

PRESS RELEASE

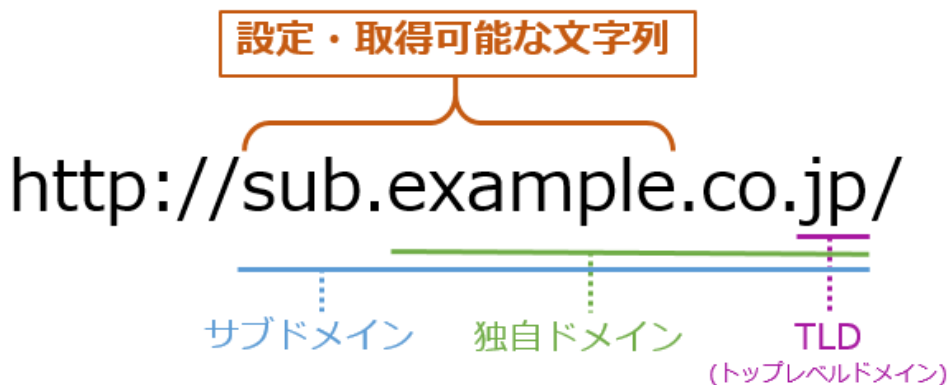
**【セキュリティレポート】2023年上半期フィッシングサイトのドメインを独自に分析
広く利用可能なドメイン「dev」が今期急増 フィッシングサイトでの悪用目立つ
～フィッシング詐欺とみられる不正送金被害件数は国内過去最多～**

情報セキュリティメーカーのデジタルアーツ株式会社(本社:東京都千代田区、代表取締役社長:道具 登志夫、以下 デジタルアーツ、証券コード 2326)は、2023年上半期に収集した国内外のフィッシングサイト URL のドメインを集計したレポートを公開しました。

警察庁が発表した最新の報告書によると、フィッシングによるものとみられるインターネットバンキングに係る不正送金被害件数は、2023年上半期において2,322件と国内過去最多となりました。さらに、被害総額は30億円※1を超えるなど、今期は特にフィッシング関連の注意が必要となっています。

■URL総数は1/3に減少 TLDは「com」が最多、昨年下半年17位の「dev」は2位に急浮上

デジタルアーツでは、日々さまざまなWebサイトについて調査・収集を行っています。今回、デジタルアーツは、2023年上半期(1～6月)に確認した国内外のフィッシングサイト URL のドメインを集計しました(IPアドレス形式のURLは除く)。なお、本レポートで扱うドメインについては、【図1】のように定義しています。



デジタルアーツの2023年の上半期におけるフィッシングサイトドメイン調査では、フィッシングサイトのURL総数が2022年下半年と比較して約1/3に減少したことがわかりました。主な要因としては、昨年下半年に急増した「サブドメインに長い文字列を用いた特徴的なパターンを持つクラスター」が減少したことによります。

また、2023年上半期のフィッシングサイトのTLDトップ20を集計したところ、「com」が1位の39.52%と最多になりました。続いて、2位が「dev」の6.85%、3位が「cn」の6.08%という結果になりました。特に2位の「dev」は、昨年下半年は17位の0.51%だったため、今期大幅に増加したことがわかります。

昨年下半年に40.95%と最多であった「top」は、今期では4.69%となり、全体シェアが約1/10に減少しています。

※1 参考 警察庁「フィッシングによるものとみられるインターネットバンキングに係る不正送金被害の急増について」

https://www.npa.go.jp/bureau/cyber/pdf/20230808_press.pdf

2023年上半期 フィッシングサイトTLDトップ20 ※右表は昨年下半年期

順位 ▲	TLD	シェア	順位 ▲	TLD	シェア
1	com	39.52%	1	top	40.95%
2	dev	6.85%	2	com	16.95%
3	cn	6.08%	3	icu	10.69%
4	top	4.69%	4	cn	4.17%
5	app	4.27%	5	co	3.92%
6	co	2.87%	6	shop	3.52%
7	io	2.49%	7	xyz	1.67%
8	org	2.41%	8	app	1.52%
9	ru	2.22%	9	net	0.98%
10	net	2.00%	10	group	0.82%
11	cfid	1.79%	11	org	0.74%
12	xyz	1.55%	12	tk	0.74%
13	shop	1.16%	13	io	0.62%
14	site	1.14%	14	live	0.60%
15	me	0.96%	15	ml	0.59%
16	id	0.95%	16	ru	0.56%
17	pl	0.84%	17	dev	0.51%
18	info	0.76%	18	tt	0.49%
19	au	0.66%	19	site	0.46%
20	link	0.66%	20	info	0.45%

■誰でも利用可能な独自ドメイン「workers.dev」が今期最多 URLは9割が同パターン

2023年上半期における独自ドメイントップ20の1位は全体の5.75%を占める「workers.dev」であり、TLDトップ20における「dev」のシェア増加を牽引していることが読み取れます。

