メールサービスの利用状況と不正利用監視

鳩野 逸生

神戸大学 情報基盤センター
hatono@kobe-u.ac.jp

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 2014 年における学生の利用状況を学部毎に行った事例について述べる．さらに，メール ID の不正利用検知を目的としたプログラムを開発し運用しているので概要を報告する．

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．一方で，情報機器の利用状況は激変しており，連絡手段もいわゆる携帯メールから, SNS における Messenger サービスまで多様化していると言われている．本稿では，学生ユーザを対象として神戸大学情報基盤センターのメールシステムの利用記録が残っている 2011 年度から 2014 年度において，メールシステムを利用したと推定されるユーザ数の年度ごとの推移を部局毎に行い利用状況の分析を行ったので報告する．

また，大学が提供するメール用アカウントは，迷惑メールの大量発信に不正利用される場合も少なくない．神戸大学においても，過去数年にメールアカウントが不正利用されたと見られるインシデントが発生している．このような状況に対処するため，神戸大学では，一定時間ごとにメールの発信状況を監視して一定条件を満たすユーザアカウントを不正利用された可能性があるものとして警告する仕組みを導入している．さらに, 不正利用をさらに早期に発見するため，外国からの送受信の状況を表示するプログラムを開発し利用しているので報告する．

2 メールサービスの提供環境

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．これは，各サービスを利用する際の状況がサービスによってかなり異なると考えられるため，一つの ID が漏洩することですべてのサービスの不正利用につながるリスクを低減することを目的に導入されたものである．

メール送信は，Postfix[1] において SASL[2] を用いて PLAIN, Digest-MD5, Cram-MD5, メール受信は，dovecot[3] 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．

3 学生ユーザの利用状況

3.1 年度・学部毎の利用者数の状況

表 1, 2 および 3 に，2011 年から 2014 年まで，入学年度毎の利用者数を示す．ただし，各年度において，9 月から翌年 3 月までのメールの利用記録から集計している．集計にあたって, 各メールユーザ ID を用いた pop/imap アクセスがかかるか，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．

表 1, 2 および 3 から，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く，理系学部 2 は極端に低い．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

Table 1 社会系学部の利用状況

社会系学部1 (学年定員 270名)

年度	H9年度生	H10年度生	H11年度生	H12年度生	H13年度生	H14年度生
2011	158	154	156			
2012	103	132	147	85		
2013	38	130	155	81	104	
2014	11	42	120	153	84	113

社会系学部2(学年定員 260名)

2011	127	94	84			
2012	108	128	147	94		
2013	44	121	152	129	103	
2014	11	30	125	154	132	95

社会系学部3(学年定員 180名)

2011	142	91	78			
2012	124	103	62	86		
2013	59	69	77	69	81	
2014	17	21	75	98	63	91

Table 2 人文系学部の利用状況

人文系学部1(学年定員 140名)

2011	51	69	98			
2012	60	39	80	102		
2013	30	62	57	77	132	
2014	4	38	77	62	115	113

人文系学部2(学年定員 280名)

2011	233	231	148			
2012	232	243	253	143		
2013	88	253	248	230	159	
2014	19	89	249	257	256	190

人文系学部1(学年定員 115名)

2011	37	56	60			
2012	42	43	50	54		
2013	13	48	47	64	62	
2014	3	10	46	51	67	58

Table 3 理系学部の利用状況

理系学部1(学年定員 150名)

2011	114	121	69			
2012	83	123	101	83		
2013	33	92	114	100	105	
2014	6	32	89	107	104	75

理系学部2(学年定員 272名)

2011	70	91	96			
2012	64	69	78	80		
2013	28	67	69	78	74	
2014	15	35	67	81	81	119

理系学部3(学年定員 140名)

2011	140	91	69			
2012	141	141	100	101		
2013	61	141	166	109	77	
2014	10	54	154	155	120	58

理系学部4(学年定員 540名)

2011	414	390	354			
2012	360	435	427	377		
2013	191	407	473	484	325	
2014	28	181	446	476	427	344

理系学部5(学年定員 200名)

