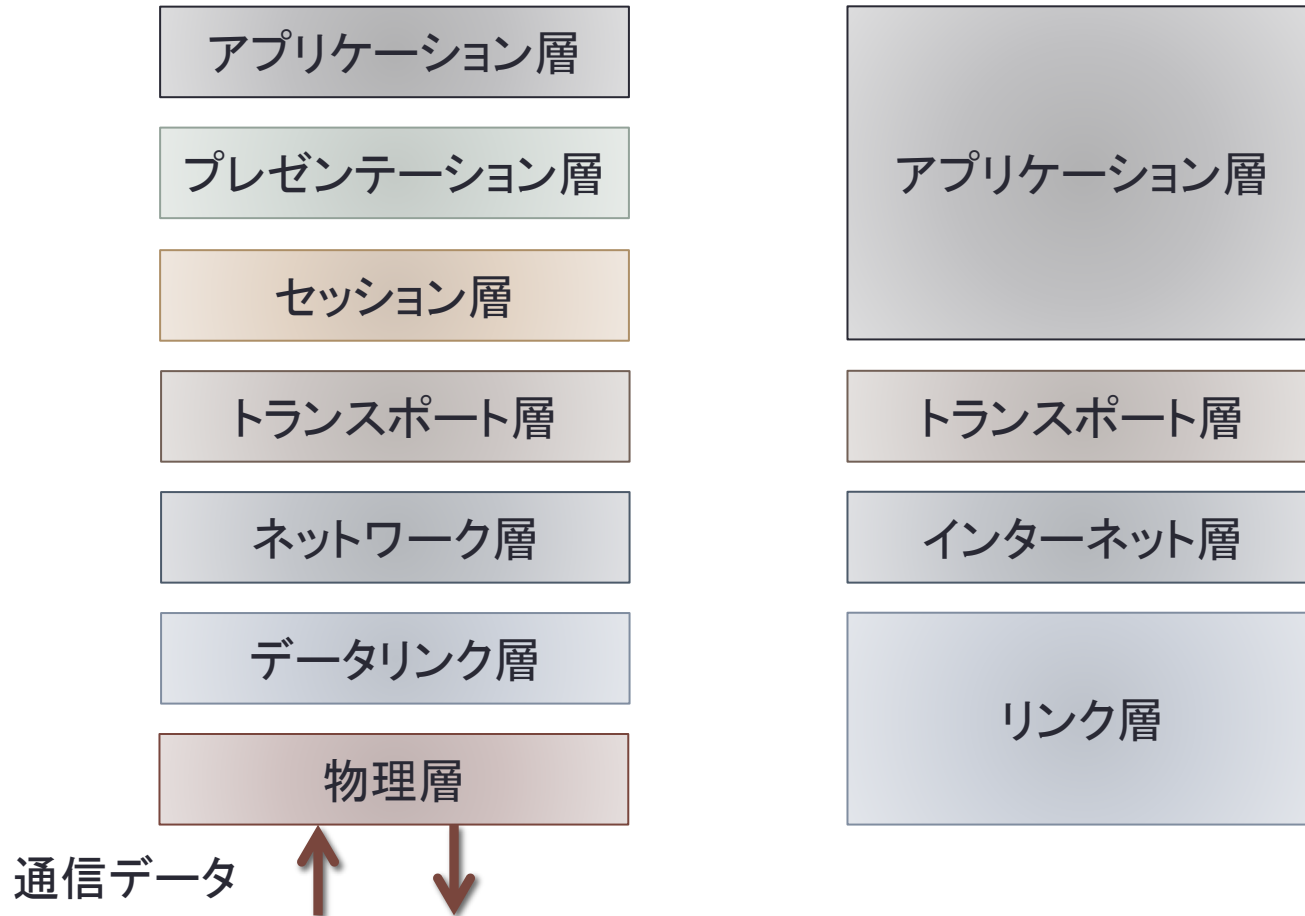


情報通信ネットワーク 第10回

理工学部情報科学科

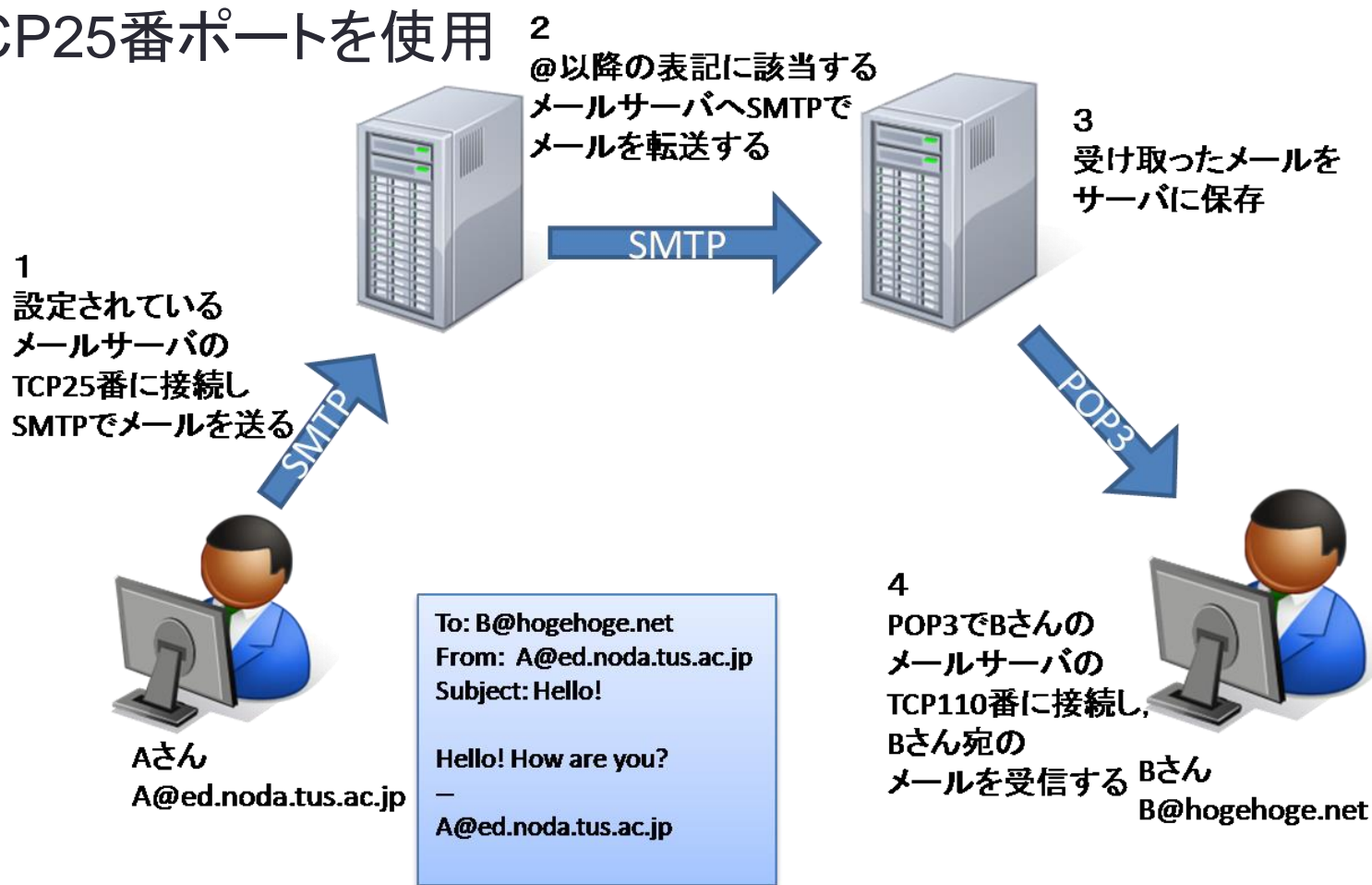
松澤 智史

本日は……アプリケーション層



SMTP(Simple Mail Transfer Protocol)

