（資料３）

迷惑メール対策に係る取組みについて

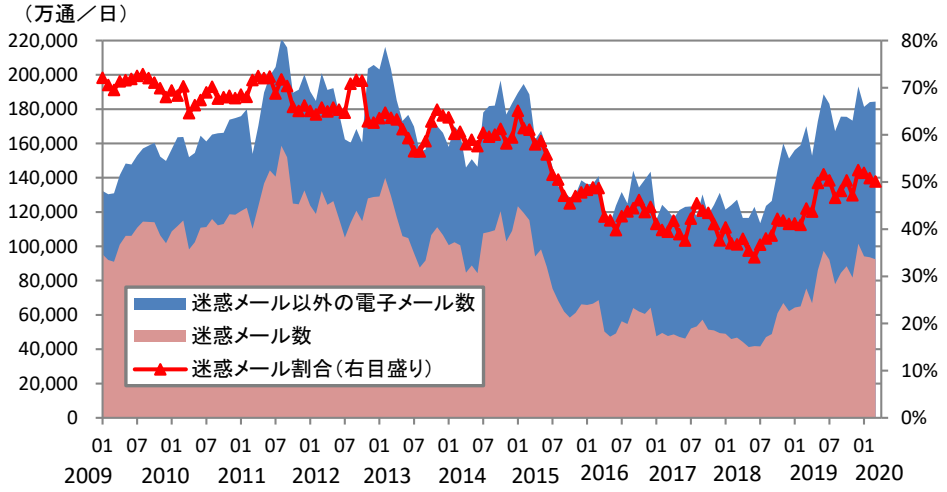
令和2年11月

総　　務　　省

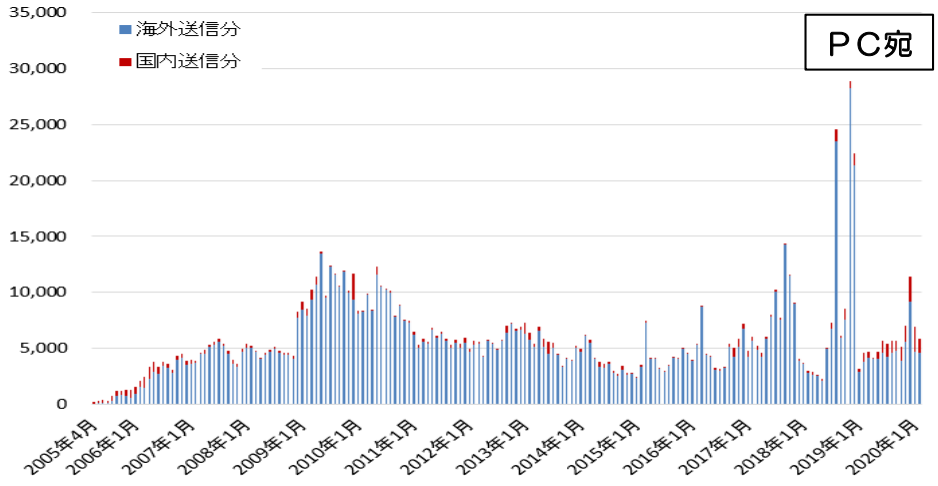
我が国における迷惑メールの現状

○　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。

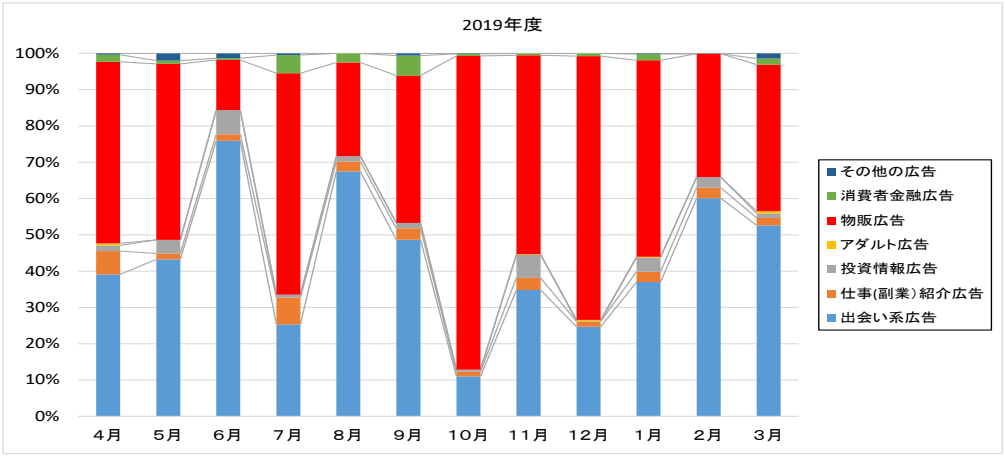
＜国内ISPにおける迷惑メール数・割合の推移（2020年3月時点）＞

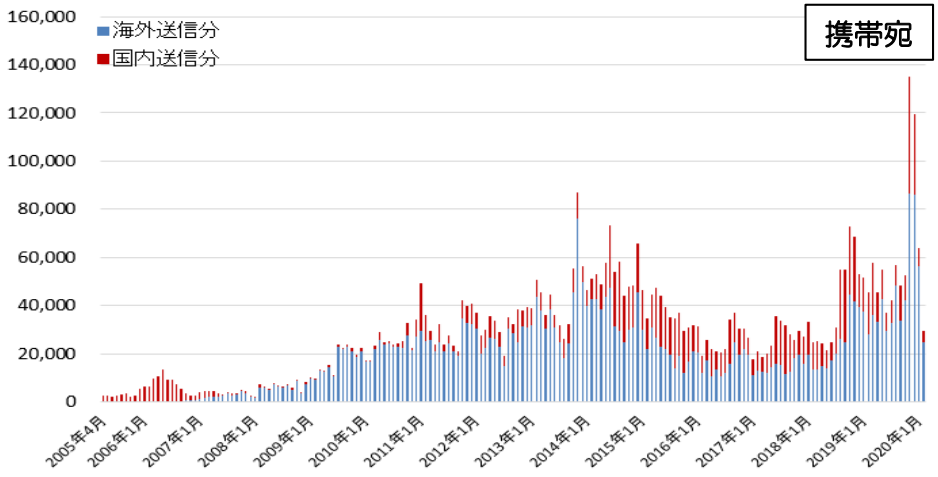


