フィッシングサイトに悪用される

ドメイン名の過去と現在

株式会社マクニカ
ネットワークス カンパニー
鈴木　一実
丸山　一郎
掛谷　勇治

富士通ディフェンス & ナショナルセキュリティ株式会社
ミネルバサイエンス研究所
谷口　剛

Table of Contents

01 サマリー

フィッシングサイトへ利用者を誘導する手段としてフィッシングメールや SMS に URL を記述するが、利用者に怪しまれないよう、URL 表記には大手ブランド名やブランドを模倣した文字列を組み合わせる等の工夫が行われてきた。しかし、最近、その手口は大きく変化している。

今回、JPCERT/CC が保有・提供するフィッシング URL について 5 年分を分析した結果、最新の攻撃手法はこうした従来の考えを覆すものであった。

- ブランド名を模倣した URL は時代遅れに。ブランド名を含まないフィッシング URL が主流。
- フィッシング URL ではドメインを悪用せず、サブドメインを悪用する手法が主流。
- DDNS や短縮 URL など、正規サービスを悪用する手法が急増。

すなわち、従来の判定方法ではフィッシングサイトの検出が困難になりつつあることを意味する。

- ブランド名などキーワードを使った比較判定が通用しない。
- ドメイン悪性評価が通用しない（FQDN 判定が必要）。
- 正規ドメインを許可リストに含めてしまうとフィッシングが紛れ込む。

フィッシング被害を減らすには、最新かつ主流の手法に対して対策する必要がある。コミュニティが蓄積した成果を読み解くことで対策に反映すべき知見を獲得できた。

02 調査手法・調査データ

この節では、本レポートの分析対象である phishurl-list について説明し、年別 URL 数、URL 分類、標的ブランド、悪用された TLD (Top-Level Domain)、そして悪用された正規サービスといった基本的な分析を順番に説明していく。

2.1 phishurl -list

本レポートでは、JPCERT/CC が公開している phishurl-list[1] を使用し、2019 年 1 月～ 2023 年 12 月の 5 年間について、日本で観測されるフィッシングサイトに用いられるドメインの動向を分析した。

phishurl-list は観測や報告で集まったフィッシング情報のうち、フィッシングコンテンツが確認されたフィッシングサイトの URL を収集したものである。図 1 のように、GitHub を介し csv 形式で提供され、観測したフィッシング URL 1 件毎に date、URL、description (被害ブランド) のデータ構造を持つ。

- ドメイン評価では、URL フィールドから FQDN を取り出して分析している。
- ブランド評価では、description フィールドをそのまま使用している。

1. https://github.com/JPCERTCC/phishurl-list

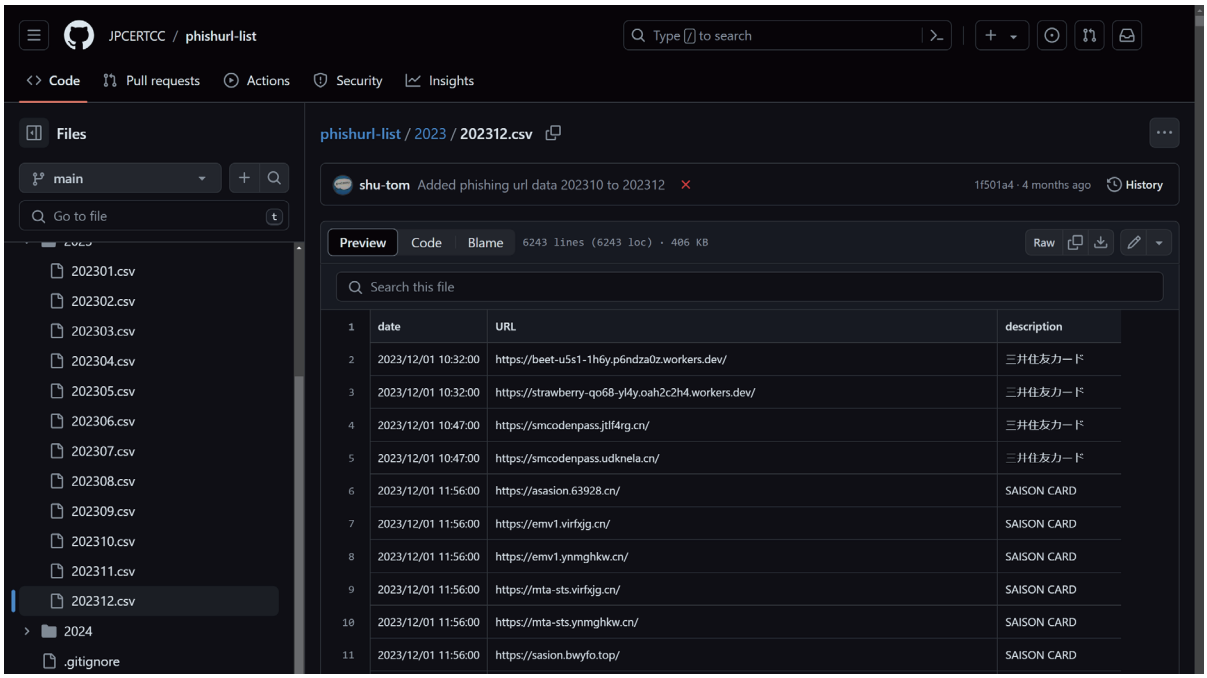


図1 phishurl-list 202312.csv

2.2 ドメインについて

本レポートの中で使用するドメインに関する単語の関係性を図 2 に示す。

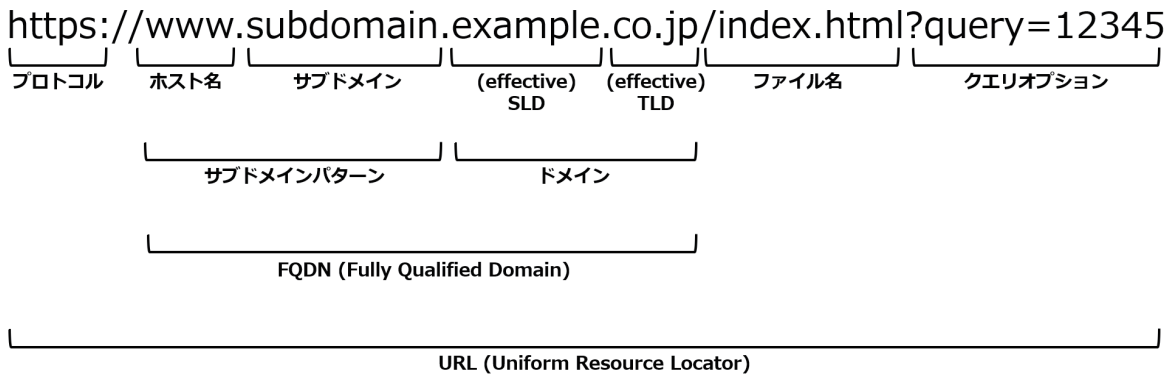


図2 URL,FQDN, ドメイン, サブドメインの関係性

本レポートでは、関連の多くの論文と同様に effective SLD (Second-Level Domain) でドメインを扱うこととする。すなわち、図 2 の場合、「co.jp」を effective TLD,「example」を effective SLD と扱い、ブランド模倣などを評価する。

また、本レポートでは、「ホスト名」+「サブドメイン」の文字列を明示的に表すために、「サブドメインパターン」という言葉を用いる（この言葉は本レポート内での用語である）。すなわち、図 2 の場合、「www.subdomain」がサブドメインパターンである。

03 フィッシングサイト URL の全体傾向

3.1 年別 URL 数、URL 分類

phishurl-list に掲載されている URL には、大きく分類して 3 種類の形式が存在する。

例 **ドメイン型**
`https://example.com/`
ドメインのみ

例 **サブドメイン型**
`https://malicious.example.com/`
サブドメインパターン + ドメイン

例 **IP アドレス型**
`https://192.0.2.1/`
IP アドレス

これらについて、2019 年 ~2023 年の期間での使用状況を調査した。
図 3 に、形式別の URL 数並びに、フィッシング URL 総数に対するサブドメイン型比率を示す。

URL 数全体については、2022 年までは毎年倍増しており、2019 年からの 3 年では 10 倍に激増していた。（2023 年は若干落ち着きを見せている）

一方、形式毎に比較した場合、サブドメイン型の増加が顕著であり、2019 年にドメイン型とほぼ同数であったものが、2020 年から増加し続け、2021 年に 79%、2022 年には 85% 超となり、全体の大半を占める状況となっている。2023 年は 2022 年と比較して比率は減少したものの、依然として約 7 割 がサブドメイン型となっている。

尚、IP アドレス型の URL は少なく、全体の 1 % 程度であった。

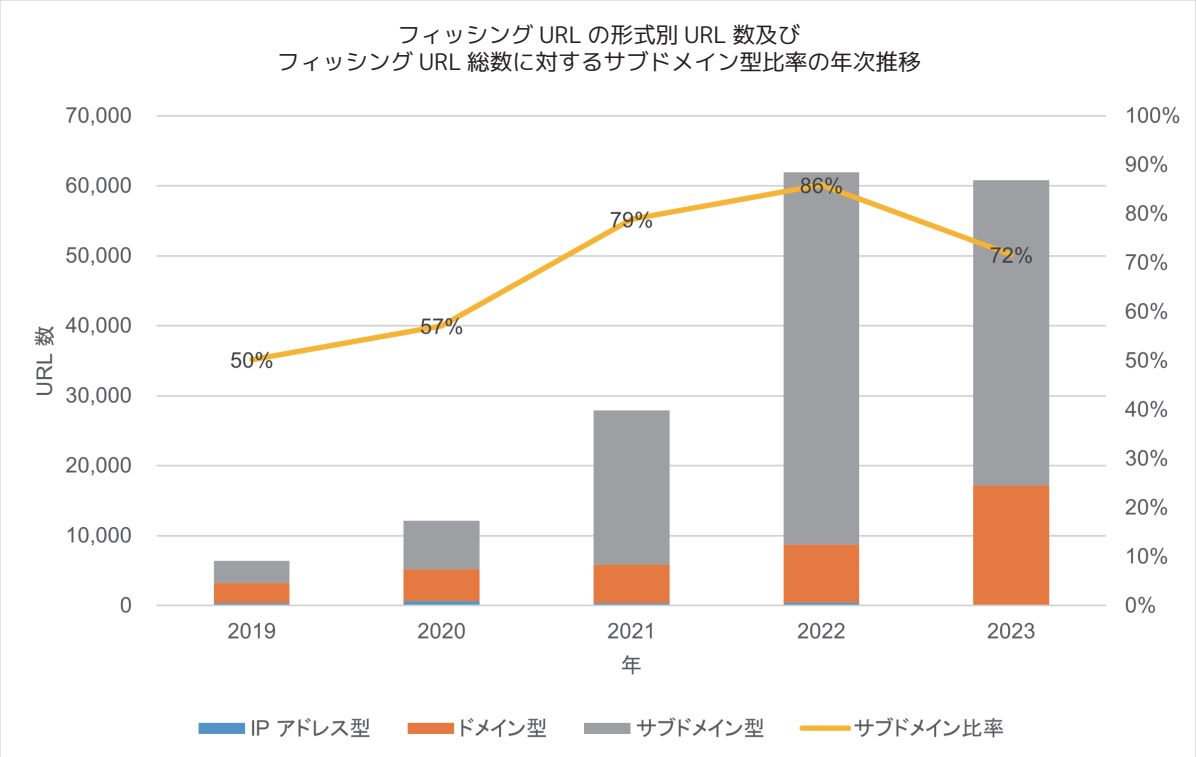


図3 phishurl-listの形式別URL数及び全体におけるサブドメイン型比率

3.2 被害ブランド分析

被害ブランドについては、上位 20 ブランドが全体の 80% を占めていることが分かった。そこで分析の観点からそれら 20 ブランドに対象を絞って調査を行った。

表1 評価対象とした上位20ブランド

ブランド名	URL 数
Amazon	25,204
三井住友カード	14,115
au	12,615
SAISON CARD	9,276
えきねっと	9,091
Apple ID	8,746
三菱 UFJ ニコス	6,926
楽天	6,753
メルカリ	6,561
ETC 利用照会サービス	6,409

