東京薬科大学における電子メールシステムの歴史とWeb 3.0

森河良太[1]、山田寛尚[1]、倉田香織[1]

1．はじめに

コロナ禍の真っ最中であった2021年頃から，**Web 3.0**（ウェブさんてんぜろ）とか**Web3**（ウェブスリー）といった言葉を耳にするようになった．18年ほど前に流行した**Web 2.0**[1]の次に来るもの，というニュアンスを感じるが，ようやく最近になってその定義が少し固まってきたように思われる．

20世紀末，俗に「ホームページ」と呼ばれた，情報を送り手（サーバ）から受け手（クライアント）へ一方的に送信するWebサイト（これは後に**Web 1.0**と呼ばれた）が大流行したが，その後，AmazonやGoogleのように，送り手と受け手が相互に情報のやり取りできるWebサイトが登場すると，ティム・オライリー氏はそれらをWeb 2.0と呼んで区別した．オライリー氏による本来のWeb 2.0の定義は，性善説に基づく理想のWebの指針・在り方であったが[1]，その中で示唆された「個人ユーザー」と「主催者が提供する最小コンテンツ」の「リンク」に関する部分が商業的利益を目的に肥大化し，「Web 2.0はバズワードである」と言われながら，Web2.0の一つの形態である「**クラウド**」へ着地したように思う．

一方，電子メールの歴史は古く，大型コンピュータを通じたメッセージのやり取りであれば，MITのCTSS（The Compatible Time-Sharing System：互換性のあるタイムシェアリングシステム）を使って1965年に行われたという．これは単純にメッセージの書かれたファイルを一つのコンピュータで共有する方法であり，現在のインターネットにおける流行で言えば，Google ドライブやNextCloudなどのオンラインストレージを使ったファイル共有サービスに相当する．また我々が現在も使っている**［ユーザ名］@［ドメイン名］**という電子メールアドレスの形式も1971年に登場している．

ここで情報の送り手と受け手を流動的に変えることができるという，電子メールのメディアとしての特徴に着眼すれば，電子メールはウェブよりも早期に誕生した双方向通信ツールと言える．しかしその電子メールは，20世紀の終わりに携帯電話のキャリアメール（ドコモのiモードやauのEZwebなど）の大波を受け，Web 2.0の時代を経た後にクラウドシステムに飲み込まれていく．本稿では，特異なメディアとしての電子メールのこれまでの変遷を振り返りつつ，Web 2.0の次の時代（Web 3.0）における電子メールの未来について考えてみたい．そのために本学の学内ネットワークTYCOONで運用されて来た電子メールシステムの歴史を，まずは紐解いてみよう．

[1] 情報教育研究センター

２．TYCOON における電子メールの歴史

現在のインターネットにおける電子メールは，主に **SMTP**（Simple Mail Transfer Protocol）を用いて送受信が行われているが，それ以前は UUCP（Unix to Unix Copy Protocol）という，Unix 上に実装されたデータ転送を行う通信プロトコルを用いて行われていた．簡単に言えば，Unix 系 OS を搭載したメールサーバを組織内に設置し，他の組織との間で電話回線や専用回線を通じてコピーし合う，言わばバケツリレーのような方法で電子メールを送受信していた．

