JP AAWG Japan Anti-Abuse Working Group

メールってどうやって届くの？
RFC復習 SMTP編

Vade Japan株式会社

関根 章弘

vade

自己紹介

関根　章弘

- 1995年頃　インターネット接続ブーム時に構築支援を行う
  要件を満たすために必要に迫られてsendmail.cfをカスタマイズ
- 2000年頃　商用サービス向けの大規模メールシステムの構築に関わる
- 海外のメール製品ベンダに所属し日本のサービスに導入
- 2003年　　迷惑メール対策カンファレンスの運営に携わる
- 2019年　　Vade Japanに入社、顧客サポートを担当

自己会社紹介

- Vade Japan株式会社（本社はフランス共和国 リール）
- AIエンジンを用いた予測的メール防衛の世界的リーダー
- 全世界で15億を超えるメールボックスを保護
- 日本国内にメール脅威の分析を行う技術チームを保有
- 2024年3月 ヨーロッパ最大のHornetsecurityグループに加わる

セッションの目的

古き良き時代にデザインされたメールシステムは、多くのMTA/MUAが良きに計らってくれているために、なんとなく送っても大部分のメールは問題なく届けられています。しかし、その中にはルール違反でエラーになっても仕方がないようなものも見られます。

しかし、スパムやフィッシングが大量に送られるようになり、最近はルール違反のメールは受信しないという方針のシステムもあります。

そのような厳格なシステムにブロックされてないようにRFCの内容をチェックします。間違いやすい点を例示して、正しいメールを確認します。

内容

1. メールの基本構造を確認します
2. メールを構成する各パートに対応したRFCの概要を確認します
   - SMTP - 5321
   - Message Format - 5322
   - MIME - 2045, 2046, 2047, 2048, 2049
3. 実際に送信されているメールでベストプラクティス、バッドプラクティスを確認します

