# サイバーセキュリティの置き薬

2021年 第10号

## 通信事業者を装ったフィッシングに注意してください。

日本サイバー犯罪対策センター（ＪＣ３）から、通信事業者を装ったフィッシングについて注意喚起が促されています。被害に遭わないように、ご注意ください。

### フィッシングの手口


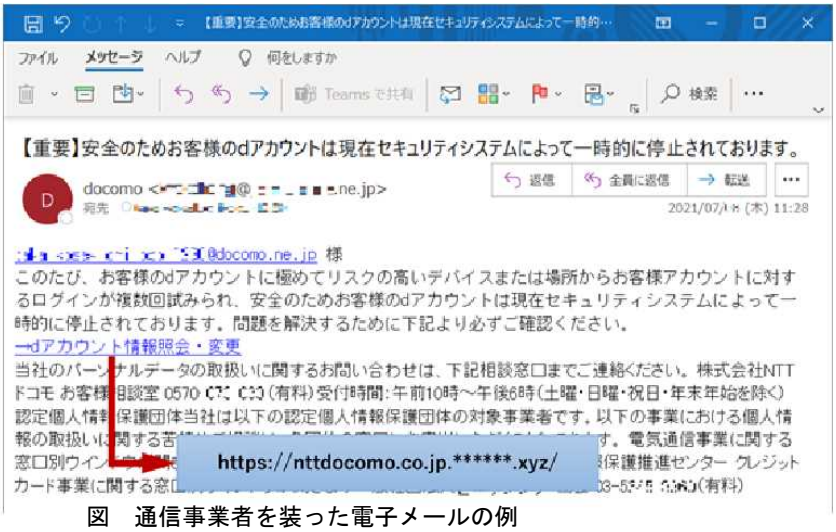


図　通信事業者を装った電子メールの例

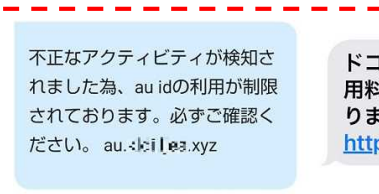


図　通信事業者を装ったＳＭＳの例

フィッシングメール/ＳＭＳは、送信元が偽装されているほか、利用者の不安を煽ったり、リンク先へのアクセスを早急に促す内容のものが多く見られます。

メッセージに含まれるリンク先をクリックすると、通信事業者を装ったフィッシングサイトへ誘導され、利用者のＩＤ、パスワードが盗まれる等の被害に遭うおそれがあり、危険です。

### 被害に遭わないために

- **電子メールやSMSのメッセージに含まれているリンク先を安易にクリックしない。通信事業者からの通知内容を確認する際は、公式サイト等から確認する。**
- **あらかじめ通信事業者のホームページを確認し、公式サイトのURLをブックマークに登録しておき、ブックマークからアクセスする。**
- **アプリのインストールは、正規のアプリ配信サイト等、信頼できるサイトから行う。**
- **ID、パスワードを入力する際は、公式サイトであることを確認した上で入力する。**
- **迷惑メールフィルタやウイルス対策ソフトの利用を検討する。**
- **通信事業者の公式サイトにおいてフィッシングに関する注意及び対策内容を確認する。**

**万が一被害に遭った場合は、通信事業者の相談窓口や最寄りの警察等関係機関にご相談ください。**

参考：一般財団法人日本サイバー犯罪対策センター
通信事業者を装ったフィッシングの注意喚起「https://www.jc3.or.jp/threats/topics/article-382.html」