第 67 回：令和 6 年能登半島地震に寄せて

掲載日：2024 年 1 月 23 日
執筆者：株式会社スクウェイブ
カウンセラー
和田　柊平

はじめに、石川県能登地方で発生した地震により被災された個人並びに事業者の皆様に、心よりお見舞い申し上げる。インフラの復旧も進んでおらず、まだまだ日常生活それ自体が大変な最中とは存じるが、一日も早いご再建をお祈り申し上げたい。

確率論から言えば、1 年のどの日に地震が起きたとしてもおかしくないはずである。しかし、1 月 1 日からこれほど大きな被害を伴う地震が起きるとは夢にも思わなかったというのが率直なところである。改めて、災害大国である日本で生活する限り、もしもの時に備えて防災対策を怠ってはならないことを身に染みて痛感した。

当社では、情報セキュリティに関するコンサルティングを行うことも少なくない。今回の地震について考える中で、防災と情報セキュリティには似ている点が数多くあるということに改めて気づかされた。その中でも類似している重要な点について、PDCA サイクルの観点から 4 つ列挙したい。

1. Plan：災害ないし情報セキュリティインシデントを想定し、リスクアセスメントを講じたうえで、防災やセキュリティ確保のための方針を立案する。企業の場合には、災害やサイバー攻撃によって影響が生じた際に備えて予め事業継続計画（BCP）を立案することで、業績に与える影響を最小限に抑えることが可能である。
2. Do：対策の実施や教育を行う。防災であれば、避難訓練や非常用グッズの確保などがこれに該当する。情報セキュリティであれば、ファイアウォールやウイルス対策システムなどの技術的対策、入退室管理やセキュリティワイヤによる盗難防止などの物理的対策、マニュアルの策定やセキュリティ教育などの人的対策がある。
3. Check：対策の監視や評価を行う。「滞りなく教育・訓練を実施したのだからそれでよし」という事なかれ主義で終わらせず、防災訓練や標的型攻撃メール訓練などについて評価項目を設定し、KPI マネジメントを行うことが重要である。情報セキュリティであれば、情報セキュリティ監査を行うことも有効である。
4. Action：態度や思考の変容、ポリシーや規定・マニュアルの更新、次なる目標の設定等に向けて、主体的に危機対応上の問題点や課題を見つけ出し、改善に結びつける。

このように、災害対策も情報セキュリティマネジメントも、事前の準備によって被害を最小限で食い止めることができるようになるという点や、その対策としてハードとソフトの両方の観点が欠かせないこと、「何もなかったからそれでよし」とはせずにPDCAサイクルを適切に回し続けること、技術や設備などのハードと教育や啓発などのソフトの両面から検討することが必要であることなどが共通しているといえる。

ところで、読者の皆様は、情報セキュリティ対策において、技術的対策、物理的対策、人的対策のどれが最も重要だと思うだろうか？多くの方が情報セキュリティと聞いてまず思い浮かべるのは、おそらくハッカーやウイルスなどではないだろうか。もちろんこうした被害が後を絶たないのは事実である以上、技術的対策の重要性については疑問の余地はない。しかし、台風接近時に田んぼや川を見に行ったりサーフィンに行ったりして亡くなる人が後を絶たないように、実際のインシデントの過半数は、紛失や置き忘れ、誤操作、クラウドの設定ミスなど、人為的なミスに起因している。だとすれば、情報セキュリティにおいてはしかるべき技術的対策や物理的対策をとったうえで最後にはやはり人的対策が肝になると言えるはずだ。

もう少しだけ台風になぞらえて話をしよう。台風接近時にニュース番組や天気予報を見ると、「海や川には近寄らないでください」と繰り返し周知されているはずである。それにもかかわらず海に行く人がいるのはなぜだろうか？もちろん、台風で海がひどく荒れているからこそ、たとえ命を落とすことになってもこのビッグウェーブに挑めるのなら後悔はないという命知らずなサーファーもいるだろう。しかし、おそらく多くの人は、心のどこかに大丈夫だろうという意識があるからこそ、ニュースや天気予報の呼びかけを無視してまで海に出かけるのではないか。

思うに、多くの情報セキュリティインシデントについても同様に、知識はあっても潜在意識に落とし込めていないことが多くのインシデントの引き金となっている。実際に、当社が情報セキュリティ対策の支援を行う中で、多くの企業から「意識向上を図りたい」という声を頂いているのはその証拠といえよう。

震災を契機として、「もしも」の時の備えを見直すべきではないだろうか。それは防災に限ったことではなく、情報セキュリティについても然りであろう。当社では、「情報セキュリティ意識レベル診断：MSIS（Mind Set for Information Security）」というサービスを提供している。当サービスは、心理学分野において、もっとも精度が高い調査法として認められている手法を用いて、情報セキュリティに対する本音を引き出すことができる意識レベル診断サービスであり、診断結果をもとに対策を打つべき対象と対策の指針を提供す

ることができる。また、KPI マネジメント支援や BCP やコンティンジェンシープランの策定や見直しの支援、情報セキュリティ監査も実施している。官民問わず、ご興味を持たれた方は、ぜひお気軽にスクウェイブまでご連絡頂きたい。