情報リテラシ 第一

2023年度1Q 5c/6c（IL1） 木曜日

担当: 地引

TA: 増井

テーマ 2 の講義内容

- E-mail の仕組み
- メール クライアントの設定
  - メール サーバ上で読み書きの処理をする場合
  - PC/スマホ上で読み書きの処理をする場合
- E-mail のセキュリティ

E-mail はオンライン コミュニケーションの基本であり、
分量が多いので、不足分は来週に行ないます。

E-mail の仕組み

E-mail とは

- 葉書郵便と仕組みは似ているが、下記の相違がある。
  - 信頼性は保証しない（書留などはない）
  - 秘匿性は保証しない（別の枠組み/法律で守っている）
- 好きな時に好きな場所から送れる
- 好きな時に好きな場所で受け取れる
- ただし、インターネットに接続していないとダメ

葉書との対比（1）

- 宛名／住所　→　ユーザ名@ドメイン名
- 郵便ポスト　→　メール サーバ（発送郵便局でもある）
- 中継郵便局（ここは、ユーザからは見えない）
- 受取郵便局　→　メール サーバ
- 投函／受取　→　メール コマンドの実行

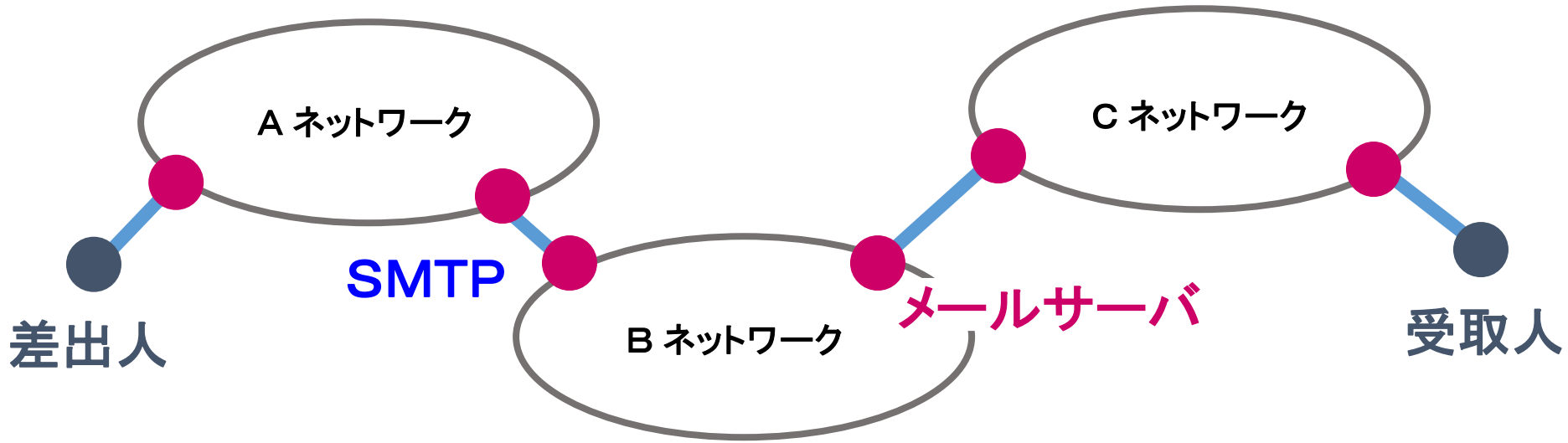
（葉書/E-mail の対応関係の詳細）

葉書との対比（2）

- 配達時間：E-mail は基本的に数秒以内
- 配達範囲：E-mail は情報端末とインターネットがあれば、どこでも受け取れる。
- 受取人数：E-mail は何人でも OK
- **秘匿性：　葉書/E-mail 共に法律で守っている**
- **信頼性：　E-mail は保証なし（サーバが溢れたら廃棄）**
- 課金：　E-mail は管理者による

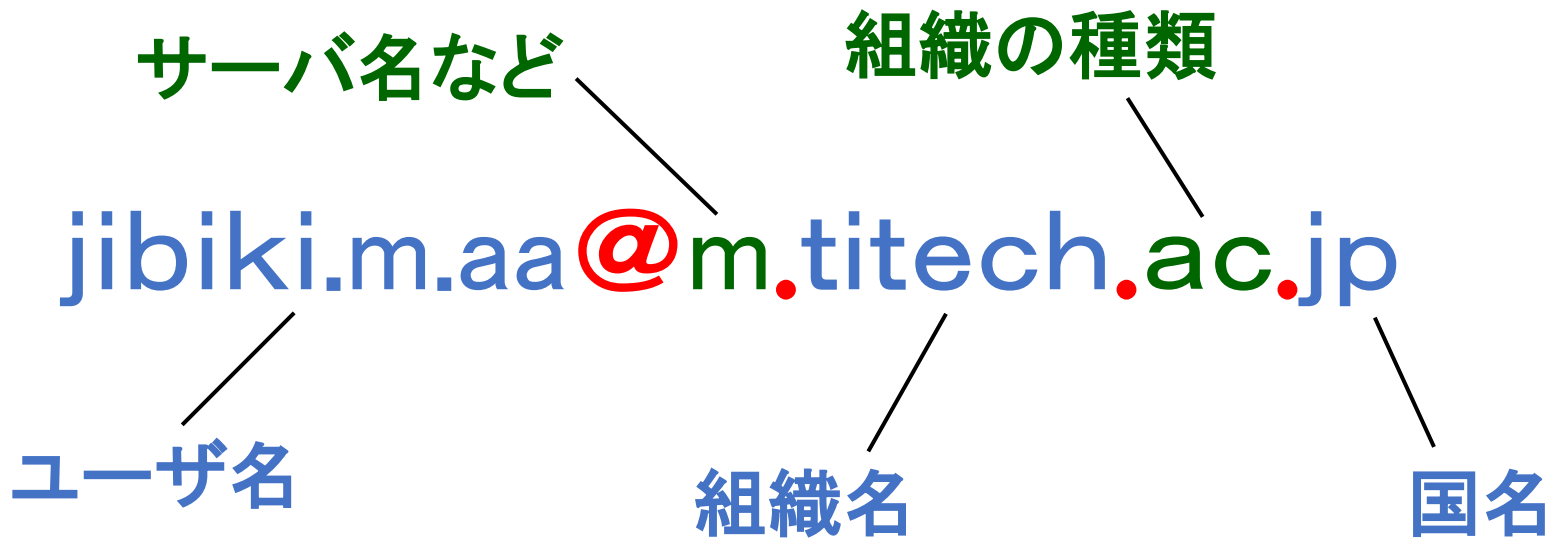
E-mail 配送の仕組み

- ネットワーク同士をバケツリレー
- 通信規約（プロトコル）→　SMTP
- 基本はインターネットなので様々なデータを送受信可能
- （当然）独立した各組織の個別管理



