第4章

デジタル社会のモラルとルール

4-1 コミュニケーションの標準的なルール

インターネットにおけるコミュニケーションのルールについて学習します。

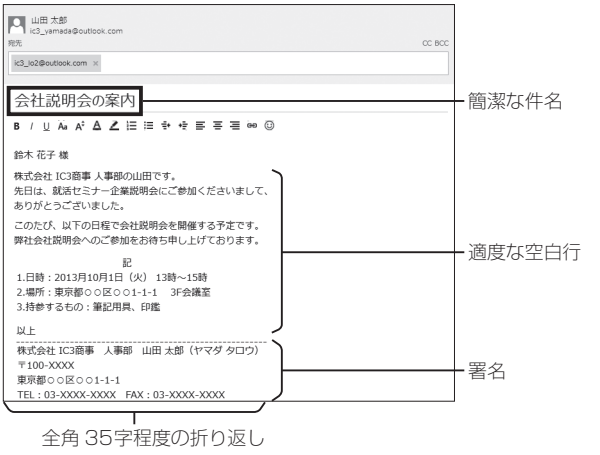
4-1-1 誤字、脱字、適切な表現

電子メールでは、ビジネス用や私用など、目的に合った文体や表現を使ってコミュニケーションを図ります。

コミュニケーション方法の違い

ビジネス用の電子メールを作成する際には、要点を簡潔にまとめ、誤字や脱字がないように注意します。件名は、用件が一目で分かるよう明確に記します。本文は、1行全角35文字程度を目安に改行して、内容の区切りに空白行を入れるなどして読みやすくします。また、同じ部署やチーム内でインスタントメッセージやグループウェアを使う際も、同様にメッセージは要点を明確かつ簡潔にまとめ、誤字や脱字がないように作成します。

良いビジネスメールの例



一方、私用のコミュニケーションにはメールやインスタントメッセージ、SNSなど、さまざまな方法を用います。電子メールはビジネス用と同様に、要点をまとめたり、改行や空白行で読みやすくしたりして、誤字、脱字には注意します。

なお、ビジネス用のパソコンや社内LANを使って、私用のコミュニケーションをとることは、セキュリティやリソース占有などの面で弊害があるので、許可されない限りは控えましょう。

■ 言葉の使い方の重要性

ビジネス用のコミュニケーションではビジネス文書と同様に敬語を用い、適切なスタイルでメッセージを作成します。一方、私用のコミュニケーションでは、くだけた表現やジョークなどを盛り込んで、より親しみのある表現として顔文字を利用してもよいでしょう。ただし、どちらのコミュニケーションにおいても、不快な表現を避けるなど、モラルやマナーを守ることが大切です。

4-1-2 標準的な表記ルール

コミュニケーションにおける標準的な表記ルールとして、次のようなことに注意します。

■ 使用できる文字

電子メールメッセージには、半角カタカナ、特殊な文字や記号は使わないようにします。半角カタカナを使用すると、受信者側で文字化けなどの問題が発生する可能性があります。また、特殊な文字や記号はOSや電子メールソフト、携帯端末の機種に依存している場合が多くあります。特殊な文字や記号を使用すると、受信者側で認識されず、別の文字が割り当てられたり、文字化けを起こしたりする可能性があります。

表4-1　メッセージに使用できる／使用できない文字と記号の例

使用できる文字	ひらがな、全角カタカナ、漢字(JIS第一標準、第二標準)、半角英数字、全角英数字
使用できる記号	、。, . ・ : ; ? ! ゛ ゜ ` ¨ ^ ￣ _ ヽ ヾ ゝ ゞ 〃 仝 々 〆 〇 ― ‐ ／ ＼ ～ ∥ ｜ … ‥ ‘ ’ “ ” ( ) 〔 〕 [ ] { } 〈 〉 《 》 「 」 『 』 【 】 ＋ － ± × ÷ ＝ ≠ ＜ ＞ ≦ ≧ ∞ ∴ ♂ ♀ ° ′ ″ ℃ ￥ ＄ ¢ £ ％ ＃ ＆ ＊ ＠ § ☆ ★ ○ ● ◎ ◇ ◆ □ ■ △ ▲ ▽ ▼ ※ 〒 → ← ↑ ↓ 〓 ∈ ∋ ⊆ ⊇ ⊂ ⊃ ∪ ∩ ∧ ∨ ￢ ⇒ ⇔ ∀ ∃ ∠ ⊥ ⌒ ∂ ∇ ≡ ≒ ≪ ≫ √ ∽ ∝ ∵ ∫ ∬ Å ‰ ♯ ♭ ♪ † ‡ ¶ ○
使用できない記号 (機種依存文字の例)	①②③④⑤⑥⑦⑧⑨⑩⑪⑫⑬⑭⑮⑯⑰⑱⑲⑳ Ⅰ Ⅱ Ⅲ Ⅳ Ⅴ Ⅵ Ⅶ Ⅷ Ⅸ ㍉ ㌔ ㌢ ㍍ ㌘ ㌧ ㌃ ㌶ ㍑ ㍗ ㌍ ㌦ ㌣ ㌫ ㍊ ㌻ ㎜ ㎝ ㎞ ㎎ ㎏ ㏄ ㎡ 平成 昭和 大正 明治 №. K.K. TEL ㊤ ㊥ ㊦ ㊧ ㊨ ㈱ ㈲ ㈹

