

迷惑メール対策に係る取組みについて

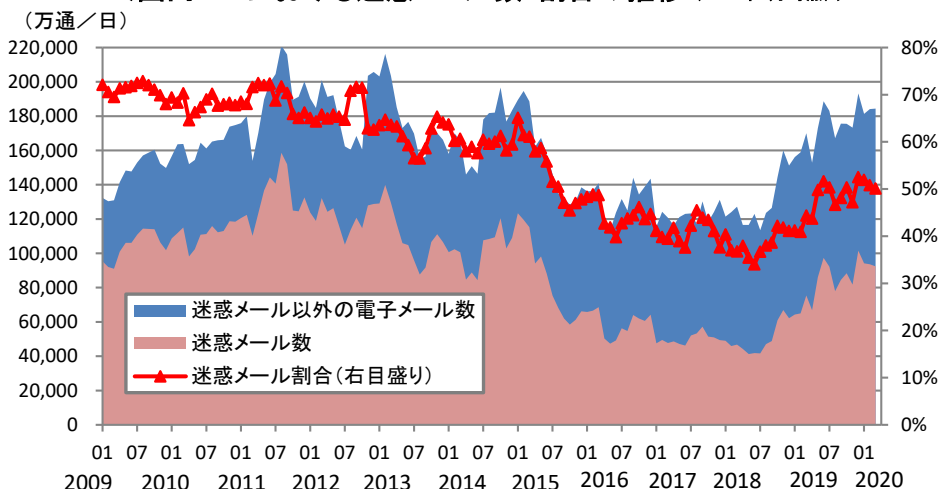
令和2年11月

総務省

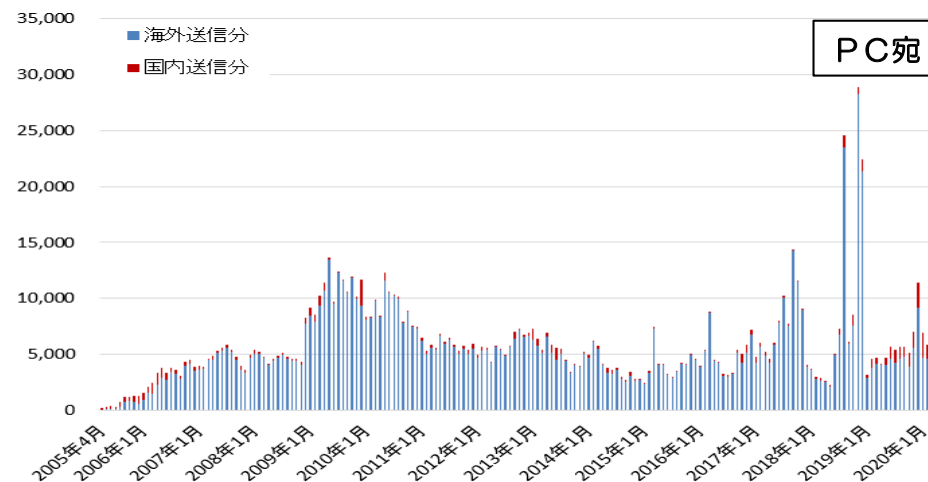
我が国における迷惑メールの現状

- 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5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9割以上、携帯アドレス宛の6割前後が外国発。
- 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8割近くを占めている。

