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

徳野 響[1,a)]　依田 みなみ[1,b)]　櫻庭 秀次[2,c)]　松野 裕[1,d)]

概要：フィッシングメール対策の精度向上にあたり，送信元メールサーバにおける逆引き（PTR レコード）設定の有無が有力視されているが，その実態は明らかでない．PTR レコードは，IP アドレスからホスト名を得るための DNS リソースレコードであり，従来の正引きと逆のプロセスを担うものである．フィッシング対策協議会の報告では，調査用メールアドレスに届いたフィッシングメールの大多数が PTR レコード未設定の送信元から発信されていることが指摘されている．しかし，メールサーバの IP アドレスを網羅する方法が限られているため，実態が明らかでなかった．そこで本論文では，JP ドメインに属するドメインのうち，SPF レコードに記載された送信元メールサーバを対象として，その IP アドレスの PTR 設定（逆引き設定）の有無を大規模に調査した．その結果，調査対象 IP アドレスの約 47.0%で PTR 設定が確認され，単一 IP（/32）指定の場合には 94.9%で PTR 設定が行われていた．さらに，許可範囲全体にわたって完全に PTR が設定されているドメインは 90.0%に達し，逆に全く設定のないドメインは 3%未満に留まった．これらの結果から，正規のメールサーバにおける PTR 設定は広く普及しており，送信元信頼性を判断する上で有効な情報となりうることが示された．

キーワード：フィッシングメール，SPF, PTR，送信ドメイン認証

A Large-Scale Analysis of PTR Records in SPF-Listed Mail Servers toward Phishing Mitigation

Hibiki Tokuno[1,a)]　Minami Yoda[1,b)]　Shuji Sakuraba[2,c)]　Yutaka Matsuno[1,d)]

Abstract: In improving the accuracy of countermeasures against phishing emails, the presence or absence of reverse DNS (PTR record) configuration on sending mail servers has been regarded as a significant indicator, although its actual status remains unclear. A PTR record is a DNS resource record that maps an IP address to a host name, functioning as the reverse process of conventional forward DNS resolution. According to reports from the Anti-Phishing Council, the vast majority of phishing emails delivered to designated investigation addresses originate from servers without PTR records. However, due to the limited methods available to comprehensively cover the IP addresses of mail servers, the actual situation has not been fully elucidated.In this study, we conducted a large-scale investigation targeting the sending mail servers specified in SPF records of domains under the JP domain, examining whether PTR records were configured for their corresponding IP addresses. As a result, PTR configuration was confirmed for approximately 47.0% of the investigated IP addresses, and for single IP (/32) specifications, the configuration rate reached 94.9%. Furthermore, 90.0% of the domains had PTR records configured across their entire permitted range, while fewer than 3% of the domains had no PTR configuration at all. These findings indicate that PTR configuration is widely adopted among legitimate mail servers and can serve as effective information for assessing the reliability of sending sources.

Keywords: Phishing email, SPF, PTR, Sender Authentication

1. はじめに

フィッシングメールとは，送信者を詐称した電子メールを用いて，機密情報の詐取や不正行為への誘導を目的とするサイバー攻撃である．フィッシング対策協議会の報告によれば，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 1,718,036 件に達し，前年の約 1.44 倍となり過去最多を記録した [1]．特に，証券会社等を装ったフィッシングが増加しており，金融庁は 2025 年 1 月 2025 年 7 月までの不正取引件数が 8,111，売却金額が約 3,307 億円，買付金額が約 2,898 億円であり被害が急増していると報告している [2]．また，警視庁，および金融庁の発表によると，令和 5 年（2023 年）11 月末時点におけるインターネットバンキングに関するフィッシングによる不正送金被害件数は 5,147 件，その被害額は約 80.1 億円に上り，いずれも過去最多を更新した [3]．これらの統計は，フィッシングが依然として深刻な情報セキュリティ上の脅威であることを示している．

