サイバーセキュリティ BCP 訓練事例

ほけんの窓口グループ株式会社 様

社会インフラである保険を通して「安心と安全」、「笑顔と幸せ」を届けることを使命とし、お客さまの「満足」と「ありがとう」を仕事の喜びとしている、ほけんの窓口グループ株式会社。同社は近年、顧客本位の業務運営の高度化に加え、デジタル社会の進展に対応した相談環境の整備や健康経営、多様な人材活躍の推進など、サービスと組織の両面から価値向上に取り組んでいる。

一方で、サイバー攻撃の高度化により、顧客情報や業務継続に直結するリスクは現実の経営課題となりつつある。とりわけ、部ごとに整備されたリスク手順書が有事に機能するのか、また自社の業務やシステムに即した実践的な訓練が不足している点は、見過ごせない課題だった。

こうした背景から同社は、実環境を踏まえたシナリオ設計と、本社の全部長層を巻き込んだ全社横断型のサイバーセキュリティ BCP 訓練に踏み切ることになった。今回、訓練を実施した経緯と効果などについて、法務コンプライアンス部長 吉田 勧司氏、同部 同課 スペシャリスト 大澤 佳織氏にお話を伺った。

統括部が担う全社セキュリティの中核機能

――情報セキュリティ統括課の主な業務内容をお聞かせください。

吉田氏　保険代理店の業務上、お客さまの個人情報を取り扱っているため、会社全体におけるセキュリティ体制の構築と、従業員においては高いセキュリティリテラシーが求められます。そこで当社では、以前から情報セキュリティ統括部門を設置し、お客さまの個人情報を含む機密情報の管理体制の構築・維持、およびセキュリティ対策における継続的なモニタリングを行っています。2025 年 7 月には、リスク管理とコンプライアンス強化のため、法務コンプライアンス部の下に情報セキュリティ統括課を新たに設置しました。法務コンプライアンス部に所属するコンプライアンス調査課、法務課、情報セキュリティ統括課が三位一体となってモニタリングする仕組みを構築しているところです。

――セキュリティ対策の取り組みについてお聞かせください。

大澤氏　大きく 2 つあります。1 つ目は、インフラやシステム周りのセキュリティ強化です。こちらはシステム部が主体となって強固なセキュリティ対策を推進します。サイバー攻撃は日々巧妙化しているので、今後も継続的に強化を図っていきます。

2 つ目は、従業員のリテラシー向上を図る教育プログラムの策定と実施です。具体的にはｅラーニングによるセキュリティ研修を年 3 回、標的型メール訓練を年 2 回、階層ごとにコンプライアンスや情報セキュリティに関する研修も設けています。さらに、法務コンプライアンス部としてコンプライアンスに関する情報を月 1 回全社に向けて発信。最近の情報漏えい事案を発信するなどして、セキュリティ対策の意識を高める取り組みを行っています。

――従業員のセキュリティ対策の意識についてはどのように感じていますか。

吉田氏　当社が「最優の会社づくりの 3 本柱」で掲げている「完璧な募集態勢の構築」に反しないように、本社はもちろん、店舗の隅々まで個人情報を管理するセキュリティ対策の意識を高く保ち、業務に取り組んでいます。

法務コンプライアンス部 情報セキュリティ統括課 スペシャリスト 大澤 佳織氏

訓練でリスク手順書の実用性を確認したい

――サイバーセキュリティ BCP 訓練を実施した背景をお聞かせください。

吉田氏　強固なセキュリティ対策の体制と仕組みを構築しているつもりですが、油断はできません。実際、サイバー攻撃によって、システムがダウンしてしまう可能性は否定できないと考えています。そこで当社ではサイバー攻撃の場面を想定し、素早いリカバリーと事業継続のためのリスク手順書を部ごとに用意しています。

ただし、リスク手順書が正しく機能するかどうか、具体的には確認できていませんでした。そのリスク手順書の実用性を確認するため、ラックのサイバーセキュリティ BCP 訓練を利用しました。

なぜ、ラックの訓練を選んだのか

――セキュリティ訓練を行うベンダーの比較・検討はされたのでしょうか。

大澤氏　ベンダー数社で訓練内容を比較・検討しました。ラックを選定した理由は 2 つあります。1 つは当社のネットワークやシステムを監視し、サイバー攻撃の兆候や異常を発見した場合は速やかに対処する JSOC（Japan Security Operation Center）※をお願いしている点です。いつもシステム周りを監視してもらっている安心感に加え、サイバー攻撃やセキュリティ対策における豊富な経験や知見もあるので、ラックなら我々が求めるサイバーセキュリティ BCP 訓練を実施してくれるのではないかという期待がありました。

もう 1 つは、当社向けにオーダーメイドした訓練を提案いただけたことです。当社としてはシステムや組織の実情を反映し、かつリスク手順書を確認できる訓練を求めていたため、オーダーメイドが必要だと思っていました。ラックがパッケージ化したセキュリティ研修・訓練を展開していることは認識していましたが、自社の組織や業務実態に合わせたオーダーメイド設計が可能だと知り、サイバーセキュリティ BCP 訓練を依頼しました。

※ 2002 年に開設した国内最大規模のセキュリティ監視・運用サービス拠点。

――サイバーセキュリティ BCP 訓練を 2 回行われていますが、その 1 回目の訓練の概要をお聞かせください。

大澤氏　1 回目も 2 回目も、本社機能を中心とした BCP がテーマの訓練です。1 回目は、リスク手順書を用意している部の担当者を集めました。ランサムウェアに感染した場合、影響が予想される業務システムに関係している部で、直接関わりがない部は参加していません。

