CISA®

Certified Information Systems Auditor™

公認情報システム監査人

サンプルテキスト

Abitus

コース・シラバスと本書の使い方

本テキストは、CISA®試験の出題範囲を基に、CISA試験対策上習得すべき、重要な概念やキーワードを豊富な図解で解説することにより、受講生の皆様が学習しやすいように構成しております。講義とテキストで重要なポイントをしっかりと理解し、MCカードに掲載のある問題を繰り返し練習することにより、効率的な学習が可能です。

コース・シラバス

上巻

下巻

アイコンについて

本テキストでは、効率的な学習を手助けする様々なアイコンを欄外にご用意しました。

補足

本文の補足事項

参考

テキスト記載内容の参照元

用語解説

本文記載事項の用語解説

例

本文記載事項の具体例

セルフ・スタディ

講義では扱わず、自己学習をするトピック

本書の使い方

トピックタイトル

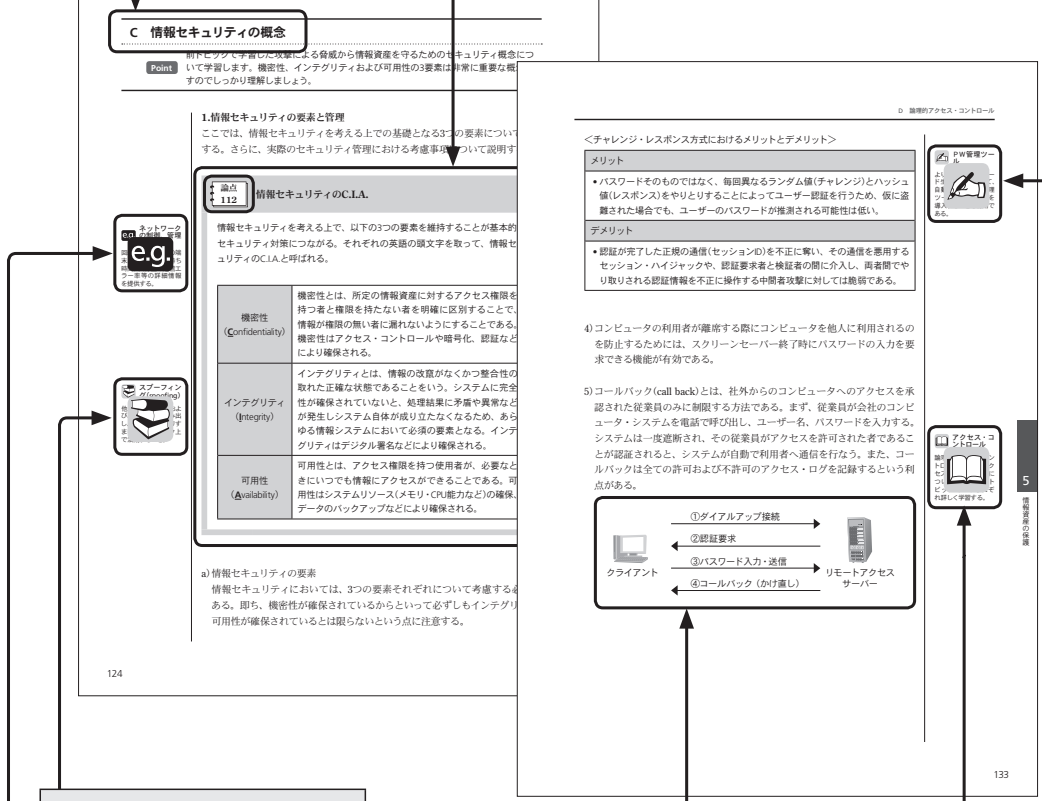
その章で学ぶタイトルです。

論点

重要な学習ポイントについては、各々論点番号と論点タイトルが表示されています。

補足

本文に記載されていることの背景等を知ることで、より理解が深まります。



用語解説

難解な専門用語も分かりやすく解説しています。

例

具体例でイメージを持つことにより、概念を自分なりに理解できます。

理解すべき重要な概念やキーワードについて豊富な図解で解説しています。

参考

テキスト記載内容の参照元、またはより詳しい情報を得るための参考となる文献です。

CISA® CONTENTS

1 情報システム監査のプロセス

2 ITガバナンスとマネジメント

3 情報システムの調達、開発、導入

4 情報システムの運用、保守、サポート

5 情報資産の保護

論点一覧

3章 情報システムの調達、開発、導入

論点一覧

4章 情報システムの運用、保守、サポート

5章 情報資産の保護

2章　ITガバナンスとマネジメント

本章では、組織体の経営戦略と情報技術戦略を整合させることを保証するITガバナンス、組織体における情報システム戦略策定の要素、リスク分析方法、及び情報システム部門内の職務の分離のあり方について学習します。
また、組織体のIT機能に障害が発生した場合において、重要な業務の運営を継続するための事業継続計画についても学習します。

2章　ITガバナンスとマネジメント

D　事業継続計画(Business Continuity Planning; BCP)

Point このトピックでは、事業継続計画の概要について解説します。BCPの目的や策定の責任、及び組織全体のBCPを構成する災害復旧計画などの個々の計画について理解を深めましょう。

1.事業継続計画(BCP)

ここでは、事業継続計画の意義と策定の責任について解説する。また、BCPに含まれる要素とそれらの目的を解説し、組織のセキュリティ活動との関わりについても触れる。

BCP
業務継続計画と呼ばれることもある。

論点 42　事業継続計画(BCP)の概念

事業継続計画(Business Continuity Planning; BCP)とは、組織体が存続していくために必要な重要機能またはオペレーションの予期しない中断による業務リスクを低減させるように設計されたプロセスである。

a)BCP策定の意義と責任

企業が災害等で被害を受けた場合に重要な業務を中断しないこと、また中断しても出来るだけ短い期間で重要な業務を再開することは、企業自らを守るためだけでなく、社会的責任という観点からも重要な課題である。経営者は業務を継続するための行動計画である「事業継続計画(Business Continuity Planning; BCP)」を構築することが望まれており、BCP策定の一義的な責任は上級経営者にある。

b)BCPに含まれる要素とその目的は以下の通りである。

e.g. 災害およびその他の中断事象
- 災害
  自然災害－地震、洪水、竜巻、豪雨、火災等。
  人的災害－テロリストの攻撃、ハッカー攻撃、ウイルス等。
- その他の中断
  システムの誤作動、不慮のファイル削除等