■ 英文メールの注意点

英文のメッセージを作成する際に、本文のメッセージをすべて大文字のアルファベットで作成すると、「怒鳴っている」や「怒っている」と受け取られる場合があります。頭文字*1などを除き、すべて大文字のアルファベットで記述するのは避けたほうが良いでしょう。強調する単語は斜体や太字にしたり、その文字にアンダーラインを引いたりします。メールソフトに斜体や太字などの文字書式を変更する機能がない場合は、強調する単語の前後に「*」（アスタリスク）を入力します。

4-1-3 話し言葉と書き言葉、ビジネス用と私用の使い分け

インターネット上のコミュニケーションで用いる言葉は大きく分けて、日常会話で使う「話し言葉」と文章で使う「書き言葉」があります。話し言葉は親しみやすさ、書き言葉は用件をより正確に伝えることに適しています。

ビジネス用では主に書き言葉を使い、私用では主に話し言葉を用いますが、ブログなどの不特定多数に公開するソーシャルメディアでは、私用であっても書き言葉や敬語を用いる方が適している場合もあります。

4-1-4 スパムメール、短縮URL、フレーミング、いじめ

インターネットでのコミュニケーションでは、さまざまなトラブルが起こる可能性があります。ここではその代表として、スパムメール、フレーミング、いじめについて学習します。

■ スパムメール

「スパムメール」とは、許可していない業者による宣伝・告知や架空請求など、さまざまな迷惑行為となるメールです。「迷惑メール」とも呼ばれ、相手から一方的に送られてきます。

スパムメールは不特定多数のユーザーに向けて大量に送信されるため、ネットワークやメールサーバーに過度な負荷がかかったり、ユーザーのメールボックスがあふれたりする被害も受けます。加えて、メール本文に書かれているURLをクリックしてしまうと、詐欺のWebサイトに誘導されたり、ウイルスを仕込まれたりするなどの被害にも遭います。

スパムメールを受信したら、基本的には開かずに削除します。本文に記載されているURLをクリックしてもいけません。メールソフトに送信元のメールアドレスやドメインを登録したり、ISPのメールフィルタリングを利用したりして、以降は受信しないようにします。万が一誤ってURLをクリックしても、ウイルス感染の可能性を低くするため、更新プログラムを適用するなどして、常にOSやブラウザーを最新版に更新します。

---

*1 頭文字：欧文で、文章の最初の文字、姓名、地名、固有名詞、略語の最初に使用する文字のことです。

スパムメールが届く原因のひとつとして、メールアドレスの流出が考えられます。掲示板への書き込み、ブログでの公開、身元が定かではない業者の懸賞サイトへの応募、アンケートの回答など、情報の入力には十分な注意が必要です。

表4-2　迷惑メールの種類と対処方法

種類	特徴	対処方法
ダイレクトメール（許可したものを除く）	一方的に、大量かつ無差別に送信される勧誘、宣伝、告知。	返信しない。 メールアドレスやコンピューターの情報を与えてしまう可能性があるため、本文中のURLをクリックしない。
架空請求メール	身に覚えのない架空の有料コンテンツの利用料や情報料を請求する悪質な詐欺。	無視する。 悪質な場合は、国民生活センター、消費生活センター、警察署、弁護士などに相談する。
チェーンメール デマメール	複数の人に宛ててメールの転送を指示するチェーンメール。嘘の情報を記述したデマメール。メールの受信者をあわてさせ、世間を騒がすことを目的とした迷惑メール。	チェーンメールは転送せずに削除する。 デマメールはインターネット検索などで同様のメールが出回っていないか調べ、嘘の情報と判明したら削除する。
フィッシング	銀行やカード会社を装い、口座番号やクレジットカード番号などの個人情報を盗むことを目的とした、本物そっくりの偽サイト（フィッシングサイト）に誘導するメール。	本文内のURLをクリックしない。 差出人名やメールに記載されているURLが、実際に利用している企業のものでも、偽装している可能性があるので、安易に信用しない。
ウイルスメール	メールの添付ファイルやHTML形式のメールに組み込まれたコンピューターウイルス。	不審なメールは開封せずに削除する。 ウイルス対策ソフトを使って検知、駆除する。ウイルスソフトの定義ファイルを常に最新の状態にする。

