クラウドと実機におけるメーリングリストサーバの運用について

クラウドと実機におけるメーリングリストサーバの運用について

太田諭之
静岡大学　技術部　情報支援部門

１．はじめに

静岡大学技術部において、メーリングリストサーバをクラウドと実機にて運用している。メーリングリストサーバは、一つのメールアドレスで複数のメールアドレスに同時にメールを送付するためのサーバである。メーリングリストサーバ内の*/etc/aliases*（メールエイリアス）ファイルを編集することで複数の送付先を決定できる仕組みである。例を挙げると、A さんが一つのメールアドレスで B さんと C さんのメールアドレスに同時にメールを送ることができる。この場合、一つ一つのメールアドレスを指定しなくてもよい。“aaa@example.com”というメールアドレスを例にみてみると、”aaa”はアカウントでメールサーバ内においてユーザを区別するために使用されるものである。@以降の”example.com“はメールアカウントを管理しているドメイン名である。静岡大学は、”shizuoka.ac.jp”のドメイン名である。ドメイン名の前にメールサーバ名（ホスト名）が入り（サブドメインとも呼ばれる)、処理の分散とアカウント名の自由度を確保している。静岡大学技術部では” tech.shizuoka.ac.jp”と”shizuoka.ac.jp”の前に、”tech”が入る。

２．メーリングリストサーバについて

現在、管理しているメーリングリストサーバの一覧を下図に示す。

種類	運用開始	送信範囲	最大送信数
静岡大学技術部メーリングリストサーバ（クラウド*1）	2007年6月23日（当初は実機にて2013年11月からｸﾗｳﾄﾞ）	静岡大学技術部職員（浜松分室・静岡分室）	43名
静岡大学工学部メーリングリスト*2サーバ（実機）	2011年3月6日 2011年10月（ﾒｰﾙﾏｶﾞｼﾞﾝ）	静岡大学工学部教員・事務職員 （一般：静岡大学工学部ﾒｰﾙﾏｶﾞｼﾞﾝ送付時*3に限る）	231名 264名（ﾒｰﾙﾏｶﾞｼﾞﾝ）

表の内容は2017/12/22現在

図１　管理しているメーリングリストサーバの一覧

表中（図 1）の注釈は下記の通り。

*1 静岡大学 情報基盤センター(http://www.cii.shizuoka.ac.jp/)及び株式会社 ITSC 様 (https://www.itsc-ltd.co.jp/) が保守。

*2 静岡大学工学部総務係より工学部メーリングリスト中の構成員について追加・削除の依頼があり、主に月はじめの人事異動時にあり、対応している。

*3 静岡大学工学部メールマガジン（年に 4 回）送付時のみメルマガ用のメーリングリストアドレスを有効化。送付終了後はメーリングリストを無効化している。

技術部メーリングリストサーバはクラウドサーバを使用している。メーリングリストは技術部職員（静岡キャンパス・浜松キャンパス）が構成員である。2007 年から使用しており、当時の OS は Vine Linux

3.1（Red Hat 系 Linux)を使用しており実機にて運用していた。その後、Fedora Core を経て現在は Cent OS を使用している。2013 年 11 月よりクラウドへ移行した。工学部メーリングリストサーバは実機を使用しており、メーリングリストは教員・事務職員が構成員である。また工学部メールマガジン（年に 4 回発行、現在まで第 25 号を掲載（2017 年 12 月現在））を主に学外の一般の方のメールアドレスへ送付するため、メールマガジン用のメーリングリストアドレスを 2011 年 10 月より使用している。

技術部メーリングリストサーバ（クラウド）のスペックについて述べる。実機が手元に無いため、コマンド（システム名等を表示するコマンド *uname –a* を使用した）から参照した情報によると、OS は、工学部メーリングリストサーバ（実機）と同様 CentOS release 6.9 (Final)、CPU：インテル Xeon E5-2640 0 @ 2.50GHz、メモリ容量：1.9GB、ハードディスク容量：200GB である。メーリングリストサーバとしてのクラウドサーバの使用のため、情報基盤センター宛に利用申請を行い、使用している。

一方、工学部メーリングリストサーバ（実機）のスペックは、機種：Dell PowerEdge T130 1 タワーサーバ、OS は CentOS release 6.9 (Final)、CPU：インテル Celeron G3930 @2.90GHz、メモリ容量：8GB、ハードディスク容量：500GB である。

