多要素認証に対してセッション ID を取得する中間者攻撃ツール Evilginx の評価

関口 智大　菊池 浩明 †

明治大学総合数理学部 †

1　はじめに

Microsoft 社の報告 [1] によれば，多要素認証 Multi-Factor Authentication(MFA) の導入が広がる一方で，Adversary-in-the-Middle（AiTM）と呼ばれる中間者攻撃型フィッシングは 2024 年に 146% 増加したとされている．太田ら [2] は国内主要 102 サイト中 87 サイト（85%）が Evilginx による AiTM 攻撃に対して脆弱である可能性を指摘している．これらの事例は，MFA を導入していても AiTM 攻撃により迂回され得ることを示している．MFA 環境に残存する脆弱性の対策が求められている．

しかし，AiTM 攻撃が MFA を迂回する具体的過程や，認証方式ごとの安全性を体系的に検証した研究は十分とはいえない．特に，中間者攻撃ツール Evilginx に関する実証的分析は不足しており，認証方式が攻撃に対してどの様に脆弱性があるか不明であった．

そこで, 本研究では，AiTM 攻撃が単一の認証をバイパスするだけでなく，セッション ID を取得することでログイン状態（セッション）を継承し得る脅威に着目する．主要な MFA 方式を対象として，AiTM 攻撃に対する単一ログイン耐性およびセッション ID 取得率を明らかにする．

本研究は，以下の新規性を有する．

- Evilginx を用いた AiTM 型中間者攻撃の挙動を再現し，各認証方式の耐性を実験的に検証する．
- Evilginx がセッション ID を取得して, ログインフェーズを経ずに侵入できるかを明らかにする．

2　基本定義

2.1　セッション ID

セッション ID は，Web サービスにおいてユーザのログイン状態を保存し，複数の対話メッセージを結びつけたセッションを管理するために一時的に発行される識別子である．

2.2　先行研究 [2]

2024 年，太田ら [2] は国内外 102 サイトの二要素認証の導入状況を調査した．調査の結果，全体の 68 サイトが二要素認証を導入し，ソーシャルログインを含めると 85 サイトで導入されていることが確認された．また，SMS, 電話,Email を用いた OTP 認証方式，認証アプリ（TOTP），専用アプリ，プッシュ通知など多くの認証方式が AiTM 攻撃に対して脆弱である可能性を指摘した．一方で，セキュリティキーやパスキーといった公開鍵暗号方式を用いる認証方式は，AiTM 攻撃に対して安全であると主張している．

3　実験

3.1　実験方法

本研究では，以下の三つの方法を用いる．

(1) Evilginx を用いて代表的な Web サイトに対する AiTM 型中間者攻撃挙動を再現し，各認証方式の耐性を検証する．
(2) Evilginx を用いて, 代表的な Web サービスのセッション ID を窃取し, ログインなしでセッションを乗っ取ることができるかを調査する．

図 1 に，中間者攻撃者が認証情報およびセッション ID を取得する一連のフローを図示する。

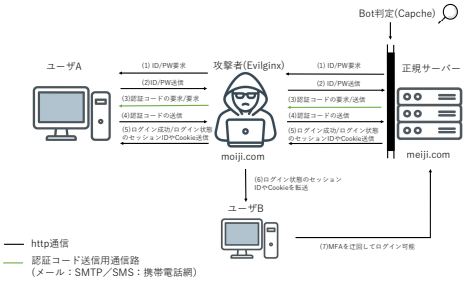

図 1　AiTM 型中間者攻撃の概要図

Evaluation of Session ID Retrieval via Adversary-in-the-Middle Attack tool Evilginx to Multi-Factor Authentication

†Tomohiro Sekiguchi, Hiroaki Kikuchi, School of Interdisciplinary Mathematical Science, Meiji University.

3.2 実験結果

3.2.1 Evilginx を用いた AiTM 攻撃の結果

表 1 に,2025 年に Web サービス 17 サイトに対して AiTM 型中間者攻撃挙動を再現した, 検証結果を示す. なお, 多要素認証を導入していないサイトを「No 2FA」,」と表記する.

表 1　認証方式別の AiTM 攻撃結果（17 サイト）

Login 確立	SessionID	個人情報	No 2FA	SMS	Email	TOTP	合計
×	✓	✓	1	2	3	4	10
×	×	✓	0	0	1	2	3
×	×	×	3	0	0	0	3

以上の結果から，17 サイト中 13 サイト（多要素認証なし，TOTP，SMS ／メール OTP）において，何らかの情報が AiTM 攻撃によって取得可能であったことが確認された．一方で，Bot 判定機構 (Captch など) を導入しているサービスでは攻撃が成立せず，認証方式に加えて，認証以外の防御機構も AiTM 耐性に大きく影響することが示唆された.

3.2.2 セッション ID を窃取

Evilginx を用いて, 代表的な Web サービスのセッション ID を窃取し，ログイン操作を行うことなくセッションを乗っ取ることが可能かを調査した.

```
[10:44:10] [dbg] POST: /user/top/
[10:44:10] [dbg] POST body =
[10:44:10] [dbg] .syosetu.com: ks2 =
    z90fe5ta39f3
[10:44:10] [dbg] .syosetu.com: autologin =
2700594%3C%3
    Ecae41c11615f29e87e3a4ad7246fa75e40df622d
957bd30fcaf12be9b79c7e3a%3C%3E1709057219
```

図 2　セッション ID 窃取

図 2 に，小説投稿サイト「小説家になろう (syosetu.com)」に対して Evilginx を用いた中間者型攻撃を実施し，cookie 挙動を観測した結果を示す. POST の中身は無く, その下に ks2 と autologin という 2 種類の cookie が確認された. 次に，別の PC 上のブラウザにおいて Google Developer Tools を用い，取得した autologin Cookie を手動で追加したところ，2FA による追加認証を行うことなくログインが成立することを確認した.

この結果から，autologin Cookie はログイン状態を管理するセッション ID として機能しており，Evilginx によって当該セッション ID が窃取されることで，認証操作を経ずにセッションが再利用可能となることが示された.

3.3 本研究の限界

(1) Evilginx による AiTM 攻撃は実験環境での検証であり，実運用環境では追加の防御策が存在する可能性がある.

3.4 本研究の倫理配慮

(1) 本研究では, アカウント本人の同意の元で行う動作検証を除いて, 実在するシステムへの検証は行っていない.

4 まとめ

本研究では，多要素認証環境が AiTM 攻撃に対してどの程度耐性を有するかを明らかにするため，Evilginx を用いた攻撃実験，認証方式の導入率比較を行った．OTP ベースの認証方式は AiTM 攻撃に脆弱である一方，Bot 判定機構など認証方式以外の追加的防御策が AiTM 耐性向上に有効であることが確認された．また，cookie を窃取して別の端末でログインが可能であることを確認した. 今後は，Passkey に対する AiTM 攻撃の影響評価や，サービス横断での認証強度比較など，より詳細な分析を進めたい.

参考文献

[1] Microsoft,“Microsoft Digital Defense Report 2024”, 2024. (https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/Microsoft%20Digital%20Defense%20Report%202024%20(1).pdf,2025 年 5 月参照)

[2] 太田和希，菊池浩明,“2FA をバイパスする中間者攻撃ツール Evilginx によるフィッシング攻撃の脅威分析”，情報処理学会第 87 回全国大会,1ZE-04, Vol. 3, pp.535-536, 2025.

[3] Evilginx Pro (https://evilginx.com/,2025 年 4 月参照)