SPN
Security Protection Network

ＳＰＮレポート

Security Protection Network Report Series.

～情報漏えい事故に関するアンケート～

第１版　2018 年１月
株式会社エス・ピー・ネットワーク

■　目次

Ⅰ．はじめに

企業や個人が、情報の価値を見直し新たな視点から活用する動きが加速しています。最近では IoT やビッグデータなどの活用化が図られようとしています。企業として、必要な情報を収集し、分析した上で、営業戦略の策定や事業の合理化、発展のために活用していくことは、今後のビジネス展開を行なっていく上で最重要課題の一つとなっていくと考えられます。

他方、飛躍的に進む情報の活用に対して、不安や懸念を示す声も大きいのも事実です。実際、情報を大量に、かつ瞬時に流通させることを可能とする技術的な発展に比して、企業の情報管理態体制個人の意識・モラルが追いついておらず、結果として従前では考えられなかった規模の情報漏えい事故や、不適切な情報発信がなされるような事件が相次いでいます。企業にとって、こうした情報管理に関する不安や懸念を解消し、個人や他の企業から安心して情報を委ねられるような体制を構築することがこれまで以上に求められています。かかる意味で、企業にとって、信頼に足る情報管理体制と情報の有効活用は車の両輪の関係にあると言えます。情報の活用ばかりに気をとられ、その管理体制の構築を疎かにしていれば、いずれ顧客や他企業からの信頼を失う事故が起き得ますし、情報管理体制を闇雲に整備したとしても、有効な活用ができなければ本末転倒です。とりわけ、情報の管理面に目をあてると、企業活動の中で得られる技術情報や顧客の個人情報、取引先企業の機密情報などは、企業にとって重要な情報資産であり、厳格な管理が求められます。万が一、情報漏えい事故が発生してしまうと、企業の経済的損失だけではなく、企業の信頼やブランドイメージにまで影響が及びます。このようなリスクに対して企業や団体を中心に、脅威に対する認識の高まりとともに情報漏えい対策への意識は高まっていると思われますが、一方で、情報漏えいに関する事故は頻繁に報じられていることから、事故の発生件数そのものは減少していないのが実情です。

事故の報道や他社の事故事例を見て、「よその会社・組織で起こっていること」、「うちの会社ではありえない」などと対岸の火事として傍観しがちです。しかし、公表されている情報漏えい事例はむしろ氷山の一角と認識すべきです。会社で管理する情報の漏えい事故は、決してほんの一握りの会社・組織での特別なことではありません。

最も懸念すべきは、根本的な原因に対応しているとは思えない対策が、まるでそれが特効薬であるかのような位置づけで講じられ、肝心な、本来取り組むべき情報セキュリティ対策が置き去りにされていることです。情報セキュリティというと、ツールに頼りがちな面がありますが、一定の条件のものを検出したりする機能的な面は重要であるものの、それを使うための体制やプロセス、自社のリスクを考慮した上で、バランスのよい情報セキュリティ対策を講じることが大切です。企業によってその規模や対策にかけるコスト、人的な体制も異なります。そのため、すべての弱点に対策はとれないというのが現実ですが、だからこそ、一番効き目のある対策はどれか、特定するために弱点を洗い出すことが重要となります。厳格な情報管理を実現させるためには、万全の（あるいは万全を目指す）情報漏えい対策が不可欠であり、それが情報漏えいを防ぐためだけではなく、企業そのものを守ることにもつながります。そのためにも、まずは情報漏えい事故による被害の実態を知ること、そして事故が発生した経路や原因など、情報漏えいについての現状を把握し、効果的な対策を計画、実行していく必要があると思われます。

この度、弊社では、企業における情報セキュリティ事故対応の準備状況や対策の実施状況の実態を把握するためにアンケート調査（以下、「本調査」という）を実施しました。本調査が、貴社における情報管理体制を最適な状態に維持するためのきっかけとなり、事故発生時の事業継続や事態を極小化するための指標として活用していただければ幸いです。

Ⅱ．本調査の総括

本調査は、全国の企業・組織（以下、「企業等」という）における情報流出/漏えい対応の準備や発生状況、情報資産の管理実態を把握することを目的としました。その結果、自社で保有する情報資産の漏えいや流出に対して危機意識を持っている企業等が 89.4%、事故発生時の対応手順や準備をしている企業等が 68.6%を占めており、自社内外問わず、相次ぐ情報漏えい事件や事故を機に、企業等の情報漏えいに対する危機意識やその準備に対する備えは高まりつつあることがうかがえます。

一方で、実際に発生した事故への対応としては、その対応に苦慮した点として「流出原因およびその経路の特定の調査」「勤務先へのクレーム」「損害賠償請求」などの直接的な被害のほか、間接的な損害として「対応のための時間外労働」「顧客や取引先が納得してくれない」「事故対応の収束が見えない」など対応担当者の先が見えない不安や対応疲れなど多大な苦労が滲む記述も確認されました。

また、今後想定・懸念される事故が、勤務先で過去発生した事故とほぼ同じ順位と構成である傾向が確認されました。これは、過去同様の事故が勤務先内で発生しているものの（にもかかわらず）、効果的な対処が検討されていない、問題や脆弱性が軽視・放置されている、といった状況から、再発するリスクが高いままであることを示しているものと読み取ることができます。言うまでもなく、事業者には、管理する情報資産ごとにその脅威を認識して、引き続き警戒レベルを緩めることなく、システム面・運用面の双方で多層的な防御策の導入や、従業員への徹底した意識づけやルールの周知など継続した取り組みが求められます。

さらに、情報漏えい事故発覚の契機は、「勤務先内から」が全体の回答数の約 6 割を占めています。一方、「勤務先外から」は、その約半数です。ただ、被害者など外部からの通報で被害が発覚した場合は、隠蔽などが疑われ、組織の管理体制を大きく問われることになりますし、事故が発生しても長期間表沙汰にならないことが多いため、漏えいした情報の規模や影響が大きくなる可能性は高まります。このような、被害が顕在化するまで侵入や情報の持ち出しの事実に"気づけていない“だけのケースも現実には多くありますので、現在の対策が本当に機能しているかどうかの確認と、情報管理上の不備や脆弱性を積極的にチェックして自ら問題に“気づける”体制作りが求められます。潜在的なリスクは既に拡大していると認識すべきであり、自社における情報管理上の不備や脆弱性をあらためてチェックし、問題をいち早く検知し対処できる仕組みと、それが機能しているかを継続的に確認する、繰り返し検証する仕組みを整える必要があります。

以下、本調査におけるトピックスをいくつかご紹介いたします。

① 情報セキュリティ対策の取り組み（図表 6）

既に実施している主な取組みとしては、「重要情報のバックアップ」「利用者や PC の認証や権限管理」「外部へのインターネット接続の監視・制限」「私用端末の業務利用禁止」「記憶媒体の管理」「紙媒体の管理（廃棄方法、持ち出し制限等）」「情報セキュリティ対策に関する教育・啓発・注意喚起」が挙げられます。

② 勤務先で発生した情報漏えい事故（図表 10）

最も影響の大きかった事故としては、「書類持ち出し時の紛失・盗難」「業務で利用する PC、記憶媒体、スマホなどの紛失・盗難」「サイバー攻撃（不正アクセス、標的型攻撃メール）」がそれぞれ 10%以上を占めており、次いで、「内部関係者（従業員、派遣社員等）の不正行為」「PC・記憶媒体や書類の誤廃棄」「業務で利用する PC やスマートフォン、業務システムやサーバのマルウェア感染」「電子メールの誤送信」がそれぞ

れ約 9%を占めています。

③　情報漏えい時に発生した被害（図表 12）
情報漏えい時の具体的な被害の事例としては、「勤務先へのクレーム」20.7%、「漏えい対象者の金銭的被害」6.1%、「空き巣・ストーカー」4.5%、「漏えい対象者の精神的被害」11.7%などが確認されました。また、「競合への営業秘密の漏えい」が 8.4%となっています。一方、「特に影響と被害はなかった」が 26.5%で最多を占めています。

④ 事故時の対応手段（図表 15）
事故時の主な対応としては、「被害者への訪問謝罪」「被害者への電話連絡、謝罪」「被害者への詫び状の送付」のほか、原因究明のための「被害範囲・影響範囲の確認」、「現場・証拠の保全」「原因究明のための調査（フォレンジック含む）」が実施されています。

⑤ 事故の再発防止策（図表 19、20）
事故の再発防止策として、「従業員に対する教育・研修」が 53.1%、「規程や運用方法・手順の改定/改善」が 36.9%を占めており、人の教育とルールの見直しに最も重きを置いていることが分かります。

その他本調査結果から留意すべき点として指摘されるのは、「図表 11：漏えいした情報の種類」で、「新商品に関する情報」、「新製品秘匿情報」、「営業秘密」、「極めて高レベルな機密情報、ここでは具体的に記載不可」「本人性格等、考えられるすべての情報」「顧客の取引情報」が記載されている点です。企業等の陥りやすい認識としては、「狙われるほど重要な情報がない」ため攻撃や持ち出しの標的にはならない、という考えがあります。ただ、企業の持つ従業員や顧客などの個人情報や営業秘密を狙う国内外の攻撃の事例では、標的となった企業は規模や業種に関わらず狙われていることがわかっています。そして、実際に標的となった場合の損害は決して小さいものではなく、業績や事業継続に大きな影響を与えるものになりがちです。これらの現実を直視し、今発生している事件・事故を自分事としてとらえ、自社の持つ情報資産とその重要性を把握した上で必要な対策を考えるべきです。

また、本調査で判明した情報漏えい流出事例から気付かされることは、今現に発生している攻撃やミスなどは特別に新しいものではなく、情報に対する脅威に大きく変化はないものの、「本来実施すべき基本的な事項が守られてない」ことが大きな事故に発展したということです。

この点、情報セキュリティ対策で重要なのは、「資産」の把握と優先付けに基づいたポリシーの策定や監査体制などの組織強化や事故発生時の対応方針・プロセスの明文化と徹底、迅速に対応できる体制の構築です。言い換えれば、「情報」を扱う「人」の部分に脆弱性があるということ、情報管理に関する内部統制システムも、システムを使う側の「人」がそれを無視・逸脱した使い方をしてしまえば、情報セキュリティ対策として機能しないということを改めて認識しなければならないのです。その意味で、情報資産に対する脅威は、既にすべての組織にとって他人事ではなく、事業継続性を維持する上での最重要対策事項だと言えます。

Ⅲ. 本調査実施概要

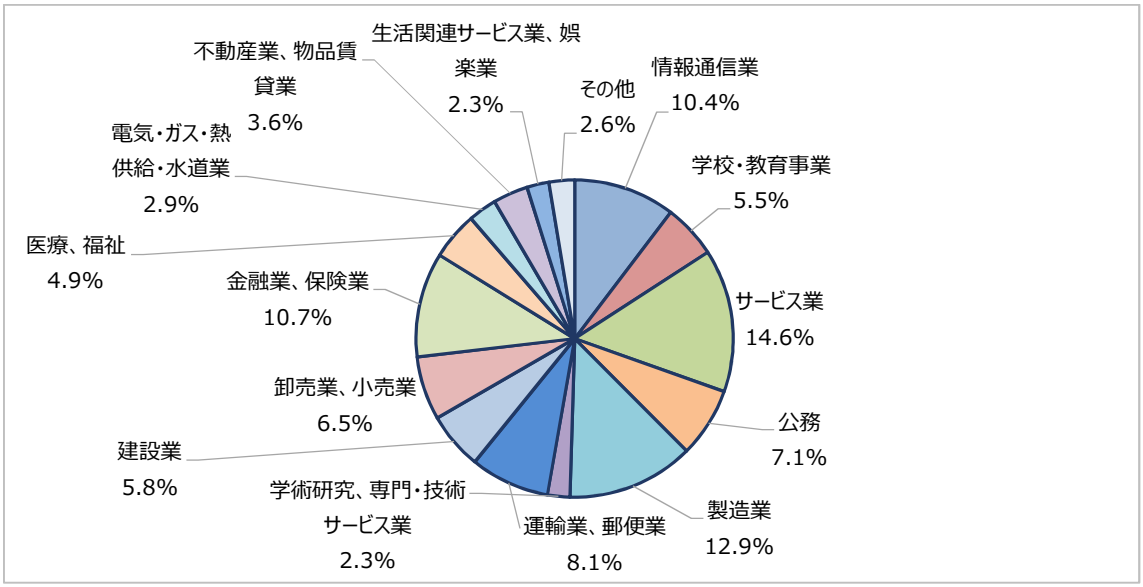
1. 調査概要

調査手法	ウェブアンケート
調査対象	全国の企業や組織で情報セキュリティ事故事案の経験や情報管理体制を把握している担当者。
調査期間	2017 年 9 月～10 月
調査項目	・ 情報セキュリティ事故対応への準備状況 ・ 情報セキュリティ事故の発生状況 ・ 情報セキュリティ事故発生時の対応状況 ・ 情報保護対策の現状と課題
有効回答数	309

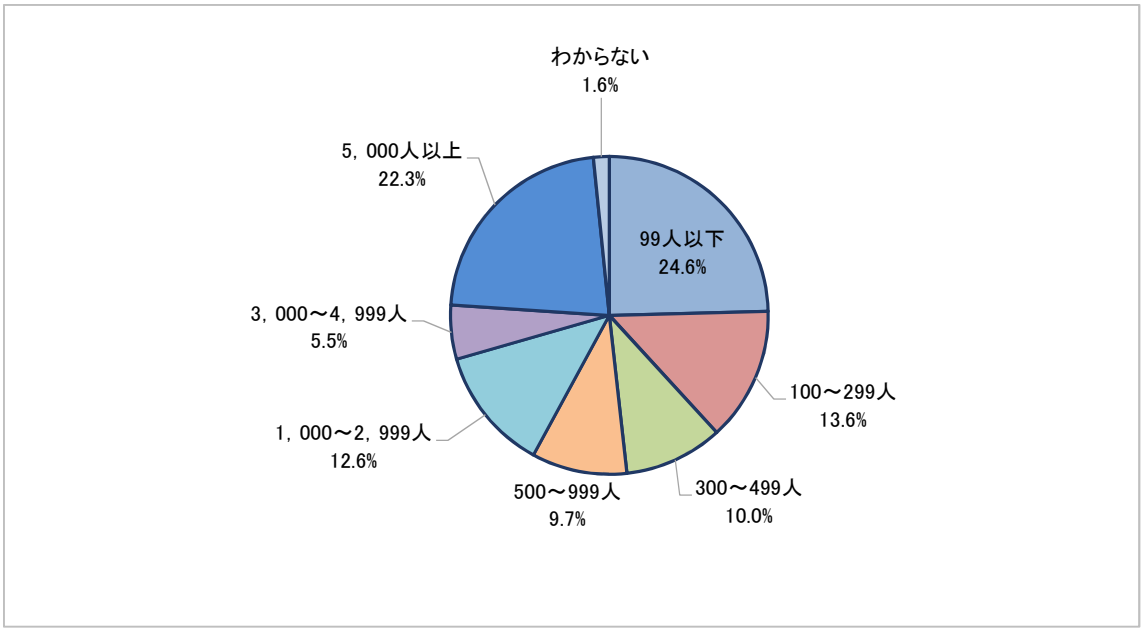
２．回答企業の概要

本アンケートの有効回答者数は 309 名で、その業種、従業員数及び所属部門は、下記図表 1、図表 2、図表 3 のとおりです。なお、回答者については、勤務先で事案の規模にかかわらず保有する情報の漏えいや流出事故対応への関与や経験を有し、事案を認知している方や情報の管理体制を認識されている方を対象としています。

