サイエンティフィック・システム研究会
システム技術分科会 2008 年度第 2 回会合資料

2009 年 1 月 29 日

私は誰？ － 組織，そしてサービスから見た認証と UPKI －

京都大学学術情報メディアセンター
岡部 寿男
okabe@i.kyoto-u.ac.jp

[Abstract]

組織における認証・認可の課題を、大学における認証システムの構築に絡めて考察する。まず「誰を認証すべきか」の視点から、大学が情報システムの利用者として扱う必要のある対象を分類し、それぞれに対するアカウント発行時の身元確認や失効の手順について、セキュリティポリシーとからめて概説する。次に NII による SSL サーバ証明書発行プロジェクトを例に、サーバの認証におけるサーバ管理者の実在性、本人性、管理責任の確認について紹介する。一方、「私は誰？」、すなわち利用者がどういう立場で情報システムを扱おうとしているかの観点から、認証と権限管理の分離の必要性について述べ、京都大学における統合認証システムの運用の状況と権限委譲の試みについて紹介する。最後に、組織をまたがる認証として、大学間連携のための全国共同電子認証基盤(UPKI)構築事業におけるプロジェクトの一つとして進めている UPKI 認証連携基盤の取り組みと実証実験の状況について述べ、組織間の認証連携(federation)の仕組みと、「私は誰？」かどこまで明らかにしてよいかなど組織間のプライバシー保護の課題についても考察する。

[Keyword]

認証・認可、認証連携、権限委譲、SSO、Shibboleth、UPKI、アカウント管理、サーバ証明書、セキュリティポリシー

1 誰を認証すべきか － アカウント管理の課題 －

政府機関の情報セキュリティ対策のための統一基準[1]においては、認証(統一基準の用語では主体認証)を「識別コード(ユーザ ID)を提示した主体が識別コードを付与された主体か否かを検証」することと定義している[1]。すなわち認証の問題とは、誰に識別コード(ユーザ ID)を付与するか(すなわち「誰を認証すべきか」)と、どのように識別コードと主体認証情報(パスワード, IC カードなど)を付与するか(すなわち「どうやって、なにを使って認証するか」)の設計が肝である。識別コードと主体認証情報の付与が適切に行えれば、どのように提示した主体が本物かを検証するところはある程度機械的に行える。

誰を認証すべきかについて、国立情報学研究所国立大学法人等における情報セキュリティポリシー策定作業部会と電子情報通信学会ネットワーク運用ガイドライン検討 WG による高等教育機関の情報セキュリティ対策のためのサンプル規程集[2]では、「A2101 情報システム運用・管理規程」において、利用者、教職員、臨時利用者の三つに分類している。しかしながら大学で正規の身分を持つ人以外にもアカウントを発行しなければならない実態があり、対象を確定するだけでも容易ではない。さらにどうやって、なにを使って認証するかについても、そのような非正規のユーザは実在性と本人性の確認すら自明ではなく運用上の苦労が多い。

特筆すべきこととして、グリッドにおけるユーザ証明書の発行を MICS プロファイル[3]に基づいて既存の学内認証基盤と連携して行う[4]場合には、学内認証基盤側のアカウント発行において対面認証が義務付けられている(should)ことである。一般に全学的な認証基盤においてグリッドを利用するユーザはごく少数と考えられ、グリッドのためだけに全ユーザに対してアカウント発行に対面認証を導入するのは現実的ではないが、対面認証を行ったかどうかの証跡を残すようにすれば対面認証済みのユーザにだけグリッド証明書をオンライン発行するようなしくみは可能である。

---

1 これに対し高等教育機関の情報セキュリティ対策のためのサンプル規程[2]では「A2101 情報システム運用・管理規程」において主体認証を「識別符号(ユーザ ID)を提示した利用者等又は電子計算機が、情報システムにアクセスする正当な権限を有するか否かを検証することをいう。」としているが、これは認証と認可を区別しておらず用語法として適切ではない。

