TYCOON 仮想化基盤の構築とアカデミッククラウドへの道

森河良太[1]、倉田香織[2]、山田寛尚[2]、宮川毅[1、2]、土橋朗[2]

1．TYCOON 仮想化基盤の構築

大学における教育研究およびそれらを支える各種業務において、ICT 機器による情報やデータの受信、発信、蓄積が広く行われるようになった。東京薬科大学でも多種多様なサービスがネットワークメディアを介して行われるようになり、それらを支えるサーバシステムに対しては、利便性とセキュリティが積極的に求められるようになってきた。GAFA や Microsoft 等の**プラットフォーマー**が提供するパブリッククラウドサービスは大変便利であるが、セキュリティの問題から、最近はその利用に慎重となるべきであるという意見も多く聞かれるようになった。また個人情報保護に関わる法的規制の強化が進み、従来は無料で提供されていたこれらのサービスを有料に切り替える動きも出ている。さらに機械学習（AI）技術の急速な普及や国際情勢の不安定化は、国家や自組織で収集したデータの囲い込みを促進する方向に導いていると言える。このような状況な中で、自組織の中にサーバを設置してセキュアなクラウドを「オンプレミス」に構築するという方法も再評価されるようになってきた。

東京薬科大学では、ICT サービスを提供する多数のサーバ機器が情報ネットワーク TYCOON（**To**Yaku **CO**mputer **O**pen **N**etwork）に接続されており、同時にパブリッククラウドも TYCOON に接続された 2 本のインターネット回線（帯域幅は 1 Gbps と 100 Mbps）を通じて利用されている。しかしメールシステムと統合認証システム以外の ICT サービスは学内に設置された個別のサーバに構築されており、多数のサーバ機器の保守や定期的な更新（5〜7 年）のため、システムの維持コストを引き上げる要因となっていた。

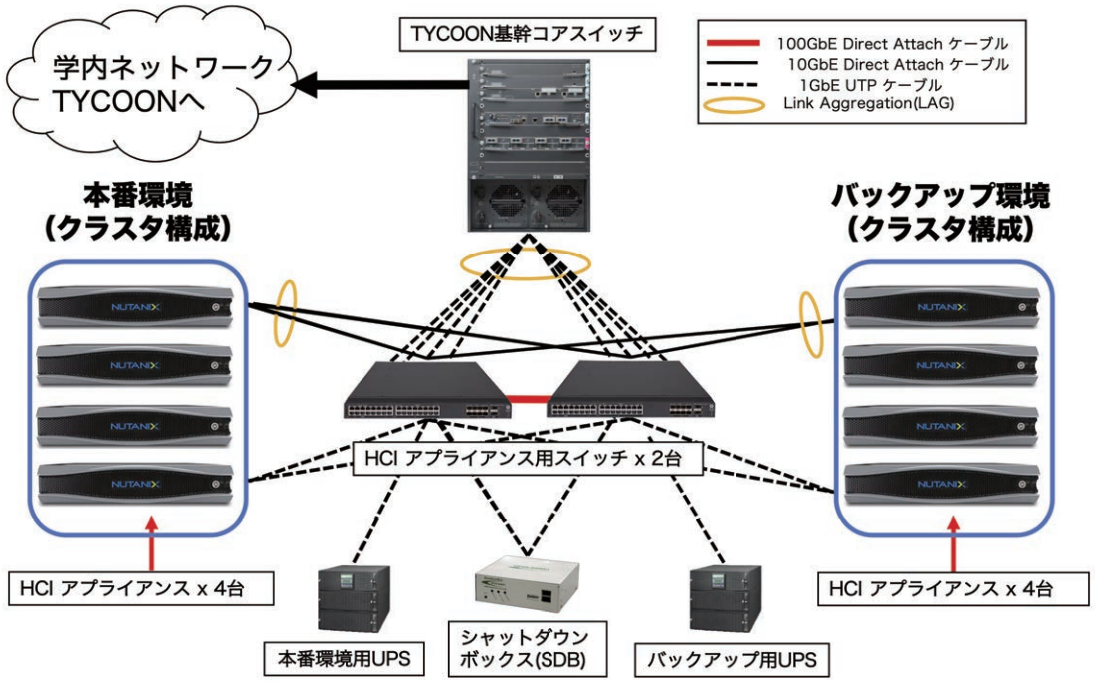
そこで本学情報教育研究センターでは、仮想化技術およびそれを使った学内設置の個別サーバの統合方法について検討を重ね[1]、2016 年 11 月の情報教育研究センターユーザー会議において説明を行った。また翌 2017 年 10 月には、同ユーザー会議において **TYCOON 仮想化基盤構想**を発表し、今後の学内における ICT 機器の導入・管理指針を提案し、議論を行った。そして **TYCOON 仮想化基盤**の具体的な仕様・構成とその管理方法について検討し、保守を含めた構築費用の見積もりを行った。特に既存の基盤サーバシステムを仮想化基盤に移行した場合に要するシステムの構築・維持・更新費用（5 年分）を計算した。その結果、仮想化基盤移行後はこれまでの全サーバのデータをバックアップし、かつ冗長化・機密化されるにも関わらず、約 2%のコストダウンとなることが判明した。以上の 2 年間

