DMARC導入に関する法的な留意点

総務省総合通信基盤局
電気通信事業部消費者行政第二課

DMARCの概要

1. DMARCの概要

（1） ドメイン管理者において、当該ドメイン名義で送信される電子メールに関して、受信時のドメイン認証が失敗した場合の取り扱い方針を宣言するとともに、後記(3)記載のレポートの送付先メールアドレスを公開する。

（2） 電子メールの受信サーバ側で、ドメイン認証（DKIM、SPF）を行った上、認証に失敗した電子メールにつき、(1)の取り扱い方針も踏まえ、以下のいずれかの処理をする。

- ○ 何もしない　：　そのまま受信者に届ける
- ○ 隔離　：　認証に失敗した旨を付して隔離する（迷惑メールとして扱う）
- ○ 拒絶　：　受信サーバから削除する（受信者は存在を認識しない）

（3） 受信サーバ側は、送信ドメイン管理者の指定した送付先メールアドレスに対し、(2)の認証結果に関するレポートを送付する。

2. 法的問題点

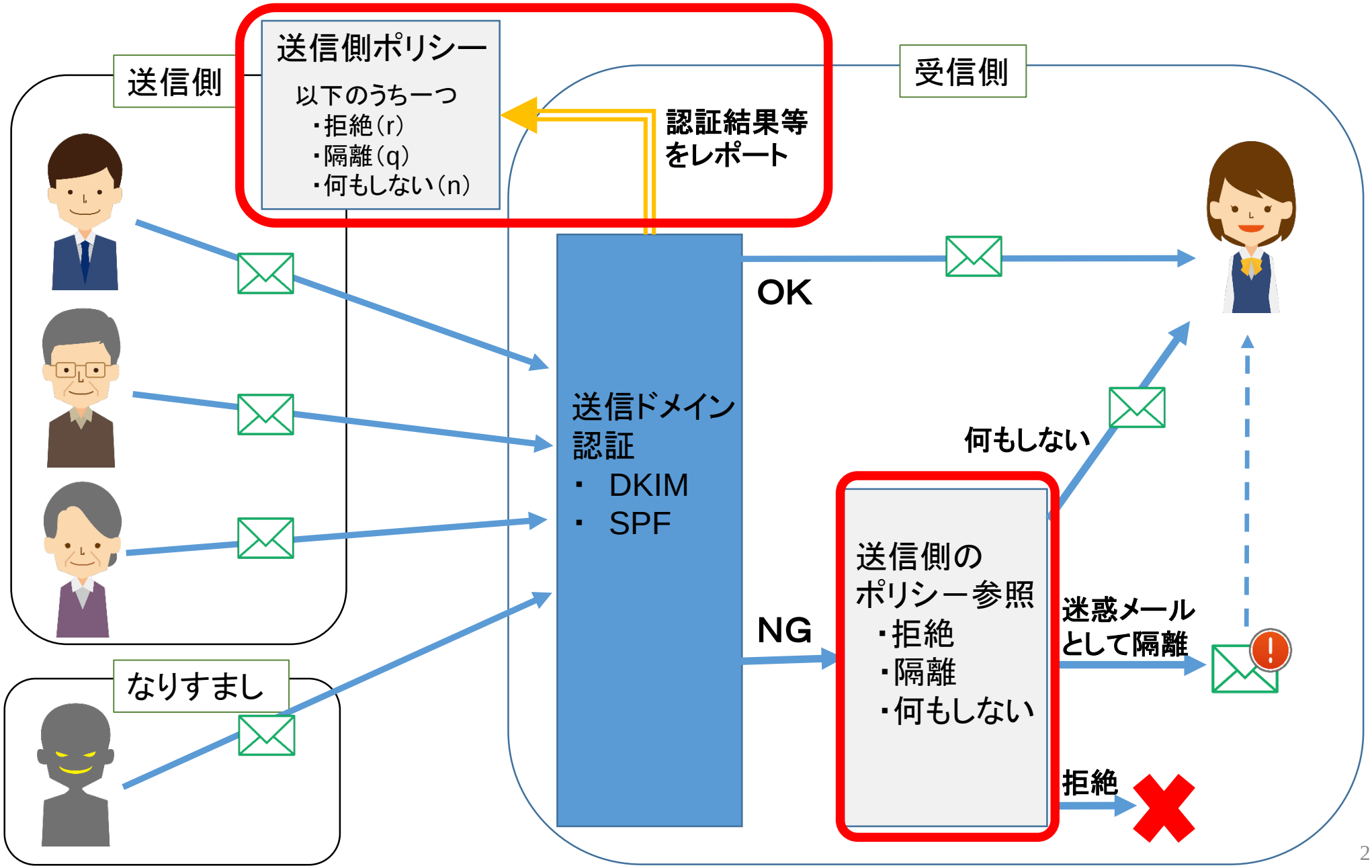
法律的に見ると、

・(2)は、**「電子メールの受信サーバにおいて、電子メールの送信ドメインを認証（チェック）し、認証できない場合には一定の措置を講ずる行為」**と解され、

・(3)は、**「認証できない通信に関する情報を、送信側管理者又はその指定する者（ISP、分析者等）に報告する行為」**と解される。

これらは、いずれも外形的に**電気通信事業法第4条に規定する「通信の秘密」を「侵害する行為」**に該当し得ることから、その可否が問題となる。

（参考）DMARCの概要図



DMARC導入にあたっての当事者の同意について

約款等による事前の包括的合意によって通信の秘密の利益を放棄させることは、① 約款の性質になじまないこと、② 同意の対象が不明確であることから、**原則として許されず、有効な同意とは解されない。**

ただし、以下の条件を満たす場合には、約款等による包括同意に基づいて提供する場合であっても、利用者の有効な同意を取得したものと考えることができる。

① 利用者が、随時、任意に設定変更できること

② 同意の有無に関わらず、その他の提供条件が同一であること（※1）

③ 同意の対象・範囲が明確にされていること

