DMARC等の送信ドメイン認証技術の導入に関する法的な留意点

平成２９年９月

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
課長補佐　冨岡健史

通信の秘密及び関連する過去の整理

迷惑メール対策と通信の秘密との関係について

- 迷惑メール等への対策の実施に当たっては、通信である電子メールに関する情報の取得・利用が必要となる場合が多く、「通信の秘密」について留意することが必要
- 「通信の秘密」は、表現の自由の保障を実効あらしめるとともに、個人の私生活の自由を保護し、個人生活の安寧を保障する（プライバシーの保護）ため、憲法上の基本的人権の一つとして、憲法第21条第2項において保障されているもの
- 憲法の規定を受け、電気通信事業法において、罰則をもって「通信の秘密」を保護する規定が定められており、電気通信事業法上「通信の秘密」は厳格に保護されている

通信の秘密の範囲

通信の秘密には、①**個別の通信に係る通信内容**のほか、②個別の通信に係る通信の日時・場所・通信当事者の氏名・住所・電話番号等の当事者の識別符号・通信回数等、**これらの事項を知られることによって通信の存否や意味内容を推知されるような事項全て**が含まれる。

※　東京地裁判決H14.4.30は、「電気通信事業法第104条の「通信の秘密」には、通信の内容のほか、通信当事者の住所・氏名・電話番号、発受信場所、通信の日時・時間・回数なども含まれると解する。」と判示する。

通信の秘密の侵害

通信の秘密を侵害する行為は、以下の３類型に大別される。なお、通信の秘密の保存自体も侵害に該当し得る。

○　**知　得**＝「積極的に通信の秘密を知ろうとする意思のもとで知り得る状態に置くこと」
○　**窃　用**＝「発信者又は受信者の意思に反して利用すること」
○　**漏えい**＝「他人が知り得る状態に置くこと」

通信の秘密の侵害とならない場合について

通信当事者の有効な同意がある場合

○　通信の秘密の侵害について、通信当事者の有効な同意がある場合は通信の秘密の侵害に当たらない。

通信当事者（発信者又は受信者）が、侵害される通信の秘密について個別具体的かつ明確に同意した場合でなければ、原則として有効な同意があるとはいえない。

ただし、通常の利用者であれば承諾することが容易に想定され、利用者が随時不利益なく同意を撤回でき（オプトアウト）、それらが十分に周知されるなどしている場合は、約款等での包括的な同意で足りるといえることがある。

違法性阻却事由がある場合

○　通信当事者の有効な同意がない場合であっても、下記のような違法性阻却事由がある場合には、通信の秘密の侵害が許容される。

(1) 法令行為に該当する場合

電気通信事業者として、刑事訴訟法第100条に基づく通信履歴の差押えに応じるなど、他の法令の規定に基づき正当に行う行為は、法令に基づく行為として違法性が阻却される。

(2) 正当業務行為に該当する場合

電気通信事業者として電気通信役務の提供等の業務を遂行するために必要であって、①目的の正当性、②行為の必要性、③手段の相当性の要件を満たす行為については、正当業務行為として違法性が阻却される。

(3) 正当防衛、緊急避難に該当する場合

通信施設に対する現に生じている攻撃に対応したり、人の生命身体に対する危険を避けるために通信の秘密を侵す場合など、正当防衛の要件（①急迫不正の侵害、②自己又は他人の権利を防衛するため、③やむを得ずした行為）　又は緊急避難の要件（①現在の危難の存在、②法益の権衡、③行為の補充性）を満たす行為については、違法性が　阻却される。

送信ドメイン認証一般の法的留意点

1.「通信の秘密」「侵害行為」該当性

個別の電子メールに係る送信ドメインは、個別の通信に係る経路情報であり、通信の構成要素として**「通信の秘密」の保障を受ける。**

宛先不明の電子メールに関して、受信側サーバにおいて電子メールの送信ドメインを機械的に確認し、認証できない場合については送信元サーバに対してエラーメールを返さないようにする行為も、通信の秘密を「当事者の意思に反して利用する」ことに当たり、**通信の秘密の「侵害」(窃用)に当たり得る**と考えられる。

→ **当事者の同意又は違法性阻却事由がない限り、「通信の秘密」の侵害に当たる。**

2. 正当業務行為該当性

(1) 行為の正当性、必要性

- 送信ドメインを偽装しているメールは、いわゆる迷惑メールとして一時に多数の者に送信されていると推定できること
- メールサーバが受信する迷惑メールの大部分があて先不明メールであること

から、送信ドメイン認証できない宛先不明メールに関してエラーメールを返さない行為は、大量送信される迷惑メールにより引き起こされる、大量の宛先不明メールに関するエラーメールにかかるトラフィックによって生じる**電子メール送受信上の支障のおそれを減少させるための行為と認められ、行為の必要性・正当性が認められる。**

※ なお、送信ドメインを認証できないということは、送信元とされるメールサーバは、実際には当該メールを送信していないことが推定されるから、受信側サーバにおいてエラーメールを送信側に返信することは通常無用のトラフィックを増加させるだけのものであって意味のない行為である。