[1] 生命科学部コンピュータ委員会
[2] 情報教育研究センター

に及ぶ準備と検討、仕様策定を経て、2018年12月に開催された本学ICT整備委員会においてTYCOON仮想化基盤を構築することを正式に提案し、2019年夏に実施することが了承された。その際にTYCOONにおける**ICT基盤整備方針**を概ね次のように説明した。

1) **今後も本学のICTの基盤となるシステムは、オンプレミスで効率的かつセキュアに構築する。**
2) **仮想化ICT基盤システムのハードウェアとアプリケーションソフトウェアの更新は独立して行い、時勢に応じたシステム更新を行えるようにする。**
3) **ハイブリッドなネットワークを構成し、セキュリティを維持しながらパブリッククラウドサービスを使い倒す。**
4) **仮想化基盤内の仮想マシン環境を学内ユーザーが手軽に利用できるような、学内クラウドサービスを提供する。**

TYCOON仮想化基盤のハードウェア構成は（図１）の通りである。仮想化基盤は4台の**HCI**（Hyper-Converged Infrastructure）[3]に対応したアプライアンス機器(Nutanix社製)とそのバックアップを行う同じく4台のアプライアンス機器、そしてそれらを繋ぐ2台のIRF(Intelligent Resilient Framework)構成のスイッチングハブから構成される。



（図１）TYCOON仮想化基盤のハードウェア構成

[3] http://www.infostor.com/storage-management/hyperconvergence-next-generation-virtualization.html（2020年1月13日閲覧）

これは従来の TYCOON メールシステム[2]や統合認証システム[3]のように、サーバ機器とストレージ機器が分離していた従来型の仮想化システムに比べて非常に単純な構成となっている。さらに HCI の特徴として、必要に応じて後からアプライアンス機器を増やして、難なくシステムをスケールアウトすることができる。また 200V 電源に接続する 2 台の強力な無停電電源装置（UPS）とシャットダウンボックス（SDB）によって、予期せぬ停電時には全システムが安全にシャットダウンするように設計されている。

このようなハードウェア構成によりセキュリティの 3 要素の 1 つである可用性が大幅に前進し、本学の ICT 基盤の堅牢性が一層向上したと言える。この TYCOON 仮想化基盤は **Titania** と命名された。

