Office 365 outlook を使用するにあたって

各位

梱山女学園では、平成 30 年度より教職員に Microsoft Office 365 が提供するメールサービス、Outlook をご利用いただきます。
Microsoft Office365 は、Web 上で利用するサービスであると共に、Windows10、Mac、iPhone、Android 上で動作するアプリケーションでも利用でき、共通のメール環境が利用可能です。
特にメールサービスでご留意いただきたい内容をご説明させていただきます。Office365 内のヘルプも充実していますので、ご理解の上サービスをご活用ください。

1. Outlook とは

Office365 は、Microsoft 社が提供するクラウドサービスです。
複数あるサービスの内、メールを中心としたサービスが Outlook となり、メール、予定表、連絡先、タスク管理がまとめられています。

2. メールを取り巻く環境

2.1. セキュリティ向上の必要性

近年、大学をはじめとする教育機関に対する不正アクセスは増加の一途を辿っています。情報処理推進機構が発表した、情報セキュリティ 10 大脅威 2018 では上位を Web サービスや、メールサービスを入り口とした脅威が大半を占めています。https://www.ipa.go.jp/security/vuln/10threats2018.html
2018 年現在、フィッシングメールの被害を受けた大学は 6 校に上り、1 万 2 千件もの情報漏洩が発生し、文部科学省も注意喚起をおこなう事態となっています。
また潜在的にはより多くのセキュリティ被害が発生していると思われます。

2.2. セキュリティ向上への取組

学園では、Web メールサービスとして Active!mail を提供するとともに、メールアプリケーション(※1)での利用も POP/IMAP にて提供してきました。
メールの利用にあたっては、Active!mail が動作する学園メールシステム側でおこなうスパムメール、ウィルス付きメール、標的型攻撃などを、受信前に隔離する対策を導入してきました。
またセキュリティについては利用者の対処も必要であることから、セキュリティ講習会を開催し、セキュリティ事故防止への取組に努めてきました。
※1　Android 7.x 標準メール(Gmail アプリ、Office Outlook 2016、Office

Outlook 2013、Office Outlook 2010、Windows Live メール（Windows 7 用 Windows Essentials 2012 に付属)、Mozilla Thunderbird (Windows/Mac/Linux 版)、AL-Mail32 等

2.3. セキュリティの現状

メールシステム、メール利用者双方の努力にも関わらず、セキュリティ事故を 0 にすることは実現できていません。毎年数件のメールアカウントの乗っ取りや、不正なメールサーバの利用が発生しており、外部へのスパムメール等 60 万通以上の送信に悪用されています。

従来のメールシステムは、ユーザー名とパスワードを、メールシステム管理者を装ったフィッシングメールや、パスワードが合致するまで機械がログインを繰り返す手法により不正に入手することにより、正規の利用者を装ってメールを送信されてしまう被害が発生していました。

2.4. セキュリティ上の課題と対応

メールアプリケーション（※1）が使用する POP/IMAP という仕組みは、ユーザー名とパスワードが判明していれば、メールサーバへログインし、メールの送受信が可能となります。これは本来求められる正常な動作であるため規制が困難でした。外国からの利用かどうか、パスワード間違いの回数など、攻撃者を判断し、不正な利用を防ぐ方策を実施してきましたが、被害を 0 にすることはできていません。

そのため、Office365 Outlook へメールを切替えるにあたり、メールの利用方法を変更し、将来的により強固なセキュリティの導入を目指すに至りました。

i. Single Sign On（SSO）を使ったログイン

Office 365 へのログインは、学園環境に整備された SSO を用います。これにより Outlook へのログインは、Web ブラウザを用いた操作をおこなう環境が必須になります。

メールサーバへ、ログイン名とパスワードを送付しメール送信をおこなうだけでは、ログインしてメールの送受信ができないため、メールアカウントの乗っ取りや、不正送信を防止する効果が期待できます。

ii. 二要素認証への対応

i の方法を用いたとしても、手動、もしくは手動を模した機械的操作により、Web ブラウザの操作による Outlook へのログインを防止することは完全にはできません。

そのためユーザー名、パスワードに加え、もう一つログイン操作毎に変更さ

れるコード番号（OTP コード）をログイン時に必要とする方式を整備しました。コード番号が手に入らないため不正利用の防止が可能です。
SSO のシステムに付随したこのシステムは、学園が提供しているメールアドレス以外のアドレスへ、コード番号を送信します。
ご申請いただければ利用可能ですので、学園情報センターへご連絡ください。 事前に学園以外のメールアドレスと受信環境（携帯電話、スマートフォン等）をご準備いただき、ぜひご活用ください。

