大丈夫と思っている
あなたのマネーが危ない！

金融犯罪
安全チェック

用心すべきポイントを
一緒にチェック
してみましょう！

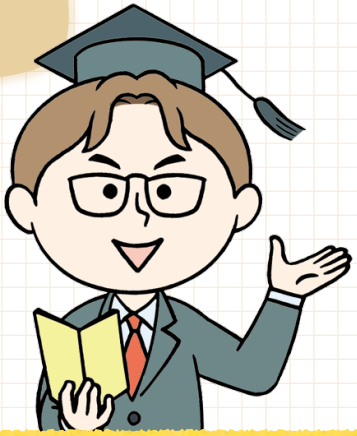
JBA JAPANESE BANKERS ASSOCIATION
一般社団法人
全国銀行協会

あなたは犯罪の手口を見破れますか？

金融犯罪に巻き込まれ ないために 用心すべきポイントを チェックしましょう！

さまざまなタイプの金融犯罪が
発生している現在、
誰もが被害者になる可能性があります。
どんな点に用心すべきか、
犯罪手口を再現したシーンをもとに
具体的な対策について学びましょう。

犯罪に巻き込まれないための
知識が十分に身についているか
どうかさっそくチェック
してみましょう！



詳しい情報は
こちらでも！

「ニセモノ」にご用心！

- オレオレ詐欺
- キャッシュカード詐取
- キャッシュカードすり替え詐欺
- 架空料金請求詐欺

3 ページへ

「うまい話」にご用心！

- 還付金詐欺
- 銀行口座の売買

11 ページへ

「インターネット犯罪」にご用心！

- マルウェアによる犯罪
- フィッシング詐欺
- クラウド等からの個人情報流出

15 ページへ

「身の回り」にご用心！

- ATM 利用者をねらった犯罪
- キャッシュカードの盗難
- キャッシュカードの偽造

21 ページへ

WEBサイトでも金融犯罪の手口と防止策をご案内！

さまざまな種類の金融犯罪について、
その手口と防止策をわかりやすく解説します。

全銀協　金融犯罪　検索

\ 金融犯罪にご用心！ /

Q 「ニセモノ」にご用心！❶

ある日、あなたのもとに息子を名乗る者から電話が。次の対応のどこに問題があるのかわかりますか?

ヒント

息子さんのピンチを救うためとはいえ、知らない人にお金を渡してしまってよかったのでしょうか?

A これが「オレオレ詐欺」の手口です！

❗ 身近な人を装ってウソの話でだます

小切手の置き忘れなど
もっともらしい話でだまし、
現金を要求してきます。
犯人は、あらかじめ名簿などを
入手して、家族構成や
勤め先などを調べている
場合もあります。
(警察官や弁護士などを装う場合も)

☑ 用心する「ポイント」はココ！

❶ 当事者本人や家族に事実を確認する。

電話で突然お金を要求されたら、一度電話を切り、当事者本人や家族の電話番号に連絡して、事実を確認しましょう。

❷ 知らない人にお金を渡さない。

「会社の同僚が取りに行く」などと言って、知らない人が現金を取りに来ます。知らない人には絶対にお金を渡さないでください。

❸ 留守番電話を活用しましょう。

在宅時でも留守番電話機能を設定し、電話の相手を確認してから電話に出るようにしましょう。犯人からの電話に「出ない」ことが一番の防犯対策です。

さらにここにもご用心！

お金を取りに来る以外にも、「銀行の窓口が閉まってしまう」などと急がせ、犯人の口座にお金を振り込ませようとする手口もあります。

Q 「ニセモノ」にご用心！❷

ある日、警察を名乗る者から
あなたの口座に関する電話が。
次の対応の問題点はどこでしょうか?

