

DKIM の導入と DMARC による評価

奥田 剛¹⁾

1) 大阪大学 大学院工学研究科

okuda@eng.osaka-u.ac.jp

Introduction of DKIM and its Evaluation with DMARC

Takeshi Okuda¹⁾

1) Graduate School of Engineering, Osaka University

概要

スパムメールなどのなりすましメールの増加に伴い、大手メールサービスプロバイダを始めとして、送信ドメイン認証技術を用いたメールフィルタリングが強化されてきている。これまで SPF のみを用いて送信ドメイン認証を行っていた組織も、DKIM や DMARC の導入がこれまでよりも強く求められるようになってきた。そこで、筆者が所属する組織では、これまで行っていた SPF に加えて DKIM 及び DMARC を導入し、その評価を行った。導入に当たっては、postfix や opendkim などのオープンソースソフトウェアを利用した。送信メールのうち、SMTP 認証を経たものに対して DKIM 署名を付加するように設定し、DKIM の公開鍵と DMARC に関する DNS レコードを設定した。DMARC の Aggregate Report から統計情報を得ることで、DKIM 署名の付加により、正規の送信者からのメールをより多くの受信者に届けることができるのを確認した。また、送信メールに対する Aggregate Report の割合が低いことも確認した。

1 はじめに

スパムメールやフィッシングメールなどのなりすましメールの増加に伴い、送信者アドレスを詐称したメールの抑制を目的とする、送信ドメイン認証技術を用いたメールフィルタリングが、大手メールサービスプロバイダを中心として強化されてきている [1, 2]。筆者が所属する組織では、管理運用するメールサーバで関連組織のメールアドレスを多数ホスティングしており、約 1 万のメールアドレスをサービスしている。これまで送信ドメインの DNS に Sender Policy Framework (SPF) レコードを設定することにより、学内 IP アドレスから送信されたメールのみ送信ドメインを認証していた [3]。しかし上記の送信ドメイン認証に基づくメールフィルタリング強化により、SPF レコードのみを設定している組織では宛先ユーザに受信されない事態が多発している。ある送信者アドレスを持つメールが、元の宛先アドレスから別の宛先アドレスに転送される際に、送信ドメインの SPF で指定されている IP アドレス以外から送信されているように見えるからである。そのため、最終的にメールを受信するサーバにおいて、SPF の認証に失敗する。これまで SPF 認証に失敗しても受信者に配送されることが多かったが、最近は SPF 認証に失敗したメールは破棄さ

れるようになってきている。

これまでこのような事態は、受信ユーザがメールの不達を申告することで初めて明らかになっていたが、Domain-based Message Authentication, Reporting, and Conformance (DMARC) の普及に伴って、受信者側サーバから送信ドメインに送られてくるレポートにより、受信者側サーバでどのような扱いを受けているかを送信側で知ることが可能になった [4]。しかし、SPF 単体の設定では、受信側メールサーバにて破棄されたメールが、正規の送信者からのメールを転送したことによるものか、第三者による送信者アドレス詐称によるものかの区別がつかないため、DomainKeys Identified Mail (DKIM) の導入も必要となる。送信メールに DKIM 署名を付加することにより、送信先において転送された場合でも、転送先で署名を検証することで送信ドメインを認証することができるからである [5]。受信側のポリシーにもよるが、SPF 認証と DKIM 認証の少なくともどちらか一方が成功すれば受信されることが期待できる。本稿では、筆者の所属する組織で管理運用するメールサーバにおいて、送信メールに DKIM 署名を付加することによる、受信側での扱いの変化を、DMARC の Aggregate Report を用いて評価したので報告する。

以降 2 章において SPF、DKIM、DMARC の概要、

3 章において DKIM の導入と DMARC の設定に関する説明、4 章において DMARC による評価の順に説明し、5 章で結果について考察する。

2 SPF、DKIM、DMARC の概要

増加し続ける送信元アドレス詐称メールを抑止するため、これまで様々な送信ドメイン認証技術が提案されてきた。そのうち、現在最も多く導入されているのが、SPF および DKIM、DMARC である。

