

通信事業者を装った メール・ショートメールに

注意



通信事業者を装ったメール・ショートメールによるフィッシング被害が急増しています。

不審なメールの特徴

ログイン確認のために、カード番号や暗証番号などの入力を求められるもの。

クレジットカード番号
<input type="text"/>
暗証番号
<input type="text"/>
セキュリティコード
<input type="text"/>



「緊急のお知らせ」
「重要なお知らせ」など
不安を煽るもの。

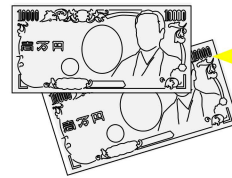
なにかあったのかな？



「通信サービスは利用停止」
「利用料金の未払い」
「支払期日」
「利用金額超過」
などの件名のメール



「プレゼント当選」などの
関心を引くメール



わあー



不正利用を疑わせる通知がくることありますが、その通知もIDやパスワードの情報を盗み取ろうとする偽物である可能性があります。



**リンク先を絶対に開かないこと。
確認は公式アプリ又は公式サイトから行うこと。**

不安に感じる事があれば、周囲の人や警察にご相談ください。

**長崎県警察本部生活安全部サイバー犯罪対策課
(連絡先 095-820-0110)**