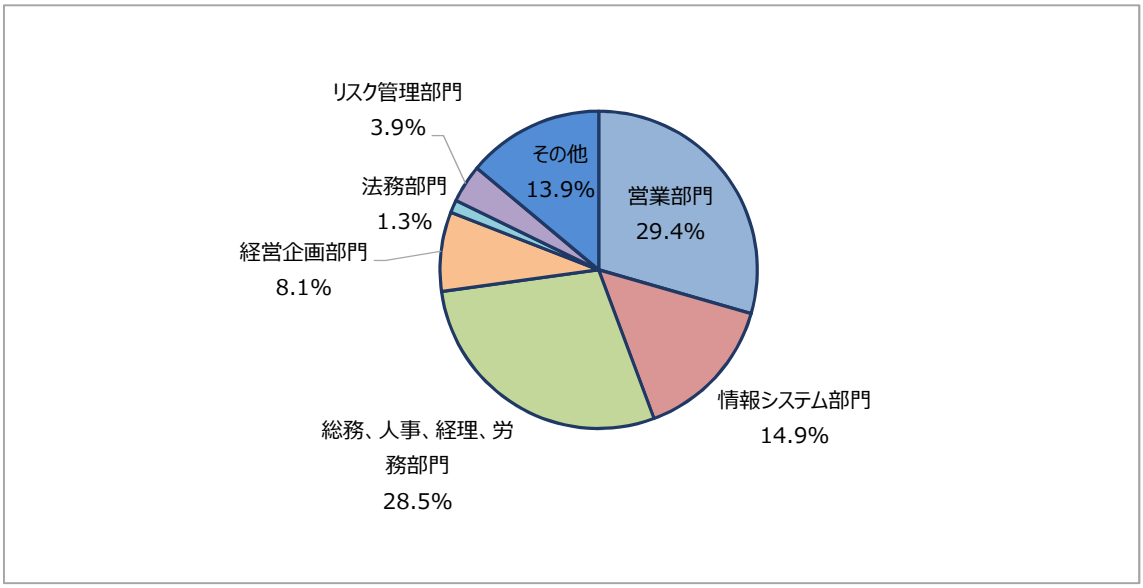
図表１ ：回答者の属性：業種



図表 2 ：回答者の属性：従業員数



図表 3：回答者の属性：所属部門

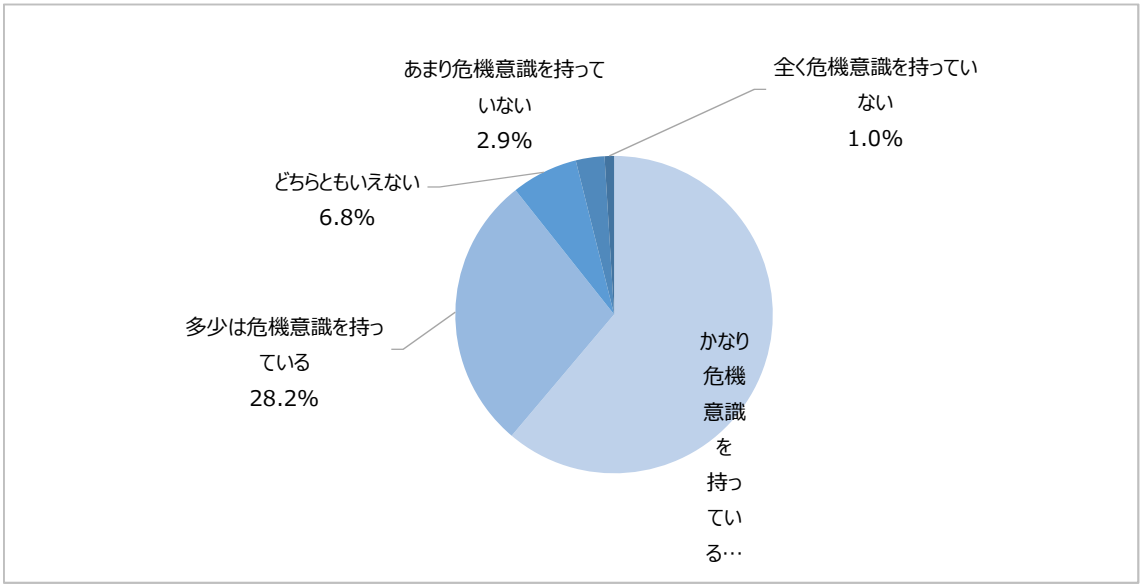


Ⅳ. 本調査結果の詳細

１. 集計結果

1-1）危機意識

図表 4：あなたの勤務先では、保有する情報（顧客情報、従業員情報、営業秘密等）の漏えいについて、優先すべきリスクとして危機意識を持っていますか。



図表 4 は、保有する情報の漏えいリスクに対する意識について尋ねたものです。

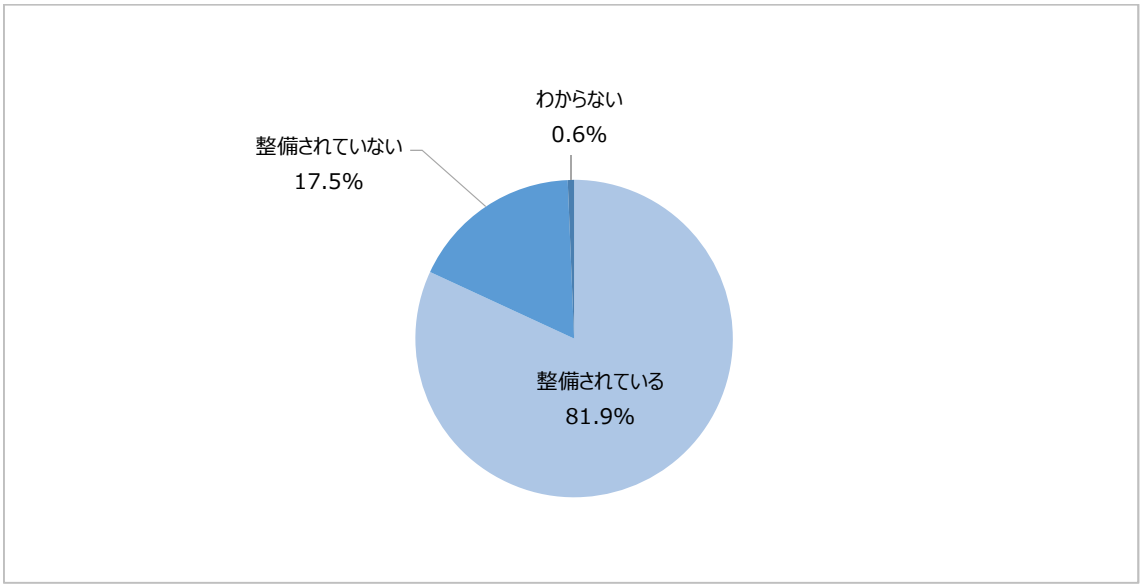
結果は、「かなり危機意識を持っている」の回答者が過半数の 61.2%、「多少は危機意識を持っている」が 28.2%となり、危機意識を持っている回答者は両者を合わせた 89.4%を占めています。自社内外問わず相次ぐ情報漏えい事件や事故を機に、企業・組織の情報漏えいに対する危機意識が高まっていることがうかがえます。企業における情報漏えいの原因は、従業員や内部関係者による管理ミス、誤操作、紛失・置き忘れなど、「うっかりミス」による情報漏えいが全体の約 8 割を占めていると言われています。

▼ 特定非営利活動法人 日本ネットワークセキュリティ協会「2016 年 情報セキュリティインシデントに関する調査報告書～個人情報漏えい編～」
http://www.jnsa.org/result/incident/data/2016incident_survey_ver1.2.pdf

例えば、重要情報が保存された USB メモリの紛失、書類の誤廃棄などが原因で発生する情報漏えいでは、社内全体に情報セキュリティ対策に関するルールが浸透しておらず、従業員一人ひとりがその重要性について理解していない可能性があります。また、従業員が手元の端末を使ってメールを送受信したり Web サイトを閲覧したりする中で、マルウェアに感染することは少なくないですし、必然的に、従業員の端末に影響を及ぼしやすいセキュリティ対策や従業員向け情報セキュリティ教育の重要性が高まることになります。従業員への影響を最小限に抑えつつ、有効な対策や教育を進めるのは簡単なことではありませんが、情報漏えい対策の第一歩は、従業員の意識改革と言っても過言ではありません。

1-2）規程・マニュアル等の整備

図表 5：あなたの勤務先では、保有する情報（顧客情報、従業員情報、営業秘密等）を管理するための規程やマニュアルが整備されていますか。



図表 5 は情報管理上の規程やマニュアルの整備状況を示したものです。81.9%が「整備されている」、17.5%は「整備されていない」と回答しています。「整備されていない」方に着目すると、この数値は決して少ない割合であるとは言えず、未だにルールそのものがなく、あったとしてもそれが明確になっていない、あるいは見直しがなされていない企業・組織が 2 割近くもあると捉えるべきです。当然、規程やマニュアルを整備するだけでは情報管理の実効性を高めることにはダイレクトにつながりませんが、情報資産を守るうえでの全社的なルールや取り組みの方針が明確に存在することは、情報を管理するための大前提です。企業として情報セキュリティの実効性を確保するためには、行なっている業務や利用しているシステムなどにおける情報セキュリティの要求レベルを明らかにして、その要求レベルを充足すべく、網羅的、体系的な対策に組織全体として取り組む必要があります。情報セキュリティの実効性確保に向けてどのようにして取り組んでいくのか、基本的な考えを経営者が示し、その基本的な考えに基づいて具体的な対策を定め、組織全体で取り組んでいくことが求められます。その中核となるのが情報資産を守る方針の策定だと言えます。規程やマニュアルは、経営者の情報セキュリティに対する強い意志を表したものであり、経営者から従業員に向けた命令書とも解釈できます。

情報資産を守る対策は画一的なものではなく、企業や組織の持つ情報や組織の規模、体制によって、大きく異なります。業務形態、ネットワークやシステムの構成、保有する情報資産などを踏まえた上で、その内容に見合った方針を作成しなければなりません。さらに、情報資産を守るという目的と実態の乖離の有無を確かめる必要があり、見直しを継続的に検証し現場に即した運用体制と周知する仕組みが不可欠となります。

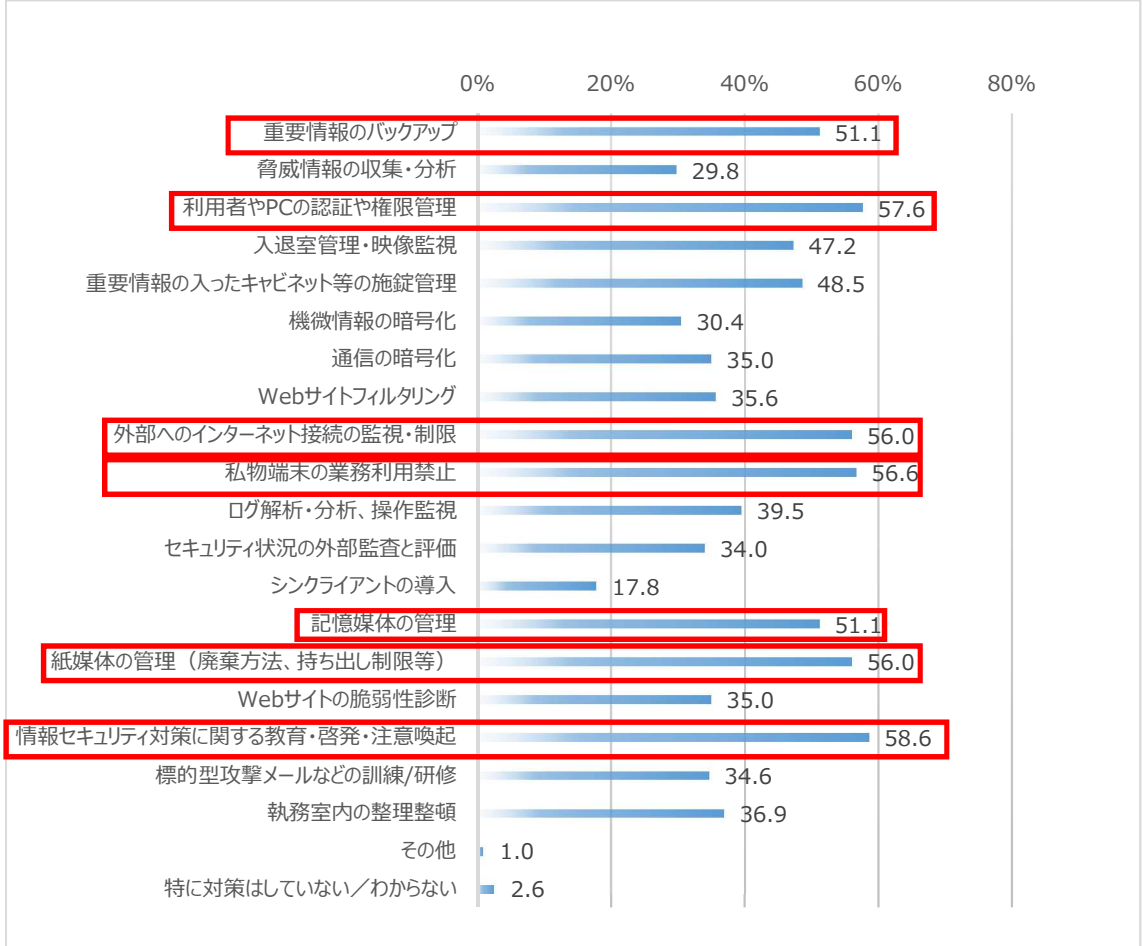
【規程・マニュアル策定時の留意事項】

- 守るべき情報資産を明確か。
- 対象者の範囲は明確か。
- できる限り具体的に記述されているか。
- 社内の状況を踏まえて、実現可能な内容か。
- 運用や維持体制を考慮しながら策定されているか。

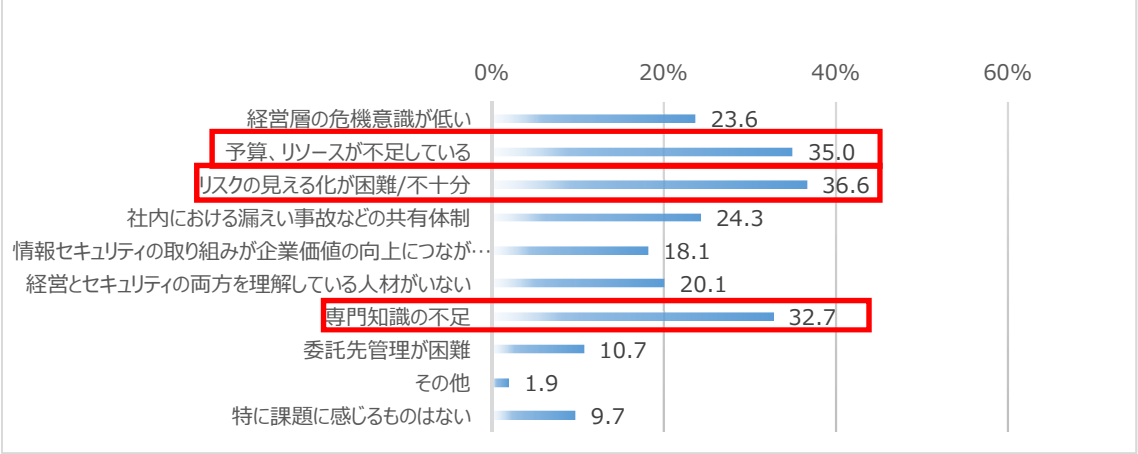
・ 形骸化を避けるために、違反時の罰則を明記しているか。
・ 見直しが適宜なされているか。
・ 運用状況の監査を行うことで実行性が担保されているか。

1-3）情報セキュリティ対策とその課題

図表 6：あなたの勤務先で実施している情報セキュリティ対策は何ですか。（複数回答）



図表 7　あなたの勤務先で、情報セキュリティ対策を進めるうえで、特に課題を感じるものを選択してください。（複数回答）



図表 6 のとおり、実際に行なわれている情報セキュリティ対策の取り組みとしては、「重要情報のバックアップ」「利用者や PC の認証や権限管理」「外部へのインターネット接続の監視・制限」「私用端末の業務利用禁止」「記憶媒体の管理」「紙媒体の管理（廃棄方法、持ち出し制限等）」「情報セキュリティ対策に関する教育・啓発・注意喚起」が 50%を超えており、その他の項目と比較して割合的にやや高いという結果が得られています。一方、情報セキュリティ対策を推進するうえでの「課題」は、図表 7 のとおり、「予算、リソースが不足している」「リスクの見える化が困難/不十分」「専門知識の不足」が高い割合を示しています。

ウィルス対策ソフト、ファイアウォール、IPS(Intrusion Prevention System)※1、WAF（Web Application Firewall）※2 など、セキュリティ対策のツールは多種多様に存在しますが、完璧な情報セキュリティ対策を目指すのであれば、これらすべてを導入して効率よく運用しなくてはなりません。しかしながら、予算も潤沢で人材も豊富な企業ならいざ知らず、とりわけ予算も人材も余裕がない中小企業では、すべての脅威に対して対抗策を講じることは難しく、これがいま、日本国内の情報セキュリティ事情における大きな課題でもあります。また、専門知識や専門の人材の不足が表しているとおり、弊社が過去に発生した情報漏えい事案において、「実は導入していたツールに（今回の事故発生の）原因を防ぐための機能は備わっていたが、その存在を知らずに初期状態のまま運用していたため、漏えいを防ぐことができなかった」というケースもありました。つまり、どんなに高価で高機能なソリューションを導入しても、理解がないままに運用していては、意味をなさないということです。

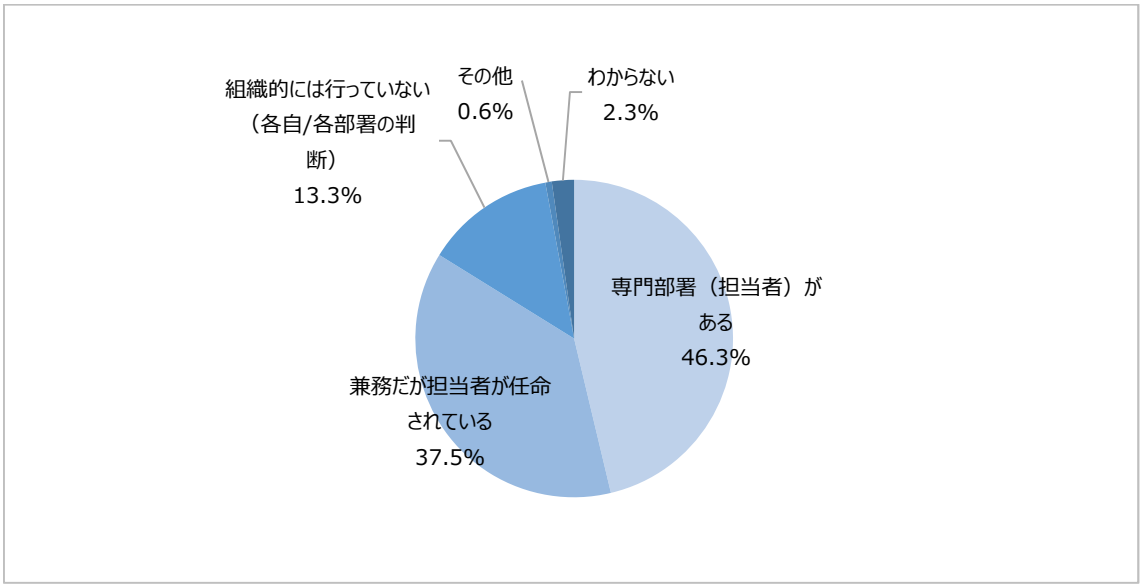
一方で、情報セキュリティ対策は、巨額の設備投資を伴うものが多いのも事実です。そのため、情報セキュリティ対策においても、力の入れどころと抜きどころ（相対的に厳格に対策しない部分があること）が重要であり、経営者はどこまで情報セキュリティ対策の現場に権限を与えるべきか、経営層が判断する情報として何を提示させるか明示する必要があります。企業がリスク管理に投入できるリソースは限られています。また、リソースの配分はあくまで自社のリスク判断事項となります。100%の未然防止は困難だという前提に立てば、リスクが高いと判断される部分にリソースを重点的に配分（投入）しよう（逆に、そうでない部分についてはより簡素化した取組みレベルで行う）とする「リスクベース・アプローチ」が実務的かつ有効だと言えます。また、情報セキュリティは、ビジネスの阻害要因ではなく、どうすれば安全に実現できるかという思考に切り替えるべきです。そうすると、情報セキュリティは、利便性の対義語ではなく、利便性を安全に実現できる手段に代わります。

