IT-BCPとシステム監査に関する考察

株式会社内田洋行　ガバメント推進営業部
（日本システム監査人協会　副会長）
荒町　弘

アジェンダ

講師略歴

IT-BCPに関するこれまでの取組み（近畿支部グループ活動概要）

IT-BCPとシステム監査　実効性のあるIT-BCPの要件

システム管理基準　システム管理基準ガイドラインの活用
（ITガバナンス）

システム管理基準　システム管理基準ガイドラインの活用
（ITマネジメント）

まとめ

講師略歴

- 1992年に大学卒業後、株式会社内田洋行入社
  IT営業として学校法人向け事務システム販売担当として活動
- 1994年より地方公共団体向けITソリューション営業として活動開始
- 2008年6月　システム監査技術者試験合格（同年SAAJ入会）
- 2009年12月　ITストラテジスト試験合格
- 2021年12月　CSA認定
- 2023年7月　東京に転勤
  現在、中央省庁／国の外郭団体、東京／神奈川の地方公共団体
  向けITソリューション及び空間構築ビジネスを担当。

SAAJ近畿支部　活動略歴

- 2008年　SAAJ入会（セミナーグループ／BCP研究プロジェクト(主査)を担
- 2010年　BCP研究会活動開始（同年A社との共同取組み開始）
- 2014年　IT-BCP体験セミナー開催／西日本支部合同研究会にて活動報告
- 2015年　IT-BCP体験セミナー開催
- 2016年　IT-BCP体験セミナー開催(大阪市ICT戦略室向け)
- 2018年　協会報2月号記事掲載【ICT部門におけるBCPへの取り組みと課題】
- 2019年　レジリエンス認証制度とシステム監査について研究
- 2020年　情報システム監査実践マニュアル第3版（グループで執筆）
  （第3部　第10章 レジリエンス認証制度とシステム監査）
- 2021年　協会報8月号記事掲載【ﾃﾚﾜｰｸ環境におけるBCPの考え方】
- 2022年　ﾃﾚﾜｰｸ環境とIT-BCPの研究～BCAO ITｻｲﾊﾞｰﾀｽｸﾌｫｰｽとの連携開始
- 2023年　IT-BCP体験セミナー開催（2月25日、10月28日）

IT-BCPに関するこれまでの取組み

（近畿支部グループ活動概要）

BCP研究会発足

特定非営利活動法人　日本システム監査人協会　近畿支部
BCP研究会（中間報告）

2011年8月20日

BCP研究会　荒町　弘

研究会発足の経緯

- 2010年度　近畿支部総会後の情報交換会にて近畿支部関西理事より提案があった
- 発起人3人がメンバを募り2010年2月17日にキックオフ→研究会発足へ
- 当初メンバは8名でスタート
- まずは参加メンバの知識共有から開始
- BCP策定支援アドバイザーの仕事を手掛けておられる川端理事にレクチャーをお願いする

目標設定

- WGを進めるにあたり、目標を設定。

1．研究会メンバとしてBCPに関する知識と理解を深める。

2．ITのビジネスリスクやリスク分析について意見交換し見解をまとめる。

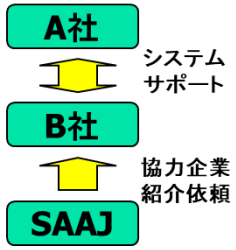
3．中小企業にフォーカスしたリスク対応ケースを作る。

A社との共同取組み

2011年8月20日

BCP研究会　荒町　弘

協力企業（A社）との接点・アプローチ



① BCPへの取組みに協力頂けそうな企業（A社）を紹介して頂く。（取引先B社に依頼）

② A社へのアプローチに際して、取引先B社へ趣旨説明を実施（8月初旬）。

③ A社への初回訪問と趣旨説明（8月中旬）。

④ A社内にて経営層を含めた検討を頂く。

⑤ BCP策定の協同取組みに対してA社より承諾を得る（9月）。

A社の概要（既存の課題など）

- 3名という少人数で全社のITを管理するため、ドキュメント整備等が追いつかない

  （セキュリティポリシーは策定したが、ドキュメントが最終纏め切れていない）
- 日常の管理については十分こなせているが、ドキュメント類を中心とする既存システムの情報資産の整理が十分できていない
- BCP策定を機に既存システムの棚卸しも改めて実施したい

A社との共同取組み

2011年8月20日

BCP研究会　荒町　弘

A社のBCP策定支援活動

- 参考とするガイドラインの検討

「地方公共団体におけるICT部門の業務継続計画（BCP）策定に関するガイドライン」を用いる

＜理由＞ICT部門に特化したガイドラインであるためA社の取組み範囲と一致する。アウトプットサンプルも提供されているため、取組みしやすい。

- 作業の範囲とアウトプット

「上記ガイドラインにおける第1部（BCP策定の基盤づくり）を作業の対象とする」

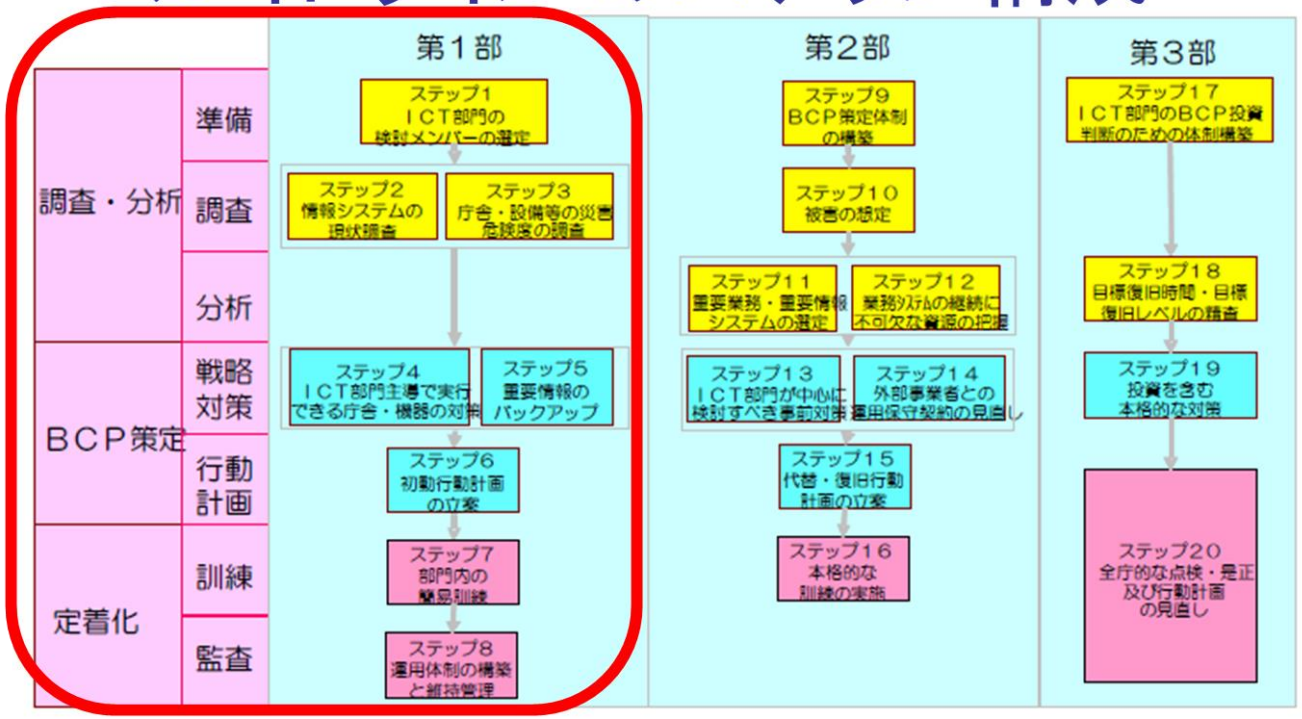
「アウトプットについてもガイドラインのサンプルを参考にし、項目の追加などA社に必要な修正を加える」

- 作業主体とSAAJの役割

BCP策定作業はA社が主体となり実施する

SAAJは作業の過程において必要な助言などを行いBCPの精度向上に向けた支援を行う

ガイドラインのステップ構成



「地方公共団体におけるICT部門の業務継続計画（BCP）策定に関するガイドライン」より抜粋

A社との共同取組み

特定非営利活動法人　日本システム監査人協会　近畿支部
BCP研究会（中間報告）

2011年8月20日

BCP研究会　荒町　弘

第１部：ＢＣＰ策定の基盤づくり
- ステップ１：ＩＣＴ部門の検討メンバーの選定
- ステップ２：情報システムの現状調査
- ステップ３：庁舎・設備等の災害危険度の調査
- ステップ４：ＩＣＴ部門主導で実施できる庁舎・設備等の対策
- ステップ５：重要情報のバックアップ
- ステップ６：初動行動計画の立案
- ステップ７：ＩＣＴ部門内の簡易訓練
- ステップ８：運用体制の構築と維持管理

第２部：簡略なＢＣＰの策定
- ステップ９：ＢＣＰ策定体制の構築
- ステップ１０：被害の想定
- ステップ１１：重要業務・重要情報システムの選定
- ステップ１２：重要情報システムの継続に不可欠な資源の把握
- ステップ１３：ＩＣＴ部門が中心に検討すべき事前対策
- ステップ１４：外部事業者との運用保守契約の見直し
- ステップ１５：代替・復旧行動計画の立案
- ステップ１６：本格的な訓練の実施

第３部：本格的なＢＣＰの策定と全庁的な対応との連動
- ステップ１７：ＩＣＴ部門のＢＣＰ投資判断のための体制構築
- ステップ１８：目標復旧時間・目標復旧レベルの精査
- ステップ１９：投資を含む本格的な対策
- ステップ２０：全庁的な点検・是正及び行動計画の見直し

「地方公共団体におけるICT部門の業務継続計画（BCP）策定に関するガイドライン」より抜粋

BCP策定に向けた取組み

- 重要業務（システム）の選定
- 優先順位づけ
- 運用状況の確認
- **現地視察・サーバ室確認**
- 改善ポイントの洗出し
- ドキュメントの整理
- BCP（簡易版）の作成

	様式名
様式１	情報システム一覧
様式２	外部事業者との関係整理
様式３	庁舎（建物）の状況把握結果
様式４	システム機器設置場所の状況把握結果
様式５	電力供給、通信手段に関するリスクの把握結果
様式６	現状の脆弱性と対策の実施計画
様式７	重要情報のバックアップの状況と対策計画
様式８	緊急時対応体制
様式９	緊急連絡先一覧
様式１０	緊急時における行動計画（初動・代替・復旧行動計画）
様式１１	被害チェックシート　簡易版
様式１２	訓練計画
様式１３	業務継続計画の運用体制

「地方公共団体におけるICT部門の業務継続計画（BCP）策定に関するガイドライン」より抜粋

A社との共同取組み

2011年8月20日

BCP研究会　荒町　弘

管理・運用状況の点検

現地視察・サーバ室確認

自家発電設備	敷地内駐車場屋根に太陽光発電設備を整備
電源設備	サーバ等全てUPS給電・停電時は太陽光発電にてサーバ室給電
地震対策	建物は新耐震基準に対応 サーバ室19インチラックは3台連結、転倒防止措置（スタビライザ） サーバ室内ラック以外の耐震・転倒防止措置（＊）
空調設備	サーバ室専用で空調有り エアコンからの漏水対策を検討（＊） 室外機の地上からの高さを上げるのが望ましい（＊）
配線設備	ケーブルラックによるラック上部配線 強電と弱電の配線区画化などは配慮が必要（＊）
水害対策	事業所が高台に位置し、河川氾濫による被害等は少ないと考えられる
火災対策	電算機用の消火設備を検討が必要（＊）

（＊）部分は今回の点検から検出された改善ポイント

管理・運用状況の点検

現地視察・サーバ室確認

環境監視	煙探知機有り、緊急時通報システムは自社開発（近々設置） 温度・湿度等の記録にはロガー設置（＊）
雷対策	建物自体の避雷設備のみ
入退室管理	サーバ室にはICT部門担当者と事業所責任者のみ許可
媒体管理	バックアップ媒体はサーバ室内に管理 区画された別の場所への保管を検討（＊）
建物の耐震	新耐震基準に対応
オフィス環境	5Sが徹底されている 無線LANにより機動性の高いオフィス

（＊）部分は今回の点検から検出された改善ポイント

システムとデータを管理するサーバ室のファシリティ面においていくつかの改善ポイントはあるが、高いセキュリティ意識とIT部門の統制が効いており、運用状況の面では十分であるといえる。

A社との共同取組み

特定非営利活動法人　日本システム監査人協会　近畿支部
BCP研究会（中間報告）

2011年8月20日

BCP研究会　荒町　弘

BCPとシステム監査

（組織体が情報システムにまつわるリスクに対するコントロールを適切に整備・運用する目的）

- 情報システムが、組織体の**経営方針及び戦略目標の実現に貢献**するため
- 情報システムが、組織体の**目的を実現するように安全、有効かつ効率的に機能**するため
- 情報システムが、**内部又は外部に報告する情報の信頼性を保つように機能**するため
- 情報システムが、**関連法令、契約又は内部規程等に準拠**するようにするため

BCPとシステム監査

（システム管理基準における事業継続計画）

Ⅰ.情報戦略　－　5.事業継続計画

ICT部門に限定
- （1）情報システムに関連した事業継続の方針を策定すること。
- （2）事業継続計画は、利害関係者を含んだ組織的体制で立案し、組織体の長が承認すること。
- （3）事業継続計画は、従業員の教育訓練の方針を明確にすること。
- （4）事業継続計画は、関係各部に周知徹底すること。
- （5）事業継続計画は、必要に応じて見直すこと。

Ⅵ.共通業務　－　7.災害対策

7.1 リスク分析
- （1）地震等のリスク及び情報システムに与える影響範囲を明確にすること。
- （2）情報システムの停止等により組織体が被る損失を分析すること。
- （3）業務の回復許容時間及び回復優先順位を定めること。

7.2 災害時対応計画

ICT部門に限定
- （1）リスク分析の結果に基づき、事業継続計画と整合をとった災害時対応計画を策定すること。
- （2）災害時対応計画は、組織体の長が承認すること。
- （3）災害時対応計画の実現可能性を確認すること。
- （4）災害時対応計画は、従業員の教育訓練の方針を明確にすること。
- （5）災害時対応計画は、関係各部に周知徹底すること。
- （6）災害時対応計画は、必要に応じて見直すこと。

7.3 バックアップ
- （1）情報システム、データ及び関連設備のバックアップ方法並びに手順は、業務の回復目標に対応して定めること。
- （2）運用の責任者は、バックアップ方法及び手順を検証すること。

※システム管理基準（2004年　第2回改訂版）を参照してのアプローチを行った。

A社との共同取組み

特定非営利活動法人　日本システム監査人協会　近畿支部
BCP研究会（中間報告）

2011年8月20日

BCP研究会　荒町　弘

BCPとシステム監査
（システム管理基準における事業継続計画）

Ⅳ.運用業務

ヒアリング
ドキュメント
現地視察
にて確認

－　4.データ管理
（1）データ管理ルールを定め、遵守すること。
（5）データのバックアップの範囲、方法及びタイミングは、業務内容、処理形態及びリカバリの方法を考慮して決定すること。
（8）データの保管、複写及び廃棄は、誤謬防止、不正防止及び機密保護の対策を講じること。
－　6.ソフトウェア管理
（4）ソフトウェアのバックアップの範囲、方法及びタイミングは、業務内容及び処理形態を考慮して決定すること。
－　7.ハードウェア管理
（2）ハードウェアは、想定されるリスクに対応できる環境に設置すること。
－　8.ネットワーク管理
（4）ネットワークは、障害対策を講じること。
－　9.構成管理
（1）管理すべきソフトウェア、ハードウェア及びネットワークの対象範囲を明確にし、管理すること。

現地視察
にて確認

－　10.建物・関連設備管理
（1）建物及び関連設備は、想定されるリスクに対応できる環境に設置すること。
（2）建物及び室への入退の管理は、不正防止及び機密保護の対策を講じること。
（3）関連設備は、適切な運用を行うこと。
（4）関連設備は、定期的に保守を行うこと。
（5）関連設備は、障害対策を講じること。
（6）建物及び室への入退の管理を記録し、定期的に分析すること。

BCPとシステム監査
（システム管理基準における事業継続計画）

Ⅵ.共通業務　－　1.ドキュメント管理
1.1 作成（5）
（1）ドキュメントは、ユーザ部門及び情報システム部門の責任者が承認すること。
（2）ドキュメント作成ルールを定め、遵守すること。
（3）ドキュメントの作成計画を策定すること。
（4）ドキュメントの種類、目的、作成方法等を明確にすること。
（5）ドキュメントは、作成計画に基づいて作成すること。

重要業務システムごとに未整備部分を見直しして再度整備

※システム管理基準（2004年　第2回改訂版）を参照してのアプローチを行った。

IT-BCP体験セミナー

１．セミナー名称　：　ＩＴ－ＢＣＰ体験セミナー
２．開催日時　　：　２０１４年１０月２５日（土）１３：００～１７：００
３．開催場所　　：　大阪大学中之島センター　講義室３０３
４．当日参加者　　：　受講者　　１０名
　　スタッフ　荒町、尾浦、金子、松井（ＢＣＰ研究プロジェクト）
　　広瀬、三橋、小河、鬼松、是松（セミナーグループ）

コース内容

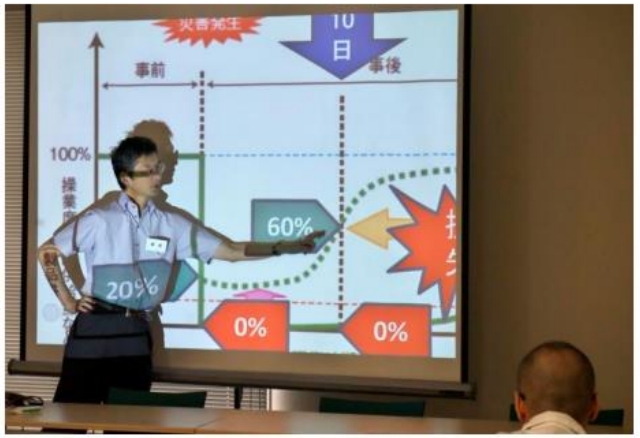
１．演習：災害発生直後の危機対応演習
初動対応の演習を通じて、ＩＴ部門はいざという時どのような判断が要求されるのか体験しグループ討議での気づきをもとにＩＴ-ＢＣＰの重要性とポイントについて学びます。

