受信側における送信ドメイン認証技術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

「通信の秘密」の保護

電気通信事業法
第4条　電気通信事業者の取扱中に係る通信の秘密は、侵してはならない。

1.「通信の秘密」該当性

「通信の秘密」とは、(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当事者の住所、氏名、発信場所等、通信日時等の構成要素を含む。

　個別の電子メールに係る送信ドメインも個別の通信に係る経路情報であり、通信の構成要素であるから通信の秘密の保障を受ける。

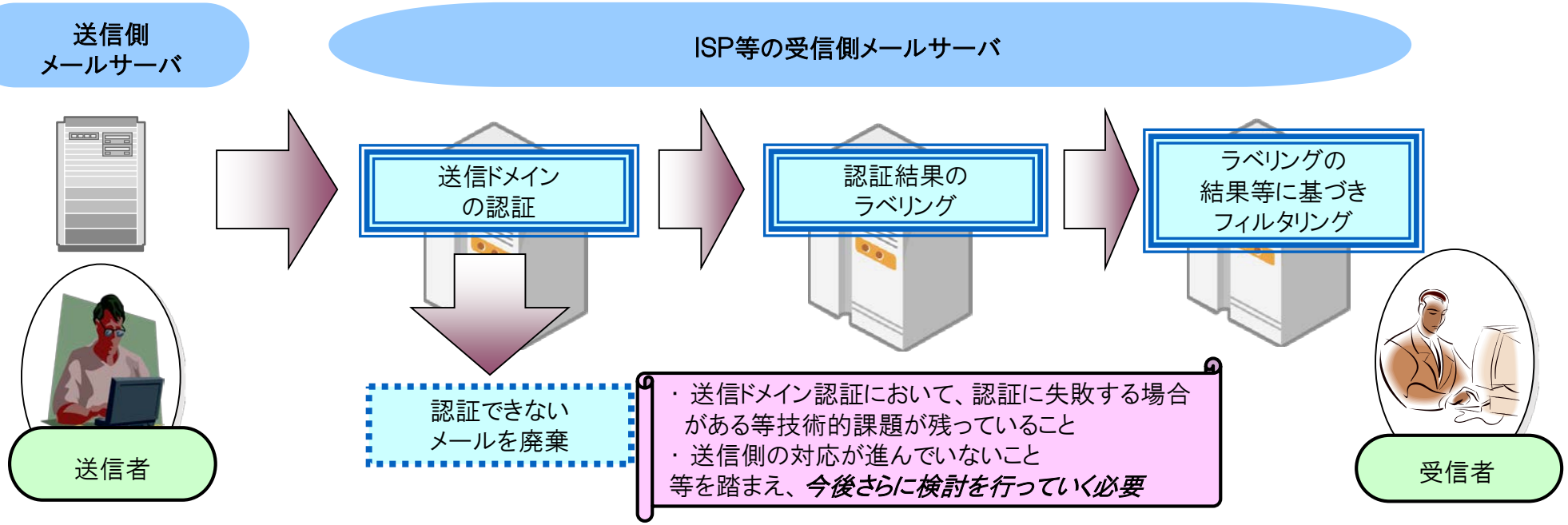
2.「侵害行為」該当性

通信の秘密を「侵害する行為」には、「発信者又は受信者の意思に反して通信の構成要素等を利用すること」（窃用すること）も含む。

「不当な差別的取扱い」の禁止

電気通信事業法
第6条　電気通信事業者は、電気通信役務の提供について、不当な差別的取扱いをしてはならない。

（2）　送信ドメイン認証を利用した受信側での対応について



1. 送信ドメイン認証技術の法的性質

技術的には違いがあるが、SPF、DKIM、DMARCのいずれも、法律的に見れば「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」と解される。

2. 法的問題点

「受信側で送信ドメインの認証を行い、認証できなかった場合に、当該メールにその旨をラベリングして配信する行為（当該ラベリングに基づき受信拒否等のフィルタリングを行うことが前提）」が、電気通信事業法との関係で問題が生じないか。

