学認と学内統一認証の自動切替

Auto exchange of GakuNin and the unified authentication of a university

松澤英之，園田誠，黒木亘，　廿日出勇
Hideyuki Matsuzawa, Makoto Sonoda, Wataru Kuroki, Isamu Hatsukade

matuzawa@cc.miyazaki-u.ac.jp, sonoda@cc.miyazaki-u.ac.jp,
wata-k@cc.miyazaki-u.ac.jp,hatukade@cs.miyazaki-u.ac.jp

宮崎大学　情報基盤センター

University of Miyazaki, Information Technology Center

概要

学術認証フェデレーションに参加することで、大学の枠を超えて相互に認証連携を行う事が可能になり、大学や出版社等が提供する Web アプリケーションを利用できる。学認に参加している大学の多くは、学内統一認証 ID を学認 ID として利用しているが、宮崎大学では、セキュリティ及びシステム変更の際に掛かる経費及び労力を考慮して、学認 ID は、学内の統一認証 ID とは別の ID を利用することにした。そこで、現在学内統一認証で運用し、なおかつ学外者に簡単に提供できる学内 Web アプリケーションサービスである宮崎大学 Web ネットワーク認証を学認用のサービスプロバイダ(SP)化するシステムの開発を行った。宮崎大学では、学認と学内統一認証は独立して運用するので、現在運用している学内統一認証を用いた認証システムには極力影響を与えないように開発を行った。

キーワード

学認，学内統一認証，自動切替, Radius

1. はじめに

大学には研究用、教育用、事務用など多種多数なシステムがあり、各システムを利用する場合、利用者を特定する或は学外者の利用を制限するために認証が行われている。システム毎に別々の ID、パスワードを作って運用すると、利用者は、システム毎に ID、パスワードを覚えなければならないので、利便性を損なう。また、セキュリティ上、システム毎にパスワードを変えることが望ましいが、システムが多数存在する場合、利用者は非常に簡単な一つのパスワードを使いまわす傾向がある。一方、各システムの運用管理者は、各自で常にユーザデータベースを最新の状態に保つ必要があり、システムが増えるにつれ管理運用のための労力が増える。

そこで、まず一つの認証システムで学内ほぼすべてのシステムを認証できるように、統一認証システムを作ることが多い。それに加え、一回の認証ですべてのシステムの利用が可能になるように、シングルサインオン(SSO)を構築する場合もある。

いま大学内システムの認証について述べたが、これに

加え、別大学、或はクラウドのシステムを利用する場合でも、自組織が管理する一つの認証システムですべての大学或はクラウドのシステムが利用出来る様になれば、利用者と運用管理者の利便性とセキュリティの観点から非常に有益である。この大学の枠を超えた認証連携が学術認証フェデレーション(学認)である。学認に参加することで、大学や出版社等が提供するWebアプリケーションを利用できる。

本研究では、現在学内統一認証で運用し、なおかつ学外者に簡単に提供できる学内 Web アプリケーションサービスである宮崎大学 Web ネットワーク認証システムを学認用のサービスプロバイダ(SP)化するシステムの開発を行った。

2. 宮崎大学統一認証

宮崎大学では、学内統一認証ができる前は、2003 年 10 月に旧宮崎大学と宮崎医科大学が統合したことなど歴史的経緯から、学内に情報センター系、事務系、及び医学部系のシステムが存在していた。情報センター系システムを除いて、各システムはシステム毎に独自で認証を行っていた。年々全学で使うシステムが増えてきていたので、各認証システムを統合するよりも、新たに全学で利用できる認証システムを構築した方がよいという事となり、2009 年 4 月に LDAP システムを用いた宮崎大学統一認証が作られた。

統一認証を導入する当時、LDAP に簡単に対応できるシステムが多くなってきたこと。又、たまたま LDAP に対応できないシステムが近々に更新を迎えていたこともあり、2-3 年程度でほぼ全てのシステムが学内統一認証に移行することが出来た。これは、他大学の現状を見る限り非常に効率よく変更が出来た事例だと思われる。

この時の統一認証は学内にいる教職員、学生が学内システムを利用する場合を想定していた。

3. 学術認証フェデレーション(学認)

3.1. 概要

学認[1]は、大学の枠を超えて、学術e-リソースを利用する大学と学術e-リソースを提供する機関・出版社等がフェデレーションで定めた規程を信頼しあうことで相互に認証連携を実現している。この認証連携を利用して、SSOで学内だけでなく他大学や商用のサービスを利用出きる様になる。特に、学内電子ジャーナルを学外から閲覧する場合は、学認の認証を利用する事を求められることが多い。

