原著論文

学術情報処理研究 No.24
JACN 2020年
DOI:10.24669/jacn.24.1_104

Office365 を用いたメールサービスに対するセキュリティ向上対策 -ログ監視，認証基盤の強化-

Security improvement measures for Office365 based mail service -Reinforcement of log monitoring and authentication procedure-

林 豊洋 †, 福田 豊 †, 佐藤 彰洋 †, 大橋 健 †

Toyohiro Hayashi†, Yutaka Fukuda†, Akihiro Satoh†, Takeshi Ohashi†

九州工業大学情報基盤センター †

Information Science and Technology Center, Kyushu Institute of Technology†

toyohiro@isc.kyutech.ac.jp, fukuda@isc.kyutech.ac.jp, satoh@isc.kyutech.ac.jp, ohashi@isc.kyutech.ac.jp†

概要

九州工業大学では 2012 年度より，卒業後も継続して利用可能な全学メールサービスの提供を開始した．メールサービスの稼働基盤には，2015 年度より Microsoft 社の SaaS である Office365 および Microsoft365(以降 365 とも称する) を活用している．本サービスには，2020 年 7 月現在で約 21,800 アカウントが存在し，在学生・在職者に加え本学の卒業生が含まれている．このような多様な利用者層が，電子メールに加えネットワークストレージやグループウェア機能を利用しているため，不正アクセスによるアカウント詐取の対象になっていた．

本学では，365 に対するセキュリティ向上対策として，ログ監視体制の強化と認証基盤の強化を検討・運用を行っている．具体的には，365 へのサインイン情報，メール送受信ログ等を学内のログ収集基盤へ集約する手法を確立した．また，サインイン時の認証強化については，365 が有する多数の実現手法の中から，実現容易性やライセンスの観点から比較検討を行い，利用者層に応じた手法を採用した．本稿ではこれらの詳細について報告する．

キーワード　メールサービス，Office365，ログ監視，多要素認証

1　はじめに

九州工業大学では 2012 年度より，卒業後も継続して利用可能な全学メールサービスの提供を開始した．提供当初より，サービスの稼働には運用コストやサービスの充実度の観点より，学外の SaaS 基盤を用いている．2015 年度からは Microsoft Office365 A1 を基盤として採用し，2019 年度末に Microsoft365 A5 へ機能レベルを拡張した．2020 年 7 月現在，在学生，在職者，卒業生を合わせ，約 21,800 アカウントが発行されている．

365 は，電子メールに加え，ネットワークストレージやグループウェア機能等を有し，多岐に渡る情報が蓄積されている傾向にあることから，しばしばアカウント詐取やデータ盗難等が報告されている．本学においても，2018 年度よりアカウント詐取の後 SPAM の送信に用いられた状況が認められ，セキュリティ向上対策が急務となった．

本学ではセキュリティ向上対策として，ログ監視体制の強化と認証基盤の強化を実施している．ログ監視体制として，学内に構築したログ収集基盤 (Splunk) と連携し，365 へのサインイン試行ログおよびメール送受信ログの取得・分析・管理者への通知システムを確立した．また，メールボックスの監査ログレベルの引き上げ等を行い，インシデント発生時のログ追跡が可能な体制としている．

認証基盤の強化としては，2019 年度よりサインイン状

況のリスク判定や利用実績の検知に基づくパスワードリセットを導入し，加えて 2020 年 3 月より全てのユーザに対する二段階認証機能の有効化設定を実施した．特に二段階認証の実現方法においては，365 ではその方法が複数存在するため，導入に際しては利便性・安全性・利用可能な機能レベルの観点で比較を行った．

2 九工大メールサービス - 本学における全学メールサービス

2.1 全学メールサービス導入の経緯

本学における全学メールサービスは，「卒業生・退職者とのコミュニケーション手段としての生涯メールサービス開始」を経て，「学内メールシステムにおける在学生向けメールサービスの廃止，生涯メールサービスへの統合」へ至った経緯を持つ．

生涯メールサービスは，本学に限らず，多くの教育機関がその重要性を認識している「卒業生・退職者らとの繋がりを維持する」ための手段の一つである．本学においては，Web インタフェースでのメール送受信が行えること，国内法に準拠した運用体系が採用されること，卒業生向けに付与するライセンス数によらず無償で利用できること等の理由から，学外の SaaS である Yahoo!メール Academic Edition を用いた生涯メールサービスの提供を決定し，2012 年度よりサービスを開始した [1]．その後，2015 年 12 月より Microsoft Office365 にシステムを移行した [2].

その後，サービスの対象者は，卒業生のみ (2012 年度) から教職員の統合 (2013 年度)，在学生・離退職者の統合 (2014 年度) に順次拡大され，現在は名称を「九工大メールサービス」と改め全学メールサービスとして提供している．

2.2 メールサービスのシステム概要 (第一期)

本学におけるメールサービスを運用するシステムの構成は，大きく (i) 利用者や対外ネットワークから見えるメールシステム本体，(ii) メールシステム本体の補助を行う管理システムに大別される．(i) は 365 が相当する．(ii) の管理システムとして，「コラボレーション支援システム」と称するシステム群を構築し運用している．管理システムは，パブリッククラウド (Amazon Web Services, AWS) 上で稼働させ，学内情報基盤との通信については AWS との IPSec セッション (AWS VPN) を確立し安全な通信を可能としている．

365 によるメールサービスを運用した当初のコラボレーション支援システムは，2015 年度から 2017 年度まで運用された (第一期システムと称する)．第一期システムは，以下の機能を有するシステムとして設計した (図-1)).