2-1. TYCOON メールシステムの誕生

本学では 1994 年 7 月に，土橋朗教授（前・情報教育研究センター長）を中心とする薬学部の 5 研究室が参加する LAN において，IIJ との UUCP 接続を行なって電子メールサービスを開始したのが最初である[2]．その 2 ヶ月後には生命科学部を中心としたグループが WIDE インターネットへの TCP/IP を行い，SMTP によるメールの送受信を開始した（接続先は東京工科大学であった）．当時は主に大学や企業の研究所がインターネットへの接続を開始していたが，その主なニーズは仮想端末（**telnet**）の利用や FTP(File Transfer Protocol)によるファイルの送受信，電子メール（e-mail）の送受信，そしてネットニュース（fj.*など）の購読であった．本学が WIDE との TCP/IP による接続を行なった当初も，ネットニュースを除く前述のサービスをユーザーに対して提供した．ただしネットワークの管理を行うために必要とされた上位層のサービスは，電子メールと DNS（Domain Name System）のみであった．勿論，この他にも LAN 配線とルータ，そして専用線回線の契約が必要となるが，当時は組織の ICT のセキュリティを守るファイアウォールも，通信の流量を調整するロードバランサーも必要なく，簡素に学内 LAN をインターネットに接続することができた．その翌年（1995 年）の 9 月には，薬学部と生命科学部の両学部，そして事務部門を結ぶ学内ネットワーク TYCOON が整備され，学内には DNS と NTP（Network Time Protocol）サービスを兼用した 5 台のメールサーバ（機器としては SunSPARC 20 が使われた）が設置された．

2-2. 初期のメールサーバにおけるセキュリティ

5 台のメールサーバには，それぞれ薬学部教員，薬学部学生，生命科学部教員，生命科学部学生，事務職員のグループをサブドメインとして振り分け，それぞれのドメインに属するユーザーを登録し，機器の管理者（root）がユーザーの管理を兼ねた．メールサーバは **Unix 系 OS**（当時は SunOS 4.1.4）上で **sendmail** というソフトウェア使って構築していたため，メールユーザーの登録は Unix の一般ユーザーとしての登録で十分であり，vipw コマンドによる /etc/passwd 等のファイルの編集によって行っていた．またユーザーには読み書きの権限を許可されたホー

ムディレクトリが与えられ,そこにメールの転送先を記した.forward というテキストファイルを作成することにより,メールを他のメールアドレスに転送することができた．また受信したメールは/var/spool/mail/というディレクトリの中に,メール受信者のユーザ名と同一のファイル名をもつ1つのファイルに順次書き加えられ,メーラ（メールクライアント）から POP や IMAP といったメール受信プロトコルを使って読むことができた．またメールサーバへ telnet を使って直接ログインし，Unix の mail コマンドや MH（Mail Handler）コマンドを使ってメールの送受信や読み書き,そして整理をすることもできた.

このように初期のメールサーバは,Unix のファイルシステムと簡単なコマンドを知っていれば,その動作原理を理解しながら確実に利用することできた．一方,現在の一般的なメールシステムでは，一般ユーザーがメールサーバに OS レベルでログインできることはほとんどない．よって現状に比べれば，当時のメールサーバの機密性と完全性に関わるセキュリティは低かったと言わざると得ない．同様にメールサーバを運用する機器も現在ほど頑強ではなく，また冗長化もされていなかったため，メールシステムの可用性も低かった．そのため電源やハードディスクドライブの故障によるシステム停止が度々発生した.

2-3. SPAM（迷惑メール）の増加とメールゲートウェイの導入

メールシステムの可用性を低下させる原因は，機器の故障によるものだけではなかった． サーバへのクラッキング（不正侵入によるデータの破壊や改ざん）や見ず知らずの第三者から送信される **SPAM（迷惑メール）**も，メールシステムの可用性を低下させるのに十分な攻撃であった.

SPAM はメールシステム導入時から TYCOON に向けて送信されていたが,その内容はコンピュータウイルスなどのマルウェアを伴わない広告的なものであり,数も少なった．そのため個々のユーザーがメーラを操作する中で，受信したメールが迷惑メールか否かを判断し，削除や隔離を行なっていた．また SPAM によって通信回線の帯域が占有されてしまうようなこともなかった.

