

(2020/12/11)

---

# メール配送システム

北海道大学 大学院理学院 宇宙理学専攻  
修士課程 1年  
茂木 遥平 / YOHEI MOTOKI

# 誰が為のプレゼンテーションか

---

## 注意

このプレゼンテーションは北海道大学EPネットワーク利用者のB4に向けてメールサーバー管理者を決める上で必要となりそうな知識を教授するためのモノです。

携帯メール, webメール,  
PCのメールソフトを介したメールなど

- 配送にはサーバ・クライアントシステムを使用
  - **メールサーバ**を経由した配送

# 目次

---

- メール配送の仕組み
- 一年間で茂木がしたこと
- EPメールサーバーの歴史と将来
- メール利用の際の注意

---

# メール配送の仕組み

---

# 電子メール(e-mail)とは

---

電子メール

ネットワークを通じてやりとりするメッセージの一つ(LINEは含まない)

携帯メール, webメール,  
PCのメールソフトを介したメールなど

- 配送にはサーバ・クライアントシステムを使用
  - **メールサーバ**を経由した配送

# メールサーバとは

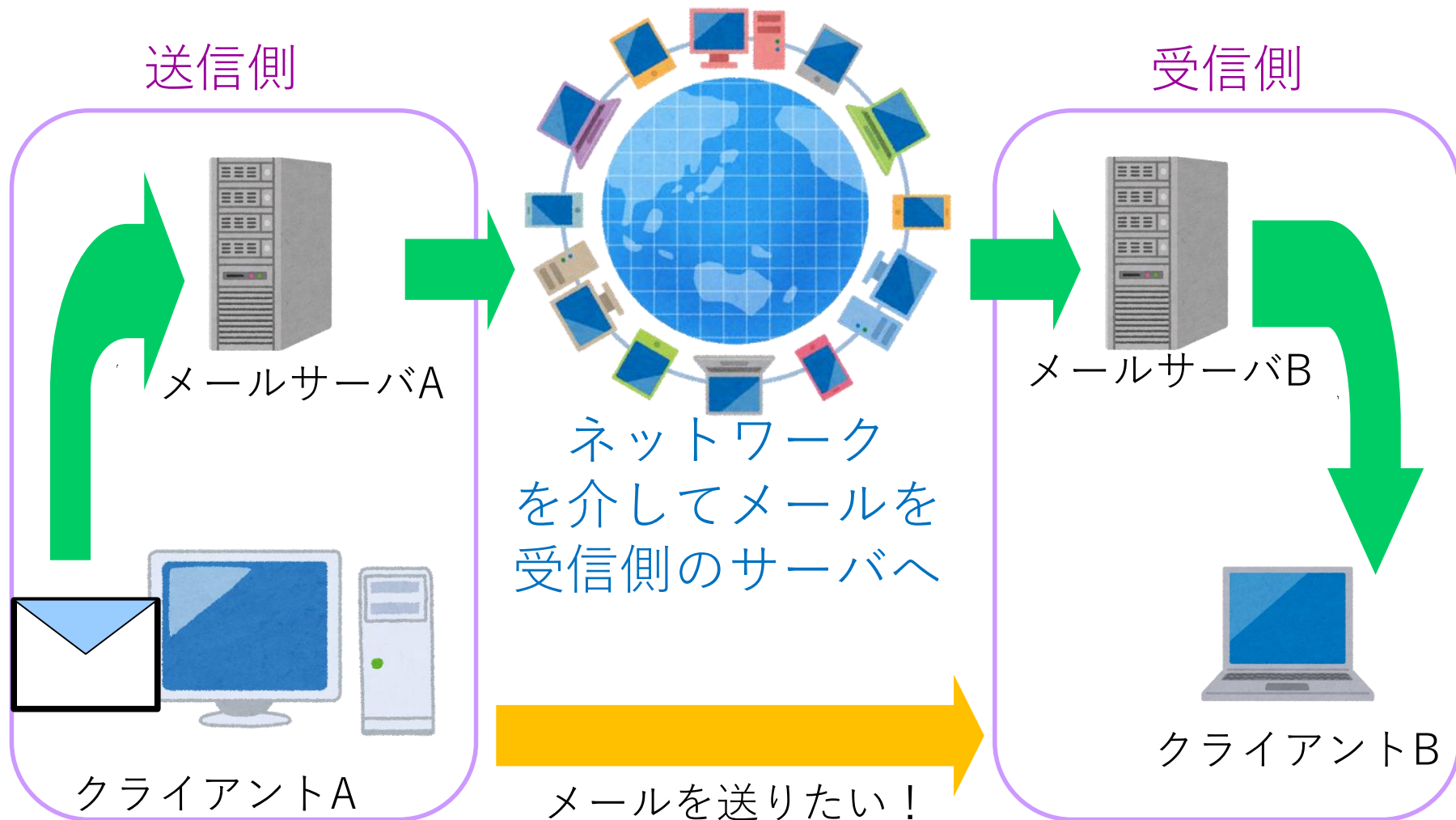
---

メールサーバ

クライアントの要求に応じて、電子メール（以下メール）の送受信サービスを提供するソフトウェア／計算機

- 手元の計算機を常時ネットワークに接続しなくてもメール受け取り可能
  - メールサーバがメールを取り置きする
- 受信する計算機が不在、破損、行方不明になっても郵便受けのようにメールを受け取れる

# メール配送の流れ



# メールアドレス

---

- 配送先を一意的に指定するための文字列(識別子)

