The Possibility of Guessing Open Ports from the Subdomain Name

サブドメイン名を用いた開放ポート推測可能性の検証

坂田 拓美[*]　小高 知宏[**]　黒岩 丈介[**]
諏訪 いずみ[***]　白井 治彦[****]

The Possibility of Guessing Open Ports from the Subdomain Name

Takumi SAKATA[*], Tomohiro ODAKA[**], Jousuke KUROIWA[**],
Izumi SUWA[***] and Haruhiko SHIRAI[****]

(Received January 31, 2022)

Today, any information which is available on the internet is often used to attack servers by attackers. DNS is one of the information sources which are used by them.

We propose a new possibility of guessing open ports from only the subdomain name. Subdomain name is a name for hosts, often named after the service running on them. It potentially means the name contains the information about running services which can help attackers to know how to intrude into the target server before sending out any packets to it.

In this paper, we examined the possibility with statistical data and machine learning. We used fastText as machine learning model to learn linguistic relations between subdomain name and open ports.

As a result, we find it possible to guess open ports from subdomain name by using machine learning.

Key words : DNS, Subdomain, Cybersecurity, Internet, Machine Learning

1. 緒言

昨今では，インターネット上の様々な情報が収集され，多種多様な目的に利用されている．インターネットを介して誰もが情報の発信者となることが可能となった情報化社会においては，これらの情報を元に生成される新たな情報は高い精度で現実世界を反映したものとなりえる．

インターネットを利用した情報収集の中でも，一般に公開された情報をもとにして目的とする情報を収集・分析する手法を OSINT (Open Source Intelligence) と呼ぶ.[1] 今日，OSINT はサイバーセキュリティにおいて重要視されており [2]，悪意のある攻撃者とシステム管理者のどちらもが積極的に活用している．

ドメイン名に関する情報も OSINT として利用できる場合がある．現在 DNS（Domain Name System）における OSINT としては，サブドメインをリストアップすることによる稼働マシンのリストアップや，whois 情報が一般的となっている.[3] しかし，これら以外にも利用方法がある可能性が考えられる．

そこで新たな情報として，サブドメインから対象サーバで稼働中のサービスを推定し，攻撃手法の選別に用

[*]大学院工学研究科 知識社会基礎工学専攻
[*]Fundamental Engineering for Knowledge-Based Society, Graduate School of Engineering
[**]知能システム工学講座
[**]Department of Human and Artificial Intelligent Systems
[***]仁愛女子短期大学 生活科学学科
[***]Jin-ai Women's College
[****]工学部 技術部
[****]Technical Division, School of Engineering

いられてしまう可能性を考える．本研究の目的は，サブドメインとサービスに関連の深い開放ポートの間に，推定可能な関係性が存在するか検証することである．本論文ではいくつかの手法で検証した結果について検討を行う．

2. 研究背景

DNS とはインターネットを利用する上で欠くことのできない仕組みのひとつである．しかし，DNS リフレクション攻撃など，DNS を悪用した攻撃手法が度々使用されていることが確認されている [4]．本章では，DNS や OSINT について述べた後に，本論文で警鐘する新たな DNS 悪用手法について述べる．

2.1 DNS の現状

本節では，DNS の利用状況と DNS がどのような攻撃に利用されているのかについて述べる．

2 つの DNS ルートサーバを管理している Verisign によると，すべての TLD に登録されているドメイン名の総数は 2021 年の 6 月末時点で 3.67 億個を超えている [5]．Web サイトを代表として，多種多様な利用がされている現代のインターネットは，数多くのサーバによって成り立っている．それらのサーバに対してドメイン名が割り当てられ管理されることで，DNS が扱うドメイン名は膨大な数へと成長した．

また，DNS が考案された当初の目的であったサーバへアクセスする際のアドレス管理の簡便化だけでなく，電子メールの送信元認証技術である DMARC[6] や，HTTPS 通信などで用いられる公開鍵証明書の発行を担う認証局の指定を行う CAA[7] などの仕組みが DNS に実装されている．これらの新たな仕組みによって，DNS が扱うデータの種類や影響範囲は拡大している．

