mstep

SC-900

Microsoft Security, Compliance, and Identity Fundamentals

試験対策

エディフィストラーニング株式会社

本セミナーの目標

- SC-900試験に合格すること。

SC-900で評価されるスキル -1

- セキュリティ、コンプライアンスおよびIDの概念を説明する(5-10%)
  - セキュリティの方法論を説明する
  - セキュリティ概念を説明する
  - Microsoftのセキュリティとコンプライアンスの原則を説明する
- Microsoft Identity and Access Management Solutionsの機能を説明する(25-30%)
  - IDの原則/概念を定義する
  - Azure ADの基本的なIDサービスとIDタイプについて説明する
  - Azure ADの認証機能について説明する
  - Azure ADのアクセス管理機能について説明する
  - Azure ADのID保護とガバナンス機能について説明する

SC-900で評価されるスキル -2

- Microsoftセキュリティソリューションの機能を説明する(30-35%)
  - Azureの基本的なセキュリティ機能を説明する
  - Azureのセキュリティ管理機能について説明する
  - Azure Sentinelのセキュリティ機能について説明する
  - Microsoft 365 Defender(Microsoft Threat Protection)による脅威保護について説明する
  - Microsoft 365のセキュリティ管理機能について説明する
  - Microsoft Intuneを使用したエンドポイントセキュリティについて説明する

SC-900で評価されるスキル -3

- Microsoftコンプライアンスソリューションの機能を説明する(25-30%)
  - Microsoftのコンプライアンス管理機能を説明する
  - Microsoft 365の情報保護およびガバナンス機能について説明する
  - Microsoft 365の内部リスク機能について説明する
  - Microsoft 365の電子情報開示機能について説明する
  - Microsoft 365の監査機能について説明する
  - Azureのリソースガバナンス機能について説明する

試験の概要

- 問題数　46(予想)
- 時間　60分
- シナリオ問題　なし
- 合格ライン　700点以上/1000点
- 日本語試験　あり
- 複数選択問題　部分的な加点あり

2021年6月28日現在

本テキストの使い方

機能の概要をつかむ

↓

問題ベースで理解する

↓

理解を深める

特に、Exam Pointと
Pointは要チェックです！

Agenda

1. 試験の概要
2. セキュリティ、コンプライアンスおよびIDの概念を説明する
3. Microsoft Identity and Access Management Solutionsの機能を説明する
4. Microsoft Azureのセキュリティとコンプライアンスソリューション
5. Microsoft 365のセキュリティとコンプライアンスソリューション

本コースのトレーニングで使用するテキストは、コンテンツ作成時点の情報であり、予告なしに変更される可能性があります。

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

セキュリティ、コンプライアンスおよびIDの概念を説明する

2

SC-900 Microsoft Security,
Compliance, and Identity Fundamentals

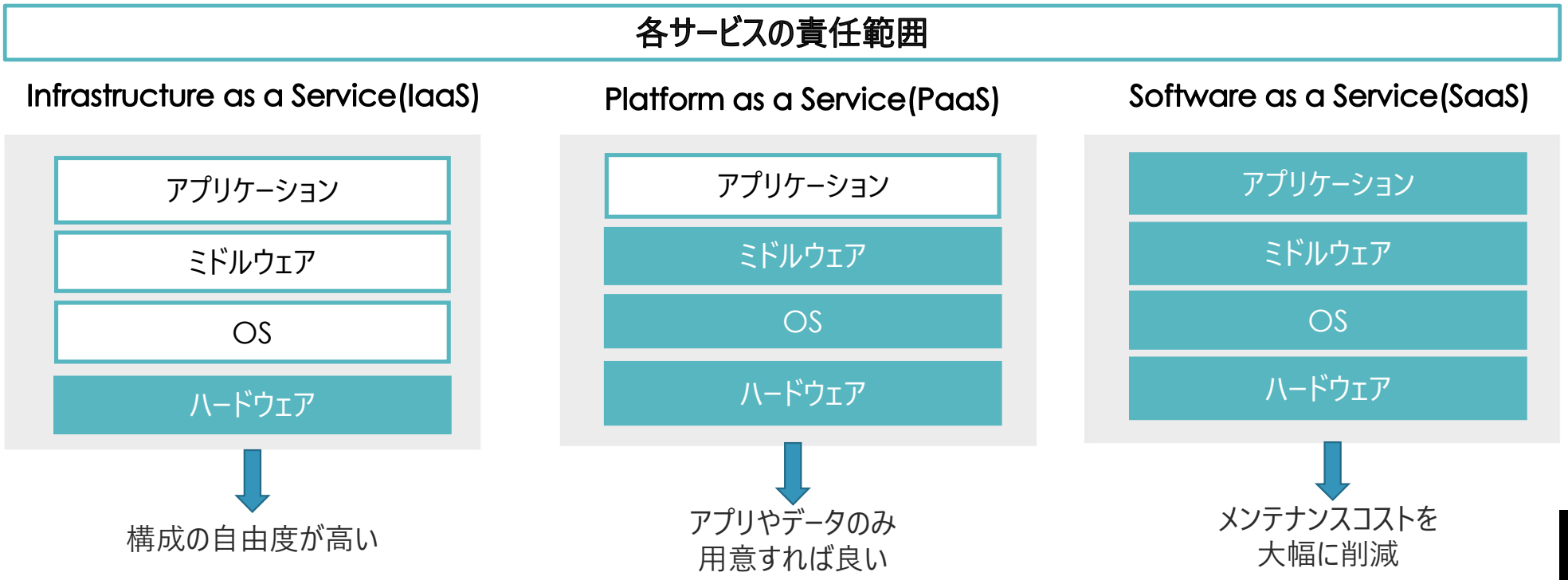
2.1
セキュリティの方法論を説明する

クラウドにおける共同責任モデル

- オンプレミス環境の場合は、ハードウェア、ソフトウェア、各種設定など、すべての責任は企業が負います。
- クラウドサービスの場合は、クラウドサービスを提供する事業者と顧客の両方に責任が生じます。
  このことを「共同責任モデル」と呼びます。

クラウドコンピューティングのサービスモデル

- IaaS(サービスとしてのインフラストラクチャ)　例：Azure仮想マシン
- PaaS(サービスとしてのプラットフォーム)　例：Azure SQL Database
- SaaS(サービスとしてのソフトウェア)　例：Microsoft 365



サービスごとの具体的な責任範囲 -1

- IaaS

  - クラウド事業者は建物、サーバー、ネットワークハードウェア、ハイパーバイザーなどの要素を管理する必要があります。
  - 顧客はOS、ネットワーク構成、アプリケーション、ID、クライアント、データの保護に対して管理する責任があるか、クラウド事業者と責任を共有しています。
- PaaS
  - クラウド事業者は、IaaSで管理する要素に加え、OSを管理する責任があります。
  - 顧客はネットワーク構成、アプリケーション、ID、クライアント、データの保護に対して管理する責任があるか、クラウド事業者と責任を共有しています。

サービスごとの具体的な責任範囲 -2

- SaaS
  - クラウド事業者は、IaaS、PaaSの責任範囲に加え、アプリケーションを提供します。
  - 顧客は、データが正しく分類されていることを確認する必要があり、ユーザーとエンドポイントデバイスを管理する責任を共有します。

顧客が必ず責任を負うもの

- 選択したサービスやデプロイ方法に関係なく、次のものについては必ず顧客側が責任を負います。
  - データ
  - エンドポイント
  - アカウント
  - アクセス管理

データは顧客側が責任を負います。

Exam Point

あなたの会社では、クラウドサービスの導入を比較検討しています。

次の各ステートメントについて、ステートメントが真の場合は、「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。

①SaaSにおいては、アプリの更新プログラムの適用の責任は顧客が持ちます。

②IaaSにおいては、物理ネットワークの管理責任はクラウドサービス事業者が持ちます。

③Azureのすべてのリソース展開において、セキュリティおよびデータについては顧客が責任を持ちます。

解答：以下を参照

①SaaSにおいては、アプリの更新プログラムの適用の責任は顧客が持ちます。

いいえ　SaaSにおいて、アプリはクラウド事業者が責任を持ちます。

②IaaSにおいては、物理ネットワークの管理責任はクラウドサービス事業者が持ちます。

はい　IaaSにおいて、物理ネットワークはクラウド事業者の責任範囲です。

③Azureのすべてのリソース展開において、セキュリティおよびデータについては顧客が責任を持ちます。

いいえ　データについては、顧客が責任を持ちますが、セキュリティは選択するクラウドサービスの形態によって、クラウド事業者が責任を持つ場合があります。

セキュリティ対策のキーワード

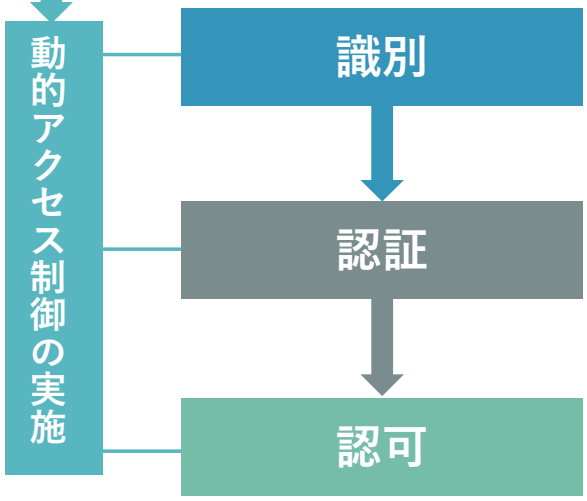
Zero Trust Security

コレです。

ゼロトラストセキュリティとは

ゼロトラスト

すべてのアクセスを、信頼されていないネットワークから発信されたものとして扱うことです。



ユーザーを識別

ユーザーとデバイスをID管理基盤に登録し、組織の資産を識別します。

身元を検証

アクセス元の身元の正当性を厳密に検証し認証します。

属性に応じてアクセス範囲を決定

セキュリティリスクを評価し、信頼性に基づきアクセスを制御します。

- ✓ ユーザー：匿名化やありえない移動によるサインイン行為など
- ✓ デバイス：デバイスが攻撃を受けている、ポリシーに準拠していないなど

マイクロソフトのゼロトラストの原則

マイクロソフトのゼロトラスト原則は、次の3つです。

- ✓ **明示的に確認する**
  常に認証と承認を、入手可能なすべてのデータポイントに基づいて行います。
  これに含まれるものとしては、ユーザーID、場所、デバイスの正常性、サービスまたはアプリ、データ分類、異常などがあります。

- ✓ **最小特権アクセスを使用する**
  ユーザーアクセスを限定するために、ジャストインタイムの必要十分なアクセス権 (JIT/JEA)、リスクベースの適応型ポリシー、データ保護を使用して、データと生産性の両方を安全に守ります。

- ✓ **侵害があるものと考える**
  被害の範囲を最小限に抑えるため、アクセスをセグメント化します。
  エンドツーエンドの暗号化を確認し、アナリティクスを使用して可視化し、脅威検出を推進し、防御を強化します。

ゼロトラストの3原則を覚えておきましょう。

Exam Point

次の各ステートメントについて、ステートメントが真の場合は、「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。

①明示的に検証することは、ゼロトラストの指針の1つです。

②侵害を想定することは、ゼロトラストの指針の1つです。

③ゼロトラストセキュリティモデルは、ファイアウォールが外部の脅威から内部ネットワークを保護することを前提としています。

解答：以下を参照

①明示的に検証することは、ゼロトラストの指針の1つです。

はい　明示的に検証することは、ゼロトラストの原則の1つです。

②侵害を想定することは、ゼロトラストの指針の1つです。

はい　侵害があるものと考えることは、ゼロトラストの原則の1つです。

③ゼロトラストセキュリティモデルは、ファイアウォールが外部の脅威から内部ネットワークを保護することを前提としています。

いいえ　ゼロトラストセキュリティモデルは、すべてのアクセスを信頼されていないネットワークから発信されたものとして扱うことです。

SC-900 Microsoft Security,
Compliance, and Identity Fundamentals

2.2
セキュリティ概念を説明する
Microsoftのセキュリティと
コンプライアンスの原則を説明する

Microsoft Cloudにおける暗号化

顧客データは、保存時、転送時とも暗号化され保護されています。

転送中のデータ

ネットワーク

- TLS
- IPSec

コンテンツ

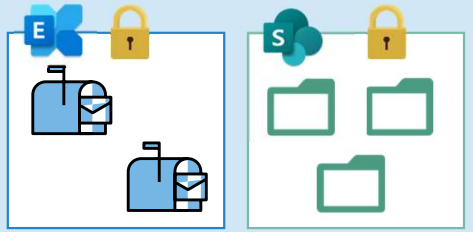
- Microsoft Information Protection
- Office 365 Message Encryption
- Office 365 Advanced Message Encryption

保存されているデータ

ハードウェア (ディスクレベル)

- BitLocker

アプリ (ファイルレベル)



Exchange Online メールボックス

SharePoint・OneDriveのファイル

- サービス暗号化
- カスタマーキー

Point

Azure仮想マシンのOSとデータディスクは、BitLocker による暗号化を行うことができます(Azure Disk Encryption)。

Exam Point

Microsoftのクラウドサービスにおいて保存時の暗号化に該当するものはどれですか。

	選択肢
A	暗号化された電子メール
B	暗号化された仮想マシンファイル
C	HTTPSを使用したWebアクセス
D	VPNを使用した通信の暗号化

解答：B

Azureの仮想マシンは、BitLockerドライブを使用して暗号化することができます。

SC-900 Microsoft Security,
Compliance, and Identity Fundamentals

2.3 Microsoftのセキュリティとコンプライアンスの原則を説明する

Service Trust Portal

Service Trust Portalには、Microsoftのセキュリティ、プライバシー、コンプライアンスに関するさまざまなコンテンツ、ツール、その他のリソースが提供されています。

Point

Microsoftのクラウドサービスに関して、公開されている独立した監査レポートを確認できます。ISO、SOC、NIST、FedRAMP、GDPRなどのデータ保護基準および規制要件への準拠について情報が提供されています。

Microsoftクラウドサービスを使用するときに、地域の基準や規制に、より簡単に準拠できるようになる、地域のコンプライアンス資料のライブラリが提供されます。オーストラリア、ドイツ、ヨーロッパ、UKの資料が確認できます。

さまざまなドキュメントやリソースを確認できます。
ホワイトペーパーや、よく寄せられる質問、コンプライアンスのガイドなどが提供されています。たとえば、Microsoftクラウドサービスがデータを保護する方法、および組織のクラウドデータのセキュリティとコンプライアンスを管理する方法に関する情報などを確認できます。

Exam Point

Microsoftのクラウドサービスが国際標準化機構(ISO)などの規制基準にどのように準拠しているかについての情報を提供するMicrosoftポータルはどれですか。

	選択肢
A	Microsoft Endpoint Manager admin center
B	Azureコスト管理+請求
C	Microsoft 365管理センター
D	Service Trust Portal

解答：D

Service Trust Portalは、規制基準にどのように準拠しているかについての情報を提供します。

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Microsoft Identity and Access Management Solutionsの機能を説明する

3

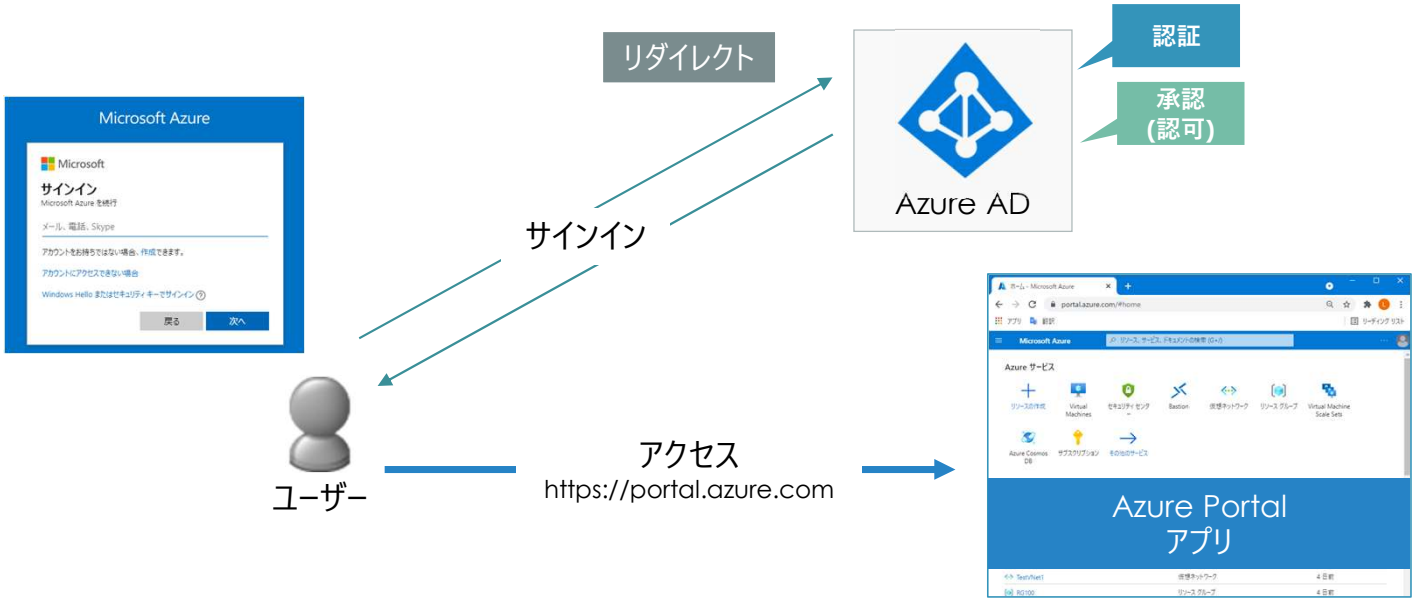
SC-900 Microsoft Security,
Compliance, and Identity Fundamentals

3.1
IDの原則/概念を定義する

Azureポータルにアクセスするときのフロー

Azureポータルにアクセスすると、認証→承認(認可)の流れで処理されます。

- 認証とは、ユーザー名やパスワードなどを使用して本人確認を行うことです。
- 承認(認可)とは、認証されたユーザーにどのような操作を許可するかを判別することです。



Point

Azureポータルにアクセスすると、最初に「認証」の処理が行われ、
次に「承認」の処理が行われます。

Exam Point

ユーザーがAzure Portalにサインインした時に、最初に行われるのはどれですか。

選択肢	
A	認証される
B	承認される
C	解決される
D	アクセス許可の付与

解答：A

- ユーザーがサインインした時に最初に行われるのは、認証です。

Exam Point

サインインしたユーザーのリソースへのアクセスを検証するプロセスのことを何と言いますか。

選択肢	
A	認証
B	承認
C	シングルサインオン
D	フェデレーション

解答：B

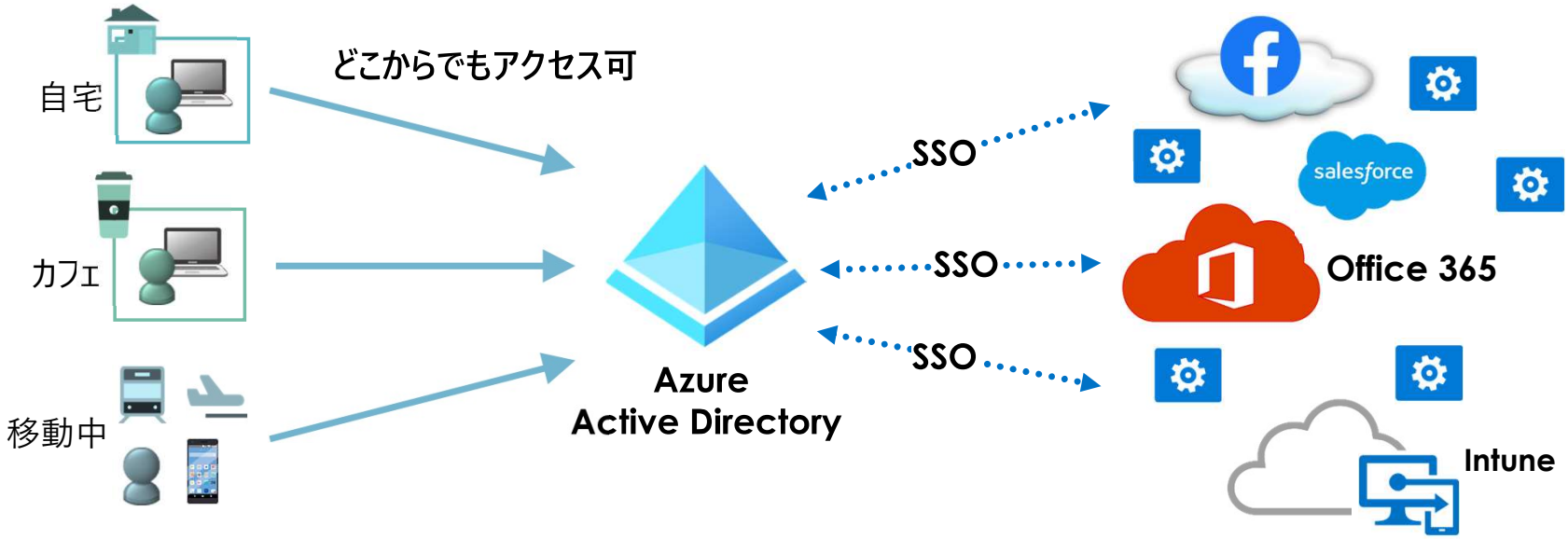
- 認証が行われた後に行われる次のプロセスは「承認」です。
  このプロセスでは、本人確認後のユーザーに、サービスやアプリケーションに対するアクセスを検証します。

SC-900 Microsoft Security,
Compliance, and Identity Fundamentals

3.2
Azure ADの基本的なIDサービスとIDタイプについて説明する

Azure Active Directoryとは

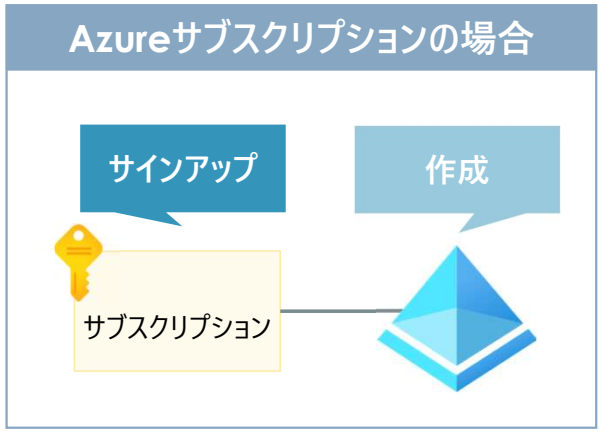
- Azure Active Directoryは、マイクロソフトのクラウドベースの**IDとアクセス管理サービス**です。

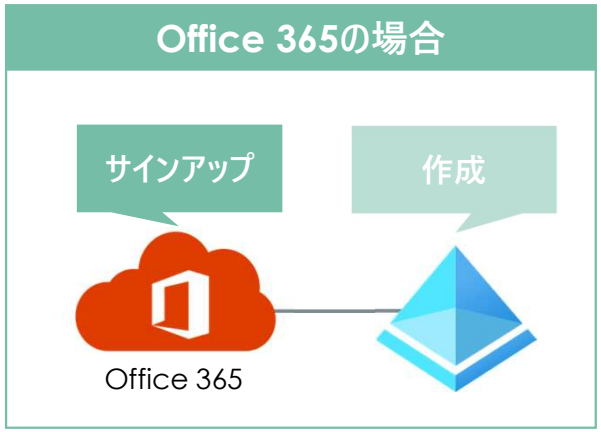


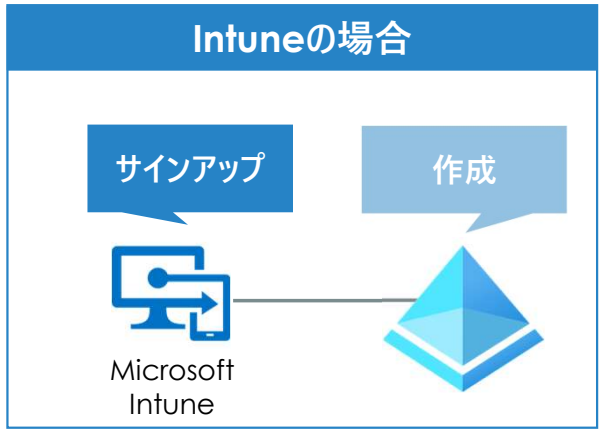
Point **Azure ADは、Identity Provider(Idp)です。Identity Providerとは、ユーザー IDを保存、検証するサービスです。**