hoge@ep.sci.hokudai.ac.jp

ローカル部

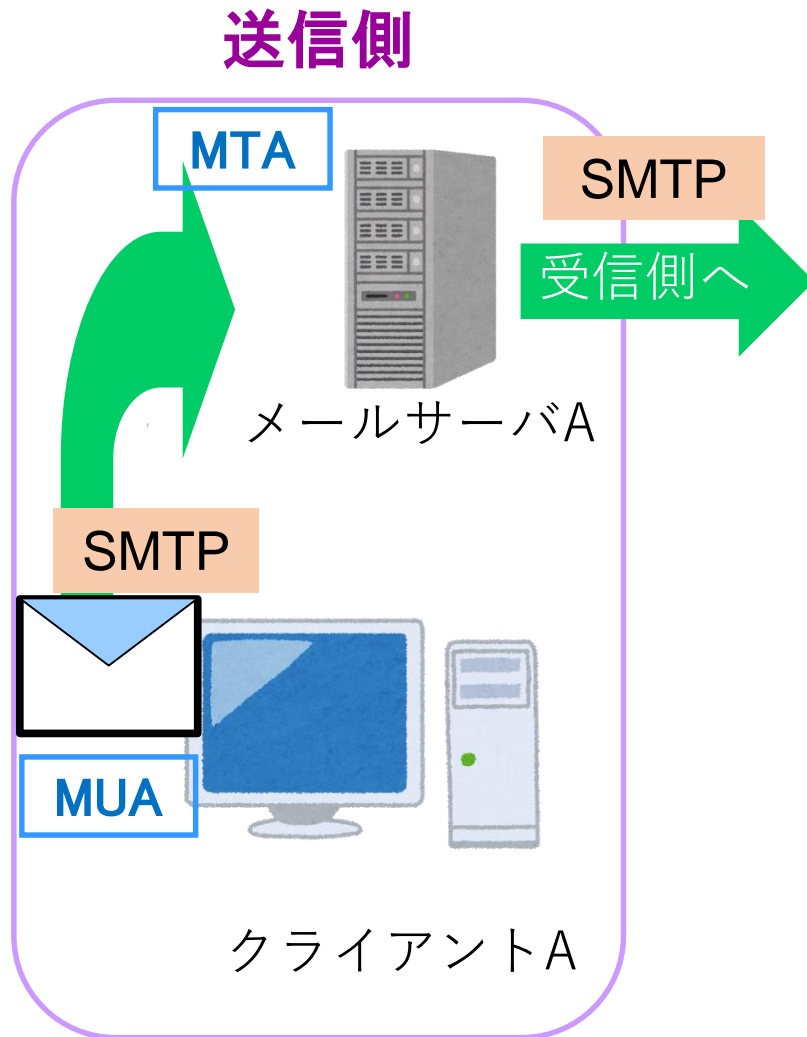
ドメイン部

**ドメイン部** : 配送先のメールサーバを指定

**ローカル部** : メールサーバ上の受取先を指定  
(具体的にはユーザ ID やアカウント名)

