メールサーバと DNS に関する実験

学籍番号 1250373
溝口 洸熙
グループ 5C

July 3rd, 2023

1　目的

本実験の目的は，電子メールサーバ（以下，メールサーバ）の構築である．

1.1　構築する理由

電子メール（以下，メール）は，言わばコンピュータネットワーク上の「郵便」のようなものである．メールの誕生により，文字や写真などバイナリファイルの共有を，ネットワークを通して行えるようになった．つまり，非接触での情報伝達が電話からインターネットへと変革するきっかけとなったのである．本実験では，メールサーバを作成し，同一ネットワーク上のコンピュータ間でメールのやりとりを行えるようにする．昨今，メールサービスは，EC などのインターネットを用いたサービスのさまざまな通達に用いられる．そこで効率的にメールを配信するために，1 つのメールアドレスで複数宛に送信できるような機能がある．本実験ではそのような機能も併せて実現する．

1.2　構築するものの概要

メールを支える技術は多数あるが，本実験ではメールサービスの根幹を成す，MTA（Mail Transfer Agent）を構築し，1 つの宛先アドレスに対して複数アドレスに配信できるメーリングリスト機能を持たせる．また，メールの配送には DNS（Domain Name System）が必要であるので，本実験では DNS サーバも併せて構築する．

2　内容

■メール送受信フロー　ここで，メールを送信してから宛先に届くまでの大まかな手続きを確認する（図 1）．送り手は，MUA（Mail User Agent）と呼ばれるソフトウェア（Thunderbird や Microsoft Outlook など）から SMTP を利用して MTA にメッセージを転送する．この際，MUA は MTA のドメイン名を保持しており，DNS の `MX` レコードを用いて MTA のホスト名を取得後，`A` レコードを用いて送信先の IP アドレスを調べる．MDA（Mail Delivery Agent）に転送されたメッセージは，取得した IP アドレス宛に SMTP で転送される．MDA はメッセージを MTA により指定された送信先に転送すること役割を担う．転送されたメッセージは，SMTP を利用して宛先 MTA へ転送され，Mail Spool（以下，Spool）へ保存される．Spool とは，宛先の MUA が，メッセージを受け取るまで一時的に保存する場所である．Spool 内のメッセージは POP を利用して宛先の MUA へ転送されると，

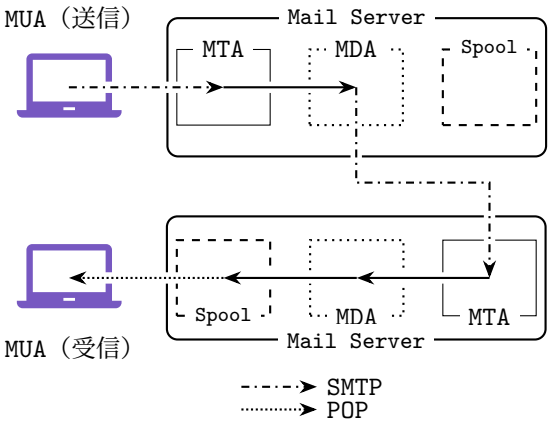

図 1　メッセージの流れ*

*本レポートで用いる図の一部はヤマハ株式会社の公開済図形（`https://network.yamaha.com/support/download/tool/`）を利用している．

Spool から削除される． [1, p.9 - p.11, p.13]

■名前解決フロー　ドメイン名に対して，対応付けられた IP アドレスへの名前解決をする．名前解決をする主な方法として DNS，ブロードキャストで問い合わせる方法 [2, p.135]，WINS（Windows Internet Name Service），NIS（Network Information Service），`HOSTS` ファイルの適用などがある．ここでは OS に依存せず，データベースを分散管理でき，大規模ネットワークでも耐えうる DNS を用いた名前解決方法を適用する．

DNS を用いた名前解決の手順を解説する．ここでは例として Web サイト `www.info.kochi-tech.ac.jp` の IP アドレスを，DNS を用いて取得する．まず，リゾルバ（ネームサーバへアクセスするクライアント）は，自身のネットワーク設定により指定されたネームサーバへ `www.info.kochi-tech.ac.jp` の IP アドレスを問い合わせる．そのネームサーバが，`www.info.kochi-tech.ac.jp` の IP アドレスを持っていない場合，まずは `root` ネームサーバへ，`jp` ネームサーバの IP アドレスを問い合わせる．次に `jp` ネームサーバへ `ac` ネームサーバの IP アドレスを問い合わせる．これを繰り返し，最後に `info` ネームサーバが `www` の IP アドレスを，リゾルバが最初に問い合わせたネームサーバへ返し，リゾルバへ応答する． [3, p.8]

