

© Copyright Microsoft Corporation. All rights reserved.

Microsoft Virtual Training Days プログラムの一部としてのみ使用できます。これらの資料のマイクロソフト以外の当事者による配布、複製、その他の使用は許可されません。



Microsoft Security Virtual Training Day: Security, Compliance, and Identity Fundamentals





セキュリティ、コンプライアンス、ID の概念について説明する

モジュール の議題

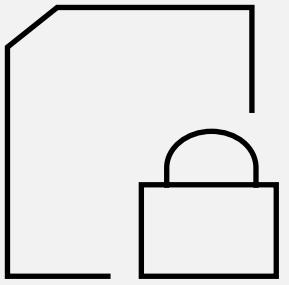


セキュリティとコンプライアンスの概念と方法について説明する



ID のコンセプトを説明する

レッスン 1: セキュリティとコンプライアンスの概念と方
法について説明する



レッスン 1 はじめに

このレッスンを終了すると、次のことができるようになります。

- ・ ゼロトラスト モデルと共有責任モデルについて説明する。
- ・ 一般的なセキュリティの脅威と、多層防御モデルを使った保護する方法について説明する。
- ・ 暗号化とハッシュの概念について説明する。
- ・ クラウド導入フレームワークについて説明する。

ゼロ トラスト方法

ゼロ トラストの原則

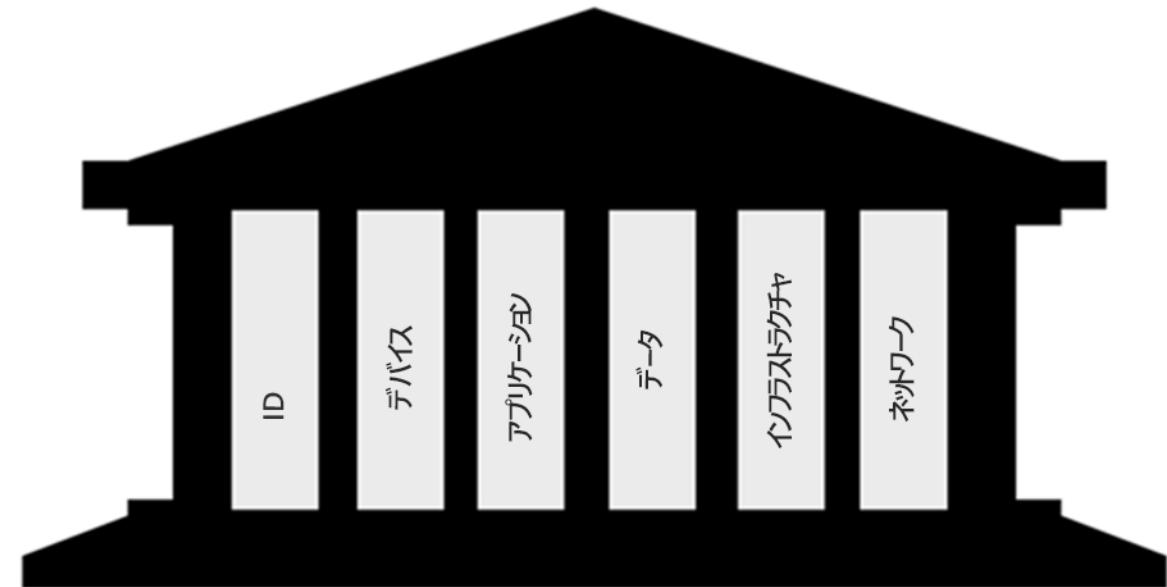
- 明示的に確認する
- 特権アクセスの最小化
- 侵害を想定する

基本的な 6 本の柱

- ID にはユーザー、サービス、またはデバイスが含まれます。
- デバイスは、データが流れることで大きな攻撃面となります。
- アプリケーションは、データが消費される方法です。
- データは属性に基づいて分類、ラベル付け、暗号化が必要です。
- インフラストラクチャは、オンプレミスであれクラウドベースかであれ、一つの脅威ベクトルを表す。
- ネットワークはセグメント化が必要。

ゼロ トラスト方法

「すべてを疑い、すべてを確認する」



明示的に確認する

特権アクセスの最小化

侵害を想定する

多層防御

多層防御では、セキュリティを層に分けて考えています:

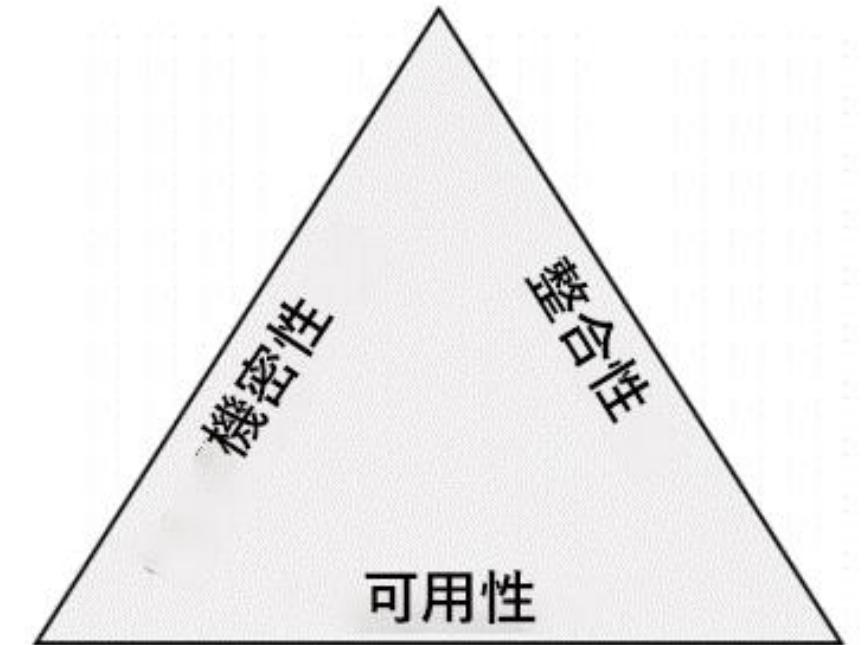
- 物理的セキュリティ: データセンターへのアクセスを許可のある人員のみに制限するなど
- ID およびアクセスのセキュリティ: インフラストラクチャと変更管理へのアクセスを管理
- 境界セキュリティ: ユーザーに対するサービス拒否が発生する前に、大規模な攻撃をフィルター処理する分散型サービス拒否 (DDoS) 保護など
- ネットワーク セキュリティ: セグメンテーションとアクセス制御を通じてリソース間の通信を制限
- コンピューティング層: 特定のポートを閉鎖することで、オンプレミスまたはクラウド内の仮想マシンへのアクセスを保護するなど
- アプリケーション層: アプリケーションが保護されており、セキュリティ上の脆弱性がないことを確保する
- データ層: ビジネスデータと顧客データへのアクセス、およびデータを保護するための暗号化を制御



機密性、整合性、可用性 (CIA)

CIA - セキュリティのトレードオフについての考え方

- ・ **機密性**とは、顧客情報やパスワード、財務データなどの機密データを保持する必要があること
- ・ **整合性**とは、データやメッセージが正しいであること。
- ・ **可用性**とは、データを必要とする人がこれを利用できるようにすること。



共同責任モデル

責任は、ワーカロードがホストされる場所によって異なります：

- サービスとしてのソフトウェア (SaaS)
- サービスとしてのプラットフォーム (PaaS)
- サービスとしてのインフラストラクチャ (IaaS)
- オンプレミスのデータセンター (オンプレミス)

共同責任モデル

担当

情報とデータ

デバイス (モバイルおよび PC)

アカウントと ID

ID とデバイス インフラストラクチャ

アプリケーション

ネットワーク制御

オペレーティング システム

物理ホスト

物理ネットワーク

物理データセンター

SaaS PaaS IaaS
オンプレミス

責任は顧客によって常に保持されます

責任はサービスの種類によって異なります

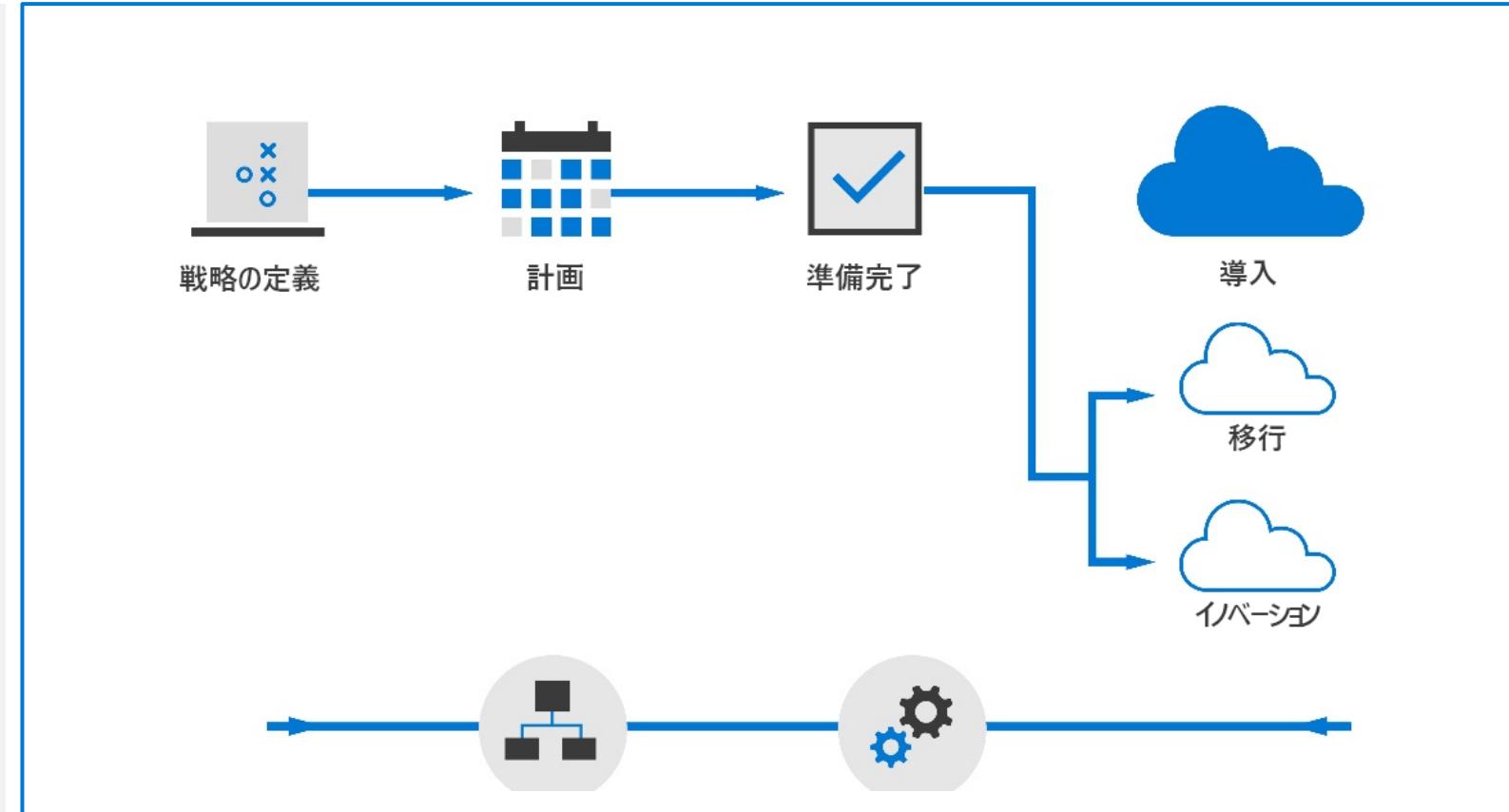
責任はクラウド プロバイダーへ転送します

Microsoft 顧客

Microsoft クラウド導入フレームワーク

Microsoft クラウド導入フレームワーク

- セキュリティとコンプライアンスの向上をサポートするドキュメント、実装ガイダンス、ベストプラクティスで構成されます。
- クラウドで成功するために必要な戦略を企業に提供し、支援します。
- ライフサイクル
 - 戦略
 - 計画
 - 準備完了
 - 導入 (移行/イノベーション)
 - ガバナンス
 - 管理



一般的な脅威



データ侵害

以下が含まれます：

- ・ フィッシング
- ・ スピア フィッシング
- ・ テクニカル サポート詐欺
- ・ SQL インジェクション
- ・ パスワードまたは銀行情報を盗む
よう意図されたマルウェア

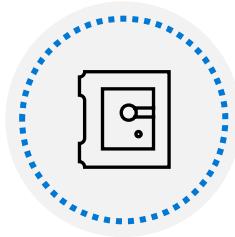


辞書攻撃

ID 攻撃の一種。

ハッカーは多数の既知のパスワードを試して ID を盗もうとします。

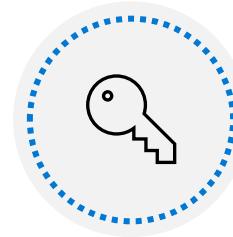
辞書攻撃は、ブルート フォース攻撃とも呼ばれます。



ランサムウェア

ファイルとフォルダーを暗号化するマルウェアの一種。

被害者から資金をゆすり取ろうとします。



妨害型攻撃

分散型サービス拒否 (DDoS) 攻撃は、アプリケーションのリソースを使い果たそうとします。

DDoS 攻撃は、どのエンドポイントでもターゲットになります。

その他の一般的な脅威には、コインマイナー、ルートキット、トロイの木馬、ワーム、悪用と悪用キットなどがあります。

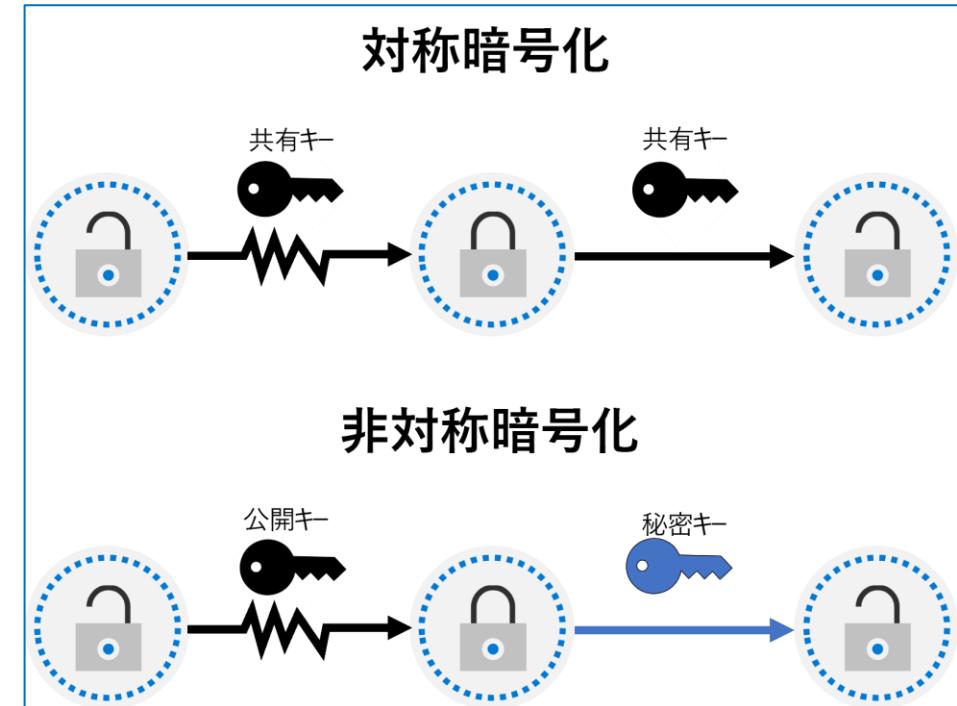
暗号化

暗号化は、承認されていない閲覧者がデータの読み取りと使用を実行できなくなるプロセスです。

- 保存データの暗号化
- 転送中のデータの暗号化

大きく分けて暗号化には二種類があります:

