KPMG
cutting through complexity

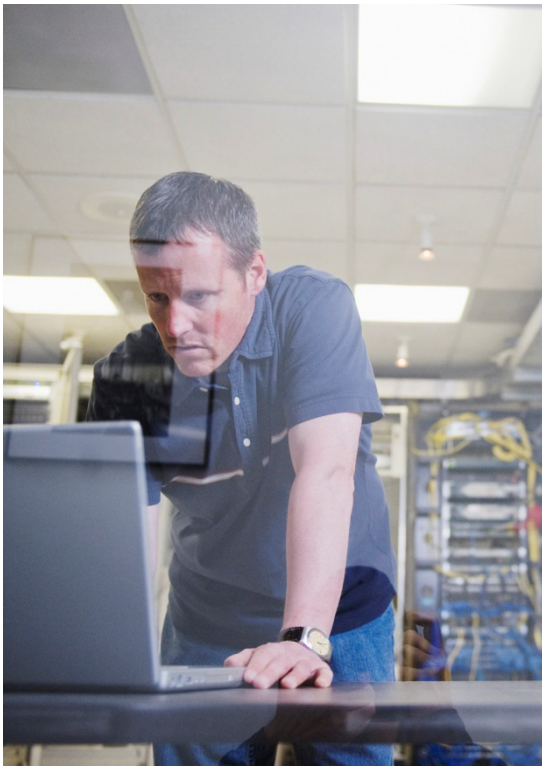
2013年8月

情報セキュリティインシデントに備えるBCMの整備

企業が運営するインターネット上のコミュニティサイトに不正侵入されて会員情報が漏洩したり、内部の人間による個人情報の不正搾取が発生するなど、企業のビジネス活動そのものが中断あるいは部分的に停止せざるを得ない事態へ発展する事例が後を絶たない。企業は継続的にその対策を進めなければならないが、必要な対策は多岐に渡り、何をどこまでやれば良いか悩んでいる企業担当者も多い。

これまではいかにしてこの様な事態を発生させないようにするか、その視点に立った対策が主であったと考えるが、日々進化し、巧妙化・多様化する手口に対して先手を打って防御策を施すのは現実的ではなく、標的型のターゲットとなった場合、その攻撃を防ぎきるのは極めて困難といえる。

本稿では、この様な状況下において、情報セキュリティリスクの顕在化（情報セキュリティインシデントの発生）は、どの企業でも発生し得るものとして考え、発生時の混乱を最小限に抑えつつ早期に事態を回復させるためにBCM[1]の対象として情報セキュリティリスクを改めて捉え直し、その体制整備におけるポイントを解説する。



1. 企業のBCPにおける情報セキュリティリスクへの対応状況

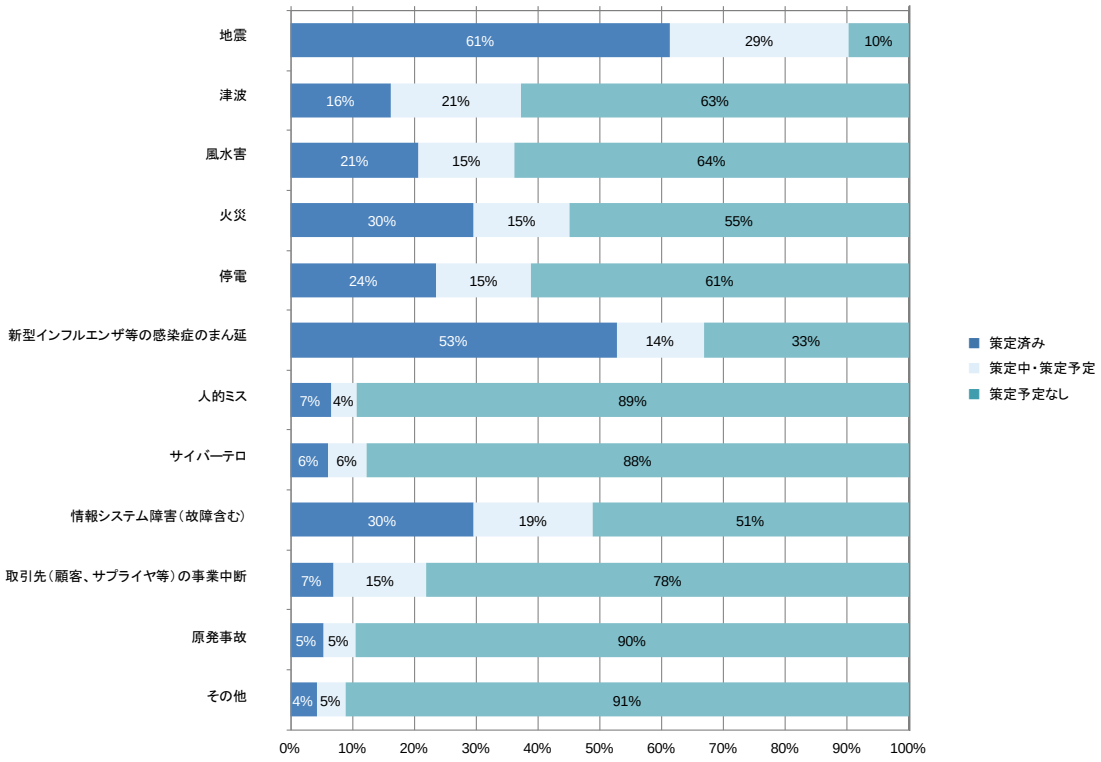
KPMGが2012年に行った事業継続マネジメント（BCM）サーベイ2012（以下、BCMサーベイ）によれば、国内企業におけるBCP[2]の必要性の認識が高まり、77%の企業がBCPを策定済み、17%が策定中・策定予定であるとの回答を得ている。