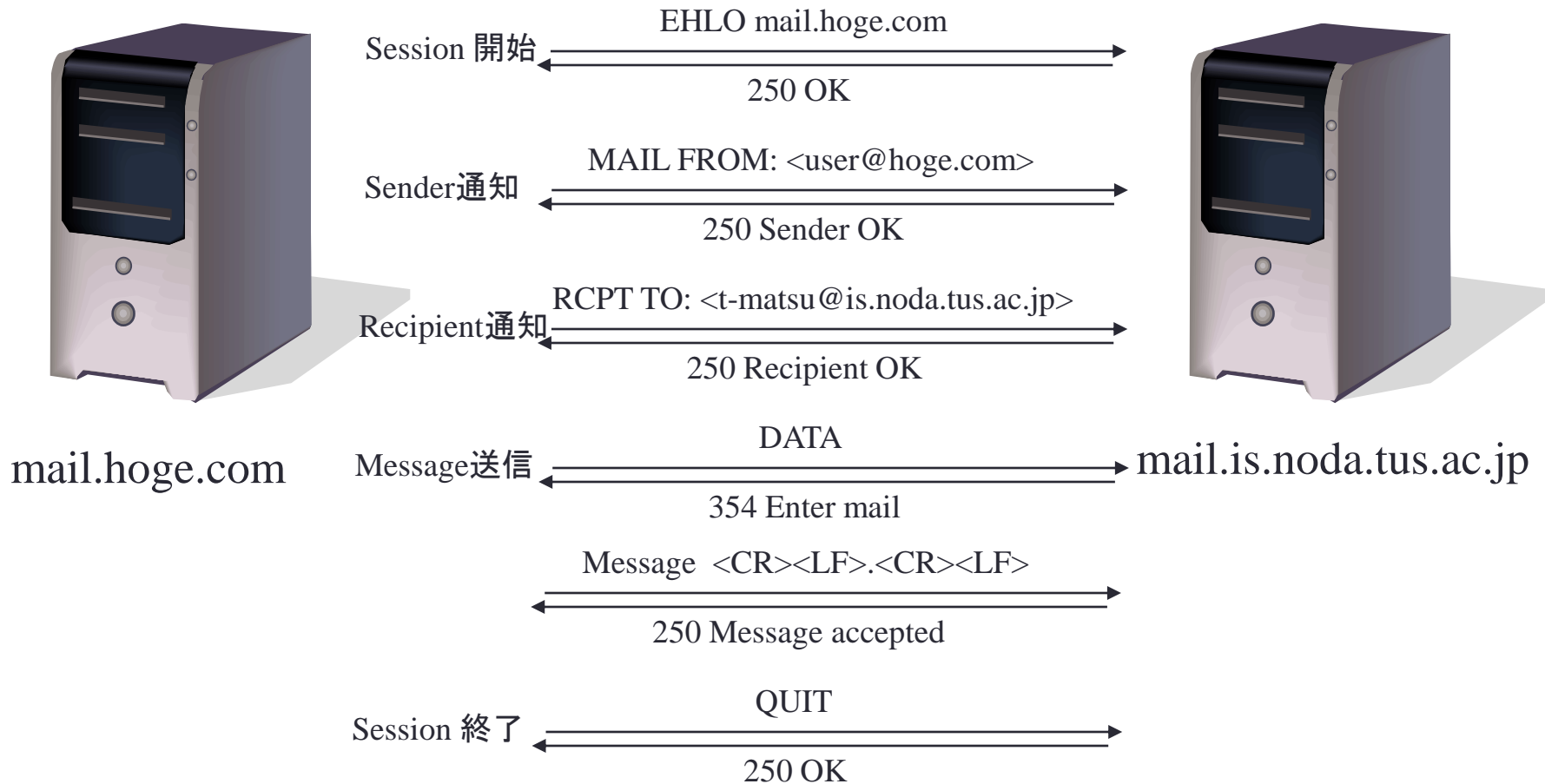
- メールの転送を行うプロトコル
- TCP25番ポートを使用



SMTPの特徴

- 7ビットの文字(テキスト)のみ転送可能
- SMTPの拡張版のESMTP(Extend SMTP)では8ビット文字に対応している ※現在はほぼESMTPが利用されている
- バイナリデータを送信するには別途Base64等を用いてテキストに変換する必要がある(後述)

