CO-005

迷惑メール対策における送信ドメイン認証の解析とその効果

Analysis and Effectiveness of Sender Domain Authentication in Anti-Spam Measures

北倉　奈菜‡　　陳　春祥‡
Nana Kitakura　　Chun-Xiang Chen

1. はじめに

近年、迷惑メールの多様化、複雑化が著しくその手法も巧妙化し、迷惑メール対策の重要性はますます高まっている[1]。

しかし、現在主流となっている多くの迷惑メール対策は、利用者にある程度の専門的な設定や判断を求めるものが多く、個人利用者にとって大きな負担となることも少なくない。例えば、フィルタルールの設定や、ヘッダ情報の確認、あるいは毎回の迷惑メール報告など、技術的知識を必要とする場面が多く存在する。このような状況では、誤って重要なメールを迷惑メールと判断してしまったり、逆に悪意あるメールを見逃してしまうリスクも高まる。このような課題に対して、個人利用者が特別な操作を必要とせず、安全かつ効率的に迷惑メールを回避できる仕組みが求められている。その一つの技術として注目されているのが「送信ドメイン認証技術」である。送信ドメイン認証技術とは、メールの送信元が正当なドメイン所有者であるかどうかを技術的に検証する仕組みであり、代表的な技術としては SPF（Sender Policy Framework）および DKIM（DomainKeys Identified Mail）がある[2][6]。SPF は IP アドレスを用いて送信メールサーバの正当性の検査を行う。DKIM は電子署名によって正当な送信者からの改ざんされていない電子メールであるかどうかを検査する[3]。

実際、これらの技術はサーバ管理者やプロバイダなどの送信元・中継側において導入が進んでおり、送信ドメイン認証の対応率は年々向上しているという報告もある[4]。しかし、それらは主に提供者側、あるいはインフラ視点からの調査であり、実際の受信者側、特に個人利用者の受信環境でどの程度有効に機能しているのかは、あまり調査されていないのが現状である[5]。また、従来の研究においても、送信ドメイン認証が「どのようなメールに適用されているか」、あるいは「迷惑メールのフィルタリングにどの程度寄与しているか」といった視点での分析は十分ではなかった。特に、送信ドメイン認証が迷惑メールの排除に実際どれだけ貢献しているのかという点については、定量的な検証が必要とされる。

そこで本研究では、著者ら自身が日常的に受信・蓄積してきたメールデータのうち、主観的に「迷惑メール」と判断したメールを対象に、SPF および DKIM といった送信ドメイン認証技術の適用状況を調査し、その傾向と有効性について検討することを目的とする。これは、一利用者の立場から、実際にどのような迷惑メールにどの程度の割合で認証技術が施されているかを把握し、現行の迷惑メール対策における送信ドメイン認証の有効性と限界を明らかにするものである。

‡県立広島大学/Prefectural university of Hiroshima

2. 送信ドメイン認証の仕組み

表 1: 送信ドメイン認証技術の概要

送信ドメイン認証技術	認証ドメイン	認証方法
SPF	envelope from	送信元 IP アドレス
DKIM	署名ドメイン	電子署名

表 1 に、本稿で利用する認証技術の特徴を示す。送信元メールサーバのドメインを用いて、受信したメールが 正規のサーバから送信されたメールであるかを検証する 仕組みである。送信ドメイン認証技術は、Sender Policy framework (SPF)、DomainKeys Identified Mail (DKIM)がよく用いられている。SPF の認証を利用するにはまず、送信者が当該ドメインのメールアドレスを利用して送信する可能性のあるサーバが宣言された SPF レコードを公開する。受信者は SPF レコードを取得し、接続元であるメールサーバの IP アドレスが含まれていれば認証成功とする。しかし一般には SPF は転送メールの認証を正しく行うことかできない。これは転送メールでは、SMTP 通信の接続元のアドレスが、中継サーバの IP アドレスとなるため、配送上の送信メールサーバのドメインで指定された SPF レコードを用いた認証に失敗するためである[3]。

DKIM は、SPF の転送に対応していないという課題を補う送信ドメイン認証である。まず送信者は DKIM の検証で用いる公開鍵を自らの DNS サーバにあらかじめ公開しておく[7]。メール送信時にメールヘッダと本文から電子署名を作成し、DKIM-Signature ヘッダとして付加した上で送信する。受信側は DKIM-Signature ヘッダから取得した送信側ドメインの DNS サーバに公開鍵を問い合わせる。取得した公開鍵を用いて電子署名から取り出したハッシュと、ヘッダと本文から作成したハッシュが一致すれば認証成功とする。この仕組みにより転送メールの認証を正しく行うことができる[3]。しかし、DKIM の署名はオリジナルメールのヘッダとボディから生成されていることから、電子メールの送信の途中でヘッダが書き換えられる場合、DKIM は検証に失敗する[4]。

