Hardening Designers Conference 2026 Day2 Tech Showcase

Microsoft Entra ID/Microsoft 365を狙う同意フィッシング

2026年7月3日(金)

NEC サイバーセキュリティ技術統括部
フォレンジックアナリシスグループ
桐下　拓也

アジェンダ

1. はじめに
2. Microsoft Entra ID/Microsoft 365とは
3. 多要素認証を突破する攻撃
4. 同意とは
5. 同意フィッシング
6. 同意フィッシングデモ
7. 同意フィッシングへの対策
8. 【参考】ConsentFix
9. まとめ

1. はじめに

はじめに

Microsoft Entra ID/Microsoft 365を対象とした
同意フィッシング(Consent Phishing)という攻撃手法について
デモを交えながら紹介します
（関連攻撃手法ConsentFixについても参考として紹介）

注意事項

目的は、攻撃手法を知り、それをもとに
セキュリティ対策の強化に繋げていただくことです

本発表の内容を悪用しないでください

2. Microsoft Entra ID/Microsoft 365とは

Microsoft Entra ID/Microsoft 365とは

Microsoft Entra ID

Microsoft が提供する
ID およびアクセス管理の
ソリューション

OAuth 2.0：
認可のための仕組み
OpenID Connect：
OAuth 2.0を拡張した認証のための仕組み

ID/アクセス管理

出典：https://www.microsoft.com/ja-jp/security/business/identity-access/microsoft-entra-id

Microsoft 365

生産性向上のための
ソリューション

例：
Exchange Online、Teams、SharePoint等

参考：
https://learn.microsoft.com/ja-jp/entra/architecture/auth-oauth2
https://learn.microsoft.com/ja-jp/entra/architecture/auth-oidc

Microsoft Entra IDで使用される主なトークン

主なトークン

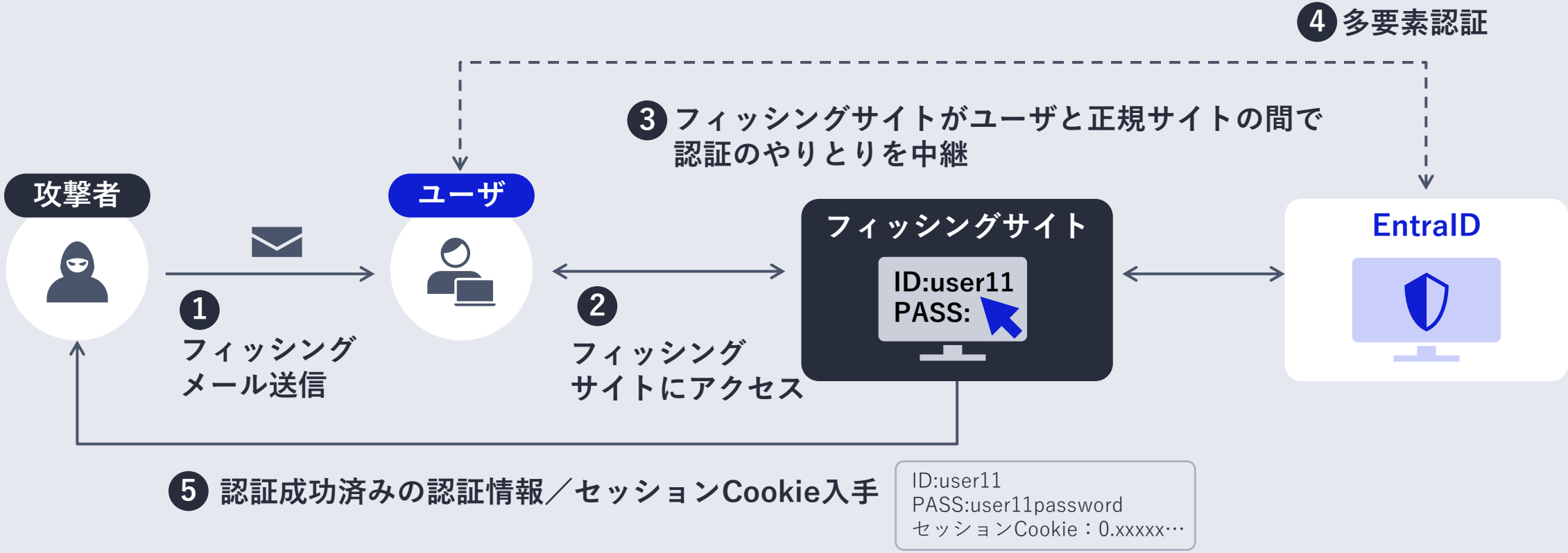
	アクセス トークン	リフレッシュ トークン	ID トークン
目的	APIアクセス	アクセストークン再取得	ユーザ認証
期限	60分~90分/120分	90日/24時間	60分
盗難影響	有効期間中対象APIへの不正アクセス	継続的にアクセストークンを再取得	一部アプリでなりすましログイン

参考：
https://learn.microsoft.com/ja-jp/entra/identity-platform/access-tokens
https://learn.microsoft.com/ja-jp/entra/identity-platform/refresh-tokens
https://learn.microsoft.com/ja-jp/entra/identity-platform/id-tokens

3.多要素認証を突破する攻撃

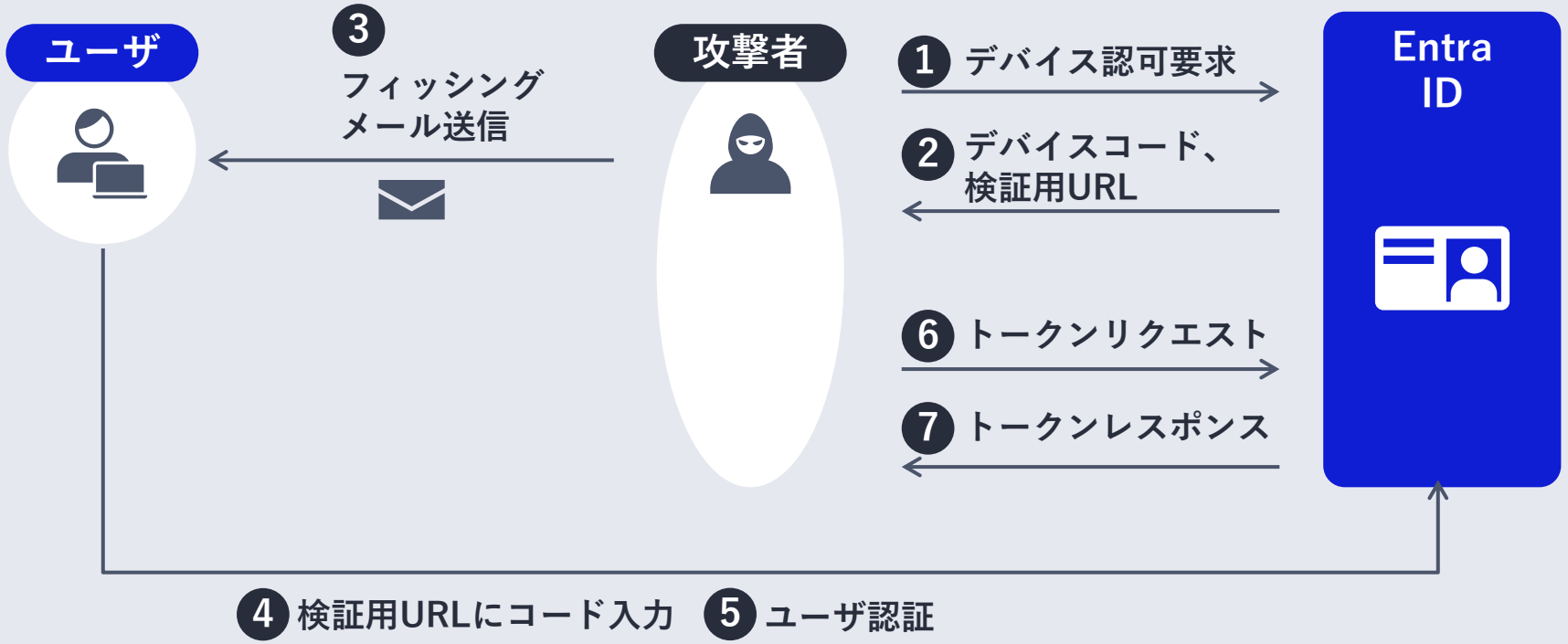
多要素認証を突破する攻撃(1/2)

従来のフィッシング(ID/Pass入手) + セッションCookie取得
例：AiTMフィッシング



多要素認証を突破する攻撃(2/2)

正規機能の悪用
例：デバイスコードフィッシング

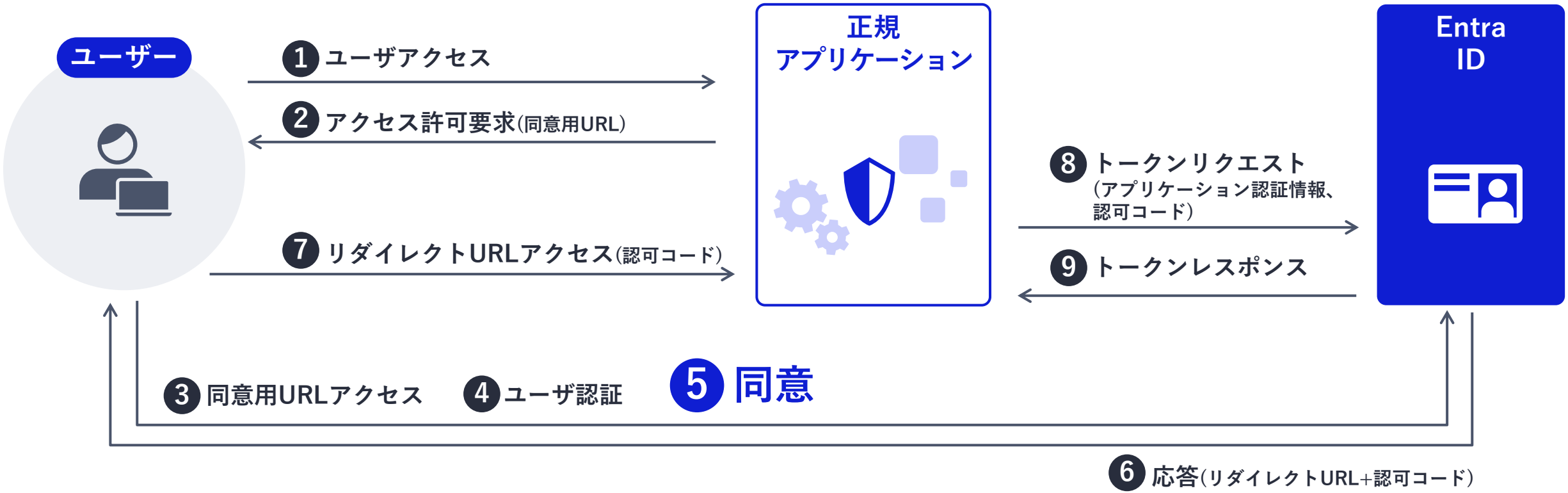


4.同意とは

同意とは(1/3)

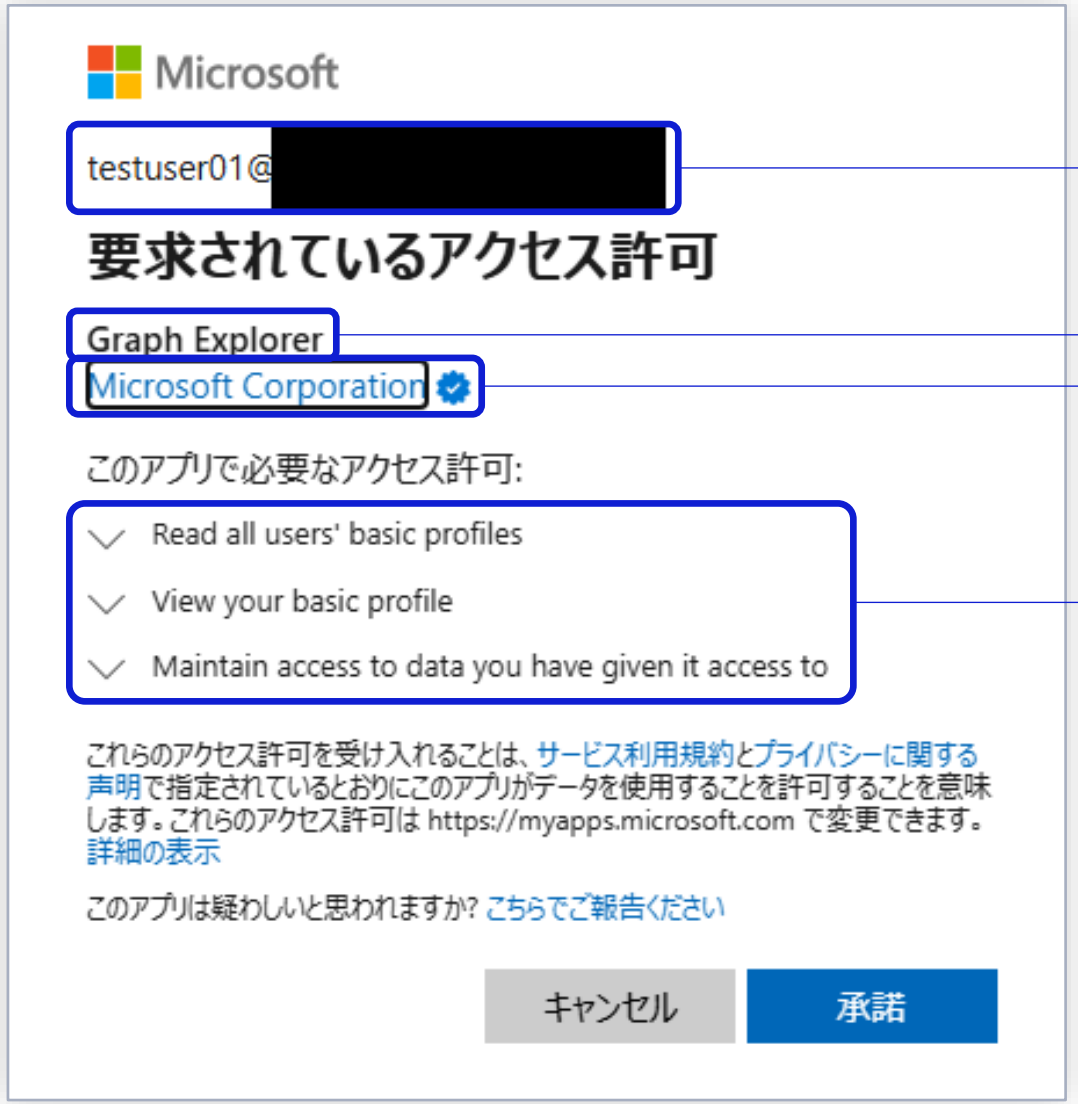
OAuth 2.0、OpenID Connectの認可コードフローを使用し、
アプリケーションが保護されたリソースにアクセスすることをユーザや管理者が許可するためのプロセス

参考：https://learn.microsoft.com/ja-jp/entra/identity-platform/v2-oauth2-auth-code-flow



同意とは(2/3)

同意画面の例



対象のユーザ

同意対象のアプリケーション名
同意対象のアプリケーションの発行元

同意対象のアプリケーションに対する
アクセス許可

同意とは(3/3)

同意に使用されるURL

同意用URL

https://login.microsoftonline.com
/common/oauth2/v2.0/authorize
?response_type=code
&client_id=“同意対象のアプリケーションID”
&scope=“アクセス許可”
&redirect_uri=“リダイレクトURL”
&response_mode=query

