

通信事業者を装った フィッシングメールに注意を



ドコモからメールが来たけど…
え？アカウント停止だって！？
メールに書いてあるリンクにアクセスしてみよう。

ちょっと待って！！そのメール、本物ですか？
メールの送信元やリンク先は偽装されていますよ。
リンク先をよく見てみると……



お客様ご利用ありがとうございます。あなたのNTTドコモアカウントは、異常な場所からアクセスされているため、ロックされています。

24時間以内にこのメッセージが確認されるまで、お客様のアカウントは保護されます。指定した期限内にこのメッセージを確認しないと、アカウントは永久にロックされます。確認ボタンを押して、アカウントが完全に安全になるまで提供する手順を完了してください。

[ログインアクティビティを確認する](#)

http://nttdocomo-co-jp.***.shop/



出典：日本サイバー犯罪対策センター(JC3)

どちらのリンク先も正規のものではありません！

図のように、フィッシングメールの手口として、通信事業者をかたり不安を煽るような内容でリンク先のフィッシングサイトにアクセスさせる手口が確認されています。

リンク先は、

- パソコン → リンク先にポインタを重ねる
- スマートフォン → リンク先を長押しする

ことで確認できる場合があるので、アクセスする前に正規のURLか確認しましょう！