SMTPのプロトコル

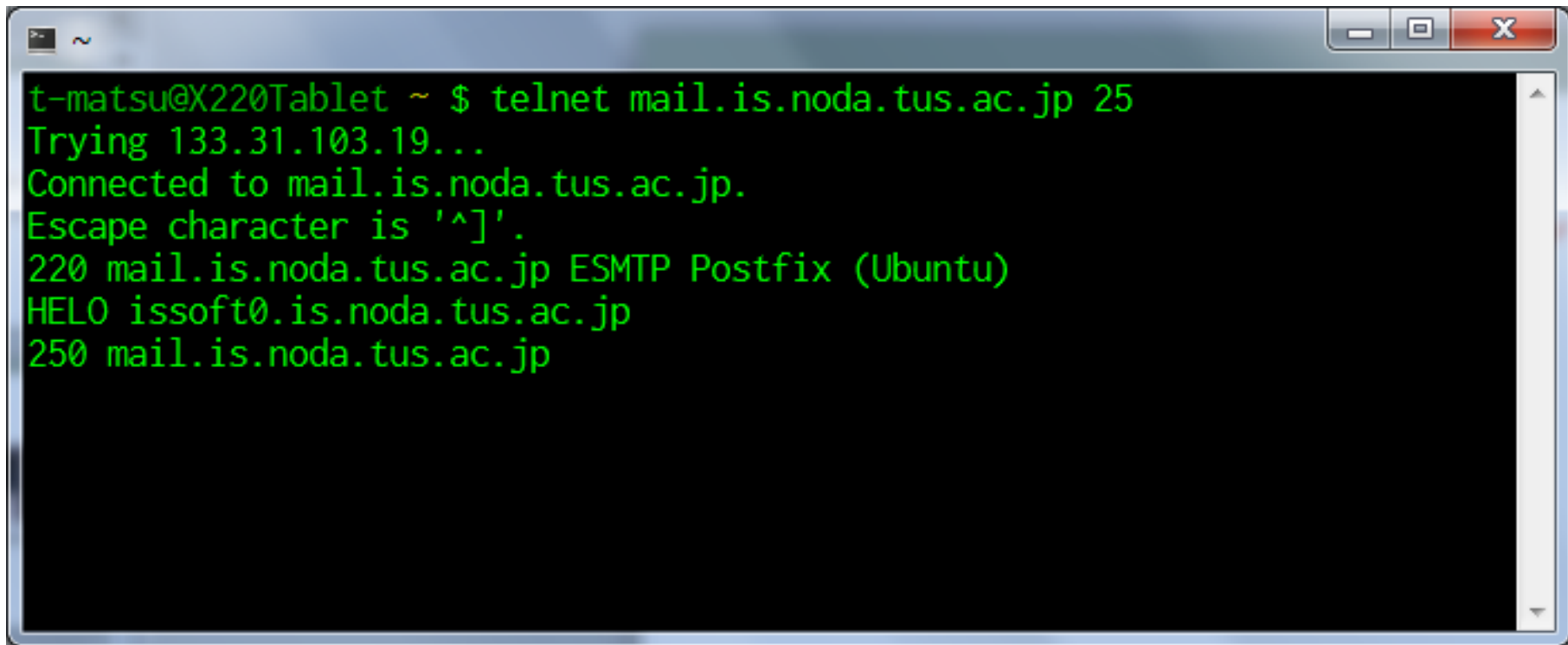


SMTPのコマンド

- HELO
- EHLO
- AUTH
- STARTTLS
- MAIL FROM
- RCPT TO
- DATA
- BDAT
- QUIT
- RSET
- VRFY
- EXPN
- HELP
- NOOP

実際にコマンドを入力してみる

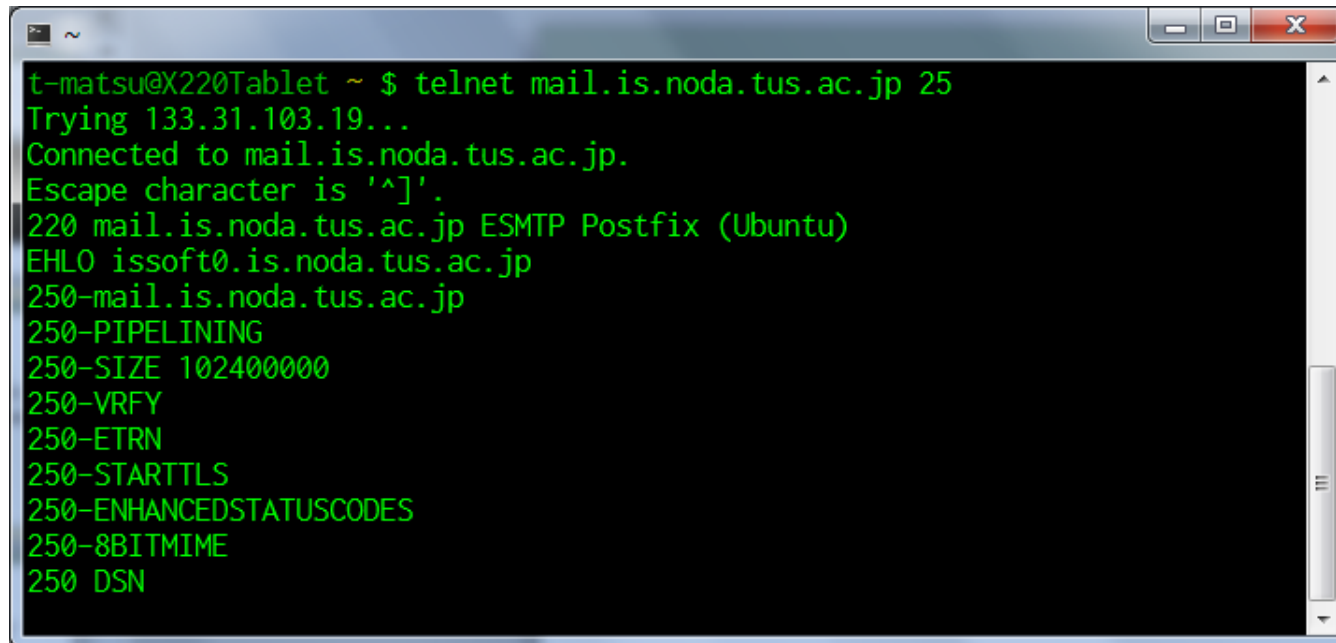
\$ telnet *Mail_Server* 25

A terminal window with a blue title bar and standard window controls. The text inside is green on a black background. It shows a telnet session from a user named t-matsu on a machine named X220Tablet. The user enters the command 'telnet mail.is.noda.tus.ac.jp 25'. The terminal shows the connection attempt to IP 133.31.103.19, successful connection, escape character information, and the SMTP banner from the mail server.

```
t-matsu@X220Tablet ~ $ telnet mail.is.noda.tus.ac.jp 25
Trying 133.31.103.19...
Connected to mail.is.noda.tus.ac.jp.
Escape character is '^]'.
220 mail.is.noda.tus.ac.jp ESMTP Postfix (Ubuntu)
HELO issoft0.is.noda.tus.ac.jp
250 mail.is.noda.tus.ac.jp
```

HELO, EHLO

- 書式: HELO(EHLO) SMTPクライアントのFQDN
- 現状: 必須
- EHLOはHELOの拡張版で, 利用できるサービスなどをサーバが通知してくれる
- FQDNの代わりにSMTPクライアントのIPアドレスでも良い

A terminal window titled '~' showing a telnet session. The user has connected to mail.is.noda.tus.ac.jp on port 25. The server responds with a list of supported extensions including ESMTP, PIPELINING, SIZE, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, and DSN.

```
t-matsu@X220Tablet ~ $ telnet mail.is.noda.tus.ac.jp 25
Trying 133.31.103.19...
Connected to mail.is.noda.tus.ac.jp.
Escape character is '^]'.
220 mail.is.noda.tus.ac.jp ESMTP Postfix (Ubuntu)
EHLO issoft0.is.noda.tus.ac.jp
250-mail.is.noda.tus.ac.jp
250-PIPELINING
250-SIZE 102400000
250-VRFY
250-ETRN
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
```


AUTH

- 書式: AUTH 使用メカニズム
- 現状: 実装されていることもある
- SASL(RFC2222)を利用して相互認証を行う
- 利用できるアルゴリズムはEHLOで通知される

STARTTLS

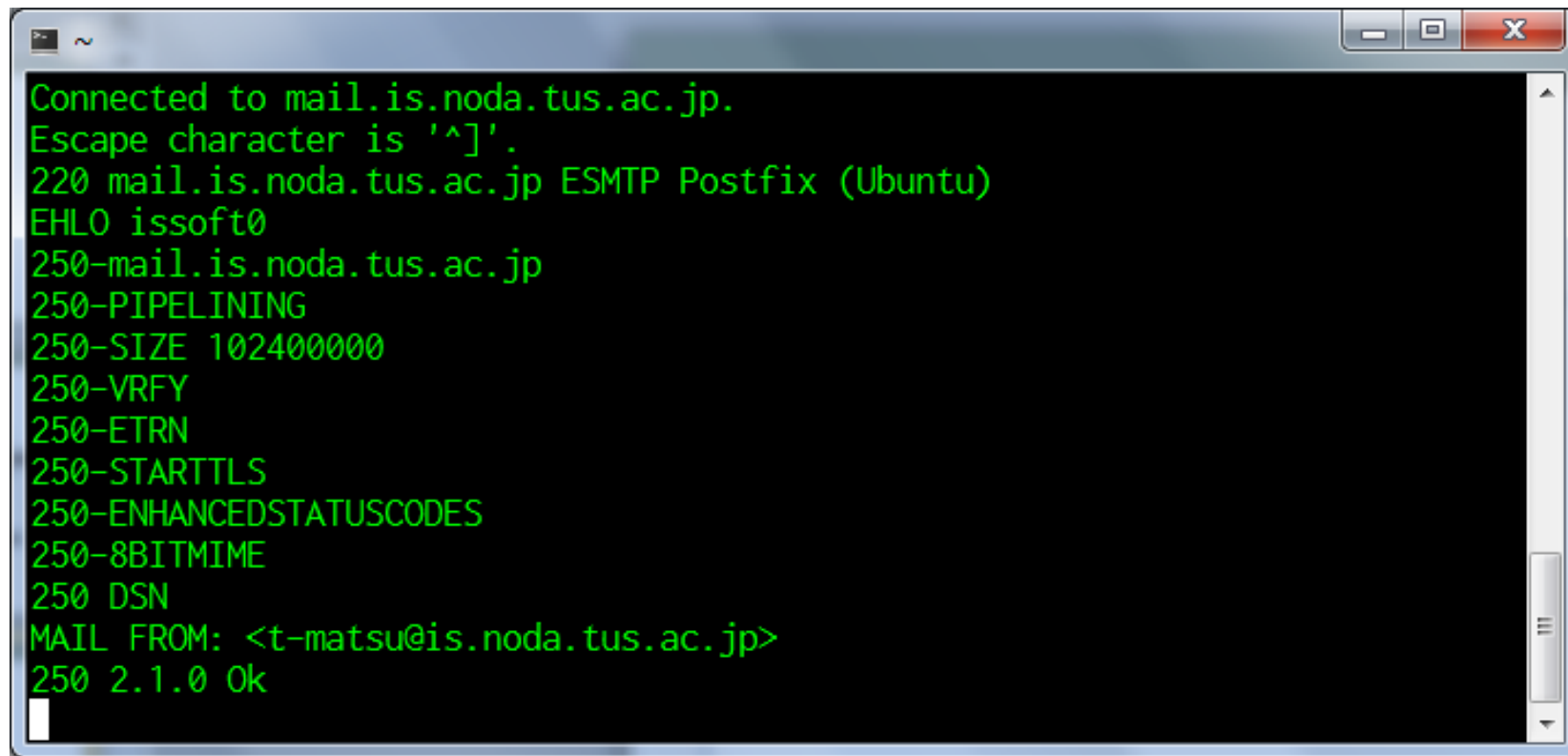
- 書式: STARTTLS
- 現状: 実装されていることもある
- TLS(Transport Layer Security, RFC 2246)による通信を開始する. その後の通信がTLSにより暗号化される.