２．講義：危機対策本部の実際　～～演習別解へのヒント～～
過去の大規模災害等における自治体の対策本部の実際を紹介しながら、ＢＣＰの発動から、本部設置、活動継続における実効性向上について提言します。

３．講義：訓練・演習で鍛える IT-BCP
IT-BCP 訓練・演習の実施状況から、某社での実機を使った訓練の紹介、有効な机上訓練のやり方としてIT 版 DIG(*)の実践を提言します。　(*)DIG・・・災害図上訓練の一手法（DisasterimaginationGame）

（抜粋）日本システム監査人協会報　2015 年 1 月号　No166

１．セミナー名称　：　ＩＴ－ＢＣＰ体験セミナー
２．開催日時　　：　２０１５年６月２７日（土）１０：００～１７：００
３．開催場所　　：　大阪大学中之島センター　６０８教室
４．当日参加者　　：　受講者　　７名
　　スタッフ　荒町、松井、金子、尾浦、伊藤（ＢＣＰ研究プロジェクト）
　　広瀬



（１）講義　「災害初動の基礎知識」～情報収集力と防災想像力を高める～
（２）演習　「巨大地震発生！！その時ＩＴ部門はどうする？」
【ケースシナリオ】
・舞台：近畿圏に30店舗のスーパーを営む従業員数1800人の会社
・災害：南海沖で地震発生！　本社（大阪）震度５強
・貴方：システム課の課員
（３）講義　「ＩＴ－ＢＣＰの現状と危機対応の原理原則」～想定外への対応～

（抜粋）日本システム監査人協会報　2015 年 9 月号　No174

IT-BCP体験セミナー

1．セミナー名称　：　ＩＴ－ＢＣＰ体験セミナー
2．開催日時　：　２０１６年7月３０日（土）１３：００～１７：００
3．開催場所　：　大阪市ＩＣＴ戦略室内　研修室
4．当日参加者　：　受講者　１６名
スタッフ　荒町、尾浦、金子、松井、伊藤（ＢＣＰ研究プロジェクト）
福本、三橋

1 オリエンテーション（担当：荒町氏）

2 講義１：「自治体ICT-BCPの現状と想定外への対応」
（担当：松井氏）

3 グループ演習　（担当：金子氏／尾浦氏（講評担当））
(1)演習１（災害発生直後の初動対応）
(2)演習２（ＩＴ－ＢＣＰのポイント検討）
(3)講師講評／演習の解説　（担当：尾浦氏・金子氏）

4 講義２：「自治体のための演習補講」
～地防計・全庁ＢＣＰとＩＴ－ＢＣＰ～　（尾浦氏）

5 講義３：「組織のＢＣＰを確実に動かすために必要な
もう一つの準備」
～職員の参集率と家族の危機管理～（伊藤氏）

（抜粋）日本システム監査人協会報　2016 年 10 月号　No187

ICT部門におけるBCPへの取り組みと課題

（１）「市町村のための業務継続計画作成ガイド」　内閣府　（平成27年5月）

地方自治体においてBCPは法定計画ではないため自治体ごとに記載内容が異なる事を踏まえ、「特に重要な6要素」として以下の項目を掲げている。

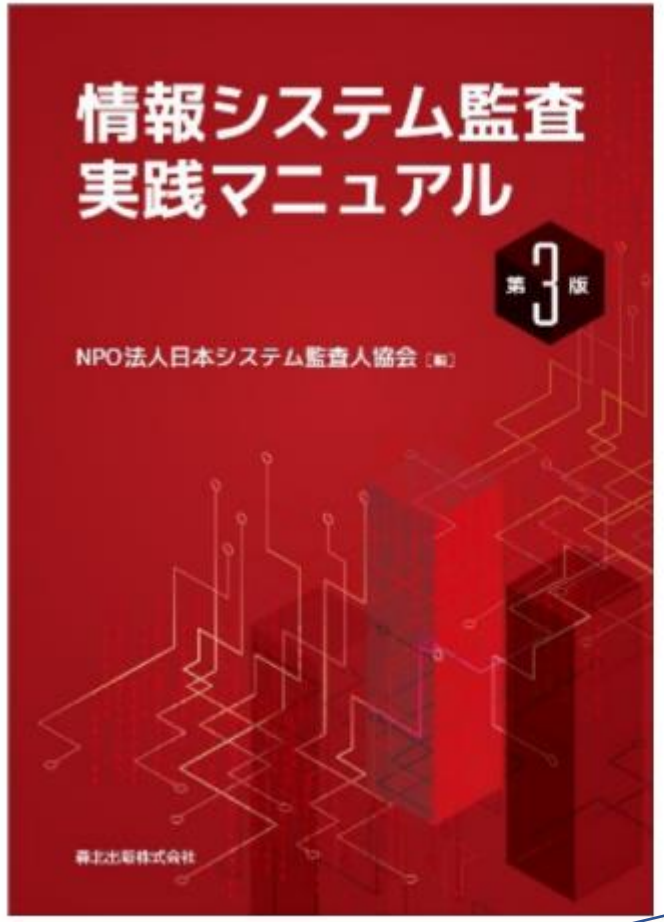
①首長不在時の明確な代替準備及び職員の参集体制
②本庁舎が使用できなくなった場合の代替庁舎の特定
③電気・水・食料等の確保
④災害時にもつながりやすい多様な通信手段の確保
⑤重要な行政データのバックアップ
⑥非常時優先業務の整理

	北海道K町	新潟県M市
CIOまたはIT統括責任者不在時の明確な代替準備及び職員の参集体制	△ 首長不在に関する記述はないが、職員の自動参集基準の記述はある。	○ 首長不在の代替基準、職員の参集体制について明確に記述されている
代替IT拠点の設定	×	○
代替IT資源（サーバー、ネットワーク）の確保	×	○
電気・水・食料等の確保	△ 水・食料の「確保」に関する記述がない。	△ 水・食料の「確保」に関する記述がない。
IT関連備品の確保	△（LANケーブル）	○（プリンタ、トナー）
LAN仮設作業	○	×（代替拠点が生きている前提）
重要な行政データのバックアップ	○「外部データ保管媒体」を前提とした記述があるので、外部保管が行われていると判断した。	○「外部保管さているバックアップデータ」を前提とした記述があるので、外部保管が行われていると判断した
重要情報システムの整理	×「優先順位をつけて復旧させるべきものから復旧させるように検討する」との記述があるので予め整理されていない模様。	○ 記述の該当部分は非公開になっているが、目次の中に「重要業務、重要システム・インフラ」という記述がある。
外部事業者への協力要請	○	○
被災者支援システム	×	○
災害対策本部設置にあたっての行動計画	○	×
訓練計画	○　毎年7月	○　毎年9月

（抜粋）日本システム監査人協会報　2018 年 2 月号　No203

情報システム監査実践マニュアル第3版（グループで執筆）

○本書の特徴



2020年6月12日　第3版第1刷　発行

1.テーマごとに監査(管理)のポイントを詳説

システム監査基準、管理基準の各項目をさらに掘り下げ、効率的・実践的な監査のポイントを 11 のテー マ別に解説。近年の社会情勢を踏まえ、IT ガバナンス、AI、アジャイル開発など、最近導入が進んでき た新しい監査テーマにも対応しています。

2.監査書類・監査チェックポイント集のダウンロードデータ付き

巻末には、監査書類の様式・作成例や監査チェックポイント集を掲載し、ダウンロードして実務で使える、書籍と対応した Web 資料も用意されています。

3.多様な執筆者陣

執筆者は、日本システム監査人協会の各研究会等で活動している会員に加え、平成30(2018)年版の基準の改訂作業に共同で参画したシステム監査学会、ISACA 東京支部の多数の会員が参画しており、日本におけるシステム監査関連 3 団体のノウハウが詰まっています。

【目次】

第1部 組織経営における情報システムの役割とシステム監査
第2部 システム監査の実践方法
第3部 システム管理基準の実践的な活用のポイント(11 の活用例)
第4部 システム監査の事例(4つの事例)
第5部 資料編(書式・監査評価のポイントを Excel ファイルで提供)

第3部　第10章 「レジリエンス認証制度とシステム監査」

テレワーク環境におけるBCPの考え方

（１）なぜサプライチェーンを考慮する必要があるのか？

ものづくりにかかわる製造業の場合、自社から見たサプライチェーンは、仕入取引先→仕入調達→運搬（入荷）→加工・組立等→運搬（出荷）→得意先へと続く供給連鎖となる。

自社になんのダメージがなくても、自社とつながる川上企業、川下企業がダメージを受けた場合、結果として事業を継続できなくなることが考えられる。例えば、仕入先が機能停止した場合、原材料の調達や外注加工がストップし、得意先が機能停止した場合、復旧するまで受注、納品が難しくなる。あるいは運送会社が機能停止した場合や、交通網など社会インフラに大きな被害が出た場合は、物流が機能しなくなり同様の結果となる。

<製造業におけるサプライチェーンのイメージ>

BCP を策定するにあたっては、自社内 のプロセスやリソースにかかわるリスク対策はもちろん重要であるが、そのビジネスが依存している外部環 境のプロセスや外部のリソースも考慮に入れる必要がある。

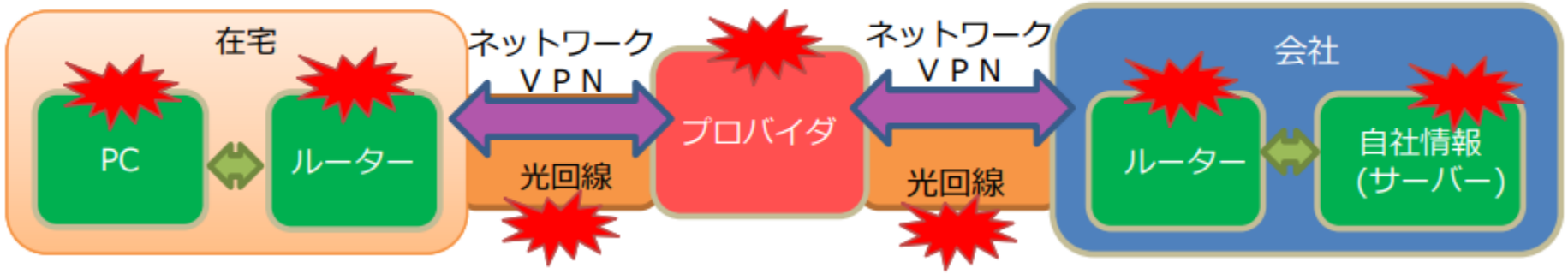
テレワーク環境におけるBCPの考え方

<テレワークにおける BCP の前提条件の違い（例）>

着眼点	拠点型のオフィス	テレワーク型のワークプレイス
被災の範囲	拠点単位に被災する	エリアで被災の程度が分かれる
初動の参集	可能であれば、拠点に参集する	可能であれば、在宅で業務を継続する
災対本部の設置	事業所内に災対本部を設置し統括管理	バーチャル環境に依存する場合もある
避難の指示	事業所の指示に従う	自治体の指示に従う
被害の受け方	拠点にあるものが一律に被害をうける	エリア・建物により被害状況が異なる
建物の強度	一般的に強固な構造	木造など脆弱な構造の場合がある
設備の復旧	組織的に復旧を試みる	単独で復旧を試みる
電源対策	予備電源がある場合がある	家庭では予備電源がない場合が多い
通信環境	予備回線がある場合がある	家庭では単独回線が多い
食料・水等	事業所で備蓄する	家庭で備蓄する

サプライチェーンを参考に、テレワークを取り巻く一般的な環境を、「情報のサプライチェーン（供給連鎖）」として置き換えてみると次のような構造になる。

<テレワーク環境における情報のサプライチェーンイメージ>



IT-BCP体験セミナー(BCAO共催)

1．テーマ　「IT-BCP 体験セミナー」

2．講師　【講義の部】細坪信二氏（BCAO 理事）　荒町弘氏（SAAJ 理事）
網本洋子氏（ISACA）
【演習の部】荒町弘氏（SAAJ 理事）

3．開催日時　2023 年 10 月 28 日（土） 13:00～17:30

4．開催場所　大阪会場（リアル会場）、東京会場（リアル会場）、Zoom（オンライン）

5．セミナー概要

日本システム監査人協会（SAAJ)と事業継続推進機構(BCAO)が連携し、事業継続（BC）の専門の視点とシステム監査の視点を融合して講義・演習を開催しました。27 名の参加者により、大阪・東京・オンラインのそれぞれの参加者は、講義の部は集合受講し、演習の部ではそれぞれチームに分かれての演習を行った。

【講義の部】「組織における BCP /IT- BCP とは、効果的な BCP /IT- BCP の策定について 」

1). 事業継続（BC）の基本 （講師：細坪信二）

2). 実効性のある BCP/IT- BCP とは（講師：荒町弘）

3). テレワークと BCP/ IT- BCP（講師：網本洋子）

【演習の部】「ケーススタディで学ぶ BCP/IT-BCP」

1). ケーススタディ（危機管理時の初動はどうすればよいの？）

2). 知識確認テスト（BCP/IT-BCP/テレワーク）

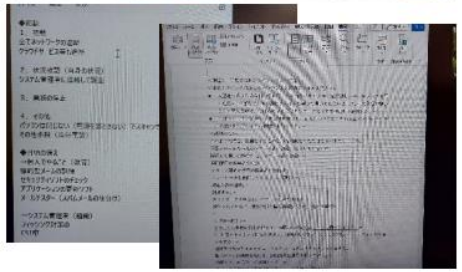
【演習の部】「ケーススタディで学ぶ BCP/IT-BCP」（危機管理時の初動はどうすればよいの？）

各チームに分かれて以下３つのケースについて内容検討の上、代表者による発表をそれぞれ行った。大阪・東京・オンラインのそれぞれのチーム（計６チーム）により活発な議論、意見交換を行われた。

（1） 自然災害に遭遇した場合の初動

（2） サイバーセキュリティ被害にあったケースを考える

（3） 生産性向上とセキュリティ対策の両立を考える



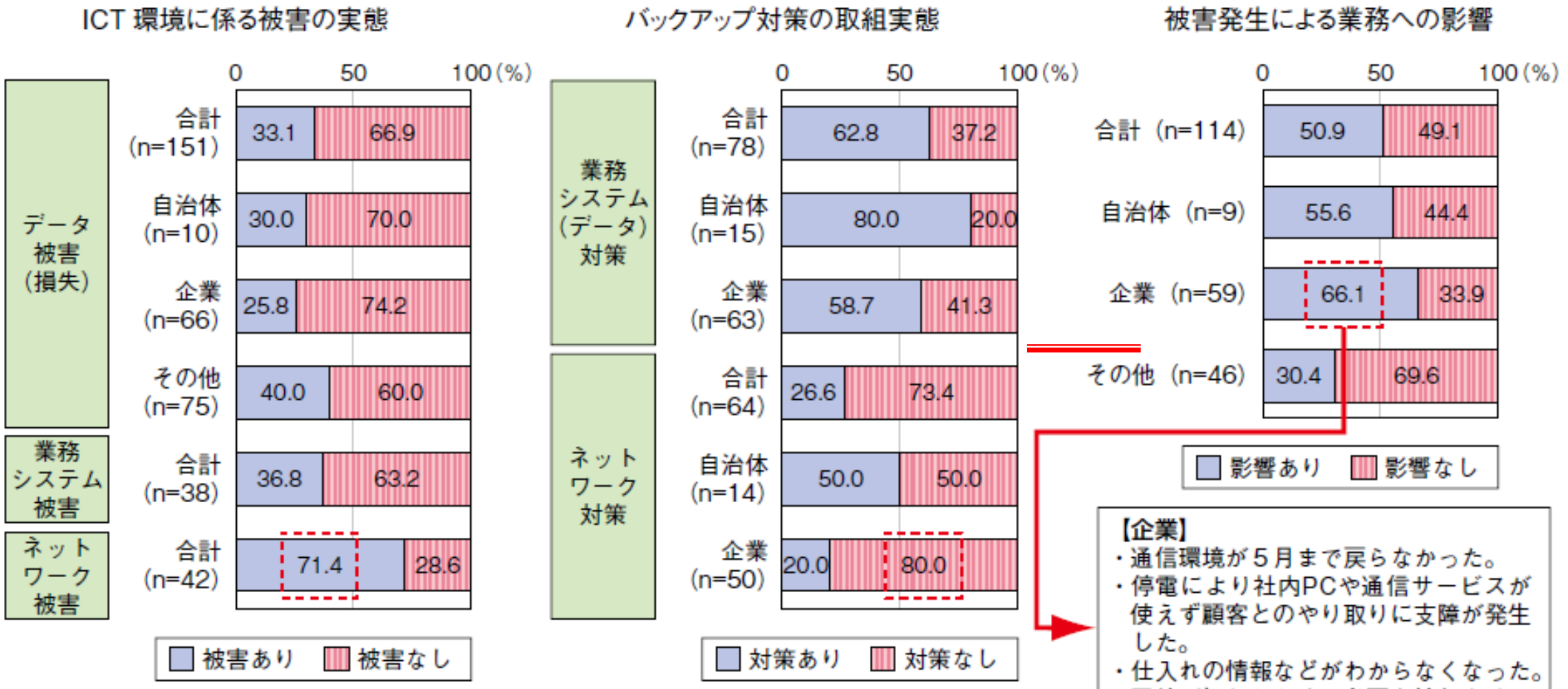
リアル参加（大阪＆東京）及びオンライン参加（Zoomミーティング）によるハイブリッドでのセミナー開催は初の試みであったが、オンラインイベントに慣れたBCAOとの共同運営によりグループに分かれての演習も円滑に運営することができた。今後も、BCAOとの協力関係を継続していく。

