ドメインパーキングを利用するドメイン名の大規模実態調査

戸祭 隆行[1,a)]　千葉 大紀[2]　秋山 満昭[2]　内田 真人[1]

概要：ドメインパーキングとは，利用していないドメイン名へのアクセスに対して広告を表示し，その広告報酬を得るための仕組みである．サイバー攻撃に利用された悪性ドメイン名がドメインパーキングを利用する事例が知られている．しかし，そのようなドメイン名が，ドメインパーキングにより管理される期間と，悪性活動に利用される期間との関係については，詳細が明らかになっていない．そこで本稿では，これらの期間の重複や時間的な前後といった時系列的な関係について，過去 19 ヶ月間にドメインパーキングを利用した実績のある合計 6,680 万件のドメイン名を対象にした大規模実態調査を行った．調査の結果，先行研究では報告されていない，ドメインパーキング利用後に悪性利用されるという特徴的な時系列パターンをもつドメイン名を新たに 3,964 件発見した．また，これまで知られていない複数のドメインパーキング事業者を同時あるいは切替えながら利用する 334 万件のドメイン名の存在が明らかになった．今回の調査結果は，ドメインパーキングの設定状況の変化を利用した悪性ドメイン名の解析を精度良く実現するために必要な情報である．

A Large-scale Analysis of Parked Domain Names

Takayuki Tomatsuri[1,a)]　Daiki Chiba[2]　Mitsuaki Akiyama[2]　Masato Uchida[1]

Abstract: Domain parking is a monetization mechanism for displaying online advertisements in unused domain names. Some domain names used in cyberattacks are known to leverage domain parking services after the attack. However, the temporal relationships between domain parking services and malicious domain names are not studied well so far. In this paper, we investigate how malicious domain names using domain parking services change over time. We conduct a large-scale measurement study using over 66.8 million domain names that have used domain parking services in the past 19 months. We newly reveal the existence of 3,964 malicious domain names after using domain parking services in addition to that before using them. Moreover, we reveal the existence of 3.3 million domain names that utilize multiple parking services simultaneously or while switching. Our study can contribute to accurate analysis of malicious domain names using domain parking services.

1. はじめに

ドメイン名は Web サイトの URL やメールアドレスの一部として広く使われている．登録されるドメイン名の数は毎年増加しており，2019 年第 1 四半期には 3 億 5,000 万件以上のドメイン名が登録されている [1]．ただし，登録されたドメイン名すべてが即座に Web サイトやメールアドレスのドメイン名として利用されるわけではない．このような利用方法のないドメイン名を対象としたドメインパーキングというサービスが存在する．具体的には，登録したドメイン名をドメインパーキングを提供する事業者（以後，パーキング事業者と表記）に預ける．パーキング事業者は，そのドメイン名へのアクセスに対し専用の Web サイトで広告を掲載・表示する．ユーザへの広告表示やユーザの広告クリックによって広告報酬が発生する．パーキング事業者に預けたドメイン名の登録者はその報酬を獲得することができる．ドメインパーキングは，数百万ドルの収益をあげる活気のあるビジネスとなっている [2]．

サイバー攻撃に利用されるドメイン名が攻撃の後にドメインパーキングを利用する事例 [3] が知られているが，ド

[1] 早稲田大学
Waseda University
[2] NTT セキュアプラットフォーム研究所
NTT Secure Platform Laboratories
[a)] cs5943vgn@toki.waseda.jp

メイン名がドメインパーキングにより管理される期間と，悪性活動に利用される期間との関係についての詳細は明らかになっていない．そこで本稿では，ドメインパーキングを利用するドメイン名について，ドメイン名が一度登録されてから失効するまでの間，さらに一度失効したドメイン名の場合は再登録が発生した前後においての，悪性利用とドメインパーキングの期間やその前後関係といった時間的な関係を大規模データセットを利用して調査する．具体的には，過去 19 ヶ月間にドメインパーキングを利用した実績のある合計 6,680 万件のドメイン名に対する大規模実態調査を行った．これは先行研究 [4] と比べて約 8 倍の規模のドメイン名のデータセットである．その結果，これまで先行研究 [3] では報告されていない，ドメインパーキング利用後に悪性利用されるという特徴的な時系列的なパターンをもつドメイン名を発見した．ドメイン名が登録されてから失効するまでの間にこのパターンが観測されたドメイン名は 3,964 件あり，さらにドメイン名が一度失効し再登録が発生した場合に，再登録の前後でこのパターンが観測されたものは 364 件存在した．また，先行研究では知られていなかった，複数のドメインパーキング事業者を同時あるいは切替えながら利用する 334 万件のドメイン名の存在が明らかになった．本研究の調査により得られたドメインパーキングと悪性利用されたドメイン名の関係は，ドメインパーキングの設定状況の変化を利用した悪性ドメイン名の解析を精度良く実現するために必要な情報である．

本研究の貢献は次の通りである．

(1) ドメインパーキングと悪性利用の時間的な関係に着目した調査を実施した．
(2) ドメインパーキングを利用したことのあるドメイン名 6,680 万件に対する過去最大規模の調査を実施した．これは先行研究 [4] と比べて約 8 倍の規模である．
(3) 先行研究 [3] では知られていない，パーキング後に悪性利用されるドメイン名を発見した．
(4) これまで知られていない複数パーキング事業者を同時あるいは切替えながら利用するドメイン名を発見した．

