ASIS インターナショナル日本支部
広報担当理事　長瀬　泰郎

ASIS インターナショナル日本支部便り

2 月度月次ｾﾐﾅｰ　「BCP の概要」

2009 年 2 月の月次セミナーでは、世界で最も大規模なセキュリティ専門家国際団体である ISSA（Information Systems Security Association）の東京支部長、米澤一樹氏を講師に迎えました。氏は金融機関とコンサルティング会社で BCP（事業継続計画）と情報セキュリティ対策に関わっています。以下は、米澤氏講演の概要です。

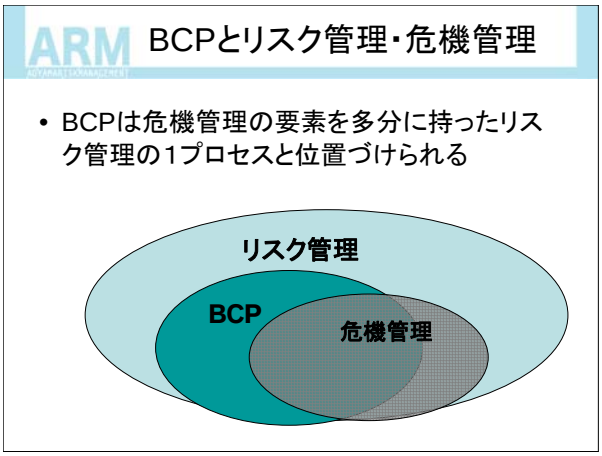
講演する米澤一樹氏

■ リスク管理、危機管理、BCP

BCP（ Business Continuity Plan）は、「事業継続計画」のことです。「不測の事態に際して、事業を継続するための計画」と定義されます。

BCP に関係する言葉に、「リスク管理」と「危機管理」があります。「リスク管理」とは、潜在的な危険（リスク）の存在とその頻度・影響度を認識して平時から必要な対策を施すことです。一方、「危機管理」とは、平時の調査研究をベースに、危機発生時に速やかに効率よく対応し、早い復旧を期すための管理です。したがって、「リスク管理」は、「危機管理」より広い概念といえます。「危機管理」は「リスク管理」の中の一つのプロセスです。

BCP では、事業の継続に影響を及ぼすリスクが顕在化したときの危機を対象にしています。ここでいう危機とは、緊急事態、食品衛生問題、犯罪、テロ、戦争、不祥事など、俗に純粋リスクと呼ばれるものです。この危機がもたらす事業プロセスへの影響を最小限に抑えるための計画です。BCP、「リスク管理」、「危機管理」の関係は次の図のようになります。



BCP とリスク管理・危機管理

■ BCP のプロセス

BCP では、まず「ビジネスインパクト分析」を行います。ビジネスプロセスの流れを整理し、その中の各ステップの重要度を評価します。続いて、次の図に示すように、これらのプロセスやステップに対して起こり得る潜在的なリスクを洗い出します。

リスクの洗い出し

- **起こり得る危険（潜在的なリスク）を周囲の環境から予測して洗い出す**

1. 過去の経験より・・・
2. 歴史上の事実より・・・
3. 過去の傾向より・・・
4. 他者の事例より・・・
5. 条件を特定してシナリオを組み立てて・・・
6. 数学的理論（ゲーム理論など）によって・・・
7. 今に潜む予兆より・・・
8. 実際にロールプレイしてみて・・・
9. 専門家に聞いて・・・
10. 時には勘にも頼り・・・

リスクの洗い出し

次に、洗い出したリスクについて、事業に与える影響の大きさとその頻度によって分類します。

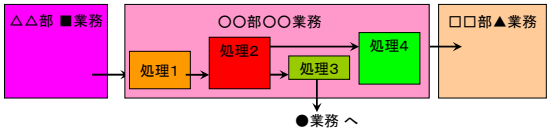
ビジネスインパクト分析（1）

- ビジネスの流れにおける各ステップの重要度と中断時の影響を洗い出す
- 中断時の影響の大きさやRTO・RPOに基づいて優先順位を決める

業務	業務ステップ	重要度	担当要員	RTO	RPO	前工程	後工程	予想損失
○○部○○業務	処理1	High		4H	4H	△△部■業務	処理2	大
	処理2	Middle		12H	24H	処理1	処理3、4	中
	処理3	Low		12H	24H	処理2	●業務	小
	処理4	High		24H	72H	処理1、2	□□部▲業務	大

ビジネスインパクト分析（2）

業務	業務ステップ	重要度	担当要員	RTO	RPO	前工程	後工程	予想損失
○○部○○業務	処理1	High		4H	4H	△△部■業務	処理2	大
	処理2	Middle		12H	12H	処理1	処理3、4	中
	処理3	Low		12H	24H	処理2	●業務	小
	処理4	High		24H	24H	処理1、2	□□部▲業務	大

