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

太田 和希 †

明治大学総合数理学部 先端メディアサイエンス学科 菊池研究室 †

1　はじめに

サイバーセキュリティの脅威の一つにフィッシング攻撃がある．2022 年に発生したデータ侵害の 36 %にフィッシングが関与している [1]．そこで，その対策として 2FA(二要素認証) が広く講じられている．しかし，Evilginx[2]，Muraena[3]，Modlishka[4] などのフィッシングツールキットの中には，中間者攻撃を行い，2FA をバイパスして不正アクセスをできるものがある．

そこで，本研究では，フィッシングツールキットの一つである Evilginx の動作確認を行い，2FA を破るかどうかを検証する．さらに，主要な Web サービスの二要素認証方式を調査して，本攻撃に対する影響を仕様から評価する．

2　準備

2.1　2FA

2FA とは，安全性を高めるために用いられる認証方式であり，認証の際に ID とパスワードだけでなく追加の認証要素を要求する認証方式である．認証要素には知識要素 (本人のみが知っていること)，所有要素 (本人のみが所有するもの)，身体要素 (本人の身体的特徴) がある．

2.2　AiTM 攻撃

Adversary-in-the-Middle(AiTM) 攻撃は中間者攻撃の一種であり．攻撃者はユーザと正規サイトの間でリバースプロキシとして働き，ログイン情報を取得する．

図 1 に AiTM 攻撃の概要を示す．1. 攻撃者 *B* からユーザ *A* に対して，フィッシング URL を含むメール等を送り，攻撃者が作り出したフィッシングサイト *B* に誘導する．2. 攻撃者は ID とパスワードを取得し，それらを正規サイト *C* に転送する．3. 正規サイト *C* はユーザ *A* に二要素認証の要求をして，メールや SNS などで 2FA コードを送る．4. 攻撃者 *B* はユーザ *A* から 2FA コードを取得し，正規サイト *C* に転送する．

これらにより，攻撃者は認証済みのセッションを取得し，サイトに不正にログインする．

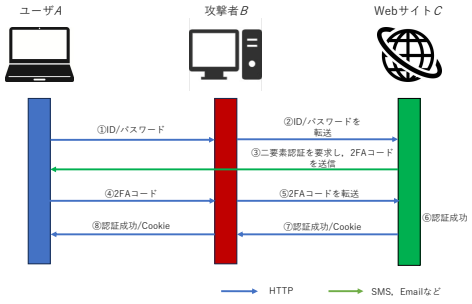

図 1　AiTM 攻撃の概要

```
: sessions 127

id           : 127
phishlet     : example
username     : ■■■■■■■■■■@■■■■■■
password     : ■■■■■■■■■
tokens       :
landing url  : https://academy.kikn.fms.meiji.ac.jp/JDxUeqmf
user-agent   : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0
Safari/537.36
remote ip    : 127.0.0.1
create time  : 2024-12-23 14:27
update time  : 2024-12-23 14:29
```

図 2　セッション

2.3　Evilginx

Evilginx とは，フィッシングツールキットの一つである．リバースプロキシとして働き，2FA をバイパスしてユーザと Web サイト間のセッションを不正に取得することができる．

Evilginx は Go 言語で書かれており，OS は Windows と Linux の両方で使用することができる．CLI でコマンドを打ち込み操作を行う．図 2 に取得したセッションの例を示す．

3　Evilginx の評価

3.1　基本動作

Evilginx は config，phishlets，lures を設定し攻撃を行う．config コマンドで，中間者として働くサーバのドメ

† Kikuchi Laboratory, Department of Frontier Media Science, School of Interdisciplinary Mathematical Science, Meiji University.