1. 学籍・人事データとの自動連携および手動操作による利用者情報の管理，蓄積等
2. 利用者情報に対応した 365 上のアカウント・ライセンス操作
3. 利用者機能，管理者機能向け Web インタフェース

ここでは，利用者情報の管理方法に関する 1. および 2. の概要について言及する．

1. **利用者情報の管理，蓄積等**　九工大メールサービスの対象者は，「在学生」「教職員」「卒業生」「離退職者」の各区分に分類され，各利用者の区分に応じた九工大メールアカウント (365 アカウント) が付与される．
   現在では，九工大メールアカウントは入学および入職時に付与され，卒業・退職後も継続して利用可能である．加えて，メールサービスの提供以前の卒業生・退職者においても，本サービスの利用権を有すると定めており，大学に籍が存在しない対象者のアカウント発行も必要となる．
   対象者の分類やアカウントの付与タイミングに対応するため，コラボレーション支援システムでは，「学籍・人事データに連携した利用者情報の作成」「区分変更 (在学 → 卒業等)」「利用者情報の手動作成」機能を有する．
   学籍・人事データは学内の統合 ID 管理システムにより集約管理されており，データの更新に連動し，参照用のユーザ管理 LDAP のレコードが更新される．コラボレーション支援システムでは，定期的にユーザ管理 LDAP のレコードを監視することにより新規ユーザを検出・利用者情報 (ID，メールアドレス，区分に対応した 365 ライセンス情報等から構成) を生成する．
2. **365 上のアカウント・ライセンス操作**　コラボレーション支援システムは，登録された利用者情報に連動し，365 上のアカウントおよびライセンス操作を行う．365 を利用するためのすべての情報は，Microsoft Azure のアカウント管理サービスである Azure AD(PaaS) に格納する必要があり，利用者情報と同期させる必要がある．
   本学では，Azure AD に対して REST (Representational State Transfer，Web API) を用いたデータ管理を可能とする Azure AD Graph API を用いて，「利用

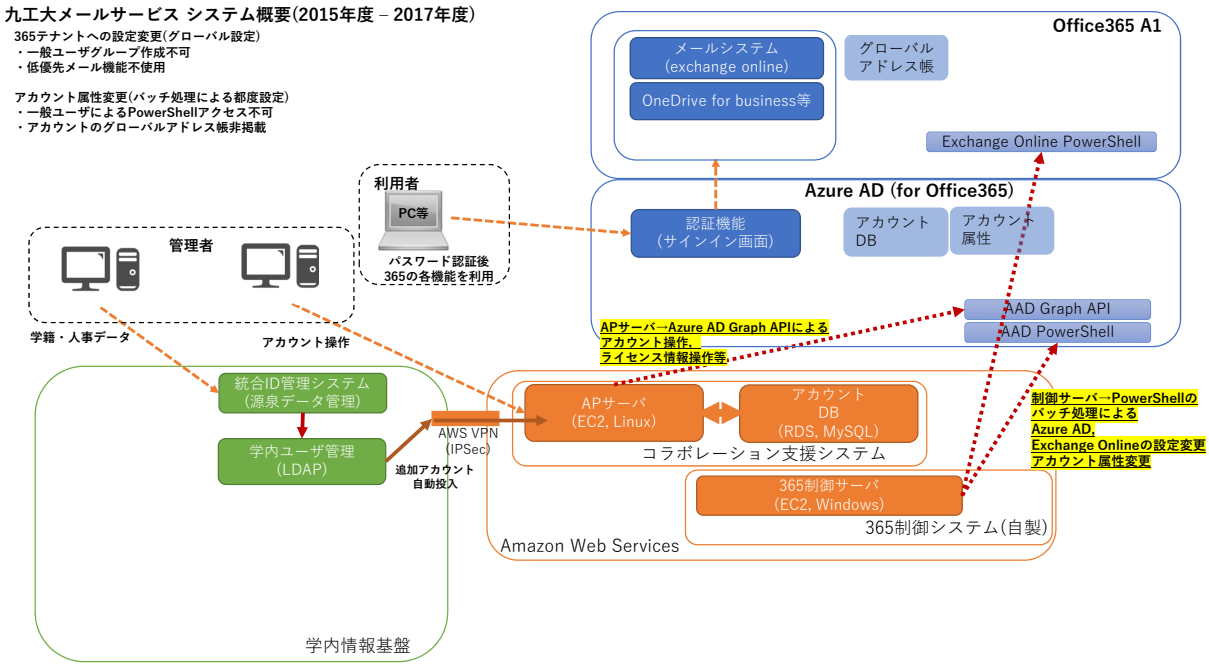


図-1　九工大メール 第一期システム構成図

者情報の作成，変更に連動した 365 アカウント操作」「区分変更に連動した 365 のライセンス変更」を実施している [3].

ただし，一部の利用者への権限操作については Azure AD Graph では実施できないため，AWS 上に 365 制御サーバ (Windows Server) を構築し，Windows PowerShell による Azure AD および Exchange Online の操作処理を併用している．本学では，セキュリティの観点から，一般ユーザによる 365 の操作や情報の閲覧範囲を限定するため，一般ユーザによるグループ作成の禁止，PowerShell による操作の禁止 (Azure AD, Exchange Online)，アカウント情報のグローバルアドレス帳への非掲載 (Exchange Online) について，PowerShell の定期的な実行により実現している (表-2, スクリプト項番 1-1,1-2,1-3,1-4).

また，作成されたアカウントに対して 365 テナントの初期ドメイン (onmicrosoft.com ドメイン) が付与される事がある，Exchange の低優先メール機能が利用者が関知しないタイミングで有効化される等，本学での運用に適さない振る舞いが確認されている．これらを抑制する処理についても PowerShell の定期的な実行により実現している (表-2, スクリプト項番 1-5,1-6).

