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

総合数理学部　先端メディアサイエンス学科

菊池研4年　太田和希

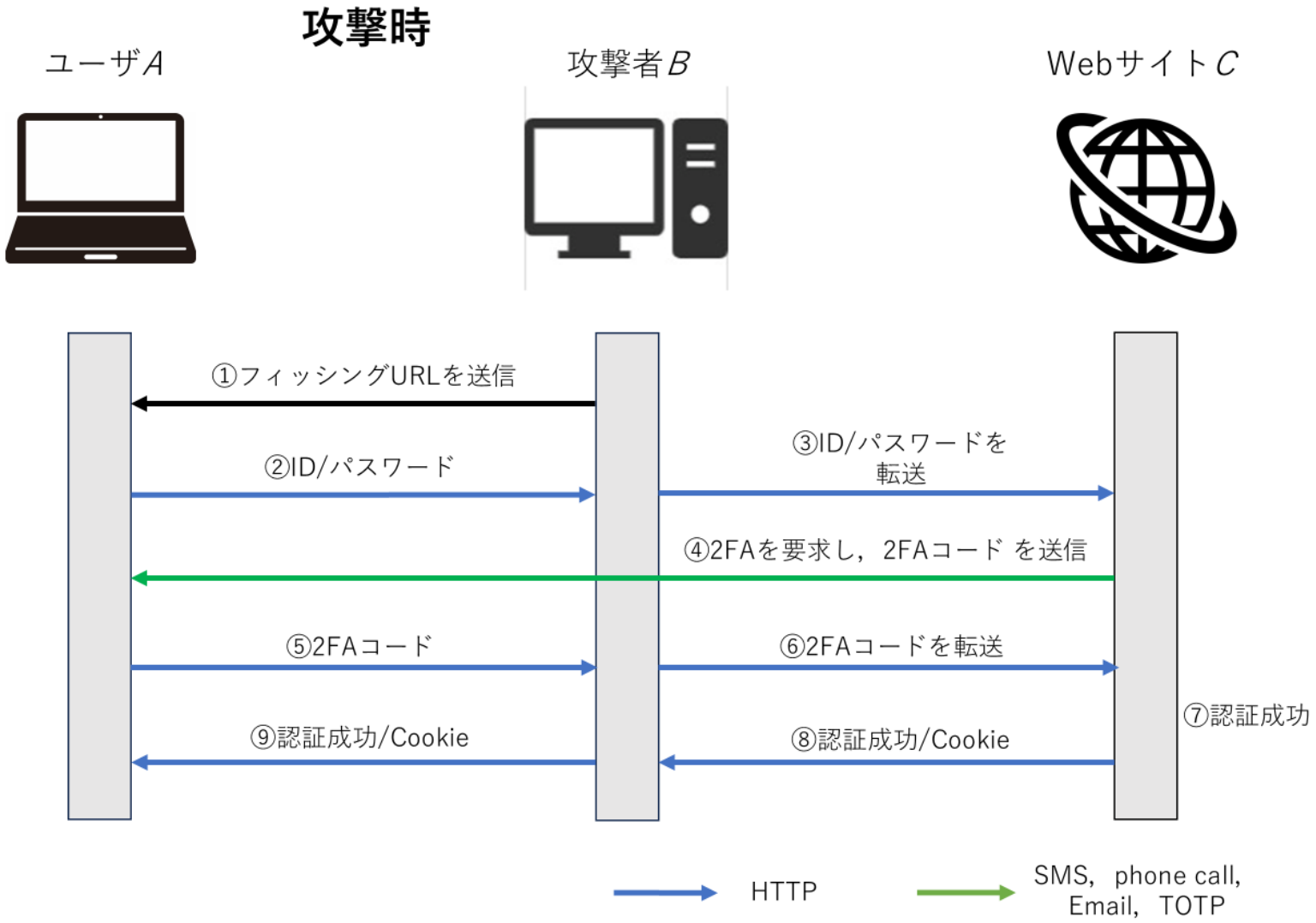
背景

- 2022年に発生したデータ侵害の36%にフィッシングが関与

- 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)