Azure Active Directoryの作成方法は？

- Azure ADテナントは、Office 365、Intune、Azureサブスクリプションをサインアップ(契約)すると自動的に作成されます。







Point

Microsoft 365をサインアップした場合も同様です。
既にAzure ADのテナントがある場合は、
既存のテナントを使用することができます。

Azure Active Directory のライセンス

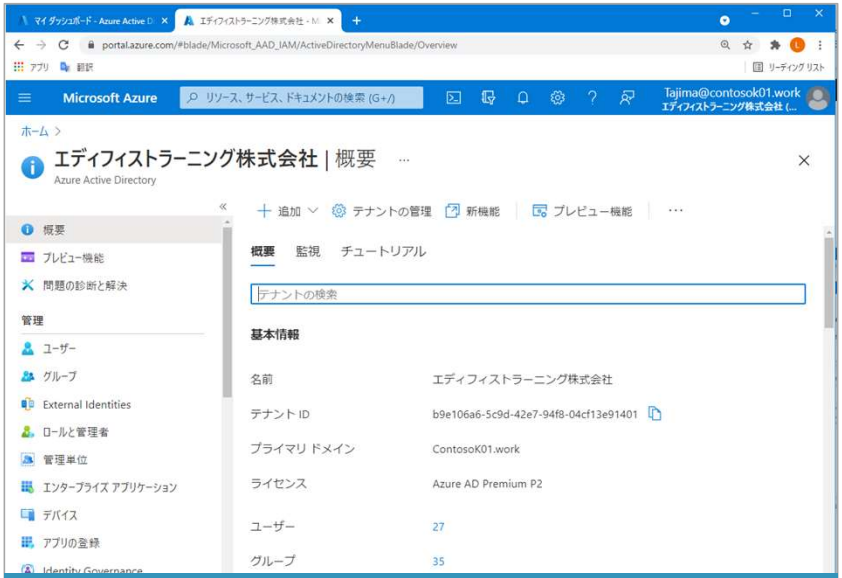
- 高度な機能使用するには、Premium P1またはPremium P2の有償ライセンスを購入する必要があります。

機能	Free	Office 365 アプリ	Premium P1	Premium P2
Core IDとアクセスの管理	✓	✓	✓	✓
企業間コラボレーション	✓	✓	✓	✓
Office 365アプリの ID とアクセス管理		✓	✓	✓
Premium機能			✓	✓
ハイブリッドID			✓	✓
高度なグループアクセス管理			✓	✓
条件付きアクセス			✓	✓
ID保護				✓
Identity Governance				✓

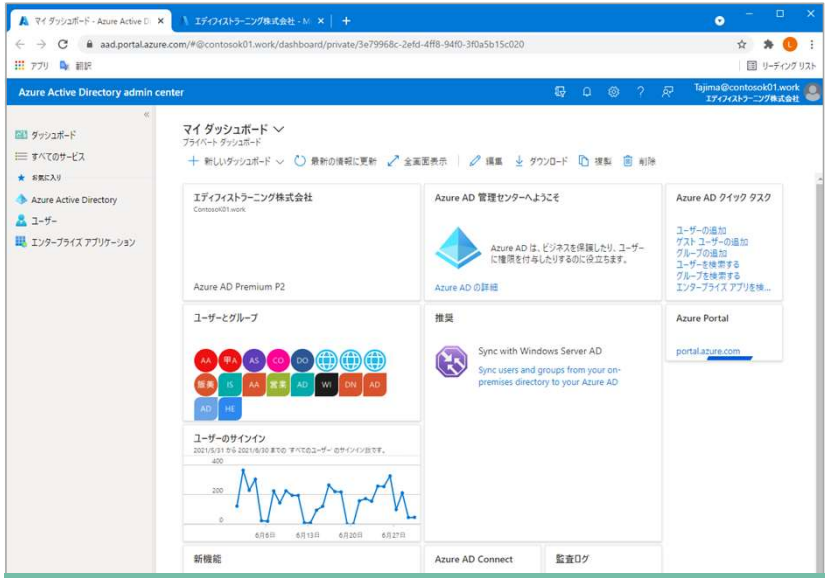
Azure ADの高度な機能を使うには、Azure ADのラインセンスを購入する必要があります。

Azure Active Directoryを管理するには？

- Azure ADの管理は、「Azure Portal」または「Azure Active Directory admin center」からできます。



Azure ポータル
(https://portal.azure.com)



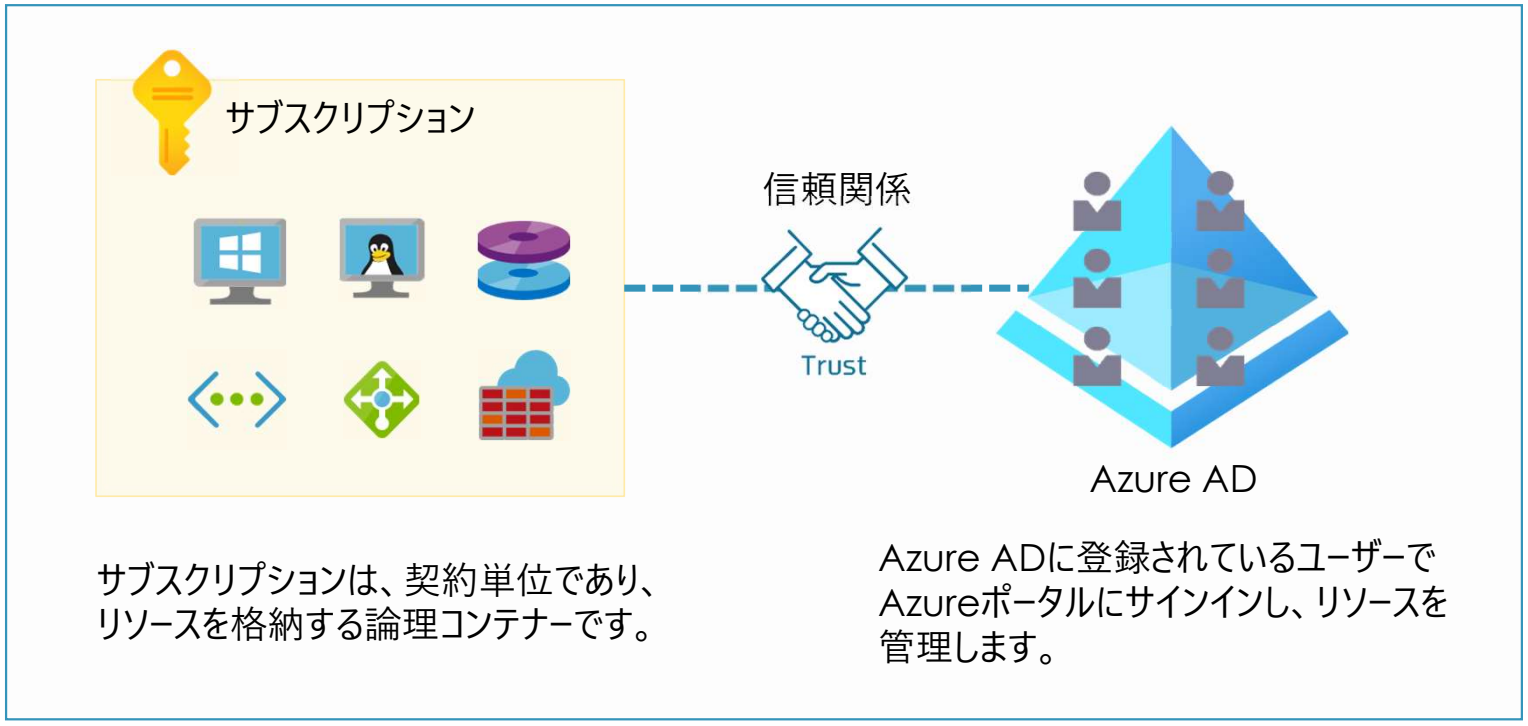
Azure Active Directory admin center
(https://aad.portal.azure.com)

Point

「Azure Active Directory admin center」は、Microsoft 365 管理センターからも起動できます。

Azure ADテナントとAzureサブスクリプションの関係

- Azureサブスクリプションをサインアップすると、Azure ADテナントが作成され、2つの間に信頼関係が結ばれます。



Exam Point

次の各ステートメントについて、ステートメントが真の場合は、「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。

①Azure ADは、Microsoft 365のサブスクリプションの一部として提供されます。
②Azure ADは、オンプレミスの環境に展開できます。
③Azure ADは、IDとアクセス管理サービスです。

解答：以下を参照

① Azure ADは、Microsoft 365のサブスクリプションの一部として提供されます。

いいえ Azure ADは、Microsoft 365のサブスクリプションにも含まれていますが、単体でライセンス購入を行うことができるため、Microsoft 365にしか含まれないものではありません。

② Azure ADは、オンプレミスの環境に展開できます。

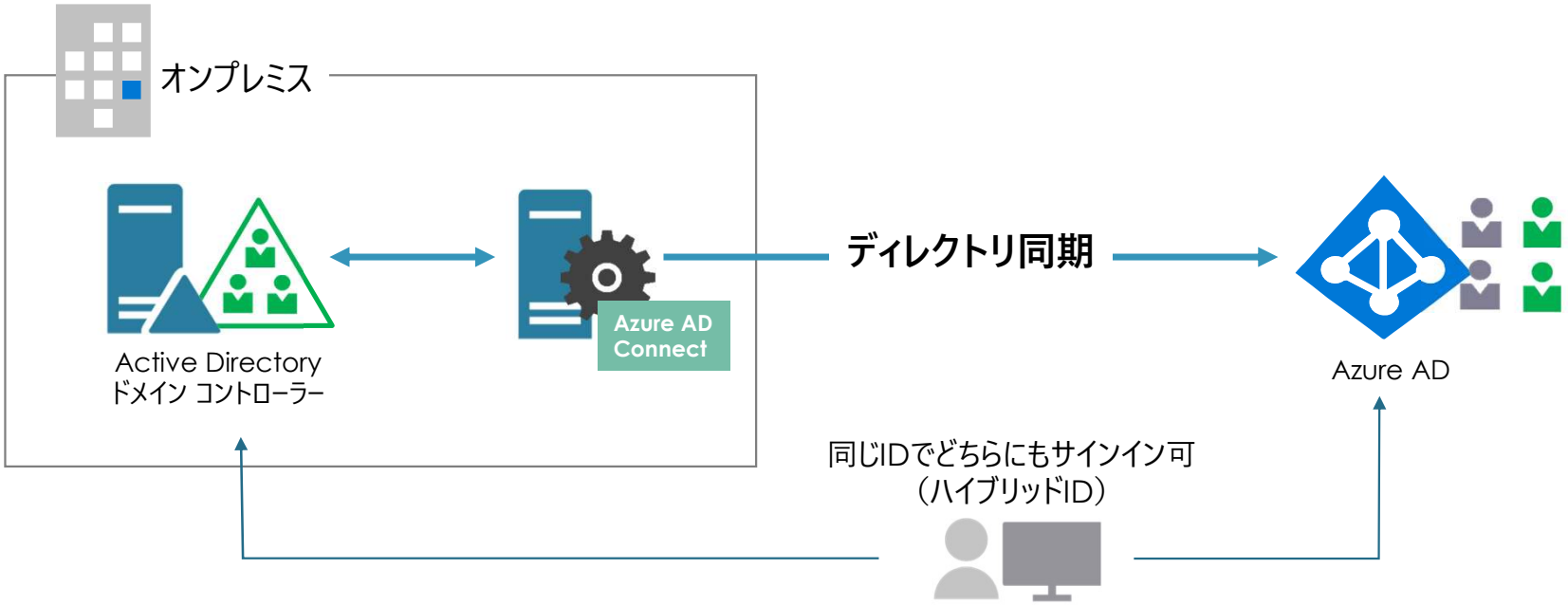
いいえ Azure ADは、Microsoftのクラウドサービスで、オンプレミスには展開できません。

③Azure ADは、IDとアクセス管理サービスです。

はい Azure ADは、IDとアクセス管理サービスです。

ディレクトリ同期

- ディレクトリ同期を実行すると、オンプレミスのユーザーをAzure ADに同期することができます。
- ディレクトリ同期を行うには、オンプレ側に「Azure AD Connect」がインストールされている Windows Server が必要です。



Point ディレクトリ同期により同期されたIDをハイブリットIDと呼び、同じIDでAD DSとAzure ADにサインインできます。

Exam Point

次の各ステートメントについて、ステートメントが真の場合は、「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。

①Azure AD Connectを使用すると、ハイブリッドIDを構成できます。
②ハイブリッドIDとは、AD DSとAzure ADの同期をとることです。
③ハイブリッドIDを実装するには、複数のMicrosoft 365テナントが必要です。

解答：以下を参照

① Azure AD Connectを使用すると、ハイブリッドIDを構成できます。

はい　Azure AD Connectを使用して、オンプレミスとAzure ADの間で同期を行うとユーザーIDなどが同期され、同じIDでオンプレミスのAD DSとAzure ADの両方にサインインできます

② ハイブリッドIDとは、AD DSとAzure ADの同期をとることです。

はい　Azure AD Connectを使用して、オンプレミスとAzure ADの間で同期を行うとユーザーIDなどが同期され、同じIDでオンプレミスのAD DSとAzure ADの両方にサインインできます

③ハイブリッドIDを実装するには、複数のMicrosoft 365テナントが必要です。

いいえ　ハイブリッドIDの構成に、Microsoft 365のテナントは不要です。

SC-900 Microsoft Security,
Compliance, and Identity Fundamentals

3.3
Azure ADの認証機能について説明する

Windows Hello

Windows Helloは、生体認証を使用した安全なサインインを提供します。

Point

3 種類の生体認証をサポートします。

- ✓ 指紋
- ✓ 顔
- ✓ 虹彩

高速な認証を実現します。

- ✓ 顔認証では、サインインにかかる時間は2秒程度です。

デバイスに保存されます。

認証に必要なPINや生体情報は、ローカルデバイスに保存されます。

スプーフィングを防止します。

スプーフィング(なりすまし)防止対策として有効です。

Windows Hello for Business

2要素認証(キーまたは証明書をデバイスに関連付け、PINまたは生体認証を組み合わせて行う)を使用した強力なサインインを提供します。

サポートするアカウント

- ✓ Microsoftアカウント
- ✓ Active Directoryアカウント
- ✓ Azure ADアカウント

複数の展開モデル

- ✓ クラウド
- ✓ オンプレミス
- ✓ ハイブリッド

Point

デバイスに保存されます。

認証に必要なPINや生体情報は、ローカルデバイスに保存されます。

2要素認証

PINや生体と、証明書や非対称キーペアを用いた安全な認証を提供します。

Exam Point

次のステートメントを完了させてください。

Windows Hello for Businessでは、認証に使用されるユーザーの生体データは、[①]

	選択肢
A	外部デバイスに保存されます。
B	ローカルデバイスにのみ保存されます。
C	Azure Active Directoryに保存されます。
D	ユーザーが指定したデバイスすべてに複製されます。

解答：B

Windows Hello for Businessで使用される生体データは、
ローカルデバイスにのみ保存されます。

Azure AD多要素認証(MFA:Multi-Factor Authentication)

多要素認証(MFA)は、複数の要素(知識、所持、特徴など)を使用して認証を行うことによって、認証の安全性を高めます。

第1要素

- ユーザー名
- パスワード

知っている(知識情報)

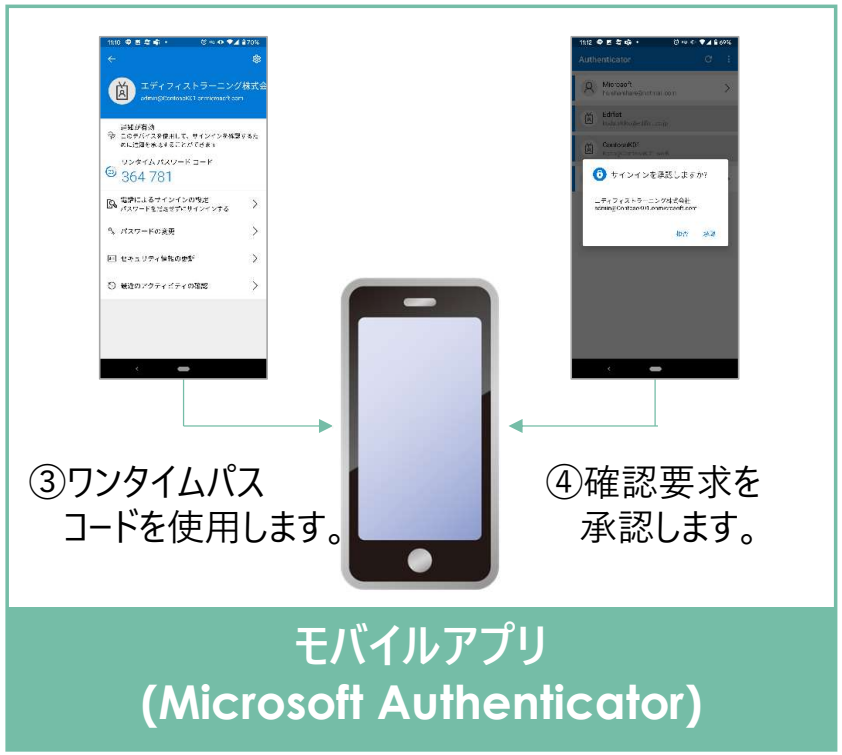
第2要素

- 会社の電話
- 携帯電話
- トークン

持っている(所持情報)

2要素目の認証方法

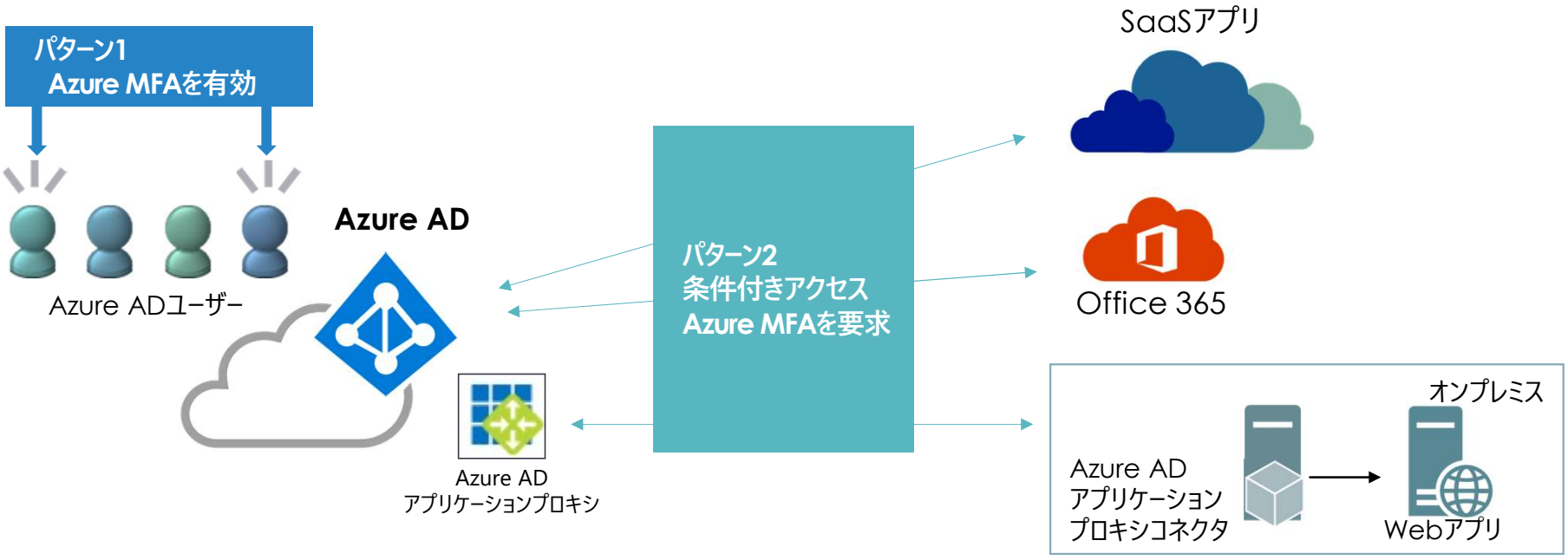
Azure AD多要素認証は、第2要素として次のものを使用することができます。



MFAの設定

MFAは次の2つの方法で設定を行うことができます。

- ✓ パターン1
  Azure ADユーザーを指定し、該当ユーザーに対して常にMFAを要求します。
- ✓ パターン2
  条件付きアクセスポリシーで、指定した条件に合致した場合、MFAを要求します。



Exam Point

次のステートメントを完了させてください。

[①]では、携帯電話に送信される確認コードなど、追加の確認が必要です。

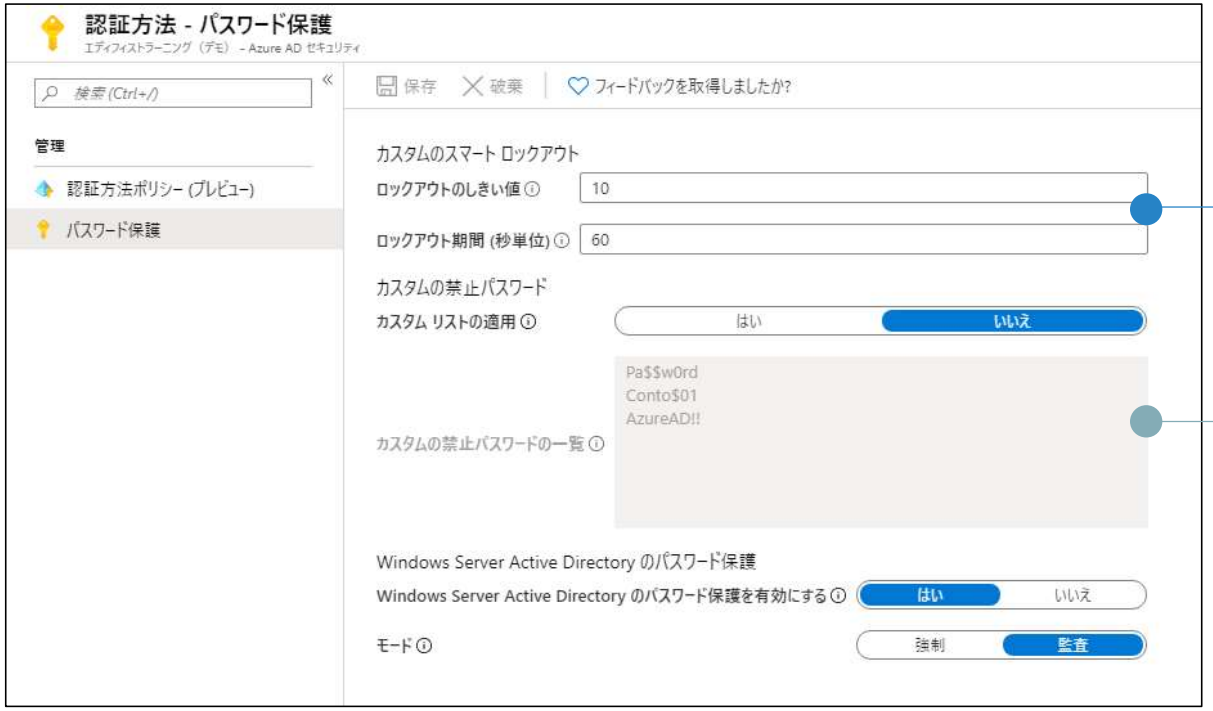
	選択肢
A	多要素認証(MFA:Multi-Factor Authentication)
B	パススルー認証
C	パスワードライトバック
D	シングルサインオン(SSO)