しかし 1999 年 9 月，本学は初めて DoS 攻撃（対象となるノードに過剰なアクセスを行い，通信を麻痺させる攻撃）を受け，メールの送受信を含む WIDE インターネットへの通信が全て停止した.しかもその DoS 攻撃は学外からの大量のアクセスによる結果ではなく，本学のメールサーバから発信された通信データによるものであった．これは学内の多くのサーバ（研究のための計算機を含む）で起動していた sendmail の脆弱性を突かれることで，SPAM の不正中継[3]を強いられた結果であった．対処のための情報が少ない中，TYCOON を管理していた当時のネットワーク運営委員会は原因の究明と技術的な対策を検討し，その結果，学外とのメールの送受信を一手に引き受けて中継するサーバ（**メールゲートウェイ**）を 2000 年 8 月に新設し，学内におけるメールの送受信の流れを作ることになっ

た．すなわちネットワーク運営委員会が管理していた複数のメールサーバは，このメールゲートウエイを中継して学外とのメールの送受信を行うことになり，集中管理されたメールゲートウェイがメール送受信の最前線に立つこととなった．その後も不正中継に関するインシデントは度々発生し，その度にメール通信経路に関する改善が重ねられた．そして 2002 年 3 月，最終的に本学のファイアウォール（1998 年 10 月に設置）の設定を改善することにより，ようやくメールの不正中継を止めることができた．

しかし学内 LAN から発信される SPAM は，それだけでは止まらなかった．SPAM を発信する**ワーム**（自律的に機能する**マルウェア**）が，学生を含む学内ユーザーのパソコンに感染する事態が頻発するようになったからである．学内における**コンピュータウイルス**の報告は，1996 年 7 月 16 日のネットワーク運営委員からの報告が最初であった．これは"Good Times"という，実際にはコンピュータウイルスではないソフトウェアに関する牧歌的なものであった．しかし 2001 年 11 月には，Windows 用のトロイの木馬型のワームである BADTRANS.B がメールに添付されて TYCOON に届くようになった．そしてワームに感染したパソコンは，ワーム自身をメールに添付した大量の SPAM を学内メールサーバに向けて発信し，メールサーバの運用を麻痺させた．このような**ウイルスメール**による被害が頻発したため，ネットワーク運営委員会は TYCOON に接続されたパソコンのもつ脆弱性を取り除くため，OS のアップデート等をユーザーに推奨した．同時にメールゲートウェイに対しては，メールに添付されたマルウェアを検知・削除するためのトレンドマイクロ社製のアプリケーション（InterScan Messaging Security）を 2004 年 5 月に導入した．これらの対策により，学内から発信される SPAM は大きく減少したが，学外から送信される SPAM については，ユーザー自身がメーラにフィルタの設定を施すなどして，SPAM を削除する否かの判断を行なっていた．メールゲートウェイにおいて SPAM を判別し，削除や隔離を行うソフトウェア製品（**SPAM フィルタ**）は既に存在したが，SPAM の判定精度が低く，重要なメールまで削除または隔離してしまう可能性があったため，導入には踏み切れなかった．

その後，SPAM の発信源となっている IP アドレスを共有し，それに基づいて SPAM の判定（**IP レピュテーション**）を行う技術が登場すると，SPAM フィルタにおける SPAM 判定の精度は劇的に上昇した．一方，TYCOON におけるメール受信量に占める SPAM の割合も徐々に増加し，2007 年 9 月には，学外から送信されて来る大量の SPAM をメールゲートウェイが処理するために 6 時間以上かかってしまうという，これまでにない異常事態が発生した．本来，電子メールは手紙のように非同期性という特徴をもったメディアであるが，携帯電話によるキャリアメールが普及する中，ユーザーはメールの送受信において生じる遅延に敏感になっていた．メール遅延に関する多くの不満が寄せられる中，ネットワーク運営委員会では SPAM フィルタの導入を急遽決定し，2008 年 4 月にウイルスと SPAM の双

方を検知・削除できる現 Cisco 社製の IronPort を選定し，メールゲートウェイとして更新した．前評判の通り，IP レピュテーションによる SPAM の判定と削除は非常に適切にはたらき，メール受信の 7 割以上を占めた SPAM をメールゲートウェイで削除することに成功した．

