第4回

人的資本経営時代の知財法務

テクノロジーの導入と知財・労働法務

TMI総合法律事務所
弁護士　瀬戸　一希

第１．はじめに

AIをはじめとする技術の普及によるデジタル化の進展や、新型コロナウイルス後のテレワークの普及によるコミュニケーションの在り方の変化は、企業の組織的な対応を大きく左右してきたことが指摘されている[1]。情報技術が発展する中で、業務や社内インフラのデジタル化により、労働者のパフォーマンスを効率化し、高めることが重要性を増している。デジタル化に関する言及は、多くの場面で、国内企業での技術導入などへの態度の硬直性や遅れを批判する文脈であった。もっとも近年では、新型コロナウイルスを契機として、ウェブ会議をはじめとするテレワークの推進等、業務のデジタル化が進展しつつある。さらに、コストの観点から、発展の著しい生成AIが業務環境に導入されることも、最近では珍しくない。以上のデジタル化に向けた環境の整備について、種々のガイドラインや労働法上の議論が生じている。

他方、前回に検討したように、デジタル化に伴う組織内でのコンテンツ・情報の利用・共有に対しては、かねてから著作権法との関係が問題とされてきた。そうした問題に加えて、企業の職場における様々な形でのテクノロジーの導入には、情報漏洩を典型として、様々な点での知財リスクが存在する（第２）。かかるリスクへの対応は、リスクの発生する場が従業員の労働環境にあることから、労働法上の知見も踏まえた対応が必要になることが関連する裁判例やガイドラインなどで問題となってきた（第３）。以下、検討・解説する。

第２．IT技術の職場への導入を巡る法的リスク

１．ソフトウェアの利用とリスク

ソフトウェアについては、そのソースコードが、著作権や、不正競争防止法上の営業秘密として保護の対象となり得る。もっとも、近年の事案では、大阪地判令和６年７月30日（令和２年（ワ）第1539号）において、ソフトウェアのソースコードに関する著作権侵害ないし、不正競争行為が主張され、いずれの請求も否定された例もある。不正競争防止法との関係では、ソースコードの重要性を前提にしつつも、管理体制の杜撰さや、就業規則などで内部情報の持ち出しが制限されていないことから、秘密管理性が否定されている。また、この事案では、著作権侵害につ

1　経済産業省「人的資本経営の実現に向けた検討会 報告書～人材版伊藤レポート2.0 ～」2025年５月20日・最終閲覧）） ４頁（https://www.meti.go.jp/policy/economy/jinteki_shihon/pdf/report2.0.pdf（(2022年５月)。

いても、創作性の議論には深く立ち入らなかったが、その上で類似しないとの結論も示された。本連載第１回で検討したように、営業秘密の保護には、一定のハードルが存在し、情報の内容によっては著作権による保護が働きにくい場合もある。そこで、著作権や不正競争防止法の、法律上の保護に加え、ソフトウェアに関しては、ライセンス条件など、契約ないし規約上の条項によって、権利者が保護を図っている場合もある。

このように、ソフトウェアの導入に際しては、知的財産権や規約による合意などで、権利の保護が図られている。そのため、違法に複製された海賊版ソフトウェアの利用や、ライセンス契約の許諾条件に反する形での利用が典型的な法的リスクとなる[2]。違法に複製されたソフトウェアの利用は、複製元のソフトウェアの権利者との間でのトラブルのリスクを有し、コンプライアンス上の問題を生じ得る。また、ソフトウェアが正規品ではないことに伴う、安全性のリスクも存在し、情報漏洩などを通じた自社の知的財産ないし機密情報の流出という問題も懸念される。

近年の知財紛争の事例においても、ソフトウェアの利用許諾の条件が争点となっている事案は散見される。例えば、東京地判令和３年３月24日（平成30年（ワ）第38486号）では、許諾の範囲を超えたプログラムの使用態様について、著作権侵害の他、許諾に関する合意内容に反しているとして債務不履行の主張がされた。さらに、大阪地判令和４年９月29日（令和３年（ワ）第4692号）[3]では、ソフトウェアの組織内部での利用に伴う複製が、合意されているプラン内での複製なのか否かという点が争点とされている。

その他、正規のソフトウェアであっても、オープンソースソフトウェア（以下「OSS」という。）として公開されているものが少なくない。こうしたソフトウェアの導入においても、導入の目的と必要な対応が整合するよう、適切に利用条件を把握して自社に導入する必要がある。OSSの利用条件として代表的なものに、ソースコードの開示や、特許権のライセンスがある[4]。当該プログラム自体がOSSではないとしても、OSSが含まれていることによって、元のOSSの利用条件が導入したソフトウェアに対しても適用される場合があり得る。プログラムの利用契約や開発委託契約について、自社への導入時に、利用規約や、他のサービスの条件の適用関係についても、把握する必要性があるといえる。

また、大阪地判令和３年７月29日（平成31年第3368号、令和元年第8944号）では、ライセンス料の支払いに関する合意が、会社法上の利益相反取引に該当するかという点が問題とされた。会社関係者が関与している他社の技術を導入する場合には注意をする必要がある。

