■2023/11/28 質疑応答まとめ

・「PC の持ち出しは避けて通れないと思いますが、専用のシンクライアントなどを導入する必要があるでしょうか」

専用のシンクライアントなどを導入するためには、サーバー設備が必要となります。
まずは、PC の持ち出しとデータの持ち出しを分離することが重要です。
持ち出しを許可する PC は、ホワイト PC に限定するなどの運用ルールを明確にすることが有効です。
そのうえで、組織として管理すべき情報を情報資産台帳で明確にし、必ず承認を得てデータを持ち出すようルールを整備することが大切です。

・「PC やデータの保護のために有効な認証アクセス管理にはどのようなものがありますか」

ID やパスワードはそれ自体が漏洩することもありますので、ﾊﾞｲｵメトリクス認証が効果的です。
ﾊﾞｲｵメトリクス認証とは、身体的特徴によって本人であることを確認する方式で、指紋認証などがあります。
?指紋認証、顔認証、静脈認証などの認証機能は普及してきていますので、検討してみてください。

・「Microsoft Defender の他にセキュリティ対策が必要なのか」

Microsoft Defender でも、エンドポイントセキュリティ対策としては効果があります。
ただし、パターンファイルのアップデートファイルが毎日一回～二回提供されているほど、攻撃のパターンは急速に増加しています。
席について PC を操作する際は、まず Windows Update を行うといった、運用の徹底が大切です。
その他にも、AI 技術を活用したセキュリティ製品などもありますので、必要に応じて異なる種類のセキュリティ製品を検討してみてください。

・「役員の事故や社員のフィッシングなど、ひっかかりやすい事故の予防対策として何が有効か」

事故の予防対策としては、教育訓練を行うことが有効です。
特に、実際に起きた事故事例に近い攻撃パターンでの標的型メール訓練などを行うことで、意識を高める効果があります。

・「会社が許可していないシャドー IT の利用を管理するにはどのように行うとよいか」

組織として許可していないシャドー IT は、一般的にインターネット経由で入手し拡散することが多く考えられます。
そのため、インターネットへのアクセスは、会社のイントラネット経由で行うよう限定することで、
UTM 機能による Web フィルタリングなどの対策を有効にすることができます。
また、端末にインストールされたシャドーアプリが存在するかどうかは、インベントリ情報を収集してアラートを出すような
MDM 機能や IT 資産管理機能の製品もありますので、検討してみてください。

・「テレワークで使用している PC の検査は会社として行うべきでしょうか」

ISMS などのマネジメントシステムでは、最低限一年に一回はリスクアセスメントを行うよう PDCA プロセスを回すことを計画します。
このような考え方で、テレワークで使用している PC についても情報システムの管理プロセスを回せるように、
年一回は会社に持参させて検査するよう計画するといった対策が考えられます。

・「初めてクラウドサービスを利用する際に気をつけたほうが良い事は何でしょうか」

クラウドサービスの利用開始にあたっては、２点、気をつけたほうが良い事があります。
一つめは、事業活動で GDPR などの個人情報の移転の制限が問われることも考えられますので、
個人情報を含むクラウドデータの保管場所が日本国内を選択できるクラウドサービスであるかを確認することが大切です。
二つめは、アカウント管理とアクセス権管理を、クラウドサービスにデータを格納し始める前にきちんと設計しておくことが大切です。
あとになってからアカウント管理とアクセス権管理を設計するのでは、データを保護することは困難になります。

・「完全在宅勤務を行う場合に気をつけることはありますか」
テレワークの接続方式で VPN のパスワードを破られた事故事例を紹介しましたが、VPN は接続してしまえば社内ネットワークそのものを扱えるため、
VPN のパスワードの管理は重要です。
また、何らかの暗号化方式で通信を行えるよう、データの管理方法、データの転送方法を限定することも

有効です。

・「サイバー攻撃を受けた場合に、被害を拡大させないために必要なことは何でしょうか」
　サイバー攻撃を受けたりセキュリティ事故が起きたことに気が付いた社員は、速やかに会社の専門部署に報告するように、
　連絡先を持参させることが重要です。
　また、会社の専門部署では、すぐに業務システムやサービスを停止できるよう、予め経営者と相談してルール化しておくことが重要です。

・「IT 担当者が不在ですが、どのような工夫が考えられますか」
　各企業におけるテレワークセキュリティの強化に向けた具体的な取り組み事例でも、社員だけでなく協力会社のメンバーで IT 担当を構成している会社もありました。
　IT 担当を構成できる IT-BPO サービスを提供しているパートナー企業を探しておくことも有効です。
　その他、サイバーセキュリティ保険に加入して初期切り分けを相談できるようにすることや、
　IPA サイバーセキュリティお助け隊サービスを契約しサーバー攻撃を受けた場合の初動対応ができるようにする、などの対策も有効です。

・「メジャーなクラウドストレージサービスで、法人契約と無料の個人ライセンスでの利用では安心できるレベルは違いますか」
　一般的には法人契約でクラウド提供事業者とサポートを含めて責任分界点を明確にしておくことをお勧めします。
　無料の個人ライセンスでの利用は個人としての利用許諾の範囲に限られることからビジネス上のサポートは期待できないと考えられます。
　安心できるレベルの違いについて、具体的な回答はいたしかねます。

以上