フィッシングメール対策の精度向上に向けて，送信元メールサーバにおける PTR 設定の有無が有力な指標として注目されている．フィッシング対策協議会の調査によれば，フィッシングメールの送信元 IP アドレスのうち，逆引きが未設定である割合は約 91.0%に上ると報告されている [4]．一方で，PTR 設定の有無を有効に活用するためには，正規のメールサーバにおいて PTR 設定が普及していることが前提となる．しかし，その普及状況は十分に明らかでなく，Simple Mail Transfer Protocol（SMTP）[5] の仕様として PTR 設定は必須ではないため，正規サーバでも未設定の可能性がある．そのため，その有無を判定基準とすると誤検知を招く懸念がある．

そこで本研究では，JP ドメインに属するドメインのうち，SPF レコードに記載された送信元メールサーバを対象として，その IP アドレスの PTR 設定の有無を大規模に調査した．また，調査の過程で得られた JP ドメインにおける SPF 設定の現状についても分析を行った．

本研究における貢献は以下に示す．

- JP ドメインを対象に，SPF レコードに記載された送信元 IP アドレスを収集し，PTR 設定の有無を定量的に評価した．
- 調査結果に基づき，PTR 設定を送信元評価に活用する有効性を検証し，これにより，運用者やセキュリティベンダーにとって実用的な知見を提供した．

[1] 日本大学
Nihon University
[2] 電気通信大学
The University of Electro-Communications
[a)] cshb25009@g.nihon-u.ac.jp
[b)] yoda.minami@nihon-u.ac.jp
[c)] sakuraba.shuji@ohsuga.lab.uec.ac.jp
[d)] matsuno.yutaka@nihon-u.ac.jp

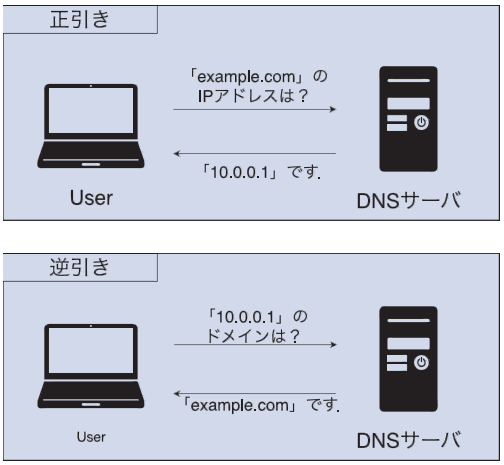

図 1 DNS における正引きと逆引き

- SPF レコードにおいて設定された過剰な許可範囲を多数確認し，国内におけるメールサーバ設定の課題を提示した．

2. 背景

2.1 DNS における逆引き

逆引きは，Domain Name System（DNS）を用いて IP アドレスに対応するホスト名を取得する仕組みである．DNS は通常，正引きによりドメイン名から IP アドレスを解決する．一方，逆引きは IP アドレスから対応するホスト名を導き出す仕組みであり，正引きと対をなす操作である．逆引きでは，Pointer（PTR）レコードが用いられ，IPv4 では in-addr.arpa，IPv6 では ip6.arpa といった記述で逆引き専用のゾーンに記録される．この PTR レコードを参照することにより，IP アドレスに関連付けられたホスト名を取得することが可能となる．DNS による正引きと逆引きの概略図を図 1 に示す．また，図 2 に IP アドレス 192.0.2.1 をドメイン名 example.com に対応づける PTR レコードの例を示す．

```
1.2.0.192.in-addr.arpa.IN PTR example.com
```

図 2 PTR レコードの例

2.2 Sender Policy Framework（SPF）[6]

SPF は，電子メールの送信ドメイン認証技術の一つであり，送信元ドメイン管理者が許可する送信メールサーバの IP アドレスを DNS の TXT レコードとして公開することで，なりすまし送信を検出する仕組みである．受信側メールサーバは，送信元 IP アドレスと SPF レコードを照合し，一致しない場合は認証失敗と判定する．これにより，送信者詐称を用いたフィッシングメールやスパムメールの受信を抑制できる．また，SPF は政府機関等による導入が促進されている Domain-based Message Authentication,