2-4. Web メールの登場とクラウドの台頭

現在，電子メールの送受信をスマートフォンのアプリやパソコンの Web ブラウザから行う **Web メール**が一般的となっているが，最初に TYCOON で Web メールのサービスを開始したのは 2000 年 2 月である．利用したアプリケーションは **Emurl** という Pacific Software Publishing 社が開発したソフトウェアであり，Microsoft 社の **Hotmail** のオンプレミス版として Windows NT 上で動作した．Web メールが TYCOON に必要となった理由は，学外からの POP や IMAP によるメールサーバへのアクセスが，セキュリティを理由に制限されていたことによる．Emurl（学内では OpenMail と呼んでいた）は既存のメールサーバに POP を使ってアクセスし，スプール（受信したメールを貯めておく領域）からメールを読み出すという，いわば Web ブラウザからアクセスできる巨大な学内共用メーラとして機能していた．その後 Emurl のサポートは終了し，本学の Web メールは 2003 年 11 月に日立アドバンストデジタル社の **GraceMail** へ更新された．

その少し後（2004 年 4 月），**Google** 社はパブリック・クラウドの代名詞となる Web メールサービスである **Gmail** の提供を開始した．それ以前にも **Yahoo!メール**（1999 年サービス開始）や先述の **HoTMaiL**（1997 年に Microsoft 社が Hotmail 社を買収して Hotmail に改名）等が Web メールとして普及していたが，Gmail はそれらの Web メールの 100 倍のメール保存容量（1GB）をユーザーに無料で提供したこと，またウイルスメールに対するセキュリティチェックもしっかりしていたことから，確実に利用者が増えていった．そして 2006 年，Google の当時の CEO であったエリック・シュミット氏は「***データもプログラムも，サーバ群の上に置いておこう．そういったものは，どこか『雲（クラウド）』の中にあればいい．必要なのはブラウザとインターネットへのアクセス．***」と述べ，**クラウドコンピューティング**を提唱したと言われている．さらに 2008 年，Gmail はスマートフォンにも対応し，日本では Yahoo!メール，goo メール（NTT）に続くシェアを確保することとなった．そして Web メールも**クラウドメール**と呼ばれるようになり，スマートフォンとの連携を通して電子メールの利用形態が大きく変化した．

2-5. Zimbra による TYCOON メールシステムの統合

クラウドという言葉が流布し始めた 2007 年頃，TYCOON では sendmail を搭載した旧来仕様の 5 台のメールサーバと 3 台の Web メールサーバ（GraceMail），メールウイルス駆除サーバ，そして SPAM フィルタサーバの計 10 台のサーバを連

携し，大学のメールシステムとして運用していた．これらのメールサーバは 2004 年に導入された LDAP 認証サーバによって，いずれも東薬 ID を使って認証することができた．Gmail のように大容量のメールをサーバ内に保存できないこと，携帯電話との連携ができないことなどから，新しいメールシステムへの移行が模索された．当時，複数のサービスを同じ ID で認証できる標準的な基盤（**統合認証基盤**）に多くのクラウドサービスは対応しておらず，TYCOON メールとしては学内にオンプレミスで構築するのが最善の方法であるという結論に至った．結果，2008 年 9 月に米 Yahoo!社が販売する **Zimbra 4.5** が導入され，SPAM フィルタ（IronPort）を除く旧来のメールシステムとの入れ替えを行った[2].

Zimbra はスケジューラやアドレス帳，簡単なファイル共有ツール（Briefcase）を備え，フィーチャーフォンやスマートフォンにも対応していた．また導入当時は，職員には 5GB，学生には 2GB のメール保存スペースを提供していた．正にオンプレミスで構築したクラウド（**プライベートクラウド**）であった．ただ Sun Microsystems 社のサーバ機器を複雑に組み合わせたサーバ構成であったため，システムのトラブルも度々生じていた．

2013 年になると Zimbra のリース契約が切れ，メールシステムの更新をする必要が生じた．この時はトランスウェア社の Active! mail 6.5 と Microsoft 社の Office365，そして VMware 社（当時）の Zimbra 8.0 が選定候補として挙がった．Office365 は**パブリッククラウド**のメールシステムであり，新しいシステムへの期待もあったが，学内の統合認証システムとの連携に技術的な不安があったことと，個人情報を含む受信メールを一企業に預けることに対する危険性から，最終的には Zimbra 8.0 に更新することとなった（同年 12 月）．この機会に Zimbra を構成するサーバ機器を HP 社製に変更し，システム自体も仮想マシン上で稼働するように変更したため，以前よりも稼働時におけるトラブルは大幅に減った．またストレージ機器の導入費用も下がったことから，メールの最大保存容量は職員 50GB，学生 9GB に増量することができた．

