あなたの預貯金が狙われている！

～ネットバンキングの不正アクセス・不正送金事案ついて～

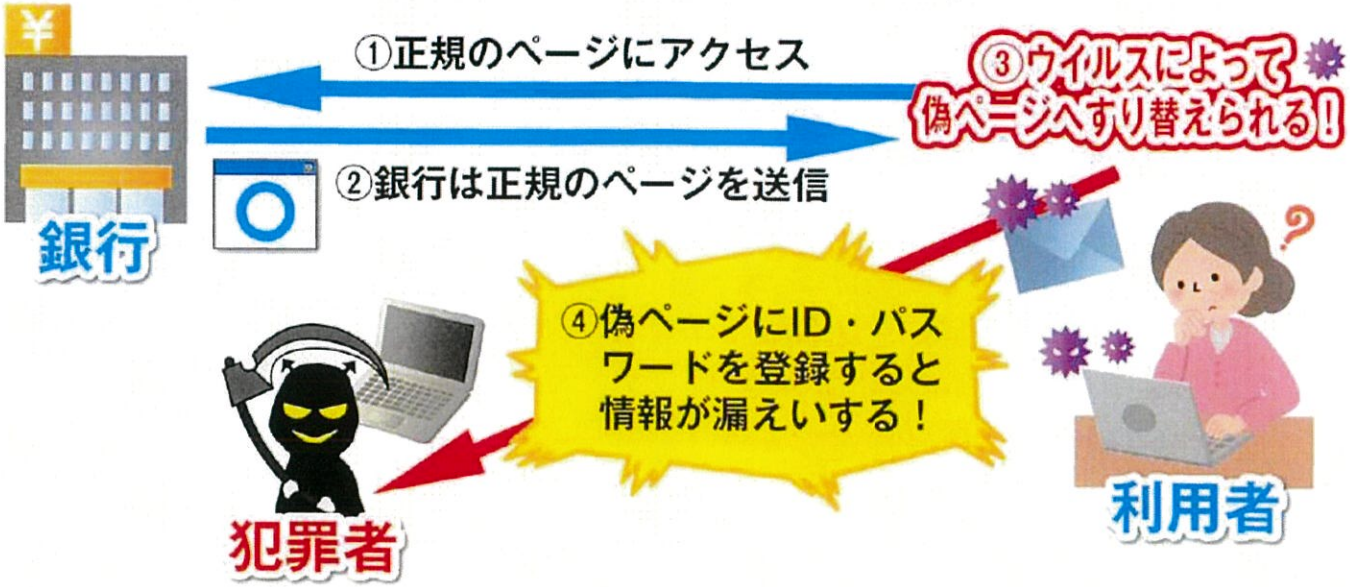
あなたは銀行などが提供している『インターネットバンキング』を利用していますか？

インターネットバンキングは、銀行へ出向くことなく、自宅や職場において残高照会や口座振り込みができる便利なサービスです。

しかし、その利用者の預貯金を狙った犯罪が全国的に発生しており、県内の利用者の被害も確認されております。

代表的な手口としては、利用者のパソコンがコンピュータウイルスに感染していることが原因で、不正に情報を入力させるインターネットバンキングのページが表示され、そこに入力したパスワードなどの情報が漏えいしてしまい、犯罪者に預貯金を奪われてしまうといったものです。

被害に遭わないためにも次に挙げる対策を実施して下さい。



不正アクセス・不正送金事案への対策

- ○ ウイルス対策ソフトの導入と自動更新
- ○ Windows 等の基本ソフト（OS）やウェブブラウザ（IE、Firefox 等）などの各種ソフトウェアを最新の状態にする。
- ○ メーカーサポート期限が経過したソフトウェア（OS を含む）を利用しない。
- ○ パスワード管理の徹底（可能であれば２段階認証の利用）
  ※ 詳しくは「重要なパスワードの管理！」のページを御覧ください。
- ○ 金融機関が提供しているセキュリティ対策を導入する。
（電子署名、フィッシング対策ソフトの導入）

警察の相談窓口

・警察本部警察安全相談窓口
TEL 098-863-9110(又は、プッシュ回線等から#9110)
・各警察署の警察安全相談窓口

いつもと違う画面が表示された場合は、銀行や警察に相談を！

重要なパスワード管理!

ＳＮＳやショッピングサイトなどの利用者から
○　ＳＮＳを乗っ取られて、友人に詐欺メッセージが送られてきた。
○　ショッピングサイトのＩＤを無断で使用され、高額な商品が購入されている。
など、ＩＤとパスワードを無断で使用された不正アクセス事案が発生しています。
ＩＤとパスワードは「印鑑」と同じように重要な役割を果たすものですので、適切に管理するために、次の事項に注意して下さい。

1　推測されやすいパスワードを設定しない

次のようなパスワードは、簡単に推測されやすいパスワードですので、使わないようにしましょう。

- ＩＤから類推できるもの
  例：ＩＤが「okinawa123」で、パスワードが「okinawa123」「okinawa」「123」など
- 利用者と関係のある文字や数字
  例：誕生日、電話番号、自分の名前、車のナンバーなど
- 辞書に載っている単語
  例：「okinawa」「keisatsu」「password」など
- 文字数が短いもの
  ※　最低でも８文字以上の文字数にしましょう。

2　パスワードを厳重に管理する

いくら推測されにくいパスワードを使っていても、他人に教えたり、貸したりすると、そこからパスワードが漏れてしまう可能性がありますので控えましょう。
また、フリーメールなどへメモの代わりとして、様々なＩＤとパスワードを記録した場合、そのメールを不正アクセスされパスワードが漏えいした例もあります。

3　ＩＤ・パスワードを使い回さない

ショッピングサイトやＳＮＳなどのインターネットサービスを利用する際に、同じＩＤとパスワードを使い回すと、漏れてしまった場合に、多くのインターネットサービスで不正アクセスの被害を受ける可能性があります。
インターネットサービスごとに、異なるパスワードを設定しましょう。

4　二段階認証を利用する

ログインするときにパスワードと携帯電話などに送られてくる第二パスワードを求める二段階認証は、万が一パスワードが漏れてしまった場合でも、第二パスワードを知ることができないため、不正アクセスを防ぐことができます。
特に、インターネットバンキングなどの発生すると被害が大きくなるサービスについては、積極的に利用するようにしましょう。

5　被害に遭った場合

パスワードを盗まれた可能性がある場合は、運営会社へ連絡して被害の状況の確認や利用休止などの手続きを行い、警察に相談して下さい。

警察の相談窓口(被害相談)

- 警察本部警察安全相談窓口
  TEL 098-863-9110(又は、プッシュ回線等から#9110)
- 各警察署の警察安全相談窓口