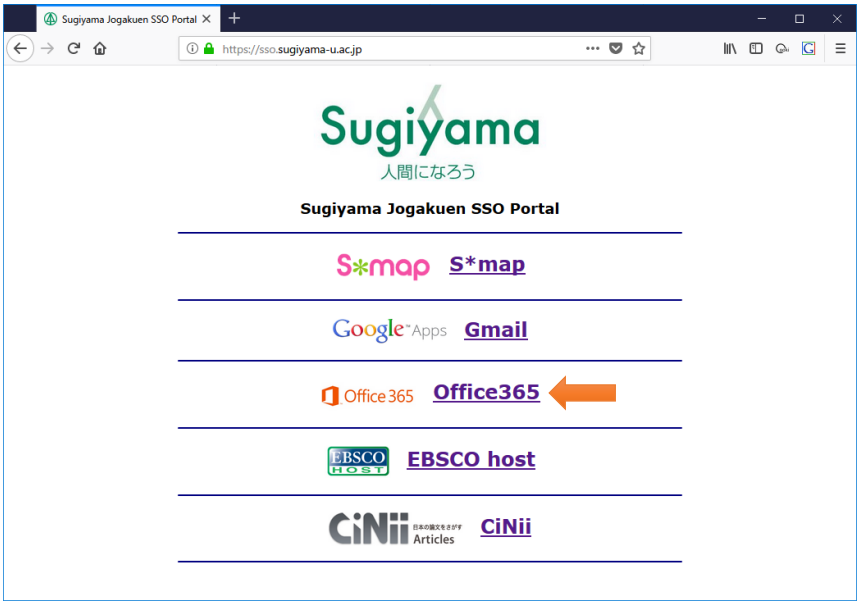
iii. Office 365 のセキュリティ機能の充実
現在は標準的な Office 365 Outlook のサービスを使用しています。
将来的には、より高度なセキュリティ機能を提供可能な契約へ移行しセキュリティ機能を充実させます。AI を活用した不正ログイン防止、ウィルス検知、振る舞いを検知してのメールの隔離、パソコン上でのファイルアクセス拒否などを実現します。

2.5. Office365 outlook でのメール利用環境
SSO と二要素認証に対応したことで、従来の POP/IMAP 方式のみを用いるメールソフトウェア(※1)は使用ができなくなります。
Web ブラウザ、もしくは Windows10、MacOS、Android、iPhone、iPad で動作するメールアプリケーション（※2）での Outlook の利用をお願いします。
※2 iOS 12 標準メール、iOS Outlook アプリ、Android Outlook アプリ、
Office365 Outlook、Windows 10 標準メール、
MacOS 10.14 (Mojave) 標準メール、
MacOS 用 Outlook アプリ（El Capitan、Mojave で動作確認）

3. メール利用方法 Web ブラウザ

3.1. アクセス方法

Office365Outlook を利用する際にアクセスする URL は、https://sso.sugiyama-u.ac.jp/になります。Chrome、Firefox、Edge、Safari 等でアクセスします。
https://portal.sugiyama-u.ac.jp へアクセスした場合でも、S*map 等 SSO 対象サービスへログイン済みで無い場合は、ログイン画面が表示されます。
ログインをブラウザが記録している場合、ログイン画面は表示されません。
Office365 のリンクをクリックします。