ラックとは、当社で用意したシナリオ案とリスク手順書をもとに綿密な打ち合わせを繰り返し、ランサムウェアで発生する事象の収束を目指していくリスクシナリオを作成しました。このとき注意したのは、参加者が違和感を持たないシナリオです。ラックの協力を得ながらリアルなストーリーのシナリオを作成し、2025 年 3 月に当社のセミナールームにおいて、約 40 名（リモートを含む）が参加したサイバーセキュリティ BCP 訓練を実施しました。

判断と行動をすり合わせた、1回目の訓練

――1回目のサイバーセキュリティBCP訓練についての評価をお聞かせください。

大澤氏　訓練は、シナリオの時系列に沿って進行し、刻々と変化する状況を参加者間で共有しながら、その場で判断や行動をすり合わせていく実践形式で実施しました。意思決定のベースとなる各部のリスク手順書は、当初想定していた通り縦割りの色合いが強く、単独では機能しきれない場面も見受けられました。

しかし、訓練を通じて他部との連携を確認できたおかげで、リスク手順書に横串を刺していくイメージを共有できました。参加者が担当者レベルだったこともあり、技術的な話を交えつつ、率直な意見が交わされる実践的な場となりました。

参加者の声としては「リスク手順書が使えるかどうか確認したことがなかったため、とても参考になった」「リスク手順書の見直しが必要と思った点があり、とても有意義な訓練だった」「実際に他部の動きなどを把握したうえで、どのように行動すべきか考えることができた」「どの部と連携すべきか明確になった」など、ポジティブな声を数多く聞くことができました。

部長層を巻き込んだ2回目の訓練

――2回目のサイバーセキュリティBCP訓練の意図をお聞かせください。

大澤氏　1回目のサイバーセキュリティBCP訓練を経て、セキュリティおよびBCPに対する意識が醸成されたのは間違いありません。ただし、全部ではなかったこと、担当者レベルで止まっている懸念があることから、もっと全社的に取り組んでいく必要があるのではないかという意見がありました。そこで、2回目のサイバーセキュリティBCP訓練は、本社の全部および部長層が参加する訓練を目指しました。

――2回目の訓練の概要をお聞かせください。

大澤氏　2回目の訓練は、1回目のサイバーセキュリティBCP訓練をベースにシナリオづくりを行いました。ただし、忙しい部長層に参加してもらうので、長時間の拘束はできません。そこで、システム面の話よりも業務に関わるフローにフォーカスした3時間の訓練としました。もちろん、2回目もラックと綿密な打ち合わせを実施しています。

各部の部長層が集まった2回目のサイバーセキュリティBCP訓練

訓練を終えて見えてきた課題

――2回目を終えたばかりですが、サイバーセキュリティBCP訓練を開催した情報セキュリティ統括課からの総括をお願いします。

大澤氏　部長層を中心に、1回目とは異なるメンバーで臨んだ2回目の訓練も、より実務に踏み込んだ有意義なものとなりました。とくにBCP対策のフローやエスカレーションなどが明確になった点は、大きな成果です。また、積極的なディスカッションを通じ、経営に近い層がセキュリティを自分事として捉えていることが可視化されたのも印象的でした。

吉田氏　当部にとっての気づきもありました。1つは情報伝達の仕方です。インシデント発生時に主導する部が曖昧だと、判断が停滞し、初動の遅れにつながりかねません。部署間をつなぐハブとして、当部が情報の集約と発信を担う必要性を強く認識しました。もう1つは、他部で行っている自然災害時の訓練との連携です。BCPの本質は「事業を止めない」ことにあり、サイバーと自然災害は分断して考えるものではありません。今後は両者を横断して整合性を取り、どの事象でも迷わず動ける一貫した対応体制へと磨き上げていきたいと考えています。

当事者意識を引き出した、オーダーメイド訓練の価値

――ラックに対する評価をお聞かせください。

吉田氏　汎用的なシナリオの場合、当事者意識を持ちにくいと考えていたため、事前に綿密な打ち合わせを重ね、自社の業務やシステム構成に即した形へとシナリオをカスタマイズしていただいた点は非常に大きな価値がありました。講師が実際のシステム名や業務の流れを織り込みながら自然に説明したことで、自分たちの現場で起きている事象として具体的にイメージでき、結果として議論の質と深さが一段引き上がったと感じています。実際、それが積極的なディスカッションにつながりました。

また、訓練中に紹介された他社事例も印象的でした。他社事例は「自分だったらどう行動するべきか」といった具合に、自社や自分に置き換えて考えることができるため、しっかり危機意識を持って訓練に取り組めたと思います。講師の柔らかい物腰と実務知見が相まって、終始緊張感と安心感が両立した場となりました。

2回目のサイバーセキュリティBCP訓練で印象的だった積極的なディスカッション

――今後の展開をお聞かせください。

吉田氏　ラックには引き続き、サイバーセキュリティBCP訓練をお願いしたいと考えています。BCP対策のプロセスと意識は店舗営業にも反映させる必要があるため、セキュリティ対策として引き続き教育プログラムを継続するとともに、次年度は地域営業本部長およびブロック長に対しても、サイバーセキュリティBCP訓練を行うことも考えています。また、経営層やCISOも含めた形で全社的に判断軸をそろえ、いざというときに迷いなく動ける体制を構築していきたいと考えています。

また、ラックには訓練にとどまらず、実際のインシデント発生時に即活用できる連絡リストや初動対応チェックリストなど、その場で使える実務的な資産についてもご提案いただけると幸いです。平時の備えを有事の行動につなげるという観点で、引き続き伴走いただけることを期待しています。

［お問い合わせ］
株式会社ラック
サービス紹介ページ
https://www.lac.co.jp/education/course/incident_response_intensive.html
https://www.lac.co.jp/education/course/rw_incident_response_intensive.html
https://www.lac.co.jp/education/course/security_training_executive.html