より安全なインターネットを実現するための仕組みが，DNS の機能を利用または拡張することにより実装されている．しかし，これによって DNS がインターネットのセキュリティにおける脆弱部となることも考えられる．

2.2 サブドメインからのサービス推測可能性

はじめに，サブドメインについて簡単に述べる．最終的にアクセスを行うホストを表す FQDN は，複数のドメインからなっている．ドメインは階層構造になっており，それらの各ドメイン間は “ . ”(ピリオド) で区切られている．サブドメインは，これら複数あるドメインの中であるドメインの配下につくドメインのことを言う [8]．

例として，“www.example.com” を考える．ドメイン名は右から左へと記述するため，右にあるものがより上位のドメインとなる．最上位となる “com” に注目して見ると，その左にある “example” または “www.example” がサブドメインということになる．つまり，一般にサブドメインは視点によって異なる．しかし，本論文では簡単のため最も左にあるドメインのみをサブドメインとする．

最も左にあるドメインは，特定のホストにつけられたものである．名付けの際には，そのホストが提供する機能や情報に基づいて，管理者または利用者にとって都合の良いものがつけられることが多いと考えられる．これが事実であれば，サブドメインから対応するホストで稼働しているサービスに関する情報を入手できてしまう可能性がある．

あるホストで稼働しているサービスに関する情報を，第三者が取得することそのものについては大きな問題ではない．攻撃者にとって，ターゲットの稼働サービスを調べることは，攻撃前に必ず行わなければならないことである．これは複雑な作業ではなく，ポートスキャンなどを実行することでできる．

サブドメインから稼働しているサービスに関する情報が分かることが問題となる理由は，ターゲットとなるホストに一切のログを残すことなく実行可能という点である．一般的な手法の一つであるポートスキャンでは，ターゲットの各ポートに対して各種パケットを送信することで開放ポートを調べる．ターゲットとなるホストにおけるファイアウォールの設定にもよるが，パケットをターゲットに送信するということは，そういった通信があったというログが残ることになる．管理者は攻撃への対策として，このログをもとにアラートを通知させることや，通信元アドレスのブロックを行うように設定できる．

それに対して，サブドメインからサービスに関する情報を入手する場合には，悪意のある攻撃者は攻撃対象となるホストのサブドメインを入手するだけで，ターゲットとの通信を行う必要がなくなる．サブドメインを入手する際には，攻撃対象である組織が管理する DNS サーバに総当りになどによる列挙が必要になる場合があるが，この通信ログが残るのは DNS サーバであり攻撃対象ではない．また，Passive DNS などのデータベースを用いることで [9]，外部への通信を最小限に抑えることも可能と言える．これらにより，攻撃対象となったホストの管理者は，攻撃を事前に察知しブロックするなどの対策をすることが不可能となる．

以上から，サブドメインからサービスを推測することが可能であった場合，セキュリティ上無視できない

脅威となると言える．本論文では，サブドメインからサービスを推測することが実際に可能であるかどうかを検証し，考察を行なった．

3. 検証方法

本章では，サブドメインからサービスを推測することが可能か検証を行う方法について述べる．

3.1 検証に用いるデータ

まず, 検証に用いるためのデータの準備を行なう．必要なデータは，サブドメインとそれと対応するホストで稼働しているサービスのペアを記録したものである．しかし，これに該当する公開されたデータセットが見つけられなかったため，サービスではなく開放ポートとのペアのデータセットを作成した．

データセットの作成の際に用いたデータは，Rapid7 が Project Sonar の一環として公開している Open Data[10] の一つである，FDNS（Forward DNS）`2021-04-23-1619136719-fdns_a.json` をデータとして用いた．

この FDNS データは，Rapid7 の DNS サーバに対してフォワードされたすべての DNS クエリへの応答が記録されたものである．その中でもクエリタイプが A, つまりドメイン名から IPv4 アドレスの名前解決を行なっているもののみを対象とした．また，利用したデータの対象期間は日本時間で 2021 年 4 月 23 日 09:16:21 から 2021 年 4 月 24 日 06:57:46 である．

このデータから IP アドレスが割り当てられていた FQDN（Fully Qualified Domain Name）のみを抽出し，重複していた FQDN も削除を行なった．こうして作成した FQDN のデータベースを元に，ポートスキャンを行い，各 FQDN とペアとなる開放ポートのデータセットを作成した．

