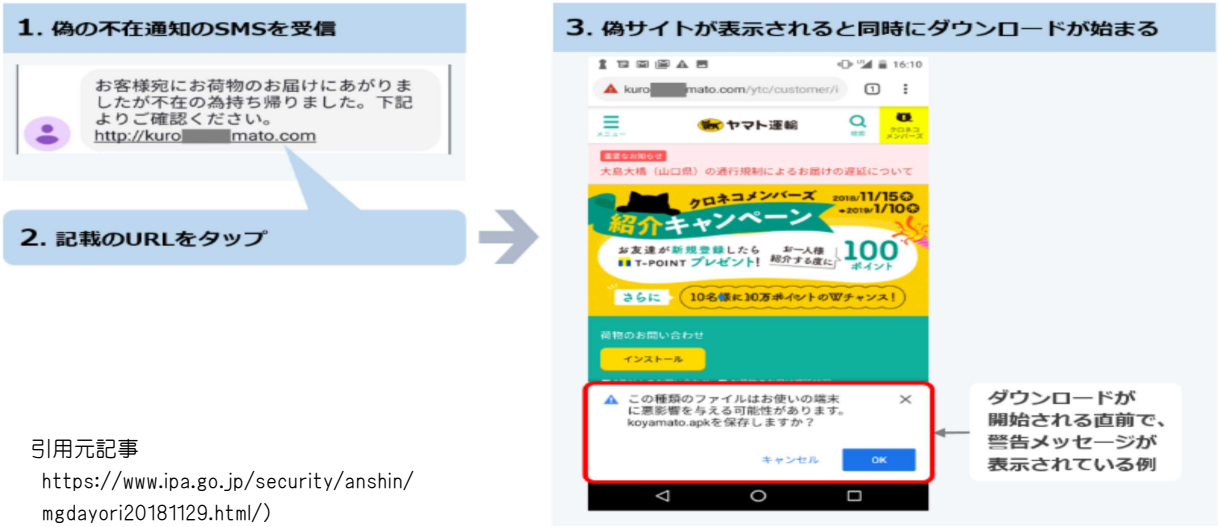
| 号　外 | サイバーセキュリティニュース | 平成30年12月26日<br>函館方面サイバーセキュリティ連絡会議事務局 |
|---|---|---|

# 宅急便業者「ヤマト運輸」の偽サイトに注意！

ヤマト運輸を騙る偽SMSが届き、Android端末で偽SMSに記載されたURLをタップすると、ヤマト運輸偽サイトに接続されると同時に**悪質なアプリを自動でインストール**される手口が報告されています。
道警察ではヤマト運輸を騙る偽サイトに関する相談は2件のみですが、今後増加する可能性は極めて高く、注意が必要です。

## 1. 偽SMSの文面やアプリインストールまでの流れ




引用元記事
https://www.ipa.go.jp/security/anshin/mgdayori20181129.html/)

## 2. 佐川急便偽サイトと何が違うのか？

独立行政法人情報処理推進機構（IPA）によると、今回、新たに把握されたヤマト運輸偽サイトはAndroid端末で偽サイトにアクセスすると、自動で悪質なアプリをインストールされる事が確認されています。
ただし、IPAではアプリインストール後の動作を確認出来ておらず、IPAに寄せられた相談において**「ヤマト運輸の不在通知を騙るSMSを、自身の端末から見知らぬ電話番号宛に多数送信される」**事例があったことから、佐川急便偽サイトのAndroid端末の場合と同様の被害が想定されます。

| 佐川 | ヤマト |
|---|---|
| SMS受信 | |
| 有り　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。下記よりご確認ください。http://sagawa-aaki.com | 有り　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。下記よりご確認ください。http://kuro[redacted]mato.com |
| 偽サイトへの誘導方法 | |
| URLタップ | URLタップ |
| アプリインストール方法 | |
| 手動 | 自動 |
| インストール後の動作 | |
| ・SMS送信<br>・iTunesカードキャリア決裁 | 現時点、特定されておらず |

## 3. 被害防止対策

被害防止対策は佐川急便偽サイトと同様に、
- メール本文内のURLリンクはタップしない
- 不審なメールか否か分からない場合は、送信元に送信事実を確認する

などです。
特に、ヤマト運輸を騙る偽サイトに関しては、偽SMS本文のURLをタップし、偽サイトに接続されると自動でアプリをインストールされることが確認されているため、

**SMS本文内のURLリンクは絶対にタップしない**

ことを徹底して下さい。

※　本協議会では、引き続き『サイバーセキュリティ出前研修』の予約を受付中です。各種教養や会合の機会に是非ご利用下さい。【連絡先】事務局（函館方面本部生活安全課）杉本、野崎　0138-31-0110（内線　3262、3265）