電子メール

電子メールの送受信の仕組み

偽造メールの問題

大東文化大学 経営学部 水谷正大

メールアドレスの構造

メールアドレスとドメイン名

メールアドレス= xxxx@ドメイン名

メッセージ送信には、そのドメイン内にある
MTAのホスト名(IPアドレス）が必要

- DNSのMX(Mail eXchange)レコードを使う

1. DNSに該当ドメインのMXレコードを問合わせ
2. DNSは該当ドメイン内にあるMTAのホスト名を返す
3. メール転送はMXレコードのホストに向けて行う

➡ DNSサービスが機能しないとメールは届かない！

ＭＸレコードの取得

```
% nslookup -q=mx st.daito.ac.jp

Server:      8.8.8.8
Address:  8.8.8.8#53

Non-authoritative answer:
st.daito.ac.jp  mail exchanger = 10 ASPMX.L.GOOGLE.COM.
st.daito.ac.jp  mail exchanger = 20 ALT1.ASPMX.L.GOOGLE.COM.
st.daito.ac.jp  mail exchanger = 20 ALT2.ASPMX.L.GOOGLE.COM.
st.daito.ac.jp  mail exchanger = 30 ASPMX2.GOOGLEMAIL.COM.
st.daito.ac.jp  mail exchanger = 30 ASPMX3.GOOGLEMAIL.COM.
st.daito.ac.jp  mail exchanger = 30 ASPMX4.GOOGLEMAIL.COM.
st.daito.ac.jp  mail exchanger = 30 ASPMX5.GOOGLEMAIL.COM.
```

➡ ドメインst.daito.ac.jpのメールサーバはGoogleが管理

用語

- メールの配信(Delivery)
  - メールサーバが管理する各ユーザのメールボックスにメールを届けること
- メールの転送(Transfer)
  - メールサーバに着信したメールの宛先が、自身が管理するユーザでない場合、他のメールサーバに送信する

着信メールの転送とは違う
メールサーバが別のメールサーバに転送

- メールルーティング(Mail routing)
  - 複数のメールサーバを経由（転送）して目的のメールサーバにメールを届ける経路

用語（2）

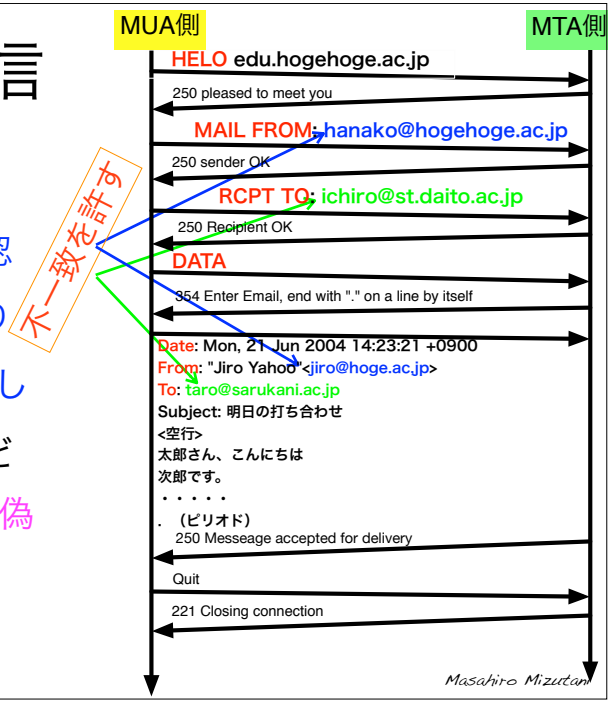
- MTA(Mail Transfer Agent)
  - いわゆるメールサーバのこと
  - メールの配送・転送機能を持つプログラム
    - Sendmail, qmailなど
- MUA(Mail User Agent)
  - いわゆるメーラー（メールソフト）のこと
  - MTAの存在を前提とし、ユーザのフロントエンドとしてメッセージの作成、MTAへの配送依頼、メッセージの読み出しを行うプログラム
    - Gmail, Outlook, Thunderbird, Mac Mailなど

メールの送信者

- メール送信者(責任を持つ投函者)情報は２種類
  - メールの送信元を詐称できる要因
- エンベロープの送信者
  - プロトコルSMTP(RFC2821)で規定された、MAIL FROM:の引数
- メールヘッダの送信者
  - メッセージ書式(RFC2822)で規定された、メッセージヘッダに記録されるFrom:, Date: , To: などのヘッダ値

