

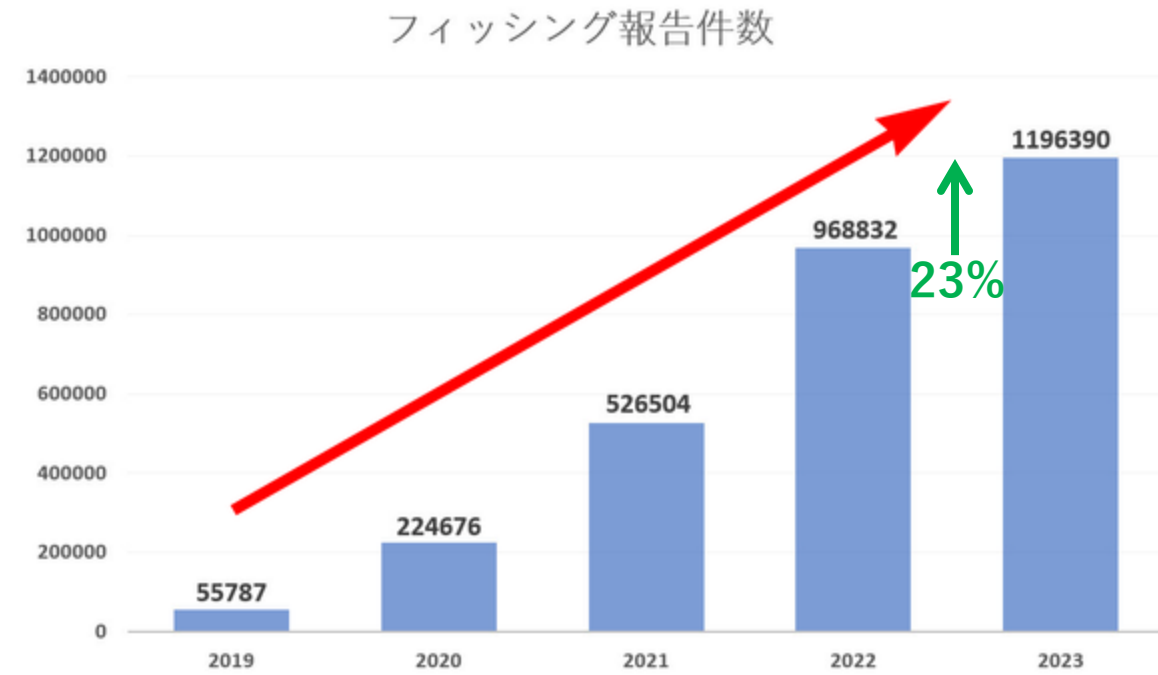
# 2FA をバイパスする中間者攻撃ツール Evilginx によるフィッシング攻撃の脅威 分析

明治大学 総合数理学部

太田和希 菊池浩明

# 背景

- 2023年フィッシングは119万件(23%増)



[Ascii, 2024年6月]