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

通常の場合

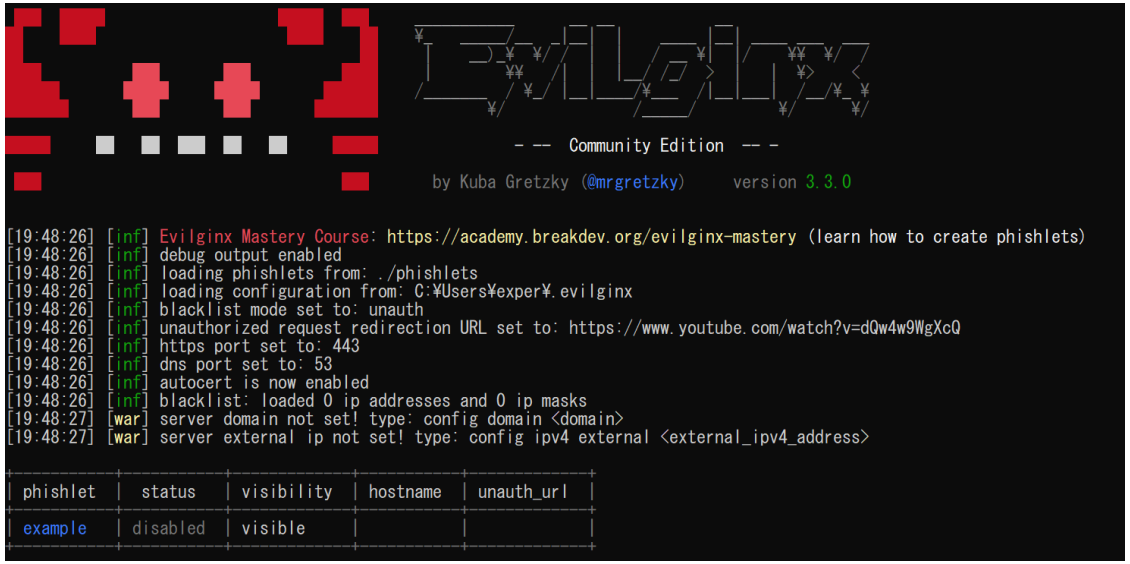
ID/パスワードを入力後、送られてくる2FAコードを入力する

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攻撃を行うツールキット



- 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

