経済産業省

資料２

「秘密情報の保護ハンドブック」・「限定提供データの指針」における生成AIに関する記載部分

令和６年３月
経済産業省知的財産政策室

（参考）「秘密情報の保護ハンドブック」について

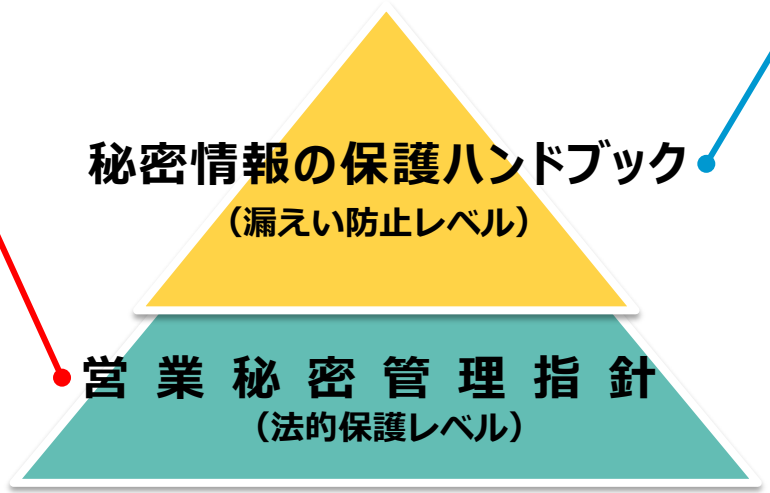
- 「営業秘密管理指針」は、不正競争防止法により「営業秘密」として法的保護を受けるために必要となる最低限の水準の対策を示すもの。　（平成１５年１月策定、２７年１月全面改定、３１年１月最終改訂）
- 「秘密情報の保護ハンドブック」は、企業が保有する「秘密情報」について、法的保護レベルを超えて、情報漏えい対策として有効と考えられる対策や推奨される包括的対策等を包括的に紹介するもの。（平成２８年２月策定、令和６年２月改訂）

https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/handbook/full.pdf

営業秘密管理指針について

- 法的保護を受けるために必要となる**最低限の水準の対策**を示すものとして平成27年1月に策定。
- その後、第四次産業革命を背景とした情報活用形態の多様化を踏まえて**平成31年１月に改訂**※。

※　外部クラウドを利用して営業秘密を保管・管理する場合も、秘密として管理されていれば秘密管理性が失われるわけではない旨等を追記。



秘密情報の保護ハンドブックについて

- 法的保護レベルを超えて、**情報漏えい対策として有効と考えられる対策**や、漏えい時に推奨される**包括的対策等**をできる限り収集して**包括的に紹介するもの**として平成28年に作成。
- より良い漏えい対策を講じたい企業の方々に、企業の実情に応じて対策を取捨選択したり、参考としていただけるよう、**様々な対策を網羅的に掲載**。
- 簡易版**「秘密情報の保護ハンドブックのてびき」**も公表。

1章	・目的及び全体構成
2章	・保有する情報の把握・評価、秘密情報の決定
3章	・秘密情報の分類、情報漏えい対策の選択及びそのルール化
4章	・秘密情報の管理に係る社内体制のあり方
5章	・他社の秘密情報に係る紛争への備え
6章	・漏えい事案への対応
参考資料	・各種契約書・規程等の参考例、各種相談窓口等の連絡先、営業秘密侵害罪にかかる刑事訴訟手続、 競業避止義務契約の有効性について　等を掲載

（参考）「限定提供データに関する指針」について（令和6年2月最終改訂）

https://www.meti.go.jp/policy/economy/chizai/chiteki/guideline/h31pd.pdf

限定提供データに関する指針について

- 限定提供データの客体要件、不正取得類型、著しい信義則類型、転得類型について、具体的な事例を交えて解説。
- 本指針は限定提供データの定義や不正競争に該当する要件等について、一つの考え方を示すものであるが、法的拘束力を持つものではない。

