**めあて** ●クレジットカードを悪用するサイバー犯罪の手口や対処法を学ぶ。

**解答**

埼玉県警察サイバー局

# 防犯 ネット犯罪から身を守る

## クレジットカード犯罪

なまえ　　年　　組　　番

点

**1** クレジットカードに関する説明として、正しい（適切な）ものを{　　}内から選び、○で囲みましょう。（各10点：30点）


▸ クレジットカードとは、物を買ったり、サービスを受けた時の代金を{ 無かったこと ・ 出世払い ・ **後払い** }にできるカードで、手元に現金がなくても支払いができる。

▸ クレジットカードは、カード番号などの情報があれば{ ウィンドウショッピング ・ **ネットショッピング** ・ お店で言うだけ }で使えてしまうので、他人に見せたり、教えてはいけない。

▸ クレジットカード不正利用被害全体のうち、番号盗用被害の割合は、{ 少ない ・ 約半分 ・ **大部分を占める** }。

※番号盗用被害とは、本人のクレジットカード本体は手元にあるのに、カード番号などの情報だけで他人に不正に買い物（決済）をされてしまう被害のこと。

**2** 次の絵の組み合わせが示す、クレジットカード犯罪の手口を下の語群から選び、記号で答えましょう。（各10点：30点）

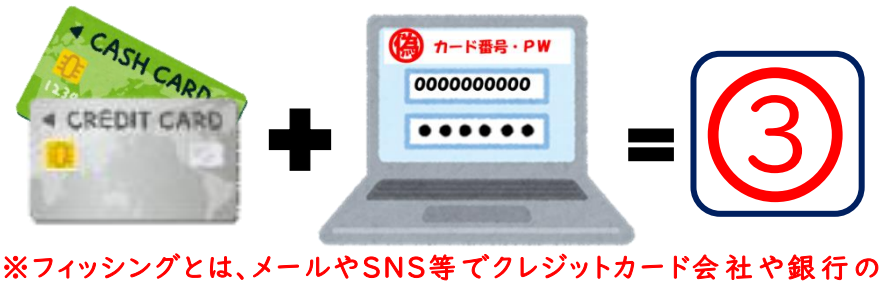
**語群**

①クイッシング　②スキミング　③フィッシング

①

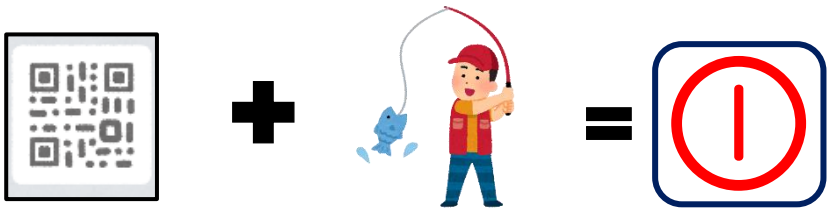

※スキミングとは、特殊な装置を使って、クレジットカード情報を盗み取る手口。

②




※フィッシングとは、メールやSNS等でクレジットカード会社や銀行のサイトにそっくりな、偽のサイトに誘導して、クレジットカード番号やキャッシュカード番号、暗証番号などを入力させ、盗み取る手口。

③



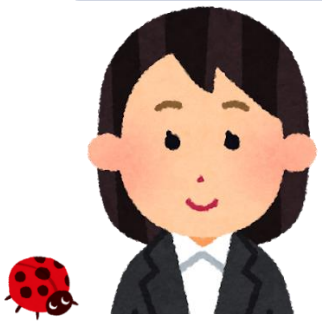
※クイッシングとは、二次元コードを悪用して、フィッシングサイトに誘導して個人情報をだまし取る手口。

**3** 次の会話は、クレジットカード会社に勤務する人からのアドバイスです。（　）に当てはまる言葉を下の語群から選びましょう。（各5点：10点）

**語群**

●SNSなどのダイレクトメッセージ　●モールス信号
●メールの受信歴　●クレジットカードの裏面

最近のフィッシングは、ショートメールや電子メールだけではなく、（SNSなどのダイレクトメッセージ）でも送られてくることもありますから、注意してください。



利用した覚えのないクレジットカードの利用があったときには、（クレジットカードの裏面）に書かれた電話番号や二次元コードを読み取って出てきた連絡窓口に電話をしてください。