具体的には、上記行為が、

・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」に該当するか。

・電気通信事業法第6条に規定する「不当な差別的取扱い」に該当するか。

が問題となる。

結　　論

- 送信ドメイン認証は、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認証し、認証できない場合に当該電子メールに対し、通信当事者の意思に反してラベリングする行為であるが、このような行為は電気通信事業法第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、大量送信される迷惑メールにより生じるサービスの遅延等の電子メール送受信上の支障のおそれを減少させるために実施する場合には、送信ドメイン認証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、送信ドメイン認証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、送信ドメイン認証は法的問題点についても整理できることから、後述のフィルタリングサービスと併せてISPによる積極的な導入が図られることが望ましい。

通信の秘密の侵害に関する検討①

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認証し、認証できない場合に当該電子メールに対し、通信当事者の意思に反してラベリングする行為は、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、通信の秘密の侵害（窃用）に当たると考えられる。

当事者の同意がない限り、「通信の秘密」を「侵す行為」に該当する。

ただし、「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認証し、認証できない場合に当該電子メールに対し、通信当事者の意思に反してラベリングする行為」が、通信の秘密侵害行為に該当する場合であっても、**違法性阻却事由があれば（正当防衛、緊急避難又は正当業務行為に該当すれば）、当事者の同意の有無に関わりなく、許される。**

1. 正当防衛、緊急避難該当性

送信ドメイン認証は、電子メール送受信上の支障が発生することを防止するために、電子メール送受信上の支障が又は支障の発生が切迫している場合に限らず常時行われる対策である。

このため、正当防衛の要件である急迫性や、緊急避難の要件である危難の現在性等を必ずしも満たすとは限らないことから、正当防衛、緊急避難に該当しない場合が想定される。

2. 正当業務行為該当性

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

(1) 行為の正当性、必要性

・ 送信元を偽装した電子メールのほとんどが迷惑メールであること
・ 迷惑メールのほとんどが送信元を偽装して送られていること
・ 広告宣伝の手段として送信される迷惑メールは、特段の事情がない限り、一時に多数の者に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、一時に多数の者に送信されていると推定できる。

したがって、大量送信される迷惑メールにより生じるサービスの遅延等の電子メール送受信上の支障のおそれを減少させるために**「送信ドメインを認証し、その結果をラベリングする行為」**については、**行為の正当性、必要性が認められる**。

(2) 手段の相当性

・ 送信ドメイン認証を行うに当たって侵害することになる通信の秘密は、送信ドメインという通信の経路情報であり、目的（フィルタリングのためのラベリングを行う行為）達成のために必要な限度を超えるものではない。
・ OP25Bや送信者認証といった他の迷惑メール対策も存在しているが、送信ドメインを偽装して送信される迷惑メールは、これらの技術では対応できない場合があることから、送信ドメイン認証の結果を「ラベリングする行為」は相当な方法と考えられる。

したがって、**「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、目的達成のために相当な方法と認められる。**

→ **正当業務行為（違法性阻却事由あり）と解釈できる。**

→ **また、正当業務行為として許容される対策として一律に実施する場合、電気通信事業法第6条に規定する「不当な差別的取扱い」には該当しない。**

（参考）ドメイン認証技術とエラーメールを返さない行為

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も、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）に当たる**と考えられる。

当事者の同意がない限り、「通信の秘密」を「侵す行為」に該当する。

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、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、受信側サーバにおいて配信できなかった旨のエラーメールを送信側に返信することは通常意味がない。

（2）手段の相当性

送信ドメイン認証を行うに当たって侵害することになる通信の秘密は、送信ドメインという通信の経路情報であり、目的（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）達成のために必要な限度を超えるものではないことから、**目的達成のために相当な方法と認められる。**

正当業務行為に該当すると解釈できる。

（３）　フィルタリング行為に関する「通信の秘密」侵害行為の該当性

送信ドメイン認証の結果のラベリング等に基づき、受信した電子メールについてフィルタリングを行うことが、電気通信事業法との関係で問題が生じないか。

具体的には、上記行為が、
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」に該当するか
が問題となる。

