フィッシング詐欺・クレジットカード不正利用に
ご注意ください

～悪質なECサイトを見つけたら、ご連絡を～

2021年のクレジットカード不正利用被害額は全国で330億円と過去最高を記録し、同年の特殊詐欺被害額（282億円）を超えています。また、フィッシングに関しても、2022年7月のフィッシング報告件数は初めて10万件を突破するなど拡大傾向です。

こうした状況を受け、関係事業者と関係省庁、関係団体が一同に会し「フィッシング、クレジットカード不正の現状と対策を考える会」を開催し、フィッシング詐欺やクレジットカードの不正利用事案に関する情報や対策を共有しました。

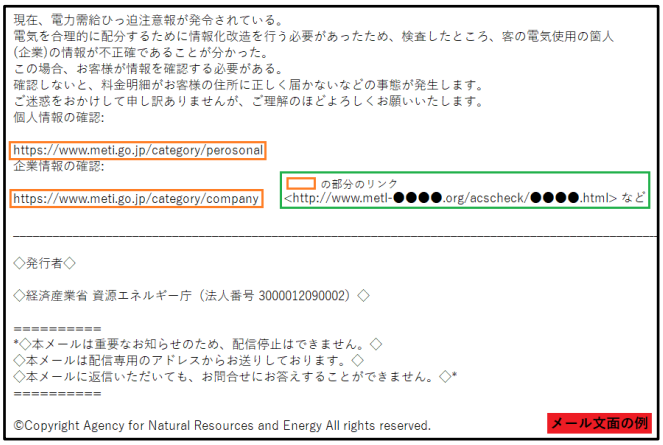
この動きを各事業者の対策につなげ、被害を未然に防いでいくため、一般のインターネット利用者（消費者）がすぐにできる対策ならびに事業者のみなさまができる有効な対策例についてご紹介いたします。

※フィッシング対策協議会　2022年7月発表

■【消費者の皆様】すぐにできる対策

不審なメールやSMSのリンクを開かない

フィッシングメールのURLを開くと、情報搾取を目的とした不正サイトに誘導されます。
また、最近ではSNS上の安売り広告などで個人情報を盗み取るサイトに誘導する手口も見られます。
身に覚えのないメール・SMS内のURLや、あまりにも安い商品を紹介するSNS内の広告・バナーはクリックしないようにしましょう。



引用：フィッシング対策協議会緊急情報
経済産業省 資源エネルギー庁をかたるフィッシング（2022/08/09）
https://www.antiphishing.jp/news/alert/meti_20220809.html

アプリ・公式サイト以外で個人の情報を入力しない

フィッシングサイトで個人の情報を入力してしまうと、クレジットカード情報などが盗み取られます。また、ものによっては不正利用者がリアルタイムで入力情報を読み取り、SMS認証なども突破してアカウントを乗っ取る手口もあります。

メールやSMSからリンクされたサイトに個人情報を入力するのは危険です。あらかじめお気に入りやブックマークなどに公式サイトを登録して利用するようにしましょう。
また、アプリのあるサービスでは、メールやSMS、SNSの広告の内容だけでなく、アプリを確認することも有効です。

なお、IDやアカウントのパスワードを他のサービスで使い回していると、そのサービスも不正利用される恐れがあります。
パスワードの使い回しは極力避け、万が一不審なサイトに個人情報を入力してしまった場合は、そのIDやアカウントと同じパスワードを使用しているほかのサービスのパスワードを速やかに変更しましょう。

引用：フィッシング対策協議会緊急情報
経済産業省 資源エネルギー庁をかたるフィッシング（2022/08/09）
https://www.antiphishing.jp/news/alert/meti_20220809.html