2. ドメインパーキング

2.1 概要

ドメインパーキングは，利用していないドメイン名をパーキング事業者に一時的に預けるサービスである．ドメインパーキングで表示されるページには様々な種類が存在する．例えば，「このドメイン名は販売中」という趣旨のページや，広告を多数表示するページや，他のページにリダイレクトさせるページが存在する．本稿では，特に広告表示やリダイレクトにより収益を得ることを目的としたものに焦点を当てる．これは，悪性利用されるドメイン名は主に収益化を目的としてドメインパーキングを利用するからである [3]．

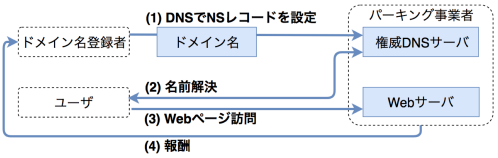

図 1　ドメインパーキングの仕組み

2.2 ドメインパーキングの仕組み

ドメインパーキングは，ドメイン名の名前解決先をパーキング事業者の権威 DNS サーバに向けることで行われる．具体的な手順を**図 1** を用いて説明する．ドメイン名登録者は，図 1 の（1）に示すようにドメイン名の NS レコードをパーキング事業者の指定する権威 DNS サーバに設定する．ユーザが当該ドメイン名へアクセスする場合には，図 1 の（2）に示すように DNS 名前解決の際にパーキング事業者の Web サーバの IP アドレスが得られ，ユーザはパーキング事業者の Web サーバへアクセスすることになる．ユーザが図 1 の（3）に示すようにパーキング事業者が用意した Web ページを訪問し，オンライン広告の表示や広告クリック，そして別のサイトへのリダイレクトを行うことで広告報酬が発生する．生じた広告報酬は，図 1 の（4）のようにドメインパーキングサービスを利用するドメイン名登録者に還元される．

2.3 ドメインパーキングと悪性活動との関係

サイバー攻撃に利用されるドメイン名が攻撃の後にドメインパーキングを利用する事例が知られている [3], [5], [6]．例えば，悪性 Web サイトのインフラとして利用される Traffic Distribution System (TDS) [3] や，マルウェアが利用する Domain Generation Algorithm (DGA) [5] や，ユーザのタイプミスによるアクセスを誘うタイポスクワッティング [6] で用意されるドメイン名が攻撃で利用された後にドメインパーキングを利用する事例が報告されている．このような事例でドメインパーキングが利用される理由は，マルウェア感染端末やユーザからのアクセスが一定数期待でき，そこから広告報酬を得られるためである．

3. 調査手法

本研究では，ドメインパーキングを利用したことのあるドメイン名の大規模な時系列情報の調査を実施する．調査手法の概要を**図 2** に示す．本調査の主要なアイデアは 2 つある．1 つは，ドメイン名とその悪性利用の時系列変化を，ドメインパーキングの設定状況の変化という新たな視点を通じて解析を試みることである．もう 1 つは，上述の解析を具現化するために，大量の DNS データからドメインパーキングを利用したことのあるドメイン名を網羅的に抽出し，さらにドメイン名登録情報やドメイン名のブラックリストの時系列変化を利用することで，ドメインパーキ

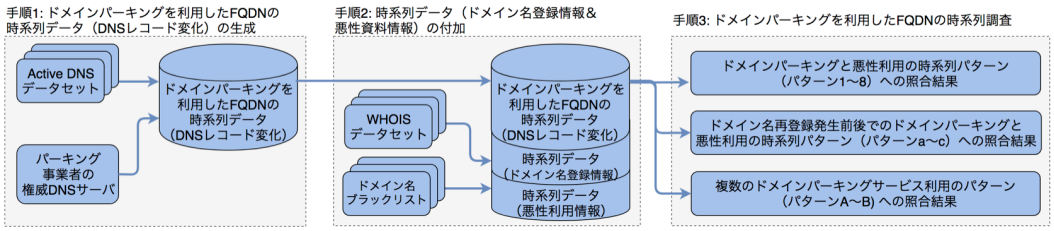

図 2　調査手法概要

ングと悪性利用の時間的な関係を調査することである．本調査は 3 つの手順で行う．この手順の説明に先立ち，以下ではまず，利用したデータセットの詳細を説明する．その後，調査の各手順について説明する．

3.1　データセット

本調査ではドメインパーキングを利用したことのあるドメイン名とその悪性利用の時間変化を網羅的に調査するために 4 種類のデータセットを利用する．以後，各データセットの詳細を説明する．

