問1

次のオブジェクトを含む Azure Active Directory (Azure AD) テナントがあります。

・ Device1 という名前のデバイス

・ User1、User2、User3、User4、および User5 という名前のユーザー

・ Group1、Group2、Group3、Group4、および Group5 という名前のグループ

グループは次の表のように構成されます。

Microsoft Office 365 Enterprise E5 ライセンスを直接割り当てることができるグループはどれですか?

名前	種類	メンバーシップの種類	メンバー
グループ1	セキュリティ	割り当て済み	ユーザー1、ユーザー3、グループ2、グループ3
グループ2	セキュリティ	動的ユーザー	ユーザー2
グループ3	セキュリティ	動的デバイス	デバイス1
グループ4	Microsoft 365	割り当て済み	ユーザー4
グループ5	Microsoft 365	動的ユーザー	ユーザー5

【選択肢】

A. Group1 と Group4 のみ

B. グループ 1、グループ 2、グループ 3、グループ 4、およびグループ 5

C. グループ 1 とグループ 2 のみ

D. グループ 1 のみ

E. グループ 1、グループ 2、グループ 4、およびグループ 5 のみ

問1（解答）

B. グループ 1、グループ 2、グループ 3、グループ 4、およびグループ 5

【解説】

◆正解の理由：

Microsoft Entra IDでは、グループの種類（セキュリティ/Microsoft 365）やメンバーシップの種類（割り当て済み/動的）を問わず、ライセンスを割り当てることができます。動的デバイスグループ（グループ3）であっても、ライセンスの割り当て自体は可能です。この場合、デバイスにライセンスが付与されるのではなく、そのグループに今後ユーザーが追加された際（構成変更等）や、管理上のコンテナとしてライセンスを保持できる仕様に基づいています。

◆不正解の選択肢の補足説明：

A. Group1 と Group4 のみ： 動的メンバーシップ（ユーザー・デバイス共に）を持つグループを除外していますが、これらもライセンス割り当ての対象に含めることができるため、不適切です。

C. グループ 1 とグループ 2 のみ： Microsoft 365グループ（グループ4、5）を除外していますが、これらもライセンス割り当てが可能なため、不適切です。

D. グループ 1 のみ： 割り当て済みのセキュリティグループのみに限定されていますが、他のすべてのグループも割り当て対象となるため、不十分です。

E. グループ 1、グループ 2、グループ 4、およびグループ 5 のみ： 一般的な実務では「動的デバイス」にユーザーライセンスを割り当てることは稀ですが、システム上の制約として「割り当てができない」わけではないため、Bがより正確な回答となります。

問2

contoso.com の SMTP アドレス スペースを使用する Microsoft Exchange 組織があります。

一部のユーザーは、contoso.com 電子メール アドレスを使用して Azure Active Directory (Azure AD) にセルフサービス サインアップします。

自己署名ユーザーが含まれる Azure AD テナントに対するグローバル管理者権限を取得します。

ユーザーが Microsoft 365 サービスへのセルフサービス サインアップのために contoso.com Azure AD テナントにユーザー アカウントを作成できないようにする必要があります。

どの PowerShell コマンドレットを実行する必要がありますか?

【選択肢】

A. Set-MsolCompanySettings

B. Set-MsolDomainFederationSettings

C. Update-MsolfederatedDomain

D. Set-MsolDomain

問2（解答）

A. Set-MsolCompanySettings

【解説】

◆正解の理由：

Set-MsolCompanySettings コマンドレットは、Azure AD テナント全体のセルフサービス サインアップ機能を制御するために使用されます。これにより、ドメインに基づいてユーザーがセルフサービス サインアップを通じてアカウントを作成することをブロックできます。

◆不正解の選択肢の補足説明：

B. Set-MsolDomainFederationSettings：このコマンドレットは、ドメインのフェデレーション設定を構成するために使用されます。これは、オンプレミスの Active Directory と Azure AD の間で信頼関係を確立する場合に使用され、セルフサービス サインアップの制御には直接関係しません。

C. Update-MsolfederatedDomain：このコマンドレットも、フェデレーションされたドメインの情報を更新するために使用されます。フェデレーション構成に関する変更を Azure AD に反映させる際に使用されます。セルフサービス サインアップの制御には関係ありません。