3.2. システム

学認では、Shibboleth(SAML)を用いてSSOを実現している。学認システムは、Webアプリケーションリソースを提供するSP (Service Provider) 、認証を行うIdP(Id Provider)、及び多数のIdPから自分の所属する組織の認証を行うIdPを選択するためのDS (Discovery Service) からなる。IdPはバックグランドのデータベースとしてLDAPシステムを利用できる。そのため、学内統一認証によく用いられるLDAPサーバと比較的簡単に連携できる。

1. ユーザはブラウザを用いて利用したいSPにアクセスする
2. 最初に学認SPへアクセス時はIdPによって認証されていないので、認証を行う自組織のIdPを選択する為に、DSに転送される
3. DSの画面で自組織のIdPを選択すると、選択したIdPに転送される
4. 転送された自組織のIdPの画面で、IDとパスワードを入力する
5. IdPで認証を受けると、IdPとSP間で認証結果と認証された個人の属性情報のやり取りが行われる
6. ユーザはSPのサービスが利用出来る様になる。このときブラウザは、認証済みのcookieを受け取る

一度、認証を受けるとcookieによって認証情報が保存されるので、別のSPに接続した場合でも、ID、パスワードを入力せずにサービスを受けられるようになる。（図-1）

3.3. 利点

学認を利用する際に各大学が管理運用する必要最小限のシステムは、自組織に所属する人物を認証するためのIdPだけで、学内の統一認証システムを管理する場合と比べさほど大変ではない。

また、学内統一認証でよく利用されるLDAPサーバ(ShibbolethではIdPサーバに相当する)で認証を行う場合は、サービスを提供するWebアプリケーション(ShibbolethではSPサーバに相当する)にID、パスワードなどセキュアな情報を送り、Webアプリケーションサーバからサーバ(ShibbolethではIdPサーバに相当する)にID、パスワードなどセキュアな情報を転送して認証を受ける。これに比べて、Shibbolethは自組織のIdPにID、パスワードなどセキュアな情報を送って認証を受けた後、各SPに対して氏名、所属など利用する際に必要な属性情報のみを提供するので、学外のSPに対してパスワード、及び個人情報が漏洩する危険性が低くなる。