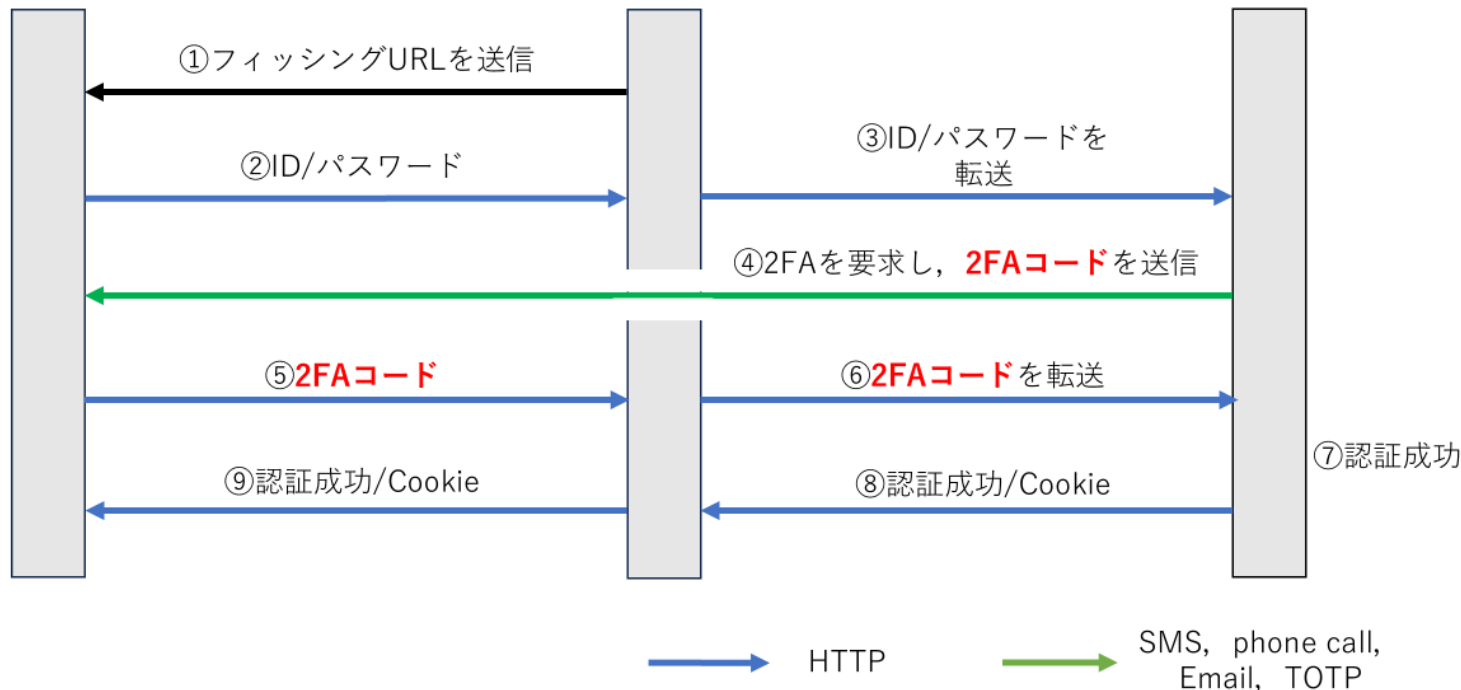
- フィッシング攻撃への対策として**二要素認証(2FA)**がある  
→しかし、**Adversary-in-the-Middle(AiTM)攻撃**によって破られる可能性がある

# Adversary-in-the-Middle攻撃(中間者攻撃)

## 攻撃時



2FAを用いた認証(SMS、phone call、Email、TOTP(認証アプリ))