・「通信の秘密」「侵害行為」該当性

フィルタリングを行い、あらかじめ設定した条件に該当する特定の通信に係る通信の秘密を検知し、通信当事者の意思に反して処理する（例：ブロックしたり、廃棄したりする）行為は、**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。

当事者の同意がない限り、「通信の秘密」を「侵す行為」に該当する。

フィルタリングは、受信者のために行う行為であるから、受信者の意思に関わらず実施する正当業務行為等の違法性阻却事由には原則として該当しない。
したがって、当事者の有効な同意を取得する必要がある。

フィルタリング導入にあたっての当事者の同意について

(1) 初期設定オフで、利用者から申込みを受けて提供する場合

一般的に、利用者の有効な同意があると考えられる。

(2) 初期設定オンで提供する場合

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、

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**許されない（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、「初期設定オン」で提供したとしても、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 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(※1)
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（信用できるデータ(※2)による裏付けが必要）
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）

※1 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 利用者を対象に無作為抽出によるアンケートを実施することなどが考えられる。

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

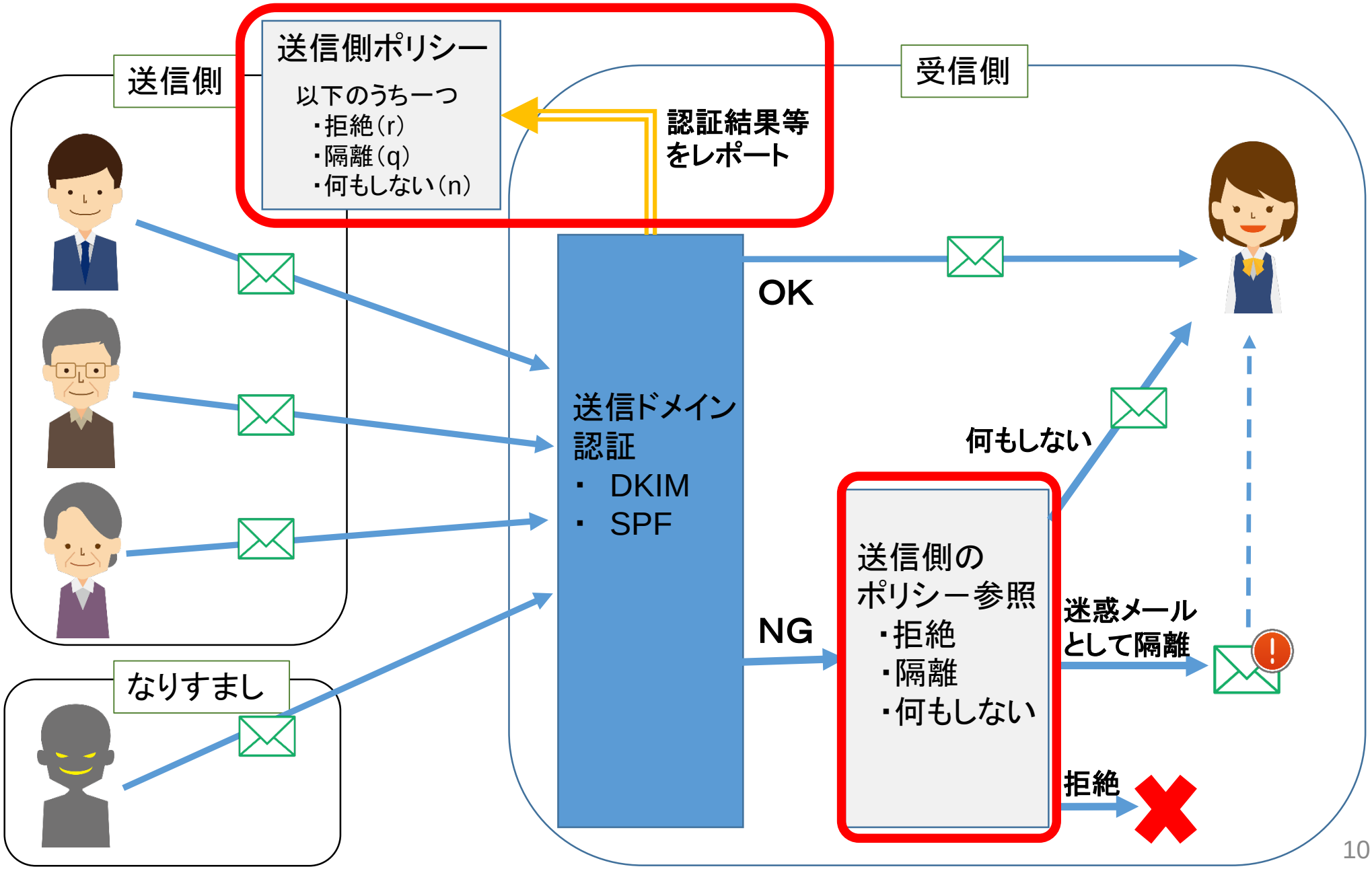
法律的に見ると、

・(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。

DMARCの概要図


送信側
送信側ポリシー
以下のうちーつ
・拒絶（r）
・隔離（q）
・何もしない（n）
認証結果等
をレポート
受信側
OK
送信ドメイン
認証
・ DKIM
・ SPF
何もしない
送信側の
ポリシー参照
・拒絶
・隔離
・何もしない
迷惑メール
として隔離
NG
拒絶
なりすまし