＜我が国着の迷惑メール送信状況の推移（2020年3月時点）＞



＜迷惑メールの広告宣伝内容別の構成比率（2019年度）＞



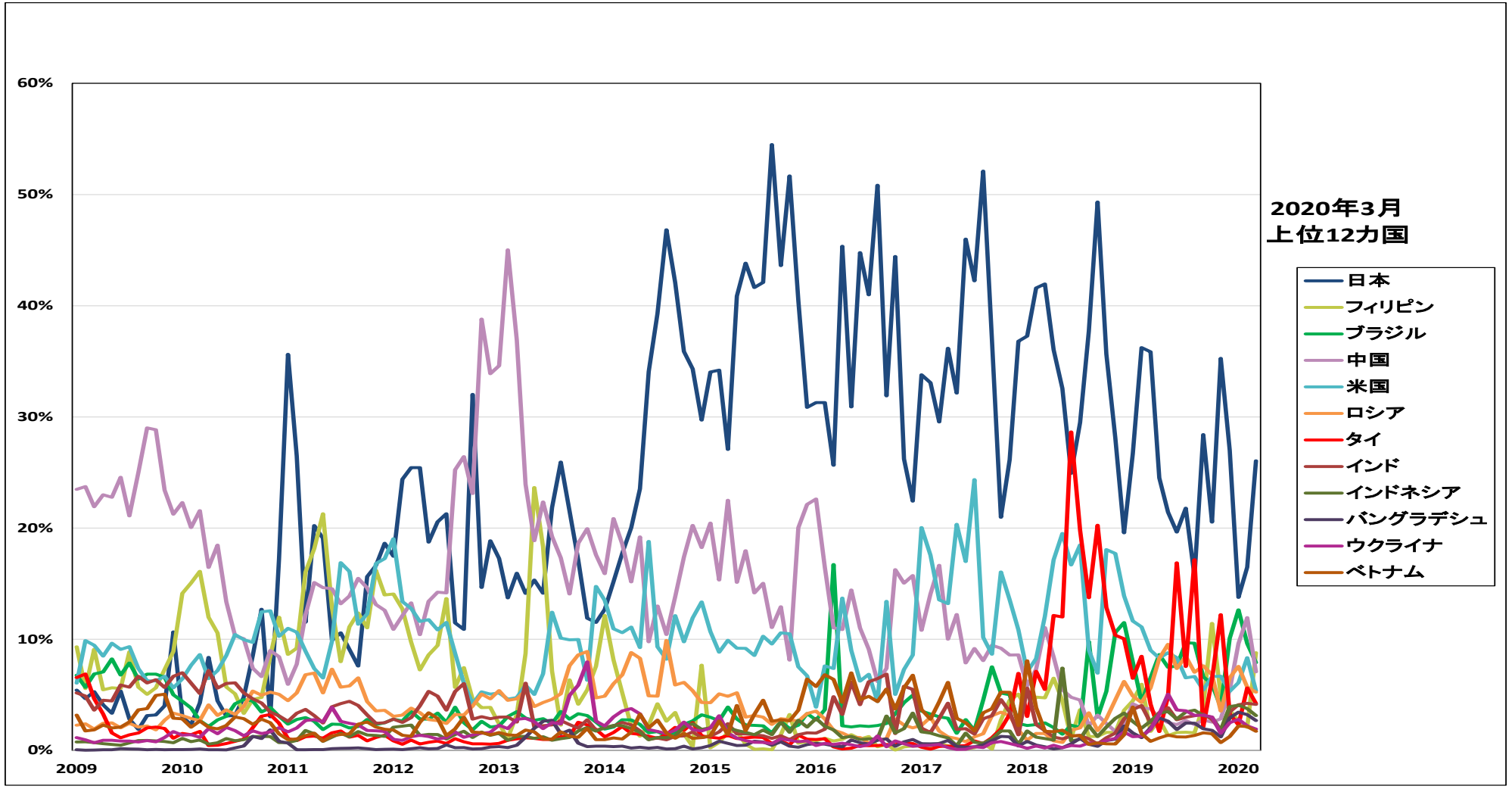


出典：一般財団法人日本データ通信協会迷惑メール相談センター調べ（相談センターのモニター機で受信した情報を分析したもの）

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＞

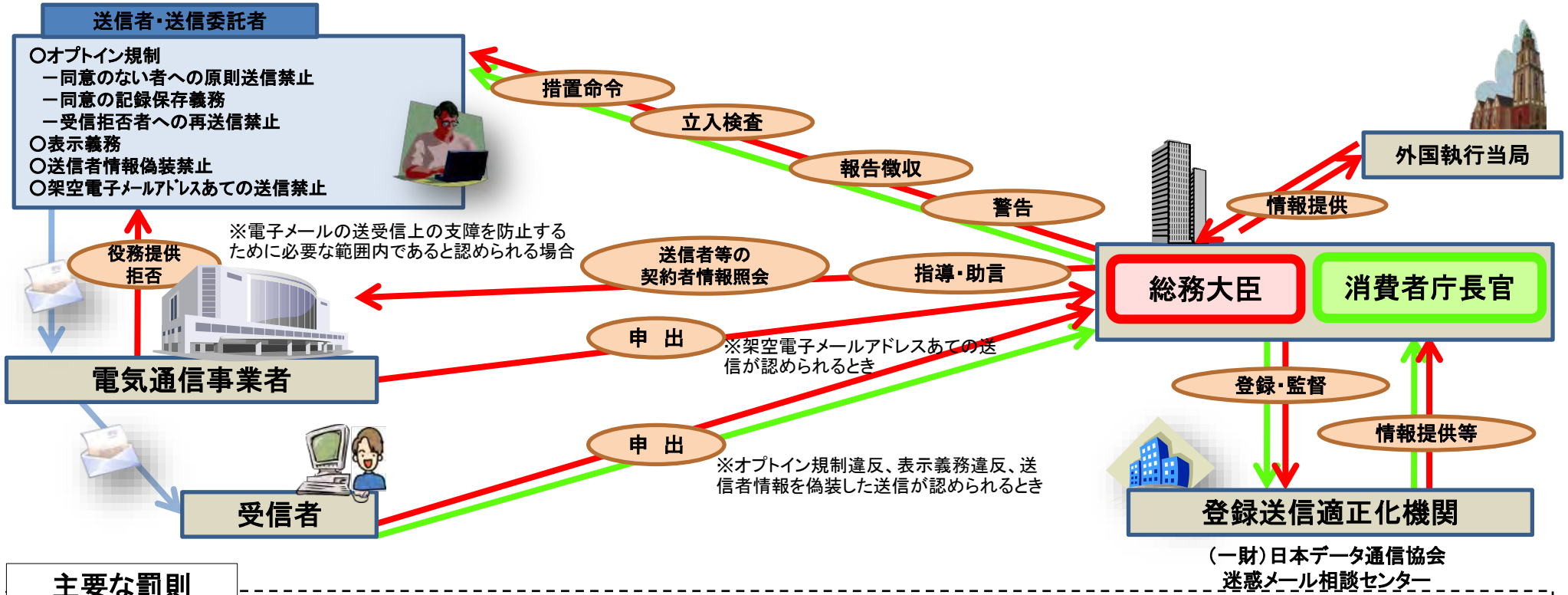


出典：一般財団法人日本データ通信協会迷惑メール相談センター調べ（相談センターのモニター機で受信した情報を分析したもの）

特定電子メールの送信の適正化等に関する法律について