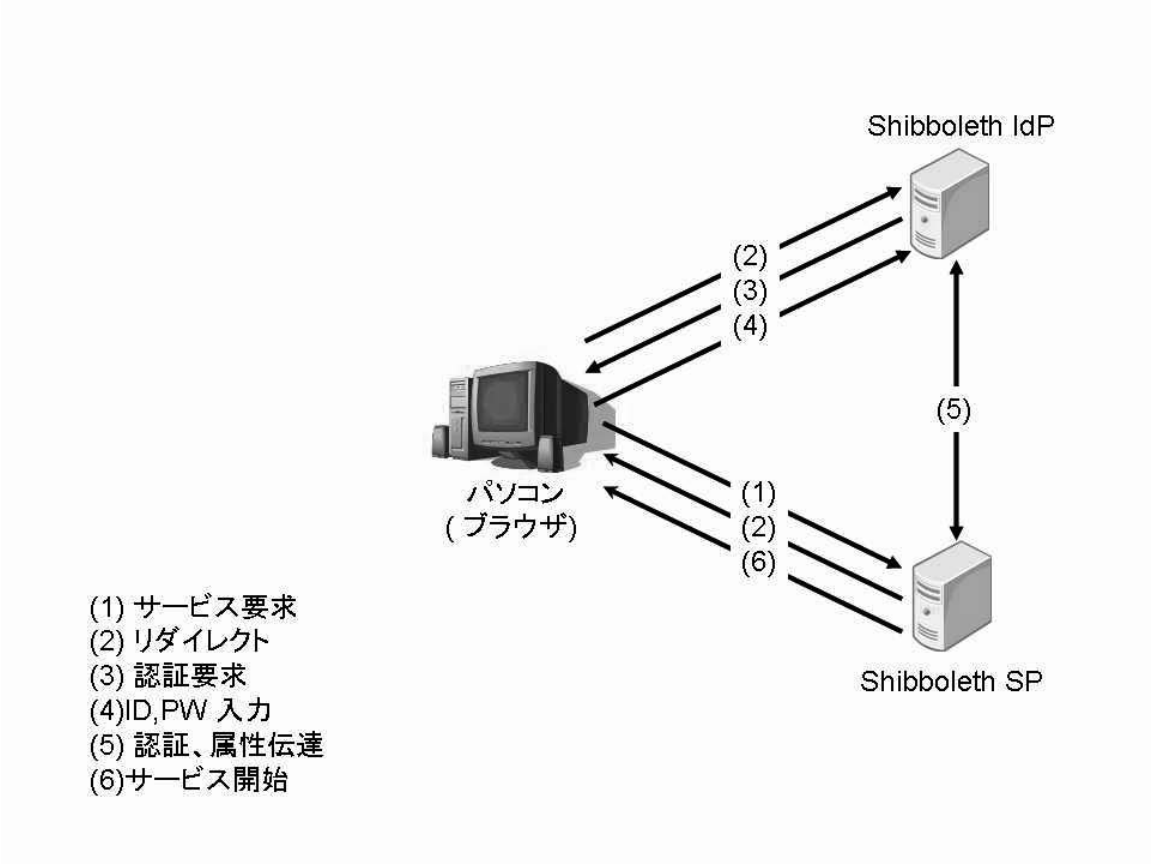

図-1 学術認証フェデレーション概念図(DS を除く)

