第15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、蔵澄 由都

第１章　はじめに

Emailは，インターネットにおける自律分散型の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，また，サイバー空間における識別子として広く利用されている．しかし，その特性を悪用したスパムやフィッシングなどの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」）は，2021年度の設立以来，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進めている．本稿では，2024年度における本WGの活動内容について記述する．

第２章　2024年度の活動

2024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，Trustworthy 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，Google，Yahooのポリシー強化について，WIDEとしての臨時対応，今後の@wide.ad.jpの変更について，メーリングリストの更新についてを主に議論した．ポリシー強化のアップデートとして，Google Workspaceは対象外になった点，spam率が常時0.1%未満，多くても0.3%未満に変更された点，TLS通信が加わった点などに触れ，ポリシー強化について改めて復習を行った．また，IIJ古賀氏が実施したWIDEメールの現状調査として，.forwardの現状調査，WIDEメールのマニュアルについての共有，POP方式への変更の依頼が行われた．また，メーリングリストの移行に関連して，WIDEメール受信ドメイン整理の共有，先述したポリシー強化に対してWIDEとして実施した対応，残りの対応について議論を行い，ToDoの整理を行った．

5月に開催されたWIDE研究会では，メーリングリストの移行に関する議論を中心にBoFを開催し，IETFなどでも使用されているmailman3に移行することで合意した．

9月に開催されたWIDE合宿では，メーリングリスト移行の作業報告，今後の移行作業の方針について，および運用方針についての議論，IIJ古賀氏によるBrand Indicators for Message Identification（BIMI）[75]の小話を行った．

12月に開催されたWIDE研究会では，メーリングリスト移行作業の進捗報告及び，IIJ古賀氏より国内キャリアメールのDMARC対応状況に関する講演を行った．

第３章　WIDE ProjectにおけるEmail運用の現状

WIDE Projectではwide.ad.jp.ドメイン名のメールシステムを運用しているほか，参加組織で利用するためサブドメインを登録ないしは参加組織に対してゾーン委任を行っている．慶應義塾大学や東京大学など一部の参加組織では，wide.ad.jpのサブドメインに対して独自のメールシステムを運用している．

しかし，これらのドメイン・サブドメインは歴史が数十年ほど長いため，インターネット上の他のメールサーバの運用現状の変更などに起因して，いくつかの不具合が発生している．特に，Googleのポリシー強化に対していくつか問題が発生しており，現状以下の対応を行っている．

DMARCポリシーについては，最低限の宣言を行っており，2024年12月現在ではp=noneとしている．また，参加組織のひとつである慶應義塾大学湘南藤沢キャンパス村井研究室のsfc.wide.ad.jpについては過去に海外で成りすましの事例が何度か発生しており，これを防ぐためにp=quarantineの設定を適用している．

DKIMとSPFについては一部対応しており，DKIMはsmtp.wide.ad.jpを経由した場合に適用されるようにしている．SPFについては，現在WIDE BB内のホストのみを許可しているが，今後はさらに制限を強化していく予定である．

また，メーリングリストやメール転送についても対応を進めており，臨時措置としてスパム率を下げるために，MXレコードをmail-gw1.sfc.wide.ad.jpおよびmail-gw2.sfc.wide.ad.jpに向ける設定としている．さらに，mail-gwの通過時点でARC検証およびシール（署名）を適用しているが，その後メーリングリストを経由する場合，メールヘッダ情報が破壊される可能性があると考えられる．例えば外部のメーリスからのメールがWIDEのメールに入ってきた場合，特にDMARCをp=quarantineやp=rejectとしているドメインの場合，意図せず転送が失敗するケースを確認している．これについては今後の対応を検討していく必要がある．

なお，一部のWIDE加入組織や特定の個人は自組織のメールサーバ等を使用してメールを送信しているため，DMARC対応するに当たってポリシーの整理や設定変更の依頼などの対応が必要と考えられる．また，現在のDMARCレポートについて，外部から情報共有あった際に収集しているが，特に解析を行っておらず，より正確にwide.ad.jpのメール全体を把握するため，DMARCレポートの解析基盤が必要と認識している．

また，sfc.wide.ad.jpではPrometheusを使用した解析基盤の試行運用を開始しているが，WIDE全体のDMARCレポートの解析は特に行っておらず，レポートの量などの事情が異なるとこから，使用リソースの拡大が必要と思われる．

第４章　メーリングリストシステムの構築

現在，@wide.ad.jpのメーリングリストはsh.wide上で運用されており，NetBSD 6.1を使用している．メーリングリストの編集は基本的にsh.wideにSSHで接続し，テキストファイル形式で管理されている．メールの配達はsendmailを使用しており，ユーザのメールと同じホスト上で動作している．DKIMおよびARCには対応しておらず，転送時にDKIM署名が破壊されるという課題があるため，早急な移行が求められている．

