九州工業大学におけるMicrosoft 365の全学展開

- 提供範囲の拡大，セキュリティの向上に対する奮闘 -

林　豊洋

九州工業大学　情報基盤センター

toyohiro@isc.kyutech.ac.jp

自己紹介

林　豊洋 (Hayashi Toyohiro)

九州工業大学　情報基盤機構

情報基盤センター　准教授

ICT利活用教育研究基盤運用室 (BYOD，全学サービス，統合ID，365，クラウド化検討など，こちらがメインの業務)

ネットワークセキュリティ基盤運用室 (全学ネットワーク，無線，VPN，セキュリティなど)

[略歴]

1999年　国立有明工業高等専門学校 電子情報工学科卒業，九州工業大学情報工学部 知能情報工学科 3年次編入学 (高専からの編入勢)

2006年　九州工業大学大学院 情報工学研究科 博士後期課程修了．博士(情報工学)

2006年　九州工業大学情報科学センター 助手

2007年　同助教

2020年　九州工業大学情報基盤センター 助教 (改組)

2021年　同准教授

[研究分野、研究テーマ]

・情報システムの構築運用

・知覚情報処理(CV，PR) (もともとはこちらでした)

講演の概要

- 九州工業大学の概要
- Microsoft 365 (Office365) 導入のきっかけ / 当初は導入予定はなかった
- SaaSの移行は難しい
- Office365がやってきた / 利便性抜群だった．ただ初期設定が大学には…
- シェアが高いシステムは狙われる
- Microsoft 365 A5導入 / MFA導入
- Teamsを使いたい，DXに活用したい．/ どの設定を変えれば良いのか…

九州工業大学の概要

国立大学法人九州工業大学

1907年開学 / 1949年大学設置 / 2004年法人化

工業系単科大学，福岡県に3キャンパス(戸畑，若松，飯塚)

学生数：約5,600名

2学部　(工学部2,300名，情報工学部1,800名)

3大学院　(工学府660名，情報工学府440名，生命体工学研究科410名)

教職員数：約620名

教員約350名，研究系職員約80名

事務・技術系職員約200名

同窓会組織(明専会)

会員数：約37,000名

Microsoft 365 (Office365) 導入のきっかけ
- 当初は「導入候補外」-

「卒業生・退職者との繋がりを強化したい」(2009年頃，経営陣の考え)

繋がりのツールとして，**卒業生・離退職者向けメールサービスの実現**可能性の検討指示

メールサービス要求仕様

最重要：永続的に提供可能

重要：問題が起きた場合，国内法が適用される運用体系

機能面

(可能であれば)メールボックスの付与(転送サービスではない)

アカウント設定不要，容易に利用できるUI (Webインタフェース)

もともとは，
数万人の卒業生がカバーできる無償のメールサービスを探していた

Microsoft 365 (Office365) 導入のきっかけ
- 当初は「導入候補外」-

「卒業生・退職者との繋がりを強化したい」(2009年頃，経営陣の考え)

繋がりのツールとして，**卒業生・離退職者向けメールサービスの実現**可能性の検討指示

メールサービス要求仕様

最重要：永続的に提供可能

重要：問題が起きた場合，国内法が適用される運用体系

機能面

(可能であれば)メールボックスの付与(転送サービスではない)

アカウント設定不要，容易に利用できるUI (Webインタフェース)

当時の候補は，
「Gmail」「Yahoo! メール」「Live@Edu (MS)」
・当時国内法適用はY! のみ
・メールサービスだけあればよい

→ Yahoo！メールAcademic導入が決まる

Microsoft 365 (Office365) 導入のきっかけ
- 当初は「導入候補外」-

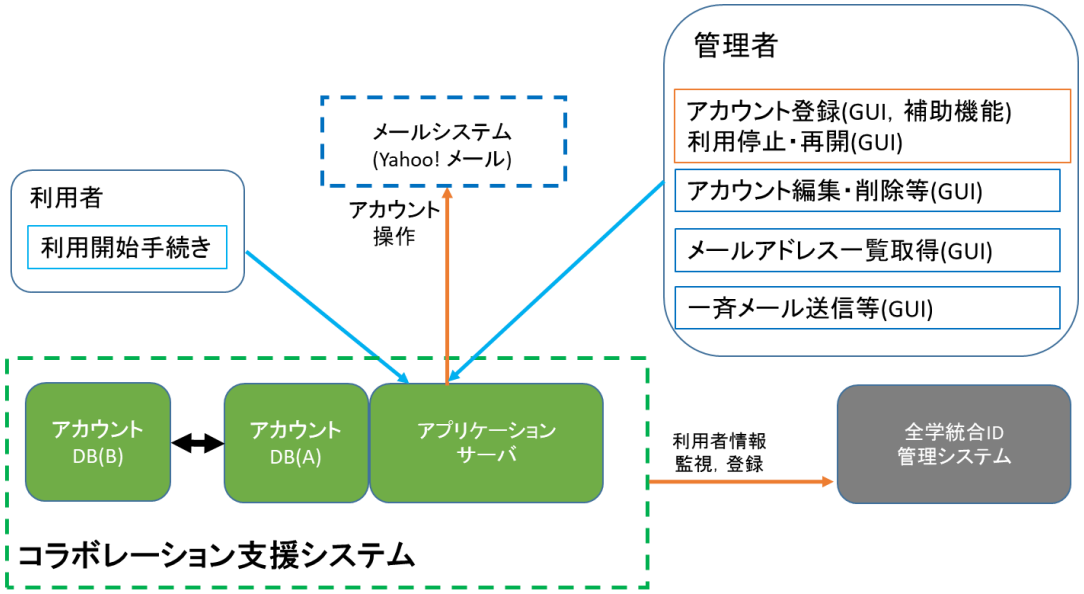
九州工業大学　生涯メールサービス
メールシステム(無償) + アカウント管理システム構築により2012年度よりサービス開始
2014年度より，在学生・教職員に利用者を拡大

SaaS : Yahoo!メール Academic Edition (教育機関は無償利用可能)

- foo@mail.kyutech.jp アカウント (Yahoo! IDと紐づく)
- Webインタフェース，SMTP，POP，IMAP
- メールボックス容量 2GB
- 卒業後は非優待ユーザ(広告受信)として永続利用可能

アカウント管理システム：学内システム

- 利用者向け機能
  - ログインサイト：Y!メール利用開始手続き(アクティベーション)
- 管理機能
  - 学内の統合ID管理システムと連携
  - ID生成を検知し，メールアカウント作成 (Y! AEに備わるREST API操作)



SaaS→SaaSへの移行
-「契約が変わる」だけでは済まない-

九州工業大学　生涯メールサービス
メールシステム(無償)＋アカウント管理システム構築により2012年度よりサービス開始
2014年度より，在学生・教職員に利用者を拡大

三年強にわたり運用していたが…

2015年2月：「Y! AEサービス終了のお知らせ(2016年6月末)」通達

- 以下の制約のもと，新たなメールシステムへの移管を行うこと
  - 提供されない情報
    利用者のメールアドレス，紐づいたYahoo!メールアドレス，
    パスワード一覧
  - アカウント，メールボックスの削除は実施しない
  - メールボックスの移行に関する依頼は受けることができない

管理者的には，相当つらい制約

SaaS→SaaSへの移行

-「契約が変わる」だけでは済まない-

2016年6月30日にサービス終了，どうするか?

移行・継続のため実施すべき事項

新たなメールシステムの選定，契約

SaaS(無償)，国内法適用，既存アカウント管理システムの改修で対応可能

→ 移行先：**Microsoft Office365** (Education E1)

