様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　２９　年　　４　月　２６　日現在

機関番号：　１５３０１
研究種目：　基盤研究(C)（一般）
研究期間：　2014～2016
課題番号：　２６３３０１５８

研究課題名（和文）ユーザおよびサービス毎に認証機構をカスタマイズ可能な統合認証システムの開発

研究課題名（英文）Development of Integrated Authentication System Allowing Users and Services to Customize Its Authentication Mechanism

研究代表者

河野　圭太（Kawano, Keita）

岡山大学・情報統括センター・准教授

研究者番号：４０３９７８９９

交付決定額（研究期間全体）：（直接経費）　　1,600,000円

研究成果の概要（和文）：様々なシステムの認証を1つの認証サーバで行う統合認証環境では、利用する認証方式をユーザやサービスの特徴を考慮して選択することにより、安全かつ便利な認証連携を実現できる。我々は、大学等の学術機関において多数の導入実績があったShibboleth IdP V2に対して、認証方式のグループ化機能を組み込むことにより、これを実現するシステムを提案し、プロトタイプを作成した。また、研究途中にリリースされたShibboleth IdP V3に対しても同様の検討を行い、外部システムとの連携をうまく機能させることで、効率的にこれを実現するシステムを提案し、本学の統合認証システムに導入した。

研究成果の概要（英文）：In an integrated authentication environment where authentication for a variety of systems is enforced using a single authentication server, selecting authentication methods in consideration of users and services characteristics enables a secure and convenient federated authentication. We proposed a system that enables such feature by incorporating a grouping function of authentication methods into Shibboleth IdP V2, widely deployed at academic institutions like universities, and developed its prototype. We also conducted similar consideration for Shibboleth IdP V3, released during the research period. As a result, we proposed a system that enables that feature efficiently, and introduced it into the integrated authentication system of our university.

研究分野：　計算機システム・ネットワーク

キーワード：　認証　統合認証　Shibboleth

１．研究開始当初の背景

統合認証環境（信頼できるいつものサーバによる一度の認証で、複数のサービスを利用できる環境）は、ユーザへ利便性を提供する一方で、パスワード等の認証情報の漏えいによる被害の範囲を拡大させる諸刃の剣となり得る。この問題を解決するためには、従来の認証システムと同様、スマートカード認証やバイオメトリクス認証等、強固な認証方式の採用による、システムへの入り口対策が有用である。

しかしながら、これらの認証方式には、ID・パスワード認証のような記憶に基づく認証方式とは異なり、特別なデバイスを必要とするものが多く、ユーザの利便性の面からは望ましいとは言い難い。実際、研究代表者の所属組織（岡山大学情報統括センター）で運用している統合認証システムにおいても、ユーザの利便性を優先した結果、単純なID・パスワード認証のみが採用されており、サービスの拡大とともに、安全性向上へ向けた対策が課題となっていた。

ここで、多様なユーザが多様なサービスを利用する統合認証環境では、それぞれのユーザやサービスが許容できる制限やリスクもそれぞれに異なる。研究開始当初、身元保証レベル（Level of Assurance：LoA）という概念に基づき、アクセスする情報資産の保護レベルに応じて利用する認証方式を選択する方法が確立されつつあったが、特に大学等の学術機関における統合認証システムとして国際的にも広く採用されているShibbolethでは、これに対する十分な実装がなされておらず、実用上の課題が多く残されていた。

２．研究の目的

本研究では、LoAの概念に基づくユーザ毎、サービス毎の認証方式選択に関して、実運用を深く考慮したシステム開発を行い、実用化に向けた課題の整理とその解決を図ることをその目的とした。また、研究の成果を、更改時期を控えた岡山大学の統合認証システムに適用することも検討した。

（１）研究開始当初、Shibbolethのバージョンは V2 であったため、これを想定した研究開発を行った。

まず、サービス毎に認証方式を選択する機能については、サービス（Service Provider：SP）からの認証要求に、そのサービスの管理者が許容する認証方式のリストを含めることで、それを実現する簡易な実装がなされていた。しかしながら、当時の実装では、単一の認証サーバ（Identity Provider：IdP）において、同種の認証方式が複数提供されることは想定されておらず、また、上位レベルの認証方式で認証した結果を、下位レベルの認証方式に対する応答（認証結果）として再利用することができなかった。そのため、IdP・SP間で、事前にIdPが提供する認証方式のリストを共有しておくことが求められ、異なる組織間での認証連携を実現する認証フェデレーションにおいては、現実的とは言えなかった。