(2) 手段の相当性

送信ドメイン認証を行うに当たり、機械的自動的に送信ドメインという通信の経路情報を識別する場合、侵害される通信の秘密が限定されており、目的達成のために必要な限度を超えるものでもないことから、メールサーバ等の負担軽減といった**目的達成のために相当な手段と認められる。**

→ **メールサーバ等の負担軽減のために送信ドメイン認証を行うことは、正当業務行為として許容されると考えられる。**

迷惑メールのフィルタリングサービスを実施する場合の法的留意点

1.「通信の秘密」「侵害行為」該当性

個別の電子メールに関して、当該電子メールに関する情報（送信ドメインなど）を知得し、あらかじめ設定した条件に該当する通信について、 通信当事者に無断で処理する行為（例：遮断する、隔離するなど）は、**通信の秘密を「発信者又は受信者の意思に反して利用する」ことに当たり、通信の秘密の窃用（侵害）に当たる**と考えられる。

当事者の同意又は違法性阻却事由がない限り、「通信の秘密」の侵害に当たる。

※ フィルタリングは、受信者のために行う行為であるから、原則として正当業務行為に該当しない

2. 有効な同意の取得

約款等による事前の包括的合意により、通信の秘密の利益を放棄させることは、

- 約款の性質になじまないこと
- 同意の対象が不明確であること

から、原則として**許されない（有効な同意とは解されない）**

原則として、利用者の個別申し込みを受けて提供する必要がある。
ただし、以下の条件を満たす場合には、約款等に基づいて「初期設定オン」で提供したとしても、利用者の有効な同意があると考えることができる。

① 同意後も、随時、利用者が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（※）
③ 同意の対象・範囲が明確に限定されていること
④ 平均的利用者であれば同意することが合理的に推定されること
⑤ フィルタリングサービスの内容について、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）

※ 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。

（参考）IP25Bに関する法的整理

- IP25B（Inbound Port 25 Blocking）は、通信の構成要素である電子メールの送信元IPアドレス及びポート番号を確認し、その結果に従って一定の電子メールをブロックする措置であることから、電気通信事業法第4条に規定される「通信の秘密」を「侵害する行為」に該当する。

- しかしながら、
  ① 他のISPの固定IPアドレスからの大量送信はほとんど見られないこと、
  ② 他のISPの動的IPアドレスから電子メールが大量送信されていること、
  ③ トラフィック全体に対する一律のレートコントロールでは、大量送信の防止措置として不十分であること

  が認められる場合には、IP25Bは正当業務行為と認められ、違法性が阻却されると考えることができる。

- また、IP25Bは一定の要件を満たした電子メールについて接続を拒否するものであることが、接続拒否を行うこと（通信の秘密の侵害（窃用））が正当業務行為として許されることから、その範囲で特定の者に限定せずに実施する限り、電気通信事業法第6条に規定される「不当な差別的取扱い」には当たらないと考えられる。

- 以上のように、IP25Bは法的問題点についても整理できることから、ISPによる積極的な導入が図られることが望ましい。

（参考） OP25Bに関する法的整理

- OP25B（Outbound Port 25 Blocking）は、通信の構成要素である電子メールの送信元IPアドレス及びポート番号を確認し、その結果に従って電子メールをブロックする措置であることから、電気通信事業法第4条に規定される「通信の秘密」を「侵害する行為」に該当する。

- しかしながら、
  ① ISPの提供するメールサーバを利用した大量送信が行われていないこと、
  ② ISPの提供するメールサーバを経由しない動的IPアドレスからの大量送信が行われていること、
  ③ 必要な限度で実施され、かつ通信の秘密を侵害しない形での代替手段がないこと
  が認められる場合には、OP25Bは正当業務行為と認められ、違法性が阻却されると考えることができる。

- また、OP25Bは一定の要件を満たした電子メールについて接続を拒否するものであることが、接続拒否を行うこと（通信の秘密の侵害（窃用））が正当業務行為として許されることから、その範囲で特定の者に限定せずに実施する限り、電気通信事業法第6条に規定される「不当な差別的取扱い」には当たらないと考えられる。

