Ｐマークニュース

＜２０２４年新春号＞　Vol. ４６

株式会社トムソンネット　Ｐマークコンサルティンググループ

目 次 と 記 事 概 要

生成 AI は、「社会を根底から変え秩序を破壊する変化」を生むとされ、社会、事業活動、生活の各分野での論議が盛んになっています。また、生成 AI 利用者の拡大に伴い、リスクも増大しています。

2024 年 1 月に総務省・経済産業省が示した、事業活動における生成 AI に対するガイドライン（パブコメ中 2024.1.20～2.19)を参照しながら、今回は、生成 AI 利用の原点とも思われる「人間中心の原則」に基づき、プライバシー・個人情報保護について概観します。

「５Ｓ」ってご存じですか。
「５Ｓ」とは“整理・整頓・清掃・清潔・しつけ”のことですから、一つひとつは子どもにも分かる言葉です。古くから生産や建設の場では口酸っぱく、言われ続けています。時にケガや命に関わることですから当然ですが、一般のオフィス内業務に就いている場合にも重要な活動です。
今回は、「５Ｓ」の重要性を情報セキュリティや個人情報保護の観点で検討してみたいと思います。

最近「ISMS」と「Ｐマーク」は何が違うのか？「どちららを取得するのがいいのか？」といった質問を受けることがよくあります。そこで今回は両者の性格を表すいくつかの項目について違いを説明します。具体的には、規格の思想・経緯の違い、準拠する規格の違い、対象（保護範囲）の違い、更新の違い、セキュリティ対策の違いといった観点から、相違点を明らかにしながら、両者の性質の違いを探りました。

以上

１．生成 AI 革命とプライバシー保護

生成AIは、2023年11月末の「Chat GPT」のオープンソース化発表以来、「社会を根底から変え秩序を破壊する変化」を生むとされ、社会、事業活動、生活の各分野での論議が盛んになっています。また、利用者の拡大に伴い、リスクも増大しています。

生成 AIでは、「人権、プライバシー・個人情報、知的財産権の侵害」や「偽情報、誤情報の生成・発信等」、これまでの AI ではなかったような新たな社会的リスクも生じています。

そこで2024年1月に総務省・経済産業省が示した、事業活動における生成AIに対するガイドライン （パブコメ中2024.1.20～2.19)を参照しながら、今回は、生成AI利用の原点とも思われる「人間中心の原則」に基づきプライバシー・個人情報保護について概観します。

（１）生成 AI とは?

ChatGPT(Generative Pre-trained Transformer)に代表される生成 AI(Artificial Intelligence 人工知能）は、あらかじめ膨大な量の情報から深層学習によって構築した大規模言語モデル(LLM（Large Language Models)）に基づき、ある単語や文章の次に来る単語や文章を推測し、「統計的にそれらしい応答」を生成するものです。大規模言語モデルのスケールはパラメーター数、即ちデータセットのサイズ学習に使われる計算量により決まるとされています。

パラメーター数とは、人間でいえば神経細胞と神経細胞のあいだを繋いでいるシナップシスの数で、その数は 100 兆ほどといわれます。ChatGPT では 1 兆から 2 兆と推測されています。

（２）生成 AI は事業活動に何をもたらすのか?

生成 AI は、文章の校正　翻訳・要約(英文からも OK)が得意であり、

・カスタマーサービスへの導入(自動応答、自動電話応対、家電のトラブル相談対応など)

・コピーライター業務(広告のコピーや説明を作成）などに活躍が見込まれます。

また、大量の情報から推論することから、「正解のある問題」の解決=多数派の意見をもとめる下記の業務などでの活躍も有望です。

・弁護士の仕事（「正解のない」弁護は得意ではない）

・医者のカウンセリング

・理想的な家庭教師等々が挙げられます。

更に、データサイエンスを駆使した経営者であれば　経営者の能力と組織内 DB にもよりますが、「データドリブン経営」でも活躍しそう。

保険業界では、具体的に下記の業務展開が企画され実施に移されているといわれています。

・社員の日常業務での活用（報告書作成、外国文献の翻訳など）

・照会応答業務での活用（商品規定・約款などを学習させ、活用）

・コールセンター業務での活用

・損害査定サービス業務での活用（自動車保険の事故対応での個別事情の反映は困難）

（3）生成 AI は社会にどんな変化をもたらすのか?

