インフラ実務スキルチェック
解説集（50問・統合版）

本資料は社内試験・勉強会・自己学習用途を目的として作成された解説集です。
各設問について、正解（選択肢付き）・解説・実務ポイントを収録しています。

Q1. ディスク容量は空いているにもかかわらず、新規ファイル作成時にエラーが発生する主な原因はどれか。

【正解】B) inode 枯渇

【解説】ディスク容量（ブロック）と inode は別管理であり、小さなファイルが大量に生成されると inode が枯渇する。

【実務ポイント】df -i で inode 使用率を確認し、ログ肥大や一時ファイルの大量生成を疑う。

Q2. systemd サービスが起動直後に停止する場合、最も典型的な原因はどれか。

【正解】A) ExecStart のパス誤り

【解説】systemd は ExecStart に指定された実行ファイルが存在しない場合、即座にサービスを停止する。

【実務ポイント】systemctl status と which コマンドで実体を確認する。

Q3. SSH 接続時にログイン完了までに時間がかかる原因として一般的なものはどれか。

【正解】C) DNS 逆引き遅延

【解説】sshd は接続元 IP の逆引きを行うため、PTR レコード未設定時にログイン遅延が発生する。

【実務ポイント】dig -x による逆引き確認、UseDNS 設定を確認する。

Q4. Linux サーバが予期せず再起動した場合、最初に確認すべきログはどれか。

【正解】C) /var/log/messages または journal

【解説】Linux で予期しない再起動が発生した場合、まず確認すべきなのは OS／カーネルレベルのイベントである。 /var/log/messages や journalctl には、kernel panic、OOM Killer の発動、手動 reboot / shutdown の痕跡、ハードウェアエラー通知などが記録される。 アプリケーションログは OS が正常稼働している前提で出力されるため、再起動原因の一次情報にはならない。

【実務ポイント】last reboot で再起動時刻を把握し、journalctl -b -1 で直前ブートのログを確認する。クラウド環境ではホスト障害か OS 内要因かを切り分ける。

Q5. CPU 使用率は低いにもかかわらず Load Average が高い場合に疑うべき要因はどれか。

【正解】C) I/O wait の増加

【解説】Load Average は CPU 使用率だけでなく、実行待ち状態（D state）のプロセス数も含めて計算される。 ディスク I/O が詰まっている場合、CPU は空いていてもプロセスは I/O 完了待ちとなり、結果として Load Average が上昇する。

【実務ポイント】top / vmstat で wa（I/O wait）を確認し、iostat でディスク待ち時間を確認する。CPU低負荷＝問題なしと判断しない。

Q6. Windows Server に RDP 接続できない場合、初動として確認すべき項目はどれか。

【正解】C) ファイアウォールとポート開放状況

【解説】RDP は TCP/3389 を使用するため、最初に確認すべきは通信経路が成立しているかである。 Windows ファイアウォール、セキュリティグループ / NW ACL、RDP サービスの起動状態を確認せずに OS や AD を疑うのは順序が逆。

【実務ポイント】Test-NetConnection -Port 3389。FW → サービス → 認証の順で切り分ける。「接続できない」と「認証できない」は別問題。

Q7. DNS 名では接続できないが、IP
アドレスでは接続できる場合の原因として考えられるものはどれか。

【正解】B) DNS 設定不備

【解説】IP 直指定で通信できるということは、ネットワーク経路およびサービス自体は正常である。
問題は名前解決フェーズに限定されるため、DNS レコード・参照先・キャッシュが疑点となる。

【実務ポイント】nslookup / dig で名前解決確認。DNS キャッシュ（OS／アプリ）に注意。TTL
切れまで直らないケースあり。

Q8. サーバ認証が不安定な場合に、OS 観点でまず疑うべき基本要因はどれか。

【正解】C) 時刻ずれ（NTP）

【解説】Kerberos、証明書認証、AD 連携などは時刻同期が前提条件となっている。
数分のずれでも、認証失敗や断続的なログイン不可といった症状が発生する。

【実務ポイント】timedatectl / w32tm /query /status。NTP
サーバ到達性確認。「たまに失敗する認証」は時刻ずれを疑う。

Q9. Linux サーバで cron が設定どおりに実行されない原因として多いものはどれか。

【正解】C) 実行パス未指定（PATH 問題）

【解説】cron は対話シェルと異なり、最低限の環境変数しか読み込まない。
そのため、コマンドの絶対パス未指定や環境変数前提のスクリプトは cron 実行時に失敗しやすい。