○　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

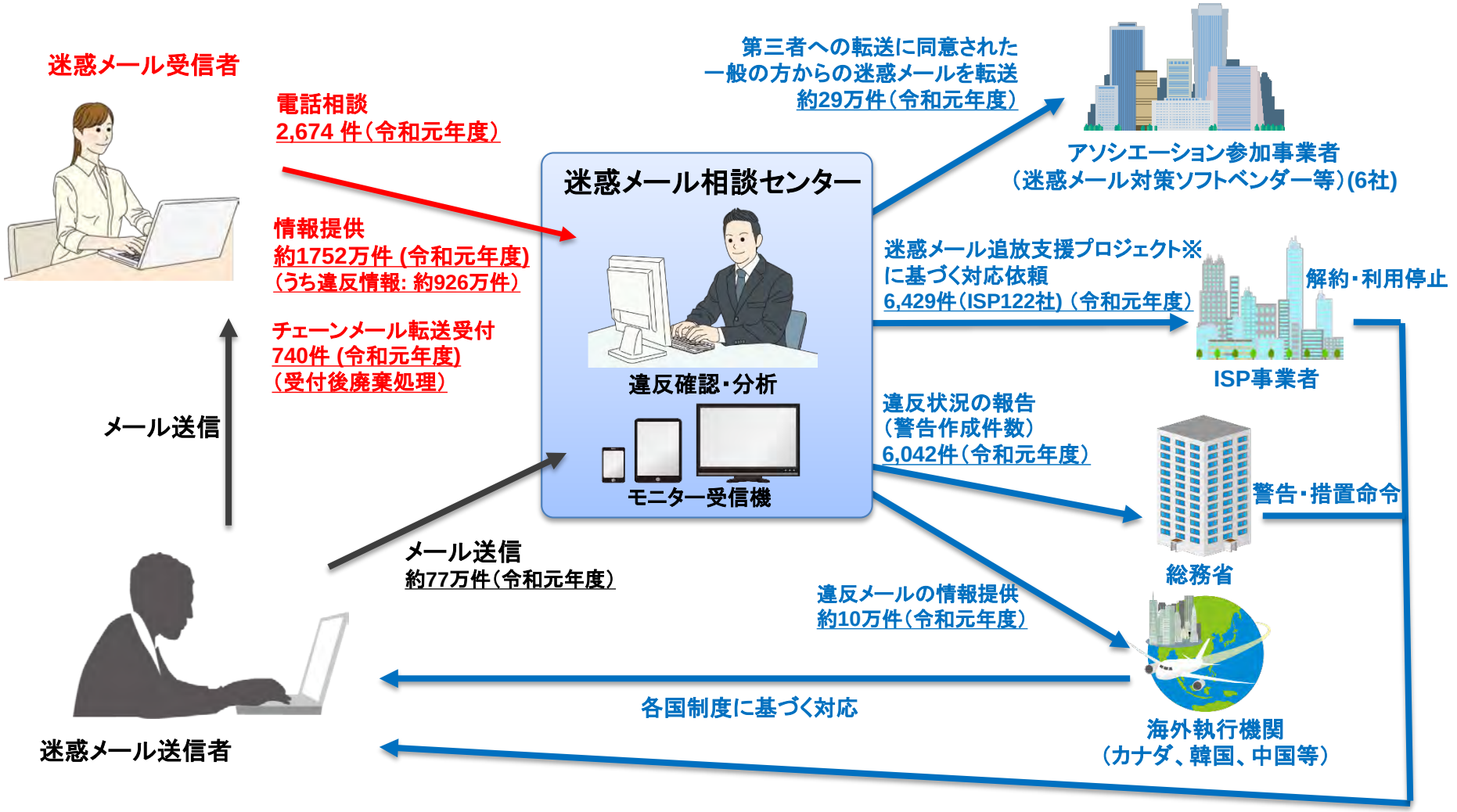


主要な罰則

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）

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

○　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事業者に通知し、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

