総務省

総務省における
迷惑メール対策について

令和４年１１月
総合通信基盤局
電気通信事業部
消費者行政第二課

小澤　孝洋

小澤　孝洋

OZAWA Takahiro

【経歴】

2011年４月 総務省入省
2013年７月 総務省 秘書課（採用担当）
2014年７月 総務省 研究推進室
2016年７月 総務省 消費者行政第二課
（通信の秘密・特殊詐欺対策）
2017年４月 内閣官房 IT総合戦略室
（IT戦略策定・デジタルガバメント・オープンデータ等）
2019年６月 高松市総務局参事・デジタル推進部長
（スマートシティ・ＤＸ・デジタル政策等）
2022年７月 総務省 消費者行政第二課（現職）
（課内総括、特殊詐欺、迷惑メール／フィッシング詐欺対策）

利用者視点からの電気通信サービスの課題

○高度化・多様化した電気通信サービスが国民各層に広く普及・浸透

- スマートフォン、タブレット型端末の普及とそれに伴う新たなサービスの出現
- IoTやAI、5G等の進展、ネットワーク仮想化技術の普及等によって、電気通信事業者やプラットフォーム事業者の多様なビジネスモデルによるサービス提供に伴うデータの利活用が大きく進展

○利用者が安心して新たなサービスを利用できる環境の整備が必要

サービス利用における安心・安全の確保

○ グローバル化する電気通信サービスへの対応
○ プラットフォーム事業者の利用者情報の適切な取扱い等の確保
○ 新しいサービスに対する利用者への情報提供
○ 青少年や高齢者への配慮（リテラシー向上等）

電気通信役務の不適正利用対策

○ 個人情報の漏えいや通信の秘密の侵害等への対応
○ インターネット上の違法・有害情報対策
○ 迷惑メール対策
○ 携帯電話・電話転送サービスの不適正利用（振り込め詐欺等）防止　等

新たなサービスに伴う課題に対する迅速な対応

Society5.0を見据えたルール整備等

安全・安心な利用環境の整備

不適正利用への対応

消費者行政第二課の所管業務の全体像

【１　「通信の秘密」と「利用者情報」の保護】

（関連法令等）・電気通信事業法第4条、第29条及び第179条の「通信の秘密」
・「電気通信事業における個人情報保護に関するガイドライン」

① 利用者情報の適切な取扱いに係る検討（外部送信規律の適正な実施、定期的なモニタリング等）
② サイバー攻撃への適切な対処
③ 電気通信事業における個人情報保護に関するガイドライン等の運用、④ 児童ポルノサイトブロッキング
⑤ 通信ログの保存と利用、⑥ デジタル市場本部、経済産業省との調整（デジタル広告市場等）
⑦ IoT推進コンソーシアムにおける議論、 ⑧ 監督（漏えい事案対応等）

【２　インターネット上の違法・有害情報対策】

（関連法令等）・特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律（プロバイダ責任制限法）

①インターネット上の違法・有害情報（誹謗中傷・偽情報等）対策（透明化に係る法的枠組みの検討、政策パッケージの推進）
②プロバイダ責任制限法改正法の施行に向けた準備
③インターネット上の海賊版対策（アクセス抑止方策、CDN対策等）
④ 違法・有害情報相談センターの運営
⑤ その他、インターネット上の違法・有害情報への対応（ヘイトスピーチ、部落差別、AV出演強要、自殺誘引、テロ対策）

【３　電気通信の不適正利用対策（特殊詐欺、迷惑メール、フィッシング詐欺対策等）】

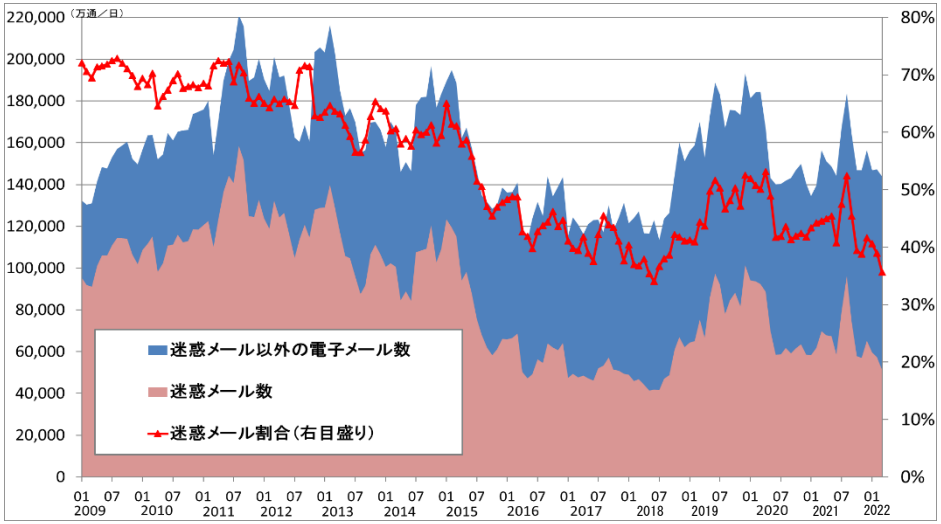
（関連法令等）・携帯音声通信事業者による契約者等の本人確認等及び携帯音声通信役務の不正な利用の防止に関する法律（携帯電話不正利用防止法）
・犯罪による収益の移転防止に関する法律（犯罪収益移転防止法）
・特定電子メールの送信の適正化等に関する法律（特電法）

① 特殊詐欺における電話利用への対策強化、 ② 携帯電話不正利用防止法及び犯罪収益移転防止法の適切な執行
③ 迷惑メール等対策の着実な実施（フィッシング対策含む）
④ FATF第4次対日相互審査対応等（犯罪収益移転防止法関係）