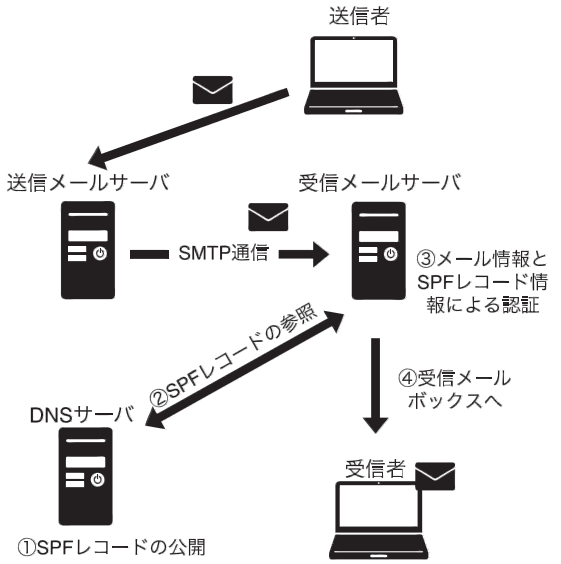

図 3 SPF の概要

Reporting and Conformance（DMARC）[7] においても重要な役割を担っており，SPF 認証結果は DMARC ポリシーの評価に利用される．SPF の概略図を図 3 に示す．

SPF レコードでは，許可を行う送信元を記載するためにメカニズムや許可・拒否を意図するための修飾子が定義されている．以下に代表的なメカニズムと修飾子を示す．

メカニズム

- 「ip4」：IPv4 のアドレスを指定する
- 「a」：指定したドメインの A/AAAA レコードの IP アドレスを参照する
- 「include」：指定したドメインの SPF レコードを参照
- 「all」：すべての送信元を指定

修飾子

- 「＋」：許可
- 「-」：拒否
- 「～」：原則拒否
- 「？」：許可・拒否を判定しない

図 4 は a メカニズムにより example.com および，ネットワーク 192.0.2.0/30 の IP アドレスを許可し，all メカニズムによりそれ以外の IP アドレスを正規でないと設定する例である．

```
example.com IN TXT “v=spf +a +ip4:192.0.2.0/30 -all”
```

図 4 TXT レコードの SPF レコードの例

3. 関連研究

送信ドメイン認証技術に関する調査は多く報告されている．2023 年，Czybik ら [8] は Tranco のドメインリストを用いて 1,200 万件のドメインを対象に SPF の採用状況を分析した．その結果，SPF が全体の 56.5%で設定されており，採用率が増加傾向にあること，また，多くのドメインで許可する IP アドレスの範囲が過度に広く設定されている問題があることを報告している．

2024 年には小林ら [9] は日本国内における官公庁，地方自治体，上場企業を調査対象として SPF，および DMARC の導入状況を調査している．これによると 91%のドメインにおいて SPF レコードが登録されており，広く普及していること，DMARC のレコードの登録率が 2023 年と比較し 38%増加し 46%で登録されていることを報告している．

Wang ら [10] は，SPF レコードに広大な IP レンジが指定されている設定の脆弱性に着目し，攻撃者がクラウドや CDN などの共有インフラから容易に該当 IP を取得し，正規ドメインを装ったメール送信が可能であることを実証した．実際に Tranco Top 1M を対象とした大規模調査では，過大な範囲指定により 23,916 ドメインが攻撃可能であることが報告されている．