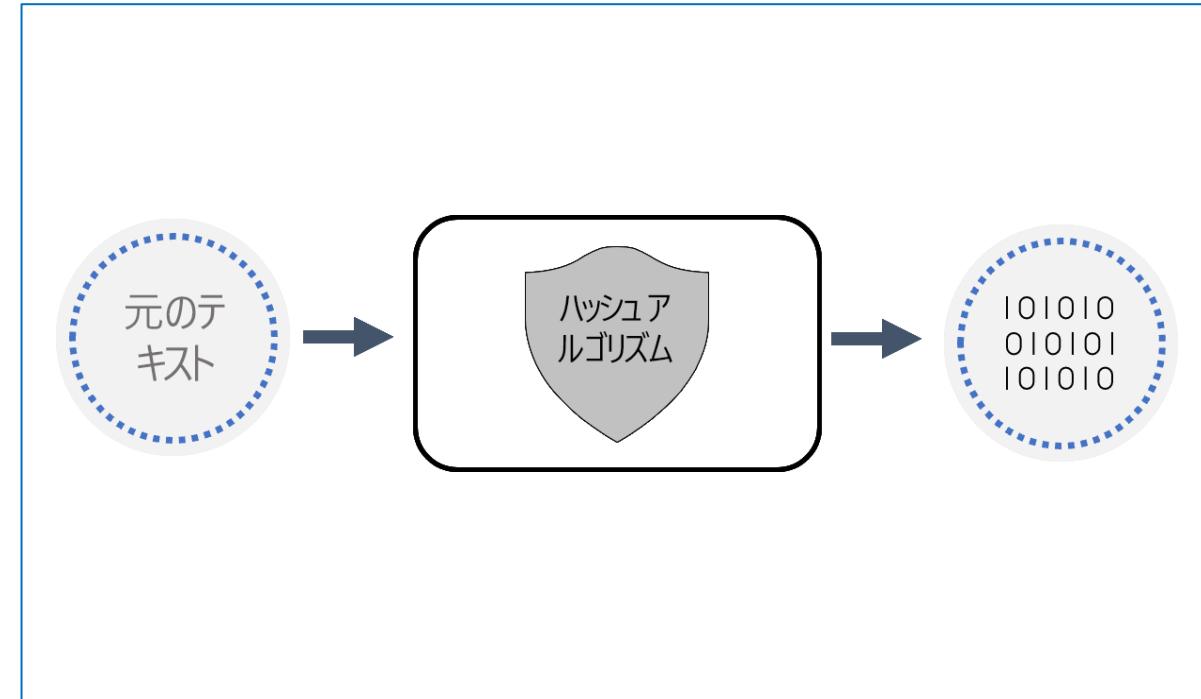
- 対称暗号化: 同じキーを使用してデータを暗号化し、復号します
- 非対称暗号化: 公開キーと秘密キーのペアを使用します



ハッシュ

ハッシュはアルゴリズムを利用し、元のテキストを独自の固定長ハッシュ値に変換します。ハッシュの機能:

- ・ 決定論的で、同じ入力が同じ出力を生成します。
- ・ 関連するデータを一意に識別するできるようにする。
- ・ 暗号化とは異なり、ハッシュ化された値を後から復号し元に戻すことは出来ません。
- ・ パスワードの保存に使用されます。パスワードを「ソルト化」することで、ブルートフォース辞書攻撃のリスクを軽減できます。



レッスン 2: ID のコンセプトを説明する



レッスン 2 はじめに

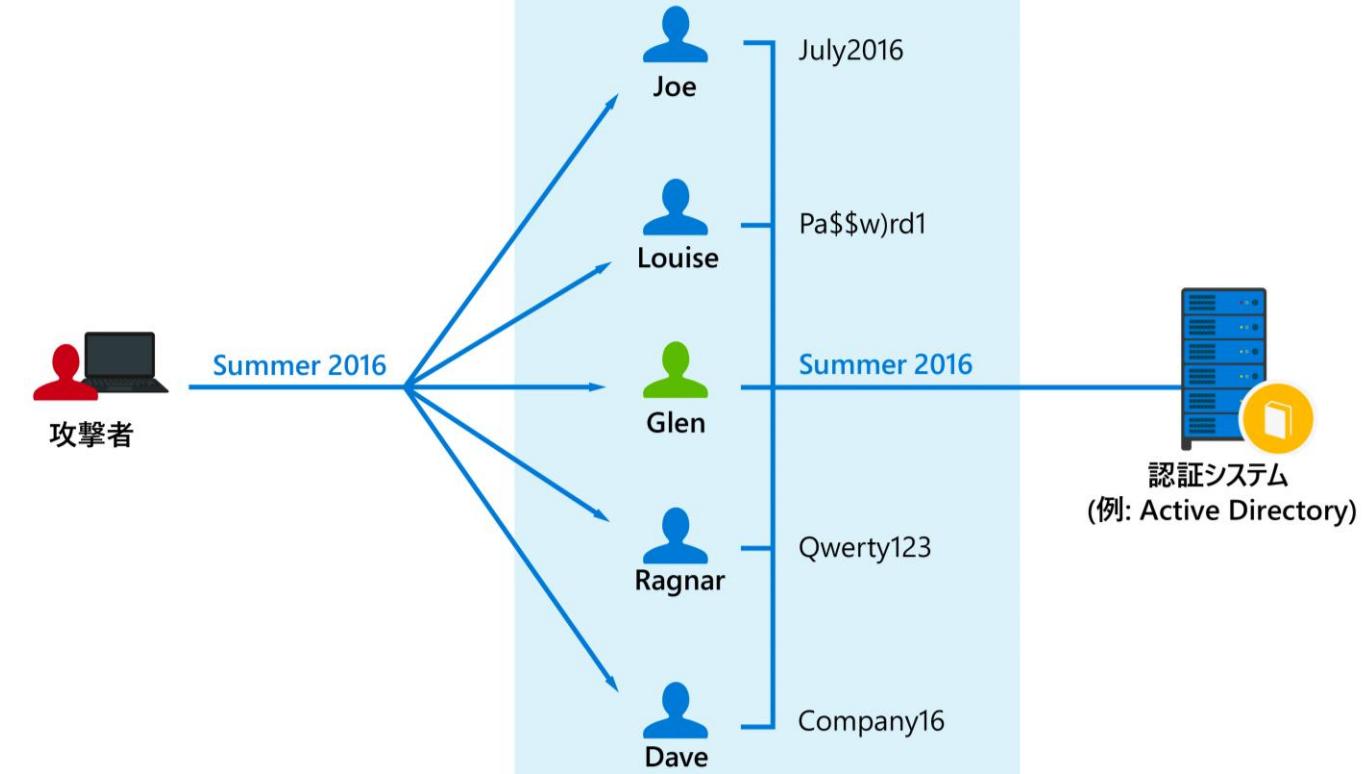
このモジュールを終了すると、次のことができるようになります。

- セキュリティ境界としての ID のコンセプトを説明する
- 認証と認可の違いを理解する
- ID 関連のサービスを説明する

一般的な ID の攻撃

セキュリティ脅威の種類:

- ・ パスワードベースの攻撃
- ・ フィッキング
- ・ スピア フィッキング



主要なセキュリティ境界としての ID

ID が、新しいセキュリティ境界となり、これを使用して、組織は資産をセキュリティで保護できます。

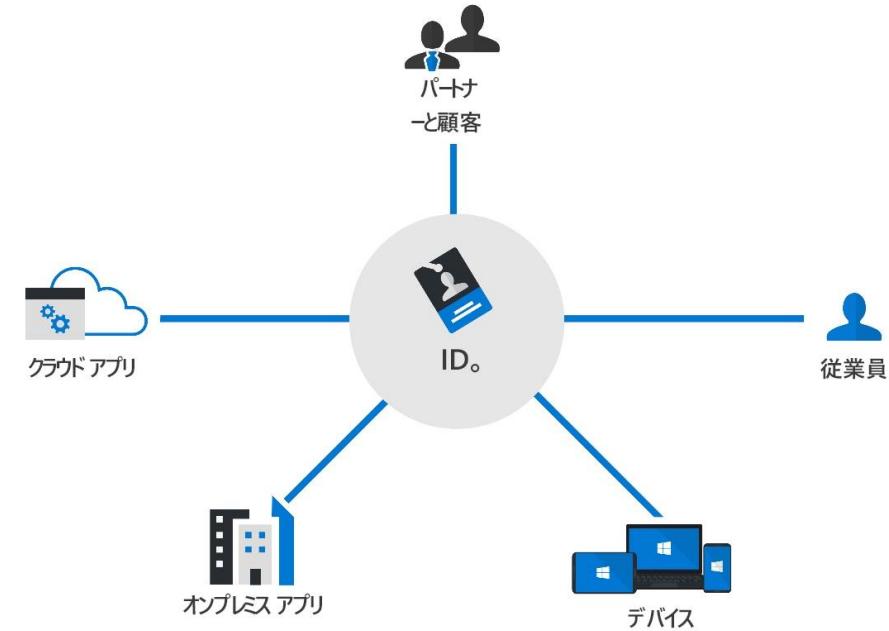
ID（アイデンティティ）とは、誰かまたは何かが検証され、認証される方法を指しています。一般的には以下に結び付けられています：

- ユーザー
- アプリケーション
- デバイス
- その他

ID の 4 つの基本的要素:

- 管理
- 認証
- 認可（承認）
- 監査

ID は新しいセキュリティ境界です



先進認証と ID プロバイダーの役割

先進認証はクライアントとサーバー間の認証および認可方法を表す総称です。



先進認証の中核は **ID プロバイダー (IdP)** です。



IdP は認証、認可、監査サービスを提供します。



IdP は認証および認可ポリシーの設定やユーザーの行動監視などを組織が実行できるようにします。



IdP と「先進認証」の基本的な能力の一つは、シングル サインオン (SSO) をサポートすることです。



Microsoft Azure Active Directory は、クラウドベースの ID プロバイダーの一例です。

フェデレーション サービスのコンセプト

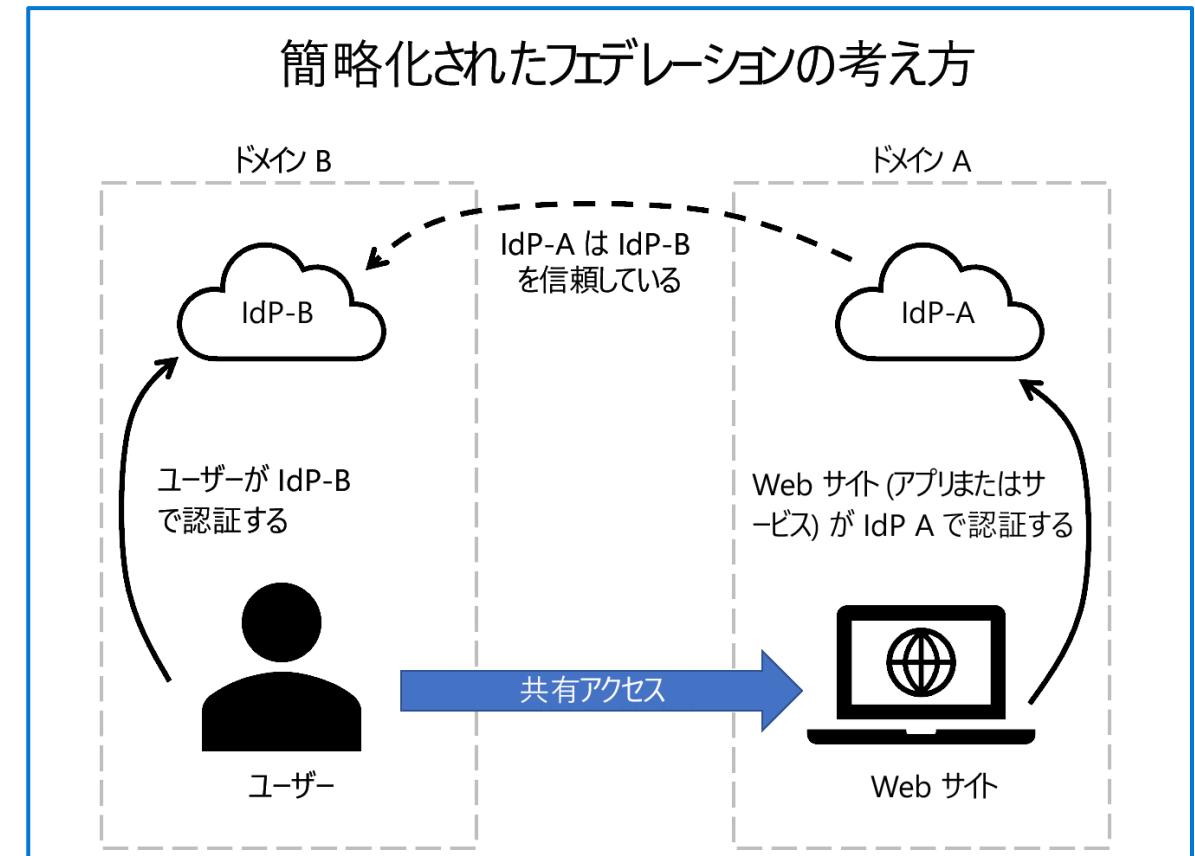
簡単にフェデレーションを説明すると:

ウェブサイトでは IdP-A での認証サービスが使われている

ユーザーが IdP-B で認証する

IdP-A と IdP-B の間には構成済みの信頼関係がある

ユーザーの資格情報がウェブサイトに渡されると、ウェブサイトはこのユーザーを信頼してアクセスを許可する



ディレクトリ サービスと Active Directory のコンセプト



ディレクトリとは、ネットワーク上のオブジェクトに関する情報を階層的に格納する構造です。



ディレクトリ サービスとは、ディレクトリ データを格納し、ネットワーク ユーザー、管理者、サービス、およびアプリケーションにそのデータを提供するサービスです。



最もよく知られているこの種のサービスは Active Directory Domain Services (AD DS) です。オンプレミス IT インフラストラクチャを備えた組織の中心的なコンポーネントです。



Azure Active Directory は ID およびアクセス管理ソリューションが進化したもので、クラウドとオンプレミス上にあるあらゆるアプリに向けて Identity as a Service (IDaaS) ソリューションを組織に提供します。

モジュールのまとめ

このモジュールでは、次のことを行いました。

- 重要なセキュリティのコンセプトと方法論をいくつか学びました。
 - ゼロ トラスト方法と、それを基盤としたゼロ トラストモデル、それら使用される 6 つの基本要素について学習しました。
 - 共同責任モデルについて学習しました。
 - 多層防御と CIA トライアドでのトレードオフについて学習しました。
 - ビジネスおよび個人データへの脅威など、一般的なサイバーセキュリティの脅威について学びました。
- いくつかの重要な ID の概念について学習しました。
 - セキュリティ境界としての ID の概念と ID の 4 つの柱について学習しました
 - ID プロバイダー、フェデレーション、ディレクトリ サービスのロールなど、ID 関連のサービスについて学習しました



Microsoft ID およびアクセス管理ソリューションの機能について説明する

レッスン 1: Azure Active Directory のサービスと ID の種類について調べる



レッスン 1 はじめに

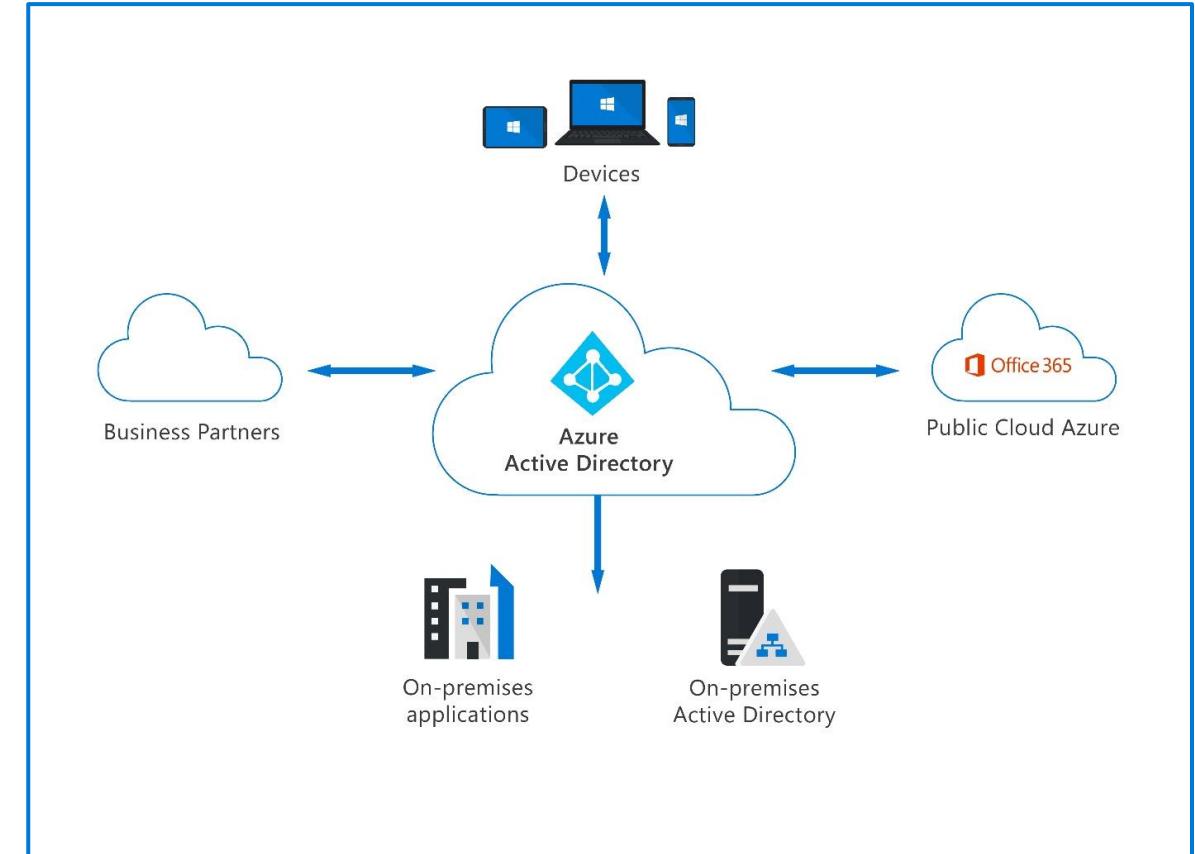
このモジュールを終了すると、次のことができるようになります。

- Azure Active Directory (Azure AD) について説明する
- Azure Active Directory でサポートされている ID のタイプを説明する

