Vol.2012-CSEC-57 No.11
Vol.2012-IOT17 No.11
2012/5/10

全学認証サーバの負荷状況と負荷分散

伊東栄典[†]　笠原義晃[†]　藤村直美[‡]

近年，大学では全学的な認証基盤構築が進んでいる．筆者らが所属する九州大学でも全学共通 ID の発行および認証基盤を構築し，学内向け情報サービスの利用者認証を一元化している．認証基盤を利用するサービスの増加に伴い，LDAP 認証サーバの負荷が上昇している．中でも電子メール利用時の認証と，無線 LAN 接続時の認証が認証サーバの負荷を増大させている．本論文では，九州大学認証基盤における負荷状況の解析結果を述べる．また，負荷分散の方法を提案し，実際に負荷分散を適用した効果について，短期間ではあるものの，その結果を示す．

A study of LDAP load balancing for University ICT services

EISUKE ITO[†]　YOSHIAKI KASAHARA[†]
NAOMI FUJIMURA[‡]

Integrated user authentication platform may realize secure and easy use intra-institutional services. So, most institutions have integrated user account, and constructed internal authentication platform. The more clients depend on the central authentication server. The loads of the authentication server will become much higher. In Kyushu University, which authors belong, the load of the authentication server becomes very high because of authentication of e-mail and wireless network service. In this paper, we analyze the load condition of the authentication server, and study some load balancing.

1. はじめに

近年，大学では全学的な認証基盤構築が進んでいる．筆者らが所属する九州大学でも，2007 年 9 月から学内の全学生・全職員に向けて全学共通 ID を発行している[1]．この全学共通 ID は，学内向け情報サービスでの利用者認証を一元化するために制定したもので，新入生には ID を印刷した IC 学生証を，新任職員には紙カードに ID を印字したカードを発行・配付している．利用者サポート窓口も運用しており，パスワード忘れ・ID カード紛失・全学共通 ID の新規発行申請および再発行申請などに対応してきた．

2011 年 3 月には学術認証フェデレーション（学認）[2]にも参加し[3]，学外の電子ジャーナルの利用時に Shibboleth 認証を利用できるようになった．Shibboleth 認証を行う IdP は学内に設置されており，利用者認証要求は IdP を経由して全学の LDAP サーバで処理される．

全学共通 ID を利用するサービスは年々増加し，2011 年 12 月現在，21 種類のサービスで利用されている．多くのサービスで全学共通 ID が利用されるようになった結果，認証機能を提供する LDAP サーバの負荷が上昇した．特に電子メールと 802.1X での無線 LAN 接続認証の負荷が高い．高負荷で LDAP サーバが応答できずにサービスを利用できない事例も発生しており，LDAP 認証サーバの負荷分散が必要になっている．

本稿では，九州大学における LDAP 認証サーバの負荷状況を調査した結果と，その結果に基づく負荷分散手法の検討，分散化後の状況を報告する．まず第 2 節では本学の認証基盤の状況を説明する．第 3 節では LDAP サーバのログから分析した LDAP サーバの負荷ついて述べる．第 4 節で検討した負荷分散方式について述べ，最後の第 5 節でまとめと今後の課題を述べる．

2. 九州大学全学共通認証基盤

まず初めに，我々が所属する九州大学で提供している全学共通認証基盤[1,4]について説明する．

2.1 認証基盤構築の経緯

大学内には多数の情報サービスが存在している．個々の情報サービスは独立に構築されていたため，従来はそのサービスのための利用者アカウント（ID・パスワード）は独自に発行されていた．このため，情報サービスの増加に従い，様々な煩雑さを発生し，それらによる情報サービスを使った作業効率の低下，サービスの拡大や充実の妨げ，および情報サービスにおける安全性低下を招いていた．この状況を改善するため，大学を含む多くの組織で，組織内情報サービスの利用者アカウントを統合する動きが出た．

