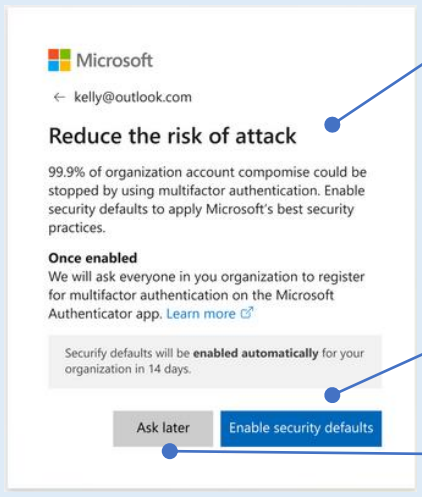
2022 年 6 月より

一部のテナントで「セキュリティの既定値」の有効化 が始まります

テナント管理者に対し、ポップアップが表示されます



ポップアップ
対象となったテナントに対して、管理者がサインインを行うと、「攻撃のリスクを軽減しましょう」という内容が書かれた案内が表示されます

[セキュリティ既定値の有効化] ボタン
テナントに対して「セキュリティ既定」の機能が有効化されます

[Ask Later] ボタン
2 日後にあらためて通知します

管理者は 14 日以内に対応をお願いします

1. **[セキュリティ既定値の有効化] ボタン** を押し、すぐに有効化
2. **[Ask Later] ボタン** を押し、あらためて検討

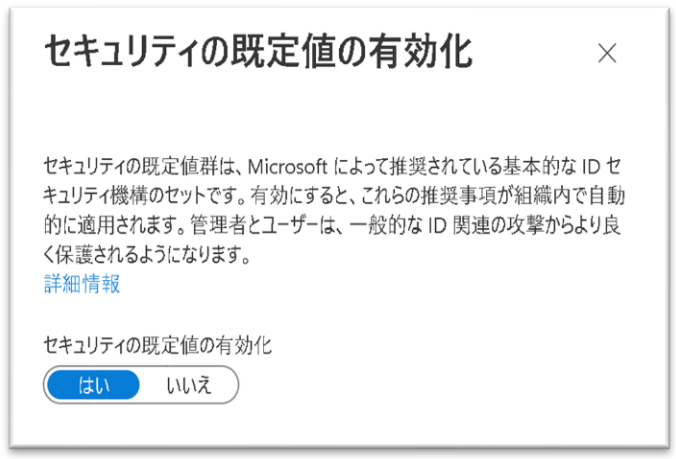
有効化しない場合

3. 一度、**[有効化] ボタン** を押し、その後 **[プロパティ]** にて無効化

対象となるテナント

- 2019 年 10 月以前に作成
- 「セキュリティの既定値」を使用したことがない
- 「条件付きアクセス 」を使用していない
- レガシー認証を積極的に使用していない

Azure AD「セキュリティの既定値」とは？



Azure ポータル > Azure Active Directory > プロパティ

- Azure AD Free に備わったセキュリティ機能
- Microsoft 推奨の ベースラインのセキュリティセット
- 主に認証強化のための 適切な多要素認証 適用
- テナント全体に対して、有効または無効の選択

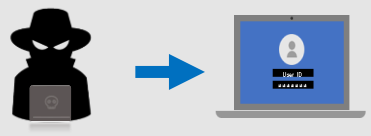
「セキュリティの既定値」を有効化した場合の設定・動作

1 Azure AD テナント内のすべての管理者、ユーザーに多要素認証の「登録」を必須化
※ Microsoft Authenticator アプリでの登録
14 日間登録を促し、以後サインインには登録が必要となります

2 管理者	3 ユーザー	4 レガシー認証	5 管理ポータル等
「常に」多要素認証要求	「必要に応じて」多要素認証要求	ブロック	「常に」多要素認証要求

多要素認証の重要性と「セキュリティの既定値」の有効化に至った背景

検証 1 : 侵害されたアカウント の分析



アカウント侵害にあったテナントは、
99.9% 以上が多要素認証未導入

多要素認証の効果

適切に多要素認証を導入することで、
単純な攻撃の 99% が防御可能

検証 2 : 有効化 テナントの実証

「セキュリティの既定値」を有効した組織は、
テナント全体の 80% 以上侵害が少ない

既に 2019 年10 月以降に作られたテナントでは既定で有効となっています
今回は 2019 年 10 月以前に作られたテナントに対しても、あらためてセキュリティ強化のご検討ください！

組織内のすべてのユーザーに対する多要素認証が難しい場合

① ユーザーごとに多要素認証を設定する

例 : 管理者や対象者のみ、多要素認証を都度要求

② 条件付きアクセスを利用する
※ Azure AD Premium P1

例 : 場所などの条件に応じて、多様認証を要求

多要素認証の設定におけるポイント

「セキュリティの既定値」の機能もしくは「条件付きアクセス」を利用することで、毎回ではなく必要に応じて多要素認証を要求するように設定することが可能です。

※ 2022 年 6 月 10 日時点の情報をもとに作成しています。今後動作や文言変更の可能性もありますのでご了承ください。

Raising the Baseline Security for all Organizations in the World (英語記事) | Microsoft Tech Community