インフラエンジニア 実務型スキルチェック（50問）回答集

Teams Forms インポート用問題の回答・詳細解説

作成日：2025-11-30
説明：このドキュメントは、Teams Forms 用に作成した50問の問題に対する正解と詳細解説をまとめたものです。カテゴリ別に整理し、各問題について解説・対処法のヒントを掲載しています。

目次

Linux（セクション）

1. ディスク空きがあるのに 'No space left on device' の原因は？

1	ディスクIO遅延
2	/home満杯
3	inode枯渇
4	swap不足

【正解】選択肢 3：inode枯渇
【解説】
正解の理由：「inode枯渇」が最も妥当です。 その他の選択肢の補足： 1. ディスクIO遅延 —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 2. /home満杯 —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 4. swap不足 —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。
対処方法：該当する原因（例：inode 枯渇であれば `df -i` で
inode 使用率を確認し、不要ファイルの削除やログローテーションを実施）を確認してください。

2. systemctl restartでサービスが即終了する原因は？

1	ExecStartのパス誤り
2	メモリ不足
3	SELinux
4	Disabled状態

【正解】選択肢 1：ExecStartのパス誤り
【解説】
正解の理由：「ExecStartのパス誤り」が最も妥当です。 その他の選択肢の補足： 2. メモリ不足 —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 3. SELinux —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 4. Disabled状態 —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。
対処方法：該当する原因（例：inode 枯渇であれば `df -i` で
inode 使用率を確認し、不要ファイルの削除やログローテーションを実施）を確認してください。

3. SSHログイン遅延の典型原因は？

1	NIC不良
2	CPU高負荷
3	PAM誤設定
4	DNS逆引き

【正解】選択肢 4：DNS逆引き
【解説】
正解の理由：「DNS逆引き」が最も妥当です。 その他の選択肢の補足： 1. NIC不良 —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 2. CPU高負荷 —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 3. PAM誤設定 —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。
対処方法：該当する原因（例：inode 枯渇であれば `df -i` で
inode 使用率を確認し、不要ファイルの削除やログローテーションを実施）を確認してください。

4. 予期せぬreboot時まず確認すべきログ？

1	secure
2	messages
3	cron
4	ssh

【正解】選択肢 2：messages
【解説】
正解の理由：「messages」が最も妥当です。 その他の選択肢の補足： 1. secure —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 3. cron —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 4. ssh —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。
対処方法：該当する原因（例：inode 枯渇であれば `df -i` で
inode 使用率を確認し、不要ファイルの削除やログローテーションを実施）を確認してください。

5. LoadAverage高いがCPU低い原因？

1	メモリ不足
2	CPUスロット
3	I/O待ち
4	カーネルパニック

【正解】選択肢 3：I/O待ち
【解説】
正解の理由：「I/O待ち」が最も妥当です。 その他の選択肢の補足： 1. メモリ不足 —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 2. CPUスロット —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 4. カーネルパニック —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。
対処方法：該当する原因（例：inode 枯渇であれば `df -i` で
inode 使用率を確認し、不要ファイルの削除やログローテーションを実施）を確認してください。

6. SELinux無効化のコマンドは？

1	setenforce 0
2	getenforce off
3	selinux disable
4	systemctl stop selinux

【正解】選択肢 1：setenforce 0
【解説】
正解の理由：「setenforce 0」が最も妥当です。 その他の選択肢の補足： 2. getenforce off —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 3. selinux disable —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 4. systemctl stop selinux —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。
対処方法：該当する原因（例：inode 枯渇であれば `df -i` で
inode 使用率を確認し、不要ファイルの削除やログローテーションを実施）を確認してください。

7. cron動作しない典型原因？

1	/tmp不足
2	crond停止
3	FW
4	時刻ずれ

【正解】選択肢 2：crond停止
【解説】
正解の理由：「crond停止」が最も妥当です。 その他の選択肢の補足： 1. /tmp不足 —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 3. FW —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 4. 時刻ずれ —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。
対処方法：該当する原因（例：inode 枯渇であれば `df -i` で
inode 使用率を確認し、不要ファイルの削除やログローテーションを実施）を確認してください。