解答：A

携帯電話に送信される確認コードなど、追加の確認が必要なのは
多要素認証です。

Azure ADのパスワード保護

Azure ADでは、[パスワード保護]ページで、ユーザーに使用して欲しくないパスワードを定義することができます。



スマートロックアウトしきい値、ロックアウト期間の設定を設定します。

ユーザーがパスワードで使用できないようにする語の一覧です。

- ✓ 最大1000語
- ✓ 大文字と小文字の区別はありません。
- ✓ 一般的な文字置換(0の場合にはoなど)が自動的に考慮されます。

Point

Point

[パスワード保護]の目的は、パスワードに特定の言葉が使われることを防ぐことです。

Exam Point

Azure Active Directoryのパスワード保護の目的は何ですか。

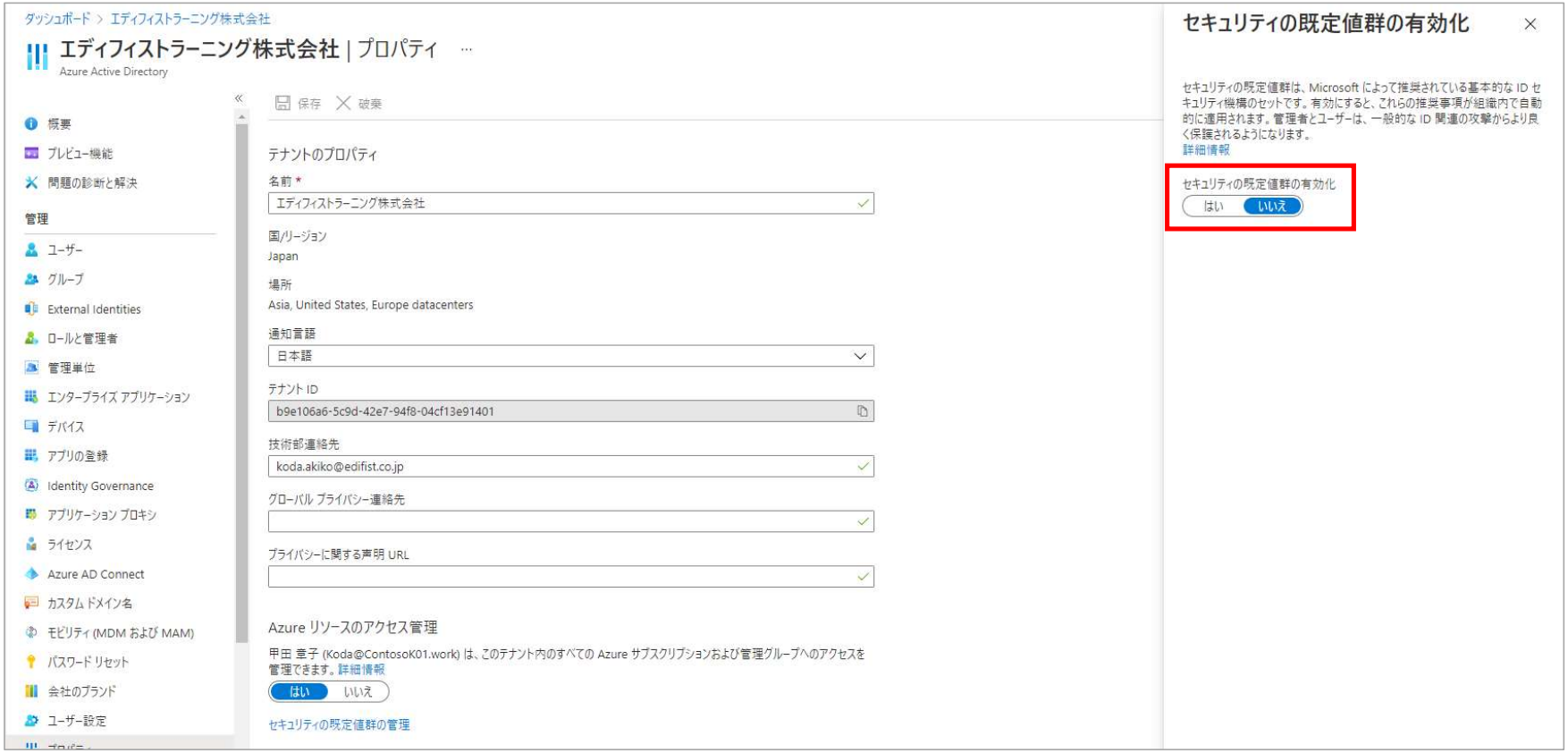
	選択肢
A	ユーザーがパスワードを変更しなければならない頻度を制御します。
B	多要素認証(MFA)を使用せずにユーザーがサインインできるデバイスを識別します。
C	グローバルに認識される暗号化標準を使用してパスワードを暗号化します。
D	ユーザーがパスワード内の特定の単語を使用するのを防ぎます。

解答：D

Azure ADのパスワード保護では、[カスタムの禁止パスワード]を有効にすることで、パスワードに特定の単語が使用されることを防ぎます。

Azure ADのセキュリティの既定値群

Azure ADのセキュリティの既定値群は、Microsoftが推奨する基本的なIDセキュリティ設定のセットです。設定を有効にすることで組織内に推奨される設定が自動的に適用されます。



Azure ADのセキュリティの既定値群で設定される内容

Azure ADのセキュリティの既定値群を有効にすると、次の設定が自動的に適用されます。

- ✓ **多要素認証の登録手続きの統一**
  テナント内のすべてのユーザーはMFAが自動的に有効になります。

- ✓ **管理者の保護**
  全体管理者やExchange管理者などの特定のロールを持つユーザーは、MFAへの登録が完了した後、サインインのたびに追加の認証を実行する必要があります。

- ✓ **すべてのユーザーの保護**
  ユーザーが新しいデバイスやアプリを使用して認証するときや、重要な役割とタスクを実行するときはMFAを求められます。

- ✓ **レガシ認証をブロックする**
  古いプロトコルによる認証要求をすべてブロックします。

Azure ADのセキュリティの既定値群を有効にすると、すべてのユーザーに対して多要素認証が有効になります。

Exam Point

次のステートメントを完了させてください。

Azure Active Directoryの既定のセキュリティを
有効にした場合、Azure ADのすべての
ユーザーに対して、[①]が有効になります。

	選択肢
A	多要素認証(MFA:Multi-Factor Authentication)
B	Azure AD Privileged Identity Management
C	Azure AD Identity Protection

解答：A

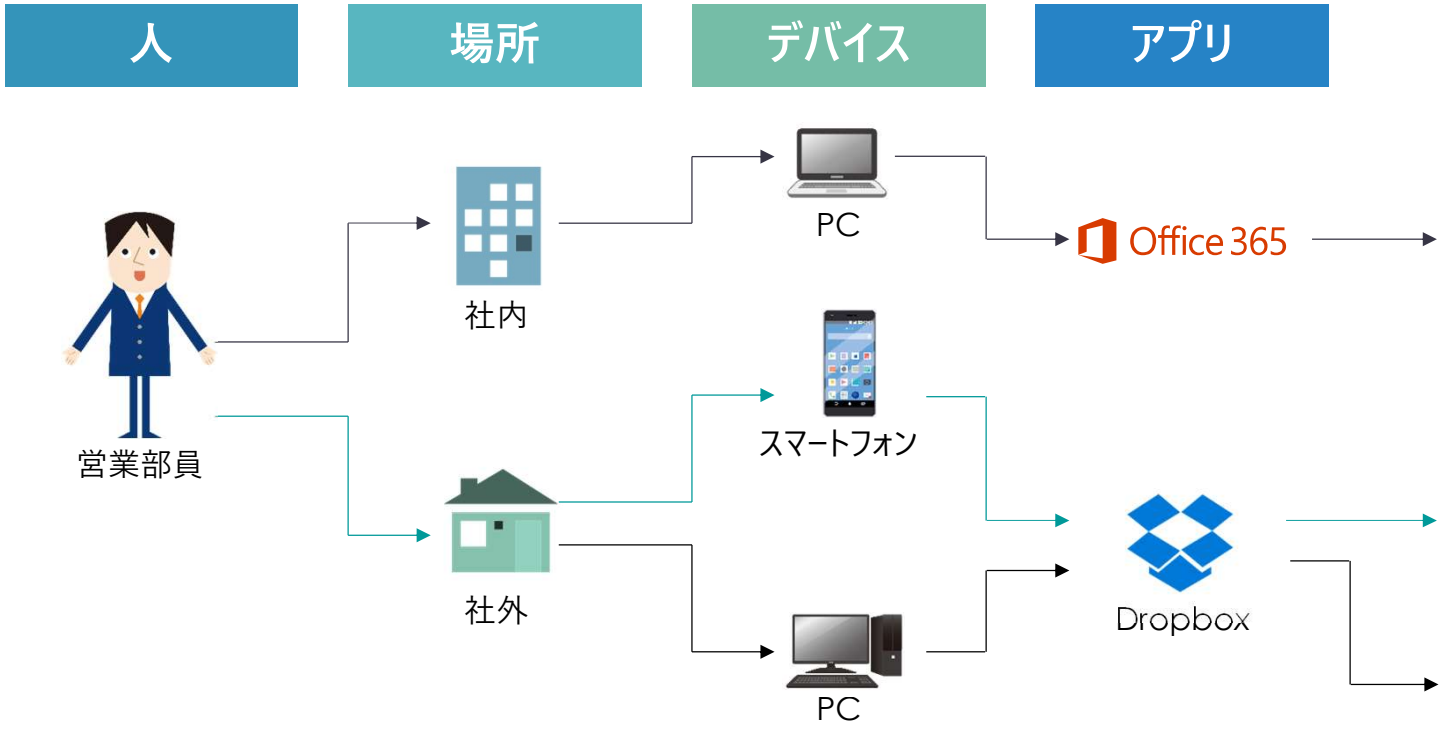
Azure ADの既定のセキュリティを有効にすると、すべてのユーザーに対して
MFAが有効になります。

SC-900 Microsoft Security,
Compliance, and Identity Fundamentals

3.4
Azure ADのアクセス管理機能について説明する

条件付きアクセス

条件付きアクセスを構成すると、デバイスや場所、ユーザーなどの条件に基づいて、条件に該当した場合にアプリへのアクセスを許可/拒否することができます。



許可の条件

- 多要素認証を強制
- デバイスは準拠済み
- ハイブリッド Azure AD に参加済み
- 承認されたクライアントアプリ

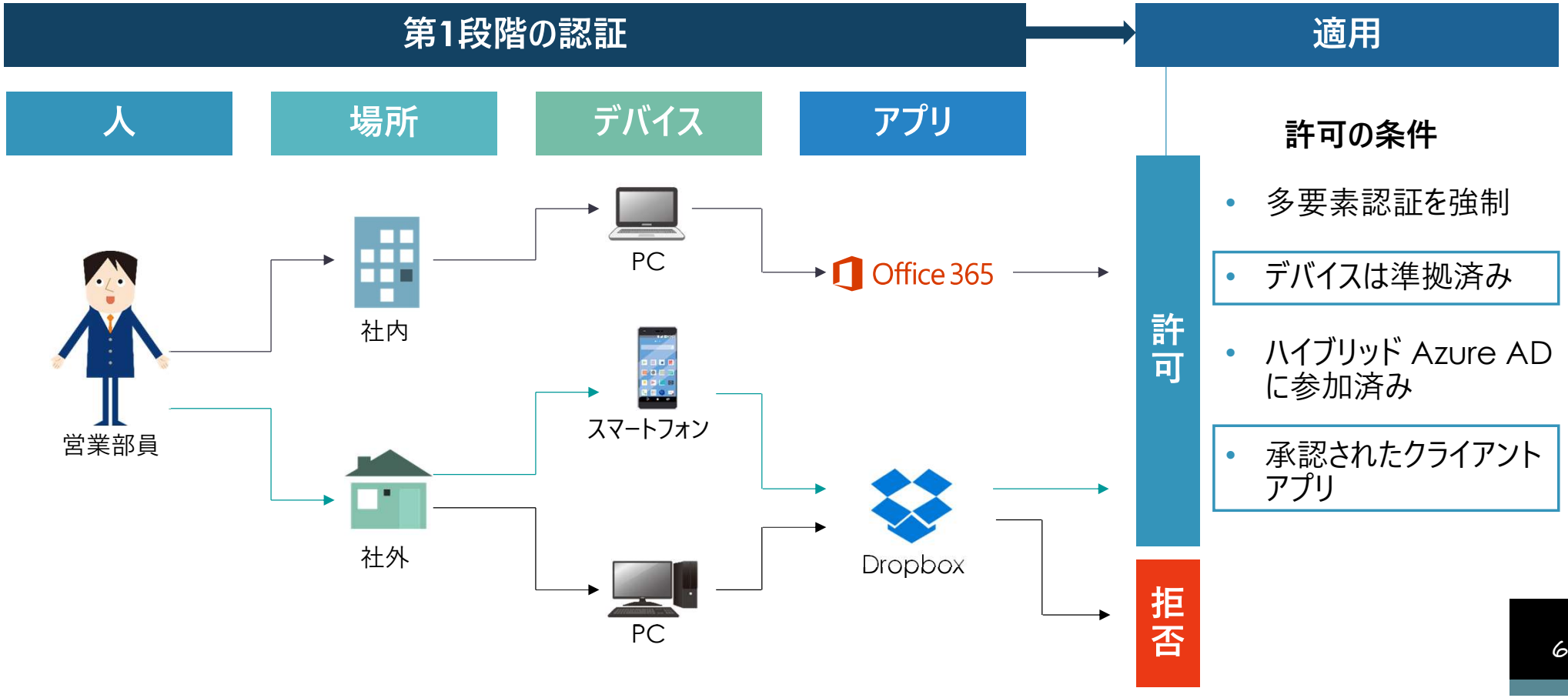
Point

アプリへのアクセスを許可する条件として、MFAを要求するように構成することができます。
Azure AD参加をしていないデバイスに対しても条件付きアクセスは適用されます。

条件付きアクセスが適用されるタイミング

Point

条件付きアクセスは、第1段階の認証が完了した時点で適用されます。



条件付きアクセスの適用対象となるユーザーとグループ

次のユーザーやグループは、条件付きアクセスの適用対象にすることができます。

適用対象のユーザーやグループ

- ✓ **すべてのユーザーと外部ユーザー**
  Azure ADに登録されているゲストユーザーや外部ユーザーを適用対象にすることができます。
- ✓ **ディレクトリロール**
  全体管理者などのロールメンバーを適用対象にすることができます。
- ✓ **ユーザーとグループ**
  指定したユーザーやグループを適用対象にすることができます。

Point

条件付きアクセスは、全体管理者などのディレクトリロールを適用対象にすることができます。

条件付きアクセスの条件

条件付きアクセスでは、次の条件を設定することができます。

Point

条件付きアクセスでは、条件(シグナル)として、デバイスプラットフォームやデバイスの状態、場所を使用することができます。

- ✓ **ユーザーのリスク**
  Azure AD Identity Protectionで検出されたユーザーのリスクレベルによってアクセスの可否を決定することができます。
- ✓ **サインインのリスク**
  Azure AD Identity Protectionで検出されたサインインのリスクレベルによってアクセスの可否を決定することができます。
- ✓ **デバイスプラットフォーム**
  使用するデバイスのプラットフォームによってアクセスの可否を決定することができます。
- ✓ **場所**
  ネームドロケーションの設定を行うことによって、信頼された場所からアクセスしている場合のみアクセスを許可することができます。
- ✓ **クライアントアプリ**
  使用を許可/拒否したいクライアントアプリの種類を指定します。
- ✓ **デバイスの状態**
  ハイブリッドAzure AD参加済みデバイスや、コンプライアンスポリシーに準拠しているとマークが付けられているデバイスを除外することができます。
- ✓ **デバイスのフィルター**
  デバイスの状態によって、アプリへのアクセスを許可/拒否することができます。
  たとえば、デバイスIDや特定のデバイス名、Azure ADの登録の状態などを指定することができます。

ネームドロケーションの構成

ネームドロケーションを構成すると、条件付きアクセスで「信頼できる場所」の指定が可能です。

Point

ユーザーのいる場所に基づいて、アプリへのアクセスを許可/拒否することができます。

信頼できる場所とは、IT部門が管理するネットワーク領域のことで
条件付きアクセスの条件として指定ができます。

Exam Point

次の各ステートメントについて、ステートメントが真の場合は、「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。

①条件付きアクセスポリシーは、シグナルとしてデバイスの状態を使用できます。
②条件付きアクセスポリシーは、第1要素の認証が終わる前に適用されます。
③条件付きアクセスポリシーは、ユーザーが特定のアプリケーションにアクセスを試みた時に
多要素認証をトリガーさせることができます。

解答：以下を参照

①条件付きアクセスポリシーは、シグナルとしてデバイスの状態を使用できます。

はい　条件として、デバイスの状態を使用することができます。
コンプライアンスポリシーに準拠していないデバイスからの接続を拒否することができます。

②条件付きアクセスポリシーは、第1要素の認証が終わる前に適用されます。

いいえ　条件付きアクセスポリシーは、第1要素の認証が完了した後で適用されます。

③条件付きアクセスポリシーは、ユーザーが特定のアプリケーションにアクセスを試みた時に多要素認証をトリガーさせることができます。

はい　条件付きアクセスポリシーは、アプリへのアクセスを許可する際に多要素認証を要求することができます。

SC-900 Microsoft Security,
Compliance, and Identity Fundamentals

3.5
Azure ADのID保護とガバナンス機能について説明する

Azure AD Privileged Identity Managementによる特権管理

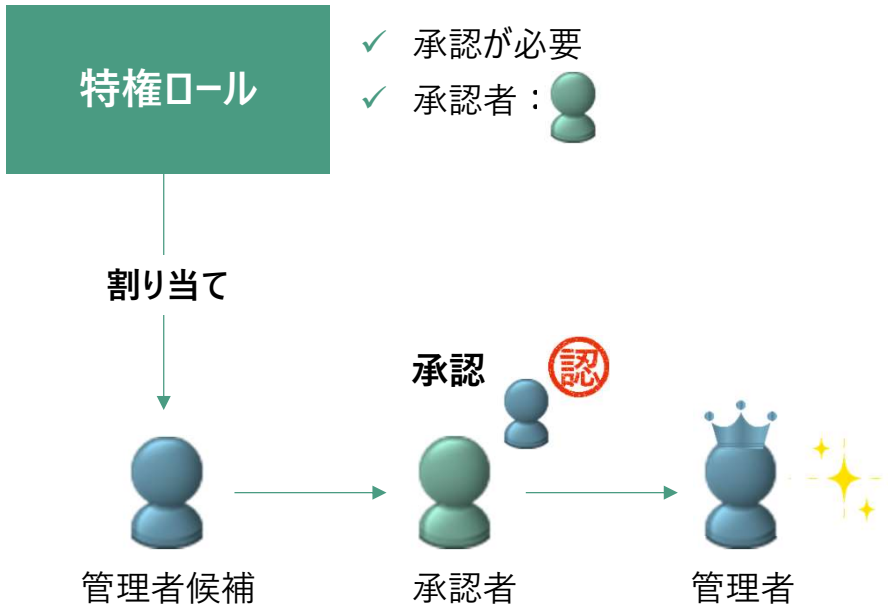
Azure AD Privileged Identity Managementを利用すると、一定期間のみ管理者ロールを付与したり、ロールを付与したときに承認者による承認が行われるように構成することができます。

Point

JITアクセス(Just-In-Timeアクセス)の提供

ロールを割り当てる際に、永続的にロールを割り当てるか、一定期間のみ割り当てるかを指定できます。

ロールを付与する際に承認を要求



Exam Point

Azureリソースを管理するためのジャストインタイム(JIT)アクセスを提供するために使用できるAzure Active Directoryの機能はどれですか。

	選択肢
A	Azure AD Identity Protection
B	条件付きアクセス
C	Azure AD Privileged Identity Management
D	認証方法ポリシー

解答：C

ジャストインタイム(JIT)アクセスを提供するために使用できるAzure ADの機能は、Azure AD Privileged Identity Managementです。

Exam Point

Azureの管理タスクを行うために、2時間の枠で管理権限を提供できる機能はどれですか。

	選択肢
A	Azure AD Privileged Identity Management
B	条件付きアクセス
C	Azure AD Identity Protection
D	多要素認証(MFA)

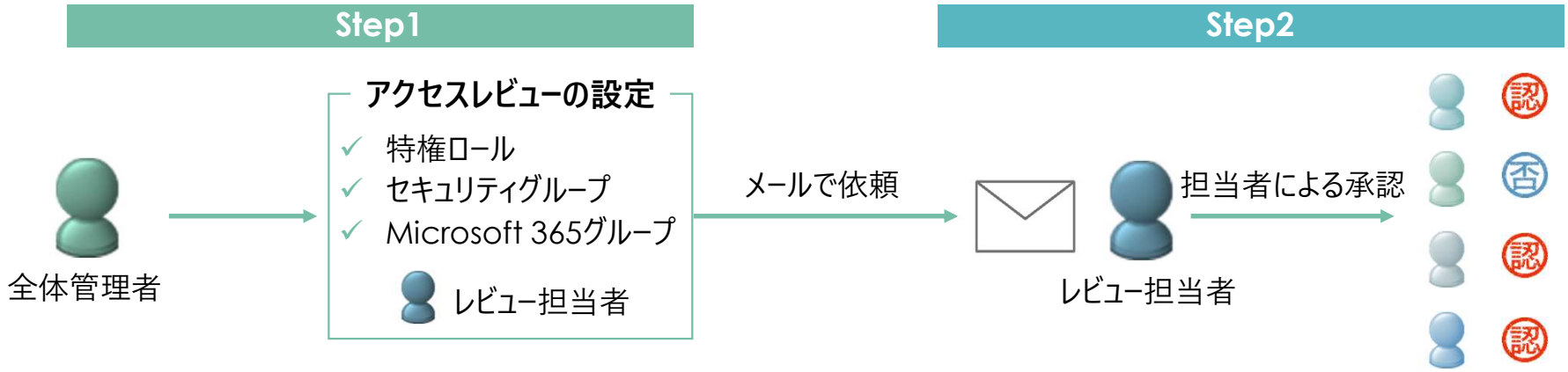
解答：A

一定期間のみ管理者権限を付与できるのは、Azure AD Privileged Identity Managementです。

アクセスレビュー

Point

定期的に特権ロールを持つメンバーやグループのメンバーをチェックし、使用されていないユーザーは削除することができます。



- ✓ チームの稼働状況を理解しているメンバーにレビューをアサインできるので適切な棚卸できます。
- ✓ アクセスレビューは定期的なサイクルで実行できるため、「やり忘れ」を防ぐことができます。
- ✓ 推奨事項を自動適用することも可能です。

Exam Point

グループメンバーシップを評価し、グループのメンバーシップを必要としなくなったユーザーを自動的に削除するために使用できる Azure Active Directory機能はどれですか。

選択肢	
A	マネージドID
B	アクセスレビュー
C	条件付きアクセスポリシー
D	Azure AD Identity Protection

解答：B

グループやロールのメンバーシップをレビューし、不要なユーザーを削除できるのは、アクセスレビューです。

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Microsoft Azureのセキュリティとコンプライアンス ソリューション