筆者らの属する九州大学では，学生の ID は情報サービスが拡充する 1995 年から学生番号（学籍番号）に基づく学生 ID で統合されていた．一方，職員については全学的な共通 ID が無かったため，2007 年に職員用の全学共通 ID を制定し，全構成員へ配付した．

2.2 学内構成員への ID 発行数

大学の主たる構成員は学生と教職員である．学生は，学部学生と大学院生からなる．正規の学生（正課生）以外に，研究生や留学生などの非正課生も在籍している．学生と教職員以外にも，特別研究員や，外部組織で雇用されている

[†] 九州大学　情報基盤研究開発センター
Research Institute for Information Technology, Kyushu University
[‡] 九州大学　芸術工学研究院
Department of Design, Kyushu University

方，訪問研究者など，様々な方が在籍している．九州大学における 2012 年 3 月現在の発行 ID 概数を表 1 に示す．

表 1　九州大学の ID 数（2012 年 3 月現在）

種類	ID 総数（概数）
正課生（学部生と大学院生）	18,000
非正課性	500
職員	9,000
派遣等	800

2.3 九州大学全学共通認証基盤の構造

図 1 に，2012 年 3 月現在の九州大学全学共通認証基盤を示す[1,4]．2012 年 3 月末現在，九州大学の全学共通 ID で利用できる学内向けサービスは 22 個である [4]．

図 1 に示すように，各サービスに提供する利用者認証用サーバとして LDAP サーバと Shibboleth サーバがある．代表的に使われている LDAP サーバは，OpenLDAP[5]で構成され ldap1 と ldap2 と名付けられた LDAP サーバ 2 台である．

代表 LDAP サーバ（ldap1, ldap2）の性能諸元を表 2 に示す．2 台とも仮想マシンとして構成している．

表 2　LDAP サーバ性能諸元

物理サーバ	
物理サーバ	NEC Eco Center Express5800/E120a
CPU	Quad Core Intel Xeon 2.3GHz ×2
Memory	4GB
HDD	160GB
VM	VMware ESXi 4
仮想マシンで構築した LDAP サーバ	
Memory	4GB
Disk	23GB
OS	Red Hat Enterprise Linux 5.8
LDAP	OpenLDAP 2.3.43

図 1 に示すように，上位の利用者管理システムから ldap1 へアカウントデータが投入されている．ldap2 は ldap1 の内容を複製するようになっており，サービスの可用性を高めている．履修登録や図書館系サービスの様なウェブ系サービスはこれらを用いている．

一方，事務用計算機システムや，低年次教育で使われる教育情報システムは，システム専用の Active Directory や LDAP サーバを保持しており，システム内の利用者認証は，内部の認証サーバを用いる構成となっている．これらのサーバにも上位システムからアカウントデータが投入されている．

