はじめに

現在のメールシステムは，その仕組みの簡便さもあり多くのコミュニケーションツールの基盤として広く普及しました．その一方で，メールを読むべきかを判断する，重要な情報である送信者を確認するための手段が備わっていなかったことにより，多くの問題が引き起こされています．例えば，送信者の確認ができないような匿名の広告宣伝メールや，実在する事業者を騙って偽のウェブサイトへ誘導することで，個人情報や金銭につながる情報を窃取するフィッシングが，大きな社会問題となっています．こうした迷惑メールは，メールに示される送信者情報が信用できないことから，受け取るべきかどうか，本当の事業者であるかどうかを判断ができないことが，大きな原因となっています．

送信ドメイン認証技術は，受信者が受け取ったメールについて，送信者情報が詐称されているかどうかをドメイン名単位で確認（認証）する技術です．この技術により，送信者情報が詐称されることによって発生する多くの問題を解決できると期待されています．

送信ドメイン認証技術には，認証する送信者情報や認証に用いる仕組みが異なる複数の方式があります．送信ドメイン認証技術を利用するためには，メールの送信側と受信側のそれぞれで，新たな設定や機能の導入が必要となります．この導入マニュアルは，主にメールシステムの管理者やメール仕様の検討や導入を計画する立場にある企画担当者などを対象に，メールシステムの仕組みや各役割についての説明，送信ドメイン認証技術の導入にあたって必要な事項をまとめています．今回の導入マニュアルの改訂にあたっては，第 2 版以降に仕様が作られた DMARC を中心に，これまでの SPF と DKIM との関係も含めて解説しています．基礎編では，電子メールの基本的な仕組みと課題，SPF，DKIM，DMARC それぞれの送信ドメイン認証技術の技術仕様，関連するメールヘッダの仕様について解説します．応用編では，これら送信ドメイン認証技術を導入する際に検討しておくべき事柄について，DMARC を導入することを前提に解説します．送信ドメイン認証技術は，メールの送信側と受信側双方での新たな設定や機能の導入が必要となりますので，メールの送信側と受信側それぞれの立場で解説します．また，巻末に参考情報や用語の索引も付属しました．

送信ドメイン認証技術は，あくまでドメイン名単位で送信者情報が正しく設定されているかを確認（認証）する技術であり，この技術だけで送受信されるメールが迷惑メールかどうかを判断できるわけではありません．しかし，この技術の活用により送信ドメイン名の詐称ができなくなれば，ドメイン名単位で受け取りたいメール，受け取る必要がないメールを確実に判断できるようになります．送信ドメイン認証技術が広く普及することで，このような受け取り判断が可能なメールが増え，それにより，迷惑メール自体も減少することが期待できます．本導入マニュアルが，メールシステムの健全な発展に貢献できることを願っています．

迷惑メール対策推進協議会 技術ワーキンググループ
主査 櫻庭 秀次
副主査 加瀬 正樹
北崎 恵凡