表 1　実験結果

		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

インと IPv4 を入力する．phishlets コマンドで，phishlet と呼ばれる特定のサイトをターゲットにするための設定ファイル (yaml) を読み込む．lures コマンドで，フィッシングサイトの URL を取得する．

また，Evilginx は TLS を欺くために Let's Encrypt から偽の公開鍵証明書を自動で取得する．

3.2　処理速度計測

正規サイトと Evilginx を用いたフィッシングサイトでページの読み込み時間，ログインにかかる時間の計測を行った．ローカル環境で行い，ターゲットとなる Web サイトには，Evilginx の学習サイトである Enilginx Mastery[5] を用いた．

3.2.1　実験目的

フィッシングサイトのほうが正規サイトよりも処理速度が遅いと仮定し，正規サイトとフィッシングサイトの処理時間の違いからフィッシングサイトのシステムの遅延を計測する．また，その遅延によって，一般ユーザが異変に気付くことができるか推測する．

3.2.2　実験方法

正規サイトとフィッシングサイトでページの読み込み時間を 50 回ずつ，ログイン時間を 30 回ずつ計測し，平均の時間を比較する．ページの読み込み時間は，ページ上のすべての要素が表示されるまでの時間として計測を行った．時間の計測には Selenium[6] を使用した．

3.2.3　結果

表 1 に実験結果を示す．読み込み時間では約 0.8 秒，ログイン時間では約 3.0 秒の差が発生した．証明書の読み込み時間，中間者を介した通信によって処理速度に差が生じたと考えられる．

一方で，計測した時間は本来使用するネットワークの状況で前後するものであるため，これらの差が生じても一般ユーザは攻撃の存在に気づくことができないと推測される．

表 2　各二要素認証方式の AiTM 耐性

二要素認証方式	AiTM 耐性	認証コード秘匿
SMS	×	×
phone call	×	×
Email	×	×
TOTP	×	×
App	×	○
push notification	×	○
USB key	○	○
passkey	○	○

4　Web サイトの脆弱性評価

4.1　仮定

二要素認証方式を 8 つの方式に分類し，AiTM 攻撃に対して脆弱であるかを仮定する．表 2 に各二要素認証方式とそれらの AiTM 攻撃への耐性を示す．

SMS，phone call，Email

SMS，phone call，Email を用いた二要素認証は脆弱であると考える．これらの認証方式は，4 桁や 6 桁のコードを取得し，打ち込む．従って，図 1 に示した AiTM 攻撃の概要のように攻撃を受けると推測される．

また，これらの方法は AiTM 攻撃以外の攻撃にも脆弱性がある．特に，SMS では SIM スワッピング攻撃 [7] や PRMitM 攻撃 [8] などを受けるリスクがある．

TOTP

認証アプリを用いた二要素認証は脆弱であると考える．この認証方式では，アプリが TOTP と呼ばれる 6 桁のコードを生成し，ユーザがそれを打ち込む．この方式は，SMS，phone call，Email などの認証方式のようにサーバ側が認証コードをインターネットにより送信することがないため，それらの認証方式よりかは安全だと言える．

しかし，ユーザが認証コードを送信する際は，特別に暗号化を施しておらず中間者によって傍受されてしまう．従って，AiTM 攻撃に対して脆弱であると推測される．

専用アプリ，プッシュ通知

専用アプリやプッシュ通知を用いた二要素認証は脆弱であると考える．これらの認証方式は Web サイトとユーザの持つアプリやデバイスの間で直接，認証要求と

認証を行う．そのため，認証コードを中間者に取得されることはない．

しかし，ユーザが認証をすることで Web サイトは正常に認証が成功したと判断し，セッションを中間者に送信してしまう．従って，AiTM 攻撃に対して脆弱であると推測される．

セキュリティキー，パスキー

セキュリティキーによる認証方式は Evilginx に対して安全であると考える．セキュリティキーは，USB や NFC などのハードウェアを用いて認証する方式である (例：YubiKey[9])．パスキーは，PC やスマートフォンで顔や指紋などを用いて認証する方式である (例：Windows Hello[10])．これらの認証方式は，デバイスが認証サーバの正しい URL を保存しているため，中間者の偽の URL を区別することが可能である．そのため，これらの認証方式は，Evilginx に対して安全であると推測される．

4.2 Web サイトの二要素認証方式の調査

4.2.1 調査目的

国内，国外のサイトを含む 102 のサイトを調査対象とした．二要素認証を導入しているか，どのような二要素認証方式をとっているのかを明らかにする．

4.2.2 調査方法

サイトの公式ドキュメントが公開されていれば参照して，対応している二要素認証の種類を調べた．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をした．二要素認証の対応状況やカテゴリの分類に 2FA Directory[11] というサイトを利用した．