新たなメーリングリストシステムとしてml.wide.ad.jpを構築している．このシステムはUbuntu 24.04.1 LTS上で運用し，MTAにはUbuntu標準レポジトリのPostfix 3.8.6を使用する．WIDE内の通信は直接mail-gwを経由せずmail.wideに送信し，メーリングリスト管理にはMailman 3.3.9を採用している．ホスト内の通信はLMTPを使用し，外部（WIDE内含む）の通信はPostfixを介してSMTPで行う．データベースはPostgreSQL 16を使用し，Webサーバ にはCaddy v2.8.4を導入することでMailman Webのリバースプロキシおよび Let's Encryptによる証明書管理を行う．Web管理画面の認証は現時点ではmoCAによるアクセス制限を実施しており，ユーザ認証についてはMailman Web側で別途実装する予定である．

全体のメールフローについては図を参照する．

今後の課題として，mail-gwによる振り分けリストの同期が必要となる．現在，mail-gwはtransport_mapsを参照して裏のホストへ配達を行っているが，このリストの同期方法について検討する必要がある．PostfixはLDAP，PostgreSQL，テキストファイルをサポートしているため，これらを活用した適切な同期方式を模索している．現状考えられる方法の一つとして，ml.wide.ad.jpのWebでリストを限定公開し，mail-gwで定期的にfetchする方式も

選択肢を検討しているが，引き続き最適な方法をWG内で検討を進めていく．

ユーザ認証については，現状Webサーバレベルでの moCA認証を必須としているが，Mailman WebはDjangoで実装されているため，SNS等のOpenID Connect（OIDC）を利用した外部アカウント連携が可能である．現状のWIDE Project内で運用されているLDAPはsh.wide.ad.jpのアカウント所有者のみを対象としているため，適切な認証方式とは言えない．Mailman Webでは，複数のメールアドレスをアカウントに紐づけて総合管理できるため，セルフサービス型の管理方式を採用し，ユーザ自身が管理可能な仕組みを構築する方針で進めている．これはIETFにおいてもDatatrackerを介さず独自認証を採用している点と類似している．

この新しいメーリングリストシステムには，Web上での操作・メンバー管理，複数のメールアドレスを統合管理できる機能，メールアドレス確認機能（アカウント作成時の確認メール送信やバウンスアドレスの自動無効化・削除），CSVやコピペによる一括メンバー管理機能，メーリングリストのアクセス制限（自己申告での加入，オーナー承認必須），アーカイブの非公開・限定公開機能などが搭載されており，運用の柔軟性が向上する見込みである．なお，WIDEでは任意のメールアドレスではなく，メンバー管理の観点でメーリングリストの加入は原則として組織のメールアドレスとしているため，Mailmanにおけるユーザ管理の検討が必要と思われる．

第５章　DMARC Report送信の開始

2024年11月頃にmail-gwに受信されたメールのDMARC検証に加え，差出人のドメイン宛に毎日のDMARCレポートを送信するように設定を完了した．この設定変更・関連実装により，wide.ad.jp宛に送信される迷惑メールなどを含め，差出元のドメインにレポートを送信し，WIDE Projectから見えたドメイン成りすましの情報共有が可能となり，DMARCの情報共有の仕組みに参加し始めた．なお，開始からすぐメール送信エラーなどの不具合が確認できているが，これらの不具合が概ね外部のドメインのDMARCポリシーの設定問題やMX制限となるため，外部のドメインにおけるDMARC不具合設定を今後調査して運用課題として認識できた．

第６章　DMARC Reportの解析

今年に入り，WIDE Project参加組織である慶應義塾大学村井合同研究室にてDMARC ruaアドレスに受信したDMARC Reportのdmarc-visualizerを用いた分析を開始している．これはsfc.wide.ad.jpのドメインから送信されたメールアドレス，もしくは同メールアドレスでのなりすましなどを監視するための取り組みである．レポートより送信元，fromアドレス，DKIMやSPFの照合結果などといった情報を人間が容易に確認できるようGrafanaを用いてグラフ・地図・表などを用いて可視化している．これにより，集積されたDMARC Reportを監視しなりすまし被害をいち早く察知し送信元を特定するなどの用途にDMARC Reportを役立てることができるようになった．個人情報をマスクし統計データ化したものは，SFC内のNOCルームにあるモニタにて常時表示する形で公開も行っている．当WGは，同様の仕組みをWIDE Project全体のメールシステム（wide.ad.jp）に導入することによって，現在WIDE Project内で課題となっているSPF対応のための送信元ホスト特定に役立てることができると考えている．従って，当該の取り組みをWG内で共有し賛同を得ることができたため今後導入を予定している．

第７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．