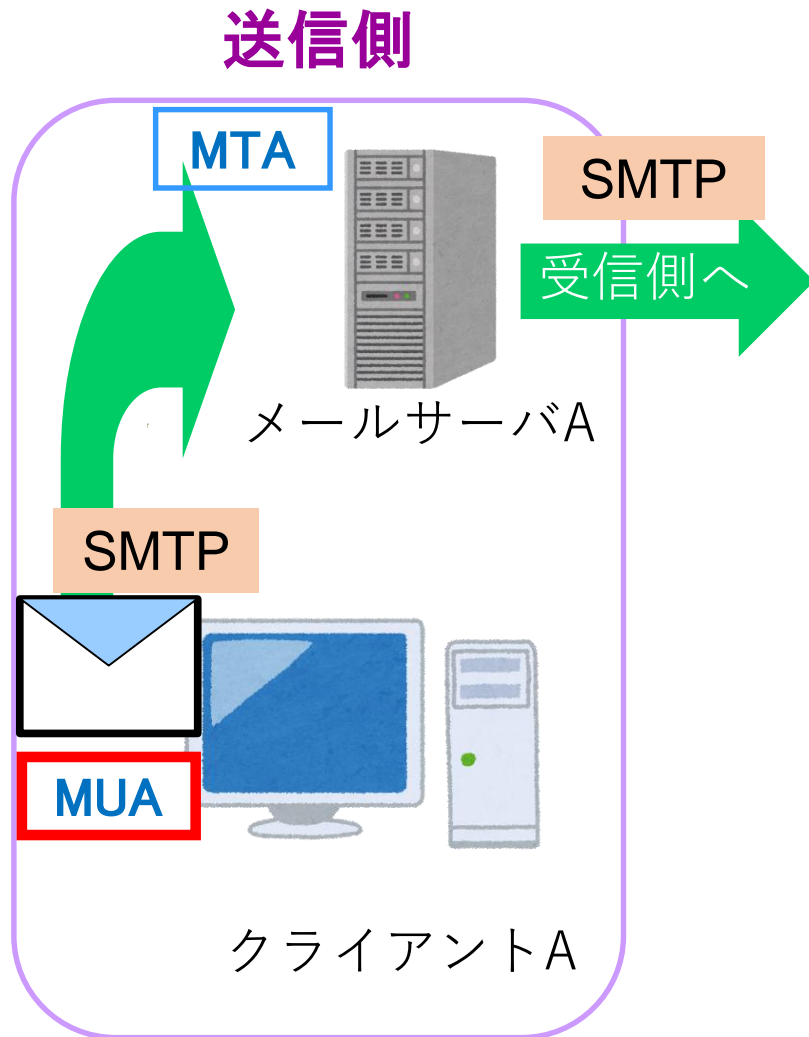


# メール送信



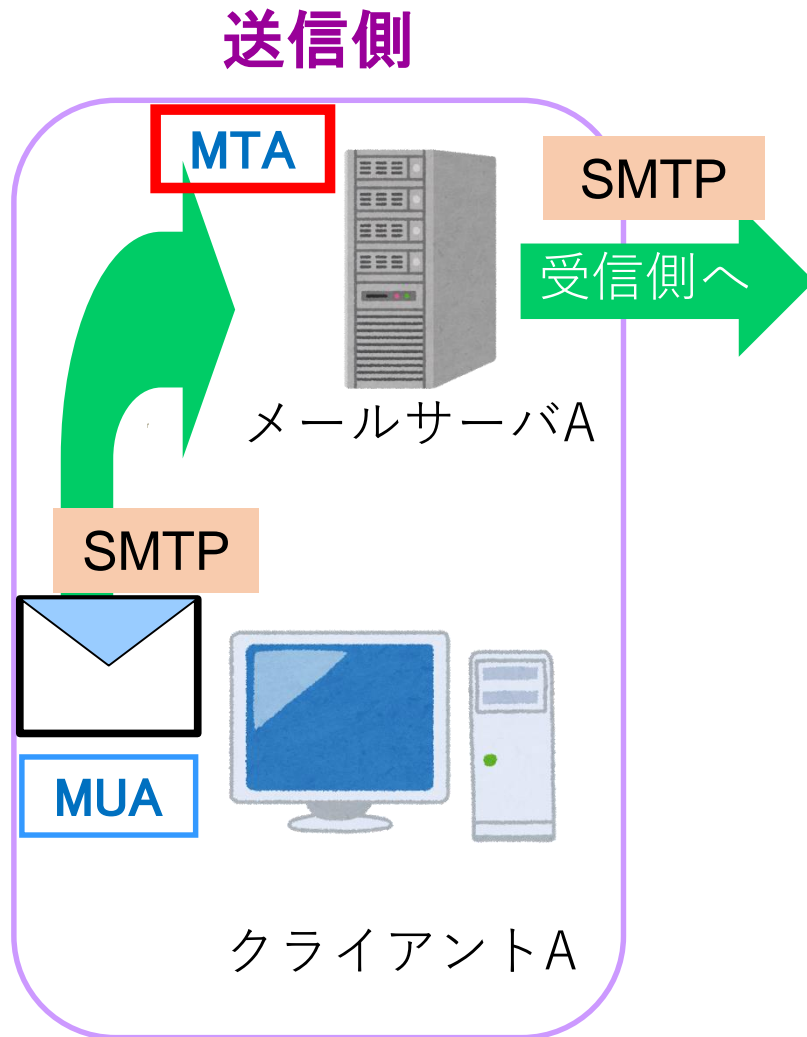
- クライアント(MUA)はメールサーバ宛にメールを送信
- 送信側メールサーバ(MTA)は受信側のメールサーバに送信
- 通信プロトコル
  - SMTP を利用

