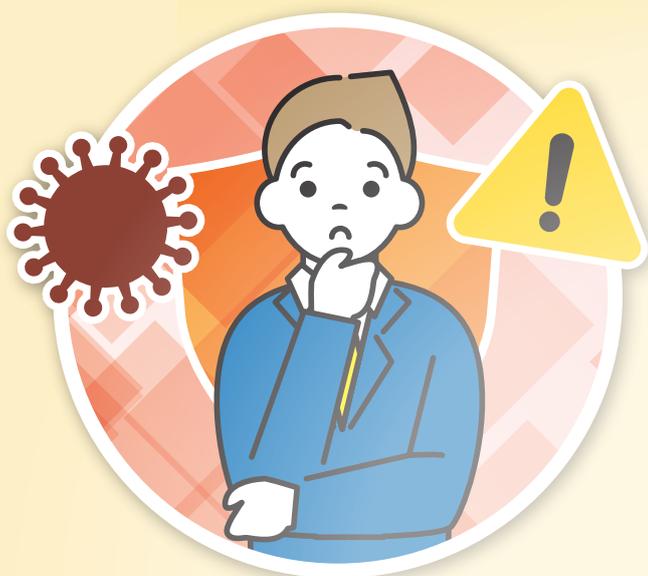


企業に求められる 情報モラル



企業に求められる 情報モラル

はじめに

企業にとって、ICT（情報通信技術）の発達によって、情報の重要性はより一層大きくなりました。業務の生産性を飛躍的に向上させ、インターネットを活用して新たなビジネスモデルも創出しています。

一方で、企業活動に必要不可欠なツールであるICTが、逆に企業の存続を危うくする事態も発生しています。不適切な情報発信による、企業のイメージが損なわれるような事例や、大量の個人情報を流出させてしまい信用が失墜する事例、また他社の知的財産権を侵害するような事例などが後を絶ちません。

経営者の皆様には、お客様や社員をはじめ、多くの人々の人権を守り、情報が持つ力を適切に活用し「情報モラル」の重要性を深く認識し、自社の情報資産をしっかり守り、持続可能な組織として今後も発展し続けるために大切なことだと理解していただきたいと思います。

また、情報を扱う部門の管理者の方や現場の担当者の皆さんも「情報モラル」を尊重することが大切だと理解し、日々の業務に取り組むことが重要です。

本誌を参考に、皆様が「情報モラル」への理解を深め、社内研修等にご活用いただき、組織としてICTを活用するにあたっての情報モラルを構築していただくと幸いです。

目次

1章

企業における情報モラル

企業の社会的責任	2
情報モラルの重要性	3
情報モラル違反による炎上	4

2章

情報モラルとは

2-1 人権への配慮	
人権侵害	6
差別	7
アンコンシャス・バイアス	7
2-2 個人情報の保護	
個人情報保護法	8
最大のセキュリティホール	9
2-3 コンプライアンス	
知的財産権	10
著作権の制限	11
ウェブアクセシビリティ	11
生成AIのモラルリスク	12

3章

情報モラル向上のために

社内ネットワークの規定整備	14
情報セキュリティ委員会の設置	15
教育・啓発・研修の実施	15

参考サイト	16・17
-------	-------

1章

企業における情報モラル

企業の社会的責任

企業が社会の中で果たすべき責任を「企業の社会的責任（CSR：Corporate Social Responsibility）」といいます。それは企業が社会的に守るべき倫理・道徳です。利潤を追求することだけが企業のミッションではありません。企業は社会を構成する一員として社会に貢献することが求められており、顧客（消費者）、社員（従業員）、株主、債権者、取引先、地域社会に支えられています。

国際標準化機構（ISO：International Organization for Standardization）は、企業の社会的責任（CSR）に関する国際規格のISO26000を定めています。ISO26000にはCSRの七つの原則が示されています。七つの原則とは、「説明責任」「透明性」「倫

理的な行動」「ステークホルダーの利害の尊重」「法の支配の尊重」「国際行動規範の尊重」「人権の尊重」です。企業は情報に関する活動においても、社会的責任を果たすことが求められます。



