第1章 はじめに

第1章　はじめに

1.1　メールの普及と送信者情報偽装の問題

現在のメールシステムは、その仕組みの簡便さによって、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。その仕組みの簡便さの一方で、送り手が誰であるかを確認する手段が備わっていなかったことにより、現在では、多くの問題が引き起こされています。例えば、第三者のメールアドレスを悪用した匿名の広告宣伝メールの送信行為や、実在するメールアドレスを騙って偽のウェブサイトへ誘導して個人情報などを搾取するフィッシングなどの犯罪行為などが頻繁に行われるようになっています。また、メールシステムでは、受け取ったメールが宛先不明など何らかの原因で配送できない場合には、送信元に対してエラーメールなどの通知文を送信する必要がありますが、これにより送信者情報を詐称された第三者へ大量の通知文が届く問題なども発生するようになっています。

1.2　送信ドメイン認証技術による対応

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単位で確認可能とする技術です。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問題の多く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。また、送信ドメイン認証技術には、その手法の違いにより、複数の方式が併存しています。さらに、メールの利用環境や利用局面の多様化により、技術的な課題以外にも、送信ドメイン認証技術を導入する際に考慮すべき事項があります。例えば、仕事に関連したメールを個人が契約した ISP（Internet Service Provider）の回線を利用して自宅から送信する場合に注意すべき点や、自社に関連したキャンペーン情報を顧客に大量送信するために外部の事業者に委託する場合に検討しておくべき点があります。また、メールシステム自体について、ISP など外部事業者のサービスを利用している場合や、専用システムであるものの運用を外部委託している場合など、利用環境の違いによって導入の方法が大きく異なる場合があります。

このため、送信ドメイン認証技術を利用する場合には、どの方式を利用すべきなのか、それぞれの方式にはどのような特徴があるのか、というような具体的な導入の手順や内容について理解することが必要になります。

1.3　本マニュアルの目的

本マニュアルは、主にメールシステムの管理者やメールの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、既にメールシステムの構造や概要についてある程度理解していることを前提として、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。また、それらの事項に加え、

メールサービスを他組織へ提供している事業者にとって有益な情報も別にまとめています。

まず、電子メールの仕組みと課題について解説を行います（第２章）。続いて、送信ドメイン認証技術について、導入の前提となる知識を整理する目的で、技術部分の解説を行います（第３章）。次に、送信ドメイン認証技術の導入の手順について解説を行います（第４章）。さらに、他者にメールサービスを提供する事業者での追加的な注意事項について、ISPでの対応（第５章）、ホスティングサービスでの対応（第６章）、配信サービスでの対応（第７章）の順に解説を行います。最後に、利用者への周知一般について、解説を行います（第８章）。また、巻末に、参考情報や用語解説をつけています。

送信ドメイン認証技術は、あくまでドメイン単位で送信者情報が詐称されているかどうかを確認可能とする技術であって、これ自体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訳ではありません。しかし、この技術の活用によりドメイン名の詐称ができなくなれば、ドメイン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決めておけば、それ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により、このような判断が可能なドメインが増え、それにより、迷惑メール自体も減少することが期待されます。本マニュアルがこのような流れに少しでも貢献できれば幸いです。

MEMO