東北大学におけるリバースプロキシ型認証連携システムの運用報告

行方 義忠[†], 安西 従道[‡], 酒井 正夫[†], 田中 弓子[†], 早川 美徳[†]

[†]東北大学教育情報基盤センター

[‡]東北大学情報部

namekata@cite.tohoku.ac.jp

概要：東北大学では，学外から本学 Web サービスへのアクセスする手段として，リバースプロキシ型の認証連携システムである東北大学セキュアリバースプロキシ（Secure Reverse Proxy: SRP）を導入しており，2010 年 4 月より全学規模で運用している．本稿では，SRP の機能と特徴を解説し，その運用実績を報告する．さらに，これまでの運用実績に元づいて，リバースプロキシ型認証連携システムでの障害対応，それに伴う総合大学において考慮すべき点についても提言する．

1　はじめに

近年の大学の情報化に伴い，e-Learning システム，研究支援用のシステム，事務システムなどが運用されている．その多くは Web システムとして提供されており，教職員だけでなく学生も日常的に利用するものとなっている．しかしながら，東北大学では，これらシステムは各部署で個別に管理されており，認証情報やセキュリティレベルの統一がなされておらず，安全性と利便性等の面で課題があった．

本学では 2004 年度の独立行政法人化以降，認証システム情報の一元管理が進められてきた．さらに，認証システムの統一化と併せて，さらなる安全性利便性を強化することを目的に，2010 年度より東北大学セキュアリバースプロキシ(SRP, https://www.srp.tohoku.ac.jp)[1]の運用が開始された．本学では，学生も含めた全構成員が SRP を利用するため，利用可能なユーザ数は約 3 万人になる．また，情報システムの新規構築または更新の際には，大学管理の認証システムおよび SRP との連携を原則しているため，連携する情報システムは年々増加し，SRP 経由でのアクセス数も増加している．これに伴い，導入当初は想定していなかった障害や運用上の問題も発生しており，その都度，試行錯誤を重ねて対応している．このような経験は，本学と同様に，認証システムの統一，安全性と利便性の強化を目指す大学にとっても有益な情報ではないかと考えられる．

このような考えのもと，筆者らは大学 ICT 推進協議会 2013 年度年次大会において，本学の SRP を紹介し，運用状況と障害対応，それらを踏まえた上で，総合大学においてリバースプロキシ型認証連携システムを導入する際に考慮するべき事項を提言している [2]．本稿では，主に前回発表以降の利用実績と，障害対応，およびリバースプロキシ型認証連携システムの導入に関して考慮するべきことを提言する．

2　東北大学セキュアリバースプロキシ

2.1 概要

本項目では SRP の動作原理の概要を簡単に説明する．詳細については，前回の報告を参照されたい[2]．

東北大学セキュアリバースプロキシ（SRP）は，動作イメージ（図 1）のように，ユーザと情報システム間の通信をリバースプロキシ方式で中継するシステムであり，市販のセキュリティ強化ソフトウェア『WisePoint』[3] を本学向けにカスタマイズしたものである．

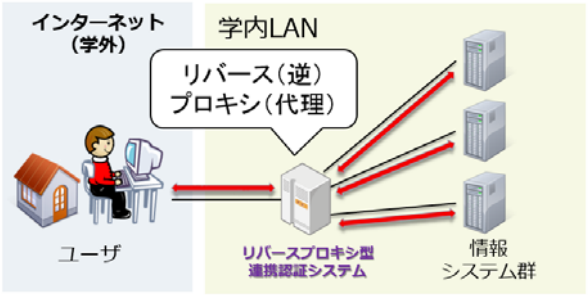

図 1 東北大学セキュアリバースプロキシ

これまで，SRP は本学の情報基盤として活用・増強されており，その連携情報システム数と設計性能は，運用開始時（2010 年 4 月）から 2014 年 10 月現在までに，表 1 のように増大さ

れている．

本学では，リバースプロキシ機能に加え，ユーザが SRP を経由して情報システムと接続されることで，不正アクセス対策を強化する「2 段階認証」と，システム間連携のための「ポータルサイト＋SSO(シングルサインオン)」の機能を提供している．各機能の詳細については次節以降で紹介する．

表 1　SRP の連携情報システム数と性能

	運用開始時 (2010 年 4 月)	現在 (2014 年 10 月)
連携情報 システム数	4	12
同時接続 可能数*	1,000	1500
スループット	200Mbps	500Mbp

