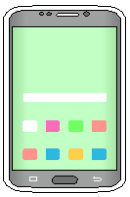
群馬県警察 Gunma Prefectural Police

サイバーポリスニュース

スマートフォンによる決済サービスの不正利用が増加！



スマホ決済（スマートフォンによる決済サービス）の利用者が増加している一方で、スマホ決済サービスに登録したクレジットカードや身に覚えのない商品購入の取引などのサービスの不正利用が多数確認され、警察への相談が増加しています。

マメ知識　スマホ決済の種類

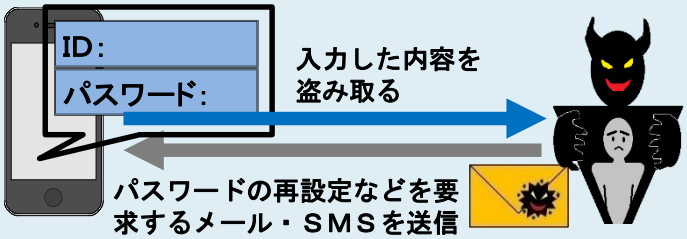
非接触型決済（非接触IC決済）	非接触ICが搭載されたスマートフォンを店舗の読み取り機にタッチしたり、かざすだけで決済できます。
QRコード決済	スマートフォンにインストールしておいたアプリに表示されるQRコードやバーコードを店舗側が読み取ったり、店舗側が用意しているQRコードを自分のスマートフォンで読み取ってから金額を入力することで決済できます。

ご注意ください、スマホ決済サービス不正利用の要因！

要因１　フィッシングによる決済サービスのＩＤ・パスワードの漏洩

犯罪者は、決済サービスのＩＤとパスワードを狙っています。メールやＳＭＳを送信して、メッセージ内のＵＲＬリンクから受信者をフィッシングサイトへ誘導し、認証情報等の入力を求めます。

そこで入力した情報は、全て犯罪者に知られてしまいます。



要因２　ＩＤ・パスワードの使い回し

犯罪者は、不正に入手したＩＤとパスワードをリスト化し、様々なサービスへのログインを試みます。同じＩＤとパスワードの組合わせを複数のサービスで共有していると、決済サービスを含む各種サービスのアカウントを全て乗っ取られてしまう危険があります。

要因３　決済アプリを入れているスマートフォンの紛失

紛失や盗難により、悪意のある第三者の手に渡ってしまうと、決済アプリを不正利用される可能性があります。

メール・ＳＭＳの事例　『ユーザ確認が必要です』、『有効期限が切れています』、『アカウントを一時停止しました』、『残高不足のお知らせ』などがあります。

○　不正利用を防ぐためのチェックポイント！

☑ 情報入力は慎重に	メールやSMSなどから誘導されたサイトでIDとパスワードの入力を求められた時は、正規のサイトかどうかをインターネットなどで確認しましょう。よく利用するサイトはブックマークに登録しておき、そこからアクセスしましょう。
☑ ID・パスワード管理を厳重に	サービスごとに異なるIDとパスワードを使用しましょう。また二要素認証などを設定できる場合は必ず有効にしましょう。
☑ 画面にロック設定	スマートフォンには必ず画面ロックをかけ紛失、盗難時のセキュリティ対策をしましょう。ロック方式には、パスワードやパターン、指紋認証、顔認証などがあります。

＜　群馬県警察サイバーセンター　TEL027-243-0110　＞