ヒント

初対面の相手にキャッシュカードを渡してしまって本当に大丈夫でしょうか？

A これが「キャッシュカード詐取」の手口です！

! 複数の登場人物で信ぴょう性を持たせ、あなたのお金をだまし取る

警察官や銀行協会職員など複数の人物が登場し、「あなたの口座が犯罪に利用されているので口座を凍結します」などの話をきっかけに、キャッシュカードの暗証番号を聞き出してキャッシュカードをだまし取ろうとします。

☑ 用心する「ポイント」はココ！

❶ カードをお預かりすることは一切ありません。

銀行協会職員などを名乗る者から質問や訪問を受けても、キャッシュカードや通帳、現金を渡さないでください。暗証番号をお尋ねすることも一切ありません。

❷ 犯人の騙(かた)る身分だけで簡単に信用してはいけません。

犯人は警察官や銀行協会職員などを装い、もっともらしいことを言って情報を聞き出そうとしてきます。「警察」「銀行協会」などのフレーズにだまされないでください。

❸ 「劇場型」の展開に注意しましょう。

複数の人物が登場し、巧みにストーリーが展開される「劇場型」の手口が特徴です。犯人のペースに巻き込まれて冷静に判断する余裕を失わないようにしましょう。

さらにここにもご用心！

百貨店店員や家電量販店店員などを装って「あなた名義のクレジットカードが悪用されている。このままだとキャッシュカードも悪用される可能性がある」などの話をきっかけに、キャッシュカードをだまし取ろうとする手口もあります。

Q 「ニセモノ」にご用心！❸

ある日、銀行協会職員を名乗る者が
あなたのもとを訪問。
次の対応の問題点はどこでしょうか？

ヒント

初対面の相手のところに
キャッシュカードを置いたまま
目を離してしまって大丈夫でしょうか？

A これが「キャッシュカードすり替え詐欺」の手口です！

❗ 目を離した隙に封筒をすり替えてキャッシュカードを盗み取る

「キャッシュカードが悪用されているので確認に行く」などの名目で警察官や銀行協会職員などになりすました犯人が被害者宅を訪れ、被害者が目を離した隙に、犯人があらかじめ用意しておいた偽物のカードが入った封筒と、キャッシュカードの入った本物の封筒をすり替えることによりキャッシュカードを盗み取ります。

☑ 用心する「ポイント」はココ！

❶ キャッシュカードは慎重に管理しましょう。

たとえ印鑑を取りに行ったほんの一瞬であっても、他人のところにカードを置いたまま目を離してはいけません。また、警察官や銀行協会職員などが自宅にカードを受け取りに行くことは絶対にないことを覚えておきましょう。

❷ 留守番電話を活用しましょう。

犯人は被害者宅を訪問する前に、警察官などを装って電話をしてきます。在宅時でも留守番電話機能を設定し、電話の相手を確認してから電話に出るようにしましょう。

❸ 被害を最小限にとどめる。

キャッシュカードを入れた封筒は封緘されるため、容易に開封ができず、被害発覚が遅くなりがちです。もしものときに備えて、預金残高のこまめなチェックやATMの利用限度額を低くする設定を行いましょう。

さらにここにもご用心！

キャッシュカードにハサミで切り込みを入れたり、小型パンチで穴をあけたりして使用できなくなったように信じ込ませたうえでキャッシュカードをだまし取る手口もあります。

Q 「ニセモノ」にご用心！❹

ある日、有料サイトの利用料を
請求するショートメッセージ(SMS)が。
次の対応の問題点はどこでしょうか?

ヒント

本当に利用したのかよく確認せずに、
有料サイトの利用料を振り込んで
大丈夫でしょうか?

A これが「架空料金請求詐欺」の手口です！

! 身に覚えのない料金が請求される

アダルトサイトや出会い系
サイトの利用料など、
身に覚えのない料金を
請求する、ショートメッセージや
電子メール、はがきが
送られてくるのが特徴です。
「職場や自宅に取り立てに行く」
などの脅迫文を盛り込み、
不安をあおって
支払いを要求します。