# MUA: Mail User Agent



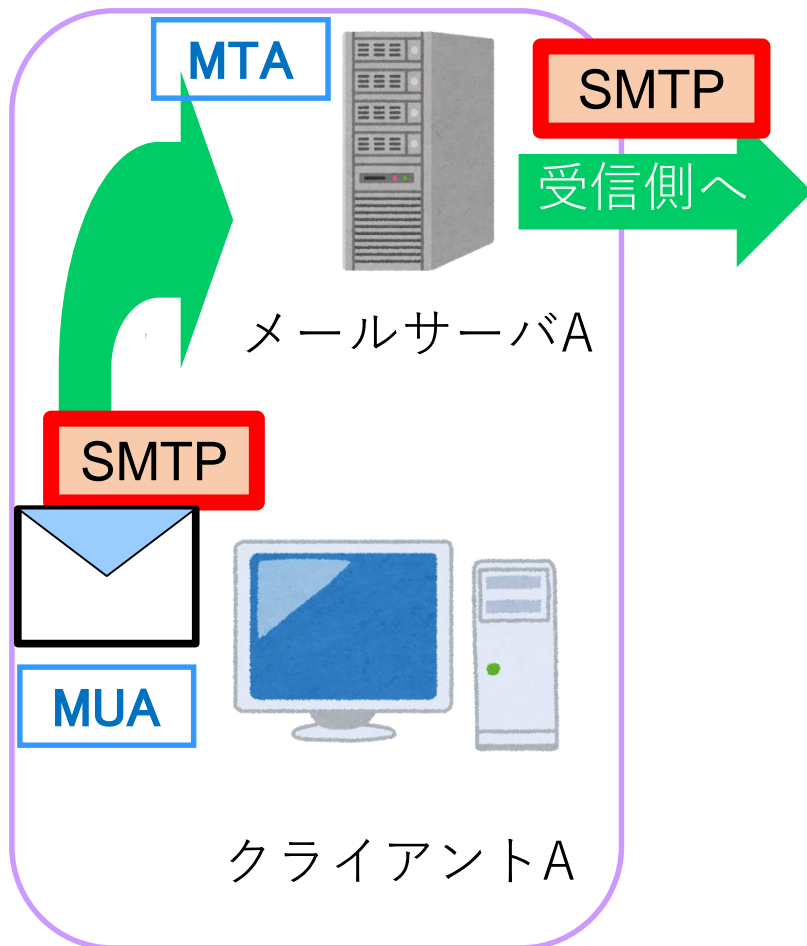
- ユーザがメールを扱うためのソフトウェア
  - 電子メールの読み書き
  - ユーザとメールサーバの仲介
- メールソフト, メールとも呼ばれる
- 例えば,  
Mozilla Thunderbird,  
Windows mail, Mewなど

