問1

次の各ステートメントについて、ステートメントが正しい場合は [はい] を選択します。それ以外の場合は、「いいえ」を選択します

①すべての Azure ADライセンス エディションには、同じ機能が含まれています。

②Azure portal を使用して、Azure ADテナントを管理できます。

③Azure ADテナントをホストするには、Azure 仮想マシンをデプロイする必要があります。

【選択肢】

A. はい

B. いいえ

問1（解答）

①:いいえ

②:はい

③:いいえ

【解説】

①「いいえ」：Azure AD（現在のMicrosoft Entra ID）には、Free、Microsoft 365 アプリ、Premium P1、Premium P2の各エディションがあり、上位版ほど条件付きアクセスやID保護などの高度なセキュリティ機能が追加されます。

②「はい」： Azure portal内の「Microsoft Entra ID（旧Azure Active Directory）」メニューから、ユーザー、グループ、ドメインなどの一元管理が可能です。

③「いいえ」：Azure ADはクラウド型のID管理サービス（IDaaS）です。ユーザーが自分でサーバーや仮想マシンを用意して構築する必要はなく、クラウド上で即座に利用できます。

問2

文を正しく完成させる答えを選択してください。

[ ] では、Azure の展開を支援するツールやガイダンスなど、Microsoft の従業員、パートナー、顧客からのベスト プラクティスを提供します。

【選択肢】

A. Azure Blueprint

B. Azure policy

C. Azure 向けの Microsoft Cloud 導入フレームワーク

D．リソース ロック

問2（解答）

C. Azure 向けの Microsoft Cloud 導入フレームワーク

【解説】

◆正解の理由：

Microsoft Cloud 導入フレームワーク（CAF）は、組織がクラウド導入を成功させるための戦略、計画、準備、採用に関するベストプラクティスやツールをまとめた公式ドキュメントです。

不正解の選択肢の補足：

A. Azure Blueprint：環境のセットアップを標準化し、繰り返し利用可能なリソース構成を定義するツールです。

B. Azure Policy：リソースが組織のコンプライアンス基準に従っているかを評価・強制するサービスです。

D. リソース ロック：誤ったリソースの削除や変更を防ぐための機能です。

問3

文を正しく完成させる答えを選択してください。

[ ] は、捜査に使用される可能性のある電子情報を識別、保持、エクスポートするために使用されます。

【選択肢】

A. カスタマー ロックボックス

B. データ損失防止 (DLP)

C. 電子情報開示

D. リソース ロック

問3（解答）

C. 電子情報開示

【解説】

◆正解の理由：

電子情報開示（eDiscovery）は、法的調査や内部調査において、証拠として利用可能な電子情報（メール、文書、チャットなど）を検索、保持、エクスポートするための機能です。

不正解の選択肢の補足：

A. カスタマー ロックボックス：Microsoftのエンジニアがデータにアクセスする必要がある場合に、顧客がその承認操作を行うための仕組みです。

B. データ損失防止 (DLP)：機密情報の意図しない流出を検知・ブロックする機能です。

D. リソース ロック：リソースの構成を保護するための機能であり、情報の収集や調査用ではありません。

問4

文を正しく完成させる答えを選択してください。

[ ] を使用して Microsoft Intune を管理できます。

【選択肢】

A. Azure Active Directory admin center

B. Microsoft 365 compliance center

C. Microsoft 365 Defender portal.

D. Microsoft Endpoint Manager admin center.

問4（解答）

D. Microsoft Endpoint Manager admin center.

【解説】

◆正解の理由：

Microsoft Intuneは、モバイルデバイスやアプリケーションの管理を行うサービスです。現在はMicrosoft Intune 管理センターという名称に移行していますが、試験上はMicrosoft Endpoint Manager 管理センターとして、デバイス管理やポリシー作成の中核ポータルとして扱われます。

不正解の選択肢の補足説明：

A. Azure Active Directory admin center：ユーザーやグループなどのID管理、および認証設定を行うための場所です。

B. Microsoft 365 compliance center：現在はMicrosoft Purviewと呼ばれ、データの保持や機密情報の保護を管理します。

C. Microsoft 365 Defender portal：エンドポイントやメール、クラウドアプリなどの脅威の検出と対応を行うセキュリティ管理画面です。

問5

文を正しく完成させる答えを選択してください。

フェデレーションは、組織間で [ ] を確立するために使用されます。

【選択肢】

A. 多要素認証 (MFA)

B. 信頼関係

C. ユーザー アカウントの同期

D. VPN 接続

問5（解答）

B. 信頼関係

【解説】

◆正解の理由：

フェデレーションは、異なるドメインや組織の間でアイデンティティ（ID）情報を共有するために「信頼関係」を構築する仕組みです。これにより、ユーザーは自組織のIDを使って、信頼された外部のシステムやクラウドサービスにサインインできるようになります。