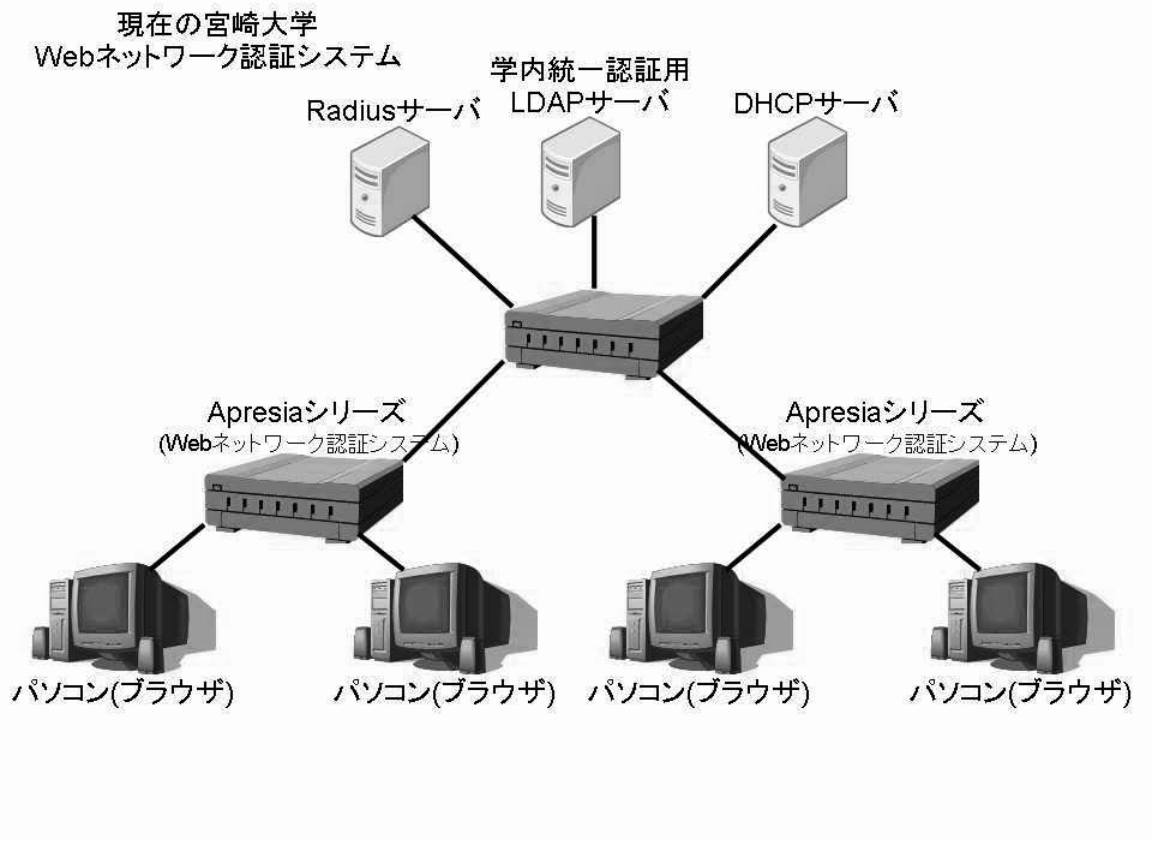

図-2 宮崎大学 Web ネットワーク認証システム

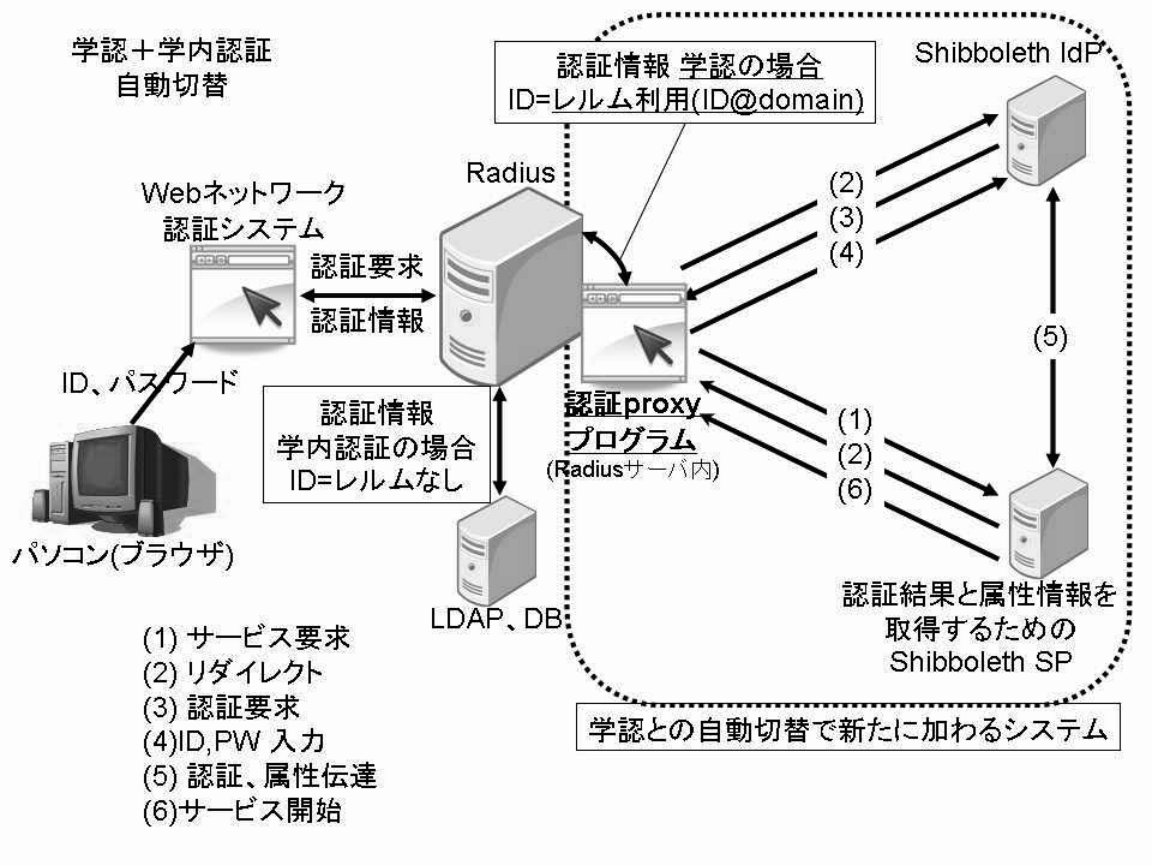

図-3 学認と宮崎大学統一認証の自動切替(DS を除く)