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。

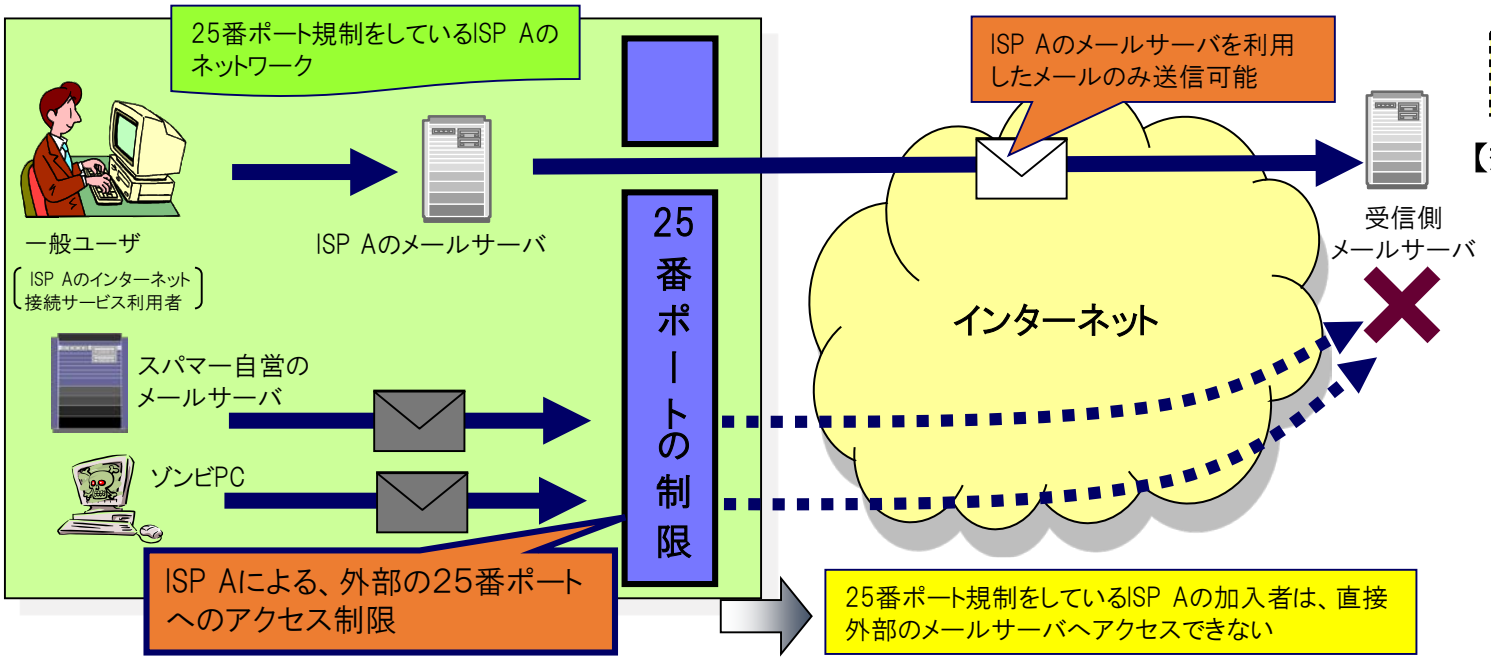
①ポリシーを踏まえて遮断を行う場合

- 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

（4）25番ポートブロック（Outbound Port 25 Blocking(OP25B)）について



メールを送信する際には、メールサーバの25番ポートにアクセスすることが標準。

【効果】

- **メールサーバを自ら設置して送信することが不可能に**
  （スパマーによる大量送信を防げるが、通常の自営メールサーバの利用も不可能に）
- **ゾンビPCからの大量メール送信が困難に**
- **インターネット接続サービスとメールサービスで異なるISPを利用している場合、メール送信が困難に**

1. OP25Bの法的性質

電気通信事業者であるISPが、その支配・管理するルータを通過するすべての電子メールの送信元（及び宛先（※））のIPアドレス及びポート番号を機械的に確認して、当該ISPが提供するメールサーバを経由せずに動的IPアドレスから25番ポートに対して送信した電子メールを割り出し、当該電子メールをブロック（25番ポートを閉じて接続できない状態にする）する行為をいう。

※特定の送信先へのメールについて、25番ポートを閉じる場合。例えば、携帯電話会社あて電子メールについてのみOP25Bを実施する場合には、宛先が携帯電話会社のメールサーバであるか否かを確認することになる。

2. 法的問題点

上記行為が電気通信時業法に抵触しないのか、具体的には、以下のような点が問題となる。

- **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」**に該当するか。
- **電気通信事業法第6条に規定する「不当な差別的取扱い」**に該当するか。

結　　論

- OP25B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。

通信の秘密の侵害に関する検討①

