

S25R およびオープンソースツールを用いたメールゲートウェイサービス運用

針木 剛¹⁾

1) 京都大学

hariki.tsuyoshi.3r@kyoto-u.ac.jp

Mail gateway service operation using S25R and open source tools

Hariki Tsuyoshi¹⁾

1) Information Dept., Kyoto Univ.

概要

京都大学では 2002 年より部局のメールサーバ向けにウイルスチェック機能を有するメール中継サービスを運用している。2015 年からシマンテック社の Messaging Gateway を用いて全 45 台の仮想マシンで構成された大規模なシステムで運用していたが、2021 年 S25R とオープンソースツールを用いた小規模で内製化したシステムに更新し、更新費用の大幅なコストカットを実現した。本稿では 2021 年に構築したシステムの詳細と約 3 年間の運用で発生した問題点とその対応、さらに 2024 年にセキュリティ強化の観点からメールホスティングサービス用途で導入したアプライアンス機器へシステム移行した経緯と作業について詳細に述べる。

1 はじめに

京都大学では全構成員向けのメールサービス導入以前から部局や研究室が独自サブドメインでメールサービスを運用し、学内に多くのメールサーバが稼働していたため、2002 年にそれら機器に流入するウイルスメールやスパムメールを排除するためメール中継サービスを運用を開始した。

2012 年に開始した学生向けのメールサービスは Microsoft 社のクラウドサービス (Live@edu) であったため中継サービスと連携することはなかったが、教職員向けのメールサービスは 2010 年にオンプレでサービス開始当初から中継サービスを継続的に利用しており、2015 年に BCP 対策として群馬県のデータセンタにシステムを移行した際もデータセンタ内にメール中継システムを追加構築したため、学内とデータセンタで合わせて仮想マシン 45 台の大規模なシステムとなった。また、2013 年から部局や研究室メールサーバ集約を目的としてメールホスティングサービスを開始し、学生メールや教職員メールへの転送機能やメーリングリスト機能の提供を開始したが、このサービスにも中継サービスが利用された。

2020 年にこのメール中継サービスの更新を控え次期システムの検討を行ったが、同じ予算内で更新予定のネットワーク機器の更新費用が高騰し、且つ予算全体の減額もあり、認証やメールなどのサーバ関連のシ

ステムにコストを掛けることが困難であることが判明した。この時点で、教職員向けのメールサービスは 2019 年に Google 社のクラウドサービス (GMail) への移行が済んでおり、またメールホスティングサービスは中継サービスと連携せず独自システムに更新予定のため、サービス規模は大幅に縮小が可能であった。更にサービス内容を見直して、必要最低限の機能を内製でシステム構築しサービスを移行する方針とした。

2 メール送信システム

2.1 既存サービスと移行方針

既存サービスでは「mailrelay.kuins.net」及び「send-mail.kuins.net」「sc-filt.kuins.net」の 3 種類のメール中継サーバ名を提供していたが、下記の方法で利用されていた。

1. 部局メールサーバの中継先
2. メール送信機能を有する Web サーバの中継先
3. 複合機などプライベート IPv4 アドレスで運用する機器の送信サーバ
4. 同じくプライベート IPv4 アドレスの個人パソコンのメールアプリの送信サーバ
5. 「sc-filt.kuins.net」に限り個別の転送先アドレスに「foo%example.net@sc-filt.kuins.net」を指定すると「foo@example.net」に中継

部局メールサーバの中継先として運用することでユー

ザの送信メールだけでなくユーザの受信メールの外部への転送メールも中継することになり、スパムチェックで検知し除外できなかったそれらのメールを数台分の IP アドレスに集約して送信していたため、IP アドレスの評価が下がりブラックリストに掲載され大学全体で送信不可となる問題が複数回発生していた。商用のシマンテック社の Messaging Gateway を用いても完全にスパムを排除することは難しく、今後同様の被害を発生させないため、リスク分散し部局メールサーバ自身から直接送信してもらう対応に変更した。

