

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

酒井 正夫[†], 行方 義忠[†], 安西 従道[‡], 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

sakai@cite.tohoku.ac.jp

概要： 東北大学では、本学情報システム群の連携強化と、それら情報システムへの学外からの不正アクセス対策のために、リバースプロキシ型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（SRP）を構築し、2010年度より全学規模で運用している。本稿では、SRPの機能を解説し、また、その運用状況と障害事例を報告する。さらに、これまでの運用経験を踏まえ、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べきことを提言する。

1 はじめに

インターネット技術の発展に伴い、大学においても情報化が進み、多様な業務やサービスがウェブ経由で行えるようになってきている。しかし、初期の情報システムの多くは、他の情報システムとの連携を考慮することなく担当部署ごとに独自に構築されていたことから、情報システムごとに異なるユーザID/パスワードと運用ルールを採用するなど、利用方法とセキュリティレベルに統一性がなく、使い勝手と安全管理に問題があった。

東北大学でも、以前は同様な問題を抱えていたが、2004年度の国立大学独立行政法人化をきっかけに学内の情報システム群の全学的・体系的整備が継続的に実施され、現在では、学内の主要な情報システムにおいて統一したユーザID/パスワードと運用ルールが採用されている。また、その次の段階として、不正アクセス対策と本学情報システム群の連携強化を目的とする、リバースプロキシ型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（SRP）[1] (<https://www.srp.tohoku.ac.jp/>) を構築し、2010年度より全学規模で運用している。

本学では、SRPの運用開始以降、全学的用途の情報システムが新規構築または更新される場合にはSRPと連携することを原則としてきたため、SRPの連携情報システム数が年々増加し、その重要度とアクセス数も増大している。それに伴い、SRP導入時には想定していなかった障害や運用上の問題も頻発しており、その都度、試行錯誤的な対処が行われてきた。このような経験は、SRPと同様なシステムの導入を今後計画している他大学にとっても有益な情報になりえる。そこで、本稿では、本学のSRPを紹介し、その運用状況を具体的な障害事例

とともに報告する。さらに、これまでの障害対応などの運用経験を踏まえ、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

東北大学セキュアリバースプロキシ（SRP）は、その名前と動作イメージ（図1）が示すように、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』[2]を本学向けにカスタマイズして構築している。

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2013年10月現在までに、表1のように増大している。

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+シングルサインオン（SSO）」の機能を利用できる。各機能の詳細を次節以降で紹介する。

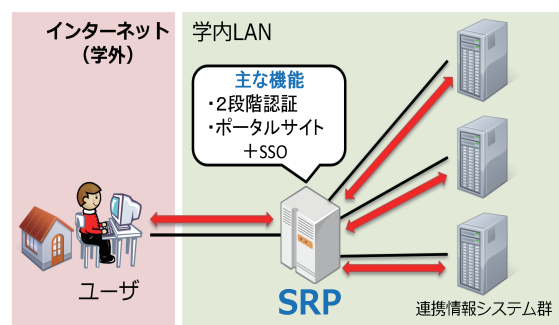


図1: SRPの動作イメージ。

表 1: SRP の連携情報システム数と設計性能の変化.

	運用開始時 (2010 年 4 月)	現在 (2013 年 10 月)
連携情報 システム数	4	15
同時接続 可能数 *	1,000	1,500
スループット	200Mbps	500Mbps

*:10 秒以内に応答可能な同時接続ユーザ数のこと.

