

利用記録の解析によるメールサービスの利用状況

鳩野 逸生

神戸大学 情報基盤センター
hatono@kobe-u.ac.jp

神戸大学 情報基盤センター
hatono@kobe-u.ac.jp

Usage of University Mail Service Analyzed by Logging Information

Itsuo Hatono

Information Science and Technology Center, Kobe Univ.

概要

神戸大学では、2008年から全構成員を対象としてメールサービスを提供している。本稿では、2011年から2015年における学生の学部および入学年度毎の利用者数、転送状況、利用場所、海外からの利用状況について、送受信記録により推定した事例について述べる

1 はじめに

神戸大学においては、1997年に全学生、2008年に全構成員を対象として情報基盤センターのアカウントを発行し、その一環としてメールの送受信サービスを提供している。前年度に、送受信記録が残っている2011年度から2014年度までの利用状況と不正利用監視について述べた [1]。

本稿においては、2011年度から2015年度の期間についての学生向けメールサービスの利用状況について、メールサービスの利用者数、転送状況に加え、海外からの利用状況、IPアドレスから推定できるメールサービスの利用場所・状況について報告する。

2 メールサービスの提供環境 [1]

神戸大学においては、全学生、教職員に対して、(1) ログイン ID、(2) ネットワーク ID、(3) メール ID という3種類の ID を発行している。各 ID は、それぞれ(1)のログイン ID は、教育用端末や主要な情報システム(学生の場合は、学務システム、教職員の場合は、会計システムなど)、(2)のネットワーク ID は、VPN 接続サービスや、全学無線 LAN サービス等のネットワーク接続サービス、(3)のメール ID は大学が提供するメールサービスでメールの送受信に利用するためのものであり、それぞれ異なった ID/パスワードをつけることができる。また学生ユーザに関しては、3ヶ所の転送先のメールアドレスを設定することができる。

メール送信は、Postfix[3]において SASL[4]を用いて PLAIN, Digest-MD5, Cram-MD5、メール受信は、dovecot[5]を用いて POP3, IMAP/PLAIN, APOP, Digest-MD5, Cram-MD5 であり、学外からは通信路の暗号化(SMTPS, POP3S, IMAPS)のみサポートしている。Webメールの機能は提供していない。

3 メールサービスの利用状況

3.1 年度、入学年度別学生ユーザの利用状況

表1, 2および3に、2011年から2015年までの入学年度毎の利用者数の推移を示す。ただし、各年度において、9月から翌年3月までのメールの受信記録から集計している。集計に当たっては、各メールユーザ ID を用いた pop/imap アクセスがかかるか、あるいは転送設定されていてかつメールが実際に転送されているユーザ数をカウントしている。後期のみを集計対象としたのは、一年次前期に全員履修の情報リテラシー授業で全員メールを授業内で利用するため、必ずしも利用の実態を反映していないと考えられるためである*1。

表1, 2および3から、2014年度までと同様に、2015年度を含めても理系学部の方が社会系、人文系学部に比べて利用者の比率(学年定員との比率)が高い傾向がある。ただし、人文系学部2のみは利用率が理系学部に比べても高い。

理系学部が高いのは、レポート等授業でメールを利用する頻度が高いためではないかと推定され

*1 昨年度の報告と同様。

表1 社会学部の利用状況

社会学部1(定員260)							
年度	2009年度生	2010年度生	2011年度生	2012年度生	2013年度生	2014年度生	2015年度生
2011	156	153	152				
2012	99	132	146	83			
2013	37	128	150	79	104		
2014	11	42	119	153	83	112	
2015	7	13	36	121	171	115	89

社会学部2(定員270)							
年度	2009年度生	2010年度生	2011年度生	2012年度生	2013年度生	2014年度生	2015年度生
2011	126	94	84				
2012	109	127	146	93			
2013	43	115	149	129	103		
2014	11	29	121	153	131	94	
2015	2	11	31	133	194	142	73

社会学部3(定員180)							
年度	2009年度生	2010年度生	2011年度生	2012年度生	2013年度生	2014年度生	2015年度生
2011	141	90	76				
2012	118	102	60	85			
2013	59	66	75	67	81		
2014	17	21	73	96	61	90	
2015	4	8	13	88	112	75	92