3. 分析方法と実験環境

本研究では、送信ドメイン認証技術がどの程度正しく運用されているかを検証するために、実際に送受信されたメールヘッダを収集・解析し、DNS 上の、現在の情報と比較を行った。

3.1 対象データ

対象としたデータは、著者らが日々受信メールのうち、迷惑メールと判断したメールである。解析においては、メールヘッダの情報のみを利用する。メールヘッダには SPF や DKIM の検証結果が記録されており、また「DKIM-

Signature」ヘッダなどから署名ドメイン(d=)およびセレクタ(s=)の情報を取得できる。加えてメールヘッダ内の「Date」ヘッダから送信日付も取得した。

本研究では、これらの情報をもとに、過去のメールに記録された SPF および DKIM の情報と、現在 DNS に存在する SPF・DKIM レコードとを比較する手法を採用した。

3.2 メールヘッダ例

```
Received-SPF: pass (mybox.example.org:
domain ofmyname@example.com designates
192.0.2.1 as permitted sender)
receiver=mybox.example.org; client-
ip=192.0.2.1;
envelope-from="myname@example.com";
helo=foo.example.com;
```

図 1 ： Received-SPF ヘッダの例

SPF ヘッダの例として、SPF の仕様書[9]で紹介されている例を図 1 に示す[9]。Received-SPF フィールドで SPF 認証の結果が示される。

```
DKIM-Signature: v=1; a=rsa-sha256;
d=example.net; s=brisbane;
c=simple; q=dns/txt; i=@eng.example.net;
t=1117574938; x=1118006938;
h=from:to:subject:date;
z=From:foo@eng.example.net|To:joe@example
.com|
Subject:demo=20run|Date:July=205,=202005=
203:44:08=20PM=20-0700;
bh=MTIzNDU2Nzg5MDEyMzQ1Njc4OTAxMjM0NTY3OD
kwMTI=;
b=dzdVyOfAKCdLXdJOc9G2q8LoXSlEniSbav+yuU4
zGeeruD00lszZVoG4ZHRNiYzR
```

図 2 DKIM-Signature:ヘッダの例

Dkim-Signature ヘッダの例として、DKIM の仕様書[8]で紹介されている例を図 2 に示す[8]。ここで署名対象ヘッダは h タグ、署名を表すヘッダは b である。

3.3 分析方法

分析にあたっては以下の手順をとった。

1．メールヘッダから SPF の検証結果、DKIM の署名ドメインおよびセレクタの値を抽出
2．日付をもとに、同一ドメインにおけるもっとも新しい署名情報のみを抽出
3．抽出された署名ドメインとセレクタに対して、DNS クエリを実行し、現在の SPF レコード、DKIM 公開鍵（TXT レコード）を取得。
4．現在の DNS 情報と過去のメールヘッダに記録された情報を照らし合わせ、一致・不一致を判定

このようにして、過去には署名されていたが現在は署名されていない、あるいはその逆のケースなど、設定の変化や継続性の有無を検出可能とした。

3.4 メール分類の基準と目的

本研究では、メールの内容に基づき、「迷惑メール」と「正規メール」に分類を行った。分類の基準は、フィッシングや架空請求メールなどのような客観的な迷惑メールと、著者らの主観的判断により行ったものであり、スパムフィルタのような自動化されたシステムでは検出しきれないケースや、ユーザーの体感に近い分類を目指した。たとえば、宣伝色の強いメールや、内容が雑多で読み手の興味を引かないもの、過去に悪質と判断された類似メールなどが「迷惑」と分類されている。

このような主観的判断を取り入れることで、実際に「迷惑だと感じられるメール」がどのような認証設定を持っているかを観察することができ、送信ドメイン認証の実用性や限界を検証するうえで有意義であると考える。

4. 検証結果

本章では、収集したメールヘッダに対して実施した送信ドメイン認証（SPF および DKIM）がどのように適用されているかを検証した。

本研究では、研究室に届いたメールの中から迷惑と判定された 35937 通を分析対象とした。これらの受信メールには、同じドメインのものが複数存在する。その様なメールに対してはドメインの重複を避けるために、受信日時が最新のもののみ抽出し解析した。重複を取り除いた場合、ドメイン数は 11539 件になる。SPF の検証結果については重複したドメインを取り除いたうえで、過去に SPF 認証が施されていた 351 件のドメインについて検証結果示している。