TLS

- SSL(Secure Socket Layer)の別名称
- sshやhttpsなどの暗号化にも使われるハイブリット暗号

MAIL FROM

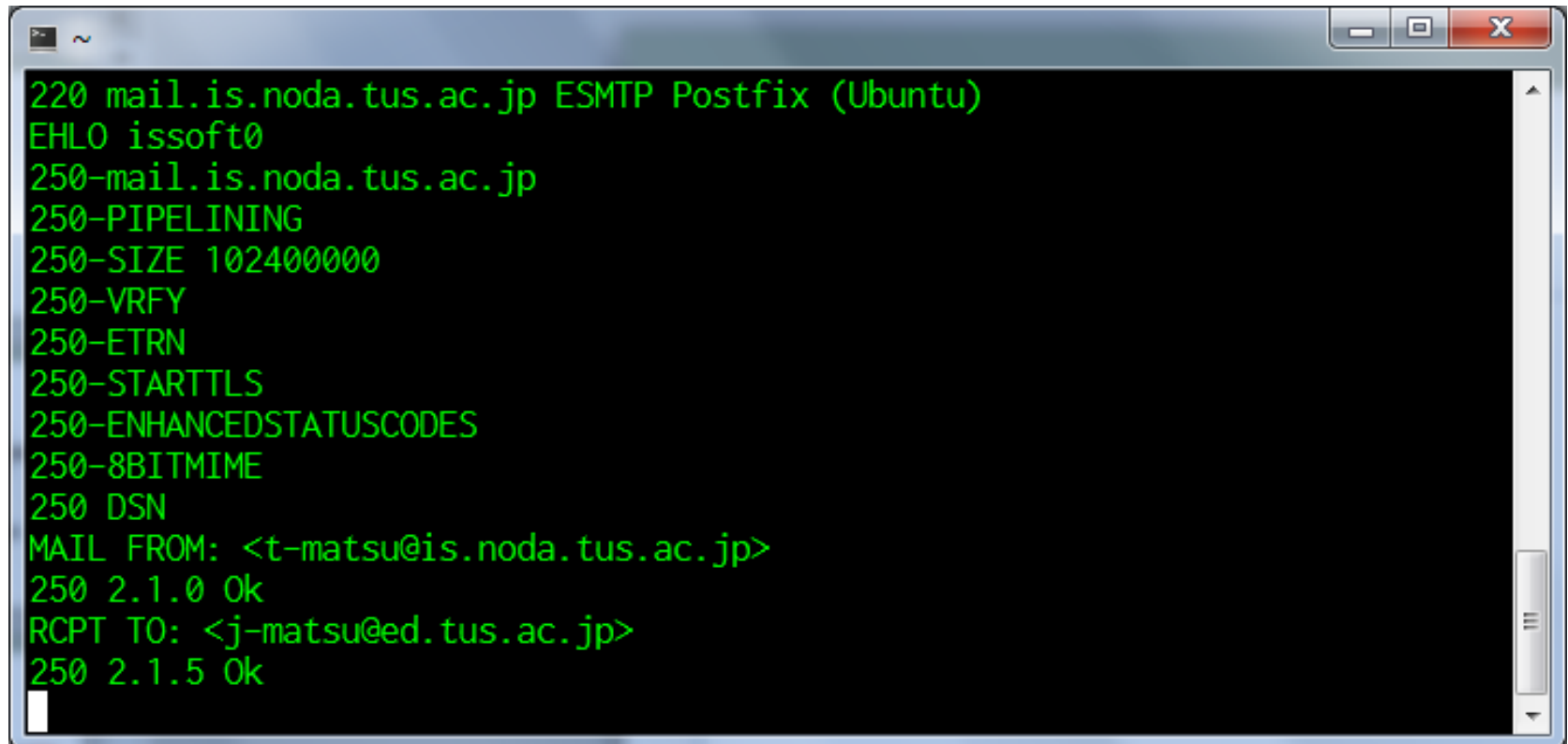
- 書式: MAIL FROM メールアドレス
- 現状: 必須
- メールの送り主を示す

A terminal window with a blue title bar and standard window controls. The text inside is green on a black background, showing an SMTP session. The user has entered 'EHLO issoft0' and the server has responded with various capabilities. The user then enters 'MAIL FROM: <t-matsu@is.noda.tus.ac.jp>' and the server responds with '250 2.1.0 Ok'.

```
Connected to mail.is.noda.tus.ac.jp.  
Escape character is '^]'.  
220 mail.is.noda.tus.ac.jp ESMTP Postfix (Ubuntu)  
EHLO issoft0  
250-mail.is.noda.tus.ac.jp  
250-PIPELINING  
250-SIZE 102400000  
250-VERFY  
250-ETRN  
250-STARTTLS  
250-ENHANCEDSTATUSCODES  
250-8BITMIME  
250 DSN  
MAIL FROM: <t-matsu@is.noda.tus.ac.jp>  
250 2.1.0 Ok  
█
```

RCPT TO

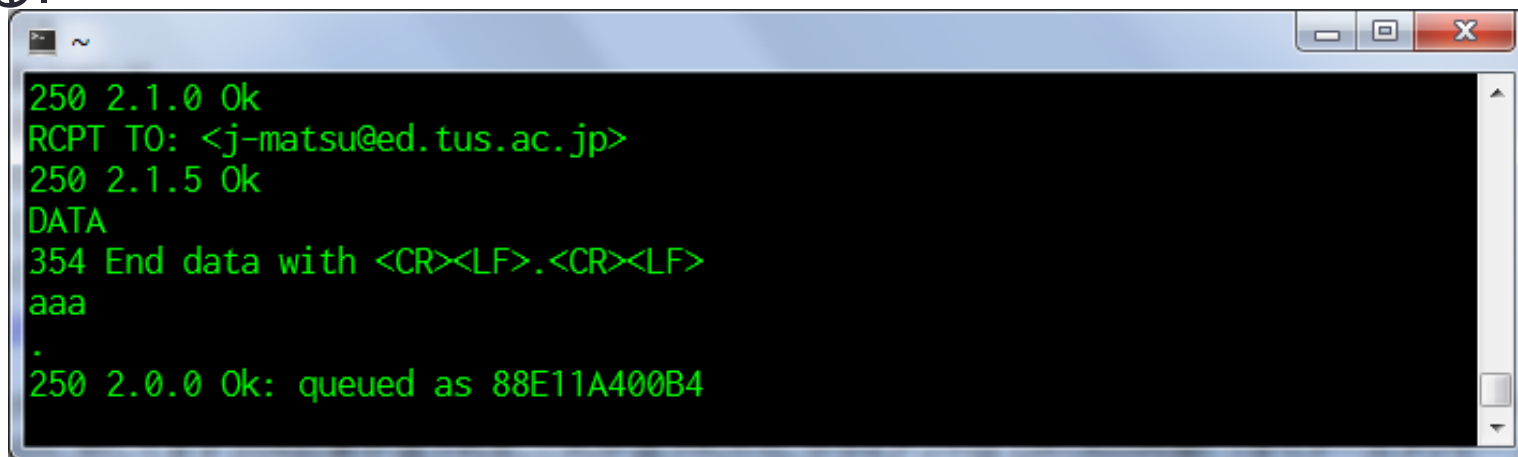
- 書式: RCPT TO メールアドレス
- 現状: 必須
- 受信者を指定する

A screenshot of a terminal window showing an SMTP session. The window has a title bar with standard Linux window controls (minimize, maximize, close). The text is green on a black background. The session starts with a 220 greeting from mail.is.noda.tus.ac.jp. The client sends EHLO issoft0, and the server responds with 250-mail.is.noda.tus.ac.jp and a list of supported extensions: PIPELINING, SIZE 102400000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, and DSN. The client then sends MAIL FROM: <t-matsu@is.noda.tus.ac.jp>, and the server responds with 250 2.1.0 Ok. Finally, the client sends RCPT TO: <j-matsu@ed.tus.ac.jp>, and the server responds with 250 2.1.5 Ok. A cursor is visible at the end of the last line.

```
220 mail.is.noda.tus.ac.jp ESMTP Postfix (Ubuntu)
EHLO issoft0
250-mail.is.noda.tus.ac.jp
250-PIPELINING
250-SIZE 102400000
250-VRFY
250-ETRN
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
MAIL FROM: <t-matsu@is.noda.tus.ac.jp>
250 2.1.0 Ok
RCPT TO: <j-matsu@ed.tus.ac.jp>
250 2.1.5 Ok
```

DATA

- 書式: DATA
- 現状: 必須
- メールデータを送信するコマンド
- 引数はなく, DATAコマンドの直後からヘッダ, 本文を送る
- データの終端はピリオド「.」の行(改行, ピリオド, 改行)で示す
- ピリオドのみの本文を送る場合は「..」のようにピリオドを2つにする.

