nagoya-u.jp メールにおける DMARC 集計レポートの仕様準拠状況の調査

宇田川 暢

東海国立大学機構 情報環境部

udagawa@icts.nagoya-u.ac.jp

A Study on the Conformance of DMARC Aggregate Reports in "nagoya-u.jp Mail"

UDAGAWA Mitsuru

Information System Operations Division, Tokai National Higher Education and Research System

概要

筆者の管理する nagoya-u.jp メールにおいて、DMARC 集計レポートを収集、分析している。その分析作業において、DMARC の仕様への適合に問題があることに気づき、調査を行った。その結果について報告する。

1 はじめに

筆者らは nagoya-u.jp を送信元ドメインとするメールサービスの運用を行っている[1]。その運用の一環として、後述する DMARC を利用し、nagoya-u.jp を送信元とした成り済ましメールの調査と対応を図っている。

2 送信ドメイン認証と DMARC

2.1 送信ドメイン認証

送信ドメイン認証技術は、メールの送信元として他のドメインに成りすますことを防ぐ技術である。受信者側で対応を行うスパムフィルタやグレイリスティングと異なり、送信側が正当なメールを送る手段を予めポリシーとして宣言する必要がある。受信者は受信したメールについて、宣言されたポリシーと合致するかを迷惑メール判定の要素の一つとして利用することができる。

2.2 SPF、DKIM および DMARC

nagoya-u.jp メールでメール送信元として利用している nagoya-u.jp ドメインの場合、正当な送信元 IP アドレスの一覧を宣言する SPF[1]（Sender Policy Framework）は、nagoya-u.jp の TXT レコードを確認することにより SPF ポリシーの有無を確認できる。しかし、公開鍵による署名を利用して成り済ましや改竄を防ぐ DKIM[2]（DomainKeys Identified Mail）については、セレクタ部分を送信者側が任意に設定可能なため、メール受信者が単純に DKIM を未設定なのか、署名されていない成り済ましメールかを判別することができないという問題がある。

この問題について、ADSP[3]（Author Domain Signing Practices）と呼ばれる仕組みが存在し、指定された DNS の TXT レコードを確認することにより DKIM 利用の有無について宣言できるとされていたが、現在では DMARC[4]（Domain-based Message Authentication, Reporting, and Conformance）に置き換えられている。DMARC は ADSP の DKIM 利用の有無に加え、そのメールドメインを送信元と名乗るメールの取り扱いについてのポリシーを宣言することができるようになっている。

2.3 DMARC 集計レポート

DMARC で宣言するポリシーの中で、受信者からのフィードバックの受け取り方法を指定することができるようになっている。その一つが DMARC 集計レポート（Aggregate Report）であり、DMARC レコードを記載したドメインを差出人としたメールについて、受信者が接続元 IP アドレスと SPF ポリシーおよび DKIM の適合や、判定結果

[1] https://datatracker.ietf.org/doc/html/rfc7208

[2] https://datatracker.ietf.org/doc/html/rfc6376

[3] https://datatracker.ietf.org/doc/html/rfc5617

[4] https://datatracker.ietf.org/doc/html/rfc7489

を統計的な情報として、基本的に 24 時間ごとにレポートを作成し報告してもらう。このレポートには統計的な情報が記録されるだけで、メールの題名や具体的な送信者を特定する情報、From アドレスのローカルパート部などは含まれない。

2.4 DMARC 認証失敗レポート

また、DMARC 認証失敗レポート（Failure Report）も仕様上は受け取ることが可能だが、レポートに送信されたメール全体が含まれるという仕様のため、サービス利用者のプライバシー確保を理由として nagoya-u.jp メールでは利用していない。ただし、運用においてどのメールが DMARC ポリシー違反により到達しなかったかという情報が重要である場合は、認証失敗レポートを受け取ることが望ましい。

しかしながら、後述する先行研究によるとほとんどのメールサービスで DMARC 認証失敗レポートの送信には対応していないと報告されている。

3 DMARC 集計レポートの分析

nagoya-u.jp メールで DMARC 集計レポートを受信するように DMARC ポリシーで設定を行った後、届いた DMARC 集計レポートの分析に取りかかった。その際に、DMARC 集計レポートのフォーマットが単純であることから、既製の OSS や SaaS などを利用するのでは無く、自前で分析ツール「DMARC プロファイラ」を作成することとした。

DMARC プロファイラの機能のひとつを図 1 として示す。図 1 は左側を送信元または最終中継サーバ、右側を受信者としたサンキーダイアグラムとなっており、中間にある工程がそれぞれ SPF、DKIM、DMARC の認証結果となっている。