3　大学における 365 利用時の課題

本学がメールサービスに用いる 365 は，本来は業務を効率化するアプリケーション群を提供する製品であるため，電子メール（Exchange Online の一機能) 以外の多数の機能が存在する．教育機関を対象とした，無償で利用可能な製品である 365 A1 においては，オンラインストレージ (Onedrive for business)，グループウェア (Sharepoint Online)，会議・コラボレーションツール (Teams) 等の有用なツールが利用可能である．

サービスの提供から数年が経過し，各利用者へのメールボックスやストレージには多くの情報が集約されている．この状況において，本学において顕著となった 365 を利用する際のセキュリティに関する課題について言及する．

3.1　サインイン方法に関する課題

前述の通り，本学では 365 が有する多くの機能を利用者に付与している．対して，365 へのサインイン方法については，初期状態であるサインイン ID(メールアドレス) とパスワードの組み合わせをそのまま用いていた．365 はメールアドレスがサインイン ID となるため，論文等においてメールアドレスを公開している場合，アカウント情報の一部が明らかであるとも言える．また，サインインの経路については，365 の Web インタフェース，Office アプリケーション等からのサインイン，PowerShell によ

るリモート接続等がサポートされており，初期状態では何れの方法でもサインインが可能である．

即ち，本学における 365 の利用形態は，多数の利用者が存在し，利用者に多くの機能が付与されるにも関わらず，そのサインインの強度は堅牢とは言い難い状態であった．これは，アカウントを詐取されるリスクが高い状態と言える．特に本学においては，卒業生のアカウントが長期間利用されず放置されており，これはパスワードの総当たり攻撃等によりアカウント詐取の対象となる．本学においても 2018 年度頃から 365 に関わるセキュリティインシデントが顕在化した．アカウントが詐取され，当該アカウントによる SPAM メールの大量送信に用いられたことが確認された．従って，全てのアカウントに対して，アカウント放置への対処や認証方式の強化が求められる．

3.2 サインインのふるまい検知・監視．ログの保存に関する課題

アカウント詐取は，単一のサインイン ID に対する短時間での大量のサインイン試行，同時に多数の接続先からのサインイン試行等を手段として行われる．このようなサインインのふるまいを検知することにより，アカウントの保護 (パスワードの初期化やアカウントの一時停止) が可能となる．また，アカウント詐取が発生した場合は，その被害状況を把握するため，当該アカウントからのメールの送受信やファイルのダウンロード記録等からの分析が必要となる．

従って，利用者の様々なログを収集し，記録・分析する手段が必要となる．

3.3 付与可能な 365 ライセンスと機能レベルの課題

365 には，上述の課題である認証方式の強化やサインインの振る舞い検知，ログの監視等の高度なセキュリティ対策機能が備えられている．しかし，無償で利用可能な 365 A1 においては，機能が利用できない・利用できるものの限定的であるものが多い．

認証方式を強化する方法である二段階認証 (MFA) を実現する機能については，365 A1 においても，全ての利用者に対して二段階認証を有効化できる [4][5]．しかし，サインインの頻度や場所を判定し，必要なときのみ二段階認証を要求する方式 (リスクベース認証) については，上位の有償製品である A3(Azure AD Premium P1, 条件付アクセス) あるいは A5(Azure AD Premium P2, Azure AD Identity Protection[6]) を要する．

危険なサインインを検知した場合は，対象のアカウントをロックする等の対策を要する．365 A1 においては，危険なサインイン発生時に管理者へ警告する機能が存在するが，判定された要因等は参照できない．従って，365 の制御 API によりログを収集蓄積し，ログ分析を行った後にアカウントのロック等を行う判断ロジックを作成する必要がある．対して 365 A5 においては，サインインの危険度判定に基づく自律的なアカウントのロック処理が実現可能である．

上記のように，365 には機能レベルに応じて利用可能なセキュリティ対策機能が大きく異なる．本学においては，必要なライセンス，ライセンス適用が可能な利用対象 (卒業生，在学生等)，本学における運用への親和性の観点から，多要素認証やセキュリティ対策機能の実現方法について 5 種類の実現方法に分類した (表-1)．これらの多様な実現方法から，適切な方法を選択する必要がある．

4 セキュリティ向上を指向したメールサービス運用システムの拡張

3 節にて言及した 365 の運用に対する課題に対応するため，本学ではメールサービスを構成するシステムの拡張を行い，ログの監視体制および認証基盤の強化を行うこととした．

2018 年度より 2019 年度までは，第一期システムを拡張することにより，セキュリティ向上対策およびログ監視・保存体制の確立を目標とした．これを第二期システムと称する．2020 年度より，より抜本的なセキュリティレベルの向上を指向し Microsoft 365 A5 への機能レベルの更新を実施した．第二期システムを拡張し，365 A5 が有する高度なセキュリティ対策機能を付加したシステムを第三期システムと称する．第二期，第三期の詳細は以下の通りである．

4.1 第二期システム

第二期システムは，365 システムとして Office365 A1(学生用, 教職員用) を利用する．在学生, 在職者それぞれに対して，Office365 A1 が有する全機能を提供している．卒業・離退職者については Exchange Online (Plan1) 相当に限定化して機能を提供している．365 上の利用者情報管理には，365 A1 に付帯される Azure AD(Office365 アプリ) を適用する．これは，Azure AD が有する機能のうち，365 の管理に最低限必要な機能に限って提供されるものである．

利用者情報の制御については，第一期システムと同様のコラボレーション支援システムにより実行される．一部のログの取得および利用者の属性情報の制御については，制御サーバ (Windows Server) およびログ収集サーバ (Windows Server) を構築し，制御用 PowerShell を定期的

表-1　365 における多要素認証の展開方法，機能の比較

機能名称	ユーザ毎のMFA	条件付きアクセス (ベースラインポリシー)	セキュリティ既定値	条件付きアクセス	Identity Protection
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
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
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
本学における運用との親和性および利用範囲	・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，在学生・在職者を含めた利用形態には不十分である **卒業生，離退職者向けに有効化**	・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，2020年3月以降機能が終息し，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 (利用者への周知後，2020年度内に有効化予定)	・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 **管理アカウント，在学生 / 在職者向けに有効化**

に実行している．上記のサーバ群は，パブリッククラウド (AWS および Microsoft Azure) 上に構築している．

加えて，学内 (オンプレミス) の構築された仮想サーバ群に，ログ収集基盤や源泉データの管理サーバが存在する．学内情報基盤とパブリッククラウド上のサーバ群とは，VPN(AWS VPN および Azure VPN，IPSec) による通信経路を設けており，アカウント情報・ログデータ等の収受が可能な設定としている．第二期システムの概要を図-2 に示す．