Arouna ら [11] は，送信ドメイン認証における PTR 設定と Forward-Confirmed reverse DNS（FCrDNS, iprev）の役割を実証的に分析している．OpenINTEL プロジェクトによる大規模 DNS 測定データを用い，約 3 億ドメインから抽出した SPF レコードを基に推定した送信候補 2,793 百万件の IP アドレスを対象に解析を行った．その結果，送信者候補 IP アドレスのうち 36.7%で PTR 設定が行われていたこと，その約 3 分の 2 が FCrDNS 構成済みである一方，多数は未対応であることを示した．さらに主要 MTA や大手プロバイダにおける検証実験を通じ，FCrDNS や SPF の `ptr` メカニズムの扱いが事業者間で一貫しておらず，PTR 設定の有無や正当性がメール受信可否に必ずしも直結していない現状を明らかにしている．

4. 調査方法

4.1 調査データ

本調査は，全 JP ドメインのリストから無作為に抽出した MX レコードを有する 1%のドメイン（12,829 件）を対象とし，2025 年 8 月 19 日に実施した．ただし，ドメインの種類や業種によって SPF 設定傾向が偏る可能性があるため，サンプリング誤差が含まれる点に留意する必要がある．さらに，本研究は単一時点での調査であるため，時間的な変動や DNS サーバ側の設定変更は反映されない．加えて，IPv6 アドレスに関する PTR 設定は対象外とした．調査データの内訳を表 1 に示す．最も多かったのは企業系の co.jp（4,347 件）で，全体の約 34%を占めた．続いて or.jp（348 件），ne.jp（77 件），都道府県名.jp（73 件），ac.jp（25 件），go.jp（4 件），lg.jp（15 件）が確認され，残りの 8,013 件は汎用 JP ドメイン名 (地域型を含む) であった．

4.2 SPF レコードの調査

SPF では，本来，送信元ドメイン管理者が許可する送信

表 1　調査データにおけるドメイン種別

種別	件数	備考
co.jp	4,347	企業
ac.jp	25	教育機関
go.jp	4	政府機関
lg.jp	15	地方公共団体
or.jp	348	非営利団体
ne.jp	77	ネットワークサービス
都道府県名.jp	73	都道府県
–.jp	8,013	汎用 JP ドメイン

メールサーバのみを記載することが想定されている．しかし，既存研究 [8][10] では，実際には広大な IP アドレス範囲が指定され，結果として多数のアドレスが許可されている事例が報告されている．このような設定は PTR 設定の調査において大きな影響を及ぼすため，調査対象データの SPF レコードにおけるプレフィックス長の指定状況を調査した．また，SPF レコードに頻出した include メカニズムによる参照ドメインを抽出し，その PTR 設定率についても調査を行った．なお，実際に参照されるプレフィックス長の指定状況を把握するため，include によって参照されるドメインは重複を除外せず，すべて集計対象とした．

4.3　PTR 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．そこで，JP ドメインから SPF レコードの抽出を行い，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処理することで許可された送信者候補 IP アドレスを抽出し，PTR 設定の有無を調査した．プレフィックス長設定の調査により，/24 が最多の記述設定であることを踏まえ，メカニズム ip4 における Classless Inter Domain Routing(CIDR) 表記/8 から/23 を除外した．CIDR 表記/24 から/32 およびその他 + 修飾子を集計対象とした結果，11,536 ドメインにおいて許可された約 70 万個の送信者候補 IP アドレスが集計された．加えて，本研究では広範囲指定を除外し，SPF レコード設定者が直接指定している IP アドレスのみを集計対象として，同様の集計を行った．結果，8,398 ドメインにおいて許可された 17,221 個の送信者 IP アドレスが集計された．

4.4　PTR 設定の調査プログラム

本研究では，調査用プログラムを Go 1.24.4 で実装し，開発と実行には Visual Studio Code 1.102.3 を利用した．また，各 IP アドレスの国情報を確認するために，MAXMIND 社の GeoLite2[12] を利用している．このプログラムでは処理を行ったドメインをキャッシュに保存し，その結果を利用することで DNS サーバへの問い合わせ回数を削減している．本研究で使用したプログラムの全体の処理フローを以下に示す。