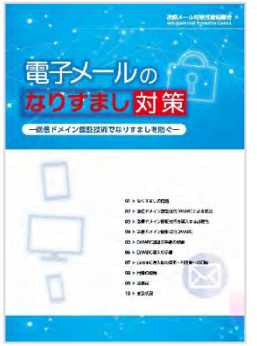
■　主な活動内容

・「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

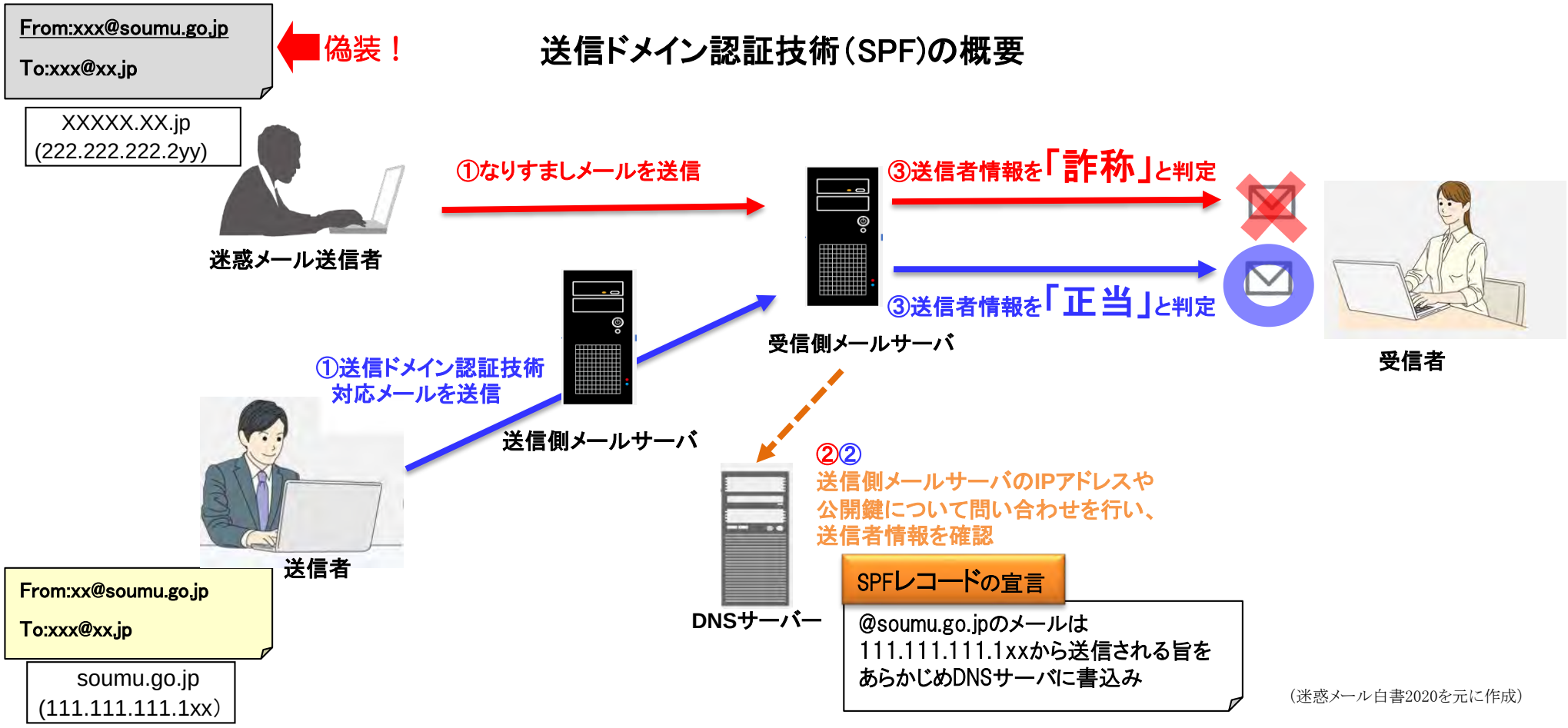
送信ドメイン認証技術導入マニュアル

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。

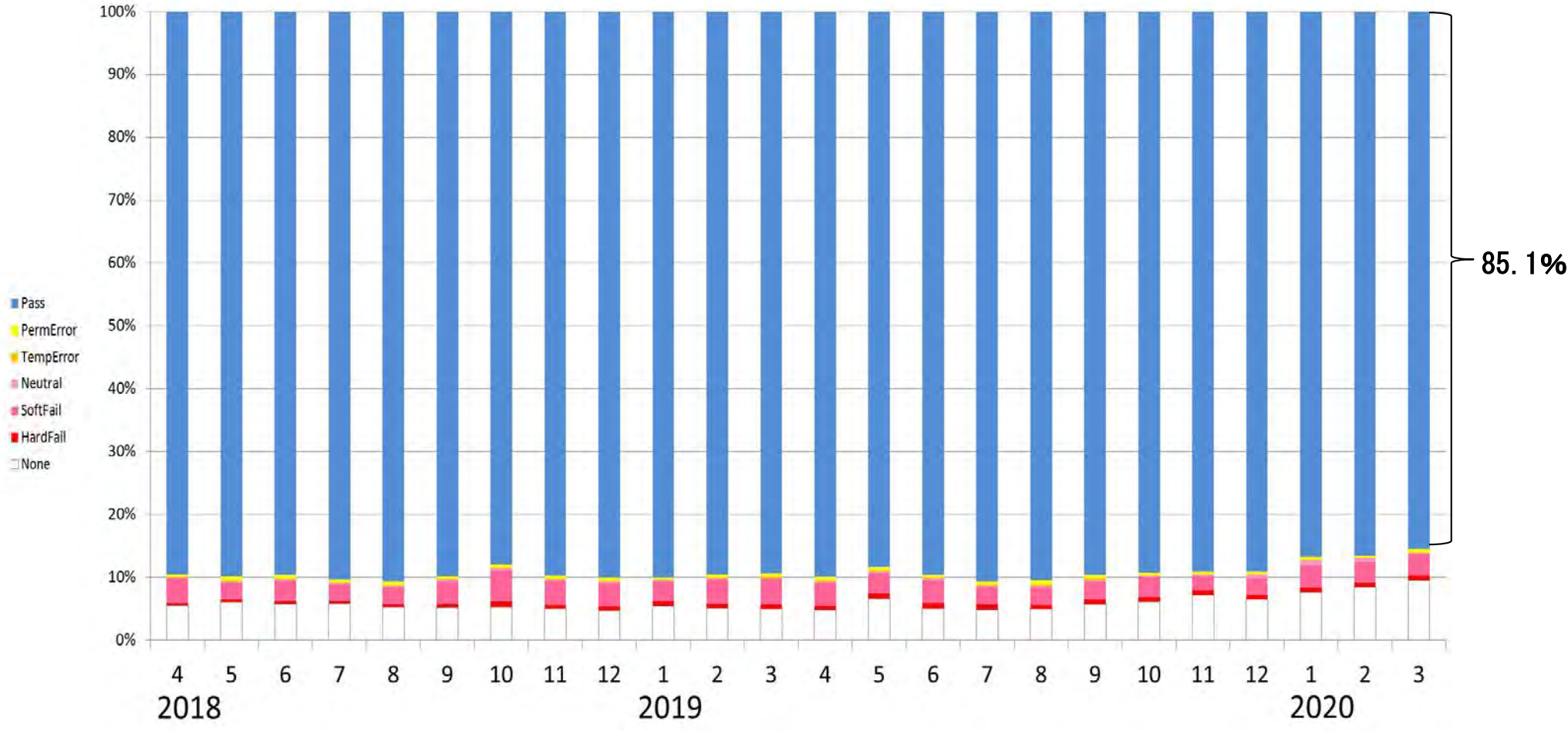


（迷惑メール白書2020を元に作成）

