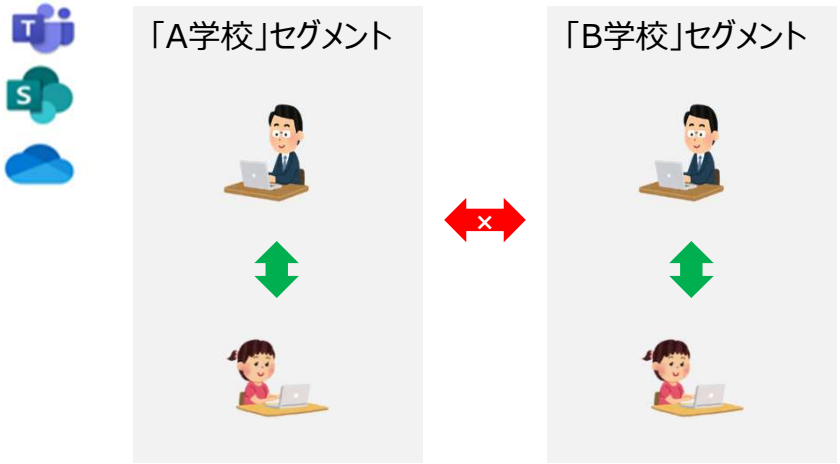
情報バリアポリシー

情報バリア（IB）ポリシーとは

- Microsoft Purviewのデータセキュリティソリューションのひとつ
- 特定のユーザー、グループ間のコミュニケーションとコラボレーションを制限するソリューション
  ※同一テナント内での利用における情報制御で、異なるテナント間に跨るものではない
- Microsoft Teams、SharePoint Online、OneDrive for Businessでサポートされている
  （制限できるアクティビティは後述）

- 活用例
  A学校の教師・生徒同士は通信できるが、B学校の教師・生徒とは通信できない



情報バリア（IB）ポリシーとは

- 必要なライセンスは以下の通り

  ※Enterpriseプランと教育プランの差分に注意（EnterpriseプランはE5から、教育プランはA1から利用可）
  - Microsoft 365 E5/A3/A5
  - Office 365 E5/A1/A3/A5
  - Microsoft 365 E5/F5/A5 compliance
  - Microsoft 365 F5 security + compliance
  - Microsoft 365 A1 for device

- 情報バリア　バージョン1(v1)は2019年に Teams 向けに提供され、2023年3月にバージョン2(v2)が一般提供された

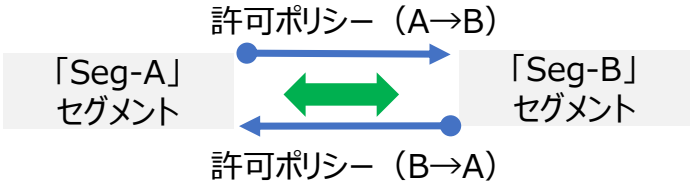
構成の概念

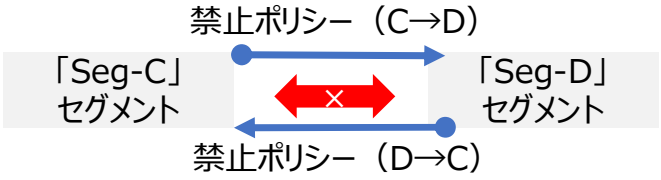
- セグメント

  Entra IDユーザの属性で定義されたグループ

- IBポリシー
  - 許可ポリシー：あるセグメントが他の特定のセグメントとのみ通信することを許可
  - 禁止ポリシー：あるセグメントと別のセグメントとの通信を禁止

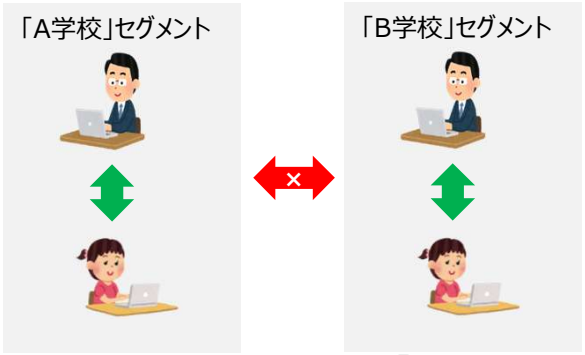
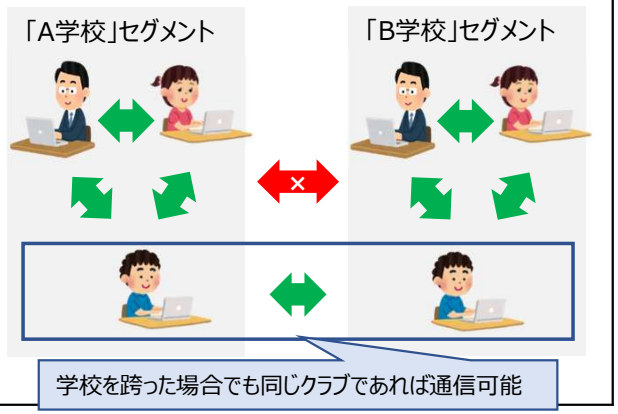
  各セグメントにはポリシーを1つだけ適用可能　※双方向にポリシーが必要、Targetを複数にすることは可能





