

# 維持管理研究会 活動報告

2022年 7月26日

特定非営利活動法人 事業継続推進機構 (BCAO)  
維持管理研究会

※ 本資料の文責は研究会にあり、BCAO全体の見解ではありません。

# 1. 研究会メンバ

2022年 7月10日現在

石川 佳代子  
石綿 麻貴子  
伊藤 享佑  
井上 正太郎  
上辻 裕己  
大下 英紀  
大島 啓一  
金子 幸泰  
國貞 至  
久保 俊一郎  
熊澤 洋平  
古村 太郎  
坂本 純一  
佐藤 栄治

澤田 信人  
柴田 藍  
清水 浩  
守護 彰克  
菅谷 豊  
高橋 哲朗  
滝川 新悟  
田中 祥子  
田中 弘明  
千葉 洋平  
徳山 賢治  
永木 良明  
橋川 秀治  
林 慎一郎

日向 健司  
福島 猛  
藤井 英志  
藤井 健太郎  
森 健  
柳本 成朗  
柳谷 諭  
山下 昌宏  
  
小田 浩史 (副座長)  
中谷 明男 (座長)

**登録メンバー 38名**

## 2. 研究会の目的（コンセプト）

BCM推進者として、**事業継続能力の向上と最新知見の習得**を図る。

- BCM活動に関する最新情報の交換・共有
- 演習の実践及び演習評価方法の研究
- 危機発生時の組織体制・ミッションの研究

### BCM推進者の主業務

- ① 組織方針に基づく年度活動計画の策定
- ② 危機対応組織の体制確立と強化
- ③ BIA／RA／継続戦略の定期的な見直し
- ④ 訓練や演習の実施、及び結果評価と改善
- ⑤ 組織の成熟度評価と経営者への報告
- ⑥ 評価改善の実施・推進

※ 本資料の文責は研究会にあり、BCAO全体の見解ではありません。

# 3. 2021年度 活動実績 (12回開催)

回	実施日	参加者	研究テーマ
117回	0415	29名	最近のサイバーインシデントとサイバー対策 … 講演ラック
118回	0520	13名	BCP担当部門とIT部門の役割の研究 (4社事例紹介)
119回	0617	17名	Webを活用したリモート対策本部のあり方 … 講演NTT-LS
120回	0715	16名	Web-EOCシステムを活用した対策本部訓練の実施
121回	0819	15名	防災対応とBCPにおける対応範囲や役割の研究
122回	0916	18名	防災・BCPに関して対策本部と現地本部のあり方の討論
123回	1021	12名	訓練演習の事例発表 (2社) と問題点・課題の検討
124回	1118	14名	ISO22398 (演習の指針) と演習計画立案の研究
125回	1216	18名	演習設計書策定の基本的な考え方と策定手順の解説
126回	0120	12名	福島第二原発の危機対応DVD視聴とリーダーのあり方を研究
127回	0217	13名	緊急事態発生時のICS体制と本部ミッションの検討
128回	0317	15名	BCPの基本要素10項目と評価シートの研究

※ 本資料の文責は研究会にあり、BCAO全体の見解ではありません。

# 4. 2021年度の主な活動

## テレワーク時代における新たな課題発見と緊急事態発生時の対応体制や役割等について研究

### 1. サイバー攻撃の事例と対策研究

- ⇒サイバーインシデントと対策について講演（ラック社）
- ⇒BCP担当とIT担当の役割について検討

### 2. リモート対策本部の研究と演習体験

- ⇒Web-EOCシステム活用について講演（NTT-LS社）
- ⇒リモート対策本部の演習体験、及び事例発表
- ⇒ISO22398（演習の指針）と演習設計の検討

### 3. 危機発生時の組織体制・役割の研究

- ⇒緊急時のICS体制と本部ミッションの検討
- ⇒BCP10の基本要素とBCM評価の検討

※ 本資料の文責は研究会にあり、BCAO全体の見解ではありません。

# 4. 主な活動実績

## 4-1. サイバー攻撃の事例と対策研究

### ① サイバーインシデントと対策について講演 (ラック社)

テレワーク増加がオリンピックの影響もあり、ランサムウェアやエモテット等のサイバー攻撃により、多くの企業が被害を受けており、ITの長期間停止や多額の金銭請求など、経営に大きな影響を受けています。サイバーセキュリティ専門家に最新の「セキュリティ攻撃の現状と課題」について講演して頂いた。