2.1 Sender Policy Framework (SPF) の説明

メールの送信者アドレスは送信者が自由に設定できるため、送信者アドレスを詐称したスパムメールが横行している。送信者アドレス詐称を防止するため、送信ドメインの DNS で、送信側メールサーバの IP アドレスを指定することで、他の IP アドレスからの送信者アドレス詐称を抑制するのが Sender Policy Framework (SPF) である [3]。SPF は導入が容易であるため、多くの組織で採用されている。

送信元メールアドレスドメインの権威 DNS サーバに、SPF レコードと呼ばれる TXT レコードを公開するのみで、そのドメインを送信者アドレスとして持つメールは指定した IP アドレスのサーバから送信されることを示唆できる。受信側メールサーバでは、直接通信した送信元 IP アドレスが、送信者メールアドレス (envelope from) のドメインの SPF レコードに指定された範囲にあるかを検証し、入っていれば SPF 認証に成功し、入っていない場合は SPF 認証に失敗する。受信側メールサーバは、認証結果とポリシーに基づいてメールを受信するか、破棄するかの扱いを決定する。

例えば図 1 の上側のフローであれば、送信者 A から受信者 B に直接配送され、IP アドレス 1 が SPF レコードで宣言されているため認証が成功する。図 1 の下側の例では、宛先 B' 宛のメールを受信者 B のメールアドレスに転送しており、転送先の受信側サーバでは受け取ったメールの送信元 IP アドレス 2 が SPF レコードの範囲に含まれないため SPF 認証が失敗する。SPF 認証に失敗したメールは、受信側ポリシーにより、受信者に配送されることも破棄されることもある。

2.2 DomainKeys Identified Mail (DKIM) の説明

上記の転送シナリオでは SPF 認証が失敗するため、送信者側サーバで本文と各種ヘッダ情報に対する電子署名を付加する DomainKeys Identified Mail (DKIM) が提案された [5]。受信側サーバでは、受信したメールのヘッダに含まれる DKIM 署名を検証することにより、メール送信者の真正性を検証できるようにする技

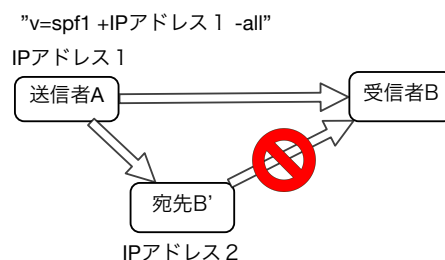


図 1 SPF 認証が成功する場合（上）と、転送により失敗する場合（下）

術である。DKIM の利用に際して、まず送信ドメインにおいて、ヘッダに署名する公開鍵を権威 DNS サーバの TXT レコードとして公開する。送信者側メールサーバでは、送信するメールの本文およびヘッダ情報からハッシュを計算し、秘密鍵でハッシュに対する電子署名を作成し、メールのヘッダに DKIM 署名として付加する。受信側メールサーバでは、受信メールの本文およびヘッダ情報からハッシュを計算し、付加された DKIM 署名を DNS の TXT レコードで公開されている公開鍵で検証する。検証が成功すれば、DKIM 認証が成功し、当該ドメインが管理するサーバから送信されたものであると認識する。

我々の観測では、最近の大手メールサービスプロバイダでは、SPF と DKIM のいずれかの認証に成功すれば、ユーザに配送し、両方に失敗すれば破棄するポリシーとなっているところが多い。上述の転送シナリオ等を考慮し、SPF と DKIM の両方を適切に設定することが推奨されている。

2.3 Domain-based Message Authentication, Reporting, and Conformance (DMARC) の説明

これまで、送信者アドレスが詐称されていることは、エンドユーザからの申告以外に送信ドメイン側で知ることはできなかった。Domain-based Message Authentication, Reporting, and Conformance (DMARC) を導入することで、受信側メールサーバから送られてくるレポートを調査することで、送信ドメインとして認証していない IP アドレスから、送信者アドレスを詐称したメールの存在を統計的に知ることができる [4]。DMARC では、送信ドメインの権威 DNS サーバの TXT レコードに、DMARC ポリシーやレポートの送り先メールアドレスを指定する。受信側サーバは送信ドメインのポリシーを参照し、認証に失敗したメールに対するアクションを決定する。そして受信したメールに関する統計的なレポート (Aggregate Report) を、指定された宛先に 1 日単位でメールで送信する。

