福岡大学が認証基盤に求める要件

中國　真教

福岡大学総合情報処理センター

[アブストラクト]

福岡大学では、全学の利用者 ID を統合的に管理する認証基盤を刷新し、2012 年 5 月に「福岡大学認証基盤システム」という名称で新システムの稼働を開始した。本システムでは、以前運用していた認証基盤で抱えていたいくつかの課題を解決でき、新機能も取り入れた。新機能の中で特筆すべきものは、SSO（Single Sign On）の機能である。本システムでは、国立情報学研究所が中心となって推進する学術認証フェデレーション（学認）で利用されている Shibboleth、Sun Microsystems 社によって開発された OpenSSO から派生した OpenAM、これら 2 つを組み合わせたハイブリッド型 SSO の仕組みを導入した。この仕組みの特徴は、単純に 2 系統の SSO 環境を導入した点ではなく、一方の SSO 環境で利用者認証を行えば、もう一方の SSO 環境にも認証結果が反映され、あたかも 1 つの系統のように見なすことができる点にある。本報告では、従来から抱えていた課題やその解決方法について述べ、新機能であるハイブリッド型 SSO の導入についても触れながら、認証基盤を刷新した現在の状況について報告する。

[キーワード]

認証基盤、SSO、Shibboleth、OpenAM、オープンソース

1. はじめに

福岡大学では、大学の情報化という目的で 2003 年頃から情報システムの導入を積極的に行った。その際、増え続ける情報システムにおける ID およびパスワードの運用管理コストの増大を懸念し、福岡大学では最初の認証基盤となる「福岡大学統合認証システム」を構築し運用を開始した。当時は、組織的かつ大規模に認証基盤を構築している大学などは少なく、認証基盤の黎明期とも言える時代であった。当然のことながら、認証基盤の中核をなすソフトウェアについてはパッケージ製品が存在しなかったため、システム内部のソフトウェアの多くは独自開発したものであった。統合認証システムの稼働開始時には 8 つの情報システムとの認証連携を開始し、各情報システムへのログインは一組の ID とパスワードだけで可能となった。利便性は飛躍的に向上した上、ID とパスワードに関わる運用管理コストを低く抑えることを実現した。時間の経過とともに認証連携を行う情報システムの数は増加し、統合認証システムの導入効果が表れていたが、次第に認証基盤における課題の数も増加したため、新たに発生した数々の課題を解決するため 2012 年 5 月に認証基盤を刷新した。現在は「福岡大学認証基盤システム」という名称で新しい認証基盤を運用している。

2. 以前の認証基盤における課題

以前運用していた認証基盤である統合認証システムは、前述のとおり「認証基盤の黎明期」に構築したものであり、暗中模索の状況でソフトウェアを独自開発して構築したものであった。その上、システムの仕様書は存在せず、詳細な設計書も残されていなかったため、統合認証システムの管理者にとってシステムの中身はブラックボックスと化していた。そのため、何らかのトラブルが発生してもシステム管理者自身による原因究明と解決が困難であり、統合認証システムを構築したベンダーに頼らざるを得ない状況が多く、統合認証システムにおける第 1 の課題は、そ

の状況から脱却することであった。

第 2 の課題としては、独自開発のプログラムであるが故、福岡大学に特化して作られたソフトウェアが多く、汎用性が低く、機能を拡充することが極めて困難な状況で、機能を拡充する度に大きな改修が必要であった点である。その一例としてSSOの機能があげられる。統合認証システムには、SSOに類する機能が既に実装されていたが、それは独自開発によるSSO機能であって、一般的なSSOとは互換性がなかった。そのため、SSOの機能を標準で備えた情報システムを導入しても、その機能を生かすことができなかった。

第3の課題は、利用者から見た課題であった。統合認証システムでは、利用者がパスワード変更を行った際、その変更結果を各情報システムへリアルタイムに反映させることができない仕様となっており、全システムへ完全に反映できるのは翌日であった。このような仕様では、利用者のパスワードが他人に知られてしまった場合、即座に利用者自身でパスワードを変更しても、翌日までは他人によってそのIDを無断利用されるかもしれないというセキュリティ上の危険性があった。利用者から見た課題はこれだけではなかった。利用者がパスワードを忘れたり、パスワードの有効期限切れで情報システムへのログインができなくなったりした場合には、統合認証システムの管理者によって「パスワード初期化」の手続きを実施しなければならない。ところが、パスワード初期化には 1 人の利用者につき 2 分以上の時間を要し、パスワード初期化の依頼を受け付ける窓口には、依頼者の行列ができることもあった。他の課題としては、学外からパスワード変更をさせないポリシーとしていたため、出張、留学、休暇などのために大学から離れた場所にいる利用者はパスワード変更ができないという課題もあった。

3. 認証基盤の刷新

統合認証システムにおける多くの課題を解決するため、新システム「福岡大学認証基盤システム」の導入検討および構築を開始した。前述の 3 つの課題の解決について重点的に検討を行い、仕様書、設計書などの資料を作成して残すことで認証基盤システムのブラックボックス化を防止した。また、標準的な仕組みを取り入れることによって、多くの情報システムとの認証連携やパスワード変更におけるリアルタイムな反映などを可能にした。そして、SSO の導入を行い、情報システムの利便性も高めた。SSO については、国立情報学研究所が中心となって推進している「学認」で利用される Shibboleth、Sun Microsystems 社によって開発された OpenSSO から派生した OpenAM、これら 2 つを組み合わせた「ハイブリッド型 SSO」の仕組みを導入した。Shibboleth だけでなく OpenAM も利用することには理由がある。Shibboleth を利用して各情報システムの間で SSO を実現するためには、各情報システムを Shibboleth に対応させるために大幅な改修作業と大きなコストが発生する可能性があると考え、既存システムとの親和性が比較的高い OpenAM も併用し、2 系統の SSO 環境の導入を検討した。しかし、SSO 環境が 2 系統存在すると、利用者に対し最大で 2 回の利用者認証を要求することになり、Single Sign On とは言えない。この課題を解決するため、2 系統の SSO 環境における利用者認証を 1 度のログインで完了できるハイブリッド型 SSO の仕組みを導入した。この仕組みは、Shibboleth や OpenAM に備わっている Rest API によって実現するものである。この仕組みにより、Shibboleth の配下または OpenAM の配下の情報システムで利用者認証を行えば、Rest API によって両系統の SSO 環境で利用者認証の結果を共有し、2 系統の SSO 環境を 1 つに融合できる。このように、OpenAM と各情報システムの親和性の高さを生かすことで認証にかかわるコストを抑え、Shibboleth を利用して学認から提供されるサービスを活用し、情報システムの整備にかかわるコストの削減を見込んでいる。

4. おわりに

本報告では、福岡大学の認証基盤における運用管理やコストに関わる過去の課題について述べ、課題を解決するために構築した新システムとその特徴ついて述べた。今後の福岡大学認証基盤システムについては、必要に応じて機能拡充を行い、ICT に関わるコスト削減を実現しながら、更なる活用の方法について模索していきたい。