メール アドレスの構造

URL（ホームページのアドレス）と似ている（ドメイン名の部分）



組織：go，ac，co，ne，or / gov，edu，com，org ほか

⇒ 但し、ビジネス上/運用管理上の理由から、
上のルールに当てはまらないドメイン構造も存在する。

E-mail の書式

よく使うメールヘッダ

メールの先頭には、(通常は見せないが)
配送処理用に以下の文字列が付けられる。

To: 宛先

Cc: コピーメールの配布先

Subject: 表題

From: 送信者

Mime-Version: MIME仕様の表示(メーラが自動的に書き込む)
文字以外のデータを添付

Content-Type: メールの中身が何であるかを指定
中身に応じて、最適なアプリを自動的に起動(ウィルス蔓延の元凶)

Reply-To: 返信先の自動設定(返信先は必ず確認しよう)

**通常は、メールソフトが便宜のため自動的に編集するが、
基本的にメール作成者は自由に編集できる。**

メール サーバ上で読み書きの処理を行なう

（このようなサービスを Web メールと呼びます）

Tokyo Tech Portal の
メニューから、呼び出します。

Web メール（1）

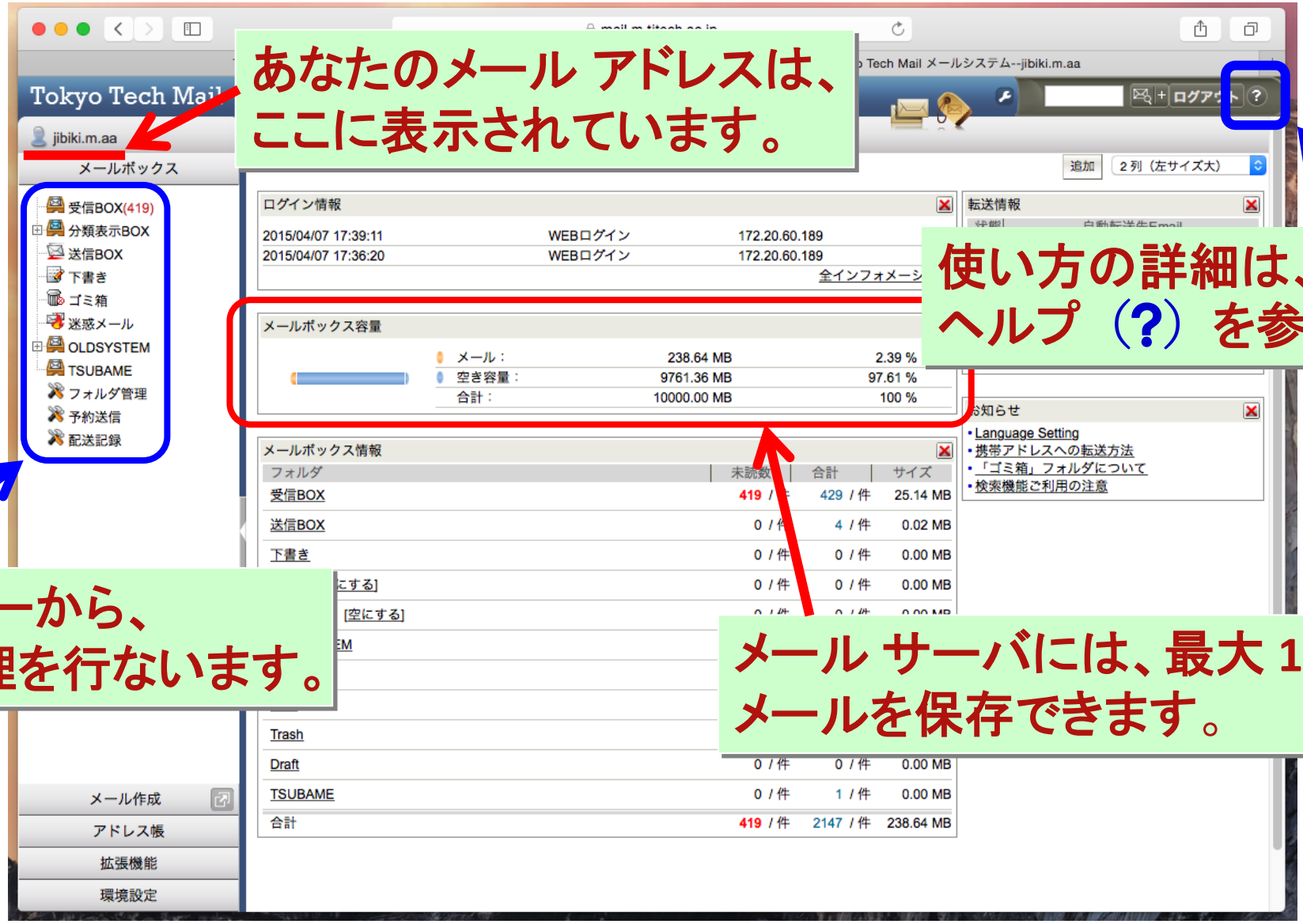
- ホーム ページ上に、メール処理用のメニューを構築
  - このような**処理用のメニュー**を**インターフェイス**と呼びます。