「部長より　チャット AI に　部下は聞き」と揶揄される企業風土が、「正解のある知識」を得意とする生成 AI によりもたらされ、より一層**ホワイトカラーの雇用が減少**すると言われています。フィンテックの活用が進む銀行などの金融機関が良い例です。生成 AI の活用により与信の自動化がすすんだ中国アリババの「芝麻信用」システムの活用事例などは、国情の違いはあるにしても、その好例といえます。

「**シンギュラリティ**」(米　レイ・カーツワイルが唱えた「技術的特異点」)は、「2020 年代までに AI と人間の知性の区別がつかなくなり、2045 年には到来する。」と言われてきました。

しかしながら、米イーロン・マスク氏は 2023.11 に「優れた小説を書き、新しい物理法則やテクノロジーを発見、発明する AI が 3 年以内に実現する」と発言しています(2024.1.9 日経)。シンギュラリティは早まりそうです。「2025 年にシンギュラリティが訪れる」(落合陽一筑波大教授)という発言もあります。(異論もあるが)。AI により社会は、確実に急速に変わりつつあります。

（4）生成 AI がもたらすリスクや厄災

AI の進化が止まらない一方で、リスクは尽きません。生成 AI では、**指示文（プロンプト）**の工夫で、より確度の高い結果が得られる一方で、回答は誤りを含む可能性が常にあります。

時には、事実と全く異なる内容や、文脈と無関係な内容などが出力されることも生じます（いわゆる**幻覚（ハルシネーション＝Hallucination**））。また、生成 AI に潜む差別や偏見、データの誤利用・乱用などのリスクも存在します。この結果、もたらされる厄災として、①プライバシー・個人情報の侵害　②著作権の侵害③フェーク情報の拡大・拡散　④悪質なサイバー攻撃の増加　⑤科学兵器の開発　などが危惧されます。

（5）「人間中心の AI 社会原則」を!!

AI の制御は、パンデミックや核戦争に並ぶ課題との認識が各国にあります。国連は 2023.10 に学者や企業人、市民団体の代表らで AI のリスクや統治を議論する諮問機関を立ち上げました。現在、AI ルールは乱立し 1000 件を超えるといわれています(2023.12.28 日経)。

政府は、2024.1.19「AI 事業者ガイドライン」を公表し、パブコメに付しています(2024.2.20 まで)。AI 利用により目指すは「人間の尊厳が尊重され、多様な背景を持つ人々が多様な幸せを追求できる持続可能な社会」であるとし、次の 10 項目について、その指針を示しています。①人間中心　②安全性　③公平性　④プライバシー保護　⑤セキュリティ確保　⑥透明性　⑦アカウンタビリティ　⑧教育・リテラシー　⑨公正競争確保　⑩イノベーション　です。

（6）**プライバシー保護**について

プライバシー保護については、下記のように指摘しています。「AI　を前提とした社会においては、個人の行動などに関するデータから、政治的立場、経済状況、趣味・嗜好等が高精度で推定できることがあります。

パーソナルデータが本人の望まない形で流通したり、利用されたりすることによって、個人が不利益を受けることのないよう、各ステークホルダーは、以下の考え方に基づいて、パーソナルデータを扱わなければなりません。①パーソナルデータを利用した AI 及びその AI を活用したサービス・ソ

リューションにおいては、政府における利用を含め、**個人の自由、尊厳、平等が侵害されない**ようにしなければならない。②パーソナルデータを利用する AI は、当該データのプライバシーにかかわる部分については、**正確性・正当性の確保及び本人が実質的な関与ができる仕組みを持たなければならない**」と。

今回は、紙面の関係もあり以上としますが、ひきつづき次号以降で、さらに詳述します。

２．事例に学ぶ：「５Ｓ」について

事例シリーズの第 23 弾です。今回は「５Ｓ」について検討してみたいと思います。

数年前になりますが、ある会社（プライバシーマーク事業者。以下「Ｘ社」）で実施したセミナーの参加者データが自社の Web サイトにアップされ、世界中から閲覧が可能になった事故がありました。不要になったはずのデータについて“整理”されていなかったのです。

