企業の情報漏洩対策に関する調査

－結果概要報告書－

平成27年9月

甲 府 商 工 会 議 所

◆調査要領

１．調 査 の 目 的：　会員事業所における情報漏洩対策の現状を把握すると共に、今後の事業を検討する際の参考資料とする。
２．調査実施機関：　甲 府 商 工 会 議 所
３．調査実施時期：　平成２７年８月１９日(水)～８月２６日(水)
４．調 査 対 象：　当所会員 ３12 事業所
５．調 査 方 法：　ＦＡＸ調査
６．有 効 回 答 数：　80
７．有 効 回 答 率：　25.6%
８．特 記 事 項：　原則、小数点以下第二位で四捨五入。

◆結果概要

本調査の結果、会員事業所における情報漏洩への対策状況は、『対策はあるが、今後も対策を講じる予定』との回答が、46.3%と最も多くなった。『未対策だが、今後は対策を講じていく予定』と回答した事業所は 25.0%と２番目に多く、更に『未対策だが、今後の対策も未定』(18.8%)が続いた。『対策済みであり、更なる対策の予定はない』とした企業は 10.0%と最も少なくなった。現状の対策状況に注目すると、43.8%の事業所は未対策となるが、その内の半数以上は今後対策を講じていく予定としている。

対策の具体的な取り組み内容については、『情報の取り扱いに関する社内規則の整備』（63.1%）が最も多く挙げられた。以下は『データの保管場所・方法の見直し』（44.6%）、『研修会等による従業員の教育』（41.5%）、『情報システムやソフトウェアの更新・強化』（36.9%）、『情報管理責任者・部署の設置』（35.4%）と続いた。

事業所が危惧している情報の流出経路・要因については、『従業員の教育不足や取扱いミス、情報の持ち出し』（72.5%）が最も回答が多く、次いで多かった『自社の情報システムへの外部からの不正アクセス』（50.0%）を上回る結果となった。

また、情報漏洩への対策をしていく上での各事業所における課題を尋ねたところ、36.3%の企業が『対策に割く時間・人員の不足』と回答した。『何から始めていいかわからない』と回答した事業所は 20.0%となり、『対策に割く資金の不足』（7.5%）を上回った。また、『その他』においては『従業員の教育』や、『従業員の意識』が挙げられた。一方、課題は『特になし』とした企業も３割程度存在している。

過去３年間に発生したトラブルについては、82.5%の企業は『特にトラブルは発生していない』と回答した。トラブル経験があると回答した企業では、『ウイルスやスパイウェアへの感染』とした事業所が 12.5%と最も多かったが、実際に個人情報の流出まで至った事業所は 1.3%のみとなった。

本調査の結果、現在の会員事業所における情報漏洩への対策は、４割超の事業所で未実施という結果となった。しかし、その内半数以上の事業所は取組みを予定しており、今後企業の情報セキュリティの強化は進んでいくと推察される。個人情報の漏洩が問題となり、企業の対応が問われる中で、企業が抱える最大の不安要素はやはり人的ミスであり、社内規則の整備や従業員の教育といった形での対策が中心となることがわかった。

◆結果詳細

Q１．『貴社の情報漏洩への対策についてお聞かせください』[択一回答]