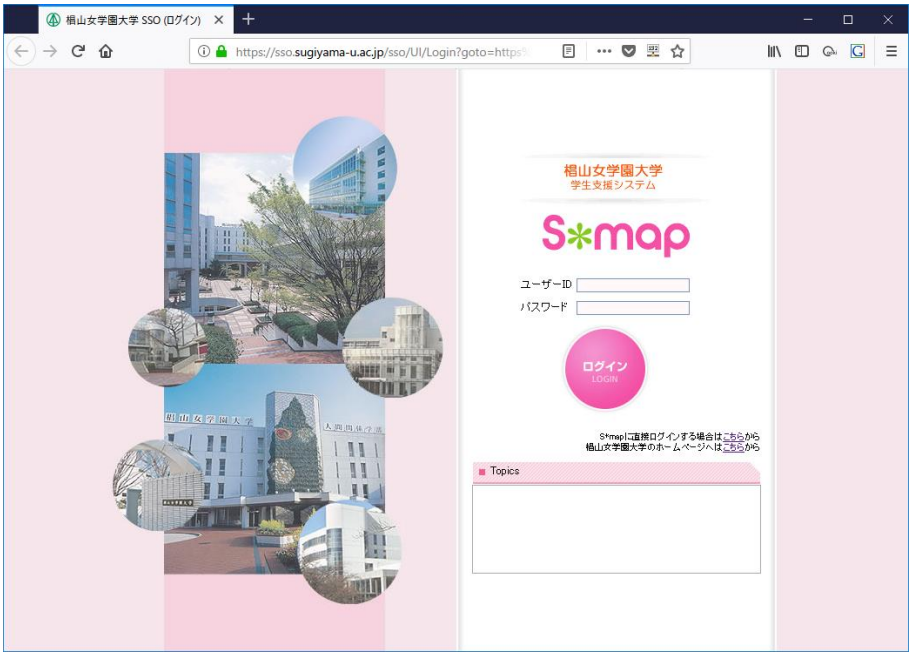


ブラウザがログインを記録している場合、メールアカウントを切替えることができません。ブラウザのプライベートモードをご利用ください。

3.2. ログイン

ユーザーID、パスワードを入力してください。

二要素認証を申請済みの場合、ログイン後にコード番号（OTP コード）を入力する画面が表示されます。ログインボタンを押すたびにメールで届きますので、最新の番号を入力してください。



※ユーザーID,パスワード

同じ仕組みですが、所属によりなじみがない呼び方になりますので、以下読み替えてください。

大学教員、及び学園職員

S*map へのログインで使用しているユーザー名・パスワード

山添教員

ファイルサーバへアクセスする際のユーザー名・パスワード

退職後の継続利用者

S*map が学園で利用開始される前、後で異なります。

S*map 開始前：教室パソコンへのログインや、ファイルサーバへ
アクセスする際に使用したユーザー名・パスワード

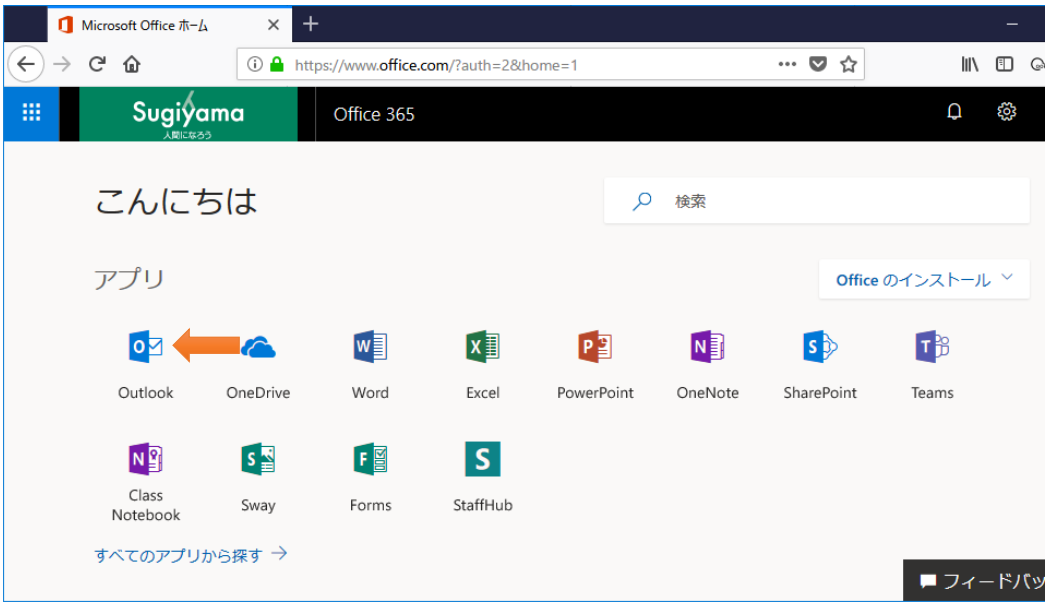
S*map 開始後：S*map へのログインで使用しているユーザー名・パスワード