※RFCの定義は非常に多岐にわたっています。このセッションでは細かな解釈には踏み込まず、基本的な項目を取り上げます

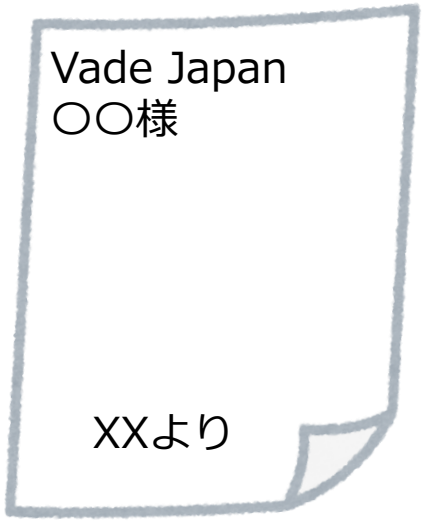
メールの基本構造

メール関連RFC

メールの構造と対応するRFC

エンベロープ

メール本体



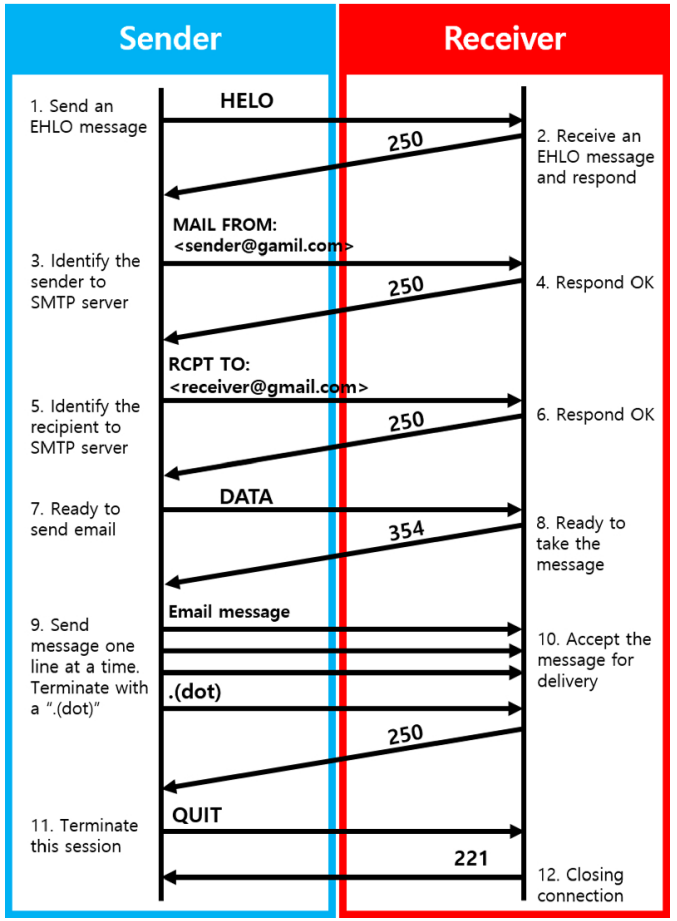
5321
Simple Mail Transfer Protocol

5322 - Internet Message Format

2045, 2046, 2047, 2048, 2049 – Multipurpose Internet Mail Extensions (MIME)

RFC5321 Simple Mail Transfer Protocol

- メールを転送する（送る）ための約束事です
- クライアント ー サーバ間のコマンド/レスポンスを定義しています
- 821→2821→5321と更新、修正、拡張されてきました
- 認証、暗号化、バイナリ・データ転送、および国際化された電子メールアドレスなど、さまざまな機能に対応した拡張性があります

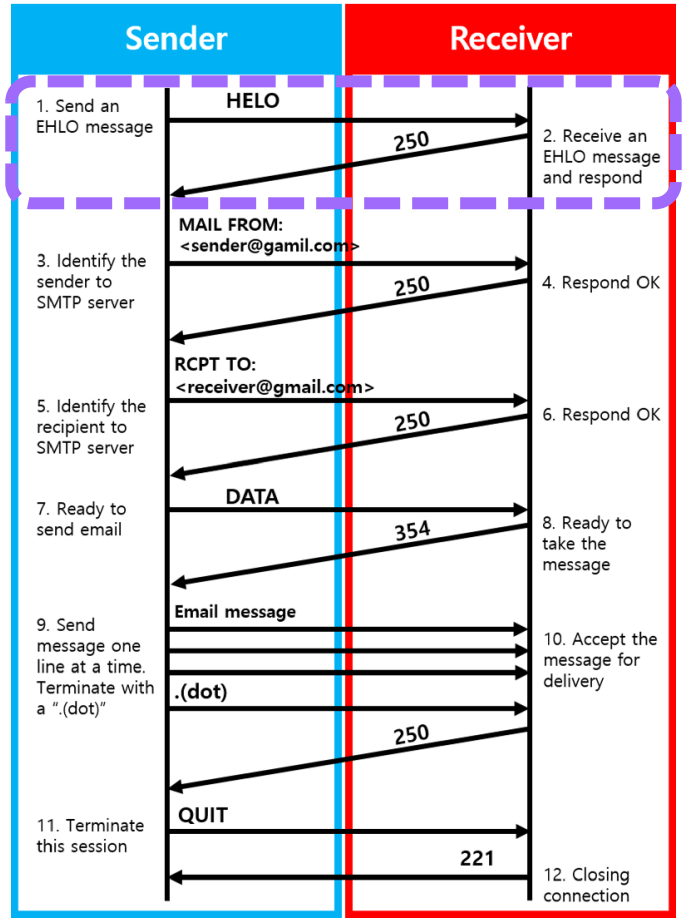


Simple Mail Transfer Protocol

- **S**imple **M**ail **T**ransfer **P**rotocol：略して**SMTP**
- 元祖のRFC822が書かれたのは1982年!!
- 基本となるコマンドは4つと、名前の通りSimpleです
  - EHLO/HELO
  - MAIL FROM
  - RCPT TO
  - DATA
- 面倒な話はRFC5322や一連のMIME関係（昨年の内容）

SMTP – step 1: EHLO/HELO

- EHLO/HELO
  - SMTP通信の開始を宣言
  - 自分の名前を紹介して挨拶します
- MAIL FROM
- RCPT TO
- DATA



SMTP – step 1: EHLO/HELO

- Syntax:
  - ehlo = "EHLO" SP (Domain / address-literal) CRLF
  - helo = "HELO" SP Domain CRLF

