≪体制整備の豆知識 Part9≫　　2025.5.21

ふうたのワンポイントレッスン

Vol.11　昨今のサイバー攻撃を踏まえた適切なセキュリティ体制および攻撃を受けた際の事業継続計画

今月は「昨今のサイバー攻撃を踏まえた適切なセキュリティ体制および攻撃を受けた際の事業継続計画」についてご説明します。

保険代理店が直面するサイバーリスクは年々高度化・巧妙化しており、特に**個人情報**や**財務情報**などの機微情報を扱う業態として、高度なセキュリティ体制と事業継続計画（BCP）が不可欠です。以下に、現在のサイバー脅威に対応した**適切なセキュリティ体制**と、**サイバー攻撃を受けた際の事業継続計画のポイント**を整理してご説明します。

1. 現在想定されるサイバー攻撃の主な種類

◯保険代理店が警戒すべき攻撃手法：

- **ランサムウェア攻撃**：システムやデータを暗号化し、解除と引き換えに金銭を要求。
- **フィッシング詐欺**：偽メール等で ID・パスワード等を窃取。
- **標的型攻撃メール**：特定の個人や企業を狙った偽装メール。
- **内部不正・誤送信**：従業者のミスや故意による情報漏えい。
- **脆弱なシステムの悪用**：ソフトウェアの未更新や設定ミスによる侵入。

2. 適切なセキュリティ体制の構築

◯技術的対策

- **EDR（Endpoint Detection and Response）やウイルス対策ソフトの導入。**
- **多要素認証（MFA）の実施。**
- **定期的なソフトウェア・OS のアップデート。**
- **メールフィルタリングの強化。**
- **VPN の適正利用とリモートアクセス管理。**

◯組織的対策

- **情報セキュリティ基本方針の策定と周知。**
- **「秘密情報管理ガイドライン」等のマニュアル整備。**

・ **アクセス権限管理の明確化と最小権限の原則の徹底。**

・ **外部業者（委託先）へのセキュリティ確認・契約の明文化。**

◯人的対策

・ **従業者向けの定期的なセキュリティ教育。**

・ **不審メールの見分け方や通報フローの教育。**

・ **情報漏えい時の報告義務・罰則の明確化。**

3. サイバー攻撃時の事業継続計画（BCP）のポイント

① 事前準備（平時の備え）

・ **事業継続計画書（BCP）の策定**

サイバー攻撃を含む各種リスクに対する対応策を網羅。

・ **データの定期バックアップ**

社外クラウド等、攻撃されない別環境に保存。

・ **連絡網の整備**

社内・取引先・保険会社への緊急連絡体制を整備。

・ **訓練の実施**

サイバー攻撃を想定した対応訓練（机上・実動）を定期実施。

② 発生時の対応

・ **初動対応マニュアルに基づく対応。**

機器のネットワーク遮断、ログ収集、被害範囲の特定。

・ **専門機関（警察・サイバーセキュリティ事業者・保険会社）への連絡。**

・ **情報公開の判断と対応（法令対応、顧客説明）。**

③ 復旧・再発防止

・ **システム復旧（バックアップからのリストア）。**

・ **原因調査と脆弱性対策。**

・ **対応記録の整理と関係者へのフィードバック。**

・ **再発防止策の強化（教育強化、システム強化等）。**

4. 保険代理店に特化した留意点

・ **個人情報保護法・金融庁ガイドラインへの適合**

保険業法上の「委託元（保険会社）」との契約に基づく情報管理義務。

・ **保険会社からの委託に伴う情報セキュリティ評価の対象**

自主的に FISC 安全対策基準や ISMS 認証の取得も有効。

- **サイバー保険の活用**

  サイバー攻撃による損害補填・専門家費用の補償など、BCP の一環として検討。

作成 ： 日本代協アドバイザー　日本創倫株式会社
専務執行役員　事業推進室長(SEO)　風間　利也
配信 ： 日本代協事務局