☑ 用心する「ポイント」はココ！

❶ 焦って連絡してはいけません。

ショートメッセージや電子メールに「すぐ連絡してください」などと書かれていても、絶対に連絡してはいけません。犯人の思うつぼです。

❷ 脅迫文は無視しましょう。

「職場や自宅に取り立てに行く」と書かれていると不安にかられますが、実際に取り立てに来ることはまずありません。身に覚えのない請求は無視しましょう。

❸ 心当たりのないショートメッセージ等には注意を。

ショートメッセージ等に記載されているURLをむやみにクリックしたり、電話番号に電話をかけないようにしましょう。怪しいと感じたら開かず、削除しましょう。

さらに
ここにも
ご用心！

一度支払うと何度もお金を振り込むよう要求されてしまいます。また、コンビニで電子マネーを購入させる手口もあります。

Q 「うまい話」にご用心！❶

ある日、市役所職員を名乗る者から電話が。次の対応のどこに問題があるのかわかりますか？

ヒント

ちょっと待ってください！
相手に言われるがままにATMを
操作して本当に大丈夫でしょうか？

A これが「還付金詐欺」の手口です！

❗「還付金があります」と騙(かた)りお金を振り込ませる

市区町村や年金事務所などの職員を装い、「医療費を還付します」「年金の未払い分を還付します」という電話をかけてきます。金融機関の無人店舗のATMやコンビニエンスストアのATMに誘い出す手口が特徴的です。

☑ 用心する「ポイント」はココ！

❶ ATMでお金を還付することはありません。

市区町村などが、医療費などを還付するためにATMの操作をお願いすることはありません。怪しいと思ったら関係機関に問い合わせてください。

❷ ATMにはお金を「受け取る」機能はありません。

ATMは自分のお金を出し入れしたり、相手先に振り込む機能などしかありません。電話相手の巧妙な説明にだまされないようにしてください。

❸ 「携帯電話を持ってATMへ」と言われたら詐欺です。

ATMコーナーで、携帯電話をご利用のお客様には、犯罪被害防止の観点から、行員などがお声かけをさせていただくことがあります。

さらにここにもご用心！

「期日が今日中に迫っている」などと急がせ、冷静に考える余裕を与えません。怪しいと思ったら電話を切り、すぐに周囲の人に相談しましょう。

Q 「うまい話」にご用心！❷

ある日、銀行口座の売買を
持ちかけるダイレクトメールが。
次の対応の問題点はどこでしょうか？

ヒント

自分の名前でつくった口座を他人に渡して本当に問題はないのでしょうか？

A 「銀行口座の売買」は犯罪です！

! 使用していない口座の売買をもちかける

インターネットやダイレクトメール、SNS、SMSで「手軽にお小遣い稼ぎをしませんか」などと、犯罪行為とにおわせないように銀行口座の売買をもちかけてきます。口座売買を行った場合、その後の口座開設を断られる場合があります。