※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。

（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

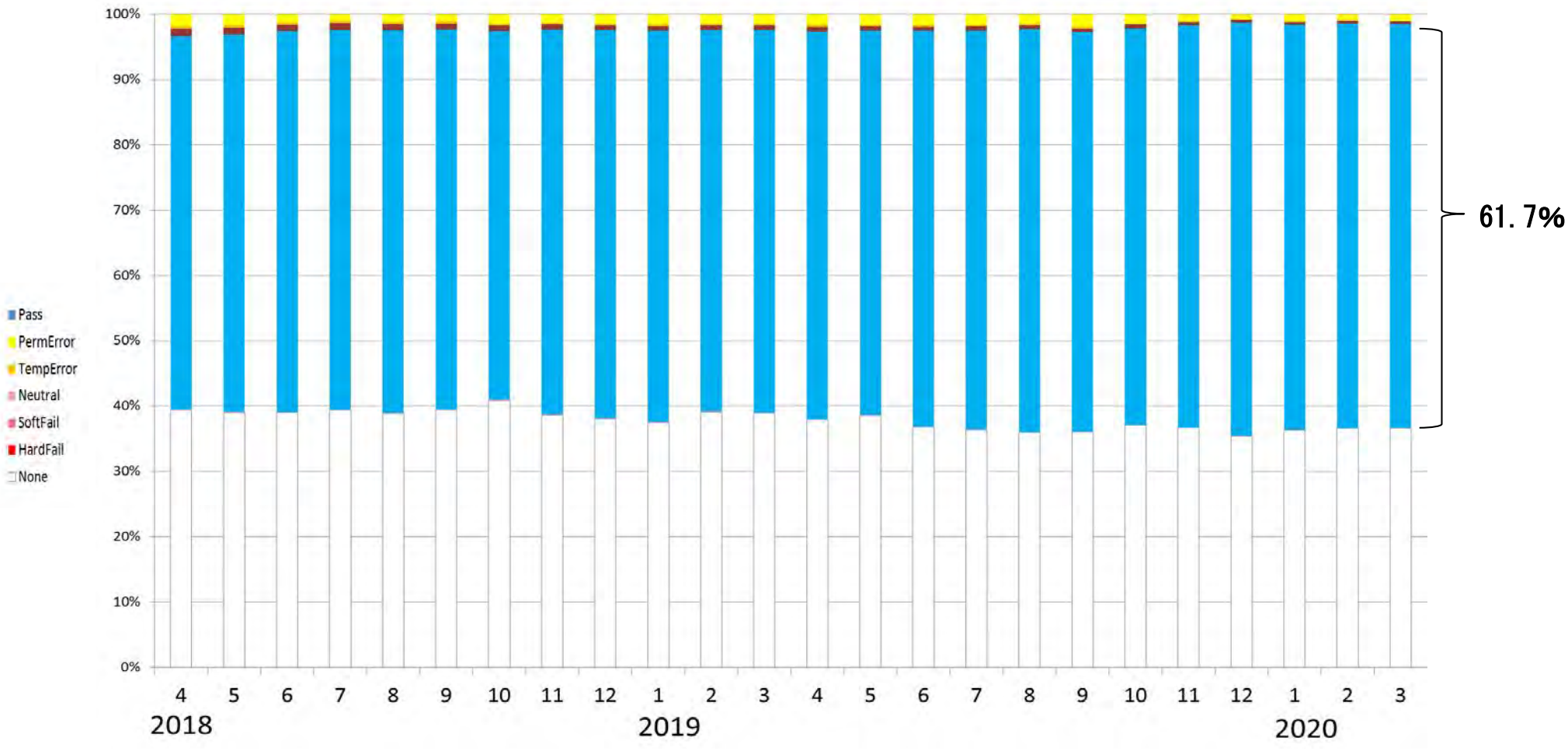


※1　SPF（Sender Policy Framework）：**送信側のメールサーバーのIPアドレス**をDNSで宣言することにより、ネットワーク的に**認証**を実施する技術。メールサーバー間の通信でやりとりされる送信者情報を用いる。

※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。

迷惑メール対策に係る利用者への周知啓発

詐欺メール対策リーフレット
そのメール、詐欺カモ！？
（(一財)日本データ通信協会）

撃退！迷惑メール
（(一財)日本データ通信協会）

迷惑メール対策白書2020
（迷惑メール対策推進協議会）

総務省HP

（一財)日本データ通信協会HP

（参考）撃退！迷惑メール　抜粋①

特集 令和時代の迷惑メール最新トレンド

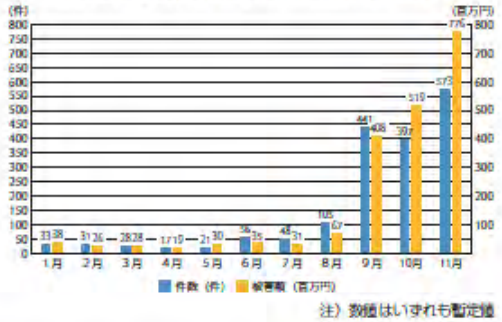
平成から令和への改元があった2019年は、迷惑メールの手口の一層の巧妙化・悪質化が進み、メールやSMSをきっかけとした被害が多く発生した年でもありました。

