YCU メール利用ガイドライン

制　定　　令和２年３月１２日
改　正　　令和８年４月　１　日

第１章　基本的事項

（目的）
第１条　このガイドライン（以下、「本ガイドライン」という。）は、公立大学法人横浜市立大学（以下「本学」という。）情報セキュリティ基本規程（平成 30 年４月１日規程第 32 号）第７条第２項の規定に基づき、本学の教職員等及び学生等（以下、「利用者」という。）を対象に提供する電子メールサービス（ドメインは「@yokohama-cu.ac.jp」「@med.yokohama-cu.ac.jp」「@fukuhp.yokohama-cu.ac.jp」「@urahp.yokohama-cu.ac.jp」「@tsurumi.yokohama-cu.ac.jp」の電子メール、以下「YCU メール」という。）の安全かつ安定的な運用のため、利用者等が遵守すべき事項について定める。

（基本理念）
第２条　YCU メールは、全学における教育・学習・研究・診療を始め学内・学外との連絡・管理・運営等、大学の業務に必要不可欠なものである。利用者は、誤った YCU メール利用が本学全体の機能不全を誘発すれば、結果として本学への信頼や社会的信用を失わせる要因になることを認識し、情報資産の適正な管理に資するよう、本ガイドラインに示す利用ルールを遵守しなければならない。

（利用原則）
第３条　利用者は、本学の情報基盤としての YCU メールを大学の業務、関係者との円滑なコミュニケーション等のために用いることとし、私的な目的で利用してはならない。
２　YCU メールアドレスの発行や廃止、認証など、メールアドレスの運用・管理の詳細については、別途、YCU メールの管理者（以下「管理者」という。）が定め周知を図るとともに、利用者はそれに沿って利用をしなければならない。
３　利用者は、YCU メールの利用において、故意又は不作為を問わず、本ガイドラインを遵守しなかったことにより本学に損害を与え、または、本学の名誉を棄損するなど重大な不利益を与えた場合、懲戒処分の対象となり得ることを認識し、YCU メールを適切に取り扱わなければならない。同様に、利用者を管理監督すべき立場の者は利用者が YCU メールを適切に取り扱うことを指導・管理しなければならない。
４　管理者は、本ガイドラインに従った適切な利用を行わず、他の利用者及び情報基盤運用管理作業に支障を及ぼす可能性があると判断した場合、当該利用者の利用を一定期間停止することができる。また、管理者は法令等の定めや本学の信頼・秩序維持など必要に応じ、利用者に通知することなくメールの送受信記録、本文、添付ファイル等についての調査又は外部への情報提供を行うことができる。
５　管理者は、総務部 ICT 推進課長とする。

（利用環境）
第４条　利用者は、YCU メールの利用にあたり、マルウェア（ウイルスなどの悪意あるプログラム）対策など、セキュリティ対策を施した端末等を使用しなければならない。

（アドレス及びパスワードの管理）
第５条　利用者は、自分の YCU メールアカウントを他人に使用させてはならない。また同様に、他人の YCU メールアカウントを使用してはならない。
２　YCU メールで使用するパスワードの管理については、別に定める「利用者認証で用いるパスワード管理ガイドライン」（平成 30 年 10 月１日施行 以下、「パスワード管理ガイドライン」という。）を遵守しなければならない。
３　利用者は、海外への長期留学・出張や、携帯電話を所持していない等の特別な事情により設定が困難な場合を除き、必ず、多要素（二段階）認証の設定を行わなければならない。なお、その際のパスワード等の管理は、前項のとおりとする。

（添付ファイルの受け渡し方法）
第６条　教職員等は、YCU メールを利用して添付ファイルを学外ドメインアドレスへ送信する場合、誤送信対策として、相手先や情報の重要度に関係なく、添付ファイルはメールから分離して別に格納する方法で

送付するものとする。相手先には格納先からダウンロード形式で取得してもらう仕組みを利用することとする。

第２章　運用指針

（禁止事項）

第７条　利用者は、以下各号に掲げる内容の電子メールを YCU メールで送信してはならない。

(1)　他人を害するもの、脅迫するもの
(2)　他人の個人情報や権利、プライバシーの保護に反するもの
(3)　猥褻なもの、いやがらせ、誹謗中傷など公序良俗に反するもの
(4)　ハラスメント及び差別に相当するもの
(5)　著作権・商標権等の知的財産権、肖像権、ライセンス権等の法的権利に違反するもの
(6)　政治活動や宗教活動のほか、商業目的や勧誘目的に相当するもの
(7)　チェーンメール、スパムメール、ジャンクメール等他の利用者の迷惑となるもの
(8)　その他、本学の信頼や尊厳を棄損するものまたは本学の便益・利益を逸失させるもの