4.2.3 選定基準

国内のサイトを 48 サイト，国外のサイトを 54 サイト調査した．対象サイトは様々なカテゴリから網羅的に選択した．また，国外のサイトは，日本でも知名度が高いサイトを優先して選択した．

4.2.4 結果

二要素認証の導入率

表 3 にそれぞれの二要素認証導入率を示す．ソーシャルログインとは，他のサービスの ID を用いてログインすることである．そのサービスが二要素認証を導入している場合，同じように二要素認証を利用することができる．

表 3　二要素認証導入率

ソーシャルログイン	国内 [%](件)	国外 [%](件)	全体 [%](件)
含まない	54.17 (26)	77.78 (37)	66.67 (68)
含む	77.08 (42)	88.89 (48)	83.33 (85)
計	(48)	(54)	(102)

全体では，102 サイトのうち 68 サイト (67 %) が，ソーシャルログインを含めると 102 サイトのうち 85 サイト (83 %) が二要素認証を導入していた．また，ソーシャルログインを含めるかにかかわらず，国内サイトより国外サイトのほうが二要素認証の導入率が高い．

表 3 から，ソーシャルログインを含めると 8 割を超えるサイトが二要素認証を導入している．これは，フィッシング攻撃が依然として増え続けている [12] からであると推測される．既存のフィッシング攻撃への対策として，2FA を用いた認証方式は有効である．そのため，ほとんどのサイトが二要素認証を導入していると考えられる．

一方，国内と国外サイトの普及率は，ソーシャルログインを含まない場合で約 23 %，含む場合で約 11 %国外サイトが上回っている．

この差は単に国内と国外の差ではなく，本調査でのサイトの選定基準に起因するものであると考える．国外サイトの選定基準として，日本でも知名度が高いサイトを優先して選定した．そのため，国外サイトは国内サイトよりユーザ数が多いサービスや大企業が運営するサービスが多いと考えられる．つまり，本調査からは国内と国外のセキュリティ意識に違いがあるとは言えず，むしろ運営する企業の規模によって差が生じるのではないかと推測される．

二要素認証方式

調査したサイトで用いられていた二要素認証方式を 8 つの種類に分類し集計を行った．図 3 に二要素認証方式別の件数を示す．二要素認証を導入しているサイトには複数の認証方式を利用しているサイトが多いため，それぞれの認証方式の合計数は 102 を超える．複数の認証方式をサポートしているサイトはあるが，複数を必須に，すなわち，単一の認証を禁じているサイトは存在しなかった．

最多は TOTP(Time-based One-Time Password) を用いた認証アプリで 51 サイト，二番目は SMS で 38 サイトとなった．

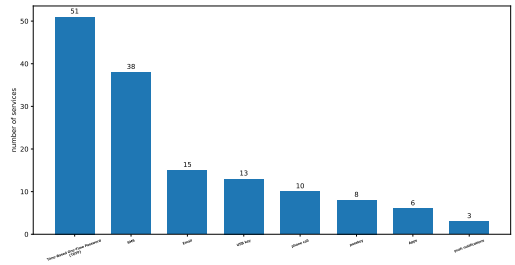

図 3　二要素認証方式

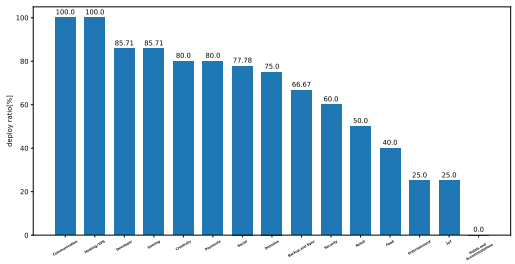

図 4　カテゴリごとの二要素認証導入率

カテゴリごとの二要素認証導入率

対象 102 サイトを 2FA Directory[11] に従い 38 カテゴリに分類した．その中から 1 カテゴリに 4 サイト以上あるカテゴリを抽出し，15 カテゴリで比較を行った．