8. sudoが突然失敗する原因？

1	PATH破損
2	sudoers誤設定
3	DNS
4	SELinux

【正解】選択肢 2：sudoers誤設定
【解説】
正解の理由：「sudoers誤設定」が最も妥当です。 その他の選択肢の補足： 1. PATH破損 —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 3. DNS —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 4. SELinux —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。
対処方法：該当する原因（例：inode 枯渇であれば `df -i` で
inode 使用率を確認し、不要ファイルの削除やログローテーションを実施）を確認してください。

9. yumが404返す原因？

1	proxy設定
2	repo無効
3	DNS逆引き
4	NTPずれ

【正解】選択肢 2：repo無効
【解説】
正解の理由：「repo無効」が最も妥当です。 その他の選択肢の補足： 1. proxy設定 —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 3. DNS逆引き —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 4. NTPずれ —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。
対処方法：該当する原因（例：inode 枯渇であれば `df -i` で
inode 使用率を確認し、不要ファイルの削除やログローテーションを実施）を確認してください。

10. 高負荷時の原因確認コマンド？

1	sar
2	vmstat

3	top
4	journalctl

【正解】選択肢 3：top
【解説】
正解の理由：「top」が最も妥当です。 その他の選択肢の補足： 1. sar —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 2. vmstat —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 4. journalctl —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。
対処方法：該当する原因（例：inode 枯渇であれば `df -i` で
inode 使用率を確認し、不要ファイルの削除やログローテーションを実施）を確認してください。

Windows（セクション）

11. RDP接続不可の典型原因？

1	FW 3389
2	CPU100%
3	Cドライブ満杯
4	Windows Update

【正解】選択肢 1：FW 3389
【解説】
正解の理由：「FW 3389」が最も妥当です。 その他の選択肢の補足： 2. CPU100% —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 3. Cドライブ満杯 —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 4. Windows Update —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。
対処方法：イベントログやサービス状態を確認し、必要に応じてサービスの依存関係や権限設定を見直してください
。

12. サービスがStartingのままの原因？

1	メモリ
2	GPO
3	依存サービス停止
4	権限不足

【正解】選択肢 4：権限不足
【解説】
正解の理由：「権限不足」が最も妥当です。 その他の選択肢の補足： 1. メモリ —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 2. GPO —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 3. 依存サービス停止 —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。
対処方法：イベントログやサービス状態を確認し、必要に応じてサービスの依存関係や権限設定を見直してください
。

13. DNSキャッシュクリア？

1	net cache reset
2	ipconfig /flushdns
3	flush /dns
4	nslookup /clear

【正解】選択肢 2：ipconfig /flushdns
【解説】
正解の理由：「ipconfig /flushdns」が最も妥当です。 その他の選択肢の補足： 1. net cache reset —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 3. flush /dns —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 4. nslookup /clear —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。
対処方法：イベントログやサービス状態を確認し、必要に応じてサービスの依存関係や権限設定を見直してください
。

14. 認証不安定の原因？

1	SMB暗号化
2	レジストリ
3	時刻ずれ
4	Defender

【正解】選択肢 3：時刻ずれ
【解説】
正解の理由：「時刻ずれ」が最も妥当です。 その他の選択肢の補足： 1. SMB暗号化 —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 2. レジストリ —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 4. Defender —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。
対処方法：イベントログやサービス状態を確認し、必要に応じてサービスの依存関係や権限設定を見直してください
。

15. IIS500の確認項目？

1	AppPool
2	IISバージョン
3	RDP人数
4	DNS

【正解】選択肢 1：AppPool
【解説】
正解の理由：「AppPool」が最も妥当です。 その他の選択肢の補足： 2. IISバージョン —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 3. RDP人数 —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 4. DNS —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。
対処方法：イベントログやサービス状態を確認し、必要に応じてサービスの依存関係や権限設定を見直してください
。

16. WindowsUpdateが長引く原因？

1	NIC
2	サービス依存

3	ストレージI/O
4	FW

【正解】選択肢 3：ストレージI/O
【解説】
正解の理由：「ストレージI/O」が最も妥当です。 その他の選択肢の補足： 1. NIC —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 2. サービス依存 —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 4. FW —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。
対処方法：イベントログやサービス状態を確認し、必要に応じてサービスの依存関係や権限設定を見直してください。