以上の法的なリスクが存在する一方、ソフトウェアを企業が導入することは、Iot、スマートファクトリーの隆盛によってソフトウェア産業以外を主たる事業としている企業でも必要性が高まっている。こうした状況を踏まえ、「ソフトウェアコンポーネントやそれらの依存関係の情報を含む機械処理可能な一覧リスト」であるSBOM（Software Bill Of Materials）によって、脆弱性とライセンス管理を行うことの重要性が指摘されてきた[5]。法務に係る点では、ライセンス管理として、ライセンス条件への違反を防止する意義が指摘されてきた。コンプライアンス上の、または法的な典型的リスクについて把握した上で、適切な管理技術に基づいて、自社に導入した

2　木山二郎＝渡邉峻＝馬場嵩士「ソフトウェアの不正利用等」ビジネス法務24巻５号130頁（2024年）。

3　当該事案の事実認定では、「加盟するソフトウェア保護団体であるザ・ソフトウェアアライアンス（BSA）の情報提供窓口」から違法複製の可能性が権利者に伝達されたという、紛争発生への経緯が示されている。専ら組織の内部で使用する場合についても、コンプライアンスの観点から、適切な権利処理がされているかという点は、注意を要する。

4　高瀬亜富＝久礼美紀子「OSS（オープンソースソフトウェア）の基本と社内利用上の注意点」知財管理75巻２号256-257頁（2025年）。

ソフトウェアへの対応をすることが必要となっている。

2．クラウドサービスの利用とリスク

効率的に安全な環境でのリソースを集約するという目的から、クラウドサービスの導入が行われてきたが、その一方で、安全管理策が技術的にクラウドベンダ側の許容範囲に限定されるという課題も指摘されてきた[6]。特に、クラウドサービスの提供形態や内容も多様[7]であり、クラウド上でソフトウェアの提供がされる場合もある。利用者が権限及び責任を持って管理するべき対象も相違しているため、個別のサービスに応じ、適切な対応が必要とある。さらにISMSとの関係で、クラウドサービスカスタマにおいては、情報セキュリティの意識向上、教育及び訓練に関する項目の実施について、固有の言及がされるなど[8]、リスク管理の重要性が存在する。

従来から契約との関係で指摘されてきた、クラウドサービスの利用者側のリスクとしては以下のようなものがある。具体的には、①ポリシ及び組織的リスク（ロックイン（Lock-In）のような他事業者への移行の困難など）、②技術的リスク（隔離の失敗（Isolation Failure）のようなストレージやルーティングの隔離が未整備であることなど）、③法律的リスク（サーバ設置国のカントリーリスクなど）とされる[9]。上記の②は、情報漏洩のリスクに繋がる問題点である。特に労務管理との関係での横断的な対応が必要になるのは、この問題への対処である。また、管理体制の整備は、格納される情報の営業秘密該当性を確保する上でも重要である。

ただし、上記の①との関係に注目すると、クラウドサービスの導入について企業が検討するべき法的な問題は、知的財産権という分析対象を広く見る場合、漏洩には限られない。移行が柔軟に行えないサービスを導入してしまう場合、自社のナレッジの自由な利用が縛られることになる。こうした状況も、自社の保有する知的財産の活用が阻害される意味では、情報にまつわるリスクとして観念する余地もあるように思われる。

①の背景としては、サービス提供者側で十分な移行手段が整備されていない場合や、サービス提供者がそもそも倒産や事業から撤退するような場合が想定されている。データの移行につい

5　独立行政法人情報処理推進機構産業サイバーセキュリティセンター中核人材育成プログラムSBOMプロジェクト「SBOM 導入・運用の手引き」（https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2024/sbn 8 o10000001y 6 j-att/sbn 8 o10000001zcl.pdf（2025年５月18日・最終閲覧））４頁（2024年12月）。

6　岡村久道「IT・ICTと営業秘密の保護：クラウドコンピューティングとの関係を中心に」知財管理67巻４号495-496頁（2017年）。ただし、従来のウェブサービスでもユーザー側のコントロールの低下（それに伴う法的問題としての、保管した情報の秘密管理性に対する影響）は見られたとの指摘もある（松尾剛行『クラウド情報管理の法律実務』60-62頁及び180-181頁（弘文堂、2016年））。

7　クラウドサービス事業者の提供するアプリケーションを利用するためのデータやアプリケーションの生成したデータに関する権限をサービス利用者が有するSaas、サービス利用者がアプリケーションの開発、アプリケーションに対する管理を行い、データやアプリケーションについての管理を行うPaas、は、サービス利用者が仮想環境上で動作しているOSを含めたすべてのソフトウェアの管理を行い、OSウェア層の脆弱性の管理にも責任を負うIaasと整理される（総務省「クラウドサービス提供における情報セキュリティ対策ガイドライン（第３版）」（https://www.soumu.go.jp/main_content/000771515.pdf（2025年５月20日・最終閲覧））23-25頁（2021年９月））。