SMTP通信

- Stateの維持
  - 相手の応答確認
  - 通信の順序あり
- 認証プロセスなし
- Date,From,Toなどはは MUAが勝手に偽装できる



telnetでメール送信実験

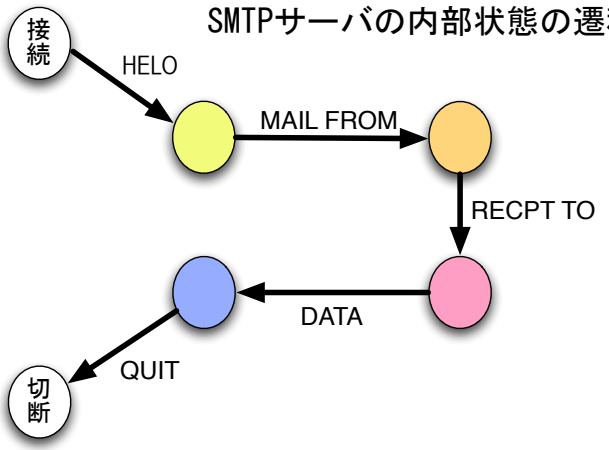
```
% telnet aspmx.l.google.com 25

Trying 74.125.129.26...
Connected to aspmx.l.google.com.
Escape character is '^]'.
220 mx.google.com ESMTP xk4si9765060pbc.177 - gsmtp
HELO
250 mx.google.com at your service
MAIL FROM:<ladygaga@gaga.com>
250 2.1.0 OK xk4si9765060pbc.177 - gsmtp
RCPT TO:<your-account@gmail.com>
250 2.1.5 OK mr7si34850236pbb.17 - gsmtp
DATA
354  Go ahead mr7si34850236pbb.17 - gsmtp
subject: Celebrate you
from: queen@daito.kingdom.jp
to: taro@st.daito.ac.jp
I would like to present you a jewel of my crown.
.
250 2.0.0 OK 1370065789 mr7si34850236pbb.17 - gsmtp
QUIT
221 2.0.0 closing connection mr7si34850236pbb.17 - gsmtp
Connection closed by foreign host.
```

<アドレス>とするのがGoogle式

subject, from, toはDATAの一部であり偽装可能

Masahiro Mizutani

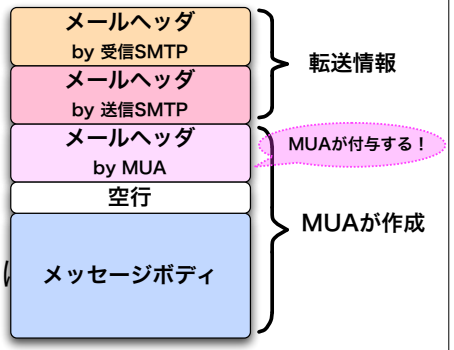
SMTPサーバの状態推移



Masahiro Mizutani

メールメッセージ

- メッセージ＝メールヘッダ + メッセージボディ
- メールヘッダ
  - 転送情報
  - From, To, Subject, Date
- メッセージボディ
  - メッセージ本文
  - 添付データ（テキスト形式に



Masahiro Mizutani

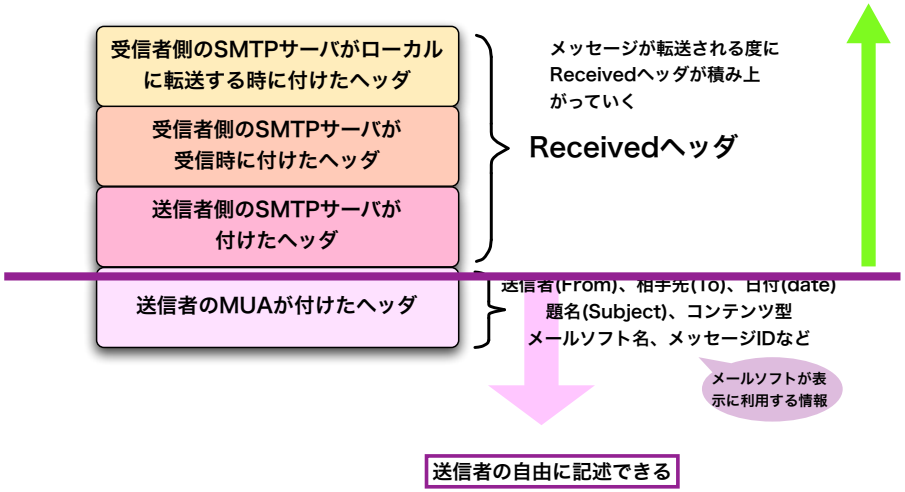
メールメッセージの例

```
Received: from smtp.sarukani.ac.jp (172.16.1.254)
  by smtp.daito.ac.jp with SMTP; 5 Jun 2013 11:17:33
Received: from tanuki.sarukani.ac.jp ([192.168.1.255])
   by smtp.sarukani.ac.jp with SMTP id abcdef1234;
   Wed, 5 Jun 2013 11:17:39 +0900
Date: Mon, 05 Jun 2013 11:17:50 +0900
From: Kitsune Tanuki<ktanuki@sarukani.ac.jp>
To: taro@st.daito.ac.jp
Subject: How are your family?
Content-Type: text/plain; charset=iso-2022-jp

Hello, Taro.
How is your family ?
```