クレジットカードの利用明細を確認する

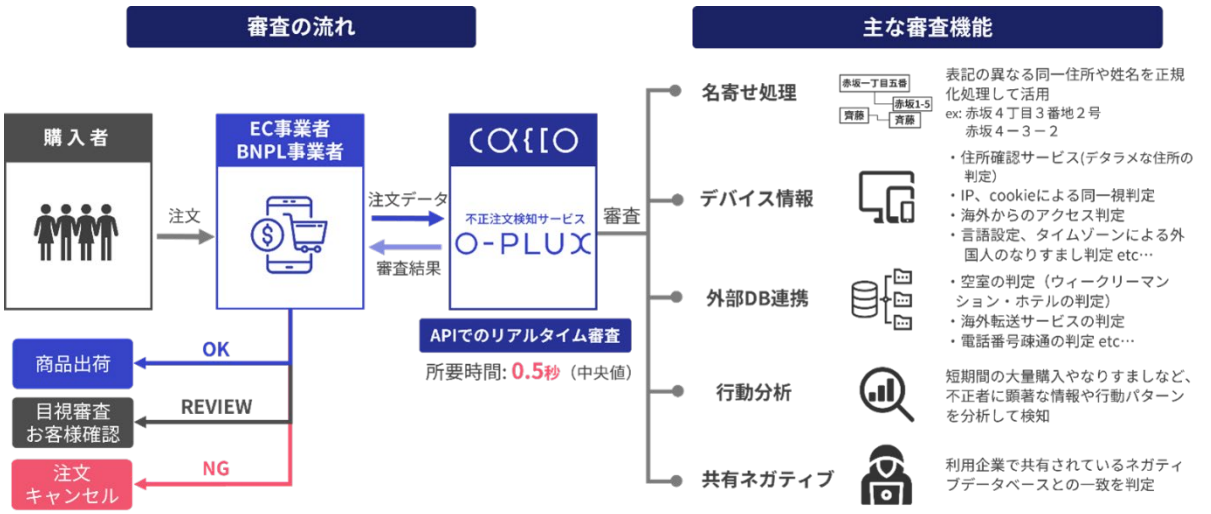
クレジットカードの利用明細は必ず確認するようにしましょう。定期的に確認することで、クレジットカードの不正利用被害を早期に把握することができます。また、身に覚えの無いクレジットカードの利用については速やかにカード会社等に連絡することで請求を止められる場合があります。ただし、不正利用されてから一定期間経過後は、請求を止めることが困難になることがありますので、ご注意ください。

■【事業者の皆様】有効な対策例

イベントでは事業者の皆様向けにいくつかの有効な対策が紹介されていました。主な対策をここでもご紹介いたします。

（クレジットカードの不正利用対策）
不正検知システムの導入や取引の目視確認

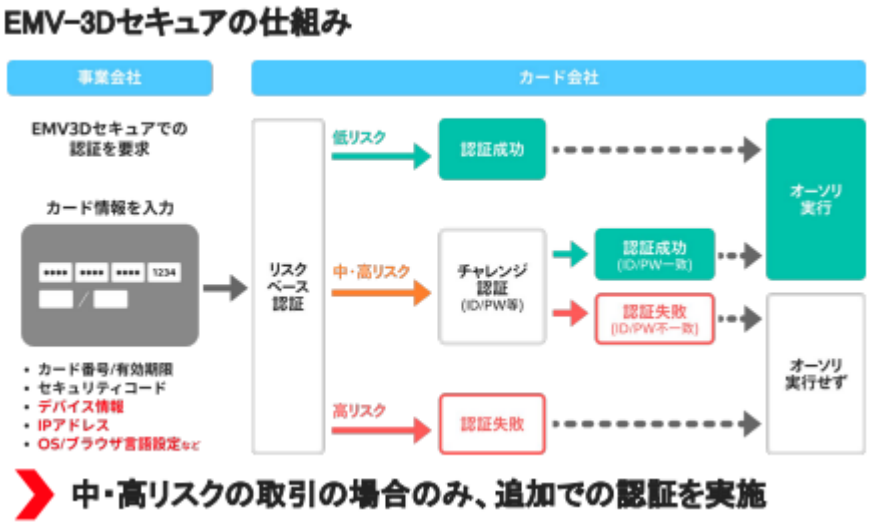
事業者の中には、独自で不正検知システムを開発・導入するとともに、怪しい決済をスタッフが目視などで注文情報を確認することで不正を防いでいることがあります。
独自の不正検知システムが開発できない場合、不正注文を検知するサービスを提供している事業者もいます。年間70億円の流通額の事業者で導入し、初年度で1億円の不正利用を検知した例もあります。このような不正検知システムの導入を検討するのも一つの方策です。



引用：かっこ株式会社説明資料

EMV-3Dセキュアの導入

クレジットカードを利用する方がカードの持ち主本人かどうかを確認する方法として、EMV-3Dセキュアがあります。
加盟店から送られる様々な情報によりリスク判定を行い、リスクに応じてカード情報に加えカード利用者にパスワード入力を求める手法です。
導入した事業者では、不正検知システムとの相乗効果で、クレジットカードの不正利用額が8か月で1/10となった例もみられました。