*10 秒以内に応答可能な同時接続数のこと

2.2 リバースプロキシ型認証連携システム

本学ではリバースプロキシ型のサービスを用いることで，学外からのアクセスに対して連携情報システムの安全性を高めている．原則的には，連携情報システムの Web サービスは学外と直接通信を行わず，SRP を経由してアクセスされる．これによりファイアーウォールで不要な通信を排除する以上の安全性が期待できる．SRP では，SRP 自身に SSL 証明書を導入し，ユーザと SRP 間の通信を暗号化している[3]．これにより，個々の連携情報システムの Web サービスの SSL 通信に脆弱性があった場合にも，それを狙った攻撃を防ぐことが期待できる．また，SRP の設定により，連携情報システムの Web サービスの学内接続向け認証ページに対する攻撃や，管理者用ページなどの特定 URL への直接アクセスなども防ぐことが可能になる．

2.3 2 段階認証

本学のように，ユーザ認証情報を一本化し，複数の Web システムにおいて利用すると，ユーザの利便性は向上する一方で，同時に，全体のセキュリティレベルが下がる危険性が懸念される．具体的には，何らかの理由により，ユーザ認証情報が漏洩した場合には，全ての Web システムに被害が及ぶ可能性がある．本学では，特に学外からの攻撃に対してのリスクを重要視しており，その対策として SRP による 2 段階認証を採用している．

SRP は，接続元 IP アドレスの検証により，ユーザが学外から接続していると判断した場合には，イメージマトリクス認証による 2 段階認証を要求する．イメージマトリクス認証とは，図 2 のように行列状に並んだ 25 枚の画像から，ユーザが事前に登録済みの 3 枚の画像を正しく選択することを求める認証方式である．この 25 枚の画像の種類と並び，および，行と列に割り当てられる数字は毎回ランダムに変更される．そして，ユーザが選択した画像の行と列の数字を SRP サーバに送ることで認証が行われる．この認証方式はチャレンジ&レスポンス方式のワンタイムパスワード認証となり，高い安全性を実現する．

図 2 イメージマトリックス認証

2.3 ポータルサイトと SSO

本学では，ユーザに対して，学内の各種 Web サービスを利用する際に SRP を経由する方法を推奨している．ユーザは，目的の Web サービスの URL が不明の場合でも，SRP を経由して専用のポータルサイトに一旦接続することで，そこからリンク集を辿り目的の Web システムに接続することができる．本学では，ユーザの種類ごとにアクセス可能な Web システムを分けており，それぞれに最適化したページ（図 3）をポータルサイトとして表示している．

なお，各 Web サービスには SRP を経由して接続するための専用 URL が設定されており，その URL に直接アクセスすることで，ポータルサイトに一旦ログインする手間を省くことも可能である．ただし，その場合でも，SRP の認証は省略できない．

また，SRP ではユーザの利便性を向上するため，

2 回目以降の連携システムでのユーザ認証を省略（自動化）する SSO （シングルサインオン）機能を使用できる．なお，現在 12 ある連携情報システムのうち SSO に対応するものは 11 である．残りの情報システム（ALC NetAcademy2）は技術的な理由で SSO に対応できていない．

学生用

職員用

図 3　ポータルサイトの画面．

3 運用状況

3.1 利用状況

2011 年 8 月から 2014 年 9 月までの，SRP の 1 日当たりのアクセス数と，2012 年 1 月から 2014 年 9 月までの 1 日当たりの利用ユニークユーザ数の月毎の平均値の推移を図 4 に示す．ここで，アクセス数とは，SRP を経由してファイルに接続された延べ数のことであり，利用ユニークユーザ数とは実際にアクセスしたユーザを 1 日ごとに学内・学外で分けてカウントしたものである．

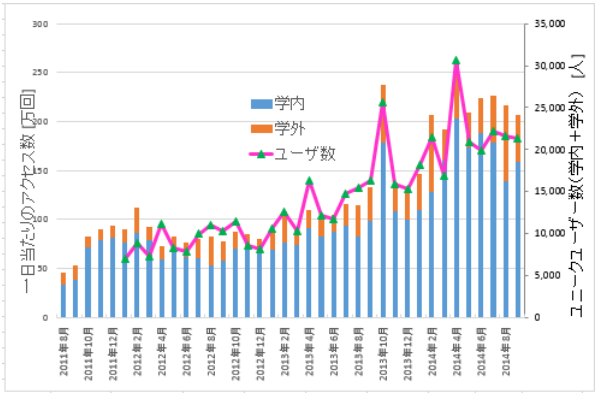

図 4　SRP の 1 日当たりのアクセス数とユニークユーザ数の月毎の平均値の推移．

この結果より，2013 年 10 月と 2014 年 4 月にアクセス数が急増していることがわかる．これは，SRP 連携システムの一つである学務情報システム（2013 年 10 月より本格稼働）において，履修登録を行う学生ユーザのアクセスが，履修登録の時期にあたる 4 月と 10 月に集中したためである．