☑ 用心する「ポイント」はココ！

❶ 口座を売る側も罪に問われます。

他人になりすまして口座を開設したり、預金通帳やキャッシュカードなどを他人に売り渡したりすることは犯罪です。

❷ 使わなくなった口座は解約を。

使わなくなった自分の口座の預金通帳やキャッシュカードを、「もう使っていないから」といって売り渡すのも犯罪です。使わない口座は解約しましょう。

❸ 安易なもうけ話には注意しましょう。

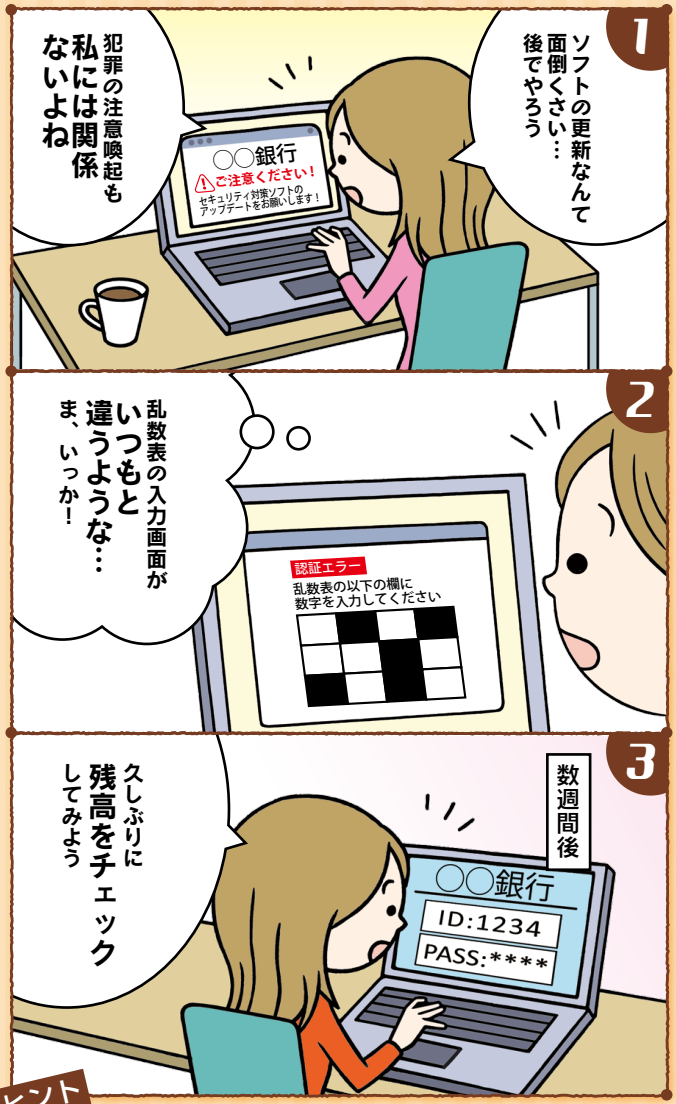
安易なもうけ話は、犯罪に巻き込まれる可能性があります。楽に収入が得られるという甘い言葉にそそのかされて、簡単に信じないようにしましょう。

さらにここにもご用心！

たとえ気軽な気持ちで始めたとしても、犯罪に加担した時点であなたも共犯者です。犯罪行為を行った場合、口座の利用が停止されたり、その後の口座開設を断られる場合があります。

Q 「インターネット犯罪」にご用心！❶

インターネット・バンキングを
利用する際に、どんな用心が必要か
チェックしてみましょう。



ヒント

いつもの取引画面と違うのに、
認証情報を入力してよかったのでしょうか？

A これが「マルウェアによる犯罪」の手口です！

! 利用者をニセ画面でだまして認証情報を盗む

不正・有害ソフト（マルウェア）に感染した端末から
インターネット・バンキングに
アクセスした際、
認証画面を書き換えたり
ニセの画面を表示させます。
そこから認証情報をだまし取り、
預金を不正に引き出します。

☑ 用心する「ポイント」はココ！

❶ マルウェアの感染を防ぎましょう。

ウェブサイトやウェブサイト上の広告、電子メールなど、マルウェアの感染源はさまざま。パソコンやスマートフォンにインストールしているソフトやOSは常に最新の状態にしておきましょう。