- 正規サイトとフィッシングサイトの見た目の違いは**URLのみ**

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？

実験内容

- 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が異変に気付くことができるか推測する

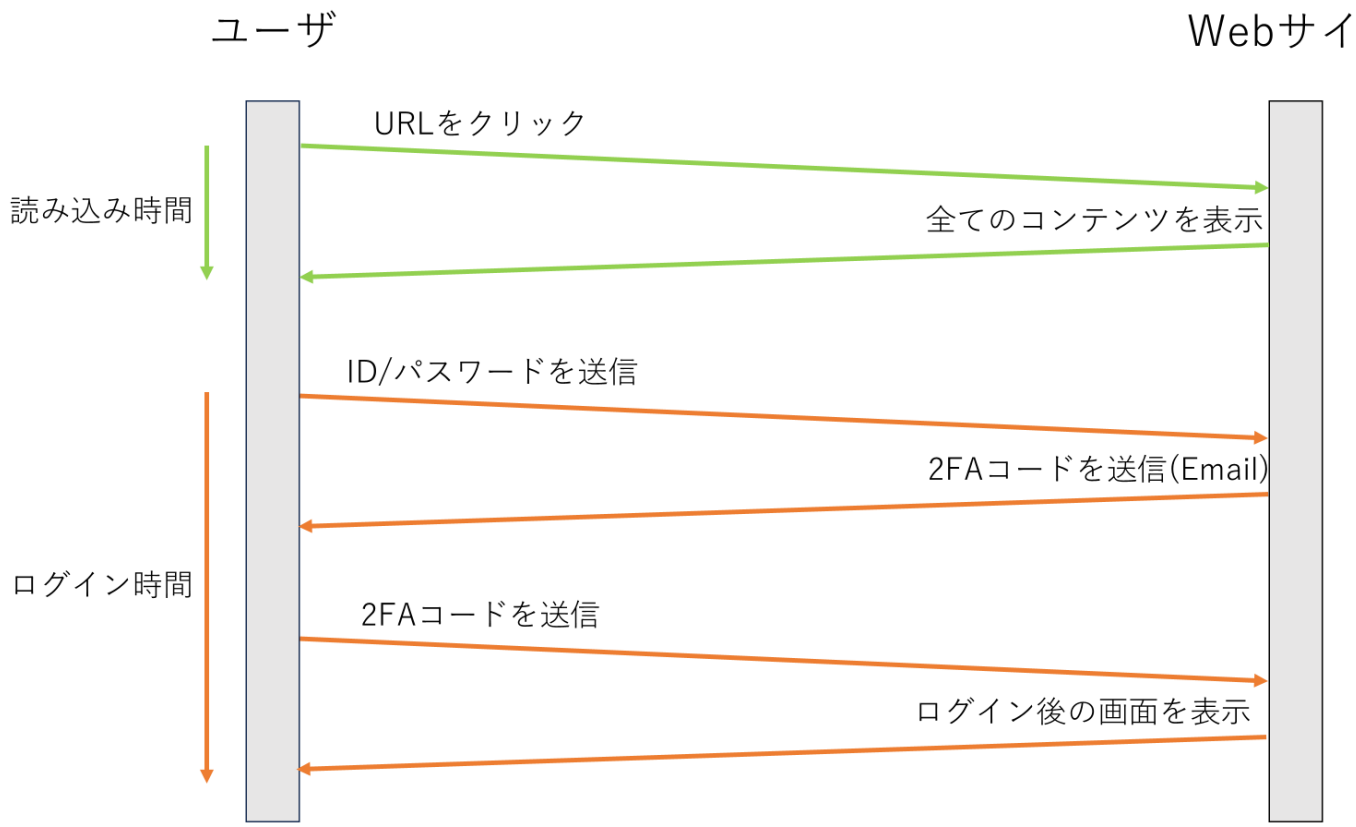
実験環境

- ローカル
- ターゲットWebサイト→Evilginx Mastery(Evilginx学習サイト)