BCPの構成要素となる計画	目的
業務復旧計画 (Business Recovery Plan; BRP)	災害発生後早急に業務活動を復旧する手続きを提供する。
オペレーション継続計画 (Continuity of Operation Plan; COOP)	30日間、代替地で組織体の必要不可欠な戦略機能を維持する手続きと機能を提供する。
支援継続計画/ IT緊急事態計画	主要アプリケーションや、全般的なサポートのシステムを回復する手続きと機能を提供する。

IT開発プロジェクトにBCPを統合することは、開発プロセスにおいてより包括的な要件定義を可能とする。

危機時の情報伝達計画	従業員又は一般市民に、現状報告を広める手続きを提供する。
サイバーインシデント対応計画	悪意のあるコンピュータ・ネットワーク上でのインシデントの発見、対応、及びその影響を制限する戦略を提供する。
災害復旧計画 (Disaster Recovery Plan; DRP)	代替地で機能の回復を促進するための詳細な手続きを提供する。
避難計画 (Occupancy Emergency Plan; OEP)	人命の喪失、怪我、及び物理的脅威に対する財産の保護のための調整された手続きを提供する。

BCPにおいて重要業務の再開は重要な優先事項であるが、最も主要な目的は人的資源の保護である。したがって、BCPにおいて避難計画は重要な構成要素である。

c) BCPにおけるセキュリティの位置づけ

1) BCPにおいて最も重要な要件の一つは、日常の業務のセキュリティの向上である。これは、事業の中断を引き起こす事象の発生の可能性を低くする対応策の導入が含まれる。例えば、データセンターを地震断層線上から避けて設置する、あるいはループ型やメッシュ型のような回復力のあるネットワークを構築するなどの対策が挙げられる。仮に中断が発生していなくても、BCPに代表される業務の目的を達成するための条件を定期的に検証しなければならない。

2) 災害復旧において、組織はITシステムの品質を確保することが重要である。したがって、ITシステムの機密性、インテグリティ、可用性を維持するための枠組みである情報セキュリティマネジメントシステム(ISMS : Information Security Management System)の実施が推奨される。

パンデミック(pandemic)

感染症(伝染病)の世界規模的な流行のことを指す言葉で、日本語では「汎発流行」や「爆発感染」といった表現が用いられることもある。代表例として、過去の例では、ヨーロッパで大流行したペストやコレラ等がある。現在において主として脅威とされているのはインフルエンザである。
パンデミック下においては、その深刻度合によっては屋外外出禁止等の措置が取られることが考えられるため、BCPの整備が非常に重要となる。

E　BCP策定のプロセス

Point　このトピックでは、BCPを策定する具体的なプロセスについて学習します。ビジネス・インパクト分析からBCPのテストに至るまでの全体の流れをしっかり理解しましょう。

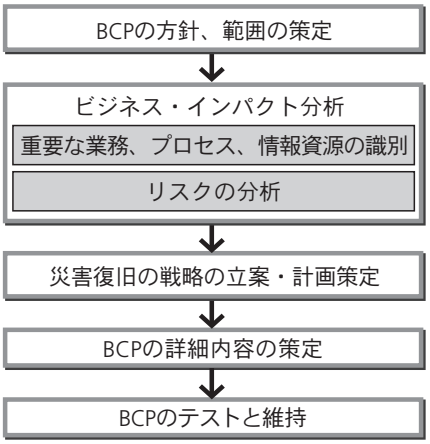
1.BCP策定のプロセス

ここでは、BCPを策定するための具体的なプロセスについて解説する。次以降の論点で学習する個々のプロセスの基礎である、組織戦略におけるBCPの位置づけや、BCP策定の大まかな流れについて説明する。

論点43　BCP策定のプロセス

- BCPは組織戦略や事業目的を参照し策定することが重要である。
- BCP策定に際しては一般に以下のプロセスを実行する。

＜BCP策定のプロセスの流れ＞



右記にある災害復旧計画(Disaster Recovery Plan; DRP)の具体的な内容説明は、下巻の第4章で行う。

a) 具体的な策定プロセス

まず最初に、BCPの方針や範囲について策定し、全体像を明確なものとする。この際、組織の戦略上重要な事業や事業のプロセスを明確にしておくことが求められる。また、BCPは組織の戦略と整合するように策定される必要がある。

次に、企業にとってのリスクとリスクが顕在化した場合の業務への影響の分析(ビジネス・インパクト分析)を行い、復旧戦略の立案及びBCPの詳細な内容策定に移る。そして策定されたBCPはその有効性を検証するためにテストを実施し、改善すべき点があれば見直しを行う。

BCPの導入についての留意事項

BCPの導入は、適切な担当者に伝達され、当該担当者がBCPのすべての面を把握した場合にのみ有効となる。

2.ビジネス・インパクト分析(Business Impact Analysis; BIA)

ここでは、ビジネス・インパクト分析を通じて行われる具体的な作業手順について解説する。特に、復旧戦略の基礎となるリスク分析が重要である。

論点44　ビジネス・インパクト分析(BIA)