ブランド名	URL 数
エポスカード	5,607
イオンカード	5,288
イオン銀行	3,839
SoftBank	3,538
ヤマト運輸	2,651
JCB	2,369
総務省	2,318
国税庁	2,301
MICARD	1,930
NTT docomo	1,913

各ブランドの被害状況について、関連するフィッシング URL の発生状況を年別に調査した。
グラフが輻輳して識別が難しいため、図 4 から図 6 の 3 つに分けて説明する。

図 4 でハイライトした Amazon、三井住友カード、Apple といった有名ブランドは、ここ 4 ～ 5 年間継続的に攻撃の標的となっていることが明確となった。また、2021 年から ETC 利用照会サービス、2022 年からはえきねっとが新たに継続的に狙われる標的となっていることも分かる。

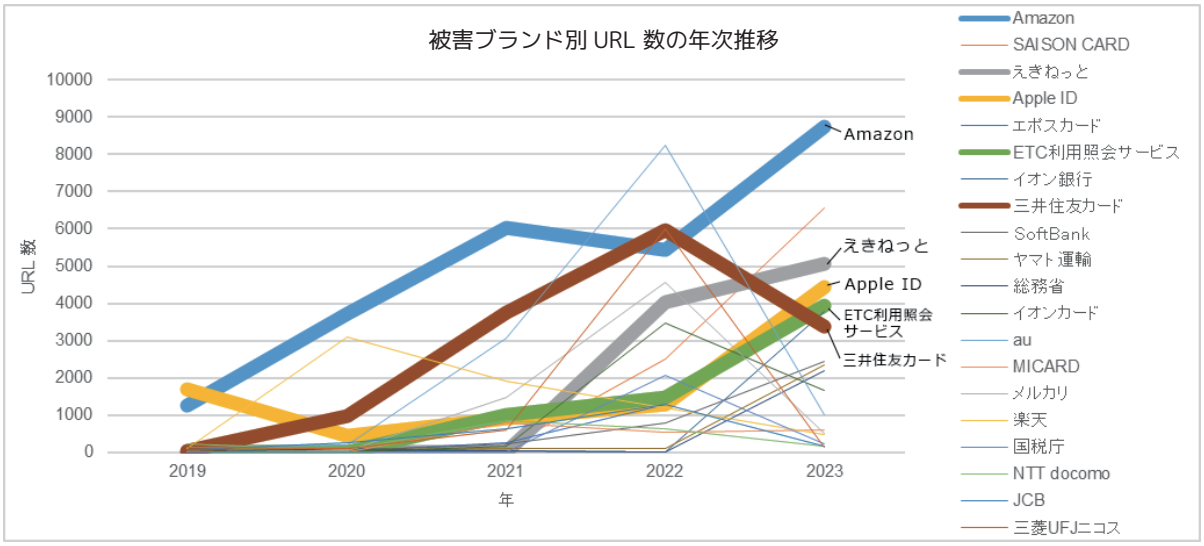


図4 被害ブランド別URL数（継続的に標的とされているブランドの強調）

図 5 でハイライトした SAISON CARD、エポスカード、イオン銀行、SoftBank、ヤマト運輸、総務省 (マイナポイント) といったブランドは、近年急増傾向となっている。一方で、図 6 のように、2022 年に急増し多くの被害を出した au、三菱 UFJ ニコス、メルカリについては 2023 年には急速に減少している。理由は不明であるが掘り下げて調査する必要がある。

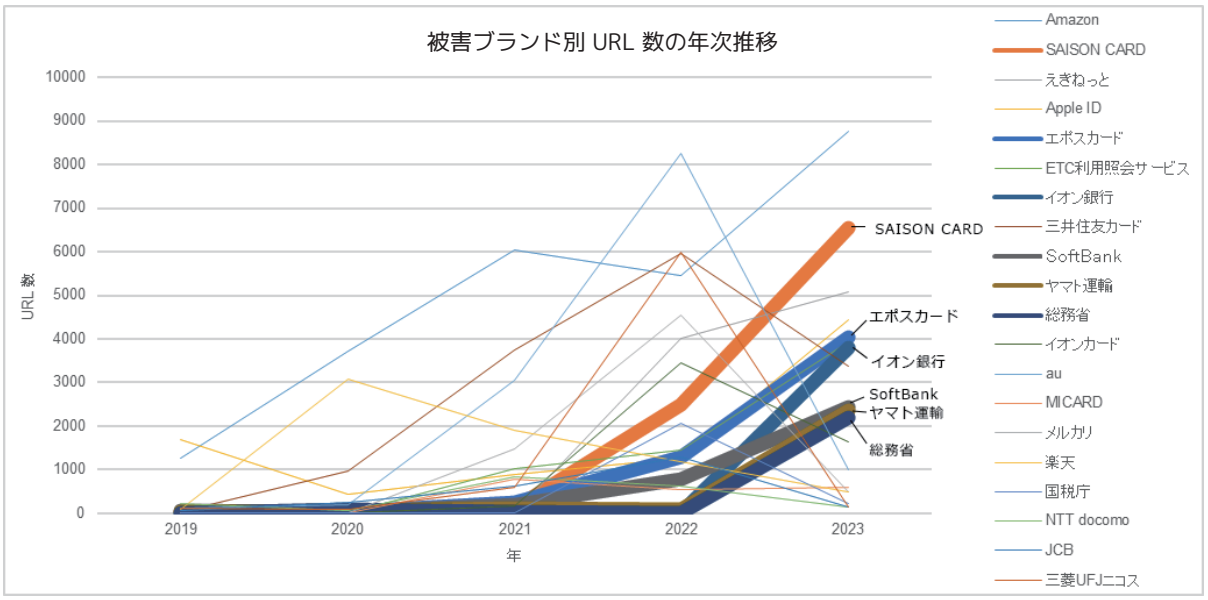


図5 被害ブランド別URL数(2023年増加傾向にあるブランドを強調)

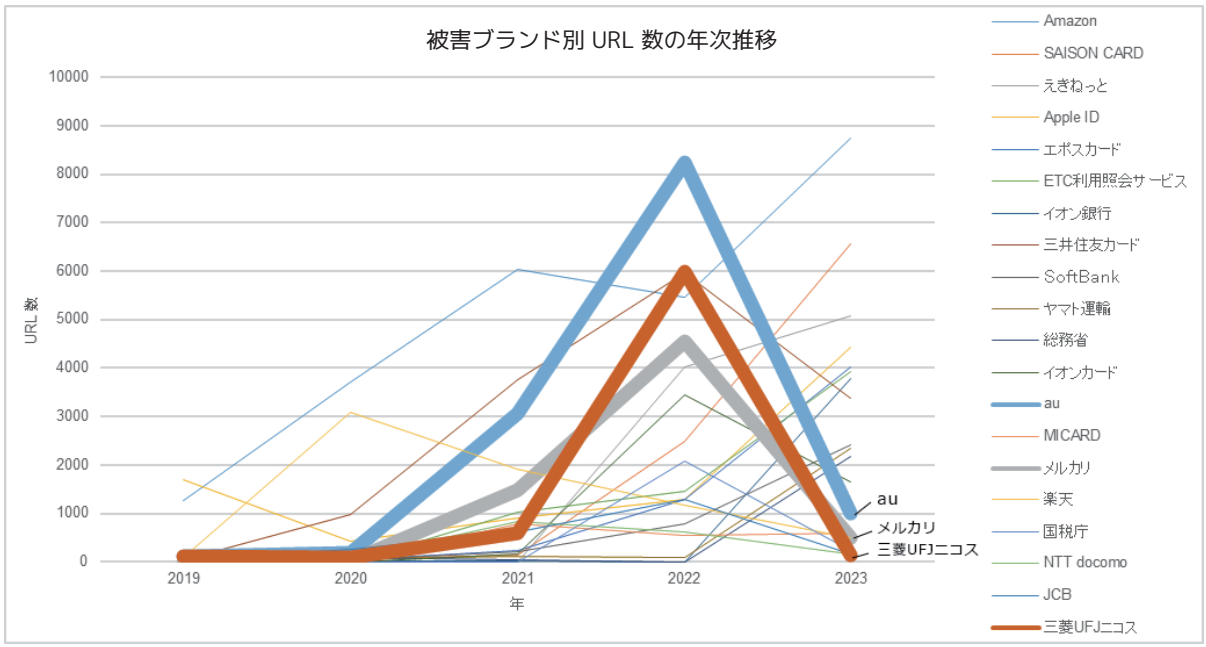


図6 被害ブランド別URL数 (2023年減少傾向にあるブランドを強調)

次に、図 7 に、2023 年の一年間における URL 数の変化を月単位でプロットしたものを示す。

SAISON CARD、エポスカード、イオン銀行といったブランドは 5 月から 8 月に 1 カ月で 2,000 を超える URL で集中的に狙われていたことが分かる。総務省はマイナポイント第二弾が 9 月末に締切られた以降に迷惑メールばらまきが始まり URL 数が急増している。

