



～事業者の皆様～

さらなるフィッシング対策強化へ！！

1 送信ドメイン認証技術（DMARC等）の導入！！

- ✓ メールアドレス偽造・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。
- ✓ なかでも、**DMARC**のなりすましメールの受信を**拒否**するポリシー「**reject**」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 フィッシングサイトのテイクダウンの促進！！

- ✓ 御社を騙るなりすましのフィッシングサイトを**認知**した際は、ホスティング事業者等にフィッシングサイトの**閉鎖依頼**を実施してください。
- ✓ 併せて、警察へもなりすましのフィッシングサイトに関する**情報提供**をお願いいたします。



3 パスキーの導入！！

- ✓ パスキーはパスワードの**不要な認証技術**で、パスワードの管理が不要ことから、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。



※ 令和7年企業向けセキュリティチラシ第1号 「フィッシング・なりすまし対策を強化しましょう！」にも掲載

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9時から午後0時、午後1時から午後4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

✓ 過去のセキュリティ情報は県警ホームページで <https://www.pref.hiroshima.lg.jp/site/cyber-security.html> >>>