ここでメールサーバとメーリングリストサーバについて述べる。

アカウント名は、メールを管理している SMTP、POP3 サーバが個人を区別するために利用する固有の名前である。一方、ドメイン名は、相手のメールボックスを管理しているプロバイダや会社などを識別するために使われる。メールの送受信には、一般的に SMTP と POP3 という 2 つのプロトコル（ネットワーク上においての通信に関する規約）が使用される。メールを送信するときは、メールを転送するためのプロトコルである SMTP が使用され、メーラから SMTP サーバへメールが送信される。メールを受け取った SMTP サーバは宛先のドメインでメールを処理している SMTP サーバに対して、同じ SMTP によりメールを転送する。受信したメールは個人ごとのメールボックスへ保存する。ここまでが SMTP サーバの役割である。また、メールを受信するときは、メールボックスからメールを読み出すための専用サーバが用意されており、ここで使用されるプロトコルが POP3 である。POP3 サーバは、クライアントからの要求に応じて、保存されているメールをメーラ（Microsoft Outlook Express、Mozilla Thunder bird など）に転送する。POP3 以外には APOP や IMAP4 が使用される場合がある。

メーリングリストサーバはメールサーバとしての運用とは異なり、指定されたメールアドレスへ転送する機能を有しているサーバの運用となる。しかし、外部からのアタックは同様に受ける恐れがあり、脅威に晒されているため運用には留意する必要がある。

３．メールにおいての脅威

SPAM メールやなりすましメールなどの脅威が広がっている。メーリングリストサーバにおいても対策が必要である。工学部メーリングリストサーバは、学内にてルータ配下に設置されており、運用している。大学内においての送信に限定されている。DMZ（非武装地帯）と呼ばれる、ファイアウォールによってネットワークの内部および外部から隔離された区域にメーリングリストサーバが設置されている。

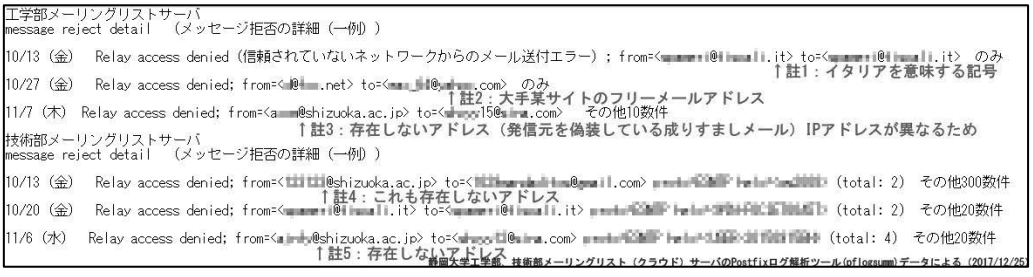

図 2　メッセージ拒否の一例（一部画像を加工しています）

図 2 はメールが拒否されている原因の一例を示したものである。註 1 から註 5 までの説明文はあくまでも可能性の一つを示している。様々な解釈が他にも考えられる。

