送信ドメイン情報を利用した迷惑メール対策

開沼　和広*

Unsolicited email using sending domain information Countermeasures

Kazuhiro Kainuma*

要旨: Google が提供する Gmail で迷惑メール対策に焦点があてられた昨今，迷惑メール対策として３つの方法が取られているが，それらの解説と学内サーバーではどういった設定を施しているかを報告する．
キーワード: SPF，DKIM， DMARC，オンプレミス，Google®，Gmail®

1.　はじめに

インターネットサービスの根幹を担うサービスの1つとして，電子メールサービスが挙げられる．SNSが台頭し，レガシーなサービスと捉えられがちだが，電子メールは未だに重要なツールである．しかし，迷惑メールが大量に出回る昨今，当校でも迷惑メール対策として procmail 等を導入したりして業務に支障が出ないようにするものの，迷惑メールは後を絶たない．

今年1月に，神奈川県公立高校入試のインターネットを使った出願に Gmail®が使えないという報道があった．これは Gmail®のアドレスでネット出願をした受験生に対し，神奈川県教育委員会のアドレスから発信されたメールが出願した受験者にメールが届かなかったというものだ．これは Gmail®を運用している Google®の迷惑メール対策ガイドラインに抵触したため，メールの配送がされなかったものだが，当校でも1月に発生したので，その Google®に対する経緯と Gmail®対策を踏まえ，ここに報告する．

2.　Google®の迷惑メール対策方針

公式発表にて，2024 年 2 月以降，Gmail®アカウントに 1 日あたり 5,000 件を超えるメールを送信する送信者に対し，送信メールを認証すること，未承諾のメールまたは迷惑メールを送信しないようにすること，受信者がメールの配信登録を容易に解除できるようにすることが義務づけられた．

しかし，公式発表より早い段階で当校より Gmail®に対してメールが送れなかったことから，2024 年 2 月を待たずして Google®のルールを適用されたか，独自のブラックリストがあり，それに載せられてしまったために当校から Gmail®アドレスに届かなかったかの，どちらかと考えられた．

3.　当校が直面した問題

昨年 11 月頃から，非常勤講師の Gmail ®アドレスに届かない，また，独自アドレスの他の非常勤講師の方にメールが送れないという相談があった．

”gmail.com”であればすぐに送れない理由が分かるのだが，独自アドレスの非常勤講師の方はメールサーバーとして，法人向けクラウドサービスの Google Workspace ®を使っているかどうかをお聞きする必要があった．もし，Google ®のメールサーバーを使っていないにも関わらず，当校のドメインからメールが送信できないという場合は，当校のメールサーバーに何らかの障害が発生していることになる．幸いにして，当校からメールが届かない独自アドレスの非常勤講師の方 2 名は，どちらの方も Google®のメールサーバーを利用していたことが判明した．

4.　問題の解決方法

4.1　SPF(Sender Policy Framework)

インターネットでメール送信に使用されるプロトコルである SMTP (Simple Mail Transfer Protocol) は，差出人のメールアドレスを自由に設定することが可能である．このため，送信元メールアドレスを偽った「なりすましメール」を簡単に送ることができてしまい，これが現在まで迷惑メールとして多く利用されてきた．

SPF は，こうしたメールアドレスにおける，なり

*山形県立産業技術短期大学校庄内校
〒 998-0102 酒田市京田三丁目 57-4
*Shonai College of Industry & Technology
3-57-4 Kyoden,Sakata City,Yamagata,998-0102,Japan

すましを防ぐための技術の一つで，DNS を利用するのが特徴として挙げられる．ドメインを SPF に対応させるには，そのドメインのプライマリ DNS の正引きゾーンデータに SPF レコードという情報を追加する．SPF レコードには，そのドメイン名を送信元としてメールを送るサーバの IP アドレス等を記述する．以下の記述は，当校のプライマリネームサーバーの，インターネット向け正引きゾーンファイルに記述した SPF レコードである．

```
shonai-cit.ac.jp. IN TXT "v=spf
+a:mail.shonai-cit.ac.jp  +mx
+ip4:210.156.xxx.xxx
include:_spf.google.com ~all"
```