図1 CSRの七つの原則

出典：「CSRとは 活動事例とメリット・デメリット、導入のプロセスを解説」朝日新聞SDGs ACTION、2023.11.08。

情報モラルの重要性

企業が経済活動を行う上で、個人情報や取引先の企業情報など様々な情報を取り扱います。また、企業には宣伝・広報という情報を発信する活動もあります。知名度を上げるための情報発信、顧客に愛着・思い入れ・親近感など持ってもらう、いわゆるエンゲージメントを高めるための情報提供も行っています。

多くの人がソーシャルメディアを使っているネット社会では、情報モラルに反する行為を行えば悪評が短時間で拡散し、企業の経営に大きなダメージを与えます。情報モラル違反による企業のダメージは多岐に渡り、その代償は非常に大きくなります。

長い時間をかけて培ってきた会社の信用が、あっという間に失墜してしまう事も少なくありません。ブランドイメージが損なわれ、顧客離れや不買に発展することもあります。その上、失った信用を回復させるには、多大な労力と長い時間を要することになります。

情報を巡る活動では、企業の社会的責任（CSR）に基づく行動が問われます。情報モラルは、企業の信頼性と持続可能性を支える重要な基盤のひとつなのです。

| 企業に与えるダメージ |

- 組織イメージのダウン → ● 株価の低下
- 社会的信用の低下 → ● 労働意欲、士気の低下
- 顧客離れ、不買 → ● 離職者の増加
- 業績の低下 → ● 就職希望者の減少
- 被害者への損害賠償 → ● 内定辞退者の増加



情報モラル違反による炎上

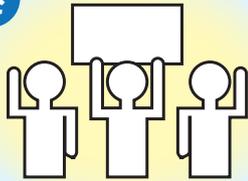
ソーシャルメディアを活用した情報発信では、認知度を上げる効果が期待できます。その手軽さから中小企業には取り組みやすい宣伝広告の手段です。反面、使い方を誤るとネット炎上を起こし、ネットの拡散力が被害を拡大させます。

民間企業にも、ネット炎上を起こして

しまった事例は数多くあります。過去の炎上事例の中で多いのは、男性・女性に関する情報発信で、ジェンダー炎上と言われます。男性・女性の社会的な役割を固定化したような表現は、炎上を招くことが多いため、注意が必要です。

炎上さしすせそ

さ



し



す



せ



そ



- さ 災害・差別 ● し 思想・宗教 ● す スпам・スポーツ・スキャンダル
● せ 政治・セクシャル（含LGBT・ジェンダー） ● そ 操作ミス（誤投稿）

出典：一般社団法人SNSエキスパート協会

ジェンダー炎上の他にも賛否両論がある話題を扱う場合も要注意です。政治的な話題や歴史認識が定まってない戦争の話題等も同様です。

従業員が個人のアカウントを使って、個人の意見を発信することは自由です。しかし、ネット上では炎上すると所属組織が明らかにされて、バッシングの矛先

が所属組織に向けられることがあり、それにより組織イメージの低下につながります。

そのようなトラブルを避けるために、従業員の情報モラル意識を高めるとともに、人権に関する意識も啓発することが重要です。

2章

情報モラルとは

企業の情報モラルとは、企業が情報を扱う際に配慮すべき考え方や行動です。情報倫理とも言います。社会貢献をしながら持続的に発展するための規範、そして他者の権利を侵害することなく健全にビジネスを進めるための規範です。

企業の情報モラルは、3つの分野に分けられます。(1) 人権への配慮、(2) 個人情報の保護、(3) コンプライアンスの3分野です。企業はこれら3つの分野での実践が求められています。

1 人権への配慮

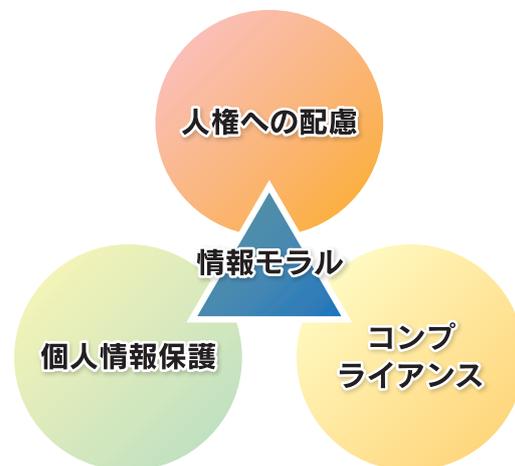
企業の社会的責任（CSR）の七つの原則の1つ「人権の尊重」に基づく行動です。雇用している従業員に対するマネジメントはもちろんのこと、人材を採用する選考での情報の扱いや、社会に向けた情報発信での表記や表現においても人権への配慮が必要です。

