Innovation for Wellbeing
SOMPOリスクマネジメント

サイバー攻撃を想定したＢＣＭコンサルティング

民間企業等のなかには、サイバーセキュリティ対策について、侵入防止の技術的対策だけを重視したりサイバー攻撃が組織のシステム部門のみで対処すべき取組みであると認識することが多く、サイバー攻撃を受けた後の全社的な危機対応・事業継続の観点を十分に考慮できていないケースもあります。

このような状態を改善するため、当社が持つ災害を想定したＢＣＭコンサルティングのノウハウおよびサイバーセキュリティの技術ソリューションと両面を活かして実効性の高いＢＣＭ構築を支援します。

❶サイバー攻撃を想定したBCPの必要性

IoTデバイスがサイバー攻撃を受けた場合、システムやネットワークの障害にとどまらず、事業中断に陥ることも懸念されます。

しかし企業では･･･

- 侵入防止策は十分に実施している。
- 対策はシステム部門所管であり、BCPは関係ない。
- コンティンジェンシープランを策定しているから大丈夫。
- 漏洩して問題となる機密情報は取り扱っていない。

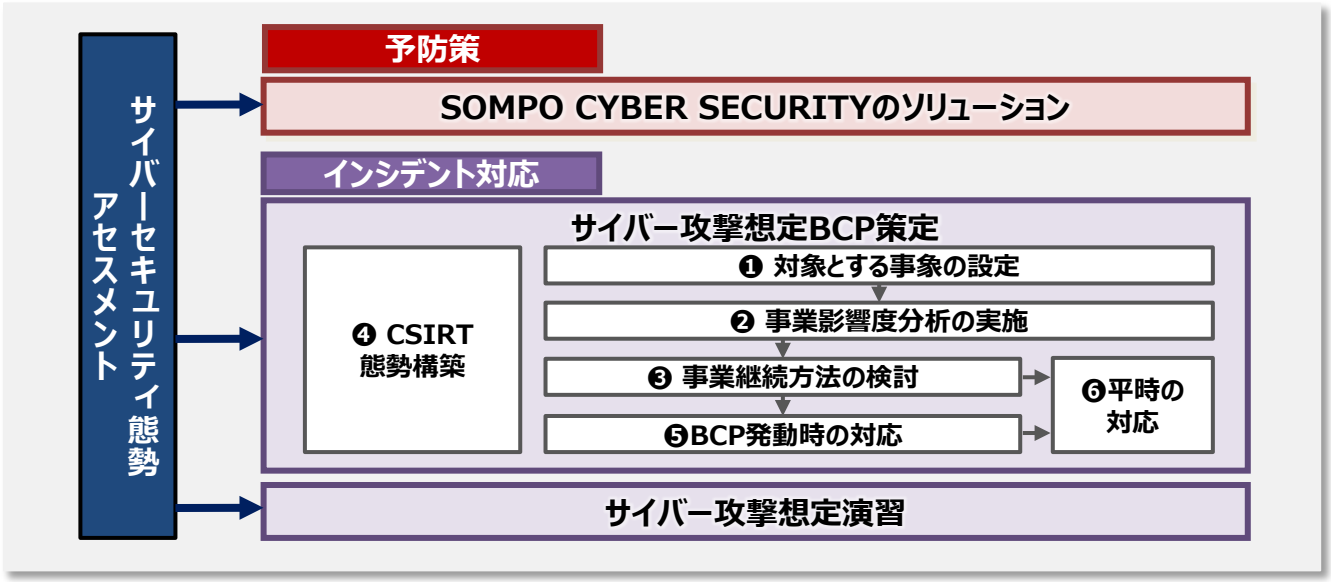
このような声をよく聞きますが大丈夫でしょうか？

サイバー攻撃を完全に防御することは難しいため攻撃を受けることを前提に、全社的な危機管理体制の構築およびBCP策定･演習が必要不可欠

❷災害BCPとサイバー攻撃想定BCPの違い

	災害ＢＣＰ	サイバー攻撃ＢＣＰ
BCP発動	気が付く	気が付かない
前提条件	行政等が公表しているハザード情報	攻撃手法が日々進化するため条件設定が困難
対策本部(事務局)	事務局は、企画部門や総務部門	事務局は、システム･セキュリティ部門
世の中の被害	インフラや企業が面的に停止	なし（加害者的立場となる可能性あり）
自社の被害	建物、設備、人、システム等	ネットワーク、システム、データ 等
重要業務	人命、お客様、自社経営のための必要最小限の業務	お客様、自社経営、法令順守のための業務（災害よりもお客様要求が厳しい）

❸コンサルティングの全体



SOMPOリスクマネジメント株式会社
事業開発部 クロス･ソリューショングループ
〒160-0023 東京都新宿区西新宿1-24-1 エステック情報ビル
http://www.sompo-rc.co.jp