不明な場合は、再発行いたしますので情報センターまでご連絡ください。

3.4. Outlook

Office365 へのログイン後、Outlook アイコンをクリックします。

メールアプリの画面が開きます。



Outlook の基本的な利用手順は別添資料をご参照ください。

学園情報センターの S*map キャビネットに保存されています。

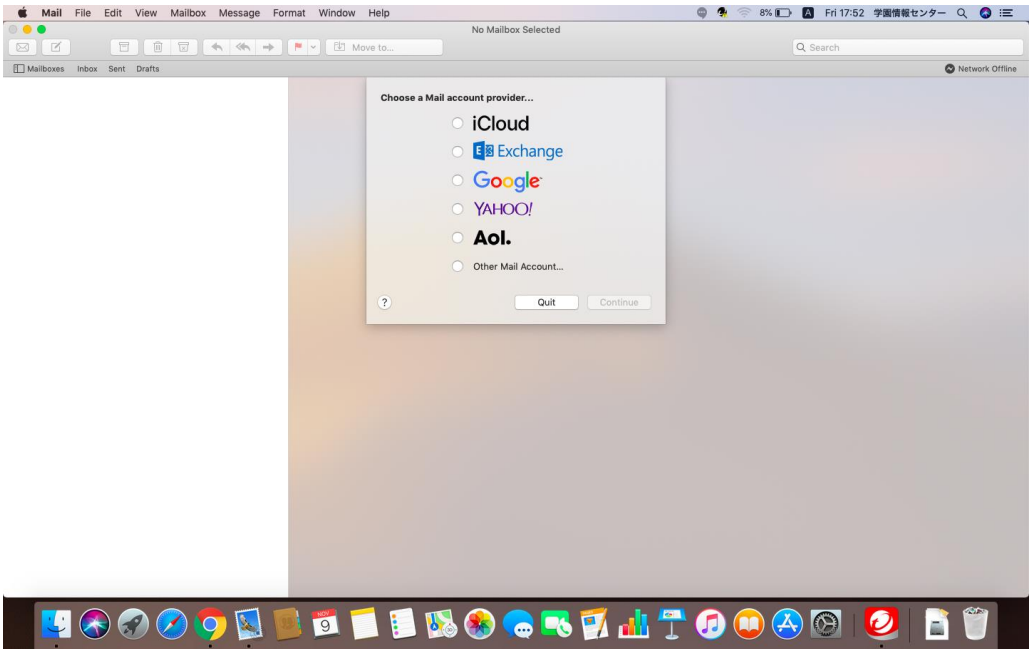
5. メール利用方法 アプリケーション編（例：MacOS Mojave 標準メール）

メールアプリケーションはおおむね同じになりますので、以下を参考にしてください。iOS 12 標準メール、iOS Outlook アプリ、Android Outlook アプリ、Windows 10 標準メール、MacOS 10.14 (Mojave) 標準メール、MacOS 用 Outlook アプリ (El Capitan、Mojave で動作確認）は、原則同様の設定になります。