Azure Active Directory

Azure Active Directory (Azure AD) は、Microsoft のクラウドベースの ID およびアクセス管理サービスです。Azure AD には次のような機能があります。

- 組織は社員、ゲスト、その他の人がサインインして必要なリソースにアクセスする仕組みを提供できるようになります。
- クラウドおよびオンプレミス アプリケーションで単一の ID システムを提供します。
- ユーザーの ID と資格情報を保護し、組織のアクセス ガバナンス要件を満たします。
- Microsoft 365、Office 365、Azure、および Dynamics 365 オンライン サブスクリプションはそれぞれ自動的に Azure AD テナントを使用します。



Azure AD ID のタイプ

Azure AD では、ユーザー、サービス プリンシパル、マネージド ID、デバイスなど、さまざまな種類の ID が管理されています。



ユーザー - Azure AD が管理する対象を表します。従業員とゲストは、Azure AD のユーザーとして表されます。



サービス プリンシパル - アプリケーションまたはサービスが特定の Azure リソースにアクセスするために使用するセキュリティ ID。アプリケーション用の ID のようなものとして考えてください。



マネージド ID - 通常は Azure サービスを使用するクラウド アプリケーションの認証で資格情報を管理するために使用されます。2 つのタイプ: システム割り当てとユーザー割り当てがあります。



デバイス - モバイル デバイスやラップトップ、サーバー、プリンターなどのハードウェアです。デバイス ID は、デバイスの所有者などのプロパティを決定するために、Azure AD でさまざまな方法で設定できます。

デモ

Azure Active Directory ユーザー設定



Azure AD の外部 ID

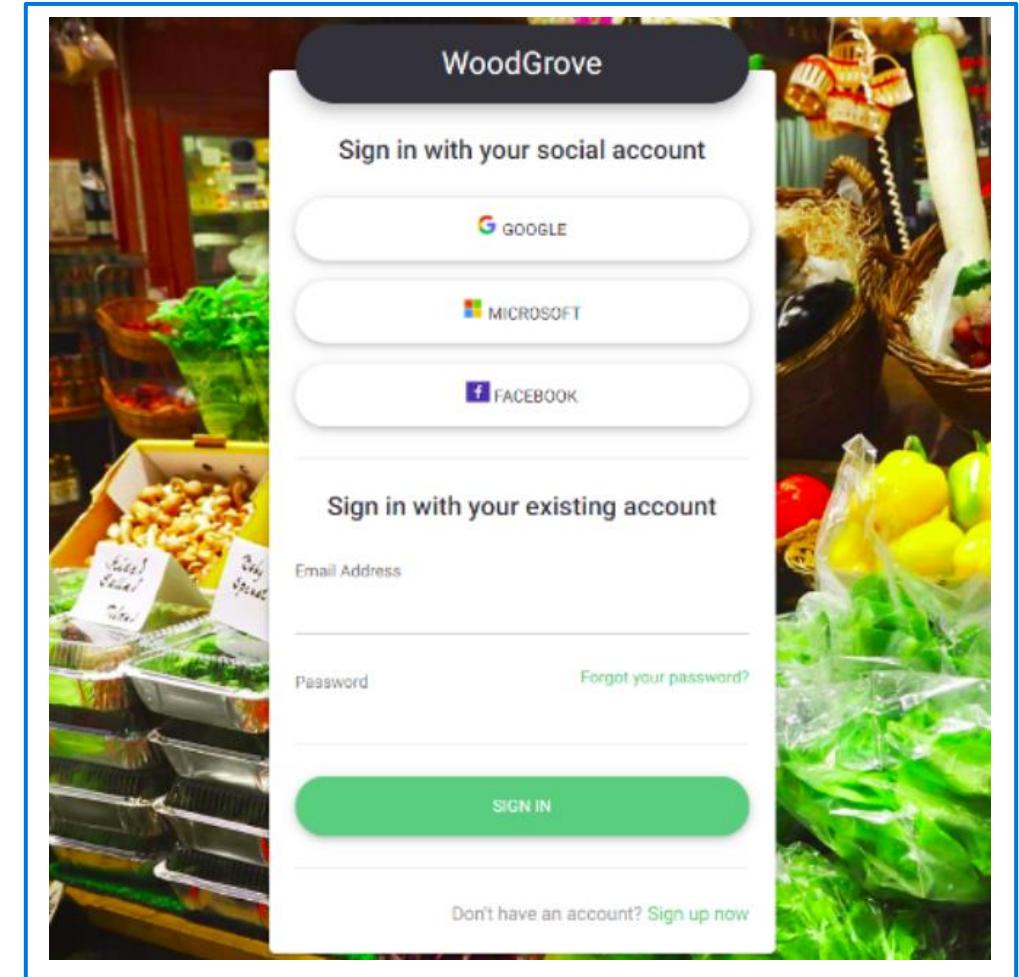
Azure AD 外部 IDには二種類があります:

B2B コラボレーション

B2B コラボレーションでは、アプリやリソースを外部ユーザーと共有することが可能

B2C アクセス管理

B2C はエンドユーザーの ID 管理と、顧客フェーシング アプリの ID 管理用のソリューション



ハイブリッド ID のコンセプト

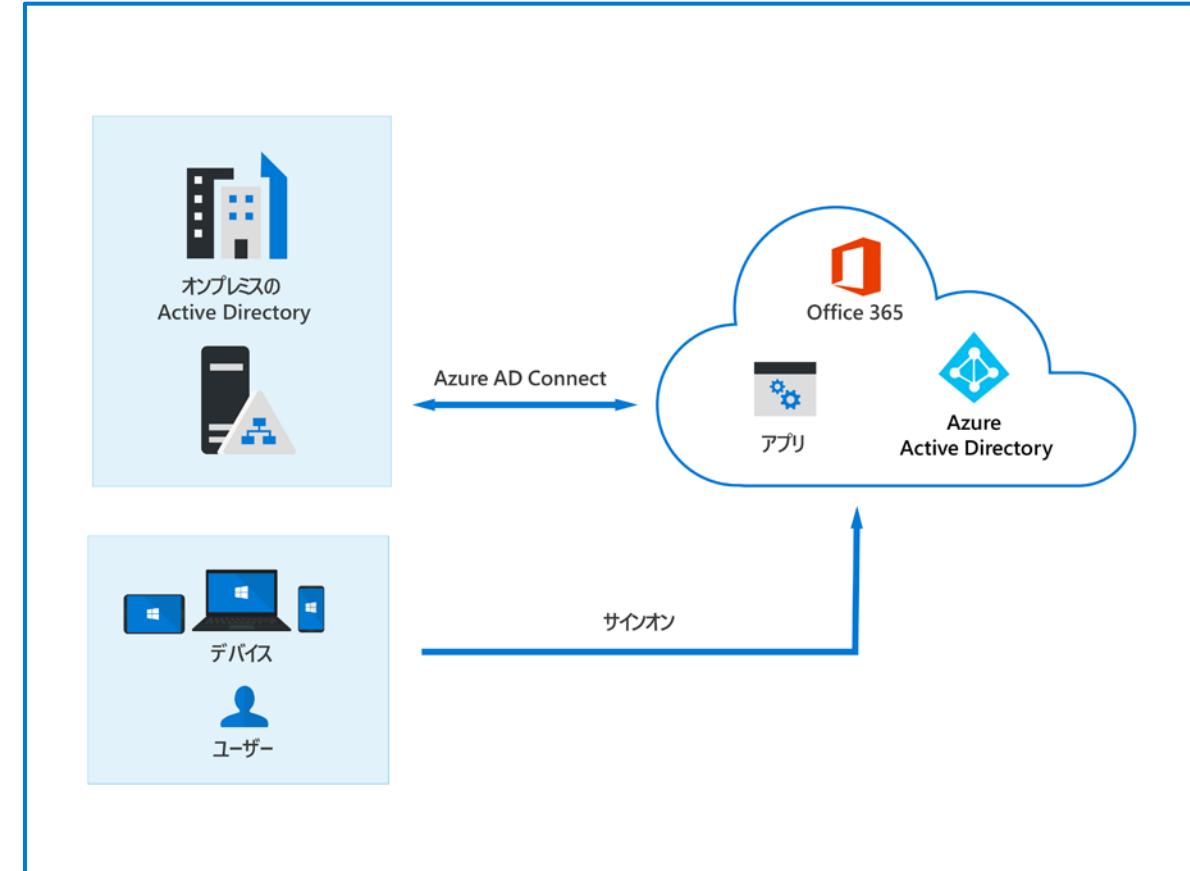
ハイブリッド ID と認証

ハイブリッド ID モデル

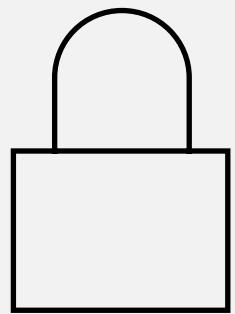
- ハイブリッド モデルを使用すると、オンプレミスとクラウドの両方のアプリにアクセスするユーザーは、オンプレミスの Active Directory で管理されるハイブリッド ユーザーになります。
- オンプレミス AD DS で更新を行うと、ユーザー アカウント、グループ、連絡先の更新はすべて、*Azure AD Connect*によって Azure AD に同期されます

認証方法

- パスワード ハッシュ同期
- パススルー認証 (PTA)
- フェデレーション認証



レッスン 2: Azure Active Directory の認証機能について説明する



レッスン 2 はじめに

このモジュールを終了すると、次のことができるようになります。

- Azure AD のセキュリティで保護された認証方法について説明する
- Azure AD のパスワード保護と管理機能について説明する

Azure AD の認証方法

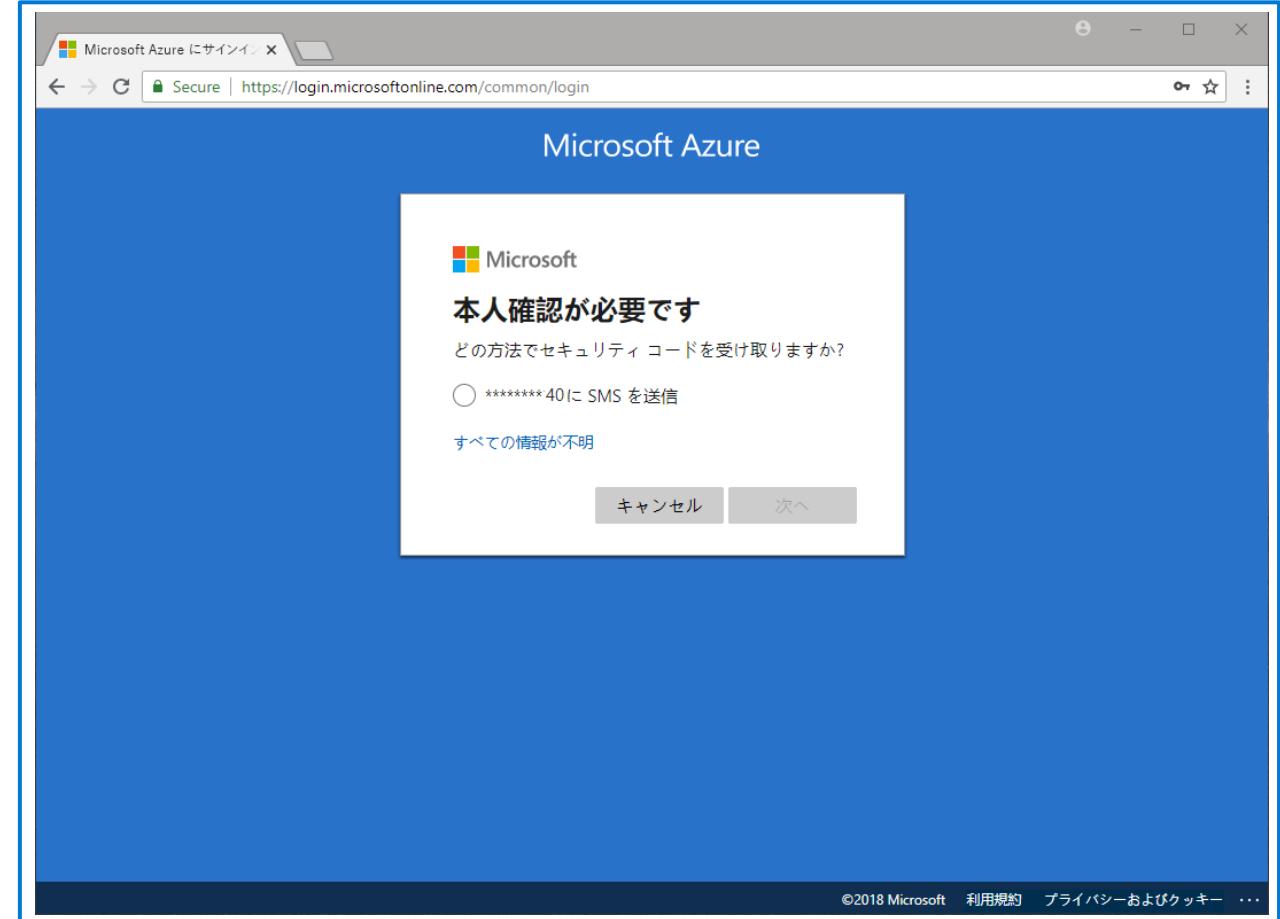
多要素認証 (MFA) とセキュリティの既定値群

MFA では複数の確認形式が必要:

- ・ ユーザーが知っているもの
- ・ ユーザーが持っているもの
- ・ ユーザー自身

セキュリティの既定値群:

- ・ Microsoft の推奨する基本的な ID セキュリティ メカニズムのセット。
- ・ セキュリティに対する姿勢を高めたいものの、どこから始めればよいのかわからない組織、または Free レベルの Azure AD ライセンスを使用している組織向けのすばらしいオプション。



Azure AD の多要素認証 (MFA)

MFA で利用できる様々な認証方法

パスワード

パスワードおよび追加確認

- 電話 (音声または SMS)
- Microsoft Authenticator
- ソフトウェアまたはハードウェアトークンを使用したOAUTH認証 (OATH)

パスワードレス

- 生体認証 (Windows Hello)
- Microsoft Authenticator
- FIDO2

悪い: パスワード	良い: パスワードと以下の組み合わせ	より良い: パスワードと以下の組み合わせ	最適: パスワードレス
123456 qwerty password iloveyou Password1	 SMS  音声	 Microsoft Authenticator  ソフトウェアトークン OTP  ハードウェアトークン OTP (プレビュー)	 Microsoft Hello  Microsoft Authenticator  FIDO2 セキュリティキー (プレビュー)

Windows Hello for Business

Windows Hello で、ユーザーは以下を認証できます。

- Microsoft アカウント
- Active Directory アカウント
- Azure Active Directory (Azure AD) アカウント
- Fast ID Online v2.0 認証をサポートする ID プロバイダー サービスまたは証明書利用者サービス

Windows Hello がパスワードよりも安全なのはなぜですか。

設定された特定のデバイスに関連付けられているハードウェアがなければ、PIN は役に立たない

Azure AD のセルフサービスパスワード リセット (SSPR)

セルフサービス パスワード リセットの利点:

- セキュリティの強化
- ヘルプデスクスタッフへの電話と要求の回数が減るため、組織の費用が節約されます。
- 生産性が向上するため、ユーザーはより早く作業に戻ることができます。

セルフサービス パスワード リセットは、次のようなシナリオで役立ちます。

- パスワードの変更
- パスワードのリセット
- アカウントのロック解除

SSPR の認証方法:

- モバイルアプリの通知
- モバイルアプリのコード
- メール

デモ

Azure Active Directory
パスワードリセットのセルフサービス (SSPR)