今回のシステム更新で 1 を対象外とするため「接続元機器を京都大学内のプライベート IPv4 アドレス、メール宛先を京都大学内メールアドレス (@*kyoto-u.ac.jp) に限定」という制限を加えた。また転送先が限定されたためウイルスやスパムチェック機能は削除した。この変更は 2 や 3 や 4 にも影響があるため利用者には事前に十分に説明し対応していただいた。また 5 のアドレス変換機能については利用件数が数件程度であったため廃止とした。

利用対象を限定したため個別にサーバを用意せずに、従来から稼働している学外接続用の HTTP プロキシや SOCKS プロキシを稼働しているプロキシサーバの仮想マシン上に学外接続用のメール機能を付与する形で実装を行った。

2.2 新サービス設定詳細

プロキシサーバ自体のファイアウォールに京都大学内のプライベート IPv4 アドレスからのメール送信である TCP の 25 番を受け付ける許可を追加し、メールサーバ Postfix に設定 1 を追加した。なお大量送信による遅延障害が発生したため、平常時の実際の送信件数から流量制限の値を定めた。

設定 1 送信設定

```
--/etc/postfix/main.cf--
mydestination = sendmail.kuins.net, sc-filt.kuins.net,
               mailrelay.kuins.net
mynetworks =
relay_domains = kyoto-u.ac.jp
smtpd_relay_restrictions = reject_unauth_destination
smtpd_client_connection_count_limit = 3
smtpd_client_connection_rate_limit = 8
smtpd_client_recipient_rate_limit = 10
smtpd_client_message_rate_limit = 10
```

移行では 3 種類のメール中継サーバ名の DNS の CNAME レコードをプロキシサーバのホスト名に向けることで実施した。

3 メール受信システム

3.1 既存サービスと移行方針

既存サービスでは MX レコードの指定先として「mx1.kuins.net」と「mx2.kuins.net」、「scmls-

1.kuins.net」と「scmls-2.kuins.net」の 2 組のホスト名を提供していた。利用者が中継サービス利用したいドメイン名を「example.kyoto-u.ac.jp」としてその MX レコードに上記ホスト名を指定すると、「kuins3mx.example.kyoto-u.ac.jp」の MX レコードに指定されたメールサーバか、または「example.kyoto-u.ac.jp」の A レコードに中継される仕組みであった。

送信側と異なり受信側は外部から直接メールの受け入れが必要であると同時に、外部からの直接攻撃により悪用されたりウイルスメールによる被害の懸念もあるため、受信側の中継サービスは維持し、ウイルスやスパムチェックの機能も維持する方針とした。

しかしながら既存サービスは利用申請手続きを設けず利用者の MX レコードや A レコード設定で自由に利用できていたため、各ドメインの正確な利用責任者が不明であり、また利用終了後も MX レコードが残っていたり利用者数の把握も困難だったことから利用申請は必須とした。利用申請時にドメイン名とその転送先が確認できるため「kuins3mx」が付与された MX レコードによる中継機能は廃止した。

3.2 新サービス設定詳細

受信メールゲートウェイサービスとして新サービスを開始し、既存利用者からは利用責任者の連絡先に加えドメイン名や中継先 IP アドレス情報などを受け付けた。新サービスは以下の機能で運用を開始した。

- 実在しない送信者ドメインは拒否
- メール受信サイズが 20MB 以上ならば拒否
- S25R に該当する送信元 IP アドレスからのメールは一旦接続を拒否、再受信後に中継
- ウィルスと判定された場合は拒否
- Authentication-Results ヘッダに SPF 及び DKIM、DMARC 情報を付与し中継
- スпамと判定された場合はヘッダを付与し中継