図 4 にカテゴリごとの二要素認証導入率，表 4，5 に調査結果の一部を示す．Communication カテゴリと Hosting/VPS(例：さくらインターネット [13]) カテゴリはともに二要素認証の導入率が 100 %であった．また，Hotels & Accomodation(例：NH Hotels[14]) カテゴリは二要素認証の導入率が 0 %であった．

4.3　考察

調査した結果，4.1 節で脆弱でないと仮定した方式であるセキュリティキー，パスキーを導入していないサイトは 102 サイトのうち 87 サイト (85 %) であった．つまり，調査を行った 85 %のサイトは AiTM 攻撃に対して脆弱であると推測される．

5　おわりに

本稿では，正規サイトと Evilginx を用いたフィッシングサイトの読み込み時間とログイン時間の計測を行った．その結果, 読み込み時間では約 0.8 秒, ログイン時間では約 3.0 秒の差が発生した．そのことから，一般ユーザは攻撃の存在に気づくことができないと推測された．

また，主要な Web サイトの AiTM 攻撃に対する脆弱性を検討した．調査の結果，85 %の Web サイトが脆弱であることがわかった．

参考文献

[1] Dataprot，“Phishing Statistics”（https://dataprot.net/statistics/phishing-statistics/，2024 年 11 月参照）

[2] Kuba Gretzky，“Evilginx”（https://github.com/kgretzky/evilginx2，2024 年 11 月参照）

[3] Muraena，“Muraena”（https://github.com/muraenateam/muraena，2024 年 11 月参照）

[4] Modlishka，“Modlishka”（https://github.com/drk1wi/Modlishka.，2024 年 11 月参照）

[5] BREAKDEV Academy，“Evilginx Mastery”（https://academy.breakdev.org/evilginx-mastery，2024 年 11 月参照)

[6] Selenim，“Selenium”（https://www.selenium.dev/，2024 年 12 月参照)

[7] Collin Mulliner，Ravishankar Borgaonkar，Patrick Stewin，and Jean-Pierre Seifert，“ SMS-based one-time passwords: Attacks and defense”, Proceedings of the 10th international conference on Detection of Intrusions and Malware, and Vulnerability Assessment，DIMVA，pp.150-159，2013.

[8] Nethanel Gelernter，Senia Kalma，Bar Magnezi，Hen Porcilan，“The Password Reset MitM Attack”，IEEE Security and Privacy，pp.251-267，2017.

[9] Yubico，“YubiKey”（https://www.yubico.com/yubikey/，2024 年 12 月参照)

[10] Microsoft，“Windows Hello”（https://www.microsoft.com/en-us/windows/tips/windows-hello/，2024 年 12 月参照)

[11] 2FA Directory，“2FA Directory”（https://2fa.directory/，2024 年 11 月参照)

[12] フィッシング対策協議会，“月次報告書”（https://www.antiphishing.jp/report/monthly/，2024 年 11 月参照)

[13] さくらインターネット，“さくらインターネット”

表 4　調査結果 (1/2)