ビジネス・インパクト分析とは、重要な業務、プロセス、およびそれに関連する情報資源を特定して、業務の中断による影響を評価する作業である。BIAの作業手順は以下の通りである。

a) 重要な業務、プロセス、情報資源の識別
b) リスク分析、優先順位付け
c) 死活的な復旧時間の考慮

以下、ビジネス・インパクト分析における上述の作業手順について解説する。これらの作業は、アンケート、インタビュー、ミーティング等のアプローチによる情報収集を通じて達成される。情報の収集においては、情報システム部門とユーザー部門でミーティングの機会を設ける等、ユーザーの関与が重要となる。

a) 重要な業務、プロセス、情報資源の識別

ビジネス・インパクト分析においては、まず組織体における重要な業務、プロセス、関連する情報資源を理解し特定する。

重要業務の特定作業では、業務のプロセスを明らかにし、どの作業がどのような順序で実施され、どの部署に関係しており、そしてその作業のためにどのような情報資源を使用しているかを明確にする。

システムの分類	説明
クリティカル(critical)	この分類にあてはまる機能は、同一の能力を持つシステムに置き換えなければ実行不可能である。手動による方法では重要なアプリケーションの代替にはならない。中断に対する許容度は非常に低い。従って中断によるコストは非常に高い。
バイタル(vital)	この分類にあてはまる機能は、短期間であれば手作業で実行可能である。中断に対する許容度はクリティカル・システムの許容度よりも高い。よって機能がある時間(通常5日以下)で復旧されれば幾らかコストは低くなる。

センシティブ（sensitive）	この分類にあてはまる機能は、許容できるコストの範囲内で、長期間において手作業で実施可能である。手作業で実施される過程においては、通常は難しい手順が発生するため、追加の要員が必要になる。
ノン・センシティブ（nonsensitive）	この分類にあてはまる機能は、より長い期間中断させられることもあり、復旧される場合においても、ほとんど、または全くコストを掛けることは無い。また中断前の状態にまで回復させることも無い。

Source: ISACA Review Manual 2009

b）リスク分析、優先順位付け

次に、関連するリスクを洗い出し、BCPの対象となるリスクの絞込みを行うと共に、リスク発生からの事態の推移（リスクシナリオ）を明らかにする。その上で、リスクの顕在化により業務が停止した場合の影響度の評価を行う。評価指標には定性的なものと定量的なものがあり、この評価結果は復旧戦略策定（DRP）における重要な資料となる。

定性的影響	顧客への影響、供給者への影響、従業員への影響、法令遵守への影響等
定量的影響	経済的、財務的影響等

BCPの対象とする業務領域は、すべての領域が望ましいが、業務中断による影響度を総合的に勘案した上で優先順位をつける。これに基づいて資源配分や業務復旧の順番を決定する。IS監査人は、BCP、DRPが全てのシステムを網羅していないことを発見した場合、網羅していないシステムのビジネス・インパクト分析を評価し、全てのシステムを網羅していないことによる影響を管理者に報告をする。

c）死活的な復旧時間の考慮

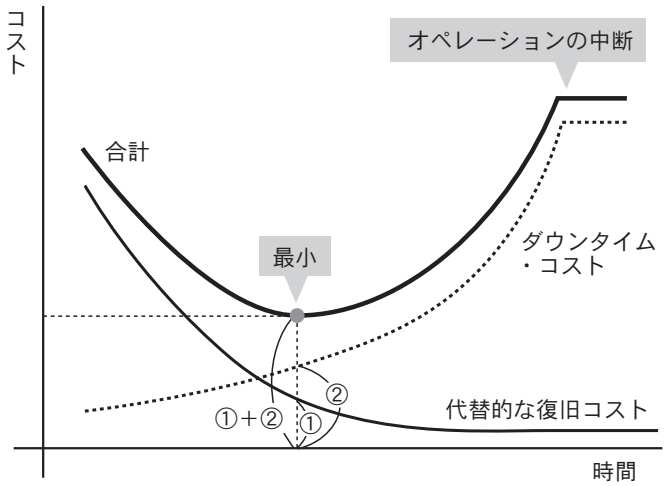
ビジネス・インパクト分析において考慮する、死活的な復旧時間とは、重大なまたは許容範囲を超えた損失が発生する前に業務プロセスを復旧しなければならない時間のことである。復旧時間を判定するための要素には以下の2つがある。

1）ダウンタイム・コスト	中断時間に関わる費用
（例）	注文、売上の減少、調達遅延、市場及びイメージの損失等。
2）代替的な復旧戦略コスト	代替的な事業継続計画にかかるコスト
（例）	定期的なテストのコスト、オフサイトのバックアップ施設、保険料、代替テストの契約費用等。

ダウンタイム・コストは、短い期間であっても時間とともに急激に増加し、ある一定時期に至るまで、増加し続ける。増加が止まるある一定の時期とは、もはや業務が機能しなくなった点を表す。
一方、代替的な復旧コストは、目標として設定した所要復旧時間が長くなるほど減少する。

BCP策定においては、この2つのコストの合計値（下図の①＋②）が最小となる点を見つけることが重要である。

＜ダウンタイム・コストと代替的な復旧コスト＞



参考　**ビジネス・インパクト分析の例**

業務名：インターネット販売業務　　リスク：情報システム障害

評価指標		重大な影響が生じると思われる停止期間	重大な影響の内容（参考数値など）	停止期間の長期化にともなう影響度の変化
事業	金銭的な損失	1日	1日の売上げ最大50％（3,000万円）減	停止日数×1日売上（6,000万円）＋α
	評判上の損失	3日	メディアなどで取り上げられる	1週間を超えると致命的
	顧客の喪失	3日	他社への乗り換え	1週間を超えると多数の利用者が他社へ乗り換える
投資家	金銭的な損失	3日	株価低下	1ヶ月を超えると致命的
		1ヶ月	配当金減少	1ヶ月以上は無配
仕入先	事業の存続	1週間	上位10社平均仕入額1,000万円	停止期間に比例、倒産はない
従業員	生活上の影響	1ヶ月	給与の未払い	解雇の発生