新たに構築したメール受信のシステム構成を表 1 に示す。CentOS7 標準または公式サイトのパッケージを用いて構成している。

表 1 メール受信サーバのシステム構成

機能	ソフトウェア名	バージョン
OS	Linux	3.10.0
MTA	Postfix	2.10.1
greylisting	mltiler-greylist	4.6.2
Virus	ClamAV	0.101.4
Spam	SpamAssassin	3.4.2
DKIM	OpenDKIM	2.11.0
SPF,DMARC	OpenDMARC	1.3.2

メールサーバは TCP の 25 番を公開し、設定 2 とした Postfix にてメールを受け付ける。運用開始当初は 8 台構成としたが利用件数から 4 台に削減した。また利用申請者には MX レコードの指定先として「mgw-r1.iimc.kyoto-u.ac.jp」と「mgw-r2.iimc.kyoto-u.ac.jp」を提示し、ホスト毎に 2 台割り当てた。

設定 2 受信設定

```
--/etc/postfix/main.cf--
mydestination = $myhostname, localhost
mynetworks =
relay_domains = kyoto-u.ac.jp
message_size_limit = 25600000
smtpd_milters = unix:/run/milter-greylst/milter-greylst.sock,
               unix:/run/clamav-milter/clamav-milter.socket, unix:/run/
               opendkim/opendkim.sock, unix:/run/opendmarc/opendmarc.sock
               , unix:/run/spamass-milter/postfix/sock
milter_default_action = accept
relay_recipient_maps = regexp:/etc/postfix/relay.regexp
transport_maps = regexp:/etc/postfix/transport.regexp
smtpd_relay_restrictions = reject_unauth_destination
smtpd_sender_restrictions = reject_unknown_sender_domain

--/etc/postfix/relay.regexp--
/@example.kyoto-u.ac.jp$/ smtp:[192.0.2.1]
:

--/etc/postfix/transport.regexp--
/@example.kyoto-u.ac.jp$/ smtp:[192.0.2.1]
:
./.* smtp:[203.0.113.1]
```

送信者ドメインとメール受信サイズはここでチェックし、それ以外は milter にて各ソフトウェアにて処理を行う。また新たな利用申請があると relay.regexp と transport.regexp 両ファイルに中継を許可するドメインと中継先を追加する運用となる。

なお中継先からのユーザが存在しないなどのバウンスメールについてはスパムである可能性が高いため、受信メールサーバの評価が下がらないように図 1 のようにクラウド IaaS のバウンス送信用サーバを経由させる。バウンスメールのみ取り扱うサーバは設定 3 のように再送回数を制限した。

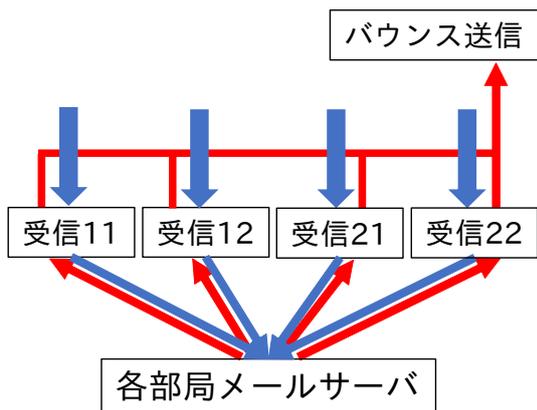


図 1 サーバ構成

設定 3 バウンス送信設定

```
--/etc/postfix/main.cf--
mydestination = $myhostname, localhost
mynetworks = [recipient server]
header_checks = regexp:/etc/postfix/header_checks.regexp
minimal_backoff_time = 300s
maximal_backoff_time = 600s
maximal_queue_lifetime = 660s
bounce_queue_lifetime = 660s
default_destination_rate_delay = 30s
```