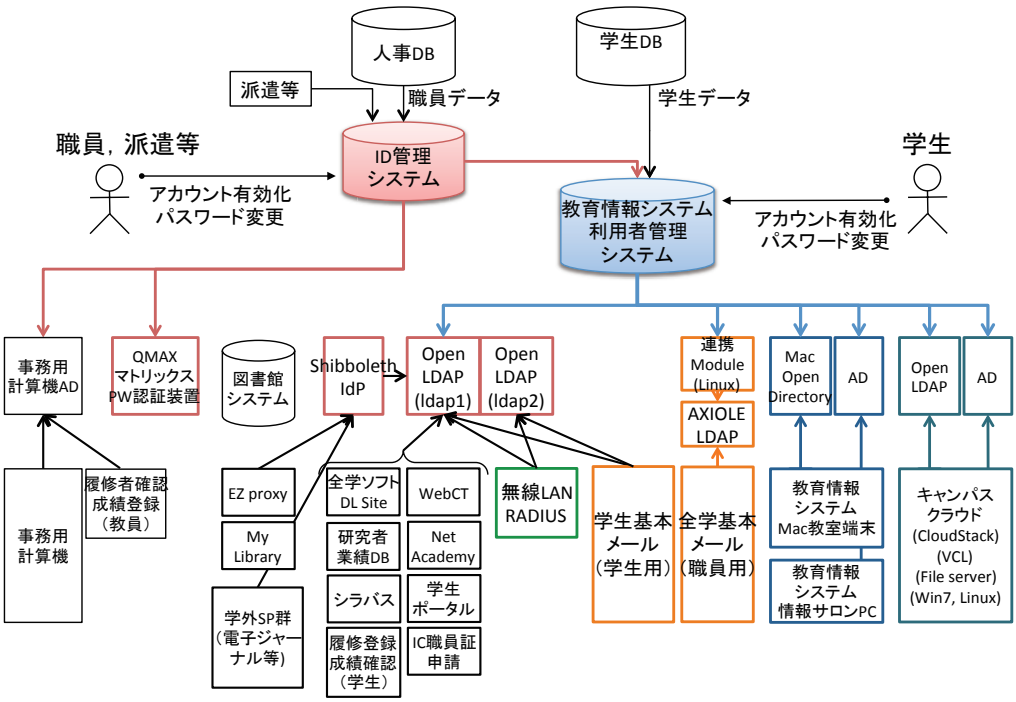

図 1　九州大学全学共通認証基盤の構成(2012 年 3 月現在)

3. 負荷状況および負荷分散

3.1 負荷の上昇

利用者認証に全学共通 ID を使うサービスが増えるにつれ, LDAP 認証サーバの負荷が上昇することとなった. 2012 年 1 月 25 日には，認証サーバの高負荷により，全学の e ラーニングシステム(Blackboard learning system, WebCT)の利用者認証失敗が発生した. 予備的な調査の結果, 認証サーバが高負荷となった理由は，学生基本メールサーバの認証要求と，無線 LAN の接続時認証であると推測された.

学生基本メールシステム[6]は，学内の全学生に対して提供しているメールサービスである．図 2 に大まかな構成図を示す．メール送信時には，迷惑メール送信を防ぐため，SMTP-AUTH によるユーザ認証を行なっている．メール受信には POP3 および IMAP4 を受け付けており，メーラで着信メールを受け取る際に利用者認証が行われる．これらの認証は，全学共通の LDAP サーバで行われる．

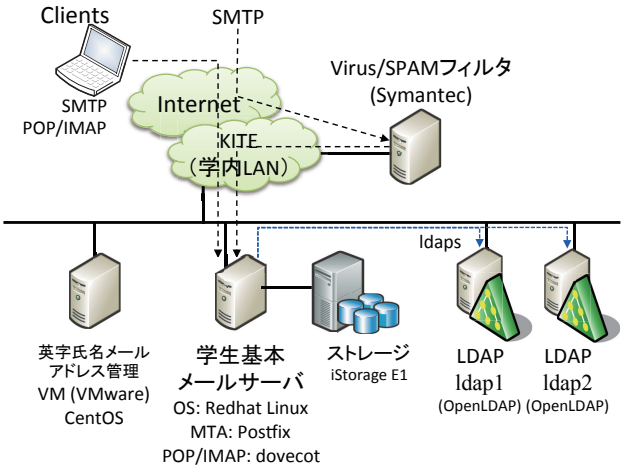

図 2　学生基本メールシステムの構成

次に高い頻度で認証要求を行うサービスは無線 LAN である．図 3 に大まかな構成を示す.