3.災害復旧戦略の立案および災害復旧計画（Disaster Recovery Plan; DRP）の策定

ここでは、BCPを構成する計画の一つである、災害復旧戦略の立案および災害復旧計画の策定について解説する。特に、DRPによって得られる効果とオペレーション・コストとの対応関係について理解することが重要である。（復旧計画に用いる指標や手法等の具体的な内容については、下巻の4章において扱う。）

論点45　**災害復旧戦略と災害復旧計画（DRP）**

- 復旧戦略は復旧手順の指針を示す。
- 災害復旧計画は、業務部門が業務作業復旧のために準拠する計画であり、BCPの技術的側面としての一部を構成する。DRPは組織の復旧戦略の重要な要素であり、災害発生時に組織がシステムを回復する際の費用対効果を考慮したうえで、上級経営者の責任で策定されるべきである。

a）復旧戦略

復旧戦略は、システムを復旧させる最善な方法を明らかにし、詳細な復旧手順を策定するための指針を示す。通常、重要な業務機能をサポートするアプリケーションを実行するITプラットフォームでは、復旧戦略は必須であり、例えば主要な物理的設備に対する災害に備えて、代替のオフサイト・バックアップを用意する等が必要である。

適切な復旧戦略は、ビジネス・インパクト分析を通じて判定された影響度に対して妥当なコストに収まるものでなければならない。復旧コストとは、起こりうる中断に備えるコストであり、また中断の際にシステムを稼動させるためのコストでもある。

b）DRP策定の意義と責任

現在は、情報システムが事業を支える重要なインフラとなっているため、企業の継続を実現するためには情報システムに対するDRPが重要である。情報システム部門にとってのDRPは、情報処理施設の復旧のための手順であり、またシステム復旧中の代替処理手続きに焦点を置く。

DRP策定は上級経営者の責任である。DRPは組織体全体のBCPと一貫性があり、これを支援するものである必要がある。

c）DRPにおける費用対効果の考慮

DRPでは、業務の復旧時間を短くするとともに、復旧にかかるコストをおさえることを目的とする。

DRP導入により、災害前後のオペレーション・コストは増加するため、得られる効果と費用を考慮して策定しなければならない。

d）災害復旧計画は継続的なプロセスであり、定期的なレビュー及び再検討が必要である。DRPの定期的なレビューをすることで、例えば以下のような重要な成果が得られる。

1）ITインフラストラクチャー（サーバー、ネットワーク等）の変更
2）組織構造の変更（新しい要員追加や役割分担変更等）
3）サポートするプロセスの成熟度増加

また上記に加え、単一な緊急事態への対処のみならず、地震等の大災害を対象とした事態への対応計画も策定される。これには、部門レベルの単一な手順に限らず、複数の場所および業務に対応すべくモジュール化された複合的な計画が含まれる。

4.BCPの詳細内容の策定

ここでは、これまでの策定プロセスで得た情報に基づいて決定されるBCPの詳細について解説する。BCPが複数存在する場合の考慮事項、BCPに含まれるべき災害宣言に関する規定、組織と責任の割り当てについて説明する。

BCPに関するガイドライン

米国では、NFPA（National Fire Protection Association）が、2004年にNFPA1600「Standard on Disaster/Emergency Management and Business Continuity Programs」を発行し、BCM（Business Continuity Management）の導入を促進している。

論点46　BCPの詳細の策定

ビジネス・インパクト分析から得た情報や経営者によって選択された復旧戦略に基づいて、詳細な事業継続計画や災害復旧計画を策定する。計画に際しては経営幹部及びユーザーの関与が非常に重要である。

a）BCPの形式と文書化

BCPは、組織の複雑さによって、事業継続や災害復旧の様々な事項に対応するために、単一の計画になる場合もあるし、複数の計画になることもある。必ずしも単一の計画へ統合する必要はないが、計画の形式を選択する際には、以下の事項について考慮すべきである。

計画の形式	考慮すべき事項
複数の計画	実行可能なBCP戦略を構築するために、計画の各々の部分は他の部分と調和していなければならない。
単一の統合された計画	あらゆる側面を網羅し、事業継続のための資源が最も効果的に使用されることが望ましい。

BCPの内容は全ての人に理解できる平易な言葉で表現され、計画書として文書化されるべきである。また、計画書のコピーはオフサイト保管されるべきである。

b）BCPの内容

BCP策定において考慮すべき要因には以下のものがある。

1）業務プロセスに影響する全ての事象と事象への対応を含めた災害前の準備
2）避難手順
3）災害発生を宣言すべき状況と宣言の方法
4）計画における責任、及び各機能の担当者の明確化
5）契約に関する情報の明確化
6）復旧オプションの段階的な説明
7）復旧および組織体の継続的オペレーションのために必要とされる資源の明確化
8）構築フェーズの段階的適用

以下、3)、4)について解説する。

3) 災害発生を宣言すべき状況と宣言の方法

小規模の事象であっても、適時もしくは適切に対応しないことにより障害を招く可能性がある。BCPにおいては災害を宣言する責任が明確にされていなければならない。

4) BCPにおける組織と責任の割り当て

計画では、災害や事象の発生におけるチームとそれぞれの責任を明確にする必要がある。主なチームには以下のようなものがある。

緊急措置チーム	最初に対応するチームであり、このチームは、指定された火災監視人、及び消火要員である。このチームの主な機能の1つは、従業員の秩序のある避難を実現し、人命を保護することである。
オフサイト・ストレージ・チーム	復旧設備で使用する媒体及び記録を取得し、梱包して発送する責任を負う。さらに復旧サイトのオペレーション中に作成された情報をオフサイト保管庫に保管するスケジュールを確立して監督する責任がある。
輸送チーム	遠い距離にある復旧サイトへの従業員の輸送を調整する責任がある。更に従業員への連絡と新しい作業場所と作業スケジュールに関する情報の提供、彼らの宿泊の手配を支援する。
復旧チーム	被災サイトの移設プロジェクトを管理する。このチームは当初実施された評価よりも、より詳細な設備、装置の損害の評価を行う。また被災サイトを再建するか、または移設するかについての判定に必要な情報を緊急管理チームに提供する。
再配置チーム	ホット・サイトから新しい情報処理施設、または復元された本来の施設へ移行するプロセスを調整する。これは情報システム処理オペレーション、通信交換、及びユーザー・オペレーションを再配置することを伴う。さらにこのチームは通常のサービス・レベルへの移行を監視する。