④ ドメイン認証の結果に係るレポートを送付する場合、レポートの内容に電子メールの本文及び件名が含まれていないこと。（※2）

⑤ DMARCの内容について、事前の十分な説明を行うこと（電気通信事業法第26条に規定する重要事項説明に準じた手続によること）（※3）

※1 DMARCを含むフィルタリングサービスを合理的な料金により提供することは問題ない。

※2 本文及びSubjectヘッダ情報のような電子メールの内容に係るヘッダ情報のいずれも含まれていないという趣旨。

※3 DMARCに関しては、以下のような点を明確に説明している必要がある。

①ポリシーを踏まえて遮断を行う場合

- 遮断を行う旨
- 遮断された場合、利用者はその内容を確認できない旨

②送信側管理者の求めに応じて報告を行う場合

- レポートに記載する事項
- 上記事項が送信側の指定した宛先に送付される旨

(参考)ドメイン認証行為の正当業務行為該当性についての従来の整理

ある行為が「正当業務行為」に該当するといえるには、(1)目的の必要性、(2)行為の正当性、(3)手段の相当性を満たすことが必要である。

○送信元を偽装した電子メールは、ほとんどが迷惑メールであること
○広告等の手段として送信される迷惑メールは、通常一度に多数の者に対して送信されていると合理的に推定できること

から、**送信ドメインを偽装しているメールは、一度に多数の者に送信されていると推定でき**、これらの遮断を目的とする**フィルタリングサービスの提供は**、当該サービスの提供について**顧客の有効な同意が得られている限り、目的として正当なものといえる**。

また、送信ドメイン認証自体において侵害する通信の秘密は、通信の経路情報である**送信ドメインに限られており**、フィルタリング等のための行為として**必要な限度を超えるものではないから**、**送信ドメインを認証し、その結果をラベリングする行為**は、フィルタリング等の**目的達成のために必要かつ相当な方法**と認められる。

したがって、フィルタリングサービスが顧客の有効な同意に基づいて提供される場合、ドメイン認証行為は、正当業務行為に該当し、このことは、DMARC実施のために行われるドメイン認証行為においても同様である。