

1	<p>①BCPは、ERMの1要素になると考えているが、ERMに関する今後の制度化や、規格化などの動きについて教えていただきたい。</p> <p>回答： BCPがERMの1要素になるというのはひとつのあり得る考え方ですが、まだ両方の分野とも方法論や規格化の発展途上の段階ですので、すっきりとは整理されている訳ではありません。このような状況でERMに関しましては、様々な方法論がありますが、リスクマネジメントそのものについての標準化はISOで31000シリーズとして具体的に開発が進んでおり、2009年10月にはガイドライン規格として公開される予定です。最新状況につきましては講演でも触れさせていただきました社会セキュリティの規格化の議論を進めているISO-TC223の状況と併せて、日本規格協会のサイトなどでご確認ください。</p> <p>②BCPの従来手法では、経済リスクに対して十分対応できそうにないが、マルチリスク対応としてのBCP手法の高度化は、今後ありうるのでしょうか？あるいはERMへ拡大、統合されていくのではないのでしょうか？</p> <p>回答： BCPの守備範囲を対応事象の観点から広げることが、あまり好ましくないと考えます。できるだけall-hazards、all-risksのスタンスを維持しながら、BCPを検証する演習のシナリオとして付け加えれば良いと考えます。BCPは何も大上段に構える必要はありません。現在、自動車製造業などで発生している状況なども、通常時のサプライチェーン途絶や注文の急な変更などへの対応を、継続的なプロセス改善に反映させることで、ある程度までBCP的にも対応できると考えます。BCMで重要なオペレーション上の「柔軟性」を、派遣労働者に求めてしまったことは経済界全体の過ちで、この教訓は、今後いかに別の分野で「柔軟性」を確保するか、といった工夫に落とし込んでいただきたいと思います。また、金融業界については、BCPの他に今回のような事象への対応としては、市場リスク・信用リスク・オペレーショナルリスクの3分野を中心にリスクマネジメントの体制を高いレベルで監督当局などから要求されていましたが、残念ながら有効ではなかったと言わざるを得ません。金融機関については、その原因を作り出した責任や構造的問題の追及と同時に、ERMやBCPをひとつのマネジメントシステムとして融合するための議論を、監督当局も含めてやっていただきたいと思います。</p>
2	<p>ERMとBCMの分岐点の考え方は？あるいは、オーバーラップする部分があるなら、その整理・位置付けは？</p> <p>回答： 世の中での関心が大変高い論点ではありますが、両方の分野がまだ発展途上でもあることから明確な回答はございません。しかし、現時点では究極の目的（ゴーイングコンサーンとしての企業の存続や社会的責任）は一致するものの、アプローチが若干違うと解釈することができます。ERMはまずリスクを洗い出して整理することから始めますが、BCMでは重要業務の抽出や発生事象の想定から始めます。（原因事象は少し後で考えます。）いずれのアプローチを採択したとしても、途中でもう一方の考え方が必要となりますので、今後はERMやBCMの組織へ導入の方法論で整理しなければならないと考えております。</p>
3	<p>①社会全体で取り組むべきBCMにおいて、複数の規格や標準の中から各組織が任意に選択することに問題はないのか？</p> <p>回答： BCMに係わる規格・標準は、個別組織が具体的に取り組む部分に関しては任意の選択で構わない、むしろ、そうでなければ実効性が確保できないと考えますが、組織外の接点や社</p>