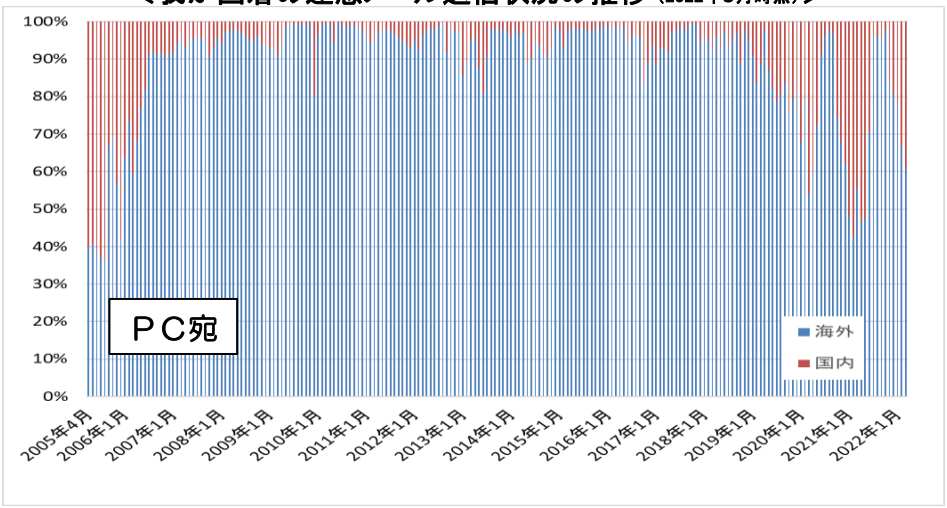
我が国における迷惑メールの現状

○　我が国の電気通信事業者が受信した電子メール中、迷惑メールが占める割合は現在は約４割前後。
○　我が国に到着した迷惑メールのうち、ＰＣアドレス宛の６割前後、携帯アドレス宛の９割以上が外国発。
○　迷惑メールのうち、出会い系サイトや物販の広告宣伝を内容とするものが約９割近くを占めている。