なお、計画には、短期、中期、及び長期にて重要な業務機能を維持するために必要とされる要員のリストと連絡を取るための情報が含まれるべきである。

ホット・サイト

詳細は下巻4章で扱う。

参考　その他のチーム

- インシデント対応チーム
  組織体の資産やプロセスに対し脅威と考えられる各々のインシデントに関する情報を受け取るためのチームである。情報処理施設において重大なインシデントが発生した場合、このチームが行うべき最優先事項は、施設においてそれ以上の被害拡大を阻止し損害を最小限に抑えるための「封じ込め」作業である。

- 損害査定チーム
  災害後に損害の程度を査定する。このチームは損害を査定し、かつ影響を受けたサイトでオペレーションを復旧するのに必要な時間を推定できる要員によって構成されるべきである。

- 緊急管理チーム
  他の復旧チーム全ての活動を調整すること、そして重要な意思決定を行うことに責任を負う。また事業継続計画の発動を判定する。他の機能としては、復旧資金の調達、及び災害から起こる法律上の問題の扱い、及び広報関連事項や報道機関からの問合せを取り扱う。

- ソフトウェアチーム
  システムパックの復旧、オペレーティング・システム・ソフトウェアのローディングとテスト、システムレベルの問題の解決に責任を負う。

- アプリケーションチーム
  システム復旧サイトへ移動し、バックアップ・システム上でユーザー・パック及びアプリケーション・プログラムを復旧する。

- セキュリティチーム
  システムのセキュリティと通信接続を継続的に監視する。システムの迅速な復旧を妨げるあらゆるセキュリティ上の問題を解決する。

- 緊急オペレーションチーム
  システム復旧サイトに常駐することになる交代勤務のオペレーター及びその監督者から構成され、災害復旧プロジェクトの全期間に渡ってシステム運用を管理する。

- ネットワーク復旧チーム
  広域音声／データ通信の経路変更、ホストネットワーク管理とシステム復旧サイトへのアクセス、データ通信への継続的支援、及び通信のインテグリティの監視について責任を負う。

- 通信チーム
  復旧サイトへ移動し、ユーザー／システムネットワークを確立するため、リモート・ネットワーク復旧チームと協働する。

- ユーザー・ハードウェアチーム
  ユーザー端末、プリンター、タイプライター、複写機その他必要な装置の搬送と設置を調整する。

- データ準備及び記録チーム
  ユーザー復旧サイトに接続された端末から、アプリケーション・データベースを更新する。

- 管理事務サポートチーム
  他のチームへの事務的な支援を行い、ユーザー復旧サイトに対するメッセージ・センターとして機能する。

- 消耗品チーム
  ベンダーに連絡を取り、継続的に必要とされる事務用品やコンピューター用品の補給を調整することでユーザー・ハードウェアチームを支援する。

- 調整チーム
  地理的に異なった場所にある様々な事業所における復旧作業を調整する責任を担う。

- 法務チーム
  あらゆるインシデントやサービスの提供不能等、様々な理由から発生する法的事項への対応に関する責任を担う。

- 復旧テストチーム
  策定された様々な計画のテストや結果の分析に関する責任を担う。

- 教育チーム
  事業継続や災害復旧手続の準備についてユーザーへ教育を行う。

5.BCPテストの実施

ここでは、策定されたBCPの有効性を評価するために実施するテストについて解説する。テストの主要な実施方法について触れたうえで、テストの計画からBCPの見直しに至るまでのプロセスについて説明する。

論点47　BCPテストの実施プロセス

- BCPテストには、テスト実施のための準備活動や、事後的なテスト結果の分析及び改善案の検討が含まれる。
- テストの実施方法には以下のものがあり、通常はこの順番で実施される。

机上評価／ペーパー・テスト	特定のサービス中断において起こり得る事象を解決する、計画の実施における主要な要員の参加による紙上での「ウォークスルー・テスト」である。参加者は、計画の全体、もしくはその一部分をチェックする。通常準備状況テストより前に行われる。
準備状況テスト	全オペレーション・テストの局所化されたテストとして実施される。このテストは、計画の異なる面から定期的に実施され、計画の妥当性についての証拠を段階的に得るコスト効率の良い方法である。
全オペレーション・テスト	全オペレーション・テストは最も包括的であり、実際の資源がシステム障害のシミュレーションに費やされる。計画におけるすべてのチームメンバーと参加者が関与する。全オペレーション・テストは、机上評価及び準備状況テストの後で実施される。

a）BCPテストの目的と計画の策定

BCPのテストを行うことは、BCPの有効性を検証し、BCPの限界を識別するために必要であり、実際に対応手順を経験することで対応力の強化にもつながる。

テストはBCPの全ての重要な構成要素を扱うべきであり、また復旧チームの主要なメンバーがテスト・プロセスに関係することが重要である。また、復旧計画の経験を広めるために、復旧管理者のローテーションが行われなければならない。

b)BCPテストにおける実施内容

テストにおいては、以下の任務を達成することが求められる。

- BCPの完全性、精度の検証
- テストに関与する担当者の業績の評価
- 事業継続チームメンバー以外の訓練と意識の評価
- 事業継続チームと外部のベンダーとの調整の評価
- 規定された処理を行うバックアップ・サイトの能力と容量の測定
- 重要な記録を復旧する能力の評価
- 復旧サイトへ再配置された機器や消耗品の状態と量の評価
- 組織体の維持に関連した情報システム処理活動及びオペレーション全体の性能の測定

c)テスト結果の文書化と分析

テストの各段階の実施中に、観察結果、問題、及び解決方法について詳細な文書を作成し保存する。そして結果は観察のみに基づく評価によらず量的に測定されて分析される。テストの成功度については量的な測定が望ましく一般に以下の尺度が適用される。

