

第135回 維持管理研究会 議事録

- 開催日時：2022年10月20日(木) 16:00~17:30
- 場所：Zoomリモート開催
- 出席者(敬称略)
井上、上辻、大下、坂本、澤田、守護、高橋、千葉、日向、柳本、山下、中谷(記)
(12名参加)
- 研究テーマ

今月の維持管理研究会は、最近DX化の推進によりIT依存度が更に高くなっているなかで、自然災害によるICT停止のみならず、サイバー攻撃によるICT停止や金銭要求なども増加している。そこで今回は、全社BCPとIT-BCPの役割や戦略に関する責任範囲などについて議論した。

中谷(全社対策本部の遣るべき事とICT責任者のミッション) 抜粋

1. 事業継続計画の必要性

■ 防災とBCP

防災
人命の安全確保、資産の保護、及び環境の保護を行い、被害を最小限に抑えるための対策を事前に施す。

BCP
自然災害等によって、事業が停止又は低下しても、重要事業を目標範囲内・経営戦略上許容できる程度まで回復し、復旧・継続する。

〔広義〕事業継続計画(BCP)

防災(拠点毎)	経営的視点(全社)
(大規模、中規模、小規模、拠点別)	(経営・財務・法的・社会的)
▶ 人命の安全確保 ▶ 物的被害の軽減 ▶ 拠点間への対策・対応 ▶ 安全管理部門・施設部門の取組み ▶ 一層層 ▶ 死者発生数 ▶ 物的損害額	▶ 結果責任による復旧戦略を執行! ▶ 重要業務の復旧優先・継続 ▶ サプライチェーンの対策・供給責任 ▶ 社会的責任を果たす ▶ 一層層 ▶ 復旧時間・復旧レベル ▶ 経営やスタッフホルガに及ぼす影響

2. 重要業務(事業)の選定

■ 自社の位置づけ

▶ 災害が発生した場合においても、お客様に重要な「製品・サービスの提供」を継続させること、地域社会に貢献を果たすことが求められる。

地域社会(国・自治体、地域住民等)

責任

取引先

自社(組織)

お客様(個人・企業)

二次取引先

二次取引先

▶ 不可欠な業務・資源の明確化
▶ 取引先(サプライヤ)の評価

▶ 継続すべき製品・サービスの明確化
▶ 目標復旧時間(RTO)

3. ビジネス影響度分析(BIA)

■ 重要事業の業務プロセス関連図

【A製品 業務フロー】

注文(受注) → 原材料仕入れ → 製造・加工・組立 → 品質検査 → 出荷(倉庫) → 納品(売上)

【業務プロセス関連図】

各業務プロセス間の相互依存関係を図示し、影響度を分析する。

4. 重要業務のリソース関連図

▶ 重要業務に必要なリソース(要素・資源)を自社と外部の観点から相関関係を洗い出します。

業務プロセス

注文 → 原材料仕入れ → 製造・検査 → 出荷 → 売上

自社リソース

要員(人材) → 建物 → 設備 → 情報システム

外部リソース

電力・水道 通信インフラ → 取引先 アウトソース → 3PL ロジスティック

5. 事業継続戦略

■ 事業継続の考え方

▶ 事業継続戦略の策定にあたっては、事業の目標復旧時間を達成するために、業務毎に出来る限り多くの戦略を検討し、最適な戦略を構築する。

【戦略案】回避・緩和・転換・実行

脆弱性に対する事前対策

▶ 収容能力満杯発生
▶ 収容率超過発生
▶ 収容率超過発生
▶ 収容率超過発生

【代替】

- 代替施設・設備の活用
- 遠隔サイトへ業務移転・移動
- 代替サプライヤへ業務移転
- 取引先とアウトソース契約
- クラウドサービス活用
- 他社との互換契約
- 結合他社から部品等の購入
- 代替で業務
- 手作業で対応

【復旧】

- 各優先順位に基づき復旧範囲
- 何もしない(事業停止)

6. 情報システムの継続戦略

▶ 業務部門から継続戦略として必要となる情報システムの継続性強化の要求が高まっています。ITサービスの停止によるリスクを明らかにしておく必要があります。

継続戦略(全社BCP)

経営環境 → 業務環境 → 業務環境 → 業務環境

継続戦略(IT-BCP)

ITサービスの継続性強化

ITサービス → ITサービス → ITサービス

7. 情報システムの現状調査

▶ 業務を遂行する為にも、必要となる情報システムと依存関係を明確にするにより、情報システムの重要度を認識し、調査を行います。

システム名	重要度	依存度	脆弱性	対策	評価
1. 総務システム	4	4	4	4	4
2. 経理システム	4	4	4	4	4
3. 製造システム	4	4	4	4	4
4. CRM	4	4	4	4	4
5. 顧客サポートシステム	4	4	4	4	4
6. 製造現場システム	4	4	4	4	4
7. 購買調達システム	4	4	4	4	4

