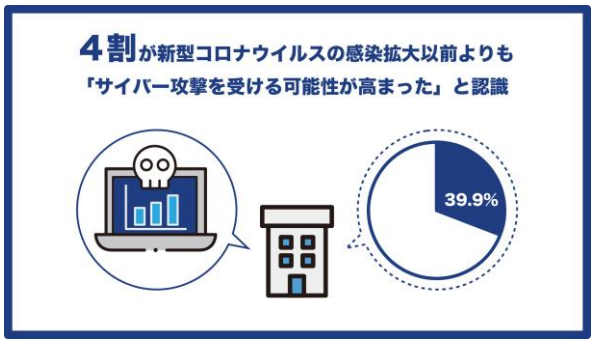
別紙

＜ポイント①＞

4 割の企業が、新型コロナウイルスの感染拡大以前と比較し、サイバー攻撃を受ける可能性が「高まった」と認識。一方、「変わらない」と認識している企業は、中小企業に多い。



・8 割の企業が、テレワークや WEB 会議を活用しており、そのうち 9 割が新型コロナウイルスの感染拡大をきっかけに導入している。さらに、自社がサイバー攻撃を受ける可能性について、4 割（39.9%）の企業が「新型コロナウイルスの感染拡大以前と比べて、サイバー攻撃を受ける可能性が高まった」と認識している。
・このことから、多くの企業にテレワーク等が浸透している中、サイバーリスクへの認識も徐々に高まっていると考えられる。
・一方、サイバー攻撃を受ける可能性は「変わらない」と認識している企業は、大企業は 53.9%なのに対し、中小企業は 62.7%であり、中小企業の方がサイバーリスクに対する危機意識が低い傾向である。

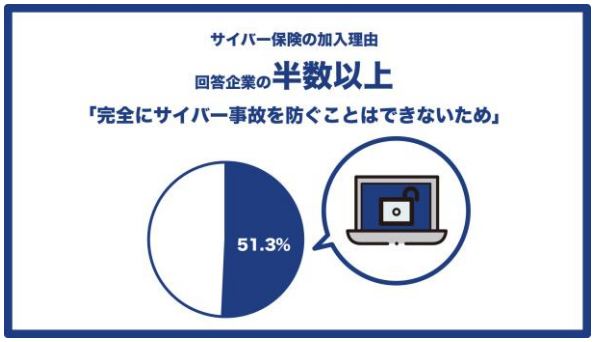
＜ポイント②＞

サイバーリスク対策における課題について最も多かった回答は「現在行っている対策が十分なのかわからない」（43.8%）。

・サイバーリスクに対する具体的な対策としては「ソフトウェア等の脆弱性管理・ウイルス対策ソフトの導入」（87.4%）が最も多く、続いて「アクセス権限・ログの管理および制御」（54.1%）など、システム上のセキュリティ対策を行っている企業が多く、ほとんどの企業が何らかのサイバーリスク対策を行っている（対策を行っていないと回答した企業は 3.6%）。しかし、サイバーリスク対策における自社の課題について聞くと、「現在行っている対策が十分なのか分からない」（43.8%）と回答した企業が最も多くなっている。
・このことから、サイバーリスク対策として、多くの企業がシステム上のセキュリティ対策を行っているものの、自社が行っている対策で、サイバーリスクに対して十分であるのか不安を感じていると考えられる。
・また、「対策をする費用が足りない」と回答した企業は、中小企業の比率が高く、中小企業では費用面もネックになっていることがうかがえる（大企業 15.7%、中小企業 23.0%）。
・一方、対策を行っていない企業は、半数以上がその理由として「サイバーリスクが発生する可能性は低いと考えているため」（55.4%）を挙げており、企業規模別では、特に中小企業の危機意識の低さが顕著となっている（大企業 35.3%、中小企業 64.1%）。

＜ポイント③＞

サイバー保険への加入理由について、半数以上が「完全にサイバー事故を防ぐことはできないため」と回答。一方、非加入理由としては「保険の補償内容や保険料についてよく知らないため」（40.7%）が最も多い。