（抜粋）日本システム監査人協会報　2023 年 11 月号　No273

IT-BCPとシステム監査
実効性のあるIT-BCPの要件

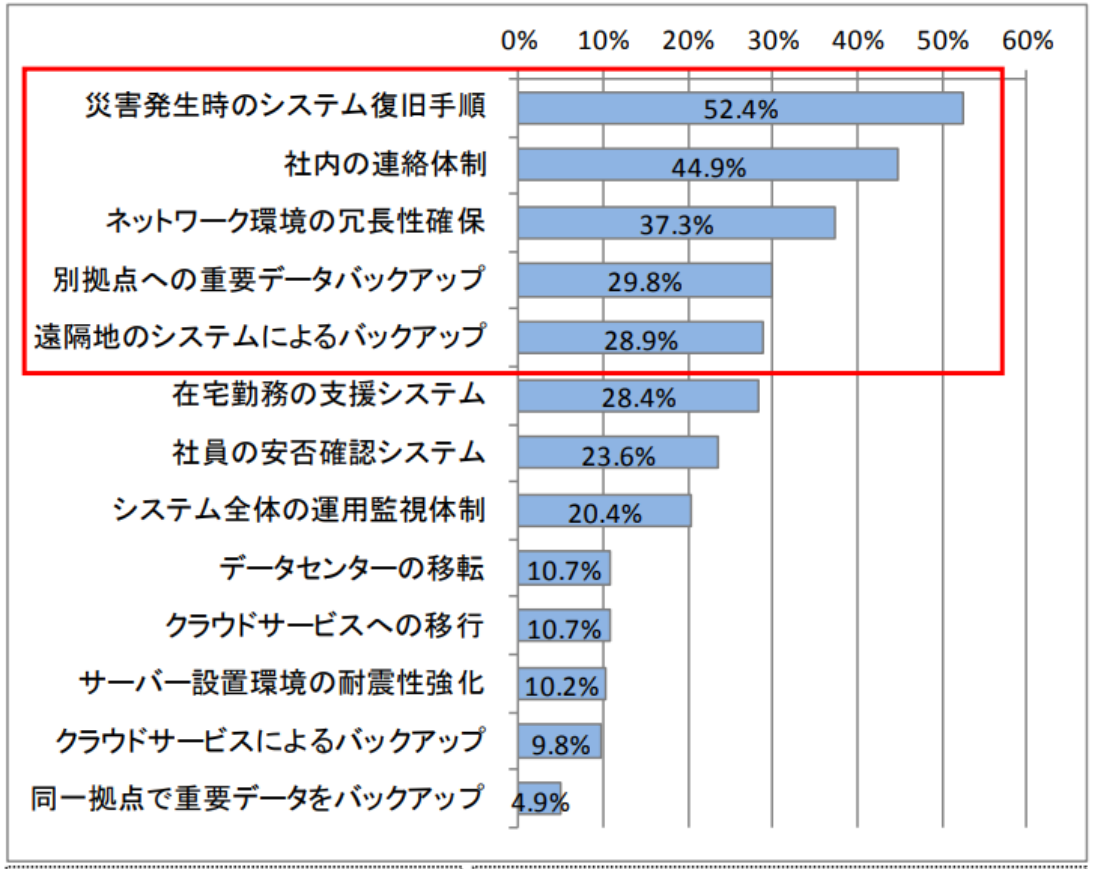
＜参考＞　IT-BCPの実効性に関する検証

東日本大震災で情報システムへ被害 ～ 業務に影響



（出典）総務省「災害時における情報通信の在り方に関する調査」（平成 24 年）

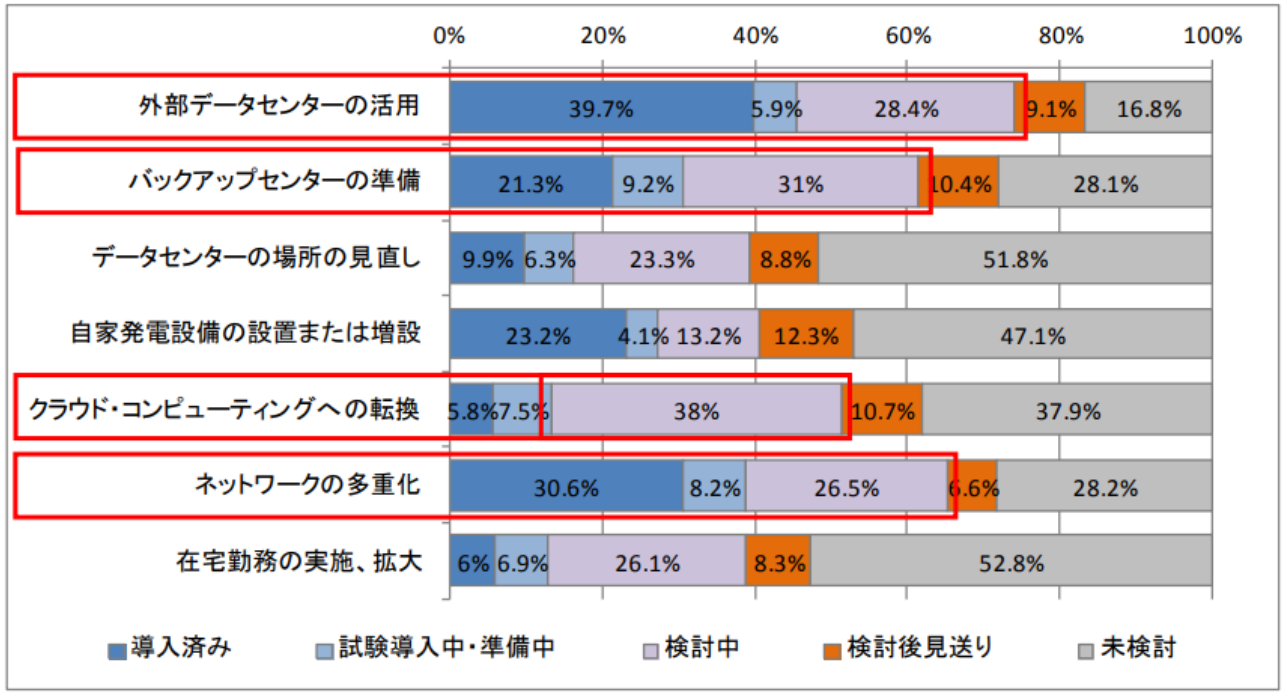
＜参考＞　東日本大震災後のIT基盤の認識



○調査時期:2011 年 3 月 30 日～4 月 5 日　○調査対象:『日経コミュニケーション』誌読者モニター225 社

出所:日経 BP 社『IT で実現する震災・省電力 BCP 完全ガイド』(2011 年 7 月)(初出:『日経コミュニケーション』2011 年 5 月号)

図 2-9 システム環境の災害対策で見直したい点(n=225)



○調査時期:2011 年 10 月 29 日～11 月 21 日　○調査対象:東証一部上場企業とそれに準ずる企業の計 4,000 社(各 IT 部門長宛送付)

出所:日本情報システム・ユーザー協会「企業 IT 動向調査 2012」(2012 年 3 月)
(掲載 URL:http://www.juas.or.jp/servey/it12/index.html)

図 2-10 BCP 策定・見直しのポイント(n=944)

出展：情報システム基盤の復旧に関する対策の調査報告書（2012年7月　独立行政法人情報処理推進機構）

情報システム基盤の復旧における検討ポイントとして以下が認識できる

「システムの分散管理（データセンター・クラウド活用）」「重要データの遠隔地バックアップ」
「ネットワークの冗長化（代替手段）」「バックアップオフィス（代替運用）」
「緊急時の連絡・初動体（組織体制）」

＜参考＞　企業におけるBCPの策定状況

事業の継続が困難になると想定しているリスク（複数回答）

		2023年					2022年			
		全体	大企業	中小企業	対前年（全体）		全体	大企業	中小企業	対前年（全体）
1	自然災害（地震、風水害、噴火など）	71.8	81.4	69.3	+0.8		71.0	80.0	68.5	−1.4
2 ↑	設備の故障	41.6	38.4	42.5	+4.0	↑	37.6	33.4	38.7	+1.8
3 ↓	感染症（インフルエンザ、新型ウイルス、SARSなど）	40.4	47.6	38.5	−13.1		53.5	58.5	52.1	−6.9
4 ↓	情報セキュリティ上のリスク	38.1	49.1	35.2	−1.5	↑	39.6	48.7	37.0	+6.7
5 ↑	物流（サプライチェーン）の混乱	34.7	38.7	33.7	+4.3	↑	30.4	29.8	30.6	+5.0
6 ↓	火災・爆発事故	34.1	38.3	33.0	+1.2		32.9	35.3	32.3	+0.1
7 ↓	自社業務管理システムの不具合・故障	32.0	38.7	30.2	+1.6	↑	30.4	35.2	29.1	+1.8
8 ↑	取引先の被災	31.4	31.8	31.3	+5.3	↓	26.1	24.7	26.5	−2.4
9 ↓	情報漏えいやコンプライアンス違反の発生	27.0	34.7	25.0	−1.9	↑	28.9	36.2	26.9	+2.5
10 ↓	取引先の倒産	25.7	20.3	27.2	−0.6	↓	26.3	21.8	27.5	−3.7
11	戦争やテロ	18.1	16.9	18.5	−0.9	↑	19.0	18.5	19.1	+6.0
12	経営者の不測の事態（経営者自身が被災し出社できないなど）	17.8	13.1	19.1	+0.2	↓	17.6	12.6	19.0	−0.8
13	製品の事故	16.8	16.2	16.9	+0.5	↓	16.3	16.5	16.3	−1.5
14	環境破壊	5.5	5.6	5.5	+0.1		5.4	5.0	5.5	−0.3
	その他	1.4	0.9	1.6	+0.4		1.0	0.3	1.2	−0.5

↑↓ 順位の変動（対2022年）　　↑↓ 順位の変動（対2021年）

出典　：　帝国データバンク調査「事業継続計画（BCP）に対する企業の意識調査」

企業の事業継続に関するリスク着眼点がサプライチェーンに遷移

新型コロナ禍を経てテレワーク等の代替手段による業務遂行は定着した

＜参考＞　企業におけるBCP策定状況

事業中断リスクに備えた実施・検討内容
（複数回答、上位10 項目）

(%)

		2023年5月		
		全体	大企業	中小企業
1	従業員の安否確認手段の整備	68.2	79.6	65.1
2	情報システムのバックアップ	57.1	68.2	54.1
3	緊急時の指揮・命令系統の構築	41.0	50.5	38.4
4	災害保険への加入	38.3	38.2	38.3
5	事業所の安全性確保（建物の耐震補強、設備の転倒・落下対策など）	35.6	43.7	33.4
6	調達先・仕入先の分散	34.4	31.5	35.2
7	多様な働き方の制度化（テレワーク、時差出勤、サテライトオフィスなど）	23.1	32.5	20.5
8	生産・物流拠点の分散	19.4	22.7	18.4
9	代替生産先・仕入先・業務委託先・販売場所の確保	17.7	15.8	18.3
10	業務の復旧訓練	14.6	21.0	12.9

注1:網掛けは、「大企業」と「中小企業」の比較で割合が高い規模を示す

注2:母数は、事業継続計画(BCP)を「策定している」「現在、策定中」「策定を検討している」のいずれかを選択した企業5,550社

出典　：　帝国データバンク調査「事業継続計画（BCP）に対する企業の意識調査」

企業のリスク対応ポイント着眼点がサプライチェーンに遷移

業務の復旧訓練については、取組み度合いが低い状況にある

＜参考＞　企業におけるBCP策定状況（2023年）

BCP を策定していない理由（複数回答）

(%)

		2023年5月		
		全体	大企業	中小企業
1	策定に必要なスキル・ノウハウがない	42.0	47.6	41.4
2	策定する人材を確保できない	30.8	36.4	30.2
3	策定する時間を確保できない	26.8	32.8	26.2
4	書類作りで終わってしまい、実践的に使える計画にすることが難しい	26.3	30.6	25.9
5	自社のみ策定しても効果が期待できない	23.8	25.2	23.7
6	必要性を感じない	20.9	14.4	21.6
7	リスクの具体的な想定が難しい	18.5	17.8	18.5
8	策定する費用を確保できない	13.4	8.5	13.9
9	ガイドライン等に自組織の業種に即した例示がない	4.9	4.3	5.0
10	策定に際して公的機関の相談窓口が分からない	3.3	1.3	3.5
11	策定に際してコンサルティング企業等の相談窓口が分からない	2.3	1.8	2.3
	その他	3.2	2.9	3.2

注1:網掛けは、「大企業」と「中小企業」の比較で割合が高い規模を示す

注2:母数は、事業継続計画(BCP)を「策定していない」企業4,910社

出典：帝国データバンク調査「事業継続計画（BCP）に対する企業の意識調査」

BCP策定の必要性は理解するものの優先順位は低くなりがちである

人材・スキル・ノウハウ不足等の事情が多く、実効性確保による効果認識が薄い

実効性のあるBCP/IT-BCPの要件

前提条件）
　経営陣や全社員において、自社の事業活動が「企業の社会的責任（CSR）を果たすため」の活動であることを理解し、活動を停滞させないことで社会貢献を継続するという認識が必要。

目的）
　組織の事業活動を継続することで社会貢献を継続する。

取組み）
　経営者のリーダーシップのもと、事業活動の継続性を保つ取組みを行う。

- 経営者自身が経営戦略／IT戦略と整合性を持つ事業継続計画「全社BCP／IT-BCP」を策定していること（**経営陣の参画性**）。
- 全社BCP／IT-BCPにおいては、自社の中核事業となる事業から優先度を付けた事業継続計画が策定できていること（事業継続計画における重要業務の優先順位付け）。
- 重要業務の優先順位に沿った、BCP及びIT-BCPにおいては、訓練と定着が重要。
- 全社BCP／IT-BCPの実効性を担保するために、継続的な社員教育と訓練を計画的に実施していること（PDCAサイクルによる運用の定着）。
- 業務に従事する**社員全員が全社BCP／IT-BCPを理解**し、日常業務における軽微なインシデント発生時においても、自ら判断し、適切な初動が行える等、**企業文化として定着していること（初動対応の全社的定着）**。

経営陣の参画性を高めるための取組み

全社BCP及びIT-BCP整備の必要性は認識されつつあるが、経営陣による主体的な関与を対外的に示す方法として、国の機関が定める各種認証制度への対応を行うことも有効だと考える。

候補の例として、情報システム監査実践マニュアル（第３版）第３部１０章に記載している「レジリエンス認証」（国土交通省）の取得や、中小企業が策定した防災・減災の事前対策に関する計画を経済産業大臣が「事業継続力強化計画」として認定する制度などがある。

いずれも制度も認証や認定を受けた組織は金融的な優遇制度を利用可能となる他、災害対策をはじめとする教育サービスも受けられるものであるため、企業の事業継続に寄与するものであると考える。

政府は、2016年に、ＢＣＰの完成度にこだわらず、災害等の被害に対して強い回復力を持ち社会全体のレジリエンスの向上に寄与できる事業者を認証するガイドライン（「国土強靱化貢献団体認証の認証に関するガイドライン」）を制定し、「国土強靱化貢献団体認証（レジリエンス認証）制度」を創設した。

レジリエンス認証トップページ｜一般社団法人 レジリエンスジャパン推進協議会 (resilience-jp.biz)
https://www.resilience-jp.biz/certification/

中小企業が策定した防災・減災の事前対策に関する計画を経済産業大臣が「事業継続力強化計画」として認定する制度です。認定を受けた中小企業は、税制措置や金融支援、補助金の加点などの支援策が受けられます。

中小企業庁：事業継続力強化計画 (meti.go.jp)
https://www.chusho.meti.go.jp/keiei/antei/bousai/keizokuryoku.htm

経営陣の参画性を高めるための取組み

レジリエンス認証取得のメリット

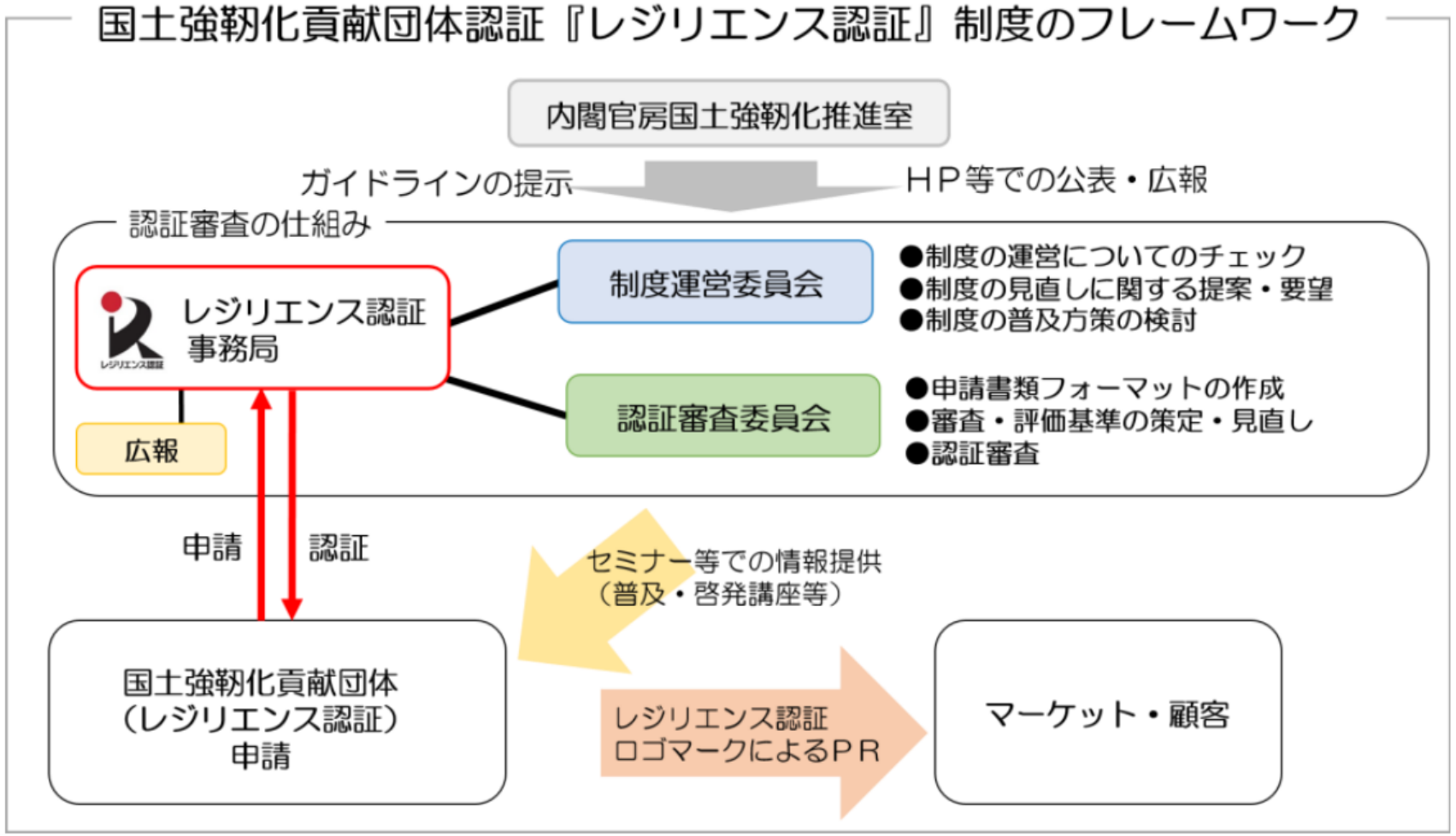
（1）自らの事業継続に関する取組を専門家の目で評価してもらうことにより、事業継続の更なる改善へのヒントを得ることが期待できます。