※Office365　Outlook アプリ版のみ【新しいメールの使い方 Office365 Outlook アプリ編】参照

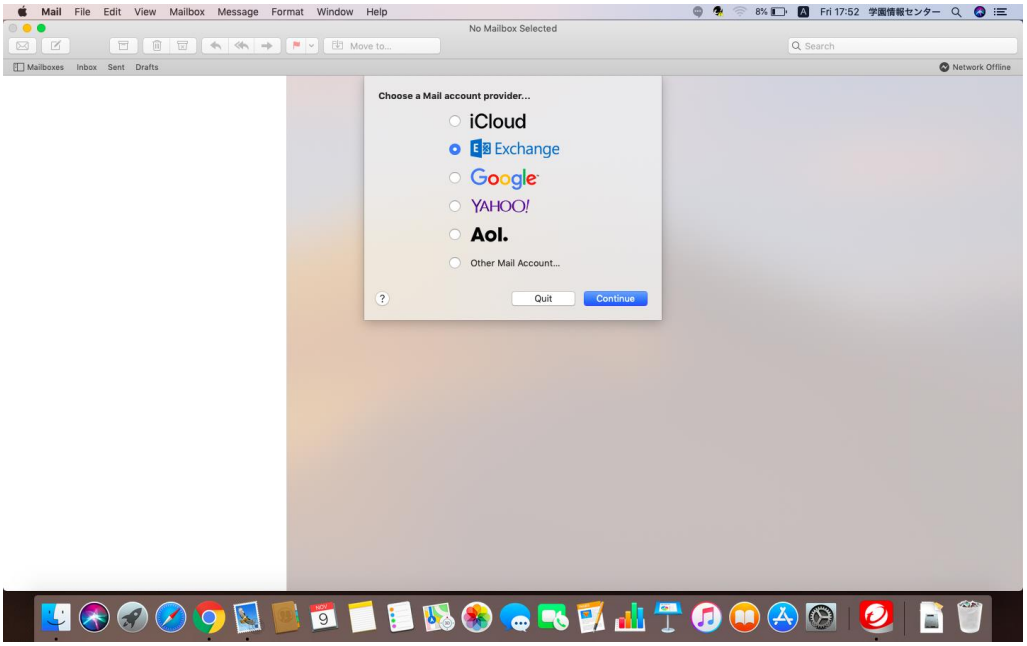
5.1. アカウント登録

メールアプリを起動し、メールアカウントの新規登録へ進む



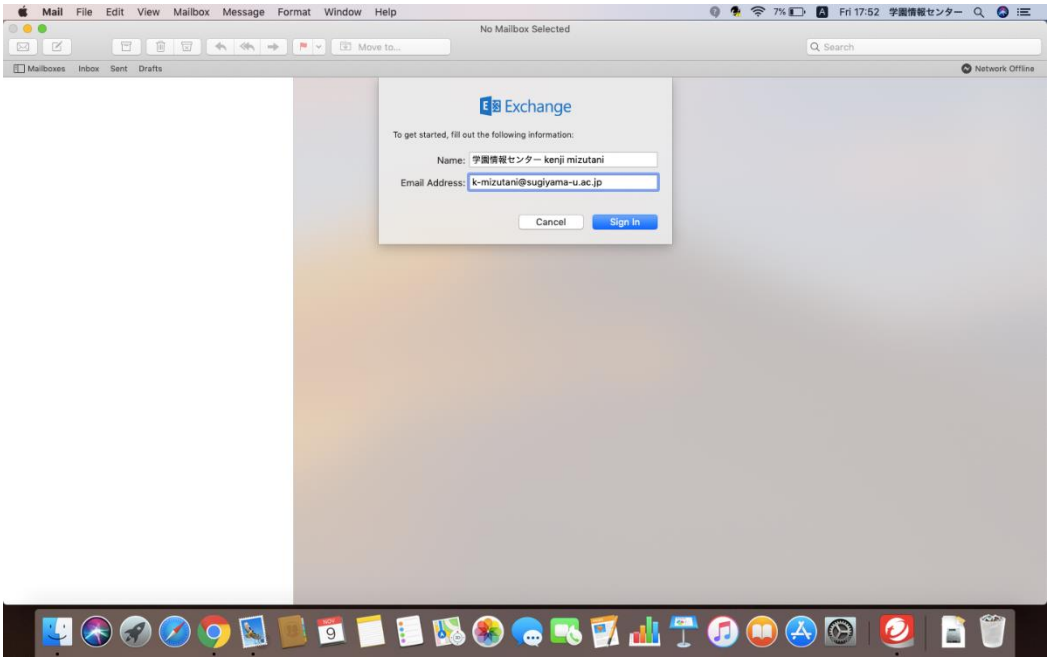
5.3. メールサービスの選択

Exchange を選択して、Continue



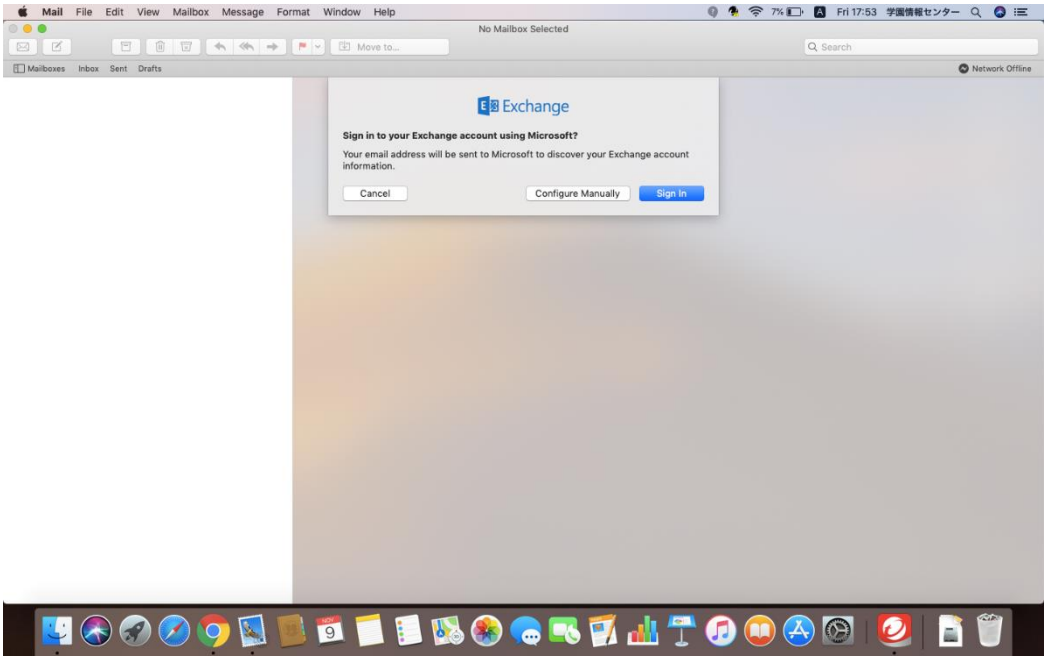
5.4. アカウントの登録

登録名称（Name）には任意の名称、Email Address には、ご自身のメールアドレスを入力。



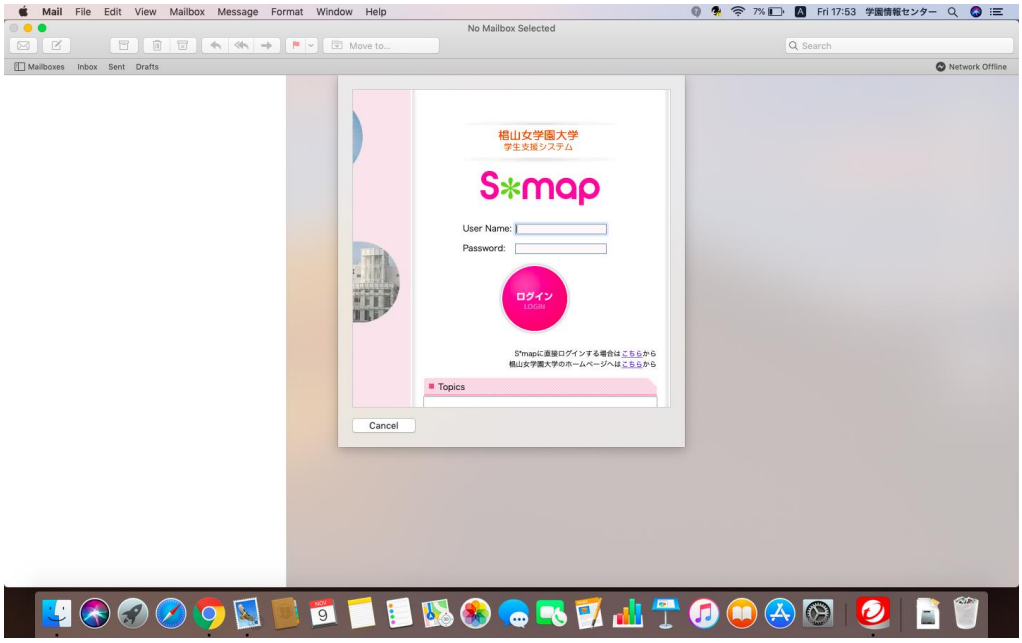
5.6. サインイン

通常は、詳細設定は不要のため、Sing in。



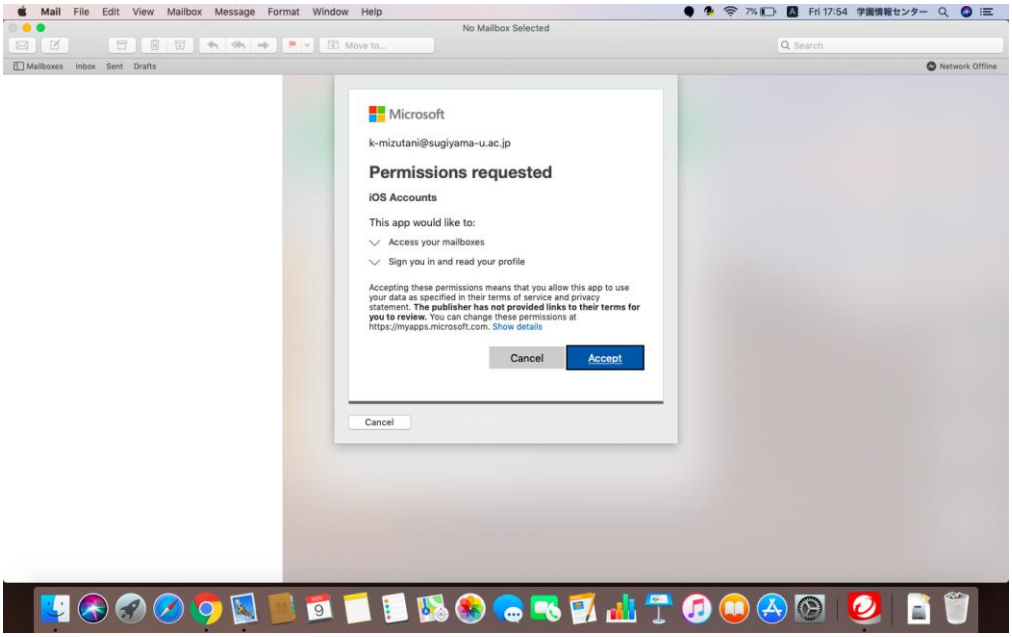
5.8. ログイン