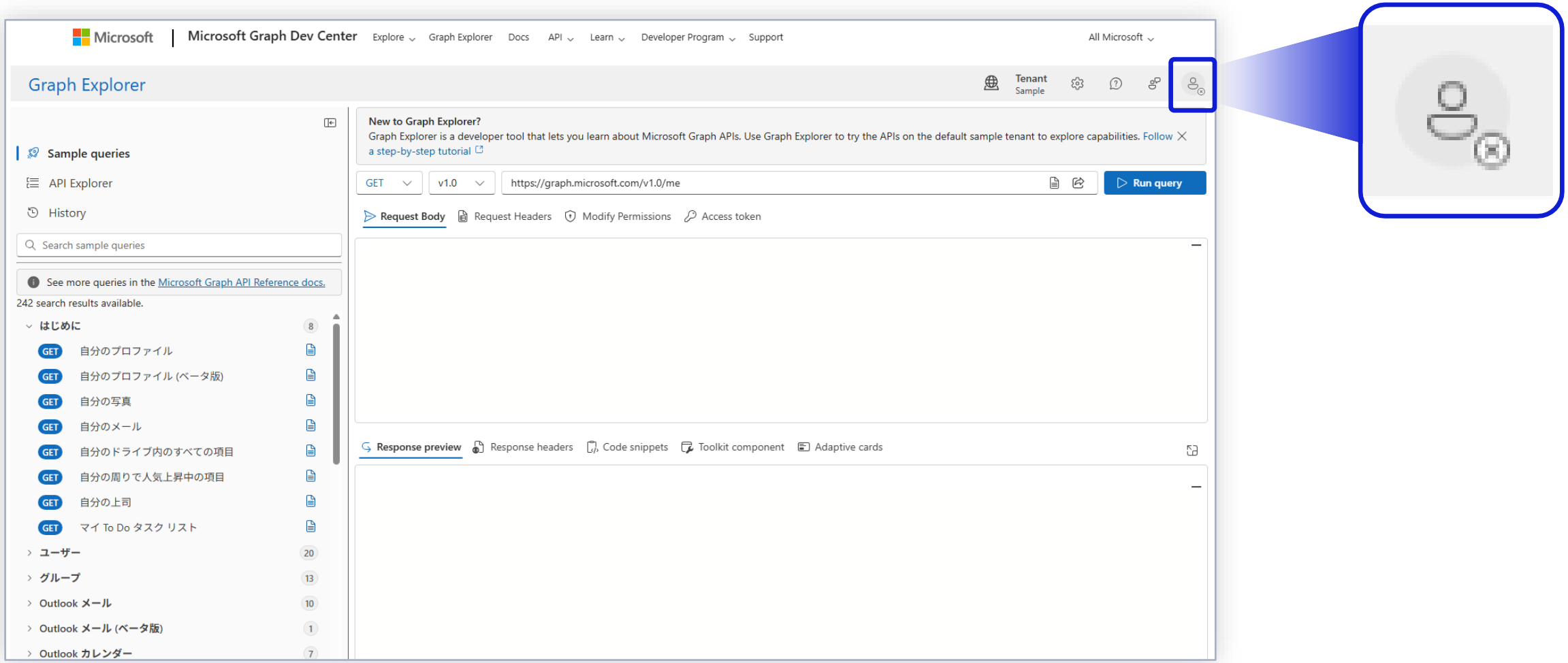
リダイレクトURL

https://xxxxx.yyy/zzzzz
?code=“認可コード”
&session_state=“セッションID”

同意とは-同意の例(1/7)

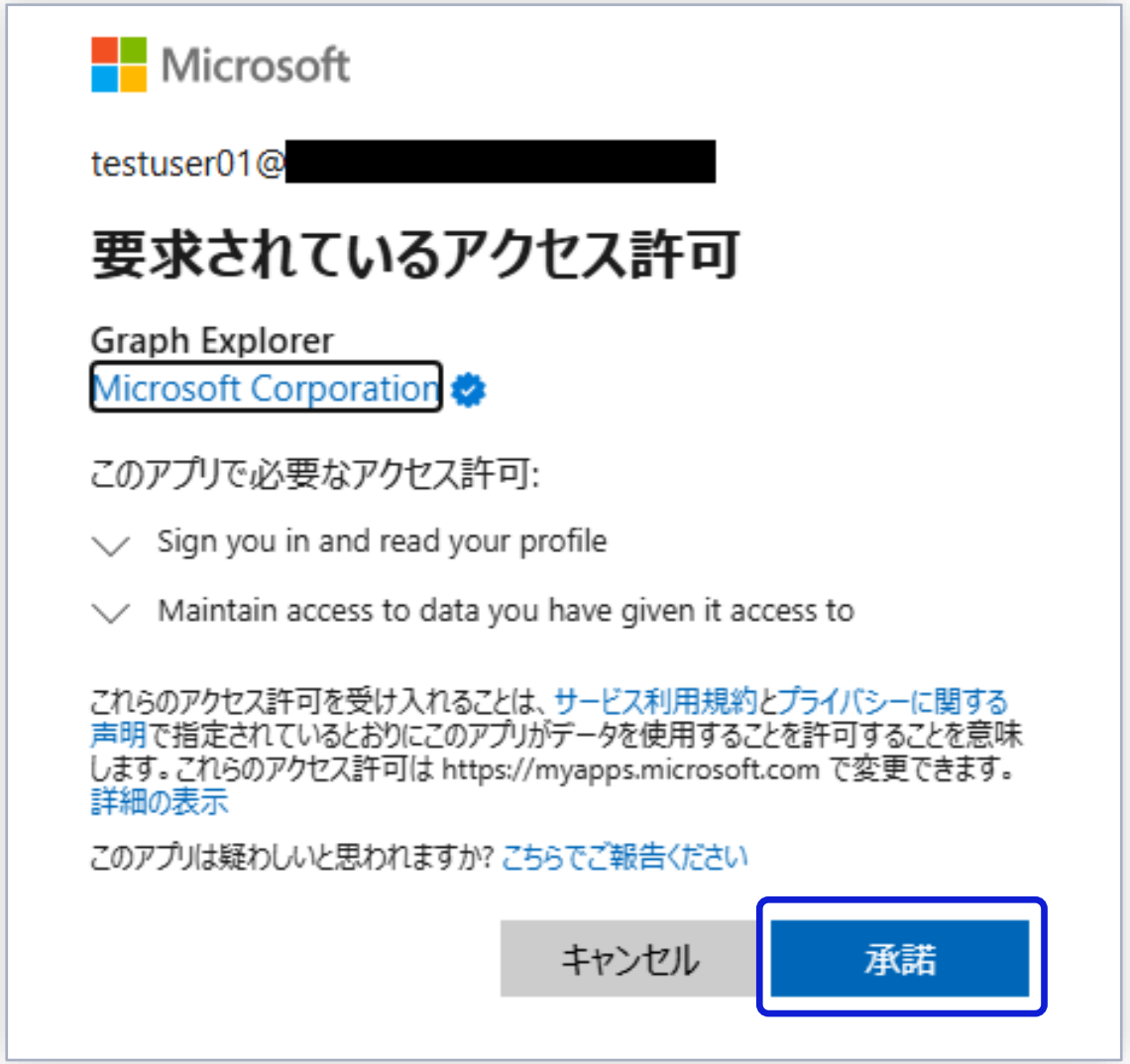
Graph Explorer：Graph APIを探索するためのアプリケーション

参考：https://developer.microsoft.com/en-us/graph/graph-explorer



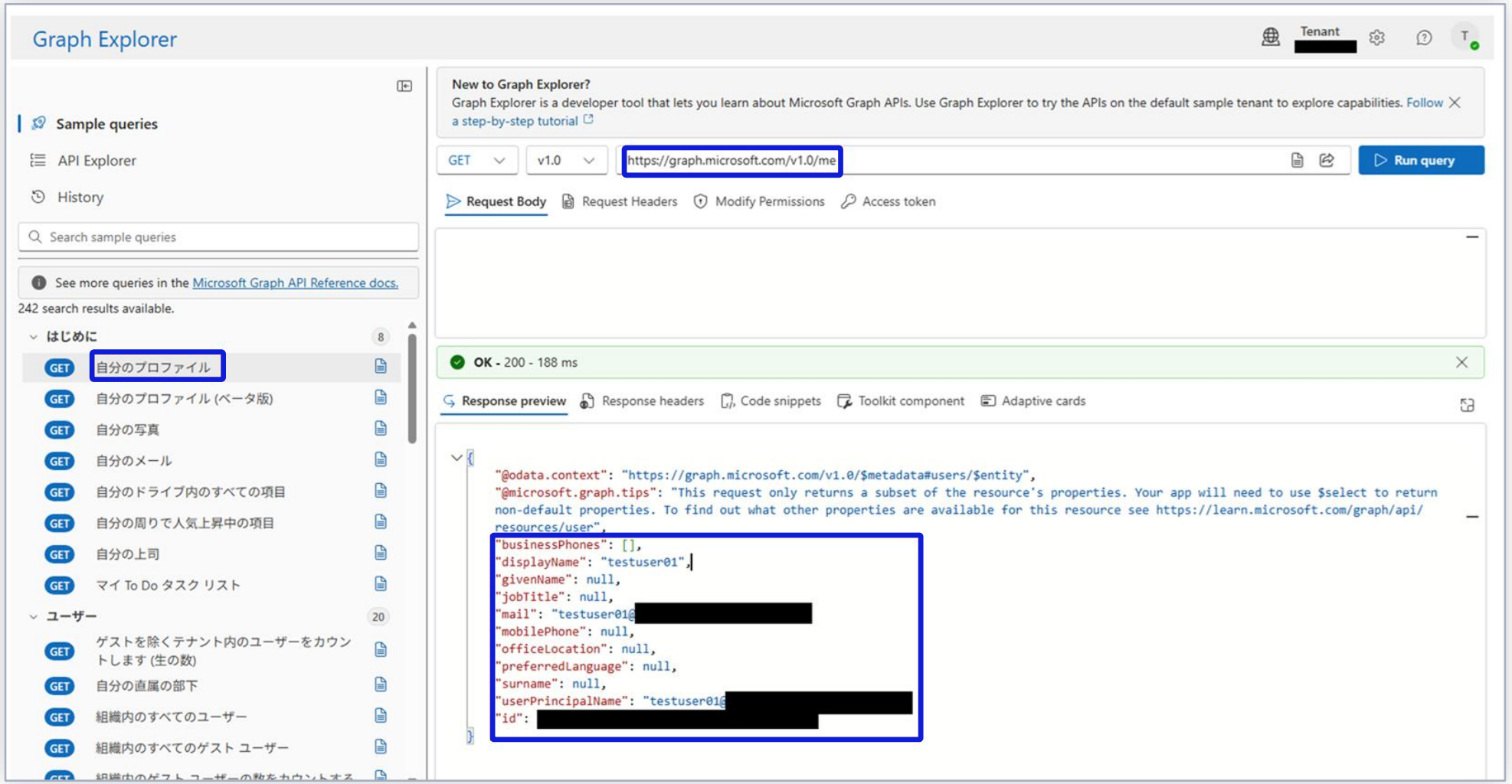
同意とは-同意の例(2/7)

Graph Explorerへの同意画面



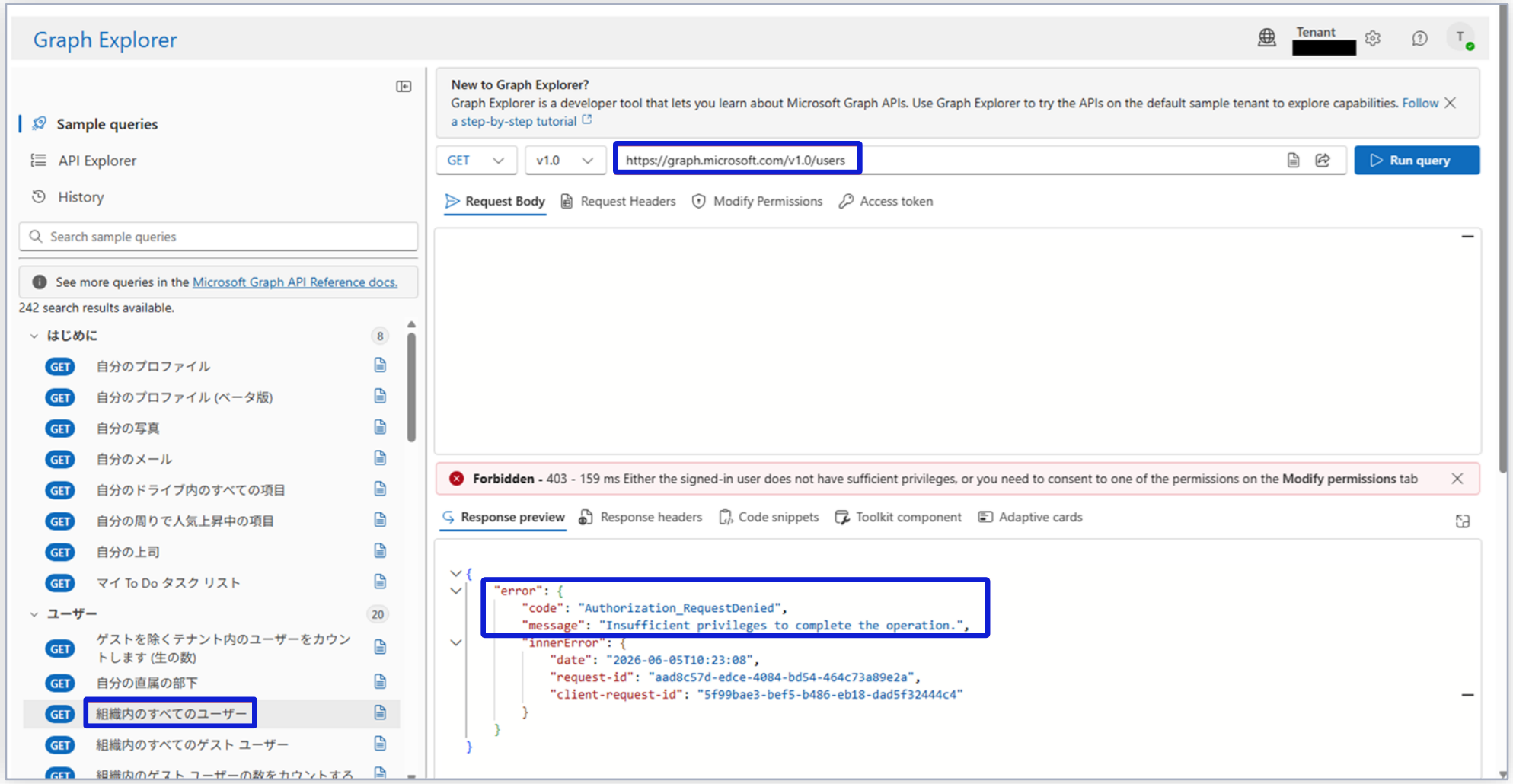
同意とは-同意の例(3/7)

Graph APIを使用した「自分のプロファイル」の取得



同意とは-同意の例(4/7)

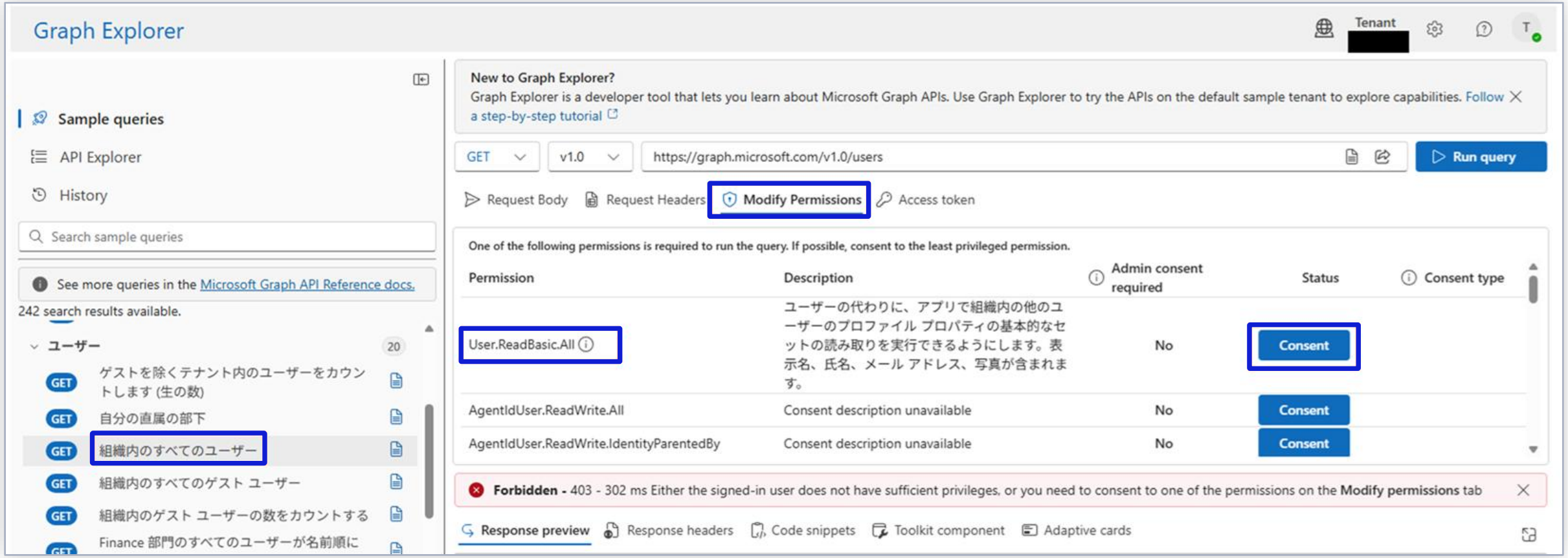
Graph APIを使用した「組織内のすべてのユーザー」の取得失敗



同意とは-同意の例(5/7)