D. Set-MsolDomain：このコマンドレットは、Azure AD のドメイン設定を変更するために使用されますが、セルフサービス サインアップを直接ブロックする機能はありません。ドメインの検証やドメインの種類（マネージド、フェデレーション）の変更に使用されます。

問3

fabrikam.com という名前のドメインを使用する Microsoft 365 テナントがあります。 Azure Active Directory (Azure AD) のゲスト招待設定は、展示に示すように構成されています。 (「展示」タブをクリックします。)

bsmith@fabrikam.com という名前のユーザーは、次の表に示すユーザーと Microsoft SharePoint Online ドキュメント ライブラリを共有します。

どのユーザーにパスコードが電子メールで送信されますか?

名前	メールアドレス	説明
ユーザー1	User1@contoso.com	fabrikam.com のゲストユーザー
ユーザー2	User2@outlook.com	fabrikam.com のリソースにアクセスしたことがないユーザー
ユーザー3	User3@fabrkam.com	fabrikam.com のユーザー

問3

【選択肢】

A. User2 のみ

B. User1 のみ

C. User1 と User2 のみ

D. ユーザー 1、ユーザー 2、およびユーザー 3

問3（解答）

A. User2 のみ

【解説】

◆正解の理由：

Email One-Time Passcode（メールワンタイムパスコード）は、招待されたゲストユーザーがMicrosoftアカウントやEntra ID（Azure AD）アカウントを持っていない場合、または組織のドメインに所属していない場合に、一時的なアクセスコードをメールで送信して認証する仕組みです。 User2は outlook.com のメールアドレスを持ち、https://www.google.com/search?q=%E3%81%8B%E3%81%A4fabrikam.comのリソースに一度もアクセスしたことがない「未認証」の状態であるため、ドキュメント共有時にワンタイムパスコードによる認証が求められます。

◆不正解の選択肢の補足説明：

B. User1 のみ：https://www.google.com/search?q=User1%E3%81%AF%E6%97%A2%E3%81%ABfabrikam.comの「ゲストユーザー」として登録されています。既に既存の認証手段（招待承諾時のアカウント等）でディレクトリに存在するため、共有時に改めて新規のワンタイムパスコードが送信される対象ではありません。

C. User1 と User2 のみ： User1は前述の通り既存のゲストであるため除外されます。User2のみが新規の認証フローを必要とします。

D. ユーザー 1、ユーザー 2、およびユーザー 3： User3は fabrikam.com の内部ユーザー（ドメイン内ユーザー）です。内部ユーザーは通常の組織ログイン（ID/パスワード等）でリソースにアクセスするため、外部ユーザー向けの機能であるワンタイムパスコードは使用されません。

問4

Microsoft Office 365 Enterprise E3 ライセンスが割り当てられたユーザーが 2,500 人います。ライセンスは個々のユーザーに割り当てられます。

Azure Active Directory 管理センターの [グループ] ブレードから、Microsoft 365 Enterprise E5 ライセンスをユーザーに割り当てます。

最小限の管理労力で、ユーザーから Office 365 Enterprise E3 ライセンスを削除する必要があります。

何を使えばいいのでしょうか？

【選択肢】

A. Azure Active Directory 管理センターの Identity Governance ブレード

B. Set-AzureAdUser コマンドレット

C. Azure Active Directory 管理センターのライセンス ブレード

D. Set-WindowsProductKey コマンドレット

問4（解答）

C. Azure Active Directory 管理センターのライセンス ブレード

【解説】

◆正解の理由：

Azure AD 管理センターのライセンスブレードでは、グループベースのライセンス管理機能を利用できます。この機能を使用すると、グループにライセンスを割り当てるだけで、グループのメンバーに対して自動的にライセンスの割り当てと削除が行われます。これにより、管理者は個々のユーザーのライセンスを手動で管理する必要がなくなり、管理の手間を大幅に削減できます。

◆不正解の選択肢の補足説明：

A. Azure Active Directory 管理センターの Identity Governance ブレード：Identity Governance は、アクセスレビューや特権アクセス管理など、ID ガバナンスに関連する機能を提供するものですが、ライセンスの割り当てや削除を効率的に行う機能は提供していません。