１年を振り返り、社会的影響や被害金額の大きかった迷惑メール・詐欺メールの事案の中から、最新トレンドをご紹介します。

トレンド1：フィッシングメールによる被害拡大

９月から、フィッシングメールにより、銀行などの金融機関を装った、偽サイトに誘導し、そこでID・パスワードを盗み取り、それを用いて金銭をだましとったと思われる不正送金被害が急増しました。９月は前月比４倍の441件とになり、10月、11月も高水準で推移しています。11月は平成24年以降最多の水準となりました。 被害の多くは、メールやSMSにより金融機関を装った偽サイトへと誘導されたことが推定されています。

不正送金事犯発生状況（令和元年11月末現在）



注）数値はいずれも暫定値

出展：フィッシングによるものとみられるインターネットバンキングに係る不正送金被害の急増について（全銀協等と連携した注意喚起） 警察庁
https://www.npa.go.jp/cyber/policy/caution1910.html

トレンド2：携帯電話会社をかたるSMS

従来より、有名企業からの宅配通知などを装ったSMSが送信されていましたが、2019年は、携帯電話会社を装ったSMSが出回りました。

国民生活センターでは、９月に携帯電話会社をかたるSMSに関する注意喚起を行いました。

その内容としては、「携帯電話会社名で、利用者に向けて『不正ログインされた可能性があるので、IDとパスワードを変更してください』等のSMSが届き、携帯電話会社のID、パスワード、暗証番号等を入力したら、その後、携帯電話会社から身に覚えのない決済メールが届いた」など、携帯電話会社をかたる偽SMSをきっかけにキャリア決済※が不正利用されたという相談が寄せられたというもので、相談事例や手口を紹介し、注意を呼びかけたものです。

国民生活センターでは、キャリア決済の限度額の見直しや２段階認証の設定などとともに、不安に思ったときは相談するようアドバイスしています。

※キャリア決済：携帯電話会社のIDやパスワード等による認証で商品等を購入した代金を、携帯電話の利用料金等と合算して払うことができる決済方法。

出典：2019年９月５日　独立行政法人国民生活センター
「携帯電話会社をかたる偽SMSにご注意！―あなたのキャリア決済が狙われています―」
http://www.kokusen.go.jp/pdf/n-20190905_1.pdf

（参考）撃退！迷惑メール　抜粋②

1章 迷惑メール・詐欺メール 撃退講座
個人情報や金銭をだまし取る詐欺メールが増えています

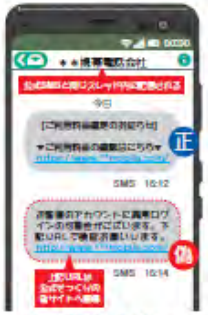
1 偽のSMSで被害急増

スマートフォンの普及により、様々なシーンでSMSが利用されるようになりました。SMSは電話番号を利用してメッセージをやりとりするサービスで、最近は、本人確認の２段階認証や企業・自治体からの情報配信として利用されることも増えてきました。一般的にSMSは受信者がメッセージに気づきやすく、開封率が高いといわれていますが、便利になった反面、こうしたSMSの特徴を悪用した詐欺が最近急増しているので注意が必要です。

●大手企業・ブランドになりすます

なりすましSMSによる事例は、2018年頃から急増しておりますが、よくある手口としては、宅配会社、携帯電話会社、通販会社などの有名企業になりすましてSMSを送るものです。このSMSにより、有名企業を装った偽サイトへ誘導した上で、ID・パスワードなどの個人情報を盗み取り、最終的に金銭をだまし取るものです。その一般的な手口は、以下の流れとなっています。

●携帯電話会社からのお知らせに紛れ込む！



なりすましSMSの中でも特に問題となっているのは、企業からの正式なSMSが届くスレッドの中になりすまされたSMSが紛れて届く事例です。

スマートフォンのSMSは、通常LINEと同じように、宛先／送信者ごとにスレッドとして表示されます。左の例では送信者が携帯電話会社の公式SMSと同一に偽装されていたため、携帯電話会社公式SMSと偽SMSが同じスレッドに表示されています。

いつもの携帯電話会社からのSMSだと思ったら実は偽のSMSで、気づかないまま詐欺サイトへアクセスしていたのです。結果、アクセスした偽サイトで携帯電話会社のID・パスワードやクレジットカード情報を盗み取られ、不正利用されてしまった被害が報告されています。

●SMSでもセキュリティ対策を！

スマートフォンの中にはアプリのログイン情報、ショッピングサイトやオンラインバンキングのアカウント情報など、重要な情報が大量に保存されています。そして、こうした情報は悪意のある攻撃者にとっての格好のターゲットとなっています。

最近、情報をだましとることを目的とした内容の詐欺メールがSMSでも送られ、被害が多数報告されるようになっています。

これから紹介する、宅配便の不在通知を装って不正なアプリをダウンロードさせて個人情報をだましとる事例やSMSのリンクから偽サイトへ誘導し、ID・パスワードなどのアカウント情報を入力させてだましとる事例など、多くの事例がみられます。