4.1 SPF 検証結果

SPF については、迷惑メールとして分類されたメールに対して、SPF の検証を実施した。具体的には、メールヘッダに記録された SPF 判定結果(Pass/Fail/None)などと対応するドメインの現在の DNS 情報を照合した。表 2 に集計結果を示す。

表 2: 迷惑メールにおける SPF の検証結果と DNS 照合の集計

現在 / 過去	SPF レコードあり	ドメインが存在しない	SPF レコードなし	DNS サーバ応答なし
Pass	256	49	14	0
Neutral	9	9	5	1
Softfail	1	1	0	0
Fail	1	0	0	0
None	1	0	1	0
Permeroor	3	0	0	0

表 2 より、過去に SPF が「Pass」と判定された迷惑メールのうち、現在も有効な SPF レコードを持つものが 256 件存在する一方、DNS 上に SPF レコードが存在しない、また

はドメイン自体が存在しないものも一定数（計 63 件）確認された。特に過去は「Pass」でありながら現在は DNS 上に SPF 情報が存在しないケース（14 件）は、ドメインが使い捨てである可能性がある。また、設定の削除・変更があった可能性を示唆する。

また、「Neutral」「Softfail」「None」といった不明確な SPF 判定が出ているメールにおいても、現在の DNS 情報と照らし合わせると、設定が不十分または欠落しているケースが複数確認された。

これらの結果から、SPF 認証は一部の迷惑メールにも「Pass」として記録されることがある一方で、DNS 上の設定状況との不一致があるケースがあることが分かった。

表 2 が示すように、過去に SPF レコードが存在し、現在も継続して SPF レコードが登録されているドメインが多数存在する要因としては、本研究では、著者らが主観的に迷惑メールと判断したメールのヘッダ情報を解析対象としているため、違法ではない広告メール（CM）なども含まれている。大手企業から送信されている広告メールの多くは、SPF が適切に設定されている場合が多い。このようなメールが迷惑メールとして扱われたことにより、解析結果において、SPF 認証済みのドメインが複数存在している傾向が見られたと考える。

4.2 DKIM 検証結果

迷惑メールにおける DKIM 署名の有無についても、過去のメールヘッダと現在の DNS レコードとを照合することで検証を行った。結果を表 3 に示す。

表 3：迷惑メールにおける DKIM の検証結果と署名の有無

過去 / 現在	署名無し	署名あり
署名無し	11448	91
署名あり	0	0

表 3 より、迷惑メールの大部分は過去および現在のいずれにおいても DKIM 署名が付与されていないことが分かる。また、過去には DKIM 署名が確認された 91 通についても現在の DNS 上では対応する署名用の公開鍵が確認されなかった。これは当該ドメインの DKIM レコードが削除または変更された可能性が示唆される。

全体として、迷惑メールにおいて DKIM の署名は多くは確認されなかったが、これは認証技術の未実装、あるいは意図的な署名回避が示唆されるのではないかと考える。

4.3 比較考察

本研究では、送信ドメイン認証技術のうち SPF について、迷惑メールに対する認証状況の実態とその効果について調査・分析を行った。SPF 認証が「Pass」と判定されたドメインのうち、約 256 件（表 2）が現在も正しく SPF レコードを保持しており、当該ドメインの運用が継続していることが確認された。一方で、認証時に使用されたドメインが既に存在しない、あるいは SPF レコードが設定されていないケースも一定数存在していた。これらは、ドメイン運用の終了や、SPF 設定の放棄といった要因によるものと考えられ、SPF の信頼性が時間とともに変化する可能性を示唆している。

また、迷惑メールであっても SPF 認証に「Pass」している例が少なからず存在した。これは、迷惑メール送信業者が独自に取得したドメインに対し、正規の SPF レコードを設定したうえでメールを送信している可能性があることを意味する。このようなケースでは、SPF 検証を通過することで受信者側の迷惑メールフィルタを回避しようとする意図が見られると考える。また違法ではない広告メールなども含まれていることが要因だと考える。一方で、「None」や「Neutral」、「Softfail」といった判定も観測されており、必ずしも明確に拒否される認証結果ばかりではないことも明らかとなった。

