横浜創英大学　電子メール利用ガイドライン

1. 本書の目的

電子メールは日々の学習・教育・研究活動において必要不可欠なものになっている。そのため、電子メールは、ルールやマナーを守った安全な方法で使用しなければ、多くの利用者に迷惑をかけることになる。その上、誤った方法による使用は学習・教育・研究活動の停止や社会的信用を失わせる要因となる可能性もある。

本書は、このようなリスクを軽減し、情報資産を保護し、電子メールを安全に利用するための手順を提供する。

2. 本書の対象者

本書は、横浜創英大学が整備・提供する電子メールを利用するすべての利用者を対象とする。

3. 電子メールソフトの設定

3.1 電子メール受信に係る設定

(1) 利用者は、受信した電子メールをテキスト（リッチテキストを含む。）として表示することとし、偽のホームページへの誘導や不正なスクリプトの実行を未然に防ぐ目的からHTMLメールの利用は注意すること。

(2) 利用者は、アンチウイルスソフトウェアに加えて、電子メールソフトウェア側においてもウイルス対策が設定可能であれば、これを実施すること。

3.2 電子メール送信に係る設定

(1) 利用者は、HTML形式の電子メールを送信しないことが望ましい。これは、当方よりHTML形式の電子メールを送信した場合、それを受信した側の情報セキュリティ水準の低下を招くおそれがあるからである。

4. 電子メールに係る全般的な注意事項

4.1 電子メールの私的利用の禁止

(1) 利用者は、電子メールシステムを、学習・教育・研究活動を遂行する上で必要な場合のみ使用することとし、私的目的のために使用しないこと。

4.2 電子メールの自動転送の禁止

(1) 利用者は、原則として要保護情報を含む電子メールを大学施設（キャンパス）外へ転送することを禁止する。

(2) 利用者は、要保護情報を含む電子メールを大学施設（キャンパス）外へ自動転送する必要がある場合には、メール転送先・理由・期間・セキュリティ対策などを明確にした上で事前に所属長の了解を得ること。

(3) 利用者は、要保護情報を含む電子メールを大学施設（キャンパス）外へ自動転送する必要性がなくなった場合には、その旨を所属長に報告すること。

4.3 大学が整備した電子メールシステム以外の情報システム利用の制限

(1) 利用者は、学習・教育・研究活動遂行にかかわる情報を含む電子メールを送受信する場合には、大学が整備した電子メールシステムを利用することが望ましい。

(2) 利用しようとする情報システム運用基本規定で、明示的に許可されている場合を除き、大学が整備した電子メールシステム以外の情報システム（個人所有の電子メールアドレス等）を用いて電子メールを送受信する必要がある場合には、所属長を得ること。

(3) 利用者は、大学が整備した電子メールシステム以外の情報システム（個人所有の電子メールアドレス等）を用いて電子メールを送受信する必要がある場合には、セキュリティ対策ソフトを導入するなど安全管理措置を講ずること。

(4) 利用者は、大学が整備した電子メールシステム以外の情報システム（個人所有の電子メールアドレス等）を用いて電子メールを送受信する必要性がなくなった場合には、その旨を所属長に報告すること。

4.4 電子メールの監視

(1) 電子メールシステムの適正な利用のため、その利用状況（あて先、内容、添付ファイル等）について証跡の取得、保存、点検及び分析が行われる可能性がある。利用者は、その趣旨を理解の上、電子メールの内容に関するモニタリング及び監査を実施していることを認識すること。

4.5 電子メールID及び電子メールアドレスの管理

(1) 利用者は、他人の電子メールID (電子メールサーバへのログインID。以下同じ。) 及び電子メールアドレスを使用しないこと。

(2) 利用者は、電子メールID及び電子メールアドレスを他人と共用しないこと。

(3) 利用者は、自己に付与された電子メールIDを、それを知る必要のない者に知られるような状態で放置しないこと。

(4) 利用者は、電子メールを利用する必要がなくなった場合は、学生は学生支援課へ、教職員は企画課へ届け出ること。

(5) 特定のサービス、職位、部門単位に付与される電子メールID及び電子メールアドレスのように、電子メールID及び電子メールアドレスを複数の関係者で共用する、あるいは担当者が引き継いで使用する必要がある場合には、利用者はその許可及び設定についてに学生は学生支援課へ、教職員は企画課へ相談すること。