2.2 2 段階認証

本学のように、複数の情報システムにおいて統一したユーザ ID/パスワードを採用することは、ユーザの利便性向上に有効であるが、一方で、学内の情報システムのセキュリティレベルや重要度は多様であることから、もしセキュリティレベルが低い情報システムでユーザ ID/パスワードの情報が漏洩した場合、重要な情報システム（例えば成績情報を扱う教務系システム）にまで被害が及ぶ恐れがある。そのため、危険度の高い学外から重要度の高いシステムを利用する場合には、ユーザ ID/パスワードによる認証の他に追加的なユーザ認証（2 段階認証）を求めることが、有効な不正アクセス対策になりえる。

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、イメージングマトリクス認証による 2 段階認証を要求する。イメージング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は毎回ランダムに変更されるため、この認証はチャレンジ&レスポンス方式のワンタイムパスワード認証となり、高い安全性を実現できる。



図 2: 2 段階認証におけるイメージングマトリクス認証の画面.



図 3: SRP のポータルサイトの画面.

2.3 ポータルサイト + SSO

ユーザが SRP 経由で連携情報システムに接続するには、情報システムごとに用意された SRP 経由専用のログインページから接続するか、または、SRP のポータルサイトに一旦接続（ユーザ認証が必要）して、そこからリンク集を辿り所望の情報システムに接続する方法の二種類がある。前者の方法は、専用ログインページの URL をユーザに周知しブックマークしてもらう手間が大変である。そのため、本学では後者の方法を推奨し、ポータルサイトへの接続を容易にするために、本学ウェブサイトの各所にポータルサイトへのログインフォームを設置している。

SRP のポータルサイトは、ユーザ ID からユーザの種類（学生/教員/職員）を判別し、それぞれに最適化したページ（図 3）を表示することが可能である。また、ポータルサイトからリンクを辿って連携情報システムに接続する場合、リンク先でのユーザ認証を省略（自動化）する SSO 機能を使用できる。なお、現在 15 ある連携情報システムのうち SSO に対応するものは 13 である。残りの 2 つの情報システムのうち 1 つ（ALC NetAcademy2）は技術的な理由で SSO が使用できず、もう 1 つは運用上の理由により SSO を使用していない。

3 運用状況

3.1 利用状況

2011 年 8 月から 2013 年 9 月までの 2 年 1 ヶ月分の、SRP の一日当りのアクセス数の月内平均値の推移を図 4 に示す。ここで、アクセス数とはユーザが SRP を経由して接続したファイルの総数のことである。

この結果より、2011 年 10 月よりアクセス数が急増していることがわかる。これは同月より、職員の

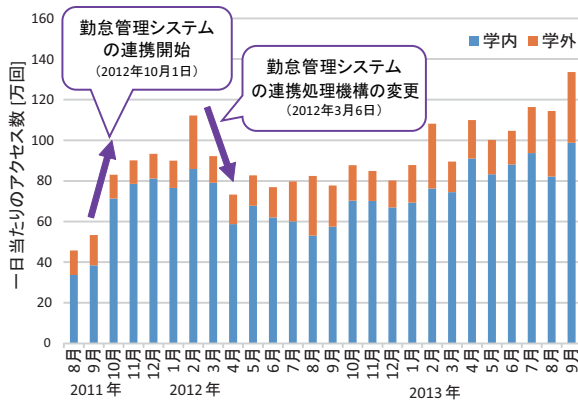


図 4: SRP の一日当たりのアクセス数の月内平均値の推移。

出出勤時刻を管理する勤怠管理システムが SRP の連携情報システムとして本格稼働したことが原因である。しかし、その後、この勤怠管理システムとの連携に問題が生じたため、その問題を回避するための改修（詳細は後述）を 2012 年 3 月に行なっている。同月よりアクセス数が急減しているのは、その影響である。この期間を無視すると、SRP のアクセス数は継続的な増加傾向にあると言える。

また、ユーザの接続元で色分けされた帯グラフより、大学が休業期間となる 2 月と 8 月は、他の月に比べて学外からの利用が多い傾向が見られる。これは、学生ユーザが自宅などから SRP を経由して学内の情報システムを利用する頻度が高まるからだと推測され、SRP が不正アクセス対策として活用されていると言える。