※1 ネットワークやコンピューターへの不正アクセスを検知し遮断するシステム。IDS（Intrusion Detection System ： 侵入検知システム）は不正アクセスを検知するのみだが、IPS は遮断する仕組まで備える。

※2 Web アプリケーションのぜい弱性を悪用した攻撃から Web サイトを保護するセキュリティ対策。Web サーバーの前段に設置して通信を解析・検査し、こうした攻撃から Web サイトを保護し、不正ログインを防ぐ役割で用いられる。

1-4）セキュリティ対策体制

図表 8:あなたの勤務先では、情報セキュリティ対策をどのような体制で行なっていますか。



図表 8 では、情報セキュリティ体制として、「専門部署（担当者）がある」46.3%、「兼務だが担当者が任命されている」37.5%、「組織的に行なっていない（各自/各部署）」13.3%という結果が得られています。規模の大きな企業で、セキュリティ部門やチームを設け、それなりの人員を割り当てている場合もあれば、中小の規模で、専任のシステム担当が居るわけでもなく、ただ、パソコンに詳しいというだけでセキュリティ担当になってしまったというようなケースも多く見受けられます。

通常、コンプライアンス・IT 担当者は、「従業員によるファイル共有は社内のポリシーに沿ったものであるか」「個人情報が含まれているファイルが不特定多数の人がアクセス可能な場所に保管されていないか」などを監視する役割を担っていますが、組織や企業で作成されるデータの膨大さを考えると、すべてを完全にカバーし、完璧な保護を情報システム部門やコンプライアンス部門だけで実行するのは、非効率的であり非現実的であるともいえます。情報セキュリティ対策を効率的に運用させるためのポイントのひとつは、情報システム部門・コンプライアンス部門が、実際にファイルの作成・更新している現場のメンバーと緊密な連携をすることです。具体的には、情報セキュリティインシデントの対応を 情報システム部門コンプライアンス部門がすべて実行するのでなく、一部は現場の担当者に対処してもらう、などという方法が考えられます。

いずれにしても、多くの企業で、「情報セキュリティ対策」はパソコンやネットワークを管理する情報システム部門の担当業務となっていますが、サイバー攻撃などの脅威が高度化するにつれ、より専門性の高い対応スキルが求められるようになってきました。体力のある企業では、社内に SOC（ソック：Security Operation Center）※1 や CSIRT（シーサート：Computer Security Incident Response Team）※2 などの専門部署を設けて監視や対応を行うところも増えてきましたが、すべての企業が高度なスキルを持った人材を確保できるわけではありません。しかし、いまや情報セキュリティのリスクを持たない企業はどこにもないといっても過言ではなく、対策をいかに講じるかが経営課題の一つとも言えます。ただ、こうした専門的な人材の技術を身につけるには、時間がかかりますし、会社の業務も熟知しなければなりません。また、社外の経験のある人材をスカウトしても、即戦力となるわけで

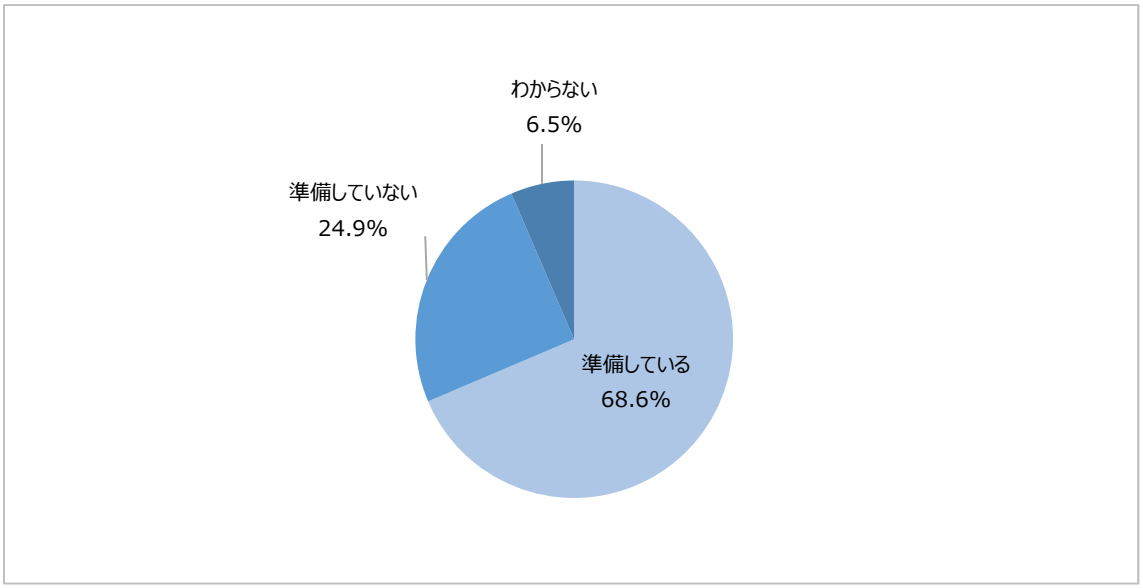
はないということが人材の育成を難しくしています。今後、IoT の普及によってインターネットにつながるデバイスが爆発的に増えるなかで、情報セキュリティリスクは大きくなる一方です。セキュリティ人材を育成することが、社内全体のリテラシーを向上させる原動力にもなりますので、企業には情報セキュリティに対する適正なコスト配分を行なう必要性が高まっていると言えると思います。

※1 企業などにおいて情報システムへの脅威の監視や分析などを行う、役割や専門組織を意味する。SOC は、ファイアウォールや侵入検知システム(IDS)といった情報セキュリティ機器、ネットワーク機器や端末のログなどを定常的に監視し、場合によっては起きた事象を分析して、 脅威となるインシデントの発見や特定、連絡を行う役割を持つ。また、そのインシデントの影響範囲を調べたり、あらかじめ想定されたリスクや指標に基づいて、インシデントを評価したりすることもある。

※2 組織内の情報セキュリティ問題を専門に扱う、インシデント対応チームやコンピュータシステムやネットワークに保安上の問題に繋がる事象が発生した際に対応する組織を指す。社内の情報システムや通信ネットワークで、ウィルス感染や不正アクセス、サービス拒否攻撃（DoS 攻撃）など情報セキュリティ上の脅威となる現象や行為が発生した際に、組織内の対応窓口となって被害の拡大防止や関連情報の収集・告知、再発防止策の策定などの活動を行う。また、外部の CSIRT と連携して事件・事故の被害情報やシステムの脆弱性についての情報を共有したり、一般利用者へ情報セキュリティに関する教育や啓発、広報などの活動を行うこともある。

1-5）有事の際の備えと準備

図表 9：あなたの勤務先では、重要情報の流出や紛失盗難があった場合の対応手順などを作成し、事故が発生した場合に備えた準備をしていますか。



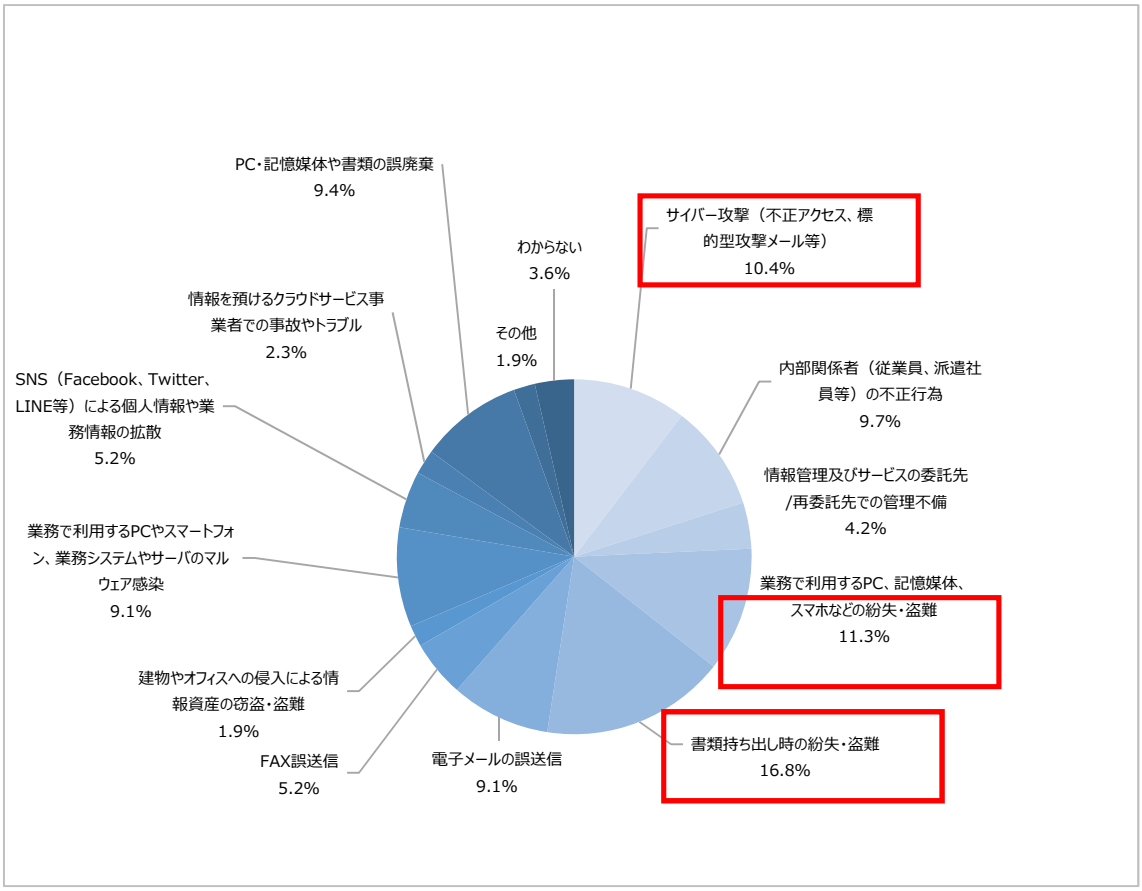
図表 9 では、事故発生時の対応手順や準備について、「準備している」が 68.6%、「準備していない」が 24.9%、「わからない」が 6.5%という結果が得られています。約 3 割が、対応手順や準備が未実施・未周知という点は、大きな懸念点だと言えます。緊急時における誤った対応は被害を大きくさせる危険がありますので、日頃から連絡体制や対応手順を確認し

ておくことが重要です。連絡体制や対応手順について、判断に迷う記述や対応方法に不明な記述がある場合には、上司・管理者に確認し、緊急時にすばやい行動がとれるよう、「初期対応」、「一時対応」、「復旧作業」等の優先順位付けされた手順を確認しておく必要があります。

また、有事の際に適切な行動が取れるかどうかは、訓練を実施することで評価できます。最悪の状況は、危機発生時にマニュアルや手順が機能しないことです。さらに、マニュアルや手順があれば、多くの人は「対策が取られている」、つまり「リスクは一定以下に抑えられている」と判断して行動してしまう点にも十分な注意が必要です。これを避けるためには、複数のシナリオを想定して、対応の要領が不明な点を繰り返し訓練することでマニュアルの有効性を評価し、改善に努めていくことが重要となります。地震、火災などの天災時に言われていることですが、いくら完璧なマニュアルを作っても、人がその通りに動けなければ意味がありませんので、従業員に対する訓練は重要です。例えば、大震災の強烈な揺れの中では、パニックになり、落ち着いて考えながら適切な行動はなかなか取れないものです。ある程度、訓練等を通じて体で覚えることが大事であり、これは情報漏えい事故についての対応でも同じだと言えます。

1-6）最も影響のあった事故

図表 10：あなたの勤務先で過去発生した情報漏えいや流出事件・事故について、被害や影響が最も重大だったものを一つ選択してください。



図表 10 は、今回の調査対象者の勤務先で発生した情報漏えい事故で最も影響の大きかったものを示しています。結果は、「書類持ち出し時の紛失・盗難」「業務で利用する PC、記

憶媒体、スマホなどの紛失・盗難」「サイバー攻撃（不正アクセス、標的型攻撃メール）」がそれぞれ 10%以上を占めており、次いで、「内部関係者（従業員、派遣社員等）の不正行為」「PC・記憶媒体や書類の誤廃棄」「業務で利用する PC やスマートフォン、業務システムやサーバのマルウェア感染」「電子メールの誤送信」がそれぞれ約 9%を占めています。

これらの管理ミスや紛失・盗難への対策は、情報管理の基本でもあり、どの企業でもルールがあり、対策が講じられているはずですが、残念ながら事故が減っていないのが現実です。どれだけ研修等でリスクを周知し、注意喚起を行なっていたとしても、ミスを完全に防止することは不可能ですが、ルールを知っていて守ろうとする気持ちがあるにもかかわらず、ルールどおりに業務を実施できない場合は、環境に問題がある可能性があります。例えば、業務量が過剰で仕事を自宅に持ち帰らなくてはならなかったり、短時間で業務を進めなくてはならなかったりする環境で、「個人情報を含むデータを社外に持ち出さない」「メールの送信前に確認を行う」というルールを設けていたとしても、確実に守っていくことは難しいのではないでしょうか。このようなケースでは、そもそもルールどおりに業務を進めることのできる環境かどうかを検証することが求められるでしょう。

ただ、ルールの存在を知っていて、それを守ることのできる環境が整っているにもかかわらず、「別に守らなくてもいいだろう」「こんなルールは意味がない」「周囲もやっているから、この程度のルール違反は大丈夫」といった、現場担当者の誤った認識や意識の低さから、ルールが守られないケースもあります。このような場合は、入社後に情報セキュリティに関する研修を義務づけたり、入社から時間の経った従業員にも一定期間ごとに研修を行ったりして、なぜそのルールが必要なのか、守らないことでどのような問題が起こりうるのかについて繰り返し教育し、ルールを守るための動機づけを行う必要があります。

また、個人が持ち歩く私物のモバイル装置や私物のスマートフォンの業務利用についても、多くの現場では企業のセキュリティポリシーに違反しながら、利便性を重視したデータの取り扱いが行われていることが浮き彫りとなっています。また、そのような働き方（自宅で業務をしなければならない）に対して、会社が何らの手立てをしないことは、事案発生後、厳しく非難されることになります。当人に悪意はないとしても、セキュリティポリシーの強化を実現しつつ、現場での利便性を兼ね合わせた代替ツールを検討するといった対策が必要となると言えます。

その他、サイバー攻撃による被害も国内外問わず毎年増加しています。昨今の情勢から、ほとんどの産業が IT と密接に結びついているため、新しい技術やサービスが広まれば、同時にサイバー攻撃を受けるリスクも高まるというジレンマにどの企業や個人も陥っています。特に、サイバー攻撃者は、情報セキュリティインフラの構造上、企業等よりも優位な立場にあります。攻撃者は防御側にあるセキュリティホールを一つ見つければ、そこから様々な攻撃を仕掛けられるのに対して、防御側は、全てのセキュリティホールを把握し対策を取ることが必要となりますが、これは事実上不可能だと言わざるを得ません。

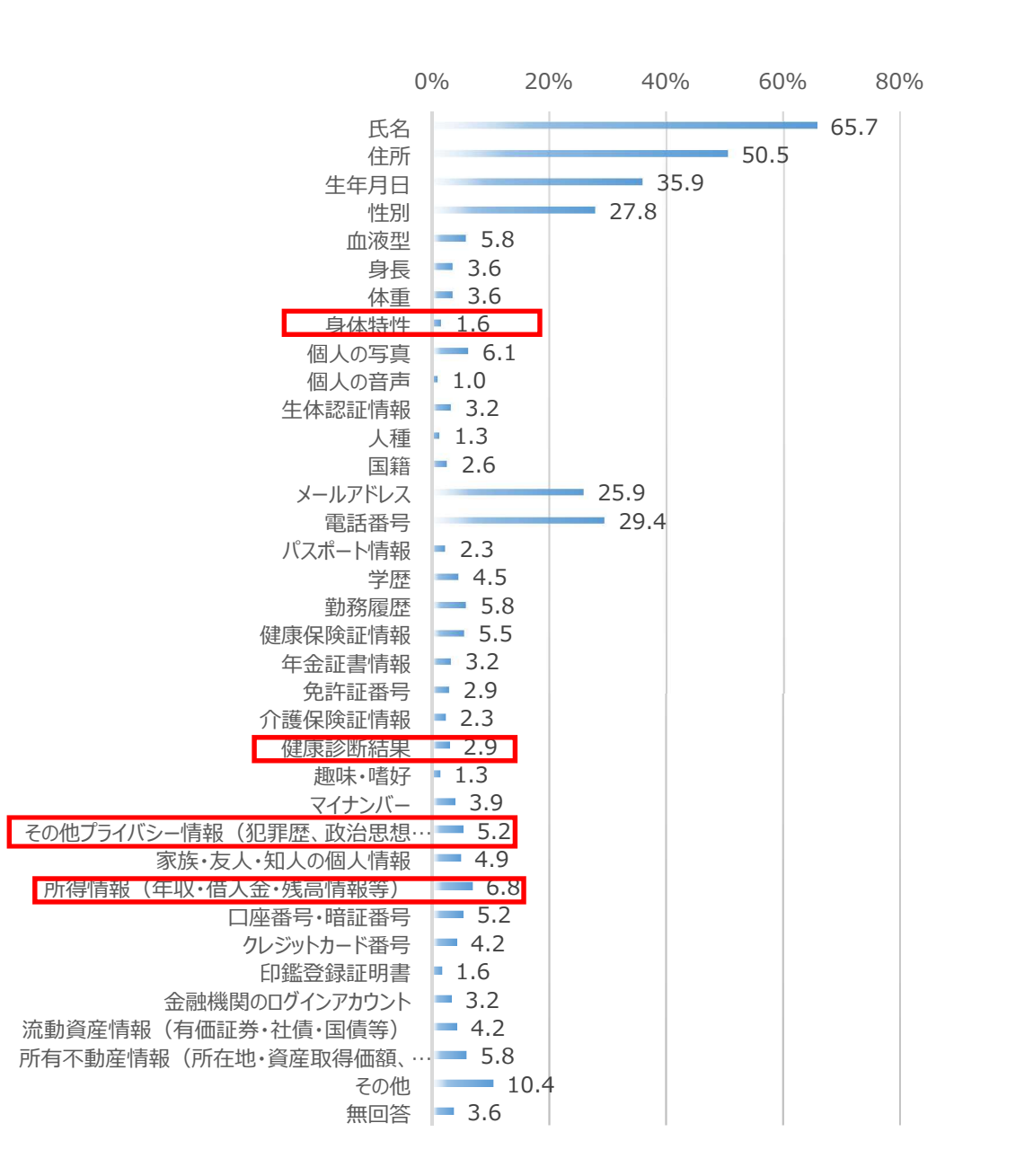
例えば、平成 27 年の日本年金機構の事故は、標的型攻撃メールが攻撃の侵入口です。標的型攻撃メールは、繰り返し似たようなレベルの内容が届くスパムメールとは異なり、一様にフィルタリングできるものではありません。日本年金機構の情報管理体制や運用上の問題点については、各方面から指摘されている通りですが、業務でパソコンを利用し、メールやインターネットに接続できる環境があれば、ウィルス対策や、システムに対する脆弱性対策を施していたとしても、どの企業も同様の攻撃を受け、踏み台にされしまう可能性・危険性があるということを十分認識する必要があります。