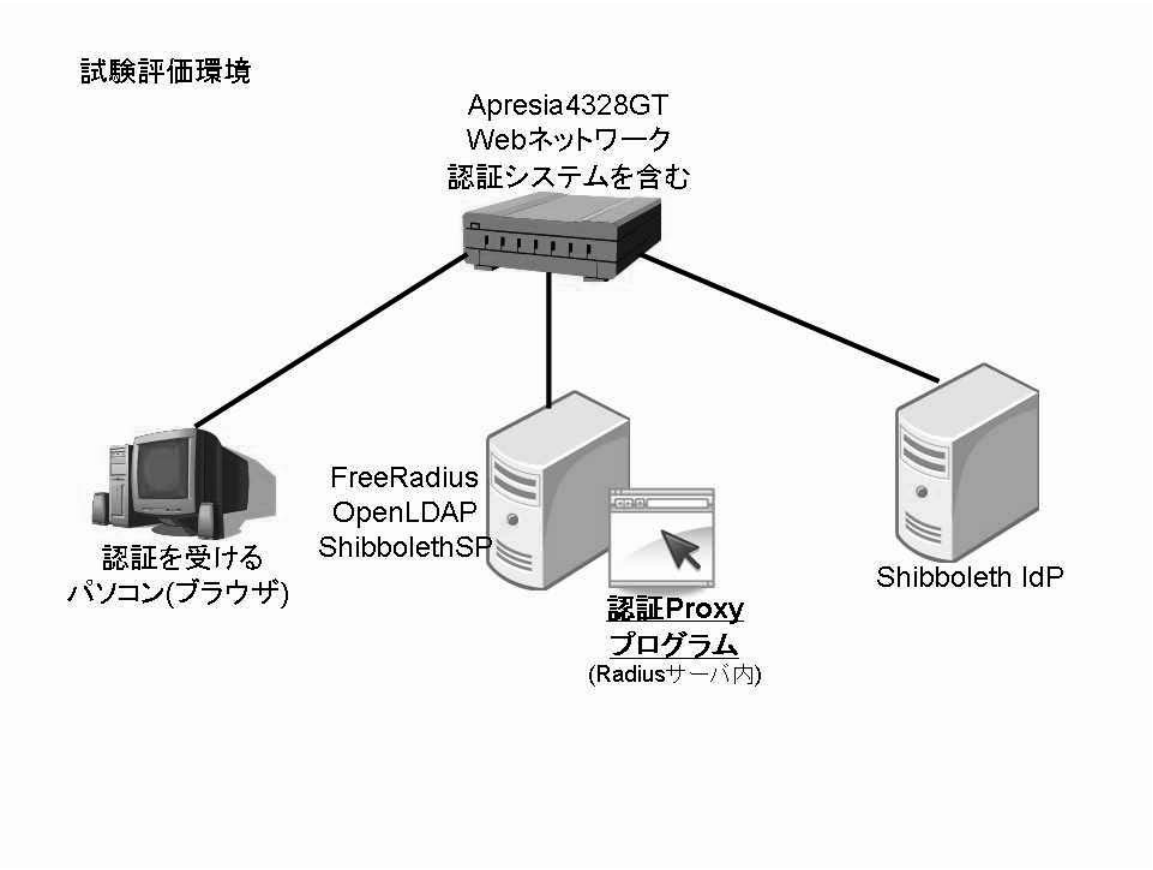

図-4 試験評価システム

学内統一認証システム(LDAPなど)単体では実現できないSSOを実現していることも利点として挙げられる。

3.4. 学認と宮崎大学統一認証

学認では、システム運用基準[2]で、認証を行う場合に自組織に所属している利用者のみを認証するように求めている。学認に参加している大学では、学内の統一認証IDを学認IDに使用している場合が多い[3][4]。また、統一認証によく利用されるLDAPシステム(Active Directoryサービスを含む)は学認認証用IdPシステムのバックグランドデータベースとして利用できるので、統一認証IDを学認IDとして利用することは自然である。しかし、宮崎大学では、以下の理由により学内統一認証IDとは別のIDを学認IDとして利用することにした。

1. 学内統一認証は主に学内からの利用を想定としている。電子ジャーナルの学外からの参照など、学認では、認証を行うIdPに学外から接続されることが予想される。学外から利用する場合、ホテルや空港など公共の場で提供されている安全でない可能性のある機器を利用したときにキーロガーによる情報流出等が想定されるため、現在の学内統一認証のセキュリティでは対応できない場合が想定される。学内統一認証を学外からの利用も想定したセキュリティレベルまで上げるためには、多大な経費がかかり現在では不可能である。
2. 学認では電子認証における保証レベル1を目指している[5]。今後もより高い安全基準を求められる可能性がある。学内統一認証IDを学認IDとして利用した場合、学認IDの保証レベルの上昇に伴い、学内統一認証のセキュリティレベルを上げることを求められる。しかし、学内事情から容易にセキュリティレベルを上げることが困難な場合も予想される。
3. 宮崎大学では、現在、SSOは実現されていない。将来、SSOを導入する時、学認IDに学内統一認証IDを利用していた場合、学認との連携を考慮してShibbolethで行うことが検討される。しかし、ShibbolethのSPに対応しているシステムは現在では少ないので、学内のSSOを実現するためには、多大な労力と経費が掛かる事が予想される。

4. 宮崎大学 Web ネットワーク認証システムにおける学認と学内統一認証の自動切替

4.1. 必要性

学内統一認証は一般に自組織に属する人物の認証を行う。しかし、ネットワーク利用時に学内統一認証で認証を行っている場合など、一時的に学外者にも提供できるIDを発行する必要に迫られる場合がある。