ISPが、その支配・管理するルータを通過するすべての電子メールの送信元IPアドレス・ポート番号を確認して、当該ISPが提供するメールサーバを経由せず動的IPアドレスから25番ポートに対して送信された電子メールを割り出し、ブロックする行為は、**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、通信の秘密の侵害（窃用）に当たる**と考えられる。

OP25Bは、当事者の同意がない限り、「通信の秘密」を「侵す行為」に該当する。

ただし、「ISPが、その支配・管理するルータを通過するすべての電子メールの送信元IPアドレス・ポート番号を確認して、当該ISPが提供するメールサーバを経由せず動的IPアドレスから25番ポートに対して送信された電子メールを割り出し、ブロックする行為」が、通信の秘密侵害行為に該当する場合であっても、**違法性阻却事由があれば（正当防衛、緊急避難又は正当業務行為に該当すれば）、当事者の同意の有無に関わりなく、許される**ことになる。

1．正当防衛、緊急避難該当性

OP25Bは、電子メールの大量送信により電子メール送受信上の支障が生じている場合又は支障の発生が切迫している場合に限らず、電子メール送受信上の支障のおそれを防止するために、**常時行われる対策**

このため、正当防衛の要件である急迫性や、緊急避難の要件である危難の現在性等を必ずしも満たすとは限らないことから、**正当防衛、緊急避難に該当しない場合が想定される。**

通信の秘密の侵害に関する検討②

2. 正当業務行為該当性

「正当業務行為」に該当するといえるには、(1) 行為の正当性、必要性 (2)手段の相当性を満たすことが必要

(1) 行為の正当性、必要性

・ ISPの提供するメールサーバを利用した電子メールの大量送信が行われていないこと
・ ISPのメールサーバを経由しない動的IPアドレスから電子メールが大量送信されていること
・ 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

を満たす場合には、ネットワークを適正に維持管理してメールサービスを運営するために、自ら提供するメールサーバを経由しない動的IPアドレスからの送信について送信制御を行う必要性、正当性が認められる。