さらに、攻撃側の巧妙さが増すことによって、受信者がだまされる可能性も高まります。そもそも利用者に攻撃メールが届かないよう、システム的な不審メールのフィルタリングによる対策を行うことは、当然ながら不可欠です。標的型攻撃メールに添付されているファ

イル、あるいはリンクからダウンロードされるファイルが行う通信や挙動をシミュレーションすることで不正なメールであることを検知（プロファイル）できる何らかの対策が必要だと言えます。

1-7）漏えいした情報の種類

図表 11：情報漏えいや流出事件・事故の対象となった情報の種類についてあてはまるものを選択してください。（複数回答）



※【その他】の内容（自由記述より一部抜粋）

- 新製品に関する情報
- 新製品秘匿情報の持ち出し
- 取引先

- 顧客の取引情報
- 顧客先情報
- 営業秘密
- 成績
- 入院情報
- 社内の売上げなど
- 言えない
- 本人性格など、考えられるすべての情報
- 極めて高レベルな機密情報、ここでは具体的に記載不可
- 業務情報
- 開発機材

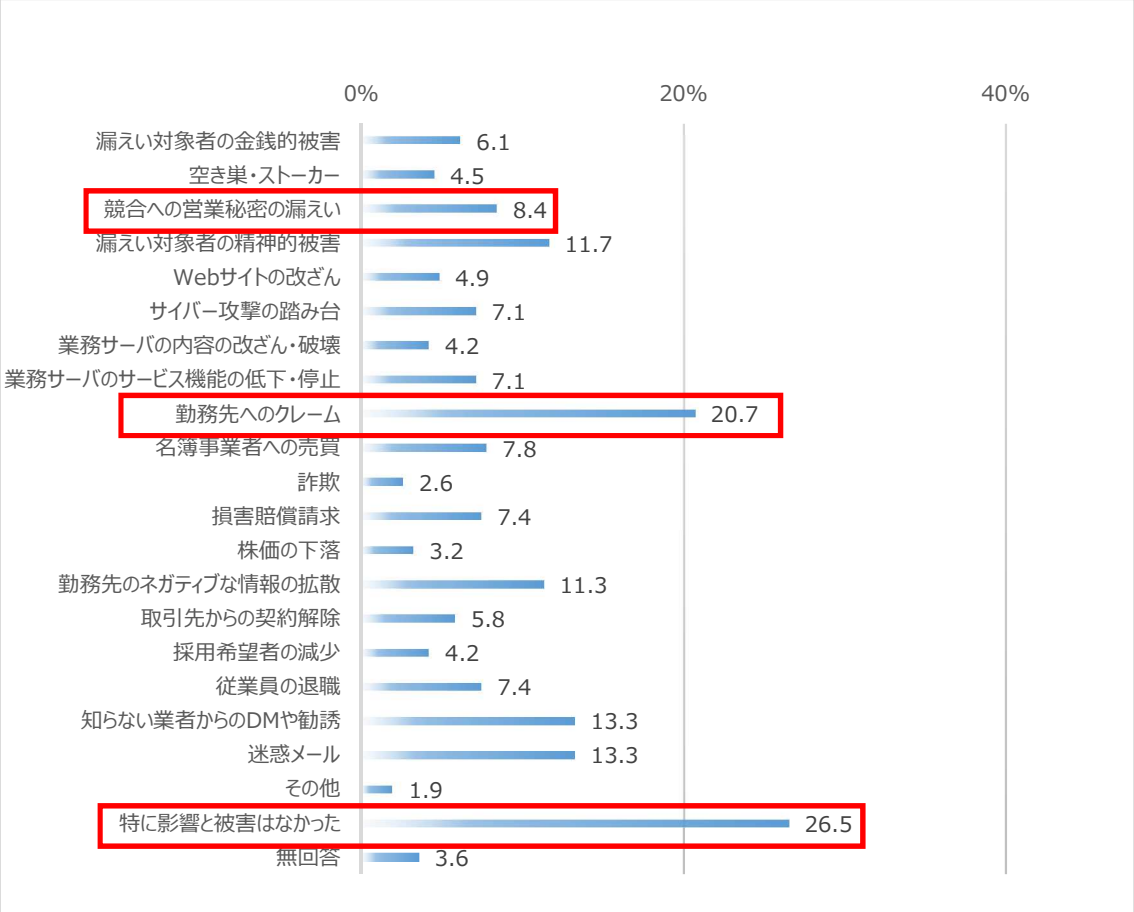
図表 11 は、発生した事故によって漏えいした情報の種類です。「氏名」65.7%、「住所」50.5%、「電話番号」29.4%、「生年月日」35.9%、「性別」27.8%、「メールアドレス」25.9%などといったいわゆる個人に関する基本情報の漏えいが割合的に多く確認されました。なお、あらためての確認となりますが、「個人情報」は氏名や生年月日など文字や数字で表現される情報に限らず映像、音声も含まれます。その他、身体、財産、職種、肩書きなどの属性に関する情報も含まれます。また、「個人情報」が暗号化されている、されていない（第三者が簡単に閲覧できない状態であるかどうか）は問われません。また「死者の情報」であったとしても生存する遺族（個人）を識別できる情報であった場合は「個人情報」になります。「個人情報」の「個人」とは日本人だけに限らず外国人も含まれます。法人、その他団体については「個人情報」ではありませんが、従業員、役員に関する情報は「個人情報」になります。

また、割合としては低いものの、「身体特性」1.6%、「健康診断結果」2.9%、「その他プライバシー情報（犯罪歴、政治思想等）」5.2%、「所得情報（年収、借入金、残高情報等）」6.8%が漏えい対象として確認されています。これらは、いわゆる「センシティブ情報」あるいは「機微情報」と言われ、具体的には身体・精神障害に関する情報、病気に関する情報や肉体的情報、また内面に関する情報、政治活動に関する情報など、一般には通常他人に知られたくない情報がこれに当たり、社会的差別などの原因となり得ることから、慎重な取扱いが求められています。こうした機微情報は、人の固定的な生体情報につながるもので、自己の努力では改善できないものであったり、他人の好き嫌いに強く影響する可能性があるなど、第三者に知られた場合の影響が大きいものでもあります。しかし同時に、こうした情報を取得しなければ成立しないサービスも存在します。医療活動や美容痩身といったサービスにあっては詳細な身体的情報の収集が必要となるため、仮に機微な情報であっても収集すべき場合があります。また、弁護士も、離婚や養育、相続など民事事件などで個人の多様な情報を収集する必要が出てくることがあります。このほか、具体的には、身体精神的情報を取得する必要がある医療機関などのほか、犯罪歴などを収集する必要のある法律事務所、本籍地の確認まで行う結婚相談所、国籍などを確認する必要のある不動産業、証券取引業など、センシティブな情報を収集しなければならない場面もあります。

漏えいした情報の種類によって、プライバシー権侵害の有無の判断や、プライバシー権侵害に基づく損害賠償額などの判断においては、漏えいや第三者に提供されるなどした情報が機微情報であるか否かは、重要な要素の一つとなります。例えば、エステティックサロンのアンケート調査等の回答の情報がウェブサイト上で閲覧可能な状態に置かれて流出したケースでは、他の情報漏えい事件と比べ、高めの損害賠償額が認定されています。

1-8）事故の影響と被害

図表 12：情報漏えいや流出事件・事故の勤務先への影響や被害について選択してください。（複数回答）



図表 12 は、情報漏えい時に実際発生した被害です。実質的な被害としては、「漏えい対象者の金銭的被害」6.1%、「空き巣・ストーカー」4.5%、「漏えい対象者の精神的被害」11.7%などが確認されました。また、「競合への営業秘密の漏えい」が 8.4%となっています。また、個人情報だけに限らず、技術情報等の営業秘密が競合他社等へ流出する場合は、当然ながら中途退職者が多く関与しています。重要な営業秘密情報が持ち出されたことにも気づかず、いつの間にか競争力を損なうようなこともあります。経済産業省の「営業秘密管理の実態に関する調査研究」によると、企業の情報管理実態については、大企業の約 40%、企業全体のおよそ 15%が「自社の営業秘密の漏えいがあった若しくはそのおそれがあった」としており、漏えいがないと回答した企業の中でも、3 割は漏えいの事実等について適切な把握などを実施しておらず、実際の漏えいはさらに高いと推測しています。また、企業の秘密情報の管理も十分ではなく、実際に営業秘密の漏えい防止策について、企業全体の約 35%、中小企業の約 40%が「取り組んでいない」と回答しています。個人情報の流出以外にも、内部からの営業秘密や技術情報の流出の対応も検討する必要があり、管理コストなど、危機管理の面でもクリアしていかなければいけない問題は山積しています。

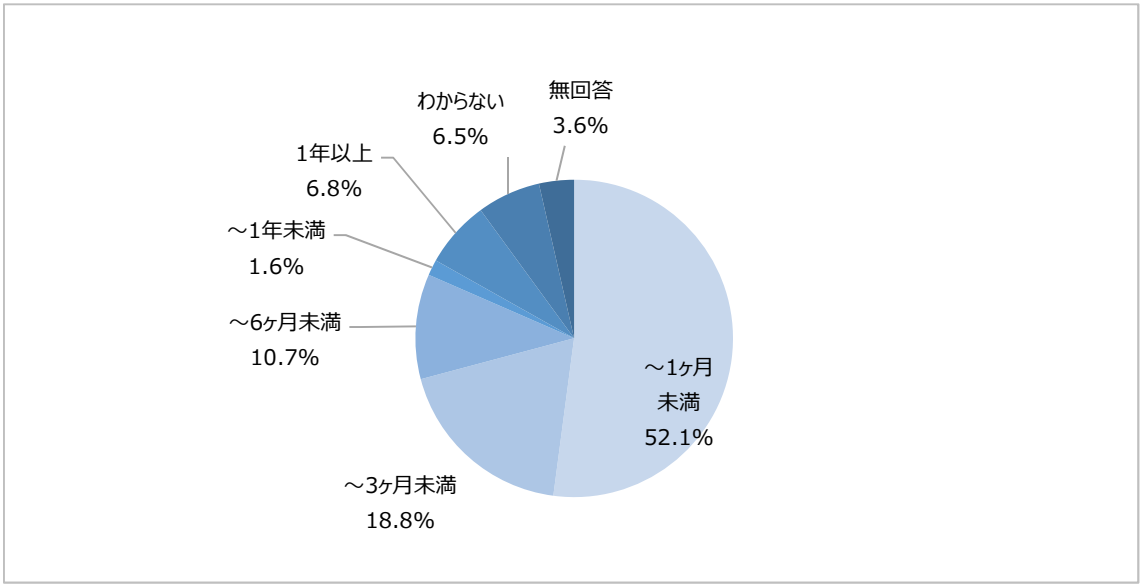
▼ 経済産業省「企業における営業秘密管理に関する実態調査結果概要」
http://www.meti.go.jp/press/2016/03/20170317004/20170317004-1.pdf

また、「勤務先へのクレーム」は、20.7%を占めており、被害の有無は別として、漏えいした情報が悪用される可能性や不安感、不適切な情報管理に対するお叱りやクレームを受けることになります。また、「特に影響と被害はなかった」が 26.5%を占めていますが、現時点で影響や被害が確認されていないだけで、本人のあずかりしらぬところで悪用されていたり、いつどこで利用されている可能性を否定することはできません。被害を受けていること、または加害者の立場となってしまっていることに自ら自発的には気が付かないこと（消費者や特定団体等の第三者からの通報で発覚するケースなど）も多くありますので、「被害がない」とは言い切れないということころに注意が必要です。

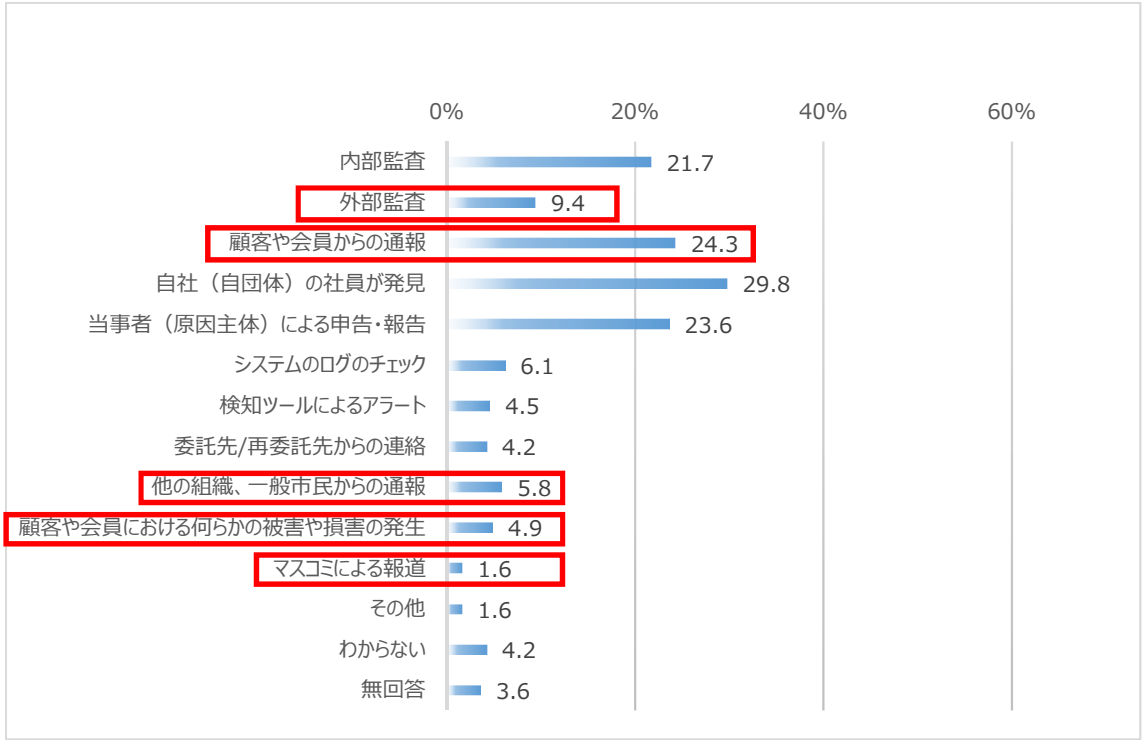
さらに、実際の被害としては、個人情報であれば迷惑なスパムメールや DM（ダイレクトメール）の送付、訪問販売に利用されることをはじめ、ストーカー行為を受けたり、本人を騙ってインターネットの各サイトで嫌がらせ行為が行われてしまうといった被害を受ける可能性があります。また家族構成も知られてしまうと「オレオレ詐欺」などの特殊詐欺にも利用されかねません。しかし、このような個人情報の不正入手に直接関わった人間が、そのまま個人情報を悪用するよりは、悪質な名簿業者や個人情報売買業者などへ情報を売るケースのほうが多く存在します。

1-9）事故発覚の契機と発覚までの期間

図表 13：情報漏えいや流出事件・事故が発生した時期と会社（団体）として発覚/認知（気づく）するまでの期間について選択してください。



図表 14:情報漏えいや流出事件・事故の発覚の契機について選択してください。(複数回答)