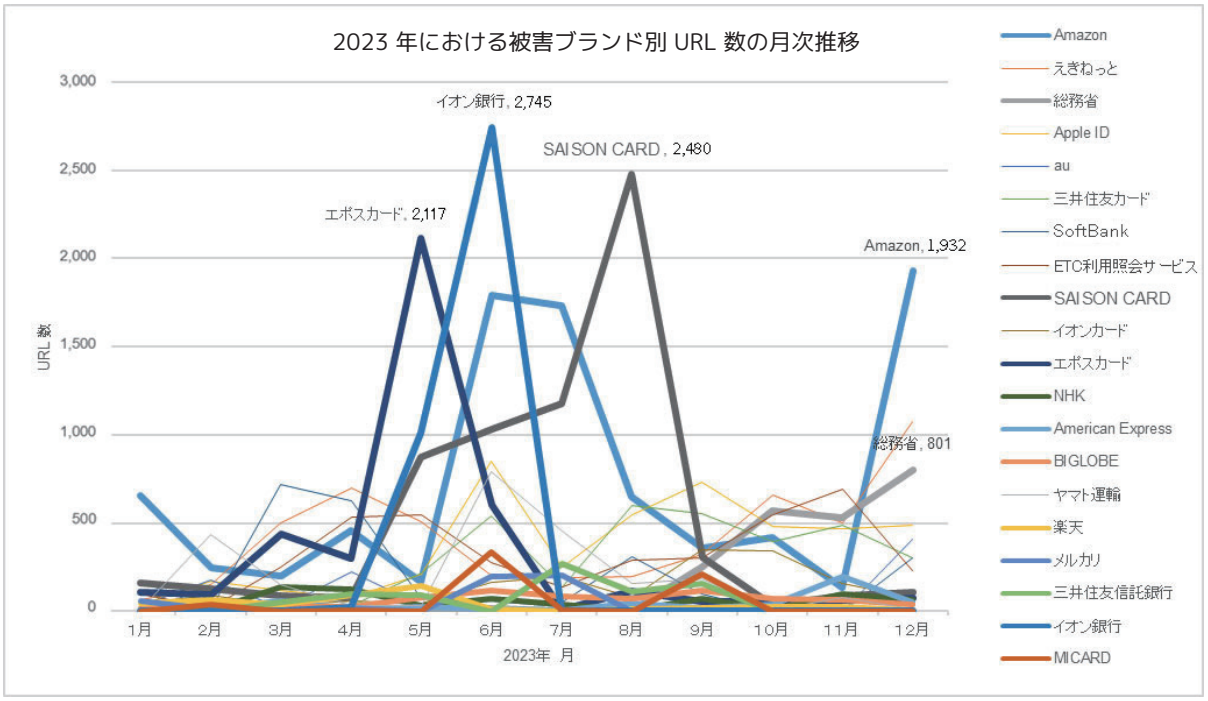


図7 2023年における被害ブランド別URL数

3.3 悪用された TLD

フィッシングに悪用される TLD にも流行がある。 phishurl-list に登場した TLD 数の変化を折れ線グラフで図 8 に示す。

全区間において .com の使用が多いが、2021 年からは .cn (中国) が急増しており、2021 年と 2022 年は .com 上回る状況となっていた。3 番目に多い .org は duckns.org (Dynamic DNS) を使用したフィッシングサイトの増加に伴い多くなっている。同じように 2023 年は workers.dev の不正使用急増に伴い .dev の件数が目立つようになった。

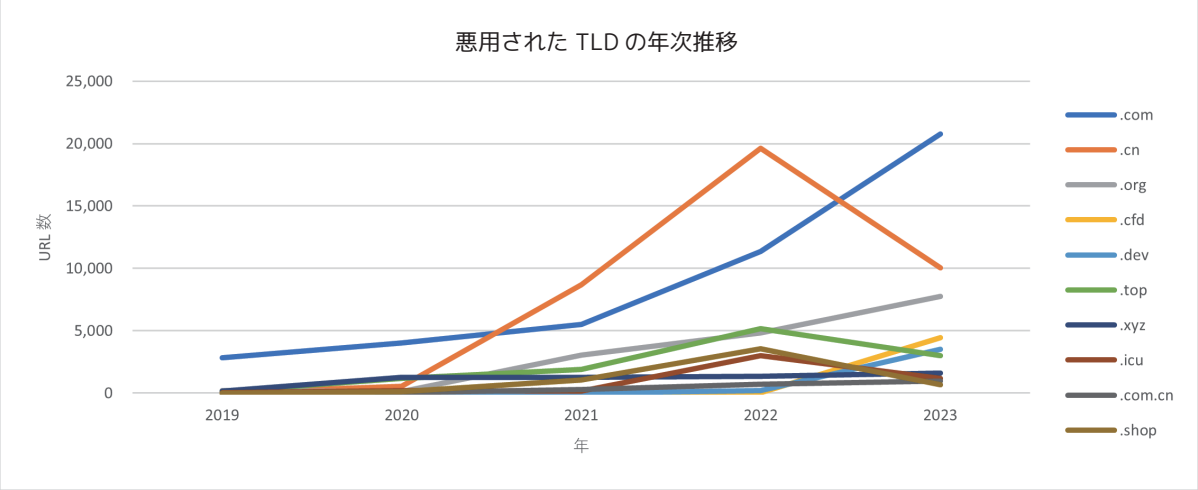


図8 悪用されたTLD数

3.4 サブドメイン型における正規サービスの悪用状況

サブドメイン型には 2 種類ある。

1. サブドメイン悪用：独自ドメインを取得しサブドメインに様々なパターンを付与
2. 正規サービス悪用：duckdns.org のような、サブドメインを使用する正規サービスを悪用

サブドメイン悪用の実態を把握するために、サブドメイン悪用と正規サービス悪用の 2 つのケースについて、それぞれの URL 数比較し、その比率を年別でプロットした折れ線グラフを図 7 に示す。数字が大きいほど正規サービス悪用が多いことを表している。

正規サービス悪用ケースは、2019 年から 2022 年までは 10 ～ 20 % で推移していたが、2023 年に 40% 超に急増していることが明らかになった。

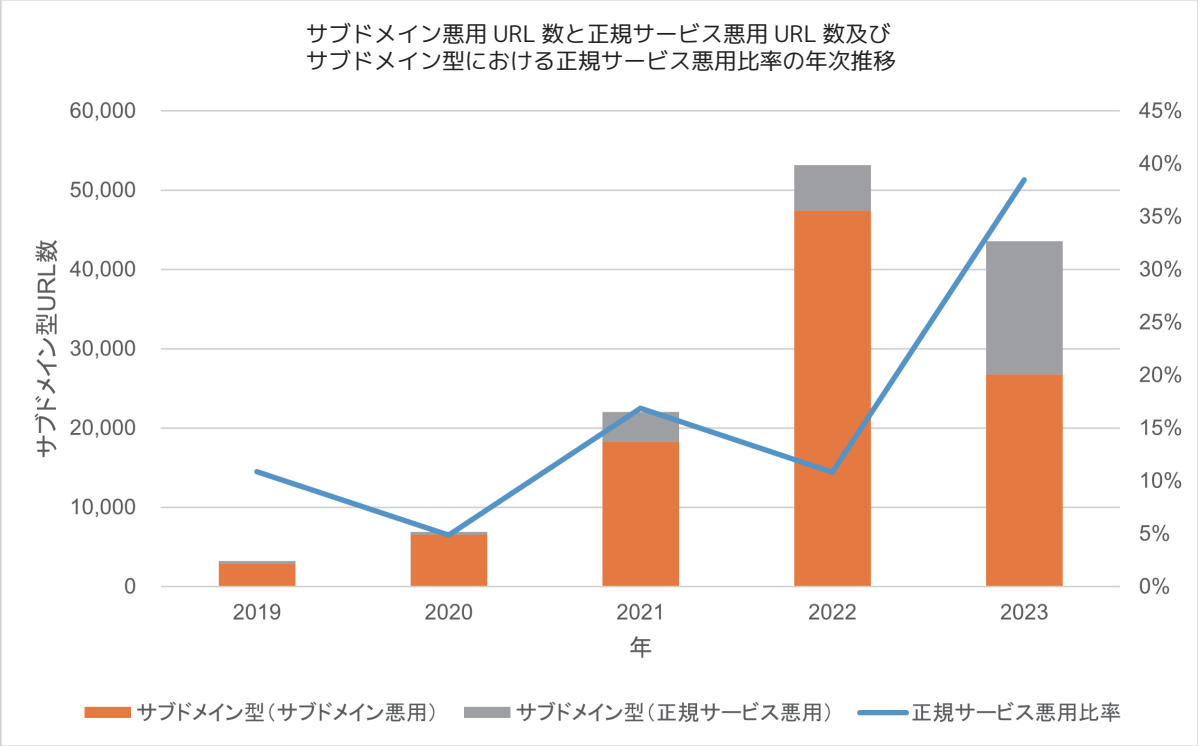


図9 サブドメイン型に対する正規サービス比率

正規サービス悪用 ケースの実態を把握するために、phishurl-list に登録されているURL 数を調査したところ、全体で 200 以上の正規サービス悪用が確認された。但し件数でみると duckdns.org と workers.dev が突出しており、他のサービスは誤差の範囲に留まった。図 10 に duckdns.org と workers.dev の不正使用数を示す。

悪用 URL 数で言うと、duckdns.org が圧倒的に多いが、2023 年は workers.dev の悪用が目立った。

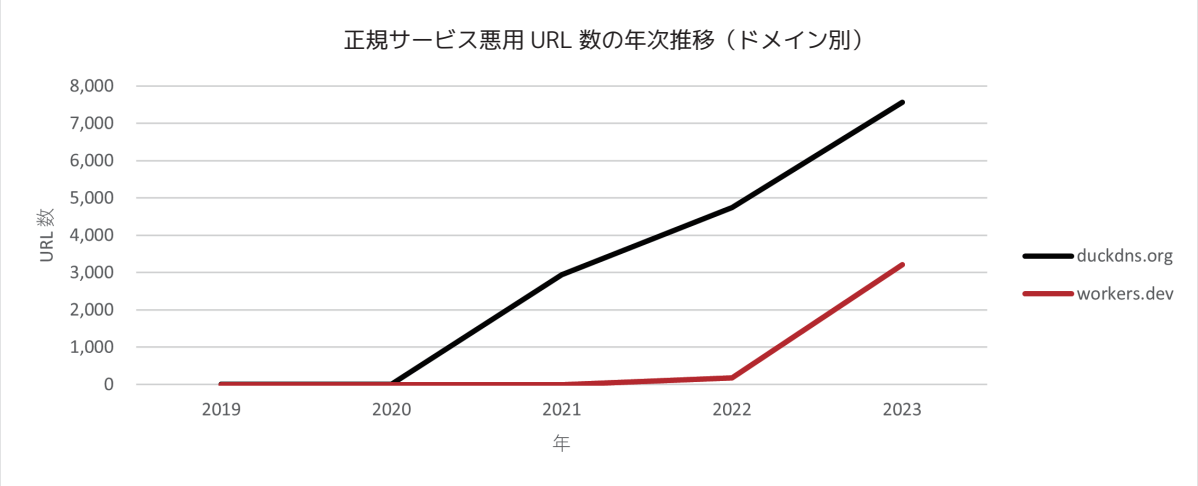


図10 正規サービス悪用型URL数

3.5 短縮 URL サービスの悪用

近年では、短縮 URL サービスの悪用も目立ってきている。
図 11 に、短縮 URL サービスの不正利用状況を示す。

2022 年は cutt.ly と tinyurl.com の悪用が目に付くが、2023 年は cutt.ly は急減し、代わって rebrand.ly が急増した。また、is.gd も増加している。短縮 URL サービスの悪用は全 URL 数と比較すると比較的低いが (2023 年は全 URL の約 1% 程度)、フィッシングサイトを確認する前にサイトが落ちてしまっているためにカウントされていない可能性も高く、注意が必要である。