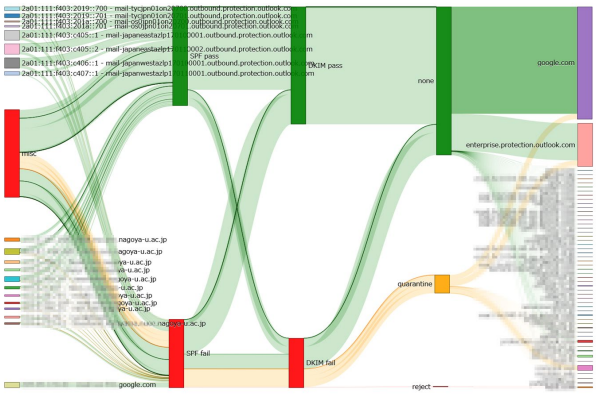

図 1 認証結果のサンキーダイアグラム
（画像のホスト名部分は一部加工している）

分析した DMARC 集計レポートの内容自体には特筆すべきものは無かったが、DMARC 集計レポートの送信元によっては、期待したような内容で送信を行っていないものがみられた。この点についてまとめ、報告を行う。

4 DMARC 集計レポートの仕様準拠

4.1 先行研究事例

DMARC レポートの仕様準拠について調査を行った先行事例として、Ashiq らによる報告[2]では、DMARC レコードの設定に対する、DMARC への対応および DMARC 集計レポートの実装の評価を行い、DMARC の実装不備による DDoS 攻撃の可能性に言及している。

Hureau らによる別の報告[3]では、より多くの MSP（Mail Service Provider）を対象に DMARC の実装を確認し、DMARC 集計レポートの Subject と XML のフォーマットについて調査、言及している。また、DMARC 集計レポートの送信に対応した MSP が少数で、DMARC 認証失敗レポートについては全てが対応していないという結果を示している。

4.2 調査手法と対象

今回、nagoya-u.jp メールにおいて受け取った DMARC 集計レポートについて、DMARC の仕様への準拠の調査を行った。つまり、nagoya-u.jp メールの利用者が正規の手段で送信したメール、および、サブドメインを含めた nagoya-u.jp のドメインを From アドレスに設定して送信された成り済ましメールなどを受信したメールサービスのうち、DMARC 集計レポートの送信に対応したもの（以下、報告ドメイン）が対象となっている。

そのため、以下のような内容は本調査の対象外となっている。

- DMARC ポリシーレコードの設定誤りなど、イレギュラーに対する挙動。
- rua タグに mailto: 以外を指定した場合での DMARC 集計レポート受信。
- ruf タグ指定時に送信される認証失敗レポートに関する事項。
- 外部ドメイン宛ての DMARC 集計レポートメール送信。

DMARC ポリシーを設定した 2024 年 1 月 26 日から 2025 年 8 月 26 日までに受信した DMARC 集計レポート計 7,853 通を調査対象としている。

5　調査内容

先述の DMARC 集計レポート分析ツールの作成にあたって、仕様への不適合が判明した部分を主に調査対象とした。なお、本章で単に「仕様」と記載した際は、RFC 7489 を指すものとする。

5.1　メールサブジェクト

メールサブジェクトについて仕様では” Report Domain: nagoya-u.jp Submitter: example.com Report-ID: <123.456>”のようなフォーマットとされているが、”Domain”が”domain”と小文字になっているもの、必要な空白が無いもの、Report-ID の値が Message-ID の書式を満たしていないものが多くみられた。本項目は SHOULD、つまり相応の理由があれば逸脱しても良いと規定されているが、報告ドメインによっては全く準拠しておらず、日本語で記述されているものすら存在した。

5.2　その他メールヘッダの問題

本項目は仕様で決められているものではないが、OpenDMARC の送信する DMARC 集計レポートのメールヘッダにおいて、Date フィールド[5]のフォーマットに問題がある[6]ことを確認している。

5.3　添付ファイルの Content-Type

マルチパートメールの添付ファイルの Content-Type について、添付ファイルが無圧縮の XML の場合は”text/xml”を、gzip 圧縮されたファイルの場合は”application/gzip”を使う事と規定されているが、仕様で言及されていない zip 圧縮され”application/zip”となっているものや、zip 圧縮、gzip 圧縮の両者で”application/octet-stream”となっているものが見られた。

gzip と異なり zip は複数のファイルを一つにまとめるアーカイブ機能を持っているが、DMARC 集計レポートでは利用する必要が無いはずである。

なお、無圧縮の XML を送信してくる報告ドメインは存在しなかった。

5.4　添付ファイルの名前

添付ファイルの名称については基本的に仕様で定められたフォーマットに従っているものの、zip 圧縮されたファイルを送信してきたものについては、拡張子が”.zip”となっていた。