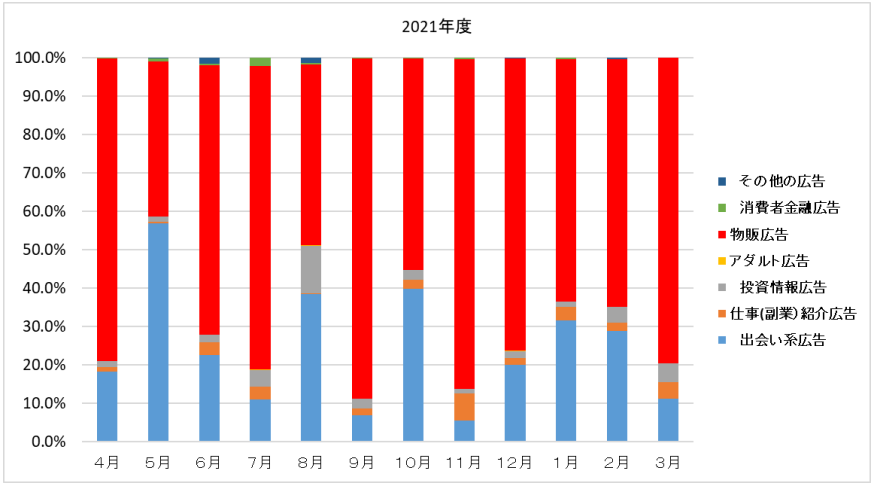
＜国内ISPにおける迷惑メール数・割合の推移（2022年3月時点）＞

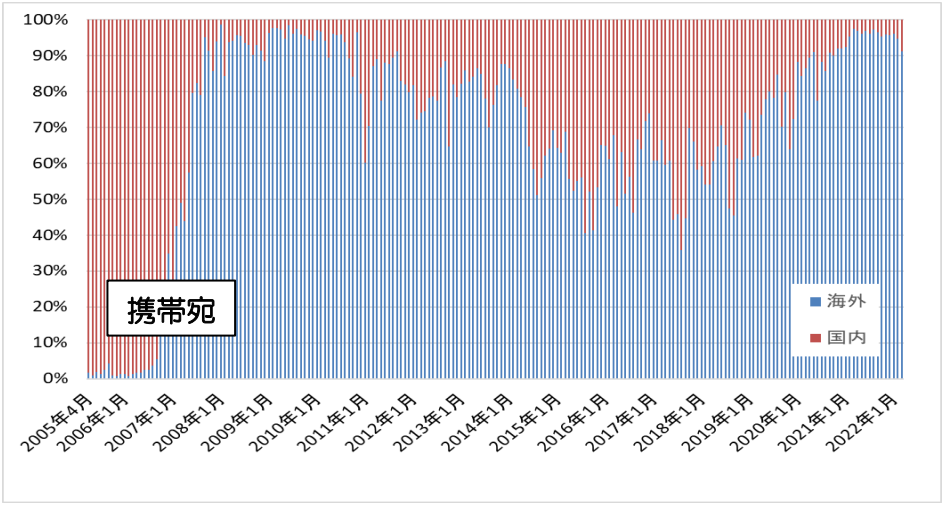


＜我が国着の迷惑メール送信状況の推移（2022年3月時点）＞



＜迷惑メールの広告宣伝内容別の構成比率（2021年度）＞



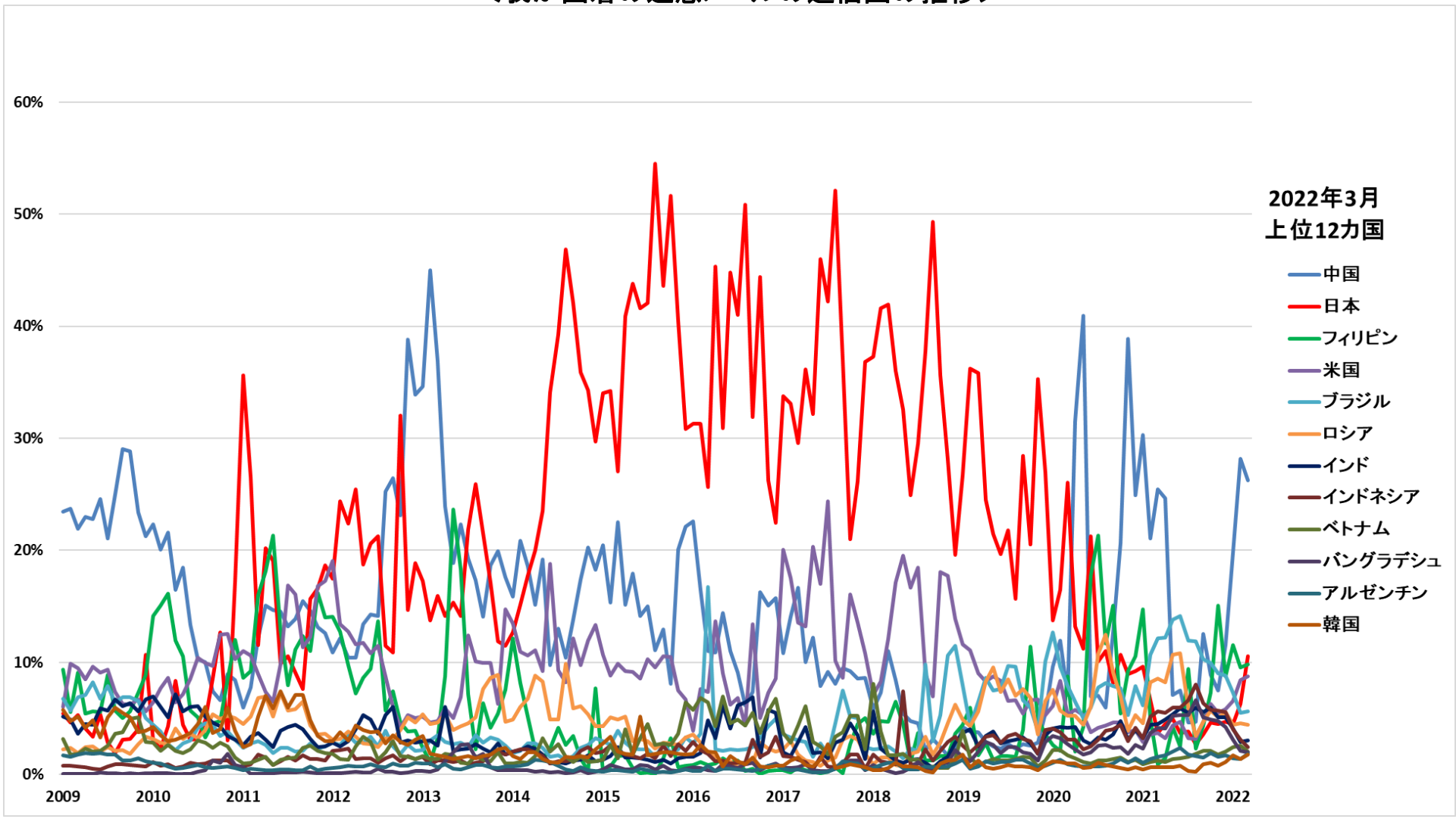


出典：一般財団法人日本データ通信協会迷惑メール相談センター調べ（相談センターのモニター機で受信した情報を分析したもの）

我が国の迷惑メール送信の動向

○　我が国着の迷惑メールの送信国は月によって変動はあるが、我が国発のものを除くと、米国・中国・フィリピン発のものが継続的に多く見られる。

＜我が国着の迷惑メールの送信国の推移＞



出典：一般財団法人日本データ通信協会迷惑メール相談センター調べ（相談センターのモニター機で受信した情報を分析したもの）

「特定電子メール法※」の概要

※特定電子メールの送信の適正化等に関する法律（平成14年法律第26号）

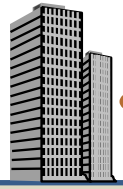
最近の執行状況	警告	報告徴収	措置命令
令和元年度	6,045	0	0
令和2年度	7,055	1	0
令和3年度	6,363	0	0

送信者・送信委託者

〇オプトイン規制
　－同意のない者への原則送信禁止
　－同意の記録保存義務
　－受信拒否者への再送信禁止
〇表示義務
〇送信者情報偽装禁止
〇架空電子ﾒｰﾙｱﾄﾞﾚｽあての送信禁止

外国執行当局

措置命令
立入検査
報告徴収
警告



情報提供

※電子メールの送受信上の支障を防止するために必要な範囲内であると認められる場合

役務提供拒否

送信者等の契約者情報照会

指導・助言

総務大臣　**消費者庁長官**

申　出

※架空電子メールアドレスあての送信が認められるとき

電気通信事業者

登録・監督

情報提供等

申　出

※オプトイン規制違反、表示義務違反、送信者情報を偽装した送信が認められるとき

受信者

登録送信適正化機関

（一財）日本データ通信協会
迷惑メール相談センター

主要な罰則

送信者情報を偽った送信			１年以下の懲役または100万円以下の罰金（法人重課：3000万円以下の罰金） ※総務大臣及び内閣総理大臣による命令の対象ともなる
架空電子メールアドレスあて送信（電子メールの送受信上の支障を防止する必要があると総務大臣が認めるとき）	受信拒否者への送信	表示義務違反	総務大臣及び内閣総理大臣による命令。命令に従わない場合、１年以下の懲役または100万円以下の罰金（法人重課：3000万円以下の罰金）
	同意のない者への送信		
同意の記録義務違反			総務大臣及び内閣総理大臣による命令。命令に従わない場合、100万円以下の罰金（法人重課：100万円以下の罰金）

迷惑メール対策推進協議会

目的

○ 迷惑メール対策に関する関係者間の緊密な連絡を確保し、最新の情報共有、対応方策の検討、対外的な情報提供などを行うことを目的とし、2008年11月27日に、迷惑メール対策に関する関係者が幅広く集まり、「迷惑メール対策推進協議会」を設立。
（座長：新美育文明治大学名誉教授、事務局：一般財団法人日本データ通信協会 迷惑メール相談センター、構成員54名（2022年10月現在））。

構成

○ 電気通信事業者、広告事業者、配信ASP事業者、セキュリティベンダー、学識経験者、関係省庁（総務省、消費者庁、警察庁）等。

○ 総会（年１回開催）のほか、幹事会を設置（年１回開催）。

○ 送信ドメイン認証技術の普及その他の技術的課題に関し、方針案の作成、基礎的資料の作成等を行うため、技術WGを設置。
（主査：櫻庭 秀次 株式会社ｲﾝﾀｰﾈｯﾄｲﾆｼｱﾃｨﾌﾞ ﾈｯﾄﾜｰｸｸﾗｳﾄﾞ本部 ｱﾌﾟﾘｹｰｼｮﾝｻｰﾋﾞｽ部 担当部長）

主な活動

○ 「情報化促進貢献個人等表彰」の受賞
2018年10月１日、総務省が行う「情報化促進貢献個人等表彰」の「企業部門」において総務大臣賞を受賞。

○ 「迷惑メール白書」の発行
2009年より、迷惑メールの現状、対策、取組等を「迷惑メール対策ハンドブック」として冊子にまとめ発行、毎年改訂。2018年から内容を見直し、名称についても新たに「迷惑メール白書2018」として発行。

○ 「送信ドメイン認証技術導入マニュアル」の発行
なりすましメールを防ぐため、電子メールの受信側が、送信側のドメイン名の正当性を確認することができる「送信ドメイン認証技術」について、企業等への導入を促すため、送信ドメイン認証技術の概要や導入に必要となる手順や内容を解説したマニュアルを取りまとめ、令和３年９月に第３版を公開・発行。