（遵守事項）

第８条　利用者は、電子メールの送受信にあたり、以下各号に掲げる項目を遵守しなければならない。

(1)　大学における業務のメールのやり取りには、特別の理由がない限り、YCU メールアドレスを用い個人が、Google や Yahoo 等のメールサービス提供企業、又はその他の ISP（Internet Service Provider）との間で登録・契約することによって利用できるメールアドレス（以下、「フリーメールアドレス」という。）を使用してはならない。また、やむを得ない場合を除き、自身のフリーメールアドレス宛てに YCU メールを送信、又は転送してはならない。
(2)　誤送信トラブルを防止するため、「メッセージを直ちに送信する」又は「自動送信する」といった初期設定は解除しておかなければならない。
(3)　複数の相手に同じ内容のメールを送る場合で他人のメールアドレスを共有する必要がない場合は、相手毎に個別に送信するか、同報者の名前が表示されない「BCC（ブラインドカーボンコピー）」機能を利用しなければならない。
(4)　個人情報を含むファイルは個人情報適正管理マニュアルに基づきパスワードをかけて送付すること。その際のパスワードの伝達方法は、極力、直前・直後の別メールでではなく、事前に相手先との間で決めたものを用いる、あるいは、電話など異なる経路で伝達しなければならない。

（推奨事項）

第９条　利用者は、YCU メールの送信に際し、以下各号に掲げる事項を参考にして送信先に配慮すること。

(1)　不特定多数の相手に送信する場合、送信先の受信環境に配慮し、文字化け防止のため、機種依存（環境依存）文字は極力使用しない。
(2)　送信先の受信環境によっては、添付ファイル（ファイル転送サーバにアップロードされたファイル）が ZIP 形式や EXE 形式の場合にファイルをダウンロードできないことがあるので、事前に確認する、又はこちらの添付ファイル形式を事前に通知するなどの対応をしておく。
(3)　オートコンプリート機能により予測変換表示された宛先の選択間違い等による誤送信を防止するため、メール送信者名の表記を YCU メールのアドレスであることの判別が付きやすいように適切に設定する。
(4)　メールの作成にあたっては、別掲１の「メールの作法（推奨）」を参考に簡潔な表現を心がける。

第３章　サイバー攻撃対策

（標的型攻撃メール対策）

第 10 条　日頃やり取りがない相手から、別掲２の「標的型攻撃メールの見分け方」の内容に該当するメールを受信した場合、それらは標的型攻撃メールである可能性が極めて高く、また、標的型攻撃の多くがそのメールを開封することから始まることを認識し、原則として、メールは開封せず削除するか、判断が難しい場合は管理者に連絡しその指示に従わなければならない。

（マルウェア対策）

第 11 条　メールに記載された URL や添付ファイルに仕組まれたマルウェアは、インストールさせるための手段が巧妙化していることから、メール等の開封にあたって利用者はそれを念頭において対応しなければ

ならない。また、これらはPCのみならずスマートフォンやタブレット等のデバイスでYCUメールを利用する場合も同様とする。

2　利用者は、標的型攻撃メール等により不審なサイトにアクセスした場合、またはマルウェア感染などが疑われる場合は、直ちに作業を中止し、当該端末等をネットワークから切り離し、管理者の指示に従わなければならない。

3　マルウェア対策は、別掲３の「マルウェア対策（メール編)」に掲げるもののほか、管理者が別に定める「マルウェア等対策手順」により実施するものとする。

（迷惑メール対策）

第12条　広告・宣伝のため、その他無差別・大量に送付される迷惑メールへの対策として、利用者は、以下各号に掲げるとおり対応しなければならない。

(1)　安易に開封、また、返信しない。

(2)　普段からYCUメールのアドレスの公表・通知等については必要最小限とし、慎重に行う。

2　YCUメールに送信されたメールが迷惑メールフィルタによりスパムメールと判定された場合等については、以下各号に掲げるとおり対処する。

(1)　受信トレイにメールが隔離された旨の通知が配信された場合

当該メールが受信できないことで業務に支障が生じる場合は、ICT推進課Webページの FAQ、迷惑メール関連、「Office365迷惑メール（スパム）フィルタについて」の対処法を参考に、受信フォルダに戻す。なお、当該メールは15日を経過すると削除され受信フォルダに戻すことができない。

(2)　迷惑メールフォルダ運用への切り替えについて

迷惑メールフォルダの運用方法の変更は申請によるものとし、申請方法等については、別途、管理者が定める。

第４章　その他

（窓口）

第13条　利用者は、以下各号に掲げる場合、管理者に連絡又は問合せをしなければならない。

(1)　YCUメールの利用において緊急に対応すべき事態が生じた場合

(2)　本ガイドラインの内容について不明な点や確認すべき事項がある場合

(3)　本ガイドラインで定めのない事項について対応が必要な場合

（別掲１）　「メールの作法（推奨)」

【件　名】
・接頭部は、用件を墨付きカッコ等で囲み、主旨を簡潔に示し標題とする。
　〈接頭部の例〉
　【送付】〇〇の資料について、【照会】××について、【回答】××の件について
　【依頼:1/15(水)締切】〇〇について（回答期限がある場合は、用件の後に日付等を記載する）