## 通常の場合

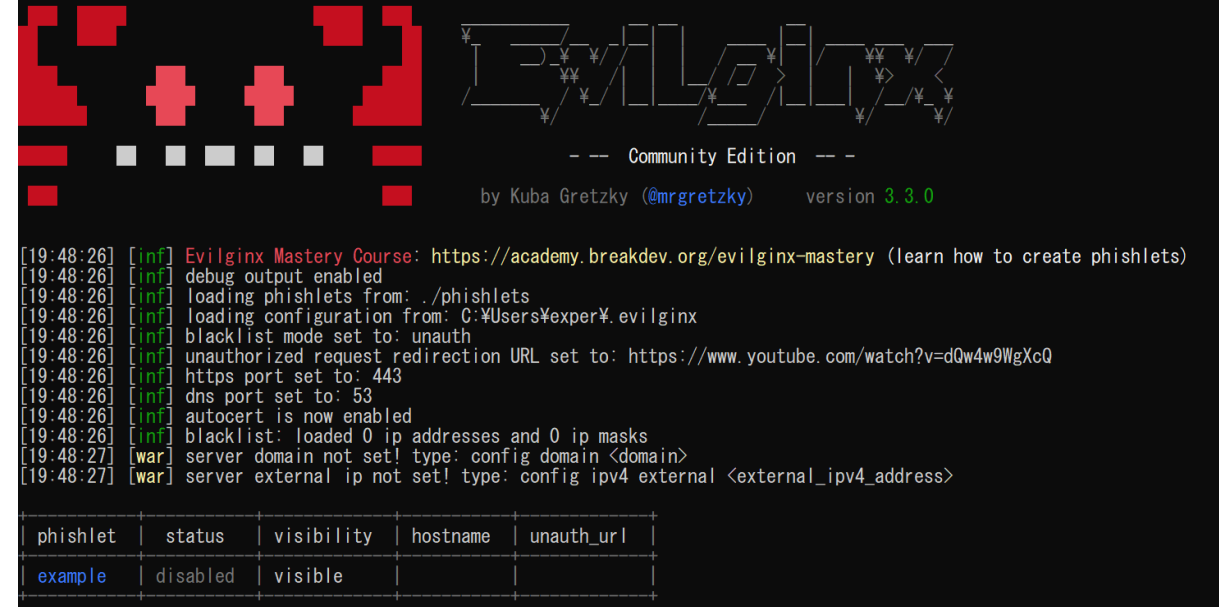
ID/パスワードを入力後、送られてくる2FAコードを入力する

## AiTM攻撃を行った場合

偽サイトに誘導し、ID/パスワード、2FAコードを転送することで2FAを破る

# Evilginx

- AiTM攻撃を行うオープンソースツールキット



The screenshot shows the Evilginx terminal interface. At the top, there is a red ASCII art logo and the text "Evilginx Community Edition" and "by Kuba Gretzky (@mrgretzky) version 3.3.0". Below this, there are several log messages indicating the startup process, including loading phishlets, configuration, and setting various options like blacklist mode, redirection URL, and ports. At the bottom, there is a table showing the status of loaded phishlets.

```
[19:48:26] [inf] Evilginx Mastery Course: https://academy.breakdev.org/evilginx-mastery (learn how to create phishlets)
[19:48:26] [inf] debug output enabled
[19:48:26] [inf] loading phishlets from: ./phishlets
[19:48:26] [inf] loading configuration from: C:\Users\exper\evilginx
[19:48:26] [inf] blacklist mode set to: unauth
[19:48:26] [inf] unauthorized request redirection URL set to: https://www.youtube.com/watch?v=dQw4w9WgXcQ
[19:48:26] [inf] https port set to: 443
[19:48:26] [inf] dns port set to: 53
[19:48:26] [inf] autocert is now enabled
[19:48:26] [inf] blacklist: loaded 0 ip addresses and 0 ip masks
[19:48:27] [war] server domain not set! type: config domain <domain>
[19:48:27] [war] server external ip not set! type: config ipv4 external <external_ipv4_address>
```

| phishlet | status   | visibility | hostname | unauth_url |
|----------|----------|------------|----------|------------|
| example  | disabled | visible    |          |            |

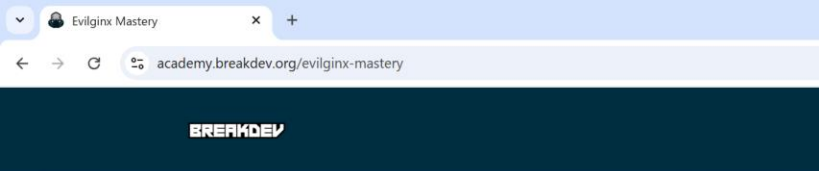
- コマンドベースで操作を行い、サーバやターゲットのウェブサイトの情報を入力して攻撃を行う
- Let's encryptを用いて偽の公開鍵証明書を中間者に発行する

# 正規サイトCと偽サイトBの違い

- 見た目の違いはURLのみ

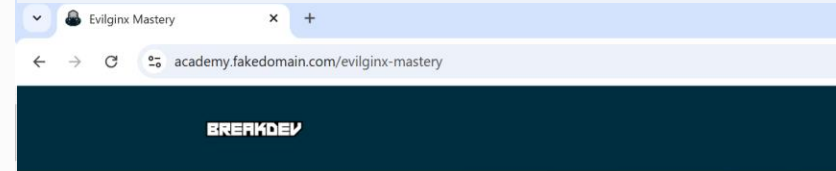
正

academy.breakdev.org/evilginx-mastery



偽

academy.fakedomain.com/evilginx-mastery





- -- Community Edition -- -

by Kuba Gretzky (@mrgretzky)

version 3.3.0

```
[17:26:58] [inf] Evilginx Mastery Course: https://academy.breakdev.org/evilginx-mastery (learn how to create phishlets)
[17:26:58] [inf] debug output enabled
[17:26:58] [inf] loading phishlets from: ./phishlets
[17:26:58] [inf] loading configuration from: C:\Users\kazuk\.evilginx
[17:26:59] [inf] blacklist: loaded 0 ip addresses and 0 ip masks
```

| phishlet | status  | visibility | hostname       | unauth_url |
|----------|---------|------------|----------------|------------|
| example  | enabled | visible    | fakedomain.com |            |