2 サーバの認証と SSL サーバ証明書

国立情報学研究所が７大学の全国共同利用情報基盤センターと共同で進めている大学間連携のための全国共同電子認証基盤(UPKI)構築事業では、サーバ証明書発行・導入における啓発・評価研究プロジェクトとして、WebTrust for CA 認定ルート認証局の下位認証局を実際に構築し、その運用と参加機関への SSL サーバ証明書発行を通じて、大学においてサーバ証明書を普及していく上で必要となる課題の整理と解決を図っているところである[5]。

サーバ証明書を価格面でも人的コストの点でも低コストに提供するためには、申請者の実在性および本人性、当該サーバの実在性とその管理責任を申請者が本当に持っているかの確認を効率化することが必要である。UPKI ではこの業務を将来は UPKI の認証基盤を用いて自動化することを念頭に、審査に関する業務をプロジェクト参加機関たる大学側に委託している。各大学での実装はすでに名古屋大学[6]、東京大学[7]などの例が報告されているが、ここでは京都大学の例を取り上げる[8]。

京都大学では平成 15 年より学内 LAN である KUINS において負担金制を導入しており、グローバルアドレスを用いる KUINS-II のサービスにおいては、DHCP を用いず固定 IP アドレスのサービスとし、IP アドレスごとに管理責任者(教職員)が一意に対応付けられている。そこで KUINS の管理のためのデータベースと連携して、当該サーバの管理責任者からのオンライン申請により申請者の実在性・本人性、サーバの実在性ならびに管理責任を確認する枠組みを設計し実装した。Web による簡単な申請フォームに必要な項目を入力することで申請ができる。また教職員対象の全学グループウェアと認証連携しシングルサインオンも実現している。

同種の大学向けサーバ証明書発行はヨーロッパにおいても TERENA[2]を中心に我々より１年先行して行われているが[9]、発行業務の自動化については我々の方が積極的に取り組んでおり、情報交換と連携の可能性の検討を行っているところである。

3 京都大学における認証基盤の構築–SSO と権限委譲

京都大学では、学術情報メディアセンターの永井靖浩教授を中心に、全学認証基盤を構築中である。これは教職員系、学生系、教育研究コミュニティ系の三系統から構成される。また平成 22 年春に職員証および学生証を IC カード化すべく準備を進めている。シングルサインオンに関しては、全学グループウェアを中核に IBM Tivoli Access Manager で構成される事務系 SSO と、それを包含する形で構築を進めている Shibboleth 2.0 による SAML ベースの SSO との二層構造になっている。

さてこのようにシングルサインオンと ID の名寄せを推進すると、これまで実態としてあった ID の貸し借りによる代理入力や役職 ID による「認可」の対処が難しくなる。そこで SSO 環境で電子証明書を利用しての権限委譲による「認可」処理(代理入力)の方式を永井らが提案し[10]、本学でも利用を検討している。

4 UPKI 認証連携基盤(UPKI-Fed) シングルサインオン実証実験

UPKI プロジェクトでは、電子ジャーナル等で用いられている Shibboleth の技術を利用して、電子ジャーナル利用、グリッドコンピュータ利用、無線 LAN 利用時の本人確認等を可能とする「UPKI 認証連携基盤」の構築を進めている。この実証のため，複数の大学等機関が IdP と呼ばれる認証サーバを構築し、技術的および制度的な検証を行うための実証実験を行っている[11]。

Shibboleth では、IdP(Identity Provider)がユーザの属性を管理する。ユーザは SP(Service Provider)からサービスを受けるにあたってまず IdP にリダイレクトされ、そこで認証されて SAML(Security Assertion Markup Language)で書かれた認証アサーションを受け取る。それを認証チケットとして SP にアクセスする。サービスの利用に際して認可の判断にユーザの属性が必要になった場合には、IdP と SP との間で属性交換がなされる。