2 個人情報の保護

個人情報は犯罪にも悪用されることがある重要な情報です。1件でも紛失や漏えいがあると、重大な事件となりえます。保有している顧客、利用者、消費者の情報は厳密に扱わなければなりません。個人情報の保護に必要なことは、情報セキュリティの整備です。情報セキュリティ事故を防止するために、技術的対策、物理的対策、人的対策を施します。

3 コンプライアンス

法令や社会的ルールを遵守することです。他者の特許や著作権をはじめとした知的財産を尊重します。プライバシー権や肖像権も尊重しなければなりません。生成AIが出力したコンテンツを使う際にも自社の責任の下で権利侵害がないことを確認する必要があります。



2-1

人権への配慮

人権侵害

企業が広報メディアとして公式に採用しているサイトやSNSからの発信はもちろんのこと、従業員が使用している個人アカウントからの発信についても、不適切な投稿には気を付けなければなりません。個人からの投稿であっても炎上を招けば、所属組織に対するバッシングに発展して、組織にダメージを与えることとなります。

企業が業務利用のために整備したネットワークについては、企業内で策定された情報セキュリティポリシーで利用規定が定められています。それに加えて、人権への配慮を行うにあたって必要なことは、従業員が使用している個人アカウントの使い方についてソーシャルメディア利用ガイドラインを策定することです。

ソーシャルメディア利用ガイドライン

の整備は、企業の情報モラルとして重要なものです。ガイドラインを整備していないと、社会的責任に基づく説明責任を果たすことはできません。

万一、人権を侵害する不適切な投稿があれば、侮辱罪や名誉毀損罪を問われる恐れや、民事上では損害賠償責任を負う可能性もあります。



情報流通プラットフォーム対処法 令和6年5月17日公布

正式名称：特定電気通信による情報の流通によって発生する権利侵害等への対処に関する法律

誹謗中傷のインターネット上の違法・有害情報に対処するため、**大規模プラットフォーム事業者に対し、①対応の迅速化、②運用状況の透明化**に係る措置を義務づける法律です。

①対応の迅速化

- ・削除申出窓口、手続の整備、公表
- ・削除申出への対応体制の整備（十分な知識経験を有する者の選任等）
- ・削除申出に対する判断、通知（原則、一定期間内）

②運用状況の透明化

- ・削除基準の策定と公表（運用状況の公表を含む）
- ・削除した場合、発信者への通知

差別

差別の被害者は、決して一部の限られた分野の人だけではありません。日本には同和問題という部落差別の問題が存在しています。また、障害のある人や生活困難者、人口の半数を占める女性も差別を受けることがあるとされています。そ

の他、性同一性障害、少数民族、犯罪被害者、刑を終えた人など考えていけば、差別の被害者は多く存在します。

企業は社会の一員として、差別する表現や差別を助長する表現の発信は慎まなければなりません。

アンコンシャス・バイアス

無意識の偏見をアンコンシャス・バイアスといいます。それは、経験、習慣、常識、固定観念による思い込みです。思い込みが決め付けとなり、差別意識となるのです。

会社の公式サイトに掲載した記事や公式アカウントから投稿した記事の中に偏見に基づく記述があれば、会社自体が偏見を持っている組織だと見なされる恐れ

があります。偏見の記述を含まない情報発信を心がける必要があります。

偏見によるトラブルを起こしてしまった企業は、ほとんどが自ら企業イメージを低下させようとして発信しているわけではありません。偏見が含まれていることに気が付かないまま発信している事がほとんどです。そこにあるのは、アンコンシャス・バイアスなのです。