:

# Research Question

1. 正規サイトとフィッシングサイトを区別できるか？
2. Evilginxに対して脆弱なサイトはどのくらいあるのか？

# 1. 正規サイトとフィッシングサイトを区別できるか？

## 実験概要

- 正規サイトとEvilginxを用いて構築したフィッシングサイトの読み込み時間やログイン時間を計測し、比較する

## 実験目的

- 処理速度の差によって一般ユーザーが異変に気付くことができるか明らかにする

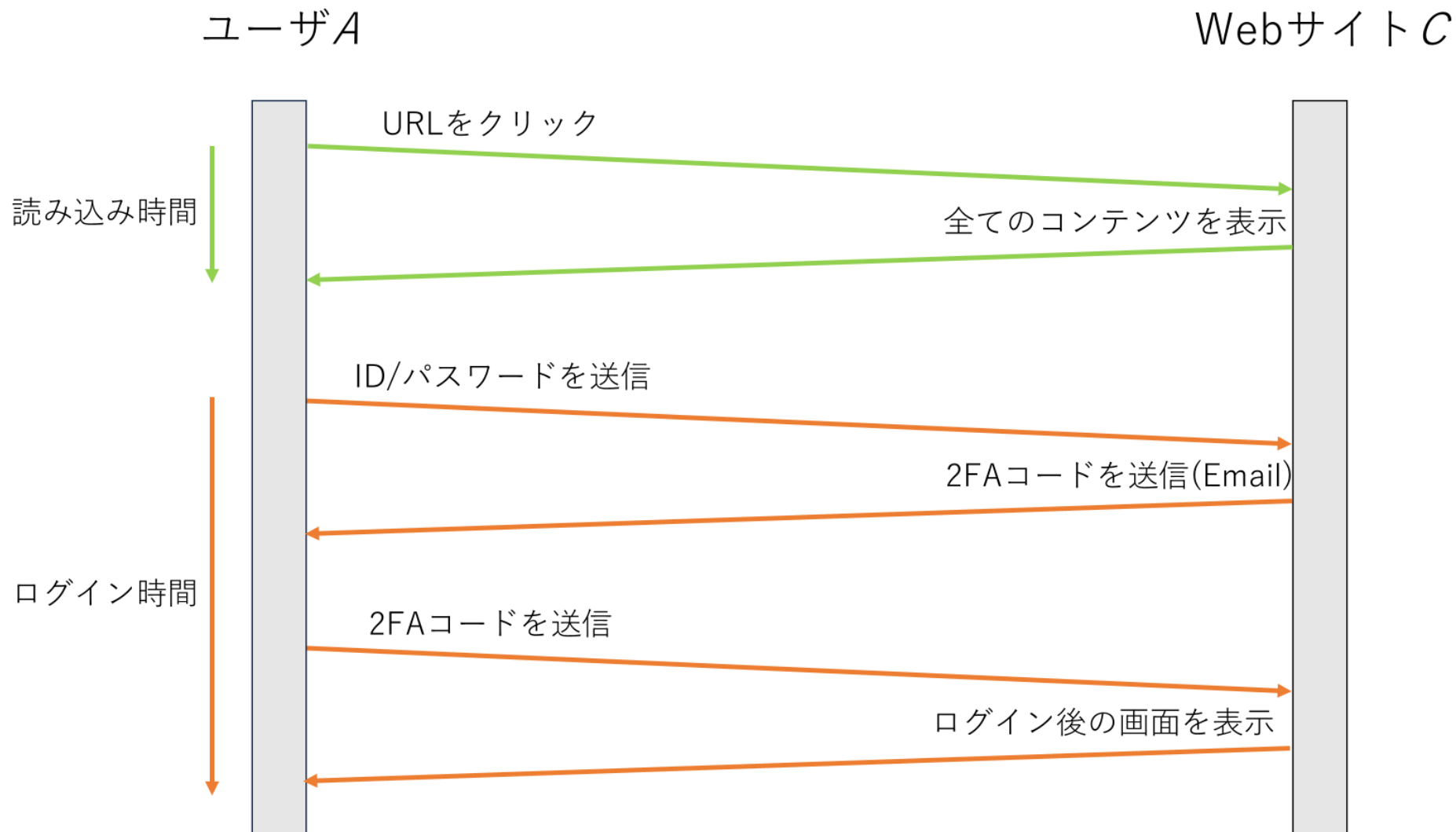
## 実験環境

- 犠牲者ユーザーA：ローカル(Windows)
- 攻撃者B：ローカル(Windows)
- ターゲットWebサイトC：Evilginx Mastery(Evilginx学習サイト、カナダ)