（1）パーキング事業者の権威 DNS サーバリスト：2.2 節で説明した通り，ドメインパーキングサービスを利用するドメイン名は NS レコードとしてパーキング事業者のもつ権威 DNS サーバを指定する．すなわち，ドメインパーキングを利用したことのあるドメイン名を特定するには，ドメイン名が指定していた NS レコードの e2LD (effective second-level domain) が，パーキング事業者が持つ専用の権威 DNS サーバの e2LD と一致するかを見れば良い．なお，e2LD とはユーザが登録可能なドメイン名の最小単位 (e.g., `example.co.jp`) のことを指す [7]．e2LD の抽出には Mozilla Foundation が提供する Public Suffix List [8] を利用した．ドメインパーキング用の権威 DNS サーバは，先行研究 [4] と同様にドメイン名の市場調査や代表的な検索エンジンでの調査に基づき手動で特定する．2015 年時点の先行研究 [4] では 15 個のドメインパーキングサービスしか対象としていないが，一方本研究では，現時点で有効なドメインパーキングサービス用の権威 DNS サーバとして**表 1** に示す 17 個を特定した．

（2）Active DNS データセット：本調査を進めるにあたり，あるドメイン名とその NS レコードの組合せのデータを大量，かつ，現時点だけでなく過去にさかのぼって入手する必要がある．一般にこのようなデータは Passive DNS あるいは Active DNS の 2 種類のアプローチで収集することができる [9]．Passive DNS はある大規模ネットワークで収集する DNS クエリと DNS レスポンスを受動的に収集するアプローチである．また，Active DNS はあらゆる手法で集めたドメイン名リストをもとに能動的に DNS クエリを送出し，DNS レコードを収集するアプローチである．本研究では，入手の容易性の観点で Active DNS のアプローチを選択し，ドメイン名とその NS レコードを収集した．具体的には，Project Sonar で公開されている Forward DNS [10] のデータセットを 2017 年 11 月から 2019 年 5 月までの 19 ヶ月分収集し利用した．収集したデータには 1 ヶ月分で約 29 億件の DNS レコードが含まれており，これは先行研究 [4] で利用した 2 年分の DNS レコード 2.5 億件の約 12 倍である．今回実際に利用した FQDN の数は 16 億件（重複なし）であり，そのうち e2LD の数は 2.1 億件（重複なし）である．

表 1　パーキング事業者の権威 DNS サーバ

パーキング事業者	権威 DNS サーバの e2LD
Above	`above[.]com`
Afternic	`afternic[.]com`
Bodis	`bodis[.]com`
CashParking	`cashparking[.]com`
DomainApps	`domainapps[.]com`
DomainSponsor	`dsredirection[.]com`
Fabulous	`fabulous[.]com`
InternetTraffic	`internettraffic[.]com`
NameDrive	`fastpark[.]net`
ParkingCrew	`parkingcrew[.]net`
ParkLogic	`parklogic[.]com`
RookMedia	`rookdns[.]com`
SedoParking	`sedoparking[.]com`
Skenzo	`ztomy[.]com`
The Parking Place	`pgl[.]net`
TrafficZ	`trafficz[.]com`
Voodoo	`voodoo[.]com`

（3）WHOIS データセット：ドメイン名の登録情報やその変化を調査するために WHOIS のデータセットを用意する．本研究では，ある商用サービスで入手した大規模 WHOIS データセットを利用する．具体的には，全登録ドメイン名のデータを 2018 年 6 月，2018 年 9 月，2018 年 12 月，2019 年 3 月の合計 4 回入手し，本調査に利用する．

（4）ドメイン名ブラックリスト：サイバー攻撃に関与したドメイン名かどうかを調査するために，ドメイン名のブラックリストを利用する．本研究の調査では，ドメインパーキングを利用したことのあるドメイン名がどのように攻撃で悪性利用されてきたのかという時系列調査を行うため，ドメイン名のブラックリストには，正確な悪性根拠情報が付与されていることと，過去から現在までさかのぼった調査が可能なこと，という要件が必要である．上記の要件を満たすブラックリストとして，ある商用のブラックリストと，公開ブラックリストである hpHosts [11] の 2 種類を数年間継続的に収集した独自データを利用する．この 2 種類の

ブラックリストはそれぞれ収集や検知の仕組みが異なるため，併用することでより偏りなく調査することが可能になる．また，攻撃種別（例．マルウェア，フィッシング）が明らかになっている悪性ドメイン名を選定した．さらに，ブラックリストに誤って正規のドメイン名が混在するリスクを排除するため，代表的なトップサイトである Alexa Top Sites [12] を参照し，過去 1 年以内に上位 10 万位以内に掲載されていたものを除外した．なお，サイバーセキュリティ研究でよく参照される VirusTotal [13] や Google Safe Browsing [14] は，調査時点の最新結果は容易に入手できるものの，今回の調査の主な目的である時系列情報の入手が困難であるためブラックリストとしては採用しない．

3.2 手順 1

手順 1 では，3.1 節で収集した（1）パーキング事業者の権威 DNS サーバリストと（2）Active DNS データセットを利用し，ドメインパーキングを利用したことのあるドメイン名を網羅的に抽出する．まず，19 ヶ月分の Active DNS データセットに含まれる FQDN と NS レコードの組合せに対し，パーキング事業者の権威 DNS サーバリストと照合する．その結果，19 ヶ月分の期間内に一度でもドメインパーキングサービスを利用したことのある FQDN を抽出することができる．本研究では，ドメインパーキングを利用した時点だけでなく，その前後の時間変化まで詳細に調査するのが目的であるため，次に抽出された FQDN をもとに再度 Active DNS データセットを走査し，一度でもドメインパーキングサービスを利用した FQDN を対象に 19 ヶ月間の DNS レコードの変化を記録した時系列データを生成する．これによって各 FQDN がどの時点でドメインパーキングを利用していたかを把握する．