(1) **入力処理**
JP ドメインリストを読み込み，正規化と重複排除を行う．

(2) **展開処理**
SPF レコードから `include` および `redirect` を再帰的に展開し，参照ドメイン集合を生成する．

(3) **解析処理**
各ドメインの SPF メカニズム（`ip4`, `a`, `mx`）を解析し，CIDR 指定は展開して IPv4 アドレス集合を得る．並列処理により各 IP の PTR 設定有無を判定し，GeoIP により国コードを付与する．

(4) **集計処理**
ドメイン単位および国別に，IP 総数・PTR 設定数・PTR 設定率を算出する．

(5) **出力処理**
結果を JSON および Parquet 形式で保存し，後続の統計分析に利用可能とした．

4.4.1　include/redirect の処理について

SPF レコードの展開にあたり, include: および redirect= による参照は再帰的に追跡し，すべての参照ドメインを列挙した．無限ループを防ぐために訪問済みドメインは再訪しない機構を設けているが，深さや件数に関する制限は設けていないため，大規模に参照が連鎖する場合には全体を列挙する挙動としている．列挙した各参照ドメインに対しての IP アドレスの抽出処理では，直下の ip4/a/mx のみを対象とし，そのドメイン内でさらに再帰的に include を展開することは行っていない．

4.4.2　タイムアウト・エラー処理について

DNS 解決には Go 言語標準ライブラリの net.LookupTXT を用い，明示的なタイムアウト制御は実装していない．したがって，DNS クエリのタイムアウト挙動は OS 既定のリゾルバ設定に依存している．また，エラーが発生した場合は当該ドメインをスキップし，後続処理に影響を及ぼさないようにした。

5.　調査結果

5.1　SPF レコードにおける IP アドレス許可範囲

全 JP ドメインのリストからランダムに抽出した 1%のドメインを対象に SPF レコードにおけるプレフィックス設定状況を集計した結果を表 2 に示す．CIDR 表記のうち，/24 が多くのドメインで設定され，その設定数は 30,873 件に上った．また，最も広大な CIDR 表記は/8 であり，全 CIDR 表記アドレスのうち，0.14%を占める．このような過剰なプレフィックス長設定は，攻撃者によるなりすましのリスクを高める要因となるため，適切な対応が求められる．

表 2　SPF におけるプレフィックス長設定状況

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	–	–

表 3　SPF において include で参照された上位 10 ドメイン

ドメイン名	設定数
spf.sender.xserver.jp	2,098
spf.protection.outlook.com	1,013
_spf.maildeliver.jp	971
_spf.lolipop.jp	907
_spf.google.com	697
_spf.onamae.ne.jp	597
_spf.bizmw.com	319
_spf.heteml.jp	302
fmx.etius.jp	237
_spf.shared-server.net	198

5.2　include による参照ドメイン

SPF レコードに頻出した include メカニズムで参照される上位 10 ドメインを表 3 に示す．さらに，表 4 にその許可 IP アドレスと PTR 設定について示す．多くのドメインは SPF レコードとして，管理者が直接設定した許可範囲に加えてメール送信サービスやレンタルサーバの送信元サーバを定義した DNS ホスト名を含んでいた．各 include 先ドメインにおける許可 IP 数は，管理者が SPF レコードで設定した許可 IP 数と比較して設定数が多く，ドメインにおける逆引き率の計算に大きく影響を与える可能性が高いことがわかった．

5.3　SPF レコードの構文エラー

調査対象ドメインのうち，35 ドメインで SPF レコードに構文エラーが確認された．そのうち，SPF レコードが複数存在したドメインは 20 ドメインである．その他には include メカニズムと redirect メカニズムによるループや，修飾子が欠落したドメインの記載といった構文エラーが観測された．これらの構文エラーは，送信ドメイン認証が正しく機能しない要因となり得る．特に SPF レコードが複数存在する場合，受信側の実装によっては正規の送信元であっても認証が失敗する可能性がある．また include や redirect によるループは，認証処理の過負荷や結果の不定性を引き起こす危険がある．