3.2 検証の流れ

本研究では，大きく分けて 2 種の手法を用いて検証を行なう．1 つはサブドメインと開放ポートの統計的なデータを用いた検証である．もう一つは機械学習を用いた検証である．本節では，それぞれの手法について検証を行う際の流れについて述べる．

3.2.1 統計的なデータを用いた検証

この手法では，サブドメインの命名に固有のパターンが存在するのかを確認するため，各サブドメインの出現割合，同一サブドメインの出現頻度分布，重複の有るサブドメインにおけるポート出現率，重複の無いサブドメインにおけるポート出現率を算出する．

各指標の算出方法は表 1 に有るとおりである．各サブドメインの出現割合の算出方法は，各サブドメインの出現総数を対象となる FQDN の総数で割った値となる．また，重複の有るサブドメインにおけるポート出現率と重複の無いサブドメインにおけるポート出現率は，対象となるホストが異なるもので計算式はどちらも条件 (重複の有るサブドメインまたは無いもの) に合うサブドメインにおける全てのポートの総出現回数を条件に合うサブドメインの総数で割った値となる．

表 1 各指標の算出方法

指標	算出方法
各サブドメインの出現割合	$\frac{\text{各サブドメインの出現総数}}{FQDN\ \text{の総数}}$
各ポート出現率	$\frac{\text{各ポートの総出現回数}}{\text{対象サブドメイン総数}}$

また，同一サブドメインの出現頻度分布は，異なる FQDN の中で同一のサブドメインが何回重複して現れるかを数え，各頻度ごとに度数を出したものである．

3.2.2 機械学習を用いた検証

統計データによる検証では，サブドメインを一つのブロックとして捉え，サブドメインの文字列の並びを全く利用していない．そのため，機械学習を用いた手法では，文字列に開放ポートの推測に用いることができる隠れた特徴が存在しないかを確認することを目的としている．

今回，学習ライブラリとして 2016 年に Facebook が公開した fastText を用いた．fastText は，Word2Vec を基に開発された自然言語処理ライブラリであり，入力された単語をベクトル空間にマッピングすることでテキストの分類を行う [11].

学習には, 用意したデータセットを学習データ：検証データ= 4：1 に分割して利用する．また, 単一ホストであっても複数の開放ポートが存在するため，マルチラベル予測を行うためのロス関数である one-vs-all を用いた．fastText には学習時に設定可能なハイパーパラメータは, 学習率とエポック数の 2 つがある．今回，これらのパラメータは学習率=0.05，エポック数=25 とした．

学習後のモデルを用いて評価するための指標には，Precision，Recall，F-measure を用いた．それぞれの計算式は表 2 に記す．ここで，$golds$ は，検証データに含まれるラベルの総数である．

表 2 学習後のモデル評価指標の算出方法

指標	算出方法
Precision	$\frac{truePositives}{truePositives+falsePositives}$
Recall	$\frac{truePositives}{golds}$
F-measure	$\frac{2*precision*recall}{precision+recall}$

サブドメインから開放ポートを推測することが可能となる特徴に，どういったものがあるのかヒントを得るため，用いるデータセットにいくつかのパターンを用意する．用意するパターンは表 3 のとおりである．なお，各パターンの () 内に書かれた数字は，そのデータセットに含まれるサブドメインの数を意味している．

表 3 データセットのパターン

パターン	11 空きポート除外	80 除外
パターン 1 (1,196,076)		
パターン 2 (1,107,946)	o	
パターン 3 (1,109,117)	o	o

データセットに行う操作は 2 種類用意した．パターン 1 では，用意したデータセットをそのまま利用し，パターン 2 とパターン 3 で各操作による予測精度への影響を見る．

11 個以上のポート除外は，多数のポートが開放されているホストを除外するためのものである．単一のホストに多数のポートが開放されている場合，そのホストでは多数のサービスが稼働されていると考えられる．このようなホストにつけられるサブドメインは，稼働サービスを基に付けられているとは考えにくいため，予測に用いることは難しいのではないかと考えられる．そのためこれを除外した際に，予測精度に対する影響を確かめる．これは，単一のホストで 11 個以上の開放ポートがあるホストそのものを，データセットから除外する．