新旧のメールシステムの併存期間を有する移行スケジュール

→ 新サービス：2015年12月開始
移行サービス：2015年12月～2016年3月末(並行稼働四か月)
旧サービス：2016年3月末終了

SaaS→SaaSへの移行
-「契約が変わる」だけでは済まない-

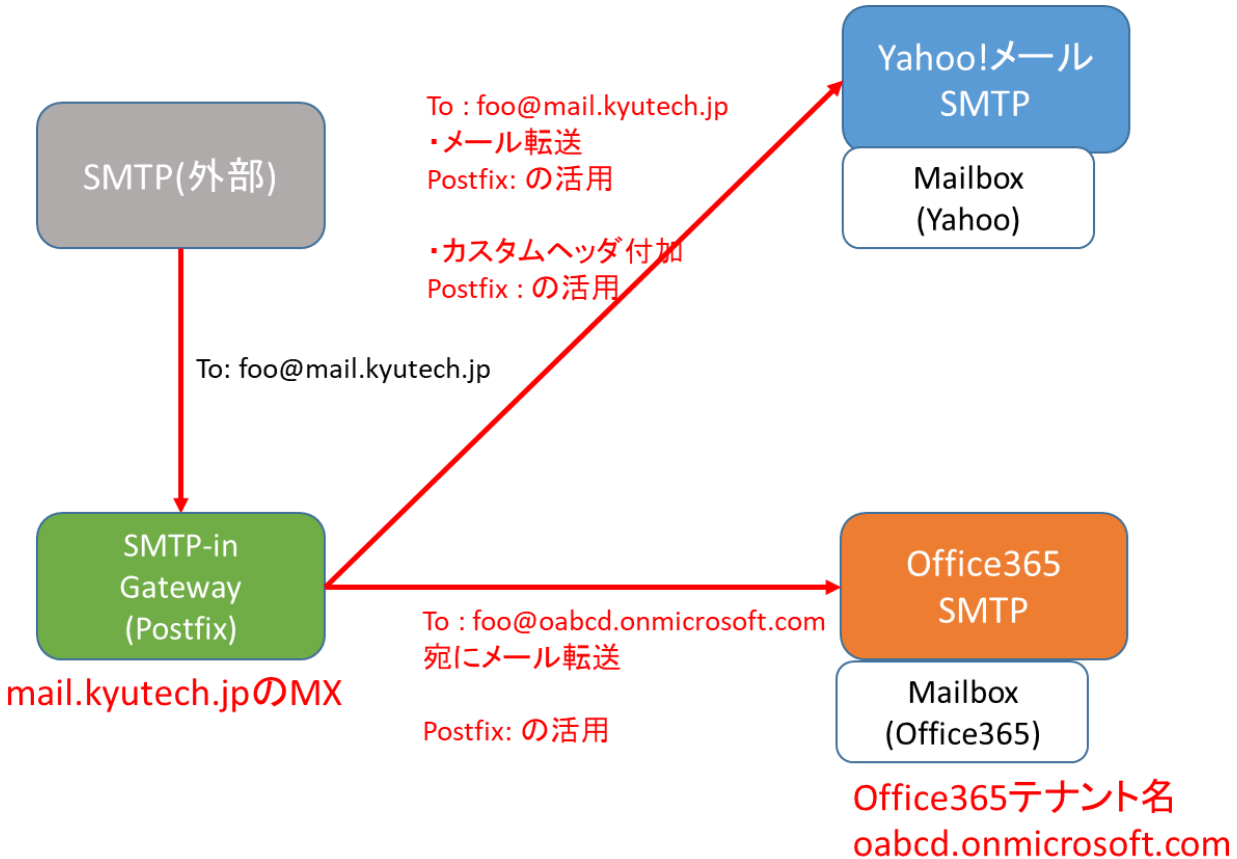
移行期間中のメール受信：Y!，Office365双方に振る

Y!メールの仕様上，中継サーバ設置が最適

メール送信：Office365のみの利用を(強く)推奨

移行サービス：2015年12月～2016年3月末(並行稼働四か月)

移行システムの構築に一苦労(メールだけで本当に良かったです)



SaaS→SaaSへの移行
-「契約が変わる」だけでは済まない-

管理システムの改修

365の制御

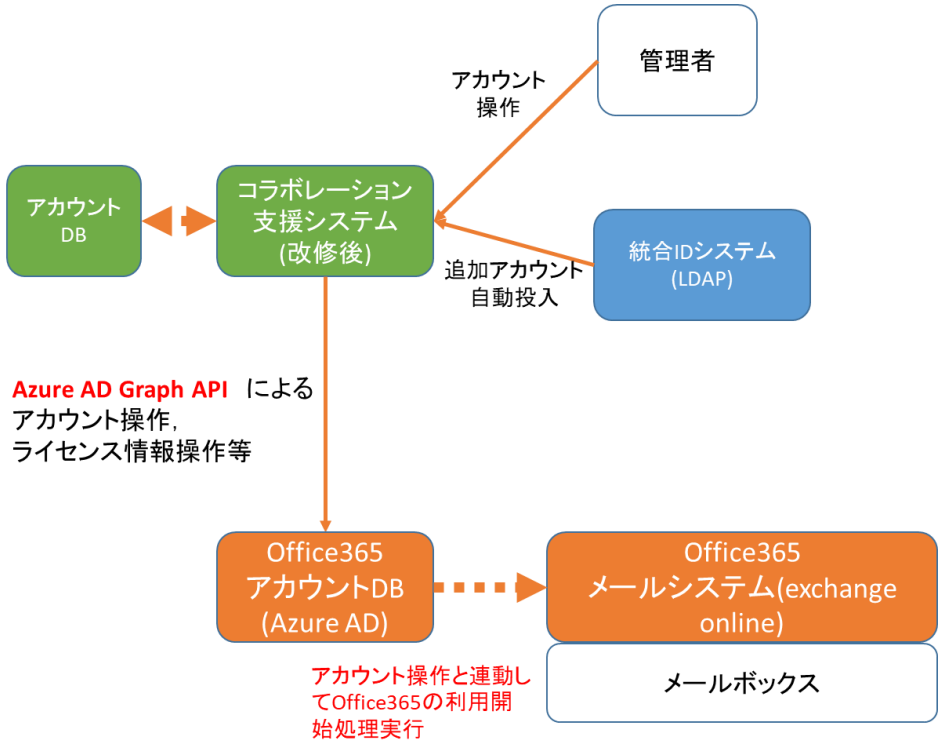
Azure AD Graph APIを活用

アカウント操作(Azure AD Connectは使わない)

ライセンス処理(PowerShellは使わない)

Graph API非対応操作は，PowerShellの定期実行で対応

学内のアカウント管理DB等は設計変更せず



Y!運用時(REST API)の管理

システムの一部改修で対応可能

Office365がやってきた
- 利用者視点，管理者視点双方で利便性抜群-

2015年12月：移行期間としてサービス開始

2016年4月：Office365に一本化，完全移行

SaaS : Microsoft Office365 Education E1

foo@mail.kyutech.jp アカウント (アカウント管理システム → Azure AD連携)

Webインタフェース，**Exchange**，SMTP，POP，IMAP

メールボックス容量 50GB

卒業後は Exchange Onlineのみ利用可能なライセンス処理を実施

アカウント管理システム：学内システム

学内の統合ID管理システムと連携

ID生成を検知し，メールアカウント作成 (Azure AD Graph API操作)

パスワード管理，ライセンス管理

Office365がやってきた
- 初期設定が本学の利用形態に対して緩い -

- 本学のO365テナントの利用者は，卒業生，離退職者，在学生，教職員
- メールアカウントの命名規則が決まっていて，管理者が作成

以下の振舞は望ましくない

- アカウント情報(の一部が類推できるものも含め)が抜ける
- 他人のアカウント情報が検索できる(教職員→学生程度であれば良いのですが…)
- 自由にアカウントが作れる

一般ユーザにそんな権限は付いていないはず
(2015年当時のお話です)

Office365がやってきた
- 初期設定が本学の利用形態に対して緩い -

導入当初のマイナートラブル，想定外の挙動

移行サービス中，メール転送がEOP対象(ブラックリスト扱い) (2015.12)

Exchange Onlineメールフロー設定変更

移行サービス中，365 → Y!メールボックスに配送されない(2015.12)

365のデフォルト動作では，同一ドメインユーザへの配送はMX参照しない仕様

Exchange Onlineメールフロー設定変更

一般ユーザがグループを定義可能(=グループメールが作られてしまう) (2015.12)

PowerShellを用いてグループポリシー変更

一般ユーザがExchange onlineにPowerShell接続可能 (2015.12)

ユーザ作成後，PowerShellを用いてユーザの権限変更(都度)

Office365がやってきた
- 初期設定が本学の利用形態に対して緩い -

導入当初のマイナートラブル，想定外の挙動

グローバルアドレス帳に全ユーザ情報が掲載 & アクセス可能 (2016.01)

ユーザ作成後，PowerShellによりアドレス帳への掲載フラグを落とす(都度)

一般ユーザがAzure ADにPowerShell接続し，他ユーザの情報を(一部)参照可能 (2016.01)

PowerShellを用いてMSOLのポリシー変更

低優先メール機能がenableになり，メールを見落とすとの指摘 (2016.04)

Exchange Onlineの設定変更により，低優先メールを無視するカスタムヘッダ付与

まれに，初期ドメインを持つ(onmicrosoft.com)ユーザが作成される(1/2000程度) (2016.04)