17. 高CPUのプロセス調査？

1	netstat
2	tasklist
3	dcdiag
4	ping

【正解】選択肢 2：tasklist
【解説】
正解の理由：「tasklist」が最も妥当です。 その他の選択肢の補足： 1. netstat —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 3. dcdiag —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 4. ping —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。
対処方法：イベントログやサービス状態を確認し、必要に応じてサービスの依存関係や権限設定を見直してください。

18. GPO反映確認？

1	gpupdate
2	dcdiag
3	whoami
4	net use

【正解】選択肢 1：gpupdate
【解説】
正解の理由：「gpupdate」が最も妥当です。 その他の選択肢の補足： 2. dcdiag —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 3. whoami —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 4. net use —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。
対処方法：イベントログやサービス状態を確認し、必要に応じてサービスの依存関係や権限設定を見直してください。

19. ドメイン参加失敗原因？

1	DNS未設定
2	FW
3	IIS
4	SMB

【正解】選択肢 1：DNS未設定
【解説】
正解の理由：「DNS未設定」が最も妥当です。 その他の選択肢の補足： 2. FW —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 3. IIS —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 4. SMB —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。
対処方法：イベントログやサービス状態を確認し、必要に応じてサービスの依存関係や権限設定を見直してください。

20. イベントログ収集の主要ID？

1	4625
2	7036
3	6005
4	1102

【正解】選択肢 1：4625
【解説】
正解の理由：「4625」が最も妥当です。 その他の選択肢の補足： 2. 7036 —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 3. 6005 —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 4. 1102 —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。
対処方法：イベントログやサービス状態を確認し、必要に応じてサービスの依存関係や権限設定を見直してください。

AWS（セクション）

21. ALBヘルスチェック失敗原因？

1	SG送信
2	IAMロール
3	VPCエンドポイント
4	ポート不一致

【正解】選択肢 4：ポート不一致
【解説】
正解の理由：「ポート不一致」が最も妥当です。 その他の選択肢の補足： 1. SG送信 —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 2. IAMロール —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 3. VPCエンドポイント —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 対処方法：CloudWatch や ALB/RDS
のログ、セキュリティグループ、ネットワーク設定を順に確認し、負荷や設定ミスを特定してください。

22. RDS接続増加原因？

1	I/O不足
2	接続プール枯渇
3	フェイルオーバ
4	パラメータ誤り

【正解】選択肢 2：接続プール枯渇
【解説】
正解の理由：「接続プール枯渇」が最も妥当です。 その他の選択肢の補足： 1. I/O不足 —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 3. フェイルオーバ —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 4. パラメータ誤り —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 対処方法：CloudWatch や ALB/RDS
のログ、セキュリティグループ、ネットワーク設定を順に確認し、負荷や設定ミスを特定してください。

23. 請求急上昇原因？

1	NATトラフィック
2	Backup
3	CW Logs
4	ALB追加

【正解】選択肢 1：NATトラフィック
【解説】
正解の理由：「NATトラフィック」が最も妥当です。 その他の選択肢の補足： 2. Backup —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 3. CW Logs —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 4. ALB追加 —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 対処方法：CloudWatch や ALB/RDS
のログ、セキュリティグループ、ネットワーク設定を順に確認し、負荷や設定ミスを特定してください。

24. S3 403理由？

1	暗号鍵
2	CORS
3	IAM不足
4	metadata

【正解】選択肢 3：IAM不足
【解説】
正解の理由：「IAM不足」が最も妥当です。 その他の選択肢の補足： 1. 暗号鍵 —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 2. CORS —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 4. metadata —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 対処方法：CloudWatch や ALB/RDS
のログ、セキュリティグループ、ネットワーク設定を順に確認し、負荷や設定ミスを特定してください。

25. Route53障害？

1	TTL長い
2	Aレコード誤記
3	ALB ARN
4	HC対象ダウン

【正解】選択肢 4：HC対象ダウン
【解説】
正解の理由：「HC対象ダウン」が最も妥当です。 その他の選択肢の補足： 1. TTL長い —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 2. Aレコード誤記 —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 3. ALB ARN —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 対処方法：CloudWatch や ALB/RDS
のログ、セキュリティグループ、ネットワーク設定を順に確認し、負荷や設定ミスを特定してください。