表2 人文系学部の利用状況

人文系学部1(定員140名)							
年度	2009年度生	2010年度生	2011年度生	2012年度生	2013年度生	2014年度生	2015年度生
2011	50	69	97				
2012	60	38	79	102			
2013	29	61	56	75	132		
2014	4	37	77	61	114	113	
2015	0	9	30	60	96	92	106

人文系学部2(定員280名)							
年度	2009年度生	2010年度生	2011年度生	2012年度生	2013年度生	2014年度生	2015年度生
2011	231	230	142				
2012	231	243	253	140			
2013	85	251	246	230	158		
2014	19	88	249	256	256	189	
2015	7	20	81	244	265	262	190

人文系学部3(115名)							
年度	2009年度生	2010年度生	2011年度生	2012年度生	2013年度生	2014年度生	2015年度生
2011	37	55	60				
2012	42	42	49	54			
2013	13	47	47	64	60		
2014	3	10	45	49	67	57	
2015	0	3	8	53	70	70	53

表3 理系学部の利用状況

理系学部1(定員150)							
年度	2009年度生	2010年度生	2011年度生	2012年度生	2013年度生	2014年度生	2015年度生
2011	112	121	69				
2012	81	122	101	83			
2013	32	90	113	99	105		
2014	6	31	86	105	104	75	
2015	1	7	35	94	124	101	89

理系学部2(定員112)							
年度	2009年度生	2010年度生	2011年度生	2012年度生	2013年度生	2014年度生	2015年度生
2011	68	89	91				
2012	63	57	75	79			
2013	27	64	63	77	72		
2014	14	33	64	79	78	119	
2015	4	16	19	75	68	95	91

理系学部3(定員140名)							
年度	2009年度生	2010年度生	2011年度生	2012年度生	2013年度生	2014年度生	2015年度生
2011	139	91	67				
2012	141	141	100	100			
2013	59	141	166	109	76		
2014	10	53	153	155	119	57	
2015	2	15	48	144	146	97	71

理系学部4(定員540名)							
年度	2009年度生	2010年度生	2011年度生	2012年度生	2013年度生	2014年度生	2015年度生
2011	413	388	353				
2012	357	433	425	376			
2013	187	404	472	484	322		
2014	28	179	445	475	426	343	
2015	13	51	201	440	456	426	367

理系学部5(定員200名)							
年度	2009年度生	2010年度生	2011年度生	2012年度生	2013年度生	2014年度生	2015年度生
2011	143	167	183				
2012	106	145	181	190			
2013	43	110	151	186	126		
2014	13	36	112	190	114	171	
2015	6	14	39	154	155	170	122

る。特に利用率が高い人文系学部2は、人文系に分類されるが理系的な授業も多くある教育内容であることが影響していると思われる。詳細な理由は、利用記録に含まれる「標題」や「添付ファイル」の状況を調査することにより推定することは技術的に可能であるが、解析に当たってメールの内容を見ることになるため実施していない。

3.2 メールサービスの利用場所/形態

受信サーバへの接続元 IP から判明した学生ユーザのメールサービス利用場所(形態)を表4に示す。表4において、「学内」は神戸大学内の IP からのアクセスであることを示す。教育用端末からの利用数がほぼ一定であるのに対して、2014年度から2015年度にかけて全学無線 LAN からの利用が急増していることが特徴的である。全学無線 LAN の利用状況から、スマートフォンからのメール受信が急増しているためであると思われる*2[2]。

一般に、一部のベンダーが提供しているフリーメールサービスにおいては、フリーメールサービスのサーバから、pop/imap によるメール受信や送信が可能であるが、表4中の「学外メールサービス」は主なフリーメールサービスからのメール受信アクセスがあるユーザ数を集計したものである。多くは、フリーメールサービスベンダーが提供するメールアプリをスマートフォン上で利用しているものと思われる*3。ただし、アクセス元が Amazon 社の AWS に割り当てられている IP であると思われるものが少なからず存在する。これも何らかのスマートフォン上のメールサービスのものであると推測しているが、実際のアプリ名などは特定できていない。

3.3 転送設定先の状況

表6に、おもな転送先の状況を示す。gmail への転送が増加しているのが分かる。また、大学の受信メールサーバにはアクセスせずに転送だけを行っているユーザも一定数(約3,000名)存在している。