◆ ４６．３%の事業所が『対策はあるが、今後も対策を講じていく予定』と回答

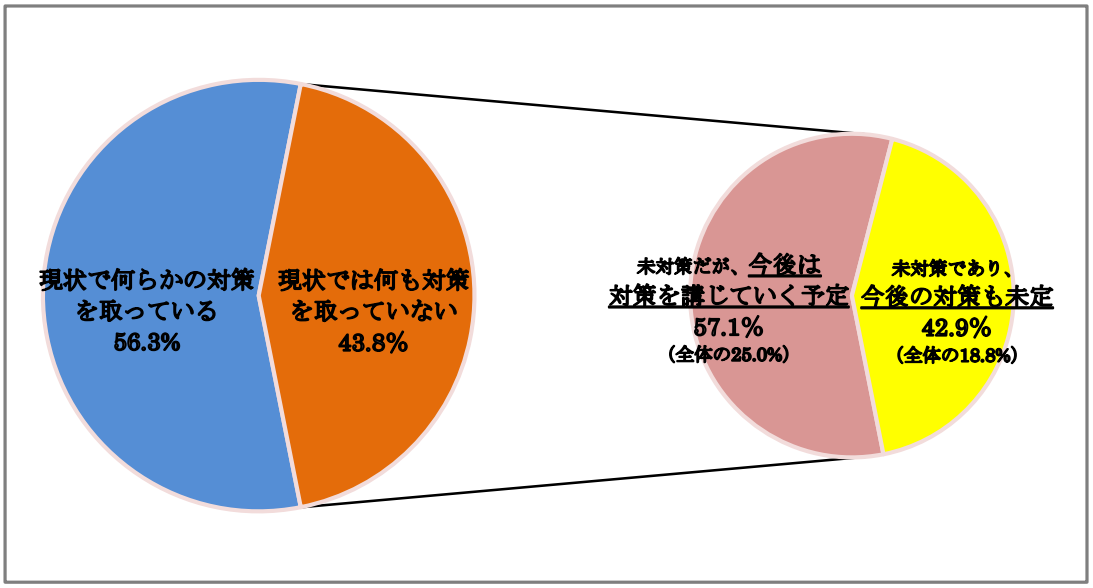
情報漏洩への対策状況を尋ねたところ、最も多い回答は 46.3%を占めた『対策はあるが、今後も対策を講じていく予定』だった。また、次いで回答の多かった『未対策だが、今後は対策を講じていく予定』は 25.0%となり、合計すると７割強の企業が今後情報セキュリティの強化に取り組む姿勢だ。しかし、一方では 18.8%の企業が『未対策であり、今後の予定も未定』と回答している。最も少なかった回答は『対策済みであり、更なる対策の予定はない』となり、全体の１割であった。〈表１〉

現状の対策状況に着目すると、現状で情報漏洩に対し何らかの対策を取っている事業所は 56.3%で、残る 43.8%の事業所では未対策であることがわかった。しかし、現状で未対策である事業所の内、半数以上が今後は対策を講じていく予定と回答している。〈表２〉

表１

	実数	構成比（%）
対策はあるが、今後も対策を講じる予定	37	46.3
未対策だが、今後は対策を講じていく予定	20	25.0
未対策であり、今後の対策も未定	15	18.8
対策済みであり、更なる対策の予定はない	8	10.0
合計	80	100.0

表２.情報漏洩対策の現状



Q２.『Q１で“対策に取り組んでいる、あるいは取り組む予定がある”と回答した方にお伺いします。貴社で現在取り組んでいる対策、あるいは取り組む予定の対策についてお聞かせ下さい。』　［複数回答　３つまで］