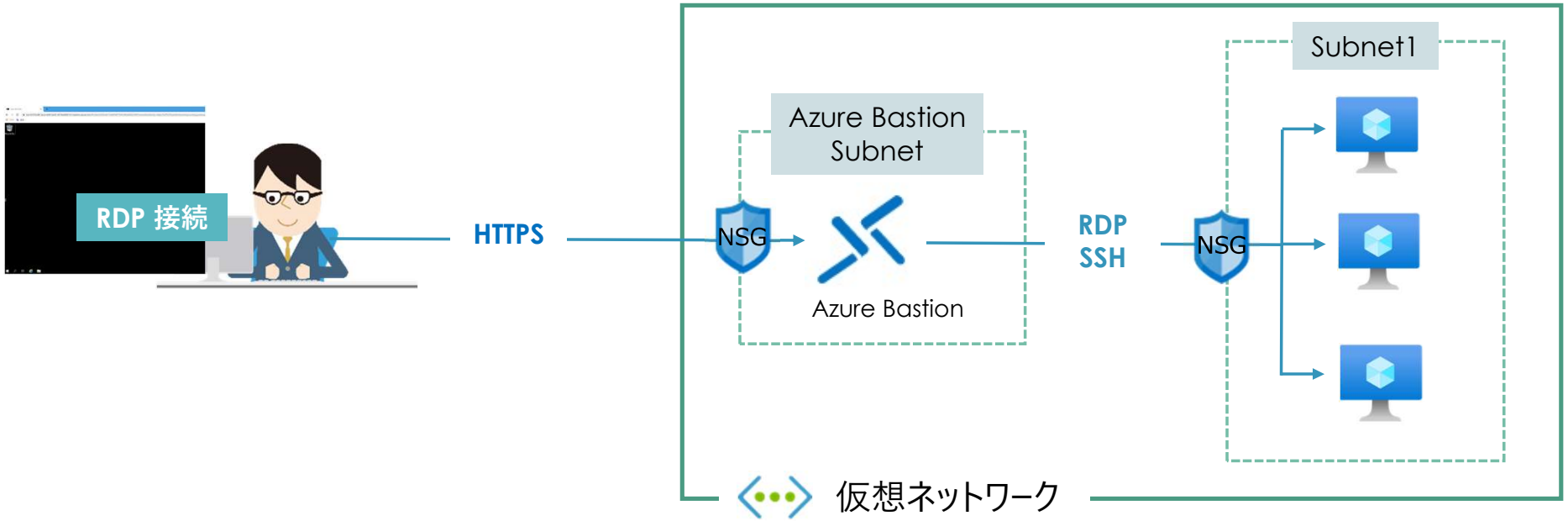
4

SC-900 Microsoft Security,
Compliance, and Identity Fundamentals

4.1 Azureの基本的なセキュリティ機能を説明する

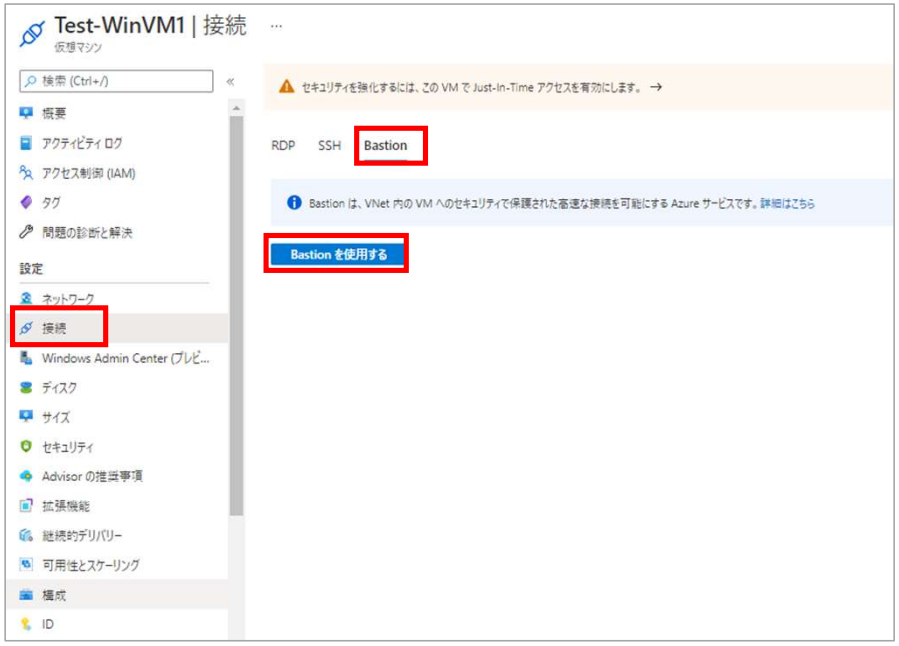
Azure Bastion

- Azure仮想ネットワーク内のVMに対して、安全かつシームレスにRDPおよびSSH接続を実行できるサービスです。
- 接続にHTTPSを使用するため、RDPやSSHをブロックしているネットワークからでもアクセスできます。

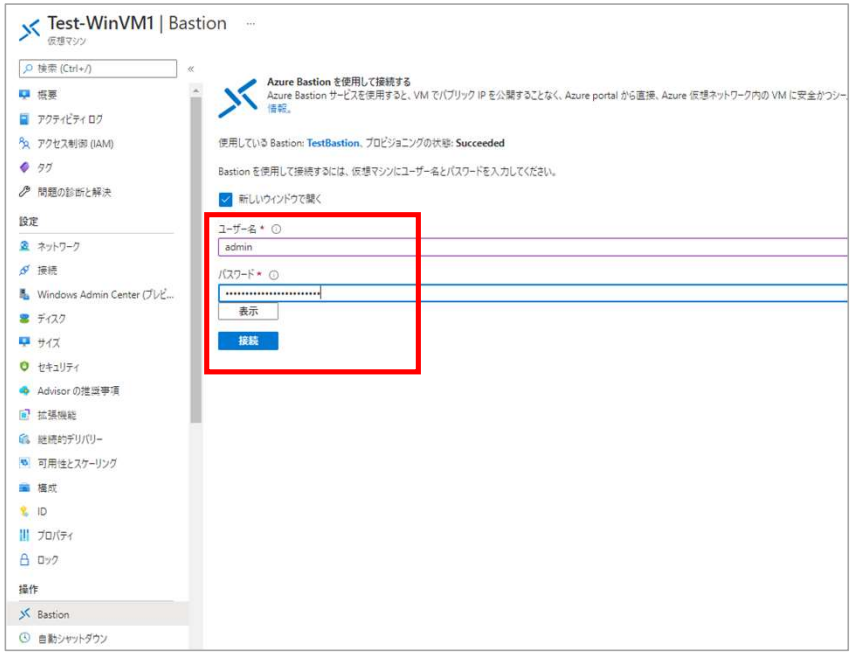


Azure Bastion経由で仮想マシン接続するには -①

- Azure Bastion経由で仮想マシンに接続するには、Azure Portalを使用します。

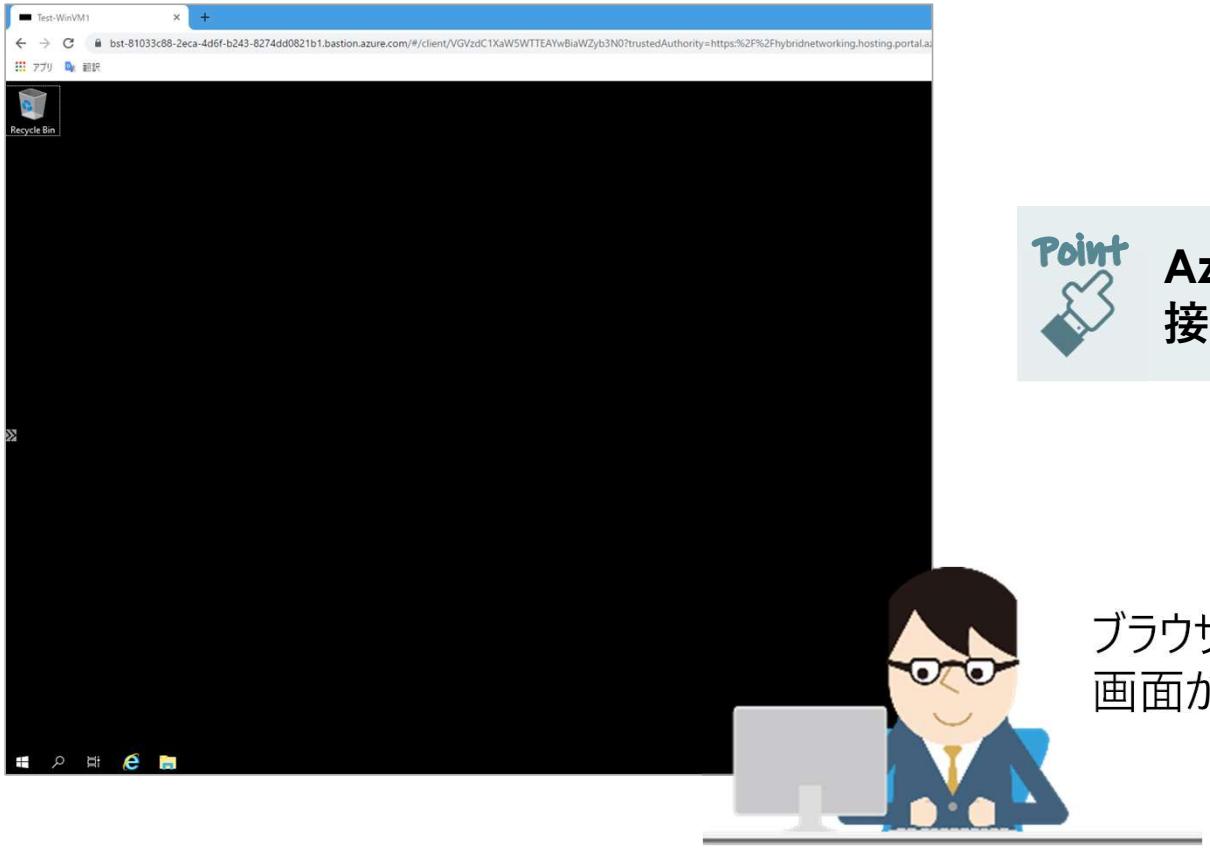


接続したい仮想マシンの [接続]メニューで、[Bastion]タブをクリックし、[Bastionを使用する]をクリックします。



仮想マシンの管理者名とパスワードを入力し、[接続]をクリックします。

Azure Bastion経由で仮想マシン接続するには -②



Point

Azure Bastion は、Azure Portal で接続します。

ブラウザーに新しいタブが追加され、RDP接続の画面が表示されます。

Exam Point

次の各ステートメントについて、ステートメントが真の場合は、「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。

①Azure Bastionは、RDP接続をセキュアに行えます。

②Azure Bastionは、仮想ネットワークごとに作成します。

③Azure Bastionは、Azure Portalを使用して接続します。

解答：以下を参照

①Azure Bastionは、RDP接続をセキュアに行えます。

はい　Azure Bastionは、RDP/SSH接続をセキュア行うサービスです。

②Azure Bastionは、仮想ネットワークごとに作成します。

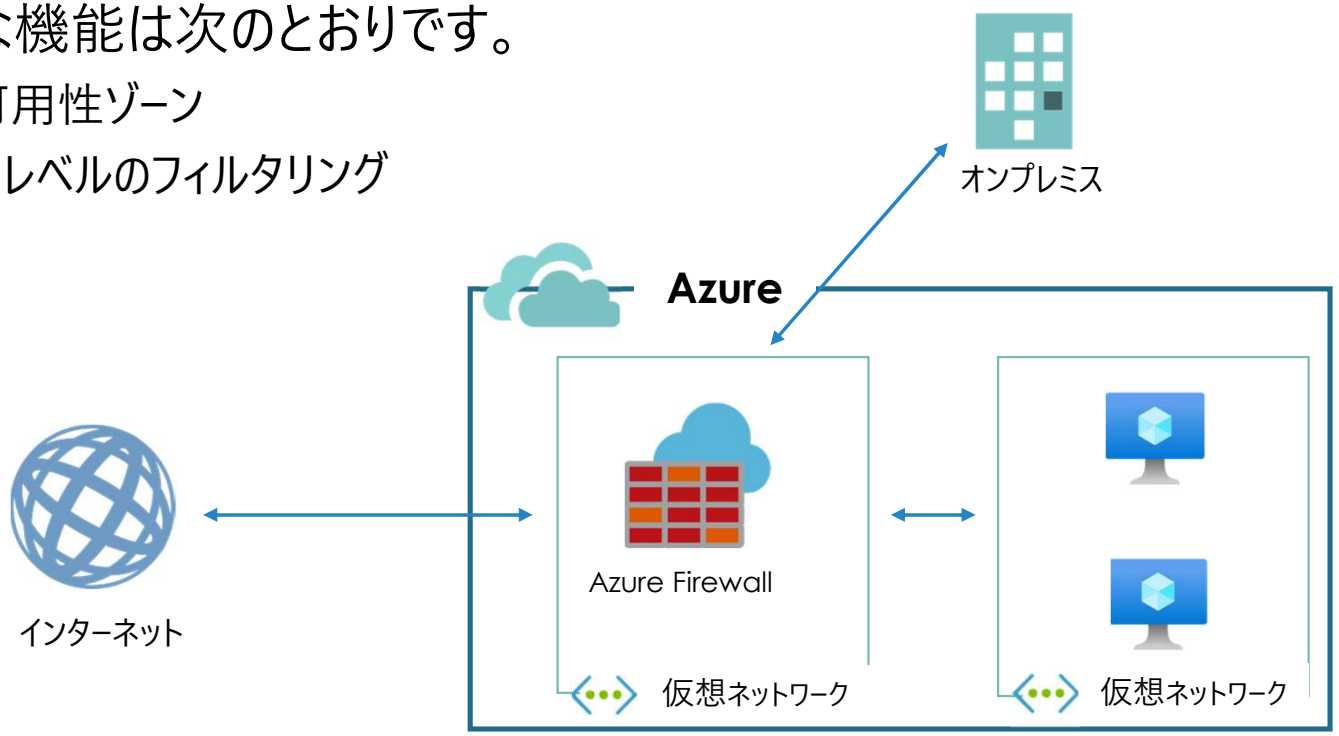
はい　Azure Bastionは、接続したい仮想マシンがある仮想ネットワークごとに作成します。

③Azure Bastionは、Azure Portalを使用して接続します。

はい　Azure Bastion経由で仮想マシンに接続するには、Azure Portal を使用して接続します。

Azure Firewall

- Azure Virtual Networkリソースを保護するファイアウォールサービスです。
- Azure Firewallサービスの主な機能は次のとおりです。
  - 組み込まれた高可用性および可用性ゾーン
  - ネットワークおよびアプリケーションレベルのフィルタリング
  - 送信SNATおよび受信DNAT
  - 脅威インテリジェンス
  - Azure Monitorとの統合



Point **Azure Firewallには、ポリシーに基づくフィルタリング機能のほか、ネットワークアドレス変換(NAT)機能があります。**

Exam Point

Azure Firewallで保護できるものは何ですか。正しいものを2つ選択してください。

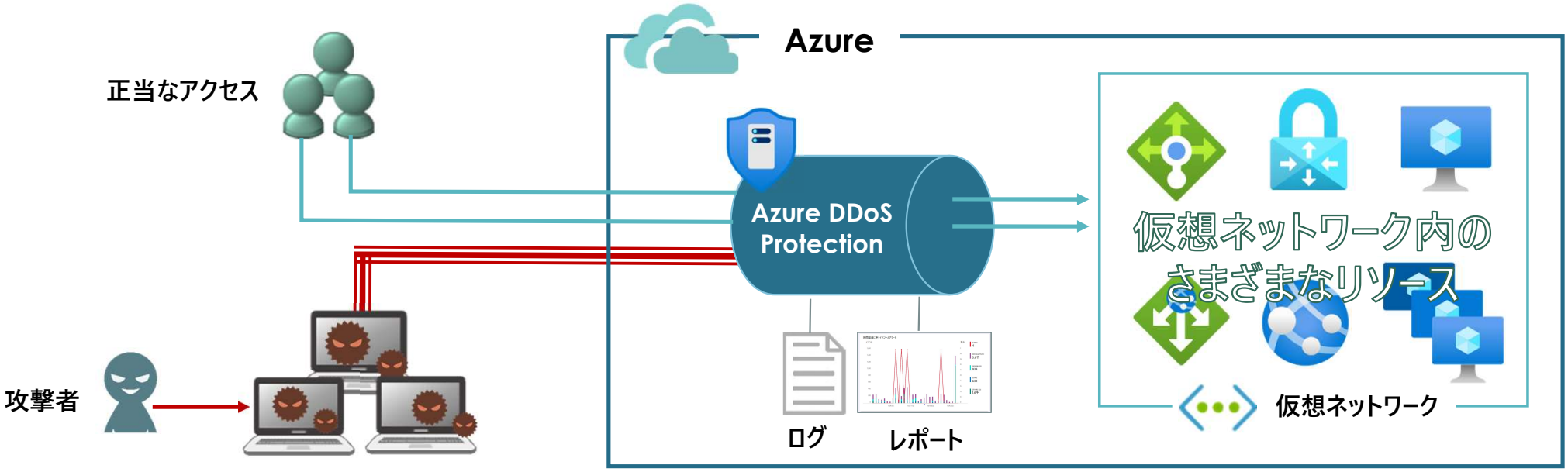
	選択肢
A	Azure ADユーザー
B	Exchange Onlineの受信トレイ
C	Azure仮想マシン
D	SharePointサイト
E	Azure仮想ネットワーク

解答：C、E

- Azure Firewallは、仮想ネットワーク内のリソースを保護できます。

Azure DDoS Protection

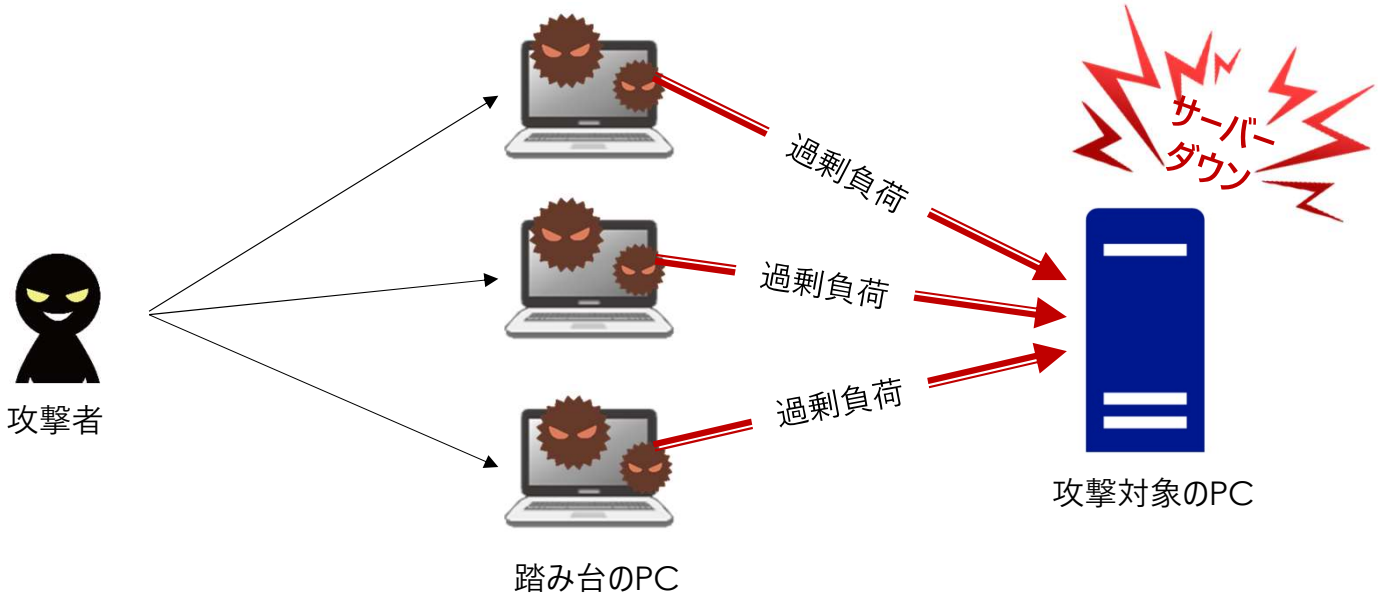
- **仮想ネットワーク**内のパブリックIPアドレス持つリソースをDDoS(分散サービス拒否)攻撃から保護するサービスです。
- 2つのEditionがあります
  - Basic(無料)
  - Standard(ログなどの機能があります)



参考：DDoS攻撃とは

- 攻撃対象のサーバーへ大量のデータや処理要求を送り付け、サーバーに負荷をかけダウンさせる攻撃です。

DoS攻撃は原則として1台のコンピューターから行われるのに対し、DDoS攻撃は大量のコンピューターから仕掛けられるので、より対処が困難。



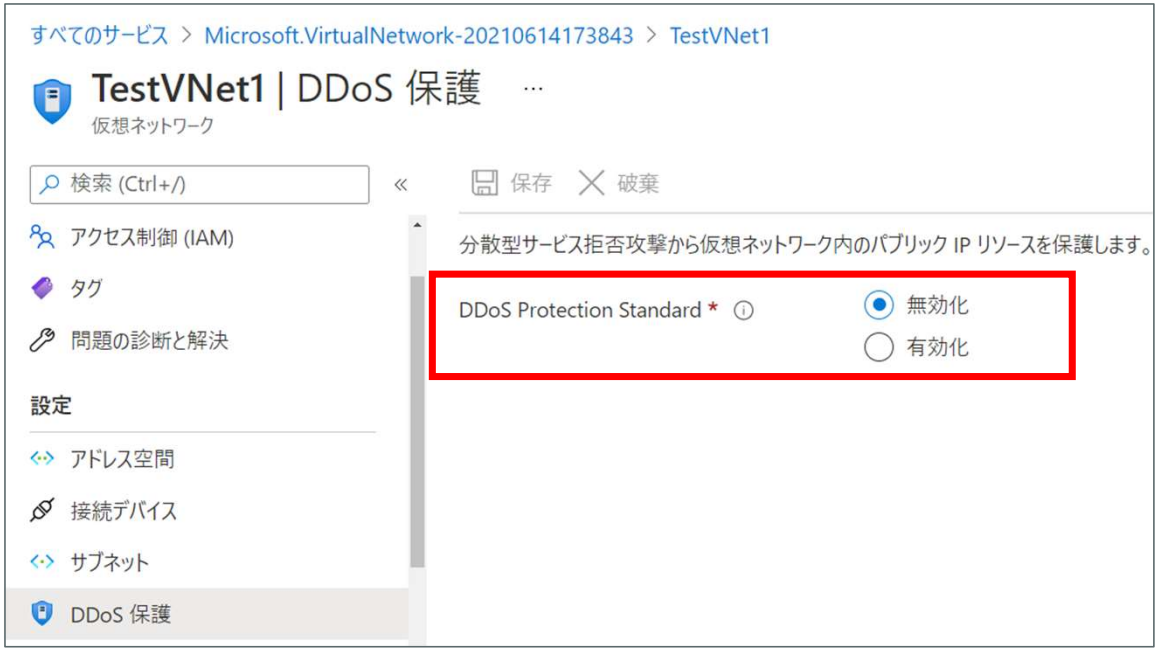
Exam Point

DDoS Protection Standardで保護できるものは何ですか。

	選択肢
A	リソースグループ
B	仮想ネットワーク
C	Azure Active Directoryのユーザー
D	Azure Active Directoryのアプリケーション

解答：B

- Azure DDoS Protectionで保護できるのは、仮想ネットワークです。
  - Azure DDoS Protection Standardエディションは、仮想ネットワークリソースのDDoS保護メニューで有効にします。