表 4　include 設定数上位 10 ドメインの PTR 設定

ドメイン名	許可 IP 数	PTR 設定割合
spf.sender.xserver.jp	392	80.9%
spf.protection.outlook.com	458752	23.6%
_spf.maildeliver.jp	2608	97.2%
_spf.lolipop.jp	4096	33.6%
_spf.google.com	223232	52.6%
_spf.onamae.ne.jp	465840	24.4%
_spf.bizmw.com	2576	38.3%
_spf.heteml.jp	768	65.5%
fmx.etius.jp	1796	54.3%
_spf.shared-server.net	1280	1.3%

5.4　PTR 設定の調査結果

SPF レコードにおいて，ip4 メカニズムの CIDR 表記/24 から/32，およびその他 + 修飾子を処理対象として逆引き処理の設定率について集計した結果を以下の図 5 に示す．調査対象 IP アドレスのうち約 47.0%で PTR 設定が確認された，全許可範囲で PTR 設定済みのドメインは 3,558 個で全体の 30.8%，PTR 設定のない（0%）ドメインは 264 個で 2.29%であった．また，CIDR 表記/32，およびその他 + 修飾子を処理対象とした集計結果を図 6 に示す．調査対象 IP アドレスのうち約 94.9%が PTR 設定が行われていた，全許可範囲で PTR 設定済みのドメインは 7,554 個で全体の 90.0%，PTR 設定のない（0%）ドメインは 211 個で 2.51%であった．図 5，図 6 ともに完全に PTR 設定のされていないドメインの割合は 3%以下であり，多くの IP アドレスにおいて，PTR 設定が行われていることが確認された．

5.5　国情報と PTR 設定率

メカニズム ip4 における CIDR 表記 /24 から /32，およびその他の + 修飾子を処理対象として収集した送信者候補 IP アドレスに関する国別の PTR 設定率を表 5 に示す．なお，表 5 では IP アドレス数が 1,000 個以上の国を抜粋した．CH（スイス），FR（フランス）の PTR 設定率が 88% 以上と高水準であった．一方，KR（韓国），IN（インド）では 30% 未満にとどまっていた．これら国別の PTR 設定率は，完全に当該国全体の慣習や水準を反映しているわけではなく，調査対象範囲に含まれる事業者の運用が統計値に強い影響を与えている可能性が高いことを留意すべきである．

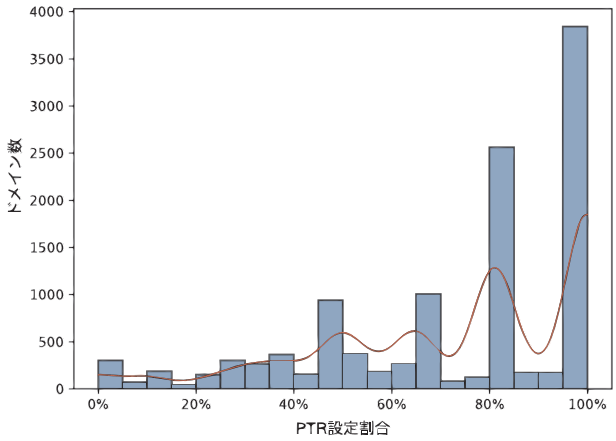

図 5 PTR レコード設定の状況 (CIDR 表記/24 から/32 のみ)

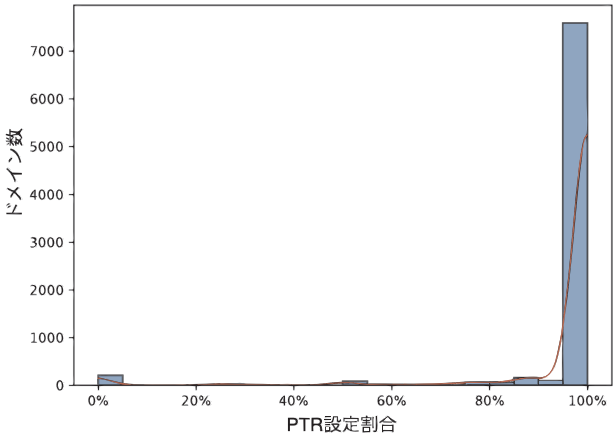

図 6 PTR レコード設定の状況 (CIDR 表記/32 のみ)