「限定提供データに関する指針」目次

限定提供データについて（II.）
- ✓ 限定提供データの定義について解説。

「不正競争」の対象となる行為について(III.)
- ✓ 各行為（「取得」「使用」「開示」）について解説。

不正取得類型について（IV.）
- ✓ 「窃取、詐欺、脅迫その他の不正手段」による取得について解説。

著しい信義則違反類型について（V.）
- ✓ 図利加害目的について解説。
- ✓ 「限定提供データの管理に係る任務に違反して行う」行為について解説

転得類型について（VI.）
- ✓ 取得時悪意の転得類型について解説。
- ✓ 取得時善意の転得類型について解説。

請求権者について（VII.）
- ✓ 請求権者について解説。

１ 「秘密情報の保護ハンドブック」

- **生成AIへの情報の不用意な入力を通じた、意図しない情報漏えいへの注意喚起**

はじめに（「秘密情報の保護ハンドブック」冒頭）

（略）

加えて、情報管理・利用のあり方は絶えず変化しており、ＡＩ（人工知能）を活用した新たな情報利用・創出の場面が増えてきており、これらを活用することで業務の効率化、新たなビジネスの創出など事業者・企業に有益なものとしてその普及・利用の拡大が期待される。一方で、例えばＡＩ開発におけるデータ学習時や**外部の生成ＡＩへの情報の不用意な入力を通じて、意図しない情報漏えいにつながる懸念も皆無ではなく、情報漏えいへの対策を講じながら新たなツールの効果的な利用を進めつつ、情報漏えいへの対策を両立させることも重要**といえます。

１ 「秘密情報の保護ハンドブック」

● 秘密情報の取扱い方法等に関するルール化についての記載

３－３　秘密情報の取扱い方法等に関するルール化（「秘密情報の保護ハンドブック」28頁）

（１）ルール化の必要性とその方法

（略）

○　さらに、近年、ＡＩ技術の進展を踏まえて、外部の生成ＡＩなどを事業・業務の中で利活用する動きが増えていますが、**利用しようとする生成ＡＩなどの情報管理の状況、すなわち入力した情報が社外に流出・公開等されてしまう可能性があるのかどうかを踏まえてこれらの利用の当否を判断する、これらの利用に当たっては社外に流出されてしまったら困る情報は使用（入力）しないといった対応を講じないと、秘密情報が社外に流出等してしまう可能性**があります。このため、**生成ＡＩなどを利用する場合には、予め許可された生成ＡＩを用いるようにするとともに、適切に定められた基準に基づいて予め許可された情報のみを使用（入力）するようにすること等とするルールを定めることは、秘密情報の漏えい防止に効果があるため、生成ＡＩなどの利用に際して従業員が遵守すべきルールを定めることが必要**です。

1 「秘密情報の保護ハンドブック」

● 「秘密情報の保護」の視点からのAI利用に関するコラムを参考として記載

（参考）「秘密情報の保護」の視点からのＡＩ利用（「秘密情報の保護ハンドブック」3頁）

近年の生成ＡＩの進展に伴い、あまりＡＩを利用してこなかった多くの企業や組織においてもＡＩのビジネスへの活用がこれまで以上に意識され、広い範囲で実際に業務への適用が始まっています。様々な業種の業務効率化を始め、利用の仕方によってはこれまでになかった新しい事業も期待できるＡＩですが、大きくクローズアップされた利便性の傍ら、ＡＩを利用する際には留意しなければならない様々なリスクが存在します。活用するケースや環境ごとにどのようなリスクがあるのかについては、経済産業省から公開されている「ＡＩ原則実践のためのガバナンス・ガイドライン」等に、リスクを洗い出す分析に関する指針について述べられています。

そうしたリスクには、情報漏えいに直結するものもあります。機械学習に基づくＡＩは大量のデータを学習して入力データの分類・判定を行いますし、生成ＡＩは質問（プロンプト）により利用者が様々なデータを入力しながら利用します。例えば以下のようなシナリオを考慮してみると、ＡＩによる情報漏えいのリスクをイメージしやすくなるかもしれません。

① **生成ＡＩ利用における組織のルール不備による情報漏えいリスク**
組織における生成ＡＩ利用のルール化とその周知が遅れ、職員が個人で秘密情報保護に関する契約に不備がある生成ＡＩを利用し、営業秘密にあたる情報を学習させてしまった。

② **サプライチェーン（委託先）での情報漏えいリスク**
ＡＩによる情報分析を委託する企業で、分析データの管理不備があり、分析を委託した営業秘密にあたる情報が漏えいした。

