

第13部

電子メール基盤運用技術の高度化

コリー・ルーク、石原 匠

第1章 はじめに

Emailはインターネットにおける自律分散的なアプリケーションプロトコルとして、黎明期から利用されてきた。SNSやメッセージングサービスが普及した現在でも、送信相手のアドレスさえ知っていれば組織をまたいでコミュニケーションをとれる手段としてや、アドレスをサイバー空間における識別子として利用するために、Emailは広く利用されている。しかし、その特徴を逆手にとったスパムやフィッシングをはじめとする不正メールの発信は後を絶たない。

Trustworthy Emailワーキンググループ(以下、“本WG”)では、2021年度の設立時から、より信頼できるコミュニケーション手段としてのEmailを確立するため、Trustworthy Emailのシステム構築・運用・普及に向けた取り組みを行う。本稿では、2023年度の本WGの活動内容について記述する。

第2章 2023年の活動

2023年度は、3月と9月のWIDE合宿および5月と12月のWIDE研究会で、email BoFセッションを開催した。現状の電子メールに関連する議論を行い、企業や大学のメールサーバ管理者や一般利用者の観点で運用方針についてのディスカッションを行った。

3月に開催されたWIDE合宿では、日本大学の相川氏より「ホスト型S/MIMEの闇」というテーマで発表とnewsh.wide.ad.jpとLDAP関連の共有、smtp.wide.ad.jp関連の共有、ディスカッションを行った。

5月に開催されたWIDE研究会では、newsh.wide.ad.jp更新関連の共有、DMARC Reportの解析についてのディスカッションを行った。

9月に開催されたWIDE合宿では、WIDEメールの運用ポリシーに関するディスカッションと共に、昨今のIETFでのDMARCワーキンググループの動きや情報共有を行った。その後Googleと米Yahooのメールポリシー強化についての情報共有、WIDEでの必要な対応についてもディスカッションを行った。

12月に開催されたWIDE研究会では、これらのメールポリシー強化対応に関する進捗確認と残るタスクの確認を中心に議論を行った。また、11月にはGoogleと米Yahooのメールポリシー強化対応についての方針を決定するためのミーティングを開催し、具体的な対応策についての決定が行われた。

第3章 Googleをはじめとする企業のメールポリシー強化

Googleと米Yahooは、2024年2月にメールポリシー強化を行うことを宣言した。この変更は、WIDE Projectだけでなく、日本国内外の組織のメールに影響される内容であり、@gmail.com宛のすべて送信を行うメールが対象となる。ポリシー強化の内容としては、Google、Yahooへメールを送信するすべての送信者は、SPF[164]、DKIM[165]に対応する、有効な正引き、及び逆引きDNSの設定、迷惑メール率を常時0.1パーセント未満、多くても0.3パーセント未満に抑える、送信時にTLS接続すること等が挙げられる。また、Google宛のメールが1日5,000通以上の場合には追加で、DMARC[166]への対応とマーケティング用のメールのList unsubscribeの実装が必要となる。

第4章 WIDEメールの現状調査

Google等のメールポリシー強化に先立って、WIDEメールの現状調査を行った。

4.1 .forwardの現状調査

.forwardの現状調査を行ったところ、全体の15パーセントがGoogle宛のMXへ転送を行っていた。そのうち、@gmail.comは33件、Google Workspaceは34件であった。MXが存在せず、配送不能なメールアドレスが26件見つかり、該当者へは対応のお願いを行った。また、.forwardでGmail宛エラーになっている7割は3名のアカウントに集中していたため、該当者に個別に連絡を行い、POP方式への変更を依頼した。

4.2 WIDEメールのマニュアル執筆

IJ古賀氏によって、WIDEメールの利用手順、GmailでWIDEメールを利用する手順等のドキュメントがまとめられた。これにより、今まで明文化されていなかったWIDEメールの利用方法の明確化、利用方法の統一化が図られた。

4.3 WIDEとしてのポリシー対応

WIDEメールの現状調査を行った結果、DMARCの対応、DKIM/SPFへの対応、スパム率への対策はおおまかにカバーできていることがわかった。メーリングリストの置き換え、ARC署名の対応等が引き続き対応が必要である。

第5章 mail-gwの構築

昨今のGmailやMicrosoft 365をはじめとする商用メールサービスプロバイダーのセキュリティ動向を調査した結果、迷惑メールだけでなくメール転送に関する問題が発生していることがわかった。複数メールアドレスを取得しているユーザのうち、利便性を高めるためにGmailや別の個人のメールアドレスに転送設定することが多く見受けられる。しかし、SMTP[167]はプロトコルとして複数サーバを経由する場合、実際の送信元となるホストの特定や署名の検証が不可になる場合が多く存在する。そ

のため、フィッシング等の一般的な迷惑メールでない場合でも迷惑メールとして取り扱われることが多く観測されている。

2021年にsfc.wide.ad.jpのサブドメインで導入したrspamd[168]を用いた迷惑メールフィルターを2023年の後半にwide.ad.jpの本ドメインにも導入し、DKIM/SPF/DMARCの検証等を強化してきた。また、Spamhaus等の脅威インテリジェンスのデータやDNSRBL(DNS Realtime Blocklist)を用いて大幅WIDEのメンバーに届く迷惑メールを減らすことができた。導入した結果、2023年12月の時点では、各メールゲートウェイで処理されている約4~6割のSMTPセッションを迷惑メールとして判定していることが確認できた。

第6章 まとめと展望

本稿では、Trustworthy EmailワーキンググループによるTrustworthy Emailの構築・運用・普及に向けた取り組みについて報告した。今年度は、WIDEメールの運用ポリシーの策定、Google等の新たなメールポリシーへのWIDEメールの対応等を主な活動として取り組んできた。メーリングリストの更新等の作業は引き続き行いつつ、来年度は運用だけでなくデータ収集、収集したデータを活用した研究活動等もワーキンググループとして取り組む計画である。