❷ 認証情報のやりとりは特に慎重に。

ニセの画面や入力欄を表示して認証情報を入力させようとしてきます。怪しいと感じたら入力する前に銀行の注意喚起などを確認しましょう。

❸ 銀行のセキュリティ対策ツールを積極的に活用する。

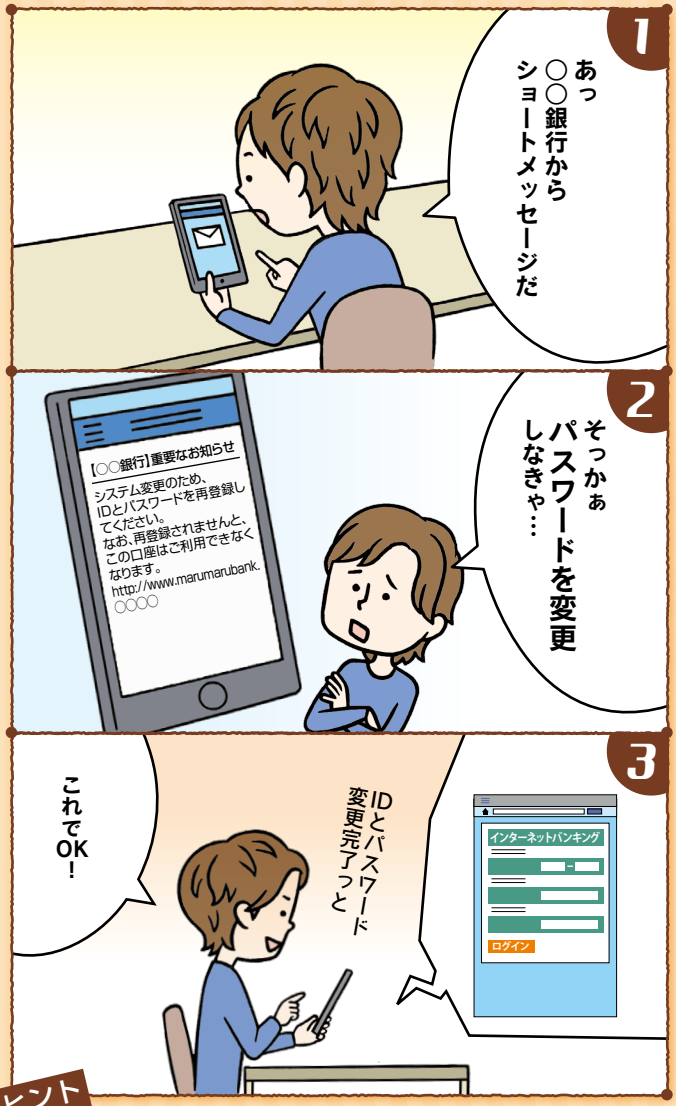
取引銀行が提供するセキュリティ対策ツールを積極的に使いましょう。預金残高のこまめなチェックや取引限度額の設定も、もしものときの被害抑制のために重要です。

さらにここにもご用心！

取引の途中からニセの画面を表示させ、その裏で自動送金する高度な手口（MITB攻撃）もあります。

Q 「インターネット犯罪」にご用心！❷

ある日、銀行を名乗るショートメッセージ（SMS）が。次の対応のどこに問題があるのかわかりますか？

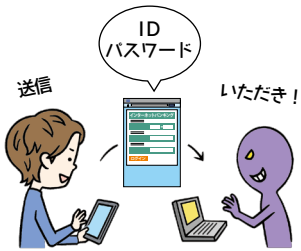


ヒント

IDやパスワード変更に関するショートメッセージを簡単に信用してしまってよかったのでしょうか？

A これが「フィッシング詐欺」の手口です！

銀行を装ったショートメッセージやメール等でIDやパスワードを盗む



件名で「重要なお知らせ」などと危機感をあおり、銀行を装ったニセのショートメッセージやメールを開かせます。URLからニセのサイトに誘導し、IDやパスワードを入力させ、それらの情報を盗みます。

☑ 用心する「ポイント」はココ！

❶ パスワードの入力を求めるショートメッセージに注意。

銀行がショートメッセージやメールでパスワード等重要情報の入力をお願いすることはありません。また、心当たりのないショートメッセージやメールは開かないようにしましょう。

❷ 銀行の注意喚起の確認を。

銀行ではウェブサイト等を通じて最新の被害手口などについての注意喚起をしています。注意喚起を見て、怪しいと思った場合はパスワード等の重要情報の入力はしないようにしましょう。

❸ 銀行のウェブサイトを「お気に入り」に登録。

取引銀行のウェブサイトを、あらかじめウェブブラウザの「お気に入り」に登録し、そこからアクセスしましょう。取引銀行がアプリを提供している場合は、アプリから操作することも有用です。

さらにここにもご用心！

メールの添付ファイルや、誘導したウェブサイト等からマルウェアに感染させることも。日頃から注意し、スマートフォンやパソコンは安全に保ちましょう。

Q 「インターネット犯罪」にご用心！❸

インターネット・バンキングを利用する際に、どんな用心が必要かチェックしてみましょう。

ヒント

IDやパスワード等の重要情報をクラウドサービスに登録してしまってよかったのでしょうか？

A 「クラウド等からの個人情報流出」に気を付けましょう。

! 気が付かないうちに口座のIDやパスワードを盗む

ウイルス感染などによって、利用しているクラウドサービスのIDやパスワードが流出した場合、第三者による不正アクセスによりクラウドサービス上に保管している情報が漏えいする可能性があります。（スマートフォンのメモアプリから漏えいする場合も）

☑ 用心する「ポイント」はココ！

❶ 認証情報の管理は特に慎重に。

クラウドサービス事業者へのサイバー攻撃やその他の要因で、預けているデータが外部に漏えいする可能性があります。万が一を想定し、クラウドサービス上に預けるデータの性質を慎重に判断することが大切です。