4.6 ニュースグループ、メーリングリスト等の発信機関への電子メールID登録の制限

(1) 利用者は、ニュースグループ、メーリングリスト等(メールマガジン、Webマガジン、フリーメール)への電子メールID登録は、情報セキュリティ情報のメール配信サービスなど、学習・教育・研究活動上必要なものに限定すること。

5. パスワードの管理

5.1 クライアントPCのログイン管理・電源管理

(1) 利用者は、クライアントPCのログインパスワードを設定すること。

(2) 利用者は、クライアントPCを利用しない時にはクライアントPCの電源を切ること。

(3) 利用者は、離席時には、各自が利用しているクライアントPCをロックすること。

5.2 電子メールパスワードの管理

(1) 利用者は、パスワードを設定すること。

(2) 利用者は、パスワードの管理に注意すること。

(3) 利用者は、パスワードを電子メールソフトに永続的に保存しないこと。ただし、電子メールの受信のたびにパスワード入力を行うことが過度に煩雑である場合には、電子メールソフトに一時保存し、クライアントPC起動後のみパスワード入力とする仕組みを利用してもよい。

(4) 利用者は、パスワードを電子メールソフトに一時保存する場合には、当該パスワードを一時保存するクライアントPCを「主体認証情報格納装置」とみなして、以下の点に配慮して安全に取り扱うこと。

- パスワードを保存したクライアントPCを本人が意図せずに使用されることのないように安全措置を講じること。
- パスワードを保存したクライアントPCを他者に付与及び貸与しないこと。
- パスワードを保存したクライアントPCを紛失しないように管理すること。紛失した場合には、直ちに学生は学生支援課へ、教職員は企画課へその旨を報告すること。

6. 電子メールの受信

6.1 電子メールの受信確認

(1) 利用者は、定期的に、電子メールの受信確認を行うこと。

6.2 電子メール添付ファイルのウイルスチェック

(1) 利用者は、アンチウイルスソフトウェアによる自動ウイルスチェックを実施すること。

(2) 利用者は、企画課が自動的にウイルスチェックを実施するように設定している場合又は自動的にウイルスチェック最新データを更新するように設定している場合は、当該設定を変更しないこと。

(3) 利用者は、受信した電子メールの添付ファイルに対して、随時、ウイルスチェックを行うこと。これは、新種のウイルスに対応したパターンファイルの提供が間に合わず、ファイル受信時のウイルスチェックにおいてウイルスが発見されなかった場合を考慮し、最新のパターンファイルを用いて過去に受信した電子メールの添付ファイルに対してもウイルスの有無を確認するための対策である。

(4) 利用者は、緊急時対応が必要な時には、学生は学生支援課、教職員は企画課からの指示に従うこと。

6.3 あて先間違いの電子メールを受信したときの対処

(1) 利用者は、あて先間違いの電子メールを受信し、送信者から正しい受信者へ再度送信する必要がある場合には、可能な範囲で送信者へあて先が間違っていたことを通知すること。

(2) 利用者は、あて先間違いの電子メールを受信した場合には、これを削除すること。

6.4 不審な電子メールを受信したときの対処

(1) 利用者は、不審な電子メールを受信した場合には、電子メールを開かず、学生は学生支援課、教職員は企画課に連絡・相談し、指示を仰ぐこと。

(2) 利用者は、電子メールに不審なファイルが添付されていた場合には、当該ファイルを開くことなく学生は学生支援課に、教職員は企画課に連絡・相談し、指示を仰ぐこと。

6.5 ウイルスに感染したときの対処

(1) 利用者は、クライアントPCがウイルスに感染した場合、又は感染したと疑われる場合には、更なる感染を未然に防止するため直ちに当クライアントPCをネットワークから分離し、学生は学生支援課に、教職員は企画課に連絡・相談し、指示を仰ぐこと。

ネットワークからの分離は、具体的には、ネットワークケーブル、無線LANカード、USBキー型無線LANアダプタなどを取り外す。または、無線LANアダプタがPCに内蔵されている場合には無線LAN機能を停止させる。