	<p>会セキュリティにより深く係わる組織の機能や役割に関しては、ある程度の標準化が「共通言語」として必要となります。前者については、組織の業態や社会的使命などに応じて選択し、後者については現在 ISO で議論されている、社会セキュリティに係わる規格開発に期待するところです。</p> <p>②社会全体での取り組みの重要性は理解できるものの、各組織は自組織における BCM/BCP の策定運用だけで精一杯の可能性もあるが、そことのバランスや有り方は？</p> <p>回答： 自組織に閉じた BCM 体制は実際には使えなかったケースが過去の事故・災害などで散見されます。やみくもに自組織の BCP の完成度を上げてみても場合によっては経営資源の無駄となりかねませんので、BCP はとりあえずあまり時間をかけずに策定し、その後の訓練・演習やちょっとした事件・事故・災害に対応しながら BCM 体制を少しずつ構築してゆくという長期戦で構えるべきでしょう。</p>
4	<p>「個人情報保護」が結局は情報漏洩等の防止であるように「事業継続」とは平たくいえば、どのような目的があるのでしょうか？「一言」で表現していただければ幸いです。</p> <p>回答： 「社会的責任」でしょうか。この背景には、組織、特に企業はゴーイングコンサーンとして存在し続けること、社会的に求められることをできるだけ安定的に供給することを前提に存在しています。規模は小さいながらも業歴の長い組織の経営陣には、このように理解されている方が結構いらっしゃるようです。</p>
5	<p>BCI 協会の資格試験が合格率 5%と聞きました。各審査機関のセミナーを聞きましたがそれほど知力経験がないのがすぐわかります。日本の BCM 審査をゆるくしすぎないで欲しいと思いますが、そのあたりの制度設計についての立場を解説して欲しい。ISO 9001 などのように一般化しても良いのですが有効さが薄れてしまいます。</p> <p>回答： ISO9000 シリーズや 14000 シリーズで一部問題になっているような審査機関の粗製乱造は回避すべきだと考えます。もちろん規格や標準は開発側からしますと、ある一定の市場を確保しなければ開発コストも回収できないこととなりますが、勢い余ってやみくもに市場の拡大を行えば、中長期的には制度自体の信用力が低下し、市場がなくなってしまう可能性もあります。ここは両者バランスを見ながら、うまく牽制機能を持たせた形で世の中に実装できればと考えております。ちなみに審査スキルの主要部分を提供する BCI は審査員の粗製乱造を好ましく思わない立場ですので、慎重な対処をしようとしています。</p>
6	<p>日本は結局、どのガイドラインを採用するのか？RAISS では、TR19 を採用するのか？とともに、日本は RAISS に合わせるのか？</p> <p>回答： BCM の分野に「日本」というくくりは存在し得ないのではないかと考えております。どのガイドラインを選択するのは、それぞれの組織が関係するステークホルダーの状況や社会的責任を認識しながら個別の「ビジネス・デザイン」として選択すべきものだと考えます。しかし一方で、組織間や地域コミュニティの観点から、共通する部分については「共通言語」としての標準化が必要となります。ここは社会セキュリティという観点で標準化を進めている ISO に期待するところです。RAISS につきましては不勉強ながら詳しく存じ上げませんが、TR19 については別途 ISO で議論されております情報システム分野の BCM のタタキ台として活用されておりますし、昨年 11 月に TR19 が正式なシンガポール規格 SS540 は ISO の TC223 にも先日持ち込まれました。</p>

1	<p>サービスレベルダウンを引き起こす情報システム事故は、(原因が) 情報セキュリティ事故ばかりではないはず。C、I、Aのうち、Aを重視した「システム管理基準」との連携も言及・取り上げるべきではないでしょうか？</p> <p>回答： 行動計画では、重要インフラ各分野は、必要又は望ましい情報セキュリティ対策の水準を安全基準等として整備することとしており、安全基準等の策定・改定を支援するために、「重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定に当たっての指針」を別に定めています。指針は、機密性（Confidentiality）、完全性（Integrity）及び可用性（Availability）のいずれも考慮して策定されています。 なお、今回は新たな行動計画の説明に重点を置いたため、安全基準等に関しては、概略のみ説明いたしました。</p>
2	<p>重要インフラ分野各社の検証レベルは、そこに記述されているレベルへの対策を各社が責任をもって行っている（完了）ということでしょうか？もしそうであれば、災害シナリオはどのレベル（地震8以上）を設定しているのでしょうか？</p> <p>回答： 第2次行動計画では、「IT障害が国民生活や社会経済活動に重大な影響を及ぼさないようにすること」を目標としていますが、このような状況に至らないIT障害についても、分野ごとに定めたレベルを逸脱したものについて、発生状況を検証することとしています。この分野ごとに定めたレベルが「検証レベル」です。 また、重要インフラサービスが国民生活や社会経済活動にとって許容可能な水準で安定的に提供され、また利用可能であると見做される状態を「サービスレベル」としてはいますが、このサービスレベルは、検証レベルを参考として各重要インフラ事業者毎に定めるものとされています。 なお、脅威については、①サイバー攻撃をはじめとする意図的要因、②非意図的要因、③災害や疾病、④他分野の障害からの波及、の4種に類型化していますが、ご指摘のようなレベルの設定はしていません。</p>

