

フィッシング対策に向けた SPF記載メールサーバのPTR レコード大規模調査

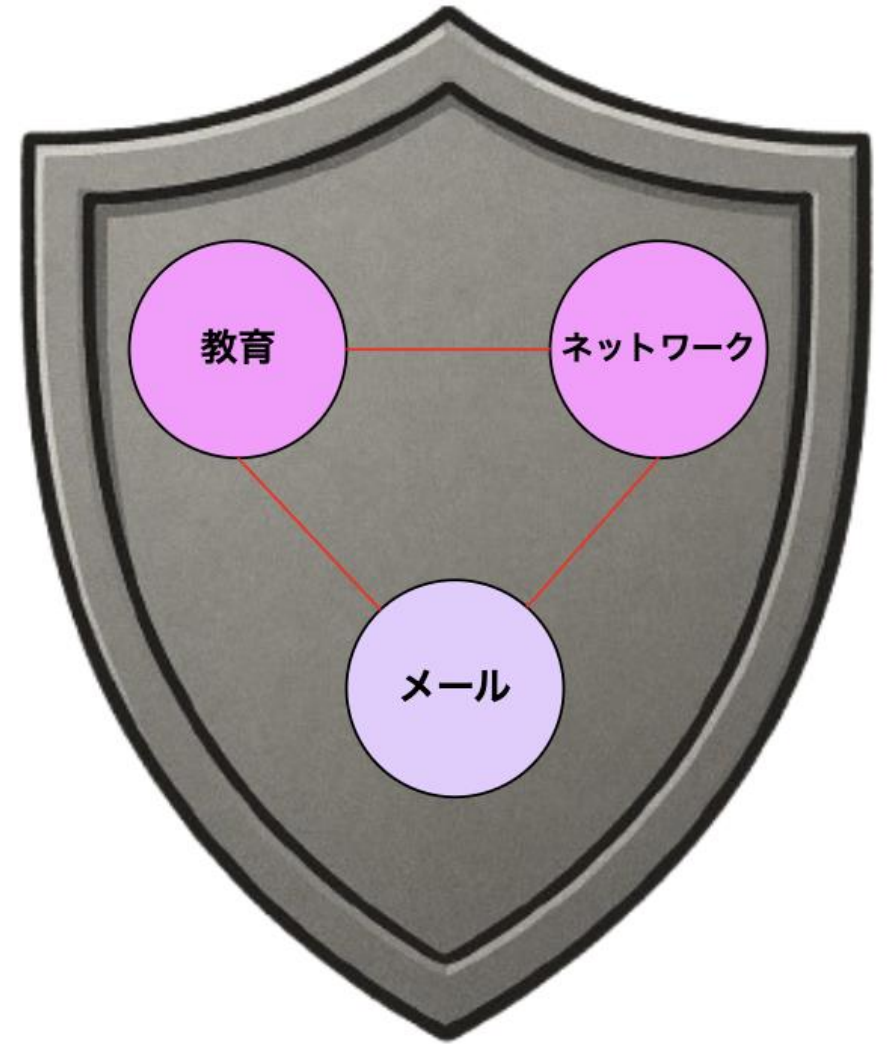
日本大学大学院 理工学研究科情報科学専攻
徳野響

自己紹介

名前：徳野 響

所属：日本大学大学院 M1

興味：メール、教育、ネットワーク



フィッシング被害

- フィッシングメール

送信者を詐称した電子メールである.