■ 短縮URL

「短縮URL」は、Webサイトの長いURLを短く表記したURLで、元のURLにリダイレクト*1する機能があります。短縮URLを使うには、短いURLに変換・提供するサービスを利用します。

短縮URLは、Twitterなどの文字数に制限のあるサービスに活用できるのがメリットですが、一方では、元のURLとは異なるURLに変換されるため、ドメイン名がわかりづらくなり、Webサイトの偽装や危険サイトへの誘導などに悪用されるケースもあります。

*1 リダイレクト：「HTTP リダイレクト」ともいいます。Web ページの URL を変更したときに、元の URL から新しい Web ページへ誘導する機能です。

代表的な汎用「短縮URL」サービス

- Google URL Shortener
- bitly
- TinyURL

フレーミング（悪意のある書き込み）

「フレーミング」とは、掲示板やソーシャルメディアなどで、相手を怒らせたり苛つかせたりする目的でメッセージを送信・投稿することです。インターネット上では「あおり」とも呼ばれます。匿名でやりとりされる掲示板やソーシャルメディアなどでは、発言した本人の特定が難しいため、フレーミングをきっかけに炎上することがあります。

相手からフレーミングと思われるメッセージを受け取っても、挑発に乗らず、冷静に返信したり、受け流したりすることが求められます。また、誤って相手にフレーミングと解釈されるメッセージを送信しないように、内容や言葉遣いを注意する必要があります。

いじめ

ソーシャルメディアなどにおいて、特定の個人や企業を誹謗中傷する「いじめ」も起こる可能性があります。いじめの対象とならないよう、メッセージを送信したり、公開したりする前に、内容が適切かどうか確認するとよいでしょう。

ネチケット

インターネットを利用する際のルールやマナーのことを「ネチケット」と呼びます。「ネットワーク上のエチケット」という言葉から生まれた造語です。インターネット上には、ブログ、Twitter、Facebook、チャット、電子メールなどのさまざまなコミュニケーションツールが普及しています。正しく安全に利用するためにはネチケットを守ることが大切です。また、企業や学校では、独自のガイドラインを設けている場合があり、それらを守ることが求められます。

4-1-5 名誉毀損、中傷

掲示板やソーシャルメディアで個人や企業を誹謗中傷する内容を投稿したり、信頼を失墜させるような噂や間違った情報を広めたりすると、「名誉毀損」になります。名誉毀損は刑法上の犯罪にあたり、不法行為として罰せられます。特に匿名の掲示板やソーシャルメディアでは、気軽な書き込みや投稿により、名誉毀損が起こりやすくなります。たとえ匿名でも、不法行為ならISPの協力によって発信者の特定は可能です。名誉毀損を行わないよう、ネチケットを守ってインターネットを利用します。

4-2 合法的かつ責任あるコンピューターの利用

ここでは合法的かつ責任あるコンピューターの利用について学習します。

4-2-1 検閲

インターネットにおける検閲とは、ユーザーがWebページを閲覧する際、コンテンツの内容をチェックし、不適切と判断すればブロックして閲覧できないようにすることです。検索エンジンの検索結果のブロックも行います。また、SNSサイトの管理者は、ユーザーが自分のホームページやソーシャルメディアから発信する情報の内容を確認します。情報が不適切なら禁止したり、削除したりして、情報を発信できないようにします。

Cookieやプライバシーの保護は、ユーザー個人が自分のパソコン上で管理します。それに対して検閲はユーザー個人ではなく、企業や団体や学校のネットワーク管理者、地域、政府によって管理されます。閲覧できるコンテンツや発信できる情報は、管理者によって決められます。

検閲を行うと、不適切な内容のWebページの閲覧や情報発信を未然に防げるメリットがあります。一方、情報統制や言論統制、表現の自由の侵害につながるというデメリットもあります。現在はデメリットの方が大きいとして、問題視されています。

インターネットに接続して、ブラウザーに正しいURLを入力しているにもかかわらず閲覧できなかったり、掲示板やソーシャルメディアへの書き込みが掲載されなかったりした場合、検閲されている可能性があるとわかります。

4-2-2 フィルタリング

「フィルタリング」とは、一定の基準でインターネット上にあるWebサイトを評価して、閲覧を制限する行為です。

フィルタリングを行うソフトウェアのことを一般的に「フィルタリングソフト」と呼びます。フィルタリングソフトは、（フィルタリング）専用のソフトウェアとして提供されていたり、OSやブラウザー、セキュリティソフトに機能の一部として組み込まれていたりします。また、ISPがフィルタリングをサービスとして提供している場合もあります。管理者が閲覧許可を設定したり、履歴をチェックしたりできます。

［保護者による制限］機能：Windows 7には、［保護者による制限］機能が搭載されています。IE 9で閲覧できるWebサイト、コンピューターを使用できる時間帯、利用できるアプリケーションやゲームを制限できます。