事業継続マネジメントにおける インシデントマネジメント の考え方

ヒューレット・パッカード
佐藤　慶浩

講師紹介

佐藤　慶浩　（さとう　よしひろ）　http://yosihiro.com/profile

ヒューレット・パッカード　北アジア地域 チーフ・プライバシー・マネージャ
（兼）　日本ヒューレット・パッカード株式会社　個人情報保護対策室　室長

（併任）　内閣官房　情報セキュリティ指導専門官

- 情報ネットワーク法学会　副理事長
- デジタルフォレンジック研究会　理事
- ISO/IEC JTC1/SC 27 専門委員会 委員、WG5小委員会 主査、WG1小委員会 委員
- 日本情報処理開発協会 ISMS技術専門部会 委員
- 情報セキュリティガバナンス研究会 法制度班　メンバー
  （科学技術振興機構研究開発プログラム「ユビキタス社会のガバナンス」プロジェクト）
- コンピュータソフトウェア協会 プライバシーマーク審査判定委員会 委員
- 経済産業省 「ITサービス継続ガイドライン」検討会 委員

目次

- インシデントマネジメントの基本
  - 用語の考察
  - 事象とインシデント
  - 事前想定と想定外対応
- ○○○に係る□△□という言葉の罠
  - 情報セキュリティ・□△□
- 事業継続マネジメントにおける
  インシデントマネジメント

インシデント
マネジメントの
基本

インシデントマネジメントの基本用語の考察

- ***3.1 Business continuity planning***
- Business continuity planning is the process to ensure that recovery of operations will be assured should any unexpected or unwanted incident occur that is capable of negatively impacting the continuity of essential business functions and supporting elements. The process should also ensure that recovery is achieved in the required priorities and timescales, and subsequently all business functions and supporting elements will be recovered back to normal.
- The key elements of this process need to ensure that the necessary plans and facilities are put in place, and tested, and that they encompass information, business processes, information systems and services, voice and data communications, people and physical facilities.

出典: ISO/IEC TR 18044 Information Security Incident Management

インシデントマネジメントの基本用語の考察

- ***3.2 Information security event***
  - An information security event is an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant.
- ***3.3 Information security incident***
  - An information security incident is indicated by a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.

出典: ISO/IEC TR 18044 Information Security Incident Management

インシデントマネジメントの基本
「事象（イベント）」と「インシデント」

- 組織では、インシデントへの対応手順や体制を整備しなければなりません。しかし、インシデントを迅速に対応できる体制が確立しても、日常的に発生している多くの事象を、現場の当事者がインシデントとして認識するのが遅れると、結果的に対応が遅れてしまいます。
- そのようにならないためには、インシデントと認識された以後のことばかりではなく、それ以前の事象にも広く注意をする必要があります。つまり、インシデントの管理をする際に、インシデントから始めるのでは不十分な管理策となってしまいます。
- そこで、インシデントとなる可能性や未知の状況を示している「事象」が、事業運営を危うくする確率及び情報セキュリティを脅かす確率が高くなることで「インシデント」に変遷するという考え方をすることが重要であり、インシデントの管理では、インシデントになる前の事象も対象とする管理策を講じなければなりません。

インシデントマネジメントの基本「事前想定」と「想定外対応」

- 計画準備段階として事前計画に基づく対応手順を充実させて、実際のインシデント発生時に、手順に従って対応することを基本にしています。しかし、その一方で、計画準備段階に用意した手順がインシデントの実情に沿わないときには、手順以外の方法による対応をするための手続きが必要であることも指摘しています。なぜなら、インシデントとは、予測不可能な状況となることもあり、その場合には、事後対応を事前計画で想定した範囲内だけで実施することは、むしろ想定外の状況に柔軟に対応をできなくなる場合がるからです。そのため、想定外の状況に遭遇した場合には、実際の担当者の判断で、事前に定められた処置とは異なる例外処置をできるようにすることも必要です。そのような例外処置についても管理するような管理策を講じることについて述べています。