A screenshot of a terminal window with a blue title bar and standard window controls. The terminal has a black background with green text. It shows the output of an SMTP session, including status codes, RCPT TO: addresses, and the DATA command being processed. The text is as follows:

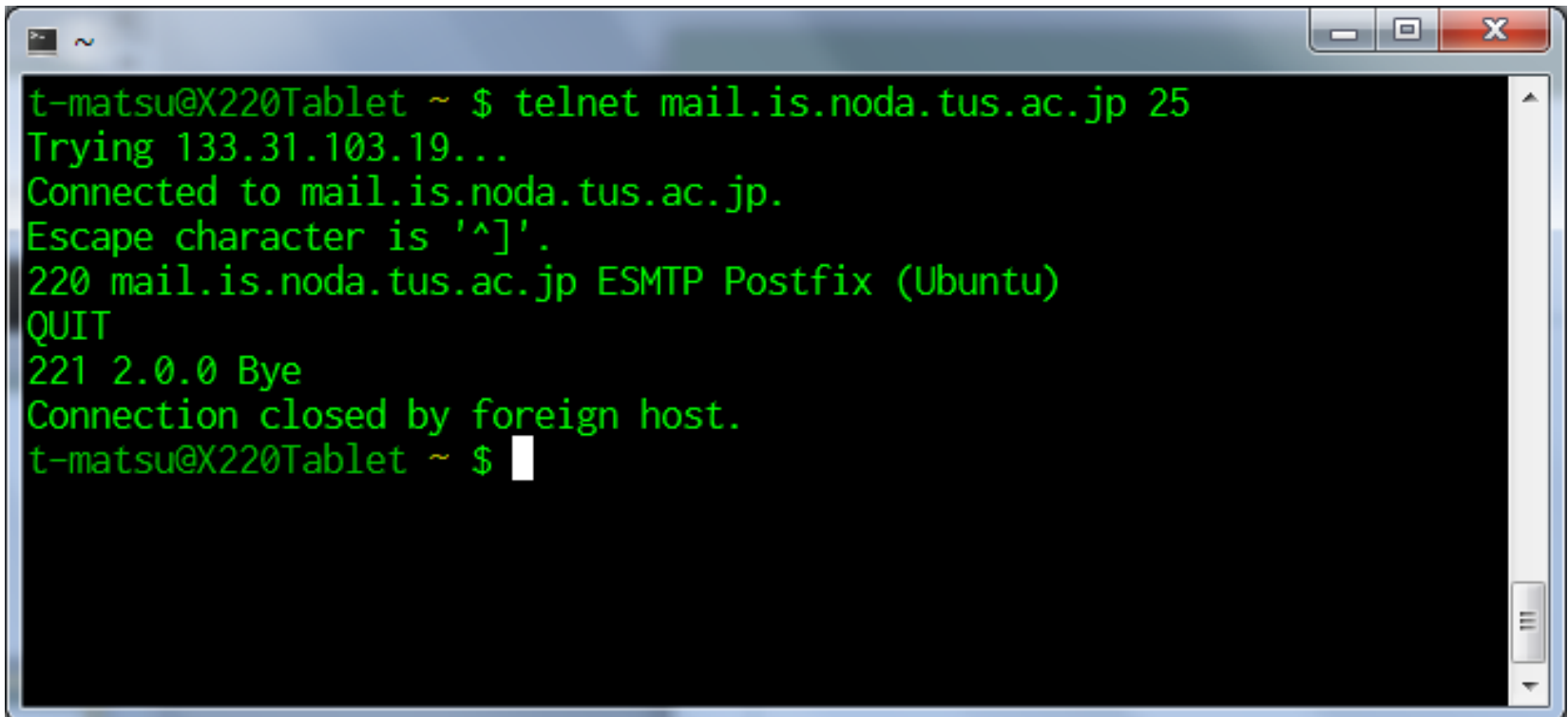
```
250 2.1.0 Ok
RCPT TO: <j-matsu@ed.tus.ac.jp>
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
aaa
.
250 2.0.0 Ok: queued as 88E11A400B4
```

BDAT

- 書式: BDAT (転送するオクテット数) [LAST]
- 現状: ほとんどのサーバで未実装
- バイナリデータを送る
- 指定したオクテット数のデータを送ると終了する
- BDATとDATAは同時に利用できない