3.3 手順 2

手順 2 では，手順 1 で作成した過去にドメインパーキングサービスを利用したことのあるドメイン名の時系列データに次の 2 種類の情報を付加する．

ドメイン名登録情報：3.1 節で収集した（3）WHOIS データセットを利用し，ドメイン名の登録日を抽出し，当該ドメイン名が登録された時期を特定し付与する．

悪性利用情報：3.1 節で収集した（4）ドメイン名ブラックリストを参照し，当該ドメイン名が悪性利用されていたかどうか，悪性利用の期間はいつからいつまでかを特定し付与する．

3.4 手順 3

手順 3 では，上記の手順 1 と 2 で作成した時系列データを用いて，ドメイン名のパーキング事業者の利用と悪性利用の時系列的な関係を調査する．具体的には，下記の節に各々示す 3 つの観点での時系列調査を行う．調査の粒度は，手順 1，2 で作成したドメイン名に関する時系列データと同じ，1 ヶ月単位である．先行研究 [2], [4] では調査時点でドメイン名がドメインパーキングを利用していたかどうかを調査しているのに対し，本研究はその時間変化まで観測・解析を行う点が大きく異なる．なお，このような複数の観点の時間変化パターンを詳細かつ大規模に調査する研究は，我々の知る限りはじめてである．

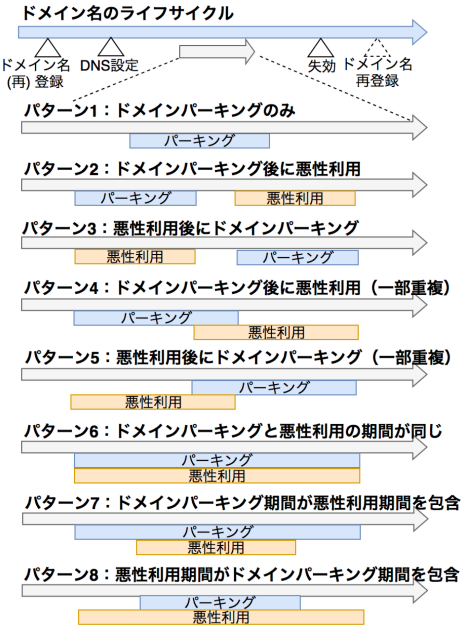

図 3 ドメインパーキングと悪性利用の時系列パターン

3.4.1 ドメインパーキングと悪性利用の時系列変化

本研究では，ドメイン名がパーキング事業者に預けられていた期間と攻撃に利用されていた期間の関係を**図 3** に示す 8 個の時系列パターン（パターン 1〜8）に分類することを提案する．これらのパターンは，ドメイン名が登録されてから失効するまでのライフサイクルにおいて，ドメインパーキングと悪性利用で考えうるすべての時系列パターンである．それぞれの時系列パターンを順に説明する．

パターン 1：ドメインパーキングのみ利用し，悪性利用されない．

パターン 2：ドメインパーキングを利用した後，期間をあけて悪性利用される．

パターン 3：悪性利用された後，期間をあけてドメインパーキングが利用される．

パターン 4：ドメインパーキングを利用した後，終了する前に悪性利用も始まり部分的に期間が重複する．パーキング事業者に預けられている間にブラックリストに入ったということは，パーキング事業者の Web サイトに表示されていた広告ページやリダイレクトの遷移先が悪性だった可能性がある．

パターン 5：悪性利用が始まった後，終了する前にドメインパーキングの利用も始まり部分的に期間が重複する．悪

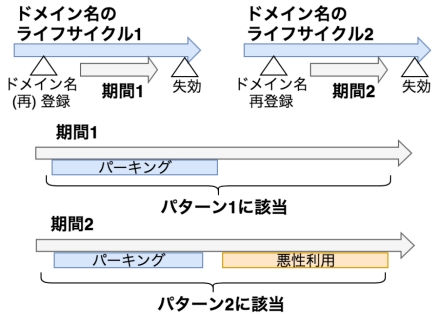

図 4　ドメイン名再登録が発生する場合の時系列パターン例

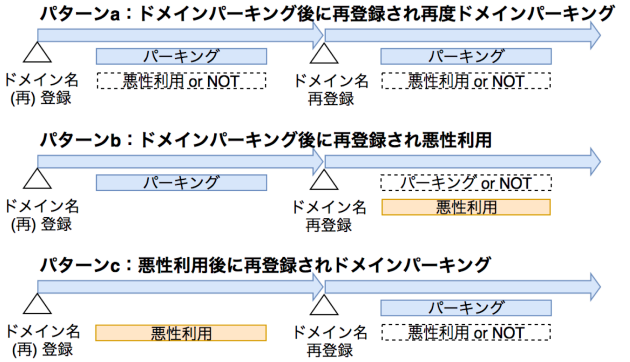

図 5　ドメイン名再登録発生前後でのドメインパーキングと悪性利用の時系列パターン

性利用の途中からパーキング事業者へ預け始めたということは，悪性利用が実質的に終了しているにもかかわらずブラックリストへの反映が遅れているか，悪性利用をされた後に，悪性な広告の表示やリダイレクト先への誘導を行なうパーキング事業者に預けられた可能性がある．