#### 3つのやるべきこと

- ◆ ITのリスクアセスメント実施
- ◆ システム（セキュリティ）構成管理の現状把握
- ◆ CSIRTの活動状況確認

APTチェックリスト等の活用により、組織のセキュリティレベルを評価しITの安全度を確認し、事業継続能力を向上させる。

※APT (Advanced Persistent Threat) 高度サイバー攻撃

※ 本資料の文責は研究会にあり、BCAO全体の見解ではありません。

# 4. 主な活動内容

## 情報セキュリティ10大脅威2021

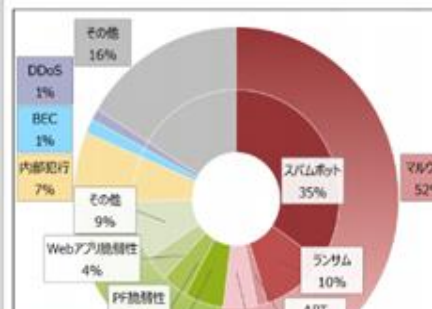


順位	内容	昨年順位
1	ランサムウェアによる被害	5
2	標的型攻撃による機密情報の窃取	1
3	テレワーク等のニューノーマルな働き方を狙った攻撃	NEW
4	サプライチェーンの弱点を悪用した攻撃	4
5	ビジネスメール詐欺による金銭被害	3
6	内部不正による情報漏えい	2
7	予期せぬIT基盤の障害に伴う業務停止	6
8	インターネット上のサービスへの不正ログイン	16
9	不注意による情報漏えい等の被害	7
10	脆弱性対策情報の公開に伴う悪用増加	14

IPA 情報セキュリティ10大脅威 2021

13

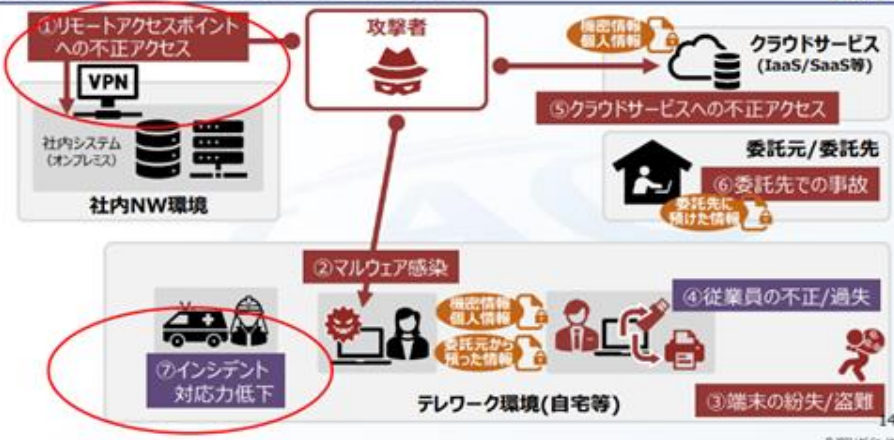
## 2020年の出動傾向



- マルウェア関連の相談が50%強
- 3割強がEmotet関連 (左図のスパムボットのほぼ全てがEmotet)
- サーバ不正侵入、内部犯行、BEC等も件数としては例年よりも増加

**推定合計1,620万人(7人に1人)がサイバー攻撃を経験 被害額は320億円に (NewWeb 220430)**

## テレワークに伴うリスク発生ポイント



14

## リスクアセスメントの実施



テレワークの導入・利用範囲拡大に伴ってリスクは確実に増加  
**テレワークを止める・抑制する方向に向かうのは間違い**  
**テレワークは逃げられない課題**