時間	規定任務の完了時間、機器配達時間、サイトまでの到着時間
数量	バックアップ・サイトで実行される作業量
件数	バックアップ・サイトでの処理のために要求された重要なデータに対して無事に届けられたデータの数。無事に復旧された最重要システムの件数等。
正確性	復旧サイトでのデータ入力の正確性と通常のデータ入力の正確性の比率等。

d)テスト結果に基づくBCPの見直し

事業継続のための計画と戦略は、定期的に更新されることが必要である。以下の要因は、事業継続の要件や計画変更の必要性に影響を及ぼす。

- 組織体のニーズの変化によって、ある時点において適切な戦略が適切ではなくなることがある。
- 新しい資源やアプリケーションが、開発、もしくは取得されることがある。
- ソフトウェア、またはハードウェア環境の変更は、現在の前提条件を旧式または不適当とすることがある。
- 中断を引き起こす恐れのある新たな事象の発生や事象の変化

F　事業継続計画の監査

Point　このトピックでは、IS監査人が事業継続計画の監査を行ううえで考慮すべき事項について学習します。

1.事業継続計画の監査

ここでは、事業継続計画におけるIS監査人の役割について解説する。

論点 48　**BCPにおける情報システム監査人の役割**

BCPにおける情報システム監査人の役割には以下を含む。

a）事業継続計画のレビュー
b）前回のテスト結果の評価
c）重要な要員へのインタビュー
d）オフサイト保管の評価
e）オフサイト施設におけるセキュリティの評価
f）代替処理契約のレビュー
g）保険適用範囲のレビュー

a）事業継続計画のレビュー

計画をレビューし、それが妥当かつ最新のものであるかを判断するために、事業継続計画を評価する。具体的には以下の項目をレビューする。

- 事業継続計画またはマニュアルの最新コピーを入手する。
- 事業継続作業の着手に関する手順文書の有効性を評価する。
- PCベース、もしくはエンドユーザーに開発されたシステムを含めて、重要なアプリケーションの識別、優先順位、及び計画された支援手順をレビューする。
- 災害時における抗堪性(こうたんせい)のレベルに基づいてアプリケーションが全てレビューされたか否か判定する。
- 全ての重要なアプリケーションが識別されたか否か判定する。
- ホット・サイトが、全てのシステム・ソフトウェアについて適正なバージョンを有しているか否かを判定する。ソフトウェアが全て互換性をもつことを検証する。（そうでなければ、システムは災害復旧中に本番データを処理することが不可能である。）
- 事業継続作業の担当者名簿、ホット・サイトの緊急連絡先、ベンダー緊急連絡先等について、その適切性、完全性をレビューする。
- 事業継続作業の担当者に対して、中断／災害状況における割り当てられた責任の理解度のインタビューを行う。
- テストについて文書化するための手順を評価する。
- マニュアルを更新するための手順を評価する。

b）前回のテスト結果の評価

BCP策定に責任を持つ者は、前回のテスト結果の履歴文書を保存しなければならない。IS監査人は、IS部門、エンドユーザー部門の両担当者によって行われたテスト結果をレビューし、テストの目標の達成度についてその網羅性、正確性を評価すると共に、必要な改善計画が組み込まれているかを判断する。

c）重要な要員へのインタビュー

IS監査人は業務オペレーションの復旧に関わる重要なスタッフへインタビューし、自身の責任、及び役割について理解しているかを確認する。これは同時にBCPの明確さと簡潔さを評価することにもつながる。

d）オフサイト保管の評価

オフサイト保管施設に存在する重要な媒体や文書は、オリジナルと同期がとられており、最新のものであることをもって評価される。また、IS監査人はオフサイト保管施設における在庫管理のレビューを実行する。

e）オフサイト施設におけるセキュリティの評価

オフサイト施設のセキュリティが、適切な物理的ならびに環境的アクセス管理を確実に備えていることを評価する。

f）代替処理契約のレビュー

IS監査人は、代替処理施設のベンダーとの契約を入手し、契約条項が全て文書化されていることを検証し、以下の項目等について確認する。

- 契約が明瞭で理解可能であること
- 他の組織体と共有で利用するサイトに適用される合意事項
- バックアップサイトの通信要件
- 保険の適用、補償範囲
- ホット・サイトにおける規則的なテストの実施
- 契約不履行時の取り決め

g）保険適用範囲のレビュー

保険は復旧に要する実費を填補することが必須である。保険料を考慮して、媒体における損害、業務の中断、装置の置換、事業継続処理などのための保険が適切かレビューする。

・ 練習問題、解答、解説については、ISACA®が発行する"CISA試験サンプル問題&解答・解説集"より抜粋しております。
（Copyright© by ISACA, reprinted with permission.）
・ 練習問題の問題番号については、アビタス編CISA®「MCカード」に掲載している番号を表示しています

295　論点042　事業継続計画（BCP）の概念

事業継続および災害復旧計画の最も主要な目的は次のどれか。

a. 重要な情報システム資産の保護
b. 業務の継続性の提供
c. 組織の損失の最小化
d. 人命の保護

303　論点043　BCP策定のプロセス

災害復旧計画（DRP）を含む業務継続計画（BCP）を策定する際、一番最初に行なうべき事項は次のどれか。

a. 復旧戦略を策定する。
b. ビジネス・インパクト分析を行なう。
c. ソフトウェア、ハードウェア、ネットワークの構成図を作成する。
d. 復旧チームメンバーを任命し、人員、役割、階層を定める。

