CyberCrime Control Project

令和６年２月

広島県警察本部
サイバー犯罪対策課
☎082-228-0110

フィッシング等による不正送金被害が急増しています！

企業も「フィッシング」による不正送金被害に！

- ☑ メールやSMS等を用いた「フィッシング」の手口により、インターネットバンキング利用者のID・パスワード等が盗まれ、預金を不正に送金される被害が急増しています。
- ☑ 個人だけではなく、企業もフィッシングによる不正送金被害に遭っているため、しっかり対策する必要があります。

一般的な対策（フィッシング被害に遭わないために）

1 金融機関（銀行・信用金庫）を装ったフィッシングメールに注意！
「不正アクセスの可能性」「取引の制限・停止」等、不安にさせるワードに注意してください。

2 メールやSMS内のリンクはクリックしない！
公式サイトをブックマークに登録しておく、公式アプリを使用する等の対策が必要です。

3 安易にID、パスワード、個人情報などを入力しない！
金融機関が、ID・パスワード等をSMS等で問い合わせることはありません。

企業としての対策（フィッシング被害に遭わせないために）

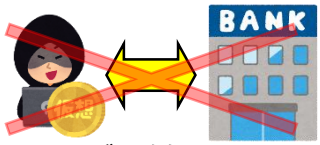
1 送信ドメイン認証技術（ＤＭＡＲＣ等）を導入する！
フィッシングメールの対策には、DMARC等の送信ドメイン認証技術の導入が有効です。
詳細は、令和５年企業向けセキュリティチラシ第８号「DMARCでフィッシングメール対策」をご確認ください。

金融機関の方へのお願い（詳細は赤枠内のＱＲコードを参照してください）

不正送金の送金先に暗号資産が利用されるケースが急増しています。
下記の対策事例を参考とした、不正送金対策の強化をお願いします。

1 振込名義変更による暗号資産交換業者への送金停止等
口座名義人と異なる依頼人名による、暗号資産交換業者への送金を拒否する。
※あらかじめ利用者に周知を図る必要があります。

2 暗号資産交換業者への不正な送金の監視強化
暗号資産と法定通貨との換金ポイントとなる暗号資産交換業者との取引に係る取引モニタリングを強化する。



暗号資産交換業者への不正送金対策の強化に関する金融機関への要請について
https://www.npa.go.jp/bureau/cyber/koho/news/20240206.html

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

☑ 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 ▶▶▶