事務所ニュース News
2025.10
K-074
発行：村田健二税理士事務所

経営バイタルの強化書 KEIEI VITAL

営業秘密の漏えいと管理の実態・対策を知っておきましょう!

「企業における営業秘密管理に関する実態調査2024」報告書

近年、営業秘密の漏えい事例は大幅に増加しており、その実態把握と管理・対策についてしっかり行うことが求められています。生成AIやクラウドサービス等の新技術の利用と営業秘密の関係についても確認しておきましょう!

1 「企業における営業秘密管理に関する実態調査2024」報告書の公表

独立行政法人情報処理推進機構（以下「IPA」という）は、8月29日「企業における営業秘密管理に関する実態調査2024」報告書を公表しました。

この調査は、企業における営業秘密の漏えいの発生状況、漏えい対策等の実態を明らかにし、営業秘密漏えいを防ぐために有用な情報を提供することを目的とし、企業・組織のセキュリティ実務担当者や経営層を対象としたアンケートによる意識調査によって実施したものです。

調査期間は、2025年1月23日~31日とし、ウェブアンケート方式により、調査対象企業の「情報システム関連部門」、「リスクマネジメント関連部門」、「サイバーセキュリティ関連部門」、「経営企画部門」、「経営層」、「その他セキュリティやリスクマネジメントに関する業務を実施している部門」に属する者を対象として、1,200人に実施しています。

調査内容は、**①営業秘密の漏えいの実態（漏えい有無、漏えい先等）、②営業秘密管理の実態（脅威と対策必要性認識、情報管理、限定提供データの保有状況等）、③営業秘密管理において実施している対策（技術的対策、環境的対策、秘密保持契約等）、④最近の動向を踏まえた対策（サプライチェーン管理、クラウドサービス・生成AI利用時等）**等となっています。また、2020年度に実施した「企業における営業秘密管理に関する実態調査2020」からの変化にも着目しつつ、企業における営業秘密の漏えいの実態や営業秘密の漏えい防止策等の実施状況が取りまとめられています※。

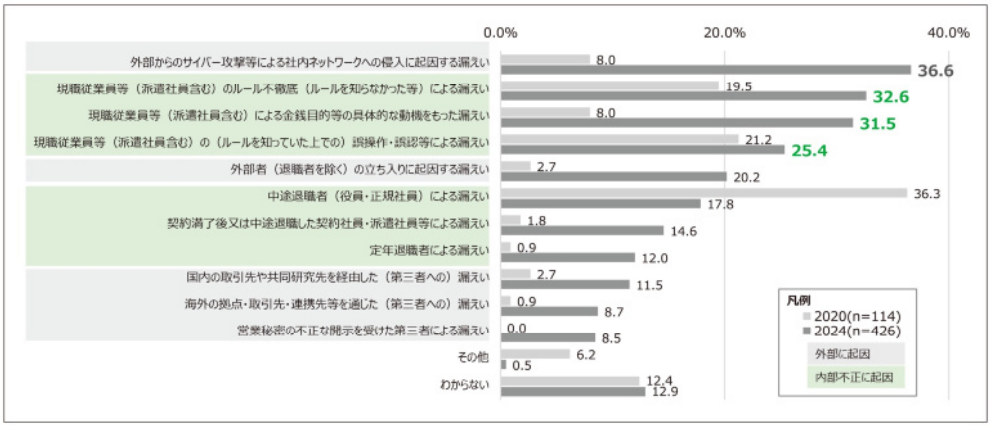
2 各設問の集計結果概要

① 営業秘密の漏えいの実態（漏えい有無、漏えい先等）

過去5年以内の営業秘密の漏えい事例について、漏えい事例・事象を認識している割合は35.5%であり、2020年度調査の5.2%と比較して認識割合が大幅に増加していました。

営業秘密の漏えいのルートについて、外部からのサイバー攻撃等に起因する漏えい（36.6%）が大幅に増加しており、次いで、現職従業員等のルール不徹底（32.6%）、金銭目的（31.5%）、誤操作・誤認等（25.4%）の内部不正相当の割合が上位を占めていました（【図1】）。

【図1】漏えいルート



漏えいした情報の種類を問う設問の回答では、漏えいした場合に公表・報道されることの多い「顧客情報」よりも、「製造に関するノウハウ、成分表等」に関して「有」と「可能性有」を選択した割合の合計が大きいことから、広く公表・報道されていない

裏面へ続く→

営業秘密漏えいのインシデントが多いことが懸念され、さらに、営業秘密の漏えいによる推定損害額を問う設問の回答では、営業秘密の漏えいによる推定損害額が「わからない」とした割合が2020年度調査の46.5%より減少して16.9%に、10億円以上とした割合が2020年度調査時の0%より増加して30%程度になっていることから、営業秘密の漏えいが事業に与える影響がより深刻になったと考えられます。

営業秘密の漏えい先について、「国内の競合他社」が最も高く54.2%、次いで「国内の競合他社以外の企業」が48.8%、「外国の競合他社」が1.4%となっていました。

② 営業秘密管理の実態（脅威と対策必要性認識、情報管理、限定提供データの保有状況等）

自社の営業秘密の漏えいに関して、現在脅威と感じ、対策が必要と考えているものについて問う設問の回答では、業種、従業員数、売上高、所属部門別で分析した結果、従業員数300人以下かつ非製造業、売上高10億円以下、経営層の区分では、「特に感じているものはない」の割合が全体に比べて高い傾向にありましたが、実際に脅威が無い可能性だけでなく、自社の保有する営業秘密にとっての脅威を認識できていない可能性も考えられました。