2019 年 8 月には，セキュリティの強化とコスト削減の見地から，学内の多くのサーバシステムが一つの仮想化基盤（**TYCOON 仮想化基盤**）に集約されることが決定し[4]，メールシステムも仮想化基盤へ移行した．TYCOON 仮想化基盤は Nutanix 社製の **HCI**（Hyper-Converged Infrastructure）に対応した最新のアプライアンス機器で構成されているため，移行後は Zimbra による TYCOON メールシステムがサービスを停止することは全くなかった．しかし，2023 年 3 月，Zimbra は学内メールシステムとしての座を Microsoft365 に譲ることとなった．

３．クラウドメールの限界と Dmail の誕生

1994 年から始まった TYCOON メールシステムの歴史を，その技術的進展と共に振り返ってみた． メールの不正中継や SPAM など，電子メールというメディ

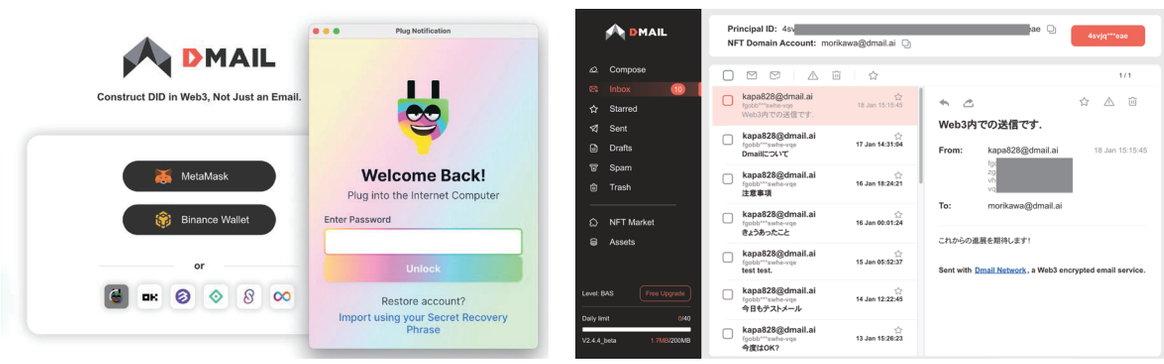
アを悪用することで発生するメールの障害は，それを防ぐための新しい技術の登場と実装によって解決が図られてきたと言えるだろう．同時にメールシステムを稼働させるサーバ機器自体の堅牢性の向上も，TYCOONメールの安定稼働に寄与した．そこで現在のクラウドメールをメールシステムの１つのゴールと考えれば，サービス構成については2008年に，仮想化を含む機器構成としては2013年に，TYCOONメールZimbraはそれぞれのゴールに概ね到達していたと言える．そのため2013年以降，TYCOONメールは安定して稼働し続け，**なりすましメール**防止のためのセキュリティの実装（**SPF**，**DKIM**，**DMARC**，**二要素認証**）や無料のOffice365を使った学内停電時におけるにシステムの冗長化（**非常用メール**）[4]など，TYCOONメールのセキュリティを計画的に向上させることができた．

しかしクラウドメールでも解決できない，最大のセキュリティ上の問題が未解決のまま残っていた．それはメールシステムの管理者による，ユーザーの個人情報の取得（閲覧）の問題である．これはクラウドメールに限らず，オンラインストレージサービスやSNS等の**サーバ-クライアント型システム**一般に言えることであり，システム管理者は何らかの方法を用いて，**個人情報**を含むユーザーのデータにアクセスすることができてしまう．組織内にオンプレミスで構築して置かれたプライベートクラウドであれば，組織内の規則に従って個人情報を守ることはできる．しかしパブリッククラウド，特に海外に拠点を持つシステムの場合はその限りではない．それ以前に，パブリッククラウドに置かれた個人の**データの所有権**はユーザー個人にはなく，契約内容に従って削除されても仕方がないということを最初から知っておくべきかもしれない．