80 番ポート除外は，多くのホストで開放されている 80 番ポートのラベルを削除することで，80 番ポートの数による影響を減らすためのものである．これは，各ホストで 80 番ポートのラベルが存在していた場合，そのラベルのみを削除する．

また，11 個以上の開放ポート除外および 80 番ポート除外のどちらもあるパターン 3 では，80 番ポート除外を行なった後に 11 個以上の開放ポート除外の操作を行う．この順番により，開放ポートが 10 個以下となり除外の対象外となったサブドメインによって，パターン 2 よりもサブドメイン数が 1,171 個増えている．

4. サブドメインと開放ポートの統計データによる検証

はじめに，代表的なサービスと開放ポートの例を表 4 に示す．この表にはサブドメインとそのサブドメインで開放されていたポートの一つ，およびそのポートを使用している関連サービスを示している．サブドメインにおける出現数では，表 4 で示した開放ポートが，そのサブドメインが付けられたホストの内，いくつのホストで開放されていたかを表している．

日常生活で最も頻繁に見かける “www” は，Web サイトで用いられる一般的なサブドメインであり，このサブドメインかつ http が使用できるように 80 番ポートが開放されているホストは，357,089 という数となっていた．反対に，“dns” や “rdp” などのプロトコル名をそのままサブドメインとして用いたものはあまり多くないことも分かる．

次に，3.2.1 節で述べた手法による結果を示す．図 1 は各サブドメインの出現割合を円グラフとして表したものであり，割合が 0.5%を超えるサブドメインが個別に示されている．図 2 は同一サブドメインの出現頻度分布を示したものである．図 3 は重複の有るサブドメインにおけるポート出現率を算出した結果のうち，上位 5 つとなったポート番号を示している．図 4 は重複の無いサブドメインにおいて，図 3 と同様に算出されたポート出現率上位 5 つが示されている．

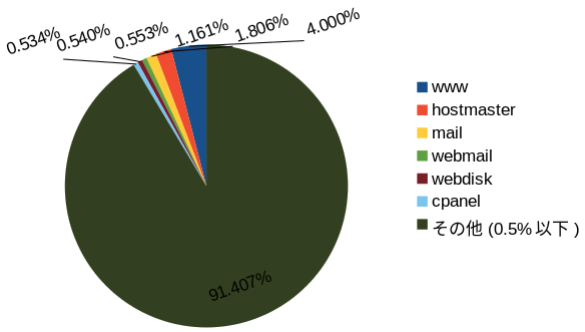

図 1 サブドメインの出現割合

図 1 を見ると，最も多く使われているサブドメインは “www” であるが，その割合はたった 4%しかないことが分かる．全体の 90%超が出現割合 0.5%以下となっており，一般的に広く設定されるサブドメインというものは無いということが言える．

図 1 から多種多様なサブドメインが利用されていることが推測できるが，実際にどれだけ重複したサブドメインが付けられることが有るのかは図 2 を見ることで分かる．図 2 は横軸が各サブドメインで重複した数，縦軸がその重複回数におけるサブドメインの種類数を

表 4 サービスと開放ポートの対応関係の例

サブドメイン	開放ポート例	関連サービス	出現数
www	80	http	357,089
dns	53	DNS	242
rdp	3389	Windows Remote Desktop	27
pop	995	POP3 over TLS	98

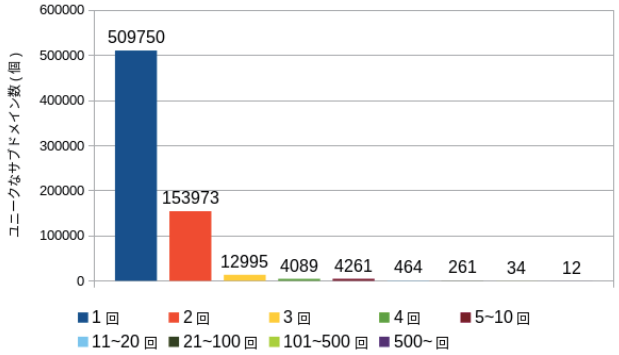

図 2 同一サブドメインの出現頻度分布

意味している．見て明らかなように，重複がない 1 回のみしか出現しなかったサブドメインの種類数が他と比較して圧倒的に多いことが分かる．重複回数が増えていくごとに，対応するサブドメインの種類数は減少していき，500 回以上重複したサブドメインはたった 12 種類しか存在しなかった．図 1 における出現割合 0.5% 以上のサブドメインは，この 500 回以上重複したサブドメインの中でも上位 6 位となる．