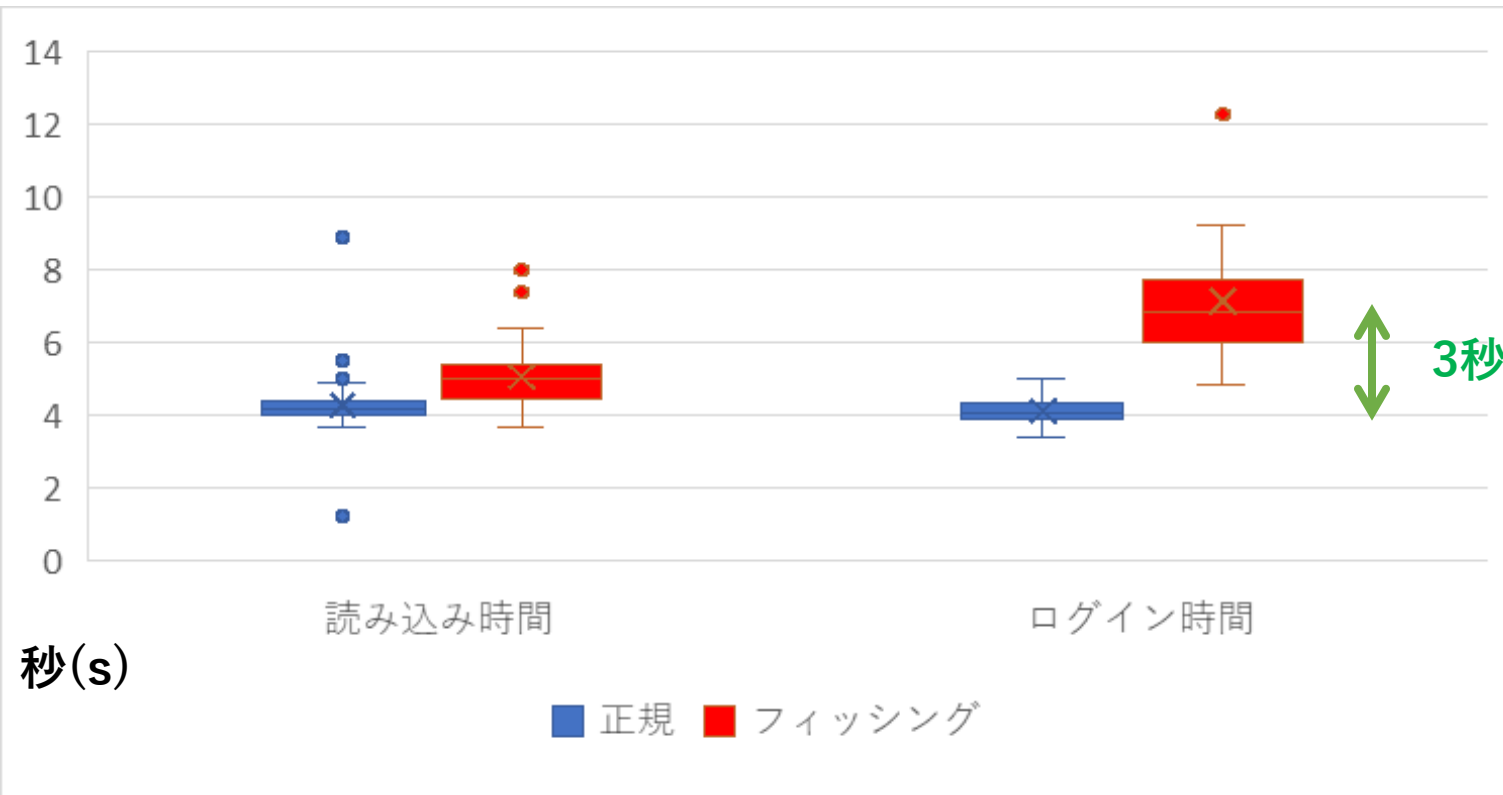
## 実験方法

- それぞれのサイトについて、読み込み時間を50回ずつ、ログイン時間を30回ずつ計測



# 1. 結果

|        |        | 平均値  | 最小値  | 最大値   | 標準偏差 |
|--------|--------|------|------|-------|------|
| 読み込み時間 | 正規     | 4.28 | 1.19 | 8.89  | 0.84 |
|        | フィッシング | 5.04 | 3.64 | 8.02  | 0.87 |
| ログイン時間 | 正規     | 4.10 | 3.38 | 4.97  | 0.41 |
|        | フィッシング | 7.14 | 4.85 | 12.40 | 1.70 |