例えば、ネットワーク認証に学認を用いた場合、学外者の認証は学外者が所属する組織のIdPによって行われるので、臨時IDの発行等の管理業務が低減される。広島大学[6]や佐賀大学[7]は、学内の無線LANを学外者が利用する場合の認証に学認を利用している。しかし、学認で採用しているShibbolethのSAMLに対応しているシステムは少ないので、学内サービスを新たに学認SPとして公開する場合に、多大な経費と労力が発生する。また、宮崎大学の様に学内統一認証IDと学認IDが統一されていない場合、学内ユーザに対して学内統一認証以外の新しい学認IDの利用を呼び掛ける必要がある。学内ユーザは、新しいサービスが開始されたわけでもないのに、システムの認証が学認IDに変更になったことによって、新しいID、パスワードを覚える必要が出てくるなど利点は無い。

4.2. 宮崎大学 Web ネットワーク認証システム

宮崎大学のWebネットワーク認証は日立電線Apresiaシリーズのスイッチングハブによって行われている(図-2)。ネットワークに接続した際、パソコンからDHCPサーバへの接続要求が起きる。ネットワーク認証を行うスイッチングハブはDHCPサーバへの接続要求をリレーするので、パソコンはIPアドレス等の情報を得ることが出来る。しかし、まだ、認証は行われていないので、スイッチングハブから外のネットワークには接続できない。そこで、パソコン使用者は認証を行うためにWebブラウザを起動する。Webブラウザは起動時にブラウザに設定されているホームページへの接続を行う。認証スイッチングハブはこのhttp(https)要求をインターセプトして認証用ID、パスワードを入力する画面をブラウザに送信する。パソコン使用者はここで認証用のID、パスワードを入力すると、認証スイッチングハブはID、パスワードを外部のRadiusサーバに転送して認証を行う。認証スイッチングハブはRadiusサーバから送られた認証結果を基にネットワークへの接続の可否を決める。

4.3. Web ネットワーク認証システムの SP 化

既存のWebネットワーク認証システムを学認で認証する方法は、

１．Webアプリケーション自体をSP化する

２．SP化したリバースProxyを通してWebアプリケーションを認証する

方法が考えられる。佐賀大学では、１の方法すなわち既

存のSSOの入り口となる佐賀大学独自開発のWebネットワーク認証システムOpengateシステムをShibbolethに対応させた[7]。統一認証IDを学認IDとして利用した場合、どちらの方法でも利用可能である。

一方、統一認証IDと学認IDを分けた場合、WebアプリケーションをShibboleth SP化するとともに、統一認証用の認証システムと学認用の認証システムを自動的に判別して切り替える必要がある。宮崎大学のWebネットワーク認証システムはアプライアンスなので、ユーザがSP化することは困難である。一方、SP化したリバースProxyを利用する場合、統一認証で認証する場合はWebネットワーク認証システムに直接アクセスして認証を行い、学認で認証する場合はリバースProxy(SP)を通して認証を行うことが考えられる。しかし、Webネットワーク認証の場合、認証を受ける前はパソコンが認証システム以外には接続できないので、リバースProxy、DSや自組織の認証を行うIdPに接続して、認証を受けることが出来ない。そこで、３.Webアプリケーションが参照している外部の認証システムを利用して、統一認証と学認をシームレスに自動的に切り替える方法を提案する。

自動切替による認証は、Webネットワーク認証システムが参照する外部のRadiusサーバのレルムを利用して実現する。Webネットワーク認証システムは入力されたID、パスワードが統一認証用か学認用か判別する必要が無いので、アクセスするクライアントは、自動切替による認証の影響を受けない。

４．これ以外にも、eduroam仮名アカウント発行システム[8]の様に学認を用いてWebアプリケーションのアカウントを発行して利用することが出来る。しかし、この場合もWebネットワーク認証の前に、Webアプリケーションを利用するパソコン等がネットワークに接続出来ている必要があるので、宮崎大学のWebネットワーク認証システムには適さない。

4.4. システム概要

システム開発においては、Webネットワーク認証システムの変更を最小限に抑え、なおかつ学認SPとしてシステムを公開できることを目指した。

統一認証を行う場合、認証システムにLDAPを利用することが多いが、Radiusサーバを通して統一認証用LDAPサーバに接続、認証するシステムも多い。宮崎大学のWebネットワーク認証システムは外部のRadiusサーバを通して、学内統一認証LDAPサーバにアクセスし、認証を行っている。また、Radiusサーバは、レルム(例：ID@domain)を利用して認証を場合分けすることが出来る。本研究では、認証システムが参照するRadius のレルムを利用して、学認と学内統一認証の自動的な切替を行った。(図-3)