【実務ポイント】スクリプト内で絶対パス指定。cron ログ（/var/log/cron）確認。手動実行できても cron
失敗は典型。

Q10. 高負荷状態の Linux サーバで、最初に実行すべき確認コマンドはどれか。

【正解】C) top / vmstat 等の負荷確認

【解説】高負荷時にいきなり再起動や設定変更を行うと原因を消してしまう。 まずは CPU・メモリ・I/O
のどこがボトルネックかを可視化する必要がある。

【実務ポイント】top → vmstat → iostat
の順。数値を見てから対処。「まず見る」ができるかが中堅以上の分かれ目。

Q11. Windows サービスが「Starting」のまま起動しない場合に考えられる原因はどれか。

【正解】B) 依存サービスの未起動

【解説】Windows サービスは他サービスへの依存関係を持つことが多く、依存先が停止していると起動処理に入れず「Starting」のまま待ち続ける。

【実務ポイント】サービスの依存関係タブ確認。sc qc
で依存関係を把握し、再起動前に依存サービスを確認する。

Q12. Windows 環境で DNS キャッシュをクリアする正しい方法はどれか。

【正解】B) ipconfig /flushdns

【解説】Windows は OS レベルで DNS
キャッシュを保持しており、名前解決問題の切り分けでは安全にキャッシュのみをクリアする必要がある。

【実務ポイント】DNS 変更後に疎通しない場合に実施。再起動より影響が小さい。

Q13. IIS で HTTP 500 エラーが発生した場合、初動対応として適切なものはどれか。

【正解】B) アプリケーションログ確認

【解説】HTTP 500 は Web サーバ自体は応答しているが、アプリ内部で例外が発生していることを示す。

【実務ポイント】IIS ログと Event Viewer（Application）を確認。500 は NW 問題ではない。

Q14. Windows Update が異常に長時間かかる場合、まず確認すべき点はどれか。

【正解】C) 更新履歴・エラーコード

【解説】更新処理停滞は内部エラーのリトライが原因であることが多く、エラーコードにより原因を特定できる。

【実務ポイント】更新履歴詳細と Get-WindowsUpdateLog を確認。

Q15. Windows 環境で CPU 使用率の高いプロセスを特定する方法はどれか。

【正解】B) タスクマネージャ／Resource Monitor

【解説】リアルタイムでどのプロセスが CPU を消費しているかを即座に確認できる。

【実務ポイント】PID を控え、スパイクか常時高負荷かを切り分ける。

Q16. グループポリシーがクライアントに反映されているか確認する方法はどれか。

【正解】B) gpresult /r

【解説】実際に適用されている GPO の結果セットを確認でき、設定画面だけでは判断できない。

【実務ポイント】ユーザ／コンピュータ両方を確認し、優先度に注意。

Q17. Active Directory ドメイン参加に失敗する典型的な原因はどれか。

【正解】B) 時刻ずれ

【解説】AD 参加は Kerberos 認証が前提であり、クライアントと DC の時刻差があると失敗する。

【実務ポイント】w32tm で時刻同期確認。DNS → 時刻 → 認証の順で確認。

Q18. Windows で不正ログインを検知する際に重要なイベント ID はどれか。

【正解】A) 4625（ログオン失敗）

【解説】4625 は認証失敗を示し、短時間に多数発生している場合は攻撃兆候となる。

【実務ポイント】発生元 IP とアカウントを確認し、監査ポリシーを有効化。

Q19. Linux サーバで sudo 実行時に認証エラーが発生する原因として考えられるものはどれか。

【正解】A) /etc/sudoers 設定不備

【解説】sudo は sudoers 設定に厳密で、記述ミスや権限不足があると実行が拒否される。

【実務ポイント】visudo で編集。グループ指定ミスに注意。

Q20. yum / dnf 実行時に 404 エラーが発生する主な原因はどれか。

【正解】C) リポジトリ URL 不正・到達不可

【解説】指定されたリポジトリが存在しない、または到達できないことを示す。

【実務ポイント】repo 定義と OS サポート期限、ミラー URL を確認。

Q21. ALB のターゲットが Unhealthy と判定される主な原因はどれか。

【正解】B) ヘルスチェック失敗

【解説】ALB はヘルスチェック設定（パス・ポート・ステータスコード）に基づいて正常性を判定する。アプリが起動していても、条件を満たさなければ Unhealthy となる。