インシデントマネジメントの基本
参考書籍

「不確実性のマネジメント」

Managing Unexpected

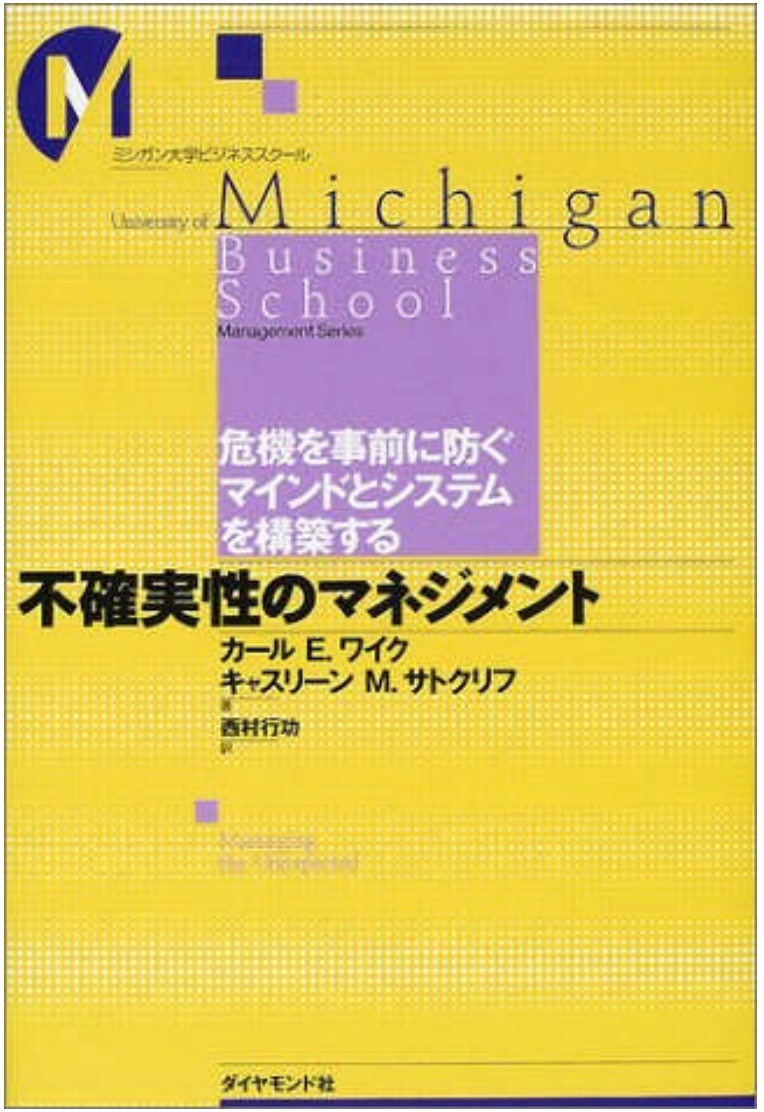
カール E.　ワイク著

キーワード:

・HRO (High Reliability Organization)

　　高信頼性組織

・マインドフル



〇〇〇に係る
□△□という言葉
の　罠

○○○に係る□△□という言葉の罠

- 情報セキュリティ・□△□

- 情報セキュリティ教育
- 情報セキュリティ監査
- 情報セキュリティ・リスクマネジメント
- 情報セキュリティ・ガバナンス

  - 「する」を付けることによる検証
  - 罠　と　カタカナの甘い誘惑

○○○に係る□△□という言葉の罠

- 情報セキュリティ・インシデントマネジメント
- 事業継続マネジメントにおける
  インシデントマネジメント

事業継続マネジメント
における
インシデントマネジメント

（事業継続マネジメントにおける）インシデントマネジメント

- ワンストップ＆ノンストップ
  - 事象を見落とさないようにする
  - 管理と判断、暫定対応、恒久対応、渉外対応
  - 事前計画の策定と、想定外（例外）対応の整備。
  - 事前計画：計画に沿った処理、役割分担、全員連携
  - 例外対応：計画に沿わない処理、役割排除、個別判断

- 解決策は問題の中にはない
  - 目的達成のために、手段を選ばないようにする

（事業継続マネジメントにおける）インシデントマネジメント

- 今後の課題：
  計測できないことは改善できない
  - ISO/IEC 27035 検討中
    Information Security Incident Management (仮)

おさらい

おさらい

- 望んでいないこと　又は　予想していなかったこと
- 事象とインシデント
- 事前想定と想定外対応
- マインドフル
- ワンストップ＆ノンストップ
- 広い視野による解決策の模索
- 計測手法の検討

情報ネットワーク法学会
随時、入会受付中
www.in-Law.jp/

本日の資料
http://yosihiro.com
/go/2009-01-28-inlaw