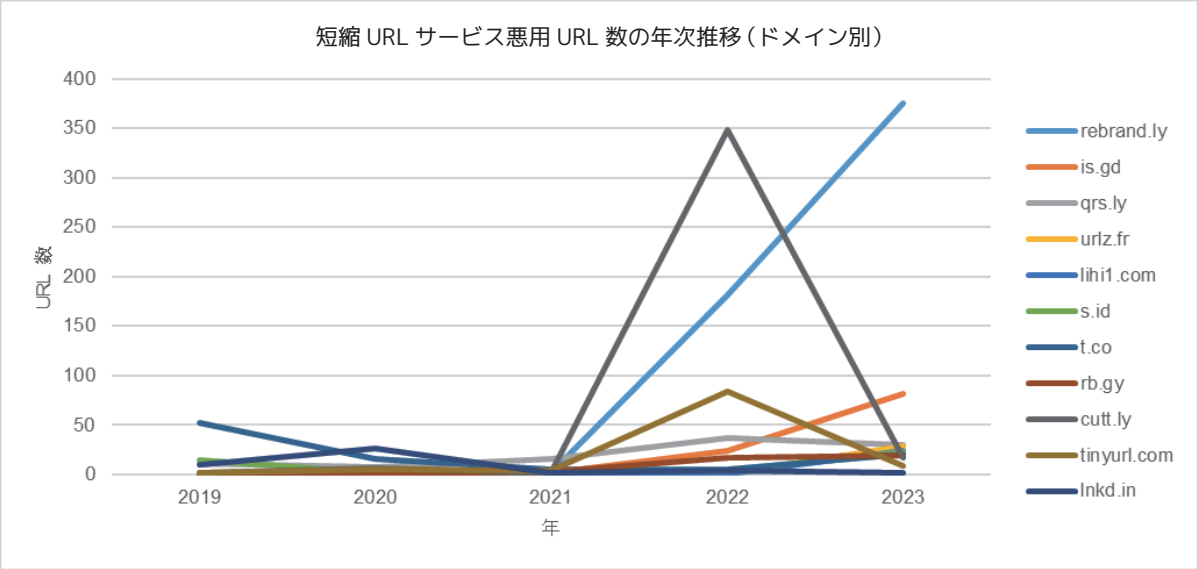


図11 悪用された短縮URLサービスドメイン

04 フィッシングサイト URL におけるドメイン悪用の傾向

この節では、フィッシングサイトにおけるドメイン悪用について説明していく。主要なドメイン／サブドメインの悪用手法は表 2 の通りである。なお、ドメイン悪用例提示のため、標的 FQDN 例として「www.macnica.co.jp」、標的ブランド名として「macnica」を用いる。

表2 主要なドメイン/サブドメイン悪用手法

手法名	手法	例
タイポスクワッティング	URL 直接入力の打ち間違えを狙う	wwwmacnica.co.jp
コンボスクワッティング	標的ブランド名をドメインに含める	www.login-macnica.co.jp
レベルスクワッティング	標的ドメインをサブドメインに含める	www.macnica.co.jp.example.com

4.1 基本的なドメイン悪用手法

4.1.1 タイポスクワッティング

タイポスクワッティングは、URL 直接入力の打ち間違いを狙う手法である。タイポスクワッティングの歴史は古く、例えば 2006 年に発表されたマイクロソフト社の Strider Typo-Patrol [2] では、5 つのタイポ生成モデルを示している 。[2]

1 Missing-dot typos
www の後のドットを消去するモデル

例
- wwwSouthwest.com

2 Character-omission typos
1 文字を省略するモデル

例
- Diney.com
- MarthStewart.com

3 Character-permutation typos
1 文字を入れ替えるモデル

例
- NYTiems.com

4 Character-replacement typos
1 文字を置き換えるモデル

例
- DidneyWorld.com
- USATodsy.com

5 Character-insertion typos
1 文字を挿入するモデル

例
- WashingtonPoost.com
- Googlle.com

2. 例示ドメインは [2] から引用

4.1.2 コンボスクワッティング

コンボスクワッティングは、例えば「**macnica-login**.co.jp」、「**support-macnica**.co.jp」のように、標的ブランド名に、「login」や「support」といった一般的なキーワードを組み合わせてドメインを構成する悪用手法である。

この手法は 2017 年に発表された論文 [3] において、以下の通り定義されている。

(1) The domain contains the trademark.
(2) The domain cannot result by applying the five typosquatting models of Wang et al [2].

4.1.3 レベルスクワッティング

レベルスクワッティングとは、ドメイン管理者はサブドメインパターンを自由に設定できることを悪用し、例えば「**macnica.co.jp**.example.com」や「**www.macnica.co.jp**.example.com」のように、標的対象の正規ドメインや正規 FQDN をサブドメインパターンに含めて運用するドメイン悪用手法である。この手法は 2019 年の論文 [4] で初めて大規模に評価された。

ブラウザでは、URL の構成上、文字列の前の方にあるサブドメインから表示していくため、特に表示領域が狭いスマートフォンでは、サブドメインパターンを正規 URL と見間違えてしてしまうリスクが指摘されている。

4.2 悪用状況の評価結果

4.2.1 タイポスクワッティングの評価結果

タイポスクワッティングは打ち間違えを狙う攻撃であるため、e メールを送信し、フィッシングサイトへのリンクをクリックさせようとするフィッシング攻撃で積極的に選択される手法ではない。

ホモグラフのような見間違えを狙う類似ドメインがタイポスクワッティングの条件に合致することもあるが、近年、タイポスクワッティングを悪用したフィッシングサイトはほとんど見られなくなってきている。そのため、本レポートでは、タイポスクワッティングを分析対象外とする。

4.2.2 コンボスクワッティングの評価結果

・4.2.2.1 評価手法について

4.1.2 節で説明したコンボスクワッティングの定義に基づき、ドメインを悪用したフィッシング FQDN に、表 1 に示した上位 20 ブランド名が含まれているかどうかを部分文字列一致で件数を数え上げた。[3]

3. 前処理として、phishurl-list に記載されたフィッシング URL から FQDN を抽出し、重複排除を行ったフィッシング FQDN リストを作成した。

表3 コンボスクワッティング評価に用いたブランド名と探索文字列

ブランド名	探索文字列	ブランド名	探索文字列
Amazon	amazon	メルカリ	mercari
三井住友カード	smbc-card	ETC 利用照会サービス	etc-meisai
au	au	エポスカード	eposcard
SAISON CARD	saisoncard	イオンカード	aeon
えきねっと	eki-net	イオン銀行	aeonbank
Apple ID	apple	SoftBank	softbank
三菱 UFJ ニコス	mufg	ヤマト運輸	kuronekoyamato
楽天	rakuten	JCB	jcb

・4.2.2.2　評価結果について

図 12 に、コンボスクワッティング悪用評価結果を示す。

2019 年と 2020 年において、ドメインのみを悪用したフィッシング FQDN の約 25 % がコンボスクワッティングを悪用していたが、これらの年をピークに、2023 年には約 2.2% まで減少している。この結果は、ドメイン部分での単純なブランド名模倣が現在ではほとんどなくなったことを示している。

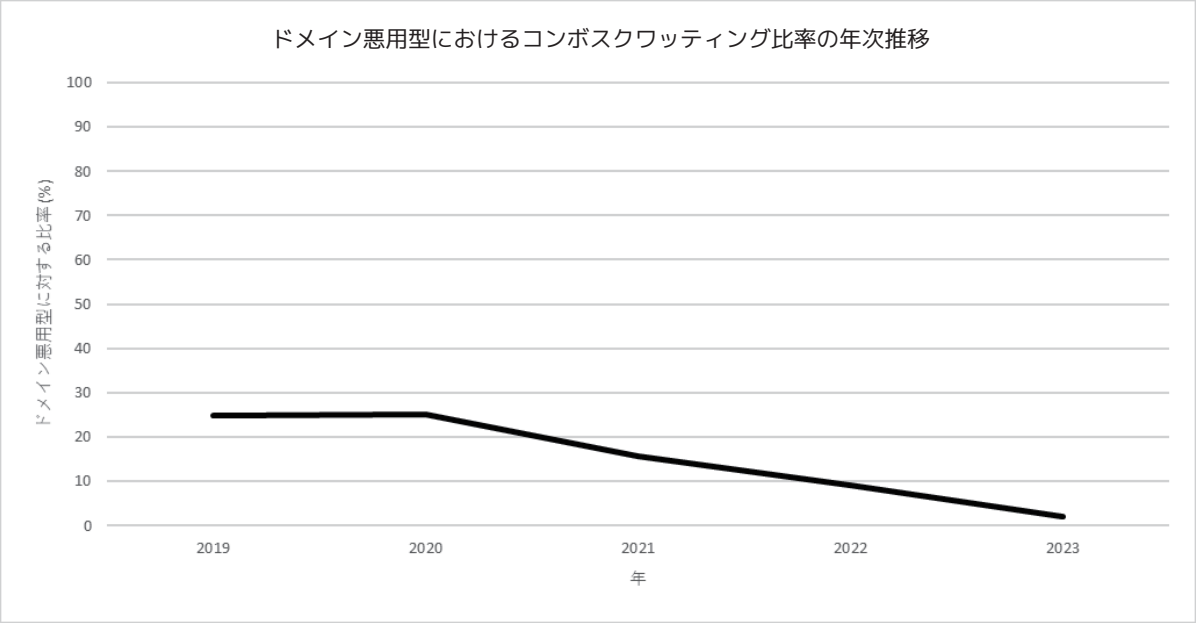


図12 コンボスクワッティング悪用評価結果

図 13 に、個別ブランドのコンボスクワッティング悪用評価結果を示す。

個別ブランドのドメイン悪用は母数自体が少ないため、ドメイン悪用自体が少ないために比率が高く出ているものは除外すると、コンボスクワッティングで狙われやすいブランドは au、楽天、JCB、国税庁であった。

