電子メール基盤運用技術の高度化

大谷亘　　ルーク，コリー
alt@sfc.wide.ad.jp　　koluke@sfc.wide.ad.jp
Trustworthy Email ワーキンググループ
email-wg@wide.ad.jp

December 31, 2021

1　概要

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，また，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，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，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 [1][1] 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，2021 年度より活動を開始した本 WG の活動目的と現在の活動内容について記述する．

2　Email を取り巻く現状

2.1　Email の利用

Email はコミュニケーション手段としてインターネット黎明期より用いられてきた．現在では企業や大学で社員や学生・教職員に対して組織ドメイン名の Email アカウントを発行することも多い．従来は組織ないし個人で Email サーバを運用する必要があったが，クラウド Email サービスプロバイダの台頭により Email サーバの構築・運用をすべてクラウド事業者に任せることで，組織ドメイン名での Email システム導入の敷居が下がったと言える．他方，携帯電話キャリアによるキャリアメールやフリーメールの利用により，ユーザは所属組織に関係なく個人の Email アドレスを手に入れることができる．

また，SNS やメッセージングサービスの普及で特に個人間のオンラインコミュニケーションの場は多様化したが，それらを含むオンラインサービスに登録する際の識別子やアカウントのパスワードリセット手段として Email アドレスを求められることがほとんどである [2]．

そのため，現在の Email システムには単なる個人間のコミュニケーション手段として以上に信頼性が求められる．

2.2　不正メールの定義と現状

ところが，エンドノードが主体となりコミュニケーション手段を成立する Email の特性上，受信者にとって価値のないメールである “迷惑メール” (“スパムメール” とも呼ばれる) や，正規の送信者になりすまして送信される “フィッシングメール”，添付ファイルや本文にリンクを記載する形でマルウェアを配布する “ウイルスメール” の送信は後を絶たない．本稿では，“迷惑メール”“スパムメール” や “フィッシングメール”，“ウイルスメール” を含む，Email を不正利用 (abuse) して送信されるメールを “不正メール” と定義する．

不正メールに関する現状に目を向けると，総務

[1] 本稿では Trustworthy Email を「利用者と管理者双方にとって信頼できる快適な電子メールの仕組み・運用手法」と定義する．

省のとりまとめ [3] によると，国内のメールトラフィック (受信) のうち 44.58% が “迷惑メール” であるとされる．また，米国連邦捜査局の調査 [4] によれば，不正メールによる攻撃の一種である Bussiness Email Compromise (BEC) や Email Account Compromise (EAC) に関する米国内外の被害は 3 年間で 1 万 6 千件以上報告されており，経済的損失は約 262 億ドルにのぼる．

これらの不正メールに関する現状に対抗するため，いくつかの技術的仕様が標準化されている．Sender Policy Framework (SPF) [5] は，正規の送信者が自らの使用する送信元 IP アドレスをドメイン名に紐付けて DNS に登録することで，受信者が送信元ドメイン名と実際に受信した際の送信元 IP アドレスとの関係を検証できるプロトコルである．DomainKeys Identified Mail (DKIM) [6] は，正規の送信者がメール送信時に電子署名を施し，その際に使用する秘密鍵に対応する公開鍵をドメイン名に紐付けて DNS に登録することで，受信者が署名検証を行い送信元ドメイン名と署名者との関係性を検証できるプロトコルである．

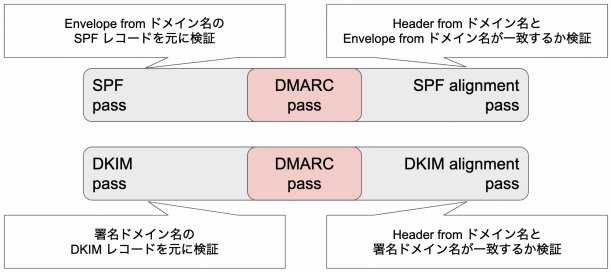

Fig. 1: DMARC による検証と SPF/DKIM との関係

Domain-based Message Authentication, Reporting, and Conformance (DMARC) [7] は，受信者が SPF や DKIM の検証に成功しなかった際の当該メールの扱い方などについて，正規の送信者がドメイン名に紐付けて DNS に登録することで宣言できるプロトコルである．正規の送信者は DMARC を用いて受信者に検証状況のレポートを送付する依頼なども宣言できる．Figure 1に DMARC による検証と SPF/DKIM の関係を示す. そのほか, Authenticated Received Chain (ARC) [8] や SMTP MTA Strict Transport Security (MTA-STS) [9]，Secure/Multipurpose Internet Mail Extensions (S/MIME) [10] などのプロトコルが標準化されている．