4.2　第三期システム

現行システムである第三期システムは，365 システムとして新たに Microsoft 365 A5(学生用，教職員用) および Exchange Online for Alumni (卒業生用) を利用する．学生用，教職員用それぞれにおいて，大学に籍がある利用者については 365 A5 が有する全機能を提供している．卒業生については Exchange Online for Alumni ライ

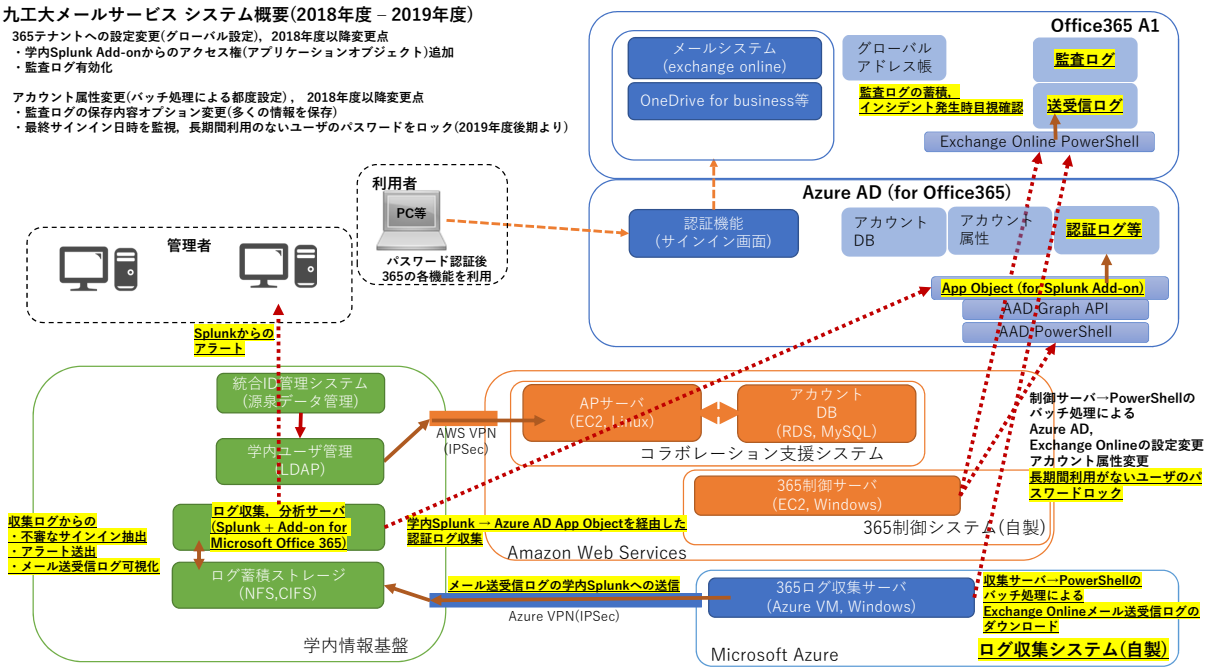


図-2　九工大メール 第二期システム構成図

センスにより Exchange Online (Plan1) の提供，離退職者については 365 A1 が有する機能を限定化し，Exchange Online (Plan1) を提供している．365 上の利用者情報管理には，在学生・在職者に対しては Azure AD Premium P2，卒業生・離退職者については Azure AD(Office365 アプリ) が適用される．システム構成および構築基盤 (学内情報基盤，パブリッククラウド) の設計については第二期システムを踏襲している．ログ監視体制・セキュリティ向上対策についても，第二期システムでの方針を踏襲しつつ，365 A5 で利用可能な高度な機能を付加している．

なお，365 ライセンスの適用ルール変更により，離退職者向けのメールサービスの提供は廃止予定である．しかし，廃止するまでの期間においてはセキュリティの強化は必要であるため，卒業生向けと同様のログ監視，認証基盤強化の体制を採る．第三期システムの概要を図-3 に示す．

5　セキュリティ向上対策

第二期システムおよび第三期システムにおいては，セキュリティ向上対策として以下のログ監視体制の強化 (第二期:3 種類，第三期:1 種類) と認証基盤の強化 (第二期:1 種類，第三期:2 種類) を実施した．

■ログ監視体制の強化

365 への認証ログ監視　取得元：Azure AD，取得対象：ID，時刻，成功/失敗，IP アドレス (第二期システム，5.1.1 節)

監査ログの監視　取得元：Azure AD，Exchange Online，取得対象：ID，時刻，利用者の機微な操作 (ファイル，メールボックスの操作，パスワード変更等) (第二期システム，5.1.2 節)

メール送受信ログの監視　取得元：Exchange Online，取得対象：ID，時刻，送信/受信，件名，宛先，メッセージサイズ (第二期システム，5.1.3 節)

リスク検知事象のアラートメールによる通知　送信元：Azure AD Premium P2 (第三期システム，5.1.4 節)

■認証基盤の強化

長期利用のないアカウントのパスワードランダム化　制御対象：Azure AD，Exchange Online (第二期システム，5.2.1 節)

卒業生・離退職者向け多要素認証有効化　制御対象:Azure AD，ユーザ毎の MFA (第三期システム，5.2.2 節)

在学・在職者，管理者向け多要素認証有効化　制御対象:Azure AD Premium P2，Identity Protection (第三期システム，5.2.3 節)