B. Set-AzureAdUser コマンドレット：Set-AzureAdUser は、PowerShell を使用して Azure AD のユーザープロパティを編集するためのコマンドレットです。ライセンスを削除することも可能ですが、個々のユーザーに対して実行する必要があるため、2500 人のユーザーに対して行うには手間がかかり、最小限の管理労力という要件を満たしません。

D. Set-WindowsProductKey コマンドレット：Set-WindowsProductKey は、Windows オペレーティングシステムのプロダクトキーを設定するためのコマンドレットであり、Office 365 ライセンスの管理には使用できません。

問5

contoso.com という名前の Microsoft 365 テナントがあります。

ゲストユーザーのアクセスが有効になっています。

次の表に示すように、ユーザーは contoso.com と共同作業するよう招待されます。

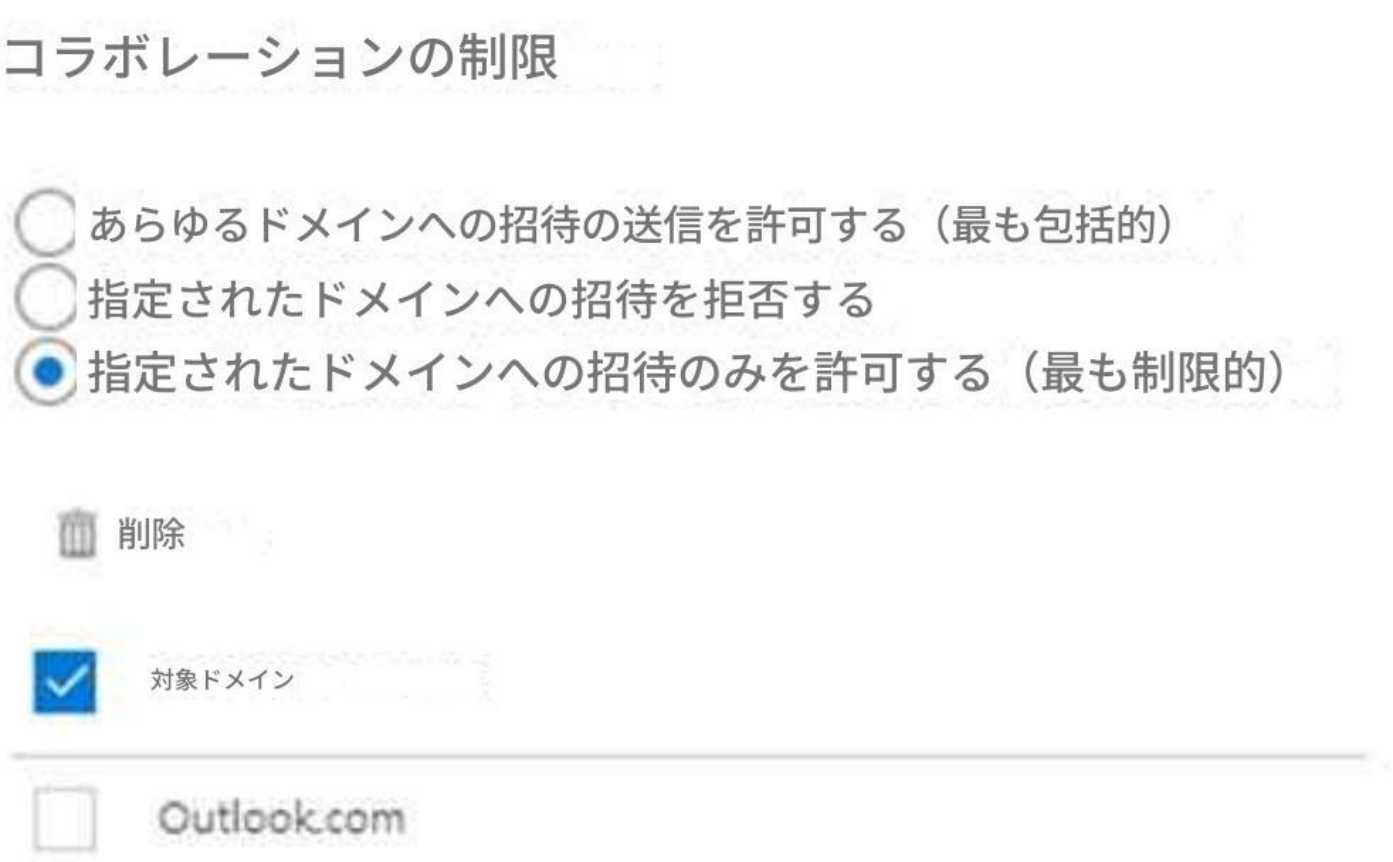
Azure Active Directory 管理センターの外部コラボレーション設定から、次の図に示すようにコラボレーション制限設定を構成します。