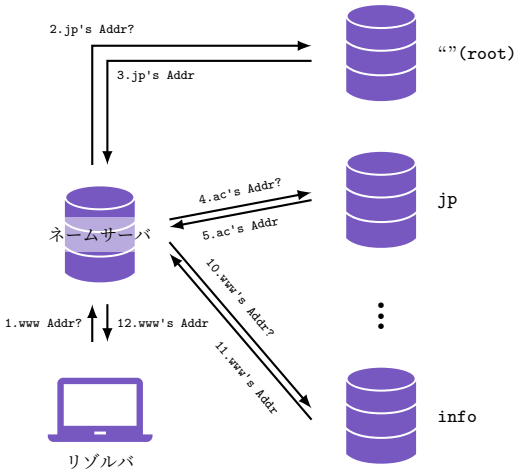

図 2　名前解決

■aliases ファイル　通常，メールサーバを設定をしない限り，メールアドレスは「`username@domain`」になる．ここで，`username@domain` のユーザ名 `username` を公開したくない場合，`aliases` ファイルに `anonymous` と `username` を対応づける設定をすることで，`anonymous@domain` でのメール受信が可能になる．この機能はユーザ名を秘匿にしたい場合だけでなく，たとえば `usernameA`，`usernameB`，`usernameC` の 3 ユーザを 1 つのエイリアス `group` と対応づけて，`group@domain` 宛に送信したメールを 3 ユーザで受信できる．

3　要素技術

3.1　ドメイン

図 3　高知工科大学情報学群ホームページ URI

DNS は UNIX ファイルシステムと同様に木構造を持っている．ファイルシステムの根（root）は `/` であるのに対して，DNS の根（ルート DNS）は空ラベル（“”）で表現される．UNIX ファイルシステムにおける木構造の各節は，「ディレクトリ」であり，DNS においてはドメインである．DNS では木構造全体の，ルートまでのラベルをドット（“.”）で連結したものが DNS の絶対名となる．これを FQDN（Full Qualified Domain Name）と呼ぶ．ホスト名 `www.info.kochi-tech.ac.jp` の FQDN は `www.info.kochi-tech.ac.jp.` である．最後の “.” は，後ろに空ラベル（“”）があることを表現している．当然，FQDN は世界に同じものが存在しないように作成する必要がある．つまり，ドメインとは木構造の部分木を構成するものであり，部分木における根の FQDN が

その部分木のドメイン名となる．DNS では，各ドメインをいくつかのサブドメインに分割し，サブドメインの管理をサブドメイン内で完結できる．たとえば，ドメイン info.kochi-tech.ac.jp において，jp のサブドメインである ac.jp は，ac.jp で終わるドメインについて責任を持つ．また，ac.jp は，kochi-tech というサブドメインをもち，kochi-tech.ac.jp が末尾につくドメイン名の責任を高知工科大学に委任している．

ここで，ゾーンという概念が登場する．ゾーンとは，名前空間において独立し，自治管理される部分である．図 4 での info.kochi-tech.ac.jp ゾーンには www，host1，host2 の 3 クライアントがあり，これらは info.kochi-tech.ac.jp によりドメインを管理されている．さらに，ac.jp ゾーンには kochi-tech ドメインは含まれていない．これは「委任（委譲）」という行為で，ac.jp から，高知工科大学へ kochi-tech 以下サブドメインの管理を委任する．つまり，ac.jp は，kochi-tech.ac.jp のサブドメインを管理しないので，ac.jp のゾーンではない． [3, p.23]