「５Ｓ」とは“整理・整頓・清掃・清潔・しつけ”のことですから、一つひとつは子どもにも分かる言葉ですが、古くから生産や建設の場では口酸っぱく言われ続けています。ケガや命に関わることですから当然ですが、一般のオフィス業務に就いている場合にも重要な活動です。

今回は「５Ｓ」を情報セキュリティや個人情報保護の観点から検討してみたいと思います。

（1）Ｘ社の事故はどうして起きたのか

Ｘ社ではインターネットを使った FAX 配信のサービスを本業にしており、セミナーをマーケティング部門で行いました。参加者は 300 人に上りそのデータ(Excel)をコピーし、営業部門にも配付しました。セミナーのアンケート集計が終わってすぐにマーケティング部門では当該のデータを消去しましたが、営業部門ではセールス活動のために当然残していました。

3 年程経った時、参加者の一人からマーケティング部門に「自分の参加したセミナーの名簿がネットで公開されている」とのクレームが入り急いで調べた所、Web サイトにアップロードされたコンテンツの中に確かにそのデータが含まれているのを発見しました。

即座に Web サイトから消去しましたが、どれだけの人に閲覧され拡散されたか知る術がありません。

原因は、コピーしたデータの管理が行き届いていなかったことと言えます。プライバシーマークの運用に照らした場合、営業部門にそのデータの利用目的・保管期限・第三者提供(HP への掲載)の可否が周知されず認識もされていなかったのでしょう。

（2）「５Ｓ」の狙い

“最新のファイルはどれだったかな？”等と、PC やサーバの中を探しまくった経験は誰しもが持っていることです。製造工業の企業において勤務時間の中で資料探しの時間が 10%を占める、との統計を目にしたこともありますが、業種が変わっても変わらない状況と想像します。

まさしく“ムダ”な時間です。

ムダは拡大する性質を持ち、自分で探すムダ、誰かに聞くムダ、聞かれた人は手を止めて話を聞くムダ、教えるムダ・・・。命に関わることでないにしても、生産性を低下させる要因の一つであり重要経営課題でもあることは明白です。

「写真 AC」サイトから引用

ここで、「５Ｓ」を分解してみます。

最初は改善活動で、“整理・整頓・清掃”です。“整理”は不要なものを処分すること、“整頓”は使いやすい場所に使いやすい状態におくこと、“清掃”は整理整頓が維持できるようにすること（“基準”が必要）で、ここまでは「３Ｓ」とも称されます。

残る“清潔・しつけ”は「３Ｓ」の支援活動に位置づけされます。“清潔”はこの稿では衛生的な視点でのことではなく、「３Ｓ」を支援する仕組み作りと、それによって正常な状態に保つことになります。“しつけ”は決められたルールが自然にできる状態にすることで、教育や研修が含まれます。

いかがかでしょうか。「５Ｓ」は工場や建設の現場に限らないテーマとお分かりになるのではないでしょうか。転職経験のある社会人(150 名)に対するアンケートで、「オフィスを見学した際の『ブラック企業』かどうかの判断ポイント」のワーストワンが「オフィスが汚い」だったとの報告もあります。具体的な声は以下のものです。

・オフィスが整理整頓できていない
・オフィスが整理整頓・清潔清掃されていない
・机の上が乱雑

「５Ｓ」をないがしろにした場合、あたら有能な人材の獲得の機会を逸失するかもしれません。

（3）「５Ｓ」のマネジメント

“今日これから５Ｓに取り組もう”と号令を掛け、「５Ｓ」を標語として掲げても当たり前過ぎて、多くの人は気合いが乗らず具体的な行動に結びつくとは思い難いです。実効性を高めるためにはマネジメントシステムとしてPDCA サイクルを回すことが肝要です。最終目標を細分化してKPI を定めて着実にステップアップを図るのが正攻法と考えます。