表5に、転送設定されていてかつ実際にメールが配送された転送先のドメインの上位20番目までを示す。gmail, yahoo.co.jp および各携帯電話会社のメールサービスへの転送が上位を占めている。この表からも、携帯メール以外のフリーメールサービスに関しては、gmail への集中が進んでいる傾向が見受けられる。

現在ほとんどの学生がスマートフォンを所持しており、いわゆる「パソコン用メアド」のメール読み書き

*2 特にスマートフォンからのメール利用は推奨していない。

*3 この数の中には、自分自身でフリーメールからの pop 等を設定しているユーザも含まれていると思われるが、大多数はスマートフォンアプリユーザであると推測している。

表4 メール利用場所/形態

	学内			外部メールサービス				国内外	
	教育用端末	全学無線LAN	その他	Gmail	Hotmail	my.com	amazonaws	国内(学外)	国外(学外)
2011年度	6960	752	2898	139	20	0	0	1991	407
2012年度	6859	1002	2947	119	23	0	0	2256	614
2013年度	7161	1227	2964	129	17	0	0	2570	677
2014年度	7456	1895	2968	125	14	0	22	2840	769
2015年度	6596	2968	2901	145	16	76	67	3461	928

表5 転送先の設定状況(上位19ドメイン)

順位	2011年度		2012年度		2013年度		2014年度		2015年度	
	転送先	設定者数								
1	yahoo.co.jp	1298	gmail.com	1314	gmail.com	1668	gmail.com	1860	gmail.com	2089
2	gmail.com	957	yahoo.co.jp	1130	yahoo.co.jp	1053	yahoo.co.jp	896	yahoo.co.jp	784
3	docomo.ne.jp	538	ezweb.ne.jp	561	ezweb.ne.jp	595	ezweb.ne.jp	618	ezweb.ne.jp	640
4	ezweb.ne.jp	527	docomo.ne.jp	517	docomo.ne.jp	522	docomo.ne.jp	504	docomo.ne.jp	502
5	softbank.ne.jp	242	softbank.ne.jp	262	softbank.ne.jp	273	softbank.ne.jp	327	softbank.ne.jp	319
6	hotmail.co.jp	194	softbank.jp	235	softbank.ne.jp	222	softbank.ne.jp	214	kobe-u.ac.jp	225
7	softbank.jp	186	hotmail.co.jp	158	kobe-u.ac.jp	180	kobe-u.ac.jp	184	softbank.ne.jp	222
8	kobe-u.ac.jp	161	kobe-u.ac.jp	146	hotmail.co.jp	143	hotmail.co.jp	138	hotmail.co.jp	116
9	hotmail.com	158	hotmail.com	120	hotmail.com	99	hotmail.com	87	icloud.com	90
10	vodafone.ne.jp	101	ocn.ne.jp	76	eonet.ne.jp	78	eonet.ne.jp	62	hotmail.com	71
11	eonet.ne.jp	91	eonet.ne.jp	74	zaq.ne.jp	68	icloud.com	53	outlook.jp	57
12	ocn.ne.jp	90	zaq.ne.jp	73	ocn.ne.jp	57	zaq.ne.jp	46	zaq.ne.jp	46
13	zaq.ne.jp	90	vodafone.ne.jp	68	vodafone.ne.jp	49	ocn.ne.jp	41	eonet.ne.jp	45
14	so-net.ne.jp	57	so-net.ne.jp	54	so-net.ne.jp	45	so-net.ne.jp	31	ocn.ne.jp	42
15	ybb.ne.jp	41	yahoo.com	34	biglobe.ne.jp	34	live.jp	29	yahoo.com	30
16	nifty.com	40	ybb.ne.jp	32	live.jp	34	biglobe.ne.jp	28	live.jp	23
17	biglobe.ne.jp	35	biglobe.ne.jp	30	ybb.ne.jp	31	vodafone.ne.jp	27	outlook.com	23
18	plala.or.jp	33	nifty.com	30	yahoo.com	29	me.com	23	so-net.ne.jp	22
19	yahoo.com	33	live.jp	28	nifty.com	28	outlook.jp	22	biglobe.ne.jp	20
20	live.jp	24	plala.or.jp	24	me.com	24	yahoo.com	22	vodafone.ne.jp	20