引数にはクライアントのFQDNまたはアドレスを指定

EHLOとHELO

EHLO (Extended HELLO)はSMTPの拡張をサポートするためにHELOを置き換えるコマンド

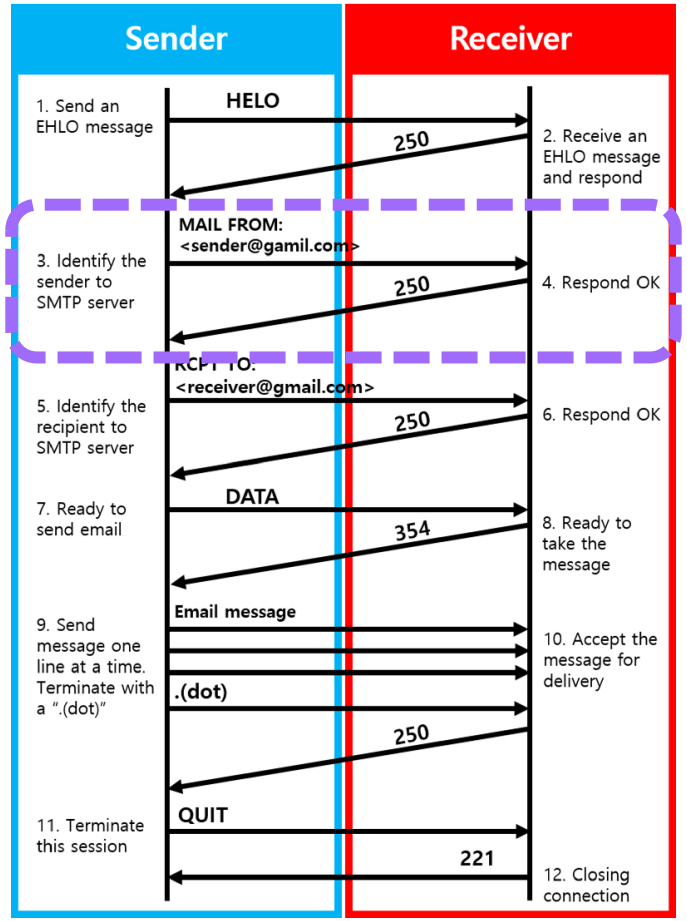
EHLOを受けたSMTPサーバーは、その応答として自身がサポートするSMTP拡張をクライアントに知らせます

応答例と対応するRFC：

250-SIZE 157286400	RFC1870
250-8BITMIME	RFC1652
250-STARTTLS	RFC3207
250-ENHANCEDSTATUSCODES	RFC2034
250-PIPELINING	RFC2197
250-CHUNKING	RFC1830
250 SMTPUTF8	RFC6531

SMTP – step 2: MAIL FROM

- EHLO/HELO
- MAIL FROM
  - メールトランザクションの開始
  - パラメーターとして送信元アドレスを宣言
- RCPT TO
- DATA



SMTP – step 2: MAIL FROM

- Syntax:
  - mail = "MAIL FROM:" Reverse-path [SP Mail-parameters] CRLF

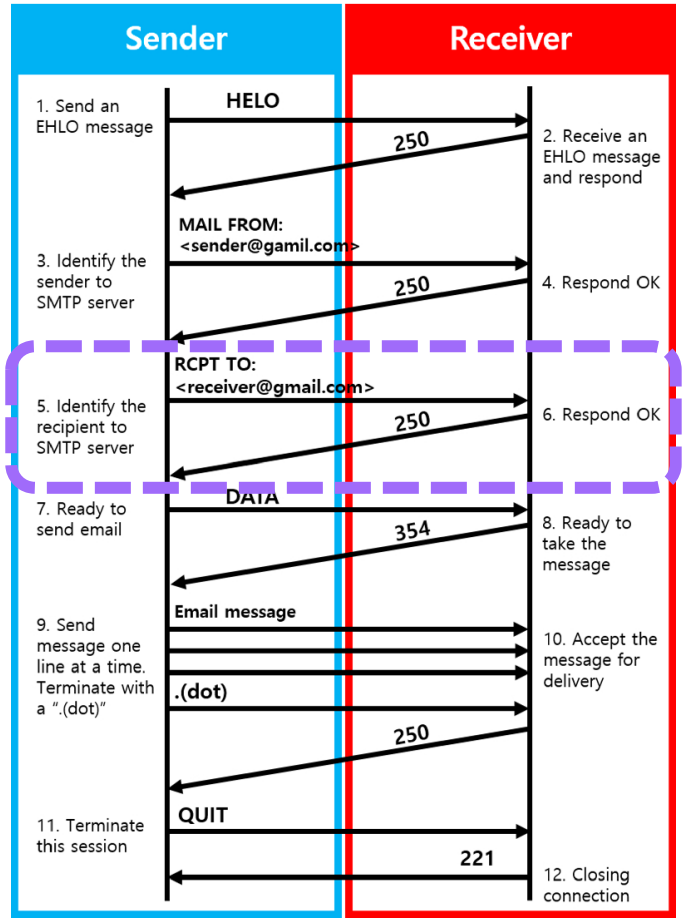
```
Return-Path: <no-reply@shanghaidazhongbc.com>
Authentication-Results:  mail.com; dkim=pass header.i=no-reply@shanghaidazhongbc.com
Received: from mail1.shanghaidazhongbc.com ([164.70.99.59]) by mx.mail.com
 (mxgmxus009 [74.208.5.20]) with ESMTPS (Nemesis) id 1M7bpz-1sygGQ1qxB-002LO6
 for <foo@mail.com>; Thu, 24 Oct 2024 10:45:20 +0200
Sender: <no-reply@shanghaidazhongbc.com>
From: =?utf-8?B?R01P44GC44GK44Ge44KJ440N440D44OI6YqA6KGM?= <no-reply@shanghaidazhongbc.com>
```