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

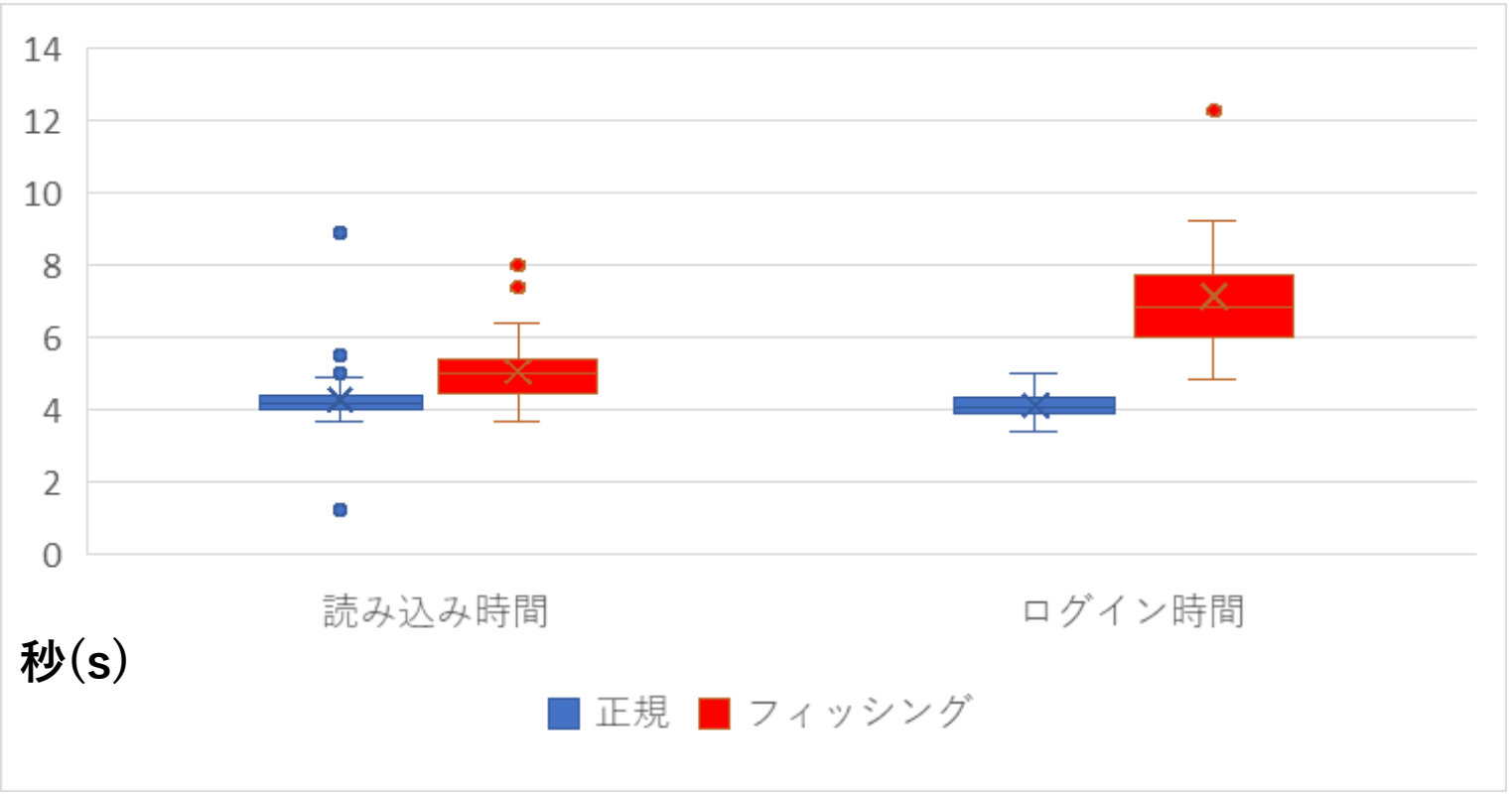
- それぞれのサイトについて、読み込み時間を50回ずつ、ログイン時間を30回ずつ計測



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

秒(s)



→一般ユーザは**気づくことができない**と推測される

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)、App、プッシュ通知、security key、passkey）