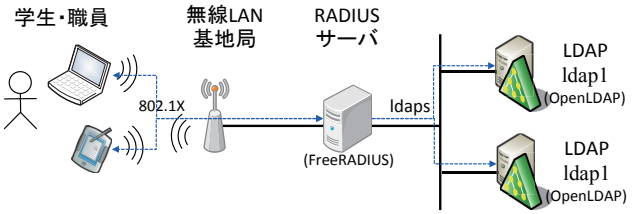

図 3　無線 LAN サービスの構成

従来からのモバイル PC に加え，現在では学生や教職員のスマートフォンと iPad 等のタブレット端末が増加している．スマートフォンやタブレット型端末には Wi-Fi（無線 LAN）接続機能がある．本学では全キャンパスに kitenet と名付けた無線 LAN サービスを提供している．kitenet では無線 LAN 接続時に 802.1X PEAP 方式での認証を要求している．図 3 に示すように，接続時の全学共通 ID での利用者認証は FreeRADIUS サーバ[7]を経由して LDAP 認証サーバへの問合わせとなる．スマートフォンやタブレット端末を使うたびに無線 LAN 接続が起こり，そのたびに認証要求が発生するため認証サーバの負荷が高くなる.

3.2 LDAP 認証サーバの負荷解析

LDAP 認証サーバのログから，認証要求の負荷状況を分析した．分析対象としたログの期間は 2011 年 12 月 1 日から 2012 年 3 月 11 日までである．表 3 に LDAP サーバのログから抜き出して分析対象とした LDAP アクションを示し，図 4 に 2 台の LDAP サーバが処理した数を示す.

表 3　分析対象とした LDAP アクション

種類	意味
ACCEPT	LDAP サーバへの接続数
Failed	(認証エラーで) LDAP 操作に失敗した数
BIND	ldap_bind を試みた回数
SEARCH	ldap_search を試みた回数

UNBIND 処理はリソースを開放してコネクションを切る操作で, ACCEPT に対応して発生するため, 数に考慮しない. Cmp など他の LDAP 操作は数が少なく，負荷分析に影響しないため省略した．Failed は各種操作で認証エラー(RESULT が err=49)になった回数で，ほとんどログイン認証のための一般ユーザによる BIND 失敗である．また，OpenLDAP のログには，BIND の後に ACCEPT が記録されている場合が極少数出現した．この原因が OpenLDAP にあるのか，syslogd にあるのか，それとも LDAP サーバが動作する仮想マシンでの時刻ズレによるものか分かっていない．不整合の件数は少ないため今回は無視した.

図 4 のデータから，全体としては ldap1 の処理件数が ldap2 より多いが，2012 年 1 月以前と以後で傾向が逆転していることが分かる．また, BIND, CONNECT の数は，日々の推移がだいたい一定数であること，2011 年 11 月までは ldap2 が多く 2012 年 1 月以降は ldap1 が多いことが分かる．また, ldap1 で最も処理数が多い日は 235 万件を超えた 2012 年 1 月 25 日であり，この日には学生から「WebCT へのログインで失敗する」との苦情が来ていた.

次に認証要求数の多い，学生基本メールと無線 LAN について調べる．表 4 に，2011 年 1 月における認証要求に関する ldap1 と ldpa2 の処理件数を示す．全件数と，学生基本メールおよび無線 LAN の件数および割合を示す.

表 4 から, 殆どの認証処理が学生基本メールと無線 LAN から来ていることがわかる．中でも学生基本メールの処理件数が多い．無線 LAN の処理は殆どが SEARCH 処理で，またコネクション数が少ないことが分かる．二つのサービスにおける認証処理について分析した.