・サイバーリスクに対して、発生予防策としてシステム上のセキュリティ対策などを行っている企業が多い一方で、発生時の様々な費用が補償される「サイバー保険」に加入している企業は 7.8%（大企業 9.8%、中小企業 6.7%）であった。
・加入理由としては、「完全にサイバー事故を防ぐことはできないため」が最も多かった（51.3%）。また、非加入理由としては、「保険の補償内容や保険料についてよく知らないため」（40.7%）が最も多く、サイバー保険の理解促進が課題である。
・一方、2 割（19.4%）の企業は、サイバー保険に「現在は加入していないが、今後加入予定」と回答している。その理由は、「会社の信用力向上につながるため」（60.4%）が最も多く、次に、加入理由と同じく「完全にサイバー事故を防ぐことはできないため」（52.0%）が続いている。
・このことから、セキュリティ対策を行っても完全に防げないサイバーリスクへの備えとして、サイバー保険が活用・検討されていることがうかがえる。

＜ポイント④＞

サイバー事故は企業規模を問わず発生。中小企業でも数千万円の被害事例がある。

・今回の調査で、全体の 13.4%の企業（205 社）がサイバー被害を受けたことがあると判明。中でも 116 社は中小企業であり、そのうち 53 社は複数回の被害を経験している。攻撃の手口については、「マルウェア」、「ランサムウェア」がともに 31.7%と多かった。
・また、サイバー被害を受けた際の被害総額について、中小企業でも「1,000 万円以上」との回答があり、たった一度の事故でも事業継続そのものを揺るがすような、数千万円規模の高額被害が発生している実態が分かった。

＜ポイント⑤＞

サイバー事故を経験したことがある企業、事故後の対応で苦労したのは「復旧対応」「原因・影響範囲の特定」「社内・社外への通知」など。

・サイバー事故を経験したことがある企業が事故発生直後の対応で苦労したことは、「復旧対応」（62.9%）が最も多く、次に「原因・影響範囲の特定」（58.5%）「社内・社外への通知」（39.0%）が続いた。
・事故が発生すると、初動対応として、原因・影響調査を実施し、データの復旧や再発防止策の策定といった対応を行う必要がある。また、情報漏えいが発生した場合は被害者への謝罪対応や、取引先等からの損害賠償請求も考えられる。
・サイバー保険は、このような各種対応費用や損害賠償額を補償するほか、IT 機器等の機能停止により一定期間業務ができない場合に生じる喪失利益や営業継続費用も補償する。さらに、保険会社によっては、標的型メール訓練サービスや専門業者の紹介サービス等を提供している。

その他、詳しくは、「サイバー保険特設サイト」（https://www.sonpo.or.jp/cyber-hoken/）をご覧ください。

＜調査の概要＞

【調査対象】帝国データバンクの企業モニター調査の登録企業（4,000 社）
【実査期間】2020 年 10 月 1 日（木）～2020 年 10 月 19 日（月）
【回答率】1,535 件／4,000 件（38.4%）
【調査実施機関】株式会社帝国データバンク　【調査手法】インターネット調査
【調査地域】全国
【調査結果ダウンロード URL】
https://www.sonpo.or.jp/cyber-hoken/data/2020-01/pdf/cyber_report2020.pdf

＜参考情報＞

■サイバー保険とは？

サイバー事故により企業に生じた第三者に対する損害賠償責任のほか、事故時に必要となる費用や自社の喪失利益を包括的に補償する保険です。

※上記の補償のほか、保険会社によっては、関連する付帯サービス（情報セキュリティ診断サービス等）を提供している場合があります。
※補償内容は、保険会社や保険会社が提供するサイバー保険のプランにより異なります。詳細は保険会社・代理店にご確認ください。

参考リンク：https://www.sonpo.or.jp/cyber-hoken/about/
（「サイバー保険特設サイト」サイバー保険とは）

■令和2年改正個人情報保護法について

令和2年6月12日に「個人情報の保護に関する法律等の一部を改正する法律」が公布されました。改正法の施行は、一部を除き公布後2年以内とされており、施行後、企業において個人情報の漏えい等が発生し個人の権利利益を害するおそれがある場合には、個人情報保護委員会への報告及び本人への通知が義務化されます。

今般の調査によると、上記の方針を知っている企業は 31.8%にとどまっています。悪質な場合は社名も公表されるなど、企業に対する規制が強まることから、サイバー事故が発生した企業を包括的にサポートする「サイバー保険」の必要性がますます高まっていくと考えられます。

参考リンク：https://www.ppc.go.jp/files/pdf/200612_gaiyou.pdf

（個人情報保護委員会HP「個人情報の保護に関する法律等の一部を改正する法律（概要）」）

以上