# MTA: Mail Transfer Agent



- メールを配送・仕分けするソフトウェア
  - 送信側  
MUAから受け取ったメールを受信側のメールサーバまで送信
  - 受信側  
サーバに届いたメールをユーザごとに振り分け
- 例えば, postfix, exim, **qmail**, sendmail など

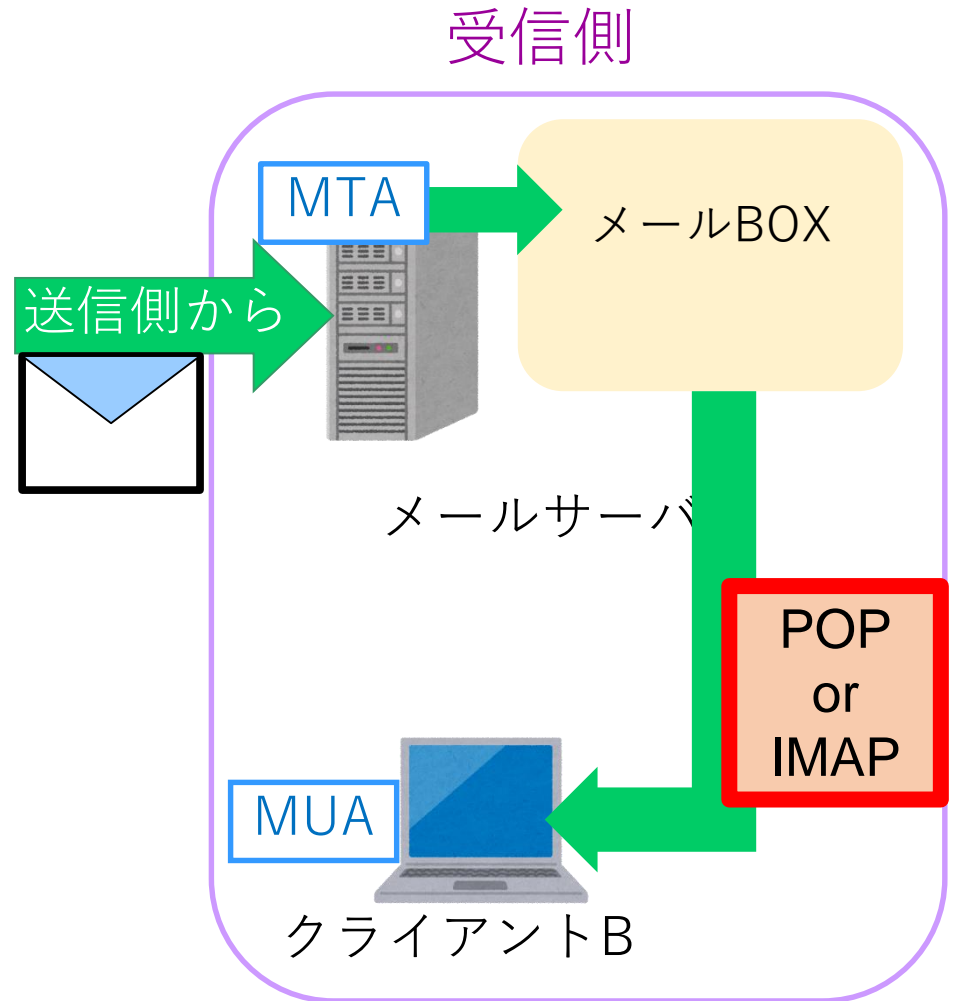
# SMTP: Simple Mail Transfer Protocol



- メール送信や配送時に用いられる通信プロトコル
  - MUA からメールサーバへの送信
  - メールサーバ間の送受信
- デフォルトでは25番ポートを使用  
(設定しだいで変更可能)

# メール受信と取得

- 受信側のメールサーバは受信したメールをユーザ毎に分けてメールBOXに保管
- 受信者はサーバが保管したメールを取得, もしくは閲覧
  - 通信プロトコル: POP, IMAP



# POPとIMAP

## POP

Post Office Protocol

- サーバからメールを**取得**するためのプロトコル
  - サーバの負担軽減可能
  - 複数端末でのメールの管理が難しい
- 110番ポートを使用
- パスワードが平文
  - そのまま使ってはいけない

## IMAP

Internet Message Access Protocol

- サーバへメールを**閲覧**していくためのプロトコル
  - サーバ容量圧迫の可能性
  - 複数端末でのメールを一元管理可能
- 143番ポートを使用
- パスワードを暗号化できる

セキュリティを高めるためにPOP over SSL,  
またはIMAP over SSL の利用を推奨

ただし今はメーラーの設定でPOPでもIMAPでも差がない

# POP/IMAP/SMTP over SSL

---