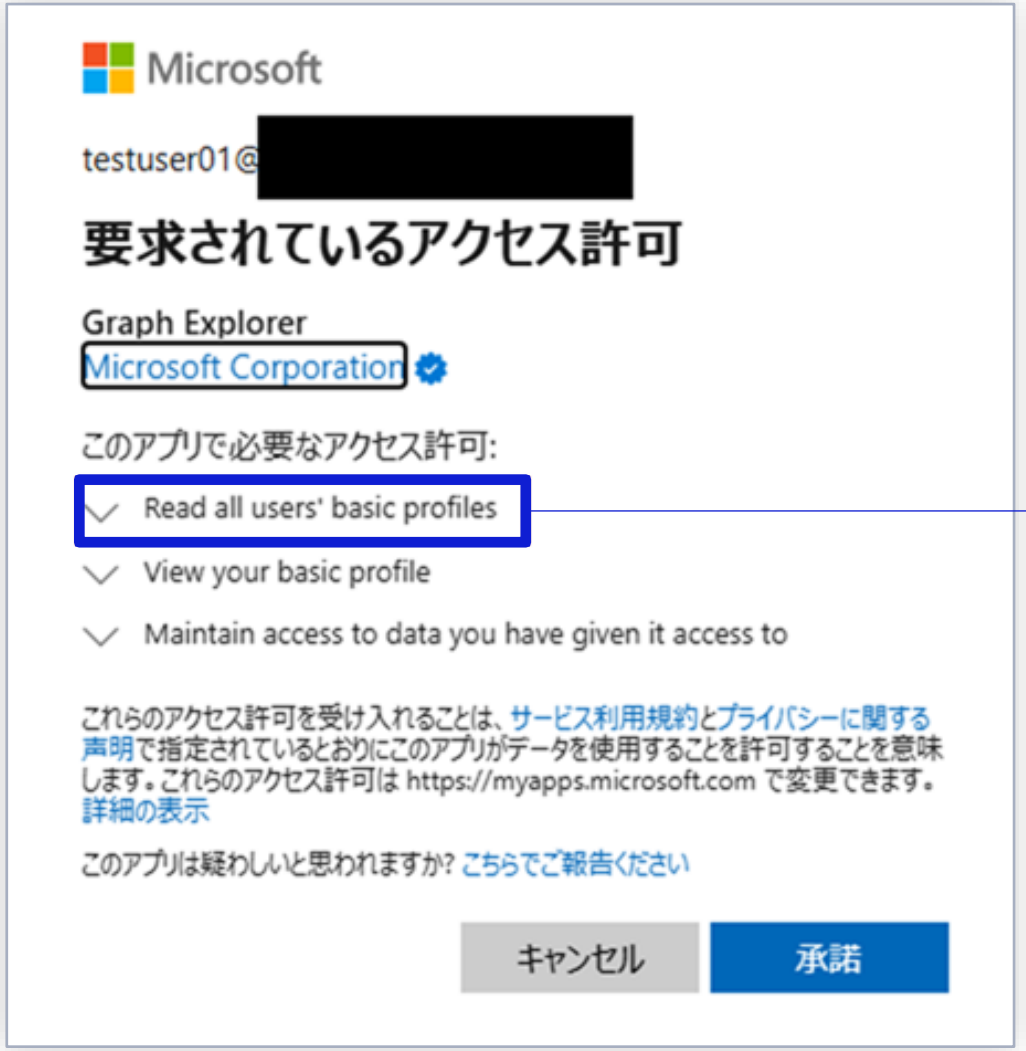
「User.ReadBasic.All」のアクセス許可への同意

参考： https://learn.microsoft.com/ja-jp/graph/permissions-reference#userreadbasicall



同意とは-同意の例(6/7)

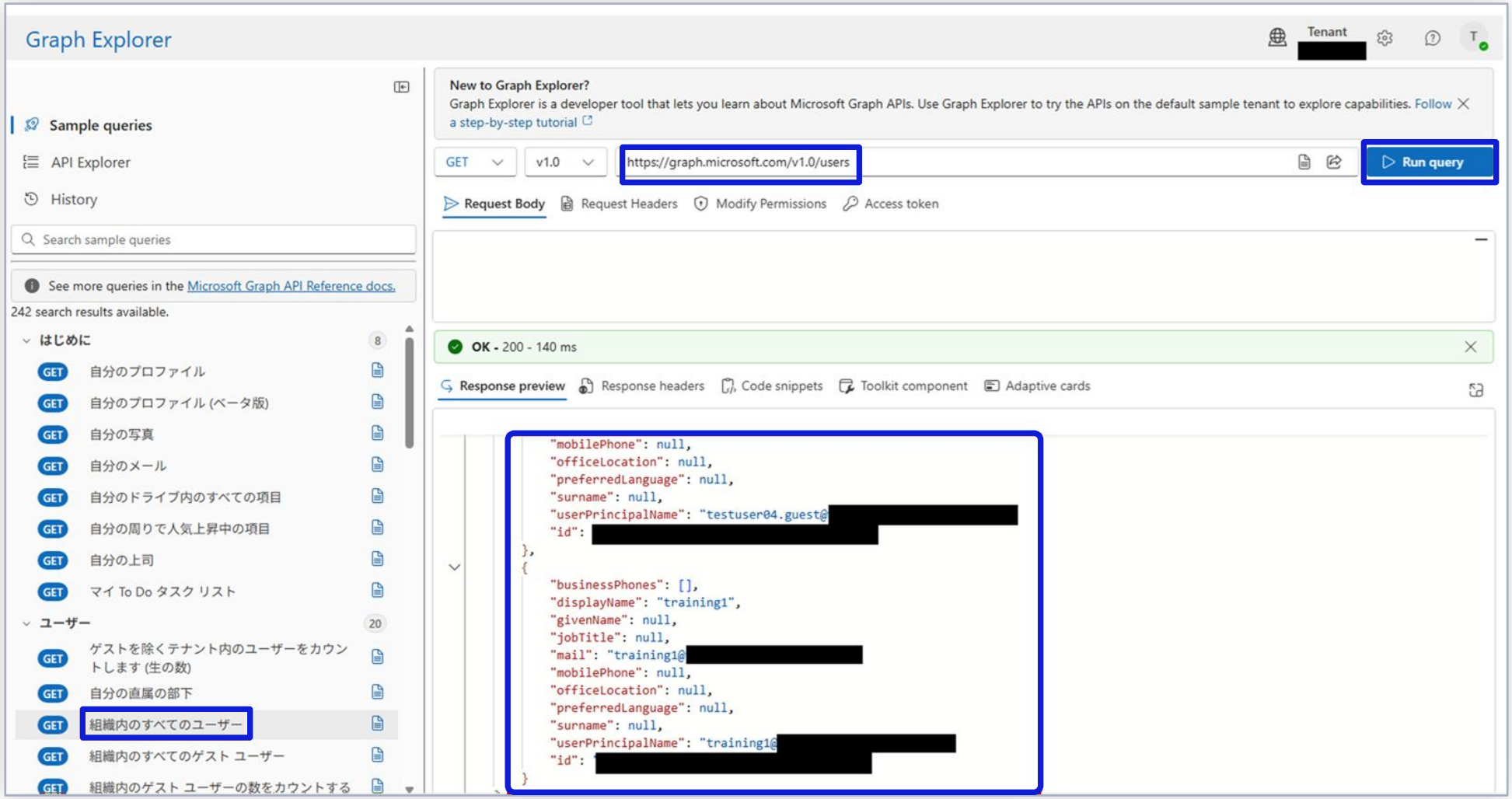
「User.ReadBasic.All」のアクセス許可への同意



「User.ReadBasic.All」のアクセス許可

同意とは-同意の例(7/7)

Graph APIを使用した「組織内のすべてのユーザー」の取得

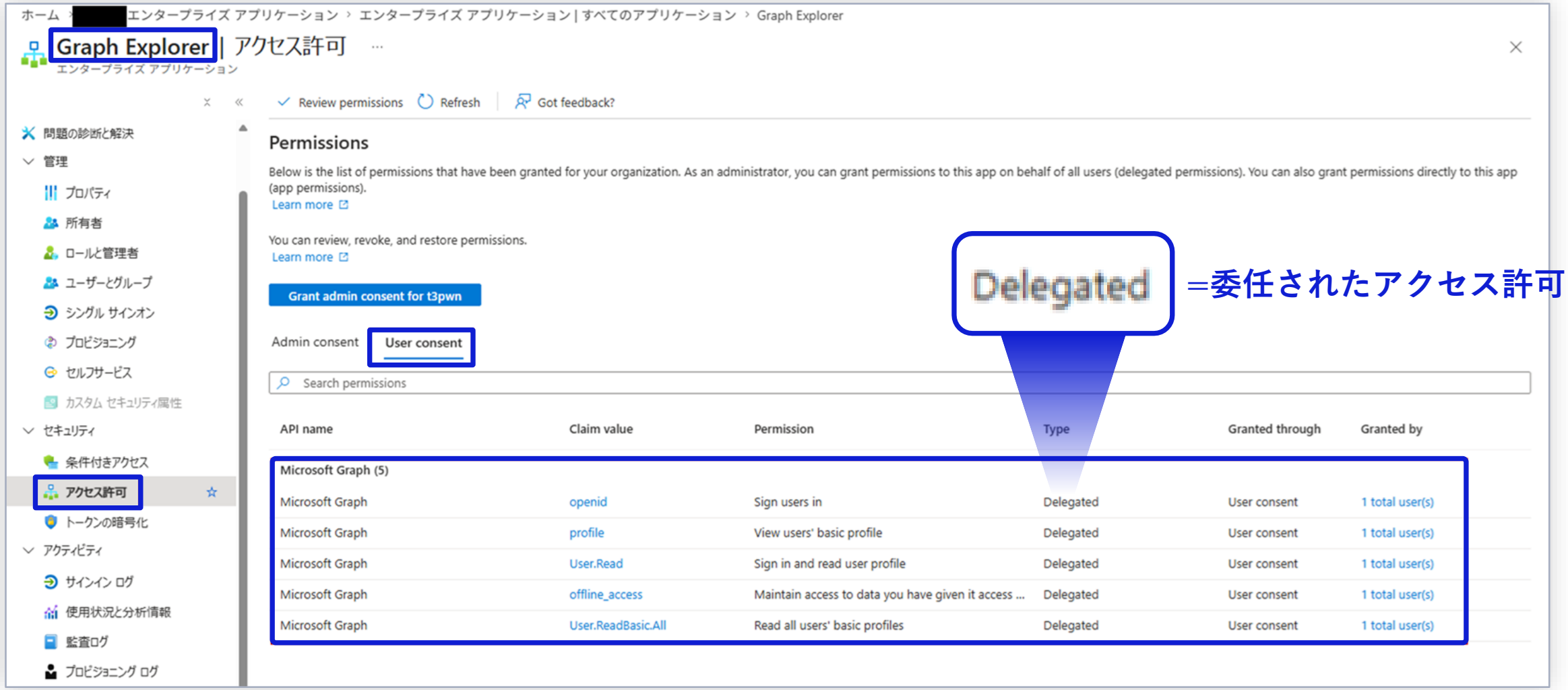


同意とは-アクセス許可(1/3)

Microsoft Entra IDポータル>エンタープライズアプリケーション

同意とは-アクセス許可(2/3)

Graph Explorerに付与されたアクセス許可



同意とは-アクセス許可(3/3)

2種類のアクセス許可

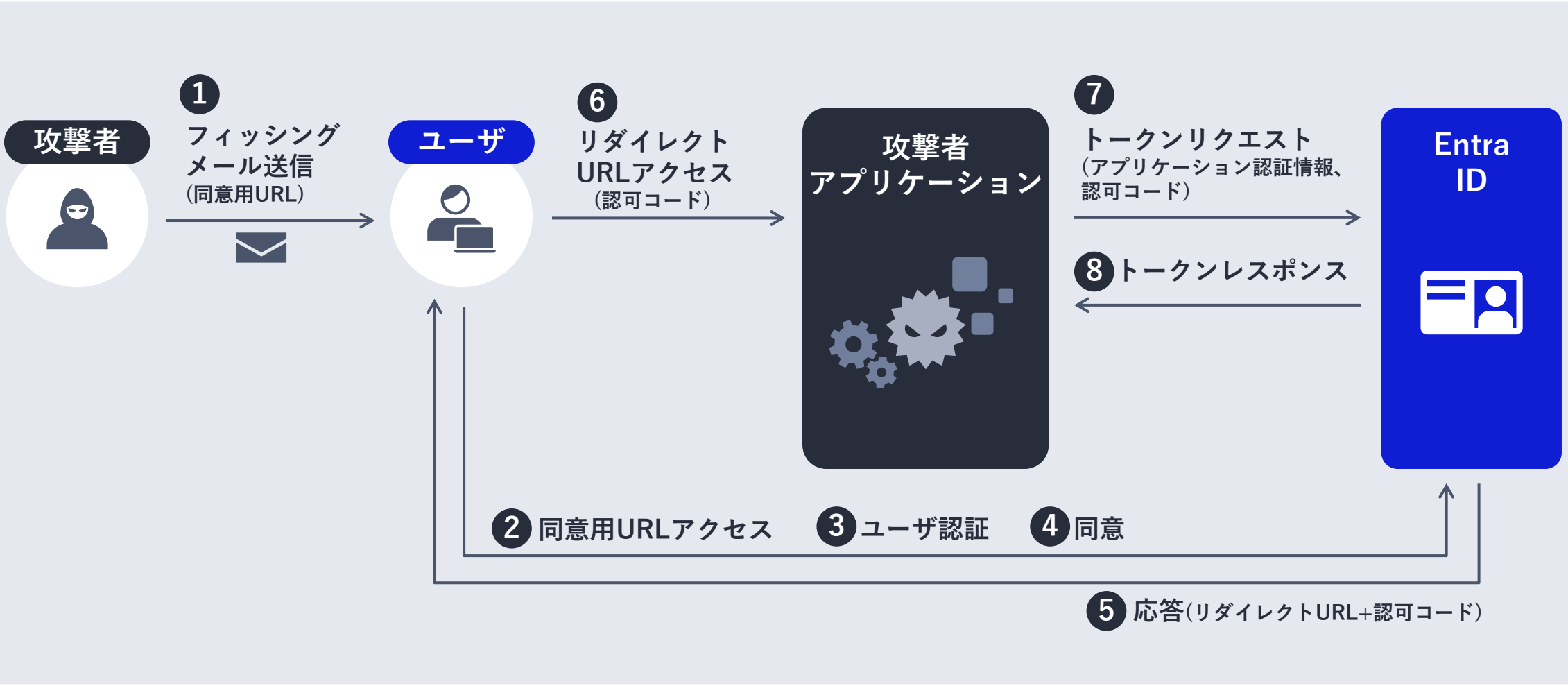
	委任されたアクセス許可 ユーザの代理として権限を使用	アプリケーションのアクセス許可 アプリケーションとして権限を使用
権限	**ユーザ**の権限	**組織**全体
同意	一部の権限を除き**ユーザ**が同意可能	**管理者のみ**が同意可能
例	「Mail.Read」の 委任されたアクセス許可 **同意したユーザの** 受信メールを読み込み可能	「Mail.Read」の アプリケーションのアクセス許可 **同意した組織の全てのユーザの** 受信メールを読み込み可能

参考：
https://learn.microsoft.com/ja-jp/graph/permissions-overview
https://learn.microsoft.com/ja-jp/graph/permissions-reference#mailread

5.同意フィッシング

同意フィッシングとは

同意の仕組みを悪用したフィッシング
ユーザ自身がアクセス許可を攻撃者アプリケーションに付与するため、多要素認証有無に関係なく有効な攻撃



6.同意フィッシングデモ

攻撃者と被害者の視点を織り交ぜながら同意フィッシングのデモを紹介

同意フィッシングデモ

- 攻撃者-準備1
- 被害者-ユーザ
- 攻撃者-悪用1
- 攻撃者-準備2
- 被害者-管理者
- 攻撃者-悪用2

同意フィッシングデモ

- **攻撃者-準備1**
- 被害者-ユーザ
- 攻撃者-悪用1
- 攻撃者-準備2
- 被害者-管理者
- 攻撃者-悪用2

同意フィッシングデモ-攻撃者-準備1(1/7)

攻撃者が管理するEntra IDでアプリケーションを登録

認可コード受け取りのためのリダイレクトは、アプリケーション登録済み
リダイレクトURLに制限（複数登録可）

同意フィッシングデモ-攻撃者-準備1(2/7)

- 作成したアプリケーションに「User.ReadBasic.All」アクセス許可を設定
- 「User.ReadBasic.All」：組織内の全てのユーザの情報を取得可能な権限

同意フィッシングデモ-攻撃者-準備1(3/7)

- デフォルト設定である「Microsoftによる同意設定の管理を許可する」の場合、ユーザが同意可能なアクセス許可は制限される
- 「User.ReadBasic.All」はデフォルト設定であってもユーザが同意可能なアクセス許可

