

# 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

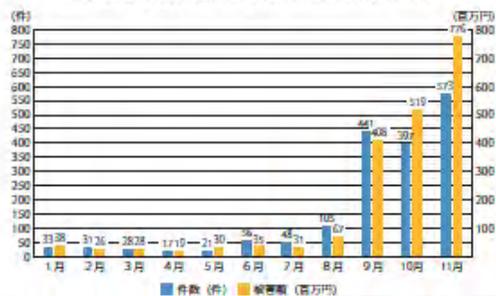
平成から令和への改元があった2019年は、迷惑メールの手口の一層の巧妙化・悪質化が進み、メールやSMSをきっかけとした被害が多く発生した年でもありました。

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）



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

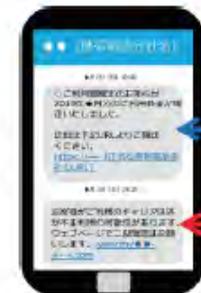
従来より、有名企業からの宅配通知などを装ったSMSが送信されていましたが、2019年は、携帯電話会社を装ったSMSが回りました。

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<sup>※</sup>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。



携帯電話会社が送る正式なSMS

携帯電話会社が送る偽SMS

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](http://www.kokusen.go.jp/pdf/n-20190905_1.pdf)

# (参考)撃退！迷惑メール 抜粋②

★1冊 迷惑メール・詐欺メール 徹底解剖  
個人情報や金銭をだましとる詐欺メールが急増している

## 1 偽のSMSで被害急増

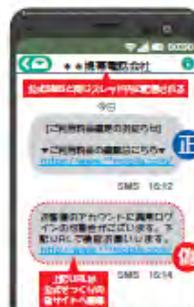
スマートフォンの普及により、様々なシーンでSMSが利用されるようになりました。SMSは電話番号を利用してメッセージをやりとりするサービスで、最近では、本人確認の2段階認証や企業・自治体からの情報配信として利用されることも増えてきました。一般的にSMSは受信者がメッセージに気づきやすく、開封率が高いといわれていますが、便利になった反面、こうしたSMSの特徴を悪用した詐欺が最近急増しているため注意が必要です。

### ●大手企業・ブランドになります

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きました。

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った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。
- ✓間違っても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)



消費者庁  
 消費者ホットライン  
 188キャラクター  
 イヤマン

# (参考)撃退！迷惑メール 抜粋④

★1冊 迷惑メール・詐欺メール 徹底解説

3

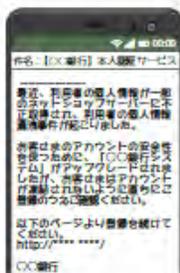
## 銀行になりすました詐欺 (フィッシング) メール

### ●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)を入力させてた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へ連絡してください。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/>