一般ユーザは3秒の差に**気づくことができない**と推測される

# Research Question

1. 正規サイトとフィッシングサイトを区別できるか？
2. Evilginxに対して脆弱なサイトはどのくらいあるのか？

## 2. Evilginxに対して脆弱なサイトはどのくらいあるのか？

Evilginx(AiTM攻撃)に対して脆弱か安全かはそれぞれのサイトが採用している**2FAの方式によって変わる**

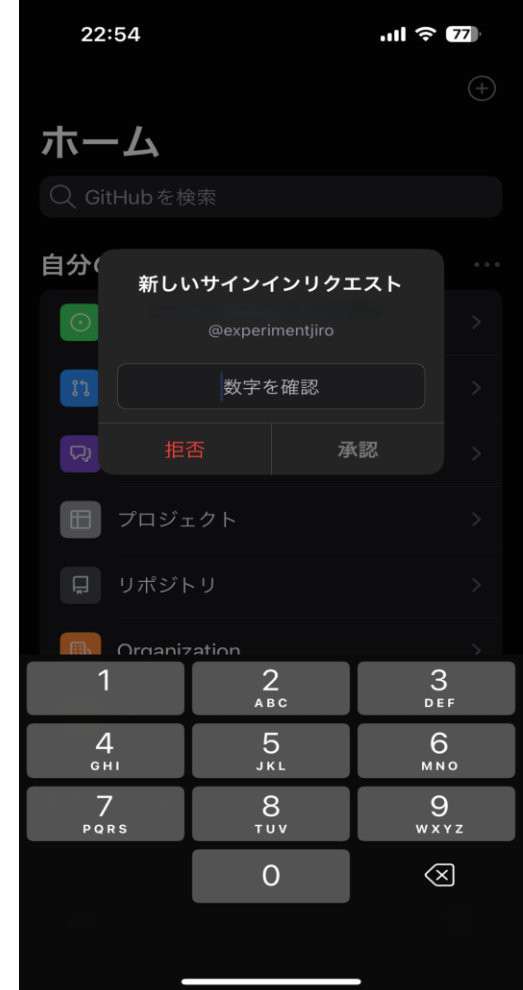
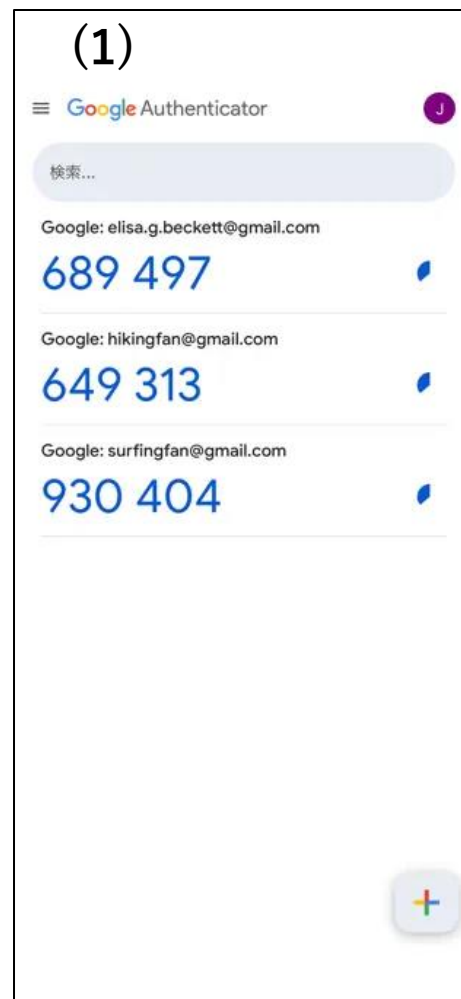
- 2FA方式を8つに分類：SMS、phone call、Email、TOTP(認証アプリ)、専用App、プッシュ通知、security key、passkey