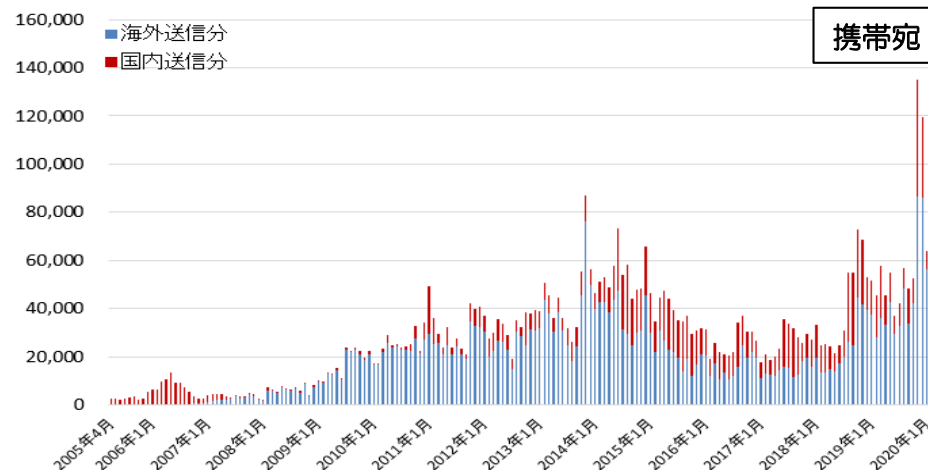
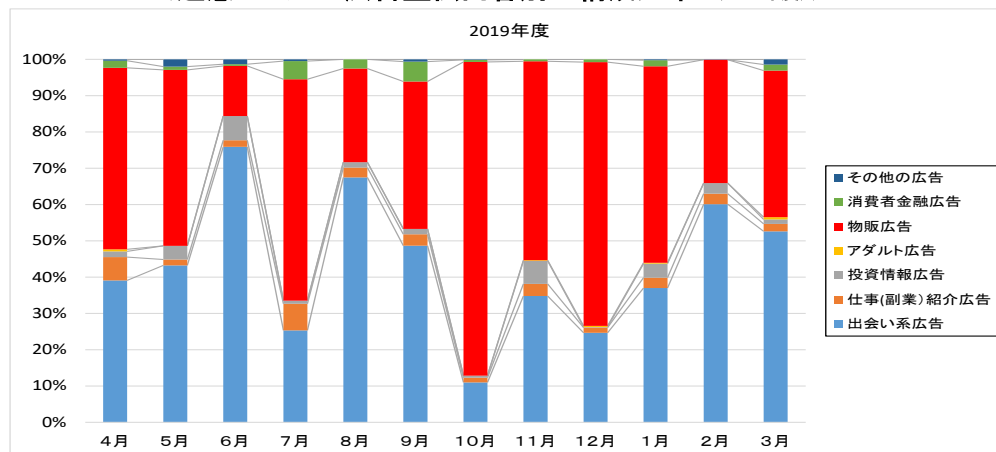
＜国内ISPにおける迷惑メール数・割合の推移（2020年3月時点）＞