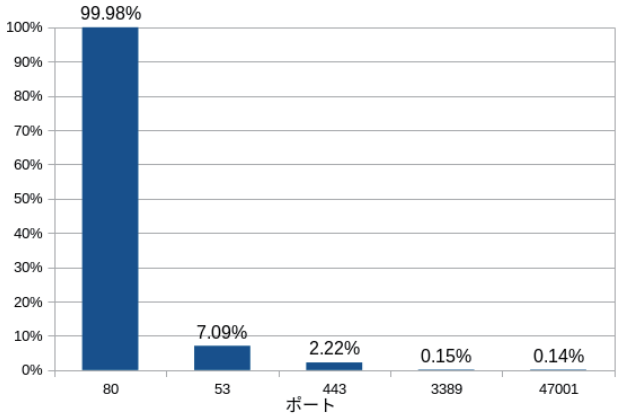

図 3 重複の有るサブドメインにおけるポート出現率の上位 5 つ

重複が有るものと，重複が無いものとでサブドメインの種類数の隔たりが大きいことが分かった．そこで，それぞれにおける開放ポートの特徴に違いがあるのかを見ることができるポート出現率についての図が図 3

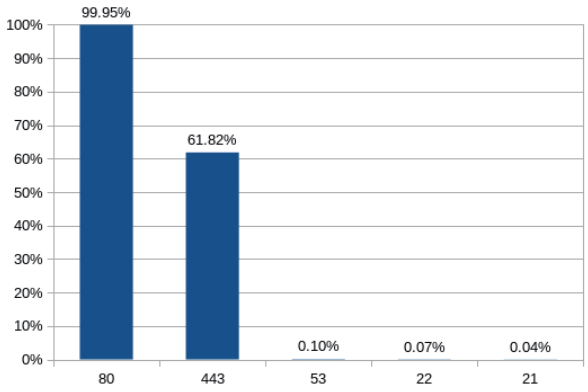

図 4 重複の無いサブドメインにおけるポート出現率の上位 5 つ

と図 4 である．

図 3 と図 4 の両方を見ると，重複の有る・無し関係なくほとんどのサブドメインが割り当てられたホストにおいて，80 番ポートが開放されていることが分かる．重複の有る・無しにおける大きな違いは，重複の無いサブドメインにおいて 80 番ポートと同じ web 系の https で用いられる 443 番ポートが次点で多く存在することである．重複の無いサブドメインにおいては 61.82%もの出現率だが，重複の有るサブドメインにおいてはたったの 2.22%と大きな差が存在する．

重複の有る・無しによるポート出現率の違いでもうひとつの興味深い点は，DNS で用いられる 53 番ポートである．443 番ポートほどではないものの，重複の有るサブドメインにおいては 7.09%となっているのに対して，重複の無いサブドメインにおいては 0.10%と小さな値となっている．これは，DNS サーバに対してよく使われるサブドメインが存在する可能性を示唆していると言える．

5. サブドメインと開放ポートの機械学習を用いた検証

本章では，3.2.2 節で述べた手法による結果を示す．表 5 には各データセットのパターンによって学習したモデルによる予測性能を示している．

マルチラベル予測の際の予測するラベル数および基

準は，予測ラベル可能性のしきい値を設定することで調整を行う．あるサブドメインにおいて予測するラベル数に制限は加えずに，予測されるラベルの確率がしきい値を超えていた場合に出力される．

