

平成 30 年度春期応用情報技術者試験 午後問 10「データセンタで行うシステム運用」徹底復習・分析レポート

1. 本問題の出題趣旨と IT サービス運用の背景分析

近年、多くの企業において、システム運用の効率化・低コスト化、高い可用性や信頼性の確保、さらには大規模災害時の事業継続計画（BCP）の策定といった経営課題に対応するため、自社内の情報システムおよびファシリティをデータセンタ（DC）へ移設・委託する動きが定着しています。このような背景を踏まえ、本問題ではデータセンタを活用したシステム運用環境を舞台に、インシデント管理、電源を中心とするファシリティ管理、および災害対策（BCP）に関する実務的な運用管理能力を多角的に問う構成となっています。

IT サービスマネジメントおよびファシリティ運用の観点から本事例の全体像を捉えるため、まずは T 社 DC が提供する主要なサービス形態である「ハウジングサービス」と「ホスティングサービス」の定義および両者における責任分界を比較・整理します。

DC サービス形態の比較

DC サービス形態	定義・特徴および責任分界（所有権・保守・監視・増設・UPS 管理）
ハウジングサービス	【定義】 顧客が所有する情報機器を DC のラック・ラックエリア（サーバ室）に設置し、顧客が専用で使用する形態。 【責任分界】 ・サーバ等の所有者：顧客 ・維持メンテナンス管理責任：顧客 ・性能監視・稼働監視主体：顧客 ・機器の増設管理責任：顧客 ・UPS（無停電電源装置）の管理主体：顧客（顧客自身が自ら設置・管理するルール）
ホスティングサービス	【定義】 T 社（DC 事業者）が所有する情報機器を DC に設置し、顧客が専用または共同で利用する形態。 【責任分界】 ・サーバ等の所有者：T 社（DC 事業者） ・維持メンテナンス管理責任：T 社（DC 事業者） ・性能監視・稼働監視主体：T 社（DC 事業者） ・機器の増設管理責任：T 社（DC 事業者） ・UPS（無停電電源装置）の管理主体：T 社（DC 事業者自身が提供・維持管理を実施）

電源設備の冗長化構造の評価

データセンタ運用における電源ファシリティは、IT サービスの継続稼働を支える最重要インフラであり、極めて高い信頼性と可用性が求められます。本事例の DC では、以下に示す多層的かつ重厚な電源アーキテクチャが構築されています。

- **商用電源（常用電源）**：電力会社から定常的に供給される電力（通常時の給電ライン）。
- **自家発電設備**：長時間の停電事故に対応するための予備電源設備。燃料等により 72 時間連続で安定的な電力供給を維持できる性能を有する。
- **UPS（無停電電源装置）**：商用電源の瞬断や、商用電源と自家発電設備との切り替えに伴う短時間の給電異常時に、内蔵蓄電池から即座に電力を供給し、電圧低下や給電断を補償する装置。通常時は常用電源により充電が行われる。

T 社 DC では、電力会社および自家発電設備からの供給経路（配線ライン）や、ホスティングサービスで提供される UPS 設備に対して、単一故障点（SPOF：Single Point of Failure）を網羅的に排除するた

めの**冗長構成（二重化）**が施されています。

ここで実務的・技術的に着目すべきは、**「T 社が提供・管理するホスティングサービス側の電源ラインが二重化で冗長保護されているのに対し、ハウジングサービスを利用する U 社の専用 UPS 環境は『一つの UPS ユニットだけから成るシステム』であり、内部冗長を持たない単一構成であった」**という決定的な事実です。このファシリティ構成上の非冗長性（SPOF の存在）こそが、後述する電源切戻し時の全停止インシデントを引き起こす構造的な前提条件となっています。

DC 運用の基本構造とサービス形態別の責任領域を整理したところで、次に実際発生した電源障害インシデントのタイムラインとその問題点について詳細に考察します。

2. 電源障害インシデントの時系列解析と事象の構造化

送電線事故に端を発する電源障害からシステム再稼働、そして深夜のバッテリー交換作業に至る一連の経緯（表 4）を把握することは、インシデント対応の遅延要因や運用プロセスの欠陥を構造的に解明する上で極めて重要です。