レルムを使わなかった場合は、従来通りにRadiusサーバを通して学内統一認証LDAPサーバにアクセスして認証を行う。

1. パソコンからブラウザを通してWebネットワーク認証システムにアクセスする
2. ブラウザ画面にID(レルムなし)、パスワードを入力する
3. ユーザが入力したID(レルムなし)、パスワードを受け取ったWebネットワーク認証システムは、認証を行うRadiusサーバにID、パスワードを転送する
4. Radiusサーバは受け取ったIDがレルムなしであることから、認証に学内統一認証を使うことを判断し、ID、パスワードをLDAPサーバに転送する。
5. LDAPサーバは、受け取ったID、パスワードから認証の可否を決定し、Radiusサーバに返答する
6. Radiusサーバは受け取った認証結果をWebネットワーク認証システムに返答する
7. Webネットワーク認証システムは認証結果を基にネットワークへの接続の可否を判断する。

一方、レルムが用いられた場合、RadiusサーバはWebネットワーク認証システムから渡されたID、パスワードをRadiusサーバにインストールされている外部プログラムに渡して認証を任せる。この外部プログラムが学認の各システムと通信して認証結果を得え、この認証結果をRadiusサーバに転送して認証を行う。つまり、この外部プログラムは、学認システムとRadiusサーバとの間で認証をProxyする機能を持つ。

先に学認での認証方法の方法で説明したように(図-1)、学認のサービスを利用する場合、Webブラウザを用いてSP、IdP、DSにアクセスする。この外部プログラム(認証Proxyプログラム)は、Radiusサーバにインストールされ、ID、パスワードをRadiusサーバから学認システムへ中継するプロキシとしての機能を持ち、認証情報をWebアプリケーションである学認システムとやり取りするため、http(https)クライアントとしての役割を持つ。

また、SPはIdPから認証結果と必要な個人の属性情報を取得する。本システムのSP(認証情報取得SP)は、認証Proxyプログラムと対話して、認証後必要な属性情報を認証Proxyプログラムに提供する。

認証Proxyプログラムは、http(https)クライアントソフトであり、一般のブラウザと同じように、

1. ヘッダー(cookie等)、html文を取得
2. リダイレクトの処理
3. html文の解析。接続先URL、入力フォームを取得
4. 1.に戻る。入力フォームがある場合は、入力データを渡す

を行う。実際のレルムを用いた場合の認証プロセスは、以下のとおりになる。

1. パソコンからWebネットワーク認証システムにアクセスする
2. ブラウザ画面にID(レルムあり)、パスワードを入力する
3. ユーザが入力したID(レルムあり)、パスワードを受け取ったWebネットワーク認証システムは、認証を行うRadiusサーバにID(レルムあり)、パスワードを転送する
4. Radiusサーバは受け取ったID(レルムあり)から認証に学認を使うことを判断し、ID、パスワードを認証Proxyプログラムに転送する
5. 認証Proxyプログラムがレルム(ID@Idpのdomain)からIDおよびIdPのドメインを取得する
6. 認証Proxyプログラムが認証情報取得SPにアクセスする
7. 認証を受けていないので、DSにリダイレクトされ、認証Proxyプログラムは、DSのhtml文からIdPのリストを取得する
8. 認証Proxyプログラムは、レルムから得られた大学ドメインを参考に7.で取得したIdPリストからIdPのURLを選択し、選択したIdPにアクセスする
9. 認証Proxyプログラムは、IdPからID、パスワードを入力するためのフォームを取得する
10. 認証Proxyプログラムは、Radiusサーバから送られたID、パスワードをIdPに送信し、認証を受ける
11. 認証結果がIdPから認証情報取得SPに送られ、認証Proxyプログラムは、認証結果と属性情報を認証情報取得SPから取得する
12. 認証Proxyプログラムは、受け取った認証結果及び属性情報をRadiusサーバに返答する
13. Radiusサーバは受け取った認証結果をWebネットワーク認証システムに返答する
14. Webネットワーク認証システムは、認証結果を基にネットワークへの接続の可否を判断する。

以上の様に、自動切替を行った場合でも、宮崎大学のWebネットワーク認証システムを利用するパソコンは、認証画面にID(レルムあり、レルムなし)とパスワードを入力するだけでネットワーク認証を受けられ、SP化の前後で利用形態に変化はない。

また、この認証自動切替は、IDにレルムを利用するときに特段の制限を設けていない。宮崎大学は学認の運用フェデレーションでIdPを立ち上げているので、学内者がIDとしてレルム(学認ID@miyazaki-u.ac.jp)を入力して学認の認証を受けることも可能である。