＜我が国着の迷惑メール送信状況の推移（2020年3月時点）＞



＜迷惑メールの広告宣伝内容別の構成比率（2019年度）＞

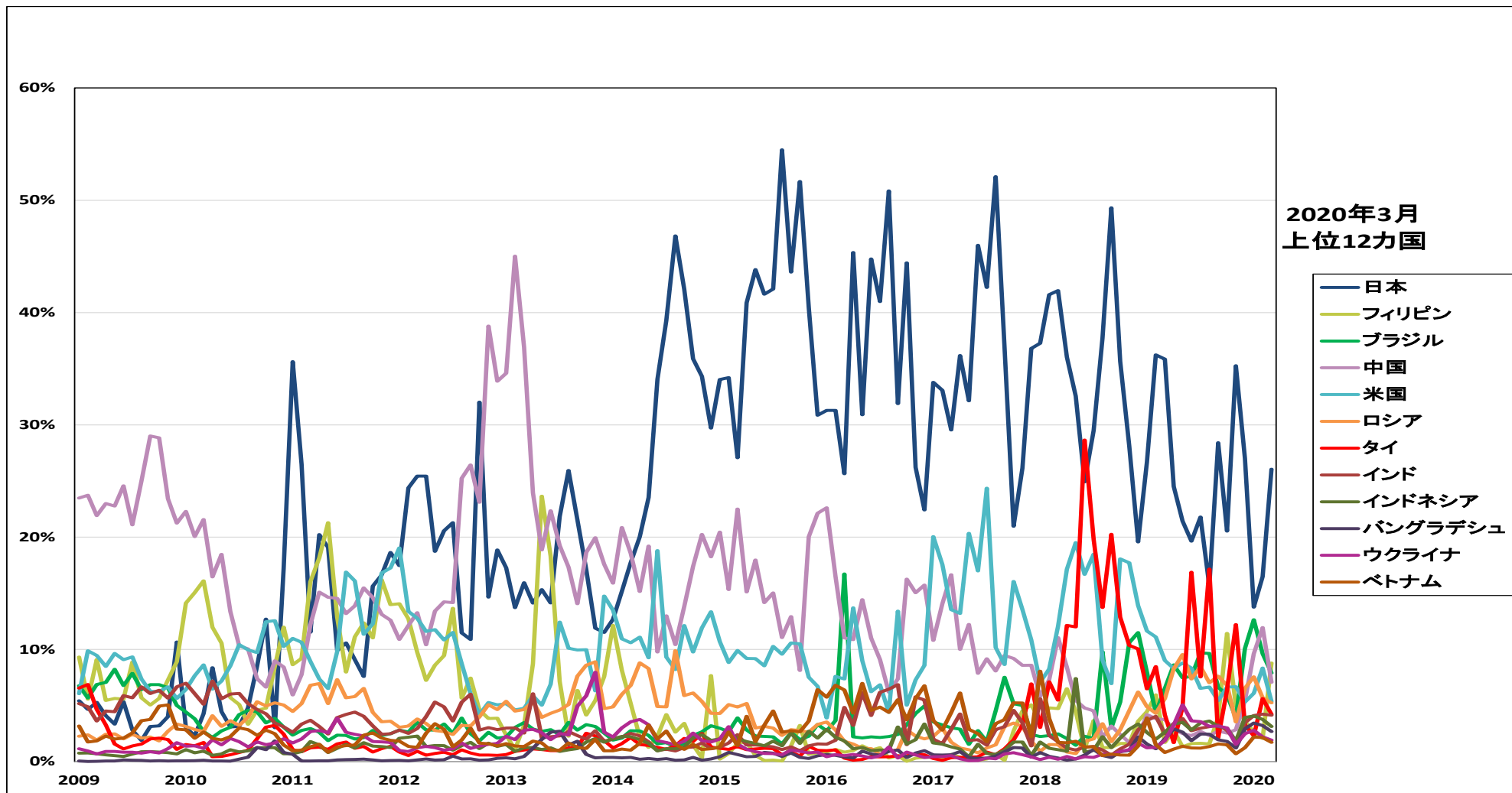


出典：一般財団法人日本データ通信協会迷惑メール相談センター調べ（相談センターのモニター機で受信した情報を分析したもの）

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＞

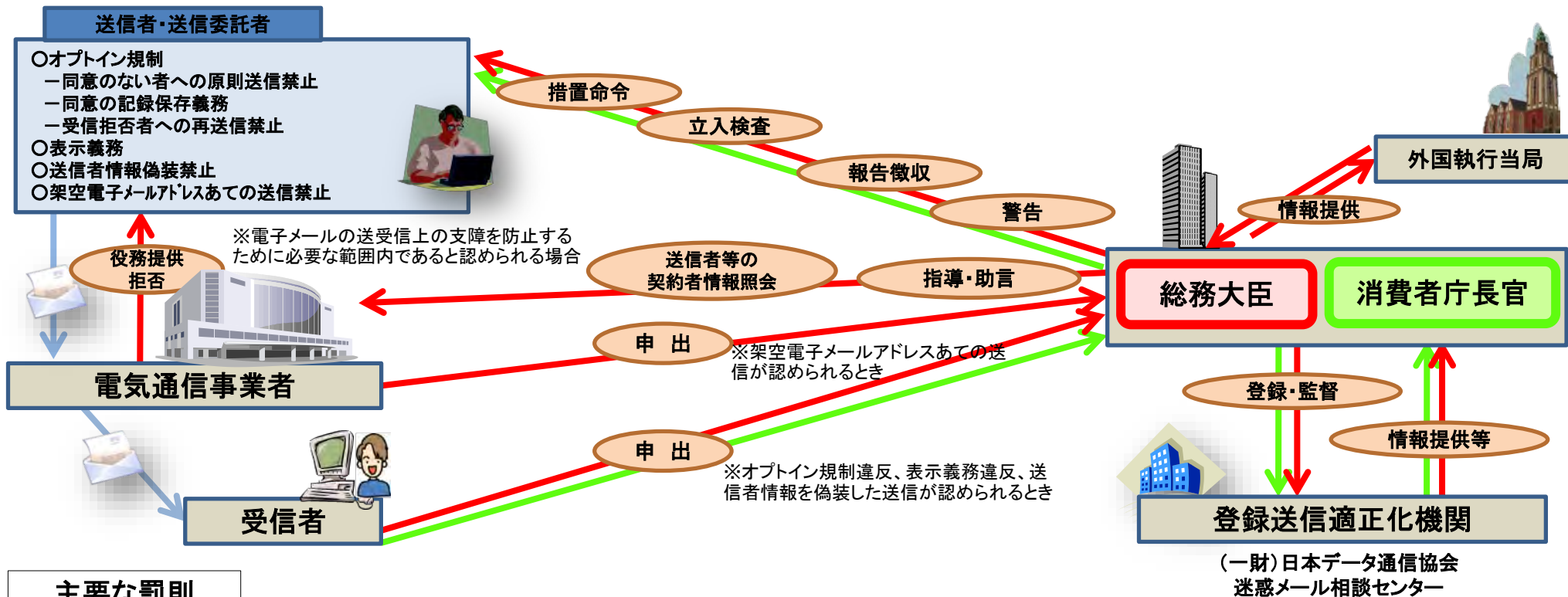


特定電子メールの送信の適正化等に関する法律について

3

- 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）は、特定電子メールの送信の適正化のための措置を講ずることにより、一時に多数の者に対してされる特定電子メールの送信等による電子メールの送受信上の支障を防止し、電子メールの利用についての良好な環境の整備等を図ることを目的としている。

特定電子メール：送信者（営利を目的とする団体及び営業を営む個人に限る。）が自己又は他人の営業につき広告又は宣伝を行うための手段として送信する電子メール



主要な罰則 (Main Penalties)