28

# 4. 主な活動内容

## ② BCP担当とIT担当の役割について検討

緊急事態発生時のBC部門（危機対応）とIT部門の役割が明確になっていない企業が多い。

IT部門担当者を全社BCPへの関与の度合いを向上（連携強化）のため、現状把握と課題について情報交換を実施しました。

### ■ S社

両部門を同一本部内に体制を変更して連携しやすくし、定期的に情報交換を行い、サイバー攻撃やウイルス等の情報を一元的に管理している。

### ■ T社

平時はそれぞれが個別に活動しているが、危機管理本部にCSIRTを設置してITトラブルやサイバー攻撃などの被害発生防止の対応を行っている。

### ■ E社

IT部門は、IT-BCPでシミュレーション訓練等を定期的実施している。

### ■ M社

主業務が金融業務であるため、IT継続が企業の生命線であり、CSIRT体制強化による運用を徹底している。

※ 本資料の文責は研究会にあり、BCAO全体の見解ではありません。



# 4. 主な活動内容

## 4-2. リモート対策本部と訓練手法の研究

### ① Web-EOCシステム活用についての講演 (NTT-LS社)

テレワークが日常化している中で、大規模地震などの緊急事態発生時における対策本部の運用に有効な「Web-EOCシステム」について、機能や運用方法を解説して頂いた。

#### 《情報収集分析・指示の流れ》

※NTT-LS講演資料（抜粋）

**連絡処理票** ↓発生状況をスマホ・PC等で入力

| 指示・依頼内容を進捗管理する「連絡処理票」


各班間や本部・支部間における、情報の周知・依頼およびタスクの管理に使用



**クロノロジー** ↓事象別に整理・分類し活動を記録

| 各班内の活動状況を記録する「クロノロジー」

班内で収集した被害情報や活動状況の記録、交代人員との引継ぎに活用

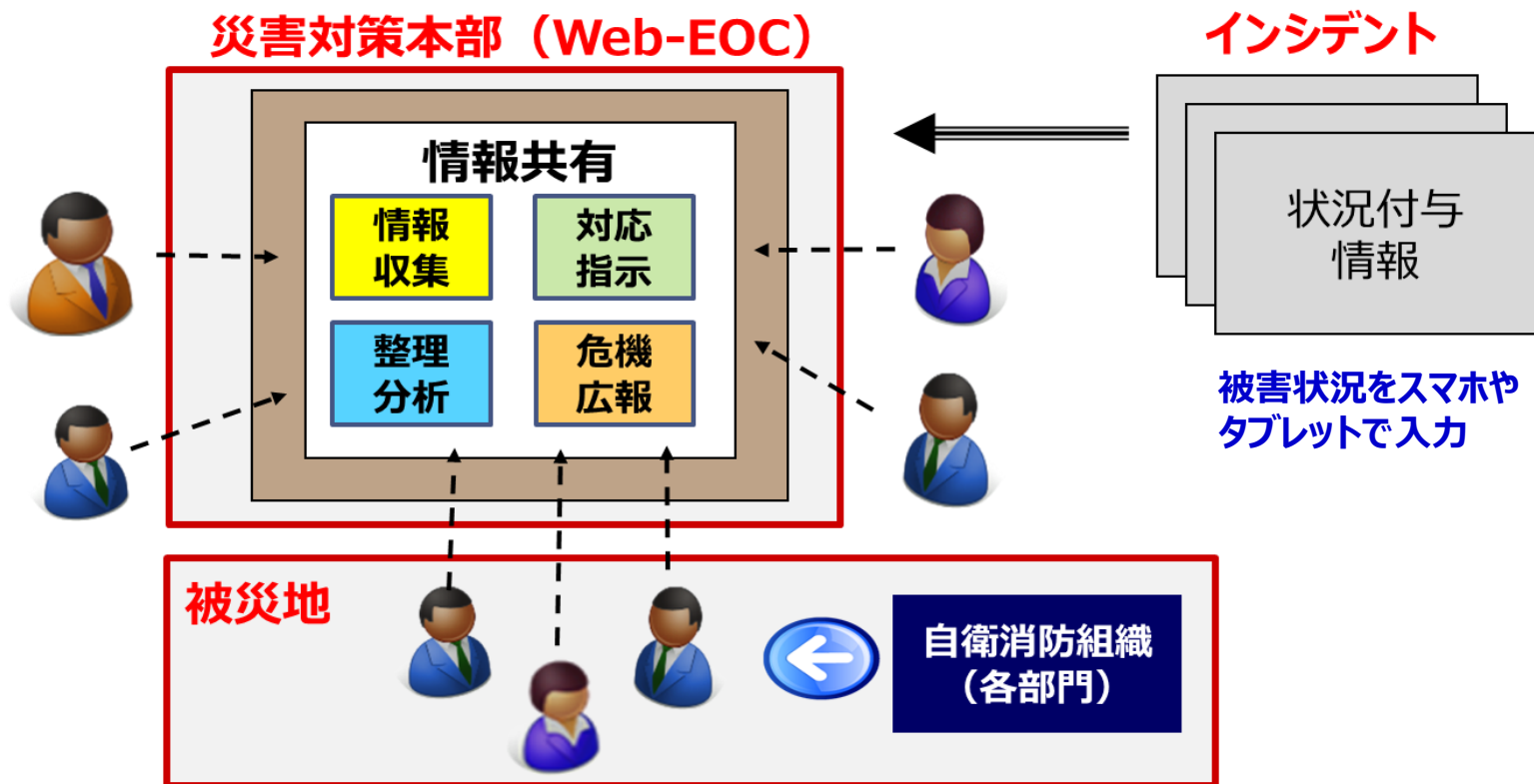


※ 本資料の文責は研究会にあり、BCAO全体の見解ではありません。

# 4. 主な活動内容

## ② リモート対策本部の演習体験

Web-EOCシステムを活用して、対策本部として対応すべき情報収集整理  
対応策の検討（優先順位）及び課題抽出とトップ報告等を体験しました。



※ 本資料の文責は研究会にあり、BCAO全体の見解ではありません。

# 4. 主な活動内容

## 演習設計書（シナリオ抜粋）

※Nakatani 策定演習シナリオ（抜粋）

WS	PDF頁	発災か	情報元	kemmei	naiyo	bunru	juy	kinky	taio_jokyo	atesak	kihyo_nichiji
WS1	P8 P11	0:00	外部情報	緊急地震速報 M7 相模湾	たたいま東京湾で大きな地震が発生しました ◆震源地 相模湾 ◆震源の深さ 30 Km ◆マグニチュード M7	周知	重要	緊急			2021/7/15 10:00
WS1	P8	0:05	社内情報	全館停電発生	・P Cが多数落下、キャビネット転倒 ・全館停電発生	周知	重要				2021/7/15 10:05