一方，SPF に対応したメール受信サーバは，メールの受信時にそのメールの送信元となっているドメインの SPF レコードを DNS で問い合わせる．送信元のサーバが SPF レコード中で許可されていない場合は，送信ドメインの詐称が行われたと判断し，最もスタンダードな対処としては，受信を拒否する処理を行う．

つまり SPF は，送信元サーバの IP アドレスと DNS を利用して，あらかじめ想定された送信元以外からのなりすましメールを検出できるようにする機構で，より多くのドメインがこの仕組みに対応することで，その効果が高くなる．以下の図 1 が SPF 検証の仕組みを説明した概略図である．

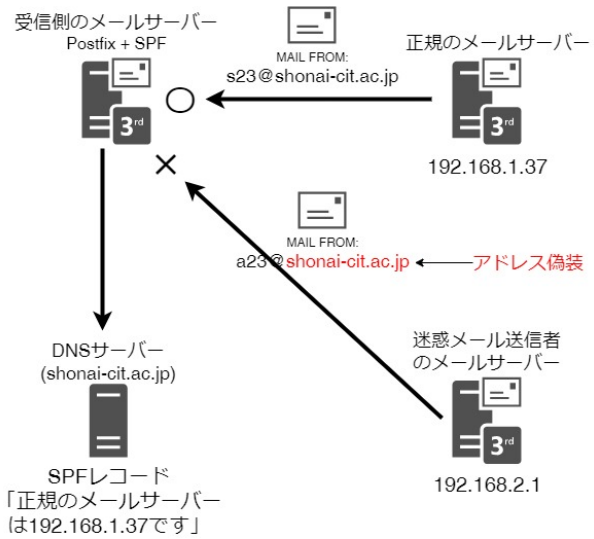

図 1: SPF 検証の概略図
Fig.1: Diagram of SPF verification

4.2 DKIM(DomainKeys Indentified Mail)

DKIM は，電子メールにおける送信ドメイン認証技術の一つであり，メールを送信する際に送信元が電子署名を行い，受信者がそれを検証することで，送信者のなりすましやメールの改ざんを検知できるようにするものである．

送信ドメイン認証技術は，送信元の IP アドレスを利用するものと，公開鍵暗号化方式を使った電子署名を利用するものがあり，DKIM は後者の方法で，送信元の秘密鍵を利用して電子署名を施してから相手側にメールを送信し，受信したメールサーバーが，送信元ドメインのプライマリ DNS サーバに公開鍵を要求し，DKIM 認証が実行された後，公開鍵と秘密鍵が一致することを検証する．図 2 に DKIM の仕組みについて示す．当校でのプライマリネームサーバーの正引きゾーンファイルの TXT レコードは以下のように記述している．

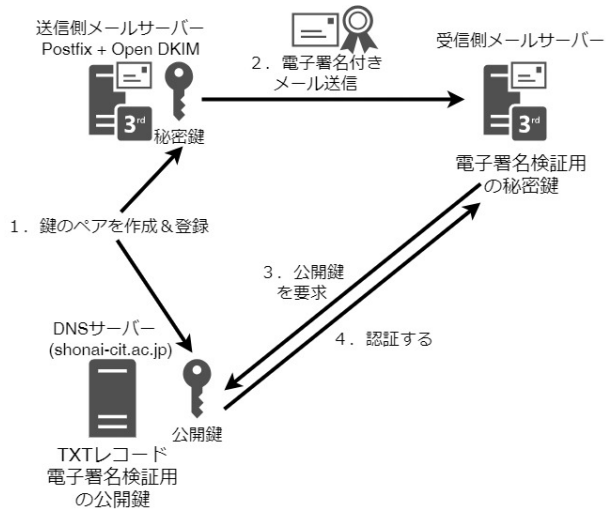

図 2: DKIM の概略図
Fig.2: Diagram of DKIM

```
240124._domainkey IN TXT "v=DKIM1; k=rsa;
""p=MIGFMA0G.........(途中略).......QAB"
```

ここで，v は DKIM のバージョンを表すため”DKIM1”を入れる．k は電子署名の鍵の形式を表し，現在は RSA 形式のみサポートしているため，RSA が値として入る．p に入る値は Base64 でエンコーディングされた公開鍵データを表す．

