

インターネット・電子メールの利用に際し、 気を付ける主なマナー・慣例等のガイドライン

1 インターネット編

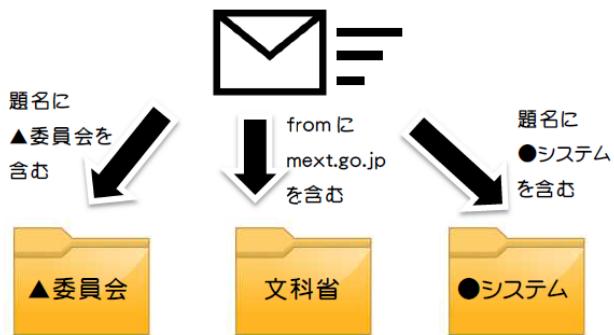
- 1.1 著作権の取扱いに注意しましょう。インターネットで公開されているからといって、これらのコンテンツ（文章、写真、動画、音楽、ソフトウェア等）を無断で利用することは、著作権の侵害になります。必ず適正な方法（引用や著作権者からの許諾を得る等）で利用してください。
- 1.2 “ Wikipedia ” のように便利な百科事典サイトがありますが、掲載されている情報が必ずしも正しいものとは限りません。内容の信頼性については、これだけに頼らず他の手法でも確認や裏付けをするように心掛けてください。
- 1.3 SNS（ソーシャル・ネットワーキング・サービス）はとても便利ですが、便利な故にそこで発信する情報に注意しましょう。自分ではそこまで重要（大したこと）ではないと思っても、他の人にとって同じとは限りません。業務上知りえたことを SNS で発信することは守秘義務に違反する可能性があります。
- 1.4 フリーの Web サービス（翻訳、ファイル共有、ファイル転送、カレンダー等）は必要最低限の利用にとどめましょう。なぜフリーで使用できるのかを十分に理解する必要があります。

2 電子メール編

- 2.1 題名（サブジェクト）はキーワードを用い、できるだけ簡潔にします。
- 2.2 本文には、送信先及び送信者を明記します。
共用アドレス（係のアドレス等）を使用する場合、送信者を名乗らないケースが多々見受けられます。係名はわかったとしても、誰が送信したかは本文を見てもわかりません。必ず明記しましょう。
- 2.3 機種依存文字は使用しません。OS（主に Windows）に設定されているフォントなので、OS 環境が違うと正しく表示できません。現在、丸囲い数字は Unicode（文字コードの業界規格）に含まれるようになり、機種依存文字から外れましたが、積極的な使用はお勧めしません。機種依存文字は環境依存文字という場合もあります。機種依存文字は IME（日本語入力）で文字変換すると右図のように漢字の横に環境依存文字と表示されます。



- 2.4 題名・本文・添付ファイル名に半角カタカナ・機種依存文字は使用しません。日本語メールの送受信に使われるエンコーディングである文字コード（ISO-2022-JP）に半角カナが含まれていないため、文字化けを起こすからです。
- 2.5 業務では HTML 形式のメールは使用しません。原則プレーンテキストのメールを使用します。HTML 形式で送付したとしても、相手が HTML 形式を見られる環境とは限りません。
セキュリティの観点からも HTML 形式のメールをやり取りする事は良くありません。HTML 形式のメールを表示するために、メール内で web ブラウザの描画エンジンが直に動きメール内容が表示されますが、例えばウィルスメールや不正サイトへの自動アクセスメールがチェックもなく開封・表示される危険があります。
- 2.6 メール本文の一行の文字数を調整しましょう。メールの自動折り返し機能などを利用して、見やすい文字幅（例：全角で 36 文字前後）で作成します。
- 2.7 ファイルを添付して、大量のあて先（例えばメーリングリスト等）に送付してはいけません。メールサーバの容量は限りある資源です。たとえ少量の添付ファイルでも何百人と送付することになれば、サーバにかかる負荷はとても大きいです。
- 2.8 不要なメールや添付ファイルはこまめに削除しましょう。メールボックスの空き容量を確保することで、PC を快適に操作することができます。業務上必要なメールや添付ファイルはファイルサーバに保存し、メール側では添付ファイル等を削除するといった工夫も必要です。
- 2.9 メールの「振り分け機能」を活用しましょう。業務によっては、日々受信するメールが 100 件を超える場合もあります。対応が必要なメールが受信箱の中で埋もれてしまわないように、“キーワード”を設定し、振り分け先のフォルダに入るよう整理しましょう。
- 2.10 一度に多くのあて先に送信する場合は、「あて先」に送信先アドレスを入れずに「BCC（ブラインドカーボンコピー）」に入れて送信します。その際のあて先は、送信者自身のアドレスを設定しましょう。そうすることで、送信先アドレスの秘密保持や受信後の誤送信を防ぐことができます。
- 2.11 「返信」と「転送」を区別しましょう。それぞれに使用するテンプレートは異なります。「転送」はメールを引用して送付するのではありません