これらの各項目についての詳細を述べる．

5.1　ログ監視体制

第二期システムにおけるログ監視体制としては，2018 年度より顕在化した 365 アカウントの詐取，その後詐取

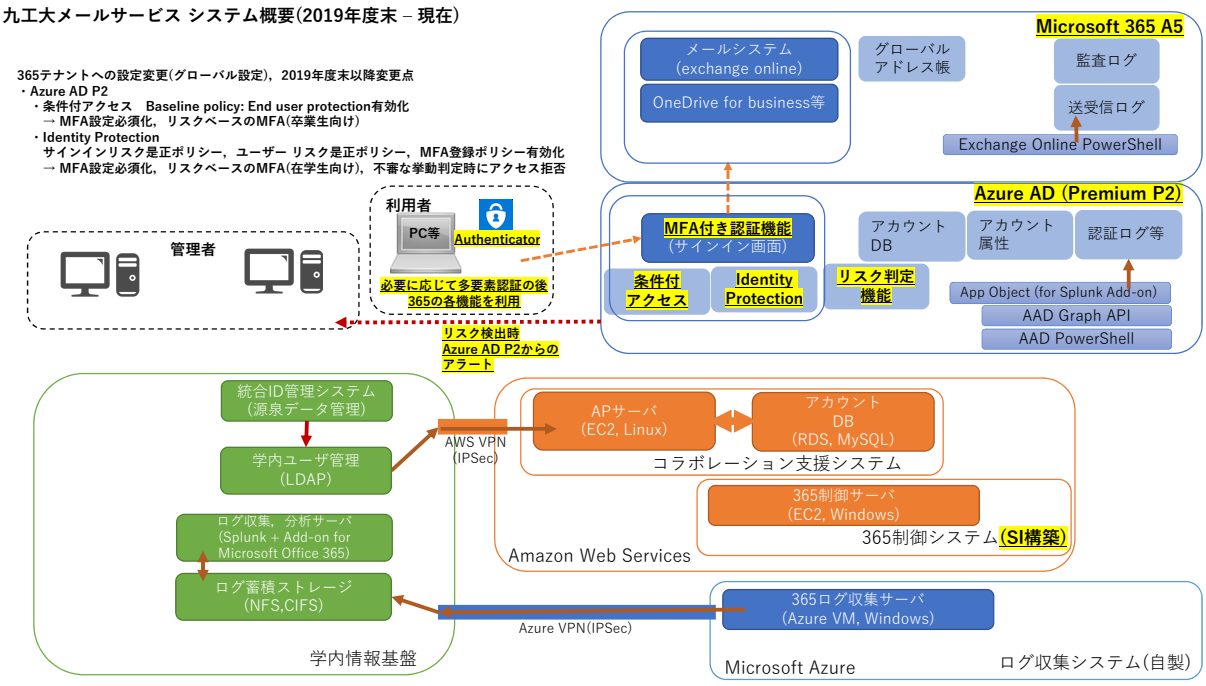


図-3　九工大メール 第三期システム構成図

されたアカウントからの SPAM 送信への対策として，アカウントの利用状況の把握を目標とした．ただし，第二期システムでは 365 A1 を用いるため，365 が有するログ分析機能や通知機能は十分に活用できない．従って，Exchange Online や Azure AD に関するログを API 経由で取得し，ログ集約・分析手法を実施している．第三期システムにおいては，Azure AD Premium P2 が有する高度なセキュリティ向上機能である Azure AD Identity Protection を積極的に活用する．

5.1.1　365 への認証ログ監視

365 へのサインイン履歴等の認証ログは，Azure AD によりサインインログとして記録される．記録されたログの長期保存や検索については，Microsoft が提供する Azure Log Analytics の利用が推奨されている．しかし，Log Analytics は，検索に用いるクエリが複雑であること，アクセス元の国名や地域を検索条件として指定できない等の理由から，本学の運用に適さないと判断した．

本学においては，学内の仮想基盤上に展開されるログ収集システム [7] を活用することとした．ログ収集システムは，収集・分析サーバ (Splunk[8]) および蓄積ストレージ (NFS, CIFS サーバ) から構成される．

Azure AD と外部システムとのデータアクセスを行うためには，Azure AD 上にアプリケーションオブジェクトと呼ばれる API アクセス用のアドオンを追加する必要がある．本システムにおいては，収集サーバ (Splunk) が外部システムに相当し，Splunk 社が提供するアドオン (Application Object for Splunk Add-on[9]) を Azure AD 上に追加している．収集サーバは定期的に Azure AD にアクセスし，365 へのサインイン履歴を取得・蓄積ストレージに保存を行う．

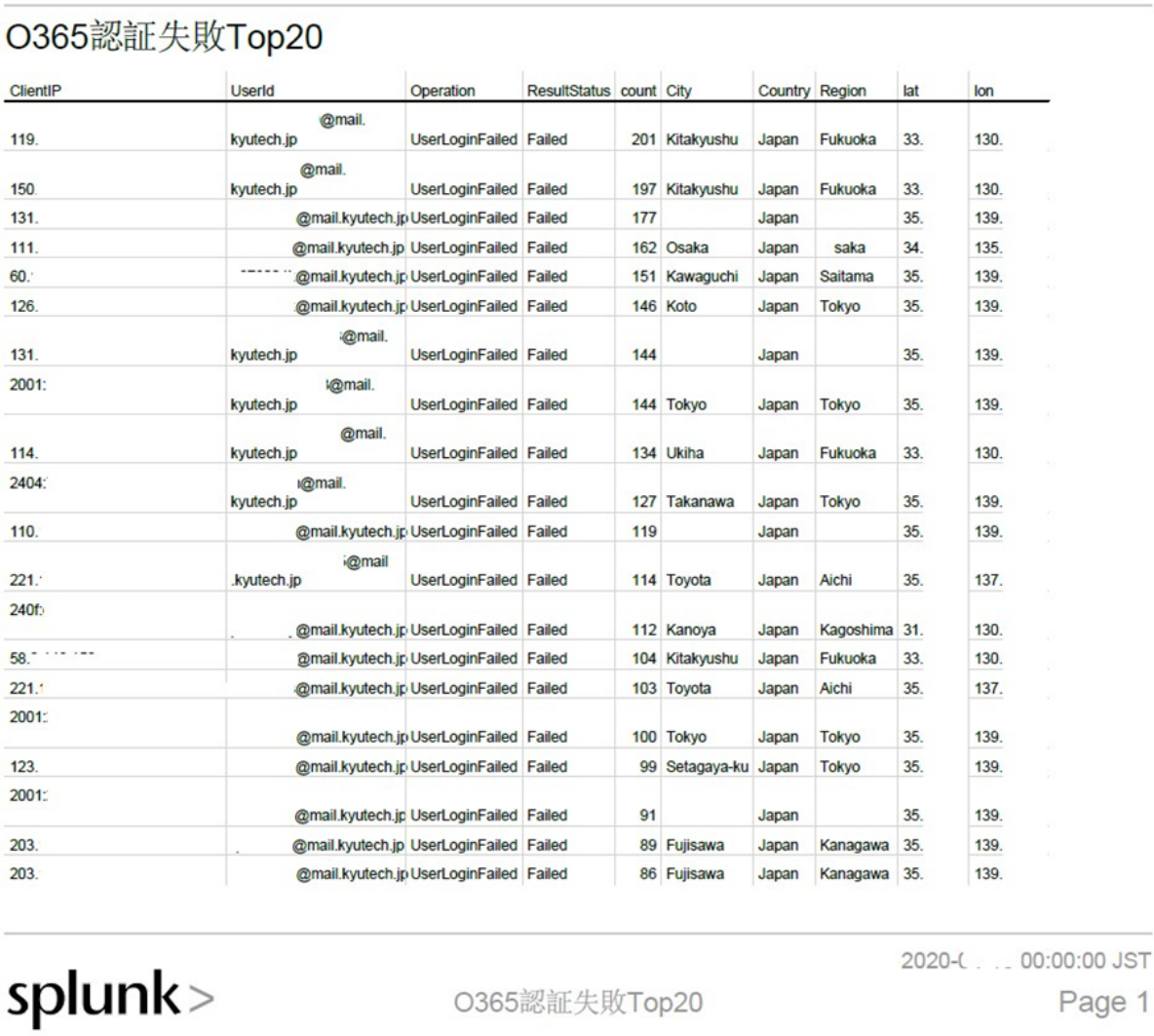
保存された認証ログは，日次処理として Splunk による分析処理が実行される．本学においては，サインインに失敗した回数が多い上位のアカウントを抽出し，管理者へ通知する機能を実装している．管理者への認証失敗レポートの例を図-4 に示す．