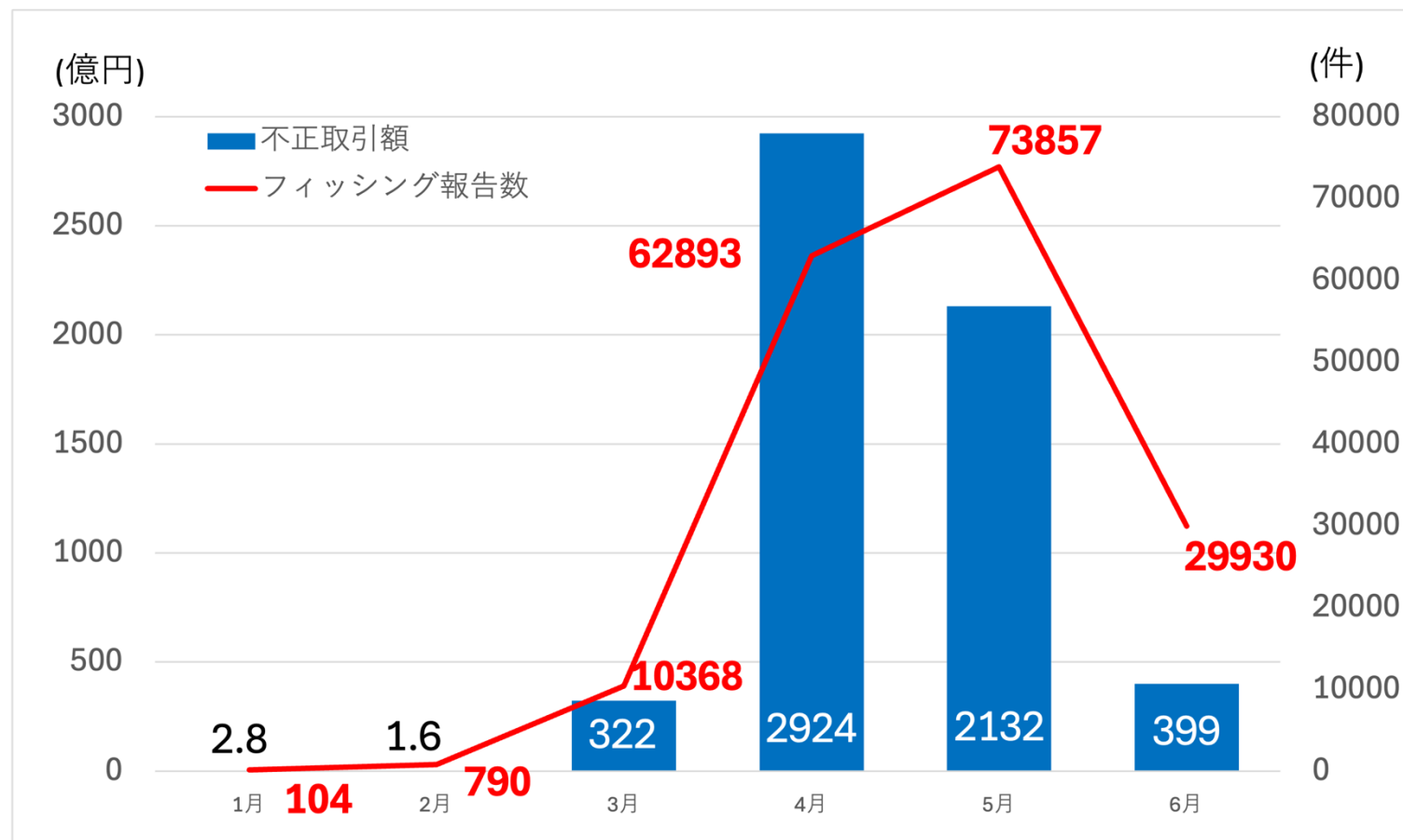
機密情報の詐取や不正行為への誘導を目的とする.

- フィッシング対策協議会の報告

2024 年1 月から12月までに受領したフィッシング報告件数は約171万件に達し, 前年の約1.44 倍と過去最多を記録したことが報告されている.

フィッシング被害

- 証券口座不正取引額とフィッシング報告件数（警察庁）



背景

- フィッシング対策協議会の報告

ある調査用メールアドレス宛に届いたフィッシングメールの送信元IP アドレスのうち、PTR（逆引き）が未設定である割合は**約91.0%**を占めると報告されている。

- フィッシングメールの検知精度向上に向けて

PTR設定（逆引き設定）の有無が有力視されている。

本研究

- 課題

正規メールサーバにおいてPTR 設定が行われていることが前提であるが、**正規メールサーバにおけるPTR設定率は明らかでない**。仮に設定率が低い場合、検知に利用すると誤検知を招く結果となる。

RQ. フィッシングメール検知でPTR設定の有無を活用できるのか？

- 本研究

JPドメインを対象に、SPFレコードに記載された送信者候補IPアドレスを収集し、PTR設定の有無を定量的に評価した。また、SPFレコードを観測し、設定された許可範囲を集計した。

調査方法(データ)

