サイバーセキュリティ通信【第13号】

平成29年10月
大分県警察本部 生活安全部
生活環境課 サイバー犯罪対策室

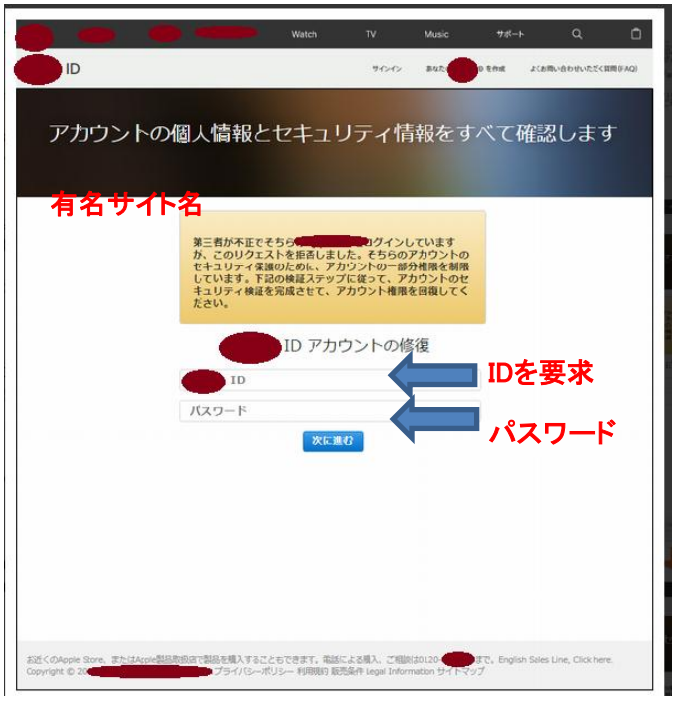
フィッシングサイトに注意を

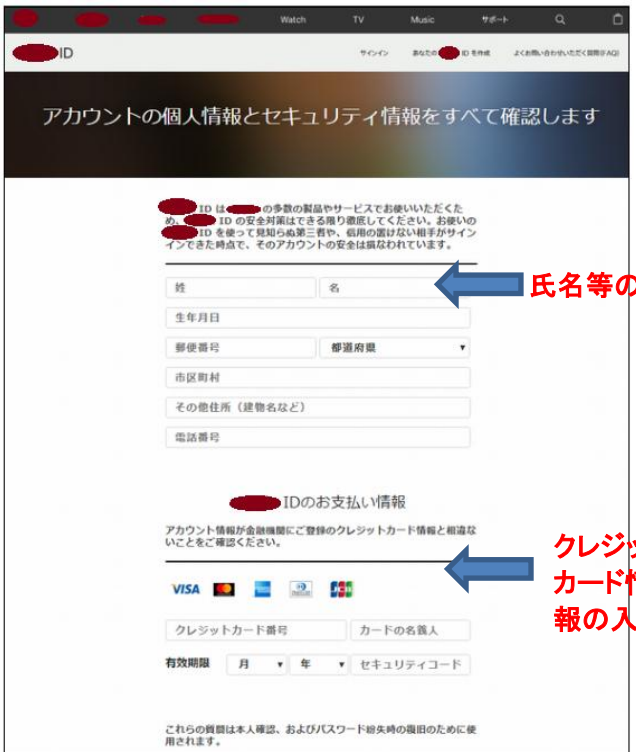
1 フィッシングとは

フィッシングとは、金融機関などの実在する有名企業を装って偽の電子メールを送り付け、メール本文中のリンクから偽のサイトに誘導し、住所、氏名、銀行口座番号、クレジットカード番号、アカウント情報、パスワードなどの個人情報を詐取する犯行のことをいいます。

ここ数年は、大手ショッピングサイトの「Amazon」やインターネット関連会社である「Apple」などの有名企業を装ったフィッシングが多発しており、大分県内でもフィッシングの被害が発生しています。

大分県内で実際に被害にあったフィッシングサイト





2 フィッシングの手口

① 有名企業を装った電子メールが届く
② 電子メールの本文にあるURLをクリックするように誘導される
③ 誘導されたURLをクリックすると、IDとパスワードを要求されるサイトが表示される
④ 名前、住所、クレジットカード番号等の個人情報を入力する画面に移行
⑤ 個人情報を入力して「次へ」のボタンを押したところで、すべて個人のデータが流出
⑥ 流出した個人情報から不正送金被害や架空請求被害等のさらなる被害発生

３　フィッシング対策

①　メールのリンクからアクセスをしない

サイトにアクセスする時は、メール本文にあるURL（リンク）からアクセスするのではなく、お気に入りに登録したアドレスからサイトにアクセスするようにしましょう。

②　ウイルス対策ソフトの導入

ウイルス対策ソフトでは、ウイルスの検知だけでなく、アクセスした先のサイトがフィッシングサイトであるかどかも判断してくれます。ウイルス対策ソフトを導入し、定期的にパターンファイルを更新しましょう。

③　暗号化通信されているかどうかの確認

氏名やクレジットカード番号などの個人情報を入力するサイトの場合、通常、通信を暗号化しています。

暗号化されているかどうかは、URLが「**https://**」から始まっているかどうかを確認して下さい。

「https://」で始まっていれば、暗号化通信が使用されているサイトです。ただの「http」であれば暗号通信されていませんので、このようなサイトに個人情報を入力することは危険です。

「**https**」の「**s**」があるかどうかをしっかりと確認して下さい。

④　慌てず落ち着いた対応

そもそもアカウント情報やクレジットカード番号を入力するような依頼がメールで送られることはありません。

あなたの情報を守れるのはあなたしかいません。慌てず落ち着いて対応しましょう。

⑤　フィッシング被害の情報を入手すること

フィッシング被害の最新情報は、

フィッシング対策協議会

https://www.antiphishing.jp

に掲載されています。

最新の情報を把握して、フィッシング被害に遭わないようにしましょう。

あなたの会社や団体で研修の一環として、サイバーセキュリティカレッジを開催しませんか？
小学生から大人まで幅広く対応できます。下記の連絡先にご相談下さい。

大分県警察本部生活安全部生活環境課サイバー犯罪対策室
サイバーセキュリティ係　　Tel:097－536－2131