また，2014 年 2 月と 8 月に学外からのアクセスが増加しているが，これは休講期間中に成績照会のために学外からアクセスしていると考えられる．

3.2 障害履歴

前回の報告[2]では，2013 年 10 月末までの障害履歴について報告しているため，本稿では，前回の報告でも紹介した 2013 年 10 月のサービス停止障害への対応を含め，それ以降に発生した主な障害事例，および再発防止策について報告する．2013 年 10 月から 2014 年 9 月までに，

サービスの停止など重大な障害とみなせるインシデントが 5 件発生している．そのうち，再現性が高く，教訓となる 2 つの障害について報告する．

3.2.1 学生向けサービスでの障害事例

本節では，前回に報告した障害ついて，その後に施した再発防止策と共に報告する．

本学では 2013 年 9 月から学生向けの Web システムとして新たに学務情報システムの運用を開始し，SRP 経由でそのサービスを提供している．学務情報システムが本格稼働した 10 月には学生の履修登録の締切日にアクセスが集中し，SRP が停止する事態に至った．再発防止のため，画像データの認証を省略することや，Web ブラウザのキャッシュを有効化することで SRP 経由での処理を軽減する試みが行われたが，満足すべき結果は得られなかった．その後の改善によって，現在では，一旦 SRP 経由で SSO が行われた後には，学内からのアクセスにのみ，ユーザと学務情報システム間で直接通信が行われるようになっている．その際，アクセス元が学内か学外かに応じて，SRP の認証後に提示されるポータルサイトのリンク先を自動的に切り替えることによって，ユーザは意識することなく同システムを利用できるように工夫した．直接通信時であっても SSL で暗号化された通信を用いており，安全性の面から見ても特段の問題は無いと考えられる．

また，同月には，大型台風による休講情報を確認するためと推測されるアクセスが集中し，遅延が発生した．この再発防止のため，SRP では，学内アクセスと学外アクセスとに割り当てられるリソース（処理能力）を調整することができるが，アクセス集中に対応するために，学外側のリソースを増強することとした．本学では，学内用と学外用のサーバ設定が異なる（学外用サーバのみ，2 段階認証を行う設定となっている）ため，現状では，学内側と学外側に割り振るリソースの動的かつ自動な変更が不可能であり，事前に手動で設定する必要がある．

3.2.2 教職員向けサービスでの障害事例

2014 年 4 月より給与明細サービスで遅延障害が発生した．問題の所在を調査したところ，SRP と給与明細サービスは単独では問題なく動作し，また，特に問題が生じる可能性のあるような設定等も確認できなかった．

さらなる原因究明の結果，通信処理に問題があることが判明した．具体的には，給与明細を提供しているサーバの OS に問題があり，起動してから一定日数経過するとポートの開放に失敗し，同時通信可能な件数が減少することが明らかになった．このため，給料日などに短期間に多数のアクセスが集中した場合等に当該システムが SRP 経由での応答ができなくなり，SRP の障害と誤解されたものと考えられる．

SRP は，複数の情報システムと連携して一元的なサービスを提供するため，今回の給与明細サービスとの連携で生じたものと同様の障害の発生は，今後も十分に想定される．特に本学のような総合大学である場合には，各連携情報システムを管理する部局が異なることが想定される．このため，連携時のテスト項目や障害発生時についてはノウハウの蓄積が必要となる．そこで，本学では運用期間中に連携障害が発生した場合に備えてチェック表を作成し対応している．

4 リバースプロキシ型認証連携システムを運用する際に考慮するべきこと

SRP のようなリバースプロキシ型認証連携システムでは，複数の Web システムと連携して動作することが前提となっている．従ってリバースプロキシ型の場合，システム障害は連携する全 Web システムの障害を意味する．