図 2 の”240124”の箇所はセレクタと呼ばれるもので，DKIM に対応するために設定をした日付を入れることが慣例的になっているようである．なお，筆者は”240124._domainkey”とだけ記述すればいいの

だが，240124._domainkey.shonai-cit.ac.jp．という記述ミスをしてしまった．

4.3 DMARK(Domain-based Message Authentication , Reporting, and Conformance)

同じ送信ドメイン認証技術でも送信元の IP アドレスを利用する SPF と，DKIM とを組み合わせた DMARC と呼ばれるメール認証技術の導入に伴い，DKIM の普及が進んでいる．図 3 に動作の概要を示す．DMARC は，電子メールの”送信者なりすまし”

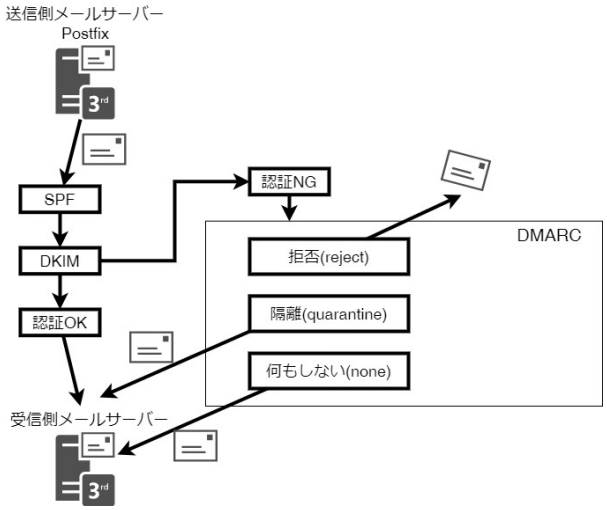

図 3: DMARC の概略図
Fig.3: Diagram of DMARC

や”メール内容の改ざん”といった不正を防ぐ事を目的とした，セキュリティ技術の 1 つである．我々はメール受信時に誰から送られてきたのかを確認するために From 行を見るが，SPF のところで触れたとおり，この From 行を詐称することが簡単に誰でもできてしまうため，”送信者なりすまし”が簡単にできてしまう．これによる悪影響は，なりすまされた個人や企業が大きく信用を失ってしまう可能性がある． この問題に取り組みため，Google ®，Facebook，Microsoft ®らが合同でなりすましメールやフィッシング対策のために”DMARC.org”を立ち上げた背景がある．

当校でのプライマリネームサーバーでの正引きゾーンファイルの DMARC に関する TXT レコードは，以下のように記述している．

```
_dmarc IN TXT "v=DMARC1; p=reject"
```

ここでタグ v は DMARC のバージョンを表し，通常は”DMARC1”とする．タグ p については認証に失敗したメールの処理方法を，none(何もしないでそのまま通す),quarantine(隔離),reject(拒否) の 3 つから選べるのだが，none の設定では Google®へはメールが送信できないようで，reject を指定すると Google®へメールを送る事ができた．

4.4 当校のメールサーバーの設定

当校のメールサーバーは Almalinux9.2 で構築し，このサーバー上にメール送信プログラムとして Postfix を使用しているので，main.cf ファイルに以下の行を加えてメールサーバーを再起動した．

```
smtpd_milters = inet:127.0.0.1:8891
non_smtpd_milters = $smtpd_milters
milter_default_action = accept
```

DKIM を有効にするため，以下の手順で作業した．

1. OpenDKIM のインストール後に公開鍵と秘密鍵のペアを作成する．
2. 上記の DKIM の節でも説明したが，公開鍵をプライマリネームサーバーに登録する．
3. ADSP レコードをプライマリネームサーバーに登録する．これは DKIM 認証に失敗した場合の取扱いを送信者側として宣言しておくための TXT レコードである．
4. /etc/opendkim.conf の編集をする．
5. /etc/opendkim/KeyTable に秘密鍵を登録する．
6. /etc/opendkim/TrustedHosts を確認する．
7. /etc/opendkim/SigningTable に `"_domainkey.shonai-cit.ac.jp"` 等の必要情報を追記する．
8. OpenDKIM を起動する．