メールソフトが付与する

Masahiro Mizutani

メールヘッダの構造



Receivedヘッダの書式

Received : from [送信MTA名]
by [受信MTA名]
via [接続方式] with [転送方式]
id [メッセージid]
for [宛先アドレス]; [日付]

telnetでPOP受信の実験

```
$ telnet pop.mailservice.jp 110
```

架空SMTPサーバ

```
Trying 210.xxx.xxx.xxx...
Connected to pop.mailservice.jp.
Escape character is '^]'.
+OK POP3 ready
USER xxxxxx@yyy.zzzz.jp
+OK
PASS wwwww
+OK server ready
STAT
+OK 2 2318
LIST
+OK 2 messages
1 1151
2 1167
.
RETR 1
.....
.....
QUIT
+OK pop.mailservice.jp closing connection
Connection closed by foreign host.
```

←passwdはそのまま送られる！！

STAT: 受信しているメールの件数とバイト数を通知

LIST: 受信しているメールの番号とバイト数を通知

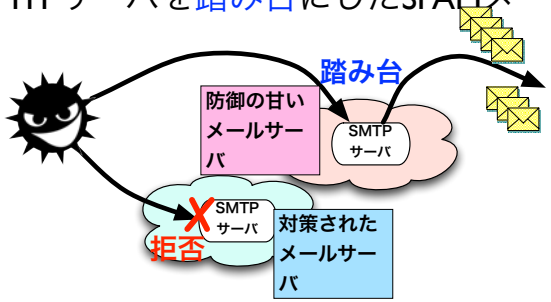
RETR: 指定したメッセージ番号のデータを受信

Gmailではpop設定をしないと読めない

pop.gmail.com
ポート：995

偽装メールの落とし穴（1）

- SMTPには認証プロセスがない
  - 管理者が防衛しない限り、誰でもSMTPサーバを利用可能
    - SMTPサーバを踏み台にしたSPAMメール



偽装メールの落とし穴（2）

- 偽メールヘッダによってメールを偽装できる
  - メールソフトの設定だけで、誰でも簡単に送信者情報（氏名とアドレス）を偽造可能
- **代理送信**ができるのもこのおかげ
  - 代理送信側にメールを送って確認する

偽装メールの落とし穴（3）

- 疑わしいメールはメールヘッダを調べる
  - しかし巧妙な偽造手口が「工夫」
    - 差出人のMUAが作成するメールヘッダとして、偽のReceivedヘッダを加えて「本物」のように偽装する手口

偽造メールの防止策

- 送信に使われたSMTPサーバが、差出人用の正規SMTPサーバかを認証する技術
  - Sender Policy Framework, Sender ID
  - Domain Keys
- 25番ポートブロック
  - 送信者がIPSが提供したSMTPサーバを経由しないで、勝手にSMTPサーバを運用してメールを送信したメールを規制する

送信ドメイン認証

- 受けとったメールが、送信者と名乗っているアドレスに示されているドメインから本当に送られているかをチェックする仕組み
- IPアドレスに基づく方法
  - Sender ID, SPFなど
- 電子署名に基づく方法
  - Identified Internet Mail, DomainKeys

OP25B（Outbound Port25 Blocking）

ISP側で許可した特定のSMTPサーバ以外のメール配信をブロックし、迷惑メール送信を防ぐ

- 外側に向かうSMTP(TCPの25番ポート)をブロック
  - Botなどを意図したスパムを防止
- 自宅（ISP)で使っているPCを外に持ち出すとメール送信できなくなる(以下の対策がある)
  - サブミッションポート587の利用（RFC2476）
- それでもSPAMメールはなくならない (- -);

Masahiro Mizutani