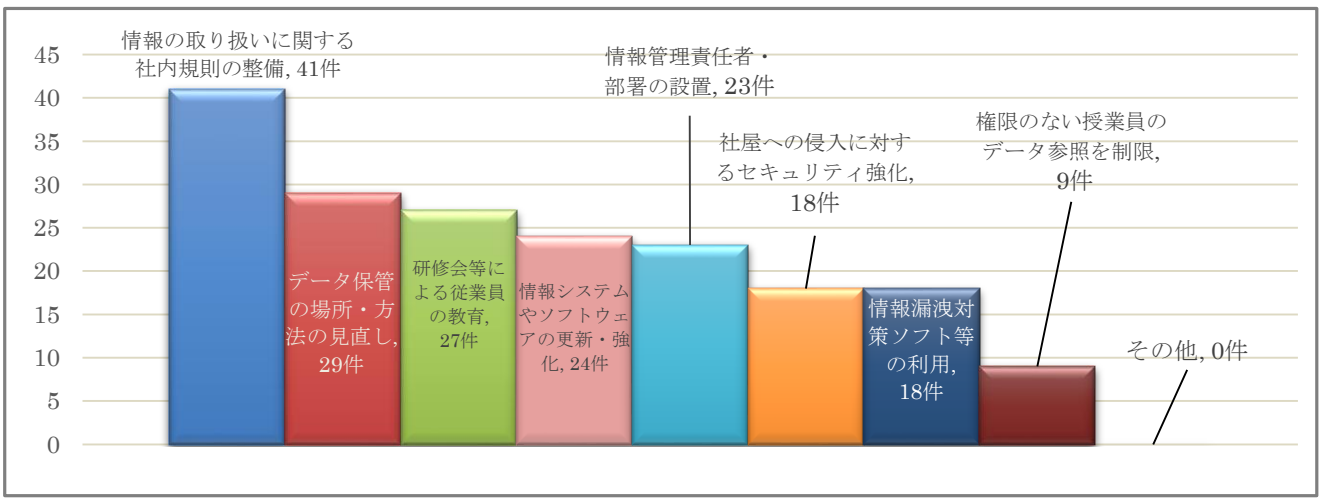
◆ ６３．１％の事業所が『情報の取り扱いに対する社内規則の整備』と回答

Ｑ１の問いにおいて、現状で情報漏洩への対策を取っている、あるいは今後対策を取っていく予定だと回答した事業所に、その対策内容を尋ねたところ、最も多かった回答は『情報の取り扱いに関する社内規則の整備』（63.1％）であった。２番目に多く挙げられたのは『データ保管の場所・方法の見直し』（44.6％）、３番目は『研修会等による従業員の教育』（41.5％）となった。以降は多い順に『情報システムやソフトウェアの更新・強化』（36.9％）、『情報管理責任者・部署の設置』（35.4％）、『情報漏洩対策ソフト等の利用』、『社屋への侵入に対するセキュリティ強化』が 27.7％で並び、最も回答が少なかったのは『権限のない従業員のデータ参照を制限』（13.8％）となった。『その他』については０％であった。

表３

	実数	構成比（%）
情報の取り扱いに関する社内規則の整備	41	63.1
データ保管の場所･方法の見直し	29	44.6
研修会等による従業員の教育	27	41.5
情報システムやソフトウェアの更新･強化	24	36.9
情報管理責任者･部署の設置	23	35.4
社屋への侵入に対するセキュリティ強化	18	27.7
情報漏洩対策ソフト等の利用	18	27.7
権限のない授業員のデータ参照を制限	9	13.8
その他	0	0.0
合計	65	

表４



Q３.『どういった経路・要因からの情報漏洩を危惧していますか』[複数回答　２つまで]

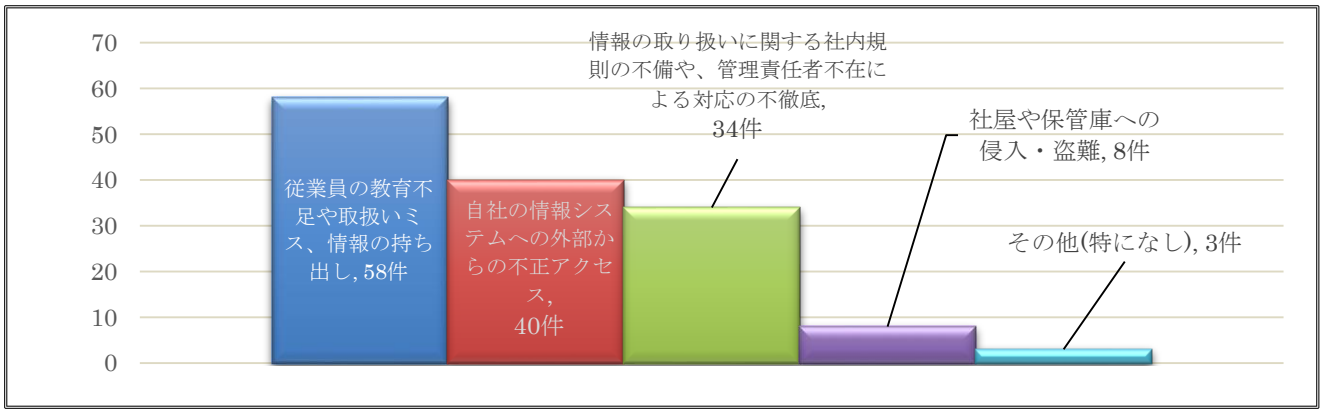
◆ 72.5%の事業所が『従業員の教育不足や取り扱いミス、情報の持ち出し』と回答

危惧している情報の流出経路・要因について尋ねたところ、72.5%の事業所が『従業員の教育不足や取り扱いミス、情報の持ち出し』と回答した。次いで多かった回答は『自社の情報システムへの外部からの不正アクセス』(50.0%) だった。更に『情報の取り扱いに関する社内規則の不備や、管理責任者不在による対応の不徹底』(42.5%) が続き、最も少なかった『社屋や保管庫への侵入・盗難』は全体の１割であった。『その他』と回答した 3.8%の事業所は全て『特になし』と回答した。

表５.