以降では，本学での運用経験を踏まえ，複合大学においてリバースプロキシ型認証連携シス

テムを運用する際に考慮するべき事項を提言する．

4.1 アクセス遅延・集中への対応

本学では，連携情報システムの追加や一時的なアクセス集中に対応するため，事前のリソースの増強や調整を行っている．しかし，リバースプロキシ型であるため，原理的に，利用率の増加に伴って応答速度が低下してしまう．特に大量の画像データをボタンやバナー等に利用している場合には遅延が発生しうる．こうした遅延に対応するため，以下の対策を提案する．

- 学内などの信用できるネットワークからのアクセスについては，認証後は Web サービスとユーザの直接通信とする．
- 画像データなどのセキュリティが不要なデータについては，Web サービスとユーザ間を直接通信とする．
- 同様にブラウザのキャッシュを活用することでネットワーク負荷の軽減を図る．

また，SRP は複数の情報システムと連携しているので，一旦特定の情報システムにアクセスが集中すると，他の情報システムにも影響が出てしまう．例えば，ひとつの連携情報システムにアクセスが集中し，その連携システムから応答がない場合，SRP のサービス全体が応答待ちとなってしまう．これに対応するため，以下の対策を提案する．

- アクセス集中が予測される連携システムに対しては，予めリソース（処理能力）を重点的に割り当てる．
- リトライ上限回数の調整により，応答待時間を軽減する．

なお，本学の SRP ではリソースの割り振りに関して，自動化するために 2 点の課題が残っている．1 つ目の課題は，SRP ではサーバ数を増やすことでリソースを増強しているが，SRP へのユーザからのアクセスが，複数のサーバに均等に割り振られず，特定のサーバに偏り，適切に負荷分散されないことである．これは，接続元 IP アドレスが同じ場合は，同じサーバで処理するという SRP の仕様と，一部の連携情報システムの仕様に起因し，SRP からは，特定の部局からその連携情報システムへの接続が，全て同じ接続元 IP アドレスに見えてしまい，特定のサーバに負荷が集中することがあるためである．2 つ目の課題は，学内外からのアクセスの変動に対して，リソースを動的かつ自動的に割り振ることが出来ないことである．このため，例えば，学内からのアクセスに対してはリソースに余裕があるが，学外からのアクセスに対しては応答できない場合が起こりえる．これらの 2 点の課題に関しては，現状では，まだ適切な解決案が出ていない．これらの課題は，運用開始後に対応することは困難であるが，これから導入を検討する場合には事前に対策することで回避可能と考えられる．そこで，以下の対策を提案する．

- リバースプロキシ型認証連携システムと連携情報システムの双方で，共通かつ連携可能な負荷分散方式を採用し，適切な負荷分散を行う．

4.2 連携障害への対応

SRP のようなリバースプロキシ型認証連携システムでは，複数の情報システムとの連携が前提である．しかし，本学のような総合大学では，それらの連携情報システムの管理部局が異なる場合も多いであろうし，運用ルール，求められるセキュリティレベルが異なることが十分に想定される．これに対応するため，以下のことを提案する．

- リバースプロキシ型認証連携システムと

連携する情報システムの管理部署が共同で運用マニュアルを作成する．

- 障害発生時のチェック表および復旧マニュアルを作成する．
- 定期的に OS 等のアップデートを確認する．

5 まとめ

本稿では，東北大学で運用しているリバースプロキシ型認証連携システムの運用状況，障害履歴とその対応を報告した．また，運用経験を踏まえて総合大学で同様のシステムを導入・運用する際に考慮するべき事項について提言した．

本稿で示したように，リバースプロキシ型認証連携システムでは，他の情報システムとの連携を前提としている．そこでは，有限な処理能力を適切に割り振ることが必要になり，そのために長期に渡る運用情報の収集とノウハウの蓄積が必要となる．また，各連携システムの運用部局との協力体制，複数部局との連携を前提とした運用マニュアルの作成が必要となる．本稿での報告と提言が，他大学における同様なシステムの運用の一助になれば幸いである．

参考文献

[1] 東北大学生のための教育系情報システムオンラインガイド：SRP の解説，
http://www.dc.tohoku.ac.jp/guide/SRP/SRP.html

[2] 酒井正夫，行方義忠，安西従道，田中弓子，早川美徳，東北大学におけるリバースプロキシ型認証連携システムの導入とその運用報告，大学 ICT 推進協議会 2013 年度年次大会，論文集 W3E-2，2013

[3] ファルコンシステムコンサルティング株式会社，
http://wisepoint.jp/wp/index.html