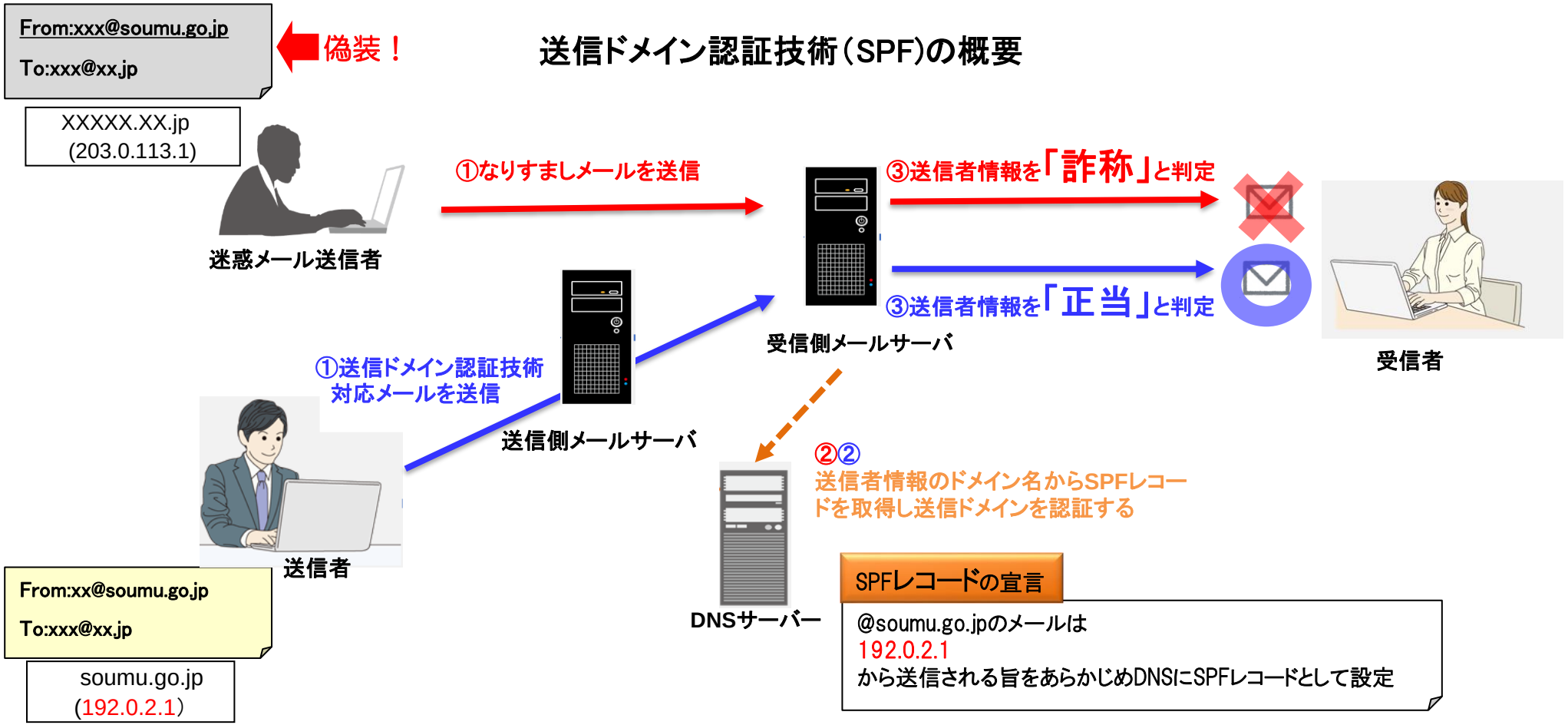
迷惑メール白書　送信ドメイン認証技術導入マニュアル

○ 送信ドメイン認証技術の普及促進
政府機関における送信ドメイン認証技術の導入を促進するため、内閣サイバーセキュリティセンター（NISC）公表の「政府機関等の情報セキュリティ対策のための統一基準」の改訂に際し、本基準を遵守するための対策事項を示した「政府機関等の対策基準策定のためのガイドライン」に、当該技術に関連した記述を追加。※

※ この他にも、（財）日本データ通信協会（令和２年度からは（財）インターネット協会）と株式会社日本レジストリサービス（JPRS）が共同で調査している、JPドメイン名における送信ドメイン認証技術の設定状況について、総務省がその結果を定期的に公表したり、企業や自治体へ導入を促すため、（財）日本データ通信協会から地方公共団体情報システム機構（J-LIS）などに対して、説明機会の付与等の働きかけを行っている。

送信ドメイン認証技術

○　フィッシングメールを含む迷惑メール送信者は、受信者にメールを開いてもらうために有名なサイトに見せかけたり、送信者を特定しづらくするため、自前のサーバー等から直接迷惑メールを送信する際、ドメインを詐称して送信することが多い。
○　受信側でこの詐称を検出できるようにするのが送信ドメイン認証技術（SPF※１、DKIM※２、DMARC※３）である
○　送信ドメイン認証技術の導入により、認証結果を踏まえ詐称と判断されたメールは受信しない等対策が可能となる。



※１　SPF（Sender Policy Framework）：送信側のメールサーバーのIPアドレスをDNSで宣言することにより、ネットワーク的に認証を実施する技術。
※２　DKIM（DomainKeys Identified Mail）：送信側のメールサーバーで作成した電子署名により認証する技術。
※３　DMARC(Domain-based Message Authentication, Reporting, and Conformance)：SPF・DKIMの認証結果を利用し総合的に送信ドメイン認証を行う技術。