カテゴリ	サイト名	国	多要素認証	ソーシャルログイン	SMS	phone call	Email	認証アプリ	専用アプリ	セキュリティキー	パスキー	プッシュ通知
Backup and Sync	Dropbox	アメリカ	○		○			○		○		○
	icloud(AppleID)	アメリカ	○		○	○				○		○
	Files.com	アメリカ	○		○		○	○		○		
	Evernote	アメリカ	○	○				○				
	firestroage	日本		○								
	infinicloud	日本										
Communication	Discord	アメリカ	○		○			○			○	
	slack	アメリカ	○		○			○				
	zoom	アメリカ	○		○			○				
	miro	アメリカ	○					○				
	LINE	日本	○						○			
	Chatwork	日本	○		○			○				
Creativity	Canva	オーストラリア	○					○				
	Adobe	アメリカ	○	○	○		○		○			
	pixiv	日本	○	○				○				
	小説家になろう	日本										
	studio	日本	○	○				○				
Developer	unity	アメリカ	○		○			○				
	readme	アメリカ	○					○				
	openAI	アメリカ	○	○				○				
	Github	アメリカ	○		○			○	○	○	○	
	Monaca	日本		○								
	Qiita	日本	○					○				
	zenn	日本	○	○								
Domains	Crazy Domains	オーストラリア	○	○	○	○						
	101domains	アメリカ	○					○				
	namecheap	アメリカ	○					○		○		
	ライブドアブログ	日本										
Entertainment	Netflix	アメリカ										
	DAZN	イギリス										
	Twitch	アメリカ	○		○			○				
	Spotify	スウェーデン		○								
	DMM	日本	○	○				○				
	コミックシーモア	日本		○								
	SHOWROOM	日本		○								
	ブックライブ	日本		○								
Food	wolt	フィンランド		○								
	UberEats	アメリカ	○	○	○			○				
	Starbucks	アメリカ			○							
	食べログ	日本	○	○								
	cookpad	日本		○								
Gaming	VRChat	アメリカ	○					○				
	Nvidia	アメリカ	○	○						○	○	
	Electronic Arts	アメリカ	○	○	○	○	○	○				
	Nintendo	日本	○	○				○				
	KONAMI	日本	○				○					
	CAPCOM	日本	○					○				
	gamewith	日本		○								
Hosting/VPS	KnownHost	アメリカ	○					○				
	PlanetHoster	カナダ	○					○				
	さくらインターネット	日本	○		○	○	○	○				
	ConoHa	日本	○					○				
Hotels and Accommodations	NH Hotels	スペイン										
	トリバゴ	ドイツ		○								
	Hotels.com	アメリカ		○								
	一休	日本		○	○							
	エアトリ	日本										
	HIS	日本										

（https://www.sakura.ad.jp/，2024 年 12 月参照)

[14] NH Hotel, “NH Hotels & Resorts”（https://www.nh-hotels.com/，2024 年 12 月参照)

表 5　調査結果 (2/2)

カテゴリ	サイト名	国	多要素認証	ソーシャルログイン	SMS	phone call	Email	認証アプリ	専用アプリ	セキュリティキー	パスキー	プッシュ通知
IoT	Xiaomi	中国		○								
	IFTTT	アメリカ	○	○				○				
	Nature	日本		○								
	TOLIGO	日本										
Payments	paypal	アメリカ	○					○				
	Stripe	アメリカ	○		○			○		○	○	
	paypay　アプリ	日本	○		○							
	Vpass	日本										
	MIXI M	日本	○	○	○		○				○	
Retail	Amazon	アメリカ	○		○	○		○				
	ZARA	スペイン										
	楽天市場	日本										
	zozotown	日本		○								
	minne	日本	○	○	○	○						
	Yahoo! JAPAN	日本	○		○		○					
Security	Norton	アメリカ	○		○	○		○		○		
	DNSFilter	アメリカ	○					○				
	Malwarebytes	アメリカ		○								
	Trend Micro	日本	○		○		○	○				
	ソースネクスト	日本										
Social	X	アメリカ	○	○	○ (有料)			○		○	○	
	instagram	アメリカ	○	○				○				
	facebook	アメリカ	○		○			○		○		
	TikTok	中国	○	○	○		○	○				
	LinkedIn	アメリカ	○	○	○			○				
	Reddit	アメリカ	○	○				○				
	yay	日本	○	○				○				
	Wantedly	日本		○								
	mixi	日本										
Cloud Computing	DigitalOcean	アメリカ	○		○			○				
	Heroku	アメリカ	○					○	○	○		
Education	udemy	アメリカ	○				○					
Task Management	Nifty	アメリカ	○					○				
Universities	Oh-o! Meiji	日本	○		○	○		○				
VPN Providers	Cyberghost	ルーマニア										
other	Google	アメリカ	○		○	○		○		○	○	○
	Microsoft	アメリカ	○		○	○	○	○		○	○	
	リクルート	日本	○		○		○	○				
	マイナビ	日本	○		○		○					
	one career	日本										
	GMO	日本	○	○			○	○				
	Mercari	日本	○		○							
	au(au ID)	日本	○		○		○		○			
	docomo(d アカウント)	日本	○		○				○			