◆不正解の選択肢の説明：

A. 多要素認証 (MFA)：複数の方法で本人確認を行う認証の強化機能であり、組織間の関係を指すものではありません。

C. ユーザー アカウントの同期：オンプレミスのID情報をクラウドにコピーして作成する仕組みであり、認証の委任を行うフェデレーションとは別の手法です。

D. VPN 接続：ネットワークを安全につなぐための通信経路の技術であり、ID管理の仕組みではありません。

問6

次の各ステートメントについて、ステートメントが正しい場合は [はい] を選択します。それ以外の場合は、「いいえ」を選択します

①システム更新プログラムを適用すると、Microsoft Defender for Cloud での組織のセキュリティ スコアが向上します

②Microsoft Defender for Cloud のセキュリティ スコアは、複数の Azure サブスクリプションにわたるリソースを評価できます

③多要素認証 (MFA) を有効にすると、Microsoft Defender for Cloud での組織のセキュリティ スコアが向上します

【選択肢】

A. はい

B. いいえ

問6（解答）

①:はい

②:はい

③:はい

【解説】

①「はい」： システム更新プログラムの適用は、推奨事項として提示される最も基本的なセキュリティ対策の一つであり、これを実行して脆弱性を解消することでセキュリティスコアが向上します。

②「はい」： Defender for Cloudは、複数のAzureサブスクリプションだけでなく、マルチクラウド（AWSやGCP）環境に対しても、セキュリティの状態を統合的に評価してスコアを表示することが可能です。

③「はい」： 管理職や一般ユーザーへのMFAの有効化は、アカウント侵害のリスクを大幅に下げるため、推奨事項の中でも高い配点が設定されており、実施することでスコアが大きく改善されます。

問7

データ保護と規制基準に関連するリスクを軽減するのに役立つアクションを完了する際の組織の進捗状況を測定するスコアはどれですか?

【選択肢】

A. Microsoft セキュア スコア

B. 生産性スコア

C. Azure Security Center のセキュリティ スコア

D. コンプライアンススコア

問7（解答）

D. コンプライアンススコア

【解説】

◆正解の理由：

コンプライアンススコアは、Microsoft Purview コンプライアンス マネージャーで提供される指標です。データ保護規制や標準への準拠状況を数値化し、リスク軽減アクションの進捗を測定します。

不正解の選択肢の補足説明：

A. Microsoft セキュア スコア： ID、アプリ、デバイスなどの全体的な「セキュリティ態勢」を測定し、改善案を提示する指標です。

B. 生産性スコア： 組織が Microsoft 365 の機能をどの程度効果的に活用しているか（共同作業の頻度など）を測定する指標です。

C. Azure Security Center のセキュリティ スコア： 現在の Microsoft Defender for Cloud 内で、Azure リソースの「セキュリティ構成の不備」を測定する指標です。

問8

Azure Sentinel と別のセキュリティ ソースの間のリアルタイム統合を提供するには何を使用しますか?

【選択肢】

A. Azure AD Connect

B. Log Analytics ワークスペース

C. Azure Information Protection

D. コネクタ

問8（解答）

D. コネクタ

【解説】

◆正解の理由：

Microsoft Sentinel は、データコネクタを使用して、Microsoft サービスやサードパーティのセキュリティソリューションからログをリアルタイムで取り込み、統合します。

不正解の選択肢の補足説明：

A. Azure AD Connect： オンプレミスの Active Directory ユーザーをクラウドの Microsoft Entra ID（旧 Azure AD）に同期するツールです。

B. Log Analytics ワークスペース： 収集したログデータが物理的に保存され、クエリを実行する「器（データベース）」です。

C. Azure Information Protection： ドキュメントやメールにラベルを付けて「分類・保護（暗号化）」するための機能です。

問9

Microsoft クラウド サービスが国際

標準化機構 (ISO) などの規制標準にどのように準拠しているかに関する情報を提供する Microsoft ポータルはどれですか?

【選択肢】

A. Microsoft エンドポイント マネージャー管理センター

B. Azure のコスト管理と請求

C. Microsoft サービス トラスト ポータル

D. Azure Active Directory 管理センター

問9（解答）

C. Microsoft サービス トラスト ポータル

【解説】

◆正解の理由：

サービス トラスト ポータルは、Microsoft クラウドサービスが ISO や SOC などの法的・規制標準にどのように準拠しているか、監査レポートや詳細な技術資料を公開しているサイトです。

不正解の選択肢の補足説明：

A. Microsoft エンドポイント マネージャー： Intune などを含む、PC やモバイルデバイスを一括管理するためのポータルです。

B. Azure のコスト管理と請求： クラウドの利用料金の確認、予算の設定、請求書の管理を行う場所です。

D. Azure Active Directory 管理センター： ユーザー、グループ、アプリの権限など、アイデンティティ管理を行うポータルです。

問10

Azure 導入の責任共有モデルでは、Microsoft が単独で管理する責任は何ですか?

【選択肢】

A. モバイルデバイスの管理

B. Azure に保存されているユーザー データに対するアクセス許可

C. ユーザーアカウントの作成と管理

D. 物理ハードウェアの管理

問10（解答）

D. 物理ハードウェアの管理

【解説】

◆正解の理由：

責任共有モデルにおいて、データセンターの建物、物理サーバー、物理ネットワークなどの物理ハードウェアの管理は、いかなるクラウドサービス形態（IaaS/PaaS/SaaS）でも、常に Microsoft が単独で責任を負います。

不正解の選択肢の補足説明：

A. モバイルデバイスの管理： クラウドの種類にかかわらず、組織（顧客）が管理すべき責任です。

B. ユーザー データに対するアクセス許可： データの所有権とアクセス制御は、常に組織（顧客）の責任となります。

C. ユーザーアカウントの作成と管理： ID のライフサイクル管理は、常に組織（顧客）の責任となります。