（2）交付を受けたレジリエンス認証マークを社員の名刺や広告等に付して、自社の事業継続のための積極的な姿勢を、顧客や市場あるいは世間一般に対してアピールすることができます。

（3）推進協議会や内閣官房国土強靱化推進室のホームページに認証取得団体として公表されます。（希望者に限ります。）

（4）推進協議会より、国土強靱化に関するセミナー・シンポジウムに関する情報が優先的に配信されます。

（5）金融機関等での優遇制度による取扱いを受けることができます。



出展：一般社団法人レジリエンスジャパン　ホームページ

レジリエンス認証制度の求める要件（審査基準）

レジリエンス認証の審査基準（事業継続関係）

（1）事業継続に係る方針が策定されている
企業の経営理念や経営方針に関連付けられた事業継続方針があること。

（2）事業継続のための分析・検討がされている
事業影響度分析及びリスク評価・分析を行い、重要業務とその目標復旧時間を明確にし、資源の脆弱性を把握している。

（3）事業継続戦略・対策の検討と決定がされている
（2）を踏まえ、目標復旧時間内に重要業務を継続・復旧させる戦略・対策を検討し、決定している。

（4）一定レベルの事業継続計画（BCP）が策定されている
目標復旧時間内に重要業務を継続・復旧させるための体制、手順等を示した計画が策定されている。

（5）事業継続に関して見直し・改善できる仕組を有し、適切に運営されている
事業継続に関して見直し・改善できる仕組みを有し、改善のための見直しが定期的に行われている。

（6）事前対策が実施されている
事業継続の実効性を高めるための事前対策が適切に行われている。

（7）教育・訓練を定期的に実施し、必要な改善が行われている
事業継続力を高めるための教育・訓練を定期的に実施し、必要な改善が行われている。

（8）事業継続に関する一定の経験と知識を有する者が担当している
事業継続に関する実務を 2 年以上積んだ実績がある者、または民間の機関が発行する事業継続に関する民間資格を保有する者が事業継続を担当している。

（9）法令に違反する重大な事実がない
国土強靱化に係る法令に関して、違反する重大な事実がない。

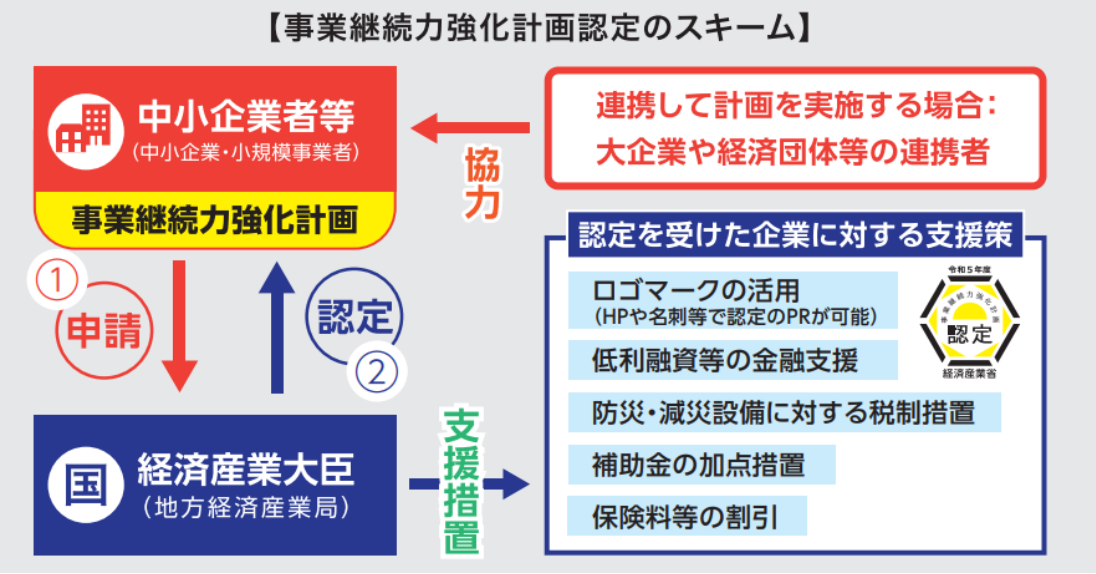
出展：情報システム監査実践マニュアル（第3版）

レジリエンス認証の要素をIT-BCP監査ポイントに加える

レジリエンス認証を参照・要約	IT-BCP監査のチェックポイント
1. 事業継続に係る方針が策定されていること	経営陣が定めた事業継続計画と整合を取った情報システムの業務継続計画を策定すること。 （システム管理基準Ⅷ.2.を参照）
2. 事業継続のための分析・検討がされていること	2. 情報システムに係る事業継続のリスクが，IT部門において分析・検討されていること。 （システム管理基準Ⅷ.1.を参照）
3. 事業継続戦略・対策の検討と決定がされていること	3. 情報システムに係わる事業継続戦略と対策が，IT部門において検討されているか。 （新規追加）
4. 一定レベルの事業継続計画（BCP）が策定されていること	4. 情報システムの事業継続計画が策定されていること。 （システム管理基準Ⅷ.2.を参照）
5. 事業継続に関して見直し・改善できる仕組を有し，適切に運営されていること	5. 情報システムに係る事業継続について，見直し改善できる仕組みを有し適切に運営されていること （新規追加）
6. 事前対策（施設の強化・装備品の確保等）が実施されていること	6. 情報システムの停止、破壊等による被害を最小にするために、建物及び関連設備は、想定されるリスクを回避できる環境に設置していること。 （システム管理基準Ⅴ.7.を参照）
7. 教育・訓練を定期的に実施し，必要な措置が取られていること	7. 情報システムの事業継続に係わる教育・訓練を定期的に実施し，必要な措置（見直し・改善）が取られていること。 （新規追加）
8. 事業継続に関する一定の経験と知識を有する者が担当していること	8. 情報システムの事業継続に関する一定の経験と知識を有するものが担当していること。 （新規追加）
9. 法令及び法令に基づく命令その他法令に違反する重大な事実がないこと	9. 情報システムに係わる法令及び法令に基づく命令その他法令に違反する重大な事実がないこと。 （新規追加）

出展：情報システム監査実践マニュアル（第3版）

経営陣の参画性を高めるための取組み



計画策定の５つのステップ

Step1　事業継続力強化の目的の検討

自然災害等が起こった際、サプライチェーンや地域経済社会に与える影響、従業員に対する責務等、自らの事業継続力強化が自然災害等による経済社会的な影響の軽減に資する観点から、目的を検討して記載します。

Step2　災害などのリスクの確認・認識

ハザードマップ等を活用し、事務所・工場などが立地している地域の災害等のリスクを確認。被災想定を基に、「ヒト」「モノ」「カネ」「情報」の4つの切り口から、自社にどのような影響が生じるかを考えます。

Step3　初動対応の検討

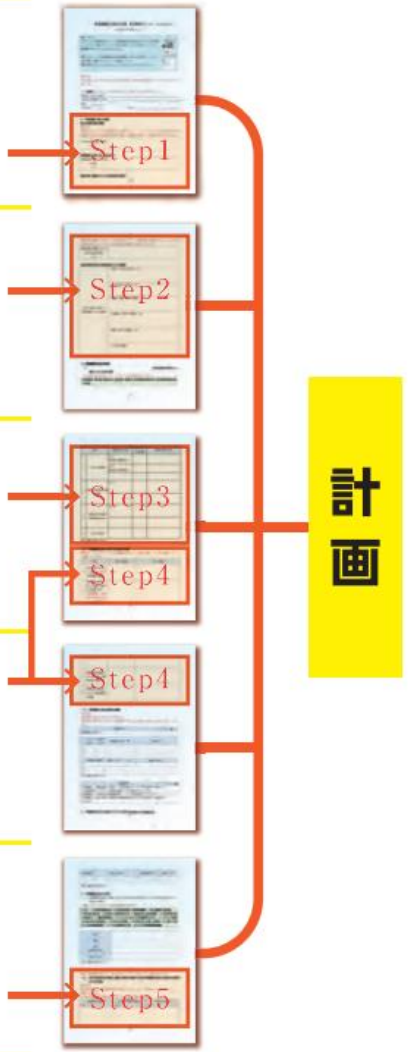
災害等が発生した直後の初動対応を検討します。その際、①人命の安全確保、②非常時の緊急時体制の構築、③被災状況の把握・被害情報の共有等の取り組みが求められます。

Step4　ヒト、モノ、カネ、情報への対応

Step2で検討したヒト、モノ、カネ、情報への影響を踏まえ、災害等に備えて事前にどのような対策を実行することが適当か検討します。

Step5　平時の推進体制

ジギョケイは策定するだけでなく、平時の取り組み（訓練）が大切です。平時から繰り返し取り組むことで、緊急時においても落ち着いて、適切に対応することができるようになります。



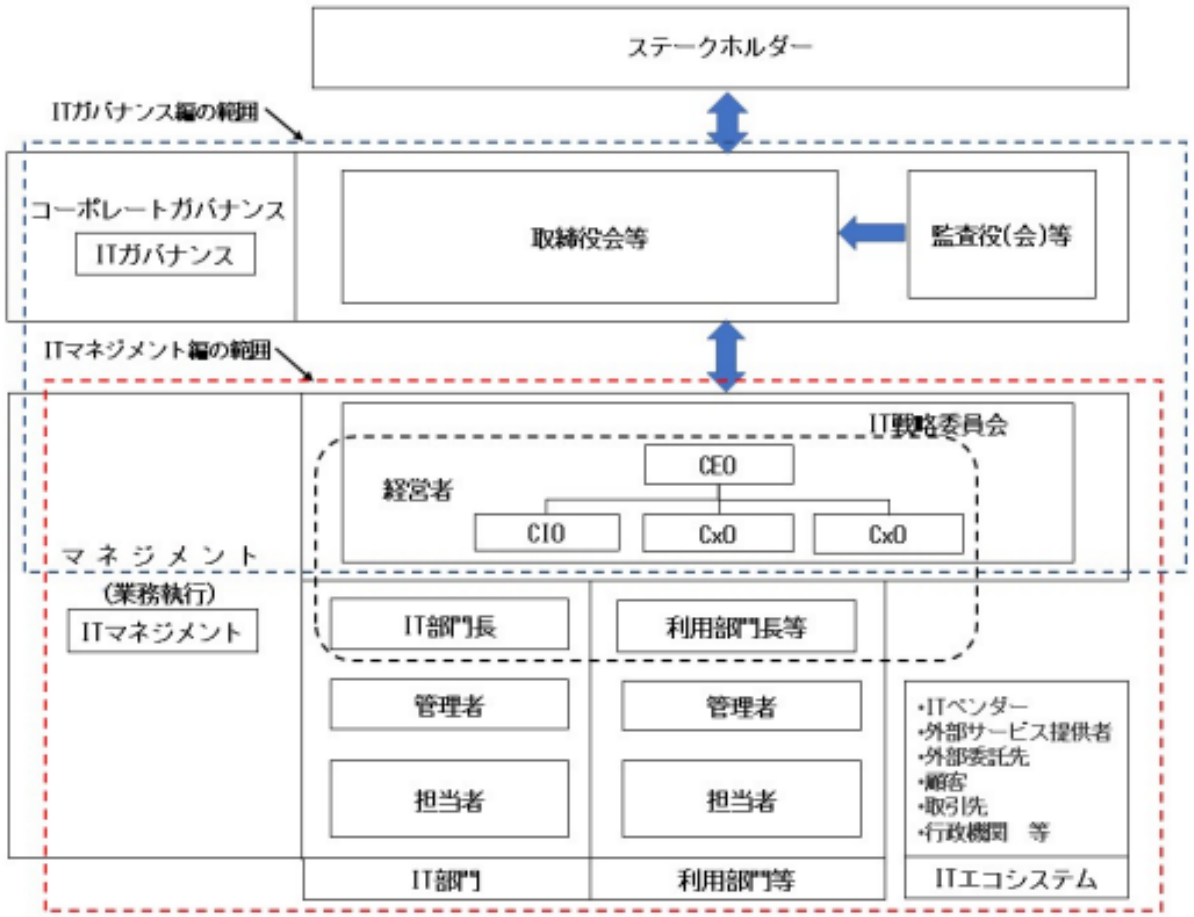
出典：事業継続力強化計画パンフレット（一部抜粋）

実効性のあるIT-BCPの要件（組織体制）

「基準」が想定する組織体の体制　（システム管理基準より抜粋）

基準では、**取締役会等が組織体のITシステムの利活用に関して責任を負う領域がITガバナンス**であり、**経営者が IT システムの利活用について責任を負う領域がITマネジメント**である」と定義している。

「取締役会等は、ステークホルダーのニーズに基づきITガバナンスを実践する実行責任と、ステークホルダーに対するITガバナンス全体の説明責任を負っており、組織体の目標を含む IT 戦略（IT ガバナンス方針と IT 基本計画）を示し、必要な実行組織の設置と適切な権限委譲を行い、経営者による実行状況のモニタリングを行う。」
「なお、監査役（会）等は、取締役会等に対する監査を行う。」
↓
実際には、取締役が経営の執行責任者を兼ねている組織が多い。事業継続性の確保は、企業の社会的責任を果たすための条件でもあるため、経営陣が負うステークホルダーへの説明責任を果たす要素となる。



事業者の規模においては、図に示したような組織が存在せず、情報システムの構築から運用までをITベンダー等に委託しているケースがある。この場合は、当該委託先を含めたパートナーシップのもと、図に示す役割分担にそれぞれの立場を当てはめて運用するのが良いと考える。

システム管理基準
システム管理基準ガイドラインの活用
（ITガバナンス）

IT-BCP監査　参照するガイドライン・基準等

システム管理基準の改訂の概要②

- ITガバナンス編の章構成・ITマネジメント編との関連、記載のポイントを以下に示す。

※同一の＜タグ名＞の記載がある項目について関連があることを意味する

大分類（編）	中分類（章）	小分類（節）	II. ITマネジメント編との関連※	記載のポイント
I．ITガバナンス	1. ITガバナンスの実践	1.1　経営戦略とビジネスモデルの確認	＜IT戦略ビジョン＞（経営戦略とビジネスモデル及びそのビジネス成果はITマネジメント全体と関連）	経営陣によるITガバナンスの実践のための直接的な活動に関わるプロセスを記載
		1.2　IT戦略の策定	＜IT戦略（ITガバナンス方針とIT基本計画）＞	
		1.3　効果的なITパフォーマンスの確認と是正	＜ITパフォーマンス評価＞	
		1.4　実行責任及び説明責任の明確化		
	2. ITガバナンス実践に必要な要件	2.1　ステークホルダーへの対応	＜IT戦略＞	ITガバナンスの実践を支える活動に関わるプロセスを記載
		2.2　取締役会等のリーダーシップ		
		2.3　データ利活用と意思決定	＜ITガバナンス方針＞	
		2.4　リスクの評価と対応	＜ITリスク管理方針＞ ＜事業継続に関する方針＞	
		2.5　社会的責任と持続性	＜ITガバナンス方針＞	

出展：システム管理基準（2023年4月26日改訂）

IT-BCP監査　参照するガイドライン・基準等

Ⅰ.2.4　リスクの評価と対応

組織体の目的及び IT 戦略の目標を達成するために、達成に及ぼす影響においてリスクを評価し、対応を行う。

＜達成目標＞

1. IT システムの利活用に関連する重要なリスクが認識され、速やかに対されている。
2. IT システムの利活用に関して、組織体が受容できるリスクのレベルが確にされ、管理されている。
3. 組織体内外の障害等に対応し、IT サービス等のレジリエンスが確保でき るよう対策されている。
4. IT システムの利活用に関する事業継続の方針が策定されている。

出展：システム管理基準（2023年4月26日改訂）

＜ガバナンス活動の例＞

1. （リスクの認識及び管理プロセスの確認）IT システムの利活用に関する重要なリスクを常に認識し、リスク管理が実施されていることを確認する。
2. （リスク対応とステークホルダーへの伝達）組織体が継続的にリスクを検知し、それに対応し、必要な対応策を関係するステークホルダーに伝える。
3. （IT リスク管理方針の開示及び IT サービスのレジリエンスの確保）組織体の目的を果たし、戦略的目標を確実に達成するために、IT リスク管理に関する組織体の方針を示すとともに、提供している IT サービス等のレジリエンスの確保を指示する。
4. （事業継続方針の策定）IT システムの利活用に関する事業継続の方針を策定する。