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

同意のない者への送信

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）

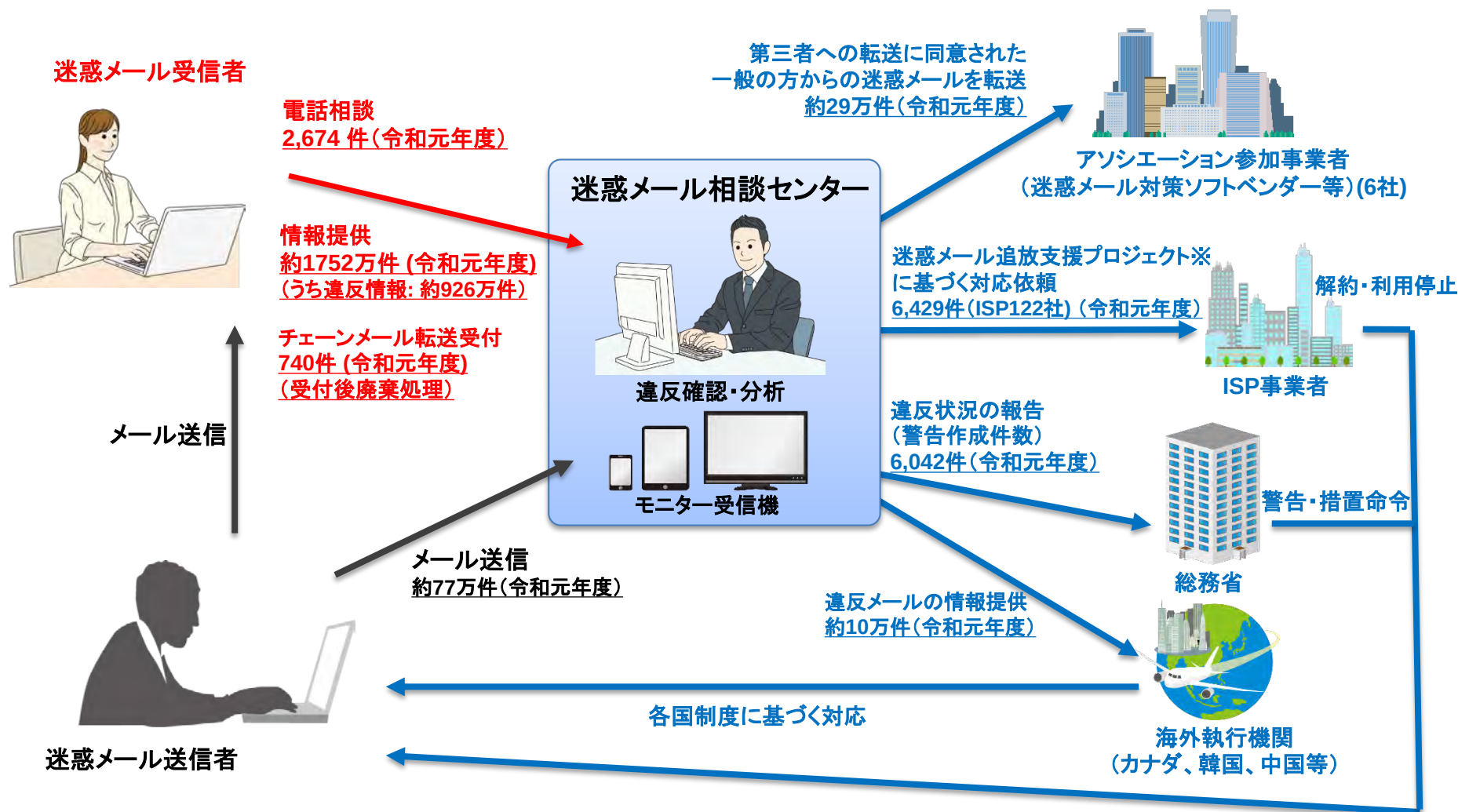
同意の記録義務違反

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）

特定電子メールの送信の適正化等に関する法律の執行体制

4

- 特定電子メールの送信の適正化等に関する法律の効率的な執行等に資するため、迷惑メールに係る受信者からの電話相談や情報提供受付を通じた情報収集、迷惑メールに係る違法性確認・分析等に関する業務について、国以外の者に委託して実施（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）が業務を受託）。



※ 総務省及び消費者庁が民間事業者による自主的なメール対策を促すために実施。特定電子メール法に違反して送信されたメール（いわゆる迷惑メール）に関する情報をISP事業者へ通知し、迷惑メール送信者の利用停止措置などの円滑な実施を促す。

(迷惑メール白書2020を元に作成)

迷惑メール対策推進協議会の取組

- 迷惑メール撲滅を目指し、産官学の迷惑メール対策の関係者間で効果的な迷惑メール対策の推進を図ることを目的として、2008年11月27日に発足。
- 緊密な連携を確保し、最新の情報共有、対策方針の検討、対外的な情報提供などを実施

■ 体制

迷惑メール対策推進協議会 (Anti-Spam mail Promotion Council(ASPC))

座長: 新美育文 明治大学名誉教授

座長代理: 櫻庭秀次 (株)インターネットイニシアティブ
アプリケーションサービス部 担当部長

構成員:

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)など56名

幹事会

技術WG

主査: 櫻庭秀次 (株)インターネットイニシアティブ アプリケーション
サービス部担当部長

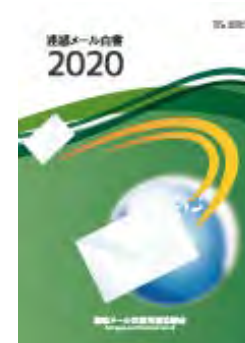
事務局

(一財)日本データ通信協会 迷惑メール相談センター

■ 主な活動内容

- ・「迷惑メール追放宣言」の採択
- ・迷惑メール対策推進協議会総会、技術WG等の開催
- ・「迷惑メール白書」「送信ドメイン認証技術導入マニュアル」
の作成・公表・周知啓発 等