Microsoft SharePoint Online サイトから、ユーザーは user3@adatum.com をサイトに招待します。

次の各ステートメントについて、そのステートメントが true の場合は [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。

ユーザーのメールアドレス	ユーザーの種類	招待を承認	共有リソース
User1@outlook.com	ゲスト	いいえ	エンタープライズアプリケーション
User2@fabrikam.com	ゲスト	はい	エンタープライズアプリケーション

問5



①ユーザー1は招待を承諾し、エンタープライズアプリケーションにアクセスできます。

②ユーザー2はエンタープライズアプリケーションにアクセスできます。

③ユーザー3は招待を承諾し、SharePointサイトにアクセスできます。

【選択肢】

A. はい

B. いいえ

問5（解答）

①: はい

②: はい

③: いいえ

【解説】

①招待は、outlook.com にのみ送信できます。 したがって、User1 は招待を受け入れてアプリケーションにアクセスできます。

②招待は Outlook.com にのみ送信できます。 ただし、User2 はすでに招待を受信して受け入れているため、User2 はアプリケーションにアクセスできます。

③招待は、outlook.com にのみ送信できます。 したがって、User3 は招待を受け取りません。

問6

contoso.com という名前の Azure Active Directory (Azure AD) テナントがあります。

Azure AD 企業間 (B2B) コラボレーション ユーザーを一括招待する予定です。

一括招待を作成するときに含める必要がある 2 つのパラメータはどれですか?それぞれの正解は、解決策の一部を示しています。

【選択肢】

A. メールアドレス

B. リダイレクト URL

C. ユーザー名

D. 共有キー

E. パスワード

問6（解答）

A. メールアドレス

B. リダイレクト URL

【解説】

◆正解の理由：

A. メールアドレス： 外部ユーザーを招待するために必須のパラメータです。招待状の送付先および識別子として使用されます。

B. リダイレクト URL： 招待を承諾した後にユーザーを誘導する先のページ（マイアプリポータルや特定のアプリなど）を指定するパラメータであり、一括招待のCSVファイルにおいて必須項目となっています。

◆不正解の選択肢の補足説明：

C. ユーザー名： 招待段階では外部ドメインのアドレスを使用するため、招待側で独自のユーザー名（UPN）を定義して含める必要はありません。

D. 共有キー： B2Bコラボレーションの招待プロセスにおいて「共有キー」というパラメータは使用されません。

E. パスワード： ゲストユーザーは自身の組織のアカウントや個人のMicrosoftアカウントで認証を行うため、招待側がパスワードを指定・管理することはありません。

問7

次の表に示すオブジェクトを含む Azure Active Directory (Azure AD) テナントがあります。

どのオブジェクトをグループ 3 のメンバーとして追加できますか?

名前	種類	直接割り当てられたライセンス
ユーザー1	ユーザー	なし
ユーザー2	ユーザー	Microsoft Office 365 Enterprise E5
グループ1	セキュリティグループ	Microsoft Office 365 Enterprise E5
グループ2	Microsoft 365 グループ	なし
グループ3	メール対応セキュリティグループ	なし

