

# フィッシングに注意！

## キャリア決済を不正利用されるトラブルが発生中！

通信事業者を装った身に覚えのないSMSが届き、本文に記載されているURLにアクセスすると、本物と見分けのつかない偽サイトに誘導され、IDやパスワードの入力を求められます。

IDやパスワードを入力してしまうと、キャリア決済などに不正利用されます。

※キャリア決済とは…

各携帯電話会社のID、パスワードを入力して携帯電話料金と合算して代金を支払うことができる決済サービスです。

本物と見分けがつかない偽サイトへ

URLにアクセスすると…

お客様センターです。ご利用料金のお支払い確認が取れておりません。ご確認が必要です。

<https://bit.ly/○○○○>



不正ログインの被害を助く、今すぐできるセキュリティ対策はこちら

ログイン アカウント

アカウントのID

次回ログインからIDの入力を省略

次へ

[IDをお忘れの方](#)

[アカウントを発行する](#)

[アカウントとは？](#)

[ご利用上の注意](#)

ご注意

～フィッシングSMS本文例～

お客様がご利用の電話料金が大変高額となっております。下記のURLでご確認が必要です。

**対策**

- 記載されたURLに安易にアクセスしない。
- 正しいサイトやアプリで正確な情報を確認する。
- ID・パスワード等の使い回しをしない。



サイバー犯罪に関する相談や情報は、

電話（サイバー110番） 082-212-3110

（受付 平日 8:30～17:00）

URL <https://www.pref.hiroshima.lg.jp/site/police3/cyber-jyoho-soudan.html>で受け付けています。

広島県警察 サイバー犯罪対策課