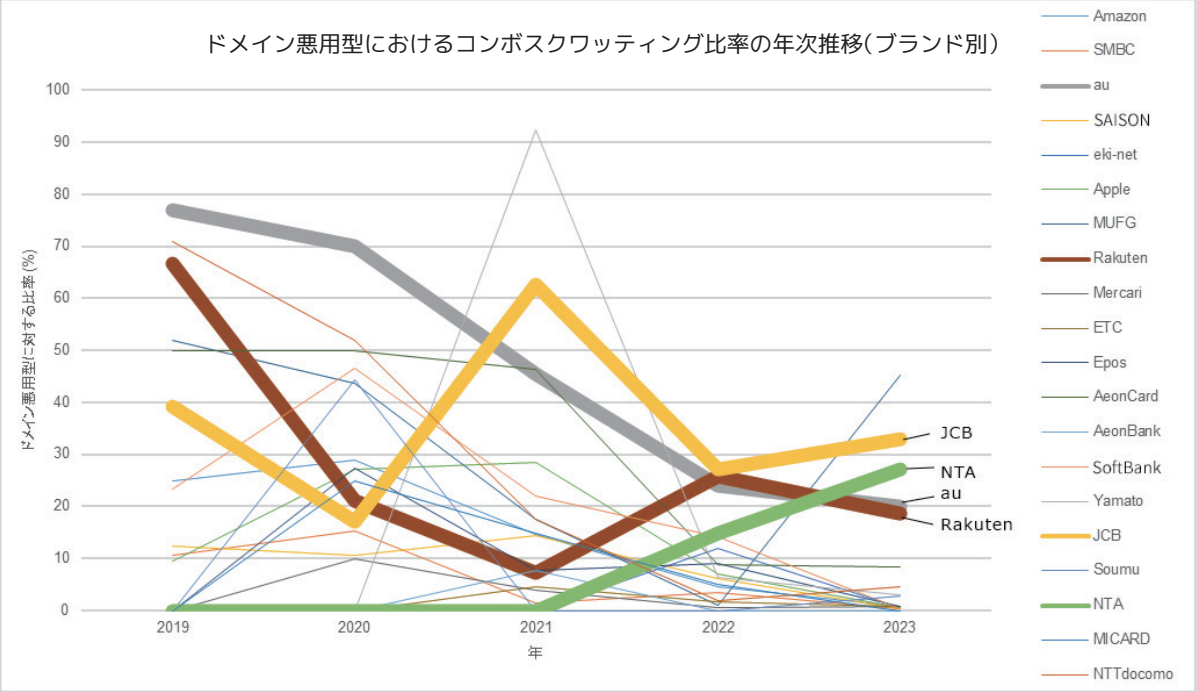


図13 ブランド別コンボスクワッティング悪用評価結果(au、楽天、JCB、国税庁強調)

4.2.3 レベルスクワッティングの評価結果

・4.2.3.1 評価手法について

攻撃者は、所有するドメインに対して任意の文字列をサブドメインパターンとして設定できることから、例えば「**www.macnica.co.jp**.example.com」に限らず、「**macnica**.example.com」や「**www.macnica**.example.com」のように、標的対象の正規ドメインだけではなく、標的ブランドの一部や正規 URL の一部もサブドメインパターンに用いることができる。

従って、本レポートでは、ブランド名と正規 URL の一部も探索対象とし、完全一致で URL を数え上げた。

表4 レベルスクワッティング評価に用いたブランド名と探索文字列

ブランド名	探索文字列
Amazon	amazon, www.amazon, amazon.co.jp, www.amazon.co.jp, amazon.com, www.amazon.com
三井住友カード	smbc-card, www.smbc-card, smbc-card.com, www.smbc-card.com
au	au, www.au, au.com, www.au.com
SAISON CARD	saisoncard, www.saisoncard, saisoncard.co.jp, www.saisoncard.co.jp
えきねっと	eki-net, www.eki-net, eki-net.com, www.eki-net.com
Apple ID	apple, www.apple, apple.com, www.apple.com
三菱 UFJ ニコス	mufg, www.mufg, bk.mufg.jp, www.bk.mufg.jp
楽天	rakuten, www.rakuten, rakuten.co.jp, www.rakuten.co.jp
メルカリ	mercari, jp.mercari, mercari.com, jp.mercari.com
ETC 利用照会サービス	etc-meisai, www.etc-meisai, etc, www.etc, etc-meisai.jp, www.etc-meisai.jp
エポスカード	eposcard, www.eposcard, eposcard.co.jp, www.eposcard.co.jp
イオンカード	aeon, www.aeon, aeon.co.jp, www.aeon.co.jp
イオン銀行	aeonbank, www.aeonbank, aeonbank.co.jp, www.aeonbank.co.jp
SoftBank	softbank, www.softbank, softbank.jp, www.softbank.jp
ヤマト運輸	kuronekoyamato, www.kuronekoyamato, kuronekoyamato.co.jp, www.kuronekoyamato.co.jp
JCB	jcb, www.jcb, jcb.co.jp, www.jcb.co.jp
総務省	soumu, www.soumu, soumu.go.jp, www.soumu.go.jp, myna, myna.go.jp, mynumbercard, mynumbercard.point, mynumbercard.point.soumu.go.jp
国税庁	nta, www.nta, nta.go.jp, www.nta.go.jp, e-tax, www.e-tax, e-tax.nta.go.jp, www.e-tax.nta.go.jp
MICARD	micard, www2.micard, micard.co.jp, www2.micard.co.jp
NTT docomo	docomo, www.docomo, docomo.ne.jp, www.docomo.ne.jp

・4.2.3.2　評価結果について

図 14 に、レベルスクワッティング悪用評価結果を示す。

2020 年においては、サブドメインを悪用したフィッシング FQDN の約 20% がレベルスクワッティングを悪用していたが、この年をピークに、2023 年には約 1.7% まで減少している。この結果は、サブドメイン部分での単純な正規ドメインやブランド名の模倣が現在ではほとんどなくなったことを示している。

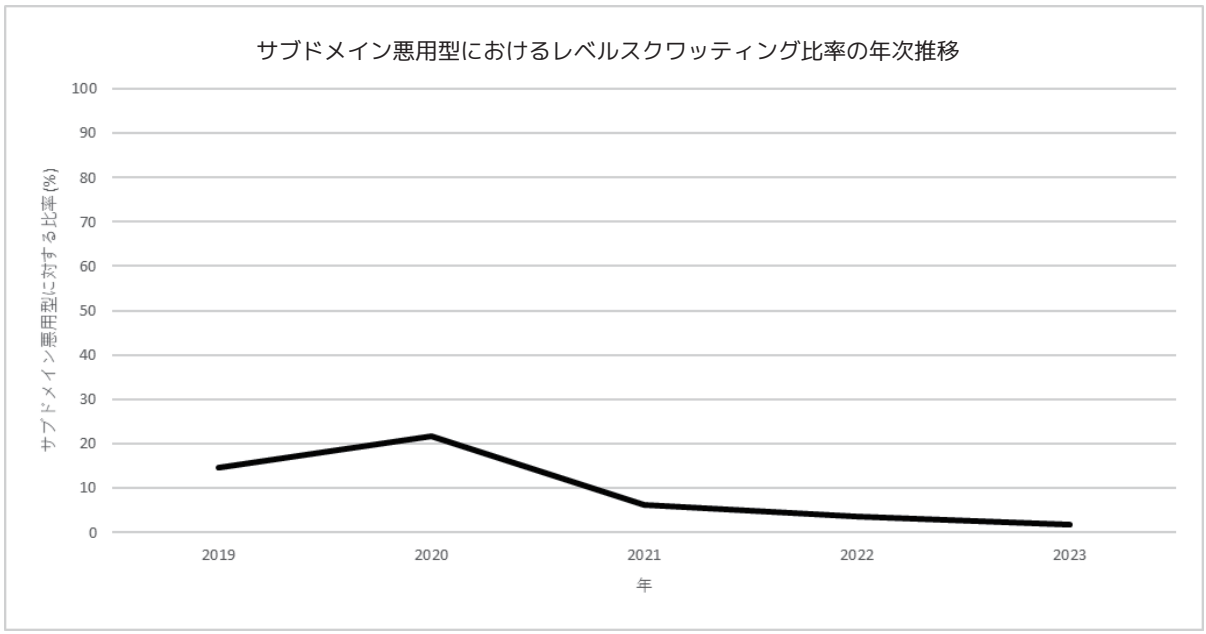


図14 レベルスクワッティング悪用評価結果

図 15 に、個別ブランド（Amazon、三井住友カード、楽天）のレベルスクワッティング悪用評価結果を示す。

2019 年から 2020 年にかけて、これらのブランドを標的としたレベルスクワッティングの悪用が目立ち、特に三井住友カードと楽天では、サブドメイン悪用 URL の約 4 割がレベルスクワッティングである。しかし、2020 年以降は減少傾向となり、2022 年以降はレベルスクワッティングがほとんど観察されなくなっている。

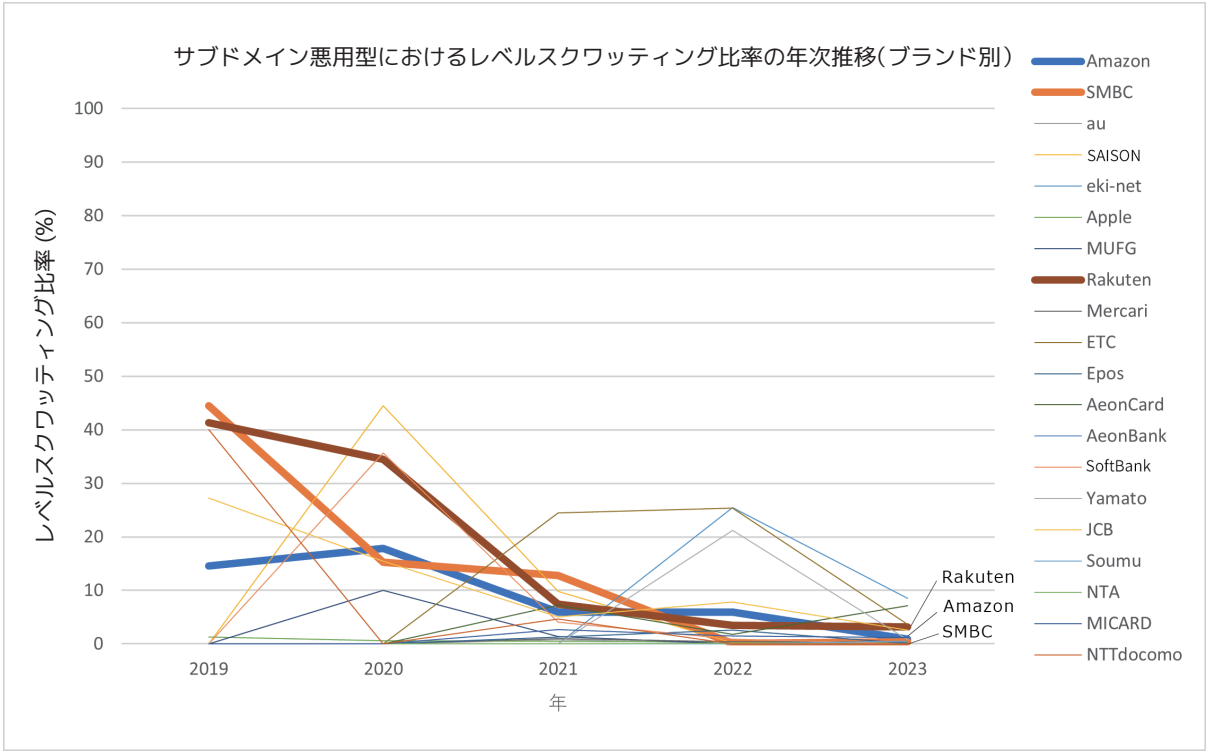


図15 ブランド別レベルスクワッティング悪用評価結果 (Amazon、三井住友カード、楽天強調)