305　論点043　BCP策定のプロセス

ビジネス・インパクト分析（BIA）を終えた後、事業継続計画プロセスにおける次のステップは、次のどれか。

a. 計画をテストし維持する。
b. 具体的な計画を策定する。
c. 復旧戦略を策定する。
d. 計画を実行する。

正解：d

人命は計り知れないほど貴重であるため、どのような事業継続および災害復旧計画においても人々の保護が主要な優先事項とされるべきである。よって正解はd。
他の全ての優先事項も重要であるが、事業継続および災害復旧計画の二次的な目的である。

正解：b

災害復旧計画(DRP)の第一ステップは、ビジネス・インパクト分析を行なうことである。他のすべてのタスクは、その後に行なう事項である。正解はb。

正解：c

事業継続計画策定における次のフェーズは、様々な復旧戦略を識別し、かつ災害から復旧するために最も適切な戦略を選択することである。戦略を選択した後に、具体的な計画を策定し、テストし、そして実行することができる。正解はc。

308　論点043　BCP策定のプロセス

組織が事業継続計画の一部としてビジネスインパクト分析(BIA)を完了した。このプロセスの次の段階は、何を策定することか。

a. 事業継続戦略。
b. テストと練習の計画。
c. ユーザートレーニングプログラム。
d. 事業継続計画(BCP)。

312　論点044　ビジネス・インパクト分析(BIA)

ビジネス・インパクト分析(BIA)の第一の目的は、次のどれか。

a. 災害後に、オペレーションを再開するための計画を提供する。
b. 組織のオペレーションの継続に影響を与える可能性がある事象を識別する。
c. 物理的・論理的なセキュリティに対する組織の方針を公表する。
d. 有効な災害復旧計画(DRP)のためにフレームワークを提供する。

315　論点044　ビジネス・インパクト分析(BIA)

情報システム監査人が、独立した立場からシステムの分類を行った際、あるシステムの機能は許容できるコストのもとで長期間手作業によっても代替可能であると判断された。この機能は次のどれに相当するか。

a. 重要(Critical)
b. バイタル(Vital)
c. センシティブ(Sensitive)
d. ノンクリティカル(Non-Critical)

321　論点044　ビジネス・インパクト分析(BIA)

組織にとって最適な事業継続戦略を決定するのは次のうちどれか。

a. 中断時間費用が最小、復旧費用が最大。
b. 中断時間費用と復旧費用の合計が最小。
c. 復旧費用が最小、中断時間費用が最大。
d. 中断時間費用と復旧費用の合計の平均。

正解：a

次の段階は、事業継続戦略である。事業継続戦略こそ、復旧するための最善の方法を特定するからである。この段階では、ビジネスプロセス、コスト、復旧に要する時間、及びセキュリティの重大性を検討しなければならない。よって正解はa。
復旧の戦略と計画の策定は、テスト計画より優先される。トレーニングを策定できるのは、BCPの実施後である。BCPを策定する前に、戦略を決定しなければならない。

正解：b

ビジネス・インパクト分析(BIA)は、事業継続計画(BCP)の立案の重要なステップの1つである。BIAは、組織のオペレーションの継続に影響を与える可能性のある種々の事象を識別する。よって正解はb。

正解：c

あるシステムの機能が、許容できるコストのもとで長期間手作業によっても代替可能とされる場合、それはセンシティブ機能として分類される。よって正解はc。
クリティカル機能とは、手作業による代替が不可能で、同一処理能力を持つ別のシステムでなくては引き継げない機能のことを指す。バイタル機能とは、手作業による代替が一応は可能だが、短期間しか持ちこたえることのできない機能のことを指し、クリティカル機能より一段階低い被害コスト・レベルを想定している。ノンクリティカル機能とは、ほとんど費用をかけずに長期間手作業による代替が可能で、復帰にもさほど時間やコストを要しない機能を指す。よってa, b, dは誤り。

正解：b

どちらの費用も最小化しなければならず、費用が最小の戦略が最適な戦略である。よって正解はb。
復旧費用が最大の戦略は、最適な戦略となり得ない。中断時間費用が最大の戦略は、最適な戦略となり得ない。中断時間費用と復旧費用の合計の平均は、最小の中断時間費用と復旧費用の合計よりも高くなる。よってa, c, dは誤り。

328　論点045　災害復旧戦略と災害復旧計画（DRP）

災害復旧計画が焦点をあてるのは次のどれか。

a. 業務継続計画の技術的側面
b. 業務継続計画の運用部分
c. 業務継続計画の機能的側面
d. 業務継続計画の全体的な調整

333　論点045　災害復旧戦略と災害復旧計画（DRP）

災害復旧計画（DRP）の導入後、その組織の障害前及び障害後のオペレーションコストはどのようになるか。

a. 減少する。
b. 変化はない。（同じである。）
c. 増加する。
d. ビジネスの性質に依存して増加または減少する。

342　論点046　BCPの詳細の策定

災害復旧の再配置チームの役割に含まれるのは次のどれか。

a. オフサイト保管のスケジュールを設定し管理すると共に、復旧に必要な媒体と記録を入手、梱包して、復旧施設に搬出する。
b. 復旧サイトが事前に決められていなければ定め、復旧サイトまでの従業員の輸送を調整する。
c. 移転プロジェクトの管理を行い、また施設や装置に対する被害のより詳細な評価を行う。
d. ホット・サイトから新しいサイトまたは修復された元のサイトへの移行のプロセスを調整する。

正解：a

災害復旧計画(DRP)は、業務継続計画の技術的側面である。業務再開計画(Business Resumption Planning)は、業務継続計画の運用部分に焦点をあてる。正解はa。

正解：c

あらゆる活動はコストを伴いDRPも例外事項ではない。DRPに関連してコストは発生するが、もしDRPが導入されなかったならば、不測のコストを被ることになる。正解はc。

正解：d

再配置チームの役割には、ホット・サイトから新しいサイトまたは修復された元のサイトへの移行のプロセスを調整することが含まれる。よって正解はd。
aはオフサイト・ストレージチームを、bは輸送チームを、cは復旧チームのことを指している。