表6 転送先の設定状況まとめ

	Gmailへ転送	hotmailへ転送	その他学外転送	学内転送	転送のみ(pop/imapによる受信無)
2011年度	957	352	3835	183	2887
2012年度	1314	278	3588	167	2878
2013年度	1668	242	3524	198	3011
2014年度	1860	225	3307	194	2955
2015年度	2089	187	3223	236	3070

が可能であるにもかかわらず、受信にあたって制約が多い携帯電話会社のいわゆる「携帯メール」への転送が、2011年から現在に至るまでほとんど変化がないことが注目される。若い世代では、連絡手段としてメールからSNSなどのメッセージングサービスに移行していると言われていたが、まだ携帯メールを連絡先として認識されているということを示唆していると思われる。

4 海外からの利用状況

4.1 海外からの利用者数

表7に、接続元のIPアドレスが存在していると思われる国毎に集計したものを示す。ただし、逆引きした結果フリーメールサービスからのアクセスと判断されるものに関しては除いている。最上位のUnited Statesに関しては、前述したgmailなどのメールサービスからのアクセスが逆引きできずに海外からのものと判定されているものが含まれている*4。

アメリカ合衆国を除けば神戸大学において留学生が多い国からの利用数が多くなっている。2015年度には、海外からのアクセス自体が多くなってきており、学生の海外における活動が活発化していることが推測される。

*4 過去のIPに対して定義されていたFQDNが、本年度(2016年度)においては変更されていた可能性があるため。

4.2 海外からの発信監視

メール送受信用のIDおよびパスワードが漏洩した場合、多くは海外に割り当てられたIPからほぼ同時に複数の国から発信される。神戸大学においては、いち早く不正利用を検知するために約2時間毎に、複数の国から発信されるメールIDの監視を行い、警告するプログラムを開発して適用している[1]。

別の日に送付された警告メールの内容例を4件表2に示す。この中で、user1, user2, user3は実際にSPAMメールの発信が行なわれていた。しかし、user4は、発信国は4カ国に渡っているにも関わらず、実際に発信されているメールの宛先等から正常なものであると判断された。発信元IPをFQDNとwhoisにより調査したところ、Germanyを発信元とするIPは、ドイツの通信会社のものであるため、user4は、レンタルWifiルータを所持してポルトガルとイギリスを訪問したものであると思われる。

このように、複数の国で利用できるレンタルWifiルータ等を所持している場合は、Wifiルータベンダに依存するため海外からの発信がユーザ自身によるものかどうかの判断を行うには、送信先により判断する必要がある。

4.3 海外からの受信監視

海外からのメール発信の正当性を総合的に判断するために、受信に関しても海外からのものに関する監視を行っている。図1に、メールの利用状況を集約するプログラムの出力例を示す。図中の、“Not observed”は、送信または受信が観測されなかったことを意味する。受信に関しては、学内あるいは自宅に設置したPC等から電源がONの状態になると本人がいない場合でもpop/imapがかかるような状態である可能性が

表7 海外 (の IP) からの利用状況

2011年度		2012年度		2013年度		2014年度		2015年度	
国名	人数								
United States	177	United States	179	United States	182	United States	150	United States	262
China	27	China	34	China	52	China	71	China	79
France	23	Korea, Repu	30	Korea, Repu	40	Korea, Repu	62	Korea, Repu	74
Korea, Repu	22	Germany	28	Taiwan	38	France	40	Taiwan	69
Italy	14	Italy	28	France	36	Taiwan	40	Italy	41
Germany	11	Taiwan	28	Italy	34	United Kingd	34	United Kingd	41
Taiwan	9	France	24	United Kingd	30	Germany	29	Germany	30
Philippines	8	United Kingd	21	Germany	26	Italy	29	Hong Kong	28
Switzerland	8	Hong Kong	18	Netherlands	19	Malaysia	25	France	25
Thailand	8	Thailand	18	Hong Kong	16	Netherlands	25	Guam	20
United Kingd	7	Malaysia	12	Thailand	14	Thailand	25	Spain	20
Belgium	6	Qatar	12	Belgium	12	Hong Kong	22	Thailand	20
Netherlands	6	Spain	12	Australia	11	Indonesia	20	Australia	19
Singapore	5	Switzerland	12	Spain	11	Philippines	18	Philippines	18
Australia	4	Austria	11	Finland	10	Australia	17	Qatar	17
Cambodia	4	Singapore	11	Indonesia	10	Qatar	17	Singapore	16
Canada	4	Finland	10	Austria	9	Spain	15	Canada	15
Hong Kong	4	Indonesia	10	Singapore	9	Belgium	14	Belgium	14