参考：https://learn.microsoft.com/ja-jp/entra/identity/enterprise-apps/manage-app-consent-policies?pivots=ms-powershell#microsoft-recommended-user-consent-policy

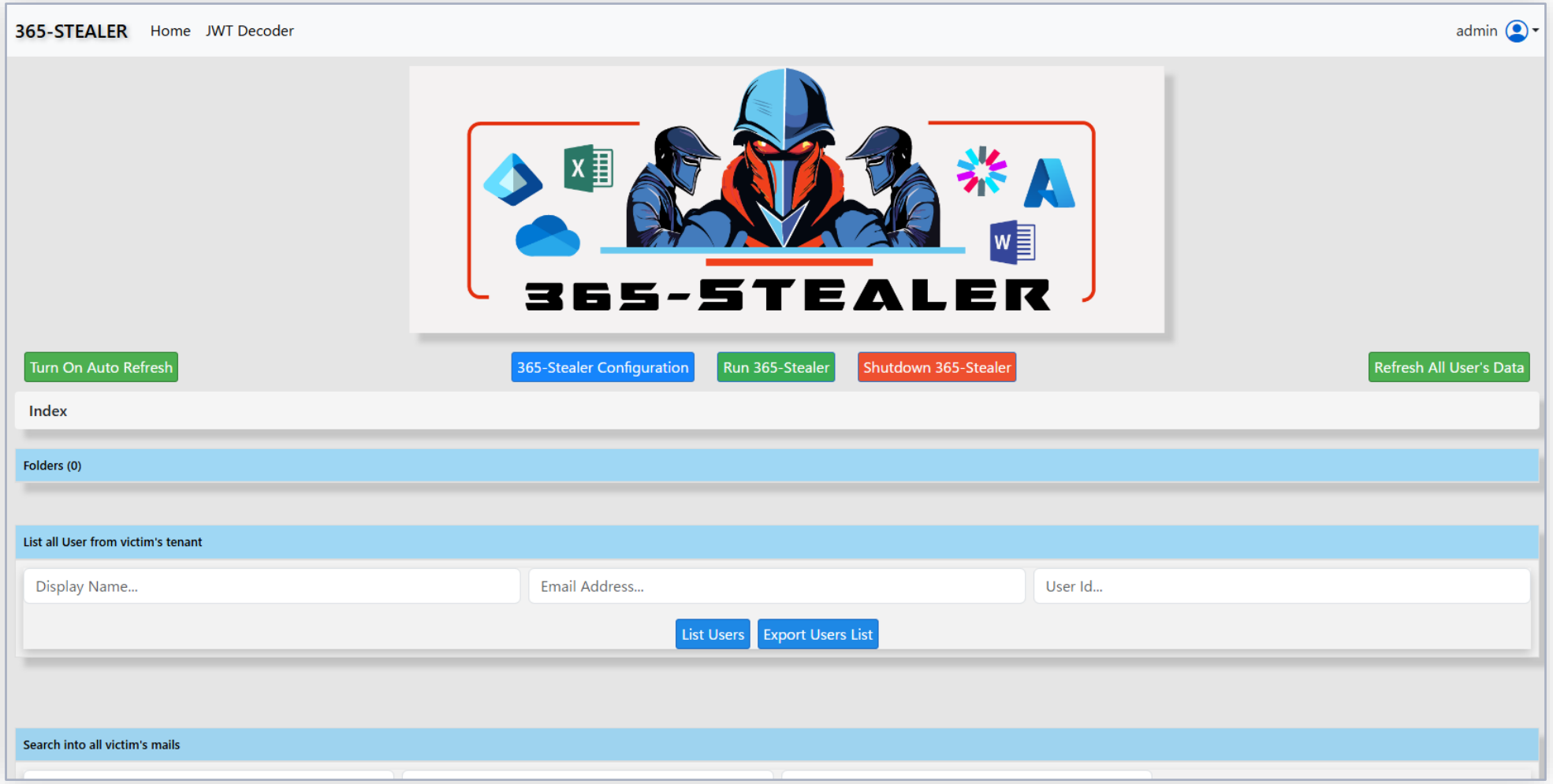
同意フィッシングデモ-攻撃者-準備1(4/7)

作成したアプリケーションのパスワードであるクライアントシークレットを作成

同意フィッシングデモ-攻撃者-準備1(5/7)

Altered Security社の365-Stealerを使用し、同意フィッシングの環境を構築

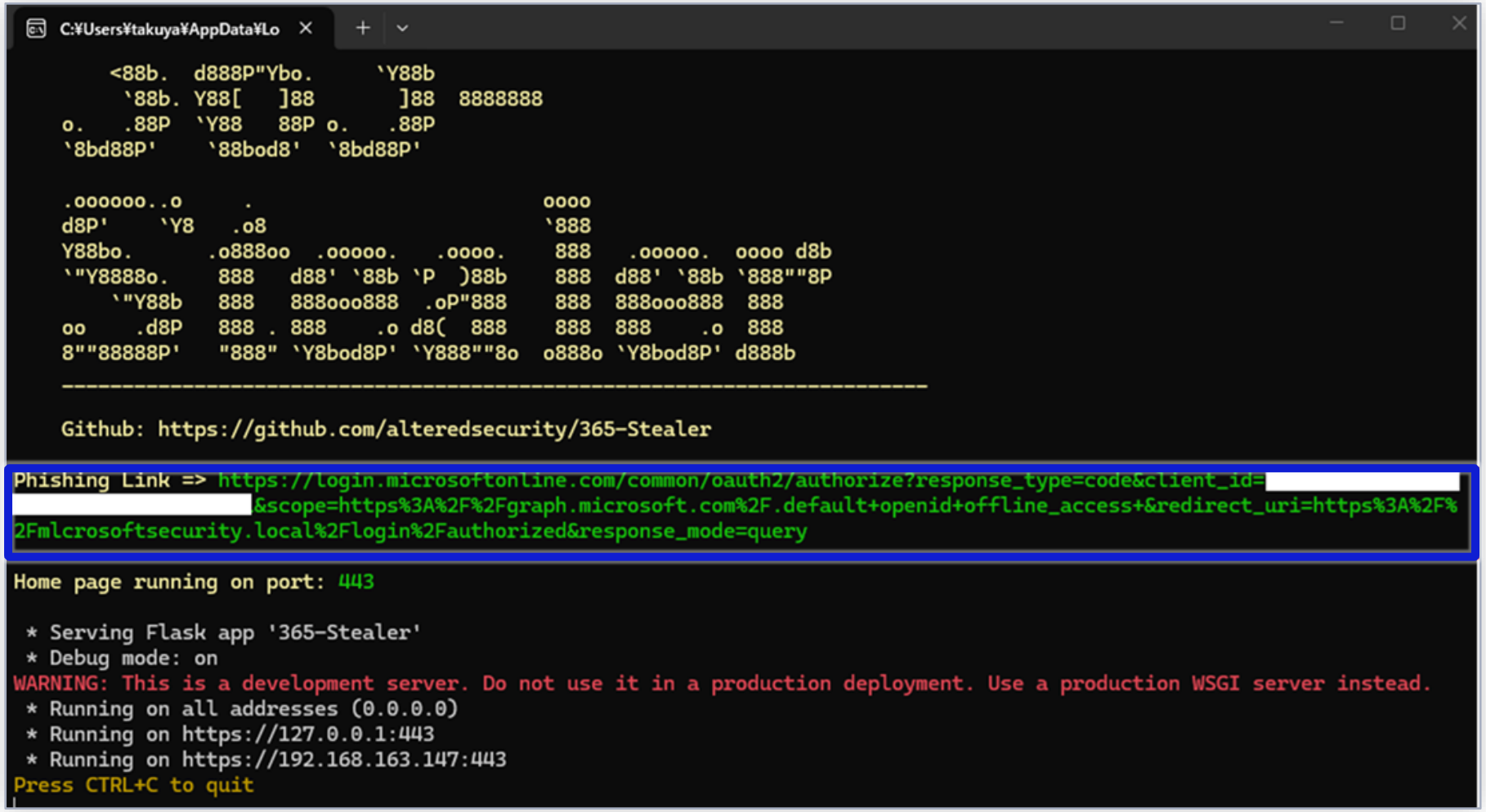
参考：https://github.com/AlteredSecurity/365-Stealer



出典：https://github.com/AlteredSecurity/365-Stealer

同意フィッシングデモ-攻撃者-準備1(6/7)

- 必要な情報を入力後、365-Stealerを再起動するとCLI上にフィッシング用URLが表示
- client_idパラメータにアプリケーションID、redirect_uriにリダイレクト先URLが含まれる



同意フィッシングデモ-攻撃者-準備1(7/7)

フィッシング用URLを含むメールをターゲットに対して送付

同意フィッシングデモ

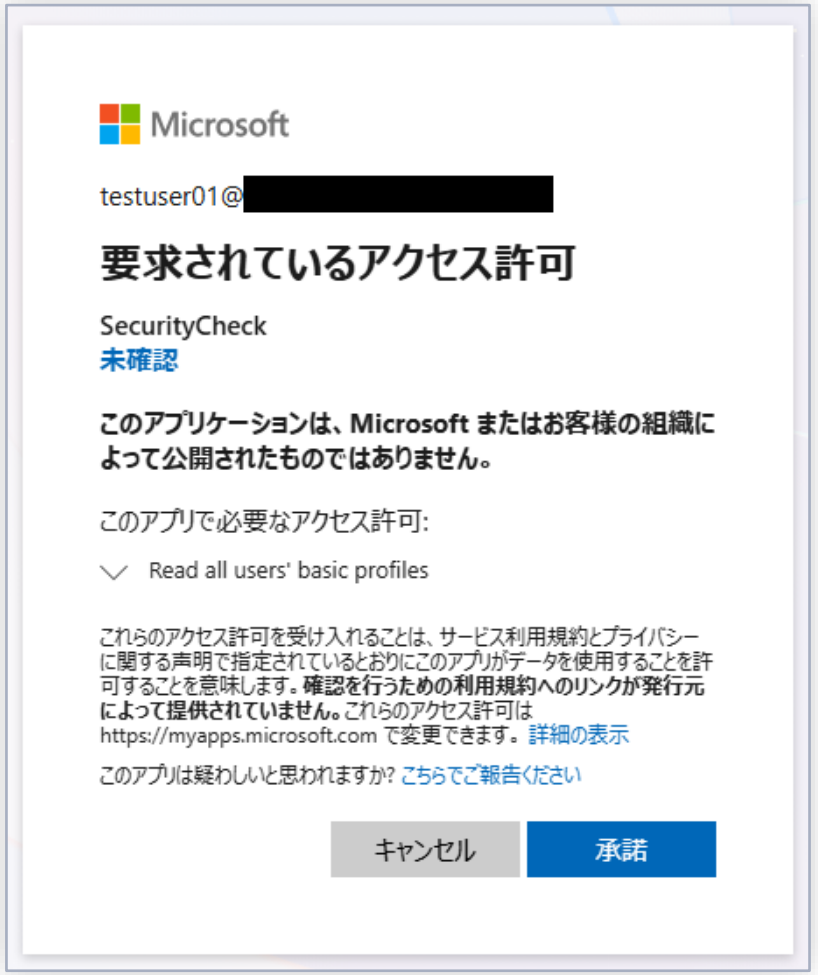
- 攻撃者-準備1
- **被害者-ユーザ**
- 攻撃者-悪用1
- 攻撃者-準備2
- 被害者-管理者
- 攻撃者-悪用2

同意フィッシングデモ-被害者-ユーザ(1/2)

- 同意フィッシングメールが被害者に届く
- フィッシング用URLはMicrosoft社正規ドメインが使用されるため、不審に思わず被害者がアクセス

同意フィッシングデモ-被害者-ユーザ(2/2)

- 攻撃者が作成したアプリケーションへの同意画面が表示、被害者は不審に思わず「承諾」
- 被害者はリダイレクトURLに飛ばされ、Microsoft社を模した攻撃者が作成したサイトが表示



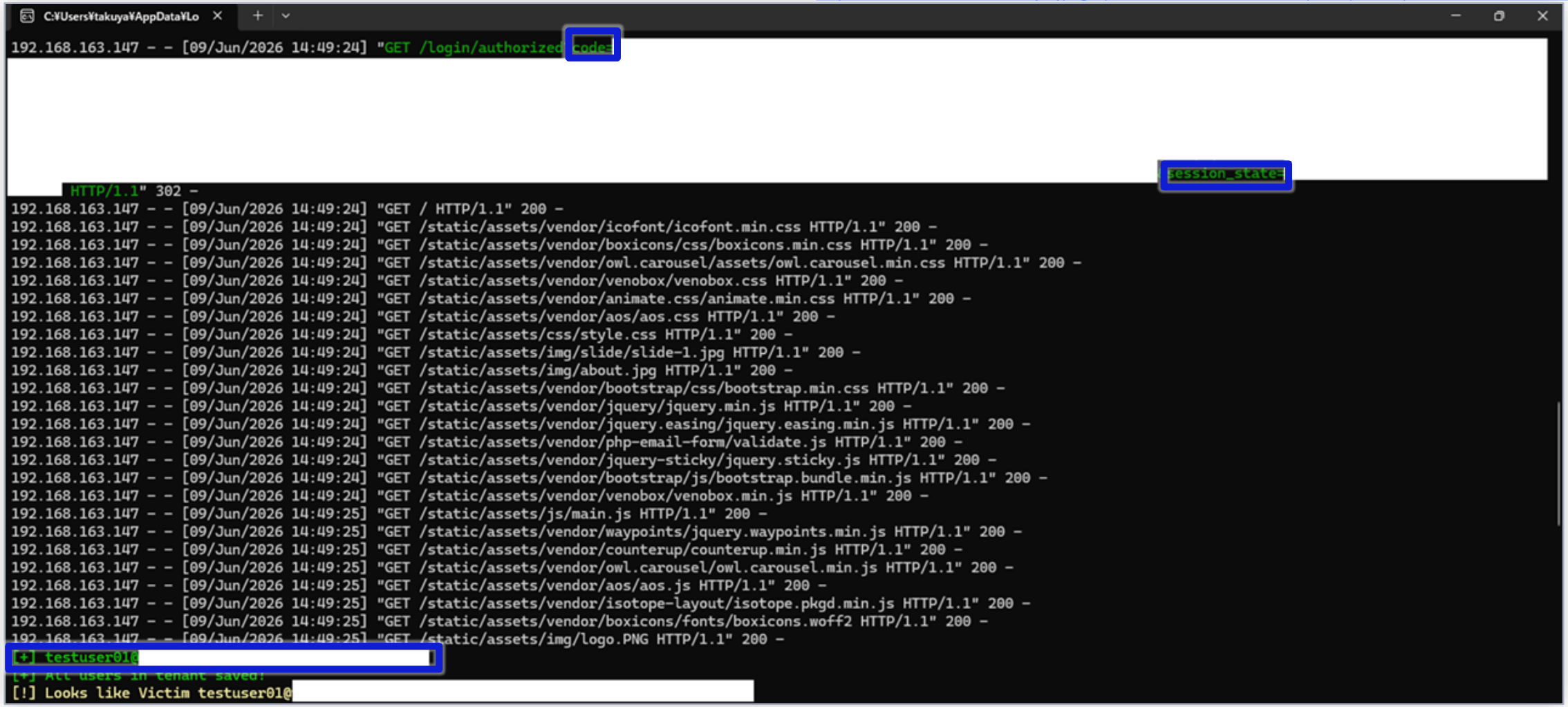
同意フィッシングデモ

- 攻撃者-準備1
- 被害者-ユーザ
- **攻撃者-悪用1**
- 攻撃者-準備2
- 被害者-管理者
- 攻撃者-悪用2

同意フィッシングデモ-攻撃者-悪用1(1/3)

