Biz Clip調査レポート（第9回）

企業の情報セキュリティ対策意識調査2018

2018.02.07

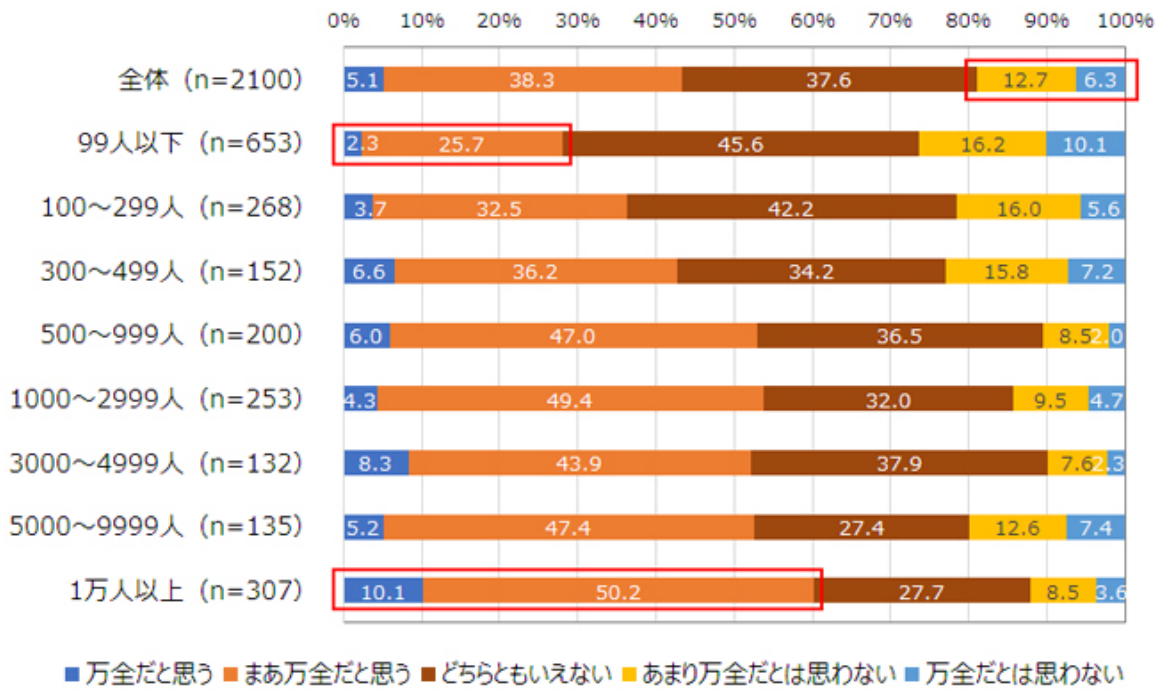
企業における情報セキュリティ対策はどの程度整備されているか。また、どんな意識を持っているか。その実態について、日経BPコンサルティングのアンケートシステムAIDAにて、同社保有の調査モニター3088人を対象に調査を実施した。

大きい企業ほど情報セキュリティ対策が万全だと認識

社内の情報セキュリティ対策に対して、「万全だと思う」と回答したのは全体でわずか5.1%。1年前の前回調査では5.4%と、0.3ポイントのダウンとなった。「まあ万全だと思う」と回答した企業は38.3%で、こちらも2017年の41.2%から2.9ポイントのダウンとなった。1年たっても、セキュリティを万全と感じている企業は少ないままだ。

一方、不備を感じる企業は、「万全だとは思わない」「あまり万全だとは思わない」を合わせて、2017年調査と同じく全体の2割となった。企業の従業員規模で見ると、情報セキュリティ対策が万全と感じる比率が高いのは、1万人以上の大企業で10.1%。「万全だと思う」と「まあ万全だと思う」を合わせると、99人以下の企業の選択率が3割未満なのに対し、1万人以上の企業では6割を超え2倍以上の割合となる。この傾向は2017年と変わらない。500人以上の企業は「万全だと思う」「まあ万全だと思う」との回答が過半数を占める一方で、499人以下の企業ではその回答が5割に満たない。従業員規模の小さい企業が、昨年と変わらず情報セキュリティ対策が十分ではないと感じている。