6.6 迷惑メールの対処

(1) 利用者は、必要以上に電子メールアドレスを公表し又は通知しないこと。

(2) 利用者は、ネットワークを経由して電子メールアドレスを開示し又は通知する場合には、アドレスを自動収集されないように、工夫を施すことが望ましい。（画像情報で貼付する、意図的に全角文字で表示する、無駄な文字列を前後に接続する等）

(3) 利用者は、送信される迷惑メールに対しては、これを無視することが望ましい。送信者へ停止要求を出した場合、その電子メールアドレスが使用されている事実を伝えてしまう結果となり、かえって迷惑メールが増加してしまう可能性もあるからである。

7. 電子メールの作成

7.1 To、Cc及び Bccの制限

(1) 利用者は、To（あて先）、Cc（カーボンコピー）及びBcc（ブラインドカーボンコピー）の総あて先件数は必要最低限とすること。

・使用するネットワークリソースは、電子メール１件の使用リソース×総あて先件数である。

(2) 利用者は、同時に多数の人へ電子メールを送信する場合、Bccを利用するか、あるいは各自に個別送信する等配慮すること。これは、その場合に電子メールアドレスをTo、Ccに列記してしまうと、当該電子メールを受信した者に、他の者の電子メールアドレスが露呈することになるからである。

7.2　電子メールの形式の制限

(1) 利用者は、HTML形式の電子メールを送信しないことが望ましい。これは、当方よりHTML形式の電子メールを送信した場合、それを受信した側の情報セキュリティ水準の低下を招くおそれがあるからである。

7.4 電子メールの内容

(1) 利用者は、要機密情報を電子メールで送信する場合は別途定められた安全措置を講ずること。

・利用者は、機密性情報を電子メールで送信する場合には、学生は学生支援課に、

教職員は企画課に届け出ること。

・利用者は、要機密情報を電子メールで送信する場合には、安全確保に留意して送信手段を決定すること。例えば以下の手段が挙げられる。

〇 外部を経由しないネットワーク(専用線等)

〇 暗号化された通信路(VPN等)

〇 暗号メール(S/MIME等)

・利用者は、検討の上決定された送信手段について電子メールシステムの部局技術担当者及び上司へ届け出ること。

・利用者は、要機密情報を含む添付ファイルを電子メールで送信する場合には、以下の保護対策の必要性を検討し、必要があると認めたときには、これを実施すること。

〇 添付ファイルに対するパスワード保護

〇 添付ファイルの暗号化(暗号化ソフトの使用等)

(2) 利用者は、要保全情報を電子メールで送信する場合には、電子署名の付与を行う必要性の有無を検討し、必要があると認めたときには、情報に電子署名を付与すること。

(3) 利用者は、電子署名の付与に用いた鍵を適切に管理すること。

(4) 利用者は、他人になりすまして電子メールを作成しないこと。

(5) 利用者は、電子メールを転送する際に、作成者の許可なく内容の変更をしないこと。

(6) 利用者は、個人情報やプライバシーの保護を考慮すること。

(7) 利用者は、次の事項に該当する電子メールの送信を行わないこと。

・ 機密保護違反（情報セキュリティポリシー・情報システム運用基本規定を遵守）

・ 権利違反（知的財産権、著作権、商標権、肖像権、ライセンス権利等）

・ セクシャルハラスメント及び人種問題に関わる内容

・ 非礼及び誹謗中傷

・ ねずみ講に相当する内容

・ 脅迫、個人的な儲け話や勧誘に相当する内容

7.5 ネチケット

(1) 利用者は、チェーンメール（同じ内容の電子メールを別の人に転送するように要請するもの等）の送信・転送を行わないこと。

(2) 利用者は、スパムメール（ダイレクトメール等営利目的を主とした無差別に発信された電子メール）、ジャンクメール（役に立たない情報が書かれている電子メール）等を送