続いて、図 16 に、個別ブランド（えきねっと、ETC 利用参照サービス）のレベルスクワッティング悪用評価結果を示す。

2021 年から 2022 年にかけては、これらのブランドを標的としたレベルスクワッティングの悪用が目立つ。えきねっとは 2023 年も約 1 割のレベルスクワッティングの悪用が見られるが、全体的に見れば、やはり 2022 年以降減少傾向である。

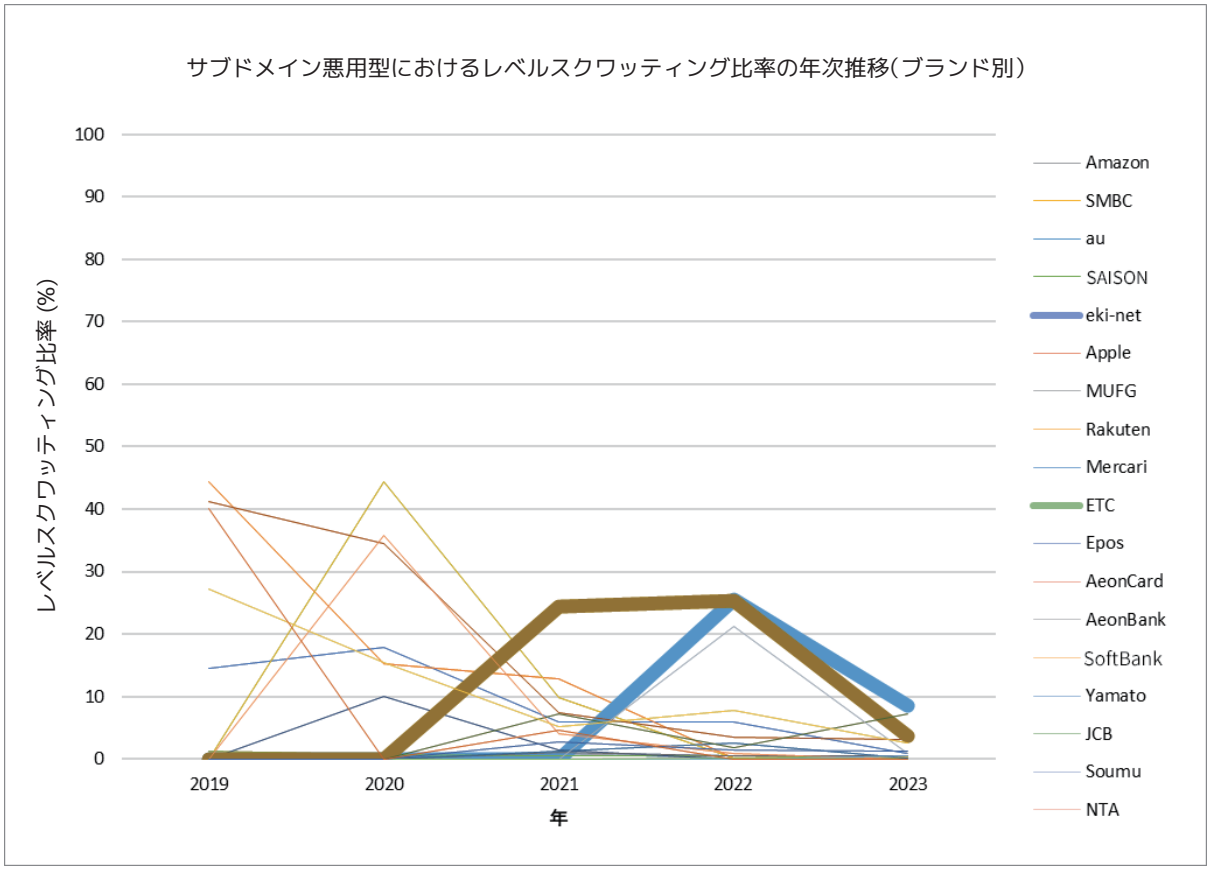


図16 個別ブランドのレベルスクワッティング悪用評価結果 (えきねっと、ETC利用参照サービス)

4.3 サブドメイン悪用パターン

4.2 節で見てきたように、単純な正規ドメインやブランド名模倣による、コンボスクワッティングやレベルスクワッティングはほとんど見られなくなった。それでは、2023 年に用いられたフィッシング FQDN にはどのようなパターンが多かったのだろうか？

結論から言えば、例えば「macn1ca」のような視覚上類似した文字列への置換（ホモグラフ）、「mcnca」のようなホモグラフではないが全体として正規ブランド名などに誤認識してしまう文字列への変形、「fjslfg」のような単語として意味を持たないランダム文字などをサブドメインパターンに用いるものが非常に多かった。

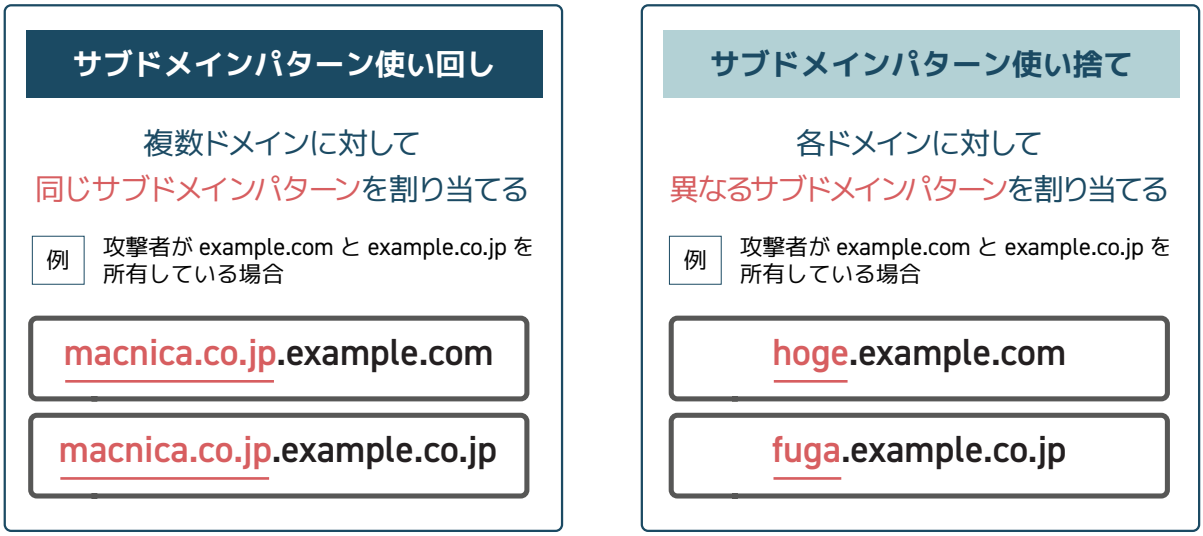
このような手法では、コンボスクワッティングやレベルスクワッティングと比較して多くの変則サブドメイ

ンパターンを容易に作り出すことが可能であるが[4]、興味深いことに、標的ブランドによってサブドメインパターンの運用方法が大きく異なっていることが今回判明した。

この節では、2023 年に悪用された FQDN をサブドメインパターンの使い回しと使い捨てという観点で深堀りしていくこととする。

4.3.1 サブドメインパターンの使い回しと使い捨て

ドメイン管理者は、サブドメインパターンを自由に設定し運用することが可能である。そのため、攻撃者が複数のドメインを取得した場合、それらのドメインに対するサブドメインの割り当て方は大きく以下の 2 つである。



4.3.2 評価手法について

表 1 評価対象とした上位 20 ブランドで示した上位 10 ブランドを分析対象とし、フィッシング FQDN がサブドメインパターン使い回しを行っているか、それともサブドメインパターンの使い捨てを行っているかを区別してカウントした。

4.3.3 評価結果について

図 17 に、サブドメインパターン使い回し率の結果を示す。

2021 年から 2022 年にかけて、多くのブランドでサブドメイン使い回しパターンが用いられていた。しかし、2023 年には、Amazon、三井住友カード、au、SAISON CARD、Apple ID といった上位ブランドの約 1 割しかサブドメインパターン使い回しが見られなくなり、約 9 割はサブドメイン使い捨てパターンへと手法が変化している。

4. 例えば、「macn1ca」「mcnca」「mcn1ca」「mcnc」「macnc」「mcn」など。

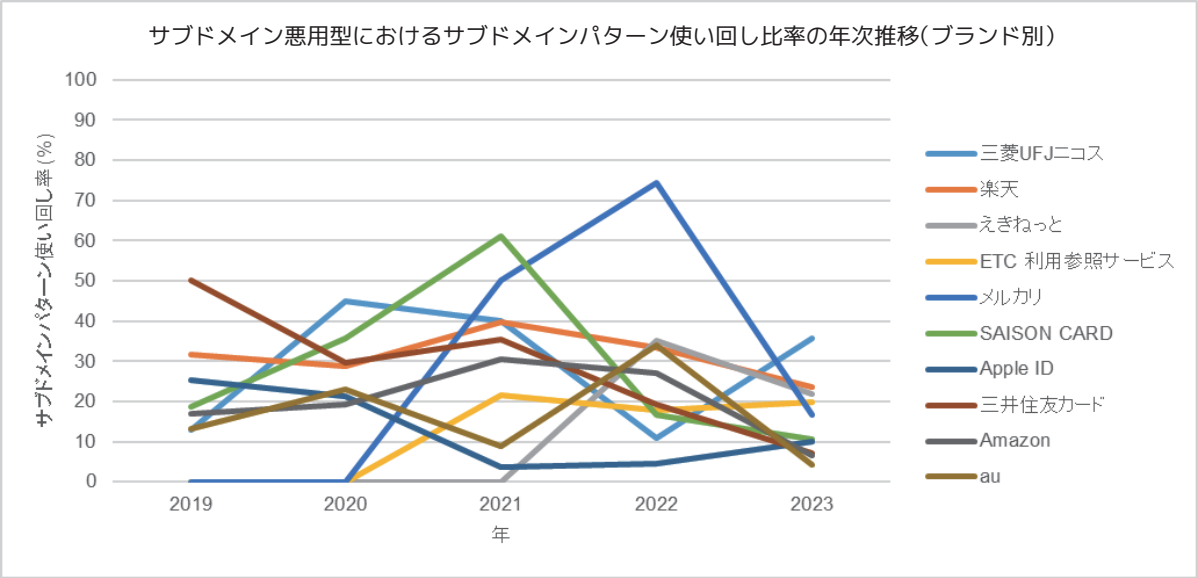


図17 サブドメイン使い回しパターン評価

図 18 に、サブドメインパターンの使い回しされたドメイン数の年別の最大を評価した結果を示す。この評価では、数が多いほど同じサブドメイン悪用パターンが多くのドメインにマップされたことを意味する。