また、ある報告ドメインで複数ある DMARC 集計レポートのうち 1 通だけ、ファイル名の報告ドメイン部分が抜けていたものがあった。

5.5 不正な XML フォーマット

DMARC 集計レポートの本体とも言える XML については、おおむね問題は無かった。ただし、先行研究のように XML 中の記述順などを詳細なチェックは行っておらず、XML の解析作業において発見したものだけとなっている。

一部の商用製品とみられるものから送信された XML の内容について、本来は”identifiers”となっているべき箇所が”identities”となっていた。また、PolicyOverrideReason について、値が空の場合にも関わらず”reason”を含めている報告ドメインがあった。

6　調査結果

6.1　報告対象の限定

全ての報告ドメインの名称を記載すると、nagoya-u.jp メール利用者が知られたくない送信先を明らかにしてしまう危険性があるため、先行研究で扱われた MSP に加え、クラウドメールセキュリティ（CES）を報告対象とした。CES はメールサービスの前段に設置することで、迷惑メール判定やアンチウィルスなどを提供する SaaS 型のサービスとなる。MSP と異なり、メールボックスそのものは提供していないサービスとなる。

6.2　解説

MSP および CES を結果から抽出したものについて表 1 として示す。調査対象期間中に DMARC 集計レポートの内容が変化したものについては、最新の状況を記載している。この表の項目の一部について必要と思われる説明を記載する。

GMO Internet Group としてムームーメールや hetemail など同グループ企業の複数社のサービスをまとめている。本来は個別に扱うべきだが、サブジェクトの Report-ID 部分に共通した特徴を持っており、同様のシステムを利用していると考えた。

KDDI については、同社の提供する dion.ne.jp、auone-net.jp、ezweb.ne.jp、au.com を含んでいる。

Microsoft については、Outlook.com だけでなく、Microsoft 365 のメールサービスである Exchange Online を含んでいる。

また、Yahoo は yahoo.com、aol.com のほか、複数国の Yahoo メールが含まれているが、Yahoo!

[5] https://datatracker.ietf.org/doc/html/rfc5322#section-3.6.1

[6] https://github.com/trusteddomainproject/OpenDMARC/blob/rel-opendmarc-1-4-2/opendmarc/opendmarc.c#L3392-L3393

Japanの提供するYahoo!メールは含まれていない。

7　まとめ

大手MSPであっても、DMARCの仕様に準拠していないものが多いことが明らかになった。些細な問題と思われるかもしれないが、DMARC集計レポートを受信し、内容を解析する際には障害となり、それぞれのケースに対して都度対応していく必要が出てくる。また、問題に気づかない場合、DMARC集計レポートの分析対象とならない可能性もある。結果として、DMARCを利用した迷惑メール対策に支障が出る可能性もあるため、MSPをはじめとしたサービス提供者は、公開されている仕様に真摯に向き合う必要があると考える。

参考文献

[1] 宇田川暢、”オンプレミスのメール転送サービスからMicrosoft 365を使ったメールサービスへの切り替えの試み”、 大学ICT推進協議会2024年度年次大会論文集、566-572、2024.

[2] Md. Ishtiaq Ashiq et al.、”You’ve Got Report: Measurement and Security Implications of DMARC Reporting”、SEC '23: Proceedings of the 32nd USENIX Conference on Security Symposium、Article No: 231、Pages 4123 - 4137、2023.

[3] Olivier Hureau et al. 、”Stress Testing the DMARC Reporting System: Compliance with Standards and Ways of Improvement”、CoNEXT '24: Proceedings of the 20th International Conference on emerging Networking EXperiments and Technologies、Pages 1 – 9、2024.

表 1　サービスごとの DMARC 仕様への準拠状況

分類	名称	サブジェクト (5.1)	Content-Type (5.3)	ファイル名 (5.4)	XML (5.5)
MSP	Amazon SES	×	×	×	○
	Bell Canada	○	○	○	○
	Comcast	○	○	○	○
	CYBERMAIL Σ	×	×	×	○
	emailsrvr.com	×	×	×	○
	Fastmail	×	○	○	○
	Google	×	×	×	○
	GMO Internet Group	×	○	○	○
	GMX	×	○	○	○
	GoDaddy	×	×	×	○
	KDDI	×	○	○	×
	Mail.ru	×	○	○	○
	mail.com	×	○	○	○
	Microsoft	×	○	○	○
	Mimecast	×	○	○	○
	NTT ドコモ	○	○	○	○
	OneOffice	○	○	○	○
	Seznam.cz	×	×	×	○
	SYNAQ	×	×	×	○
	Yahoo	○	○	○	○
	Zoho	×	○	○	○
CES	Cisco Secure Email	○	○	○	○
	Trend Micro Email Security	×	×	×	○
	使えるメールバスター	×	×	×	○

※RFC 7489 に適合していると思われる項目について○を、そうでないものは×としている。列名のカッコ中の数字は、対応する章番号を表している。