QUIT

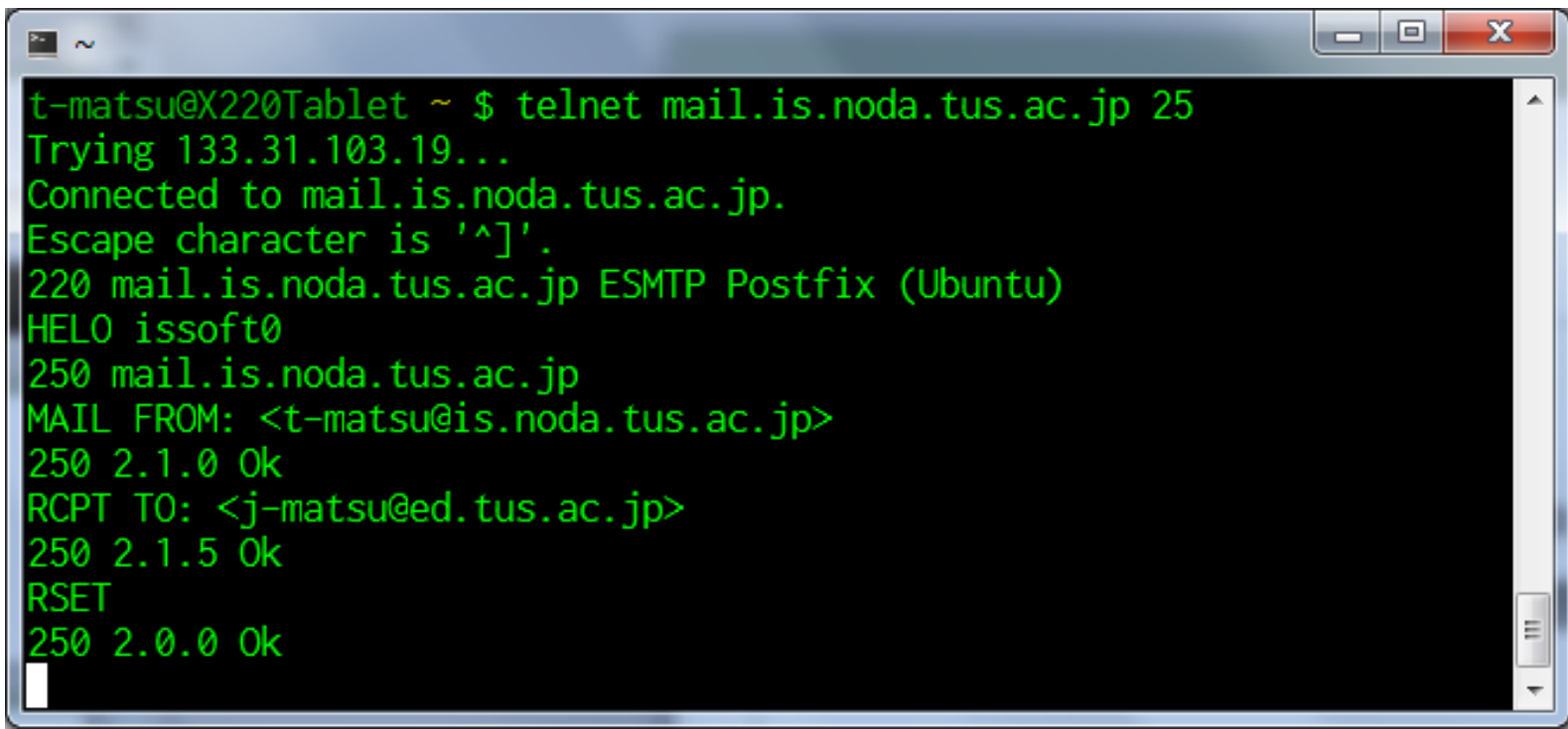
- 書式: QUIT
- 現状: 必須
- メールセッションを終了する

A terminal window with a dark background and green text. The window title bar shows a tilde icon and standard Linux window controls (minimize, maximize, close). The text in the terminal shows a telnet session initiated from a host named 't-matsu@X220Tablet'. The user enters 'telnet mail.is.noda.tus.ac.jp 25'. The terminal shows the connection attempt, the IP address '133.31.103.19...', and the successful connection to 'mail.is.noda.tus.ac.jp'. It displays the escape character '^]' and the server response '220 mail.is.noda.tus.ac.jp ESMTP Postfix (Ubuntu)'. The user then enters 'QUIT', and the server responds '221 2.0.0 Bye'. Finally, the terminal shows 'Connection closed by foreign host.' and the prompt 't-matsu@X220Tablet ~ \$' with a cursor.

```
t-matsu@X220Tablet ~ $ telnet mail.is.noda.tus.ac.jp 25
Trying 133.31.103.19...
Connected to mail.is.noda.tus.ac.jp.
Escape character is '^]'.
220 mail.is.noda.tus.ac.jp ESMTP Postfix (Ubuntu)
QUIT
221 2.0.0 Bye
Connection closed by foreign host.
t-matsu@X220Tablet ~ $
```

RSET

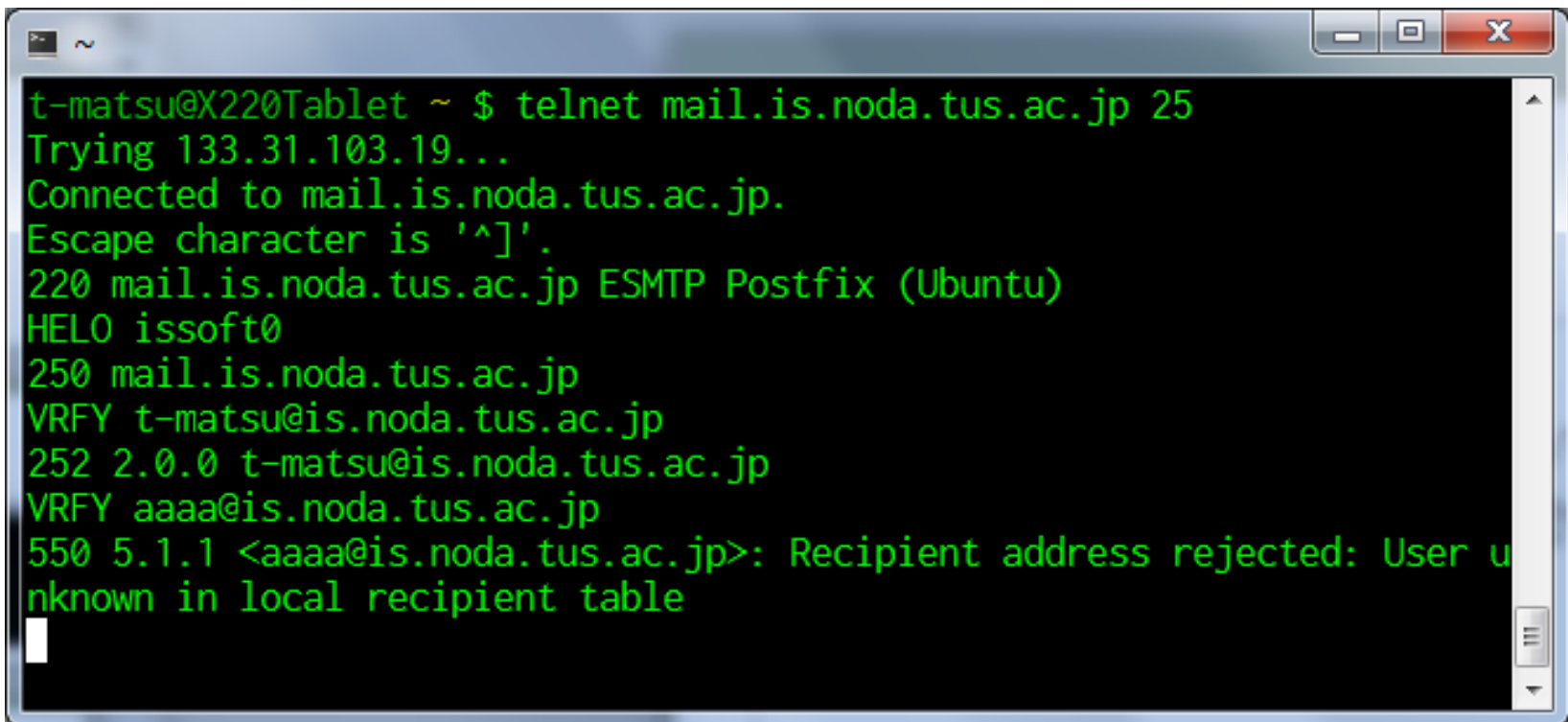
- 書式: RSET
- 現状: 必須
- 現在のメールトランザクションを中止する
(HELOまたはEHLO直後の状態にもどる)

A terminal window with a dark background and green text. The window title bar shows a home icon, a tilde symbol, and standard window controls (minimize, maximize, close). The text in the terminal shows a telnet session to mail.is.noda.tus.ac.jp. The user enters '25' and the server responds with '220 mail.is.noda.tus.ac.jp ESMTTP Postfix (Ubuntu)'. The user then enters 'HELO issoft0' and the server responds with '250 mail.is.noda.tus.ac.jp'. The user enters 'MAIL FROM: <t-matsu@is.noda.tus.ac.jp>' and the server responds with '250 2.1.0 Ok'. The user enters 'RCPT TO: <j-matsu@ed.tus.ac.jp>' and the server responds with '250 2.1.5 Ok'. Finally, the user enters 'RSET' and the server responds with '250 2.0.0 Ok'.

```
t-matsu@X220Tablet ~ $ telnet mail.is.noda.tus.ac.jp 25
Trying 133.31.103.19...
Connected to mail.is.noda.tus.ac.jp.
Escape character is '^]'.
220 mail.is.noda.tus.ac.jp ESMTTP Postfix (Ubuntu)
HELO issoft0
250 mail.is.noda.tus.ac.jp
MAIL FROM: <t-matsu@is.noda.tus.ac.jp>
250 2.1.0 Ok
RCPT TO: <j-matsu@ed.tus.ac.jp>
250 2.1.5 Ok
RSET
250 2.0.0 Ok
```


VRFY

- 書式: VRFY メールアドレス
- 現状: セキュリティ上無効になっていることもある
- メールアドレスが存在するか確認する



```
t-matsu@X220Tablet ~ $ telnet mail.is.noda.tus.ac.jp 25
Trying 133.31.103.19...
Connected to mail.is.noda.tus.ac.jp.
Escape character is '^]'.
220 mail.is.noda.tus.ac.jp ESMTP Postfix (Ubuntu)
HELO issoft0
250 mail.is.noda.tus.ac.jp
VRFY t-matsu@is.noda.tus.ac.jp
252 2.0.0 t-matsu@is.noda.tus.ac.jp
VRFY aaaa@is.noda.tus.ac.jp
550 5.1.1 <aaaa@is.noda.tus.ac.jp>: Recipient address rejected: User unknown in local recipient table
```