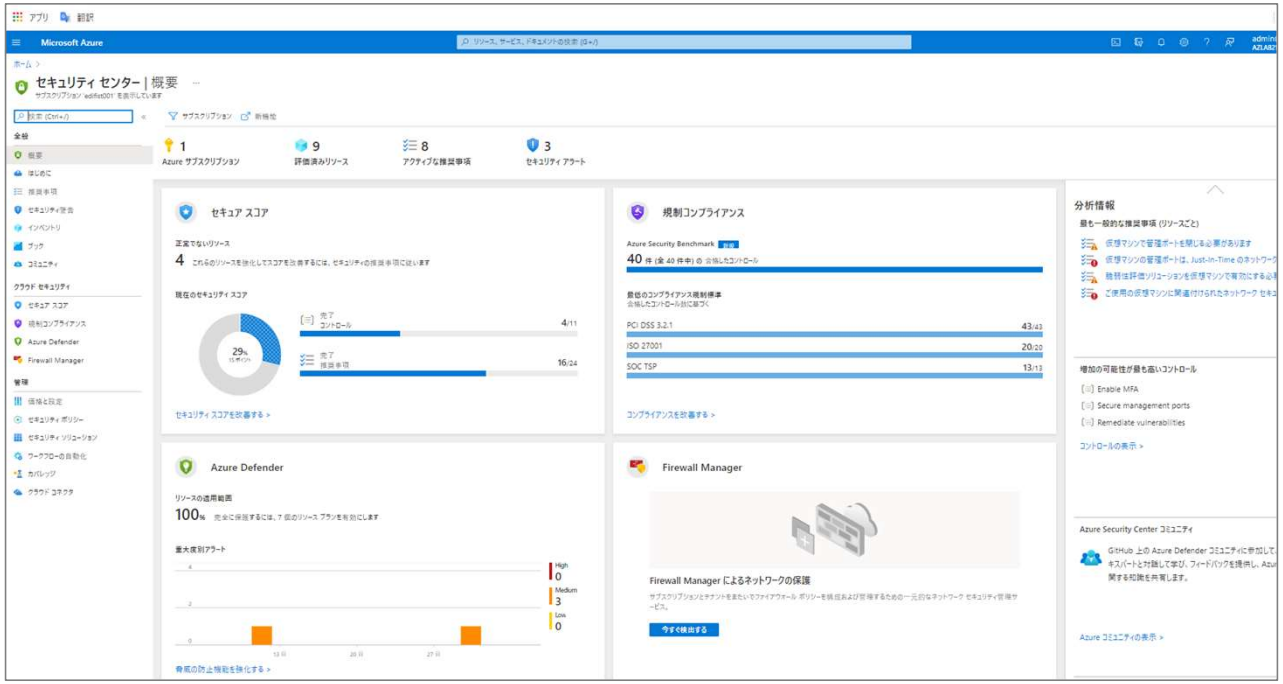


SC-900 Microsoft Security,
Compliance, and Identity Fundamentals

4.2 Azureのセキュリティ管理機能について説明する

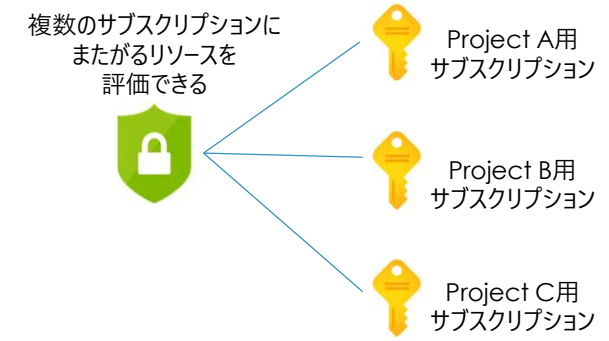
Azure Security Centerとは

- Azureのリソースとオンプレミスの物理サーバー/仮想マシンのセキュリティログを収集し、Microsoftの機械学習を使って脅威を検出、アクションの推奨を行います。



Point

複数のサブスクリプションにあるリソースを横断的に評価できます。



Azure Security Centerのセキュアスコア

- Azure Security Center には、主に2つの目標があります。
  - 現在のセキュリティ状況を把握すること
  - セキュリティを効率的かつ効果的に向上させること

現在のセキュリティ構成を
スコアで表示

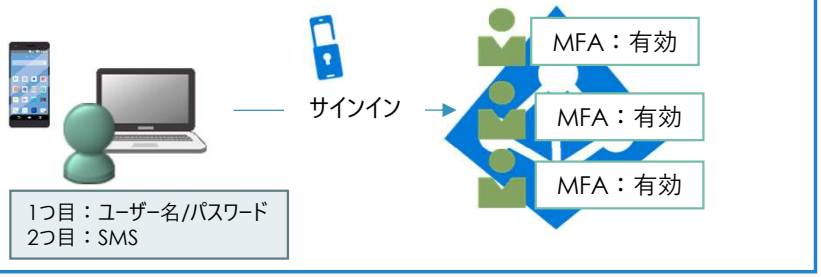
- ✓ セキュリティを強化するための推奨事項が表示される。
- ✓ 推奨内容を手動で実行することも推奨事項の項目にある[修正]オプションからも実行可能

主なセキュアスコアを上げるための項目

多要素認証(MFA)の有効化

10点 UP

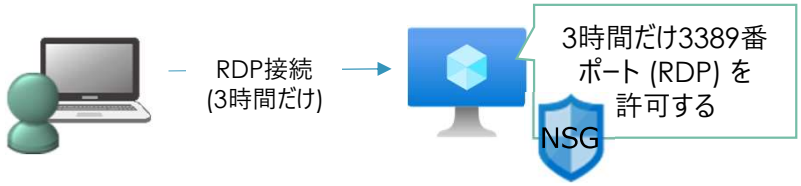
- ✓ 全ユーザーに多要素認証を有効にする。



管理ポートのセキュリティ保護

8点 UP

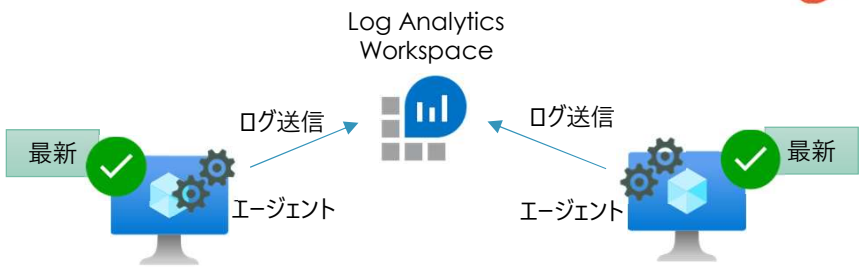
- ✓ Just-In-Time ネットワークアクセス制御によって、RDP/SSH接続が必要な時のみVMのポートを許可する。



システム更新プログラムの適用

6点 UP

- ✓ 仮想マシンに更新プログラムを適用する



脆弱性の修復

6点 UP

- ✓ 脆弱性評価ソリューションをVMで有効化する
- ✓ ソフトウェアとセキュリティの構成の誤りを可視化し、軽減のための推奨事項を提示する。

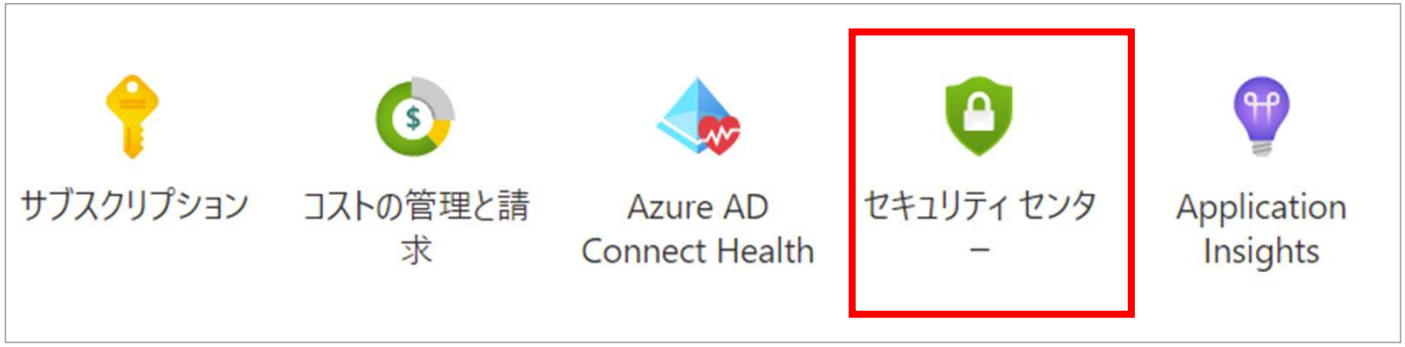
Exam Point

Azureのセキュアスコアを表示するツールはどれですか？

	選択肢
A	サブスクリプション
B	Security Center
C	Application Insights
D	コストの管理と請求
E	Azure AD Connect Health

解答：B

- セキュアスコアを表示できるのは、Azure Security Centerです。



Exam Point

次の各ステートメントについて、ステートメントが真の場合は、「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。

①MFAを有効にすると、Azure Security Centerの組織のセキュアスコアが向上します。

②システムアップデートを適用することは、Azure Security Centerで組織のセキュアスコアを上げます。

③Azure Security Centerのセキュアスコアは、複数のAzureサブスクリプションにまたがるリソースを評価できます。

解答：以下を参照

①MFAを有効にすると、Azure Security Centerの組織のセキュアスコアが向上します。

はい　MFAを有効にすると、Azure Security Centerのセキュアスコアが10点上がります。

②システムアップデートを適用することは、Azure Security Centerで組織のセキュアスコアを上げます。

はい　仮想マシンにLog Analytics エージェントをインストールすると、Log Analytics Workspaceにログが送信され、更新プログラムが自動管理されます。推奨事項「システムの更新プログラムの適用」が適用されているとセキュアスコアが6点上がります。

③Azure Security Centerのセキュアスコアは、複数のAzureサブスクリプションにまたがるリソースを評価できます。

はい　Azure Security Centerは、複数のAzure サブスクリプションにまたがるリソースを評価できます。

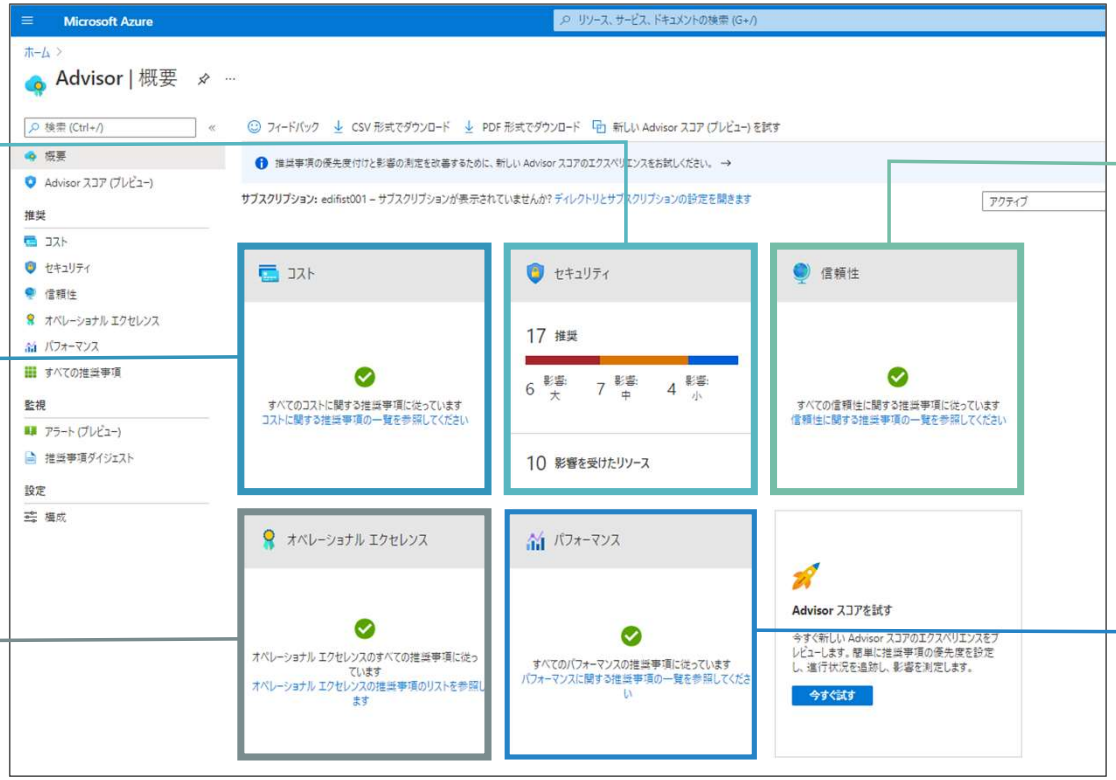
Azure Advisor

- リソースの構成と利用統計情報が分析され、5つの分野を改善するための アドバイスを提供してくれるサービスです。

セキュリティ
セキュリティ侵害に至る可能性がある脅威と脆弱性を検出します。

コスト
Azure 全体の支出を最適化し、削減します。

オペレーショナル エクセレンス
プロセスとワークフローの効率性、リソースの管理性、デプロイに関するベストプラクティスの実現を支援します。



信頼性
ビジネスに不可欠なアプリケーションの継続稼働を確保し、さらに向上させることができます。

パフォーマンス
アプリケーションの速度を向上させます。

Exam Point

Azure の推奨事項を表示するサービスは何ですか。

	選択肢
A	Azure Log Analytics
B	Azure Advisor
C	Azure Monitor
D	サブスクリプション

解答：B

- Azure Advisorは、5つのカテゴリーの項目を改善するためのアドバイス(推奨事項)を表示してくれるサービスです。

SC-900 Microsoft Security,
Compliance, and Identity Fundamentals

4.3
Azure Sentinelのセキュリティ機能について説明する

統合型の脅威対策ソリューション

Microsoftは、統合型の脅威対策ソリューションとして、以下を提供します。

- ✓ SIEM
- ✓ XDR

Azure Sentinelは

クラウドネイティブな

Point

SIEM + SOAR です！

SIEMとは

SIEMって何だろう ？

セキュリティ情報イベント管理

Security **I**nformation **E**vent **M**anagement

ネットワーク機器やサーバーなどの異なるソースからセキュリティ情報を収集し、
横断的に分析する「統合ログ管理」製品です。

SOARとは

SOARって何だろう ？

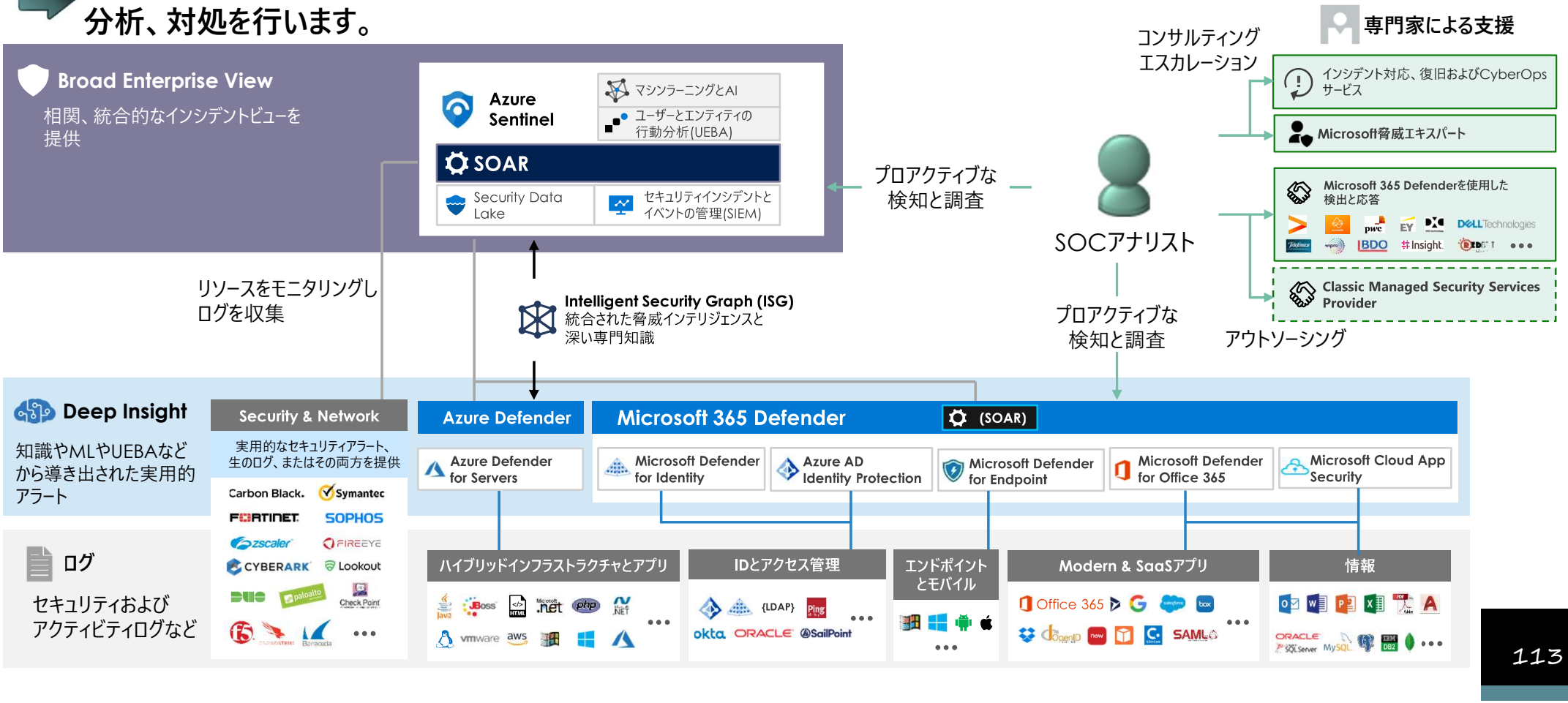
セキュリティ運用の自動化と対応

Security **O**rchestration, **A**utomation and **R**esponse

情報の収集と分析、優先順位の設定	インシデントに対する対応を自動化	関係各所への連絡や担当者のアサイン

マイクロソフトのサービスで実現するAzure Sentinelとの連携

さまざまなサービスを接続して、統合的にログを管理し、プロアクティブに脅威を検出し、分析、対処を行います。



Exam Point

Azure SentinelのXDR機能を提供する機能はどれですか。

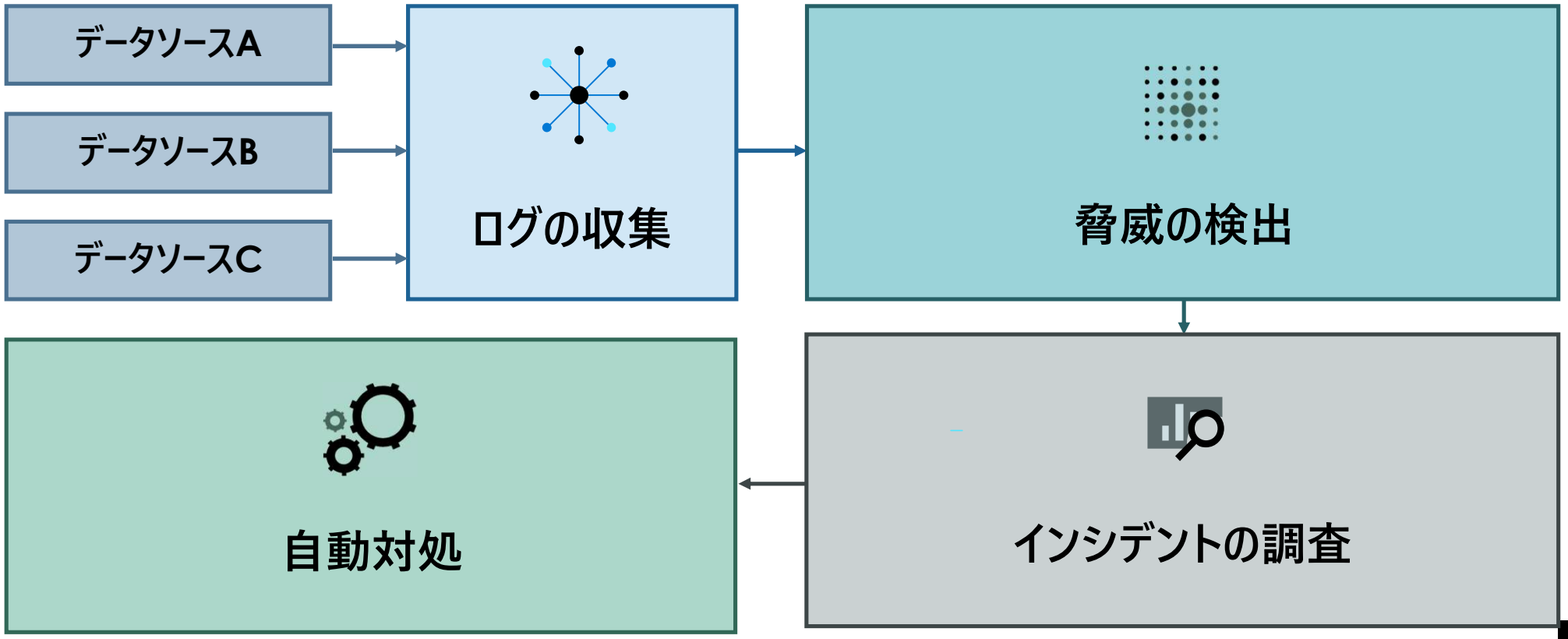
	選択肢
A	Microsoft 365 Defenderとの統合
B	Azure Monitorブックのサポート
C	Azure Application Insightsのサポート
D	Microsoft 365コンプライアンスセンターの統合

解答：A

Azure Sentinelは、Microsoft 365 Defenderと統合することで、Microsoft 365 DefenderのアラートをAzure Sentinelで検出し、分析や自動対処を行うことができます。

