

※ 旧AIU損害保険株式会社のプレスリリースになります。

ABPR130002

プレスリリース

2013年1月23日

国内200名の経営者を対象に「情報漏えいリスクに対する意識調査」を実施
～「自然災害」よりも「情報漏えい」に対する脅威が約10%上回る結果に～

AIU保険会社（日本における代表者 会長兼CEO 小関誠、以下AIU）は、2012年12月に販売を開始した『CyberEdge』の潜在的なニーズを把握し、国内経営層の「情報漏洩リスクに対する意識」を明らかにすることを目的として、経営者200名を対象に意識調査を実施しました。

<調査結果 トピックス>

経営者が意識する脅威は“情報セキュリティ領域のリスク”

全8項目（法務法令・コンプライアンス、自然災害、外部からのサイバー攻撃、情報漏えい、為替変動、訴訟、労務、顧客及び取引先）のリスク因子が脅威であるか否かを聞いたところ、東日本大震災でより一層意識が高まっているものと思われた「自然災害のリスク（70.5%）」よりも、「情報漏えいに関するリスク（81.0%）」を脅威とする経営者が多いことが明らかとなりました。また、「外部からのサイバー攻撃のリスク（67.5%）」も「為替変動リスク（46.0%）」や「労務リスク（61.5%）」を上回る結果となり、“情報セキュリティ領域のリスク”への意識の高さがうかがえます。

情報漏えい発生時、“事実確認と原因究明”の重要性を意識する傾向に

情報漏えい発生時に最も重要だと認識している対応策を聞いたところ、「速やかな事実確認の徹底（55.0%）」と「原因の究明と把握（21.0%）」が重要視されていることが明らかとなりました。

サイバー攻撃被害への想定対策費用は平均“約1億2,000万円”

自社がサイバー攻撃の被害にあった際、その対策にかかる想定費用を聞いたところ、全体平均で“約1億2,000万円”という結果が算出されました。想定費用は従業員数が多くなればなるほど高く、1,000人以上の企業では約3億4,000万円となり、100人から300人規模の企業と比較すると、約10倍の差がありました。

海外拠点の約70%が“無防備に近い”

海外拠点を持つ企業の経営者（62名）のうち、海外拠点がサイバー攻撃を受ける可能性を想定し、対策を取っている経営者は約20%にとどまりました。一方で、約70%の経営者が「想定はしていたが、対策は取れていない／検討中（38.7%）」、「想定はしておらず、対策は取っていない（30.6%）」と回答しており、海外拠点における対策が充分とは言い難い現状が明らかとなりました。

<調査概要>

方法： インターネット調査

対象： 日本国内在住の経営者200名

* 資本金5,000万円以上、従業員100人以上の経営者・役員が調査対象

期間： 2012年12月21日～23日

備考： 地域・性別・世代別等割り付けなし

[詳しい資料はこちら](#)

最終更新日：2013/01/23 CO-00040P

© AIG, Inc.