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

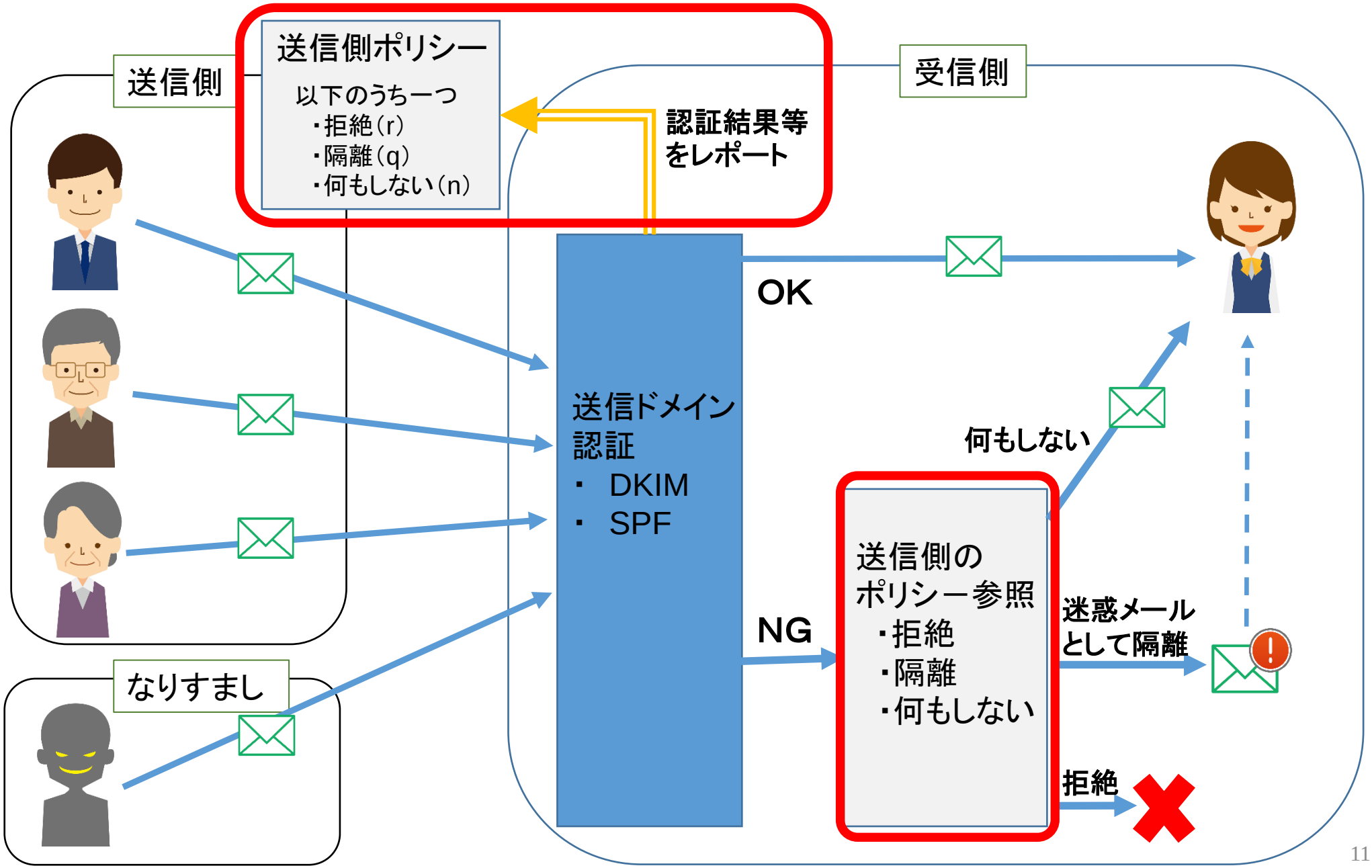
法律的に見ると、

・(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。

DMARC導入によるメリット

○　SPFはメール送信元から配送経路の詐称を検知、DKIMは電子署名を利用することで署名者の認証およびメール本文の改ざんを検知可能。

○　DMARCは、SPF・DKIMの認証結果を利用し総合的に送信ドメイン認証を行う技術であるため、SPF・ DKIMを導入するメリットに加え、受信者に表示される送信者アドレスの詐称に対応可能であること等からフィッシングメールに非常有効。

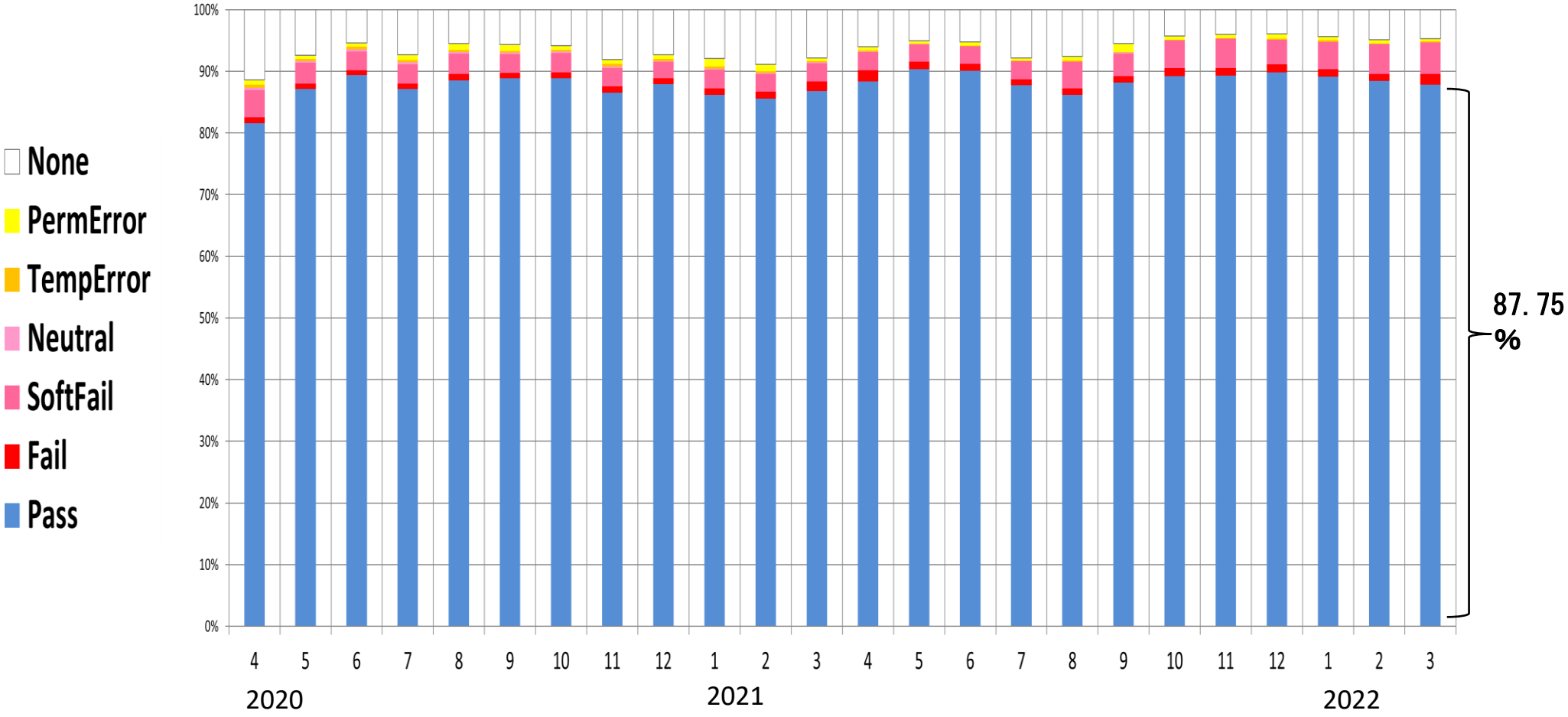
○　消費者委員会意見（令和２年１２月３日）においてフィッシングメールの受信防止対策として、特にDMARC普及が求められている。