Aggregate Report は XML 形式で記述されており、処理したメールの送信ドメインと送信元 IP アドレス、SPF 認証と DKIM 認証の結果、件数が記載されている。この Aggregate Report は、受信メールアドレス毎、送信ドメイン毎に送られるため、複数の送信ドメインをホストしている送信側の管理者は、毎日多数の Aggregate Report のメールを受け取ることになる。

3 DKIM の導入と DMARC の設定

筆者の所属する組織のメールサーバでは関連する組織のドメインを多数ホスティングしている。このメールサーバは学内に設置されており、これまで DNS の SPF レコードで学内 IP アドレスのみを送信側メールサーバの IP アドレスとして指定してきた。SPF の TXT レコードでは、送信ドメインとして認証する送信メールサーバの IPv4 アドレス及び IPv6 アドレスのみ記載し、それ以外は除外する -all としている。しかし、SPF だけでは受信側で SPF 認証に失敗したメールが、正規のメールが転送されて SPF 認証に失敗したのか、悪意のある第三者にアドレス詐称されて失敗したのかが不明である。

そこで、DKIM を導入し、送信するメールのヘッダに DKIM 署名を付加するようにした。利用したのはオープンソースソフトウェアの postfix [6] と opendkim [7] である。送信サーバの postfix で受信したメールのうち、SMTP AUTH で送信者認証したものを opendkim に渡す。opendkim では、From ヘッダにホスティングしているドメインが含まれているメールに対してのみ DKIM 署名を付加するように設定している。DKIM 署名の対象ヘッダは RFC6376 の推奨項目を参考に設定している [5]。あらかじめ、ホストしているすべてのドメインに対する DKIM 署名用の秘密鍵・公開鍵ペアを openssl で作成し、公開鍵を DNS の TXT レコードとして登録している。

DMARC のポリシーは、レポートを受け取ることを目的として、p=none に設定し DNS の TXT レコードに登録している。これは認証に失敗したメールに対して、何もしないよう受信サーバに要求するものである。同レコードの rua に指定したメールアドレス宛に、受信側からの Aggregate Report が送られてくる。これらの設定を表 1 にまとめている。

4 Aggregate Report による評価

上記の通り、SPF の宣言と送信サーバによる DKIM 署名を設定し、DMARC に従って送信されてくる Ag-

表 1 SPF、DKIM、DMARC の設定

SPF	"v=spf1 +<関係する IPv4 及び IPv6 アドレス>-all"
DKIM	"v=DKIM1; h=sha256; k=rsa; p=<公開鍵>" SMTP-AUTH 経由のメールで、 かつホスティングしているドメイン からのメールのみ署名 署名対象は From, Sender, To, CC Subject, Message-Id, Date
DMARC	"v=DMARC1; p=none; rua=<メールアドレス>"

gregate Report を用いて DKIM 署名の効果を検証する。検証期間は 2023 年 10 月 1 日から同年 12 月 2 日までである。10 月 1 日から 10 月 14 日までの 2 週間は DKIM 署名を付加せず、10 月 15 日以降は DKIM 署名を付加する設定にしている。前述の通り、毎日多数の Aggregate Report が受信サーバから送られてくるため、SaaS 型 DMARC 分析サービスである PowerDMARC [8] に Aggregate Report を集約して集計し、評価する。

4.1 DKIM 署名による DMARC 非準拠率の低減

DMARC の Aggregate Report からは、SPF 認証と DKIM 認証それぞれの成否がわかるため、両方に成功した場合といずれか一方に成功した場合は送信ドメイン認証に成功したことになる。