**4** クレジットカードの利用に関して正しい話をしている人をすべて選び、記号で答えましょう。（30点）

ア

3年位前に引っ越したけど、住所変更は面倒なので、クレジットカード会社に連絡していませーん。

イ

クレジットカード情報をアプリなどに登録するとき、「どのアプリに何のクレジットカードを登録したか」を記録してるよ。

ウ

いろんなクレジットカード会社のアプリを使っていますが、私は物忘れが多いので、アプリのパスワードは、どれも同じにしています。

エ

クレジットカード会社のサイトとそっくりな怪しいサイトがあるから、私はクレジットカード会社のアプリからしかアクセスしてません！

答え　イ　エ

うら **めあて** ●クレジットカードを悪用するサイバー犯罪の手口や対処法を学ぶ。 **解答**

埼玉県警察サイバー局

# 防犯 ネット犯罪から身を守る

## クレジットカード犯罪

なまえ　　年　組　番

点

**5** クレジットカード犯罪に関する問題です。 □ の犯罪手口の対策方法を □ から選び、線でつなぎましょう。（各5点：20点）

| | |
|---|---|
| 偽・詐欺サイト | パソコンとスマートフォンにのぞき見防止フィルタを貼る。 |
| 不正アクセス | IDとパスワードはアプリやサイトごとに変えて、二段階認証や多要素認証を設定する。 |
| ソーシャルエンジニアリング | インターネットブラウザにID・パスワード・カード情報などを保存せず、専用のパスワードを管理するアプリを使う。 |
| インフォスティーラー | ネットショッピングの時に、商品が安すぎないか、会社概要の住所や連絡先、ＵＲＬが偽物ではないか等をしっかり調べる。 |

※偽物のサイト に誘導して、ID・パスワード・カード情報などをだまし取る手口

※他人のID・パスワードを入力するなどして、他人のアカウントにアクセスする行為

※パスワードの入力画面をのぞき見るなどして、重要な情報を盗み取る行為

※インターネットブラウザに保存されたID・パスワード・カード情報などを盗み取るコンピュータウイルス

OSバージョンを最新にしたり、パスワードを長く、記号を使って複雑にするなどの、基本も忘れずにね！

**6** 下の人たちが話している内容が正しいものには○、誤りには×を □ の中に記載しましょう。（各5点：30点）

クレジットカードの利用状況なんて自分で使ってるんだから、確認する必要ないでしょ。

×

最近のフィッシングメールは、本物そっくりに作られていて、見分けることは難しいって聞いたよ！

○

Ｉ回だけ使える秘密の合言葉を入力したりして、クレジットカードを使っている人が本人かどうかを確認する仕組みがあるよ！

○

※この仕組みを「EMV3-Dセキュア」といいます。

偽サイトのＵＲＬをまとめているサイトがあるからネットショッピングをするときは、そういうサイトをチェックすることも大事なのさっ☆

○

不正利用されたときにすぐ分かるよう、クレジットカードの利用通知サービスを設定した方が良いぜ。

○

「クレジットカード情報の更新」というメールが届いたら、メールの中のＵＲＬから登録すれば良いんだよ！

×

## サイバー犯罪から大事な情報を守るために

フィッシングや偽ショッピングサイトの手口は、年々、巧妙かつ悪質化しています。

クレジットカードは大変便利ですが、その利便性は正しい自己管理があってこそ成り立つものです。

犯罪者は、利用者の「今しかない」と思わせる言葉で心の隙を狙っています。「自分は大丈夫」「自分は関係ない」と思わず、日頃から最新の犯罪手口を確認しましょう。特に金銭にまつわる話には日頃から注意を払い、「メールのリンクからアクセスをしない」「利用明細をこまめに確認する」といった行動を習慣化していただき、被害に遭うリスクを下げましょう。

もしも迷ったり、被害に遭ったかもしれないと思った時には、一人で悩まず、すぐにクレジットカード会社や警察などへ相談していただき、被害を最小限に抑えましょう。

あなたの大切な資産と生活を守るため、サイバーセキュリティに関する下記情報サイトを活用してください。

埼玉県警察ホームページ

サイバーテスト回答はこちら!!

埼玉県警察サイバー対策課公式Ｘ