2022 年と 2023 年のえきねっとでは、「www.eki-net」という正規 FQDN の一部分がサブドメインパターンとして悪用され、「www.eki-net.com」という正規 FQDN の悪用と合わせると、約 500 のドメインで使い回しされていた。また、2023 年の ETC 利用参照サービスでは、実に 600 以上のドメインでサブドメインパターンの使い回しがされていた。

続いて、2020 年の楽天では、「rakuten.co.jp」という正規ドメインを用いた典型的なレベルスクワッティングが 約 500 のドメインで用いられていた。図 14 と関連付けると、楽天を標的としたサブドメイン悪用 URL の約 35% がレベルスクワッティング悪用であった。また、2022 年の au では、300 を越えるドメインでサブドメインパターンが使い回されていた。しかし、両者とも、2023 年ではサブドメインパターンの使い回しは減少し、サブドメインパターンの使い捨てへと変化している。

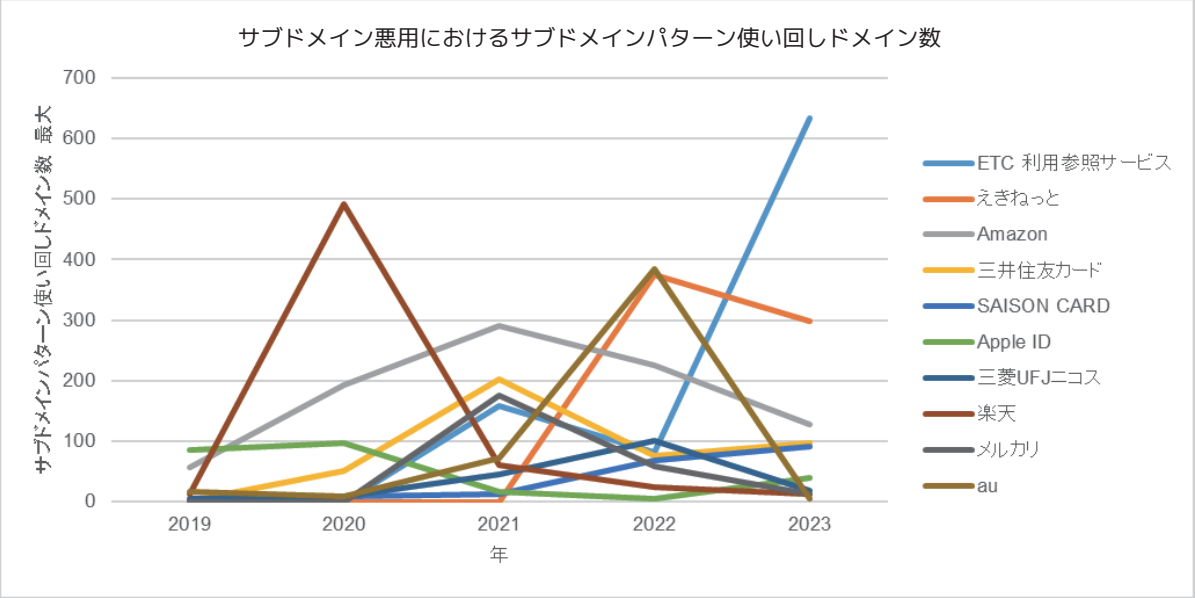


図18 サブドメイン使い回しパターン　ドメイン数　最大

4.3.4　サブドメインパターンの使い回しが行われているブランド毎の評価

・4.3.4.1　えきねっと

表 5 に、えきねっとを標的としたフィッシング URL のサブドメインパターンを示す。

2022 年に最も多く見られたサブドメインパターンは「www.eki-net」であり、[5] ではこのサブドメイン悪用パターン使い回しを逆手にとってフィッシングサイト追跡に成功した結果について報告した。2022 年を全体的に見ると、「eki-net」「ekl」「eki」といった文字列をベースにパターンを生成しているような印象を受ける。

2023 年になると、www.eki-net の悪用も続いたものの、5 位から 8 位のような、「eki」という単語を長い文字列の一部に含めた変則的なパターンが見て取れる。

表5 えきねっとを標的としたサブドメインパターン

2022 年		2023 年	
www.eki-net	375	emv1	299
ekl.net	217	www.eki-net	242
eki-net	208	ekicomjp	179
www.eki-net.com	124	mta-sts	177
wwww	122	www.eki-co-jp-adrm-info	167
www.eki	112	www.il-ekii-co-jp.open	161
eki-net.com.personal	97	www.go-eki-co.jp-anoa	120
www.eki-service	96	www.ekii-co-jp.admc-infor	114
eki	91	service	111
ekl-not	84	www.eki.login	105

図 19 に、えきねっとのレベルスクワッティングと、部分文字列 (eki) を含むサブドメインパターンの比率を示す。なお、レベルスクワッティングと判定された場合には、部分文字列悪用とは判定しないようにした。

2022 年は、正規 URL やブランド名を含めたレベルスクワッティングも一定数見られたが、2023 年はレベルスクワッティングから「eki」を含むサブドメインパターンへ移行し、半分以上を占める結果となった。

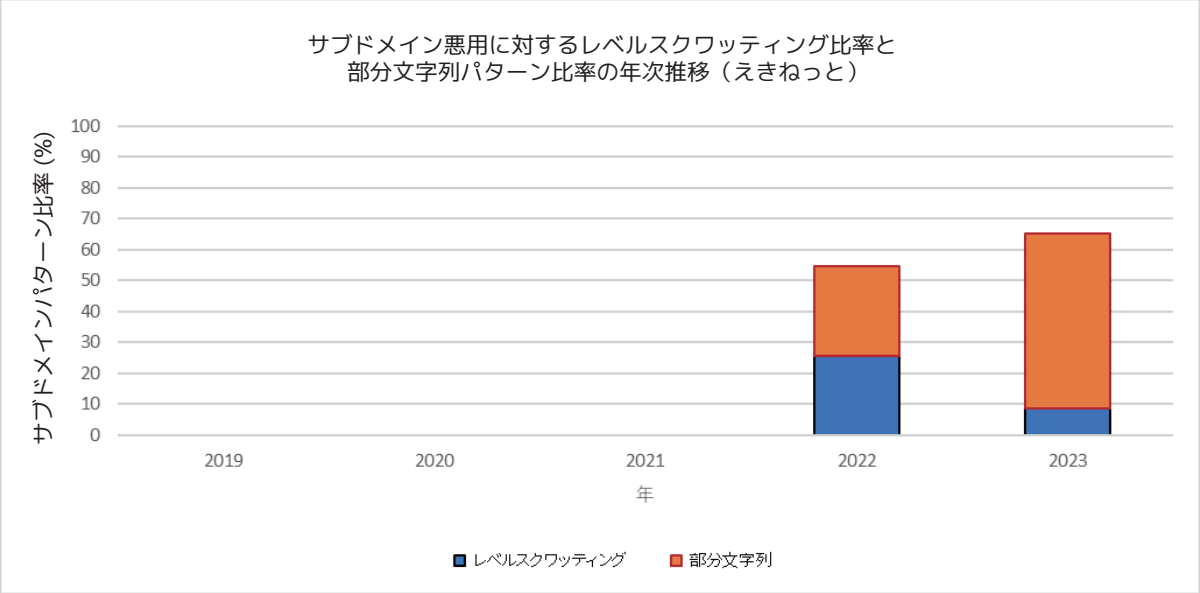


図19 レベルスクワッティングと部分文字列悪用比率:えきねっと

・4.3.4.2　ETC 利用参照サービス

表 6 に、ETC 利用参照サービスを標的としたフィッシング URL のサブドメインパターンを示す。

2022 年は、「etc-meisai」をベースに「meisai」の部分を変形させたパターンの悪用が目立つ。

2023 年になると、サブドメインパターンとして、コンボスクワッティングのような etc に「login」や「userinformation」といった一般的な文字列を組み合わせて、etc を装う悪用が目立つ。

いずれにせよ、etc を中心に生成したサブドメインパターンを使い回す戦略のようである。

表6 ETC 利用参照サービスを標的としたサブドメインパターン

2022 年		2023 年	
etc-maisai	81	www.etc.login	633
etc	81	www.etc.userinformation	281
www.etc-meisia	71	www2.etc-meisai.jp	123
etc-meisai.jp	64	www2.etc-merisai.jp.login	100
etc-melsal	61	www2.etc-merisai.jplogin	86
etc-meisei	48	www2.etc-meisai.jpetcrfunccode1013000000	53
www.etc-meisai	47	www.etc.userlogin	53
etc-meisla	41	www.etc-noreply	50
www.etc-meisai.jp	28	www.etc-meisai	46
www2.etc.miasei	24	mq.mbd	39

図 20 に 、ETC 利用参照サービスのレベルスクワッティングと部分文字列 (etc) を含むサブドメインパターンの比率を示す。レベルスクワッティングと部分文字列悪用の区別はえきねっと同様、重複した場合にはレベルスクワッティング優先にした。

2021 年と 2022 年ではレベルスクワッティングも多かったが、2023 年では 7 割以上が「www.etc.login」のような etc を悪用したサブドメインパターンを用いていた。ETC 利用参照サービスが標的の場合の特徴といえる。