- SSL/TLSを用いたPOP/IMAP/SMTPプロトコル
  - 通信内容をすべて暗号化する
  - パスワードだけでなくメール本文も暗号化
- POPs/IMAPs/SMTPsとも呼ばれる
- 995/993/465番ポートをそれぞれ使用  
(デフォルト)
- メールとサーバによっては非対応なので注意(EPサーバーは対応しているよ!!)

# webメール

---

- webブラウザでメールを閲覧, 送信するためのメールソフトウェア
  - webアプリケーションを用いてMUAと同等な機能を実装
- ブラウザとサーバの間で, 主にHTTP/HTTPSをプロトコルとして使う。サーバー間ではSMTP通信
- 例えば, Gmail , Yahoo!メール
- 機能面では電子メールと変わらないが、インターネットに接続できるPCや端末があれば利用可能な点で便利



---

# 一年間で茂木がしたことと感想

---

# 茂木がしたこと・すること一覧

---

- 毎週のパッケージ更新 & 報告
- パスワードチェック
- 証明書再発行
- サーバー再構築
- サーバー再起動(パッケージ更新にlinux-imageが入っているときに実施。頻度は3-4か月に一回とか?)

# EPサーバー管理に対する茂木の感想

---

- 作業時はマニュアルどおりにコマンドを打つだけなので、そこまで負担ではない。
- でも正直いってしまうとめんどくさい。
- サーバー管理がちゃんとできるようになるためにはそれなりの時間がある。ノリとテンションで何とかかなりもする。
- サーバー管理ができるようになりたいと思う人にとっては、このサーバー管理プロジェクトはすごくいい環境だと思う。
- 何かしら問題があったときは、教官方や先輩方が助けてくれる。(メールが使えないとみんな困っちゃうからね)
- 責任感の強い人は向いていないと思う。個人的にはあくまで勉強のためという認識でいいと思っています。