WS1	P17	1:00	社内情報	平塚工場の負傷者情報（重傷者2名）	製造部 <b>Xさん（男性）</b> 天井から落下した蛍光灯が頭部にあたり頭からかなり出血しています。 管理部 <b>Yさん（女性）</b> 転倒したキャビネットで胸を強打し、倒れて意識が朦朧としています。（妊婦） 電話が繋がらず、救急車を呼ぶことが出来ません。2名とも医務室に運び込んでいます。 【ヒント】平塚工場への対応で追加の指示があれば記入ください	依頼	重要	緊急			2021/7/15 11:00
WS1	P14	2:00	外部情報	通信状況（携帯通話不可、メール大幅遅延）	◆固定電話や携帯電話は、輻輳し通話できません。 ◆携帯メールは大幅に遅延 ◆モバイルカードによるインターネット接続は利用可能	周知					2021/7/15 12:00
WS1	P14	2:05	外部情報	停電情報（首都圏広域で停電）	◆電気は首都圏広域で停電発生	周知					2021/7/15 12:05
WS1	P14	2:10	外部情報	断水情報（神奈川県南部で断水）	◆水道は、神奈川県南部で断水	周知					2021/7/15 12:10
WS1	P15	2:15	社内情報	本社事務所の状況（7/15 12時時点）	◆建物壁や窓ガラスに損傷なし ◆事務所内で火災は発生なし ◆ロッカーが倒れて書類散乱 ◆全館で停電 ◆ルータは、UPSで稼働中（8H程度）	周知					2021/7/15 12:15
WS1	P16	2:20	社内情報	平塚工場の状況（7/15 12時時点）	◆地震発生により、全員が外に避難しており、 出勤者全員の安否確認は取れていますが、 負傷者が多数おり、応急手当をしています。 ◆建屋の一部外壁にひび割れが見られますが、倒壊の危険性はありません。 ◆工場内の設備等が大きく損傷しており、復旧には、数ヶ月は必要である。	周知					2021/7/15 12:20
WS1	P16	2:25	社内情報	所沢工場の状況（7/15 12時時点）	被害なし	周知					2021/7/15 12:25
WS1	P19	3:00	課題	本部長への状況報告準備をお願いします（1回目）	本社勤務の3名が対策本部員として参加 他はリモート参加として演習して下さい。 対策本部として問題点・課題を洗い出し早急に対応すべきことを検討して、経営責任者に報告願います。 【ヒント】これまでの情報をもとに①問題点・課題 ②対策を簡潔書きで記入ください	依頼				44392.54167	
WS2		8:00			***8時間経過*** (これ以降はWS1の状況付与への回答はしないでください)	周知					2021/7/15 18:00
WS2	P21	8:00	外部情報	周辺地域の状況	◆ターミナル駅は会社員や買物客で大混雑である。 ◆周辺の人々が外に避難しており、道路周辺でも多くの人で溢れています。 ◆当社のビル建物内に多くの人が入ってきています。	周知					2021/7/15 18:00
WS2	P22	8:05	外部情報	ニュース報道（交通機関、通信、病院）	◆首都圏南部で交通機関ストップ (東海道・京浜東北・横須賀・京急・相鉄等) ⇒橋げた落下の復旧には、最低2週間以上必要 ⇒線路の調査が完了し、電力が回復した路線から復旧 ◆主要幹線道路は緊急車両優先 ⇒一般車両は通行禁止（東京北部、埼玉、千葉は解除） ◆京浜地区のタンク炎上は鎮火 ⇒ガソリンスタンドに長い行列ができており、入手が難しい ◆通信：固定、携帯電話とも輻輳しており、繋がりにくい ◆病院：多数のケガ人が押しかけて、殆どの病院が大混乱	周知					2021/7/15 18:05