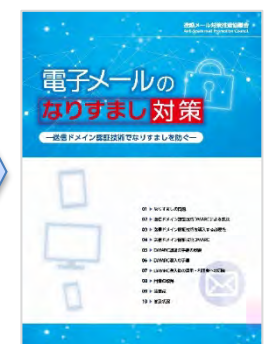
迷惑メール白書



送信ドメイン認証技術 導入マニュアル

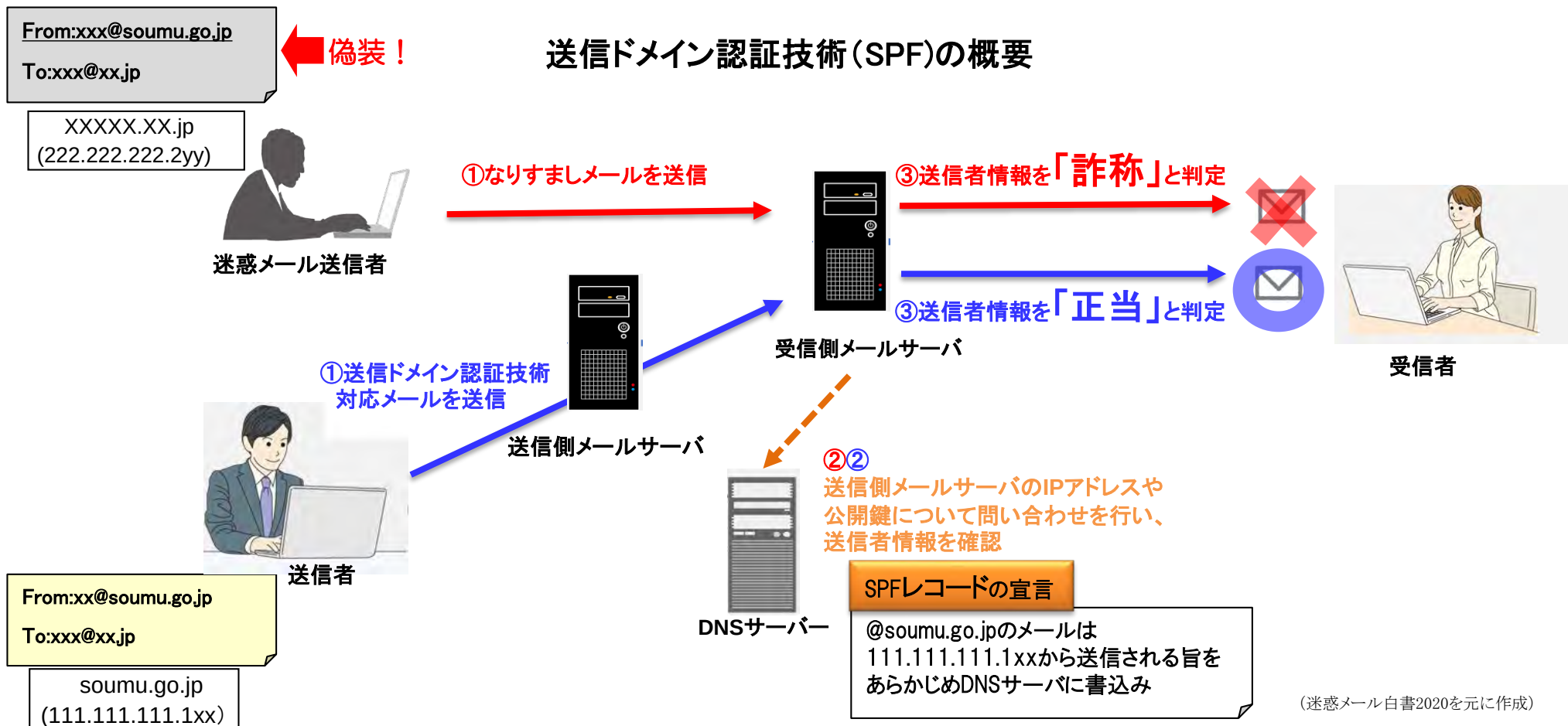


電子メールのなりすまし対策 —送信ドメイン認証でなりすましを防ぐ— (一財)日本データ通信協会



送信ドメイン認証技術による技術的対応

