■2023/1/24 質疑応答まとめ

・「テレワークにおけるマイナンバー管理の留意点について」

まずは、組織として特定個人情報事務取扱責任者／担当者を明確にして、ルールを整備することが大切です。
会社で取り扱うマイナンバーが多い場合は、やはり専用のマイナンバー管理システムが必要となります。
会社で取り扱うマイナンバーが少ない場合は、ファイルや紙での管理でもかまいませんが、必ず施錠管理が必要となります。
ルールが曖昧でマイナンバーを受領したのに施錠されていなかったとなると、これはマイナンバー管理がなされていないことになります。

・「テレワークで公衆 Wi-Fi を使用させないようにするには」

技術的な対策方法もありますが、人に着目したルールで統制することが基本となります。
テレワーク実施までの手続きの【テレワーク実施の申請と承認プロセスの例】にあるように、二段階の承認プロセスとし、予め安全衛生/セキュリティ等に関する事前確認を行うことが有効となります。
この事前確認のプロセスで、公衆 Wi-Fi を使用しないことについて、社員に具体的な留意点や手順を示して確認させたうえで誓約させることでけん制を働かせることができます。

・「テレワークでどこまでセキュリティ対策が必要なのか」

セキュリティ対策では、完全に守りきるための 100 点の対策はありません。
テレワーク環境におけるセキュリティ・リスクの一例として「情報セキュリティの３要素 CIA」を確認しましたが、テレワーク環境におけるセキュリティ・リスクを、想定される脅威と具体的な脆弱性から洗い出してみましょう。
そして、総務省テレワークセキュリティガイドライン等の適用場面で「セキュリティ対策の優先度の検討」が必要だとあるように、自社のテレワーク環境の現状と改善点を把握し、テレワークのセキュリティ対策として推奨される対策の中から、対処方法を決定していきましょう。

・「個人携帯電話を社用に転用した場合のセキュリティ対策」

個人携帯電話を社用に転用した場合、社用の連絡先を個人携帯電話に登録する必要が生じます。
この場合、個人情報の管理という点からは、個人を特定されないように情報管理する手順を具体的に定めて社員に周知することが大切になります。
例えば、必要最小限の連絡先に限る、連絡先の相手の社名や氏名は A、B、など個人を特定されない記号に限る、一定期間ごとに不要な連絡先を点検/削除し報告を求める、などの情報管理手順が考えられます。

・「社員のセキュリティ意識を高めるには」

組織として留意することは、情報セキュリティ規程の整備と教育訓練です。
社員のセキュリティ意識を高めるには、より実践的な経験が有効と考えられます。
例えば、ご参加の皆様のご心配されておられるメールセキュリティについては、標的型メール訓練を実施されることも有効ではないでしょうか。

・「テレワークの定着に向けた企業の課題のトップに、出社時と比べて職場の人とのコミュニケーションが取りづらいことが挙げられているが、３割の企業が対応済みとのこと。どのような対応が考えられるか。」

テレワークにおけるコミュニケーションは、典型的な課題の一つといえます。
テレワークが普及し始めた頃は、常時、映像システムで仕事の状況を確認できるようにしていた企業もあったほどです。
企業の対応方法としては、まずチャットツールなどのクラウド型のコミュニケーション環境が整備されてきたことから、一つは技術的な対応が考えられます。
また、企業としては技術的な対応以外に、これまで社員との面談といえば定期的な評価面談に限られていたところ、テレワークをきっかけとして 1on1 ミーティングなどの手法を積極的に取り入れて、社員のエンゲージメントの向上を図っていく取り組みが多く見られるところです。

・「テレワークにおいて生産性を向上させるには」

テレワークといえば、時間と場所の自由度が向上することにより知的生産性の向上が期待できます。
一方で、現業などのテレワークが実施できないと思われている業務も存在します。
このような場合でも、例えば前後の業務フローを見直すことによりテレワークでも実施できるといった小単位の業務を特定の曜日に固めることができれば、週一日はテレワークが実施できることになります。
つまり、テレワークをきっかけとして BPR（業務見直し）を行うことが、テレワークを通じて生産性を向上させる一つの重要な取り組みとなるわけです。

以上