これで設定が完了し，DKIM の動作がすると考えていたがエラーが発生し，DKIM 認証が行われなかった．これは 6. のところで opendkim.conf ファイルに，TrustedHosts と InternalHosts がデフォルト設定のままだとエラーが起こるため，それぞれ別々に指定するべきだったことが分かった．具体的に opendkim.conf には

```
ExternalIgnoreList refile:/etc/opendkim/
TrustedHosts
InternalHosts refile:/etc/opendkim/Internal
Hosts
```

と記述し，TrustedHosts には

```
127.0.0.1
::1
```

と記述し，InternalHosts には

```
0.0.0.0/0
::1
```

と記述したところ，DKIM 認証が無事に通った．

4.5 Google®の対応

まず，1 月 25 日に SPF,DKIM,DMARC の対応を終え，外部サイトへのメール送信で 3 つの認証の確認をした．外部サイトには Yahoo!メールを利用し，受信したメールを開くと，ヘッダーの部分に”このメールの認証情報”というところがあるので，そこをクリックすると図 4 の画面が表示された．

Google®に対して”当校のドメインがブラックリストに載っているならば，それを解除し，当校からのメールを受け取れるようにして欲しい”と伝えた (図 5 参照)．Google®のサポートセンターは英語のみの受付だったが，その返答は”対応に少なくても 2 週間は欲しい”ということだった．実際には 2 週間に満たない 2 月 6 日に、Gmail®や Google®のメールサーバーを利用している、独自アドレスを持った非常勤講師の方にメールが送ることができるようになった．

図 4: 外部サイトへのメール送信時の認証
Fig.4: Authentication when sending e-mail to external sites

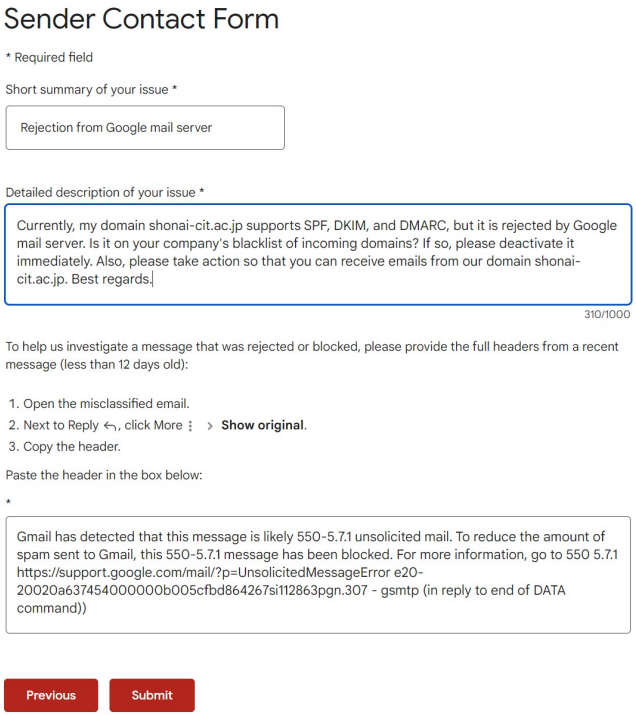

図 5: Google®への要請
Fig.5: Request for Google—®

5. おわりに

今回の Google®による迷惑メール対策は社会現象の一つとなり，システム管理者としても考えさせられることが多かった．迷惑メール対策の考え方について，筆者は受信側で最大限努力をするべきであり，当校では procmail を導入したり，迷惑メールの統計をとり，procmail のレシピに活かそうと考えている．

迷惑メール対策の考え方として Yahoo!メールの運用ポリシーが最も共感出来る．筆者は当該メールを 20 年以上使用しているが，迷惑メールで困った事は一度もない．迷惑メール対策としてフィルタが優秀であり，かつフィードバックに優れているため，高い迷惑メール撃退率を誇っていると思われる．基本的にはどんなメールも受け入れ (それこそ SPF,DKIM,DMARC の対応が取られていない組織からのメール)，勝手にメールを破棄したり，拒否するということをせず，それでなお利用者の利便性を損なわないという，高い次元でのメール運用ポリシーは賞賛すべきものだと思われる．

参考文献

一般社団法人　日本ネットワークインフォーメーションセンター