるオープンソースソフトウェアが用いられる．本認証連携技術は Internet2/MACE プロジェクトにおけるプロジェクトの下で開発が始められ，日本に限らず世界中の学術機関で利用されるフレームワークとなってきた.

本学ではこの Shibboleth を用いることで学内構成員向け SSO 環境を運用しており，また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,Shibboleth での SSO 環境下で生じる問題と認可制御の問題をとりあげ,実運用に寄与する拡張機能に関する設計上の方針を述べ,方向性を検討する.

２．検討課題

Shibboleth の構成は,SP(Service Provider), IDP(Identity Provider)，DS(Discovery Service)と,それらにアクセスする UA(User Agent)からなる．主に Web リソースを対象とするが,本学では Desktop SSO も実現している.

UA によりユーザが SP の扱うオンラインリソースにアクセスする際には,IDP で事前に認証されている必要がある．そのため,IDP は認証およびユーザ属性を扱うバックエンドサービス(LDAP のようなディレクトリサービスや RDBMS)を利用する[2].また IDP が必要に応じて取り扱うユーザ属性に基づく認可制御を SP 側で実施する形で,認証と認可の役割を担っている[3].DS は認証源のインタフェースとなる IDP を選択する機能をオプションとして提供するが,単一の IDP に基づく単一組織内での Shibboleth では不要である．以上におおまかな Shibboleth の認証および認可の枠組みをまとめたが,実際の運用上は,(0)SSO ならではの運用問題に加え(1)認証強度の多段化や(2)多用な認可制御が求められる.

(0)は,組織の形態や対象とするアプリケーションに依存して多様である．例えば,SSO の対象とすべきアプリケーションのガイドライン策定や,複合的なセッション保持時間の問題,共有端末での実装上の取決めなどが考えられる．これらは,SSO により一度認証が行われると，WEB プラウザを終了しない限り何度でもログインが可能となる利便性とのトレードオフとなる．つまり，一度の認証で横断的に各コンテンツにアクセスできる利点はあるが，反対にそれによるリスクの見積もりと対策が必須という事である．特に,よりセキュアな環境を求めるコンテンツ（以下，高コンテンツ）への適用が課題となる.

高コンテンツへの対策として,(1)や(2)の検討および実装が進められている.

３．設計方針の検討

前節(1)では,パスワードの運用方針の強化,OTP(OneTimePassword)やマトリクス認証といった単独機能での強度を高める取り組がある．加えて,Shibboleth 上も多要素認証(Multi Factor Login Handler)への対応が進んでおり,国内実装事例も報告され始めている．本質的には,認証強度の問題は,個人認証を技術的に高度化しようとする位置づけと捉えており,アクセスしている Subject が真の Subject であるかどうかの検証手段の多様性に関する問題である．したがって,リソース提供側の要求する信頼性に応じた認証強度の切り替えが可能かどうかがポイントと見なせる．また,これは個人を認証する事であり,擬人や役職による認可へも適用できない.

Designing Flexible Secure-Authorization based on Shibboleth
†Yosuke Seki, The University of Tokushima

Copyright ©2013 Information Processing Society of Japan.
All Rights Reserved.

そこで,本学では(2)の認可制御を多様化,多段化することを検討している.

認可制御を検討する上での基本的な考え方は,認証された特定個人に対するアクセス認可を行うという事であり,認証の層の上に,認可の層を置くモデルでとらえている. 例えば,SSO の世界での認証のみの連携を検討するならば,Kerberos その他の仕組みとの本質的な差別化は図れないが,Shibboleth にはまず個人属性による認可制御が実装できる特徴がある.

属性認可の大前提は,オンライントランザクションの中で属性をサーバからサーバへと流通させる事であるが,それゆえ,属性プロバイダには事前に個人に紐づけられた特定の属性名,属性値をセットしておく必要がある. この場合,認可権限移譲が即時にはできないといった運用上の問題も出てくることになる. つまり,「これ代わりに君がやっておいて」といった意味合いの処理がすぐに出来ないという問題である. 秘書等への権限移譲の仕組みは,他大学でも検討・実装事例は報告があるが,やはり事前準備の手間と時間はかかる.

本稿の検討では,認証された個人間で,特定の高コンテンツに対してアクセス可能な物理的なセキュリティ情報を付加して認可強化することを考える. 例えば,事務部署内で共有のセキュリティトークンや証明書を共有して利用する運用となる. これは,通常の個人認証および属性認可された後で追加して使うものであり,これがないと認証および属性認可された後でも使えないようなリソースへ適用する. (図1に示す.)

したがって,本物理的なセキュリティ情報には個人に関連する情報は含まれないが,これがないとリソースへのアクセスができない. また,事前に属性テーブルを管理する手間を軽減できる(無論,本物理的なセキュリティ情報自体を管理する手間は必要である).

この仕組みは,従来の ID+パスワードでの利用で可能なオンラインリソースに対しては,通常の Shibboleth による認証認可のみでよく,特定の部署のみが利用するようなシステムも Shibboleth 化する必要があるようなケースでの適用を考えている. なお,本枠組みそのものは,多要素認証を要するような認証強度を高める要請への対応も可能である. 実際の物理的なセキュリティとしては,運用に応じて,例えば USB トークン,学生証,職員証,証明証入り IC カードなどから検討する.

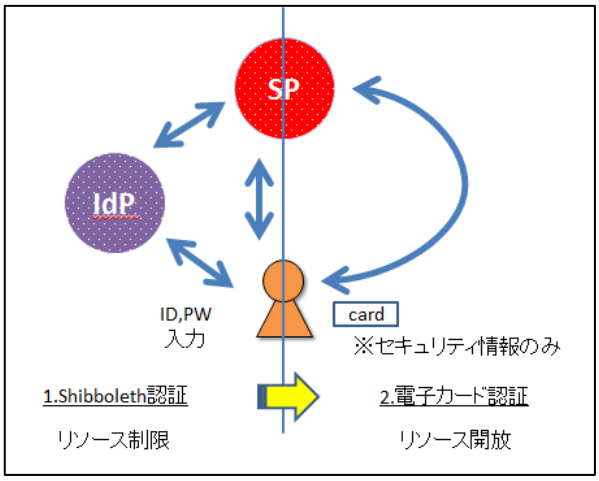

図1 認可制御の多段化
Fig1. Flexible Secure-Authorization of Permission

4. まとめ

本稿では, Shibboleth 認証におけるセキュリティレベルの多重化について述べた. SSO のフラットな認証連携に, 個人属性とは別のセキュリティ情報を用いた多段認可を追加することで, より高いセキュリティ,柔軟な認可環境の提供が可能となる. 実際の運用上は,高コンテンツ毎に個別の物理的な追加セキュリティ情報が必要では利用者に不便であり,紛失時のリスクも高くなる. このため, 今後は単独の物理セキュリティにより複数のコンテンツに対応できる様に設計する必要がある.

参考文献

[1]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

[2]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)

[3]金西計英, 松浦 健二, 三好 康夫,高木 知弘,嵯峨山 和美,矢野 米雄 「大学間 WEB サービス連携のための Shibboleth を用いた認可管理機能の実現」, 日本教育工学会論文誌,32(Suppl), 93-96, 2008

Copyright ©2013 Information Processing Society of Japan.
All Rights Reserved.