

ここで紹介するニュースは、ほとんどの場合、日頃からOS・アプリケーション・アンチウイルスのデータベース等を常に最新の状態に保つこと、併せて、UTM導入等によるネットワーク全体の防御を行うことで対策できます。

## ●佐川急便をかたるSMS急増…不正なAndroidアプリインストールの可能性

<http://nlab.itmedia.co.jp/nl/articles/1807/27/news084.html>  
<http://www2.sagawa-exp.co.jp/whatsnew/detail/721/>



### このニュースをザックリ言うと…

- 7月19日（日本時間）に佐川急便より、同26日には内閣サイバーセキュリティセンター（NISC）より、**佐川をかたる偽のショートメール（SMS）が大量送信されている**として注意喚起が出されています。

- 佐川急便の注意喚起ページによると当該SMSは、「お客様宛にお荷物のお届けにあがりましたが不在の為持ち帰りました。配送物は下記よりご確認ください」と書かれた後に偽のWebサイトへのリンクが貼られており、アクセスすると不正な.apk拡張子のファイル（Androidアプリのインストーラー）をダウンロードさせるものとなっています。

- アプリをインストールしたユーザからは、**外部に不正なスパムを送信したり、勝手にプリペイドカードを購入させられる**等の被害が報告されています。

### AUS便りからの所感等

- 偽サイトは、不審なアプリをインストールさせようとするリンクの箇所を除いて、本物の佐川急便のページと寸分たがわぬ外見となっている模様です。

- 佐川急便では「SMSで利用者に連絡することはない」として、これまで確認された同社をかたるメールの情報をまとめており、6月にも同様のSMSの他、**差出人が「佐川<<急>>」、件名が「お問い合わせ詳細について」、本文は不審なリンクのみというメールの存在も確認されています。**

- 根本的な回避策として、不正なAndroidアプリをうっかりインストールしてしまうことのないよう、「**提供元不明のアプリ**」のインストールは許可しない設定とすることが肝要であり、併せて、上記の佐川急便からの情報やTwitter等SNSでの報告を随時確認するとともに、本物のページへはブラウザにブックマークを登録してアクセスする等の自衛策をとるようにしましょう。



2018年07月27日 12時50分 公開

### 佐川急便を名乗るスパムが急増、SMSから偽サイトに誘導 自動でプリペイドカードを買われるなどの被害も 注意しましょう。

[ねとらぼ]



以前から被害が報告されていた、佐川急便の名を語ったスパムメールが急増しています（[関連記事](#)）。佐川急便の公式サイトでは7月19日より、「佐川急便を装った迷惑メールが届くというお問い合わせが急増しております」として**再度注意喚起**。26日には内閣サイバーセキュリティセンターからも**注意が呼びかけ**られています。

お客様宛にお荷物のお届けにあがりましたが不在の為持ち帰りました。  
配送物は下記よりご確認ください。  
<https://www.sagawa-exp.co.jp/>

うっかりアクセスしてしまう文面に注意（佐川急便 - 佐川急便を装った迷惑メールにご注意ください）



### 佐川急便を装った迷惑メールにご注意ください

2018.07.27

佐川急便を装った迷惑メールが届くというお問い合わせが急増しております。  
このような迷惑メールに記載されているアドレスにアクセスしたり、添付ファイルを開いたりされるとコンピューターウイルスに感染する恐れがございますのでご注意ください。なお、当社ではショートメールによるご案内は行っておりません。

迷惑メールであるか分からないなど、不明な点がございましたら佐川急便Webサイト内「ご意見・お問い合わせ」までお問い合わせください。

- 事例1 送信者：01085264506814 ※ショートメールで届きます **NEW**
- 事例2 差出人：佐川<<急>> **NEW**
- 事例3 通知 ※ショートメールで届きます
- 事例4 差出人：佐川急便<information@XXXXXXXXXXXX.jp>
- 事例5 件名：[佐川急便] 請求内容確定のご案内
- 事例6 件名：出荷完了メール
- 事例7 件名：出荷サービス受け付けました。
- 事例8 件名：商品本日発送
- 事例9 件名：佐川、メール、配・送センター
- 事例10 件名：[TRY×3] 【発送連絡】（送信専用）
- 事例11 件名：Fwd：商品発送のお知らせ、Fwd：佐川急便
- 事例12 件名：宅配便お届けのお知らせ。
- 事例13 差出人：佐川飛脚、メール便<mail@1ea2c.mnztzm9e35x8.XXX>
- 事例14 件名：佐川です。
- 事例15 件名：佐川より不審通知【\*\*\*\*\*@\*\*\*\*\*様