パターン 6：ドメインパーキングを利用する期間と悪性利用の期間が同じ．パーキング事業者が表示させる広告や誘導するリダイレクト先が悪性なものだったか，再登録される前の過去の悪性利用でブラックリストに入り，悪性利用が終わった後もブラックリストに反映されず残り続けている可能性がある．

パターン 7：ドメインパーキングを利用する期間が悪性利用の期間を包含する．パーキング事業者が表示させた広告や誘導したリダイレクト先がたまたま悪性なもので，預けられたドメイン名がブラックリストに入ったが，悪性な広告の表示やリダイレクト先の誘導がそのあとされず，後にブラックリストから除外されたと考えられる．

パターン 8：悪性利用の期間がドメインパーキングの利用期間を包含する．悪性利用が終わった後に，悪性な広告やリダイレクト先へ誘導するパーキング事業者に預けられたか，パーキング事業者に預けられた後も，悪性利用が終わったことがブラックリストに反映されていないことが考えられる．

なお，本調査の 19 ヶ月の観測期間内に，ドメイン名が失効し再登録される場合がある．その場合，ドメイン名の登録から失効までのライフサイクルが複数回存在することになるため，上記のパターンも複数回存在する観測されることになる．例えば，**図 4** に示す状況が観測された場合，あるドメイン名に対し，期間 1 と期間 2 でそれぞれでパターン 1 と 2 という計 2 個のパターンを観測することになる．

3.4.2　ドメイン名再登録発生前後でのドメインパーキングと悪性利用の時系列変化

また，本研究では，ドメイン名が失効された後に第三者に取得されるドロップキャッチがサイバー攻撃で多用されている事実 [15], [16], [17] を鑑み，ドメイン名の再登録が発生したドメイン名については，その前後のパターンの変化を**図 5** に示す 3 個の時系列パターン（パターン a〜c）に分類してさらに調査する．前節の時系列パターンがある一度のドメイン名の登録から失効までのライフサイクルを対象としているのに対し，本節では再登録の前後にどのように変化するかを調査する点が異なる．なお，1 つのドメイン名が複数回の再登録が行われた場合，それらを複数の別々のパターンとして認識する．それぞれのパターンの詳細は次の通りである．

パターン a：ドメインパーキングを利用したドメイン名が失効して再登録された後，再度ドメインパーキングを利用するパターン．悪性利用の有無は問わない．

パターン b：ドメインパーキングされたドメイン名が失効して再登録された後，悪性利用されるパターン．再登録後のドメインパーキングの有無は問わない．

パターン c：悪性利用されたドメイン名が失効して再登録された後，ドメインパーキングを利用するパターン．再登録後の悪性利用の有無は問わない．

3.4.3　複数のパーキング事業者を利用するドメイン名の時系列変化

さらに本研究では全 19 ヶ月の調査期間を 1 ヶ月単位で解析する際に，複数回パーキング事業者に預けられるドメイン名や預けられたパーキング事業者の種類，その変化についても調査する．なお，パーキング事業者の区別は，ドメイン名に設定された権威 DNS サーバの e2LD を見て行なっている．例として，`ns1.parking1.example` と `ns2.parking1.example` なら同じパーキング事業者，`ns1.parking2.example` のように e2LD が異なる場合は異なるパーキング事業者と判断する．

複数のパーキング事業者の利用のパターンは，**図 6** に示す 3 通りが考えうる．これは複数のパーキング事業者の利用の全パターンを網羅している．

パターン A：観測期間中に複数種類のドメインパーキングサービスを利用していたドメイン名

パターン B：パターン A の中で，同時期に複数のドメインパーキングサービスを利用していたドメイン名

パターン (A ∧ ¬ B)：パターン A の中で，同時期に複数

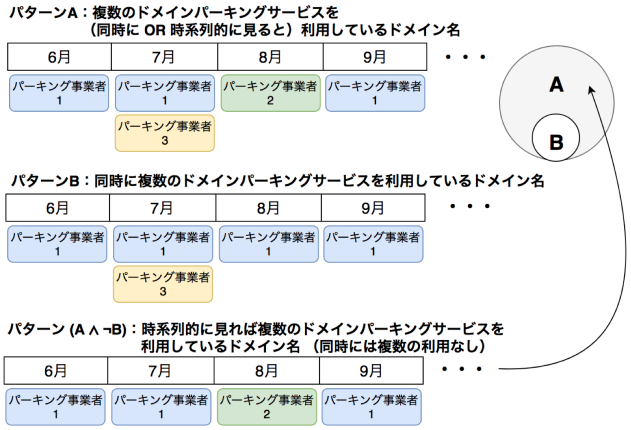

図 6　複数のパーキング事業者利用のパターン

表 2　ドメインパーキングを利用したことのあるドメイン名の各ブラックリストとの照合結果

ブラックリスト名	FQDN 件数	e2LD 件数
商用ブラックリスト	235,746 (0.35%)	8,037 (0.06%)
hpHosts	267,704 (0.40%)	23,478 (0.16%)
合計	432,811 (0.65%)	29,636 (0.20%)