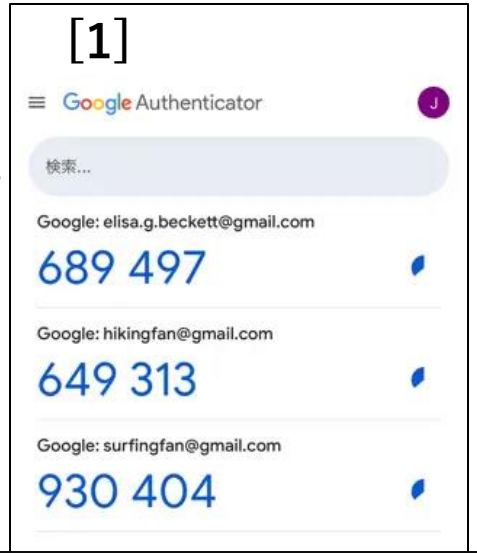
2-1　それぞれの2FA方式が脆弱か安全かを仮定

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

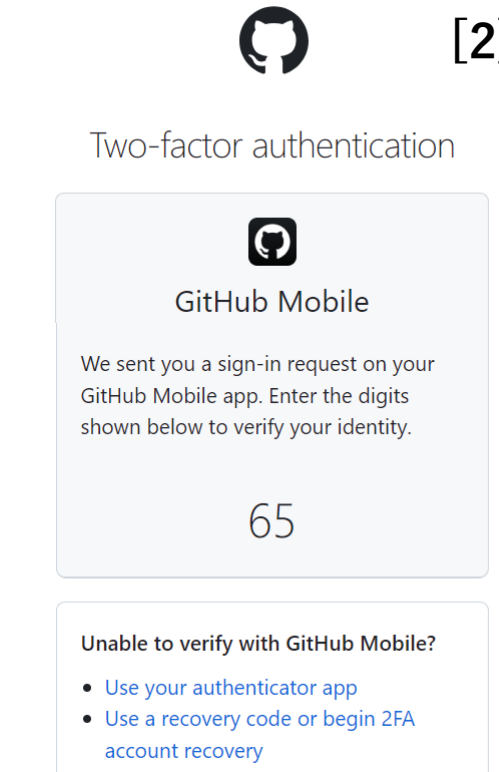
2-1　2FA方式と攻撃耐性

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

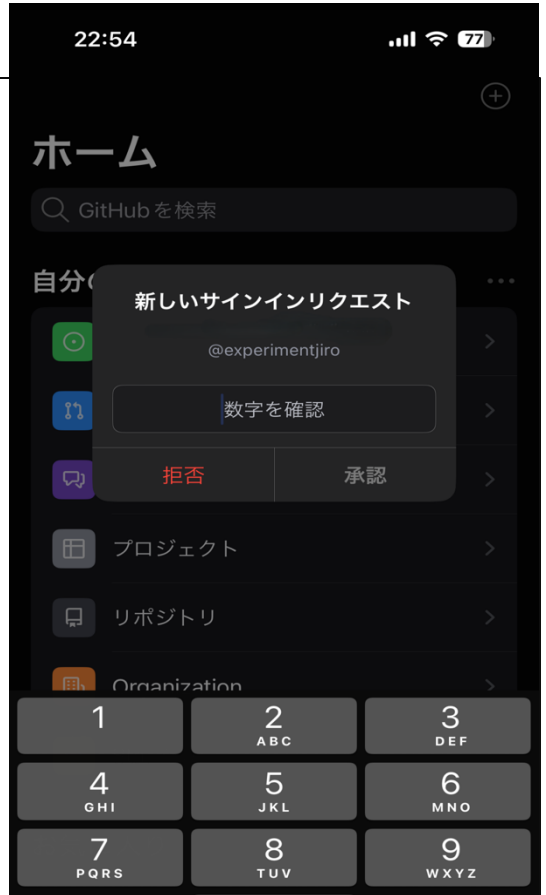
[1]



[2]

