



auやau関連サービスをかたる フィッシングメールにご注意ください！

【偽SMSの例】

【auからの重要なお知らせ】
ご利用金額が設定した金額を超えました。ご確認が必要です。
[https://bit.ly/3\[redacted\]](https://bit.ly/3[redacted])

【KDDI】利用料金の未払い金があります。お支払期限を過ぎた利用料金があります。ご確認ください。
[https://bit.ly/3\[redacted\]](https://bit.ly/3[redacted])



au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/3\[redacted\]](https://bit.ly/3[redacted])



不正アプリのインストールへ誘導される場合もあります。

【誘導されるフィッシングサイト】

お客さまへの重要なお知らせ

利用料金の未払い金があります。

お支払期限を過ぎた利用料金があります。お支払いをお願いいたします。

[支払い状況を確認する](#)

出典:フィッシング 対策協議会
URL : <https://www.antiphishing.jp/>

全国的に、au利用料金の「未払い金」や「au PAY」などのKDDIグループサービスからのお知らせや通知を装ったEメールやSMSにより、偽サイト(フィッシングサイト)に誘導され、IDやパスワードを入力してしまったことで、不正決済されるという被害が発生しています。

被害を防止するため、サービスを利用する際には、メールに記載されているURLを押さずに、必ず公式のアプリやブックマークからアクセスしてください。