アンコンシャス・バイアスの例



2-2

個人情報の保護

個人情報保護法

企業が所有する機密性の高い情報に、顧客の個人情報があります。お客様から預かった個人情報を1件でも流出させると大きな問題となります。

取り扱う個人情報の数に関わらず名簿を管理している事業者は、すべて個人情報保護法が対象とする「個人情報取扱事業者」になります。事業者の中には、マンションの管理組合、NPO法人、自治会、同窓会などの非営利組織も含まれます。

外国人に関する情報も、国籍の区別なく、特定の個人を識別できる情報であれば、個人情報に当たります。日本国内の

個人情報取扱事業者が、外国に住む外国人の個人情報を取得・利用・提供する場合には、個人情報保護法に従った取扱いが必要になります。

写真も映像も特定の個人を識別することができる場合には、個人情報に当たります。テープに記録された音声データも保護対象の個人情報です。

個人情報の種類は、個人情報保護法の改正のたびに追加されており、現時点では「特定個人情報」「個人識別符号」「要配慮個人情報」などが定められています。

個人情報の内容と種類

●個人情報

生存する個人の情報であって、特定の個人を識別できるものや、個人識別符号が含まれるもの

●特定個人情報

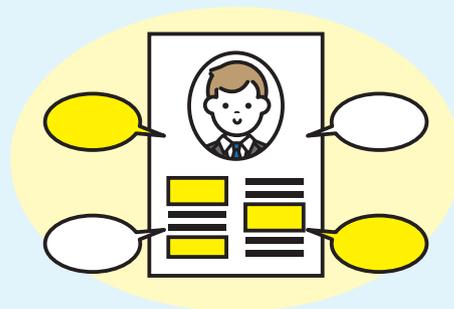
氏名、生年月日その他の記述等で特定の個人を識別できるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができるものを含む）

●個人識別符号

個人の身体の特徴（指紋、虹彩、声紋、静脈、顔など）をデータとしたものや、サービス利用等において利用者ごとに割り振られる符号（旅券番号、運転免許番号、マイナンバーなど）

●要配慮個人情報

本人の人種、信条、社会的身分、病歴、犯罪の経歴、犯罪により害を被った事実その他本人に対する不当な差別、偏見その他の不利益が生じないようにその取扱いに特に配慮を要するもの

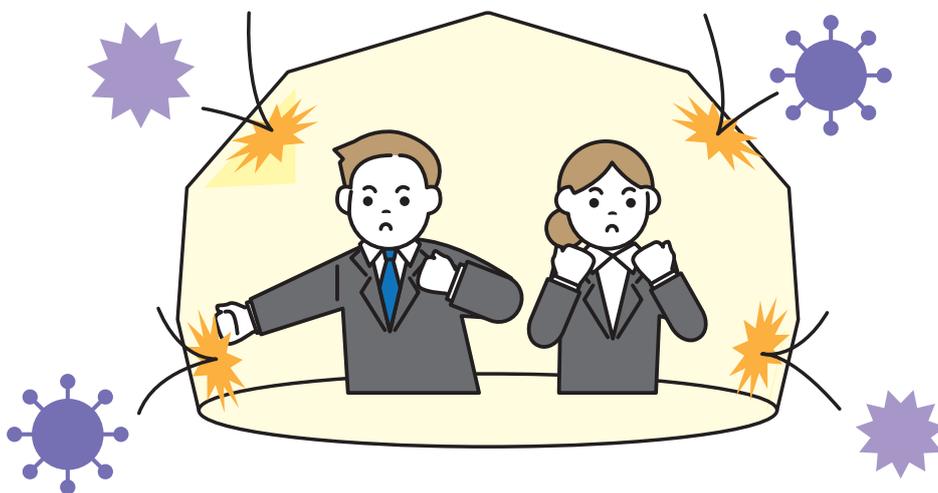


最大のセキュリティホール

昨今、サービス、医療・福祉、教育、行政など様々な分野で個人情報の流出事故が起きています。不正アクセスや盗難など外部要因もありますが、業種を問わず情報セキュリティ事案の半数以上が「紛失、誤送信、誤操作、置き忘れ」などの人的ミスによって引き起こされています。このことから情報セキュリティ上の最大の脅威は人的ミスと言えます。つまり、