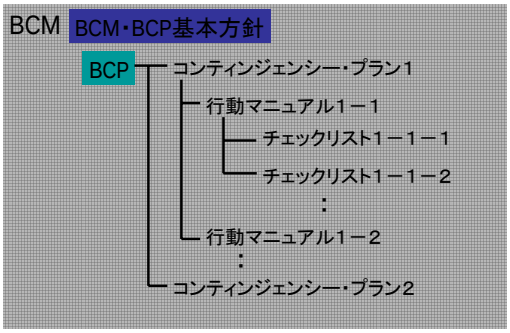


ビジネス・インパクト分析

この後、ビジネスの流れにおける各業務ステップの重要度と、それが中断したときの影響を洗い出します。そして、RTO（業務が復旧するまでに許される時間）や RPO（業務復旧時点に必要とされるデータ類）なども組合せて、中断時の損害の大きな業務を優先的に対策する方針を作ります。当然、この決定には、経営層が参画することが欠かせません。

以上で決定した方針に基づき、BCP 計画を策定します。基本計画書を作成し、コンティンジェンシープラン、行動マニュアル、チェックリストなどを整備します。行動マニュアルやチェックリストは、分量が少なく、また、読み違いがないようにすることが大事です。計画そのものも、精緻になり過ぎないように注意することが必要です。

BCP計画の構成例



BCP 計画の構成例

策定された BCP 計画は、テストと訓練によってその有効性を確認する必要があります。これは、実際の業務担当者が実際の業務環境の中で、特に平日の業務時間内に行うことが大事です。この結果を検証して、必要に応じて計画の見直しを行います。

往々にして、「やった」という満足感によって、未解決のまま放置された問題の存在を忘れさせてしまうことがあります。「一度やって終わり」は、いちばん悪いパターンです。「終わり」のポイントを「訓練とテストの終了」ではなく、「結果の検証と対応の終了」にすべきです。

BCP では、関係者だけではなく、組織の構成員全員が当事者として取り組む土壌を形成することが重要です。また、BCP 関係者への一種の特権付与

や優先度の高い部門への傾斜的予算配分を容認することも肝要です。

■ 国内外の動き

BCP は、1990 年代から欧米で意識され始め、2001 年の 9.11 を機にガイドライン等が各国で発行されるようになりました。アジアではシンガポールが積極的に普及を図っています。

日本では 1995 年の阪神淡路大震災後、注目され、2007 年の中越沖地震でさらに全国的に知られるようになりました。内閣府、経済産業省、中小企業庁によるガイドラインも整備されています。

ARM 各省庁のガイドライン比較

発行元	名称	対象リスク	内容
内閣府	事業継続ガイドライン	災害による事業中断	方針と方法論
経済産業省	事業継続計画策定ガイドライン	情報システムの使用不能、及び、情報セキュリティ・インシデント	方針と方法論
中小企業庁	中小企業BCP策定運用指針	事業中断をもたらすあらゆるリスク	方針と方法論、テンプレートとチェックリスト

各省庁のガイドライン比較

米澤氏は、現在の BCP が、もっぱら大災害対策や大規模システムダウン対策の延長上で捉えられていることについて、「どうしても準備が大掛かりになり、頑張って対策しても、そこで力尽きてメンテナンスがおろそかになるケースが多い」と感じており、「できることから始める」のが現実的な対策の一歩ではないか。例えば事業所の火災対策は BCP の第一歩として最適な対策の一つではないか。キーパーソンが突然いなくなる場合の対策を考えることも、業務の属人化を防ぐ効果があると述べて講演を締めくくりました。

ASIS インターナショナル日本支部の月次セミナーへのお誘い

ASIS インターナショナル日本支部は、月次セミナー(「セキュリティミーティング」)を開いています。産業セキュリティに興味がある方ならどなたでも参加できます。お申し込みはホームページから！

■ 開催日

毎月第三火曜日　午後 6 時半より

■ 場所

日本支部のホームページでご確認ください。
www.asis-japan.org

■ 参加費

2,000 円(ASIS 会員・非会員同一料金)

また、1 月からは、世界的に有名なセキュリティ専門家資格、CPP、PSP の受験を目指す人々が集まって開くスタディグループが発足しました。

一定以上の受験希望者が集まれば、日本国内での受験が可能になります。

興味のある方は、日本支部ホームページをご覧ください。

このコーナーへのお問い合わせや入会お申込みは
ASIS インターナショナル日本支部　事務局まで

〒101-0021　東京都千代田区外神田 2-2-17
日本保安人事株式会社内
TEL　03-3255-3468　　FAX　03-3258-7630
E-Mail info@asis-japan.org
www.asis-japan.org