【DMARC導入によるメリット】

メール受信側	○ 受信者に表示される送信者アドレスの詐称に対応可能 SPF/DKIMで認証したドメイン名と、受信者がメールを開いた際に表示される送信者アドレスのドメイン名が一致しているか確認 ○ 認証に失敗したメールの処理に受信側が迷わない 認証に失敗した場合の処理方法（DMARCポリシー）を送信側が指定
メール送信側	○ 認証失敗時の処理方法を表明可能 認証に失敗した場合の扱い（DMARCポリシー）を送信側が指定 ○ メール送信環境の確認、改善が可能 フィードバックレポートによる認証結果の把握 ○ なりすましメールの送信状況や送信元を把握することができる フィードバックレポートによる認証結果の把握

送信ドメイン認証結果の導入状況①（ＳＰＦ）

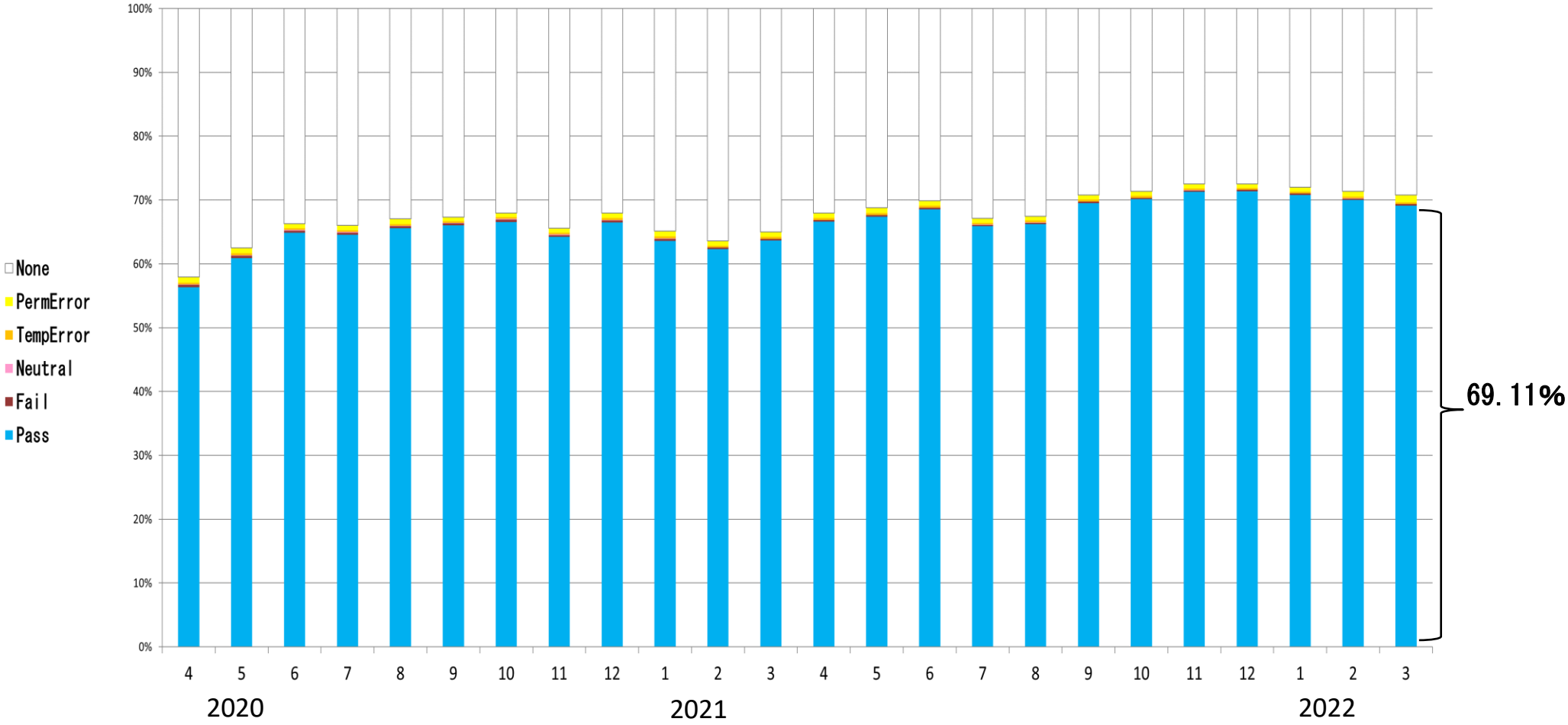
○　送信ドメイン認証結果を調査したところ、SPF（※１）に対応しているメールは約９割



※1　SPF（Sender Policy Framework）：**送信側のメールサーバーのIPアドレス**をDNSで宣言することにより、ネットワーク的に**認証**を実施する技術。
　　メールサーバー間の通信でやりとりされる送信者情報を用いる。
※2　電気通信事業者７社の協力により、総務省が取りまとめ。

