

本物そっくり？

フィッシングメールを見破るポイント



三井住友カードを装ったフィッシングメールが増加しております。

以前は「不自然な日本語」や「怪しいデザイン」で見分けやすいものでしたが、最近では本物そっくりのメールが作成され、**内容だけでは見分けることが難しくなっています。**

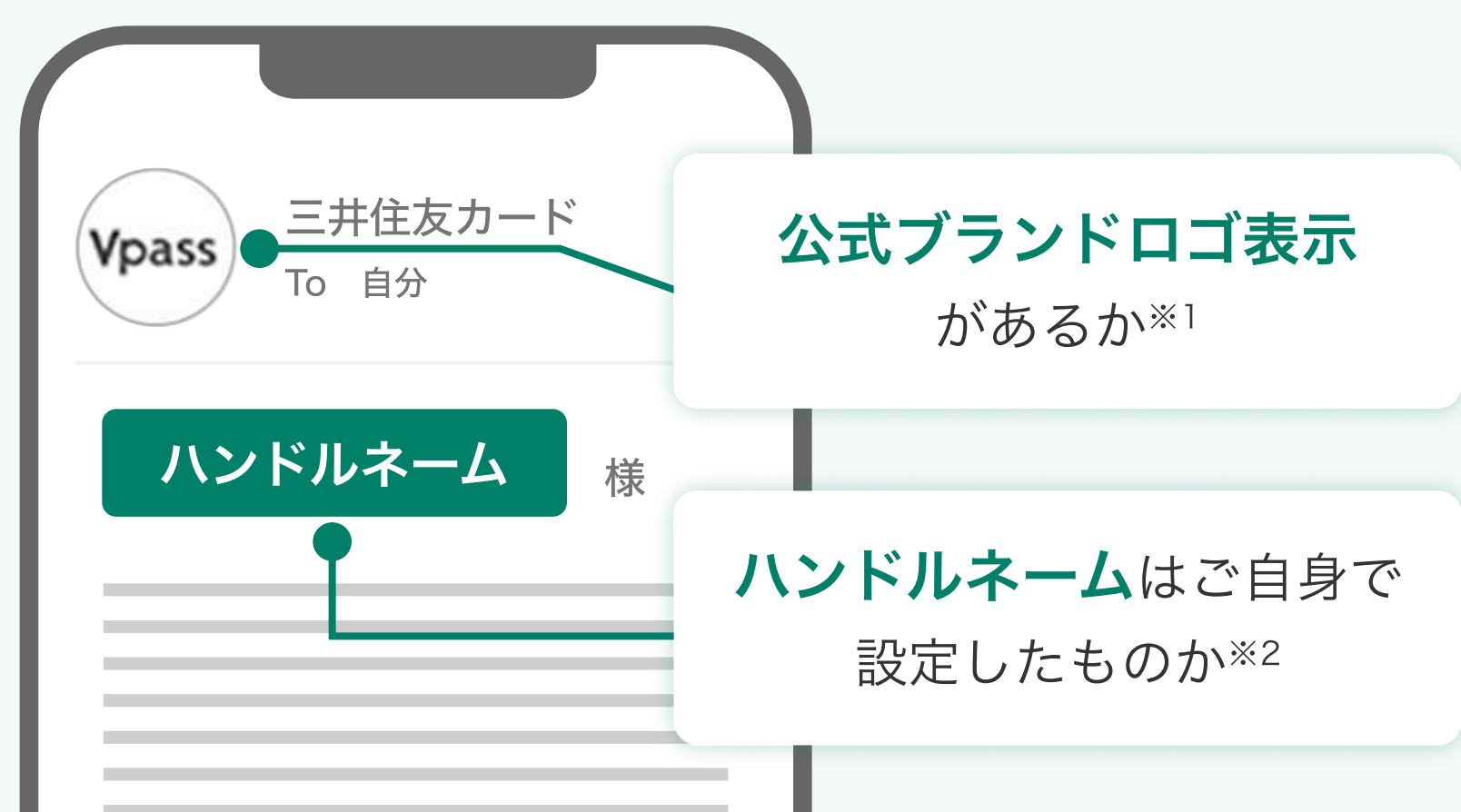
(例) Vポイント有効期限のお知らせを装う事例

こちらは実際に確認されたフィッシングメールの例です。ロゴや本文が巧妙に作られていますのでご注意ください。



公式ブランドロゴやハンドルネームを確認しましょう

本物であれば公式ブランドロゴや正しいハンドルネームが記載されています。



※1 公式ブランドロゴの表示はお使いのメールプロバイダー、アプリによって異なります。

※2 ハンドルネームの未設定の場合はカード名称又は名字が表示されます。なお、一部弊社からのメールにおいてもハンドルネームが表示されないものもございます。

チェックページを活用しましょう

弊社ではメールやSMSの真偽を確認できるページを用意しています。迷った場合はぜひご利用ください。

※ フィッシングメールとの区別のため、URLリンクを載せておりません。

チェックページは以下で確認が行えます。

1. インターネットでVpassを検索
2. Vpassページ上部の「サービス」をタップ
3. 「安心・安全サービス」の「不審なメール・SMSのチェックサービス」をタップ



セキュリティ通信編集部より

最後までお読みいただきありがとうございます。

最近のフィッシング詐欺は非常に巧妙化しており、「本文やデザインだけで見分ける」のは難しくなっています。

公式ブランドロゴやハンドルネームを確認し、冷静な対応で詐欺被害を防ぎましょう。

[過去のセキュリティ通信はこちら](#) >