26. EC2が100%CPU時の確認は？

1	CloudTrail
2	top
3	SSM
4	ALBログ

【正解】選択肢 2：top
【解説】
正解の理由：「top」が最も妥当です。 その他の選択肢の補足： 1. CloudTrail —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 3. SSM —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 4. ALBログ —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 対処方法：CloudWatch や ALB/RDS
のログ、セキュリティグループ、ネットワーク設定を順に確認し、負荷や設定ミスを特定してください。

27. Lambdaタイムアウト原因？

1	DLQ
2	メモリ不足
3	VPC内部
4	ログ不足

【正解】選択肢 3：VPC内部
【解説】
正解の理由：「VPC内部」が最も妥当です。 その他の選択肢の補足： 1. DLQ —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 2. メモリ不足 —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 4. ログ不足 —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 対処方法：CloudWatch や ALB/RDS
のログ、セキュリティグループ、ネットワーク設定を順に確認し、負荷や設定ミスを特定してください。

28. CloudWatchLogs増加原因？

1	Retention短い
2	PutLog頻度

3	ログレベル高い
4	S3連携

【正解】選択肢 3：ログレベル高い
【解説】
正解の理由：「ログレベル高い」が最も妥当です。 その他の選択肢の補足： 1. Retention短い —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 2. PutLog頻度 —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 4. S3連携 —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 対処方法：CloudWatch や ALB/RDS
のログ、セキュリティグループ、ネットワーク設定を順に確認し、負荷や設定ミスを特定してください。

29. S3鍵問題のデバッグ？

1	KMSログ
2	S3ログ
3	KMS権限
4	CloudTrail

【正解】選択肢 4：CloudTrail
【解説】
正解の理由：「CloudTrail」が最も妥当です。 その他の選択肢の補足： 1. KMSログ —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 2. S3ログ —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 3. KMS権限 —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 対処方法：CloudWatch や ALB/RDS
のログ、セキュリティグループ、ネットワーク設定を順に確認し、負荷や設定ミスを特定してください。

30. EBS性能低下原因？

1	IOPS不足
2	EIP
3	SG
4	EC2タイプ

【正解】選択肢 1：IOPS不足
【解説】
正解の理由：「IOPS不足」が最も妥当です。 その他の選択肢の補足： 2. EIP —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 3. SG —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 4. EC2タイプ —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 対処方法：CloudWatch や ALB/RDS
のログ、セキュリティグループ、ネットワーク設定を順に確認し、負荷や設定ミスを特定してください。

31. EC2起動不可原因？

1	SG
2	IAMロール
3	AMI破損
4	AZ障害

【正解】選択肢 3：AMI破損
【解説】
正解の理由：「AMI破損」が最も妥当です。 その他の選択肢の補足： 1. SG —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 2. IAMロール —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 4. AZ障害 —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 対処方法：CloudWatch や ALB/RDS
のログ、セキュリティグループ、ネットワーク設定を順に確認し、負荷や設定ミスを特定してください。

32. ALB502原因？

1	EC2
2	ALB
3	DNS
4	Route53

【正解】選択肢 1：EC2
【解説】
正解の理由：「EC2」が最も妥当です。 その他の選択肢の補足： 2. ALB —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 3. DNS —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 4. Route53 —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 対処方法：CloudWatch や ALB/RDS
のログ、セキュリティグループ、ネットワーク設定を順に確認し、負荷や設定ミスを特定してください。

Network/Web（セクション）

33. ping通らずWeb通る原因？

1	MTU
2	L3故障
3	ICMP遮断
4	DNS逆引き

【正解】選択肢 3：ICMP遮断
【解説】
正解の理由：「ICMP遮断」が最も妥当です。 その他の選択肢の補足： 1. MTU —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 2. L3故障 —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 4. DNS逆引き —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 対処方法：ICMP/HTTP の違い、DNS 設定、SSL/TLS
ハンドシェイク、CDN の挙動などを個別に確認してください。