- Web ブラウザを用いて、メールの読み書きを実行

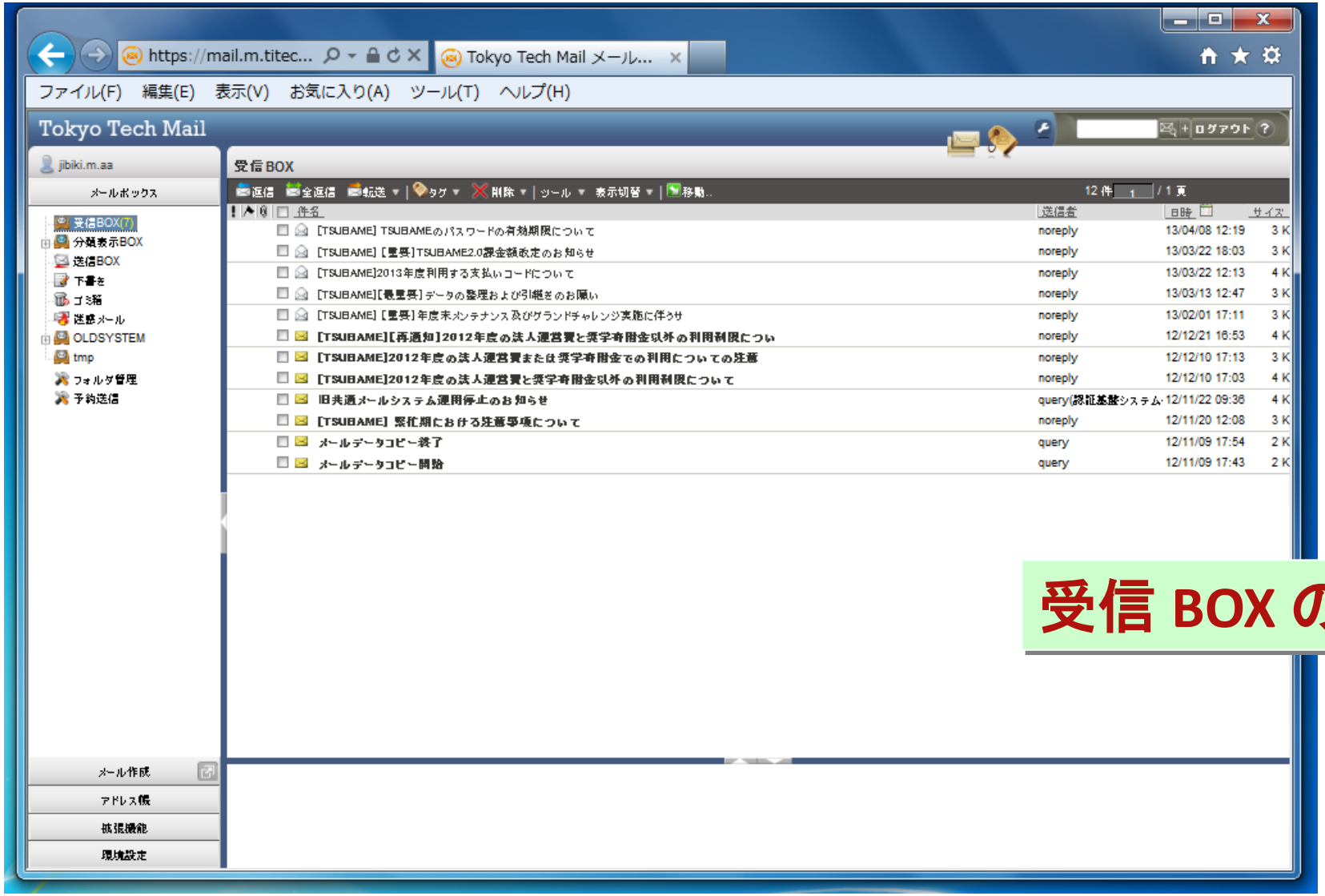
- **メールそのものは、メール サーバが管理**
  - 東工大では Tokyo Tech Portal がメールを管理
  - メール本体は、Tokyo Tech Portal に保存されている。

- **ホーム ページ上でメールを処理できることから、様々な情報端末上でメールを読み書きできる。**

Web メール（2）


あなたのメール アドレスは、
ここに表示されています。
使い方の詳細は、ここにある
ヘルプ（?）を参照しましょう。
ここのメニューから、
メールの処理を行ないます。
メール サーバには、最大 10 GBの
メールを保存できます。
Tokyo Tech Mail
jibiki.m.aa
メールボックス
受信BOX(419)
分類表示BOX
送信BOX
下書き
ゴミ箱
迷惑メール
OLDSYSTEM
TSUBAME
フォルダ管理
予約送信
配送記録
ログイン情報
2015/04/07 17:39:11 WEBログイン 172.20.60.189
2015/04/07 17:36:20 WEBログイン 172.20.60.189
メールボックス容量
メール： 238.64 MB 2.39 %
空き容量： 9761.36 MB 97.61 %
合計： 10000.00 MB 100 %
メールボックス情報
フォルダ 未読数 合計 サイズ
受信BOX 419 / 429 / 件 25.14 MB
送信BOX 0 / 4 / 件 0.02 MB
下書き 0 / 0 / 件 0.00 MB
Trash
Draft 0 / 0 / 件 0.00 MB
TSUBAME 0 / 1 / 件 0.00 MB
合計 419 / 2147 / 件 238.64 MB
転送情報
お知らせ
Language Setting
携帯アドレスへの転送方法
「ゴミ箱」フォルダについて
検索機能ご利用の注意
メール作成
アドレス帳
拡張機能
環境設定

Web メール（3）



受信 BOX のイメージ

PC/スマホ上で読み書きの処理を行なう

メールの読み書き処理は、どこで行なうべきか

- Web メールは手軽で便利だけど、**Tokyo Tech Portal に負担を掛ける。**
  - Tokyo Tech Portal は、メールサービスの提供だけではない。
- 教育システム（演習室内の PC）からメールを読み書きする場合は、教育システムに用意された機能を利用する方が望ましい。
  - 但し、Web メールでは自動的に対応してくれた部分を、ある程度、自分で対応する必要がある。

もう少し正確に言うと、ユーザが自由に使える計算能力の高い情報端末（教育システム or 個人所有の PC 等）があれば、そちらを利用する方が望ましい。

E-mail の送信/受信に必要なもの

- 宛名／住所　→　ユーザ名@ドメイン名
  - 東工大のメール アドレスが該当
- 郵便ポスト　→　メール サーバ（発送郵便局でもある）
- 中継郵便局（ここは、ユーザからは見えない）
- 受取郵便局　→　メール サーバ
- 投函／受取　→　メール コマンドの実行

メール用アプリから見て、
これらは明確ではないので
（要は、どこにあるか不明）、
個別に設定が必要となる。

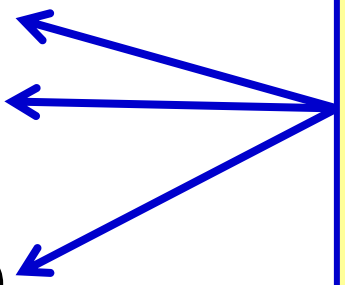
これらは、プロトコルで決まっているため、
メール用アプリ（例えば、これから説明する Thunderbird）が自動的に対処してくれる。