8　日本能率協会審査登録センター編著『2022年改訂「ISO27001/27017」対応・導入マニュアル』153頁（日刊工業新聞社、2024年）。

9　経済産業省 商務情報政策局 情報セキュリティ政策室「クラウドセキュリティガイドライン活用ガイドブック 2013年度版」（https://www.meti.go.jp/policy/netsecurity/downloadfiles/cloudseckatsuyou2013fy.pdf（2025年３月28日・最終閲覧））44-45頁（2013年）。

て、公正取引委員会は公取委命令令和６年12月24日として、独占禁止法19条に基づく排除措置命令（一般指定14項違反）を下した事例が、注目を集めた。

この事案では、労務管理サービスにおいて、他社サービスに切り替えることを制限するような、企業の対応が問題とされた。具体的には、労務情報を管理するサービスを提供していた企業は、ユーザーが自ら登録した自社の作業員情報につき、個人情報の保護を理由にするなど[10]して、合理的な理由なく当該作業員情報の提供を拒むことで、他社サービスへの移行を妨害しようとした。そうした行為の一環として、サービス提供企業は、作業員情報の加工・複写・複製といった行為を制限するなどした。公正取引委員会の排除措置命令を受け、サービス提供企業は、仕様変更を迫られた。前提として、基本的な他社の権利を侵害しないようにするため、規約ないし約款の記載[11]を遵守することは重要であるが、その内容の法的な不当性に疑義がある場合には、専門家への相談を行った上、適切に対処する必要がある。

さらに、クラウドサービスの知的財産権侵害の問題も存在する。クラウド型の在宅医療対応電子カルテ及びレセプトシステムの著作権が問題とされた、東京地判令和４年８月30日（平成30年（ワ）第17968号）では、開発委託されて、導入されたクラウドサービスについて、その導入後の改変が著作権侵害に該当するかが問題とされた。当該事案では、契約上の譲渡対象となる著作権の範囲と、改変された範囲が問題とされている。契約上の内容や規約の把握は重要となる。

３．生成AIの利用とリスク

近時、生成AIの飛躍的な発展によって、企業において導入する例は増えている。典型的な導入例としては、チャットボットの形式による問い合わせ窓口の効率化、社内での文章作成業務の効率化、RAG（検索拡張生成：Retrieval-Augmented Generation）による社内情報検索の効率化といったものが想定されてきた[12]。

他方、生成AIの利用に際しても、法的リスクが存在する。生成AIに特有の問題もあれば、従来のソフトウェア、クラウドサービスの導入において検討されてきた問題の延長上の議論もある。

前者については、例えば、著作物の膨大な学習を前提とする技術的な特性との関係から、生成AIの利用に伴う、学習や生成の各段階について、どのような場合に著作権侵害が生じるのかという点が問題となる。著作権法30条の４との関係では、他者による学習を禁止することで適用を排除しようとする、いわゆるオーバーライド条項の問題が存在する。この種の条項や規約の文言

10　当該サービスでは、自社のみでなく他のユーザー（協力会社）が登録した、社員情報も帳票として出力可能であった。他のユーザーの社員情報が含まれる帳票の他社への提供は、個人情報保護法上、正当化され得ることや、ユーザー間での情報の更新権限との関係上、一定の場合に、適切な範囲での情報の流出を制限する措置をサービス提供者が行うことは独占禁止法上、問題とならないことから、情報の提供・移転の拒否が行われる目的が重要であるとの指摘がある（管野みずき「判批」ジュリスト1608号７頁（2025年））。

11　経済産業省 商務情報政策局 情報セキュリティ政策室・前掲注９）46頁では、契約面でのリスクへの対応のため、SLA（サービス合意書：Service Level Agreement）を締結することの重要性が説かれている。契約と一体化する、SLAを交渉の中で具体化し、合意の内容とすることによって、サービスの内容が、ユーザー側に不利にならないようにすることが期待されている。

12　独立行政法人情報処理推進機構産業サイバーセキュリティセンター中核人材育成プログラム７期生生成AIのセキュリティリスクと対策プロジェクト「テキスト生成AIの導入・運用ガイドライン」（https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2024/f55m8k0000003spo-att/f55m８k0000003svn.pdf（2025年５月20日・最終閲覧）27頁（2024年）。

がある場合において、対書となる情報が学習された場合の解釈は、明確な議論が定まっていない事情[13]がある。そのため、権利者との間での紛争発生のリスクが存在する。

適用がされる場合にも、著作権法30条の４の具体的な適用の整理は、ガイドラインレベルで図られている状況にある。同条では、著作権者の利益を不当に害さずに、「著作物に表現された思想又は感情を自ら享受し又は他人に享受させることを目的としない」非享受目的での「情報解析」の用に供される場合には、著作権が制限されるとされる。