346　論点046　BCPの詳細の策定

複数の国にITオペレーションセンターがある組織で中断のないオペレーションを確保する最良の方法を次の中から選びなさい。

a. 主要な手順文書の配布
b. ビジネスパートナー間の互恵協定
c. 強力な上級経営幹部のリーダーシップ
d. 業務継続計画(BCP) に関する従業員の研修

358　論点047　BCPテストの実施プロセス

事業継続計画のテストの主要な目的はどれか。

a. 従業員を事業継続計画に親しませるため。
b. 全ての残余リスクが扱われていることを保証するため。
c. 可能性のある全ての災害シナリオを実行するため。
d. 事業継続計画の限界を識別するため。

349　論点047　BCPテストの実施プロセス

事業継続計画(BCP)に適用すべき適切なテスト方法は、次のどれか。

a. パイロット・テスト
b. ペーパーテスト
c. ユニットテスト
d. システムテスト

正解：d

a. 手順文書は常に最新の状態に維持し、主要な場所に配布しなくてはならない。ただし、従業員が計画内での自らの役割を把握していなければ、文書のみでは不十分である。
b. 互恵協定は、類似した装置やアプリケーションを持つ2社以上の企業間の緊急時処理合意である。通常、互恵協定の参加者は緊急時に処理時間をお互いに提供することを約束している。事業運営の場所を持つことは業務継続において不可欠な要素だが、必ずしも互恵協定である必要はない。たとえば、一部のケースでは各従業員の自宅から事業運営を行うことがある。
c. 上級経営幹部は災害時にリーダーシップをすばやく発揮できるわけではない。このため、従業員がBCPにおける自らの役割を充分に把握しておくことが最も重要である。
d. 災害時には命令系統が中断される可能性がある。このため、従業員がBCPにおける自らの役割を把握しておくことは重要である(どこに報告して、どのように職務を遂行するかなど)。計画に関する従業員の研修は、地理的に離れたオフィスのあるビジネスにとっては特に重要である。通信が中断される可能性がより高いためである。

正解：d

事業継続計画のテストは、存在するかもしれない限界の最高の証拠を与える。よって正解はd。
従業員を事業継続計画に親しませるというのは、テストの二次的な利益であるためaは誤り。残余リスクを事業継続計画で扱うことは費用効率が悪く、可能性のある全ての災害シナリオをテストするのは現実的ではないためb, cは誤り。

正解：b

ペーパーテストは、BCPをテストするのに適している。それは、計画全体、または計画の一部のウォークスルーであり、特定の災害において発生しうる事態を解決する計画実行の主要担当者が参加する。正解はb。
a, cおよびdは、BCPに適していない。

353　論点047　BCPテストの実施プロセス

次に示す災害復旧に関するテスト手法のうち、計画の有効性を判定する上で最も効果的な方法はどれか。

a. 準備テスト
b. ペーパーテスト
c. 全オペレーション・テスト
d. 実際のサービス停止

372　論点048　BCPにおける情報システム監査人の役割

事業継続計画(BCP)の有効性を評価する最も良い方法は、次のどれをレビューすることか。

a. 計画及び、計画と適切な基準との比較
b. 前回のテストの結果
c. 緊急事態における手順と従業員に対する訓練
d. オフサイトにおける記録保管と環境コントロール

376　論点048　BCPにおける情報システム監査人の役割

情報システム監査人は業務継続計画(BCP)について、組織体の主要な利害関係者にインタビューをして、彼らが役割と責任を理解しているか判断する。情報システム監査人は、次のどれの評価を試みているか。

a. 事業継続計画の明確さと簡潔さ
b. 事業継続計画の妥当性
c. 事業継続計画の有効性
d. 情報システムとエンドユーザーの緊急時の効率的な対応能力

正解：a

準備テストには(各フェーズにおける)全体環境のシミュレーションが含まれており、チームが実際のテストのシナリオへの理解を深め、準備を整える上で役立つ。よって正解はa。
b, c, dは、根拠を得るための方法としては経済的な方法ではない。ペーパーテストは全体計画のウォークスルーテストであるが、シミュレーションは含まれておらず、学習できる内容も少ない。また、チームが試験計画をよく理解したという確証を得ることは困難である。dはほとんどの場合に推奨されない。またcは経営者による承認が必要と考えられ、多くの場合、テストの実施は容易でないかまたは現実的でなく、そのテスト自体が大事故の引き金になる可能性もある。

正解：b

前回のテスト結果から、事業継続計画の有効性の証拠が得られる。正解はb。
基準と比較することは、事業継続計画が重要な側面に対処することを保証するが、計画の有効性についてはなにも明らかにしないためaは誤り。緊急事態における手順のレビューや、オフサイトにおける記録保管状況と環境コントロールのレビューは、計画の一部の側面に対する見識を提供するが、計画の全体的な有効性を保証するには不十分であるためc, dは誤り。

正解：a

情報システム監査人は、主たる利害関係者が彼らの役割と責任をどの程度よく理解しているか評価するためにインタビューすべきである。利害関係者全員が災害時の彼らの役割と責任を詳細に理解していれば、情報システム監査人は、事業継続計画が明確且つ簡潔であると判断することができる。よって正解はa。
妥当性を評価するには、計画をレビューし、適切な基準と比較すべきであるためbは誤り。有効性を評価するには、前回のテスト結果をレビューするべきであり、これが有効性を評価する最良の判断であるためcは誤り。緊急時の手続と従業員の訓練は、組織体が有効に対応する計画を導入しているか否かを判断するためにレビューされなければならない。dは誤り。

CISA®

Certified Information Systems Auditor™

サンプルテキスト

2013年 7 月15日 第 4 版第 1 刷発行
2015年 4 月 1 日 第 5 版第 1 刷発行

編者：三輪　豊明

発行：株式会社アビタス

Abitus

〒151-0053
東京都渋谷区代々木 2 - 1 - 1
新宿マインズタワー15F
03-3299-3222（phone）
03-3299-3777（facsimile）
http://www.abitus.co.jp