メール ID	送信	受信	転送先
xxxx430X@stu.kobe-u.ac.jp	Not observed	学内, 国外 (Cambodia)	
xxxx001X@stu.kobe-u.ac.jp	Not observed	国外 (United States), 国外 (China),	
		外部メールサービス (Gmail)	
xxxx060X@stu.kobe-u.ac.jp	Not observed	国外 (Korea, Republic of), 国外 (Hong	
		Kong), 国内 (学外),	
		外部メールサービス (Gmail), 国外 (
		Singapore)	
aaa@ky.kobe-u.ac.jp	国外: United States, 国内, 国外:	Not observed	yyy@zz.xx
bbcc@xx.kobe-u.ac.jp	Germany		uuu@xx
	国外: Thailand	学内	
zzz10stu.kobe-u.ac.jp	国外: Switzerland	国外 (Switzerland)	
zzz20stu.kobe-u.ac.jp	国外: United States	国外 (United States)	l1@n.jp
zzz30stu.kobe-u.ac.jp	学内, 国外: United States	学内, 国外 (United States)	

図1 メール ID の外国からの送受信状況の例

```

2016年9月aa日検出
ユーザID 国名
user1@x.kobe-u.ac.jp: Azerbaijan, India, Armenia, Vietnam,
United Kingdom, United States, China,
Thailand, Italy, Taiwan

2016年9月bb日検出
ユーザID 国名
user2@x.kobe-u.ac.jp: Bulgaria, Nigeria, Vietnam
% 2016年8月cc日検出
ユーザID 国名
user3@x.kobe-u.ac.jp: Belarus, United Kingdom, Indonesia, Norway,
(略)
Russian Federation, Estonia

% 2016年8月dd日検出
ユーザID 国名
user4@x.kobe-u.ac.jp: United Kingdom, Portugal, Germany
    
```

図2 多国からの発信警告例

あり、受信 IP だけではユーザがメールを受信している場所を特定することは困難であると考えられる。例えば、図1のxxxx430X@stu.kobe-u.ac.jpは、カンボジアと学内からアクセスが観測されているが、学内あるいはカンボジア国内に設置されているPCから定期的に受信動作がかかっている可能性がある。また、xxxx060X@stu.kobe-u.ac.jpは、同一日に韓国、香港、シンガポール、国内から受信が観測されているが、この情報からだけでは受信場所を特定することは困難であり、双方とも経過観察が必要となる。

5 まとめ・今後の課題

本稿では、2011年度から2015年度の期間についての学生向けメールサービスの利用状況について、メールサービスの利用者数、転送状況に加え、海外からの利用状況、IPアドレスから推定できるメールサービスの利用場所・状況について報告した。

その結果、(1) 携帯メールを連絡先として利用している学生は一定数存在、(2) フリーメールへの転送先はgmailが増加の傾向にある、(3) メール送受信に際しては通常のメールソフトだけでなく、スマートフォン等の「まとめ読みメールアプリ」によるものが増加しつつある、ことなどが判明した。2016年9月のシステム更新で、メール送受信ログに、imapにおける端末情報および送信におけるUser-Agentの情報も出力するように設定を変更している。今後は、利用しているメールソフト等の集計等も行っていく予定である。

参考文献

- [1] 鳩野: メールサービスの利用状況と不正利用監視, 2015年度大学ICT推進協議会年次大会講演論文集, 2015.
- [2] 鳩野: 全学無線LAN利用ログ情報の解析と応用, 情報処理学会研究報告 (IPJSig Technical Report), 2015-IOT-31, 2015.
- [3] <http://www.postfig.org/> (2016年10月現在)
- [4] <http://asg.web.cmu.edu/sasl/index.html> (2016年10月現在)
- [5] <http://www.dovecot.org/> (2016年10月現在)