先ずは目的を設定することですが、「個人情報管理台帳」にある“保管期限”を過ぎたものが会社に存在しないこと、それを維持することがゴール(KGI)になります。取っ掛かりのKPI として、サーバ内では管理責任者の不明な情報、個人にとっては契約が終わった特定の顧客の情報を整理することから始めるのも一法です。廃棄に不安が残るのであれば年度別に仕分けしておき、次回までの期間内に利用や参照のなかったものは、後日機械的に気持ちよく処分する方法もあります。

次には最終利用日から一定期間経った情報の処分、のようにKPI を変えて段階を踏んで行けば必ず「個人情報管理台帳」に定めた保管期限が守れる、即ち最終目標に到達します。

年度の終わり等のタイミングで達成度の点検を行い、次のKPI の参考に供することでPDCA サイクルが一巡します。

（5）まとめ

いわゆる情報(紙、データ)には、データベースのように表の形式で整斉と整理された“構造化情報”と、紙やWord ファイル、図や文を含んだExcel ファイル等の“非構造化情報”がありますが、仕事の上では非構造化情報の方が多数を占めていると言われています。しかも非構造化情報は往々にして個々人に管理が委ねられています。

PMS 規程に沿った個人情報保護の活動が「５Ｓ」活動を包含していることにお気づきと思います。PMS の運用が広く会社全体の情報管理の上での体質化にも繋がります。都度都度もいいのですが、運用の確認の時や最低でも年末の大掃除の時など定期的な情報整理をルール化し習慣にしていただければと期待しています。

３．P マークと ISMS の違いについて

最近「ISMS」と「P マーク」は何が違うのか？　どちららを取得するのがいいのか？　といった質問を受けることがよくあります。そこで今回は両者の差異について以下でご説明します。

（1）「ISMS」と「P マーク」の規格の思想・経緯の違いについて

P マークは個人情報保護法が発端となっており、個人情報の持ち主のプライバシーを保護するという思想です。

これらの個人情報を適切に守るために、P マーク制度は 1998 年に誕生しました。そしてその翌年には、P マークの準拠規格である JISQ15001 が制定され、この規格にもとづいて P マーク認証が行われています。現在 P マーク取得事業者は約 17,600 社程です。

一方、ISMS は組織が保有している情報資産それぞれに、どのような脅威 が存在しており、脆弱性があるのかを認識したうえでリスクを算出・軽減するための対策が目的となっています。

P マークは、あくまでも顧客の個人情報を守るためのものですが、ISMS は自社の情報資産を守るための枠組みであり、その延長線上に顧客の個人情報の保護も含まれています。

特に ISMS では、情報資産に対する漏洩・滅失・棄損ではなく、機密性 ・完全性 ・可用性のバランスを意識したものとなるため、必ずしも個人情報の保護だけを目指すわけではないということになります。ISMS の取得事業者数は現在約 7,600 社程です。

（2）準拠する規格の違い

ISMS と P マークでは、準拠する規格が異なります。ISMS（Information Security Management System）は、国際標準規格である ISO /IEC27001 にもとづいて運用されます。日本においては、日本工業規格 として JISQ27001 の規格にもとづいて運用されております。

P マークは、日本工業規格である JISQ15001 にもとづいており、JISQ15001 は個人情報保護法をベースとして生まれた規格です。そのため、P マークが適用されるのは、日本国内のみとなります。

（3）対象（保護範囲）の違い

ISMS と P マークの対象範囲の違いとしては、「保護する情報資産の対象」と「取得可能範囲の対象」という 2 点に違いがあります。

ISMS では、（1 部署のみ等、企業が自由に設定可能）の個人情報を含む情報資産に対するリスク対応が対象であるのに対して、P マークでは、企業全体における個人情報が保護の対象となります。P マークは、あくまで個人情報の保護を目的としているため、その他の企業が有する情報資産の保護は対象にはなりません。

そして、取得可能範囲の対象の違いとは、企業内で ISMS と P マークを適用する範囲のことをいいます。ISMS では、企業全体での取得だけではなく、対象を限定して（特定の部署のみ）認証取得することが可能です。しかし、P マークは、適用範囲が企業全体に限られているため、個人情報を有していない部署でも規格に則って業務を遂行する必要があります。

（4）更新の違い

ISMS、P マークともに、認証取得をして終わりではなく、定期的な更新を行わなければなりません。ISMS では 3 年ごとの更新審査が行われます。また、P マークでは 2 年ごとの更新審査が必要です。