3.2 障害履歴

運用開始（2010 年 4 月）から 2013 年 10 月末までの 3 年 6 ヶ月の運用期間において、本学が SRP の保守業者に対して障害対応を依頼した件数は合計 60 件である。その障害の内訳は、サービス全体が停止する重大なものが 9 件、機能の一部に限定的な問題が生じたものが 18 件、動作遅延に関するものが 12 件、その他（ユーザに実質影響の無い程度のもの）が 21 件である。その中で、教訓となる障害事例のいくつかを、本学がとった対処方法とともに、次節以降で具体的に報告する。

3.2.1 動作遅延障害の事例

前述の勤怠管理システムは、2011 年 10 月の本格稼働直後から、ユーザが急増する朝と夕方の時間帯に深刻な動作遅延を起こした。本節では、その事例の詳細を報告する。

勤怠管理システムは、その用途上、混雑時間帯の同時接続ユーザ数が非常に大きいのが特徴である。その後の原因調査において、SRP を経由しない場合や、SRP 経由であってもユーザが少人数の場合

には動作遅延が起こらないことから、大量の同時接続による SRP 側での膨大なデータ通信処理（高負荷）が問題の原因と推測された。

はじめは、SRP の負荷分散装置および各種サーバソフトウェアの設定変更やバージョンアップによる対処を実施したが、劇的な改善は見られなかった。そこで、最終的には、SRP の連携処理機構の変更を行い、ユーザが SRP 経由で勤怠管理システムに接続した際には、SSO によるユーザ認証のみを行い、その後のリバースプロキシ通信（ユーザと勤怠管理システム間の通信の中継）は行わず両者を直接接続することにした。この変更を実施した 2012 年 3 月 6 日以降は、SRP 側での膨大なデータ通信処理を根本的に削減することができ、実際、混雑時の動作遅延は改善した。なお、リバースプロキシ通信を行わないことで外部から攻撃を受けるリスクは高まるが、両者間が暗号化（SSL）通信であることと、学外からの勤怠管理システムへの接続は SRP 経由であっても禁止されているため深刻な影響はない。

3.2.2 サービス停止障害の事例

本節では、膨大なユーザの使用により SRP のサービス全体が停止した事例の詳細を報告する。

SRP にこの障害を誘発したのは、本学の教務系管理を一手に引き受ける学務情報システムであり、2013 年 9 月より稼働と連携を開始したばかりの新システムである。SRP と連携する一般的な情報システムは、ユーザが学外からの利用時にのみ SRP 経由での接続に限定し、学内 LAN からの利用時には SRP を一切利用せずに直接接続することも許可する運用ルールを採用している。しかし、学務情報システムはその重要さから安全性を重視し、学内 LAN からの利用時にも、その接続を SRP 経由に限定しているのが特徴である。

SRP のサービス全体が停止する障害は、学務情報システムでの後期授業の履修登録受付最終日である 10 月 11 日（金）19 時頃に起こった。はじめに、SRP を構成するサーバの再起動など基本的な対処を試したが復旧せず、その後、保守業者と連携した原因調査が行われた。その結果、SRP のデータベース（Oracle）サーバが毎日作成するリカバリファイルの容量が上限（8GB）に達していたことが原因と判明し、その上限を 10GB（後に 20GB）に拡張することで翌日の 3 時頃に復旧した。この日は、一日中、膨大な数の学生ユーザが SRP 経由で学務情報システムを利用し、リカバリファイルを増大させた。なお、後の検証によると、通常 1 日に作成されるリカバリファイルのサイズは 1GB 程度である。過去に同様な障害は発生していないことから、当日のデータ通信量は（おそらくユーザ数も）過去最大に達していたと推測される。

4 SRP 型システムを導入する際に考慮すべきこと

SRP のようなリバースプロキシ型認証連携システムは、他の情報システムと連携して動作することが前提のため、全体として十分な性能は発揮するためには、SRP と情報システムの双方が適切に動作する必要がある。また、SRP がサービス停止障害を起こした場合、その影響は連携する全ての情報システムに及ぶため、SRP と情報システムの双方の部署での情報共有と障害への共同対応が必要となる。