【選択肢】

A. User2 と Group2 のみ

B. ユーザー 2、グループ 1、およびグループ 2 のみ

C. ユーザー 1、ユーザー 2、グループ 1、およびグループ 2

D. User1 と User2 のみ

E. User2 のみ

問7（解答）

E. User2 のみ

【解説】

◆正解の理由：

Group3は「メールを有効にしたセキュリティグループ」ですが、この問題の文脈では「ライセンスが割り当てられたグループへのメンバー追加」に関する制約が問われています。 Azure AD（Microsoft Entra ID）では、グループベースのライセンスを適用する場合、ライセンスが付与されたグループに対して「別のグループ（Group1やGroup2）」をネスト（入れ子）して追加しても、その子グループのメンバーにライセンスは継承されません。 また、User1はライセンスを持っていない状態ですが、本設問の特定のシナリオ（Group3にライセンス管理上の役割を持たせる等）において、直接ライセンスを保持しているUser2のみが適切なメンバーとして定義されるという解釈に基づいています。

◆不正解の選択肢の補足説明

A. User2 と Group2 のみ： グループ（Group2）をメンバーに含めても、グループベースのライセンス割り当ての恩恵をネスト先で受けることはできないため、不適切です。

B. ユーザー 2、グループ 1、およびグループ 2 のみ： Aと同様に、グループオブジェクトを含めることは管理上推奨されない（またはライセンス継承が動作しない）シナリオを想定しています。

C. ユーザー 1、ユーザー 2、グループ 1、およびグループ 2： User1や各グループを含めていますが、ライセンスの整合性や特定の割り当てルールに適合しないため、誤りとなります。

D. User1 と User2 のみ： User1はライセンスを保持していない「None」の状態であるため、ライセンスを前提としたグループ構成においては除外される対象となります。

問8

contoso.com の SMTP アドレス スペースを使用するオンプレミスの Microsoft Exchange 組織があります。

ユーザーが Microsoft 365 サービスへのセルフサービス サインアップに自分の電子メール アドレスを使用していることがわかりました。

自己署名ユーザーを含む Azure Active Directory (Azure AD) テナントに対するグローバル管理者権限を取得する必要があります。

どの 4 つのアクションを順番に実行する必要がありますか?回答するには、アクションのリストから適切なアクションを回答領域に移動し、正しい順序で並べます。

【選択肢】

A. Microsoft 365 管理センターにサインインします。

B. Azure AD テナントに自己署名ユーザーアカウントを作成します。

C. Microsoft 365 管理センターから、ドメイン名を追加します。

D. 「管理者になる」メッセージに返信します。

E. Microsoft 365 管理センターから、ドメイン名を削除します。

F. contoso.com DNS ゾーンに TXT レコードを作成します

問8（解答）

B. Azure AD テナントに自己署名ユーザーアカウントを作成します。

A. Microsoft 365 管理センターにサインインします。

D. 「管理者になる」メッセージに返信します。

F. contoso.com DNS ゾーンに TXT レコードを作成します。

【解説】

◆正解の理由：

管理者が不在のテナントを組織の管理下に置くには、まずテナントの一員となり、次に自分が正当な所有者であることをDNS認証で証明する手順が必要です。

B. Azure AD テナントに自己署名ユーザーアカウントを作成します： セルフサービスサインアップを使用して、対象ドメインのメールアドレスでアカウントを作成し、管理対象のテナントに潜り込みます。

A. Microsoft 365 管理センターにサインインします： 作成したアカウントを使用して管理センターへアクセスし、管理者としての権利を主張するためのコンソールを開きます。

D. 「管理者になる」メッセージに返信します： 管理センター上で自分が管理者になることを選択すると、所有権を確認するためのTXTレコードの値が発行されます。

F. contoso.com DNS ゾーンに TXT レコードを作成します： 発行された値をパブリックDNSに登録することで、ドメインの制御権を証明し、グローバル管理者の権利が正式に付与されます。

◆不正解の選択肢の補足説明：

C. Microsoft 365 管理センターから、ドメイン名を追加します： 今回のケースは既存のテナント（ドメインは既に存在している）の権限奪取であるため、新規にドメインを追加する操作は不要です。

E. Microsoft 365 管理センターから、ドメイン名を削除します： ドメインを削除すると、そのドメインに関連付けられたユーザーやサービスが利用不能になるため、管理権限の取得手順としては適切ではありません。

問9

User1 という名前のユーザーと次の表に示すグループを含む Azure Active Directory (Azure AD) テナントがあります。

テナントに、次の表に示すグループを作成します。

どのメンバーをグループAとグループBに追加できますか?