のドメインパーキングサービスを利用していなかったドメイン名．

まずパターン A に当てはまるドメイン名を抽出し，ブラックリストを参照して悪性利用について調査した．さらにそのサブセットのパターン B をより詳細に調査した．具体的には，調査時点での VirusTotal [13] の掲載情報を調査し，さらにドメイン名に実際にアクセスして，どのようなページが表示されるかを調査した．

4. 調査結果

3 節で示した手法に基づく調査結果を順に説明する．

4.1 調査対象ドメイン名の概要

今回の調査対象である観測期間中にパーキング事業者に預けられたことのあるドメイン名について説明する．3.2 節の手順 1 を実行した結果，過去にドメインパーキングを利用したことのあるドメイン名は，FQDN 単位で 6,680 万件，e2LD 単位で 1,450 万件存在した．この調査対象件数はパーキングの調査を行っている先行研究 [4] に比べて 8 倍以上多いだけでなく，その時系列変化まで以後詳細に調査する点が本研究の特長である．次に，調査対象のドメイン名に対し 3.3 節の手順 2 を実行し，2 つのブラックリストとの一致数を FQDN 単位と e2LD 単位で集計した件数と調査対象件数に対する割合を**表 2** に示す．なお，e2LD（例．`example.com`）を共有する複数の FQDN（例．`www.example.com`）が存在するため FQDN と e2LD 件数に差異がある．悪性ドメイン名である割合は全体の 1%未満と高くないことがわかるが，件数としては FQDN 単位で 43 万件，e2LD 単位で 2.9 万件以上の大規模データである．

表 3　図 3 の時系列パターンへの該当ドメイン名数

パターン	FQDN 件数	e2LD 件数
パターン 1	215	148
パターン 2	1,477	704
パターン 3	84,329	3,291
パターン 4	2,487	1,086
パターン 5	23,022	1,543
パターン 6	5,916	2,891
パターン 7	47,885	1,344
パターン 8	245,388	10,475

4.2 ドメインパーキングと悪性利用の時系列変化の調査

3.4.1 節で説明した，ドメイン名が登録されてから失効するまでの間のドメインパーキングと悪性利用の時系列パターンを調査する．具体的には，前節の調査対象ドメイン名に対し，図 3 に示した時系列パターン（パターン 1〜8）への該当状況を調査する．調査結果を FQDN 単位と e2LD 単位で集計した結果を**表 3** に示す．今回定義したすべての時系列パターン（パターン 1〜8）に該当するドメイン名が確認された．最も特筆すべきことは，これまで先行研究 [3] では報告されていない，ドメインパーキング利用後に悪性利用されるという特徴的な時系列的パターン（パターン 2，4）をもつドメイン名を計 3,964 件発見したことである．これは現在ドメインパーキングを利用しているドメイン名が，今後悪性利用される候補として継続的に検査する価値があり，またその特性を他の悪性ドメイン名解析技術に応用可能であることを示している．また，本調査では先行研究 [3] で報告された，悪性利用後にドメインパーキングされる時系列パターン（パターン 3，5）が計 107,351 件存在することも確認できた．これは本調査手法が先行研究と同様に妥当なものであることを示すと同時に，2013 年時点で報告されていた傾向が 2017 年から 2019 年の最新時点でも継続していることを示している．パターン 6〜8 の結果については，上記で言及したパターン 2〜5 と比べると比較的長期にわたりドメインパーキングと悪性利用が観測されるものである．この結果は，今回利用したブラックリスト（3.1 節参照）が，すでに実質的に攻撃に利用されていないドメインパーキングに預けられてるドメイン名であってもブラックリストとして掲載され続けている可能性や，マルウェア感染端末からの該当ドメイン名へのアクセスが継続しておりブラックリスト提供者による悪性判定が継続している可能性があることを示している．

4.3 ドメイン名の再登録発生前後でのドメインパーキングと悪性利用の時系列変化の調査

3.4.2 節で説明したドメイン名の再登録発生の前後での時系列変化を調査する．具体的には，図 5 に示した時系列パターン（パターン a〜c）への該当状況を調査する．調査結果を**表 4** に示す．まず，再登録前にドメインパーキングを利用していて，再登録後に再度ドメインパーキングをするパターン a に該当する FQDN が 29 万件以上観測された．

表 4　図 5 の時系列パターンへの該当ドメイン名数

パターン	FQDN 件数	e2LD 件数
パターン a	293,934	122,926
パターン b	475	388
パターン c	81,149	4,918

なお，このような複数回ドメインパーキングを利用するドメイン名の存在に着目した調査結果は次節で示す．次に，再登録前にドメインパーキングを利用していて，再登録後に悪性利用されるパターン b に該当する FQDN は 475 件存在することを発見した．これは現在ドメインパーキングを利用しているドメイン名が一度失効して再登録された場合に，今後悪性利用される候補として利用可能であることを示している．最後に，再登録前に悪性利用していて，再登録後にドメインパーキングを利用するパターン c に該当する FQDN を 8 万件以上特定した．これはマルウェア感染端末からのある程度のアクセス数を見込める悪性ドメイン名が再登録されドメインパーキングで収益化を行っているという先行研究 [3] の報告を裏付ける結果である．