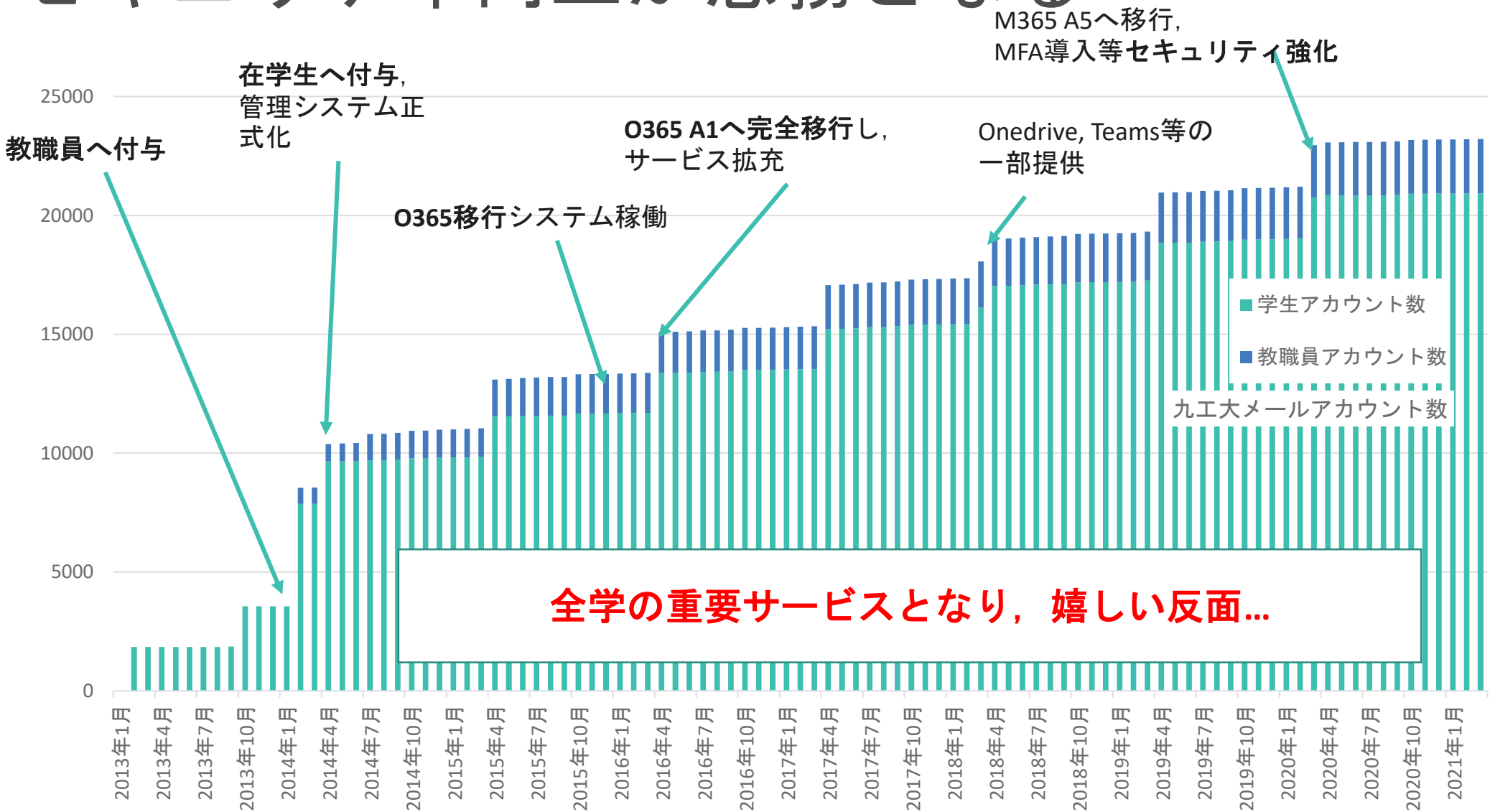
定期的にドメインの異なるユーザを監視し，PowerShellを用いて変更

項番 (下段： 導入期)	振る舞い	対応策	設定内容・実行周期および対応するPowerShellスクリプト
1-1 (一期)	一般ユーザが グループ定義可能 (メールアドレス 重複の可能性が出る)	グループポリシー 変更 (グループ定義不可)	実行周期：一度(設定後永続的に反映) Set-OwaMailboxPolicy -Identity "OwaMailboxPolicy-Default" -GroupCreationEnabled $False
1-2 (一期)	一般ユーザが Exchange onlineに PowerShell接続可能	ユーザ作成後にユーザ の権限変更	実行周期：新規ユーザ作成を周期的に検知(本学では30分周期) Set-User user@contoso.com -RemotePowerShellEnabled $False
1-3 (一期)	グローバルアドレス 帳が利用可能	ユーザ作成後にアドレ ス帳への反映を取り消 す	実行周期：新規ユーザ作成を周期的に検知(本学では30分周期) Set-Mailbox -Identity user@contoso.com -HiddenFromAddressListsEnabled $True
1-4 (一期)	一般ユーザが Azure ADにPowerShell 接続可能 (他ユーザの情報を 閲覧可能)	グループポリシー 変更 (他ユーザの情報閲覧不 可)	実行周期：一度(設定後永続的に反映) Set-MsolCompanySettings -UsersPermissionToReadOtherUsersEnabled $False
1-5 (一期)	低優先メール機能が 任意のタイミングで 有効となる	Exchange Onlineの設定変 更 (低優先メールを無視す るカスタムヘッダ付加)	Exchange Onlineのメールフロー，トランスポートルールを新規追加 条件：全メッセージ 処理：メールヘッダに「X-MS-Exchange-Organization-BypassClutter : true」を付加 となるトランスポートルールを作成
1-6 (一期)	まれに，第二ドメイ ン名 (xxx.onmicrosoft.com) としてユーザが作成 される	第二ドメインが付され たユーザを定期的に検 出，変更	実行周期：新規ユーザ作成を周期的に検知(本学では30分周期) $t = $u.UserPrincipalName -split "@" $newupn = $t[0] + "@mail.kyutech.jp" Set-MsolUserPrincipalName -UserPrincipalName $u.UserPrincipalName -NewUserPrincipalName $newupn

項番 (下段： 導入期)	振る舞い	対応策	設定内容・実行周期および対応するPowerShellスクリプト
1-1 (一期)	一般ユーザが グループ定義可能 (メールアドレス 重複の可能性が出る)	グループポリシー 変更 (グループ定義不可)	実行周期：一度(設定後永続的に反映) Set-OwaMailboxPolicy -Identity "OwaMailboxPolicy-Default" -GroupCreationEnabled $False
1-2 (一期)	一般ユーザが Exchange onlineに PowerShell接続	ユーザ作成後にユーザ の権限変更	実行周期：新規ユーザ作成を周期的に検知(本学では30分周期)
1-3 (一期)	グローバルア 帳が利用可能		
1-4 (一期)	一般ユーザが Azure ADにPow 接続可能 (他ユーザの情報を 閲覧可能)	(他ユーザの情報閲覧不 可)	Set-MsolCompanySettings -UsersPermissionToReadOtherUsersEnabled $False
1-5 (一期)	低優先メール機能が 任意のタイミングで 有効となる	Exchange Onlineの設定変 更 (低優先メールを無視す るカスタムヘッダ付加)	Exchange Onlineのメールフロー，トランスポートルールを新規追加 条件：全メッセージ 処理：メールヘッダに「X-MS-Exchange-Organization-BypassClutter : true」を付加 となるトランスポートルールを作成
1-6 (一期)	まれに，第二ドメイ ン名 (xxx.onmicrosoft.com) としてユーザが作成 される	第二ドメインが付され たユーザを定期的に検 出，変更	実行周期：新規ユーザ作成を周期的に検知(本学では30分周期) $t = $u.UserPrincipalName -split "@" $newupn = $t[0] + "@mail.kyutech.jp" Set-MsolUserPrincipalName -UserPrincipalName $u.UserPrincipalName -NewUserPrincipalName $newupn

MSのサポートに問い合わせ，数日内に具体的な回答が提示され改善!
(当時はFastTrackでなく，直接MSに問い合わせていました)

シェアが高いシステムは，狙われる
- セキュリティ向上が急務となる -



シェアが高いシステムは，狙われる
- セキュリティ向上が急務となる -

生涯メールサービスの提供開始 (Yahoo!メール, 2012/3)

全教職員へのアドレス付与(2014/1)

管理システムの正式化(2014/4)

入学時 + 在学生へのアドレス付与 (九工大メールへの改称, 2014/4)

Office365への移行+移行システムの構築 (2015/10)

Microsoft 365 A5への移行 (サービス強化)

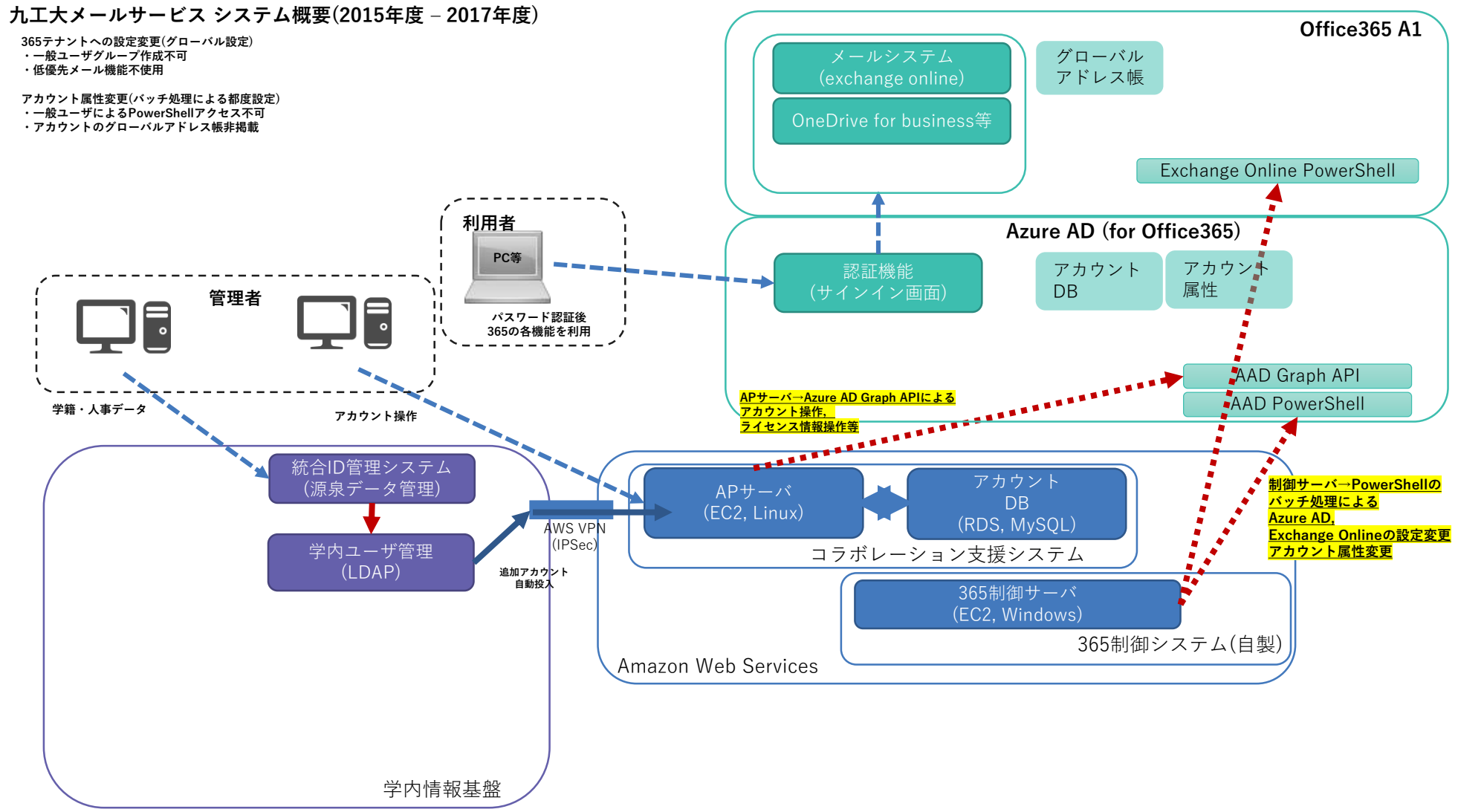
セキュリティ強化(ログ保存方法等の確立，MFA導入)