Azure Sentinelの全体像

Azure Sentinelの全体像を確認します。

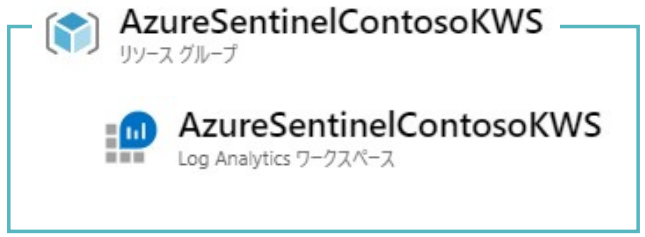


Azure Sentinelのオンボードの手順

ログの収集

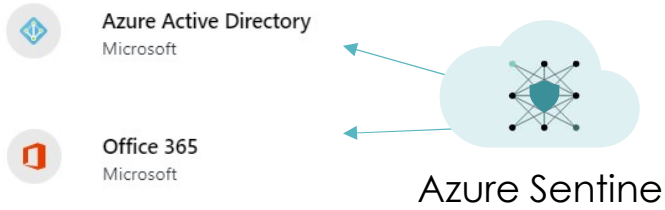
Azure Sentinelのオンボードは、次のプロセスで行います。

Step1：ワークスペースの作成



Azure Sentinelで使用する
Log Analyticsワークスペースを作成します。

Step2：データソースの接続

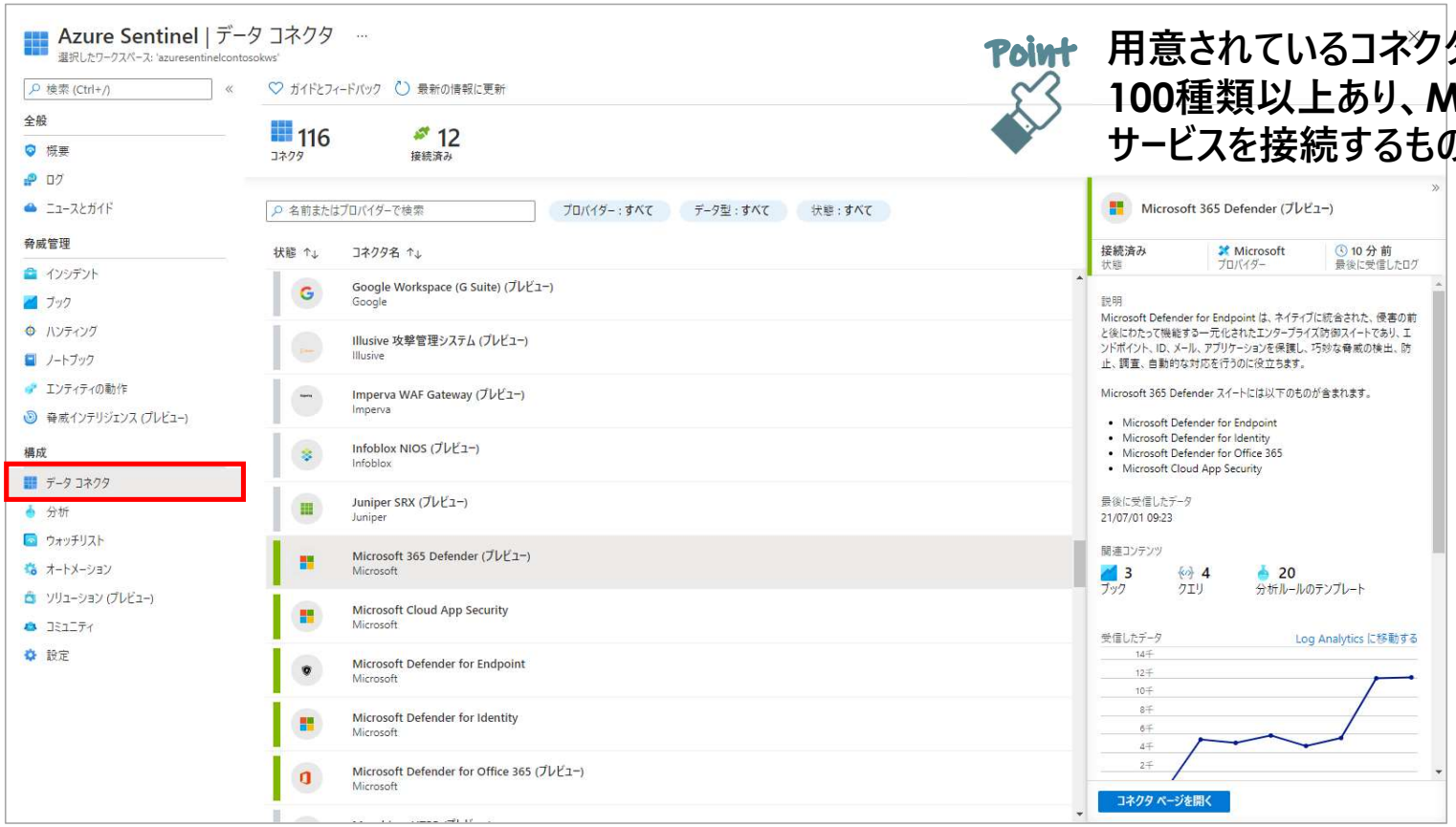


必要なデータソースに接続します。

簡単な手順ですぐに利用できます。

コネクタを使用したデータ接続

Azure Sentinelを使用してログを分析する最も簡単な方法は、データコネクタを使用してデータソースを接続することです。



Point

用意されているコネクタは、
100種類以上あり、Microsoft以外の
サービスを接続するものも数多くあります。

Exam Point

Azure Sentinelと別のセキュリティ ソースとの間で、リアルタイムの統合を提供するために何を使用しますか。

	選択肢
A	Azure AD Connect
B	Log Analytics Workspace
C	Azure Information Protection
D	コネクタ

解答：D

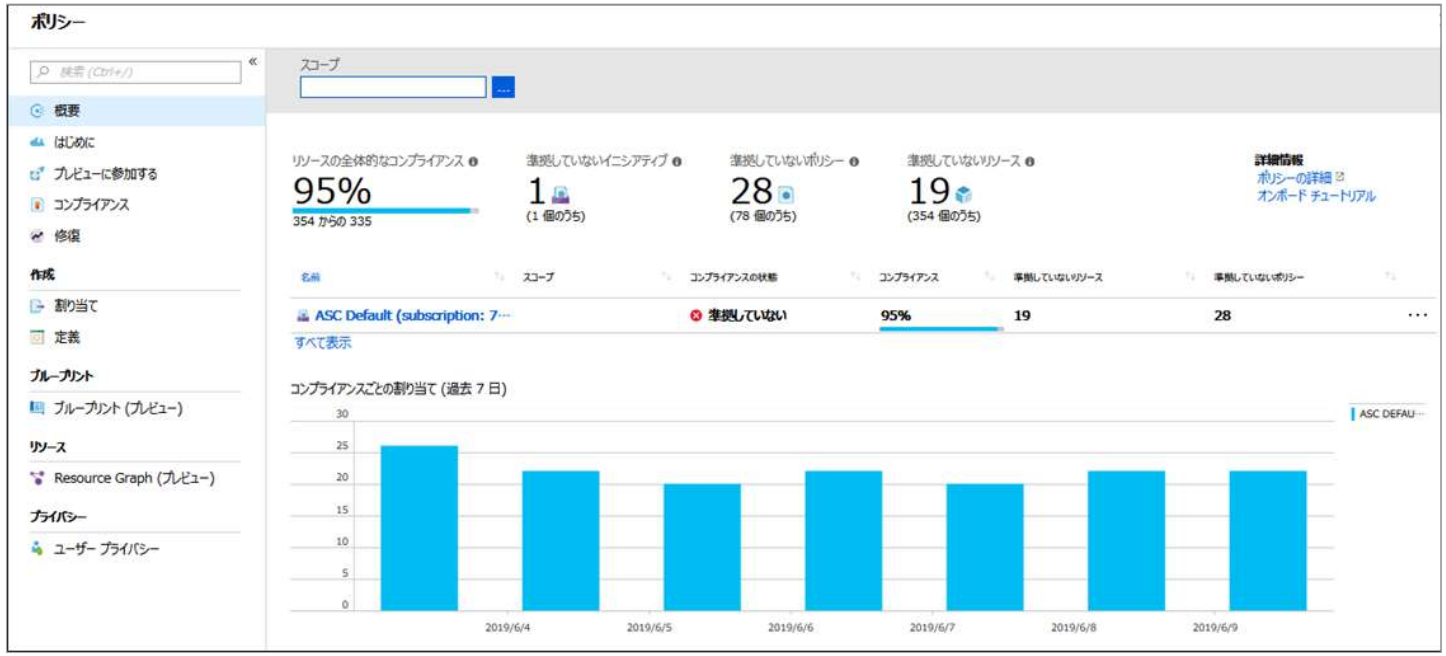
Azure Sentinelは、さまざまなデータソースと接続するために、データコネクタを使用します。

SC-900 Microsoft Security,
Compliance, and Identity Fundamentals

4.4 Azureのリソースガバナンス機能について説明する

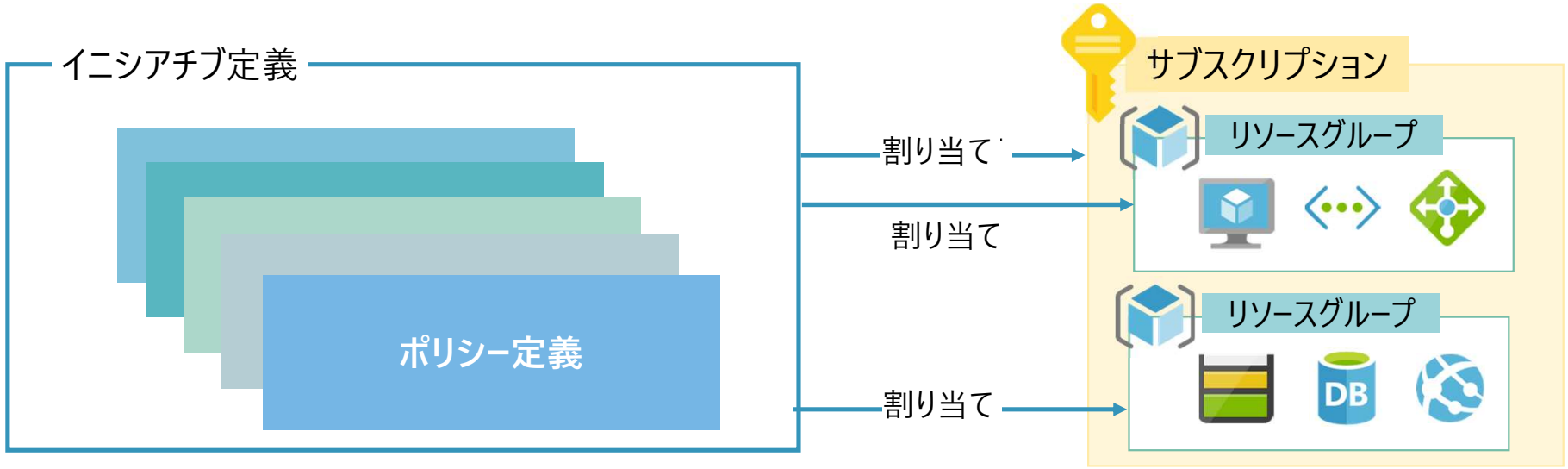
Azure Policy

- Azure Policyは、ITガバナンスを実現するためのサービスです。
  - リアルタイムのポリシーの評価と強制が行われます。
  - リソースの自動修復機能を使用して、問題を迅速かつ効果的に解決することも可能です。



Azure Policyのオブジェクト

- ポリシー定義またはイニシアチブ定義を次のスコープに割り当てます。
  - 管理グループ(複数のサブスクリプションを束ねる論理コンテナー)
  - サブスクリプション
  - リソースグループ

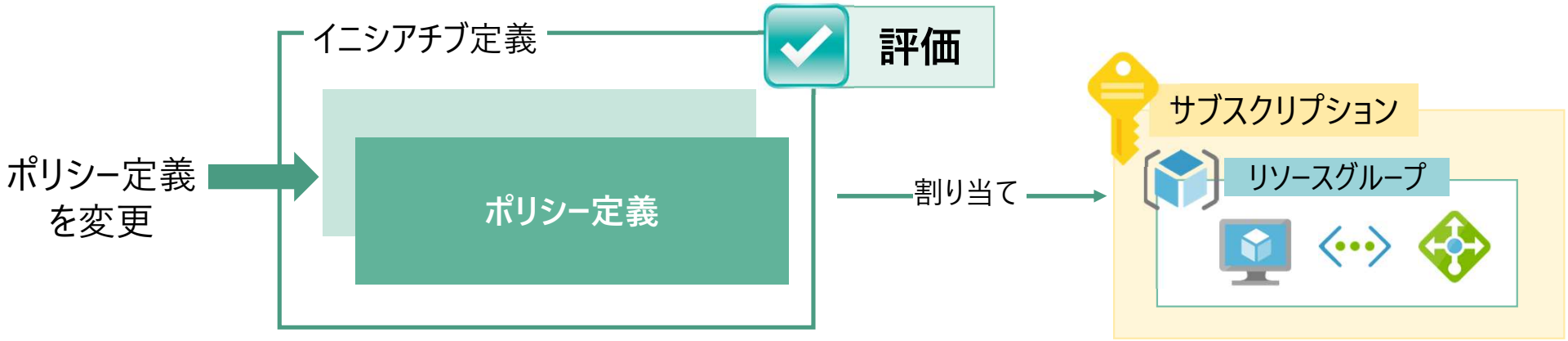


Point

イニシアチブ定義とは、複数のポリシー定義をグループ化するものです。
グループを単一の項目として操作するので、割り当てと管理がシンプルになります。

Azure Policyの評価のタイミング

- Azure Policyは、次のイベントまたはタイミングによって評価がトリガーされます。
  - リソースが、ポリシー割り当てのスコープ内で作成、削除、または更新される。
  - ポリシーまたはイニシアティブがスコープに新たに割り当てられる。
  - スコープに割り当てられているポリシーまたはイニシアティブが更新される。
  - 標準コンプライアンス評価サイクル(24時間ごとに実行)



Exam Point

次の各ステートメントについて、ステートメントが真の場合は、「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。

①Azureポリシーは自動修復をサポートします。

②データが特定のデータ保護基準に準拠しているかどうかを評価できます。

③Compliance評価は、対象となるリソースが作成されたとき、または変更された時にのみ行われます。

解答：以下を参照

①Azureポリシーは自動修復をサポートします。

はい　Azure Policyは、自動修復をサポートしています。

②データが特定のデータ保護基準に準拠しているかどうかを評価できます。

はい　Azure Policyは、ポリシーに準拠しているかどうかを評価します。

③Compliance評価は、対象となるリソースが作成されたとき、または変更された時にのみ行われます。

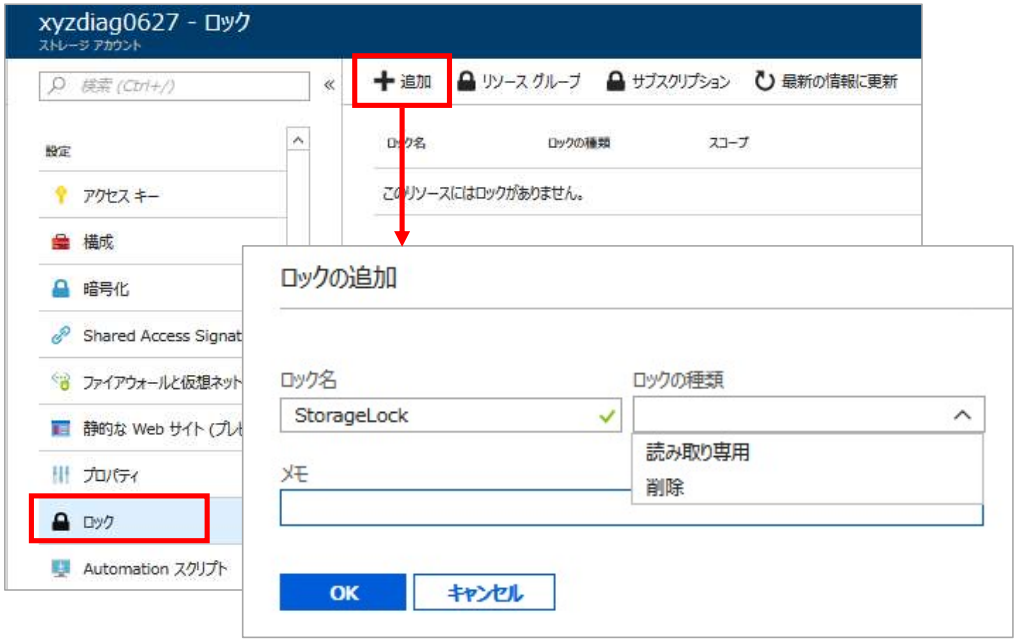
いいえ　Azure Policyは特定のタイミングで評価されます。

- ✓ リソースがポリシー割り当てのスコープ内で作成、更新、削除される
- ✓ ポリシーまたはイニシアティブがスコープに新たに割り当てられる
- ✓ ポリシーまたはイニシアティブが更新される
- ✓ 標準のコンプライアンス評価サイクルで、24時間ごとに実行される

リソースロック

- サブスクリプション、リソース グループ、および リソースをロックすることで、組織のユーザーが誤って重要なリソースを削除したり変更したりすることを防止できます。

- 2つのロックレベル
  - **削除(CanNotDelete)**
    - ユーザーは、リソースの読み取りと更新は実行できますが、削除は実行できません。
  - **読み取り専用(ReadOnly)**
    - ユーザーは、リソースの読み取りを実行できますが、リソースの更新や削除は実行できません。



Exam Point

次の各ステートメントについて、ステートメントが真の場合は、「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。

①Azureサブスクリプションに、リソースロックを設定できます。

②リソースロックは、リソースに対して1つだけ作成できます。

③リソースロックが適用されたリソースが入っているリソースグループを削除できます。

解答：以下を参照

①Azureサブスクリプションに、リソースロックを設定できます。

はい　リソースロックは、サブスクリプション、リソースグループ、リソースに作成できます。

②リソースロックは、リソースに対して1つだけ作成できます。

いいえ　リソースロックは、1つのスコープあたり最大20個まで作成できます。

③リソースロックが適用されたリソースが入っているリソースグループを削除できます。

いいえ　リソースにロックを適用すると、リソースグループもロックがかかり削除できなくなります。

AzureのMicrosoftクラウド導入フレームワークとは

- AzureのMicrosoftクラウド導入フレームワークには、Microsoftの従業員、パートナー、顧客からのクラウド導入のベストプラクティスがまとめられています。
- クラウドの導入作業に役立つ一連のツール、ガイダンス、体験談が提供されます。

戦略	業務上の正当な理由と導入による予想される結果を定義する
計画	ビジネスの結果に合わせて実行可能な導入計画を調整する
準備完了	計画された変更のためにクラウド環境を準備する
移行	既存のワークロードを移行して最新化する
イノベーション	新しいクラウドネイティブソリューションまたはハイブリッドソリューションを開発する
ガバナンス	環境とワークロードを管理する
管理	クラウドソリューションおよびハイブリッドソリューションのための運用管理
整理	組織のクラウド導入作業をサポートするチームと役割を連携させます

Exam Point

次のステートメントを完成させてください。
[①]は、Microsoftの従業員、パートナー、および顧客からのベストプラクティスを提供します。
これには、Azure展開における支援のためのツールとガイダンスが含まれます。

	選択肢
A	Azureのマイクロソフトクラウド導入フレームワーク
B	Azure Policy
C	Azure Blueprint
D	リソースロック

解答：A

- AzureのMicrosoftクラウド導入フレームワークには、Microsoftの従業員、パートナー、顧客からのクラウド導入のベストプラクティスがまとめられています。
- クラウドの導入作業に役立つ一連のツール、ガイダンス、体験談が提供されます。

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Microsoft 365のセキュリティとコンプライアンス ソリューション

5

SC-900 Microsoft Security,
Compliance, and Identity Fundamentals

5.1
Microsoft 365 Defenderによる脅威保護について説明する

Microsoft 365 Defender

Microsoft 365 Defenderは、Microsoft 365テナントのID、エンドポイント、クラウドアプリ、メールやドキュメントを保護します。

ID

Azure Active Directory

Microsoft Defender for Identity

エンドポイント

Microsoft Defender for Endpoint

クラウドアプリ

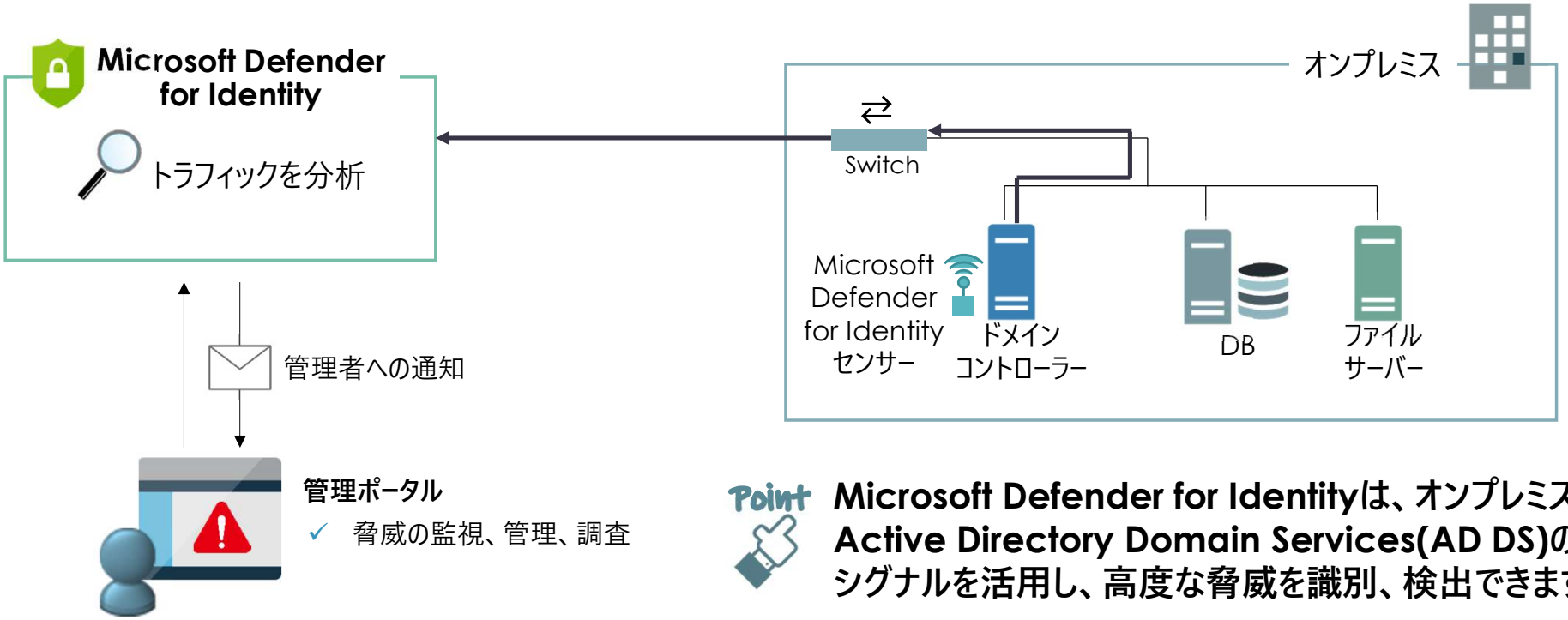
Microsoft Cloud App Security

メールとドキュメント

Microsoft Defender for Office 365

Microsoft Defender for Identity

Windows Server Active Directoryへの資格情報を狙った攻撃を検知するクラウドベースのサービスです。



Point **Microsoft Defender for Identityは、オンプレミスのActive Directory Domain Services(AD DS)のシグナルを活用し、高度な脅威を識別、検出できます。**

Exam Point

次のステートメントを完了させてください。

[①]は、オンプレミスのActive Directoryの信号を活用して高度な脅威を識別、検出、調査するクラウドベースのソリューションです。

	選択肢
A	Microsoft Cloud App Security
B	Microsoft Defender for Endpoint
C	Microsoft Defender for Identity
D	Microsoft Defender for Office 365

解答：C

Microsoft Defender for Identityは、オンプレミスのAD DSのシグナルから脅威を検出するクラウドベースのサービスです。

Microsoft Defender for Endpoint

Microsoft Defender for Endpointは、予防保護、侵害後の検出、自動調査、および対応のためのクラウドベース統合プラットフォームで、次の機能をサポートします。

1.脅威と脆弱性の管理

センサーに基づいてエンドポイントのリアルタイムな脆弱性と構成ミスを検出し、シームレスな修復を行います。

2.攻撃表面の縮小

Point

脅威や攻撃に対して脆弱になる場所を最小限に抑えることで、攻撃面を減らします。

3.次世代の保護

コンピューターの学習、大規模なデータ分析、詳細な脅威抵抗調査、クラウドインフラストラクチャを通じて、企業組織のデバイスを保護します。

4.エンドポイントの検出および応答

リアルタイムかつ実用的な高度な攻撃を検出しアラートを作成します。

5.自動調査と修復

Point

自動化された調査と修復機能を使用して、個別に調査する必要があるアラートの量を大幅に削減します。

6.Microsoft脅威エキスパート

セキュリティオペレーションセンター(SOC)に専門家レベルの監視と分析を提供するサービスです。独自の環境での重大な脅威を逃さないようにします。

Exam Point

Microsoft Defender for Endpointの2つの機能は何ですかか。

選択肢	
A	自動調査と修復
B	転送の暗号化
C	シャドウITの検出
D	攻撃の回避

解答：A、D

Microsoft Defender for Endpointの機能として正しいのは、自動調査と修復、攻撃表面の縮小(攻撃の回避)です。

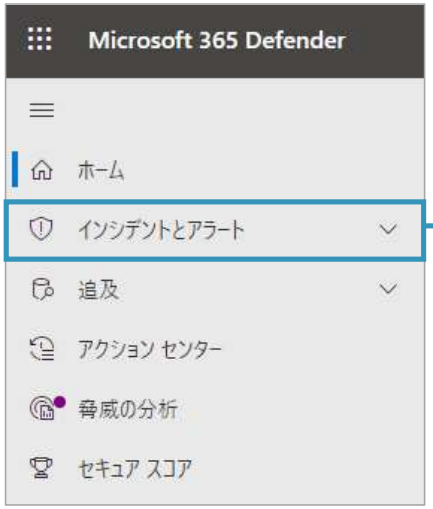
SC-900 Microsoft Security,
Compliance, and Identity Fundamentals