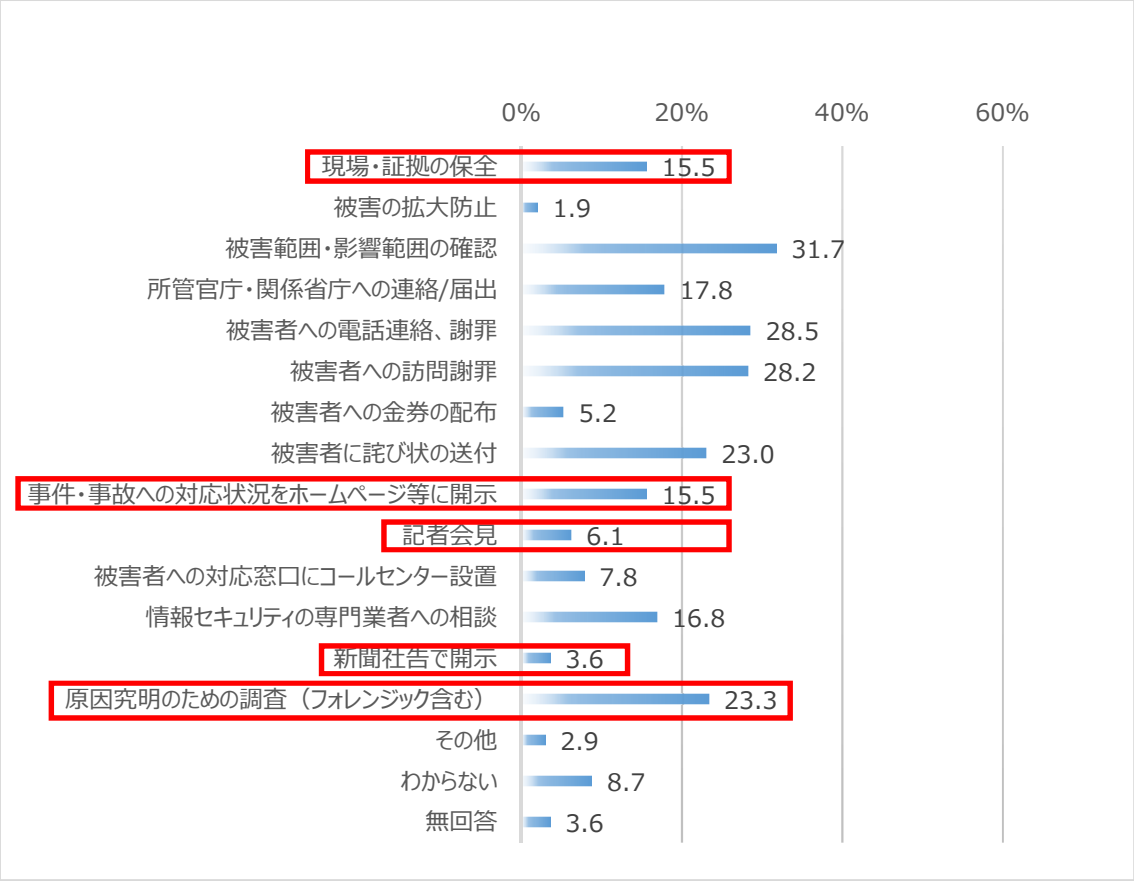


図表 13 は、事件・事故が発生してから企業・組織として認知するまでの期間を示しています。「1 ヶ月未満」での発覚が 52.1%、「3 ヵ月未満」は 18.8%、「6 か月未満」が 10.7%、「1 年未満」が 1.6%、「1 年以上」が 6.8%という結果となっています。事故が発生してから、発覚するまでの期間が短ければ短いほど、速やかな対応や被害等の拡散を防ぐ手立てを講じることができます。一方で、数年前に流出した情報が今になって被害が発覚し、対応に追われるケースも実際にあります。

図表 14 は、情報漏えい事故発覚の契機を示しています。「自社（自団体）の社員が発見」「顧客・会員からの通報」「当事者（原因主体）による申告・報告」「内部監査」がそれぞれ 20%以上を占めています。図表 14 の項目を大別すると、事故発覚の契機は「勤務先内から」と「勤務先外から」に分けることができます。大別した結果をみると、「勤務先内から」が全体の回答数の約 6 割を占めています。一方、「勤務先外から」は、その約半数です。ただ、被害者など外部からの通報で被害が発覚した場合は、隠蔽などが疑われ、組織の管理体制を大きく問われることになりますし、事故が発生しても長期間、表沙汰にならないことが多いため、漏えいした情報の規模や影響が大きくなる可能性が高まります。このような、被害が顕在化するまで侵入や情報の持ち出しの事実に"気づけていない"だけのケースも現実には多くありますので、現在の対策が本当に機能しているかどうかの確認と、情報管理上の不備や脆弱性を積極的にチェックして自ら問題に"気づける"取り組みが求められます。

1-10）事故対応の手段

図表 15：情報漏えいや流出事件・事故への対応としてとった手段について選択ください。



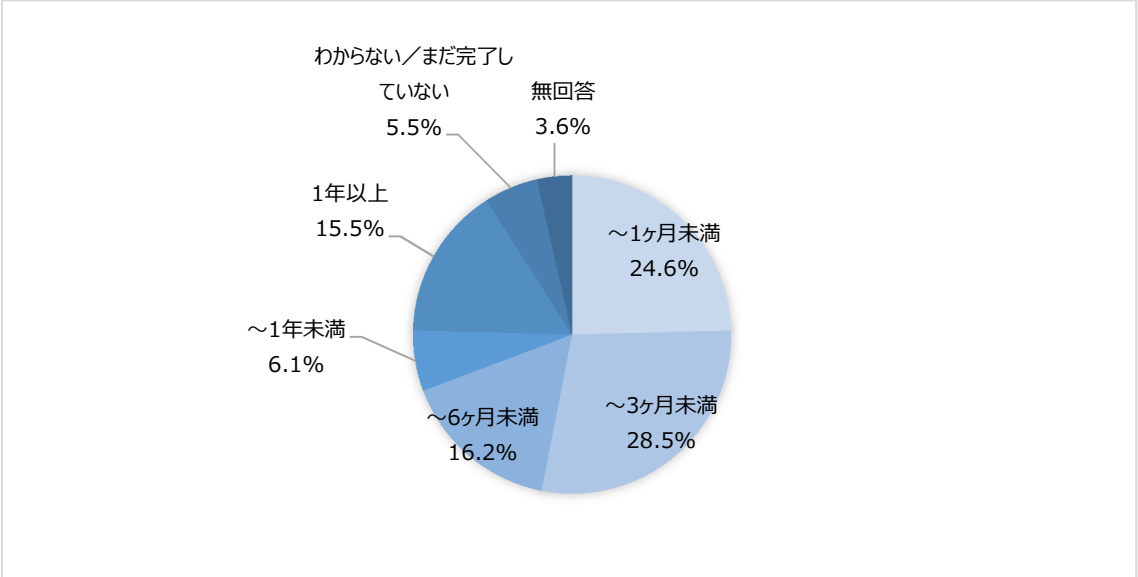
図表 15 は、事故時の対応手段について示しています。「被害者への訪問謝罪」、「被害者への電話連絡、謝罪」、「被害者への詫び状の送付」がそれぞれ 20%を超えており、被害者への周知の手段については、漏えいした件数や種類によって適切なものを検討されているものと考えられます。また、被害者に対して注意喚起や説明を実施するには、「被害範囲・影響範囲の確認」31.7%、「現場・証拠の保全」15.5%、「原因究明のための調査（フォレンジック含む）」23.3%などをいかに迅速に行なうかがポイントになります。多くの情報漏えい事案は情報通信機器やネットワークを介しておこなわれるため、電子メールやアクセスログの解析、会社が貸与した PC のフォレンジック調査などについては、専門業者に委託することで有益な証拠が得られる場合があります。特に IT システムに関しては、不用意な動作によって、証拠が滅失してしまうおそれもあることから、早期の段階からフォレンジック業者への依頼、あるいは連絡調整等をおこなうことが望まれます。

また、被害者や世間への周知や謝罪の手段として「記者会見」が 6.1%、「新聞社告で開示」3.6%を占めていますが、一般的には、情報漏えい事案での記者会見や社告の掲載は稀なケースだと考えられます。ただ、大企業による不祥事で、違法性が問われたり、人的被害や死亡者が出ていたり、負傷者が出ていたり、企業として生命・身体・財産に関わるなどの重大な危機を発生させてしまった場合には、強く説明責任を求められることになります。例えば、自社工場での事故（爆発など）、航空機や鉄道事故、工事現場での事故、食中毒や医療事故などの場面です。その都度、当該企業は何が起きたのか、なぜ起きてしまったのかなど、説明責任が問われることになります。企業活動において危機が発生した際、慎重に判断する必

要があるのが、公表（情報開示）の手段です。しかし、ステークホルダーや社会に対する影響を勘案し、説明責任を果たす必要性がある事案のときは、公表をしなければなりません。その際の説明責任とは、迷惑をかけたことに対する謝罪の意の表明であったり、例えば個人情報の漏えいがあった場合などは注意喚起のためであったり、起きている危機や想定される危機によって変わってきます。

1-11）収束までの期間

図表 16：情報漏えいや流出事件・事故で、発生してから対応が完了したと判断するまでに要した期間を選択してください。



図表 16 は、発生した情報漏えい事件・事故の対応が完了するまでの期間を表しています。「3 ヵ月未満」が 28.5%、「1 ヶ月未満」が 24.5%、「6 ヶ月未満」が 16.2%、「1 年未満」が 6.1%、「1 年以上」が 15.5%、「わからない/まだ完了していない」が 5.5%を占めています。

組織として、事故対応の一連の処理の中でもっとも重要なことは、常に状況を判断できるような情報伝達の手順やルールを確立しておくことです。過去に発生した情報漏えい事故などでは、組織幹部への情報伝達が遅れたり、正確な情報が伝わらなかったりしたために、もっとも大切な初動処理にミスが発生して、事故の被害をさらに拡大させ、対応が長期化してしまっているケースが数多く見受けられます。

なお、弊社は、「事故が発生したかもしれない」と企業から緊急対応依頼（要因の調査や応急処置）を受けることが多いのですが、実際に対応が一段落した時点で、関係者から振り返っての反省点でよく聞く内容が以下の事項です。

- マネジメントシステムを導入・運用していたにもかかわらず事故が発生してしまった。
- ここ数年、セキュリティポリシーや情報セキュリティ対策の見直しや対策強化などの改善をしていなかった。
- 防御策のために情報セキュリティ製品機器を導入していたが、初期設定のままで運用されていた。当時の導入担当者が退職したまま後任もいなかった。
- 公開用 Web システム導入当初は、情報セキュリティ診断等を都度実施・改善をしていた。その後のシステムやアプリケーションの仕様変更が頻繁に行われていたために診断・改善をしていなかった。

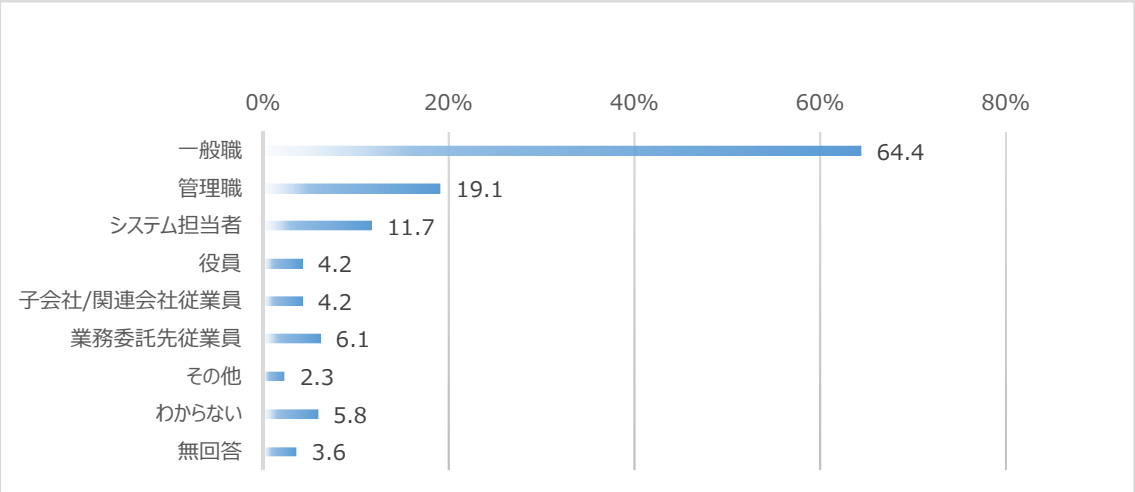
・　サーバのパッチ適用は、製品ベンダーや開発会社からの動作保障が得られないため適用を見送っていた。適用すべきか判断がつかないまま放置されてきた
・　廃棄したはずのサーバや削除したはずの機密データが残っていた。
・　必要なログが残されておらず、原因究明ができない結果となった。

このように、コスト面での問題やリソース不足などにより対策の遅れや先送りをした経緯が多々あり、ある程度危惧していたにもかかわらず、対応できずに事故が起こってしまった悩ましい現実があります。さらに、経営難もしくは急成長に伴う営業最優先の中、課題が山積みとなり、情報セキュリティ対策の優先度が下げられていたといったことも要因として挙げられます。

また、顧客からの問い合わせや指摘、提携先・委託先からの報告や検知システムのアラート等により、情報漏えいの可能性のある事故報告が突然上がってきたことにより、事故調査よりも復旧を優先し、事故発生要因の特定ができなくなったことから、その後の告知・報告等の対応が遅れ、被害者への対応が後回しになったケースもあります。初動対応については、経営と現場責任者の認識次第で事故後の経営リスク（損失）が大きく左右されるほど重要です。経営側の姿勢として、「事実をきちんと迅速に把握し、顧客に告知すること」、現場の役割として「実害の有無・影響範囲を迅速に把握し、経営に伝えること」が極めて重要となります。

1-12）事件・事故に関与した当事者

図表 17：情報漏えいや流出事件・事故を起こした（関与した）当事者について選択してください。



図表 17 では、事件・事故に関与した当事者が、「一般職」64.4%、「管理職」19.9%、「システム担当者」11.7%、「役員」4.2%、「子会社/関連会社従業員」4.2%、「業務委託先従業員」6.1%という結果が得られています。

広く周知されている通り、情報漏えいの主な原因は、一般従業員による誤送信・誤廃棄・紛失等・設定ミス等のヒューマンエラーが挙げられますが、多くの企業ではそれらを体系的に理解する機会が少ないため、効果的な予防、再発防止対策がなされていないのが現状です。まずは、経営者から従業員まで、誰もが当事者になる可能性があると自覚しなければなりません。また、セキュリティポリシーや、情報漏えいに関する従業員教育は、形骸化してしまいがちです。そうさせないためにも、特に普段から用いる頻度が高いもののルールを徹底的

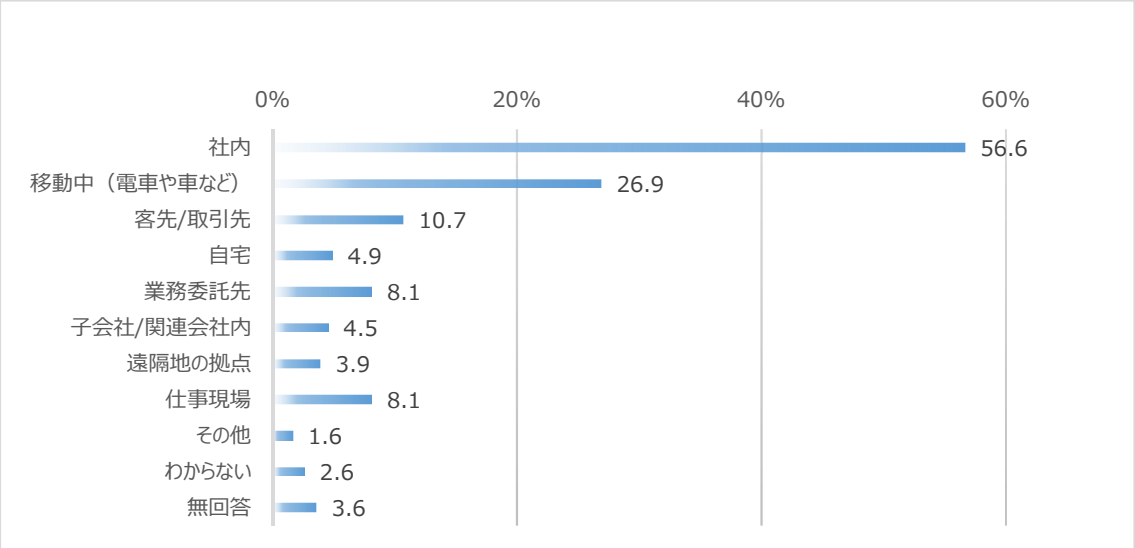
に順守させることから始めてみることも重要だと言えます。

また、サイバー攻撃の標的となるのも、その多くが役員や一般社員であり、十分な知識等をもっていない場合も少なくありません。したがって、標的型攻撃メールに対する訓練や演習、アンケートを通じて、自社内でそのリスク（開封状況など）を把握することも重要となります。演習や研修、注意喚起を繰り返すことで問題点を抽出し、それを改善するとともに、インシデントの処理になれておくことで、組織全体でのサイバー攻撃への対応力を向上させることが、被害の拡大を未然に防ぐ意味でも重要だと言えます。

その他にも、取引先企業などになりすましてメールを送り、偽の銀行口座に多額の現金を振り込ませる「ビジネスメール詐欺」という新たなサイバー犯罪の詳細な手口が多発しています。FBI によると、本手口で 13 年 10 月～16 年 6 月に世界で 2 万 2 千件以上、約 31 億ドルの被害があったと言います。正に、企業版「振り込め詐欺」であり、世界的に被害が拡大していることから、日本企業も看過できない脅威だと言えます。昨年 4 月には IPA（情報処理推進機構）が日本国内へのビジネスメール詐欺攻撃が多発しているとの注意喚起を行っていましたが、12 月になって、実際に航空会社が約 3 億 8000 万円のビジネスメール詐欺被害に遭っていたことが報道されました。ビジネスメール詐欺は、取引先を装った偽のメールを送付することで、偽の（攻撃者の）銀行口座に多額の金銭を送金させるというものです。攻撃者はターゲットがメールでやり取りする相手やその取引内容、文章のクセまでを事前に詳しく調べ挙げたうえで、詐欺を実行に移します。“企業版の振り込め詐欺”ではありますが、不特定多数をターゲットとする振り込め詐欺やスパムメールとは攻撃の精度が格段に違い、エンドユーザーが詐欺メールだと見破るのは非常に困難だとも言われています。また、マルウェアやフィッシング URL が添付されるわけではないため、多くのセキュリティ製品もすり抜けてしまう可能性もあります。このようなメールの送付先は CFO や経理部長などの役職者です。この脅威については、技術的な対策や人の注意だけで騙しを完全に防ぐことは非常に困難ではありますが、実際の攻撃を見てみると、注意すれば不審な点に“気づける”こともあります。典型的な手口を知ることや訓練などを行って攻撃に備え、多層的な防御策の一つとして、情報を取り扱う「人」の注意力を高めるとともに、送金前のチェック体制（内部統制システムの実効性）を強化するなど複数の防御策を怠らないことが肝要です。