信しないこと。

(3) 利用者は、電子メールに題名を付けること。また、題名は電子メールの内容が分かるように具体的かつ簡潔に書くこと。

(4) 利用者は、俗語的表現やあらかじめ定められていない省略語を使用しないこと。

(5) 利用者は、機種依存文字コードを使用しないこと。

(6) 利用者は、ToとCcとの使い分けを意識し、送信する電子メールに対する返事を要求する時には、To（あて先）を使用すること。

8. 電子メールの送信

8.1 送信時の注意

(1) 利用者は、To（受信者）の記述に誤りがないかを確認してから送信すること。

(2) 利用者は、電子メールにファイルを添付し送信する際に、当該ファイルのウイルスチェックを行うこと。

8.2 電子メールの暗号化

(1) 利用者は、要機密情報を電子メールで送信する場合には、暗号化を行う必要性の有無を検討し、必要があると認めたときは、情報を暗号化すること。

- 暗号メール(S/MIME等)
- 添付ファイルの暗号化(暗号化ソフトの使用等)

(2) 利用者は、暗号化された情報の復号に用いる鍵を適切に管理すること。

(3) 利用者は、暗号化された情報の復号に用いる鍵のバックアップを取得しておくこと。

8.3 添付ファイルのパスワード保護

(1) 利用者は、要機密情報を含む添付ファイルを電子メールで送信する場合には、パスワードを用いて保護する必要性の有無を検討し、必要があると認めたときは、添付ファイルにパスワードを設定すること。

［操作手順］　文書ファイルのパスワードのかけ方（Word®の場合）
Word®の[ファイル]メニューから[名前を付けて保存]を選択した後、[ツール]から[全般オプション]を選択し、[読み取りパスワード]を設定する。

(2) 利用者は、保護に用いたパスワードについては、あらかじめ受信者と合意した文字列を用いるかあるいは、電子メールで送信せずに電話などの別手段を用いて伝達することが望ましい。

8.4 電子メール送信時における情報漏えい防止の確認事項

(1) 利用者は、添付ファイルを電子メールで送信する場合には、当該電子ファイルの付加情報等から不用意に情報が漏えいすることがないか確認すること。

- 「プロパティ」に作成者や修正者等の個人情報が残っていないか
- 一見すると表示されていない部分（「非表示」の設定箇所、非表示としたコメント、裏に隠れたシート等）に要機密情報が含まれていないか
- 変更履歴が必要以上に保存されていないか

8.5 電子メールへの署名付与

(1) 利用者は、要保全情報を電子メールで送信する場合には、電子署名の付与を行う必要性の有無を検討し、必要があると認めたときには、情報に電子署名を付与すること。

(2) 利用者は、電子署名の付与に用いた鍵を適切に管理すること。

8.6 電子メール送信時の受信確認機能の使用制限

(1) 利用者は、トラフィック増を防止するため、電子メール送信時の受信確認は必要最低限の使用とすること。

8.7 電子メールを誤って送信したときの対処

(1) 利用者は、電子メールを誤って送信した場合、相手先（受信者）へのフォローは発信者責任で実施すること。

8.8 ウイルスを送信したときの対処

(1) 利用者は、誤ってウイルスを送信したことが判明した場合、直ちに学生は学生支援課に、教職員は企画課に連絡・相談し、指示を仰ぐこと。

9. 電子メールの保存・削除

9.1 メールボックス（クライアントPC側）における電子メールの保存・削除

(1) 利用者は、本文や添付ファイルに要機密情報が含まれている電子メールを保存する場合

には、暗号化等の措置を講じた上で保存することが望ましい。

(2) 利用者は、本文や添付ファイルに要保全情報が含まれている電子メールについては、適宜バックアップすること。

(3) 利用者は、不要なメッセージは速やかにクライアントPCから削除すること。

(4) 利用者は、本文や添付ファイルに要機密情報が含まれている電子メールを削除する場合には、その機密性に配慮し、復元が困難な状態にすること。

10. 本手順に関する相談窓口

(1) 利用者は、緊急時の対応及び本書の内容を超えた対応が必要とされる場合には、学生は学生支援課に、教職員は企画課に相談し、指示を受けること。

(2) 利用者は、本書の内容について不明な点及び質問がある場合には、学生は学生支援課に、教職員は企画課に連絡し、回答を得ること。