株式会社エス・ピー・ネットワーク
総合研究室

ＳＰＮレポート 2018 年
Security Protection Network Report Series.
～情報漏えい事故に関するアンケート～
【要約版】

1. はじめに

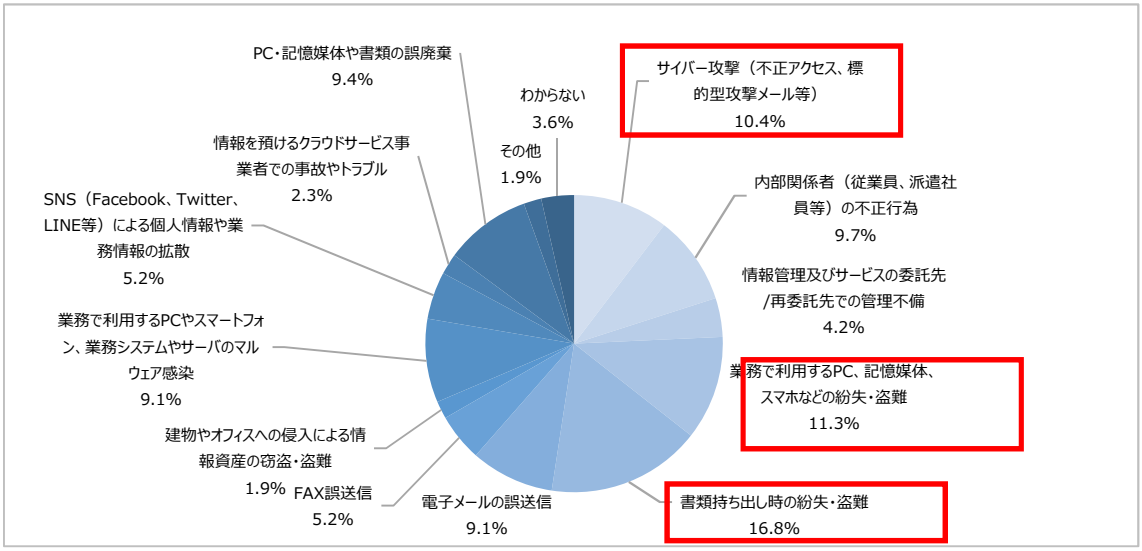
この度、弊社では、企業における情報セキュリティ事故対応の準備状況や対策の実施状況の実態を把握するためにアンケート調査（以下、「本調査」という）を実施しました。本調査が、貴社における情報管理体制を最適な状態に維持するためのきっかけとなり、事故発生時の事業継続や事態を極小化するための指標として活用していただければ幸いです。