生成AIを利用する企業の立場からすると、導入した生成AIによって生成された表現物が他社の権利を侵害していないかという点が懸念の中心となると考えられる。生成AIの利用による著作権侵害については、利用者が「既存の著作物（その表現内容）を認識しており、生成AIを利用して当該著作物の創作的表現を有するものを生成させた場合」には侵害が成立する可能性が高く、「利用者が既存の著作物を認識していなかった」場合には、学習用データに当該著作物が含まれている場合には侵害が成立し得るとされ、含まれていない場合には侵害が成立しないとの整理が、文化庁によってされてきた[14]。

また、機密性･可用性･完全性として整理されてきた従来の情報セキュリティへの対策に加え、推論対象データに混入した情報によって意図しない推論がAIによって行われるというリスクも指摘するガイドラインもみられる[15]。

他方、後者の従前のIT技術の導入における問題の延長上に位置付けられる論点[16]としては、ベンダーロックインの問題が指摘されている。さらに生成AIのサービスが、クラウドサービスプロバイダのPaaSを利用している場合には、アップデートによってユーザーが制約を受ける、アップデートの対応に関するリスクが存在する。また、Saas型である場合には費用対効果の把握が必要とされる。さらに、生成AIにおいても、サービスに関する利用規約は十分に確認する必要がある。ソフトウェアやコンテンツと同様、規約によって商用利用が制限されている場合、会社での利用はトラブルとなる可能性がある。自社の提供するサービスに組み込む場合にも、ソフトウェアの場合と同様、生成AIのサービス提供事業者の規約が、さらに適用されることになるのかという点も含め注意を要する。

以上の他、特に法的に問題として従来から注目されてきたのは、自社の保有する情報が、外部に漏洩しないかという点である。生成AIが採用する学習の仕組みに起因し、企業が学習用データとした自社の機密情報や顧客の個人情報が、漏洩するというリスクが指摘されている[17]。この点についても、利用・導入をしようと考える生成AIの学習や生成における仕組みや規約、契約

13　議論状況について、例えば今村哲也「著作権契約法」コピライト62巻740号45-46頁（2022年）。

14　文化審議会著作権分科会法制度小委員会「AIと著作権に関する考え方について」（https://www.bunka.go.jp/seisaku/bunkashingikai/chosakuken/pdf/94037901_01.pdf（2025年５月20日･最終閲覧））33-35頁（2024年３月15日）。ただし、既存の著作物が学習用データに含まれている場合には、生成AIの開発・学習段階で当該著作物へのアクセスが客観的に認められるものの、「生成・利用段階において生成されることはないといえるような状態が技術的に担保されているといえる場合」には、著作権侵害とならないことが想定されると整理されている。

15　総務省＝経済産業省「AI事業者ガイドライン（第1.0版）」（https://www.meti.go.jp/press/2024/04/20240419004/20240419004-1.pdf（2025年５月20日・最終閲覧））16頁（2024年４月19日）。

16　以下でのクラウドサービスの延長とした論点は、デジタル庁「テキスト生成AI利活用におけるリスクへの対策ガイドブック（α版）」（https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/c1959599-efad-472e-a640-97ae67617219/fe843dc6/20240610_resources_generalitve-ai-guidebook_01.pdf（2025年５月20日・最終閲覧））42-44頁（2024年６月10日）の整理を参考とした。

プランを理解した上で、適切な対応をすることが必要となる。

４．テレワークに伴う知財リスク

テレワークの法的リスクとしては、前回に検討したような、資料の共有による著作権侵害のリスクという論点が議論されてきた。テレワークの導入時に留意すべき法的なリスクとしては、さらに外部からの攻撃や、内部での不適切な対応による情報漏洩のリスクが存在する。

具体的には、テレワークに伴い、不適切な資料や備品の持出しや、従業員の権限外の操作や情報への不正なアクセス、マルウェアの感染などによって漏洩するリスクが高まることが懸念される。こうした漏洩に伴い、出願前の特許発明の情報が公知となり、権利化をする際に支障となるというリスクや、テレワークの実施によって資料や情報のコピーや持ち出しが常態化して秘密管理が形骸化する（その結果、営業秘密該当性が損なわれる）リスクが指摘されてきた[18]。

第３．知財リスクを踏まえた労働法上の対応

１．技術導入に関するリスク管理の全体的傾向

社内へのクラウドを始めとするテクノロジーの導入については、ISMSに関する一般規格である、ISO/IEC27001：2022が存在する他、クラウドサービスに関する規格やガイドラインにおいて、言及が見られる。クラウドサービスに関する文脈においても、組織的管理策、人的管理策、物理的管理悪、技術的管理策が類型化されてきた[19]。