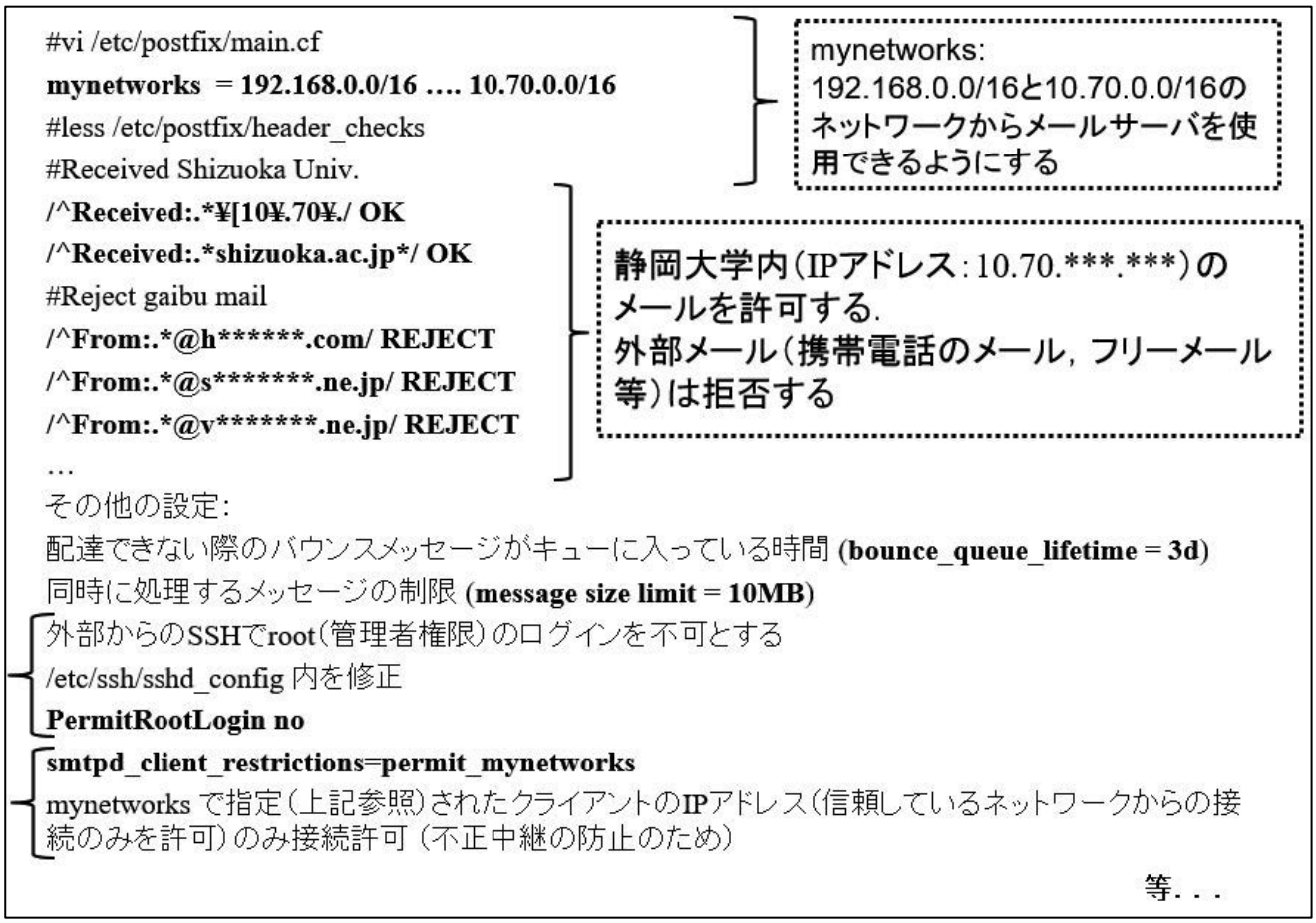

図 3　サーバのセキュリティ設定についての一例

図 3 はサーバの設定を実際に示した一例である。図中において、特定できる表示を伏せ字にしている。

工学部メーリングリストのアドレス追加・削除は、静岡大学工学部総務係の担当より人事異動の際に連絡があり、随時対応している。メーリングリストのアドレス一覧は、Microsoft Excel にて管理しており、個人名とメールアドレスのリストが記されている。このリストに情報を追加・削除することで容易にメーリングリストの管理を行うことができる。なお、このファイルは読み込みの際にパスワードを掛けておりセキュリティを強固なものとしている。

４．クラウドサーバと実機サーバの違い

クラウドサーバ:

メリット	デメリット
OSのアップデートは業者が対応している	直接、実機がないためリモートのログインのみ
サーバ実機がないため節電となり、場所もとらない	大学外にサーバが設置されていることがある

外部からのアタックは両者とも常に受けている！

実機サーバ:

メリット	デメリット
直接端末でコマンドから操作可能	自らシステムアップデートを頻繁に行う必要がある
学内ネットワークの設置によりセキュリティが比較的高く保たれる	長期休暇（年末年始、夏季休暇など）はセキュリティ対策のためサーバを停止しておく必要がある

図 4　実機サーバとクラウドサーバの違い

クラウドサーバと実機サーバの違いを図 4 にまとめた。クラウドサーバは、OS のアップデートについては業者に対応頂いている。実機サーバは、直接端末でコマンドから操作可能である（GUI（Graphical User Interface）環境もインストールされている）、端末故障時（BIOS 電池切れ、HDD 故障）は実機がある場合は予備機と差し替えることによりすぐに対応可能である。