- 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。



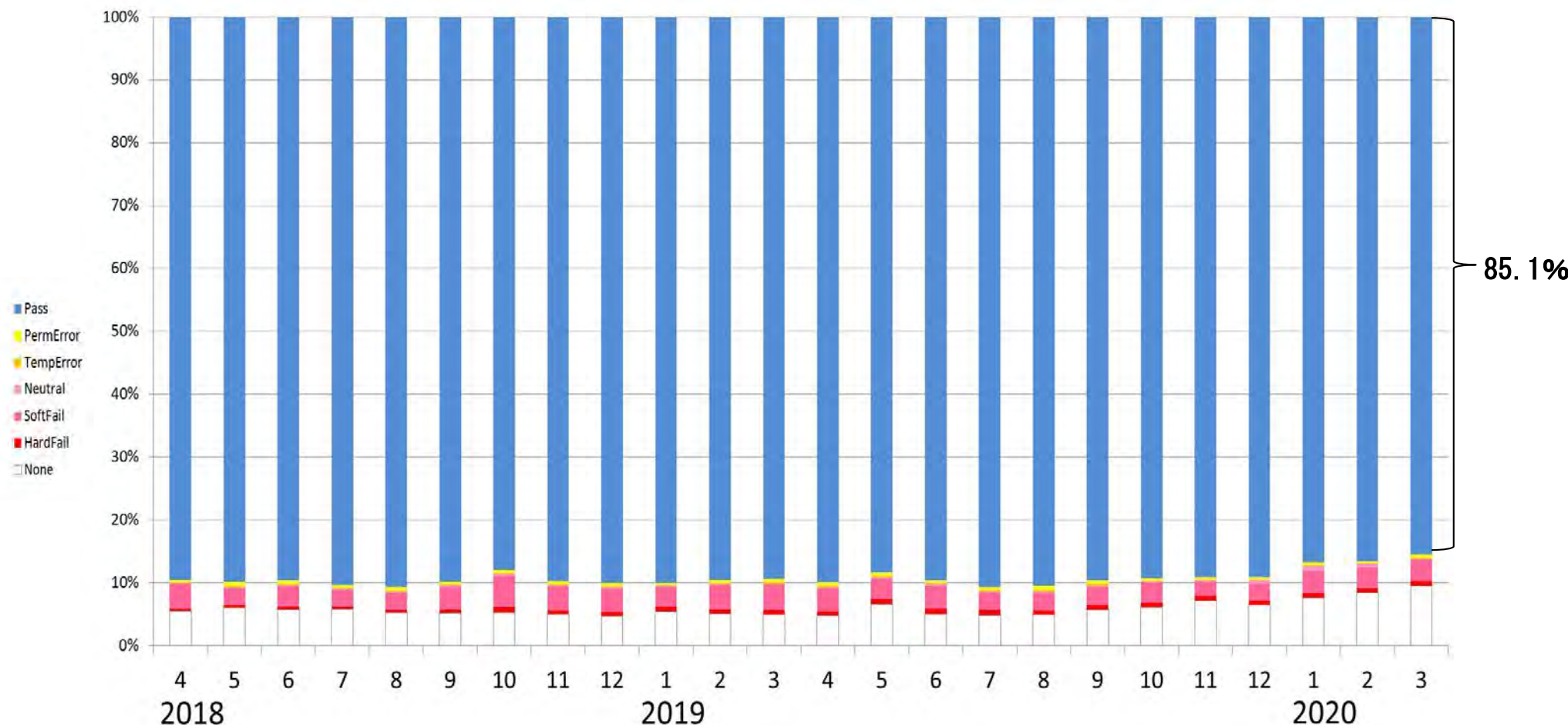
※1 SPF (Sender Policy Framework) : 送信側のメールサーバのIPアドレスをDNSで宣言することにより、ネットワーク的に認証を実施する技術。