また、法的な観点からは、第２で検討したように、テクノロジーの導入・利用による他者の知的財産権を中心とする権利侵害、及び自社の機密情報の漏洩といった問題の防止が重要となる。基本的な対応方針は、就業規則や社内整備を導入して、従業員に対して情報を周知し、従業員の違反行為の発生時に懲戒処分や民事責任の追及を行うというような整理がされてきた[20]。懲戒解雇については、第三者への漏洩に至らない事案であっても、会社側の相応な管理によって、有効性が肯定され得ることも指摘されており[21]、適切な管理措置の実施は重要である。特に他者に持ち出された場合には、流用された事実を立証することは難しいことも少なくない。例えば、知財高判令和元年８月21日（平成30年（ネ）第10092号）では、共通するスペルミスや開発環境の共通性などの事情から、流用を立証しようとしたが、これらの主張は認められなかった。情報そのものに関する事実のみでなく、アクセス態様や、持出しに前後する従業員の行動についての記録といった、周辺的な事情から、事後的な紛争発生時に主張を補強できるよう、適切な情報管理と証拠の確保をする必要がある。

また、近年の技術的な発展の恩恵を得ているのは企業のみではなく、従業員側も同様である点にも留意を要する。情報漏洩について、クラウドストレージサービスが用いられる事例（知財高判令和６年８月29日（令和６年（ネ）第10028号）など。）もあり、大規模な漏洩に繋がらないよ

17　例えば、井上乾介＝福井佑理「生成AIの法的リスクと実務上の留意点」知財ぷりずむ257号58頁（2024年）、菰口高志「競業避止、営業秘密の持出し・持込み防止に関する労働法実務の論点整理」ビジネス法務25巻１号107頁（2025年）など。

18　平井佑希「テレワーク環境における知財実務上の留意点とその対策」知財管理71巻６号769-770頁及び774-775頁（2021年）。

19　日本能率協会審査登録センター編著・前掲注８）81頁。

20　木山＝渡邉＝馬場前掲・注２）133-135頁。

21　熊谷善昭「判批」経営法曹218号87-88頁（2023年）。

う、企業側の適切な対応に必要性は高まっている。さらにテクノロジーの導入については、典型的には購入や従業員による改良・開発であるが、リースによる場合[22]もあり、様々な法的・技術的な導入形態に応じたリスク管理が必要となる。

2　ソフトウェアやサービスへのリスク対応

ソフトウェアやサービスを自社で開発などして導入する場合、退職後の従業員との間で、権利関係についての適切な処理を行う必要がある。大阪地判令和元年５月21日（平成28年（ワ）第11067号）では、職務著作に該当するか否かが、在職中に開発したプログラムについて問題とされた。基本的に創作性の観点で判断がされているが、当該事案では、元従業員が在職中の開発やその後の改変への関与に関する点も認定されている。社内で利用するIT技術の開発・導入に関係した従業員の管理態様は、いずれにしても、把握する必要があると考えられる。

さらに、退職時の従業員との合意内容についても注意を要する。大阪地判令和７年２月17日（令和５年（ワ）第11871号）では、退職後に元従業員である原告が著作権の他、元勤務先である被告との合意を理由とする訴えを提起した。この事案では、プログラムの改変に元従業員の合意を必要とする条項に合意するよう、元従業員の側から被告に求めていたが、拒否されたことが認定されている。さらに、従前の改変に際しての同意取得のフローないし運用形態について、当該元従業員の「職位」を前提としていた、との被告の合理的意思についても考慮された。合意が成立しない場合には、在職時の運用に趣旨が問題となることもあり、管理体制について継続的な整備をすることは、関係者の退職後の紛争対応にも資する場合もあると考えられる。

実際に技術的な手段によって情報の漏洩がされるような場合には、適切な処分が必要となる。東京地判令和４年12月26日（令和２年（ワ）第20153号、令和３年（ワ）第31095号）では、「アップロード行為後に本件データファイル等が原告の支配領域から出ていないことは、被告会社がサイバーセキュリティ対策を行って、システム監視やログ分析を行った結果、本件アップロード行為が早期に発覚した結果であるに過ぎないことが推認され、原告に特に有利に考慮すべき事情ということはできない」とされており、流出がないという事情は解雇の有効性に関して従業員に有利な事情とされない場合があるという形で、適切な手続を踏まえた前提での早期の対応が重要であることが示されている。

その他、東京地判令和５年11月27日（令和２年（ワ）第27963号）でも、同様の判断がされた。当該事案では、クラウド型ストレージサービス及び仮想デスクトップを通じたアクセスが企業で導入されていたが、転職の決定後に情報の持ち出しを元従業員が行っていたことで問題となった。裁判所は、原告である元従業員の本件での行為が被告である企業の情報管理規程への違反を認め、かつ懲戒解雇の社会的相当性も肯定した。具体的な考慮要素は、目的が退職後の利用であり、大量の情報を私的領域である自身のストレージに保管したものであり、情報量の多さや、被告会社側の業務分野に照らした場合の情報の重要性が従業員サイドでも認識可能であること、情報の中には秘密保持契約の相手方からの責任追及のリスクを有する重大な情報も含まれていたことから、非違行為の重大性を評価した。業務遂行の目的も兼ねていた可能性の存在や、手口自体が稚拙で隠蔽の意図が見られないこと、持ち出しの発覚後に会社の指示に応じたこと、第三者への漏洩がなかったこと、過去の懲戒処分歴が存在しないことを元従業員側に有利な事情としてい