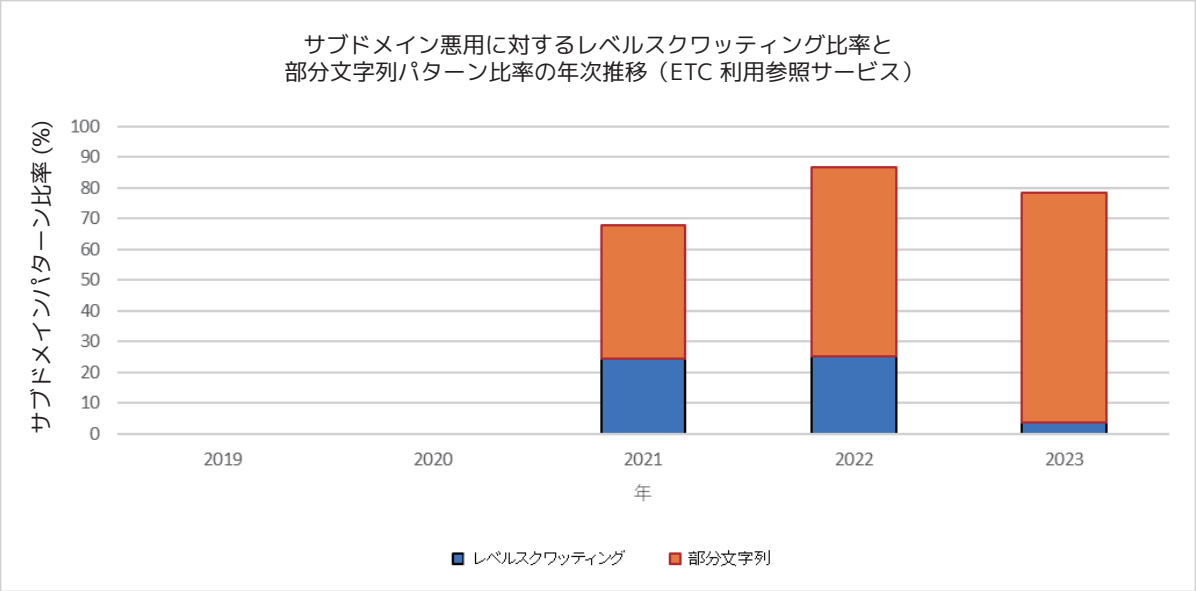


図20 レベルスクワッティングと部分文字列悪用比率:ETC利用参照サービス

4.3.5　サブドメインパターンの使い捨てが行われているブランド毎の評価

・4.3.5.1　au

表 7 に、au を標的としたフィッシング URL のサブドメインパターンを示す。

2022 年では、少し長めの文字列の中に「au」という文字列を紛れ込ませて使い回す戦略がとられていた。
2023 年では、URL 数自体が急減したこともあるが、ほとんどがランダム文字列の使い捨てとなっている。

表7 auを標的としたサブドメインパターン

2022 年		2023 年	
connecct-login	385	net	6
connecti-auonepay-jp	318	gonnecct-login	3
inof-auoneo-jp	211	ekl.net	2
au-pay-auoneo	174	orgbidusgg	2
aiu.kdda	155	fsdelkf	2
bwut-au-pay	112	cvonnecct-login	2
auopay-auoneo-jp	109	pirhnslkdhg	2
kddio-fsi-com	82	www.au-one	2
doneg-jp	59	ysfbaslhf	2
connecti-auonei-jp	57	ospajdapsd	2

・4.3.5.2　Apple ID（ランダム文字）

表 8 に、Apple ID を標的としたフィッシング URL のサブドメインパターンを示す。

2022 年と 2023 年において、表 8 に出した文字列も含め、apple 自体、あるいは類似文字列を悪用したパターンは全体の中のごく一部で、ほとんどがランダム文字列となっている。

表8 Apple IDを標的としたサブドメインパターン

2022 年		2023 年	
aaaaa	5	aaaaa	39
apple	4	appleid	18
owqrxdvkyo	3	apple-account	12
ooumpvnswd	3	0	10
tcqzjxvmwx	3	apple	7
appleid.apple.com	3	axuts	5
xdfvkytimh	3	7	4
sopvtvjonp	3	gnnnl	4
eeymzudjbo	3	2	4
pbdaikemad	2	l	4

・4.3.5.3　Amazon

表 9 に、Amazon を標的としたフィッシング URL のサブドメインパターンを示す。

図 15 で見たように、Amazon のレベルスクワッティングが多かったのは 2020 年までで、2022 年と 2023 年はタイポスクワッティングの条件にあてはまるものもあるが、amazon を変形させ類似文字列とも言えない amazon 風の変形パターンが目立つ [5] 。また、日本の ccTLD である「jp」を「ip」に変形が目に付く [6]。

約 9 割がサブドメインパターン使い捨てであるが、一方で、多くのドメインで使い回すパターンも多い。

表9 Amazonを標的としたサブドメインパターン

2022 年		2023 年	
amzanao.co.ip	226	www.amazom	127
www.anazom.co.jp	174	amzone.co.jp	100
anazno.co.ip	129	amzanao.co.ip	78
amazon	102	s	71
s	96	www.arnozansigin	62
amzanon.co.ip	87	www.anazom.userinformation	50
support	66	account	41
account	62	mq.mbd	37
amazon.co.jp	60	www2.amazaon.co.jp.login	32
www.anazom	59	www.amzanao.co.ip	28

・4.3.5.4　SAISON CARD

最後に、表 10 に、SAISON CARD を標的としたフィッシング URL のサブドメインパターンを示す。

2022 年は 、「www」.「saison 風の文字列」.「saison 風とも言えないような文字列」というサブドメインパターンを生成する戦略だったようである [7] 。

2023 年は、正規ドメインである saisoncard.co.jp のうち「saisoncard」の部分を変形させ、サブドメインパターンとして用いる戦略だったようである [8] 。いずれにせよ、正規 FQDN をそのまま悪用せず何らかの変形する戦略であったようである。

5. 例 : amzone.co.jp.(攻撃者のフィッシングドメイン)

6. 例 : amazanao.co.ip.(攻撃者のフィッシングドメイン)

7. 例 : www.scaieccaisn.seseccaoin.(攻撃者のフィッシングドメイン)

8. 例 : www.saiseccerd.co.jp.(攻撃者のフィッシングドメイン)

表10 SAISON CARDを標的としたサブドメインパターン

2022 年		2023 年	
apl.saisoncarb.co.jp	68	emv1	91
www.scaieccaisn.seseccaoin	30	service	47
www.saiseocn.saeseon	29	wwwsaisoncald	45
www.saeisocen.scaseeoe	29	_.s1	42
www.saesoccin.scaseein	27	s1	41
www.saeisoen.scaseoe	26	www.saiseccerd.co.jp	20
www.saiseoccin.saeseceon	26	www.saiaoncacard.co.jp	20
www.saesocciin.scasecein	25	www.saisonoacrd.co.jp	20
www.scaiecasn.sescaoin	24	www.saisoncacrd.co.jp	20
www.saiseoccn.saeseeon	24	www.saiconsacrd.co.jp	20

05 まとめ

フィッシングサイトの URL について、構成文字列の悪用箇所は、現在、ドメイン部分ではなくサブドメインパターンが中心である。サブドメインパターンはドメインオーナーが自由に付与できるため悪用の方法は幅広いとともに、ドメイン部分を悪用しないため、ドメイン判定によるフィッシングサイト検出は無効となる。

現在主流のサブドメイン悪用についても、旧来からのブランド模倣型（例：macnica-login.example.co.jp や www.macnica.co.jp.example.com）は限定的となり、ランダム文字列からなるサブドメインも目立ち始めている。また、正規サービス（duckdns.org など DDNS サービス、t.co など短縮ＵＲＬサービス）を活用した URL 生成が顕著になっている。こうした傾向は、従来の判定技術ではフィッシングサイトの検出率が低くなることを意味する。

URL に基づくフィッシングサイト検知では、以下の理解が重要である；

- ドメイン部分を悪用しないため、ドメイン部分だけで悪性判定を行う手法はフィッシングサイトに対する識別カバー率がほぼ無い。サブドメイン部分を含むＦＱＤＮ全体を判定対象にすることが必要である。
- ブランド名称を模倣したドメイン名の生成は主流ではない。ブランド名を一致判定キーワードとする URL 悪性判定法では、フィッシングサイトに対する識別力は限定的である。（少数の特定ブランドに対しては現時点でも有効）
- 短縮 URL や DDNS など正規サービスを悪用するフィッシング URL が大幅に増えている。正規サービスの URL を許可リスト型で運用することは高いリスクを持っている。

フィッシングアクターはセーフブラウズ、スパムメールフィルタ、迷惑 SMS 拒否設定などの強固なフィルターを突破すべく URL の悪用方法を変化させている。phishurl-list の分析からその変化傾向と最新動向が明らかとなった。結果、従来の URL 判定技術ではフィッシングサイトが検出できなくなりつつあることが判明した。一方で phishurl-list の元になっているアンチフィッシングコミュニティによるフィッシングサイト検出能力の高さは特筆に値し、コミュニティによる継続的な対策が攻撃者側の URL 模倣戦略を断念させたという言い方もできる。コミュニティが蓄積した成果を読み解き、新たな対策技術につなげることが重要である。

06 参考文献・引用情報

[1] phishurl-list. https://github.com/JPCERTCC/phishurl-list

[2] Wang, Yi-Min, et al. “Strider Typo-Patrol: Discovery and Analysis of Systematic Typo-Squatting.” SRUTI 6.31-36 (2006): 2-2.

[3] Kintis, Panagiotis, et al. “Hiding in plain sight: A longitudinal study of combosquatting abuse.” Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. 2017.

[4] Du, Kun, et al. “TL; DR hazard: a comprehensive study of levelsquatting scams.” Security and Privacy in Communication Networks: 15th EAI International Conference, SecureComm 2019, Orlando, FL, USA, October 23–25, 2019, Proceedings, Part II 15. Springer International Publishing, 2019.

[5] 谷口剛、えきねっとをかたるフィッシングから Club J-WEST への標的切替の追跡ーサブドメインを悪用したフィッシングの脅威，第 7 回フィッシング対策勉強会．2023 年 1 月 20 日．

マクニカは、1972 年の設立以来、最先端の半導体、電子デバイス、ネットワーク、サイバーセキュリティ商品に技術的付加価値を加えて提供してきました。従来からの強みであるグローバルにおける最先端テクノロジーのソーシング力と技術企画力をベースに、AI/IoT、自動運転、ロボットなどの分野で新たなビジネスを展開しています。
その中でセキュリティにおいては、最先端のセキュリティ商材を提供する中で独自の研究機関を有し、日本の企業に着弾したサイバー攻撃や対策をリサーチしています。

富士通ディフェンス＆ナショナルセキュリティ株式会社(略称FDNS)は、防衛省・自衛隊の情報通信システムの開発・構築から防衛関連の電子機器・情報通信システムのサポート、更には安全保障やセンサー・システムの調査や研究を行うことで日本の安全保障(安心・安全)を支えております。
また、防衛で培った高い技術力を民需システムにも一部展開している会社です。

株式会社マクニカ

本社　〒222-8561 横浜市港北区新横浜1-6-3 マクニカ第1ビル
〒222-8563 横浜市港北区新横浜1-5-5 マクニカ第2ビル
TEL.045-476-2010 FAX.045-476-2060

西日本営業所　〒530-0005 大阪市北区中之島2-3-33 大阪三井物産ビル 14階
TEL.06-6227-6916 FAX.06-6227-6917