❷ パスワードの使い回しを避ける。

万が一、クラウドサービスの情報が流出した場合、流失したものと同じIDとパスワードを他のサービスでも利用していた場合、他のサービスでも不正アクセスを受ける危険性が高まります。IDやパスワードは、個別のサービスごとに異なるものを設定し、使い回しをしないことが大切です。

❸ セキュリティ対策ツールを組み合わせて利用を。

銀行は、インターネット・バンキングの不正利用防止のためにさまざまなセキュリティ対策ツールを提供しています。複数のツールを組み合わせるなどして効果的に使いましょう。

さらにここにもご用心！

不正に入手した口座情報をもとに、キャッシュレス決済サービス（○○ペイ、○○Payなど）のアカウントを開設するとともに銀行口座と連携したうえで、預金を不正に引き出す手口もあります。

Q 「身の回り」にご用心！❶

ATMを利用するために銀行に。
次の行動のどこに用心が
必要でしょうか?

ヒント

ATMの利用中に声をかけられましたが
キャッシュカードから目を離してしまって
大丈夫でしょうか?

A これが「ATM利用者をねらった犯罪」の手口です！

ATM利用者の注意をそらしカードや現金を盗む

ATMでの現金引き出しや入金時などに利用者の注意をそらし、そのスキに現金やキャッシュカードを盗みます。また、肩越しに暗証番号をのぞき見するケースもあります。

☑ 用心する「ポイント」はココ！

❶ ATM操作時は、周囲に怪しい人物がいないか確認を。

ATMにはミラーで後ろを確認できるものも多くあるので、利用時は周囲に怪しい人物がいないか確認しましょう。また、操作が完全に終わるまでは絶対に離れないようにしましょう。

❷ 多額の現金を扱うのは、人通りの多い昼間に。

人通りの多い昼間の時間帯であれば、犯人も利用者の注意をそらすような派手な行動が難しくなります。

❸ キャッシュカードを盗まれたら、すぐに口座を停止。

万が一、キャッシュカードを盗まれた場合は、直ちに銀行に連絡し、口座の利用を停止してください。

さらにここにもご用心！

ATMの利用者を尾行・待ち伏せし、ひったくりなどを行う手口もあります。大金を扱う際は、信頼できる人と一緒に行くようにしましょう。

Q 「身の回り」にご用心！❷

電車の中でついついうたた寝…。
被害を防ぐために
どんな用心が必要でしょうか?

ヒント

電車でうたた寝をしてしまうこと、誰でもありますよね。日頃からどんな用心が必要か考えてみましょう。

A 「キャッシュカードの盗難」はいつでも起こり得ます!

キャッシュカードと一緒に盗んだものから暗証番号を推測

置き引きやスリ、
ひったくりや車上荒らしなどで
キャッシュカードを盗み、
さらに一緒に盗んだ運転免許証
や保険証などから暗証番号を
推測して、お金を引き出します。