【実務ポイント】ヘルスチェックパス実体、ALB→ターゲットの SG 通信、ステータスコードを確認。

Q22. ALB 経由の通信で 502 エラーが発生する場合に疑うべき要因はどれか。

【正解】B) バックエンドアプリ異常

【解説】502 は ALB がターゲットから正常な応答を受け取れなかったことを示す。ALB 自体ではなくアプリ側異常が原因のことが多い。

【実務ポイント】ターゲット側ログ最優先。ALB とアプリのタイムアウト値不一致に注意。

Q23. RDS への接続数が増加し続ける原因として考えられるものはどれか。

【正解】B) コネクションリーク

【解説】アプリが DB コネクションをクローズせず使い回さない場合、RDS の接続数は増加し続ける。DB 側ではなくアプリ設計の問題が多い。

【実務ポイント】RDS メトリクスで接続数推移確認。再起動は一時回避に過ぎない。

Q24. AWS の月額請求額が急増した場合、最初に確認すべきサービスはどれか。

【正解】B) Cost Explorer

【解説】請求増加時はリソース停止前に、どのサービス・リージョンで増えたかを可視化する必要がある。

【実務ポイント】日次・サービス別で確認。NAT Gateway やデータ転送が典型原因。

Q25. S3 へのアクセスで 403 エラーが返る原因として正しいものはどれか。

【正解】B) IAM / バケットポリシー不備

【解説】403 はオブジェクト不存在ではなく権限不足を示す。IAM、バケットポリシー、BPA の影響を受ける。

【実務ポイント】IAM→バケットポリシー→BPA の順で確認。403 と 404 の意味の違いを理解。

Q26. Route53 を使用しているにもかかわらず名前解決できない場合の確認ポイントはどれか。

【正解】B) レコード設定・委任状態

【解説】レコードがあっても親ドメインから正しく委任されていなければ解決されない。外部レジストラ利用時に多い。

【実務ポイント】NS レコード一致確認、TTL 反映遅延に注意。dig で解決段階を確認。

Q27. EC2 の CPU 使用率が常に高止まりしている場合の対処として適切なものはどれか。

【正解】B) スケール（垂直／水平）検討

【解説】恒常的な高負荷はリソース不足が原因であることが多く、再起動では解消しない。

【実務ポイント】一時的か恒常的かを見極め、インスタンスタイプ変更や ASG を検討。

Q28. Lambda 関数がタイムアウトする原因として考えられるものはどれか。

【正解】B) 外部通信遅延（VPC / NAT）

【解説】VPC 内 Lambda は外部通信時に NAT を経由するため、構成不備や遅延でタイムアウトしやすい。

【実務ポイント】実行時間メトリクス確認、VPC/NAT 構成確認、タイムアウト値調整。

Q29. CloudWatch Logs のデータ量が急増した場合に疑うべき要因はどれか。

【正解】B) 不要なログ出力増加

【解説】CloudWatch Logs は出力量課金であり、デバッグログや無限ループ出力で急増する。

【実務ポイント】ログレベル見直し、保持期間設定、出力頻度制御。

Q30. EBS の I/O 性能が期待どおりに出ない場合に確認すべき設定はどれか。

【正解】B) ボリュームタイプ／IOPS 設定

【解説】EBS 性能はボリュームタイプと IOPS 設定に依存する。仕様上限を超える性能は出ない。

【実務ポイント】ボリュームタイプ確認、CloudWatch で I/O wait 確認。gp3 検討。

Q31. EC2 インスタンスが起動しない場合、初動として確認すべき項目はどれか。

【正解】B) システムログ・ステータスチェック

【解説】OS 起動前の問題はインスタンス内部から確認できないため、AWS 提供ログを確認する。

【実務ポイント】ステータスチェック結果、システムログ、AMI/ボリューム破損の可能性。

Q32. オートスケーリングが期待どおりに動作しない原因として考えられるものはどれか。

【正解】B) スケーリング条件不適切

【解説】ASG は条件を満たさなければ動作しない。しきい値や評価期間の設定ミスが多い。

【実務ポイント】CloudWatch アラーム条件確認、テスト発火確認。

Q33. IAM 設計で避けるべき典型的なアンチパターンはどれか。

【正解】C) 管理者権限の常用付与

【解説】過剰権限は誤操作・侵害時の影響範囲を拡大させる。最小権限が基本。

【実務ポイント】管理者権限は一時付与、ロール利用、定期棚卸し。

Q34. AWS 環境で障害調査を行う際に最初に確認すべきログはどれか。

【正解】B) CloudTrail / サービスログ

【解説】CloudTrail により誰が何を変更したかを把握でき、設定変更起因の障害切り分けが早い。

【実務ポイント】変更履歴有無確認、手動操作と自動化の区別。

Q35. KMS 関連のエラーが発生した際に確認すべき点はどれか。

【正解】B) キーの有効状態・権限

【解説】KMS エラーはキー無効化や IAM 権限不足が原因のことが多い。

【実務ポイント】キー状態確認、IAM ポリシー確認、削除待機に注意。

Q36. ping は通らないが Web アクセスは可能な場合に考えられる理由はどれか。

【正解】B) ICMP 制御

【解説】ping は ICMP を使用するが、多くの環境では ICMP を遮断している。一方 HTTP/HTTPS は TCP を使用するため通信可能な場合がある。