5.2
Microsoft 365のセキュリティ管理機能について説明する

Microsoft 365セキュリティセンター(Microsoft 365 Defender)

Microsoft 365セキュリティセンターは、検出された脅威を確認したり、詳細な分析を行ったり、自動的に対応をすることができます。

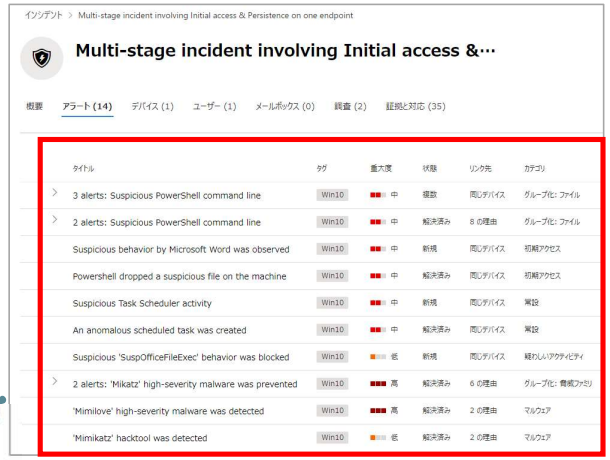
Microsoft 365セキュリティセンターによる脅威の検出と対応



インシデントとアラート

疑わしいイベントや悪意のあるイベントやアクティビティを検出するとアラートを作成します。
個々のアラートは、攻撃に関する貴重な手がかりを提供しますが、攻撃は通常、デバイス、ユーザー、メールボックスなど、さまざまな種類のエンティティに対してさまざまな手法で行われます。
結果、テナント内の複数のエンティティに対する複数のアラートが通知されます。
個々のアラートを組み合わせて攻撃に関する洞察を自身で行うと、困難で時間がかかりますが、Microsoft 365 Defenderは、自動的にアラートと関連情報をインシデントに集約します。

1つのインシデントを選択します。



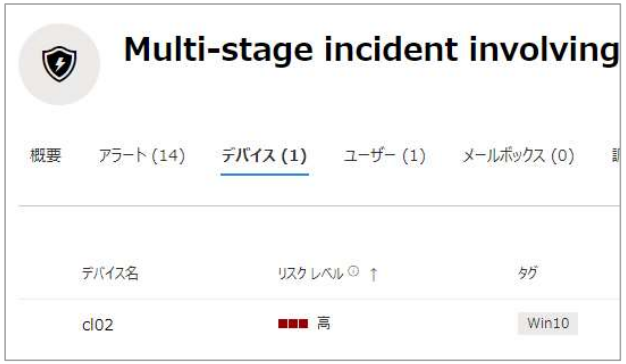
Point

関連付けられているアラートを表示できます。

[インシデント]ページ

[インシデント]ページでは、インシデントに関わったデバイス、ユーザー、メールボックス、ファイル、プロセスなどを表示することができます。

関連したユーザー



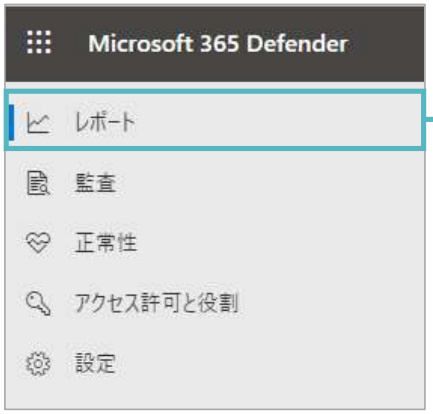
関連したデバイス

関連したファイル

Point

[インシデント]ページでは、アラートに関連したデバイスを表示できます。

Microsoft 365セキュリティセンターによる脅威の検出と対応



レポート

セキュリティ、エンドポイント、メールやコラボレーションなどさまざまなレポートを表示します。

Point

セキュリティレポートを表示すると、セキュリティの傾向を表示し、IDの保護状態を追跡することができます。

Exam Point

次のステートメントを完了させてください。

Microsoft 365セキュリティセンターの[①]を使用すると、セキュリティの傾向を表示し、IDの保護状態を追跡できます。

	選択肢
A	インシデント
B	ハンティング
C	攻撃シミュレーター
D	レポート

解答：D

Microsoft 365セキュリティセンターの[レポート]ページのセキュリティレポートでは、セキュリティの傾向に関する情報を表示し、ID、データ、デバイス、アプリ、インフラストラクチャの保護の状態を追跡することができます。

SC-900 Microsoft Security,
Compliance, and Identity Fundamentals

5.3
Microsoft Intuneを使用したエンドポイントセキュリティについて説明する

マイクロソフトのMDM製品

Microsoft Intune

- Microsoft Intuneでは次の2種類の管理を行います。
  - MDM(モバイルデバイス管理)
    - デバイスを登録して使用
    - 登録されたデバイスを一元管理
    - セキュリティ設定の強制や準拠の確認

  - MAM(モバイルアプリケーション管理)
    - デバイス上の基幹業務アプリの管理や保護を提供
    - 基幹業務アプリから作成されたデータを保護

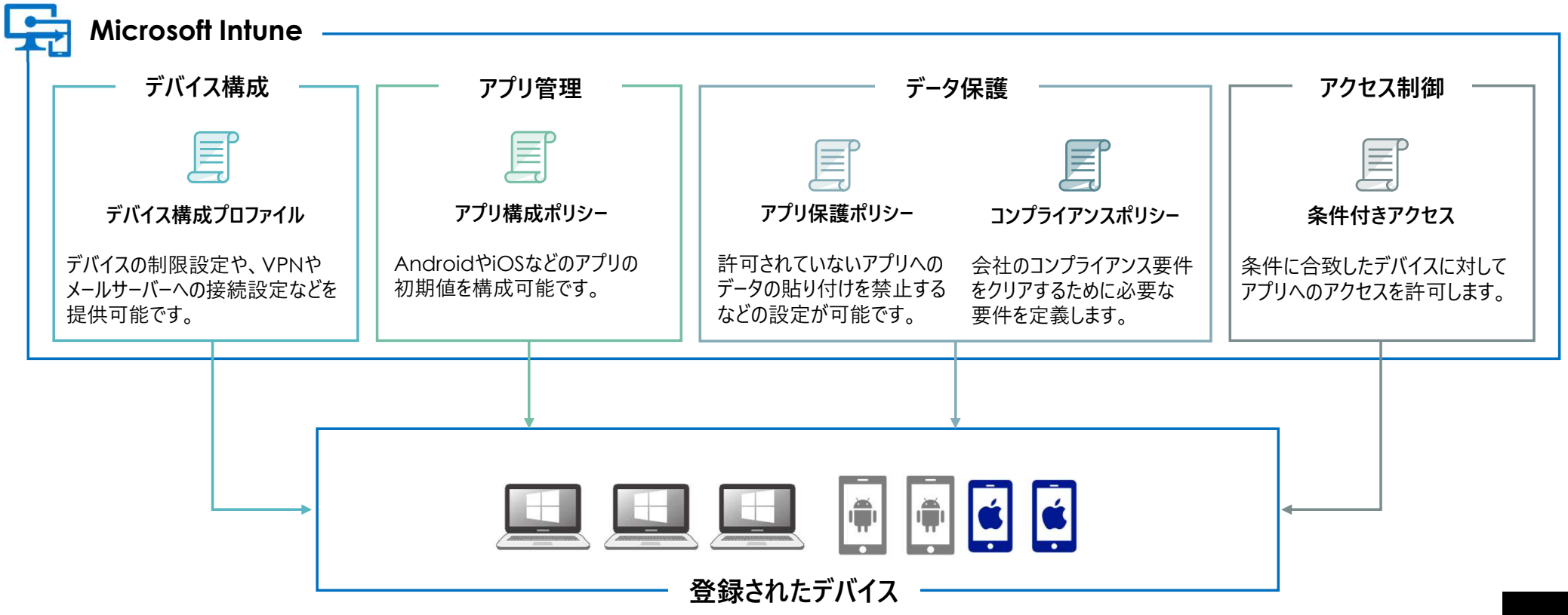
Microsoft Intune

Point

Microsoft Intuneを管理するツールは、Microsoft Endpoint Manager admin centerです。

Microsoft Intuneで構成可能なポリシー

Microsoft Intuneでは、次のポリシーが構成可能です。



Exam Point

Microsoft Intuneの管理ツールは何ですか。

	選択肢
A	Microsoft 365セキュリティセンター
B	Microsoft 365コンプライアンスセンター
C	Microsoft Endpoint Manager admin center
D	Azure AD管理センター

解答：C

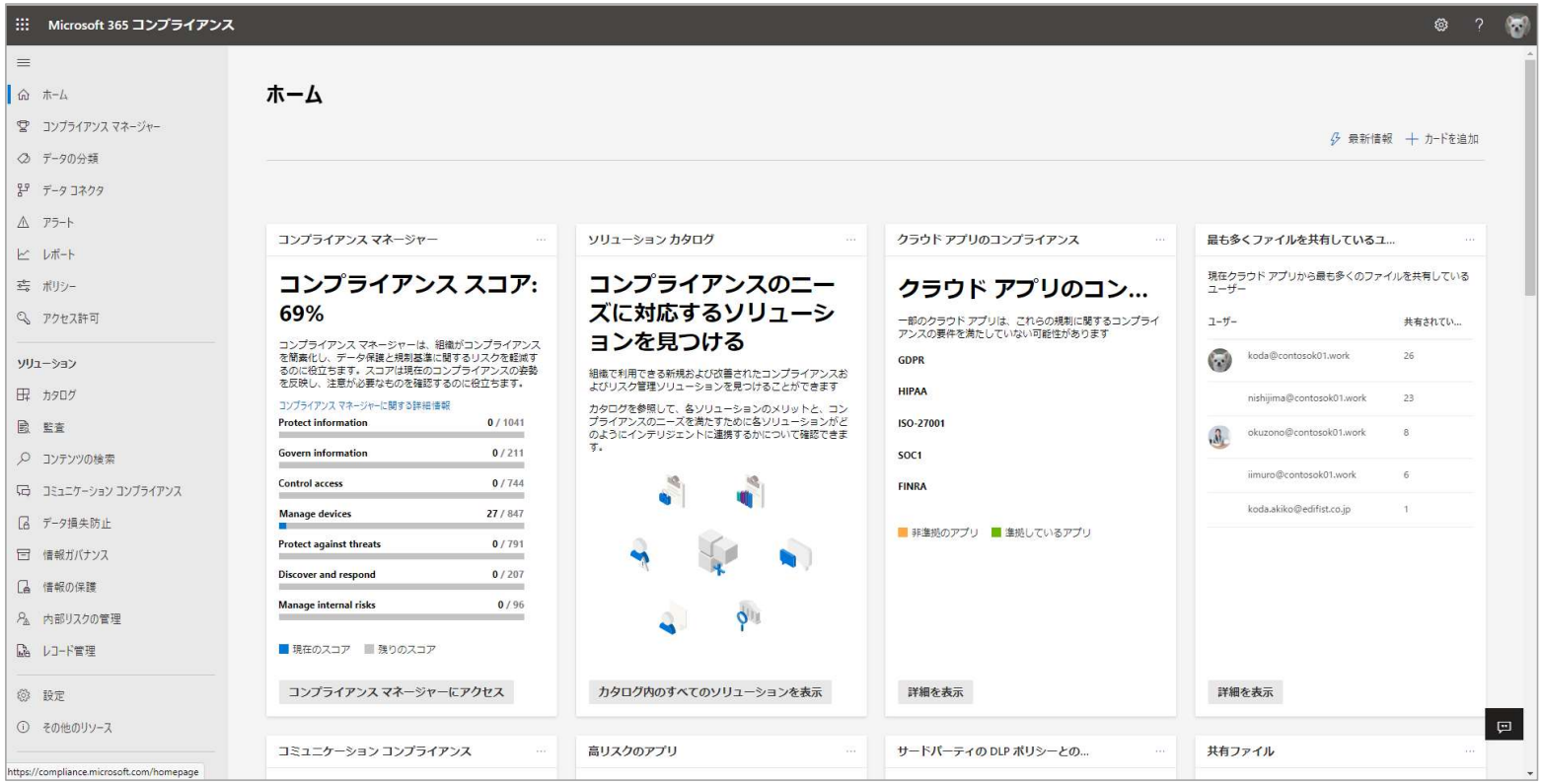
Microsoft Intuneの管理ツールは、Microsoft Endpoint Manager admin centerです。

SC-900 Microsoft Security,
Compliance, and Identity Fundamentals

5.4 Microsoftのコンプライアンス管理機能を説明する

コンプライアンス機能を管理するツール

Microsoft 365コンプライアンスセンターで、さまざまなコンプライアンス機能を管理することができます。



Point

Microsoft 365コンプライアンスセンターでは、情報保護、情報ガバナンス、データ損失防止などの設定を管理することができます。

Exam Point

情報保護、情報ガバナンス、データ損失防止などの機能を管理することができるツールは次のうちどれですか。

	選択肢
A	Microsoft 365セキュリティセンター
B	Azure AD管理センター
C	コンプライアンスマネージャー
D	Microsoft 365コンプライアンスセンター

解答：D

情報保護、情報ガバナンス、データ損失防止などの機能を管理できるのは、Microsoft 365管理センターです。

コンプライアンスマネージャー

Microsoftのクラウドサービスに関連する規制コンプライアンスアクティビティを管理するための、ワークフローベースのリスク評価ツールで、Microsoft 365コンプライアンスセンターから確認することができます。

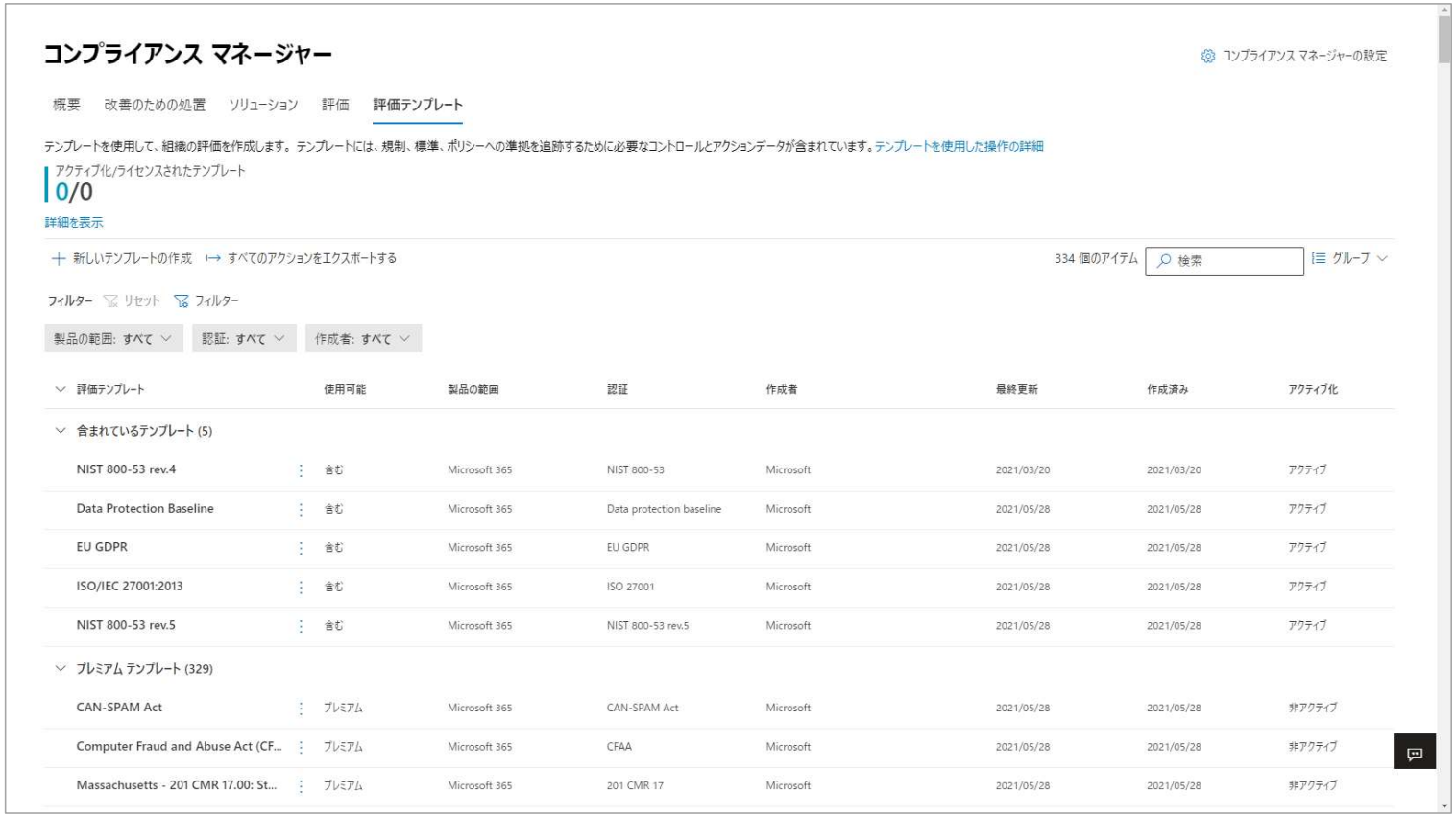
- ✓ **Microsoftとユーザー企業側のコンプライアンススコアが確認できます。**
- ✓ ユーザー企業側で不足している設定がある場合、内容を確認し、設定を行うことでスコアを上げることができます。
- ✓ **コンプライアンスマネージャーは、Microsoft 365テナントを自動的にスキャンしてシステム設定を検出し、継続的に更新します。**

コンプライアンスマネージャーは、データ保護および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確認、実装する際の組織の進捗状況を測定します。

評価テンプレート

コンプライアンスマネージャーでは、さまざまな評価テンプレートが用意され、さまざまな標準や規制に準拠しているかを確認することができます。

Point



Exam Point

次の各ステートメントについて、ステートメントが真の場合は、「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。

①コンプライアンスマネージャーは、顧客が管理するコントロールのみを追跡します。

②コンプライアンスマネージャーは、評価を作成するための事前定義されたテンプレートを提供します。

③コンプライアンスマネージャーは、データが特定のデータ保護基準に準拠しているかどうかを評価するのに役立ちます。

解答：以下を参照

①コンプライアンスマネージャーは、顧客が管理するコントロールのみを追跡します。

いいえ コンプライアンスに関するコントロールは、顧客とMicrosoftが行います。
Microsoftが管理するコントロールも追跡され、コンプライアンススコアとして表示されます。

②コンプライアンスマネージャーは、評価を作成するための事前定義されたテンプレートを提供します。

はい NISTやGDPRなどさまざまな事前定義されたテンプレートを使用することができます。

③コンプライアンスマネージャーは、データが特定のデータ保護基準に準拠しているかどうかを評価するのに役立ちます。

はい 事前定義されたテンプレートを使用し、規制や標準に準拠しているかを評価できます。

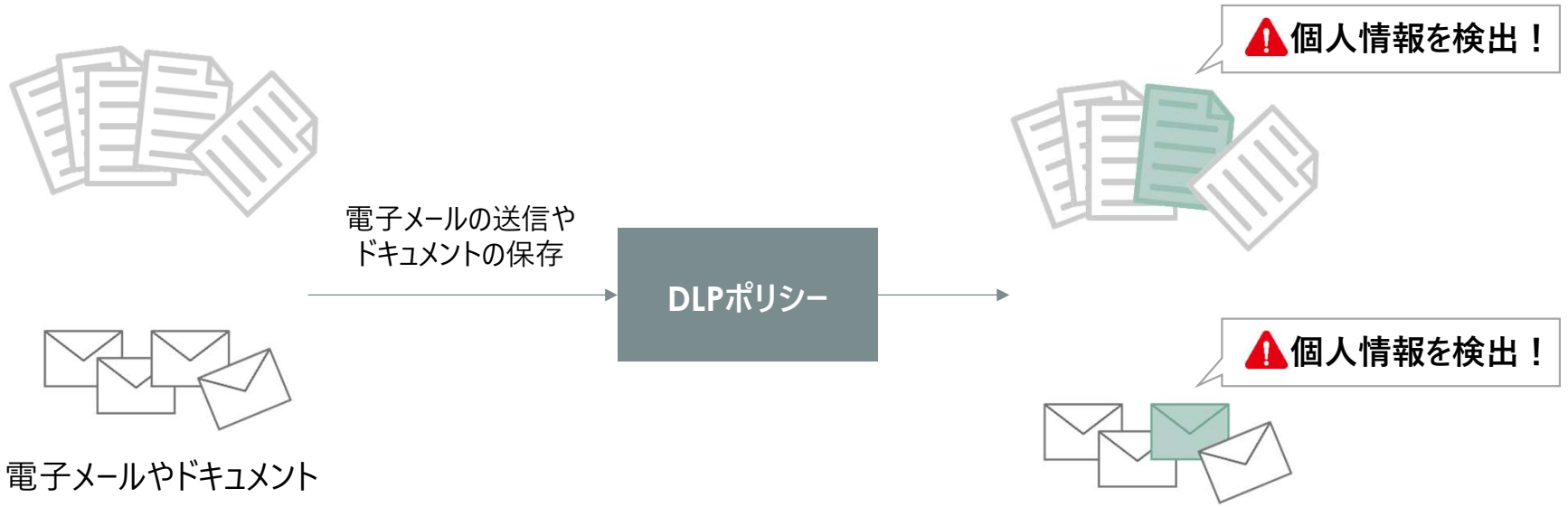
SC-900 Microsoft Security,
Compliance, and Identity Fundamentals

5.5
Microsoft 365の情報保護およびガバナンス機能について説明する

データ損失防止(DLP)