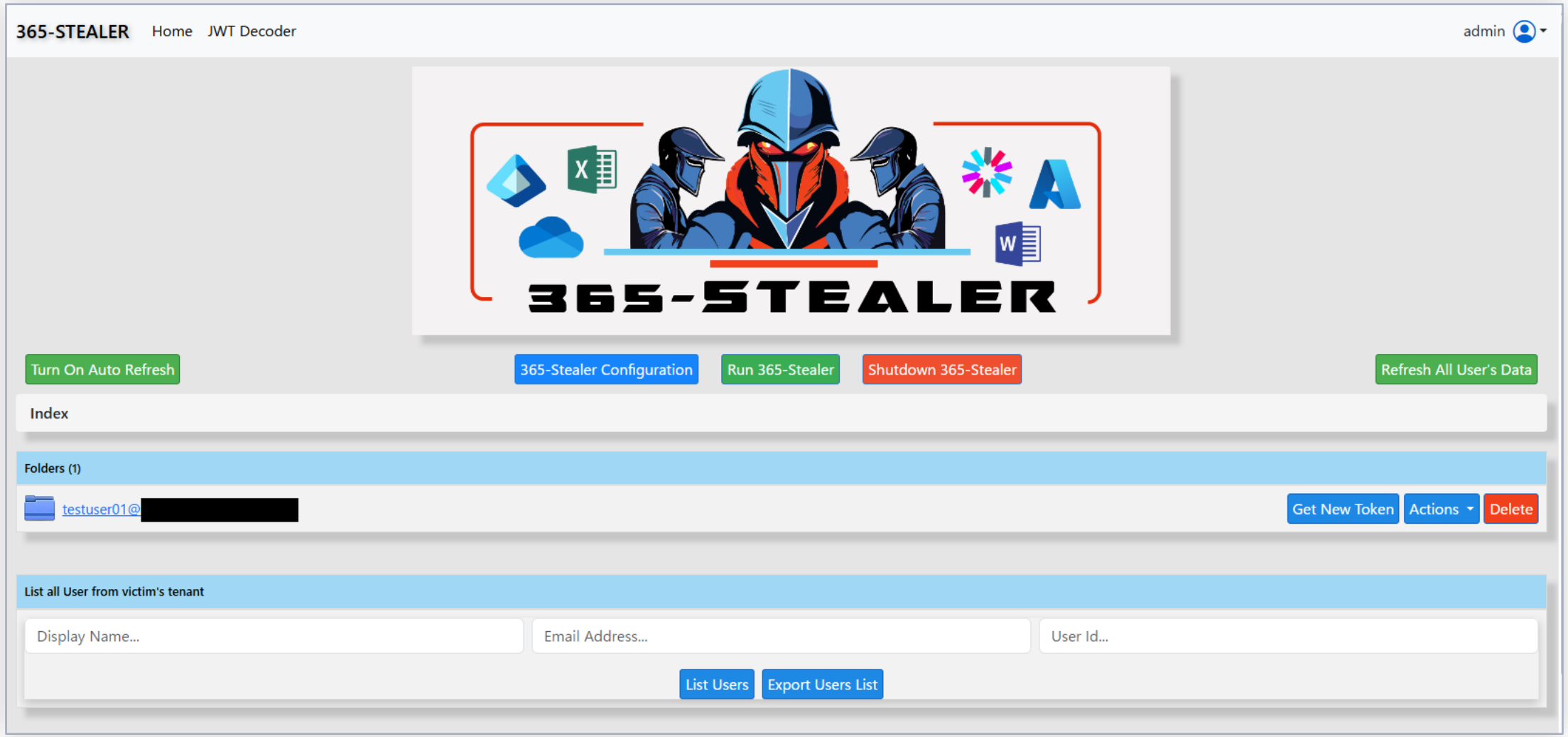
被害者が同意後にリダイレクトすることで365-StealerのCLI上に認可コードが表示
認可コードとAppID、クライアントシークレットを用いてアクセストークンを入手

参考： https://learn.microsoft.com/ja-jp/graph/auth-v2-user?tabs=http#step-2-request-an-access-token



同意フィッシングデモ-攻撃者-悪用1(2/3)

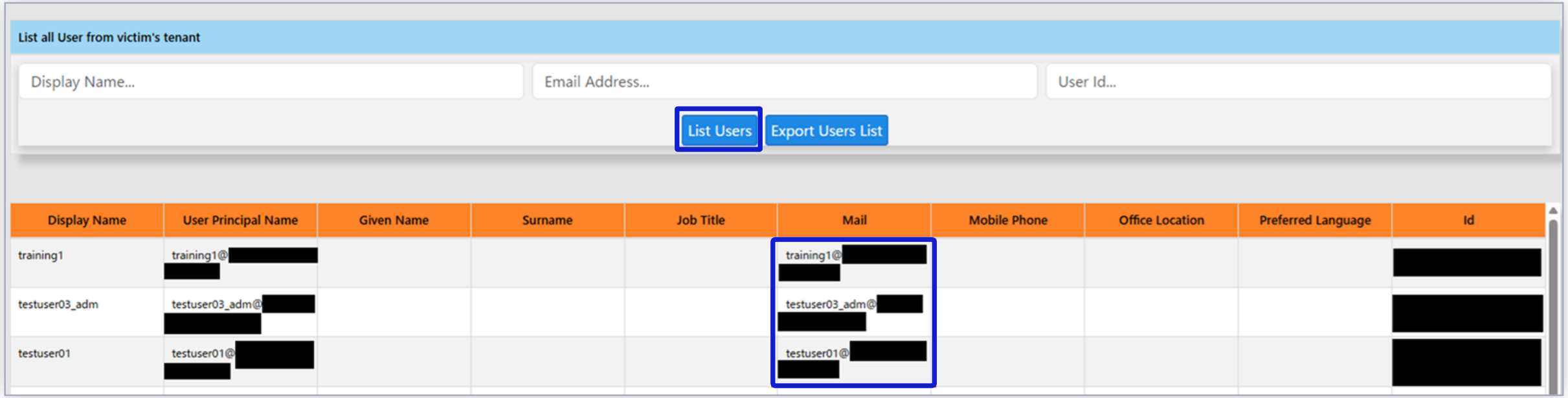
365-StealerのGUIを更新すると被害にあったユーザが表示される



出典：https://github.com/AlteredSecurity/365-Stealer

同意フィッシングデモ-攻撃者-悪用1(3/3)

- 被害者は「User.ReadBasic.All」のアクセス許可に同意
- 365-Stealer上の「List Users」を選択し、被害者テナントの全てのユーザの情報を出力
- 管理者と推測するtestuser03_admをターゲットに更に同意フィッシングを仕掛ける



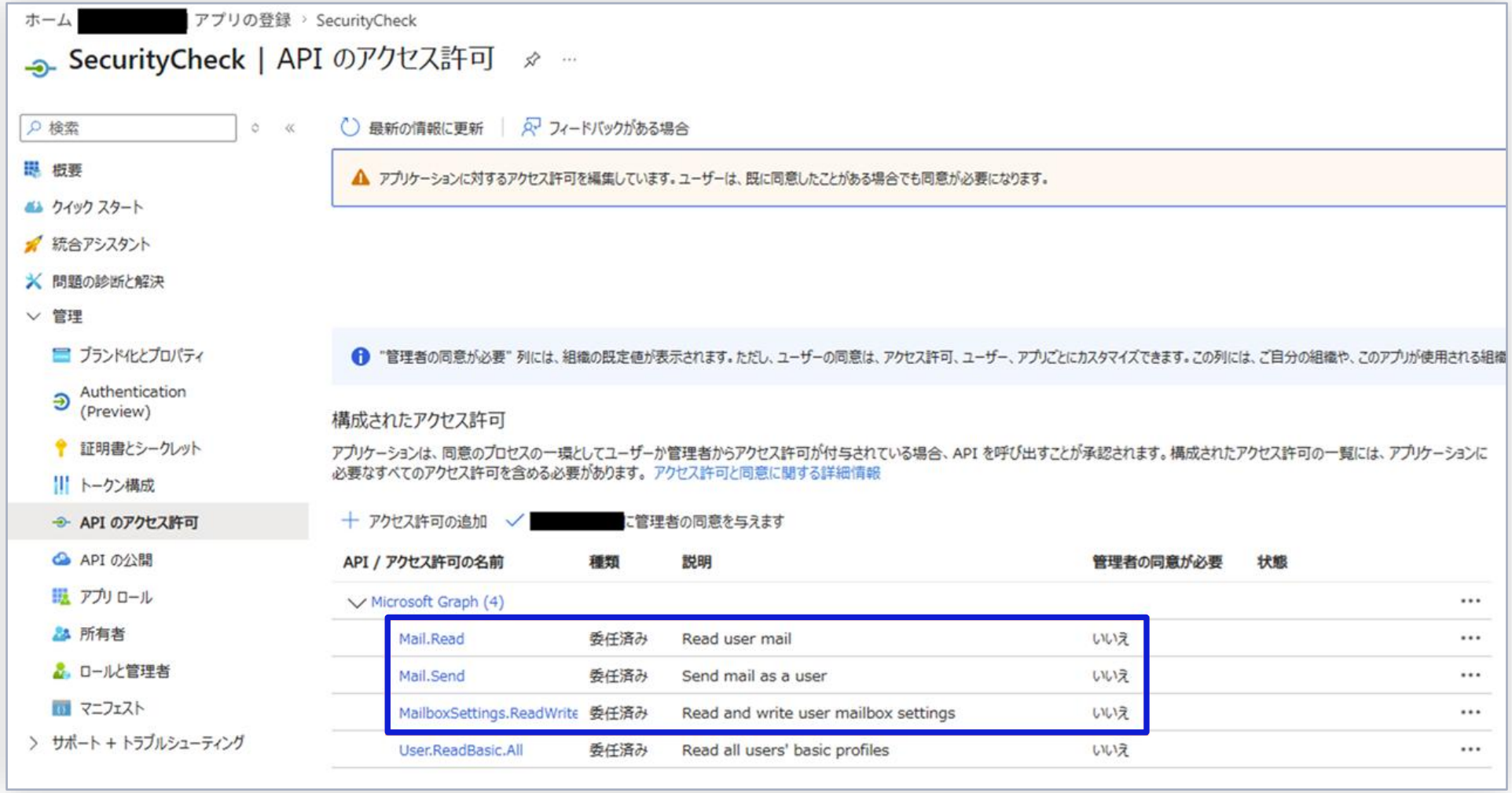
同意フィッシングデモ

- 攻撃者-準備1
- 被害者-ユーザ
- 攻撃者-悪用1
- **攻撃者-準備2**
- 被害者-管理者
- 攻撃者-悪用2

同意フィッシングデモ-攻撃者-準備2(1/2)

次のターゲットが管理者と仮定して、メール関連の委任されたアクセス許可を作成したアプリケーションに設定

参考：
https://learn.microsoft.com/ja-jp/graph/permissions-reference#mailsend
https://learn.microsoft.com/ja-jp/graph/permissions-reference#mailboxsettingsreadwrite



同意フィッシングデモ-攻撃者-準備2(2/2)

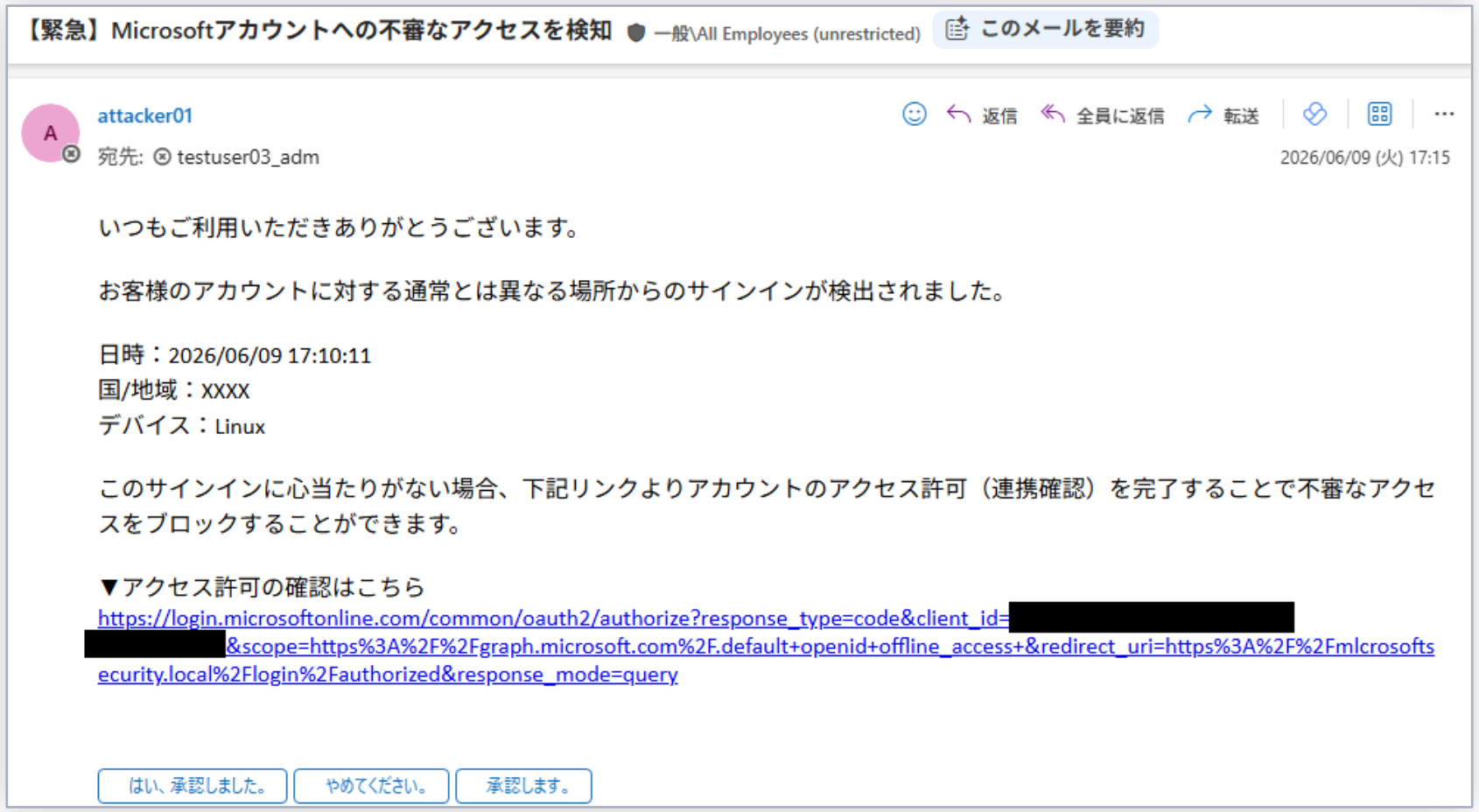
次のターゲットに対して、同意フィッシングを試行

同意フィッシングデモ

- 攻撃者-準備1
- 被害者-ユーザ
- 攻撃者-悪用1
- 攻撃者-準備2
- **被害者-管理者**
- 攻撃者-悪用2

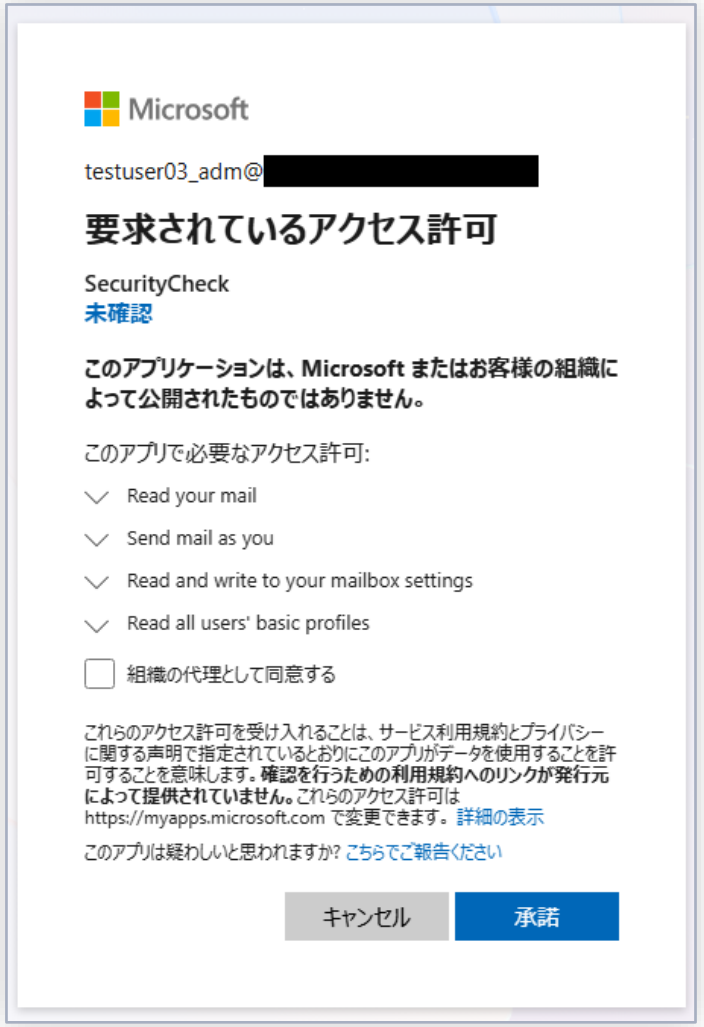
同意フィッシングデモ-被害者-管理者(1/2)

- 同意フィッシングメールが被害者に届く
- フィッシング用URLはMicrosoft社正規ドメインが使用されるため、不審に思わず被害者がアクセス



同意フィッシングデモ-被害者-管理者(2/2)

- 攻撃者が作成したアプリケーションへの同意画面が表示、被害者は不審に思わず「承諾」
- 被害者はリダイレクトURLに飛ばされ、Microsoft社を模した攻撃者が作成したサイトが表示