RFC5322

- Reverse-pathは送信者のメールボックス、ただし返信によってメールループが発生する可能性のあるNDNなどでは空（null）になる場合があります
- MAILコマンドはトランザクション開始のために一度だけ実行

SMTP – step 3: RCPT TO

- EHLO/HELO
- MAIL FROM
- RCPT TO
  - メールの受信アドレスを指定
- DATA



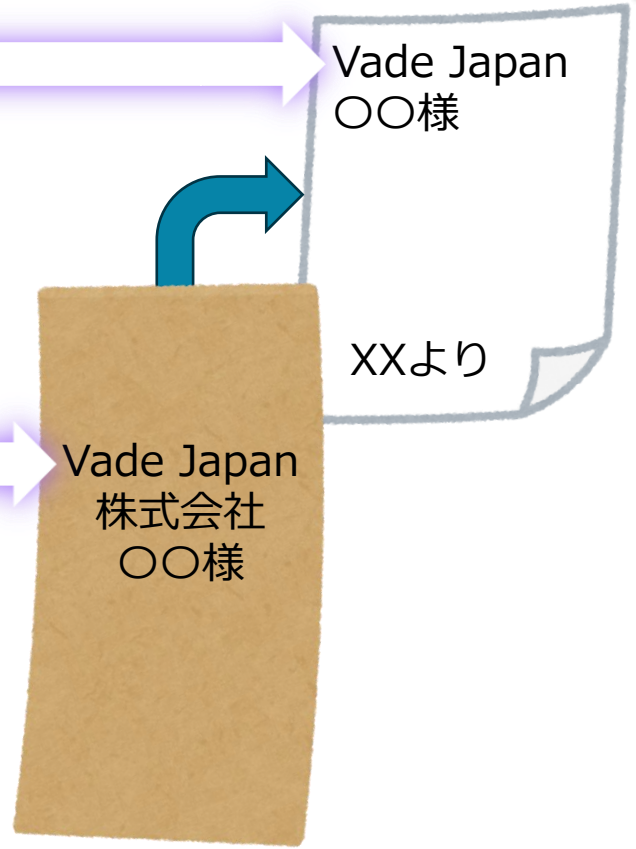
SMTP – step 3: RCPT TO

- Syntax:
  - rcpt = "RCPT TO:" ("<Postmaster@" Domain ">" / "<Postmaster>" / Forward-path) [SP Rcpt-parameters] CRLF