34. HTTPS遅い原因？

1	BGP
2	TLSハンドシェイク
3	CPU
4	MTU

【正解】選択肢 2：TLSハンドシェイク
【解説】
正解の理由：「TLSハンドシェイク」が最も妥当です。 その他の選択肢の補足： 1. BGP —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 3. CPU —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 4. MTU —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 対処方法：ICMP/HTTP の違い、DNS 設定、SSL/TLS
ハンドシェイク、CDN の挙動などを個別に確認してください。

35. DNS名NGでIP可？

1	DNS問題
2	FW
3	MTU
4	Switch負荷

【正解】選択肢 1：DNS問題
【解説】
正解の理由：「DNS問題」が最も妥当です。 その他の選択肢の補足： 2. FW —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 3. MTU —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 4. Switch負荷 —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 対処方法：ICMP/HTTP の違い、DNS 設定、SSL/TLS
ハンドシェイク、CDN の挙動などを個別に確認してください。

36. NAT越え不可？

1	TTL
2	VPN
3	BGP
4	PF誤り

【正解】選択肢 4：PF誤り
【解説】
正解の理由：「PF誤り」が最も妥当です。 その他の選択肢の補足： 1. TTL —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 2. VPN —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 3. BGP —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 対処方法：ICMP/HTTP の違い、DNS 設定、SSL/TLS
ハンドシェイク、CDN の挙動などを個別に確認してください。

37. Web遅い原因？

1	VLAN
2	ARP
3	CDNミス
4	DNS反射

【正解】選択肢 3：CDNミス
【解説】
正解の理由：「CDNミス」が最も妥当です。 その他の選択肢の補足： 1. VLAN —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 2. ARP —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 4. DNS反射 —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 対処方法：ICMP/HTTP の違い、DNS 設定、SSL/TLS
ハンドシェイク、CDN の挙動などを個別に確認してください。

38. TCP3WAY不成立原因？

1	SYN拒否
2	TTL
3	Aレコード
4	ARP

【正解】選択肢 1：SYN拒否
【解説】
正解の理由：「SYN拒否」が最も妥当です。 その他の選択肢の補足： 2. TTL —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 3. Aレコード —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 4. ARP —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 対処方法：ICMP/HTTP の違い、DNS 設定、SSL/TLS
ハンドシェイク、CDN の挙動などを個別に確認してください。

39. Web断続的切断原因？

1	ISP
2	DNS TTL
3	SSL更新
4	L4負荷

【正解】選択肢 4：L4負荷
【解説】
正解の理由：「L4負荷」が最も妥当です。 その他の選択肢の補足： 1. ISP —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 2. DNS TTL —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 3. SSL更新 —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 対処方法：ICMP/HTTP の違い、DNS 設定、SSL/TLS
ハンドシェイク、CDN の挙動などを個別に確認してください。

40. DNS遅延の確認？

1	dig +trace
2	ipconfig

3	curl
4	ping

【正解】選択肢 1：dig +trace
【解説】
正解の理由：「dig +trace」が最も妥当です。 その他の選択肢の補足： 2. ipconfig —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 3. curl —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 4. ping —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 対処方法：ICMP/HTTP の違い、DNS 設定、SSL/TLS
ハンドシェイク、CDN の挙動などを個別に確認してください。

41. HTTP500の主原因？

1	FW
2	アプリ
3	DNS
4	TLS

【正解】選択肢 2：アプリ
【解説】
正解の理由：「アプリ」が最も妥当です。 その他の選択肢の補足： 1. FW —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 3. DNS —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 4. TLS —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 対処方法：ICMP/HTTP の違い、DNS 設定、SSL/TLS
ハンドシェイク、CDN の挙動などを個別に確認してください。

42. CDN無効時の挙動？

1	直接Origin
2	エラー
3	TTL無限
4	HTTPS不可

【正解】選択肢 1：直接Origin
【解説】
正解の理由：「直接Origin」が最も妥当です。 その他の選択肢の補足： 2. エラー —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 3. TTL無限 —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 4. HTTPS不可 —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 対処方法：ICMP/HTTP の違い、DNS 設定、SSL/TLS
ハンドシェイク、CDN の挙動などを個別に確認してください。