２．TYCOON 仮想化基盤とサーバによるサービス

2-1. 仮想化基盤に移行したサーバサービス

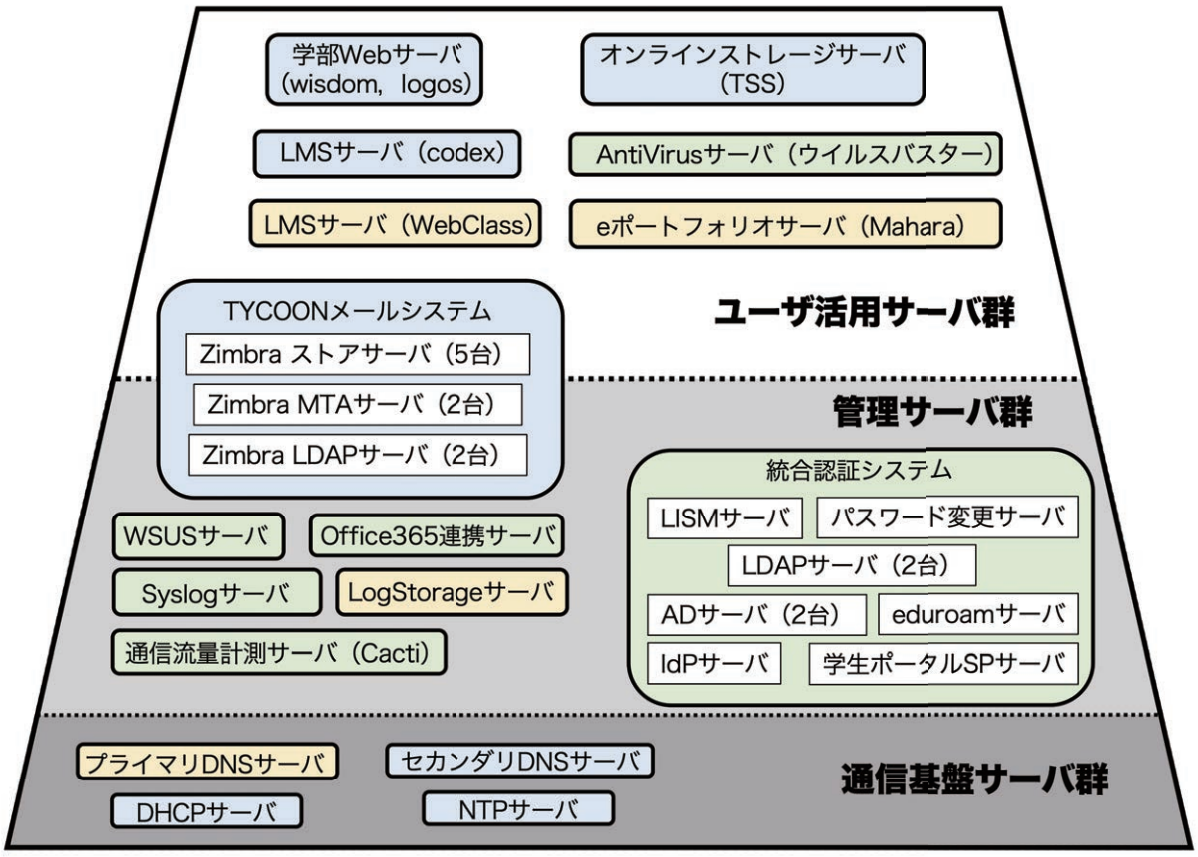
TYCOON 仮想化基盤を構成する機器は、2019 年 7 月中旬より学内への設置が開始され、既存の学内サーバの一部（無線用 DHCP サーバ、セカンダリ DNS サーバ、TYCOON メールシステム、学部 Web サーバ、Codex）が 8 月末までに仮想化基盤へ**仮想マシン**として移行（仮想化）した。また **Nextcloud**[4]というオープンソースソフトウェアを用いて学内に構築したセキュアなオンラインストレージサービスは、10 月 1 日に正式稼働を開始した。これが TYCOON 仮想化基盤の第 I 期工事の内容である。その後は 2020 年度に第 II 期工事が、2021 年度以降に第 III 期工事が行われる予定であるが、それらは全てハードウェア保守期限が切れた既存サーバ機器に対して実施される移行工事である。