(2) 手段の相当性

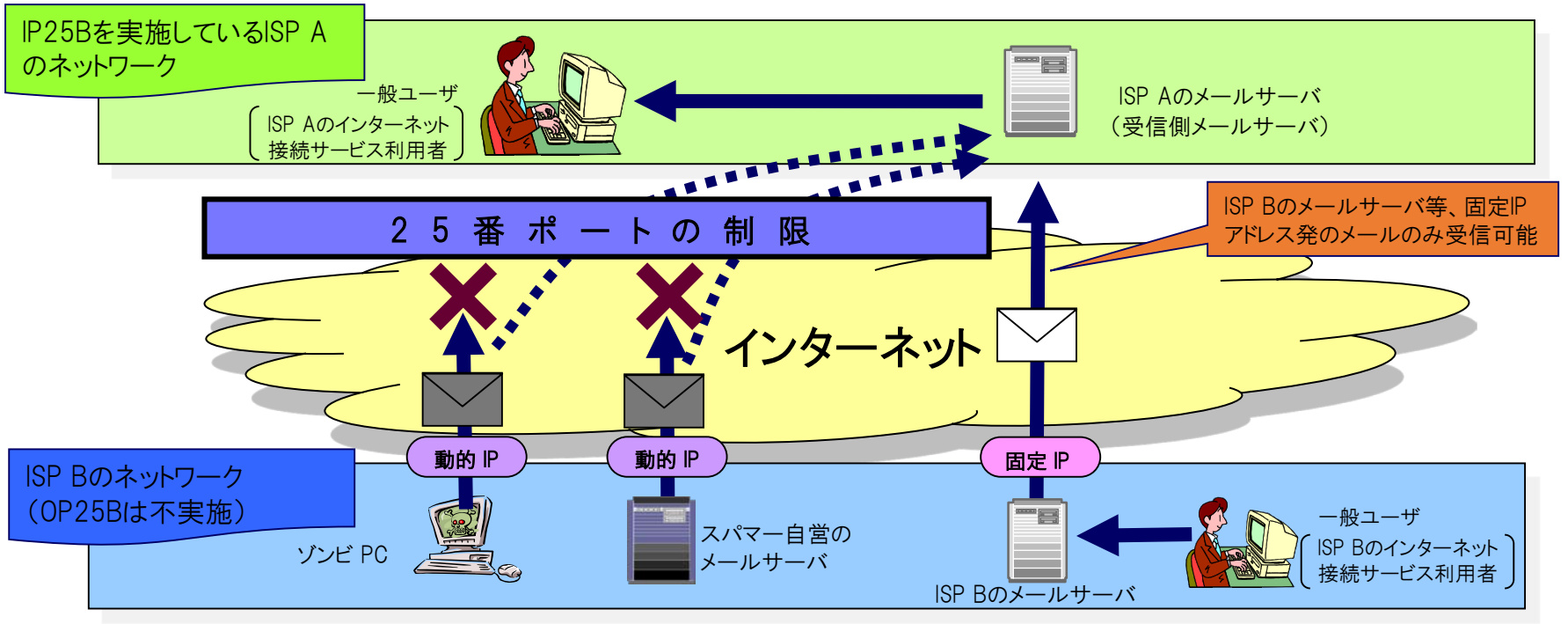
・ OP25Bを行うに当たって侵害することになる通信の秘密は、送信元IPアドレス・ポート番号という通信の経路情報であり、目的達成のために必要な限度にとどまると言える。
・ 迷惑メールに対しては、他にも複数の対策（送信ドメイン認証、サーバにおける送信者認証等）が講じられているが、送信側ISPにおいてそもそもインターネット上に迷惑メールが送信されることを防止する対策であるOP25Bは、適正にメールサービスを運営すると言う目的達成のために相当な方法と考えられる。

以上から、**ISPが、その支配・管理するルータを通過するすべての電子メールの送信元IPアドレス・ポート番号を確認して、当該ISPが提供するメールサーバを経由せず動的IPアドレスから25番ポートに対して送信された電子メールを割り出し、ブロックする行為は、目的達成のために必要かつ相当な方法と認められる。**