Azure AD のパスワード保護・管理機能



グローバル禁止パスワード リスト



カスタム禁止パスワード リスト

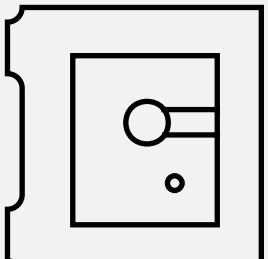


パスワード スプレーに対する保護



ハイブリッド セキュリティ

レッスン 3: Azure Active Directory のアクセス管理機能について説明する



レッスン 3 はじめに

このモジュールを終了すると、次のことができるようになります。

- 条件付きアクセスとその利点について説明する
- Azure AD ロールについて説明する

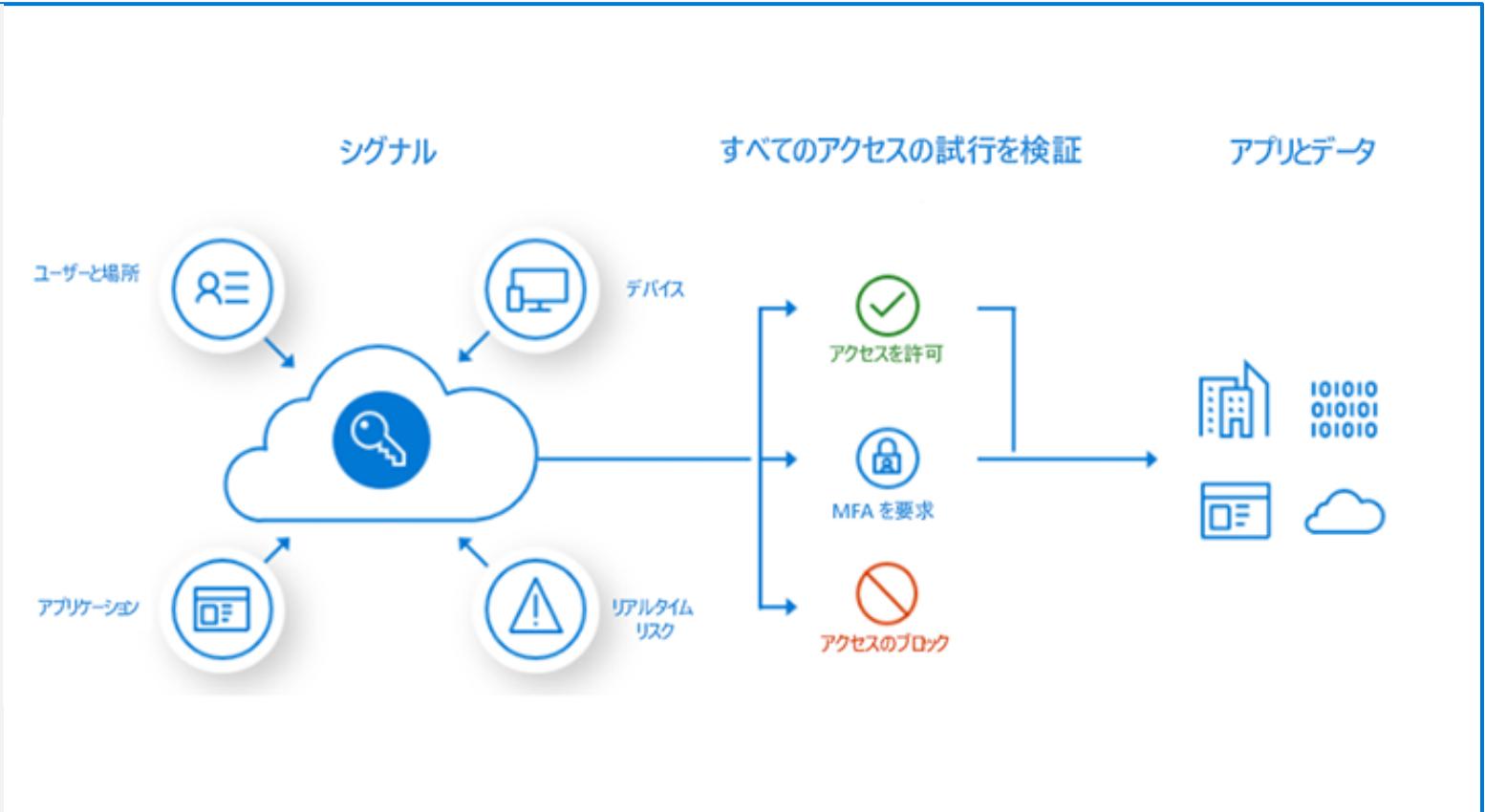
条件付きアクセス

条件付きアクセスのシグナル:

- ・ ユーザーまたはグループのメンバーシップ
- ・ ネームド ロケーション情報
- ・ デバイス
- ・ アプリケーション
- ・ リアルタイムのサインイン リスク検出
- ・ クラウド アプリまたはアクション
- ・ ユーザー リスク

アクセス制御:

- ・ アクセスをブロック
- ・ アクセス権を付与する
- ・ アクセス権を付与する前にひとつ以上の条件を満たすことを義務付ける
- ・ 特定のクラウド アプリケーション内で限定的なエクスペリエンスを有効にするため、セッション制御に基づいてユーザーのアクセスを管理する



デモ

Azure Active Directory
の条件付きアクセス



Azure AD のロールベースのアクセス制御 (RBAC)

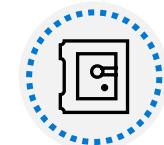
Azure AD ロールでは、Azure AD リソースを管理するためのアクセス許可が制御されます。



組み込みのロール



カスタム ロール

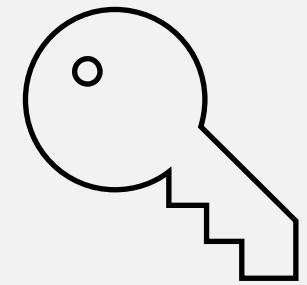


Azure ロールベースのアクセス制御



ユーザーが必要なアクセスだけを許可する

レッスン 4: Azure Active Directory の ID 保護およびガバナンス機能について説明する



レッスン 4 はじめに

このモジュールを終了すると、次のことができるようになります。

- Microsoft Azure Active Directory の ID ガバナンス機能について説明します。
- Privileged Identity Management (PIM) の利点について説明します。
- Azure Active Directory Identity Protection の機能について説明します。

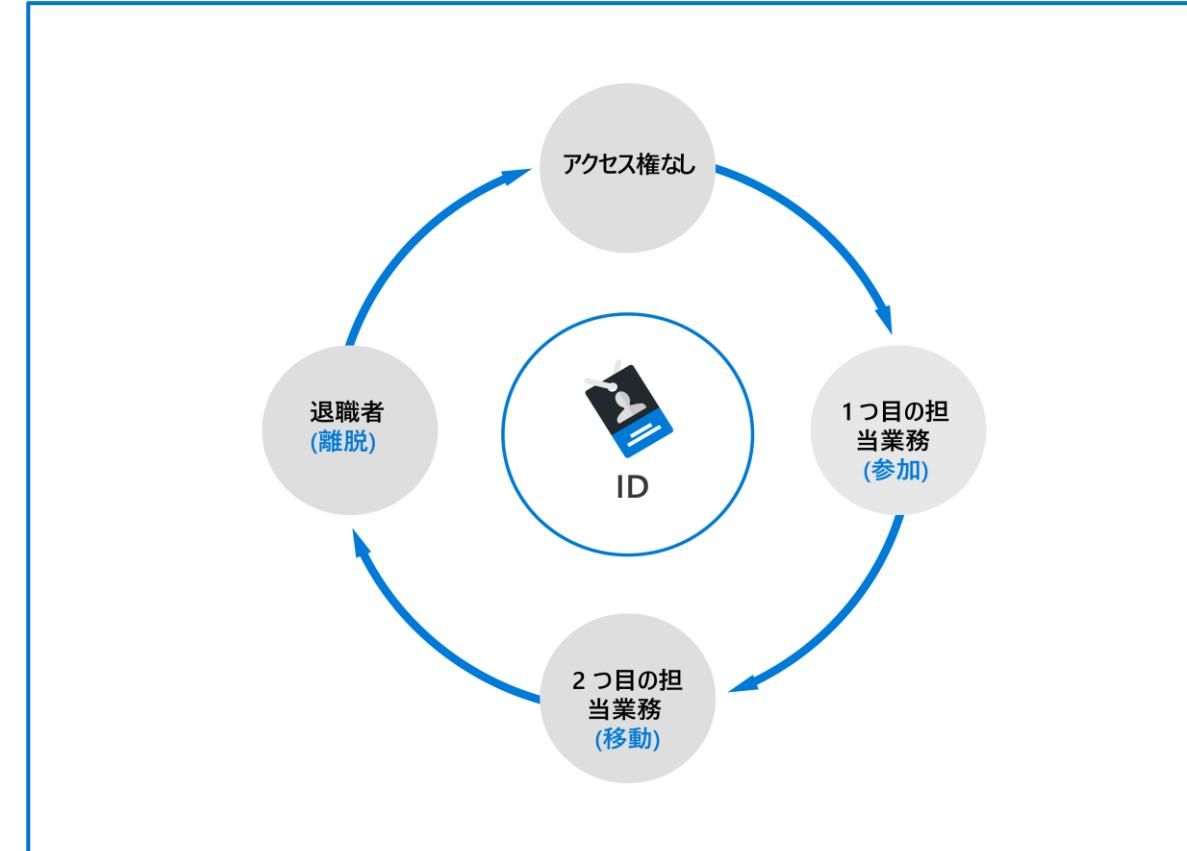
Azure AD の ID ガバナンス

Azure AD ID ガバナンスのタスク

- ID ライフサイクルの管理。
- アクセスのライフサイクルの管理。
- 管理のための特権アクセスのセキュリティ保護。

ID ライフサイクル

- 入社: 新しいデジタル ID が作成されます。
- 移動: アクセス許可を更新します。
- 退社: アクセスは削除が必要かもしれません。



エンタイトルメント管理とアクセス レビュー

エンタイトルメント管理

- 組織が ID とアクセスのライフサイクルを大規模に管理できるようにする ID ガバナンス機能です。
- アクセス要求ワークフロー、アクセス割り当て、レビュー、および有効期限を自動的に管理します。

アクセス レビュー

- 組織はグループ メンバーシップ、エンタープライズ アプリケーションへのアクセス、およびロールの割り当てを効率的に管理できます。
- 適正な人員のみがリソースにアクセスできるようにします。
- ユーザーとゲスト双方のアクセス権をレビューして管理するために使用されます。

Azure AD の使用条件

- ユーザーがデータやアプリケーションにアクセスする前に情報をユーザーに提示できます。
- ユーザーが法律またはコンプライアンス要件に関する免責事項を読んだことを確認します。

Contoso

FrickelsoftNET の Finance Web アプリへのユーザーのアクセスを確認してください

Sarah Hoelzel さんあなたの組織において、FinanceWeb アクセス レビューで、1 人以上のユーザーの Finance Web アプリへの継続的なアクセスを承認または拒否するよう要求されました。レビュー期間は 2020 年 9 月 5 日までとなります。

FinanceWeb チームの皆さん - FinanceWeb アプリケーションにアクセスできるユーザーのリストを確認してください。アプリを使用していないユーザーからの望ましくないアクセスの削除にご協力ください。詳細情報: <https://finweb.contoso.com/access/reviews>

[レビューを開始する >](#)

アクセス レビューの実施方法や Azure Active Directory のアクセス レビューの詳細についてはこちらをご覧ください。

[プライバシーに関する声明](#)

Microsoft Corporation, One Microsoft Way, Redmond, WA 98052

促進者



Privileged Identity Management (PIM)

PIM を使用すると、組織内の重要なリソースへのアクセスを管理、制御、監視できます。



正確なタイミング。必要な時期になるまでは特権アクセスが提供されません。



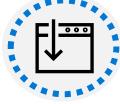
期限付き。ユーザーがリソースにアクセスできる日時を示す、開始日と終了日が割り当てられます。



承認ベース。権限のアクティブ化に特定の承認が必要です。



可視化。特権ロールがアクティブ化されると、通知が送信されます。



監査可能。完全なアクセス履歴がダウンロード可能です。

Azure Identity Protection

組織は 3 つの主要なタスクを実行できるようになります。

- ID ベースのリスクを自動的に検出して修正する。
- ポータルのデータを使用してリスクを調査する。
- さらに分析するために、リスク検出データをサードパーティのユーティリティにエクスポートする。

リスクを分類して計算できます。

- リスクを低、中、高の 3 つのレベルに分類します。
- サインインのリスクとユーザー ID のリスクを計算します。

3 つのレポートを組織に提供します。

- 危険なユーザー
- リスクの高いサインイン
- リスク検出

モジュールのまとめ

このモジュールでは、次のことを行いました。

- Azure AD と、Azure AD がサポートするサービスと ID の種類について学習しました
- MFA を含む Azure AD の認証機能について説明する
- 条件付きアクセスと Azure AD RBAC を使用した Azure AD のアクセス管理機能について説明する
- PIM、エンタitlement管理、アクセス レビューなど、Azure AD の ID 保護およびガバナンス機能について説明します。
- Azure AD Identity Protection の機能



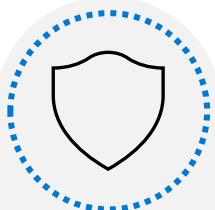
Microsoft セキュリティ ソリューションの機能について
説明する(Segment 1 of 2)

レッスン 1: Azure の基本的なセキュリティ機能について説明する



レッスン 1 はじめに

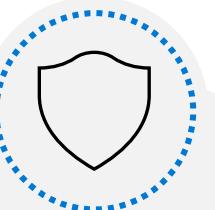
このモジュールを修了すると、次のことができるようになります。



Azure セキュリティ機能について説明する



AzureにてVMを保護する方法を説明する



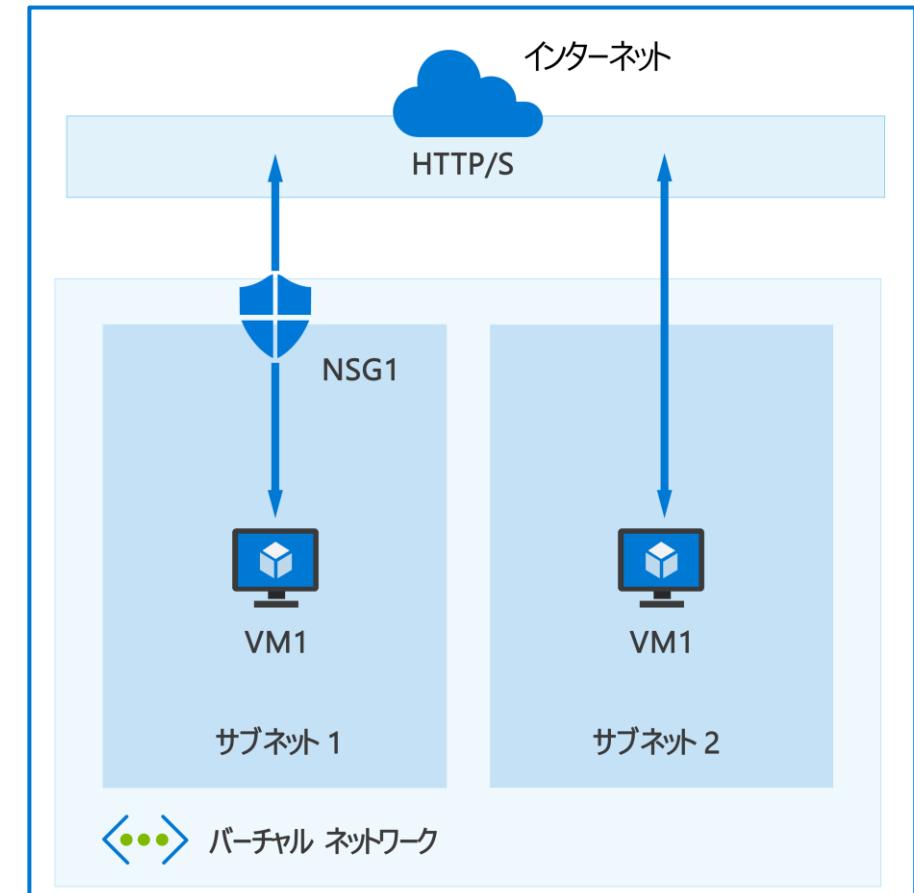
Azure上のデータを保護する方法を説明する

Azure ネットワーク セキュリティ グループ

ネットワーク セキュリティ グループ (NSG) を使用すると、Azure 仮想ネットワーク内の Azure リソースが宛先または送信先となるネットワーク トラフィックを許可または拒否できます。

- NSG は Vnet の複数のサブネットまたはネットワーク インターフェイスと関連付けられます。
- NSG は受信および送信セキュリティ規則で構成されます。
- 各規則は、次のプロパティが 1 つ以上指定されています。