【図1 社内の情報セキュリティ対策は万全か(従業員数別)】



社内の情報資産管理の脅威は「標的型攻撃による情報流出」

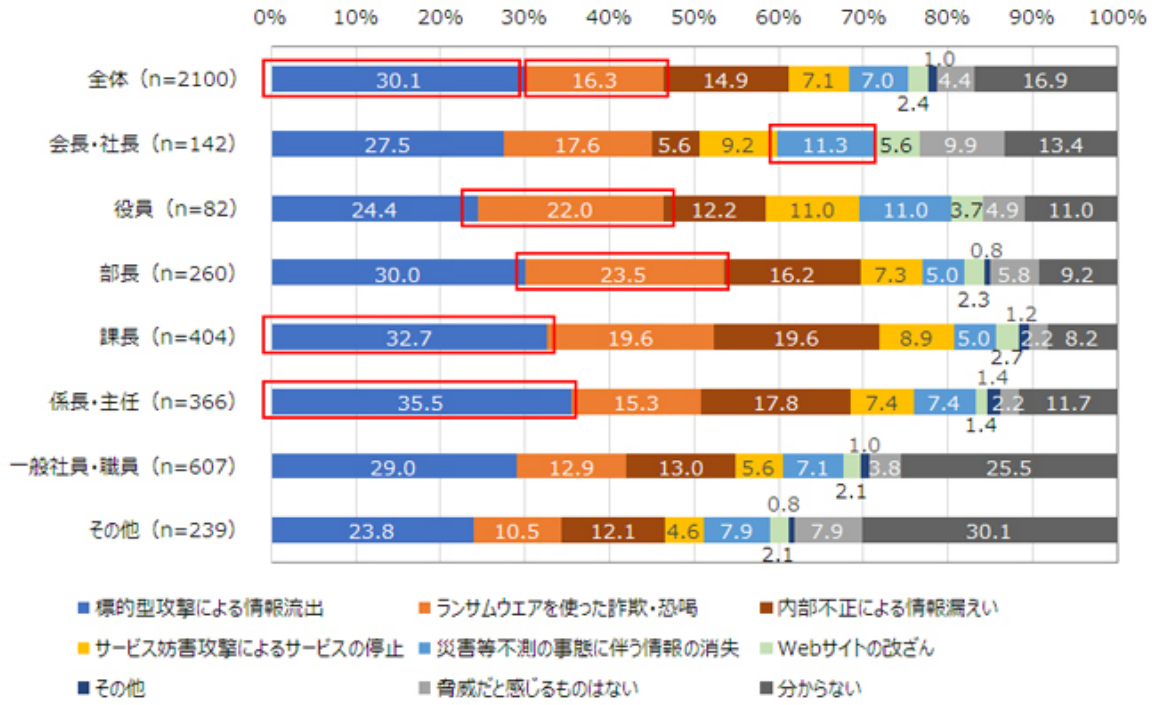
社内の情報資産管理で最も脅威と感じているのは、「標的型攻撃による情報流出」だ。全体の30.1%が選択した。前回の26.4%から3.7ポイントアップした。それに続くのが「ランサムウエアを使った詐欺・恐喝」で、16.3%が選択。昨年の10.2%から6.1ポイントのアップとなった。昨年、身代金型ウイルスであるランサムウエアの被害が話題となったことが大きく影響した形