2. 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

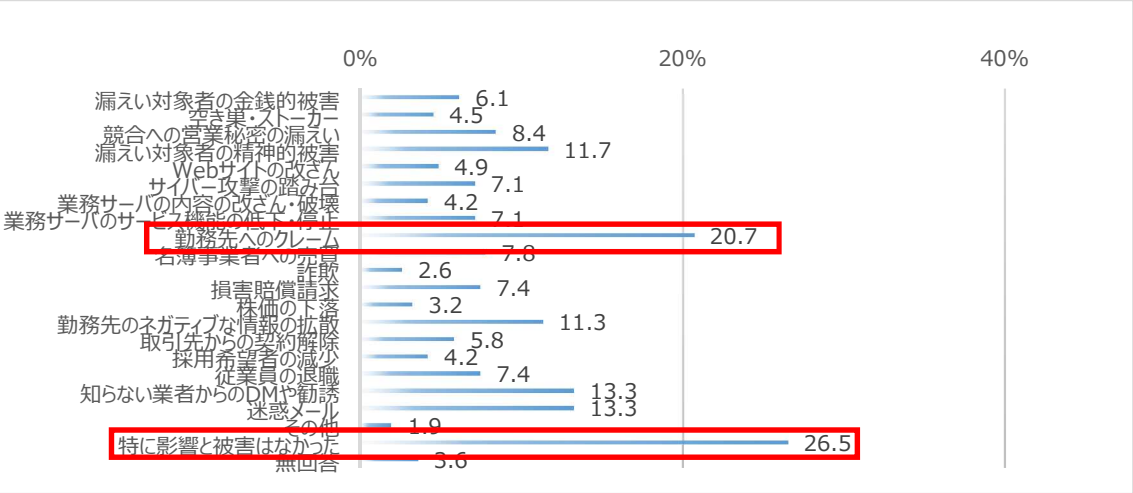
3. 調査結果

① 勤務先で発生した最も影響の大きかった情報漏えい事故



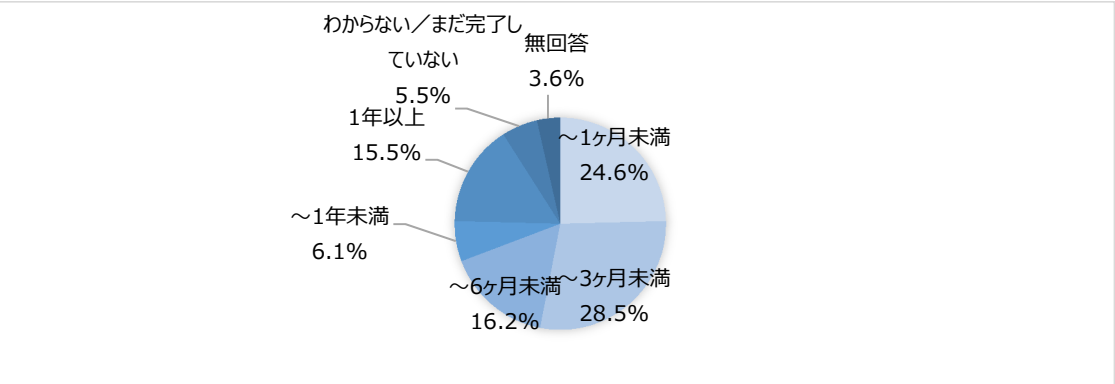
最も影響の大きかった事故としては、「書類持ち出し時の紛失・盗難」「業務で利用する PC、記憶媒体、スマホなどの紛失・盗難」「サイバー攻撃（不正アクセス、標的型攻撃メール）」がそれぞれ 10%以上を占めており、次いで、「内部関係者（従業員、派遣社員等）の不正行為」「PC・記憶媒体や書類の誤廃棄」「業務で利用する PC やスマートフォン、業務システムやサーバのマルウェア感染」「電子メールの誤送信」がそれぞれ約 9%を占めています。

② 情報漏えい時に発生した被害



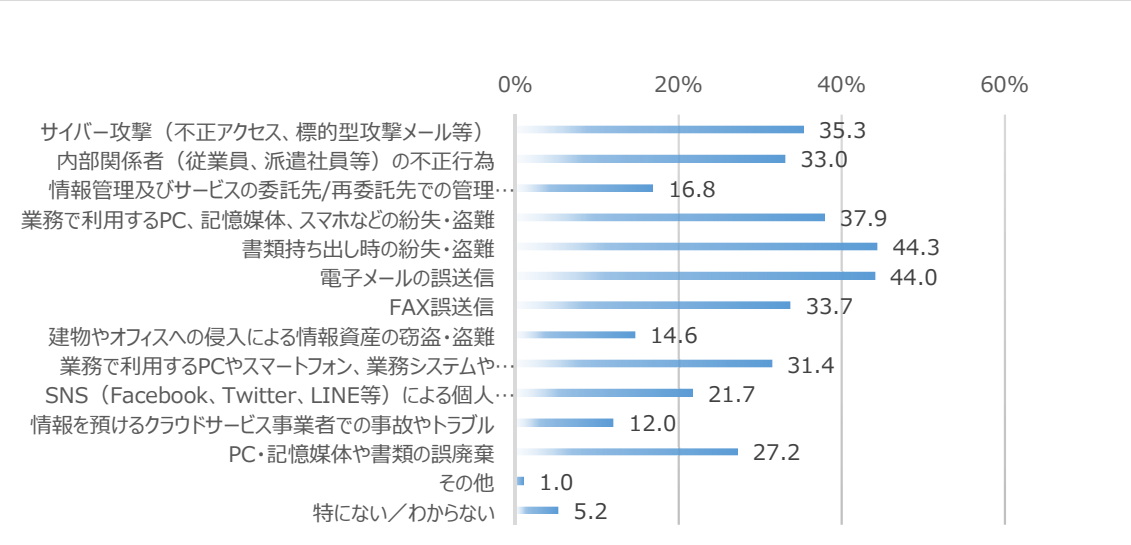
「勤務先へのクレーム」は、20.7%を占めており、漏えいした情報が悪用される可能性や不安感、不適切な情報管理に対するお叱りやクレームへの対応に苦慮していることがうかがえます。また、「特に影響と被害はなかった」が 26.5%を占めていますが、現時点で影響や被害が確認されていないだけで、知らないところで悪用されている可能性は否定できません。被害を受けていること、または（踏み台にされるなど）加害者の立場となってしまっていることに自発的には気が付かないこと（消費者や特定団体等の第三者からの通報で発覚するケースなど）も多くありますので、「被害がない」とは言い切れない点に注意が必要です。

③ 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



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は、「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。事故対応においては、情報伝達の手順等を確立しておくことが重要です。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、極めて重要な初動対応に遅れやミスが生じ、事故の被害を拡大させ、結果的に対応が長期化してしまった事例も数多く見受けられます。

④ 今後、想定・懸念される事故



今後想定・懸念される事故をあげてもらったところ、勤務先で過去発生した事故とほぼ同じ傾向であることが確認されました。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、効果的な再発防止が検討されていない、いまだ問題や脆弱性が軽視・放置されているなど、既に顕在化したリスクであっても十分に管理できていないのが実態だと読み取ることができます。事業者は、事故発生の有無に関わらず、自社の情報資産に応じたリスク管理を徹底するために、システム面・運用面の双方において継続的に高いレベルで取り組むことが求められます。

⑤ 事故対応に苦慮した点（自由記述より一部抜粋）

- 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
- 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
- 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
- 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
- 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　など

実際の事故対応に苦慮した点として、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。

4.　調査結果をふまえて

実際に事故が発生すれば、様々なことを組織として判断することになりますが、そのため必要な情報を、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、「こうなっているはずだ」「こうすべきだ」というものと実態（現実）とが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」などの状況が次々と判明し、そこではじめて「何もできていない」「何も分かっていない」現実に向き合うことになります。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、リスク管理のあり方として相応しくありません。他社で発生した問題はいつか自社にも起こる問題だと捉え、「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」という視点で常に考え、自社の現状を検証し続けることが重要です。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、改善すべき事項などがみえてきます。その反復が緊急事態における適切かつ速やかな対応を裏付けることになります。

以上