ブラウザでのログインと同一です。

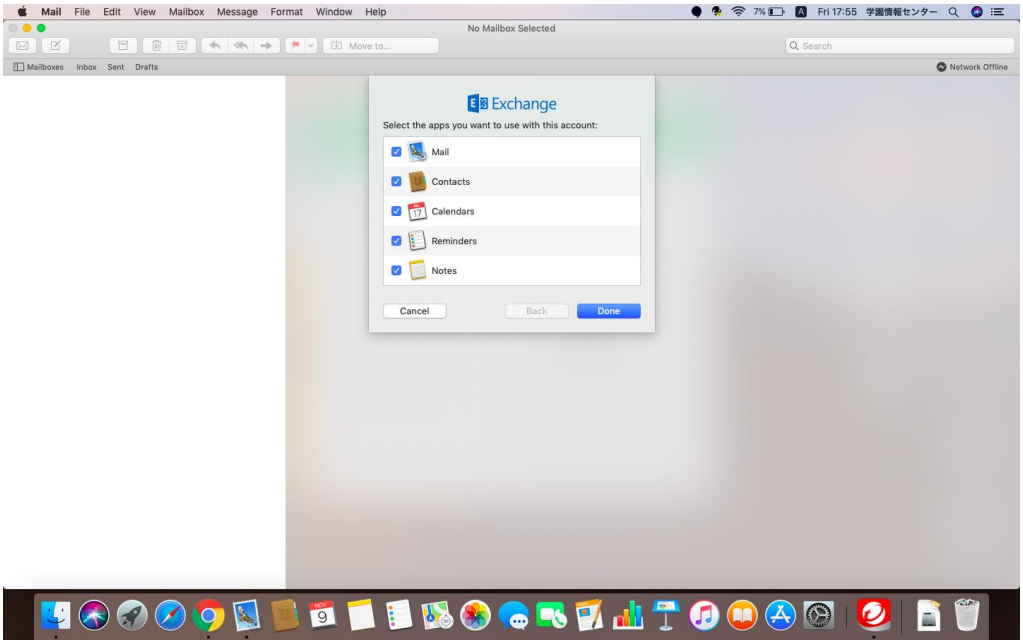


5.9. アクセス権の設定

アプリケーションによっては、アクセス権の確認がありますので内容を確認の上、Accept してください。



アクセスを許可するアプリケーションにもチェックを入れ Continue。



以上で完了です

7. 基本的なメール環境

Office 365 Outlook では、学園情報センターにて以下の設定をおこなっています。

項	機能	設定
1	マルウェア検知	マルウェア（不正ソフトの疑いがあるファイル）が検出された際、情報センターから通知をお送りします。 送受信できませんので、正当な内容の場合、別の手段で送受信を試みてください。 （通知文面は項.8 を参照）
2	添付ファイル フィルター	次のファイルを添付している場合、マルウェアの疑いがあるため送受信禁止となります。 .ace .ani .app .docm .exe .jar .reg .scr .vbe .vbs
3	通知	学園から送信した場合は、送信者へ通知します。 noc@sugiyama-u.ac.jp を使って学園情報センターからメールにてご連絡します。（通知文面は項.8 を参照）
4	スパム フィルター	スパムメールは隔離します。 一日一回、隔離したメールの一覧お送りしますので、正規のメールである場合は手動で隔離状態の解除をお願いします。 （通知文面は項.8 を参照）
5	メールサイズ	35MB 程度

8. マルウェア検知、スパムメールの通知について
学園情報センター（Microsoft 社）から、利用者へお送りする通知は以下になります。下記に当てはまらない場合は、フィッシングメールの可能性がありますので、お問合せください。学園情報センターでは、Web サイト（URL）をクリックしてログイン情報を入力させるような問合せ方法を取っていませんので、ご注意ください。
（2018 年 11 月現在）

8.1. マルウェアを受信した際に、送信されます。心当たりのないメールの場合、対応は必要ありません。心当たりがある場合、送信者に連絡して受信可能なファイル形式で送付いただくか、メール以外の方法をご検討ください。