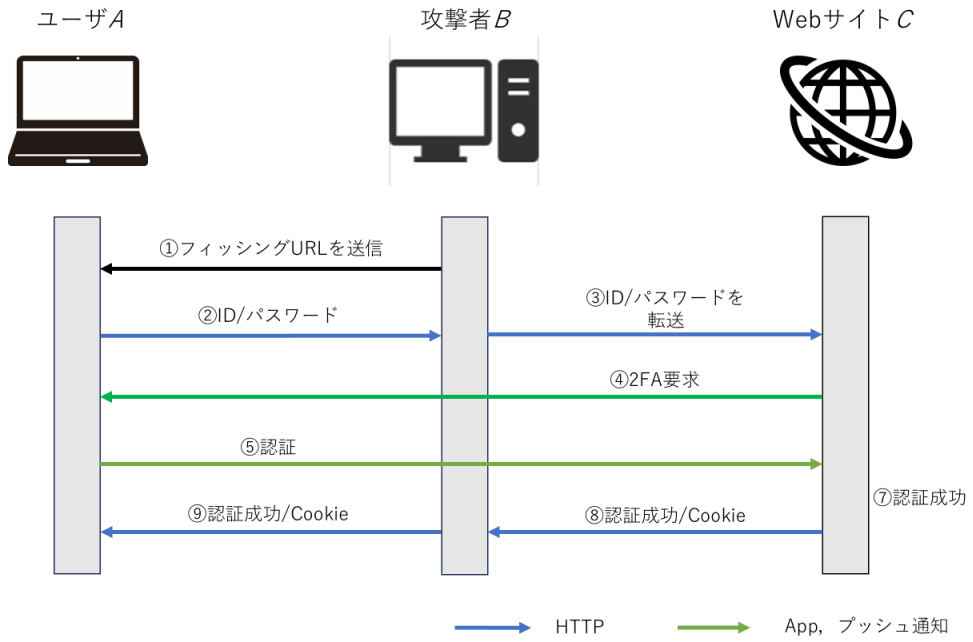


[3]



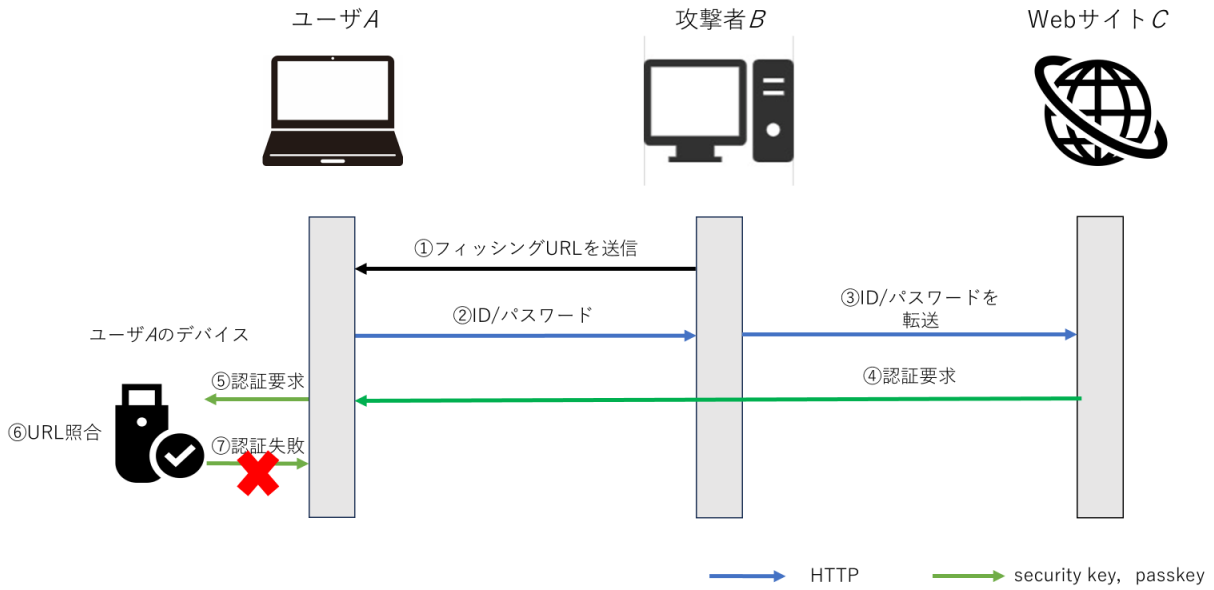
2-1　2FA方式と攻撃耐性

- App，プッシュ通知(脆弱)



→サーバが正常に認証されたと判断する

- 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

2-2　主要なWebサイトの2FAの調査

調査内容

- 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て調査

2．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)

サイト名	SMS	phone call	Email	TOTP(認証アプリ)	apps	プッシュ通知	security key	passkey	結果
Dropbox	○			○		○	○		安全
LINE					○				脆弱
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？
　→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？
　→**約85%**のサイトが脆弱