EXPN

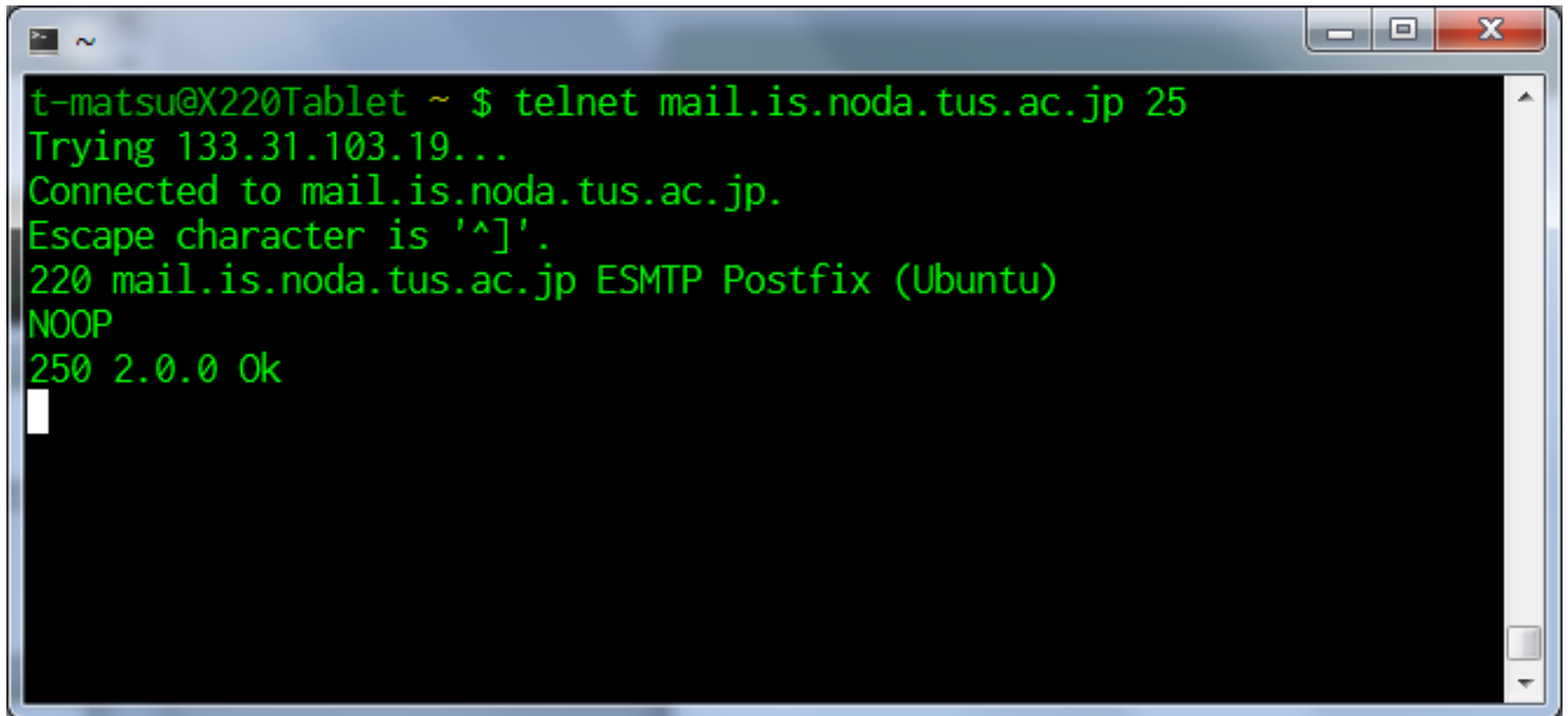
- 書式: EXPN アドレス
- 現状: セキュリティ上無効になっていることもある
- メーリングリストアドレスであればメンバーリストを表示する
- 対象が個人のメールアドレスであればVRFYと同じように振舞うかエラーを返答する(実装により異なる)

HELP

- 書式: `HELP コマンド名`
- 現状: 実装されていることもある
- 引数にコマンド名を入れるとそのコマンドのヘルプを返答する
- 引数無しの場合は簡単なヘルプを返答する

NOOP

- 書式: NOOP
- 現状: 必須
- なにもしない(NO OPeration)

A terminal window with a dark background and green text. The window title bar shows a home icon, a tilde symbol, and standard window controls (minimize, maximize, close). The text in the terminal shows a telnet session initiated from a host named 't-matsu@X220Tablet'. The user connects to 'mail.is.noda.tus.ac.jp' on port 25. The server responds with '220 mail.is.noda.tus.ac.jp ESMTP Postfix (Ubuntu)'. The user then sends the 'NOOP' command, and the server responds with '250 2.0.0 Ok'.

```
t-matsu@X220Tablet ~ $ telnet mail.is.noda.tus.ac.jp 25
Trying 133.31.103.19...
Connected to mail.is.noda.tus.ac.jp.
Escape character is '^]'.
220 mail.is.noda.tus.ac.jp ESMTP Postfix (Ubuntu)
NOOP
250 2.0.0 Ok
```

E-Mailは簡単に偽装できる

- Fromは送信側が自己申告
- なりすまし可能
→犯罪の温床となる
- 低いコストで送信可能
 - なりすましと合わせると凶悪なツールとなる

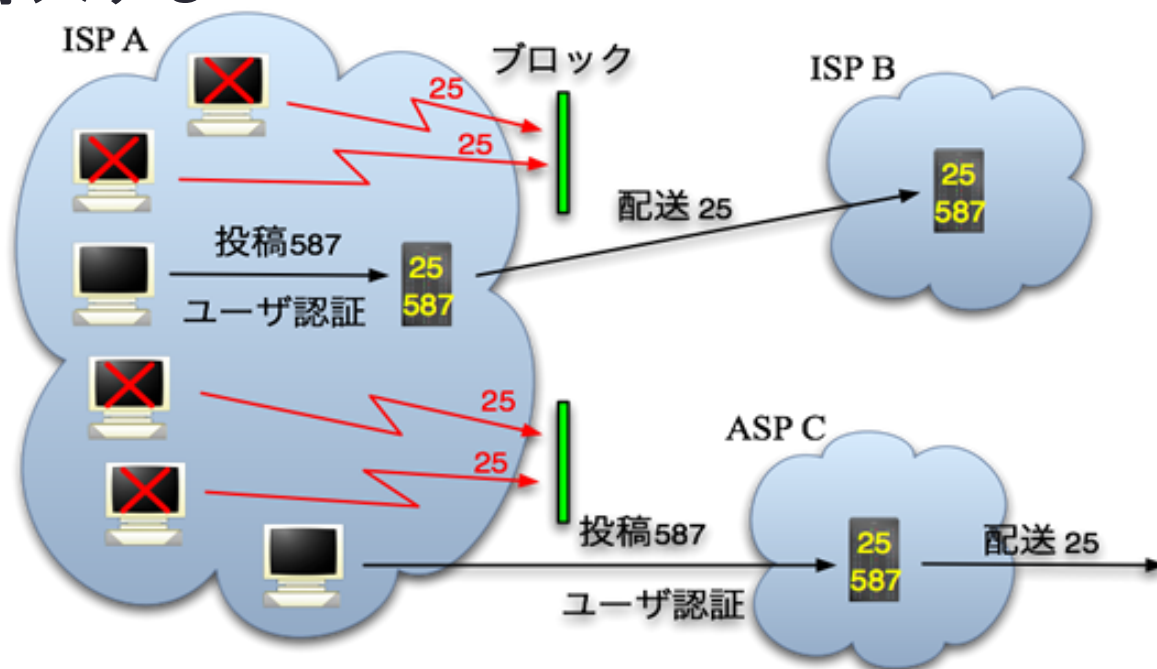
SMTPとあわせて使用される技術

- OP25B (Outbound port 25 Blocking)
- POP before SMTP
- SMTP認証

これらはすべてSMTPのセキュリティの欠如をカバーするための追加技術で、SPAMメール対策の技術である

OP25B (Outbound port 25 Blocking)

- 外に出るパケットの25番ポートをルータでブロックする
 - 25番ポートを通すのは内部のメールサーバからの接続のみ
 - このままだと外部のメールサーバを利用しているユーザも遮断する
- 代替ポート(投稿(Submission)ポート)587を設ける
- 配送に認証を導入する



POP before SMTP

- SMTPの認証を行う技術である
- POPにはユーザ認証があるため、SMTPの送信を行う前にPOPでの接続を行わせる

- POPでの接続後一定時間はSMTP送信が可能になる



メールサーバー

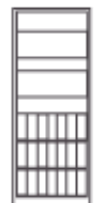
誰だかわからない人のメールは送れないから**拒否**

- 従来のSMTPとPOPをあわせたものなので、メールクライアントに追加の実装等は一切必要ない



メールの受信 →

メールの送信 →



メールサーバー

受信は認証があるから**OK**
送信も直前の受信と同じアドレスからなので**OK**

SMTP認証(SMTP Authentication)

