

リスク管理

9月11日である。6年前のこの日をきっかけに世界のリスクマネジメントは、その中心的課題に事業継続計画(BCP)とセキュリティという項目を加えた。



それらは、外部からのテロ攻撃等で事業中断せざるを得ない状況下であっても、その経営にかかわる影響を自らの許容範囲に抑えるためのBCPであり、もう一つは、意図を持った他者からの企業への攻撃への対抗策、つまり個別企業のセキュリティ対策である。

BCPは、このリスクマネジメントABCシリーズでも以前詳述したが、国際的には、9・11の事件をきっかけに米国の金融業を中心に、いわゆる情報オリエンテッドな業種において特に

リスクマネジメント

ABC

9・11の教訓 BCP

01年9月11日の世界貿易センタービル(ブルームバーグ)



そのものが危うくなる可能性を自覚し、対策を講じてきた。それは、従来のリスク対策の中でも最も基本的・保守的で、高コストとなるリスク回避(Risk Avoidance)であった。テロ活動を象徴とする人の意思にかかわるリスクに対しては、結局は、同じ機能の施設を複数設置し被害を最小化するという方策が単純であつても最も有効であるといつことである。

た。意図を持った他者の攻撃は、それが実行された後では、損害の回復を満足できるレベルまで行うことが出来ない場合がほとんどである。

したがって対策はそのような行為をしようにしても攻撃をさせない仕組み、壊滅的被害に遭わないような方策の事前準備、起こってしまったことを前提にした方策等が主流となる。重要拠点

取り組まれてきた。これらの業種では、顧客情報、トランザクション情報の喪失が、その後の事業に決定的なダメージを与える恐れがあり、経営と

もう一つはセキュリティについてである。人を介しての不正、破壊行為等への対策として、わが国においても、ようやく従業員、取引相手に対する背景調査(スクリーニング)、施設・設備の脆弱性調査等を踏まえてセキュリティ対策の重要性が認識されてき

減に向けた対策も考えなければならぬであろ

未然防御の確立が重要

(日本総合研究所)