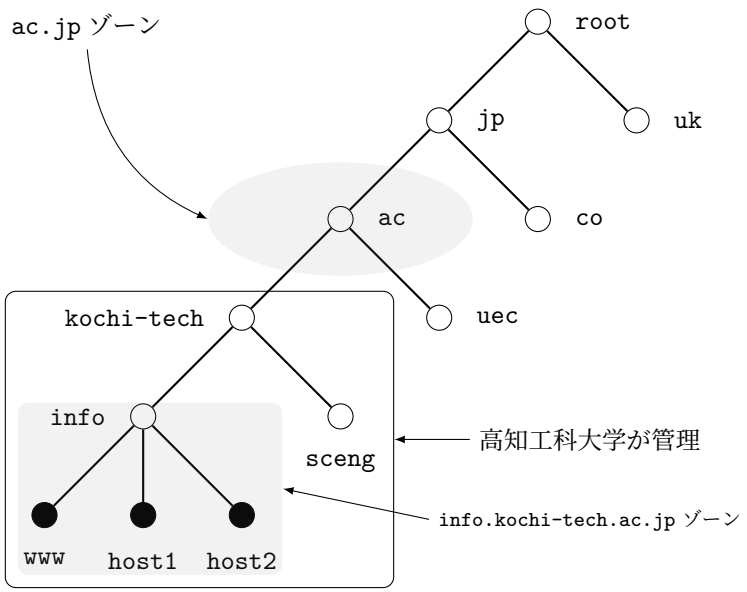

図 4　ドメインの木構造とゾーン

3.2 SMTP と POP3

■SMTP　SMTP とは，OSI 参照モデル第 7 層に属する，メール転送プロトコルである．ポート番号は 25 番である．図 1 より，MUA から MTA，MTA から MTA へのメール転送に用いられる．これをメールリレーという．SMTP サーバには telnet でアクセスし，コマンドを入力することでメールを配信する．telnet で電子メールサーバにアクセスし，メールを配信する手続きを示す．ここでは mail.example.com へアクセスする．

src. 1　SMTP コマンド入力

```
$ telnet mail.example.com 25
Trying 10.232.45.151
Connected to mail.example.com.
Escape character is '^]'
220 mail.example.com ESMTP Postfix
HELLO mail.example.com
250 mail.oreilly.com
MAIL FROM: <info.oreilly.com>
```

```
250 Ok
RCPT TO: kdent@example.com
250 Ok

DATA
354 End data with <CR><LF>.<CR><LF>

Date: Mon, 8 Apr 2003 15:38:21 -0500
From: Customer Service <info@oreilly.com>
To: <kdant@example.com>
Reply-To: <service@oreilly.com>
Message-ID 01a4e2238200842@mail.oreilly.com
Subject: Have you read RFC 2822?

This is the start of the body of the message. It could continue
for many lines, but it dosen't.
.

250 Ok: queued as 5FA26B3DFE
quit
221 Bey
Connection closed by foreign host.
```

引用 [4, p.18]

また，SMTP には認証機能がないが，認証元が詐称されることを防ぐため，POPbefreSMTP や SMTP 認証が用いられる [5, p.173].

■POP3　POP とは，図 1 より，Spool から外部 MUA で受信するためのプロトコルである．SMTP を用いたメッセージの受信は，送信されたメッセージが宛先 MUA まで到達するため，宛先 MUA が常にメール受信可能状態でなければならない．POP を用いることで，常に電源が入っている POP サーバまで到達したメッセージは，MUA の要求時にメッセージを受信できる．POP を用いてメッセージを転送した場合，Spool 内のメールは削除される．POP3 は POP のバージョン 3 である．　[6, p.200, p.281]

3.3　第三者リレー

オープンリレー，第三者中継とも呼ぶ．オープンリレーは以下のように説明されている．

“メールリレーを誰にでも許可するメールサーバ” 引用 [4, p.53]

つまり，オープンリレーを許可しているサーバでは，認証なく誰でもそのサーバを利用してメールを送信できるので，スパムメールなどの温床になる [4, p.53].

4 作業記録

ネットワークの設定（IP アドレスやデフォルトゲートウェイの設定）は完了している．

表 1 設定事項

ネットワーク	デフォルトゲートウェイ	192.168.0.9
サーバ	IP アドレス	192.168.0.161
	FQDN	server.c5.exp.info.kochi-tech.ac.jp.
	ホスト名の別名	www.c5.exp.info.kochi-tech.ac.jp. smtp.c5.exp.info.kochi-tech.ac.jp. pop.c5.exp.info.kochi-tech.ac.jp.
クライアント	IP アドレス	192.168.0.162
	FQDN	client.c5.exp.info.kochi-tech.ac.jp.