1-13）事件・事故が起こった場所

図表 18：情報漏えいや流出事件・事故が起こった場所について選択してください。



図表 18 は、情報漏えいの事故・事件が起こった場所で、「社内」が 56.6%、「移動中（電車や車など）」が 26.9%、「客先取引先」が 10.7%、「業務委託先」が 8.1%、「仕事現場」が 8.1%、「子会社/関連会社内」が 4.5%を占めています。

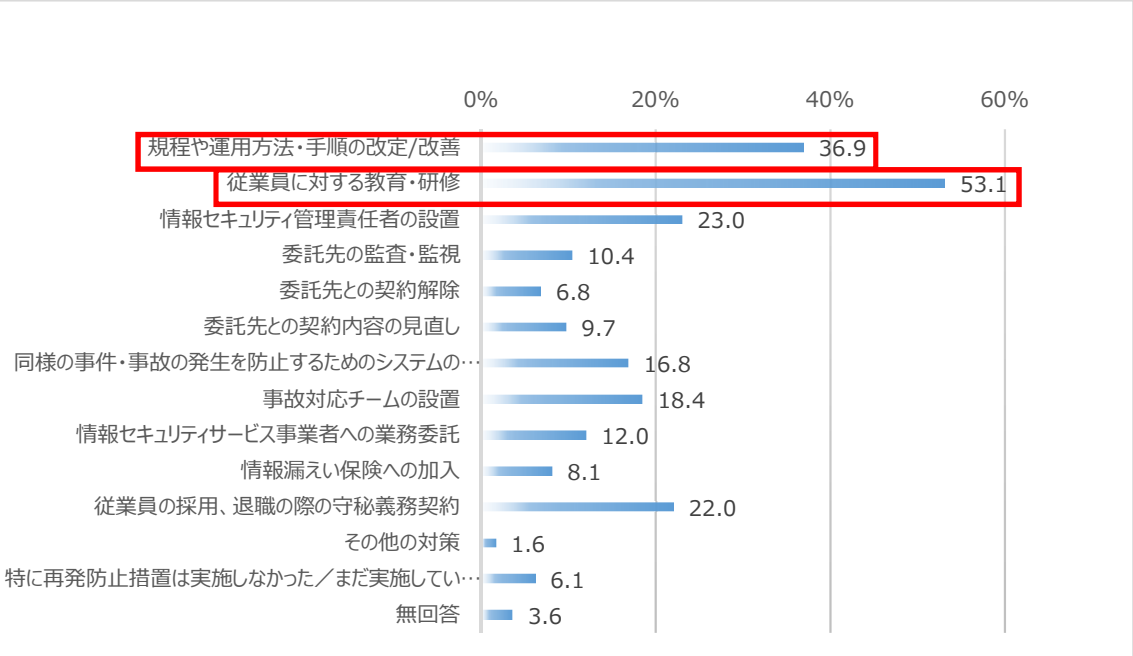
中でも、取引先や業務委託先で個人情報や機密情報を漏えいしてしまった場合は、事態の把握に時間を要する可能性があります。また、機密保持契約などを締結していたとしても、発注元としての監督責任を果たしていないことになり、その責任が発注元にも及びます。そのため、取引先、業務委託先などへの情報漏えい対策の要求は厳しくする必要があります。

例えば、実際にあった事例として、役所から委託を受けた企業が、個人情報の入ったハードディスクを役所のサーバ室から持ち帰り、それを紛失してしまったというケースや廃棄を依頼された業者が運搬途上で個人情報を散逸させてしまったケースなどがあります。このように、業務を委託した企業が情報漏えい事故を起こしてしまうことも少なくないことから、取引先企業への情報漏えい対策のチェックや監視に積極的に取り組む企業が増えています。

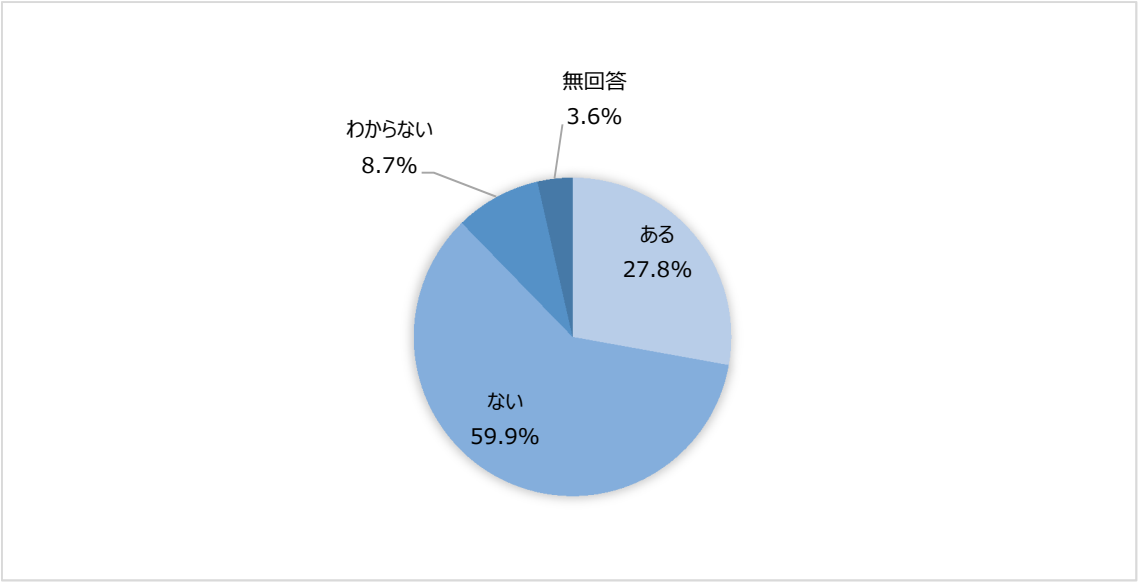
また、他社のソフトウェア開発を委託されている企業などでは、機密情報を入手、保持することも多いため、取引先企業から情報漏えい対策を実施するための社内の体制を確認されたり、「ファイル交換ソフトがインストールされた端末が社内ネットワーク上に存在していないかどうか、すべての端末を確認し、証明書を提出してください」といったように、情報漏えい対策に取り組んでいることを証明するよう求められることがあります。情報漏えい対策に関するチェックや、監視体制についての業務委託先からの回答結果によっては、取引の停止や、取引内容の見直しなどの厳しい措置を取る企業も増えています。また、契約の際に、IEC/ISO27001 やプライバシーマークなどの認証を取得している企業が、契約をスムーズに進められる傾向もあります。特に、情報漏えい対策に力を入れている企業との取引、信頼関係の構築には、情報漏えい対策への取り組みが重要になります。

1-14）再発の頻度と再発防止策

図表 19：情報漏えいや流出事件・事故の再発防止措置について選択してください。（複数回答）



図表 20：情報漏えいや流出事件・事故は、同様の事故が過去二回以上発生したことがありますか。



図表 19 は、情報漏えい事件・事故後の再発防止措置を示しています。「従業員に対する教育・研修」が 53.1%、「規程や運用方法・手順の改定/改善」が 36.9%を占めており、再発防止として、人の教育とルールの見直しに最も重きを置いていることがうかがえます。また、図表 20 は、過去 2 回以上事件・事故が発生したことが「ある」27.%、「ない」59.9%、「わからない」8.7%という結果となっています。

情報資産のセキュリティをパーツで考えた場合に、システムとして有効なものはたくさんあり、様々なソリューションを導入することも一つの方法ですが、それだけでは、リスクを防ぐことに限界があるのも事実です。システムを過剰に強固にした結果、通常の業務に支障をきたしてしまうこともあります。従業員への情報セキュリティに対する理解やモラル、情報倫理の欠如がボトルネックになっている場合、システムでの対策にコストをかけるよりも、「教育」に投資したほうが、効果的である場合も多いと言えます。教育が不十分な場合に起こるセキュリティリスクには、例えば、一般的なものとして、以下のものが挙げられます。

- 重要情報が入っている PC やモバイル端末、USB などを持ったまま飲み会に参加し、電車内に置き忘れたり、置き引きに遭ったりする。
- フリーソフトのインストールや、メールで送られてきた不審な URL のクリック、添付ファイルを開くことなどによってウィルス感染してしまう。
- 宛先間違いなどメールの誤送信や、推察されやすいパスワードの設定、付箋に書いてデスク周りに貼るといった安易なパスワード管理。
- ブログや SNS に社内の重要情報を書き込んだり、重要情報の書かれた書類などが写り込んだ写真を投稿したりする。

これらの行為は、本人に悪気がなく行われるケースが大半です。正しい知識がないために、無自覚のうちにリスクの高い行動をとったり、誤った情報管理の方法が社内に定着してしまったりしているわけです。まずは、なぜ情報セキュリティについての知識が大切なのか、何のための研修なのかを明確にして、それを周知することが必要です。情報セキュリティの

話は、ややもすると「面倒臭い」「業務に支障が出る」といったイメージを持たれがちです。そのため、「なぜ」の部分をまず理解してもらうよう心がける必要があります。実施形式は企業の規模によっても違ってくると思いますが、新入社員や中堅社員、管理職など対象者を階層別に分け、それぞれの対象者の知識や業務内容に合わせた内容で実施するのが効果的だと考えられます。また、複数の日程を用意して、全員が必ず受けられるようにすることも大切です。そうすることが、実際の研修内容の浸透だけでなく、「従業員全員が情報セキュリティについて考えなくてはならない」という会社からの強いメッセージにもつながります。

具体的には、新入社員や若手社員など情報セキュリティに関する知識をまだあまり持っていない対象者には、サイバー攻撃の種類などの基礎知識、個人情報や機密情報の扱い方、不審なメールの見分け方や取り扱い方法といった基本的な知識について教育することが必要です。そのうえで、業務のなかで遭遇する可能性のあるリスクへの対処方法や、注意するべきこと、やってはいけないことなどを一つずつ例示しながら教える必要があるでしょう。

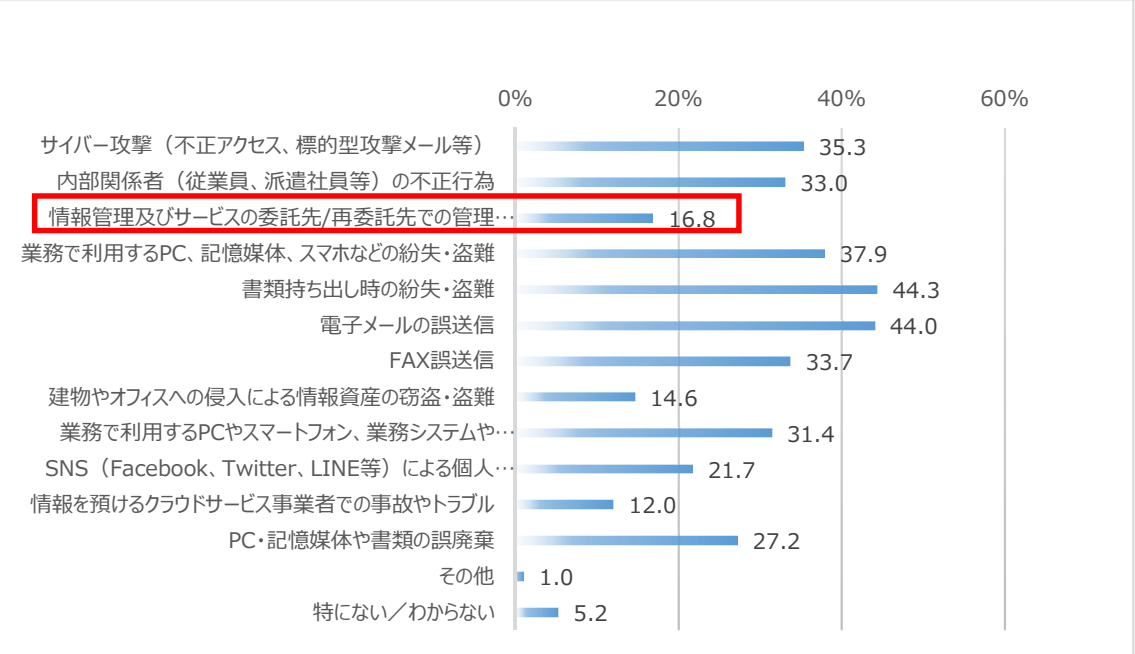
また、過去に研修を受けていて、情報セキュリティについてある程度知識があると思われる従業員も、「わかったつもり」になっていて、かえってヒューマンエラーのリスクが高いことがあります。知識やルールを再確認するだけでなく、新たな脅威など最新の情報を学ぶためにも、定期的に教育を実施することが望ましいと言えます。ここでも、具体的に実施するべきこと、してはいけないことを明確にして、それらが守られなかった場合にどのような問題が発生するのかを繰り返し伝えることが重要です。

従業員一人ひとりに情報セキュリティ意識を高めてもらうためには、情報セキュリティトラブルがちょっとしたミスで起こりうること、発生した場合に社内外に大きな影響をおよぼすトラブルに発展する可能性があることをきちんと理解してもらい、情報セキュリティに関する問題を全員が「自分ごと」としてとらえて業務に取り組めるような環境を築くことが重要です。

また、社内の風通しが悪く、質問や相談、トラブルの報告などがしづらい雰囲気があると、自己判断でリスクの大きい行動をとってしまったり、トラブルを起こした従業員がそれを隠そうとしたりすることにつながり、さらに大きなトラブルを生む可能性もあります。そのため、「迷ったときは上司や情報システム部などにすぐに聞く」「万が一トラブルを起こしてしまった場合には迅速に報告する」など、情報共有しやすい雰囲気を作っておくことも大切です。

1-15）今後懸念される事故

図表 21：あなたの勤務先で、今後想定・懸念される情報漏えいや流出事件・事故について選択してください。複数回答



今後想定・懸念される情報漏えいや流出事件・事故について選択して理由や把握している事情。（自由記述から一部抜粋）

- 個人の危機意識が不十分
- メール連絡が著しく多いため
- ダブルチェック不備
- 社員の意識の低さ
- 人間なので間違うことがあり得るから
- 現在も誤公布や誤送付による情報漏えいが絶えない
- 対応人員の確保
- 予算がない
- 内部犯罪はなかなか防げない
- 絶対ないとは言いきれない
- 週に一度はどこかの部署でメールや FAX の誤送信があるため
- 転職が多く顧客情報を持っていったことが発覚することが多々あるため
- 毎日漏えいリスクについては事例の共有があるがそれでも思いもよらない事件が次々と起こるため
- 従業員の意識啓発と体制維持が難しいと感じているため
- 私物 PC の持ち込みがある
- 人間は間違える
- 職員の情報守秘義務の重要性意識の欠如

図表 21 は、調査対象者の勤務先で今後起こりうる、情報漏えい事故や事件について示し

たものです。今後想定・懸念される事故は、勤務先で過去発生した事故とほぼ同じ順位と構成である傾向が確認されました。これは、すでに社内で発生していることで当該事故形態に関する認知が進んでいることに加え、効果的な対処が検討されていなかったり、問題や脆弱性が軽視・放置されていたりと、再発するリスクが未だに高いことの表れと読み取れることができます。事業者は、管理する情報資産ごとに脅威を認識して、引き続き警戒レベルを緩めることなく、システム面・運用面の双方で多層的な防御策の導入や、従業員への徹底した周知など継続した取り組みが求められます。

図表 21 の「情報管理及びサービスの委託先/再委託際での管理不備」は 16.8%と他の項目と比べて割合的には低くなっていますが、弊社での事案対応経験からすると、今後特に留意が必要な点だと言えます。