- RCPTコマンドを複数回使用して複数の受信者を指定可能です
  - To/Cc/Bcc の区別はありません

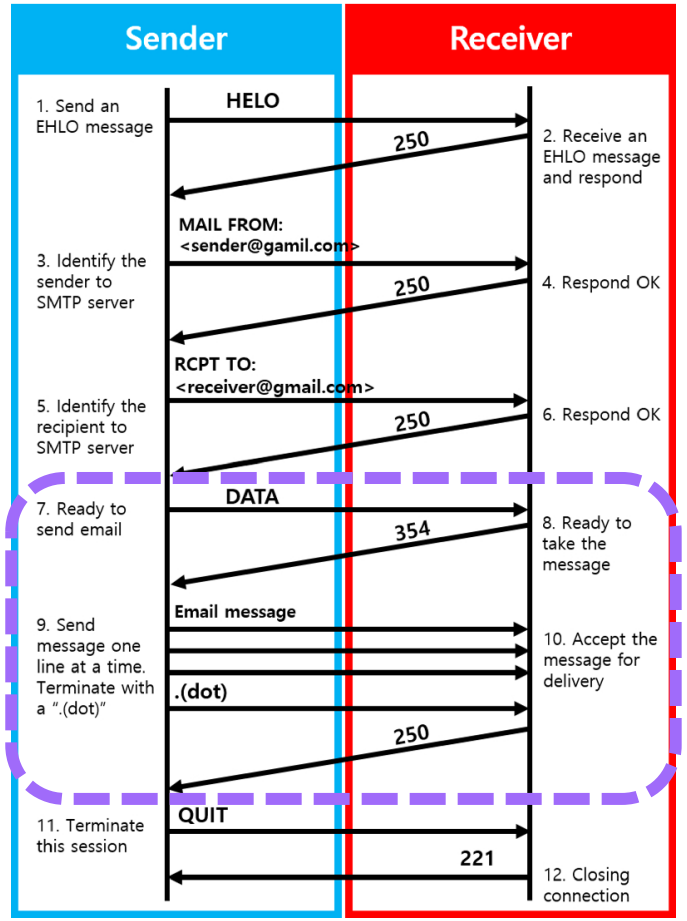
宛先の種類

- To: <アドレス>
- Cc: <アドレス>
- Bcc: <アドレス>（受信者には見えない）
  - 手紙（メール）の頭についている宛名
  - 封筒の中に入っているので配達とは無関係
  - RFC5322
- RCPT TO: <アドレス>
  - 封筒に書いてある配達に使う住所、宛名
  - 手紙（メール）の外側なので見えない
  - To/Cc/Bcc の区別はない
  - RFC5321



SMTP – step 4: DATA

- EHLO/HELO
- MAIL FROM
- RCPT TO
- DATA
  - メールヘッダー、本文、添付ファイルを送信
  - ‘.’（ピリオド）のみの行で終了



SMTP – step 4: DATA

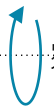
- Syntax:
  - data = "DATA" CRLF
- サーバーは354応答を送信し、その後に送信されるデータをメールデータとして扱います
- メールデータの終端は‘.’（ピリオド）のみの行です
  - The mail data are terminated by a line containing only a period, that is, the character sequence "<CRLF>.<CRLF>”, …
- ピリオドのみの行を渡すときは“..”にします

SMTP – step 4: DATA

- SMTPで送信できるデータはASCII文字です
  - The mail data may contain any of the 128 ASCII character codes,…
- 日本語文字列やバイナリーデータ（画像などの添付ファイル）をつける時にはエンコードしてASCII文字列として送信します
  - base64 または quoted-printable
  - 参考：RFC5322, 2045~2049
- RFC1652 8BITMIMEを使えばASCII文字の制限を外せます

SMTPトランザクション

S:	220 foo.edu SMTP server ready	バナーメッセージ
C:	EHLO host.foo.edu	FQDNをアナウンスしたHELO/EHLOコマンド
S:	250-foo.edu 250-PIPELINING 250 SIZE	EHLOに対して対応するSMTP拡張を応答
C:	MAIL FROM:<chris@foo.edu>	RFC5321 From (Return-Path)を宣言 ← SPFチェック対象
S:	250 OK	成功応答
C:	RCPT TO:<pat@bar.com>	RFC5321 To (宛先mailbox)を宣言
S:	250 OK	成功応答
C:	DATA	データ送信宣言
S:	354 Start mail input; end with <CRLF>.<CRLF>	データ受信待機応答
C:	Blah blah blah... ...etc. etc. etc.	RFC5322コンテンツデータ（メールヘッダー、本文、添付ファイル）送信
C:	.	データ終端
S:	250 OK	メール処理結果を応答
C:	QUIT	コネクション終了
S:	221 foo.edu closing connection	終了応答