また，機械学習や集合知の概念を用いてスパムメールをフィルタリングする技術の研究も盛んに行われており，商用のアプライアンスとして導入されているものもある．

3 WIDE Project における Email 運用の現状

WIDE Project においては `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．

また，WIDE Project ではスパムメールとその対策技術に関して, 過去に Antispam Working Group [11] が調査研究や提案を行っていた．

4 本 WG の目的

本 WG は, 運用者とユーザの双方にとって信頼でき快適な Email システムについて研究し，WIDE Project および参加組織のネットワークに対してそれを実装することを目的としている．目的達成のため，具体的な活動内容を 3 つのカテゴリに分類し，それぞれの役割にフォーカスして活動することとした．

1. **実運用・実験環境としての WIDE Project 及び参加組織における Email システム構築**
   前述の WIDE Project 及び参加組織における Email システムについて，既存の基準やベストプラクティスを元に信頼できるシステム設計を行い，順次実装・移行を行う．それぞれの過程で発見した課題等は 3 項の活動に利用する．

2. **インターネットにおける Email の現状調査及び Trustworthy Email 実現のための課題探索**
   現状のインターネットで運用されている Email システムについて，信頼性における指標を考案し，それに基づいた調査を行う．調査を元に，インターネットにおける技術実装や運用の課題を

明らかにする．

3. **外部組織との連携に基づくインターネット Email への応用**
   1 項や 2 項で発見した課題について，解決策を検討しまとめる．成果物は WIDE Project 外に公開する．また，他組織での信頼できる Email システムの実装・運用に向けて全般的な情報提供を行い，フィードバックに基づいて様々な環境での検討を継続的に行い，以てインターネット全体での Email システムへの信頼性向上を目指す．

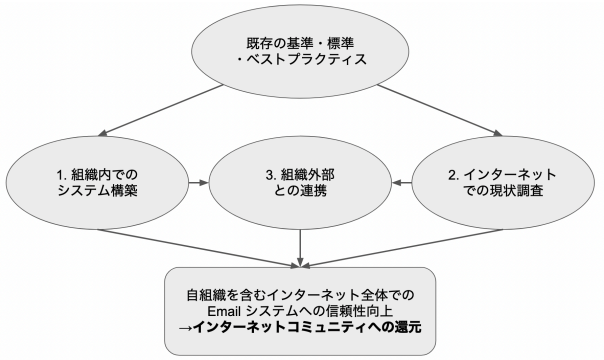

Fig. 2: 本 WG の活動目的

以上の活動目的について，Figure 2にまとめる．

5 WIDE 合宿と研究会における活動

5.1 WG 設立以前の活動

2020 年度には，前述した不正メールの現状を鑑みて，WIDE Project および参加組織のネットワークでの Email システムへの信頼性向上に向け，WIDE 研究会や WIDE 合宿において有志で不正メール BoF を複数回開催した．不正メール BoF では，WG チェアである大谷とコリー (慶應義塾大学) より `wide.ad.jp.` の現状の運用に対する問題提起や，WG メンバである古賀氏 (IIJ) から DMARC をはじめとする送信ドメイン認証技術について説明があった．参加組織内で WIDE Project とは別に Email システムの運用を担当しているメンバも多数参加し，各々の組織内での Email システムの見直しを行うきっかけとなった．

5.2 WG 設立後の活動

2021 年度には，不正メール BoF での議論を元に本 WG を設立した．WIDE 合宿や研究会においては不正メール BoF に引き続き，BoF の形で各種報告や議論を継続している．WG チェアである大谷とコリー (慶應義塾大学) からは，全体の話題提供及び慶應義塾大学における運用や取り組みについて発表があった．WG メンバである古賀氏 (IIJ) からは，送信ドメイン認証技術の運用に関する議論や，参加組織ネットワークでの送信側 DMARC 対応状況に関する報告があった．報告では，第 1 回不正メール BoF 開催前と比較して参加組織の約 4% で新たに送信者として DMARC に対応したことが発表された．WG 担当ボードである尾上氏 (ソニー) からは，`wide.ad.jp.` ドメイン名での Email システムの詳細な説明と，Trustworthy Email 実現に向けた改善点や実装方法について議論があった．