第 I 期～第 III 期の間に仮想化基盤へ移行した（する）サーバサービスの概略図を（図２）に示す。これらはコスト削減のために仮想化基盤へ単純に寄せ集められたものではなく、それぞれが互いに ICT 基盤としての役割を果たすための通信を適切に行なっている。そのため仮想化基盤の外部に送受信される通信量も抑制でき、学内ネットワークの通信負荷を下げるだけでなく、**機密性**を向上させることにも寄与している。（図２）ではサーバサービスを「**通信基盤サーバ群**」、「**管理サーバ群**」、「**ユーザ活用サーバ群**」に分けて図示しているが、仮想化基盤内の実際のネットワークセグメントも、それぞれの役割や機密性に応じて分割・制御されている。また普段ユーザが利用するサーバは「ユーザ活用サーバ群」に含まれるが、それらを陰で支える、いわば黒子としてのサーバが多数存在することも理解して頂けるかと思う。

このように TYCOON 仮想化基盤は一つのクラウドを構成しており、一般にはパブリッククラウドに対して**プライベートクラウド**と呼ばれるべきものである。すなわち 2018 年度の ICT 整備委員会で示した **ICT 基盤整備方針１）**を具現化した

[4] https://nextcloud.com/（2020 年 1 月 13 日閲覧）

ものである。またHCIを利用していることから、従来型の仮想化基盤よりもハードウェアとソフトウェアの管理の分離が明確となり、それぞれの更新・管理を別個に行えるようになったことから、**ICT基盤整備方針２）**についても達成されたとみることができる。



（図２）TYCOON仮想化基盤に収納された各種サーバ。一つ一つが仮想マシンとして稼働している。水色は第Ｉ期(2019年度)に移行したものを示す。緑色（第II期、2020年度）と橙色（第III期、2021年度以降）は将来計画を示す。

2-2. すべてを仮想化基盤に集約することは得策か？

それでは学内の全てのサーバサービスおよびパブリッククラウドをTYCOON仮想化基盤に移行・集約し、管理・運用することは理にかなったことであろうか？答えは`No!'である。端的に言えば事故や災害等で肥大化した仮想化基盤システムが破壊されてしまった場合、インターネットの根幹であるTCP/IP通信も事実上、止まってしまうからである。そのため（図２）で示された「通信基盤サーバ群」については、学内の各建屋にある程度分散して配置する必要がある。そうすれば建屋ごとの最低限の通信能力が確保され、仮想化基盤が破壊された状況でも、学外のWebサーバやファイルサーバ、メールサーバにアクセスすることができるのである。

逆に最初から全ての「ユーザ活用サーバ群」を学外に出して、全てをパブリッククラウドで賄う方が良いのでは？という単純な逆転の発想が浮かぶかもしれない。確かに一般家庭がそうである。しかし組織内における情報資源のセキュリティ確保とインターネット通信回線への過大な負荷を考えただけでも、数千人のユーザーが存在する本学の規模においては、現状、セキュリティとコストの面からこの発想は否定せざるを得ないであろう。

以上の理由から、教育棟と研究棟にはDNSとDHCPを管理するサーバ（アプライアンス機器）をそれぞれ2組ずつ、またネットワークセンターには仮想化基盤に収容しないDNSサーバとNTPサーバを、それぞれ継続して運用する方針である。またファイアウォールで仕切られたセキュリティレベルの高いネットワーク（事務系ネットワークやCBTネットワーク）については、これまで通り独自のDNSサーバやDHCPサーバを運用していく必要がある。その他にも無線LANコントローラのように通信量が非常に大きいにも関わらず、仮想化基盤内の仮想マシンとの直接通信量が少ないサーバについては、個別のサーバ機器で運用するべきである。