宛先が複数あるときは繰り返す

応答コード

- SMTPの応答コードは３桁の数字
- １桁目は応答の分類
  - 2yz　　肯定的な完了応答
  - 3yz　　肯定的な中間応答
  - 4yz　　一時的なエラー状態による否定的な完了応答
  - 5yz　　永続的なエラー状態による否定的な完了応答
- 2桁目は応答のカテゴリ
- 3桁目は応答のサブカテゴリ

SMTPを拡張するRFCリスト

- RFC1652 - SMTP Service Extension for 8bit-MIMEtransport [8BITMIME]
- RFC1830 - SMTP Service Extensions for Transmission of Large and Binary MIME Messages [CHUNKING, BINARYMIME]
- RFC1845 – SMTP Service Extension for Checkpoint/Restart [CHECKPOINT]
- RFC1870 - SMTP Service Extension for Message Size Declaration [SIZE]
- RFC2034 - SMTP Service Extension for Returning Enhanced Error Codes [ENHANCEDSTATUSCODES]
- RFC2197 - SMTP Service Extension for Command Pipelining [PIPELINING]
- RFC2852 – Deliver By SMTP Service Extension [DELIVERBY]
- RFC3207 - SMTP Service Extension for Secure SMTP over Transport Layer Security [STARTTLS]
- RFC3461 - Simple Mail Transfer Protocol (SMTP) Service Extension for Delivery Status Notifications (DSNs) [DSN]
- RFC4954 - SMTP Service Extension for Authentication [AUTH]
- RFC6531 - SMTP Extension for Internationalized Email [SMTPUTF8]
- RFC8689 - SMTP Require TLS Option [REQUIRETLS]

SMTPを拡張するRFC

代表的なMTAのEHLO応答

Gmail
250-SIZE 157286400
250-8BITMIME
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-PIPELINING
250-CHUNKING
250 SMTPUTF8

Microsoft
250-SIZE 49283072
250-PIPELINING
250-DSN
250-ENHANCEDSTATUSCODES
250-STARTTLS
250-8BITMIME
250-BINARYMIME
250-CHUNKING
250 SMTPUTF8

Hornetsecurity
250-PIPELINING
250-SIZE 157286400
250-ETRN
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN

SMTPを拡張するRFC

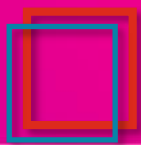
- SIZE
  - 受信可能な最大サイズを通知
- PIPELINING
  - 一度に複数コマンドを送り、まとめて応答を返す効率的な通信
- ENHANCEDSTATUSCODES
  - 詳細なエラー情報を定義
- STARTTLS
  - TLS通信が可能
- 8BITMIME
  - 8ビットMIMEデータを受信可能

RFC2034 - Enhanced Error Codes

S:	220 foo.edu SMTP server ready	
C:	EHLO host.foo.edu	
S:	250-foo.edu 250-PIPELINING 250 SIZE	
C:	MAIL FROM:<chris@foo.edu>	
S:	250 OK	250 2.1.0 Originator <chris@foo.edu> ok
C:	RCPT TO:<pat@bar.com>	
S:	250 OK	250 2.1.5 Recipient <pat@bar.com> ok
C:	DATA	
S:	354 Start mail input; end with <CRLF>.<CRLF>	
C:	Blah blah blah... ...etc. etc. etc.	
C:	.	
S:	250 OK	250 2.6.0 Message accepted
C:	QUIT	
S:	221 foo.edu closing connection	221 2.0.0 Goodbye

LMTP

Local Mail Transfer Protocol



Local Mail Transfer Protocol

- RFC2033
- Simple → Local
  - 外部への配送用ではない、内部のメッセージストアとの通信
- MDA (Message Delivery Agent)、メッセージストアへ効率的に配送
  - 複数の宛先に送る際に宛先ごとのステータスを返せる
  - SMTPは全体に対して単一のステータスを返す

LMTPトランザクション

S: 220 foo.edu LMTP server ready
C: LHLO foo.edu
S: 250-foo.edu
S: 250-PIPELINING
S: 250 SIZE
C: MAIL FROM:<chris@bar.com>
S: 250 OK
C: RCPT TO:<pat@foo.edu>
S: 250 OK
C: RCPT TO:<jones@foo.edu>
S: 550 No such user here
C: RCPT TO:<green@foo.edu>
S: 250 OK
C: DATA
S: 354 Start mail input; end with <CRLF>.<CRLF>
C: Blah blah blah...
C: ...etc. etc. etc.
C: .
S: 250 OK
S: 452 <green@foo.edu> is temporarily over quota
C: QUIT
S: 221 foo.edu closing connection