【署　名】
・送信者を明確にするため、本文の末尾等に署名を記載する。
　また、署名の末尾に本学や当該課等で取り組む課題や標語、URL 等を記載するのも良い。
　〈教職員等の場合の例〉
　　氏名、所属、連絡先（所在地・電話番号・メールアドレスなど)。最後に標語等。
　〈学生等の場合の例〉
　　氏名、学部・学科・学年・学籍番号など。

【本　文】
・原則として、時候の挨拶は省略。先に結論（主旨）を記載し必要に応じ理由等を続ける。また、長文を避け、簡潔な表現になるよう心がける。
・適宜、句読点や改行を入れる。内容が変わるところでは段落を分け、行間を空けるなど内容がスムーズに伝わるよう工夫する。

【配　信】
・会議案内など複数人に同報送信されたメールへの返信は、原則として、「送信者のみ」に行う。
　儀礼的な返信や共有すべき明確な理由がない場合には「全員に返信」の機能は多用しない。
・案件の混同を避けるため、同じ相手に続けて送信する場合でも、案件が異なる場合は、別途、新規メールを作成する。
・緊急その他やむを得ない場合を除き、業務時間外に何らかの返信（回答）を求めるか、そうした印象を与えるメールは送信しない。

【メール送信者名】
・誤送信対策のため、メールの送信者名に所属名等を併記することとする。標記の仕方は所属の事情に合わせて所属ごとに定める。
　〈メール送信者名の例〉
　　市大　学（横浜市大 ICT 推進課)、市大　学（YCU ICT 推進担当）　など

（別掲２）　「標的型攻撃メールの見分け方」

【件　名】
・取材や講演の依頼、問合せ、調査などが掲げられている。
　（本文の URL や添付ファイルを開かないとその真偽が確認できないようになっている。）
・件名が議事録、資料等の開封を促す内容である。
・セキュリティや感染症に関する「注意喚起」や公的機関からの「お知らせ」を装っている。
・システム管理者、金融機関などを装い、受信者に ID やパスワード等の入力をさせようとする。

【差出人】
・フリーメールのアドレスである。
・メール本文や署名に記載された所属やメールアドレスと異なっている。

【本　文】
・日本語の言い回しが不自然である
　（例）公式（公用）文なのに“ハロー!”で始まっている。
　　「〇〇について、あなたは××します。」など、言い回しが直訳的である。
・英文又は通常日本語では使用されない漢字（繁体字、簡体字）が使われている。
・実在する名称、組織名を一部に含め URL が記載されている。
・文字列として表示されている URL と実際のリンク先の URL が異なる。

・本学のメールセキュリティシステムからの警告通知文が差し込まれている。(教職員等のみ)
（例）差出人が本学教職員等で、業務内容に関連した内容にもかかわらず、
メール本文冒頭に以下の一文がある場合、不審メールの可能性が高いです。
■[YCU Notice] 受信履歴・送信履歴のない送信元です。URL 接続要注意。■

※ 生成 AI によるチェック
・送信元のメールアドレスをコピー、生成 AI にペーストし、プロンプトで「このメールアドレスは怪しいか」と聞き、結果を踏まえて正当性を判断する。
・メール本文をコピーし、生成 AI にペーストし、「これはフィッシング詐欺か」とフィッシングの可能性を生成 AI に確認し、結果を踏まえて正当性を判断する。
※ この他、次の情報セキュリティサイト等で公開している事例、傾向、見分け方等を参考にする。
◇IPA（独立行政法人情報処理推進機構）
https://www.ipa.go.jp/security/index.html
◇一般社団法人 JPCERT コーディネーションセンター（JPCERT/CC）
https://www.jpcert.or.jp/at/2020.html

（別掲３） 「マルウェア対策（メール編)」

【準 備】
・次の全てを実施しておく。
①利用する端末等にウイルス等対策ソフトをインストールする。
②定義ファイルを自動的に更新する機能を有効にする。
③電子メールを自動的にチェックする機能がある場合はその機能を有効にする。
④不審な Web サイトを開いたときにウイルス等の混入を阻止できる設定などを行っておく。
⑤オペレーティングシステム（OS）その他のソフトウェアはその都度アップデートし、常に最新の状態を保つ。

【対 応】
①件名や送信元などが不審なメールや添付ファイルを受信した場合は、開かずに削除する。
なお、削除の判断が難しい場合は、管理者に連絡しその指示に従う。
②電子メールで添付ファイルを送信する場合、当該ファイルがマルウェアに感染していないことを確認してから送信すること。
③マルウェア感染に備え重要なデータは一定の頻度で別の機器にバックアップを行い、適宜、復元の手順を確認しておく。