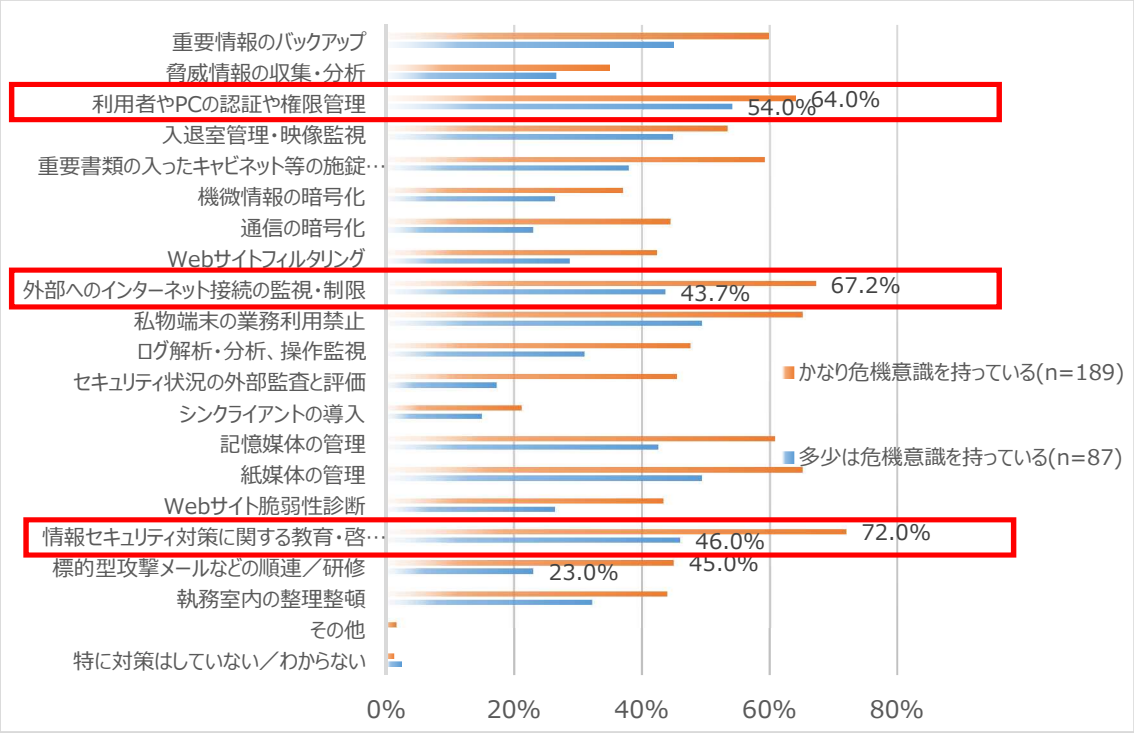
貴社では、業務委託先や再委託先企業の情報セキュリティレベルをどれくらい把握しているでしょうか。委託元は、委託先が再委託する相手方、再委託する業務内容及び再委託先の個人データの取扱方法等について、委託先から事前報告又は承認を求めることや委託先を通じて定期的に監査を実施する等、委託先が再委託先に対し監督を適切に果たすこと、安全管理措置を講ずることを十分に確認することが望ましいと言えます。また、委託関係においては、今後、BPO（Business Process Outsourcing）における個人事業主やフリーランスの活用や、BCP（Business Continuity Plan）における有事の際の在宅勤務等、様々な場面で情報セキュリティに対するモラルや問題も厳しく問われていくことになります。

また、海外拠点における委託先（業務委託先及び物品調達先）における情報セキュリティ対策も同様で、自国内の自社拠点に比べると十分ではないといえるのではないでしょうか。海外拠点については、法制度や商慣習、文化の違いによる特性があり、共通の基準・ルールを単純に適用できない点が問題となります。特に EU では、新たなプライバシー保護規制として、一般データ保護規則（GDPR：General Data Protection Regulation）が 2018 年 5 月から適用されます。違反すると、最大で全世界の年間売上高の 4%または 2000 万ユーロのいずれか高い方という非常に高額な制裁金が課されるとされており、現地の従業員や顧客等の個人データを取り扱う企業においてはその遵守が求められます。このような中、海外企業の M&A が増加すると、異文化の企業群を横断的にグリップする、（グローバルレベルでの）情報セキュリティガバナンスの確立が極めて重要になります。リスクに対する認識の共有、統一基準と現地の裁量のバランス、情報セキュリティ対策や事故報告の徹底、見える化など、手間をかけ成熟度を高める取り組みが必要となります。また、委託先については、発注元として対応の遵守を求めるだけでなく、委託元がイニシアチブを取る形で委託先の教育・啓蒙活動に取り組み、底上げを図る必要があります。

２．危機意識と対策の準備状況

2-1）危機意識と実施している対策

図表 22：情報漏えいを優先すべきリスクとして危機意識を持っている企業のセキュリティ対策



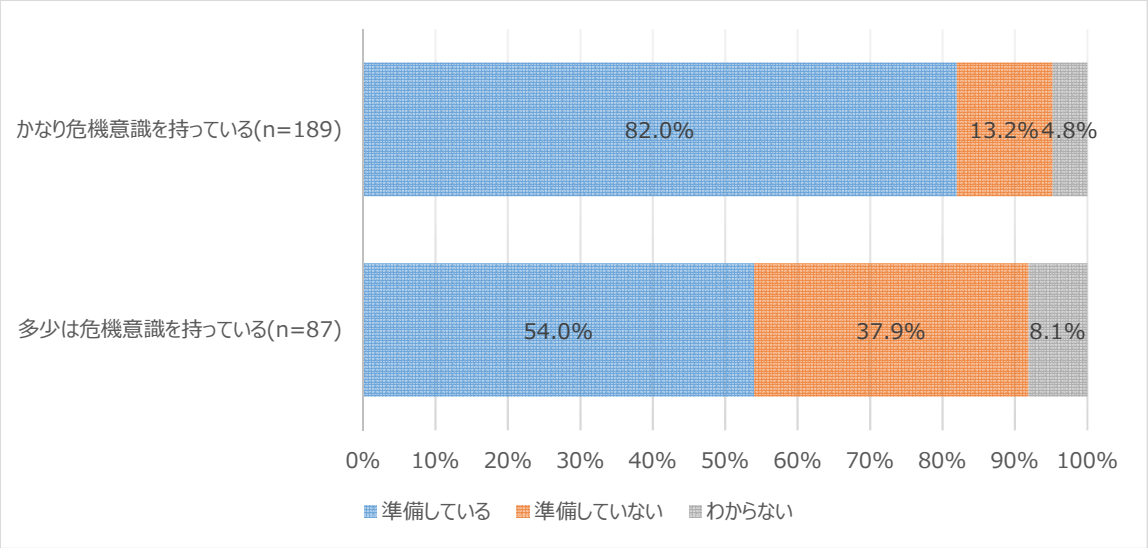
図表 22 は、「情報漏えいを優先すべきリスクとして危機意識を持っている企業のセキュリティ対策」です。対策としては特に、「利用者の PC の認証や権限管理」、「外部へのインターネット接続の監視・制限」、「情報セキュリティ対策に関する教育・啓発・注意喚起」が高い割合を示しています。

情報セキュリティ対策は、技術的なイメージが先行する傾向があり、「技術的なもの」とか「難しいもの」と敬遠されがちです。無論、技術的な要素の必要性は否定しませんが、技術的な側面だけで捉えてしまうと、組織全体で対処する性格を有する情報セキュリティにおいて、組織管理の課題がカバーされなくなる懸念が生じます。

特にサイバーセキュリティを取り巻く環境変化のスピードが年々早くなってきている状況下にあっては、攻撃側の変化にあわせて、防御側も迅速な組織的変化が求められるようになります。こうした状況においてサイバー攻撃によってもたらされる被害の予防、被害が発生した場合の対処のいずれにおいても、組織的管理の観点からの取組み、とりわけリスク管理、危機管理、経営者の意思決定などは非常に重要な要素となります。このことは、組織が大きいほど重要となります。しかしながら、日本においては、厳しい予算のなかで IT 担当部署が技術的問題を中心に対応しているケースが散見される一方で、世界各国におけるサイバーセキュリティの取組みにおいては、非技術的観点の重要性が高まっており、「サイバーセキュリティ=技術の問題」からの脱却が進んでいます。また、組織によって「脅威」そのものが異なり、自組織のサイバー脅威を正しく理解し、正しくおそれ、正しく対応することが何よりも重要だと言えます。

2-2）危機意識と緊急対応の準備

図表 23：情報漏えいを優先すべきリスクとして危機意識を持っている企業の事故への準備状況



図表 23 は、「情報漏えいを優先すべきリスクとして危機意識を持っている企業の事故への準備状況」です。「かなり危機意識を持っている」場合は、82%、「多少危機意識を持っている」場合は、54%が事故に備えた準備しているという結果が得られました。

情報セキュリティの分野におけるインシデントとは、コンピューターやネットワークのセキュリティを脅かす事象、すなわち、ウィルス感染や不正アクセス、不正侵入、データの改ざん、情報漏えいなどを指し、意図的であるか偶発的であるかを問いません。また、インシデントレスポンスとは、上記インシデントに対し、主に原因の調査や対応策の検討、サービス復旧や再発防止策の実施などの対応を適切に行うことです。最近は、サイバー攻撃が増加傾向にあり、その範囲も広範にわたっています。こうした状況下で、情報セキュリティ対策を万全に施していたとしても、すべてのインシデントを未然に防ぐことは不可能です。

そこで、インシデントが発生した場合に迅速に対応し、被害の拡大を最小限にするための「適切な事後対応」が求められます。特に、標的型攻撃メールなどのように、特定のターゲットに対し、周到に、時間をかけて準備され、継続的に実行されるサイバー攻撃などに対応していくためには、常にメンバーや組織内で知識を共有し、事故の発生を前提としたポリシー策定や手順を確立しておくことが重要です。

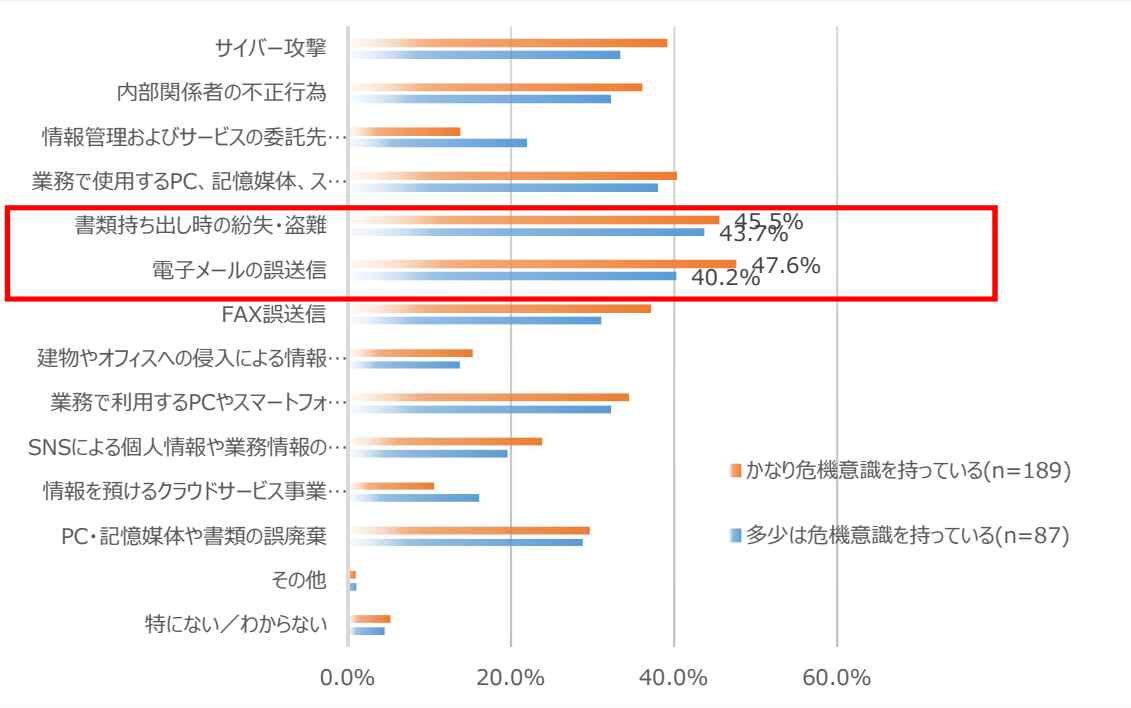
昨今の情勢を見てのとおり、ほとんどの産業が IT と密接に結びついているため、新しい技術やサービスが広まれば、同時にサイバー攻撃を受けるリスクも高まるというジレンマにどの企業や個人も陥っています。特にサイバー攻撃者は、情報セキュリティインフラの構造上、企業や組織よりも優位な立場にあります。攻撃者は防御側にあるセキュリティホールを一つ見つければ、そこから様々な攻撃の手口を仕掛けられるのに対して、防御側は、全てのセキュリティホールを把握し対策を取ることが必要となりますが、これは事実上不可能だと言わざるを得ません。

また、サイバー攻撃などの被害を受けやすい企業の特徴として、IT 環境の未整備、セキュリティアップデートの適用管理が不十分、ウィルス対策ソフトの利用が限定的、PC 機器等の持ち出しや持ち込みの管理が未実施、事故対応体制が未整備など IT ガバナンスが十分で

はない組織であると考えられます。
事業者は、取るべき対策を整理するとともに今回の攻撃を踏み台にした次なる攻撃を想定し、警戒レベルを上げて、システム面・オペレーション面双方での多層的な防御策の導入、従業員の意識高揚などに、早急に取り組むことが求められます。

2-3）危機意識と今後想定される事故

図表 24: 情報漏えいを優先すべきリスクとして危機意識を持っている企業が想定している事故



図表 24 は、「情報漏えいを優先すべきリスクとして危機意識を持っている企業が想定している事故」です。今後想定される事故として「書類持ち出し時の紛失・盗難」、「電子メールの誤送信」の割合が高いことが示されています。情報漏えいに対する危機意識が高い企業は、利用頻度としては高くリスクとしては見落とされがちな事案について、何かしらの対策をとるべきだという認識を持っていることがうかがえます。
特にメールの誤送信は、事故の要因として、システムの不具合によるものもあれば、To と Cc、Bcc の誤認識、打ち間違え等によるうっかりミスや不注意等の多様な形態があります。その他よくありがちなパターンとしては、メールの転送と返信を間違えてしまったり、オートコンプリート（候補表示）で宛先を間違えてしまうこともあります。また、電子メール送信時は、誤送信しても送信者自身がその事態に気づかないことが多いことも大きな特徴です。メールアドレス一つだけでも、個人情報に該当するケースが多く、誤送信事故が発生すれば企業として管理体制や対応の質が問われることになります。さらに、メールアドレスだけではなく、社外秘の内容や機密情報といった営業秘密や機微な情報が添付もしくは記載されていれば、それだけで企業にとって極めて重大な事故に発展しかねません。
電子メールは今や業務に欠かせない重要な情報通信手段でありますが、未だに事故が多く発生しています。電子メールの誤送信対策としては、システム的な施策（送信前の承認や

自動暗号化等）以外にも、人的な脆弱性を克服していくためにも、各自が電子メールを送信する際に宛先、送信内容、同報送信の種類、添付ファイルを十分確認するプロセスについて、あらためて（何度でも）注意喚起し続ける必要があります。

Ⅴ．事故への備え

本調査では、情報漏えいや流出事件・事故対応で対応に苦慮した点を質問しました。その結果、以下のような回答がありました。（自由記述より一部抜粋）

- 謝るとき
- 解決に時間がかかった
- 状況の把握とそれに対するサポート
- 退職者が新製品の秘匿情報を持ち出し、退職後に発覚。社員としての罰則が適用できず警察沙汰になった
- 原因の究明と関係者への謝罪および、今後の防止策
- 一連の対応方法
- 紛失した情報機器が見つからなかった。情報がどこに漏れているかわからなかった
- 被害の全貌
- 漏えいした情報の内容の特定
- 公表をどこまでするか、誰まで報告するかの判断
- 紛失時期の特定が遅れ、全ての対応に影響を及ぼした
- 対処するための時間と労力
- 繰り返し誤送信が起きる
- 対応マニュアルが出来ていなかった
- 事態の収拾
- 紛失したケース記録の対象者のご家族に対しての謝罪・再発防止策の全組織的な取り組み
- 顧客からのクレーム対応
- 賠償の支払
- 犯人特定まで時間を要したこと
- 時間外勤務
- 顧客へのお詫び。報道発表
- 情報が流出したかどうか、および流出の影響がない（流出していない、または消去された）ことを確認することが難しい
- どうしていいかわからず、混乱した
- 現実的な拡散防止策、再発予防
- マスコミへの公表時期
- 誤った複数の相手に対して顧客情報を添付して送信してしまった。全ての送り先に情報の削除依頼をしたが、すべて実行されたのかの確認が難しい。添付ファイルの顧客にも情報漏えいの事実を伝え謝罪対応し、膨大な時間と労力が掛かった。どれだけの金銭がかかったかは不明。
- 事象発生後の初動対応が想定よりも開始するまでに時間がかかった
- 酒に酔ったうえで、個人情報記載書類の紛失で、当該書類の発見のため町中を探したこと
- 顧客対応は了承を得ることで比較的容易に解決したものの、会社自体が厳格な規定を

定めており始末書等作成に多大な時間を費やした。また、組織の成績に影響を及ぼした
- 海外拠点対応が大変
- 原因の追究。様々な流出経路があるので特定が難しい
- データの復旧が業者ではなく、一職員に任せられたこと
- 頻繁に起こらないことなので、初動に手間取った
- どこに相談すべきか
- ログの解析
- ゴミの中から書類を探した
- 相手側が訴える旨を申し出たこと
- ルールはあるが、従業員がしっかり守っているか完全には把握できない
- 本人が雲隠れしてしまって捜査機関との情報が共有できなかったが、3 ヵ月後捜査機関によって検挙逮捕されて、全貌が明らかになった
- 客先常駐のスタッフが外を移動中に突風により個人情報資料を紛失したため、回収が困難だった
- お客様がご立腹でなかなか話しができなかった
- 問題意識の希薄さと、おわび行脚の時間的ロス
- 管理がいっそう厳しくなった
- 通常業務として平行してことにあたる大変さ
- 極めて高度な標的型攻撃を受け、漏えい発覚後から、先ずは漏えいした情報の分析、どのように漏えいしたのか、原因と経緯を調査するのに途方もない時間と費用が必要であった
- 判明するまでに、時間を要した。名簿の売り先から取り戻すプロセスが煩雑だった
- 社員がカバンごとひったくりされた
- 被害対象者に対する損害賠償の確定にかかる交渉
- 詳しい人がいない
- 機材紛失した当事者が叱責を恐れてか、盗難と嘘をついたため、警察への届出など余計な作業が発生した
- 休日明けの報告になったので、初動に遅れが生じた
- 社内教育の徹底と再発防止策
- 委託先の管理
- お客様に謝罪をしようにも、個人情報を紛失しているため連絡がとれなかった
- 解決に金額の目処がたてにくいこと
- 問題解決にかかりきりになり他の仕事がおろそかになった

上記のように「流出原因およびその経路の特定の調査」「勤務先へのクレーム」「損害賠償請求」などの直接的な被害のほか、間接的な損害として「対応のための時間外労働」「顧客や取引先が納得してくれない」「事故対応の収束が見えない」など対応担当者の先が見えない不安や対応疲れなど多大な苦労が滲む記述も確認されました。

