eRanger

イー・レンジャーのかわら版 (2025 年 12 月第 110 号)

■　フィッシングかと思ったらここを見て

フィッシング対策協議会の報告書によると、2025 年の報告件数は前年を上回る勢いです。
（https://www.antiphishing.jp/report/）

メールや SMS に「偽のリンク」を送り、クリックした先の Web サイトから情報を盗み出すのが主な手口です。

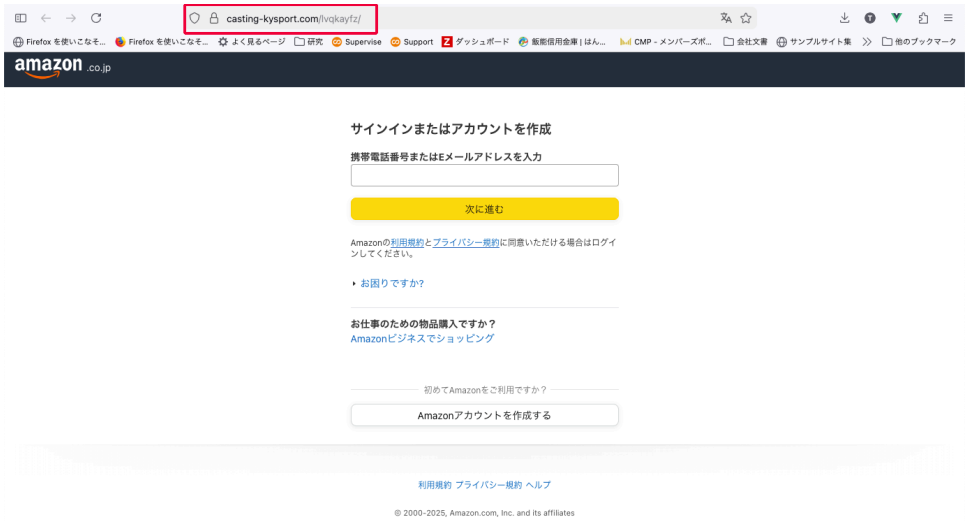
1. 差出人は簡単に偽装できるので注意が必要です

下は、実際に Amazon を騙ったフィッシングメールです。

「開封したメールが偽物かどうか」を判断する１つの手段は、差出人のアドレスを確認することです。ですが、差出人が「no-reply@amazon.co.jp」となっています。（**正しいアドレスに見えます**）**メールシステムの仕様上「差出人は簡単に偽造できる」**ので注意が必要です。

2. リンクをクリックしたらドメイン名を確認する習慣を

メールや SMS にあるリンクを開いた場合には、**一旦手を止めて**「ドメイン名」を確認する習慣を持ちましょう。
下は先のフィッシングメールにある「アカウントを確認」ボタンをクリックしたところです。



いかにも Amazon らしい画面ですが、**ドメイン名が「amazon.co.jp」ではありません。amazoncojp.com のようなそれらしい偽アドレス**が使われることもありますので、注意が必要です。