スマートフォンにもパソコンの対策と同様のセキュリティ対策が必要です。大切な個人情報をだましとられないように、不審なSMSにも十分注意するようにしましょう。

（参考）撃退！迷惑メール　抜粋③

2 大手宅配会社の不在通知を装うたSMS

宅配便業者になりすました詐欺のSMSによる被害が継続して報告されています。

この手口は、荷物の不在通知や発送完了などのお知らせを装い、SMSに記載されたURLをクリックさせ、宅配便業者になりすました偽のサイトへ誘導し、そのサイトからAndroid向けの不審なアプリをインストールさせようとするものです。

（独）情報処理推進機構（IPA）のレポート※によると、アプリをインストールしてしまった場合、その端末から詐欺のSMSが多数へ送信されたり、"1日あたりのSMS送信上限数に達した"というメッセージが表示されたりするなどの被害が報告されています。

また、被害にあったスマートフォンのアカウントが不正利用され、身に覚えのない携帯電話事業者の提供するキャリア決済の請求が発生したり、Google Playアカウント、端末に紐づくSNS等のサービスのアカウントへの不正ログインも報告されています。

最近では、iPhoneなどのiOS端末では「Apple ID」と「パスワード」をだましとる偽サイトへ誘導されることも確認されています。

※2018年8月8日掲載「安心相談窓口だより」（宅配便業者をかたる偽ショートメッセージに関する相談が急増中～　誘導されるままAndroid端末にアプリをインストールしないように！　～）

メールの特徴

- SMSで届く
- 荷物の不在通知や発送完了メールなどを装う
- 佐川急便を装ったアプリのインストールを要求する（Android端末）
- 「Apple ID」と「パスワード」の入力を要求する（iOS端末）

対処法

- ✓身に覚えのない不在通知やお知らせのSMSは無視をしましょう。
- ✓本文内のURLは絶対にタップ（クリック）しないようにしましょう。サイトを表示してしまったときは、ブラウザを閉じて、アカウント情報などの入力はしないようにしましょう。
- ✓公式サイト以外からアプリをインストールするのはやめましょう。Android端末は「Google Play」、iOS端末は「App Store」からのみ、アプリをダウンロードするようにしましょう。
- ✓間違って不審なアプリをインストールしないように、Android端末は「提供元不明のアプリ」のインストールを許可（ON）しないように設定しましょう。（詳しくは51ページ）

相談窓口：

消費者庁
消費者ホットライン
188キャラクター
イヤヤン

■ **消費者ホットライン**
電話番号：（局番なし）188（通話料有料）
※接続先により受付時間が異なります。
※一部のIP電話などからはつながりません。

■ **情報セキュリティ安心相談窓口**
［IPA（独立行政法人 情報処理推進機構）］
電話番号：03-5978-7509
受付時間：平日10：00～12：00、
13：30～17：00（年末年始・祝祭日は除く）

■ **各携帯電話事業者**（詳しくは64ページ）

（参考）撃退！迷惑メール　抜粋④

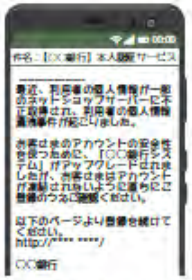
3

銀行になりすました詐欺（フィッシング）メール

あなたの預金が狙われています

金融機関になりすまし、ネットバンキング利用者へのお知らせメールを装ったフィッシング詐欺の事例もあります。

「安全性向上のためにパスワードを変更してください」などと緊急性を強調して、本物そっくりの偽サイトへ誘導し、利用者のアカウント情報(店番号・口座番号、契約者番号、乱数表、暗証番号など)を入力させてだましとろうとする手口です。



フィッシング詐欺にだまされてしまうと、犯罪者がこの方法でだましとったアカウント情報を使って正規のサイトにログインし、利用者の銀行口座から不正送金してしまうなどの被害が報告されています。

メールの特徴

・「口座が不正に利用される懸念がある」「漏洩した名簿にあなたが含まれている」「インターネットバンキングのセキュリティ強化に必要」などと緊急を装う内容

対処法

✓金融機関がメールで個人情報を求めることはありません。個人情報を入力させるようなメールが着信しても、メールに記載されたURLをクリックしたり、メールの問い合わせ先へ連絡したりするのはやめましょう。

✓偽サイトは本物そっくりに作成しているため、本物と見分けるのは困難です。金融機関のサイトを確認する必要がある場合には、普段使用しているブックマークからアクセスするか、公式サイトで確認した金融機関のヘルプデスクへ連絡するようにしましょう。

✓フィッシング詐欺の被害にあった時は、速やかにご利用の金融機関窓口に連絡してください。また、金銭被害にあった場合には、最寄りの警察署へ相談してください。

✓偽サイト対策には、「100%安心」といった対策を示すことは困難ですが、セキュリティ対策ソフトを最新の状態にアップデートして、「提供元不明のアプリ」のインストールを許可しないといった設定も有効です。

相談窓口

■ 警察相談ダイヤル

電話番号：#9110（通話料有料）
受付時間：平日8：30～17：15（各都道府県警察本部で異なります）
（土日・祝日及び時間外は、一部の県警を除き、当直または音声案内での対応となります）

もっと知りたい

フィッシング対策協議会ではフィッシングに関する緊急情報やフィッシング事例の紹介を行っています。

■ フィッシング対策協議会
https://www.antiphishing.jp/