内部不正を誘発する環境や状況について、経営層では最も高くなっていたものが、「当てはまるものはない」でしたが、「同じ業務を同じ人が長期継続」、「少ない人数で業務を回している」ことが内部不正を誘発する要因となることも強く認識されており、サイバーセキュリティ部門やリスクマネジメント部門ではこれら以外にも、「人間関係等への恨みが大きい」「借金のある人が営業秘密を扱う」「弱みを握られて脅迫されている」ことが内部不正誘発の要因となることが認識されていました。

企業において営業秘密の管理を行うに当たっては、営業秘密とそれ以外の情報との区分や秘密性のレベルに応じた格付けを実施することが重要情報を管理するための基本であり、企業の重要情報管理状況を把握する上で重要となっています。また、組織として営業秘密の管理ルールを定めた上で、従業員等に周知し、組織的に運用することにより、従業員等に営業秘密を持ち出す気を起こさせないようにすることも重要なこととなっています。

営業秘密とそれ以外の情報との区分及び格付けの実施の有無を問う設問の回答では、「営業秘密とそれ以外の情報とを区分していない」割合は22.3%であり、今後も改善の余地が大きいと考えられます。ただし、営業秘密情報を区分して管理している割合が2020年度調査から増加している点では、対策が進展していると考えられます。

③ 営業秘密管理において実施している対策（技術的対策、環境的対策、秘密保持契約等）

営業秘密管理においては、組織が保有する営業秘密の性質、従業員の規模、予算などに合わせて、技術的対策や環境的対策、秘密保持契約の締結等の法的な対策を行うことが重要となります。

技術的対策の中でもサーバーのアクセスログの管理やメールの監視などの対策は、不正行為の抑止と早期発見の観点、不正競争防止法における営業秘密の要件である秘密管理性の観点から、営業秘密管理における重点項目となっています。

不正アクセス防止の実施状況について、従業員数301人以上の製造業は何らかの対策を実施している割合が90.3%であり、従業員数が多い製造業ほど対策を実施しています。また、実施している対策は「営業秘密を一般情報と分離して保管」が最も高くなっています（28.1%）。

環境的対策の実施状況を把握するために、不正に持ち出せば見つかるような何らかの環境を整える対策として実施しているものがあるかどうかについても質問をしていますが、その対策については、実施割合は高くても20~30%程度にとどまっていました。

特に営業秘密情報を外部に電子メールで送信する際に、環境面での情報漏えい対策として注意すべき「外部への電子メール送信時のチェック機能導入」は20%に達しておらず、電子メールの利用時の対策（「電子メールの添付ファイルの制限または禁止」「電子メール送信時の上長確認フローを運用（必ず上司等がCCに追加される設定を行っている等）」でも2020年度調査時からその割合が微増はしたものの20%弱に留まったことも合わせて考えると、全体的に電子メールの利用の際の情報漏えい対策への意識が依然として低いと考えられます。

営業秘密管理においては、秘密保持契約の締結や競業避止義務契約の締結も法的な対策として有効なものと考えられます。

④ 最近の動向を踏まえた対策（サプライチェーン管理、クラウドサービス・生成AI利用時等）

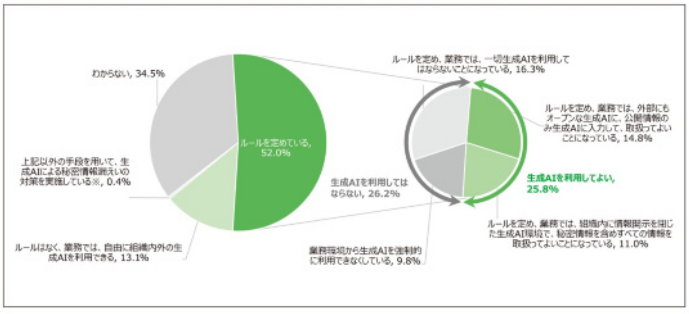
生成AI の業務利用可否と取扱い可能な情報の種別について、生成AIの業務利用可否について、何らかのルールを定めているのは52.0%となっており、そのうち、生成AIを利用してよいこととしている割合は25.8%、利用してはならないとしている割合は26.2%となっています（【図2】）。

クラウドサービスを使用した営業秘密の共有や参照について、クラウドを利用した秘密情報の共有を実施している割合は50.4%となっており、2020年度調査と比較して大幅に増加しています（【図3】）。

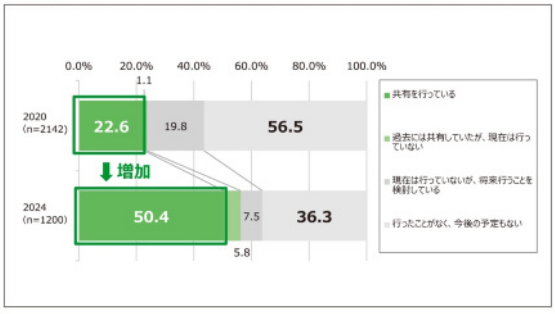
企業のデジタル化の中でクラウドサービスや生成AIの利用、テレワークの活用が進んできていますが、クラウドサービスの利用においては、利用者側の設定ミスやパスワードの管理の不備などが原因で、情報漏えいにつながるリスクがあり、また、生成AIの利用においては、営業秘密等の機密情報を誤ってプロンプトに入力することで、その情報が学習データとして利用されるおそれがあります。

自組織の営業秘密を保護するためにも、クラウドサービスや生成AIの利用、テレワークに関してルールを定め、従業員等が適切に情報を取扱えるようにする必要があります。

【図2】生成AIの業務利用可否と取扱い可能な情報の種別



【図3】クラウドサービスを使用した営業秘密の共有や参照



※「企業における営業秘密管理に関する実態調査2024」報告書（IPA）（URL：https://www.ipa.go.jp/security/reports/economics/ts-kanri/tradesecret2024.html）