また各 milter はそれぞれ設定 4 とした。

設定 4 各 milter 設定

```
--/etc/mail/greylst.conf--
socket "/run/milter-greylst/milter-greylst.sock" 660
peer 192.168.xxx.1
peer 192.168.xxx.3
peer 192.168.xxx.4
greylst 30m
timeout 4h
autowhite 5d
subnetmatch /24
racl whitelist domain /.../
:
racl greylst domain /^[.+\]$/ msg "S25R rule 0"
racl greylst domain /^[^.*][0-9][^0-9].[^0-9].*/ msg "S25R
rule 1"
racl greylst domain /^[^.*][0-9][0-9][0-9][0-9][0-9]/ msg "S25R
rule 2"
racl greylst domain /^[^.*][0-9][^0-9].[^0-9].[^0-9].[a-z]/
msg "S25R rule 3"
racl greylst domain /^[^.*][0-9]\.[^0-9][0-9]/ msg "S25R
rule 4"
racl greylst domain /^[^.*][0-9]\.[^0-9][0-9]\.[^0-9].[^0-9].*/
msg "S25R rule 5"
racl greylst domain /^(dncpldialup|ppp|lachsrxv|ds1
)[^0-9]/ msg "S25R rule 6"

--/etc/clamd.d/scan.conf
LocalSocket /run/clamd.scan/clamd.sock

--/etc/mail/clamav-milter.conf--
MilterSocket unix:/run/clamav-milter/clamav-milter.socket
ClamdSocket unix:/run/clamd.scan/clamd.sock
MaxFileSize 25M
OnInfected Reject

--/etc/opendkim.conf--
Mode v
Socket local:/run/opendkim/opendkim.sock

--/etc/opendmarc.conf--
Socket unix:/run/opendmarc/opendmarc.sock
SoftwareHeader false
SPFIgnoreResults true
SPFSelfValidate true

--/etc/mail/spamassassin/local.cf--
clear_headers
add_header all Flag _YESNOCAPS_
add_header all Status _YESNO_ score=_SCORE_ required=_REQD_
tests=_TESTS_
add_header spam Report _REPORT_
add_header spam Level Spam
normalize_charset 1

--/etc/sysconfig/spamass-milter--
EXTRA_FLAGS="-m -r 15 -P /run/spamass-milter/spamass-milter.pid
-- -s 25600000"

--/etc/sysconfig/spamass-milter-postfix--
SOCKET="/run/spamass-milter/postfix/sock"
```

Postfix にて導入した送信者ドメイン拒否では、旧来から「localhost」や「*.localdomain」といったドメイン名で送信されるシステム管理者向けのメールが届かなくなることから、事前通知を徹底して FQDN 名に変更していただいた。

greylisting では利用者からのクレームがあれば適宜ホワイトリストでドメイン名や IP アドレスサブネットを追加したが、運用開始時点から S25R サイト [1] 提供のホワイトリストを適用していたため約 3 年間の運用でクレームを受けたのは最初の 1 年間のみで 7 件であり、ほとんど運用コストは生じなかった。

また ClamAV と SpamAssassin については自動アップデート機能を有しており、それらを利用することで更新についても同様に運用コストは生じなかった。

最後に OpenDKIM と OpenDMARC については転送先サーバ側での SPF 検証不可に対する配慮であったが、SPF に加えて DKIM と DMARC 情報も追加で提供するようにした。

障害についても約 3 年間で特に発生せず安定した運用を行えた。例えば、前システムにおいて DNS キャッ

サーバ障害が発生した際に、大規模構成で複雑な中継条件のためバウンスが送信元に返信されず削除されるなど大きな障害を発生させたことから、受信サーバ自身で DNS キャッシュサービスを稼働しさらに予備的にクラウドサービスも設定するなどシステム安定化に関する対策を講じており、2024 年 3 月と 4 月に発生した数分程度の DNS キャッシュサーバ障害を回避できている。このように前システムの障害事例を解析し構築時に改善した結果が奏功したと思われる。