最大のセキュリティホールは「人」です。

情報セキュリティ対策には主に3種類あります。「技術的対策」「物理的対策」「人的対策」です。人が最大のセキュリティホールであることから、特に人的対策には重点的に取り組む必要があります。組織において、人的ミスを防止するための対策が極めて重要なのです。



参考：「情報セキュリティに関する調査研究」2022年度調査研究報告書、
西東京市情報政策専門員 佐藤佳弘、2023年3月31日、P.2

情報セキュリティ対策の3分野

技術的対策

ハードウェアやソフトウェアによる対策。
ウイルス対策ソフトの導入や暗号化によるデータ保護など

物理的対策

機器、設備による対策。
ドアの施錠、生体認証の導入、監視カメラの設置、警備システムの導入など

人的対策

ミスや不正など、人によるセキュリティリスクに対応するための対策。
教育・研修の実施、マニュアル・ルールの整備など

2-3

コンプライアンス

知的財産権

知的財産は企業活動の生命線ともなる重要な情報です。知的財産には、著作権をはじめとして、特許や商標などいくつかの種類があり、それぞれが法令によって保護されています。

企業が時間とコスト、労力をかけて築き上げてきた知的財産に敬意を払うこと

はビジネス上の作法であり、重要な事項です。もちろん、自社の知的財産は守らなければなりません。そして、他社の知的財産を無断で利用したり、盗み取るとは、刑事上の責任を負うこともある重大なモラル違反です。

No.	知的財産権	根拠となる法律	保護対象
1	特許権	特許法	発明
	実用新案権	実用新案法	物品の形状、構造等に関する考案
	意匠権	意匠（いしょう）法	工業デザイン等
	商標権	商標法	商品やサービスを表す表示
2	著作権	著作権法	著作物
3	半導体回路配置利用権	半導体集積回路の回路配置に関する法律	半導体集積回路の回路配置
4	育成者権	種苗法	植物の新たな品種
5	営業秘密	不正競争防止法	営業秘密

※近年、知的財産権の対象は拡大される傾向にあり、今後、上記以外にも様々なものが保護の対象となる可能性があります。



著作権の制限

文章、イラスト、写真、動画、音楽など、人の手によって創作されたコンテンツは、著作権法によって保護される著作物です。複製を作る行為や改変する行為、またネットに掲載する行為は、著作権者の許諾を得ずに行えば著作権法違反となります。

ただし、著作権者の許諾を得ずにも自由に使うことができるケースもあります。著作権法 30 条から規定されている著作権制限規定に該当する場合があります。

誰もが恩恵に預かっているのは、「私的使用のための複製」です。新聞や雑誌は著作物ですので、会議や打合せで配布す

るためにコピーをとると著作権法違反（複製権侵害）となります。しかし、自分のためのコピーは「私的使用のための複製」ですので、著作権侵害になりません。

引用も著作権法が認めている行為であり、著作権者の許諾を得ることなく著作物を使用することができます。ただ、引用は公正な慣行に合致し目的上正当な範囲内で行う必要があります。出所を明記するなどのルールがあるので、文化庁が公表しているガイドラインに従って、正しく引用してください。

ウェブアクセシビリティ

高齢者や障害者を含め、誰もがウェブで提供される情報や機能を支障なく利用できることがウェブアクセシビリティです。利用者の障害の有無や程度、年齢や利用環境に関わらず、ウェブで提供されている情報やサービスを誰もが利用できることが理想です。誰もがアクセスできるホームページのデザインをウェブのユニバーサルデザインといいます。

例えば、目が見えない人は、スクリーンリーダーを使ってウェブ上の文字を認識します。もしも「日 時」と空白文字

を挟んで示されていると、「[にちじ]」ではなく「ひ、とき」と読み上げます。これでは意味がわかりません。空白文字を挟まずに「日時」と表示する必要があります。

厚生労働省によると障害者手帳の所持者は 610 万人と推計されています。そのうち視覚障害は 27 万 3 千人、聴覚・言語障害は 37 万 9 千人、肢体不自由は 158 万 1 千人です。ウェブアクセシビリティの恩恵を受ける人は、多く存在していることがわかります。

