3. サイバー攻撃による想定事故例

業種	攻撃種類	事故内容	主な想定被害額
製造業	IoT(※)機器に対するサイバー攻撃	自動車部品メーカーAで、インターネットに接続された機械が不正アクセスを受け、システムがオフラインとなり、生産ラインが12時間停止した。	原因調査費用:約1,000万円 喪失利益　:約5,000万円
教育機関	標的型攻撃による情報流出	B大学は、標的型メールによる不正アクセスを受け、個人情報が流出。職員がウイルスに感染した添付ファイルを開封したことで、不正アクセスが発生し、感染した端末より個人情報を抜き取られた。同様のメールは複数の職員に送られていた。	原因調査費用　:約800万円 ウイルス除去費用:約300万円
小売業	ウェブサイトの改ざん	食品販売業者Cのサーバーが不正アクセスを受け、一部サイトが改ざんされた。閲覧者は、意図しない第三者のサイトに誘導され、誘導先のサイトでウイルスに感染させられた。	損害賠償金　:約1,000万円 システム復旧費用:約800万円 弁護士費用　:約300万円 謝罪広告費用　:約200万円
製造業	DDoS(※)攻撃	衣料品メーカーD社は、DDoS攻撃を受け、4日間WEBサイトを停止した。	システム復旧費用 :約400万円
サービス業	企業内部の不正行為	ATMの保守管理業務を受託しているE社の元従業員によって、ATMの取引データから顧客のクレジットカード情報を不正に取得され、偽造キャッシュカード作成・保持されていた。	損害賠償金　:約700万円 モニタリング費用:約200万円
物流業	不正アクセス	物流業者Fが不正アクセスを受け、クレジットカード情報が流出。決済代行会社から連絡を受けて、社内と第三者機関で調査を行った結果、クレジットカード決済利用者1,000件近くの情報が、外部に流出していた。	損害賠償金:約3,000万円 見舞品費用:約100万円 弁護士費用:約200万円

(※)DDos … 相手方の通信機器等に大量のデータ等を送りつけてシステムを正常に稼働できない状態に追い込む攻撃手法のこと。

(※)IoT・・・コンピュータなどの情報・通信機器だけでなく、世の中に存在する様々な物体(モノ)に通信機能を持たせ、インターネットに接続したり相互に通信することにより、自動認識や自動制御、遠隔計測などを行うこと。