送信ドメイン認証結果の導入状況②（DKIM）

○　送信ドメイン認証結果を調査したところ、DKIM（※１）に対応しているメールは約７割

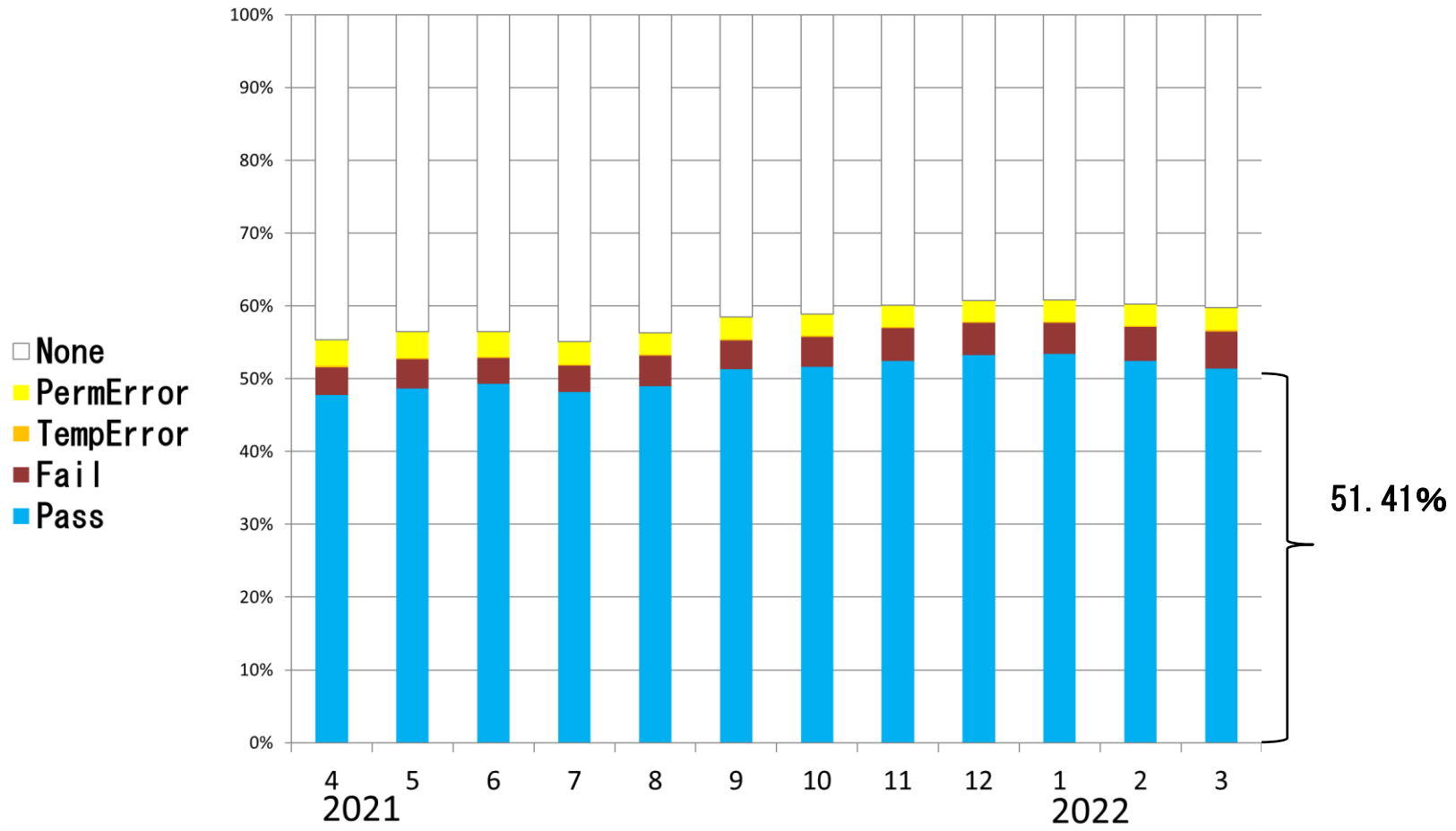


※１　DKIM（DomainKeys Identified Mail）：**送信側のメールサーバーで作成した電子署名**により**認証**する技術。送信元情報の真偽及び電子メールの本文の改ざんの有無を確認することができる。

※２　電気通信事業者４社の協力により、総務省が取りまとめ。

送信ドメイン認証結果の導入状況③（DMARC）

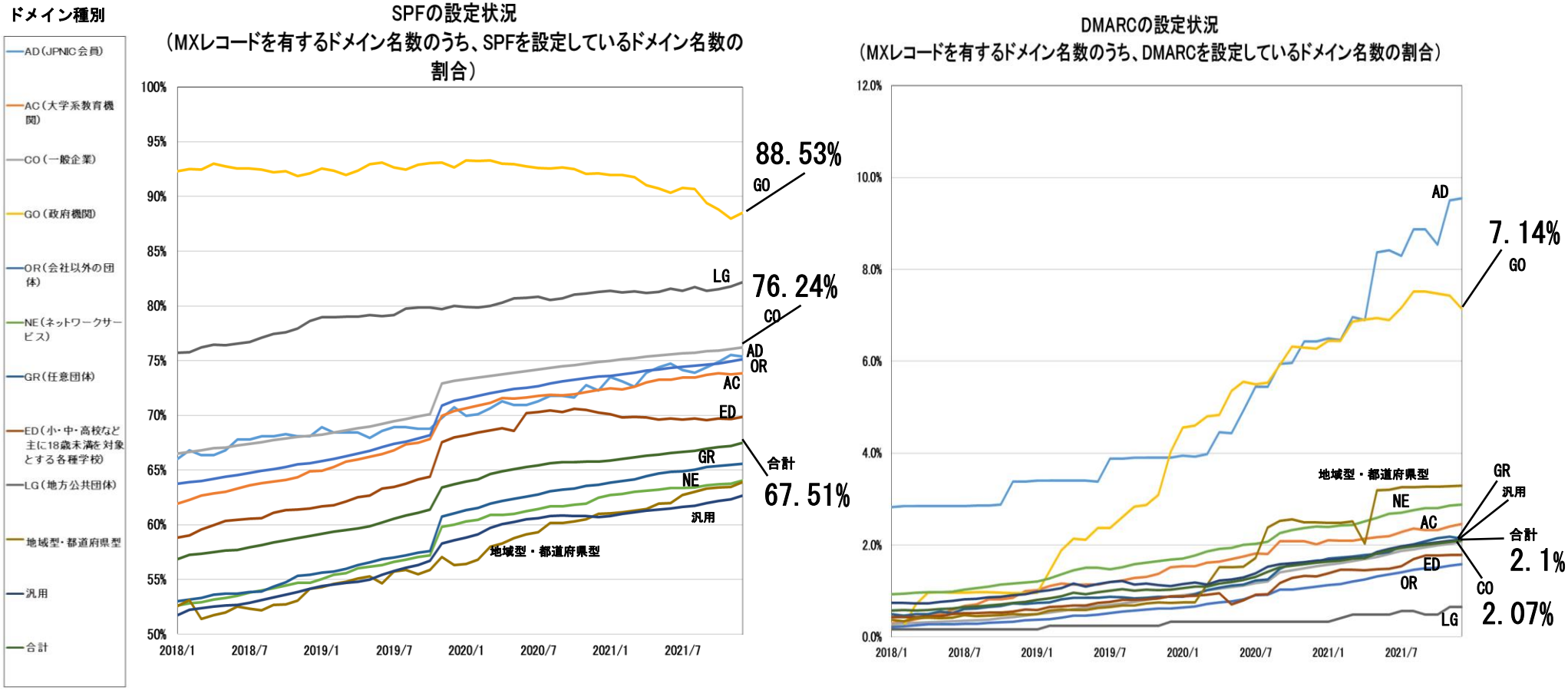
○　送信ドメイン認証結果を調査したところ、DMARC（※１）に対応しているメールは約５割