本研究における調査データ

種別	ドメイン数（調査データ）	割合（調査データ）	割合 (JPRS登録)
co.jp	4,347	33.69%	28.61%
or.jp	348	2.70%	2.41%
ne.jp	77	0.60%	0.72%
都道府県型.jp	73	0.57%	0.56%
ac.jp	25	0.19%	0.23%
lg.jp	15	0.12%	0.11%
go.jp	4	0.03%	0.05%
汎用JPドメイン	8,013	62.11%	67.31%

JPRS株式会社の公表しているドメイン割合とも近く **データの偏りは少ない**。

調査方法

SPFレコードの調査

全JPドメインから抽出された1%のドメイン（12,829 件）を対象
ランダム抽出によるサンプリング誤差が含まれる。

IPv4アドレスを対象としている。

単一時点（2025年08月19日）での調査である。

- 観測対象

SPFレコードにおけるIPアドレス許可範囲

includeメカニズムにより参照されるドメイン

調査方法

PTR（逆引き）設定の調査

SPFレコードは、送信元ドメインの管理者が許可する送信メールサーバのIP アドレスを記載するため、送信者候補IP アドレスを推測することが可能である。

- SPF レコードから送信者候補IPアドレスの抽出
 - 各ドメインにおいて許可を意味する+ 修飾子を持つ記述を対象メカニズムip4 におけるCIDR表記/8 から/23 を除外
 - /24~/32： 11,536ドメインにおいて許可された約70万IP
 - /32のみ： 8,398ドメインにおいて許可された17,221IP

結果

- CIDR

/24が最多であり，その設定数は30,873であった．

最も広大なCIDRは/8であり，設定数のうち，0.14%を占める．

現実的なメールサーバ数に対して過剰な許可範囲を設定していることがわかる．

CIDR	総数	CIDR	総数
/8	95	/21	2,710
/9	6	/22	2,937
/10	9	/23	6,116
/11	5	/24	30,873
/12	22	/25	4,242
/13	25	/26	11,428
/14	20	/27	3,070
/15	2,099	/28	4,304
/16	4,584	/29	2,299
/17	3,298	/30	146
/18	1,236	/31	691
/19	5,641	/32	1,335
/20	5,577	—	—