S: 220 foo.edu SMTP server ready
C: EHLO foo.edu
S: 250-foo.edu
S: 250-PIPELINING
S: 250 SIZE
C: MAIL FROM:<chris@bar.com>
S: 250 OK
C: RCPT TO:<pat@foo.edu>
S: 250 OK
C: RCPT TO:<jones@foo.edu>
S: 550 No such user here
C: RCPT TO:<green@foo.edu>
S: 250 OK
C: DATA
S: 354 Start mail input; end with <CRLF>.<CRLF>
C: Blah blah blah...
C: ...etc. etc. etc.
C: .
S: 250 OK
または 452 Requested action not taken: insufficient system storage
C: QUIT
S: 221 foo.edu closing connection

復習

RFC5322バッドプラクティス

ヘッダー

- 必須ヘッダー
  - Date
  - From
  - Message-ID
- 宛先ヘッダー(To/Cc/Bcc)
  - ヘッダーには1つ以上のアドレスを書く (one or more addresses)
  - ヘッダーは無くても良い(0~1個)
- 複数書いてはいけないヘッダーがある

Field	Min number	Max number	Notes
trace	0	unlimited	Block prepended - see 3.6.7
resent-date	0*	unlimited*	One per block, required if other resent fields are present - see 3.6.6
resent-from	0	unlimited*	One per block - see 3.6.6
resent-sender	0*	unlimited*	One per block, MUST occur with multi-address resent-from - see 3.6.6
resent-to	0	unlimited*	One per block - see 3.6.6
resent-cc	0	unlimited*	One per block - see 3.6.6
resent-bcc	0	unlimited*	One per block - see 3.6.6
resent-msg-id	0	unlimited*	One per block - see 3.6.6
orig-date	1	1	
from	1	1	See sender and 3.6.2
sender	0*	1	MUST occur with multi-address from - see 3.6.2
reply-to	0	1	
to	0	1	
cc	0	1	
bcc	0	1	
message-id	0*	1	SHOULD be present - see 3.6.4
in-reply-to	0*	1	SHOULD occur in some replies - see 3.6.4
references	0*	1	SHOULD occur in some replies - see 3.6.4
subject	0	1	
comments	0	unlimited	
keywords	0	unlimited	
optional-field	0	unlimited	

宛先ヘッダー（To/Cc/Bcc）

- 宛先ヘッダー(To/Cc/Bcc)
  - ヘッダーには1つ以上のアドレスを書く
    (one or more addresses)
  - 複数のアドレスはカンマ区切りで1つのヘッダーに書く
  - 宛先ヘッダーは無くても良い(0~1個)
    →アドレスが無ければ付けない
- 間違った例：

To: ”Mr. Foo" <foo@example.com >
❌Cc: アドレスが空の宛先ヘッダーは付けない
❌Bcc: <bar@example.com> Bccは送らない（見えてしまうとBlind Ccにならない）

必須ヘッダがない

- Dateがない例

```
        for <aaaaaaaa@xxxxxxxx.xx.jp>; Thu, 26 Oct 2023 00:07:56 +0900
Received: (from nobody@localhost)
        by cp24-web-asg.i-0246a39c017c97696 (8.14.7/8.14.7/Submit) id 39PF7ueG022651;
        Thu, 26 Oct 2023 00:07:56 +0900
Message-Id: <202310250507.39PF7ueG022651@cp24-web-asg.i-0246a39c017c97696>
To: aaaaaaaa@xxxxxxxx.xx.jp
Subject: =?utf-8?B?44GT44Cg44K4440j440L440844K6V0VTVOOBruWkj...?=
From: info@xxxxxxxx-yyyyyyyy.jp
Mime-Version: 1.0
X-Mailer-Unique-Code:
Content-Type: text/plain; charset="utf-8"
Content-Transfer-Encoding: base64

44GT44Gu5bqm44Gv44CQ44K4440j440L440844K6V0VTVOOBruWkj+S8keOBvzIwMjMg44Cc56We
44Gh44KD44KT77yG5rWB5pifIOelnTMw5q2z77yB440P440D440U4408440Q440844K5440H4408
```

- Message-ID:は内容の確認も重要
- Date:とMessage-ID:は忘れずに付けて送りましょう

Thank you