これらの課題を解決するため、本研究では、IdP における認証方式のグループ化機能を開発し、異なる組織間での事前の情報共有を必要最低限に抑えることを目指した。

（２）研究途中に Shibboleth のバージョンが V2 から V3 へと変更され、機能面でも大幅な変更があった。岡山大学の統合認証システムの更改にあたっては、Shibboleth IdP V3 を利用することが求められたため、以降の開発および研究成果の適用にあたって、Shibboleth IdP V3 における対応を検討することにした。

Shibboleth IdP V3 では、Shibboleth IdP V2 とは異なり、一つの認証方式に複数の認証コンテキストを紐づけることや、一つの認証コンテキストを複数の認証方式に紐づけることが可能になった。このため、サービス毎に認証方式を選択する方法については、標準機能で実施可能となった。

しかしながら、Shibboleth IdP では、既に組み込まれている認証方式が少なく、我々が利用しようとしたワンタイムパスワード認証に対する実装がないことや、学内・学外からのアクセスの別により、要求する認証レベルを変更する実装がないことが課題となった。この対応として、Shibboleth IdP V3 の機能を拡張することも検討したが、リリース直後で情報も不足し、頻繁なシステム変更も予想される状況で、過度にシステムの機能に依存することはリスクが高いと判断した。

そこで、Shibboleth IdP V3 の標準機能と外部システムの機能をうまく組み合わせ、目的を達成するシステムを構築することとした。

３．研究の方法

（１）IdP で同種の認証方式を提供することを考慮した場合、複数の組織が連携する認証フェデレーション環境では、各 IdP で提供されている認証方式とその LoA すべてを SP 管理者が事前に把握しておく必要があった。この制限をなくすため、本研究では、IdP で提供する認証方式をグループ化し、SP が IdP への認証要求に含める許容認証方式をグループ形式で指定できる機能を開発した。

具体的には、SP からリダイレクトされた認証要求に対して、LoA 等に対応するグループ形式で指定された SP が要求する認証方式を、当該 IdP で提供されている個別認証方式へと変換する機能、IdP から SP へ返却する認証応答における個別認証方式の記載を、グループ形式へと逆変換する機能を開発した。このような開発方法の採用により、従来の機能によるシングルサインオンの実現を保ったまま、

認証方式のグループ化を実現した。
　また、本研究では、実運用開始後のメンテナンス性を考慮し、Tomcat のフィルタ機能を用いてこれらの機能を実装した。Shibboleth IdP のソースとは独立させ、フィルタとして実装することにより、IdP のバージョンアップ作業時等に影響を及ぼしにくい構成とした。
　本機能の実現に向けて、認証方式の形式変換を実行するタイミングが課題となった。認証連携にあたっては、IdP・SP 間で複数のメッセージがやり取りされるため、形式変換のタイミングによっては、既存の Shibboleth IdP が提供するシングルサインオン機能が正しく働かなくなる可能性があった。そこで、Shibboleth IdP における認証処理のシーケンスを分析し、新たな機能を挿入しやすく、既存の機能を阻害しないタイミングを特定し、実装を行った。

（2）統合認証システムの更改にあたり、学内において、レベル 1：常に ID・パスワード認証のみ、レベル 2：学外からは追加の認証を必須、レベル 3：学内からも追加の認証を必須、の 3 レベルを規定し、ユーザおよびサービス毎にレベルを選択できることを要件とした。
　この実現にあたり、OpenAM の認証モジュールおよび認証連鎖の機能を使うことで、研究の目的で記述した問題を解決することにした。そこで、Shibboleth IdP に OpenAM のエージェントを導入し、Shibboleth IdP の認証を OpenAM で実施することを検討したが、単純な方法では Shibboleth IdP と連携するサービス群が一つの巨大なサービスとして見えてしまい、サービス毎に認証レベルを選択する運用ができないことが課題となった。
　そこで、Shibboleth IdP において RemoteUser ログインフローを認証レベル毎に用意し、OpenAM 側では接続元 IP アドレスと対象 URL によって制御を変更するようにした。さらに、これらのログインフロー毎に異なる AuthnContextClassRef を定義し、サービス側の設定で要求する認証レベルを変更できるようにした。
　また、ユーザ毎の認証レベルを変更するにあたり、OpenAM のアダプティブリスク認証を活用することにした。アダプティブリスク認証では、LDAP 上の特定の値に基づいて、認証の状態を変更する機能があるため、LDAP 上に「利用者が常にレベル 2 以上の認証を要求するかどうか」を示す属性を用意し、「要求する」場合にはワンタイムパスワード認証を追加で求めるようにした。