	実数	構成比(%)
従業員の教育不足や取扱いミス、情報の持ち出し	58	72.5
自社の情報システムへの外部からの不正アクセス	40	50.0
情報の取り扱いに関する社内規則の不備や、管理責任者不在による対応の不徹底	34	42.5
社屋や保管庫への侵入・盗難	8	10.0
その他(特になし)	3	3.8
合計	80	

表６



Q４.『情報漏洩対策を講じる上で最も課題となっている事はどのような点ですか』[択一回答]

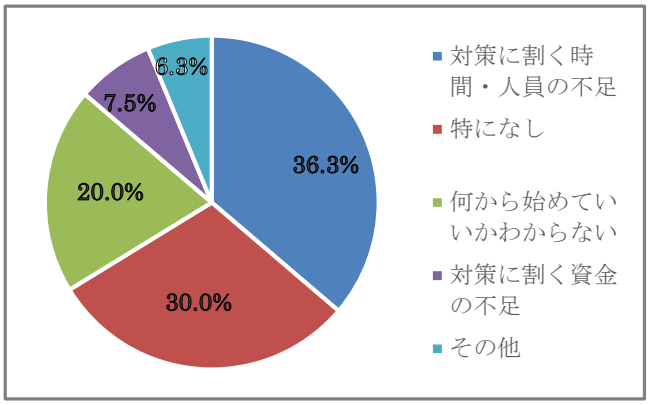
◆ ３６．３%の事業所が『対策に割く時間・人員の不足』と回答

情報漏洩対策を講じる上で課題となっている事を尋ねたところ、36.3%の事業所が『対策に割く時間・人員の不足』と回答し、最多となった。しかし、次いで多くなったのは 30.0%の『特になし』である。以下は『何から始めていいかわからない』（20.0%）、『対策に割く資金の不足』（7.5%）と続いた。『その他』（6.3%）は、『従業員の教育』（３件）、『従業員の意識を高めること』、『システム面での対応』といった回答があった。

表７.

	実数	構成比（%）
対策に割く時間・人員の不足	29	36.3
特になし	24	30.0
何から始めていいかわからない	16	20.0
対策に割く資金の不足	6	7.5
その他	5	6.3
合計	80	100.0

表８



Q５.『貴社で過去３年間に発生したことがある、情報セキュリティに関するトラブルについてお聞かせください』　［複数回答　あてはまるもの全て］

◆ ８２．５%の事業所が『特にトラブルは発生していない』と回答

過去３年間で自社で起きた情報セキュリティに関するトラブルについて尋ねたところ、82.5%の事業所が『特にトラブルは発生していない』と回答し、最多となった。一方で、残る １７.5%の事業所が情報セキュリティに関するトラブルを経験したということになるが、その内で最も多かったのは『ウイルスやスパイウェアへの感染』（12.5%）で１割強の事業所が経験している。『情報機器（ノート PC・USB メモリ等）の紛失』、『紙媒体情報の紛失・盗難』はともに 3.8%の事業所が経験していると回答、『他者によるデータの破壊・改ざん』、『個人情報等の電子データの流出』はそれぞれ 1.3%の事業所が経験している事がわかった。

表９

	実数	構成比（%）
特にトラブルは発生していない	66	82.5
ウイルスやスパイウェアへの感染	10	12.5
情報機器の紛失（ノート PC・USB メモリ等）	3	3.8
紙媒体情報の盗難・紛失	3	3.8
他者によるデータの破壊・改ざん	1	1.3
個人情報等の電子データの流出	1	1.3
合計	80	

以上