【実務ポイント】ping 不可＝NW断と即断しない。curl 等で TCP レイヤ確認。

Q37. HTTPS 通信のみが遅延する場合に疑うべき要因はどれか。

【正解】B) TLS ハンドシェイク処理

【解説】HTTPS では TLS ハンドシェイクが発生し、証明書や暗号設定不備で遅延が起こる。

【実務ポイント】curl -v で TLS 処理確認。証明書チェーンを点検。

Q38. NAT 環境下で外部通信できない場合の典型的な原因はどれか。

【正解】B) NAT 設定不備

【解説】NAT ではルートや変換設定が正しくなければ外部通信は成立しない。

【実務ポイント】ルーティングテーブルと NAT デバイス稼働を確認。

Q39. Web サイトの表示が断続的に遅くなる原因として考えられるものはどれか。

【正解】B) 負荷分散不備／リソース枯渇

【解説】特定条件下でのみ遅延する場合、LB 配下ノードの偏りや一部障害が疑われる。

【実務ポイント】LB ログとノード別メトリクス確認。

Q40. TCP の 3 Way Handshake が完了しない場合に問題がある可能性が高い箇所はどこか。

【正解】B) ネットワーク／FW

【解説】Handshake 未完了は TCP パケットが遮断されていることを示し、NW/FW が原因となる。

【実務ポイント】tcpdump や FW ログで SYN/SYN-ACK 確認。

Q41. HTTP 500 エラーが返る場合の原因として適切なものはどれか。

【正解】B) アプリケーション内部エラー

【解説】HTTP 500 はサーバ内部処理失敗を示し、通信自体は成立している。

【実務ポイント】アプリログ最優先。500 と 502 の違いを理解。

Q42. DNS 応答が遅い場合の切り分け方法として正しいものはどれか。

【正解】B) dig / nslookup による応答確認

【解説】dig 等によりどの DNS サーバで遅延しているかを切り分けられる。

【実務ポイント】キャッシュ／権威 DNS の違いを意識。

Q43. CDN を無効化した場合に想定される影響はどれか。

【正解】B) オリジンサーバ負荷増加

【解説】CDN がキャッシュしていたリクエストがすべてオリジンに集中する。

【実務ポイント】無効化は一時対応に留め、負荷増加を想定。

Q44. Web サービスの疎通確認に curl を使う利点はどれか。

【正解】B) HTTP レイヤ確認が可能

【解説】curl によりステータスコードやヘッダを直接確認できる。

【実務ポイント】curl -I でヘッダ確認。

Q45. DNS キャッシュが原因の障害で見られる典型的な挙動はどれか。

【正解】B) 特定環境のみ接続不可

【解説】キャッシュは環境ごとに保持されるため、環境差分が発生する。

【実務ポイント】TTL とキャッシュクリア有無を確認。

Q46. サーバ認証方式として推奨されるものはどれか。

【正解】B) 公開鍵認証

【解説】公開鍵認証はパスワード認証より漏洩リスクが低い。

【実務ポイント】鍵管理と失効管理を徹底。

Q47. IAM 運用で最も重要な原則はどれか。

【正解】B) 最小権限の原則

【解説】必要最小限の権限により影響範囲を限定できる。

【実務ポイント】定期棚卸しと一時権限付与。

Q48. Web 攻撃によりサーバ負荷が急増した場合の初動対応として適切なものはどれか。

【正解】B) トラフィック遮断・可視化

【解説】まず被害拡大防止と攻撃内容把握が優先される。

【実務ポイント】WAF/FW で遮断しログ保全。

Q49. WAF が有効に機能しているか確認する際に参照すべき情報はどれか。

【正解】B) WAF ログ

【解説】どのルールがマッチしたかを確認する必要がある。

【実務ポイント】Block/Count の区別と誤検知確認。

Q50. セキュリティインシデント発生時に最初に行うべき対応はどれか。

【正解】B) 影響範囲把握と証跡保全

【解説】即復旧すると証拠が失われる可能性があるため、保全が最優先。

【実務ポイント】証跡保全→エスカレーション→手順書対応。