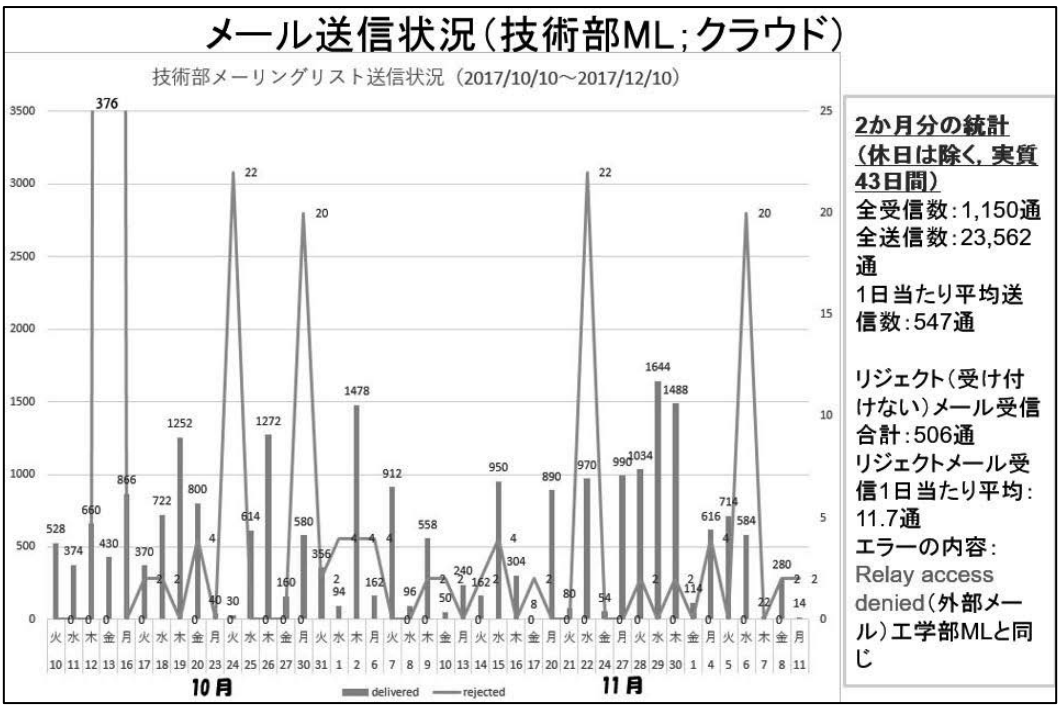

図 5　メール送信状況（技術部メーリングリストサーバ（クラウド））

技術部メーリングリストサーバ（クラウド）において送信したメールの数（棒グラフ；左縦軸で単位は「通」）と何らかの理由によりリジェクト（受け付けない）されたメールの数（折れ線グラフ；右縦軸で

単位は「通」）の合計を図 5 に示した。集計期間は、2017 年 10 月から 12 月までの 2 ヶ月間（土曜日・日曜日・祝日を除く）である。全体送信数は、クラウド : 23,562 通、実機 : 43,212 通である。

