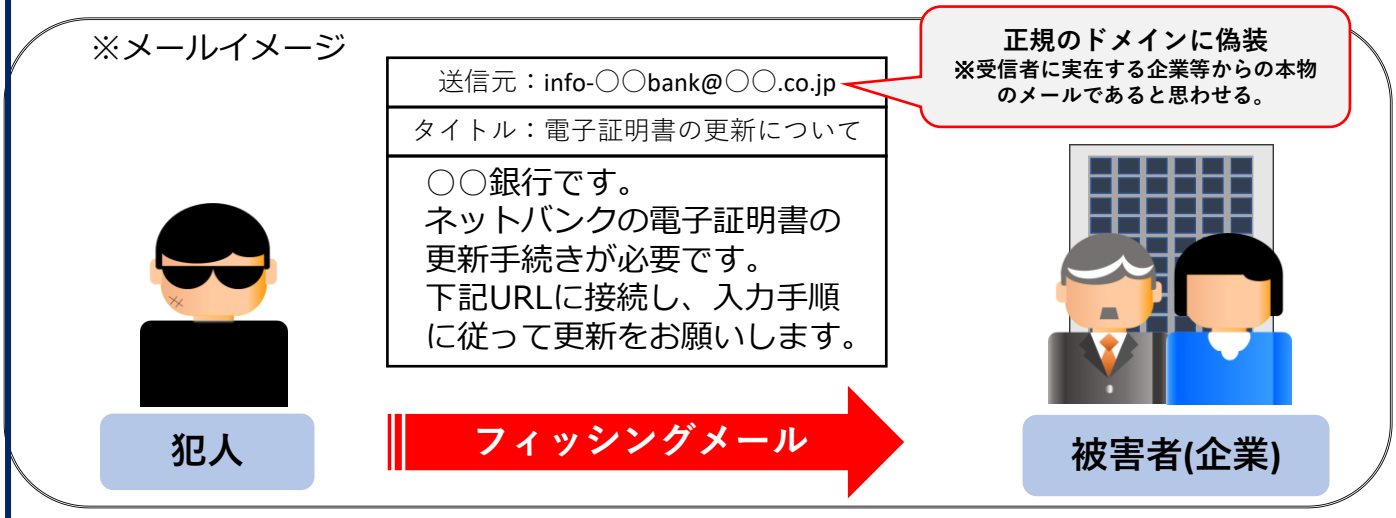
vol. 1
令和7年1月23日
鹿児島県警察本部
サイバー犯罪対策課
Tel 099-206-0110

かごしまサイバー通信

インターネットバンキングに係る不正送金の被害が急増！

不審なメールに注意！そのメール、なりすましかも？

【手口の概要】
1　犯人が金融機関、EC事業者、物流事業者等の実在する企業を騙った電子メール等を被害者に送信。
2　犯人が被害者をフィッシングサイトに誘導、インターネットバンキングのアカウント情報等を入力させて、盗み取る。
3　フィッシングサイトに入力させたアカウント情報等を使って、犯人が被害者の口座から資産を不正に送金する。



フィッシング被害に遭わないための対策！

◆ **送信ドメイン認証技術等（DMARC等）の導入によるなりすましメール対策**
DMARCの導入、フィッシングサイトのテイクダウン（閉鎖）、次世代認証技術（パスキー）の導入などの取組がフィッシング対策に有効です。

Tips

DMARCとは･･･
電子メールにおける送信ドメイン認証技術の一つです。
送信ドメイン所有者が、送信ドメインになりすましたメールをどのように処理するかを表明するものです。

もしも、被害に遭ってしまったら警察に通報・相談を！

最寄りの警察署又はサイバー犯罪相談窓口 ➡ https://www.npa.go.jp/bureau/cyber/soudan.html

被害を潜在化させないためにも「実質的な被害がなかった」「社内だけで対応できた」場合でも、ためらうことなく通報をお願いします。

警察庁 National Police Agency