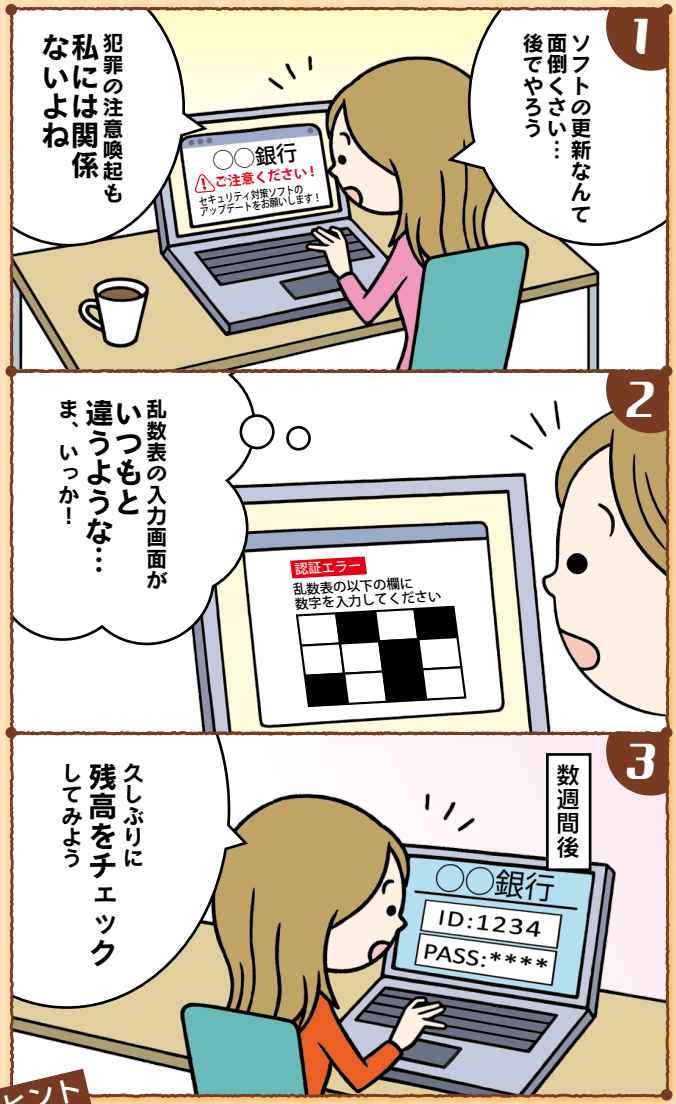
Q 「インターネット犯罪」にご用心！❶

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。