5. 試験評価

この認証Proxyプログラムを使って、実際の宮崎大学のWebネットワーク認証システムを模した独立した試験評価環境を構築して、非常に簡単な試験評価を行った(図-4)。Webネットワーク認証システムとして、現在宮崎大学で使われている日立電線Apresiaスイッチングハブを用いた。また、学認の代わりとして、Idpと認証情報取得SPからなるローカルフェデレーションを作った。比較のために、レルムを用いないOpenLDAPを使った認証システムも立ち上げている。試験評価で使用したシステムは、以下の通り。

- Webネットワーク認証システム Apresia4328GT
- サーバ1(認証Proxyプログラム及び認証情報取得SPを含む):CentOS 5.8
  FreeRadius 2.1.12
  OpenLDAP 2.3.43
  Shibboleth SP 2.4.3
- サーバ2:CentOS 5.7
  Shibboleth IdP 2.3.3

この評価環境で認証を行ったところ、OpenLDAPを使った認証と比べてほとんど遅延も無く学認を模したローカルShibbolethフェデレーションを使ったシステムでも認証できることが確認できた。

但し、この試験評価環境は単独のパソコンからのアクセスであるので、実際のネットワーク環境でネットワークによる遅延、Webネットワーク認証システムからの認証要求が集中するRadiusサーバの遅延、学認システムへの認証結果の遅延を考慮する必要がある。更に、現在の認証ProxyプログラムはRadiusサーバへ複数の認証要求が来ることを考慮していない。

6. まとめ

宮崎大学のWebネットワーク認証において、アプライアンス製品であるWebネットワーク認証システムが参照する外部のRadiusサーバのレルムを利用し、Radiusサーバの外部プログラムである認証Proxyプログラムと認証情報と属性を認証Proxyプログラムに渡すSPを作成することで、学認と学内統一認証を自動的に切り替えてシームレスに認証出来る様になった。これにより、Webネットワーク認証システムを利用するパソコンのアクセスが制限される状況であっても、安価に、アプライアンス製品であるWebネットワーク認証システムに影響を与えずに学認のSP化することができるようになった。

本研究では宮崎大学のWebネットワーク認証システム

をSP化するシステム開発を行った。しかし、本研究ではWebアプリケーションであるWeb認証システムに対しては一切変更を加えていないので、Webアプリケーションが外部認証システムとしてRadiusサーバを利用しているのであれば、同様にWebアプリケーションをSP化できると思われる。このSP化手法は学認と学内統一認証を自動的に切り替えて利用する場合だけでなく学内統一認証IDを学認IDとして利用している場合でも同様に利用でき、第４のSP化手法として有効である。

学認では、個人情報保護の観点から、個人が自分の属性情報をSPに送付するかどうかを選択できるuApprove.jpというプログラムを用意している。これは、IdPにアクセスした際、アクセスする本人がブラウザを使って送付する属性情報を選択する。Webアプリケーションの認証プロセスを利用して認証Proxyプログラムを走らせるので、ID、パスワード、ドメインとあらかじめ決められた情報しか取得、送信することが出来ない。よって、uApprove.jpには対応できない。今回の認証Proxyプログラムを利用したSPを運用する組織が必要最小限の個人情報の取得を心がける必要がある。

本研究では、宮崎大学のWebネットワーク認証をモデルとした試験環境での運用だけで、まだ実環境での負荷試験などは行っていない。今後は、様々な実環境でも十分に運用できるプログラムに仕上げていく必要がある。

参考文献

[1]学術認証フェデレーション　学認　GakuNin、
https://www.gakunin.jp/ja/
[2]学術認証フェデレーション運用基準(Ver.1.2)、
https://www.gakunin.jp/docs/files/GakuNin_System_SpecV1.2.pdf
[3]ゲスト利用者のネットワーク認証に活用／広島大学、
https://www.gakunin.jp/docs/files/12hiro.pdf
[4]江藤博文,大谷誠,渡辺健次,只木進一:Opengateとシングルサインオン,電子情報通信学会技術研究報告. SITE, 技術と社会・倫理, Vol.108, No.459, pp.259-264(2009)
[5]学認参加機関の各IdPの運用に関するアンケートの実施について：世界標準に適合したトラストサークルの確立に向けて、https://www.gakunin.jp/docs/fed/loa
[6]広島大学情報メディア教育センター:学内情報コンセント、
http://www.media.hiroshima-u.ac.jp/services/hinet/cup#anchor-3
[7]佐賀大学情報基盤センター：学認向け無線LANゲスト利用サービス(Opengate)、
http://www.cc.saga-u.ac.jp/gakunin/
[8]SAML連携によるeduroam仮名アカウント発行システムの実装、
https://upki-portal.nii.ac.jp/docs/files/SSO_report_2009kyoto.pdf