これらの結果から、SPF が単体で迷惑メール判定の決定的な基準となるわけではなく、その限界も存在することが分かる。特に、SPF は IP アドレスに依存した技術であるため、転送によりドメイン名と IP アドレスの対応関係が変わると、SPF の認証結果は「Fail」となる[10]。また、「Pass」となっていても送信内容が悪質である可能性は否定できず、SPF はあくまで「送信元 IP が正規であるかどうか」を検証する仕組みにすぎない。そのため、SPF による認証結果のみでメールの安全性を判断することには慎重さが求められる。

一方、DKIM については、過去に署名があったと判定されたドメインはわずか 91 件であり、それらは、現在は署名を持たない状態であった（表 3）。DKIM 署名が迷惑メールにおいて付与されていない傾向は確かに見られるが、その背景には複数の要因が考えられる。まず、DKIM の導入には一定の技術的ハードルがあることだと考える。例えば鍵管理の複雑さである。DKIM では公開鍵を DNS に安全に配置・維持する必要がある[11]。また、正規送信者が鍵を定期的に更新している場合は、迷惑メール送信側に鍵が漏洩したとしても悪用されないというメリットがある一方で、過去の署名との不一致が生じやすい。これが「DKIM の持続性が低い」と見える原因にもなっていると考える。

加えて、DKIM は署名対象外のヘッダが改ざんされる可能性を残しており、なりすまし対策として万能ではない[4]。こうした技術的制限を熟知した迷惑メールの送信業者は、DKIM をあえて使用せず、他の手法を利用している可能性もある。さらに一部の迷惑メールは正規の配信サービスを悪用することで DKIM を通過することもあり、ドメイン認証のみで迷惑性を判断するには限界があることも示唆された。過去・現在ともに署名が存在しないケースが大多数を占めたが、迷惑メールにおける DKIM の有効性を検証するためには正規メールの DKIM 対応率も調査する必要があると考える。

以上の結果から、SPF は一定の有効性を保っているものの、その信頼性はドメインの維持管理に依存しやすく、DKIM に関しては鍵を更新することによって過去の署名と一致しない傾向が示唆されたと考える。ただし、これらの知見は、主観的に分類されたメール群に基づくため、完全な網羅性は担保されない。今後はより客観的な基準に基づく大規模データを用いることで、より一般化可能な知見の獲得が期待される。

4.4 SPF と DKIM の技術比較

SPF（Sender Policy Framework）と DKIM（DomainKeys Identified Mail）は、いずれもメール送信者の正当性を検証するための技術であるが、その仕組みと特徴には明確な違いがある。SPF は、送信元 IP アドレスと送信ドメインが許可された関係にあるかを DNS により確認するものであり、メールの配送経路に着目した仕組みである。これにより、なりすましをある程度防ぐことができるが、'Envelope From' アドレスに不正な送信者が所有するドメインを含めることで SPF を通過し、表示される 'From' アドレスに正当なドメインを偽装されてしまうという限界がある [12]。

一方、DKIM は、メール本文と選定したヘッダに対して送信者の秘密鍵による電子署名を付与し、受信者側が対応する公開鍵を DNS から取得して検証する仕組みである。これにより、メールが改ざんされていないことや、署名したドメインの正当性を確認することが可能となる。ただし、署名されていないメールを拒否するかどうかは運用ポリシーに依存するため、署名がない＝即スパムという扱いはできない。

本研究では、これらの技術的背景を踏まえ、SPF と DKIM のそれぞれがどのように迷惑メールに適用されているかを検証し、その活用状況の違いに着目した。特に、DKIM 署名の低頻度および現在の DNS との不一致は、運用上の難しさや、迷惑メール送信者側の対応コストの高さを示している可能性がある。

5. おわりに

本研究では、著者らに届いた実際の迷惑メールを対象に、送信ドメイン認証技術である SPF および DKIM について、過去のメールヘッダに記載した SPF、DKIM 情報と現在の DNS 情報を照合し、その有効性を検証した。SPF については、一定数のメールが過去に認証を通過しており、現在も正しい SPF レコードを保持していることが確認された。一方、DKIM に関しては、署名が存在する迷惑メールはごくわずかであり、現在も有効な署名を保持しているケースは確認されなかった。

これらの結果は、SPF は運用継続性が比較的高いこと、DKIM の有効性は運用次第で維持されないことがあるという特徴も示していると考える[13]。また、迷惑メールの分類には主観的な要素を含んでおり、現実の運用に即した形での分析を意識した点も、本研究の特徴である。ユーザーが迷惑と感じるメールの多くにおいて SPF や DKIM が設定されていなかったり、設定されていても一致しなかったりしたケースがあった。これは、ドメイン認証技術が、少なくとも主観的に「好ましくない」と感じられるメールをある程度弾くための基準となり得ることを示唆していると考える。