今回のバリデーション時には，予測ラベル可能性のしきい値を，0.6，0.5，0.4，0.3 の 4 種類で行なった．

表 5 機械学習による開放ポート予測性能

予測しきい値		パターン 1	2	3
0.6	Precision	0.953	0.855	0.882
	Recall	0.994	0.849	0.806
	F-measure	0.9730	0.8520	0.8423
0.5	Precision	0.952	0.849	0.875
	Recall	0.997	0.859	0.815
	F-measure	0.9740	0.8540	0.8439
0.4	Precision	0.952	0.843	0.869
	Recall	0.998	0.866	0.822
	F-measure	0.9745**	0.8543*	0.8448*
0.3	Precision	0.950	0.824	0.862
	Recall	0.998	0.879	0.827
	F-measure	0.9734	0.8506	0.8441

表 5 内の F-measure 欄で “*” が付けられた項目は，各パターン内で最も良い値となっていることを示している．また，全 3 パターンの中で最もよい値には “**” が付けられている．予測しきい値は 4 種類で行なったが，全てのパターンにおいて最も良い結果となったのは 0.4 となった．

データセットに対して操作を行なっていないパターン 1 が F-measure において最も良い 0.9745 という結果となり，操作が増えるにつれて結果が悪くなっていることから，できる限り多くのデータを入力することが重要であると言える．

もっとも結果の良かったのパターン 1 における 0.9745 という数値は，攻撃時の下調べとして行われる作業を考えると，実際に利用可能となってしまうほど高い値と言える．つまり，この手法を用いることでサブドメインから開放ポートを推測することは可能である．

6. 考察

統計的データを用いた手法と機械学習を用いた手法の 2 つで検証を行なった．今回の結果からは，統計的データをもとに開放ポートを推測することは難しいが，文字列の特徴から開放ポートとの関係性を見出す機械学習を用いる手法では，開放ポートの推測は可能であることが分かった．

統計的データを用いた検証においては，重複したサブドメインが付けられることは少ないということが分かった．このことから，悪意を持った攻撃者があるホストに関する下調べをする際に，そのホストのサブドメインと同一のホストにおいてどのようなポートが開放されていたかという情報をもとに推測することは困難であると言える．

しかし，推測するサービスを一部に絞った場合，適応可能な条件も存在する可能性が考えられる．一例としては，図 3 にあった DNS に用いられている 53 番ポートである．重複の有るサブドメインと重複の無いサブドメインで有為にポート出現率が異なる 53 番ポートは，このデータを基に考えることも可能となる．

サービスの推測ではないが，サブドメインから推測できる情報の攻撃への悪用として考えた場合，53 番ポートよりも明確な差が重複の有るサブドメインと重複の無いサブドメインの間で存在する 443 番ポートも利用できてしまう可能性が考えられる．重複の有るサブドメインでは 443 番ポートの出現率が低いことから，通信内容が暗号化される HTTPS による通信がほとんどされていないことを意味する．つまり，中間者攻撃の実行を考えている攻撃者が，どのサーバへのトラフィックをターゲットにするか選定を行う際に，サブドメインの重複があるものから優先的に確認していくことで，選定を効率化できてしまう可能性が有る．

機械学習を用いた検証においては，表 5 よりパターン 1 において F-measure が 0.9745 という非常に予測精度の高いモデルが学習可能であることが分かった．このことから，サブドメインに使われる文字列には，明確に開放ポートとの関係性が存在していると言える．

パターン 1 に対して，パターン 2，パターン 3 とデータセットに対する操作が増えるたびに予測精度は悪化した．これは，パターン 2 では 11 個以上のポートが開放されているホストを除外し，パターン 3 では更に 80 番ポートのラベルを除外したため，学習に利用されるデータ数が減少したことによる影響だと考えられる．

特に，80 番ポートは図 3 および図 4 から，他と比較して圧倒的な割合で存在していることが分かっている．この数の差から，モデルが 80 番ポートを出力するだけでモデル性能を向上させることができてしまい，80 番ポートの過学習を起こしてしまっている可能性が考えられる．

パターン 3 で 80 番ポートを除外したが，これによる精度に対する影響は予測しきい値 0.4 において F-measure が，パターン 2 と比較して 0.0095 しか減少していないことは注意すべきである．全てのサブドメインで 80 番ポートを出力するだけで向上していたと仮定すると，