表 5 IP アドレスの国別 PTR 設定

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

6. 考察

6.1 既存研究との比較

Arouna ら [11] による調査では，Alexa Top 1M ドメインを対象に SPF レコードを収集し，/8 以下を除外した /9〜/32 の IP レンジを解析している．その結果，全体における PTR 設定率は 36.7%であったことが報告されている．これに対して本研究では，/24〜/32 に限定した JP ドメインを対象とした結果，PTR 設定率は 47.0%であった．両者は調査対象範囲が異なるため，単純比較はできないが，本研究の JP ドメインに限定した分析では，/24〜/32 の細分化されたレンジにおいても PTR 設定率が比較的高いことが確認された．このことは，日本のドメイン運用において PTR 設定が比較的徹底されている可能性を示している．

6.2 JP ドメインにおける PTR 設定

本研究の結果，SPF レコードにおいて /32 などの単一 IP アドレスが指定されている場合には，大部分で PTR 設定が確認された．これは，管理者が明示的にメールサーバとして利用する IP アドレスを指定しているため，PTR 設定も併せて行われていることを示唆している．一方で，/24 などの CIDR を指定している場合には，単一 IP 指定と比較して PTR 未設定の IP アドレスが増加し，全体の PTR 設定率を押し下げている．この要因として，許可範囲内の多くの IP アドレスが実際にはメール送信に用いられておらず，Web サーバや未使用アドレスを含んでいる可能性が高いことが挙げられる．すなわち，「逆引き未設定＝メールサーバ設定の不備」とは必ずしも当てはまらない，「メールサーバ以外の IP を SPF に含めた結果」として逆引き率が低下している構造的要因が存在すると考えられる．このことから，SPF レコードにおける許可範囲をメールサーバに限定した最小構成へと適切に設定すれば，単一 IP 指定の場合と同様に高い PTR 設定率が得られると推測される．本研究では，CIDR 表記/24 から/32 を対象とした調査を行い，PTR 設定が全く行われていないドメインは 2.29%であり，PTR 設定が広く行われている可能性を示した．しかし，PTR 設定率が 1%から 99%のドメインの範囲にあるドメインの多くは，管理者が直接許可した IP アドレスと include メカニズムによる参照ドメインが混在している．そのため，ドメイン管理者により許可された IP アドレスには PTR 設定がされていないが，参照ドメインにおいて PTR 設定がなされているために PTR 設定率が 0%でないドメインも存在すると考えられ，PTR 設定のないドメインの割合は 2.29%から増加する可能性がある．

6.3 SPF における IP アドレス許可範囲

SPF レコードにおける IP アドレス許可範囲として，自身の管理下のメールサーバ以外の IP アドレスを記載する場合には，ホスティングサービスなどにより，第三者に利用される可能性がないことを確認する必要がある．仮に，関係者以外が許可された IP アドレスをメール送信に利用可能である場合，これらのドメイン名で SPF 認証を pass するメールを送信できることになる．また，SPF 認証を pass

するために DMARC でも認証を pass できるようになる．これは，当該ドメインに関係しない第三者が，そのドメイン名の正規の送信者であるかのようなフィッシングメールを送信できることを意味する．そのため，ドメイン名の管理者は，SPF レコードにおける IP アドレス許可を適切に管理し，記載された IP アドレスから正規の送信者情報に偽装することができないように設定を行うべきである．