③ **ＡＩの悪用による情報漏えいリスク**
ＡＩの悪用によりフィッシングメールのなりすましが巧妙化して職員がだまされ、営業秘密にあたる情報が漏えいした。

ＡＩの利活用が日々の業務により一層密接に関わってくる潮流の中、**ＡＩを利用する際は、「こうしたリスクがある」という前提に基づき、自組織における営業秘密に関するＡＩの処理は何が想定されるのか、そうした処理に関するＡＩ利用ルールやデータ管理ルールはどうなっているのか等の確認が必要**です。**ＡＩを自社の業務やサービスに導入していない場合でも、個人が生成ＡＩを利用する場合のルールは重要**です。**自分のＰＣで営業秘密に関する質問をする、等の使い方は避けるべき**でしょう。さらに、ＡＩを直接利用しないとしても、ＡＩを悪用したフェイクコンテンツやなりすましによる営業秘密窃取のリスクが生じています。

ＡＩの導入はさらに加速することが予想されますが、そのリスクについて最新の情報を収集し、組織のルールを作りながら効果的にＡＩを利活用することが望まれます。「ＡＩ原則実践のためのガバナンス・ガイドライン」
https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/pdf/20220128_1.pdf

2 「限定提供データに関する指針」

- **データセットも限定提供データの保護対象となり得る旨を記載**

4．「技術上又は営業上の情報」について （「限定提供データに関する指針」14頁）

法第２条第７項の保護の対象は、「技術上又は営業上の情報」と規定している。

(1)「技術上又は営業上の情報」の考え方

「技術上又は営業上の情報」には、利活用されている（又は利活用が期待される）情報が広く該当する。具体的には、「技術上の情報」として、地図データ、機械の稼働データ、**ＡＩ技術を利用したソフトウェアの開発（学習）用のデータセット（学習用データセット）**や**当該学習から得られる学習済みモデル**等の情報が、「営業上の情報」として、消費動向データ、市場調査データ等の情報があげられる。

※ 本指針中における「データ」には、テキスト、画像、音声、映像等が含まれる。

2 「限定提供データに関する指針」

● 取得したデータの「使用」に関する記載

3．「使用」について（「限定提供データに関する指針」21頁）

「使用」とは、データを用いる行為であるが、具体例としては、データの作成、分析等に用いる行為が該当するものと考えられる。

＜原則として「使用」に該当すると考えられる具体例＞　**※抜粋**

- **取得したデータを用いて研究・開発する行為**
- **取得したデータを用いて物品を製造し、又は、プログラムを作成する行為**
- **取得したデータからＡＩ技術を利用したソフトウェアの開発（学習）用 の学習用データセットを作成するために分析・解析する行為**
- **取得したデータをＡＩ技術を利用したソフトウェアの開発に利用する行為**

なお、**取得したデータを使用して得られる成果物（データを学習させて生成された学習済みモデル、データを用いて開発された物品等）がもはや元の限定提供データとは異なるものと評価される場合**には、その使用、譲渡等の行為は**不正競争には該当しない**。

ただし**成果物が、取得したデータをそのまま含むデータベース等、当該成果物が取得したデータと実質的に等しい場合や実質的に等しいものを含んでいると評価される場合**には、当該成果物を使用する行為は、取得したデータの**「使用」に該当する**と考えられる。

2 「限定提供データに関する指針」

● 取得したデータの「開示」に関する記載

4．「開示」について（「限定提供データに関する指針」21頁）

「開示」とは、データを第三者が知ることができる状態に置くことをいう。実際に第三者が知ることまでは必要がなく、必ずしも「開示」の相手方が「取得」に至っていることも必要ではないと考えられる。

なお、**取得したデータを用いて生成されたデータベース等の成果物を開示する行為は、その成果物が元データと実質的に等しい場合や実質的に等しいものを含んでいると評価される場合**には、**元データの「開示」に該当することは「使用」の場合と同様**である。

＜原則として「開示」に該当すると考えられる具体例＞　**※抜粋**

- 第三者がアクセス可能なホームページ上にデータを掲載する行為
- 大量のデータをタブレットやスマートフォン等のディスプレイやスクリーン上に表示させ、それを第三者に閲覧させる行為

なお、**取得したデータを使用して得られる成果物（データを学習させて生成された学習済みモデル、データを用いて開発された物品等）がもはや元の限定提供データとは異なるものと評価される場合**には、その譲渡等の行為は**不正競争には該当しない**。