5.1.2　監査ログの監視

365 への操作に関するログは監査ログと呼ばれ，様々な利用者の操作が取得可能である．本学においては，365 へのサインインや属性変更 (パスワード変更等) に関するログ (Azure AD が対象)，メールボックスの操作に関するログ (Exchange Online) を取得対象とする．メールボックスの操作に関するログは，初期状態では詳細な情報が取得できないため，アカウント作成時に詳細な情報が取得できる設定としている (表-2, スクリプト項番 2-1)．これらの取得されたログは 365 の管理コンソールから検索が可能である [10].

5.1.3　メール送受信ログの監視

九工大メールにおけるメールの送受信数は，平日において平均 36,000 通 (ログのサイズ:約 16MB), 休日や休暇期間において平均 12,000 通 (ログのサイズ：約 5MB) と



O365認証失敗Top20

ClientIP	UserId	Operation	ResultStatus	count	City	Country	Region	lat	lon
119.	@mail. kyutech.jp	UserLoginFailed	Failed	201	Kitakyushu	Japan	Fukuoka	33.	130.
150.	@mail. kyutech.jp	UserLoginFailed	Failed	197	Kitakyushu	Japan	Fukuoka	33.	130.
131.	@mail.kyutech.jp	UserLoginFailed	Failed	177		Japan		35.	139.
111.	@mail.kyutech.jp	UserLoginFailed	Failed	162	Osaka	Japan	saka	34.	135.
60.	@mail.kyutech.jp	UserLoginFailed	Failed	151	Kawaguchi	Japan	Saitama	35.	139.
126.	@mail.kyutech.jp	UserLoginFailed	Failed	146	Koto	Japan	Tokyo	35.	139.
131.	@mail. kyutech.jp	UserLoginFailed	Failed	144		Japan		35.	139.
2001:	@mail. kyutech.jp	UserLoginFailed	Failed	144	Tokyo	Japan	Tokyo	35.	139.
114.	@mail. kyutech.jp	UserLoginFailed	Failed	134	Ukiha	Japan	Fukuoka	33.	130.
2404:	@mail. kyutech.jp	UserLoginFailed	Failed	127	Takanawa	Japan	Tokyo	35.	139.
110.	@mail.kyutech.jp	UserLoginFailed	Failed	119		Japan		35.	139.
221.	@mail .kyutech.jp	UserLoginFailed	Failed	114	Toyota	Japan	Aichi	35.	137.
240f:	@mail.kyutech.jp	UserLoginFailed	Failed	112	Kanoya	Japan	Kagoshima	31.	130.
58.	@mail.kyutech.jp	UserLoginFailed	Failed	104	Kitakyushu	Japan	Fukuoka	33.	130.
221.	@mail.kyutech.jp	UserLoginFailed	Failed	103	Toyota	Japan	Aichi	35.	137.
2001:	@mail.kyutech.jp	UserLoginFailed	Failed	100	Tokyo	Japan	Tokyo	35.	139.
123.	@mail.kyutech.jp	UserLoginFailed	Failed	99	Setagaya-ku	Japan	Tokyo	35.	139.
2001:	@mail.kyutech.jp	UserLoginFailed	Failed	91		Japan		35.	139.
203.	@mail.kyutech.jp	UserLoginFailed	Failed	89	Fujisawa	Japan	Kanagawa	35.	139.
203.	@mail.kyutech.jp	UserLoginFailed	Failed	86	Fujisawa	Japan	Kanagawa	35.	139.