- 名前	- 優先度
- 送信元または送信先	- プロトコル
- 方向	- ポート範囲
- アクション	



デモ

Azure ネットワーク セキュリティ グループ



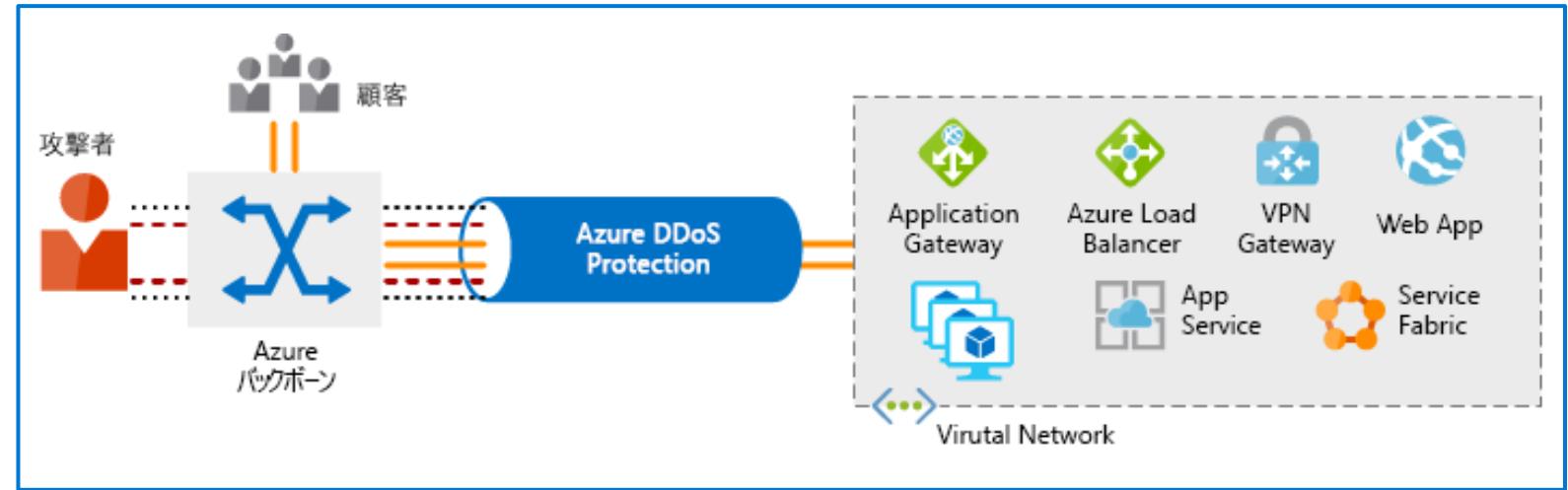
Azure の DDoS 保護

分散型サービス拒否 (DDoS) 攻撃を受けるとリソースは反応しなくなります。

Azure DDoS Protection はネットワークトラフィックを分析し、DDoS 攻撃とみなされるものはすべて破棄します。

Azure DDoS Protection の階層:

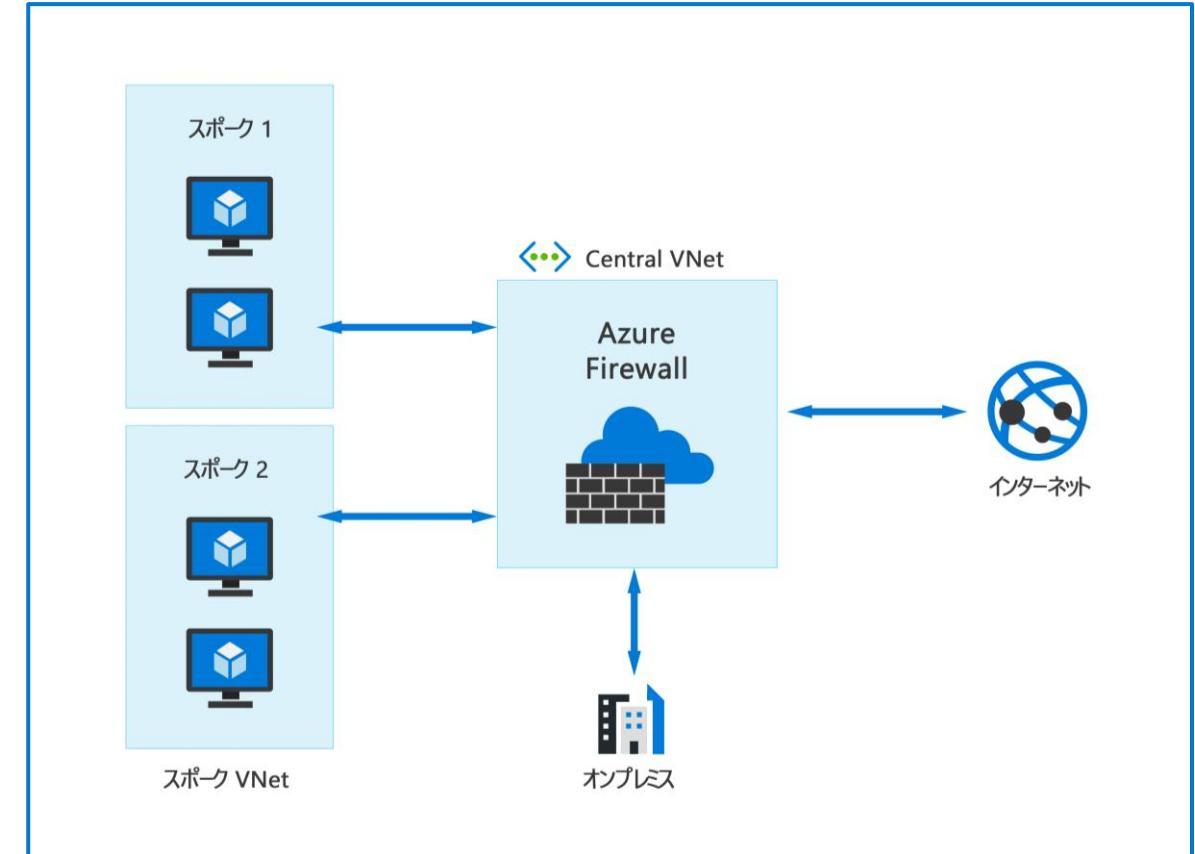
- Basic
- 標準



Azure Firewall

Azure Firewall は攻撃者から Azure 仮想ネットワーク (Vnet) リソースを保護します。次の機能が含まれます。

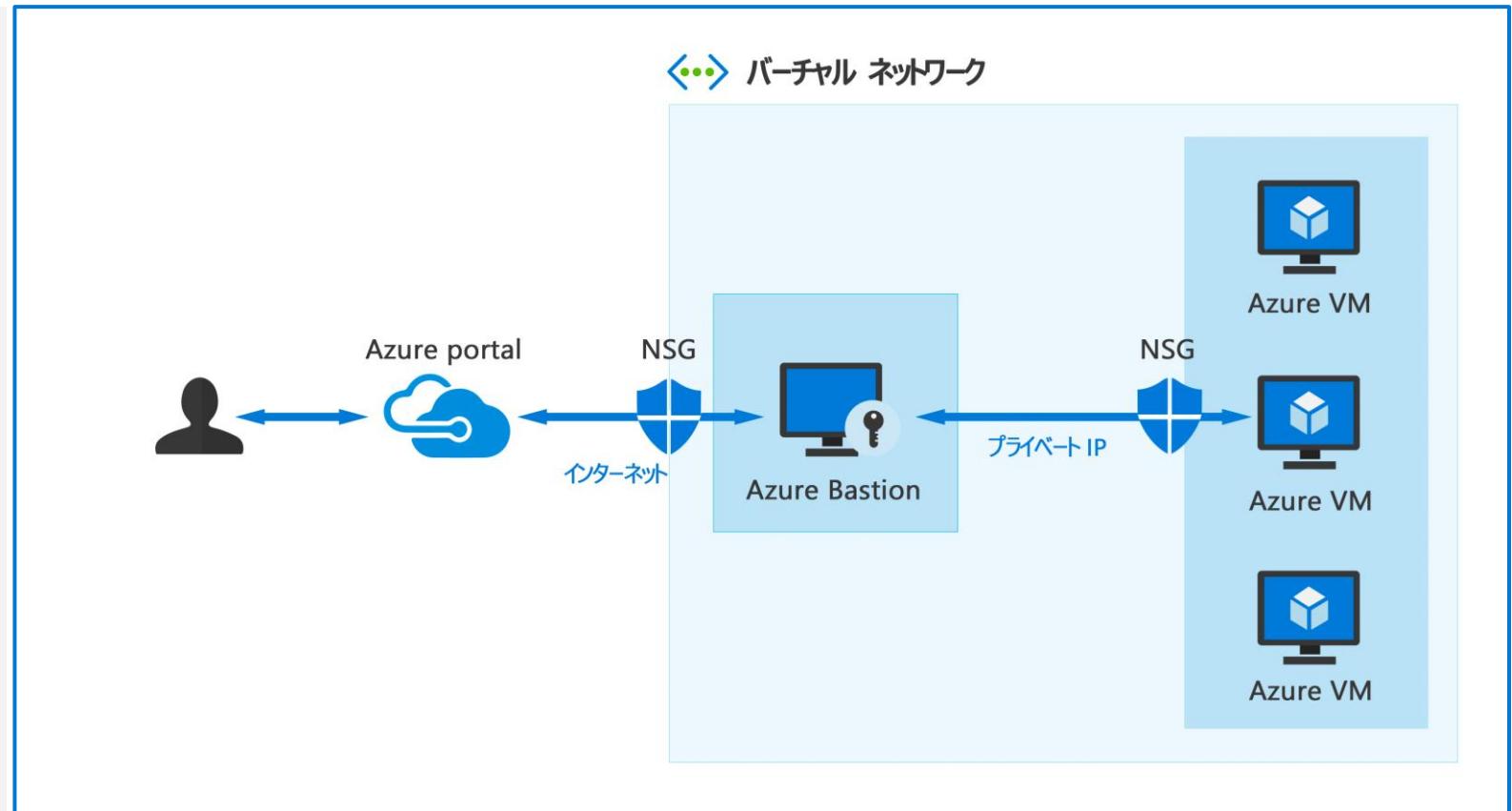
- 組み込まれた高可用性および可用性ゾーン
- 送信 SNAT および受信 DNAT
- 脅威インテリジェンス
- ネットワークおよびアプリケーション レベルのフィルタリング
- 複数のパブリック IP アドレス
- Azure Monitor との統合



Azure Bastion

Azure Bastion はトランスポート層セキュリティ (TLS) を使用して Azure ポータルから直接、VM への安全な接続を提供します。次の機能が含まれます。

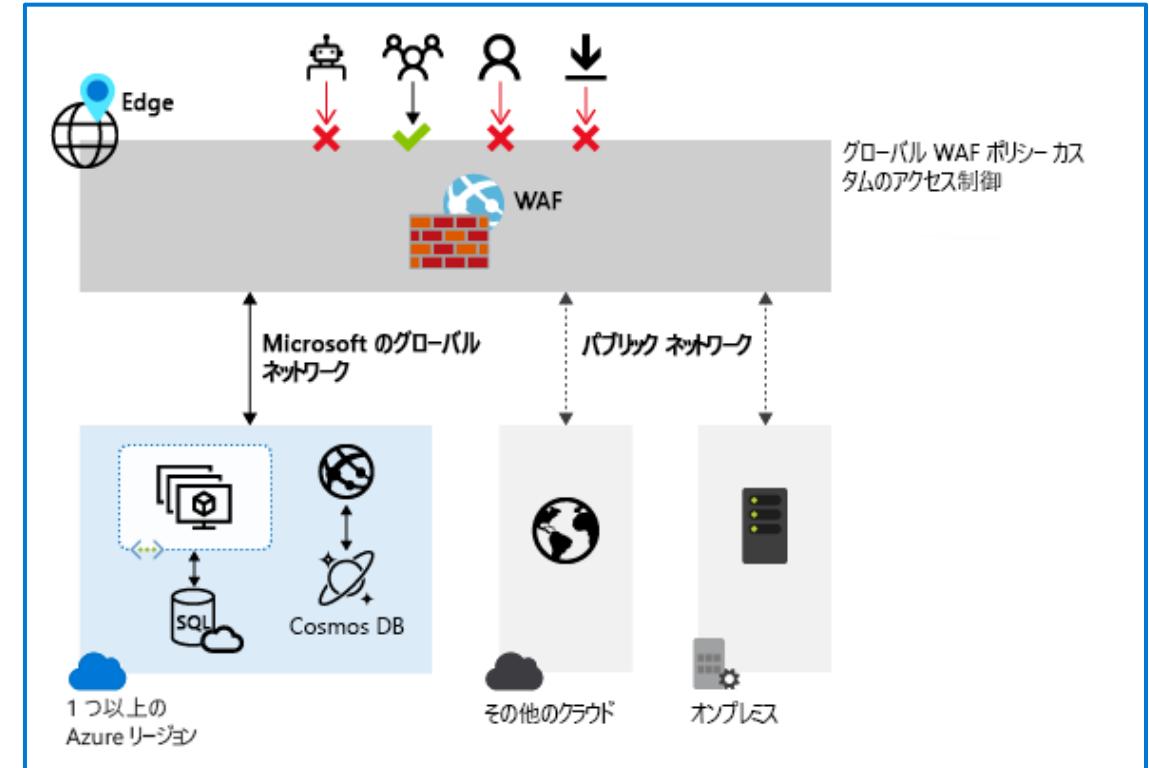
- Azure portal で直接 RDP および SSH を使用。
- TLS 経由のリモート セッションと RDP / SSH のファイアウォール トラバーサル。
- Azure VM ではパブリック IP が不要。
- NSG を管理する面倒が不要。
- ポート スキャンからの保護。
- ゼロデイ エクスプロイトからの保護。



Web アプリケーション ファイアウォール

Web アプリケーション ファイアウォール (WAF) は、一般的なエクスプロイトや脆弱性から Web アプリケーションを集中的に保護します。

- よりシンプルなセキュリティ管理
- セキュリティの脅威に対する応答時間の改善
- 一か所で既知の脆弱性を修正
- 脅威と侵害に対する保護



Azure のデータ暗号化方法および Key Vault 使用方法

Azure での暗号化



Azure Storage Service Encryption



Azure Disk Encryption



Transparent Data Encryption (TDE)

Azure Key Vault とは?



シークレット管理



キー管理

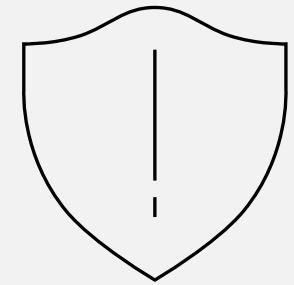


証明書管理



HW または SW でサポートされているシークレットを格納

レッスン 2: Azure のセキュリティ管理機能について
説明する



レッスン 2 はじめに

このモジュールを終了すると、次のことができるようになります。



Azure のセキュリティ管理機能について説明する



Microsoft Secure Score の利点とユースケースについて説明する



クラウドのセキュリティ体制管理およびセキュリティベースラインを理解する

クラウド セキュリティ態勢管理

クラウドのセキュリティ体制管理 (CSPM) はクラウドのセキュリティ管理を改善するためのツールです。

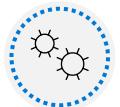
CSPM はツールとサービスを組み合わせて利用します。



ゼロ トラスト ベースの
アクセス制御



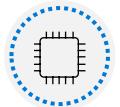
リアルタイムのリスク
スコア付け



脅威および脆弱性の管理
(TVM)



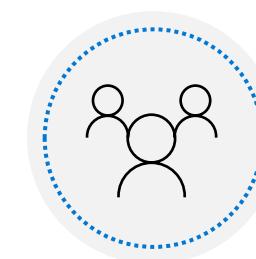
共有しているリスクの
検出



技術的ポリシー:



脅威モデリング
システムおよびアーキテクチャ



CSPM は多くのチームで役に立ちます。

- 脅威インテリジェンス チーム

- 情報技術

- コンプライアンスおよびリスク管理チーム

- ビジネスリーダーと SME

- セキュリティアーキテクチャと運用

- 監査チーム

Azure Security Center

マシン、データ サービス、アプリケーション全体でセキュリティ体制を強化します。

継続的な評価 – 最大限の保護を提供するには何を修正する必要があるのかに関する推奨事項に順番を付けたリスト。

脅威からの保護 - IaaS、Azure 以外のサー
バ、PaaS で脅威を検出して保護します。

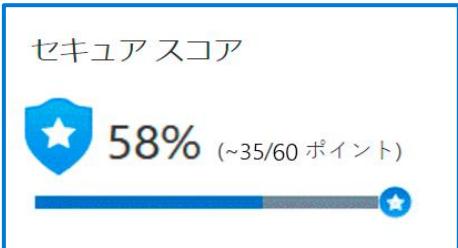
ネットワーク マップ - 各ノードが適切に構成さ
れているかどうかを確認するためのワークフロー
のトポロジー表示。

より迅速なセキュリティ保護 - 他の
Microsoft セキュリティソリューションと統合し
てあらゆる Azure リソースで完全なセキュリ
ティを提供します。



Azure セキュア スコア

セキュア スコアは、パーセントの値で Azure portal ページに表示されます。セキュリティスコアを向上させるには、推奨事項リストのセキュリティの推奨事項を修復してください。



システムの更新プログラムの適用		 + 2% (1 ポイント)	上昇の可能性: 0.96 現在のスコア: 5.04 最大スコア: 6	4 個中 1 個のリソース	<div style="width: 25%; background-color: red;"></div> <div style="width: 75%; background-color: limegreen;"></div>
お使いの仮想マシンに Log Analytics エージェントをインストールする				なし	<div style="width: 100%; background-color: limegreen;"></div>
お使いのマシンで Log Analytics エージェントの正常性の問題を修正する		4 個中 1 個の仮想マシン	<div style="width: 25%; background-color: red;"></div> <div style="width: 75%; background-color: limegreen;"></div>		
保存時の暗号化を有効にする		4 個中 4 個のリソース	<div style="width: 100%; background-color: red;"></div>		
仮想マシンでディスクの暗号化を適用する必要があります		4 個中 4 個の仮想マシン	<div style="width: 100%; background-color: red;"></div>		
承認されていないネットワーク アクセスを制限する		1 個中 1 個のリソース	<div style="width: 100%; background-color: red;"></div>		
インターネットに接続されている仮想マシンをネットワークに接続しない		なし	<div style="width: 100%; background-color: limegreen;"></div>		
ご使用の仮想マシンに関連付けられたネットワーク セキュリティグループを確認する		1 個中 1 個の仮想マシン	<div style="width: 100%; background-color: red;"></div>		
仮想マシン上の IP 転送を無効にする必要があります		なし	<div style="width: 100%; background-color: limegreen;"></div>		



デモ

Azure Security Center



Azure Defender

Azure Defender の範囲



サーバー



App Service



ストレージ



SQL



Kubernetes



コンテナー レジストリ



Key Vault

ハイブリッド クラウド保護



Azure 以外のサーバーを
保護します。



他のクラウド (AWS、GCP など)
内の仮想マシンを保護する。

Azure Defender アラート

高度な保護

脆弱性評価

Azure セキュリティ ベンチマーク用のセキュリティ ベースライン

Azure のセキュリティ ベースラインは環境のセキュリティを保護する際に一貫したエクスペリエンスを提供します。Azure セキュリティ ベンチマーク (ASB) からの規範的なベスト プラクティスと推奨事項を適用して、Azure でワークフロー、データ、サービスのセキュリティを向上します。各推奨事項には次の情報が含まれます。



Azure ID: 推奨事項に対応する Azure セキュリティ ベンチマーク ID。



推奨事項: 推奨事項はコントロールの高度な説明を提供します。



ガイダンス: 推奨事項の根拠と、その実装方法に関するガイダンスへのリンク。

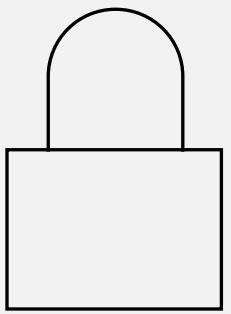


責任: コントロールの実装担当者は?