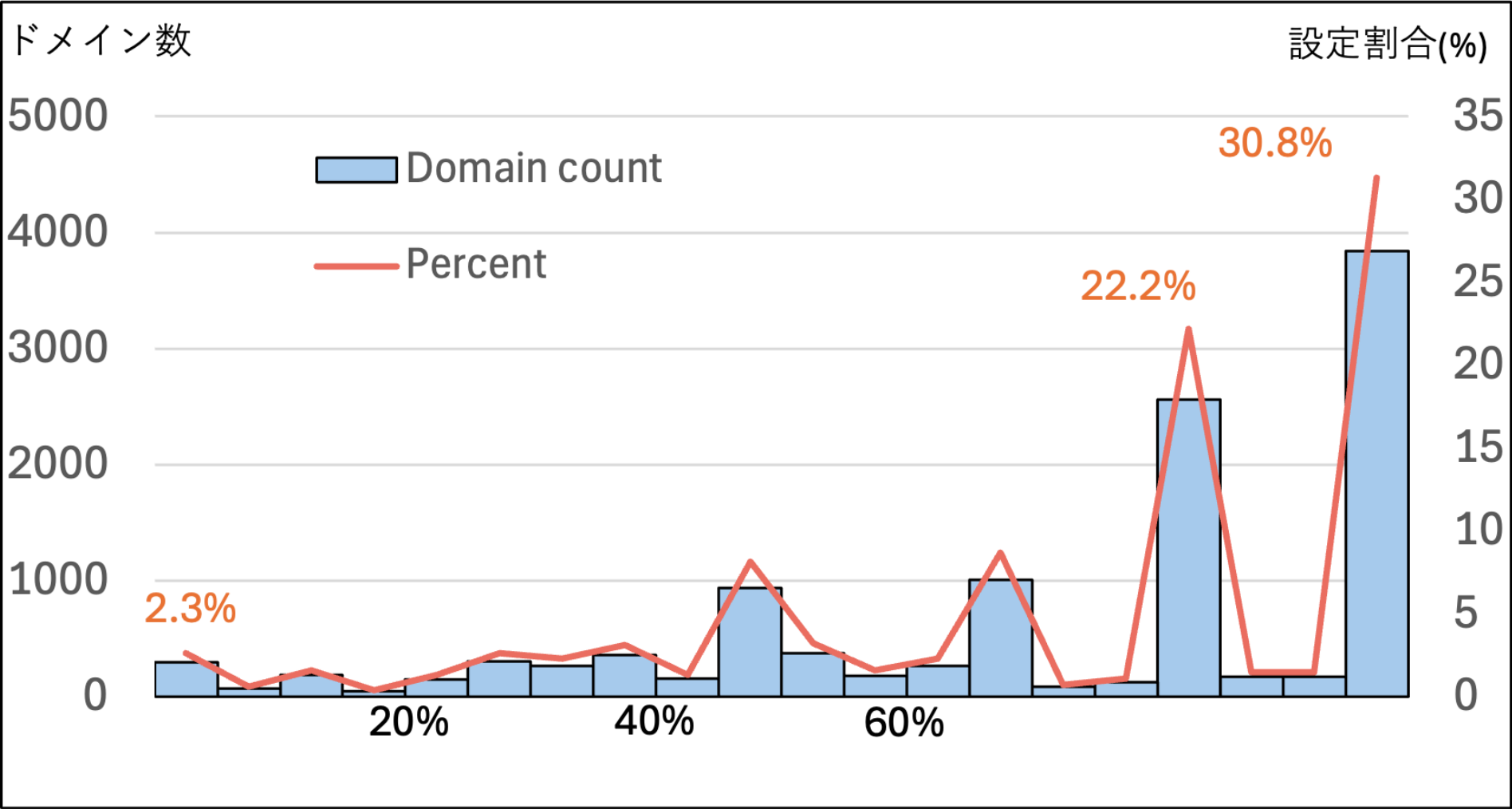
結果

SPFにおいてincludeで参照された上位10ドメイン

ドメイン名	Includeでの設定数	許可IP数	設定割合
spf.sender.xserver.jp	2,098	392	80.9%
spf.protection.outlook.com	1,013	458752	23.6%
_spf.maildeliver.jp	971	2608	97.2%
_spf.lollipop.jp	907	4096	33.6%
_spf.google.com	697	223232	52.6%
_spf.onamae.ne.jp	597	465840	24.4%
_spf.bizmw.com	319	2576	38.3%
_spf.heteml.jp	302	768	65.5%
fmx.etius.jp	237	1796	54.3%
_spf.shared-server.net	198	1280	1.3%

