CyberCrime Control Project

令和５年７月

広島県警察本部
サイバー犯罪対策課
☎082-228-0110

御社のメールアドレスを騙る・なりすましメール・フィッシングメール 対策！！

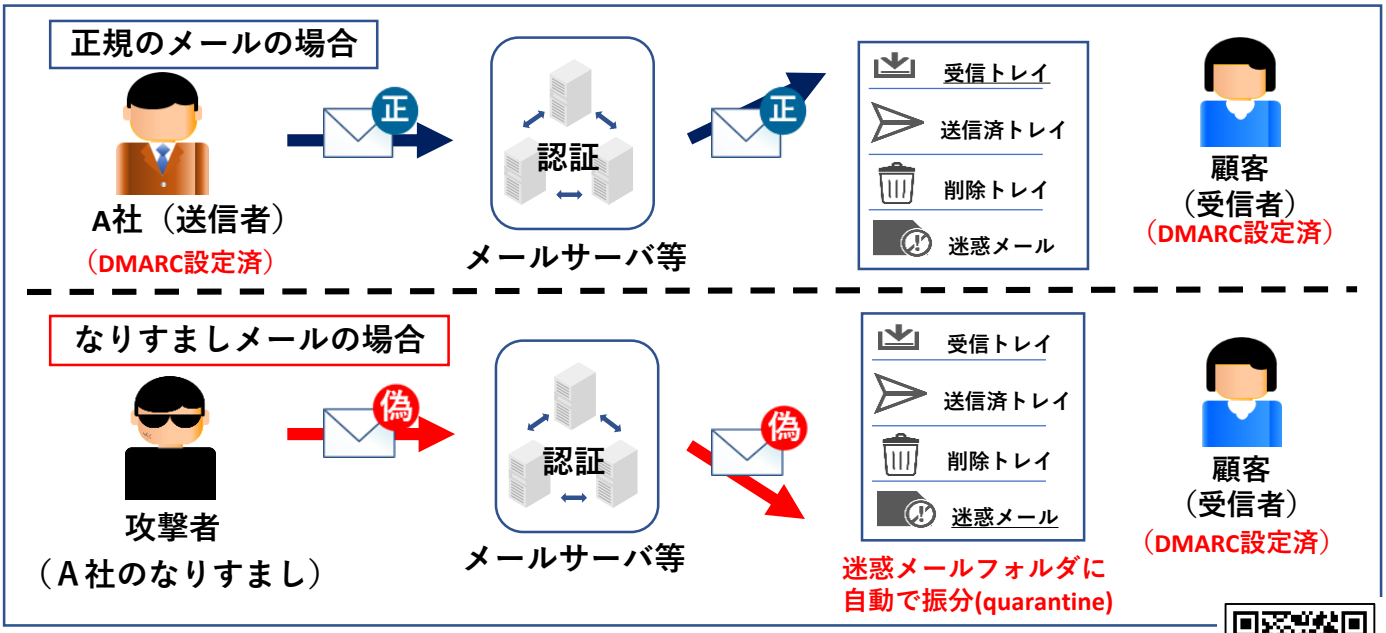
フィッシングメール（なりすましメール）を防ぐには？

- メールアドレスを詐称して送られるなりすましメールの中でも、受信者をフィッシングサイト等に誘導し、個人情報を抜き取ろうとするものをフィッシングメールと言います。
- フィッシングメール（なりすましメール）の対策には、SPF（IPアドレスによる検証）やDKIM（電子署名による検証）と言った、メールの送信元情報を検証し、正規のメールかどうかを識別する送信ドメイン認証技術の導入が有効です。
- さらに、SPF及びDKIMの認証結果を利用し、認証精度をより高めることのできる、DMARCは非常に有効な対策方法です。

DMARCを設定すると何ができるの？

- SPFやDKIMの場合、送信元の認証に失敗したメールを拒否するかどうかを受信側で設定する必要があるため、設定によっては、フィッシングメール等を受信してしまう場合があります。
- DMARCを設定することで、認証に失敗したメールについて、
  - ・reject　　＝受信を拒否する
  - ・quarantine＝迷惑メールとして取り扱う

  といった処理を送信側から指示することができます。（ただし、送信側、受信側ともに設定が必要です。）
  ※GmailやYahoo!メール等のサービスはDMARCに対応しています。
- DMARCの動作概要（quarantineに設定した場合）は次のとおりです。



自社のメールサーバーへのDMARCの導入方法については、迷惑メール対策推進協議会が公表している、「送信ドメイン認証技術導入マニュアル」を参考にしてください。
https://www.dekyo.or.jp/soudan/aspc/report.html

ウェブサイト改ざん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