また、次ページの図表1に示す通り、リスク別のBCP策定状況としては地震が61%と最も多くなっており、前回の2010年の調査から2年が経過する間に東日本大震災が発生し、多くの人々が実体験をもって改めて事業継続の重要性、必要性を考えさせられたことも、この調査結果に影響を及ぼしているものと推測される。続いて、新型インフルエンザなどの感染症のまん延が53%、情報システム障害（故障含む）が30%、その他津波、風水害、火災、停電などの回答を得た。これは実際に事業中断に繋がった原因としてあげられた回答とほぼ類似の傾向を示しており、経験を通じてBCPを策定・改善してきているといえる。ただ、新型インフルエンザなどの感染症のまん延について事業中断の原因として回答した企業は0%であったにも拘わらず、多くの企業がBCPの対象リスクとして捉えその策定を進めてきているのは、その発生可能性が高く、実際に発生した際の影響が大きいとの危機意識があるからと考えられる。

1 BCM：Business Continuity Management（事業継続マネジメント）

2 BCP：Business Continuity Plan（事業継続計画）

【図表1】リスク別のBCP策定状況（複数回答）



新型インフルエンザなどの感染症のまん延と同様に高い危機意識を持って取り組むべきリスクとして、最近では特にサイバーテロ等の情報セキュリティリスクが注目されている。上記のBCMサーベイではサイバーテロを対象としたBCPの策定を行っていると回答した企業は6%、策定中を合わせても12%であり、88%の企業が策定予定なし、と回答している。実際に多くの企業が不正侵入などによる被害を受けている昨今の状況からすると、サイバーテロを含む情報セキュリティリスクへの備えは不足しているものと考えられる。

2. 情報セキュリティリスクへの対策の種類

企業のインターネット上のサイトへ不正に侵入するための手段や、サイトの機能を妨害するためのDDOS（Distributed Denial of Service）攻撃等の手法、巧みに内容を装ったメールに添付されたコンピュータウィルスによる操作方法など、情報セキュリティを脅かす手口は日々進化を遂げながら多様化している。実際に情報セキュリティリスクの顕在化によって、事業の中断や場合によってはビジネスそのものを取りやめざるを得ない事態にまで発展した事例も数多く存在している。企業の経営者にとって、他人事ではなく自社においても十分に発生し得るリスクである事の認識を改めて持つ必要がある。

ひとたび情報セキュリティリスクが顕在化してしまうと、社会的な信用を棄損するだけではなく、お客様へのお詫びや状況説明のために多くの従業員を振り分けなければならず、さらに原因追究や被害の拡大を防止するために情報システムを部分的に停止せざるを得ない事態に発展する可能性がある。この様な事態においては、もはや通常通りの業務を遂行する事は困難であり、経営判断によるBCPの発動を経て、限られたリソースの中で優先すべき最小限の業務を遂行しつつ、同時に緊急対応としての原因分析、被害範囲の特定、被害拡大の防止に向けた暫定対処、社内外に対する報告・情報公開を行う必要がある。