8. システムの重要度分析

▶ 現状調査では、システムマップ(重要度・脆弱性)を基に、脆弱性の観点から重要業務プロセス、および継続戦略の策定から調査を行います。

システム名	重要度	脆弱性	対策
1. 総務システム	4	4	4
2. 経理システム	4	4	4
3. 製造システム	4	4	4

システム脆弱性調査シート

8. 危機管理の組織体制

▶ 災害発生時の組織体制・機能により、事業継続・復旧能力に大きな差が生じます。業種・活動分野・活動内容に応じて組織体制・訓練(演習)も検討し実施しておくことが重要です。

危機対策本部

全社対策本部

現地対策本部

指揮官(本部長)

副指揮官(本部副長)

情報管理チーム

業務管理チーム

危機対策チーム

連絡調整チーム(連絡員)

※リーダとしての必須行動
状況認識の統一、活動目標の共有、目標達成手段の合意、担当者決定

9. 対策本部の役割

▶ 緊急対応とは、緊急事態発生時に「人命安全・資産(財産)・環境を保護すること及び危機広報を明確にすることである。

危機広報(情報提供)

ステークホルダーへの情報提供(お客様、取引先、社外、自治体、報道機関、社員など)

対策本部

人命の安全確保
資産の保護
環境の保護
事業継続

人命の安全確保
社会との関係の安全確保(従業員など含む)
資産の保護
会社の資産(財産)保護(火災・盗難・情報セキュリティ)
環境の保護
地域の環境保護(大気・水質・騒音・土壌汚染)
事業継続
重要業務の継続・早期復旧(経営戦略上不可欠な業務)

After Action Review

10. 危機対策本部

▶ 危機管理をシミュレーション・スコープ外に対して迅速かつ情報提供を行う。各スコープ外への迅速かつ正確な情報提供を確実にし、復旧方法を明確に定め被災者への支援を確保することを目指す。