☑ 用心する「ポイント」はココ！

❶ キャッシュカードを入れているものを手放さない。

キャッシュカードを入れている財布やバッグ、脱いだ上着などから目を離さないようにしましょう。電車の網棚や、自動車の車内などにも放置しないように注意しましょう。

❷ 暗証番号は、推測されにくいものに。

キャッシュカードの暗証番号は、生年月日や住所、電話番号などの、他人に推測されやすいものは避けましょう。

❸ 暗証番号の管理に注意。一緒に携帯しない。

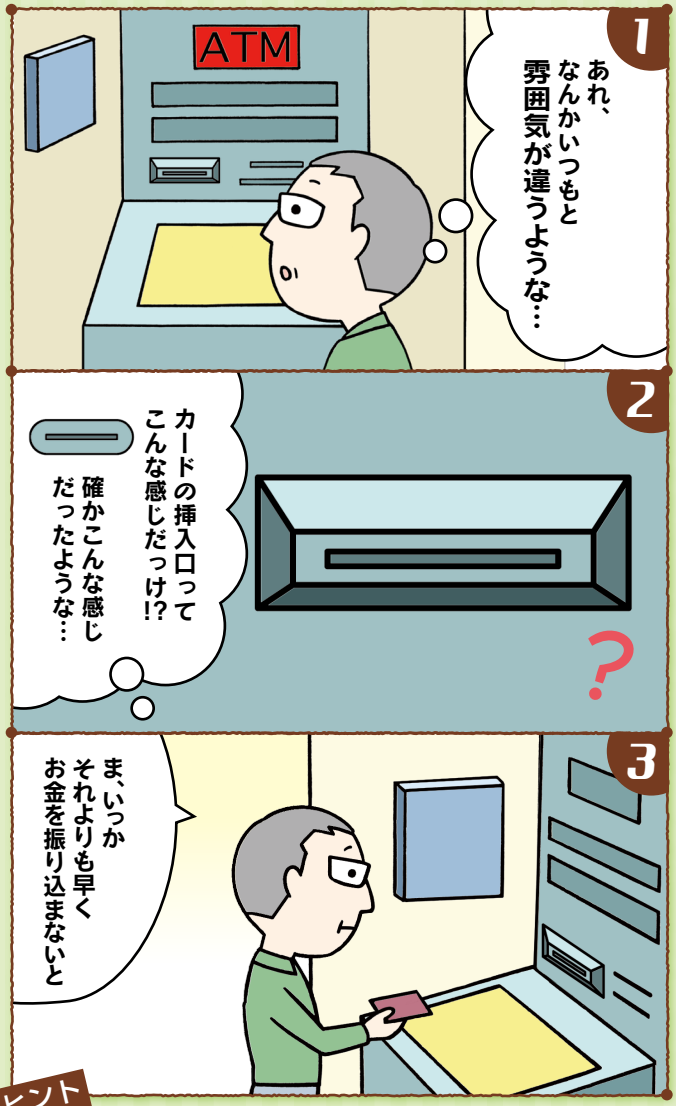
暗証番号を書いたメモなどはもちろん、番号を推測できるようなものを一緒に携帯しないようにしましょう。本人に過失がある場合、被害に遭っても補償の対象にならない場合があります。

さらにここにもご用心！

通帳記入やインターネット・バンキングなどをこまめに行い、残高や不審な引き出しがないかどうかをチェックすることも、被害を大きくしないために大切です。

Q 「身の回り」にご用心！❸

ATMを利用する際に、
どんな用心が必要か
チェックしてみましょう。



ヒント

いつもと様子が違うと感じている
にもかかわらずキャッシュカードを
挿入してよかったのでしょうか？

A これが「キャッシュカードの偽造」です！

キャッシュカードを偽造し現金を引き出す

ATMに設置した
カード読み取り機や、
セーフティボックスに預けた
手荷物から、
キャッシュカードの磁気データ
を盗みます。そのデータから
カードを偽造します。

☑ 用心する「ポイント」はココ！

❶ ATM周辺に不審なものがないか確認する。

ATMのカード挿入口や、暗証番号を盗撮する小型カメラなどがないか確認しましょう。不審に思ったときは利用せず、銀行に問い合わせてみましょう。

❷ キャッシュカードの暗証番号の盗難に注意。

ゴルフ場やホテルなどでセーフティボックスの暗証番号が盗撮され、カード情報を盗難（スキミング）される手口もあります。セーフティボックス利用時の番号は、キャッシュカードの暗証番号とは違う番号にしましょう。

❸ 偽造されにくいカードなどのサービスを活用。

銀行によっては、偽造しにくいICカードや、生体認証カードなどのサービスを提供しています。積極的に活用しましょう。

さらにここにもご用心！

カードを偽造され、暗証番号が盗まれると、知らない間にお金を引き出されます。通帳記入などでこまめに残高を確認しましょう。

一般社団法人
全国銀行協会
WEB https://www.zenginkyo.or.jp/

ご相談は全国銀行協会相談室へ

0570-017109
※一般電話からは、市内通話料金で
ご利用いただけます。
または
TEL 03-5252-3772
受 付 日：月～金曜日
（祝日および銀行の休業日を除く）
受付時間：午前9時～午後5時

令和3年9月版