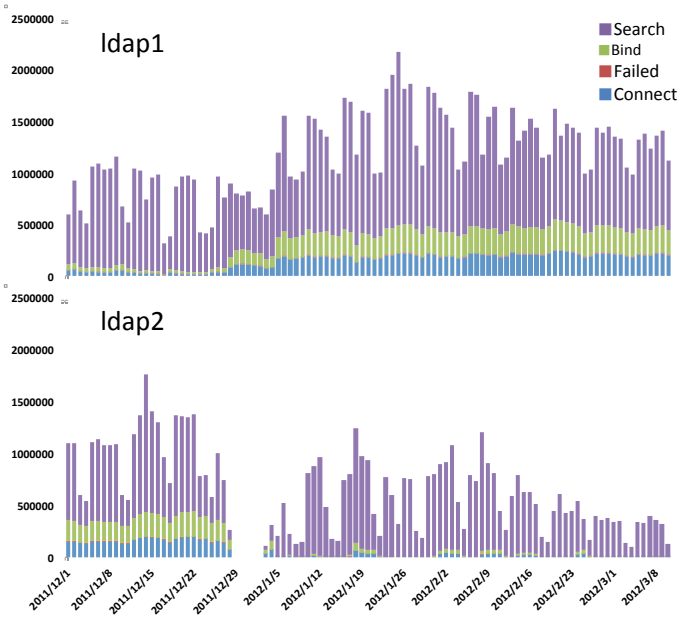

図 4　ldap1,ldap2 の処理数（2011/12/01～2012/03/11）

表 4　ldap1,ldap2 の処理件数（2012 年 1 月）

		CONNECT	Failed	BIND	SEARCH	合計
ldap1	ldap1 全体	5,385,500	167,250	6,580,029	29,455,706	41,588,485
	学生基本	4,732,197	153,811	5,890,494	14,002,143	24,778,645
	メール	87.87%	91.96%	89.52%	47.54%	59.58%
	無線 LAN	589	0	527	14,797,866	14,798,982
		0.01%	0.00%	0.01%	50.24%	35.58%
ldap2	ldap2 全体	353,127	13,491	393,171	14,917,005	15,676,794
	学生基本	337,708	6,055	372,345	1,625,293	2,341,401
	メール	95.63%	44.88%	94.70%	10.90%	14.94%
	無線 LAN	496	0	439	13,272,734	13,273,669
		0.14%	0.00%	0.11%	88.98%	84.67%

