D10-4

ネットワーク監視システムの Shibboleth 化

関 陽介, 松浦 健二, 松村 健, 上田 哲史, 佐野 雅彦, 矢野 米雄

徳島大学 情報化推進センター

seki@ait.tokushima-u.ac.jp

概要：徳島大学では、情報化推進センターにおいて、ネットワーク資源監視を全学的に分散運用されている各システムに展開している。本書ではその例として、監視システムの認証・認可基盤をローカル認証から Shibboleth 化する試みについて述べる。

1 はじめに

徳島大学においては，情報化推進センターの改組以降，大学全体の ICT サービスに対して，一定のサービスレベルを確保すべくプロジェクト体制をとって業務遂行を展開している．アカデミックな教員主体で様々な施策を実施しようとした場合には，学術的な閉鎖的設計になりがちであるが，現場の構成員には依然その成果還元がなされにくい状況もある．原因としては,まだユーザ視点に立った設計運用に慣れてない点が挙げられる．

本センターにおいては，昨今の内外状況を検討し，フィールド実践を主眼としたサービス重視にシフトしている．したがって，大学環境（構成員の特性，キャンパスネットワーク環境等）をサービスフィールドとする研究開発や実践展開を行い，得られた知見を現場にフィードバックしたいと考えている．

以上の背景の下，本センターでは，所掌範囲におけるネットワークレンジを広げることとし，ネットワーク資源監視を増強することとなった．また，並行して標準的な技術による認証連携環境も構築されていく状況であったため，この監視装置に適用することとした．本稿ではその検討経緯や，実装設計について述べる．

2 情報基盤サービスを取り巻く環境

2.1 学外動向

ICT サービスは，業務系システム，一般コミュニケーションシステム等，それぞれの特性を考慮した運用形態が図られつつある．したがって従来のオンプレミス運用のみという思想での設計・導入は少なくなってきている．例えば，政府や自治体においても，外部委託できる部分はポリシ改定が検討され，実際に行われている．それ以前から，民間企業あるいは個人レベルでは，コミュニケーションサービスに関するクラウドサービス導入が浸透し，それに追従する形で大学等高等教育機関でもパブリッククラウドサービスを導入し始めている．

東日本大震災以降は災害対策の視点からも，この傾向がさらに加速している．

サービスの適正範囲の外部委託に際しても，一定水準の情報セキュリティが確保されなければならない．一定水準のセキュリティが確保されれば，組織間の信頼関係の下での，サービスの相互依存も始まることとなる．例えば，各大学間でのサービスあるいはそのコンテンツの相互補間，増強である．そのような環境には，共通化された連携基盤が必須であり，認証連携がその中核機能となる．日本においては，国立情報学研究所を中心とした「学認」がある．なお，本学はテストフェデレーションへの参加から運用段階にまだ至っていないが，学認のさらなる展開は期待される．

2.2 学内情勢

徳島大学に限らず，多くの大学にはインターネット黎明期から活躍してきたスキルフルな教職員が各部局に何人かは存在していた．それらのボランティアベースでの支線（基幹網に対する下位ネットワーク）管理が継続されなくなりつつあると共に，構成員が総ユーザ化する状況となっている．これにはネットワークや管理業務の高度化とともに，ウィルスなどリスク対策の負担増加，本務および関連業務のバランス維持，インセンティブなど,多種多様な事情が関係している．さらには，人事面の流動化の促進等も理由としてはあろう．

本学の規模（５学部，約１万人）においては，大学全体を幾つかの部局単位に細分化して，部局

内での自治的な管理体系を当初は進めてきた．しかし，上述の現状からは，各部局で過去に構築してきた WEB サービスやメールサービスの運用管理を部局単位で維持していくのは無理が生じることとなった．そこで，各部局からは情報化推進センターでのサーバ管理等を請負・委託（ハウジング，ホスティング，およびサーバ統合化等）することへの期待が高まっていた．以上の結果，情報化推進センターへの改組(平成22年7月)後には，それ以前の原則であった基幹はセンター，支線は部局での管理という体制を見直す契機となった．