SPF、DKIM 両方の認証が失敗し、DMARC 非準拠と判断されたメールの割合を図 2 に示す。図中の赤い線は日毎の非準拠率、黒い横線上の数値は非準拠率の 7 日間の平均である。DKIM 署名を設定していない初めの 2 週間の非準拠率の平均は約 23.2% であった。10 月 15 日以降、DKIM 署名を設定している期間の非準拠率の平均は約 14.6% で、DKIM 認証のみに成功している率が約 7.4% となっていた。SPF のみでドメイン認証を行っていた時には、転送するサーバの IP アドレスが送信ドメインの SPF に入っておらず認証が失敗していたが、10 月 15 日以降 DKIM 署名が付加されたことで、おおよそ DKIM 認証のみに成功した分だけ非準拠率が低減したと考えられる。

さらに図 2 からは、DKIM 署名を付加することで、転送メールによるドメイン認証失敗が少なくなり、日毎の非準拠率が全体的に低くなっているのがわかる。それにより、アドレス詐称による DMARC 非準拠が

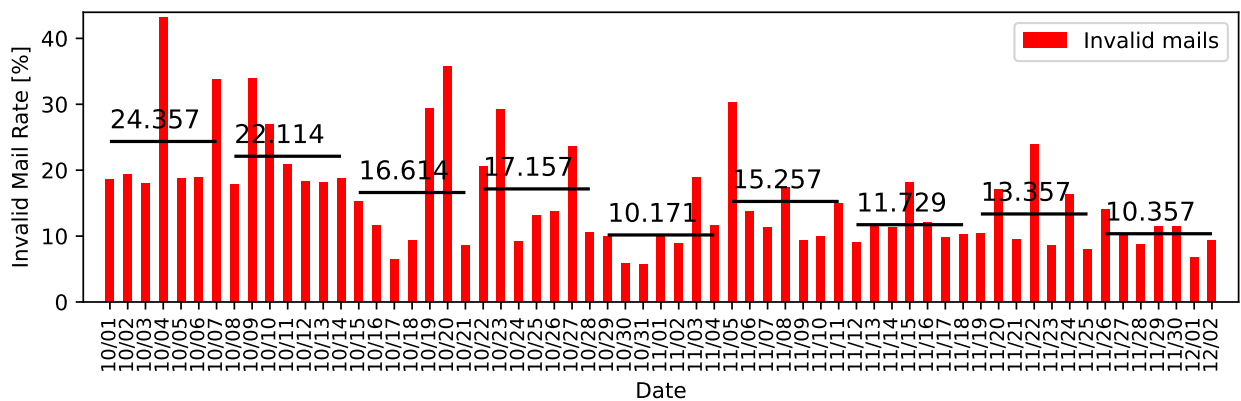


図2 DMARC の Aggregate Report から算出した DMARC 非準拠メールの割合

際立つようになった。図中で非準拠率が7日間平均よりも高い日には、関連学会や本学関係団体が管理するメールサーバから、本学のメールアドレスを利用してメールを送信したことによる送信ドメイン認証の失敗が多数発生していたことを確認している。本検証の期間外ではあるが、非準拠率が50%を超える日には、海外のサーバから本学のメールアドレスを詐称したスパムメールが多数送信されていたことも確認した。これらは、Aggregate Reportに含まれる送信元IPアドレスと、スパムブロックリストやWHOISサービスなどから調査することが可能である。

4.2 DMARC Aggregate Report の回答率

2023年9月からの、自サーバが外部に送信したメール件数に対するAggregate Reportによって報告されたメール件数の月毎の割合を図3に示す。DMARCを設定した2023年9月はレポートの割合が約10.5%であったが、レポートの割合が徐々に増加し、12ヶ月間の平均は約14.6%、最大約16.3%であった。DMARCのAggregate Reportを送信する組織が徐々にではあるが増えてきていると推測される。外部のメーリングリストへの配信など、送信サーバで把握できていないメール送信や、スパムメールなど送信元アドレスを詐称したメールに対する報告数の増加などがあるため、送信に対する報告の正確な割合ではないことには注意が必要である。受信側サーバがSPFとDKIMによるドメイン認証に対応していても、DMARC Aggregate Reportの作成と送信に対応していない、あるいは返信する設定にしていないなどの理由により、レポートの回答率が低い値に留まっていると推測される。DMARCのAggregate Reportを作成して送信するためには受信側サーバの計算機資源を必要とするため、送信を抑制している可能性がある。