## ●3分の2がルータのID・パスワードを未変更、4割が管理画面の存在を知らず…Avast調査

<https://internet.watch.impress.co.jp/docs/news/1133918.html>



### このニュースをザックリ言うと…

- 7月20日（日本時間）、アンチウイルスベンダーのAvast社より、日本国内の1032人を対象に7月に実施した「ルータのセキュリティに関する調査結果」が発表されました。
- 調査結果では、「**ルータの管理ページにログインし、工場出荷時のログイン情報を変更したことが一度もない**」との回答が**37%にのぼり**、次いで「管理ページにログインしたことがあるものの、ログイン情報を変更せず使用し続けていた」が31%、一方で「アカウント情報を変更したことがある」は32%に留まっています。
- また、**ウェブ管理ページにログインしたことのある人の43%が「ルータのファームウェアをアップデートしたことがない」と回答した**とのこと。

### AUS便りからの所感等

- 発表では、ログイン情報が工場出荷時から変更されていないルータにマルウェアが侵入した例として、5月下旬に警告が出されたVPNFilter（「AUS便り 2018/05/28号」参照）やSatoriが挙げられており、いずれも大規模なボットネットを構築するものとなっています。
- **インターネット上から接続可能な複合機・IoT機器等を検索できる「SHODAN」では、同様に外部から管理画面にアクセス可能なルータも対象となっており、もしもそういう設定になっていてかつログイン情報を変更していなければ、たちどころに侵入されること**でしょう。
- 社内や自宅のネットワークで使用する機器については全て存在を把握、ログイン情報を必ず変更するようにした上で、ファームウェア等のアップデートがないか定期的に確認する管理体制を整えることが重要です。

INTERNET Watch

3分の2がルータのID/パスワードを未変更、4割が管理画面の存在を知らず～Avast調査  
認証情報の変更、ファームウェア更新が必要最低限のセキュリティ対策

岩崎 幸守 2018年7月20日 13:07

ツイート リスト いいね 173 シェア 81 Pocket 81

Avastは、日本国内の1032人を対象に7月に実施したルータのセキュリティに関する調査結果を発表。ルータのIDやパスワードをデフォルト設定から変更したことがあるのは32%だけだったという。

ルータの管理画面にログインしたことはあってもID・パスワードを変更したことがない人は31%、そもそもルータの管理画面にログインしたことがない人が37%だった。

## ●突然「Googleメンバーシップ・リワード」のページが表示…フィッシングへ誘導する不正な広告に注意

<https://did2memo.net/2018/04/07/malicious-web-page-rewards-for-google-users-page-2018-04-07/>



### このニュースをザックリ言うと…

- 7月21日（日本時間）以降、**Webサイト閲覧中に突然「Googleメンバーシップ・リワード」の画面が表示される**という報告が相次いでいます。
- **表示される画面はGoogleのキャンペーンをかたるフィッシングで、iPhone X・iPad Air 2およびSamsung Galaxy S6が当たると偽って個人情報やクレジットカードを入力させようとする模様**です。

### AUS便りからの所感等

- 4月にも、Googleや日本郵便をかたり、iPhone等をプレゼントすると称した同様のフィッシングが発生しています（「AUS便り 2018/04/09号」参照）。
- 「Googleメンバーシップ・リワード」というフィッシングサイトの存在もこの時から同様に確認されており、**一時の鎮静化を経て再度活発化したもの**とされています。
- 7月27日現在、Google ChromeやFirefoxによるフィッシングサイトへのアクセスはアンチフィッシング機能により遮断される模様であり、フィッシングを回避するために、こういったブラウザやアンチウイルス、そしてUTMのセキュリティ機能は必ず有効にすることを推奨致します。

### 情報科学屋さんを目指す人のメモ

セキュリティ > 偽サイト > 当選詐欺 >

「Googleメンバーシップ・リワード」のGoogleギフト当選詐欺に注意 (2018年7月21日急増中) 156,640 views

Google (79) セキュリティ (80)

本日、「Googleメンバーシップ・リワード」という画面が突然表示され、「iPhone X」（Googleギフト）が当選したというユーザーが急増しています。

しかし、この「Googleメンバーシップ・リワード」という、Googleの利用に対する感謝の気持ちで行われているようなプレゼントキャンペーンですが、Google社が行っているキャンペーンではありません。つまり、Google社になりました隣の当選ページです。

個人情報やクレジットカードの番号を入力してしまわないように注意してください。