ここでインターネットにおける一つの発明を簡単に紹介したい．それは2008年に**サトシ・ナカモト**と名乗る人物（またはグループ）によって発明された**ビットコイン（暗号資産）**である[5]．これは中央銀行のように中央集権的な管理者を持たない分散型の**デジタル通貨**であり，ユーザーは**暗号通貨ウォレット**（あるいは単に**ウォレット**）を通して他のユーザーに**P2P**（peer to peer）通信で暗号資産を送信できる．当然，暗号資産も通貨であるので，その送金に関する情報（**トランザクション**）の記録と管理が必要となるが，それは**ブロックチェーン**と呼ばれるP2Pネットワーク上に作られた**分散型台帳**に対して，巧妙な暗号化を用いて行われる．そのためブロックチェーンは，それに参加している全てのノードに記録されることになる．ビットコインは2009年に使用が開始され，現在はビットコインの他にも**イーサリアム**など，様々なブロックチェーンがインターネットを介して動いている．特にイーサリアムでは，ブロックチェーン上で人を介さずに自動で契約を行うことのできるプログラム（**スマート・コントラクト**）の実装に成功し，ブロックチェーン上でプログラムを動かすことができることを示した．

そして現在，**Internet Computer**と呼ばれる次世代のブロックチェーン基盤の開発が**Difinity財団**[6]によって始まっている．Internet Computerでは，ブロック

チェーンをあたかも一つの巨大なコンピュータのように扱い，専用のプログラミング言語 **Motoko** によって実装される **Canister** と呼ばれる新しいスマート・コントラクトを使い，大容量のデータを保存したり，アプリケーションを動かしたりすることができる．つまりクラウドのようなWebサービスを，参加者の合意によって統制されたブロックチェーン上で運営することができるのである．おそらくこれが **Web3.0** の本質であり，Web2.0 では成し得なかった世界の姿であろう．



（図）Web3 に構築された新しいメールサービス Dmail．分散型 ID（DID）で管理するため，現時点では”Plug”というオンラインウォレット（Web ブラウザの機能拡張として動作する暗号資産の財布，左図）にサインインすることで Dmail を利用できる．右図は 2023 年 1 月の時点における Dmail の操作画面（ver.2.4.4 beta）．

その一例として，Internet Computer で最初に動いた分散型電子メールである **Dmail** [7]の一部を紹介する（上図）．未だβ版であり，電子メールとしての機能は簡素であるが，個人のメールアカウントがウォレットと紐づくため，暗号資産と同程度のセキュリティを有する．またメールアドレスそのものが暗号資産として売買可能な **NFT（非代替性トークン）**である．もちろん，自分の受信したメールをパブリッククラウドのように他人にスキャンされることもない．

Zimbra が本学のメールシステムとして導入された 2008 年，既に Web 3.0 の萌芽が顔を出していたのだ．

【参考文献】

[1] 森河良太，宮川毅，林昌樹，東京薬科大学研究紀要，第 10 号(2007) 77-82.
[2] 森河良太，倉田香織，宮川毅，小杉義幸，土橋朗，東京薬科大学研究紀要，第 18 号(2015) 27-34.
[3] 山守一徳，太田義勝，分散システム/インターネット運用技術シンポジウム 2001，(2001)109-114.
[4] 森河良太，倉田香織，山田寛尚，宮川毅，土橋朗，東京薬科大学研究紀要，第 23 号(2020) 75-82.
[5] Satoshi Nakamoto, https://bitcoin.org/bitcoin.pdf （2023 年 1 月 18 日確認）
[6] https://dfinity.org/ （2023 年 1 月 18 日確認）
[7] https://dmail.ai/ （2023 年 1 月 18 日確認）