こうしてみると、P マークよりも ISMS のほうが、更新頻度が少ないように感じます。しかし、実際には ISMS は、3 年ごとの更新審査だけではなく、毎年の維持審査を受ける必要があるのです。P マークにおいては 2 年ごとの更新審査の際には、前回の更新審査以降の管理状況や運用状況について審査が行われます。

一方で、ISMS では実質毎年審査が行われているので、審査が行われる期間は短くなります。そのため、更新期間については、ISMS と P マークでは異なるものの、企業が負うことになる負担としては、さほど大きな違いはないと考えられます。

（5）セキュリティ対策の違い

ISMS には、適切なマネジメントシステムを構築するための、具体的な 114 の管理策があります。この中から、企業規模や保有している情報資産、そして費用対効果などを勘案したうえで、必要な管理策を選択していくこととなるのです。

一方 P マークでは、企業の実態に沿った個人情報保護のためのセキュリティ対策を講じる必要があります。たとえば、P マークにおいては、個人情報を取得する際に、取得方法のいかんにかかわらず、その利用目的を明示しなければなりません。このように、セキュリティ対策としては ISMS と P マークはまったく異なっており、ISMS のほうが柔軟な対策を講じることができます。しかし、対策法が指定されている P マークは、取得の際検討の必要がなく、指示された対策を運用するだけで構わないと捉えることができます。

ISMS は、企業が持つ情報資産に対するリスク対応を実行するための仕組みや運用体制を構築することを目的としており、P マークは顧客の個人情報を保護することを目的としている認証制度です。

ISMS では、「機密性 」「完全性 」「可用性」の視点でリスク評価 を行い、対策を進めていく必要があります。例えば、「ローカル PC にデータ保存しているため、社内で共有しづらい。そのため、クラウドサービスを導入し、情報共有を簡単に行えるようにしよう。」など情報を使いやすくすることもマネジメントシステムの目的として適しています。

P マークでは、「漏洩」「滅失」「毀損」の視点でリスク評価を行い、対策を進めていく必要があります。個人情報保護法で定められた以上の、個人情報保護の対策を打つことになり、ISMS とは根本の考え方に違いがあります。

（6）最後に

ISMS と P マーク、どちらを運用したほうがいいかについては、一般的には、保険代理店のように BtoC タイプで顧客の個人情報を多く取得して事業を行う企業については「P マーク」が適しています。そして外部からの情報処理により個人情報を預かるケースの多い BtoB 企業に関しては「ISMS」がおすすめと言えます。

４．トピックス

（１）2023 年の大型個人情報漏えい事故について

東京商工リサーチでは上場企業とその子会社が公表した個人情報の漏えい事故を毎年年初に発表しています。今年も一月下旬に 2023 年度の事故統計を公表しました。
昨年も以下の通り大型の個人情報持出し事故が発生しています。

①2023 年に発生した最大の個人情報の流出事故は、ＮＴＴグループ（日本電信電話）で発生した 928 万人分の個人情報流出でした。
グループ会社が受託していたテレマーケティング業務で、長年にわたってクライアントの顧客情報を従業員が不正に持ち出したもので、流出被害に遭ったクライアントは、民間企業のほか自治体など 69 団体にも及び、関係先が対応に追われ各所に波及しました。

②2 番目はデリバリー大手の「出前館」で、システムの誤設定により顧客のアカウント情報 924 万 4,553 件が閲覧の恐れがあったと公表しました。
出前館にて特定の操作でのログインで、個人情報が閲覧可能状態となる不具合が発生し、共有した PC やスマホで出前館サービスを使った顧客の出前館サービスアカウント情報の一部が閲覧可能状態となった。

③大型個人情報流出事故の 3 番目は、ＮＴＴグループのＮＴＴドコモの 596 万人分です。業務委託先の元派遣社員が顧客情報を含む業務情報を不正に外部に持ち出したものです。
NTT ドコモによれば、インターネット接続サービス「ぷらら」と映像配信サービス「ひかり TV」の利用者の個人情報が流出し、業務委託先のグループ会社の元派遣社員が情報を不正に外部に持ち出していたと発表しました。

以上