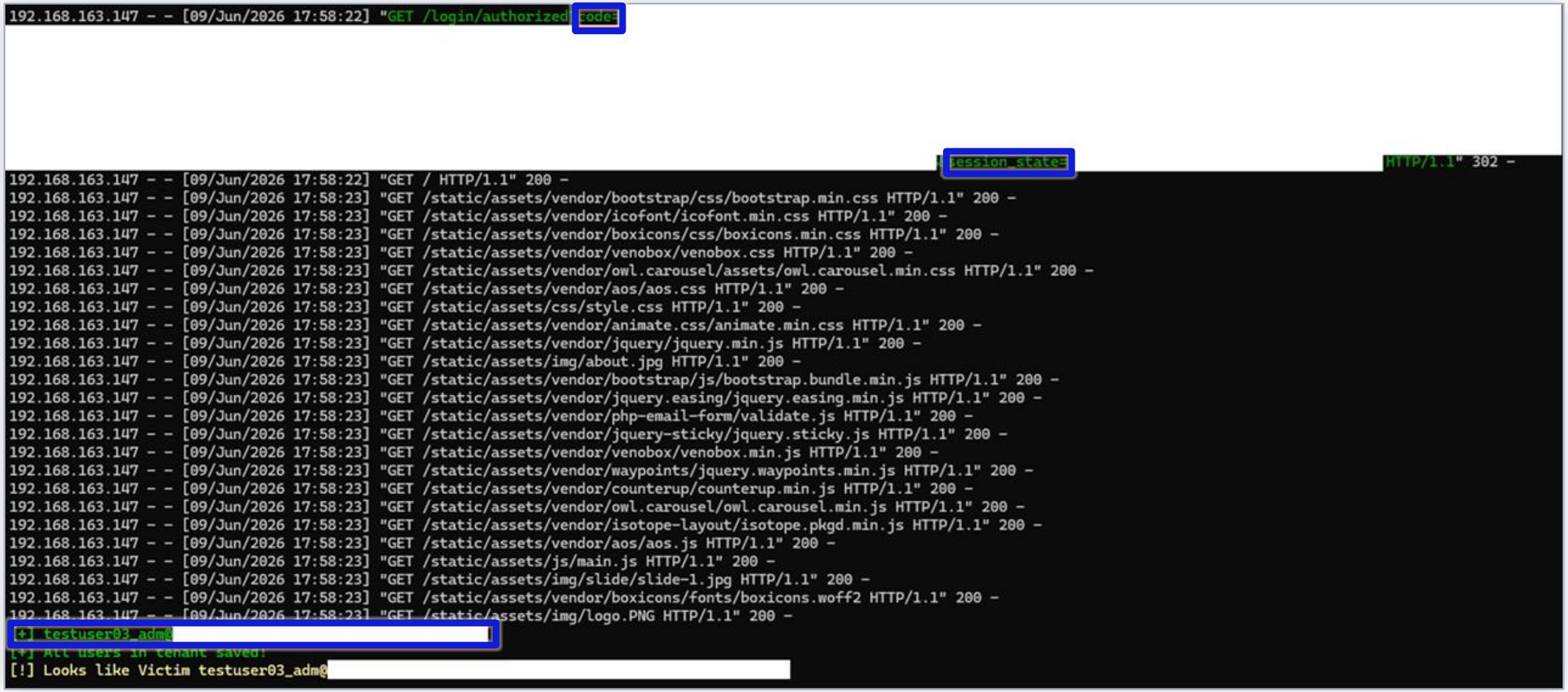


同意フィッシングデモ

- 攻撃者-準備1
- 被害者-ユーザ
- 攻撃者-悪用1
- 攻撃者-準備2
- 被害者-管理者
- **攻撃者-悪用2**

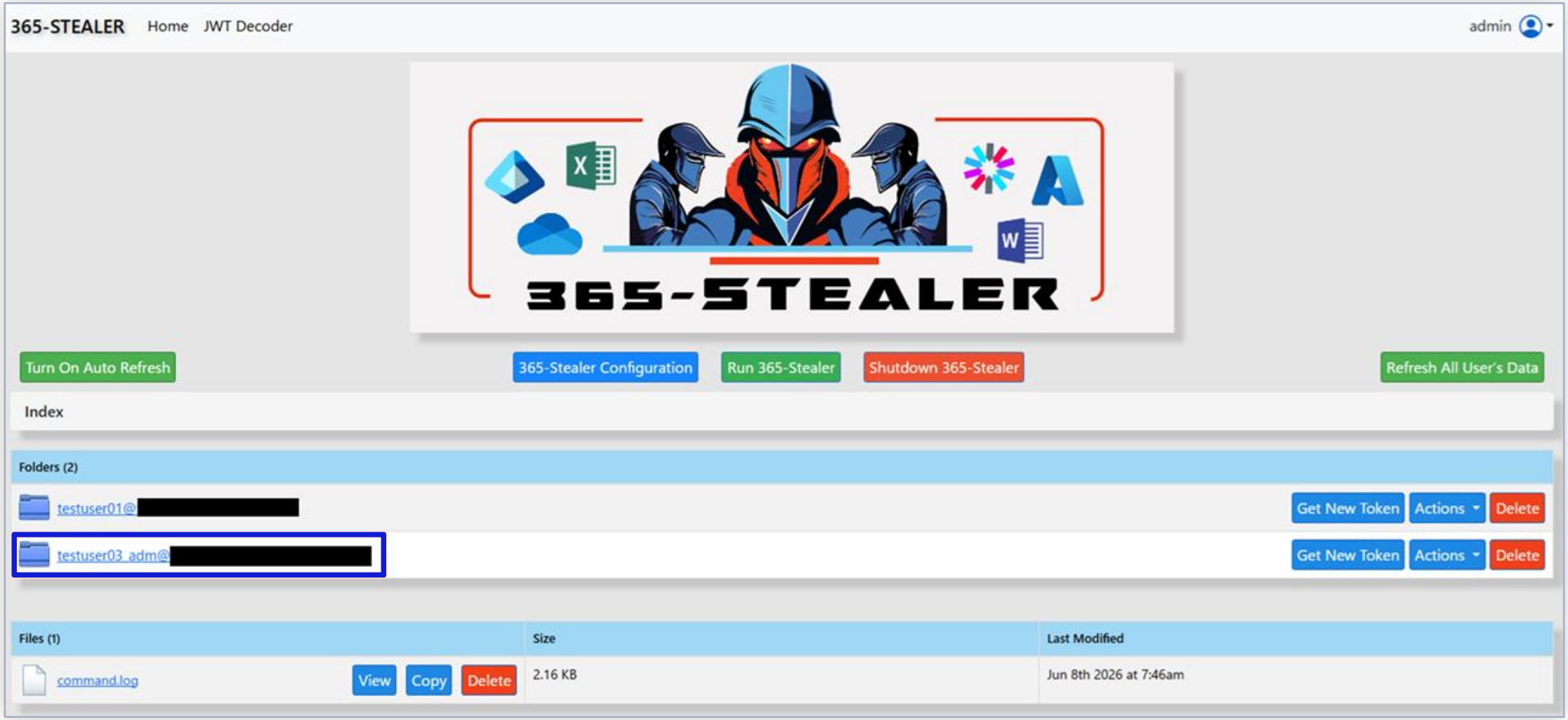
同意フィッシングデモ-攻撃者-悪用2(1/4)

被害者が同意後にリダイレクトすることで365-StealerのCLI上に認可コードが表示



同意フィッシングデモ-攻撃者-悪用2(2/4)

365-StealerのGUIを更新すると被害にあったユーザが追加される



出典：https://github.com/AlteredSecurity/365-Stealer

同意フィッシングデモ-攻撃者-悪用2(3/4)

- 被害者は「Mail.Read」のアクセス許可に同意
- 365-Stealer上で被害者の受信メールを閲覧

いつもご利用いただきありがとうございます。

お客様のアカウントに対する通常とは異なる場所からのサインインが検出されました。

日時：2026/06/09 17:10:11
国/地域：XXXX
デバイス：Linux

このサインインに心当たりがない場合、下記リンクよりアカウントのアクセス許可（連携確認）を完了することで不審なアクセスをブロックすることができます。

▼アクセス許可の確認はこちら
https://login.microsoftonline.com/common/oauth2/authorize?response_type=code&client_id=[redacted]
[redacted]&scope=https%3A%2F%2Fgraph.microsoft.com%2F.default+openid+offline_access+&redirect_uri=https%3A%2F%2Fmlcrosoftsecurity.local%2Flogin%2Fauthorized&response_mode=query

6.**Subject:Re: パスワードについてFrom:** testuser01@[redacted]
ToRecipients: testuser03_adm@[redacted]
CcRecipients: []
BccRecipients: []
ReplyTo: []
Flag: notFlagged
HasAttachments: False

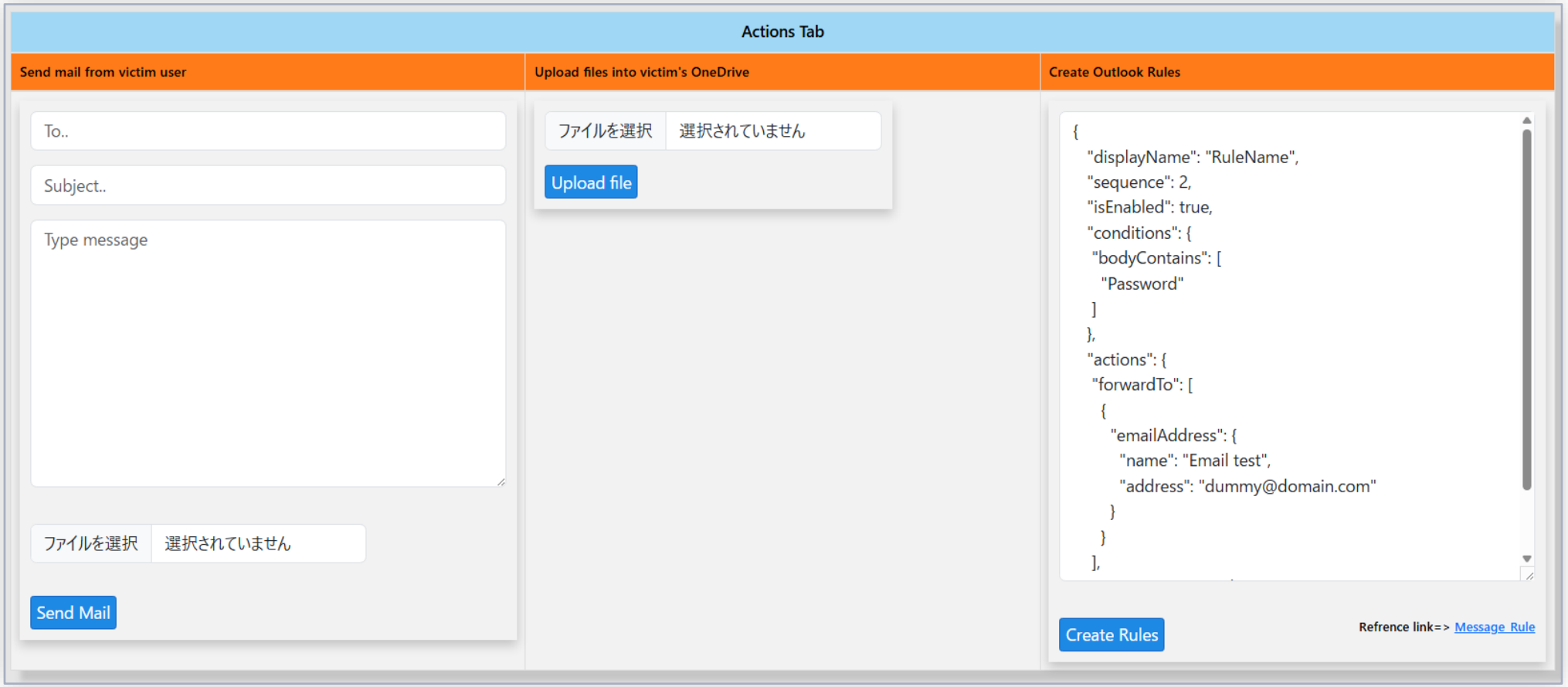
ありがとうございます。
ログインできました。

差出人: testuser03_adm <testuser03_adm@[redacted]
送信日時: 2026年6月8日 11:02
宛先: testuser01 <testuser01@[redacted]
件名: パスワードについて

一時的なパスワードを発行しました。
パスワード：XXXXXXXX

同意フィッシングデモ-攻撃者-悪用2(4/4)

- 被害者は「Mail.Send」「MailboxSettings.ReadWrite」のアクセス許可に同意
- 365-Stealer上で被害者としてメール送信、メールルールの設定追加が可能
  - 内部フィッシングやビジネスメール詐欺に悪用可能



7.同意フィッシングへの対策

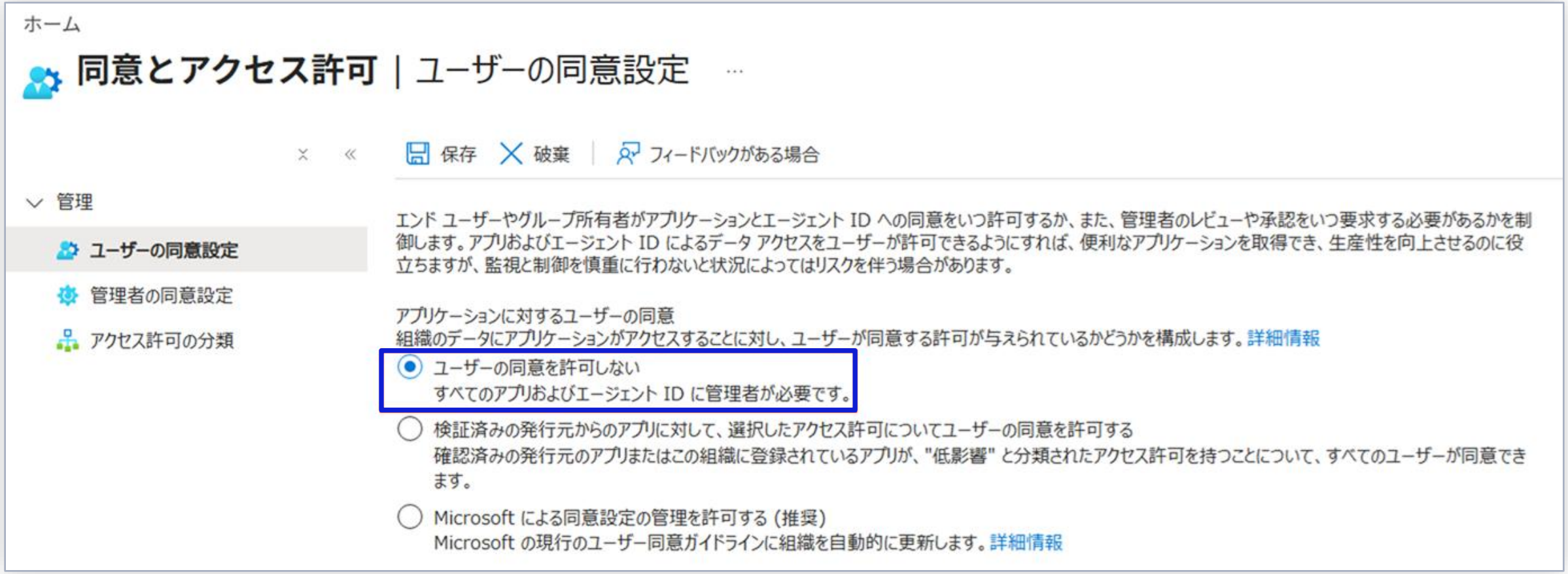
同意フィッシングへの対策

Microsoft 社が対策や調査方法をまとめているため、参照推奨

- 同意フィッシングから保護する
  - https://learn.microsoft.com/ja-jp/entra/identity/enterprise-apps/protect-against-consent-phishing
- アプリの同意付与に関する調査
  - https://learn.microsoft.com/ja-jp/security/operations/incident-response-playbook-app-consent
- Microsoft 365 で不正な同意許可を検出して修復する
  - https://learn.microsoft.com/ja-jp/defender-office-365/detect-and-remediate-illicit-consent-grants
- 危険な OAuth アプリを調査して修復する
  - https://learn.microsoft.com/ja-jp/defender-cloud-apps/investigate-risky-oauth
- [Manage OAuth apps] (OAuth アプリの管理)
  - https://learn.microsoft.com/ja-jp/defender-cloud-apps/manage-app-permissions

同意フィッシングへの対策-防御-ユーザの同意制限(1/2)

- 「ユーザの同意を許可しない」を選択することでユーザの同意を禁止可能
- Entra IDポータル>エンタープライズアプリケーション>セキュリティ>同意とアクセス許可>ユーザーの同意設定



同意フィッシングへの対策-防御-ユーザの同意制限(2/2)