22　東京地判令和６年３月13日（令和３年（ワ）第4858号、令和５年（ワ）1134号）や、東京地判令和５年12月８日（令和２年（ワ）第11828号、令和２年（ワ）第27579号、令和２年（ワ）第28996号）といった事案ではリースによってテクノロジーの導入がされたことが認定されている。

る。また、情報管理体制の杜撰さとして主張された実態の一部は事実とする余地を認めつつも、一部社員の逸脱した行動の存在を理由に、情報管理規程の運用が全く根拠を失っている状態にあったとはいえないとして、結果的に懲戒処分を有効としている。

このように、懲戒手続を実施するに当たっては、処分の相当性の根拠となる事情を事後的に、早期に示すことができるようにする必要がある。具体的には、社内規程に違反したアクセスの有無を検証するためのアクセスログや、不正な情報の複製・保存を検証するためのダウンロードの有無や、媒体の使用履歴を確認する必要がある。これらの情報は、サービスの提供形態によっては、必ずしもユーザー企業の側で確保できるとは限らない。例えば、クラウドコンピューティング環境で生成される様々な情報も含め、プロバイダ側から提供を受けられるような合意（交渉が難しい場合においては提供を受けられる範囲の明確化）をしておくことが望ましいと考えられる[23]。

また、大阪地判令和２年10月１日（平成28年（ワ）第4029号）などで問題とされてきたように、転職者が自社システムの導入・開発に関与する場合、前職の他社の機密情報となるソースコードなどの利用がされていないかという点についても留意する必要がある。

さらに自社に導入したソフトウェアに組み込まれたOSSや、他者のサービスの規約を把握することは、元従業員と会社の間での紛争にも意義を有する場合がある。具体的には、徳島地判令和７年１月16日（令和５年（ワ）第38号）において、元従業員が開発して導入されたプログラムに関する紛争発生時には、プログラムの開発に用いられた統合開発環境の規約の商用利用などに関する記載が、過失相殺や損害の算定に関して検討された。なお、採用時の身元保証書の提出は近時では行わない会社も増えていることが指摘されているが[24]、この事案では身元保証がされていた元従業員の親族にも請求がされ、認められており、必要に応じて作成することも考えられる。

また、サービスを利用するに際しては、利用者権限の設定も問題となる。営業秘密管理指針では、外部クラウドを利用して情報を管理する場合、階層制限にも続くアクセスの制限や、不正取得のリスクが顕在化している場合における人事異動・退職ごとのパスワードの変更、私的メールへの転送制限、物理的なUSBやスマートフォンの接続制限によって、秘密管理該当性を高める提案がされている[25]。ただし、これらは情報漏洩対策として重要であるとしつつも、秘密管理性の確保には必須ではなく、重要な情報であることが明らかであれば、秘密管理性との関係では、誓約書や就業規則による合意で十分となる場合もあるとされている。

具体的な事例としては、クラウドサービスに保存されていた機密情報について従業員が不正にアクセスして、情報を自宅に持ち出して漏洩に繋がったとの主張がされて紛争になった大阪地判平成29年１月12日（平成27年（ワ）第7288号）では、「アクセスにセキュリティーキーが必要なクラウドコンピューティングシステムを用い，原告事業所に勤務する各従業員にそれぞれ割り当てられたセキュリティーキーに設定されたIDとパスワードを入力」することが必要であったことが、秘密管理性の根拠として考慮されている。この事案では、IDとパスワードが形式的であることから、秘密管理性を否定する主張が被告からされたが、他の従業員には明らかではなかったとして認められなかった。しかし漏洩リスク全般を最小化する意味からすれば、形式的ではないパスワードの設定が必要であると考えられる。

反対に、情報の重要性が低く、管理態様も不十分とされる場合には、業務用のPCにUSBでの

23　日本能率協会審査登録センター編著・前掲注８）131-132頁。

24　東京弁護士会労働法制特別委員会編著『新労働事件実務マニュアル 第６版』347頁（ぎょうせい、2024年）。

25　経済産業省「営業秘密管理指針」（https://www.meti.go.jp/policy/economy/chizai/chiteki/guideline/r7ts.pdf）14-15頁（最終改訂：2025年１月30日）。

接続をできないようにする技術的制限が付されていて、秘密保持や競業避止の誓約書を退社時に作成させていても、営業秘密該当性が否定されるような場合もある（東京地判令和４年５月31日（令和元年（ワ）第12715号））。さらに、大阪地判令和５年４月17日（令和３年（ワ）第11560号）でも、クラウドサーバー上に保存されている情報の営業秘密該当性が否定された。業務上使用するクラウドサーバーへの第三者への自由なアクセスの禁止をすることは当然であり、目的外でのダウンロードを全般的に禁止することも秘密としての管理には当たらず、社内規定や入社時の誓約書にも秘密管理の記載がない一方で退職時の誓約書には過度に広範な対象への記載がされていることが指摘された。なお、当事者はダウンロードごとに許可を求める体制の存在を主張していたが、そうした体制の存在は認定されなかった。単に運用体制の規則を定めるに留まらず、具体的な管理体制を事後的に証明できるようにすることも重要である。