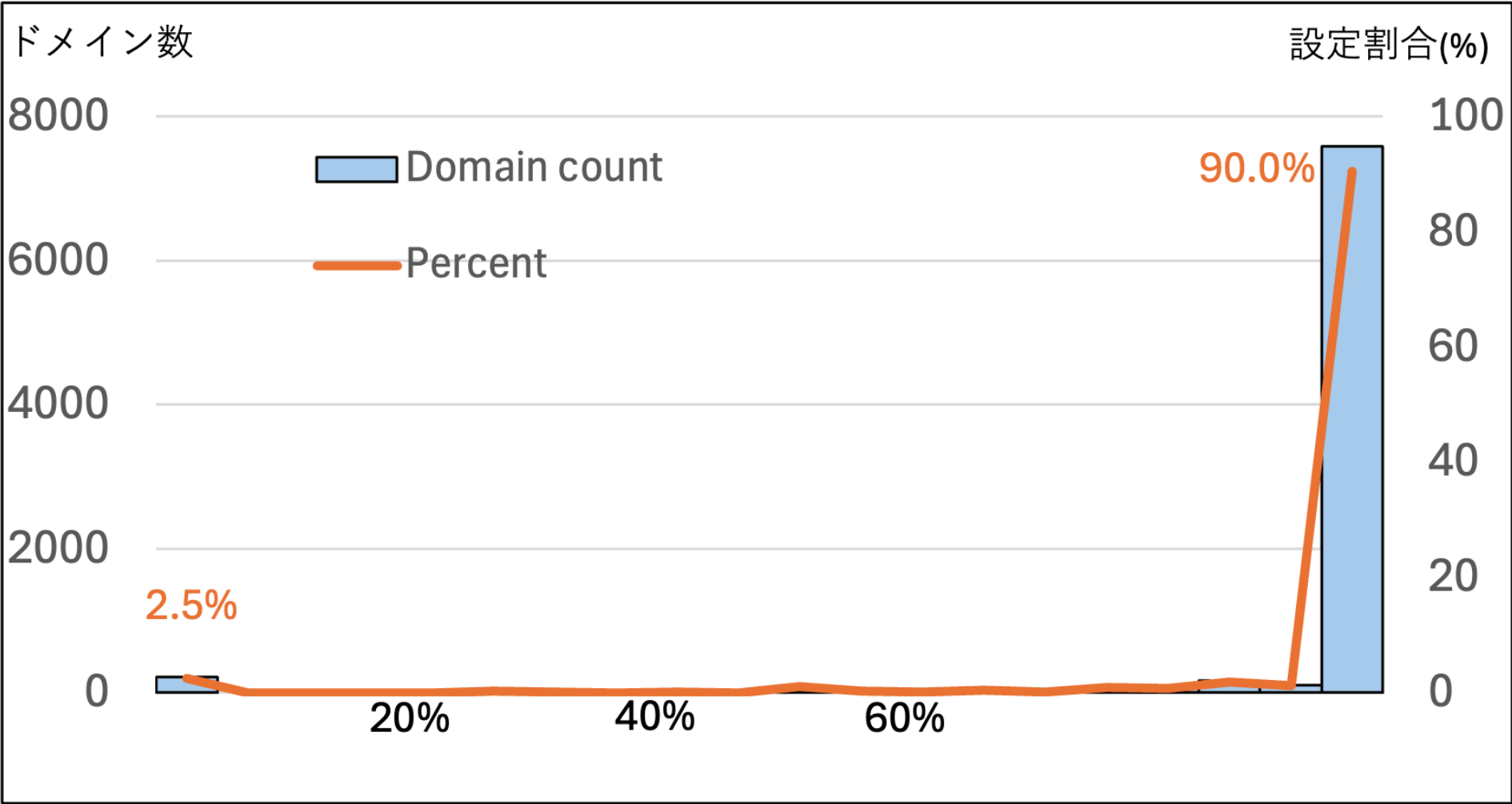
結果

計測対象：CIDR/24~/32(調査対象IPアドレスの47.0%で設定有)