メール サーバの設定に必要なもの

- メール サーバの名前 or アドレス
  - 受信用と送信用の 2 種類がある。
- メール サーバとの通信方式
  - こちらも受信用と送信用を分けて設定する。
  - **通信方式**のことを**プロトコル**と呼びます。
  - メールの受信/送信プロトコルとは、例えば、次のような情報を交換する手順などです。
    - ≫ E-mail の書式に従ったメールの受信/送信の要求
    - ≫ メールの受信/送信中に、ネットワークが途切れた場合の再開方法
    - ≫ サーバに届いているメール数の確認
    - ≫ サーバにメールを残しておく期間の設定，その他
- 一般に、通信を用いたサービス毎にプロトコルが存在します。

【重要】東工大のメール環境

- 認証に必要な情報（似た設定が複数あるので混乱しないように）
  - 名前：受信者に表示する自分の名前
  - **ユーザ名：共通メール認証 ID（Tokyo Tech Portal より取得）**
  - メール アドレス：「**** . * . ** @ m . titech . ac . jp」
  - パスワード：Tokyo Tech Portal のパスワード
- メール サーバ名（送信と受信で異なるので注意）
  - 受信：「mailv3 . m . titech . ac . jp」
  - 送信：「smtpv3 . m . titech . ac . jp」
- 受信プロトコル（どちらでもよい）
  - POP3 + SSL/TLS (995)
  - IMAP + SSL/TLS (993)
- 送信プロトコル
  - SMTP + SSL/TLS (465)

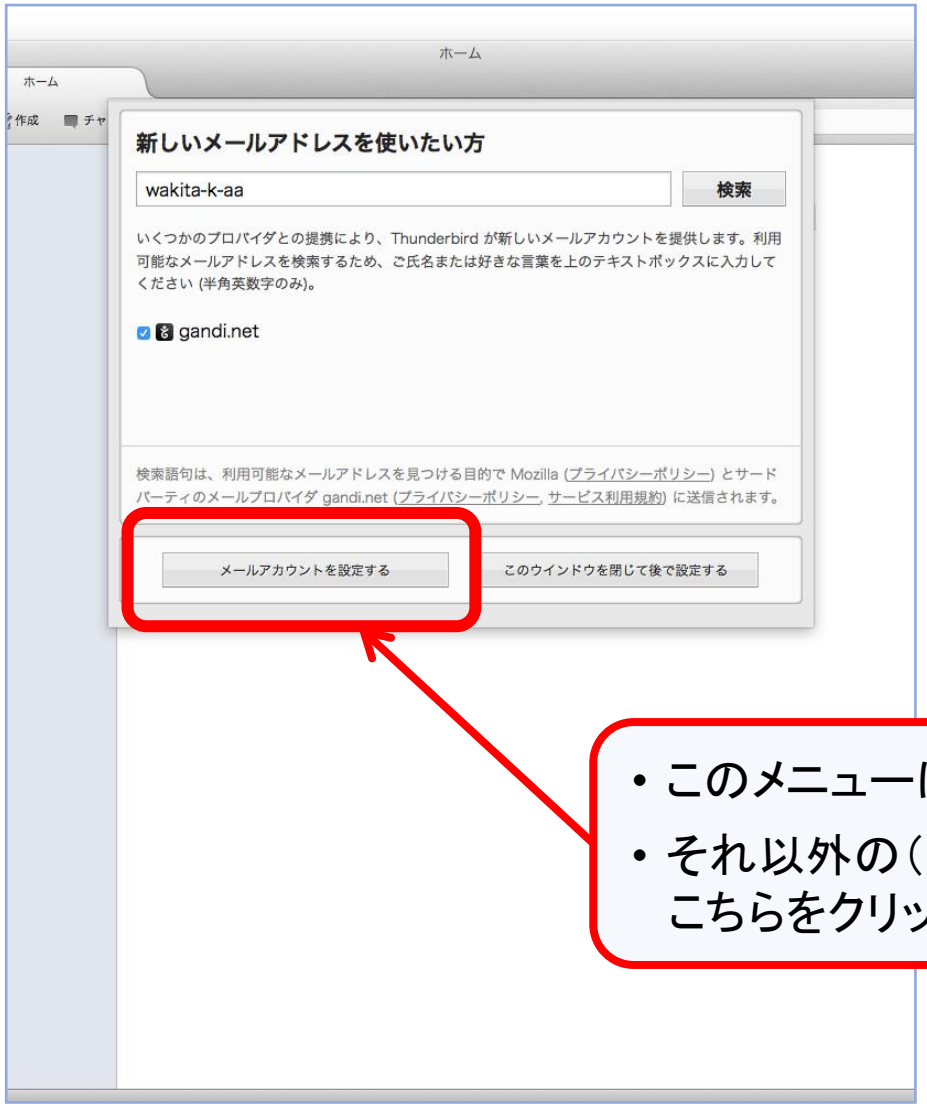


- 一般に、一つのサーバ上で、
  複数のサービスを提供することがあります。
- 例えば、Tokyo Tech Portal では、
  メール以外のサービスも提供しています。
- **サーバに対して、どのサービスを要求するかは、
  番号（ポート番号）で表します。**

共通メール認証 ID

- サーバにログインをする場合、ユーザ ID（ログイン名/アカウント名）とパスワードを入力する。
  - サーバは、サービス要求者をユーザ ID で識別する。
- メール サーバであれば、ユーザ ID として一般的にメール アドレスを使う。
  - 複数のメール アドレスを提供するメール サーバでは、各メール アドレスの @ より前の部分をメール アカウント名として管理する場合がある。
- 但し、**メール アドレスは様々な場面で公開されるため、秘匿性が低い。**
  - 最近のセキュリティ事情では、ユーザ ID（東工大で言えば学籍番号）も秘匿の対象
- **東工大では、メール サーバのユーザ ID として、共通メール認証 IDを用意**
  - **Tokyo Tech Portal より共通メール認証 ID を作り直した場合は、Thunderbird の設定も修正する必要がある。→ 忘れ易いので要注意**