2-1 それぞれの2FA方式が脆弱か安全かを仮定

2-2 サイトの2FA方式を調査し、脆弱なサイトの割合を求める

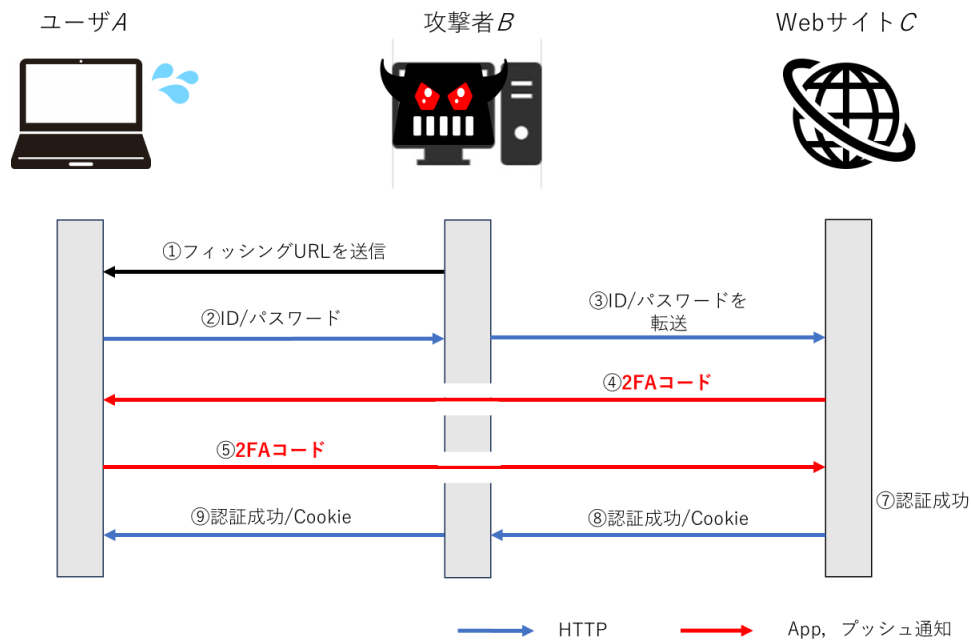
## 2-1 2FA方式と攻撃耐性の仮定

| 2FA 方式       | AiTM 耐性 | 例                       |
|--------------|---------|-------------------------|
| SMS          | ×       |                         |
| phone call   | ×       |                         |
| Email        | ×       |                         |
| TOTP(認証アプリ)  | ×       | Google Authenticator(1) |
| 専用 App       | ×       | GitHub アプリ (2)          |
| プッシュ通知       | ×       |                         |
| security key | ○       | YubiKey(3)              |
| passkey      | ○       | Windows Hello           |