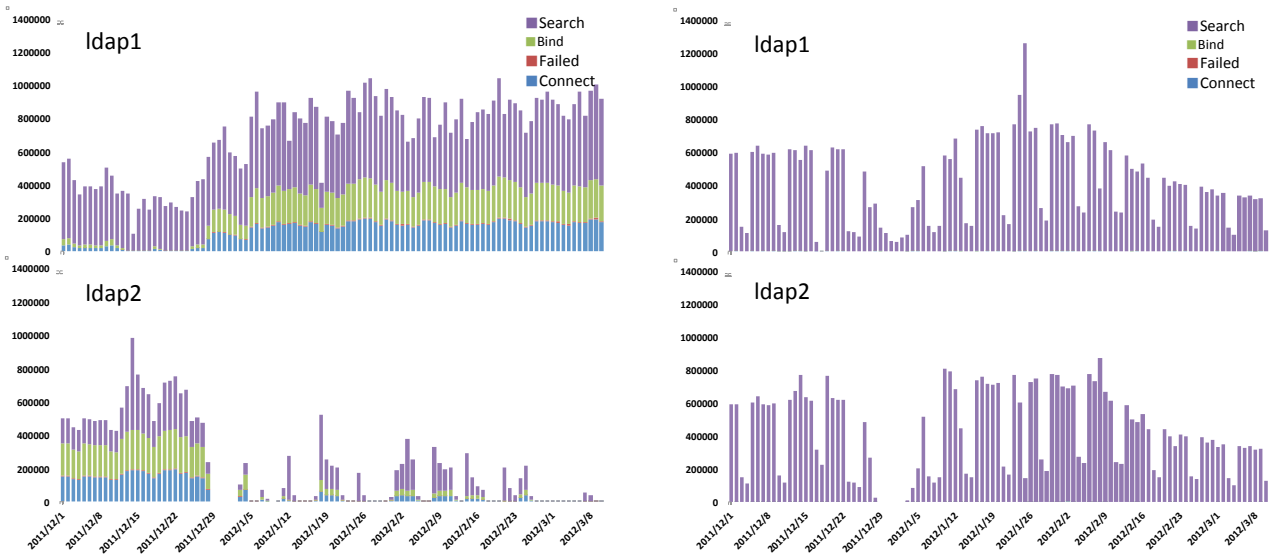

図 5　学生基本メール（左）および無線 LAN (kitenet)（右）からの ldap1,ldap2 の処理数（2011/12/01～2012/03/11）

3.3 メールサーバからの認証処理分析

図 5 の左側に学生基本メールサーバから送られる日毎の認証要求数を示す．表 4 から，学生基本メールから大量の CONNECT, BIND, UNBIND, SEARCH が来ることが分かる．本学の学生基本メールでは MTA に Postfix, POP/IMAP サーバに Dovecot を用いている．これらのサービスではユーザ認証に OS が提供する PAM 認証を使用している．PAM では pam_ldap を利用しており，認証要求が発生した単位で BIND を発行して利用者認証を行う．このため, POP, IMAP, SMTP-AUTH で接続する際に CONNECT と BIND/UNBIND が発生し，その数が多くなっている．

図 5 を見ると，一日約 2 万回の CONNECT，約 2 万回の BIND が定常発生している．その理由を調査したところ，原因は Gmail や Yahoo 等からのアクセスであった．Gmail 等は POP サーバを設定でき, 学生の中には本学の学生基本メールサーバに届いたメールを Gmail 側で POP 取得設定をする者がいる．Gmail は，利用者が実際に Gmail へログインしている／していないに関わらず，定期的（デフォルトでは 1 時間おき）に POP でのメール取得を試みる. その為，一定回数の POP アクセスが常にメールサーバに届き, それが LDAP 認証サーバへの認証要求回数となっている．これにより，曜日を問わず認証要求が定常的に発生している．

また，図 5 から認証に関するアクセスが，2011 年までは ldap2 に，2012 年からは ldap1 に偏っている．学生基本メールサーバで利用している nss_ldap や pam_ldap では，ldap.conf での host や uri の設定を参照している．これらの設定値はそのまま LDAP ライブラリ関数である ldap_open(host, port)あるいは ldap_initialize(ldp, uri)に渡される．これらの関数は，引数に空白で区切った複数のサーバ名を書けるものの，先頭に指定された LDAP サーバから順番に接続を試行し，接続できた LDAP サーバを使う．このため，先頭に指定したサーバのみに負荷が集中する．ldap1 と ldap2 の保守作業等の事情により, 2011 年まで ldap2 を先頭に指定していたため ldap2 の処理数が多く，2012 年から ldap1 を先頭にしたため ldap1 の処理数が増えることになった．

プライマリとして指定したサーバへの接続失敗した時以外, セカンダリ以降に指定したサーバは使われないため，負荷分散ができていないことが判明した．

3.4 無線 LAN の RADIUS サーバからの認証処理分析

図 5 の右側に無線 LAN の RADIUS サーバから送られる日毎の認証要求数を示す．この図を見ると，学生基本メールと異なり，無線 LAN では平日に処理が多く，週末と休日は少ないという周期が出ている．また二つの LDAP サーバへの処理数が，均等に分散していることも分かる．無線 LAN サービスで 802.1X 認証に用いている FreeRADIUS では，LDAP サーバの設定時に複数のサーバに対して redundant-load-balance という指定ができる．この設定では複数のサーバを round robin で使い，かつ一部が停止すると生きている LDAP サーバを使うようになっている．このため，2 台のサーバへの均等な負荷分散が実現している．

無線 LAN からの処理はほぼ SEARCH のみである．またコネクションの数が少ない．FreeRADIUS サーバは，認証サーバへの接続を複数確立して，それを長時間使い続けることができる．SEARCH が多く BIND が少ない理由は，pam_ldap とは認証方法が異なりユーザ ID とパスワードをつかった BIND 処理が不要なためである．本学の LDAP サーバでは sambaNTPassword 属性を提供している．ここに PEAP 認証に必要なパスワードのハッシュ値が入っているため, SEARCH で検索し MS-CHAP v2 で処理することで認証処理ができる．