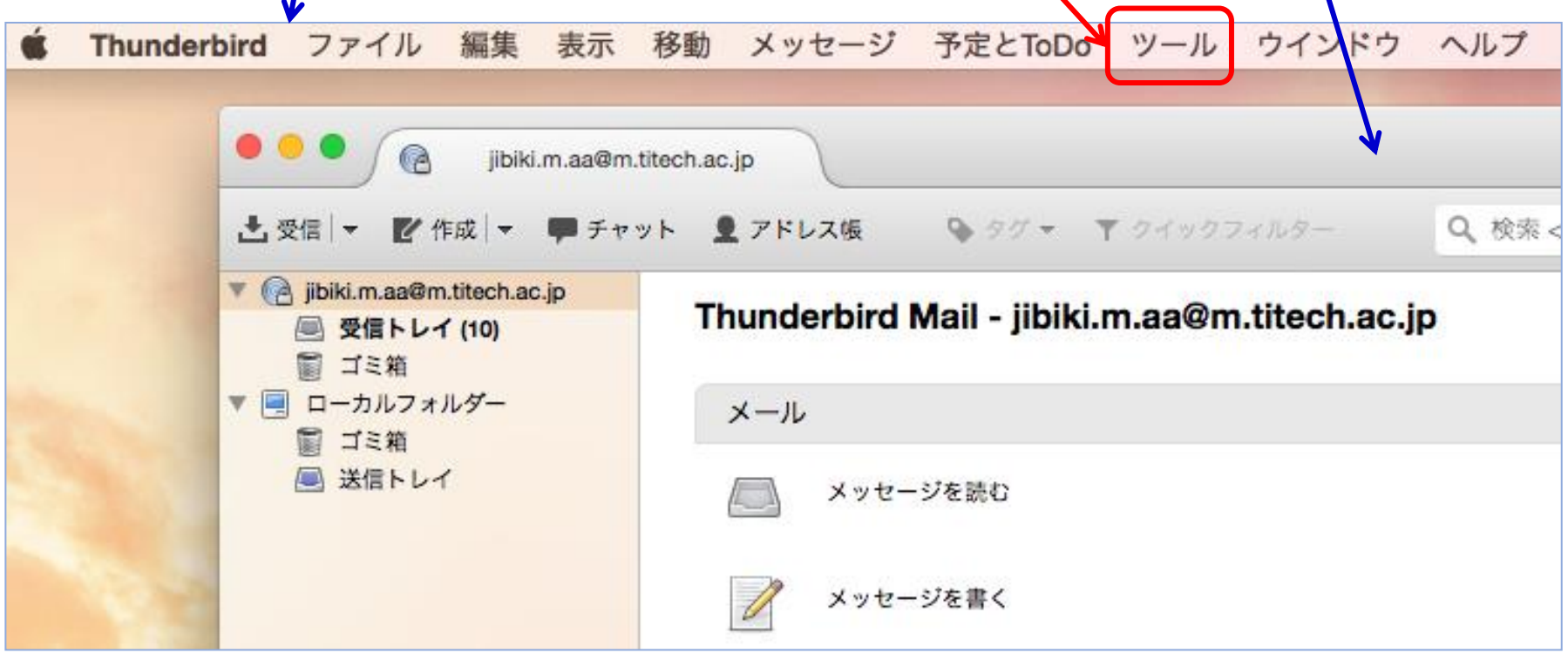
Thunderbird の設定（補足1）



- このメニューは、参考として gandi.net を利用する例
- それ以外の（当然、東工大も含む）メール設定は、こちらをクリックする。

Thunderbird の設定（補足2）

- Mac 上のアプリは、メニューが**アプリ ウィンドウの上端**ではなく、**画面全体の上端**に表示されます。
- アカウントに関する設定は、この **“ツール” メニュー**以下にあります。



E-mail の整理

- 多くのメールをやり取りするうちに、読み終えたメールが溜まってきます。
  - 既読のメールを全て廃棄できればよいのですが、保存しておいた方がよいメールもあります。
  - ただ溜めておくだけでは、保存してあるメールから必要な情報を得られません。

- メールは、**グループ分けして保存**しておきます。
  - 分野毎にグループ分けして保存する方法は、メールの保存だけではありません**（あらゆる情報整理の基本です）。**
  - グループの分け方に規則はありません**（腕の見せ所です）。**

E-mail のセキュリティ

電子メールを取り巻く危険

- 不正アクセス
  - メールアカウント情報（アカウント名/パスワード）の流出
  - 秘匿情報は、しっかり守りましょう !!
- 通信の盗聴
  - 通信路の途中に盗聴装置を挟む ⇒ 気付かれない。
  - メール本文/添付ファイルを**暗号化**して送るのがベスト
- メッセージの改竄
  - 転送中のメールを、途中でこっそり書き換える。
  - 暗号化して送ってあれば、書き換えも困難
    （書き換えるには、暗号文を平文に戻す必要がある）
- **メール サーバの詐称**
  - **偽物のサーバを使って、重要な情報を詐取**

この後、出て来る。
覚えておこう。

（対策）メール サーバの詐称

サーバの真贋を見極める技術：

⇒ SSL（Secure Socket Layer）を利用（通信路の暗号化）

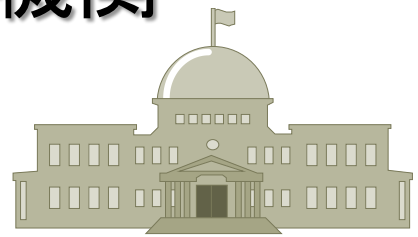
- サーバが、世界的に信頼されている認証組織から、正規のサーバであることを証明してもらう（**証明書の発行**）
- 正統である証を他に見せる場合、暗号化された通信路を使用
  - **秘密鍵 + 公開鍵**（アルゴリズムの詳細は、セキュリティの回で説明します）
- **この暗号通信を利用できる者 & 正統性を示す証明書**

  ⇒ 確かに正規のサーバだ！

東工大では、一般的なメールの受信/送信用プロトコルに、SSL を追加したプロトコルを用いています。

SSL によるサーバー認証のイメージ（1）

認証機関



正当な公開鍵
(*1：次スライド参照)

ユーザ

○：正当な公開鍵で開ける
×：同、開けない

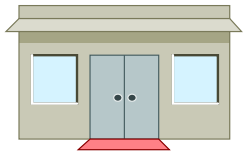
○

×

正当な公開鍵

正当な秘密鍵で暗号化された
認証用データ(ドメイン名)

偽の秘密鍵で暗号化された
認証用データ(ドメイン名)