情報セキュリティリスクへの対策としては、これまでにもファイヤウォールの導入やシステム上のアプリケーションプログラムによる対策（セキュアコーディングの実施等）、ウィルス対策ソフトウエアの導入などの様々な予防的な対策が行われてきた。だが、これらの予防的な対策だけではなく、情報セキュリティリスクが顕在化した状態（セキュリティインシデントの発生）を早期に発見するための発見的な対策と、発生後に適切な対応を行う事で事態を安定化させるための回復的な対策の充実が急務である。発見的な対策としてはシステム上の様々なログを一元的に管理し、その相関関係を分析する事で異常を検知するツールや仕組みが有効である。また、回復的な対策としてはBCPの対象として情報セキュリティリスクを捉え、緊急対応の仕組みと優先業務を遂行するための仕組みを整備し、訓練を通じて組織へ浸透させていく事が有効である。

3. 態勢整備のポイント

情報セキュリティリスクに対するBCPの策定や体制としてのBCMの整備においては、組織内CSIRT（Computer Security Incident Response Team）の考え方が参考になるであろう。JPCERTコーディネーションセンターから公表されているガイドラインによれば、情報セキュリティ上の危機管理体制に求められる機能を次の通りに整理している。

【図表2】情報セキュリティ上の危機管理体制に求められる機能

	脆弱性対応	脆弱性情報の収集、影響分析、パッチ適用
	緊急対応	危機発生時の通報受付、対応方針決定、問題解決
	事象分析	データ分析による原因追究、再発防止策の検討
	普及啓発	従業員向けの教育・啓発活動
	注意喚起	被害拡大の防止に向けた関係先への注意喚起
	その他インシデント関連業務	対処計画の確認に向けた演習の実施など
緊急対応	モニタリング	事象の検知、報告受付
緊急対応	トリアージ	事実確認、対応の判断
緊急対応	インシデントレスポンス	分析、対処、エスカレーション、連携
緊急対応	リスクコミュニケーション	報告・情報公開

出所：有限責任中間法人 JPCERT コーディネーションセンター「経営リスクと情報セキュリティ～CSIRT：緊急対応体制が必要な理由～」（平成20年12月）を基に著者作成

緊急対応におけるトリアージの中で行われる対応の判断は、経営者自らが行う必要がある。先述のとおり、事態によっては表面的には正常に稼働している情報システムを部分的に停止させ、情報セキュリティインシデントを発生させた原因の追及や影響範囲の特定のための作業を行わなければならず、社内外へ大きな影響を及ぼす判断をしなければならないからである。また、同様にインシデントレスポンスの際においても経営者の関与を欠かす事はできない。情報システムに関わるからといってシステム部門だけに任せるのではなく、経営者の下でリスク管理部門が中心となり、経営企画部門、総務部門、業務部門が集い、刻々と明らかになってくる情報を分析し、都度適切な対応を行っていく必要がある。

実際に情報セキュリティインシデントが発生した際に、これらの緊急対応を円滑に機能させるためには、正常時から繰り返し訓練を重ね、組織の中へ浸透させていく地道な取組みが欠かせない。情報セキュリティに関しては複雑な情報システムの仕組みや難解な技術用語によって抵抗感を抱く経営者も多いかもしれないが、ビジネスの基盤として情報システムは欠かすことができず、組織に存在する様々な情報の活用が経営戦略にとってますます重要になってきている状況において、その裏に潜むリスクへの対応も経営者の責務として認識を高め、十分な備えが整備される事が望まれる。

KPMGビジネスアドバイザリー株式会社
シニアマネジャー　山下 雅和

KPMGビジネスアドバイザリー株式会社

東京本社
〒100-0004
東京都千代田区大手町1丁目9番7号
大手町フィナンシャルシティ サウスタワー
TEL ： 03-3548-5305
FAX ： 03-3548-5306

名古屋事務所
〒451-6031
名古屋市西区牛島町6番1号 名古屋ルーセントタワー
TEL ： 052-571-5485

ba.kpmg.or.jp