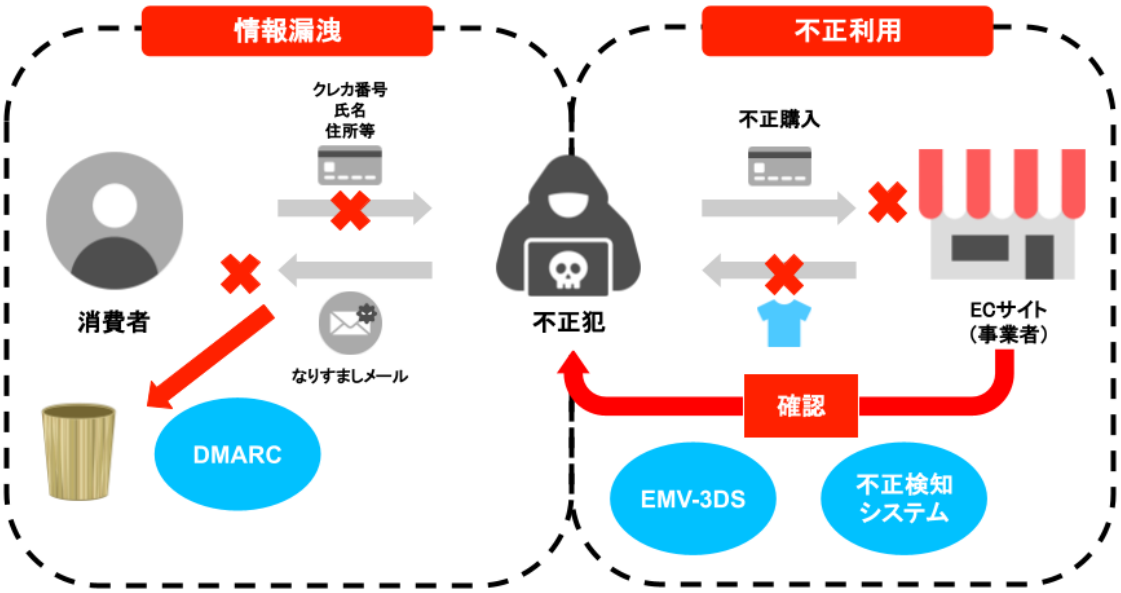


引用:株式会社メルカリ説明資料

（フィッシング対策）

ブランドを騙られないための送信ドメイン認証技術（DMARC等）の導入

消費者様にメールを送信する事業者側が送信ドメイン認証技術（DMARC等）を導入することにより、事業者様のドメインになりすましメールを迷惑メールフォルダに隔離したり、メールボックスに到達させないようにすることが可能になり、消費者様をフィッシングから守ることができます。



■偽ショッピングサイトにご注意ください

参考：JC3脅威情報（2022/10/28）
https://www.jc3.or.jp/threats/topics/article-462.html

正規のショッピングサイトを模倣する等して、利用者から購入代金を騙し取ったり、粗悪品を販売したりする「偽ショピングサイト」が見られます。これら偽ショッピングサイトで商品を購入してしまった場合、商品が届かないことが多く、届いたとしても、偽物、全く別のもの、空箱の場合もあります。
こうした偽ショッピングサイトは、検索結果からの誘導の他、最近では、SNS上に表示される広告から誘導されるケースも確認されています。

被害に遭わないための対策

（１）実在する会社であることを確認する

初めて利用するショッピングサイトでは、会社概要等で、事業者の氏名（名称）、住所、電話番号が記載されているか確認しましょう。なお、架空の情報や実在する会社を騙っていることもあるため、名称や連絡先等を検索し、実在する会社が運営しているサイトか否かを確認しましょう。

（２）偽ショッピングサイトの特徴に注意する

偽ショッピングサイトには以下のような特徴があります。
●商品価格が他のサイトと比べて極端に安価・割引率が高い。値引き前の価格も示して異常に安売りしているかのように見せているサイトや広告には特に注意。
●支払い方法としてクレジットカード決済が可能と記載があるものの、決済時に口座振込のみ可能であると限定される。
●口座名義人が法人口座ではなく個人口座が案内される場合、その名義が会社概要などに記載された代表者と異なる名義の口座となる。
●文章の繋がりや単語などが不自然な日本語表現や、単なる誤記と考えにくい場合がある。
●URLのドメインに「.xyz」「.top」等のTDL（トップレベルドメイン）を使用している。

（３）セキュリティ対策ソフトの利用

市販のセキュリティ対策ソフトを導入することで、偽ショッピングサイトへのアクセスを防ぐことが期待できます。

■悪質ECサイトホットラインについて

SIAでは「悪質ECホットライン」を設けています。このホットラインでは、正規サイトを模倣し金銭や個人情報を収集する目的として作成された詐欺サイトやフィッシングサイト等の悪質なサイトの通報を受け付けています。
普段利用しているウェブサイトと異なるサイトを確認した場合にはこちらにご連絡をお願いいたします。

（悪質サイト例）
銀行振込等で支払いしても商品が発送されなかった場合
クレジットカード情報等を盗まれた可能性がある場合
運営するサイトを第三者によって改ざんされた場合
運営するサイトのコンテンツ（会社情報等）を悪用された場合

悪質ECサイトを通報する ▶▶ 悪質ECサイトホットライン
※犯罪に遭われたとお考えの場合には警察にもご相談ください。

消費者や事業者のみなさま双方で対策や注意点の情報に触れ、不正利用を防止していきましょう。