※ 本資料の文責は研究会にあり、BCAO全体の見解ではありません。

# 4. 主な活動内容

## ③ 訓練・演習内容の事例発表

自社で実施した訓練・演習内容について、可能な範囲で説明して頂いた。  
南海トラフ大地震（山下さん、守護さん）

## ④ ISO22398（演習の指針）と演習設計の検討

国際標準「ISO22398-演習の指針」に関する基本的な考え方の概要解説、及び組織に合致した演習計画の立案について検討しました。

### 4-1. 演習プログラムの計画策定 第4章

トップマネジメント (経営者)	①	演習プログラムの目的が達成されるように徹底する。
	②	演習プログラムを運用管理する力量を備えた人材を任命する。 (演習プログラム管理者)
演習プログラムに 盛り込む事項	①	ニーズ分析 演習プログラムの必要性の明確化
	②	支援基盤 トップマネジメントによる支援基盤、及びコミットメントの確保
	③	演習プログラムの狙い及び目的 演習の意図の提示
	④	演習プロジェクトの領域、種類、期間、場所、日程 演習プロジェクトの実施内容の提示
	⑤	演習プロジェクトチームの選任 演習プロジェクトの計画策定、演習実施、評価を行う人材の任命
	⑥	必要なリソース、及び予算 演習プロジェクトに必要な要員、装備、資金等の確保
	⑦	機密保持、情報セキュリティ、安全衛生、その他 演習プロジェクトを実施する上で対応しなければならない事項

### 5-2. 演習タイプの決定 第5章 (演習タイプの事例)

演習の 種類	警報発令演習	参加者の対応と警報発令の仕組みを確認する。
	始動演習	適切な対策本部立上げに対応する能力を確認・育成する。 「警報発令訓練」に続いて実施する。
	スタッフ演習	組織内の日常プロセス、スタッフ、情報のもとで行動し、共通の現状認識を構築し、何を決断すべきか提案能力を高めることを目指す。
	意思決定演習	意思決定プロセスを演習する。明確かつ時宜を得た意思決定能力、時間的制約を考慮して、関係者間の連携を図る能力を含む場合もある。
	マネジメント演習	警報発令・始動演習、及びスタッフ意思決定演習の組合せ。役割、組織体制、標準作業手順に力点を置く。
	協力演習	様々な組織や部門間で共に取組み行動するために実施する。 (垂直連携、水平連携、官民連携、地域社会連携)
	危機管理演習 (モック)	模擬的な危機発生状態で、危機管理計画に記載する自らの役割を訓練し、熟達する機会を提供する。
	戦略的演習	戦略的なレベルで実施する包括的な演習活動 (本社危機管理、政府-官庁スタッフ、自治体連携)
	演習キャンペーン	共通の全体的な組織体制において繰り返し実施される一連の演習

