サイバー対策

◆現状・問題点（わからないが多すぎる）

・狙われる所、脆弱性、防御方法等ほとんどがわからないことばかり。
・攻撃手法の変化が激しく、従来の防御技術では対抗できない。
・セキュリティ専任担当者、対応システムの導入費用の制約がある。
・従業員へのセキュリティ教育の実施も 100%防御は不可能で限界がある。
・言葉の壁で相手の要求がよく理解できない、まして交渉もできない。
・攻撃を受けた時、どこに連絡・依頼するのか、どう対応するのかわからない。　等々

◆一般的な対策

① バックアップ（必須）
② 識別　資産等を環境を考慮して管理・特定
③ 防御　認証やアクセス制御、組織的な保守・対策
④ 検知　攻撃を事前に検知できれば防御可能
⑤ 対応　攻撃対して求められる対応策
⑥ 復旧　事業を継続させるために早期復旧
（②～⑥は米国国立標準研究所が公開したサイバーセキュリティフレームワークより）

◆サイバー攻撃からの損失回避（サイバー対策の最優先事項）

サイバー攻撃による企業の損失と対策
① **身代金**　データのバックアップがあり復旧できれば不要
　防止策は、**有効なデータバックアップ**
② **対応費用**　フォレンジックや交渉費用、見舞金や賠償金等
③ **復旧費用**　侵入の原因を取除きアプリやデータを再設定、ＢＣＰとしても重要
④ **休業損失**　システムを再稼働できるまでの遺失利益
　②③④は以下の理由で**サイバー保険**が有利です

・対応は専門性が高く、費用的にも普段から準備・契約しにくい。
いつ発生するかわからないサイバー攻撃に備えて、調査費用や対応費用などをあらかじめ予算に組み込むのは難しい
・サイバー専門業者に依頼することで対応時間が短縮できる可能性大。
（一般的には時間が短く済めば、対応費用も休業損失も安くなる 早期復旧）
・必要に応じて複数の専門業者の手配とその費用の支払いを確保できる。
事故の調査やリカバリー対応を躊躇なく迅速に開始することができ、被害の深刻化を防止することが期待できます。
・保険は費用対効果がよく、契約すればすぐに効果が出る即効性がある。

◆資料

サイバー保険の機能

・初期対応・調査　フォレンジック等
・事故対応　必要に応じて　広報サービス、サイバー恐喝対応、コールセンター設置、クレジットモニタリング、見舞金賠償金等の支払い、弁護士相談費用
・データ復旧費用
・事業中断費用

識別、防御、検知

・**メールシステムを含めクラウド化**
クラウドシステムは継続的なアップデート等により、セキュリティが継続的に強化されながらユーザーにとっては簡素化されていく。
・**認証システムの最新化**、パスワードの強化・パスワードレス認証
・ウイルス対策ソフトの導入、基本的な予防策の教育
・ＯＳやアプリ、ネットワーク機器のファームウェアを最新版にアップ
・ＵＴＭ、ログ管理システム等の導入、脆弱性診断、セキュリティ診断　など

有効なバックアップ（サイバー対策と災害・BCB 対策として）

・社内ネットワークから完全に切り離すか、消去変更できない装置を使用
・別の場所へ複数のバックアップ

ＶＰＮ等のネットワーク機器

・最近のランサム被害の多くは、この部分の脆弱性を狙われている。
・リースや貸与になっていてコントロールできず、ファームウェアのバージョンアップもできていないことが多い。また勝手に手を入れるとシステムメンテナンス対象外になる場合も。

メール対策（サイバー攻撃の 9 割以上はメール経由）

・サイバー攻撃の主な入口となるメールに、信頼できるクラウドメールを使う。
・信頼できるクラウドメールの迷惑メールフィルターはかなり優秀。
・そもそもクラウドメールはブラウザーに表示しているだけで、添付ファイルのダウンロードをしない限りパソコンには入らない。

閉域網

・完全でなくメンテナンス回線が開いている例が大半で、そこから攻撃を受ける。
・閉域網で安心と、OS やアプリ、パッチが最新版になっていない事が多い。
・完全な閉域網の場合は大規模でメンテナンスに多額のコストがかかる。

ＢＣＰ

・サイバー攻撃に関わらずＢＣＰとして最も重要なことは、災害などが起こったときに必要になってくる復旧資金の確保となります。これを確保する手段としては、保険が一般的に最も費用対効果の高い手段と考えられます。