「workers.dev」は、Cloudflare社(Cloudflare, Inc.)が提供するCloudflare Workersというサービスで、広く利用可能なドメインです。実際に、無料プランにおいては、リクエスト回数やメモリに制限があるものの、毎日10万リクエストまで無料で利用でき、高速かつ安価という特徴を持っていることから、フィッシングサイトで悪用されたと考えられます。これが今期「workers.dev」が増加した要因だと予想しています。

また、プロジェクトごとに以下の形式でURLを発行し、サードレベルドメインを自由に設定することが可能です。

```
https://[プロジェクト名].[ユーザー設定の文字列].workers.dev/
```

中でも以下のURLパターンが多く見受けられ、「workers.dev」を利用したフィッシングサイトURLの9割は当パターンであったことが分かっています。さらに、「workers.dev」に絞った頻出単語の上位はURLパターンの[固有の単語]が占めていました。実際に模倣されたブランドには、日本の大手携帯キャリア会社や有名クレジットカード会社なども確

認できました。

```
https://[固有の単語]- [固有の単語]- [4桁の英数字].[ユーザー設定の文字列].workers.dev/
```

フィッシング攻撃は、引き続き組織や個人にとって深刻な脅威となっています。攻撃者は、URL 生成パターンを変更するなど新たな手法を模索し、防御策を回避しようとしています。

そのため、新たな攻撃手法を含めた情報収集と引き続きのセキュリティ対策が重要です。

●フィッシングサイトの URL をブロックするデジタルーツの「i-FILTER」

デジタルーツでは日々さまざまな情報をもとにデータの収集を行っています。「i-FILTER」Ver.10 では、フィッシングサイト URL はフィルターデータベースへと迅速に配信され、[フィッシング詐欺]や[迷惑メールリンク]や[違法ソフト・反社会行為]カテゴリにてブロック可能です。またフィルターデータベースに反映されていない URL についても「ホワイト運用」を行うことで、デジタルーツが安全を確認した URL にのみアクセスを許可し未知のフィッシングサイトや悪性 URL をブロックすることができます。さらに「クレデンシャルプロテクション」機能では、正規のサイトと判別が困難な改ざんサイトに設置されたフィッシングサイトであっても、ユーザーが ID・パスワードを送信しようとした際にこれをブロックすることが可能です。

<https://www.daj.jp/bs/i-filter/>

●メール本文中に含まれる URL の偽装判定が可能な「m-FILTER」

「m-FILTER」は、送信元や添付ファイルの拡張子、メール本文中に含まれる URL の偽装判定などが行えるメールセキュリティ製品です。「脅威 URL ブロック」オプション※は、「i-FILTER」利用ユーザー以外でも、メールの本文と添付ファイル内の URL をデジタルーツが運用しているクラウド上のデータベースに問い合わせます。もしも危険な URL が記載されている場合は、メールをブロックします。

※2022 年 12 月 9 日より、本オプションの名称を「URL カテゴリ判定」から「脅威 URL ブロック」に変更しております。

※本オプションは「i-FILTER」をお持ちでないユーザー様に向けた機能となります。

<https://www.daj.jp/bs/mf/>

●2023 年上半期フィッシングサイト ドメイン集計のレポートはこちら

以下、弊社コーポレートサイト上にて公開しております。

https://www.daj.jp/security_reports/33/

デジタルアーツ株式会社 概要

Web、メール、ファイルなどのセキュリティソフトウェアの提供を核に事業展開する情報セキュリティメーカーです。
1995年の創業以来、「より便利な、より快適な、より安全なインターネットライフに貢献していく」を企業理念とし、有害情報の閲覧を制限するWebフィルタリングソフトを開発、以来企業・公共・家庭向けに情報セキュリティ製品を提供しております。

東京都千代田区大手町 1-5-1 大手町ファーストスクエア ウエストタワー14F ▶URL: <https://www.daj.jp/>

<本リリースに関するお問い合わせ>

デジタルアーツ株式会社 広報課 関 TEL : 080-8163-0311/ E-mail : press@daj.co.jp

- ※ デジタルアーツ、DIGITAL ARTS、i-FILTER、i-FILTER Anti-Virus & Sandbox、i-FILTER@Cloud Anti-Virus & Sandbox、i-FILTER@Cloud D アラート発信レポートサービス、info board、Active Rating System、D-SPA、Anti-Virus & Sandbox for D-SPA、NET FILTER、SP-Cache、White Web、ZBRAIN、クレデンシャルプロテクション、ホワイト運用、m-FILTER、m-FILTER MailFilter、m-FILTER Archive、m-FILTER Anti-Spam、m-FILTER Anti-Virus & Sandbox、m-FILTER@Cloud Anti-Virus & Sandbox、m-FILTER@Cloud D アラート発信レポートサービス、m-FILTER File Scan、Mail Detox、m-FILTER EdgeMTA、EdgeMTA、FinalCode、i-フィルター、DigitalArts@Cloud、Desk、Desk Event、StartIn、f-FILTER、D アラートおよび D コンテンツその他の弊社・弊社製品関連の各種名称・ロゴ・アイコン・デザイン等はデジタルアーツ株式会社の登録商標または商標です。
- ※ その他、上に記載された会社名および製品名は、各社の商標または登録商標です。