障害対応タイムラインの整理

時刻	事象の概要	ステータス／処理分類
13:00	送電線事故により DC への電力供給が途絶。DC は自家発電を開始。自家発電が安定稼働するまでの間、U 社 UPS が蓄電池運転でサーバへ電力を供給。DC より L 氏へ状況連絡。	初動対応（自動切替・通知）
13:05	自家発電の稼働により常用電源が指定許容範囲内で安定。U 社 UPS は通常運転状態へ復帰。	通常運転復帰
14:30	電力会社からの電力供給復旧と安定供給を確認。DC は切戻し判断を行い、L 氏へ連絡。	切戻し準備・事前連絡
14:40	DC が切戻し作業を開始。U 社 UPS が蓄電池運転を開始したが間もなく給電停止し、サーバおよび U システムが停止。運用監視コンソールに“異常”メッセージが出力され、L 氏が DC に確認依頼。	障害発生（1）：電源完全停止（項番 4）
14:50	DC より電源切戻し完了とサーバ停止状態の回答を受け、L 氏が DC にサーバ起動を依頼。	状況確認・起動依頼
15:00	L 氏がサーバ起動を確認後、U システム開始作業を行うが稼働せず。コンソールに「データベース異常」メッセージが出力。L 氏が上長へ報告し、上長が復旧対策本部の設置を依頼。	障害発生（2）：DB 起動失敗（項番 6）・階層的エスカレーション
15:10	DC にて他システムの正常稼働を確認し、自家発電設備の運転を停止。	DC ファシリティ正常化
15:15	U 社内に復旧対策本部が発足。調査により、急な停止によるデータベース不整合が判明。回復手順未確立のため開発課による作業が必要と特定。	原因特定・対応方針決定
15:25	開発課がデータベースの回復作業を開始（約 30 分で完了）。	機能的エスカレーション（専門部署による作業）
15:55	L 氏が U システムの開始作業を行い、システムが再稼働。	システム復旧完了

深夜	UPS の保守業者が U 社 UPS の蓄電池交換を実施。	根本原因に対する保守作業
----	-------------------------------	--------------

障害発生要因の多角分析

本インシデントでは、外部からの給電事故を直接の引き金としながらも、自社運用の領域において 2 つの致命的なボトルネックが発生し、障害被害を著しく拡大させました。

1. U 社 UPS の蓄電池劣化による切戻し時の給電停止（項番 4）

- **要因分析：** 数日前の自動セルフチェックにおいて運用監視コンソールに「蓄電池の劣化が進んでいる」旨のメッセージが出力されていたにもかかわらず、その重要度分類が「通知（インシデントとして扱わない）」に設定されていたため、担当の L 氏は調査・対処を実施しませんでした。さらに、交換推奨時期を超過していたにもかかわらず、運用課と保守業者間でのスケジュール調整が怠られていました。
- **メカニズムと影響度：** U 社 UPS が単一構成（非冗長）であったため、商用電源への切戻し時（電源ラインの一時的な切り離し）に劣化していた蓄電池が給電状態を維持できず即座に電力供給がダウンし、稼働中のサーバ群が物理的に遮断されました。

2. データベース不整合による起動失敗（項番 6）

- **要因分析：** サーバ電源の突発的な遮断により、**「U システムが正常に停止していなかったこと（適切な OS/DBMS のシャットダウンプロセスを経ずに強制終了したこと）」**が直接原因となり、メモリ上のデータ未書き込みやトランザクション不整合が生じました。さらに、運用課において手動回復の手順（SOP）が事前に整備されておらず、L 氏が「階層的エスカレーション（上長報告・対策本部立ち上げ）」のみを優先させたため、DB 保守を担う「開発課」への「機能的エスカレーション」にタイムラグが生じました。
- **メカニズムと影響度：** 不整合が発生した状態での起動再試行が繰り返された上、専門部署への引き継ぎが遅れたことで、不必要なダウンタイムが 1 時間以上伸長する事態となりました。

相互関係と構造的影響： ファシリティ管理の欠陥（イベント分類ミスと部品サイクル軽視による UPS 停止）が一次障害として電源遮断を引き起こし、それがアプリケーション・データ層での二次障害（DB 不整合）を誘発しました。さらに運用ルールの不備（回復手順の未確立およびエスカレーション経路の遅延）が重なったことで、MTTR（平均修理時間）および RTO（目標復旧時間）を著しく悪化させる要因となりました。

障害の時系列と問題点を明確にした上で、次に設問ごとの具体的な解説と正解に導く思考プロセスへ進みます。

3. 設問別詳細解説と解答の論理的思考プロセス

試験対策および実務における知見定着の観点から、設問の解答根拠をソーステキストおよび ITSM の標準理論に基づいて導出するプロセスを論理的に解説します。

設問 1（DC サービス形態とファシリティ）

（1）ハウジングサービスの特徴についての選定

- **論理的解説：** ハウジングサービスは、DC 事業者のラック空間や電源設備等を借用し、自社所

有のサーバ機器等を持ち込んで運用する形態です。したがって、設置されたサーバハードウェア自体の所有権、保守メンテナンス、監視、増設などの責任はすべて顧客側に帰属します。