2-3. 仮想化基盤へのサーバサービス移行における工夫

第Ⅰ期において既存のサーバ機器を仮想マシンに移行する際、単純に物理サーバ上で稼働しているシステムを仮想化基盤上の仮想マシンに移行する（**P2V**：Physical to Virtual）のではなく、幾つかの統合や合理化を併せて行った。

まずWebサーバ（ホームページサーバ）については、これまで学内に分散配置していた研究室や委員会、個人等のWebサーバを一つの仮想マシンに統合した。その結果、Webサーバを構成するミドルウェア（Apache、PHP、MySQL等）の保守管理、特に脆弱性対応のための作業コスト（人的コストを含む）が大幅に削減された。しかし統合によるコンテンツへの影響はほとんど無く、ユーザは今まで通りホームページを更新することができている。

TYCOONメールシステム(Zimbra)については、基盤となるOSをライセンス料が有料であるRedHatから無料のオープンソースであるCentOSに変更し、長期的な視点でのコスト削減を行った。またその際にアプリケーションを長期間利用可能（LTS：Long-term Support）なバージョンである8.8.15にアップデートした。

またこれまで学内で古くから利用されてきた様々な形態のファイルサーバは、より使い勝手の良いオンラインストレージサーバに置き換え、**TSS**（**TYCOON Secure Storage**）と命名してサービスを提供している。このサーバはNextcloudという無料のオープンソースソフトウェアを利用して構築されており、機能的にはDropboxやGoogle Driveに似ている。すなわち自分のパソコンや携帯機器のデータを直接あるいはWebブラウザを通じてTSSに保存したり、それを他のユーザ(外部関係者を含む)と共有したりすることができる。ただしDropboxやGoogle Driveとは異なり、学内で設置・管理された仮想化基盤上に構築されているので、

プラットフォーマーによる個人情報の収集を心配する必要もない。

ただTSSの難点を挙げるとすれば、ユーザが保存できるファイルの全容量の上限が、学生は1GB、職員は10GBという点である。これまで学内に設置されていたファイルサーバの容量よりは大きいが、マイクロソフトのOneDrive（上限1TB）等と比べると、セキュアとは言え容量の点では見劣りする。そこでそれを補完する機能が、TSS（Nextcloud）における「**外部ストレージ機能**」である。Nextcloudには外部ストレージ、例えば研究室に設置したNAS（Network Attached Storage）やGoogle Drive、OneDrive等を一つのフォルダとみなして接続(マウント)する機能がある。この設定をユーザレベルで行えば、個人または研究室等で管理する外部ストレージの持つ容量をTSSに加えることができる。情報教育研究センターでは、研究室で所有するNASをftp、sftp、SMB、WebDAV等のプロトコルを通じてTSSにマウントしている事例を確認している。またGoogle DriveやSharePoint（OneDrive）で提供されるオンラインストレージも、仕様上はTSSにマウントすることが可能である。しかしパブリッククラウド側の仕様が度々変更されるために、安定したマウントは期待できないので、それ相当のスキルを持つユーザ以外にはお勧めしない。これはパブリッククラウドの根源的な技術的閉鎖性、**ユーザ側におけるアンコントローラブル**な管理仕様の表れ、と言えるであろう。