Azure Security Center の監視: Azure Security Center はコントロールを監視しますか?

レッスン 3: Azure Sentinel のセキュリティ機能について説明する



レッスン 3 はじめに

このモジュールを終了すると、次のことができるようになります。



Microsoft Secure Score の SOAR、XDR のセキュリティのコンセプトを説明する

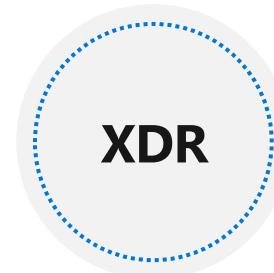


Microsoft Secure Score の 統合された脅威防止を提供する方法を 説明する



Microsoft Secure Score の 機能を説明する

SIEM、SOAR、XDR



セキュリティインシデントおよびイベント管理とは

SIEM システムは、インフラストラクチャ、ソフトウェア、リソースなど、資産全体からデータを収集するために組織が使用するツールです。分析を行い、相関関係や異常を検索し、アラートとインシデントを生成します。

セキュリティオーケストレーション自動対応とは

SOAR システムは、SIEM システムなどの多くのソースからアラートを受け取ります。次に、SOAR システムは、アクション主導の自動化ワークフローおよびプロセスをトリガーして、問題を軽減するセキュリティタスクを実行します。

拡張検出および応答とは

XDR システムは、組織のドメイン全体にわたり、自動化されたインテリジェントな統合セキュリティを提供するように設計されています。これは、ID、エンドポイント、アプリケーション、電子メール、IoT、インフラストラクチャ、クラウド プラットフォームにわたる脅威の防止と検出、および脅威への対応に役立ちます。

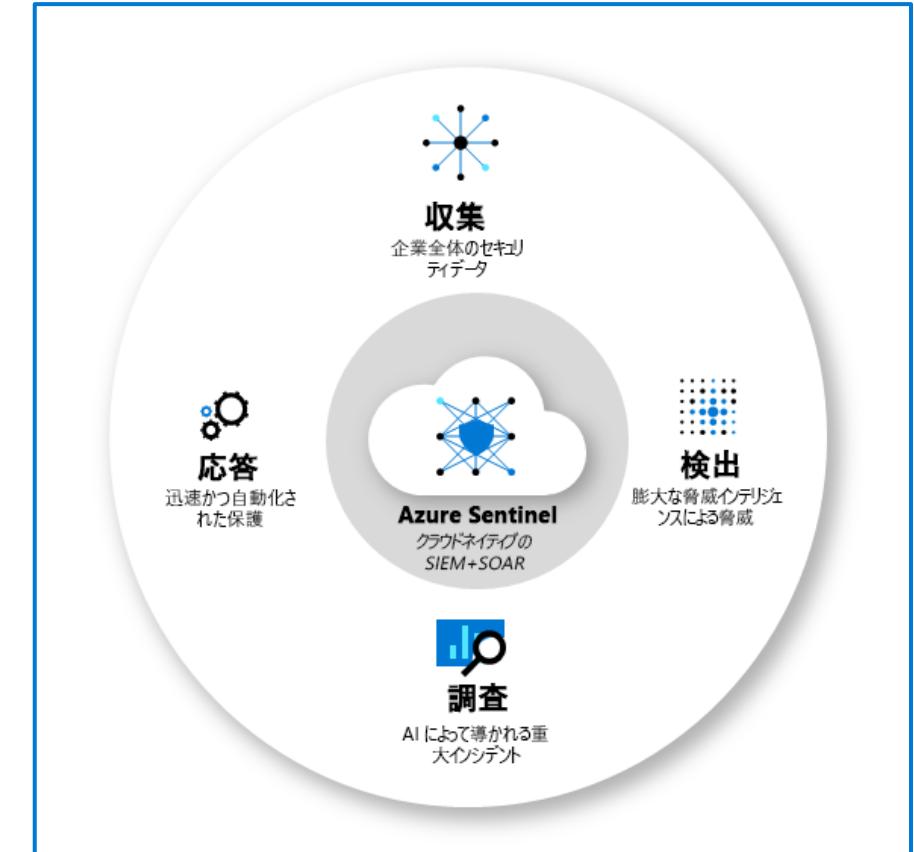
Sentinel は脅威防止の統合機能を提供 (スライド 1)

オンプレミスと複数のクラウドの両方のすべてのユーザー、デバイス、アプリケーション、インフラストラクチャ全体でクラウド規模のデータを収集します。

これまで検出されなかった脅威を検出し、分析と比類のない脅威インテリジェンスを使用して誤検知を最小限に抑えます。

人工知能を使用して脅威を調査し、Microsoft での長年にわたるサイバーセキュリティ作業を活用して、不審な活動を大規模に探します。

組み込みのオーケストレーションと共にセキュリティタスクの自動化により、インシデントに迅速に対応します。



Sentinel は脅威防止の統合機能を提供 (スライド 2)



Sentinel をデータに接続: Microsoft ソリューションのコネクタを使用してリアルタイムの統合を提供します。



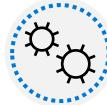
ワークブック: Azure Sentinel と Azure Monitor ワークブックを統合してデータを監視します。



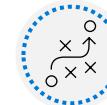
分析: 組み込み分析アラートを使用して、疑わしいことが発生した場合は通知を受けるようにします。



インシデント管理: インシデントは、有効にしたアラートがトリガーされたときに作成されます。



セキュリティの自動化とオーケストレーション: Azure Logic Apps と統合してワークフローを作成



プレイブック: 応答を自動化して調整する際に役立つ手順のコレクション。



調査: 潜在的なセキュリティの脅威の範囲を把握して根本原因を見つけます。

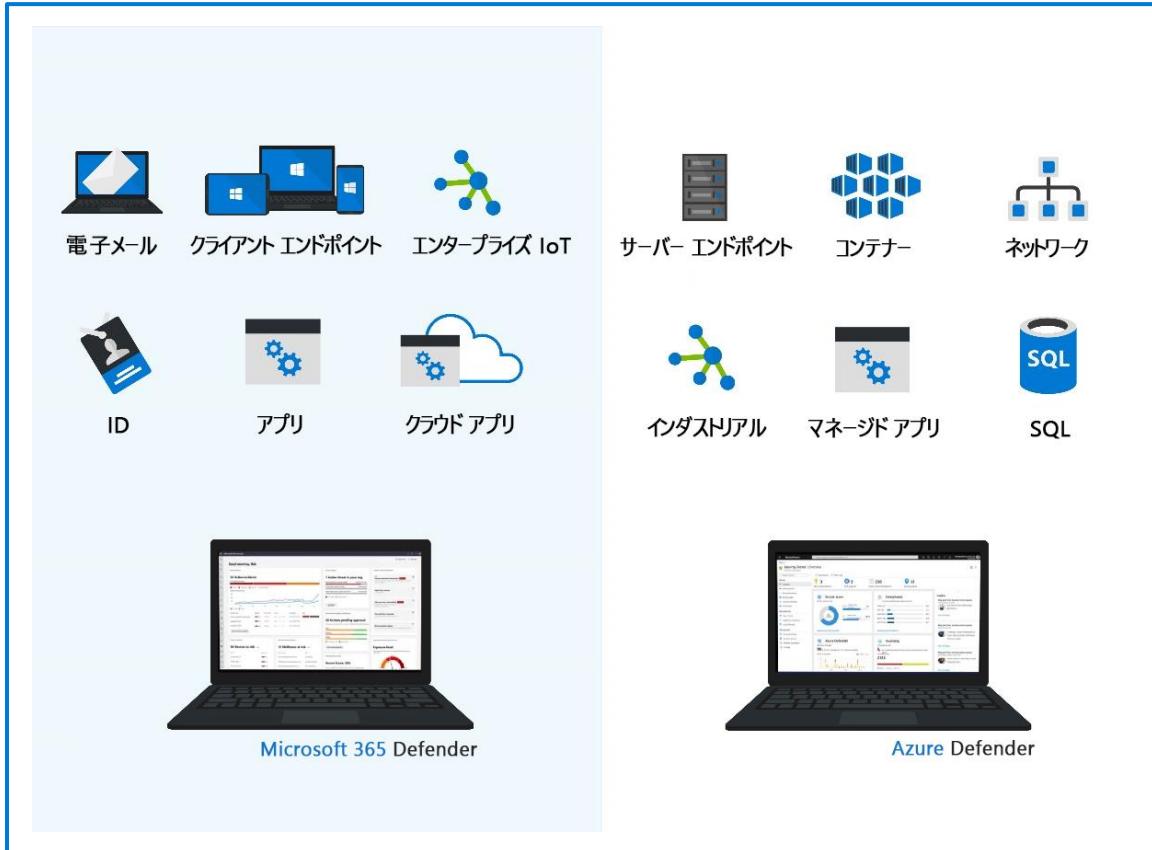


検索: 検索クエリ ツールを使用して、アラートがトリガーされる前に脅威をプロアクティブに探します。



統合された脅威の防止: XDR と Microsoft 365 Defender および Azure Defender の統合。

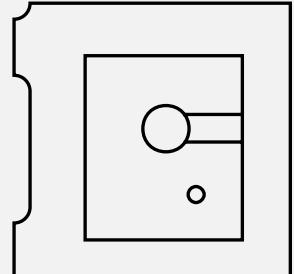
Sentinel は脅威防止の統合機能を提供 (スライド 3)





Microsoft セキュリティ ソリューションの機能について
説明する(Segment 2 of 2)

レッスン 4: Microsoft 365 Defender を使用した脅威に対する保護について説明する



レッスン 4 はじめに

このモジュールを完了すると、次のことができるようになります。



Microsoft Secure Score のについて説明する



Microsoft Secure Score のが高度な攻撃に対する統合保護機能を提供する方法を説明する



Microsoft Secure Score のデータと資産の保護に役立つ方法を説明する

Microsoft 365 Defender サービス

Microsoft 365 Defender



脅威の検出、防止、調査、応答をネイティブに調整します。



ID、エンドポイント、アプリ、電子メール、コラボレーションを保護します。

統合された Microsoft 365 Defender エクスペリエンス



ID

Microsoft Defender
for Identity



エンドポイント

Microsoft Defender
for Endpoint



アプリ

Microsoft Cloud
App Security

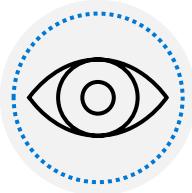


電子メール/コラボレーション

Microsoft Defender
for Office 365

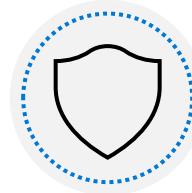
Microsoft Defender for Identity

Microsoft Defender for Identity は以下の主要な分野に対応します。



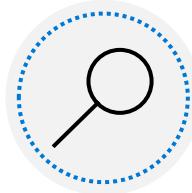
ユーザーの動作とアクティビティを監視してプロファイリングする

Microsoft Defender for Identity では、ネットワーク全体でユーザーのアクティビティと情報（アクセス許可やグループメンバーシップなど）が監視され、各ユーザーの行動ベースラインが作成されます。



ユーザーの ID を保護して攻撃面を減らす。

Defender for Identity では、ID 構成と推奨されるセキュリティのベストプラクティスに関する重要な分析情報が得られます。セキュリティレポートとユーザー プロファイルの分析を行います。



サーバー キル チェーン攻撃全体で不審なアクティビティと高度な攻撃を特定する

- 偵察
- 侵害された資格情報
- 横方向の移動
- ドメインの支配



アラートとユーザー アクティビティの調査

Defender for Identity は、一般的なアラート ノイズを減らすように設計されています。これにより、シンプルなリアルタイムの組織攻撃タイムラインで、関連のある重要なセキュリティアラートのみが提供されます。

Microsoft Defender for Office 365

Microsoft Defender for Office 365 の機能

1

脅威防止ポリシー

2

レポート

3

脅威の調査および対応機能

4

自動調査・対応機能

Microsoft Defender for Office 365 プラン 1

- 安全な添付ファイル
- 安全なリンク
- SharePoint、OneDrive、
Microsoft Teams 用の安全な添付ファイル
- フィッシング対策保護
- リアルタイムの検出

Microsoft Defender for Office 365 プラン 2

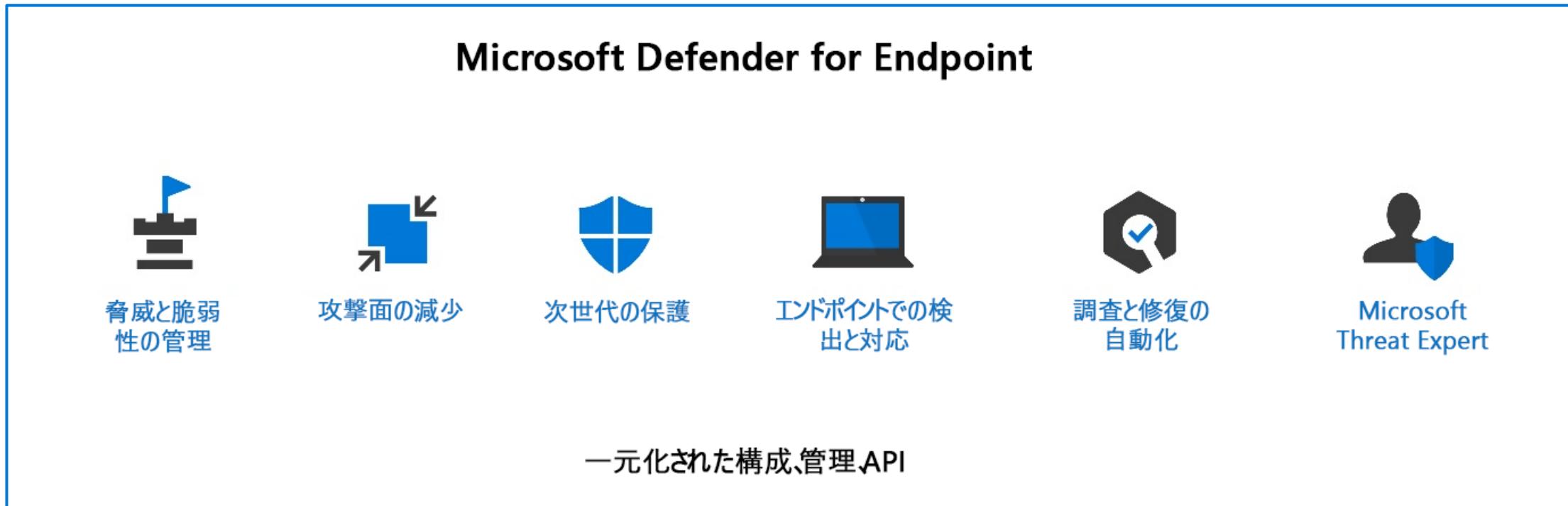
- 脅威トラッカー
- 脅威エクスプローラー
- 自動調査と
応答 (AIR)
- 攻撃シミュレーター