※ 本資料の文責は研究会にあり、BCAO全体の見解ではありません。

# 4. 主な活動内容

## 4-3. 危機発生時の組織体制と役割

### ① 緊急時のICS組織と本部ミッションの検討

緊急事態発生時の組織体制の在り方や緊急時の対応方法についてICS体制をベースに緊急時対応すべきミッションや指揮命令系統等について意見交換を行った。

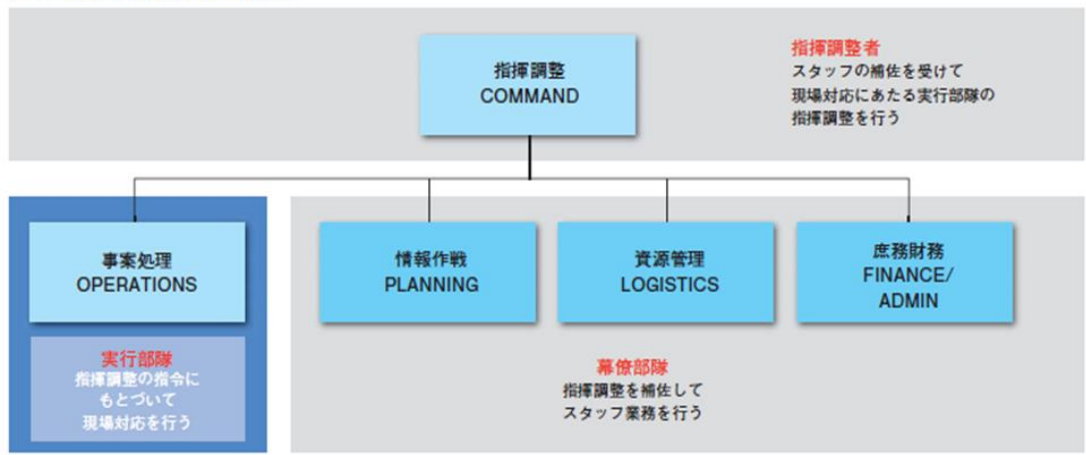
緊急事態発生時の組織体制や基本行動（やるべきこと）について、各社の現状などを含めて、あるべき対策本部体制について検討した。

対策本部組織体制において、経営トップの社長を対策本部長に据えている企業が多くある。しかし経営トップは、経営的な観点から長期的な戦略や顧客対応（広報含む）に専念すべきである。現在のインシデント対応は、対策本部長に任せて定期的な状況を報告と重要ポイントのみを指示することが理想である。