また、当該従業員の権限喪失時に、適切な引継ぎが実施されるようにしておく必要もある。東京地判令和４年11月10日（令和３年（ワ）第20325号）では、管理者となっていた取締役が退任後も、自らが管理者であり続けたことについて、合理的に必要がなかったとして、適切に引継ぎをせず、会社が解約できずに発生した経済的負担を、忠実義務違反による損害として認定した。このように、適切な者に設定しない場合、当該従業員の退職後に、管理者の引継ぎでトラブルとなり、解約ができず会社の損害となることも懸念される。

さらに業務上、必要との要望があるテクノロジーの導入がされない場合、従業員との間でのトラブルが生じる可能性がある。最終的に否定されているが、必要なソフトの導入との関係で、業務環境が改善されないことがパワーハラスメントとして東京地判令和４年11月25日（令和３年（ワ）第7465号）において主張されている。技術の導入について見送る場合についても、特に強く要望している従業員に対しては、その理由をリスクの有無や程度、管理の難易度、予算などの観点から具体的に伝達し、納得を得ておくことで、トラブルを回避するが必要な場面も考えられる。

３．テレワークの実施と対応

ISMSの一般的な規格である、ISO/IEC 27001：2022では、その附属書Aの「人的管理策」において、リモートワークに関する項目が存在している。ISO/IEC 27001：2013以来、リモートワークの項目は存在しており、通信を前提としない、組織の外部での作業全般を想定してきた[26]。例えば、第三者の画面閲覧や物品の紛失といった点が通信を伴わないリスクとして考えられている[27]。法的な観点での従来からの検討も規格と同様、リモートワークの実施におけるリスクは、通信のセキュリティの脆弱性という観点と、物理媒体の紛失ということが従来から想定しており、通信に限らず、組織外部での労働に伴うリスク全般に対応する必要がある[28]。

さらにテレワークの導入に際しては、接続するネットワークの方式に加え、会社によってデバイスを貸与する方式で行うのか、それとも個人のデバイスで行うのかという点でも、対応するべきリスクの程度が異なることが指摘されている[29]。個人の私物を用いるBYOD（Bring Your

---

26　中尾康二＝山下真編著『ISO/IEC27001：2022（JIS Q 27001：2023）情報セキュリティマネジメントシステム要求事項の解説』114-115頁（日本規格協会、2023年）。

27　総務省「テレワークセキュリティガイドライン 第５版」（https://www.soumu.go.jp/main_content/000752925.pdf（2025年５月20日））91頁以下（2021年）で、典型的なリスクについて解説されている。

28　東京弁護士会労働法制特別委員会編著・前掲注24）333頁。

29　日本能率協会審査登録センター編著・前掲注８）158-159頁。

Own Device）による場合、企業側の調達コストの低減に対し、具体的なリスクとしては、紛失の他、機密情報の持出しリスクが指摘されている[30]。私物の情報端末が用いられる場合、上記のようなリスクは増すことになる。しかし、情報端末に対する監視・監督を無制限に行うことは、労働者のプライバシーとの関係上、難しい（東京地判平成13年12月３日（平成12年（ワ）第12081号、平成12年（ワ）第16791号）を参照。）。自社の情報や、私物端末によるアクセスの範囲などを踏まえ、適切な範囲での制限によって対応できるリスクであるのかどうかという観点からの具体的な検討が必要になる。不正の兆候がある場合には、私物の端末についての提出を求めることを、BYODの条件として、従業員と合意するという工夫も行われてきた[31]。

また、自社からの貸与による場合にも、常にリスクがないものではない。貸与したデバイスについても、必要な業務や雇用期間が満了した場合には、適切に回収される必要がある。その際に、従業員との間で紛争が生じる可能性がある。具体的には、東京地判令和６年２月19日（令和３年（ワ）第19469号、令和３年（ワ）第19613号、令和３年（ワ）第22581号）において、貸与されていたパソコンのパスワードの開示を会社側が要請した行為について、従業員側からパワーハラスメントとして不法行為を構成する旨が主張された。裁判所は、会社側が貸与した物品であり、開示に要する従業員側の負担や、緊急時の対応のためのパスワードの開示の必要性を考慮し、開示の拒否について合理的な理由がないことから、従業員の主張を採用していない。本件では労働組合を通じた開示の依頼や、従業員側の療養中であるため回答できないとの言い分を踏まえた、対応がされたことも認定されている。必要な物品の回収や、情報の開示について、事前に運用を定めておくことで、従業員側が反発をした際、適切な対応ができるよう準備する意義は少なくない。