実際に事故が発生した場合、様々なことを組織として判断することになりますが、そのための根拠となる情報は、十分に入手できないことも珍しくありません。事故調査において重要なネットワーク構成図、情報資産の扱われ方や被害者の感情など、理想や本来望ましい姿とこれまでの実態は異なっていることがほとんどです。「守られていたはずのものが守られていなかった」、「ルールが守られていなかった」、「報告が遅かった」、「ログが残っていなかった」、「顧客が納得してくれない」などの状況が判明し、はじめて現実を直視せざるを得

ないことが多いといえます。事故の規模が大きくなればなるほど、対応方針や役割の分担、得られた情報の集約方法の決定、対応担当者間の定期連絡のインターバルの決定などとともに、先を読み隅々まで目を配った司令塔の役割が必要となります。情報漏えいによる事故や被害事例を見て、「他社のこと」「うちでは起きない」などいった反応は、有事を見据えた場合、相応しくありません。本来であれば、他社の問題はいつか自社に起きる問題としてとらえて、「同じことが起きた場合に、自社はどうなってしまうだろうか」という観点で考え、不足点を補うために何が必要かを平時において考えるべきところです。そうすることで、現状の体制的な問題点や、技術的な問題点などがみえてきます。また、世の中で発生した新しい攻撃や脅威に対して、自社組織の新たな問題が明らかになった場合であっても即時に対応できるわけではありません。対応までにどのくらいの期間を要するのか、その間のリスクはどのように管理・対応するのかなどを、経営層や管理層と組織的に共有しておくことが重要となります。

また、事故対応の現場は、概して発生している問題を過小評価し、「あまり大したことは起こっていない」ことにしようとすることがあります。さらに、自社で管理しているシステムやサービスで情報セキュリティ上の問題が起きてしまった場合、それを上層部に報告すると責任を追及されることが予想されるため、「隠蔽」しようとすることがあります。もちろん目の前に事実がありながらすべてを隠しきることはできませんが、「情報が流出したと100%いえる証拠がないため、情報漏えいはない。したがって、上層部に報告する必要はない」などといった具合に結論づけてしまうケースも実際にありました。さらに、経営層に報告しても「大した情報は漏れていません」で終わらせるケースもありました。実際、情報漏えいに繋がるサイバー攻撃が起きても、100%流出したと言い切れる証拠が残っているケースはほとんどありません。「流出したかもしれない」という状況で、悪い方に判断して（最悪を想定して）対処できるかどうかは、関係者の意識もさることながら、悪い情報に対する組織としての姿勢も大きく影響します。問題は、現場が隠そうとすることだけではなく、悪い問題を報告しやすい組織風土になりきれていないことであり、この観点は実効性のあるコンプライアンスを確保するためにも不可欠です。また、情報漏えい発生時にどうしても「個人情報」のみがフォーカスされ、それ以外の情報漏えいに対する意識が欠如してしまうことも問題です。個人情報保護法を背景に、個人情報に関わる情報の漏えいには敏感になる企業は増えつつありますが、（中小規模の企業等を中心に）自社の経営や技術に関する情報が漏えいしても、それは自社の情報にすぎず、仕方ないと考える風潮すらあるように思われます。もちろん個人情報はしっかり守らなければなりませんが、自社の情報をこのように軽視してもよいはずはありません。国内外のライバル企業に知られると競争上致命的な営業秘密、知的財産、設計図などさまざまな情報が社内には存在していますし、システム設計図などが漏えいしたことで、別のサイバー攻撃に利用されたと考えられる事案はすでに発生しています。こういった攻撃被害の詳細は広く情報公開されることが少なく、一般に十分に認知されていません。情報漏えいによる組織やビジネスの実害が何であるかを考え尽くすことは非常に難しいですが、少なくとも情報漏えいのリスクを過小評価せず、防いでいくことが、長期的には自組織のビジネスを守ることに繋がると言えます。

また、事故発生時の対応フローやマニュアル的なものは多く存在しますが、弊社の経験上、いずれも具体的な対応に必要なすべての観点を網羅的に事細かに説明したものとはなっていない傾向が見受けられます。その理由は、事故対応は、事案ごとに、影響の大きさ、対応の考え方や対策方法、具体的な調査作業、意思決定、メディア対応、記者会見など一つひとつの要素が異なってくることにより非常に複雑になるためです。また、ニュース記事などか

らある企業がサイバー攻撃によりクレジットカー情報を漏えいしたとか、個人情報を漏えいした、サイバー攻撃により顧客向けサービスが停止した、などといった概要情報は得ることはできます。しかし、事案の発生・検知・対応・収束・教訓といったすべての流れが事細かに表に出ることはほとんどありません。現在、国内でもサイバー攻撃の発生を想定した訓練を実施する企業や組織が増えてきましたが、多くの場合、「自社が対応可能な事案」を想定し、既存の仕組みが想定どおりに動くのかのチェックや、いわゆる標的型攻撃メールを模擬的に送信してそのうち何人が開封したかをチェックするといったレベルにとどまっています。中には、標的型攻撃メールを開封した従業員に人事的な処罰を与えている組織もあると聞きますが、そのようなことをすれば本物の標的型攻撃メールをうっかり開いてしまった場合、処罰をおそれて誰も報告しなくなるという本末転倒の結果になってしまうことが懸念されます。当事者にとって悪い情報も、組織上層部に早期にエスカレーションされる組織風土に如何に醸成していくかは、事故対応において非常に重要な組織的課題だと言えます。

Ⅵ. 巻末資料

１．アンケート調査項目

Q1. あなたの勤務先では、保有する情報（顧客情報、従業員情報、営業秘密等）の漏えいについて、優先すべきリスクとして危機意識を持っていますか。

□ かなり危機意識を持っている
□ 多少は危機意識を持っている
□ どちらともいえない
□ あまり危機意識を持っていない
□ 全く危機意識を持っていない

Q2. あなたの勤務先では、保有する情報（顧客情報、従業員情報、営業秘密等）を管理するための規程やマニュアルが整備されていますか。

□ 整備されている
□ 整備されていない
□ わからない

Q3. あなたの勤務先で実施している情報セキュリティ対策は何ですか。（いくつでも）

□ 重要情報のバックアップ
□ 脅威情報の収集・分析
□ 利用者やPCの認証や権限管理
□ 入退室管理・映像監視
□ 重要情報の入ったキャビネット等の施錠管理
□ 機微情報の暗号化
□ 通信の暗号化
□ Webサイトフィルタリング
□ 外部へのインターネット接続の監視・制限
□ 私物端末の業務利用禁止
□ ログ解析・分析、操作監視
□ セキュリティ状況の外部監査と評価
□ シンクライアントの導入
□ 記憶媒体の管理
□ 紙媒体の管理（廃棄方法、持ち出し制限等）
□ Webサイトの脆弱性診断
□ 情報セキュリティ対策に関する教育・啓発・注意喚起
□ 標的型攻撃メールなどの訓練/研修
□ 執務室内の整理整頓
□ その他
□ 特に対策はしていない／わからない

Q4. あなたの勤務先では、情報セキュリティ対策をどのような体制で行っていますか。
最もあてはまるものをお答えください。

□ 専門部署（担当者）がある
□ 兼務だが担当者が任命されている
□ 組織的には行っていない（各自/各部署の判断）
□ その他
□ わからない

Q5. あなたの勤務先で、情報セキュリティ対策を進めるうえで、特に課題と感じるものを選択してください。（いくつでも）

□ 経営層の危機意識が低い
□ 予算、リソースが不足している
□ リスクの見える化が困難/不十分
□ 社内における漏えい事故などの共有体制
□ 情報セキュリティの取り組みが企業価値の向上につながると認識されていない
□ 経営とセキュリティの両方を理解している人材がいない
□ 専門知識の不足
□ 委託先管理が困難
□ その他
□ 特に課題に感じるものはない

Q6. あなたの勤務先では、重要情報の流出や紛失盗難があった場合の対応手順などを作成し、事故が発生した場合に備えた準備をしていますか。

□ 準備している
□ 準備していない
□ わからない

Q7. あなたの勤務先で過去発生した情報漏えいや流出事件・事故について、被害や影響が最も重大だったものを一つ選択してください。※ご自身が対応（関与）した情報漏えいや流出事件・事故についてお答えください。

□ サイバー攻撃（不正アクセス、標的型攻撃メール等）
□ 内部関係者（従業員、派遣社員等）の不正行為
□ 情報管理及びサービスの委託先/再委託先での管理不備
□ 業務で利用するPC、記憶媒体、スマホなどの紛失・盗難
□ 書類持ち出し時の紛失・盗難
□ 電子メールの誤送信
□ FAX誤送信
□ 建物やオフィスへの侵入による情報資産の窃盗・盗難
□ 業務で利用するPCやスマートフォン、業務システムやサーバのマルウェア感染
□ SNS（Facebook、Twitter、LINE等）による個人情報や業務情報の拡散
□ 情報を預けるクラウドサービス事業者での事故やトラブル

□ PC・記憶媒体や書類の誤廃棄
□ その他
□ わからない

Q8. Q7 で選択した情報漏えいや流出事件・事故の対象となった情報の種類についてあてはまるものを選択してください。（いくつでも）

□ 氏名
□ 住所
□ 生年月日
□ 性別
□ 血液型
□ 身長
□ 体重
□ 身体特性
□ 個人の写真
□ 個人の音声
□ 生体認証情報
□ 人種
□ 国籍
□ メールアドレス
□ 電話番号
□ パスポート情報
□ 学歴
□ 勤務履歴
□ 健康保険証情報
□ 年金証書情報
□ 免許証番号
□ 介護保険証情報
□ 健康診断結果
□ 趣味・嗜好
□ マイナンバー
□ その他プライバシー情報（犯罪歴、政治思想等）
□ 家族・友人・知人の個人情報
□ 所得情報（年収・借入金・残高情報等）
□ 口座番号・暗証番号
□ クレジットカード番号
□ 印鑑登録証明書
□ 金融機関のログインアカウント
□ 流動資産情報（有価証券・社債・国債等）
□ 所有不動産情報（所在地・資産取得価額、借入情報等）
□ その他

Q9. Q7 で選択した情報漏えいや流出事件・事故の対象となった情報の件数を教えてください。
※不明な場合は、おおよその件数をお答えください。

□ （　　）件

Q10. Q7 で選択した情報漏えいや流出事件・事故で、発生してから対応が完了したと判断するまでに要した期間を選択してください。

□ ～1 ヶ月未満
□ ～3 ヶ月未満
□ ～6 ヶ月未満
□ ～1 年未満
□ 1 年以上
□ わからない／まだ完了していない

Q11. Q7 で選択した情報漏えいや流出事件・事故の勤務先への影響や被害について選択してください。（いくつでも）

□ 漏えい対象者の金銭的被害
□ 空き巣・ストーカー
□ 競合への営業秘密の漏えい
□ 漏えい対象者の精神的被害
□ Web サイトの改ざん
□ サイバー攻撃の踏み台
□ 業務サーバの内容の改ざん・破壊
□ 業務サーバのサービス機能の低下・停止
□ 勤務先へのクレーム
□ 名簿事業者への売買
□ 詐欺
□ 損害賠償請求
□ 株価の下落
□ 勤務先のネガティブな情報の拡散
□ 取引先からの契約解除
□ 採用希望者の減少
□ 従業員の退職
□ 知らない業者からの DM や勧誘
□ 迷惑メール
□ その他
□ 特に影響と被害はなかった

Q12. Q7 で選択した情報漏えいや流出事件・事故を起こした（関与した）当事者について選択してください。（いくつでも）

□ 一般職
□ 管理職
□ システム担当者
□ 役員
□ 子会社/関連会社従業員
□ 業務委託先従業員
□ その他
□ わからない

Q13. Q7 で選択した情報漏えいや流出事件・事故が起こった場所について選択してください。（いくつでも）

□ 社内
□ 移動中（電車や車など）
□ 客先/取引先
□ 自宅
□ 業務委託先
□ 子会社/関連会社内
□ 遠隔地の拠点
□ 仕事現場
□ その他
□ わからない

Q14. Q7 で選択した情報漏えいや流出事件・事故で対応に苦慮した点を教えてください。

□ （ ）

Q15. Q7 で選択した情報漏えいや流出事件・事故が発生した時期と会社（団体）として発覚/認知（気づく）するまでの期間について選択してください。
□ ～1 ヶ月未満
□ ～3 ヶ月未満
□ ～6 ヶ月未満
□ ～1 年未満
□ 1 年以上
□ わからない

Q16. Q7 で選択した情報漏えいや流出事件・事故の発覚の契機について選択してください。（いくつでも）

□ 内部監査
□ 外部監査
□ 顧客や会員からの通報

□ 自社（自団体）の社員が発見
□ 当事者（原因主体）による申告・報告
□ システムのログのチェック
□ 検知ツールによるアラート
□ 委託先/再委託先からの連絡
□ 他の組織、一般市民からの通報
□ 顧客や会員における何らかの被害や損害の発生
□ マスコミによる報道
□ その他
□ わからない

Q17. Q7 で選択した情報漏えいや流出事件・事故への対応としてとった手段について選択ください。（いくつでも）

□ 現場・証拠の保全
□ 被害の拡大防止具体的に
□ 被害範囲・影響範囲の確認
□ 所管官庁・関係省庁への連絡/届出
□ 被害者への電話連絡、謝罪
□ 被害者への訪問謝罪
□ 被害者への金券の配布
□ 被害者に詫び状の送付
□ 事件・事故への対応状況をホームページ等に開示
□ 記者会見
□ 被害者への対応窓口にコールセンター設置
□ 情報セキュリティの専門業者への相談
□ 新聞社告で開示
□ 原因究明のための調査（フォレンジック含む）
□ その他
□ わからない

Q18. Q7 で選択した情報漏えいや流出事件・事故の再発防止措置について選択してください。（いくつでも）

□ 規程や運用方法・手順の改定/改善
□ 従業員に対する教育・研修
□ 情報セキュリティ管理責任者の設置
□ 委託先の監査・監視
□ 委託先との契約解除
□ 委託先との契約内容の見直し
□ 同様の事件・事故の発生を防止するためのシステムの導入
□ 事故対応チームの設置
□ 情報セキュリティサービス事業者への業務委託
□ 情報漏えい保険への加入
□ 従業員の採用、退職の際の守秘義務契約

□ その他の対策
□ 特に再発防止措置は実施しなかった／まだ実施していない

Q19. Q7 で選択した情報漏えいや流出事件・事故は、同様の事故が過去二回以上発生したことがありますか。

□ ある
□ ない
□ わからない

Q20. あなたの勤務先で、今後想定・懸念される情報漏えいや流出事件・事故について選択してください。（いくつでも）

□ サイバー攻撃（不正アクセス、標的型攻撃メール等）
□ 内部関係者（従業員、派遣社員等）の不正行為
□ 情報管理及びサービスの委託先/再委託先での管理不備
□ 業務で利用する PC、記憶媒体、スマホなどの紛失・盗難
□ 書類持ち出し時の紛失・盗難
□ 電子メールの誤送信
□ FAX 誤送信
□ 建物やオフィスへの侵入による情報資産の窃盗・盗難
□ 業務で利用する PC やスマートフォン、業務システムやサーバのマルウェア感染
□ SNS（Facebook、Twitter、LINE 等）による個人情報や業務情報の拡散
□ 情報を預けるクラウドサービス事業者での事故やトラブル
□ PC・記憶媒体や書類の誤廃棄
□ その他
□ 特にない／わからない

Q21. Q20 の選択肢を選択した理由や把握している事情を可能な範囲で教えてください。

□ （　　）

Q22. 以下の項目の内容について最もあてはまるものをお答えください。
※ここでいう「事故」とは情報漏えいや流出事件・事故を意味します。（以降設問も同様です）

1. 他部署や他拠点、委託先では事故は発生していると思いますか。
2. あなたの勤務先では、他部署、他拠点、委託先で発生した事故は全社的に共有や注意喚起がなされますか。
3. あなたの勤務先に情報漏えい事故や事件の報告・体制はありますか。
4. あなたの勤務先では軽微なものでも事故として取り扱いますか。

□ はい
□ いいえ
□ わからない

Q23. あなたの勤務先では軽微なもので事故として扱われないものはどのようなものがありますか。(例：メールの宛先間違い、社内での紛失など)

□ (　　)

２．回答者の属性調査項目

Q24. あなたの勤務先の業種について以下の中からお答えください。※複数ある場合は、主な勤務先についてお答えください。

□ 情報通信業
□ 学校・教育事業
□ サービス業
□ 公務
□ 製造業
□ 学術研究、専門・技術サービス業
□ 運輸業、郵便業
□ 建設業
□ 卸売業、小売業
□ 金融業、保険業
□ 医療、福祉
□ 電気・ガス・熱供給・水道業
□ 不動産業、物品賃貸業
□ 生活関連サービス業、娯楽業
□ その他

Q25. あなたの勤務先の従業員数について以下の中からお答えください。
※複数ある場合は、主な勤務先についてお答えください。
※パートやアルバイトも含めてお答えください。
※子会社やグループ会社も含めてお答えください。

□ 99 人以下
□ 100～299 人
□ 300～499 人
□ 500～999 人
□ 1，000～2，999 人
□ 3，000～4，999 人
□ 5，000 人以上
□ わからない

Q26. あなたが勤務先で所属している部門について以下の中からお答えください。
※複数ある場合は、主に所属している部門についてお答えください。

□ 営業部門
□ 情報システム部門

☐ 総務、人事、経理、労務部門
☐ 経営企画部門
☐ 法務部門
☐ リスク管理部門
☐ その他

編集・発行　　株式会社エス・ピー・ネットワーク

本社：東京都杉並区上荻一丁目２番１号インテグラルタワー
TEL　03-6891-5556　　FAX　03-6891-5570
E-Mail　info@sp-network.co.jp