※ 本資料の文責は研究会にあり、BCAO全体の見解ではありません。

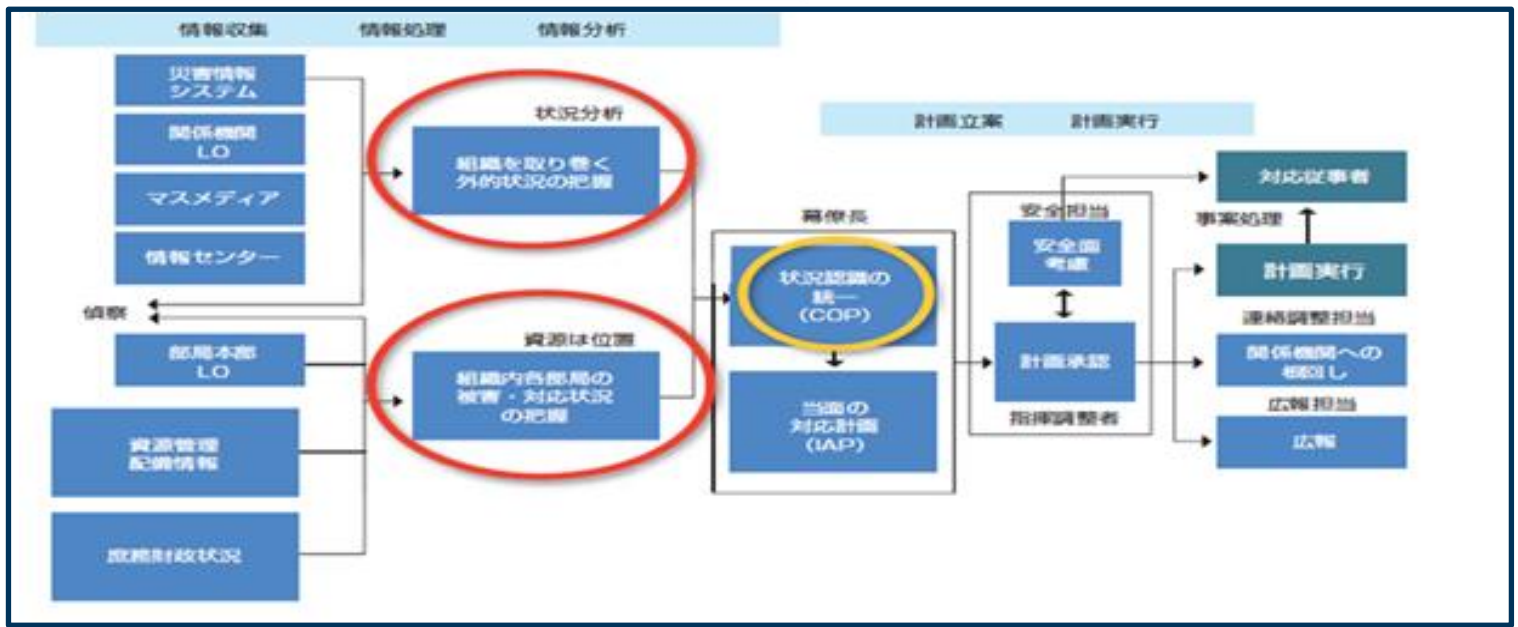
# 4. 主な活動内容

図1 危機対応に必要な5つの機能



経営トップ（社長）以外の役員等を  
責任者として対策本部長に配置する。

＜発生インシデント＞  
 想定内 80%  
 想定外 20%（トップ判断）  
 ※緊急時行動手順書は必須である。



※ICS解説書（抜粋）

※ 本資料の文責は研究会にあり、BCAO全体の見解ではありません。

# 4. 主な活動内容

## ② BCPの基本要素とBCM評価の検討

### 《専門業務10項目 (Professional Practices) 》

- |                  |                  |
|------------------|------------------|
| ①プロジェクト導入とマネジメント | ⑥事業継続計画の作成と実施    |
| ②リスク評価とコントロール    | ⑦啓発と訓練プログラム      |
| ③ビジネス影響度分析       | ⑧事業継続計画の演習・監査・維持 |
| ④事業継続戦略の策定       | ⑨危機広報            |
| ⑤緊急対応とオペレーション    | ⑩外部機関との調整        |

### BCP関連の各社推進状況！

- ⇒ BC関連のドキュメントは、クラウドに保存し共有している。  
利点としては、テレワーク下でも資料の参照が容易であり、文書の更新が簡単に行える。また全社員が容易に閲覧できる利点もある。
- ⇒ 緊急時に、ネットワークが正常であることが前提になっており、緊急時に閲覧出来ない可能性があるため、重要書類のみ印刷し管理している。  
しかし複数個所にあると管理が十分出来ない。などの意見があった。

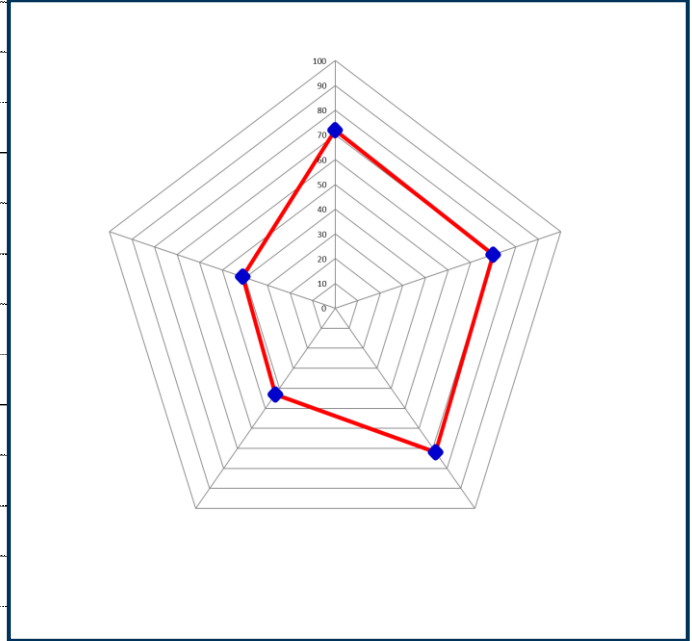
※ 本資料の文責は研究会にあり、BCAO全体の見解ではありません。

# 4. 主な活動内容

## BCM推進状況 評価チェックシート (抜粋)

※Nakatani 策定評価シート (抜粋)