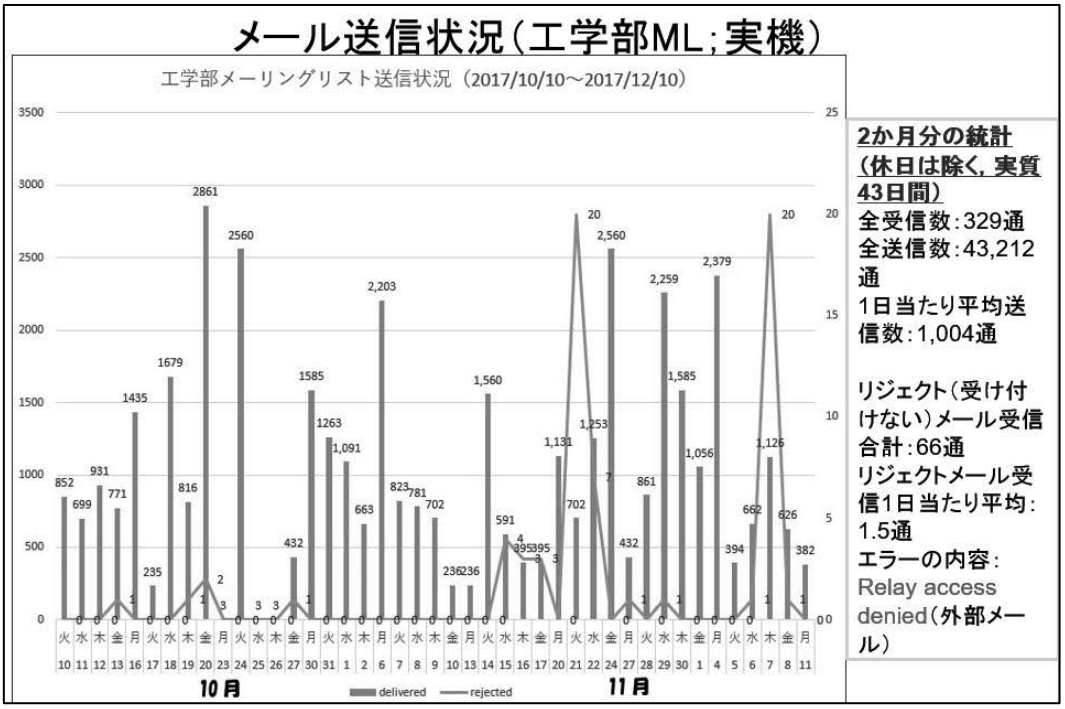

図 6　メール送信状況（工学部メーリングリストサーバ（実機））

工学部メーリングリストサーバ（実機）においても図 6 に示した。技術部メーリングリストサーバ（クラウド ; 図 5）と異なり、メールがリジェクトされる回数（折れ線グラフ）が少ない頻度であることが分かる。1 日当たりの平均をみると、技術部メーリングリストサーバ（クラウド）は、11.7 通であるのに対し、工学部メーリングリスト（実機）は 1.5 通であることがわかる（1 日でリジェクトされているメール受信数が技術部メーリングリストサーバ（クラウド）では最大 1 日 376 通にのぼることもあった。）。この原因については現在調査中である。