出展：システム管理基準ガイドライン（2023年8月10日公表）

IT-BCP監査　参照するガイドライン・基準等

Ⅰ.2.5　社会的責任と持続性

組織体が存続し、長期に成果を挙げ続けるために、IT システムの利活用に関する組織体の意思決定の透明性を確保し、より広範な社会的期待に応え、現在及び将来のステークホルダーのニーズを満足させるように組織体のデジタル活用能力を維持・向上させる。

＜達成目標＞

1. IT に関する意思決定を適切に行うため、本編に示した基準と整合する方針が策定され、意思決定の結果に対して組織体内での責任者が明確にされている。
2. IT を用いた自動的な意思決定のリスクを評価し、それに基づいて対策が講じられている。
3. ステークホルダーのニーズに応える上で有効な IT エコシステムが構築されている。
4. IT ガバナンス方針とその実践により、IT に関するリスクが増大する環境であっても、事業活動とデータが確実に保護されている。

出展：システム管理基準（2023年4月26日改訂）

＜ガバナンス活動の例＞

1. （ステークホルダーのニーズに関するリスクの特定）ステークホルダーの IT に関するニーズに影響を与えるリスクを特定し、リスクの内容と IT システムの利活用によるビジネスチャンスを明確にする。
2. （IT エコシステムへの適切な対応）組織体が長期にわたって持続的発展を行うために、組織体が利用している IT エコシステムのニーズを理解し、適時かつ効果的に対応する。
3. （自動的な意思決定への対応）IT を用いた自動的な意思決定については、その透明性を確保し、意図しない結果が生じた場合には、適切に対処する仕組みを構築して、社会的責任を果たすようにする。
4. （サービス品質の維持）IT システムの利活用によって必要な品質要件を満たすサービスの提供を維持し、組織体の目的と目標の達成に貢献する。
5. （IT サービスのレジリエンス確保）ビジネス機能が IT に依存していることを認識して、提供する IT サービスのレジリエンスを確保する。
6. （倫理的行動）組織体の IT システムの利活用は、倫理規範を遵守して行うとともに、ステークホルダーや経済・自然環境に悪影響を与えることがないように配慮する。

出展：システム管理基準ガイドライン（2023年8月10日公表）

経営陣の参画によるIT-BCP

経営陣とIT管理者及び従業員が一体となった「事業継続」に向けた取組みを行えていることを確認する。

想定リスク
1）大規模な自然災害や火災
2）感染症のパンデミック
3）社会インフラ
（電気，ガス，上下水道，通信等の障害）
4）情報システムの重大な障害
5）サイバー攻撃
6）情報漏洩
7）テロ等による破壊
8）本部，コンピュータセンター，拠点等への立ち入り不能　等

IT-BCP

自社の事業概要
IT-BCP策定の目的（事業継続方針）
事業活動に影響を与える事象（リスク）の分析
リスクの事業活動への影響度合い（範囲）
リスクの事業活動への影響度合い（損失）
情報システム等の脆弱性分析
優先復旧業務・システムの選定
必要な対策の実装

社員への周知
訓練計画策定・訓練実施

評価・見直し

全社BCP

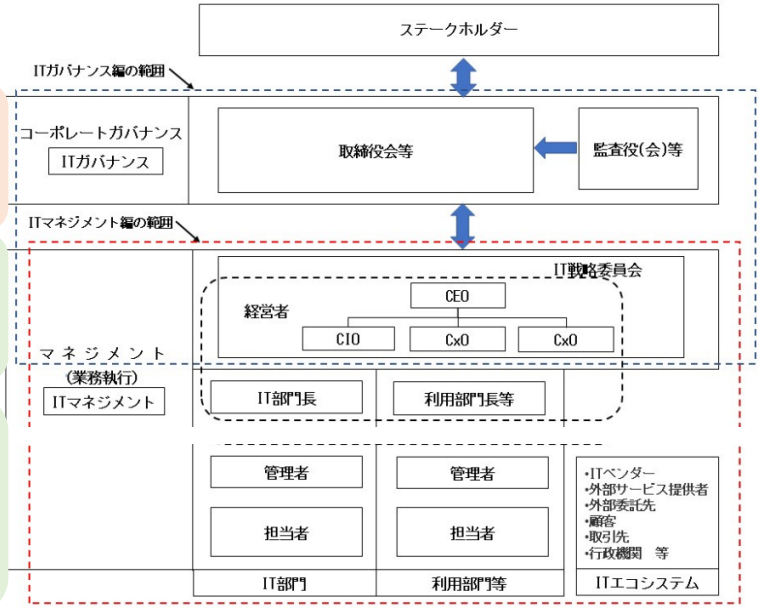
経営計画
事業計画

経営理念
ビジョン

経営
（ITｶﾞﾊﾞﾅﾝｽ）

業務執行
（ITﾏﾈｼﾞﾒﾝﾄ）

業務執行
（IT部門）
（利用部門）



経営陣は自社の事業継続に関する方針を明確に示し、株主や取締役等のステークホルダーに対して説明することが求められる。また、取引先等のサプライチェーンを構成するのステークホルダーとも相互に事業を停滞させないための取組みを共有するは企業価値の向上にも寄与すると考える。
ITへの依存性の高い情報システムについてはIT-BCPとしての事業継続計画の策定も求められる。

経営陣の参画によるIT-BCP
(ITに依存する業務の把握と運用形態)

自社の情報システムの運用形態をITガバナンス／ITマネジメント双方の視点で把握できていることを確認する。

　自社で全ての情報資産を管理するシステムとクラウドサービス等を活用して運用するシステムではシステム運用に関する「責任範囲」が異なる。
　業務の重要度に応じた、優先復旧対象システムの運用形態についても経営陣は把握しておく必要がある。

IT-BCP

自社の事業概要
IT-BCP策定の目的（事業継続方針）
事業活動に影響を与える事象（リスク）の分析
リスクの事業活動への影響度合い（範囲）
リスクの事業活動への影響度合い（損失）
情報システム等の脆弱性分析
優先復旧業務・システムの選定
必要な対策の実装

社員への周知
訓練計画策定・訓練実施

評価・見直し

経営（ITｶﾞﾊﾞﾅﾝｽ）

業務執行（ITﾏﾈｼﾞﾒﾝﾄ）

業務執行（IT部門）

自社の情報システム一覧・運用形態

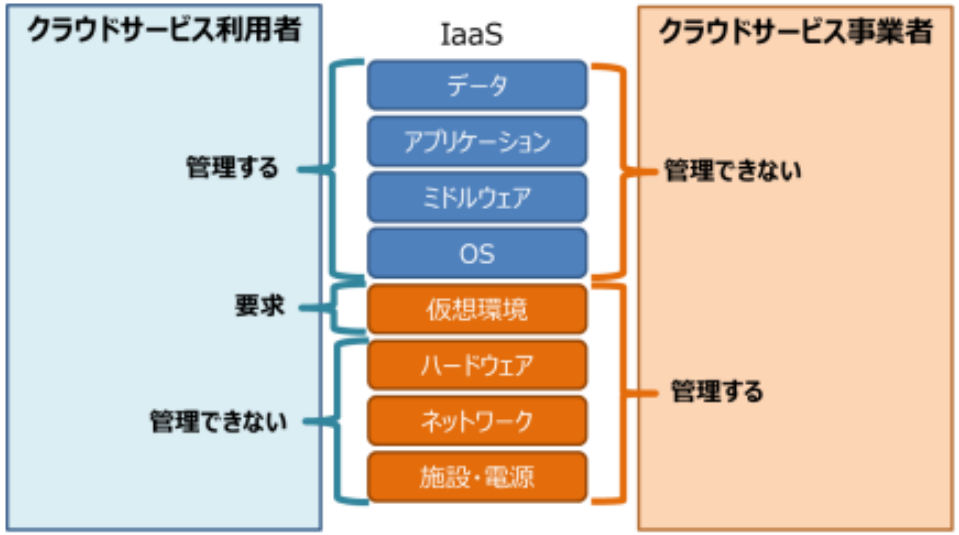
人事管理システム
販売管理システム
物流システム生産管理システム
購買管理システム
ネットワーク管理　等

	オンプレミス	IaaS	PaaS	SaaS
データ管理	○	○	○	○
アプリケーション	○	○	○	
ミドルウェア	○	○		
OS	○	○		
仮想基盤	○			
ハードウェア	○			
ネットワーク	○			
施設・電源	○			

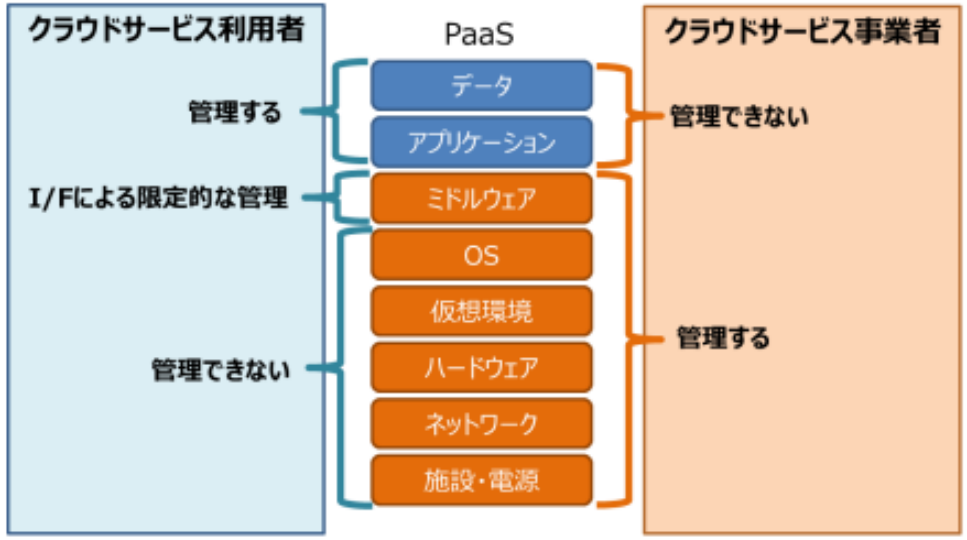
責任共有モデルによる責任範囲（総務省資料を参考とした）
○部分　→　自社が責任を持つ範囲　　網掛け部　→　事業者が責任を持つ範囲

自組織の利用するシステムにおける責任範囲を理解する

責任共有モデル



※ランタイムはミドルウェアの一部と位置付けています



※ランタイムはミドルウェアの一部と位置付けています

IaaS を利用するクラウドサービス利用者は、クラウドサービス事業者との契約・SLA に基づき、ゲスト OS[8]等が動作するための仮想環境の構築と管理をクラウドサービス事業者に要求できる。クラウドサービス利用者は、仮想環境上で動作している OS を含めたすべてのソフトウェアの管理を行う。OS やミドルウェア層での障害対応や、ミドルウェアに対するパッチ適応やぜい弱性対応などは、クラウドサービス利用者の責任となる。

クラウドサービス事業者は、仮想環境層以下の実装、設定、更新及び運用を管理するとともに、データセンター内のネットワークインフラも管理する。

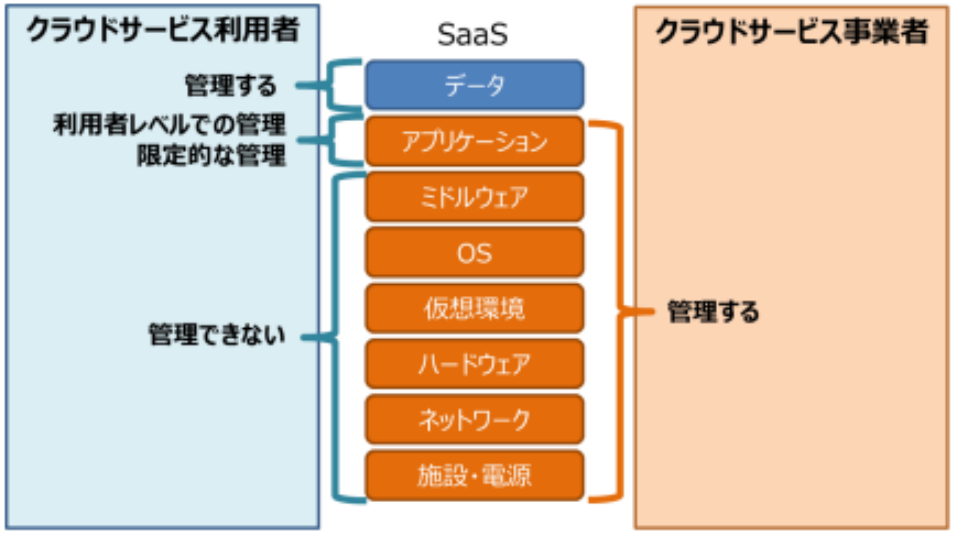
PaaSを利用するクラウドサービス利用者は、クラウドサービス事業者との契約・SLAに基づいて、アプリケーションの開発、アプリケーションに対する管理を行う。クラウドサービス利用者は、クラウドサービス事業者が提供するプログラミング環境やSQL[7]等のユーティリティインターフェースを利用してミドルウェア層を利用する。また、クラウドサービス利用者は、クラウドサービス事業者が提供するセキュリティ機能（データバックアップ機能、認証機能、データ暗号化機能、ファイアウォール機能、ログ管理機能等）を正しく理解して設定する必要がある。

クラウドサービス事業者は、ミドルウェア層以下の実装、設定、更新及び運用を管理するとともに、データセンター内のネットワークインフラも管理する。

出展：クラウドサービス提供における情報セキュリティ対策ガイドライン（第３版）

自組織の利用するシステムにおける責任範囲を理解する

責任共有モデル



※ランタイムはミドルウェアの一部と位置付けています

SaaS を利用するクラウドサービス利用者は、クラウドサービス事業者が提供するアプリケーションを利用するためのデータやアプリケーション上で生成したデータの管理（データに対する編集・削除等の行為）をする権限と責任を有する。アカウント管理などの限定的な管理権限をクラウドサービス事業者から付与され、外部からのアクセス権限を設定する場合がある。

（注）アプリケーションのバージョンアップや機能の追加により、設定が不適切なものとなってしまい、情報漏洩に至ることが想定されるため、クラウドサービス事業者は、クラウドサービス利用者がバージョンアップによる情報セキュリティへの影響を見定めることができるよう、適切な情報提供を行う必要がある。

クラウドサービス事業者は、契約・SLA に基づくサービスをクラウドサービス利用者に提供するために、アプリケーション層以下の実装、設定、更新及び運用を管理するとともに、クラウドサービス利用者に限定的な管理権限等を提供する場合がある。

出展：クラウドサービス提供における情報セキュリティ対策ガイドライン（第３版）

事業継続に関する監査ポイント

（1）経営陣は、情報戦略及び情報システムに関連した事業継続の方針を策定していること。	
＜主旨＞ 組織の事業継続性を確保するため、情報戦略や情報システムに関連した事業継続の方針を定める必要がある。	
① 経営陣は、情報戦略や情報システムに関連した事業継続の対象範囲を明確にしていること。	事業継続方針、事業継続計画の策定（更新）手順書
1）システムリスクアセスメント結果を基にするなど、合理的な範囲が設定されるルールとしていること。	事業継続方針、事業継続計画の策定（更新）手順書
② 経営陣は、情報戦略や情報システムに関連した事業継続の方針を策定し、文書化していること。	事業継続方針、事業継続計画の策定（更新）手順書
1）システムリスクアセスメント結果を基にするなど、合理的な要求水準が設定されるルールとしていること。	事業継続方針、事業継続計画の策定（更新）手順書
③ 事業継続の対象範囲には、災害時対応計画等も含むこと。	事業継続方針、事業継続計画の策定（更新）手順書
1）システムリスクアセスメント結果を基にするなど、リスクの観点はシステム障害、人的ミス、サイバーセキュリティ、災害などを考慮して作成すること。	事業継続方針、事業継続計画の策定（更新）手順書
④ 事業継続方針は、情報システム管轄役員以外の経営陣が確認・承認していること。	承認された事業継続計画
（2）事業継続計画は、利害関係者を含んだ組織的体制で立案し、経営陣が評価して承認していること。	
＜主旨＞ 事業継続にかかわる事象が発生した場合にすべての利害関係者が円滑に対応できるようにするため、利害関係者を含んだ組織体制で実行性の高い事業継続計画を立案し、経営陣が評価をして承認する必要がある。	
① 事業継続計画は、利害関係者を含んだ組織体制で立案していること。	事業継続計画の策定（更新）手順書 事業継続計画（システムリスク）の検討会議議事録 事業継続計画、組織図、組織規程
1）ビジネス全体の事業継続方針と統合・整合していること。	関係者ヒアリング、事業継続の方針、会社全体の事業継続計画との調整会議議事録、事業継続計画
2）システム部門単独で事業継続方針を決定していないこと。	事業継続計画
3）経営の役割・責任が明記されていること。	関係者ヒアリング、事業継続計画
② 事業継続計画を経営陣が評価して承認していること。	承認された事業継続計画

出展：情報システム監査実践マニュアル（第3版）

事業継続に関する監査ポイント

(3) 経営陣は、事業継続計画を、関係各部門への周知徹底を指示することと、その結果をモニタすること。	
＜主旨＞ 事業継続計画の実行性を高めるため、経営陣は事業継続計画を関係者に周知徹底する必要がある。	
① 経営陣は、周知徹底の方法を明確にしていること。	関係者ヒアリング、事業継続方針、事業継続計画
1)事業継続計画を基に、システム部門ではセキュリティ要件(二重化、バックアップ要件等)の見直しと課題対応、災害時の対応手順書(縮退運用)、復旧手順書等のマニュアル類の作成を行うことを指示していること。	関係者ヒアリング、事業継続方針、事業継続計画
2)事業継続計画を基に、ユーザ部門は手作業等で業務を行うためのマニュアルを整備することを指示していること。	関係者ヒアリング、事業継続方針、事業継続計画
3)関係者への周知・研修を実施するよう指示していること。	関係者ヒアリング、事業継続方針、事業継続計画
4)関係者により訓練を実施するよう指示していること。	関係者ヒアリング、事業継続方針、事業継続計画
5)訓練(災害対策テスト)により発見された課題に対応するよう指示していること。	関係者ヒアリング、事業継続方針、事業継続計画
② 経営陣は、周知徹底されたことをモニタリングしていること。	事業継続訓練の実施記録、訓練結果の経営への報告書 課題対応の進捗報告書
1)経営陣が訓練に参加していること。	事業継続訓練の実施記録
2)訓練の結果と課題について報告を受けていること。	課題対応の進捗報告書
3)主要な課題について進捗報告を受けていること。	課題対応の進捗報告書