正当な事業者

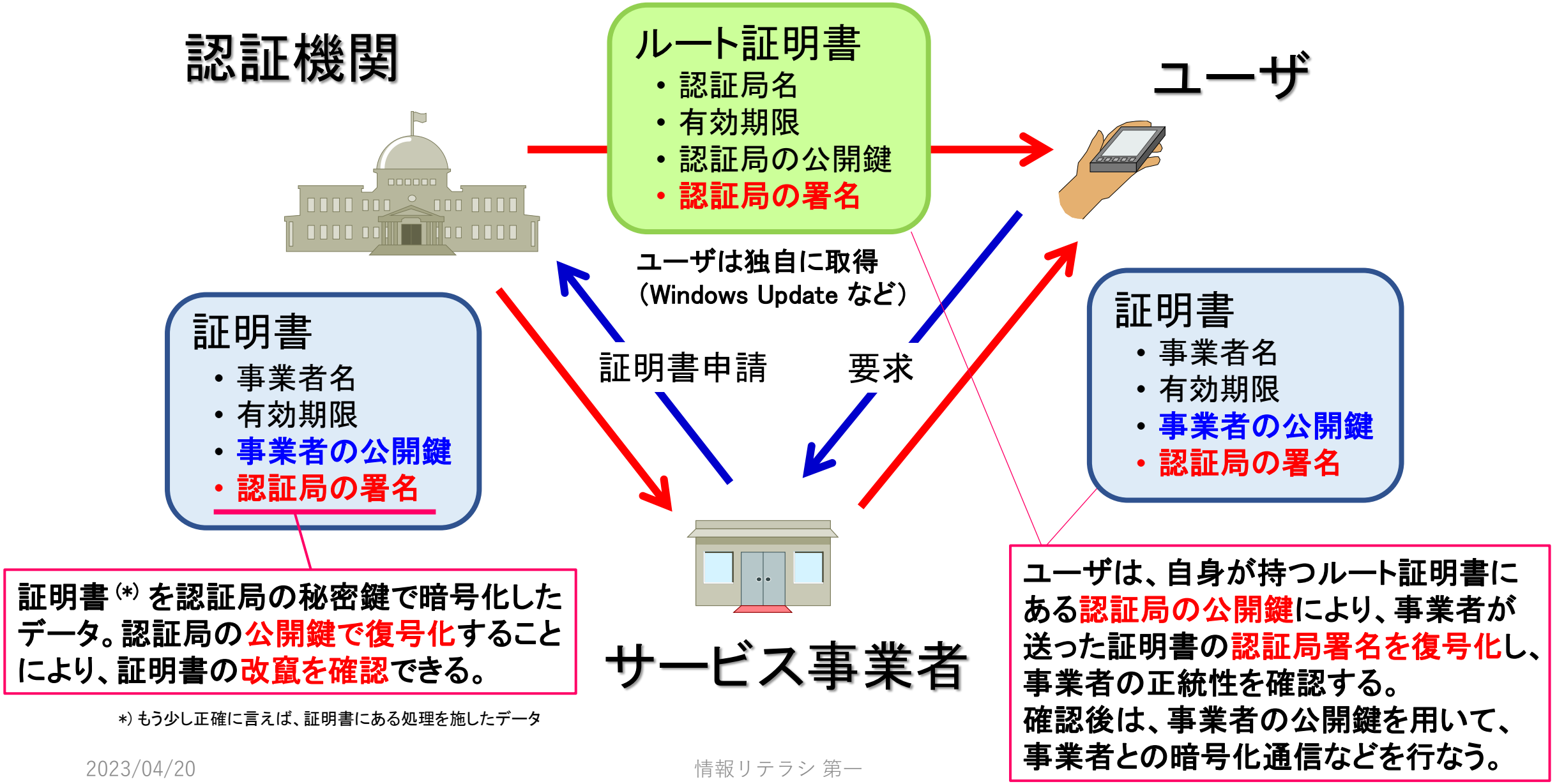
悪意のある
第三者

SSL によるサーバー認証のイメージ（2）

- 事業者の公開鍵を認証局が保証（前スライド *1）
  - ミソ：事業者の公開鍵を認証局の秘密鍵で暗号化 → これが証明書
    事業者の公開鍵は認証局の公開鍵でのみ復号可能 → 認証局が保証
  - 前スライドでは、（簡略化のため）“認証局 → ユーザ” としているが、
    実際は、“認証局 → 事業者 → ユーザ” の経路で渡される。

- 第三者が事業者の証明書を盗んだとしても、
  第三者は事業者の秘密鍵を持っていないので、意味がない。
  - 例えば、第三者が偽の秘密鍵で暗号化したメッセージは、
    ユーザが証明書経由で取得した事業者の公開鍵で復号化できない。

参考：SSL によるサーバー認証の詳細



*) もう少し正確に言えば、証明書にある処理を施したデータ

とは言え、過信は禁物

- 但し、SSL で完全に守られているわけではありません。
- 偽サーバと偽ユーザがグルになった場合は、排除が難しい。
  - メールはバケツ リレー形式で転送されますが、世界にはサーバ間で偽物を排除していない NW 事業者もあり（これを事業者 F と呼ぶことにしましょう）、リレーのどこかで偽物が紛れ込んでしまいます。。
  - 他の NW 事業者は F を排除したいのですが、F には正当なサーバ/顧客も存在するため、これを一概に全て排除するのは難しい面があります。
  - 極端な例として、例えば Amazon がコストの観点から F を利用しているからと言って（悪さはしてない）、Amazon との接続を断つことは現実的ではありません。
  - 現状では、F 内の怪しいサーバを一つ一つ遮断して行くという状況です。

厄介な偽装メール（1）

From: Amazon <account-update@amazon.com>
To: .....
Date: Tue, 16 Jun 2020 16:23:30 +0900
Subject: Amazonセキュリティ警告

Amazon お客様: .....

Amazon に登録いただいたお客様に、Amazon アカウントの情報更新をお届けします。
残念ながら、Amazon のアカウントを更新できませんでした。

アカウント情報の一部が誤っている故に、お客様のアカウントを維持するため Amazon アカウントの 情報を確認する必要があります。下からアカウントをログインし、情報を更新してください。
Amazon ログイン

