

Apple を騙るフィッシング詐欺のメール事例 (フィッシング対策協議会サイトから抜粋)

「**件名**」については、

「**【重要】Apple アカウントの異常通知**」「**Apple に関するお知らせ**」「**Apple Store お客様のアカウント認証に関するお知らせ**」「**Apple お客様のアカウント認証に関する重要なお知らせ**」等

メールの本文

Apple をご利用いただき誠にありがとうございます。

システムによる定期的なチェックの結果、お客様のアカウントについて再認証が必要となりました。

「**認証手順**」

当社の公式ウェブサイトへアクセスしてください。

「**Apple Store にサインイン**」

画面に表示される指示に従い、必要な手続きを完了してください。

「**注意事項**」

このメールを受信してから 48 時間以内に認証を完了してください。そうしない場合、お客様のアカウントは一時的に凍結される可能性があります。

敬具

アップル株式会社

▶ サイトの URL

メール内の URL

https://asdk●●●●.cc/index.php?id=●●●●

https://8711●●●●.cc/index.php?id=●●●●

http://waf4yhfdg.●●●●.us/index.phpindex.php?id=●●●●

http://fsfefsg2323.●●●●.us/index.php?id=●●●●

転送先の URL

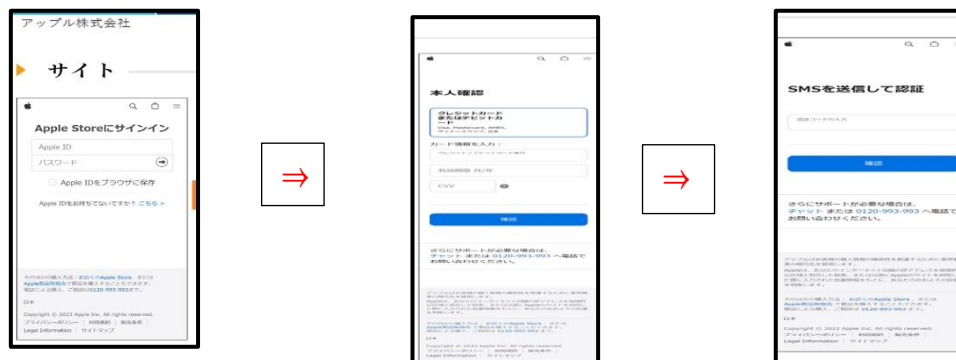
https://87●●●●.cfdf

※上記以外のドメイン、URL も使われている可能性があります。

※ URL にパスやパラメータが付いていることがあります。

※ 「●●●●」部分は伏字化しており、実際の URL とは異なります。

「**Apple Store にサインイン**」すると



※ 事例では、「システムの定期的なチェックの結果、アカウントについて再認証が必要となりました」(システムの定期的なチェックはおかしい)などと記載し偽サイトに誘導、誘導先では、「Apple ID ・パスワード」・カード情報「クレジット/デビットカード番号・有効期限月/年・セキュリティコード・認証コード」等の入力が求められます。

※ フィッシング詐欺メールにアカウント・パスワードやクレジットカード情報等を入力しない。

※ フィッシングメールに情報を入力した場合

① ID/パスワードを入力した場合

- すぐにパスワードを変更します。
- 他のサービスで同じ ID(メールアドレス)を使っている場合には、推測されやすい安易なパスワードを使っていれば、変更します。

② クレジットカード情報を入力した場合

- すぐにクレジットカード会社の紛失・盗難窓口に連絡し、利用停止と必要に応じて再発行の手続きを行います。

③ インターネットバンキングの認証情報を入力した場合

- すぐに金融機関に連絡します。