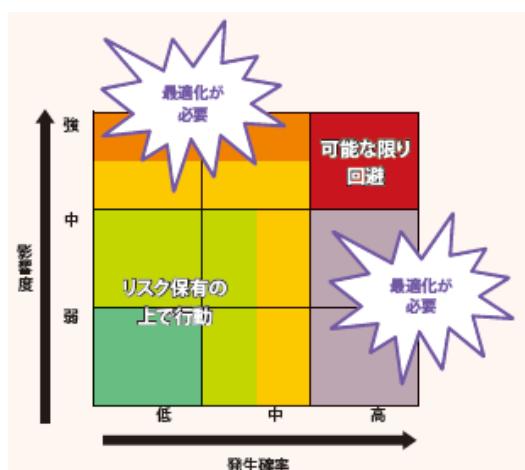


ので、「引用符 (>、|など)」を付けない方が相手も見やすく好まれます。

- 2.12 電子メールはインターネット等を利用し送受信するため、機器の故障等により紛失する可能性があります。重要な連絡の場合は、受信確認を行うよう配慮してください。例えば、外部の方に送る場合は「受信確認の返信をお願いします」や、公募等で申し込みに電子メールで送ってもらう等の場合は「申し込み後 1 週間以内に本学から確認メールを送ります。確認メールが届かなかった場合は 係へ連絡をください。」等の確認を行うことを推奨します。メールの設定で「自分」のメールアドレスを間違えたり、件名を「空欄」で送信したりすると受信側で迷惑メール扱いにされる場合がありますので注意してください。
- 2.13 本学事務局の電子メールは Office365 を使用しています。(2017.7 現在 クラウドシステム) インターネットブラウザを使用してメールサーバにログインしますので、メール専用のソフトウェアは使用しません。
-  **個人のメールボックス 50GBまで**
1メールサイズ 25MBまで
- なお、業務で使用するメールアカウントを外部のフリーメール (gmail、yahoo 等) へ転送しないでください。学外からメールを確認したい方は、情報システム係へその旨相談願います。

3 情報セキュリティ編

- 3.1 個人情報の取扱いには十分に注意してください。取り扱う情報の重大性を認識し、それに見合った対応を行ってください。不安な場合は、上司、同僚又は担当部署等に相談してください。
- 3.2 OS、ソフトウェア、情報セキュリティ対策ソフトは、最新バージョンに更新することを心掛けましょう。
- 3.3 様々なサイトで ID・パスワードの入力を要求されることがあります、これら ID 情報が第三者に見られるような状況にならないよう、適切に管理してください。例えば、Excel ファイルで ID・パスワードを管理し、Excel ファイルにパスワード付ける。
- 3.4 不審なウェブページにはアクセスしないでください。ウェブページへ接続しただけでウイルスに感染するケースが増えています。また、のような URL が記載されたメールが届くケースもありますが、絶対にアクセスしないでください。



- 3.5 身に覚えのないメールには注意してください。送信者が身近な人間だったとしても、メールアドレスを詐称している場合があります。メールヘッダーで送信経路の確認したり、関係部署や周囲の人間に送信状況などを確認・相談してください。
- 3.6 便利だと思っても、信頼性の少ないソフトウェアを不用意にインストールしてはいけません。必ず担当部署に相談してください。
- 3.7 電子ファイルには普通に開いただけでは見えない「プロパティや個人情報」が埋め込まれています。特にデジカメ等で撮影したファイルには、EXIF（エグジフ：写真用メタデータを含む画像ファイルフォーマット）や位置情報が含まれている場合がありますの、ウェブページでの公開や外部へ送る場合等には注意してください。外部に公開する場合、原則としてこれら EXIF 情報は削除する
ようにしましょう。
- 3.8 MS Office のファイルは、必ず最新版の形式で作成するようにしましょう。古いファイル形式（.doc、.xls、.ppt 等）は、最新バージョンの Office ファイルよりファイル自体のセキュリティレベルが低くなっているため、最新の Office ソフトでは使用できない場合があります。特に、既にある古いファイル形式を再使用する場合は、必ず最新形式に変換保存した上で使用してください。



4 その他

- 4.1 クライアント PC での作業は、原則デスクトップにファイルを作成しないようにしましょう。デスクトップは、文字通り「机の上」です。きれいに整理整頓をしましょう。業務用のファイルはファイルサーバで管理しています。本来あるべき場所に作成し、必要に応じショートカット等で対応してください。
- 4.2 ファイルやフォルダは、業務内容を主項目として、年度毎にフォルダを作成しましょう。同じように変更履歴を残す意味でも、必要に応じ日時で世代管理する工夫も必要です。
- 4.3 ファイルやフォルダ名は、記号や空白は使用せず、「_（アンダーバー）」や「-（ハイフン）」を利用し、キーワードを付け簡潔に作成します。
例：DDos サービス不能攻撃_事務連絡_2015.11.25.pdf
- 4.4 作成した文書や資料には、作成（更新）した日及び作成部署名を明記しましょう。（例：右上ヘッダー部に「2018.12.12 総合情報課」など）



- 4.5 明らかに不要なファイルは削除しましょう。なお、不要だと思われるファイルには、後で確認し削除できるように目印を付けましょう（例：「不要__」、「未使用__」など）。
- 4.6 業務で使用するデータ等は、必要に応じバックアップを行うよう心掛けましょう。特に PC のローカルディスクに保存しているデータ等はシステム的なバックアップが行われていませんので注意が必要です。
- 4.7 最近のデジカメは高画質化して、画質によっては 1 ファイル当たりのサイズが数 MB となる場合もあります。保存するハードディスクも“貴重”な“限りある”資源ですので、利用目的に応じて適切な画質で撮影してください。
- 4.8 事務局では PC 操作をすべて記録しています（どこの Web サイトにアクセスしたか、何を実行したか、メールの送受信等）。

以上

長岡技術科学大学の情報セキュリティ関連情報は
こちらのページから確認できます。

公式 HP→ 学内専用ページ

学内限定情報→ 情報ネットワーク・情報セキュリティの取扱い

学内 info→ 情報ネットワーク・情報セキュリティの取扱い

URL : <http://www.nagaokaut.ac.jp/j/gakunai/security/security-top.html>