図-4　ログ収集，分析サーバによる 365 への認証失敗レポート

なる．本学においては，パブリッククラウド (Microsoft Azure) 上にログ収集サーバを配置し，収集サーバ上で PowerShell による収集処理を実施する．収集したログは，学内情報基盤内の蓄積ストレージに対して CIFS プロトコルを用いて転送する．また，転送されたログは，前述の認証ログ監視と同様に，Splunk による分析処理が実行される．

なお，365 システムの制約として，メールの送受信に関するログは，一般的な syslog 等では取得できず，PowerShell 等を用いて API を経由した取得が必要となる [11]．また，API の仕様についても，形式が「指定したアカウント，期間における送受信ログの取得」となるため，全てのアカウントに対するバッチ処理を要する．本学が適用するメールログ取得用の PowerShell スクリプトを表-2 内の項番 2-3 に示す．取得に要する時間は平日の送受信数において約 3 時間を要する．従って，リアルタイムにログを取得し，振る舞いを検知することは困難である．

5.1.4　リスクを検知した事象のアラートメールによる通知

第三期システムにおいては，Azure AD Identity Protection が利用可能となった．本機能を用いることで，ユーザの不審な振る舞いを検知し，リスクの程度 (低 - 高) が判定される．ユーザの不審な振る舞いとリスクの程度の例として，メールフォワードの設定 (リスク低)，短時間での大量の電子メールメッセージやオンラインストレージ上のファイル削除 (リスク中)，大量のメール送信 (リスク高) 等が検出可能である．また，ユーザの不審なサインインについても検知され，リスクの程度が判定される．短時間で複数地域からのサインインが試行される場

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

図-5　Exchange Online から取得したメール送受信ログの例

合や，Tor をはじめとする匿名ネットワークからのサインインはリスク高と判定される．

本学においては，振る舞いやサインインのリスク検知後，管理者へアラートを通知し，管理者が手動にてアカウントのロックを行う運用を実施している．365 A5 では，クラウドシステムへのアクセス制御基盤である Cloud App Security[12] と連携し，「不正アクセスの検知に基づき，自動的にアカウントのロックを行う」等の高度な対策が可能であるが，リスクの誤検知が危惧されること，パラメータの調整が複雑であることから今後の課題とする．

5.2　認証基盤の強化

第二期システムにおいては，認証基盤の強化策として，Exchange Online や Azure AD の情報を取得および制御することにより，不正なサインインを低減させることを目標とした．

第三期システムにおいては多要素認証の導入を目標とした．3.3 節で述べた通り，Azure AD にて利用可能な機能レベルは 365 のライセンスに応じて異なり，多要素認証の実現方法も多岐にわたる．本学においては，必要なライセンス，ライセンス適用が可能な利用対象 (卒業生・離退職や，在学生・教職員等)，運用への親和性に基づく実現方法の分類 (表-1) を用いて，利用者層に応じた手法を採用する．

5.2.1　長期利用のないアカウントのパスワードランダム化

本学においては 2020 年 9 月現在，365 上に約 21,800 アカウントが存在している．対して，90 日平均のアクティブユーザ数は約 7,000 であり，多くのアカウント (主に卒業生に付与) は長期間利用されていない状況にある．また，第二期システムの運用当初は，利用者認証がパスワード認証のみであったことから，総当たり攻撃によるアカウント詐取が試みられていた．対して，第二期システムで用いる 365 A1 はアカウントに対する攻撃へのリアルタイムな対策機能を有しておらず，独自の対策が求められた．本学では，パブリッククラウド上に設置した 365 制御サーバ (Windows Server) 上において，Exchange Online への最終サインイン日時を取得し，長期間 (90 日以上) 経過した場合は利用がないと判断し，パスワードをランダム化する月次処理を実施している．本処理に要する情報の取得およびパスワードのランダム化は，PowerShell による Exchange Online および Azure AD に対する処理のみで実現可能である (表-2, スクリプト項番 2-2).

本処理によってパスワードがランダム化されたアカウント数の一例であるが，2019 年度末 (2020 年 2 月) において，365 上に存在した約 19,200 アカウントに対して，

90 日以上サインインがなくパスワードがランダム化された数は約 9,800 であった．長期間利用のないアカウントに付与されるパスワードが定期的に変更されるため，セキュリティ向上に寄与していると言える．特に卒業生および離退職者についてはアカウントの放置が多く，かつ適用可能なライセンスが 365 A1 相当に限定化されるが，本機能は 365 A1 を有していれば実現可能であるため，セキュリティ向上に対して効果的な手段である．

5.2.2 卒業生・離退職者向け多要素認証有効化

卒業生に付与可能な 365 ライセンスは，Exchange online for Alumni と称される．このライセンスは，365 A1 のうち，Exchange Online (Plan1) のみが利用者に提供されるものと等価である．また，4.2 節で述べた通り，離退職者についてはメールサービスの提供を廃止する予定であるが，サービス提供中においては，365 A1 の機能を限定し，Exchange Online (Plan1) を付与している．

上記の 365 ライセンスに適用される Azure AD の機能レベルは基本機能となる Azure AD(Office365 アプリ) となり，適用可能な多要素認証の実現方法は，表-1 中の「1. ユーザ毎の MFA」「2. 条件付アクセス (ベースラインポリシー)」「3. セキュリティ既定値」の 3 種類である．このうち，2. が本学との親和性が高い方法であったが，2020 年 3 月以降設定不可となったこと，3. は既存環境の設定変更を要するユーザが多く生じることから，1. を選択した．

1. は対象とするアカウントに対して，個別に多要素認証を有効化する設定を付加する必要がある．本学においては，PowerShell スクリプトを定期的に実行し，対象とするアカウントを検出・多要素認証の有効化を実施している (表-2，スクリプト項番 3-1).

5.2.3 在学・在職者，管理者向け多要素認証有効化

本学においては，在学生および教職員に対しては，365 A5 を適用しているため，適用される Azure AD の機能レベルは Azure AD Premium P2 となり，多要素認証に関する全機能が利用可能である．従って，多要素認証の実現方法も，表-1 に示した全 5 種類となる．近年では，学生や教職員は不定期に入学や採用がなされ，ID の発行もそれに連動するため，多要素認証の設定に関する運用コストは極力下げる必要がある．また，学外からの 365 へのサインインも多いため，そのサインインが正規のものであるか判定できることが望ましい．

このような状況に対応する最適な方法は，本学では Azure AD Identity Protection が有する MFA 登録ポリシーおよびサインインリスクポリシーの適用であると判断した．MFA 登録ポリシーは，二段階認証が未設定のアカウントに対して，サインイン時に設定を促す機能である．365 へ追加された新規のアカウントに対して，管理者が個別に設定することなく，二段階認証の有効化を行わせることが可能となる．前述のユーザ毎の MFA と異なり，アカウントは自動的に二段階認証有効化の実施対象となる．サインインリスクポリシーは前述の通り，ユーザの不審なサインイン (リスク) を検出し，サインインの振る舞いを制御する機能である．本学においては，サインインのリスクが小以上と判定された場合，二段階認証を要求する設定としている．

