電子メール利用上の注意

本学では，学生，教職員に電子メールアカウントを発行し，情報交換に欠かせない手段として利用されています。

大変便利な電子メールですが，高い利便性の一方で利用者自身が安全配慮を怠ったことによる個人情報や秘匿データの漏えい事件が発生しています。万が一重要な情報が漏えいした場合は，利用者自身や本学の社会的信用を落とすだけでなく，多くの関係者に迷惑をかけることになります。

本学では，システム的なセキュリティ対策を実施していますが，利用するのは「人」です。情報漏えいを防ぐにはみなさんの安全な利用が必須となります。電子メールは情報交換の道具であり，利用方法を間違えるだけで，情報が漏えいする可能性があること，利用者本人が加害者となってしまう可能性があること，甚大な被害を与える可能性があること，を理解してください。

電子メールの安全な利用のために，次の事項に注意してください。

1 強固なパスワードを設定する

本学のパスワードポリシーに従って，強固なパスワードを設定してください。そのうえで，次の文字列を使用しないよう注意してください。

① 辞書に載っている単語
② 氏名，生年月日，電話番号等の個人情報
③ キーボードの配列順
④ ローカルパート（メールアドレスの＠マークまでの文字列）
⑤ 規則的に手を加えた文字列
例：似た文字に置き換える（0とo，Sと$等）
最初だけ大文字にする(pass⇒Pass)
最後に記号をひとつだけ足す(Pass⇒Pass!)
⑥ 同じ文字列の繰り返し
例：PASSPASS

2 パスワードの使い回しをしない

電子メールアカウントを乗っ取られるインシデントが断続的に発生しています。その原因の多くは，メールIDとパスワードを外部のWEBサービスにも使い回していることにあります。

本学発行のメールアカウントを外部サービスに登録する必要がある場合，必ずパスワードを別にしてください。

3 不審なメールの「リンクをクリックしない」「添付ファイルを開かない」

受信メールの中には，個人情報の窃取，受信者 PC の他者攻撃用踏み台化，金銭目的の恐喝等を意図して悪質な動作をする「マルウェア」をインストールさせようとするものがあります。差出人の氏名，メールアドレス，件名，本文の内容を確認し，不審な点がある場合は絶対にメール内のリンクをクリックしたり添付ファイルを開いたりしないで下さい。

万一，不審なメールのリンクをクリックしたり添付ファイルを開いたりしてしまったら，直ちに LAN ケーブルをはずすか無線 LAN をオフにして，サポートデスクに連絡してください。

4 「標的型攻撃メール」の可能性を常に意識する

受信メールの差出人，件名，メール本文の内容に何ら不審な点が感じられなかったとしても油断は禁物です。「標的型攻撃」のメールである可能性も考えておく必要があります。これは，実在する団体やサービスを装ってメールを送りつけ，リンクによって偽のホームページに誘導し，ID・パスワード，個人情報等を盗み取ったり，添付ファイル内のマルウェアをインストールさせて PC を乗っ取り，受信者が所属する組織へのさらなる攻撃を行ったりするものです。リンクをクリックする前に，リンクのアドレスがメール本文の内容と関係するものであるか確認して下さい。添付ファイルならば，それを開く前に，ファイル拡張子の確認やウイルスチェック等により安全であることを確認して

ください。もし安全かどうか判断に迷う場合には，サポートデスクに相談してください。

※不審なメールの見分け方や対応方法，標的型攻撃メールについては以下のページも参照してください。
「不審なメールに注意してください！！」　（学内ネットワークからのみアクセス可）
(http://www.meiji.ac.jp/isc/intra_only/note_email.pdf)

5 メール送信時に宛先を確認する

メールを送信する前に宛先に誤りが無いか，必ず確認してください。メールの誤送信による個人情報の漏えいが起きています。

多数の人にメールを送信する場合は，宛先の「CC」，「BCC」を目的に応じて使い分けをしてください。「CC」で送信すると他の人からもメールアドレスが確認できるため，メールアドレスの流出となりますので注意してください。

CC： 指定した人のアドレスが他の人に見える(誰に送信したか共有したい場合に使用)。

BCC: 指定した人のアドレスが他の人には見えない(誰に送信したか隠したい場合に使用)。

6 個人情報等の機密情報をメール本文に記載しない

メールは他者に盗み見られる可能性を否定できません。個人情報等の機密情報をメール本文に記載しないよう注意してください。

7 機密情報を含む添付ファイルは暗号化する

機密情報を含む添付ファイルを送信する場合には，必ずパスワードをかけてください。パスワードは別メール等で送信するのではなく，郵送など別の方法で送付するか，あらかじめ当事者間で決めておくことが望ましいです。

8 自動転送の設定をむやみにしない

機密情報を含む場合には，別のメールアドレスに転送しないでください。転送先がウイルスに感染する等の理由により，情報が漏えいする可能性があります。

9 PC やスマートフォンのセキュリティ管理をしっかり行う

近頃のネット犯罪は巧妙かつ複雑となっています。自身の PC やスマートフォンにセキュリティソフトを導入する，またはインターネットサービスプロバイダによるセキュリティサービスを利用するよう心掛けてください。

また，OS やセキュリティソフトのアップデートはその都度行い，常に最新の状態にしてください。

電子メールを利用する上で，どう対処したらよいか分からない場合，インシデントが発生した場合には，速やかに各キャンパスサポートデスクへ連絡してください。

【連絡先】

駿河台サポートデスク（12号館7階）	03-3296-4286
和泉サポートデスク（メディア棟1階）	03-5300-1190
生田サポートデスク（中央校舎5階）	044-934-7711
中野サポートデスク（低層棟4階）	03-5343-8072

発行元：　情報メディア部　システム企画事務室

発行日：　２０１８年１２月１０日