2016年度以降,

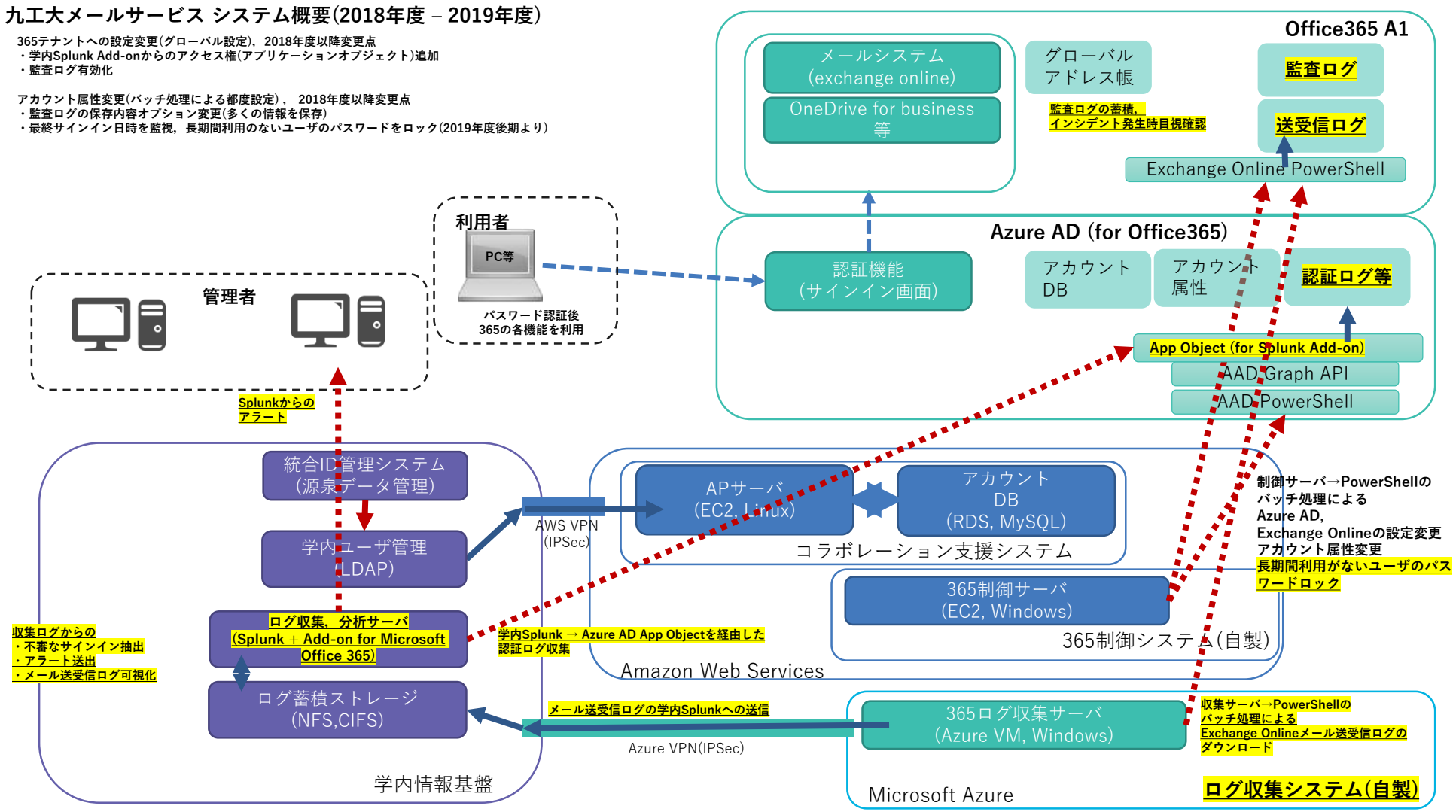
- **アカウントの詐取(と思われる)が発生**
- **レガシー認証時代**
- **ID / PASS認証のみ**
- **E1ライセンスではアラートが上がらない**
- **ログ(特にmaillog)の取得が難しい**