出展：情報システム監査実践マニュアル（第3版）

システム管理基準
システム管理基準ガイドラインの活用
（ITマネジメント）

IT-BCP監査　参照するガイドライン・基準等

システム管理基準の改訂の概要⑥

- （続き）

※1 赤字は現行基準にも存在するプロセス、青字はJIS X 0170に存在しないプロセス
※2 同一の＜タグ名＞の記載がある項目について関連があることを意味する

大分類（編）	中分類（章）	小分類（節）※1	I. ITガバナンス編との関連 ※2	記載のポイント
II. ITマネジメント	7. 廃棄プロセス	7.1 廃棄計画	＜IT戦略＞	
		7.2 廃棄の実施		
		7.3 廃棄結果の検証		
	8. 外部サービス管理	8.1 外部サービス利用計画の策定	＜IT戦略＞	クラウドサービスを含む外部サービスの利用において留意すべき特有の事項をまとめて記載 外部サービスの利用効果については、「外部サービスの評価」を通じてITガバナンスへフィードバックされる
		8.2 外部サービスの選定と契約		
		8.3 外部サービスの運用管理		
		8.4 外部サービスの評価	＜ITパフォーマンス評価＞へのフィードバック	
		8.5 サービスレベル管理		
	9. 事業継続管理	9.1 リスクアセスメント	＜事業継続に関する方針＞	従来は、業務継続管理を対象としていたため、JIS Q 22301等を参考にして節を見直し 事業継続管理の結果については、「業務継続計画の評価及び見直し」を通じてITガバナンスへフィードバックされる
		9.2 業務継続計画の策定		
		9.3 業務継続計画の管理		
		9.4 訓練、演習及びテストの実施		
		9.5 業務継続計画の評価及び見直し	＜ITパフォーマンス評価＞へのフィードバック	

出展：システム管理基準（2023年4月26日改訂）

参照するガイドライン・基準等

Ⅱ.9.1　リスクアセスメント

情報システムに影響を与える重大事故、サイバー攻撃、災害、テロ等に対する対応策を具体化するため、影響範囲、業務の重要性及び緊急性を明確にし、復旧優先度を設定する。その際には、必要に応じて、地政学的要因やサプライチェーンに関連する要因についても考慮する。

＜達成目標＞

1. 情報システムに影響を与える脅威が洗い出され、リスク事象が特定されている。
2. リスク事象の発生時に、情報システムに生じる影響度が想定されている。
3. 事業の優先順位を踏まえて、優先して復旧する業務と情報システムの関連性が明らかにされている。
4. 優先して復旧する業務で利用する情報システムに対して、最大許容停止時間及び目標復旧時間が定められている。

出展：システム管理基準（2023年4月26日改訂）

＜管理活動の例＞

1. （リスク事象の特定）重大事故、サイバー攻撃、災害、テロ等の脅威を洗い出し、リスク事象を特定する。
2. （影響範囲の特定）リスク事象の発生時に情報システムに与える影響度を特定する。
3. （事業が被る影響度の分析）情報システムの停止等によって事業が被る影響度を分析し、それを踏まえて業務の復旧の重要度及び緊急度を分析する。
4. （優先業務と情報システムの関連性）業務復旧の優先順位と情報システムの復旧の優先順位の整合を取る。
5. （最大許容停止時間及び目標復旧時間の設定）業務復旧の優先度を踏まえて、効率的に業務を復旧するために、業務の最大許容停止時間及び目標復旧時間を定める。

出展：システム管理基準ガイドライン（2023年8月10日公表）

＜管理活動の例：1＞（リスク事象の特定）
重大事故、サイバー攻撃、災害、テロ等の脅 威を洗い出し、リスク事象を特定する。

＜リスク＞
脅威を洗い出し、リスク事象を特定しなければ、業務継続を実施するための業務継続計画を策定できない。
＜着眼点＞
① 重大事故、サイバー攻撃、災害、テロ等の脅威を洗い出し、リスク事象を特定する。
② 重大事故、災害等の脅威は、組織体全体の視点から可能な限り広範囲に洗い出す。

出展：システム管理基準ガイドライン（2023年8月10日公表）

(1) 情報システム部門長は、自然災害等のリスク及び情報システムに与える影響範囲を明確にすること。	
＜主旨＞ 情報システム部門長は、情報システムにかかわる災害時、テロによる破壊行為発生時及びサイバー攻撃の情報システムの対応策を具体化するため、地震、洪水、テロ及びサイバー攻撃等のリスク及び情報システムに与える影響範囲を明確にする必要がある。	
① 自然災害は、すべて想定するとともに、テロ等による破壊及びサイバー攻撃も含めていること。	事業継続計画(BCP)
想定されるリスクの洗い出し(例) 1) 大規模な自然災害や火災 2) 感染症のパンデミック 3) 社会インフラ(電気, ガス, 上下水道, 通信, 公共交通機関等)の障害 4) 情報システムの重大な障害 5) サイバー攻撃 6) 情報漏洩 7) テロ等による破壊 8) 本部, コンピュータセンター, 拠点等への立ち入り不能　等	リスク分析書、リスク評価書
② 被災の規模は、業務継続が困難となる規模を含めて想定していること。	事業継続計画(BCP)、リスク分析書、リスク評価書
③ 被災の想定は、地理的、組織的、物理的及び業務的視点から検証していること。	事業継続計画(BCP)、リスク分析書、リスク評価書
④ 想定した影響範囲について、将来を考慮していること。	事業継続計画(BCP)、リスク分析書、リスク評価書
⑤ 事業継続に関わる情報セキュリティ管理基準の該当事項を参照し確認すること。	事業継続計画(BCP)

出展：情報システム監査実践マニュアル（第3版）

・リスク分析のプロセスにおいて、過去のインシデント等の参考情報を収集したうえで自組織が直面した場合の被害想定が検討されていることを確認する。

＜管理活動の例：2＞（影響範囲の特定）
リスク事象の発生時に情報システムに与える影響度を特定する。

＜リスク＞
リスク事象の発生時に情報システムに与える影響度を特定しなければ、業務継続計画の策定において、対応策の優先順位付けが適切に行えない。
＜着眼点＞
① 影響度は、地理的、組織的、物理的及び業務的視点から評価し、業務継続が困難となるケースを含めて評価する。
② 影響度は、現在だけではなく将来を踏まえて評価する。
③ 外部サービス利用時の影響度は、例えば、情報システムの設置場所、バックアップデ ータの保管場所、外部サービス提供者が取得している認証等を考慮して評価する

出展：システム管理基準ガイドライン（2023年8月10日公表）

(2) 情報システム部門長は、情報システムの停止等により組織体が被る損失を分析すること。	
＜主旨＞ 情報システム部門長は、情報システムに係る被災の程度に応じた業務の復旧の重要性及び緊急性を明確にするため、情報システムの停止等によって組織体が被る損失について利害関係者を入れ、分析する必要がある。	
① 情報システムの停止及び機能縮退によって組織体が被る損失を分析する対象範囲には、影響を受ける業務を網羅していること。	事業継続計画(BCP)、リスク分析書、リスク評価書
② 利害関係者の合意を得ること。	事業継続計画(BCP)
③ 損失の分析は、組織体の損害及び社会的損害を明確にしていること。	事業継続計画(BCP)
④ 業務の復旧の重要性及び緊急性を明確にしていること。	事業継続計画(BCP)
⑤ 事業継続に関わる情報セキュリティ管理基準の該当事項を参照し確認すること。	事業継続計画(BCP)

出展：情報システム監査実践マニュアル（第3版）

・影響度の評価においては、中長期の経営計画（事業計画）等の内容を踏まえて行われていることを確認する。

＜管理活動の例：3＞（事業が被る影響度の分析）

情報システムの停止等によって事業が被る影響度を分析し、それを踏まえて業務の復旧の重要度及び緊急度を分析する。

＜リスク＞

情報システムの停止等によって事業が被る影響度を評価しなければ、業務継続計画において誤った優先順位付けを行い、業務継続が適切に行えない可能性がある。

＜着眼点＞

① 情報システムの停止及び機能縮退により影響を受ける業務を特定する。
② 影響度の評価には利用部門等の関係者を参画させる。
③ 影響度分析では、組織体の損害だけではなく社会的損害も含めて評価する

出展：システム管理基準ガイドライン（2023年8月10日公表）

・業務プロセスごとに、情報システムの停止によって発生する損失や影響を具体的に定義したうえで、業務の重要度や復旧に向けた優先度が検討されているかを確認する。
・影響度として、サプライチェーンに対する影響も考慮しているかを確認する。

＜管理活動の例：4＞（優先業務と情報システムの関連性）
業務復旧の優先順位と情報システムの復旧の優先順位の整合を取る。

＜リスク＞
業務復旧の優先順位と情報システムの復旧の優先順位の整合を取らなければ、業務継続計画で誤った優先順位付けを行ってしまう可能性がある。
＜着眼点＞
① 業務の優先順位を評価し、情報システムとの関連性を整理して、情報システムの優先順位を検討する。

出展：システム管理基準ガイドライン（2023年8月10日公表）

(3) 情報システム部門長は、業務の復旧許容時間及び復旧優先順位を定めること。	
＜主旨＞ 情報システム部門長は、情報システムにかかわる被災による業務の停止及び影響を最小限にとどめ、効率的に復旧するため、業務の復旧許容時間及び復旧優先順位を定める必要がある。	
① 復旧許容時間及び復旧優先順位の設定は、業務の重要性、緊急性、影響範囲及び他の業務との整合性及び実現可能性を考慮していること。	事業継続計画(BCP)、災害時対応体制図
優先順位付けする項目(例) 1) 継続すべき業務(手作業などの代替手段を含む)と継続を断念してもよい業務 2) システム，アプリケーション，データ 3) 拠点 4) 物的資産	
② 復旧許容時間及び復旧優先順位の設定理由を明確にしていること。	事業継続計画(BCP)、回復優先順位表
③ 復旧許容時間及び復旧優先順位を関係者が合意していること。	事業継続計画(BCP)、ヒアリング
④ 事業継続に関わる情報セキュリティ管理基準の該当事項を参照し確認すること。	事業継続計画(BCP)

出展：情報システム監査実践マニュアル（第3版）

・情報システムの構成や運用体制によっては、システム停止状態からの復旧が自組織だけで円滑に対応できない場合が考えられる。クラウドサービスを利用している場合は、責任共有モデルで示す利用形態等を考慮した復旧計画となっていることを確認する。（復旧に向けた取組みの主体者は自組織／事業者等）

＜管理活動の例：5＞（最大許容停止時間及び目標復旧時間の設定）

業務復旧の優先度を 踏まえて、効率的に業務を復旧するために、業務の最大許容停止時間及び目標復旧時間を定める。

＜リスク＞

業務の最大許容停止時間及び目標復旧時間を定めなければ、業務継続計画の策定におい て情報システムの優先順位付けを適切に行えず、業務継続に影響を及ぼす可能性がある。

＜着眼点＞

① 業務の最大許容停止時間及び目標復旧時間を踏まえて、情報システムの目標復旧時間 （RTO）、目標復旧レベル（RLO）、目標復旧時点（RPO）を検討する。

② 情報システムの復旧活動を支援するために必要な資源（ヒト・モノ・カネ）及びサプライチェーンにおける依存関係を考慮して検討する。

出展：システム管理基準ガイドライン（2023年8月10日公表）

・情報システムの構成や運用体制によっては、システム停止状態からの復旧が自組織だけで円滑に対応できない場合が考えられる。クラウドサービスを利用している場合は、責任共有モデルで示す利用形態等を考慮した復旧計画となっていることを確認する。（復旧に向けた取組みの主体者は自組織／事業者等）

参照するガイドライン・基準等

Ⅱ.9.2　業務継続計画の策定

重大事故、災害等の発生時に、適切な措置を迅速、円滑かつ確実に実行するために、情報システムの業務継続計画を策定する。

＜達成目標＞

1. リスクアセスメントの結果を踏まえて設定した復旧目標に基づいて、組織体の事業継続計画と整合が取れた情報システムの業務継続計画が策定され、承認されている。
2. 情報システムの業務継続計画の実効性が確保されている。
3. 情報システムの業務継続計画において、従業員の教育、訓練、関係者及び一般利用者に対するコミュニケーション等の方針が明確にされている。
4. 情報システムの業務継続計画が関係者に周知されている。

出展：システム管理基準（2023年4月26日改訂）

＜管理活動の例＞

1. （業務継続計画の策定）事業継続計画と整合が取れた情報システムの業務継続計画を策定する。
2. （業務継続計画の周知）情報システムの業務継続計画を関係者に周知する。
3. （業務継続計画の実現可能性）情報システムの業務継続計画の実現可能性を検証する。
4. （教育・訓練計画）関係者（外部委託先を含む）の教育・訓練計画を策定する。
5. （利用者及び関係者に対するコミュニケーション）関係者及び一般利用者に対するコミュニケーションの方針を明確にする。

出展：システム管理基準ガイドライン（2023年8月10日公表）

＜管理活動の例：1＞（業務継続計画の策定）
事業継続計画と整合が取れた情報システム の業務継続計画を策定する。

＜リスク＞
事業継続計画と情報システムの業務継続計画の整合が取れていなければ、災害及び重大事故発生時の業務継続に重大な影響を及ぼす可能性がある。
＜着眼点＞
① 業務継続計画の策定及び見直しのルールを定めて、事業継続計画と整合した業務継続計画を策定する。
② 業務継続計画には、発動基準、体制、要員、指揮命令系統、連絡手段、リソース調達、 バックアップ、代替処理対策、復旧対策、予算等を含める。
③ バックアップ（バックアップサイト、バックアップシステム、バックアップデータ等。 外部サービスを含む）は、同時被災しない場所となるように考慮する。
④ 将来の経営環境及び情報システムに関わる業務の変化に対応できるように柔軟性、拡張性を持つ計画を策定する。
⑤ 業務継続計画を承認する。
⑥ 事業継続に関わる情報セキュリティ管理基準の該当事項を参照する

出展：システム管理基準ガイドライン（2023年8月10日公表）

（1）情報システム部門長は、リスクアセスメントの結果に基づき、経営陣が定めた事業継続計画と整合を取った情報システムの業務継続計画を策定すること。	
＜主旨＞ 情報システム部門長は、災害及び重大事故発生時に混乱することなく、適切な措置を迅速に確実に実行するために、事業継続計画と整合した情報システムにかかわる業務継続計画を策定する必要がある。	
① 情報システム部門長は、業務継続計画の策定ルールを明文化すること。	業務継続計画書、コンティンジェンシープラン
② 情報システム部門長は、関係者と協議し、事業継続計画と整合した業務継続計画を作成すること。	事業継続計画（BCP）、業務継続計画書、コンティンジェンシープラン
③ 情報システム部門長は、業務継続計画に、バックアップ、代替処理対策、復旧対策等を記載されることを確保すること。	業務継続計画書、コンティンジェンシープラン
④ 情報システム部門長は、将来の経営環境及び情報システムにかかわる業務の変化を考慮して業務継続計画を作成すること	リスク想定シナリオ、リスク評価書、業務継続計画書、コンティンジェンシープラン

出展：情報システム監査実践マニュアル（第3版）

＜管理活動の例：1＞（業務継続計画の策定）
事業継続計画と整合が取れた情報システム の業務継続計画を策定する。

出展：システム管理基準ガイドライン（2023年8月10日公表）

(2) 情報システム部門長は、情報システムに係る災害及び重大事故発生時に対応した業務継続計画を作成し、承認を得ること。	
＜主旨＞ 情報システム部門長は、災害及び重大事故発生時に混乱することなく、情報システムに係る適切な措置を迅速に実行するため、経営陣が定めた災害及び重大事故発生時に対応した情報システムの業務継続計画を関係者に周知徹底する必要がある。	
① 情報システムに係る災害及び重大事故発生時に対応した業務継続計画が作成され、承認されていること。	業務継続計画書、コンティンジェンシープラン、稟議書
業務継続計画に盛り込む内容（例）（注）外部へ委託した業務も含む 1）想定する緊急事態と被害 2）影響を受ける業務 3） 業務の優先度 4） 代替手段を用いた業務の継続方法 5） 必要となるリソース 6） 緊急時体制（報告・連絡体制を含む） 7） 緊急時行動計画（初期対応・暫定対応・復旧対応） 8） 目標復旧時間・目標復旧水準 9） 教育・訓練、維持管理方法	
② 経営陣が業務継続計画を承認していること。	業務継続計画書、コンティンジェンシープラン、取締役会議事録
③ 情報システム部門長は、業務継続計画を関係者に周知徹底していること。	業務継続計画書、コンティンジェンシープラン配布先一覧
④ 事業継続に関わる情報セキュリティ管理基準の該当事項を参照し確認すること。	業務継続計画書、コンティンジェンシープラン
⑤ 業務継続計画作成にあたって、製造拠点・倉庫，本社（本部）・支社（支所）等の所在地について、ハザードマップ等，官公庁・自治体等が公表している災害等に関する資料を参照すること。	業務継続計画書、コンティンジェンシープラン

出展：情報システム監査実践マニュアル（第3版）

＜管理活動の例：2＞（業務継続計画の周知）
情報システムの業務継続計画を関係者に周知する。

＜リスク＞
業務継続計画が関係者に周知されていなければ、重大事故、災害等の発生時に業務継続計画を確実に実行できない。
＜着眼点＞
① 情報システムに係る業務継続計画を関係者に周知する。
② 業務継続計画の最新版を、関係者が必要なときに参照可能な状態で管理する。