v1とv2の違い

- 情報バリアポリシーのv1とv2の主な違いは、機能の拡張と柔軟性の向上

	v1	v2	
	レガシーモード	シングルセグメントモード	マルチセグメントモード
最大セグメント数	250	5,000	5,000
ユーザー割当てセグメント数	1	1	1～10
ポリシーの種類	許可ポリシー 禁止ポリシー	許可ポリシー 禁止ポリシー	許可ポリシー
Exchange Onlineとの統合	Exchange Onlineのアドレス帳ポリシー（ABP）に基づく	Exchange OnlineのABPに依存せず、より柔軟な設定が可能	
ユーザーの可視性	許可ポリシーに含まれるユーザーには、IB以外のグループやユーザーが表示されません	IB以外のグループやユーザーも表示されるようになります	
構成イメージ			

情報バリアと SharePoint と OneDrive

- SharePoint と OneDrive では、以下のアクティビティを制限できる
  - サイトへのメンバーの追加
  - ユーザーによるサイトまたはコンテンツへのアクセス
  - 別のユーザーとのサイトまたはコンテンツの共有
  - サイトの検索

情報バリアと Teams

- Microsoft Teams では、以下のアクティビティを制限できる
  - ユーザーの検索
  - チームにメンバーを追加する
  - 他のユーザーとのチャット セッションを開始する
  - グループ チャットを開始する
  - ユーザーを会議に招待する
  - 画面を共有する
  - 電話をかける
  - 別のユーザーとのファイルの共有
  - リンクの共有を介したファイルへのアクセス

情報バリアと Exchange Online

- IB ポリシーでは、メール メッセージ内のグループおよびユーザー間での通信と共同作業を制限することはできない
- メールの通信を定義および制御する必要がある場合には、Exchange メール フロー ルールの使用をご検討ください。

- v2（シングルセグメントモードおよびマルチセグメントモード）の場合
  - IBポリシーは Exchange Online アドレス帳ポリシー (ABP) に基づかない
  - ABP を使用している組織では、情報バリアを有効にしても既存の ABP には影響を与えない
  - 関連する IB セグメントとポリシーを持つユーザーに対して ABP が定義されていない場合、これらのユーザーのアドレス一覧が空欄になった ABP が自動的に作成される
  - ABP は、情報バリアで構成するセグメントに一致させることを推奨
- v1（レガシーモード）の場合
  - IB ポリシーは Exchange Online アドレス帳ポリシー (ABP) に基づく
  - IB ポリシーが作成されると、ABP が自動的に作成される
  - 既存の ABP ポリシーは IB によって作成された ABP との互換性がない
  - IB ポリシーを定義して適用する前に、所属している組織内の既存ABPをすべて削除する必要がある

懸念点

- 情報バリアを設定した状態であればTeams内においては対象セグメントをブロックした際に
  対象セグメントに存在するユーザの検索は行えない状態となるがMicrosoft 365上では検索が可能である。
  以下の手順において回避策は講じる事は行えるが管理者含め対象ユーザの検索が不可能となる為、注意が必要
  ※SharePoint のひと検索と使用されている仕組みは同じであるため、
  本設定を有効にすることで Microsoft 365 の検索ウインドウからの検索も制限できる

◆ 1.AD 同期をご利用の場合

- オンプレミス側で "msExchHideFromAddressList" が $True に設定されているユーザーは、ひと検索に表示されなくなる動作となることを公開情報より確認しております。

◆ 2. AD 同期を未利用の場合

- Azure AD のコマンドとなりますが、AD 同期を利用されていない環境では以下とおり Set-AzureADUser にて ShowInAddressList を $False に設定することで Microsoft365 の検索ウインドウからの検索にもヒットしない動作となることを確認いたしました。
- PS> Set-AzureADUser -ObjectId "アカウント(例:gakuseiA@XX.onmicrosoft.com)" -ShowInAddressList $false;

設定が反映されるまで、約半日程度を見込んでおります。

(最長で 2、3日ほど時間を要した事例も確認しております。)

※テナント内の全アカウントを検索対象から除外したい場合には、全アカウント分を１ユーザ毎にコマンドレットでコマンド投入する必要があります。