1	<p>①「マインドフル」について、もう一度説明していただくとありがたいです。</p> <p>回答： 日々の様々な事象について「注意深く」関心を持つことが大切ということの意味しています。インシデントマネジメントで言えば、大きな事故の前に小さな事故の兆候がある場合があります。そのようなときに、その兆候を見逃さないようにすれば、大きな事故を未然に防ぐことができる場合もあります。</p> <p>②組織ないしはトップがコーポレートガバナンスのようなポリシー策定をしない／動かない場合、可能な限りの部署がそれぞれインシデント対策を立てることは、やはり無意味なのでしょうか？</p> <p>回答： 無意味ではありません。組織全体でのガバナンスがなければ、局所的に対策せざるを得ない状況になることもあると思います。ただし、その場合には、対策に必要なコストが、「そのためだけに使うコストとしては大き過ぎる」と言われてしまうかもしれません。それは全体でやらないからに他ならないのですが、そのように受け取られることがあるということです。したがって、対策をすべきですが、部署個別での対策の場合には、それに対する否定的な意見により対策を進めるのが比較的困難になる場合があると思います。</p>
2	<p>BS 25999-2 の事業継続マネジメントは、ISO/IEC 27035 (18044) のインシデントマネジメントの体系を作って、その中で活用するという考えでしょうか？両者の関係をどう考えますか？</p> <p>回答： 現時点で両規格に相互の関係はありません。それぞれは相互に補完する関係にあるもので、どちらかが他方を包含する関係にはならないものと思います。両者の関係が整理されると理想的ですが、それぞれの規格は異なる体系に属して作成されているため、当面は、規格を使う側の組織で整合をはかる必要があるものと思います。</p>
3	<p>ワンストップの組織は通常の企業では、どのような組織（部門）ですか？ex.HP さんでは？</p> <p>回答： ワンストップの連絡窓口をどのような手段で実現するのかによるものと思います。たとえば、電話にするのか電子メールにするのかなどです。一般的とは言えませんが一例として、弊社では緊急時連絡先の電話番号を設けて、それを記載したカードを全社員に配布しています。実際の受け付けは総務部門が担当しています。留守番電話と自動転送電話機能を併用した上で、受付担当者自身が被災することも想定して、東京と大阪に分散させています。また、災害時の安否確認にはウェブと電子メールの報告先も同カードに記載しており、機械的な処理をすればよい報告と人が内容を判断しながら受け付ける必要のある報告とを使い分けています。</p>
4	<p>社内でも説明用に使いたいので自分の PC を 1 つの組織と考えた場合、</p> <ul style="list-style-type: none"> ・ Windows などの OS は何にあたるのでしょうか？ ・ マネジメントシステムは、Windows 上で言えばどのアプリ又はサービスに相当するのでしょうか？ <p>回答： どの説明箇所についてのご質問かが定かではないのですが、PC という装置と組織を関連</p>

付けることは難しいかもしれません。情報セキュリティの製品評価基準である 15408 を使って組織を評価することが困難なのと同様です。その場合には、組織の評価には 27001 や 27002 の方が適しています。

PC における OS の位置づけは、何を主体に考えるかによって変わるものと思いますが、CPU から見れば、OS を含むすべてのソフトウェアは実行すべき命令ですから、CPU を人とするならば、ソフトウェアは組織で言えばルールに相当するものと思います。OS が基本ルールだとすれば、アプリケーションは、OS の上で追加して実行される個別のルールかもしれません。しかし、PC においては与えられたルールが違反されるということは故障などを除いて一般的には発生しません。

マネジメントシステムの構築の一般的な手法は、計画して、実行し、それを確認して、必要に応じて見直すことです。PC にたとえるよりも、人の行為についてを対象とする説明をするのが適しているものと思います。