４．研究成果

（1）従来の方法では、SP 側で、それぞれの IdP で提供している全認証方式とその LoA を把握し、要求するレベル以上の LoA を有する全認証方式を認証要求に含める必要があった。一方で、本研究では、事前に合意された LoA（グループ形式）に基づく認証方式の要求ができるため、SP 側で、それぞれの IdP で提供されている個別認証方式を把握する必要がない。このように、異なる組織の IdP・SP 間での事前の情報共有を最小限とすることにより、実用的なレベルでの運用を可能とする仕組みを開発した。
　研究の方法で述べたように、従来の認証機能において個別認証方式の形式による処理を保つことにより、個別認証方式の形式による指定と併用する場合や、複数のグループに所属する認証方式が存在する場合にも、厳密なシングルサインオンを提供できるようになった。例えば、所属する認証フェデレーション内の LoA1 を有する認証方式としてスマートカード認証による利用者の認証を実施した後、自組織内の LoA2 を有する認証方式としてスマートカード認証を要求する場合にも、既に実施済みのスマートカード認証により、実際の認証を省略することができた。
　また、一般的に利用されている Shibboleth SP の実装を用いて認証方式の選択を要求する場合には、認証応答に含まれる利用した認証方式が、本来要求した認証方式と同じものであるかどうかを確認する設定が必要となることが分かったため、これらの運用上の注意点についても整理し、論文中に示した。
　さらに、本研究で開発した認証要求内の認証方式変換機能を、岡山大学の統合認証システムに実際に組み込んだ。本研究の期間中に、岡山大学の事務情報システムが更改され、多要素認証の導入が行われたが、Shibboleth で認証連携する SP が巨大な一つの SP として扱われてしまい、個別に多要素認証を設定することができなかった。そこで、本研究の成果を応用し、特定サブネットからの特定 SP に対する認証要求内の認証方式の書き換えを行うことにより、目的を果たすシステムを構築できた。

（2）本研究では、研究の方法で示したような方法で、岡山大学の統合認証システムに、ユーザおよびサービス毎に認証機構をカスタマイズできる機能を取り込んだ。
　本研究の成果により、実環境において、サービスの管理者が 3 レベルから成る認証のレベルを選択し、ユーザに適用される認証方式を選択できるようになった。また、岡山大学の認証情報を統合的に管理している統合認証管理システムにおいて、「常にレベル 2 以上の認証を要求して欲しいがどうか」をユーザが制御できる機能を用意し、それを LDAP に反映させる機能を提供することで、前述の仕組みにより、ユーザが自身の認証レベルを選択できるようになった。
　岡山大学では、VPN システムの更改に伴い、学外・学内からの別に関わらず多要素認証（従来の ID・パスワード認証に加えて、電子メールまたはモバイルアプリケーションを

利用したワンタイムパスワード認証を追加）を必須とするような運用を始めたが、本研究の成果を活用することにより、スムーズな導入が実現できた。LoA に基づく認証方式選択の実用化を目的として実施した本研究において、このように研究の成果が実際のシステム運用につながったことは、大きな成果であると考えている。

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計１件）

① 河野 圭太、中村 素典、Shibboleth における認証フェデレーションのための認証方式グループ化機能の開発、情報処理学会論文誌、査読有、Vol.57、No.3、2016、pp.1008－1021、
http://id.nii.ac.jp/1001/00158110/

〔学会発表〕（計５件）

① 河野 圭太、稗田 隆、中村 素典、Shibboleth と OpenAM の連携による認証レベルを考慮した統合認証システムの構築、大学 ICT 推進協議会 2016 年度年次大会、2016 年 12 月 14 日、国立京都国際会館（京都府・京都市）
② 河野 圭太、OpenAM との連携による LoA を考慮した Shibboleth V3 の認証、大学 ICT 推進協議会 認証連携部会 2015 年度第 2 回部会、2016 年 3 月 16 日、熊本大学（熊本県・熊本市）
③ 河野 圭太、岡山大学事務情報システムにおける多要素認証の導入、大学 ICT 推進協議会 2014 年度年次大会、2014 年 12 月 10 日、AER（宮城県・仙台市）
④ 河野 圭太、藤原 崇起、稗田 隆、岡山大学事務情報システムにおける Shibboleth との連携を考慮した多要素認証の導入、情報処理学会 インターネットと運用技術研究会、2014 年 10 月 9 日、岩手県立大学アイーナキャンパス（岩手県・盛岡市）
⑤ 河野 圭太、中村 素典、Shibboleth IdP における LoA を考慮した認証方式グループ化機能の開発、情報処理学会 インターネットと運用技術研究会、2014 年 6 月 28 日、新潟大学五十嵐キャンパス（新潟県・新潟市）

６．研究組織
(1)研究代表者
河野　圭太（KAWANO, Keita）
岡山大学・情報統括センター・准教授
研究者番号：４０３９７８９９

(2)連携研究者
中村　素典（NAKAMURA, Motonori）
国立情報学研究所・学術基盤推進部・教授
研究者番号：３０２６８１５６