項	確認項目	確認内容	評価	コメント
方針・目的	①	事業継続の方針や目的は明確になっていますか、また会社の経営方針とリンクしていますか (誰のために、何のために、どんな目的で、何故やるのか等)	3	
	②	全社の事業継続方針・目的と各事業部(関連会社等)の事業継続戦略は合致していますか 全社方針に基づき、各事業部(関連会社)の戦略は策定されていますか	3	
	③	事業継続すべき対象範囲や事業内容は、主要顧客の要求(国・自治体含む)や財務諸表への影響を考慮して策定されていますか	3	
	④	国・自治体の法令・規制、及び顧客との契約等の情報を収集・精査し、重要な事業に影響がないか定期的に(最低1回/年)に確認していますか	3	
	⑤	事業継続の方針や目的は文書化(要約)し、全従業員(パート・アルバイト・派遣社員含む)に配布し周知徹底していますか	3	
B I A / R A	⑥	企業の合併や部門売却を行った場合、B I A を再度実施して重要業務を見直していますか また新規事業(新商品含む)を開始した場合も同様に B I A を行っていますか	3	
	⑦	重要な取引先の増加(又は減少)した場合、再度 B I A やリスク分析を実施していますか また拠点の増設や閉鎖時も同様に実施していますか	3	
	⑧	拠点の移転や建物建替、及び設備導入時には、リスクを再評価して環境変化の有無や対応状況を再確認していますか	3	
	⑨	新たな脅威やリスク(サプライチェーン含む)が発生していないか定期的(1回/年以上)に確認して 自社リスクの見直しを実施していますか	3	
	⑩	国・自治体及び防災関連団体等から発行される広報誌や書籍の定期購読、及びセミナー等に参加し 最新情報を収集していますか	3	
事業継続戦略	⑪	利害関係者の名簿(会社名・責任者/担当者・連絡先・緊急連絡手段等)を定期的に収集し代替の 連絡手段を含めて管理できていますか	3	
	⑫	事業継続戦略に必要な重要リソース(設備・ITシステム、サプライヤ等)を一元的に管理し、対策実施 状況を継続的に管理できていますか	3	
	⑬	重要な業務継続の資源・リソース及び部品等の調達ルートは、複数確保(取引先・拠点)していますか	3	
	⑭	重要な取引先とその製品・サービス等の調達に必要な「災害時基本契約」は締結していますか	3	
	⑮	災害発生時に地域自衛消防団及び自治体との協力体制が取れるよう定期的に協議していますか	3	
文書管理	⑯	文書・記録の管理ルールが明確に定められていますか (管理者、管理台帳、配布管理、保管場所、版数管理、保管と保存期間など)	3	
	⑰	各種ドキュメント(ERP/IMP/B CP/B RP等)は、定期的に見直し実施されていますか (人事異動や組織変更、及び重要顧客や取引先の変更などの見直し)	3	
	⑱	利害関係者の名簿(会社名・責任者氏名・連絡先等)や緊急時の連絡手段は、定期的を確認し 更新していますか	3	
	⑲	対策本部要員は、各種ドキュメントの最新版(又は行動チェックシート)を印刷して保管していますか	3	
	⑳	B C M活動に関する記録は、整理・分類されて保管していますか (文書と記録が混在していないこと)	3	



※ 本資料の文責は研究会にあり、BCAO全体の見解ではありません。



## 6. 今年度の活動テーマ（2022年度）

**B C 推進者として、マネジメント力の向上を図り、  
更なる危機対応能力の向上を目指す。**

### ①サイバー攻撃と対策の研究（継続）

⇒最新のサイバー攻撃の種類と対策手法

⇒ITセキュリティとOTセキュリティの違いと注意事項

### ②訓練・演習と災害事例研究（継続）

⇒緊急時の対策本部に役立つツールの研究

⇒今後の災害事例と事前対応策の研究

### ③重要サプライヤの評価手法の研究

⇒お客様や取引先の評価手法の研究

※ 本資料の文責は研究会にあり、BCAO全体の見解ではありません。

# ご清聴ありがとうございました

**BCPは経験を積み重ねて、見直し改善  
していくことが最大の防御となります。**



**特定非営利活動法人  
事業継続推進機構  
維持管理研究会**

A Specified Non-Profit Japanese Corporation  
Business Continuity Advancement Organization (BCAO)