出展：システム管理基準ガイドライン（2023年8月10日公表）

（5） 情報システム部門長は、業務継続計画を関係各部に周知徹底すること。	
＜主旨＞ 情報システム部門長は、情報システムにかかわる業務継続計画に定めた具体策を習熟し、確実に実行するため、従業員の教育訓練の方針及び計画を明確にし、業務継続計画の教育訓練を定期的に行う必要がある。	
① 業務継続計画に対応した訓練に基づいて、教育訓練を定期的に実施していること。	コンティンジェンシープラン訓練計画書、コンティンジェンシープラン訓練実施記録
② 教育訓練の結果を記録し、業務継続計画に反映していること。	コンティンジェンシープラン訓練実施記録、コンティンジェンシープラン訓練実施結果評価書
③ 事業継続に関わる情報セキュリティ管理基準の該当事項を参照し確認すること。	業務継続計画書、コンティンジェンシープラン
④ 教育訓練にあたっては、外部委託先との共同訓練も検討すること。	コンティンジェンシープラン訓練計画書
⑤ バックアップシステムが正常に稼働することを確認する訓練も実施すること。また、バックアップシステム稼働後の本番システムへの切り戻しと正常稼働の確認も行うこと。	コンティンジェンシープラン訓練計画書

出展：情報システム監査実践マニュアル（第3版）

・利用部門に対する確認事項として以下を確認する。
　システム利用部門の担当者が業務継続計画の内容についての理解ができているか。

＜管理活動の例：3＞（業務継続計画の実現可能性）
情報システムの業務継続計画の実現可能性を検証する。

＜リスク＞
業務継続計画の実現性を検証しなければ、災害及び重大事項発生時に業務を継続することができない。
＜着眼点＞
① 業務継続計画の実現可能性を検証し、必要な改善を行う。
② 検証は、関係者が参画して行う。

出展：システム管理基準ガイドライン（2023年8月10日公表）

(6) 情報システム部門長は、業務継続計画を必要に応じて見直すこと。	
＜主旨＞ 情報システム部門長は、情報システムにかかわる業務継続計画について、経営環境及び業務の変化等に対応して、実現可能性を保持するため、適時に見直しを行う必要がある。	
① 見直しのルールを明文化していること。	コンティンジェンシープランの維持管理手続
② 見直しによる変更は、理由が明確であること。	コンティンジェンシープラン見直しのレビュー結果
③ 変更した計画を経営陣が承認し、関係者に周知徹底させていること。	取締役会議事録、稟議書、関係者通達
④ 事業継続に関わる情報セキュリティ管理基準の該当事項を参照し確認すること。	業務継続計画書、コンティンジェンシープラン
⑤ 経営方針の変更、業務の重要性の変更及び人事異動・組織変更が発生した場合、業務継続計画の見直しを行うこと。	取締役会議事録、稟議書、コンティンジェンシープラン見直しのレビュー結果
⑥ 環境変化・情報技術の革新により、リスクシナリオなどの変化が生じた場合、業務継続計画の見直しを行うこと。	取締役会議事録、稟議書、コンティンジェンシープラン見直しのレビュー結果
⑦ 同業他社の重大障害事例等の情報を入手した場合、自社の業務継続計画の見直しを行うこと。	取締役会議事録、稟議書、コンティンジェンシープラン見直しのレビュー結果

出展：情報システム監査実践マニュアル（第3版）

＜管理活動の例：4＞（教育・訓練計画）
関係者（外部委託先を含む）の教育・訓練計画を策定する。

＜リスク＞
業務継続計画について、関係者（外部委託先を含む）に対する教育・訓練計画を策定しなければ、業務継続計画で定めた対策を確実に実施できない。
＜着眼点＞
① 業務継続計画の実効性を高めるために、関係者（外部委託先を含む）の教育・訓練の方針を明確にする。
② 教育訓練の方針を踏まえた関係者（外部委託先を含む）の教育・訓練計画を策定し、実施する。
③ 訓練の結果明らかになった課題は、業務継続計画の改善に反映させる。

出展：システム管理基準ガイドライン（2023年8月10日公表）

（5） 情報システム部門長は、業務継続計画を関係各部に周知徹底すること。	
＜主旨＞ 情報システム部門長は、情報システムにかかわる業務継続計画に定めた具体策を習熟し、確実に実行するため、従業員の教育訓練の方針及び計画を明確にし、業務継続計画の教育訓練を定期的に行う必要がある。	
① 業務継続計画に対応した訓練に基づいて、教育訓練を定期的に実施していること。	コンティンジェンシープラン訓練計画書、コンティンジェンシープラン訓練実施記録
② 教育訓練の結果を記録し、業務継続計画に反映していること。	コンティンジェンシープラン訓練実施記録、コンティンジェンシープラン訓練実施結果評価書
③ 事業継続に関わる情報セキュリティ管理基準の該当事項を参照し確認すること。	業務継続計画書、コンティンジェンシープラン
④ 教育訓練にあたっては、外部委託先との共同訓練も検討すること。	コンティンジェンシープラン訓練計画書
⑤ バックアップシステムが正常に稼働することを確認する訓練も実施すること。また、バックアップシステム稼働後の本番システムへの切り戻しと正常稼働の確認も行うこと。	コンティンジェンシープラン訓練計画書

出展：情報システム監査実践マニュアル（第3版）

・外部委託先の要員に異動や追加などの変更があった場合には、初期教育としての教育訓練が行われているか、利用部門に確認する。

＜管理活動の例：5＞（利用者及び関係者に対するコミュニケーション）
関係者及び一般 利用者に対するコミュニケーションの方針を明確にする。

＜リスク＞
関係者及び一般利用者に対するコミュニケーションの方針を明確にしなければ、災害及 び重大事項発生時に業務継続計画に定めた対策を円滑かつ確実に実行することができない。
＜着眼点＞
① リスク事象の発生前、発生時及び発生後における、関係者及び一般利用者に対するコミュニケーションの方針を明確にする。
② 事業の中断・阻害の発生時における、通信手段を確保する。
③ 外部機関との組織的なコミュニケーションを明確にする

出展：システム管理基準ガイドライン（2023年8月10日公表）

(4) 情報システム部門長は、業務継続計画の中で、従業員の教育訓練及びリスクコミュニケーションの方針を明確にすること。	
＜主旨＞ 情報システムにかかわる業務継続計画に定めた具体策を習熟し、確実に実行するため、従業員の教育訓練及びリスクコミュニケーションの方針を明確にし、訓練を定期的に行う必要がある。	
① 情報システムにかかわる業務継続計画に基づいて、教育訓練の方針を明確にしていること。	コンティンジェンシープラン訓練計画書
② 教育訓練の方針を踏まえた教育訓練計画を策定していること。	コンティンジェンシープラン訓練計画書
③ 災害及び重大事故発生時におけるリスクコミュニケーションの方針を明確にすること。	業務継続計画書、コンティンジェンシープラン
④ 事業継続に関わる情報セキュリティ管理基準の該当事項を参照し確認すること。	業務継続計画書、コンティンジェンシープラン
⑤ 災害及び重大事故発生時における対策本部の設置基準、組織の構成・役割および指揮命令系統を明確にすること。	緊急対策本部運営要領
⑥ 損害状況の把握・収集および伝達方法を定めること。	損害状況評価チェックリスト
⑦ 緊急時広報活動の事前準備（想定問答集、ホームページ掲載文、ポスターひな形等）を行うこと。	緊急時広報活動手続

出展：情報システム監査実践マニュアル（第3版）

・組織的なインシデント対応体制（CSIRT等）が整備されており、システム利用部門の従事者が理解できていることを確認する。

参照するガイドライン・基準等

Ⅱ.9.3　業務継続計画の管理

業務継続計画で定めた復旧目標を実現するために、情報システムのバックアップ及び代替処理を含む復旧手続及び体制の実現可能性を確保する。

＜達成目標＞

1. 業務の復旧目標に対応した、情報システムの構成要素についてバックアップ方法及び手順が定められている。
2. 代替処理を含む復旧手続及び体制の実現可能性が検証されている。
3. 情報システムの運用状況に対する監視機能が設けられ、情報システムの可用性が維持されている。
4. 情報システムの運用に要求される稼動率が確保され、情報システムの可用性が維持されている。

出展：システム管理基準（2023年4月26日改訂）

＜管理活動の例＞

1. （バックアップ手順の策定）情報システムを確実に復旧させるための業務の復旧目標に対応したバックアップ手順を定める。
2. （バックアップ手順の検証）定められたバックアップ手順の実効性を検証する。
3. （代替処理手続及び体制）情報システムが停止した場合、復旧するまでの間に業務を継続させるために必要な代替処理及び体制を定め、その実効性を検証する。
4. （復旧手続及び体制）停止した情報システムを円滑かつ確実に復旧させるための手続及び体制を定め、その実効性を検証する。
5. （運用状況の監視機能）情報システムの運用状況の監視機能を設ける。
6. （可用性の維持）情報システムの運用に要求される稼動率を確保し、可用性を維持する。

出展：システム管理基準ガイドライン（2023年8月10日公表）

＜管理活動の例：1＞（バックアップ手順の策定）
情報システムを確実に復旧させるため の業務の復旧目標に対応したバックアップ手順を定める。

＜リスク＞
情報システムに関わる業務の復旧目標に対応したバックアップ手順が定められていなければ、復旧作業を効率的かつ確実に実施できない。
＜着眼点＞
① 業務別にバックアップ対象を明確にし、関連業務のバックアップとの整合を取る。
② 業務の復旧目標に対応したバックアップ手順を定め、権限者の承認を得る。

出展：システム管理基準ガイドライン（2023年8月10日公表）

（1）情報システム部門長は、情報システム、データ及び関連設備のバックアップ方法及び手順を業務の復旧目標に対応して定めること。	
＜主旨＞ 情報システム部門長は、情報システムにかかわる復旧作業の効率及び経済性を考慮して、確実に復旧させるため、業務の復旧目標に対応して、バックアップ方法及び手順を定める必要がある。	
① 業務別にバックアップの対象を明確にし、関連業務のバックアップとの整合を図っていること。	システム別業務別復旧手順書、バックアップ手順書
② 業務の復旧許容時間及び復旧順位に対応して、バックアップ方法及び手順を定めていること。	システム別業務別復旧手順書、バックアップ手順書
バックアップを取得するにあたっての留意事項（例） 1）適切な世代管理レベル（二世代前、三世代前まで等）を設定すること。 2）回復に要する時間及びその間の影響を考慮して、取得サイクルを定めておくこと。 3）バックアップが正常に取得できていることを確認すること。 4）必要に応じてバックアップ取得対象範囲の見直しを行うこと。例えば、データベースの拡張やファイルの新設を行った場合等。	
バックアップ保管方法 1）分散保管：バックアップファイルを同一建物内もしくは比較的近距離の場所で保管する（火災等、局所災害に有効）。 2）隔地保管：バックアップファイルを遠距離の場所で保管する（地震等、大規模災害に有効）。	
③ バックアップ要員及び予算を確保していること。	業務継続計画書、コンティンジェンシープラン
④ 復旧作業に必要なドキュメントのバックアップは定期的に整備すること。また、重要な変更は速やかに反映すること。	システム別業務別復旧手順書、バックアップ手順書

出展：情報システム監査実践マニュアル（第3版）

＜管理活動の例：2＞（バックアップ手順の検証）
定められたバックアップ手順の実効性を検証する。

＜リスク＞
バックアップ手順の実効性を検証しなければ、適切なバックアップが取得できず、業務継続ができない。
＜着眼点＞
① バックアップ手順の実効性を検証する計画を策定し、それに基づいて検証する。
② 検証結果を記録し、問題点があれば、バックアップ手順を改善する。

出展：システム管理基準ガイドライン（2023年8月10日公表）

(2) 情報システム部門長は、情報システムにかかわるバックアップ方法及び手順を検証すること。	
＜主旨＞ 情報システム部門長は、定められたバックアップ方法及び手順の実現の可能性を確認するために、運用の責任者とバックアップ方法及び手順を検証する必要がある。	
① 情報システム部門長は、実現可能性を検証する計画を策定していること。	検証計画
② 情報システム部門長は、検証結果を記録し、バックアップ方法及び手順に反映していること。	検証結果記録書

出展：情報システム監査実践マニュアル（第3版）

＜管理活動の例：3＞（代替処理手続及び体制）
情報システムが停止した場合、復旧するまでの間に業務を継続させるために必要な代替処理及び体制を定め、その実効性を検証する。

＜リスク＞
情報システム停止時に必要な代替処理及び体制を定め、その実効性を検証しなければ、 業務継続に重大な影響を及ぼす。
＜着眼点＞
① 代替処理の責任者、要員（外部委託先を含む）、指揮命令系統を明確にする。
② 実現可能性の検証計画を策定し、それに基づいて検証する。
③ 検証結果を記録し、問題点があれば、代替処理手続及び体制を改善する。

出展：システム管理基準ガイドライン（2023年8月10日公表）

(3) 情報システム部門長は、復旧までの代替処理手続及び体制を定め、検証すること。	
＜主旨＞ 停止した情報システムを復旧するまでの間、業務を継続するため、代替処理手続及び体制を定める必要がある。 また、その実現可能性を確認するため、ユーザ及び運用の責任者と検証する必要がある。	
① 代替処理の要員及び予算を確保していること。	業務継続計画書、コンティンジェンシープラン
② 代替処理の責任者及び指揮命令系統を明確にしていること。	コンティンジェンシープラン、システム別業務別復旧手順書（復旧順位、復旧フェーズ、代替措置、指揮命令･連絡体制図等）
③ 実現可能性を検証する計画を策定していること。	検証計画
④ 検証結果を記録し、代替処理手続及び体制に反映していること	検証結果記録書

出展：情報システム監査実践マニュアル（第3版）

・利用部門に対する確認事項として以下を確認する。
　システム利用部門の担当者が業務継続計画の内容についての理解ができているか。

＜管理活動の例：4＞（復旧手続及び体制）
停止した情報システムを円滑かつ確実に復旧 させるための手続及び体制を定め、その実効性を検証する。

＜リスク＞
停止した情報システムを復旧させる手続及び体制を定め、その実効性を検証しなければ、 情報システムを円滑かつ確実に復旧することができない。
＜着眼点＞
① 復旧処理手続及び体制（進捗管理を含む）を定め、関係者に周知する。
② 実現可能性の検証計画を策定し、それに基づいて検証する。
③ 検証結果を記録し、問題があれば復旧手続及び体制を改善する。

出展：システム管理基準ガイドライン（2023年8月10日公表）

(4) 情報システム部門長は、復旧手続及び体制を定め、検証すること。	
＜主旨＞ 停止した情報システムを円滑かつ確実に復旧までの手続及び体制を定める必要がある。その実現可能性を確実にするため、ユーザ及び運用の責任者が検証する必要がある。	
① 業務の復旧許容時間及び復旧優先順位に対応して、復旧処理手続及び体制を定めていること。	システム別業務別復旧手順書（復旧順位、復旧フェーズ、代替措置、指揮命令･連絡体制図等）
② 復旧の推進状況を関係者に周知徹底する体制を定めていること。	システム別業務別復旧手順書（復旧順位、復旧フェーズ、代替措置、指揮命令･連絡体制図等）
③ 復旧の要員及び予算を確保していること。	業務継続計画書、コンティンジェンシープラン
④ 実現可能性を検証する計画を策定していること。	検証計画
⑤ 検証結果を記録し、復旧手続及び体制に反映していること。	検証結果記録書
⑥ 情報収集，情報伝達及び情報共有化のため、異なる複数の通信手段を確保すること。また、重要な外部委託先等との連絡体制についても考慮すること。	システム別業務別復旧手順書（復旧順位、復旧フェーズ、代替措置、指揮命令･連絡体制図等）
⑦ 組織図や緊急連絡網等は最新状態に維持管理すること。また、全役職員に周知徹底すること。	システム別業務別復旧手順書（復旧順位、復旧フェーズ、代替措置、指揮命令･連絡体制図等）
⑧ 復旧の要員の人事異動の際、確実に後任者に引き継ぎを行うこと。	引継書
⑨ 復旧体制要員について、必要とする要員のスキルや人数を考慮すること。また、特殊なスキルを要する担当者等については、代理者を定めること。	システム別業務別復旧手順書（復旧順位、復旧フェーズ、代替措置、指揮命令･連絡体制図等）

出展：情報システム監査実践マニュアル（第3版）

＜管理活動の例：5＞（運用状況の監視機能）
情報システムの運用状況の監視機能を設ける。

＜リスク＞
災害及び重大事項発生時に情報システムの運用状況を監視する機能がなければ、業務継続計画の実効性を確保できず、情報システムを早期に復旧できない可能性がある。
＜着眼点＞
① 災害及び重大事項発生時に情報システムのレスポンスタイムを監視し、必要に応じて制御する機能を設ける。
② 情報システムのリソース使用率を監視し、必要に応じて制御する機能を設ける。

出展：システム管理基準ガイドライン（2023年8月10日公表）

（1）運用管理者は、情報セキュリティ方針に基づいて、運用システムへのアクセス管理ルールを作成し、情報システム部門長の承認を得て、適切に運用すること。	
⑥ 特権的アクセス権の適用範囲を確認し、定期的な監視を行うこと。	アクセス管理ルール、アクセス権調査記録
（1）ネットワークの管理者は、ネットワーク管理ルールを定め、遵守状況を確認すること。	
③ ネットワークの稼動状況を常時監視できる体制を作っていること。	運用体制図
（3） ネットワークの管理者は、ネットワークへのアクセスコントロール及びモニタリングを実施すること。	
⑧ 高いセキュリティレベルが要求されるネットワーク環境では、ネットワークの利用状況を常に収集して監視し、異常が発生した場合の原因究明手続を定めていること。	モニタリング分析評価結果、インシデント対応マニュアル
（4）ネットワークの管理者は、ネットワーク監視ログを定期的に分析すること。	
② ネットワーク機器の監視ログの出力に関する設定を有効にしていること。	ネットワーク機器設定台帳
③ 監視ログ分析作業の効率化に関する対策を検討し、実施していること。	ログ管理手順書
④ 監視ログへのアクセスコントロールを行っていること。	アクセス管理ルール、アクセス権付与記録
⑤ 監視ログを適切に管理し、一定期間保存後に適切に廃棄していること。	ログ管理手順書、ログ管理実施記録
⑥ 監視ログの分析結果についての対応を検討し、選択していること。	モニタリング分析評価結果、是正処置実施報告書
⑦ ネットワーク監視の有効性を評価し、必要に応じて改善していること。	ログ管理手順書更新記録
① 関連設備の稼動状況を監視していること。	設備運用管理ルール、モニタリング分析評価結果
（3）運用管理者は、サービスを継続的に改善すること。	
① 運用管理者は、サービス目標に基づいた利用部門の利用状況を定期的に監視すること。	モニタリング分析評価結果