本学では 2020 年 3 月より Identity Protection による多要素認証の有効化を開始した．その実績の一例を示す．対象となる在学生のアカウント数は 5,699 であるが，2020 年 4 月までの有効化実施済み数は 3,391，5 月までの実施済み数は 4,018 である (約 81%)．また，対象となる教職員のアカウント数は 1,202 であるが，2020 年 4 月までの有効化実施済み数は 434，5 月までの実施済み数は 489 である (約 50%)．特に在学生については，2020 年 4 月に新入生のアカウントが新規追加されているが，それらに対する二段階認証の有効化設定は自律的に実施されており，管理者の運用コストの低減が実現されている．

なお，在学生・教職員ともに有効化未実施のアカウントが存在する．在学生において有効化未実施のアカウントは，大学院に進学した学生が学部時に取得したアカウントのみを利用しており，有効化されていないものと推察される．教職員において有効化未実施のアカウントは，本メールサービスを積極的に利用しない職域 (パートタイム職員や事務職員) に付与されたものと推察される．これらの詳細な分析は今後の課題とする．

5.3 365 制御用の PowerShell スクリプト

本学における 365 の運用に際し，要する振る舞いの変更，要する対応策，具体的な制御用の PowerShell スクリプトについて，表-2 に示す．

6 むすび

本稿では，九州工業大学における Office365 システムに対するセキュリティ向上対策について報告した．本学においては，卒業生を含めた全学向けのメールサービスとして 365 が活用されてきたが，アカウントが詐取され，SPAM の送信に用いられる状況が見受けられた．この問題に対処するため，当初は主にログの監視に注力し，365 へのサインインやメールの送受信ログを学内のログ収集分析基盤 (Splunk) と連携し，不審な振る舞いを検出する

システムを確立した．

その後，根本的には認証基盤の強化が必要であると判断し，本学においては 365 の機能レベルについて，A1 から A5 に拡張した．特に，365 A5 で利用可能な高度な多要素認証基盤である Azure AD Identity Protection を活用し，利用者への負担が少ない (リスクベース認証)，かつ管理者の運用コストが低減される (利用者への多要素認証の自動的な展開) 多要素認証方式が運用可能となった．

今後もセキュリティ向上を図るため，Cloud App Security による運用の自動化や，Office 365 Advanced Threat Protection[13] による電子メールに含まれる不正なハイパーリンクの検出等，365 A5 が有する機能の分析と検証を推進する．

また，メールサービスの今後の課題としては，離退職者向けのサービス提供廃止に伴う対象の 365 アカウントの取扱い方針の決定 (アカウントを削除するか，パスワードのリセットによるロックとするか)，在学生および在職者アカウントに含まれる二段階認証未設定者について，学年や職域等の詳細分析を実施が挙げられる．

参考文献

[1] 林 豊洋，本学における生涯メールサービスの提供について，九州工業大学情報科学センター広報第 26 号，pp.3-14，2014.

[2] 林 豊洋，九州工業大学における生涯メールサービスの移行，大学 ICT 推進協議会 2017 年度年次大会，2017.

[3] Azure Active Directory Graph API，Microsoft Azure AD documentation, https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-graph-api (2020 年 8 月 3 日参照)

[4] Azure Active Directory pricing，Microsoft Azure AD documentation, https://azure.microsoft.com/en-us/pricing/details/active-directory/ (2020 年 8 月 3 日参照)

[5] What are security defaults?，Microsoft Azure AD documentation, https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults (2020 年 8 月 3 日参照)

[6] Azure AD Identity Protection documentation，Microsoft Azure AD documentation, https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/ (2020 年 8 月 3 日参照)

[7] 中村 豊，佐藤 彰洋，福田 豊，和田 数字郎，岩崎 宣仁，九州工業大学における全学セキュア・ネットワークの更新- 2019 年度における更新について-，九州工業大学情報科学センター広報第 32 号，pp.3-10，2020.

[8] Splunk Enterprise - ビッグデータ分析ソフトウェア,https://www.splunk.com/en_us/software/splunk-enterprise.html (2020 年 8 月 3 日参照)

[9] Splunk Add-on for Microsoft Office 365, splunkbase, https://splunkbase.splunk.com/app/4055/ (2020 年 8 月 3 日参照)

[10] 管理者、代理人、および所有者のアクセスのメールボックス監査ログ設定を構成する，Microsoft Docs - Exchange Server, https://docs.microsoft.com/en-us/exchange/policy-and-compliance/mailbox-audit-logging/enable-or-disable (2020 年 8 月 3 日参照)

[11] メッセージトレースの取得，Microsoft Docs - Module: exchange, https://docs.microsoft.com/en-us/powershell/module/exchange/mail-flow/get-messagetrace (2020 年 8 月 3 日参照)

[12] Microsoft Cloud App Security overview, Microsoft Docs - Enterprise Mobility + Security, https://docs.microsoft.com/en-us/cloud-app-security/what-is-cloud-app-security (2020 年 8 月 3 日参照)

[13] ATP Safe Links, Microsoft Docs - Microsoft 365, https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/atp-safe-links (2020 年 8 月 3 日参照)

表-2　365 の運用に要する振る舞いの変更，PowerShell スクリプト

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
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
3-1 (三期)	ユーザー毎の多要素認証を有効化する	・対象のアカウントに多要素認証を有効化 ・本学においては，卒業生および離退職者が対象	実行周期：周期的に卒業生，離退職者アカウントを検知(本学では30分周期) $st = New-Object -TypeName Microsoft.Online.Administration.StrongAuthenticationRequirement $st.RelyingParty = "*" $st.State = "Enabled" $sta = @($st) # 対象のアカウントに対して多要素認証を有効化 Set-MsolUser -UserPrincipalName user@contoso.com -StrongAuthenticationRequirements $sta