※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。

(参考)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

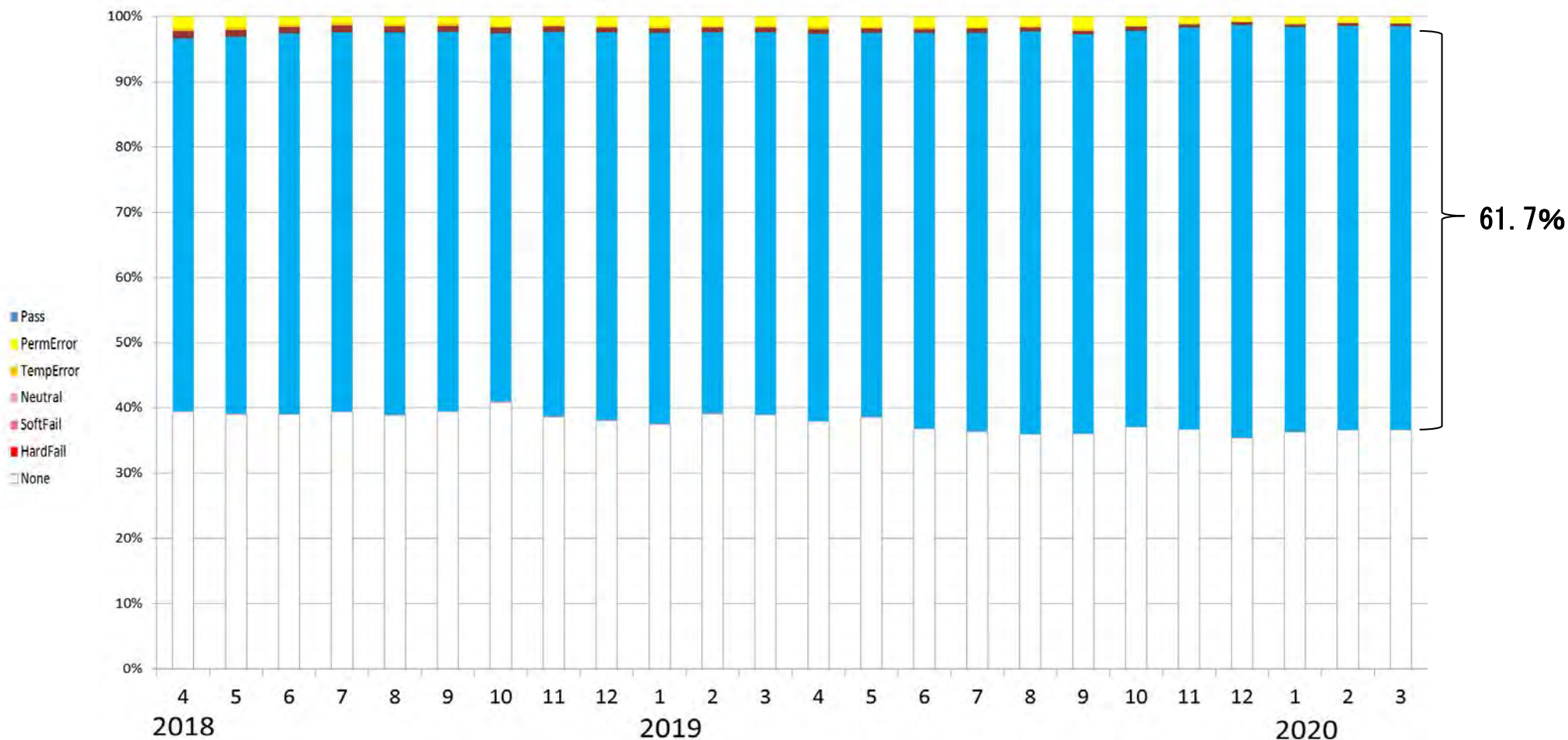


※1 SPF (Sender Policy Framework) : 送信側のメールサーバーのIPアドレスをDNSで宣言することにより、ネットワーク的に認証を実施する技術。メールサーバー間の通信でやりとりされる送信者情報を用いる。

※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。

(参考)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6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。