加えて、主観的基準による判定は、標準的なスパムフィルタでは検出されにくいが、ユーザー個人の感覚においては迷惑とされるメールにも適用される。こうしたメールがドメイン認証で弾かれているケースがあったことは、今後のフィルタリングのカスタマイズ性向上の示唆ともなり得る。と考えられる。

6. 今後の課題と展望

本研究は、著者らに届いた迷惑メールという限定的なサンプルに基づいているため、取得メールの網羅性や客観性に課題がある。また、DKIM の検証においては、セレクタ情報の欠落や、ドメインごとの運用ポリシーの違いによる影響も考慮する必要がある。これらを踏まえ、より信頼性の高い結果を得るには、今後以下のような取り組みが有効であると考えられる。

・より広範なメールの収集（期間・件数の拡大）
・正規メールへの解析
・メール受信者の趣味嗜好によらない、完全に法律違反である迷惑メールへの解析

今後も迷惑メールの手法は進化していくと考えられる中で、送信ドメイン認証の運用実態と有効性を継続的に評価し、どのような技術が現場に適しているかを検討していくことが求められる。

参考文献

[1] 林 治尚 、“迷惑メールはなぜ届くのか”、電気学会誌、128 巻 4 号、p.215~218 (2008) 。
[2] 櫻庭 秀次、依田 みなみ、清 雄一、田原 康之、大須賀昭 彦、“送信ドメイン認証を用いた送信者レピュテーション構 築手法の提案”、情報処理学会論文誌、Vol. 62、No. 5、pp. 1173 1183、May 2021。
[3] 田中 俊基、福山 雅深、山井 成良、北川 直哉、“利用者端末における DMARC を用いたなりすましメール警告システムの設計と実装” 、インターネットと運用技術シンポジウム 2015 、IOST2015、2015 年 11 月。
[4] 桜庭秀次、“定期観測レポート”、Internet Infrastructure Review (IIR)、 Vol. 47、 pp. 4-9、 Jun 2020。
[5] 北倉 奈菜、陳 春祥、“送信ドメイン認証を用いたスパムメール対 策の現状と解析”、2021 年度(第 72 回)電気・情報関 連学会中国支 部連合大会、2021 年 10 月 23 日。
[6] 陳 春祥、下馬場 もえ、 “深層学習を用いた電子メールの自動分類”、2024 年情報科学技術フォーラム(FIT)、2024 年 9 月 6 日。
[7] 東角 芳樹、伊豆 哲也、武中 正彦、吉岡 孝司、“部分完全性保証技術 PLAT:送信ドメイン認証への適応”、情報処理学会研究報告、2007 CSEC-38(49)、2007 年 7 月。
[8] D. Crocker, T. Hansen:RFC 6376: DomainKeys Identified Mail (DKIM) Signatures，Internet Engineering Task Force（IETF），2011 年，https://datatracker.ietf.org/doc/html/rfc6376（2025 年 5 月 28 日参照）
[9] S. Kitterman:RFC 7208: Sender Policy Framework (SPF) for Authorizing Use of Domains in Email，Internet Engineering Task Force(IETF),2014 年,https://datatracker.ietf.org/doc/html/rfc7208（2025 年 5 月 28 日参照 ）
[10] 迷惑メール対策委員会：「SPF と転送の相性問題に対する解決案」、インターネット協会 https://salt.iajapan.org/wpmu/anti_spam/admin/operation/suggestion/spf-sugg_a02/ （2025 年 5 月 28 日参照）
[11] Allman, E.: “DomainKeys Identified Mail (DKIM) Development, Deployment, and Operations”,RFC 5863，IETF，2010 年 5 月，https://tex2e.github.io/rfc-translater/html/rfc5863.html （2025 年 5 月 28 日参照）
[12] Proofpoint, Inc.: “Sender Policy Framework (SPF)とは何か”、https://www.proofpoint.com/us/threat-reference/spf （2025 年 5 月 28 日参照）
[13]迷惑メール対策推進協議会『迷惑メール対策マニュアル（第 3 版）』、一般財団法人 日本データ通信協会、2022 年、https://www.dekyo.or.jp/soudan/data/anti_spam/meiwakumanual3/manual_3rd_edition.pdf (2025 年 5 月 28 日参照）