なお、24時間以内にご確認がない場合、誠に申し訳ございません、お客様の安全の為、アカウントの利用制限をさせていただきますので、予めご了承ください。

Amazonカスタマーサービス

メール アドレスを見る限り（@amazon.com）、
本物の Amazon から届いているように見える。

厄介な偽装メール（1の続き）

Received: from bvea650705 ([192.168.154.11])
by bvea650725 with LMTP id +JtmGXpz6F4+Z
; Tue, 16 Jun 2020 16:23:38 +0900
Received: from biglobe.ne.jp ([192.168.154.11])
by bvea650705 with LMTP id iP09GXpz6F6pWg
; Tue, 16 Jun 2020 16:23:38 +0900
Received: from rcpt-impgw.biglobe.ne.jp **by** biglobe.n
id QAA30245; Tue, 16 Jun 2020 16:23:38 +0900 (JST)
..... (認証情報等は省略)
Received: from **sa12.dkjahsdkjahsdk09.xyz (sa12.asdacxzxcz09.xyz [107.179.123.140] (may beforged))**
by **rcpt-impgw.biglobe.ne.jp** (hngd/5416110419) with ESMTP id 05G7NZi0030121
; Tue, 16 Jun 2020 16:23:37 +0900
..... (認証情報等は省略)
Received: by sa2.dkjahsdkjahsdk09.xyz id
(envelope-from <service07@sa2.dkjahsdk

転送メールを、どのメール サーバが、
どのメール サーバより受け取ったかの記録。
上に行くほど、受信者に近いサーバの情報
(下ほど送信者に近い → 怪しさ up ?)。

送信メール サーバに付いている括弧書きは、
受信サーバが調べた送信サーバの情報。
送信サーバが自称する情報と括弧書きとに違いある場合は、
何らかの目的のために詐称されている可能性が高い。

.xyz は、個人でブログ運営をする場合など、利用者数が非常に多いドメイン。
BIGLOBE (日本の大手プロバイダ) も、明確に問題が発覚するようになれば
sa12.…xyz (107.179.123.140) からの接続を受け付けないが、
顧客の利便に配慮しつつ詐称サーバにきめ細かく対応することは難しい。

さらに手の込んだ例

厄介な偽装メール（2）

From: DCカード <info@cr.mufg.jp>
Subject:【重要なお知らせ】【三菱UFJ ニコス　Net Branch】ご利用確認のお願い

いつも弊社カードをご利用いただきありがとうございます。

メール アドレスを見る限り（@cr.mufg.jp）、
本物の“三菱UFJニコス”から届いているように見える。

昨今の第三者不正利用の急増に伴い、弊社では「不正利用監視システム」を導入し、24時間365日体制でカードのご利用に対するモニタリングを行っております。

このたび、ご本人様のご利用かどうかを確認させていただきたいお取引がありましたので、誠に勝手ながら、カードのご利用を一部制限させていただき、ご連絡させていただきました。

つきましては、以下へアクセスの上、カードのご利用確認にご協力をお願い致します。
ご回答をいただけない場合、カードのご利用制限が継続されることもございますので、予めご了承下さい。

■ご利用確認はこちら

HTML 形式のメールとして送付され、
クリックを促すリンクが張り付けられている。

■発行者■
三菱ＵＦＪニコス銀行
※本メールは送信専用です。
※本メールは「**Net Branch**」にメールアドレスをご登録いただいた方にお送りしています。

厄介な偽装メール（2の続き）

```
Return-Path: <khphxiir@cr.mufg.jp>
Received: from bvea650707 ([192.168.154.54])
        by bvea652482 with LMTP id WDQaNlXQiGD1GAAAMmdaJg
        ; Wed, 28 Apr 2021 12:02:45 +0900
Received: from biglobe.ne.jp ([192.168.154.54])
        by bvea650707 with LMTP id 6AHgNVXQiGD+GwAAxRyf7Q
        ; Wed, 28 Apr 2021 12:02:45 +0900
Received: from rcpt-impgw.biglobe.ne.jp by biglobe.ne.jp (
        id MAA03626; Wed, 28 Apr 2021 12:02:45 +0900 (JST)
Received: from imta0015.biglobe.ne.jp (snd00002-bg.im.kddi.ne.jp [27.86.113.2])
        by rcpt-impgw.biglobe.ne.jp (hngd/4910241220) with ESMTP id 13S32jk2003577
        ; Wed, 28 Apr 2021 12:02:45 +0900
Received: from cr.mufg.jp by imta0015.biglobe.ne.jp with ESMTP
      id <20210428030244165.XRIF.93007.cr.mufg.jp@biglobe.ne.jp>
      ; Wed, 28 Apr 2021 12:02:44 +0900
```

biglobe のメール サーバが受け取った際、
送信メール サーバに括弧書きが付いていないので、
送信サーバは詐称されていないように見える。

厄介な偽装メール（2の続き）

Authentication-Results:
- 受信メール サーバが、送信メール サーバの身元を調査した結果、“Received: from …” に記録できるほどの確定情報がない場合、身元の怪しさをスコア形式で表示する。
- DNS や公開鍵暗号による電子署名**など**を用いて調査する。調査方法に応じて SPF/DKIM/DMARK といった種類がある。
- 先ほどのメールでは、SPF のスコアは怪しい（fail）と記録されている。