8.2. 禁止されている添付ファイル形式を送付しようとした際に、送信されます。
送信可能なファイル形式で送付いただくか、メール以外の方法をご検討ください。

8.3. スパムメールを隔離した際の通知メールです。受信して良い内容の場合、受信トレイに開放をクリックしてください。

項	通知	文例	
1	マルウェア検知	**送信者メールアドレス**	**quarantine@sugiyama-u.ac.jp**
		Sender:Sugiyama Jyogakuen Gakuen Jyoho Center Subject: Suspected of malware Gakuen Jyoho Center no Policy niyori kinshi sareteiru kakuchoushi no tenpu file wo kenshutu moshikuha Malware no utagai no aru tenpu fike wo kenshutu shimashita. Detected attachments with extensions prohibited by organization's policies or detected attached files suspected of malware. Otoiawasesaki contact information:172-4531　Gakuen Jyoho Center jyoho@sugiyama-u.ac.jp	

2	添付ファイルフィルター	送信者メールアドレス	quarantine@sugiyama-u.ac.jp

差出人: 学園情報センター
送信日時: 2018 年 11 月 8 日 15:42 <<送信日時>>
宛先: <<メール送信先メール、もしくは氏名>>
件名: 添付ファイルが送信できませんでした

学園情報センターのポリシーにより禁止されている拡張子の添付ファイルを検出もしくはマルウェアの疑いのある添付ファイルを検出しました。

Detected attachments with extensions prohibited by organization's policies or detected attached files suspected of malware.

お問合せ先
contact information:172-4531　Gakuen Jyoho Center jyoho@sugiyama-u.ac.jp

--- Additional Information ---:

Subject: <<送信したメールの件名>>
Sender: <<送信者のメールアドレス>>
Time received: 11/8/2018 6:42:12 AM <<システム時間>>
Message <<メッセージ ID・ランダム>>
ID:OSAPR01MB26121DC0CC6C8B3855614D7D88C50@OSAPR01MB2612.jpnprd01.prod.outlook.com
Detections found:
test.docm　　docm<<ファイル形式>>

3	スパムメール隔離通知	送信者メールアドレス	quarantine@messaging.microsoft.com

<<受信日時>>
<<受信者名>>
受信トレイ

プライバシーを保護するため、このメッセージの一部のコンテンツはブロックされました。ブロックされた機能をもう一度有効にするには、 ここをクリックしてください。
この送信者からのコンテンツを常に表示するには、 ここをクリックしてください。
フラグを設定します。

Office 365

様 <<受信者メールアドレス>>

あなたの受信トレイへの新着メールのうち、Office 365 がスパムと判定したことが理由で受信トレイに配信しなかったものは <<隔離日時>> 時点で <<メール数>> 通ありました。 該当するものをここで確認して、その処理を選択できます。検疫対象となったメッセージに関する情報をさらに取得するには、セキュリティ/コンプライアンス センターの検疫ページに移動してください。ログインするには職場または学校のアカウントが必要です。

このメールからは、次のことができます。
メッセージを解放して受信トレイに戻します。このメッセージがスパムではない場合は［受信トレイに解放］を選択すると、メッセージが受信トレイに送信されます。
このメッセージを Microsoft に送信します。［迷惑メールではないメールとして報告］を選択すると、このメッセージのコピーが分析のために Office 365 から Microsoft に送信されます。

送信者	件名	日付（UTC）	サイズ	解放	レポート
<<送信者名、メールアドレス>>	<< 件 名 >>	<<隔離日時>>	22302	受信トレイに解放	迷惑メールではないメールとして報告

© 2018 Microsoft Corporation. All rights reserved.｜ 利用規約 ｜ プライバシーに関する声明

9. その他

9.1. メールアドレス

山添キャンパス教員の方を除き、着任時に申請した[各自固有の文字列]@sugiyama-u.ac.jp となります。

9.2. 誤って重要なメールを削除した場合の対応

短期間（30 日以内）であれば、ご自身で復元可能です。
それ以降は、復元できません。メールを受信トレイから減らしたい場合は、アーカイブ化や、フォルダへの移動をお願いします。

9.3. 共有パソコンでの利用

ブラウザにログイン情報が記録されている場合、自動的にログインしてしまいます。ブラウザのキャッシュを削除してください。もしくはブラウザのプライベートモードを使用してください。

9.4. 複数アドレスの使用

共有パソコンでの使用と同じくログイン情報が記録されている場合は、自動的にログインしてしまいます。ブラウザのキャッシュを削除してください。もしくはブラウザのプライベートモードを使用してください。

本件に関する連絡先
学園情報センター　内線：172-4531/jyoho@sugiyama-u.ac.jp