3 ネットワークサービスの統合監視

3.1 ネットワーク資源監視

前説で述べたように，大学全体の支線管理においても，管理対象を広げることとなったが，部局固有の事情は残る．そこで，センターでは８段階の管理種別を定め，明確に管理方針の区分を定義する必要はあった．例えば，資産管理的な意味合いだけでなく，技術的な意味での管理範囲（特権ユーザを取得して対応など）も視野に入れる対応である．

そこで，最も基本的な管理サービスの一つは，ネットワークリソースの死活監視である．本学では，以前から，IPAudit,MRTG を用いたコアスイッチ等のトラヒック監視を運用してきた．しかし，多様なネットワーク実装形態でのサーバ等の多様な死活監視を実現するには別の枠組みが必要という議論から，特に OSS 実装系の解を検討し，Nagios（http://www.nagios.org/）を追加導入することとした．Nagios はオープンソース系の統合監視システムとしては，実績も多く，したがってシステム自体の情報量も多いシステムの一つと言える．また，「見える化」を実現するには，リソースのグラヒック表示なども実装しており，本学事情には適した解であった．

3.2 統合認証と SSO

大学環境では，LDAP あるいは AD によるディレクトリサービスを導入しているところが多い[1]．ディレクトリサービスの典型的な応用には，統合認証基盤としての利用がある．本学でも，統合認証基盤としては，学生向けには AD，教職員にはLDAPを切り分けた利用を長年運用している[2]．統合認証やそれを応用したシングルサインオン実装には，CAS[3]等も実績があるシステムである．しかし本学では，先に述べた学認での採用もあり，また最初から組織間連携を実装していた Shibboleth を採用した認証認可連携基盤を構築した．Shibboleth では，ディレクトリサービスあるいはデータベース上の個人属性を利用した認可制御が可能な枠組みと言える．本学ではポータルや LMS，業務系システムや一般的な WEB，WebDAV 等にて対応している．

3.3 NW 資源管理システムのシボライズ

上記の二つを組み合わせる事とした．すなわち，ネットワークリソース監視システムにも認証認可連携基盤を適用するものである．何でも統合認証基盤に乗せるべきという訳ではないが，認可機構の設計および実装によっては，例えば，各支線等でのコミッタに対しての負荷軽減や，異動時の対応にも応用できる可能性が高い．具体的には，各視線の管理者に，一定のアクセスを認証認可の枠組みの中で提供できる．

4 まとめ

本稿では，徳島大学におけるネットワークリソース監視システムへの Shibboleth 化について述べた．昨今の大学における情報系センターの果たす役割は，クラウド化の時勢と共に，大きく変化しようとしている．このような中でもオンプレミス系サービスは一定数残る事も多く，そのような環境においては，認可機構を持った認証基盤および SSO 環境が今後も必要と考える．

参考文献

[1] 秋山 豊和, 寺西 裕一, 岡村 真吾, 坂根 栄作, 長谷川 剛, 馬場 健一, 中野 博隆, 下條 真司, 長岡 亨, 「大阪大学における全学 IT 認証基盤の構築」, 情報処理学会論文誌, Vol.49, No.3, pp. 1249-1264, 2008.

[2] 松浦 健二, 金西 計英, 大家 隆弘, 上田 哲史, 中川 昌宏, 矢野 米雄：徳島大学における大学内外システム連携のための認証認可検討, 電子情報通信学会 2009 年総合大会講演論文集, pp.141-142, 2009.

[3] 内藤 久資, 梶田 将司, 小尻 智子, 平野 靖, 間瀬 健二, 「大学における統一認証基盤としての CAS とその拡張」, 情報処理学会論文誌, Vol.47, No.4, pp.1127-1135, 2006.