---

# EPメールサーバーの歴史と将来

---

# メールサーバーの歴史（石渡正樹談）

---

- いつEPサーバーが作られたんだか分からない。  
(epnetfanのウェブサイトを見てみたら1999年でした。)
- 理学情報システムがまだなかったころ、地球物理学科のメールサーバーとして現在のepmailサーバーが作られる。Epnetfan設立。
- 何年だかわからないけど理学情報システムが作られたことによってepサーバーが学科のメールサーバーとしての役割を失った。

# メールサーバーの歴史

---

- EPサーバーの歴史についてまとめられたドキュメントは今のところなさそう。
- 構築時のメンバーである倉本さんや小高さんに今後詳しいお話を聞いていきたい。
- Epnetfanの写真集を見てみると色々分かりそう。

# なぜ今もepmailサーバーがあるのか

---

- メールングリスト機能などが使えて便利だった(小高談)
- 地球物理学科だった時代(平成五年以前)から現在まで継続利用しているユーザーがいる。(石渡談)
- 現在は学生にサーバーについて学ばせるという教育的な目的がある。(利用者はサービスを受けられる代わりに多少の不便は受容しないといけない。)  
(石渡談)

# サーバー立ち上げ(1999年)

---



<https://www.ep.sci.hokudai.ac.jp/~epnetfan/photo/1999/server/>



# EPメールサーバーの将来について

---

昔は自分たちでメールサーバーを持たないとメールが利用できなかったが、状況は変わってきている。

一度今後の方針について話し合いがあったものの、現在も状況は変わらず。。。(サーバー廃止時にどうするかといった深い内容までは議論されていなかった気がする。)

**EPサーバーの歴史や現在の運営状況などを踏まえたうえで、今一度しっかりと考える機会を設けたらいいじゃないでしょうか??**

茂木個人としては管理に興味のある学生がいたならば管理を担当してもらおう形でのよいのではないのでしょうかと考えます。

---

# メールを 利用する際の注意

---

# メール利用の際の注意・マナー 1

---

- 相手の立場になって読み返す
- 最初に宛名を書き, 次に名乗る
  - 例 倉本さま  
新井です
- 機種依存文字を使わない
  - 半角カタカナ, 「①」, 「TEL」, 「Ⅱ」など
- あまり大きなファイルを添付しない
  - 10 MB 以上のメールは北大外と送受信できない
- HTML 形式のメールに注意
  - 初期設定が HTML 形式のメールがある

燃え盛る炎と凍てつく波、君はどちら...

From: "World of Warships"

2017年4月14日 15:12

# Clash of Elements 始動!

艦長の皆さん!

World of Warships に新たなキャンペーン「Clash of Elements」が幕を開けようとしています!

火の陣営と水の陣営、あなたの好みのチームを選び、特別キャンペーンに挑戦しましょ

返信

全返信

転送

削除

その他

## htmlメールの一例

# メール利用の際の注意・マナー 2

---

- クレジットカード番号, 暗証番号, パスワードなどを送らない
  - 盗聴される恐れがある
- 悪質なメールに注意
  - スпамメール (迷惑メール), 詐欺メール
    - 迂闊に信じない
    - 特にフィッシング詐欺に注意
  - ウイルスメール
    - 添付ファイルを無闇に開かない
    - URL は安易にアクセスしない

# まとめ: メール配送のしくみ

---

- メール配送のしくみ
  1. クライアント (MUA) からメールサーバ (MTA) へメールを送信
    - ...使用プロトコル: SMTP
  2. 送信側のメールサーバ (MTA) から受信側のメールサーバ (MTA) へメールを送信
    - ...使用プロトコル: SMTP
  3. 受信側のメールサーバ (MTA) はメールをメールBOX に仕分け
  4. 受信側のクライアント (MUA) がメールBOX からメールを取得 (見る)
    - ...使用プロトコル: POP, IMAP