4.4　複数のパーキング事業者を利用するドメイン名の時系列変化の調査

3.4.3 節で説明した，複数のパーキング事業者の利用を調査する．具体的には，図 6 に示したパターン（パターン A・B）への該当状況を調査する．調査の結果を**表 5** に示す．この調査結果で最も特筆するべきことは，先行研究では知られていなかった，パターン A に該当する複数のパーキング事業者を同時あるいは切替えながら利用する FQDN が 334 万件も存在するという事実が判明したことである．また，上記のうち同時期に複数のパーキング事業者を利用するパターン B に限定すると 829 件の FQDN が特定された．このような複数のパーキング事業者を利用する理由として，広告表示による収益の最適化を試みている可能性がある．例えば，モバイルアプリに表示される広告に関する先行研究 [18] では，収益の最適化のため複数の広告ネットワークを切替えている事例が報告されている．

表 5 に示したドメイン名に対し，FQDN 単位と e2LD 単位でブラックリストと照合した結果を**表 6** に示す．パターン A については各々のブラックリストで数千件の一致したものが存在した．一方で，パターン A の部分集合であるパターン B についてはそれぞれ 1 件しか存在しなかった．

パターン B に該当する同時期に複数のパーキング事業者を設定していた特徴的なドメイン名についてより詳細に解析した結果を報告する．まず，829 件の FQDN を対象に VirusTotal [13] の結果を参照した．その結果，VirusTotal に含まれる 60 種類以上の検知エンジンのうち 1 種類以上が悪性判定した FQDN が 47 件存在した．この 47 件の FQDN について実際に Web ブラウザでアクセスを行い，現時点の Web サイトや内容を手動で調査・分類した．分類結果を**表 7** に示す．調査時点でドメインパーキングを利用していたものが計 39 件存在し，広告やリダイレクトやドメイン名売買仲介といった収益目的の Web サイトに到達することが確認できた．

表 5　図 6 のパターンへの該当ドメイン名数

パターン	FQDN 件数	e2LD 件数
パターン A	3,342,028	1,551,815
パターン B	829	829

表 6　複数のパーキング事業者に預けられたドメイン名のブラックリスト照合結果

パターン	商用ブラックリスト	hpHosts
パターン A（FQDN）	2,865	7,744
パターン A（e2LD）	1,011	2,948
パターン B（FQDN）	1	1
パターン B（e2LD）	1	1

表 7　図 6 のパターン B に該当し VirusTotal で悪性判定された FQDN の分類結果

結果	FQDN 件数
ドメインパーキング（広告）	20
ドメインパーキング（リダイレクト）	11
ドメインパーキング（ドメイン名売買仲介）	8
応答なし	6
非悪性サイト	1
不明	1
合計	47

4.5　制約

本研究で実施した調査に関する制約が 2 つ存在する．1 つ目は，Dynamic DNS に代表されるような複数の異なるユーザが共通の e2LD を使う FQDN がドメインパーキングを利用する場合には正しく時系列パターンを特定できないという制約である．これはそもそもドメイン名の登録日は e2LD 単位であり，Dynamic DNS のサービス自体の e2LD の登録日しか得られないためである．2 つ目は，本研究で利用した Active DNS データセットにおいて，時期やタイミングによってあるドメイン名に対応する NS レコードが欠損する場合があり，その場合に正しく時系列パターンを特定できないという制約である．例えば，3 月，4 月，6 月にはある同一のパーキング事業者の NS レコードが記録されているが，5 月には NS レコードが欠損する場合がある．今回の調査では，このような欠損するデータについては，欠損する時期の前後で同一のデータである場合には，欠損していた時期にも同じパーキング事業者を利用していたとみなして処理を行った．

5.　関連研究

関連研究はドメインパーキングを主に解析している研究と，多様な悪性ドメイン名を主に解析し副次的にドメインパーキングを言及している研究に大別できる．

ドメインパーキング解析：文献 [4] は，ドメインパーキングを利用する 800 万件のドメイン名のデータから 3,000 件をランダムサンプリングしてドメインパーキングのエコシ

ステムの詳細な解析を行っている．また，ドメインパーキングを利用しているドメイン名にアクセスするとマルウェアやオンライン詐欺につながるリスクがあることを明らかにしている．我々の研究は，文献 [4] よりも大規模な合計 6,680 万件のドメインパーキングを利用する FQDN のすべてを対象に解析し，さらにその時系列変化までみている点で大きく異なる．また，文献 [2] では，ドメインパーキングで表示される広告や収益化の観点で解析を行っている．特に，23 個のドメイン名を研究者自らが購入し，そのドメイン名へのクローリングやトラヒック観測を行う能動的な手法により，広告不正やトラヒックスパムの存在を明らかにしている．我々の研究は，研究倫理の観点で受動的な観測のみを利用し，また非常に大規模かつ時系列解析を行っている点で大きく異なる．