- 以上のように、OP25Bは法的問題点についても整理できることから、ISPによる積極的な導入が図られることが望ましい。

ＤＭＡＲＣに関する法的留意点

DMARCの概要

1　送信側において講じる措置

（1）送信ドメイン認証に必要な設定を行う

（2）当該ドメイン名義で送信される電子メールに関し、認証が失敗した場合の取り扱い方針を宣言する

（3）レポート（後記2(3)）の送付先メールアドレスを公開する

2　受信側において講じる措置

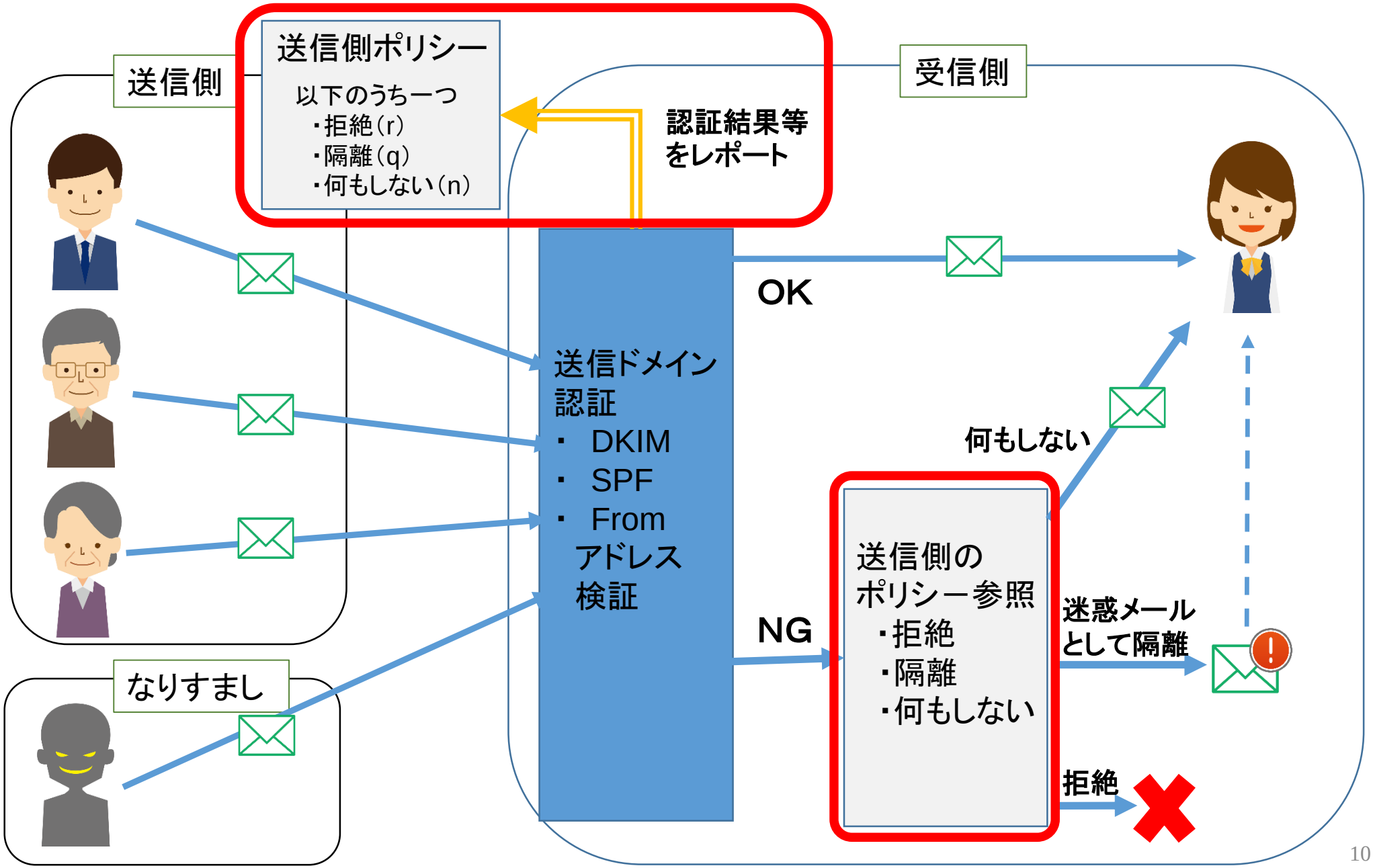
（1）電子メールサーバに受信する際に、送信ドメイン認証を行なう。

（2）2(1)の認証に失敗した電子メールにつき、1(1)の取り扱い方針を踏まえ、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）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、認証結果に関するレポートを送付する。

（参考）DMARCの概要図



DMARCに関して生じる法的問題点

○　送信側の行為について
通信の秘密を利用する要素はない。

→ **「通信の秘密」との関係では直ちに問題は生じない。**

※　一般利用者に対するメールサービスとして提供している場合、ポリシーで拒絶を宣言するときは、利用者に対する説明という観点から認証に失敗されたメールが拒絶されることなどを周知する必要があると解される。

○　受信側の行為について
・ ドメイン認証と認証結果に基づき拒絶、隔離を行う行為は、
「電子メールの受信サーバにおいて、電子メールのヘッダ情報等を知得・利用して送信ドメインを認証（チェック）し、認証できない場合に一定の措置を講ずる行為」
・ 認証結果に基づいてレポートを送信する行為は、
「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」
と理解される。
これらは、いずれも外形的には**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。

→ **当事者の同意又は違法性阻却事由がない限り、「通信の秘密」の侵害に当たる。**

※　ポリシーに従った処理をすることは外形的にはフィルタリングと同種の行為であること、レポートの送信についても、メールサービスの提供の為に不可欠な措置とはいえないことから、原則としては正当業務行為に該当しない。

DMARC導入に関する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ることは、**原則として許されない。**
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。

- 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
- 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

おわりに

≪参考≫

送信ドメイン認証技術等の導入に関する法的解釈について
【http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/m_mail/legal.html】