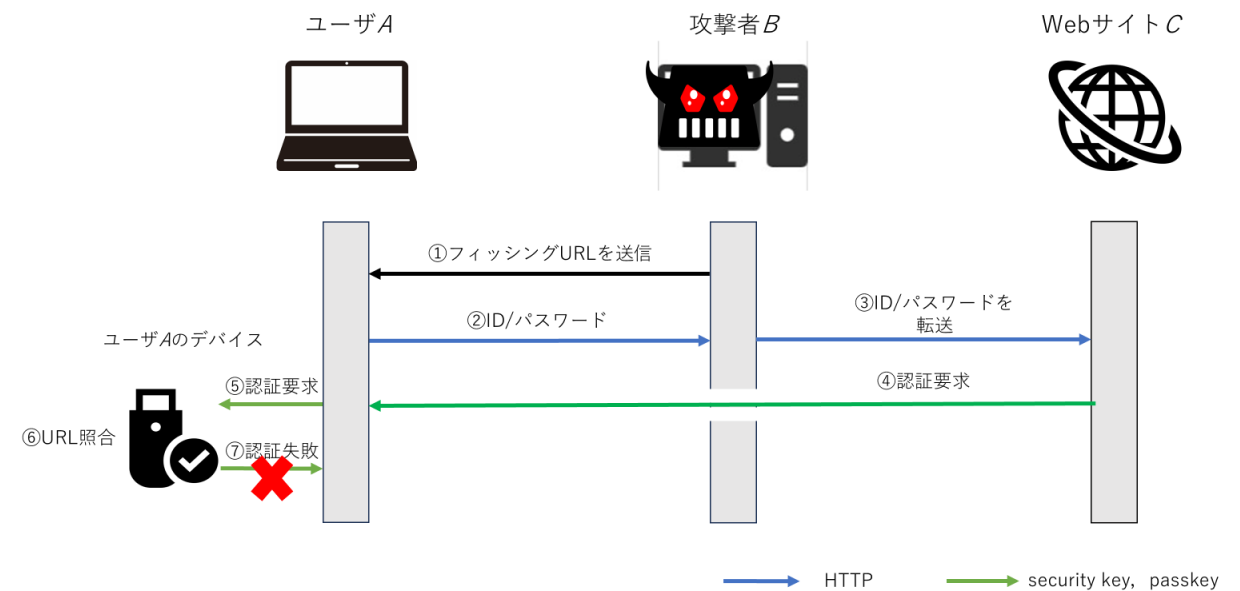
# なぜ専用AppはAiTMに脆弱なのか？

- 専用App, プッシュ通知(脆弱)



→ 攻撃者は2FAコードを盗聴できないが認証には成功する

- security key, passkey(安全)



→ デバイスが正しいURLを保存し、偽のURLと区別が可能。2FAコードは使用されず、公開鍵暗号技術で認証が実施される

## 2-2 主要なWebサイトの2FAの調査

### 調査概要

- 国内 48サイト、国外 54サイトの計102サイトの2FA方式を調査

### 調査目的

- 主要なWebサイトが採用している全2FA方式を明らかにして、Evilginxに対して脆弱なサイトの割合を調査する

### 調査方法

- サイトの**公式**ドキュメントを参照
- ドキュメントがないサイトは自ら**アカウントを作成**し正規ユーザの立場で調査

(情報処理学会「サイバーセキュリティ研究倫理チェックリスト」確認済)

## 2. 調査結果

- 102サイトのうち87サイトが脆弱  
→調査した**約85%**のサイトがEvilginxに対して脆弱

### 調査結果(一部)

**脆弱**

**安全**

| サイト名          | SMS | phone call | Email | TOTP(認証アプリ) | 専用 App | プッシュ通知 | security key | passkey | 結果 | 件  | %    |
|---------------|-----|------------|-------|-------------|--------|--------|--------------|---------|----|----|------|
| Dropbox       | ○   |            |       | ○           |        | ○      | ○            |         | 安全 | 15 | 15 % |
| LINE          |     |            |       |             | ○      |        |              |         | 脆弱 | 87 | 85 % |
| pixiv         |     |            |       | ○           |        |        |              |         | 脆弱 |    |      |
| unity         | ○   |            |       | ○           |        |        |              |         | 脆弱 |    |      |
| Crazy Domains | ○   | ○          |       |             |        |        |              |         | 脆弱 |    |      |



# まとめ

1. 正規サイトとフィッシングサイトを区別できるか？

→3秒の差であり、ユーザが攻撃に気づくのは**難しい**

2. Evilginxに対して脆弱なサイトはどのくらいあるのか？

→102サイトについて87サイト(**85%**)が脆弱

- 2FAや公開鍵証明書があっても攻撃を受ける可能性があることがわかった
- 技術的措置だけでなく、教育や標的メールに対する訓練などの人的な対策が重要である

[illegible]

[illegible]