6 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．2 章と 3 章では，現状での Email のユースケースや不正メールの定義・現状，WIDE Project における Email 運用について振り返り，Email システムにおける信頼性確保の重要性を確認した．4 章では，本 WG の活動目的についてまとめた．5 章では，活動目的に基づいたこれまでの WIDE 合宿と研究会での活動についてまとめた．今年度は 4 章でまとめた活動目的について着手できていない点があり，今後はメンバ同士の連携に基づきより活発にそれぞれの活動を継続していきたい．

References

[1] S. Rose, J. S. Nightingale, S. Garfinkel, and R. Chandramouli, “Trustworthy email,” National Institute of Standards and Technology, Gaithersburg, MD, Tech. Rep. NIST SP 800-177r1, Feb. 2019. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-177r1.pdf

[2] T. Innocenti, S. A. Mirheidari, A. Kharraz, B. Crispo, and E. Kirda, "You've Got (a Reset) Mail: A Security Analysis of Email-Based Password Reset Procedures," in *Detection of Intrusions and Malware, and Vulnerability Assessment*, L. Bilge, L. Cavallaro, G. Pellegrino, and N. Neves, Eds. Cham: Springer International Publishing, 2021, vol. 12756, pp. 1–20, series Title: Lecture Notes in Computer Science. [Online]. Available: https://link.springer.com/10.1007/978-3-030-80825-9_1

[3] 総務省, "電気通信事業者１０社の全受信メール数と迷惑メール数の割合（2021 年 3 月時点）," 総務省, Tech. Rep., Mar. 2021. [Online]. Available: https://www.soumu.go.jp/main_content/000693529.pdf

[4] Federal Bureau of Investigation, "Internet Crime Complaint Center (IC3) | Business Email Compromise The $26 Billion Scam," Sep. 2019. [Online]. Available: https://www.ic3.gov/Media/Y2019/PSA190910

[5] S. Kitterman, "Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1," Internet Engineering Task Force, Request for Comments RFC 7208, Apr. 2014, num Pages: 64. [Online]. Available: https://datatracker.ietf.org/doc/rfc7208

[6] M. Kucherawy, D. Crocker, and T. Hansen, "DomainKeys Identified Mail (DKIM) Signatures," Internet Engineering Task Force, Request for Comments RFC 6376, Sep. 2011, num Pages: 76. [Online]. Available: https://datatracker.ietf.org/doc/rfc6376

[7] M. Kucherawy and E. Zwicky, "Domain-based Message Authentication, Reporting, and Conformance (DMARC)," Internet Engineering Task Force, Request for Comments RFC 7489, Mar. 2015, num Pages: 73. [Online]. Available: https://datatracker.ietf.org/doc/rfc7489

[8] K. Andersen, B. Long, S. Blank, and M. Kucherawy, "The Authenticated Received Chain (ARC) Protocol," Internet Engineering Task Force, Request for Comments RFC 8617, Jul. 2019, num Pages: 35. [Online]. Available: https://datatracker.ietf.org/doc/rfc8617

[9] D. Margolis, M. Risher, B. Ramakrishnan, A. Brotman, and J. Jones, "SMTP MTA Strict Transport Security (MTA-STS)," Internet Engineering Task Force, Request for Comments RFC 8461, Sep. 2018, num Pages: 29. [Online]. Available: https://datatracker.ietf.org/doc/rfc8461

[10] B. C. Ramsdell, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification," Internet Engineering Task Force, Request for Comments RFC 3851, Jul. 2004, num Pages: 36. [Online]. Available: https://datatracker.ietf.org/doc/rfc3851

[11] 山本和彦, "迷惑メール低減に関する技術開発と普及," WIDE Project, Tech. Rep., Mar. 2013. [Online]. Available: https://www.wide.ad.jp/About/report/pdf2012/part29.html