Shibboleth/SAML 型の認証連携では IdP はユーザが SP からどのようなサービスを受けているか直接は知らない。また属性交換が不要なサービスについてはユーザがどこの SP にアクセスしているかも IdP にはわからない。このように、IdP はユーザの認証に責任を持つにもかかわらず、ユーザにとっては IdP に「私がどこにいるか、どこで何をしているか」を隠すことができる。

---

2 http://www.terena.org

一方、認証チケットに実名をいれず仮名を用いることにより、SP はユーザがどの IdP に所属するかはわかるものの誰であるかまでは知りえない。仮名を使い分けることで複数の SP が結託し名寄せすることも防げる。これにより、意図しない形でプライバシー情報が漏出するような事故を防止することができる。すなわち「私は誰か」を、真に必要な時以外は明らかにしないでサービスを受けられる。

5 まとめ

大学における認証と、組織をまたいでの認証から認証連携への流れについて述。各大学できっちりとした認証基盤を構築するとともに、それらを連携させて組織間で積極的に信頼関係を築くとともに、不必要な個人情報をやりとりをしないよう配慮することで、組織の壁を越えたサービスの提供をプライバシー保護と両立する形で実現できるのではないかと考え、その基盤としての UPKI を今後も推進していく所存である。関係各位のご理解とご支援をお願いする。

謝辞 日頃からご議論くださる国立情報学研究所ネットワーク運営・連携本部認証作業部会ならびに同大学学術ネットワーク研究開発センター認証基盤グループの各位に感謝する。

参考文献

[1] 情報セキュリティ対策会議: 政府機関の情報セキュリティ対策のための統一基準（第３版）, http://www.nisc.go.jp/active/general/kijun01.html (2008).

[2] 国立情報学研究所国立大学法人等における情報セキュリティポリシー策定作業部会, 電子情報通信学会ネットワーク運用ガイドライン検討 WG: 高等教育機関の情報セキュリティ対策のためのサンプル規程集 (2007 年度版), http://www.nii.ac.jp/csi/sp/ (2007).

[3] The Americas Grid Policy Management Authority: Profile for Member Integrated X.509 Credential Services (MICS) with Secured Infrastructure Version 1.0, IGTF-AP-MICS-1.0.pdf, http://www.tagpma.org/node/38 (2007).

[4] Kento Aida: Cyber Science Infrastructure and Grid Operation, Middleware Workship in 25th APAN Meeting Hawaii (2008).

[5] 島岡政基, 谷本茂明, 片岡俊幸, 中村素典, 曽根原登, 岡部寿男: UPKI プロジェクトにおけるオープンドメインサーバ証明書発行・導入, 電子情報通信学会 2008 年総合大会 BS-8-2 (2008).

[6] 平野靖, 内藤久資: UPKI イニシアティブ『サーバ証明書発行・導入における啓発・評価研究プロジェクト』と名古屋大学における事例, 名古屋大学情報連携基盤センターニュース Vol.6 No.4 (2007).

[7] 西村健, 佐藤周行: 東京大学におけるサーバ証明書発行体制の構築と課題, 情報処理学会研究報告 No.2008-DSM-048, pp.79-84 (2008).

[8] 京都大学情報環境機構 KUINS 運用委員会, 国立情報学研究所サーバ証明書プロジェクトによる SSL サーバ証明書の発行について, KUINS ニュース No.57 (2007).

[9] J. Meijer: Community SSL/TLS Server Certificate, Middleware Workship in 25th APAN Meeting Hawaii (2008).

[10] 古村隆明, 永井靖浩, 橋本正一, 青柳真紀子, 高橋健司: 電子証明書を利用した権限委譲方式の提案, 電子情報通信学会 2008 講演論文集, D-9-12 (2008).

[11] 片岡俊幸: 実証実験の状況とフェデレーション(UPKI-Fed) 構築について, UPKI イニシアティブシングルサインオン実証実験中間報告会資料集 https://upki-portal.nii.ac.jp/item/idata/odatao/SSO_mid_session_ref/ (2008).