4.1 DNS サーバ構築

BIND を用いて DNS サーバを構築する．BIND のバージョンは 9.18.16 である．

1. パッケージマネジャ apt をアップデートした後，apt を用いて BIND をインストールする．

```
$ sudo su Enter
# apt update Enter
# apt install bind9 Enter
```

2. BIND 全体の設定として named.conf を操作する．

src. 2 /etc/bind/named.conf

```
// This is the primary configuration file for the BIND DNS server named.
//
// Please read /usr/share/doc/bind9/README.Debian.gz for information on the
// structure of BIND configuration files in Debian, *BEFORE* you customize
// this configuration file.
//
// If you are just adding zones, please do that in /etc/bind/named.conf.local
include "/etc/bind/named.conf.options";
include "/etc/bind/named.conf.local";
include "/etc/bind/named.conf.default-zones";
```

3. これから編集するファイル named.conf.options のデフォルトファイルを別名で保存する.

```
# cd /etc/bind Enter
# cp -p named.conf.options named.conf.options.org Enter
```

4. ここでは BIND が動作するワーキングディレクトリの指定をするために named.conf.options を編集する.

src. 3 /etc/bind/named.conf.options

```
options {
    directory "/var/cache/bind";
};
```

5. ゾーンファイルを指定する. named.conf.local にはゾーンファイルのパスを記述する. ドメイン名を c5.exp.info.kochi-tech.ac.jp に設定し, ゾーンファイルのパスを/etc/bind/c5.zone にする.

src. 4 /etc/bind/named.conf.local

```
zone "c5.exp.info.kochi-tech.ac.jp" {
    type primary;
    file "/etc/bind/c5.zone";
};
```

6. ルートゾーンの設定を確認する. ルートゾーンは “.” で表されており, ルートサーバのアドレスは/usr/share/dns/root.hints に記述されている.

src. 5 /etc/bind/named.conf.default-zones

```
zone "." {
    type    hint;
    files   "/usr/share/dns/root.hints";
}
```

7. ゾーンを設定する. 最後に “.” がない場合はゾーンのドメイン名が補完される.

TTL キャッシュの有効期限を記す.

SOA レコード このサーバがゾーン内で最も信頼するに値するものであることを示すもの. SOA レコードの中には次の項目を設定する.

- サーバの FQDN, メールアドレスの FQDN (“@” を “.” に置換する).
- シリアル番号.
- セカンダリサーバがプライマリサーバに情報更新がないか問い合わせる間隔.
- リフレッシュ失敗時に, 際リフレッシュする時間間隔.
- 生存時間.

NS レコード ネームサーバの FQDN を記す.

A レコード ホスト名と IP アドレスを対応づける.

CNAME レコード ホスト名の別名を設定する.

MX レコード メールアドレスのドメイン名とサーバの FQDN を対応づける. [3, p.69 - p.71]

src. 6 /etc/bind/c5.zone

```
$TTL 100
@ IN SOA server.c5.exp.info.kochi-tech.ac.jp. postmaster.c5.exp.info.kochi-
  tech.ac.jp. (
    2023061901
    100
    100
    100
    100 )
            IN  NS      server.c5.exp.info.kochi-tech.ac.jp.
server      IN  A       192.168.0.161
client      IN  A       192.168.0.162
www         IN  CNAME   server
smtp        IN  CNAME   server
pop         IN  CNAME   server

c5.exp.info.kochi-tech.ac.jp IN MX server.c5.exp.info.kochi-tech.ac.jp.
```

8. DNS クライアントの設定を変更し，変更を適用する．

src. 7 /etc/netlpan/00-install-config.yaml

```
# This is network config written by 'subiquity'
network:
    version: 2
    ethernets:
        enp0s31f6:
            addresses:
                - 192.168.0.161/24
            routes:
                - to: default
                  via: 192.168.0.9
            nameservers:
                addresses:
                    - 127.0.0.1 # 自分自身
                search: [c5.exp.info.kochi-tech.ac.jp] # ドメイン名
            dhcp4: false
```

```
# netplan apply Enter
```

9. bind9 と named を再起動して，設定を反映させる．

```
# systemctl restart bind9 Enter
# systemctl restart named Enter
```