出展：情報システム監査実践マニュアル（第3版）

・インシデント発生時には対象システムだけでなく、全社ネットワークや情報システムの状況を把握する必要があるため、監査ポイントとして全社の情報システム運用管理面の確認を行う必要がある。

＜管理活動の例：6＞（可用性の維持）
情報システムの運用に要求される稼動率を確保し、可用性を維持する。

＜リスク＞
情報システムの運用に要求される稼動率を確保し、可用性を維持しなければ、業務継続 が困難となる。
＜着眼点＞
① 災害及び重大事項発生時に業務継続計画で定められた可用性を確保し、業務への影響 を最小限にとどめる。出展：システム管理基準ガイドライン（2023年8月10日公表）

（1）運用管理者は、情報セキュリティ方針に基づいて、運用システムへのアクセス管理ルールを作成し、情報システム部門長の承認を得て、適切に運用すること。	
⑥ 特権的アクセス権の適用範囲を確認し、定期的な監視を行うこと。	アクセス管理ルール、アクセス権調査記録
（1）ネットワークの管理者は、ネットワーク管理ルールを定め、遵守状況を確認すること。	
③ ネットワークの稼動状況を常時監視できる体制を作っていること。	運用体制図
（3） ネットワークの管理者は、ネットワークへのアクセスコントロール及びモニタリングを実施すること。	
⑧ 高いセキュリティレベルが要求されるネットワーク環境では、ネットワークの利用状況を常に収集して監視し、異常が発生した場合の原因究明手続を定めていること。	モニタリング分析評価結果、インシデント対応マニュアル
（4）ネットワークの管理者は、ネットワーク監視ログを定期的に分析すること。	
② ネットワーク機器の監視ログの出力に関する設定を有効にしていること。	ネットワーク機器設定台帳
③ 監視ログ分析作業の効率化に関する対策を検討し、実施していること。	ログ管理手順書
④ 監視ログへのアクセスコントロールを行っていること。	アクセス管理ルール、アクセス権付与記録
⑤ 監視ログを適切に管理し、一定期間保存後に適切に廃棄していること。	ログ管理手順書、ログ管理実施記録
⑥ 監視ログの分析結果についての対応を検討し、選択していること。	モニタリング分析評価結果、是正処置実施報告書
⑦ ネットワーク監視の有効性を評価し、必要に応じて改善していること。	ログ管理手順書更新記録
① 関連設備の稼動状況を監視していること。	設備運用管理ルール、モニタリング分析評価結果
（3）運用管理者は、サービスを継続的に改善すること。	
① 運用管理者は、サービス目標に基づいた利用部門の利用状況を定期的に監視すること。	モニタリング分析評価結果

出展：情報システム監査実践マニュアル（第3版）

・インシデント発生時には対象システムだけでなく、全社ネットワークや情報システムの状況を把握する必要があるため、監査ポイントとして全社の情報システム運用管理面の確認を行う必要がある。

参照するガイドライン・基準等

Ⅱ.9.4　訓練、演習及びテストの実施

事業継続計画に基づいた情報システムの業務継続計画を最新の状態にして実効性を高めるために、定期的に訓練を実施し、実現可能性を検証する。

＜達成目標＞

1. 代替処理を含む復旧手続の訓練が実施されている。
2. 訓練を定期的に実施し、復旧手続が最新の状態に維持されている。
3. 訓練結果がレビューされ、必要な改善が実施されている。

出展：システム管理基準（2023年4月26日改訂）

＜管理活動の例＞

1. （訓練の実施）目的や効果に応じて適切な業務継続計画の手順の訓練を実施し、その実効性を維持、向上させる。
2. （訓練の定期的実施）外部及び内部環境の変化に伴い業務継続計画の実効性が低減することのないように、定期的に訓練を実施する。
3. （業務継続計画の最新化）業務継続計画は、常に最新の状態に維持する。

出展：システム管理基準ガイドライン（2023年8月10日公表）

＜管理活動の例：1＞（訓練の実施）
目的や効果に応じて適切な業務継続計画の手順の訓練を実施し、その実効性を維持、向上させる。

＜リスク＞
事業継続計画で定めた手順について、その目的や効果に応じた訓練を実施しなければ、 有効な訓練を実施できず、業務継続計画の実効性を確保できない可能性がある。
＜着眼点＞
① 業務継続計画の手順毎にその狙いと達成目標を踏まえて、適切なシナリオを策定し、それに基づいた訓練を実施する。
② 訓練実施結果、明らかになった問題点に関する改善策を含めた訓練実施報告書を作成し、報告する

出展：システム管理基準ガイドライン（2023年8月10日公表）

（1）情報システム部門長は、情報システムにかかわる適切な業務継続手順・計画が、事業継続目的に合致していることを確かにするために、手順に基づき訓練を実施すること。 また、訓練は、策定後の維持管理のために、定期的に訓練の目的に応じて適切な訓練を実施、継続していること。	
＜主旨＞ 情報システム部門長は、目的や効果に応じて適切な業務継続手順・計画の訓練を実施し、実効性を高めていく必要がある。	
① 情報システムの事業継続マネジメントシステムの適用範囲及び達成目標と合致していること。	業務継続計画書、コンティンジェンシープラン
② 明確に定められた狙いと達成目標をもって、周到に計画された適切なシナリオに基づいていること。	業務継続計画書、コンティンジェンシープラン、システム別業務別復旧手順書（復旧順位、復旧フェーズ、代替措置、指揮命令・連絡体制図等）
③ 該当する利害関係者を含めた業務継続の取り組み全体について、長期にわたる総合的な妥当性を確認すること。	業務継続計画書見直しのレビュー結果
④ 業務の中断・阻害のリスクを最小限に抑えること。	業務継続計画書、コンティンジェンシープラン、システム別業務別復旧手順書（復旧順位、復旧フェーズ、代替措置、指揮命令・連絡体制図等）
⑤ 訓練実施結果、提案、及び改善するための処置を含めた正式な訓練実施報告書を作成すること。	コンティンジェンシープラン訓練実施記録、コンティンジェンシープラン訓練実施結果評価書
⑥ 継続的な改善を促進する観点からマネジメントレビューを行うこと。	マネジメントレビュー結果
⑦ 定期的に実施され、また組織内又は組織が活動する事業環境に大きな変化があった場合、実施すること。	コンティンジェンシープラン訓練計画書
⑧ 訓練の実施結果に対する有効性の評価を行うこと。	コンティンジェンシープラン訓練実施結果評価書
⑨ 担当者の交替や機器構成等の変更があった場合、その重要性・影響度の評価を行い、必要に応じて訓練計画の見直しを行うこと。	コンティンジェンシープラン訓練計画書

出展：情報システム監査実践マニュアル（第3版）

＜管理活動の例：2＞（訓練の定期的実施）
外部及び内部環境の変化に伴い業務継続計画の実効性が低下することのないように、定期的に訓練を実施する。

＜リスク＞
定期的に訓練を実施しなければ、外部及び内部環境の変化によって業務継続計画の実効性が低下し、事業を継続できない可能性がある。
＜着眼点＞
① 組織体の内部及び外部の環境変化による業務継続計画の実効性を検証するために、定期的及び環境変化時に、訓練を実施する。

出展：システム管理基準ガイドライン（2023年8月10日公表）

(2) 情報システム部門長は、訓練の実施手順に則り実施し、マネジメントレビューを行い、マネジメントサイクル(PDCA)を回すこと。	
＜主旨＞ 情報システム部門長は、国内外の状況変化や時間の経過により陳腐化させないために、業務継続計画策定後も、定期的に訓練を繰返し実施する必要がある。 また、業務継続計画は、訓練により常に最新の状態に更新をする必要がある。	
① 業務継続計画の訓練の実施手順は、次の手順及び実施項目を含めること。 ・訓練計画の策定 ・訓練評価項目の策定 ・訓練シナリオの策定 ・訓練の実施 ・マネジメントレビュー ・業務継続計画の改善/更新	業務継続計画訓練計画書
② 訓練結果を反映すること。 ・実施の優先順位 ・情報システム/予算/体制/備蓄 ・サプライチェーンマネジメント　等	業務継続計画訓練実施記録、業務継続計画訓練実施結果評価書
③ 訓練の結果及び実施結果に対する有効性の評価を経営陣に対して報告すること。	業務継続計画訓練実施記録、業務継続計画訓練実施結果評価書
④ 業務継続計画訓練の実施にあたり、外部委託先、サプライチェーン及び取引先の参画も考慮すること。	業務継続計画訓練計画書
⑤ 訓練方法・訓練内容の見直しを行い、訓練実施の形骸化を避けるとともに、実行難易度の低い訓練の繰り返しとならないようにすること。	業務継続計画訓練計画書

出展：情報システム監査実践マニュアル（第3版）

＜管理活動の例：3＞（業務継続計画の最新化）
業務継続計画は、常に最新の状態に維持する。

＜リスク＞
業務継続計画を最新の状態に維持しなければ、業務継続計画の実効性が低下し、業務を継続できない。
＜着眼点＞
① 訓練結果や内部及び外部の環境変化に対応して、業務継続計画を常に最新の状態に維持する。

出展：システム管理基準ガイドライン（2023年8月10日公表）

(2) 情報システム部門長は、訓練の実施手順に則り実施し、マネジメントレビューを行い、マネジメントサイクル(PDCA)を回すこと。	
＜主旨＞ 情報システム部門長は、国内外の状況変化や時間の経過により陳腐化させないために、業務継続計画策定後も、定期的に訓練を繰返し実施する必要がある。 また、業務継続計画は、訓練により常に最新の状態に更新をする必要がある。	
① 業務継続計画の訓練の実施手順は、次の手順及び実施項目を含めること。 **・訓練計画の策定** **・訓練評価項目の策定** **・訓練シナリオの策定** **・訓練の実施** **・マネジメントレビュー** **・業務継続計画の改善/更新**	業務継続計画訓練計画書
② 訓練結果を反映すること。 **・実施の優先順位** **・情報システム/予算/体制/備蓄** **・サプライチェーンマネジメント　等**	業務継続計画訓練実施記録、業務継続計画訓練実施結果評価書
③ 訓練の結果及び実施結果に対する有効性の評価を経営陣に対して報告すること。	業務継続計画訓練実施記録、業務継続計画訓練実施結果評価書
④ 業務継続計画訓練の実施にあたり、外部委託先、サプライチェーン及び取引先の参画も考慮すること。	業務継続計画訓練計画書
⑤ 訓練方法・訓練内容の見直しを行い、訓練実施の形骸化を避けるとともに、実行難易度の低い訓練の繰り返しとならないようにすること。	業務継続計画訓練計画書

出展：情報システム監査実践マニュアル（第3版）

参照するガイドライン・基準等

Ⅱ.9.5　業務継続計画の評価及び見直し

情報システムの業務継続計画を適切かつ有効なものとするために、定期的（業務継続計画の発動時を含む）に業務継続計画の評価、見直し及び改善を行う。

＜達成目標＞

1. 業務継続計画を発動した場合、対処が完了した後に業務継続計画の評価及び見直しが実施されている。
2. 定期的に業務継続計画の評価及び見直しが実施されている。

出展：システム管理基準（2023年4月26日改訂）

＜管理活動の例＞

1. （リスク事象発生後の業務継続計画の評価及び見直し）情報システムに関わる業務に影響を与える重大なリスク事象が発生した場合、対処が完了した後に業務継続計画を評価し、見直しを行う。
2. （業務継続計画の定期的評価及び見直し）業務継続計画が適切かつ有効であることを、定期的に評価し、見直しを行う。

出展：システム管理基準ガイドライン（2023年8月10日公表）

＜管理活動の例：1＞（リスク事象発生後の業務継続計画の評価及び見直し）
情報システムに関わる業務に影響を与える重大なリスク事象が発生した場合、対処が完了した後に業務継続計画を評価し、見直しを行う。

＜リスク＞
重大なリスク事象が発生した場合、業務継続計画を評価・見直さなければ、業務継続計画の実効性を確保できず、事業を継続することが困難となる。
＜着眼点＞
① 重大なリスク事象発生時に実施した業務継続手順及び能力の適切性、妥当性及び有効性を評価する。

出展：システム管理基準ガイドライン（2023年8月10日公表）

(1) 情報システム部門長は、情報システムにかかわる業務の中断･阻害を引き起こす事故が発生し、業務継続計画の発動に至った場合、事故発生後に業務継続計画の評価及び見直しを行うこと。	
＜主旨＞ 情報システム部門長は、情報システムにかかわる業務に影響を与える重大な事故が発生した場合、事故後に業務継続計画を評価し、見直す必要がある。	
① 業務継続手順及び能力の適切性、妥当性及び有効性の継続を確保するために、それらの評価をすること。	業務継続計画見直し評価結果報告書
② 計画の見直しを、定期的なレビュー、訓練、試験、事故発生後の報告、及びパフォーマンス評価を通して行うこと。	レビュー結果、業務継続計画見直し評価結果報告書
③ 適用される法令及び規制の要求事項の順守、業界のベストプラクティスとの適合、並びに業務継続計画方針及び目的との適合を定期的に評価すること。	外部情報等収集結果に基づく業務継続計画見直し評価結果報告書
④ あらかじめ定められた間隔で、また大きな変更があった場合にも、評価を実施すること。	業務継続計画見直し評価結果報告書
定期的な評価以外の見直し事由（例） 1）訓練を実施した結果、業務継続計画に不具合が判明した場合 2）経営方針の変更により業務継続計画が影響を受ける場合 3） 社会情勢や技術環境の変化に伴い、システム変更等が発生した場合 4） 人事異動･組織変更が発生した場合 5） 重要な業務について、その内容に変更が生じた場合 6） 従来、業務継続計画では考慮していなかった業務について、その重要性が高まった場合 7） 業務遂行の前提となる組織や拠点施設･インフラ･システム構成等（クラウドなどのアーキテクチャを含む）の条件に変更が生じた場合 8） 政府の取組みやガイドライン等が変更された場合 9） 同業他社等における事故･障害事例が公表された場合 10）中央防災会議等の検討結果が公表された場合 11）最新の環境変化や状況変化に即し、システムリスクなどの内容に変化が生じた場合　等	
⑤ 情報システムにかかわる業務に影響を与える重大な事故が発生した場合、システム的要因の分析のみにとどまることなく、人的要因（要員の繁忙による集中力の低下、要員不足等）等、根本原因の究明を行い、必要に応じて業務継続計画の評価及び見直しを実施すること。	業務継続計画見直し評価結果報告書

出展：情報システム監査実践マニュアル（第3版）

＜管理活動の例：2＞（業務継続計画の定期的評価及び見直し）
業務継続計画が適切かつ 有効であることを、定期的に評価し、見直しを行う。

＜リスク＞
業務継続計画が適切かつ有効であることを、定期的に評価し、見直しが行われなけれ ば、業務継続計画の実効性を確保することができず、事業を継続することが困難となる。

＜着眼点＞
① 業務継続計画の有効性を定期的に評価し、問題があれば必要な改善を行う。
② 見直した業務継続計画を承認し、関係者に周知する。

出展：システム管理基準ガイドライン（2023年8月10日公表）

(2) 情報システム部門長は、業務継続計画が、引き続き、適切かつ有効であることを確実にするために、あらかじめ定められた間隔で、業務継続計画の評価及び見直しを行うこと。	
＜主旨＞ 情報システム部門長は、業務継続計画が適切かつ有効であることを、あらかじめ定められた間隔で評価し、見直す必要がある。	
① 前回の見直しの結果と取られた処置の状況を確認すること。	業務継続計画見直し評価結果報告書
② 業務継続計画に関連する外部及び内部の課題の変化による、見直しを実施すること。	業務継続計画見直し評価結果報告書
③ リスクアセスメント、事業影響度分析、業務継続計画及び関連する手順の更新を実施すること。	業務継続計画の維持管理手続
④ 情報システムにかかわる業務継続計画に影響を与える可能性のある組織内外の環境変化に対応するための手順及び管理策を修正すること。	業務継続計画見直し評価結果報告書

出展：情報システム監査実践マニュアル（第3版）

まとめ

経営陣と業務執行部門によるIT-BCP

- 経営陣は経営目的と事業継続計画の必要性、全社BCPとIT-BCPに関する深い理解が必要（重要業務のITへの依存性）。
- 経営陣は自社の事業継続力を高める取組みも視野に入れた検討を行うことが望ましい（国の推奨する認証取得を目指すなど、自社の企業価値向上につながる取組み）
- 経営陣とIT部門の強い連携のもと、利用部門におけるIT-BCPの認識度を高める取組みを継続する（図上訓練やワークショップ実施など）。
- リスク対策で講じた技術的措置を超える（想定外）の事象が発生した場合の対応についても考慮すること（経営陣も参画しての訓練の実施など）。
- システム管理基準／ガイドラインや関連るガイドライン等の積極的活用によりIT-BCP監査のベストプラクティスを目指し組織と共有する。

参考文献等（Webサイト含む　）

システム管理基準（2023年年4月26日改訂）	経済産業省
システム管理基準ガイドライン（2023年年8月10日）	特定非営利活動法人日本システム監査人協会
システム監査基準（2023年4月26日改訂）	経済産業省
システム監査基準ガイドライン（2023年8月10日）	特定非営利活動法人日本システム監査人協会
情報システム監査実践マニュアル（第3版）	NPO法人日本システム監査人協会
情報システム基盤の復旧に関する対策の調査報告書	独立行政法人情報処理推進機構
レジリエンス認証制度	一般社団法人レジリエンスジャパン推進協議会HP
事業継続力認定制度	中小企業庁HP

※Webサイト参照部分は団体名の末尾に「HP」と記載。

ご清聴ありがとうございました。