悪性ドメイン名解析：文献 [3] では，悪性 Web サイトのインフラとしても利用される Traffic Distribution System (TDS) とドメインパーキングの実態調査が行われており，TDS の半数はドメインパーキングを利用することが解明されている．また，文献 [5] は，マルウェアやボットネットに利用される 43 種類のドメイン名生成アルゴリズム (DGA) で生成された 1,800 万件のドメイン名に対する調査を行っており，そのうち 6,458 件のドメイン名が調査時点でドメインパーキングを利用している実態を示している．文献 [6] は，ユーザのタイプミスを狙うタイポスクワッティングと呼ばれる種類のドメイン名についての調査を行う中で，ドメインパーキングを利用しているものも特定している．さらに，文献 [7] は，様々な種別の悪性ドメイン名に対し，そのドメイン名の特性を考慮した対策を決定する手法を提案しており，その中でドメインパーキングを一つの種別として識別し，そのような悪性ドメイン名に対する対策方法を議論している．上記いずれの研究とも異なり，我々の研究では特定の悪性用途やドメイン名の種別を限定せずドメインパーキングを利用するドメイン名を大規模に調査し，パーキングと悪性利用との時間的関係をみて，先行研究 [3] で報告されていた逆の順，つまりドメインパーキング利用後に悪性利用されるドメイン名を確認したほか，複数のパーキング事業者を利用するドメイン名が存在することを明らかにした．

6. まとめ

本稿では，ドメインパーキング利用と悪性活動の時系列パターンの調査を行った．過去 19 ヶ月間にドメインパーキングを利用した実績のある合計 6,680 万件のドメイン名を対象にした大規模実態調査を行った結果，先行研究では報告されていない，ドメインパーキング利用後に悪性利用されるという特徴的な時系列パターンをもつドメイン名や，複数のドメインパーキング事業者を同時あるいは切替えながら利用するドメイン名の存在を明らかにした．本研究の調査結果は，ドメインパーキングの特性を利用した悪性ドメイン名解析へ貢献することが期待できる．

謝辞　本研究の一部は，日本学術振興会における科学研究費補助金基盤研究（C）（課題番号 17K00135）による支援を受けている．ここに記し謝意を表す．

参考文献

[1] Verisign: Domain Name Industry Brief (DNIB), https://www.verisign.com/en_US/domain-names/dnib/index.xhtml.
[2] Alrwais, S. A., Yuan, K., Alowaisheq, E., Li, Z. and Wang, X.: Understanding the Dark Side of Domain Parking, *Proc. USENIX Security* (2014).
[3] Li, Z., Alrwais, S. A., Xie, Y., Yu, F. and Wang, X.: Finding the Linchpins of the Dark Web: a Study on Topologically Dedicated Hosts on Malicious Web Infrastructures, *Proc. IEEE S&P* (2013).
[4] Vissers, T., Joosen, W. and Nikiforakis, N.: Parking Sensors: Analyzing and Detecting Parked Domains, *Proc. NDSS* (2015).
[5] Plohmann, D., Yakdan, K., Klatt, M., Bader, J. and Gerhards-Padilla, E.: A Comprehensive Measurement Study of Domain Generating Malware, *Proc. USENIX Security* (2016).
[6] Agten, P., Joosen, W., Piessens, F. and Nikiforakis, N.: Seven Months' Worth of Mistakes: A Longitudinal Study of Typosquatting Abuse, *Proc. NDSS* (2015).
[7] Chiba, D., Akiyama, M., Yagi, T., Hato, K., Mori, T. and Goto, S.: DomainChroma: Building actionable threat intelligence from malicious domain names, *Computers & Security* (2018).
[8] Mozilla Foundation: Public Suffix List, https://publicsuffix.org/list/.
[9] Kountouras, A., Kintis, P., Lever, C., Chen, Y., Nadji, Y., Dagon, D., Antonakakis, M. and Joffe, R.: Enabling Network Security Through Active DNS Datasets, *Proc. RAID* (2016).
[10] Rapid7 Open Data: Forward DNS (FDNS), https://opendata.rapid7.com/sonar.fdns_v2/.
[11] Malwarebytes: hpHosts, https://hosts-file.net/.
[12] Alexa Internet, Inc.: Alexa Top sites, https://www.alexa.com/topsites.
[13] VirusTotal: VirusTotal, https://www.virustotal.com/.
[14] Google: Google Safe Brawsing, https://developers.google.com/safe-browsing/.
[15] Hao, S., Kantchelian, A., Miller, B., Paxson, V. and Feamster, N.: PREDATOR: Proactive Recognition and Elimination of Domain Abuse at Time-Of-Registration, *Proc. ACM CCS* (2016).
[16] Lever, C., Walls, R. J., Nadji, Y., Dagon, D., McDaniel, P. D. and Antonakakis, M.: Domain-Z: 28 Registrations Later Measuring the Exploitation of Residual Trust in Domains, *Proc. IEEE S&P* (2016).
[17] Lauinger, T., Onarlioglu, K., Chaabane, A., Robertson, W. and Kirda, E.: WHOIS Lost in Translation: (Mis)Understanding Domain Name Expiration and Re-Registration, *Proc. ACM IMC* (2016).
[18] Mhaidli, A. H., Zou, Y. and Schaub, F.: "We Can't Live Without Them!" App Developers' Adoption of Ad Networks and Their Considerations of Consumer Risks, *Proc. SOUPS* (2019).