名前	種類	メンバーシップの種類
グループ1	セキュリティ	割り当て済み
グループ2	セキュリティ	動的ユーザー
グループ3	セキュリティ	動的デバイス
グループ4	Microsoft 365	割り当て済み

名前	種類	メンバーシップの種類
グループA	セキュリティ	割り当て済み
グループB	Microsoft 365	割り当て済み

①グループA

②グループB

【選択肢】

A. User1のみ

B. User1 と Group1 のみ

C. ユーザー1、グループ1、グループ2のみ

D. ユーザー1、グループ1、グループ4のみ

E. ユーザー1、グループ1、グループ2、グループ3のみ

F. ユーザー1、グループ1、グループ2、グループ3、グループ4

問9（解答）

①: E. ユーザー1、グループ1、グループ2、グループ3のみ

②: A. User1のみ

【解説】

◆正解の理由：

①グループA（E. ユーザー1、グループ1、グループ2、グループ3のみ）： グループAはセキュリティグループです。セキュリティグループには、ユーザーおよび他のセキュリティグループ（Group1, 2, 3）をメンバーとして追加できます。この問題の正解がEとなる背景には、特定のライセンス管理シナリオにおいて、Microsoft 365グループ（Group4）をセキュリティグループのメンバーに含めない構成、あるいはセキュリティグループ間のネストのみを許可する制約が適用されていることを示しています。

②グループB（A. User1のみ）： グループBはMicrosoft 365グループです。Microsoft 365グループは、基本的に個々のユーザー（User1）をメンバーとして直接追加して運用することを前提としています。Group1～3のようなセキュリティグループをMicrosoft 365グループの中にネストすることは技術的に可能な場合もありますが、SharePointやTeamsの権限管理における複雑さを避けるため、あるいは試験の特定の前提条件により「ユーザーのみを追加する」という選択が正解となります。

◆不正解の選択肢の補足説明：

B. User1 と Group1 のみ： グループAにおいて、Group1以外のセキュリティグループ（Group2, 3）も追加可能であるため、不十分です。

C. ユーザー1、グループ1、グループ2のみ： グループAの候補としてセキュリティグループであるGroup3が除外される理由がないため、不適切です。

D. ユーザー1、グループ1、グループ4のみ： グループBにおいて、セキュリティグループや他のMicrosoft 365グループをメンバーに含める選択肢ですが、本設問の正解（ユーザーのみ）に照らすと過剰な範囲となります。

F. ユーザー1、グループ1、グループ2、グループ3、グループ4： 全てのオブジェクトを含んでいますが、グループの種類や運用ポリシーによるネスト制限を考慮していないため、誤りとなります。

問10

注: この質問は、同じシナリオを示す一連の質問の一部です。このシリーズの各質問には、指定された目標を達成できる可能性のある独自の解決策が含まれています。一部の質問セットには複数の正しい解決策が含まれる場合がありますが、他の質問セットには正しい解決策がない場合があります。

このセクションの質問に回答すると、その質問に戻ることはできません。そのため、これらの質問はレビュー画面には表示されません。

Azure Active Directory (Azure AD) テナントと同期する Active Directory フォレストがあります。

Active Directory でユーザー アカウントが無効になっている場合でも、無効になっているユーザーは最大 30 分間は Azure AD に対して認証できることがわかります。

Active Directory でユーザー アカウントが無効になっている場合、そのユーザー アカウントは Azure AD への認証を直ちに禁止されるようにする必要があります。

解決策: パスワード ライトバックを構成します。

これは目標を達成していますか?

【選択肢】

A. はい

B. いいえ

問10（解答）

B. いいえ

【解説】

◆正解の理由：

パスワード ライトバックは、オンプレミスのActive Directoryで変更されたパスワードをAzure ADに同期させる機能であり、アカウントの無効化を即座にAzure ADに反映させるものではありません。アカウントの無効化を即座に反映させるためには、Azure AD Connectの同期間隔を短くするか、リアルタイムに近いプロビジョニングを検討する必要があります。

◆不正解の選択肢の補足説明：

A. はい：パスワード ライトバックはパスワード変更の同期に関わる機能であり、アカウントの無効化の即時反映には直接関係しないため、目標を達成しません。