3.3 システム運用実績

受信メールゲートウェイサービスは 3 年間で計 84 件の利用申請があり図 2 は 2024 年 3 月 3 日から 5 月 3 日までの 2 ヶ月間のメール受信件数を示している。受信サーバでの拒否は「送信者拒否」「中継拒否」「サイズ拒否」「S25R 拒否」「スパムウィルス拒否」があるがほぼ「送信者拒否」と「S25R 拒否」で拒否されていることが分かる。また全受信件数に対する受信サーバでの拒否メール件数とした「拒否率」は日によってばらつきはあるが 50% から 90% の高い数字となっている。なお部局メールサーバに中継するメールは恒常的に 1 日あたり 3 万から 4 万件で変化が少なく、加えて不達の間い合わせもないことから、おそらく不要なメールは正しく拒否されていると思われる。

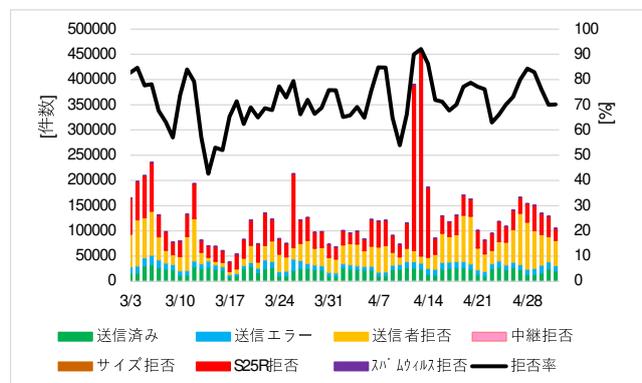


図 2 メール受信件数と拒否率

3.4 システム更新と移行

2024 年 6 月末のシステム OS サポート期限に伴い次期システムの検討を行った。添付ファイルなどメール本文に含まれるウィルスについては ClamAV、URL へのクリックから感染するようなウィルスについては SpamAssassin での対応となるが、図 2 にあるように検知件数としては大きくない。「送信者拒否」と「S25R 拒否」にて拒否済みであれば問題ないが、ウィルス検知に関して本システムの継続だけでは不安が残る結果

となっている。

一方でメールホスティングサービスでは独自に商用メールアプライアンス機を導入し、ウィルススパムチェックを行っており、商用データベースで精度の高い検知とメール除去サービスを提供している。当該アプライアンス機器の処理能力を検討し、受信メールゲートウェイでのドメイン数と受信件数を追加しても運用可能であると判断できたため、システムのサポート期限までに移行する方針でサービス担当部署と合意し、各ドメインの移行を実施した。

前サービスの移行と異なり、本サービスでは利用責任者や連絡先情報が明確であったため移行案内も利用責任者本人に直接通知を行った。利用責任者の移行作業を最小限に抑えるため下記の作業手順の 1、2、及び 4 を依頼し、7 月 10 日に移行を希望する全ドメインの移行が完了した。

1. 継続利用確認の申請
2. 事前試験メール受信確認
3. サービス提供者側で MX レコードを商用アプライアンス機のホスト名に変更
4. メール受信確認

4 まとめ

- S25R とオープンソースツールを用いて肥大化したメール中継サービスを最小限のシステムに移行し導入コストを大幅に削減した
- 受信メールの 50% から 90% を占める不正メールを除外できた
- 安定運用に配慮したシステム構成で 3 年間で障害がゼロであり、運用コストも最小限に抑えられた
- ただしセキュリティ面での強化が必要ならば商用アプライアンスのデータベース活用も必要である

謝辞

商用アプライアンス機への移行で共同作業いただき、また今後の受信メールゲートウェイサービスの運用をご快諾いただいたメールホスティングサービス担当のみなさまに感謝致します。

参考文献

- [1] 阻止率 99% のスパム対策方式の研究報告
<http://www.gabacho-net.jp/anti-spam/anti-spam-system.html> (参照 2024-10-21)