- SMTPを拡張したESMTPで追加実装された認証機能
- メール送信時にアカウント, パスワードを求めるように変更
- ユーザのメールクライアントも対応していないと使用できない

近年はほとんどのメールクライアントが対応したため,
POP before SMTPよりSMTP認証を用いられることが多い

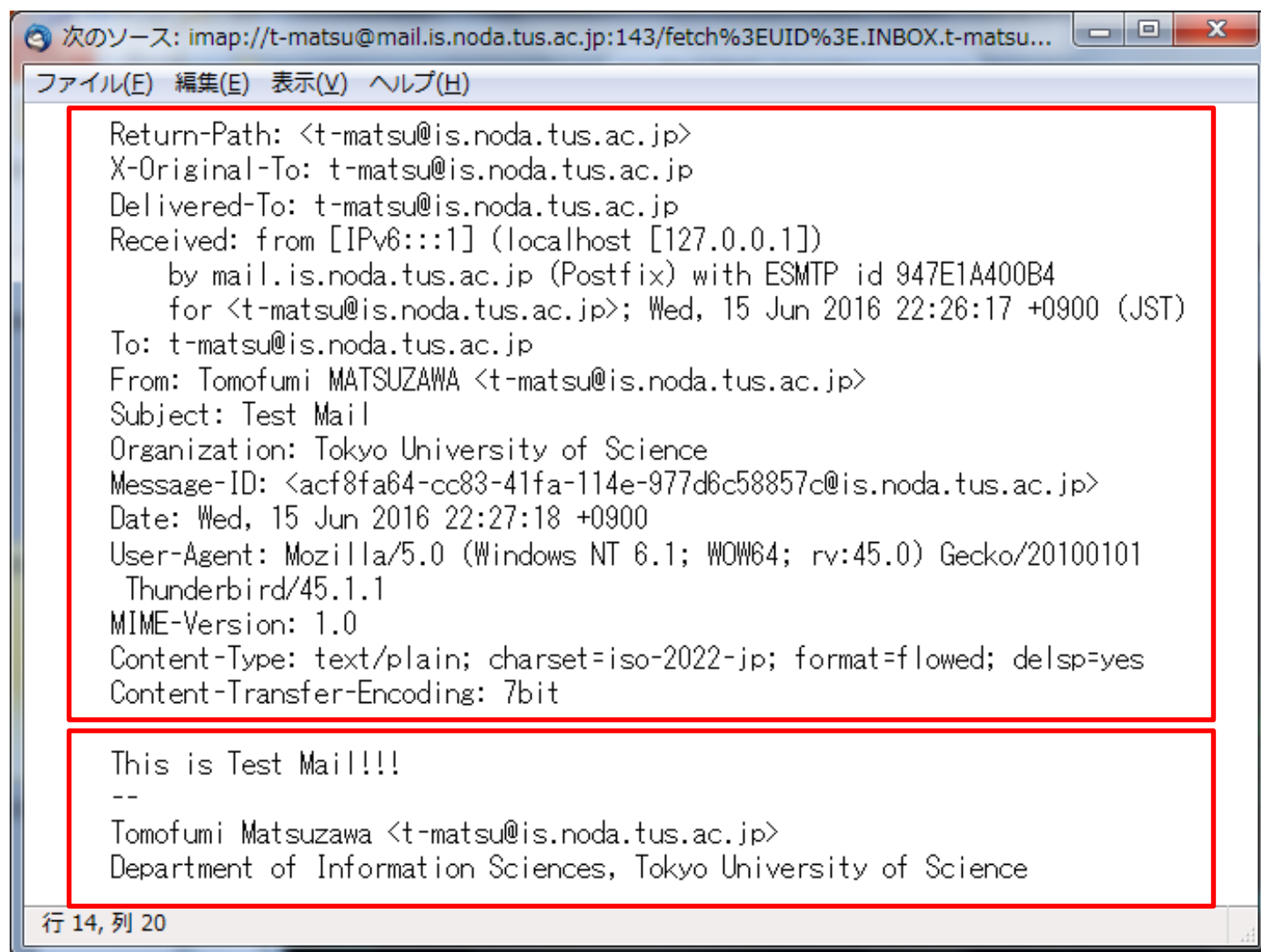
電子メールのヘッダとボディ

メールはヘッダとボディに分けられる

- ヘッダ
 - ヘッダ名：内容の書式
- ボディ
 - 本文

どちらもDATAで送る

電子メールのヘッダとボディ



ヘッダ

ボディ

MIME

- Multipurpose Internet Mail Extensions
- 規格上ASCII(テキスト)のみしか扱えないメールで様々なフォーマットを扱えるように拡張した規格
- MIMEで導入されたヘッダ
 - MIME-Version 現在は1.0のみ
 - Content-Type
text/plain text/html image/png video/mpeg application/pdf など
 - Content-Transfer-Encoding
7bit 8bit base64 binary など 8bitとbinaryは特殊条件が必要

Base64

- Binaryファイルを(無理やり)テキストに変換するルール
- 送信側でテキストに変換し, 受信側でBinaryに復元する
- 変換ルール
 - 元データを6ビットずつに分割
 - 各6ビットの値を変換表を使って4文字ずつ変換
- 変換表
 - A-Z a-z 0-9 + / =を使う (=は余った部分を埋める際に使う)
 - 000000→A 000001→B 000010→C...110011→z 110100→0...
111101→9 111110→+ 111111→/
- 変換例 (文字列: “ABCD”の場合)
 - 16進数: 41,42,43,44 2進数: 01000001, 01000010, 01000011, 0100 0100
 - 6ビットごとに分割 010000, 010100, 001001, 000011, 010001, 000000
 - 4文字ずつ変換 QUJD RA==

ファイル(E) 編集(E) 表示(V) ヘルプ(H)

From: Tomofumi MATSUZAWA <t-matsu@is.noda.tus.ac.jp>
Subject: base64 test
Organization: Tokyo University of Science
Message-ID: <9bb9d36f-7d0a-9b5b-96ba-cfdc19b03b9c@is.noda.tus.ac.jp>
Date: Thu, 16 Jun 2016 10:55:47 +0900
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:45.0) Gecko/20100101
Thunderbird/45.1.1
MIME-Version: 1.0
Content-Type: multipart/mixed;
boundary="-----65AC7D1BA2BEC21D2A116526"

This is a multi-part message in MIME format.

-----65AC7D1BA2BEC21D2A116526

Content-Type: text/plain; charset=iso-2022-jp; format=flowed; delsp=yes

Content-Transfer-Encoding: 7bit

base64 test mail.

--

Tomofumi Matsuzawa <t-matsu@is.noda.tus.ac.jp>

Department of Information Sciences, Tokyo University of Science

-----65AC7D1BA2BEC21D2A116526

Content-Type: application/pdf;

name="=?UTF-8?B?5p2+5r6k5pm65Y+yMjUzNTA0ODIucGRm?="

Content-Transfer-Encoding: base64

Content-Disposition: attachment;

filename*0*=iso-2022-jp''%1B%24%42%3E%3E%5F%37%43%52%3B%4B%1B%28%42%32%35;

filename*1*=%33%35%30%34%38%32%2E%70%64%66

JVBERi0xLjQNCiXl48/TDQozMCAwIG9iag0KPDwgDQovTGluZWYyaXpIZCAxIA0KL0wgMjQz
MzI3IA0KL0ggWyaA4NzIgMjQIF0gDQovTyAzMyANCi9FIDU4ODMwIA0KL04gNCANCi9UIDI0
MjYwMSANCi4+IA0KZW5kb2JqDQogICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAg
ICAgICAgICAgICB4cmVmDQozMCAxNA0KMDAwMDAwMDAwNyAwMDAwMCAuIA0wMDAwMDAwNjYx

今回のまとめ

- SMTP
 - メール転送プロトコル
 - 古いプロトコルであるため、セキュリティ等様々な問題がある
 - 近年では、POP before SMTPやOP25B,SMTP認証など追加の技術と一緒に使用される
- 電子メール
 - ヘッダ部とボディ部にわかれる
 - 仕様上7bitテキストしか扱えない
 - Binaryに対応したMIME (Base64など)が用いられている

質問あればどうぞ

次回はアプリケーション層(つづき)！