危機対策本部

行政機関
地域住民
取引先・サプライヤ
現場部門
社主・メディア
お客様
従業員・家族

守護（VUCA時代の経営トップ判断の重要性）抜粋

<p>10月度 BCOA維持管理研究会</p> <p>全てのサービスがDXに向かうVUCAの時代</p> <p>経営トップ判断の重要性</p> <p>立山マシン株式会社 東京営業所 守護部長</p>	<p>VUCAの時代とDX</p> <p>VUCAの時代をもたらした要因の1つは、情報通信技術（IT）の飛躍です。クラウドに代表されるデジタル技術が最新のITで駆動し、ある地点で起きた変化がITと連携し共有され、様々な形で反映されます。ITの飛躍で、私たちの見える社会は複雑性が増し、変化の早い社会となりました。</p> <p>「昔のDX」 vs 「今のDX」</p> <ul style="list-style-type: none"> Amazon毎日配達：配送サービスに顧客から頼まれ、頼み、依頼 社内業務のクラウド化：IT活用、IT活用による効率化 新鮮な予約サービス、Suicaの連携：ネットワーク、連携が重要 社内業務のクラウド化：IT活用、IT活用による効率化 ユニクロ無人レジ：AI活用、AI活用による効率化 サプライチェーン最適化ソリューション：物流最適化による効率化 <p>GoogleやAmazon、Appleなどのビッグテック（Big Tech）と呼ばれる企業は、最先端のITを使いこなし、圧倒的なスピードと拡張力を持ってサービスを展開（DX）し、業務の拡大を続けています。</p> <p>それ故、Big Techのサプライチェーンの一員、その対抗者、従業者の事業者、そしてDXによるサービスを享受する一般消費者ともにITが絡んでいない時代となりました。</p>	<p>10月度 維持管理研究会の「テーマ」と守護の視点</p> <p>□10月度 維持管理研究会の「テーマ」 全社BCPとI-T-BCPの役割や戦略に関する責任転換 全社対策本部の運営のべきことICT責任者のミッション</p> <p>□守護の視点 今月のテーマに関連した具体例として冒頭には銀行で起きた連続システム障害について説明します。一連の被害に於いて被害をおこなった金融機関は、数々の課題の根本原因を突き詰める銀行システムに対する経営トップの責任に於いて指摘しています。</p> <p>一方、情報通信技術（IT）の飛躍によるVUCAと言われるビジネス環境は、関係者問わず我々の生活を取り巻いています。事業者は何かの形でDXに言われるビジネス形態が進展、関係者問わず我々の生活を取り巻いています。このビジネス環境下で求められる経営とは、圧倒的なスピードで変化に対応する経営。十分な準備でも、その時点での意思決定を行動に移す経営と捉えられます。</p> <p>先述のDX企業でも見られるビジネスの複雑化ITが、ITシステム障害による業務の停滞、影響が及びません。従って、ITシステム障害発生時には即座に全社対策本部を立ち上げ、障害によるビジネスへのインパクトを最小限に抑止する方針（広範囲）を決定すべきです。それが、全社BCP、I-T-BCPを全社BCPの一環として、ICT責任者は連発に障害の原因究明、復旧方針、復旧見込時間等を全社対策本部に報告する責任です。</p>
<p>VUCAの時代に求められる経営</p> <p>社会環境が複雑性を増し 将来の予測が困難な状況</p> <p>Volatility (変動性) Uncertainty (不確実性) Complexity (複雑性) Ambiguity (曖昧性)</p> <p>圧倒的なスピード 目標達成を速く達成し、競争優位性を確保し、成長を遂げる</p> <p>求められる圧倒的なスピード 環境の変化。その時点での意思決定の速さ、実行。</p>	<p>VUCA時代のBC(緊急事態対応)</p> <p>これまで vs VUCAの時代</p> <p>緊急時 日常</p> <p>緊急時 日常</p> <p>緊急時：主に日本国内で発生する天災、事故等による自社およびSCMの被災 対応策：緊急時のBCP準備で対応 知覚：十分早い情報収集の上、判断、対応する時間があった</p> <p>VUCAの時代：「DX先進企業」 緊急時 日常 緊急時：世界中で日々発生する天災、人災、国際的紛争、制度変更等の様々な変化 対応策：トップ意識の会社で影響を判断の上、対応知覚：最新の状況と変化をリアルタイムで把握し、その時点で意思決定を行動に移す必要がある</p>	<p>CISOへの権限移譲だけで済むのか？</p> <p>影響を最小化する サイバーセキュリティの初期対応（BCP） 「感染拡大を防ぐ」 「社内/社外ネットの遮断」 全社の色々な業務に「影響大！」</p> <p>影響を最小化する サイバーセキュリティの初期対応（BCP） 「感染拡大を防ぐ」 「社内/社外ネットの遮断」 全社の色々な業務に「影響大！」</p> <p>影響を最小化する サイバーセキュリティの初期対応（BCP） 「感染拡大を防ぐ」 「社内/社外ネットの遮断」 全社の色々な業務に「影響大！」</p>
<p>トップが関与するBCM ※良い事例</p> <p>情報伝達2時刻ルール 「すぐやる、すぐ進む」を実践 日本経済新聞 2022年6月22日付 社説「危機対応の原則」</p> <p>「何を待つべき」を明確に 「何を待つべき」を明確に 「何を待つべき」を明確に</p> <p>「何を待つべき」を明確に 「何を待つべき」を明確に 「何を待つべき」を明確に</p>	<p>補足：東芝 ニューノーマル時代のゼロトラストシフト</p> <p>ゼロトラストネットワーク</p> <p>東芝がゼロトラストネットワークを推進し、社内社外を完全に分離してセキュリティを確保し、リスクを低減している。社内社外を完全に分離してセキュリティを確保し、リスクを低減している。社内社外を完全に分離してセキュリティを確保し、リスクを低減している。</p>	<p>補足：東芝 EDR、ツールによるエンドポイント対策の強化</p> <p>Endpoint Detection and Response (エンドポイントでのセキュリティ対策の強化)</p> <p>Endpoint Detection and Response (エンドポイントでのセキュリティ対策の強化)</p> <p>Endpoint Detection and Response (エンドポイントでのセキュリティ対策の強化)</p>

5. 意見交換（感想など）

緊急事態発生時の経営トップの立ち位置やあるべき姿が議論の中心となった。

<中小規模>

全社対策本部では、経営トップが責任者となり、リーダーシップを発揮して具体的な指示をすべきである。

<中堅・大企業>

全社対策本部に経営トップは参加せず、緊急対応はリスク責任者に任せる。緊急対応マニュアルに従い判断・指示し、記載のない事象のみ経営トップに相談する。（2・8理論）

経営トップの主要業務は、現状を客観的に把握し、将来を見据えた経営戦略を検討すべきである。

ICT無くしては、企業として何も出来なくなっている現状においては、IT部門は、全社対策本部責任者の直轄組織として、全社BCPの優先順位（RTO）に準じた復旧対応に徹することが重要である。

<次回予定>

・2022年 11月 17日（木）16:00~17:30

以上