2011	143	167	183			
2012	108	145	181	190		
2013	45	111	153	186	126	
2014	13	38	114	190	115	171

```
Subject: Security Alert on SMTP.kobe-u.ac.jp! Found
   suspicious users whose mail passwords have cracked!!
From: smtpAlert@yyyy.kobe-u.ac.jp
To: sraff@yyy.kobe-u.ac.jp
Date: Sun, 26 Jul 2015 23:00:01 +0900 (JST)
X-Mew: No MIME-Version

ログファイル：/var/log/SYSLOG/2015/07/26/beniitotombo.log
Sun Jul 26 23:00:01 2015:
     smtp のパスワードがクラックされた可能性があるユーザがいます！

以下のユーザ ID から 1 日に 3ヶ国以上の国からの送信要求があります!
ユーザ ID 国名
abc@xxx.kobe-u.ac.jp: Belarus Hong Kong Thailand Brazil
                  Italy India Ukraine Spain Russian Federation
                  Ireland Netherlands Hungary Austria
                  United Kingdom  Finland Poland France
                  Canada Kazakhstan United States Taiwan
                  Denmark Portugal Germany
                  Iran, Islamic Republic of Vietnam
                  Virgin Islands, British Turkey China
当日の外国からのアクセス集計
Austria 1
Belarus 1
Brazil 1
(略)
Vietnam 2
Virgin Islands, British 1
```

Fig. 1 多国からの発信警告例

めであると推定される．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．また入学年度により顕著な差がある場合も見受けられるが，原因は不明である．

近年は，学生は学生間の連絡にメールを利用せず SNS のメッセージサービスを利用していると言われているが, 2011 年-2014 年の利用傾向は大きな差は見当たらないことから, 大学におけるメール利用は，大学の教育・研究にのみ用いられていると推測される．

3.2 転送設定先の状況

表 4 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 19 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．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」への転送がまだ依然として多いことが傾向として見られる．

4 不正利用監視

4.1 多数国からの発信監視

2012 年頃から，メール ID/パスワードの流出によるメールの不正送信が年数件発生している．不正発信が行なわれる際の特徴として，

- 大量のメールが発信される．
- 多くの国から同時に発信される．

が観測された．この状況に対して，一定時間毎にメール ID 毎に発信元 IP の国情報を調査し，3 カ国以上の発信が一日に行なわれた場合警告するプログラムを開発し運用している．Fig.1 に警告メールの例を示す．本プログラムは, 2013 年 11 月より利用しており，不正送信インシデントすべてを検知した．しかし，一日 3 カ国という条件は，ヨーロッパ等短い時間で多国を訪問可能な地域の場合誤検知する可能性がある．そのため，最終的にインシデントであると判断する際には，送受信情報を目視している [1].

4.2 外国からの送受信監視

不正送信インシデントにおけるメール ID の不正利用の状況を検知した日時から遡って分析したところ，多数の国から大量発信が行なわれる前に不正送信と見られる少数のメールが外国の IP から発信される傾向があることが判明した．取得したメール ID とパスワードが実際に利用可能かどうかテストしているものと推測される．不正利用を早期発見するためには，この「少数の不正発信」を発見する必要がある．

このような状況を発見することを目的として，各メール ID の送受信における送信元 IP を分類して表示するプログラムを開発した．Fig.2 に出力の例を示す．この中で，外国からのみ送信が行なわれている，あるいは送受信が国内/学内で行なわているにもかかわらず送信に外国からのものがあるメール ID が不正送信の疑いがあるものとして抽出可能である．Fig.2 では yyy2@opal.kobe-u.ac.jp, yyy3@port.kobe-u.ac.jp が該当する (後に送受信記録の確認により不正送信と断定). しかし，メール受信は，学内等に設置された固定 PC から継続して受信動作が行なわれている可能性があり，最終的な判断には送受信記録の確認が必要である．

本プログラムの利用開始以降，ほとんど場合において大量発信が行なわれる前に不正送信を検知している．

5 まとめ・今後の課題

本稿では，神戸大学におけるメールの利用状況およびメール ID 不正利用検知のために開発したプログラムについて述べた．メール不正利用に関して，該当者に対してパスワード漏洩経路に関して聞き取り調査を行ったが，漏洩経路の特定には至らなかった．また，利用されていたパスワードは十分に複雑であった場合も多く，しかも大規模な辞書攻撃も観測されていなかっ