しかし、実際には SRP と情報システムは別々のシステムであるため適切な連携が難しい場合があり、単体で動作する情報システムでは起こり得ない障害や運用上の問題が発生し、その解決には経験的なノウハウが重要となる場合も多い。

以降では、本学でのこれまでの運用経験を踏まえ、大学において SRP と同様なリバースプロキシ型認証連携システム（SRP 型システム）を導入する際に考慮すべきことを提言する。

4.1 動作遅延障害への対処

本学では、SRP と新規に連携する情報システムを構築する場合、その情報システムの通信方式や利用形態などを事前調査し、必要に応じて SRP 側の改修や性能増強を行っている。また、情報システム側でも SRP との連携を前提にした認証/通信機構の設計を行なっている。そのため、SRP を経由した情報システムの動作自体には、問題が起こることはほとんど無い。しかし、情報システムによっては、データ転送量が大きいことなどが原因で、動作遅延が起こる場合がある。

動作遅延は、ユーザの操作性を損なう重大な問題である。そこで、本稿では、3.2.1 節の事例を踏まえ、SRP 型システムのデータ通信処理の負荷を減らすために、以下のことを提言する。

- 情報システム側は、ウェブブラウザのキャッシュを活用するなどの工夫により、ユーザと情報システム間でのデータ転送量を軽減する。
- ユーザが学内 LAN から SRP 型システムを経由して情報システムに接続した場合、それ以降の通信は、ユーザと情報システム間を直接通信させることも可能なように、SRP 型システムと情報システムを設計する。

4.2 サービス停止障害への対処

3.2.2 節で紹介した SRP のサービス停止障害の事例では、早期の復旧に失敗し、サービス停止が長期化してしまった。そのため、SRP のサービス停止中は、サービス再開を待つ連携情報システムの運用

部署とそのユーザに対して、復旧目処などの情報を断続的に発信した。しかし、連携情報システム数が年々増加していたことから、その手間と時間は膨大であり、しかも、担当職員には臨機応変的な判断が求められることから、その正確性や確実性にも不安があった。

本稿では、これらの経験を踏まえ、障害耐性の向上と障害発生時の影響軽減のために、以下のことを提言する。

- SRP 型システムは、ユーザ数やデータ通信量の増大に対してロバスト（頑強）に設計し、インパルス的な負荷の発生時にも、サービスの完全停止には至らないようにし、また、負荷減少後は自動復旧されるようにする。
- SRP 型システムには、状態監視/通知機能を組み込み、サービス停止リスクが高まった場合には管理者宛てに、また、サービスが完全に停止した場合には、連携情報システムを含む全ての関係者宛てに自動でメール通知されるようにする。
- 情報システム側は、SRP 型システムのサービスが停止した場合でも、単独でのサービス継続が可能なように設計する。
- SRP 型システムのサービス停止時の復旧作業フロー／マニュアルを、SRP 型システムと連携情報システムに関連する全ての部署が**共同**で作成する。

5 まとめ

本稿では、東北大学が導入し運用するリバースプロキシ型認証連携システムである SRP を紹介し、その障害履歴と対処方法を含めた運用状況を報告した。また、これまでの運用経験を踏まえて、大学において SRP 型システムを導入する際に考慮すべきことの幾つかを提言した。

本稿で示したように、他の情報システムとの連携を前提とする SRP のような情報基盤システムは、単独で動作する一般的な情報システムと較べて構築と管理が難しく、その適切な動作と運用のためには十分なリソースと学内横断的な協力体制、また、長期に渡るノウハウの蓄積が必要となる。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導入や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> (2013/10/30 アクセス)。
- [2] 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> (2013/10/30 アクセス)。