だ。前回2番目であった「内部不正による情報漏えい」は14.9%の3番目となった。

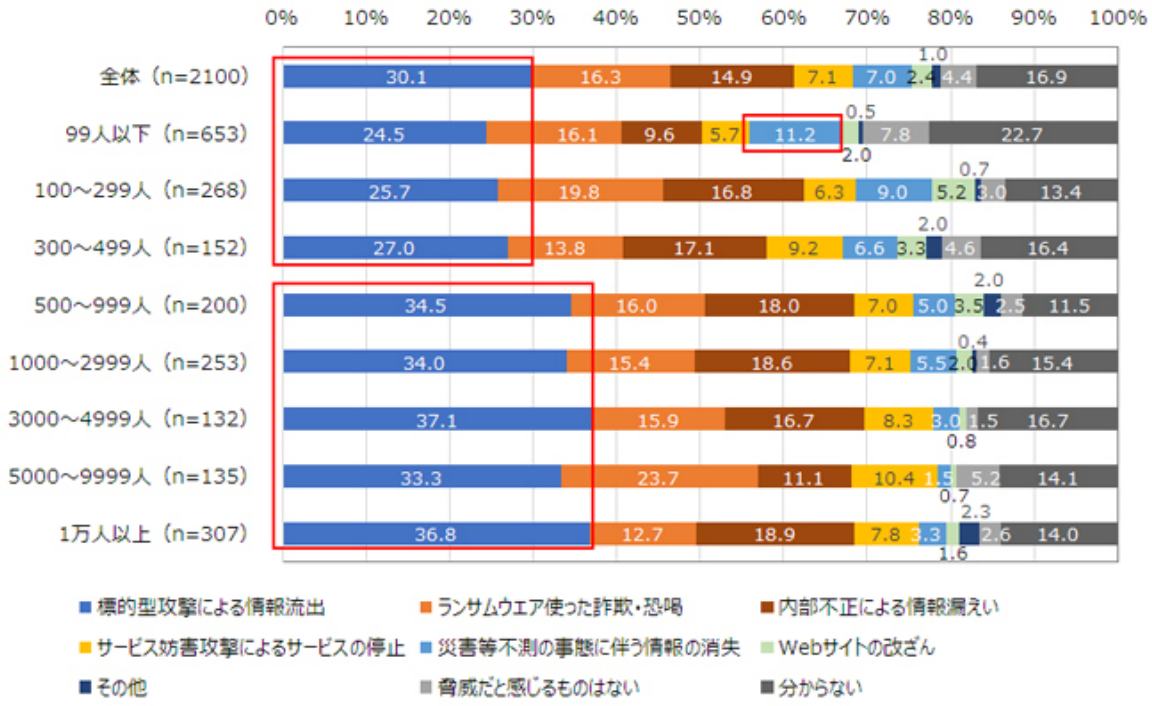
役職別で見ると、「標的型攻撃による情報流出」に対し、最も脅威と感じている人が多い役職は、昨年と同じく係長・主任で35.5%、差がなく課長の32.7%となっている。「ランサムウエアを使った詐欺・恐喝」については、部長の選択率が23.5%と最も高く、続いて役員の22.0%となった。役員においては、「標的型攻撃による情報流出」とほぼ差がない。会長・社長が昨年最も脅威と感じた「災害等不測の事態に伴う情報の消失」は11.3%の選択率で、今回の調査では第3位。標的型攻撃、ランサムウエアの脅威が上回った。

従業員規模で見ると、「標的型攻撃による情報流出」については、500人以上の企業と499人以下の企業で差が見られた。500人以上の企業はそれぞれ3割を超えたが、499人以下の企業ではすべて3割を切った。一方、従業員規模が小さい企業のほうが選択率が高くなったのは、昨年と同じく「災害等不測の事態に伴う情報の消失」だ。99人以下の企業が11.2%と1割が選択した。クラウド対応や、分散管理の進み具合が起因していると考えてよいだろう。

【図2-1社内の情報資産管理で最も脅威と感じること(役職別)】



【図2-2 社内の情報資産管理で最も脅威と感じること(従業員数別)】



「ウイルス対策」は対応済み。各対策とも大企業ほど導入率が高い… 続きを読む