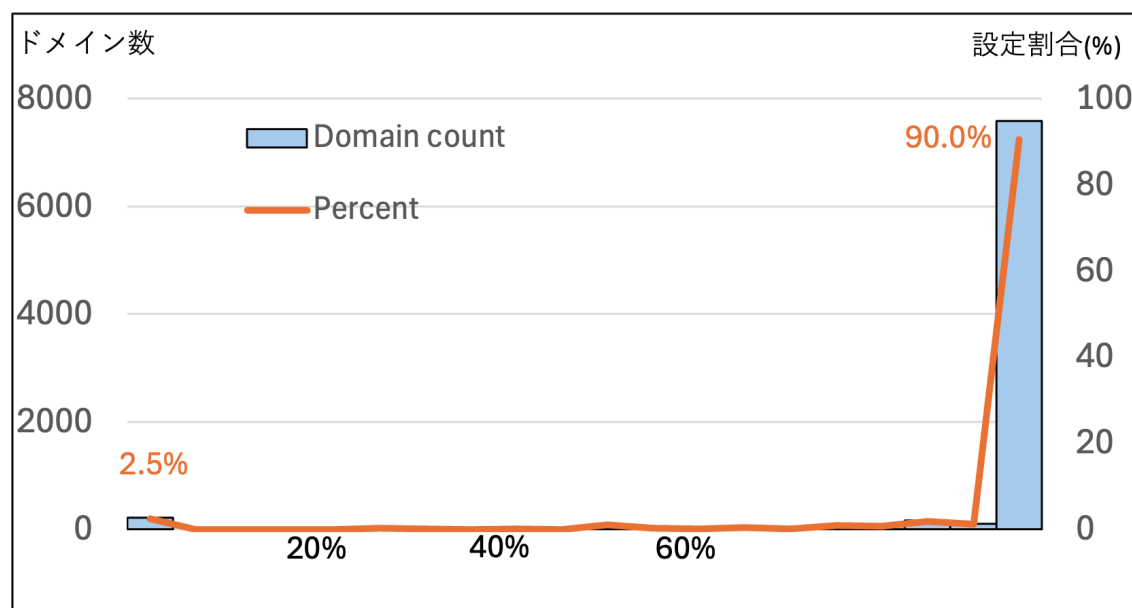
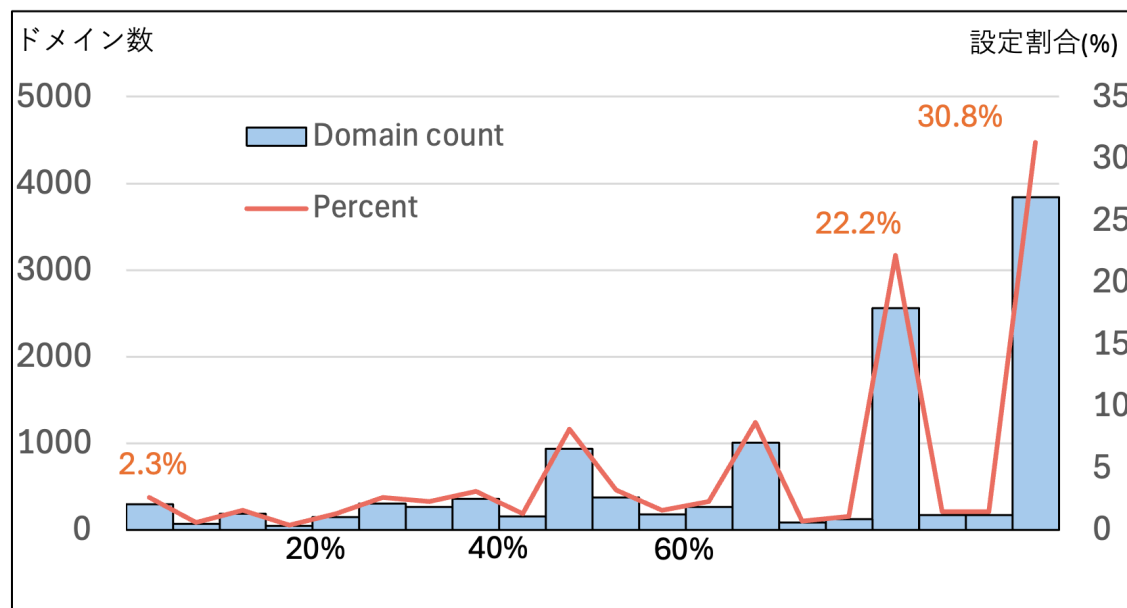


結果

計測対象：CIDR/32のみ(調査対象IPアドレスの94.9%で設定有)



結果



CIDR/24~/32の結果, CIDR/32のみの結果
ともに設定のされていないドメインの割合は3%以下である.

結果

国別のPTR 設定 (CIDR/24~/32)
IPアドレス数1,000個以上の抜粋

設定率 高

CH(スイス), FR(フランス)

設定率 低

KR(韓国), IN(インド)

「**国別の逆引き普及率**」の考慮が有効である可能性がある。

国コード	PTR 設定数	IP アドレス数	設定割合
CH	1,532	1,544	99.2%
FR	3,441	3,872	88.9%
HK	1,463	2,291	63.9%
CA	1,059	1,721	61.5%
GB	1,137	2,164	52.5%
JP	161,908	324,383	49.9%
DE	2,154	4,577	47.1%
SG	1,238	2,675	46.3%
NL	1,078	2,684	40.2%
IE	890	2,231	39.9%
CN	1,947	5,346	36.4%
KR	1,074	3,739	28.7%
IN	278	1,167	23.8%

結論

範囲を限定した上での調査ではあるが、SPF レコードに記述された多くのIPアドレス(/32のみでは、94.9%)においてPTR 設定が行われていることが確認された。

この結果から、**正規メールサーバにおいてPTR 設定は広く普及しており、フィッシングメール検出に活用可能である**と推測される。しかし、PTR設定のないドメインも観測されたことから、国別の設定割合を踏まえ、**SPF/DMARCの後段階でドメイン評価スコアにPTR有無**を組み込むといった活用が妥当であると考ええる。