３．プラベートクラウドからアカデミッククラウドへ

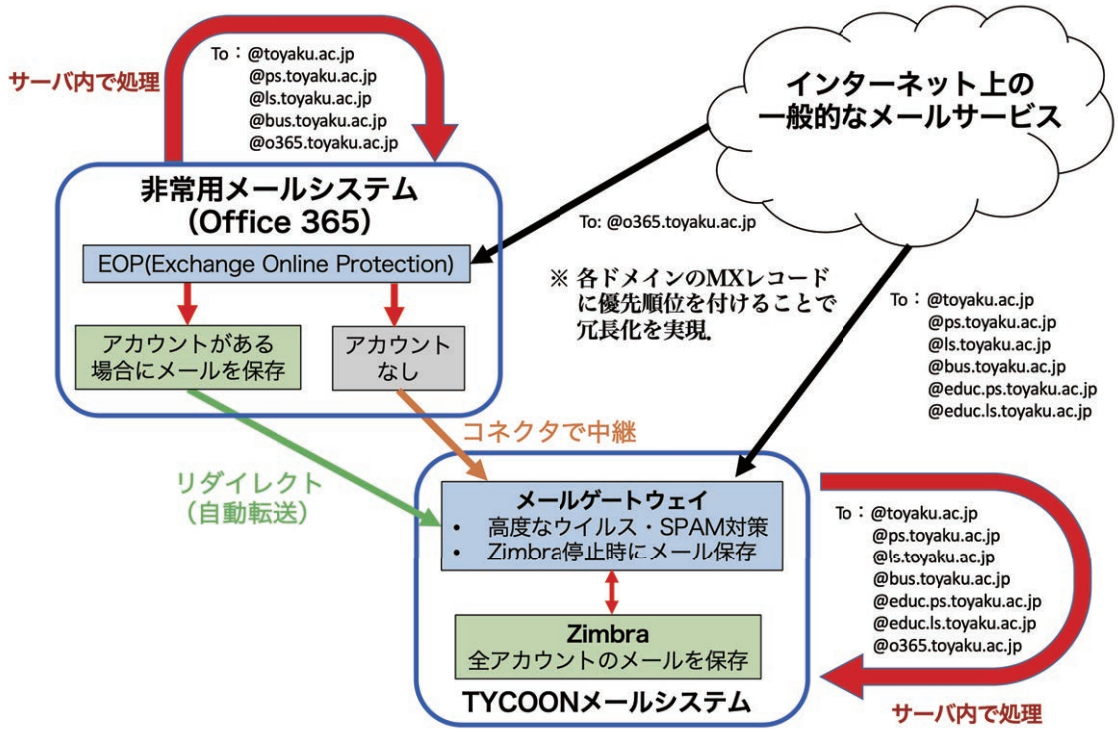
3-1．ハイブリッドクラウドを目指すTYCOON仮想化基盤

TSS（Nextcloud）の外部ストレージ機能を使ってGoogle DriveやSharePointを簡単に接続できない可能性があることは、少々残念な事実である。しかしNextcloudは、2016年にownCloudという優秀なオンラインストレージソフトウェアから分岐して誕生した比較的新しいソフトウェアであるにも関わらず、日本では京都大学や名古屋大学を始めとした多くの大学や研究所で爆発的に導入・活用されている。よって今後の継続的な機能改良も期待されるであろう。それを注視しつつ、より根源的な解決方法を模索・検討し、本学**ICT基盤整備方針３）**を実現していくことは、今後の本学のICT基盤整備における重要課題であると考える。すなわちプライベートクラウドを中心に据えた複数のパブリッククラウドとの**疎結合**による**ハイブリッドクラウド**の実現が、TYCOON仮想化基盤の向かう先であると考える。TSSについては、今後も実証的な検討作業を繰り返し、より使い勝手の良いものに改良していく必要があろう。勿論、そのような基盤構築におけるセキュリティの確保は、最も優先すべき大前提である。

一方、既にハイブリッドクラウドとして稼働している本学のICTシステムが存在する。それは平時に利用するTYCOONメールシステム（Zimbra）とTYCOONメールシステムが利用できない場合に活躍する**TYCOON非常用メールシステム**（Office 365）の連携システムである。

3-2. ハイブリッドクラウドとしての TYCOON 非常用メールシステム

本学では年末に、電気系統の定期点検のための学内一斉停電が実施される。期間は約 1 日であるが、この間に学内 ICT サービスも全て停止する。そうなると学外から本学ユーザ宛に送信される電子メールは、TYCOON メールシステムと SMTP による接続が確立できないために、送信側の MTA サーバに暫く滞留することになる。これは電子メールシステムの一般的な仕様であるが、学内停電時でも学外からの電子メールをすぐに読んで返信したいという要望は絶えることはなかった。また 2018 年 7 月には、「本学ネットワークのセキュリティーを維持しながら、パブリッククラウドの利用も進めるように」という大学の要望もあった。