- **ア（誤り）**：顧客所有の機器であるため、維持メンテナンス責任は顧客自身にあります。
- **イ（正解）**：サーバ稼働状態や性能監視（CPU/メモリ/ディスク使用率等）は、機器を管理する顧客側が行います。
- **ウ（誤り）**：サーバの増設判断および作業手配は所有者である顧客が行います。
- **エ（誤り）**：サーバは顧客が自前で調達・所有するものであり、T社から提供されるものではありません。

- **正解：イ**

(2) 空欄[a]に当てはまる字句

- **論理的解説**：DCにおいて単一障害点（SPOF）を排除し、高い信頼性を維持・確保するためには、供給経路や各種機器を多重化（二重化）しておく必要があります。問題文中では「電力会社及び自家発電設備からの電力供給経路並びにホスティングサービスで提供しているUPSは、全て[a]にしている」と示されており、これに該当する技術用語は「冗長構成」（または「二重化」）です。
- **正解：冗長構成**（別解：二重化）

設問2（インシデント管理とエスカレーション）

(1) 下線①（L氏が調査を行わなかった点）に対する改善内容

- **論理的解説（ITIL イベント管理の視点）**：ITILの「イベント管理（Event Management）」において、システムから発せられるイベントメッセージは「情報（通知）」「警告」「異常（例外）」に適切に分類されなければなりません。U社の標準ルールでは「警告」または「異常」と分類されたメッセージのみをインシデントとして扱い、調査・対応を行う規定になっていました。しかし、「蓄電池の劣化が進んでいる」という重大な障害予兆メッセージが「通知（インシデントとして扱わない）」に設定されていたため、L氏は対応を行いませんでした。蓄電池劣化による電源障害を未然に防ぎ、適切な調査・交換手配を行わせるためには、本メッセージの分類をインシデント取り扱い対象である**“警告”**へと見直すことが不可欠です。
- **解答例**：蓄電池の劣化を示すメッセージの種類を“警告”とする。（28字 / 制限文字数：35字以内）

(2) 下線②（機能的なエスカレーション）の具体的内容

- **論理的解説（階層的エスカレーション vs 機能的エスカレーション）**：インシデント対応における「階層的エスカレーション（Hierarchical Escalation）」とは、役職や組織の管理ラインに沿って上長へ報告し、組織的判断や対策本部の設置を仰ぐ手続きです。一方、「機能的エスカレーション（Functional Escalation）」とは、担当者のスキルを超えた専門的技術問題が発生した際に、適切な専門知識・権限を持つ技術部署へ直接調査や復旧支援を依頼する手続きを指します。L氏は「データベース異常」のメッセージを確認した際、上長への報告（階層的）のみを行いましたが、UシステムのDB運用・保守を担当している専門部署である**「開発課」**へ直ちに対応・支援を依頼する（機能的）べきでした。

- 解答例：開発課にインシデントの対応を依頼する。(19 字 / 制限文字数：25 字以内)

(3) 再発防止策として早期に実施すべきことの選定

- 論理的解説（プロアクティブな問題管理とアセット管理）：今回のインシデントの根本原因は、UPS 蓄電池の交換推奨時期を超過していたにも関わらず、運用課と保守業者との間で適切な調整が行われず放置されていた点にあります。「プロアクティブな問題管理」および「ライフサイクル・アセット管理」の観点から、ハードウェア構成部品の寿命に基づく交換周期を厳密に管理・遵守することが最も根本的かつ即効性のある再発防止策です。
 - ア、ウ、エは事象の根本要因に対する直接的な解決策にはなりません。
- 正解：イ（U 社 UPS の構成部品交換周期の遵守）

設問 3（BCP・災害対策と提案）

(1) 下線③で T 社が用意している計画の名称

- 論理的解説：広域停電や大規模震災などの不測の事象が発生した際、事業継続への影響を最小限に抑え、あらかじめ定めた復旧目標時間内で重要な IT サービスを復旧・再開するための非常時対応計画は、一般に「ディザスタリカバリプラン（DRP：Disaster Recovery Plan）」、「コンティンジェンシープラン」、あるいは「緊急時対応計画」と呼ばれます。
- 解答例：ディザスタリカバリプラン（別解：コンティンジェンシープラン / 緊急時対応計画 / 制限文字数：20 字以内）

(2) 下線④（障害対策訓練の有効性向上）に向けた要請内容

- 論理的解説（対策シナリオの矛盾検知と実効性検証）：DC 事業者（T 社）が単独で策定・実施する障害対策訓練では、机上の想定にとどまり、実際の顧客運用現場における実作業や連携手順と乖離してしまうリスクがあります。訓練の有効性を真に向上させるためには、実際に現場で U システムを運用管理している「運用課」から担当者を選定・参加させることが求められます。実務担当者が訓練に参加することで、**「現実の運用業務に照らし合わせた際の災害対策シナリオの矛盾や手順のギャップを現場目線で発見・指摘し、解消すること」**が可能となります。
- 解答例：運用課から担当者を選定し、該当者に障害対策訓練に参加してもらう。(32 字 / 制限文字数：40 字以内)