等の問題が顕在化

E1ライセンスで頑張ったセキュリティ向上
- ログ収集，放置アカウント(卒業生)のロック等 -



E1ライセンスで頑張ったセキュリティ向上
- ログ収集，放置アカウント(卒業生)のロック等 -

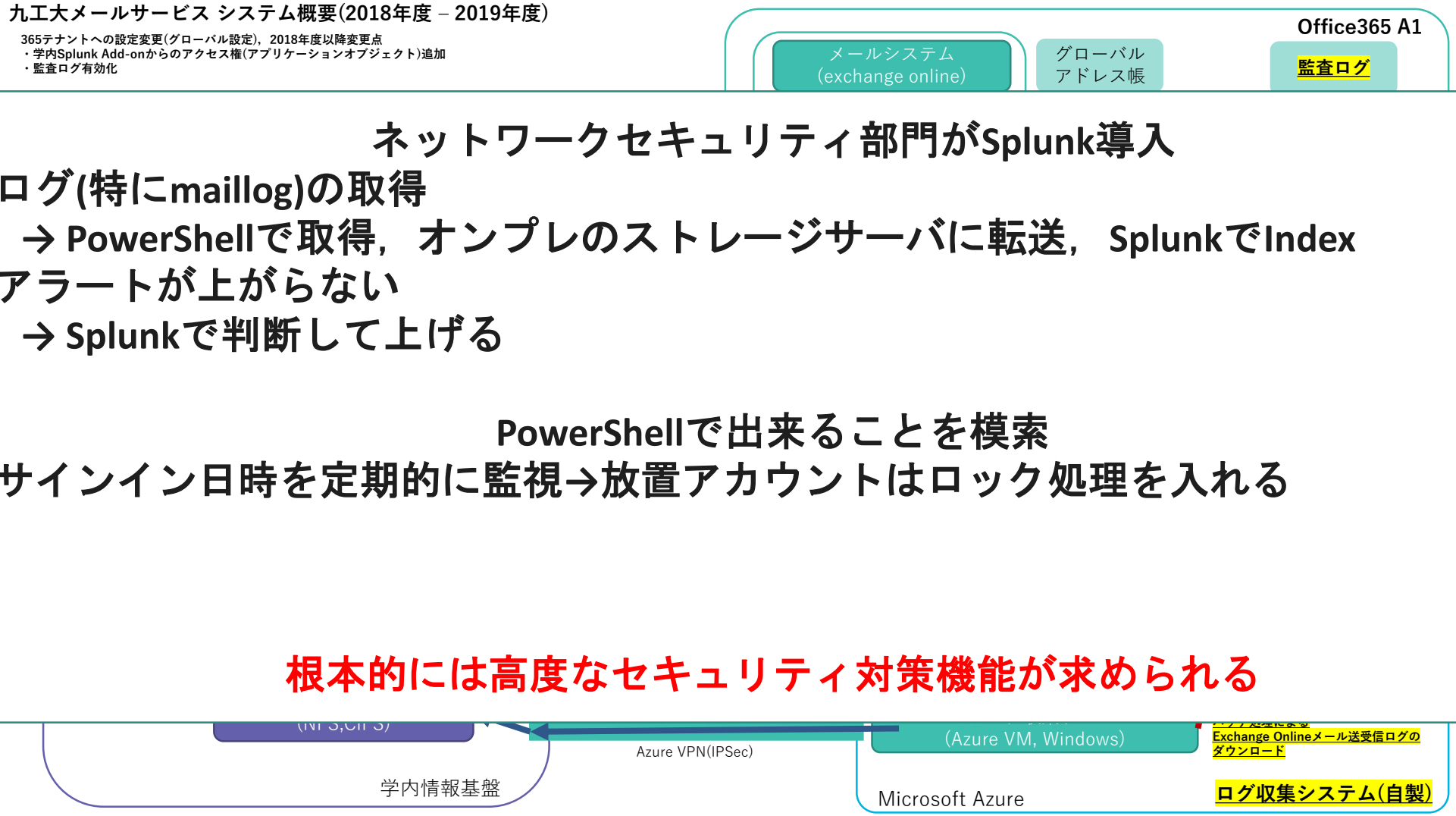


項番 (下段： 導入期)	振る舞い	対応策	設定内容・実行周期および対応するPowerShellスクリプト
2-1 (二期)	監査ログを詳細化する	ユーザ作成後にメールボックス監査設定変更	実行周期：新規ユーザ作成を周期的に検知(本学では30分周期) # サインイン，メールの作成，削除等もログへの保存対象とする Set-Mailbox -Identity user@contoso.com -AuditEnabled $true -AuditDelegate @{add="FolderBind,Move,MoveToDeletedItems,SendOnBehalf"} -AuditOwner @{add="Create,HardDelete,SoftDelete,Update,MailboxLogin,Move,MoveToDeletedItems"}
2-2 (二期)	一定期間サインインがない場合， パスワードをランダム化する	・全てのAzure AD登録ユーザをスキャン ・最終サインイン日時から一定期間経過したユーザのパスワードをランダム化	実行周期：タスクスケジューラにて，月に一度実行 Get-Mailbox -ResultSize unlimited | Select-Object -Property PrimarySmtpAddress,WhenCreated foreach($u in $userlist) { $us = Get-MailboxStatistics -Identity $u.PrimarySmtpAddress \| Select-Object -Property LastLogonTime if($us.LastLogonTime -le (Get-Date).AddDays(-90)) { Set-MsolUserPassword -UserPrincipalName $u.PrimarySmtpAddress } }
2-3 (二期)	ユーザ毎のメール送受信ログを取得し， csvファイルとして保存する	・全てのAzure AD登録ユーザをスキャン ・ユーザのメール送信，受信ログを取得 ・csvファイルに保存後ファイルサーバに送信	実行周期：タスクスケジューラにて，日に一度実行 $csvfnd = Get-Date -Format "yyyy-MM-dd-HH-mm-ss" $csvfn = "C:¥maillog¥maillog_$csvfnd.csv“ $csvfn_logserv = “Z:¥maillog¥maillog¥maillog_$csvfnd.csv“ #Z: はCIFSサーバ $userlist = Get-Mailbox -ResultSize unlimited \| Select-Object -Property PrimarySmtpAddress foreach($u in $userlist) { #24時間分のユーザ毎の送信ログ取得，csvに追加 Get-MessageTrace -StartDate (Get-Date).AddDays(-1) -EndDate (Get-Date).AddDays(1) -SenderAddress $u.PrimarySmtpAddress | Export-CSV $csvfn -Append -Encoding UTF8 -NoTypeInformation #24時間分のユーザ毎の受信ログ取得，csvに追加 Get-MessageTrace -StartDate (Get-Date).AddDays(-1) -EndDate (Get-Date).AddDays(1) -RecipientAddress $u.PrimarySmtpAddress | Export-CSV $csvfn -Append -Encoding UTF8 -NoTypeInformation } # CIFSサーバにコピー Copy-Item -Path $csvfn -Destination $csvfn_logserv

E1ライセンスで頑張ったセキュリティ向上
- ログ収集，放置アカウント(卒業生)のロック等 -

メッセージID (一部のみ掲載)	送受信時刻	送信者メールアドレス (一部のみ掲載)	受信者メールアドレス (一部のみ掲載)	件名 (省略)	配信結果	配信サーバ IPアドレス (一部のみ掲載)	クライアント IPアドレス (一部のみ掲載)	メッセージ サイズ	メッセージトレースID (メールヘッダに付加) (一部のみ掲載)	ログ取得時刻
<**********@mail.kyutech.jp>	2020/4/13 8:29	**********@mail.kyutech.jp	**********	**********	Delivered	67.***.***.***	126.***.***.***	16167	a03569ef-**-**-**-******	2020/4/13 8:14
<**********>	2020/4/12 23:53	**********	**********@mail.kyutech.jp	**********	Delivered		219.***.***.***	12549	18c25115-**-**-**-******	2020/4/13 8:14
<**********>	2020/4/12 23:22	**********	**********@mail.kyutech.jp	**********	Delivered		167.***.***.***	99684	473856ca-**-**-**-******	2020/4/13 8:14
<**********@OSAPR01MB5076.jpnprd01.prod.outlook.com>	2020/4/13 11:44	**********@mail.kyutech.jp	**********	**********	Delivered	17.***.***.***	2400:****:****:****:****:****:****:****	15235	4ca75c63-**-**-**-******	2020/4/13 8:14
<**********@mail.kyutech.jp>	2020/4/13 9:14	**********@mail.kyutech.jp	**********@mail.kyutech.jp	**********	Delivered		150.***.***.***	18026	a44669b2--**-**-**-******	2020/4/13 8:14
<**********@mail.kyutech.jp>	2020/4/13 0:50	**********	**********@mail.kyutech.jp	**********	Delivered		150.***.***.***	27178	8b8f2c33-**-**-**-******	2020/4/13 8:14
<**********>	2020/4/13 11:26	**********	**********@mail.kyutech.jp	**********	Delivered		131.***.***.***	17903	822c4711-**-**-**-******	2020/4/13 8:14
<**********>	2020/4/13 5:59	**********	**********@mail.kyutech.jp	**********	Delivered		131.***.***.***	16544	55f3bd4e-**-**-**-******	2020/4/13 8:14
<**********@mail.outlook.com>	2020/4/13 3:03	**********	**********@mail.kyutech.jp	**********	Delivered		131.***.***.***	18152	3985246c-**-**-**-******	2020/4/13 8:14
<**********>	2020/4/13 18:14	**********	**********@mail.kyutech.jp	**********	Delivered		142.***.***.***	56907	53e76f2e-**-**-**-******	2020/4/13 8:14
<**********>	2020/4/13 7:12	**********	**********@mail.kyutech.jp	**********	Delivered		183.***.***.***	1142799	2c1f37fb-**-**-**-******	2020/4/13 8:14
<**********>	2020/4/13 10:02	**********	**********@mail.kyutech.jp	**********	Delivered		219.***.***.***	18764	22611dfd-**-**-**-******	2020/4/13 8:14
<**********>	2020/4/13 8:41	**********	**********@mail.kyutech.jp	**********	Delivered		203.***.***.***	19111	2ca4bec2-**-**-**-******	2020/4/13 8:14
<**********>	2020/4/13 7:38	**********	**********@mail.kyutech.jp	**********	Delivered		168.***.***.***	276782	410c04d8-**-**-**-******	2020/4/13 8:14
<**********>	2020/4/13 7:07	**********	**********@mail.kyutech.jp	**********	Delivered		150.***.***.***	15705	052dee09-**-**-**-******	2020/4/13 8:14
<**********>	2020/4/13 5:58	**********	**********@mail.kyutech.jp	**********	Delivered		210.***.***.***	25372	ece7d201-**-**-**-******	2020/4/13 8:14
<**********>	2020/4/13 5:34	**********	**********@mail.kyutech.jp	**********	Delivered		210.***.***.***	25377	b82e4f83-**-**-**-******	2020/4/13 8:14

E1ライセンスで頑張ったセキュリティ向上
- ログ収集，放置アカウント(卒業生)のロック等 -



ネットワークセキュリティ部門がSplunk導入

- **ログ(特にmaillog)の取得**
  → PowerShellで取得，オンプレのストレージサーバに転送， SplunkでIndex
- **アラートが上がらない**
  → Splunkで判断して上げる

PowerShellで出来ることを模索

- **サインイン日時を定期的に監視→放置アカウントはロック処理を入れる**

根本的には高度なセキュリティ対策機能が求められる

Microsoft 365 / A5 導入

2019年度

Office365のセキュリティ向上の必要性に加え，他のソフトウェアライセンス包括契約の見直しのタイミングを迎える

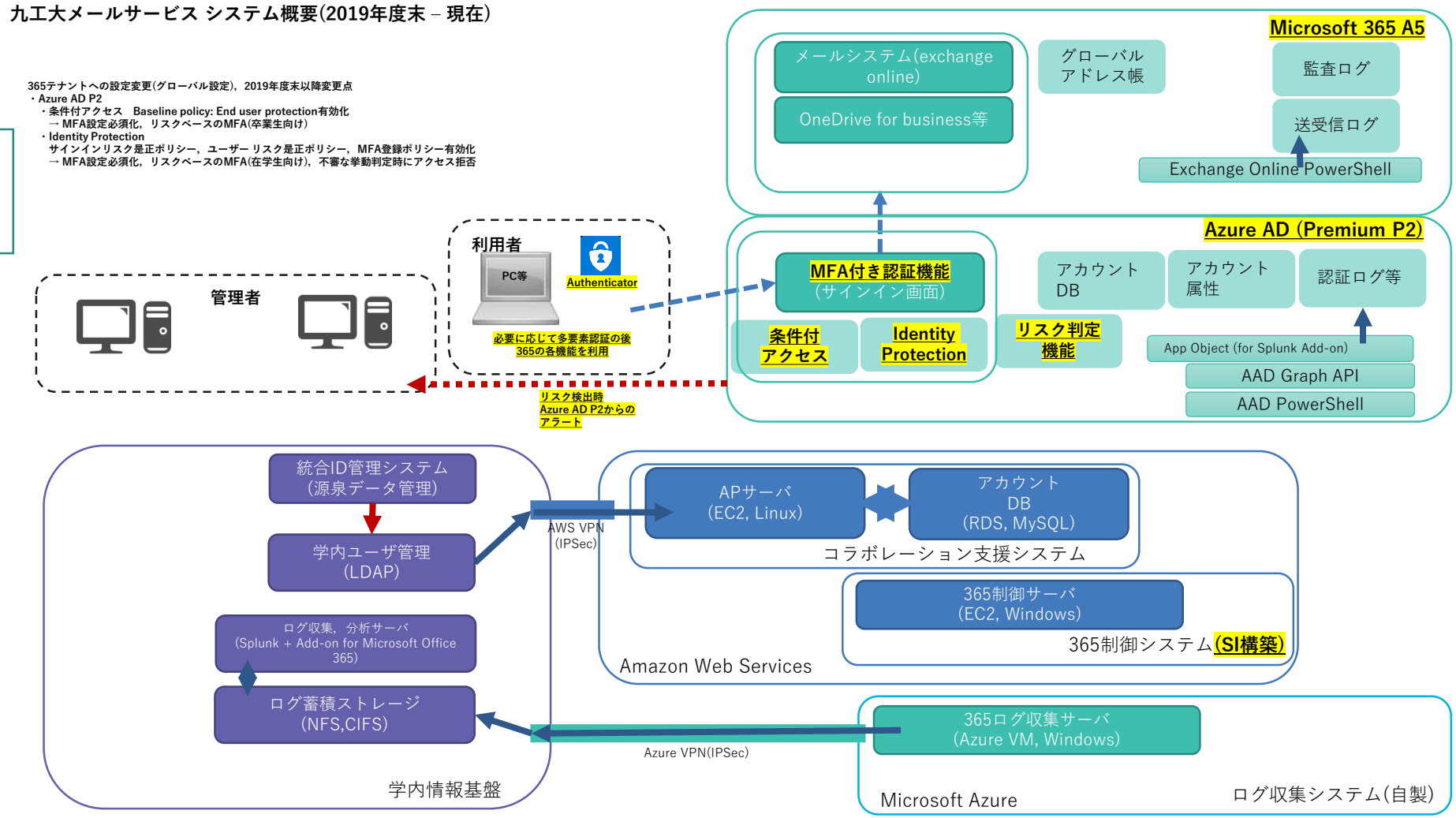
- キャンパスアグリーメント(Microsoft EES)の取り扱いが変更
  - OfficeやWindowsを調達していたものが，M365契約前提に
- AntiVirus関連の契約見直し
  - Defender ATP (Win / Mac) の方が良いのでは
- M365の上位ライセンスの持つ機能群
  - Azure AD Premiumを使いたい
  - Intuneを使いたい
  - 将来的にはPBXをTeams電話に移行したい