4.2 メールサーバの構築

Postfix を用いてメールサーバを構築する．Postfix のバージョンは 3.8.1 である．

1. パッケージマネジャ apt をアップデートした後，apt を用いて Postfix，POP をインストールする．

```
$ sudo su Enter
# apt update Enter
# apt install postfix Enter
~~~in Menu~~~
1. [Internet Site] Enter
2. mail name: c5.exp.info.kochi-tech.ac.jp Enter
~~~~~~~~~~~~~~
# apt install dovecot-pop3d Enter
```

2. ネットワークセグメントとサーバの FQDN を追加する．

src. 8 /etc/postfix/main.cf

```
myhostname = server.c5.exp.info.kochi-tech.ac.jp.
mynetworks = 192.168.0.0/24
```

3. POP3 認証を有効にする．

src. 9 /etc/dovecot/conf.d/10-auth.conf

```
disable_plaintext_auth = no
```

4. Postfix，dovecot を再起動する．

```
# systemctl restart postfix Enter
# systemctl restart dovecot Enter
```

5. aliases ファイルを編集し，newaliases コマンドで適用する．list@c5.exp.info.kochi-tech.ac.jp 宛のメールが記述した 4 ユーザへ配信される．

src. 10 /etc/aliases

```
list: k.mizo, s.shio, k,kikk, k.fuku
```

4.3 MUA の設定

MUA として Thunderbird を用いる．以下の項目を適切に入力する．

設定済みユーザ名	k.mizo
パスワード	********
名前	MIZOGUCHI Koki
電子メールアドレス	k.mizo@c5.exp.info.kochi-tech.ac.jp
送信メールサーバ	smtp.c5.exp.info.kochi-tech.ac.jp
受信メールサーバ	pop.c5.exp.info.kochi-tech.ac.jp
POP3 アカウント	k.mizo
パスワード	********

4.4 動作確認

あるユーザから list@c5.exp.info.kochi-tech.ac.jp 宛にメールを送信する．設定した 4 ユーザへ，正しくメールが配信されていることが確認できた．

5 考察

現在，DNS の抱えるリスクはセキュリティである．DNS の安全性を高めるために，DNSSEC（DNS Security Extensions）が開発された．DNS のセキュリティ脆弱性は，DNS 応答レコードの偽造や改竄，正しいゾーン管理者により作られたゾーン情報でないことにある．DNSSEC では，応答レコードに公開鍵暗号方式を用いたディジタル署名を付加することで改竄検知できる．

しかしながら，DNSSEC は DNS 通信の傍受を防止することは目的としていない．リゾルバと DNS サーバ間の通信は暗号化されていない [7]．つまり，この通信を傍受することにより，リゾルバがどのサイトへアクセスしたか，通信を傍受している第三者が追跡できる．これは，DNS サーバとリゾルバ間で公開鍵暗号方式を用いて鍵交換し，共通鍵暗号方式（XOR）を用いて暗号化するハイブリッド暗号方式を施すことで対策できる．しかし，DNS を用いた名前解決ごとに暗号化処理を施すのは，リゾルバ，DNS サーバともに負荷が大きくなるであろう．簡易的な解決方法は，鍵交換の間隔を長くすることだが，大規模なネットワーク上の DNS では，鍵管理に対して効率が悪くなる．DNS の通信傍受に対する影響と，その対策については今後の研究テーマにしたい．

参考文献

[1] 荒木靖宏. Postfix 詳解: MTA の理解とメールサーバの構築・運用. オーム社, 2004.

[2] 五十嵐順子. いちばんやさしいネットワークの本（技評 SE 選書）. 技評 SE 選書. 技術評論社, 2010.

[3] Paul Albitz, Cricket Liu 共著. DNS&BIND 第 4 版. O'Reilly, Heidelberg, Germany, feb 2002.

[4] Kyle D. Dent. Postfix 実用ガイド. O'Reilly, Heidelberg, Germany, aug 2004.

[5] 原山美知子. インターネット工学（シリーズ知能機械工学）. シリーズ知能機械工学. 共立出版, 2014.
[6] 竹下隆史. マスタリング TCP/IP 入門編 第 4 版. オーム社, 第 4 版, 2007.
[7] 三田村健史, 佐藤新太. DNSSEC 解説 - DNS におけるセキュリティ拡張の導入. 情報処理, Vol. 52, No. 9, pp. 1158–1165, aug 2011.