



## フィッシング・なりすまし対策を強化しましょう！

### 金融機関、EC事業者等を騙るフィッシングメールが急増！

- ✓ 金融機関やEC事業者等を騙ったメール等から偽サイトへ誘導し、**ID・パスワード**等を盗む手口が多発し、それに伴いインターネットバンキングの預金が**不正に送金**される被害が**急増**しています。
- ✓ フィッシングメールは、**実在する企業等からの本物のメール**であると思わせるため、ドメイン名をなりすまして送信されることが多くありますが、対策として**送信ドメイン認証技術**を導入することが有効です。

## フィッシング・なりすまし対策を強化しましょう！

### 1 送信ドメイン認証技術（DMARC等）を導入する！

メールアドレス偽装・なりすましの対策には、DMARC等の送信ドメイン認証技術の導入が有効です。詳細は、令和5年企業向けセキュリティチラシ第8号「DMARCでフィッシングメール対策」をご確認ください。

(<https://www.pref.hiroshima.lg.jp/uploaded/attachment/540340.pdf>)



### 2 パスキーを導入する！

パスキーはパスワードの不要な認証技術です。パスワードの管理が不要なことから、ユーザーの利便性が向上します。認証に生体情報（指紋や顔）などが必要なため、盗むことが困難です。フィッシングサイトではパスキーを利用できないため、顧客をフィッシング被害から守る対策として、非常に有効です。



## ランサムウェアなどによるサイバー犯罪被害の相談・通報は・・・

- ▶ サイバー110番 ☎082-212-3110（平日午前8時30分から午後5時までの間）
- ▶ 広島県警察本部サイバー犯罪対策課（代表☎082-228-0110）
- ▶ 最寄りの警察署