Authentication-Results: rcpt-imp.biglobe.ne.jp; **spf=fail**

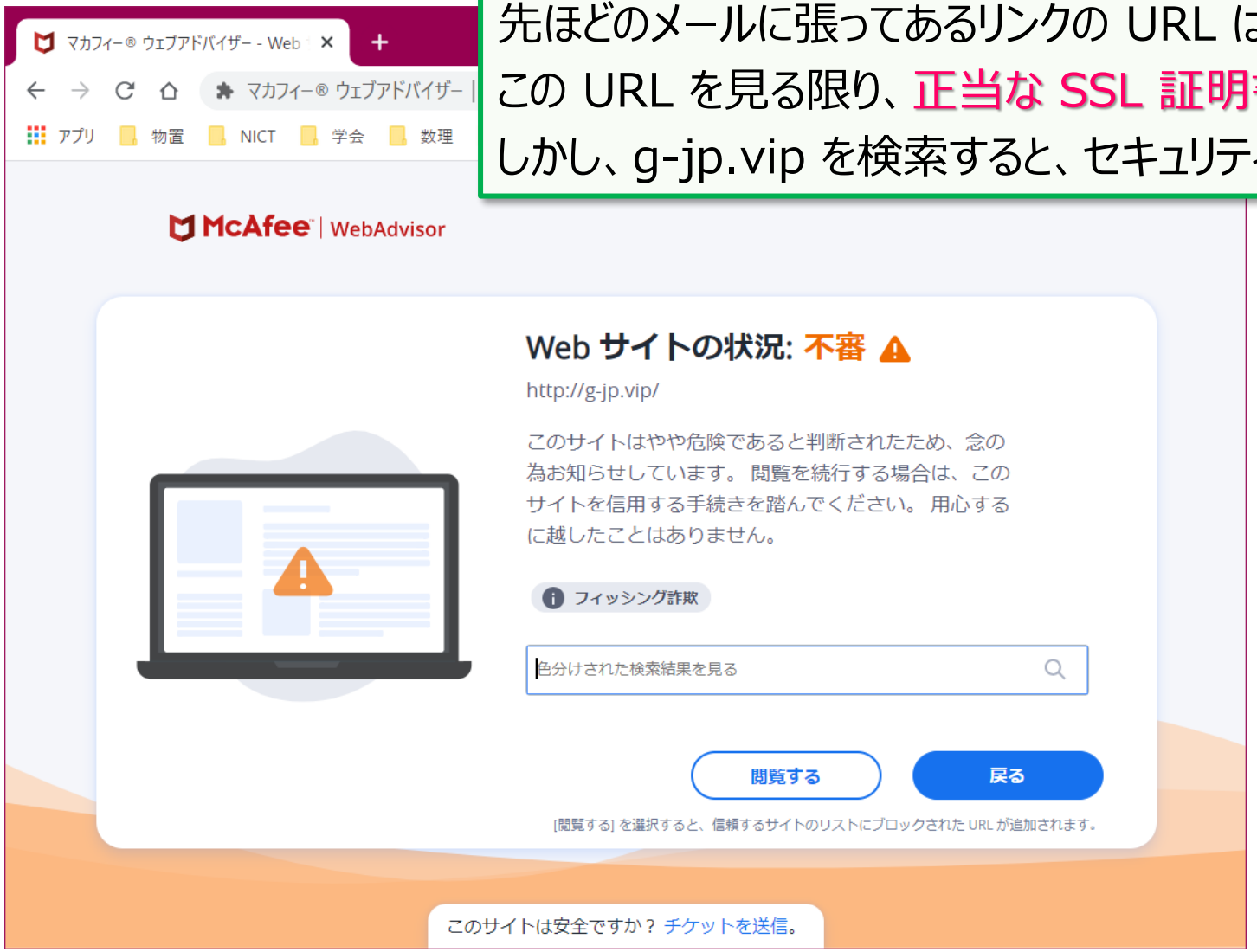
smtp.mailfrom=khphxiir@cr.mufg.jp

プロバイダのビジネス上、怪しいというだけでメールを削除してよいかどうかは、考え方の難しい所です（利便性/経済性とセキュリティのバランス，調査を受ける側のセキュリティ対策）。

しかしながら、
プロバイダが扱うメールの量は膨大なので、
全てのメールを徹底的に調べることは、
現実的ではありません。

例えば、問い合わせに回答がない場合は、未定(時間切れ)として扱うしかないですよね。

厄介な偽装メール（2の続き）



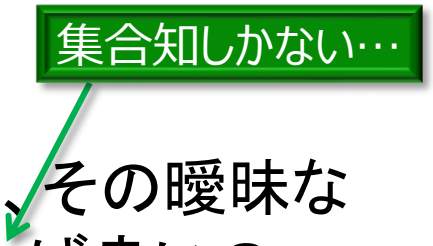
先ほどのメールに張ってあるリンクの URL は、https://www.g-jp.vip/ でした。
この URL を見る限り、**正当な SSL 証明書も取得**しているようです。
しかし、g-jp.vip を検索すると、セキュリティ会社から左図の情報が表示されました。

今回の事例で言えば、張られている URL が三菱UFJニコスと全く違うので、事前に気付くことができます。

しかし、常にそう都合良く気付けるでしょうか。

SSL 証明書で守られないもの

- SSL 証明書では、ユーザが接続するサーバのドメイン名が保証される。
  - mailv3.m.titech.ac.jp に SSL で接続する場合、
    接続先は必ず mailv3.m.titech.ac.jp であることが保証される。
  - つまり、接続先が mailv3.m.titech.ac.jp のフリをすることはできない。
- https でホーム ページに接続する場合も同じ。
  - 接続先となるサーバのドメイン名を見れば、怪しいサイトかどうか分かる。
  - www.apple-???.com などは怪しいと予想される。
- 関西を中心に展開する大手家電量販店の上新電機のホーム ページは、www.joshin.co.jp というドメイン名である。
  - では、joshinweb.jp というドメイン名は怪しいページなのだろうか？
  - 悪意のある組織が**曖昧なドメイン名**で SSL 証明書を取得した場合、その曖昧なドメイン名が正当な組織と関係があるかどうか、どうやって判断すれば良い？



そこで重要となるのが E-mail のマナー（セキュリティ上の必要性）

by 世界の正当なNW管理組織群

- **東工大のアドレス**からメールを出す意味。
  - 東工大のアドレス（要はメール サーバ）は基本的に詐称できない。
  - **東工大の学生**という立場からメールを出していることを、**電子的に保証**している。
  - gmail のアドレス：誰でも取れる。どんな立場でメールを出したのか不明。

- **公的な提出の場合は、件名にその旨（例えば提出物名など）を表記し、本文中にも、差出人名/詳細な提出物名などの情報を書く。**
  - 携帯から友人にメールを出す場合とは異なる。
  - いい加減な表記では、廃棄されても文句は言えない。
  - いくら提出したと主張しても、取り上げてもらえない。
  - **標的型メールの被害は深刻 → 標的型メールでないことを様々な手段で証明**
    - **≫ メール アドレスだけで十分？　東工大ポータルは、何故 2 段階認証なのか。**

悪意のある偽装メールへの対策

- セキュリティ啓発ページなどには、対策が紹介されているが、攻撃者もこれを見ている。
  - 例えば、文字化けのあるメールは怪しいとか。送信者のメール アドレスが不自然とか。
- **添付ファイルのあるメールが届いたら、これを開けてもよい合理的な理由に思い当りますか（以下は、一例）。**
  - 自分が送ったメールの返信として、添付ファイルが来た？
  - 私が知っている〇〇から、近々送ると言っていた？
  - 心当たりのない差出人ならば、情報検索で確認できる？
  - 私に届いた理由（例えば本文の意味など）は合理的か？
  - 事件やイベント関係だとしたら、情報検索で確認できる？
  - 会員番号など、明記されるべき秘密情報は入っている？

オンライン世界における正当性

- 「…など」が大事
- 複数の手段で正当性を調べる。
  - 現実的な対策：重大性に応じて調べる数/調べ方を判断
- 実例は、またお見せします。

今後の予定

- 情報検索
  - 人為的な規則に従い、整理が試みられている情報群
  - 全体を対象とした整理規則が存在しない情報群