ウェブの望ましいデザイン

- 目が見えなくても情報が伝わる・操作できること
- キーボードだけで操作できること
- 一部の色が区別できなくても情報が欠けないこと
- 音声コンテンツや動画コンテンツでは、音声がかえなくても何を話しているかわかること



出典：「ウェブアクセシビリティ導入ガイドブック」デジタル庁、2024年3月29日発行、P.9

ウェブで提供されている情報や機能を利用できないということが起きないように、

その時々ルールに対応したホームページを作成することが求められています。

| JIS X 8341-3 |

正式名称「高齢者・障害者等配慮設計指針—情報通信における機器、ソフトウェア及びサービス—第3部：ウェブコンテンツ」ウェブアクセシビリティに関する JIS 規格
高齢者や障害のある人を含む全ての利用者が、使用している端末、ウェブブラウザ、支援技術などに関係なく、ウェブコンテンツを利用することができるようにすることを目的とした JIS 規格。
なお、8341は「やさしい」から来ています。

生成 AI のモラルリスク

生成 AI は、予め与えられた学習データやネットから得た情報を基に文章、画像、音楽などを生成する人工知能です。業務生産性の向上が期待される反面、権利侵害などの情報モラル上のリスクも懸念されています。

通常の生成 AI は、コンテンツの生成時に使用した情報の引用元を明らかにしていません。そのため生成 AI が出力したコンテンツには、著作権、商標権、意匠権、

肖像権、パブリシティ権、プライバシー権などの権利を侵害しているリスクが潜んでいます。

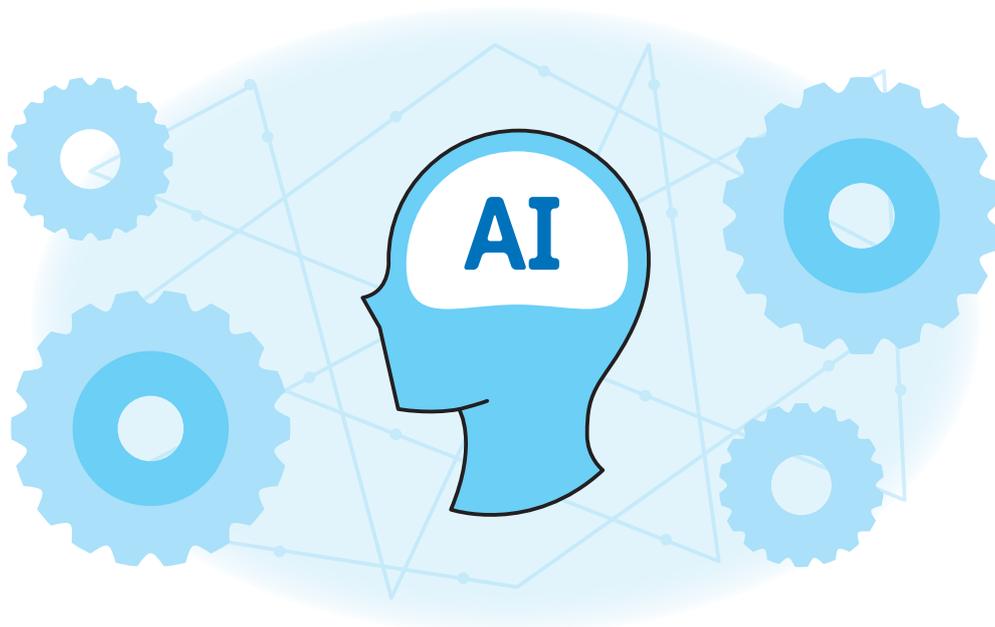
また、生成 AI が参考にした情報の真贋も保障されていません。従って、出力したコンテンツに誤情報が混じる危険があります。ネットサーフィンで得られた情報を利用する場合と同様に、利用者自身が生成 AI の出力内容を慎重に確認することが必要です。

| AI の懸念・リスク |

- ・ プライバシーの侵害、犯罪への使用など人権や安心を脅かす行為にどう対処するか？
- ・ 機密情報の流出、サイバー攻撃の巧妙化などセキュリティ上のリスクにどう対処するか？
- ・ 誤情報、虚偽情報、偏向情報等が蔓延する問題にどう対応するか？
- ・ AIが知的財産権を脅かしていないか？
- ・ 透明性をどのように確保すべきか？
- ・ AIの利用に当たっての責任をどのように考えるか？
- ・ 諸外国におけるルール形成、国際的な規律・標準の検討などにどのように対応するか？