無線 LAN の RADIUS サーバからは，現状ではできうる限りの負荷分散が実現していることが分かる．

4. 負荷分散方法の検討

負荷分散の方法として，以下の 3 つを検討する．

（1） 負荷分散装置の設置
（2） DNS ラウンドロビンによる分散
（3） TCP セッション再利用による CPU 負荷削減

4.1 負荷分散装置の設置

TCP やアプリケーション層の通信を分散する負荷分散装置（load balancer）を置き，その背後に複数の LDAP サーバを置く方法である．この方法は，負荷分散装置に充分な信頼性・可用性があれば，最も良い方法であろう．利用者側は負荷分散装置が代表するホスト名に対し, LDAP（LDAPS）アクセスを行えばよい．SSL アクセラレータが有れば，暗号化通信に関する暗号処理の負荷も軽減できる．

この方法の一番の問題は費用である．負荷分散装置は価格が高く，また SSL アクセラレータをつければ更に費用が高くなる．もう一つの問題として，負荷分散装置自体が壊れた場合，複数ある LDAP 認証サーバを全て利用出来なくなる．負荷分散装置の多重化によって解決可能だが，費用の問題はさらに大きくなる．

4.2 DNS ラウンドロビンによる負荷分散

DNS ラウンドロビンを使うと，一つのホスト名に対し複数の IP アドレスを順番に返すことが出来き, これにより複数サーバへのアクセス分散が可能になる．この手法を LDAP サーバでも適用できる．代表となる LDAP サーバの名前を宣言し，このホスト名に対して複数 LDAP サーバが持つ IP アドレスを返すようにする. 本学では ldap1 と ldap2 の二つを運用しているため，ldap.iii.kyushu-u.ac.jp という名前で ldap1 と ldap2 のアドレスが交互に返るようにすれば，負荷分散が可能になる. DNS とクライアントの設定変更で済むためコストがかからない．

しかし，この方法は LDAP クライアントがホストと IP

アドレスの対応をキャッシュしている場合はうまく動作しない．他にも DNS での負荷分散として SRV リソースを利用した手法もあるが，クライアントが未対応の場合も多い．

4.3 TCP セッション再利用による CPU 負荷削減

本学の学生基本メールは，認証やユーザ情報取得のたびに接続を使い捨てている．そのため TCP ハンドシェイクの処理や，TLS（ldaps）接続する際の公開鍵暗号処理が毎回発生する．メールサーバへのアクセスが多くなれば，TCP ハンドシェイクおよび TLS の数も増え，この処理だけでも負荷が重くなる．これは nss_ldap や pam_ldap の仕様になるため，これらを使う限り負荷を避けられない．nss_ldap による負荷は nscd（Name Service Caching Daemon）[8]によるキャッシュによりある程度軽減されるが，pam_ldap による認証はキャッシュされないという問題点もある．

認証要求に付随する接続処理の負荷を下げるには，学生基本メールサーバ側で，リモート ID 認証メカニズムに関するより新しい実装である SSSD（System Security Services Daemon）を使う方法も考えられる．SSSD を使うとコネクションが SSSD Data Provider プロセスからの一つになると記述されており[9]，一度接続した通信コネクションを使いまわすことが可能になる．SSSD には認証情報のキャッシュが実装されており，LDAP サーバへの負荷軽減が期待できる．ただしコネクションが一つであるため複数の LDAP サーバへ query を分散することはできない．

実際に pam_ldap/nss_ldap から SSSD に移行する場合，現状のシステムから設定から大きく変更されることになるため，実運用しているサービスに適用するためには充分な事前テストが必要となる．

5. 負荷分散後の状況

2012 年 3 月 8 日より，DNS ラウンドロビンの設定を行い，学内の各サービス担当者へ通知した．特に LDAP サーバへの負荷の偏りが大きかった学生基本メールで， 2012 年 3 月 12 日より，DNS ラウンドロビンによるアクセスに切り替えた．具体的には，学生基本メールサーバの ldap.conf で，代表 LDAP サーバ名（ldap.iii.kyushu-u.ac.jp）で LDAP 参照するように設定した．また，同時に nscd.conf で nscd による hosts のキャッシュを無効にした．