設問と解答のサマリ

設問番号	正解・解答例	解説のキーポイント
設問 1 (1)	イ	ハウジングサービスにおける機器の維持・保守・性能監視責任はすべて顧客側にある。
設問 1 (2)	冗長構成 （別解：二重化）	SPOF を排除し、高い稼働率と信頼性を確保するための構成方式。
設問 2 (1)	蓄電池の劣化を示すメッセージの種類を“警告”とする。	イベント管理の見直し。インシデント対象外の「通知」から対応対象の「警告」へ変更する。
設問 2 (2)	開発課にインシデントの対応を依頼する。	階層的報告にとどまらず、DB 運用を担当する技術専門部署（開発課）へ即座に機能的エスカレーション

		を行う。
設問 2 (3)	イ	予防保守・アセット管理徹底のため、部品交換周期の遵守を最優先で実施する。
設問 3 (1)	ディザスタリカバリプラン （別解：コンティンジェンシープラン／緊急時対応計画）	広域災害や大規模障害に備えた緊急時対応計画。
設問 3 (2)	運用課から担当者を選定し、該当者に障害対策訓練に参加してもらう。	現場の運用担当者を訓練に巻き込むことで、対策シナリオの矛盾や課題を発見・修正する。

設問ごとの解答根拠と背景理論を網羅した上で、最後に本事例から得られるシステム運用およびファシリティ管理の実務的教訓を取りまとめます。

4. 実務に活かすシステム運用・ファシリティ管理の教訓

過去問分析のゴールは、解法の丸暗記ではなく、自社のシステム運用やファシリティ管理体制における脆弱性を洗い出し、改善策へ昇華させることにあります。本事例から抽出された実務上の教訓を以下のチェックリストとして提示します。

運用改善チェックリスト

- ITIL イベント管理に基づく監視メッセージ分類の最適化・SOP 化
 - 各種機器（UPS 等のファシリティ設備含む）から発せられるログ・メッセージについて、単なるステータス表示（通知）と障害予兆（警告）の線引きを定期的に見直す。
 - 「警告」検知時には自動的に一次対応チケットが起票されるインシデント管理手順を SOP（標準作業手順書）化する。
- ライフサイクル・アセット管理と部品交換計画の厳格化
 - UPS 蓄電池やファン等の劣化消耗部品について、保守業者任せにせず、自社の予防保守スケジュールに組み込んで Lifecycle Management を徹底する。
 - 「アラートが出ていないから」と交換を先延ばしにせず、構成部品交換周期の遵守を徹底する。
- デュアル・エスカレーションパスの整備と RTO（目標復旧時間）短縮
 - 重大インシデント発生時には、組織的判断を仰ぐ「階層的エスカレーション」と、専門部署に技術対処を委ねる「機能的エスカレーション」を並行して即座に実行する体制を整備する。
 - 専門部署（開発課等）への緊急連絡ルートや一次対応マニュアルをあらかじめ策定し、復旧時間（RTO）の短縮を図る。
- 非正常停止（電源断）に備えたリカバリ手順の事前確立
 - 突発的な電源断により DBMS 等のアプリケーションが正常終了しなかった場合の不整合回復手順（Rollback / Rollforward / 整合性チェック等）をドキュメント化し、運用担当者が即座に参照・実行できる状態を整備する。
- DC 事業者との協働 BCP 訓練による対策シナリオの矛盾解消
 - DC 事業者が提供する DRP（ディザスタリカバリプラン）や災害対策訓練には、自社の実務運用担当者を積極的に参加させる。

- 実業務に即した模擬訓練を通じて、対策シナリオに潜む手順の矛盾、連絡体制の欠陥、運用ギャップを発見・修正する継続的改善（PDCA）サイクルを回す。

まとめ

どれほど堅牢な物理ファシリティ（自家発電機や二重化電源）を誇るデータセンタを利用していたとしても、顧客側の設備における「単一故障点（SPOF）」の放置、監視メッセージの誤評価、ならびにエスカレーションの遅れが存在すれば、システム全体としての可用性は著しく低下します。

システムの安定稼働とインシデント発生時の被害最小化を実現するためには、ファシリティの物理的構成管理から ITSM の各種プロセス（イベント管理・インシデント管理・問題管理）、そして組織的な BCP 訓練に至るまで、**「ファシリティ管理と運用体制の密接かつ組織的な連携」**を確立することが不可欠です。