[1] Postfix/Dovecot のログから送受信記録を簡易に検索・表示するプログラムを開発している．

Table 4 転送先の設定状況 (上位 19 ドメイン)

2011年度		2012年度		2013年度		2014年度	
転送先	人数	転送先	人数	転送先	人数	転送先	人数
yahoo.co.jp	1274	gmail.com	1321	gmail.com	1692	gmail.com	1887
gmail.com	985	yahoo.co.jp	1123	yahoo.co.jp	1052	yahoo.co.jp	907
docomo.ne.jp	559	ezweb.ne.jp	575	ezweb.ne.jp	602	ezweb.ne.jp	623
ezweb.ne.jp	542	docomo.ne.jp	543	docomo.ne.jp	527	docomo.ne.jp	505
softbank.ne.jp	242	softbank.ne.jp	257	i.softbank.jp	282	i.softbank.jp	326
hotmail.co.jp	196	i.softbank.jp	241	softbank.ne.jp	223	softbank.ne.jp	217
i.softbank.jp	192	hotmail.co.jp	158	kobe-u.ac.jp	175	kobe-u.ac.jp	184
kobe-u.ac.jp	163	kobe-u.ac.jp	145	hotmail.co.jp	146	hotmail.co.jp	141
hotmail.com	160	hotmail.com	119	hotmail.com	100	hotmail.com	91
vodafone.ne.jp	102	ocn.ne.jp	78	eonet.ne.jp	76	eonet.ne.jp	58
zaq.ne.jp	91	zaq.ne.jp	74	zaq.ne.jp	67	icloud.com	53
eonet.ne.jp	90	eonet.ne.jp	73	ocn.ne.jp	59	zaq.ne.jp	45
ocn.ne.jp	89	vodafone.ne.jp	70	vodafone.ne.jp	50	ocn.ne.jp	40
so-net.ne.jp	59	so-net.ne.jp	54	so-net.ne.jp	45	so-net.ne.jp	31
ybb.ne.jp	41	yahoo.com	36	live.jp	37	live.jp	28
nifty.com	38	biglobe.ne.jp	31	biglobe.ne.jp	35	biglobe.ne.jp	27
biglobe.ne.jp	37	nifty.com	30	yahoo.com	30	vodafone.ne.jp	27
yahoo.com	33	ybb.ne.jp	30	nifty.com	29	me.com	23
plala.or.jp	32	live.jp	27	ybb.ne.jp	29	outlook.jp	23

メール ID	送信	受信	転送先
xxx1@people.kobe-u.ac.jp	Not observed	国内 (学外), 国外 (United States)	
xxx2@people.kobe-u.ac.jp	Not observed	国外 (Switzerland), 国外 (France)	
xxx3@crystal.kobe-u.ac.jp	Not observed	国外 (United States)	eeee@mac.com
xxx4@tiger.kobe-u.ac.jp	Not observed	国外 (Malaysia)	
yyy1@stu.kobe-u.ac.jp	国外: Switzerland	Not observed	
yyy2@opal.kobe-u.ac.jp	国外: Egypt, 国内	学内, 国内 (学外)	jjjj@gmail.com
yyy3@port.kobe-u.ac.jp	国内, 国外: Saudi Arabia, 学内	国内 (学外), 学内	kkk@gmail.com
zzz1@stu.kobe-u.ac.jp	国外: Switzerland	国外 (Switzerland)	
zzz2@stu.kobe-u.ac.jp	国外: United States	国外 (United States)	
zzz3@stu.kobe-u.ac.jp	国外: United States	国外 (United States)	lll@ezweb.ne.jp
zzz4@stu.kobe-u.ac.jp	国外: Switzerland	国外 (Switzerland)	
zzz4@stu.kobe-u.ac.jp	学内, 国外: United States	学内, 国外 (United States)	

Fig. 2 メール ID の外国からの送受信状況

た．以上のことから，パスワード, ID の流用した別のサイトから流出したものであると推測している．

今後は，パスワード利用に関してユーザに対する啓蒙を強化すると共に，検知プログラムの改良を行う予定である．

参考文献

[1] http://www.postfig.org/ (2015 年 10 月現在)

[2] http://asg.web.cmu.edu/sasl/index.html (2015 年 10 月現在)

[3] http://www.dovecot.org/ (2015 年 10 月現在)