- 設定変更後にユーザがアプリケーションに対して同意できなくなる
- ただし、設定変更後でも管理者であればアプリケーションに同意可能

同意フィッシングへの対策-防御-管理者の同意フレームワーク(1/6)

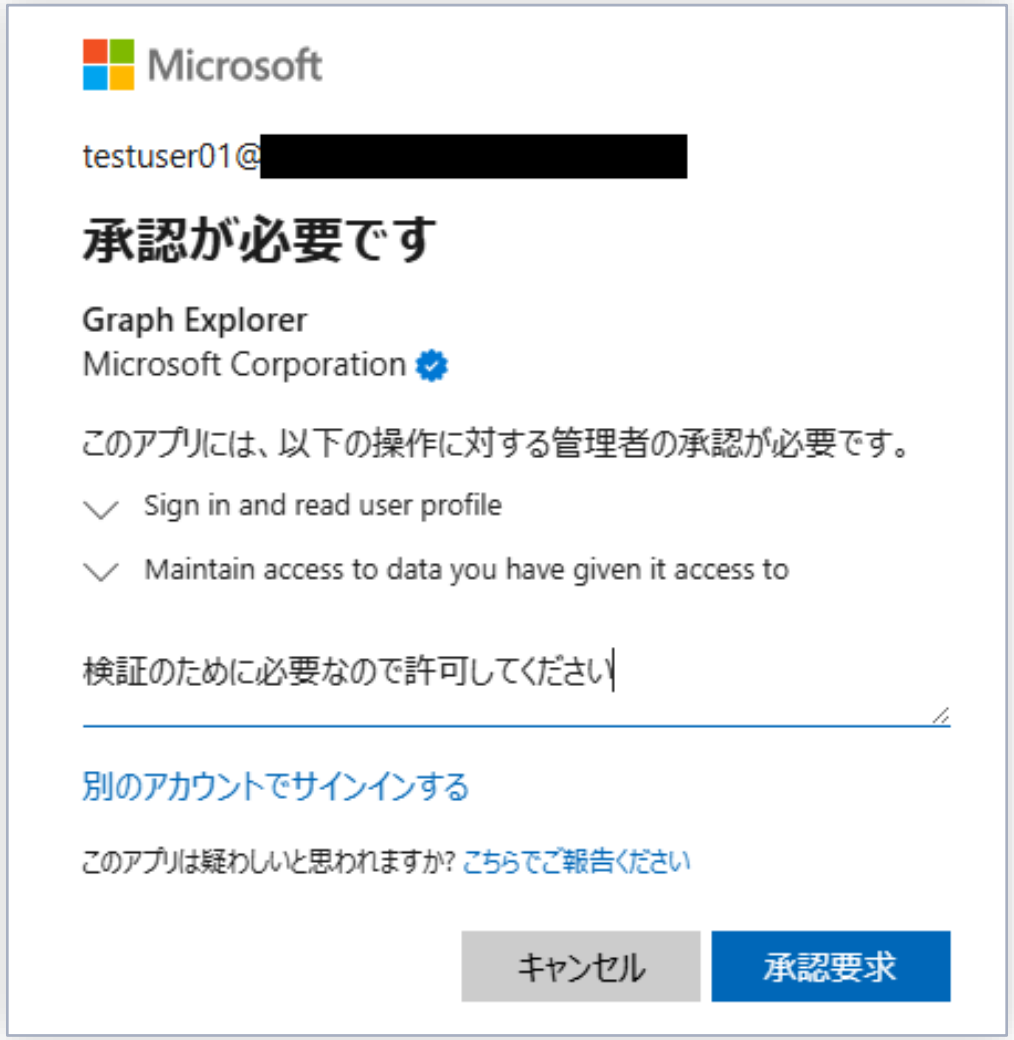
ユーザの同意を管理者がコントロールしたい場合、管理者の同意フレームワークが有効

- 「管理者の同意設定」にて設定可能
- レビュー担当者を設定する必要あり

参考： https://learn.microsoft.com/ja-jp/entra/identity/enterprise-apps/admin-consent-workflow-overview

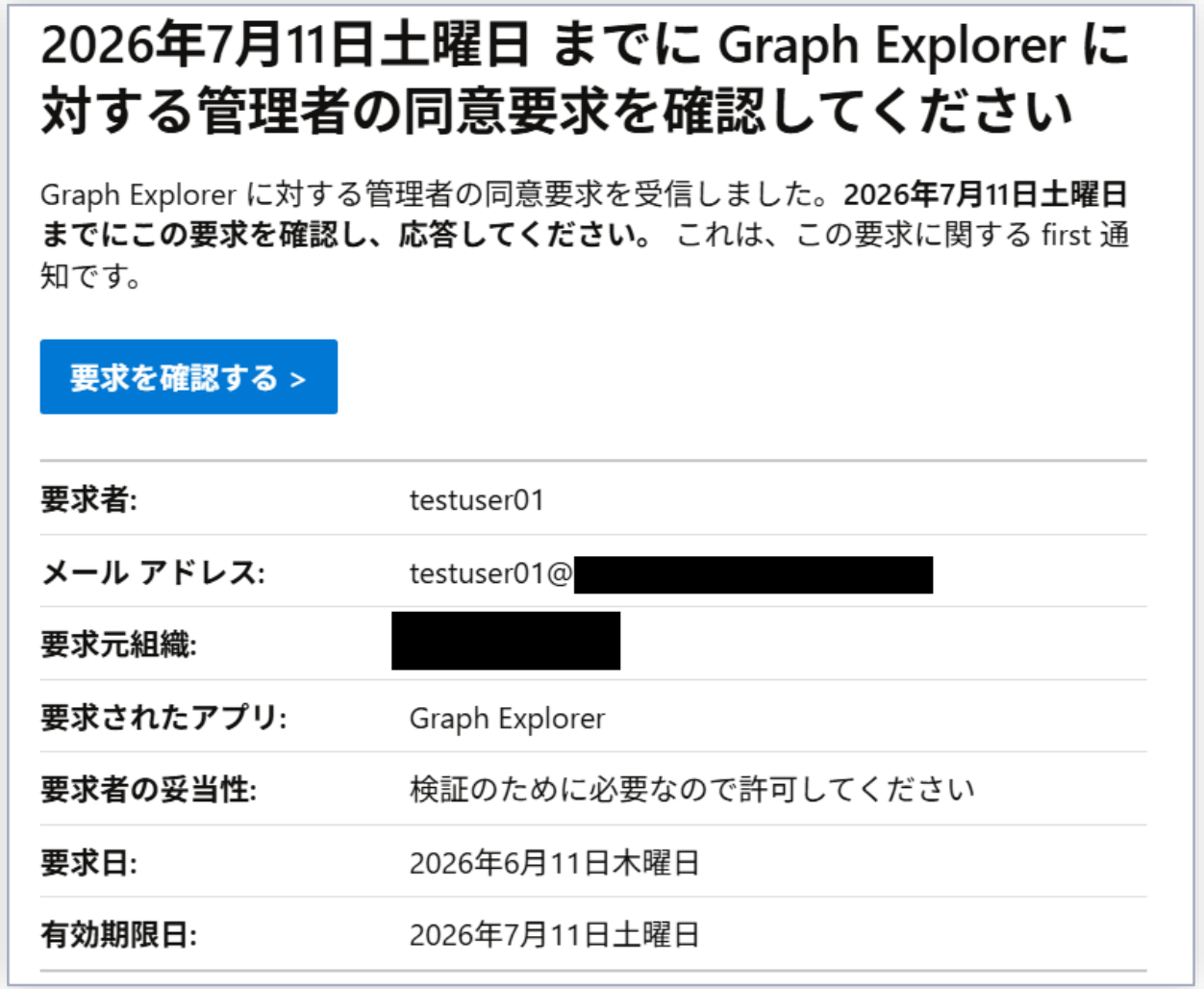
同意フィッシングへの対策-防御-管理者の同意フレームワーク(2/6)

ユーザが同意できない場合、レビュー担当者に対して同意要求が可能



同意フィッシングへの対策-防御-管理者の同意フレームワーク(3/6)

レビュー担当者にアプリケーションに対する管理者の同意要求メールが届く



2026年7月11日土曜日 までに Graph Explorer に対する管理者の同意要求を確認してください

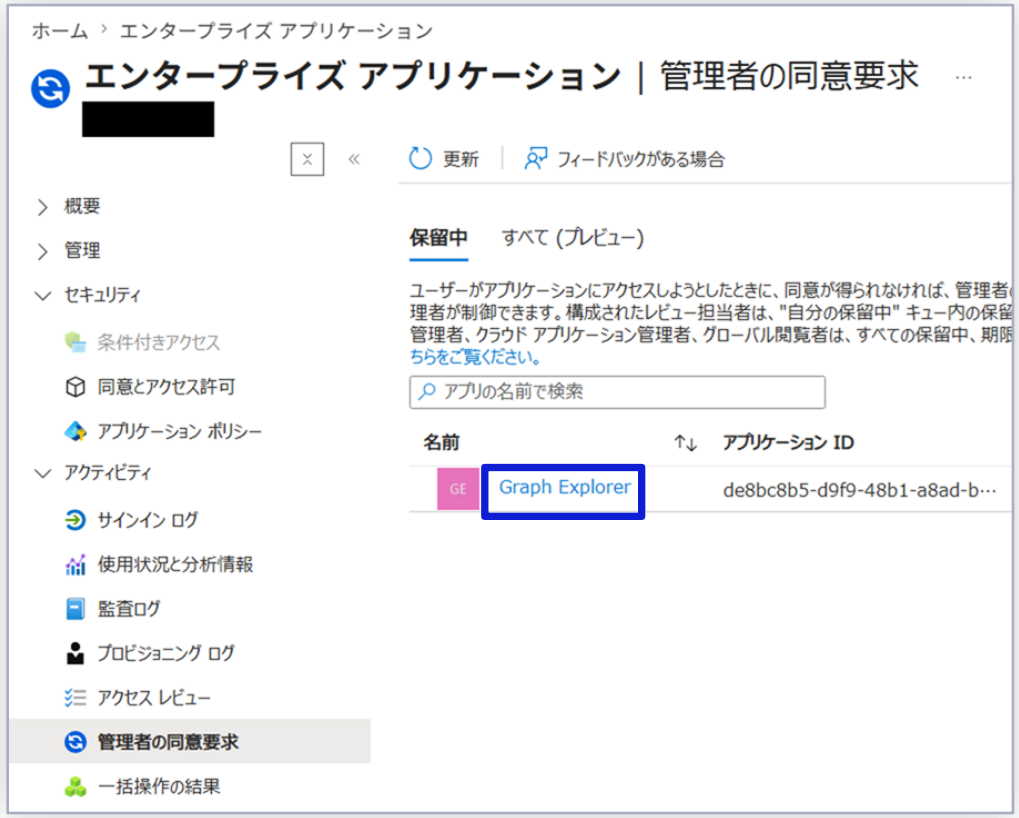
Graph Explorer に対する管理者の同意要求を受信しました。**2026年7月11日土曜日までにこの要求を確認し、応答してください。** これは、この要求に関する first 通知です。

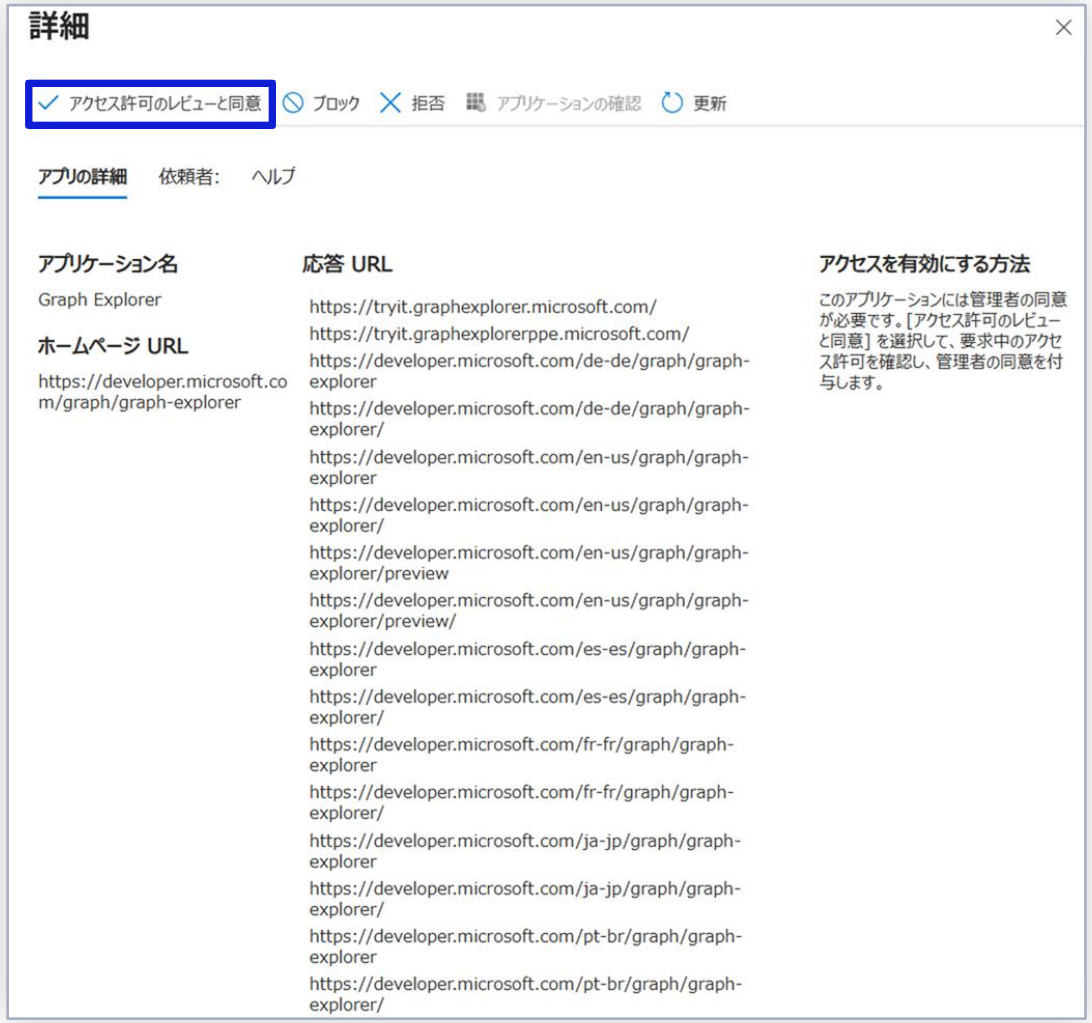
要求を確認する >

要求者:	testuser01
メール アドレス:	testuser01@[redacted]
要求元組織:	[redacted]
要求されたアプリ:	Graph Explorer
要求者の妥当性:	検証のために必要なので許可してください
要求日:	2026年6月11日木曜日
有効期限日:	2026年7月11日土曜日

同意フィッシングへの対策-防御-管理者の同意フレームワーク(4/6)

レビュー担当者が対象のアプリケーションを選択し、「アクセス許可のレビューと同意」を選択





同意フィッシングへの対策-防御-管理者の同意フレームワーク(5/6)

アクセス許可を確認し、問題がなければ「承諾」を選択

同意フィッシングへの対策-防御-管理者の同意フレームワーク(6/6)

- 同意フレームワークでの同意は「管理者の同意」となる
- 「管理者の同意」では、全てのユーザが同意なしに承諾したアプリケーションを利用可能に
- テナント全体での利用が適さないアプリケーションは別方法で個別に同意付与可能

参考：
https://learn.microsoft.com/ja-jp/entra/identity/enterprise-apps/user-admin-consent-overview#admin-consent
https://learn.microsoft.com/ja-jp/entra/identity/enterprise-apps/grant-consent-single-user?pivots=msgraph-powershell#grant-consent-on-behalf-of-a-single-user

同意フィッシングへの対策-事後対応(1/2)

アプリケーションを非アクティブ化することで一時的にアクセス許可を無効化可能

- Entra IDポータル>管理>エンタープライズアプリケーション>“不正なアプリケーション”>プロパティ
- アプリケーションを削除することでも対応可能だが、調査が完了するまでは非アクティブ化を推奨

参考：https://learn.microsoft.com/ja-jp/entra/identity/enterprise-apps/disable-user-sign-in-portal

同意フィッシングへの対策-事後対応(2/2)