※１　DMARC（Domain-based Message Authentication, Reporting, and Conformance）：SPF・DKIMの認証結果を利用し総合的に送信ドメイン認証を行う技術。
※２　電気通信事業者４社の協力により、総務省が取りまとめ。

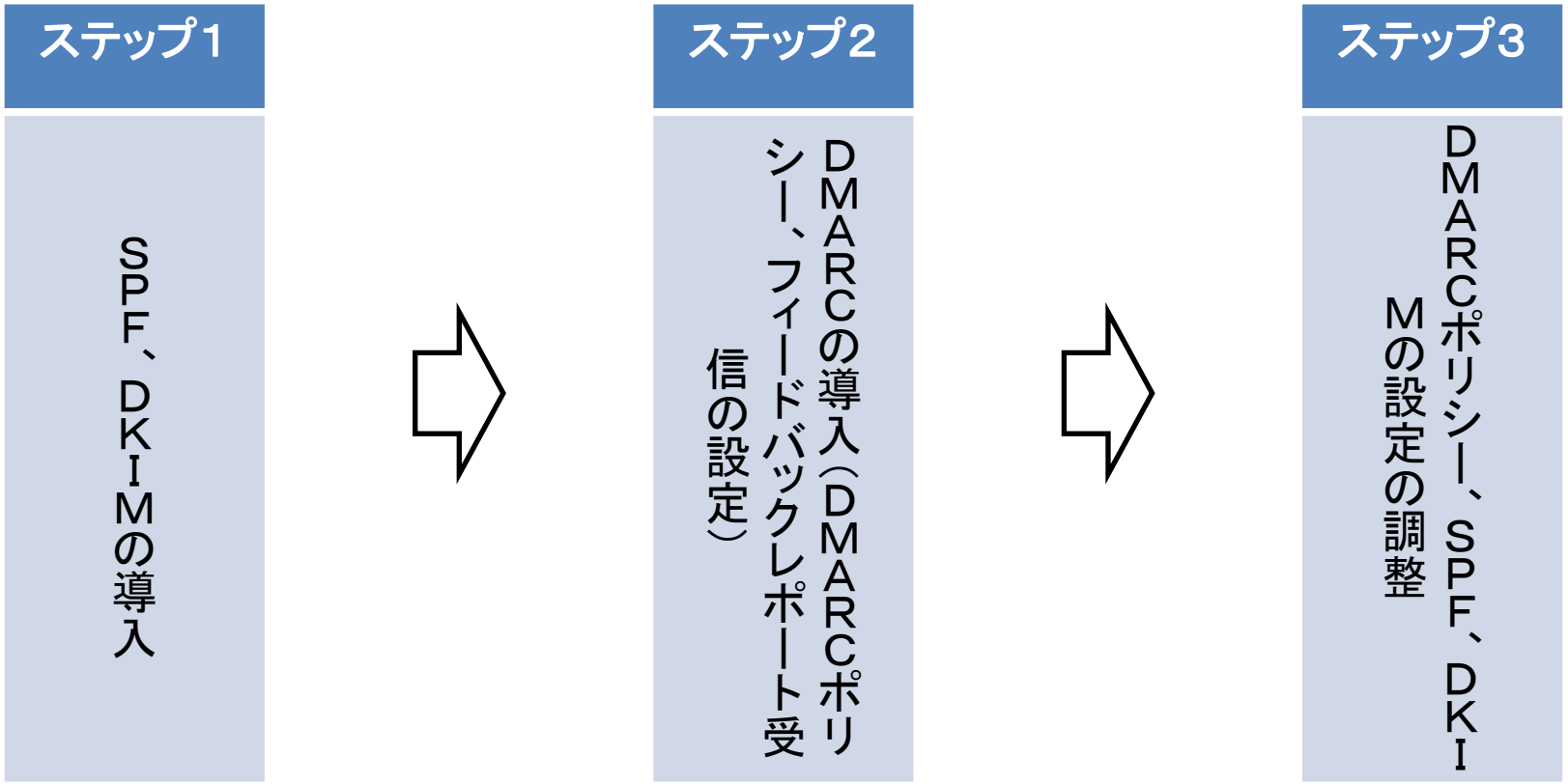
JPドメインにおける送信ドメイン認証技術の導入状況

○　JPドメイン名における送信ドメイン認証技術の導入状況は、全体としては
SPF：67.51%のドメインで導入、DMARC：2.1%のドメインで導入しており、
政府機関（GO）におけるSPFの導入は約90% 、DMARCの導入は7.14%（2021年12月時点）



注１　SPF：Sender Policy Framework。送信側のメールサーバーのIPアドレスをDNSで宣言することにより、ネットワーク的に認証を実施する技術。
　　メールサーバー間の通信でやりとりされる送信者情報を用いる。
注２　DMARC：SPFと電子署名の技術を用いるDKIMの認証の結果を元にして、認証に失敗した電子メールの取扱いを送信側で宣言する技術。

DMARCの導入手順



・まず、SPFおよびDKIMを導入します。

※１　SPF、DKIMのいずれかを導入すればステップ２のDMARCの導入は可能

※２　SPF及びDKIMの導入方法の詳細は、https://www.dekyo.or.jp/soudan/data/anti_spam/201108MN_all.pdf

DMARCの導入

・認証に失敗したメールの扱い（拒否、隔離、何もしない）を決めるDMARCポリシーを設定

・フィードバックレポート受信のための設定

を行います。

・フィードバックレポートに基づき、 DMARCポリシー、SPF、DKIMの設定の調整を行います。

送信ドメイン認証技術導入マニュアル（第３版）の公開

○送信ドメイン認証とは、ドメインを詐称して送信されるフィッシングメールを含む迷惑メールについて、受信側で詐称を検出できるようにする技術。

○　データ通信協会では、これまで、2010年7月に送信ドメイン認証技術導入マニュアルを作成、公表し、2011年8月にこれを改訂、マニュアル第二版を公開するなど、送信ドメイン認証技術の普及に取り組んでいる。

○令和３年9月27日に、送信ドメイン認証技術導入マニュアル第三版を公開し、新たな技術であるDMARC ※を中心に、企業等への導入を促すため、送信ドメイン認証技術の概要や導入に必要となる手順や内容を解説。

○総務省においてもDMARCを含めた送信ドメイン認証技術の設定状況を公表するなど普及に取り組んでいる。

※　DMARC(Domain-based Message Authentication, Reporting, and Conformance):SPF・DKIMの認証結果を利用し総合的に送信ドメイン認証を行う技術。

最後に

DMARCの積極的な導入を
お願いします。