Microsoft Defender for Office 365 可用性

- Microsoft 365 E5
- Office 365 E5
- Office 365 A5
- Microsoft 365 Business Premium

Microsoft Defender for Endpoint

Microsoft Defender for Endpoint はエンタープライズ ネットワークがエンドポイントを保護できるよう設計されたプラットフォームです。



Microsoft Cloud App Security

Microsoft Cloud App Security では、すべての Microsoft およびサードパーティのクラウド サービスにわたってサイバーセキュリティを特定して対処するために、クラウド サービスへの豊富な可視性、データ移動の制御、高度な分析が提供されます。

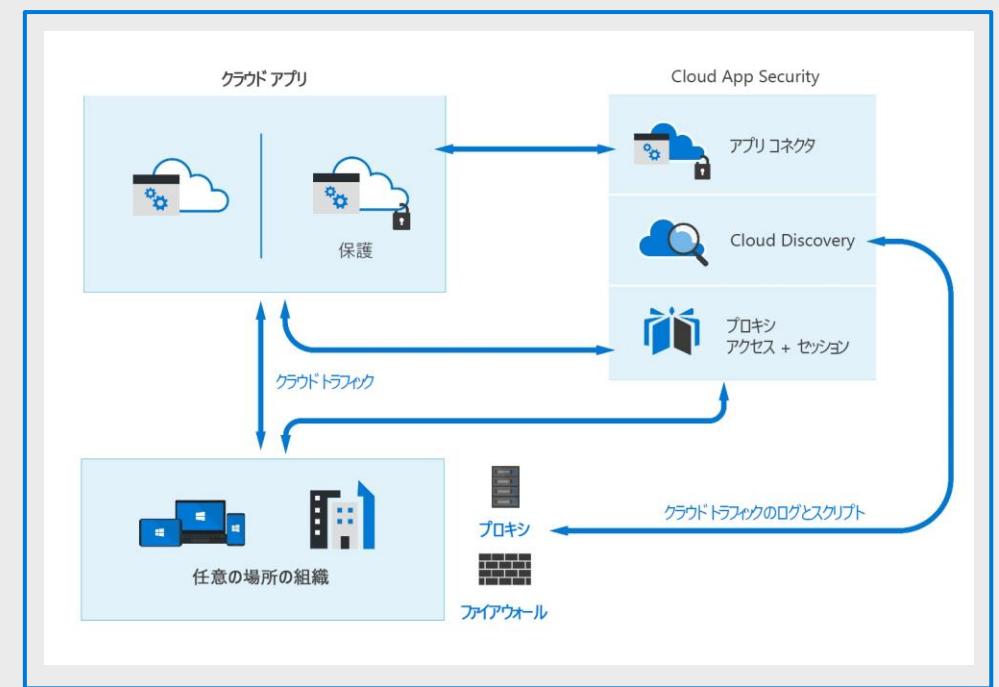
Cloud App Security フレームワーク

- ・シャドウ IT の使用を検出して制御する
- ・あらゆる場所で機密情報を保護する
(クラウド内)
- ・サイバーセキュリティと異常から保護する
- ・クラウド アプリのコンプライアンスを評価する

Office 365 Cloud App Security

Azure Active Directory の拡張 Cloud App Discovery

Microsoft Cloud App Security アーキテクチャ



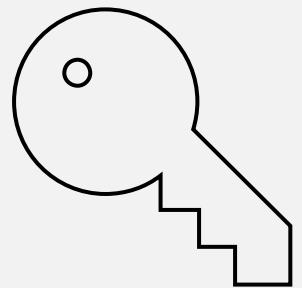


デモ

Microsoft Cloud App Security (MCAS)



レッスン 5: Microsoft 365 のセキュリティ管理機能 について説明する



レッスン 5 はじめに

このモジュールの内容は次のとおりです。



Microsoft 365
Defenderについて説明して探す
ポータル



Microsoft
Secure Score の
使用方法を説明
する。



セキュリティレポートとダッシュボード
を探す。



Microsoft 365
のインシデント管
理機能について
説明する。

Microsoft 365 Defender ポータル

Microsoft 365 Defender ポータルは、保護、検出、調査、電子メールへの対応、コラボレーション、ID、デバイスの脅威を中央ポータルに統合します。



組織のセキュリティの状態を表示します。

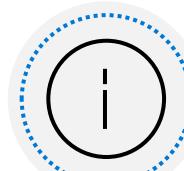


デバイス、ユーザー、アプリを設定するために行動します。



疑わしいアクティビティのアラートを取得します。

Microsoft 365 Defender ナビゲーション ペインには、次のオプションなどが含まれています。



インシデント & アラート



検出



アクション center



脅威分析



セキュリティ保護スコア



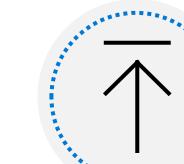
学習ハブ



エンドポイント



メール & コラボレーション



レポート



アクセス許可 & ロール

Microsoft セキュア スコアの使用方法について説明する

Microsoft セキュア スコアは、会社のセキュリティ体制を示します。

ライセンスのエディションやサブスクリプション、プランに関わらず、製品で可能な改善点がすべて表示されます。

以下に対する推奨事項をサポートします。

- Microsoft 365
- Azure Active Directory
- Microsoft Defender for Endpoint
- Microsoft Defender for Identity
- Cloud App Security



デモ

Microsoft 365 Defender ポータル



セキュリティレポートとダッシュボード

Microsoft 365 Defender ポータルには、レポートセクションが含まれています。以下に示すのは、一般的なセキュリティレポートです。

既定では、次のカテゴリにグループ化されています。

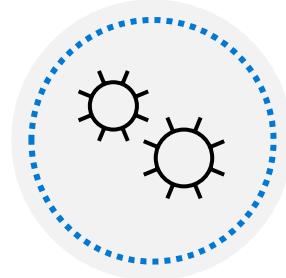
- **ID** - ユーザー アカウントと資格情報。
- **データ** - 電子メールとドキュメントのコンテンツ。
- **デバイス** - コンピューター、携帯電話、その他のデバイス。
- **アプリ** - プログラムおよび付随オンラインサービス。

カードはトピック別にグループ化できます（リスク、検出の傾向、構成と正常性、その他）。

The screenshot shows the Microsoft 365 Security Report dashboard for Contoso Electronics. The left sidebar lists navigation items: Home, Incident & Alert, Pursue, Action Center, Threat Analysis, Security Score, Learning Hub, Mail & Collaboration, Investigation, Explorer, Application, Confirmation, Attack Activity, Threat Tracker, Exchange Message Tracking, Attack Simulation Training, Policy & Rule, Reports, and Audit. The main content area is titled "Report" and displays sections for "ID", "Data", and "Devices". The "ID" section shows 0 users at risk. The "Data" section shows the user with the most shared files and users sharing files from cloud apps. The "Devices" section shows administrators being reduced. A red box highlights the "ID" section, another red box highlights the "Data" section, and a third red box highlights the "Devices" section. A fourth red box highlights the "Category Grouping" dropdown in the top right corner.

ID およびインシデント管理

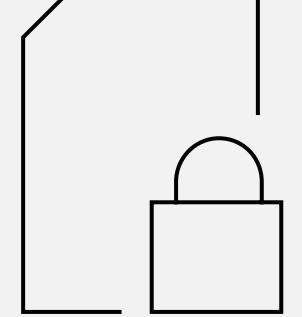
インシデントは、疑わしいイベントが見つかった場合に作成され、攻撃の包括的なビューとコンテキストを提供する相関関係のあるアラートのコレクションです。



インシデント管理

インシデントの管理は、脅威を確実に抑制して対処する際に重要です。Microsoft 365 Defender では、デバイス、ユーザー アカウント、およびメールボックスでインシデントを管理できます。

レッスン 6: Microsoft Intune でのエンドポイントのセキュリティについて説明する



レッスン 6 概要

このモジュールを終了すると、次のことができるようになります。



Intune とは
何か説明する。



Intune で利用でき
るツールを説明する。



Microsoft
Endpoint
Manager
を使用してデバイスを
管理する方法を説
明する。

Intune

Microsoft Intune は、モバイル デバイス管理 (MDM) とモバイル アプリケーション管理 (MAM) に焦点を当てたクラウドベースのサービスです。



Intune でデバイスを登録して管理すると、管理者は次の操作を実行できます。

- 登録されたデバイスを確認し、組織のリソースにアクセスしているデバイスのインベントリを取得します。
- デバイスがセキュリティと正常性の基準を満たすように構成します。
- ユーザーが Wi-Fi ネットワークに簡単にアクセスできるように証明書をデバイスにプッシュするか、VPN を使用して接続する。
- ユーザーとデバイスに関するレポートを表示し、準拠しているかどうかを確認する。
- デバイスが紛失、盗難、または使用されなくなった場合は、組織のデータを削除します。



Intune でアプリを管理すると、管理者は次の操作を実行できます。

- モバイル アプリを追加して、ユーザー グループとデバイスに割り当てます。
- 特定の設定を有効にしてアプリを起動または実行するように構成し、デバイスに既に存在するアプリを更新する。
- どのアプリが使用されているかに関するレポートを表示し、その使用状況を追跡します。
- アプリから組織データのみを削除して選択的なワイプを行います。

Intune のエンドポイントセキュリティ

デバイスの管理

ポリシーを使用してデバイスのセキュリティを管理

セキュリティベースラインの管理

デバイスのコンプライアンスポリシーを使用

Microsoft Intune でのロールベースのアクセス制御

条件付きアクセスの構成

- デバイスベースの条件付きアクセスにより、準拠している管理対象デバイスのみがネットワークのリソースにアクセスできるようにします。
- アプリベースの条件付きアクセスにより、Intune で管理されていないデバイスのユーザーによるネットワークリソースへのアクセスを管理できます。

Microsoft Defender for Endpointとの統合

- Android
- iOS/iPadOS
- Windows 10 以降

モジュールのまとめ

このモジュールでは、次のことを行いました。

- Microsoft 365 Defender とそのコンポーネント ソリューションによる脅威の保護について学習しました。Microsoft Defender for Identity、Microsoft Defender for Endpoints、MCAS、Microsoft Defender for Office365。
- Microsoft 365 Defender ポータルと Secure Score を使用した Microsoft 365 のセキュリティ管理機能について学習しました。
- Microsoft Intune について学習しました。



Microsoft コンプライアンス ソリューションの機能について説明する

モジュール の議題



Microsoft のコンプライアンス管理機能について説明する



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



Microsoft 365 のインサイダー リスク機能について説明する



電子情報開示および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

レッスン 1: Microsoft のコンプライアンス管理機能について説明する



レッスン 1 はじめに

このモジュールを修了すると、次のことができるようになります。

- Service Trust Portal の利点について説明します。
- Microsoft のプライバシー原則について説明する。
- Microsoft 365 コンプライアンス センターを詳細に確認する。
- コンプライアンス マネージャーの利点について説明する。

一般的なコンプライアンス ニーズ

データを保護するための複数の手段:



自身のデータについてもアクセスできる権限を個人に付与する。



自身に関するデータを必要に応じて修正または削除できる権限を個人に付与する。



データの最低または最高保持期間を導入する。



必要に応じてデータにアクセスして調査する権限を政府および規制機関に与える。



処理できるデータとその実行方法に関する規則を定義する。

Service Trust Portal

Service Trust Portal は以下を提供します。

- Information
- ツール
- Microsoft のセキュリティ、プライバシー、コンプライアンスの実践に関する他のリソース

以下にアクセスできます。

- Service Trust Portal
- コンプライアンス マネージャー
- 信頼性関連ドキュメント
- 業界および地域
- セキュリティ センター
- リソース
- マイ ライブラリ

Microsoft のプライバシーに関する原則



制御: 使いやすいツールと明確な選択肢で、お客様が自らのプライバシーを制御できるようにします。



透明性: 誰でも情報に基づいた意思決定を行えるようにするために、データの収集と使用の透明性を維持します。



セキュリティ: 強力なセキュリティと暗号化を使用して Microsoft に委託されたデータを保護します。



強力な法的保護: 現地のプライバシー法を尊重し、基本的な人権としてのプライバシーの法的保護に取り組みます。



コンテンツベースのターゲット設定なし: メール、チャット、ファイル、その他の個人的なコンテンツを使用したターゲティング広告を行いません。



お客様の利益: Microsoft が収集したデータはお客様に利益をもたらし、お客様の経験を向上させるために使用されます。



デモ

Service Trust Portal



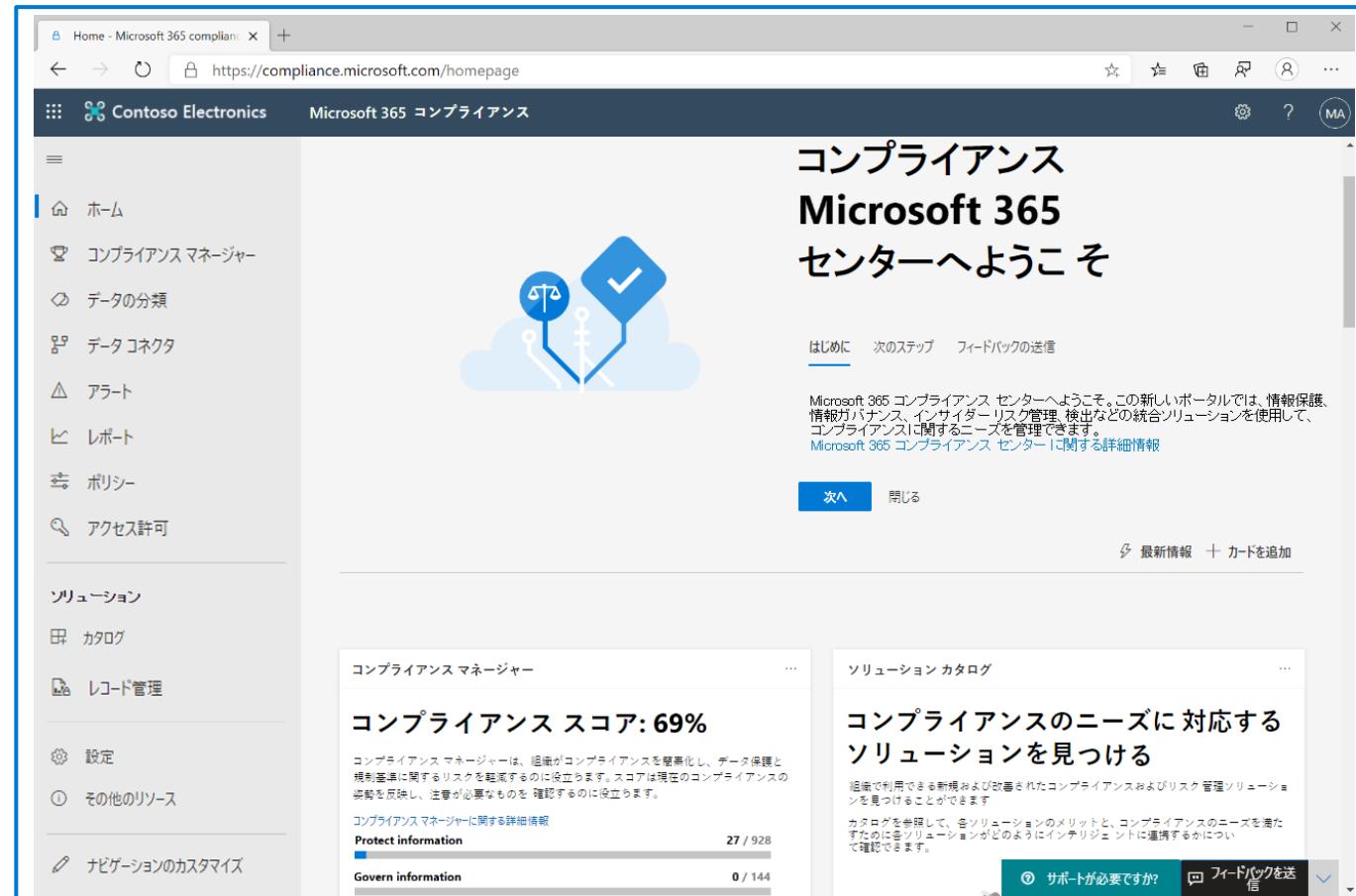
Microsoft 365 コンプライアンス センター

Microsoft 365 コンプライアンス センター ポータル

- 組織がコンプライアンス法権を満たす方法を表示したビュー
- コンプライアンスを支援するために使用できるソリューション
- 警告に関する情報
- そして他にも...

