SOMPO CYBER SECURITY

サイバー攻撃想定（机上・実機）訓練

近年、標的型攻撃メールやWebサイトの改ざん等のサイバーセキュリティ事故が後を絶たず、サイバーセキュリティ態勢の強化は喫緊の課題といえます。一方で、サイバーリスクにどのように対応すればよいか、また、サイバーリスクに対してどのように進めればよいかといったお悩みをお持ちの企業も増えています。

❶サイバー攻撃対応の必要性

貴社のサイバーセキュリティ態勢は大丈夫ですか？

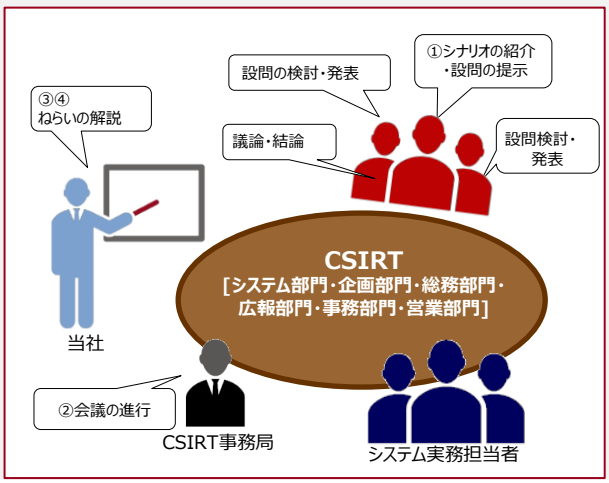
- 事故対応態勢は作ってみたものの自信がない
- CSIRTや事故対応態勢をこれから整備したいが何を検討すべきか不明
- サイバー攻撃への対応経験がなく、実際に事故対応態勢が機能するか不安・・・・・など

❷ご提案内容

サイバー攻撃想定訓練

経営者層、情報セキュリティ担当者、危機管理担当等を訓練参加者とし、サイバーセキュリティ事故を想定したシナリオでインシデント対応を確認し、課題抽出していくサービスです。

①訓練の企画	● 訓練の目的、訓練形態、参加者、訓練シナリオ等の明確化 ● 訓練時に用いる各種資料の作成支援
②訓練の実施	● 事前説明会等の実施 ● 訓練当日の支援、講評
③訓練の評価 課題整理	● 訓練報告書の作成 ● 訓練評価（チェックリスト）取りまとめ
④訓練結果の反映	● 課題に対する対策の実施プラン作成・アドバイス



❸訓練内容

訓練	内容
サイバー攻撃想定 机上訓練	経営層、情報セキュリティ担当者、危機管理担当者等を訓練参加者とし、サイバーセキュリティ事故を想定した検討シナリオに準じ、自社の対応を時系列で検討する机上の訓練です。
サイバー攻撃想定 実機訓練	仮想企業の訓練環境を再現し、その訓練環境内でサイバー攻撃を受けた場合に求められるログ解析等による原因究明・封じ込めや、社内外の調整、仮想企業における事業の継続等を検討する体験型の訓練です。

ＳＯＭＰＯリスクマネジメント株式会社
サイバーセキュリティ事業本部
〒160-0023
東京都新宿区西新宿一丁目24番1号
TEL：0120-211-180　E-mail：cyber@sompo-rc.co.jp
URL:https://www.sompocybersecurity.com/