出典：内閣府「AIを巡る主な論点」第1回AI戦略会議（2023年5月11日）資料2、P.4



出典：かんでんCSフォーラム

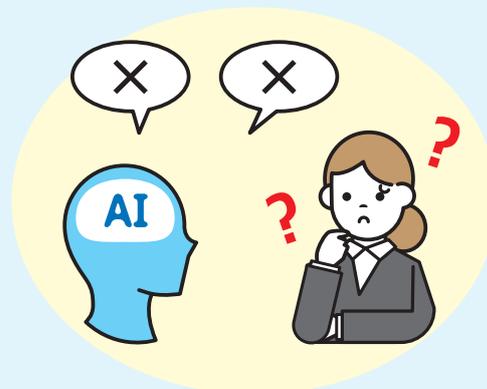
権利侵害の他には情報漏えいのリスクもあります。利用者が入力した情報が学習データとして利用されることがあるからです。そのため、個人情報やプライバシー情報を入力すると情報漏えいにつながる恐れがあります。個人情報の入力には第三者提供と見なされ、個人情報保護法

違反を問われるリスクもあります。

生成 AI が出力したコンテンツについては、無条件に利用するのではなく、利用するにしても、事前に利用上のガイドラインやチェックルールを策定しておくことが重要です。

| ハルシネーション (hallucination) |

人工知能 (AI) が事実に基づかない情報を生成する現象。「でっち上げ」と言われます。インターネット上の情報には誤りや偏りが含まれています。ネット上のデータを学習している場合、適切な回答を生成できず、ハルシネーションが発生すると考えられています。ハルシネーションを完全に防ぐ方法はないため「生成 AI が間違った情報を提示する可能性がある」という前提で利用することが大切です。



3章

情報モラル向上のために

社内ネットワークの規定整備

組織が整備したネット環境

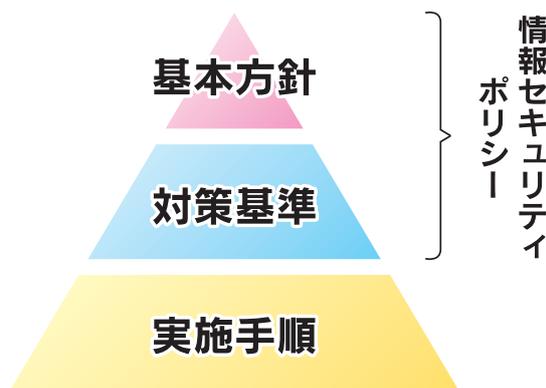
組織が整備したネットワークの利用について規定を整備します。不正アクセス、プライバシー侵害、誹謗中傷、セクハラ、その他の違法目的での利用、業務外利用などの禁止事項を明記します。これらの禁止事項は、情報セキュリティポリシーにも記載される事項となります。

チェック体制の整備

公式アカウントから発信する内容についてチェック体制を整備します。全ての投稿を上司が事前に決裁する方式や広報部門が決裁してから発信するという従来の書類ベースの手続きでは、ネットの速

ソーシャルメディア利用ガイドライン

個人アカウントでのソーシャルメディア利用に関するガイドラインです。個人のアカウントだから「従業員の良識に任せればよい」という整理では組織のリスクマネジメントとして、十分ではありません。個人アカウントからの投稿でも炎



報性を失ってしまいます。ネットの特性を活かしたタイムリーな情報発信を実現させるためには、現場でのダブルチェックなどフットワークの良いチェック体制を検討することが重要です。

上すれば所属組織にダメージを与えるからです。もし、ガイドラインを整備していない段階で情報モラル違反の重大な事案が発生した場合、企業は「ガイドラインすらなかったのか」として二重の責任を負ってしまう可能性があります。