さらに、デバイスを調達する場合に、貸与先との間での紛争予防を考える必要もある。東京地判令和６年２月29日（令和４年（ワ）第29221号）は、被告である会社の代表者が貸与を受けたスマートフォンについて海外で行った操作が問題とされた。同様に、調達先から貸与を受ける場合には、貸与後に実施可能な操作方法や通信方法について契約上の料金に関する定めが存在する可能性がある。従業員に対してのテレワークの規則を定める際、デバイスなどの備品の調達元との間での紛争予防や経済的負担を意識した内規を定める必要がある。

４．生成AIの導入に関する対応

生成AIの導入について、クラウドサービスなどと比べると、そのものが問題となっており、直接に参考となる裁判例は現状、特に存在しない。生成AIの導入対象となる業務や分野は、日々変化していることから、企業の導入に伴う運用形態も様々で、発展の途上にあるといえる。広範に存在するリスクに対して適切な対応を選択するため、導入に対する従業員・部署の必要性や、対象とする業務を事前に明確化することの重要性が特に高いことが指摘されることもある[32]。

かねてから職場での導入に際して懸念されてきたのは、外部の提供するAIへの情報の入力を従業員が行い、情報が漏洩することであった。漏洩が発生する原因となる、導入されるAIのデータ管理の仕組みを踏まえ、ユーザー側で行うべき操作や管理体制を整える重要性が、過去の漏洩事案を踏まえ、指摘されてきた[33]。

30　松尾剛行『AI・HRテック対応 人事労務情報管理の法律実務』200-201頁（弘文堂、2019年）。

31　森本大介「営業秘密漏えいの典型的類型と初動対応」ビジネス法務24巻５号40-41頁（2024年）。

32　中崎尚『生成AI法務・ガバナンス：未来を形作る規範』366-367頁（商事法務、2024年）。

33　独立行政法人情報処理推進機構産業サイバーセキュリティセンター中核人材育成プログラム７期生生成AIのセキュリティリスクと対策プロジェクト・前掲注12）50-51頁。

もっとも、サービス内容も多様化する中で、生成AIの利用に伴うリスクは、単純に情報を入力することによって、外部に漏洩するというリスクには限られない状況にある。例えば生成AIの生成物が高度化することに伴い、不正確・不適切な情報をユーザーが気づかずに利用してしまう、「過度の信頼」と整理されるリスク[34]は今後、重要性を増すと考えられる。生成AIの導入に際して、運用上の規則などを企業内で策定する場合、情報の正確性についての確認や、外部への誤った情報の提供の際の対応の手順についても検討・整備し、従業員が安心して活用できる環境を整える必要性が考えられる。

さらに、法的な観点からは、外部への漏洩だけではなく、内部での情報の移転・移動の問題も存在する。具体的には、社内情報の効率的な参照を可能にするために、情報がAIに集約される場合、学習成果として情報の生成がされることによって、ある部署で秘密の情報として管理されている情報が、他部署でも実質的に参照可能になるという、部署間での秘密管理性の観点の問題も生じることになる。ここでは会社内に限られた情報の利用を前提にしており、外部への漏洩とは別の、営業秘密の保護におけるリスクとなる。この点は企業の関心を集めたため、秘密管理指針が改訂・追記されており、ある部署で保管されている情報が、別部署で出力された場合に、直ちに秘密管理性が失われるものではないことなどが記載されるに至った[35]。

以上のように、特に発展が著しく、利用するサービスについて従前のイメージにのみ基づいて対応する場合には、実際に潜在的に存在するリスクへの対応として十分ではない場合も考えられる。ただし、問題となるリスクを把握した上で、基本的な方針は適切な運用を社内で定め、従業員の活動を確保しつつ、問題発生時には適切な法的措置を講じることのできる体制の整備を行うという、基本的な方針は、生成AIの導入に際しても大きくは変わらないと考えられる。

第4．終わりに

生成AIを中心としてIT技術が急速に発展する中で、企業のテクノロジー導入に伴う問題は、日々、新たな法的論点を生じている。企業側としては一定の指針が必要になる一方、法改正による対応の迅速性や網羅性が難しい中で、ソフトローによる対応が適宜、行われてきた。もっとも、ガイドラインについては作成省庁も様々であり、その趣旨や目的も異なり、紛争の対象となる事実との対応も問題となるため、企業側の対応が難しいことに変わりはない。

しかし、リスクの存在のみを専ら重視し、テクノロジーの導入に躊躇することは、他社との競争条件を悪化させることにもなりかねない。企業の技術導入の際、問題となり得る法的な論点を過去の技術との差異も踏まえて、適切に把握し、必要な技術を支障なく導入できるよう、法務サイドからの支援を行う必要性が高まっている。

（以上、次回に続く）

34　独立行政法人情報処理推進機構産業サイバーセキュリティセンター中核人材育成プログラム７期生　生成AIのセキュリティリスクと対策プロジェクト・前掲注12）56頁。

35　改訂の経緯や、かかる状況を受け、就業規則などによって出力される情報に触れる可能性のある別部署についても統制を行うことの重要性について黒川直毅＝望月孝洋＝石原優輝＝中村彩希「「営業秘密管理指針」改訂概要の解説」NBL1290号８-９頁（2025年）。