→ OP25Bは、正当業務行為（違法性阻却事由あり）と解釈できる。

→ 正当業務行為として許容される対策として一律に実施する場合、
OP25Bは、電気通信事業法第6条に規定する「不当な差別的取扱い」には該当しない。

（５）25番ポートブロック（Inbound Port 25 Blocking(IP25B)）について



1. IP25Bの法的性質

IP25Bとは、電気通信事業者であるISPが、その支配・管理するルータを通過（流入）するすべての電子メールの送信元のIPアドレス及びポート番号を機械的に確認して、動的IPアドレスと判断できるIPアドレス（または送信元ISPから予め提供されている動的IPアドレスのリストに掲載されているIPアドレス）から当該ISP（受信側ISP）の25番ポートに対して、ダイレクトに送信された電子メールを割り出し、当該電子メールをブロック（25番ポートを閉じて接続できない状態にする）する行為をいう。

2. 法的問題点

そこで、上記行為が電気通信時業法に抵触しないのか、具体的には、以下について検討する。

- **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」**に該当するか。
- **電気通信事業法第6条に規定する「不当な差別的取扱い」**に該当するか。

結　　論

- IP25B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 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。

通信の秘密の侵害に関する検討①

ISPが、その支配・管理するルータを流入するすべての電子メールの送信元IPアドレス・ポート番号を確認して、動的IPアドレスから当該ISPの25番ポートに対して直接送信された電子メールを割り出し、ブロックする行為は、**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、通信の秘密の侵害（窃用）に当たる**と考えられる。

IP25Bは、当事者の同意がない限り、「通信の秘密」を「侵す行為」に該当する。

ただし、「ISPが、その支配・管理するルータを流入するすべての電子メールの送信元IPアドレス・ポート番号を確認して、動的IPアドレスから当該ISPの25番ポートに対して直接送信された電子メールを割り出し、ブロックする行為」が、通信の秘密侵害行為に該当する場合であっても、**違法性阻却事由があれば（正当防衛、緊急避難又は正当業務行為に該当すれば）、当事者の同意の有無に関わりなく、許される**ことになる。

1. 正当防衛、緊急避難該当性

IP25Bは、電子メールの大量送信により電子メール送受信上の支障が生じている場合又は支障の発生が切迫している場合に限らず、電子メール送受信上の支障のおそれを防止するために、**常時行われる対策**

このため、正当防衛の要件である急迫性や、緊急避難の要件である危難の現在性等を必ずしも満たすとは限らないことから、**正当防衛、緊急避難に該当しない場合が想定される**。

通信の秘密の侵害に関する検討②

2. 正当業務行為該当性

「正当業務行為」に該当するといえるには、(1) 行為の正当性、必要性、(2)手段の相当性を満たすことが必要

(1) 行為の正当性、必要性

- 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
- 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
- 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

を満たす場合には、ネットワークを適正に維持管理してメールサービスを運営するために、他のISPの動的IPアドレスからの送信について受信制御を行う正当性、必要性が認められる。

(2) 手段の相当性

- IP25Bを行うに当たって侵害することになる通信の秘密は、送信元IPアドレス・ポート番号という通信の経路情報であり、目的達成のために必要な限度にとどまると言える。
- 迷惑メールに対しては、他にも複数の対策（送信ドメイン認証、OP25B等）が講じられているが、受信側ISPのみが対応するだけで効果をあげることができる迷惑メール対策であるIP25Bは、適正にメールサービスを運営するという目的達成のために必要かつ相当な方法と考えられる。

以上から、**ISPが、その支配・管理するルータを流入するすべての電子メールの送信元IPアドレス・ポート番号を確認して、動的IPアドレスから当該ISPの25番ポートに対して直接送信された電子メールを割り出し、ブロックする行為は、目的達成のために必要かつ相当な方法と認められる。**

IP25Bは、正当業務行為（違法性阻却事由あり）と解釈できる。

正当業務行為として許容される対策として一律に実施する場合、IP25Bは、電気通信事業法第6条に規定する「不当な差別的取扱い」には該当しない。