ソーシャルメディア利用ガイドラインの項目例

1. 法令遵守
2. 守秘義務と機密保持
3. プライバシーの保護
4. 人権や倫理の尊重
5. 免責文の記載

(免責文の例)〇〇の所属であることを明らかにして投稿する場合には、自身の発言、行動が〇〇の意見・見解を代表、代弁するものではないことを明記してください。

情報セキュリティ委員会の設置

トラブル事案に迅速に対応する組織が情報セキュリティ委員会です。情報に関するトラブルの報告を受けた管理職は、すぐさま情報セキュリティ委員会に報告します。被害者の救済、マスコミ対応、削除手続き、仮処分申立て、法的措置などは、情報セキュリティ委員会が統一的な窓口として動くこととなります。

情報セキュリティ事案は、一刻を争うため即座に対応しなければなりません。放置するとネット炎上等に発展し、時間の経過と共に被害が広がるからです。いち早く火消しの対処をして、それ以上の

拡散を防がなければなりません。その役割を担うのが情報セキュリティ委員会です。



教育・啓発・研修の実施

規定やルール、ガイドライン、情報セキュリティポリシーなどを整備した後は、教育・啓発・研修を実施して周知徹底を図ることが重要です。そのため、情報モラル研修の実施が求められます。情報モラルの基礎知識を得ると共に、モラル意識を高めるための研修です。情報モラル研修は、2つの側面から行う事が一般的です。それは、コンプライアンスの側面と情報セキュリティの側面です。

コンプライアンス研修では主に権利侵

害を扱います。情報セキュリティ研修では主に情報の扱い方を扱います。この2つを情報モラル研修として実施することが望まれます。

情報モラルの意識向上のためには、毎年度の継続した情報モラル研修の実施が重要です。対象者は、正社員だけでなく、契約社員、派遣社員、パート、アルバイトも含まれなければなりません。また、役員など経営層も含めるべきでしょう。

情報モラル研修

●コンプライアンス研修

- ・人権
- ・著作権
- ・肖像権、プライバシー権
- ・バブリティ権
- ・商標権、意匠権、特許権

●情報セキュリティ研修

- ・個人情報
- ・特定個人情報
- ・個人識別符号
- ・秘密情報、顧客情報
- ・標的型攻撃への対策

参考サイト

◆中小企業庁 人権啓発支援

https://www.chusho.meti.go.jp/soudan/jinken_pamf/index.html

◆経済産業省 ビジネスと人権～責任あるバリューチェーンに向けて～

<https://www.meti.go.jp/policy/economy/business-jinken/index.html>

◆法務省 人権擁護局

<https://www.moj.go.jp/JINKEN/index.html>

◆政府広報オンライン ウェブアクセシビリティとは? 分かりやすくゼロから解説!

<https://www.gov-online.go.jp/useful/article/202310/2.html>

◆デジタル庁 ウェブアクセシビリティ導入ガイドブック

<https://www.digital.go.jp/resources/introduction-to-web-accessibility-guidebook>

◆個人情報保護委員会 個人情報保護法等

<https://www.ppc.go.jp/personalinfo/>

◆特許庁 知的財産権について

<https://www.bunka.go.jp/seisaku/chosakuken/seidokaisetsu/chitekizaisanken.html>

◆内閣府 AI戦略

<https://www8.cao.go.jp/cstp/ai/index.html>

◆独立行政法人情報処理推進機構(IPA) 情報セキュリティ教材

- ・今こそ考えよう 情報モラルセキュリティ
<https://www.ipa.go.jp/security/imakoso/>
- ・一般初心者向け情報セキュリティ教材
https://www.ipa.go.jp/security/sec-tools/general_security_materials.html
- ・5分でできる！情報セキュリティポイント学習（企業向け・学校指導者向け）
https://www.ipa.go.jp/security/sec-tools/5mins_point.html

経済産業省中小企業庁委託事業

ウェブサイト：www.chusho.meti.go.jp/soudan/jinken_pamf/index.html

公益財団法人ハイパーネットワーク社会研究所

〒870-0037 大分県大分市東春日町51-6 大分第2ソフィアプラザビル4階

TEL 097-537-8180 FAX 097-537-8820

メール：info-moral@hyper.or.jp ウェブサイト：www.hyper.or.jp

〈2024年12月発行〉