それによって良い値となっていたRecallが減少したものの，80番ポートによる過学習がなくなったことでPrecisionが改善したものと考えられる．

パターン2とパターン3は，F-measureで比較した場合にはパターン2が性能の良いモデルとなるが，圧倒的多数となっている80番ポートを除外してこの性能を維持しているパターン3の方が，広範囲で適用可能であると言える可能性が有る．

また，パターン1とパターン2およびパターン3間の予測精度の差が大きい．この差から，11個以上のポートが開放されているホストの除外を行う際に稼働サービスを基に付けられているとは考えにくいと予想していたが，これは間違っていたことになる．つまり，サブドメインと11個以上の各開放ポートの間には，予測可能となるような特徴量が存在していると言える．

7. 結言

本研究では，サブドメインのみを用いることで，攻撃時に行われる事前作業の簡易化およびステルス化ができてしまう可能性について検証を行なった．

本研究で警鐘しているサブドメインの新たな悪用方法は，あるホストに対する侵入経路を提供するようなものではないが，確実に攻撃へのハードルを下げるものである．これが実際に可能であるかどうかを検証し，対策を考えることは，インターネットへの依存が高まる現代においては重要なことであると言える．

今回，統計的データによる検証と機械学習による検証を行なった結果，統計的データによってサブドメインから開放ポートを推測することは困難であるが，機械学習を用いることで可能であることが実証された．これが意味することは，サブドメインと開放ポート間にはそれらを結びつける特徴量が存在するということである．

サブドメインのみで開放ポートが分かるということは，稼働サービスの推測も可能であるということである．こういった状況は，セキュリティ上の問題である．今後の課題として，サブドメインの命名規則に関して，新しく開放ポートの推測が困難なものに変えていく必要性がある．

推測困難なサブドメインと言っても，ただランダムな文字列にするというだけでは課題が残る．ドメインは人間にとって分かりやすい文字列を，IPアドレスの変わりにニックネームのように用いることが目的の一つである．それに対して，利用者にとっても，管理者にとっても難解な名前をつけることは，ドメインの目的に反してしまうことになる．

そのため，外部に公開されるサブドメインはランダムな文字列にしながらも，管理する際のインターフェイスには外部には公開されない管理用の名前をもとに作業するなどの手法を採用する必要があると考えている．この手法の場合，利用者にとっては難解な名前のままではあるが，管理者にとっては管理用の名前を用いることで緩和することができる．しかし，外部に公開される名前と管理用の名前を関連付けするというレイヤが増加するため，システムとしての複雑さが増すことは問題として残る．

サブドメインから開放ポートが推測できるという問題は，致命的な脆弱性とはならないが，攻撃面を可能な限り小さく抑えるためにこの問題の解決を行うのは重要であると考える．

参考文献

[1] M. Glassman and Min Ju Kang: Computers in Human Behavior, 28-2, 673-682 (2012).

[2] J. Pastor-Galindo and P. Nespoli and F.G. Mármol and G. M. Pérez: IEEE Access, 8, 10282-10304 (2020).

[3] OSINT Techniques for Domain POIs, https://mediasonar.com/2020/09/17/osint-techniques-for-security-poi-domains/ (2021/7).

[4] C. Fachkha and E. Bou-Harb and M. Debbabi: 2014 6th International Conference on New Technologies, Mobility and Security (NTMS), IEEE, 1-5 (2014).

[5] The Domain Name Industry Brief Q2 2021, https://www.verisign.com/assets/domain-name-report-Q22021.pdf (2021/10).

[6] RFC7489 Domain-based Message Authentication, Reporting, and Conformance (DMARC), https://datatracker.ietf.org/doc/html/rfc7489 (2021/5).

[7] RFC8659 DNS Certification Authority Authorization (CAA) Resource Record, https://datatracker.ietf.org/doc/html/rfc8659 (2021/5).

[8] RFC1034 DOMAIN NAMES - CONCEPTS AND FACILITIES, https://datatracker.ietf.org/doc/html/rfc1034 (2021/5).

[9] F. Weimer: In FIRST conference on computer security incident, FIRST, 98 (2005).

[10] Rapid7 Labs - Open Data, https://opendata.rapid7.com/ (2021/5).

[11] A. Joulin and E. Grave and P. Bojanowski and T. Mikolov: Proc. of the 15th Conf. of the EACL, 2, 1-5 (2014).