Microsoft 365 E5導入が決まる
(教職員数が少ないので可能だったのかもしれません)

Microsoft 365 / A5 導入
- 二段階認証の導入，何種類もある実現方法 -

- A5と言えば，Azure AD P2!　監査ログ等が詳細に確認できる!　振る舞い検知付のMFA！

まずはMFA導入を進めることに



Microsoft 365 / A5 導入
- 二段階認証の導入，何種類もある実現方法 -

365 (Azure AD)における，サインインセキュリティ強化の実現方法(本学における比較)

機能名， 本学における利用	ユーザ毎のMFA 卒業生，離退職者向けに有効化	条件付きアクセス(ベースライン ポリシー) End user protection有効化を想定していたが，2020年3月以降機能終息(当時のロードマップ)	セキュリティ既定値 2020年度中に有効化 (当時のロードマップ)	条件付きアクセス	Identity Protection 管理アカウント，在学生 / 在職者向けに有効化
必要な製品 ライセンス (Academic)	365 A1以上	365 A1以上	365 A1以上	365 A3 (Azure AD Premium P1)以上	365 A5 (Azure AD Premium P2)以上
機能概要	指定したアカウントに対して多要素認証を必須とする	4種類のセキュリティ強化のプリセットが適用可能(プリセット内容は編集不可能) ・End user protection ：一般ユーザに対してMFA設定必須，リスクの高いサインインと判定された場合，MFAが必要となる ・Block legacy authentication : MFA非対応アプリケーションを利用不可とする ・Require MFA for admins, Require MFA for Service Management : 管理者向けのMFA設定必須	条件付アクセス(ベースライン)の全てを一括適用	利用される状況(アカウント，ネットワーク，機材，リスクレベル等)のリスク判定条件を手動で定義し，アクセスのブロック，MFAの必要性等を判断する	利用される状況のリスクが自律的に判定され，アクセスのブロック，MFAの必要性等を判断する 3種類のポリシーが適用可能 ・MFA登録ポリシー : MFA設定を必須とする ・サインインリスクポリシー : サインインの頻度や場所を判定し，MFAを要求する ・ユーザリスク是正ポリシー : 不正アクセスを判定し，サインインをブロックする
設定対象	アカウント単位	テナント内の全アカウント	テナント内の全アカウント	特定のアカウント，グループ，全アカウント等設定可能	特定のアカウント，グループ，全アカウント等設定可能

Microsoft 365 / A5 導入
- 二段階認証の導入，何種類もある実現方法 -

365 (Azure AD)における，サインインセキュリティ強化の実現方法(本学における比較)

機能名， 本学における利用	ユーザ毎のMFA 卒業生，離退職者向けに有効化	条件付きアクセス(ベースライン ポリシー) End user protection有効化を想定していたが，2020年3月以降機能終息(当時のロードマップ)	セキュリティ既定値 2020年度中に有効化 (当時のロードマップ)	条件付きアクセス	Identity Protection 管理アカウント，在学生 / 在職者向けに有効化
必要な製品 ライセンス (Academic)	365 A1以上	365 A1以上	365 A1以上	365 A3 (Azure AD Premium P1)以上	365 A5 (Azure AD Premium P2)以上
MFA(Authenticator等による多要素認証)の登録タイミング	設定以降の365へのサインイン時に登録が必要	(End user protection) 初回サインイン後二週間以内に登録が必要 (二週間以内はMFAなしでサインイン可能)	初回サインイン後二週間以内に登録が必要 (二週間以内はMFAなしでサインイン可能)	初回サインイン後二週間以内に登録が必要 (二週間以内はMFAなしでサインイン可能)	(MFA登録ポリシー適用) 初回サインイン後二週間以内に登録が必要 (二週間以内はMFAなしでサインイン可能)
MFAが必要となるタイミング	サインイン時に原則必要 (「信頼済みIP」適用によりサブネット単位で除外可能)	(End user protection) リスクの高いサインインと判定された場合必要	リスクの高いサインインと判定された場合必要	リスクの高いサインインと判定された場合必要	(サインインリスクポリシー適用) リスクの高いサインインと判定された場合必要
レガシー認証 (MFA非対応アプリケーション専用のパスワード生成)	対応	対応 (Block legacy authenticationを適用しない場合)	不可能となる	対応	対応
不正アクセスのブロック	なし	なし	なし	なし	(ユーザー リスク是正ポリシー適用) リスクレベルに応じて自動的にサインインのブロック可能

Microsoft 365 / A5 導入
- 二段階認証の導入，何種類もある実現方法 -

365 (Azure AD)における，サインインセキュリティ強化の実現方法(本学における比較)

機能名， 本学における利用	ユーザ毎のMFA 卒業生，離退職者向けに有効化	条件付きアクセス(ベースラインポリシー) End user protection有効化を想定していたが，2020年3月以降機能が終息	セキュリティ既定値 2020年度中に有効化	条件付きアクセス	Identity Protection 管理アカウント，在学生 / 在職者向けに有効化
管理者へのアラート，ログ	アラート：なし ログ：リスク発生に関する概要記録	アラート：なし ログ：リスク発生に関する概要記録	アラート：なし ログ：リスク発生に関する概要記録	アラート：アカウントへのリスク発生時に発報 ログ：リスク発生に関する概要記録	アラート，ログ： リスクレベル等を含めた詳細情報の発報，記録
備考，本学における運用との親和性	・有効化設定がアカウント単位であるため，適用範囲が柔軟である反面，全アカウントへの展開が煩雑となる ・リスクベースではないため，サインインの度に多要素認証が必要となる → 全アカウント適用が煩雑であり，本学の利用形態には不十分である	・推奨されるセキュリティ要件に対応するプリセットが用意されており，365ライセンスを有していれば利用可能 ・4種類を個別に有効化可能 ・プリセット内容の編集は不可能 → 一括したMFA必須化可能，レガシー認証が残せるため，本学には適していたが，2019年末から利用が非推奨．設定不可となる	・ベースラインポリシーに相当する設定が一括適用される → レガシー認証非対応となるため，IMAP / SMTPが不可能となり利用者への影響大	・ベースラインポリシーと異なり，リスク判定条件を構築可能 ・設定対象のアカウントを柔軟に設定可能 ・後述のIdentity Protectionを組み合わせると，自律的なリスク判定条件を組み込むことも可能 → 本学ではIdentity Protectionが利用できるため，適用しない	・リスク判定と対処方法が自律的に決定されるため，運用コストが低減できる ・リスクレベルに応じてMFAが要求されるため，利用者の負担が低い ・不正アクセスの判定，ブロックが可能 → 本学では，在学生 / 在職者向けの運用に適している

Microsoft 365 / A5 導入
- 二段階認証の導入，何種類もある実現方法 -

- Identity Protection (MFAポリシー)による，MFA導入
  - MFAポリシーにより，既存ユーザを含め，サインイン時にMFA登録要求がかかる
  - ふるまい検知により，リスク高の状況のみMFA要求される

大変良い！・・・のですが・・・

  - MFA(モダン認証)になるが，レガシー認証はまだ止まっていない
    - IMAP / POPアクセス時はMFAにならない(2022/10に解消のロードマップ)
    - 条件付アクセスで止めると，既存ユーザへのアナウンスが問題に…
  - あまりリスク高判定にならない(喜ばしい反面，MFA設定したか忘れるほど上がらない)
  - MFAデバイスを飛ばした利用者への対応
    - 卒業生が機種変更でAutenticator飛ばした際．どうやって本人確認して再設定させるか?

Microsoft 365 / A5 導入
- 利用形態の変化，需要が増加 -

- M365 E5 導入以前より，メール以外の機能に関する問い合わせはあった
  - Onedriveは使えないのか?
  - (Skype for Business時代から) Teams会議は使えないのか?
  - Teams は使えないのか?

