

要認証サイトのマッシュアップについての考察

阿部, 英司
九州大学システム情報科学研究府 : 修士

伊東, 栄典
九州大学情報基盤研究開発センター : 准教授 : 情報学

笠原, 義晃
九州大学情報基盤研究開発センター : 助教 : 情報学

<https://hdl.handle.net/2324/15957>

出版情報 : 第62回電気関係学会九州支部連合大会, 2009-09
バージョン :
権利関係 :

要認証サイトのマッシュアップについての考察

阿部英司* 伊東栄典** 笠原義晃**

*九州大学システム情報科学府情報理学専攻 〒812-8581 福岡市東区箱崎 6-10-1

**九州大学情報基盤研究開発センター 〒812-8581 福岡市東区箱崎 6-10-1

1. はじめに

近年情報サービスの増大に伴い、複数サービスの情報を組み合わせ新しいサービスを構築するマッシュアップが行われるようになった。例えば自分に関係のある複数サイトの情報を1つのサイトで閲覧できるポータルサイトなどが公開されている。認証を必要としないサービスから公開情報を取得することは容易であるが、要認証サービスから利用者に関するプライバシー情報などを取得する場合は認証処理が問題となる。

利用者の認証処理の煩雑さを軽減するために、一度の認証で複数のサービスを利用可能にする SSO (Single Sign-On) が研究開発されており、異なる組織間においても SAML[1], Shibboleth[2]などの分散 SSO が提案および実装されている。共通の認証基盤を用いることで、要認証サービスからの情報取得やサービスの相互提供も可能となる。そこで、要認証サービスからの情報を取得する具体的な方法が求められている。

我々はサービス連携のための組織間認証連携についての研究を行ってきた[3][4]。我々はマッシュアップサービスとしてポータルサイトを想定しており、本稿では我々が検討している分散 SSO の仕組みを利用した異なる組織間のサービスをマッシュアップする仕組みや試作システムについて述べる。

2. マッシュアップに関する考察

青柳ら[5]は要認証サイトから情報を取得する方法として、利用者がマッシュアップサイトを仲介し認証処理を行うことで、マッシュアップサービスが要認証サービスから利用者の情報を取得する方法を検討している。前提として、マッシュアップサイトは信頼できる組織が運営し利用者情報を不正に扱うことはない。彼女らの手法では認証処理を行うためにページを複数回リダイレクトする必要がある。我々は、利用者がマッシュアップサービスに ID・パスワードなどの利用者情報を渡すことで、マッシュアップサービスが自動的に認証処理を行い、要認証サービスから情報を取得する方法を検討している。我々の手法は実装が簡単であり、ページのリダイレクトが必要ではないため、利用者にとってより利便性の高い方法といえる。我々が検討しているマッシュアップサービスの概念図を図 1 に示す。



図 1 マッシュアップサービスの仕組み

3. 試作システムおよび評価

試作システムでは Shibboleth 認証を必要とする複数サービスから情報を取得し、1つの画面に表示するサイトを構築した。利用者はサービス利用開始時に自分の Shibboleth ID とパスワードをマッシュアップサイトの入力フォームに入力する。マッシュアップサービスは HTTP ユーザエージェントインスタンスを作成し要認証サービスで認証を行い、ページの情報を取得し、利用者へマッシュアップサービスを提供することができた。試作システム的环境を表 1 に示す。

表 1 試作環境

OS	FreeBSD 7.0
Web Server	Apache 2.2
Programming	Ruby 1.8
HTTP User Agent	Mechanize 0.8

試作システムにおけるマッシュアップページを表示するまでの処理速度は平均して 3 秒程度であり、実用化のためには処理時間の短縮が必要である。また、Ruby で作成した HTTP ユーザエージェントは JavaScript を処理できないという問題も発生した。これら問題は JavaScript で HTTP ユーザエージェントを作成することによって改善が可能なのであると考えている。

4. まとめ

本稿では我々が検討している要認証サービスのマッシュアップ機構について述べた。今後の計画として九州大学と同じ認証基盤の Shibboleth IdP 構築し、九州大学用の Google Apps を Shibboleth 認証対応とする。iTunes U, YouTube, SNS, 就職活動サイトなどの要認証サービスの情報を取得できる Google ガジェットを作成し、九州大学用のポータルを構築する。研究成果や開発システムの公開と、具体的なマッシュアップサービスを実現していきたい。

5. 参考文献

- [1] John Kemp, Security Assertion Markup Language.(SAML, 15 March 2005, <http://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf>)
- [2] The Shibboleth project (2000), <http://shibboleth2.edu/>.
- [3] 阿部 英司, 伊東 栄典, “PKI 手法を用いた組織間での利用者認証連携についての検討”, 電子情報通信学会第 19 回データ工学ワークショップ (DEWS 2008), C1-6, Mar. 2008.
- [4] 阿部 英司, 伊東 栄典, 笠原 義晃, 中國 真教, “認証つきサービスにおける組織間連携のための PKI と OpenID の融合”, 情報処理学会第二回インターネットと運用技術研究会 (情処研報 IOT-2-2008), pp.17-22, Jul. 2008.
- [5] 青柳 真紀子, 岡本 学, 下村 道夫, “Web サービスマッシュアップにおける認証方式に関する一考察”, 暗号と情報セキュリティシンポジウム, 4DI-4, 2009.