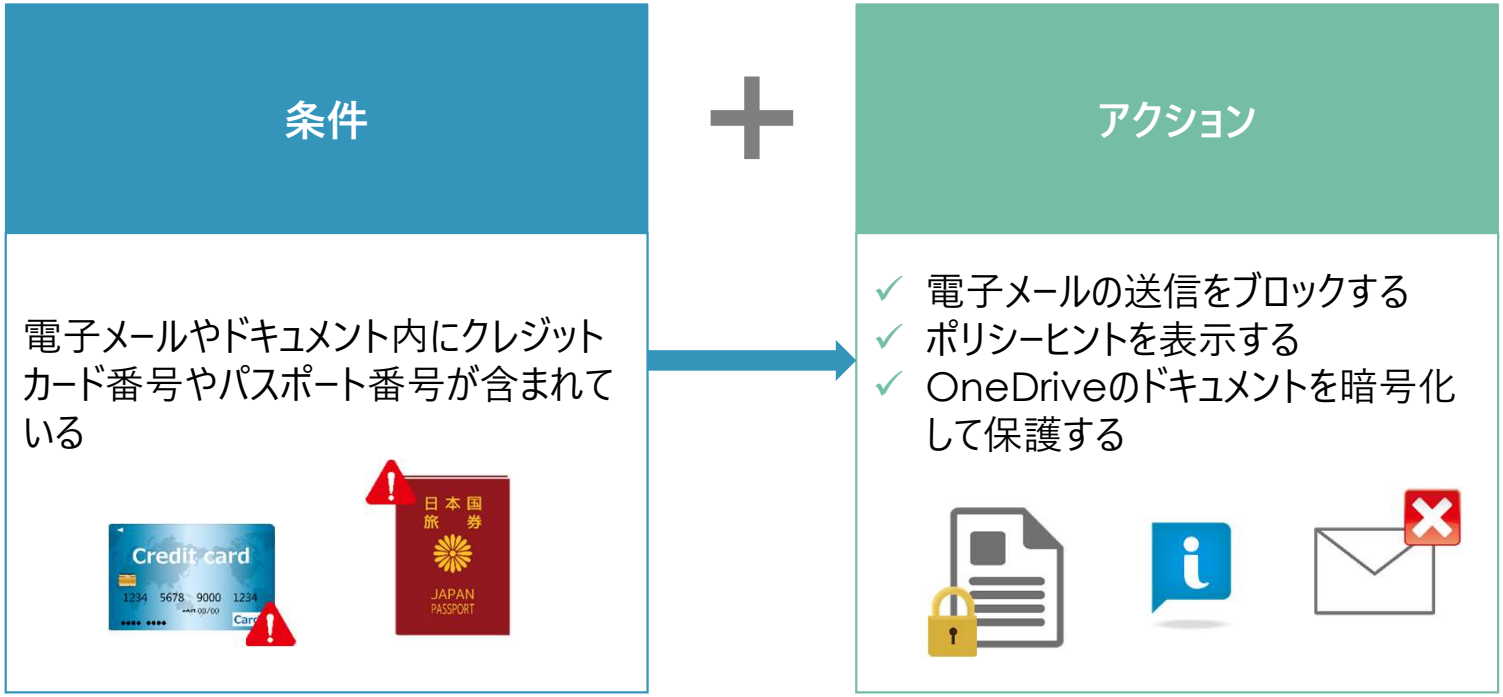
DLP機能を実装すると、ドキュメントやメールに含まれるPII情報を検出して個人情報の流出を防ぐことができます。

PII(Personally Identifiable Information)とは個人を特定できる情報のことで、免許証やパスポート番号、クレジットカード番号などが該当します。



DLPポリシーの構成

DLPポリシーは、次の2つで構成されます。

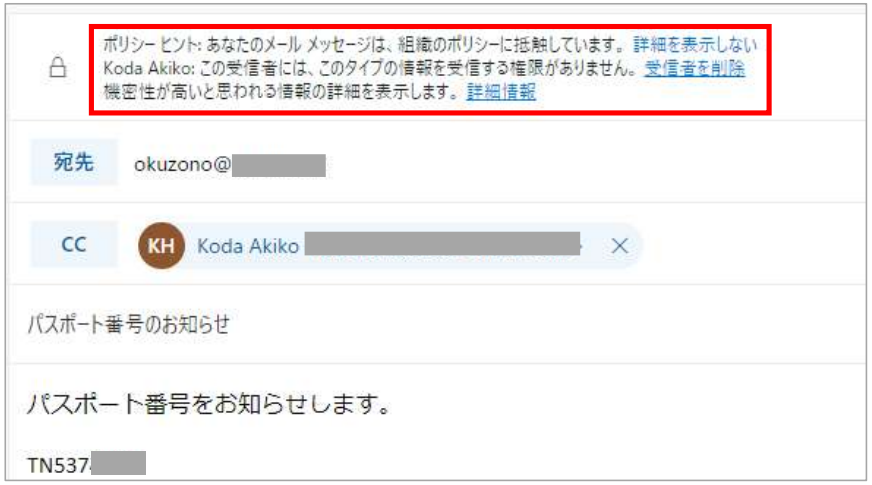


Point

クレジットカード情報を電子メールで送信しようとした場合にブロックされるように構成するには、DLP(データ損失防止)を使用します。

ポリシーヒント

DLPポリシーで定義した条件に抵触する場合、ポリシーヒントが表示されるよう構成されていると ドキュメントや電子メールにヒントが表示されます。



電子メールのポリシーヒント

Officeアプリケーションのポリシーヒント

Exam Point

Microsoft 365でデータ損失防止(DLP)ポリシーを使用して実装できるタスクはどれですか。2つ選択してください。

	選択肢
A	組織のポリシーに違反するユーザーにポリシーヒントを表示します。
B	エンドポイントのデバイスを暗号化します。
C	機密情報を含むOneDriveのドキュメントを保護します。
D	セキュリティベースラインをデバイスに適用します。

解答：A、C

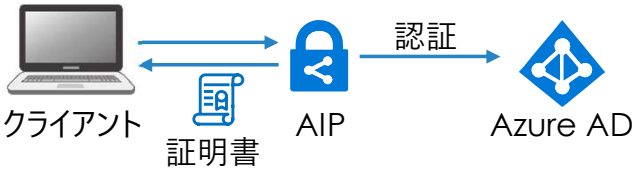
データ損失防止ポリシーを利用すると、個人情報などが検出された場合に、電子メールの送信をブロックしたり、ポリシーヒントを表示したり、OneDriveやSharePoint内のドキュメントを暗号化したりすることができます。

Azure Information Protection

企業の重要な情報を守り、適切に管理するためのソリューションです。

認証

- ✓ クライアントの資格情報は、Azure ADによって認証されます。
- ✓ 認証後は、AIPによって証明書が発行されます。

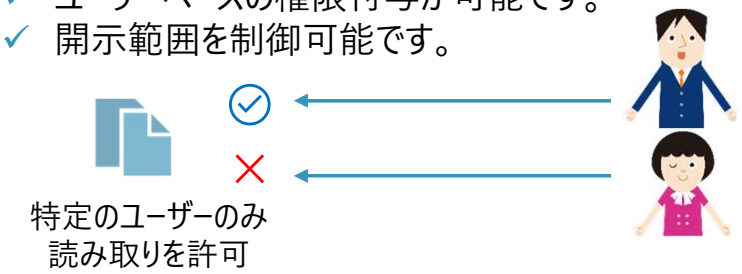


ラベルによる分類と暗号化

- ✓ ラベルを適用することでドキュメントやメールの保護が可能です。
- ✓ ラベルの自動適用が行えます。
- ✓ データの保存場所にかかわらず保護されます。

権限の制御

- ✓ ユーザーベースの権限付与が可能です。
- ✓ 開示範囲を制御可能です。



追跡と対処

- ✓ ドキュメントのアクセスを追跡できます。
- ✓ 不正アクセスが発覚した場合権限をはく奪できます。

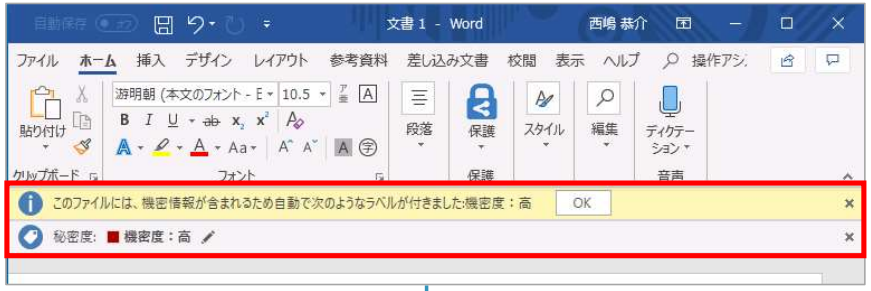
Azure Information Protectionによるラベリング

手動でラベリング

管理者があらかじめ定義したラベルをクリックすることで
適用できます。

自動でラベリング

ドキュメントに含まれている内容に応じて自動的にラベルを
適用できます。



DLP(データ損失防止)で定義されている機密情報(クレジットカード番号や免許証の番号など)が含まれている場合や、開発コードなど企業特有の機密情報が含まれている場合などに、
自動的にラベルを適用することができます。

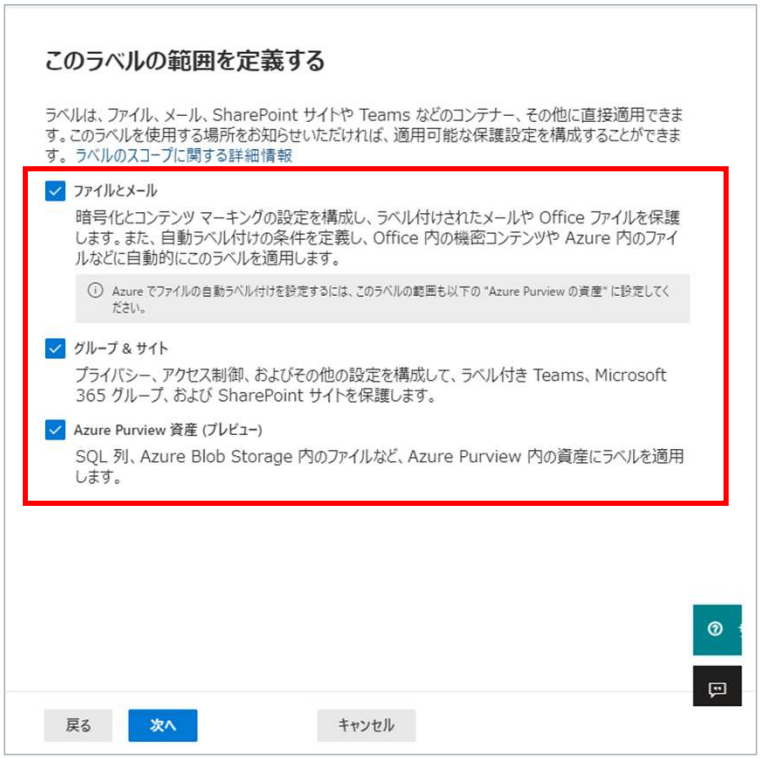
組み込みの情報およびカスタムの情報を指定できます。

ラベルに含められる情報

ラベルには、次の情報を含めることができます。

- ✓ **ドキュメントやメールに対するアクセス許可の設定**
  ユーザーなどに対してアクセス許可の設定を行います。
- ✓ **視覚的なマーキング**
  ヘッダー、フッター、透かしなどを挿入します。
- ✓ **自動適用される場合の条件**
  DLPポリシーやカスタムのキーワードなどを指定します。
- ✓ **自動適用/推奨適用**
  自動で適用するか、推奨として表示するかを指定します。

Step：秘密度ラベルの作成 -1



[ラベルに名前を付けてヒントを作成する]ページが表示されたことを確認し、ラベルの名前、ユーザー向けおよび管理者向けの説明を入力して、[次へ]ボタンをクリックします。

ラベルを適用する範囲を指定して、[次へ]ボタンをクリックします。

Step：秘密度ラベルの作成 -2

ラベル付けされたファイルやメールにどのような保護を適用するかを指定し、[次へ]をクリックします。

ラベル付けされたファイルやメールにどのような保護を適用するかを指定し、[次へ]をクリックします。

Exam Point

次の各ステートメントについて、ステートメントが真の場合は、「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。

①秘密度ラベルはドキュメントを暗号化するために使用できます。

②秘密度ラベルはドキュメントにヘッダーとフッターを追加できます。

③秘密度ラベルは電子メールに透かしを入れることができます。

解答：以下を参照

①秘密度ラベルはドキュメントを暗号化するために使用できます。

はい　秘密度ラベルには、アクセス制御の設定を含めることができます。
これによりデータが暗号化され、特定の人のみがアクセスできるようになります。

②秘密度ラベルはドキュメントにヘッダーとフッターを追加できます。

はい　秘密度ラベルが適用されているドキュメントに、カスタムヘッダー、フッター、透かしを追加できます。

③秘密度ラベルは電子メールに透かしを入れることができます。

いいえ　透かしを入れることができるのはドキュメントのみで、電子メールには適用されません。

Exam Point

特定の状態に基づいて自動的にコンテンツを暗号化できるMicrosoft 365コンプライアンスセンターの機能は何ですか。

	選択肢
A	電子情報開示
B	保持ポリシー
C	秘密度ラベル
D	コンテンツ検索

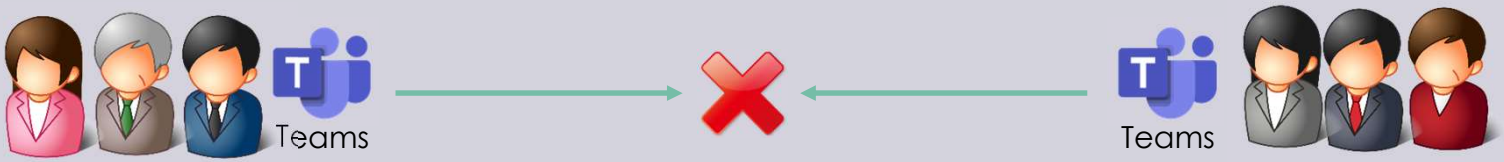
解答：C

- 秘密度ラベルによって、自動的にドキュメントやメールに暗号化したり、透かしなどを入れるできます。

SC-900 Microsoft Security,
Compliance, and Identity Fundamentals

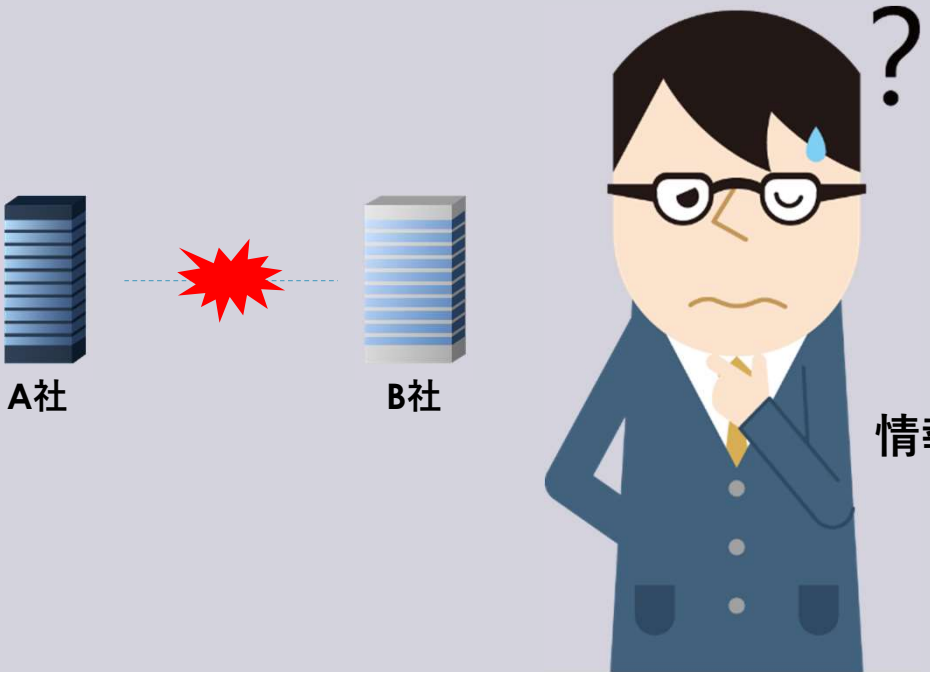
5.6
Microsoft 365の内部リスク機能について説明する

特定のチーム同士を通信させたくない



A社金融システム
開発チーム

B社金融システム
開発チーム



A社とB社はライバル同士なので、
情報漏洩を防ぐためチーム間通信をブロックしたい・・・・

Information Barriers

これで実現できます！

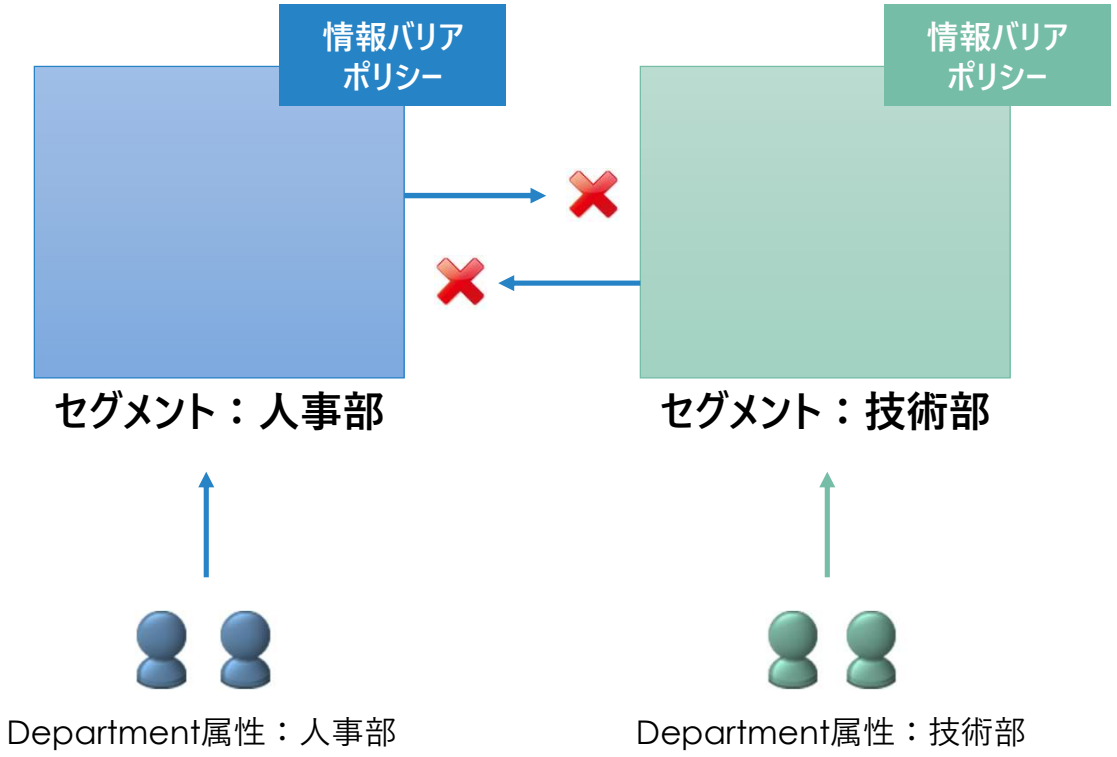
Information Barriers

Point

組織のグループ間の通信をブロックします！
試験では、「情報バリア」と表現される場合があります。

Information Barriersの構成イメージ

Information Barriersの構成イメージは次の通りです。



1. 通信をブロックしたい単位で
セグメントを構成します。

2. セグメント間でのTeams通信を
ブロックするために情報バリア
ポリシーを構成します。

3. 情報バリアポリシーを適用します。

Exam Point

次のステートメントを完了させてください。

[①]を使用すると、組織内のグループ間の通信を制御することができます。

	選択肢
A	カスタマーロックボックス
B	Azure AD Privileged Identity Management
C	情報バリア
D	条件付きアクセス

解答：C

Information Barriersを使用すると、組織内のグループ間の通信をブロックするなどの制御を行うことができます。

Exam Point

Microsoft 365で、情報バリアポリシーを実装する場合のユースケースは何ですか。

	選択肢
A	Microsoft 365への非三次元アクセスを制限します。
B	組織内の特定のグループ間で、Microsoft Teamsでのチャットを制限します。
C	組織内の特定のグループ間で、Exchange Onlineでの電子メールの送受信を制限します。
D	外部の電子メール受信者に対するデータ共有を制限します。

解答：B

Information Barriersは、Microsoft Teamsのチーム間の通信を制限したり、SharePointサイトやOneDriveへのアクセスを制限します。

SC-900 Microsoft Security,
Compliance, and Identity Fundamentals

5.7
Microsoft 365の電子情報開示機能について説明する

eDiscoveryとは

訴訟に関する資料を自らが収集し、開示する制度のことで、米国民事訴訟の手続きのひとつです。
米国民事訴訟手続きは、次のプロセスで行われます。

米国に拠点のある会社や米国企業と取引をする会社、ドル取引をする会社などが対象になるため、
米国に拠点がなくても対象となります。

Microsoft 365のeDiscovery(電子情報開示)

Microsoft 365のeDiscoveryなら、
証拠の保全、検索、エクスポートが可能です！

eDiscovery

eDiscoveryの種類

eDiscoveryには、次の2種類があります。

- コア
  - 基本的なeDiscoveryであるケースの作成、コンテンツのホールド、コンテンツの検索、エクスポートなどが含まれます。
- Advanced
  - コアの機能に加えて、レビューセットやケースデータの分析などを行うことができます。

コアeDiscoveryの構成手順

コアeDiscoveryを使用すると、訴訟で証拠として使用する電子的情報を検索したり、保留したりすることができます。コアeDiscoveryの構成手順は次の通りです。

Step1：アクセス許可を付与します。

Step2：新しいケースを作成します。

Step3：コンテンツの場所を保留します。

Step4：コンテンツ検索を作成して実行します。

コンテンツ検索の前に、コンテンツの保存されている場所を保留します。

Exam Point

コアeDiscoveryにおいてコンテンツを検索する前に行っておくことは何ですか。

	選択肢
A	弁護士/依頼人の特権の検出を構成します。
B	高速分析を実行します。
C	結果をエクスポートしダウンロードします。
D	保留リストを作成します。

解答：D

コンテンツ検索を行う前には、保留リストを作成しておきます。

SC-900 Microsoft Security,
Compliance, and Identity Fundamentals

5.8
Microsoft 365の監査機能について説明する

Microsoft 365の高度な監査

- 次のライセンスを所有している場合、高度な監査を利用できます。
  - Office 365 E5
  - Microsoft 365 E5
  - Microsoft 365 E5 Compliance

- 高度な監査を利用すると次のようなメリットが得られます。
  - さまざまな種類の監査済みアクティビティを可視化できます。
  - 監査ログの長期保存を行うことができます(最大10年)。
  - 既定の監査ログポリシーでは、次のアクティビティが監査され1年間保存されます。
    - Azure Active Directory
    - SharePoint
    - Exchange

Advanced Auditの特徴

Microsoft 365のさまざまなサービスのさまざまな種類の監査済みアクティビティを可視化できます。
迅速かつ効果的なフォレンジックおよびコンプライアンス調査を強化することができます。

監査ログの長期保管

Exchange、SharePoint、および Azure Active Directoryの監査レコードが1年間保持されます。
監査ログ保持ポリシーを使用すれば、**最大10年保存できます。**

Point

データアクセスの高速化

すべての組織には、最初に1分あたり2,000件の要求のベースラインが割り当てられます。この制限は、組織のシート数とライセンスサブスクリプションに応じて動的に増加します。**E5組織は、E5以外の組織の約2倍の帯域幅を利用できます。**

Point

重要なイベントの監査

メールボックスアイテムへのアクセス監査アクションを新たにサポートしました。
このアクションは、**メールプロトコルとメールクライアントがメールデータにアクセスしたときにトリガーされます。**

Point

Exam Point

次の各ステートメントについて、ステートメントが真の場合は、「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。

①Microsoft 365の高度な監査を使用すると、電子メールアイテムがいつアクセスされたかを識別できます。

②Microsoft 365の高度な監査は、コア監査と同じ監査ログの保持期間をサポートします。

③Microsoft 365の高度な監査では、監査データにアクセスするために顧客専用の帯域幅が割り当てられます。

解答：以下を参照

①Microsoft 365の高度な監査を使用すると、電子メールアイテムがいつアクセスされたかを識別できます。

はい　メールプロトコルとメールクライアントがメールデータにアクセスしたときに監査ログが作成されます。

②Microsoft 365の高度な監査は、コア監査と同じ監査ログの保持期間をサポートします。

いいえ　高度な監査は、Microsoft 365 E5ライセンスなどで利用できます。E3ライセンスが割り当てられているユーザーの場合、監査ログは90日保存されます。

③Microsoft 365の高度な監査では、監査データにアクセスするために顧客専用の帯域幅が割り当てられます。

はい　監査ログにアクセスする際、すべての組織には、最初に1分あたり 2,000件の要求のベースラインが割り当てられます。E5組織は、E5以外の組織の約2倍の帯域幅を利用できます。


Microsoft