  → 本学のセキュリティポリシー上，クラウドサービスの利用は承認制．したがって当初は「使えない」

  → 個別に承認 (機微情報の取り扱い禁止の条件等はあり)

- 現在利用可能なサービス(公式に)
  - Exchange Online
  - Onedrive for Business
  - Teams会議

- 実験ベースで，Teams，Forms，PowerAutomate (Flow)を検証中
  - Teamsは2022年度より正式化予定

Teamsの全学展開
- 自由度が高く，本学に適した設定の模索 -

- Teams (Teams会議ではない方) はM365の機能群を組み合わせたようなサービス
  - Teamを作ると，裏側で365グループが作成される
    - 本学では，任意の名前でグループが作れないよう，一般ユーザのグループ作成を禁止
  - チームにメンバーを追加する際，検索が走る (招待コードを使う場合は別)
    - 本学では，アドレス帳の検索(グローバルアドレス帳への掲載をしない)を制限

現在の設定値ではチームが作れない & 制限を緩めると好き勝手にチームが作られる
いきなり本学の想定から外れる

Teamsの全学展開
- 自由度が高く，本学に適した設定の模索 -

- Teams (Teams会議ではない方) はM365の機能群を組み合わせたようなサービス
  - Teamを作ると，裏側で365グループが作成される
    - 本学では，任意の名前でグループが作れないよう，一般ユーザのグループ作成を禁止

・作成時指定したグループ名に，prefixが付くように設定 (自力で発見…)
testteam -> grp_testteam となる
・グループの作成権限は，基本的にDrop
・グループが作れるsecurity groupを定義し，運用者のアカウントを追加

  - チームにメンバーを追加する際，検索が走る (招待コードを使う場合は別)
    - 本学では，アドレス帳の検索(グローバルアドレス帳への掲載をしない)を制限

アドレス帳ポリシーの定義 (FastTrackより教示)
・sg A : 教職員，sg B : 教職員以外とする場合，以下のポリシーを作成しアカウントに割り付け

・Policy A : sg B を検索可能
・Policy B : すべて検索不可

Teamsの全学展開
- 自由度が高く，本学に適した設定の模索 -

- Teams (Teams会議ではない方) はM365の機能群を組み合わせたようなサービス
  - チャネルに貼ったファイルのアクセス権 (Sharepoint上)
    - 標準では外部公開可能
  - チャット(チャネルではない)に貼ったファイルのアクセス権(Sharepoint上)
    - 共有可能 & 共有設定の初期値が，全体公開

アクセス権，共有設定を厳しくする (FastTrackより教示)

・デフォルトの公開設定をメンバーのみに限定化(チャネルは可能)
・チャットに貼ったファイルのアクセス権を外部共有にする際，共有コード設定を既定値に
・外部公開されたファイルの定期的監査 (csvを抜くしかない模様…)

  - その他
    - 作成後放置されたチームの棚卸問題
    - チャネルへの3rdパーティ製アプリケーションが貼れる(ように見える)
    - 検証するごとにいろいろ出てくる

Teamsは，模索段階です

DX推進ツールとしてのM365
- ExchangeやTeamsだけではない-

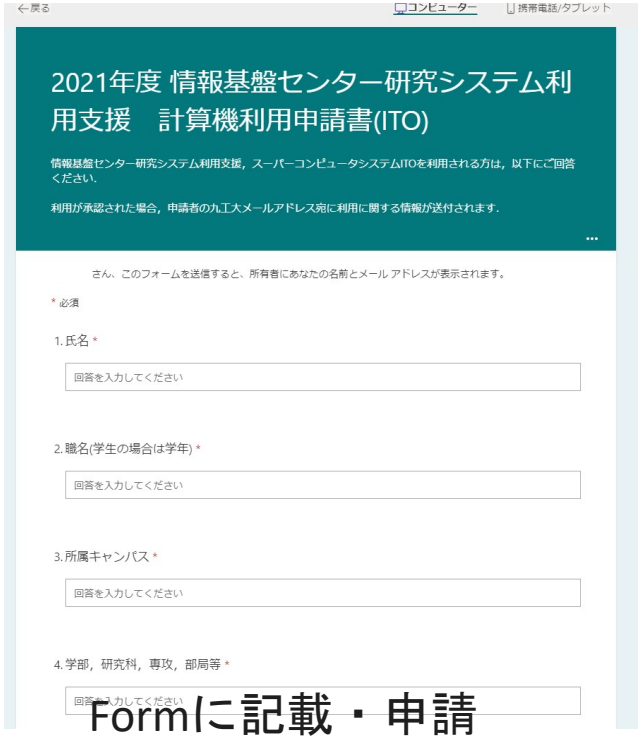
ー例：ワークフローのシステム化・Webインタフェース化ツールとして，**Microsoft 365の機能群を活用**

利用申請受付：Forms

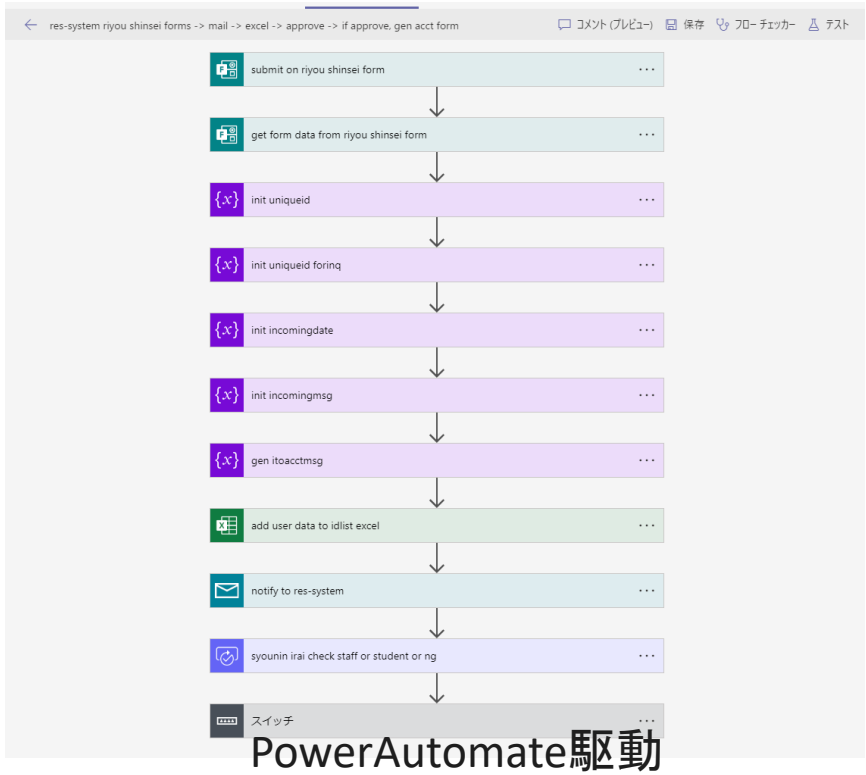
利用申請，承認処理，アカウント通知作成，ワークフロー遷移：PowerAutomate

台帳管理：Excel Online (Sharepoint)