Security（セクション）

43. 推奨される認証方式？

1	パスワード
2	鍵認証
3	rootログイン
4	秘密鍵共有

【正解】選択肢 2：鍵認証
【解説】
正解の理由：「鍵認証」が最も妥当です。 その他の選択肢の補足： 1. パスワード —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 3. rootログイン —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 4. 秘密鍵共有 —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。
対処方法：ログの保全と分析（CloudTrail, WAFログ,
Windowsイベント等）、侵害の兆候があれば隔離とフォレンジックを実施してください。

44. IAMベストプラクティス？

1	Admin付与
2	AccessKey保存
3	ロール運用
4	ポリシー大量

【正解】選択肢 3：ロール運用
【解説】
正解の理由：「ロール運用」が最も妥当です。 その他の選択肢の補足： 1. Admin付与 —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 2. AccessKey保存 —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 4. ポリシー大量 —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。
対処方法：ログの保全と分析（CloudTrail, WAFログ,
Windowsイベント等）、侵害の兆候があれば隔離とフォレンジックを実施してください。

45. Web攻撃で負荷上昇？

1	XSS
2	SQLi
3	DDoS
4	CSRF

【正解】選択肢 3：DDoS
【解説】
正解の理由：「DDoS」が最も妥当です。 その他の選択肢の補足： 1. XSS —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 2. SQLi —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 4. CSRF —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。
対処方法：ログの保全と分析（CloudTrail, WAFログ,
Windowsイベント等）、侵害の兆候があれば隔離とフォレンジックを実施してください。

46. rootkit疑い確認？

1	shadow
2	不審lsmod
3	known_hosts
4	ntp.conf

【正解】選択肢 2：不審lsmod
【解説】
正解の理由：「不審lsmod」が最も妥当です。 その他の選択肢の補足： 1. shadow —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 3. known_hosts —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 4. ntp.conf —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。
対処方法：ログの保全と分析（CloudTrail, WAFログ,
Windowsイベント等）、侵害の兆候があれば隔離とフォレンジックを実施してください。

47. WAF確認？

1	CWアラーム
2	OSログ
3	WAFログ
4	ALBログ

【正解】選択肢 3：WAFログ
【解説】
正解の理由：「WAFログ」が最も妥当です。 その他の選択肢の補足： 1. CWアラーム —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 2. OSログ —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 4. ALBログ —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。
対処方法：ログの保全と分析（CloudTrail, WAFログ,
Windowsイベント等）、侵害の兆候があれば隔離とフォレンジックを実施してください。

48. 不審ログインイベントID？

1	4625
2	7036
3	1100
4	1001

【正解】選択肢 1：4625
【解説】
正解の理由：「4625」が最も妥当です。 その他の選択肢の補足： 2. 7036 —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 3. 1100 —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 4. 1001 —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。
対処方法：ログの保全と分析（CloudTrail, WAFログ,
Windowsイベント等）、侵害の兆候があれば隔離とフォレンジックを実施してください。

49. MITM防止？

1	DNS
2	TLS
3	UDP
4	IGMP

【正解】選択肢 2：TLS
【解説】
正解の理由：「TLS」が最も妥当です。 その他の選択肢の補足： 1. DNS —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 3. UDP —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 4. IGMP —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。
対処方法：ログの保全と分析（CloudTrail, WAFログ,
Windowsイベント等）、侵害の兆候があれば隔離とフォレンジックを実施してください。

50. 侵害時確認？

1	CloudTrail
2	CPU
3	RDS
4	S3

【正解】選択肢 1：CloudTrail
【解説】
正解の理由：「CloudTrail」が最も妥当です。 その他の選択肢の補足： 2. CPU —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 3. RDS —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。 4. S3 —
選択肢として可能性はあるが、一般的にはこの状況では主要因ではないため不正解です。
対処方法：ログの保全と分析（CloudTrail, WAFログ,
Windowsイベント等）、侵害の兆候があれば隔離とフォレンジックを実施してください。

付録：採点ロジック

カテゴリ別の重み付けに基づき、各カテゴリの正答率を合算して総合スコアを算出します。
計算式：カテゴリスコア = (正答数 / カテゴリ問題数) × カテゴリ重み。総合スコア =
全カテゴリスコアの合計 × 100。

カテゴリ構成：Linux 10問（25%）、Windows 10問（20%）、AWS 12問（30%）、Network/Web
10問（15%）、Security 8問（10%）