（図 3）TYCOON 非常用メールシステムにおけるメールフローの概念図

そこでメール送受信システムのハイブリッド化による二重化について、TYCOON 仮想化基盤構築の第 III 期に実現する計画として、2018 年 12 月の ICT 整備委員会にて説明を行った。そしてこの計画は結果的に前倒しで実行されることになり、翌 2019 年 7 月に TYCOON 非常用メールシステムの運用が開始された。

TYCOON 非常用メールシステムは、TYCOON メールシステムの可用性を高めるため、Microsoft のアカデミック EES 包括ライセンスである「Office 365 A1」（無償）を契約して構築したシステムである。具体的には、（図 3）のようにパブリッククラウドである Office 365 の電子メールサービス Microsoft Exchange Online を使ってハイブリッドなシステムを構築した。TYCOON メールシステムに障害やメンテナンスが発生した際、予め設定した DNS における MX レコードの順

位付けにより、本学ドメイン（@toyaku.ac.jp）宛の学外からの電子メールをExchange Online において受信できるようにしている。ここで Office 365 のExchange Onlineにアカウントを持つユーザは、Office 365のポータルサイトにサインインして受信したメールを確認し、@o365.toyaku.ac.jp のメールドメインを使って返信することができる。そして障害から復旧した後は、再び TYCOONメールシステムにメール送受信が一元化される。

なおセキュリティ意識の高いユーザは、電子メールの送受信に Office 365 やGmailのようなパブリッククラウドの利用を避ける傾向にあるので、TYCOON非常用メールのアカウントについては、ユーザからの申請があった場合に作成している。このようにユーザの考え方や立場を尊重するのであれば、ハイブリッドクラウドではサービスの利用の有無に関してヘテロな状態を許容し、それに基づいた運用を行なっていく必要があろう。このヘテロな思考の中に、大学らしいクラウドである**アカデミッククラウド**の本質があるように思う。

４．東薬ユーザがつくるアカデミッククラウド

クラウドという言葉は 2006 年頃に登場し、急激に普及していったが、干支が一回りする（12年）頃には、世界中でクラウドに対する様々な反省や反動が聞かれるようになった。それは地政学的にはグローバリズムに対するナショナリズムの反発と結びついているのかもしれないが、組織対個人という視点でクラウドの変遷を眺めてみると、インターネットの鼓動が聞こえてくるようで大変興味深い。ただ文明に飼い慣らされた我々は、第三者としてそれらを観察する立場ではあり得ず、日々スマホと共に生きる中でそのことを意識する必要があるのではないか。そしてそういった思索は、大学というアカデミックな場で育まれるものであると思うし、そこからアカデミッククラウドが生まれるようにも思う。

もしユーザの皆様にICT活用に関する良いアイデアがあったら、本学 **ICT基盤整備方針４**）にあるように、TYCOON仮想化基盤システムを学内クラウドサービスとして利用してみては如何であろうか。情報教育研究センターは仮想化基盤という器を整備し、セキュアなデータの保存とネットワーク通信の環境を提供するが、それをどう活用するかは、ユーザの皆様に頼る部分が非常に大きいのである。

なお本稿の主題であるTYCOON仮想化基盤システムの構築において、楠理事長、松本常務理事、安田常務理事の皆様、および財務企画部長、総合企画課の皆様には大変ご助力頂きました。この場を借りて感謝申し上げます。

【参考文献】

[1] 森河良太，倉田香織，宮川毅，土橋朗，東京薬科大学研究紀要，第 22 号（2019）17-24.

[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] 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 19 号（2016）51-58.