# まとめ: メールの構造とセキュリティ

---

- メールの構造
  - メールヘッダ: 宛先, 送信者, 件名, 経路等の情報
  - 空白行: メールヘッダと本文を分ける
  - 本文 (ボディ)
- メールに関するセキュリティ
  - 暗号化・復号: 盗聴を無効化する手段
    - 秘密鍵暗号化方式: 同じ一種の鍵 (秘密鍵) を使用
    - 公開鍵暗号化方式: 対となる異なる二種の鍵 (公開鍵, 秘密鍵) を使用
  - デジタル署名: 偽装, 改ざんを発見する仕組み

# まとめ: メール利用時の注意事項

---

- メールを利用する際の注意・マナー
  - メール送信時の注意
    - 読む人の立場に立って考える
    - 個人情報を送らない
  - メール受信時の注意
    - 悪質なメールに気を付ける  
スパムメール, 詐欺メール, ウイルスメール



# 参考文献(1)

---

- inex2016 講義資料  
<http://www.ep.sci.hokudai.ac.jp/~inex/y2016/0715/lecture/pub/index.html>
- 情報セキュリティ入門 - デジタル署名：ITpro, Nikkei Business Publications, 2016  
<http://itpro.nikkeibp.co.jp/article/COLUMN/20060704/242422/>  
(訪問日: 2016/07/10)
- 古くて新しい、電子メール暗号化対応とその手法 - @IT, ITmedia Inc, 2016  
<http://www.atmarkit.co.jp/fsecurity/rensai/mailsec04/mailsec01.html>  
(訪問日: 2016/07/10)
- メール受信方式は、POPとIMAP、どっちが便利？,まなぶろぐ。| デザインオフィススズキ, 2014 <http://manablog.dosuzuki.com/diary/post-1963/>  
(訪問日: 2016/07/10)

# 参考文献(2)

---

- IMAPとPOPの違いを比較してみた。メリットデメリットは？, ケンズニュース～旬で話題の時事ニュース分かりやすくまとめました！, 2016  
<http://kensnews.net/?p=604>  
(訪問日: 2016/07/10)
- IT用語辞典 e-Words, 株式会社インセプト, 2016,  
<http://e-words.jp/>  
(訪問日: 2016/07/10)
- 一般財団法人日本情報経済社会推進協会 電子署名・認証センター,  
JIPDEC, 2016,  
<http://esac.jipdec.or.jp/index.html>  
(訪問日: 2016/07/10)
- Email\_client, Wikipedia, 2016  
[https://en.wikipedia.org/wiki/Email\\_client](https://en.wikipedia.org/wiki/Email_client)  
(訪問日: 2016/07/10)

# 参考文献(3)

---

- メールの送受信を暗号化するPOP3s/IMAP4s/SMTPs (over SSL) とは - @IT, , ITmedia Inc, 2016  
<http://www.atmarkit.co.jp/fwin2k/win2ktips/973mailovssl/mailovssl.html>  
(訪問日: 2016/07/10)
- OpenSSL日本語サイト: The Open Source toolkit for SSL/TLS, The OpenSSL Project, 1999  
<http://www.infoscience.co.jp/technical/openssl/>  
(訪問日: 2016/07/10)
- ネットワークプログラミングの基礎知識, 68user, 2007,  
<http://esac.jipdec.or.jp/index.html>  
(訪問日: 2016/07/10)

# 参考文献(4)

---

- 共通鍵暗号方式, CapmNetwork, 2015  
<http://capm-network.com/?tag=%E5%85%B1%E9%80%9A%E9%8D%B5%E6%9A%97%E5%8F%B7%E6%96%B9%E5%BC%8F>  
(訪問日: 2016/07/10)
- 3分間 NetWorking, 3 Minutes Networking, 2002,  
(訪問日: 2016/07/10)  
<http://www5e.biglobe.ne.jp/%257eaji/3min/index.html>
- 総務省－インターネット等を利用する方法による選挙運動の解禁等  
(2009)  
(訪問日: 2016/07/10)  
[http://www.soumu.go.jp/senkyo/senkyo\\_s/naruhodo/naruhodo10\\_2.html](http://www.soumu.go.jp/senkyo/senkyo_s/naruhodo/naruhodo10_2.html)