機能の集約：Teams

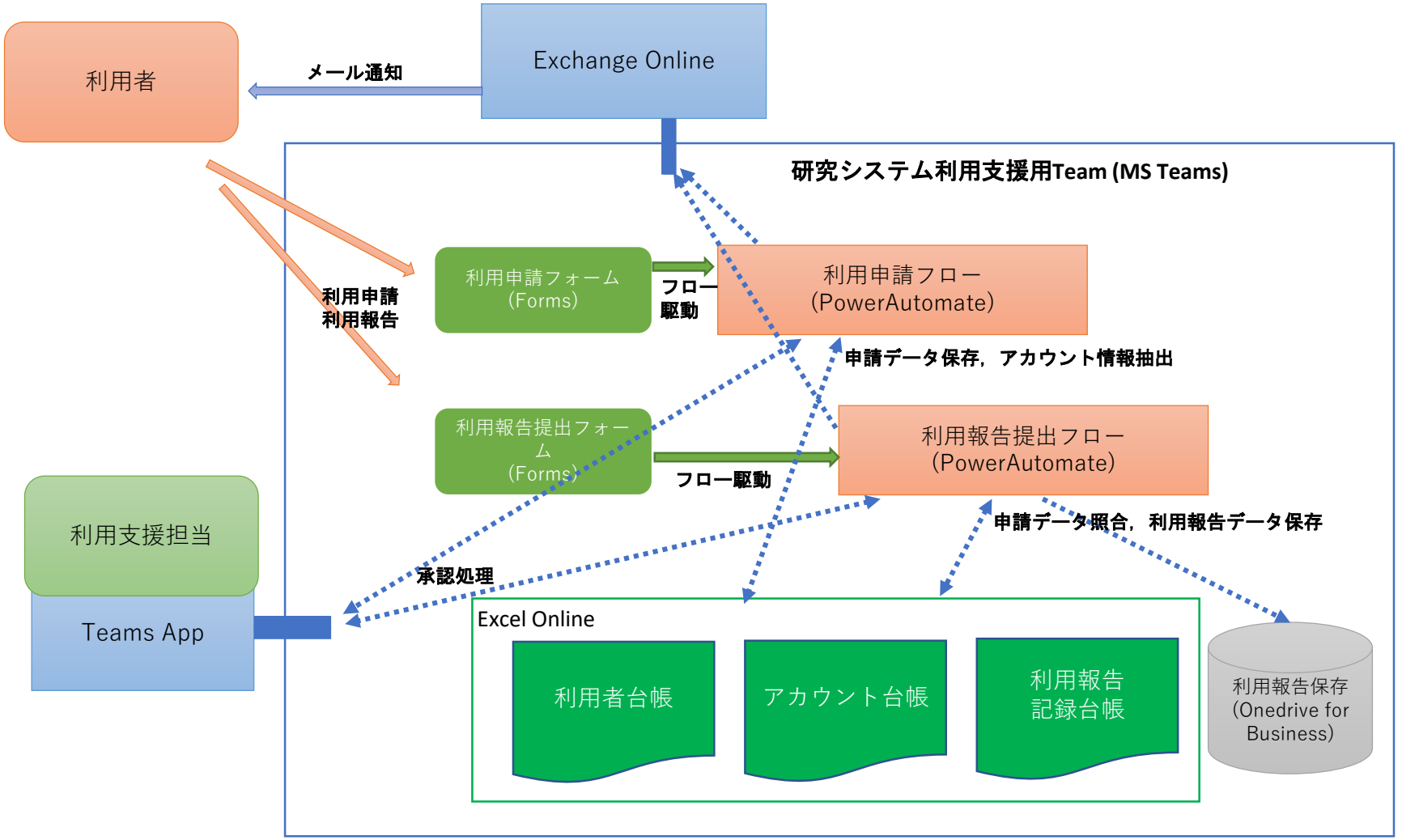


Formに記載・申請



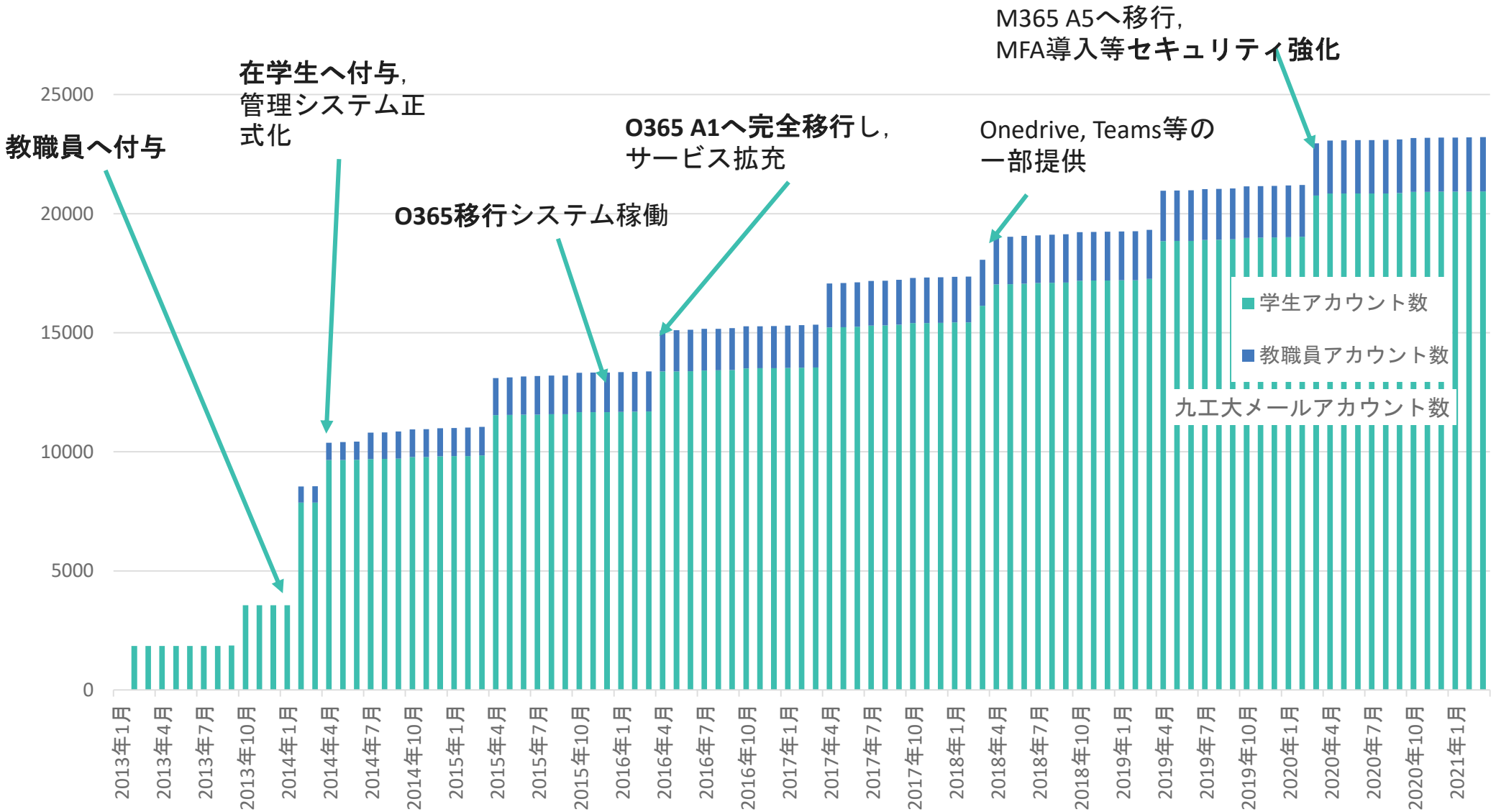
PowerAutomate駆動

DX推進ツールとしてのM365
- ExchangeやTeamsだけではない-

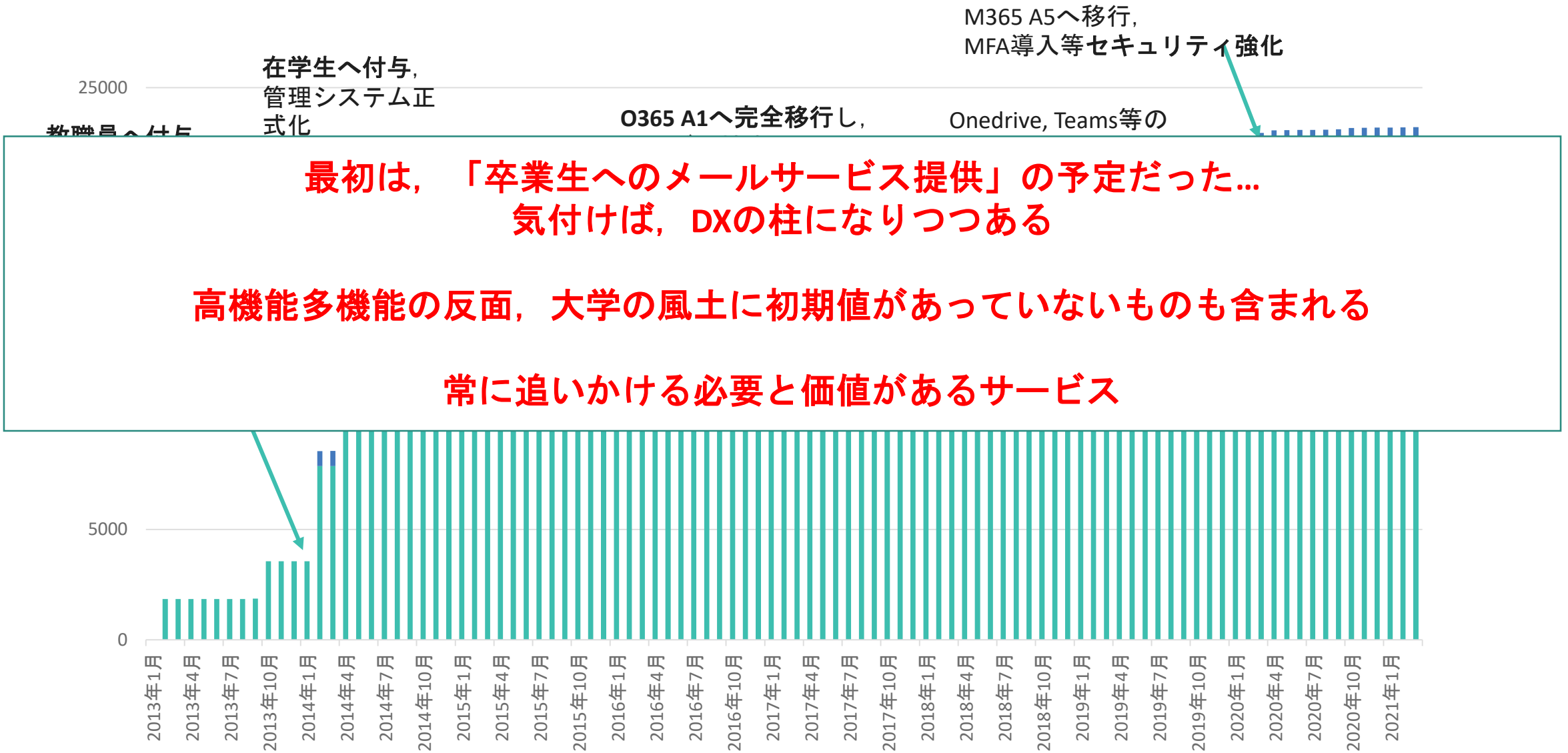


まとめに代えて

最初は，「卒業生へのメールサービス提供」の予定だった…



まとめに代えて



最初は，「卒業生へのメールサービス提供」の予定だった…
気付けば，DXの柱になりつつある

高機能多機能の反面，大学の風土に初期値があっていないものも含まれる

常に追いかける必要と価値があるサービス