6.4 国別の PTR 設定

本研究では，SPF レコードに記載された IP アドレスを国別に調査した．結果として，国ごとに PTR 設定の普及度に大きな差がみられた．特に設定率の低い地域からメールの受信を行う必要がある場合には，PTR 設定の有無を条件に識別を行うと誤検知が発生する可能性が高いため，その活用には十分に注意する必要がある．PTR 設定率の違いを踏まえ，グローバルなメール受信環境では，一律の PTR チェックではなく，国別の逆引き普及率を考慮したチェックが理想的である．

7. まとめ

本研究では，JP ドメインの 1%を対象とした調査により，PTR レコード設定の普及状況を明らかにした．SPF レコード設定の調査により，JP ドメインにおいても，多くのドメインで広範囲の IP アドレス許可を行っていることが確認された．このような広範囲に対する許可は攻撃者によるなりすましのリスクを高めるため，対応を行う必要がある．SPF レコードに記述された IP アドレスの大部分において PTR 設定が行われていることが明らかとなった．特に，CIDR 表記/32 およびその他 + 修飾子を含めた場合には約 94.9%の IP アドレスで PTR 設定が確認され，許可範囲全体に対して完全に PTR 設定を有するドメインは 90.0%に達した．一方で，PTR 設定が全く行われていないドメインは全体の 3%未満に留まり，極めて少数であることが示された．これらの結果から，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．

今後は，全 JP ドメインを対象とした調査を実施し，より網羅的かつ精緻な分析を行う予定である．また，主要なメール提供サービスを集計から除外することを予定している．これにより，フィッシング対策における PTR レコード活用の有効性について，より強固に裏付けられると期待される．

謝辞 本研究の一部は，JSPS 科研費 JP25K21182, JP25K15109 の助成を受けたものです．

参考文献

[1] フィッシング対策協議会:フィッシングレポート 2025, 入手先 ⟨https://www.antiphishing.jp/report/phishing_report_2025.pdf⟩ (2025.08.14).
[2] 金融庁：インターネット取引サービスへの不正アクセス・不正取引による被害が急増しています，入手先 ⟨https://www.fsa.go.jp/ordinary/chuui/chuui_phishing.html⟩ (2025.08.22).
[3] 警視庁・金融庁：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（注意喚起），入手先 ⟨https://www.npa.go.jp/bureau/cyber/pdf/20231225_press.pdf⟩ (2025.08.14).
[4] フィッシング対策協議会：2025/06 フィッシング報告状況，入手先 ⟨https://www.antiphishing.jp/report/monthly/202506.html⟩ (2025.08.14).
[5] J. Klensin：Simple Mail Transfer Protocol，RFC5321, 2008.
[6] S. Kitterman：”Sender policy framework (SPF) for authorizing use of domains in email, version 1”, RFC7208, 2014.
[7] M. Kucherawy and E. Zwicky：“Domain-based message authentication, reporting, and conformance (DMARC),” RFC7489, 2015.
[8] Czybik, S., Horlboge, M., Rieck, K.: Lazy gatekeepers: a large-scale study on SPF configuration in the wild, In: ACM Internet Measurement Conference, ACM (2023).
[9] 小林淳史, 佐々木満春，岩佐功，石橋圭介: 送信ドメイン認証技術の導入状況とその考察, Computer Security Symposium, CSS(2024).
[10] Wang, C., Kuranaga, Y., Wang, Y., Zhang, M., Zheng, L., Li, X., Chen, J., Duan, H., Lin, Y., Pan, Q.: Break-SPF: How Shared Infrastructures Magnify SPF Vulnerabilities Across the Internet, In: Network and Distributed System Security, NDSS (2024).
[11] Arouna, A., Fontein, R., Meijerink, B., Livadariu, I., Jonker, M.: On the Role of Forward-Confirmed reverse DNS in E-mail Authentication, In: Traffic Measurement and Analysis Conference (TMA), European Union (2025).
[12] MaxMind：GeoLite2 Free Geolocation Data，入手先 ⟨https://dev.maxmind.com/geoip/geolite2-free-geolocation-data/⟩ (2025.08.20).