非アクティブ化後に攻撃者が作成したアプリケーションと紐づく365-Stealerで アクセストークン取得の失敗を確認

出典：https://github.com/AlteredSecurity/365-Stealer

同意フィッシングへの対策-検知

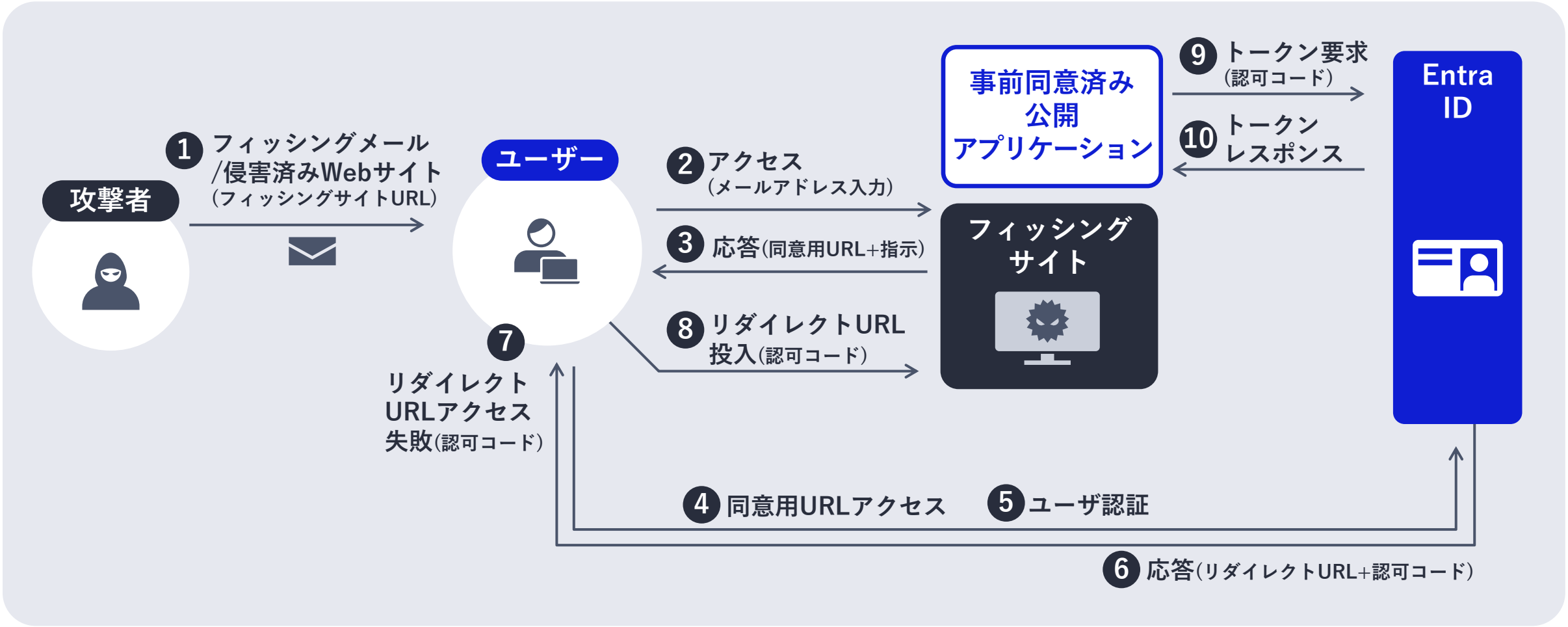
Entra ID監査ログで「Consent to application」イベントを探すことが有効

8.【参考】ConsentFix

【参考】ConsentFix-流れ

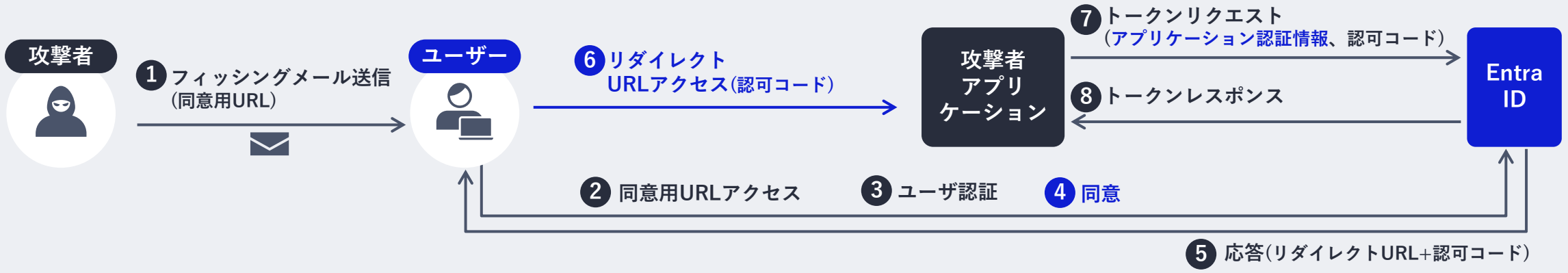
- 同意フィッシング(Consent Phishing)で使用された認可コードフローの悪用とClickFixを組み合わせた攻撃
- 事前同意済みのアプリケーションを使用し、認可コードの受け渡しを被害者自身にさせる

参考： https://www.proofpoint.com/jp/blog/threat-insight/clipboard-compromise-powershell-self-pwn

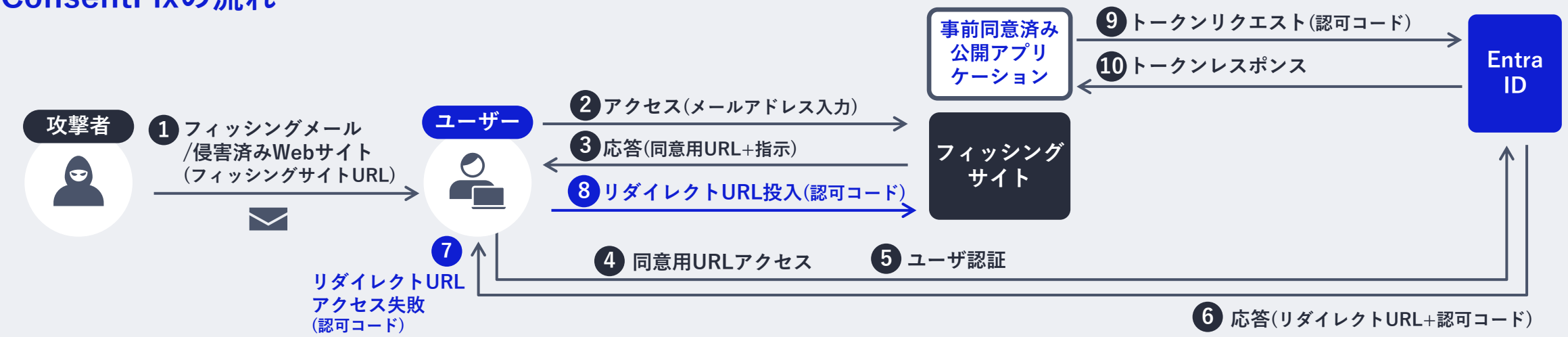


【参考】ConsentFix-同意フィッシングとの比較

同意フィッシングの流れ

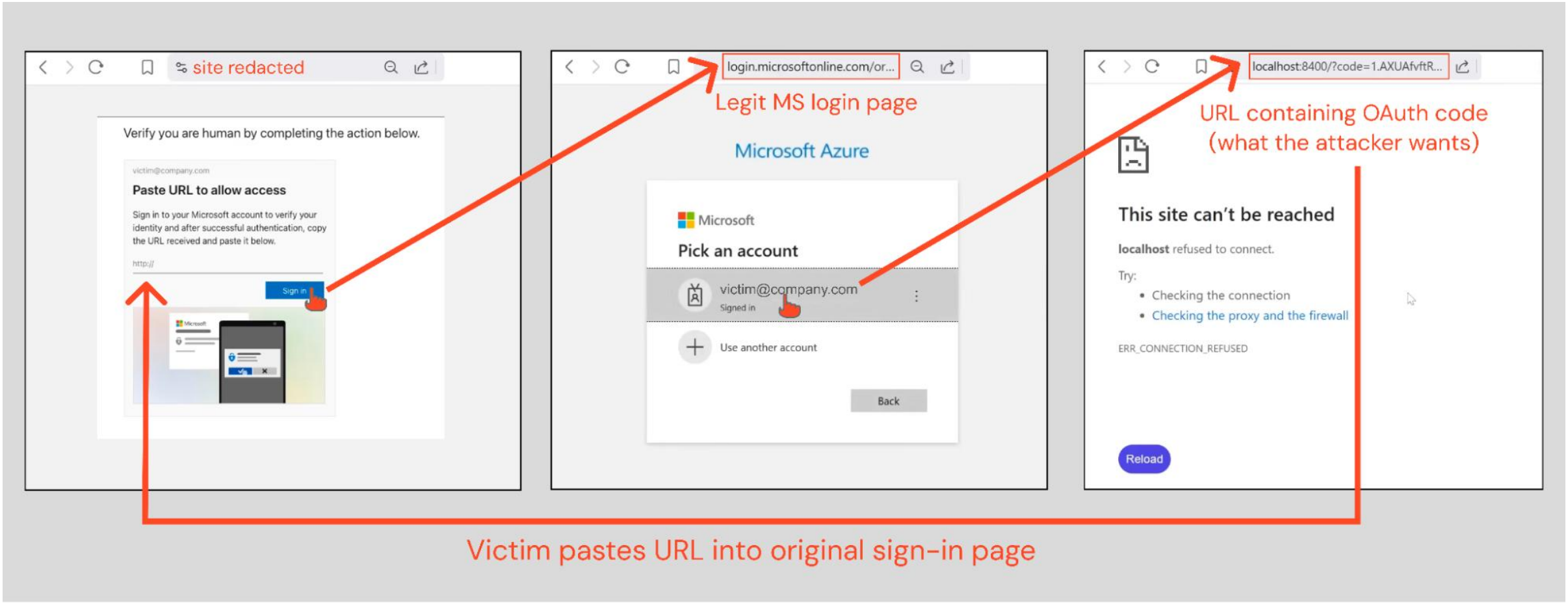


ConsentFixの流れ



【参考】ConsentFix-画面イメージ

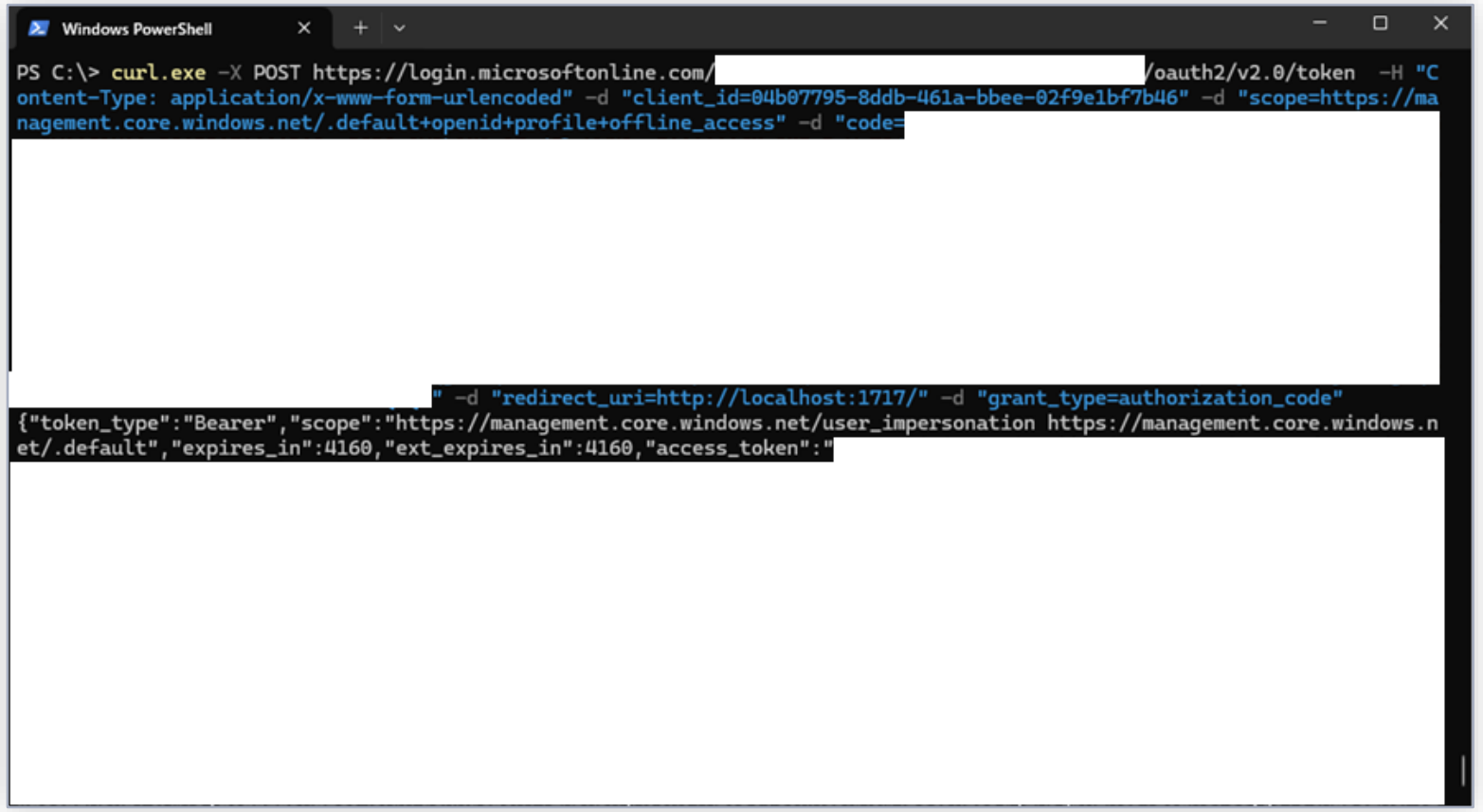
Push Security社が確認したConsentFixの画面イメージ



出典：https://pushsecurity.com/blog/consentfix/

【参考】ConsentFix-手順再現

- 公開情報から読み取ることができるConsentFixの手順をAzure CLIのアプリケーションIDを指定し再現
- リダイレクトURLにlocalhostを指定した場合でも異なるIPアドレスから認可コードと
  アクセストークン発行が可能



【参考】ConsentFix-対策(1/4)

- **ConsentFixは事前同意済みアプリケーションを悪用する、同意フィッシングの対策は有効でない**
- **ConsentFixに悪用され得るアプリケーションについて下記参照**
  - Entra ID First Party Apps & Scope Browser 参考：https://entrascopes.com/
- **事前同意済みのアプリケーションのサービスプリンシパルを作成し、ユーザ割り当てを必須にする**
  - 例：Azure CLI

参考：https://www.glueckkanja.com/en/posts/2025-12-31-vulnerability-consentfix

```
PS C:¥> Connect-MgGraph -Scopes "Application.ReadWrite.All", "AppRoleAssignment.ReadWrite.All"
Welcome to Microsoft Graph!

Connected via delegated access using [redacted]
Readme: https://aka.ms/graph/sdk/powershell
SDK Docs: https://aka.ms/graph/sdk/powershell/docs
API Docs: https://aka.ms/graph/docs

NOTE: You can use the -NoWelcome parameter to suppress this message.
NOTE: Sign in by Web Account Manager (WAM) is enabled by default on Windows systems and cannot be disabled when using th
e default ClientId.
To disable WAM run Set-MgGraphOption -DisableLoginByWAM $true and then use a custom ClientId.

PS C:¥> New-MgServicePrincipal -AppId "04b07795-8ddb-461a-bbee-02f9e1bf7b46"

DisplayName         Id                                   AppId                                SignInAudience
-----------         --                                   -----                                --------------
Microsoft Azure CLI [redacted]                           04b07795-8ddb-461a-bbee-02f9e1bf7b46 AzureADandPersonalMicr...


PS C:¥>
PS C:¥> Update-MgServicePrincipal -ServicePrincipalId [redacted] -AppRoleAssignmentRequired:$true
PS C:¥>
```

【参考】ConsentFix-対策(2/4)

前項の対策により、Azure CLIに紐づく認可コードが発行できなくなったことを確認

【参考】ConsentFix-対策(3/4)

Azure CLIの利用が必要なユーザをサービスプリンシパルに割り当てる

```
PS C:¥> New-MgServicePrincipalAppRoleAssignedTo -ServicePrincipalId [redacted] -PrincipalId [redacted]
[redacted] -ResourceId [redacted] -AppRoleId "00000000-0000-0000-0000-000000000000"

DeletedDateTime Id                                   AppRoleId                            CreatedDateTime     PrincipalDisplayName
--------------- --                                   ---------                            ---------------     --------------------
                [redacted]                           00000000-0000-0000-0000-000000000000 2026/06/15 12:42:38 testuser01


PS C:¥>
```

【参考】ConsentFix-対策(4/4)

Azure CLIの利用が必要なユーザに認可コードが発行され、Azure CLIを利用可能であることを確認

9.まとめ

まとめ

同意フィッシングは
多要素認証を突破する
強力な攻撃

低権限のアクセス許可でも
攻撃者の情報収集に悪用され、
更なる攻撃に繋がる可能性あり

攻撃に対する脅威を認識いただき、
少しでもセキュリティ対策の強化に繋がれば幸いです

\Orchestrating a brighter world