図 6 に，2012 年 3 月 12 日から 2012 年 3 月 30 日時点までの学生基本メールサーバからくる ldap1,ldap2 の処理件数を示す．

図 6 を見ると 3 月 15 日から認証に関する処理が分散している．ただ，DNS ラウンドロビンおよび nscd の設定変更は 3 月 12 日に行ったにもかかわらず，実際に効果が出てきたのは 3 日後の 3 月 15 日からになっている．その原因はわかっていないため，今後調査する必要がある．

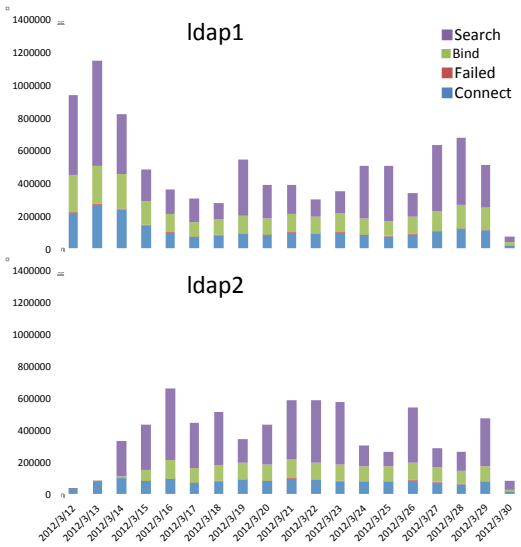

図 6　学生基本メールからの ldap1,ldap2 の処理数
（2012/03/12～2012/03/30）

6. おわりに

本稿では，九州大学における LDAP 認証サーバの負荷状況を調査した結果と，その結果に基づく負荷分散手法の検討および分散化後の状況を述べた．サーバのログ分析により，学生基本メールサービスからの認証要求が多いことが分かった．負荷分散方式として三つの方法を考え，当面の対処として DNS ラウンドロビンを使った負荷分散方法を実際に行った．その結果，とりあえずの対処ではあるものの，負荷分散ができていることが分かった．今後は，学生基本メールや無線 LAN サービスがそれぞれ独自の LDAP 認証サーバを導入・運用するようにし，大学全体の LDAP 認証サーバを使わないようにすることで根本的な解決を図ることを計画している．

参考文献

1) 菅尾貴彦, 戸川忠嗣, 太田美和, 橘倉聡, 平野広幸, 伊東栄典, 市川広大, 先立英喜: 全学共通認証基盤サービスの手続きの電子化について, 第 30 回 全国共同利用情報基盤センター 研究開発連合発表講演会 研究開発論文集, pp.77-86 (2008).
2) 学認, https://www.gakunin.jp/docs/fed
3) 伊東栄典, 片岡真, 牧瀬ゆかり: Shibboleth 認証基盤構築と学術認証フェデレーションへの参加 −今後の e リソースサービス基盤にむけて−, 九州大学附属図書館年報 2009/2010, pp.11-15 (2010). http://hdl.handle.net/2324/18319
4) 九州大学 SSO ポータル, https://sso.kyushu-u.ac.jp/
5) OpenLDAP, http://www.openldap.org/
6) 藤村直美, 戸川忠嗣, 笠原義晃, 伊東栄典: 姓名をベースにしたアドレスによる学生基本メールの運用について, 情処研報 2011-IOT-14(10), pp.1-6 (2011).
7) FreeRADIUS, http://freeradius.org/
8) nscd (name service cache daemon), http://linux.die.net/man/8/nscd
9) SSSD, http://docs.fedoraproject.org/en-US/Fedora/15/html/Deployment_Guide/sect-SSSD_User_Guide-Introduction-SSSD_Features.html, accessed on Mar.16, 2012.