5 考察

これまで転送先で送信ドメイン認証に失敗していた転送メールが、DKIMを導入することにより、送信ドメイン認証が成功するようになり正常に受信されることをDMARCのAggregate Reportから確認できた。また、送信者メールアドレスを詐称したスパムメールの発生を送信側で確認できるようになった。図2から、DMARC非準拠のメールが依然10%程度観測されているが、送信者認証を経ずに学内ドメインを利用してメールを送信している本学関係の学外サービスや計測機器などがあることもAggregate Reportから明らかになった。DKIM署名が付加された正規のメールであっても、メーリングリストなどでSubjectなどのヘッダの一部が書き換えられる場合、受信側でDKIM署名の検証に失敗して破棄されることがあることも、Aggregate Reportと各種ログの突合で分かった。

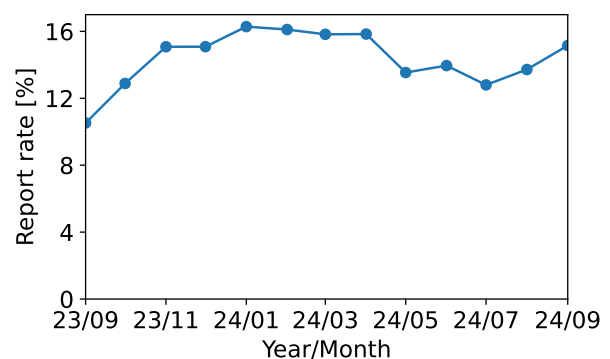


図3 外部に送信したメール件数に対する受信したAggregate Reportの割合

6 まとめと今後の課題

DKIMを導入することで、正規の送信者からのメールをより多くの受信者に届けることが可能になり、そのことをDMARCのAggregate Reportから確認することができた。

今後、DMARCのポリシーをより厳格なp=rejectに設定することで、アドレス詐称メールを受信されなくするようにする予定であるが、より厳格なDMARCポリシーに移行するためには、前述の本学が関係する団体に対して、ポリシーに従ってメールを送信するように調整する必要がある。また、筆者の所属する組織がホストするドメインにおいて、メール受信に用いているアプライアンス型メールゲートウェイがDMARCのAggregate Report送信に対応していないため、Aggregate Report送信に対応するよう変更する必要がある。DKIM署名とメーリングリストなどによるヘッダ書き換えに関する問題は、Authenticated Received Chain (ARC)を導入することで一部回避可能である[9]。しかし、ARCの運用に関していくつかの問題が指摘されているため[10, 11]、導入に際しては注意が必要である。

参考文献

- [1] Google, Email sender guidelines,
<https://support.google.com/a/answer/81126>, Accessed 2024/10/16.
- [2] Yahoo, Sender Requirements & Recommendations,
<https://senders.yahooinc.com/best-practices/>, Accessed 2024/10/16.
- [3] Internet Engineering Task Force (IETF),
Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1, RFC 7208, 2014.
- [4] Internet Engineering Task Force (IETF),
Domain-based Message Authentication, Reporting, and Conformance (DMARC), RFC 7489, 2015.
- [5] Internet Engineering Task Force (IETF),
DomainKeys Identified Mail (DKIM) Signatures, RFC 6376, 2011.
- [6] The Postfix Home Page,
<https://www.postfix.org/>.
- [7] OpenDKIM, <http://www.opendkim.org/>.
- [8] Spelldata Inc., PowerDMARC,
<https://maildata.jp/>, Accessed 2024/10/16.
- [9] Internet Engineering Task Force (IETF),

The Authenticated Received Chain (ARC) Protocol, RFC 8617, 2019.

- [10] K. Shen et. al., Weak Links in Authentication Chains: A Large-scale Analysis of Email Sender Spoofing Attacks, In USENIX Security 21, pp. 3201–3217, 2021.
- [11] E. Liu, et al., Forward Pass: On the Security Implications of Email Forwarding Mechanism and Policy, In 2023 IEEE 8th EuroS&P, pp. 373-391, 2023.