ナビゲーション

- アラート、レポート、ポリシー、コンプライアンス ソリューションなどにアクセスする。
- カスタマイズされたナビゲーション ウィンドウのオプションを追加または削除する。
- ナビゲーション コントロールをカスタマイズする。



コンプライアンス マネージャー

コンプライアンス マネージャーは以下を提供することでコンプライアンスを簡素化してリスクを減らします。

- 一般的な標準に基づく事前構築済みの評価
- リスク評価を完了するためのワークフロー機能
- 詳細な改善処置
- 全体的なコンプライアンス体制を示すコンプライアンス スコア

コンプライアンス マネージャーの主要要素

- 統制
- 評価
- テンプレート
- 改善活動



コンプライアンス スコア

コンプライアンス スコアの利点:

- 組織は最新のコンプライアンス体制を把握できます。
- リスクを低減する可能性に基づいて組織が処置に優先順位を付けられます。

コンプライアンス スコアの概要

- アクション
 - 改善された処置
 - Microsoft の処置
- 処置のタイプ (および処置のサブカテゴリ)
 - 必須 (予防、検知、または是正)
 - 裁量的 (予防、検知、または是正)





デモ

Microsoft 365 コンプライアンス センター



レッスン 2: Microsoft 365 の情報保護とガバナンス の機能について説明する



レッスン 2 はじめに

このモジュールを修了すると、次のことができるようになります。

- データ分類機能について説明する。
- レコード管理について説明する。
- データ損失の防止について説明する。

データについて理解し、データを保護し、データを管理する



データの把握: データの全体像を把握し、オンプレミス、クラウド、ハイブリッド環境で重要なデータを特定します。



データを保護します。暗号化、アクセス制限、視覚的なマーキングなどの柔軟な保護アクションを適用します。



データ損失防止: 危険な行動を検出し、機密情報の偶発的な共有過剰を防止します。



データの管理: 準拠した方法でデータとレコードを自動的に維持、削除、格納します。



Microsoft 365 コンプライアンス センターのデータ分類機能



機密情報の種類



トレーニング可能な分類器: 事前にトレーニングされた分類器とトレーニング可能なカスタム分類器



データの把握と確認



コンテンツ エクスプローラー: 管理者はそれを使用して、概要ペインに要約されているコンテンツを詳しく調べることができます。



アクティビティ エクスプローラー: 組織全体でラベルの付いたコンテンツを使用して何が行われているのか監視できます

秘密度ラベルとポリシー

秘密度ラベル

次のようなラベルがあります。

- カスタマイズ可能
- クリア テキスト
- 永続的

用途:

- 電子メールとドキュメントを暗号化します。
- コンテンツにマークを付けます。
- ラベルを自動的に適用します。
- サイトやグループなどコンテナー内のコンテンツを保護します。
- サードパーティのアプリやサービスに秘密度ラベルを拡張します。
- 保護設定を使用せずにコンテンツを分類します。

ラベル ポリシー

ポリシーを使用すると管理者は以下を実行できます。

- ラベルを表示できるユーザーとグループを選択する
- 新しい電子メールとドキュメントすべてに既定のラベルを適用する
- ラベル変更の根拠を説明するよう求める
- ラベルを適用するようユーザーに求める(必須ラベル)
- ユーザーをカスタム ヘルプ ページに関連付ける

メールまたはドキュメントに秘密度ラベルが適用されると、そのラベルに構成されている保護設定がコンテンツに適用されます。

デモ

秘密度ラベル



データ損失防止 (DLP) について説明する

DLP は機密情報を保護し、不注意による開示を防ぎます。

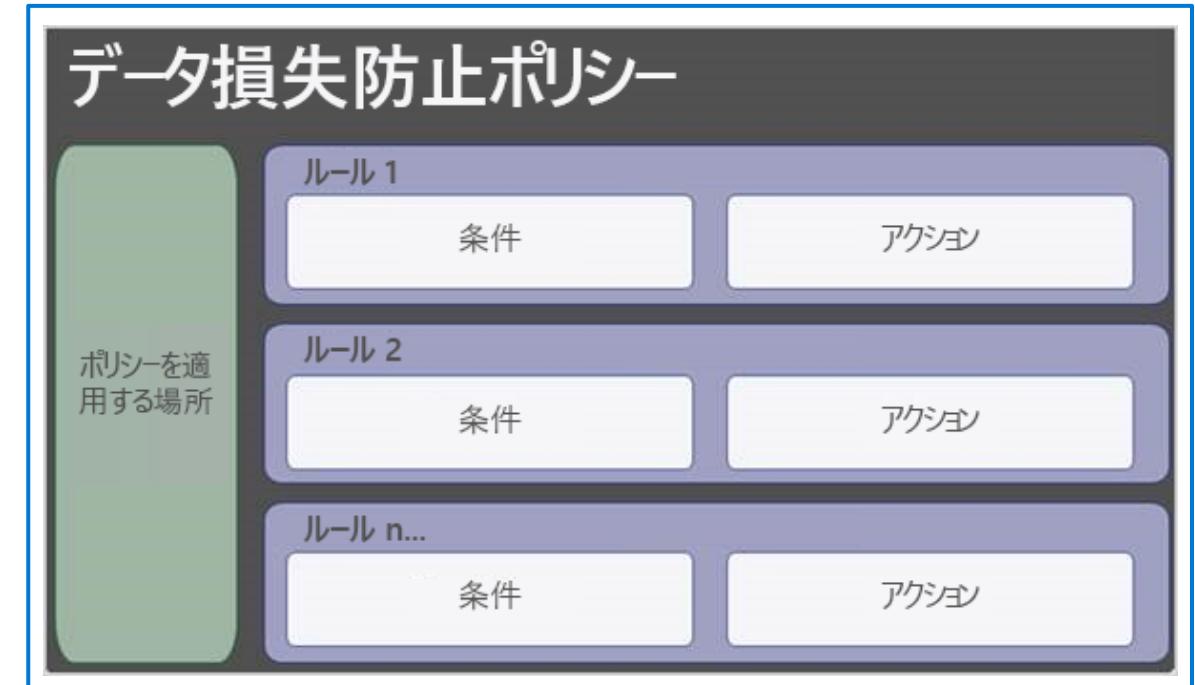
- DPL ポリシーを使用し、機密データを識別して自動的に保護することにより、情報を保護します。
- Microsoft 365 – OneDrive for Business、SharePoint Online、Exchange Online、Microsoft Teams 全体で機密情報を保護します

エンドポイントのデータ損失防止

- DLP は Windows 10 デバイスに拡張されました。
- 項目の作成、対処、印刷、名前の変更などのアクティビティを監査および管理する

Microsoft Teams でのデータ損失防止

- DPL 機能は Microsoft Teams のチャットとチャネル メッセージに拡張されました。



保持ポリシーと保持ラベル

保持期間の設定は SharePoint、OneDrive、Teams、Yammer、Exchange で利用できます。コンテンツが必要な期間のみ維持され、その後は恒久的に削除されるようにすることで組織が情報を管理して監督できるようにします。

保持ポリシー

- サイトまたはメールボックス レベルで適用されます。
- 複数の場所や具体的な場所またはユーザーに適用できます。
- 項目はコンテナーから保持期間の設定を継承します。
- 項目が移動されると、保持期間の設定は新しい場所に移りません。

保持ラベル:

- 項目レベルで適用されます。
- 電子メールとドキュメントが一度に保有できるのは、割り当てられた単一の保持ラベルのみです。
- 保持ラベルの保持設定は、Microsoft 365 テナントのコンテンツと一緒に移動します。
- 手動または自動で適用できます。
- 保持ラベルは、コンテンツが完全に削除される前のコンテンツの廃棄レビューをサポートします。

レコード管理

Microsoft 365 のレコード管理は、組織が自らの法的な義務に配慮できるよう支援し、規制を遵守していることを示す上で役立ちます。

- コンテンツがレコードとしてラベル付けされている場合、次のことが行われます。
 - 特定のアクティビティをブロックするための制限が実施されます。
 - アクティビティがログに記録されます。
 - 保持期間の終了時に、廃棄の証明が残されます。
- 項目にレコードとしてマークを付けるため、管理者は保持ラベルを設定します。

保持期間中

- ユーザーが削除してもアイテムを保持する

- アイテムをレコードとしてマークする

ユーザーは電子メールの編集や削除ができなくなり特定のユーザーのみがラベルの変更や削除ができるようになります。SharePoint や OneDrive のファイルを削除することはできませんがアイテムのレコードの状態がロックされているかロック解除されているかによって他の操作がブロックまたは許可されます。[詳細情報](#)

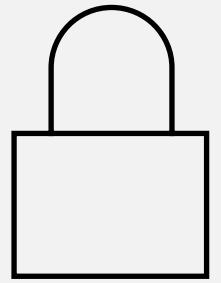
- アイテムを規制レコードとしてマークする

保持期間の終了時

- アイテムを自動的に削除する

現在保存されている場所からアイテムを削除します。

レッスン 3: Microsoft 365 のインサイダー リスク機能について説明する



レッスン 3 はじめに

このモジュールを修了すると、次のことができるようになります。

- 重大なインサイダー・リスクを組織が特定し、適切なアクションを実行するために Microsoft 365 がどのように役立つかを説明する。

Microsoft 365 のインサイダー リスク ソリューション (スライド 1)



インサイダー リスク管理は、組織内の悪意のある不注意なアクティビティを検出、調査、対処できるようにすることで、内部リスクを最小限に抑えるのに役立ちます。



通信コンプライアンスは、組織内の不適切なメッセージを検出、キャプチャ、処理するのに役立つため、通信リスクを最小限に抑えるのに役立ちます。サポートされるサービス: Microsoft Teams、Exchange Online、Yammer、組織内のサードパーティの通信。



情報バリアを使用すると、2つの内部グループ間の通信とコラボレーションを制限して、組織内で利益相反が発生するのを防ぐことができます。Microsoft Teams、OneDrive for Business、SharePoint Online などでサポートされています。

Microsoft 365 のインサイダー リスク ソリューション (スライド 2)

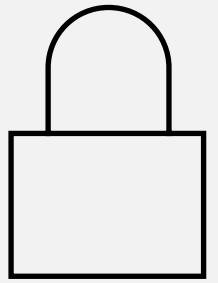


特権アクセス管理により、Office 365 の特権 Exchange Online 管理タスクに対するきめ細かいアクセス制御が可能になります。



カスタマー ロックボックスは、Microsoft が顧客のコンテンツにアクセスして、顧客の情報なしにサービス操作を実行できないようにします。サポートされるサービス: Exchange Online、SharePoint Online、OneDrive for Business。

レッスン 4: 電子情報開示および監査機能について 説明する



レッスン 4 はじめに

このモジュールを修了すると、次のことができるようになります。

- 電子情報開示の目的とコンテンツ検索ツールの機能について説明する。
- コアおよび高度な電子情報開示ワークフローについて説明する。
- Microsoft 365 のコアおよび高度な監査機能について説明する。

電子情報開示と検索

電子情報開示の目的

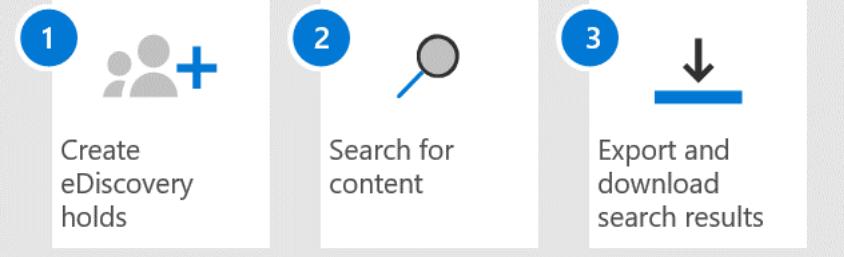
- ・ 会社が訴訟に関わった際、証拠として使用できる電子情報を検索します。
- ・ Exchange Online メールボックス、Microsoft 365 グループ、Microsoft Teams、SharePoint Online、OneDrive for Business サイト、Skype for Business の会話、Yammer チームでコンテンツを検索します。
- ・ メールボックスとサイトで見つかったコンテンツの識別、保持、エクスポートに使用します。

コンテンツ検索

- ・ Exchange Online メールボックス、SharePoint Online サイト、OneDrive for Business、チーム、Microsoft 365 グループ、Yammer グループを検索する
- ・ 検索クエリを構築して条件を使用
- ・ 複数の検索を作成、報告、削除
- ・ キーワードの統計情報を表示
- ・ サードパーティのデータを検索
- ・ より複雑な検索関連タスク用の PowerShell スクリプト

コアおよび高度な電子情報開示ワークフロー

Core eDiscovery workflow



Advanced eDiscovery ワークフロー



コア電子情報開示

1. ケースに関連する可能性のあるコンテンツ（メールボックス、サイト、パブリック フォルダー）を保持するためにホールドを作成します。
2. ケースに関連するコンテンツの検索を作成および実行します。
3. 検索結果をエクスポートし、ダウンロードします。

高度な電子情報開示はコア電子情報開示に基づいています

1. 特定のユーザーに関連付けられていない関係者（カストディアン）とデータソースを追加します。
2. 組み込みコレクション ツールを使用して、ケースに関連するコンテンツのデータソースを検索します。
3. レビュー セットに追加されたデータは、元の場所から安全な Azure Storage の場所にコピーされます。高速検索用に最適化するために、データのインデックスが再度作成されます。
4. さまざまなツールと機能を使用して、ケース データを表示および分析し、データ セットをケースに最も関連性のあるものに削減することを目標とします。
5. ケース データをエクスポートしてダウンロードする

Microsoft 365 の監査機能

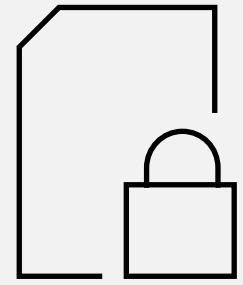
コア監査

- 組織がユーザーと管理者のアクティビティを把握できるようになります。
- 監査されたアクティビティから監査レコードが生成され、これは監査ログに保存されます。
- 監査ログを検索するには、検索機能を有効にして適切なロールを割り当てる必要があります。
- 結果はフィルタリングされ、CSV ファイルにエクスポートされます。

高度な監査 - コア監査、加えて:

- 監査ログの長期保有
- Office 365 マネージメント アクティビティ API への高帯域幅アクセス
- 調査のための重要なイベントへのアクセス
 - MailItemsAccessed
 - 送信
 - SearchQueryInitiatedExchange
 - SearchQueryInitiatedSharePoint

レッスン 5: Azure のリソース ガバナンス機能について 説明する



レッスン 5 はじめに

このモジュールを修了すると、次のことができるようになります。

- Azure のリソース ガバナンス機能のいくつかについて説明する。

Azure Resource Manager ロック

Azure Resource Manager ロック

- リソースが誤って削除または変更されるのを防ぎます。
- 親スコープでロックを適用すると、そのスコープ内のすべてのリソースは同じロックを継承します。
- 管理プレーンで発生している操作にのみ適用されます。
- 実際のリソースの変更は制限されますが、リソースの操作は制限されません。

ロック レベル

- CanNotDelete
- ReadOnly

Azure Blueprints

- Azure Blueprints は、Azure リソースの反復可能なセットを定義する方法の 1 つです。
- 組織のコンプライアンス要件を満たす環境をすみやかに提供します。
- 複数のサブスクリプションで同時に Azure リソースを提供してすばやく届けられるようにします。
- 以下を含むさまざまなリソース テンプレートやアーティファクトのデプロイを宣言によって調整する手法です。
 - ロールの割り当て
 - ポリシーの割り当て
 - Azure Resource Manager テンプレート (ARM テンプレート)
 - リソース グループ
- ブループリント オブジェクトは複数の Azure リージョンにレプリケートされます。
- ブループリントの定義とブループリントの割当の関係は維持されます。

Azure Policy

関数:

- Azure Policy は、標準の施行を支援し、組織全体でコンプライアンスを評価するよう設計されています。
- コンプライアンス ダッシュボードを使用して、環境の全体的な状態を評価するために役立つ集計ビューにアクセスできます。
- Azure Policy の一般的なユースケースには、リソースの整合性、規制コンプライアンス、セキュリティ、コスト、管理のガバナンスの実装が含まれています。
- Azure Policy は、Azure 内のすべてのリソースと Arc 対応リソース (Azure の外部でホストされている特定のリソースの種類) を評価します。

ポリシーの評価は以下によってトリガーできます。

- ポリシー割り当てのスコープでリソースが作成、削除、更新されています。
- ポリシーまたはイニシアチブが新しくスコープに割り当てられる。
- スコープに割り当てられたポリシーまたはイニシアチブが更新される。
- 標準のコンプライアンス評価サイクル (24 時間ごとに発生)。

非準拠リソースへの応答の例

- リソースへの変更を拒否する。
- リソースへの変更をログに記録する。
- 変更の前または後にリソースを修正する。
- 準拠している関連リソースをデプロイする。

デモ

Azure Policy



モジュールのまとめ

このレッスンでは、次の内容を学習しました。

- Service Trust Portal、Microsoft 365 コンプライアンス センター、Microsoft プライバシー原則など、Microsoft のコンプライアンス管理機能について学習しました。
- 機密性と保持ラベル、DLP など、Microsoft 365 の情報保護およびガバナンス機能について学習しました。
- Microsoft 365 のインサイダー リスク機能について学習しました
- Microsoft 365 の電子情報開と監査機能について学習しました
- Azure ポリシー、リソース ロック、ブループリントなど、Azure のリソース ガバナンス機能について説明します。