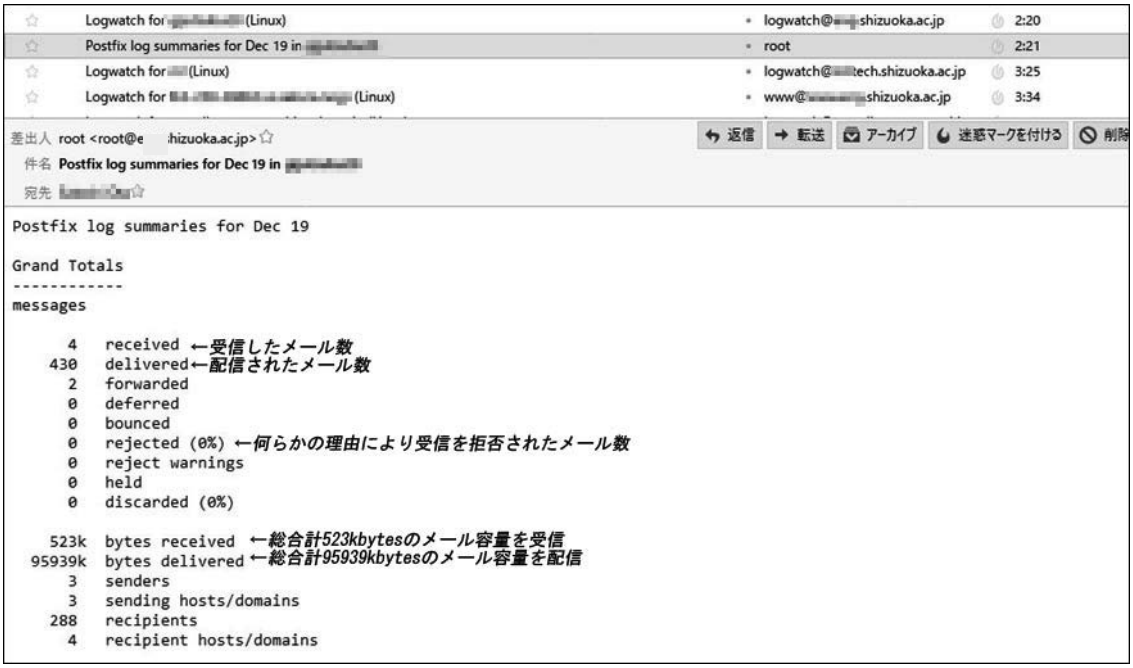

図 7　Pflogsumm よりメールにて送られたメールログファイルの要約情報

メールの受信・送信状況を確認するために Pflogsumm というプログラムを動作させている。前日のメー

ルログファイル（デフォルト：*/var/log/maillog*）からサマリ（要約）を作成して管理者へメールを毎日決まった時間に送信される（図 7 参照）。毎朝 2:50 ころ[1]送信される仕組みである。当初、メーリングリストサーバを実機にて運用した際の OS は Vine Linux（2007 年当時技術部メーリングリスト運用のため、2013 年 11 月よりクラウドサーバにて運用）であったが、現在はサーバスペックの高性能化、メーリングリストサービスの提供が静岡大学情報基盤センター[2]からされ、運用が容易となった。一方でサーバを狙った悪意のある攻撃も巧妙化・増加しており日々の対策が求められる。毎日のシステムアップデート、メールログの監視を引き続き注視していき、安心・安定したメーリングリストの運用を心掛けたい。

５．まとめ

登録されているメーリングリストのメールアドレスは、2018 年 3 月から旧メールアドレス (***@ipc.shizuoka.ac.jp) から新メールアドレス(***@shizuoka.ac.jp)へ移行し、旧メールアドレスは 2017 年度末（2018 年 2 月から 3 月）に廃止予定である。そのため、メールエイリアスのアドレスを旧メールアドレスから新メールアドレスに書き換える必要がある。静岡大学情報基盤センターが提供するメーリングリストサービスの使用を検討する。ただし、学外のメールアドレス登録制限や登録人数の制限がある（一例：メンバー数 100 名上でメンバー範囲が学外を含む場合ほぼ運用リスク値の値によりサービス提供が不可能の場合がある。）。また、メールを送信する際のメールサイズが 1MB 以下の制約がある。

メーリングリストサーバの OS について、CentOS release 6.9 から CentOS release 7.0 への乗り換えの検討を行う。

以上、様々なメーリングリストの運用方法があるが、それぞれ持つ能力を生かした方法で今後、運用していきたい。

６．参考文献・引用文献

[1] 株式会社アイドゥ：「インターネット&Web しくみ事典」株式会社ワークスコーポレーション（2004）， P.82-83.

[2] 荒木靖宏：「Postfix 詳細－MTA の理解とメールサーバの構築・運用－」株式会社オーム社, (2006).

[3] 静岡大学 情報基盤センターホームページ ，＜http://www.cii.shizuoka.ac.jp/>（2017 年 12 月 20 日データ取得）

[4] 辻秀典：「できる PRO CentOS 6 サーバ」株式会社インプレスジャパン，（2013）.

[5] デル株式会社(Dell Japan)ホームページ，<http://www.dell.com/jp/business/p/poweredge-t130/pd>（2017 年 12 月 21 日データ取得）

[6] 日経 BP ムック：「すべてわかるセキュリティ大全 2018」日経 BP 社，（2017）.

[7] 八木毅ら：「実践サイバーセキュリティモニタリング」コロナ社，（2016）.

[8] Postfix ログ解析ツール導入(pflogsumm) CentOS で自宅サーバ構築, <https://centossrv.com/postfix-pflogsumm.shtml>，（2017 年 12 月 20 日データ取得）

[9] Postfix Log Entry Summarizer “pflogsumm.pl “ <http://jimsun.linxnet.com/postfix_contrib.html>（2017 年 12 月 21 日データ取得）

[10] SPED 理工系英和辞典　小学館, japanknowledge LIB ホームページ：<http://japanknowledge.com/library/>　（2017 年 12 月 21 日データ取得）

[1] 毎正時（例：2:00 や 3:00 など）を避ける理由は、他のサービスの実行と被らないようにするためである。

[2] 静岡大学情報基盤センターメーリングリストサービス（http://www.cii.shizuoka.ac.jp/in/?page_id=10137）（2017 年 12 月 21 日現在）